Analysis of Digital Evidence in Identity Theft Investigations

Olga Angelopoulou

A submission presented in partial fulfilment of the requirements of the University of Glamorgan / Prifysgol Morgannwg for the degree of Doctor of Philosophy

July 2010
Certificate of Research

This is to certify that, except where specific reference is made, the work described in this thesis is the result of the candidate. Neither this thesis, nor any part of it, has been presented, or is currently submitted, in candidature for any degree at any other University.

Candidate:  ________________________________

Director of Studies:  ________________________________

Date:  ________________________________
To my parents,

Apostolos and Athanasia.

Στους γονείς μου,

Απόστολο και Αθανασία.
Regard your good name as the richest jewel you can possibly be possessed of - for credit is like fire; when once you have kindled it you may easily preserve it, but if you once extinguish it, you will find it an arduous task to rekindle it again. The way to gain a good reputation is to endeavour to be what you desire to appear.

Socrates, Greek philosopher
Acknowledgements

I read somewhere at some point that a PhD is 10% brains, 10% luck and 80% stubbornness and perseverance and it eventually appeared correct, at least in my case. I always find it interesting to read the acknowledgments part of other people’s work. It proves the reader that no piece of work can be achieved with the effort of a single person. It is my turn to be thankful for those who tried to stand by me and support me to this long and demanding journey.

First of anyone else, I need to thank my parents, without them I would be no one. They are those who sacrificed their own wants, in order to sponsorship me and make all my dreams come true, even the wildest ones in my life. Thank you for being who you are. It’s the least I can say, because words are not enough to express my love and respect.

Stelios, the man who stood next to me all those hard days during my research and acted as my tutor. But, it’s not just that. The most important is that he managed to survive my moods and support me psychologically. This is what I needed the most anyway. Probably, I would have either gone crazy or given up without him. Thank you for believing in me.

Dr. Iain Sutherland, my supervisor at the University of Glamorgan, who even if he had a million things in his mind and sort of ‘inherited’ me, we managed to bring this piece of work to an end. Thank you for your help.

DC Tim Williams and Jon Evans, Gwent police, computer crime investigators for their invaluable assistance for applying this work in practice and their precious advice during the design of the research. Thank you very much.

Konstantinos Xynos, co-researcher and office roommate at the University of Glamorgan, for most of the time. He assisted on the framework’s experiment with his specialised knowledge on where to find malware and how to attack systems. Thank you Kosta.

Last but not least, my brother Panos, for being so far and still so close. He should be one of the few that manages to do that with such a success. Thank you bro for being next to me, when I needed you the most.

Thank you all, who were close to me all these years, each one on your own special way of assisting and supporting me. Life is not a one woman’s show anyway!

In life every end has a new beginning... Just because, everything happens for a reason!
Abstract

Identity Theft could be currently considered as a significant problem in the modern internet driven era. This type of computer crime can be achieved in a number of different ways; various statistical figures suggest it is on the increase. It intimidates individual privacy and self assurance, while efforts for increased security and protection measures appear inadequate to prevent it. A forensic analysis of the digital evidence should be able to provide precise findings after the investigation of Identity Theft incidents. At present, the investigation of Internet based Identity Theft is performed on an ad hoc and unstructured basis, in relation to the digital evidence. This research work aims to construct a formalised and structured approach to digital Identity Theft investigations that would improve the current computer forensic investigative practice. The research hypothesis is to create an analytical framework to facilitate the investigation of Internet Identity Theft cases and the processing of the related digital evidence.

This research work makes two key contributions to the subject: a) proposing the approach of examining different computer crimes using a process specifically based on their nature and b) to differentiate the examination procedure between the victim’s and the fraudster’s side, depending on the ownership of the digital media. The background research on the existing investigation methods supports the need of moving towards an individual framework that supports Identity Theft investigations. The presented investigation framework is designed based on the structure of the existing computer forensic frameworks. It is a flexible, conceptual tool that will assist the investigator’s work and analyse incidents related to this type of crime. The research outcome has been presented in detail, with supporting relevant material for the investigator. The intention is to offer a coherent tool that could be used by computer forensics investigators. Therefore, the research outcome will not only be evaluated from a laboratory experiment, but also strengthened and improved based on an evaluation feedback by experts from law enforcement.

While personal identities are increasingly being stored and shared on digital media, the threat of personal and private information that is used fraudulently cannot be eliminated. However, when such incidents are precisely examined, then the nature of the problem can be more clearly understood.
# Table of Contents

Certificate of Research ........................................................................................................ i  
Acknowledgements ............................................................................................................. iv  
Abstract .................................................................................................................................. v  
Table of Contents ................................................................................................................. vi  
List of Tables ......................................................................................................................... xiv  
List of Figures ....................................................................................................................... xvi  
List of Acronyms .................................................................................................................. xviii  
Glossary of key terms .......................................................................................................... xix  
Glossary of the ID theft framework terms ............................................................................... xxi  

Chapter 1 The Problem ......................................................................................................  1  
1.1 Identity and Identity Theft ...........................................................................................  1  
1.2 Legislation and Identity Theft .....................................................................................  4  
1.3 The extent of the problem ..........................................................................................  7  
1.4 The Research Hypothesis .........................................................................................  9  
  1.4.1 Aims and Objectives ............................................................................................  9  
1.5 The Research Methodology ....................................................................................... 10  
  1.5.1 Discussion on research approaches ..................................................................... 10  
  1.5.2 The research plan ................................................................................................. 11  
1.6 Structure of the Thesis .............................................................................................. 13  

Chapter 2 State of the Art ................................................................................................. 14  
Overview ............................................................................................................................. 14  
2.1 Computer Crime, Computer Forensics and Digital Evidence .................................. 15  
  2.1.1 Computer Crime .................................................................................................. 15  
  2.1.2 Computer Forensics ............................................................................................ 16
2.1.3 Digital Evidence……………………………………………………………………..17
2.2 Identity Theft in the Digital Environment ……………………………………..19
  2.2.1 Traditional ID Theft……………………………………………………………………..20
  2.2.2 Innovative ID Theft……………………………………………………………………..21
    2.2.2.1 Online ID Theft Techniques…………………………………………………………..22
    2.2.2.3 Offline ID Theft Techniques ……………………………………………………………..28
  2.2.3 Internet Fraud, Identity Theft and its Forms ……………………………………32
2.3 Identity Theft Response ……………………………………………………………37
  2.3.1 Recommendations for Prevention and Detection……………………………..37
  2.3.2 Issues on Detecting and Investigating ID Theft Cases ……………………..40
2.4 Forensic Investigation of Online ID Theft………………………………………43
  2.4.1 The Theory of ID theft investigation …………………………………………………..43
  2.4.2 The Practice of ID theft investigation …………………………………………………..43
2.5 Computer Forensics Frameworks and Methodologies ……………………..48
  2.5.1 Carrier and Spafford ………………………………………………………………………..50
  2.5.2 Casey ……………………………………………………………………………………….52
  2.5.3 Reith et al. …………………………………………………………………………………….52
  2.5.4 Beebe and Clark …………………………………………………………………………….53
  2.5.5 U.S. Department of Justice ………………………………………………………………..54
  2.5.6 Association of Chief Police Officers (ACPO) ………………………………………….55
  2.5.7 Discussion on the existing frameworks and methodologies ………………..56
    2.5.7.1 Specific frameworks/ guidelines ……………………………………………………..61
    2.5.7.2 Limitations and properties of the ID theft investigation framework ……63
Summary ………………………………………………………………………………………….66
Chapter 3 ID Theft Investigation Framework Outline …………………………..67
Overview ……………………………………………………………………………………….67
  3.1 The significance of ID Theft standalone investigation ……………………………..68
3.2 Design Principles ................................................................. 73
3.3 ID Theft Investigation Framework Design ................................. 75
  3.3.1 High Level structure of the ID Theft Investigation Framework .... 75
    3.3.1.1 Inputs and Outputs ......................................................... 77
  3.3.2 Low Level structure of the ID Theft Investigation Framework ... 78
    3.3.2.1 Practitioners’ requirements gathering ............................. 78
    3.3.2.2 The structure of the framework ....................................... 79
Summary ....................................................................................... 84

Chapter 4 The ID Theft Investigation Framework ......................... 85
Overview ....................................................................................... 85
4.1 High Level Inputs and Outputs .................................................. 86
4.2 Overview of the Low Level ID Theft Investigation Framework ...... 89
  4.2.1 Summary of High Level stages and Example Scenario ............ 92
4.3 Structure of the Low Level Analysis .......................................... 94
4.4 Phase 1, Media Analysis .......................................................... 96
  4.4.1 Phase 1 Overview .............................................................. 96
  4.4.2 Digital Media ....................................................................... 97
    4.4.2.1 Process 1, Source Identification ....................................... 98
    4.4.2.2 Process 2, Digital Media Collection .................................. 101
    4.4.2.3 Process 3, Image Acquisition ........................................... 102
  4.4.3 ID Theft Data ................................................................. 104
    4.4.3.1 Process 4, Evidential Data Identification .......................... 104
    4.4.3.2 Process 5, Target Identification ......................................... 106
    4.4.3.3 Process 6, Threat Agent Identification/ Intention ............... 108
4.5 Phase 2, Evidence Analysis ..................................................... 109
  4.5.1 Phase 2 Overview .............................................................. 109
  4.5.2 ID Theft Data Analysis ....................................................... 112
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5.2.1 Process 7, Data Analysis</td>
<td>112</td>
</tr>
<tr>
<td>4.5.2.2 Process 8, Target Analysis</td>
<td>114</td>
</tr>
<tr>
<td>4.5.2.3 Process 9, Threat Agent Analysis</td>
<td>123</td>
</tr>
<tr>
<td>4.5.3 Evidence</td>
<td>125</td>
</tr>
<tr>
<td>4.5.3.1 Process 10, Evidence Collection</td>
<td>126</td>
</tr>
<tr>
<td>4.5.3.2 Process 11, Evidence Categorisation</td>
<td>128</td>
</tr>
<tr>
<td>4.6 Phase 3, Scenario Construction</td>
<td>131</td>
</tr>
<tr>
<td>4.6.1 Phase 3 Overview</td>
<td>131</td>
</tr>
<tr>
<td>4.6.2 Evidence Classification</td>
<td>133</td>
</tr>
<tr>
<td>4.6.2.1 Process 12, Structure of Evidential Data</td>
<td>133</td>
</tr>
<tr>
<td>4.6.2.2 Process 13, Structure Threat Agent's Profile</td>
<td>136</td>
</tr>
<tr>
<td>4.6.2.3 Process 14, Structure Analysed Digital Evidence</td>
<td>138</td>
</tr>
<tr>
<td>4.6.3 Scenario</td>
<td>139</td>
</tr>
<tr>
<td>4.6.3.1 Process 15, Scenario Outline</td>
<td>140</td>
</tr>
<tr>
<td>4.6.3.2 Process 16, Scenario Preparation Documentation</td>
<td>140</td>
</tr>
<tr>
<td>4.7 Phase 4, Evaluation</td>
<td>142</td>
</tr>
<tr>
<td>4.7.1 Phase 4 Overview</td>
<td>142</td>
</tr>
<tr>
<td>4.7.2 Scenario Examination</td>
<td>143</td>
</tr>
<tr>
<td>4.7.2.1 Process 17, Scenario Testing/ Evaluation</td>
<td>144</td>
</tr>
<tr>
<td>4.7.2.2 Process 18, Scenario Clarification</td>
<td>145</td>
</tr>
<tr>
<td>4.7.3 Case</td>
<td>146</td>
</tr>
<tr>
<td>4.7.3.1 Process 19, Case Construction</td>
<td>146</td>
</tr>
<tr>
<td>4.7.3.2 Process 20, Case Clarification</td>
<td>147</td>
</tr>
<tr>
<td>4.7.3.3 Process 21, Case Evaluation</td>
<td>147</td>
</tr>
<tr>
<td>4.7.3.4 Process 22, Evidential Case Representation</td>
<td>148</td>
</tr>
<tr>
<td>Summary</td>
<td>150</td>
</tr>
</tbody>
</table>
Chapter 5 Framework Verification and Assessment .......................... 152

Overview .................................................................................................. 152

5.1 Evaluation Objectives.............................................................................. 153

5.1.1 Chosen evaluation methods............................................................. 154

5.1.1.1 Evaluation Experiment .............................................................. 154

5.1.1.2 Police Review ........................................................................... 154

5.2 Evaluation Experiment ........................................................................ 155

5.2.1 Aim of the evaluation...................................................................... 155

5.2.2 Sources of data for the scenario ...................................................... 156

5.2.2.1 Evaluation Scenario .................................................................. 158

5.2.3 Evaluation Experiment Decisions.................................................... 161

5.3 Police Review ..................................................................................... 165

5.3.1 Aim of the interview ..................................................................... 165

5.3.2 General questions on ID Theft investigations ............................... 166

5.3.3 Specific questions on the methodology........................................... 167

Summary .................................................................................................. 169

Chapter 6 Evaluation of experiments ................................................ 170

Overview .................................................................................................. 170

6.1 Application of Laboratory Experiment ............................................. 171

6.2 V. Victim ........................................................................................... 172

6.2.1 Phase 1: Media Analysis ............................................................... 172

6.2.1.1 Summary of Pma .................................................................... 172

6.2.1.2 Digital Media .......................................................................... 172

6.2.1.3 ID Theft Data Identification ................................................... 176

6.2.2 Phase 2: Evidence Analysis ........................................................... 179

6.2.2.1 Summary of Pea .................................................................... 179

6.2.2.2 ID Theft Data Analysis ........................................................... 179
6.2.2.3 Evidence.................................................................................. 186
6.2.3 Phase 3: Scenario Construction................................................. 189
  6.2.3.1 Summary of Psc.................................................................. 189
  6.2.3.2 Evidence Classification...................................................... 189
  6.2.3.3 Scenario............................................................................ 193
6.2.4 Phase 4: Evaluation .................................................................. 195
  6.2.4.1 Summary of Pe .................................................................. 195
  6.2.4.2 Scenario Examination......................................................... 196
  6.2.4.1 Case.................................................................................. 197
6.3 F. Fraudster .................................................................................. 200
6.4 Discussion of the results.............................................................. 206
6.5 Presentation of expert review ...................................................... 208
  6.5.1 Expert Review...................................................................... 209
  6.5.2 Discussion on the expert review .............................................. 215
    6.5.2.1 Evaluation issues on the field expert review ...................... 217
6.6 The properties of the framework ............................................... 218
Summary .......................................................................................... 220
Chapter 7 Conclusion and further research ..................................... 222
Summary .......................................................................................... 222
7.1 Contribution to science.............................................................. 223
  7.1.1 The research objectives......................................................... 224
  7.1.2 Project Review.................................................................... 225
7.2 Further Research ........................................................................ 227
7.3 Conclusion ................................................................................ 229
References ...................................................................................... 231
Appendices ...................................................................................... 249
Appendix A: .................................................................................... A1
<table>
<thead>
<tr>
<th>Phase 1: Media Analysis</th>
<th>Phase 2: Evidence Analysis</th>
<th>Phase 3: Scenario Construction</th>
<th>Phase 4: Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix G:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Level Flowchart</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix H:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abstracted procedure for the investigator</td>
<td>Examination of the evidence</td>
<td>Interpretation of the evidence</td>
<td>Validation of the Evidence</td>
</tr>
<tr>
<td>Appendix I:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documenting Procedure for the investigator</td>
<td>Appendix J:</td>
<td>Gwent Police Review</td>
<td></td>
</tr>
<tr>
<td>Appendix K:</td>
<td></td>
<td>Gwent Police e-mail communication</td>
<td></td>
</tr>
<tr>
<td>Appendix L:</td>
<td></td>
<td>EnCase Victim Report</td>
<td></td>
</tr>
<tr>
<td>EnCase Fraudster Report</td>
<td></td>
<td>Victim Investigation - Evidential Files ScreenShots</td>
<td></td>
</tr>
<tr>
<td>Appendix M:</td>
<td></td>
<td>EnCase Fraudster Report</td>
<td></td>
</tr>
<tr>
<td>Fraudster Investigation - Evidential Files ScreenShots</td>
<td>Appendix N:</td>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>
List of Tables

Table 1: Summary of the ID theft Techniques .......................................................... 19
Table 2: ID Theft classification as appears in literature ......................................... 36
Table 3: Disks obtained / analysed ........................................................................ 45
Table 4: Origin of disks investigated ....................................................................... 45
Table 5: Type of information on Residual disks .................................................... 45
Table 6: Personal identity information useful for identity theft ............................. 46
Table 7: Frameworks’ Comparison Table ............................................................... 60
Table 8: Process 1 - Source Identification .............................................................. 101
Table 9: Process 2 - Digital Media Collection ...................................................... 102
Table 10: Process 3 - Image Acquisition .............................................................. 103
Table 11: Process 4 - Evidential data identification .............................................. 106
Table 12: Process 5 - Target identification ............................................................ 108
Table 13: Process 6 - Threat Agent identification / intention ................................ 109
Table 14: Process 7 - Data Analysis .................................................................... 114
Table 15: Process 8 - Target Analysis (V. Victim) ............................................... 119
Table 16: Process 8 - Target Analysis (F. Fraudster) ........................................... 123
Table 17: Process 9 - Threat Agent Analysis ....................................................... 125
Table 18: Process 10 - Evidence Collection ......................................................... 128
Table 19: Process 11 - Evidence Categorisation ................................................... 130
Table 20: Process 12 - Structure of evidential data .............................................. 135
Table 21: Process 13 - Structure Threat Agent’s profile ...................................... 138
Table 22: Process 14 - Structure analysed digital evidence ................................ 139
Table 23: Process 15 - Scenario Outline ............................................................... 140
Table 24: Process 16 - Scenario Preparation Documentation ............................... 141
Table 25: Process 17 - Scenario Testing / Evaluation ................................. 144
Table 26: Process 18 - Scenario Clarification ........................................... 145
Table 27: Process 19 - Case Construction ................................................ 146
Table 28: Process 20 - Case Clarification ............................................... 147
Table 29: Process 21 - Case Evaluation .................................................. 148
Table 30: Process 22 - Evidential Case Representation ............................. 149
Table 31: Systems’ Specifications ......................................................... 156
Table 32: Victim’s applications and utilities installed ................................. 162
Table 33: Fraudster’s applications and utilities installed ............................ 162
Table 34: Pma - Digital Media Documenting procedure ......................... 175
Table 35: Pma - ID Theft Data Identification Documenting procedure ........ 178
Table 36: Pea - ID Theft Data Analysis Documenting procedure ............... 186
Table 37: Pea - Evidence Documenting procedure ................................... 189
Table 38: Pea - Evidence Classification Documenting Procedure .............. 193
Table 39: Psc - Scenario Documenting Procedure ................................... 195
Table 40: Pe - Scenario Examination Documenting procedure .................. 197
Table 41: Pe - Case Documenting Procedure ......................................... 199
Table 42: The accomplishment of the framework's properties ................. 218
Table 43: Design issues met ................................................................. 221
Table 44: Research Objectives ............................................................. 224
Table 45: Decision making questions and answers .................................. 226
List of Figures

Figure 1: Disk Capacity percentages .............................................................. 44
Figure 2: ID Theft Investigation Framework Phases ........................................ 76
Figure 3: Investigation Framework Variables’ and representation ..................... 77
Figure 4: The input / output practice ............................................................. 78
Figure 5: Representation of the framework's elements (lowest level)................. 80
Figure 6: ID Theft Framework Complexity (see App.-II) .................................. 82
Figure 7: ID Theft Framework Relationships (see App.-III) ............................. 83
Figure 8: Phase 1 - Media Analysis ............................................................. 87
Figure 9: Phase 2 - Evidence Analysis .......................................................... 87
Figure 10: Phase 3 - Scenario Construction ................................................... 88
Figure 11: Phase 4 - Evaluation .................................................................. 88
Figure 12: Phase 1, Media Analysis Representation (Low Level) ....................... 89
Figure 13: Phase 2, Evidence Analysis Representation (Low Level) .................. 90
Figure 14: Phase 3, Scenario Construction Representation (Low Level) .......... 91
Figure 15: Phase 4, Evaluation Representation (Low Level) ........................... 91
Figure 16: Phase 1 - Media Analysis Breakdown ........................................... 97
Figure 17: Relationships between phases 1 and 2 ....................................... 109
Figure 18: Phase 2 - Evidence Analysis Breakdown ..................................... 111
Figure 19: Relationships among phases 1, 2 and 3 .................................... 131
Figure 20: Phase 3 - Scenario Construction Breakdown ............................... 132
Figure 21: Relationships among phases 1, 2, 3, 4 ....................................... 142
Figure 22: Phase 4 - Evaluation ................................................................. 143
Figure 23: Processes that contribute on defeating the defence ....................... 148
Table 30: Process 22 - Evidential Case Representation ............................... 149
Table 31: Systems' Specifications ................................................................. 156
Figure 24: Graphical Representation of the research experiment and its parts. 158
Figure 25: Scenario Representation ............................................................ 160
Figure 26: Stages of the experiment execution ........................................... 163
Figure 27: Decision making procedure ...................................................... 225
Figure 28: Phishing e-mail example ........................................................... D4
Figure 29: Defrauded PayPal web page I .................................................... D5
Figure 30: Defrauded PayPal web page II .................................................. D6
Figure 31: PayPal login confirmation ......................................................... D6
Figure 32: Web transaction during a Web spoofing attack ......................... D9
Figure 33: Victim's Hash Value ................................................................. L3
Figure 34: perfnw.dll ............................................................................... L4
Figure 35: e-mail addresses ..................................................................... L5
Figure 36: My Documents folder ............................................................. L6
Figure 37: Fraudster's Internet Bookmarks .............................................. M4
Figure 38: Victim's log on fraudster's system .......................................... M5
Figure 39: malware.zip file from plugged in device ................................ M6
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACPR</td>
<td>Australasian Centre for Policing Research</td>
</tr>
<tr>
<td>APWG</td>
<td>Anti-Phishing Working Group</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed circuit television</td>
</tr>
<tr>
<td>CIFAS</td>
<td>Credit Industry Fraud Avoidance System</td>
</tr>
<tr>
<td>DFRWS</td>
<td>Digital Forensics Research Workshop</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>ERD</td>
<td>Entity Relationship Diagram</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>ID theft</td>
<td>Identity Theft</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>I.T.</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITRC</td>
<td>Identity Theft Resource Centre</td>
</tr>
<tr>
<td>O.S.</td>
<td>Operating System</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio frequency identification</td>
</tr>
<tr>
<td>SOCA</td>
<td>Serious Organised Crime Agency</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>U.K.</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Modelling Language</td>
</tr>
<tr>
<td>UoG</td>
<td>University of Glamorgan</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>U.S.</td>
<td>United States</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
</tbody>
</table>
## Glossary of key terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus software</td>
<td>Program that aims to detect and remove computer viruses and malware</td>
</tr>
<tr>
<td>Bots</td>
<td>Programs that execute automated tasks</td>
</tr>
<tr>
<td>Browser helper object</td>
<td>BHO - A component of the Internet Explorer web browser created for added functionality. Some malware have been created as BHOs.</td>
</tr>
<tr>
<td>Browser hijacking</td>
<td>Browser information stealing</td>
</tr>
<tr>
<td>Collection Technique</td>
<td>The method of accumulation</td>
</tr>
<tr>
<td>Computer Forensics</td>
<td>The science that deals with computer collection, investigation and analysis techniques</td>
</tr>
<tr>
<td>Digital Data</td>
<td>Information that can be stored and used by a computer</td>
</tr>
<tr>
<td>Firewall</td>
<td>A software program or a hardware device designed to protect a computer system or network from unauthorized access</td>
</tr>
<tr>
<td>Fraudster</td>
<td>A person acting with deceptive intentions. Also referred as criminal, perpetrator</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>The crime that fraudulently uses private information without the owner’s knowledge</td>
</tr>
<tr>
<td>Incident</td>
<td>An event or occasion</td>
</tr>
<tr>
<td>Integrity</td>
<td>The state of being complete, integrated</td>
</tr>
<tr>
<td>Investigation</td>
<td>The thorough and systematic analysis of a matter</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Liability</td>
<td>The state of being legally responsible</td>
</tr>
<tr>
<td>Malicious Software / Malware</td>
<td>Software that is able to exploit vulnerabilities in a computer system</td>
</tr>
<tr>
<td>Private information</td>
<td>Personal information</td>
</tr>
<tr>
<td>Procedure</td>
<td>A series of activities performed in a precise way</td>
</tr>
<tr>
<td>Rootkit</td>
<td>A software tool that fraudulently gains unauthorised administrator level access to a system</td>
</tr>
<tr>
<td>Security Policy</td>
<td>A set of rules and guidelines written for the secure control of a system or organisation</td>
</tr>
<tr>
<td>Timestamp</td>
<td>The identifier that denotes the date/time alteration to a file</td>
</tr>
<tr>
<td>Verification</td>
<td>The demonstration of accuracy</td>
</tr>
<tr>
<td>Victim</td>
<td>A person who is deceived. Also referred as target</td>
</tr>
<tr>
<td>Zombie machine</td>
<td>A compromised by an attacker machine that is used remotely for malicious actions without the owner’s knowledge</td>
</tr>
</tbody>
</table>
Glossary of the ID theft framework terms

Activity
A customised, focused ID theft guideline that clarifies the required actions set by the processes

Evaluation
The phase of the framework that assesses the results of the examination

Evidence Analysis
The phase of the framework that analyses the digital media for evidence

Input
The criteria that should be satisfied for the phase to operate

Instruction
an internal, further detailed degree of direction that follows an activity

Media Analysis
The phase of the framework that contacts the crime scene and acquires the digital media

Objective
The declaration of an instruction

Output
The result of the criteria satisfied in the input

Phase
An individual procedural component inside the framework

Process
A centralised, structured approach for the satisfaction of the I/O

Scenario Construction
The phase of the framework that the evidence is categorised and a scenario outlined
In this chapter the reader can find

- the definition and extension of ID theft;
- the research aims and objectives;
- the research methodology;
- the outline of the thesis.

1.1 Identity and Identity Theft

The fraudulent use of another person’s personal details has become an increasingly significant concern. One million Internet shoppers were Internet fraud victims on 2004 (Hinde, 2004b), 8.3 million American adults victims in 2005 (Goodin, 2007), while one in ten Britons was a victim in 2006 (Taylor, 2006). Attacks on financial institutions have risen from 39% in 2003 to 83% for 2004 (McKenna, 2004). In the UK fraud on plastic cards on 2003 cost £402 million (Cybersource, 2004). According to the ITRC (2009), there was a 47% increase in data breaches comparing to them in 2007. In addition, Identity Theft was the first among a list of twenty consumer complaints in 2008 in the United States receiving 26% (FTC, 2009). While the British population is approximately 61 million people, in March 2008 the number of National Insurance numbers was 76.8 million. (CIFAS, 2009)

The following sections examine the issues surrounding the techniques involved in the investigation of the theft of an individual’s identity from a computer system over the Internet. In order to comprehend the nature of this research, there are a number of important terms which need to be clearly defined. These are quoted below. The definitions’ meanings of the words that are of importance to this thesis are indicated first.
Identity is defined as:

\[
\text{noun (pl. identities)} \quad \text{the characteristics determining who or what a person or thing is} \quad (\text{The Oxford Dictionary of English})
\]

Theft is defined as:

\[
\text{mass noun} \quad \text{the action or crime of stealing: he was convicted of theft} \quad (\text{The Oxford Dictionary of English})
\]

The growth in identity related fraud resulted in the need for the establishment of specific terminology in order to identify this particular type of crime. Identity Theft is defined by the Home Office (2009) as:

Criminals can find out your personal details and use them to open bank accounts and get credit cards, loans, state benefits and documents such as passports and driving licenses in your name.

A paraphrased definition could be:

Identity theft is the use of your personal identity in the form of personal information by another individual for their financial gain.

However, it may be argued that the gain is not necessarily always financial. Identity Theft may be aimed at satisfying some other objective; espionage, terrorism, revenge, illegal immigration or assuming a new identity to avoid criminal charges (Newman and McNally, 2005). However it is generally accepted that the end objective of Identity Theft is usually some form of financial gain as suggested by Gerard G. J. et al. (2004a), who defined it as:

Identity theft is the criminal act of assuming the identity of another person with the expectation of gain. The gain is normally financial as a result of improperly extending credit, allowing banking transactions, establishing cellular telephone or other utility service, or gaining governmental benefits.

The ITRC (2003) argued amongst others that Identity Theft is a high profit, low risk, low penalty crime.
The problem

The FTC (2007) describes it as:

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

Therefore, based on the above and for the purpose of this thesis, ID theft can be defined as someone’s action of using any sort of distinct personal private information with fraudulent intention; mainly for financial gain.

ID theft is part of the broader term Identity Fraud. The terms are quite often confused and used improperly. Sproule and Archer (2006) differentiate the terms and give the following definition for Identity Fraud:

Identity fraud is the subsequent crime when a false identity is used in order to gain goods, services, benefits or avoid obligations.

ID theft engages the actual theft of someone’s identity and often leads to Identity Fraud that deals with the actual fraudulent action. The Home Office (2009) gives the following definition for Identity Fraud

...the use of that stolen identity in criminal activity to obtain goods or services by deception. Stealing an individual’s identity does not, on its own, constitute identity fraud and this is an important distinction.

The ACPR (2004), defines Identity Fraud as

the gaining of money, goods, services or other benefits through the use of a false identity.

The above definitions include both individuals and corporations. The theft of corporate identity, while arguably resulting in a larger financial loss, is less frequent than the theft of an individual’s identity; Smiley (2004) defines it as:

Corporate identity fraud is the wrongful taking of the identity of a corporation.

Moreover, any type of crime that deals with forged identities is referred to as Identity Crime. According to the Home Office (2009), Identity Crime is

a generic term for identity theft, creating a false identity or committing identity fraud.
The above definitions aim to distinguish the fine line between ID theft and ID fraud. Identity Theft is the main interest and purpose of this research and it should not be confused with Identity Fraud. Based on the above definitions, the theft of someone’s private information usually leads to fraud.

1.2 Legislation and Identity Theft

In 1999 CIFAS recorded 9,000 Identity Fraud cases in the UK, in 2001 there were 24,000 cases, in 2003 46,000 and in 2007 the number increased to 77,500 cases (CIFAS, 2009). As the number of incidents has increased, a number of countries have enacted legislation in relation to ID theft in an attempt to protect potential victims and deter the fraudsters. One current problem is that there is considerable variation in the legislation, so an action that is considered as legal in the U.K. might be illegal in China (Mintz, 2002). Another difficulty is the rapid transformation of technology and methods that are used from cybercriminals.

The following paragraphs discuss the legislative measures in the UK and the US and the recent legislative addition of the E.U. Both the UK and the US present extensive research and statistical results in literature concerning ID theft. For this reason, data and the law from the US are chosen for comparison and discussion in addition to the UK, where the research takes place, and so is the main focus for the research.

Personal information is protected under the Data Protection Act 1998 in the UK. This Act deals with the manipulation of personal information from an organisation.

An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. (Data Protection Act, 1998)

Potentially, it protects personal information that could be used in an ID theft incident. The legislation has been adopted in a way to cover and protect victims of ID theft. The Fraud Act 2006 is a criminal offence in the UK since January 2007. The purpose of this Act as stated in its introduction is:
An Act to make provision for, and in connection with, criminal liability for fraud and obtaining services dishonestly. (Fraud Act, 2006)

It is the first UK anti-fraud legislation and the sentences for the offences can lead to a maximum of ten years imprisonment. The Act is divided into three sections that explain how fraud is committed:

- Fraud by false representation
- Fraud by failing to disclose information and
- Fraud by abuse of position.

In addition, the Act creates offences for possession, making or supplying articles for use in frauds, participating in fraudulent business and obtaining services dishonestly.

Furthermore, the UK introduced the Identity Cards Act 2006 that aims to limit the number of fraudulent identities.

An Act to make provision for a national scheme of registration of individuals and for the issue of cards capable of being used for identifying registered individuals; to make it an offence for a person to be in possession or control of an identity document to which he is not entitled, or of apparatus, articles or materials for making false identity documents; to amend the Consular Fees Act 1980; to make provision facilitating the verification of information provided with an application for a passport; and for connected purposes. (Identity Cards Act, 2006)

The offences under the Identity Cards Act include the possession of false identity documents, unauthorised disclosure of information, providing false information and tampering with the Register. This Act not only makes law the Identity Cards, but also refers to the use of any type of personal identification document that could be used fraudulently.

However, the identity card scheme was abandoned on May 2010 for the UK and European Union nationals. The intention is to reduce the control of the state over decent, law-abiding people and hand power back to them (Identity and Passport Service, 2010).
Nonetheless, ID theft is a global problem. The majority of countries around the world have enacted laws in order to protect their citizens from ID theft and punish fraudsters at the same time.

In the United States, it is considered a standalone crime since 1998 as defined in the Identity Theft and Assumption Deterrence Act (1998) and belongs to federal crimes, where the establishment of the Offence is made as follows:

- knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.

In the H.R. 2622, Fair and Accurate Credit Transactions Act of 2003, the American Identity Theft legislation provides the state approach of combating ID theft and protecting the consumers. Based on the U.S. Federal Trade Commission’s (FTC) report for National and State Trends in Fraud and Identity Theft (2004), of the 635,173 complaints received, 246,570 were ID theft reports. The most common form of reported ID theft was credit card fraud, followed by phone or utilities fraud, bank and employment fraud. It is very important to note that only 30% of victims notified a police department. It can therefore be assumed that the majority of people are either reluctant to contact law enforcement agencies preferring not to make their ID theft incident known or they are not aware of the crime at all.

The European Union adopted the Stockholm programme in 2009 that among others includes the criminalisation of ID theft. The legislation is planned to become active in 2012. The same programme will review the 1995 EU Data Protection Directive that handles data protection and security in Europe (European Commission, 2010). Because the legislation is not active yet, there is not enough information published about it.

The E.U. consists of countries with different legislative backgrounds and some of them only recently joined the Union. This fact urges the need of creating a European-wide legislation for protecting the member countries. At the same time it shows that ID theft is a problem that needs to be covered by law also for the citizens of the E.U.
The US due to its large population and high ID theft incidents number designed an ID theft specific Act. It shows the importance and the severity of this type of crime that it needs specialised treatment and is considered as a standalone crime. The number of Identity Fraud victims in the US was over 11 million people in 2009 (Javellin Strategy and Research, 2010) showing a rise from previous years. Even though the US attempted first to punish ID theft with a maximum imprisonment period of 15 years, it didn’t manage to regulate it while the number of incidents continued to increase.

On the contrary, the UK aims to control the situation by initially embedding ID theft in legislation for data protection. This was an attempt at controlling ID theft. It only became a criminal offence a few years ago with the Fraud Act 2006. However, the intensity of the problem required legislation that concentrates on its control by forcing stronger measurements against it.

It seems appropriate to find out how ID theft occurs and how the era of the Internet-based world has resulted in an increase. This will lead the reader to understand how the evidence traces that may be left behind after an ID theft incident should be used and the role of the computer forensics investigator.

1.3 The extent of the problem

Some statistical data that influence the financial value of transactions on computer systems are listed below in order to represent the severity of the situation:

- An average bank robbery can be about $5000, while a computer identity thief can extract more than 10 times this amount daily, without leaving evidence and the crime is usually discovered months later. (Hammond, 2003)
- ID theft can take to victims up to 300 hours attempts for dealing with banks and credit cards. (Porter, 2004)
- Fraud is estimated to cost the UK at least £13.9 billion a year. (Levi et al., 2007)
- The Federal Trade Commission (FTC) received about 215,000 complaints for ID theft in 2003 that is the largest consumer complaint category (42%) and represents 249% growth from 2001. (CyberTrust, 2005)
• During December 2008 there were 31,173 web sites detected that were infecting computers with password stealing malware. At the beginning of the same year, January 2008, this number was 827% lower. (APWG, 2008)

• In 2007 losses from plastic card fraud cost the UK £535.2 million, while £34.1 million was related to card identity theft. (CIFAS, 2009)

• The Identity Fraud Steering Committee (2008) estimated that ID Fraud costs the UK economy £1.2 billion or £25 per adult each year.

It is fairly difficult to prevent ID theft incidents. Saunders and Zucker (1999) describe it as a neoteric crime (new crime) and emphasize its magnitude. ID theft has a significant human component being strongly influenced by the way people treat personal information. When an individual discovers he/she is an ID theft victim, their personal details have been already used fraudulently (Dwan, 2004). It also seems that most fraudsters of this kind of crime are not acting individually, but rather organised and well equipped. Indeed ID theft is nowadays directly linked to drug trafficking, money laundering and terrorism. (Collins, 2003)

The research presented in this thesis is directed towards:

• developing a detailed understanding of ID theft and its key characteristics;
• distinguishing computer and Internet related crime investigations according to their nature;
• the creation of a computer forensics investigation framework that focuses on the handling of ID theft incidents.
1.4 The Research Hypothesis

ID theft increasingly has the potential to have a significant impact on people and requires a specific method of analysis, therefore:

It is proposed to create an analytical framework to facilitate the investigation of Internet Identity Theft cases and the processing of the related digital evidence.

This will enable the investigator / forensic analyst to:

- Successfully identify evidence related to Identity Theft cases.
- Assess the capabilities required from the perpetrator.
- Effectively assess the ongoing threat to the victim.

The construction of a formalized and structured approach that would assist the investigative practice is considered valuable, as this would enhance the identification and preservation of evidence. The practitioners could modify the examination procedure of ID theft with a focused crime specific framework.

When an ID theft crime is discovered, the case will need supportive and structured guidance to be resolved promptly and mitigate further problems. The research outcome of this work is an analytical framework for digital investigation of online ID theft intending to inform and guide the practice of the computer forensics professional. In the existing literature such a framework has not been identified.

1.4.1 Aims and Objectives

The aim of this research is to develop a framework for the forensic investigation of ID theft incidents. In order to achieve this, the following key objectives have been constructed:

1) Analyse the state of the art in order to identify and investigate the different types of Identity Theft.
2) Develop a conceptual framework for analysing the process of Identity Theft investigation and assess the digital evidence.
3) Evaluate the framework based on case studies and expert opinion in order to assess the proposed framework’s impact on processing online Identity Theft cases.

1.5 The Research Methodology

1.5.1 Discussion on research approaches

This section briefly describes the various research approaches that were considered for this project. It clarifies how to acquire the required knowledge and design programme of work to ensure the successful completion of the project. It is imperative then to refer to some areas that surround research methodology theory and combine them with practice.

The preparation of a research should be based on a proposal of work method (Hughes and Cotterell, 2002). Wilson (1999) points out research methods as the observation of science. Hughes and Cotterell (2002) declare that methodologies and methods are rather confused and overlapped terms; however “methodology is the set of methods that are used on a project”. Methodology is studying methods and argues about philosophical theories of the research process; whereas, method is an exact procedure of data collection concerning these philosophical theories.

There are two wide methodological approaches; the logical and the empirical positivism (see Hughes and Cotterell (2002)). Based on the methodological approaches, we are lead to the two main research methods, the quantitative and the qualitative. The following paragraphs provide briefly the characteristics of each one and compare them in order to decide the appropriate one for this work.

The quantitative method is related to positivism that claims a scientific approach is ideal for explaining and exploring physical and human events. It is designed for collecting data proper for statistical analysis and is mostly linked with experiments and questionnaires. The qualitative method is related with the anti-positivist that rejects the scientific approach, the hermeneutics that attempts to interpret and phenomenology that studies the event. The qualitative method relies on observation and unstructured interviews. It is actually called so in order to be distinguished from quantitative. (Wilson, 1999).
Qualitative and quantitative are different perspectives, have different assumptions, and look at different things. (Ratcliff, 2004)

In many occasions the researcher needs to adopt a combination of both methods; the mixed method that involves aspects of collection and analysis of both types (Creswell and Clark, 2006). To include only quantitative and qualitative methods falls short for the major approaches being used today (Creswell, 2002). Several publications defend the mixed method research, Creswell et al. (2002), Onwuegbuzie and Leech (2006), Rocco et al. (2003), Spratt et al. (2004), Chatterji (2004), are only an indication to provide the principles that need to be followed in such an approach.

Mixed research is supported by the ‘compatibility thesis’, where quantitative and qualitative methods are compatible and the ‘philosophy of pragmatism’, where the researcher is allowed to use any method that is proven useful for the research despite any assumptions (Johnson and Christensen, 2004).

The nature of this research work requires data collection and analysis that belong in both qualitative and quantitative methods. In order to reach the desired results data from both approaches should be connected and those are described on the following section, where the research plan is introduced after the study of the research methods and their applications occurred.

1.5.2 The research plan

The research methodology that is planned for this work consists of four major parts and is based on the mixed methods research. Each part follows, is linked with and is focussed on fulfilling the proposed objectives of the project:

1) The first part of the research raises the need to comprehend the different aspects of ID theft in relation to the way personal information can be stolen. This is achieved by using the data retrieved as key-findings of a hard disks’ case study – observation of facts. The author took part in a 265 hard disk drive case study (Jones et al., 2006). The results of this analysis provide the essential information concerning the types of the personal data that can be stolen when stored in digital systems. This raises the need for extended
research in the area of ID theft incidents in order to assist the work of the computer forensics investigator.

2) The second part examines the state of the art in relation to current practice in the investigation and analysis of ID theft. The research findings justify the key terms and satisfy the need to comprehend the methods used to accomplish ID theft. The areas of concern are:
   
i)  The types of ID theft that exist on the real world;
   
ii) The ID theft techniques that are used by the fraudsters;
   
iii) The issues that are raised from detecting and investigating ID theft.

3) The information obtained from investigating and analysing the nature of the attacks assists in the creation of a conceptual framework for analysing the process of ID theft. The procedure can acknowledge the information that can be stolen and the way the fraudster can achieve this.

4) The validation of the research is achieved in two parts:

   Part A:

   Applying the conceptual framework on an experimental analysis of residual data from hard disk drives that will be accomplished by:
   
i)  The researcher will behave as the fraudster in a closed network attack in the laboratory (case study experiment);
   
ii) The researcher will use the residual evidence and act as a forensic examiner, analysing the hypothetical victims’ and fraudster’s hard disk drives.

   Part B:

   Using law enforcement expert advice and feedback:
   
i)  Feedback of the application of the investigation framework on a real case received by the Gwent Hi-tech Crime Unit;
   
ii) Open-ended interview with a Gwent Hi-tech Crime Unit detective (qualitative results).
The case study research uses a qualitative method, aiming to emphasise on the phenomenon in its initial stage by collecting data (Benbasat et al., 1987). The full page graphical representation of the research methodology followed can be found in Appendix A2.

1.6 Structure of the Thesis

The second chapter of this thesis summarises the key aspects of ID theft and the investigation of this type of crime. It analyses the state of the art concerning ID theft and describes the extent of the problem. It discusses the existing computer forensic investigation frameworks and outlines the need for further attention on the area based on existing hard disk study analysis. Moreover, the relationship between computer crime, digital evidence and ID theft is discussed and the detailed requirements for this research are set. In the third chapter, the differentiation of ID theft towards other computer crime incidents and the design of the proposed investigation framework can be found. The fourth chapter presents in detail the implementation of the ID theft investigation framework and its functionality. Chapter five describes the evaluation methods used for this work by applying theory in practice, while the sixth chapter demonstrates the experiment that took place and the results of the evaluation processes. The seventh and final chapter highlights some of the problems encountered during the lifetime of the research and outlines suggestions for further research on the subject.
State of the Art

This chapter reviews

► Computer Crime and Digital Evidence;
► ID theft and Modus Operandi;
► issues concerning detecting, preventing and investigating ID theft;
► existing Computer Forensics investigation frameworks.

Overview

This chapter examines and reviews the existing literature relating to Identity Theft. In particular, literature that is essential for the integration of the research to the real world.

It is necessary to explore areas that are involved with the problem, as described in Chapter 1 and endorse the hypothesis of the research. Therefore, the following subject areas are going to be reviewed:

• Computer crime: An examination of general issues that are related to computer crime.

• Identity Theft: A discussion on the different types of ID theft, as these influence the development of the proposed framework.

• Computer forensics: A discussion on the existing frameworks and methods that are used in digital investigations.

• Digital evidence: A review of issues that influence digital investigations and are related to digital evidence.

• Other issues that refer to the actual research outcome, as this will be presented in the following chapters.
Parts of this chapter were presented and published in the proceedings of the 2nd International Conference of Global E-Security 2006 (Angelopoulou et al., 2006), 1st Annual Workshop on Digital Forensics and Incident Analysis 2006 (Fragkos et al., 2006) and the International Journal of Electronic Security and Digital Forensics 2007 (Angelopoulou et al., 2007).

2.1 Computer Crime, Computer Forensics and Digital Evidence

The following sections provide background information concerning significant areas related to this research. Computer crime, computer forensics and digital evidence are defined and some significant affirmations from the literature are provided.

2.1.1 Computer Crime

Those types of crime where a computer or any other electronic device is involved in order to perform the crime or as the target of it are considered as computer crimes (Parliamentary Office, 2006). Stephenson (1999) on the other hand defines it simple as “crimes directed at a computer or a computer system”. The term appears in a number of alternatives or subcategories such as cybercrime, electronic crime (e-crime) and high-tech crime.

Criminals are becoming increasingly adept at taking advantage of technology both to perform the criminal act and to avoid detection. Mohay et al. (2003) comments that

...computers will probably be involved in crimes that no one has ever imagined. New kinds of computer-related or assisted crimes emerge constantly...

Based on Mohay et al. (2003) while the use of computers and the Internet become even more popular, at the same time fraudsters’ take advantage and increase their ways of attacking systems. The computer can be used in three different ways in order to assist a crime. It can be used as the ‘tool’ that the fraudster uses for performing the crime, the ‘target’ that the fraudster manages to attack and
penetrate and the ‘storage area’ that he can use in order to save information involving the crimes. (Shinder and Titel, 2002).

The term Computer Crime covers a number of offences: copyright theft, child pornography, fraud, malware, and harassment. They can be categorised in different ways, according to the methods used in order to prevent them. Icove et al. (1995) approach this categorisation by grouping them into the following computer crime breaches:

- Physical security breaches
- Personnel security breaches
- Communications and data security breaches
- Operations security breaches

The perpetration of a particular crime or ‘breach’ involves a number of stages or actions; each one with a specific purpose. This suggests that an analytical investigation based procedure will enable a more straightforward, focused and speedier analysis as the investigator will follow a based-on-crime process. The ID theft investigation framework could assist on this as a specialised crime specific framework for ID theft.

### 2.1.2 Computer Forensics

Forensic science is used to give insight to the chain of events that occurred during a crime. The Oxford English dictionary defines the word forensic as

1. relating to or denoting the application of scientific methods to the investigation of crime.
2. of or relating to courts of law.

Therefore, according to Schweitzer (2003), computer forensics is

the science of acquiring, retrieving, preserving, and presenting data that has been processed electronically and stored on computer media.
Caloyannides (2001) defines it as

the collection of techniques and tools used to find evidence in a computer.

The above definitions are supplementary one to another and both useful for the appreciation of computer forensics.

Computer forensics encompasses all aspects of the investigation of computer related crime in dealing with a number of situations from industrial espionage to damage assessment. Mohay et al. (2003) mention the first computer forensic practices back in the 1970s with mainframe computer systems. However, it was not until the 1980s that the need for computer forensics started to develop from the law enforcement side (Mohay et al., 2003). Nevertheless, it is only the last few years that terms like computer forensics and digital evidence along with the internet revolution have been made widely known to the public along with the expertise that is demanded in the industry (Sheetz, 2007).

Residual data on digital media can provide evidential information for a variety of different crimes. There has been a body of on-going work examining the need for standardising the computer forensic investigation. Valuable attempts for formalising procedures have been published from both the law enforcement/industry and the academia (see section 2.5). These are discussed in a later section on this chapter, as they are considered part of the core of this research.

2.1.3 Digital Evidence

Digital evidence originates from evidence; the Oxford English dictionary defines it as

- information or signs indicating whether a belief or proposition is true or valid.

- [Law] information used to establish facts in a legal investigation or admissible as testimony in a law court.

Therefore, digital evidence is any kind of digitally processed information that is stored in any sort of digital media. The data strengthens or negates the assumption
of an electronic crime in the terms of the investigation process. It can be therefore presented as supportive proof in a court of law. (Carrier B.D., 2006b)

In the late 20th century Dr. Edmund Locard, director of Lyons Institute of Forensic Medicine, defined an important theorem for the foundation of the forensic science that is widely known as the Locard Exchange Principle:

Any action of an individual, and obviously, the violent action constituting a crime, cannot occur without leaving a mark. What is admirable is the variety of these marks. Sometimes they will be prints, sometimes simple traces, and sometimes stains (Chisum W., J., and Turvey B.E. (2006) from Locard, 1934).

The theorem has been transformed and misinterpreted during the years aiming to cover the science needs (Chisum, Tervey, 2006). The simplest form that can be found in literature is “with contact between two items, there will be an exchange” (Thornton, 1997).

Casey (2003) has noted that this theory is relevant to the digital world as a digital exchange between two devices results in an exchange of information. For example, a request to view a web page from a client may be logged on the server and the web page, if downloaded, may then reside temporarily on the client. As Palmer (2002) argues, the purpose of digital evidence is to provide consistent, relevant data that could be presented in a court of law or a public forum and it does not only fall under law enforcement.

The digital evidence in ID theft investigations is determined by the nature of the crime. When digital devices are involved in ID theft incidents, there is going to be significant residual data following the criminal act that can be retrieved by applying computer forensic techniques. The digital investigation of computer based ID theft requires the expertise of a computer forensic investigator to ensure that critical evidence is presented with accuracy. The understanding of the importance of the delicate digital evidence for computer forensics will assist the design of the ID theft investigation framework.
2.2 Identity Theft in the Digital Environment

Personal identity is increasingly being stored and used in a range of digital forms. This can leave individuals exposed to possible threats as a result. Examples include; phishing e-mails, web spoofing and numerous other techniques. This emerging and developing trend in crime can result in complex investigations that involve information technology, both as a medium for analysis and as evidence at the same time (Shinder and Cross, 2008, Kovacich and Boni, 1999). Fraudsters are obtaining more sophisticated technological ways and manage to conceal their crimes.

<table>
<thead>
<tr>
<th>Traditional ID Theft Techniques</th>
<th>Innovative ID Theft Techniques</th>
<th>Technical Skills Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stolen wallets or bags</td>
<td>Phishing</td>
<td>High</td>
</tr>
<tr>
<td>Stolen mail</td>
<td>Web-Spoofing</td>
<td>High</td>
</tr>
<tr>
<td>Deceased people</td>
<td>Pharming</td>
<td>High</td>
</tr>
<tr>
<td>Dumpster diving</td>
<td>Social Engineering</td>
<td>Low to high</td>
</tr>
<tr>
<td>Burglars</td>
<td>Malicious Software and Keyloggers</td>
<td>Medium to very high</td>
</tr>
<tr>
<td>Shoulder surfing</td>
<td>Storage Devices and Media</td>
<td>Low to high</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Card Cloning</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Biometrics</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>CCTV Cameras</td>
<td>Medium to low</td>
</tr>
<tr>
<td></td>
<td>Data Retrieval</td>
<td>Low to high</td>
</tr>
<tr>
<td></td>
<td>PDA’s, Mobile Phones and Bluetooth</td>
<td>Low to high</td>
</tr>
</tbody>
</table>

Table 1: Summary of the ID theft Techniques

Table 1 summarises all different methods by which ID theft can be performed. They are divided into two main categories: the traditional techniques, commonly found prior to the widespread use of IT and the innovative, computer-aided techniques, supported by technology. The technical skills required by the attacker are noted on the table as well, related with the work of Owen (2005); a detailed categorisation matrix can be found on Appendix C based on Owen (2005) and Sproule and Archer (2006). The types of threats have been combined against online identities and the ways to achieve illegitimate profit as they result from the literature. It is an attempt to identify and record any digital evidence that may be
found per category. Other factors of concern for an investigation are also recorded, such as the required skills and capability profile of the fraudster. The detailed categorisation matrix (Appendix C) is a concentrated table that includes all necessary information per ID theft technique. It appears as a valuable tool considered for the design and implementation of the ID theft framework, because of the concentrated information it contains.

The traditional, non-computer related techniques are briefly discussed on the following paragraphs although they are not the main interest and purpose of this research. It is reasonable to assume as in some cases non-computer and computer based techniques may both appear. The digital ID theft techniques are then examined.

2.2.1 Traditional ID Theft

ID theft can be perpetrated in a number of ways. Discarded documents containing personal details can provide a rich source of personal identity information with dumpster diving (Wall, 2007). Another popular traditional way of obtaining personal identity information is the shoulder surfing, spying someone while entering a PIN number or password (Peltier, 2006). Simple forms of deception can also be used to extract the information from the victim; an example would be an attacker poses as a legitimate government official or business person collecting personal data door to door (FTC, 2003). Other methods include the so called brute force techniques such as the stealing of wallets and purses containing identification and credit and bank cards or the removal of personal documents during a burglary. In particular stolen mail, where the fraudster may have access to bank and credit card statements, pre-approved credit offers, checks and tax information, can be used to gather information for an ID theft (Biegelman, 2009).

This may be followed up by social engineering. The fraudster contacts the person who has lost his card claiming that they found it, asks for personal details and then uses this information fraudulently (Dwan, 2004). He may apply for and get a new credit card using someone else’s personal details and never react on a demand for payment, resulting in an offence against the legitimate owner. The fraudster may comprise a phone service or a bank account; replicate checks or even acquire properties in the same way. Other cases may include the bankruptcy of the victim.
or criminal records by giving stolen personal details in case of an arrest (FTC, 2003).

There are also a number of cases which appear in literature, where a deceased person’s identity is used to purchase a property, apply for a loan or a credit card or to obtain other financial services. According to CIFAS (2007), the UK’s fraud prevention service around 70,000 families; have found out that their deceased family member has been a victim of impersonation.

The ITRC (Foley, 2003) reports that the information about the deceased person can be obtained from a number of sources: obituaries, death certificates or the Death Index that in the UK is available from the General Records Office. In addition, the financial institutions are not notified instantly after someone’s death that leaves the fraudsters with plenty of time for action. The redirection of the dead person’s mail to another address, a birth certificate request or even a national insurance number could help the ID thief not only commit financial fraud, but also build a new identity using another’s identity. These cases usually involve people that are about the same age as the deceased or in some cases from the same family. HALO is the deceased fraud prevention system in UK; its extensive database contains 7m records of deceased people and gets updated monthly in order to provide early notification of a possible identity fraud for those businesses that subscribe to the service (HALO, 2010).

2.2.2 Innovative ID Theft

This section analyses the different ID theft techniques and methods of perpetration that are based on technology. An understanding of each of these techniques and how they are applied by ID thieves in order to achieve their goal is essential in understanding how the digital investigation should proceed. The section is divided into two subsections, the online and the offline techniques of innovative ID theft.

Both online and offline techniques involve digital media and devices. Therefore, they can retain digital residual data that can be used as evidence when retrieved with computer forensic methods. As mentioned in chapter 1 (see section 1.4), the purpose of this research is the digital investigation of online ID theft. For this
reason the online techniques are discussed in more detail than the offline. Some additional information on the technical aspects of the online techniques has been added on Appendix D based on the background research undertaken.

### 2.2.2.1 Online ID Theft Techniques

The online ID theft techniques are applied over the use of the Internet. The fraudsters have developed technologically sophisticated ways in order to attack their target. Online ID theft leaves evidence behind onto the victim’s side and potentially on the fraudster’s system; the individual who has developed and applied the technique. The understanding of how each different technique works will assist to its detection and investigation. The online techniques are discussed individually in the following paragraphs.

**Phishing**

As stated in Kruck and Kruck (2006) the etymological root of the word phreaking\(^1\) has been used in order to transform the word fishing to phishing (APWG, 2003). The hacking magazine alt.2600 first introduced the term on January 1996. (Hinde, 2004a)

Phishing is a method that is used to gain users’ personal identity information in order to achieve ID theft with the use of deceitful e-mail messages that are supposed to be sent from trustworthy businesses. It was rated as among top ten frauds in 2004 (Forman, 2004) and has been highlighted in the front page of The Times (2005). Phishing attacks involve the mass distribution of spoofed e-mail messages in which the reply addresses, links, and branding appear to come from banks, insurance agencies, retailers or credit card companies. It existed in the early internet period as carding or brand spoofing (James and Stewart, 2005). Initially, it was classed as social engineering, by malicious crackers that achieved it over the phone. As fraudsters become more sophisticated, it was transformed to spam e-mail messages and forged web pages. (Russell, 2004)

---

\(^1\) Phreaking refers to the unauthorized use of the public phone systems for making free calls. (Shinder and Titel, 2002)
The messages appear authentic by using all corporate logos and formats similar to those that are used by the official companies. The threat lies in the request of personal identity information, for instance account numbers, passwords and other private information, supposedly for auditing, security or confirmation purposes. One example would be a case in the UK dealt with by the National Hi-tech Crime Unit. In April 2004, an unemployed 21 year old British man from Lytham St Anne's was arrested for a Phishing attack against the Co-operative bank and targeting the Smile Internet Bank. (Anon, 2004)

Phishing attempts can make use of a combination of techniques (see Appendix D – The method of Phishing) in order to trick the user into revealing private information. This usually can include the following combination: spoofed e-mails that use social engineering to convince users to be redirected to spoofed web pages on private or anonymous web servers (Berghel, 2006). In addition, zombie machines are used (Jakobsson and Myers, 2007), the result of bot infected computers. They can control a system through a communication channel (Symantec, 2007). Phishing, malware and spyware can involve bot infections and lead to ID theft.

More information about phishing and an analysis on a phishing e-mail can be found on Appendix D.

Web-spoofing

Spoofing attack is considered any attack that leads the victim in a correct decision for an imaginary environment, with misleading effects for the real environment (Felten et. al, 1997). An FBI Press Release (2003) mentioned among others that spoofing was then considered as:

The hottest and most troubling, new scam on the Internet ... contributing to a rise in Identity Theft, credit card fraud, and other Internet frauds.

Web Spoofing is the method by which the users believe that they are on the original website, while they visit a counterfeit one and is the alternative to phishing. “Web Spoofing is pretending to be somebody else’s web site” (Johnson, 1998). It requires high-skilled fraudsters, in order to redirect the user to the
State of the Art

deever’s web site. When any personal identity information is entered, it is going to be stored and used for malicious reasons.

Web pages can be duplicated by skilled web designers or reuse of the original code they are exact copies of the original with all the content correctly linked to the original web page. The main difference is that there are minor changes that allow for user information to be stored on the fraudster’s servers. The ID thief impersonates a respectable corporate identity and aims to replicate the company’s website, where the potential victims’ information is stored. Therefore, any credit card numbers, bank accounts, and other personal and private information entered by the user are managed by the ID thief.

There are some cases where a fraudster will copy a complete website and bring up the website clone on to a website with a similar name e.g. www.goglobaltech.com, may become www.goglobaltechs.com (note the additional ‘s’).

More information about web spoofing can be found on Appendix D.

Pharming

Pharming is the rather recent similar to phishing, but more complicated and technically demanding (Brody et al., 2007). It intercepts a client-server communication and redirects the user to the fraudulent destination. The user doesn’t have to click on any e-mail link, as she/he has been already redirected to a malicious web page that appears as legitimate. This is achieved by DNS hijacking and cache poisoning. The fraudsters exploit a vulnerability of a DNS server, modify the domain name server of a legitimate web site and redirect to the fraudulent. (Ollmann, 2005)

Man-in-the-middle attacks are involved with pharming as with phishing and web-spoofing (see Appendix D). However, DNS cache poisoning is a rather advanced method used by the fraudsters and it does not only serve the pharming attacks, e-mail or SSL session hijacking. It also redirects the user to a different IP address that can cause Denial-of-service (DOS) attacks or plant malware/ spyware on the computer and block antivirus updates (Yuan et al., 2006).
Hallam-Baker (2005), explains DNS spoofing attacks. Stamm et al. (2006), provide an example that concerns pharming involving home routers and a browser that runs Javascript and Java applets. The popular secure e-mail provider Hushmail has been a pharming victim. On April 2005, the Hushmail users were redirected to a spoofed web site, as the company’s DNS records had been altered (Leyden, 2005).

Malicious software and Key Loggers

According to Skoudis and Zeltzer (2003), malicious software or malware is

...a set of instructions that run on your computer and make your system do something that an attacker wants it to do.

It includes computer viruses, worms, Trojan horses, spyware and adware.

Various types of malware are developed on a daily basis, including malware developed for information gathering. A Trojan horse is one example of code used to penetrate a system, possibly with the objective of obtaining passwords and personal details. Trojan software can keep a log from keystrokes or take a screenshot when a customer is visiting a financial web site and e-mail the information to the fraudster (Unknown, 2005). The Trojan PWSteal.Bancos (Symantec, 2005) disguises itself in different formats and if the user runs it, it acts as a key logger, sends back bank information and displays bogus bank web pages. Panda Security (2009b) reveals that on an average of 37,000 security threats they receive daily, 71% of them are Trojans mainly created for ID theft.

Spyware, another form of malicious software, is designed for exploiting infected computers basically for marketing purposes. Therefore, the activity of the web browser is monitored resulting to routing of HTTP requests to the web sites that are advertised through the spyware. Pop-up advertisements are delivered and theft of personal identity information is achieved, including obtaining financial information from users. There are cases that spyware was used by ID theft rings in order to retrieve and store user information remotely. The information Sunbelt Software, an antispyware firm, revealed after research on a spyware that is part of the CoolWebSearch (CWS) browser hijacking tools would concern any online user. There was remotely personal saved information that was retrieved, including
chat sessions, user names, passwords and bank information (Vijayan, 2005). A recent report from Panda Security (2009a) mentions twelve important malware types that can capture personal data.

Keyloggers can be used to capture data entered by the user. They can be hardware or software. The hardware version is usually installed as an extension between the keyboard and the port. An executable file needs to be installed on the system for the software key loggers and can be kept perfectly hidden from the potential victim.

They can be installed as part of another program, or manually by an installer with a user interface. They can track keystrokes on specific programs or the entire activity on a system. Keyloggers are considered as a threat that cannot be easily prevented for personal identity information (Chahrvin, 2007). They belong on the malicious software category and can be part of a Trojan horse, which may be used as well for collecting information on a phishing attack. Subramanyam et al. (2003) have tested and reviewed a number of different keyloggers and concluded how simple it is to buy or even write them. In 2007 there were six known key-loggers that are able to capture banking details (Bonner, 2007). Heron (2007) mentions that there was a 1300% increase on the use of keyloggers between 2002 and 2005 and analyses the different types of hardware and software keyloggers and how they function.

Data Retrieval

Personal information is nowadays stored extensively on computers from authorities’ records to home computers. Furthermore, when extended to the online world personal information is stored from online registration forms to online communities and databases.

People tend to share personal identity information on the Internet, e.g. social networking or recruiting web sites. They are inclined to widely disclose personal identity information on social networking web sites such as Facebook, MySpace, Hi5 and LinkedIn that as a result leaves them vulnerable to fraudsters. The procedure of retrieving information of a potential victim is straightforward when there is access to his online profile. However, Bilge et al. (2009) describe more
sophisticated ways that an ID thief could gain access to social network profiles with profile cloning and cross-site profile cloning.

A number of different databases store great amounts of personal information; from utilities providers to electoral register entries and from insurance policies to previous addresses (Newman and McNally, 2005). The databases are portable and extensively employed online. A persistent ID thief could recover the past and present of an individual by exploring hacking techniques. Though, a more frequent case for ID thieves to steal personal identity information is to hack into corporate databases and obtain clients’ personal identity and financial information.

One of the latest examples is the case of an American, Albert Gonzalez, who employed servers around the globe and with SQL injection attacks\(^1\) managed to steal 130 million credit and debit cards from multiple corporations (Gross et al., 2009). Apparently he committed the largest ID theft that ever occurred in the U.S. (Kerber and Herbst-Bayliss, 2009). Another example involves the California State University at Chico found out that a computer including names, addresses and Social Security numbers had been compromised by hackers and had to alert 59,000 students, faculty, and staff (Greene, 2005). Furthermore, the recruiting company’s Monster database was recently penetrated and ID thieves managed to retrieve names, phone numbers and e-mail addresses (Cohn, 2009).

**Online Social Engineering**

Social Engineering is the manipulation of individuals for retrieving sensitive information and the intention is usually fraudulent. Some old-fashioned methods that are linked with ID theft are traditionally used, such as dumpster diving, shoulder surfing and direct theft (Lively, 2004).

Computers are usually a secondary tool for the social engineer, as communication skills appear more useful. However, the combination of technology, the internet and persuading expertise appear advantageous for the fraudster. The naivety of the

\(^1\) SQL injection exploits security vulnerabilities on databases.
end users concerning security issues in the online environment is the advantage of the social engineers that aim to mislead their victim (Marshall and Tompsett, 2005). Online social engineering is any type that involves the internet and the misleading of the user. It is used in a variety of forms, such as phishing and malware (as discussed above); spear phishing and Nigerian scam (see Appendix D). A phishing e-mail for instance is an effort to convince an end-user to follow a provided link and supply financial details.

Social engineering is a psychological method of attack and an acting charisma can be an asset for the social engineer, even when performing online. The aim is to convince the potential victim willing to disclose any information the attacker needs to retrieve. Attacks can be conducted either by influencing the victim psychologically to provide the requested data or by having physical access. ID thieves occasionally may act as network administrators and request passwords online or even sent malicious e-mail attachments pretending to come from a legitimate sender (Granger, 2001).

More information for the types of social engineering can be found on Appendix D.

The current online ID theft techniques were discussed in the previous paragraphs as a result of the Internet misuse. The fraudsters have discovered multiple ways for stealing their victim’s identity online; phishing, web spoofing, pharming, malicious software, keyloggers, data retrieval and online social engineering. The importance of studying these techniques in relation to this research is the understanding offered of how they can be achieved. This will assist the design and development of the ID theft framework, where the online techniques play a fundamental role.

**2.2.2.3 Offline ID Theft Techniques**

The methods that are mentioned in the following sections are not penetrated online. However, they are computer-aided and have been developed and advanced due to the extensive use of information technology.

These techniques of achieving ID theft usually reside at the fraudster’s premises or the fraudster should have physical contact with the piece of equipment. They
are mostly devices that when the appropriate methods are applied, they will allow the ID thief to achieve his intention.

Storage Devices and Media

As the demand for storage devices grows, so will the theft of personal data from such devices. Storage devices and media include the following items: hard disks, USB flash drives, floppy disks and CDs and they are widely used on a daily basis. They can act as a fraud and theft tool as they can hold user sensitive information; this information can be extracted from either stolen or sold storage devices / media, where files, personal identity information, e-mail messages, logs, Internet activity, etc. are stored.

A study conducted at the University of Glamorgan (Jones et al, 2006) showed that out of 105 hard drives, 57% of them contained sensitive personal identity information. Poor end-of-life disposal practices and the lack of encryption make data easy to retrieve. This threat increases as more and more commonly used devices, like media players, are capable of storing large amounts of data in them, with very short transfer times. McKinley (2004) provides as an example an industrial spy that uses a USB flash drive to store a rival’s information on.

A variety of storage devices and media have been involved in scandals concerning lost data, such as hard disks, laptops, compact disks and flash drives. There is much recent discussion in the news regarding the loss of personal and private data of the British government and the threat of the data being sold to ID thieves (Oates (2007), Stratton (2008)). A hard disk that was sold on eBay containing one million customers’ bank details is another remarkable incident (Newling, 2008).

Card Cloning

Card Cloning can be broken down into two parts: the credit card information retrieval process and the credit card cloning process. The retrieval of credit card information does not require a technically skilled person; the credit card cloning process is carried out by a person with basic technical skills in order to manipulate a card replication machine and reproduce credit cards. This is due to the fact that credit cards still use re-writable magnetic stripes, even though they have been replaced with Chip & PIN technology over the last few years. Card cloning is a
very important part of ID thieves’ work. PINs and passwords can be retrieved with the use of cameras or card readers on tampered bank cash point machines. This is a growing threat, as more and more often tampered cash point machines are discovered. Another worrying fact is the illegal use of swipe handheld devices by store employees in order to gain customers’ personal identity information. (Gerard et al., 2004b)

Biometric
Biometric identification has been proposed as a counter measure for ID theft. It is a method that aims to replace vulnerable passwords; however fraudsters have discovered numerous ways to breach a biometric system. It is possible to deceive biometric technology by tampering with machines that read biometric data or altering the records that are contained within them. Residual fingerprints left behind on scanners can be re-used by breathing on the glass, cooling down the sensors to give false information, using graphite powder to dust the fingerprint and then copy it to a “jelly finger”. Facial recognition can also be duped in some cases by playing someone’s video at the reader and gaining access to a system. (Hamadi, 2004)

It is often that someone has physical access to such devices and since these devices transform physical information into digitized information, special loggers can store the information being sent from the device to the authentication machine. This information can then be replayed and the un-authorised person can gain access. Biometrics can be dangerous if they allow an ID thief to acquire information about a person’s physical features (e.g. finger), which can permit him/her to create a replica and use at will.

Surveillance systems
CCTV and RFID cameras (Engberg et al., 2004) monitor the behaviour of people; therefore they could follow the steps of a specific person. An individual may be unaware that a camera is recording him. The motive is often a PIN number collection and this method is widely used from fraudsters on cash machines (Masters and Turner, 2007).
A potential fraudster may take advantage of a system vulnerability to gain access on surveillance systems, which are now used in various locations from commercial stores to public streets. As Engberg et al. (2004) mention this could give the ID thief the privilege to monitor the behaviour of a potential victim and copy his daily life and habits.

In addition, the wide spread of free open access wireless networks and the increase of IP enabled camera equipment, is an easy and inexpensive method to install a wireless camera. When connected to the Internet it can be remotely accessed and controlled (Fischer and Green, 2004).

**PDA’s, Mobile Phones and Bluetooth**

Fraudsters have discovered a number of deceptive techniques in order to take advantage of the wide use of PDAs and mobile phones. Both devices can provide a variety of personal identity information when stolen, such as contact numbers, pictures and personal files. However, some knowledge on technology is required when forensic data extraction is needed.

Access on a Bluetooth device is related to ID theft as the fraudster gains complete access of the device and personal data can be stolen. A number of exploits have been identified, such as Bluesnarfing that is able to retrieve the calendar, the address book, contacts and multimedia files from a mobile phone. An old technique (Ward M., 2003) used a flaw in the Bluetooth implementation in certain phones, in order to acquire the address book. Since the majority of mobile devices (e.g., mobile phones, PDAs, PCs, etc) have Bluetooth capabilities and users tend to leave them operational, they can disclose personal data.

The offline ID theft techniques on this section; storage devices and media, card cloning, biometric, surveillance systems, PDA’s mobile phones and Bluetooth, describe briefly the computer-aided, but not Internet based techniques that ID theft can be achieved. A fraudster can take advantage of any of these techniques and leave digital evidence behind. Their study was essential, as with the online techniques, in order to be able to identify and later examine how they can be achieved. The ID theft framework needs to incorporate them as additional to the online techniques.
2.2.3 Internet Fraud, Identity Theft and its Forms

Internet fraud refers to any deceptive method that takes advantage of online services and includes e-mail spam, spoofed web pages, ID theft and web banking. Research in the first half of 2010 (UK Statistics Authority, 2010) has shown that 73 per cent of homes in the UK have internet access. This is an increase of 5 million households since 2006. A comparison with previous years shows that the percentage was 57 per cent of households in 2006, 49 per cent in 2004 and just 13 per cent of homes in 1999 (UK Statistics Authority, 2006).

31 million people used the Internet for purchases in 2010 equivalent to 62 per cent of all adults. 87 per cent of Internet users confessed their concern about online fraud (UK Statistics Authority, 2010).

As the number of Internet users worldwide continues to grow, so too will the accounts of cyber-related criminal activity. (Schweitzer, 2002)

The wide use of broadband connections promotes the user being online all day, a longer duration of exposure to malware or other possible attacks.

Pfleeger (2000) suggests four potential motives for the computer fraudster: power, fame, money and ideology. May (2004) indicates three motives: financial gain, revenge, fresh start. Nevertheless, almost everything in today’s world involves the power of money. It is undoubtedly that the financial motive is the strongest and is directly linked with the purpose of offences related to ID theft. As Biegelman (2009) effectively mentions:

...all of these motives point to a need or desire for money.

In the literature there are multiple ways of distinguishing the motive of ID theft crimes, based on the viewpoint of the author. However, there is limited discussion on the subject. The research on ID theft is based mainly on the threat itself and the methods the fraudsters can gain access to confidential data (see Marshall and Tompsett (2005), Granova and Eloff (2004), Long (2005)). Several sources examine ID theft, based on the intended target; the individual or the corporate (see Copes and Vieraitis (2007), Sproule and Archer (2006), Wilding and Parker (2002), BusinessLink (2008)). As individual ID theft is related with those
incidents that involve any personal data retrieved in order to obtain profit in someone else’s name. On the other hand, corporate ID theft concerns stealing a corporate identity that may be achieved by fraudulently abusing the company’s information and submitting forms such as the change of the business’s registered address. In addition, there could be also a combination of the above in which case the fraudster uses the identity of a person that works for a corporation and applies for a corporate account (credit or debit cards).

However, it is imperative to examine some interesting classifications of ID theft types that appear in literature based on the foundation of the crime. The understanding of how ID theft can be classified will lead to a proposed classification that can later be inherited in the ID theft investigation framework.

Finch (2003) categorises ID theft in total and partial. Total concerns cases that the ID thief takes up permanently someone else’s identity in order to begin a new life in his name. On the contrary, partial occurs when the fraudster uses the personal details of another person temporarily.

The American Privacy Rights Clearinghouse (APRC) (2006), categorises ID theft in two forms, the Account takeover and the Application fraud. In such a classification, the account takeover takes place when the fraudster uses the existing private information of the victim in order to acquire goods and services, while the application fraud concerns the cases where the fraudster uses the personal details of the victim in order to apply for financial services in that name. This type of ID theft takes longer for the victim to discover it, as they do not receive any statements concerning those transactions.

Tipton and Krause (2004) identify the threats as inside and outside, where an inside attack concerns those incidents where the fraudster has a wide knowledge of the target. It is usually related to corporations, when a member of the staff that knows exactly the organisation’s vulnerabilities decides to take advantage of his knowledge for his own profit. The identical situation exists on ID theft as well, considering these attacks that come from inside; cases when the victim and the fraudster are related, giving him the advantage of treating the information respectively, either concerning an individual or a corporation. According to Denning (1999) the greatest risk to information security are the internal users who
unintentionally reveal secrets to contractors, partners, customers, visitors, or outsiders requesting information.

Many computer security sources state that the majority of network administrators fear the ‘threat from within’ as more often the internal users of a company may imply a greater security risk than the external threats. Unsuspected employees may give a company’s private information rather straightforwardly to smart fraudsters. Then, these imposters are going to find the appropriate way to target the business and extract the information they need. In addition, research has proved that 70% of the total ID thefts start with an employee who steals personal data from the company he works for (Hinde, 2004d).

On the other side, the outside attacks deal with those cases that the attacker selects a target and tries to identify the Achilles heel of the system and gain access. The cases that the victim is chosen at random are usually those where he happened to have exposed his personal identity information on the wrong place, the wrong moment, either because he didn’t have the awareness to protect himself, or wasn’t cautious enough.

Particularly interesting is the study of the ITRC (2007), where ID theft is classified in four forms: financial, criminal, identity cloning and business or commercial.

1. Financial ID Theft: This type of case typically focuses on your name and Social Security number (SSN). This person may apply for telephone service, credit cards or loans, buy merchandise, lease cars or apartments.

2. Criminal ID Theft: The imposer in this crime provides the victim’s information instead of his or her own when stopped by law enforcement. Eventually when the warrant for arrest is issued it is in the name of the person issued the citation- yours.

3. Identity Cloning: In this crime the imposer uses the victim's information to establish a new life. They work and live as you. Examples: Illegal aliens, criminals avoiding warrants, people
hiding from abusive situations or becoming a "new person" to leave behind a poor work and financial history.

4. Business or Commercial Identity Theft: Businesses are also victims of identity theft. Typically the perpetrator gets credit cards or checking accounts in the name of the business. The business finds out when unhappy suppliers send collection notices or their business rating score is affected. (ITRC, 2007)

However, it is interesting to mention that the ‘Identity Theft: The Aftermath 2003’ report was only distinguishing ID theft in three categories: financial, criminal and identity cloning (ITRC, 2003). The commercial appears faintly for the first time in the Aftermath 2004 with minimal discussion on this type. This indicates that corporate identity fraud is becoming an area for increasing concern (Murray (2006), This is Money (2006), Wilding and Parker (2002)). The Aftermath 2003 study takes as examples real victims and drawing upon these cases those three forms are defined. Ultimate purposes for ID theft could be either financial and other resource and privilege gains or protection of one’s real identity and masquerading behind another, mostly legitimate entity. ID thieves can also take advantage of an organisation’s good name in order to attract individuals and hence then there is a case of a double ID theft, the corporation’s and the consumer’s (Dwan, 2004).

The ITRC appears as the most systematic classification among the examined. However, it seems like criminal and identity cloning forms are quite similar, while business or commercial embed both. Therefore, based on the background research so far, ID theft cases can be distinguished in two main types: financial, where the fraudster has financial potential and identity, where the fraudster steals an identity.

By parting evidence in two categories, the collection can be easier and more structured, as the main prospect for ID theft is mostly financial. However there are numerous cases that the fraudster aims to create a new picture of him/her on someone else’s name in order to create a new life. This raises the need to distinguish the evidence search in two categories, while both include potential criminal and fraudulent activity.
This extent to which the different types of ID theft are going to influence the investigation process needs to be determined. In such an approach, whenever the investigator has to deal with financial ID theft cases, he can first focus on credit history, transactions made on the victim’s name, applications for bank account opening, loans and credit cards, and the way they were done, phone companies that the offender had accounts, tax records and bankruptcy records. Based on the ITRC (2007) report, these accounts and records are involved with financial ID theft and could provide information.

On the other hand, concerning identity ID theft cases the investigator will need to take under consideration financial evidence, as well as national insurance numbers, driving licence records, employment records, passport records, business records, property records and criminal records. These records could provide evidential information of an identity ID theft. Table 2 represents the classification of ID theft as it appears in literature.

Table 2: ID Theft classification as appears in literature

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Total</td>
<td>Account Takeover</td>
<td>Inside</td>
<td>Financial</td>
<td>Financial</td>
<td>Financial</td>
</tr>
<tr>
<td>2  Partial</td>
<td>Application Fraud</td>
<td>Outside</td>
<td>Criminal</td>
<td>Identity</td>
<td>Identity Cloning</td>
</tr>
<tr>
<td>3  Identity Cloning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Business-commercial</td>
</tr>
<tr>
<td>4  Business</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.3 Identity Theft Response

Financial organisations obviously have an interest in reducing the risk of ID theft on their customers’ accounts. In the majority of cases the end users discover that they are ID theft victims only after their personal details have already been used fraudulently (Dwan, 2004). On the other side, most fraudsters of this kind of crime are not alone, but rather organised and well equipped. As Collins (2006) mentions, technology drives crime and even though IT security is important it still cannot solve ID theft.

This section aims to provide the recommendations that can be found in the literature concerning the prevention and detection of ID theft, as well as issues that arise in the detection and investigation. The purpose of these paragraphs is to present the current situation and later contemplate the effect of this study in the design of the framework, intending to facilitate computer forensics. There are multiple sources that recommend protection measures to the individuals; however the situation seems that these are not taken into further consideration. Then, the complexity of the ID theft investigations is discussed.

2.3.1 Recommendations for Prevention and Detection

There may be some time between the perpetration of the ID theft and the victim realising that his personal data has been stolen. Even though, ID theft is a familiar term to the majority of people in technologically advanced countries, users may not be sure whether they have been victims or not. According to FTC (2003) the majority of people discovered they were victims by monitoring their accounts. The fact is only fifty per cent of the victims finally find out how thieves retrieved their personal data (DeMarrais, 2003). Both individuals and organisations need to be proactive, protect their personal assets and prevent them from being stolen and used for malicious reasons. Only in such a way could the risk be minimised.

The FTC (2003) recommends protection methods for consumers and organisations, such as ordering a copy of their credit report, creating passwords for their accounts, storing important documents in secure places, and getting informed about who has access and at what level, and about their personal identity information at work. While several laws are trying to limit consumers’ liability
from ID theft, $48 billion loss came from businesses and financial institutions comparing to $5 billion loss of the consumers (DeMarrais, 2003). The situation shows that ID thieves have studied the ‘psychology of advertising’ as they know how to use the consumers’ trust. It may be assumed that ID thieves with the purpose of taking advantage of an organisation’s good name in order to attract individuals are performing a double ID theft, the corporations’ and the consumers’ (Dwan, 2004).

Another prevention objective is to limit misinformation. Potential victims should be educated and aware of the situation. Albrechtsen (2006) performed a study concerning the users’ viewpoint of information security. This study revealed the majority of the interviewees were aware about their responsibility in security. However, they were unfamiliar and even confused with the actual activities they should carry out to protect their online activity. In addition, they believe that documentation, guidelines and media campaigns are of no influence on them and they need a user-involving approach.

Furnell (2005) reveals a U.S. survey, where 67% of the correspondents appear to have either no antivirus installed on their system or an out of date one installed. In the same survey 72% of the users did not have a properly configured firewall. Symantec (2007) discloses that 95% of targeted attacks are directed to home users. A UK survey by BitDefender shows that less than 50% of the users have updated antivirus software. However, on the same survey over 80% of the respondents were worried about online ID theft (MJO Associates, 2008).

The results of the surveys draw a picture of users that are highly exposed to online threats. Despite the fact that numerous efforts are made to inform the end users about online threats and computer security, they appear ineffective. Immediate precautions should be taken and educating the end users appears urgent, because a computer system without antivirus and/or firewall is open to ID thieves. Small from Computer Associates (CA, Inc.), says about ID theft that the weakest point is people (Dwan, 2004).

The lack of the user awareness in relation with industrial security flaws, position the end-users in a vulnerable situation about protecting themselves (TACD, 2007).
Clements et al. (2006) support with a survey the importance of education of end users for preventing ID theft.

A recent research report from Lloyds TSB shows that 76% of citizens of the UK are worried about ID theft, while two in three are not aware of how to protect themselves. The financial organisation aimed to contribute by launching an advisory awareness service (Lloyds TSB, 2009). Organisations need to become even more active in how they will manage to assist the awareness of the users, while at the same time detect and prevent ID theft. When ID theft cannot be totally prevented, because of the human factor, then there should be an effort on detecting it immediately in order to minimise any possible loss.

The detection controls in a corporate environment comprise authorisation, internal auditing and whistleblower hotlines that alert the employees of the company about committed fraud. There may also be automated detection systems that process large volume of transaction data based on a specific pattern. In the event of something suspicious arising, then this can be investigated further. However, fraud from the inside company couldn’t be detected with such a method (Porter, 2004).

It is vital for an organisation to be familiar with the background of an employee that is going to be hired, especially in case he/she is going to manipulate sensitive data. The verification of an employee’s references from previous employment should be carefully examined. Gerard et al. (2004a) give a very detailed description of internal controls and information security. A review of these controls can be found in Appendix D.

However, it is important to treat information both personal and corporate with confidentiality in order to eliminate ID theft incidents. Because of the human factor, prevention can easily fail though; in such cases detection and investigation need to take action.
2.3.2 Issues on Detecting and Investigating ID Theft Cases

When a security breach takes place, it has to be considered that there should be a law violation in order to consider it as a crime, therefore evidence to prove this is essential. Evidence can be defined as any proof that can support the actual process of the incident.

The investigator of an ID theft incident has first of all to deal with and understand the motivation of the fraudster. A thief who targets unsecure systems is a relatively different case than someone who decides to attack an organisation in order to steal specific information. The impulse of the attacker can prove his knowledge, skills and intention (Casey, 2003). Fraudsters are cautious not to leave traces behind, mislead the investigator with anti-forensic techniques (Harris (2006), Smith (2006), Forte and Power (2007)) and remain undetected for a long period of time.

The ID theft fraudster does not always need to have advanced technical knowledge. Persuading and deceptive skills are always an advantage, as for social engineering. For instance, a shoulder surfer needs to be quick and observant, while someone who performs phishing or pharming attacks needs to know how to clone a URL, programming and web designing in order to design a professional web-site and write malicious code.

As mentioned earlier (see section 2.2.2.1), phishing emails can be often difficult to identify, although simple spelling mistakes usually give them away. A user can identify the unusual email if the email only contains a large image instead of text, which is linked to the spoofed web page. In some cases e-mails contain virus or have Trojan infected files attached.

Spoofed web pages can be identified from spelling mistakes and omissions. For example, when a login web page is spoofed and the original has been updated. The spoofed pages are not maintained and consequently the changes are not conducted on the spoofed webpage.

It is also important to understand how the fraudsters choose a target. Financial profit is their main objective. When targeting individuals the profit may be less
and when the target is corporate a large turnover may come at once. However, if someone targets and steals a large amount of money from a company or its clients, the loss will be easier to identify and more intensively investigated. For the individual on the other hand it can also take a longer period of time to find out that he/she is an ID theft victim. Meanwhile, the fraudster is free to hit other targets.

In ID theft, a person takes control of and abuses someone else’s personal and private authentication information; it belongs to criminal offences. There are people who unfortunately act unethically and against laws in order to gain financial profit. The aim of controlling a type of e-crime with the extent of ID theft requires both ethical and legal issues to be taken under consideration. In the past it used to be loss of goods and properties, but now it has also come to loss of personal private data. (Pfleeger, 2000).

In addition, individuals often do not often adopt any measures to protect themselves. They can provide personal identity information to anyone asked, carry their credit and debit cards in their wallets that might get stolen, they have their PINs and passwords written on pieces of paper that they carry in their wallet or they save them as records in their mobile phones. In addition, they visit unreliable web sites and purchase goods by entering their bank account details without considering online security.

When records on an individual’s or in a company’s name are found, the fraudster can be identified as many of his movements are going to be revealed. Though, there might be a team of thieves, acting with the same identity on multiple locations, or one person that performs with more than one identity, or a combination of them. These can make the investigation more complicated; while at the same time reveal more information about someone’s activities.

There are a number of problems that deter the preservation of evidence trail. The most important is that fraudsters tend to discover more and more sophisticated behaviour and manage to hide traces that can prove their guilt. It is a widely known that the majority of ID thieves do not work on their own, but in groups. This means that even when a case is revealed, the members of the group will still have the time to act undetected for a period of time. Furthermore, information that
involves personal data might be refused to the investigator in the first place, before the case is submitted to court aiming to personal data protection. There are also more technical difficulties such as the way the electronic devices used for the crime and how information can be retrieved from them. This requires the expertise of an investigator.

Even though not all ID theft incidents result in prosecution, when this happens the investigator needs to represent the result of the evidence analysis in an appropriate manner. Evidence in the court of law needs to be factual and detailed. The information presented needs to be complete as a statement and unbiased. All original electronic media related to the case must be preserved, not only their data. It is required to record any relevant information related with the electronic source the data was created. (Pierce, 2003)

The evidence from a computer system or network presented in the court needs to be based on the following standards:

- **Authenticity**, the evidence can be related with the events of the incident;
- **Demonstrational**, it can be presented in a form that can be submitted to the court;
- **Best Evidentially**, to represent the evidence in the more complete form;
- **Probative**, the information can be presented practically (Stephenson, 2002).

No matter the detailed investigation of the examiner it should be noticed that in the court hearing, the defence will try to dispute both the analyst and the evidence, e.g. Trojan defence (see Haagman and Ghavalas (2005)). Their job is to convince the jurists that there is not enough evidence and that the offender is not the criminal. For this reason, the material provided in the court should leave no doubt of their authenticity and need to be complete. It will enhance the professional scrutiny of the investigator when the case is represented without deficiency (Michaud, 2001). This thesis aims to develop a framework that could also support the accurate presentation of authentic data in court; because of its specialisation in this specific type of crime.
2.4 Forensic Investigation of Online ID Theft

2.4.1 The Theory of ID theft investigation

ID theft in its online form is considered a relatively new method of fraud and there is not enough guidance for forensic investigators. This is because of the commercial use of the Internet and the development of computer forensics only over the last twenty years. However, the wide use of broadband Internet connections is more recent and promotes the user leaving his computer constantly online (Saxby, 2004). In addition, the attention in computer forensics has been concentrated in creating formal guidance regarding the investigation of all types of computer crimes, rather than examining the digital media in relation to the type of the computer crime.

The investigator will have to unfold the digital trail of evidence and try to present potential explanations of how such a crime occurred. This digital trail involves examining how a crime was committed using computers and the Internet. The investigation should identify how the leak of personal identity information occurred that made it possible to conduct a misuse of resources such as a credit card number. It should also include details of the misuse such as dates, goods purchased and amounts spent. If possible the fraudster should also be identified. The latter is perhaps one of the most challenging tasks as, unlike DNA evidence, computer records can identify user accounts that are logically, not physically, linked to individuals (Tryfonas et al., 2006).

2.4.2 The Practice of ID theft investigation

The background research confirms that the ID theft situation is becoming more intense (see sections 1.3 and 2.2) concerning the number of the ID theft incidents and the techniques used. Actual user data of how ID theft was achieved is difficult to obtain, however an analysis of approximately 260 second hand disks that was conducted in 2006 by the Information Security Research Group (ISRG) at the University of Glamorgan provided a body of test data.

A third party organisation purchased the disks from the second hand market providing a degree of anonymity. The research was sponsored by British Telecom
(BT) (Jones, 2006) and the Life Cycle Services (LCS), where a number of hard disks were studied in order to identify and study the data that can be revealed from randomly purchased hard disks from different countries (U.K., Germany and North America).

Such a research provides awareness concerning end-user and corporate knowledge regarding data exposure. The overall number of disks analysed led to important results, such as statistical reports concerning the users’ familiarity with techniques like wiping data from their hard disks. The capacity of personal identity information revealed that it can even lead to ID theft by thoroughly profiling the victim, as there were multiple cases where personal identification details could be retrieved.

In the disk study the majority of the disks were between 500MB and 10GB. The chart below represents the disk capacity, from which it is possible to assume approximately the year which it was manufactured. This can lead the analyst to a simple deduction that the operating system would be most likely from around that period. This was validated since the majority of the systems contained older operating systems (e.g., MS Dos, MS. Windows 98, NT, 2000 and ME) (Fragkos et al., 2006). The chart on figure 1 represents the disk capacity:

![Figure 1: Disk Capacity percentages](image)

The actual sample size of hard disks was 259; while 124 were unreadable, 70 wiped and finally 65 of them were investigated. 4 of them contained illicit material and were handled to the police. The table below represents the total number of disks provided and how these numbers decreased by excluding disks that matched certain criteria.
Comparing the total numbers of disk provided (259) with the number of the disks that has been actually investigated (61), it is clear that only 23.5% of the disks were processed. Thirty seven of those disks contained commercial data along with twenty eight that derived the presence of individual data, such as bank accounts and credit cards, lifestyle information, e-mail accounts and instant messenger discussions logs (see table 4). In addition, family names, addresses and photos were retrieved. For example, a hard disk gave enough information to assume that it belonged to an ex-employee of a trucking company. Job applications, documents, letters written to the bank, a car insurance claim and account details were recovered from the disk.

<table>
<thead>
<tr>
<th>Disks Investigated</th>
<th>Commercial Data Present</th>
<th>Individual data present</th>
</tr>
</thead>
<tbody>
<tr>
<td>65 - 4 (illicit material)</td>
<td>37</td>
<td>28</td>
</tr>
</tbody>
</table>

Table 4: Origin of disks investigated

The findings in the 65 disks that were analysed revealed the following information by type of personal identity information that could be used maliciously (see table 5).

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Number of disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Names</td>
<td>44</td>
</tr>
<tr>
<td>e-mail Addresses</td>
<td>34</td>
</tr>
<tr>
<td>Business Disks</td>
<td>38</td>
</tr>
<tr>
<td>Financial Data</td>
<td>12</td>
</tr>
<tr>
<td>Personal User Information</td>
<td>10</td>
</tr>
<tr>
<td>Username</td>
<td>4</td>
</tr>
<tr>
<td>Full Address</td>
<td>3</td>
</tr>
<tr>
<td>Date</td>
<td>28</td>
</tr>
</tbody>
</table>

Table 5: Type of information on Residual disks
It is important to notice that of the above disks, those that contained a full address also contained a valid e-mail address in addition with other recoverable data, whilst 1 of them held financial information as well. Furthermore, 10 disks that belong to the business disks group contain financial data and e-mail addresses, which at the same time states them a feasible target of a potential ID thief.

According to the literature research presented in this chapter (sections 2.2.2. and 2.2.3.), an ID thief usually bases on specific information acquired by the victims. The motive is to achieve using the data for his personal and financial gain. Table 6 below presents the information that could be retrieved from second hand disks and the fraudster would probably search for, in no particular order.

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>1</th>
<th>Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>Full Address and previous addresses</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Email Address</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Telephone numbers</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Credit Card details</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Other family details / names</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Bank Account Information</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Financial Evidence: Passport Number, Driving Licence, National Insurance Number, Business, Property, Criminal Records</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Possible passwords</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Utility Bills</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>Other Personal Information: Date of birth / marital status</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Occupational Information: Employment details, Monthly income</td>
</tr>
</tbody>
</table>

Table 6: Personal identity information useful for identity theft

The combination of some of the types of information from the above table could give the fraudster full control of the victim’s life. For example, the fraudster discovers a telephone number, occupational information and some bank details of a potential victim. He could probably phone him and with social engineering techniques claim that he calls from a bank or a financial organisation, provide the occupational information and request more personal details.

Another example could be a phishing attempt, where the potential thief needs the victim’s full name, e-mail address, bank and/or credit card account information
such as the financial institution’s name). If providing some financial evidence as well, the other party could be easily convinced that the e-mail is not a scam. Obtaining a number of elements of the personal identity information in the table could assist the ID thief in more types of theft, such as registering for online services, requesting and obtaining loans and credit cards. No matter the potential of the theft, the victim is always harmed financially, while the fraudster will both ‘steal’ money from the victim and cost money when the ID theft is discovered and he will try to recover his name.

The results of the disk study enhanced and reinforced the need for researching ID theft further and aided in the construction of the initial hypothesis of the research as cited in chapter one (section 1.4.). The matter that any type of personal identity information revealed from a hard disk can be eventually used for committing ID theft proves the sensitivity of the situation.

The background research confirmed that the only attempts of the current researchers concern guidelines of controlling and eliminating ID theft (Shaobo et al. (2007), Lepofsky (2004), Saunders and Zucker (1999), Jamieson et al. (2007)), while the investigation of ID theft incidents happens around the general computer forensic frameworks.

The following section discusses the existing investigation methods.
2.5 Computer Forensics Frameworks and Methodologies

As already mentioned in chapter one (section 1.4), there is no framework identified in the literature that investigates ID theft. The aim of the current implemented frameworks and methodologies is to create general procedures for digital investigations from data recovery to computer crimes. For this purpose, the generic term digital forensics is mostly used, broadening computer forensics and including all types of digital media that could be forensically examined. Palmer (2001) defines digital forensics as:

- the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

In order to justify the need for developing an independent framework for investigating ID theft incidents, the existing frameworks need to be reviewed and their deficiency in investigating ID theft should be indicated. There is no specific framework or methodology for ID theft investigations in order to compare it with the proposed one. Therefore, the existing generic computer/digital forensic frameworks will be reviewed.

There are over hundred (Leong, 2006) different models that appear in literature concerning digital forensics investigations attempting to aid the analysis of computer crime incidents. A digital investigation relies both on the system and the human aspect (Beebe and Clark, 2005). This is a distinctive characteristic of computer crimes, because the human factor is involved. Current frameworks are broad and try to cover all different aspects of investigations; whereas computer crime incidents and ID theft in particular, as explained in the previous sections, have become targeted and sophisticated. Therefore, the investigation should also become targeted and sophisticated.
A framework can be defined as:

- a supporting structure around which something can be built or
- a system of rules, ideas or beliefs that is used to plan or decide something (Cambridge Advanced Learner’s Dictionary)

This is what the existing frameworks and methodologies provide. However, none of these focus on a specific type of crime in order to adjust the investigation to the set requirements and retrieve evidential data according to the suspected crime.

For almost a decade now, a number of attempts have been made for creating standards for computer forensic investigations. Farmer and Venema (1999) gave general guidelines, focused on the UNIX platform and developed the Coroner’s Toolkit. Mandia and Prosise (2001) gave detailed instructions for specific platforms and focused on computer crime. Lee et al. (2001) studied the investigation of the crime scene, without analysing the entire investigative process. Ó Ciardhuáin (2004), attempted to process the investigation from the information flow side rather than simply focusing on the evidence. Also, efforts in the terms of published books have been made for formalising computer forensic investigations (Schweitzer (2003), Stephenson (1999), Marcella and Greenfield (2002)). These contributions can be described as field manuals and even though they provide valuable guidelines they lack in different areas. For instance, Marcella and Greenfield provide a comprehensive guide about tools, techniques and criminal profiling; however, they focus on legal aspects and keep the actual examination on a high level.

The examination of the present frameworks and methodologies is intended to provide the base for designing the proposed framework. The literature shows that the majority of published examination models are based on their predecessors. Digital evidence and investigations consist of, and combine, numerous different aspects (e.g. technology, devices, systems, nature of the investigation). In such a case it is reasonable to suggest that a possible further improvement is to generate specific formalised approaches to the investigations, as they are always going to differ according to the perspective of the researchers that implement it.
The understanding of present works is going to support the development of a new framework that investigates ID theft. Therefore, the fundamental and most important, as they appear in literature, are discussed below. Their strengths and weaknesses are highlighted in order to give insight for considering the implementation of the ID theft framework.

2.5.1 Carrier and Spafford

Carrier and Spafford have a number of different publications concerning digital investigations; two of these were considered as more enlightening and are discussed herein. In their first published paper, Carrier and Spafford (2003) apply issues to the digital crime scene that are relevant to the physical crime scene. The Integrated Digital Investigation Model concentrates on the computer as the crime scene aiming to provide the digital evidence. The digital crime scene is therefore derived from the physical. This initial framework includes seventeen phases that are based on the existing to date frameworks and is organised in the following five groups:

1. Readiness Phases
2. Deployment Phases
3. Physical crime scene investigation phases
4. Digital crime scene investigation phases
5. Review phase

Carrier and Spafford (2003) have created a checklist of conceptual high-level phases. Their aim is to propose and describe the procedure required in the digital investigation research field. The phases have been applied on existing frameworks and demonstrate an alternative approach to this research area. They study the computer as an individual part of the physical crime scene and treat it accordingly. The model is aimed to be general, abstracted and apply to all types of computer forensic investigations.

Later, in 2006, they introduced the Computer History Process Model, evolving the previous model. Carrier’s doctorate thesis (2006a) is based on it as well. The final framework is published including the following four phases:
1. Observation
2. Hypothesis Formulation
3. Prediction
4. Testing and Searching

They do not claim that the existing frameworks are not correct for specific processes. However, they declare that their proposed model focuses on a different perspective that contributes to them.

The Observation phase observes states and events; the researcher needs to observe the field in order to create a clear picture about the processes and the activities that take place on the investigation. The Hypothesis Formulation focuses on the results of the observation phase and is able to categorise the techniques that will aid the analysis of the findings. The Prediction phase supports the Hypothesis Formulation as the results of this part will prove whether or not the Hypothesis is formed on a structured base and will lead the researcher to the last phase. In Testing and Searching, the tests and experiments that take place in a generally approved manner will probably result in new predictions and evaluate the Hypothesis the researcher has set.

They effectively stated that the purpose of the forensic investigation is to reconstruct the ‘history’ of the digital media under investigation. They also argue that the history of the digital media is unknown to the investigator. Therefore, this is what he needs to investigate those events that resulted altering the state of the media. However, it is based on computationally complex models, a scientific approach that may not be easily comprehensive by the investigators. In addition, the authors argue that the framework’s aim is to assist the existing frameworks and has been tested.

The Computer History Process Model will be further discussed in this chapter, rather than the Integrated Digital Investigation Model, as it is a more recent work and contributed as a research work towards a doctorate.
2.5.2 Casey

Casey (2004) is considered to have published the epitome of computer forensic investigations (Kessler, 2007) on Digital Evidence and Computer Crime. He provides a general computer forensics framework that depicts the relationships among law, computer science, forensic science, and behavioural analysis. The model Casey presents consists of the following four phases:

1. Recognition
2. Preservation, collection, documentation
3. Classification, comparison, individualisation
4. Reconstruction

The first two phases of the framework handle the crime scene, while the analysis of the evidence takes place in the following two phases. Based on Casey, the reconstruction phase can lead the investigator to identify additional evidence and revisit them. The framework contains tasks for the first responders and can be applied on both standalone and networked systems. The findings of the evidence examination are interpreted in a way that could stand in a court of law.

2.5.3 Reith et al.

Reith et al. (2002) attempted to extend the existing framework from the Digital Forensics Research Workshop (DFRWS) (Palmer, 2001) on a standardised process and aid the law enforcement and judicial systems. The Abstract Digital Forensics Model consists of the following nine phases:

1. Identification
2. Preparation
3. Approach strategy
4. Preservation
5. Collection
6. Examination
7. Analysis
8. Presentation

9. Returning evidence

The first three phases of the framework involve the response to the incident, phases three and four the data collection and six and seven the examination of the digital media. In such a distinction of the phases the model becomes more complicated.

The authors themselves admit that the proposed framework is not tested and does not maintain, but it is assumed that it will maintain the chain of custody; a rather important issue for the investigation of computer forensic incidents involving law enforcement and courts.

2.5.4 Beebe and Clark

Beebe and Clark (2005), present a flexible and usable framework that approaches digital investigations on a multi-tier basis; differentiating itself from existing approaches. The Hierarchical Objectives-based Framework extends on Carrier and Spafford’s (2003) single-tier approach (Tipton and Krause, 2004). It consists of six phases, but also includes sub-phases, principles and objectives.

1. Preparation

2. Incident response

3. Data collection

4. Data analysis

5. Findings presentation

6. Incident Closure

Phases one and two respectively involve the preparation of the digital evidence and the response action towards incident. The data collection phase collects the digital evidence that is analysed on the data analysis phase. The second-tier of this phase is also discussed in their research paper. The findings presentation phase documents the findings of the data analysis and the incident closure phase closes the investigation and preserves the related information.
It aims at assisting general investigations rather than being crime specific. The authors claim that the framework is expandable and this was achieved by working on the advantages of existing works and combining different aspects.

2.5.5 U.S. Department of Justice

Electronic Crime Scene Investigation: a Guide for First Responders is the U.S. Department of Justice (2008), structured digital investigation framework. It is intended for responding to the digital crime scene investigation and applies to law enforcement officers. This is the updated version of the U.S. Department of Justice (2001) that failed to be all-inclusive, as commented in the recent version of the document. The updated model consists of the following phases:

1. Preparation: recognize, identify
2. Collection: seize, secure, evaluate, label, document the scene
3. Preservation: package, transportation, storage
4. Examination
5. Analysis
6. Report

This generalised process does not differentiate the computer from other digital media and there is little guidance concerning the actual examination and analysis of the system (Carrier and Spafford, 2003). As it aims to concentrate on the first responders it basically refers on the physical crime scene and the traditional forensics.

Even though, the method is rather systematic for the first three phases, it covers the examination, analysis and report in only one chapter. This effectively adjusts it to a guideline for the crime scene and not a framework that could efficiently assist the computer forensics investigator.
2.5.6 Association of Chief Police Officers (ACPO)

The Good Practice Guide for Computer-Based Electronic Evidence provided by ACPO (2007) is accepted in both the public and the private sector. It is the UK standard that provides the procedure that should be followed by the practitioners and focuses on the collection of evidence. These guidelines are considered as essential instruction to computer forensic investigation and cover different aspects of computer crimes and electronic devices. It comprises of four fundamental principles that are further explained in the original document:

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The guidelines in addition include the Recovery Process that consists of four processes/ phases for computer-based electronic evidence recovery:

1. Collection Phase
2. Examination Process
3. Analysis Phase
4. Report or statement

The collection phase searches, recognises, collects and documents the electronic evidence. The examination process is examined the medium for evidential data, while the analysis phase tests the outcome of the examination for its relevance to
the existing case. The report or statement describes the findings on a forensically sound manner.

The ACPO (2007) Recovery Process is a standard general approach that covers computer forensic investigations. As the guide aims to concentrate on the collection of evidence, limited information is provided for the overall procedure.

2.5.7 Discussion on the existing frameworks and methodologies

The existing computer forensic frameworks are attempts to formalise the procedure of computer forensic investigations, even if their generic nature does not approach the investigation in great detail. They all appear to have positive and negative features that will be discussed in the following paragraphs. This will assist to generate the properties that the ID theft investigation framework needs to contain. In addition, some investigation frameworks that do not only focus on computer forensics, but are related with computer crimes and ID theft contribute to this incorporation. They are discussed in this section as well.

The Computer History Process Model (Carrier and Spafford, 2006) approaches the digital investigation from a different perception than others; the computer history. It is the aspect that the researchers approach the forensic investigation; the fact that it discloses the history of the computer system similar to the physical investigation. The four phases that constitute the Carrier and Spafford (2006) framework (section 2.5.1) are concentrated and descriptive to their content. They manage to verify the idea even though there is a differentiation between the physical and the digital world.

It concentrates on mathematical theory aiming to act as the model that the practical computer forensic models could be based on. The model is highly theoretical with some practical implication (Carrier, 2008). This suggests limited applicability to actual investigations. It would appear that the actual purpose of this work is to assist the academic, rather than the practitioners. However, this framework is a model that the ID theft framework could be built upon. The authors have created a framework that comes from an academic perspective and can be applied to existing frameworks.
In Digital Evidence and Computer Crime (Casey, 2004) has presented a generic model to fit all computer crimes. The interesting part of his framework that is extensively analysed in his book is the evidence processing cycle that prompts the examiner to revisit a phase, when additional information is required. An element that is significant for an investigation and should also be contemplated for the design of the ID theft framework. It is considered as a standard towards a forensic investigation (Ieong, 2006).

Casey (2004) presented a framework that would be general enough to include all procedures of the computer forensics investigation. He even refers to the extraction of data from different digital media, different operating systems and mobile devices. However, it is not focused on a specific area. This positions it as an all-purpose guide and reference to computer forensic investigations.

The book also applies the framework on both computer systems and network environments. This makes it a versatile tool that can be adopted from different investigations. The author has stated in the book that it is written with computer security professionals, law enforcement officers, attorneys and forensic scientists in mind. This book is an effort to formalise the procedure and refer to anyone involved in the computer forensics process. The knowledge acquired from Casey (2004) contributes to the design of the ID theft investigation framework, but due to its non direct link with formal academic research it was decided not to be used as the base model of the framework.

The Abstract Digital Forensics Model (Reith et al., 2002) is a framework intended to be adjusted in the examination of all different, present and future, types of computer crimes and technology. It is descriptive, broad and developed in the terms of the evidence collection and the technology. In addition, it covers a wide range of digital devices.

An interesting feature of this framework is the fact that the authors have tended to create a model that could be adopted for the development of specific methodologies based on a technology or type of e-crime (Ó Ciardhuáin, 2004). This approach strengthens the assumption of creating an ID theft specific investigation framework. Their model is considered, but it was decided not to be used as the base of the proposed framework. The purpose of this framework is to
be considered as a ‘standard’, a broad system that could embed all types of e-crimes. The ID theft framework targets to serve as a tool for the investigator. Therefore, it needs to be focused and detailed concerning ID theft.

The Hierarchical Objectives-based Framework (Beebe and Clark, 2005) proposed a multi-tier investigation framework. It is looking for evidence with more detail, on a lower level, unlike other frameworks and appears well structured overall. This approach is useful for the design of the ID theft framework. However, such an effort on a general investigation framework could also become the weakness of an approach that attempts to assist all types of computer crime investigations. It is easy to overlook some aspects when everything is attempted to be included.

The authors comment that they tend to adjust their method in order to include different types of devices and operating systems. This could cause problems with applicability to future systems.

The Electronic Crime Scene Investigation: a Guide for First Responders (U.S. Department of Justice, 2008) published the American governmental guidelines of approaching computer forensic investigations. There is an interesting part of this framework that needs to be noted. It is the categorisation of evidence based on the type of crime and the potential locations that the investigator should focus his examination for evidential data. Among these crimes ID theft is also present and potential digital evidence is proposed to be found in

- computers, mobile devices, records of online purchases, removable media,
- external data storage devices, PDAs, address books, contact lists, online banking software, information regarding internet activity, financial asset records, electronic money transfers, laminators, calendars or journals, forged documents and false identification, victim information and credit card data, copies of signatures, printed e-mail, notes, letters, ID pictures, check cashing cards and scanners.

An inconsistency appears for the term digital evidence and the highlighted terms. The above evidential types provided are not necessarily digital evidence. For example, laminators and printed e-mails refer to physical evidence and can be used as additional to the digital.
The list with the above digital devices can be useful for the design of the ID theft framework, as it states where related evidence can be found. However, the model is actually a first response and does not focus on the examination of the media. On the contrary, the objective of the ID theft framework is the examination of the media in order to provide relevant evidence with ID theft.

Reith et al. (2002) and the U.S. Department of Justice (2008) separate the analysis and the examination in different phases in the framework. The analysis is about searching and extracting data for them, while the examination is about generating evidential data from the extracted source (Beebe and Clark, 2004). This could be confusing for the practitioners.

The Good Practice Guide for Computer-Based Electronic Evidence (ACPO, 2007) serves the purpose of a formal standard for the UK. It was designed by police officers for police officers and it is therefore a practical guide. Computer forensic investigators across the UK tend to adopt it. However, the guidelines state that digital evidence can be accepted under certain circumstances even when it does not comply with the guide.

Even though it is a general procedure that tends to cover everything, the last edition of ACPO (ACPO, 2007) gives weight on volatile data, network forensics and the Trojan defence. Because of its structure and the fact that it is not an analytical framework it cannot be used as the base for the proposed work. However, it is an accredited guide and should be taken under consideration for the design of the ID theft framework.

Table 7 is a diagram of the existing models and the proposed ID theft framework at a high level (see section 3.3). The table is also the first presentation of the proposed framework’s phases. It was decided to be placed here rather than in the next chapter, where the framework is explained and presented, because it keeps up the continuity of the discussion of this section.

The existing models cannot be compared with the ID theft, due to the fact that they tend to serve different purposes. The table demonstrates where the ID theft framework meets the phases of the existing on the definition and the purpose of the corresponding phases.
<table>
<thead>
<tr>
<th>Carrier and Spafford (2003)</th>
<th>Media Analysis</th>
<th>Evidence Analysis</th>
<th>Scenario Construction</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observation</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Hypothesis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prediction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing and Searching</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preservation, collection, documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classification, comparison, individualisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reconstruction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reith et al. (2002)</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Identification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preparation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approach strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preservation</td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examination</td>
<td></td>
<td></td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Returning evidence</td>
<td></td>
<td></td>
<td></td>
<td>P</td>
</tr>
<tr>
<td>Beebe and Clark (2005)</td>
<td>P</td>
<td>P</td>
<td></td>
<td>P</td>
</tr>
<tr>
<td>Preparation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident response</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data collection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Findings presentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Closure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preparation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preservation</td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examination</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACPO (2007)</td>
<td>P</td>
<td>P</td>
<td></td>
<td>P</td>
</tr>
<tr>
<td>Collection Phase</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examination Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis Phase</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report or statement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7: Frameworks’ Comparison Table
2.5.7.1 Specific frameworks/ guidelines

The increase of computer related crimes lead to the need for computer forensics. Over the last years this term became broader and includes more than computers as special guidelines are published concerning specific devices. Guidelines on PDAs (Jansen and Ayers, 2004), mobile phones (Jansen and Ayers, 2007), internet forensics (Sekar et al., 2004) are sub disciplines of computer forensics and common in the field. The requirement for the development of these specialised areas in computer forensics has demonstrated the need for more focused frameworks and guidelines.

In the literature some research has been identified that has a similar philosophical approach to the one proposed in this thesis. Katos and Bednar (2008) propose a cybercrime investigation framework for developing investigation support among the stakeholders that influence the investigation. It is not a framework that provides guidelines for the investigation procedure, but rather an information system that acquires the information provided by those that take part during a forensics investigation. Their system is generic in order to cover all different types of computer crime, but can be adjusted to a specific type of crime. They mention ID theft as one type of crime to which their model is applicable. Their method aims to assist the forensic investigation in a flexible approach. It could be compared with the presented ID theft investigation framework only in the terms that approaches the investigation in the type of the offence.

However, as a support system it aims before the actual investigations guidelines. It uses mathematical theories as a base standard, probabilities and open problems that make it complex and confusing in some areas. On the other hand, it is a presented system that could maintain the investigation based on the type of crime. Their work though, seems to be under development and their publication does not compare their proposed system with any other similar frameworks or computer forensic investigation frameworks.

In a different aspect there is a call for specific forensic investigation such as the Voice over Internet Protocol (VoIP). Slay and Simon (2008) raised this concern. They propose the development of a software tool that could assist forensic investigations by extracting packets that can reconstruct a VoIP conversation.
Criminals could potentially misuse a tool similar to the proposed one, retrieve conversations and threaten someone’s privacy, or even take advantage of VoIP wiretapped conversations. In both cases the law enforcement should discover a way of recovering such conversations. Even though the product of Simon and Slay’s (2008) research is a software tool and not an analytical framework, it adds to the argument that due to the increase in computer crimes, there is a need to investigate each computer crime independently.

Ferraro and Casey (2005) have published a book aiming to assist the investigation of child exploitation and pornography. Even though the book focuses on the legal aspect, there are specific guidelines that refer to the forensic investigation of the specific type of crime that are enhanced with examples. It seems that the existing published work of Casey (2004) is used throughout the book and applied to child exploitation. The forensic examination of the criminal’s computer system is presented in only one chapter. However, the contact with a physical crime scene is extensively discussed and how an internet investigation can prove the illegal activity and track the criminal. Also, advice on how to secure the evidence and handle it is provided. It provides guidance up to the stage of the trial.

The interesting approach is that it aims to cover the internet investigation, the actual computer and other digital devices investigation, as well as the handling of servers and networks. There has been already one attempt to provide specific guidelines for computer forensic investigations, based on the type of crime. The investigation of child exploitation and pornography is based on different aspects than ID theft due to the different legal and ethical issues involved. This guideline is mostly focused on the legal side, probably because of Ferraro’s law background. It could have been used as a model for the ID theft framework if it was more concentrated on the digital side and if there was more detailed breakdown on the digital investigation. However, the type of crime the book examines is different than ID theft and is dependent on one of the two authors’ existing work. Casey’s (2004) existing Digital Evidence and Computer Crime is already considered to contribute to the design of the ID theft investigation framework.
2.5.7.2 Limitations and properties of the ID theft investigation framework

The planning of a framework that concentrates on the forensic investigation of a single computer crime is not unproblematic. It was seriously considered at the initialisation of this research that this framework should be one step further than the existing ones. The areas that the research had to concentrate on were two; computer forensics and ID theft.

The growth of online ID theft was discussed in a previous section (see section 1.3). The suggestion that this type of crime is expanding, forms the base for the argument for further research. It is an area that demands an approach to assist the handling of the related digital evidence. Under the same philosophy each computer crime should be treated under specific guidelines, simply because each computer crime contains different attributes. The way an investigator should handle for example a child pornography incident is rather different than ID theft (see section 2.5.7.1) due to the content of the digital evidence and the places that this evidence can be discovered in the digital media.

There were a number of problems indicated when trying to build a crime specific investigation framework. There was an argument raised in the beginning of the research that there may be no need for specific guidelines on ID theft, as long as the existing frameworks can also be applied for ID theft investigations. Section 3.1 aims to give the answer to this argument. In brief, the work of the forensic investigator can become a faster and more accurate procedure, when he knows exactly where to search for evidence.

Another issue that appeared was that the product of the research cannot be a high level framework similar to existing ones. No matter how researchers in computer forensics have currently approached the investigation, the proposed work should include specific areas. These are those related with online ID theft and should reach a very low investigation level. In order to achieve it the different types of ID theft can be accomplished needed to be studied and comprehended. The problem with this is that fraudsters tend to develop new ways of acting and the framework should be built in a flexible way that would allow possible near future techniques to be included.
When a very low level framework is being designed though, another concern is raised. The method should include guidelines about the different digital evidence that could be discovered when examining a victim’s and a fraudster’s system. In order to cover this and avoid confusion the framework should be split at some point and guide the investigator towards evidential points that involve the associated part (see section 3.1).

Currently evidence uncovered during an investigation is not classified into particular categories using existing frameworks. This is due to their high-level approach. However, a low level framework has the ability to define special activities that could classify the evidential data based on its quality and relevance to the incident that is being investigated. Such an approach would support the construction of a scenario that could describe what has happened to the penetrated or the rogue system. Then, the investigator would be able to create a focused picture of the incident.

Another issue that was highlighted when reviewing the existing frameworks was that an examination methodically collects information that could profile the perpetrator. The information that is gathered could assist in providing such data. The existing frameworks though do not seem to process it in order to create the fraudster’s profile. If such information was maintained under some constant values for avoiding confusion the investigator could prove that there may be unvarying procedures from the fraudsters that commit a specific type of e-crime.

Ferraro and Casey (2005) claim that the only way not to miss any evidence is to perform a full-blown examination. A type of examination that includes and examines every instance of the digital media. This may be a case for computer forensic investigations and had to be taken seriously under consideration as the ID theft framework had to be persistent; it should ensure that everything is included. The existence of specialised investigation frameworks in the field though, strengthened the premise that it can be achieved.

Another identified difficulty is the low level of the investigation that the framework needs to achieve. Digital media tend to use different operating systems that are developed in different modes. An analytical framework though needs to facilitate all of them. In order to overcome this problem the framework needs to
maintain a conceptual approach that can encompass a range of systems. At the same time a popular Operating System should be selected and examples should be provided, where possible.

Based on the above issues the framework’s design needs to consider the following:

- An in depth understanding and knowledge of ID theft in order to avoid overlooking evidential data.
- To be easily comprehended and applied by the practitioner.
- To include all different systems and technologies, in order to be flexible.

The review of the existing computer forensics frameworks and the above considerations assist in developing the properties that the ID theft framework needs to conform to and are stated below:

- It should divide the investigation concerning the victim or the fraudster.
- It should provide classified evidence.
- It should provide profiling of the fraudster.

The ID theft framework aims to approach the investigation from a different aspect than the existing ones based on the issues discussed on this section. The properties the framework needs to include were generated after the review of the existing literature. Their combination with the aims and objectives of the research (see section 1.4.1) were the principles of the design of the framework that is introduced on the next chapter.
Summary

This chapter aimed to present the relevant state of the art in relation to ID theft investigation techniques. It defined important terms for the understanding of this work and then reviewed ID theft in its online dimensions and techniques. A brief report on traditional ID theft techniques was given and then a more detailed analysis on the innovative ID theft techniques.

Then, issues on the forensic investigation of online ID theft were raised and discussed. The last part of this chapter reviewed existing computer forensic frameworks, methodologies and guidelines in order to identify the properties that the proposed framework needs to include.

The review taken on existing works proves that the forensic investigator may benefit from additional guidance on deciphering ID theft incidents. Therefore, there is a lack of:

1. Structured evidence specifically based on the type of e-crime;
2. Structured profiles of the fraudsters;
3. Prevention and detection techniques for eliminating the problem.

If such work existed, then less effort would be required from the digital forensic investigators for resolving a case.
In this chapter the reader can

- identify the need to construct an ID theft investigation framework;
- understand the planning and design of the presented framework;
- be introduced to the framework’s functionality.

Overview

The previous chapter highlighted the increasing use of online identities and the corresponding increasing risk of identity theft. Internet users are requested to provide personal identity information to perform a number of transactions; online shopping, memberships, social networking, and many others. The increased number of online activities has lead to an increased number of recorded ID theft victims.

The ID theft crimes that occur in digital environments and later require computer forensics investigation suggest that it would be useful to develop a systematic approach for the analysis of ID theft incidents.

This chapter addresses the issues relating to investigating ID theft in a digital environment. Examinations of this type of crime are discussed and the plan of an ID theft computer forensics investigation framework is presented.
3.1 The significance of ID Theft standalone investigation

As determined in the preceding chapters, ID theft is considered a significant threat for individuals and corporations and consists of multiple types of crime. It involves numerous ways of achieving it, both with and without a digital environment. The growth of technology has transformed it to an e-crime and this is where this research focuses. The intention at this point is to demonstrate the reasons that online ID theft should be examined under an individual, crime-focused investigation framework.

The nature of the crime is one of its major differences from other types of computer crimes and consequently the way the digital evidence should be treated. ID theft is a result of a combination of crimes, as these were described on chapter two (see section 2.2). For example, a bank robbery can be achieved purely by force or purely via a computer (hacking) or by some form of combination of the two, e.g. forced extraction of password. However, the victims of the bank robbery will immediately or soon after realise the robbery against them. An ID theft incident, is achieved either by traditional techniques, e.g. shoulder surfing, or innovative, e.g. phishing, or a combination of both such as social engineering. However, there may be a period of time before the victims realise the crime has occurred.

For the purpose of this thesis, all computer based evidential elements will be represented with the term online, whereas all other, secondary elements will be called offline. Consequently, the investigator needs to take into consideration the volume of the offline sources that influence the outcome of the investigation, as a number of offline methods could have been used to assist in committing the crime. The amount of offline evidence that could be added to an ID theft investigation, such as card cloning machines and stolen mail differentiate this type of crime from other computer related and raises the need of treating this type of computer crime in an individual manner.

A characteristic example of this could be the comparison between a hacking offence and an online ID theft incident. In most cases, the source of evidence
available from a hacker is his system and usually intermediate systems that have been used and revealed the method of attack. The investigator will have to trace all evidential data from there. In an ID theft incident the digital evidence also depends on the fraudster’s computer and intermediate systems. However, there are also other factors, such as a card cloning machine that could enhance the evidence. Any supplementary sources that could be found on the crime scene support the investigation and can therefore contribute as evidence for ID theft.

According to FTC, ID Theft Data Clearinghouse (2007) the total number of complaints in 2006 was 246,035, establishing ID theft the top complaint category in consumer fraud with 36 percent. In order to support the need of investigating an ID theft related computer crime as an independent entity an example of an ID theft case for financial purposes can be considered. Based on Cook (2008), the investigator can first focus on credit history, transactions made in the victim’s name, applications for bank accounts, loans and credit cards. The evidence would consist of data, logs etc. formats through various systems within one or even multiple financial organisations. As a result, the investigation is complicated and time-consuming. With identity-related ID theft cases, the investigator will need to consider not only the financial evidence but the personal information gained and subsequent actions triggered by a hijacked identity.

The current computer forensic investigation frameworks are generic and they aim to deal with a number of different computer related crimes from hacking to copyright violation. In respect to the existing computer forensic frameworks (see chapter 2, section 2.5) and based on the continuing rise of ID theft (Grant, 2009), the need to assist the computer forensic investigation of ID theft related crime is imperative.

The growth of e-crime leads to the point that the investigation procedure needs to be focused on different perspectives each time. Different sort of evidence is required, according to the type of crime in order to be concentrated on the unique aspects that characterise it. Simply because the use of the Internet and the public dependency will only grow, there is the argument that methods should be developed to efficiently cope efficient with this rapidly spreading threat (Marwaha et al., 2005). Computer forensic investigators need to be able to use
constructed methods that facilitate and support their actual aim; to provide evidence after the investigation of an incident.

Kay (2006) divides computer crimes in two categories, where the computer is used to commit a crime and where the computer is the target of the crime. A victim’s machine should provide conformational information, so that the theft of data or the fraud against the user will be proved. On the fraudster’s machine the evidential data should be treated in such a way that will reveal the intention of theft. Due to the fact that so many different crimes are involved and alternative techniques can be followed by the fraudsters, ID theft investigations are more complex than other types of crime (Roberson, 2008). Therefore, online ID theft investigations are also considered as more complex for the same purpose.

The proposed ID theft framework is a consecutive procedure that aims to provide a detailed approach for the investigator and specify how evidential data should be treated under this type of e-crime. It also adds knowledge to the examiner as it is not only based on the analysis of the digital media, but also on gathering information about the target of the crime and the fraudster. The framework consists of two levels; a high level, where the basic functionality is presented and then it expands on a low level framework in order to collect the ID theft related specific data.

A prerequisite for the application of the ID theft framework is that the type of the crime is known before the examination. A further requirement once the crime has been identified, is the system being examined. The examiner needs to be aware if they are analysing the victim’s or the fraudster’s system as outlined in the next section.

Victim and Fraudster
An ID theft, like almost all different types of crime, involves two parts, victim and criminal or fraudster. The Oxford Dictionary of English defines victim as a person who is tricked or duped and the fraudster as a person intending to deceive.

The victim is the dupe, the prey, the target. The specific word has been selected in order to describe the person that has been affected emotionally or financially by ID theft.
The word fraudster has been chosen for this work among its synonyms (criminal, deceiver, perpetrator), as it approaches more accurately the intention of the person to commit fraud by acting deceitfully.

There is an approach of distinguishing and discriminating the investigation process between the victim and the fraudster in this research work. It differentiates it among different investigation frameworks as such an approach has not been identified in the literature. The ID theft framework reaches on a very low level of the investigation. The collected data is organised and classified while investigating the crime. This property of the framework adds the need to understand the system on which the data originates.

Different pieces of evidence can be discovered on each side (victim-fraudster) concerning the technique that has used to perpetrate the crime. While the online ID theft techniques can leave evidence on both the victim’s and the fraudster’s system (see chapter 2), it tends to contain different elements on each side (see chapter 4). For example, a phishing e-mail could leave evidence on the victim’s internet logs, while on the fraudster’s system, information about the building of the scam could be found. A malware might leave unknown running processes on the victim’s machine and a source code library on the fraudster’s machine.

This is going to assist the investigator as it aims to focus the examination of the digital media on the side of interest. Therefore, the investigator will work on a structured ground under a procedure that includes only these elements that he needs to search for. A structured approach can reduce the duration that is required for the examination and reduce the chance of evidential material being overlooked.

Classification of evidence

In addition to the above, the proposed framework not only assists the investigation, but also classifies the gathered evidence and attempts to profile the fraudster. The information that is being collected comes from a different aspect depending on whether the media under investigation belongs to the victim or the fraudster. The classification of evidence aims to recognize and categorize evidential data based on the discovered findings.
As digital evidence is fragile (Kornblum, 2002), the investigator needs to precisely preserve and classify the ID theft related. For this reason the preservation of evidence can be maintained when it is structured and classified. The nature and purpose of the evidence appears beneficial for the quality of the findings, when constructing the case report on a later stage. The ID theft framework follows the classification of evidence as derived from and structured upon the admissibility of evidence that appears extensively in computer forensics literature (for example Casey, 2004; Schweitzer, 2003; Palmer, 2002).

The collection of classified evidence among a number of different investigations could also result in assisting future ID theft incident analysis. It is important to capture features of past ID crimes to aid the investigation of future crimes.

**Fraudster Profiling**

Marcella and Greenfield (2002), discuss the concept of profiling the fraudster. The application on the ID theft investigation framework depends on the fact that the victim and the fraudster are going to provide profiling elements from different perspectives. The profiling of the fraudster is drawn from a different aspect when it comes from the victim’s hard disk and different from the fraudster’s hard disk.

Rogers (2003) argues that computer based investigation procedures need to develop in a similar way to procedures in the classic forensic science and include the profiling of the criminal (fraudster). Numerous studies refer to the importance of profiling the fraudster (for example, O’ Block et. al., 1991; Turvey, 2002; Kocsis, 2006). However, it is mainly based on the sex, race, age etc.

This framework aims to identify and analyse the activities taken by the fraudster, in order to understand his methods and techniques. Information will be gathered based on the complexity of the attack that could reveal for example whether there is an intention of financial or identity ID theft (see chapter 2, section 2.2.3). The collection of evidence is able to provide such identification and offer additional valuable indications about the objective of the attack and the skills of the fraudster.

The following sections of this chapter will expand the above arguments, describing the theoretical procedure of designing and implementing the ID theft investigation framework.
3.2 Design Principles

The following paragraphs are going to explain the rationale of this work and set its principles. The framework design was presented at the 5th Australian Digital Forensics Conference (Angelopoulou, 2007).

Fundamentally, a framework is considered as a tool to aid in planning, monitoring and evaluation of research projects (Carrier, 2006). A framework is required in order to achieve a comprehensive and repeatable procedure. In the case of ID theft, it should answer to what information might be stolen and how this information could be stolen. However, on a flexible way that will comply with current and future technologies. The way of achieving this is presented in chapter four, where the framework is thoroughly described.

The major aim of the framework is to collect, construct and represent the evidential data that reveal an ID theft incident. The overall procedure needs to give answers to questions similar to

1. Does file X exist?
2. Did event Y occur? (Carrier and Spafford, 2006)

In case a specific file exists, for example one with malicious content, then the analysis should confirm whether that file has been executed and as a result influences the investigation. The outcome of the analysis should provide accurate results after the analysis of the medium, based on what exists and what has occurred. The investigator should be able to examine every file and any event that influences the behaviour of the system.

As highlighted in chapter two (section 2.5), a review of existing frameworks failed to identify an existing framework targeted at investigating ID theft. Therefore, the proposed work cannot expand or improve an existing ID theft framework; instead the principles of some of the forensics frameworks examined in chapter 2 form the basis for the new framework. The aimed approach to ID theft investigations differs from existing research works. However, the different perspective that Carrier and Spafford (2006) adds to computer forensic investigations was chosen as a basic model for the structure of the proposed framework. However, all of the frameworks that were analysed (see section 2.5) contributed in the design to a degree as outlined in the following sections.
Beebe and Clark (2005) were based on the Carrier and Spafford (2003) model and extended it on a low level that appeared beneficial for the design of the ID theft framework. The ACPO guidelines have been of significant importance while planning this framework. However, these are generic and address the investigation of computer crimes in general. In addition, the U.S. Department of Justice (2001) guidelines have been taken under consideration for the design of the framework. This approach appears as more detailed than the ACPO, as described in the previous chapter and the knowledge gained from its study partially assisted on the design of the proposed framework.

Casey (2004) has also added to computer crime investigations with his methodology. The model is general, in order to include all types of digital investigations. However, some core features were valuable for the design of this framework as well. Reith et al. (2002) focused their model on the law enforcement by creating an extended model. It also assisted in the development of the ID theft framework.

The following section describes how the existing investigation frameworks have contributed to the implementation of the proposed ID theft investigation framework.
3.3 ID Theft Investigation Framework Design

The background research of the existing computer forensic frameworks suggests that the most suitable approach for the ID theft investigation framework would be first to identify and define the key phases. It is based on the Carrier and Spafford (2006) high level model as that distinguishes each phase in such a discrete manner that fits this research.

The processes required for the lifecycle of each phase are based upon ACPO (2007), U.S. Department of Justice (2008), Casey (2004), Reith et al. (2002) Beebe and Clark (2005) and obviously Carrier and Spafford (2006). The framework is classified into two levels. The high level gives the opportunity to the investigator to understand the basic structure of the investigation approach.

Then, the low level of the framework, is a more advanced and detailed stage, where the examination steps become ID theft specific. The procedure unfolds at this level, as it aims to provide all the detailed steps required during the investigation and is adjusted to the needs of an ID theft incident.

### 3.3.1 High Level structure of the ID Theft Investigation Framework

The investigation is divided into phases, where every phase represents a major procedure during the ID theft investigation lifecycle. The purpose of the phase is to collect and include procedures that are related with each other. When these procedures are completed the outcome of the phase will be created. Then, the examination can continue to the next phase and search for further information in another group of investigation procedures.

After the literature research and consideration of the existing computer forensics frameworks (see section 2.5), it was decided that four phases are sufficient to constitute the ID theft framework, as in Carrier and Spafford (2006), Casey (2004) and ACPO (2007). There is no need to expand its structure with more phases as in other models. The four phases support and maintain its consistency and functionality. The naming of each phase is adjusted to the needs of the ID theft framework. The terminology chosen for defining each phase is considered to be
representative for the needs of the proposed framework and could be comparable to the Carrier and Spafford (2006) model.

The purpose of presenting the framework at the highest level first is to introduce a simple, conceptual outline to the reader (Beebe and Clark, 2005). This states the highest level of the framework’s formulation that is presented in figure two.

The graphical method used is based on the UML activity diagram, as a flexible and commonly understood method. It is preferred among other methods because it is a simple demonstration of what occurs during an operation (Schmuller, 2004). It represents not only sequential, but also parallel operations, required for the design of the framework.

The four key phases at the high level of the model are: Media Analysis, Evidence Analysis, Scenario Construction and Evaluation. The Media Analysis phase is concerned with identifying information of evidential value collected from the media. This forms the foundation for the Evidence Analysis phase, where the digital media is examined for evidential data. Information of evidential value derived from the Evidence Analysis phase should be included in the Scenario Construction phase. This is closely linked with the Evaluation phase, where particular attention should be paid for assessing the produced scenario. The scenario that is produced in the Scenario Construction phase collects the evidential items that resulted from the previous phase and aims to construct a possible scenario concerning the history of the incident. This scenario will be assessed in the Evaluation phase.
The forensic analyst needs to have a start and an end point during the analysis of the digital media. At some stage in the examination though, he may need to circulate among the intermediate phases when additional information is required. The structure is inherited from the software engineering’s iterative waterfall model that supports the same principle (Mall, 2004).

The information flow in figure 2 highlights the fact that the analyst should always be able to return from the Evidence Analysis to the Media Analysis. The analyst may need to search for any further data that might appear of value during the examination of the media. In the same way the analyst may need to revisit the Evidence Analysis at any stage in the Scenario Construction for any information that could emerge and indicate further investigation. Then, the Scenario Construction will need to be validated. However, the Evaluation phase involves the possibility to recall any of the previous phases of the investigation process in order to prove the objectivity of the research outcome. Figure 3 sets the variable names of the phases in order to be used during the discussion of the framework and demonstrates the lifecycle of the ID theft investigation framework with the variables.

<table>
<thead>
<tr>
<th>Description</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Investigation</td>
<td>I</td>
</tr>
<tr>
<td>Media Analysis</td>
<td>Pma</td>
</tr>
<tr>
<td>Evidence Analysis</td>
<td>Pea</td>
</tr>
<tr>
<td>Scenario Construction</td>
<td>Psc</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Pe</td>
</tr>
</tbody>
</table>

Figure 3: Investigation Framework Variables’ and representation

### 3.3.1.1 Inputs and Outputs

The inputs and the outputs define the processing requirements of each phase and are integrated in the high level of the framework. Their existence is imperative as they constitute the purpose of the phase and define the object and the subject of the examination.

Every phase receives an input; it is the object that needs to be entered into the phase, examined for a particular set of features and the results forming the output. This output is the subject of the phase that should be also examined in order to
provide its own results. The importance of the output will be verified in the following phase, where it will be used as an input. Consequently, the initial input of the framework should always be the digital media under investigation and the final output should always be the case that has resulted after the examination.

The practice of using the output of the preceding phase as an input to the subsequent supports the coherence of the research outcome and functionality (see Beebe and Clark (2005), Ó Ciardhuán (2004)). The I/O practice is presented in figure four. It highlights the necessity of the procedures presented at this level of the framework. The I/Os support the procedure in the terms of continuity during the investigation’s lifecycle. They are individually presented in chapter four, on the analysis of the framework.

![Figure 4: The input / output practice](image)

3.3.2 Low Level structure of the ID Theft Investigation Framework

3.3.2.1 Practitioners’ requirements gathering

The detectives of Gwent police were requested for a meeting when a draft version of the framework was designed. The aim was to contribute with their practical knowledge in the low level of the framework and verify that each necessary task was covered from the design. Eventually, there were meetings in the form of informal interviews that assisted the requirements gathering for the framework.

The practitioners initially described how an investigation is performed in a real environment. They mentioned the procedures they follow and the way they normally treat ID theft. The idea of a crime specific framework was appealing to them. Then, there was a discussion on the draft version of the framework. Due to the fact that framework reaches the investigation on a low level, it needs to incorporate all possible areas that the examination could retrieve evidence from.
The components were designed and specific questions were addressed to the detectives concerning the applicability of these components.

Their point of view was particularly useful for the construction of the final structure of the framework. The practitioners’ requirements gathering assisted the development of the framework and its aim to become a tool for the investigators.

### 3.3.2.2 The structure of the framework

The following paragraphs provide a detailed review of the structure of the framework to demonstrate its usability; outlining the key phases, processes, activities, and instructions. Table 7 (section 2.5.7) compares the proposed framework with the existing. The comparison was enlightening in the terms of realising the actual breakdown the ID theft framework needs to consist of. It assisted on setting the design requirements and the properties of the framework (see section 2.5.7.2). There is no other ID theft specific framework in the literature in order to compare the breakdown of each phase. Therefore, the terminology was chosen based on the background research of the generic models as the most representative and descriptive for each element.

The **phases** are individual procedural components inside the framework. The names that were selected to represent them describe their purpose in the terms of the ID theft investigation. The **input** and the **output** of the phase form the criteria that should be satisfied for the phase to operate, and the resulting output. They both consist of a number of **processes** that are a centralised, structured approach for the satisfaction of the I/O. However, on a low level the processes need the **activities** as a customised, focused ID theft guideline that clarifies the required actions set by the processes. All processes produce activities, but some activities need to focus on a further detailed level, the **instructions**.

The instructions act as directions for the activities and offer additional characteristics to the examiner. Some instructions throughout the framework require declarations about their application and these are called **objectives** as they intent to clarify the purpose of the instruction. Figure 5 represents the breakdown of the elements that constitute the framework.
In detail, the investigative framework consists of four phases as shown in figure 5. In order to assist the ID theft investigation, the research outcome of this work should provide an in-depth procedure integrated among these four phases.

As each phase includes an input and an output, the output that is produced in every phase is used as an input to the following phase (see Beebe and Clark (2005), Ó Ciardhuáin (2004)). A phase also consists of processes that appear for the first time on the low level.

There are twenty-two processes in the framework and the actual analysis of the digital media in the terms of ID theft occurs from process four to fourteen among three phases.

The processes satisfy the needs that their preceding input or output processes require. The processes relate to evidence produced either from the victim’s or the fraudster’s side where necessary. This division depends on what the process attempts to identify. Internally each of the processes contains one or more activities. They provide the fragmentation of the procedure for the practical achievement of the process’s function. In other words, the detailed route the investigator needs to follow in order to fulfil the requirements set by the process. Activities are used either as an input or as an output to the process, based on their nature. Therefore, they hold the characteristic I/O in front of their classification in order to be identified throughout the framework (see section 3.3.1.1).

Figure 5: Representation of the framework’s elements (lowest level)
Some activities need to provide comprehensive direction that can be found in the instructions. They are expected to determine the purpose of the activity and provide the effective application of the process. The instructions answer the question of ‘where’ the supportive data can be discovered. In fact they reach into detail, concerning the expected findings for the investigator, and at the same time, they are as generic as possible to be flexible.

The instructions are followed by the objectives that answer the question of ‘what’ the investigator is expected to discover during the execution of the activity. The instruction is the last action of the activity. It mainly adds a value to the required activity. The instructions and the objectives are considered as embedded detailed add-ons to the activities as they provide additional information for assisting the investigator.

In summary: Every phase requires some form of Input; this is then modified or examined by the Processes present within that particular phase. In turn the phases are built up from a number of Activities. These activities may then contain Instructions and Objectives although this is not always the case. Not all activities include instructions and not all instructions an objective. Once a phase has completed all of the required activities, instructions and objectives, the output from that phase becomes the input for the next.

The investigation framework complexity and the relationships among the phases can be found in Appendix F (II-III). Because of their size only an in text preview of the graphs can be found in figures 6 and 7 aiming to provide an overview to the reader. Each stage of the framework is represented in a different colour and shape, in order to create clear illustration of the graphical demonstration for the practitioner. Vivid colours have been chosen for assisting a symbolic recall of the framework’s breakdown to the reader, as recommended by the work of Stone (2002, 2006).

In figure 6 the centre clear circle of the diagram represents the framework and the four phases can be found inside it in indigo circles. The framework expands its tasks with the I/Os, fuchsia for the input, teal for the output. The victim is purple and the fraudster violet diamond. All the events of the framework are symbolized in assorted different colours. The processes are represented in pink squares, the input
activities in orange oval and the output activities in sky blue. The instructions, where applicable, are yellow round corner rectangle and the objectives are green yellow hexagons.

Figure 7 illustrates the four phases on the corners in indigo circles of a four-sided figure and the rotation among them is represented with single or double ended arrows according to the framework’s need. The input of each phase is a circle coloured in lime and the output in turquoise. The processes are in lavender colour embedded in each I/O that they fit in. The orange circle represents the input of the process and the pink the output of the process. The round corner rectangle in green colour in the corresponding process stands for the distinction between the victim and the fraudster. The dotted lines signify the relationships among the phases.
These diagrams do not follow a standard diagram symbolisation as they need to be comprehensible to the investigators that may not be experienced in reading formal modelling techniques. The selected diagram symbolisation uses a combination of mind map (Buzan, 2003) and organisation chart (Koontz and Weihrich, 2008). They were chosen among other methods as they expand and satisfy the purpose of creating commonly understandable, uncomplicated diagrams.

The relationships that occur in each phase independently can be found in Appendix F (IV). The relationships aim to preserve the chain of custody (Mohay et al., 2003; Stephenson, 1999; Mandia et al., 2003), vital for forensically sound evidential data. The instructions and the objectives are not included in diagrams III and IV, as their functionality is embedded in the corresponding activity.
Summary

ID theft is a type of old fashioned crime that transformed into a cybercrime because of the intense ‘investment’ in online sources. To investigate this and other computer related crime there have been a number of developments in the area of computer forensics. As a result, a number of procedures have been developed to guide the forensic process. Due to the nature of ID theft it has been suggested that a specific e-crime driven investigation framework is required.

This chapter has presented the design principles of the proposed ID theft investigation framework which distinguishes the examination in the victim’s and the fraudster’s side. It classifies the evidence and profiles the fraudster. This type of investigation method aims to provide results on a more crime-focused basis regarding an ID theft incident.

In the following chapter, the framework is analysed. It provides a detailed approach for the investigator to follow in case of an ID theft incident.
This chapter analyses

► the structure of the investigation framework;
► the purpose of every Phase;
► the functionality of every Phase; and
► can be used as a reference to the investigative procedure.

Overview

The ID theft investigation framework is an analytical tool to aid the computer forensics investigator in analysing ID theft incidents. The structure and functionality of this framework builds upon comparable existing investigative forensic frameworks, as discussed on chapters two and three. Unlike current generic frameworks, it focuses on the examination of a specific computer crime and presents detailed low-level procedures to be undertaken. Furthermore, the investigation process divides the examination on the fraudster and the victim’s part. The aim is to guide the investigator towards specific examination processes throughout the analysis.

The following sections describe the flow of the ID theft investigation framework to the lowest level. The methodology is supported, where appropriate, by an example of evidence based on the current technology, operating systems and applications. The examples are mostly based on the Windows XP operating system, as it is considered the most popular desktop operating system over the last years and from the initiation of this research project. (Johnston et al., 2003)

The following sections provide a detailed guide outlining the full functionality of the framework and justifying its design. The chapter is literally divided in two parts. First the inputs and outputs of the high level phases are presented and then the low level of the framework is explained. The flow of the ID theft investigation framework is presented altogether in an index list form on the low level in
Appendix E. This document only arranges the list of all tasks serving the purpose of an overview for the framework.

An abstracted procedure for the investigator can then be found in Appendix H. This document is intended to become a field manual for the investigator. It gives guidelines and summarises the purpose of every phase and provides basic information for every stage of the framework, so that the investigator could return to it anytime during the examination and get some further information.

Appendix I provides a documenting procedure for assisting the investigator on recording the whole investigation and analysis. It is a table based document that can be used for the recording of the findings related with the case. It is suggested as a primary documentation tool for the ID theft investigation framework as it provides all the elements of the framework that are required for the investigation.

4.1 High Level Inputs and Outputs

The previous chapter explained the need of the framework to expect receiving an input and producing an output in each phase as well as the interaction among the phases. At this section, the I/Os of the framework will be presented and described. Their functionality needs to be clarified at the high level and provide the required justification for continuing to the low level of the framework.

Media Analysis Phase

The media analysis phase (Pma) does not differ in nature from the existing frameworks discussed in chapter two. The procedure that the investigator is required to undertake at this phase is established from previous works (see chapter 2) as it involves the contact with the crime scene and the media acquisition. Phase 1 cannot be excluded from the framework as it maintains its continuation and cohesion.

It requires as an input any type of digital storage media that could give as an output possible ID theft data to further the investigation. At this point the term ‘digital media’ is going to represent any type of computer storage device.
Possible digital storage media incorporated into the media analysis include computer/ laptop/ server hard disks, external hard disks, RAID hard disks, PDAs, memory cards, PCMCIA cards, mobile phones/ SIM cards, USB memory sticks, tape back-ups, floppy disks, CDs and DVDs. These are only indicative as they are based on the current technology. The handling of each storage media is in accordance to the ACPO preservation guidelines (ACPO, 2007).

An ID theft investigation does not differ from other computer crimes in requiring specialized processing of the media that constituted the crime. Even though the most common media for analysis is the hard disk drive (Beebe and Clark, 2005), occasionally the processing may need to begin from that media that is suspected to contain the most valuable evidential data.

Evidence Analysis Phase

The Evidence Analysis phase (Pea) takes as input the possible ID theft data provided by the Pma and analyses it. At any time during an investigation additional data relevant to the investigation may become available, in which case the analyst may need to return to the previous phase relating to the analysis of the Digital Media.

The aim of the investigator is to discover evidence at this stage that can be connected with ID theft. This is the required output. At the end of this phase the examiner should hold unprocessed evidential data that he should deal with in the third phase.
Scenario Construction Phase

The input of the Psc should be the Evidence (the output) from the Pea. The aim is to process and classify the evidence to produce a Scenario as an output. The way will be explained in the following sections, at the low level of the framework.

The scenario is the chain of events constructed by the investigator based on the findings of the media examination. Only when sufficient information is gathered, the analyst is able to provide the possibilities to explain how the evidence was created. At this stage it may be necessary for the analyst to search for further details on any of the two previous phases (Pma and Pea). The importance of evidence reconstruction is mentioned by Carrier and Spafford (2004) and Beebe and Clark (2004).

![Scenario Construction Diagram](image1.png)

Evaluation Phase

The evaluation phase (Pe) takes the output from the scenario construction in order to present the final output for the whole investigation. Its purpose is to examine the produced from the previous phase output and in order to evaluate and verify the outcome of the investigation. The evaluation is an important procedure of the investigation. Every framework that exists in the literature and considered for the design of the ID theft framework attempts to verify and present the outcome of the investigation (E.g. Carrier and Spafford, 2003; Casey, 2004; ACPO, 2007)

The output of this case is a constructed case that includes all the evidential material that was discovered. In case there is a need, the analyst should be able again to revisit all previous phases for the validation of the analysis.

![Evaluation Diagram](image2.png)
The two levels of the framework (high and low) can be found on Appendix F (I) represented on organisational charts. In addition, Appendix G corresponds to a flowchart diagram of the high level of the ID theft investigation framework.

### 4.2 Overview of the Low level ID Theft Investigation Framework

Each phase contains one or more processes that define the procedure that needs to be followed in order to satisfy the input and the output of each phase. They define activities that assist in the fulfilment of each process. These will be further explained in the following sections, where each phase is individually analysed. The framework’s evidence source distinction between the victim’s or the fraudster’s system area also appears in this section. Where the framework is split a letter V stands for the victim and an F for the fraudster corresponding to the separation.

The phases contain specific inputs and outputs which must be satisfied, in order to continue to the next phase. The processes are incrementally numbered within the phases to demonstrate the logical continuity of the framework.

An initial informal meeting with members of the Gwent police assisted on the design of the low level. The police investigators added their practical knowledge to some of the key aspects included in this work. They recommended key areas that the investigation should focus and how the evidence should be treated.

In this section each phase is presented and accompanied from a figure that represents it. A brief description of each phase follows.

![Figure 12: Phase 1, Media Analysis Representation (Low Level)](image-url)
Phase 1, is structured according to the ACPO (2007) guidelines and the U.S. Department of Justice (2008). The processes required to support the Digital Media input, identify the available evidential sources on the crime scene -1-, collect them from the crime scene -2- (Casey, 2004) and image the digital media -3- under investigation at the computer forensics laboratory. These processes are a standard crime scene work, as described on the existing frameworks as well.

The investigator is then requested to identify evidential data -4- concerning either a victim (V), or a fraudster (F). Whichever is identified, the discrimination of the framework should be followed until the end of the investigation. General information that identifies the target -5- and the threat agent -6- should be revealed. The output of these set of processes is ID Theft Data.

Phase 2 takes as an input the ID Theft Data identified in the previous phase. This is achieved by identifying the available for analysis data -7-, analyse the target -8-, by differentiating the procedure for the victim (V) or the fraudster (F). Also, the analysis of the threat agent -9- based on the findings is provided by the process. The evidence is collected in process -10- and classified in -11-. The output is Evidence.

Figure 13: Phase 2, Evidence Analysis Representation (Low Level)
Phase 3. Scenario Construction

Process 12. Structure of evidential data
Process 13. Structure threat agent’s profile
V. Victim
F. Fraudster
Process 15. Scenario outline
Process 16. Scenario preparation

Phase 3 takes the Evidence Classification as an input and structures the evidential data -12- and the threat agent’s profile -13-. Different information is classified by the victim’s (V) and the fraudster’s (F) medium. Then, the analysed digital evidence is prepared -14- for the output of the phase that it will be converted into a scenario of what has occurred. The scenario outline -15-, aims to represent the incident, based on the discovered evidence and prepares draft documentation with the investigator’s prediction -16-. The output is the Evidence.

Phase 4. Evaluation

Process 17. Scenario Testing/Evaluation
Process 18. Scenario Clarification
Process 19. Case Construction
Process 20. Case Clarification
Process 22. Evidential Case

Figure 14: Phase 3, Scenario Construction Representation (Low Level)

Figure 15: Phase 4, Evaluation Representation (Low Level)
Phase 4 evaluates the 3 previous phases. The input is the scenario examination as resulted from the previous phase. It needs to be tested -17- and clarified -18- in order to ensure the validity of the procedure.

The output of the framework is going to be a Case. The case needs first to be constructed -19- including all the evidential files, then clarified -20- in relation to the requirements of the case and evaluated -21- to ensure confirm that all included evidence is valid. The last process is the representation of the case -22-, where the case report is constructed.

4.2.1 Summary of High Level stages and Example Scenario

The following scenario demonstrates a hypothetical application of the framework. It is an initial attempt to apply it, aiming to create an overview of what has been discussed up to this point. It involves an incident with little information and an indication that ID theft has been committed.

South Wales’ police visit a suspect for credit card fraud. On site they discover blank credit cards and a computer that could be used as a tool. They collect the potential evidence and transfer it to the lab for investigation. The ID theft investigation framework will be applied for the examination.

Media Analysis phase

The analysis begins with process 1. The investigator is supplied with the digital media for this investigation; the system’s hard disk for this case. The detectives have already collected, and identified it (Process 2). The analyst is imaging (Process 3) the hard disk. The purpose is to identify data that might indicate ID theft. Process 4 informs the next stage of the process confirming whether the evidence has been collected from a victim or a fraudster. However, for this case the evidence is derived from the fraudster. From this point and on, the investigation would follow the framework devised for examining the case based on the fraudster perspective.

Process 5 identifies the target, that could be a vulnerable system, or information published on the public domain, where the fraudster could focus for potential victims. Process 6 aims to identify the threat agent and his purposes. Any
information gathered so far that could reveal his intention. At the end of this phase, ID theft data should be present, concerning the prospects of the fraudster. This will be analysed on the next phase.

Evidence Analysis phase

It aims to analyse the evidence from the original media, the investigator analyses the ID theft data under three processes: 7, 8, 9; data, target and threat agent respectively. The target analysis is divided to victim and fraudster, as each category guides the investigation towards a different perspective. For this scenario, the fraudster perspective must be followed.

The output of the phase should be evidence derived from the analysis of the digital media. Process 10 collects the evidential data that occurred from the three previous processes and then this data will need to be classified, on process 11 based on their content.

Scenario Construction

At this point, the evidence extracted from the investigation needs to be classified. Process 12 structures the evidential data, while 13 structures the threat agent’s profile that is divided into the victim’s and the fraudster’s side, as there is going to be different sort of data gathered to give the investigator the information required to construct the attacker’s profile. Process 14 structures the analysed digital evidence that refers to the incident.

The output is Evidence and the processes that follow are 15, the scenario outline and 16, the documentation preparation. At this point the investigator has a clear overview concerning the investigation. He could tell with structured evidence whether the suspected individual has committed ID theft.

Evaluation

The input is the scenario examination, Process 17 evaluates the scenario assumption and 18 clarifies the scenario. The output gives the investigator a case he needs to construct (Process 19), clarify (Process 20) and evaluate (Process 21). Finally, process 22 is the evidential case representation, the computer forensic report. All evidential data discovered will be described in a manner that could also be admissible in a court of law, charging the fraudster of the case.
The above scenario is a brief representation of how the high level of the framework could be applied in practise. The investigator benefits from a customised, structured ID theft procedure that guides him throughout the investigation of a suspected ID theft. The framework covers the investigation from the first contact with the crime scene to the analysis of the evidence and the construction of the case report for a court prosecution.

The following sections continue with the analysis of the low level of the framework, where detailed guidelines for its functionality are provided.

4.3 Structure of the Low Level Analysis

The phases of the investigation framework are analysed based on the structure below and each one is accompanied by a representative graph that includes the stakeholders of the phase. The specific breakdown of presenting the framework has been selected, as it guides the reader each time one step forward in the phase while studying and describing it. It follows the structural flow of the framework and explains each task successively as it moves from the high to the low level.

Phase Overview: a brief description of the phase at the low level. A figure accompanies the description of every phase. The purpose is to familiarise the reader with the objective of the phase.

Input/ Output Overview: a description and the purpose of the input of the phase are provided in more detail than section 4.1. Then the description and the purpose of the output are produced. It presents what the investigator is searching for (input) and what he expects to generate (output).

Processes’ Specification: the description and the purpose of each process (see section 4.2) that is necessary to generate their required I/Os. The following sections explain the processes in more detail.

Process Table: this is a flowchart type table where the breakdown of every process in a phase is presented. The grey areas of a table indicate that no data is present.

The numbering of the tasks that constitute the framework has been mentioned in previous paragraphs. However, it would be beneficial to explain it further here to detail the breakdown of the framework.
The four phases are numbered sequentially from one to four. Then, follow the input and the output of the phase that are referred in the framework by their names (e.g. Digital Media). The processes are numbered from one to twenty two and continue successively among the phases. The word Process is found in front of their number to emphasise them.

The activities follow the processes. The letter I stands for the input process and the letter O for the output process. Next to the letter the activity receives the number of the process it belongs to and a succeeding number that differentiates it among the others. For example I.1.2 is the second input activity of process one or O.2.1 is the first output activity of process two. At this stage the framework is divided between activities that deal with the victim examination and activities that deal with the fraudster. Where an instruction is required it is denoted by the word Instruction and the corresponding number. The instructions are not successively numbered, but renumbered among the phases, as they refer to the activities they belong. Therefore, the objectives, where applicable, follow the same tactic as they refer to their instructions. They are represented by the word Objective, the number of the instruction and a successive number. For example, Objective 1.3 is the third objective of the first instruction.

This structure was selected as the most logical and easiest to represent the framework. Because of the extent of the framework, a characteristic symbolisation of each task should be chosen. This symbolisation should be straightforward for the investigator to distinguish it among the tasks of the framework.

The framework aims to guide the practitioner through the investigation of ID theft. In some areas it becomes detailed on how an activity needs to be carried out. However, intentionally in most areas it directs the procedure without detailing a method. The investigator may choose a convenient approach for him, based on his experience and availability of tools. As a result, the flexibility of the framework is preserved.
4.4 Phase 1, Media Analysis

4.4.1 Phase 1 Overview

The Media Analysis (Pma) aims to identify, secure and examine the source of digital media. It includes the first contact with the crime scene. It recognises and handles the media; therefore receives the name Media Analysis.

Therefore, during the Media Analysis phase, the investigator should identify, collect and secure the media that may provide digital evidence and begin the process to discover possible ID theft data. Pma requires the following input and produces the following output:

Input: Digital Media, the identification and forensically sound preservation of digital media. Although this is part of standard forensic practice it is included here for the completeness of the framework.

Output: ID Theft Data, the identification of evidential data relating to ID theft and the initial distinction between the victim’s and the fraudster’s evidential data. In addition, the target identification provides the intention of the fraudster, as well as the threat agent’s identification and intention. For example, a victim’s vulnerable system could show an initial attempt of an external, individual attempt to steal personal data. Figure 16 introduces the processes, followed by their activities.
4.4.2 Digital Media

The purpose of these processes is to give the investigator an insight into conducting the first on scene response related to an ID theft incident. However, the procedure that needs to be followed is based on the generic frameworks and guidelines (see section 2.5).

It consists of the following three processes:

1. Source identification
2. Digital media collection
3. Image Acquisition

The following sections describe in detail their application along with the activities that are included in the process and any instructions and objectives that may appear.
4.4.2.1 Process 1, Source Identification

One of the most important processes during the investigation, the source identification component of the model is in agreement with widely acceptable existing computer forensic guidelines (ACPO (2007), U.S. Department of Justice (2008)). This basic step cannot be avoided or altered, as the investigator or first-on-scene officer must identify digital media that may contain relevant information to prepare for further analysis (Beebe and Clark, 2005). The process includes the following activities:

**Media selection (I.1.1.):** The media selection activity refers to the search of defining the digital media, present at the crime scene that need to be collected and examined, and to create and maintain the required chain of custody. For its completeness, it requires two instructions to be followed as these are declared in section 3.1:

- Instruction 1. Online Data
- Instruction 2. Offline Data

**Live System (I.1.2.):** This covers the possible need to treat a live system. It does not apply to all cases; however, when the system is still active the investigator should behave according to Grance et al. (2004) and follow the instruction:

- Instruction 1. Check the operating system

**Keep record of the scene (O.1.1.):** It is the product of the input activities I.1.1 and I.1.2. Lee (2001) mentions the recording of the scene can include documenting, photographing, and in some cases video recording. He noted an apparently insignificant, slight error in the collection of the evidence has the possibility to destroy an entire case. Furthermore, to keep record of every online and offline data found in the scene, e.g. the amount of memory installed on the system (Carrier and Spafford, 2003). The recording of the scene can be used as an evidential element in court.

The instructions that were met above dictate:

- **Instruction 1. Online Data:** is considered any data that is directly linked with the computer system. Instruction 1 requires the following two objectives:
Objective 1.1. Evidential computer storage components: At this point, the investigator needs to search for any computer storage components that can provide evidence and select them. E.g. unplugged USB flash memory, CDs.

Objective 1.2. Computer storage media: it refers to all computer storage media that the investigator will be able to use for the analysis. E.g. Hard disk

Instruction 2. Offline Data: In agreement to Shinder and Tittel (2002), it is the physical evidence, which can be seen or touched. There is, in most cases, a significant number of offline data that can influence the outcome of the investigation. It is always, considered as additional evidence, other than the computer system itself (Marcella and Greenfield, 2002). For instance, a fraudster’s case may identify ‘tools’ that have been used from the fraudster. The outcome of the investigation could be influenced, when these tools are proved to have an effect on the result. The most commonly known offline data are mentioned on objective 2.1.:

Objective 2.1. Any offline data that can be used as additional evidence: based on the current knowledge possible offline data is described below, in order to stretch their importance and link with the purpose of the objective (Shinder and Tittel, 2002 and Marcella and Greenfield, 2002):

Computer peripherals: any type of computer peripheral that could reveal information of evidential value, e.g. a printer could retain a copy of data in memory or hardware keyloggers that could be found attached on a victim’s machine and register the key logs.

Telephone devices: any type of telephone device can hold personal data. Mobile phones can store a decent amount of personal data that can be used as evidence, but also modern cordless phones for example, can save contact number or even send text messages.

Personal belongings: anything personal that could be used as source of evidence. For example, books or magazines found near a fraudster’s working area and provide elements of his work. Printouts at the fraudster’s site, software purchase receipts and notes could be evidential as well.

Litterbins: are always good sources of discovering people’s habits. For example, a victim’s litterbin can show that the victim throws away bank statements without
shredding them first. The victim could be simply questioned about such an occasion, but when dealing with the fraudster it could add information that he has recently discarded, such as notes.

Card cloning devices: this type of device should immediately alert an investigator, as it is a popular tool among fraudsters for cloning for example, credit cards.

Video screening equipment: may be used when having someone under surveillance in order to uncover his daily habits (Wright et al., 2008). E.g. hidden cameras installed in someone’s property.

Digital camera: may keep a number of photographs in the memory that could be used for constructing a case. E.g. prove that a fraudster was stalking for possible victims.

on Live System activity:

Instruction 1. Check the operating system: Keep track and capture any volatile information that can be available from the system at that specific moment. The live system acquisition has been discussed by a number of experts, who examine live systems (Adelstein, 2006). The included objectives are:

Objective 1.1. Shutdown: after capturing the information, the investigators should either shut down the system or immediately proceed with objective 1.2 and immediately disconnect it. The purpose of this dual option depends on the nature of the machine. As recommended by Gwent police (Appendix K), if the machine runs a server O.S. then it should be shut down to avoid data corruption.

Objective 1.2. Disconnect: after having the system shut down first or by simply unplugging the system from the back of the computer to avoid activating a backup power supply.
The following table represents the Source Identification process with its activities and highlights the instructions and their objectives.

| Process 1: Source Identification |  
|---------------------------------|-------------------------|-------------------|-------------------|
| I.1.1. Media Selection | I.1.2. Live system | O.1.1. Keep Record of the scene |
| 1. online Data | 1. check operating system |  |
| . evidential computer storage components | . shutdown |  |
| . computer storage media | . disconnect |  |
| 2. offline Data |  |  |
| . any offline data that can be used as additional evidence |  |  |

Table 8: Process 1 - Source Identification

4.4.2.2 Process 2, Digital Media Collection

The actions taken during the Digital Media Collection provide the investigator with the sources of evidential material. During this process, the investigator will collect the digital media, based on the ACPO (2007), U.S. Department of Justice (2008), (Marcella and Greenfield, 2002).

As the process’s name instructs, the following activities need to be performed, according to traditional computer forensic collection methods (Casey, 2004):

Identify different digital media (I.2.1.): The examiner of the incident should identify the different digital media available for this activity, in order to be able to proceed to the next activity. I.2.1 involves one instruction:

Instruction 1. Generic digital device storing personal data

Secure / isolate digital media (I.2.2.): Securely extract digital media from the system in order to avoid alteration or damage (Marcella and Greenfield, 2002).

Collect / package digital media (I.2.3.): The secure collection and packaging of the media according to the guidance of the U.S. Department of Justice (2008). This activity encloses the sealing of the collected media as part of Document (O.1.2) that maintains the chain of evidence.

Document (O.1.2.): The investigator needs to document the process of acquiring the digital media collected for analysis. This is also performed in order to preserve the chain of custody (Marcella and Greenfield, 2002).

Identify different digital media activity (I.2.1.) requires the following instruction:
Instruction 1. Generic digital device storing personal data: Any digital device that can save personal data can also be used to accomplish an ID theft. According to the current technology, the following devices can be used by a fraudster. However, future technology may present additional devices and for this reason, these devices are not specifically mentioned into the framework, but only as a current guide to the investigator (see section 4.1): Computer / Laptop / Server Hard Disk, External Hard Disk, Mobile Phone / SIM Card, Raid Hard Disks, Tape Back-ups, CD / DVD, PCMCIA cards, Memory Cards, USB Memory Stick, PDA, Floppy Disk.

The table representation of the Digital Media Collection process:

<table>
<thead>
<tr>
<th>Process 2. Digital Media Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Generic digital device able to store personal data</td>
</tr>
</tbody>
</table>

Table 9: Process 2 - Digital Media Collection

4.4.2.3 Process 3, Image Acquisition

The Image Acquisition process mandates the bit-stream back up of the digital media. Best practice requires a bit-stream copy of the media that includes all the areas of the disk to perform a thorough computer forensic investigation. The Common Digital Evidence Storage Format Working Group (DFRWS CDEFS) (2006) proposed the standardisation of the digital evidence storage for the advantage of the investigator. They suggest that the digital evidence should be stored and transmitted in a single format; however, this approach was abandoned less than a year later due to the lack of resources.

This process consists of the following activities:

Select appropriate tool (1.3.1.): This is based on the type of case, the investigator’s preference and training. It can be achieved in a number of ways. E.g. dd UNIX command.

Protect media from possible alteration of data (1.3.2.): It is very important for the whole procedure to ensure the media is protected from any form of alteration, usually with a hardware write blocker. The investigator should preserve
the digital media from alteration caused by viruses, physical damage, data corruption and any other possible risks that could destroy the evidence.

Image the original media (I.3.3.): After the selection of the tool and the protection of the media, the investigator needs to create the image according to the National Institute of Standards and Technology (NIST) (as cited in Schweitzer, 2003).

Store safely original media (I.3.4.): The original media should be stored at a safe place, e.g. an evidence locker. Limited access should be given to these lockers in order to minimise potential problems with the integrity of the chain of evidence.

Back-up the image, work on that (I.3.5.): Because of the risk of damaging or losing the image of the media, it is recommended that the investigator should create a back-up copy of the image and work on this copy. The computer forensic analysis suites, such as Guidance EnCase back up the image automatically, so there is no need for an additional copy.

Create Cryptographic Value (I.3.6.): The cryptographic algorithms appreciated by computer forensics people as they calculate a file’s checksum for verification, e.g. MD5 or SHA-1. They evaluate the association between the original media and its copy for the investigator’s gain and prove the integrity of the evidence for the representation in a court. (Carrier and Spafford, 2003). Both images should be checked. Best practice dictates that the cryptographic hash is taken straight after the image is made.

The table below reflects the breakdown of the process:

<table>
<thead>
<tr>
<th>Process 3. Image Acquisition</th>
<th>I.3.1. Select appropriate tool</th>
<th>I.3.2. Protect media from possible alteration of data</th>
<th>I.3.3. Image the original media</th>
<th>I.3.4. Store safely original media</th>
<th>I.3.5. Back-up the image, work on that</th>
<th>I.3.6. Create Cryptographic Value</th>
</tr>
</thead>
</table>

Table 10: Process 3 - Image Acquisition
4.4.3 ID Theft Data

Once digital media has been collected and preserved, evidence related to the ID theft incident should then be sought. ID Theft Data is the preparation of the detailed media analysis. The ID theft investigation framework is a detailed procedure that requires ID theft as the object of the crime. Therefore, in the case where no ID theft suspicious or related data is identified, then the application of the framework and perhaps the case would terminate at this point. A more generic computer investigation should be considered as more suitable or a specific framework more appropriate to the investigation.

The application of the ID theft framework assumes prior knowledge of an ID theft for it to be applied. It would be either based on the report from a victim or on evidence from a fraudster.

In addition, multiple ‘specialist frameworks’ could be placed after the Digital Media input of Phase 1 to deal with other specific types of computer crime. The ID theft framework is designed to accommodate this future work.

At this point, the digital media will be transferred from the crime scene to the laboratory for further analysis. The investigator is required to perform a quick initial search of the image in order to maintain an overview of its contents before the detailed analysis on the next phase.

ID Theft Data consists of three processes that are examined in detail in the following sections:

4. Evidential data identification

5. Target identification

6. Threat Agent identification / intention

4.4.3.1 Process 4, Evidential Data Identification

The Evidential Data Identification process provides the first distinction of the ID theft investigation framework from the generic existing computer forensic frameworks, as it distinguishes the procedure between the victim (V) and the fraudster (F). It is the initial categorisation of the evidential data and after
ensuring all contingences of the process, the examination can be performed under the corresponding flow.

In most cases, the examiner is aware whether the media belongs to the victim or the fraudster category, however this process aims to identify and verify it. The findings intend to strengthen the continuity of the evidence and its validation as the investigation will be focused on the side of interest only. The activities on both sides of this process assist this validation towards the investigator and verify the source of the crime (Victim-Fraudster).

The activities that need to be undertaken on this process for a Victim’s (V) digital media are:

Existence of malicious software (I.4.1.V): Most types of unusual system processes may hide a malicious code existence in the system, virus vaults and logs (Schweitzer, 2003) and it may be responsible for stealing personal data. The existence of malicious code can be identified in slightly different places, depending on the operating system. For example, for Windows operating systems the investigator should identify whether malicious code is running at the start-up folders, the scheduled tasks or the memory cache and verify the creation of new registry keys and files (Carvey, 2004). An antivirus scan will also assist in this function.

Existence of unsecured transactions (I.4.2.V): It involves any type of transaction that could take place over an unsecure, unencrypted network. This can be identified for example, by the media’s history log, where the investigator can discover with a glance, the user’s web browsing habits. The purpose of this activity is to provide clues whether the victim could have exposed private information while carrying out unsecured transactions.

Vulnerable system (I.4.3.V): Establishing a lack of security software can show that the system has been vulnerable to an attack. The user has not taken under consideration the protection of the system; for example, no firewall or no antivirus is installed (Shinder and Titel, 2002).

Victim evidential data list (O.4.1.V): It is the product of the above activities, where the identified evidential elements are listed.
The activities for the Fraudster’s (F) side are:

Existence of malicious software code (I.4.1.F): Not only is considered what is written in I.4.1.V activity, but also and with more emphasis the existence of malicious source code in the media. For example, the creation of programming code from the fraudster in order to achieve his purposes. The fraudster may be writing his own malicious scripts.

Forensic extraction software (I.4.2.F): Forensic extraction software in a computer system that has been suspected for ID theft could mean that the user himself is trying to retrieve data for digital media, with malicious purposes, e.g. to discover personal data.

Hacking tools (I.4.3.F): A collection of hacking applications in a digital media usually reveals the intention of the user to exploit them. The investigator can easily identify such type of applications by conducting a search throughout the media. They can be recognised by their name that usually reveals their use. At this stage, the identification involves only those applications that do not involve an altered file name.

Fraudster evidential data list (O.4.1.F): As in O.4.1.V, the product of the above activities, where the identified elements are listed.

The table represents the Evidential Data Identification process, the categorisation between victim and fraudster and the required activities:

<table>
<thead>
<tr>
<th>Process 4. Evidential data identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>V. Victim</td>
</tr>
<tr>
<td>I.4.1.V existence of malicious software</td>
</tr>
<tr>
<td>I.4.2.V existence of unsecured transactions</td>
</tr>
<tr>
<td>I.4.3.V vulnerable system</td>
</tr>
<tr>
<td>O.4.1.V Victim evidential data list</td>
</tr>
<tr>
<td>F. Fraudster</td>
</tr>
<tr>
<td>I.4.1.F existence of malicious software</td>
</tr>
<tr>
<td>I.4.2.F forensic extraction software</td>
</tr>
<tr>
<td>I.4.3.F Hacking tools</td>
</tr>
<tr>
<td>O.4.1.F Fraudster evidential data list</td>
</tr>
</tbody>
</table>

Table 11: Process 4 - Evidential data identification

4.4.3.2 Process 5, Target Identification

While proceeding with this process, the investigator is expected to identify the reason the machine became a target. It is beneficial for the outcome of an ID theft investigation to be able to determine the source of the problem by recognising significant causes. Such data can be collected from either the victim’s or the
The ID Theft Investigation Framework

fraudster’s side. It aims to add information concerning the investigation based on the initial findings as this was identified on the previous process. The framework aims not only to identify the clues of an ID theft incident, but also to add knowledge on what caused it by an initial attempt to identify and categorise the available information up to this point. This process will assist and will be used for the classification of the evidence on process eight, later in the framework and produces a listing of the identified information.

The activities of the Target Identification are:

**Vulnerable systems (I.5.1.)**: It concerns unsafe systems that can easily become targets of unlawful use. The investigator needs to state at this point whether he considers the system under investigation as vulnerable, based on the collected information so far, for example no antivirus is installed. A vulnerable system is more likely to become a target of an attack than a protected system. The purpose is to determine if the system has been part of the crime, based on its unsecure exposure on the Internet.

**Published information (I.5.2.)**: According to the evidential findings revealed so far, the investigator is expected to be able to identify published personal information that could have been used for fraudulent purposes. E.g. Evidence of information being published on social networking web sites. This is an activity for adding some additional information for the profiling of the target identification. However, the user could have placed all sorts of personal information on a networking web site, but had his credit card skimmed in a restaurant. Any similar situation cannot be covered from the computer-based ID theft framework. It is related with traditional or offline ID theft. If such a case exists, it will be revealed during the detailed analysis of the media. The victim could volunteering provide such information to the investigator.

**Individual/ Corporate (I.5.3.)**: Determine whether the target has been an individual (personal computer connected on the internet) or corporate (business computer connected on the internet). However, this piece of information is most of the times available to the investigator before the initialisation of the examination. In case of a business medium, the examiner proceeds with the assistance of the corporate security policy as additional to the framework. Such a
policy is going to help him identify any inconsistencies between the processes that run to the system and the security principle of the organisation. However, this does not interfere with the flow of the framework’s processes.

Target Identification list (O.5.1.): A list that includes the target identification data as provided from the previous activities.

The Target Identification process table follows:

<table>
<thead>
<tr>
<th>I.5.1. vulnerable systems</th>
<th>I.5.2. published information</th>
<th>I.5.3. individual / corporate</th>
<th>O.5.1. Target Identification list</th>
</tr>
</thead>
</table>

Table 12: Process 5 - Target identification

4.4.3.3 Process 6, Threat Agent Identification/ Intention

According to Bidgoli (2004), a threat agent is:

An individual or organisation that has the potential to realise a threat against a specific target.

Therefore, in the case of investigating an ID theft incident, the threat agent is interpreted as the fraudster. However, no matter whether the investigation concentrates on the victim’s or the fraudster’s perspective, it is of great importance for the analyst to identify the intention of the fraudster. It is going to add expertise and intelligence on the way future investigations will take place as the investigator will be considering the identification of the fraudster during the analysis and he will be keeping track of it. This can be achieved from the collection of information added at this stage and analysed on the following phase (Process 9).

The activities of the Threat Agent Identification / Intention process are:

Internal/ External attack (I.6.1.): Concerning the ID theft evidential data discovered, the incident should be considered either as a direct internal network attack or as an external source (Vidalis and Jones, 2005). It is based on the way the system has been accessed. This piece of information is going to give the first hints for profiling the threat agent in process nine.

Individual/ Corporate (I.6.2.): This activity provides the threat agent’s intention, based on the information revealed so far from activity I.5.3. The
The examiner should determine whether the fraudster retrieved private information from an individual or a corporate system (Vidalis and Jones, 2005). This can later reveal information about the intelligence and the intention of the fraudster.

Threat agent identification list (O.6.1.): The output activity creates a list with the data identified so far from I.6.1 and I.6.2.

The table showing the functions of the Threat Agent identification / intention:

<table>
<thead>
<tr>
<th>Process 6. Threat Agent identification / intention</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.6.1. internal / external attack</td>
</tr>
<tr>
<td>I.6.2. individual / corporate</td>
</tr>
<tr>
<td>O.6.1. Threat agent identification list</td>
</tr>
</tbody>
</table>

Table 13: Process 6 - Threat Agent identification / intention

4.5 Phase 2, Evidence Analysis

4.5.1 Phase 2 Overview

After the detection of the ID Theft Data (Process 2), the investigator is requested to examine the digital media in detail and identify specific clues concerning the crime in phase two. He should create the evidence trail that will help him confirm an ID theft incident.

As described in chapter three, the examiner may consider returning to phase 1 at any time for the accurate and precise outcome of the investigation. He may go back to the previous phase in order to re-examine a whole process or a single activity. Figure 17 is a fragment of the framework’s relationships as already presented in chapter three and found on a full page version on Appendix F (IV). The purpose is to show the interaction between phases one and two.

Figure 17: Relationships between phases 1 and 2
Pea produces the input and output below:

**Input:** ID Theft Data Analysis, examines in detail the ID theft data discovered in the overview of evidence that was completed in process two as part of the Media Analysis phase. However, the examiner will analyse in detail the data on the digital media. Furthermore, during this input he will analyse the target of the attack, based on the owner of the digital media (victim or fraudster) and analyse the fraudster, according to the findings.

**Output:** Evidence, it presents the specific ID theft data that was discovered from the Digital Media which forms of the input of this phase. It is the attempt to collect and classify the evidence discovered after the analysis of the digital media, verifying the ID theft incident.

The following sections look at each process of the phase independently and describe the use of every activity it consists of. Figure 18 represents the phase.
The ID Theft Investigation Framework

ID Theft Data Analysis

Phase 2

Evidence Analysis

Evidence Collection

Process 10. Evidence Collection
I.10.1. Use evidential finding list, O.8.1.V or O.8.1.F
O.10.1. Create list of evidence based on ID Theft types
O.10.2. Target evidence list
O.10.3. Threat agent evidence list
(from Process 9)

Process 11. Evidence Categorisation
I.11.1. Use evidential sorting list, O.8.1.V or O.8.1.F
O.11.1. Create evidence classification list

II.8.1. Malicious Software
II.8.2. Local-based e-mail
II.8.3. Web-based e-mail
II.8.4. Embedded Object scripting access languages
II.8.5. Recently accessed documents
II.8.6. URL information
II.8.7. Security permissions
II.8.8. Application histories
II.8.9. Instant message history log
II.8.10. Databases
II.8.11. Spreadsheets
II.8.12. Number systems
O.8.1.V. List evidential findings

F. Fraudster
II.8.1.F. Internet bookmarks
II.8.2.F. Steganographic search
II.8.3.F. Embedded Object scripting access languages
II.8.4.F. Installed Software
II.8.5.F. Track illicit software use
II.8.6.F. Recently Accessed Documents
II.8.7.F. Filenames
II.8.8.F. URL information
II.8.9.F. Local based e-mail
II.8.10.F. Web based e-mail
II.8.11.F. Operating System registry entries
II.8.12.F. Security permissions
II.8.13.F. Instant message history log
II.8.14.F. Malicious software
II.8.15.F. Malicious source code existence
II.8.16.F. Web server communication
II.8.17.F. Databases
II.8.18.F. Spreadsheets
II.8.19.F. Images
II.8.20.F. File Processes
II.8.21.F. Number Systems
O.8.1.F. List evidential findings

Process 9. Threat Agent Analysis
I.9.1. Intention
I.9.2. Motivation
I.9.3. Knowledge / Skills

I.7.1. Identify all files of the system
I.7.2. Recover deleted files
I.7.3. Slack / Unallocated space
I.7.4. Hidden partitions
O.7.1. Define files that can be used as evidence

Figure 18: Phase 2 - Evidence Analysis Breakdown
4.5.2 ID Theft Data Analysis

The purpose of the ID theft Data Analysis is to perform a detailed examination for ID theft related evidence. The investigator has already identified ID theft information from Processes 4, 5 and 6 in phase 1. While the output of the previous phase (ID Theft Data) produces observation, detection and identification of fraudulent use of someone’s identity, in the ID Theft Data Analysis the investigator’s aim is to analyse this information. The analysis of this data is of significant importance, because the evidence related to the case will be examined.

The ID Theft Data Analysis at its completion produces the ‘facts’ that the examiner needs.

It consists of three processes that will be explained in this section:

7. Data Analysis Process
8. Target Analysis Process
9. Threat Agent Analysis Process

4.5.2.1 Process 7, Data Analysis

The Data Analysis aims to identify evidential data pertinent to the case in every single part of the digital media. As the most common medium of computer forensic investigations is the hard disk, the examples provided mostly refer to a hard disk analysis. However, the framework is focused on the file system and it can be applied to any digital device. The following activities are part of the process:

Identify all files of the system (I.7.1.): As in a traditional computer forensics investigation, evidential data can be discovered in all parts of the digital media. It is a prerequisite for the investigator to identify all the areas that files can be retrieved.

The activity refers to the following instructions:

Instruction 1. Existing files
Instruction 2. Deleted, remaining
Instruction 3. Hidden data
Instruction 4. Encrypted / password protected
Instruction 5. Temporary files / folders

Recover deleted files (1.7.2.): When the deleted files have been identified, they should be recovered in order to examine their content (Kizza, 2005). For example, a hex editor can be used to identify them.

Slack / Unallocated space (1.7.3.): The use of special tools can help the investigator examine the slack and unallocated space of the medium, as information such as network logon names and passwords can be stored there. For example, analyse the Windows O.S. swap file as outlined in Wang et al. (2005).

Hidden partitions (1.7.4.): They are created mainly to store files that the user does not desire to be visible in the operating system. Farmer and Venema (2005), provide information about revealing hidden partitions. An ID thief could hide sensitive data this way. However, there are cases that a hidden partition could be installed by the manufacturer. Still in such a case it should be recovered and examined. Applications such as Norton Partition Magic can uncover a hidden partition.

Define files that can be used as evidence (O.7.1.): This function aims to collect the files identified in the previous activities that could be used as possible evidence. The investigator can collect and archive the evidential data discovered, in order to create a concrete structure of the files. These files will be analysed in detail at the following activity.

The instructions that were met above in Identify all files of the system (I.7.1.) disclose:

Instruction 1. Existing files: search through all the existing files that appear in the medium during the search.

Instruction 2. Deleted, remaining: check the deleted, but remaining files that exist in the medium. The investigator is able to retrieve deleted data that have remained and can probably provide additional proof. (Wang et al., 2005)

Instruction 3. Hidden data: possible illicit data can be missed if the hidden files are not viewed (Gallegos, 2005). The investigator needs to check the system for hidden files. For example, a fraudster could hide a file that contains information about his victim or even employ rootkits to hide his action.
Instruction 4. Encrypted / password protected: Encrypted files are significant and with the aid of special tools the decryption and password recovery of files can be managed. Casey (2002) proposes practical approaches on overcoming encryption. The existence of encrypted files raises suspicion on its own.

Instruction 5. Temporary files / folders: Wang (2003) recommends file shredders in order to wipe temporary files from a system. However, in case the user has not done so, files with extensions such as *.tmp and *.chk can provide information to the investigator about the user’s actions. The framework attempts to identify these cases with Instruction 5, even though they cannot be guaranteed. Any anti-forensic techniques that may have been used complicate the life of the investigator (Kessler, 2007b).

The representation table of the Data Analysis process:

<table>
<thead>
<tr>
<th>Process 7. Data Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.7.1. Identify all files of the system</td>
</tr>
<tr>
<td>1. existing files</td>
</tr>
</tbody>
</table>

Table 14: Process 7 - Data Analysis

4.5.2.2 Process 8, Target Analysis

The Target Analysis concentrates on the analysis of data that connect solely with the victim (V.) or the fraudster (F.). This process provides the investigator with detailed activities concerning the analysis of the digital media and the practice that will reveal the requested information for the ID theft case. It is important to mention at this point that the ID framework describes the procedure of identifying the ID theft evidence. An amount of the activities in this process can be interrogated using the search features of most forensics software to find the evidence. The purpose of this process though is to describe the procedure and demonstrate what evidential findings are connected with ID theft.
The initial identification of evidential data appeared in process four. At this stage, the investigator is required to use this information as an initial input and analyse in depth the elements of the system that provided ID theft data.

In order to prove ID theft, the investigator is required to examine some further parts of the fraudster’s digital media in comparison with the victim’s. Therefore, the fraudster’s side includes more activities to be undertaken than the victim’s media. For example, there is no actual need to examine the pictures on the victim’s digital media. This would not add any value to the analysis, whereas it is important to examine the fraudster’s images, as they could indicate a filing of potential or past victims.

In the following section, Target Analysis - V. Victim is first described and represented and then the Target Analysis - F. Fraudster.

The activities for the Victim (V.) are:

**Malicious software (I.8.1.V):** Perform a thorough anti-virus check with a collection of antivirus programs. An infected with malicious software system could mean that personal data may be stolen. The activity examines the identified malicious software from I.4.1.V.

Skoudis and Zeltser (2003) provide a very detailed reference on the characteristics of malicious software and code and give guidelines to the investigator on how to analyse incidents that involve malware, based on the malware’s behaviour and timeline. In addition, Carvey (2004) provides an insight of the footprints left behind by malware, as well as the detection of rootkits that can be of great value for the investigation procedure.

The activity requires the following instructions:

Instruction 1. Monitors web-browser activity / network traffic
Instruction 2. Accesses contact list records
Instruction 3. Accesses clipboard contents
Instruction 4. Trojans that collect personal info
Instruction 5. Software Keylogger (hosted)
Local based e-mail (1.8.2.V): The e-mail correspondence of the user can reveal the relationship between the user and other contacts. The investigator proceeds with the rules and procedure he would follow for forensically analysing e-mail messages, although he concentrates on evidence that is related solely with the ID theft incident.

According to the ACPO (2007) guidelines, the e-mail headers are available usually from the e-mail client program of the user. They can reveal information about the sender, the receiver, the date of the message and even the content. In such a case, valuable data concerning the e-mail exchange of the user can be revealed. It is specifically valuable for incidents where Phishing is involved. The storage archives can assist to the e-mail analysis, e.g. *.dbx, *.pst, *.mbx.

Web-based e-mail (1.8.3.V): The web-based mail relates to the web browser and its analysis is based on a different perspective than the local based e-mail. Information about the existence of web-mail account logins can be found on cookies, history, typed URLs and cache of a system for windows systems. As Akin (2003) mentions, web-based mail has to deal with the amount of information that is stored locally by the web browsers. Any open relays that promote spam e-mail should be examined by their originated IP address as well as the e-mail headers.

A sophisticated attack will involve anonymous web servers, proxy servers and anonymous SSH tunnels. The investigator in order to trace evidence, he should examine the e-mail headers and discover the original IP address. The actual investigation is also based on classic techniques for analysing e-mail and is combined with information extracted from the URL, as described below. For example, the index.dat file can provide information for a Hotmail webmail account.

Embedded Object scripting access languages (1.8.4.V): As long as web pages embed scripting languages such as JavaScript, hidden threats lie beneath. The victim’s storage media may reveal evidence of worms that send information back to the fraudster (Evers, (2006), Lemos, (2006)).

Recently accessed documents (1.8.5.V): The recently accessed documents as identified on the hidden files on Windows O.S. (\Documents and
Settings\user\Recent\) can provide valuable information to the investigator concerning the files and folders the user has accessed relatively recently. However, the recent documents history can be disabled for the Windows, by altering the Registry key \[HKEY_CURRENT_USER\Software\Microsoft Windows\CurrentVersion\Policies\Explorer\] (PC Tools, 2002). On KDE Linux for instance, the recently accessed documents are stored in \[../home/user/.kde/apps/share/RecentDocuments\]. The user can avoid them being recorded only by changing the permission of the folder to read only (Greene, 2002). In such a case, the investigator is unable to recover any information.

**URL information (I.8.6.V):** Examine the information being kept on the system from the use of the Internet. The activity also inspects the identified unsecured transactions from I.4.2.V. For example, the index.dat file of the Internet Explorer can give valuable URL information about the user’s actions. Such information includes web browser history, cookies, and temporary internet files. The examiner can reconstruct the web activity of the user. (Jones, 2003) The default path for Windows O.S. is \[...\Temporary Internet Files\Content.IE7\index.dat\]

There are two instructions here:

Instruction 1. URL cache
Instruction 2. URL activity record

**Security permissions (I.8.7.V):** The security permissions that have been set to the operating system can recover potential insecurities. The security event log should be examined in order to check any alterations and login dates and time. The detailed examination identified the vulnerable system referring to I.4.3.V.

**Application histories (I.8.8.V):** Similar to I.8.5.V, the history kept by several applications can reveal his footprints. The log files of suspicious installed applications should be examined. They can provide information, such as access times.

**Instant message history log (I.8.9.V):** In case instant messengers are installed, the history log (when enabled), as well as the user’s contact list could provide valuable information to the investigator of the digital media.

**Databases (I.8.10.V):** Possible evidence resides in databases nowadays, as they are widely used by computer users in order to assist their daily activities. The
The investigator needs first to check the existence of databases. In case an ID thief gains access to such information on a victim’s medium, he could use it for his own purposes. A user could maintain databases that include assets and financial records for instance.

**Spreadsheets (I.8.11.V):** A victim may use the spreadsheets under the same perspective with the databases (I.8.10.V.) and store financial information.

**Number systems (I.8.12.V):** Number system searches can reveal information about stored phone numbers, addresses, security pins, postcodes, etc. and assist the investigator identify possible information leaks and uses.

**List evidential findings (O.8.13.V):** This output activity produces a summary with the evidential findings resulted after the analysis of the victim’s medium.

The instructions of Malicious software (I.8.1.V) request during the analysis that the examiner identifies the following at the behaviour of the malware:

**Instruction 1. Monitors web-browser activity / network traffic:** whether the malware monitors the web-browser activity or monitors the network traffic of the machine.

**Instruction 2. Accesses contact list records:** whether the malware accesses the victim’s contact list records.

**Instruction 3. Accesses clipboard contents:** whether anything saved temporarily in the clipboard contains financial information, such as bots, aiming to financial information.

**Instruction 4. Trojans that collect personal info**

**Instruction 5. Software Keylogger (hosted)**

The URL information (I.8.6.V.) activity holds the following instructions:

**Instruction 1. URL cache:** Can be viewed with the help of special tools such as the Web Cache Illuminator (2008) and investigate all the cache memory of the system, including visited web pages and images.

**Instruction 2. URL activity record:** Can reveal the typed URLs from the user, which is important information concerning the user’s activity and web site visiting habits.
The following table represents the Target Analysis process for the victim (V):

<table>
<thead>
<tr>
<th>Process 8. Target Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>V. Victim</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.Monitors web-browser activity/network traffic</td>
<td>1.URL cache</td>
<td>2.URL activity record</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.Accesses contact list records</td>
<td>2. ACCESS activity record</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.Accesses clipboard contents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.Trojans that collect personal info</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.Hosted Software keylogger</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 15: Process 8 - Target Analysis (V. Victim)

The activities for the Fraudster (F.) are:

**Internet bookmarks (I.8.1.F.):** A detailed exploration of the Internet bookmarks reveals information about that person’s habits. Even if the web page names have been saved with an alternative name in order to avoid tracing, the investigator needs to verify every page.

**Steganographic search (I.8.2.F.):** Steganography is a technique used by fraudsters to ensure the masking of a file. As it is quite difficult to identify the existence of such a technique, Schweitzer (2003) recommends the use of Stegdetect (2004), a tool that discovers the existence of steganographic methods. The use of these methods refer to the fraudster’s side, as it is possible to attempt embedding evidence to ‘innocent’ files or images, in order to avoid those being uncovered. Kessler (2004) writes on behalf of the Federal Bureau of Investigation (FBI) and provides useful guidelines concerning the forensic investigation of Steganographic techniques.
In addition, the existence of steganographic software should also be checked in the system. It would reveal the fraudster’s intention to use it.

**Embedded Object scripting access languages (I.8.3.F.):** The same as V. Victim, activity I.8.4.V.

**Installed software (I.8.4.F.):** The software installed on the user’s machine can indicate his intention and lead the investigator to important clues about his habits. Such as forensic extraction software that was identified in I.4.2.F. It is not about examining the legal software installations, but rather the purpose and intention of using the installed application. For example, the intruder may use tools like web design software aiming to conduct DNS Poisoning or Man-in-the-middle attacks for pharming or phishing respectively.

The activity requires the following instructions:

Instruction 1. Web design applications  
Instruction 2. Existence of Anti-Forensics applications  
Instruction 3. System process eraser

**Track illicit software use (I.8.5.F.):** Illicit software can be identified by the .exe files on a hard disk search, the System Registry and the System Information. (Marcella and Greenfield, 2002)

**Recently Accessed Documents (I.8.6.F.):** The same procedure that was followed in activity I.8.5.V.

**Filenames (I.8.7.F.):** The computer criminals tend to hide sensitive content files; the investigator needs to examine the filenames of the system. Any suspicious or inconsistent filenames can provide potential information left available by the fraudster.

**URL information (I.8.8.F.):** The same as I.8.6.V. In addition, any information that can be extracted from discussion forums and internet blogs would be of the interest of the investigator, as they would reveal the concerns and interests of the fraudster.

The instructions that are needed for this activity are:

Instruction 1. URL cache  
Instruction 2. URL activity record
Local based e-mail (I.8.9.F.): The same as activity I.8.2.V.

Web-based e-mail (I.8.10.F.): The same as activity I.8.3.V.

Operating System Registry entries (I.8.11.F.): The system registry files can provide a review of the system and valuable information for the fraudster’s latest actions. The latest typed URLs for example on Windows O.S. can be retrieved from My Computer\HKEY_CURRENT_USER \Software\Microsoft\InternetExplorer\TypedURLs

Security permissions (I.8.12.F.): The same as activity I.8.7.V.

Instant message history log (I.8.13.F.): The same as activity I.8.9.V.

Malicious software (I.8.14.F.): The discovery of malicious software in the media could mean that the fraudster is maintaining a malicious software archive that has already used or intends to use. E.g. Trojan horses or botnets. The examiner can use MD5 or SHA1 hashes and NIST hash sets to check this software. Alternatively he could refer to the Common Malware Enumeration (2007) list for any additional information on the identified malware or to communities, such as Offensive Computing (2009). Additional information about the functionality of the malware is provided there and also the actual malware can be downloaded.

Malicious source code existence (I.8.15.F.): It is not only the identification and examination of the malicious software that provide evidential data for the fraudster’s purposes, but also the existence of writing or altering malicious source code. This has obviously been already identified in I.4.1.F. The investigators need programming skills to reverse engineer and identify the content of the unknown malicious code and connect it with the ID theft incident. Otherwise, he needs to refer to a programmer.

Web server communication (I.8.16.F.): In cases where the investigation reveals evidence linked with web server communication, instances of malicious actions, Denial-Of-Service attacks and DNS Poisoning should be examined according to the classic computer forensic investigation method. There are great possibilities that such communications are linked with the ID theft incident. These communications could involve intermediate machines. The analysis of network
traffic and additional tools, e.g. packet sniffers could probably reveal information about the web server communication (Kessler and Fasulo, 2007).

**Databases (I.8.17.F.):** The same as V. Victim, function I.3.14. The fraudster could maintain data for exploiting new victims or even hold information about perpetrated attacks. However, it is quite unlike for a sophisticated fraudster to disregard the possibility of being discovered and such information being revealed.

**Spreadsheets (I.8.18.F.):** The same as I.8.10.V. The spreadsheets can have the same value as the databases for the fraudster, as he could possibly keep track of his actions.

**Images (I.8.19.F.):** The image files found on the fraudster’s disk can provide additional evidence, as the investigator may discover images from past victims, possible victims, or even contacts of the fraudster. For instance, the fraudster could collect pictures for forging passports.

**File Processes (I.8.20.F.):** This function refers to any process of the files that appear as suspicious to the system during the investigation so far. For example, the investigator has identified duplicates of a file in several places then, he should compare the consistency of these files.

**Number systems (I.8.21.F.):** The same as activity I.8.12.V.

**List evidential findings (O.8.1.F):** The same as activity O.8.1.V.

The purpose of the instructions on this activity for the Installed software (I.8.4.F.):

**Instruction 1. Web design applications:** It can indicate the fraudster’s activity on phishing or malicious web site designing.

**Instruction 2. Existence of Anti-Forensics applications:** It can indicate the fraudster’s intention to alter data with anti-forensic techniques. (Davies et al., 2004)

**Instruction 3. System activity eraser:** It involves the identification of any type of software that wipes data from the media. It indicates the fraudster’s intention to erase evidence, it can be also considered as an anti-forensic technique. However, it stands as an individual data file in order to stretch the importance of wiping data, rather than altering. E.g. Wipe Expert 1.6. (2006)
For the URL information (I.8.8.F.),

Instruction 1. URL cache: The same as activity I.8.6.V< Instruction 1.

Instruction 2. URL activity record: The same as I.8.6.V< Instruction 2.

Table 16 summarizes Process 8. Target Analysis – F. Fraudster:

<table>
<thead>
<tr>
<th>Process 8. Target Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>F. Fraudster</strong></td>
</tr>
<tr>
<td>I.8.1.F. Internet bookmarks</td>
</tr>
<tr>
<td>I.8.2.F. Steganographic search</td>
</tr>
<tr>
<td>I.8.3.F. Embedded Object scripting languages</td>
</tr>
<tr>
<td>I.8.4.F. Installed Software</td>
</tr>
<tr>
<td>I.8.5.F. Track illicit software use</td>
</tr>
<tr>
<td>I.8.6.F. Recent Documents</td>
</tr>
<tr>
<td>I.8.7.F. Filenames</td>
</tr>
<tr>
<td>I.8.8.F. URL information</td>
</tr>
<tr>
<td>I.8.9.F. Local based e-mail</td>
</tr>
<tr>
<td>I.8.10.F. Web based e-mail</td>
</tr>
<tr>
<td>I.8.11.F. O.S. Registry entries</td>
</tr>
<tr>
<td>I.8.12.F. Security permissions</td>
</tr>
<tr>
<td>I.8.13.F. Instant message history log</td>
</tr>
<tr>
<td>I.8.14.F. Malicious source code</td>
</tr>
<tr>
<td>I.8.15.F. Malicious software</td>
</tr>
<tr>
<td>I.8.16.F. Web server communication</td>
</tr>
<tr>
<td>I.8.17.F. Databases</td>
</tr>
<tr>
<td>I.8.18.F. Spreadsheets</td>
</tr>
<tr>
<td>I.8.19.F. Images</td>
</tr>
<tr>
<td>I.8.20.F. File Processes</td>
</tr>
<tr>
<td>I.8.21.F. Number Systems</td>
</tr>
</tbody>
</table>

Table 16: Process 8 - Target Analysis (F. Fraudster)

### 4.5.2.3 Process 9, Threat Agent Analysis

This process analyses the threat agent, in other words, it is the contribution of findings of processes eight and nine. Without the knowledge gained from the Data Analysis and the Target Analysis, the examiner is not able to create an overall viewpoint about the Threat Agent.

The collection of information and analysis of the data provided concerning the fraudster is independent from the owner of the media (victim or fraudster). It is going to supply invaluable elements for his profiling and knowledge to the investigator.
The process consists of three activities:

**Intention (I.9.1.):** According to the information discovered the investigator should be able to put in the picture the intention of the fraudster. This is going to be based on the different forms of ID theft. For example, in the case where only identification data is stolen, then the intention of the threat agent appears to be identity ID theft. In some cases there may not be enough detail to prove this, but there should be indications in relation to the findings that support the fraudster’s intention.

Therefore, the instructions for this activity are:

Instruction 1. Financial  
Instruction 2. Identity

**Motivation (I.9.2.):** Vidalis and Jones (2004) present a threat agent list, where each different type of threat agent is motivated by his beliefs. In agreement with his motive, the threat agent penetrates the system. At this point, the function of the activity will give insight to the investigator.

This activity requests one instruction:

Instruction 1. Target

**Knowledge/ Skills (I.9.3.):** The findings of the investigation so far provide information about the skills of the attacker. The investigator gets an insight about the background knowledge of the fraudster, the group that the threat agent belongs (Jones and Ashenden D., 2005), conspiracy intentions or an innovative attacker.

The instructions of the Intention (I.9.1.) activity apply to the following, based on the different forms of ID theft (see section 2.2.3)

**Instruction 1. Financial:** The purpose of the ID thief is to gain access to financial information for financial gain.

**Instruction 2. Identity:** The purpose of the ID thief is to gain access to someone’s identification information or impersonate an individual for acquiring a new identity.

The instruction of the Motivation (I.9.2.) activity requires:
Instruction 1. Target: The objective of the attack’s motive needs to be identified. For example, whether the attack was motivated over an organised group or whether the target was a vulnerable system.

The following table reflects to the structure of the process:

<table>
<thead>
<tr>
<th>Process 9. Threat Agent Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Financial</td>
</tr>
<tr>
<td>2. Identity</td>
</tr>
</tbody>
</table>

Table 17: Process 9 - Threat Agent Analysis

4.5.3 Evidence

Evidence is the required outcome after the analysis. The investigator needs to begin structuring the collection of data that compose the evidence. Even though the analyst is not able to provide evidence, but indications of evidence, he should be able to determine it. Providing raw data does not justify the value of the findings. Therefore, the Evidence Analysis phase should present evidential data under such justification that can lead the investigator to the next phase (Scenario Construction).

In order to achieve this, the examiner is required to gather the results from ID Theft Data Analysis, and use them in order to assemble the evidential data and classify it. The investigator will be able to collect the data under a concrete and structured basis that is explained below.

For the manipulation of the output, two processes are constructed:

10. Evidence Collection

11. Evidence Classification
4.5.3.1 Process 10, Evidence Collection

It is the first process the investigator should proceed after the analysis, as he needs to collect the evidential data from ID Theft Data Analysis. By simply identifying the evidential data during the analysis, the examiner has only raw data concerning the ID theft incident that needs to be gathered and sorted. The activities of this process use the information gathered from processes seven, eight and nine. The purpose is merely to facilitate the evidence collection under a single process. Evidence Collection consists of the following activities:

Use evidential findings list O.8.1.V or O.8.1.F (I.10.1.): Use the lists of evidential data that resulted from the analysis of the target (Process 8), in order to continue to the next activity, where the evidence will be sorted based on the type of ID theft.

List of evidence based on ID Theft types (O.10.1.): The investigator is requested to categorise the evidential data identified according to the different forms of ID theft (see section 2.2.3 and I.9.1). These are created in two instructions. The categorisation is similar to Process 9< I.9.1, although examined from a content perspective that is explained in the Instructions part of this section:

Instruction 1. Financial
Instruction 2. Identity

Threat Agent Evidence list (O.10.2.): It uses information from the Threat Agent Analysis (Process 9). The investigator is requested to list the evidence that has been collected for the threat agent. The purpose is to gather information related with the threat agent.

The instructions of the List of evidence based on ID theft types (O.10.1.) require the following instructions and some objectives are also required for each instruction. The objectives that appear here classify information that is directly linked with their name. Consequently, no further clarification is provided. The evidential data is classified; however, there can be information overlap, as evidential data discovered do not necessarily belong only in one form of ID theft.

Instruction 1. Financial: This list is going to include all financial information gathered after the analysis of the digital media. The objectives that are included indicate the categories that financial data belong and are the following:
Objective 1.1. Credit histories
Objective 1.2. Transactions
Objective 1.3. Application names
Objective 1.4. Phone records
Objective 1.5. Tax records
Objective 1.6. Bankruptcy records
Objective 1.7. Documents on other people’s names
Objective 1.8. Dates of birth

Instruction 2. Identity: It concentrates on evidential data that deals with an individual’s identity and the following objectives categorise it:

Objective 2.1. Financial Evidence
Objective 2.2. National Insurance (N.I.) Numbers
Objective 2.3. Driving licence
Objective 2.4. Employment records
Objective 2.5. Passport records
Objective 2.6. Business records
Objective 2.7. Property records
Objective 2.8. Documents on other people’s names
Objective 2.9. Dates of birth
Objective 2.10. ID Card copies
Objective 2.11. Criminal records
The representation table of the process follows:

<table>
<thead>
<tr>
<th>Process 10. Evidence Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Financial</td>
</tr>
<tr>
<td>· Credit histories</td>
</tr>
<tr>
<td>· Transactions</td>
</tr>
<tr>
<td>· Application names</td>
</tr>
<tr>
<td>· Phone records</td>
</tr>
<tr>
<td>· Tax records</td>
</tr>
<tr>
<td>· Bankruptcy records</td>
</tr>
<tr>
<td>· Documents on other people’s names</td>
</tr>
<tr>
<td>· Dates of birth</td>
</tr>
<tr>
<td>2. Identity</td>
</tr>
<tr>
<td>· Financial Evidence</td>
</tr>
<tr>
<td>· N.I. Numbers</td>
</tr>
<tr>
<td>· Driving licence</td>
</tr>
<tr>
<td>· Employment records</td>
</tr>
<tr>
<td>· Passport records</td>
</tr>
<tr>
<td>· Business records</td>
</tr>
<tr>
<td>· Property records</td>
</tr>
<tr>
<td>· Documents on other people’s names</td>
</tr>
<tr>
<td>· Criminal records</td>
</tr>
</tbody>
</table>

Table 18: Process 10 - Evidence Collection

4.5.3.2 Process 11, Evidence Categorisation

When the evidence has been identified, collected and sorted the framework suggests it should be categorised according to their quality and value. Casey (2004) supports the categorisation of evidence in comparison with traditional forensics. The categorisation can strengthen the association of the findings with the fraudster, where greater importance is given to the most relevant evidential findings. The detailed ID theft investigation that the framework provides, allows the investigator to attempt a categorisation of the findings. Computer forensic investigations in practice show that the evidence identified is not always of the same strength in order to prove the alleged ID theft incident, especially when this needs to be provable in a court of law. Because of the subjective treat of evidential data, the skilled computer forensics investigator should be able to determine the quality of the evidence discovered.
It dictates the creation of the following activities:

**Use evidential findings list, O.8.1.V or O.8.1.F respectively (1.11.1.):** In order to satisfy the need of categorising the evidence, the analyst needs also to use the appropriate evidential findings list in this function.

**Create evidence classification list (O.11.1.):** Concerning ID theft investigations it is advantageous for the investigator to classify the evidence during his examination. In fact, this activity will produce three lists under its three instructions. These three instructions were chosen for the sorting of evidence, because they categorise the findings in three groups: the most relevant and crucial, the relevant, but not crucial and the not directly referring to the case. It is exactly the number of instructions that was considered appropriate for the ID theft framework. The reason this activity has been included is to assist the admissibility of the evidence. Findings considered as irrelevant will not be excluded from the final report to avoid issues from the defence. The investigator will include all evidence, while giving more emphasis to the strongly relevant to the case. For example, considering an examination where plenty of e-mail communication is involved; it may only be a small number of those found considered as directly linked with the case. Casey (2004) on the other hand, attempts a classification of the digital source.

The evidence is sorted based on the following:

- **Instruction 1. Strongly Evidential**
- **Instruction 2. Evidential**
- **Instruction 3. Irrelevant**

The above instructions require in detail:

**Instruction 1. Strongly Evidential:** This list is only going to include the findings that exemplify the premise and can present its validity without any doubts. In case the investigator considers no evidence as strongly evidential, then this list will remain blank. The same applies for the following two as well.

**Instruction 2. Evidential:** The evidential findings comprise this list. The piece of information revealed after the analysis of the media and is linked with the incident, but does not strongly support the ID theft incident. It is the pieces that
complete the puzzle, although they need to be corroborated with other evidential findings. This piece of evidence belongs to this list.

**Instruction 3. Irrelevant:** There could be some elements revealed at the completion of the ID Theft Data Analysis that seemed meaningful for the examination. However, after the completion of Evidence Collection (Process 10), this evidence is considered irrelevant with the investigation and is listed under this data file. Still, it should be mentioned in the documentation of the incident for later purposes.

The table that represents the process is:

<table>
<thead>
<tr>
<th>Process 11: Evidence Categorisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Strongly Evidential</td>
</tr>
<tr>
<td>2. Evidential</td>
</tr>
<tr>
<td>3. Irrelevant</td>
</tr>
</tbody>
</table>

Table 19: Process 11 - Evidence Categorisation
4.6 Phase 3, Scenario Construction

4.6.1 Phase 3 Overview

The third phase of the ID theft investigation framework aims to construct a scenario based on the evidential data that has been identified and collected so far. The investigator has completed the analysis of the media in Pea. However, the procedure of structuring the collected evidence in a scenario that attempts to describe the history of the incident, based on the findings is significant. At this stage, the investigator will be able to revisit the collected and categorised evidence from Phase 2 and classify the evidence and construct the scenario.

During this phase the examiner may need to return to any of the two previous phases, in order to search for additional evidential data. He is required to group the evidential data and create a scenario for the incident. Figure 19 below signifies the relationships among phases one, two and three (see Appendix F (IV) for the relationships in full page representation):
The phase maintains the following input and required output:

**Input:** Evidence Classification, the investigator is expected to use the information from Evidence (Phase 2<output>) and structure the evidential data, the threat agent’s profile according to the information collected, occurring the victim or the fraudster, and consequently structure the analysed digital evidence.

**Output:** Scenario, it is the reconstructed narrative, based on the evidence discovered. The investigator outlines the scenario and prepares the documentation that will be used on the last phase of the ID theft investigation framework.

Figure 20 outlines the structure of Psc.
4.6.2 Evidence Classification

The input of the phase accommodates the need of processing the evidential data gathered in phase two. Evidence will be used at this stage in order to assist the investigator identify the categories the evidential data belongs; group and appoint it accordingly. This procedure consists of three processes, where each one structures the evidence from different perspective and are analysed further in this section. The categorised evidential data of the Evidence classification will be then used in the construction of the Scenario, the output of the phase.

The processes that constitute the Evidence Classification:

12. Structure of Evidential Data
13. Structure Threat Agent’s Profile
14. Structure Analysed Digital Evidence

4.6.2.1 Process 12, Structure of Evidential Data

The purpose of the Structure of Evidential Data is to collect the evidence that has been discovered during the Media Analysis (Phase 2), structure and categorise it. The intention is to represent the evidential data in a manner that will correspond to the type of the content and the amount that it is linked with the case.

The activities that construct the process are:

Use evidence as of processes 10 and 11 (I.12.1.): The evidential data identified in Evidence (output, Phase 2), is studied and classified in Evidence Collection (Process 10) and Evidence Categorisation (Process 11). Therefore, I.12.1 aims to accumulate these findings in order to use them in the following activity.

Categorisation of evidential data (O.12.1.): The purpose of this categorisation is to arrange the collected evidence that resulted from I.12.1 based on their content. The categories that evidence falls into are described in instructions of the activity. However, there is no prerequisite that the discovered evidence will necessarily belong to a defined instruction. They are mainly for guidance towards the investigator. The Target Evidence List (O.10.2.) and the Evidence Classification List (O.11.1.) have already provided the detection of data
that indicate an ID theft incident. For this categorisation, the investigator should only use Instruction 1 and/ or Instruction 2 of O.11.1. Instruction 3 holds only irrelevant data that do not need to be included in this categorisation. O.12.1 activity is going to use these as collected in I.12.1 and group them to the following instructions:

Instruction 1. E-mail
Instruction 2. Internet Related
Instruction 3. Malware
Instruction 4. Hacked Databases
Instruction 5. Malicious Tools
Instruction 6. Documents
Instruction 7. Application Logs
Instruction 8. System Vulnerabilities
Instruction 9. Other

Their purpose is explained below. The related activities to the following instructions are borrowed from Target Analysis (Process 8) that shows their functionality and relationships in the framework. Activities O.10.2 and O.11.1 also used process eight to proceed.

Instruction 1. E-mail: All evidence concerning e-mails will be grouped under this instruction. It is the output of the evidence analysed in activities I.8.2.V, I.8.3.V or I.8.9.F, I.8.10.F.

Instruction 2. Internet Related: All the information that is related with the Internet activity is going to be grouped under this instruction. The depending activities from the Target Analysis are I.8.4.V, I.8.6.V or I.8.1.F, I.8.3.F, I.8.4.F, I.8.16.F.

Instruction 3. Malware: Any type of malicious activity that is identified in the system will be reported in this instruction, I.8.1.V or I.8.14.F, I.8.15.F.

Instruction 4. Hacked Databases: In case there was some evidence discovered concerning hacked databases or spreadsheets (because of the similarity of their content) in the digital media under investigation it should be listed under this instruction. It involves I.8.10.V, I.8.11.V or I.8.17.F, I.8.18.F.
Instruction 5. Malicious Tools: Traces indicating the use of hacking tools or installed hacking applications should be collected here. The dependent activities are I.8.1.V or I.8.4.F., I.8.5.F.

Instruction 6. Documents: All types of documents that can be used as supportive evidence belong to instruction 6, e.g. a document where the victim holds details about his financial status. The dependent activities are I.8.5.V or I.8.6.F, I.8.7.F, I.8.16.F.

Instruction 7. Application Logs: The evidential log files that have been identified after the analysis will be used in this instruction after the I.8.8.V, I.8.9.V or I.8.13.F activities.

Instruction 8. System Vulnerabilities: It aims to identify vulnerabilities identified to the system due to the security permissions set. The dependent instructions are I.8.7.V or I.8.8.F, I.8.9.F.

Instruction 9. Other: Other residual information that has been collected and can be used as evidence is categorised under this instruction. The dependent activities are I.8.12.V or I.8.2.F, I.8.11.F, I.8.15.F, I.8.21.F. The following table represents the process:

<table>
<thead>
<tr>
<th>Process 12. Structure of Evidential Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.12.1. Use evidence from Processes 10 and 11</td>
</tr>
<tr>
<td>1. E-mail</td>
</tr>
<tr>
<td>2. Internet Related</td>
</tr>
<tr>
<td>4. Hacked Databases</td>
</tr>
<tr>
<td>6. Documents</td>
</tr>
<tr>
<td>7. Application Logs</td>
</tr>
<tr>
<td>9. Other</td>
</tr>
</tbody>
</table>

Table 20: Process 12 - Structure of evidential data
4.6.2.2 Process 13, Structure Threat Agent’s Profile

The Threat Agent’s Profile aims to collect the evidence identified during the Threat Agent Analysis (Process 9) and listed in O.10.3. (Threat Agent Evidence list). As in Structure of Evidential Data (Process 12), the investigator is expected to structure the data that concern the threat agent and maintains in an unprocessed form after the Pea (Phase 2). Marcella and Greenfield (2002), highlight the importance of profiling the fraudster.

The key issue for this process is to determine the findings based on the victim’s and the fraudster’s side. The profiling that will be drawn is going to be under a different perspective depending on the vector. The activities of the process are the following in respect to Vidalis and Jones (2005) as their work fits the needs of the framework.

Use threat agent evidence list O.10.3. (I.13.1.): Use the list that was created in O.10.3 (Process 10) in order to aid the profiling of the threat agent.

The output activities for the Victim (V) are:

Reveal technical skills (O.13.1.V): The information discovered after the analysis of the victim’s side is obviously going to reveal clues concerning the technical skills of the fraudster. Brute force attacks and IP Spoofing are good examples for low and high technical level accordingly for the threat agent’s skills. In addition, the security measures considered by the owner of the system can reveal the required by the threat agent technical skills to manage the attack.

Reveal programming skills (O.13.2.V): It is the abilities of the threat agent based on the method of the attack. The evidential data identified can show whether the intruder has programming skills, e.g. use of personal written scripts or an opportunist by using already written code.

Ability to convince someone (O.13.3.V): The fraudster’s social engineering skills that are possibly identified after the media analysis. A phishing attack for example, could show that the threat agent has programming skills to develop the phishing and social engineering skills to conceal the fraud and convince the victim.
Ability to keep stealth action (O.13.4.V): The complexity of the attack is going to show the ability of the attacker to keep activities stealthy. The vulnerabilities of the system and the technical skills of the fraudster combined could possibly leave minimum traces for the investigator to identify further information about his actions.

The activities for the Fraudster (F.) are:

Sophistication of tools (O.13.1.F): The collection of tools – programming, hacking, and security - identified in the fraudster’s side can provide insight about his actions. Such tools can show the complexity of his capabilities.

Level of expertise (O.13.2.F): It is depended to the previous activity, as the sophistication of the tools that are installed and probably also used by the attacker are able to define his level of expertise. The more advanced and complex the tools, the more experienced and advanced the threat agent.

Use of defensive techniques (O.13.3.F): There is no sophisticated intruder acting without considering the use of defensive techniques. These techniques would let him act unattended. For example, someone may accomplish a man-in-the-middle attack and introduce a third party involvement to the investigation.

Identify purpose of attacking (O.13.4.F): It is whether the method of the attack reveals that the fraudster acts based on his ego or his curiosity. The investigator should be able to draw a picture regarding the purpose of the attack.

Identify motivation (O.13.5.F): Jones (2002) refers to the components of the threat agent’s motivation. According to this categorization, an ID thief has personal gain as a motive. However, the evidential data can disclose more than just this. Information that concerns a limited number of attacked systems for example indicates that the threat agent works in a focused target group.

Identify opportunities (O.13.6.F): This activity is a combination of O.13.1.V and O.13.4.V, in interdependence with his level of expertise O.13.2.F and motivation O.13.5.F. The opportunities of attacking a system differ according to the motive, the flexibility and the background of the fraudster, as well as with his capabilities. However, an attack to an unsecure system provides different aspect to his profiling than an attack to a protected, secure, or even business system.
The table below corresponds to the Structure Threat Agent’s Profile process:

<table>
<thead>
<tr>
<th>Process 13. Structure Threat Agent’s Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>V. Victim</td>
</tr>
<tr>
<td>I.13.1. Use Threat Agent Evidence list</td>
</tr>
<tr>
<td>O.13.1.V. Ability to convince someone</td>
</tr>
<tr>
<td>O.13.3.V. Ability to keep stealth action</td>
</tr>
<tr>
<td>O.13.1.F. Sophistication of tools</td>
</tr>
<tr>
<td>O.13.3.F. Use of defensive techniques</td>
</tr>
<tr>
<td>O.13.4.F. Identify motivation</td>
</tr>
</tbody>
</table>

4.6.2.3 Process 14, Structure Analysed Digital Evidence

This process aspires to collect the evidential data that have been categorised in the previous two processes (12 and 13). The investigator needs then to create a structured set of findings that will include the key aspects of the overall analysis. The purpose is to identify the amount of information that can be retrieved from evidence that involves a specific individual.

The activities that constitute this process are:

**Structure all sort of valuable information** (I.14.1.): This activity includes valuable evidential data for the outcome of the investigation, independent from its source. In other words, the investigator collects the outputs of the previous activities and works with these in order to continue to the next activity. The purpose is to list the piece of information that kept the attention of the examiner during the analysis of the digital media. E.g., picture files from scanned or forged passports that have been used for impersonation are imported from O.12.1. (Categorisation of evidential data).

**Identify evidential aspects** (I.14.2.): At this function, the investigator needs to identify the evidential aspects of the structured information from the previous activity in order to give emphasis. For instance, if the examiner has identified in I.14.1 image files as evidential to the case, then he needs to declare the element that makes these images valuable for the outcome of the investigation. There could be more information discovered concerning the life of the person, whose passport has been scanned and saved as an electronic file. Therefore, the
investigator should conclude to a list, where all these similar evidential aspects are added. For example, if a national insurance number, a driving license copy and financial records all found to concern the same person; they should be listed under this activity.

**Group the evidential aspects (O.14.1.):** This is the activity that the evidential aspects identified above will be categorised in a way that the investigator can create a structured approach of the evidential aspects. Following the example of I.14.1 and I.14.2, the investigator needs to group all four evidential files that refer to an individual.

E.g. Victim = passport image, national insurance number, driving license copy, financial records

The following table represents the Structure Analysed Digital Evidence process:

|-----------------------------------------------|

Table 22: Process 14 - Structure analysed digital evidence

### 4.6.3 Scenario

As mentioned on chapter three, the purpose of reconstructing a story is valuable for the investigator as he can present a coherent and efficient chronicle of the evidence he identified so far. The scenario is the ‘prediction’ (Carrier, 2006), based on which the findings will be evaluated on the next phase. The examiner has the choice to return to any process in the previous phases during this output. Scenario structures the evidential data from the whole procedure so far.

This output will be used as an input to the next and final phase of the ID theft investigation framework, where the validation of the procedure is targeted.

There are two processes for the Scenario:

15. Scenario Outline Activity

16. Scenario Preparation Documentation Activity
4.6.3.1 Process 15, Scenario Outline

The Scenario Outline aims to create the scenario plan. This process uses information from the Evidence Classification (Phase 3 input). Furthermore, it uses sources from a number of processes met so far, such as the offline data from activity I.1.1< Instruction 2.

The activities of the process are:

**Use evidence as of I.1.1.< Instruction 2, Phase 1 Output, Phase 2 Output, and Phase 3 Input (I.15.1.):** The investigator needs to use all offline evidential data discovered in Phase 1, activity I.1.1., offline data (Instruction 2). The results from the ID Theft Data Identification (Phase 1, output), Evidence (Phase 2, output) and Evidence Classification (Phase 3, input) are going to be of equal importance for this process. The purpose of the investigator is to collect the outcomes and use them on the next activity.

**List valuable data gathered (O.15.1.):** This activity lists the valuable data that was gathered during I.15.1. The outcome of this list will produce an outline of groups, according to the type of the evidence. For example, all offline data identified in Phase 1 will be filed together; all evidential data concerning a certain person will be also filed together.

The representation table of the process follows:

<table>
<thead>
<tr>
<th>Process 15. Scenario Outline</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.15.1. Use evidence as of I.1.1.&lt; Instruction 2, Phase 1 Output, Phase 2 Output, and Phase 3 Input</td>
</tr>
</tbody>
</table>

Table 23: Process 15. - Scenario Outline

4.6.3.2 Process 16, Scenario Preparation Documentation

The Scenario Preparation Documentation aims to employ the findings of the analysis of the digital media and prepare the scenario that will attempt to reconstruct the history of the incident. There is no actual written documentation of this scenario as there is no need for the investigator to pursue such practise; it is only the merging of the evidential data. The case documentation will be constructed in the Phase 4.
The data collected in process 15 will be now used and gathered before the evaluation of the case. The scenario will be evaluated in the next phase, where similar results to process 16 should occur. The process consists of the following two activities:

**Use Scenario outline list from O.15.1. (I.16.1.)**: The list created in O.15.1. (List Valuable Data Gathered), is going to be used at this stage in order to help the investigator continue to the following activity.

**Merge evidential data gathered (O.16.1.)**: The overall collection and merging of the evidential data aims to create the actual documentation and case preparation. The examiner brings in the front the evidential elements gathered and ensued by the classification. Therefore, he is prepared to continue with the evaluation of the findings.

The following table represents process 16:

<table>
<thead>
<tr>
<th>Process 16. Scenario Preparation Documentation</th>
</tr>
</thead>
</table>

Table 24: Process 16 - Scenario Preparation Documentation
4.7 Phase 4, Evaluation

4.7.1 Phase 4 Overview

The only premise for the last Phase of the investigation framework is that the examiner has already completed the previous three phases. The phases are interconnected and allow revisiting the previous phases for further examination. The Evaluation phase endorses this re-examination of any of the previous three phases for evaluating purposes. The method supports the functionality and flexibility of the phase. The cohesion of the discovered evidential data will be verified during the evaluation. Same as in previous phases the following diagram is an overview of the relationships among the phases and can be found in a readable version on Appendix F (IV).

![Figure 21: Relationships among phases 1, 2, 3, 4](image)

The investigator is required to evaluate the whole examination and present the case by testing the Scenario. Phase 3 produced a Scenario in an attempt to construct the history of the incident, based on the digital evidence. The forensic examiner ought to appraise these results in Phase 4 and convert them to an
admissible report. The Evaluation phase requires the following input and output respectively:

**Input:** Scenario Examination, the investigator needs to test the scenario that has been drawn after the Scenario Construction (Phase 3) and clarify it, according to the evidential data discovered.

**Output:** Case, the examiner makes use of the Scenario Examination in order to construct a case. This case needs then to be clarified, evaluated and documented for the representation purposes.

The following figure represents the phase:

<table>
<thead>
<tr>
<th>Process 17. Scenario Testing/Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.17.1. Use the outputs of Phases 1, 2 and 3</td>
</tr>
<tr>
<td>I.17.2. Check validation/ entirety of the outputs</td>
</tr>
<tr>
<td>O.17.1. Create evaluation list</td>
</tr>
<tr>
<td>Process 18. Scenario Clarification</td>
</tr>
<tr>
<td>I.18.1. Use evaluation list from O.17.1.</td>
</tr>
<tr>
<td>I.18.2. Clarify the impact of evidential data</td>
</tr>
<tr>
<td>O.18.1. Create scenario clarification list</td>
</tr>
</tbody>
</table>

**Figure 22: Phase 4 - Evaluation**

### 4.7.2 Scenario Examination

The investigator is required to use as an input the Scenario output of phase three. The purpose is to validate the outcome of the evidential data that resulted in the previous phases. On phase one the media that can provide indicative evidence is analysed, on phase two the resulting evidence, while on phase three the evidence is collected and the creation of a scenario is attempted. For the sequence and coherence of the procedure, the investigator uses the above in order to ensure the validity of the scenario.
This will be accomplished in the following two processes:

17. Scenario Testing / Evaluation

18. Scenario Clarification

4.7.2.1 Process 17, Scenario Testing/ Evaluation

The importance of this process lies beneath the need for appraisal. Martinez (2005) emphasizes the needs for evaluation. A rephrase of his statement in terms of the specific procedure stresses that it is essential for effectively carrying out planned activities, and the extent to which it is achieving its stated objectives and anticipated results.

Therefore, the undertaken method needs to be effectively verified according to the results that have been developed. In such an approach, the investigator is going to be able to ensure the validity of the examination. The activities that compose the process are:

Use the outputs of Phases 1, 2 and 3 (I.17.1.): The investigator needs to make use of the outputs of the previous phases in order to revise his outcomes as gathered in the Scenario Preparation Documentation (Process 16). The investigator may decide the use of a virtual machine (Carrier, 2006) for rebuilding the events that appraise the initial premise of the ID theft incident.

Check validation / entirety of the outputs (I.17.2.): The revision of the outcomes send the investigator to this activity, where he is required to check the validation and the entirety of the outputs. It is important to certify that the procedure has been accomplished under a concrete, structured basis.

Create evaluation list (O.17.1.): The evaluation list aims to include the crucial data that have been identified after the evaluation. In case any amendments to the previous processes took place, these have to be listed in this function.

The representation table of the process is:

<table>
<thead>
<tr>
<th>I.17.1. Use the outputs of Phases 1, 2 and 3</th>
<th>I.17.2. Check validation / entirety of the outputs</th>
<th>O.17.1. Create evaluation list</th>
</tr>
</thead>
</table>

Table 25: Process 17 - Scenario Testing / Evaluation
4.7.2.2 Process 18, Scenario Clarification

The purpose of this process is to allow the confirmation of the scenario. To ensure that it is directly supported by the results of the Scenario Testing/Evaluation (Process 17). The activities that constitute the process are:

**Use evaluation list from O.17.1. (I.18.1.):** For this activity the examiner needs to use as an input the output of the previous process (O.17.1.). An evaluation list has been created and it now needs to be used in order to proceed to the clarification of the evidence.

**Clarify the impact of evidential data (I.18.2.):** The investigator needs to explain the effect of the evidential data in relation to the incident. As long as the investigation has been completed and the evidential data has been assessed, their implication needs to be stated.

**Create scenario clarification list (O.18.1.):** Create a list that includes the impact of clarified data as identified on I.18.2. This list will be used on the last process.

The representation table of the process is the following:

<table>
<thead>
<tr>
<th>Process 18. Scenario Clarification</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.18.1. Use evaluation list from O.17.1.</td>
</tr>
</tbody>
</table>

Table 26: Process 18 - Scenario Clarification
4.7.3 Case

The Scenario evaluated the findings of the analysis and defined a situation based on which the actual case is going to be constructed. The purpose of this process is to verify the vulnerable digital evidence has been treated sensibly and interpreted in a case report that reflects the ID theft incident and the findings. The handling of accurate, constructed evidence results to a precise representation of the case in the court. Therefore, the case will need to fulfil the following processes after the evaluation of the Scenario (Phase 4, input):

19. Case Construction
20. Case Clarification
21. Case Evaluation
22. Evidential Case Representation

4.7.3.1 Process 19, Case Construction

The Case Construction aims to build the foundation of the case representation, as this is essential for the admissible digital evidence handling. The examiner needs to use the output of Process 18, in order to define the necessary evidential data for the constructed case and convert the scenario to a filed case.

Consecutively, two activities are required:

Use data from scenario clarification list O.18.1. (I.19.1.): The examiner is requested to use activity O.18.1 (Process 18) as the input of this activity. Then, he can continue to the next activity.

Construct the case (O.19.1.): It aims to the actual construction of the case. In other words, it is the initial attempt of the actual documentation of the case, after the testing of the scenario (Process17).

The following table reflects the process:

<table>
<thead>
<tr>
<th>Process 19. Case Construction</th>
</tr>
</thead>
</table>

Table 27: Process 19 - Case Construction
4.7.3.2  Process 20, Case Clarification

Even though the case has been constructed, the examiner needs to link the representation of the evidence with the impact of the case in order to confirm the evidential findings. For those cases that an expert witness is required to testify in court, the legal aspects of the evidence should be included as well. These will be used in the next process that the case will be evaluated. The purpose of process 20 is accomplished in a single activity.

Clarify the constructed case from O.18.1. (I.20.1.): The clarification of the constructed case aims to the justification of the evidential data related with the initial premise. The investigator ought to clarify the reasons that the related digital evidence is considered as connected to the specific examination and attach them to the case. In addition, the source of the evidence, as well as its handling must be clarified. (Casey, 2007)

The representation table of the process:

<table>
<thead>
<tr>
<th>Process 20. Case Clarification</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.20.1. Clarify the constructed case</td>
</tr>
</tbody>
</table>

Table 28: Process 20 - Case Clarification

4.7.3.3  Process 21, Case Evaluation

The Case Evaluation aims to test the outcome of the constructed case. Before the examiner proceeds to the final construction of the case report, he needs to ensure the validity of the constructed case, based on the fourth phase (Report or statement) of the ACPO (2007) guidelines’ Recovery Process.

This process is considered as a final review of the supported digital evidence. Three activities are going to carry this out:

Use the scenario evaluation list from O.17.1. (I.21.1.): Return to the Scenario Evaluation List (O.7.1.) in order to ensure that all evidential aspects are included in the case.

Check validation (I.21.2.): As in I.17.2. (Check Validation/ Entirety of the outputs) the investigator needs to ensure the structured layout of the case, according to the scenario evaluation list that was used on I.21.1.
Confirm case evaluation (O.21.1.): When the validity of the case has been certified, the investigator needs to confirm the official outcome of the case.

The table that pictures the activity:

|-----------------------------|

Table 29: Process 21 - Case Evaluation

4.7.3.4 Process 22, Evidential Case Representation

The evidential case representation depicts the case in the terms of creating a testimonial report that can be presented in a court of law. The examiner is going to create a formal document that includes the outcome of his work. The process consists of the following two activities.

Create the testimonial report (I.22.1.): The purpose is to represent the evidence in a structured way that could be comprehended from non-computer specialists. Kennedy (2006) mentions that the examiner needs to take under consideration the defence of the case and create his plan for defeating it. The structured form of the ID theft framework assists in this by the collection and categorisation of the evidence that has been already produced on phase 2 (Processes 10 and 11) and classification of the evidence on phase 3 (Processes 13, 14 and 15).

The investigator needs to present all the findings of the examination in a manner that indicates the evidence from the technical, scientific point of view. In addition, it should be interpreted in a way to be read and comprehended by a jury. When the case needs to be presented in a court of law, then the findings should be interpreted in an appropriate way that support the offence, based on the ACPO (2007) principles. Solon and Harper (2004) provide comprehensive guidelines of
how the evidence should be presented in the court and strengthen the importance of a structured, well-written report.

The activity needs the following instructions in order to achieve the above:

Instruction 1. Include all case evidence
Instruction 2. Describe all case evidence

ID Theft case investigation report (O.22.1.): All evidence that has been identified and evaluated so far contribute to the final product of the investigation, the ID theft case investigation report.

The instructions that appear on activity I.22.1 have the following purpose:

Instruction 1. Include all case evidence: The investigator includes all evidence that has been already included and evaluated in Case Evaluation (Process 21) and by using this continues to the next instruction.

Instruction 2. Describe all case evidence: The examiner is requested to describe all the evidential data in a report that describes the procedure he has followed, the findings and his conclusions.

The table below represents the process:

<table>
<thead>
<tr>
<th>Process 22. Evidential Case Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.22.1. Create the testimonial report</td>
</tr>
<tr>
<td>1. Include all case evidence</td>
</tr>
</tbody>
</table>

Table 30: Process 22 - Evidential Case Representation
Summary

A detailed approach to the findings of the investigation process based on the evidence left behind on a victim’s and fraudster’s digital storage media respectively was presented in this chapter. The importance of this reflects to the fact that the forensic investigator needs to be provided with a thorough and comprehensive approach that explicates this research work. The analysis of the ID theft investigation framework presented all the aspects and the instances that construct it. The framework consists of four phases; every phase consists of a varying number of processes, necessary to satisfy the input and the output that define the phase. Every process holds a number of activities, while some activities require some instructions and objectives in order to specify their purpose.

The low level analysis of the framework was presented with the following structure:

- Overview of every phase;
- Representation figure of the phase;
- Description and purpose of the inputs and outputs;
- Effect and operational aspect of every process;
- Purpose and functionality of every activity;
- Details on the application of instructions and objectives;
- Representation table of every process.

The actual aim throughout the development of the ID theft framework has been the satisfaction of the hypothesis statement of this research, to facilitate the investigation of computer-based ID theft and the handling of the related evidence. The investigator is required to identify and analyse the digital media that constituted to the crime. The analysis of the evidence aims to assist him identify the evidential data able to construct a scenario concerning the story behind the incident. The evaluation of the scenario is going to clarify the case and represent it. Throughout this procedure, information that concerns the target of the crime (victim) and the threat agent (fraudster) is gathered. The purpose is not only to
profile them both and collect material that enlightens the incident’s conditions, but also to defeat the defence.

The following two chapters of this thesis will plan and execute respectively the application of the investigation framework in practice in order to prove its validity and reveal the achievement of the hypothesis.
In this chapter the reader can
- find the need for evaluation;
- find the evaluating techniques that pursue this research;
- find the definition of the laboratory experiment.

Overview

There are a number of approaches in literature for evaluating research work, suggested methods are: content analysis, accountability, decision oriented, objectives based, testing programs, experimental research, and adversary. The evaluation approach answers to what works, for whom, in what circumstances, and why (Pawson and Tilley, 1997). In dealing with the challenge of an appropriate assessment for this project, two avenues of evaluation have been selected; they were considered to satisfy the needs of this work based on the background reading of evaluation methods.

1. Based on the research methodology followed throughout this research, a case study in terms of a lab experiment has been selected. It appeared as the most appropriate method for evaluating the theory and defending the research outcome of this research. The purpose is to manage the validation of the research outcome via a laboratory experiment, in an attempt to prove or disprove the hypothesis.

2. The support of members of the Hi-tech Crime Unit, Gwent Police Headquarters, enabled an external assessment. A qualitative study interview was conducted (Appendix J) after the end of the framework’s implementation, applying the investigators’ experience on ID theft incidents to the investigation framework. The police detectives also agreed to apply the ID theft framework stages to an existing investigation to provide a valuable practical assessment.
Therefore, this thesis makes use of the following evaluation methods and based on:

a. The laboratory experiment

b. The assessment and the interview of Gwent Police

5.1 Evaluation Objectives

There are a number of different approaches to evaluation, based on the nature of the research. The objective is to prove that a piece of work and the assumptions are valid and applicable to the real world.

Because literature provides endless theoretical material serving the purpose of evaluation some definitions have been selected to stress and clarify the importance of evaluation.

An elastic word that stretches to cover judgements of many kinds (Weiss, 1972)

An evaluation examines a programme from a number of different perspectives and looks for causal linkages between programme activities and outcomes. Programme evaluation is a theory-focused activity that also considers the relevance of the various components of a programme and makes predictions about future developments. (Clarke, 1999)

The systematic collection of information about the activities, characteristics and outcomes of programmes to make judgements about the programme, improve programme effectiveness and/or inform decisions about future programming (Patton, 1997)

In general terms, the evaluation procedure proves or disproves the initial project hypothesis. Therefore any weaknesses of the project results can be identified. In such a case this can provide assistance for any future modifications and improvements on the plan. Furthermore, confirm the fulfilled project objectives. (Hutton, 2001)
5.1.1 Chosen evaluation methods

5.1.1.1 Evaluation Experiment

This research was focussed on examining the hypothesis: to create an analytical framework to facilitate the investigation of computer-based ID Theft and the handling of the related digital evidence. The aim of the experiment is to test this hypothesis (Leedy and Ormrod, 2005). There should be no alternative hypothesis to the research derived from the experiment outcome (Barnes et al., 2005).

The case study approach appears to be the most appropriate for this research, as already described on chapter one (also see Leedy and Ormrod, 2005). The case study scenario will be based on data extracted from forensic case work and will therefore be built upon real life examples. Then, the laboratory experiment will be based on the scenario and the ID theft investigation framework will be applied for the analysis. Meister and Rabideu (1965), include laboratory experiments in ‘observational methods of data collection.

5.1.1.2 Police Review

The evaluation of the Hi-tech Crime Unit investigators will also be used to determine the framework applicability in an investigative environment. A number of interviews with members of the Gwent police took place during the design and implementation of the framework (see section 4.2). In these meetings the investigators assisted by adding knowledge and expertise from their practical experience. Once the framework was constructed the investigators contributed to the assessment by applying it on a suitable case. The intention was to determine if the framework contributed to the investigation. The feedback at this stage was in the form of a questionnaire.
5.2 Evaluation Experiment

5.2.1 Aim of the evaluation

The laboratory experiment for assessing the framework was based on the review of a number of existing ID theft cases. These cases suggested that a common method of personal identity data being harvested from a PC was by the use of malicious software\(^1\). In these cases the victim’s computer system is infected with malicious code, which records personal identity data and makes it available to the fraudster. To test the presented framework two systems were required which contained evidence that leads to ID theft. One system will represent the victim and the other the fraudster. The following test protocol was used:

1. A closed network with two computers was created
2. Computer A is the ‘fraudster’, Computer B is the ‘victim’.
3. Both computers were populated with background data.\(^2\)
4. A fellow researcher acts as the fraudster to the ‘victim’ machine.\(^3\)
5. He attacks the machine and plants the malware.
6. This malware tracks personal details.\(^4\)
7. The system is infected.\(^5\)
8. Both computers are examined by using the framework.
9. The examination starts from the ‘victim’ machine\(^6\)

\(^1\) See chapter 2: Malicious software and keyloggers
\(^2\) The data that populate the disks are suitable to the purpose of each computer machine.
\(^3\) The initial plan was that the researcher would act as the fraudster; however the idea of using an independent third party for the execution of the malicious code approaches the realistic side of the event.
\(^4\) The researcher is not aware of the type malware planted by his ‘assistant-attacker’ to the victim’s machine.
\(^5\) The type and extent of the infection is unknown.
\(^6\) As this is considered to be discovered first, according to the scenario that follows in this chapter.
The computer systems that were used for the experiment have the following description:

<table>
<thead>
<tr>
<th></th>
<th>Fraudster</th>
<th>Victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Pentium III 800Mhz</td>
<td>Pentium III 800Mhz</td>
</tr>
<tr>
<td>Memory</td>
<td>256 MB</td>
<td>256 MB</td>
</tr>
<tr>
<td>Hard disk</td>
<td>Fujitsu 20GB</td>
<td>Fujitsu 20GB</td>
</tr>
<tr>
<td>Optical devices</td>
<td>Samsung CD-ROM</td>
<td>Samsung CD-ROM</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows XP S.P. 2</td>
<td>Windows XP S.P. 2</td>
</tr>
</tbody>
</table>

Table 31: Systems’ Specifications

5.2.2 Sources of data for the scenario

The scenario written for the experiment is supported and based on real incidents; despite the fact that there is limited detailed information available concerning the exact methods used to perpetrate an ID theft. However, news articles and journals provide an invaluable assistance. Amongst the inexhaustible sources of real life ID theft incidents, the following are a minor overview of these sources:

- ‘ID theft is inescapable’ (Greene, 2005),
- ‘ID theft ring escapes shutdown’ (Anon, 2005a),
- ‘I was a victim of ID theft’ (Anon, 2005b),
- ‘UK police arrest copycat phisher’ (Leyden, 2004),
- ‘Arrest’ (Wolfe, 2007),
- ‘How cyber-crime became a multi-billion-pound industry’ (Lush, 2007)
- ‘Identity impairment: The problems facing victims of identity fraud’ (Furnell, 2007)
- ‘Identity theft: No help for consumers’ (Matejkovic and Lahey, 2001)
- ‘Cybercrimes Of The 21st Century’ (Riem, 2001)

The news stories may contain a degree of journalistic licence (Greene (2005), Anon (2005a), Anon (2005b), Leyden (2004), Wolfe (2007), Lush (2007)). However, there is a large collection of victims’ stories and cases found on the Privacy Rights Clearinghouse web site (2007), the Better Business Bureau (BBB online, 2003) and the Get Safe Online web site (2009). The fictional scenario has been constructed using commonly occurring elements found in the above cases.
A common scenario is the ID theft victim reports a suspected crime. The data loss is the result of a malware infection on a vulnerable computer system. The ID theft framework has been applied to this case in the following way:

a. Examine the victim’s machine in a forensic manner to determine a malware infection.

b. Identify and examine the timeline and behaviour (data possibly extracted) of the malware.

The results of the investigation should lead the examiner to:

a. the collection of evidential data concerning the fraudster.

b. identify the way the fraudster attacked the victim’s machine.

There are three stages that need to be fulfilled during the experiment:

1. the network attack from the ‘fraudster’ to the ‘victim’ machine;

2. the forensic analysis based on the investigation framework from the ‘victim’s’ side;

3. the analysis of the ‘fraudster’s’ machine that the researcher will be expectantly led to this by the evidence discovered to the victim’s disk.

However, it should be acknowledged that the victim’s machine may frequently guide the investigator to a compromised third party connection. The term third party in this context refers to the use of an intermediate computer by the fraudster.

In a case where the forensic analysis drives the researcher in such a perspective, then the intermediate machine should be examined under the same terms with a fraudster’s machine. This is because that machine was used to perpetrate and affect with fraudulent activity. However, such an approach could be mostly applied in theory. Access on a third party system usually cannot be granted, and in a number of occasions multiple intermediate systems could interfere. The use of zombie machines involved in attacks has influenced and raised questions on how they should be treated legislatively (Rasdale, 2006). In a case where third party machines were involved to the attack, these would probably be identified during the analysis of the digital media.
Nevertheless, the specified experiment involves a one-to-one attack due to the limitations of the laboratory experiment. It is considered as a reasonable representation of a real life targeted attack. They may involve personal information extracted by social engineering or even from social networking web sites (see section 2.2.2.1). Dunne (2008) gives a detailed example of how he managed to gather personal information for a targeted attack against an individual.

Figure 24 represents the layout of the introduced experiment:

![Graphical Representation of the research experiment and its parts](image)

### 5.2.2.1 Evaluation Scenario

This part of the evaluation procedure is based on a single case study and will be verified under its experimental form called as single subject design, borrowing the term from quasi-experimental research design (Dereshiwsky, 1998). The idea is based on real incidents and cases that have been found published during this research (see section 5.2.2). Among these contributed the experiences of Nasir Ahmed in Anon (2005b), the Nevada, Texas and Pensylvania consumers from BBB Online (2003), James from Furnell (2007), Lamar Christian from Matejkovic and Lahey (2001). Also, added the story 'It was full of spyware’ on Get Safe Online (2009) and the story of Levine on Riem (2001). However, there is the need to underline that the following story is not a representation of a real incident.
The Background

The potential victim uses the internet from his home computer extensively. He uses the following services: web banking services, online shopping and communicates via instant messaging and e-mails.

Stages

Day 1

The victim routinely checks his online banking site and notes a potentially large charge on his credit card. The victim contacts his credit card company who agrees to investigate his case.

Day 2

A number of weeks later the victim receives a letter from a financial organisation stating an outstanding balance of a number of thousand pounds on a recently acquired loan. The victim corresponds with the loan company and determines the fraudulent activity. The application had been made online and in his name.

The man asked for further details concerning the payment method and the bank account that the loan was issued on. He tended to use one particular bank account for all his payments.

Day 3

A few days later there was another incident. He received a new letter from another loan company acknowledging his successful application. The man was now fully convinced that this series of events was more than just a coincidence.

He decided to contact the police as the situation seemed fraudulent. The man had never considered ID theft as a threat before. He was motivated to collect all his evidence and visit the nearest police department. Furthermore, he thought he should request more details about the transaction from the loan and the credit card companies.
Day 4

On his visit to the police station an officer kept record of his story, asked him a number of questions about his life, personal and social, and how concerned he was about computer security. The man didn’t even use antivirus software. ID theft is an assumption and his residence is not a crime scene. The police officers suggested they should investigate his personal computer as that is the machine he uses extensively for personal use and stores his personal records. Therefore, the man returned home, shut down his computer and carried it to the forensics department at the police station.

Day 5

At this stage it is not essential to retrieve any other background information about the negotiation between the man, the police officers and their questions. The fact of interest is the forensic investigation of his computer system. This computer forensics investigation should now take us to the stage that the ID theft incident will be proved or disproved. The purpose is to ensure appropriate application and functionality of the framework. Therefore, the above scenario should validate the previously described investigation framework and meet the requirements for its purpose.

Figure 25: Scenario Representation
5.2.3 Evaluation Experiment Decisions

The major concern of the actual experiment is to approach the above scenario to the most possible realistic perspective. The experimental assessment of the framework requires an actual computer infrastructure. This required some decisions to be taken as to the systems specification in terms of both hardware and software. The following issues were addressed:

1. **Hard drive capacity:** This had little impact on the scenario as a whole, however for a speedy imaging and analysis a limited capacity drive was selected.

2. **Bandwidth and processing power:** These do not influence the experiment.

3. **Pre-existing data on the drive:** The decision was not to remove pre-existing data on the drive as this would, for the investigative stage, simulate what an investigator would expect to find on a hard drive. Providing a degree of background information from which the evidence would need to be extracted.

The following paragraphs aim to resolve all different decisions that were taken concerning issues about the laboratory experiment. The decisions are the result of the background study (see chapter 2).

One of the issues that needed to be resolved was which operating system would be ideal to install on the victim’s, fraudster’s and investigators hard drive. There are a number of operating systems available (Linux, Mac OS X, Microsoft Windows, Solaris); based on Johnston et al. (2003) it was decided that Windows XP was the operating system most commonly in use in the home environment. It may be argued that Windows Vista or 7 are replacing this to a degree but at the point of inception XP was the most popular O.S. and so remains the platform of choice for this project.

Then, there should be decided which applications should be installed on the system. It is essential, based on the scenario, to show the Internet interactivity from the victim’s side. The selected applications were chosen according to their popularity and the researcher’s personal experience of exploiting them. The user should have installed the following applications (see table 32) in order to justify the use of the computer system as an entertainment system:
Concerning the fraudster’s hard disk, the following applications will be installed for the same reasons as described above:

<table>
<thead>
<tr>
<th>Fraudster’s applications</th>
<th>e-mail accounts</th>
<th>Password cracking and hacking tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Microsoft Office XP</td>
<td>g. <a href="http://www.gmail.com">www.gmail.com</a></td>
<td>h. Brutus A2</td>
</tr>
<tr>
<td>b. MSN Live v.8</td>
<td></td>
<td>i. Cain and Abel</td>
</tr>
<tr>
<td>c. uTorrent</td>
<td></td>
<td>j. John the Ripper</td>
</tr>
<tr>
<td>d. Adobe Acrobat Reader 8.0</td>
<td></td>
<td>k. Back Orifice</td>
</tr>
<tr>
<td>e. Adobe Flash Player 9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. Mozilla Firefox 2.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The above applications were practically used during the experiment in order to populate the hard disk’s contents. Any additional software or tools installed on the fraudster’s machine are not of the preference of the author, but a fellow researcher specializing in network security who volunteered to assist the attack. This way, the author was not aware of the actual object of the investigation (the Trojan), which approaches a real life investigation.

Another issue was whether to install any security products (antivirus, antispyware, or firewall) on the machine. It has been suggested in earlier chapters that one avenue exploited by ID theft fraudsters is the lack of appropriate security at the end user’s computer. This vulnerability enables the system to be infected with malware capable of capturing personal information. For the purpose of the experiment and based on the review in chapter 2 no antivirus was installed on the system.

A major concern was the network and Internet connectivity of the computers. During the lifetime of the research and the data population the two computer machines were connected on a local network through a network switch in order to
achieve the closed network access control scheme. The attack takes place over the closed, secure network as presented in Figure 24 above.

The Internet connection seems to be the strongest constraint for fulfilling the experiment. It is unlikely to have Internet access on a controlled environment, execute malicious software considering all the threats involved and have conflicts with the university’s security policy as a result.

However, it is impossible to reach to accurate results after the hard disk analysis in a case where the malicious code is not executed. The purpose of this work is to investigate online ID theft incidents. Therefore, the execution of the malware over the Internet appears of vital importance for the successful completion of the experiment.

The question now is how the university policy that reasonably condemns the use of malware even for research purposes will be bypassed. The solution to this matter is to plant the malware on a standalone computer machine that is connected to the Internet but not connected to a computer network. This had to be achieved outside the university settings. The malware should be executed offline. Still the purpose of the experiment is to demonstrate the functionality of the ID theft framework, even if some restrictions apply due to the sensitivity of the private information.

Figure 26 represents the stages of the experiment execution as explained in a previous section of this chapter.

There are a number of forensic tools available, but the ideal for the purpose of the experiment should be chosen. On the market there are currently two leading forensics tools used by investigators; Encase from Guidance Software (2010) and FTK from AccessData (2010). Both these tools were available to use. Open source tools were not considered as both of the commercial tools are feature rich. Encase was selected as the author has extensive experience of using it. Other
forensic tools required included a hardware write blocker device for the experiment disks in order to prevent any alteration on the evidence hard disks. Also, a disk editor, in order to view any raw data on the disk and an MD5 utility is also required, because this way the integrity of the image and the original source. These are covered by the EnCase. Due to the complexity of steganography (see section 4.5.2.2) and the time restrictions of the experiment it was decided that steganalysis would not be included in the evaluation.

Another important issue to be resolved was the most appropriate ID theft method for the experiment. The Information Security Forum (2005) warned about ‘sophisticated and well-organised Trojan attacks’ a few years ago. These types of attacks are directly linked with online fraud and ID theft. Nowadays, a number of sources refer to plenty of incidents discussing about these new generation Trojan attacks (see Lowe (2009), Rodriguez (2009), Jaques (2008), MCRC (2008), Washkuch (2008), Thompson (2007)).

Therefore, because of the common use of Trojan horse attacks and their injected sophistication, the ideal method of attack for the experiment is considered to be a form of Trojan horse that steals personal data. It was chosen to use a malware from the Banker family. It satisfies the needs of the experiment and is popularly used by the attackers to date. Ståhlberg (2007) gives a detailed view of the Trojan that belongs to this family and their extent. Their purpose is to steal financial information from the machines they are installed on. Trojan.Banker was downloaded from Offensive Computing (2009).

However, while this experiment was planned, there were some thoughts of using a remote administration Trojan-tool, such as Back Orifice, for penetrating the victim’s system. These tools can remotely access a system’s files, log keystrokes and get passwords; they can also steal private data from the victim’s machine. Attention to the threat that arises from Back Orifice related to ID theft was also mentioned by Tarsavage (2007).

Such types of attacks though are application based. The way they work could be an issue for someone who attempts an attack, as well and an immediate alert on a security application. A Trojan could also be an alert, but customised malicious
software may act unattended on a system until reported. For this reason, the use of a Trojan appears more appropriate than the remote administration tool.

1. Is there any benefit for the outcome of the investigation if the researcher is not aware of the type of malware installed?

Another concern was whether there would be any benefit for the outcome of the investigation if the researcher is not aware of the type of malware installed and the nature of the attack. This is advantageous as in such a case the researcher does not work on a concrete and predefined process to discover something predefined. She is trying to identify the penetration of the system with the aid of the ID theft investigation framework, rather than trying to determine the incident based on the type and nature of the malware used. For this reason the researcher is unaware of the malware’s name and attributes at this stage.

Additional to this, it should be determined how the attack should be manipulated among the different ways that it could be managed. However, for this experiment it is part of the initial premise that the researcher is not aware of the attacker’s selected attack method. The attacker will choose the most appropriate line of attack for spreading the selected malware.

### 5.3 Police Review

#### 5.3.1 Aim of the interview

Based on Patton (1987), the qualitative interviewing in the terms of evaluation, aims to identify the point of view of the people that a piece of work is addressed. Also, identify their terms, opinions and thinking of personal perception and knowledge. There is an extensive background concerning the design of an interview and is useful to mention the three different types of interviews: the informal conversational interview, the interview guide approach and standardised open-ended interview (Patton, 2002). Clarke (1999), states that there is nothing more than ‘general advice’ on how to conduct an interview and no right way of doing it. The advantage of interviews is their data collection method (Leedy and Ormrod, 2005). The researcher is able to gather data for the core of the research and interpret it accordingly.
The meeting with the Hi-tech Crime Unit was conducted in the manner of an informal interview. The framework was presented and discussed with the members of the crime unit concerning its probable impact on real life incidents and obtain their feedback concerning the research work. However, the whole conversation was based on the already constructed questions from the researcher and consists of two parts:

a. general questions concerning ID theft investigations by the Gwent Police

b. questions based on the presented ID theft investigation framework

5.3.2 General questions on ID Theft investigations

1. How do you value the idea of discriminating the investigation of computer crimes based on their method?
   This question aims to record the investigator’s point of view for discriminating the examination based on the type of the crime.

2. Considering this method of investigation do you believe it can correspond to a valuable tool for the investigator?
   The investigator needs to give his point of view for the presented framework in respect to the existing used methodologies.

3. Do you believe that the procedure has the ability to speed up the investigation?
   The question aims to identify the investigator’s opinion, concerning the duration of the examination process, by the application of the presented framework.

4. Do you believe that the framework identifies all evidential aspects related to Identity Theft incidents?
   The practical experience of the investigator may identify some evidential aspects that are not stated in the framework.

5. Do you normally use evidence classification methods? If yes, how do you normally classify the evidence?
   It is a general question that aims to identify whether the police investigators use methods to categorise the evidence and in which way.
6. Does the framework facilitate the investigation of Internet Identity Theft cases and the processing of the related digital evidence?

This question was composed in order to identify the actual value of the framework towards digital evidence.

5.3.3 Specific questions on the methodology

7. Are the data flows and graphical representation of the framework supportive for the investigator?

A number of different data flows and graphs have been produced to support the framework and the purpose of the question is to understand whether these were found useful.

8. Are the inputs and the outputs of the procedure properly defined?

The question involves the inputs and the outputs of each activity and whether these were structured in accordance to the needs of the examination.

9. Are the inputs and the outputs those that you expected to identify?

By following the previous question, the purpose is to discover whether the investigator expected the framework to produce different inputs and outputs.

10. Do the aspects of the methodology assess the capabilities required from the perpetrator?

The purpose of this question is to make sure whether the framework exposes the capabilities the fraudster owns.

11. Does the methodology effectively assess the ongoing threat?

The question concerns the degree that the framework effectively covers the issues that involve ID theft.

12. Is the procedure generic enough in order to be applicable to all different systems?

The question aims to identify whether the investigator believes that the framework is flexible enough to be applied on different operating systems.

13. Do you believe that the evidence classification presented by the ID theft investigation framework is of your benefit?
The investigator is requested to give his point of view for the classification of the evidence described in the framework and whether he finds it beneficial in this type of case.

14. Did you identify any additional evidential data by the use of the presented framework? (comparing to the methodology you normally apply)

The purpose of this question is to ensure that the framework includes all types of evidence that can be found during the analysis.

15. Did you find the ‘Abstracted procedure for the investigator’ helpful during the analysis?

The ‘Abstracted procedure for the investigator’ can be found on Appendix H. It is an instruction booklet, created to guide the investigator during the analysis. The question aims to confirm the value of the booklet.

16. Did you find the ‘ID theft investigation framework’ form helpful during the analysis?

The document is found on Appendix I and it is used as the documentation of the investigation. The investigator is requested to give an answer on how useful this document was for him.

The results of these questions are discussed in the following chapter.
Summary

A research project needs to be reviewed and evaluated and verify its validity to the research world. The described verification procedure of this chapter aims to examine the validity of the ID theft framework.

The responsibility of the researcher is to identify the appropriate evaluation method/s that needs to be followed, in order to conclude in an accurate final result. The theoretical clarification and description concerning the methods that have been selected for the evaluation of the ID theft investigation framework have been presented. This chapter also described how theory will be applied in practice. For the needs of this project and in order to strengthen the evaluation process, two different ways of evaluation are combined:

1. Case study:
   - Applied on a laboratory experiment

2. Police Interview
   - Gwent Police’s application of the framework on a suitable case
   - Feedback in the form of an open-ended interview
This chapter presents

- the results of the laboratory experiment; and
- comments the feedback submitted by Gwent HTCU.

Overview

This chapter represents the application of the evaluation methods that were presented and discussed in the Framework Verification and Assessment (see chapter 5) in order to validate the research outcome.

After executing the closed network attack, the ID theft investigation framework was applied to the evidence left on the experimental system. The results are presented in the following sections. Screenshots and accompanied proof concerning the execution of the experiment can be found on Appendices L and M.

Each phase of the ID theft framework corresponds to the following structure, based on the analysis that was presented in chapter four:

**Description**: A brief summary of the phase activities including a summary of the appropriate inputs and outputs followed by its input and output regarding the experiment.

**Process**: A summary of the processes and their activities and their practical application.

**Comments**: Any important comments that arose during the application of the framework.

**Table**: An abstract table of the Documenting Procedure for the Investigator at the end of each process, as found on Appendix I.
The practical application of the Documenting Procedure for the Investigator is also demonstrated in this chapter, as it is used as the model for describing the experiment.

Later on this chapter, the reader will find a discussion that concerns the feedback received from Gwent Police, Hi-tech Crime Unit, after the application of the framework on an existing ID theft case. A questionnaire was supplied to the police detectives for assessing the proposed framework. The answers and comments of the questionnaire are discussed, while the original papers can be found on Appendix J. Furthermore, all communication e-mails exchanged with the police detectives can be found on Appendix K. Detective Tim Williams applied the framework on an existing case. Some of the original comments the investigator raised are quoted in this section in order to emphasise his observations during the analysis.

6.1 Application of Laboratory Experiment

The purpose of the laboratory experiment is to apply the ID theft investigation framework to the scenario case study described in the chapter 5. The practical application is intended to satisfy the objectives of the research and demonstrate the work flow of the framework.

Initially, the ID theft investigation framework was applied to the victim’s perspective. Then, the activities that concern the fraudster’s side were employed. This is due to the large number of the activities that constitute the framework, only the specified fraudster activities are extensively described on the second section. These are the parts of the framework that differentiate the fraudster from the victim. They concentrate on these specific processes of the framework rather than the whole investigation that is already demonstrated on the analysis of the victim. However, the framework was also fully applied during the experiment for the fraudster’s side.

The report produced by EnCase can be found on Appendix LI.
6.2 V. Victim

6.2.1 Phase 1: Media Analysis

6.2.1.1 Summary of Pma

The first phase involves the analysis of the digital media found on the crime scene and the identification of the significant evidential ID theft data. It consists of the following input and output:

Input: Digital Media, describes the procedure that should be undertaken when the investigator comes into the first contact with the crime scene and comprises of three processes. Because of the nature of the experiment, this input cannot be applied practically in the testing. However, it is considered to be functional as it is based on existing frameworks (see chapter 4).

Output: ID Theft Data Identification, the investigator is expected to browse the digital media in order to detect the aspects that confirm ID theft related evidence. It consists of three activities that involve this identification.

6.2.1.2 Digital Media

Process 1. Source Identification

This process applies to the first contact with the crime scene. The investigator needs to identify the computer related elements on the crime scene. As such application cannot be applied to a fictional scenario; the relevance to the framework will be as follows.

Input Activities

<table>
<thead>
<tr>
<th>I.1.1. Media Selection</th>
<th>Instruction 1. Online data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Objective 1.1. Evidential computer storage components</td>
</tr>
<tr>
<td></td>
<td>Objective 1.2. Computer storage media</td>
</tr>
<tr>
<td></td>
<td>Instruction 2. Offline data</td>
</tr>
<tr>
<td></td>
<td>Objective 2.1. Any offline data that can be</td>
</tr>
</tbody>
</table>
I.1.2. Live system

Instruction 1. Check operating system

Objective 1.1. Shutdown
Objective 1.2. Disconnect

Comments

The law enforcement team is considered to search the crime scene. According to the scenario the victim delivers his computer system to the police department, as it is a common recommendation in incidents similar to the scenario. The process is accomplished by searching for online data in computer related mediums. In such an application the victim’s computer is identified. No additional storage media is found that could be used for further analysis related with the ID theft incident. For the collection of the online mediums the system was shut down by the victim. Therefore, there is no live system involvement.

Expected Output Activity

O.1.1. Keep record of the scene

The crime scene is supposed to be found with the minimum alterations after the incident was reported to the law enforcement officers. The room contained a study desk, where a shut down desktop computer system was fitted at the time of the visit. Photographs of the room could have been taken in order to validate and ensure the visit in a proper application of the activity.

Process 2. Digital Media Collection

Input Activities

I.2.1. Identify different digital media
Instruction 1. Generic device storing personal data

I.2.2. Secure/isolate digital media

I.2.3. Collect/package digital media
**Expected Output Activity**

**O.2.1. Document**

The computer has a 20GB Fujitsu hard disk installed. No other digital media is identified on the system. The computer system is considered isolated and packaged, then collected and transported to the computer laboratory. The collected computer system had the following configuration: Pentium III 800 MHz, 256 MB RAM, hard disk 20GB, Samsung CD-ROM and installed operating system is Windows XP S.P. 2. No additional digital storage device was identified or collected.

**Process 3. Image Acquisition**

**Input Activities**

I.3.1. Select appropriate tool

I.3.2. Protect media from possible alteration of data

I.3.3. Image the original media

I.3.4. Store safely original media

I.3.5. Back-up the image, work on that

I.3.6. Create Cryptographic Value

**Comments**

The selected tool for the acquisition is the EnCase Enterprise 4.20. The hard disk was connected to the dedicated imaging machine in order to be acquired. EnCase FastBloc\(^1\) was used in order to protect the media from alteration of data. The image file was created on another dedicated computer machine on the network and saved under a filename that specified date of the acquisition and the owner of the disk. The imaging process took approximately two hours to proceed. When it was completed, the original hard disk was disconnected from the FastBloc and safely stored into a cabinet. A customised tag indicating details about the origin of the disk was installed before being stored. EnCase automatically creates a back-up

---

\(^1\) The write-protect device supplied to accompany the EnCase software
of the case, therefore a back-up of the image is unnecessary. The hash value of the image was created with the use of the EnCase. That was: 4878389711654C78866E5EA1C61B02D (Appendix L II).

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process 1. Source Identification</td>
<td></td>
</tr>
<tr>
<td>I.1.1. Media Selection</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Online data</td>
<td>P</td>
</tr>
<tr>
<td>Objective 1.1. Evidential computer storage components</td>
<td>P</td>
</tr>
<tr>
<td>Objective 1.2. Computer storage media</td>
<td>Hard Disk</td>
</tr>
<tr>
<td>Instruction 2. Offline data</td>
<td></td>
</tr>
<tr>
<td>Objective 2.1. Any offline data that can be used as additional evidence</td>
<td></td>
</tr>
<tr>
<td>I.1.2. Live system</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Check operating system</td>
<td></td>
</tr>
<tr>
<td>Objective 1.2. Shutdown</td>
<td></td>
</tr>
<tr>
<td>Objective 1.2. Disconnect</td>
<td></td>
</tr>
<tr>
<td>O.1.1. keep record of the scene</td>
<td>P</td>
</tr>
<tr>
<td>Process 2. Digital Media collection</td>
<td></td>
</tr>
<tr>
<td>I.2.1. Identify different digital media</td>
<td>P computer system</td>
</tr>
<tr>
<td>Instruction 1. Generic device storing personal data</td>
<td></td>
</tr>
<tr>
<td>I.2.2. Secure/isolate digital media</td>
<td>P</td>
</tr>
<tr>
<td>I.2.3. Collect/package digital media</td>
<td>P</td>
</tr>
<tr>
<td>Process 3. Image Acquisition</td>
<td></td>
</tr>
<tr>
<td>I.3.1. Select appropriate tool</td>
<td>EnCase</td>
</tr>
<tr>
<td>I.3.2. Image the original media</td>
<td>P</td>
</tr>
<tr>
<td>I.3.3. Protect media from possible alteration of data</td>
<td>P Write blocker</td>
</tr>
<tr>
<td>I.3.4. Store safely original media</td>
<td>P</td>
</tr>
<tr>
<td>I.3.5. Back-up the image, work on that</td>
<td>P</td>
</tr>
<tr>
<td>I.3.6. Create Cryptographic Value</td>
<td>P</td>
</tr>
</tbody>
</table>

Table 34: Pma - Digital Media Documenting procedure
6.2.1.3 ID Theft Data Identification

Process 4. Evidential data identification

Input Activities

I.4.1.V. Existence of malicious software

I.4.2.V. Existence of unsecured transactions

I.4.3.V. Vulnerable system

Comments

Existence of malicious software was identified at this stage. The system was checked with two different antivirus programs, Zonealarm and PC Tools. The reason for using these particular antivirus programs is that they are both popular, award winning commercial software. The author held a license for Zonealarm Antivirus (Zonealarm, 2010) at the period of the experiment, so it was considered as a respectable and well functioning antivirus. The PC Tools Antivirus (PC Tools, 2010) was available for free download. The purpose for using two similar antivirus programs is to ensure the consistency of the antivirus search in the digital media. Both programs identified that the system hosts two different types of malware that steal bank details. The alert on Zonealarm was Trojan.Win32.Agent.dtx and Trojan_Spy.Win32.banker.cpv, while PC Tools found Trojan.Agent.CWQA and TrojanSpy.Banker.LZY. A number of unknown .dll files exist in the system folder. These will be further analysed on the following phase, in order to identify whether the malware has been executed on the system and important files have been infected.

No antivirus or firewall was installed to the system, which makes it more vulnerable to the identified malware. In addition, a number of bank transactions were identified in the registry entries, leading to possible unsecured transactions.

Expected Output Activity

O.4.1.V. Victim evidential data list

The victim’s evidential data list is the following:

- Existence of malware identified
- unrecognised *.dll files
- unsecure transactions
- vulnerable system

Process 5. Target identification

Input Activities

I.5.1. vulnerable systems
I.5.2. published information
I.5.3. individual/ corporate

Comments

The system is exposed to different vulnerabilities as identified on the previous process. Therefore, the target was a vulnerable system. The owner of the media has published personal information on social networking web sites (Facebook, Hi5). The target is an individual system as it is already known from its owner (case study).

Expected Output Activity

O.5.1. Target identification list

The target identification list as is was identified:

- vulnerable system
- no security software installed
- accounts on social networking web sites identified
- individual system

Process 6. Threat agent identification/ intention

Input Activities

I.6.1. internal/ external attack
I.6.2. individual/ corporate
Comments

An external attack, as the system is not connected to a local network. The threat agent characteristic towards its target is an individual system.

Expected Output Activity

O.6.1. Threat agent identification list

The threat agent identification list at this stage is:

- external attack
- individual system

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process 4. Evidential data identification</td>
<td></td>
</tr>
<tr>
<td>V. Victim</td>
<td></td>
</tr>
<tr>
<td>I.4.1.V. Existence of malicious software</td>
<td>P</td>
</tr>
<tr>
<td>I.4.2.V. Existence of unsecured transactions</td>
<td>P</td>
</tr>
<tr>
<td>I.4.3.V. Vulnerable system</td>
<td>P</td>
</tr>
<tr>
<td>O.4.1.V. Victim evidential data list</td>
<td>P</td>
</tr>
<tr>
<td>Process 5. Target identification</td>
<td></td>
</tr>
<tr>
<td>I.5.1. vulnerable systems</td>
<td>P</td>
</tr>
<tr>
<td>I.5.2. published information</td>
<td>P Networking web sites</td>
</tr>
<tr>
<td>I.5.3. individual/ corporate</td>
<td>Individual</td>
</tr>
<tr>
<td>Process 6. Threat agent identification / intention</td>
<td></td>
</tr>
<tr>
<td>I.6.1. internal/ external attack</td>
<td>External</td>
</tr>
<tr>
<td>I.6.2. individual/ corporate</td>
<td>Individual</td>
</tr>
<tr>
<td>O.6.1. Threat agent identification list</td>
<td>P</td>
</tr>
</tbody>
</table>

Table 35: Pma - ID Theft Data Identification Documenting procedure
6.2.2 Phase 2: Evidence Analysis

6.2.2.1 Summary of Pea

The second phase of the framework involves the examination of the evidence. It receives as input, the output of phase one and is therefore constructed.

Input: ID Theft Data Analysis, the investigator is required to examine the identified ID theft data (output of phase one). It includes three processes for the analysis.

Output: Evidence, the evidential data that arose during the analysis is collected and categorised. This involves two processes.

6.2.2.2 ID Theft Data Analysis

Process 7. Data Analysis

Input Activities

| I.7.1. Identify all files of the system | Instruction 1. Existing files |
|                                          | Instruction 2. Deleted, remaining |
|                                          | Instruction 3. Hidden data |
|                                          | Instruction 4. Encrypted/ password protected |
|                                          | Instruction 5. Temp files/ folders |

I.7.2. Recover deleted files

I.7.3. Slack / Unallocated space

I.7.4. Hidden partitions

Comments

All files that can be analysed for evidence have been identified. The deleted files were retrieved from the disk image; the unallocated space can be examined. No hidden partitions were discovered. Two zip files were present in C:\Documents and Settings\user\My Documents
Expected Output Activity

O.7.1. Define files that can be used as evidence

Files that can be used as evidence at this stage are:

- Existing files
- Deleted, remaining
- Temp files/folders
- Recovered deleted files
- Slack / unallocated space

Process 8. Target Analysis

Input Activities

I.8.1.V. Malicious software/ code

| Instruction 1. Monitors web-browser Process/ network traffic
| Instruction 2. Accesses contact list records
| Instruction 3. Accesses clipboard contents
| Instruction 4. Trojans that collect personal information
| Instruction 5. Software Keylogger (hosted)

I.8.2.V. Local-based e-mail

I.8.3.V. Web-based e-mail

I.8.4.V. Embedded Object scripting access languages

I.8.5.V. Recently accessed documents

I.8.6.V. URL information

| Instruction 1. URL cache
| Instruction 2. URL Process record

I.8.7.V. Security permissions

I.8.8.V. Application histories

I.8.9.V. Instant message history log
I.8.10.V. Databases

I.8.11.V. Spreadsheets

I.8.12.V. Number systems

Comments

The identified malwares installed in the system are both Trojans that collect financial information and record keystrokes (keylogger). It immediately highlights the fact that the system would be vulnerable and the data may have been extracted this way. Based on antivirus internet reports (Sophos (2009), F-Secure (2009), Threat Expert (2009)) concerning the files that are created by the malicious software, a number of .dll files were identified (C:\Windows\System32\mscorews.dll, C:\Windows\System\shdocvsw.dll etc.). It is important to identify the behaviour of the malware and files that can be created or altered by it, in order to verify that it has run on the system. Because of the existence of malware the registry keys were examined, created files and directories, running processes and open ports. The behaviour of the Trojan-Spy:W32/Banker.CPV shows that it acts as a Browser Helper Object (BHO) on Internet Explorer, the web browser internet history appears. The following entries on the registry linked with the malware were discovered:

- HKLM\Software\Helper
- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{327C3AF0-4EF6-4f8a-9A8D-685A4815D9F8}  
- HKLM\Software\Classes\CLSID\{327C3AF0-4EF6-4f8a-9A8D-85A4815D9F8}  
- HKLM\Software\Classes\CLSID\{327C3AF0-4EF6-4f8a-9A8D-685A4815D9F8}\InprocServer32  
- HKLM\Software\Classes\CLSID\{327C3AF0-4EF6-4f8a-9A8D-685A4815D9F8}\ProgID  
- HKLM\Software\Classes\CLSID\{327C3AF0-4EF6-4f8a-9A8D-685A4815D9F8}\TypeLib
Local based e-mail was not identified on the system. However, information concerning web-based e-mail was retrieved. The user appears to have web-based e-mail accounts on Hotmail and Yahoo. The names of the accounts that were identified for the user are: jacobss05@yahoo.co.uk and jacobs.st@hotmail.com. A large number of e-mail contacts were identified in the search. Some personal e-mails were retrieved of no particular value. An e-mail contact scissors@email.com appears to have sent the compressed files game.zip and funny.zip to jacobss05@yahoo.co.uk that were saved on C:\Documents and Settings\user\My Documents folder and identified in I.7.1 as attachments\(^1\). The date the e-mail was sent is the 20\(^{th}\) of May 2008. The files were exported and unzipped. The analysis system alerted the files as virus infected.

Some work information was also retrieved from the retrieved e-mails on the user’s system and also published information on the Facebook and the Hi-5 platform.

The system is JavaScript enabled. The recently accessed documents didn’t illustrate anything suspicious concerning the victim’s story. The URL information was retrieved. The temporary internet files were checked and multiple browsing histories were identified. The user was using web banking internet sites (www.natwest.co.uk, www.hsbc.co.uk), where information login was retrieved. The alerts were Trojan.Win32.Agent.dtx and Trojan_Spy.Win32.banker.cpv, identical with those identified from Zonealarm on the image virus scan.

The security permissions of the Windows system were not altered and nothing valuable was retrieved from application histories. It appears that the system had Windows Live Messenger installed since 2006 and Yahoo Messenger on 2008. The history logs that were retrieved didn’t provide any evidence other than personal conversations. There was no database software installed on the system.

\(^1\) The e-mail was managed to be downloaded without activating the web server’s antivirus system, because it was planted to the system and not sent at the execution of the experiment. This information was revealed by the ‘attacker-fellow researcher’ that executed the case study scenario. The systems were connected to the internet when a dummy e-mail was sent to the victim by the fraudster’s machine representing the attack without alerting. Then, the malware was saved to the system and executed in order to install the Trojans.
There was a spreadsheet Microsoft Excel file, where the user kept track of his bank accounts balance (Bank Accounts 060408.xlsx). The file was un-erased.

Extensive number system searches that took place with EnCase included bank account number, post code, date of birth and telephone numbers.

Expected Output Activity

O.8.1.V. List evidential findings

The evidential findings list is:

- Malware evidence included:
  C:\Windows\System32\mscorews.dll
  C:\Windows\System\shdocvs.dll
  C:\Windows\System\edlin.dll
  C:\Windows\System\perfnw.cpl

- Registry entries

- User’s e-mail accounts
  jacobss05@yahoo.co.uk
  jacobs.st.hotmail.com

  and other e-mail accounts with recent contact:
  j.g.evans@gmx.xo.uk
  emma01@mail.org
  cocopika@hotmail.com
  scissors@email.com

- MSN contacts

- Yahoo! Messenger contacts

- Web-banking activities
  Logins on: www.natwest.com and www.hsbc.co.uk

- JavaScript

- User’s bank account numbers
- Virus infected e-mail attachments received:
  game.zip and funny.zip
- MS Excel file holding bank account numbers
  C:\Documents and Settings\user\My Documents\Bank Accounts 060408.xlsx
- Work information:
  Book publisher
- Post code:
  NP20 5EH
- Telephone numbers
- Date of birth:
  05/04/1969

Process 9. Threat Agent Analysis
Input Activities

I.9.1. Intention
   Instruction 1. Financial
   Instruction 2. Identity

I.9.2. Motivation
   Instruction 1. Target

I.9.3. Knowledge / Skills

Expected Output Activity
None

Comments
The existence of a Trojan that captures and steals financial information shows financial intention from the fraudster. The target that worked as motivation seems to be an independent unsecure internet connected system. The fraudster discovered an easy target that used minimum security measures and exploited it.
The skills of the fraudster so far declare him as a conspiracy, opportunist, innovative attacker, may belong to organised crime.

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process 7. Data Analysis</strong></td>
<td></td>
</tr>
<tr>
<td>I.7.1. Idenitify all files of the system</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Existing files</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 2. Deleted, remaining</td>
<td></td>
</tr>
<tr>
<td>Instruction 3. Hidden data</td>
<td></td>
</tr>
<tr>
<td>Instruction 4. Encrypted / password protected</td>
<td></td>
</tr>
<tr>
<td>Instruction 5. Temp files / folders</td>
<td>P</td>
</tr>
<tr>
<td>I.7.2. Recover deleted files</td>
<td>P</td>
</tr>
<tr>
<td>I.7.3. Slack / Unallocated space</td>
<td>P</td>
</tr>
<tr>
<td>I.7.4. Hidden partitions</td>
<td>P</td>
</tr>
<tr>
<td>O.7.1. Define files that can be used as evidence</td>
<td>P</td>
</tr>
<tr>
<td><strong>Process 8. Target Analysis</strong></td>
<td></td>
</tr>
<tr>
<td>V. Victim</td>
<td></td>
</tr>
<tr>
<td>I.8.1.V. Malicious software / code</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 1. Monitors web-browser activity / network traffic</td>
<td></td>
</tr>
<tr>
<td>Instruction 2. Accesses contact list records</td>
<td></td>
</tr>
<tr>
<td>Instruction 3. Accesses clipboard contents</td>
<td></td>
</tr>
<tr>
<td>Instruction 4. Trojans that collect personal info</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 5. Software Keylogger (hosted)</td>
<td>P</td>
</tr>
<tr>
<td>I.8.2.V. Local-based e-mail</td>
<td></td>
</tr>
<tr>
<td>I.8.2.V. Web-based e-mail</td>
<td>P</td>
</tr>
<tr>
<td>I.8.3.V. Embedded Object scripting access languages</td>
<td>P</td>
</tr>
<tr>
<td>I.8.4.V. Recently accessed documents</td>
<td>P</td>
</tr>
<tr>
<td>I.8.5.V. URL information</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. URL cache</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 2. URL activity record</td>
<td>P</td>
</tr>
<tr>
<td>I.8.6.V. Security permissions</td>
<td>P</td>
</tr>
<tr>
<td>I.8.7.V. Application histories</td>
<td>P</td>
</tr>
<tr>
<td>I.8.8.V. Instant message history log</td>
<td>P</td>
</tr>
<tr>
<td>I.8.9.V. Databases</td>
<td></td>
</tr>
<tr>
<td>I.8.10.V. Spreadsheets</td>
<td></td>
</tr>
</tbody>
</table>
Evaluation of experiments

I.8.11.V. Number systems

O.8.1.V List evidential findings

<table>
<thead>
<tr>
<th>Process 9. Threat Agent Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.9.1. Intention</td>
</tr>
<tr>
<td>Instruction 1. Financial</td>
</tr>
<tr>
<td>Instruction 2. Identity</td>
</tr>
<tr>
<td>I.9.2. Motivation</td>
</tr>
<tr>
<td>Instruction 1. Target</td>
</tr>
<tr>
<td>I.9.3. Knowledge / Skills</td>
</tr>
</tbody>
</table>

P unsecure system
P conspiracy, opportunist

Table 36: Pea - ID Theft Data Analysis Documenting procedure

6.2.2.3 Evidence

Process 10. Evidence Collection

Input Activity
10.1. Use evidential findings list, O.8.1.V or O.8.1.F.

Expected Output Activities

<table>
<thead>
<tr>
<th>O.10.1. Create list of evidence based on ID Theft types</th>
<th>Instruction 1. Financial Instruction 2. Identity</th>
</tr>
</thead>
</table>

O.10.2. Threat agent Evidence list (Process 9 is used as input)

Comments

The evidential findings list O.8.1.V is used as an input and the created outputs are:

O.10.1. Financial

- Identified Malware evidence
- Web-banking activities
- User’s bank account numbers
- Virus infected e-mail attachments received and saved on (game.zip and funny.zip)
- MS Excel file holding bank account numbers (C:\Documents and Settings\user\My Documents\Bank Accounts 060408.xlsx)
- Date of birth

Identity
- User’s e-mail accounts
- MSN contacts
- Yahoo! Messenger contacts
- Post Code
- Telephone Numbers
- Date of birth
- Business record

O.10.2.
- Financial intention because of the behaviour of the malware
- Independent unsecure internet connected system
- Innovative attacker may belong to organised crime

At this stage the actual categorisation of the findings has begun. Process 10 uses the evidence that was discovered during the ID Theft Data Analysis (Processes 7, 8 and 9). It satisfies its purpose that is to collect all these findings and sort it according to the ID theft type (O.10.1) and the threat agent related findings.

Process 11. Evidence Categorisation
Input Activity
I.11.1. Use evidential findings list, O.8.1.V or O.8.1.F respectively

Expected Output Activity
O.11.1. Create evidence classification list
| Instruction 1. Strongly Evidential
| Instruction 2. Evidential
Instruction 3. Irrelevant

Comments

- Strongly Evidential: Malware evidence, Virus infected e-mail attachments.
- Evidential: Web-banking activities, User’s bank account numbers, MS Excel file holding bank account numbers, Work information, Post code, Telephone numbers, Date of Birth.
- Irrelevant: MSN contacts, Yahoo! Messenger contacts, personal instant messenger log files, personal e-mail communication.

The above classification list refers to and sorts the findings that are directly linked with ID theft. The data included in the Strongly Evidential are inarguable findings related with ID theft. In this case, malware that records financial information and virus infected e-mail attachments are strongly evidential findings that reveal the involvement of an ID thief.

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process 10. Evidence Collection</strong></td>
<td></td>
</tr>
<tr>
<td>I.10.1. Use evidential findings list, O.8.1.V or O.8.1.F.</td>
<td>P</td>
</tr>
<tr>
<td>O.10.1. Create list of evidence based on ID Theft types</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Financial</td>
<td></td>
</tr>
<tr>
<td>Objective 1.1. Credit histories</td>
<td>P</td>
</tr>
<tr>
<td>Objective 1.2. Transactions</td>
<td>P</td>
</tr>
<tr>
<td>Objective 1.3. Application names</td>
<td></td>
</tr>
<tr>
<td>Objective 1.4. Phone records</td>
<td></td>
</tr>
<tr>
<td>Objective 1.5. Tax records</td>
<td></td>
</tr>
<tr>
<td>Objective 1.6. Bankruptcy records</td>
<td></td>
</tr>
<tr>
<td>Objective 1.7. Documents on other people’s names</td>
<td></td>
</tr>
<tr>
<td>Objective 1.8. Dates of birth</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 2. Identity</td>
<td></td>
</tr>
<tr>
<td>Objective 2.1. Financial Evidence</td>
<td>P</td>
</tr>
<tr>
<td>Objective 2.2. N.I. Numbers</td>
<td></td>
</tr>
</tbody>
</table>
6.2.3 Phase 3: Scenario Construction

6.2.3.1 Summary of Psc

The third phase of the framework interprets the evidence identified on Pea in order to reach effective conclusions. It receives as input the output of the previous phase. It is constructed as following:

**Input:** Evidence Classification, the identified categorised evidence will be classified.

**Output:** Scenario, creates an outline of the scenario that involves the evidential findings.

6.2.3.2 Evidence Classification

<table>
<thead>
<tr>
<th>Process 11. Evidence Categorisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.11.1. Use evidential findings list, O.8.1.V or O.8.1.F.</td>
</tr>
<tr>
<td>O.11.1. Create evidence classification list</td>
</tr>
<tr>
<td>Instruction 1. Strongly Evidential</td>
</tr>
<tr>
<td>Instruction 2. Evidential</td>
</tr>
<tr>
<td>Instruction 3. Irrelevant</td>
</tr>
</tbody>
</table>

Table 37: Pea - Evidence Documenting procedure
Expected Output Activity

O.12.1. Categorisation of evidential data

Instruction 1. E-mail
Instruction 2. Internet Related
Instruction 3. Malware
Instruction 4. Hacked Databases
Instruction 5. Malicious Tools
Instruction 6. Documents
Instruction 7. Application logs
Instruction 8. System Vulnerabilities
Instruction 9. Other

Comments

1. e-mail accounts and communication identified:
   user and contacts e-mail accounts

2. Internet related:
   JavaScript installed, web banking logins and activity, social networking account logins, instant messengers and contacts

3. Malware:
   Malware evidence .dll files and registry entries

4. Hacked databases:
   None

5. Malicious Tools:
   Virus infected e-mail attachments received

6. Documents:
   MS Excel file holding bank account numbers

7. Application logs
   Instant message history log files
8. System Vulnerabilities

   No security permissions altered

9. Other

   Work information, Post code, Telephone numbers, Date of birth

Process 13. Structure threat agent’s profile

Input Activity

I. 13.1. Use Threat agent Evidence list O.10.2

Expected Output Activities

O.13.1.V Reveal technical skills

O.13.2.V Reveal programming skills

O.13.3.V Ability to convince someone

O.13.4.V Ability to keep stealth action

Comments

The threat agent’s profile has been structured according to O.10.2.

O.13.1.V. Technical skills by the fraudster in order to effectively use the malware

O.13.2.V. Programming skills to create and distribute the malware

O.13.3.V. Persuasion skills to convince someone run the malware

O.13.4.V. The malware would have been identified if the system had antivirus installed.


Input Activities

I.14.1. Structure all sort of valuable information

I.14.2. Identify evidential aspects

Comments

The most relevant evidential data identified during the examination linked with the incident is the following (I.14.1.): Malware evidence, Virus infected e-mail
attachments saved in C:\Documents and Settings\user\My Documents\funny.zip and C:\Documents and Settings\user\My Documents\games.zip, Web-banking activities, User’s bank account numbers, MS Excel file holding bank account numbers, Work information, Post code, Telephone numbers, Date of Birth.

The evidential aspects that belong together in a group are identified (I.14.2.) and prepared to be presented at the output of the process.

Expected Output

O.14.1. Group the evidential aspects

All evidence involved with the malware is grouped as it states the most critical information identified: antivirus results, malware behaviour, .dll entries, registry entries, and virus infected e-mail attachments. This output is the result of I.14.1 and I.14.2.

The Evidence Classification aims to organise the findings before preparing the Scenario of the case. Some of the activities may seem repeatable to the reader. However, they adhere to the logical continuation of the process and they are fully represented in this section in order to demonstrate their functionality.

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process 12. Structure of evidential data</strong></td>
<td></td>
</tr>
<tr>
<td>I.12.1. Use evidence as of Processes 10 &amp; 11</td>
<td>P</td>
</tr>
<tr>
<td>O.12.1. Categorisation of evidential data</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. E-mail</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 2. Internet Related</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 3. Malware</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 4. Hacked Databases</td>
<td></td>
</tr>
<tr>
<td>Instruction 5. Malicious Tools</td>
<td></td>
</tr>
<tr>
<td>Instruction 6. Documents</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 7. Application logs</td>
<td></td>
</tr>
<tr>
<td>Instruction 8. System Vulnerabilities</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 9. Other</td>
<td></td>
</tr>
<tr>
<td><strong>Process 13. Structure threat agent’s profile</strong></td>
<td></td>
</tr>
<tr>
<td>I. 13.1. Use Threat agent Evidence list O.10.2</td>
<td></td>
</tr>
</tbody>
</table>
6.2.3.3 Scenario

Process 15. Scenario Outline

Input Activity

I.15.1. Use evidence as of I.1.1.< Instruction 2, Phase 1< ID Theft Data Identification, Phase 2< Evidence, and Phase 3< Evidence Classification

Expected Output Activity

O.15.1. List valuable data gathered

Comments

I.15.1. is used and creates the following valuable data gathered (O.15.1.). The list is not presented here for avoiding repetition, as it uses the outputs of phases one, two and three and these are already indicated on the previous sections. I.1.1< Instruction 2 contains no relative data with this examination. The scenario outline list is used as an input on the next process.

Process 16. Scenario Preparation Documentation

Input Activity


Expected Output Activity

O.16.1. Merge evidential data gathered
Comments
All evidential data from process fifteen (O.15.1.) is gathered in order to continue to phase four. The purpose of process 16 is to document everything that will be included in the case in the last phase.

The evidential data gathered include:

Victim evidential data list (O.4.1.V.): Existence of malware identified, unrecognised *.dll files, unsecure transactions, vulnerable system

Target identification list (O.5.1.): vulnerable system, no security software installed, accounts on social networking web sites identified, individual system

Threat agent identification list (O.6.1.): external attack, individual system

Financial information (O.10.1.): Identified Malware evidence, Web-banking activities, User’s bank account numbers, Virus infected e-mail attachments received and saved on (game.zip and funny.zip), MS Excel file holding bank account numbers (C:\Documents and Settings\user\My Documents\Bank Accounts 060408.xlsx), Date of birth

Identity information (O.10.1.): User’s e-mail accounts, MSN contacts, Yahoo! Messenger contacts, Post Code, Telephone Numbers, Date of birth, Business record

Threat agent evidence list (O.10.2.): Financial intention because of the behaviour of the malware, Independent unsecure internet connected system, Innovative attacker may belong to organised crime

Evidence classification list (O.11.1.): Strongly Evidential data identified: Malware evidence, Virus infected e-mail attachments, Evidential: Web-banking activities, User’s bank account numbers, MS Excel file holding bank account numbers, Work information, Post code, Telephone numbers, Date of Birth, Irrelevant: MSN contacts, Yahoo! Messenger contacts, personal instant messenger log files, personal e-mail communication.

Categorisation of evidential data (O.12.1.): e-mail accounts and communication identified: user and contacts e-mail accounts; Internet related: JavaScript installed, web banking logins and activity, social networking account logins, instant messengers and contacts; Malware: Malware evidence .dll files and registry
entries; Hacked databases: None; Malicious Tools: Virus infected e-mail attachments received; Documents: MS Excel file holding bank account numbers; Application logs: Instant message history log files; System Vulnerabilities: No security permissions altered; Other: Work information, Post code, Telephone numbers, Date of birth

The threat agent’s profile (O.13.1- 4.V): Technical skills by the fraudster in order to effectively use the malware, Programming skills to create and distribute the malware, Persuasion skills to convince someone run the malware. The malware would have been identified if the system had antivirus installed.

Group the evidential aspects (O.14.1.): All evidence involved with the malware; antivirus results, malware behaviour, .dll entries, registry entries, virus infected e-mail attachments.

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process 15. Scenario Outline</td>
<td>P</td>
</tr>
<tr>
<td>1.15.1. Use evidence as of I.1.1.&lt; Instruction 2, Phase 1&lt; ID Theft Data Identification, Phase 2&lt; Evidence, and Phase 3&lt; Evidence Classification</td>
<td>P</td>
</tr>
<tr>
<td>O.15.1. List valuable data gathered</td>
<td>P</td>
</tr>
<tr>
<td>Process 16. Scenario Preparation Documentation</td>
<td>P</td>
</tr>
<tr>
<td>1.16.1. Use Scenario outline list from O.15.1.</td>
<td>P</td>
</tr>
<tr>
<td>O.16.1. Merge evidential data gathered</td>
<td>P</td>
</tr>
</tbody>
</table>

Table 39: Psc - Scenario Documenting Procedure

6.2.4 Phase 4: Evaluation

6.2.4.1 Summary of Pe

The Pe evaluates the scenario and produces the case report. The following input and output are required:

Input: Scenario examination, where the output of phase three is tested and clarified.

Output: Case, the actual case documentation is created based on the evaluated evidential findings.
6.2.4.2 Scenario Examination

Process 17. Scenario Testing/ Evaluation

Input Activities

I.17.1. Use Phase 1< ID Theft Data Identification, Phase 2< Evidence, and Phase 3< Scenario

I.17.2. Check validation/ entirety of the outputs

Comments

The outputs from the previous phases are used and their validity is checked among the phases. No mistakes were identified.

Expected Output Activity

O.17.1. Create evaluation list

The evaluation list includes the most crucial data of the examination as this was stated in O.11.1. Malware evidence, Virus infected e-mail attachments. No amendments were made, and the validity of the evidential files was confirmed.

Process 18. Scenario Clarification

Input Activities

I.18.1. Use evaluation list as of O.17.1.

I.18.2. Clarify the impact of evidential data

Comments

The evaluation list is used (O.17.1.); the impact of evidential data is clarified according to the evidence.

Expected Output Activity

O.18.1. Create scenario clarification list

The scenario clarification list for this activity is identical with O.17.1, as no amendments were made. Therefore, it is constructed as following:

Malware evidence, Virus infected e-mail attachments and also the output of O.16.1 that states all evidential data gathered.
Table 40: Pe - Scenario Examination Documenting procedure

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process 17. Scenario Testing / Evaluation</td>
<td></td>
</tr>
<tr>
<td>I.17.1. Use Phase 1&lt; ID Theft Data Identification, Phase 2&lt; Evidence, and Phase 3&lt; Scenario</td>
<td>P</td>
</tr>
<tr>
<td>I.17.2. Check validation / entirety of the outputs</td>
<td>P</td>
</tr>
<tr>
<td>O.17.1. Create evaluation list</td>
<td>P</td>
</tr>
<tr>
<td>Process 18. Scenario Clarification</td>
<td></td>
</tr>
<tr>
<td>I.18.1. Use evaluation list from O.7.1.</td>
<td>P</td>
</tr>
<tr>
<td>I.18.2. Clarify the impact of evidential data</td>
<td>P</td>
</tr>
<tr>
<td>O.18.1. Create scenario clarification list</td>
<td>P</td>
</tr>
</tbody>
</table>

6.2.4.1 Case

Process 19. Case Construction

Input Activity

I.19.1. Use data from the scenario clarification list O.18.1

Comments

The scenario clarification list is used as it emerged from O.16.1 and O.17.1 in order to create the output of the activity.

Expected Output Activity

O.19.1. Construct the case

The outline of the case is created at this activity as it is given from the input I.19.1. The representation of the evidence should be linked with the impact of the case. It is not entirely stated at this section as the evidential data has been indicated on the previous sections.

The investigator could also follow this activity as a draft of the case documentation that he is required to compose in a later process.
Process 20. Case Clarification

Input Activity

I.20.1. Clarify the constructed case from O.18.1.

Comments

The relation of the evidential data is justified in accordance to the initial premise that is the ID theft incident that the user of the computer system appears to have fallen as a victim.

To summarise, the victim appears to have received an e-mail attachment with the files funny.zip and games.zip from scissors@email.com. The user saved into the C:\Windows\user\My Documents folder these files, unzipped them and installed the two Trojans, TrojanSpy.Banker.LZY and Trojan.Agent.CWQA. The behaviour of the Trojans in relation to the created files identified during the forensic analysis justifies the ID theft incident.

Expected Output Activity

None


Input Activities

I.21.1. Use the scenario evaluation list from O.17.1.

I.21.2. Check validation

Comments

Again the output of process 17 is used in order to evaluate the constructed case as this was outlined in process nineteen.

Expected Output Activities

O.21.1. Confirm case evaluation

The official outcome of the case is confirmed at this activity based on the evidential findings that constructed it.
Process 22. Evidential Case Representation

Input Activity

I.22.1. Create the testimonial report

| Instruction 1. Include all case evidence |
| Instruction 2. Describe all case evidence |

Comments

All case evidence as it was identified in phases one, two and three and included at this process and described.

Expected Output Activity

O.22.1. ID Theft Case Investigation Report

The case report includes everything as mentioned on I.22.1. The report is not extensively written at this activity. It includes all case evidence that was described on the previous cases in a manner that could support a juridical judgement.

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process 19. Case Construction</td>
<td>P</td>
</tr>
<tr>
<td>I.19.1. Use data from the scenario clarification list O.18.1</td>
<td>P</td>
</tr>
<tr>
<td>O.19.1. Construct the case</td>
<td>P</td>
</tr>
<tr>
<td>Process 20. Case Clarification</td>
<td>P</td>
</tr>
<tr>
<td>I.20.1. Clarify the constructed case from O.18.1</td>
<td>P</td>
</tr>
<tr>
<td>I.21.1. Use the scenario evaluation list from O.17.1.</td>
<td>P</td>
</tr>
<tr>
<td>I.21.2. Check validation</td>
<td>P</td>
</tr>
<tr>
<td>O.21.1. Confirm case evaluation</td>
<td>P</td>
</tr>
<tr>
<td>Process 22. Evidential Case Representation</td>
<td>P</td>
</tr>
<tr>
<td>I.22.1. Create the testimonial report</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 1. Include all case evidence</td>
<td>P</td>
</tr>
<tr>
<td>Instruction 2. Describe all case evidence</td>
<td>P</td>
</tr>
<tr>
<td>O.22.1. ID Theft Case Investigation Report</td>
<td>P</td>
</tr>
</tbody>
</table>

Table 41: Pe - Case Documenting Procedure
The application of the ID theft investigation framework on the victim’s side demonstrated the functionality of the framework. In addition, it verified that the processes that constitute it support the initial premise that aims to facilitate the investigation of computer based ID theft as well as the handling of the related digital evidence.

6.3 F. Fraudster

The parts of the framework that involve the analysis from the fraudster’s side will be presented at this section. The victim’s analysis presented results that profiled the fraudster’s intention and motives. However, the design of the experiment as this was described on chapter 5 included the attacker’s computer system in the specifications. This allows the analysis of the fraudster’s hard disk. The framework has been applied on the digital media; however it is partially presented in order to demonstrate its functionality on fraudster (F).

Therefore, processes four, eight, nine, ten and thirteen will be presented. These processes include the fraudster’s division and some of the analysis that involves him, in order to compare the results with the evidential findings from victim (V). The reports produced by the EnCase and accompany the investigation can be found on Appendix M. It is important to mention that the hard disk was checked for viruses prior to the examination with Zonealarm and PC Tools and no viruses were identified.

Process 4. Evidential data identification

Input Activities

I.4.1.F. existence of malicious software code

I.4.2.F. forensic extraction software

I.4.3.F. hacking tools

Comments

Expected Output Activity

O.4.1.F. Fraudster evidential data list
On the fraudster evidential data list, the following elements were identified:

- no existence of malicious software code (written scripts), programming code existed in the system, but not written by the user (implementation of the MD5 message-digest algorithm (C language source code)).
- Encase, AccessData, WinHex, MD5 Digest were installed in the system
- Cain and Abel (Brute force), RAR Password Cracker, Password Tools folder

Process 8. Target Analysis

Input Activities

I.8.1.F. Internet bookmarks

I.8.2.F. Steganographic search

I.8.3.F. Embedded Object scripting access languages

I.8.4.F. Installed software

Instruction 1. Web design applications
Instruction 2. Existence of Anti-Forensics applications
Instruction 3. System Process eraser

I.8.5.F. Track illicit software use

I.8.6.F. Recently Accessed Documents

I.8.7.F. Filenames

I.8.8.F.URL information

Instruction 1. URL cache
Instruction 2. URL Process record

I.8.9.F. Local based e-mail

I.8.10.F. Web based e-mail

I.8.11.F. Operating System Registry entries

I.8.12.F. Security permissions
I.8.13.F. Instant message history log
I.8.14.F. Malicious software (Trojan code / bot)
I.8.15.F. Malicious source code existence
I.8.16.F. Web server communication
I.8.17.F. Databases
I.8.18.F. Spreadsheets
I.8.19.F. Images
I.8.20.F. File Processes
I.8.21.F. Number systems

Comments

The Internet bookmarks that were identified provided the support of malicious interests that were bookmarked (http://sectools.org/crackers.html, http://www.password-crackers.com/en/articles/12/, http://www.nirsoft.net/, http://www.nmrc.org/pub/faq/hackfaq/hackfaq-05.html, http://kerpass.wordpress.com/2007/01/25/phishing-dns-poisoning-man-in-the-middle/). As well as interest on forensic examinations and hacking courses (http://www2.cit.cornell.edu/services/training/courses/chfi.html, http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm). A print screen image can be found on Appendix M II. The installed software did not include web design, anti-forensic or system process eraser applications. However, as mentioned on O.4.1.F forensic extraction software and hacking tools were identified. The recently accessed documents provided a large amount of information concerning the user. It effectively showed a link to C:\Documents and Settings\user\Desktop\brutus-aet2, a brute forcing application that wasn't identified on process four. In addition a file concerning malware presentation was identified (C:\Documents and Settings\user\Local Settings\Temp\Rar$D100.547\malware.ppt). These also identify some suspicious for the filenames activity. In addition a search for filenames in malware returned the following that belongs to an external plugged in device, probably a USB memory stick: LEGO::P:\Research\Malware\malware2.zip, C:\Documents and
Settings\user\Desktop\Malware\malware.zip from the recent files. A snapshot can be found on Appendix M II. However, the archived file was never saved on the hard disk on a further archived files search (covers activities I.8.15.F. and I.8.16.F as well).

The URL information was retrieved for the bookmarks identified so far and revealed the user’s online visits. The user was mostly using Mozilla Firefox as it provided more activity than Internet Explorer. The cookies.txt and the downloads.rdf files were observed, but they didn’t appear to have any malicious code downloads. The user was active on .avi downloads instead. Searches on the Windows Temporary Internet Files appear to include malware searches. Facebook activities but not logins to an account were found. The existence of the account could be linked with searches for potential targeted identities. Furthermore, activity on the malware forum, www.offensivecomputing.net was discovered.

There was no local based e-mail browser used. However, there was web based e-mail activity and contacts. E-mail accounts were retrieved from Google mail and mail.com through online access. The e-mail logins that were used were l.h.scissors@googlemail.com and scissors@email.com. The activity of the e-mail account was extensive by sending and receiving e-mails with individuals as well as subscriptions. Among these, the e-mail message that was sent to jacobss05@yahoo.co.uk with the file attachments funny.zip and games.zip was identified.

The operating system entries and the security permissions didn’t show any alterations. Instant Messenger log files show the victim’s e-mail Jacobs.st@hotmail.com added as a contact among others (e.g. fsr0000F.log, fsr00010.log). Appendix M II provides this information. Web server communication was not identified in the system. No spreadsheet or database files were also created or saved in the disk. A number of the victim’s pictures were identified on the fraudster’s hard disk.

Expected Output Activity

O.8.1.F. List evidential findings

- Malicious and forensic interests on Internet bookmarks
- Forensic extraction software and hacking tools
  Cain and Abel, RAR Password Cracker, Password Tools, Brutus, EnCase
- Recently accessed documents
- Filenames
  \texttt{LEGO\cdot P:\Research\Malware\malware2.zip}
- URL information
  Malware searches
  Facebook activity
  www.offensivecomputing.net
- Active e-mail accounts
  l.h.scissors@googlemail.com
  scissors@email.com
- Instant Messenger contacts
  Jacobs.st@hotmail.com

Process 9. Threat Agent Analysis

Input Activities

I.9.1. Intention
  Instruction 1. Financial
  Instruction 2. Identity

I.9.2. Motivation
  Instruction 1. Target

I.9.3. Knowledge / Skills

Comments

Based on the findings the intention of the threat agent could match both financial or identity as the fraudster’s hard disk appear to have a number of different research activities on malware, forensic extraction software and hacking tools.

The target is any vulnerable, unsecure system that could accept the malware attachment and execute it. The knowledge/skills of the threat agent match I.9.3 on
Victim (V), as the findings declare him as a conspiracy, opportunist attacker. However, he cannot belong to organised crime, as he is mostly described as a novice researching the malware capabilities.

**Process 10. Evidence Collection**

**Expected Output Activity**

O.10.2. Threat agent Evidence list (Process 9 is used as input)

- Financial and/or Identity
- Vulnerable, unsecure to malware system
- Conspiracy, opportunist, novice attacker

**Process 13. Structure threat agent’s profile**

**Input Activity**

I. 13.1. Use Threat agent Evidence list O.10.2

**Expected Output Activities**

O.13.1.F Sophistication of tools
O.13.2.F Level of expertise
O.13.3.F Use of defensive techniques
O.13.4.F Identify purpose of attacking
O.13.5.F Identify motivation
O.13.6.F Identify opportunities

**Comments**

The output of O.10.2 is used in order to structure the threat agent’s profile.

O.13.1.F. The sophistication of tools identified state him as an opportunist. The evidential findings didn’t provide any information about the fraudster compiling complex methods (e.g. customised malicious scripts). Therefore, the fraudster took advantage of an occasional victim.

O.13.2.F. The attacker is not advanced based on the findings in his digital media.
O.13.3.F. Anonymous mail servers or man-in-the-middle attacks were not identified as defensive techniques during the analysis. However, the straightforward method of contacting the victim could reveal some social engineering techniques.

O.13.4.F. The purpose of attacking appears to be either curiosity or ego; to prove that he was able to achieve ID theft.

O.13.5.F. The motivation appears to be personal financial gain.

O.13.6.F. The above outcomes are used in order to assume and outline the profile of the fraudster.

This part aimed to apply the required for the fraudster processes of the framework. Even though there were limitations concerning the laboratory experiment, the processes were applied successfully and provided valuable results that could also represent evidential ID theft data of a real incident.

6.4 Discussion of the results

The ID theft framework needs to be a tool that combines theory and practice in order to assist the investigator. This was a major concern at the beginning of the design and the implementation, as the academic background needed to incorporate practical issues. However, the framework had to be low level and specific, and at the same time generic in order to be able to adopt different circumstances. The validity of this effort wouldn’t be supported without an experimental evaluation.

The laboratory experiment had some limitations (see chapter 5, section 5.2.3) due to the sensitivity of ID theft. For this reason, the experiment was not executed under completely realistic circumstances. A real fraudster would attack the system remotely by sending a sophisticated malware, aiming to breach the system’s firewall and antivirus. On the closed network attack the malware should not be able to send data over the Internet, because of the risk of having a leak of private information. Therefore, the only solution that would approach reality was to plant the malware. The fellow researcher that assisted the experiment acted as the fraudster planted the malware and executed it offline on the system; rather than try to open the e-mail attachment. Nevertheless, the purpose of the experiment is to demonstrate the functionality of the framework and not to penetrate the victim’s
system. The web-based e-mail providers have embedded malware detection systems and would not allow opening the attachment.

However, the execution of the malware offline has probably resulted in missing the creation of some files and registry entries that are considered to be created by the specific malware. The entries that were not identified in the victim’s system were subject to the Viruses and Spyware analysis of Sophos (2009) that provided information about the action of the malware. This was not considered as a disadvantage for the application of the framework. The purpose of the experiment was to verify whether it can be successfully applied on an ID theft investigation without omitting any evidential aspects. It appears that both the victim and the fraudster part did not miss anything of vital importance that could provide misleading results.

An initial consideration was that ideally the evidence that results from the victim’s investigation would provide enough information to lead to the fraudster. The profiling of the fraudster does give some indications about his behaviour, but there is not enough guidance to lead on discovering the perpetrator. However, there is intelligence gathering on profiling each fraudster with the evidence that is left behind on a victim’s machine.

The framework may be very precise in phases three and four where the discovered evidence needs to be sorted and evaluated. It could be an issue that an investigator would prefer to spend less time treating the evidence than required. The structure of the ID theft framework guides the investigator during the examination, so that he knows every step he needs to follow. The scenario construction and the evaluation phases are designed based on science and theory, and need to have a complete structure. Therefore, they are detailed and approach the handling of evidence in a way that may be questioning for the investigator. The last two phases could be condensed and satisfy the same purposes in less processes.

As mentioned already, the framework did not fail to identify evidential data after the experiment. While chapter two presented all the different techniques that online ID theft can be achieved and the framework was created around these techniques, the experiment only examined the malware occasion. It is considered that the rest of the techniques can also be successfully applied in the framework,
but they are untested. The reason that the framework was not applied in all techniques was mainly practical. Setting up experiments to cover all techniques would require time and resources. The demonstration of the framework’s functionality on a popular ID theft technique (malware) should be representative for all techniques.

The detailed description of the experiment in the previous sections aims to provide the most possible information concerning its execution. Both parts of the framework, concerning the victim and the fraudster, provided the desired results and indicated that the framework could be applied in any ID theft technique.

In order to avoid the evaluation of the experiment to appear one sided; the contribution of the expert review resolves this issue. The following sections intend to provide from an expert’s side of view that the evaluation of the ID theft framework could not only be successfully applied to a controlled environment, but also on the real world.

6.5 Presentation of expert review

This section details the second part of the evaluation undertaken on the ID theft framework. It presents the expert evaluation that was received from Gwent Police, Hi-tech Crime Unit. The feedback provided some suggestions concerning the framework, but it was overall positive and encouraging. The comments and discussion on the questionnaire received by the experts appears in the following section.

An evaluation based on the opinion of an expert on the field is invaluable. Therefore, the expert advice of the Gwent police officers was requested in order to establish and validate the objective of the research. During winter 2007, an initial approach was made to the police officers. The purpose was to explain the intention of the research and how their practical experience and guidance would be important for this piece of work. Their practical experience enlightened sections on the development of the framework, especially the evidence analysis (Phase 2-Pea).
6.5.1 Expert Review

The police officers agreed to assist and provide an insight concerning the evidence that is left behind after an ID theft incident. Their instructive comments informed the design stage and were used during the implementation period. Furthermore, the officers gave permission for their names and emails to be incorporated into this thesis.

In May 2008 a draft of the framework (comprising chapters 3 and 4) was sent to Detective Jon Evans. The email also briefly outlined the aim of the research. In addition to the outline of the framework, all the produced graphs that illustrate the framework and its phases were sent, accompanied by the ‘Abstracted Procedure for the Investigator’ document (Appendix H). The purpose is to assist the experts in how to use and apply the ID theft framework for the investigation of a real incident and differentiate the examination from their usual procedure.

Detective Jon Evans forwarded the attached material to Detective Tim Williams; the expert officer, who deals with the computer forensic examination of relevant incidents. He replied with an insightful and detailed e-mail (see Appendix K) mentioning some areas in the framework that he believed would be valuable for the practical approach of each activity. His comments were taken under consideration. However, some of them were considered as too broad for the purpose of the current framework, some others were included but probably not recognized before the application of the framework and some others valuable (see section 6.5.2.1). Therefore, some amendments were made to suit the latest comments.

The purpose of this framework is to formalise the procedure on a theoretical and practical basis, in order to be applicable on numerous ID theft cases regardless the technology that is involved. Effectively in the same e-mail DC Williams mentioned:

... I have not been able to apply the framework to a live job, as I do not have a job that fits the criteria at the moment. However it does seem to be a complete and comprehensive coverage of handling an ID theft. I do like the idea of a framework as it prevents overlooking some crucial
part of an investigation and frameworks are present in so many other areas of policing.

On a later e-mail he noted:

...the outline framework doesn’t seem to be missing anything major in an investigation of this type. You have obviously put a lot of effort into it.

A few days later DC Williams replied with the filled in questionnaire that was applied on an already investigated case. That case was examined with the traditional method that Gwent police is using and the findings were already known. Consequently, it was much more efficient for the detective to apply the ID theft framework and try to identify the crucial evidence he was supposed to conclude and evaluate the results. This method was additionally beneficial for the framework as it was immediately compared with a verified by the police procedure.

The detective answered the questionnaire and the results are discussed below (see section 5.3). The completed questionnaire can be found on Appendix J.

On the first question the investigator was asked to value the idea of discriminating the investigation of computer crimes based on their method, where he answered that he totally agrees and commented that

If the method of committing the crime is known and is reliable, then it is more efficient to concentrate your investigation efforts to areas known to be affected, rather than following the same routine for all offences.

On the second question that was asking whether an ID theft framework can be a valuable tool for the investigator. The detective also answered that he totally agrees.

The third question concerned the data flows and graphical representation of the framework and whether they were supportive for the investigator and the he agreed, however he noted that

Some of the graphical representations may need explaining to investigators before they are used. Although I can see that the graphical files are not meant to be used as a standalone description.
The fourth question was about the effectiveness of the framework and whether it would speed up the investigation and the detective partially disagreed, while he commented the following:

My disagreement isn’t a negative thing. The framework is comprehensive and would give an investigator more things to look at, which may have been overlooked or forgotten, therefore extending the initial examination, but this may lead to a time saving later on if there is no need to return to a case.

The fifth question aims to discover whether the framework identifies all evidential aspects related to Identity Theft incidents. The interviewee totally agrees with this and points out the following comment:

When applying the framework I did not discover anything missing that would have a detrimental effect on the investigation; neither could I think of anything else to add. However a framework, like software, will probably have a few minor bugs, and they will be discovered the more they are used. This framework appears to have the ability to be “tweaked” should the need arise.

The sixth question involved the produced inputs and the outputs of the framework and whether the investigator believed that these were defined properly. In this question the expert answered that he totally agreed, without giving any comments.

The seventh question was of a similar manner and enquired the investigator to answer if the inputs and the outputs were those that he expected to identify. He answered that he totally agreed, revealing that he was asked to examine areas of the media that he had already identified and detected as an expert.

On the eighth question he was required to answer whether such a type of framework assesses the capabilities of the fraudster. The interviewee agreed with the probability that the findings can sketch the profile of the fraudster. The ninth question aims to verify whether the framework effectively assesses the ongoing threat of ID theft and the investigator answered that he agrees. However, he raised the following comment:

Short term: yes. The method of ID theft is fluid and the criminals are constantly re-inventing themselves. Whilst we may have an idea of what
is happening now and the methods being employed, this will change in the future as criminals get to know investigators capabilities. However the framework is future-proof and new areas of examination can be added as would any such procedure.

The tenth question enquires whether the framework is generic enough to be applicable in different systems, meaning the different operating systems and the interviewee answered in such a manner and agreed totally, while he commented:

If by systems you mean Computer Operating systems, then yes. I don’t think it would make any difference what computer was being used. It does not limit the investigator.

The eleventh question examines the general reflection of the framework towards an investigation by asking if the framework facilitates the investigation of Internet ID theft cases and the processing of the related digital evidence. DC Williams totally agreed with that, while he mentioned:

I didn’t have the opportunity to apply the framework to an active search warrant, but the framework brings structure to gathering digital evidence pre-delivery to the forensic lab, so I don’t see any particular problem with this. The framework certainly brings structure to an investigation. I have had moments in the past where I stare blankly into space wondering what I am doing and where I am going. The framework brought a structure I could follow and tick-off as I progressed the case.

The twelfth question was asking whether the interviewee normally uses evidence classification methods and if yes how the evidence is usually classified. The purpose was to identify the existing procedure of the police department, without a structured approach that the presented framework provides. The investigator replied the following:

Normally our evidence is either classed as admissible or not (but still disclosable) there are varying strengths to admissible evidence, but this is not normally broken down. With changes in law, what has been inadmissible can now be used as evidence of bad character or knowledge and expertise of computer systems. In criminal cases the evidence overall has to be of such strength as to be beyond all
reasonable doubt. Civil cases are on a balance of probabilities. Therefore, the strength of the evidence will vary depending on the court hearing the case.

There is also a classification of evidence that undermines the prosecution and assists the defence, which has to be disclosed at some point during the prosecution.

His response reveals that the classification of the evidence according to the procedure the police follows is based on the prosecution and the defence, rather than the quality of the collected information that can be used as evidence.

The thirteenth question adds to the previous by asking whether the evidence classification presented by the framework is of the investigator’s benefit. He answered that he agrees with this, while he commented:

From a Police/CPS perspective I think it will highlight where the strengths and weaknesses of a case are. I am not sure if classifying the evidence would require some additional work on the case or if this would aid the enquiry. My case did not require classification so I cannot comment further. It would need to be put into practice and commented on after a few applications.

It proves that he comprehends the purposes of classifying the evidence that is to identify the strengths and weaknesses of the incident. However, this could be an additional workload for the investigator. The fact that the detective did not actually classify the evidence on his case cannot defend a negative aspect on the classification.

The fourteenth question asked whether the investigator identified any additional evidential data with the application of the framework, comparing to the procedure he normally uses. His answer was negative and he mentioned the following:

I didn’t, but that is simply because the evidence wasn’t there. I did have extra logs and files to check thanks to the framework, which perhaps I would have missed or would have had to come back to at a later date.

The last two questions involved the additional material that was provided to the detective in order to assist the investigation. The fifteenth question aims to value
the importance of the ‘Abstracted procedure for the investigator’ (Appendix H) document that was provided for fulfilling the analysis. The interviewee totally agrees with the existence of this document and commented that

There is enough of a description so that the investigator knows what is required.

The sixteenth question involved the ‘ID theft documenting procedure for the investigator’ form and whether that was found useful during the analysis (Appendix I). The interviewee agreed with the idea of this document, however he commented the following

I didn’t use it. This is new to me so I needed the ‘Abstracted procedure for the investigator’ document as it was a bit more descriptive. However, most of the headings are obvious as to what is required and with a few applications it would take over as the main document to follow.

At the end of the questionnaire on question seventeen, the interviewee was prompted to provide comments and recommendations concerning the framework. The purpose of this section was to let the interviewee express his general opinion about the framework. The correspondence was satisfying and supported the positive feedback that was outlined by the rest of the questionnaire. The exact words of the expert are quoted below and those phrases that are considered as most important are highlighted.

There is always some reluctance to change the way an offence is investigated, but e-crime is becoming a very complex area of investigation with some serious offences being committed. It is becoming apparent that an investigator needs to complete a structured investigation that can be followed by others and reach the same conclusion and or results. The phrase “We need to be singing from the same song book” comes to mind.

I am not a fan of catch all check lists as you may have to spend time explaining to a court or defence barrister why you didn’t look at a particular area that is on the list (a check list is a disclosable document if used). The idea of a framework that is offence specific is more appealing.
Using a framework that caters to a particular offence ensures that you do exactly what is required, keeps an investigator on-track, reduces the chance of overlooking an area where evidence could reside and affords some flexibility for the individual.

It is clear that a lot of work has gone into this framework and it fitted well into my case. It was a little difficult at first, but with repeated use this will get easier the more it is used as with any other new policy or procedure. I would certainly consider using it again when it is finally published. I also think it would make a good foundation for any offence specific investigations.

On the first paragraph the interviewee stresses the need of a structured approach towards e-crime as this becomes even more popular. This need is supported by the development of the ID theft investigation framework, concerning the ID theft related incidents. As he mentions on the second paragraph the idea of an offence specific framework can also confront the defence that would try to debate other methods of investigation. The benefit the investigator extracts from this method of investigation is that he keeps the analysis focused on its purpose as mentioned above. However, the most important matter DC Williams raises is that he would certainly consider using this work when published. His last words show that the presented work can satisfy not only scientific needs, but also assist investigations in real life.

6.5.2 Discussion on the expert review

The previous section is a demonstration of the views that were provided from the field expert. It was chosen to quote some of the comments received from Gwent Police in order to stress their value.

The best of effort was given to create the questionnaire in a way to provide a general evaluation of the framework. DC Williams was positive with the idea of a crime specific framework and his responses showed that he appreciated its purpose with the first application. It was not the intention of the above section to provide a one sided review that shows no flaws to the ID theft framework, but to reassure the demonstration of its positive aspects.
However, the fact that the feedback was overall positive shows that the initial research hypothesis was validated:

It is proposed to create an analytical framework to facilitate the investigation of Internet Identity Theft cases and the processing of the related digital evidence.

The framework facilitated the investigation of computer based ID theft and handled the related digital evidence. This was confirmed while the investigator stated that he could have overlooked some evidential data he would probably need to return on a later stage of the investigation to find them. The application of a structured flow that assists the ID theft investigation guided him not to miss any evidence.

The investigator believes that the framework does not accelerate the investigation required time. However, a repetition of the framework could possibly familiarise the investigator with the process and eventually require less time for its application.

The supporting material that accompanies the framework aims to cover any queries that an investigator could generate. The Abstracted procedure for the investigator (Appendix H), the document that explains the functionality of the framework was beneficial for the expert. Therefore, this paper appointed its purpose to act as a field manual to what the framework requires. The detective commented that he did not use the form ID theft investigative methodology, which after the evaluation of the work was renamed to ID theft investigation framework, Documenting Procedure for the investigator. This naming was considered as more suitable for its purpose.

The detective commented that the graphical representations may need some explanation. Still the reason that the graphs were chosen to be represented in a simple form was to be easily comprehended by anyone. Definitely some explanation about the philosophy of the framework’s design would make them easier to understand. The purpose of the graphs though is to accompany the framework and not to stand alone.

The detective agrees with the fact that the framework assesses the capabilities required from the fraudster and the ongoing threat of ID theft. However, he
effectively mentions that future methods could be developed by the fraudsters. The positive argument he raises on that is that he considers the framework as a future-proof design that could adopt upcoming procedures.

The field expert believes the ID theft framework is a structured approach towards the processing of the digital evidence. It is an acknowledgement that the work has achieved one of its main targets. The flexibility of the framework was also mentioned as the expert believes that it is not limited and could be applied to different operating systems. Even though, the feedback involved only the view of a single expert, his comments are indicative that the ID theft framework could be applied in the real world and return accurate results of the investigation.

### 6.5.2.1 Evaluation issues on the field expert review

The meetings and the evaluation of the field experts provided a number of alternative perspectives for the framework. These requested some clarifications of some areas of the framework that were taken under consideration during and after the evaluation. They need to be mentioned at this stage to support the evaluation and provide an overall assessment of this research. Some points could be considered as weaknesses and others as optional considerations.

The framework could have included internet specific guidelines that would refer to remote data storage. The field expert mentioned that there are warrant issues due to territory problems in order to manage the access on remote systems and cloud environments. Such an approach is particularly interesting, but it seems a research area on its own. There are also other issues on that, as a fraudster could delete remote data at any time, which would complicate the investigation. Also, there should be implications concerning privacy rights in order to achieve access on the remote server. There should be given particular effort on this type of investigation and the ID theft framework would lose its focus if these areas were included. However, they are considerable for future development or amendments.

A limitation of the framework is that it is basically built upon standalone systems. It could be applied to networks as well, but there are not special activities referring to networked systems. The handling of offline data on activity I.1.1 should have included routers as well as the field expert has effectively indicated. The routers are commonly used and security logs, DHCP lists, access through a
firewall and port forwarding could provide evidential data. Because the network forensics is a special category and might include more additional aspects, they weren’t considered at the design of the framework.

Activity I.1.2 considers the handling of a live system. There are two objectives provided, shutdown and disconnect. Effectively the detective has commented that they are taught to pull the plug from the computer, which is in accordance with the ACPO (2007) guidelines or shutdown the system. So, in this case, the disconnect objective could have been clearer in order to avoid unplugging the wall socket.

The field experts have also pointed out some more effective comments on the communication and meetings we had. These add to the framework the expertise of the practitioner. The comments concerned how to examine the virus program logs, treat steganography, if suspected, and compressed files. These indications can be found on Appendix K. However, it is considered that they mainly refer to the way an investigator practically analyses the evidence. Some of them are mentioned in chapter four; some others are left with the side of the investigator and his experience. After all, the purpose of the framework is to facilitate the investigation, to show the way the examination should be treated, rather than describe of the examination process.

6.6 The properties of the framework

The properties that the ID theft investigation framework needs to include were presented at chapter 2 (see section 2.5.7.2). Table 43 demonstrates that the evaluation of this research work supported that these properties were successfully met. It is a combination of the laboratory experiment and the expert review.

<table>
<thead>
<tr>
<th>The properties of the ID theft investigation framework</th>
<th>P Processes 4, 8 and 13 of the framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>It should divide the investigation concerning the victim or the fraudster.</td>
<td>P Processes 5, 11 and 12 of the framework</td>
</tr>
<tr>
<td>It should provide classified evidence.</td>
<td></td>
</tr>
<tr>
<td>It should provide profiling of the fraudster.</td>
<td></td>
</tr>
</tbody>
</table>

Table 42: The accomplishment of the framework’s properties
The application of the framework in the case study showed that the required results were discovered for both, the victim and the fraudster. The investigation can follow a different direction based on the subject of the examination. The first property concerning the separation between the victim and the fraudster is met on processes 4, 8 and 13 of the framework and according to the laboratory experiment (see sections 6.2.1.3, 6.2.2.2, 6.2.3.2 and 6.3) it was satisfied.

Even though the best of effort was made on the design of the questionnaire, there appears to have an omission that was only noticed when the results were studied. There is no question assigning the separation of the investigation on the victim and the fraudster side. However, the Gwent police was aware of that since our early meetings discussing the design of the framework. Then, they supported this separation. According to the feedback they provided no negative comments were raised that could influence this feature of the ID theft framework.

Another property that was set for the framework was to classify the evidence. The classification of the evidence is designed in order to organize the evidential findings and as it was experienced from the laboratory experiment it didn’t require much time. The findings were already there. The advantage is that the findings will be processed for the case construction, when the evidential data is already classified (see sections 6.2.1.3, 6.2.2.3, 6.2.3.2 and 6.3).

The investigator provided a different aspect on classification, based on the procedure that the police follow. They classify the case as admissible or not, challenge the prosecution and assist the defence. In one of our e-mail communications he reckons that there may be an issue in court if some evidence has not been disclosed by the police. The classification does not intend to leave any evidential findings outside the final report of the case. Perhaps some initial findings could be considered as irrelevant, but they should still be considered.

The positive comment of the expert is that the classification of the evidence could draw attention to the strengths and weaknesses of the case. He worries though, whether this would require extra time during the investigation (see section 6.5.1).

The experiment collected appropriate material that could give an outline of the fraudster’s intentions (see sections 6.2.1.3, 6.2.2.2, 6.2.3.2 and 6.3). The purpose of the profiling is more to gather intelligence that would assist future
investigations. Due to the results of the experiment it was demonstrated that evidential data discovered can assist on drawing the profile of the fraudster that has committed ID theft. It derives only from the available evidential data of a specific case though, which could make the profiling subjective.

Apparently, the questionnaire omitted a question concerning the profiling of the fraudster. The investigator did not comment about it at any point in order to discuss his opinion at this stage. However, the profiling of the fraudster is based on the evidential findings and the construction of the scenario, where the detective provided positive feedback.

Even though the questionnaire for the expert review had omitted some of the properties the framework needed to include, the combination of the police feedback and the experiment showed that these properties were met for this application.

**Summary**

The purpose of this chapter was to evaluate the ID theft investigation framework and support its validity. This was achieved by employing two evaluation methods as introduced in chapter 5.

The application of the framework on a laboratory based experiment involved a victim and a fraudster. The case study scenario that was composed concerned the implication of a computer user who noticed that he had a number of daily incidents connecting him with ID theft. The examination of the hard disk that was identified on his system showed that malware that steals financial information was installed. The application of the ID theft framework was successful. Then, the hard disk that was used for the fraudster’s purposes was analysed in order to apply the framework on the fraudster’s side processes and evaluate their practice. The application of these processes provided accurate results.

The second part of this chapter demonstrated the feedback that was received from a field expert from Gwent police. The answers from the questionnaire that was provided to the detective were discussed. It worth repeating an important comment among his positive feedback: it does seem to be a complete and comprehensive coverage of handling an ID theft. The expert also mentions that he
considers using the framework in real incidents as he is tempted by the idea of an offence specific investigation structure.

In chapter 2 some issues were raised concerning the design of the framework. Based on them (see section 2.5.7.2) the following premises needed to be considered before its implementation. The evaluation chapter supports table 42 showing where these concerns were eliminated.

<table>
<thead>
<tr>
<th>Design issues</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>A deep understanding and knowledge of ID theft in order to avoid overlooking evidential data.</td>
<td>Sections 6.4 and 6.5.2</td>
</tr>
<tr>
<td>To be easily comprehended and applied by the practitioner.</td>
<td>P</td>
</tr>
<tr>
<td>To be comprised of all different systems and technologies, in order to be flexible.</td>
<td>Sections 6.4, 6.5.1 and 6.5.2</td>
</tr>
</tbody>
</table>

Table 43: Design issues met

The results of the laboratory experiment and the field expert review confirmed that the framework has the ability to recover evidential data that is there, without overlooking any evidence. The practitioner comprehended and applied the framework on the second part of the evaluation, while he also provided positive feedback. The experiment was executed in a controlled environment in order to evaluate its functionality. The field expert applied the framework in an already investigated case, where the evidential findings were established. Both instances showed that it is a flexible tool that can be adopted in different environments.

However, the framework could have been applied in all different types of ID theft and could have received feedback from more field experts. Then, the precision and verification of the framework would have been preserved and would have established the ID theft framework. Even though there were multiple restrictions that did not permit such an evaluation approach, the laboratory experiment and the expert review contributed in providing indicative and supportive results of the validity of this work.

The evaluation showed that even though there might have been some weaknesses that appear to exist in the framework it is a complete ID theft investigation approach. It could be applied in real life investigations and provide accurate results concerning this type of e-crime.
Conclusion and further research

In this chapter the reader can

► find a summary of the thesis;
► find the conclusions of the research;
► discover recommendations for further research on the subject.

Summary

This chapter aims to provide a brief summary to the reader of what has been achieved in this thesis, discuss the various problems that appeared during the lifetime of the research and finish with suggestions for future work and research on the subject.

Technological innovations contributed in the increase of ID theft in the digital environment. Computer forensics has provided a number of different investigation frameworks and guidelines in order to assist the investigators. However, these are generalised in order to be flexible and appropriate for all types of computer crime. The extensive increase of ID theft incidents, and the complexities of ID theft in a digital environment, both suggest a need for a specific methodical framework for investigating digital ID theft. This approach can support the investigator, focus the procedure on the type of the crime and produce reliable, repeatable results.

To develop the framework a review of ID theft was undertaken, and the different types identified. A framework that is especially designed for examining ID theft related cases was developed. The evaluation and assessment of the framework was supported by officers from the Gwent Hi-tech Crime Unit. The sensitivity of personal data and legal and ethical implications caused some limitations for the execution of the laboratory experiment. Nevertheless, the results were a
suggestive demonstration that the investigation framework can be applied on ID theft cases.

7.1 Contribution to science

The execution of the experiment as well the feedback obtained after the application of the framework from the Hi-tech Crime Unit indicated the practicability of the framework and that the outcome of this work could be applied to actual cases. Computer forensics investigations require a structured and formal approach. Standards and formal procedures concerning digital investigations are still progressing and developing and this work contributes to the effort to improve the digital investigative process.

The presented work has successfully introduced, constructed and assessed a formalised and structured approach that assists the computer forensics investigator in handling digital evidence of computer-based ID theft. The rapid growth of ID theft incidents demanded a guided, analytical framework that is especially designed for investigating these incidents.

This research work examined ID theft, its different techniques and characteristics, in order to recognise the uniqueness of this type of crime. It maintained the idea that different types of computer crime should be treated separate, in relation to their nature. The product of the research was the development of the investigative framework that differentiated the procedure between the victim’s and the fraudster’s side. This approach directs the investigator in the examination of the digital media.
7.1.1 The research objectives

The research objectives are set in the formulation of a research project. It is of great importance then for the researcher to be able to identify whether the research objectives have been met. Then, the outcome of the work is validated Table 44 represents the appointed objectives.

<table>
<thead>
<tr>
<th></th>
<th>Research Objective</th>
<th>Chapters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Analyse the state of the art in order to identify and investigate the different types of Identity Theft</td>
<td>P Chapter 2</td>
</tr>
<tr>
<td>2</td>
<td>Develop a conceptual framework for analysing the process of Identity Theft investigation and assess the digital evidence.</td>
<td>P Chapters 3 and 4</td>
</tr>
<tr>
<td>3</td>
<td>Evaluate the framework based on case studies and expert opinion in order to assess the proposed framework’s impact on processing online Identity Theft cases.</td>
<td>P Chapters 5 and 6</td>
</tr>
</tbody>
</table>

Table 44: Research Objectives

The first objective was met with the completion of Chapter 2, where the state of the art was studied and analysed. The different types of ID Theft were examined and the need for research on the subject was established. The examination of the existing literature set the requirements for this work.

The second objective refers to the implementation part of this research. Chapters 3 and 4 handle the design, the development and the analysis of the framework. The reader can find in detail how this objective was met by referring to these chapters.

The third objective concerns the evaluation of this work. The application of the research outcome in the real world was introduced on Chapter 5, where the two main evaluation methods to be applied were presented. This chapter demonstrates in the previous sections the results of the laboratory experiment and the evaluation feedback from the Gwent Police, Hi-tech Crime Unit. The positive experiment outcome and the evaluation feedback satisfied the third objective.
7.1.2 Project Review

Some issues that concern the planning, analysis and design of a research work need to be determined at its conclusion. This procedure is called decision making (Buchanan and O’Conell (2006), Leedy and Ormord (2005)) evaluation approach, where the answer should be usually a simple ‘yes’ or ‘no’ and the questions formed have been based on the overall content and behaviour of the research taken place and its outcome.

There is a large theory behind the term decision making. The Harvard Business Review on Decision Making (2006) appeared of great value background reading. Harris (1998) defines decision making as the process of sufficiently reducing uncertainty and doubt about alternatives to allow a reasonable choice to be made from among them. In simple words, decision making helps the researcher to identify the positive or negative status of his research. By following the ‘whether’ kind of decisions the researcher is requested to answer with a simple ‘yes’ or ‘no’.

The decision making evaluating approach provides an inner assessment for the assessment of the work. Leedy and Ormord (2005) suggest decision making in the form of a checklist for evaluating qualitative research projects. For this research, the decision making questions are based on the methods and findings of the research. In order for the researcher to be able to give accurate answers to the questions, the following procedure should be followed as presented from Harris (1998):

![Decision making procedure](image)

Figure 27: Decision making procedure

The following questions have been constructed as a result of the effort taken so far. They are inner enquiries that regard the value and the quality of this research work. Some research issues during the research were resolved with these questions in mind intending to affirmative answers. The questions and their answers are presented in table 45 below.
## Decision making Question and Answers

<table>
<thead>
<tr>
<th>Decision making Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Can the benefits of the project be assessed?</td>
<td>Yes, the ID theft framework is the research outcome and its benefits were evaluated with the execution of the experiment.</td>
</tr>
<tr>
<td>2. Is the final outcome of the project useful and original?</td>
<td>Yes, the final outcome is useful to the real world, according to the feedback of Gwent police and the evaluation of the framework. The originality of the work relies on the fact that a similar research work does not exist in the literature.</td>
</tr>
<tr>
<td>3. Is there enough justification with background reading and citation of sources?</td>
<td>Yes, it appears that the number of different sources used and cited prove that the author performed adequate research on the existing literature.</td>
</tr>
<tr>
<td>4. Can the project be realistically applied on such type of investigations and does it follow a concrete methodology / technology?</td>
<td>Yes, the combination of a laboratory experiment and the application of the framework on a law enforcement case suggest that the research outcome can be applied on the real world under a concrete method.</td>
</tr>
<tr>
<td>5. Does the project fulfil the aims and objectives of the design? Does it apply to the hypothesis for the contribution of science?</td>
<td>Yes, as presented on the previous section the objectives set in the beginning of the research were met. An attachment between the author and the hypothesis for the contribution to science existed throughout the research years in order to ensure and support the initial statement. The result indicates that it was successful.</td>
</tr>
<tr>
<td>6. Are the techniques that have been used for the analysis of the project thoroughly described?</td>
<td>Yes, even though a number of amendments had to be conducted in order to ensure this. To the best of the author’s knowledge, even a non-expert reader should understand the content.</td>
</tr>
<tr>
<td>7. Are tables, figures and graphs understandable and clarifying for the reader?</td>
<td>Yes, the best effort has been done so that the captions of the tables, figures and graphs that have been used are indicative of their content and can stand on their own.</td>
</tr>
</tbody>
</table>

Table 45: Decision making questions and answers
7.2 Further Research

The evaluation of this work demonstrated that individual examination methodologies concerning the different types of computer crimes can contribute to the investigative process.

In applying the ID theft investigation framework the investigator needs to be aware of the procedure he needs to follow. A future development would be the creation of an application that would guide the investigator during the process and assist in recording his findings. This way, the output functions that result after the examination can be structured automatically without any interference from the investigator. The results will be gathered faster at the end of the investigation, while the examiner will be occupied only with the input functions of the framework.

Such an approach could be achieved with the implementation of an application that keeps all data in a database, and provides the investigator with a step-by-step procedure that involves further required actions. Such an application could be either stand alone or online by linking the findings of different laboratories examining similar cases.

There may also be a need for the development of other specific methodologies according to the type of computer crime that has been perpetrated. However, it is recognised that there may be a situation where a complex crime has occurred. In such a case, this approach would fail to apply.

In order to overcome this issue, the categorisation of the digital media examination based on the computer crime, should be combined under one automated tool. Even if the investigator is unaware of the type of crime at the beginning of the investigation, he will be able to follow a structured procedure that identifies certain clues. These clues will provide initial results that adhere to certain types of crime. This ‘sorting’ the evidence will eventually result to profiling the type of crime according to the findings.

A creation of an online database that includes all different computer crimes could be the answer. The investigator interacts and simultaneously examines the media with the selected analysis tool. The database processes all the functions automatically and produces the listings that are the required outputs. It could even
create the documentation of the investigation. An improved version of such a database could also combine different types of crimes, in order to include more complex or mixed cases.

Another alternative for the computer forensics world could be the implementation of the following idea. An online database can keep records of all different evidential findings for all computer crimes. The automated system can produce statistical results that concern specific types of crime on a regional basis. It could be also applied on a national or international base, for example an online tool that holds data concerning all computer forensic investigations in the European Union. There are two actual benefits out of such an application:

1. The online automated tool is an intelligent instrument that manages to gather evidence about different types of computer crimes. This information can be shared among the investigators for a collective structured and in depth collection of data. Therefore, the examiners could benefit in working time and effort from references to previous investigations and existing results.

2. The result of this information gathering from different sources could lead to a deep understanding of the nature of the incidents. For example, the profiling of the ID thief aids to a deeper understanding of the purposes and the actions of the fraudster. Furthermore, collections of the attacks that concern all different types of computer crimes lead to the understanding of each different type of crime respectively. The effect in the long run is the understanding of the areas in which enhanced computer security is required.

Although, it may be considered impractical or of little use for its cost, knowledge exchange would occur if such a tool could efficiently work. As a result, practitioners, law enforcement agencies, and researchers would benefit from such an approach and proactively deal with computer crimes.
7.3 Conclusion

The rationale of this research work is the implementation of a conceptual analytical ID theft investigation framework. Based on the existing literature there are a number of different computer forensics methodologies that examine digital evidence. The initial purpose was to ‘facilitate the investigation of computer-based ID theft and the handling of the related digital evidence’, as stated on the hypothesis. The need was born due to the continuous growth of ID theft figures based on the incidents reported.

Some key issues had to be considered. ID theft is an old type of crime that has taken advantage of the growth of new technology. The ID thief can perform his actions with a combination of techniques, computer-based or not. Therefore, the outcome of an ID theft investigation is influenced by not only the evidential information identified during the computer investigation, but also by the findings that concern the crime scene. As in most crimes, ID theft requires two parts, a victim and a fraudster (or criminal). In order to establish a tool for the investigator, the methodology had to differentiate the examination for both parts.

The initial assumption was that the investigation of the victim’s digital media would lead the investigator to identify the fraudster. However, this cannot be achieved in all cases, as the intruders attempt to conceal their activity. Though the attempt to profile the fraudster and categorise the gathered digital evidence appears of value for the digital investigation.

A major limitation in the development of the analysis was the limited volume of existing literature in the area. In order to provide a broad scope for research an extensive review of related material on methodologies was required. Related sources needed to be researched and examined for ensuring that they are used and referred appropriately in this work. The availability of background material on actual ID theft examples also caused some difficulty when considering the assessment of the investigation framework. It seems that the authorities intentionally do not publish in detail the methods ID thieves follow for achieving fraud, in order to avoid providing facts that could be followed by potential fraudsters.
Despite good computer security practices taken in relation to private information, there is a possibility of ID theft while the computer that contains the data is connected to the Internet. Crime follows the money and ID theft is for the most part about money. It is therefore likely that number of incidents containing the misuse of identity data will continue. As Schneier (2004), effectively mentions:

It’s clear that computer security is not a problem that technology can solve. Security solutions have a technological component, but security is fundamentally a people problem.

Computer forensics is employed in cases when computer security fails. As long as computer security retains a human component, then there will be a need for computer forensics and further research will be required in the field.

The development of an ID theft framework is only a small component in this research area, where there is scope for work to develop a number of processes.

The Internet is a valuable tool but with a significant degree of risk that cannot easily be eliminated. Even though there have been efforts to identify the threats, eliminate the risks, inform and educate the users, attacks against someone’s good name cannot be totally omitted. There lies the need for computer forensics. It can effectively recover a computer machine’s history, after people have failed on computer security.

There is no happiness where there is no wisdom;
No wisdom but in submission to the gods.
Big words are always punished,
And proud men in old age learn to be wise.

Sophocles, Antigone, Greek tragic dramatist
References


Cambridge Advanced Learner's Dictionary, 2008, Cambridge dictionaries online


Dinev T., October 2006, Why Spoofing is serious Internet Fraud, COMMUNICATIONS OF THE ACM, Vol. 49, No. 10


Hinde, S., 2004a, “All you need to be a phisherman is patience and a worm”, Computer Fraud & Security, Volume 2004, Issue 3, Pages 4-6


Hinde S., Bupa, 2004c, Banking on security and control?, Computer Fraud and Security, Volume 2004, Issue 8, Page 4-6


References


McDowell K., November 2006, Now that we are all so well-educated about spyware, can we put the bad guys out of business?, SIGUCCS '06: Proceedings of the 34th annual ACM SIGUCCS conference on User services


Owen P., 2005, Investigation & Evaluation into how Identity Theft can be carried out and methods of protection against it. Unpublished master’s thesis, University of Glamorgan, Wales


References


Russell K., Phishing, Computerworld, 1/19/2004, Vol. 38 Issue 3, p44, 1p; (AN 12081860)


Appendix A:

Research Methodology
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DATA</strong>&lt;br&gt;Disk Study: 259 Hard Disks</td>
<td><strong>DATA</strong>&lt;br&gt;Journals&lt;br&gt;Books&lt;br&gt;Internet Websites&lt;br&gt;Reports</td>
<td><strong>DATA</strong>&lt;br&gt;Information of the attacks</td>
<td><strong>ANALYSIS</strong>&lt;br&gt;Experiments</td>
</tr>
</tbody>
</table>

- **Cyberattack**
  - Phishing
  - Pharming
  - Malicious software etc.
- **Targeted Facilitated Cyberattack**
  - Stolen IDs
  - Dumpster Diving
  - Deceased People etc.

- **Forensic Framework**

- **Information**
- **Attacks**

- **Part 4.1**
  - Closed Network Attack
- **Part 4.2**
  - What is left behind?

- **Stealable** ID Information
- **Attacks**: "How are IDs stolen?"
- **Forensic Procedure**: "What might be stolen and how?"
- **Evaluation of the Procedure**: "Using Evidence of the attacks"
Appendix B:

Academic Publishing

Journal Research Paper

On-line ID Theft Techniques, Investigation and Response
Olga Angelopoulou, Paula Thomas, Konstantinos Xynos and Theodore Tryfonas
oangelop@glam.ac.uk, pthomas@glam.ac.uk, kxynos@glam.ac.uk, ttryfona@glam.ac.uk
Information Security Research Group
Faculty of Advanced Technology
University of Glamorgan
CF37 1DL Pontypridd
United Kingdom

Abstract
ID theft, especially in its on-line form, is currently one of the most prevalent types of computer crime. The limited end-user awareness as well as the retention and business processing of large amounts of personal data in a manner that does not meet security and regulatory requirements provide plenty of opportunities to fraudsters. A number of organisations have produced guidelines of good practice targeted to individuals and organisations, however the matter is still on the rise. In this paper we review computer-based techniques employed by fraudsters in order to steal IDs and refer to published guidelines and the documented good practice against those. We discuss the issues related to the investigation of such incidents and provide the grounds for the development of a framework to assist in their forensic examination.

Keywords
e-Crime, ID theft, incident investigation, digital evidence, computer forensics

Introduction
According to a study of the Identity Theft Resource Center (2003), ID theft is distinguished in three forms: financial, criminal and identity cloning. The study takes as examples real victims, and drawing upon these cases those three forms are defined. Ultimate purposes for ID theft could be either financial and other resource and privilege gains or protection of one’s real identity and masquerading behind another, mostly legitimate entity. ID thefts can also take advantage of an organisation’s good name in order to attract individuals and hence then there is a case of a double ID theft, the corporation’s and the consumer’s (Dwan, 2004).

Identity theft can occur in many forms, for example, by lost or stolen wallets, discarded documents containing personal details, phishing e-mails etc. According to The Identity Theft Resource Center (2003), students, old people and the military appear to be more vulnerable to ID theft than any other group of people. By the time the end user has found out that they
have been a victim of identity theft, is already too late and their personal details have been
used for fraudulent purposes (Dwan, 2004). It also seems that most perpetrators of this kind
of crime are not alone, but rather organised and well equipped. Indeed, ID Theft is nowadays
directly linked to drug trafficking, money laundering and terrorism (Collins, 2003).

Based on the U.S. Federal Trade Commission's report for National and State Trends in Fraud
and Identity Theft 2004 of the 635,173 complaints received, 246,570 were ID theft reports.
The most common form of reported identity theft was Credit Card fraud, followed by phone or
utilities fraud, bank fraud, and employment fraud. It is very important to note that only 30% of
victims notified a police department. It can therefore be assumed that the majority of people
are not aware that they could have contacted law enforcement agencies and prefer not to
make their ID theft incident known.

In 1999 20,000 cases of ID Theft were reported in the UK, in 2001 there were 53,000 and in
2003 the number had almost doubled. It can take a victim up to 300 hours of work when
dealing with the consequences of their ID theft with banks and credit card companies (Porter,
2004). This emerging and developing trend in crime triggers complex investigations that
require extensive use of information technology, both as a medium for analysis and as
evidence at the same time. Fraudsters are obtaining more sophisticated technological ways
and manage to conceal their crimes.

For example, in ID theft cases for financial purposes, the investigator can first focus on credit
history, transactions made on the victim’s name, applications for bank accounts, loans and
credit cards. This evidence trail is to be recovered in the form of data, logs etc. formats
through various systems within one or even multiple financial organisations. As a result, the
investigation is complicated and time-consuming. With identity-related ID theft cases, the
investigator will need to consider not only the financial evidence but the personal information
gained, subsequent actions triggered by a hijacked identity etc.

In this paper we discuss how ID theft can occur in the interconnected world and what
evidence may be left behind for the computer forensic investigator. We intend to provide an
initial insight into this computer-fuelled crime in order to facilitate the analyst in identifying and
analysing the related digital evidence.

ID Theft Techniques and Digital Evidence

Techniques and tools of identity thieves

Information can be obtained from stolen wallets or handbags which usually contain
identification papers, driving licences, credit and bank cards, etc. Alternatively, someone’s
personal mail might be stolen to gain bank and credit card statements, pre-approved credit
offers and tax information. The techniques used to collect this information include searching
through household litter bags, burglary, social engineering or even identification of a
deceased person.

The identity theft criminals may contact a person who has lost his credit card claiming that
they found it, ask for personal details and then use it in a fraudulent manner (Dwan, 2004).
They may apply for a new credit card using someone else’s personal details, buy items they
never pay for and the offence will be against the legitimate owner. They might even bankrupt
on someone’s account or give stolen personal details in case of an arrest (Federal Trade
Commission, 2003).

High-tech techniques for ID theft require the use of a computer, and usually the Internet, in
order to gain the required information. The techniques that are used require at least
intermediate information technology knowledge and skills and the most common techniques
are detailed below.

Phishing

Phishing is used to gain personal information by sending e-mail messages that appear to
come from trusted organisations. A Phishing attack takes the form of a mass distribution of
'spoofed' e-mail messages in which the reply addresses, links, and branding appear to come
from banks, insurance agencies, retailers or credit card companies. The messages look
authentic by using corporate logos and formats similar to those that are used by the official companies. The threat is perceivably dangerous when personal information is requested for auditing or verification purposes, for example, personal account numbers, passwords and other private information. In April 2004, an unemployed 21 year old British man was arrested by the UK National Hi-tech Crime Unit, allegedly for a phishing attack against The Co-operative bank and targeting the Smile Internet Bank. However this man was just an amateur and according to the police he is not related with the organised crime (news article ‘Police Catch UK Phisher’, 2004).

Web-spoofing

Web Spoofing is the method by which the users believe that they have been directed to the official website of a company. Instead, they have actually been directed to a ‘spoofed’ website where any personal information that is entered, will be stored and used for malicious purposes. The web pages will have been designed by skilled web designers and are often an exact copy of the original company’s website. The important difference is that there are minor changes that allow for user information to be stored on the fraudster’s servers.

Malicious software: Spyware, Viruses and Trojans

Spyware is designed for exploiting infected computers usually for marketing purposes. The activity of the web browser is monitored, resulting to routing of HTTP requests to the websites that are advertised through the spyware. Also, pop-up advertisements are can be delivered or theft of personal information can be achieved, including users’ financial information. Recently, spyware was used by an identity theft ring to retrieve and store remotely, user information. This was identified by research conducted by an anti-spyware firm, Sunbelt (Vijayan, 2005).

Some Trojan Horses are security-breakers that have the ability to steal passwords and personal details and forward them through a number of ways to the fraudsters. Smart Trojan software can keep a log from keystrokes (key-loggers) or takes a screenshot when a customer is visiting a financial web-site and the information is then forwarded to the fraudster (news item ‘Exit old fashion phishing […], 2005).

Biometrics circumvention

Biometrics was supposed to be a countermeasure for Identity Theft. Even though it is a relatively new method for identity verification and the aim is to replace the vulnerable passwords, there are already numerous ways of the fraudsters to dump a biometric system. It can be easy to deceive biometric technology by tampering machines that read biometric data or altering the records that are contained within them. Finger prints that are left behind on scanners can be re-used by breathing on the glass, cooling down the sensors to give false information, using graphite powder to dust the fingerprint and then copy it to a “jelly finger” etc. Facial recognition can also be duped in some cases by playing someone’s video at the reader and gaining access to a system (Hamadi, 2004).

Other Techniques

Other techniques, not discussed in further detail here as we focus on on-line ID theft, may include card cloning (Gerard et al., 2004), attacks on off-line kept data (e.g. back-up copies and disaster recovery facilities) or data media in general (McKinley, 2004) and use of CCTV footage etc.

Forensic Investigation of On-line ID Theft

Identity Theft in its on-line form is considered as a relatively new method of fraud and there is not enough guidance for forensic investigators. The investigator will have to unfold the digital trail of evidence and try to present potential explanations of how such a crime occurred. This digital trail involves examining how a crime was committed using computers and the Internet. The investigation should identify how the leak of personal information occurred that made it possible to conduct a misuse of resources such as a credit card number. It should also
include details of the misuse such as dates, goods purchased and amounts spent. If it is possible the perpetrator should also be identified. The latter is perhaps one of the most challenging tasks as, unlike DNA evidence, computer records can identify user accounts that are logically, not physically, linked to individuals (Tryfonas et al., 2006).

Forensic extraction and analysis of data from a computer hard disk will detail much of this information. However, the conversion of data to evidence is a lengthy and costly process that, at the end of the process, has also to be made understandable to a jury. Therefore, there would be value in creating an analytical framework to facilitate the investigation of Internet Identity Theft cases and the handling of the related digital evidence. The construction of a formalised and structured approach that would assist the computer forensic investigative practice in terms of identification of evidence, presentation in a court of Law etc. presents an opportunity for further research.

Towards such a direction, in Table 1 we have combined the types of threats against on-line identities and the means to achieve illegitimate gains (or simple masquerade through ID theft) in a systematic analytical framework. We try to identify and record the digital evidence that may be found per category. Other factors of concern for an investigation are also recorded, such as required skills and capability profile of the perpetrator etc. Forensics professionals can then refer to this when they have to examine a case concerning internet identity theft. The main idea is that the professional is able to identify and understand the crime scene through such a framework.

ID Theft Response - Detection and Prevention

According to the Federal Trade Commission (FTC, 2005) the majority of people discovered they were victims by monitoring their accounts. However, it is only fifty per cent of the victims that finally find out how thieves retrieved their personal data (DeMarrais, 2003). The majority of ID theft incidents in the UK can be traced back to a suspicious phone call (Edwards, 2005). This fact alone raises concerns about communication of individuals’ personal information and the precautions that are required when such an exchange is needed. Further to precautions on releasing personal information to not trusted sources, both individuals and organisation have to be suspicious of the ways personal data can be stolen and used for malicious reasons. According to the FTC, individuals should order a copy of their credit report from credit card bureaus in order to check whether the information held there is accurate. Personal information at home should be held in a secure place and individuals should be informed about who has access to their personal information in the workplace.

From an organisational point of view, the security community has now accepted that in organisations a major security threat against information comes from inside. Research has proved that 70% of the total identity thefts start from employees who steal personal data from the company they work for (Hinde, 2004). The majority of companies cannot cope with well organised attacks coming from internal sources, or even instances of an employee giving out information unintentionally (Porter, 2004). Hence, in the light of the rising figures of on-line ID theft, the protection of personal information of clients and other affiliates held by organisations is much more than a compliance issue. Indeed, the same FTC survey shows that $48 billion loss was of businesses and financial institutions comparing to $5 billion loss of the consumers (DeMarrais, 2003). Therefore, organisations need to become more active on how they detect and prevent ID theft. Regulatory compliance with the Data Protection Act is then a very important issue in a company’s security architecture agenda and its information security and privacy policy.

The detection controls comprise authorisation, internal auditing and whistleblower hotlines that alert the employees of the company about a committed or potential fraud underway. From a technological perspective automated detection systems that process large volumes of transaction data and look to highlight any suspicious actions based on specific patterns should be used (Porter, 2004). In addition to monitoring business information for external instances of ID theft, there is also the need to protect corporate information with references to identification and related information from the threat from

---

1 For Table 1, see Appendix C
within. In order to prevent such internal instances of identity theft, personal information held inside the company should be treated with the appropriate confidentiality. Information assets that contain such personal and sensitive information should be protected in terms of allowed access (Solomon et al., 2003) and destruction/disposal of those electronic or paper-based records (Gerard et al., 2004).

The most common measure for protecting unauthorised access to a computer network is to use passwords. However, problems arise when users choose easily guessed words for a password. In addition, they should change their secret password regularly in order to avoid any problems (Gerard et al., 2004). File encryption is commonly used as most database software packages provide built-in encryption and decryption of data. In addition, hardware or software firewalls have a wide use and are necessary in any company to limit the risk of intrusion to its network. Access logs should be kept for those files that contain personal and private data. Internal auditors of the company should have the authorisation to analyse and evaluate these audit records (Gerard et al., 2004).

Conclusions and Further Research

Hardly is ID theft or a simple masquerade a new crime; however it is now fuelled by information technology resulting in high numbers of such crimes committed annually, corporate liabilities and financial loss – and of course personal inconvenience. As ID fraudsters have discovered new tools, so must forensic investigators and Law practitioners in order to be able to cope with this trend and tackle it effectively. A responsive plan should include components of prevention and detection, reaction and investigation of incidents.

However, whilst prevention and reaction can be largely covered within the organisation’s security architecture plans, given an emphasis in meaningful compliance with regulations such as the Data Protection Act, detection and investigation require new tools and methods. Through such a perspective, we try to initiate a framework for the investigation of this crime, by recording artefacts of evidential value and creating suspect profiles against potential instances of hi-tech ID theft. Such a systematic approach to explaining ID theft will hopefully facilitate the understanding of the crime scene by the forensic investigator.

Table 1 is an initial attempt to address this issue and it demonstrates how a categorisation of ID theft incidents against the method used, the required skills behind the attack, the technologies exploited and the potential digital evidence left behind can provide an investigative insight. Potential future work would include a detailed categorisation of the majority of known ID theft attacks (or a meaningful, representative grouping of those), a detailed recording of potential evidence in the corresponding crime scenes, guidance on how to locate and extract these artefacts in an evidentially sound manner etc. A review of secondary empirical data from published cases and public court proceedings may also complement or cross-validate this approach.

References and Relevant Sources


Conference Research Papers


ID Theft: A Computer Forensics’ Investigation
Framework

Olga Angelopoulou
University of Glamorgan
oangelop@glam.ac.uk

Abstract
The exposure of online identities grows rapidly nowadays and so does the threat of having even more impersonated identities. Internet users provide their private information on multiple web-based agents for a number of reasons, online shopping, memberships, social networking, and many others. However, the number of ID Theft victims grows as well, resulting to the growth of the number of incidents that require computer forensics investigation in order to resolve this type of crime. For this reason, it appears of value to provide a systematic approach for the computer forensics investigators aiming to resolve such type of computer based ID Theft incidents. The issues that demand individual examinations of this type of crime are discussed and the plan of an ID Theft computer forensics investigation framework is presented.

Keywords
ID theft, incident investigation, digital evidence, computer forensics, computer crime, computer forensic investigator

INTRODUCTION
According to the Credit Industry Fraud Avoidance System (CIFAS) (2007), the UK’s Fraud Prevention Service, in 2006 alone 80,000 cases of ID Theft were recorded, comparing to 9000 cases in 1999. It appears as the wide use and the anonymity occurring on the Internet has influenced a number of people proceeding to Internet related, non-legitimate actions.

This is a global problem. ID Theft is considered as a standalone crime since 1998 in the United States as defined in the Identity Theft and Assumption Deterrence Act (1998) and belongs to federal crimes, where the establishment of the Offence is made as follows:

“knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.”

In the H. R. 2622, Fair and Accurate Credit Transactions Act of 2003, the American Identity Theft legislation provides the state approach of combating ID Theft and protecting the consumers. Based on the U.S. Federal Trade Commission’s (FTC) report for National and State Trends in Fraud and Identity Theft 2004, of the 635,173 complaints received, 246,570 were ID Theft reports. The most common form of reported ID Theft was Credit Card fraud, followed by phone or utilities fraud, bank and employment fraud. It is very important to note that only 30% of victims notified a police department. It can therefore be assumed that the majority of people are either not aware that they could have contacted law enforcement agencies or prefer not to make their ID theft incident known.

In plain words, the intention and plan of the person who decides to steal someone’s identity, the ID Thief, is to collect the more personal details the possible for the person he’s interested in, attempt to use this information for the largest personal gain of his and finally continue his life under someone else’s name. It seems that the popular saying ‘there is no perfect crime’ is not taken seriously from some individuals. However, the world’s history has proved that no matter the precautions and strategies followed to combat a crime regardless its nature, the fraudsters will discover a way to conduct it. Under no circumstances should people give up the effort of eliminating a type of crime, nevertheless there should be also invented radical and innovative ways of discovering and uncovering evidence of those already taken place.
Based on the above unfolds the rationale of this paper presenting a piece of under development work. The first aim is to provide some insight of the basic terms, ID Theft and Digital Evidence and their sequence in order to lead to the successful computer forensics investigation. The issues concerning the importance of such an individual approach of ID Theft incidents towards Computer Crime are discussed; the design of the proposed ID Theft Investigation Framework is presented and defended by an example.

**ID THEFT AND THE DIGITAL EVIDENCE**

The fraudulent use of another’s personal details has become an increasingly significant concern. One out of ten people in Britain was a victim of online fraud during 2006 revealed a survey, corresponding to 3.5 million British internet users (unknown, 2007). Attacks on financial institutions have risen from 39% in 2003 to 83% for 2004 (McKenna, 2004).

The Home Office (2006) defines Identity Theft as:

> “Criminals can find out your personal details and use them to open bank accounts and get credit cards, loans, state benefits and documents such as passports and driving licenses in your name.”

Identity theft (ID Theft) can be perpetrated in a number of ways. Discarded documents containing personal details can provide a rich source of personal information. Simple forms of deception can also be used to extract the information from the victim an example would be an attacker poses as a legitimate government official or business person collecting personal data door to door. Other methods include the so called ‘brute force’ techniques such as the stealing of wallets and purses containing identification and credit and bank cards or the removal of personal documents during a burglary. In particular stolen mail, where the perpetrator may have access to bank and credit card statements, pre-approved credit offers, checks and tax information, can be used to gather information for an ID Theft. This may be followed up by social engineering. The perpetrator contacts the person who has lost his card claiming that they found it, asks for personal details and then uses this information fraudulently (Dwan, 2004).

However, personal identity is increasingly being stored and used in a range of digital forms. This can leave individuals exposed to possible threats as a result. Examples include; Phishing e-mails, web spoofing and numerous other techniques. This emerging and developing trend in crime can result in complex investigations that involve information technology, both as a medium for analysis and as evidence at the same time. Fraudsters are obtaining more sophisticated technological ways and manage to conceal their crimes.

The following table summarises all different methods by which ID Theft is performed, separated in offline and online:

<table>
<thead>
<tr>
<th>Offline Techniques</th>
<th>Online Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stolen wallets or bags</td>
<td>Phishing</td>
</tr>
<tr>
<td>Stolen mail</td>
<td>Pharming</td>
</tr>
<tr>
<td>Deceased people</td>
<td>Web-Spoofing</td>
</tr>
<tr>
<td>Dumpster diving</td>
<td>Social Engineering</td>
</tr>
<tr>
<td>Burglars</td>
<td>Card Cloning</td>
</tr>
<tr>
<td>Shoulder surfing</td>
<td>Storage Devices and Media</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Biometrics</td>
</tr>
<tr>
<td></td>
<td>Malicious Software</td>
</tr>
<tr>
<td></td>
<td>Key-logger</td>
</tr>
<tr>
<td></td>
<td>CCTV Cameras</td>
</tr>
<tr>
<td></td>
<td>Data Retrieval</td>
</tr>
</tbody>
</table>

Table 146: Summary of offline and online ID Theft Techniques

Digital evidence is any kind of digitally processed information that is stored in any sort of digital media. The data strengthens or neglects the assumption of an electronic crime in the terms of the
investigation process. It can be therefore presented as supportive proof in a court of law. (Carrier B., 2006)

In the late 20th century Dr. Edmund Locard, director of Lyons Institute of Forensic Medicine, defined an important theorem for the foundation of the forensic science that is widely known as the Locard Exchange Principle:

“Any action of an individual, and obviously, the violent action constituting a crime, cannot occur without leaving a mark. What is admirable is the variety of these marks. Sometimes they will be prints, sometimes simple traces, and sometimes stains” (Chisum W., J., and Turvey B.E. (2006) from Locard, 1934).

The theorem has been transformed and misinterpreted during the years aiming to cover the science needs (Chisum, Tervey, 2006). The simplest form that can be found in literature is “with contact between two items, there will be an exchange” (Thornton, 1997). Casey (2003) has noted that this fact holds true in the digital world as a digital exchange between two devices results in an exchange of information. For example a request to view a web page from a client may be logged on the server and the web page, if downloaded, may then reside temporarily on the client.

As stated from Marcella and Greenfield (2002), computer forensics demands accurate evidence and results of the investigation. For this reason, the use of state of the art equipment and methods should be used in order to reassure it. The world of Computer Forensics is dealing with a number of situations from industrial espionage to damage assessment and holds back to the beginning of the 1980s. Nevertheless, the last few years have made it widely known to the public and demand even more expertise. It is by nature a science that requires detail by all means and there is where the handling of the digital evidence should be based.

THE “SOLITARY” OF ID THEFT TOWARDS COMPUTER CRIME INCIDENTS

Initially, it is worth mentioning some issues concerning computer crime in general. Those types of crime where a computer or any other electronic device is involved in order to perform the crime or as the target of it are considered as computer crimes (Postnote Computer Crime, 2006). The criminals become more and more sophisticated nowadays and attempt to use technology by any means in order to avoid detection and perform the crime in greater detail and excess deception. A simple glance on news articles enhances the anxiety to information security people and the need to eliminate the problem. However, this could only happen on a virtual world as the use of computers and online transactions becomes only wider, giving the fraudsters’ the chance to increase their ways of attacking systems.

Computer crime involves different types of offences as hacking, copyright, child pornography, fraud, viruses, and harassment. They can be categorised in different ways, according to the methods used in order to prevent them. Icove et al. (1995) in Computer Crime classify them with this approach, grouping them in:

- Physical security breaches
- Personnel security breaches
- Communications and data security breaches
- Operations security breaches

Each security breach involves several fraudster actions that lead to computer crime. Hence, computer crime as a general matter can be treated based on the facts and the incidents that surround it. This basically requires treating computer crimes independently, in order to achieve a more analytical and in depth examination of a case. The investigation process time will be accelerated as the investigator will be able to follow specific steps once the type of the crime is revealed and he will be able to track on a certain process.

Concerning the current research, the digital investigation of computer based ID Theft is a computer crime that requires the expertise of a computer forensic investigator in order to be resolved. The digital evidence that comes into sight after the analysis of a related to crime computer misuse is of critical value as it should be efficient to accuse someone with a crime or not. Therefore, the manipulation of the evidential data should be treated sensibly and with sensitivity.
As described in a number of existing published sources, ID Theft is besides considered as a major threat for individuals and corporations and consists of multiple types of crime. It involves multiple ways of achieving it, either by the aid of technology or not. This is the major difference from other types of computer crime and the way the digital evidence should be treated.

In view of this influence, for the function of science, it could be considered that all technology aided evidential elements will be represented with the term ‘online’, whereas all non-technology aided will be called ‘offline’. Consequently, the investigator has to take into consideration the volume of the offline sources that influence the outcome of the investigation, as a number of offline techniques could have been used to commit the crime. A characteristic example of this issue could be the offence of hacking. In such a case, the actual evidence will be hidden inside the suspect’s computer, as the hacker’s only weapon is that; and the assigned to the incident investigator will have to trace all evidential data from there. At the same time, in a computer-based ID Theft incident the investigator’s findings depend on the fraudster’s computer, in addition other sources, such as a card cloning machine and forged documents could enhance the evidence. However, this is not the purpose of the computer forensics investigator, but still differentiates this type of crime from any other computer related and raises the need of treating this type of computer crime in an individual manner.

Based on FTC’s Identity Theft Data Clearinghouse (2007), ID Theft was established as the top complaint category in consumer fraud with 36 percent. Therefore, in order to support the need of treating a computer crime as an independent entity, an example of an ID Theft case for financial purposes can be considered, where the investigator can first focus on credit history, transactions made on the victim’s name, applications for bank accounts, loans and credit cards. This evidence trail is to be recovered in the form of data, logs etc. formats through various systems within one or even multiple financial organisations. As a result, the investigation is complicated and time-consuming. With identity-related ID Theft cases, the investigator will need to consider not only the financial evidence but the personal information gained, subsequent actions triggered by a hijacked identity etc.

The difficulty the investigators need to face when dealing with an ID Theft incident and what really makes this type of crime individually-treated is that they actually have to face two investigative categories; victim or perpetrator. This is where all starts, as the need to distinguish and separate the investigation process is going to differentiate such a detailed process from others. A victim’s machine should provide such evidential data that will be able to prove the fraud against the computer user, while on the perpetrator’s machine the evidential data should be treated in such a way that will reveal the deception’s proof. One might argue that the existing computer forensic investigation frameworks can cover this argument. However, a generic guideline cannot reach to a far detailed phase of the investigative process as it aims to cover all different types of computer related crimes. In respect to the existing computer forensic frameworks and based on the substantial increment of ID Theft the need to aid the computer forensic investigation of this type of crime leads to the point that the investigation process needs to be focused on a different perspective each time as different sort of evidence is required.

Figure 1: The different aspects of evidence concerning ID Theft incidents
People who work at this field need to be able to use constructive methods in order to facilitate their actual aim that is to provide evidential data after a computer forensic investigation. The threat of becoming an ID Theft victim becomes even greater day by day for everyone, especially those who use the Internet by any mean, make transactions, socialize, interact, anything that someone could take part on through it. Simply because the use of Internet and the public dependency will only grow, there should be invented and developed efficient ways that could cope with this rapidly spreading threat.

The following sections are going to support the above arguments on a practical approach, describing the theoretical procedure of designing and implementing such a computer forensics investigation framework.

**DESIGN DESCRIPTION**

There is the need at this stage to describe ‘why’ and ‘how’ the foundation of this work is set. For this reason, the following paragraphs are going to set the principles of this work.

The fact is that in order to accomplish a comprehensive and structured investigation about a computer forensic case, the steps followed should be of extreme diligence. The procedure that is followed should give an answer to the question of what information might be stolen and how this information could be stolen. The major aim is to collect the data that give evidence and can prove a possible attack. Only after a detailed and constructed approach the data analysis can return and verify the only premise that might appear in the beginning of the research; that the investigator has to deal with an ID Theft case.

Fundamentally, a framework is considered as tool to aid in planning, monitoring and evaluation of research projects (Carrier, 2006). The general investigation scientific method presented by Carrier and Spafford at the DFRWS 2006 though, structures a checklist of high-level phases on a theoretical foundation in order to propose and describe a procedure in a digital investigation research field. The phases have been applied on existing frameworks and demonstrate an accurate approach to the specific area of research. These include:

- **Observation**, where the researcher needs to observe the field in order to create a clear picture about the processes and the activities that take place on the investigation.
- **Hypothesis Formulation**, where the researcher focuses on the results of the observation phase and is able to categorise the techniques that will aid the analysis of the findings.
- **Prediction**, this phase will support the Hypothesis Formulation as the results of this part will prove whether or not the Hypothesis is formed on a constructed basis and will lead the researcher to the last phase.
- **Testing and Searching**, where the tests and experiments that take place on a generally approved manner will probably result to new predictions and evaluate the Hypothesis the researcher has set.

The procedure described should give answers to questions for the existence of an x file to a y event and should be responded accurately only after a successful analysis of the data. The investigator should be able to have access and examine each one of them, every file and any event that influences the file’s behaviour.

**ID THEFT INVESTIGATION FRAMEWORK DESIGN**

For the ID Theft Investigation Framework the research of the existing literature has revealed that the most suitable approach would be first to identify and define the phases that will lead the researcher to the appropriate procedures, based on the model described above and consequently the implementation of a conceptual framework that will aid the forensic investigator. The idea is based on the concept of handing over the procedure on a fundamental basis. This way the process will correspond to any possible procedure during the investigation. The presented process is adjusted to the needs that an ID Theft incident investigation requires as it is going to be analysed on the following chapter. The phases at the first level of the process follow a generic pattern. However, in the advance of the process the model will reveal the second level phases that contain the processes of the framework and the third level phases, including the activities that tae place. Every Phase is influenced by the inputs and the outputs (I/Os) that resign it.

Therefore, the study should be distinguished in four phases, where every phase represents a major procedure throughout the ID Theft investigation lifecycle. The impact on every phase is featured from
all influential actions taken place on each phase. This states the first level of the framework’s formulation.

According to the procedure that is proposed to guide the researcher in order to formulate the investigation process, the above graph outlines the first level of it. There is always one start and one end point concerning the investigation. The forensic analyst needs to begin under a concrete method and finish so. Hence, the Media Analysis (Observation) is the phase that appears of extreme importance in order to provide the data that will prolong to the Evidence Analysis (Hypothesis Formulation). The findings of the disk analysis will move forwards to the analysis and the decision whether this evidence can stand as accurate to the Scenario Construction (Prediction), where it is going to validate or not the Evidence Analysis. However, the analyst should always be able to return from the Evidence Analysis to the Media Analysis for any further data that might appear of value during the examination of the media, as well as he should always be able to revisit the Evidence Analysis at any stage in the Scenario Construction for any information that could emerge and indicate further investigation. Then, the Scenario Construction will need to be evaluated in order to prove its validation that is going to direct to the end of the process. However, the Evaluation phase requires the possibility to recall any of the previous phases of the investigation process in order to prove the objectivity of the research outcome. The following table sets the Variable Names at this Phase of the process in order to be used during this level of the procedure.

<table>
<thead>
<tr>
<th>Description</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Investigation</td>
<td>I</td>
</tr>
<tr>
<td>Media Analysis</td>
<td>Pma</td>
</tr>
<tr>
<td>Evidence Analysis</td>
<td>Pea</td>
</tr>
<tr>
<td>Scenario Construction</td>
<td>Psc</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Pe</td>
</tr>
</tbody>
</table>

Table 2: First Level Investigation Process Variable Names
A graphical representation demonstrates the process that is proposed to be followed from the ID Theft Investigation Framework concerning an Incident.

![Graph 2: Incident Investigation Process Lifecycle](image)

Every phase at this level of the investigation process needs to respond to an input and an output (I/O) practice. This provides the necessity of defining the processes and the activities that will be set for the further analysis of this research. The I/Os support the general process in the terms of continuity during the investigation’s lifecycle. Below, there is a graphical representation of every phase in correspondence with the First Level I/Os that manipulate it. Every phase of the process requires as an input the output of the preceding phase for supporting the coherence of the research outcome.

**Media Analysis**

The Pma requires as an input any type of Digital storage Media that could give as an output possible ID Theft data in order for the further investigation to take place. At this point the term Digital Media is going to represent any type of computer storage device.

![Graph 3: Phase 1. Media Analysis I/Os](image)

**Possible Digital storage media**

<table>
<thead>
<tr>
<th>Media</th>
<th>Possible Digital storage media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer / Laptop / Server Hard Disk</td>
<td>PCMCIA cards</td>
</tr>
<tr>
<td>External Hard Disk</td>
<td>Memory Cards</td>
</tr>
<tr>
<td>Mobile Phone / SIM Card</td>
<td>USB Memory Stick</td>
</tr>
<tr>
<td>Raid Hard Disks</td>
<td>PDA</td>
</tr>
<tr>
<td>Tape Back-ups</td>
<td>Floppy Disk</td>
</tr>
<tr>
<td>CD / DVD</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3: Possible Digital storage Media**
Evidence Analysis

The Pea takes as input the possible ID Theft data provided by the Pma and will try to convert it to Evidence. At any time during an investigation further data may significantly come into view and the analyst will return to the previous phase for the analysis of the Digital Media.

Graph 4: Phase 2. Evidence Analysis I/Os

Scenario Construction

The input of the Psc should be anything else but the Evidence from the Pea aiming to produce a Scenario as an output. The scenario is the ‘story’ that is created by the investigator based on the findings of the media examination. Only when the required information is gathered, the analyst is able to present a coherent and efficient chronicle of the evidence. The reconstructed story of what has taken place to the original media. At this Phase it may be required for the analyst to search for further details on the two previous phases.

Graph 5: Phase 3. Scenario Construction I/O
Evaluation

The Pe uses the Scenario from the Psc as an input in order to present the Case that is also the required output of the whole investigation. At this stage the Media Analysis will be either proved or disproved. However, the analyst needs to be able to revisit all previous Phases for the validation of the research outcome.

First Level Investigative Process

Phase 1. Media Analysis

Process 1.1. Digital Media
    Activity 1.1.1. Source Identification
    Activity 1.1.2. Digital Media collection
    Activity 1.1.3. Copy/image the source

Process 1.2. ID Theft Data
    Activity 1.2.1. Evidential data identification
        a Victim
        b Fraudster
    Activity 1.2.2. Target identification
    Activity 1.2.3. Threat agent identification/intention

Phase 2. Evidence Analysis

Process 2.1. ID Theft Data
    Activity 2.1.1. Data Analysis
    Activity 2.1.2. Target Analysis
        a Victim
        b Fraudster
    Activity 2.1.3. Threat Agent Analysis

Process 2.2. Evidence
    Activity 2.2.1. Evidence Collection
    Activity 2.2.2. Evidence Classification

Phase 3. Scenario Construction

Process 3.1. Evidence
    Activity 3.1.1. Structure of evidential data
    Activity 3.1.2. Structure threat agent’s profile
        a Victim
        b Fraudster
    Activity 3.1.3. Structure analysed digital evidence

Process 3.2. Scenario
    Activity 3.2.1. Scenario Outline
    Activity 3.2.2. Scenario Preparation Documentation

Graph 6: Phase 4. Evaluation I/O

On a theoretical basis the Investigation Process obtains the following instruction format that is going to be analysed in detail on the analysis chapter. Each phase, the processes (I/Os) and the activities of the first level of the investigation framework are list numbered in order to create a logical continuation. By progressing the activities at this level of the procedure appear, where the separation of the framework in two parts comes into sight, the victim’s and the perpetrator’s that are going to lead to the second level of the Investigation Process.
EXAMPLE FICTIONAL SCENARIO

Assuming there is a computer hard disk delivered to a computer forensics lab from a major company suspecting an employee for computer misuse, but without any further details. Consequently, this is going to be the first attempt to apply the above described first level framework, in an incident that the analyst is not provided with any further information.

In such a case, and for Phase 1 of the investigation process, the investigator receives the input of the Process 1.1 that needs to collect (Activity 1.1.1), identify (Activity 1.1.2) and image (Activity 1.1.3) the hard disk. The output process of this Phase is the 1.2, where for the needs of this example is ID Theft Data or even data that could stand as ID Theft evidence and this is what the investigator is challenged to discover. The Activity 1.2.1 reveals the first element, whether the evidence belongs to a victim or a fraudster. From this point the investigation process on a lower level framework should progress under a bipolar perspective according to the data provided from 1.2.1. However, for this example it can easily give the first glance charging the employee as a fraudster committing ID Theft from his work computer, including every instance of it, inside the company or towards outside targets. His machine could also state him as a victim of ID Theft, meaning that the company has probably got information leak to the outside. There is when Activity 1.2.2 identifies the target, that could be a vulnerable system, or information published on the public domain, as well as the Activity 1.2.3 where the threat agent and his intentions can be identified.

Phase 2, aims to analyse the evidence from the original media on Process 2.1, the investigator analyses the ID Theft data under three Activities 2.1.1, 2.1.2 and 2.1.3, data, target and threat agent accordingly. The target analysis activity is divided to victim and fraudster, as the inputs for each category are different and guide the investigation towards different perspective. In case the employee has been a victim, the investigator will be able to analyse the target from this side, if the employee was the fraudster perhaps the investigator will be able to collect more details about the target. Therefore, the Process 2.2 provides the evidence with the Activities 2.2.1 that collects the evidence and 2.2.2, where the evidence is classified.

Phase 3 constructs the scenario of the incident. At this point, Process 3.1 is the evidence extracted from the investigation, where Activity 3.1.1 structures the evidential data, while 3.1.2 structure the threat agent’s profile that is divided to the victim’s and the fraudster’s side, as there is going to be different sort of data gathered to give the investigator the information required to construct the attacker’s profile. Activity 3.1.3 structures the analysed digital evidence that refers to the incident as a whole. In such a manner, on Process 3.2 the activities that follow are 3.2.1, the scenario outline and 3.2.2, the documentation preparation. At this point the investigator has a clear aspect about his suspect. He could tell with structured evidence whether the suspected employee has committed ID Theft or has only been another victim.

However, he owes to continue with Phase 4, the evaluation of the scenario. So, on Process 4.1 that is the scenario, Activity 4.1.1 is followed, evaluates or not the scenario assumption and 4.2.2 clarifies the scenario. Process 4.2 leaves the investigator with a case where he needs to construct it (Activity 4.2.1), clarify it (Activity 4.2.2) and evaluate it (Activity 4.2.3). The last Activity 4.2.4 for the investigator is the evidential case representation, the computer forensic report, where all evidence will be described and could also stand in a court of law, charging the fraudster of the case that could be either the victim or not.
CONCLUSION:

When someone who can describe his relation with computers and the Internet as professional or even as advanced user, reaches to the point that feels insecure and suspicious with the interaction with them, then it obviously appears that the situation requires some attention. The statistics prove that the ID Theft is a type of old fashioned crime that transformed into a Cybercrime because of the intense ‘investment’ of online sources. There may be more ‘bad’ people in the world than good ones and the spur of committing the perfect crime that will never be revealed still runs in some people’s minds.

This situation leads to the improvement of tools and popularity of studying and research in computer forensics the last few years. It is the type of science that corresponds to the needs of digital investigations. Therefore for the conditions where ID Theft is combined with computer usage, computer forensics is the type of science that will be requested to provide the evidence. In such a perspective, there should be an effort to provide the computer forensic analysts with more detailed and concrete procedures that will help them accomplish their target.

For this reason, with respect and based on the computer forensics frameworks aiming to aid digital investigations, there is an approach of investigating ID Theft incidents with an independent investigation methodology. The ID Theft investigation framework distinguishes the examination in the victim’s and the fraudster’s side and the first level of this investigation process analysis was hence presented. This type of investigation method aims to provide results on a more focused basis regarding an ID Theft incident. Future work includes a more detailed approach to the findings of the investigation process based on the evidence left behind on a fraudster’s digital storage media and the victim’s accordingly. An experimental assessment on fictional cases by analysing reliable, residual data from hard disk drives will validate the research; and that will be accomplished in two parts, where the researcher behaves as the perpetrator in a closed network attack in the laboratory, and where the researcher uses the evidence that is left behind (from the first experiment) and acts as a forensic examiner, analysing the hypothetical victims’ hard disk drives.

REFERENCES:


An empirical methodology derived from the analysis of information remaining on second hand hard disks.

Grigoris Fragkos1, Vivienne Mee1, Konstantinos Xynos1, Olga Angelopoulou1
1Information Security Research Group
University of Glamorgan,
CF37 1DL, Wales, UK
{gfragkos, vmmee, kxynos, oangelop}@glam.ac.uk

Abstract. In this paper we present the findings of an analysis of approximately 260 second hand disks that was conducted in 2006. A third party organisation bought the disks from the second hand market providing a degree of anonymity. This paper will demonstrate the quantitative outcomes of the analysis and the overall experiences. It will look at how analysts can expand their tools and techniques in order to achieve faster results, how one can organise the analysis based on the way information is found and finally a holistic picture of the case should be generated following the proposed methodology.

Keywords: disk analysis, second hand disks, corporate data, computer forensic analysis, Forensic Race

1 Introduction

During 2006 we organised a research initiative on the analysis of residual data on second hand hard disks. In this respect a number of hard disks where studied in order to identify and understand the data that can be revealed from randomly purchased hard disks from a number of different countries. The sample countries/regions included the U.K., Germany and North America.

It is vital to be aware of the importance and utilisation of a disk study for the computer forensics science [1]. The researcher gains awareness concerning end-user and corporate knowledge regarding data exposure. Unaware users can become victims of espionage and blackmail. By analysing disks that contain any personal data for research reasons the possibility of espionage is prevented, while on the other hand people that hear about this study get informed about the way their data can be retrieved and used for malicious reasons. Therefore, from the researcher’s point of view, potential criminal activity can be identified where sensitive data is available and can be used for such purposes.

The overall number of disks analysed lead to results that should be considered further, such as statistical reports concerning the users’ familiarity with techniques like wiping data from their hard disks and thus securing their privacy when disposing of disks. In any case that data is left behind in hard disks there is a fraud risk for the user. Consequently, the capacity of personal information revealed can even lead to Identity Theft by thoroughly profiling the victim, as there were multiple cases where personal identification details could be retrieved.

This disk study signifies issues not only for the research community, but for the general user awareness as well. Further to discussing those issues based on our experience of taking part in this disk study, in this paper we propose a methodology that could be implemented in order to simplify and manage a disk study research procedure.

2 Forensic Race

As a result of the disk study, a new terminology, “Forensic Race” was brought about. The word race differentiates the species from one kind to the other. Consequently, the term “Forensic Race” determines the race of a computer’s hard disk or any type of digital data repository. The “Forensic Race” of a hard disk is based on a hard disk’s capacity, operating system and in combination with the nature of the data contained within the disk drive.

In the disk study, it was found that the majority of the disks were between 500 Mega Bytes and 10 Giga Bytes with an overwhelming 69 per cent (see Fig 1). From the disk’s capacity it is possible to assume approximately the year from which it was manufactured. This, most likely can then lead the analyst to a simple deduction that the Operating System would be from around that period. This was validated
since the majority of the systems contained old Operating Systems (e.g., MS Dos, MS. Windows 98, NT, 2000 and ME).

As a result of the ‘Forensic Race’ term, an investigator could predict the approximate time period required. During an analysis, the size of the disks and the amount of information stored on them contributes to this variable. The majority of the disks had low capacity therefore the time period took for each one to be investigated was substantial. This is not always holds true since the demand to store more and larger files requires larger hard disks. Consequently, future disk studies will consist of disks that will have massive capacity. Therefore, the investigation will demand a time management schedule in order to contact the analysis in a reasonable period of time.

With the time factor in mind, it is very helpful, from an investigators point of view, to have an idea of the race of the disks you are dealing with in advance. Thus, it is makes sense to know is you are dealing with a Dwarf or a Gnome or if you are dealing with a Cyclops or a Giant (see Table 1). What one wouldn’t want to deal with is a Black Giant.

Table 1. Classification sample of a disk’s Forensic Race

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Giant</td>
<td>Large Capacity – Vast amount of data present</td>
</tr>
<tr>
<td>Cyclops</td>
<td>Large Capacity – Very few data present</td>
</tr>
<tr>
<td>Dwarf</td>
<td>Low Capacity – Vast amount of data present</td>
</tr>
<tr>
<td>Gnome</td>
<td>Low Capacity – Very few data present</td>
</tr>
<tr>
<td>Blue</td>
<td>Corporate data present</td>
</tr>
<tr>
<td>Green</td>
<td>Individual data present</td>
</tr>
<tr>
<td>Black</td>
<td>Illicit Material</td>
</tr>
</tbody>
</table>

A hard disk can be classed as a Cyclops, as a Dwarf, as Gnome etc.

- **The Cyclops** is a hard disk that has a large capacity that even a one eye person could easily see that it contains almost no data and definitely no illicit material.
- **On the contrary, a Dwarf** is a small capacity hard disk that contains a vast amount of data that would take days to investigate. The disks classify themselves according the data they do contain.
- **A Gnome** is a small capacity hard disk that contains a small amount of legitimate data.

It is possible to expand the list of the Forensic Race categories depending on how detailed the investigator would like to categorise findings of an investigation.

### 3 A proposal for an empirical approach
The methodology of computer forensics investigation calls out for a more empirical approach. Instead of just following an out of the book procedure, while investigating a case, the consideration of past experience along with an empirical approach could lead to a far more efficient analysis. The required experience and knowledge to deal efficiently with the vast amount of information contained within the disks, has been developed through the investigation of a series of data repositories in the past. However, the time allocated for the analysis was 3 months for approximately 260 disks. Within that
time the disks had to be imaged, recovered, data carved, cross referenced with existing data or data already recovered from other disks, characterise and categorise the nature of the data recovered. After completing the disk study [2] [1] the need for a more flexible methodology was raised. The investigators felt that they shouldn’t arrange the disks to be analysed based on their criteria but let the disks decide which one it is going to be investigated in what order.

The Table 2 represents the total number of disks provided and how this number went down by excluding disks that matched certain criteria.

<table>
<thead>
<tr>
<th>Disk Category</th>
<th>Excluding List</th>
<th>Total Number of Disks</th>
<th>Excluding List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faulty / Unreadable</td>
<td>124</td>
<td>259</td>
<td></td>
</tr>
<tr>
<td>Wiped</td>
<td>70</td>
<td>135</td>
<td></td>
</tr>
<tr>
<td>Handed to the police</td>
<td>4</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>61</td>
<td></td>
</tr>
</tbody>
</table>

Comparing the total numbers of disk provided (259) with the number of the disks that has been actual investigated (61) it is clearly that the only the 1/4 (23.5%) of the disks were processed (see Table 2).

The proposed methodology tries to generate an informative table that will provide with some internal information of how a disk study should start and in which order to be conducted.

1. Start by excluding the faulty disks, this is the easiest part. Indisputably, these are the one that cannot be imaged due to physical damage and need special equipment or resources in order to be investigated.

2. An automated procedure that checks for wiped drives that contain no data is the second step of the methodology.

3. The third step is more complex and advanced than the previous steps. It involves four different applications which will sift through the date on the disk images.
   - The first application will try to locate (within the present data) and/or recover (deleted) any pictures (photographs, image files) of any type. By examining the different headers and footers of various image files, the application can extract full or partial known image file types. Researchers form the Information Research Group (ISRG) within the University of Glamorgan conceived the idea and developed a program which proves that this is possible.
   - The second application will extract all the thumb.db files by locating them or recovering them from the slack space. Then a smart application goes through the thumb.db files and extracts all the pictures stored in them. The special case with the thumb.db file is that it stores forever (until wiped) a backup preview version of the user’s pictures even if they have been deleted or even wiped. Furthermore, a small preview of a picture is more likely to be found when stored with others in one single file, than trying to recover the large version of a picture spread across the hard disk and most possibly been overwritten in various parts. Researchers from the Information Security Research Group (ISRG) within the University of Glamorgan have also conceived this idea and have developed a program [3] which proves that this is possible. Recently, a tool called Vinetto [7] was released that extracts pictures and generates reports too.
   - The third application extracts the directory names form the index.dat file(s) (see Fig. 2) and tries to locate/recover the contents. This is where the Operating System (OS) is caching the user’s activity. The conceived idea that extracts the thumb.db files was slightly modified to extract the contents (directory names and URLs) of the index.dat files.
   - Last but not least, the fourth application that tries to extract the registry file of the user. Further investigation in the registry can reveal a vast amount of information if needed that could totally end up profiling the user. Information such as software installed, hardware installed, user’s Internet activity and habits can all be retrieved from the Registry alone [4].

Once these four steps have been completed, the informative table of internal information gives the investigator a brief overview of what the investigation is going to entail, and which disks have priority over others for further analysis.
3.1 Further details about the methodology
By having a collection of the pictures contained into the disk it is fairly easy to identify potential illicit material within the hard disk. Thus, in a very small period of time the pictures will do their best to help the investigators identify disks that has to be reported to the police immediately. Especially with the MS Windows® OS, a list of the original files that are shipped with the Operating System can be produced. For every MS Windows® distribution a list of MD5 hashes of each file can be generated. Thus, during the investigating process, a number of approximately 50,000 files (depends the distribution) can be excluded from the processing cycles of the investigation’s procedure. Additionally, this will also minimise the successful hits returned when searching keywords by focusing at the unknown for the system files which however are the user’s data.

The registry file contains many secrets that are waiting to be revealed. A quick search through specific locations in the registry, if this is possible of course, could reveal the origins of the disk. The company name used to register software, the computer name, the type of installed programs, quick list of URLs visited; network shares and previously connected devices provide a good chance to the investigator to identify if the data present belong to some kind of company, to some individual as home user or both (see Table 3).

Table 3. Origin of disks investigated

<table>
<thead>
<tr>
<th>Disks Investigated</th>
<th>Commercial Data Present</th>
<th>Individual data present</th>
</tr>
</thead>
<tbody>
<tr>
<td>65</td>
<td>37</td>
<td>28</td>
</tr>
</tbody>
</table>

4 Advantages of the proposed methodology
Taking under consideration all this information revealed by the automated process and by having in mind the idea of how to classify the “Forensic Race” of a disk. It is fairly possible to start organising the investigation according to the estimated time that has to be spent on each case. The approximate idea of which disk contains what kind data can easily lead us to start with the larger in capacity disks that seems to contain a lot of corporate data and continue with the smaller in capacity disks that also seems to contain data from companies. That way we can leave all the disks that seem to contain data about individuals for the end of the investigation. Additionally, large disk that have been identified to contain very few data can be also left for the end of the investigation. Finally, disks that seem to have been originated from the same source (i.e. same company) can be grouped together from the beginning of the investigation despite their capacity.

By checking the time spend for each disk to be investigated in a random order to the overall time spend to complete the disk study one could see that the overall timeframe could be minimised. There have been disks that were only 6 GB in capacity and took ten times more time to investigate than disks that where double in size. Having an approximate idea of how long could take you to investigate a disk can be really helpful while organising such large scale projects.

- Disks that were found to belong to a specific group (i.e. from the same individual or the same company) should be crossed referenced every time new data were identified. Another example would be disks that have foreign origin.
- It is also very convenient to know from the beginning that you have to deal with a number of disks in different foreign languages. Consequently, these disks will be allocated to the proper people in order to perform the investigation in that foreign language. Otherwise in the middle of a study could end up trying to find a translator.
4.1 Providing some examples

The process of extracting information from the thumb.db files and index.dat files is similar.

The character C is the 81st byte of the file

URL | 100 | [Address]

Fig. 3. Pattern of extracting the web addresses

There are numerous locations by which information can be extracted to give an analyst a further understanding of what data is present on the disk. As mentioned before it is possible to get usernames, company names and a user’s internet activity all just solely from the Registry. Mee et al [5] have given some examples of what and where this information can be extracted from the Registry. The following tables summarises these examples illustrating the keys which hold the information.

<table>
<thead>
<tr>
<th>Root Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_CURRENT_USER</td>
<td>Current logged-on user data</td>
</tr>
<tr>
<td>HKEY_USERS</td>
<td>Data about all the user accounts on the machine</td>
</tr>
<tr>
<td>HKEY_CLASSES_ROOT</td>
<td>File association and Object Linking and Embedding (OLE) registration information</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE</td>
<td>System related information</td>
</tr>
<tr>
<td>HKEY_DYN_DATA</td>
<td>Performance data</td>
</tr>
<tr>
<td>HKEY_CURRENT_CONFIG</td>
<td>Information about the current hardware profile</td>
</tr>
</tbody>
</table>
Table 5. System information which can be extracted

<table>
<thead>
<tr>
<th>Registry Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\Hardware\Description\System\CentralProcessor\0\ProcessorNameString</td>
<td>Name of the processor that the system is running</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\Hardware\Description\System\system</td>
<td>BIOS that the machine is running the BIOS date of both the video BIOS and the system BIOS.</td>
</tr>
</tbody>
</table>

Table 6. Illustrates sample locations in the registry whereby Software related information can be extracted

<table>
<thead>
<tr>
<th>Registry Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion key</td>
<td>Operating system installed, its service pack, system default path, and the registered owner can also be found in this Registry root key</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion key \CSDVersion</td>
<td>Service pack name that has been installed</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion key \Winlogon</td>
<td>Can be set to allow a user to automatically log onto the system, whenever the system boots</td>
</tr>
</tbody>
</table>

Table 7. Illustrates sample information related to specifically to users in which can be extracted from the Registry

<table>
<thead>
<tr>
<th>Registry Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Profile List</td>
<td>Lists all current and deleted users that has access to the machine, identified by their SID.</td>
</tr>
<tr>
<td>HKEY_USERS\SID\Software\Microsoft\Internet Explorer\TypedURLs</td>
<td>Stores all the typed URLs that the user typed into Internet Explorer</td>
</tr>
<tr>
<td>HKEY_USERS\SID\Software\Microsoft\MSNMessenger\PerPassportSettings\</td>
<td>Gives information about the location of the default path for received files for the user’s MSN Messenger software</td>
</tr>
<tr>
<td>HKEY_USERS\SID\Software\Microsoft\Messenger Service\ListCache\Net Messenger Service</td>
<td>Holds the entire user’s MSN contact list</td>
</tr>
<tr>
<td>HKEY_USERS\SID\Software\Microsoft\SearchAssistant\ACMru\5683</td>
<td>User’s recent searches in Windows</td>
</tr>
</tbody>
</table>

5 Conclusions
The proposed methodology of this paper is based on experience. Simple forensic applications could easily help the investigators to organise their study in advance when dealing with unknown quantities of data to be analysed. We believe that in the near future a system could be build that will be able to perform all the steps presented here automatically. Consequently, computer forensics investigators will be able to deal with a large number of high capacity disks in an efficient way.

5.1 Acknowledgements
Completing a disk study of approximately 260 disks is not a trivial task. Firstly, we would like to thank Dr. Andy Jones, Dr. Craig Valli, Dr. Iain Sutherland, Dr. Andrew Blyth, Paula Thomas for providing the disks and organising the disk study. In addition we would like to express our appreciation to our colleagues’ researchers within the ISRG for the team effort to finish the disk study on time. Which include: Theodore Tryfonas, Michael Pilgernmann, Stilianos Vidalis, Huw Read, and Abdulrazzaq Al-Murjan. Last but not least, Vivienne Mee would like to acknowledge the support of EPSRC and DSTL.

References
On-line ID Theft Techniques, Investigation and Response

Olga Angelopoulou, Paula Thomas, Konstantinos Xynos and Theodore Tryfonas
oangelop@glam.ac.uk, pthomas@glam.ac.uk, kxynos@glam.ac.uk, ttryfona@glam.ac.uk

Information Security Research Group
School of Computing
University of Glamorgan
CF37 1DL Pontypridd
United Kingdom

Abstract

ID theft, especially in its on-line form, is currently one of the most prevalent types of computer crime. The limited end-user awareness as well as the retention and business processing of large amounts of personal data in a manner that does not meet security and regulatory requirements provide plenty of opportunities to fraudsters. A number of organisations have produced guidelines of good practice targeted to individuals and organisations, however the matter is still on the rise. In this paper we review computer-based techniques employed by fraudsters in order to steal IDs and refer to published guidelines and the documented good practice against those. We discuss the issues related to the investigation of such incidents and provide the grounds for the development of a framework to assist in their forensic examination.

Keywords

e-Crime, ID theft, incident investigation, digital evidence, computer forensics

Introduction

According to a study of the Identity Theft Resource Center (2003), ID theft is distinguished in three forms: financial, criminal and identity cloning. The study takes as examples real victims, and drawing upon these cases those three forms are defined. Ultimate purposes for ID theft could be either financial and other resource and privilege gains or protection of one’s real identity and masquerading behind another, mostly legitimate entity. ID thefts can also take advantage of an organisation’s good name in order to attract individuals and hence then there is a case of a double ID theft, the corporation’s and the consumer’s (Dwan, 2004).

Identity theft can occur in many forms, for example, by lost or stolen wallets, discarded documents containing personal details, phishing e-mails etc. According to The Identity Theft Resource Center (2003), students, old people and the military appear to be more vulnerable to ID theft than any other group of people. By the time the end user has found out that they have been a victim of identity theft, is already too late and their personal details have been used for fraudulent purposes (Dwan, 2004). It also seems that most perpetrators of this kind of crime are not alone, but rather organised and well equipped. Indeed, ID Theft is nowadays directly linked to drug trafficking, money laundering and terrorism (Collins, 2003).

Based on the U.S. Federal Trade Commission’s report for National and State Trends in Fraud and Identity Theft 2004 of the 635,173 complaints received, 246,570 were ID theft reports. The most common form of reported identity theft was Credit Card fraud, followed by phone or utilities fraud, bank fraud, and employment fraud. It is very important to note that only 30% of victims notified a police department. It can therefore be assumed that the majority of people are not aware that they could have contacted law enforcement agencies and prefer not to make their ID theft incident known.

In 1999 20,000 cases of ID Theft were reported in the UK, in 2001 there were 53,000 and in 2003 the number had almost doubled. It can take a victim up to 300 hours of work when dealing with the consequences of their ID theft with banks and credit card companies (Porter, 2004). This emerging and developing trend in crime triggers complex investigations that require extensive use of information technology, both as a medium for analysis and as evidence at the same time. Fraudsters are obtaining more sophisticated technological ways and manage to conceal their crimes.
For example, in ID theft cases for financial purposes, the investigator can first focus on credit history, transactions made on the victim’s name, applications for bank accounts, loans and credit cards. This evidence trail is to be recovered in the form of data, logs etc. formats through various systems within one or even multiple financial organisations. As a result, the investigation is complicated and time-consuming. With identity-related ID theft cases, the investigator will need to consider not only the financial evidence but the personal information gained, subsequent actions triggered by a hijacked identity etc.

In this paper we discuss how ID theft can occur in the interconnected world and what evidence may be left behind for the computer forensic investigator. We intend to provide an initial insight into this computer-fuelled crime in order to facilitate the analyst in identifying and analysing the related digital evidence.

ID Theft Techniques and Digital Evidence

Techniques and tools of identity thieves

Information can be obtained from stolen wallets or handbags which usually contain identification papers, driving licences, credit and bank cards, etc. Alternatively, someone’s personal mail might be stolen to gain bank and credit card statements, pre-approved credit offers and tax information. The techniques used to collect this information include searching through household litter bags, burglary, social engineering or even identification of a deceased person.

The identity theft criminals may contact a person who has lost his credit card claiming that they found it, ask for personal details and then use it in a fraudulent manner (Dwan, 2004). They may apply for a new credit card using someone else’s personal details, buy items they never pay for and the offence will be against the legitimate owner. They might even bankrupt on someone’s account or give stolen personal details in case of an arrest (Federal Trade Commission, 2003).

High-tech techniques for ID theft require the use of a computer, and usually the Internet, in order to gain the required information. The techniques that are used require at least intermediate information technology knowledge and skills and the most common techniques are detailed below.

Phishing

Phishing is used to gain personal information by sending e-mail messages that appear to come from trusted organisations. A Phishing attack takes the form of a mass distribution of ‘spoofed’ e-mail messages in which the reply addresses, links, and branding appear to come from banks, insurance agencies, retailers or credit card companies. The messages look authentic by using corporate logos and formats similar to those that are used by the official companies. The threat is perceivably dangerous when personal information is requested for auditing or verification purposes, for example, personal account numbers, passwords and other private information. In April 2004, an unemployed 21 year old British man was arrested by the UK National Hi-tech Crime Unit, allegedly for a phishing attack against The Co-operative bank and targeting the Smile Internet Bank. However this man was just an amateur and according to the police he is not related with the organised crime (news article ‘Police Catch UK Phisher’, 2004).

Web-spoofing

Web Spoofing is the method by which the users believe that they have been directed to the official website of a company. Instead, they have actually been directed to a ‘spoofed’ website where any personal information that is entered, will be stored and used for malicious purposes. The web pages will have been designed by skilled web designers and are often an exact copy of the original company’s website. The important difference is that there are minor changes that allow for user information to be stored on the fraudster’s servers.

Malicious software: Spyware, Viruses and Trojans

Spyware is designed for exploiting infected computers usually for marketing purposes. The activity of the web browser is monitored, resulting to routing of HTTP requests to the web sites that are advertised
through the spyware. Also, pop-up advertisements are can be delivered or theft of personal information can be achieved, including users’ financial information. Recently, spyware was used by an identity theft ring to retrieve and store remotely, user information. This was identified by research conducted by an anti-spyware firm, Sunbelt (Vijayan, 2005).

Some Trojan Horses are security-breakers that have the ability to steal passwords and personal details and forward them through a number of ways to the fraudsters. Smart Trojan software can keep a log from keystrokes (key-loggers) or takes a screenshot when a customer is visiting a financial web-site and the information is then forwarded to the fraudster (news item ‘Exit old fashion phishing[…]’, 2005).

Biometrics circumvention

Biometrics was supposed to be a countermeasure for Identity Theft. Even though it is a relatively new method for identity verification and the aim is to replace the vulnerable passwords, there are already numerous ways of the fraudsters to dump a biometric system. It can be easy to deceive biometric technology by tampering machines that read biometric data or altering the records that are contained within them. Finger prints that are left behind on scanners can be re-used by breathing on the glass, cooling down the sensors to give false information, using graphite powder to dust the fingerprint and then copy it to a “jelly finger” etc. Facial recognition can also be duped in some cases by playing someone’s video at the reader and gaining access to a system (Hamadi, 2004).

Other Techniques

Other techniques, not discussed in further detail here as we focus on on-line ID theft, may include card cloning (Gerard et al., 2004), attacks on off-line kept data (e.g. back-up copies and disaster recovery facilities) or data media in general (McKinley, 2004) and use of CCTV footage etc.

Forensic Investigation of On-line ID Theft

Identity Theft in its on-line form is considered as a relatively new method of fraud and there is not enough guidance for forensic investigators. The investigator will have to unfold the digital trail of evidence and try to present potential explanations of how such a crime occurred. This digital trail involves examining how a crime was committed using computers and the Internet. The investigation should identify how the leak of personal information occurred that made it possible to conduct a misuse of resources such as a credit card number. It should also include details of the misuse such as dates, goods purchased and amounts spent. If it is possible the perpetrator should also be identified. The latter is perhaps one of the most challenging tasks as, unlike DNA evidence, computer records can identify user accounts that are logically, not physically, linked to individuals (Tryfonas et al., 2006).

Forensic extraction and analysis of data from a computer hard disk will detail much of this information. However, the conversion of data to evidence is a lengthy and costly process that, at the end of the process, has also to be made understandable to a jury. Therefore, there would be value in creating an analytical framework to facilitate the investigation of Internet Identity Theft cases and the handling of the related digital evidence. The construction of a formalised and structured approach that would assist the computer forensic investigative practice in terms of identification of evidence, presentation in a court of Law etc. presents an opportunity for further research.

Towards such a direction, in Table 1 we have combined the types of threats against on-line identities and the means to achieve illegitimate gains (or simple masquerade through ID theft) in a systematic analytical framework. We try to identify and record the digital evidence that may be found per category. Other factors of concern for an investigation are also recorded, such as required skills and capability profile of the perpetrator etc. Forensics professionals can then refer to this when they have to examine a case concerning internet identity theft. The main idea is that the professional is able to identify and understand the crime scene through such a framework.

1 For Table 1, see Appendix C
ID Theft Response - Detection and Prevention

According to the Federal Trade Commission (FTC, 2005) the majority of people discovered they were victims by monitoring their accounts. However, it is only fifty per cent of the victims that finally find out how thieves retrieved their personal data (DeMarrais, 2003). The majority of ID theft incidents in the UK can be traced back to a suspicious phone call (Edwards, 2005). This fact alone raises concerns about communication of individuals’ personal information and the precautions that are required when such an exchange is needed. Further to precautions on releasing personal information to not trusted sources, both individuals and organisation have to be suspicious of the ways personal data can be stolen and used for malicious reasons. According to the FTC, individuals should order a copy of their credit report from credit card bureaus in order to check whether the information held there is accurate. Personal information at home should be held in a secure place and individuals should be informed about who has access to their personal information in the workplace.

From an organisational point of view, the security community has now accepted that in organisations a major security threat against information comes from inside. Research has proved that 70% of the total identity thefts start from employees who steal personal data from the company they work for (Hinde, 2004). The majority of companies cannot cope with well organised attacks coming from internal sources, or even instances of an employee giving out information unintentionally (Porter, 2004). Hence, in the light of the rising figures of on-line ID theft, the protection of personal information of clients and other affiliates held by organisations is much more than a compliance issue. Indeed, the same FTC survey shows that $48 billion loss was of businesses and financial institutions comparing to $5 billion loss of the consumers (DeMarrais, 2003). Therefore, organisations need to become more active on how they detect and prevent ID theft. Regulatory compliance with the Data Protection Act is then a very important issue in a company’s security architecture agenda and its information security and privacy policy.

The detection controls comprise authorisation, internal auditing and whistleblower hotlines that alert the employees of the company about a committed or potential fraud underway. From a technological perspective automated detection systems that process large volumes of transaction data and look to highlight any suspicious actions based on specific patterns should be used (Porter, 2004). In addition to monitoring business information for external instances of ID theft, there is also the need to protect corporate information with references to identification and related information from the threat from within. In order to prevent such internal instances of identity theft, personal information held inside the company should be treated with the appropriate confidentiality. Information assets that contain such personal and sensitive information should be protected in terms of allowed access (Solomon et al., 2003) and destruction/disposal of those electronic or paper-based records (Gerard et al., 2004).

The most common measure for protecting unauthorised access to a computer network is to use passwords. However, problems arise when users choose easily guessed words for a password. In addition, they should change their secret password regularly in order to avoid any problems (Gerard et al., 2004). File encryption is commonly used as most database software packages provide built-in encryption and decryption of data. In addition, hardware or software firewalls have a wide use and are necessary in any company to limit the risk of intrusion to its network. Access logs should be kept for those files that contain personal and private data. Internal auditors of the company should have the authorisation to analyse and evaluate these audit records (Gerard et al., 2004).

Conclusions and Further Research

Hardly is ID theft or a simple masquerade a new crime; however it is now fuelled by information technology resulting in high numbers of such crimes committed annually, corporate liabilities and financial loss – and of course personal inconvenience. As ID fraudsters have discovered new tools, so must forensic investigators and Law practitioners in order to be able to cope with this trend and tackle it effectively. A responsive plan should include components of prevention and detection, reaction and investigation of incidents.
However, whilst prevention and reaction can be largely covered within the organisation’s security architecture plans, given an emphasis in meaningful compliance with regulations such as the Data Protection Act, detection and investigation require new tools and methods. Through such a perspective, we try to initiate a framework for the investigation of this crime, by recording artefacts of evidential value and creating suspect profiles against potential instances of hi-tech ID theft. Such a systematic approach to explaining ID theft will hopefully facilitate the understanding of the crime scene by the forensic investigator.

Table 1 is an initial attempt to address this issue and it demonstrates how a categorisation of ID theft incidents against the method used, the required skills behind the attack, the technologies exploited and the potential digital evidence left behind can provide an investigative insight. Potential future work would include a detailed categorisation of the majority of known ID theft attacks (or a meaningful, representative grouping of those), a detailed recording of potential evidence in the corresponding crime scenes, guidance on how to locate and extract these artefacts in an evidentially sound manner etc. A review of secondary empirical data from published cases and public court proceedings may also complement or cross-validate this approach.

References and Relevant Sources


Appendices


Appendix C:

A categorisation of computer-based ID theft techniques

The associated attackers’ profiles and the potential digital evidence left on the crime scene

<table>
<thead>
<tr>
<th>ID Theft Technique</th>
<th>Attacker’s Profile</th>
<th>Methods / Tools</th>
<th>Technology</th>
<th>Characteristics</th>
<th>Popularity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phishing</strong></td>
<td>To gain/get:</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bank Accounts</td>
<td></td>
<td>Official e-mail or web site claim</td>
<td>No use of port 80, mainly use of port 4903</td>
<td>Growing very fast, about 56% per month (R. Lininger et al, 2005)</td>
</tr>
<tr>
<td></td>
<td>• Cheque Books</td>
<td></td>
<td>• Unsecured wireless mediums</td>
<td>• e-mails - image map or with encoded URL in JavaScript</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Credit Cards</td>
<td></td>
<td>• Unregistered domains</td>
<td>• Respond to “SHS” web server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Loans</td>
<td></td>
<td>• Key-loggers</td>
<td>• Run on “zombie” machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Financial account hijacking</td>
<td></td>
<td>• HTTP requests routing</td>
<td>• Trojan code hits exploitable machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pop-up windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• URL cloning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Trojan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Key-loggers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pop-up windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• URL cloning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Trojan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Key-loggers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pop-up windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• URL cloning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Trojan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Key-loggers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pop-up windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• URL cloning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Trojan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Key-loggers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web-spoofing:**
The method that the users believe they are on a website that actually they aren’t.

<table>
<thead>
<tr>
<th>ID Theft Technique</th>
<th>Attacker’s Profile</th>
<th>Methods / Tools</th>
<th>Technology</th>
<th>Characteristics</th>
<th>Popularity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spyware, Viruses and Trojans</strong></td>
<td>• Infect a computer to gain access to personal information</td>
<td>High and Very Technical</td>
<td>Programming software</td>
<td>Malicious code</td>
<td>Growing as most users can get convinced</td>
</tr>
<tr>
<td></td>
<td>• To retrieve financial information</td>
<td></td>
<td></td>
<td>• Pop-up windows</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Infected web sites</td>
<td></td>
</tr>
</tbody>
</table>

**Motivation**

- To gain/get:
  - Bank Accounts
  - Cheque Books
  - Credit Cards
  - Loans
  - Financial account hijacking

**Skills**

- High
- Considered to belong on organised crime

**Methods / Tools**

- Official e-mail or web site claim
- Unsecured wireless mediums
- Unregistered domains

**Technology**

- Graphics
- Pop-up windows
- URL cloning
- Trojan
- Key-loggers

**Characteristics**

- No use of port 80, mainly use of port 4903
- e-mails - image map or with encoded URL in JavaScript
- Respond to “SHS” web server
- Run on “zombie” machines
- Trojan code hits exploitable machines

**Web-spoofing:**

- Store personal information
- Use passwords and personal details for malicious reasons

**Skills**

- High
- Redirection to the fraudster’s web site

**Methods / Tools**

- Web servers
- Web page design software
- Domain name registration

**Technology**

- URL rewriting

**Characteristics**

- Professionally designed web pages
- Copied web pages linked to the original
- Information is redirected and stored to the fraudster’s server
- Respond to “SHS” web server

**Spyware, Viruses and Trojans:**

- Malicious software that can gain access on a system and infect it.

**Skills**

- High and Very Technical
- The fraudster needs to have high standard programming skills

**Methods / Tools**

- Programming software
- Malicious code
- Pop-up windows
- Infected web sites

**Technology**

- HTTP requests routing
- Monitored web browser activity, network traffic, e-mail, clipboard contents, keystrokes

**Characteristics**

- Growing at an alarming rate and considered as an explosion in privacy issues.
<table>
<thead>
<tr>
<th>Key Loggers:</th>
<th>Medium to Technical</th>
<th>Biometrics circumvention:</th>
<th>Data Retrieval:</th>
<th>Storage Devices and Media:</th>
<th>PDA’s, Mobile Phones and Bluetooth:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking personal data a user may enter. Can be hardware or software. Software key loggers belong to spyware.</td>
<td>To track data entered on a computer</td>
<td>Biometrics at the first stage was supposed to fight Identity Theft as a countermeasure for not duplicating a human identity, however there are already numerous ways of the fraudsters to dump a biometric system.</td>
<td>To gain/ get:</td>
<td>Hard Disks, USB Sticks, Floppy Disks and C.D.’s, as well as stolen computers are a source for stealing personal data.</td>
<td>The wide use of PDAs, Mobile Phones and Bluetooth is a matter of deception for retrieving personal data.</td>
</tr>
<tr>
<td>• Track data entered on a computer</td>
<td>• Physical presence of the fraudster required in order to install the hardware key logger</td>
<td>• Physical access to such devices</td>
<td>• Simple extraction of copying files</td>
<td>• Acquire address book</td>
<td>• Acquire address book</td>
</tr>
<tr>
<td>• To have access on personal information</td>
<td>• Installation of the software, even remotely</td>
<td>• Physical access is transformed to digitized</td>
<td>• Forensic extraction software</td>
<td>• Retrieve personal details stored (even photos)</td>
<td>• Retrieval of personal information</td>
</tr>
<tr>
<td>• To retrieve financial information</td>
<td>• Software can be installed as part of another software</td>
<td>• Security breaches</td>
<td>• Only basic knowledge of how to extract data</td>
<td>• Gain complete access on the device</td>
<td>• Technical, None when the device is stolen</td>
</tr>
<tr>
<td>• Software key loggers belong to spyware.</td>
<td>• Hardware key loggers are invisible</td>
<td>• Access to public shared information</td>
<td>• Computers stolen, discarded or sold information.</td>
<td>• PDAs and Mobile phones can be treated also as storage devices:</td>
<td>• Knowledge on how to extract data</td>
</tr>
<tr>
<td>• Key logger software code can be downloaded free</td>
<td>• Key logger software code can be downloaded free</td>
<td>• E-mail messages</td>
<td>• Simple extraction and copying of the files</td>
<td>• Simple extraction and copying of the files</td>
<td>• Bluetooth technology is still unsecure</td>
</tr>
<tr>
<td>• Physical presence of the fraudster required in order to install the hardware key logger</td>
<td>• Specific applications are targeted and others are ignored</td>
<td>• Logs/Internet activity</td>
<td>• Forensic extraction software</td>
<td>• Forensic extraction software</td>
<td>• Stolen PDAs and mobile phones</td>
</tr>
</tbody>
</table>

**Growing at an alarming rate**

**Static, however the ID Theft interest on this subject is expected to grow**

**Growing as the demand for storage devices grows**

**Growing as more and more personal information is published on Internet**
### Card Cloning:
A very important part of Identity Thieves’ work. Card Cloning needs a person with basic technical skills in order to manipulate a card replication machine and reproduce credit cards.

- **To replicate bank account cards, credit cards**
- **Low to Basic Technical**
  The fraudster should know how to process the card replicate machine
- **Skimming devices**
- **Card replication machines**
- **Appropriate computer software**
- **Card reader**
- **Compromised ATM**
- **Tampered ATM machines**
- **Fraudsters own card replication equipment**

### Social Engineering:
The method used for retrieving personal information from someone by claiming to be another person.

- **To gain/get:**
  - Bank Accounts details
  - Passwords
  - Personal information
- **Conspiracy**
  The fraudster only needs to convince the victim
- **Official e-mail claim**
- **Official phone call claim**
- **E-mail**
- **Graphics**
- **Influence the victim’s psychology**
- **Co-operation with the victim**
- **Legitimate-look e-mail messages**

### CCTV / Wireless Cameras:
CCTV can be monitoring the behaviour of a person, even following his steps. Often the motive is a PIN Number collection and for this reason widely used on ATM machines from fraudsters.

- **How a person behaves**
  - States how the thief should then behave
- **Medium to Low**
  The fraudster should know how to process
- **Camera operation**
- **Knowledge of filming and processing video**
- **Camera hardware**
- **Video processing software**
- **Video Tapes**
- **Expensive camera equipment**
- **Unofficially installed cameras**

Growing as the use of cameras extends
Review of preventing internal ID Theft

All paper documents that contain sensitive information in a company should be protected by being accessed only by authorised employees in designated areas as well as computer printers and fax machines should also be accessed in controlled areas (Solomon et al., 2003). The records that are no longer necessary for a company to maintain should be very carefully treated when destroying them. The corporation should follow three principles in order to avoid any unauthorised access to its data. First, there should be a plan of how these documents are going to be destroyed and second, consistency of what is going to be destroyed. Specific schedule should be followed and data should be destructed on the same manner. Third, documentation should be kept and maintained for a period of time about data that have been obliterated. (Gerard G. J., et al., 2004)

Any electronic data storage medium in an organisation should be controlled, and these devices should be tracked from the time they are part of the organisation’s property until the moment they are disposed. Anyone who is related with computer forensics understands the reason. There is a way to retrieve information from a hard disk to a memory stick. Therefore, company’s sensitive data should not be found unprotected. (Gerard G. J., et al., 2004)

The most common measure for protecting unauthorised access to a computer network is to use passwords. However, problems arise when users choose easily guessed words for a password. In an ideal world a password should be combination of letters, numbers and special characters, with not exact words and the employees have to keep in mind that they should never let anyone know their password. In addition, they should change their secret password from time to time in order to avoid any leak. (Gerard G. J., et al., 2004)

Databases with encrypted files can also store information that concerns data that should not be revealed and add security to the company’s data. File encryption is commonly used in many organisations as most of database software packages provide built-in encryption and decryption of data. In addition, firewalls either hardware or software have a wide use and are necessary in any company to limit the risk of intrusion to its network. However, they are not considered as “unbeatable” and hackers quite often manage to force an entry. Even though, a firewall can monitor a) network traffic in case an intruder tries to have access to the network, b) changes to files by hackers and c) access log files that can be evidence in case someone has forced into the network. Furthermore, access logs should be kept for those files that contain personal and private data. This way, the organisation can audit the files that have been accessed and preceded by an employee in order to avoid security threats. Internal auditors of the company will have the authorisation to analyse and evaluate these records. (Gerard G. J., et al., 2004)

A very important issue in a company’s secure function is to compose an information security and privacy policy. The actual purpose of designing a policy for a computer system is to decrease the risks that can appear on it. During the performance of a risk analysis to a system it is easy for the administration to identify the vulnerabilities the system might be exposed. As long as computer networks may appear weaknesses due
to illegal use, each individual should be responsible for his actions that concern his access to the system and should respect the terms of using it. In addition the company should “invest” on insurance concerning cyberspace. Many insurance companies provide it and a firm can be compensated in case of proved loss due to ID Theft. (Gerard G.J., et al., 2004)

The Method of Phishing

Phishing has the form of an official e-mail claiming to come from an online bank or retailer, because in fact is a scam that steals personal information. The danger that arises from these e-mails is that they actually look legitimate, sometimes even more professional than the organisation’s site. Phishers use graphics, pop-up windows or even URLs identical with the official organisations’. The present situation is exposed even to the involvement of Trojans and key loggers in these e-mail messages. In addition, experts believe that organised crime is behind Phishing attacks. (Malim, 2004) The life of a Phishing web site on the Internet is average 4.0 days, according to an Anti-Phishing Working Group (2006) investigation. However, based on their latest report, the longest time online for a site is 30 days.

On summer 2003 the U.S. Federal Bureau of Investigators (FBI), announced about Phishing that is the: “hottest, and most troubling, new scam on the Internet.” Many financial organisations have been Phishing targets since then, for instance eBay, Natwest Bank, Paypal, Citibank and a number of others. The major problem caused by these Phishing attacks is the loss of reliance customers’ show towards the security a financial institution can provide them, which means more loss of money for the banks.

NatWest Bank had to set up and maintain a telephone number for customer service in the period the web site was shut down; however many customers felt disappointed (Hinde, 2004). Citibank on the other hand, informs the customers about the situation and advises them how to protect themselves, mainly by sending them warning messages. However, banks support that even if they take protection measures, nothing is going to be achieved when the customers are not aware of the situation. In addition there is a group of banks that meet in order to find enhanced ways for addressing the problem. As safety measure, they scan the Internet for direct abuse of their brand, expecting better software protection from browsers as well. (McKenna, 2004)

Phishing and Countermeasures

Based on Tuliani (2004), the threat of Phishing won’t be prevented easily. The industry will introduce stronger user authentication as a countermeasure to Phishing. A simple way for succeeding this would be the use of one-time passwords, provided either by a text message on a mobile phone or by USB tokens, valid only for one use and then expire. Such methods are not widely, because of a number of restrictions, including the user unawareness and the cost.

In addition, a number of different Anti-Phishing tools have been implemented aiming to prevent the user entering a phishing web site and eventually eliminate the amount
of incidents. However, it appears that the tools alone cannot the answer to the problem. (Zhang et al. (2007), Downs et al. (2006))

Anatomy of a Phishing e-mail

In this section, an existing Phishing e-mail is going to be analysed, so that the actual techniques used by the fraudsters can be presented and identified. The e-mail examined, is a well designed PayPal Phishing scam that on a first glance looks legitimate and well constructed. Many users could become victims of this attempt, as there is nothing really suspicious, except the request of updating the personal information.

![Figure 28: Phishing e-mail example](image-url)

- No recipient e-mail address
- The link redirects to another web address: https://www.ppp-info-update.com/ssl/secure/128bit/manage/account/w
- There is no personalised greeting
Even though, the above Phishing e-mail is sophisticated; there are also some points that should be taken under consideration when the e-mail recipient feels threatened by Phishing:

- The link that appears in the Phishing e-mails is always different from the destination web address. This can be verified by checking the e-mail’s status bar.
- Often account details and numbers are included that are incorrect, trying to create a more official looking request.
- Poor use of the English language is also a common characteristic, extended even on spelling and grammar mistakes.

The following picture illustrates the log-in page that follows when the e-mail receiver clicks on the link. The defrauded PayPal home page represents an almost identical copy of the legitimate one. As you can verify below the card’s PIN number is requested and should draw suspicions to the user. On the other hand the web page is similar to a legitimate, while any links transfer the user to the original PayPal site where the victim can be deceived quite effortless again.

Figure 29: Defrauded PayPal web page 1
Other oddly required information is the Social Security Number and the Driver’s License number as it can be noticed below.

However, if any information is filled in the user will be transferred to the following web page as confirmation of the user account.

The above example is no longer online as the fraud was exposed. As mentioned on the first picture, the login page transfers the victim to the Phishing web site:


The SSL certificate used by the Phishing site, does not match its domain and the browser should notify the user about that. The certificate used is stolen so that they avoid entering valid information. This cert used is s.p8.hostingprod.com that is registered with Yahoo! that leads to the conclusion that the fraudsters might be using a hosting package. This Phishing domain is registered to:

http://whois.domaintools.com/ppp-info-update.com
There are numerous Phishing examples on the web and as the situation gets worse nowadays, when the Phishing e-mails will be more sophisticated and deceptive. (Darugar, 2006)

**Spear Phishing**

Spear Phishing is a targeted and more personal Phishing attempt requesting for private information. It is a Phishing e-mail supposed to come from a well-known source of a company, such as administrators or human resource departments, massively sent to all staff. Even if only one person replies, the fraudsters can gain access to the company’s resources. (McDowell, 2006) It is more sophisticated than a classic Phishing attack; as the electronic message appears to be sent form the same domain with the target. Spear Phishing attacks emerge on a rise while the damage caused can be massive and the use of social engineering is more artistic and intelligent and can also serve spyware. Based on the IBM’s Global Security Index Report, in January 2005 there were 56 cases of Spear Phishing, whilst in June same year the incidents rose to 600,000. (Larkin, 2005)

On the Credit Union Information Security Professionals Association (C UISPA) case, the Spear Phishing e-mail attempt not only contained grammatical and spelling errors, but also Internet Explorer’s security flaw, by which the attackers could achieve a DOS (Denial-of-Service) attack and also execute or even use the legal user’s log-in privileges in order to run malicious code remotely. While the employees of the company are unaware of the threat, the fraudsters can break the security in simple steps. The employee receives the Phishing e-mail that requests to log-in in an organisation's software application or a spoofed web page that appears as the company's legitimate one. While the employee logs-in the, most probable, attached key logger records the keystrokes and as a result the fraudster gets access to the company's private information. Therefore, one more time the end-user's education appears vital. (Credit Union Journal, 2006)

According to William Pelgrin, director of the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) in Albany, there was a test Phishing scenario in the period between March and May 2005, when the New York CSCIC sent spear Phishing e-mails to almost 10,000 employees in order to discover whether they would reveal their personal information, in five state agencies. The results were remarkable: over 75% of the recipients opened the e-mail, 17% clicked on the link, and 15% tried to reveal their passwords. However, on a similar occasion a couple of months later, when the users were aware of the situation, a little 8% of the employees only opened the message. (Vijayan, 2005)

People can get easily deceived from Spear Phishing as the e-mails’ text is familiar to them, comes from a trustworthy source and even anti-spam software may miss to recognise the threat. In addition in most of these messages there are hidden Trojan-horse key loggers. (Security Director’s Report, 2005)
Based on the Credit Union National Association, Inc. (2006) web site one of the latest trends on Phishing scams is the cash rewards’ e-mails in exchange of answers concerning customer satisfaction. There is always a targeted organisation, on a spoofed website, that inquires feedback about its services. The bank account information is claimed to be requested for depositing the cash reward.

Below there is a sample of such a Phishing e-mail:

Dear Credit Union Customer,

You have been chosen by our online department to take part in this quick and easy 5 question survey. In return we will credit $20 to your account - Just for your time! Helping us better understand how our customers feel benefits everyone.

This survey serve as a useful tool in determining how we are doing and how we can improve. With the information collected we can decide to direct a number of change to improve and expand our online services.

We kindly ask you to spare two minutes of your time in taking part with this unique offer!

[Confirm Now]


your $20 Reward Survey with CUNA® Reward services.

The information you provide us is all non-sensitive and anonymous. No part of it is handed down to any third party groups. It will be stored in our secure database for maximum of 3 days while we process the results of this nationwide survey. Please do not reply to this message. For any inquiries, contact Customer Service.


Common Characteristics on Phishing attacks

Phishing is considered as a form of a Man-in-the-Middle attack (MITM), where the user can communicate with the attacker, but in the meanwhile the attacker communicates with the bank in real-time. In such a case neither the bank nor the user are aware of the attacker’s existence, claiming they have a secure connection. A Man-in-the-Middle attack has total control of the system, meaning that the attacker can even disconnect the user and submit his instruction to the bank. In order to avoid this threat the user only needs to prevent it happening, something that is beyond the current technology. (Oppliger et al. (2006), Dhamija, and Tygar (2005))

The APWG (2004) uncovered a common pattern used by fraudster when employing Phishing web sites. They determined that the web sites were hosted on machines appearing to be operated by the attacker. The hosts didn’t have registered domains. In addition none of the sites was running on port 80, most of them were on port 4903. All these analysed Phishing web sites were not intending to exploit financial organisations. The received Phishing e-mails were either an image map or with encoded URL in JavaScript. The JavaScript web sites were used with a popup page on top covering the original site. All the web sites on the research were responding as
SHS web server (small HTTP Server). This kind of attack may be running on zombie machines, while the attacker makes use of Trojan code hitting exploitable machines and installing the SHS, running for as many days as required for obtaining the information.

The method of Web Spoofing

Methods of achieving Web Spoofing

Web spoofing is considered as a hard-to-detect method. However, there is an almost ‘concrete’ method followed in order to publish a spoofed web site. The actual procedure is illustrated on the figure below:

Every time a user requests a web page from a web browser, the web browser calls for that page over the network from the web server that hosts the page. However, when a fraudster discovers network security vulnerability, can pass over this procedure, attack the network and manage to use the web traffic arbitrary.

a. **Universal Resource Locator (URL) rewriting:**

It is the easy deception method used by the attacker. The aim is to lead the victim visit his spoofed web page. The URL is rewritten on a Web page providing the link for the requested web page, while indicating the attacker’s web server. The rewriting is usually difficult for the victim to point it out. Therefore, when the victim clicks on the link on his web browser, the attacker’s server is going to request the valid Web page.

However, at the same time, the content of the original web page is rewritten for the attacker’s needs and presented to the victim’s browser.

This way, the fraudster manages to copy the whole URL for his spoofed web page and the result is that anytime the victim uses a new link form this page, will always stay and use the attacker’s web page on his web server, without the user’s knowledge. Assuming that the original web site is [url] www.victim.com [/url], the attacker could...
rename it as [url] http://www.victim.com [/url]. Therefore, each time the victim tries to visit the specific web page will be entrapped to the fraudster’s web server.

b. Forms:

As long as a URL can be spoofed, so can a web based form. A submitted form is URL encoded and the reply is plain HTML. Consequently, every time a form is completed on a spoofed web page, the procedure appears to continue as normal. However, the information is submitted to the fraudster’s web server, who has the opportunity to process the data according to his needs and will and then transfer them to the legitimate server, the same procedure is also followed for the reply forms.

c. Secure Sockets Layer (SSL):

SSL is a protocol created to encrypt data on web transactions in order to protect any sensitive information transferred on the web. Even though it is considered as the ‘top requirement’ for establishing a secure transaction, it appears as weak related to web browsers and fraudsters. While the victim connects to the fraudster’s web server, even the secure connection indicator will appear as normal, but the transaction will take place through the fraudster’s server instead. (Felten et al., 1997) In general terms though, the SSL protocol is considered as invulnerable for the man-in-the-middle attacks, the threat emerges by the exploits of the software applications on the users’ computers. (Emigh, 2006)

There are three principles that make a web site unique:

1. The domain name that is the unique name each web site owns as its identifier. They can be purchased online that protects the identity of the imposer who is going to choose a very similar name to the target’s original one. It is usually difficult for the user’s eye to spot on the difference at the first glance.

2. The content, the most important issue concerning a web site, as it needs to be identical to the original. The majority of web sites include HTML code (HyperText Markup Language).

3. The web hosting service that is going to make the web site available. The fraudster may even have the opportunity to defraud and create custom e-mail addresses on the legitimate company’s name.

When the fraudster achieves to manipulate all of them, he has achieved the attack.

The man-in-the-middle attack is also performed on the web spoofing attacks, the same way with phishing attacks. Once the attacker achieves this, it is easy then to perform the supervision of the web page and manage the attack.

Common Characteristics on Web Spoofing attacks

There are some common characteristics that reveal the redirection to a ‘spoofed’ web page. In cases where user authentication is required any incorrect login attempt is usually prompted as correct, as the entries cannot be handled. However, some of the latest web spoofed sites appear display messages for incorrect login.
Another common feature is the JavaScript handling that controls all links and content, in order to avoid showing the genuine web address. In case the user saves the HTML page, he won’t be able to retrieve it, as there is a .dll component that rules the code generation on the browser, as well as the JavaScript code that is inherited on the fraudster’s web server. Ye et al. (2000) argue that standard internet browsers, user interfaces, SSL sessions and their certificates can be forged, while the JavaScript session has the ability to replace the original web address on the address bar with a forged one at the top of the browser window. (Dinev, 2006)

The method of Pharming

Common Characteristics on Pharming attacks

The target of a pharming attack for conducting ID theft is the computer, not the individual (Mahmood, 2006). Bocij (2006) supports that they are difficult to be suspected, detected and revealed, as they basically refer to web sites that the user reasonably visits, ‘pulled to the web site’, such as a web banking site. Pharming occurs due to the alteration of a single IP address, which means that the fraudster targets a specific group of people, e.g. customers of a specific bank. This gives them the ability to have a large profit, as they will act unattended and the risk of being exposed is low.

DNS cache poisoning seems to be the most popular way of achieving pharming, while the pharm sites are hosted on botnets. The APWG (2005), refer to registration of similar domain names and attacks on search engines as future pharming methods.

Social Engineering

Types of Social Engineering

Impersonation is the most relevant word to social engineering. The attacker pretends either in person or over the phone to be a trustworthy person, depending on the objective; a convincing situation to persuade an individual to reveal a piece of private information. This might be a user ID, password or any other type of information sensitive or not, that appears valuable for the fraudster.

Reverse social engineering is considered as the most dangerous type. For this case, the social engineer behaves as an authorised person to help a company’s employees overcome a problem. Any trouble that has appeared is caused by the hacker usually by disrupting the network’s traffic, therefore the victim is going to contact the attacker persuaded that he can solve the problem. (Gartner, 2002) Then, the fraudster, either creates a trustworthy relationship with the victim, or achieves a direct attack. (Gragg, 2002)

One suggested example for social engineering is that a company’s competitors or former employees might try to harm a business by accessing a company’s private information. They can use social engineering techniques in order to achieve their purpose (Hiemstra, 2004). According to Denning (1999) the information flow from
the employees could be limited if the users were trained in security awareness and were instructed on requesting further details before disclosing sensitive data.

Stasiukonis (2006) conducted an experiment and placed twenty USB flash drives in areas frequently visited by a credit union’s employees. They contained a specially written Trojan program, planted in image files, which would email any logins, passwords and other sensitive information to him. Fifteen were collected by the employees and immediately plugged into their company’s computers.

Anaphora on Nigerian 419 scam

The Nigerian 419 scam first appeared in the early 1980s originally as a request usually from the central bank or other official government agency. This scam is considered as the third largest industry in Nigeria has cost more than five billion dollars all over the world the last fifteen years and at least 15 people have lost their lives until 1998. (Mintz, 2002)

It belongs to the advance fee fraud and is also popular as the Nigerian letter or 419 scam. According to the Internet Fraud Watch in the USA, it is a 2% of all scam complaints, however considered third in the top ten scam list. The scam starts either with a bulk e-mail or bulk fax gathering similar letters to companies and individuals usually with a wealth background. It requests usually an investment of a large amount of money to be made through the recipient’s account due to the limits exist in Nigeria (the amount is usually in dollars).

In case the recipient reply to such a letter then gets in contact with the defrauders asking him to pay advance fees, transfer taxes, performance bonds etc. and every time he pays he will be asked to pay something else in advance.

Characteristics of the Nigerian Scam

- The situation appears urgent by the deceivers
- The victim is usually requested to travel to Nigeria
- Sometimes actual Nigerian officials and government buildings are used
- The victim’s account numbers are asked
- Different kinds of processing fees are asked to be paid
- They demand to keep the transaction confidential
- They often use a Nigerian U.S. or U.K. resident for the transaction
- Really often someone pretends to be a Nigerian loyalty person (Quatloos, 2006)

The Nigerian penal code prohibits the action and many web sites informing the people about the fraud, however the activity cannot be minimised. According to the fraud department of the Metropolitan Police (2008) losses of the scam have reached four to five million dollars.
Appendix E:

ID Theft Investigation Framework Flow
Phase 1. Media Analysis

**Digital Media**

**Process 1. Source Identification**

**Activities**

I.1.1. Data browse

<table>
<thead>
<tr>
<th>Instruction 1. Online data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective 1.1. Evidential computer storage components</td>
</tr>
<tr>
<td>Objective 1.2. Computer storage media</td>
</tr>
</tbody>
</table>

Instruction 2. Offline data

| Objective 2.1. Any offline data that can be used as additional evidence |

I.1.2. Live system

<table>
<thead>
<tr>
<th>Instruction 1. Check operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective 1.1. Shutdown</td>
</tr>
<tr>
<td>Objective 1.2. Disconnect</td>
</tr>
</tbody>
</table>

O.1.1. Keep record of the scene

**Process 2. Digital Media collection**

**Activities**

I.2.1. Identify different digital media

| Instruction 1. Generic device storing personal data |

I.2.2. Secure/ isolate digital media

I.2.3. Collect/ package digital media

O.2.1. Document

**Process 3. Image Acquisition**

**Activities**

I.3.1. Select appropriate tool

I.3.2. Protect media from possible alteration of data

I.3.3. Image the original media

I.3.4. Store safely original media

I.3.5. Back-up the image, work on that

I.3.6. Create Cryptographic Value
ID Theft Data Identification

Process 4. Evidential data identification

Activities

V. Victim
I.4.1.V. Existence of malicious software
I.4.2.V. Existence of unsecured transactions
I.4.3.V. Vulnerable system
O.4.1.V. Victim evidential data list

F. Fraudster
I.4.1.F. Existence of malicious software code
I.4.2.F. Forensic extraction software
I.4.3.F. Hacking tools
O.4.1.F. Fraudster evidential data list

Process 5. Target Identification

Activities

I.5.1. Vulnerable systems
I.5.2. Published information
I.5.3. Individual/Corporate
O.5.1. Target identification list

Process 6. Threat agent identification / intention

Activities

I.6.1. Internal/External attack
I.6.2. Individual/Corporate
O.6.1. Threat agent identification list

Phase 2. Evidence Analysis

ID Theft Data Analysis

Process 7. Data Analysis

Activities

I.7.1. Identify all files of the system
Instruction 1. Existing files
Instruction 2. Deleted, remaining
Instruction 3. Hidden data
Instruction 4. Encrypted / password protected
Instruction 5. Temp files / folders
I.7.2. Recover deleted files
I.7.3. Slack / Unallocated space
I.7.4. Hidden partitions
O.7.1. Define files that can be used as evidence

Process 8. Target Analysis
Activities
V. Victim
I.8.1.V. Malicious software / code
Instruction 1. Monitors web-browser Process/network traffic
Instruction 2. Accesses contact list records
Instruction 3. Accesses clipboard contents
Instruction 4. Trojans that collect personal info
Instruction 5. Software Keylogger (hosted)

I.8.2.V. Local-based e-mail
I.8.3.V. Web-based e-mail
I.8.4.V. Embedded Object scripting access languages
I.8.5.V. Recently accessed documents
I.8.6.V. URL information
Instruction 1. URL cache
Instruction 2. URL Process record

I.8.7.V. Security permissions
I.8.8.V. Application histories
I.8.9.V. Instant message history log
I.8.10.V. Databases
I.8.11.V. Spreadsheets
I.8.12.V. Number systems
O.8.1.V. List evidential findings
Activities
F. Fraudster
I.8.1.F. Internet bookmarks
I.8.2.F. Steganographic search
I.8.3.F. Embedded Object scripting access languages
I.8.4.F. Installed software
Instruction 1. Web design applications
Instruction 2. Existence of Anti-Forensics applications
Instruction 3. System Process eraser
Appendices

I.8.1.F. Track illicit software use
I.8.2.F. Recent Documents
I.8.3.F. Filenmes
I.8.4.F. URL information
  Instruction 1. URL cache
  Instruction 2. URL Process record
I.8.5.F. Local based e-mail
I.8.6.F. Web based e-mail
I.8.7.F. Operating System Registry entries
I.8.8.F. Security permissions
I.8.9.F. Instant message history log
I.8.10.F. Malicious software (Trojan code / bot)
I.8.11.F. Malicious source code existence
I.8.12.F. Web server communication
I.8.13.F. Databases
I.8.14.F. Spreadsheets
I.8.15.F. Images
I.8.16.F. File Processes
I.8.17.F. Number systems
O.8.1.F. List evidential findings

Process 9. Threat Agent Analysis

Activities
I.9.1. Intention
  Instruction 1. Financial
  Instruction 2. Identity

I.9.2. Motivation
  Instruction 1. Target

I.9.3. Knowledge / Skills

Evidence

Process 10. Evidence Collection

Activities
I.10.1. Use evidential findings list, O.8.1.V. or O.8.1.F.

O.10.1.Create list of evidence based on ID Theft types
  Instruction 1. Financial
  Objective 1.1. Credit histories
<table>
<thead>
<tr>
<th>Objective 1.2. Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective 1.3. Application names</td>
</tr>
<tr>
<td>Objective 1.4. Phone records</td>
</tr>
<tr>
<td>Objective 1.5. Tax records</td>
</tr>
<tr>
<td>Objective 1.6. Bankruptcy records</td>
</tr>
<tr>
<td>Objective 1.7. Documents on other people’s names</td>
</tr>
<tr>
<td>Objective 1.8. Dates of birth</td>
</tr>
</tbody>
</table>

**Instruction 2. Identity**

<table>
<thead>
<tr>
<th>Objective 2.1. Financial Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective 2.2. N.I. Numbers</td>
</tr>
<tr>
<td>Objective 2.3. Driving licence</td>
</tr>
<tr>
<td>Objective 2.4. Employment records</td>
</tr>
<tr>
<td>Objective 2.5. Passport records</td>
</tr>
<tr>
<td>Objective 2.6. Business records</td>
</tr>
<tr>
<td>Objective 2.7. Property records</td>
</tr>
<tr>
<td>Objective 2.8. Documents on other people’s names</td>
</tr>
<tr>
<td>Objective 2.9. Dates of birth</td>
</tr>
<tr>
<td>Objective 2.10. ID Card copies</td>
</tr>
<tr>
<td>Objective 2.11. Criminal records</td>
</tr>
</tbody>
</table>

O.10.2. Threat agent Evidence list (Process 9 is used as input)

**Process 11. Evidence Classification**

**Activities**

I.11.1. Use evidential findings list, O.8.1.V. or O.8.1.F. respectively

O.11.1. Create evidence classification list

<table>
<thead>
<tr>
<th>Instruction 1. Strongly Evidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction 2. Evidential</td>
</tr>
<tr>
<td>Instruction 3. Irrelevant</td>
</tr>
</tbody>
</table>
Phase 3. Scenario Construction

Evidence Classification

Process 12. Structure of evidential data

Activities
I.12.1. Use evidence as of Processes 10 and 11
O.12.1. Categorisation of evidential data

Instruction 1. E-mail
Instruction 2. Internet Related
Instruction 3. Malware
Instruction 4. Hacked Databases
Instruction 5. Malicious Tools
Instruction 6. Documents
Instruction 7. Application logs
Instruction 8. System Vulnerabilities
Instruction 9. Other

Process 13. Structure threat agent’s profile

Activities
I. 13.1. Use Threat agent Evidence list O.10.2
V. Victim
O.13.1. V Reveal technical skills
O.13.2. V Reveal programming skills
O.13.3. V Ability to convince someone
O.13.4. V Ability to keep stealth action
F. Fraudster
O.13.1. F Sophistication of tools
O.13.2. F Level of expertise
O.13.3. F Use of defensive techniques
O.13.4. F Identify purpose of attacking
O.13.5. F Identify motivation
O.13.6. F Identify opportunities


Activities
I.14.1. Structure all sort of valuable information
I.14.2. Identify evidential aspects
O.14.1. Group the evidential aspects
Scenario

Process 15. Scenario Outline

Activities

I.15.1. Use evidence as of I.1.1.< Instruction 2, Phase 1< ID Theft Data Identification, Phase 2< Evidence, and Phase 3< Evidence Classification

O.15.1. List valuable data gathered

Process 16. Scenario Preparation Documentation

Activities


O.16.1. Merge evidential data gathered

Phase 4. Evaluation

Scenario Examination

Process 17. Scenario Testing/ Evaluation

Activities

I.17.1. Use Phase 1< ID Theft Data Identification, Phase 2< Evidence, and Phase 3< Scenario Examination

I.17.2. Check validation / entirety of the outputs

O.17.1. Create evaluation list

Process 18. Scenario Clarification

Activities

I.18.1. Use evaluation list as of O.17.1.

I.18.2. Clarify the impact of evidential data

O.18.1. Create scenario clarification list

Case

Process 19. Case Construction

Activities

I.19.1. Use data from the scenario clarification list O.18.1

O.19.1. Construct the case

Process 20. Case Clarification

Activities

I.20.1. Clarify the constructed case from O.18.1.

Activities
I.21.1. Use the scenario evaluation list from O.17.1.
I.21.2. Check validation
O.21.1. Confirm case evaluation

Process 22. Evidential Case Representation

Activities
I.22.1. Create the testimonial report
Instruction 1. Include all case evidence
Instruction 2. Describe all case evidence
O.22.1. ID Theft Case Investigation Report
Appendix F:

Data Dependencies
I. Representation of Dependencies and Processes

High Level Phases

High Level Processes
II. Representation of the ID Theft Investigation Framework Complexity
III. Representation of the ID Theft Investigation Framework Relationships
IV. The relationships of each Phase
Phase 1: Media Analysis
Phase 2: Evidence Analysis
Phase 3: Scenario Construction
Phase 4: Evaluation
Appendix G:

High Level Flowchart
Appendix H:

ID Theft Investigation Framework

Abstracted procedure for the investigator
Initialization of the investigation

P1. MEDIA ANALYSIS

DIGITAL MEDIA: Identify, collect and image the available digital media

Process 1. Source Identification,

Identify the source of information, follow the Activities:

I.1.1. Media Selection: observe and identify all the evidential aspects, based on the following instructions:

Instruction 1. online
Instruction 2. offline

where for online the investigator is searching for

Objective 1. evidential computer storage components
Objective 2. computer storage media

and for offline stands

Objective 2.1. any offline data that can be used as additional evidence

continue to

I.1.2. Live system: check the operating system in case the system is running, continue to

O.1.1. Keep Record of the scene: Record the current scene, close Source Identification (Process 1), and continue to Digital Media Collection (Process 2).

Process 2. Digital Media Collection,

Prepare for the digital media acquisition, follow the functions:

I.2.1. Identify different digital media: identify the different digital media available in the crime scene, where different digital media is

Instruction 1. Generic digital device able to store personal data,

continue to

I.2.2. Secure/ isolate digital media: Securely detach the digital media by avoiding any alteration or damage and continue to
Appendices

I.2.3. Collect/package digital media: Securely collect and package the media for the transport to the lab, continue to

O.2.1. Document: Verify the process by documenting the procedure undertaken, close Activity, continue to Image Acquisition (Process 3).

Process 3. Image Acquisition,

The digital media is transferred to the lab, preparation for imaging initiates, the following activities occur:

I.3.1. Select appropriate tool: select the preferable tool for imaging the media, continue to

I.3.2. Protect media from possible alteration of data: protect the media from any other possible risks that could alter the evidence, continue to

I.3.3. Image the original media: create the image of the medium, continue to

I.3.4. Store safely original media: store original media in limited access storage locker, continue to

I.3.5. Back-up the image, work on that: create a back-up copy of the image and work on this copy, continue to

I.3.6. Create Cryptographic Value: calculates the file’s checksum for the integrity of the evidence, ensure completion of the process, close Image Acquisition (Process 3), and continue to ID Theft Data Identification.

ID THEFT DATA IDENTIFICATION: Initial identification, browsing for ID Theft Data, create viewpoint, preparation for the next Phase (Evidence Analysis)

Process 4. Evidential data identification: Identify whether the medium belongs to a victim or a fraudster, follow the activities

for Victim (V):

I.4.1. V. Existence of malicious software: Identify malicious software running on the system, continue to

I.4.2. V. Existence of unsecured transactions: Identify unsecure, unencrypted network transactions, continue to
I.4.3.V. Vulnerable system: Identify the lack of computer security software, proves that the system has been vulnerable to an attack, continue to

O.4.1.V. Victim evidential data list: The products of the above activities, where the identified elements are listed, close Evidential data identification (Process 4), continue to Target identification (Process 5).

for Fraudster(F):

I.4.1.F. Existence of malicious software code: Not only malicious software existence as in I.4.1.V., but also the existence of malicious source code, continues to

I.4.2.F. Forensic extraction software: Identify forensic extraction software existence, continue to

I.4.3.F. Hacking tools: Existence of hacking applications to the system, according to the findings, continue to

O.4.1.F. Fraudster evidential data list: As in O.4.1.V., the products of the above activities, where the identified elements are listed, close Evidential data identification (Process 4), and continue to Target identification (Process 5).

Process 5. Target identification: Identify the reason that led the machine to become a target, follow the activities

I.5.1. Vulnerable systems: Identify an unsecure system that can easily become target of unlawful use, continue to

I.5.2. Published information: Identify published personal information on the internet that could have been used for fraudulent purposes, continue to

I.5.3. Individual / corporate: Determine whether the target has been an individual or corporate system. If corporate, refer to the organisation’s security policy, continue to

O.5.1. Target identification list: A list that includes the target identification data, as provided from the activities of this process, close Target Identification (Process 5), and continue to Threat Agent identification/ intention (Process 6).

Process 6. Threat Agent identification/ intention: Identify the intention of the fraudster, based on the existing observation, follow the activities

I.6.1. Internal/ external attack: Identify whether the incident is considered as a direct internal network attack or as an external source, continue to
I.6.2. Individual/ corporate: State the threat agent’s intention. Determine whether the target appears as individual or corporate.

O.6.1. Threat Agent identification list: The output activity that creates a list with the data identified on I.6.1 and I.6.2.

Keep track of the evidential data provided from this Phase and complete Media Analysis (P1). The purpose is to use the results (output) of the Phase as the significant link to the input of the next Phase. Continue to Evidence Analysis (P2).
Examination of the evidence

P2. EVIDENCE ANALYSIS

ID THEFT DATA ANALYSIS: Analyse the medium, aiming to identify and collect the evidential data. It requires the use of a selection of analysis tools.

Process 7. Data Analysis: Identify evidential data in every single part of the digital media, based on the classic computer forensics investigation, follow the functions

I.7.1. Identify all files of the system: Identify all the areas of the digital media that files can be retrieved, these are

Instruction 1. Existing files: all the existing files that appear in the medium during the search

Instruction 2. Deleted, remaining: retrieve deleted data that have remained and can probably provide additional proof

Instruction 3. Hidden data: check the system for hidden files

Instruction 4. Encrypted/ password protected: identify encrypted and password protected files, attempt decryption

Instruction 5. Temporary files/ folders: identify temporary files and folders on the system

continue to

I.7.2. Recover deleted files: Recovered the deleted files in order to examine their content, continue to

I.7.3. Slack / Unallocated space: Examine the slack and unallocated space of the medium, continue to

I.7.4. Hidden partitions: Check the system for hidden partitions that could contain sensitive data, continue to

O.7.1. Define files that can be used as evidence: Collect the files identified in the previous functions and can be used as evidential aspects to the following activity, close Data Analysis (process 7), continue to Target Analysis (Process 8).
Process 8. **Target Analysis**: Analyse the data that connect either with the victim (V.) or the fraudster (F.), according to the existing findings, follow the activities

For **Victim (V.)**

I.8.1.V. Malicious Software: Perform a thorough anti-virus check with a collection of Antivirus programs. Identify whether the system has been infected with malware, this should perform the following in order to be linked with ID Theft

Instruction 1. Monitors web-browser activity/ network traffic

Instruction 2. Accesses contact list records

Instruction 3. Accesses clipboard contents

Instruction 4. Trojans that collect personal info

Instruction 5. Software Keylogger (hosted)

continue to

I.8.2.V. Local-based e-mail: Analyse the e-mail correspondence of the user. Identify information about the sender, the receiver, the date of the message and the content, continue to

I.8.3.V. Web-based e-mail: Web-based mail has to deal with the amount of information that is stored locally by the web browsers, continue to

I.8.4.V. Embedded Object scripting access languages: Analyse the purpose of existence of Embedded Object scripting access languages, continue to

I.8.5.V. Recently accessed documents: Identify whether track of recent documents is kept from the system, examine their content, continue to

I.8.6.V. URL information: Examine the information being kept to the system from the use of the Internet, in the terms of

Instruction 1. URL cache: investigate all the cache of the system, including visited web pages and images.

Instruction 2. URL activity record: reveal the typed URLs

continue to

I.8.7.V. Security permissions: Examine the security event log, check for alterations, continue to

I.8.8.V. Application histories: Examine the history kept by the installed applications, continue to
I.8.9.V. Instant message history log: Examine the history log (when enabled) and the contact list of the possibly installed instant messengers, continue to

I.8.10.V. Databases: Examine the content of the databases, where applicable, for financial records saved, continue to

I.8.11.V. Spreadsheets: Examine the content of the spreadsheets, where applicable, for financial records saved, continue to

I.8.12.V. Number systems: Perform searches that can reveal information about stored phone numbers, addresses, security pins, postcodes, etc.

O.8.1.V. List evidential findings: The output activity that creates a list with the evidential findings from Target Analysis, close Target Analysis (Process 8), and continue to Threat Agent Analysis (Process 9)

For Fraudster (F.)

I.8.1.F. Internet bookmarks: Visit and examine every page that appears in bookmarks for content verification, continue to

I.8.2.F. Steganographic search: Examine the existence of steganographic methods undertaken, continue to

I.8.3.F. Embedded Object scripting access languages: Analyse the purpose of Embedded Object scripting access languages existence, continue to

I.8.4.F. Installed Software: Examine the system for existence of installed software that promotes ID Theft, these are

Instruction 1. Web design applications: Can indicate the fraudster’s activity on Phishing or malicious web site designing

Instruction 2. Existence of Anti-Forensics applications: Can indicate the fraudster’s tension to alter data with Anti-Forensic techniques

Instruction 3. System activity eraser: Identification of software that wipes data and activities.

continue to

I.8.5.F. Track illicit software use: Examine the existence of hacking tools and shared files for Peer-to-Peer applications, continue to

I.8.6.F. Recently Accessed Documents: See I.8.5.V., continue to

I.8.7.F. Filenames: Examine the filenames of the system for suspicious content, continue to
I.8.9.F. URL information: See I.8.6.V.

Instruction 1.URL cache: See I.8.6.V.< Instruction 1

Instruction 2.URL activity record: See I.8.6.V.< Instruction 2.

continue to

I.8.10.F. Local based e-mail: See I.8.2.V., continue to

I.8.11.F. Web based e-mail: See I.8.3.V., continue to

I.8.12.F. Operating System registry entries: Examine the registry entries of the system as valuable information for the fraudster’s latest actions can be revealed, continue to

I.8.13.F. Security permissions: See I.8.7.V., continue to


I.8.15.F. Malicious software: Examine the system for malicious software archive that the fraudster may have used or intends to use, examine the behaviour of the malware, and continue to

I.8.16.F. Malicious source code existence: Examine the existence of writing or altering malicious source code and its behaviour, continue to

I.8.17.F. Web server communication: Examine information linked with web server communication, it can reveal instances of malicious actions, Denial-Of-Service attacks and DNS Poisoning, continue to

I.8.18.F. Databases: See I.8.10.V., continue to

I.8.19.F. Spreadsheets: See I.8.11.V., continue to

I.8.20.F. Images: Examine for identification of images from past victims, possible victims, or even contacts that the fraudster collects information, continue to

I.8.21.F. File Processes: Examine processes of the files that appear suspicious to the system during the investigation so far, continue to

I.8.22.F. Number Systems: See I.8.12.V.

O.8.1.F. List evidential findings: The output activity that creates a list with the evidential findings from Target Analysis, close Target Analysis (Process 8), and continue to Threat Agent Analysis (Process 9)

Process 9. Threat Agent Analysis: Analyse the purposes of the Threat Agent, based on the findings, follow the activities
I.9.1. Intention: Identify the intention of the fraudster, based on the findings and the different ID Theft types:

Instruction 1. Financial: The purpose of the ID thief is to gain access to financial information.

Instruction 2. Identity: The purpose of the ID thief is to gain access to someone’s identification information or impersonate an individual.

I.9.2. Motivation: Determine the motive of the threat agent, in the terms of

Instruction 1. Target: Identify the objective of the attack

I.9.3. Knowledge / Skills: Determine the background knowledge of the fraudster, the group that the threat agent belongs, close Threat Agent Analysis (Process 9), and continue to Evidence.

EVIDENCE: It involves the determination of the evidence, as raw data as evidence does not justify the value of the findings. The outcome (output) leads to the P3 Scenario Construction, where the evidence is defined.

Process 10. Evidence Collection: Collect the evidential data that was gathered on the previous process and follow the activities

I.10.1. Use evidential findings list, O.3.2.(A) or O.3.3.(B): In order to satisfy the need of classifying the evidence, the analyst needs to use the appropriate evidential findings list also in this function.

O.10.1. Create list of evidence based on ID Theft types: Categorise the evidential data identified from the analysis according to the different forms of ID Theft:

Instruction 1. Financial, all financial information gathered after the analysis of the digital media is included

Objective 1. Credit histories

Objective 2. Transactions

Objective 3. Application names

Objective 4. Phone records

Objective 5. Tax records
Objective 6. Bankruptcy records

Objective 7. Documents on other people's names

Objective 8. Birth dates

Instruction 2. Identity, evidential data that has to do with an individual's identity,

Objective 1. Financial Evidence

Objective 2. National Insurance (N.I.) Numbers

Objective 3. Driving licence

Objective 4. Employment records

Objective 5. Passport records

Objective 6. Business records

Objective 7. Property records

Objective 8. Documents on other people's names

Objective 9. Dates of birth

Objective 10. ID Card copies

Objective 11. Criminal records

continue to

O.4.2. Threat agent Evidence list: List the evidence that has been collected after the Threat Agent Analysis (Process 9), close Evidence Collection (Process 10), and continue to Evidence Classification (Process 11).

Process 11. Evidence categorisation: Categorise the findings of the analysis by determining their quality, follow the activities

I.4.2. Use evidential findings list, O.8.1.V. or O.8.1.F.: use the appropriate evidential findings list also in this function as an input.

O.4.4. Create evidence classification list: Provide three lists where evidence is classified based on its gravity, the categorisation is

Instruction 1. Strongly Evidential: include the findings that exemplify the premise and promote its validity
Instruction 2. Evidential: include the findings that are linked with the incident, but is not outstanding.

Instruction 3. Irrelevant: include findings that seemed meaningful in the beginning of the examination and are considered irrelevant after the completion of Evidence Collection (Process 10).

P2 Evidence Analysis is completed with the creation of the classification lists. The output Evidence is linked with the manipulation of data at the Evidence Classification input on the next Phase. Continue to P3 Scenario Construction.
Interpretation of the evidence

P3. SCENARIO CONSTRUCTION

EVIDENCE CLASSIFICATION: Use the outcomes of P2, identify the categories that the evidential data belong, group and appoint it accordingly.

Process 12. Structure of evidential data: Collect the evidence that has been discovered during P2. Evidence Analysis, structure and categorise it in order to draw a constructed picture concerning the evidential data. Follow the activities

I.12.1. Use evidence as of Processes 10 and 11: Collect this evidence listed and classified on O.10.1. and O.10.2., use it in the next activity, continue to

O.12.1. Categorisation of evidential data: Categorise the evidential data from the previous activity, based on their content

Instruction 1. E-mail: from I.8.2.V., I.8.3.V. or I.8.9.F, I.8.10.F.

close Structure of Evidential Data (Process 12), continue to Structure Threat Agent’s profile (Process 13).

Process 13. Structure Threat Agent’s profile: Collect the evidence identified during the Threat Agent Analysis (Process 9). Determine the findings based on the victim’s and the fraudster’s side.
I.13.1. Use threat agent evidence list O.10.3.: Use the list that was created from Evidence Collection (Process 10) Threat Agent Evidence list O.10.3., in order to aid the profiling of the threat agent, continue to

For **Victim (V.)**

O.13.1.V. Reveal technical skills: structure the technical abilities of the fraudster according to the techniques undertaken, as low and high technical level, continue to

O.13.2.V. Reveal programming skills: based on the method of the attack and the quality of the programming scripts, continue to

O.13.3.V. Ability to convince someone: social engineering skills that are possibly identified after the media analysis, continue to

O.13.4.V. Ability to keep stealth action: the complexity of the attack, as combined from the vulnerabilities of the system and the technical skills of the fraudster, close Structure Threat Agent’s profile (Process 13), continue to Structure Analyzed Digital Evidence (Process 14).

For **Fraudster (F.)**

O.13.1.F. Sophistication of tools: the identified collection of tools at the fraudster’s side that provide his capabilities complexity and background, continue to

O.13.2.F. Level of expertise: the more advanced and complex the tools that have been used, the more experienced and advanced the threat agent, continue to

O.13.3.F. Use of defensive techniques: identification of techniques that indicate stealth action, continue to

O.13.4.F. Identify purpose of attacking: draw a picture regarding the purpose of the attack (ego or curiosity), continue to

O.13.5.F. Identify motivation: identify data that indicate a more than personal gain motive, continue to

O.13.6.F. Identify opportunities: combine the lists created from O.13.1.F to O.13.5.F. in order to identify the opportunities, close Structure Threat Agent’s Profile (Process 13), continue to Structure analysed digital evidence (Process 14).

**Process 14. Structure analysed digital evidence:** Create a structured set of evidential data that includes the key aspects of the overall analysis, based on Structure of
Evidential Data (Process 12) and Structure Threat Agent’s Profile (Process 13), follow the activities

I.14.1. Structure all sort of valuable information: list the piece of information that kept your attention examiner during the analysis of the digital media, continue to

I.14.2. Identify evidential aspects: declare the data that link the piece of evidence together. The number of times an evidential file appears in the medium and concerns the same individual, continue to

O.14.1. Group the evidential aspects: Collect the evidential aspects from Identify Evidential aspects I.14.2. and group them close Structure analysed digital evidence (Process 14), and continue to Scenario, the output of the Phase.

SCENARIO: ‘Predict’ and present a coherent and efficient chronicle of the evidence identified and classified so far.

Process 15. Scenario Outline: Use the evidential sources identified during the analysis and classification to create lists, follow the activities

I.15.1. Use evidence as of I.1.1.< Instruction 2, Phase 1< ID Theft Data Identification, Phase 2< Evidence, and Phase 3< Evidence Classification: Collect the evidential outputs and use them on the next activity, continue to

O.15.1. List valuable data gathered: List the valuable data that has been gathered during the previous activity I.15.1.; produce an outline of groups, according to the type of the evidence, close Scenario Outline (Process 15) , continue to Scenario Preparation Documentation (Process 16)

Process 16. Scenario Preparation Documentation: Prepare the scenario, according to the listed valuable data of the Scenario Outline (Process 16), follow the activities

I.16.1. Use Scenario outline list: Use the list created in the List valuable data gathered O.15.1., continue to

O.16.1. Merge evidential data gathered: Collect and merge the overall evidential data in order to prepare the documentation

P3 Scenario Construction is completed with the production of a draft scenario. Continue to P4 Evaluation.
Validation of the Evidence

P4. EVALUATION

SCENARIO EXAMINATION: Evaluate the examination that has taken place so far in order to present the case by testing the Scenario output from P3 Scenario Construction.

Process 17. Scenario Testing/ Evaluation: Verify and clarify the scenario, according to the evidential data discovered, follow the functions

I.17.1. Use the outputs of Phases 1, 2 and 3: Use of the outputs of the previous Phases in order to revise his outcomes as gathered in Scenario Preparation Documentation (Process 16), continue to

I.17.2. Check validation / entirety of the outputs: Check the validation and the entirety of the outputs, continue to

O.17.1. Create evaluation list: Include the crucial data that have been identified after the evaluation and create the evaluation list, mention amendments to previous activities. Close Scenario Testing/ Evaluation (Process 17), continue to Scenario Clarification (Process 18)

Process 18. Scenario Clarification: Confirm the outcome of the scenario, its dependencies and agreement with the results of Scenario Testing/ Evaluation (Process 17), follow the activities

I.18.1. Use evaluation list from O.17.1.: At this function the examiner needs to use as an input the output of the previous process, continue to

I.18.2. Clarify the impact of evidential data: Explain the effect of the evidential data in relation to the incident, state the implication of the results.

O.18.1. Create scenario clarification list: Create a list that includes the impact of clarified data as resulted from the previous activity. Close Scenario Clarification (Process 18), continue to Case, the output of P4 Evaluation.
CASE: Present in this process, present accurate, constructed evidence results for the submission and representation of the case

Process 19. Case Construction: Build the foundation of the case representation, use the output of the previous process, and follow the activities

I.19.1. Use data from the scenario clarification list O.18.1.: Use the output of the Process 18 and continue to

O.19.1. Construct the case: Create a constructed outline of the case, close Case Construction (Process 19), and continue to Case Clarification (Process 20).

Process 20. Case Clarification: Link the representation of the evidence with the impact of the case, follow the activity

I.20.1. Clarify the constructed case: Justify the relation of the evidential data with the initial premise, clarify the sources. Close Case Clarification (Process 20), and continue to Case Evaluation (Process 21).

Process 21. Case Evaluation: Ensure the validity of the constructed case, follow the activities

I.21.1. Use the scenario evaluation list from O.17.1.: Refer to the Scenario Evaluation list activity O.17.1. in order to ensure that all evidential aspects are included, continue to

I.21.2. Check validation: Ensure the structured layout of the case, according to Check validation/ entirety of the outputs I.17.2. activity, continue to


Process 22. Evidential Case Representation: Create a formal document that includes the outcome of his work, follow the activities

I.22.1. Create the testimonial report: Represent all the findings of the examination on a manner that adheres to the evidence from the technical and scientific point of view and can be interpreted in a way to be read and comprehended by a jury. Therefore, follow
Instruction 1. Include all case evidence: includes all evidence that has been already included and evaluated in Case Evaluation (Process 21).

Instruction 2. Describe all case evidence: use information from Instruction 1 and describe all the evidential data and the procedure undertaken.

O.22.1. ID Theft case investigation report: This is the final output, as all evidence has been described in the report and the final product of the investigation is the ID Theft case report.

P4 Evaluation closes with the representation of the case and terminates the ID Theft Investigation Framework.
Appendix I:

ID theft Investigation Framework

Documenting procedure
ID Theft Investigation Framework

Documenting Procedure for the investigator

FORENSIC EXAMINER NAME:

ID THEFT FORENSIC CASE NUMBER:

Requester:

Current date and time:

Receive Date:

Open Date:

Complete Date:

Working Hours:

Significant problems:

Keywords’ identifiable list:
# Phase 1. Media Analysis

## Digital Media

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process 1. Source Identification</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I.1.1. Media Selection</strong></td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Online data</td>
<td></td>
</tr>
<tr>
<td>Objective 1.1. Evidential computer storage components</td>
<td></td>
</tr>
<tr>
<td>Objective 1.2. Computer storage media</td>
<td></td>
</tr>
<tr>
<td>Instruction 2. Offline data</td>
<td></td>
</tr>
<tr>
<td>Objective 2.1. Any offline data that can be used as additional evidence</td>
<td></td>
</tr>
<tr>
<td><strong>I.1.2. Live system</strong></td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Check operating system</td>
<td></td>
</tr>
<tr>
<td>Objective 1.2. Shutdown</td>
<td></td>
</tr>
<tr>
<td>Objective 1.2. Disconnect</td>
<td></td>
</tr>
<tr>
<td><strong>O.1.1. Keep record of the scene</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Process 2. Digital Media collection</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I.2.1. Identify different digital media</strong></td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Generic device storing personal data</td>
<td></td>
</tr>
<tr>
<td><strong>I.2.2. Secure/isolate digital media</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I.2.3. Collect/package digital media</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Process 3. Image Acquisition</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I.3.1. Select appropriate tool</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I.3.2. Protect media from possible alteration of data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I.3.3. Image the original media</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I.3.4. Store safely original media</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I.3.5. Back-up the image, work on that</strong></td>
<td></td>
</tr>
<tr>
<td><strong>I.3.6. Create Cryptographic Value</strong></td>
<td></td>
</tr>
</tbody>
</table>

## Comments on Digital Media
## ID Theft Data Identification

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process 4. Evidential data identification</td>
<td></td>
</tr>
<tr>
<td>V. Victim</td>
<td></td>
</tr>
<tr>
<td>I.4.1.V. Existence of malicious software</td>
<td></td>
</tr>
<tr>
<td>I.4.2.V. Existence of unsecured transactions</td>
<td></td>
</tr>
<tr>
<td>I.4.3.V. Vulnerable system</td>
<td></td>
</tr>
<tr>
<td>O.4.1.V. Victim evidential data list</td>
<td></td>
</tr>
<tr>
<td>F. Fraudster</td>
<td></td>
</tr>
<tr>
<td>I.4.1.F. existence of malicious software code</td>
<td></td>
</tr>
<tr>
<td>I.4.2.F. forensic extraction software</td>
<td></td>
</tr>
<tr>
<td>I.4.3.F. hacking tools</td>
<td></td>
</tr>
<tr>
<td>O.4.1.F. Fraudster evidential data list</td>
<td></td>
</tr>
<tr>
<td>Process 2. Target identification</td>
<td></td>
</tr>
<tr>
<td>I.5.1. vulnerable systems</td>
<td></td>
</tr>
<tr>
<td>I.5.2. published information</td>
<td></td>
</tr>
<tr>
<td>I.5.3. individual/ corporate</td>
<td></td>
</tr>
<tr>
<td>Process 3. Threat agent identification / intention</td>
<td></td>
</tr>
<tr>
<td>I.6.1. internal/ external attack</td>
<td></td>
</tr>
<tr>
<td>I.6.2. individual/ corporate</td>
<td></td>
</tr>
<tr>
<td>O.6.1. Threat agent identification list</td>
<td></td>
</tr>
</tbody>
</table>

**Comments on ID Theft Data Identification**
# Phase 2. Evidence Analysis

## ID Theft Data Analysis

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process 7. Data Analysis</strong></td>
<td></td>
</tr>
<tr>
<td>I.7.1. Identify all files of the system</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Existing files</td>
<td></td>
</tr>
<tr>
<td>Instruction 2. Deleted, remaining</td>
<td></td>
</tr>
<tr>
<td>Instruction 3. Hidden data</td>
<td></td>
</tr>
<tr>
<td>Instruction 4. Encrypted / password protected</td>
<td></td>
</tr>
<tr>
<td>Instruction 5. Temp files / folders</td>
<td></td>
</tr>
<tr>
<td>I.7.2. Recover deleted files</td>
<td></td>
</tr>
<tr>
<td>I.7.3. Slack / Unallocated space</td>
<td></td>
</tr>
<tr>
<td>I.7.4. Hidden partitions</td>
<td></td>
</tr>
<tr>
<td>O.7.1. Define files that can be used as evidence</td>
<td></td>
</tr>
<tr>
<td><strong>Process 8. Target Analysis</strong></td>
<td></td>
</tr>
<tr>
<td>V. Victim</td>
<td></td>
</tr>
<tr>
<td>I.8.1.V. Malicious software / code</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Monitors web-browser activity / network traffic</td>
<td></td>
</tr>
<tr>
<td>Instruction 2. Accesses contact list records</td>
<td></td>
</tr>
<tr>
<td>Instruction 3. Accesses clipboard contents</td>
<td></td>
</tr>
<tr>
<td>Instruction 4. Trojans that collect personal info</td>
<td></td>
</tr>
<tr>
<td>Instruction 5. Software Keylogger (hosted)</td>
<td></td>
</tr>
<tr>
<td>I.8.2.V. Local-based e-mail</td>
<td></td>
</tr>
<tr>
<td>I.8.2.V. Web-based e-mail</td>
<td></td>
</tr>
<tr>
<td>I.8.3.V. Embedded Object scripting access languages</td>
<td></td>
</tr>
<tr>
<td>I.8.4.V. Recently accessed documents</td>
<td></td>
</tr>
<tr>
<td>I.8.5.V. URL information</td>
<td></td>
</tr>
<tr>
<td>Instruction 3. URL cache</td>
<td></td>
</tr>
<tr>
<td>Instruction 4. URL activity record</td>
<td></td>
</tr>
<tr>
<td>I.8.6.V. Security permissions</td>
<td></td>
</tr>
<tr>
<td>I.8.7.V. Application histories</td>
<td></td>
</tr>
<tr>
<td>I.8.8.V. Instant message history log</td>
<td></td>
</tr>
<tr>
<td>I.8.9.V. Databases</td>
<td></td>
</tr>
</tbody>
</table>
### Process 8. Threat Agent Analysis

**I.9.1. Intention**

Instruction 1. Financial  
Instruction 2. Identity

**I.9.2. Motivation**
Instructions 1. Target

1.9.3. Knowledge / Skills

Comments on ID Theft Data Analysis
## Evidence

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process 9. Evidence Collection</strong></td>
<td></td>
</tr>
<tr>
<td>I.10.1. Use evidential findings list, O.8.1.V. or O.8.1.F.</td>
<td></td>
</tr>
<tr>
<td>O.10.1. Create list of evidence based on ID Theft types</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Financial</td>
<td></td>
</tr>
<tr>
<td>Objective 1.1. Credit histories</td>
<td></td>
</tr>
<tr>
<td>Objective 1.2. Transactions</td>
<td></td>
</tr>
<tr>
<td>Objective 1.3. Application names</td>
<td></td>
</tr>
<tr>
<td>Objective 1.4. Phone records</td>
<td></td>
</tr>
<tr>
<td>Objective 1.5. Tax records</td>
<td></td>
</tr>
<tr>
<td>Objective 1.6. Bankruptcy records</td>
<td></td>
</tr>
<tr>
<td>Objective 1.7. Documents on other people’s names</td>
<td></td>
</tr>
<tr>
<td>Objective 1.8. Dates of birth</td>
<td></td>
</tr>
<tr>
<td>Instruction 2. Identity</td>
<td></td>
</tr>
<tr>
<td>Objective 2.1. Financial Evidence</td>
<td></td>
</tr>
<tr>
<td>Objective 2.2. N.I. Numbers</td>
<td></td>
</tr>
<tr>
<td>Objective 2.3. Driving licence</td>
<td></td>
</tr>
<tr>
<td>Objective 2.4. Employment records</td>
<td></td>
</tr>
<tr>
<td>Objective 2.5. Passport records</td>
<td></td>
</tr>
<tr>
<td>Objective 2.6. Business records</td>
<td></td>
</tr>
<tr>
<td>Objective 2.7. Property records</td>
<td></td>
</tr>
<tr>
<td>Objective 2.8. Documents on other people’s names</td>
<td></td>
</tr>
<tr>
<td>Objective 2.9. Dates of birth</td>
<td></td>
</tr>
<tr>
<td>Objective 2.10. ID Card copies</td>
<td></td>
</tr>
<tr>
<td>Objective 2.11. Criminal records</td>
<td></td>
</tr>
<tr>
<td>O.10.2. Target Evidence list</td>
<td></td>
</tr>
<tr>
<td>O.10.3. Threat agent Evidence list</td>
<td></td>
</tr>
<tr>
<td><strong>Process 10. Evidence Categorisation</strong></td>
<td></td>
</tr>
<tr>
<td>I.11.1. Use evidential findings list, O.8.1.V. or O.8.1.F.</td>
<td></td>
</tr>
<tr>
<td>O.11.1. Create evidence classification list</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. Strongly Evidential</td>
<td></td>
</tr>
<tr>
<td>Instruction 2. Evidential</td>
<td></td>
</tr>
</tbody>
</table>
Appendices

Instruction 3. Irrelevant

Comments on Evidence
Evidence Analysis Worksheet
# Phase 3. Scenario Construction

## Evidence Classification

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process 12. Structure of evidential data</strong></td>
<td></td>
</tr>
<tr>
<td>I.12.1. Use evidence as of Processes 10 &amp; 11</td>
<td></td>
</tr>
<tr>
<td>O.12.1. Categorisation of evidential data</td>
<td></td>
</tr>
<tr>
<td>Instruction 1. E-mail</td>
<td></td>
</tr>
<tr>
<td>Instruction 2. Internet Related</td>
<td></td>
</tr>
<tr>
<td>Instruction 3. Malware</td>
<td></td>
</tr>
<tr>
<td>Instruction 4. Hacked Databases</td>
<td></td>
</tr>
<tr>
<td>Instruction 5. Malicious Tools</td>
<td></td>
</tr>
<tr>
<td>Instruction 6. Documents</td>
<td></td>
</tr>
<tr>
<td>Instruction 7. Application logs</td>
<td></td>
</tr>
<tr>
<td>Instruction 8. System Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Instruction 9. Other</td>
<td></td>
</tr>
<tr>
<td><strong>Process 13. Structure threat agent’s profile</strong></td>
<td></td>
</tr>
<tr>
<td>I.13.1. Use Threat agent Evidence list O.10.2</td>
<td></td>
</tr>
<tr>
<td>V. Victim</td>
<td></td>
</tr>
<tr>
<td>O.13.1.V. Reveal technical skills</td>
<td></td>
</tr>
<tr>
<td>O.13.2.V. Reveal programming skills</td>
<td></td>
</tr>
<tr>
<td>O.13.3.V. Ability to convince someone</td>
<td></td>
</tr>
<tr>
<td>O.13.4.V. Ability to keep stealth action</td>
<td></td>
</tr>
<tr>
<td>F. Fraudster</td>
<td></td>
</tr>
<tr>
<td>O.13.1.F. Sophistication of tools</td>
<td></td>
</tr>
<tr>
<td>O.13.2.F. Level of expertise</td>
<td></td>
</tr>
<tr>
<td>O.13.3.F. Use of defensive techniques</td>
<td></td>
</tr>
<tr>
<td>O.13.4.F. Identify purpose of attacking</td>
<td></td>
</tr>
<tr>
<td>O.13.5.F. Identify motivation</td>
<td></td>
</tr>
<tr>
<td>O.13.6.F. Identify opportunities</td>
<td></td>
</tr>
<tr>
<td><strong>Process 13. Structure analysed digital evidence</strong></td>
<td></td>
</tr>
<tr>
<td>I.14.1. Structure all sort of valuable information</td>
<td></td>
</tr>
<tr>
<td>I.14.2. Identify evidential aspects</td>
<td></td>
</tr>
<tr>
<td>O.14.1. Group the evidential aspects</td>
<td></td>
</tr>
</tbody>
</table>
### Comments on Evidence Classification

#### Scenario

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process 14. Scenario Outline</strong></td>
<td></td>
</tr>
<tr>
<td>I.15.1. Use evidence as of I.1.1.&lt; Instruction 2, Phase 1&lt; ID Theft Data Identification, Phase 2&lt; Evidence, and Phase 3&lt; Evidence Classification</td>
<td></td>
</tr>
<tr>
<td>O.15.1. List valuable data gathered</td>
<td></td>
</tr>
<tr>
<td><strong>Process 15. Scenario Preparation Documentation</strong></td>
<td></td>
</tr>
<tr>
<td>I.16.1. Use Scenario outline list from O.15.1.</td>
<td></td>
</tr>
<tr>
<td>O.16.1. Merge evidential data gathered</td>
<td></td>
</tr>
</tbody>
</table>

### Comments on Scenario
Phase 4. Evaluation

Scenario Examination

<table>
<thead>
<tr>
<th>Processes, Activities, Instructions, Objectives</th>
<th>Corresponding Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process 17. Scenario Testing / Evaluation</td>
<td></td>
</tr>
<tr>
<td>I.17.1. Use Phase 1&lt; ID Theft Data Identification, Phase 2&lt; Evidence, and Phase 3&lt; Scenario</td>
<td></td>
</tr>
<tr>
<td>I.17.2. Check validation / entirety of the outputs</td>
<td></td>
</tr>
<tr>
<td>O.17.1. Create evaluation list</td>
<td></td>
</tr>
<tr>
<td>Process 18. Scenario Clarification</td>
<td></td>
</tr>
<tr>
<td>I.18.1. Use evaluation list from O.7.1.</td>
<td></td>
</tr>
<tr>
<td>I.18.2. Clarify the impact of evidential data</td>
<td></td>
</tr>
<tr>
<td>O.18.1. Create scenario clarification list</td>
<td></td>
</tr>
</tbody>
</table>

Comments on Scenario Examination
### Processes, Activities, Instructions, Objectives

<table>
<thead>
<tr>
<th>Process 19.</th>
<th>Case Construction</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.19.1. Use data from the scenario clarification list O.18.1</td>
<td></td>
</tr>
<tr>
<td>O.19.1. Construct the case</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process 20.</th>
<th>Case Clarification</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.20.1. Clarify the constructed case from O.18.1.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I.21.1. Use the scenario evaluation list from O.17.1.</td>
<td></td>
</tr>
<tr>
<td>I.21.2. Check validation</td>
<td></td>
</tr>
<tr>
<td>O.21.1. Confirm case evaluation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process 22.</th>
<th>Evidential Case Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.22.1. Create the testimonial report</td>
<td></td>
</tr>
<tr>
<td>Instruction 3. Include all case evidence</td>
<td></td>
</tr>
<tr>
<td>Instruction 4. Describe all case evidence</td>
<td></td>
</tr>
<tr>
<td>O.22.1. ID Theft Case Investigation Report</td>
<td></td>
</tr>
</tbody>
</table>

### Comments on Case
Appendix J:

Gwent Police Review
# Gwent Police HTCU

## ID Theft Investigation Framework

### Evaluation Questionnaire

**Officer’s Name:**  DC Tim Williams, Computer Crime Investigator  

**Date:**  27/5/08

Please answer the questions below after you have applied the ID Theft investigation framework on an existing case. Where applicable, you can rate your answer from 1 to 5 (Strongly disagree to strongly agree) by selecting the appropriate number. Some personal comments are desired as well.

1. How do you value the idea of discriminating the investigation of computer crimes based on their method?

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Totally</td>
<td>Partially</td>
<td>Agree</td>
<td>Partially</td>
<td>Totally</td>
</tr>
<tr>
<td>Agree</td>
<td>Agree</td>
<td></td>
<td>Disagree</td>
<td>Disagree</td>
</tr>
</tbody>
</table>

   Comments on rating: If the method of committing the crime is known and is reliable, then it is more efficient to concentrate your investigation efforts to areas known to be affected, rather than following the same routine for all offences

2. Considering this method of investigation do you believe it can correspond to a valuable tool for the investigator?

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Totally</td>
<td>Partially</td>
<td>Agree</td>
<td>Partially</td>
<td>Totally</td>
</tr>
<tr>
<td>Agree</td>
<td>Agree</td>
<td></td>
<td>Disagree</td>
<td>Disagree</td>
</tr>
</tbody>
</table>


Comments on rating:

3. Are the data flows and graphical representation of the framework supportive for the investigator?

<table>
<thead>
<tr>
<th></th>
<th>Totally Agree</th>
<th>Partially Agree</th>
<th>Agree</th>
<th>Partially Disagree</th>
<th>Totally Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disagree</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Comments on rating: Some of the graphical representations may need explaining to investigators before they are used. Although I can see that the graphical files are not meant to be used as a standalone description.

4. Do you believe that the procedure has the ability to speed up the investigation?

<table>
<thead>
<tr>
<th></th>
<th>Totally Agree</th>
<th>Partially Agree</th>
<th>Agree</th>
<th>Partially Disagree</th>
<th>Totally Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disagree</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Comments on rating: My disagreement isn’t a negative thing. The framework is comprehensive and would give an investigator more things to look at, which may have been overlooked or forgotten, therefore extending the initial examination, but this may lead to a time saving later on if there is no need to return to a case.

5. Do you believe that the framework identifies all evidential aspects related to Identity Theft incidents?

<table>
<thead>
<tr>
<th></th>
<th>Totally Agree</th>
<th>Partially Agree</th>
<th>Agree</th>
<th>Partially Disagree</th>
<th>Totally Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disagree</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Comments on rating: When applying the framework I did not discover anything missing that would have a detrimental effect on the investigation; neither could I think of anything else to add. However a framework, like software, will probably have a few minor bugs, and they will be discovered.
the more they are used. This framework appears to have the ability to be “tweaked” should the need arise.

6. Are the inputs and the outputs of the procedure properly defined?

<table>
<thead>
<tr>
<th>Totally</th>
<th>Partially</th>
<th>Agree</th>
<th>Partially</th>
<th>Totally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Agree</td>
<td></td>
<td>Disagree</td>
<td>Disagree</td>
</tr>
</tbody>
</table>

Comments on rating:

7. Are the inputs and the outputs those that you expected to identify?

<table>
<thead>
<tr>
<th>Totally</th>
<th>Partially</th>
<th>Agree</th>
<th>Partially</th>
<th>Totally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Agree</td>
<td></td>
<td>Disagree</td>
<td>Disagree</td>
</tr>
</tbody>
</table>

Comments on rating:

8. Do the aspects of the methodology assess the capabilities required from the perpetrator?

<table>
<thead>
<tr>
<th>Totally</th>
<th>Partially</th>
<th>Agree</th>
<th>Partially</th>
<th>Totally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Agree</td>
<td></td>
<td>Disagree</td>
<td>Disagree</td>
</tr>
</tbody>
</table>

Comments on rating:

9. Does the methodology effectively assess the on going threat?

<table>
<thead>
<tr>
<th>Totally</th>
<th>Partially</th>
<th>Agree</th>
<th>Partially</th>
<th>Totally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Agree</td>
<td></td>
<td>Disagree</td>
<td>Disagree</td>
</tr>
</tbody>
</table>

Comments on rating: Short term: yes. The method of ID theft is fluid and the criminals are constantly re-inventing themselves. Whilst we may have an idea of what is happening now and the methods being employed, this will change in the future as criminals get to know investigators capabilities. However the
framework is future-proof and new areas of examination can be added as
would any such procedure

10. Is the procedure generic enough in order to be applicable to all different
systems?

<table>
<thead>
<tr>
<th>Totally</th>
<th>Partially</th>
<th>Agree</th>
<th>Partially</th>
<th>Totally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Agree</td>
<td>Disagree</td>
<td>Disagree</td>
<td></td>
</tr>
</tbody>
</table>

Comments on rating: If by systems you mean Computer Operating systems,
then yes. I don’t think it would make any difference what computer was being
used. It does not limit the investigator

11. Does the framework facilitate the investigation of Internet Identity Theft
cases and the processing of the related digital evidence?

<table>
<thead>
<tr>
<th>Totally</th>
<th>Partially</th>
<th>Agree</th>
<th>Partially</th>
<th>Totally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Agree</td>
<td>Disagree</td>
<td>Disagree</td>
<td></td>
</tr>
</tbody>
</table>

Comments on rating: I didn’t have the opportunity to apply the framework to
an active search warrant, but the framework brings structure to gathering
digital evidence pre-delivery to the forensic lab, so I don’t see any particular
problem with this. The framework certainly brings structure to an
investigation. I have had moments in the past where I stare blankly into space
wondering what I am doing and where I am going. The framework brought a
structure I could follow and tick-off as I progressed the case.

12. Do you normally use evidence classification methods? If yes, how do you
normally classify the evidence?

Normally our evidence is either classed as admissible or not (but still
disclosable) there are varying strengths to admissible evidence, but this is not
normally broken down. With changes in law, what has been inadmissible can
now be used as evidence of bad character or knowledge and expertise of
computer systems. In criminal cases the evidence overall has to be of such strength as to be beyond all reasonable doubt. Civil cases are on a balance of probabilities. Therefore, the strength of the evidence will vary depending on the court hearing the case.

There is also a classification of evidence that undermines the prosecution and assists the defence, which has to be disclosed at some point during the prosecution.

13. Do you believe that the evidence classification presented by the ID Theft investigation framework is of your benefit?

<table>
<thead>
<tr>
<th>Totally Agree</th>
<th>Partially Agree</th>
<th>Partially Disagree</th>
<th>Totally Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comments on rating: from a Police/CPS perspective I think it will highlight where the strengths and weaknesses of a case are. I am not sure if classifying the evidence would require some additional work on the case or if this would aid the enquiry. My case did not require classification so I cannot comment further. It would need to be put into practice and commented on after a few applications.

14. Did you identify any additional evidential data by the use of the presented framework? (comparing to the methodology you normally apply)

I didn’t, but that is simply because the evidence wasn’t there. I did have extra logs and files to check thanks to the frame-work, which perhaps I would have missed or would have had to come back to at a later date.

15. Did you find the ‘Abstracted procedure for the investigator’ helpful during the analysis?

<table>
<thead>
<tr>
<th>Totally Agree</th>
<th>Partially Agree</th>
<th>Partially Disagree</th>
<th>Totally Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Comments on rating: There is enough of a description so that the investigator knows what is required

16. Did you find the ‘ID theft investigative methodology’ form helpful during the analysis?

<table>
<thead>
<tr>
<th>Totally Agree</th>
<th>Partially Agree</th>
<th>Partially Disagree</th>
<th>Totally Disagree</th>
</tr>
</thead>
</table>

Comments on rating: I didn’t use it. This is new to me so I needed the Abstracted procedure for the investigator document as it was a bit more descriptive. However, most of the headings are obvious as to what is required and with a few applications it would take over as the main document to follow

17. Any additional comments and recommendations.

There is always some reluctance to change the way an offence is investigated, but e-crime is becoming a very complex area of investigation with some serious offences being committed. It is becoming apparent that an investigator needs to complete a structured investigation that can be followed by others and reach the same conclusion and or results. The phrase “We need to be singing from the same song book” comes to mind.

I am not a fan of catch all check lists as you may have to spend time explaining to a court or defence barrister why you didn’t look at a particular area that is on the list (a check list is a disclosable document if used). The idea of a framework that is offence specific is more appealing

Using a framework that caters to a particular offence ensures that you do exactly what is required, keeps an investigator on-track, reduces the chance of overlooking an area where evidence could reside and affords some flexibility for the individual.
It is clear that a lot of work has gone into this framework and it fitted well into my case. It was a little difficult at first, but with repeated use this will get easier the more it is used as with any other new policy or procedure. I would certainly consider using it again when it is finally published. I also think it would make a good foundation for any offence specific investigations.
Appendix K

Gwent Police e-mail communication
1st e-mail contact: DC Jon Evans, Monday 19/05/2008

Hi Olga,

Just a quick email to confirm I have received the ID frame work evaluation and will be giving it attention in due course.
btw can I send this on to a contact I have within the NPIA (National Police Improvement Agency)?
http://www.npia.police.uk/

Regards,
Jon.

Angelopoulou O (AT) wrote:
>
> Dear Jon,
>
> Following our last contact, I'm grateful that you have agreed to
> evaluate my research project. I'm sending you the appropriate
> documentation that will help you comprehend the presented methodology,
> some flowcharts and graphs that support the design, a form that I
> would like you to fill in and a questionnaire that I would like you to
> answer.
>
> In order to make your life easier I need to summarise some key issues.
> As we have already discussed, the specified research work implements a
> conceptual ID Theft investigation framework. Initially the purpose is
> to maintain the idea that there should be a different methodology
> applied by the forensics investigator concerning the nature of
> different e-crimes. In addition, the methodology differentiates from
> others, by discriminating the analysis to the fraudster’s and the
> victim’s side, as different findings are requested from each side.
>
> The application of a conceptual framework may differ with the actual
> practical process and the procedure you already follow; however the
> purpose is to create a structured, formal approach to the procedure
> that needs to be undertaken.
>
> The framework consists of four phases and every phase is accomplished
Appendices

> in two processes. Every process requires a number of activities to be
> undertaken and produce appropriate outputs. As a result, the functions
> serve this need, receive inputs and produce outputs.
>
> The documents that I’m sending you are the last draft chapters of my
> PhD thesis; therefore, they are quite extended and detailed. For this
> reason, in some cases you will find references to some other chapters.
> Also the figures, graphs and references to appendices do not have
> correct numbering.
>
> The ‘Design’ file explains the purpose and the structure of the
> framework and you may find it useful for understanding how the
> framework works. The ‘Functionality of the ID Theft investigation
> framework’ is the chapter that analyses every process of the
> methodology. I suppose that you will need to refer to this one as
> well, for understanding the aim of every different function. The
> ‘Abstracted procedure for the investigator’ acts as a handbook that
> you may need to make use of. It includes the very basic purpose of
> every phase and its components and my intention is to provide it as a
> manual that the investigator can refer at any point during the
> analysis. The attached graphs and flowcharts represent the framework.
> Their filenames stand for the purpose of the graph or the flowchart.
>
> The ‘ID Theft investigative methodology’ file intends to aid the life
> of the investigator during the analysis and maintain the chain of
> custody. You are supposed to use the form when you apply the framework
> on the case, and keep track of the progress of the procedure. This
> form can also be used for producing the documentation of the case.
>
> The attached questionnaire should be answered after the application of
> the methodology. I would really appreciate it if some of your
> colleagues would like to fill in the questionnaire as well. In this
> case I could reach to more convincing results for the evaluation purposes.
>
> I hope the whole procedure will not consume much of your time.
>
> I would like to include the completed questionnaires as appendices to
> the thesis only with your permission. In case you don’t want your
names to be published, then these will be kept separately. Whether you
prefer the replies to remain unpublished, then the access to the
questionnaires will be restricted between me and my supervisor, Dr.
Ian Sutherland. Additionally, if you would like me to send you a copy
of the work that includes your feedback; I would be more than happy to
do so.

Your feedback is going to be of great value for the assessment of the
project and once again I would like to mention how much I appreciate
your help. Feel free to contact me anytime regarding any queries you
may have. In case you thought there is no deadline for your reply, I
would be just waiting for a prompt response.

Yours sincerely,

*Olga Angelopoulou*
Research Student
Faculty of Advanced Technology
University of Glamorgan
Pontypridd
CF37 1DL
United Kingdom
Tel: +44 (0)1443 483246
E-mail: oangelop@glam.ac.uk

2nd and 3rd e-mail contact: DC Tim Williams, 21/05/2008
Glad I could be of some help. Unfortunately I don’t have the time to go through all of the
descriptive notes, but the outline frame work doesn’t seem to be missing anything major in an
investigation of this type. You have obviously put a lot of effort into it and I wish you the best of
luck with it.

I will always be willing to help out where I can

Tim

From: Angelopoulou O (AT) [mailto:oangelop@glam.ac.uk]
Sent: 21 May 2008 10:01
To: DC Tim Williams
Subject: RE: ID theft Investigation framework eval

Hi Tim,

this is only a quick e-mail to say many many thanks for your reply.

I really appreciate it that you dedicated some of your time to write these comments, they are so valuable for me.

You have the practical experience, I don’t; and it’s so important to see your point of view.

I will consider your notes and send you back any necessary clarifications.

Thanks again,

Olga

Hi Olga,

I was enquiring the other day on how you were getting on with the framework. You must have heard me, because you emailed Jon with your draft.

I have had a look through the Framework, but not had a chance to go through all of the descriptive notes that go with each point. I have only really looked at the descriptive notes where I marked some points of interest.

I have a few things that might be worth consideration. However, bear in mind I have not read all the notes so they may already be covered and/or are just not necessary for your framework.

Point 1.1 covers offline data. Routers are becoming the norm in most households and may be worth mentioning separately as an item to seize and interrogate. Most now have security logs and DHCP lists or show deliberate access through a firewall or port forwarding.

Point 1.1 also covers recording the scene (photo and video) Is it worth mentioning that these also become exhibits and need to be handled in the same fashion as any other.

Point 1.1.5 covers packaging exhibits, How about the “sealing” of evidence bags to show that they have not been tampered with during transit or storage.
Point 1.3 covers acquisition which is then broken down into sub-points. It might be worth rearranging them so that protection from alteration of media is higher on the list. Select appropriate tool left as first and then protect the media (hardware write blockers etc) then on to the imaging.

Where you mention checksums to ensure integrity, I usually highlight that the created checksums were compared to the checksums of the original media for verification.

Point 3.1.1 It is probably encompassed within Existing Files, but is it worth mentioning compressed files separately? Not all forensic programs mount zipped files and as you know text is not searchable in a compressed files. Furthermore most virus checkers will mount and scan a compressed file, but if another compressed file is within the archive it will not be scanned. I have seen a few Trojans being hidden in this fashion.

Point 1.3.6 to 1.3.16 - Have you thought about checking virus vaults and virus program logs on the victim computer

Point 1.3.18 I attended a lecture recently on steganography, It was mentioned that we should compare md5 hash values on identical images with the same byte size if we suspect steganography is being used. Although not conclusive it could help especially if the victims computer is also available to run a search on the hash value

Point 1.3.24 URL information. Although covered in point 1.3.27 I also like specifically to check typed URLs in the registry, this shows an intention to visit the site and it cannot be blamed on a "pop-up".

Point 4.1.1.1 - 4.1.1.8 - I know this isn’t a definitive list but Credit card numbers might be worth an entry on its own. Encase has a script to locate them and they can identify a victim(s)

Point 4.2 - Mentions Evidence classifications. Have you thought about unused material whereby a file is known from the beginning that it has no evidential value. It often becomes an issue in court when it is overlooked and not disclosed. Although not strictly evidence, the defence will assume that it is the "best evidence" to clear their client when not disclosed properly and will accuse the police of deliberately hiding it. So it needs to be handled properly and made known.

Have you also considered classifying data that actually undermines the prosecution or supports the defence? This evidence still needs to be disclosed.
Point 8 presentation of the evidence. Most of the time I find that I need to really dumb down my reports, avoid wherever possible anything too technical and keep it simple. So it would be worth an investigator thinking about the audience that will be reading the report and cater to them accordingly

Lastly have you considered securing remote data stored on a server eg googlemail with 6Gb storage for files and emails. This is not covered in a warrant, but might host a wealth of evidence. It is an absolute nightmare getting to this, due to territorial problems, but should be considered prior to executing a warrant as the fraudster could access it post-warrant and delete the lot. Although this might be in need of its own framework

I hope this could be of some help to you. Don't worry about responding to the above points, I only throw them in for you to consider just in case you have overlooked something. I have not been able to apply the framework to a live job, as I do not have a job that fits the criteria at the moment.

However it does seem to be a complete and comprehensive coverage of handling an ID theft. I do like the idea of a framework as it prevents overlooking some crucial part of an investigation and frameworks are present in so many other areas of policing.

Best of luck with this and if there is anything I can do to help just drop me a line.

Tim
DC 459 Tim Williams
Computer crime Investigator
Gwent Police Hi-tech Crime Unit
Police HQ
Cwmbran
Gwent
Np44 2XJ
Tel 01633 643032
Fax 01633 877643

4th and 5th e-mail contact: DC Tim Williams, 23/05/2008
I am sure I can find a few past cases that I can put this to or at least something close. Obviously I may have to miss out certain parts, but I am sure that your framework is modular so I don’t anticipate any problems. I will look at it next week and email the results back to you. If you prefer a paper copy for authenticity I can post them.

Have a good weekend

Tim

From: Angelopoulou O (AT) [mailto:oangelop@glam.ac.uk]
Sent: 23 May 2008 10:37
To: DC Tim Williams
Subject: RE: ID theft Investigation framework eval

Hello Tim,

thank you for the additional observations. Both comments were really useful.

I respect that your time is limited, and really appreciate it that you’ve sent me all these comments. I thought from the beginning that it would be quite probable for you not to have an ID theft incident for a long time after I sent you the framework. The framework is more a theoretical than a practical approach to the investigation, in order to be as general as possible. Even if you have an already solved case on your mind and you would like to apply it in theory in order to see whether you can reach the same results and answer the questionnaire, then it would be great for me. Just to show concentrated results from your evaluation in the thesis. I know that you have already spent quite a few hours reading the framework and trying to understand how it works and I don’t intend to be awkward. Even if you don’t complete the questionnaire, I am still able to use your comments as a personal contact.

Thanks again.

Regards,

Olga

From: DC Tim Williams [mailto:timwilliams@gwentpolice.org]
Sent: Fri 23/05/2008 09:12
To: Angelopoulou O (AT)
Subject: RE: ID theft Investigation framework eval

Olga,

1 other point I forgot to mention, Within your notes for "The functionality of the ID Theft investigation framework.pdf" You mention shutdown the computer or simply unplug. Investigators are taught to pull the plug from the back of the computer not the wall socket, just in case there is a backup power supply. We are also taught that if the machine is a server running a server OS, then it should be shut down as you would normally (especially if the server is used for a business) This is to avoid the risk of data corruption which could lead to problems for the business.

Jon is going to try and look over it this weekend, he has been busy on a warrant and not had the time yet. He did mention that under the classifications of evidence, a sub heading or mention of intelligence could be a bonus. Sometimes we look at computers and the evidence is insufficient for a prosecution, but we do gather intelligence from it, emails, contacts and financial records etc.

If I get a job I can use this on I will complete the questionnaire, but there is no case of ID theft outstanding yet and no warrants planned for the next few weeks.

Regards

Tim

6th e-mail contact: DC Tim Williams, 27/05/2008

Olga,

Attached is a questionnaire that I have completed in respect of a case that I had finished, but used the framework to review my work. It wasn’t a straightforward ID theft, but I used it just the same. There are some questions I couldn’t answer, either because I wasn’t sure of what was being asked, or it just didn’t fit with the job I had done. If some of the answers are not in context to the question, just put it down to me not understanding the question!

Hope it helps out. Anything else, just drop me a line.

Tim
Appendix L

EnCase Victim Report
Victim Investigation – Evidential Files ScreenShots

Figure 33: Victim’s Hash Value
Figure 35: E-mail addresses
Figure 36: My Documents folder
Appendix M

EnCase Fraudster Report
Fraudster Investigation – Evidential Files ScreenShots
Figure 37: Fraudster's Internet Bookmarks
Figure 38: Victim’s log on fraudster’s system
Figure 39: malware.zip file from plugged in device