Architecture and Design of Process Based Framework for Mobile Forensics (PBFMF)

Masoud. H. Al Tawqi

Submitted for the Degree of
Doctor of Philosophy
from the
University of Surrey

Institute for Communication Systems (ICS)
Department of Electronic Engineering
Faculty of Electronics and Physical Sciences
University of Surrey
Guildford, Surrey GU2 7XH, UK

June 2017

© M.H. Al Tawqi 2017
Abstract

Over the last two decades, the world has witnessed a vast increase in smart phones devices usage, where mobile phone devices have become an integral part of our daily routine. As a result, this has created security issues and lead to an increased dependency on smartphone usage, criminal activities and/or illegal practices. This increase in crimes committed by or via smartphones has made it a necessity for digital forensics experts to come up with reliable tools that can be used to help in extracting data from those smart phones.

Currently mobile forensics work is fragmented and although attempts have been made to develop conceptual frameworks for mobile devices in the past few years, there is however, no common framework adopted to date that meets the needs of the ever changing and expanding world of mobile devices. A comprehensive survey of mobile forensics frameworks in this research revealed that current frameworks tend to focus on targeting specific operating systems, responding to specific issues, or use complicated steps that make it difficult for users to follow. Some are also based on desktop and non-mobile device models. Also, tools analysis was carried out benefitting from NIST guidelines, where areas in which each tool should be tested and how the test should be conducted are specified. The results of the Tools Analysis were not encouraging, and quite surprising that many challenges that existed at the advent of the mobile devices have not been solved.

Without the existence of a generalized Process Based Framework for Mobile Forensics (PBFMF) to provide the appropriate guidelines, steps and procedures to be followed during the digital forensic phases, it will not be as simple as it might appear to extract data in an appropriate way from smartphones even with the utilisation of the most popular tools. Based on the research and analysis in this thesis, it was clear that there is a need for a set of effective methods to ensure that extracted and examined information from mobile phones devices are not tampered with, accepted by a court of law, or can be relied upon as an undisputed means of proving that something has or has not taken place. A new PBFMF that is platform independent, open architecture, extensible and capable of integrating newer mobile device technologies is presented in this thesis. It formulates a better understanding of the barriers to using forensics tools effectively and appropriately.

Key words: Processed Base Framework, Mobile Forensics Tools, Digital Forensics, Operating Systems, Smart Phones.

Email: m.altawqi@surrey.ac.uk
Acknowledgments

First of all, I thank almighty Allah for helping me to accomplish this work by giving me the health, inspiration and confidence. Second, I would like to thank all those who helped me during this research period and made this project possible. In particular, I extend my great gratitude and special thanks to my supervisors, Dr. Haitham Cruickshank and Prof. Zhili Sun for their generous assistance, confidence building, guidance and encouragement to embark this project.

Many thanks also to my colleagues and friends especially my best friend Mr. Khalid Al-Maskari, for the endless support and help I received from him, without his assistance and encouragement, it would have been difficult to accomplish this study. I also thank MoHE, CRAFO, my best friends Col. Saleh Al-Maskari, Hisham Al-Binali and Yousuf Al-Harthy for their encouragement and support.

I would like to explore my deep love and appreciation to my father, Sheikh Humaid Abdullah Rashed Al-Tawqi, who died in 1994, and to my mother, Zwaina Mohamed Al-Namani. Their love was a source of motivation throughout the years of my education and in my personal life. My love and appreciation are also extended to my brothers and sisters.

My most sincere gratitude is due to my wife, Jokha Al Suqri, for her patience and encouragement throughout my accomplishments. Her unending support made this project possible. Finally, I come to my children, my sons, Humaid and Abdullah, and my daughters Misk, Teeb and Shatha, to whom I am grateful for their love, patience, and understanding, in view of the many years, months, days and hours that this study has taken away from our time together.
Dedication

To my family and my beloved ones. I dedicate this work to thank the Almighty God for the journey so far.
Contents

ABSTRACT ................................................................................................................................. II

ACKNOWLEDGMENTS ............................................................................................................... III

DEDICATION .............................................................................................................................. IV

CONTENTS ............................................................................................................................... V

LIST OF FIGURES ..................................................................................................................... XI

LIST OF TABLES ....................................................................................................................... XIV

GLOSSARY OF TERMS ............................................................................................................. XV

TERMINOLOGY LIST OF DEFINITIONS .................................................................................. XVIII

1 INTRODUCTION ...................................................................................................................... 1
   1.1 MOTIVATION ....................................................................................................................... 2
   1.2 RESEARCH OBJECTIVES .................................................................................................. 3
   1.3 PROBLEM STATEMENT ..................................................................................................... 4
   1.4 METHODOLOGY ............................................................................................................... 5
   1.5 RESEARCH CONTRIBUTIONS .......................................................................................... 7
   1.6 STRUCTURE OF THE REPORT ........................................................................................ 8

2 MOBILE FORENSICS TECHNICAL REVIEW ....................................................................... 10
   2.1 BACKGROUND .................................................................................................................. 10
   2.2 SMART-PHONE DEVICE OPERATING SYSTEM TECHNOLOGIES .................................. 11
       2.2.1 Google Operating System (Android) .......................................................................... 14
       2.2.2 Apple’s Operating System (iOS) ................................................................................. 15
   2.3 CELLULAR NETWORK CHARACTERISTICS AND OPERATING SYSTEMS .................. 16
   2.4 FORENSIC PROCEDURES ................................................................................................ 17
   2.5 FORENSIC PHASES .......................................................................................................... 19
       2.5.1 Preservation and Handling ......................................................................................... 20
       2.5.2 Extraction and Storage ............................................................................................. 22
       2.5.3 Examination and Analysis .......................................................................................... 27
       2.5.4 Reporting .................................................................................................................... 29
   2.6 CAUSES AND FACTORS CONTRIBUTING TO THE PROBLEM ..................................... 30
2.7 FACTS AND STATISTICS HIGHLIGHTING DIGITAL FORENSICS CHALLENGES ........................................... 33
2.8 CURRENT AREAS OF INTEREST AND RELATED RESEARCH ................................................................. 34
2.9 RIGHTS OF PRIVACY AND ANONYMITY ..................................................................................................... 36
  2.9.1 Privacy Background over the Net ........................................................................................................... 37
  2.9.2 Examples of Privacy Related Issues ....................................................................................................... 38
  2.9.3 Laws related to privacy ............................................................................................................................ 38
  2.9.4 Smart-phone Devices Security ............................................................................................................... 39
  2.9.5 Smart-phone Devices Usability ............................................................................................................... 39
  2.9.6 Importance of Privacy ........................................................................................................................... 40
2.10 SUMMARY.................................................................................................................................................. 40

3 MOBILE FORENSICS TOOLS ANALYSIS ................................................................................................. 42
  3.1 INITIAL MOBILE FORENSICS TOOLS ANALYSIS .................................................................................. 44
    3.1.1 Oxygen Forensic Suite 2014 ................................................................................................................ 46
    3.1.2 Computer Aided Investigative Environment (CAINE) 5.0 ............................................................... 48
    3.1.3 Digital Evidence & Forensics Toolkit (DEFT) 8 ................................................................................. 50
  3.2 ADVANCED MOBILE FORENSICS TOOLS ANALYSIS ........................................................................... 52
    3.2.1 MobilEdit Analyst v 8.5 Forensic Tool ................................................................................................. 53
    3.2.2 Mobile Phone Examiner Plus v 5.6.0.8 ............................................................................................... 56
    3.2.3 Autopsy v4.0 ......................................................................................................................................... 60
    3.2.4 Device Seizure v 7.4 .............................................................................................................................. 62
    3.2.5 NowSecure Community Edition v 3.2 .............................................................................................. 65
  3.3 SUMMARY.................................................................................................................................................. 67

4 FORENSICS FRAMEWORKS ANALYSIS ................................................................................................. 71
  4.1 A FRAMEWORK FOR DESIGNING BENCHMARKS FOR MOBILE DEVICES .............................................. 72
    4.1.1 Overview ............................................................................................................................................... 72
    4.1.2 Analysis ............................................................................................................................................... 72
    4.1.3 Recommendation ............................................................................................................................... 73
  4.2 TOWARDS A UNIFIED FORENSIC FRAMEWORK ..................................................................................... 73
    4.2.1 Overview ............................................................................................................................................... 73
    4.2.2 Analysis ............................................................................................................................................... 74
    4.2.3 Recommendation ................................................................................................................................... 75
  4.3 ONTOLOGY-BASED FORENSIC ANALYSIS ............................................................................................. 75
    4.3.1 Overview ............................................................................................................................................... 75
    4.3.2 Analysis ............................................................................................................................................... 76
    4.3.3 Recommendation ................................................................................................................................... 76
4.4 **FORENSICS METHODOLOGY FOR PRIVACY ASSESSMENT** ............................................................. 77
   4.4.1 Overview................................................................................................................................. 77
   4.4.2 Analysis................................................................................................................................. 78
   4.4.3 Recommendation.................................................................................................................. 78
4.5 **TESTING THE HDFI PROCESS MODEL** ................................................................................. 79
   4.5.1 Overview................................................................................................................................. 79
   4.5.2 Analysis................................................................................................................................. 79
   4.5.3 Recommendation.................................................................................................................. 81
4.6 **DEVELOPING PROCESS FOR MOBILE DEVICE FORENSICS** ........................................... 81
   4.6.1 Overview................................................................................................................................. 81
   4.6.2 Analysis................................................................................................................................. 82
   4.6.3 Recommendation.................................................................................................................. 83
4.7 **DATA MINING BASED ANALYSIS** ......................................................................................... 83
   4.7.1 Overview................................................................................................................................. 83
   4.7.2 Analysis................................................................................................................................. 84
   4.7.3 Recommendation.................................................................................................................. 84
4.8 **EFFICIENT FRAMEWORK FOR MOBILE DEVICES** ......................................................... 85
   4.8.1 Overview................................................................................................................................. 85
   4.8.2 Analysis................................................................................................................................. 86
   4.8.3 Recommendation.................................................................................................................. 86
4.9 **LIMITATIONS OF DISCUSSED FRAMEWORKS** ................................................................. 86
   4.9.1 Most of the research done is specific to Android based devices............................................. 86
   4.9.2 The methods used are focused on solving a specific issue..................................................... 86
   4.9.3 Lack of data mining techniques.............................................................................................. 87
   4.9.4 No mention of utilizing big data............................................................................................ 87
   4.9.5 Need for an open ended, extensible framework................................................................. 87
   4.9.6 Too many steps are used...................................................................................................... 87
   4.9.7 Too difficult to create a single program................................................................................. 88
   4.9.8 Need for a truly generalized framework specific to mobile forensics................................. 88
   4.9.9 Many obstacles by industry in creating standards for mobile forensics............................... 88
4.10 **SUMMARY** ............................................................................................................................ 88

5 **PROPOSED FRAMEWORK ARCHITECTURE AND DESIGN** ................................................. 90
   5.1 **BENCHMARKS USED FOR FRAMEWORK DESIGN** ............................................................ 91
   5.2 **DESIGN GOALS** .................................................................................................................. 91
      5.2.1 Platform Independent (Cross platform) and open architecture......................................... 92
5.2.2 Simplified design
                        ........................................................................................................... 93
5.2.3 Preserves the integrity of the evidence
                        ........................................................................................................... 93
5.2.4 Streamlined Reporting
                        ........................................................................................................... 93
5.2.5 Extensible framework to accommodate IoT and other future technologies
                        ........................................................................................................... 93
5.3 Community wide acceptance
                        ........................................................................................................... 93
5.4 Mobile data privacy
                        ........................................................................................................... 94
5.5 The Proposed Process Based Framework for Mobile Forensics Tools (PBFMF) ........................................ 95
  5.5.1 First Responder Triage (Preservation)
                        ........................................................................................................... 95
  5.5.2 Acquisition
                        ........................................................................................................... 104
  5.5.3 Analysis
                        ........................................................................................................... 107
  5.5.4 Reporting
                        ........................................................................................................... 107
5.6 Abstract Model
                        ........................................................................................................... 109
5.7 Summary
                        ........................................................................................................... 110

6 EVALUATION OF THE PROPOSED PROCESS BASED FRAMEWORK (PBFMF) .............................................. 112

  6.1 Application of the PBFMF Framework (1st Scenario)
                        ........................................................................................................... 112
    6.1.1 Arrival on the Scene
                        ........................................................................................................... 113
    6.1.2 Documenting the scene
                        ........................................................................................................... 113
    6.1.3 Identify State of the Device
                        ........................................................................................................... 115
    6.1.4 Write Blocker
                        ........................................................................................................... 115
    6.1.5 Connect Approved Tools
                        ........................................................................................................... 116
    6.1.6 Acquisition
                        ........................................................................................................... 120
    6.1.7 Analysis
                        ........................................................................................................... 125
    6.1.8 Reporting
                        ........................................................................................................... 125

  6.2 Application of the Framework (2nd Scenario)
                        ........................................................................................................... 125
    6.2.1 State of the Device
                        ........................................................................................................... 126
    6.2.2 Connect approved tools
                        ........................................................................................................... 126
    6.2.3 Acquisition
                        ........................................................................................................... 127
    6.2.4 Analysis
                        ........................................................................................................... 128
    6.2.5 Reporting
                        ........................................................................................................... 131

  6.3 Comparing other frameworks to the PBFMF
                        ........................................................................................................... 132
    6.3.1 Developing Process for Mobile Device Forensics
                        ........................................................................................................... 132
    6.3.2 Implementing Digital Forensic Framework for Android Smart Phones
                        ........................................................................................................... 133

  6.4 Summary
                        ........................................................................................................... 135

7 CONCLUSION AND FUTURE WORK
                        ........................................................................................................... 136

  7.1 Conclusion
                        ........................................................................................................... 136
APPENDIX B: FRAMEWORK GUIDELINES FOR WEB-BASED TOOL DEVELOPMENT .... 193
List of Figures

Figure 2-1: Mobile Device Tool Classification System[47] .......................................................... 25
Figure 2-2: FTK Screenshot Usability Survey [67] ........................................................................ 31
Figure 2-3: Encase Screenshot Usability Survey [67] .................................................................... 31
Figure 2-4: Mock-up Reporting Tool Presented in the Survey [67] .................................................. 33
Figure 2-5: The RFID is shown as the little black dot [78] .............................................................. 38
Figure 3-1: Oxygen Forensic Extractor Screen .................................................................................. 47
Figure 3-2: Oxygen Forensic Reporting Information Screen ............................................................ 47
Figure 3-3: Oracle VM VirtualBox Manager ..................................................................................... 49
Figure 3-4: CAINE Mobile Forensics Tools ...................................................................................... 49
Figure 3-5: IP Backup Analyser ........................................................................................................ 50
Figure 3-6: DEFT Mobile Forensics tools ........................................................................................ 51
Figure 3-7: IP Backup Analyser 2 Plugins and Reports Menu ............................................................ 51
Figure 3-8: iPhone 4 Recovered Image of the Logical File Information ............................................. 55
Figure 3-9: An Image showing that the Tool is a 20 Day Free Trial .................................................. 57
Figure 3-10: Device Seizure Trial Version limits the Recovery to Contacts ....................................... 63
Figure 3-11: An Image showing that Logical Extraction is possible with Full Version Only ............. 65
Figure 3-12: An Example of an Image Acquired by NowSecure Community Edition v3.2 .......... 66
Figure 4-1: Windows Mobile Device Forensics Model [34] ................................................................ 74
Figure 4-2: Symbian Mobile Forensics Model [34] ......................................................................... 74
Figure 4-3: Ontology-Based Mobile Device Framework [36] ............................................................ 76
Figure 4-4: HDFI Model [37] .......................................................................................................... 80
Figure 4-5: Evidence Extraction Phases [98] .................................................................................... 82
Figure 4-6: Android OS Architecture [33] ...................................................................................... 85
Figure 5-1: PBFMF Design Goals ................................................................................................... 92
Figure 5-2: PBFMF is a Cross Platform and an Open Architecture .................................................. 92
Figure 5-3: Example of a Faraday Bag .............................................................................................. 98
Figure 5-4: Example of a Write blocker .......................................................................................... 99
Figure 5-5: An Abstract Example of the First Responder Triage Process ....................................... 104
Figure 5-6: An Abstract Example of the On-Site Acquisition Process ............................................ 105
Figure 5-7: An Abstract Example of the Laboratory Acquisition Process ........................................ 106
Figure 5-8: A Representation of the Reporting Process Steps ......................................................... 109
### List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-9</td>
<td>The Abstract Model Representation of the PBFMF</td>
<td>110</td>
</tr>
<tr>
<td>6-1</td>
<td>Crime scene Photo with identification of the device</td>
<td>114</td>
</tr>
<tr>
<td>6-2</td>
<td>Viewable Contacts in the device</td>
<td>114</td>
</tr>
<tr>
<td>6-3</td>
<td>Browser’s Bookmarks</td>
<td>115</td>
</tr>
<tr>
<td>6-4</td>
<td>Paraben Mobile Device Portable Acquisition System</td>
<td>116</td>
</tr>
<tr>
<td>6-5</td>
<td>Santoku Features</td>
<td>117</td>
</tr>
<tr>
<td>6-6</td>
<td>Santoku initial boot options</td>
<td>117</td>
</tr>
<tr>
<td>6-7</td>
<td>Santoku device forensics tools</td>
<td>118</td>
</tr>
<tr>
<td>6-8</td>
<td>LG device USB options</td>
<td>118</td>
</tr>
<tr>
<td>6-9</td>
<td>Android Phone in the VM</td>
<td>119</td>
</tr>
<tr>
<td>6-10</td>
<td>Connected device</td>
<td>120</td>
</tr>
<tr>
<td>6-11</td>
<td>Successful push of the package to the device</td>
<td>121</td>
</tr>
<tr>
<td>6-12</td>
<td>AFL Logical extraction options</td>
<td>121</td>
</tr>
<tr>
<td>6-13</td>
<td>Extracted device data</td>
<td>122</td>
</tr>
<tr>
<td>6-14</td>
<td>Extracted data folders</td>
<td>122</td>
</tr>
<tr>
<td>6-15</td>
<td>Mobiledit dashboard</td>
<td>123</td>
</tr>
<tr>
<td>6-16</td>
<td>Backup in progress</td>
<td>124</td>
</tr>
<tr>
<td>6-17</td>
<td>Data backup results</td>
<td>125</td>
</tr>
<tr>
<td>6-18</td>
<td>Mobiledit with connected device</td>
<td>127</td>
</tr>
<tr>
<td>6-19</td>
<td>Successful backup of the device data</td>
<td>127</td>
</tr>
<tr>
<td>6-20</td>
<td>Mobiledit recovered data</td>
<td>128</td>
</tr>
<tr>
<td>6-21</td>
<td>Thumbnail images of requested evidence</td>
<td>129</td>
</tr>
<tr>
<td>6-22</td>
<td>Connection to the ADB</td>
<td>129</td>
</tr>
<tr>
<td>6-23</td>
<td>Andriller launched in Santoku</td>
<td>130</td>
</tr>
<tr>
<td>6-24</td>
<td>Extraction in process</td>
<td>130</td>
</tr>
<tr>
<td>6-25</td>
<td>Failed escalation attempt</td>
<td>134</td>
</tr>
<tr>
<td>A-1.1</td>
<td>An Image of the Logical File information Recovered from the iPhone4</td>
<td>151</td>
</tr>
<tr>
<td>A-1.2</td>
<td>Discovered Artifact of a Graphic Image of the Logical Acquisition</td>
<td>154</td>
</tr>
<tr>
<td>A-2.1</td>
<td>An Example of the Information Recovered from the Rooted Android</td>
<td>160</td>
</tr>
<tr>
<td>A-3.1</td>
<td>An Image of the Email Information Recovered from the Rooted Android</td>
<td>169</td>
</tr>
<tr>
<td>A-3.2</td>
<td>An Example of Emails Discovered by Autopsy</td>
<td>169</td>
</tr>
<tr>
<td>A-4.1</td>
<td>An Example Showing that DSTrial Version Tool Recovers Contacts Only</td>
<td>178</td>
</tr>
<tr>
<td>A-4.2</td>
<td>An Image of Failed Connection on Rooted Samsung by Device Seizure</td>
<td>181</td>
</tr>
<tr>
<td>A-5.1</td>
<td>NowSecure Community Edition Acquired Information of Samsung Device</td>
<td>187</td>
</tr>
<tr>
<td>B-1</td>
<td>Overview of the Proposed Framework Phases Representation</td>
<td>194</td>
</tr>
</tbody>
</table>
List of Figures

Figure B-2: Overview of the Proposed Forensics Output Framework and Tool Model............. 196
Figure B-3: Overview of the Proposed Model Design and Information Flow.......................... 197
Figure B-4: The Website, www.mobileforensicsanalysis.com, to import Programs Results ...... 198
Figure B-5: The Website provides the User with a Way to upload the Results File.................. 198
List of Tables

Table 2-1: Summary of Various Operating Systems ................................................................. 13
Table 2-2: Summary of current areas of interest and related research ................................... 36
Table 3-1: Summary of Top Digital Forensics Tools ................................................................. 44
Table 3-2: Summary of Tools used for Analysis and Framework Development ....................... 45
Table 3-3: Summary of Phones and Operating Systems used with Various Forensics Tools ..... 45
Table 3-4: Tested Mobile Devices .............................................................................................. 53
Table 3-5: Summary of Tools Analysis Findings ........................................................................ 68
Table 3-6: Summary of Tools Analysis Findings ........................................................................ 70
Table 4-1: Selected Applications and if data at rest is stored in clear text [44] ......................... 77
Table 4-2: Summary of Frameworks Analysis and Findings ..................................................... 89
Table 5-1: Analysed Forensic Frameworks compared to the proposed PBFMF ......................... 111
Table A-1. 1: Tested Mobile Devices used for Testing MobilEdit – Analyst version 8.5 ............ 150
Table A-1. 2: Data Objects and Elements used for Populating Analysed Mobile Devices .......... 153
Table A-1. 3: MobilEdit Analyst v8.5 Findings of Android and iOS Mobile Devices ................. 156
Table A-2. 1: Tested Mobile Devices used for Testing MPE Plus version 5.6.2.0 ....................... 159
Table A-2. 2: Data Objects and Elements used for Populating Analysed Mobile devices ......... 162
Table A-2. 3: MPE Plus version 5.6.2.0 Findings of Android and iOS Mobile Devices ............... 165
Table A-3. 1: Tested Mobile Devices used for Testing Autopsy version 4.0 ............................... 168
Table A-3. 2: Data Objects and Elements used for Populating Analysed Mobile Devices .......... 171
Table A-3. 3: Autopsy version 4.0 Findings of Android and iOS Mobile Devices ....................... 174
Table A-4. 1: Tested Mobile Devices used for Testing Device Seizure version 7.4 .................... 177
Table A-4. 2: Data Objects and Elements used for Populating Analysed Mobile Devices .......... 180
Table A-4. 3: Device Seizure version 7.4 Findings of Android and iOS Mobile Devices ............. 183
Table A-5. 1: Tested Mobile Devices used for Testing NowSecure Community Edition v3.2 .... 186
Table A-5. 2: Data Objects and Elements used for Populating Analysed Mobile Devices .......... 189
Table A-5. 3: NowSecure Findings of Android and iOS Mobile Devices .................................. 192
Table C- 1: Mobile Device Tool Specification ............................................................................ 205
Glossary of Terms

ACPO – Association of Chief Police Officers

ADF – Anti Digital Forensics

API – Application Program Interfaces

APK – Application Package File

BSD – Berkeley Software Distribution, sometimes called Berkeley Unix

BYOD – Bring Your Own Device

CAINE 5 – Computer Aided Investigative Environment version 5

CCTV – Closed Circuit Television

CDMA – Code Division Multiple Access

CNIC – Cellular Network Isolation Card

CFTT – Computer Forensics Tool Testing

CSV – Comma-Separated Values/ Character-Separated Values

DEFT 8 – Digital Evidence & Forensics Toolkit version 8

DFRWS – Digital Forensic Research workshop

ECHR – European Convention on Human Rights

EPL – Eclipse Public License

EKA2 – EPOC Kernel Architecture 2

EU – European Union

FAT – File Allocation Table

FTK – Forensics Tool Kit

GPS – Global Positioning System

GREP – Generalized Regular Expression Patterns

GSM – Global System for Mobile Communications

HCI – Human Computer Interaction
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCI-S</td>
<td>Human Computer Interaction Security</td>
</tr>
<tr>
<td>HDFI</td>
<td>Harmonised Digital Forensic Investigation</td>
</tr>
<tr>
<td>HFS</td>
<td>Hierarchical File System</td>
</tr>
<tr>
<td>HPA</td>
<td>Host-protected Areas</td>
</tr>
<tr>
<td>IIA</td>
<td>Intelligent Investigation Algorithm</td>
</tr>
<tr>
<td>ICCID</td>
<td>Integrated Circuit Card Identification</td>
</tr>
<tr>
<td>ICF</td>
<td>Internet Connection Firewall</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>iDEN</td>
<td>Integrated Digital Enhanced Network</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IPPs</td>
<td>Information Privacy Principles</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>JTAG</td>
<td>Joint Test Action Group</td>
</tr>
<tr>
<td>MFP</td>
<td>Mobile Forensic Program</td>
</tr>
<tr>
<td>MIAT</td>
<td>Mobile Internal Acquisition Tool</td>
</tr>
<tr>
<td>MMS</td>
<td>Multimedia Messaging Service</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Station International Subscriber Directory Number</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>NPPs</td>
<td>National Privacy Principles</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PAAP</td>
<td>Preservation, Acquisition, Analysis and Presentation</td>
</tr>
<tr>
<td>PBF</td>
<td>Process Based Framework</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
</tbody>
</table>
PUK – Personal Unblocking Key
RDF – Resource Description Framework
RFID – Radio Frequency Identification
RIM – Research in Motion
RTOS – Real-time Operating System
SANS – System Administration, Networking, and Security Institute
SDFT – Smart-phones Digital Forensics Tools
SDK – Software Development Kit
SIM – Subscriber Identity Module
SMS – Short Message Service
TXT – Text File (existing within a computer file system)
UICC – Universal Integrated Circuit Card
UN – United Nations
USB – Universal Serial Bus
USIM – Universal Subscriber Identity Module
VOIP – Voice over IP
WMSs – Windows Mobile Smart-phones
XML – eXtensible Mark-up Language
Terminology List of Definitions

Andriller: is software utility with a collection of forensic tools for smartphones. It performs read-only, forensically sound, non-destructive acquisition from Android devices. It has other features, such as powerful Lock screen cracking for Pattern, PIN code, or Password; custom decoders for Apps data from Android (and some Apple iOS) databases for decoding communications [1].

Android: A mobile operating system developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets [2].

Airplane Mode: A setting available on many smartphones, portable computers, and other electronic devices that, when activated, suspends radio-frequency signal transmission by the device, thereby disabling Bluetooth, GPS, telephony, and Wi-Fi [3].

Big Data Analysis: A term for a large data set that outgrow the simple kind of database and data handling architectures that were used in earlier times, when big data was more expensive and less feasible [4].

Core Requirements: A requirement that every forensic tool must feature so that it remains consistent with all types of smart-phones.

Data at Rest: Generally refers to data stored in persistent storage (disk, tape) [5].

Database format (SQLite): An in-process library that implements a self-contained, serverless, zero-configuration, transactional SQL database engine. Unlike most other SQL databases, SQLite does not have a separate server process [6].

Data Mining: refers to the activity of going through big data sets to look for relevant or pertinent information [4].

Digital Forensics: 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 facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations [7].

Exculpatory Evidence: Evidence favourable to the defendant in a criminal trial that exonerates or tends to exonerate the defendant of guilt [8].
**Flasher Tools:** Is an application which mainly helps you to flash Stock ROM, Custom recovery and fixes in some extreme cases (firmware update, Flash recovery, unbrick bricked android device etc.) [9].

**Framework:** A layered structure indicating what kind of programs can or should be built and how they would interrelate [10].

**Inculpatory Evidence:** Evidence that shows, or tends to show, a person's involvement in an act, or evidence that can establish guilt [11].

**Investigators:** Law enforcement officers, who may lack the technical knowledge but mainly engaged from the criminal investigation aspects.

**iOS:** A mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod touch [12].

**Jailbreak:** an instance of gaining access to the operating system of an Apple smartphone to remove restrictions imposed by the manufacturer or operator [13].

**Mobile Forensics:** is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions [14].

**Mobile Law:** The emerging legal discipline and jurisprudence that impacts, pertains to, is associated with or has a bearing upon complicated legal issues concerning mobiles, communication devices of any kind whatsoever, mobile networks, mobile platforms, mobile computers and laptops, as also all data, and information, in any form, digital or otherwise, which is hosted, generated, sent, received or transmitted, in any manner whatsoever, using the said mobile devices and platforms [15].

**NAND – Also known as the Sheffer stroke:** is a connective in logic equivalent to the composition NOT AND that yields true if any condition is false, and false if all conditions are true [16] and [17].

**NOR:** A predicate in logic equivalent to the composition NOT OR that yields false if any condition is true, and true if all conditions are false [18] and [17].

**Ontology:** A formal naming and definition of the types, properties, and interrelationships of the entities that really or fundamentally exist for a particular domain of discourse. It is thus a practical application of philosophical ontology, with a taxonomy [19].

**Operating Systems:** Is the most important software that runs on a computer. It manages the computer's memory and processes, as well as all of its software and hardware. It also allows you to communicate with the computer without knowing how to speak the computer's language [20].
**Optional requirements:** Requirements that are only needed on some forensic tools for certain types of smart phones or operating systems.

**Platform:** A group of technologies that are used as a base upon which other applications, processes or technologies are developed. In personal computing, a platform is the basic hardware (computer) and software (operating system) on which software applications can be run [21].

**Privacy:** The claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others [22].

**Rooting:** Is a means of unlocking the operating system so you can install unapproved apps, deleted unwanted bloatware, update the OS, replace the firmware, overclock (or under clock) the processor, customize anything and so on [23].

**Security:** The extent which a computer system is protected from data corruption, destruction, interception, loss, or unauthorised access [24].

Security Experts: Personnel with technical knowledge, who will investigate smart phones for the purposes of maintenance, data recovery and reverse engineering purposes.

**SIMfill:** A tool created by the National Institute of Standards and Technology (NIST) to automatically generate the test data for study cases.

**Triage:** The process of examining problems in order to decide which ones are the most serious and must be dealt with first [25].

**Usability:** The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use [26].
1 Introduction

It is a fact that mobile phone devices have become an integral part of our daily routine, where ordinary citizens use them for making calls, texting messages, browsing the internet, viewing emails, taking photos, recording videos, playing games and communicating with others via various available online social networks [27]. In fact, over the last two decades, the world has witnessed a vast increase in smart phones devices usage, to the point where teenagers and children are also provided with these devices by their parents to make the communication with them easier and faster. In this respect, Pew Research Centre [28] highlighted in 2017 that 95% of Americans own cell phones, 77% of which are smart phones when compared to only 35% in their first survey of smartphone ownership conducted in 2011. It also highlights that just over 10% of American adults are “smartphone-only” internet users with no traditional home broadband service.

As a result, this has created security issues as most users are not equipped to track, manage, or secure those devices or the data held in them; and it leads to an increased dependency on smartphone usage, criminal activities and/or illegal practices, to the point where Mobile Laws were introduced in various countries, such as India as an example. Mobile Law is defined by Pavan Duggal, Advocate, Supreme Court of India and President, Mobilelaw.Net [15] as “The emerging legal discipline and jurisprudence that impacts, pertains to, is associated with or has a bearing upon complicated legal issues concerning mobiles, communication devices of any kind whatsoever, mobile networks, mobile platforms, mobile computers and laptops, as also all data, and information, in any form, digital or otherwise, which is hosted, generated, sent, received or transmitted, in any manner whatsoever, using the said mobile devices and platforms”. Since smart phones are simply portable computing devices, they can be used in committing digital crimes. Examples of crimes that can be committed by or via smartphones are but not limited to: Mobile pornography, theft of identity, mobile cyber defamation, mobile cyber stalking, mobile software piracy, mobile credit card fraud, and mobile phishing.

Increase in crimes committed by or via smartphones has made it a necessity for digital forensics experts to come up with reliable tools that can be used to help in extracting data from those smart phones. As a result, it has become essential for both investigators (law enforcement officers, who may lack the technical knowledge but mainly engaged from the criminal investigation aspects) and security experts (personnel with technical knowledge, who will investigate smart phones for the
purposes of maintenance, data recovery and reverse engineering purposes) to focus their efforts on improving their technology and methods for obtaining information from smart-phones in a formal way that ensures court admissibility of the gathered evidence. A further driver is the fact that the likelihood of catching a suspect in possession of a mobile phone in a crime scene is usually much greater than the chance that they will have a laptop or desktop with them at the time of the incident.

It must be emphasised that mobile forensics science is not only about convicting suspected persons in a criminal investigation (Inculpatory Evidence), but more importantly about exonerating innocent persons, for example where it is possible to prove that they were in a different place other than the crime scene (Exculpatory Evidence). In this respect, for example, mobile forensics played a major role in exonerating a falsely accused university student of inappropriate communications with a teenager female, through the analysis of his phone and SIM card, where it was proved that no contact whatsoever took place between the teenage female and the student [29].

Unfortunately, without the existence of a generalized Process Based Framework to provide the appropriate guidelines and to regulate the steps to be taken and the procedures to be followed during the digital forensic phases, it will not be as simple as it might appear to extract data in an appropriate way from smart-phones even with the utilisation of the most popular tools. To this end, it was clear that there is a need for a set of effective methods to ensure that extracted and examined information from mobile phones devices are not tampered with, so that gathered evidence is accepted by a court of law, or can be relied upon as an undisputed means of proving that something has or has not taken place.

From this perspective, it is worth mentioning that the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence [30] gives advice on the collection and preservation of digital data including mobile devices, but it does not dictate how forensic analysis should be carried out, as it will differ massively between systems/devices. The International Standard Organisation (ISO) has also many standards dealing with digital forensic regulations and guidelines. Amongst these are [31]: ISO/IEC 27035 which deals with all aspects of incident management; ISO/IEC 27037 which deals with identification, collection, acquisition and preservation of digital evidence; ISO/IEC 27041 which deals with assuring suitability and adequacy of investigative methods; and ISO/IEC 27042 which deals with analysis and interpretation of digital evidence.

1.1 Motivation

Smart-phones and their operating systems are changing rapidly, and there is a lag from the time a new phone comes out to the time until a Smart-phones Digital Forensics Tool (SDFT) can be
updated or enhanced; though there are some good open source and/or commercial SDFT available in the market, unfortunately, those tools are either only good for limited brands of smart phones or operating systems.

It is important to note that forensic tools have varying capabilities and may not be designed for use by all operating systems. Security experts and forensics investigators typically select a tool based on the operating system, rather than the best available SDFT. Furthermore, the problem lies in the rate at which the smart-phones and their operating systems evolve, compared to the rate at which mobile forensics tools can be updated to encapsulate these changes. Consequently, these tools can become out-dated in a very short period of time.

As a result, it has become very difficult to achieve a comprehensive assessment of newly released SDFT, as the demand for releasing newer tools and the time and effort it takes to understand their capabilities creates a usability/complexity issue, in addition to the fact that most of these tools are not tailored - in most cases - to suit the needs of both the investigators and the security experts.

“A framework is a layered structure indicating what kind of programs can or should be built and how they would interrelate” [10]. Therefore, a Process Based Framework is a framework that emphasises how best practices and appropriate procedures are adhered to, rather than that a program should be layered or structured. The decision to venture into this area of research is necessitated by the motivation for establishing a Process Based Framework that produces guidelines for best practice mobile forensics, where differing use scenarios can be covered for each tested forensic tool.

1.2 Research Objectives

The principal objectives of this research are:

- Survey previously designed/proposed mobile forensics frameworks, so that appropriate guidelines are set, where an overview of each framework will be provided along with the impression based on the analysis as well as recommendations for areas that the framework may lack or need to be improved on.

- Understand how data is stored in popular operating systems, like the Android and the Apple iOS, and how data can be tampered with and what needs to be done to minimize or eliminate that possibility.

- Analysis and review of well-known mobile forensics tools/technologies used to extract, track, and report information from smart-phones devices. In addition, research mobile
forensics tool usability, or lack thereof, and understand the barriers, if any, to usability with various smart-phones devices and operating systems.

- Design and present a Process Based Framework for Mobile Forensics (PBFMF), which will have ability to use many forensic tools with various phones to ensure improved results and a consistent quality of forensic investigation, through the provision of the guidelines and appropriate procedures to be followed when conducting a digital investigation task.

- Test the PBFMF by implementing the steps/stages in it to highlight its benefits and at the same time compare the results with the other proposed frameworks, while following the NIST standards, and checking the difference in results in terms of how better they are after those steps were implemented.

1.3 Problem Statement

It has been revealed that utilization of Smart-phones Digital Forensics Tools (SDFT) is causing a serious problem for both practitioners (experts) and investigators, where an appropriate solution needs to be provided to solve the problem, so that a better understanding of the barriers to using forensics tools effectively and appropriately is formulated. The following are some examples of other problems that were faced while researching about this topic:

Need for an open ended, extensible framework [32]: The discussion of the papers and research done so far indicates that there is a greater need for developing a generalized and extensible framework to address current and future developments in the mobile industry. The “Internet of Things” or IoT promises to disrupt the current computing structure as we know it. Developing a more extensible framework will help provide guidelines for future investigation where smartphones are only one aspect of the mobile forensics industry.

Need for a truly generalized framework specific to mobile forensics [33]: Although there are frameworks that have been recommended in the research we reviewed, some were based on current digital and non-mobile devices. Although it is natural to develop frameworks based on prior experience with similar technology, the research done thus far suggests that the framework should be specific to general current mobile devices with an eye towards future mobile devices and integrating the IoT technologies into the framework.

Too difficult to create a single program [34] [35]: The variety of the tools used for investigation clearly indicate the difficulty of creating a single application capable of extracting and analysing data for all platforms. It is also a statement of the difficulty of keeping these applications up to date.
because the pace of new technologies far outperforms the updates to the tools and applications being used to analyse mobile devices.

Too many steps are used [34]: Based on the current work that has been reviewed, it seems that there are many steps, procedures and sub procedures that are required or recommended by each framework. Many of these steps can be generalized and should not be specific to a platform or a device. The complexity of these procedures and sub procedures makes it difficult for mobile analysis to be completed in a consistent manner. The focus should be on the documentation, analysis and presentation rather than customizing the steps to the platforms being investigated.

The methods used are focused on solving a specific issue [36]: Most research done thus far seems to be specific to solving a problem and is not generalized enough to accommodate potential outliers and to address issues that may not be present in the well-defined and controlled environment the research is being conducted under. To provide a more generalized framework, further study must be conducted to take into account current and future trends of mobile devices.

Most of the research done is specific to Android based devices [37]: The reviews conducted by the researcher shows that the majority of the reviews are specific to Android based smartphones, partly because Android’s market share is higher than any other platform and partly because the Android platform is Linux based, which is an open source platform. That, however, should not be enough of a factor to limit the research to these devices in general. More Mobile Forensics based research needs to be applied to Apple smartphones since they place second in the mobile device platform market share. Although Apple’s iOS is proprietary, not open source, additional research is needed to ensure a framework for forensic mobile devices will apply to the leading platforms in the industry.

1.4 Methodology

The research methodology’s initial step was to carry out analysis on three mobile forensics tools of the ones currently available to the mobile forensics community. It was determined that those tools will benefit from creating and developing a standard Process Based Mobile Forensics Framework. The three analysed tools are: Oxygen Forensics Suite 2014 [38], Computer Aided Investigative Environment (CAINE) version 5.0 [39] and Digital Evidence & Forensics Toolkit (DEFT) version 8 [40]. These three tools were selected because they contain mobile forensics tools built into them. They also cover different platforms, Oxygen is a Windows based commercial software while CAINE and DEFT are Linux based and open source.
The research methodology’s second step was to design and carry out an experiment for analysis of five mobile forensic tools. The five forensic tools under evaluation are installed on a dedicated host computer operating with the required platforms as specified by the tools. The focus is concentrated on the two-major dominating operating systems, iOS and Android. Therefore, each forensic tool is examined on four different devices; once on an iPhone 6 device (iOS 9.2.1), once on a jailbroken iPhone 4 device (iOS 7.1.2), once on a Samsung SM-G316HU (Android 4.4.4) device, and finally on a rooted Samsung GT-S6812i (Android 4.1.2) device. The reason for one of the two iPhones being jailbroken and one of the two Androids being rooted, is that the difference in the analysis can be observed and therefore a better view is gained.

The next step used in this thesis is based on analysing previously designed/proposed mobile forensics frameworks prior to establishing the proposed Process-Based Framework, so that appropriate guidelines are set, since they are essential for investigators when examining acquired data from confiscated mobile devices to ensure that every single source of information is beneficial and no essential piece of information is missed or ignored. In doing so, two of the analysed frameworks were benefited from for the Process Based Framework 1) “Towards a Unified Forensic Investigation Framework of Smartphones”, which recommends that guidelines be developed for each model or a set of series of smartphones, where it proposes that examination of each model of smart phones should be customized based on the prepared guidelines for that specific model. 2) “Efficient Generalized Forensics Framework for Extraction and Documentation of evidence from Mobile Devices”, where authors’ premise was to define an efficient generalized framework for extraction and documentation of evidence.

The last step was to apply the PBFMF to an actual case, where two different mobile forensic scenarios were looked at and applied to the proposed framework. In addition, a comparison of two other mobile existing forensic frameworks was made in order to compare their strengths and weaknesses to the newly proposed framework.

Additionally, information in the form of proposed Framework pseudo code will be detailed to help provide a road map for mobile forensics software developers and technology companies to create investigation tools that are based on the proposed Framework. This is achieved by providing enough information for developers to see what is needed to develop a tool, based on the proposed framework. However, this is only a guideline of what needs to happen and not an exact implementation.
1.5 Research Contributions

The novel work undertaken in this thesis sets out appropriate recommendations and solutions for how to overcome this problem, drawing on extensive research of forensic methods and studies. In this work, the following contributions are made:

Proposal of an extensible Mobile Forensics Framework: Based on the research and analysis completed in this thesis, the proposed mobile forensics framework was based on: platform independence, open architecture, extensibility, simplified design, and streamlined reporting. The proposed process based framework is composed of four main processes: First Responder Triage, Acquisition, Analysis, and Reporting.

Implementation of the Proposed Process Based Framework: The proposed framework was then put into practical use, and two different mobile forensic scenarios were examined based on the proposed framework. In addition, a detailed comparison of two other existing mobile forensic frameworks was completed. The purpose of the comparison was to review the strengths and weaknesses of each framework and to compare both to the newly proposed framework. Results of the comparison have shown that the PBFMF provides a step by step process based framework for an examiner to follow, and this framework is viable and a robust structure that the industry not only can use, but it also needs.

Mobile Forensics Framework Analysis: A comprehensive survey of mobile forensics frameworks was examined in this research. Certain criteria were taken into account when examining mobile forensics. An overview of each framework was provided along with the impression based on the analysis as well as the recommendations for areas that the framework may lack or need to be improved upon. The outcome of the analysis clearly indicated a need for a framework that is platform independent, extensible and capable of integrating newer mobile device technologies.

Mobile Forensics Tools Analysis: Conduct forensic tools analysis to test and check their reliability following NIST testing procedures, while comparing the obtained results with those of NIST ones in the case of the tools already tested by NIST so that a differentiation of their findings is established. This research used the outcome reports provided by NIST where they specify the areas in which each tool should be tested and how the test should be conducted. Measuring these tools in the same way provides for a better comparison.

Operating Systems Comparison Table: The table was created to provide a comparison of the different operating systems. In this table, information was provided about some of the most
popular mobile phone operating systems, where information regarding different models of phone can be found.

Mobile Device Tool Specifications Table: A table of tools specifications was established (see Appendix C), benefitting from the methodology developed by NIST to determine if a tool can accurately acquire specific data objects populated onto the device or SIM. The table consisted of two major requirements; the Mobile Device Tool-Core Requirement (MDT-CR) or/and the Smart Phone Tool-Core Requirement (SPT-CR), and the Mobile Device Tool-Requirement Optional (MDT-RO) or/and the Smart Phone Tool-Core Requirement (SPT-RO).

Framework Pseudocode: A pseudo code representation based on the research and analysis presented in chapter 7 was developed and presented to provide an abstract model. The pseudocode could be used by mobile forensics software developers to create new tools to better represent the forensics framework proposed in this research (see Appendix D).

1.6 Structure of the Report

This thesis is organized into 9 chapters and 5 appendices. In addition to this chapter, the remaining chapters of this thesis are structured as follows:

Chapter 2 is a Mobile Forensics Technical Review chapter which in turn gives an overview of smart-phone operating systems technologies, where examiners must have the necessary skills and credentials to be able to parse this data; cellular network characteristics where finding out about it should be the first step to be taken by an examiner, since it will determine the forensic tool to be used for data acquisition, examination and analysis; and forensic procedures stages and steps, where researchers have established that mobile phone forensic procedures should include four steps; preservation, acquisition, analysis and presentation (PAAP). The chapter also presents causes and factors contributing to the problem, highlights facts and statistics about digital forensics challenges, discusses some of the articles written and research conducted about this field subject, in an attempt to explore previous related studies on the subject area, and reviews rights of privacy and anonymity.

Chapter 3 gives an initial analysis of three forensic tools of the ones currently available for the mobile forensics community and the challenges faced by the researcher while installing those tools. In addition, it gives an overview of the preparation for setting up the environment for advance analysis for testing five forensic tools and the challenges faced by the researcher while installing those tools. The chapter then presents the methodology of how the analysis of the five mobile forensics tools will be conducted while benefitting from the outcome reports provided by NIST. At
the end, a summary of the findings of the analysis results of all analysed mobile forensics tools was provided.

**Chapter 4** analyses eight previously proposed frameworks by various researchers. In this chapter, an overview of each framework was provided along with the analysis based on the analysis as well as recommendations for areas that the analysed framework may lack or need to be improved upon, in addition to the findings of those discussed frameworks. The result highlighted the need for a Process-Based Framework that is platform independent, extensible and capable of integrating newer mobile device technologies to remedy the issues that were revealed in this chapter, to help ease and reduce the difficulties faced by investigators while using Mobile Forensics Tools such as minimizing or eliminating the possibility of tampering with the data.

**Chapter 5** discusses in details the architecture and design goals of the proposed process based framework, which is composed of four main processes; First Responder Triage, which consists of many steps, starting from the arrival at the scene and ending at the storage and transporting of the device; Acquisition process, which involves determining the type of acquisition, manual or tool based; Analysis process, which proposes steps to be followed for appropriate ways of analysing acquired data; and Reporting process which establishes guidelines to be used specific to what should be included in the report.

**Chapter 6** explains in detail the implementation of the Proposed Process Based Framework, where it was applied to an actual case. Two different mobile forensic scenarios were looked at and applied to the proposed framework, since the most accurate method for testing the framework is to apply it to a number of different scenarios. In addition, a comparison of two other mobile existing forensic frameworks to the researcher's proposed framework were made to review the strengths and weaknesses of each and compare both to the newly proposed framework.

**Chapter 7** is the final chapter, and it concludes the thesis by providing a brief summary of key contributions and gives direction for future research work.
Chapter 2: Mobile Forensics Technical Review

2 Mobile Forensics Technical Review

2.1 Background

Digital Forensics is “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 facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations” [7]. Its branches are divided into many related electronic devices, amongst which are: computer forensics, network forensics, data analysis forensics, database forensics and mobile device forensics, where the last mentioned is the subject of this research.

As the term implies, mobile device forensics is the extraction of information from mobile devices, under forensically sound conditions, for the purpose of reconstruction of any events found to be criminal. Though the term mobile device can mean any digital device consisting of an internal memory that is easily moved around such as a Personal Data Assistants (PDA), Global Positioning System (GPS) device, tablet, video camera, or other devices, it will only refer to smart phones for the purpose of this research, while the tools and software covered will be those used to extract information from smart phones.

When a mobile device is confiscated for investigative purposes, some immediate questions that need to be considered relate to how the device should be handled; when it can be preserved; how the data should be retrieved; where the data is stored; whether the device actually works; and finally, how the whole process should be documented and reported. As mentioned in Chapter One, unlike the computer forensics field, the mobile forensics field is lacking in standardised processes and interoperability features, which have not kept up with advancements in the smart phone field. It is also difficult to find previous or current studies to help researchers determine the most appropriate and useful forensic tools to use, so it is important to make the case for a forensic tool/framework that can analyse data from different operating systems and/or different forensic tools. Explaining and showing how there is sufficient commonality in the different operating systems to build an appropriate platform will resolve these problems.
Some of the challenges faced when acquiring data, aside from the very large amount to be analysed when the device is first acquired and stored properly, is that acquired data exists in its rawest format, making it hard for examiners to interpret and understand its contents. Examiners must therefore have the necessary skills and credentials to be able to parse this data, and these credentials are likely to be the first things questioned by an attorney in a court of law.

The type of forensic tool used in the investigation is also essential, since out-dated ones may not be useable and reliable. Adhering to rules of evidence is also essential, since the procedures used in gathering the evidence will determine its admissibility in court. Therefore, when acquiring evidence from a device, it is essential that [41]:

- It has been acquired without being altered or damaged, since it can be easily modified.
- The process is repeatable and defensible, since data is relatively fragile.

There are several items on the list of evidence sources to review when a device is under investigation: phonebook; calendar items; to do list; electronic mail; instant messages; web information; electronic documents; photos; videos; audio; GPS coordinates; social media data; subscriber identifiers; equipment identifiers; service provider; last dialled numbers; phone number log; short text messages; enhanced messages; multimedia messages; last active location (voice and data); and other networks encountered.

### 2.2 Smart-phone Device Operating System Technologies

The operating system (OS) determines the reliability of the functionality of a phone, as well as its capability of carrying out tasks and managing its memory. The phone OS is also considered as a platform that allows developers to download and run their applications, depending on the source model and whether it is an “open” or “closed” source OS. To provide protection of data during “battery run out” or in the event of “reset”, operating systems of mobile devices are stored in the flash ROM in either NAND (a type of non-volatile flash memory storage technology that does not require power to retain data) or NOR. However, 3rd generation operating systems of mobile devices are only stored in NAND due to the need for greater storage capacity, in addition to their improved density, faster speed transactions and lower cost. While NOR flashes are faster, they are more expensive, and take longer to erase and write new data [17].

Unlike computer operating systems, mobile devices (smartphones mainly) have many known famous operating systems, amongst which are Apple's operating system (iOS), Google's operating system (Android); Microsoft's operating system (Windows Phone and Windows Mobile);
Blackberry's operating system (RIM); and Nokia's operating system (Symbian). There are also less common OS, which makes it difficult for one single tool to be interoperable with all of them and makes the task of forensics analysis quite challenging.

With the multitude of operating systems currently on the market, the focus—when analysing the forensics tools—will be concentrated on the two dominant operating systems on which more extensive research will be conducted: Android OS, which is an open-source and proprietary operating system for smart-phones (some of the software is free while some is licensed), and Apple's operating system (iOS), which is closed-source and was developed initially for iPhones, then later extended to cover iPads and iPods, which means that all iOS software must be licensed.

The Android operating system's dominant market share (65%) along with the second most popular operating system - Apple's iOS (20%) - leaving only 15% of the smart phone market to the rest of the operating systems as of December 2012 [42]. This market share of the two operating systems have even increased as it was estimated that in 2015 a range of 90% - 98.6% of mobile devices shipment in the world consisted only of the two major operating systems [43]. This is due to the fact that iOS is only used by Apple products such as iPads and iPhones, while Android is more widely used by other mobile phone brands and tablets, including Samsung's products. Although the Windows phone operating system shows promise from a forensics standpoint, a decision was reached not to examine it in this research because of its smaller market share and fewer online communities compared to Android and Apple.

In Table 2-1 below, information is provided about some of the most popular mobile phone operating systems, where information regarding different models can be found. The table was created in order to provide a comparison of the different operating systems.
<table>
<thead>
<tr>
<th>OS</th>
<th>Bada</th>
<th>Symbian</th>
<th>Windows</th>
<th>BlackBerry</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developer</td>
<td>Samsung</td>
<td>Nokia</td>
<td>Microsoft</td>
<td>RIM</td>
<td>Google</td>
<td>Apple</td>
</tr>
<tr>
<td>Language</td>
<td>C++</td>
<td>C++</td>
<td>C, C++</td>
<td>C++</td>
<td>C, C++,</td>
<td>C, C++,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Java(UI)</td>
<td>Objective-C</td>
</tr>
<tr>
<td>OS Family</td>
<td>Posix</td>
<td>RTOS</td>
<td>MS Mobile</td>
<td>Mobile OS</td>
<td>Unix-like</td>
<td>Unix-like/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BSD</td>
</tr>
<tr>
<td>Working State</td>
<td>Replaced</td>
<td>Active-</td>
<td>Current</td>
<td>Current</td>
<td>Current</td>
<td>Current</td>
</tr>
<tr>
<td></td>
<td>by Tizen</td>
<td>updates</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source model</td>
<td>Open source</td>
<td>Closed (was</td>
<td>Closed Source</td>
<td>Closed Source</td>
<td>Open +</td>
<td>Closed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>open)</td>
<td></td>
<td></td>
<td>proprietary</td>
<td>source</td>
</tr>
<tr>
<td>Marketing Target</td>
<td>smart-phones</td>
<td>smart-phones</td>
<td>smart-phones</td>
<td>smart-phones</td>
<td>smart-phones</td>
<td>smart-phones</td>
</tr>
<tr>
<td>Available Languages</td>
<td>multi-lingual</td>
<td>multi-lingual</td>
<td>multi-lingual</td>
<td>multi-lingual</td>
<td>multi-lingual</td>
<td>multi-lingual</td>
</tr>
<tr>
<td>Package Manager</td>
<td>Samsung Kies</td>
<td>Nokia store, six, six, jad, jar</td>
<td>Windows Phone Store XAP</td>
<td>BlackBerry Desktop Manager</td>
<td>Google Play, APK</td>
<td>App store</td>
</tr>
<tr>
<td>Kernel Type</td>
<td>RTOS, Linux</td>
<td>EKA2</td>
<td>Hybrid</td>
<td>Java virtual machine</td>
<td>Monolithic</td>
<td>Hybrid (XNU)</td>
</tr>
<tr>
<td>Default User Interface</td>
<td>TouchWiz, graphical</td>
<td>QT Framework</td>
<td>graphical</td>
<td>Graphical</td>
<td>Graphical</td>
<td>Cocoa Touch</td>
</tr>
<tr>
<td>License</td>
<td>proprietary</td>
<td>EPL</td>
<td>Commercial</td>
<td>Proprietary</td>
<td>Apache</td>
<td>Proprietary EULA</td>
</tr>
</tbody>
</table>

Table 2-1: Summary of Various Operating Systems
2.2.1 Google Operating System (Android).

Android is a “multi-process platform relying on the standard Linux facilities for processes and users management” [33]. It is an open source and proprietary operating system for smartphones, which means that some of the software is free with others being licensed. The operating system was developed by Google and first released in 2008, with Nougat 7.1.2 being the latest release, which was last updated on 4th of April, 2017.

Along with C and C++, Java was used as the programming language for Android applications, where each Application Package File (APK) runs in a separate process inside its own Dalvik (relying on the Linux kernel for threading and memory management) virtual machine. For security reasons, applications are by default not permitted to impact other applications as a result of any operations. This means that applications cannot perform any operations on end users' private data, such as contacts or messages, for the sake of accessing the network for device-state management. Permission statuses are defined in a static way and cannot be altered once they are installed. Exceptions are issued to the developer, who is given a certificate to establish and manage relationships between applications prior to their installation [33], and further declaration of permissions is usually needed.

According to Stirparo and Kounelis [44], the storage of internal data is controlled by the Android’s Application Program Interfaces (APIs) in an SQLite database format, and external data storage is left open for applications to decide which part to store data in. These locations can include external SD cards where files have less security, or the embodied NAND flash one, where the developer is granted control for naming or locating the file in addition to deciding its type. The developer can also “store key value pairs of primitive data types in a lightweight XML format”, or in the network where data is stored remotely. The most common standards for Android directories, as stated by Stirparo and Kounelis are:

- Shared prefs: Shared preferences in XML format.
- Lib: Custom library files required by an application.
- Files: Files the developer saves to internal storage.
- Cache: Files cached by the application, web browser or other apps that use the WebKit engine.
- Databases: SQLite databases and journal files.
In order for an Android device to be rooted, permissions need to be given to the investigator to take action in the root directory of a device’s memory, thus performing acquisition. Once permission is granted, a developer must have an Android Software Development Kit (SDK) available to launch to run shell scripts to extract data through the command line interface feature [32]. Although it is believed that rooting an Android device makes it easier from an investigative standpoint, an experiment carried out by Barghouthy and Marrington [45] proved that this is not necessarily true. They concluded it is not advisable to root the device, since rooted devices do not have any advantage over non-rooted ones, especially when evidentiary data has been deleted. Although it is necessary for some commercial tools to have Android devices rooted for them to execute a physical acquisition, it is worth mentioning that the above discussed experiment works on “facilitating physical acquisition of the Android’s flash memory (Android device’s secondary memory) through the prism of reconstructing private browsing sessions in an Orweb tool and does not apply to the acquisition of live memory - the Android device’s RAM”.

2.2.2 Apple's Operating System (iOS).

Apple's operating system (iOS) is a closed source operating system developed initially for iPhones and later extended to cover iPads and iPods, which means that all of its software must be licensed. It differs from other operating systems in that it is not licensed to be installed on non-Apple hardware. In terms of file system examination, iPhones use HFSX which is unique to Apple computer systems and make it possible to perform a forensic analysis of a physical forensic duplicate of mobile devices using file system forensic tools [46]. Also, all third-party applications must pass a vetting process by Apple to be featured in the iStore. The operating system was first released in 2007, and the latest known released version is iOS 10.3.3, which was last updated on 19th of July, 2017. It consists of four layers: the Cocoa Touch layer and the Media layer (user domain), which as the name implies, contains users’ files; the Core Services layer (local domain) consists of the libraries and applications directories, and the Core OS layer (system domain) contains software installed by Apple [32]. Along with C and C++, Objective-C is used as the programming language for iOS applications. iOS is considered more secure than the Android operating system and harder to break into because of the way the Android is fragmented by the manufacturers, and hence bypassing the PIN is a challenge for investigators.

iOS devices from the 3G release onwards are installed with a Data Protection feature, which is [47] “the combination of hardware-accelerated encryption and an authenticated cryptographic scheme, allowing any file or piece of information to be encrypted or decrypted with a separate key”, which meant that those devices have the capability of remotely wiping of data contained in them. This
feature can only be avoided by isolating devices from all available radio communications such as Wi-Fi, Bluetooth or 3G communications, although, devices installed with iOS 4 or later have the capability of encrypting all backup data when using iTunes. Acquisition tools only need to be capable of communicating with the device’s backup services for them to be able to recover a large amount of clear text data even if the password is not known to the attacker.

2.3 Cellular Network Characteristics and Operating Systems

Knowledge of the cellular phone network used is essential, where finding out about it should be the first step to be taken by an examiner, since it will determine the forensic tool to be used for data acquisition, examination and analysis. The two most commonly used types of digital cellular networks [48] are: Global System for Mobile Communications (GSM), which is mostly used in Europe, but is also used in the United States, where The SIM comes as a separate component that is interchangeable from one mobile device to another, and Code Division Multiple Access (CDMA), which is mostly used in the United States and does not come with a separate Subscriber Identity Module (SIM) in the mobile device, which results in all data being stored on the mobile device. It must be noted that appropriate definition of CDMA is “a channel access method used by various radio communication technologies” [49] or “a sort of multiplexing that facilitates various signals to occupy a single transmission channel. It optimizes the use of available bandwidth” [50].

Another type of cellular phone network (but not as common as the earlier two) is the Integrated Digital Enhanced Network (iDEN), which has the same characteristics of a GSM device with the additional ability of push-to-talk, a two-way radio system.

Subscriber Identity Modules (SIMs) are protected by default by Personal Identification Numbers (PINs), which consist of 4-8 digits where three attempts are usually allowed to unlock them; and Personal Unblocking Keys (PUKs), which are known by the service provider and consist of 8 digits, where 10 attempts are usually allowed to gain access to PIN-protected SIMs. SIMs have two identifiers which are both considered trustworthy, reliable and traceable, since they cannot be edited: 1) The Integrated Circuit Card Identification (ICCID), which consists of 19 or 20 digits and is always retrievable even if PIN-protected. The first 2 digits refer to the Major Industry Identifier (MII), the second 2 digits refer to the Country Identifier (CI) or country dialling code, the third 2 digits refer to the Issuer Identifier Number (IIN), the following 12 digits refer to the Individual Account Identification Number (IAIN) and the last digit, which refers to Check Digit. 2) The International Mobile Subscriber Identity (IMSI) number, which consists of 15 digits, can be PIN protected, where the first 3 digits refer to the Mobile Country Code (MCC), the second 2 digits refer
to the Mobile Network Code (MNC) and the last 10 digits refer to the Mobile Station Identification Number (MSIN). There are many tools and websites that help interpret the significance of these numbers, such as the International Numbering Plans site, which provides an analysis of IMSI numbers and many other resources such as phone numbers, International Mobile Equipment Identity (IMEI) and SIM numbers analysis.

Handsets come with IMEI numbers which consist of 15 digits (sometimes featuring an additional 2 digits) to indicate the Software Version (SV). The first 8 digits refer to the Type Allocation code (TAC) for identifying the make, model and country of origin, the second 6 digits refer to the Serial number (SNRI) and the last digit refers to the Check Digit. As mentioned earlier, the International Numbering Plans site can provide an analysis of IMEI; however, typing *#06# will reveal it without the need to remove the battery or look at the back of the phone. Also, typing *#2820# will reveal the phone’s IP. The Mobile Station International Subscriber Directory Number (MSISDN) is another identifier of a mobile subscriber which is used to connect a call to the mobile phone and can be considered the phone number of the card. Since it is user-editable, it therefore cannot be considered reliable, and a confirmation will need to be sought from the service provider.

The following needs to be adhered to when:

- A SIM PIN is active:
  - Ask the owner for the PIN.
  - Visit websites that can provide default PINs.
  - Request the PUK from the service provider.

- A handset security code is active:
  - Ask the owner for the code.
  - Visit sites that can provide default security codes.
  - Download the manual of the handset.
  - Attempt physical extraction via cable or JTAG.
  - Attempt chip-off as last resort.

### 2.4 Forensic Procedures

Before proceeding with any investigation of smart phones, an investigator must adhere to the proper procedures of handling evidence when the device is seized, while consequently labelling it, and
preserving it. NIST also suggests that examiners or analysts will need to be well-prepared in advance by establishing the following objectives [47]:

- Gather information about the individual(s) involved (who).
- Determine the exact nature of the events that occurred (what).
- Construct a timeline of events (when).
- Uncover information that explains the motivation for the offense (why).
- Discover what tools or exploits were used (how).

Whilst it is a fact that what can be extracted by mobile forensics tools does differ between mobile systems, this is always going to be the case as mobile systems run different OS and file systems - in the same way computers do (e.g. HFS, NTFS, FAT etc). This means that the information retrieved from each platform/operating system will differ, which can be attributed to the platform/operating system, which means that the forensic tool will not be in a position to overcome or compensate for this. In addition, there is no universal file structure for mobile devices, which, frustratingly, means that the method of storing data on these devices differs between manufacturers. It was deduced that this is a contributing factor to why forensic acquisitions of mobile phone devices are normally conducted in one of two ways: physical or logical [52].

Every investigator would love a one-stop shop, where a “one-size-fits-all” tool will analyse everything without question. The problem is that the complexity and maintenance required to do this is almost incomprehensible. At this point in time, the best that can be done is to establish guidelines/frameworks for ‘best practice’ mobile forensics where differing scenarios are covered, as well as the best practice approach for each. It is believed that, currently, there is no one single tool that will be able to achieve this, as there is no unifying accrediting body in the UK (or elsewhere) that could confirm that every single aspect of any program is 100% reliable.

Some might argue that the difficulty of mobile device forensic tools is not in their complexity, and that these tools are, for the most part, incredibly easy to use. This is true to an extent, as those tools can literally auto-detect the connected device. In this instance, all that would be needed would be to click "Next", "Next", "Finish", and the process is done. Unfortunately, when an examiner connects the tested device, three scenarios would happen: either a) the device is accepted and the examiner can carry out a full logical/physical read of the device, or, b) the device is accepted but the examiner can only get a partial read, because of various reasons such as the device’s security or encryption, which might only allow getting the SMSs and the pictures, or c) the device is not
accepted because the forensic tool’s firmware has not been updated with the newest drivers to read the tested device.

Third party tools/scripts are considered as one factor contributing to the problem. There is a plethora of sites/blogs on the Internet where someone might write a python script to grab data from mobile devices then share it online. Many people might then download the script, run it on their devices and get results (and sometimes take these results to court!). These tools/scripts, although tested by the author, would not have been subject to scrutiny from the wider forensic community and therefore cannot be completely relied upon.

One of the solutions, which sounds as though it might solve this problem, is the requirement for a standardised mark-up language for forensics that permits the development and extension of new forensic analyses, so that we have a common processing platform that accepts XML-based instructions, where the instructions form the basis of the forensic analysis. Having an open and standardised model will enable such a tool to be extensible and quickly adapted to new analyses and systems. It is not easy, however, to ensure that competing vendors would work together on a standardized language as they need to differentiate themselves commercially for the sake of business benefits. This is not to say that legislation could not force vendors to work in a compliant manner, e.g. standardization of Universal Serial Bus (USB) charging on mobile phones, which has been enforced within the EU to achieve this objective.

2.5 Forensic Phases

According to the National Institute of Standards and Technology (NIST), researchers have established that mobile phone forensic procedures should include four steps: preservation, acquisition, analysis and presentation (PAAP).

- Preservation is a method of carefully maintaining the evidence (the smart phone) in the same way it was received, and will mostly depend upon whether it was found in the ON or OFF state.

- Acquisition is the step where information is extracted from the mobile phone and is usually comprised of two known types, logical or physical.

- Analysis and examination is the third step, and as the term implies, it is the stage where gathered information and collected data is revealed for examination and hence, analysis.

- Reporting or presentation is the final stage, when the case is completed and a report highlighting the evidence found is produced and submitted.
2.5.1 Preservation and Handling

Preservation is the confiscation of the investigated mobile device before, during and after conducting appropriate investigations in the same condition it was received. This mostly depends upon whether it was found to be in the ON or OFF state, ensuring that all correct procedures were adhered to, to preserve the original state of the evidence (device), and having the evidence accepted in court. In addition to device confiscation, NIST [47] advises that “any associated hardware such as media cards, UICCs, power adapters, device sleeves, or peripherals, should be seized along with related materials such as product manuals, packaging, and software”. When a data examiner is storing digital evidence, the storage procedures must be adhered to, so as to ensure that the digital evidence [53] is stored in a secure, climate-controlled environment, and is not exposed to magnetic fields, moisture, dust, vibration, or any other elements that may damage or destroy it.

2.5.1.1 Evidence Collection

In terms of Evidence Collection, an examiner will need to have knowledge and understanding of the following general guidelines [54]:

- Adhering to proper decontamination procedures of damaged mobile devices caused by fluids or damaged screens.
- Determining risks and consequences associated with manipulating the mobile phone data to be examined.
- Adhering to applicable legal authority and case law.
- Verifying the data extracted from the mobile phone.
- Distinguishing between GSM, CDMA and iDEN cell phones.
- Considering the various types of identity cards (e.g., SIM, USIM and CSIM).
- Ascertaining the physical characteristics of various SIM card sizes and Identification (IMSI vs. ICCID).
- Determining the types and locations of data stored on SIM cards.
- Differentiating between handset lock, PIN lock and PUK.
- Being aware of when a phone should warrant a higher level of analysis when the process-based lab’s capabilities are not available.
Locating backup files used by each Smartphone on the computer synced to the mobile phone, such as Gmail account username/password for Android-based devices and iTunes backup files for iOS-based devices.

2.5.1.2 Isolation.

Unless all necessary measures have been carried out, there is a greater chance of an owner being able to change the device's status or remotely delete all essential data if the device is connected to the Internet. Phones which cannot be processed immediately must be turned off, followed by removing the battery to preserve call logs; prevent deleted data from being overwritten, prevent the mobile phone from being reached by data destruction signals; and prevent improper mobile phone handling [54]. However, if the mobile phone must be left on, then precautions must be taken in the form of radio isolation, where a mobile device is isolated from all radio networks such as wireless and Bluetooth networks. This is accomplished through Faraday Bags, utilizing appropriate laboratories, removing SIM cards, enabling airplane mode, or switching off the mobile. Two of the most common techniques are [47]:

- Radio Isolation Containers. Some devices are installed with security enhancements to monitor their improper handling, which might trigger them to lock down and even destroy their contents. This feature is known as Anti-Digital Forensics (ADF), where sets of techniques and measures are used by end users to protect their devices from being hacked in legitimate cases, or from being investigated in less honourable situations. Other security enhancements/features that mobile devices can be equipped with are:
  - Malicious Programs: These programs can be activated if a specific action is carried out on the device.
  - Key Remapping: Hardware keys may be remapped to perform a different function than the default.
  - Geo Fencing: Devices will wipe their data if they enter a certain geographic area.

An examination of a device can be conducted safely on site, providing that portable shielded containers or shielded work areas such as Faraday tents are used. However, NIST reports that in a field test conducted at Purdue University, many of the shielding devices did not prevent network communication in all cases. The reasons behind this failure were attributed to: [47] “the materials not providing enough attenuation, leaks or seams in the shield or the conductive shield acting as an antenna”. This proves that shielding equipment must be validated before being used by investigators.
Cellular Network Isolation Cards. In this instance, Cellular Network Isolation Cards (CNIC), which are considered tool-specific (not interchangeable between the tools of various manufacturers), are used to mimic the original UICC. This is done so that the handset is denied network access, especially the types of handsets that cannot be booted without the UICC while data acquisition is granted without fearing Wi-Fi interference. CNICs are a good means to help prevent some users from mistakenly inserting foreign UICCs into the mobile device for data acquisition, which can mess up some of the internal memory original data elements such as call logs and SMS messages.

2.5.2 Extraction and Storage

Extraction is the step where information is imaged or obtained from the mobile phone and will usually take one of two known forms, logical or physical. The idea of extraction and storage is to start researching how technology devices store data, how it can be extracted, and moving closer to the target procedures. Below are some questions that should be answered:

- Conceptually, how does storage work?
- How is data retrieved?
- Does it matter what device data is stored in?
- Is the smart phone device’s data different than other computers?
- Can data be extracted and stored the same way regardless of the device used?
- Is it going to be different in the future?

Data extraction should be done following specific procedures to ensure that there is no tampering and that the extraction is done correctly. Storing the data is an important step as well, and should be done carefully. Specific procedures will need to be established and followed to ensure that data tampering does not occur. When considering storage, investigators should review how the data is stored in the device prior to and after it has been extracted from the device. Storage could also mean the actual storage of the device itself, which—in this case—will be discussed under the preservation section of this report, since it will be explained in further detail when examining the proper handling of an investigated device.

When dealing with the acquisition of data, different researchers categorise acquisition differently. For example, Mohtasebi and Dehghantanha [34] categorise acquisition into local and remote terms. Local acquisition, or, “On the Phone Tools” is a method utilizing a forensic software tool, which is installed onto the mobile device to copy stored data to a removable memory, where a logical image...
is saved. In this example, several studies have proved that these tools tend to miss a great amount of forensically sound artefacts from the investigated phone. This is true in the case of the Mobile Internal Acquisition Tool (MIAT), which was developed specifically for Windows Mobile Smart-phones (WMSs) to perform a logical acquisition [55]. While the remote acquisition is achieved by running a forensic software tool on a workstation or employing a forensic device, it can also be accomplished via connecting the device to a desktop computer wirelessly or through the use of a wire. The conclusion Mohtasebi and Dehghantanha reached was that the remote method is considered more practical, as many related tools were found to be compatible with many smart phones compared to the number of local data acquisition tools although these methods need fewer resources and can be used in a more rapid secession. They [34] also suggest that utilising both methods will strengthen the credibility of the data gathered.

Other means of acquisition methods (the most common known) are the logical and physical methods, which follow the computer forensics categorisation format. The logical acquisition is by far the most preferred method due to the existence of different mobile platforms. They are also easier for tools to extract since no physical removal of the device parts is performed. In terms of removable media, logical acquisition is used when a device to be tested is found in its active state, followed by the physical acquisition of the associated media after it has been removed. Otherwise, if the device is found to be in the off state, the removable media is acquired physically first and then tested before handling the mobile device. Also, the state of the device dictates whether the SIM or the internal memory is analysed first. If the device is found to be in the ON state, then the SIM is analysed afterwards. Otherwise, it is analysed before the device’s internal memory is examined when the device is found to be in the OFF state. The other factor to be considered besides the state of the device is the radio isolation, so that remote connection to the device is avoided to prevent modification to objects of the file system, as in the case of logical acquisition where deleted data are erased beyond recovery. Logical and physical extraction was discussed by Anobah et al [56], but from a different prospective. The discussion was about how the extraction is conducted, not about the outcome of it.

On the occasion of investigating memory cards, it must be noted that deleted data is not recoverable logically. Imaging of the card will be required so that it can be analysed with a more suitable forensic tool that can be aided with an external media reader. On the other hand, acquiring the data from the memory physically will give the investigator the capability of checking its contents, and probably the ability to recover deleted files. However, precautions must be taken so that recovery of data is blocked by triggering the content protection features incorporated into the card.
Another categorisation was based on a tool classification system (Mobile Forensics Pyramid), which is displayed in Figure 2-1 [57]. The pyramid starts at the bottom with the manual extraction being the easiest and cheapest method and ends up with micro read extraction being more technical, invasive, time consuming, and expensive. In this situation, examiners are required to dismantle the mobile devices, or physically dismantle the device and remove the flash memory chip as in the case of the Chip Off method. Manual acquisition tends to utilize photographing, video recording or manually writing and recording the found data into a sheet of paper while browsing through the investigated device’s stored data. The contents are helpful in providing a report of the followed forensic process, the captured data, and can also cross check that the evidence provided is consistent with the available records.

When physically acquiring data via JTAG (Joint Test Action Group), its interface is used to extract the contents of the memory from the device, which permits full binary extraction while not altering the device’s contents. This JTAG process is good in that it is less intrusive, but it does require a noticeable amount of time and knowledge of the device to acquire the capability to interpret the extracted binary data. Because of this fact, it can be considered as the middle ground of the manual and logical acquisition methods, where there is some sort of interaction and the chip off and the micro read methods where there is an interaction or dismantlement of the device. A similar acquisition method is the Hex dump [54], which gives the examiner access to allocated and unallocated data stored on the mobile phone. This method, however, may require the use of many tools to be able to process it, and it is time-consuming for the analysis. During the Chip Off process, the removed chip will need to be connected to a device programmer by a specially designed socket.

The following are examples of some commercial device programmers available [46]: “Data I/O FlashPAK II (www.dataio.com), Xeltek SuperPro 5000 (http://www.xeltek.com), and BPM Microsystems (http://www.bmpmicro.com)”.

One of the other approaches of physically acquiring forensic duplicates of mobile devices is through the utilisation of “software agents” [46] by the forensic tool, which is run on the mobile device in order to acquire data from it. It must be taken into consideration that if the agent is not run on the device, then there will be no data acquired as a result. Also, it must be noted that running such agents on investigated devices can end up overwriting some of the data, which is deemed necessary for the sake of acquiring sought-after data when other means of acquiring data are exhausted.

The extraction level needed will depend on the type of investigation required. It must be noted that once a higher level of classification system in the pyramid is attempted, then it will not be possible for a lower level to be trailed for acquisition purposes of the same previously attempted device. Also, though Micro Read level is included, it will only be used as the last cure for attempting to
recover data from a mobile device, as there is a greater chance of damaging evidence on the device. However, there is an advantage of limitlessly accessing the phone’s internal memory, as this process will not be bounded by the restraints of the operating system. It is worth noting that this action will only be attempted in the case where national security is jeopardised and none of the other four techniques are applicable for such a situation. NIST [47] and [58] stated in its Guidelines on Mobile Device Forensics report that “There are no known U.S. Law Enforcement agencies performing acquisitions at this level” and “Currently, there are no commercially available Micro Read tools”.

![Figure 2-1: Mobile Device Tool Classification System[47]](image)

There are different methods for recovering data from obstructed devices and they fall under three categories: software-based, hardware-based and investigative. The first two methods are combined to access the device through bypassing authentication mechanisms. Cold boot attacks are examples of such a method, which have the password recovery ability of locked Android based devices. The devices are cooled 10 degrees below Celsius, followed by disconnecting and reconnecting the battery at 500ms intervals [59], but it must be taken into consideration that the removal of the battery may delete the contents of a volatile memory. In some cases, it may also affect date and time values. Though some mobile device users choose the manufacturer default passcodes or weak passwords, it is not advisable to try to unlock them, as doing so may trigger the devices to wipe their memories or increase the level of security since they come with a set number of allowable attempts before restricted access occurs. A framework was specifically designed by Huber et al. to address mobile device forensics based on cold boot attacks [60].

Capabilities may vary from one forensic tool to another, and therefore, examiners will need to check these capabilities with already acquired test mobile devices. They will also need to use their
expertise to compare the output of one tool against another for consistent result verifications in addition to attending to all necessary required training on the tools used.

Prior to deciding which forensic tool should be considered, criteria were recommended by NIST [47] and [61] as a fundamental set of requirements to help determine when these tools should be employed:

- **Usability** – the ability to present data in a form that is useful to an investigator
- **Comprehensive** – the ability to present all data to an investigator so that both inculpatory and exculpatory evidence can be identified
- **Accuracy** – the quality of the output of the tool has been verified
- **Deterministic** – the ability for the tool to produce the same output when given the same set of instructions and input data
- **Verifiable** – the ability to ensure accuracy of the output by having access to intermediate translation and presentation results
- **Tested** – the ability to determine if known data present within the mobile device internal memory is not modified and has been reported accurately by the tool

The other important sources of data acquisition are the service providers, who can be approached for releasing data related to the suspect device through the identification of the phone number, the subscriber or equipment identifiers, or in other cases to disable service. In addition, investigators can benefit from the Grey Box Enhanced 911 technology feature, which enables mobile devices to process 911 calls along with providing the geographic location of the device used, even when network coverage is weak or a user's contract has been terminated.

An expert can establish procedures for a process-based framework to improve the mobile forensics technical operation, but these procedures must have been tested and validated independently with the same models of smartphones and their relevant operating systems. It must be emphasised that testing and validation procedures should properly record and document all steps taken. The type of case investigated must also be taken into account, so that certain strategies are followed accordingly. A good example in this instance is a child pornography case, where an investigator is expected to pay more attention to the device’s images, while in a case of accessing prohibited websites, an investigator can be expected to give more attention to internet browsing history files [62].

Finally, an examiner will – in addition to what has been discussed earlier about the different types of acquisitions- need to have the knowledge and understanding about the following [54]:

Tool functionality, their limitations and whether an additional examination is needed.

Identifying mobile phones that contain one or more SIM cards.

The need for a sufficient battery charge of at least 50% to proceed with the data extraction.

Understanding that processing memory cards may not provide deleted data from the memory card while in the smart phone, and that they may provide different results while residing inside of the device instead of being processed externally.

Identify what information can be stored in a handset, on a SIM card and in which locations.

2.5.3 Examination and Analysis

Analysis and examination is the third step, and as the term implies, it is the stage where gathered information and collected data is revealed for examination and hence, for analysis. The examination and analysis process usually follows once the acquisition process has taken place, when it is time to uncover all acquired digital evidence, whether it was hidden or obscured, so that a final report of the contents can be produced. The analysis process differs from the examination in that it looks at examined data (evidence) scientifically to decide whether correct procedures were adhered to and whether results can be depended upon. In other words, “examination is a technical process that is the province of a forensic specialist, while analysis may be done by roles other than a specialist, such as the investigator or the forensic examiner [47].”

Prior to selecting a tool to be used for acquisition, examination, or analysis, the margin of error and confidence interval should be calculated and taken into consideration. This can be achieved by conducting experiments with the specific tools over different types of mobile devices and operating systems to determine how data is formatted. One good example of this is the Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST), which publishes related reports about the strengths and weaknesses of forensic tools after they have been tested comprehensively for their ability to acquire mobile devices data. Also, since examination processes might vary depending on the device model, operating system and type of applications installed, it will always be wise prior to selecting any forensic tool to have an appropriate set of guidelines to be followed that is specific to the device model and operating system. Also, some tools can cause issues when including or downloading appropriate drivers.

It is important to note that these tools have varying capabilities and may not be appropriate for all operating systems. However, it is common to expect these tools to have the ability to be used for examination and analysis along with the data acquisition in the first place, although there are fewer
tools, which will only perform one or two processes and depend on other forensic tools for interoperability. In such cases, “examination and analysis using 3rd party tools are generally accomplished by importing a generated mobile device memory dump into a mobile forensics tool that supports 3rd party mobile device images” [47]. Therefore, security experts (the person in charge of finding/acquiring relevant information from the system) and forensics investigators (the person in charge of deciding what information is useful or not) typically will select the tool based on the tested operating system rather than the best available SDFT. This is a result of determining the type of information to be recovered and presented, and is why tools must be tailored to suit the needs of both security experts and investigators. In respect to this, it is worth knowing that some tools have simple search engines only capable of performing basic searches, while others might have rich search engines capable of performing generalized regular expression pattern (GREP) type searches.

From an analytic point of view, the following criteria were listed in *A Guide for Law Enforcement* by the U.S. Department of Justice [63] outlining what to look for in the extracted data:

- **Timeframe analysis** – Useful in determining when events have occurred in the system to associate them to a specific individual by either reviewing the time and date stamps contained in the file system metadata to link files of interest to the timeframes relevant to the investigation or reviewing system and application logs that may be present.

- **Data hiding analysis** – Can detect and recover hidden data that may indicate knowledge, ownership, or intent by correlating file headers to corresponding file extensions to identify any mismatches. It can also gain access to password-protected, encrypted, and compressed files. Also, it can be used for steganographic purposes and to gain access to host-protected areas (HPA), which indicate an attempt to conceal data.

- **Application and file analysis** – Where additional steps in the extraction and analysis processes may be indicated through identifying information relevant to the investigation. This is done by examining file content and metadata, correlating files to installed applications, identifying unknown file types, and examining user-configuration settings.

- **Ownership and possession** – This is useful in identifying the individuals who created, modified, or accessed a file and determining the ownership and possession of questioned data through associating the subject with the device at a particular date and time, identifying non-default locations of files of interest, recovering encrypted and protected passwords and identifying the contents of files that may indicate possession or ownership.

In this aspect, it is worth mentioning that the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence has been around for several years (the first version was
published in 2007, while the latest version is 5.0 and came out in October 2011). This guide
gives advice on the collection and preservation of digital data including mobile devices, but does
not dictate how forensic analysis should be carried out, as it will differ massively between
systems/devices. Below are the four principles recommended by ACPO for mobile devices seizure
and examination [64]:

- **Principle 1**: Data that is contained on the cell phone must not be altered and may be used
  in court.

- **Principle 2**: In some situations, the investigator may find it necessary to access the original
data stored on the cell phone. In these cases, the investigator must be proficient enough to
  perform this task and be able to give evidence explaining the relevance and the implications
  of their actions.

- **Principle 3**: Action logs of all processes applied to the cell phone should be made and
  conserved. The same results must be achieved if an independent third party examines the
  evidence.

- **Principle 4**: The person in charge of the investigation is responsible for making certain that
  the law and the core principles are followed.

### 2.5.4 Reporting

Special attention should be paid to the documentation of the whole process, starting from the
preservation, acquisition and storage of data, examination and analysis, and ending with the
reporting stage. Since investigators are faced with the challenges of timely recording as well as
documenting their procedures in producing the report, these actions, in many cases prove to be vital
for the report's acceptance or rejection by the court. Some tools are designed with built-in reporting
features that can be customised depending on individual needs and templates are available to
generate the output of all data acquired or to produce only selected relevant information. This data,
if not produced manually, is generated in one of the commonly known file-extension formats (.pdf,
.doc, .txt, .html, .csv). The report can also be in a hard-copy or soft copy format, and the type of
data to be presented will be the factor determining if the report is to be printed or instead turned in
on removable media such as a flash drive or external hard drive. Inconsistencies in time and date
need to be noted by recording those on the handset against those of a reference clock.
Chapter 2: Mobile Forensics Tools’ Technical Review

2.6 Causes and Factors Contributing to the Problem

Studies and surveys have revealed that SDFT tools vary in their capability for extracting different sets of evidences from different operating systems. During an investigation, the user’s perceived difficulties in being able to use those forensic tools in the desired manner may be attributed to the complexity of the software in front of the user. The other contributing factor, however, is a consequence of the fact that these tools become quickly outdated, with the ongoing, rapid production of new smart-phones devices and new versions of mobile operating systems.

Previous research and studies have revealed that there is a serious problem with utilizing and benefiting from SDFT that needs to be addressed by all levels of digital forensics stakeholders, starting from programmers and developers, security experts and ending with ordinary investigators. Approaches have differed, however, from one researcher to another in their method of tackling the issue. Amongst those researchers are Wazid et al [65] from the Cyber Forensics – India web site, who reached the conclusion that one of the most common challenges encountered by forensics tools/software within mobile devices is the tremendous amount of data, which is tremendous as a result of the continuous, on-the-move usage of mobile devices in people’s daily lives: be it to make calls, text people, e-mail friends, browse the net, take photos or videos, navigate through maps, and/or communicate with others through social networks. All these activities make it difficult to recover traces of events and evidence.

Another challenge is regarding the usability of forensics tools, where it was observed by Gunsch [66] that digital forensics tools are too technical and thus difficult to utilize fully. Consequently, the tools need to be tailored to suit the needs of both the security experts and the investigators (practitioners). Further usability issues were demonstrated in a user study by Hibshi et al [67], in which, interviewees demanded better designed tools capable of accommodating the requirements of users, interface systems, and operating intelligence. In particular, a “get evidence button” was a requirement for most surveyed users, i.e. to click on a button that can describe and present the information they are looking for. The study suggested that interfaces were overloaded with information and consistency was lacking amongst different tools, and even within different versions of the same tools. Figure 2-2 below, gives a clearer idea of how better interfaces can make life simpler to users; while complicated ones, where script language knowledge is required, as shown in Figure 2-3 can confuse users and end in unexpected results.
In addition to the usability and interoperability issues, the following are considered as major contributors to this problem.
Different operating systems: Unlike computer operating systems, mobile devices (smart-phones mainly) have many well-known operating systems, amongst which are Apple's Operating System (iOS), Google’s Operating System (Android), Microsoft’s Operating System (Windows Phone and Windows Mobile), Blackberry’s Operating System (RIM), and Nokia’s Operating System (Symbian). In addition, there are other, less popular operating systems, making it difficult for a single tool to be interoperable with all of them, and hence making the task of forensics analysis more challenging.

Tools are out-dated quickly: Smart-phones and their operating systems are changing rapidly, and there is a lag from the time a new phone comes out to the time until a Smart-phones Digital Forensics Tool can be updated or enhanced; the problem lies in the rate at which the smart-phones operating systems evolve, compared to the rate at which mobile forensics tools can be updated to encapsulate these changes.

Ease of reach by owner remotely: Unless all necessary measures and precautions are taken by the security expert or practitioner to protect the information held on the device in possession, e.g. by using a Faraday Bag, removing the SIM card, or utilizing an appropriate laboratory, then there is a good chance for the owner, if the device is connected to the internet, to be able to change the device's status or even remotely wipe all essential data within the device, including images, videos, SMS, documents and e-mails.

Anti-digital forensics (ADF): Such techniques and measures can be used by end users to protect their devices either from being hacked (in the case of a legitimate intention), or from being investigated (in the case of a criminally-minded person).

Smart-phones Digital Forensics Tools (SDFTs) are too technical: The process of installing, testing and using forensic tools has proven to be cumbersome and there was little commonality among those tools. There is a lack of clear information on how to install and configure forensic tools, as a great deal of time has been spent configuring those tools, working with their technical support documentation and web support. Some of the tools that were researched did not work as advertised, while others lacked in areas where they should have excelled.

Manufactures do not standardize on software and hardware components: the ability for investigators to gain access to the data in the smart phones varies and is not easily achieved. There are also barriers based on each manufacturer’s design process and if data encryption is invoked.

Tools are not user friendly: The demand for releasing newer tools and the time and effort it takes to understand their capabilities creates a usability/complexity issue. As a result, it has become very difficult to achieve a comprehensive assessment of newly released SDFT.
Chapter 2: Mobile Forensics Tools’ Technical Review

- **No uniform method of protecting the privacy of the data:** In many of the applications that were tested, usernames, passwords, conversation threads and links, location information, and financial information were stored in clear text and were accessible by simple and open source tools.

- **Large amount of data:** The result of the continuous, on-the-move usage of mobile devices is creating a tremendous amount of data, which makes it difficult to recover traces of events and evidence.

- Report of evidence: It can be a burden for investigators to concentrate on both the investigation in hand, as well as the need to report and document all investigative actions, which in many cases can prove to be vital for the acceptance or rejection of the report by the court. Fig. 2-4 below is an example by [67], of a screen-shot of a sample reporting-assistant tool illustrating how this problem could be tackled with a good reporting tool.

![Recent Actions Recorder](image)

Figure 2-4: Mock-up Reporting Tool Presented in the Survey [67]

### 2.7 Facts and Statistics Highlighting Digital Forensics Challenges

To illustrate the problems regarding the usability and interoperability of digital forensics tools in general, it is helpful to consider the results of user surveys. An online Digital Forensics Survey was conducted by the System Administration, Networking, and Security Institute(SANS) [68] and completed by more than 450 participants, where its ultimate purpose was to uncover the technical challenges faced by users of digital forensics tools, the findings were as follow:
• Only 54% of respondents indicated that their digital forensics capabilities are reasonably effective.

• Participants revealed that deficiencies in standards, tools and training are the major difficulties faced when dealing with forensics tools.

• Participants highlighted a gap in both capability and usability within used forensics tools.

• In terms of techniques and tools used, 62% pointed out that they acquire the device via physical data extraction (basic technique), while 59% interviewed the owner of the device (non-technical solution), and 55% pointed out that they acquire the device via logical data extraction. SANS suggests that this could be due to immaturity of tools or and investigators’ lack of experience with the tools.

Finally, a conducted study by McMillan et al [69] regarding the Increase in Mobile Phone Evidence in Criminal Activities presented in the 46th Hawaii International Conference on System Sciences, highlighted the following facts and issues.

• There was an indication that mobile phone evidence within criminal court cases is rising over time with some correlations to specific crimes, especially between images/videos and sexually-related crimes, which supports the argument that mobile phone devices are, potentially, a growing facilitator in criminal activity.

• The study indicated that mobile devices have the potential to be involved in a large variety of crimes, ranging from white-collar to terrorism and murder, and it reported that 64% of all drug-based analysis came from mobile phones, while 15% of all requests were related to illegal pornographic images.

2.8 Current Areas of Interest and Related Research

A research paper presented in the 8th Asia Joint Conference on Information Security by Chung-Nan et al [70], discussed the development of forensic software that is specifically intended for core use on iOS, with the utilization of Objective-C and Shell Script. In addition, there is an initiative by the National Institute of Standards and Technology (NIST) to design and implement a smart phones forensic program system for the iOS platform to enable the logical acquisition of data, when combined with an open source device (libimobile device (libiphone for short)) to extract data from a device. This approach provides quick access to data through the official USB teleport to investigators, so that the operating difficulty can be overcome when screens are locked, enabling
crucial information to be retrieved. In addition, the research is also conducting a comparison between iTunes and libimobile device to achieve better understanding of the problem space.

A further area of development is the creation of laboratories for Mobile Phone Forensics Undergraduate Courses at Purdue University, College of Technology, Computer and Information Technology [71]. The goal of these laboratories is to enhance the techniques and methods for hands-on forensics investigation. A collection of more than 800 unique phones was used to help build these labs. The Purdue University is planning to include in the future other mobile devices in addition to mobile phones, such as gaming devices, hand-held GPS systems, and VOIP and satellite phones.

Another research paper presented in the 45th Hawaii International Conference on System Sciences by Azadegan et al [72], discussed three anti-forensics Android applications that protect devices from being investigated by either completely deleting the contact list data (“Sudden Death”), partially deleting the data marked as sensitive (“Erase Sensitive Data”), or completely replacing the data with fake data (“Replace All Data”). This research confirmed the shortfall of current forensic tools and recommended the redesign of mobile phones forensics tools in order to enable accurate forensic data acquisition. As a result, this research is concentrating on extending those applications related to the protection of the phone's stored data, so that it is difficult for these (anti-forensic) applications to prevent the process of data extraction.

Another issue which is the subject of this thesis, is the difficulty of mobile forensics tools to extract the same type of information from various mobile devices and their operating systems. This problem prevails - despite the fact there are well-recognised commercial and open source forensics tools such as Ufed from Cellebrite; the Katana Forensics Tool Lantern; Blacklight Forensics Software; Paraben’s Device Seizure; and Micro Systemation XRY. Messmer [73] referred to what was highlighted by Darren Hayes, a computer forensics professor at Pace University, as he estimates that less than 40% of the smart-phone models in use today can be imaged. This point is supported by Andrew Hoog, co-founder and chief investigative officer at Chicago-based start-up via Forensics, who identified another contributing example of this issue, i.e. that there are more than 800 Android devices differing from each other in their operating systems. Hence, it has been clearly demonstrated that it is hard for forensic tools to keep up with the fast advancement in technology.

One other issue highlighted regarding the area of mobile forensics tools, is the research into the technical and legal aspects of mobile phone investigations, as findings by McMillan et al [69], discussed earlier in “Facts and Statistics”, revealed that there is a “lack of substantial, empirical research into how law enforcement is trying to tackle the growing issue of mobile phones within
crime”, requiring a more comprehensive research to be conducted in order to acquire a better understanding of the technical problems associated with mobile phone forensics. Table 2-2 summarizes the discussed current areas of interest and related research.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Area of research</th>
<th>Findings/Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The development of a forensic software that is specifically intended for the core use on iOS with the utilization of Objective-C and Shell Script</td>
<td>To overcome operating difficulty when screens are locked and hence crucial information is retrieved</td>
</tr>
<tr>
<td>2</td>
<td>Creating laboratories for courses in mobile phone forensics</td>
<td>Enhance the techniques and methods for hands-on forensics investigation</td>
</tr>
<tr>
<td>3</td>
<td>Extension of applications related to the protection of the phone’s stored data to prevent Anti-forensics ones from deleting data.</td>
<td>It confirmed the shortfall of current forensic tools and urged for the redesigning of mobile phones forensics tools for them to be able to accurately perform data acquisition</td>
</tr>
<tr>
<td>4</td>
<td>The difficulty of mobile forensics tools to extract the same type of information from various mobile devices and their operating systems</td>
<td>It was established that it is hard to keep up with the pace as a result of the fast advancement in technology</td>
</tr>
<tr>
<td>5</td>
<td>Investigating the Increase in Mobile Phone Evidence in Criminal Activities</td>
<td>Revealed that there is a lack of substantial research into how law enforcement is tackling the growing issue of mobile phones within crime</td>
</tr>
</tbody>
</table>

Table 2-2: Summary of current areas of interest and related research

### 2.9 Rights of Privacy and Anonymity

To be able to communicate with the rest of the world in an efficient way, people will need to start using various communication technologies provided for them, amongst which are smart-phones. However, this will not be free of risk, as individuals might start experiencing new security risks, vulnerabilities and intrusion of privacy. It is unlikely that any one would be in favour of having their personal information revealed publically, as privacy is “the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others”, [22] or in short, “the right to be left alone”. To this end, it can confidently be stated that a main concern of people these days is their privacy, and many may feel that it no longer exists with the wide use of communication technology. In today’s world, much information
about individuals is kept in central databases, which may be subject to exploitation by hackers and intruders or other persons who are not authorized.

Regarding this aspect, people’s concerns are valid and justified, especially if we know that uses of social services and welfare in many countries for identification purposes include valuable information about individuals such as their taxation, unemployment support, health and education status. The perceived value of this data opens the door to attempts by intruders to obtain and benefit from the stored information. As suggested by [74] Banisar, privacy can be divided into four major concepts: information privacy; privacy of communications; bodily privacy; and territorial privacy. The first two concepts are relevant to and will be covered by this research. We will therefore aim to analyse critically the importance and effectiveness of legal regulation in relation to the rights of human privacy and anonymity.

2.9.1 Privacy Background over the Net

Privacy means the freedom from intrusion, and the control of information about oneself, in addition to other definitions concerned with protecting sensitive personal information from being accessed without the prior knowledge or permission of the individual concerned. What is interesting about new technologies (smartphones in this instance) is that once they are used, it becomes easier for a person to access information, which is generally the motivation for using the technology. An undesirable consequence, however, is that it will also become easier for others to track the person as a result of the technology, though few people would be in favor of enabling others to watch over them. In this respect, studies reveal that privacy is invaded in many shapes and forms, and that people’s privacy is invaded often and easily in ways they would not imagine, as tracking methods can vary depending on the hardware used by the individual. As a result, many countries have faced public dissatisfaction over the invasion of their privacy, where the main fears of individuals, as stated by[75] include:

- People can be de-humanized.
- Governments and some organizations gain enhanced power over individuals.
- Society is becoming driven by technology-assisted bureaucracy, rather than by elected government.
2.9.2 Examples of Privacy Related Issues

Good examples of concerns for individuals include the selling of Tesco’s customer information, which was reported in 2005; the demands of the American Authorities for Google to allow them to observe what people are viewing on the Internet; and the ease of purchasing a list containing valuable information about children by a person assuming the name of a convicted murderer [76]. Another example related to privacy issues is the use of the Radio Frequency Identification (RFID) tags containing silicon chips, which according to [77], was invented in 1969 and patented in 1973 for the purpose of tagging cats, dogs and cars so they can be tracked remotely through the retrieval of the data stored within. Utilization of these devices has advanced these days to where they are now attached to, or incorporated into, products, as in the case of the Tesco–Gillette trial. In this trial, RFID tags were used by Gillette at a Tesco store in Cambridge (see Figure 2-5 below), [78], where Gillette shelves were fitted with RFID devices, which were able to sense removal of packages from the shelf and then take pictures of a customer handling them without their knowledge or acceptance.

Figure 2-5: The RFID is shown as the little black dot [78]

2.9.3 Laws related to privacy

From an early stage, privacy has been regarded as a fundamental human right, and many countries and organizations have taken the necessary steps to preserve it. This can be seen by the attention given to the subject, which is addressed by the United States judicial tradition of privacy protection (1890); the Universal Declaration of Human Rights (1948); and the Council of Europe’s Human Rights Convention (1950). In comparison, it must be noticed that no law existed in United Kingdom regarding privacy until 1998, when the Human Rights Act was approved. This law incorporates the
European Convention on Human Rights (ECHR), and the EU 1995 directives [79] and enforces the principles in English courts. Prior to this, privacy was protected through the means of linking cases in front of the court to similar ones within other areas of law, such as defamation laws and law of confidence. EU Directives concerning fair practices of information were passed in 1995, and came into effect in October 1998, which led to either amendments to laws in other European countries, the establishment of new laws (as in Italy); or their implementation whenever possible (as in the United Kingdom).

Australia is another example of a country paying special attention to privacy regulation. The country has established a Privacy Act which consists of two principles of law: the Information Privacy Principles (IPPs) mainly concerned with federal agencies and private sector organisations; and the National Privacy Principles (NPPs) dealing with the rights of individuals and national security agencies [80]. The Australian Privacy Act is similar to other privacy laws, covering almost the same concerns and issues addressed by other Acts such as EU directives and ECHR.

2.9.4 Smart-phone Devices Security

Nowadays, computing technologies support both mobile devices and desktops. If an attacker can manipulate smart-phones in the same way as a desktop, then they will become a target of attack. The more that people rely on smart-phones, the greater the tendency and interest of attackers to exploit these devices. One motivating factor for targeting smart-phones is the fact that they are ON almost all the time, which provides a greater opportunity for hackers to attack these devices. In addition, threats are becoming greater because of the widespread use of games downloaded onto them, along with the expanded popularity and use of social network applications via smart-phones, which can provide avenues of attack, as well as the attraction of online banking and payment transactions.

2.9.5 Smart-phone Devices Usability

Ease of use or “usability” is generally the most important factor to be considered when evaluating, and hence accepting any device. In this respect, a Delphi-method study [81] conducted amongst different groups of potential smart phone users, established that “there are relatively few tasks that are used with great frequency”. This study discusses the challenges of using mobile phones, and presents a new method for evaluating their usability. The method utilizes the computing power of the so-called “smartphone” to record user activities, including actions, sounds and screens. The recorded data is then transferred via a Wi-Fi network to the observer in a silent manner that does
not disturb the user. Experiments were conducted to confirm that this method meets the requirement of remote usability testing. The results showed that the data recording worked efficiently without disturbing the user, and that the data transfer was timely in an environment with good signal. It is concluded therefore that this method can be a practical way to study the usability of mobile phones.

### 2.9.6 Importance of Privacy

The current era of technology has made it impossible for individuals to be completely isolated from each other, or to maintain their historical level of privacy. Information about individuals can now be easily gathered and stored by specialist organisations and institutions, whether for the purposes of governmental surveillance of citizens, or for commercial exploitation of customers by companies. Concerns about privacy are evolving to form real barriers that could even scare people from using the technology. As a result, it has become necessary for governments to develop initiatives, controls and regulations to assess the impact of privacy breaches and ensure that security measures are adequate and that privacy can be protected. Breaches in these two areas are being treated increasingly seriously through tougher directives and legislation to discourage and prevent hackers from committing acts that cause harm to citizens.

The points discussed earlier about the concerns of individuals regarding their privacy invasion are of such importance that reasonable measures have now been taken by governments to address the public concerns of citizen rights to privacy. The Australian Privacy Act and European Directives regarding privacy were discussed as good examples to illustrate the importance of the issue. Privacy will always be a key factor to be considered and observed when dealing with smart-phones end-users. In particular, the principles noted in this section should always be adhered to, in order to ensure that privacy is not impeached in the pursuit of mobile security forensics.

### 2.10 Summary

In summary, this chapter began with a definition of what Digital Forensics is, and then narrowed the definition to Mobile Forensics; it also discussed in depth about smart-phone operating system technologies where a table was provided to serve the purpose; it then concentrated specifically on the most used famous ones, the Android operating system (Google) and the iOS operating system (iPhone); it explained how important knowledge is, where examiners must have the necessary skills and credentials to be able to parse this data; cellular network characteristics, in that finding out about them should be the first step taken by an examiner, since it will determine the forensic tool to be used for data acquisition, examination and analysis; and forensic procedures stages and steps,
where researchers have established that mobile phone forensic procedures should include four phases: preservation, acquisition, analysis and presentation (PAAP).

It was seen clearly that friendly usability of SDFT along with their interoperability to fully operate with various operating systems is not as easy as providers and/or practitioners might wish it to be. The main difficulties faced by investigators in regard to the problem of usability are the difficulty of relating different tools to each other, and sometimes even having difficulties understanding the features of newer versions of previously used tools; the other major drawback is the lack of interoperability of tools with different operating systems. The routes of this problem are well known and have been the subject of much research in the field, where many recommendations and solutions have been proposed to reduce the effects of this problem on practitioners dealing with these tools on a daily basis.
The industry standard tools for mobile analysis are XRY and Cellebrite. In addition, the newest versions of Guidance Software’s EnCase and Access Data’s FTK also purport to read mobile devices. However, it will take some time before these two become ‘reliable’ as they have always been computer forensic tools, rather than purpose-built mobile forensic tools like XRY and Cellebrite. On the other hand, there are other mobile forensic tools that read mobile data but only from a specific set of devices/operating systems. Lantern is a good example of a tool specifically built to deal with specific operating systems, which is iOS in this case. Another example is Oxygen Forensic Suite, which is utilising an agent application to enable it to perform both logical and physical acquisition of data. Finally, EnCase, which starts acquisition with the SIM and then proceeds to the device, [32] “claims that the WaveShield technology used in it, is the only extensively tested technology, to ensure integrity of evidence and reliability for field acquisitions”.

When considering forensic tools, it must be realised that most of them rely on the operating system through the utilisation of commands and protocols. This, as a result, will require the phone to be operational (On), so that visible data is recovered. Flasher tools are good examples of those which can be used for acquiring data from the flash memory non-invasively [82]. As discussed earlier, the recovery of deleted data will have to be done through physical acquisition. Also, it must be noted that besides acquiring data from smart phone devices, a forensic tool must not alter the data contents, and at the same time, must maintain the integrity of the calculated hashes.

The most important thing to keep in mind when designing a forensic tool or software is to make sure that it meets both the 1) core requirements, where every tool must feature, and which must remain consistent with all types of smart-phones, and the 2) optional requirements, where they are only needed on some tools for certain types of smart phones or operating systems. In addition, tools must undergo certain tests to prove that they are capable of what they were meant for, followed by an assertion statement to report that the tool was checked and performed according to the set conditions. Since investigators are sometimes forced to use different forensic tools to ensure that all evidence is extracted from the examined device, this is by itself good justification for the need for a tool that is capable of displaying all acquired data and information from one device, which in a way is aiding investigators in displaying those acquired results from different toolsets and by different methods.
Listings of best mobile forensics tools were not easy to find, and most of the listings shown in the table below are either for computer forensics, digital forensics, or forensics investigation tools in general. However, it is worth highlighting that most of the mentioned tools have capabilities of investigating mobile devices. All attempts were made to test and analyse some of the top best popular known tools on this research, but due to obstacles and limitations beyond the control of the researcher, only some of the top tools were tested. Some of the obstacles and limitations can be attributed to the fact that some of the tools were available for a 14 to 30-day evaluation period, and in best cases for a 6-month trial period; other tools had to be purchased and some tools were too expensive for the researcher to purchase. Although, there were a number of successes while working with mobile forensic tools, the biggest problem encountered was with the drivers and getting the tool to recognize the phone, especially the iPhones in particular. Another challenge faced with trial versions in that they do not provide full functionality, such as not allowing extraction of files.

The following are some of the tools that were attempted but ran into issues when trying to installing them: Elcomsoft Password Digger, Belksoft Evidence Center Ultimate, Lima application, Blackbag, Paladin, and Katana. While there was a success in testing and evaluating the following tools: CAINE, DEFT, OXYGEN Forensic Suite, Autopsy (Kali virtual machine), MobilEdit Analyst, Mobile Phone Examiner Plus (FTK MPE), Device Seizure v 7.4, NowSecure (Santoko) Community Edition v 3.2, Santoku virtual machine image (6.1.5), AF Logical OSE tool (6.1.6), Andriller tool and Exif tool (6.2.4), USB Write Blocker.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 SIFT</td>
<td>Digital Forensics Framework</td>
<td>Autopsy</td>
<td>SIFT</td>
<td>Autopsy</td>
</tr>
<tr>
<td>2 ProDiscover Basic</td>
<td>OCFA</td>
<td>DEFT</td>
<td>CAINE</td>
<td>Encrypted Disk Detector</td>
</tr>
<tr>
<td>3 Volatility</td>
<td>CAINE</td>
<td>The Volatility Framework</td>
<td>KALI</td>
<td>Wireshark</td>
</tr>
<tr>
<td>4 The Sleuth Kit</td>
<td>X-Ways Forensics</td>
<td>Santoku</td>
<td>DEFT</td>
<td>Magnet RAM Capture</td>
</tr>
<tr>
<td>5 FTK Imager</td>
<td>SIFT</td>
<td>DFF</td>
<td>Martiux</td>
<td>Network Miner</td>
</tr>
<tr>
<td>6 Linux “dd” utility</td>
<td>EnCase</td>
<td>OCFA</td>
<td>Santoku</td>
<td>NMAP</td>
</tr>
<tr>
<td>7 CAINE</td>
<td>Registry Recon</td>
<td>CAINE</td>
<td>Volatility</td>
<td>RAM Capturer</td>
</tr>
</tbody>
</table>
### Initial Mobile Forensics Tools Analysis

A parallel desktop was installed in a MacBook Air, so that some forensic tools could be tested using Windows, as most of those tools can only be installed on Windows platform. Windows 10 was then installed on the parallel desktop followed by installation of Mobile Forensic Software. Unfortunately, 10 days later, Windows 10 ceased working, which meant reinstalling Windows along with Office and other appropriate applications, followed by reinstallation of the Mobile Forensic Software again. All of which required re-obtaining newer keys for the operating systems and their related applications for activation purposes.

---

<table>
<thead>
<tr>
<th>#</th>
<th>Oxygen Forensics Suite</th>
<th>The Sleuth Kit</th>
<th>X-Ways Forensics</th>
<th>Linux &quot;dd&quot; utility</th>
<th>Forensic Investigator</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Free Hex Editor Neo</td>
<td>Libforensics</td>
<td>Helix3 Enterprise</td>
<td>Sleuth Kit (Autopsy)</td>
<td>FAW</td>
</tr>
<tr>
<td>10</td>
<td>Bulk Extractor</td>
<td>Volatility</td>
<td>The Sleuth Kit (TSK)</td>
<td>Xplico</td>
<td>HashMyFiles</td>
</tr>
<tr>
<td>11</td>
<td>DEFT</td>
<td>WindowsSCOPE</td>
<td>SIFT</td>
<td></td>
<td>USB Write Blocker</td>
</tr>
<tr>
<td>12</td>
<td>Xplico</td>
<td>TCT</td>
<td>Xplico</td>
<td></td>
<td>Crowd Response</td>
</tr>
<tr>
<td>13</td>
<td>LastActivityView</td>
<td>Oxygen Forensic Suite</td>
<td>Oxygen Forensic Suite</td>
<td></td>
<td>NFI Defraser</td>
</tr>
<tr>
<td>14</td>
<td>DSI USB Write Blocker</td>
<td>Bulk Extractor</td>
<td>PlainSight</td>
<td></td>
<td>ExifTool</td>
</tr>
<tr>
<td>15</td>
<td>Mandiant RedLine</td>
<td>Xplico</td>
<td>EnCase</td>
<td></td>
<td>Toolsley</td>
</tr>
<tr>
<td>16</td>
<td>PlainSight</td>
<td>Mandiant RedLine</td>
<td>Registry Recon</td>
<td></td>
<td>SIFT</td>
</tr>
<tr>
<td>17</td>
<td>HxD</td>
<td>COFEE</td>
<td>LibForensics</td>
<td></td>
<td>Dumpzilla</td>
</tr>
<tr>
<td>18</td>
<td>HELIX3</td>
<td>P2 eXplorer</td>
<td>XRY</td>
<td></td>
<td>Browser History</td>
</tr>
<tr>
<td>19</td>
<td>Paladin Forensic Suite</td>
<td>PlainSight</td>
<td>Mandiant RedLine</td>
<td></td>
<td>ForensicUserInfo</td>
</tr>
<tr>
<td>20</td>
<td>USB Historian</td>
<td>XRY</td>
<td>P2 eXplorer</td>
<td></td>
<td>Black Track</td>
</tr>
<tr>
<td>21</td>
<td></td>
<td>HELIX3</td>
<td>Bulk Extractor</td>
<td></td>
<td>Paladin</td>
</tr>
<tr>
<td>22</td>
<td>Cellebrite’s UFED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CAINE</td>
</tr>
</tbody>
</table>

**Table 3-1: Summary of Top Digital Forensics Tools**
For this report, three mobile forensics tools of the ones currently available for the mobile forensics community have been investigated, as can be seen in (Table 3-2) below. It was determined that those tools will benefit from creating and developing a standard Process Based Mobile Forensics Framework.

<table>
<thead>
<tr>
<th>Tool Name</th>
<th>Version</th>
<th>O/S</th>
<th>License</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deft</td>
<td>8</td>
<td>Linux/Windows (DART)</td>
<td>Open Source</td>
<td>“A distribution made for Computer Forensics, with the purpose of running live on systems without tampering devices.”</td>
</tr>
<tr>
<td>CAINE</td>
<td>5</td>
<td>Linux</td>
<td>Open Source</td>
<td>“Offers a complete forensic environment that is organized to integrate existing software tools as software modules and to provide a friendly graphical interface.”</td>
</tr>
</tbody>
</table>

Table 3-2: Summary of Tools used for Analysis and Framework Development

The three tools are: Oxygen Forensics Suite 2014 [38], Computer Aided Investigative Environment (CAINE) version 5.0 [39] and Digital Evidence & Forensics Toolkit (DEFT) version 8 [40]. These three tools were selected because they contain mobile forensics tools built into them. They also cover different platforms: Oxygen is a Windows based commercial software while CAINE and DEFT are Linux based and open source. To start with, we used iPhone devices to test these tools to gain a good understanding of their strengths, weaknesses, and how reporting is structured. Additional Mobile Forensics Tools will be installed to become more familiar with commercial and open source tools that exist in the market (see chapter 5 for Advanced Forensics Tools Analysis).

We also used mobile smart phone devices with different operating systems (Table 3-3).

<table>
<thead>
<tr>
<th>Device Brand</th>
<th>Model</th>
<th>Version</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>iPhone</td>
<td>4</td>
<td>iOS 7</td>
</tr>
<tr>
<td>Samsung</td>
<td>Focus</td>
<td>2</td>
<td>Windows 7.5</td>
</tr>
<tr>
<td>Generic</td>
<td>S580</td>
<td>S580</td>
<td>Android 4.1</td>
</tr>
</tbody>
</table>

Table 3-3: Summary of Phones and Operating Systems used with Various Forensics Tools
Chapter 3: Mobile Forensics Tools Analysis

3.1.1 Oxygen Forensic Suite 2014

The Oxygen software was easy to install and it provided wizard like installation instructions. The process took around 30 minutes to install and it did not create any issues. The Oxygen software offers an extractor option where users can select different types of forensic analysis options (Figure 3-1). The Oxygen software was able to detect the iPhone connected to the computer and provided us with wizard like forms to guide us through what we want to test. After entering the basic information required in the wizard forms, Oxygen software took about two hours to perform its analysis. The information provided by the reporting engine was comprehensive and the interface was easy to use. The reporting screen is divided into different sections (total of 16 sections) and contained information specific to each section (Figure 3-2).

Some of the strengths of the Oxygen Forensic Suite 2014 are:

- Easy to install: Oxygen provided easy to use screens for guidance during the installation process. Very few decisions needed to be made to ensure correct installation of this software.
- Easy to follow extraction options: Simple and easy to follow forms are used throughout this software which makes it a preferred option for many users that are not familiar with Linux based setup.
- Many report analysis exporting options: The reports can easily be exported into many of the common formats (e.g. PDF, Excel, XML). The ability to extract the forensics information is critical for exchange of information and comparison with other mobile forensics software.

Oxygen Forensic Suite 2014 has a few disadvantages:

- Price: unlike the other two tested forensic software packages, Oxygen is commercial software and requires a relatively significant investment to purchase.
- File size: The size of the reports was very large and may create issues for users without adequate hard drives.
- Weak plug and play option: We tried using other mobile phones to test with this tool but drivers were required to be installed in order for Oxygen to read the devices correctly. It also didn't provide enough information to troubleshoot these issues.

Overall, the software use was satisfactory, with the conclusion that additional testing will be required to sufficiently become familiar with the software and to be able to create the proposed framework.
Figure 3-1: Oxygen Forensic Extractor Screen

Figure 3-2: Oxygen Forensic Reporting Information Screen
3.1.2 Computer Aided Investigative Environment (CAINE) 5.0

CAINE is a digital forensics project developed in Italy and is a Linux based software. CAINE is open source software which means that many developers can add and improve this software. It also offers a Windows based beta version but we were not able to test CAINE in that platform because it did not work during our testing process. The installation was extremely difficult and required much trial and error. We eventually had to install a Virtual Machine first and then install CAINE inside the virtual machine (Figure 3-3). Oracle VM VirtualBox Manager was installed first, and then CAINE was installed inside the VM VirtualBox. Once installed, CAINE provides many options for the forensics community but its Mobile Forensics offerings are limited (Figure 3-4). The tool for analysing iPhones can only be used with backups of iPhone and not with the actual device.

The main strength of the CAINE software is:

- Open source software: CAINE is open source which means that no monetary investment is required. It also means that the software can be improved by many developers.

CAINE software has a few disadvantages:

- Installation: Installing CAINE was very difficult and very few and inadequate instructions were provided.
- Lack of Mobile Forensics options: Only two options were provided for mobile devices, iPhone and Blackberry devices. The Blackberry is a command based tool and will require users to be familiar with scripting to benefit from such a tool.
- No original iPhone analysis utility: The iPhone utility was an open source tool and not a tool developed by CAINE (Figure 3-5). The "IP Backup Analyser 2" was developed at MIT and is used by a few other mobile forensic programs. The following direct link (http://www.ipbackupanalyzer.com) can be used for more experiments.
- Limited Reporting options: The IP Backup Analyser 2 provides very limited reporting options and does not provide any good export functionality options.
Figure 3-3: Oracle VM VirtualBox Manager

Figure 3-4: CAINE Mobile Forensics Tools
DEFT is an open source software based on Linux and runs as a virtual application. Like CAINE, DEFT is also developed in Italy and can be installed on a windows machine. DEFT has more mobile forensic tools than CAINE but it also uses "IP Backup Analyser 2" as the iPhone analyser (Figure 3-6). The IP Backup Analyser 2 uses a backup of an iPhone to analyse the information in the files. It then provides "Plugins" and "Reports" (Figure 3-7) to display the information from the iPhone device. The "Plugins" and "Reports" combination provide basic information about the device being analysed.

The main strength of the DEFT is:

- Open source software: Like CAINE, DEFT is open source.

DEFT software has a few disadvantages:

- Installation: Like CAINE, DEFT was very difficult to install and no information was provided on how to navigate the environment once it was installed.
- No original iPhone analysis utility: Like CAINE, the iPhone utility was an open source tool and not a tool developed by DEFT.
- Limited Reporting options: The IP Backup Analyser 2 provides very limited reporting options, and is not geared to provide good exporting options.

Figure 3-6: DEFT Mobile Forensics tools

Figure 3-7: IP Backup Analyser 2 Plugins and Reports Menu
3.2 Advanced Mobile Forensics Tools Analysis

In its attempt to establish a methodology for testing computer forensic software tools and to determine if a tool can accurately acquire specific data objects populated onto the device or SIM, NIST developed specific and common rules to govern tool specifications [88] and [89]. This can clearly be seen in (Appendix C) which illustrates accurate acquisition copies of data objects from the device. In this appendix, an explanation with examples is provided on the step by step procedures of confirming testing assertions of a specific tested forensic tool, which was found to be very useful to use as a guideline when testing or comparing between various forensic tools, through the utilisation of the NIST outcome reports applied on various forensic tools.

NIST gives an explanation about abbreviations included within the table, such as: The ID column identifies the assertion, where SPT-CA-01/ MDT-CR, for instance, stands for Smart Phone Tool-Core Assertion-1/ and Mobile Device Tool-Core Requirement respectively, and at the same time implying that it is a core assertion, which means that the tested tool must be capable of carrying out the mentioned task. While SPT-AO-01/MDT-RO stands for Smart Phone Tool-Assertion Optional-1/ and Mobile Device Tool-Requirement Optional respectively, implying that it is an optional assertion, which means that it will only be tested if a tool supports the feature. Assertions are stated in the Test Assertion column to describe conditions that can be checked after a test is executed, while additional information pertaining to the assertion is provided in the Comments column.

NIST also provides an overview of how individual test assertions are measured. These assertion measurements are divided into Connectivity, Data Acquisition and Interpretation, which include (Presentation, Subscriber and Equipment Related Data, Personal Information Management (PIM) Data, Call Logs, Text Messages (SMS, EMS, MMS), Stand-alone Multi-media Data, Application Data and Internet Related Data), Location Related Data, Tool Acquisition Variations, Device Data Not Modified, Generated Reports / Preview-Pane, Case File/Data Protection, SIM PIN/PUK Authentication, Physical Acquisition, Non-ASCII Character Presentation, Stand-alone Acquisition, Hashing and GPS Reporting. In addition, NIST provides Abstract Test Cases to describe the combinations of test parameters required to fully test each assertion and the results expected for the given combination of test parameters.

In order to address the research questions mentioned earlier so that an enhanced Process Based Framework is established, an experiment for analysis of certain tools was designed. Forensic tools under evaluation were installed on a dedicated host computer operating with the required platforms as specified by the tools. In this case, tests were run on a Windows 10 version 1511 laptop with 32 GB of RAM. Each examined forensic tool was examined on four different devices; once on an iPhone 6 device (iOS 9.2.1), once on a jailbroken iPhone 4 device (iOS 7.1.2), once on a Samsung
SM-G316HU (Android 4.4.4) device, and finally on a rooted Samsung GT-S6812i (Android 4.1.2) device. The reason for one of the two iPhones being jailbroken and one of the two Androids being rooted, was so that the difference in the analysis can be observed and therefore a better view is gained. Table 3-4 presents information about the tested devices.

<table>
<thead>
<tr>
<th>Make</th>
<th>Model</th>
<th>Operating System</th>
<th>Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iPhone</td>
<td>iPhone 4</td>
<td>Apple (jailbroken)</td>
<td>7.1.2</td>
</tr>
<tr>
<td>Apple iPhone</td>
<td>iPhone 6</td>
<td>Apple</td>
<td>9.2.1</td>
</tr>
<tr>
<td>Samsung</td>
<td>GT-S6812i</td>
<td>Android (Rooted)</td>
<td>4.1.2</td>
</tr>
<tr>
<td>Samsung</td>
<td>SM-G316HU</td>
<td>Android</td>
<td>4.4.4</td>
</tr>
</tbody>
</table>

Table 3-4: Tested Mobile Devices

A testing table template was created following NIST procedures, where testing results of tools and hence their analysis can be found in Appendix A.1 - A.5. The objectives were to compare the obtained results with those of NIST ones in the case of the tools already tested by NIST so that a differentiation of their findings is established, or to test and check the reliability of those not tested by NIST while - as stated earlier - following their testing procedures, where the internal memory of the source devices was populated with a known dataset, so that a better understanding is captured. This way, a case can be built up for a framework that can provide appropriate guidelines on how to use forensics tools. Though there are many other operating systems, the focus was concentrated on the two-major dominating operating systems, iOS and Android, although Windows phone operating system is promising. The decision was reached not to cover it because of the small market share it currently has, in addition to it not having as many communities compared to the other two.

Reports of tested tools, as can be seen in the appendixes, are divided into five sections. Section 1 identifies and provides a summary of any significant anomalies observed in the test runs. Section 2 identifies the mobile devices used for testing. Section 3 lists the testing environment and the internal memory data objects used to populate the mobile devices. Section 4 provides an overview of the test case results reported by the tool. Finally, section 5 lists advantages and disadvantages of the tested tool, along with a comparison of the findings of NIST when the tool has been tested by NIST.

3.2.1 MobilEdit Analyst v 8.5 Forensic Tool

MobilEdit Analyst v8.5 is mobile forensic software for data acquisition from phones, smartphones and other mobile devices. For more information about the discussed tool, refer to MobilEdit Web
Chapter 3: Mobile Forensics Tools Analysis

The tool was tested for its ability to acquire active data from the internal memory of supported mobile devices. Below is a summary of the report findings; the full detailed report can be found in Appendix A.1.

3.2.1.1 Major Highlights

- **Connectivity**
  - On the first attempt the tool failed to recognize the Samsung phones, this was despite downloading the drivers for the Android and the iPhone. It took numerous attempts to get the Android devices recognized. The devices had to be placed in Developer mode then the acquisition could take place. The acquisition was only for the logical data; the tool does not perform physical acquisitions of the phone. Eventually, acquisition was completed on both Samsung devices.
  - With the iPhones, again there were connection problems. The iPhone 6 was recognized and the data was backed up from the phone. The iPhone 4 was not recognized despite numerous attempts and manual download of the drivers. The cable had to be an official cable for the phone to be recognized; once the phone was recognized, all of the logical data was acquired successfully.
  - The lack of capability to perform a physical acquisition is a major concern if the analyst is trying to recover anything that has been deleted.

- **Equipment / Subscriber related data:**
  - All Subscriber related data (i.e., MSISDN) was acquired for all devices.

- **Personal Information Management (PIM) data:**
  - The file system was recovered on the iPhone 6, but not the iPhone 4. Since the iPhone 4 was the one that had been jailbroken. It may have prevented the access, although a jail broken phone is usually the easier one to conduct an acquisition on. The tool installs an app on the phone, so that might have had something to do with it. A similar result was obtained with the rooted phone. The phone that was not rooted produced the file system, whereas the rooted phone did not successfully acquire the file system.
  - Contacts/address book entries were acquired for all devices.
  - Calendar entries were acquired for all devices.
  - Memo/Note entries were acquired for all devices.
  - The call logs were empty.

- **Internet Related Data:**
  - The phones had been cleared of bookmarks, but the bookmark folders were recovered.
Chapter 3: Mobile Forensics Tools Analysis

- **Social Media Related Data:**
  - Social media related data was non-existent in the phones during logical data extraction.

- **Case File Data Protection:**
  - Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

- **Internal Memory Data Objects:**
  - MobilEdit Analyst version 8.5 was measured by analyzing logically acquired data from the internal memory of pre-populated mobile devices. An example of the Logical File information recovered from the iPhone4 is shown in the following figure:

![Files - iPhone](image)

**Figure 3-8: iPhone 4 Recovered Image of the Logical File Information**

### 3.2.1.2 Test Results

This section provides the test cases results reported by the tool. Sections 3.2.1.2.1 and 3.2.1.2.2 below identify the mobile device operating system type (i.e., Android, iOS) used for testing MobilEdit Analyst v8.5.

#### 3.2.1.2.1 Android Mobile Devices

All of the data from a logical view was accessed and acquired by the tool. The file systems were only acquired from the device that had not been rooted. The submitted devices had gone through a pseudo wipe which made the logical acquisition fairly easy. Having said that, despite the attempted wiping of the device, there were SMS messages as well as other artifacts discovered (two graphic images and one video).
3.2.1.2.2 iOS Mobile Devices

Connecting to the iOS devices proved to be a big challenge; the acquisition required iTunes, and the version had to be the latest one or the connection would not identify the phone. It took numerous attempts to connect to the phone, and at one point the cable had to be changed to the official cable for the iPhone 4; without it, the connection would not work. The file system was acquired on the iPhone 6 that had not been jailbroken, but on the jailbroken iPhone 4 the acquisition of the physical file system failed which is a result different than expected.

3.2.1.3 Tool Analysis Summary

The MobilEdit Analyst tool is adequate for e-discovery and other types of cases where the perpetrator does not have knowledge about hiding information etc., but without the capability of physical acquisition the tool is not a solid choice for a forensics tool. In this case, the tool could not obtain a physical image of the jailbroken iPhone4 and the rooted Samsung GT-S6812i. Having said that, the tool provided data (not all the data) for all 4 phones. As with any forensics solution, there is no perfect tool, and a blend of two or more tools is best.

- Advantages:
  - Ease of acquisition once device is discovered.
  - Simple menu and easy to follow format.
- Disadvantages:
  - Too difficult to recognize devices.
  - Has to maintain constant connection to the Internet.
  - Logical acquisitions only.
  - Did not discover as much as some of the other tools even with logical acquisition only.

- When comparing findings of this report with those of NIST ones, the following were observed:
  - Similar results were experienced with respect to connectivity.
  - There was no problem experienced with acquisition of the phone device data.
  - The sample set for testing was much smaller and less diverse than the NIST report.

3.2.2 Mobile Phone Examiner Plus v 5.6.0.8

Mobile Phone Examiner Plus is a stand-alone mobile investigation solution that includes enhanced smart device acquisition and analysis capabilities. With a different approach to digital mobile forensics, “MPE+ allows mobile forensics examiners to take control of the investigation by
providing them with unique tools necessary to quickly collect, easily identify and effectively obtain the key data other solutions miss” [91]. As can be seen from Figure 3-9 below, the tool was a 20-day free trial. The tool was tested for its ability to acquire active data from the internal memory of supported mobile devices. Below is a summary of the report findings, where the full detailed report can be found in Appendix A.2.

Figure 3-9: An Image showing that the Tool is a 20 Day Free Trial

3.2.2.1 Major Highlights

- **Connectivity**
  - No matter what measures were explored, the tool was not able to detect the iPhone devices. Research was conducted and numerous attempts were made without success on the iPhone. The tool has the best options and analysis, but no reviews could be obtained of the iPhone’s information while testing. The capability of physical examination was identified, so that was attempted, and the iPhones were recognized, but the tool continued to prompt for the phone’s password when there was not one, and as a result the physical extractions were not successful.
  - Acquisition was completed on both Samsung devices, and therefore the summary below of the results that follow is for the Samsung (Android) devices only.

- **Equipment / Subscriber related data:**
• All Subscriber related data (i.e., MSISDN) was acquired for the Samsung devices.

  ▪ **Personal Information Management (PIM) data:**
    • The file system was recovered on the rooted phone, but not on the phone that had not been rooted.
    • Contacts/address book entries were acquired for both Samsung devices.
    • Calendar entries were acquired for both Samsung devices.
    • Memo/Note entries were acquired for both Samsung devices.
    • The call logs were empty.

  ▪ **Internet Related Data:**
    • The phones had been cleared of bookmarks, but the bookmark folders were recovered.

  ▪ **Social Media Related Data:**
    • Social media related data was non-existent in the phones during logical data extraction.

  ▪ **Case File Data Protection:**
    • Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

  ▪ **Internal Memory Data Objects:**
    • Mobile Phone Examiner Plus was measured by analyzing logically acquired data from the memory of sample phones.

### 3.2.2.2 Test Results

This section provides the test cases results reported by the tool. Sections 3.2.2.2.1 and 3.2.2.2.2 identify the mobile device operating system type (Android in this case) used for testing MPE Plus v5.6.0.8.

#### 3.2.2.2.1 Android Mobile Devices

All of the data from a logical view was accessed and acquired by the tool. The file systems were only acquired from the device that had been rooted. The submitted devices had gone through a pseudo wipe which made the logical acquisition fairly easy. The rooted Android phone allowed for a physical acquisition, and this is when the tool excelled by carving out 664 images and files from the file system that was much more detailed than other tools. The only downside of this was the tool locked at 99.9% complete and did not provide the completion message ever. Additionally, the physical extraction took more than 3 hours and 100 GB of hard drive space, which is considered excessive.
3.2.2.2 iOS Mobile Devices

Despite numerous attempts and following the instructions and FAQs from the support site, the acquisition of the iOS devices was not possible.

3.2.2.3 Tool Analysis Summary

The Mobile Phone Examiner Plus tool is adequate for examination of the Android based phones, and provided an adequate means to extract information for forensics analysis. The tool has provided data for only 2 of the 4 phones. However, the data extracted was above and beyond the other phone tools, especially when it came to the file carving capability from the physical file system. As with any forensics solution, there is no perfect tool, and a blend of two or more tools is best.

- **Advantages:**
  - Ease of acquisition of the Android devices, and extraction of the data for information analysis.
  - Extraction and details of the device information was better and more than the other tools once the device was recognized.
  - The file carving capability and results were exceptional.
  - Simple menu and easy to follow format.

- **Disadvantages:**
  - Too difficult to recognize devices, especially when it comes to the inability to gather information from the iOS phones.
  - Program stability seemed to be an issue, numerous crashes of the tool, seemed to work best on Windows 10.

- When comparing findings of this report with those of NIST ones, the following were observed:
  - The NIST report is from 2014.
  - The NIST experience of not recovering subscriber data was not witnessed in this testing.
  - There were no call logs missed with the data set of this testing as reported in the NIST testing.
  - Application data was recovered in the testing but was not recovered in the NIST testing.
  - The testing from the NIST report was not indicative of what was experienced in this testing.
3.2.3 Autopsy v4.0

Autopsy v4.0 is the premier end-to-end open source digital forensics platform. Built by Basis Technology with the core features you expect in commercial forensic tools, “Autopsy is a fast, thorough, and efficient hard drive investigation solution that evolves with your needs”. For more information about the discussed tool, refer to Basistech web page [92]. The tool was tested for its ability to acquire active data from the physical file system of the device. Below is a summary of the report findings, where the full detailed report can be found in Appendix A.3.

3.2.3.1 Major Highlights

- **Connectivity**
  - The Autopsy tool does not acquire the data from the phone, but instead it requires a phone image to be added to it.
  - Acquisition of the physical file system from the MobilEdit tool was used as the data source for the Autopsy tool.
  - Only the data for the rooted Android phone was successfully added as a data source.
  - Numerous attempts to add other phones physical images were not successful.

- **Equipment / Subscriber related data:**
  - All Subscriber related data (i.e., MSISDN) was acquired for the rooted Samsung device.

- **Personal Information Management (PIM) data**
  - The file system was recovered on the rooted phone only.
  - Contacts/address book entries were acquired for the rooted Samsung device.
  - Calendar entries were acquired for the rooted Samsung device.
  - Memo/Note entries were acquired for the rooted Samsung device.
  - The call logs were empty.

- **Internet Related Data:**
  - The phone had been cleared of bookmarks, but the bookmark folders were recovered.

- **Social Media Related Data:**
  - Social media related data was non-existent in the phone.

- **Case File Data Protection**
  - Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

- **Internal Memory Data Objects:**
• Autopsy was measured by analyzing file system acquired data from the memory of sample phones.

3.2.3.2 Test Results

This section provides the test cases results reported by the tool. Sections 3.2.3.2.1 and 3.2.3.2.2 identify the mobile device operating system type (Rooted Android) used for testing Autopsy v4.0.

3.2.3.2.1 Android Mobile Devices

The file system was only acquired from the device that had been rooted. The submitted devices had gone through a pseudo wipe which made the logical acquisition fairly easy. Despite the attempted wiping of the device there were a number of artifacts recovered from the physical image of the file system. The tool was good in taking the file system image and extracting the pertinent information.

3.2.3.2.2 iOS Mobile Devices

Despite numerous attempts and following the instructions and FAQs from the support site, the acquisition of the iOS devices was not possible due to the inability to acquire the image.

3.2.3.3 Tool Analysis Summary

The Autopsy tool is more than adequate for examining the Android based phones that have been rooted and a physical image extracted. Having said that, the tool provided data for only 1 of the 4 phones due to the requirement for an image, but the data extracted was comparable to other tools, especially when it came to the file carving capability from the physical file system. As with any forensics solution, there is no perfect tool, and a blend of two or more tools is best.

• Advantages:
  • Open Source.
  • Comprehensive dashboard.
  • The file carving capability and results were exceptional.
  • Simple menu and easy to follow format.
  • Simple process of analysis.
  • Simple installation, best of all the tools tested.

• Disadvantages:
  • Requires the image of the file system.
  • No capability to acquire a file system.
• The tool did not provide thumbnails of the carved files. This might be a setting, but it was not discovered during the testing
  ▪ As for comparison purposes, could not discover any reports for the Autopsy tool within the NIST list of reports for the purpose of comparing with this report.

3.2.4 Device Seizure v 7.4

“Device Seizure v 7.4 was the first mobile forensic tool on the market. Designed from the ground up for forensically sound examinations of cell phones and other devices, DS set the industry standard for mobile investigations”. For more information about the discussed tool, refer to Pareben’s web page [93]. The tool was tested for its ability to acquire active data from the internal memory of the phone device. Below is a summary of the report findings, where the full detailed report can be found in Appendix A.4.

3.2.4.1 Major Highlights

  ▪ Connectivity
    • The Device Seizure tool loads its own drivers during the installation process; this is to assist with the detection of a phone when it is connected.
    • The tool was able to detect the phones when connected, but depending on a number of factors, the tool could not provide the extraction of the information that was required for the testing.
    • Despite this, the tool does have some excellent capabilities; however, with the limitations and the restrictions on the trial version of the tool, it makes it difficult to evaluate the tool.
  ▪ Equipment / Subscriber related data:
    • All Subscriber related data (i.e., MSISDN) was acquired for all of the tested devices apart from the rooted Samsung GT-S6812i.
  ▪ Personal Information Management (PIM) data
    • Contacts/address book entries were acquired for all of the tested devices apart from the rooted Samsung GT-S6812i.
  ▪ Internet Related Data:
    • The phone had been cleared of bookmarks, but the bookmark folders were recovered.
  ▪ Social Media Related Data:
    • Social media related data was non-existent in the phone.
Case File Data Protection

- Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

Internal Memory Data Objects:

- Device Seizure version 7.4 was measured by analyzing the contacts from all of the tested devices apart from the rooted Samsung GT-S6812i. This is because the Trial version limits the recovery to contacts only. This is shown in Figure 3-10:

![Device Seizure Trial Version limits the Recovery to Contacts](image)

**Figure 3-10: Device Seizure Trial Version limits the Recovery to Contacts**

### 3.2.4.2 Test Results

This section provides the test cases results reported by the tool. Sections 3.2.4.2.1 and 3.2.4.2.2 identify the mobile device operating system type (Android or iOS) used for testing Device Seizure v7.4.

#### 3.2.4.2.1 Android Mobile Devices

The Device Seizure tool successfully connected to 1 of the 2 Android devices, the connection and acquisition failed on the device that was rooted “the Samsung GT-S6812i”. The phone was connected through the OS, but Device Seizure did not connect to it despite seeing it. The Device Seizure tool did not do a good job of extracting information from the Android devices.

#### 3.2.4.2.2 iOS Mobile Devices
Device Seizure did not experience any problems with the iPhone devices. Each device was recognized, and the information gathered and then a report generated. The process was much smoother than the one with Android devices.

### 3.2.4.3 Tool Analysis Summary

The Device Seizure tool was disappointing when it came to anything other than the iPhones. The extreme restrictions and limitations of the Trial version make the tool virtually impossible to evaluate. This is a concern, because without being able to evaluate it, there is no way you could recommend a purchase of it. The Device Seizure product was one of the first mobile forensics tools on the market, and to see the limited functionality of the tool is disheartening. Maybe if the tool is purchased it will be much better, but without being able to test it properly, it would be difficult to justify a purchase of the tool. As with any forensics solution, there is no perfect tool, and a blend of two or more tools is best.

- **Advantages:**
  - Works well with the iOS devices.
  - Comprehensive dashboard.
  - Simple menu and easy to follow format.
  - Simple process of analysis.

- **Disadvantages:**
  - Restrictions on the trial version.
  - Inability to recognize one of the Android phones.
  - Loads a large number of drivers that require a large amount of disk space.

- When comparing the findings of this report with those of NIST ones, the following were observed:
  - The testing was limited by having the trial version.
  - Results for the data acquisition were consistent with the NIST results.
  - Subscriber related data was recovered for the Android device, and like NIST not consistent across all devices.
  - Concur with the problems of the recovery of the iPhone data.
  - Despite the difference in the versions and the time of the testing, the NIST results are similar to those of this testing with Device Seizure being disappointing when it comes to mobile phone forensics.
3.2.5 NowSecure Community Edition v 3.2

The NowSecure Community Edition v3.2 allows the user to complete filesystem, backup, and logical extractions, root Android devices, recover SMS messages, contacts, call logs, and more. For more information about the discussed tool, refer to NowSecure web page [94]. The tool was tested for its ability to acquire active data from the internal memory of the supported mobile devices. Below is a summary of the report findings, where the full detailed report can be found in Appendix A.5.

3.2.5.1 Major Highlights

- **Connectivity**
  - The NowSecure Community Edition tool did an exceptional job with the Android devices, but only had limited success with the iPhone devices. This can be attributed to the fact that the tool is a trial version, its capability of acquiring data from iPhone devices would have been much better if it was a purchased one.

- **Equipment / Subscriber related data:**
  - All Subscriber related data (i.e., MSISDN) was acquired for all of the tested devices apart from the iPhone 6 (full version was required for the jailbroken iPhone 4).

- **Personal Information Management (PIM) data**
  - Contacts/address book entries were acquired for all of the tested devices apart from the iPhone 6 (full version was required for the jailbroken iPhone 4 for the logical data to be extracted).

  ![Figure 3-11: An Image showing that Logical Extraction is possible with Full Version Only](image-url)

- **Internet Related Data:**
  - The phone had been cleared of bookmarks, but the bookmark folders were recovered
for all of the tested devices apart from the iPhone 6.

- **Social Media Related Data:**
  - Social media related data was non-existent in the phone.

- **Case File Data Protection**
  - Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

- **Internal Memory Data Objects:**
  - NowSecure Community Edition v3.2 was measured by analyzing the data from all of the tested devices apart from the iPhone 6. An example of the results of this is shown in the figure below:

   ![Figure 3-12: An Example of an Image Acquired by NowSecure Community Edition v3.2](image)

### 3.2.5.2 Test Results

This section provides the test cases results reported by the tool. Sections 3.2.5.2.1 and 3.2.5.2.2 identify the mobile device operating system type (i.e., Android, iOS) used for testing NowSecure Community Edition v3.2.

#### 3.2.5.2.1 Android Mobile Devices

The NowSecure Community Edition v 3.2 tool successfully connected to both of the Android devices. Once connected, the software performed a logical analysis of the data on the phones which resulted in the successful extraction of the data contained within the phones.
3.2.5.2.2 iOS Mobile Devices

NowSecure Community Edition v3.2 was able to recognize one of the iPhone phones, but the limitations of the Community Edition resulted in the tool not extracting any information from the iPhone devices as it asked for the full version for the recognized jailbroken iPhone 4.

3.2.5.3 Tool Analysis Summary

NowSecure Community Edition v3.2 was downloaded as a virtual machine that is installed within the Santoku software distribution. The virtual machine was installed on Windows 10 version 1511 within VMware Workstation 121.1. The NowSecure Community Edition v3.2 tool did a very good job with the Android devices, but did not perform as expected with the iPhone devices. The information extracted with the tool was very good, and exceeded expectations for the most part.

- **Advantages:**
  - Works well with the Android devices.
  - Instant recognition of the device once connected in the VM.
  - Comprehensive dashboard.
  - Simple menu and easy to follow format.
  - Simple process of analysis.

- **Disadvantages:**
  - Restrictions on the Community version for iPhones.
  - Inability to recognize one of the iOS phones.
  - Inability to generate a report from the data without paying for a full version.
  - No physical acquisitions of any device unless the tool’s version is a commercial one.

- As for comparison purposes, could not discover any reports for the NowSecure Community Edition v3.2 tool within the NIST list of reports for the purpose of comparing with this report.

3.3 Summary

The tools that were tested in the initial analysis provided different mechanisms for analysing mobile forensic information and did not have a common thread by which information can be analysed, reported and displayed. In the researcher’s opinion, just the fact that it took so much time, required much research and trial and error, and there were many obstacles when trying the different mobile forensics applications (installing, setting up and configuring, connecting devices, testing and analysing these tools, looking at the reported data, consistency, etc.), builds a strong case for
creating a new framework, as there were so many problems working with most of the software. It is now believed more than any other time that with the issues faced so far that the proposed framework is desperately needed for the mobile forensics community. Below is a comprehensive table highlighting the initial analysis results of the three tested tools.

<table>
<thead>
<tr>
<th>Pros</th>
<th>CAINE</th>
<th>DEFT 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Easy to Install</td>
<td>- Open Source/Free</td>
<td>- Open Source/Free</td>
</tr>
<tr>
<td>- Reports can easily be exported into many of the common formats</td>
<td>- software can be improved by many developers</td>
<td>- software can be improved by many developers</td>
</tr>
<tr>
<td>- Simple and easy to follow forms are used throughout this software</td>
<td>- offers a Windows based beta version</td>
<td>- has more mobile forensic tools than CAINE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cons</th>
<th>IP Backup Analyser 2 provides very limited reporting options</th>
<th>- very difficult to install and no information was provided on how to navigate the environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Commercial</td>
<td>- installation was extremely difficult and required much trial and error</td>
<td>- No original iPhone analysis utility and analysis of iPhones can only be used with their backups</td>
</tr>
<tr>
<td>- drivers were required to be installed in order for Oxygen to read the devices correctly</td>
<td>- Mobile Forensics offerings are limited (iPhone and Blackberry)</td>
<td>- IP Backup Analyser 2 provides very limited reporting options</td>
</tr>
<tr>
<td>- size of the reports was very large</td>
<td>- No original iPhone analysis utility and analysis of iPhones can only be used with their backups</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-5: Summary of Tools Analysis Findings

In the case of the advanced analysis, the testing started out trying to show a sampling of different forensics tools and the data extraction capabilities when used with the two most popular platforms on the market, the Android and iOS. Additionally, comparisons were made to the reports that have been published from NIST. For the most part, the comparisons showed similar results from the tools; however, the results were not completely the same across the tools. A part of this could be attributed to the different dates of the testing, but moreover, it is believed this is a result of the changing characteristics of the mobile devices, and the smaller data set used for testing. Further research would need to be conducted; this research needs to use a similar data set to that of the NIST work. A concern is that the results from 10 years ago show the exact same types of difficulties, and with all of the advances in technology, we have not been able to make the same strides with respect to extraction of data from these devices; as a result, the research and development of a standard framework is needed more than ever. This becomes even more of a societal concern when you look at the fact that the industry is attempting to “connect” anything and everything from cars.
to medical devices as we continue to approach the “connected” world.

Based on the research, it is clear that society is approaching this connected world, but the tools are lagging behind. Another time that this can be compared to is when the society wanted wireless connections on everything, yet the industry knew the existing protections of Wired Equivalent Privacy (WEP) had some serious implementation flaws, and the IEEE committee was quite a way from developing the 802.11i standard, so the key industry players formed the Wi-Fi Protected Alliance (WPA) and came out with their own protection mechanisms that could be used in the interim. Some of these of course were not much if any better than the existing WEP, but it was an alternative and provided a better sense of security for the society who adopted wireless. For this to happen in the mobile device space, we need the main two vendors, Apple and then the Samsung group to work together like the WPA members did and produce something that can be used in the interim as this problem tries to be solved. At the time of this paper, there are no signs of this taking place. As a point of reference, the industry cannot even get Apple to adopt the universal USB connector for its chargers like the other device vendors have. Below is a comprehensive Table (3-6) to highlight the analysis results of all five tested tools:

<table>
<thead>
<tr>
<th></th>
<th>MobilEdit</th>
<th>MPE Plus</th>
<th>Autopsy</th>
<th>Device Seizure</th>
<th>NowSecure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>Did not recognize Samsung phones unless placed in Developer mode. Jailbroken iPhone4 was not recognized until an official cable was used. Only logical data was acquired.</td>
<td>Acquisition was completed on only Samsung devices, Tool could not provide physical capability.</td>
<td>Tool requires a phone image to be added to it to acquire the data from it. Only the rooted Android data was added successfully.</td>
<td>Tool loads its own drivers during the installation. The tool could not provide the extraction of the information that was required for the testing.</td>
<td>For the tool being a trial version, it did an exceptional job with the Android devices, but only had limited success with the iPhone devices.</td>
</tr>
<tr>
<td>Personal Information Management (PIM)</td>
<td>The file system was not recovered on the jailbroken iPhone 4 and the rooted Samsung GT-S6812i.</td>
<td>Acquisition was completed on both phones, but did not recover the file system on the rooted phone.</td>
<td>The file system was recovered on the rooted phone only.</td>
<td>Contacts/address book entries were not acquired for the rooted Samsung.</td>
<td>Contacts/address book entries were not acquired for the iPhone 6.</td>
</tr>
<tr>
<td>Comparison of NIST Report Findings</td>
<td>Experienced similar results with respect to connectivity.</td>
<td>NIST experience of not recovering subscriber data, missing call logs</td>
<td>No reports for the Autopsy tool within the NIST list of reports for</td>
<td>Data acquisition results were consistent with the NIST results.</td>
<td>No reports for the Autopsy tool within the NIST list of reports for</td>
</tr>
<tr>
<td>Advantages</td>
<td>Disadvantages</td>
<td>Overall</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------</td>
<td>--------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ease of acquisition once device is discovered.</td>
<td>Difficult to recognize devices. Has to maintain constant connection to the Internet. Logical acquisitions only. Did not discover as much as other tools.</td>
<td>Adequate for e-discovery and other types of cases where perpetrator has no knowledge about hiding information. Tool provided data for all 4 phones.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ease of acquisition of the Android devices. Simple menu and easy to follow format</td>
<td>Too difficult to recognize iOS phone devices. Program stability seemed to be an issue, numerous crashes of the tool, seemed to work best on Windows 10.</td>
<td>Adequate for examination of Androids. Best in data extraction with the file carving capability from the physical file system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Source, Comprehensive dashboard, Simple analysis process. Simple installation. Simple menu and easy to follow format</td>
<td>Requires the image of the file system. No capability to acquire a file system. Did not provide thumbnails of the carved files.</td>
<td>Tool is adequate for examination of the Android based phones that have been rooted and a physical image extracted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Works well with the iOS devices. Comprehensive dashboard. Simple process of analysis. Simple menu and easy to follow format.</td>
<td>Restrictions on the trial version. One of the Android phones recognized. A large number of drivers are loaded which requires a large amount of disk space.</td>
<td>The extreme restrictions and limitations of the trial version make the tool virtually impossible to evaluate.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Works well with the Androids, recognition of device is instant once connected in the VM. Comprehensive dashboard. Simple process of analysis.</td>
<td>Restrictions on the Community version for iPhones. Physical acquisitions and ability to generate reports from the data is only for full versions</td>
<td>Tool did a very good job with the Android devices, but did not perform as expected with the iPhone devices</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3-6: Summary of Tools Analysis Findings
4 Forensics Frameworks Analysis

Having analysed Mobile Forensics Tools in the previous chapter, it has become a necessity for this research to analyse previously designed/proposed mobile forensics frameworks prior to establishing the proposed Process-Based Framework, so that appropriate guidelines are set, since they are essential for investigators when examining acquired data from confiscated mobile devices to ensure that every single source of information is beneficial and no essential piece of information is missed or ignored. Four criteria were provided by the United States Supreme Court to all other courts on how to accept evidence when designing a framework [95]:

- The theory or technique utilized must have been tested, and that test must be replicable.
- The theory or technique must have been subject to peer review and publication.
- The error rate associated with the technique must be known.
- The theory or technique must enjoy general acceptance within the scientific community.

Below, is the analysis of some of the proposed frameworks by various researchers, which, as a result highlighted the need for a Process-Based Framework that is able to help ease up and reduce the difficulties faced by investigators while using Mobile Forensics Tools. The analysed framework research is as follows:

- Towards a Unified Forensic Investigation Framework of Smartphones.
- Ontology-Based Forensic Analysis of Mobile Devices.
- The MobiLeak Project: Forensics Methodology for Mobile Application Privacy Assessment.
- Testing the Harmonised Digital Forensic Investigation Process Model-Using an Android Mobile Phone.
- Developing Process for Mobile Device Forensics.
- Data Mining based Crime-Dependent Triage in Digital Forensics Analysis.
Chapter 4: Forensics Frameworks Analysis

4.1 A Framework for Designing Benchmarks for Mobile Devices

4.1.1 Overview

In this study called “A Framework for Designing Benchmarks of Investigating Digital Forensics Tools for Mobile Devices” by Yates and Chi [32], the authors used a tool (SIMfill) created by the National Institute of Standards and Technology (NIST), to do the following:

- Automatically generate the test data for their case study.
- Place the test data on a tested mobile device via USB cable connection.
- Perform an acquisition from each mobile device by a different forensic tool and document the data acquired.
- Repeat the process to ensure consistency and accuracy of acquired data.
- Compare results of acquired data in terms of type, time taken and whether it is admissible as evidence or not.

In doing so, the study discusses the fact that there are no standards for mobile forensic investigations. The proliferation of mobile device operating systems makes it difficult to develop standards for testing and standardizing forensic tool techniques. It is suggested that data types should be used to determine the standards and benchmarks to be used. The study describes the technologies being used for mobile devices and some of the operating systems that are widely available. A brief summary is provided discussing data acquisition suggestions, both logical and physical, based on each operating system.

The logical acquisition consists of forensic tools being used to extract data without removing any physical parts from the device. Logical acquisition varies based on each device and its underlying operating system. It is argued that physical acquisition should be considered but as a final resort because it may prevent the device from being used in legal proceedings.

4.1.2 Analysis

This study provides a basic overview of the challenges faced in the mobile forensics world and briefly highlighted some of the more popular operating systems such as: Android, iPhone, Blackberry, Windows Mobile, and Symbian operating systems. The study also discusses digital forensics tools such as: FTK Mobile Phone Examiner, Oxygen Forensic Suite, EnCase Neutrino, Paraben's Device Seizure among other tools, but none of the discussed tools has been used to establish a standard. It does not provide specific recommendations on how to overcome these challenges. The study suggests that it is easier to establish mobile forensics standards for computers
because of the limited number of operating systems while mobile device operating systems are varied in their design and the way they operate.

4.1.3 Recommendation

While there are more operating systems being used by mobile devices, iPhone and Android are dominating the market place. It is estimated that in 2015 a range of 90% - 98.6% of mobile devices shipment in the world consisted only of the two major operating systems, Google Android and Apple iOS operating systems [43]. In our view, it is imperative that a framework for investigating mobile devices be developed for forensic analysis based on the aforementioned operating systems. A comprehensive study of the structure of the operating systems and how they differ should guide the development of the framework.

4.2 Towards a Unified Forensic Framework

4.2.1 Overview

This study by Mohtasebi and Dehghantanha[34] “Towards a Unified Forensic Investigation Framework of Smartphones” discusses the fact that the current variety of smartphones makes it difficult to use a common framework for investigation. Because manufacturers do not standardize on software and hardware components, the ability for investigators to gain access to the data in these phones varies and is not easily achieved. There are also barriers based on each manufacturer's design process and the use of encryption within the device. The paper discusses local and remote data acquisitions and the pros and cons of each method, and advises the use of both local and remote acquisition methods to mitigate the issues preventing the preservation of 100% of the integrity of the data held in the internal memory of the smart phones. It also focuses on two models, the Windows Mobile model (Figure 4-1) and the Symbian model (Figure 4-2). The challenges faced of not being able to acquire data from smart-phones easily was also stressed by Ahmed et al. [96] in their research paper “Forensic Preservation of Digital Evidence on Mobile Devices from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices (EGFFMD)”.

73
The study provides information about Data Acquisition methods, local and remote. Local acquisition provides faster and more efficient access to the data but it may also alter the state of the device being investigated. In remote data acquisition, the data is gathered by employing network or other remote means. It also discusses Data examination, where it is asserted that the variation in manufacturing decisions on how to store the data negatively correlates to the investigator’s ability to examine the data without making alterations. Alterations of data make it very difficult to be acceptable in a law court and therefore, additional steps must be taken to ensure minimal alteration of the data contained in the mobile devices. The study recommends that guidelines be developed for each model or a set of series of smartphones. A similar study by Barmpatsalou et al. provided “A critical review of 7 years of Mobile Device Forensics” to show how the field of forensics has advanced [35].

### 4.2.2 Analysis

The study discusses, in length, the Windows Mobile model and the Symbian model for forensic investigation of smartphones. Data acquisition examines the data acquired and determines which
Chapter 4: Forensics Frameworks Analysis

investigation processes are most important in the mobile forensics investigation. Focus is given to the Windows Mobile Model of investigation where adhering to the investigation process and obtaining search warrants is paramount to the integrity of the data being collected. The twelve phases of the Windows Mobile model are discussed further and compared to the Symbian model where some phases are combined. The preference of the authors in this study is to utilize the Windows investigation module, with minor changes, considered more appropriate for the investigation of smartphones.

4.2.3 Recommendation

The study focuses on two models for investigation of smartphones, the Windows Mobile Model and the Symbian Investigation model. It also proposes developing guidelines for each smartphone or series of smartphones. No emphasis has been taken into reviewing and developing a framework for more common devices like the Android and iPhone smart devices. The study’s proposal states that examination of each model of smart phones should be customized based on the prepared guidelines for that specific model. It does not, however, specify what these guidelines are.

The recommendation of developing a guideline for each device will be time consuming and will not contribute to developing a common framework for use by all devices. It is our belief that a common framework for mobile forensics must be developed and should encompass the technologies that are being used on a daily basis. Furthermore, the phases discussed in this study can be reduced and streamlined in order for them to be applied to all devices.

4.3 Ontology-Based Forensic Analysis

4.3.1 Overview

This research “Ontology-Based Forensic Analysis of Mobile Devices” focuses [36] on the analysis phase of mobile forensics. This paper was cited in other research such as the one by Mohammed and Clarke [97]. The time required to analyse data along with the complexity of the data are the two biggest obstacles for the analysis of mobile devices. Ontology-based analysis is the approach that this paper is recommending to solving the above-mentioned obstacles. Ontology is a philosophical term describing the theory of existence that has been adapted by the technology world to describe the specifics of a concept. This technique is championed by Semantic Web and is described in this research in detail. The proposed approach recommends modelling and annotating specific elements of mobile devices using the Resource Description Framework (RDF). By using metadata of the objects that exist in a mobile device, a knowledge base of information can be created and used to greatly reduce the time it takes to analyse complex data sets (Figure 4-3).
Ontology based modelling is used to categorize specific elements of an environment. Through the use of RDF, mobile device vocabulary can be defined to help create a knowledge base of concepts which then can be interconnected to analyse data in a timely manner. Data will be extracted from mobile devices and assigned to ontological elements that are mapped to concepts defined in a specific domain. Multiple domains can then be created, each with similar annotated data from the mobile device. Domains can then be connected based on the relationships they represent, thus enabling data to be processed and analysed in an expedited fashion. By using an ontology based approach to analyse mobile devices, this research surmises that a knowledge base can be created and used by automated processes to interpret the data without the need for manual intervention.

**4.3.2 Analysis**

Ontology based modelling is used to categorize specific elements of an environment. Through the use of RDF, mobile device vocabulary can be defined to help create a knowledge base of concepts which then can be interconnected to analyse data in a timely manner. Data will be extracted from mobile devices and assigned to ontological elements that are mapped to concepts defined in a specific domain. Multiple domains can then be created, each with similar annotated data from the mobile device. Domains can then be connected based on the relationships they represent, thus enabling data to be processed and analysed in an expedited fashion. By using an ontology based approach to analyse mobile devices, this research surmises that a knowledge base can be created and used by automated processes to interpret the data without the need for manual intervention.

**4.3.3 Recommendation**

This research focuses on one element of the mobile forensics framework, specifically the analysis phase. It recommends a somewhat novel approach to solving issues associated with the complexity of data in mobile devices as well as the volume of data in those devices. By creating metadata to reflect what is collected without having to specify the data, and by storing data in domains, a knowledge base will be developed to help with data analysis. In order for this approach to function properly, large sets of data will need to be collected and categorized in the knowledge base for it to
be beneficial. It is our belief that more research is needed to determine whether this approach is best used for the analysis phase of mobile forensics.

### 4.4 Forensics Methodology for Privacy Assessment

#### 4.4.1 Overview

This paper “The MobiLeak Project: Forensics Methodology for Mobile Application Privacy Assessment”[44] discusses the privacy aspects of Mobile Forensics, specifically mobile device data at rest, and focusing on Android devices. Millions of mobile devices are lost or stolen each year. The data stored in these mobile devices can be used to cause harm to the owners of the devices, as well as potentially render mobile forensic analysis of such devices unusable. Data in mobile devices exists in three states: Data at Rest, Data in Use and Data in Transit. Data at Rest is where data is stored in a mobile device and is not in the process of being used or electronically transmitted. The Android operating systems permit applications to store data in different storage devices, internal or external, and different directory structure. Developers of mobile apps decide on the structure that fits their applications.

Therefore, personal, financial and other sensitive data can be stored as clear text and without any encryption, which makes it easy for hackers and wrongdoers to tamper with data. The paper investigated common mobile applications and displayed how data, including sensitive data is being stored in each of these applications (Table 4-1). Furthermore, open source tools exist where such data can be easily extracted. The degree of ease by which this data can be extracted and tampered with could pose serious risk to the integrity of the mobile forensics analysis process. The paper concludes that guidelines to storing data are available and should be applied in mobile environments and more work needs to be done to determine data storage during transmission and use.

<table>
<thead>
<tr>
<th>APP</th>
<th>VERSION</th>
<th>CATEGORY</th>
<th>USERNAME</th>
<th>PASSWORD</th>
<th>PERSONAL INFO</th>
<th>ACTIVITY INFO</th>
<th>DOCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropbox</td>
<td>2.1.6</td>
<td>Productivity</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>eBay</td>
<td>1.8.15</td>
<td>Shopping</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Exemore</td>
<td>4.0.4</td>
<td>Productivity</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Groupon</td>
<td>2.0.22.65</td>
<td>Shopping</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Kiwi Local</td>
<td>1.11.3</td>
<td>Social</td>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>2.4.3</td>
<td>Social</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>n/a</td>
</tr>
<tr>
<td>MyMonster</td>
<td>1.6</td>
<td>Business</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PayPal</td>
<td>3.3.0.0</td>
<td>Finance</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>TweetDeck</td>
<td>1.0.14</td>
<td>Social</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
</tr>
<tr>
<td>Twitter</td>
<td>3.2.2</td>
<td>Social</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>n/a</td>
</tr>
<tr>
<td>Skype</td>
<td>2.8.0.920</td>
<td>Communication</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 4-1: Selected Applications and if data at rest is stored in clear text [44]
4.4.2 Analysis

This research reviews some of the most commonly used mobile applications in Android devices to determine the probability of data leaks and the need for better methods of storing data at rest. The researched categories included usernames, passwords, personal information, activity, and document storage. Some of the applications reviewed for this paper include Dropbox, LinkedIn, PayPal, Twitter, eBay, and Skype. Applications developed for the Android operating system are not required to store data in a specific location or format. Standard directories exist but developers decide if they want to utilize these directories. Five methods exist for storing data in an Android device, specifically:

- Internal storage.
- External storage.
- Remotely using Network storage or the cloud.
- Database format (SQLite).
- XML format.

It was clear from the results of the research, shown in the above table, that there is no uniform method of protecting the privacy of the data. In many of the applications that were tested, usernames, passwords, conversation threads and links, location information, and financial information were stored in clear text and were accessible by simple open source tools. A more standard method of storing data should be utilized as well as using encryption for data of sensitive nature.

4.4.3 Recommendation

Although this paper discusses the privacy of data in mobile devices and not the mobile forensics tools or framework to be used for data analysis, it is important to have a good understanding of how data is stored in mobile devices. The research focuses on determining data at rest storage in Android devices. It is important to expand this research to understand how data is stored in other popular operating systems, like the Apple iOS. Of most importance is to understand how data can be tampered with and what needs to be done to minimize or eliminate that possibility.
4.5 Testing the HDFI Process Model

4.5.1 Overview

This paper “Testing the Harmonised Digital Forensic Investigation Process Model-Using an Android Mobile Phone” [37] reviews the steps used for the Harmonised Digital Forensic Investigation (HDFI) process model and then applies a scenario, using an Android phone, to test the validity of the model. The HDFI model consists of 14 phases, each phase having sub procedures and each phase needing to be completed prior to the next phase. The phases of the HDFI process model are:

- Incident Detection Process.
- First Response Process.
- Planning Process.
- Preparation Process.
- Incident Scene Documentation Process.
- Digital Evidence Collection Process.
- Digital Evidence Transportation Process.
- Digital Evidence Storage Process.
- Digital Evidence Analysis Process.
- Digital Evidence Interpretation Process.
- Presentation Process.
- Investigation Conclusion Process.

This paper indicates that in 2013, 75% of the smartphones in the market were Android based phones and, therefore, the writers decided to apply this process model on an Android based phone. Commercial mobile forensics software was utilized for some of the steps described above.

4.5.2 Analysis

This research discusses the HDFI model in detail, looking at each step and then applies a simulated test, using an Android phone to determine if the HDFI process model works well with mobile devices. The scenario being used is that an SMS message is injected with scareware and sent to a
client requesting bank account information. The customer reported the incident and the process was
initiated. The investigation is conducted by different users based on each step. A toolkit was used
to examine the Android Mobile device. The writers conclude that the 14-step model (Figure 4-4)
will adequately accommodate Android mobile device forensics but there is a potential for the
investigation to be derailed because of the many personnel that get involved in the process.

Figure 4-4: HDFI Model [37]
4.5.3 Recommendation

This paper looked at a specific scenario to determine the validity of the HDFI process model for mobile forensics. The testing was limited to a single mobile device using the Android operation system. It also seems that the test scenario was fitted to work with the model. There was no testing of Apple iOS devices. The HDFI model may be suited for general digital forensics, but it seems to be too complex for mobile forensics. In our opinion, some of the steps prescribed in this model will not adequately work in a mobile environment. Furthermore, many of the steps require manual processing and involve different personnel, which may create a breakdown for completing the investigation in a timely fashion. The handoff of processes among the investigation team introduces additional burdens. A better method should be used to address this issue. There was also no in-depth analysis of the processes and sub processes of this model. We recommend using the HDFI model as a comparison to other models and create a framework that is better suited to mobile devices regardless of operating systems.

4.6 Developing Process for Mobile Device Forensics

4.6.1 Overview

The author of this paper “Developing Process for Mobile Device Forensics” [98] focuses on the need to have consistent and repeatable methods for the examination process in Mobile forensics. The variety of mobile devices, operating systems, storage types, and mobile accessories makes it difficult to standardize the process of examination but it is imperative to develop a process that can be used in legal settings. The integrity of the data as well as the preservation of the data are paramount to ensuring accurate forensic analysis. The guidelines discussed in this paper specific to the examination process are:

- The Intake Phase
- Identification Phase
- Preparation Phase
- Isolation Phase
- Processing Phase
- Verification Phase
- Documentation/Reporting
- Presentation
Archiving

Each phase is designed to help ensure that the examination process is done methodically and can stand on its own in a court of law or any other setting. This paper recommends following a guideline for examining evidence, documenting the examination phase and ensuring the preservation of the data being examined. Further emphasis is placed on the ability to make the evidence repeatable and defensible, if a need arises.

4.6.2 Analysis

This paper provides an insight into the phases required to achieve a court admissible mobile forensic examination process (Figure 4-5).

- The first phase, Evidence Intake, details the type of data that is requested and is intended to identify the goals of the investigation process.
- The Identification phase is intended to determine what entity, or entities, are requesting the data and what should be examined. The author argues that the specifics of the examination request will determine the type of tools that are best suited for that examination.
- The Preparation phase is meant to set the roadmap of how the examination process should be accomplished. In this phase, specific tools should be identified, noting that there may be a need to use multiple tools to accomplish the stated goal. There are also different types of

Figure 4-5: Evidence Extraction Phases [98]
Chapter 4: Forensics Frameworks Analysis

extraction and acquisition that must be decided on during this phase. Cell Phone Tool Levelling System (Brothers, 2009) can be used to assess the depth of the investigation.

- The Isolation phase is meant to ensure that no new evidence is introduced once the investigation has begun. This can be accomplished by using existing techniques, like Faraday bags, signal jamming, radio frequency shielding or other methods, or turning the mobile device off or using “Airplane mode” or equivalent mode.

- The Processing Phase is when the tools are used to extract the required data.

- The accuracy and integrity of the data being extracted must occur at the verification phase, a process that can be accomplished manually or by using additional tools.

- The formal Documenting and reporting phase is the next phase but it should be integrated into all of the previous phases.

- The Presentation phase must be planned to clearly identify what is needed to adhere to the original requirements of the examination. Presenting to a court requires different preparation than presenting to other entities.

- The final phase, Archiving, is meant to ensure that the examined data is preserved and is usable to help with any future requirements and record keeping.

4.6.3 Recommendation

Although this paper focuses on the examination process of mobile forensics, and how law enforcement views the best way for data examination, it is important to note that the phases discussed here, with some modifications, may be utilized in the proposed framework. However, many of the steps discussed in this paper are manual and further research is needed to determine a better and more automated method of accomplishing the same tasks.

4.7 Data Mining based Analysis

4.7.1 Overview

This paper “Data Mining based Crime-Dependent Triage in Digital Forensics Analysis” by Bertè et al[62], discusses applying the data mining procedure to digital forensic processes in order to reduce the amount of time it takes to review digital evidence, increase efficiency of the investigation and to determine the validity of the evidence being examined. The approach recommends assigning a ranking system to the digital evidence based on the post mortem data mining theory, by giving priority to each inspected computer based upon the likelihood that a computer has been used to commit one of the following crimes: child pornography, copyright violation, hacking, murder and terrorism. It is hoped that this method can augment digital investigations aiming to immediately
identify the most suspect computers. Traditionally, triaging is the process of extracting data from the confiscated device on site followed by the analysis of the extracted data. This is especially useful for locked devices when found in an unlocked state so that the available data can be accessed and used. Post mortem forensics consists of four phases, namely: 1) forensic acquisition which means retrieving data storage devices. 2) Feature extraction and normalization, completed matrix, where investigators extract specific features based on the data being acquired and normalize the data. 3) The context and priority definition phase focuses on the type of crime being investigated including timelines related to the crime in question. This phase is also referred to as reduced matrix. 4) Data classification and triaging uses the reduced matrix and applies data mining algorithms to reach the intended goal.

### 4.7.2 Analysis

This paper assesses the current investigation techniques of digital evidence and concludes that they are not sufficient to reach a timely conclusion to the enormous amount of data contained in storage devices and the limited techniques currently being used by law enforcement departments. The authors propose using a new approach to rank evidence based on data mining algorithms developed to meet specific crime types. The proposed approach is composed of four phases, with the premise that in order for investigators to reach a conclusion in a relatively short time, certain types of data need to be extracted and correlated. Then, a matrix is created of that data and a ranking is given to the data to determine the probability that the crime was committed. Data structures are created and summarized, then a knowledge base consisting of machine learning algorithms is used to compare the investigated data against the knowledge base, thus, determining if the crime was likely committed. This technique is also referred to as trainingset, which is a collection of similar events which create a pattern that can be used to electronically cross examine the data against the trainingset.

### 4.7.3 Recommendation

The field of data mining is of great interest to the mobile forensics community. This paper applies some of the techniques of data mining to an extent, to reduce the large amount of data being processed, but this researcher believes that a simple application of data mining may inadvertently make the investigation less accurate. However, the correct application of data mining algorithms may greatly improve the speed by which digital investigations get completed as well as yield a higher probability of determining a more accurate outcome of the investigation. We recommend the use of big data analysis as well as data mining, as a method to further refine the investigation process.
4.8 Efficient Framework for Mobile Devices

4.8.1 Overview

The authors (Ahmed and Thakare) of this article “Efficient Generalized Forensics Framework for Extraction and Documentation of evidence from Mobile Devices” [33] discuss the struggle mobile investigators of Android powered devices face due to the lack of standards of acquisition techniques. Therefore, the authors reached the conclusion that there is a need for a more generalized framework for the extraction of data and the documentation of evidence for Android based devices. As of January 2012, Android has 46.3% of the smartphone device market share. The authors argue that the number will be much higher in the future due to the popularity of Android devices as well as Google’s plan to introduce additional devices, like tablets, televisions, gaming devices, vehicles and other future devices. This proved to be true, as it was estimated that in 2015 a range of 90% - 98.6% of mobile devices shipment in the world consisted only of the two major operating systems, Google Android and Apple iOS operating systems [43]. The struggle for analysing these devices, based on the author’s assumption, is due to the lack of knowledge and tools.

The paper reviews basic concepts of digital evidence, mobile forensics, smartphones, as well as the Android history and system architecture. It further describes the Android architecture (Figure 4-6) which consists of the Application component, Application framework component, Libraries component, Android Runtime Component, and Linux Kernel component. The approach proposed in this paper is to acquire data from Android devices and store the data in external storage, thereby eliminating the need to connect to the device again.

![Android OS Architecture](image-url)

---

Figure 4-6: Android OS Architecture [33]
4.8.2 Analysis

This paper assumes that there is a need to create a general framework for acquiring data from Android devices. The proposed methodology for extracting Android digital evidence is by extracting the data from the device’s internal storage, copying the data to an external and removable memory card while the device is powered on (hot plug) without removing the battery, so that data is not altered during the seizure process, then applying necessary shields, e.g. Faraday cage, before applying the Efficient Generalized Forensics Framework Acquisition App. The App will be used to ensure extraction of data and avoid any locking problems, before it is installed in the Forensic Workstation with an SD Card Reader.

4.8.3 Recommendation

The authors’ premise is to define an efficient generalized framework for extraction and documentation of evidence, but unfortunately, the proposed approach is specific to Android devices and the proposed methods do not address some of the more common scenarios related to mobile devices. The paper did not address the documentation of evidence process. The proposed framework will need to be further reviewed to determine if it will be effective and usable for a more general approach to mobile data extraction.

4.9 Limitations of Discussed Frameworks

In addition to the limitations discussed below, table 6-2 summarises main features of proposed frameworks by other researchers:

4.9.1 Most of the research done is specific to Android based devices

The reviews conducted by the researcher shows that the majority of the reviews are specific to Android based smartphones, partly because Android’s market share is higher than any other platform and partly because the Android platform is Linux based, which is an open source platform. That, however, should not be enough of a factor to limit the research to these devices in general. More Mobile Forensics based research needs to be applied to Apple smartphones since they place second in the mobile device platform market share. Although Apple’s iOS is proprietary, not open source, additional research is needed to ensure a framework for forensic mobile devices will apply to the leading platforms in the industry.

4.9.2 The methods used are focused on solving a specific issue

Most research done thus far seems to be specific to solving a problem and is not generalized enough
to accommodate potential outliers and to address issues that may not be present in the well-defined and controlled environment the research is being conducted under. To provide a more generalized framework, further study must be conducted to take into account current and future trends of mobile devices.

4.9.3 Lack of data mining techniques

Although data mining is an important field in digital forensics, there is very little mention of utilizing data mining techniques to reduce the manual steps that are needed for a comprehensive investigation. The data mining techniques should also be updated to reflect the increasing dependency of this field in other industries and determine the best way to effectively utilize data mining in mobile forensics investigations.

4.9.4 No mention of utilizing big data

In the past few years, “big data” has become an essential tool used by many industries for discovery and analysis. Big data is both structured and unstructured data. The mobile forensics community can benefit a great deal from using big data as part of the analysis process. Using big data will significantly lower the time it currently takes to move through the investigation process. It will also provide more accuracy and result in creating better analysis tools.

4.9.5 Need for an open ended, extensible framework

The discussion of the papers and research done so far indicates that there is a greater need for developing a generalized and extensible framework to address current and future developments in the mobile industry. The “Internet of Things” or IoT promises to disrupt the current computing structure as we know it. Developing a more extensible framework will help provide guidelines for future investigation where smartphones are only one aspect of the mobile forensics industry.

4.9.6 Too many steps are used

Based on the current work that has been reviewed, it seems that there are many steps, procedures and sub procedures that are required or recommended by each framework. Many of these steps can be generalized and should not be specific to a platform or a device. The complexity of these procedures and sub procedures makes it difficult for mobile analysis to be completed in a consistent manner. The focus should be on the documentation, analysis and presentation rather than customizing the steps to the platforms being investigated.
4.9.7 Too difficult to create a single program

The variety of the tools used for investigation clearly indicate the difficulty of creating a single application capable of extracting and analysing data for all platforms. It is also a statement of the difficulty of keeping these applications up to date because the pace of new technologies far outperforms the updates to the tools and applications being used to analyse mobile devices.

4.9.8 Need for a truly generalized framework specific to mobile forensics

Although there are frameworks that have been recommended in the research we reviewed, some were based on current digital and non-mobile devices. Although it is natural to develop frameworks based on prior experience with similar technology, the research done thus far suggests that the framework should be specific to general current mobile devices with an eye towards future mobile devices and integrating the IoT technologies into the framework.

4.9.9 Many obstacles by industry in creating standards for mobile forensics

It is evident from the research done thus far that there is little work being done by the mobile industry to help mobile forensic investigators. This is a symptom of the digital industry in general and has proven to be problematic in the past. Current and future development of mobile devices will greatly benefit by integrating forensic processes when developing new products.

4.10 Summary

Based on the limitations discussed in section 6.9, it is important that a broader framework be created to remedy the issues that were revealed in this chapter, such as minimizing or eliminating the possibility of tampering with the data. It is also as important that the framework be open ended and extensible to encompass newer mobile technologies that are beginning to roll out in the market today and in the future. The framework should also address current deficiencies in the testing tools common in today’s market. Many of the tools the researcher attempted to test, or was able to test, were cumbersome and there was little commonality among those tools. A new mobile forensic framework needs to be developed to help address this area as well. The framework should be specific to current mobile devices and generalized so that it will apply to the leading operating systems platforms in the industry, with an eye towards future mobile devices and integrating the Internet of Things (IoT) technologies into the framework. Finally, the framework should also minimise the many steps and sub procedures that were discussed in this chapter, so that mobile analysis can be completed in a consistent manner. Table 4-2 below gives a findings’ summary of analysed frameworks in terms of: issues solved, concentration of phase, number of steps/stages
used, research recommendations and whether the framework was specific to mobile forensics tools, or for computer forensics in general.

<table>
<thead>
<tr>
<th>Analysed Framework</th>
<th>Issues Solved</th>
<th>Phase Concentration</th>
<th>Steps Used</th>
<th>Research recommendations</th>
<th>Specific to Mobile Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>A F/W for Designing Devices’ Benchmarks</td>
<td>No specific recommendations to solve the issue</td>
<td>Mainly acquisition phase</td>
<td>A tool (SIMfill) created by NIST was used</td>
<td>None of the tools discussed were used to establish a standard</td>
<td>Yes/ Most popular operating systems</td>
</tr>
<tr>
<td>Towards a Unified Forensic F/W</td>
<td>No emphasis for developing a F/W for more common Oss</td>
<td>Data acquisitions phase</td>
<td>Compared Windows Mobile 12 phases to 4phase Symbian model</td>
<td>Recommends developing guidelines for each model, but does not specify them</td>
<td>Yes/ Windows Mobile and Symbian model</td>
</tr>
<tr>
<td>Ontology-Based Forensic Analysis</td>
<td>An approach to solve issues associated with data complexity is recommended</td>
<td>Analysis phase</td>
<td>Collect and categorize large sets of data is needed for this approach to be beneficial</td>
<td>It recommends modelling and annotating specific elements of mobile devices using (RDF) to reduce time taken for analysis</td>
<td>Yes/ Generally all Operating Systems</td>
</tr>
<tr>
<td>Forensics Methodology for Privacy Assessment</td>
<td>It focuses on determining data at rest from Android devices</td>
<td>Privacy aspects of Mobile Forensics</td>
<td>Identification of target application, Population &amp; Acquisition of data, and Analysis</td>
<td>Reviews used applications to determine data leaks and the need for better methods of storing data at rest</td>
<td>Discusses privacy of data in devices, not the tools or frameworks</td>
</tr>
<tr>
<td>Testing the HDFI Process Model</td>
<td>Many personnel involved in the process which may derail it</td>
<td>All phases</td>
<td>Each phase has sub procedures &amp; needs to be completed prior to the next one</td>
<td>Testing limited to a single Android device</td>
<td>Suits general digital forensics, but too complex for mobile one</td>
</tr>
<tr>
<td>Developing Process for Mobile Forensics</td>
<td>Further research is needed to determine a more automated method</td>
<td>Examination process phase</td>
<td>9 phases to ensure examination process is done properly and admissible</td>
<td>Recommends following a guideline for discussed phases.</td>
<td>Yes/ Generally all Operating Systems</td>
</tr>
<tr>
<td>Data Mining based Analysis</td>
<td>may improve the speed of completing digital investigations</td>
<td>Phases are acquisition, extraction, context and classification</td>
<td>Propose using a new approach to rank evidence based on data mining algorithms</td>
<td>Recommends assigning a ranking system based on the post mortem data mining theory</td>
<td>No/ Computer forensics</td>
</tr>
<tr>
<td>Efficient Framework for Mobile Devices</td>
<td>Avoid locking problems while extracting data before installed in the Forensic Workstation</td>
<td>Extraction phase</td>
<td>Hashing is performed before and after acquisition to insure the integrity of the data</td>
<td>Proposes to acquire data and store it in external storage, to eliminate the need to connect to the device again</td>
<td>Yes/ Android devices</td>
</tr>
</tbody>
</table>

Table 4-2: Summary of Frameworks Analysis and Findings
5 Proposed Framework Architecture and Design

The previous chapters focused on researching existing frameworks used by, or created for, the mobile forensic community. Although attempts have been made to develop conceptual frameworks for mobile devices in the past few years, most of the research completed in previous chapters demonstrated a need for developing a more robust and extensible framework to focus on existing and emerging mobile technologies. Current frameworks tend to focus on targeting specific operating systems, i.e. Android, iOS, or responding to specific issues. Some are also based on desktop and non-mobile device models that are not suited to an increasingly interconnected world.

Throughout this research, an attempt to work with a variety of the tools that are available on the market has been made, and this has proved challenging. The results of the Tools Analysis were not encouraging, and quite surprisingly a lot of the challenges that existed at the advent of the mobile devices have not been solved. The reality is, not one of the tools used in testing functioned in a completely acceptable manner. Moreover, the vendors need to deliver better solutions to this ever-expanding market. This fact further validates the need for a new framework in the area of mobile forensics.

As the number of mobile devices is projected to more than triple in the next few years, common methods of acquiring, analysing, and reporting data will greatly help streamline a mobile world that is ever advancing. It is also of critical importance for the framework to gain forensic community acceptance for it to have a higher probability of being used in the mobile forensic community. For that to occur, it is believed that the design of the framework should be more generalized to accommodate a highly competitive industry.

A new generalized and mobile specific Process Based Framework is presented in this chapter. The new output framework is an attempt to standardize information and to enable users to gain a better understanding of what the mobile forensic tools are trying to provide. The framework focuses on design areas consisting of open architecture, platform independence (ability to accommodate mobile forensic software across different platforms), extensibility to accommodate IoT devices, simplified design, evidence integrity, and streamlined reporting. Discussion regarding a future implementation of a web based tool that utilizes the proposed Framework will be outlined in Appendix B. In addition, procedures highlighting each step of the Framework are also provided in
Appendix D. Diagrams and figures are provided throughout this chapter to illustrate the framework design goals and specifications.

5.1 Benchmarks used for Framework Design

For a case to be built up for a framework that can provide appropriate guidelines on how to use forensics tools, a testing table template was created following NIST procedures to govern tool specifications, so that the obtained results with those of NIST ones can be compared so that a differentiation of their findings is established. Also, analysis conducted on chapter 4 about previous frameworks revealed that current frameworks tend to: focus on targeting specific operating systems, i.e. Android, iOS; respond to solving specific issues; be based on desktop and non-mobile device models that are not suited to an increasingly interconnected world; or have too many steps.

Some of the analysed frameworks in chapter 4 were used as a benchmark for the Process Based Framework for Mobile Forensics (PBFMF) such as: 1) “Towards a Unified Forensic Investigation Framework of Smartphones”, which recommends that guidelines be developed for each model or a set of series of smartphones, where it proposes that examination of each model of smart phones should be customized based on the prepared guidelines for that specific model. This will be time consuming and will not contribute to developing a common framework for use by all devices. 2) “Efficient Generalized Forensics Framework for Extraction and Documentation of evidence from Mobile Devices”, where authors’ premise was to define an efficient generalized framework for extraction and documentation of evidence, but unfortunately, the proposed approach was specific to Android devices and the proposed methods did not address some of the more common scenarios related to mobile devices, such as the documentation of evidence process.

As a result, a new generalized and mobile specific Process Based Framework is built and designed. The framework focuses on design areas consisting of open architecture, platform independence, simplified design process, extensibility to accommodate the current and future market of these devices, evidence integrity, and streamlined reporting.

5.2 Design Goals

Based on the analysis and findings of chapters 3 and 4, the following section is a detailed discussion of the design goals, Figure 5-1:
Chapter 5: Proposed Framework Architecture and Design

There is a need to discuss the importance of the framework not being linked to a specific technology, smartphone or/and operating system, as many of the existing frameworks are tied to either Android, Windows or iOS devices. It would be more appropriate to have the framework available across different platforms and create an architecture that is open and responsive to current and future technology trends. It is also important to ensure the new platform will be open and adoptable for IoT devices, Figure 5-2.

5.2.1 Platform Independent (Cross platform) and open architecture

Figure 5-1: PBFMF Design Goals

Figure 5-2: PBFMF is a Cross Platform and an Open Architecture
5.2.2 Simplified design

One of the main issues of not having usable mobile forensics architecture is that some of the proposed solutions may be too difficult to incorporate by manufacturers and can slow down the production cycle. The proposed framework should be part of the design process similar to how security in desktop operating systems have become part of the development process rather than being an afterthought as was the case a few years ago. This simplicity in design can be incorporated by manufacturers without a lot of overhead.

5.2.3 Preserves the integrity of the evidence

Since mobile devices are used worldwide, it will be important for the framework design to ensure data integrity and privacy to avoid introducing any steps that may make it more difficult for courts and law enforcement to have the evidence admissible to courts. A good example of how to develop forensics procedures to suit law and enforcement agencies in Thailand was presented by Klomklin and Lekcharoen [99].

5.2.4 Streamlined Reporting

The framework should propose simplified reporting to make it easy for the community to use these reports. Currently used mobile forensics software reports are difficult to review and compare data across different platforms. It is important for the framework to provide guidelines for simplifying reporting requirements.

5.2.5 Extensible framework to accommodate IoT and other future technologies

Since mobile devices are ever evolving and technology is moving away from desk-based computing to devices, gadgets and appliances and because the number of devices will be growing exponentially in the next 5-10 years, the framework will need to emphasize the IoT and the role it will play in the near future. Current frameworks are based on desk-based architecture and are not suited for the "anywhere and everywhere convergence" of technology.

5.3 Community Wide Acceptance

For the framework to gain community wide acceptance, it is essential that security and privacy are integrated into the design process of mobile devices rather than it being an afterthought. This is a simple and highly needed requirement but it may be difficult to implement because of the competing standards out there and the speed by which mobile technology moves. Describing the benefits the
community will gain by adopting a common framework will be important. Adoption should also, in the long run, make the industry less susceptible to increasing malicious attacks. Furthermore, the framework will need to get support from the main forensics entities. This support should be from both the NIST and the law enforcement community. This support could be achieved through providing exposure for the framework across the different communities by submitting papers and speaking about the framework at conferences that are both sponsored and/or hosted by the different industry agencies.

5.4 Mobile Data Privacy

With the ubiquity of mobile devices and its availability to users around the world, a big concern is the privacy of user data. Users have transformed their communication where general and sensitive information is being stored in mobile devices. Furthermore, cloud technology has made it easier for people to share information. Privacy and security breaches have risen in the past few years and will more likely increase in the future.

One of the reasons for privacy breaches is that the mobile industry is working to make it easier for users to consume data. The more data users store and consume in their mobile devices, the easier it is for malicious users to gain a broader knowledge of all aspects of a user’s information. Usability, from an industry perspective, is much more important than privacy. Because of the inherent complexity associated with enhanced digital privacy and security, most users are not interested in using encryption or secure algorithms to protect their data.

Another reason is that manufacturers are constantly in a rush to introduce new products to the market in order for them to increase their market share. Research and Development time has been reduced to ensure a better market share for the products. Access to mobile data is becoming easier with the use of extraction tools. This can be an advantage for law enforcement personnel but these tools can also be used by malicious users to gain unlawful access to information. Determining what is reasonable and what is unreasonable access can be tricky and may lead the industry to move in one direction or another.

Privacy advocates have legitimate concerns about the ease by which hackers could access private data. There is also a concern about laws being in favour of seizing data and devices without proper investigation procedures. The trend, when it comes to raising privacy concerns, has been shifting towards less privacy because of the greater need for collecting data by application developers. Privacy advocates are aware of this trend and are trying to advocate for more accountability by everyone involved in the development and dissemination of mobile devices and data.
Although the majority of users feel that their mobile networks and App developers should be accountable for mobile privacy breaches, mobile device users have a responsibility to educate themselves about ways they can protect themselves against unlawful use of their data. Although it may be time consuming for the average user to learn the intricacies of better ways to improve the probability of their devices not being hacked, it is important that they spend time educating themselves on this issue and being aware of the many complex issues related to data privacy.

App Developers have also created a market where they, at times, offer their product for free or for a minimal fee to entice users to use their Apps. Apps collect an enormous amount of data such as analysing the frequency use of the app, the geo-location of the user, contact information, as well as many other data functions. Currently, there are no standard guidelines used by App developers for the type of data they can collect from users without their knowledge or consent.

The proposed framework uses specific steps to reduce the possibility of mobile data privacy breaches. Mobile device data privacy protection starts with device isolation, the proper use of triage, into determining the chain of custody as well as how to transport the data. These steps will be discussed later in this chapter as part of the proposed framework. Mobile forensics investigators should have a responsibility to ensure privacy issues are considered when analysing mobile data. A forensics investigator will have untethered access to a mountain of data each time they investigate a device. Sometimes, the investigation may be specific to certain information rather than general data requirements.

### 5.5 The Proposed Process Based Framework for Mobile Forensics Tools (PBFMF)

#### 5.5.1 First Responder Triage (Preservation)

It is essential that the initial steps are provided and followed as much as possible, so that the devices, and moreover, the potential evidence is handled in a forensically sound manner. The lead team that responds needs to have a step by step process to follow when they arrive on site. The following steps are offered to provide that process to the first responders. In the explanation of this process, the legal aspects will not be covered. The correct search and seizure authorization is based on the jurisdiction and the laws that apply there, so for this component in the process it is assumed that the legal authority has been obtained for the processes as defined within. Another component that will not be addressed is the possibility that the first responder will have to conduct interviews with the personnel at the scene as well as any potential subjects. The process will specifically deal with the triage stage of the process.
5.5.1.1 Arrival on Scene

Once the investigator arrives on scene, he/she has to make a quick decision on how he/she is going to proceed with the investigation, and will need to evaluate what type of methods he/she is going to use as he/she progresses to the evidence collection and preparation for transfer. A bulk of mobile device data is volatile, and as such it is dynamically changing on a regular basis, so the time spent in the evaluation of the scene could be critical and delays could result in the potential evidential data being changed, or even destroyed or lost either intentionally or accidentally. This is why it is imperative that these investigators receive adequate first responder training before they conduct an investigation on an actual potential crime or incident scene.

Another consideration that needs to be reviewed is when the potential crime scene contains a hazard to the investigators. There is a chance that the area could contain hazardous chemicals or other items that could harm the investigators; therefore, the evaluation of the crime scene is critical before anyone enters into the area. If there is suspicion or doubt then the investigator should not enter the crime scene area until competent authorities have determined the scene is safe.

One last thing that the arrival on the scene investigator needs to consider is when the mobile devices are in a compromised state, and that is when the device itself has some form of contamination in it, this could be immersion in liquid, blood or a number of other factors. This process will not be elaborated on, but any time a device is found to be in a compromised state, the device should be left in that state and then transported to a lab for further examination and analysis.

5.5.1.2 Documenting the scene

The importance of documenting the scene prior to performing the forensics process cannot be overstated; it is an essential aspect to handling an investigation. Investigators should not only concern themselves with the electronic forms (smart phones in this case) of evidence, but also the other types of potential evidence. This could be in the form of invoices, manuals and any other documentation types of sources. These forms of physical evidence could assist with determining a PIN or other protection mechanism of the device since many people write this information down.

An element to this is the photographing of the potential crime scene, and in some cases actually drawing sketches and diagrams of the scene as well.

With mobile devices, it is important to record the state and condition of the device as well as any other hardware associated with the device. If the device is connecting to a computer or another type of device then the investigator might need to take the device the smart phone is connected to as well. This is all part of the initial requirements when an investigator arrives on the scene.

The investigator needs to avoid touching or contaminating the mobile device when photographing it and the environment where the device is found. If the device’s display is in a viewable state, the
screen’s contents should be photographed and, if necessary, recorded manually, capturing the time, service status, battery level, and other displayed icons. Additionally, the investigator should wear rubber gloves, not only for the protection of the device but also for his own protection. Once the investigator has fully evaluated the crime scene and created complete and detailed documentation then and only then should the investigator continue with the process as defined here.

5.5.1.3 State of the device

The state of the device cannot be overlooked as the procedures vary depending on this. The following guidelines are the recommended processes to follow once on site

5.5.1.3.1 Off

If the device is in the “OFF” state then it is left in the OFF state, and anything that is discovered in the vicinity of the phone is documented. One of the first things needing to be established when the phone is in the OFF state is whether or not it has a charge on it, or the battery charge is exhausted and that is why it is in the OFF state. No matter the reason for the OFF state, it is still essential that power is provided to the device, and the device is taken OFF of the network. With the device in the OFF state it is not as critical to identify and correspondingly connect the charging device; in fact with the device in the OFF state, it is recommended that the device be transported to a forensics facility and the acquisition be conducted there.

5.5.1.3.2 On

When the responders arrive on the scene and discover the phone in the “ON” state, then time is of the essence. The critical process when the phone is in this state is to take the phone OFF of the network. Following this we need to ensure there is a charger connected to the phone for transit. With the device in the “ON” state, the first responders have the option of conducting the initial collection of evidence on site, but again this is not the preferred method or approach to be used.

5.5.1.4 Take off the network (Isolation)

5.5.1.4.1 Faraday bag or structure

Device isolation is important to maintain the integrity of the investigation as well as ensure data privacy. The preferred method to take the device OFF of the network is to use some form of a Faraday bag, as can be seen in Figure 5-3 below, or another form of electromagnetic shielding; these are available from a number of different manufacturers. Whichever one is chosen, it is imperative that the capability to keep the device OFF the network while it is connected to the charger is maintained; this is often an area that causes the signal to “leak”. Any cable that is
connected to the device can cause leakage around the cable or the entrance of the cable through the Faraday container; therefore, it is critical that the placement of the device into a container is done carefully and all of the connections completely sealed around the entry point.

![Figure 5-3: Example of a Faraday Bag](image)

5.5.1.4.2 *Cellular Network Isolation Card (CNIC)*

A CNIC mimics the identity of the original UICC. This technique permits acquisition without concern of wireless interference; however, the technique does involve insertion of a foreign SIM card in most cases, and as such should not be the method of choice unless there are no other methods available to the team.

5.5.1.4.3 *Other methods*

- If there is not a Faraday bag, CNIC or any other type of electromagnetic shielding available, there are a couple of things the responder can do, one of which is to take the device to a basement or another location to get it off the net. Additionally, while it is not the best choice, the phone can be wrapped in aluminium foil to remove the phone from the network. If this approach is used, it takes 7 or more wraps of the foil to potentially take the phone OFF the network. Again, this is not a recommended approach, but in an emergency it can be used if necessary.

- Keeping the mobile device ON, but radio isolated, shortens battery life and increases power consumption. This is because some of the device manufactures will increase the power to maximum to try and pick up the signal. After some period, failure to connect to the network may cause certain mobile devices to reset or clear network data that otherwise would be useful if recovered

5.5.1.4.4 *Write blocker*
Once it has been established that the device is OFF the network, and connected to some form of a charging source, the process and preparation for the acquisition is ready to start. The investigator has to maintain the integrity of the devices at all times to be part of a solid process that protects the data, and information that is handled has to be processed as if the evidence might go to litigation; therefore, it is imperative that the investigator carries out this procedure and protects the data. The process for doing this is to install a write blocker (Figure 5-4), which is a device that once installed will not allow any writes to the device by ensuring that the data is not modified once the tool is connected.

![Figure 5-4: Example of a Write blocker](image)

5.5.1.5 Connect approved tools

Based on the research that was conducted as part of this study, this is one of the most important areas that needs to be completed. The research has indicated that currently there is no tool adequate for meeting the needs of the forensics community; therefore, finding a standard methodology for tool testing is imperative to the success of being able to conduct a standard based forensics methodology. It is hoped that this will be addressed by the vendors once a framework is put into place and adopted. The ideal situation would be for vendors to create tools that can meet the requirements as outlined in the framework. This is something that is an area for follow on research, the vendors need to work with the industry and provide a solid tool that can work for the variety of devices that continue to be released onto the market.

Currently, this is a major problem with the tools that are reported to be the best ones for conducting mobile forensics, and this problem is going to be exacerbated by the continued pursuit of connecting anything and everything to create the “Internet of Things.” It is hoped that this research will be extended such that vendors will explore a solution to the problems that have been identified during
the research. In the interim, there could be a list of tools identified and offered as “approved” tools for different components of the forensics process. While this is not ideal, it does provide an opportunity to set the usage of the framework in motion and to continue the development and enhancement of the framework as time passes.

5.5.1.6 Scenarios

To exercise the framework process and steps, the research will address two different types of scenarios within this first responder triage stage, and this will assist in the development of both a checklist for first responders as well as examples for follow-on research. The intent of this section is to maintain the premise that securing and evaluating the scene is the first step of the triage process, and it is a critical one. Any improper handling of the device and/or peripheral hardware at the site could result in damage or loss of evidence; furthermore, the entire process is subject to inspection if the evidence that is collected is used in a court of law.

The first responder will need to follow a set of guidelines to ensure the collected evidence can survive this type of scrutiny. The first responder will need to be well versed in the characteristics of the different types of mobile devices and additional hardware that might be encountered at the scene. Unfortunately, this is often overlooked when it comes to assigning investigators to respond to a crime scene. There is a multitude of areas that could contain evidence and as such the first responder needs to know this.

5.5.1.6.1 Scenario One:

In this scenario, an investigator arrives on the scene and discovers an iPhone6 that has a blank screen; further examination of the phone determined that the phone is in the OFF state. The following steps are recommended to go forward.

- Document and photograph the scene.
- Leave the phone in the current OFF state.
- Search for any additional equipment for the phone.
- Isolate the phone from the network with a Faraday bag or equivalent.
- Obtain and provide power to the device when possible.
- Secure the device and associated equipment for transport.
- Complete the evidentiary chain of custody.
- Transport the device.
5.5.1.6.2 Scenario Two:

In this scenario, an investigator arrives on scene and discovers an Android device that is in the ON state. Since the device is in the ON state, there are a number of additional steps that must be considered by the first responder on the scene. These steps will be addressed before the steps within the process are covered. When the device is in the ON state, the responder needs to record the screen of the device and note the time, and compare it to the local time at the scene. The documentation of this will be essential for the collection of the data. Following the recording of the time, the responder needs to identify the level of battery remaining on the device and then provide power to the device. This is critical because if the device battery exhausts its charge then the state and information that is contained in the volatile memory of the device will not be accessible, which could contain evidence directly related to the investigation. As soon as possible the device needs to be removed from the network and isolated.

As has been discussed, this can be accomplished with a device that is known as a Faraday container/bag. This container/bag is the type that can reduce or even prevent the electromagnetic emanations from the device. Having said that, it is important to note that the capability of these containers/bags has been tested and they do not function as specified in many cases. According to NIST, the following steps are recommended to go forward. While many manufacturers claim the effectiveness of their shielding device, it is important to understand that the effectiveness of the isolation device is based upon the attenuating signal between specific decibels. Therefore, the effectiveness of the isolation containers/bags tested were not 100% effective in most cases and devices used to preserve evidence require verification [58, 100].

The essential component is that the first responders should have either tested the method of isolation that they are going to use, or at the very least have some form of test results to know if the method of taking the device OFF of the network is going to work. When the device is discovered to be in the ON state then the following steps are the recommended approach to follow:

- Document and photograph the crime scene.
- Leave the device in the ON state.
- Isolate the phone from the network with a Faraday container/bag or equivalent.
- Obtain and provide power to the device when possible.
- Photograph the screen of the device if it is visible.
- Secure the device and associated equipment for transport.
- Complete the evidentiary chain of custody.
- Transport the device.
When a device is discovered to be in the ON state there are a number of security mechanisms that might be encountered. While we do not have these considerations when the device is discovered to be in an OFF state, we do have them as soon as the device is powered ON and the state changes. The following is a list of examples of some classes of modifications to consider:

- **Security Enhancements** – A variety of login, biometric, and other authentication mechanisms are available for mobile devices. Many of these are used in lieu of password in today’s mobile devices. If the investigator does not handle these correctly, then the device could lock down and even destroy its contents. The presence of some devices is constantly monitored and any change in the state of the device can result in the device going into some form of protection mode.

- **Malicious Programs** – While not as prevalent as many make out, there is a chance the mobile device will have some form of malicious software (malware) on it. Many of these types of software are designed to take control of the mobile device and in doing so, the data that is extracted from the device could be considered suspect.

- **Key Remapping** – Another thing that is not common but is a possibility is the changes to the hardware key mapping on the phone; this could be a protection mechanism setup by the device owner as a trigger that if a common hardware key is used then a program could execute and wipe or destroy the data that is considered potential evidence on the phone.

- **Geo Fencing** – There is the possibility that the device owner is of a high skill set and has configured the device to a state known as “Geo Fencing” and that is to automatically wipe the device if the geographic coordinates of the device change. While this is not a common configuration there is a chance that the device owner could deploy something like this. Another variant on this technique is to deploy mobile Wi-Fi towers to determine the device location at any given time.

- **Explosives and Booby Traps** – There is a chance the mobile device may be rigged with either explosives, or it could also be part of an explosive trigger device. This is another reason why if the device is found to be in the ON state, it is imperative for it to be removed from the network expeditiously; the trigger could be an incoming call, a text message or even pressing a key sequence. The danger of this requires that the first responders be well trained in a multitude of subjects.

- **Alarms** – Another method that has been used is using the phone’s alarm system to trigger a remote wiping application. This is not something that is common, but it is something that is possible.
5.5.1.7 Storage and Transport

After the steps identified have been followed, it is time to prepare the device for storage and transport. There are two critical things that need to be considered. This consideration is based on the state of the device at the time. If the device is in the OFF state then the critical factor is to store it in an appropriate container that is properly sealed, then label it for transport in accordance with the specifications of the investigating body. When the device is discovered in the ON state, this presents a completely different dynamic. The two critical considerations are maintaining power to the device and ensuring the device is OFF of the network. It is critical that the investigator has confidence and knows if the method of removing the device from the network has been successful. Transporting the device in an appropriate manner will help ensure a more effective privacy and security of the data contained in the device.

Once the device is transported to the forensics facility, the recommended approach is to transfer the evidence using the approved transfer of custody form. The acquisition process on the device should then take place; if this is not possible then the device and its associated hardware need to be transferred to an evidence custodian for storage. The storage of the device needs to be in an approved location that is cool and dry; furthermore, the continuing power to the device if it was found to be in an ON state needs to be discussed with the evidence custodian. If the device is OFF of the network and isolated, then the power consumption will be increased and as such, as soon as power is removed from the device the battery will drain quickly; therefore, it is recommended to not remove power from the device unless there is an extreme set of circumstances that requires it to be removed. An abstract example of the process is shown in Figure 5-5.
As identified in the abstract diagram, the installation of the write blocker is only in the case of the acquisition of the device at the scene. This is considered a rare event, but there is a chance that the acquisition will need to be done at the scene and that is why it is listed as part of the process.

5.5.2 Acquisition

The acquisition process consists of two main types of acquisition, and that is manual or tool based; therefore, the acquisition process will start with a decision step by the investigator to see if this is going to be a manual or tool based acquisition. The components of the manual investigation steps were covered earlier in this section; therefore, the focus will be on the tool based acquisition process step. With the smartphones of today provided by both Android and iOS there are a number of protections that can be used, and quite commonly are, to protect the device as stated throughout this chapter. This will require the process steps to take this into account and make the determination of this prior to the acquisition process. The steps of the on-site acquisition are as follow:

- Document the type of acquisition that is going to be attempted, manual or tool based.
- Ensure the write protection is in place.
- Verify the device is isolated as much as possible.
- Ensure the device has adequate battery remaining.
- Obtain and provide power to the device when possible.
- Photograph the screen of the device if it is visible
- Secure the device and associated equipment for transport.
- Complete the evidentiary chain of custody.
- Transport the device.

### 5.5.2.1 On Site Acquisition

As indicated within this document, it is rare that the acquisition will be conducted at the site of the triage, because the first responder examiner will have a different level of skills, and it cannot be assumed that they will be qualified to deal with all of the obstructions and possible challenges that can be encountered, so it is to be avoided. Since there is a chance that the triage will require this, an example of this is shown in Figure 5-6:

![Figure 5-6: An Abstract Example of the On-Site Acquisition Process](image)

The last step that is indicated in Figure 5-6 represents a significant amount of the acquisition process, and will be discussed as the first step of a laboratory acquisition.
5.5.2.2 Laboratory Acquisition

The ideal situation for execution of the forensics framework is to perform the acquisition at the digital forensics laboratory. The importance of this is reflected by the fact that the lab will have the complete tool suites of the organization; furthermore, it can reflect well if the evidence is used in litigation due to the fact that the lab represents a location that is dedicated to conducting the forensics process. This can also assist in the fact that the process is defined as a formal and repeatable sequence of events. While not mandatory for the submission of evidence, it can assist in enforcing the evidence collection process since the lab location can represent a professional forensics capability; moreover, there are certification and accreditation bodies that can certify the laboratory as a qualified forensics laboratory. As an example, the following are certification and accreditation bodies:

- American Society of Crime Laboratory Accredited Laboratory Index[101].
- American Society of Crime Laboratory International Testing Program [102].

The process step for the acquisition will be contingent on the parameters that have been discussed in this chapter. An example of the process steps is shown in Figure 5-7. The figure below highlight that if the device is not obstructed then the acquisition can start right after an approved tool is connected. Otherwise, the device will need to be unlocked first through the use of various means discussed earlier.

![Figure 5-7: An Abstract Example of the Laboratory Acquisition Process](image-url)
5.5.3 Analysis

The process of Analysis and Examination is largely dependent on the data that has been collected; if the data has been collected in a forensically sound manner, then the analysis of the data should produce the same results no matter how many times it is analysed. The experience of the investigator is critical when it comes to performing forensic analysis of the evidence. There are a number of challenges that are encountered when examining the data, and they are for the most part related to the ability of the tool to extract or in many cases carve the remnants of whatever type of data the device has either manipulated or stored. This of course will largely depend on the tool and whether it can perform a physical acquisition on the device or not. If the tool can only perform a logical acquisition then there will be data that is not recovered from the file system such as anything that has been deleted on the device. An example of the steps of the acquisition process is as follows:

- Determine if the acquisition is to be manual or tool based.
- If the decision is made for a manual acquisition then the process as defined within this document and the associated references shall be adhered to.
- Is the device an obstructed device?
- Select the type of JTAG process to use.
- For a tool based acquisition, ensure the device is protected from being written to, with the installation of a write blocker.
- Acquire the data.

5.5.4 Reporting

Reporting is the final stage when the case is completed and a report highlighting evidence found is produced and submitted. It is the process where summarised information is prepared to outline the steps that were taken and the final results of the investigation. Therefore, it is essential to have all necessary actions and observations recorded, highlighting the date, time, and summary of results of conducted tests and examinations. NIST recommends that [47] “A good report relies on solid documentation, notes, photographs and tool-generated content”.

In addition to describing the methods and tools used in the process (Refer to Overview of Smartphones Operating Systems Technologies and Forensics Procedures chapter for more information), and the investigator's ability to defend the utilized tools in court, two sources of recommended procedural practices - NIST's Guidelines on Mobile Device Forensics Report [47] and the National Institute of Justice's Electronic Crime Scene Investigation: A Guide for First Responders Report, [53] state that reports may include the following information:

- Identity of the reporting agency and of the submitter, date of evidence receipt and of report.
- Case identifier or submission number, investigator, and examiner identity and signature.
Chapter 5: Proposed Framework Architecture and Design

- Descriptive list of items submitted for examination, such as make, and model.
- Tools, software, equipment and set-up used in the examination.
- Brief description of steps taken during examination, such as string searches, graphic image searches, and recovering erased files.
- Supporting materials such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation.
- Examination documentation should be preserved according to policy and include:
  - Sufficient detail to enable another examiner to repeat the findings independently.
  - Documentation of any anomalies in the data acquisition.
  - Substantive communication notes regarding the case.
- Report of findings:
  - Seek to address case-specific requests from the investigator.
  - Identify the scope and/or purpose of the examination.
  - Provide a detailed description and/or photographs of the mobile phone examined.
  - Supplement reports related to the examination.
  - Include examiner name and date of exam.
  - Information regarding the packaging and condition of the phone.
  - Provide the relevant information in a clear and concise manner.
  - Should be reviewed according to organizational policy.
- Details of findings:
  - Specific files related to the request and other files that support the findings.
  - String searches, keyword searches, text string searches and graphic image analysis.
  - Internet-related evidence, such as website traffic analysis.
  - Indicators of ownership, which could include program registration data.
  - Description of relevant programs on the examined items.
  - Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies.

5.5.4.1 Reporting Process Steps

The reporting step of the forensics framework as indicated in this section is represented in process blocks as shown in Figure 5-8. As can be seen in the figure below, besides the introduction and the conclusion of the report, it will include a report and details of the findings.
Chapter 5: Proposed Framework Architecture and Design

5.6 Abstract Model

Based on the research and analysis presented in this chapter, an abstract model that represents the forensics framework process is developed and presented. This model is a high-level representation of the process block steps presented in this research. This is represented in a pseudo code that will allow for it to be easily mapped into a programming syntax (see Appendix D). An example of the model is shown in Figure 5-9.

As can be seen, the Abstract Representation Model consists of all 4 PBFMF steps; starting with the First Responder Triage (Preservation) which shows the situation if an acquisition is to be conducted at the scene; Acquisition where a write blocker is to be installed if it is to be at the scene in addition of following other essential steps for the laboratory one; Analysis and ending up with Reporting. In addition, more detailed information can be found, such as the preparation phase, moving into sub information details of the 4 major steps, where linked procedures of how to implement the PBFMF are offered.
5.7 Summary

In this chapter, we examined the reality that at the time of this research there are no frameworks that meet the needs of the ever changing and expanding world of mobile devices, and the chapter proposed a framework model that is based on an open architecture, provides platform independence, and extensibility to accommodate the current and future market of these devices. Furthermore, the framework provides for streamlined reporting and a simplified design process. Summary Table 5-1 illustrates some of the existing mobile forensic frameworks and how each compares to the proposed PBFMF framework in the main categories discussed in this chapter (refer to section 5.1, pages 92-94 for the criteria explanation for the (y-axis) of the table below). Within this chapter, we discussed the challenges to the framework from the standpoint of having an approved tool that we
can connect to provide the required capabilities that the current research has shown is non-existent with the current tools of today.

<table>
<thead>
<tr>
<th>Framework</th>
<th>Platform Independent</th>
<th>Extensible</th>
<th>Simplified design</th>
<th>Streamlined Reporting</th>
<th>Specific to Mobile Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing Process for Mobile Forensics</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Efficient Framework for Mobile Devices</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>The HDFI Process Model</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Implementing Digital Forensic Framework for Android Smart Phones</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Ontology-Based Forensic Analysis</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Process Based Framework for Mobile Forensics (PBFMF)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Towards a Unified Forensic Investigation Framework of Smartphones</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 5-1: Analysed Forensic Frameworks compared to the proposed PBFMF

The tools analysis highlighted that there was no tool adequate for the requirements; the framework was put forward to concentrate on the two most popular operating system devices and then provide a standard process to follow. In summary, the chapter presented a model that can be used to apply the framework against different mobile device scenarios, which means that the framework is all about applying the process and providing a usable and reportable output.
6 Evaluation of the Proposed Process Based Framework (PBFMF)

In this chapter, two different mobile forensic scenarios will be looked at and applied to the proposed PBFMF framework. In addition, a comparison of two other mobile forensic frameworks to the researcher's proposed framework will be made in order to review the strengths and weaknesses of each and compare both to the newly proposed framework. The most accurate method for testing the framework is to apply it to several different scenarios, and in this section, this is what has been done. The two scenarios are as follows:

- An LG E400G mobile phone with Android 4.X OS is used for the 1st scenario.
- A Samsung Galaxy S II mobile phone with Android 4.1.2 is used for the 2nd scenario.

Neither of these devices have been rooted, nor obstructed. It is interesting to note that the latest technologies of mobile phones have made it very difficult to get data and information from a device when it is obstructed and is locked by a PIN. This was made evident with the recent Federal Bureau of Investigation (FBI) in the United States requesting assistance from Apple with the obstructed iPhone [103]. As the technology continues to advance, the reality is that obtaining anything from these encrypted devices is less and less likely.

6.1 Application of the PBFMF Framework (1st Scenario)

The scenario for the 1st device (an LG E400G mobile phone with Android 4.X OS) is that of a phone discovered at a site where a violation of corporate policy has occurred, and someone has connected their phone as a tether to the corporate network and provided images to the Internet. The investigation is to see if it can be discovered what web sites the suspect has visited on the device, and if there are any images on the device that could have been sent to the Internet. The acquisition process for device will be an onsite acquisition.

Based on the Process Based Framework for Mobile Forensics (PBFMF), the following steps will be applied:

- Arrival on the Scene.
- Evaluate the crime scene.
- Documenting the scene.
- Identify state of the device
Chapter 6: Evaluation of the Proposed Process Based Framework (PBFMF)

- Remove device off the network
- Maintain the integrity of the device (Write Blocker)
- Connect approved tools
- Acquisition
- Analysis
- Reporting

6.1.1 Arrival on the Scene

When the investigator arrived at the scene, there was no personnel in the vicinity; the scene was an office where the suspect worked.

- Assessment of the scene
  - There was nothing identified at the scene that could pose harm to the investigator; therefore, the scene assessment is evaluated as safe and the investigation can continue.
  - The device was observed to not contain a SIM card and as such it was not connected to a mobile device provider.
  - Based on the fact that the SIM card is not installed, there is no requirement to take the device off of the network. There is a possibility that the device could be connected to a wireless connection, but as indicated in the Figure above, this is not the case with this device. This allowed the investigator to make the determination that the device is in an off-network state and no method of communication is currently taking place, so the investigation can continue to the next step in the framework.

6.1.2 Documenting the scene

The device was discovered at a scene that was used by the suspect as a work space; there are a number of items that were discovered at the scene that in a forensics investigation would be processed. The items include an external hard drive, several USB drives and a laptop computer. For the purposes of this applied practice testing of the framework, this investigation will concentrate on the mobile device component only.

As shown in the Figure 6-1 above, the device is not connected to the laptop at the scene; this would make for a much more complex forensics investigation, but in this scenario there is no connection with the phone and laptop. While In Figure 6-1, the side view of the crime scene is presented and shows the scene along with the peripherals and other data related components.
At this point documenting of the crime scene is complete and the investigator can move on to the next step. Prior to doing so, based on the information discovered at the crime scene and the guidance provided by the framework, we have a device that is not obstructed, and has nothing preventing interaction with it; therefore, the decision was made to interact with the device and record the viewable information and document it prior to proceeding to the next step. The first thing that the investigator looked at is the contact information, an example of this is shown in Figure 6-4. As can be seen from the image, only two viewable contacts were discovered in the device.

Call Log was the next item examined; there was nothing discovered within the log, so the next item investigated was the browser history. There was nothing visible, but there were a number of Bookmarks located within the phone as can be seen in Figure 6-5.
Further manual review of the device did not indicate anything of interest. However, the investigation of the mobile device will continue in order to find out if a violation of corporate policy had been committed.

### 6.1.3 Identify State of the Device

As already revealed during the investigation thus far, the device is in the “On” state, and as such the investigation will continue with the steps as identified in the framework. The critical component since the device is in the “On” state is to ensure that it is taken off the network; but with the revelation of the SIM card being removed, there is no requirement to take the device off the network. The next part of the process is to ensure that the device has power and remains powered on since this can lead to a complete loss of data; the impact of this has been mitigated by the investigator being able to conduct somewhat of a manual investigation by browsing the data that is visible on the device. Despite this, it is still imperative to maintain power on the device since there might be a routine set that could make the device unusable should it be rebooted or lose power. This possible threat of “bricking” the mobile device makes it essential to maintain power to the device, and this was accomplished by connecting an EasyAcc 26000mAh Power Bank (4A Input 4.8A Smart Output) External Battery Charger.

### 6.1.4 Write Blocker

As identified in the framework, connection of a Write Blocker to protect the data from being written to on the device is another major consideration for our investigation. The process for the Write Blocker was met with the Paraben Mobile Device Portable Acquisition System being carried to the
scene (Figure 6-7). This kit contains special cables that are configured for extraction of data in a forensically sound matter and have a write blocking capability built-in.

Figure 6-4: Paraben Mobile Device Portable Acquisition System

### 6.1.5 Connect Approved Tools

With the device connected to a special write blocking cable, it is safe to continue with the process and steps of the framework. Therefore, the next step of the framework is to connect approved tools.

As has been identified throughout the research, the connection of approved tools can be a challenge, and based on this we will list the challenges faced with the tools as the investigator attempts to connect then acquire the data for a device.

The first tool that the investigator decided to use is the Santoku virtual machine image; information about the tool is shown in Figure 6-8. The Santoku tool contains three main functionalities, and can be used for much more besides the forensics capability. There are two methods that can be chosen to deploy the machine in a virtual environment, they are as follow:

- **Live.** This is considered the simplest and quickest way to deploy the Santoku machine with the live ISO image. The downside of this is that the machine cannot be written to, and any data and information from this process will have to be written to some form of media such as USB for extraction and saving of the evidence data.

- **Hard drive installation.** The hard drive installation allows the investigator to write information that was discovered to the machine, and there is no requirement to use temporary storage; the biggest disadvantage to this is the fact that the machine will have to be installed to the hard drive, and this is not only time consuming, but can also fail and not be a successful setup.
Both of the options were considered as part of the research, and since the live option is the quickest setup, this is the option that was selected to demonstrate the connection of the approved tool. The process is to use the virtual software tool, and create a machine that boots from the ISO image; an example of the initial boot options when the ISO image is mounted is shown in Figure 6-9.

Once the live machine has booted, the system will login automatically; the Santoku menu is located at the bottom of the screen, and within the tool are a number of different categories of tools. The tools for the mobile device forensics are shown in Figure 6-7.
Now that the machine is booted and the tools have been looked at, the next and the most difficult step is to get the device to be recognized in the virtual machine after it has been connected to it. Once the host machine recognizes it, we can attempt to connect to the device within the virtual machine. As has been shown throughout this research, the process is not as simple as it might sound, and continues to be one of the biggest challenges to establish a suitable forensics capability for the industry. Eventually, the phone was connected to the machine using the special write blocking cable from the Paraben Company. At first, the phone was not recognized by the host operating system of Windows 10; the Device Manager was reviewed and it was discovered that the device was not in any list. The machine was then rebooted and once the machine came back online, the device was connected again, and the device displayed a menu to set the USB mode of the connection. This is shown in Figure 6-8 below.

![Figure 6-7: Santoku device forensics tools](image)

![Figure 6-8: LG device USB options](image)
As can be seen from the figure, the setting is for “PC software” which matches what the device needed to be set to by clicking on “OK”. The connection is then completed and successful, and is indicated by the USB icon shown at the top of the screen.

Once the device is successfully connected to the host machine, it can be disconnected from the host operating system of Windows 10, which is accomplished via the Removable Devices menu item shown in Figure 6-13.

The connection is then completed and successful, and is indicated by the USB icon shown at the top of the screen.

Once the device is successfully connected to the host machine, it can be disconnected from the host operating system of Windows 10, which is accomplished via the Removable Devices menu item shown in Figure 6-13.

The next step in the process is to enable the USB debugging capability, where its setting is found under the Settings | Applications | Development.

Once the USB debugging is selected, a message box explaining what the debugging option means and requesting acceptance to enable it is displayed, since it is a development type of option. The key in this option is that all of the data is allowed to be copied and/or extracted back and forth without any form of notification of what is taking place, which is a requirement to be able to access the data on the device. Once the debugging mode is enabled it is identified with an icon that shows it is enabled.

The process to verify that the device is connected and visible on the bridge is to enter the commands which will enable communication with the bridge. This is accomplished with `adbdevice command line`. An example of the output of this command that shows the device is connected is shown in Figure 6-10.
As can be seen from the above image, an LG device is connected. This means that different approved tools can now be connected to the device. As stated earlier, if the device is obstructed and/or PIN locked then the connection cannot be successful in most cases.

### 6.1.6 Acquisition

The next step is to use the tool by acquiring the data from the device using the connected tool. Different tools can be attempted based on availability and the investigator’s own preference. In this case, the **AF Logical OSE tool will be used**, which is an open source software package that is provided for conducting Android forensics. For the software to work, it has to plant an agent onto the device, and accepting the installation of the software is also required for the tool to be installed. To successfully install the tool, the process is to push the package and enter the following command: **AF Logical OSE**. Once the command is entered, the package should then be pushed to the device. An example of this is shown in Figure 6-11.
Once the package is pushed onto the device, we can continue with the logical data extraction of the information by just pressing the **Enter** key. However, prior to that, an interaction needs to be established with the agent that is found within the applications on the device, which can be accessed by clicking on **Applications | AF Logical OSE**. Once, the application has opened, the next step is selecting the data to extract from the device, and these options are shown in Figure 6-18.

Once desired options are selected, we will need to click on **Capture**. Once the Capture button has been selected, a notification message that the extraction was successful will be displayed. Once the
extraction is complete, enter is pressed on the Santoku machine to extract the data from the device. The result of this for the LG device is shown in Figure 6-19.

![Figure 6-13: Extracted device data](image)

The tool will then extract the files and write them to the `/root/aflogical-data`, and stores the information in a folder that reflects the date of the device. An example of this is shown in Figure 6-14.

![Figure 6-14: Extracted data folders](image)

As the image shows, this device has a date that is set in the year 1980; this is probably an indication that there have been attempts to wipe this device's data. However, more can be discovered once the data reviewed has been written to these folders. Upon further examination of the data that was logically extracted, it was discovered that all of the data on the phone had been wiped. There is a chance that the data could be extracted using a physical acquisition, but that would require the
device to be rooted; since this is a violation of corporate policy, the decision was made to stop with a logical acquisition.

Before moving on within the framework, it was decided that another previously reviewed tool (Mobiledit) should be used as part of the forensics process, where the tool version was 9.0.1.21194 at the time of the investigation. As this researcher has discovered, the free and open source tools usually do not provide enough data for the investigator on their own; therefore, the Mobiledit tool will be used in the trial version mode to see if the results are any different, and whether or not more data can be extracted than the Santoku tool managed. Once the Mobiledit tool was installed, the device was connected to the machine, and the tool loaded the appropriate drivers; at the completion of the process, the tool listed the device and information about it on the dashboard as can be seen in Figure 6-15.

![Mobiledit dashboard](image)

**Figure 6-15: Mobiledit dashboard**

The investigator can then select from the different options, where the first option is to back up the data from the device. As with investigation with the Santoku tool, where the acquisition is logical. Once the **Backup/Restore** option is selected, the menu opens for the investigator to select which operation is being performed. Once the selection is made for the Backup, the selection screen for what data to backup appears.

Once the data is selected, the extraction of the data from the device will start. As noted in Figure 8-22, all data options were selected to be backed up, which could take a long time to complete. An example of the process once it has started is shown in Figure 6-16.
Chapter 6: Evaluation of the Proposed Process Based Framework (PBFMF)

Once the process has completed a review of the icons shows that other than the file system and application on the phone, there was nothing else found on the device. This is reflected in Figure 6-17. At this point, the investigation has shown with two different forensics tools that without a physical extraction there is no evidence of violation of the corporate policy.
6.1.7 Analysis

Since there is no data found on the device, there is nothing to perform analysis on; so in this investigation, it seems that the device went through some form of a wiping. With the date set to 1980, this is another indication that the device had had tools used on it that do wipe data. A physical acquisition would be required, but that would require the rooting of the device, and in a case like this that would not be recommended. The investigator was able to perform a manual investigation of the device as well, and did not discover anything of interest.

6.1.8 Reporting

As the framework has shown, this is the last step of the process, and it is where the investigator explains the process he/she has used, and the methods of how the data was protected while the investigation was being conducted. For this case, the investigator would list the following abstract steps.

- Informed of a potential policy violation
- Arrived on the scene
- Assessed the scene for any hazards to the team
- Documented and photographed the scene
- Noted all of the peripherals located within the scene
- Examined the state of the device
- Device was discovered to be in an “ON” state
- Proceeded in accordance with the guidance of the PBFMF
- Conclusion

For the purpose of this research, the steps will not be expanded on. The intent here was to take the framework and apply it as has been shown. It was discovered during interviews with the suspect that the phone had been wiped using the Cellebrite Universal Forensics Extraction Device (UFeD).

6.2 Application of the Framework (2nd Scenario)

The scenario for the 2nd device (a Samsung Galaxy S II mobile phone with Android 4.1.2OS) is that of a phone that has been retrieved from the home of a potential homicide suspect; based on the interview of the subject, the claim is that the suspect was not with the victim on a trip abroad, and could not have perpetrated the crime against a female whom is reported to have been found dead in her hotel room. The phone was confiscated via a search warrant of the suspect’s home, and it has
been tagged and bagged and presented to the investigator for examination. Based on this, there is no required examination at the crime scene, and this will be a laboratory investigation.

Due to the fact that the device was provided to the investigator, the framework will be followed as per the following items:

- State of the device
- Take device off the network
- Maintain the integrity of the device
- Connect approved tools
- Acquisition
- Analysis
- Reporting

This is another example of the extensibility of the framework, and that is the capability to be used with a variety of different scenarios.

### 6.2.1 State of the Device

The device was received by the investigator in the “Off” state. Since the device is in the “Off” state, it is not known if the device needs to be taken off the network or the status of the battery. Based on this, the device is taken to a Faraday room where there is no possible leakage of electromagnetic radio frequencies. At the completion of this isolation, the device is connected to the external battery pack so that power is provided in case the device is in a low or drained battery state. There is a chance that the device is off because the battery has been exhausted.

Once the device has been connected to the battery source, the next process is to power the device on so that a determination can be made on the next step using the guidance from the framework. Once the device is powered on, it is now in the same category as a device that was found in the “On” state. The received device is examined to see if there is any obstruction on the device; if there is, significant challenges are faced for conducting the forensics investigations. In the case of this investigation, the device is not obstructed. The isolation room of the device is confirmed by the existence of the icon that shows there is no signal being received by the device.

### 6.2.2 Connect approved tools

As was presented in the first scenario, the first step of the process is to connect the device and ensure it has a write blocker installed. The next thing needed is to get the device recognized by the machine operating system, where the device is connected to see if the operating system recognizes it. The first investigative tool deployed is the Mobiledit tool, which is launched to see if the device has
been connected and recognized. An indication of the software being launched when the device has been connected and recognized is shown in Figure 6-26.

![Connected device](image)

**Figure 6-18: Mobiledit with connected device**

**6.2.3 Acquisition**

The next step is to attempt to back up the data from the phone; as before, the **Backup/Restore** option is clicked. This will result in the device being accessed and the data being backed up from the phone. Once this option is selected, a default setting will be presented for the operation.

Based on the desired information from the prosecutor, the default settings will suffice for what we are attempting to extract from the device. Once the data options are selected, **Next** is clicked and then the process will start. The time it will take the process to complete will depend on the amount of information included in the device. An example of the results from this operation is shown in Figure 6-28.

![Backup results](image)

**Figure 6-19: Successful backup of the device data**
The results of the backup extraction show a large amount of information from the device as shown in Figure 6-29 below.

![Samsung Galaxy S II Skyrocket (Read-Only)](image)

Figure 6-20: Mobiledit recovered data

### 6.2.4 Analysis

Since the Mobiledit tool has discovered data on the device, the next step of the process is the Analysis; returning to the framework for guidance, we need to analyze the following data:

- Analyze text logs
- Analyze call logs
- Analyze data from Apps
- Analyze Photos
- Analyze other relevant data

A review of the default settings of the tool shows that the option is not selected to extract the media; therefore, the investigator conducts another backup of the device with the selection of the media content. The media is extracted and the images are discovered by the tool. A review of the images from the device show there are photos that appear to be from a location adjacent to the hotel, where the female was reported to have been found dead. These photographs were tagged and examined at the hexadecimal level to see if amplifying information can be discovered from them. The thumbnail images of the data that have been extracted are shown in Figure 6-21.
One of the media items that was recovered is a video in the format of a MOV file. This video provides what appears to be dialogue between the victim and whomever is operating the camera. At this point, the decision was made to connect the device to another tool and look for any additional information that the Mobiledit tool has missed, and additionally compare the results of the data extracted from the two tools.

The second tool that was used is the Andriller tool, which is another Android type of forensics tool. It is a commercial tool, but does provide a 14-day license trial. The tool can be run on Windows, but will have to have the drivers installed, just like the other tools that have been discussed in this research. Because of this, the investigator downloaded the software to the Santoku virtual machine by accessing the web site www.andriller.com. As required by the AFLogical-OSE, the Android Debug Bridge (ADB) will be used by entering in a terminal window `adb devices` to verify the device is connected to the machine. An example of this is shown in Figure 6-22.

As indicated in the image and from the output of the command, the device is connected and recognized by the Santoku virtual machine. The tool has to be first extracted, and once it has been downloaded, `tar -zxvf<filename>` is entered and then the tool is run by entering `/Andriller` in the folder that was used for the extraction. An example of the tool launching in Santoku is shown in Figure 6-23.
Chapter 6: Evaluation of the Proposed Process Based Framework (PBFMF)

Figure 6-23: Andriller launched in Santoku

Once the tool has launched, the extraction is started by clicking the Go! Button. An example of the results of clicking the button is shown in Figure 6-24.

Figure 6-24: Extraction in process

The Andriller tool extracts a great deal of data from the device. At the completion of extraction, a report is created that is formatted in HTML.
Chapter 6: Evaluation of the Proposed Process Based Framework (PBFMF)

Based on the analysis thus far, a decision was made to try to examine the exif data from the discovered phone images. Within the Santoku distribution there is a tool for conducting this, and that is the Exif tool (a tool capable of reading, writing and editing meta information in a wide variety of files).

Investigation of the data does not show anything related to the GPS coordinates at the time of the photo. At this point, there has been enough evidence and the investigation can proceed on to the next step in the process.

6.2.5 Reporting

For this scenario, there are more details to report on than in the 1st scenario. The report summarization is as follows:

- A request was received to highlight that a device had been recovered using a search warrant and it was part of an investigation into a potential homicide, and this device was part of the seized components from the residence of a potential suspect.
- The device was received in an “Off” state and the investigator followed the guidance of the Process Based Framework for Mobile Forensics Tools (PBFMF).
- Following the steps and guidance of the PBFMF, the device was isolated and connected to an approved forensics tool in a forensically sound manner.
- There were three tools that were used by the forensics investigator: Mobiledit, Andriller and AFLogical-OSE.
- The examination of the phone showed that the device was not in a rooted state.
- All of the extractions of the device were logical in nature, and based on the examination of the results from the extractions this was sufficient to extract the required data.
- The recovered images showed 7 graphic images that were in the JPEG format, and one video that was in the MOV format. This data appears to show the incident’s location.
- At this discovery, it was decided to examine the exif data of the images, and see if there was any evidence that could be extracted to show the location of the device when the pictures were taken. The results of this examination were negative, and as such there is no meta data contained within the images to identify the location of the phone at the time the images were taken.
- The meta data of the phone did confirm the images were taken on the same date that the victim was vacationing.
- This report has shown that the device has been connected to a wireless network and the images could be from that location. Additionally, a quick browsing of the hotel’s website
and its surroundings showed similar images of those that were discovered during the investigation.

6.3 Comparing other frameworks to the PBFMF

As was discussed earlier in chapter 4, there are other frameworks that were developed for mobile forensics. Based on this researcher's proposed framework, one of those discussed frameworks (Developing Process for Mobile Device Forensics) by Murphy[98], in addition to another framework (Implementing Digital Forensic Framework for Android Smart Phones) by Alamin and Babiker [104], will be compared and discussed in regard to the findings of this later evaluation of the (PBFMF).

6.3.1 Developing Process for Mobile Device Forensics

This research has identified that the majority of the existing frameworks are specific to one type of device, and the PBFMF has the benefit of being neutral; that is why the work from Murphy is being used in comparison with the first scenario. This framework by Murphy starts with the **Intake** phase whereby how the documentation is processed leads to the start of the forensics investigation. It is different from the PBFMF in that within the later framework, the focus is on the arrival at the scene. It is believed that the framework Murphy has provided is set with the first phase to match that of a typical in-house police type of investigation; since Murphy is a detective, then that would make sense from the standpoint of starting with the paperwork process. The view of this research is that the process of the PBFMF provides more details and is based on the requirements of a first responder on scene.

Murphy's work further shows the point from that of a law enforcement investigation; in the **Identification** phase, details are explained about the legal authority and other requirements such as a search warrant and how to proceed in different situations. This is not something the PBFMF expanded on, and this is because the law is different from one country to another and it may also depend on the jurisdiction.

Within the **Preparation** phase of the Murphy work, we are presented with a table that shows the different types of examinations that are available with different tools. Within the PBFMF the framework presents an application of different tools to a sample set of the available tools; therefore, the PBFMF provides actual data with first-hand knowledge of the process and more importantly the data extraction results. The information contained within the Murphy paper does not match with what was discovered during the actual application of the PBFMF to different devices, and this research has shown that the data listed in the table is not representative of the software tools at this time. The PBFMF research avoids this by not focusing on the tool aspect; the research has
Chapter 6: Evaluation of the Proposed Process Based Framework (PBFMF)

mentioned the challenges that are presented when a framework presents theoretical data vice application of the framework against mobile devices and that is time; since what works at the time of the research may not, and more than likely will not, work the same when further research is conducted. The data that is contained within the Murphy work is from the work of Kessler in 2010, and the constant change of the devices makes the majority of the data invalid at the time of the research for the PBFMF.

The Isolation phase within the Murphy work reflects the same logic and information for the most part of the PBFMF; there are some variations and this is based on the time between Murphy's work and the research for the PBFMF. The Murphy work refers to the acquisition phase as the Process phase, and within this the explanation of the challenges with respect to the different tools being able to provide the data in a forensically sound manner can be analysed.

In the Verification phase, the importance of checking the data for integrity as it is extracted and in the comparison of the data to ensure the extracted information is correctly presented by the tool, takes place. Within the PBFMF the framework explains this as the process of tool validation, and this is in accordance with the guidance from NIST. Based on this, it is the opinion of this researcher and further validated with the results of the application of the framework to different devices, that the additional step of comparing the extracted data at the hexadecimal level with the data reported by the tool is not required in an investigation, nor additional steps are, since the PBFMF has complied with NIST guidelines.

The one phase that is in the Murphy work but not in the PBFMF is the phase for Archiving. This is the explanation and presentation of the fact that the extracted evidence has to be stored and remain in storage for a period of time. The exact amount of time is dependent on many factors. The PBFMF did not address this, because the framework is more focused on first responders and the triage operations. Although the PBFMF will help reduce data privacy breaches, archiving and storing the data is a process that will occur after the evidence is transferred to the forensics lab facility.

6.3.2 Implementing Digital Forensic Framework for Android Smart Phones

This framework is focused on the Android platform, so it is not as extensible as the PBFMF. The comparison will therefore only be on the process as it relates to an Android platform. The research and framework in this paper has the advantage of being ubiquitous across all of the different mobile devices, indeed any device that has a memory to include the Internet of Things (IoT) and the growing number of Unmanned Aerial Vehicles (UAVs), because the basis of PBFMF is its ability to be applied to any device/appliance that stores data in memory devices.

The Android Digital Forensic Framework presents the Android Software Development Kit (SDK) as part of their research, and this is not something that was presented with the research within the
PBFMF; this is because the framework presented here is not only vendor neutral when it comes to the platforms, but also when it comes to the tools that can be used. The PBFMF is platform independent and was designed to respond to any mobile device operating system.

Within the Android Digital Forensic Framework, the research shows that as a part of the SDK the Android Debug Bridge (ADB) is the component that is used to connect to the device; again, this is covered here within the research for the PBFMF. The Android Digital Forensic Framework explains the process of connecting the ADB with the device, and this explains that there are commands that can be done on the device using the ADB interface. There are similarities here to the data contained in this research and development of the PBFMF, but with the Android Digital Forensic Framework there is no explanation of applying the framework outside of a theoretical setting. There is a table however, that can be used as a reference for the commands to be used for the extraction, so for the Android device this guidance from the Android Digital Forensic Framework explains more of the how than is explained in the research and process explained within the PBFMF. Additionally, within the table the commands that can be used to take the device off of the network using the ADB are shown. The challenge with this, and it is addressed in the PBFMF, is that the delay of connecting the device, then running the ADB could cause a significant amount of the data within the device to change.

The Processing and Verification phase explained in the Android Digital Forensic Framework shows that the data can be extracted from the device using the ADB, but the first command that is shown for the device shows escalation of privileges using the su command. For this to happen the device has to be rooted, and this requires a significant amount of change of the data on the device. An example of an attempt to execute the command as provided in Android Digital Forensic Framework is shown in Figure 6-25.

![Figure 6-25: Failed escalation attempt](image)

The next phase that the Android Digital Forensic Framework explains is the Documentation, Presentation and Archiving. It is at this point where the Android Digital Forensic Framework shows the limitations of the ADB in that the ADB does not provide any capability for this required phase. The Android Digital Forensic Framework explains an example of a tool to meet the needs
of this phase and that is the tool **lowmanio Foreman**, which is an open source forensic case management system. It helps the forensic practitioner to organize cases. This is one area that is not addressed in the PBFMF, and this is because the research has shown it is not required, and is provided by the tools that have been featured and examined within this research.

### 6.4 Summary

In this chapter, the research has identified the need to take the proposed framework (PBFMF) and apply it to an actual case. The process was to identify two different scenarios, and apply the framework to each scenario. At the completion of using the proposed framework to apply to these two scenarios, the framework was then compared to two different existing mobile forensic frameworks. It is the view of this researcher that both of the compared frameworks have somewhat similar process steps to the PBFMF, but they do not provide a complete and comprehensive solution that can be applied to any device that is encountered. This research has identified that the PBFMF has the benefit of being neutral and platform independent.

The results in this section have shown that the PBFMF provides a step by step process and framework for an examiner to follow, and this framework is viable and a robust process that the industry not only can use, but also needs. The research throughout this paper has shown the need for future work to take the challenges that have been identified and provide a request to the main vendors of the mobile devices to assist by standardizing the data contained within their devices, and outputting that data into a format like that of XML as provided in this research.
7 Conclusion and Future Work

Mobile phone usage has exploded in the last two decades and the technologies that support mobile devices are constantly evolving. This field of mobile forensics, which is derived from digital forensics, is a relatively new field. Currently mobile forensics work is fragmented and there have been attempts to develop a common framework for use by the mobile community. However, no common framework has been adopted to date. The introduction of the IoT in the past few years is also rapidly changing the landscape of digital investigation and mobile forensics. The future of mobile forensics will undergo major transformations because the technology continues to bridge the gap between what is considered a device (i.e. desktop, laptop, phone, tablet, etc.) and appliance (i.e. home appliance, cars, etc.) The convergence of these technologies will make it difficult for the mobile forensics community to continue viewing investigation as an individual task and will have to start rethinking conventional wisdom regarding mobile investigation. To provide a solution to these issues, the objectives of the research were to (1) propose a new mobile forensics framework that could be used by the mobile forensics community as standard for investigation; (2) examine the usability of mobile forensics tools and better understand the complexities preventing the mobile forensics community from effectively using such tools; (3) conduct analysis of previously designed/proposed mobile forensics frameworks, so that appropriate guidelines are set; (4) research mobile forensics tool interoperability, or lack thereof, and understand the barriers, if any, to interoperability; (5) research current security and forensics standards in the mobile industry and gain a good understanding of such standards; (6) explore newer technologies such as IoT, big data and cloud based devices to determine how effective current mobile forensics software is working with these new technologies.

7.1 Conclusion

In summary, the key contributions of this thesis are:

Proposal of an extensible Mobile Forensics Framework: Based on the research and analysis completed in this thesis, the proposed mobile forensics framework was based on platform independence, open architecture, extensibility, simplified design, and streamlined reporting. The proposed process based framework is composed of four main processes, First Responder Triage, Acquisition, Analysis, and Reporting. The First Responder Triage process consists of arrival at the scene, evaluating the scene, documenting the scene, removing the device from the network, installing a write blocker, establishing the chain of custody, stringing the device and transporting...
the device. The Acquisition process involves determining the type of acquisition, manual or tool based, and based on that, additional steps will be triggered. The Analysis Process depends on the data being acquired. Physical acquisition of data has some advantages over the logical acquisition of data, specifically related to deleted records. This process identifies such issues and proposes steps to be followed for appropriate ways of analysing acquired data. Finally, the Reporting Process establishes guidelines to be used specific to what should be included in the report, report introduction, report findings, finding details and report conclusion.

**Mobile Forensics Framework Analysis:** A comprehensive survey of mobile forensics frameworks was completed in this research. Certain criteria were taken into account when examining mobile forensics. An overview of each framework was provided along with the impression based on the analysis as well as recommendations for areas that the framework may lack or need to be improved on. Overall, the analysis of many of the existing frameworks fell short in certain areas, most were geared towards a specific operating system, mainly, Android based operating system. The existing frameworks also tended to solve for a specific issue rather than being a more open and extensible framework. Most of the existing frameworks used many steps that made it confusing for users to follow and difficult for developers to adopt. The outcome of the analysis clearly indicated a need for a framework that is platform independent, extensible and capable of integrating newer mobile device technologies.

**Mobile Forensics Tools Analysis:** There are currently many players in the digital forensics industry. Some of the digital tools were modified to respond to the mobile nature of the technology. New mobile specific forensics tools were developed as well. Most of the existing tools have core and optional requirements. This research used the outcome reports provided by NIST where they specify the areas in which each tool should be tested and how the test should be conducted. Measuring these tools in the same way provides for a better comparison. Many tools were acquired via direct purchasing, trial basis or limited/light version downloads. The test methodology used was to install the test tools on the preferred environment by the tool developer (e.g. Windows operating system, Linux-based operating system, Virtual Machine, etc.). Four devices were used to test each tool. The devices were iPhone 6, Jailbroken iPhone 4, Samsung SM-G316HU, and Samsung GT-S6812i. The aforementioned devices were used to gain a better understanding of the test results. The results of each of the tools tested were divided into connectivity, PIM data, Case File Data Protection, Internal Memory Data Objects, and finally a summary of the findings. Generally, the outcome of the analysis showed similar test results but the difficulty was in installing and configuring some of these tools. There is also a greater need for mobile forensics tools that respond to a more connected world where data is not contained in one device.

**Implementation of the Proposed Process Based Framework:** It was identified that there was a need to take the proposed framework (PBFMF) and apply it to an actual case, where two different
mobile forensic scenarios were investigated and the PBFMF was applied to each case. In addition, a comparison of two other existing mobile forensic frameworks were made in order to review the strengths and weaknesses of each and compare both to PBFMF. This research has identified that the majority of the existing frameworks are specific to one type of device, where the PBFMF has the benefit of being neutral and device agnostic. Results have shown that the PBFMF provides a step by step process and framework for an examiner to follow, and this framework is viable and a robust process that the industry not only can use, but also needs.

**Operating Systems Comparison Table:** The table was created to provide a comparison of the different operating systems (see Table 3-1). In this table, information was provided about some of the most popular mobile phone operating systems, where information regarding different models of phone can be found.

**Mobile Device Tool Specifications Table:** This research benefited from the methodology developed by NIST to establish combined specific and common rules to govern tool specifications for testing computer forensic software tools and to determine if a tool can accurately acquire specific data objects populated onto the device or SIM. The table consisted of two major requirements; the Mobile Device Tool-Core Requirement (MDT-CR) or/and the Smart Phone Tool-Core Requirement (SPT-CR), where the tested tool must be capable of carrying out the mentioned task; and the Mobile Device Tool-Requirement Optional (MDT-RO) or/and the Smart Phone Tool-Core Requirement (SPT-RO), which is only applicable if a tool provides the capability defined after it has been tested for conformance to these optional requirements (see Appendix C).

**Framework Procedures:** Procedures representation of the PBFMF was also provided based on the research and analysis presented in this chapter. The procedures were developed and presented in an abstraction layer so software developers of mobile forensic tools could create software that will adhere to the PBFMF (see Appendix D).

### 7.2 Future Research Work

This thesis proposes developing a new framework to unify mobile forensics investigations; the work presented here can be extended in the future to accommodate new and emerging technologies as well as address issues related to the mobile forensics tools currently being used in the market. Below is a direction of future work in which my present work could be extended:

**Web-based Unified Reporting:** Currently, mobile forensics tools utilize different output formats to generate their reports. Most of the reporting formats are proprietary and specific to the mobile forensics tools. We have proposed developing a web based website (Appendix B) where users could enter results generated by different mobile forensics tools and the web based site will translate these
reports into a common format to be used industry wide. Creating such a web based reporting repository will provide a unified way of examining results of mobile forensic investigations. It will also create a repository where the mobile forensics community could learn more about the trends of the investigations as well as help the research community forecast common threads and the future direction of the industry.

**IoT Framework Extension:** The future of the Internet will be based on IoT extensions. Technology has moved from the personal computer to an interconnected web of devices that manage every aspect of human interactions with each other and with appliances. The IoT technologies are currently in the process of revolutionizing the world and it will continue to become a cornerstone of everyday life. The mobile forensics framework proposed in this thesis will need to be expanded to accommodate IoT devices and to determine the chain of custody for connected storage (Appendix E). The framework will also need to extend and accommodate devices that might have not been thought of as being part of mobile forensics investigations.

**Better Mobile Forensics Tools Process:** As this thesis reports, there are many digital forensics tools that have been around for a few years. Some are more widely available than others. But as the research indicates, the process of installing, testing and using these tools has proven to be cumbersome. A great deal of time has been spent by this writer configuring these tools, working with their technical support documentation and web support. Unfortunately, some of the tools that were researched did not work as advertised. Others disappointed in areas where they should have excelled. The complexity of these tools creates many challenges for the forensics community. The lack of clear information on how to install and configure these tools will need to be further reviewed and analysed, and recommendations for the mobile forensics software community should be developed to help the industry be more mature and consistent when it comes to installing, configuring and testing these tools.

**Data Mining:** Data mining should be of great interest to mobile forensics investigators, as it will help provide visual representation of the data in addition of achieving efficiency in mobile forensics investigations. As the volume and frequency of incidents conducted by using mobile devices, a study in how data mining could improve mobile forensics analysis should be further studied. Data mining algorithms could be utilised to identify digital crime patterns [105] and cluster data in ways that could not only expedite the process of identifying crimes, but also enable the mobile forensics community to stay in step with the proliferation of mobile crimes. Data mining algorithms [106] could be used to develop models that investigators and mobile forensics tools could use to predict more accurately how mobile crimes are committed and provide greater insights into the process of committing mobile crimes. Data mining is an iterative process which means that as the mobile forensics community start using it on a regular basis, it will greatly help reduce the complexity of investigating an ever changing mobile world.
Bibliography


Appendix A: Test Results for Forensic Tools

A.1 Test Results for MobilEdit Analyst Forensics Tool

Tool Tested: MobilEdit - Analyst

Software Version: v8.5

Supplier: Compelson Labs

Address: COMPELSON Labs, Na Zertvach 34, 180 00, Prague 8, Czech Republic

Email: support@mobiledit.com


A.1.1 Results Summary

MobilEdit Analyst v8.5 is mobile forensic software for data acquisition from phones, smartphones and other mobile devices. For more information about the discussed tool, refer to MobilEdit Web Page [90]. The tool was tested for its ability to acquire active data from the internal memory of supported mobile devices. There were a number of challenges encountered when using the tool, which were as follow:

Connectivity:

- There were a number of challenges with connection; at the first attempt the tool failed to recognize the Samsung phones, this was despite downloading the drivers for the Android and the iPhone. It took numerous attempts to get the Android devices recognized. The devices had to be placed in Developer mode then the acquisition could take place. The acquisition was only for the logical data; the tool does not perform physical acquisitions of the phone. Eventually, acquisition was completed on both Samsung devices.

- With the iPhones, again there were connection problems. The iPhone 6 was recognized and the data was backed up from the phone. The iPhone4 was not recognized despite numerous attempts and manual download of the drivers. The cable had to be an official cable for the phone to be recognized; once the phone was recognized; all of the logical data was acquired successfully.

Equipment / Subscriber related data:

- All Subscriber related data (i.e., MSISDN) was acquired for all devices.
Personal Information Management (PIM) data:

- Contacts/address book entries were acquired for all devices.
- Calendar entries were acquired for all devices.
- Memo/Note entries were acquired for all devices.
- The call logs were empty.
- The file system was recovered on the iPhone 6, but not the iPhone 4. The iPhone 4 was the one that had been jailbroken, which may have prevented the access although a jail broken phone is usually the easier one to conduct an acquisition on. The tool installs an app on the phone, so that might have had something to do with it. A similar result was obtained with the rooted phone. The phone that was not rooted produced the file system, whereas the rooted phone did not successfully acquire the file system.

Internet Related Data:

- The phones had been cleared of bookmarks, but the bookmark folders were recovered.

Social Media Related Data:

- Social media related data was non-existent in the phones during logical data extraction.

Case File Data Protection:

- Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

GPS Related Data:

- GPS data i.e. longitude/latitude coordinates were not reported for any device.

### A.1.2 Mobile Devices

The following table lists the mobile devices used for testing MobilEdit – Analyst version 8.5.

<table>
<thead>
<tr>
<th>Make</th>
<th>Model</th>
<th>OS</th>
<th>Firmware</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iPhone</td>
<td>iPhone 4</td>
<td>Apple (jailbroken)</td>
<td>7.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td>Apple iPhone</td>
<td>iPhone 6</td>
<td>Apple</td>
<td>9.2.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Samsung</td>
<td>GT-S6812i</td>
<td>Android (Rooted)</td>
<td>4.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td>Samsung</td>
<td>SM-G316HU</td>
<td>Android</td>
<td>4.4.4</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table A-1. 1: Tested Mobile Devices used for Testing MobilEdit – Analyst version 8.5
A.1.3 Testing Environment

The tests were run on a Windows 10 laptop with 32 GB of RAM. This section describes the selected test execution environment, and the data objects populated onto the internal memory of mobile devices.

A.1.3.1 Execution Environment

MobilEdit Analyst version 8.5 was installed on Windows 10 version 1511.

A.1.3.2 Internal Memory Data Objects

MobilEdit Analyst version 8.5 was measured by analyzing logically acquired data from the internal memory of pre-populated mobile devices. An example of the Logical File information recovered from the iPhone4 is shown below in Figure A-1.1.

![Files - iPhone](image)

Figure A-1.1: An Image of the Logical File information Recovered from the iPhone4
Table A-1.2 defines the data objects and elements used for populating mobile devices provided the mobile device supports the data element.

<table>
<thead>
<tr>
<th>Data Objects</th>
<th>Data Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address Book Entries</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Regular Length</em></td>
</tr>
<tr>
<td></td>
<td><em>Maximum Length</em></td>
</tr>
<tr>
<td></td>
<td><em>Special Character</em></td>
</tr>
<tr>
<td></td>
<td><em>Blank Name</em></td>
</tr>
<tr>
<td></td>
<td><em>Regular Length, email</em></td>
</tr>
<tr>
<td></td>
<td><em>Regular Length, graphic</em></td>
</tr>
<tr>
<td></td>
<td><em>Regular Length, Address</em></td>
</tr>
<tr>
<td></td>
<td><em>Deleted Entry</em></td>
</tr>
<tr>
<td></td>
<td><em>Non-ASCll Entry</em></td>
</tr>
<tr>
<td><strong>PIM Data</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Datebook/Calendar</em></td>
</tr>
<tr>
<td></td>
<td><em>Regular Length</em></td>
</tr>
<tr>
<td></td>
<td><em>Memos</em></td>
</tr>
<tr>
<td></td>
<td><em>Maximum Length</em></td>
</tr>
<tr>
<td></td>
<td><em>Special Character</em></td>
</tr>
<tr>
<td></td>
<td><em>Blank Entry</em></td>
</tr>
<tr>
<td><strong>Call Logs</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Incoming</em></td>
</tr>
<tr>
<td></td>
<td><em>Outgoing</em></td>
</tr>
<tr>
<td></td>
<td><em>Missed</em></td>
</tr>
<tr>
<td><strong>Text Messages</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Incoming SMS - Read</em></td>
</tr>
<tr>
<td></td>
<td><em>Incoming SMS - Unread</em></td>
</tr>
<tr>
<td>Data Objects and Elements used for Populating Analysed Mobile Devices</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing SMS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming EMS - Read</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming EMS - Unread</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing EMS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Non-ASCII SMS/EMS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>MMS Messages</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming Audio</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming Graphic</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming Video</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing Audio</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing Graphic</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing Video</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Application Data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device Specific App Data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Stand-alone data files</strong></td>
<td></td>
</tr>
<tr>
<td><strong>None</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Graphic</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Internet Data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Visited Sites</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Bookmarks</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Location Data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>None</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Social Media Data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>None</strong></td>
<td></td>
</tr>
</tbody>
</table>

Table A-1. 2: Data Objects and Elements used for Populating Analysed Mobile Devices
A.1.4 Test Results

This section provides the test cases results reported by the tool. Sections A.1.4.1 – A.1.4.2 identify the mobile device operating system type (i.e., Android, iOS) used for testing MobilEdit Analyst v8.5. The Test Cases column (logical memory acquisition) in Table A-1.3 is comprised of two sub-columns that define a particular test category and individual sub-categories that are verified when acquiring the logical memory for supported operating systems within each test case. Each individual sub-category row shows results for each operating system tested. The results are as follows:

- **As Expected**: the mobile forensic application returned expected test results – the tool acquired and reported data from the mobile device successfully.
- **Partial**: the mobile forensic application returned some data from the mobile device.
- **Not As Expected**: the application failed to return expected test results – the tool did not acquire or report supported data from the mobile device successfully.
- **NA**: Not Applicable – the mobile forensic application is unable to perform the test or the tool does not provide support for the acquisition for a particular data element.

### A.1.4.1 Android Mobile Devices

All of the data from a logical view was accessed and acquired by the tool. The file systems were only acquired from the device that had not been rooted. The submitted devices had gone through a pseudo wipe which made the logical acquisition fairly easy. Having said that, despite the attempted wiping of the device, there were SMS messages as well as other artifacts discovered (two graphic images and one video). Of course this is only a logical acquisition, and a physical acquisition is more than likely expected to recover more data.

![Figure A-1. 2: Discovered Artifact of a Graphic Image of the Logical Acquisition](image)

### A.1.4.2 iOS Mobile Devices

Connecting to the iOS devices proved to be a big challenge; the acquisition required iTunes, and the version had to be the latest one or the connection would not identify the phone. It took numerous attempts to connect to the phone, and at one point the cable had to be changed to the official cable for the iPhone 4; without it, the connection would not work. The file system was acquired on the
iPhone 6 that had not been jailbroken, but on the jailbroken iPhone 4 the acquisition of the physical file system failed which is a result different than expected.

<table>
<thead>
<tr>
<th>MobilEdit version 8.5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test Cases – Logical Memory Acquisition</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Equipment/User Data</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>PIM Data</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Call Logs</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>SMS Messages</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>MMS Messages</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Stand-alone Files</strong></td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Application Data</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Internet Data</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Social Media Data</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Acquisition</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Case File Data</strong></td>
</tr>
<tr>
<td><strong>Protection</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Physical</strong></td>
</tr>
<tr>
<td><strong>Acquisition</strong></td>
</tr>
<tr>
<td><strong>Non-ASCII</strong></td>
</tr>
</tbody>
</table>

Table A-1. 3: MobilEdit Analyst v8.5 Findings of Android and iOS Mobile Devices
A.1.5 Tool Analysis Summary

The MobilEdit Analyst tool is adequate for e-discovery and other types of cases where the perpetrator does not have knowledge about hiding information etc., but without the capability of physical acquisition the tool is not as solid a choice for a forensics tool as some of the others on the market. In this case, the tool could not obtain a physical image of the jailbroken iPhone4 and the rooted Samsung GT-S6812i. Having said that, the tool provides data (not all the data) for all four phones, and that is above and beyond the other phone tools. As with any forensics solution, there is no perfect tool, and a blend of two or more tools is best.

Advantages:
  • Ease of acquisition once device is discovered.
  • Simple menu and easy to follow format.

Disadvantages:
  • Too difficult to recognize devices.
  • Has to maintain constant connection to the Internet.
    • Hopefully this is only a trial license requirement
  • Logical acquisitions only.
  • Did not discover as much as some of the other tools even with logical acquisition only.

When comparing findings of this report with those of NIST ones, the following were observed:
  • Similar results were experienced with respect to connectivity.
  • There was no problem experienced with acquisition of the phone device data.

The sample set for testing was much smaller and less diverse than the NIST report.
A.2 Test Results for Mobile Phone Examiner Plus Forensics Tool (MPE Plus)

Tool Tested: Mobile Phone Examiner Plus

Software Version: v5.6.0.8

Supplier: Access Data

Address: 588 West 400 South Suite 350, Lindon, UT 84042

Email: support@accessdata.com

www: http://www.accessdata.com

A.2.1 Results Summary

Mobile Phone Examiner Plus is a stand-alone mobile investigation solution that includes enhanced smart device acquisition and analysis capabilities. With a different approach to digital mobile forensics, MPE+ allows mobile forensics examiners to take control of the investigation by providing them with unique tools necessary to quickly collect, easily identify and effectively obtain the key data other solutions miss. MPE+ provides ANY organization with an integrated solution to address BOYD Risk, Big Data and Mobile Device Evidence, all in one tool. For more information about the discussed tool, refer to ACCESSDATA web page [91]. The tool was tested for its ability to acquire active data from the internal memory of supported mobile devices. There were a number of challenges encountered when using the tool. These and the results of the testing are as follow:

Connectivity:

- There were a number of challenges with connection, especially with the iPhone devices; no matter what measures were explored, the tool was not able to detect the iPhone devices. Research was conducted and numerous attempts were made without success on the iPhone. The tool has the best options and analysis, but no reviews could be obtained of the iPhone’s information while testing. The capability of physical examination was identified, so that was attempted, and the iPhones were recognized, but the tool continued to prompt for the phone’s password when there was not one, and as a result the physical extractions were not successful either.

- Acquisition was completed on both Samsung devices only, and therefore, the results that follow are for the Samsung (Android) devices only.

Equipment / Subscriber related data:

- All Subscriber related data (i.e., MSISDN) was acquired for the Samsung devices.
Personal Information Management (PIM) data:
- Contacts/address book entries were acquired for both Samsung devices.
- Calendar entries were acquired for both Samsung devices.
- Memo/Note entries were acquired for both Samsung devices.
- The call logs were empty
- The file system was recovered on the rooted phone, but not on the phone that had not been rooted.

Internet Related Data:
- The phones had been cleared of bookmarks, but the bookmark folders were recovered.

Social Media Related Data:
- Social media related data was non-existent in the phones during logical data extraction

Case File Data Protection:
- Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

GPS Related Data:
- GPS data i.e. longitude/latitude coordinates were not reported for any device.

A.2.2 Mobile Devices

The following table lists the mobile devices used for testing MPE Plus version 5.6.2.0

<table>
<thead>
<tr>
<th>Make</th>
<th>Model</th>
<th>OS</th>
<th>Firmware</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iPhone</td>
<td>iPhone 4</td>
<td>Applejailbroken</td>
<td>7.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td>Apple iPhone</td>
<td>iPhone 6</td>
<td>Apple</td>
<td>9.2.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Samsung</td>
<td>GT-S6812i</td>
<td>Android Rooted</td>
<td>4.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td>Samsung</td>
<td>SM-G316HU</td>
<td>Android</td>
<td>4.4.4</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table A-2. 1: Tested Mobile Devices used for Testing MPE Plus version 5.6.2.0
A.2.3 Testing Environment

The tests were run on a Windows 10 laptop with 32 GB of RAM. This section describes the selected test execution environment, and the data objects populated onto the internal memory of mobile devices.

A.2.3.1 Execution Environment

Mobile Phone Examiner Plus version 5.6.2.0 was installed on Windows 10 version 1511.

A.2.3.2 Internal Memory Data Objects

Mobile Phone Examiner Plus was measured by analyzing logically acquired data from the memory of sample phones. An example of the information recovered from the rooted Android is shown in the following image.

![Figure A-2.1: An Example of the Information Recovered from the Rooted Android](image-url)
Table A-2.2 defines the data objects and elements used for populating mobile devices provided that the mobile device supports the data element.

<table>
<thead>
<tr>
<th>Data Objects</th>
<th>Data Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book Entries</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Regular Length</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Maximum Length</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Special Character</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Blank Name</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Regular Length, email</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Regular Length, graphic</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Regular Length, Address</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Deleted Entry</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Non-ASCII Entry</strong></td>
</tr>
<tr>
<td>PIM Data</td>
<td></td>
</tr>
<tr>
<td>Datebook/Calendar</td>
<td><strong>Regular Length</strong></td>
</tr>
<tr>
<td>Memos</td>
<td><strong>Maximum Length</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Special Character</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Blank Entry</strong></td>
</tr>
<tr>
<td>Call Logs</td>
<td><strong>Incoming</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Outgoing</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Missed</strong></td>
</tr>
<tr>
<td>Text Messages</td>
<td><strong>Incoming SMS - Read</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Incoming SMS - Unread</strong></td>
</tr>
<tr>
<td>Category</td>
<td>Data Objects</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Outgoing SMS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming EMS - Read</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming EMS - Unread</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing EMS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Non-ASCII SMS/EMS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>MMS Messages</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming Audio</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming Graphic</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incoming Video</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing Audio</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing Graphic</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing Video</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Application Data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Device Specific App Data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Stand-alone data files</strong></td>
<td><strong>None</strong></td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Graphic</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Internet Data</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Visited Sites</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Bookmarks</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Location Data</strong></td>
<td><strong>None</strong></td>
</tr>
<tr>
<td><strong>Social Media Data</strong></td>
<td><strong>None</strong></td>
</tr>
</tbody>
</table>

Table A-2. 2: Data Objects and Elements used for Populating Analysed Mobile devices
A.2.4 Test Results

This section provides the test cases results reported by the tool. Sections A.2.4.1 – A.2.4.2 identify the mobile device operating system type (Android) used for testing MPE Plus v5.6.0.8.

The Test Cases column (logical memory acquisition) in Table A-2.3 is comprised of two sub-columns that define a particular test category and individual sub-categories that are verified when acquiring the logical memory for supported operating systems within each test case. Each individual sub-category row shows results for each operating system tested. The results are as follows:

- **As Expected**: the mobile forensic application returned expected test results – the tool acquired and reported data from the mobile device successfully.
- **Partial**: the mobile forensic application returned some data from the mobile device.
- **Not As Expected**: the application failed to return expected test results – the tool did not acquire or report supported data from the mobile device successfully.
- **NA**: Not Applicable – the mobile forensic application is unable to perform the test or the tool does not provide support for the acquisition for a particular data element.

A.2.4.1 Android Mobile Devices

All of the data from a logical view was accessed and acquired by the tool. The file systems were only acquired from the device that had been rooted. The submitted devices had gone through a pseudo wipe which made the logical acquisition fairly easy. Having said that, despite the attempted wiping of the device, there were SMS messages as well as other artifacts discovered as shown in the following image:

![Image of a graphic image of the logical acquisition](image.png)

**Figure A-2. 2: Discovered Artifact of a Graphic Image of the Logical Acquisition**

The rooted Android phone allowed for a physical acquisition, and this is when the tool excelled by carving out 664 images and files from the file system that was much more detailed than other tools. The only downside of this was the tool locked at 99.9% complete and did not provide the completion message ever.
A.2.4.2 iOS Mobile Devices

Despite numerous attempts and following the instructions and FAQs from the support site, the acquisition of the iOS devices was not possible; therefore, the results for the iOS are all N/A.

<table>
<thead>
<tr>
<th>Test Cases – Logical Memory Acquisition</th>
<th>Mobile Device Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td>Connectivity</td>
<td></td>
</tr>
<tr>
<td>Non Disrupted</td>
<td>As Expected</td>
</tr>
<tr>
<td>Disrupted</td>
<td>As Expected</td>
</tr>
<tr>
<td>Report</td>
<td></td>
</tr>
<tr>
<td>Preview-Pane</td>
<td>N/A</td>
</tr>
<tr>
<td>Generated Reports</td>
<td>As Expected</td>
</tr>
<tr>
<td>Equipment/Equipment/User Data</td>
<td></td>
</tr>
<tr>
<td>IMEI</td>
<td>As Expected</td>
</tr>
<tr>
<td>MEID/ESN</td>
<td>As Expected</td>
</tr>
<tr>
<td>MSISDN</td>
<td>As Expected</td>
</tr>
<tr>
<td>PIM Data</td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td>As Expected</td>
</tr>
<tr>
<td>Calendar</td>
<td>As Expected</td>
</tr>
<tr>
<td>To-Do List/ Tasks</td>
<td>As Expected</td>
</tr>
<tr>
<td>Memos</td>
<td>As Expected</td>
</tr>
<tr>
<td>Call Logs</td>
<td></td>
</tr>
<tr>
<td>Incoming</td>
<td>As Expected</td>
</tr>
<tr>
<td>Outgoing</td>
<td>As Expected</td>
</tr>
<tr>
<td>Missed</td>
<td>As Expected</td>
</tr>
<tr>
<td>SMS Messages</td>
<td></td>
</tr>
<tr>
<td>Incoming</td>
<td>As expected</td>
</tr>
<tr>
<td>Outgoing</td>
<td>As Expected</td>
</tr>
<tr>
<td>MMS Messages</td>
<td></td>
</tr>
<tr>
<td>Graphic</td>
<td>As Expected</td>
</tr>
<tr>
<td>Audio</td>
<td>As Expected</td>
</tr>
<tr>
<td>Category</td>
<td>Type</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Stand-alone Files</td>
<td>Video</td>
</tr>
<tr>
<td></td>
<td>Graphic</td>
</tr>
<tr>
<td></td>
<td>Audio</td>
</tr>
<tr>
<td></td>
<td>Video</td>
</tr>
<tr>
<td>Application Data</td>
<td>Documents</td>
</tr>
<tr>
<td></td>
<td>Spreadsheets</td>
</tr>
<tr>
<td></td>
<td>Presentations</td>
</tr>
<tr>
<td>Internet Data</td>
<td>Bookmarks</td>
</tr>
<tr>
<td></td>
<td>History</td>
</tr>
<tr>
<td>Social Media Data</td>
<td>Facebook</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
</tr>
<tr>
<td></td>
<td>LinkedIn</td>
</tr>
<tr>
<td>Acquisition</td>
<td>Acquire All</td>
</tr>
<tr>
<td></td>
<td>Selected All</td>
</tr>
<tr>
<td></td>
<td>Select Individual</td>
</tr>
<tr>
<td>Case File Data Protection</td>
<td>Modify Case Data</td>
</tr>
<tr>
<td>Physical Acquisition</td>
<td>Readability</td>
</tr>
<tr>
<td></td>
<td>Deleted File Recovery</td>
</tr>
<tr>
<td>Non-ASCII Character</td>
<td>Reported in native format</td>
</tr>
<tr>
<td>Hashing</td>
<td>Hashes reported for acquired data objects</td>
</tr>
<tr>
<td>GPS Data</td>
<td>Coordinates(Long/Lat)</td>
</tr>
</tbody>
</table>

Table A-2. 3: MPE Plus version 5.6.2.0 Findings of Android and iOS Mobile Devices
A.2.5 Tool Analysis Summary

The Mobile Phone Examiner Plus tool is adequate for examination of the Android based phones, and provided an adequate means to extract information for forensics analysis. The tool has provided data for only 2 of the 4 phones. However, the data extracted was above and beyond the other phone tools, especially when it came to the file carving capability from the physical file system. As with any forensics solution, there is no perfect tool, and a blend of two or more tools is best.

Advantages:

- Ease of acquisition of the Android devices, and extraction of the data for information analysis.
- Extraction and details of the device information was better and more than the other tools once the device was recognized.
- The file carving capability and results were exceptional.
- Simple menu and easy to follow format

Disadvantages:

- Too difficult to recognize devices, especially when it comes to the inability to gather information from the iOS phones
- Program stability seemed to be an issue, numerous crashes of the tool; seemed to work best on Windows 10.

When comparing findings of this report with those of NIST ones, the following were observed:

- The NIST report is from 2014.
- The NIST experience of not recovering subscriber data was not witnessed in this testing.
- There were no call logs missed with the data set of this testing as reported in the NIST testing.
- Application data was recovered in the testing but was not recovered in the NIST testing.

The testing from the NIST report was not indicative of what was experienced in this testing.
A.3 Test Results for Autopsy Forensics Tool

Tool Tested: Autopsy
Software Version: v4.0
Supplier: Basis Technology
Address: One Alewife Center, Cambridge, MA 02140-2323
Email: info@basistech.com
www: http://www.basistech.com

A.3.1 Results Summary

“Autopsy v4.0 is the premier end-to-end open source digital forensics platform. Built by Basis Technology with the core features of a commercial forensic tools, Autopsy is a fast, thorough, and efficient hard drive investigation solution that evolves with your needs”. For more information about the discussed tool, refer to Basistech web page [92]. The tool was tested for its ability to acquire active data from the physical file system of the device. There were a number of challenges encountered when using the tool. These challenges along with the results of the testing are as follow:

Connectivity:

- The Autopsy tool does not acquire the data from the phone, but instead it requires a phone image to be added to it.
- Acquisition of the physical file system from the MobilEdit tool was used as the data source for the Autopsy tool. An indication of the tool dashboard after adding the data source is shown in the following image.
- Unfortunately, only the data for the rooted Android phone was successfully added as a data source. Numerous attempts to add another phone’s physical image were not successful.

Equipment / Subscriber related data:

- All Subscriber related data (i.e., MSISDN) was acquired for the rooted Samsung device.

Personal Information Management (PIM) data:

- Contacts/address book entries were acquired for the rooted Samsung device.
- Calendar entries were acquired for the rooted Samsung device.
- Memo/Note entries were acquired for the rooted Samsung device.
- The call logs were empty.
- The file system was recovered on the rooted phone only.
Internet Related Data:

- The phone had been cleared of bookmarks, but the bookmark folders were recovered.

Social Media Related Data:

- Social media related data was non-existent in the phone.

Case File Data Protection:

- Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

GPS Related Data:

- GPS data i.e. longitude/latitude coordinates were not reported for the device.

### A.3.2 Mobile Devices

The following table lists the mobile devices used for testing Autopsy version 4.0

<table>
<thead>
<tr>
<th>Make</th>
<th>Model</th>
<th>OS</th>
<th>Firmware</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iPhone</td>
<td>iPhone 4</td>
<td>Apple</td>
<td>7.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>jailbroken</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple iPhone</td>
<td>iPhone 6</td>
<td>Apple</td>
<td>9.2.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Samsung</td>
<td>GT-S6812i</td>
<td>Android</td>
<td>4.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rooted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samsung</td>
<td>SM-G316HU</td>
<td>Android</td>
<td>4.4.4</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*Table A-3. 1: Tested Mobile Devices used for Testing Autopsy version 4.0*

### A.3.3 Testing Environment

The tests were run on a Windows 10 laptop with 32 GB of RAM. This section describes the selected test execution environment, and the data objects populated from the physical image of the mobile devices.

#### A.3.3.1 Execution Environment

Autopsy version 4.0 was installed on Windows 10 version 1511.

#### A.3.3.2 Internal Physical Memory Data Objects

Autopsy was measured by analyzing file system acquired data from the memory of sample phones.
An example of the email information recovered from the rooted Android is shown in the following image:

![Image of the Email Information Recovered from the Rooted Android](image1.png)

**Figure A-3. 1: An Image of the Email Information Recovered from the Rooted Android**

Since Autopsy has a feature, where it uses the results to determine if the extension has been tampered with and/or possibly trying to hide, which other tools did not have [107]. The Autopsy tool was able to discover file system extension mismatch, and this was not possible with any other tool. The tool was also able to discover a number of email addresses, and the results were in more detail than with other tools. An example of this is shown in the following image.

![Table of Email Addresses](image2.png)

**Figure A-3. 2: An Example of Emails Discovered by Autopsy**
Table A-3.2 defines the data objects and elements used for populating mobile devices provided that the mobile device supports the data element.

<table>
<thead>
<tr>
<th>Data Objects</th>
<th>Data Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book Entries</td>
<td></td>
</tr>
<tr>
<td>Regular Length</td>
<td></td>
</tr>
<tr>
<td>Maximum Length</td>
<td></td>
</tr>
<tr>
<td>Special Character</td>
<td></td>
</tr>
<tr>
<td>Blank Name</td>
<td></td>
</tr>
<tr>
<td>Regular Length, email</td>
<td></td>
</tr>
<tr>
<td>Regular Length, graphic</td>
<td></td>
</tr>
<tr>
<td>Regular Length, Address</td>
<td></td>
</tr>
<tr>
<td>Deleted Entry</td>
<td></td>
</tr>
<tr>
<td>Datebook/Calendar</td>
<td>Regular Length</td>
</tr>
<tr>
<td>Memos</td>
<td>Maximum Length</td>
</tr>
<tr>
<td>Special Character</td>
<td></td>
</tr>
<tr>
<td>Blank Entry</td>
<td></td>
</tr>
<tr>
<td>Call Logs</td>
<td></td>
</tr>
<tr>
<td>Incoming</td>
<td></td>
</tr>
<tr>
<td>Outgoing</td>
<td></td>
</tr>
<tr>
<td>Missed</td>
<td></td>
</tr>
<tr>
<td>Text Messages</td>
<td></td>
</tr>
<tr>
<td>Incoming SMS - Read</td>
<td></td>
</tr>
<tr>
<td>Incoming SMS - Unread</td>
<td></td>
</tr>
<tr>
<td>Outgoing SMS</td>
<td></td>
</tr>
</tbody>
</table>
### Test Results for Autopsy Forensics Tool

This section provides the test cases results reported by the tool. Sections 3.4.1 – 3.4.2 identify the

<table>
<thead>
<tr>
<th>Table A-3. 2: Data Objects and Elements used for Populating Analysed Mobile Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming EMS</strong></td>
</tr>
<tr>
<td>- Read</td>
</tr>
<tr>
<td>- Unread</td>
</tr>
<tr>
<td><strong>Outgoing EMS</strong></td>
</tr>
<tr>
<td><strong>Non-ASCII SMS/EMS</strong></td>
</tr>
<tr>
<td><strong>MMS Messages</strong></td>
</tr>
<tr>
<td>- Audio</td>
</tr>
<tr>
<td><strong>Incoming Audio</strong></td>
</tr>
<tr>
<td><strong>Incoming Graphic</strong></td>
</tr>
<tr>
<td><strong>Incoming Video</strong></td>
</tr>
<tr>
<td><strong>Outgoing Audio</strong></td>
</tr>
<tr>
<td><strong>Outgoing Graphic</strong></td>
</tr>
<tr>
<td><strong>Outgoing Video</strong></td>
</tr>
<tr>
<td><strong>Application Data</strong></td>
</tr>
<tr>
<td><strong>Device Specific App Data</strong></td>
</tr>
<tr>
<td><strong>Stand-alone data files</strong></td>
</tr>
<tr>
<td>- None</td>
</tr>
<tr>
<td>- Audio</td>
</tr>
<tr>
<td>- Graphic</td>
</tr>
<tr>
<td>- Video</td>
</tr>
<tr>
<td><strong>Internet Data</strong></td>
</tr>
<tr>
<td><strong>Visited Sites</strong></td>
</tr>
<tr>
<td><strong>Bookmarks</strong></td>
</tr>
<tr>
<td><strong>Location Data</strong></td>
</tr>
<tr>
<td>- None</td>
</tr>
<tr>
<td><strong>Social Media Data</strong></td>
</tr>
<tr>
<td>- None</td>
</tr>
</tbody>
</table>

A.3.4 Test Results

This section provides the test cases results reported by the tool. Sections 3.4.1 – 3.4.2 identify the
mobile device operating system type (Rooted Android) used for testing Autopsy v4.0. The Test Cases column (physical memory acquisition) in Table A-3.3 is comprised of two sub-columns that define a particular test category and individual sub-categories that are verified when acquiring the physical memory (phone image) for supported operating systems within each test case. Each individual sub-category row shows results for each operating system tested. The results are as follows:

- **As Expected**: the mobile forensic application returned expected test results – the tool acquired and reported data from the mobile device successfully.
- **Partial**: the mobile forensic application returned some data from the mobile device.
- **Not As Expected**: the application failed to return expected test results – the tool did not acquire or report supported data from the mobile device successfully.
- **NA**: Not Applicable – the mobile forensic application is unable to perform the test or the tool does not provide support for the acquisition for a particular data element.

### A.3.4.1 Android Mobile Devices

The file system was only acquired from the device that had been rooted. The submitted devices had gone through a pseudo wipe which made the logical acquisition fairly easy. Having said that, despite the attempted wiping of the device there were a number of artifacts recovered from the physical image of the file system.

The Autopsy tool did a good job of taking the file system image and extracting the pertinent information; the capability of the tool is on par with those on the commercial side of the market.

### A.3.4.2 iOS Mobile Devices

Despite numerous attempts and following the instructions and FAQs from the support site, the acquisition of the iOS devices was not possible due to the inability to acquire the image; therefore, the results for the iOS are all N/A.

<table>
<thead>
<tr>
<th>Autopsy v 4.0</th>
<th>Mobile Device Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test Cases – Physical Acquisition</strong></td>
<td>Android (rooted)</td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
<td>Non Disrupted</td>
</tr>
<tr>
<td></td>
<td>Disrupted</td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td>Preview-Pane</td>
</tr>
</tbody>
</table>
### A.3 Test Results for Autopsy Forensics Tool

<table>
<thead>
<tr>
<th>Category</th>
<th>Generated Reports</th>
<th>IMEI</th>
<th>MEID/ESN</th>
<th>MSISDN</th>
<th>Contacts</th>
<th>Calendar</th>
<th>To-Do List/ Tasks</th>
<th>Memos</th>
<th>Incoming</th>
<th>Outgoing</th>
<th>Missed</th>
<th>Graphic</th>
<th>Audio</th>
<th>Video</th>
<th>Documents</th>
<th>Spreadsheets</th>
<th>Presentations</th>
<th>Bookmarks</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Equipment/ User Data</strong></td>
<td>Generated Reports</td>
<td>IMEI</td>
<td>MEID/ESN</td>
<td>MSISDN</td>
<td>Contacts</td>
<td>Calendar</td>
<td>To-Do List/ Tasks</td>
<td>Memos</td>
<td>Incoming</td>
<td>Outgoing</td>
<td>Missed</td>
<td>Graphic</td>
<td>Audio</td>
<td>Video</td>
<td>Documents</td>
<td>Spreadsheets</td>
<td>Presentations</td>
<td>Bookmarks</td>
<td>History</td>
</tr>
<tr>
<td><strong>Generated Reports</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>IMEI</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>MEID/ESN</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>MSISDN</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>PIM Data</strong></td>
<td>Generated Reports</td>
<td>IMEI</td>
<td>MEID/ESN</td>
<td>MSISDN</td>
<td>Contacts</td>
<td>Calendar</td>
<td>To-Do List/ Tasks</td>
<td>Memos</td>
<td>Incoming</td>
<td>Outgoing</td>
<td>Missed</td>
<td>Graphic</td>
<td>Audio</td>
<td>Video</td>
<td>Documents</td>
<td>Spreadsheets</td>
<td>Presentations</td>
<td>Bookmarks</td>
<td>History</td>
</tr>
<tr>
<td><strong>Contacts</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Calendar</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>To-Do List/ Tasks</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Memos</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Call Logs</strong></td>
<td>Generated Reports</td>
<td>IMEI</td>
<td>MEID/ESN</td>
<td>MSISDN</td>
<td>Contacts</td>
<td>Calendar</td>
<td>To-Do List/ Tasks</td>
<td>Memos</td>
<td>Incoming</td>
<td>Outgoing</td>
<td>Missed</td>
<td>Graphic</td>
<td>Audio</td>
<td>Video</td>
<td>Documents</td>
<td>Spreadsheets</td>
<td>Presentations</td>
<td>Bookmarks</td>
<td>History</td>
</tr>
<tr>
<td><strong>Incoming</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Outgoing</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Missed</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>SMS Messages</strong></td>
<td>Generated Reports</td>
<td>IMEI</td>
<td>MEID/ESN</td>
<td>MSISDN</td>
<td>Contacts</td>
<td>Calendar</td>
<td>To-Do List/ Tasks</td>
<td>Memos</td>
<td>Incoming</td>
<td>Outgoing</td>
<td>Missed</td>
<td>Graphic</td>
<td>Audio</td>
<td>Video</td>
<td>Documents</td>
<td>Spreadsheets</td>
<td>Presentations</td>
<td>Bookmarks</td>
<td>History</td>
</tr>
<tr>
<td><strong>Incoming</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Outgoing</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>MMS Messages</strong></td>
<td>Generated Reports</td>
<td>IMEI</td>
<td>MEID/ESN</td>
<td>MSISDN</td>
<td>Contacts</td>
<td>Calendar</td>
<td>To-Do List/ Tasks</td>
<td>Memos</td>
<td>Incoming</td>
<td>Outgoing</td>
<td>Missed</td>
<td>Graphic</td>
<td>Audio</td>
<td>Video</td>
<td>Documents</td>
<td>Spreadsheets</td>
<td>Presentations</td>
<td>Bookmarks</td>
<td>History</td>
</tr>
<tr>
<td><strong>Graphic</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Stand-alone Files</strong></td>
<td>Generated Reports</td>
<td>IMEI</td>
<td>MEID/ESN</td>
<td>MSISDN</td>
<td>Contacts</td>
<td>Calendar</td>
<td>To-Do List/ Tasks</td>
<td>Memos</td>
<td>Incoming</td>
<td>Outgoing</td>
<td>Missed</td>
<td>Graphic</td>
<td>Audio</td>
<td>Video</td>
<td>Documents</td>
<td>Spreadsheets</td>
<td>Presentations</td>
<td>Bookmarks</td>
<td>History</td>
</tr>
<tr>
<td><strong>Graphic</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Application Data</strong></td>
<td>Generated Reports</td>
<td>IMEI</td>
<td>MEID/ESN</td>
<td>MSISDN</td>
<td>Contacts</td>
<td>Calendar</td>
<td>To-Do List/ Tasks</td>
<td>Memos</td>
<td>Incoming</td>
<td>Outgoing</td>
<td>Missed</td>
<td>Graphic</td>
<td>Audio</td>
<td>Video</td>
<td>Documents</td>
<td>Spreadsheets</td>
<td>Presentations</td>
<td>Bookmarks</td>
<td>History</td>
</tr>
<tr>
<td><strong>Documents</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Spreadsheets</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Presentations</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>Internet Data</strong></td>
<td>Generated Reports</td>
<td>IMEI</td>
<td>MEID/ESN</td>
<td>MSISDN</td>
<td>Contacts</td>
<td>Calendar</td>
<td>To-Do List/ Tasks</td>
<td>Memos</td>
<td>Incoming</td>
<td>Outgoing</td>
<td>Missed</td>
<td>Graphic</td>
<td>Audio</td>
<td>Video</td>
<td>Documents</td>
<td>Spreadsheets</td>
<td>Presentations</td>
<td>Bookmarks</td>
<td>History</td>
</tr>
<tr>
<td><strong>Bookmarks</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td><strong>History</strong></td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
</tbody>
</table>
### A.3 Test Results for Autopsy Forensics Tool

#### A.3.5 Tool Analysis Summary

The Autopsy tool is more than adequate for examining the Android based phones that have been rooted and a physical image extracted. Having said that, the tool provided data for only 1 of the 4 phones due to the requirement for an image, but the data extracted was comparable to other tools, especially when it came to the file carving capability from the physical file system. As with any forensics solution, there is no perfect tool, and a blend of two or more tools is best.

Advantages:

- Open Source.
- Comprehensive dashboard.
- The file carving capability and results were exceptional.
- Simple menu and easy to follow format.
- Simple process of analysis.
- Simple installation, best of all the tools tested.

<table>
<thead>
<tr>
<th>Social Media Data</th>
<th>Facebook</th>
<th>As Expected</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter</td>
<td>As Expected</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>LinkedIn</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acquisition</th>
<th>Acquire All</th>
<th>Not as expected</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Selected All</td>
<td>Not as expected</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Select Individual</td>
<td>Not as expected</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case File Data Protection</th>
<th>Modify Case Data</th>
<th>As expected</th>
<th>As expected</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Physical Acquisition</th>
<th>Readability</th>
<th>N/A</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Deleted File Recovery</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-ASCII Character</th>
<th>Reported in native format</th>
<th>As expected</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Hashing</th>
<th>Hashes reported for acquired data objects</th>
<th>Not as expected</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>GPS Data</th>
<th>Coordinates(Long/Lat)</th>
<th>N/A</th>
<th>N/A</th>
</tr>
</thead>
</table>

Table A-3. 3: Autopsy version 4.0 Findings of Android and iOS Mobile Devices
Disadvantages:

- Requires the image of the file system.
- No capability to acquire a file system.
- The tool did not provide thumbnails of the carved files. This might be a setting, but it was not discovered during the testing.

Could not discover any reports for the Autopsy tool within the NIST list of reports for the purpose of comparing with this report.
A.4 Test Results for Device Seizure Trial Forensics Tool

Tool Tested: Device Seizure Trial

Software Version: v7.4

Supplier: Paraben

Address: 21690 Red Rum Drive Ste 137, Ashburn, VA 20147

Email: support@paraben.com

www: http://www.paraben.com

A.4.1 Results Summary

“Device Seizure v7.4 was the first mobile forensic tool on the market. Designed from the ground up for forensically sound examinations of cell phones and other devices, DS set the industry standard for mobile investigations”. For more information about the discussed tool, refer to Pareben’s web page [93]. The tool was tested for its ability to acquire active data from the internal memory of the phone device. There were a number of challenges encountered when using the tool. These challenges along with the results of the testing are as follow:

Connectivity:

- The Device Seizure tool loads its own drivers during the installation process; this is to assist with the detection of a phone when it is connected. The tool was able to detect the phones when connected, but depending on a number of factors, the tool could not provide the extraction of the information that was required for the testing. Despite this, the tool does have some excellent capabilities; but with the limitations and the restrictions on the trial version of the tool, it makes it difficult to evaluate the tool.

Equipment / Subscriber related data:

- All Subscriber related data (i.e., MSISDN) was acquired for all of the tested devices apart from the rooted Samsung GT-S6812i.

Personal Information Management (PIM) data:

- Contacts/address book entries were acquired for all of the tested devices apart from the rooted Samsung GT-S6812i.

Internet Related Data:

- The phone had been cleared of bookmarks, but the bookmark folders were recovered.
A4. Test Results for Device Seizure Trial Forensics Tool

Social Media Related Data:
- Social media related data was non-existent in the phone.

Case File Data Protection:
- Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

GPS Related Data:
- GPS data i.e. longitude/latitude coordinates were not reported for the device

A.4.2 Mobile Devices

The following table lists the mobile devices used for testing Device Seizure version 7.4

<table>
<thead>
<tr>
<th>Make</th>
<th>Model</th>
<th>OS</th>
<th>Firmware</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iPhone</td>
<td>iPhone 4</td>
<td>AppleJailbroken</td>
<td>7.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td>Apple iPhone</td>
<td>iPhone 6</td>
<td>Apple</td>
<td>9.2.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Samsung</td>
<td>GT-S6812i</td>
<td>AndroidRooted</td>
<td>4.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td>Samsung</td>
<td>SM-G316HU</td>
<td>Android</td>
<td>4.4.4</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table A-4. 1: Tested Mobile Devices used for Testing Device Seizure version 7.4

A.4.3 Testing Environment

The tests were run on a Windows 10 laptop with 32 GB of RAM. This section describes the selected test execution environment, and the data objects populated from the physical image from mobile devices.

A.4.3.1 Execution Environment

Device Seizure Trial version 7.4 was installed on Windows 10 version 1511.
A.4.3.2 Internal Physical Memory Data Objects

Device Seizure version 7.4 was measured by analyzing the contacts from all of the tested devices apart from the rooted Samsung GT-S6812i. This is because the Trial version limits the recovery to contacts only. This is shown in the following image:

Figure A-4. 1: An Example Showing that DSTrial Version Tool Recovers Contacts Only

Table A-4.2 defines the data objects and elements used for populating mobile devices provided that the mobile device supports the data element.

<table>
<thead>
<tr>
<th>Data Objects</th>
<th>Data Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book Entries</td>
<td></td>
</tr>
<tr>
<td>Regular Length</td>
<td></td>
</tr>
<tr>
<td>Maximum Length</td>
<td></td>
</tr>
<tr>
<td>Special Character</td>
<td></td>
</tr>
<tr>
<td>Blank Name</td>
<td></td>
</tr>
<tr>
<td>Regular Length, email</td>
<td></td>
</tr>
<tr>
<td>Regular Length, graphic</td>
<td></td>
</tr>
<tr>
<td>Regular Length, Address</td>
<td></td>
</tr>
<tr>
<td>Deleted Entry</td>
<td>Non-ASCII Entry</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>PIM Data</strong></td>
<td></td>
</tr>
<tr>
<td>Datebook/Calendar</td>
<td>Regular Length</td>
</tr>
<tr>
<td>Memos</td>
<td>Maximum Length</td>
</tr>
<tr>
<td></td>
<td>Special Character</td>
</tr>
<tr>
<td></td>
<td>Blank Entry</td>
</tr>
<tr>
<td><strong>Call Logs</strong></td>
<td></td>
</tr>
<tr>
<td>Incoming</td>
<td></td>
</tr>
<tr>
<td>Outgoing</td>
<td></td>
</tr>
<tr>
<td>Missed</td>
<td></td>
</tr>
<tr>
<td><strong>Text Messages</strong></td>
<td></td>
</tr>
<tr>
<td>Incoming SMS - Read</td>
<td></td>
</tr>
<tr>
<td>Incoming SMS - Unread</td>
<td></td>
</tr>
<tr>
<td>Outgoing SMS</td>
<td></td>
</tr>
<tr>
<td>Incoming EMS - Read</td>
<td></td>
</tr>
<tr>
<td>Incoming EMS - Unread</td>
<td></td>
</tr>
<tr>
<td>Outgoing EMS</td>
<td></td>
</tr>
<tr>
<td>Non-ASCII SMS/EMS</td>
<td></td>
</tr>
<tr>
<td><strong>MMS Messages</strong></td>
<td></td>
</tr>
<tr>
<td>Incoming Audio</td>
<td></td>
</tr>
<tr>
<td>Incoming Graphic</td>
<td></td>
</tr>
<tr>
<td>Incoming Video</td>
<td></td>
</tr>
<tr>
<td>Outgoing Audio</td>
<td></td>
</tr>
<tr>
<td>Outgoing Graphic</td>
<td></td>
</tr>
</tbody>
</table>
### A.4.4 Test Results

This section provides the test cases results reported by the tool. Sections A.4.4.1 – A.4.4.2 identify the mobile device operating system type (Android or iOS) used for testing Device Seizure v7.4. The Test Cases column (logical memory acquisition) in Table A-4.3 is comprised of two sub-columns that define a particular test category and individual sub-categories that are verified when acquiring the logical memory for supported operating systems within each test case. Each individual sub-category row shows results for each operating system tested. The results are as follows:

- **As Expected**: the mobile forensic application returned expected test results – the tool acquired and reported data from the mobile device successfully.
- **Partial**: the mobile forensic application returned some data from the mobile device.
- **Not As Expected**: the application failed to return expected test results – the tool did not acquire or report supported data from the mobile device successfully.
- **NA**: Not Applicable – the mobile forensic application is unable to perform the test or the tool does not provide support for the acquisition for a particular data element.

#### A.4.4.1 Android Mobile Devices

The Device Seizure tool successfully connected to 1 of the 2 Android devices, the connection and

<table>
<thead>
<tr>
<th>Application Data</th>
<th>Outgoing Video</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand-alone data files</td>
<td>None</td>
</tr>
<tr>
<td>Internet Data</td>
<td>Visited Sites</td>
</tr>
<tr>
<td>Location Data</td>
<td>None</td>
</tr>
<tr>
<td>Social Media Data</td>
<td>None</td>
</tr>
</tbody>
</table>

Table A-4.2: Data Objects and Elements used for Populating Analysed Mobile Devices
acquisition failed on the device that was rooted “the Samsung GT-S6812i”. An example of this and information that was extracted is shown in the following image:

![Failed Connection Image](image_url)

**Figure A-4.2: An Image of Failed Connection on Rooted Samsung by Device Seizure**

As the previous image indicates there is an error message for a connection error, but that is not the actual cause. The phone is connected through the OS, but Device Seizure does not connect to it despite seeing it. The Device Seizure tool did not do a good job of extracting information from the Android devices.

### A.4.4.2 iOS Mobile Devices

Device Seizure did not experience any problems with the iPhone devices. Each device was recognized, and the information gathered and then a report generated. The process was much smoother than the one with Android devices.

<table>
<thead>
<tr>
<th>Device Seizure v7.4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test Cases – Logical Memory Acquisition</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Equipment/ User Data</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Test Results for Device Seizure Trial Forensics Tool

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>As Expected</th>
<th>As Expected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PIM Data</strong></td>
<td>Contacts</td>
<td>As Expected</td>
<td>As Expected</td>
</tr>
<tr>
<td></td>
<td>Calendar</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>To-Do List/ Tasks</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Memos</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Call Logs</strong></td>
<td>Incoming</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Outgoing</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Missed</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>SMS Messages</strong></td>
<td>Incoming</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Outgoing</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>MMS Messages</strong></td>
<td>Graphic</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Audio</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Video</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Stand-alone Files</strong></td>
<td>Graphic</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Audio</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Video</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Application Data</strong></td>
<td>Documents</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Spreadsheets</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Presentations</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Internet Data</strong></td>
<td>Bookmarks</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>History</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Social Media Data</strong></td>
<td>Facebook</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>LinkedIn</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Table A-4. 3: Device Seizure version 7.4 Findings of Android and iOS Mobile Devices

<table>
<thead>
<tr>
<th>Acquisition</th>
<th>Acquire All</th>
<th>Not as expected</th>
<th>As Expected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Selected All</td>
<td>Not as expected</td>
<td>As Expected</td>
</tr>
<tr>
<td></td>
<td>Select Individual</td>
<td>Not as expected</td>
<td>As Expected</td>
</tr>
<tr>
<td>Case File Data Protection</td>
<td>Modify Case Data</td>
<td>As expected</td>
<td>As expected</td>
</tr>
<tr>
<td>Physical Acquisition</td>
<td>Readability</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Deleted File Recovery</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Non-ASCII Character</td>
<td>Reported in native format</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Hashing</td>
<td>Hashes reported for acquired data objects</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>GPS Data</td>
<td>Coordinates(Long/Lat)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### A.4.5 Tool Analysis Summary

The Device Seizure tool is disappointing when it came to anything other than the iPhones. The extreme restrictions and limitations of the Trial version make the tool virtually impossible to evaluate. This is a concern, because without being able to evaluate it, there is no way you could recommend a purchase of it. The Device Seizure product was one of the first mobile forensics tools on the market, and to see the limited functionality of the tool is disheartening. Maybe if the tool is purchased it will be much better, but without being able to test it properly, it would be difficult to justify a purchase of the tool. As with any forensics solution, there is no perfect tool, and a blend of two or more tools is best.

**Advantages:**
- Works well with the iOS devices.
- Comprehensive dashboard.
- Simple menu and easy to follow format.
- Simple process of analysis.

**Disadvantages:**
- Restrictions on the trial version.
- Inability to recognize one of the Android phones.
- Loads a large amount of drivers that requires a large amount of disk space.
When comparing findings of this report with those of NIST ones, the following were observed:

- The testing was limited by having the trial version.
- Results for the data acquisition were consistent with the NIST results.
- Subscriber related data was recovered for the Android device, and like NIST not consistent across all devices.
- Concur with the problems of the recovery of the iPhone data.

Despite the difference in the versions and the time of the testing, the NIST results are similar to those of this testing, with Device Seizure being disappointing when it comes to mobile phone forensics.
A.5 Test Results for NowSecure Community Edition Forensics Tool

Tool Tested: NowSecure Community Edition

Software Version: v 3.2

Supplier: NowSecure

Address: 1046 Lake St, Oak Park, IL 60301

Email: support@nowsecure.com

www: http://www.nowsecure.com

A.5.1 Results Summary

The NowSecure Community Edition v 3.2 allows the user to complete filesystem, backup, and logical extractions, root Android devices, recover SMS messages, contacts, call logs, and more. For more information about the discussed tool, refer to NowSecure web page [94]. The tool was tested for its ability to acquire active data from the internal memory of the supported mobile devices. There were a number of challenges encountered when using the tool. These challenges along with the results of the testing are as follow:

Connectivity:

- The NowSecure Community Edition v 3.2 tool did an exceptional job with the Android devices, but only had limited success with the iPhone devices. This can be attributed to the fact that the tool is a trial version; its capability of acquiring data from iPhone devices would have been much better if it was a purchased one.

Equipment / Subscriber related data:

- All Subscriber related data (i.e., MSISDN) was acquired for all of the tested devices apart from the iPhone 6 (full version was required for the jailbroken iPhone 4).

Personal Information Management (PIM) data:

- Contacts/address book entries were acquired for all of the tested devices apart from the iPhone 6.

Internet Related Data:

- The phone had been cleared of bookmarks, but the bookmark folders were recovered for all of the tested devices apart from the iPhone 6.

Social Media Related Data:

- Social media related data was non-existent in the phone.
Case File Data Protection:

- Any attempts to leave an area where data had been collected received a warning to the analyst to save the data from the acquisition or it would be lost.

GPS Related Data:

- GPS data i.e. longitude/latitude coordinates were not reported for the device.

A.5.2 Mobile Devices

The following table lists the mobile devices used for testing NowSecure Community Edition v3.2.

<table>
<thead>
<tr>
<th>Make</th>
<th>Model</th>
<th>OS</th>
<th>Firmware</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iPhone</td>
<td>iPhone 4</td>
<td>Apple (jailbroken)</td>
<td>7.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td>Apple iPhone</td>
<td>iPhone 6</td>
<td>Apple</td>
<td>9.2.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Samsung</td>
<td>GT-S6812i</td>
<td>Android (Rooted)</td>
<td>4.1.2</td>
<td>N/A</td>
</tr>
<tr>
<td>Samsung</td>
<td>SM-G316HU</td>
<td>Android</td>
<td>4.4.4</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table A-5.1: Tested Mobile Devices used for Testing NowSecure Community Edition v3.2

A.5.3 Testing Environment

The tests were run on a Windows 10 laptop with 32 GB of RAM. This section describes the selected test execution environment, and the data objects populated onto the internal memory of mobile devices.

A.5.3.1 Execution Environment

NowSecure Community Edition v3.2 was downloaded as a virtual machine that is installed within the Santoku software distribution. The virtual machine was installed on Windows 10 version 1511 within VMware Workstation 121.1.

A.5.3.2 Internal Physical Memory Data Objects

NowSecure Community Edition v3.2 was measured by analyzing the data from all of the tested devices apart from the iPhone 6. The results of this are shown in the following images:
Table A-5.2 defines the data objects and elements used for populating mobile devices provided the mobile device supports the data element.

<table>
<thead>
<tr>
<th>Data Objects</th>
<th>Data Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book Entries</td>
<td></td>
</tr>
</tbody>
</table>
### A.5 Test Results for NowSecure Community Edition Forensics Tool

<table>
<thead>
<tr>
<th>Test Category</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regular Length</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Maximum Length</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Special Character</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Blank Name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Regular Length, email</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Regular Length, graphic</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Regular Length, Address</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Deleted Entry</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Non-ASCII Entry</strong></td>
<td></td>
</tr>
<tr>
<td><strong>PIM Data</strong></td>
<td></td>
</tr>
<tr>
<td>Datebook/Calendar</td>
<td><strong>Regular Length</strong></td>
</tr>
<tr>
<td>Memos</td>
<td><strong>Maximum Length</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Special Character</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Blank Entry</strong></td>
</tr>
<tr>
<td><strong>Call Logs</strong></td>
<td></td>
</tr>
<tr>
<td>Incoming</td>
<td></td>
</tr>
<tr>
<td>Outgoing</td>
<td></td>
</tr>
<tr>
<td>Missed</td>
<td></td>
</tr>
<tr>
<td><strong>Text Messages</strong></td>
<td></td>
</tr>
<tr>
<td>Incoming SMS - Read</td>
<td></td>
</tr>
<tr>
<td>Incoming SMS - Unread</td>
<td></td>
</tr>
<tr>
<td>Outgoing SMS</td>
<td></td>
</tr>
<tr>
<td>Incoming EMS - Read</td>
<td></td>
</tr>
<tr>
<td>Incoming EMS - Unread</td>
<td></td>
</tr>
<tr>
<td>Outgoing EMS</td>
<td></td>
</tr>
</tbody>
</table>
Table A-5. 2: Data Objects and Elements used for Populating Analysed Mobile Devices

A.5.4 Test Results

This section provides the test cases results reported by the tool. Sections A.5.4.1 – A.5.4.2 identify the mobile device operating system type (i.e., Android, iOS) used for testing NowSecure Community Edition v 3.2.

The Test Cases column (logical memory acquisition) in Table A-5.3 is comprised of two sub-columns that define a particular test category and individual sub-categories that are verified when
acquiring the logical memory for supported operating systems within each test case. Each individual sub-category row shows results for each operating system tested. The results are as follows:

- **As Expected:** the mobile forensic application returned expected test results – the tool acquired and reported data from the mobile device successfully.
- **Partial:** the mobile forensic application returned some data from the mobile device.
- **Not As Expected:** the application failed to return expected test results – the tool did not acquire or report supported data from the mobile device successfully.
- **NA:** Not Applicable – the mobile forensic application is unable to perform the test or the tool does not provide support for the acquisition for a particular data element.

### A.5.4.1 Android Mobile Devices

The NowSecure Community Edition v 3.2 tool successfully connected to both of the Android devices. Once connected, the software performed a logical analysis of the data on the phones which resulted in the successful extraction of the data contained within the phones.

### A.5.4.2 iOS Mobile Devices

NowSecure Community Edition v3.2 was able to recognize one of the iPhone phones, but the limitations of the Community Edition resulted in the tool not extracting any information from the iPhone devices as it asked for the full version for the recognized jailbroken iPhone 4.

<table>
<thead>
<tr>
<th>NowSecure v3.2</th>
<th>Mobile Device Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Cases – Logical Memory Acquisition</td>
<td>Android</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Non Disrupted</td>
</tr>
<tr>
<td></td>
<td>Disrupted</td>
</tr>
<tr>
<td>Reporting</td>
<td>Preview-Pane</td>
</tr>
<tr>
<td></td>
<td>Generated Reports</td>
</tr>
<tr>
<td>Equipment/ User Data</td>
<td>IMEI</td>
</tr>
<tr>
<td></td>
<td>MEID/ESN</td>
</tr>
<tr>
<td></td>
<td>MSISDN</td>
</tr>
<tr>
<td>PIM Data</td>
<td>Contacts</td>
</tr>
<tr>
<td>Category</td>
<td>Subcategory</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Calendar</td>
<td></td>
</tr>
<tr>
<td>To-Do List/ Tasks</td>
<td></td>
</tr>
<tr>
<td>Memos</td>
<td></td>
</tr>
<tr>
<td>Call Logs</td>
<td></td>
</tr>
<tr>
<td>Incoming</td>
<td></td>
</tr>
<tr>
<td>Outgoing</td>
<td></td>
</tr>
<tr>
<td>Missed</td>
<td></td>
</tr>
<tr>
<td>SMS Messages</td>
<td></td>
</tr>
<tr>
<td>Incoming</td>
<td></td>
</tr>
<tr>
<td>Outgoing</td>
<td></td>
</tr>
<tr>
<td>MMS Messages</td>
<td></td>
</tr>
<tr>
<td>Graphic</td>
<td></td>
</tr>
<tr>
<td>Audio</td>
<td></td>
</tr>
<tr>
<td>Video</td>
<td></td>
</tr>
<tr>
<td>Stand-alone Files</td>
<td></td>
</tr>
<tr>
<td>Graphic</td>
<td></td>
</tr>
<tr>
<td>Audio</td>
<td></td>
</tr>
<tr>
<td>Video</td>
<td></td>
</tr>
<tr>
<td>Application Data</td>
<td></td>
</tr>
<tr>
<td>Documents</td>
<td></td>
</tr>
<tr>
<td>Spreadsheets</td>
<td></td>
</tr>
<tr>
<td>Presentations</td>
<td></td>
</tr>
<tr>
<td>Internet Data</td>
<td></td>
</tr>
<tr>
<td>Bookmarks</td>
<td></td>
</tr>
<tr>
<td>History</td>
<td></td>
</tr>
<tr>
<td>Social Media Data</td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
</tr>
<tr>
<td>LinkedIn</td>
<td></td>
</tr>
<tr>
<td>Acquisition</td>
<td></td>
</tr>
<tr>
<td>Acquire All</td>
<td></td>
</tr>
<tr>
<td>Selected All</td>
<td></td>
</tr>
</tbody>
</table>
A.5 Test Results for NowSecure Community Edition Forensics Tool

<table>
<thead>
<tr>
<th>Case File Data Protection</th>
<th>Select Individual</th>
<th>As Expected</th>
<th>As Expected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify Case Data</td>
<td></td>
<td>As expected</td>
<td>As expected</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Acquisition</th>
<th>Readability</th>
<th>N/A</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Deleted File Recovery</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

| Non-ASCII Character         | Reported in native format | N/A         | N/A         |

| Hashing                    | Hashes reported for acquired data objects | N/A         | N/A         |

| GPS Data                   | Coordinates(Long/Lat) | N/A         | N/A         |

Table A-5.3: NowSecure Findings of Android and iOS Mobile Devices

A.5.5 Tool Analysis Summary

The NowSecure Community Edition v3.2 tool did a very good job with the Android devices, but did not perform as expected with the iPhone devices. The information extracted with the tool was very good, and exceeded expectations for the most part.

Advantages:

- Works well with the Android devices.
- Instant recognition of the device once connected in the VM.
- Comprehensive dashboard.
- Simple menu and easy to follow format.
- Simple process of analysis.

Disadvantages:

- Restrictions on the Community version for iPhones.
- Inability to recognize one of the iOS phones.
- Inability to generate a report from the data without paying for a full version.
- No physical acquisitions of any device unless the tool’s version is a commercial one.

Could not discover any reports for the NowSecure Community Edition v3.2 tool within the NIST list of reports for the purpose of comparing with this report.
Appendix B: Framework Guidelines for Web-based Tool Development

One of the main difficulties with existing Mobile Forensic Tools is that the output or results of the tools vary by manufacture, version and, at times, the operating system being used. The information presented by these tools may excel in one area but lack in others. A consistent output across different tools is desirable to ensure that users are aware of all the possible risks associated with their investigation. Although Mobile Forensic Software provides adequate information for users, a new framework for displaying these results will greatly benefit the users of the software.

The new output framework can be accomplished by providing a mechanism for reports from the different Mobile Forensic Software to be inputted into a new web based tool which will translate these results into a common output format. The common output from the new tool will provide users a consistent way to viewing and assessing data. The framework will be developed based on existing information and complemented by the assessment of the industries need for a common and standard format to interpreting forensic data.

B.1 Mobile Forensics Framework Stages

As stated earlier, there are only a few set standards for computer forensics and no known set standards for mobile digital forensics that is based purely on the needs of the mobile forensics process. This makes it a necessity that a framework is created in order for proper guidelines to be established. In addition, this is justified as being a strong reason for the need for forensics tools capable of displaying all needed data and information from different devices. Thus, as can be seen in Figure B-1 below, the proposed methodology for creating a web based tool will consist of the proposed stages mentioned in chapter 7 for designing the process based framework, in addition to a few other stages such as data modelling and mining:

- **Data Preservation:** In this stage, it is essential that the data is preserved in a forensically sound manner. The steps outlined in section 7.5.1 must be followed during triage to ensure the proper handling of the device to be investigated. Data preservation includes steps for evaluating the scene, documenting the scene, identifying the state of the device being investigated, establishing chain of custody and transporting the device.
Appendix B: Framework Guidelines for Web-based Tool Development

- **Acquisition:** In this stage, a decision regarding the type of data acquisition will be made. Acquiring device data can either be a manual or a tool based process. Acquisition can also be on-site or off-site depending on the investigation needs. Off-site acquisition, in a digital forensics laboratory is most ideal since a lab environment will be equipped with the tools required according to certification and accreditation organizations.

- **Analysis:** In this stage, the data will be examined and the investigation will focus on identifying the different aspects of the data. Data analysis will be based on best practices and will be developed with platform independent concepts. Analytical software tools will be utilized to ensure the data is being analysed for specific categories.

- **Reporting:** The final stage of the Mobile Forensics Framework is to report the results of the analysis. The reporting should present both summary and detailed information of the steps taken and the results of the investigation. The reporting can be done by utilizing a common format to be specified by this project.

![Figure B- 1: Overview of the Proposed Framework Phases Representation](image-url)
B.2 Proposed Forensic Output Framework and Web Based Tool Model

In support of the proposed framework, there will be a need to develop a platform independent web-based tool that supports the preservation of evidence and/or chain of custody, regardless of the technology being used, which will ensure that the information gathered and presented in front of a court of law is accepted, and can be relied upon as a solid means of proving that something has or has not taken place.

The proposed tool for translating output into a common format will accept output and results from disparate software regardless of the operating system or the output type. The new tool will use an internally developed algorithm to determine the data being provided. The proposed tool will use XML technology to format the data in accordance with the new output framework. While Figure B-2 is the proposed forensic output of the framework and the tool model, Figure B-3 is an overview of the proposed model design and information flow.
Appendix B: Framework Guidelines for Web-based Tool Development

Figure B-2: Overview of the Proposed Forensics Output Framework and Tool Model

1. Users login to the newly created website, www.mobileforensicsanalysis.com

2. Users Upload their mobile forensics results files to the website

3. Results are stored in servers for analysis and data warehousing

4. Programming is applied to identify source of the data and to prepare for analysis

5. Analysis is applied and the results are processed using the new framework

6. Results are displayed in the website using XML. Results are used for trend analysis
Appendix B: Framework Guidelines for Web-based Tool Development

Figure B-3: Overview of the Proposed Model Design and Information Flow
As can be seen in Figure B-4, a website is to be developed (www.mobileforensicsanalysis.com) to accept data results from the Mobile Forensic Software and uploaded by users to determine the best way to process the data and display the results for users. The website will also provide users with a way to upload the results file (Figure B-5). The combination of the output framework and the web-based tool will provide users with a way to compare results in a consistent way.

Figure B-4: The Website, www.mobileforensicsanalysis.com, to import Programs Results

Figure B-5: The Website provides the User with a Way to upload the Results File
B.3 Design Goal

The goal for this design is to be:

- Conformative with common standards: The framework will focus on providing users with a standard way of thinking about common issues of forensic investigation.
- Platform independent: The tool will be platform independent and will accept data using common data formats such as comma delimited/.csv, .xml, .txt, spreadsheet, PDF and other common import standards.
- Open source: The tool will be built using open source standards and will be available for the open source community to enhance it over time.
- Simplified User Interface: The interface will utilize a simplified user interface design to allow for maximum usability and remove any complexity inherent in forensic tools.
- Recommended action: The tool’s Intelligent Investigation Algorithm (IIA) will analyse the data provided and make recommendations to provide users with potential recommendation for follow up or action plan.
- Research utility: Over time, the accumulated results will be utilized as a tool to provide tips on common mobile forensic issues and may be utilized as a research tool.

B.4 Design Requirements

The design requirements are discussed from both the framework and tool perspective

- Framework requirements
  - The framework will be divided into different sections based on the type of information categories presented.
  - The framework will be available for the mobile forensic community to review and recommend future updates and enhancements.
  - The framework should be simple and easy to understand.
  - The framework will be scalable.

- Tool Requirements
  - Tool design will be simple and user friendly.
  - The tool will provide an easy way for users to import/upload output results.
  - The imported results will be encrypted and secure.
  - Analyses of the output will be done in a short time frame.
  - Results will be presented in a modular way.
  - Users will be able to view all or sections of the results based on a combination of options on the web site.
Appendix B: Framework Guidelines for Web-based Tool Development

- Results will be aggregated to provide a summary section for future needs.

B.5 Design Assumptions

- Existing and future mobile forensic tools have data export functionality, as the export functionality is important for the proposed tool to perform its functions.
- Users of the proposed tool accept the terms of use for the proposed tool.
- Users are willing to upload the output results onto the proposed web site.
- Users of the website are willing to share high level results with other users.
- The framework will extend existing mobile forensic program result formats.

B.6 Summary

Overall, the process of installing, configuring, testing, and analysing mobile forensic tools was a time-consuming task and required much research and trial and error. However, the process was helpful in that it emphasized that the mobile forensics community should benefit from creating our proposed process based framework and the reporting web based tool. The conclusion is that developing a common framework for reporting and analysing data as well as providing a common web-based tool for users will help users regardless of the platform they use.
Appendix C: Mobile Device Tool Specifications Table

This Appendix benefited from the methodology developed by NIST to establish combined specific and common rules to govern tool specifications for testing computer forensic software tools and to determine if a tool can accurately acquire specific data objects populated onto the device or SIM. The table below consists of two major requirements; the Mobile Device Tool-Core Requirement (MDT-CR) and/or the Smart Phone Tool-Core Requirement (SPT-CR), where the tested tool must be capable of carrying out the mentioned task; and the Mobile Device Tool-Requirement Optional (MDT-RO) and/or the Smart Phone Tool-Core Requirement (SPT-RO), which is only applicable if a tool provides the capability defined after it has been tested for conformance to these optional requirements.

### C.1 Requirements for Core Features

Mobile Device Tool-Core Requirement (MDT-CR) means that the tested tool must be capable of carrying out the mentioned task. The same applies to Smart Phone Tool-Core Requirement (SPT-CR), where MDT replaces SPT and vice versa[108].

- **MDT-CR-01**: Forensic tool shall have the ability to recognize supported devices via the vendor-supported interfaces (e.g., cable, Bluetooth, Infrared).
- **SPT-CR-02**: Forensic tool shall have the ability to identify non-supported devices.
- **MDT-CR-03**: Forensic tool shall have the ability to notify the user of connectivity errors between the device and application during acquisition.
- **MDT-CR-04**: Forensic tool shall have the ability to provide the user with either a preview pane or generated report view of data acquired. (once acquisition is completed)
- **MDT-CR-05**: Forensic tool shall have the ability to logically acquire all application supported data objects present in internal memory without modifying the data objects present on the device, such as:
  - Subscriber-related information, equipment related information, address book entries, maximum length address book entries, address book entries containing special characters, address book entries containing blank names, email addresses associated with address book entries, graphics associated with address book entries, (datebook, calendar, note entries), (maximum length datebook, calendar, note entries), call logs (incoming/outgoing/missed), corresponding date/time
stamps and the duration of the call for call logs, ASCII text messages, MMS messages, Internet related data, ..etc.

- In addition to:
  - If a cellular forensic tool provides the user with an “Acquire All” device data objects acquisition option, then the tool shall complete the acquisition of all data objects without error.
  - If a cellular forensic tool provides the user with a “Select All” individual device data objects, then the tool shall complete the acquisition of all individually selected data objects without error.
  - If a cellular forensic tool provides the user with the ability to “Select Individual” device data objects for acquisition, then the tool shall acquire each exclusive data object without error.
  - If a cellular forensic tool completes two consecutive logical acquisitions of the target device without error, then the payload (data objects) on the mobile device shall remain consistent.

C.2 Requirements for Optional Features

Mobile Device Tool-Requirement Optional (MDT-RO); if a tool provides the capability defined, the tool is tested for conformance to these optional requirements. The same is applicable to Smart Phone Tool- Requirement Optional (SPT-RO), where MDT replaces SPT and UICC with SIM, and vice versa. The following optional features are identified:

UICC acquisition.

- MDT-RO-01: Forensic tool shall have the ability to recognize supported UICCs via the vendor supported interface (e.g., PC/SC reader, proprietary reader, internal).
- SPT-RO-02: Forensic tool shall have the ability to identify non-supported SIMs.
- MDT-RO-02: Forensic tool shall have the ability to notify the user of connectivity errors between the UICC reader and application during acquisition.
- MDT-RO-03: Forensic tool shall have the ability to acquire all application-supported data objects present in the UICC memory (presented in a useable format).
  - Such as Abbreviated Dialing Numbers (ADN), maximum length ADNs, ADNs containing special characters, Last Numbers Dialed (LND), ASCII SMS text messages, corresponding status (i.e., read, unread) for text messages, deleted text messages that have not been overwritten etc.
  - In addition to
    - If a forensic tool provides the user with an “Acquire All” SIM data objects acquisition option, then the tool shall complete the acquisition of all data objects without error.
Appendix C: Mobile Device Tool Specifications Table

- If a forensic tool provides the user with “Select All” individual SIM data objects, then it shall complete the acquisition of all selected data objects without error.
- If a cellular forensic tool provides the user with the ability to “Select Individual” SIM data objects for acquisition, then the tool shall acquire each exclusive data object without error.

Presentation.

- SPT-RO-05: Forensic tool shall have the ability to provide a presentation of acquired data in a human-readable format via a generated report.
- SPT-RO-06: Forensic tool shall have the ability to provide a presentation of acquired data in a human-readable format via a preview pane view.
- SPT-RO-07: Data Integrity: Forensic tool shall have the ability to protect previously acquired data objects within a saved case file from modification.
- SPT-RO-08: Password-protected UICCs: Forensic tool shall have the ability to provide the user with the ability to unlock a password protected UICC before acquisition.
- SPT-RO-09: PIN Attempts: Forensic tool shall have the ability to present the remaining number of CHV1/CHV2 PIN unlock attempts.
- SPT-RO-10: PUK Attempts: Forensic tool shall have the ability to present the remaining number of PUK unlock attempts.
- SPT-RO-11: Physical acquisition: Forensic tool shall have the ability to perform a physical acquisition of the device’s internal memory for supported devices.
  - In addition to acquisition of active and deleted address book entries, acquisition of active and deleted calendar, notes entries, call logs, SMS messages, EMS messages, audio files, graphic files, video files.
- SPT-RO-12: Non-ASCII character support: Forensic tool shall have the ability to present data objects containing non-ASCII characters acquired from the internal memory of the mobile device or UICC. Non-ASCII characters such as (address book entries/ADNs and text messages) shall be printed in their native representation.
- SPT-RO-13: Stand-alone Acquisition: Forensic tool shall have the ability to acquire internal memory data without modifying data present on the UICC.
- SPT-RO-14: Hashing: Forensic tool shall have the ability to compute a hash for individual data objects.
- SPT-RO-15: GPS Coordinates: Forensic tool shall have the ability to acquire GPS related data present in the internal memory.
### Appendix C: Mobile Device Tool Specifications Table

<table>
<thead>
<tr>
<th>ID</th>
<th>Test Assertion</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDT</td>
<td>If a mobile device/cellular forensic tool provides support for connectivity of the target device then the tool shall successfully recognize the target device via all tool-supported interfaces (e.g., cable, Bluetooth, IrDA).</td>
<td>Connect supported device via tool-supported interface(s); Acquire data.</td>
</tr>
<tr>
<td>CR-01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPT</td>
<td>If a cellular forensic tool attempts to connect to a non-supported device then the tool shall notify the user that the device is not supported.</td>
<td>Attempt acquisition of a non-supported device.</td>
</tr>
<tr>
<td>CR-02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDT</td>
<td>If connectivity between the mobile device and mobile device/cellular forensic tool is disrupted then the tool shall notify the user that connectivity has been disrupted.</td>
<td>Begin acquisition; Disconnect interface or interrupt connectivity during acquisition.</td>
</tr>
<tr>
<td>CR-03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDT</td>
<td>If a mobile device forensic tool completes acquisition of the target device without error then the tool shall have the ability to present acquired data objects in a useable format via either a preview-pane or generated report (once acquisition is completed).</td>
<td>Acquire device data; Review data for readability in a useable format.</td>
</tr>
<tr>
<td>CR-04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDT</td>
<td>If a mobile device forensic tool completes acquisition of the target device without error then all supported data elements shall be presented in a useable format.</td>
<td>Acquisition of tool supported data elements.</td>
</tr>
<tr>
<td>CR-05</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDT</td>
<td>If a mobile device/cellular forensic tool provides support for connectivity of the target SIM then the tool shall successfully recognize the target SIM via all tool-supported interfaces.</td>
<td>Connect UICC/SIM via tool supported interface(s); Acquire data.</td>
</tr>
<tr>
<td>RO-01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPT</td>
<td>If a cellular forensic tool attempts to connect to a non-supported SIM then the tool shall notify the user that the SIM is not supported.</td>
<td>Attempt acquisition of a non-supported SIM.</td>
</tr>
<tr>
<td>RO-02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDT</td>
<td>If a mobile device/cellular forensic tool loses connectivity with the SIM reader then the tool shall notify the user that connectivity has been disrupted.</td>
<td>Begin acquisition; Disconnect interface or interrupt connectivity during acquisition.</td>
</tr>
<tr>
<td>RO-03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDT</td>
<td>If a cellular forensic tool completes acquisition of the target SIM without error then the SPN shall be presented in a useable format.</td>
<td>Acquisition of SPN</td>
</tr>
<tr>
<td>RO-04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPT</td>
<td>If a cellular forensic tool completes acquisition of the target SIM without error then the ICCID shall be presented in a useable format.</td>
<td>Acquisition of ICCID</td>
</tr>
<tr>
<td>RO-05</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPT</td>
<td>If a cellular forensic tool completes acquisition of the target SIM without error then the IMSI shall be presented in a useable format.</td>
<td>Acquisition of IMSI</td>
</tr>
<tr>
<td>RO-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPT-RO-07</td>
<td>If the case file or individual data objects are modified via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification.</td>
<td>Alter case file; Attempt to reopen altered case file with application</td>
</tr>
<tr>
<td>SPT-RO-08</td>
<td>If the SIM is password-protected then the cellular forensic tool shall provide the examiner with the opportunity to input the PIN before acquisition.</td>
<td>Input correct SIM PIN; Acquire SIM</td>
</tr>
<tr>
<td>SPT-RO-09</td>
<td>If a cellular forensic tool provides the examiner with the remaining number of authentication attempts then the application should provide an accurate count of the remaining PIN attempts.</td>
<td>Input incorrect PIN; Check tool output for correct number of remaining PIN attempts</td>
</tr>
<tr>
<td>SPT-RO-10</td>
<td>If a cellular forensic tool provides the examiner with the remaining number of PUK attempts then the application should provide an accurate count of the remaining PUK attempts.</td>
<td>Input incorrect PUK; Check tool output for correct number of remaining PUK attempts</td>
</tr>
<tr>
<td>SPT-RO-11</td>
<td>If the cellular forensic tool supports a physical acquisition of the target device then the tool shall complete the acquisition without error.</td>
<td>Physical Acquisition; Data is presented in a useable format.</td>
</tr>
<tr>
<td>SPT-RO-12</td>
<td>If the cellular forensic tool supports display of non-ASCII characters then the application should present address book entries/ADNs in their native format.</td>
<td>Acquisition of address book entries/ADNs containing non-ASCII characters</td>
</tr>
<tr>
<td>SPT-RO-13</td>
<td>If the cellular forensic tool supports standalone acquisition of internal memory with the SIM present, then the contents of the SIM shall not be modified during internal memory acquisition.</td>
<td>Acquire data in Stand-alone acquisition mode; Check SIM status flags (e.g., Read, Unread) associated with text messages</td>
</tr>
<tr>
<td>SPT-RO-14</td>
<td>If the cellular forensic tool supports hashing for individual data objects then the tool shall present the user with a hash value for each supported data object.</td>
<td>Acquire data; Check known hash values for consistency</td>
</tr>
<tr>
<td>SPT-RO-15</td>
<td>If the cellular forensic tool supports acquisition of GPS data then the tool shall present the user with the longitude and latitude coordinates for all GPS-related data in a useable format.</td>
<td>Acquire data; Check GPS data for consistency</td>
</tr>
</tbody>
</table>

Table C-1: Mobile Device Tool Specification
Appendix D: Framework Procedures

Evaluate the Scene

START EVALUATION

DETERMINE METHOD TO BE USED

// assess crime scene

WHILE IN CRIME SCENE

IF scene is a hazard THEN

Is Hazard = Chemical?
Is Hazard = Physical?
Is Hazard = Other?

DO NOT ENTER SCENE

Report Scene to Authorities

END IF

// assess the type of device

IF Device is volatile THEN

Transport device to a lab as soon as possible

ELSE

Continue Scene Evaluation

END IF

// assess device contamination status

IF Device is immersed in liquid OR

IF Device is contaminated with blood OR

IF Device is contaminated with ..
THEN Device is contaminated

END IF

SEND device to a lab for further examination

CONTINUE to Documenting the Scene

METHOD

Method is determined

END EVALUATION
Appendix D: Framework Procedures

Documentation, State Identification and Network Removal

WHILE AT THE SCENE DO

If Document = Invoice OR
IF Document = Manual OR
IF Document = Other types of documents THEN
    Do not contaminate documents
    Document what is in the Scene
    Photograph the documents
END IF
IF Device is connected to other devices THEN
    Determine if other devices can be put in custody
END IF
// determine device state
IF Device State = OFF THEN
    LEAVE Device in OFF State
    IF device is NOT charged
        // disconnect the device from the network
        IF Faraday bag is available THEN
            Use Faraday bag to take device off network
        ELSE IF Cellular Network Isolation Card (CNIC) is available
            Use CNIC to take device off network
        ELSE
            Use any other method to take device off network
        END IF
    END IF
    Transport Device to a forensics facility
ELSE IF Device State = ON THEN

ELSE

END IF
// disconnect the device from the network

IF Faraday bag is available THEN
  Use Faraday bag to take device off network
ELSE IF Cellular Network Isolation Card (CNIC) is available
  Use CNIC to take device off network
ELSE
  Use any other method to take device off network
END IF

IF a Charger is connected to Device THEN
  Secure a Charger for the Device
  Transport Device to a forensics facility
ELSE Secure a Charger for the Device
  Transport Device to a forensics facility
END IF

END IF

// maintain the integrity of the device

IF acquisition is done at scene THEN
  Install a write blocker
END IF

END WHILE
Storage and Device Transportation

START

IF Device state = ON THEN

    DO NOT remove power

END IF

Locate Container

Place Device in Container

Seal the Container

Label the Container

Transport the Container

END
ACQUISITION PROCESS

START ACQUISITION

CASE

WHEN ACQUISITION = MANUAL THEN
  Document acquisition = Manual
  Dismantle mobile device
  Remove memory, if applicable
  If Photographing is available then
    Document utilizing Photographing
  Else if Video recording is available then
    Document utilizing video recorder
  Else
    Write and record data using paper
  End IF

WHEN ACQUISITION = AUTOMATED THEN
  Isolate the Device

  Secure the device and associated equipment for transport

  If Write Protection is not in set then
    Set write protection in device
  End

  If battery remaining is not adequate then
    Provide power to the device

  Photograph the screen of the device
Complete the evidentiary chain of custody.

Transport the device.

END

END ACQUISITION
ANALYSIS PROCESS

START ANALYSIS

CASE

WHEN ACQUISITION = MANUAL THEN

Perform analysis on Data available through the manual process

WHEN ACQUISITION = AUTOMATED THEN

IF Physical Acquisition = TRUE AND IF Logical Acquisition = TRUE THEN

Analyse Deleted data
Analyse GPS data
Analyse text logs
Analyse call logs
Analyse data from Apps
Analyse Photos
Analyse other relevant data

ELSE IF Physical Acquisition = FALSE AND IF Logical Acquisition = TRUE THEN

Analyse text logs
Analyse call logs
Analyse data from Apps
Analyse Photos
Analyse other relevant data

END IF

END

END ANALYSIS
REPORTING PROCESS

START REPORTING

Create **Report Findings** Section

Address case-specific requests from the investigator

Identify the scope of the examination

Provide a detailed description of the device

Detail examination information

List examiner name and date of exam

Create **Finding Details** Section

Specify files related to the request and the findings

Include

- String searches

- Keyword searches

- Text string searches

- Graphic image analysis.

- Web site traffic analysis

- Other Related analysis

Description of relevant programs on the examined items.

IF Techniques used to hide or mask data THEN

List encryption OR
Steganography OR

Hidden attributes OR

Hidden partitions OR

File name anomalies.

END IF

Create Conclusion Section

Write Summary Information

END REPORTING