2014

Up-dating investigation models for smart phone procedures

Brian Cusack
Auckland University of Technology

Raymond Lutui
Auckland University of Technology

DOI: 10.4225/75/57b3e1a3fb87c

12th Australian Digital Forensics Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

UP-DATING INVESTIGATION MODELS FOR SMART PHONE PROCEDURES

Brian Cusack, Raymond Lutui
Auckland University of Technology, Auckland, New Zealand
brian.cusack@aut.ac.nz, raymond.lutui@aut.ac.nz

Abstract

The convergence of services in Smart Technologies such as iPhones, Androids and multiple tablet work surfaces challenges the scope of any forensic investigation to include cloud environments, devices and service media. The analysis of current investigation guidelines suggests that each element in an investigation requires an independent procedure to assure the preservation of evidence. However we dispute this view and review the possibility of consolidating current investigation guidelines into a unified best practice guideline. This exploratory research proposes to fill a gap in digital forensic investigation knowledge for smart technologies used in business environments and to propose a better way to approach smart technology investigations.

Keywords
Investigation, Models, Smart Devices, Evidence, Preservation

INTRODUCTION

At present digital forensic investigators are faced with many different digital forensics investigation process models advocating best practices for extracting and preserving evidence. Smart technologies have created a problem where an investigator must apply many previously used models to collect and preserve digital evidence. The proliferation of investigation process models has arisen from the rapid and continuous innovation of devices, systems and applications for business use. Different proprietary designs, software, and access controls have influenced the adoption of digital forensic investigation models and the continuing revision of best practice. Individuals and businesses are very much dependent on computers, corporate networks, mobile devices and the Internet to conduct their daily tasks. The new generation of digital mobile devices are known as smart devices because of their processing power, memory and storage spaces are very similar to that of a desktop computer. These smart devices are capable of storing, transmitting and processing large amounts of private and confidential data (Owen & Thomas, 2011, p.25). Over the past decade, these smart devices have become a target for criminal and civil evidence gathering. As a result, it is very important that digital forensic investigators can complete their investigation effectively and efficiently within the constantly changing technological environment. In order for the investigators to achieve best practice goals the forensic investigation process models require constant updating and adapting to the new challenges. According to Tanner & Dampier (2009), digital forensic models are divided into three categories as Investigative models, Hypothesis models and Domain models (p.291).

Digital forensics comprises of various areas that relate to different technologies. There are four main areas and these are Computer forensics, Network forensics, Mobile forensics and Cloud forensics (Lin et al., 2011, p.387). Computer forensics is defined as the use of specialised techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction or computer usage, examination of residual data, authentication of data by technical analysis or explanation analysis of technical features of data and computer usage (Hankins et al., 2009, p.233). Network forensics on the other hand is defined as the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyse and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorised activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities (Palmer & Corporation, 2001, p.27). Mobile phone forensics is defined by the National Institutes of Standards and Technology as, the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods (Jansen & Ayers, 2007, p.6). Final type of digital forensic is known as Cloud forensics. Cloud forensic is defined as a mixture of traditional computer forensics, small-scale digital device forensics and network forensics. Therefore, Cloud forensics is the application of digital forensic science in the cloud computing environments (Ruan et al., 2013, p.38).

In the Appendix we list the assessed digital forensic investigation models that span an evolution from computer forensics in the 1990s until smart phone investigation models of 2012. These models form the basis of the analysis and we observe the different variations. The remainder of this paper is structured to review previous literature on digital forensic investigation models, potential problem areas, verification of the problem, an improved model and a discussion of its application.

PROBLEM AREAS

The convergence of computing and communications on mobile devices along with the application services and commercial services delivers an information rich environment for the user. The consequence is that much evidence is available but it is often stored in many locations and is in large quantities. Mobile smart devices have advanced functionalities with the ability to combine many functions onto one device such as, camera, video, Internet access, calendar, address book just to name a few. The devices are running on operating systems similar to a PC which allows users to install third party applications. Security and privacy protection became a major concern when business and private users' realised the amount of private information and data that these smart devices hold (Lin, et al., 2006, p.386). The smart devices have the ability to establish wireless connectivity and most of them also have the ability to utilise the cellular network. These devices also support multimedia applications and messaging services with GPS, gyroscopes, and accelerometers sensors built in. Smart devices advancement and growth in usages and popularity gives rise to very large data sets (Wang, et al., 2012, p.52; Leavitt, 2011, p.11). Also, the pervasiveness and ubiquitous nature of these smart devices increase the complexity of the situation for the forensic investigators (Bednar, et al., 2008, p.3). While business and private users embrace the mobility and advancements of these technologies, criminals also find other ways to utilise these devices to conduct illegal activities (Lin, et al., 2011, p.386; Dezfouli, et al., 2012, p.186). As a result, to deal with this emerging and growing new phenomenon, previous digital forensic investigation guidelines require revisiting and reviewing (Hankins, et al., 2009, p.230).

Most smart technology devices access cloud environments for the information services. Cloud computing has been defined in various ways for instance, Furht (2010, p.3) defined Cloud computing as, "a new style of computing in which dynamically scalable and often virtualized resources are provided as a services over the Internet". According to Mollah, et al. (2012, p1), Cloud computing is a, "TCP/IP based development and integration of computer technologies such as fast microprocessor, huge memory, high-speed network and reliable system architecture." The National Institute of Standards and Technology released their Special Publication 800-145 and defined Cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The cloud is said to be a network of data centres working together to provide powerful applications, platforms and services that can be accessed by its users over the Internet (Abhishek & Mahasweta, 2011, p.3). For investigation purposes a number of problems arise (Mell & Grance, 2011, p.2). Cloud computing has four various deployment models.

Private Cloud	Community Cloud	Public Cloud	Hybrid Cloud
This model refers to a cloud infrastructure that may be owned and operated by an organisation for private use only	This model refers to a cloud infrastructure that is owned, managed and used exclusively by a community with similar concerns such as security requirements, policies or mission	This model refers to an infrastructure that is open to the general public. This infrastructure may be owned and operated by an academic institution, government organisation or a business	This model refers to an infrastructure which is a combination of two or more of the other three models. This particular model allows the infrastructure to remain exclusive while they are bound by standards or branded technologies

Table 1. Cloud computing various deployment models (Mell & Grance, 2011, p.3).

Each structure has to be evaluated prior to investigation and the relevant evidence preservation assurances taken. In some instances the cloud presents insurmountable problems for evidence acquisition on account of the structures.

A third problem is the current divisions that are made regarding digital forensic areas of expertise (see figure 1). Each area of investigative expertise has evolved in keeping with technological developments and the systems developments. When any of the components of the illustrated digital forensic areas are involved in an investigation, the investigator needs to follow proper investigation procedure. These are scientifically proven techniques and methods to obtain and analyse digital evidence is such a way that publically accepted standards are complied. These standards are often written as professional guidelines and declared in the forensic report to substantiate admissibility. The adoption of a scientifically proven method to preserve, acquire, analyse, document evidences obtained from digital sources will help with the admissibility of the evidence in the court of law (Ademu, Imafidon & Preston, 2011, p.175). The identified problems for investigators in relation to smart technologies are the volumes of data involved, the distribution of that data in different systems, formats and jurisdictions and the constraints provided by different best practice guidelines.

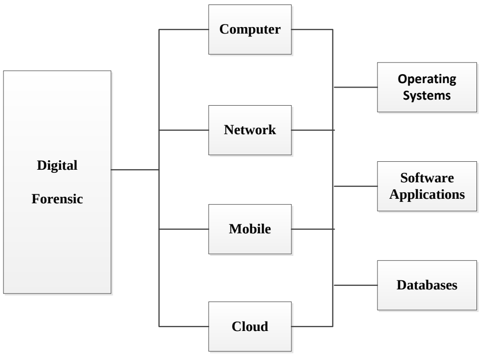


Figure 1. Digital forensic expertise divisions

PILOT STUDY VERIFICATION OF PROBLEMS

To prove that the problem areas located in the literature analysis exist in practice a pilot study was set up with an iPad and a case scenario. The pilot study was set up to confirm (or otherwise) the issues, problems and gap identified in the literature analysis for a smart device digital forensic investigation. The test bed in Figure 2 shows three different wireless accesses to three different types of wireless network environments. The test bed was set up to reflect a crime scene in which the criminal accesses a private company's information system via a business mobile smart device and exercises the following actions. Access the company's web server and defaces the company's website. Accessed the company's mail server and sent out fake e-mails to the company's suppliers and downloads the company's sensitive documents and uploads them in to a cloud account via wireless access from a cafeteria. The actions were executed using the iPad 4 with Wi-Fi and 3G capabilities.

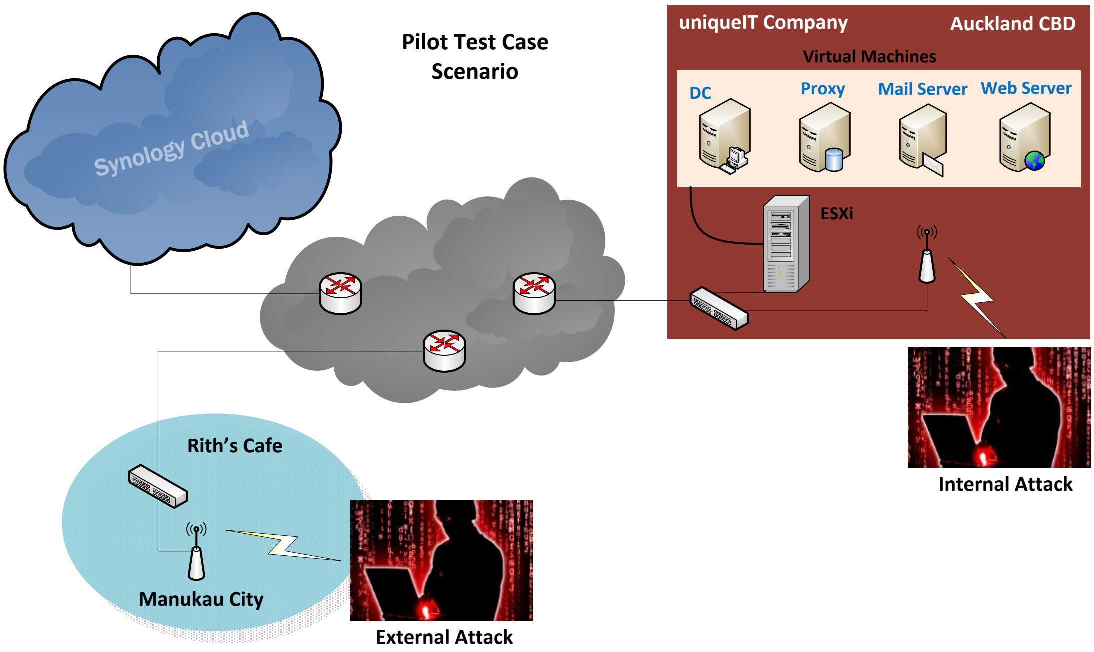
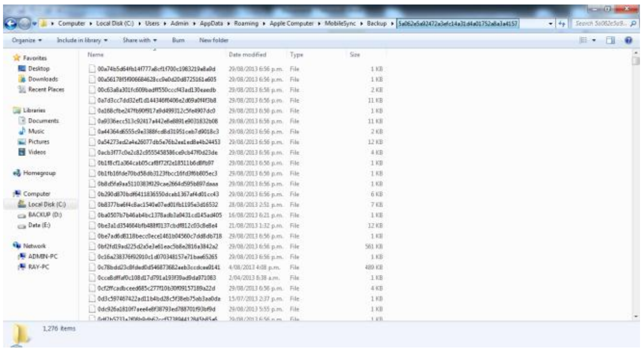


Figure 2. Test bed for the pilot study.

The machine that was employed during the forensic investigation process was running on a 64bit Microsoft Windows 7 Professional with service pack one. The computer also ran on Intel core i7-2600 processor with eight gigabytes of memory. To examine the iPad, a logical acquisition approach was the technique employed in this test case scenario. Logical acquisition is defined as a bit-by-bit copy of objects stored logically such as directories and files stored on a logical store of the device such as the file system partition (Jansen & Ayers, 2007, p.13). Three different tools were installed on the forensic computer. These were iTunes 11.0.5.5 which is a free backup utility provided by Apple that comes with the iPad 4. Since our pilot study utilises an Apple mobile device and also only required to take a logical acquisition of the device, we take advantage of the free logical backup utility (iTunes) provided by Apple (Bader & Baggili, 2010, p.1; Said, Yousif & Humaid, 2011, p.122). This was followed by an in-depth examination and analysis of the acquired backup copy. To analyse the acquired data, SQLite database browser was also employed to read the databases and the plistEditor Pro v2.1 was employed to read the .plist files (Bader & Baggili, 2010, p.1). Prior to acquiring data from the iPad, the automatic synchronisation feature of iTunes was disabled. The iPad was then connected to the computer through the USB cable. The data acquisition process was then initiated manually, once completed, the iPad was disconnected to avoid further unwanted processes from taking place. Data acquired from the iPad goes to the iTunes default backup location which is *C:\Users\Admin\AppData\Roaming\Apple Computer\MobileSync\Backup\*. The name of the folder containing the data extracted from the iPad is very long which is a combination of forty hexadecimal characters *"5a062e5a92472a3efc14a31d4a01752a8a3a4157"* representing the unique identifier of the iPad. The names of the acquired files also adopted the same naming convention which signifies the unique identifier for each data source obtained from the iPad (Bader & Baggili, 2010, p.7).



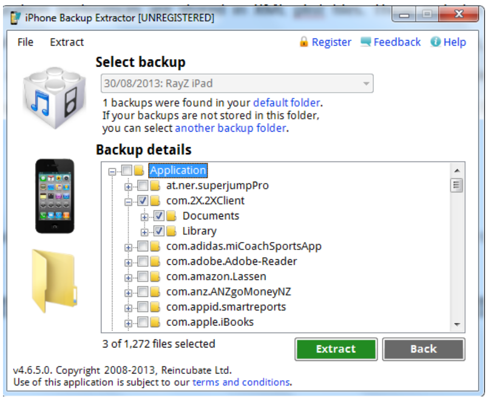
Computer ▸ Local Disk (C:) ▸ Users ▸ Admin ▸ AppData ▸ Roaming ▸ Apple Computer ▸ MobileSync ▸ Backup ▸ 5a062e5a92472a3efc14a31d4a01752a8a3a4157

Name	Date modified	Type	Size
00a74b5d64fb14f777a8cf1f700c1983219e8a9d	29/08/2013 6:56 p.m.	File	1 KB
00a56178f5f906684628cc9e0d20d8725161e605	29/08/2013 6:56 p.m.	File	1 KB
00c63a8a301fc609badff550ccc f43ad130eaedb	29/08/2013 6:56 p.m.	File	2 KB
0a7d3cc7dd32ef1d144346f6406e2d69a0f4f3b8	29/08/2013 6:56 p.m.	File	11 KB
0a168cfbe247fb90f917a9d499312c5fe4907dc0	29/08/2013 6:56 p.m.	File	1 KB
0a9336ecc513c92417a442e8e8891e9031832b08	29/08/2013 6:56 p.m.	File	11 KB
0a44364d6555c9e3388fcd8d31951ceb7d9018c3	29/08/2013 6:56 p.m.	File	2 KB
0a54273ed2a4e26077db5e76b2ea1ed8e4b24453	29/08/2013 6:56 p.m.	File	12 KB
0acb3f77c0e2c82c9555458586ce9cb47f0d23de	29/08/2013 6:56 p.m.	File	4 KB
0b1f8cf1a364cab05caf8f72f2e18511b6d8fb97	29/08/2013 6:56 p.m.	File	1 KB
0b1fb16fde70bd58db3123fbcc16fd3f6b805ec3	29/08/2013 6:56 p.m.	File	1 KB
0b8d5fa9aa5110383f029cae2664d595b897daaa	29/08/2013 6:56 p.m.	File	1 KB
0b290d870bdf6411836550dcab1367af4d01cc43	29/08/2013 6:56 p.m.	File	6 KB
0b8377be6f4c8ac1540e07ed01fb1195e3d16532	28/08/2013 2:51 p.m.	File	7 KB
0ba0507b7b46ab4bc1378adb3a9431cd145ad405	16/08/2013 6:21 p.m.	File	1 KB
0be3a1d354684bfb488f0137cbdf812c03c8e8e4	21/08/2013 1:32 p.m.	File	12 KB
0be7ad6d8118becc0ece1461b04560c7dd8db718	29/08/2013 6:56 p.m.	File	1 KB
0bf2fd19ad225d2a5e3e61eac5b8e2816a3842a2	29/08/2013 6:56 p.m.	File	561 KB
0c16a238376f92910c1d070348157e71bae65265	29/08/2013 6:56 p.m.	File	1 KB
0c78bdd23c8fded0d546873682aeb3ccdcea0141	4/08/2013 4:08 p.m.	File	489 KB
0cce8dffaf0c108d17d791a193f39ad9da971083	2/04/2013 8:38 a.m.	File	1 KB
0cf2ffcadbceed685c277f10b30f09157189a22d	29/08/2013 6:56 p.m.	File	4 KB
0d3c597467422ad11b4bd28c5f38eb75ab3aa0da	15/07/2013 2:37 p.m.	File	1 KB
0dc926a1810f7aee4e8f38793ed788701f93bf9d	29/08/2013 5:55 p.m.	File	1 KB
0df2b5233a2f08b9db62ccf57389441284 5b85a6	29/08/2013 6:56 p.m.	File	1 KB

1,276 items

Figure 3. Data acquired from the iPad.

The extracted data showed in Figure 3 came in three different file formats; the plist file, mddata files and the mdinfo files. The plist files are Apple's property list file format which stores data in plaintext and can be read using plist editor software. The mddata files stores data in raw binary format while the mdinfo file contains encoded metadata for the corresponding binary mddata files. In general, the iPad operating system (iOS) stores data in binary list and database files. Other information such as the device's status, application settings and user's configuration preferences are stored in XML plist files. These includes time zone, pairing records with devices and computer, email accounts, network identification, browser history, cookies and bookmarks. Information such as text messages, email messages, contacts list, call logs, notes, calendar are stored in SQLite database files. However, to read the binary files, a parsing tool called "iPhone Backup Extractor" is used (Bader & Baggili, 2010, p.7). Various tools and techniques are applied and the iPhone backup extractor was the analysis tool that is employed to read the extracted binary files into a readable format as it shows in Figure 4.



Select backup

30/08/2013: RayZ iPad

1 backups were found in your default folder.
If your backups are not stored in this folder,
you can select another backup folder.

Backup details

- □ Application
  - □ at.ner.superjumpPro
  - ☑ com.2X.2XClient
    - ☑ Documents
    - ☑ Library
  - □ com.adidas.miCoachSportsApp
  - □ com.adobe.Adobe-Reader
  - □ com.amazon.Lassen
  - □ com.anz.ANZgoMoneyNZ
  - □ com.appid.smartreports
  - □ com.apple.iBooks

3 of 1,272 files selected

v4.6.5.0. Copyright 2008-2013, Reincubate Ltd.
Use of this application is subject to our terms and conditions.

Figure 4. The iPhone Backup Extractor.

During the test, an application called 2xClient was used to access the private network from the iPad. The record was located in a folder named *"com.2X.2XClient"* as it showed in Figure 5.

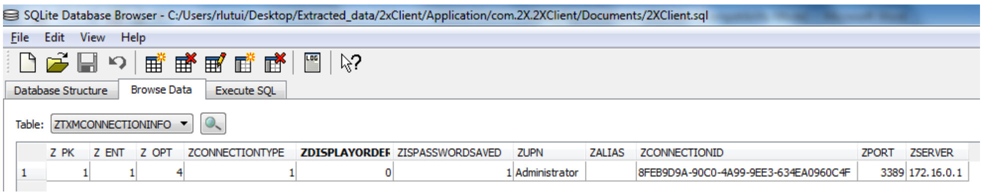
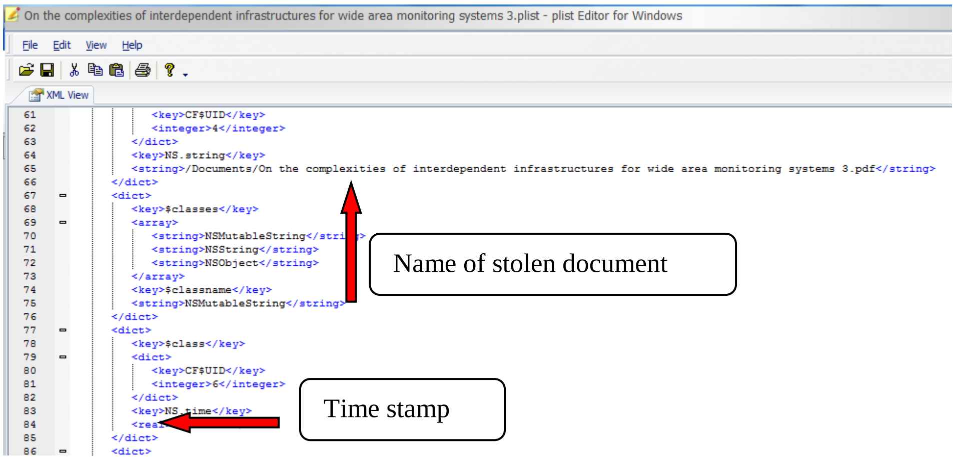

SQLite Database Browser - C:/Users/rlutui/Desktop/Extracted_data/2xClient/Application/com.2X.2XClient/Documents/2XClient.sql
File
Edit
View
Help
Database Structure
Browse Data
Execute SQL

Table: ZTXMCONNECTIONINFO

	Z PK	Z ENT	Z OPT	ZCONNECTIONTYPE	ZDISPLAYORDEF	ZISPASSWORDSAVED	ZUPN	ZALIAS	ZCONNECTIONID	ZPORT	ZSERVER
1	1	1	4	1	0	1	Administrator		8FEB9D9A-90C0-4A99-9EE3-634EA0960C4F	3389	172.16.0.1

Figure 5. 2xClient SQLite file.

Figure 6 shows that the connection record, stores the username used (Administrator), the connection ID, the access port number and IP address of the server that the iPad accessed.


On the complexities of interdependent infrastructures for wide area monitoring systems 3.plist - plist Editor for Windows
File
Edit
View
Help
XML View

```
            <key>CF$UID</key>
            <integer>4</integer>
        </dict>
        <key>NS.string</key>
        <string>/Documents/On the complexities of interdependent infrastructures for wide area monitoring systems 3.pdf</string>
    </dict>
    <dict>
        <key>$classes</key>
        <array>
            <string>NSMutableString</stri  >
            <string>NSString</string>
            <string>NSObject</string>
        </array>
        <key>$classname</key>
        <string>NSMutableString</string>
    </dict>
    <dict>
        <key>$class</key>
        <dict>
            <key>CF$UID</key>
            <integer>6</integer>
        </dict>
        <key>NS.time</key>
        <rea
    </dict>
    <dict>
```

Name of stolen document

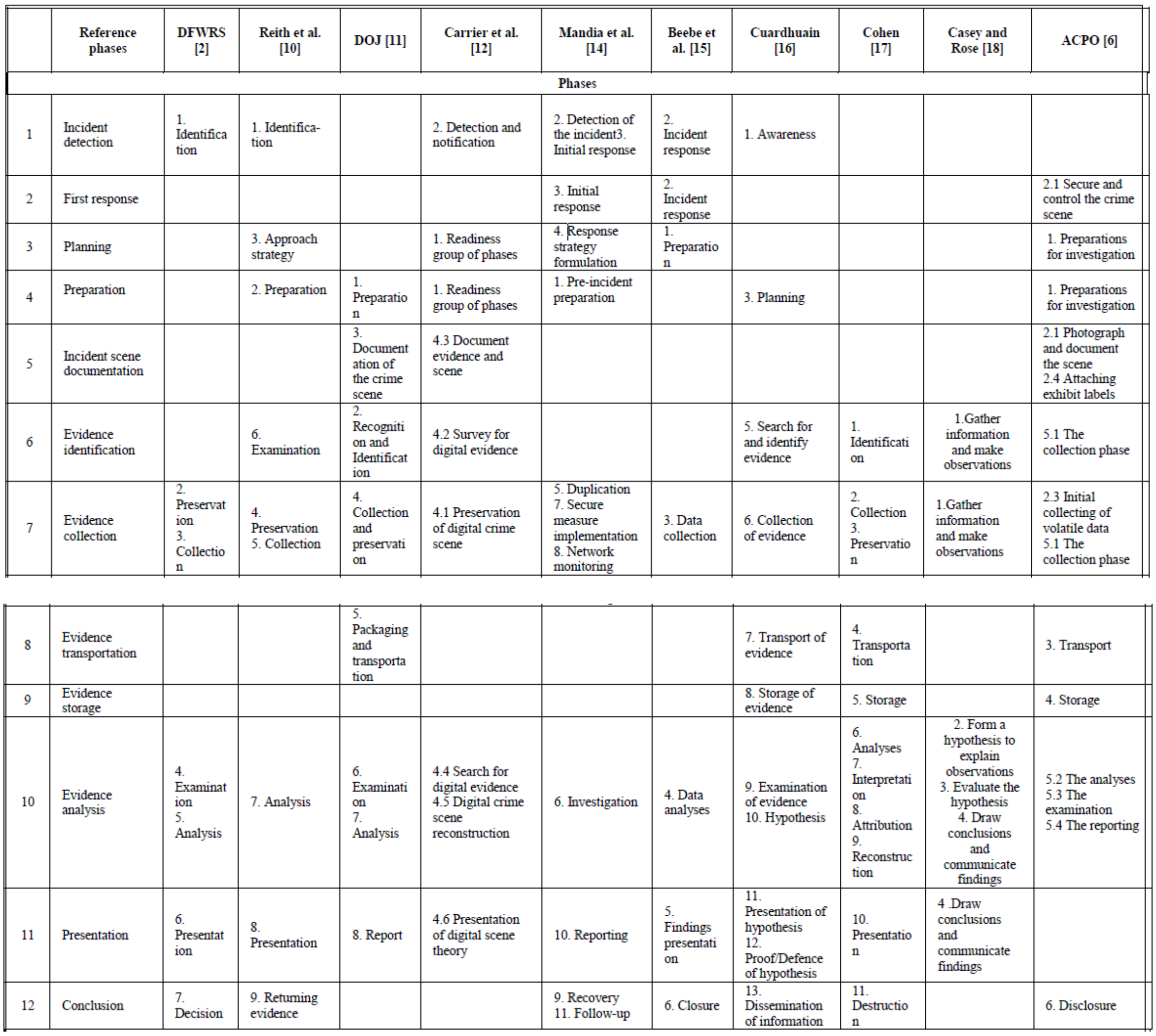
Time stamp

Figure 6. plist file record on com.comcsoft.iTransferPro.

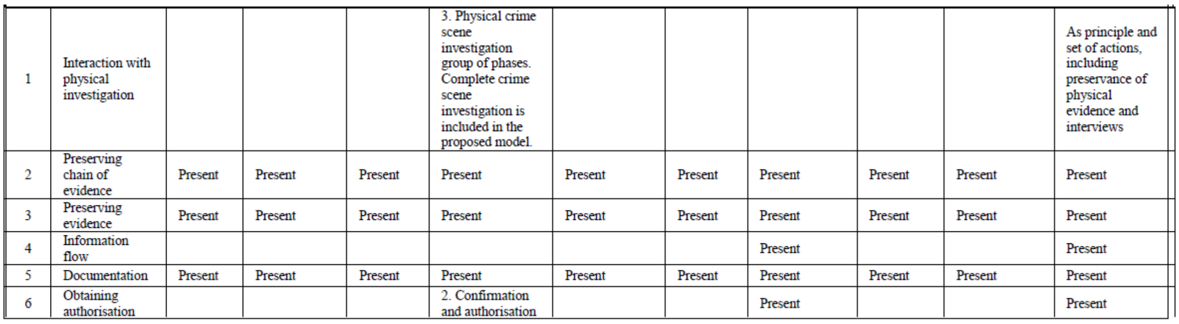
An online Unix Time Conversion tool was used to convert *"397282107"* to *"Wed, 04 Aug 2013 04:08:27 GMT"*. The Pilot study shows the scope of digital forensic investigation on a smart device (with scenario tests). It indicates that the three problems identified from literature are present. The problem of large data quantities can only be resolve through automation and the problem of cloud connectivity can be managed by setting limits to investigation. However the problem of many independent approaches remains outstanding where there is apparent redundancies between approaches and a requirement to be updated to the new technologies, services and related service integrations.

EVALUATING MODELS

(Note this section reviews and discusses briefly the 13 Digital Forensic investigation models shown in the Appendix that had to be removed for the file size requirement. It is available from the authors.) Each model has been evaluated for its principles, phases and the other elements included to locate necessities, redundancies and gaps between the models. Figure 7 provides example of the analytic framework and the types of resolution that may be achieved using reference phases and investigation interaction criteria as the units of analysis. The first model was the Computer Forensic Investigation Process model (1995). This model focuses exclusively in the investigation process beginning with data acquisition. The model does not define how the investigator can approach a crime scene. The model also puts emphasis on the evaluation stage by providing three extra investigation steps within the evaluation stage. Digital evidence must be analysed without bias or modification (Reith et al., 2002, p.3). As an improvement, the six phase Investigative model from the DFRWS was developed for computer and network forensics (Palmer & Corporation, 2001, p.17). The DFRWS investigative model addresses the short comings of the computer forensic investigation processes in the Computer Forensic Investigation model (1995). The DFRWS model was also developed to cover not only forensic investigation on computers but networks as well. The progressive development and comparative analysis of each model can be traced until the recent models developed for cloud environments. Martini & Choo proposed a digital forensic investigation framework for cloud computing in the year 2012. This cloud investigation framework consists of four phases which are the evidence source identification and preservation phase, collection phase, examination and analysis and the reporting and presentation phase. The digital forensic framework for cloud computing was developed based on the frameworks developed by McKemmish in 1999 and Kent et al. in 2006. However, the key difference is the iteration feature implemented on the evidence source identification and preservation phase and the examination and analysis phase. Due to the fact that virtualization is the key element in implementing cloud computing, this provides forensic investigators with more challenges. The decentralised nature of how data is processed in the cloud creates new disruptive challenges for investigators. As a result, the traditional ways of acquiring data are no longer practical (Birk & Wegener, 2011, p.1).



	Reference phases	DFWRS [2]	Reith et al. [10]	DOJ [11]	Carrier et al. [12]	Mandia et al. [14]	Beebe et al. [15]	Cuardhuain [16]	Cohen [17]	Casey and Rose [18]	ACPO [6]
Phases											
1	Incident detection	1. Identification	1. Identification		2. Detection and notification	2. Detection of the incident3. Initial response	2. Incident response	1. Awareness			
2	First response					3. Initial response	2. Incident response				2.1 Secure and control the crime scene
3	Planning		3. Approach strategy		1. Readiness group of phases	4. Response strategy formulation	1. Preparation				1. Preparations for investigation
4	Preparation		2. Preparation	1. Preparation	1. Readiness group of phases	1. Pre-incident preparation		3. Planning			1. Preparations for investigation
5	Incident scene documentation			3. Documentation of the crime scene	4.3 Document evidence and scene						2.1 Photograph and document the scene 2.4 Attaching exhibit labels
6	Evidence identification		6. Examination	2. Recognition and Identification	4.2 Survey for digital evidence			5. Search for and identify evidence	1. Identification	1.Gather information and make observations	5.1 The collection phase
7	Evidence collection	2. Preservation 3. Collection	4. Preservation 5. Collection	4. Collection and preservation	4.1 Preservation of digital crime scene	5. Duplication 7. Secure measure implementation 8. Network monitoring	3. Data collection	6. Collection of evidence	2. Collection 3. Preservation	1.Gather information and make observations	2.3 Initial collecting of volatile data 5.1 The collection phase
8	Evidence transportation			5. Packaging and transportation				7. Transport of evidence	4. Transportation		3. Transport
9	Evidence storage							8. Storage of evidence	5. Storage		4. Storage
10	Evidence analysis	4. Examination 5. Analysis	7. Analysis	6. Examination 7. Analysis	4.4 Search for digital evidence 4.5 Digital crime scene reconstruction	6. Investigation	4. Data analyses	9. Examination of evidence 10. Hypothesis	6. Analyses 7. Interpretation 8. Attribution 9. Reconstruction	2. Form a hypothesis to explain observations 3. Evaluate the hypothesis 4. Draw conclusions and communicate findings	5.2 The analyses 5.3 The examination 5.4 The reporting
11	Presentation	6. Presentation	8. Presentation	8. Report	4.6 Presentation of digital scene theory	10. Reporting	5. Findings presentation	11. Presentation of hypothesis 12. Proof/Defence of hypothesis	10. Presentation	4 .Draw conclusions and communicate findings	
12	Conclusion	7. Decision	9. Returning evidence			9. Recovery 11. Follow-up	6. Closure	13. Dissemination of information	11. Destruction		6. Disclosure



1	Interaction with physical investigation				3. Physical crime scene investigation group of phases. Complete crime scene investigation is included in the proposed model.						As principle and set of actions, including preservance of physical evidence and interviews
2	Preserving chain of evidence	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
3	Preserving evidence	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
4	Information flow							Present			Present
5	Documentation	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
6	Obtaining authorisation				2. Confirmation and authorisation			Present			Present

Figure 7. Investigation model evaluation (Valjarevic & Venter, 2012, p.8).

Valjarevic and Venter (2012) concluded that there are significant disparities between the existing digital forensic investigation process models. These inequalities relate to the following; the number of phases of the model, the scope of the model, the similarities of the phases name, the hierarchy levels and the principle behind the construction of the investigation process model. The proposal for a new working model is presented in the next section.

THE PROPOSED WORKING MODEL

The investigation model evaluation conducted by Valjarevic & Venter in 2012 shown in Figure 7 was organised around the attributes of reference phases and investigation interaction. Our evaluation of the same models was conducted by focusing on the relevancy of the model to an investigation involving a smart device. As a result it was evident that existing models have different concepts regarding the purpose of the use application. Most of the existing models have different names for the phases but a similar purpose. We believe that in order to integrate all of the digital forensic expertise divisions without compromising the efficiency and the effectiveness of the investigation, a revised digital forensic investigation process model is required. This new model needs to be able to provide the investigator with a clear definition of the investigation path, and also to clearly define the external links to other repositories of evidence. However, most importantly, these processes must be achieved without sacrificing the integrity and the credibility of the evidences. Figure 8 shows the result of our analysis.

The main feature of our working model is the relevant pathways that may be taken in relation to a particular investigation. An investigator is to start with the device at the incident detection process. The relevant pathways allow a traditional forensics method and/or to branch out at the external links process to a cloud environment or to a computer and networking environment or to both. In this way the redundancies and exceptions created in the analysis of the appended models are removed so that an investigator has clear direction for investigation processes and decision making. Once the acquired data from a smart device is analysed and criminal activities on private network and cloud environment are found, the working model clearly defines the required investigatory steps. In the verification study the results and IP address of servers that were accessed in a private network were clearly identifiable and also the cloud account that was used to transfer the scenario stolen documents. In such discovery, there is no need for the investigator to pick up another model but just follow processes defined in this model. For instance, there is no need to go through processes such as deciding strategies on how to approach a new thread of investigation. The investigator only needs to acquire the required access permission and go straight to the IP address that was found on the mobile device. This minimises the volume of data that the investigator has to acquire and analyse. Effectiveness and efficiency is an important element of an investigation because, it minimises the chance of making a mistakes. The iterative features built into the model assure duplication of processes is eliminated and regardless of the number of pathways required to complete the investigation one report will be delivered.

The following definitions assist the interpretation of the proposed working model (see Figure 8):

- **Incident Detection Process:**
  This phase initiated an investigation which is usually triggered by a phone call reporting a crime or a mobile device found in a crime scene.
- **First Response Process:**
  Another part of the initialisation process in this model deals with the first awareness of an incident, acknowledging the incident and starting the process by involving the stakeholders. This can be achieved by a system or an individual and involves further reporting to the system administrator or the stakeholders or investigator.
- **Approach strategy:**

This phase is concerned with the development of a method or strategy on how to approach the investigation to maximise the collection of potential untainted evidence while minimising the impact to the victim.

- **Evidence Source Preservation:**
  This phase is concerned with identifying sources of potential evidence in a digital forensics investigation. This involves the identification of potential evidence collection methods whether by traditional or digital forensics. Irrespective of the identified source of potential evidence, forensic investigator needs to ensure the proper preservation of the evidence. This will involve isolating, securing and preserving the state of both potential physical and digital evidences.
- **Potential Evidence Collection:**
  This phase involves the physical crime scene and the acquisition of potential digital evidences by employing standardised and accepted methods.
- **Examination:**
  This phase involves an in-depth systematic search of potential evidences that relate to the alleged crime.
- **Trace Potential Evidences External Links:**
  After an in-depth systematic examination of potential evidences on a smart mobile device, alleged crime is traced down based on evidences acquired from previous phases such as:
  i. IP addresses which linked to a private local area network.
  ii. Name of cloud provider or username that identified a link to cloud service provider that was used in the alleged crime.
- **Analysis:**
  This phase is concerned with reconstructing the fragments of data, drawing conclusions from the evidence found and determining their significance. An iteration feature is implemented in this phase to allow the investigator to go back to the preservation to reconfirm or further investigate potential evidences found in the data.
- **Presentation/Report:**
  This phase involves summarising and explaining the conclusions of the investigation.
- **Return Evidence/Storage/Chain of Custody**
  This phase ensures that the chain of custody, storage and the return of physical and digital evident follows the proper procedure for handling evidence.

The preparation phase for Network and Cloud forensics is as follows:

- **Preparation phase:**
  In addition to preparing for an investigation in a private local area network or the Cloud environment, this phase also involves obtaining the required authorisation from local legal bodies for further investigation and access to more information from this environment.

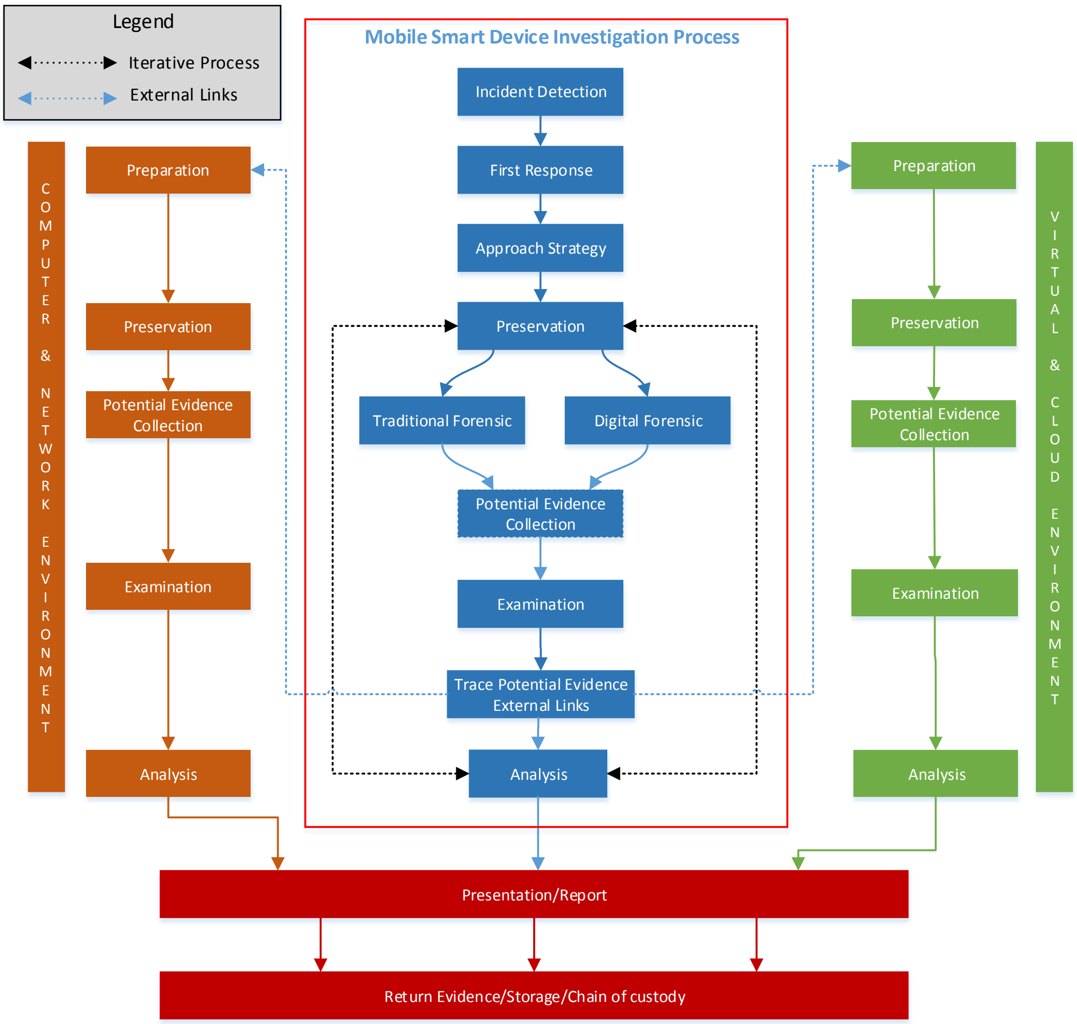

Legend
Iterative Process
External Links
Mobile Smart Device Investigation Process
Incident Detection
First Response
Approach Strategy
Preservation
Traditional Forensic
Digital Forensic
Potential Evidence Collection
Examination
Trace Potential Evidence External Links
Analysis
COMPUTER & NETWORK ENVIRONMENT
Preparation
Preservation
Potential Evidence Collection
Examination
Analysis
VIRTUAL & CLOUD ENVIRONMENT
Preparation
Preservation
Potential Evidence Collection
Examination
Analysis
Presentation/Report
Return Evidence/Storage/Chain of custody

Figure 8. A Smart Technologies Digital Forensic Investigation Model

CONCLUSION

The literature analysis of digital forensic investigation frameworks showed three main problems when one or more selections of the frameworks were applied to smart technology investigations. The pilot study verification of the problems confirmed that big data, cloud environments and the division of focus into many models weaken the capability of the investigator to apply an efficient and effective approach to smart technology investigations. Our contribution shows that a relevant model can be constructed (figure 8) from the necessities, redundancies and gaps in the other established models. This is exploratory research and further work is proceeding to test the model in practice.

REFERENCES

Abhishek, K., & Mahasweta, S. (2011). Cloud Computing. In *Cloud Computing* (pp. 3-29): CRC Press. Retrieved from http://dx.doi.org/10.1201/b11149-3. Retrieved 2013/06/02. doi:doi:10.1201/b11149-3 10.1201/b11149-3

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A New Approach of Digital Forensic Model for Digital Forensic Investigation. *IJACSA) International Journal of Advanced Computer Science and Applications*, *2*(12).

Bader, M., & Baggili, I. (2010). iPhone 3GS forensics: Logical analysis using apple iTunes backup utility. *Small Scale Digital Device Forensics Journal, 4*(1), 15.

Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. *Proceedings of the Fourth Digital Forensic Research Workshop* (pp. 1-9). Citeseer: DFRW

Bednar, P. M., Katos, V., & Hennell, C. (2008, 9-9 Oct. 2008). Cyber-Crime Investigations: Complex Collaborative Decision Making. *Proceedings of the third International Annual Workshop on Digital Forensics and Incident Analysis, 2008. WDFIA '08.* (pp.3-11). Malaga: IEEE. doi:10.1109/wdfia.2008.7

Birk, D., & Wegener, C. (2011, 26-26 May 2011). Technical Issues of Forensic Investigations in Cloud Computing Environments. *Proceedings of the 2011 IEEE Sixth International Workshop on the Systematic Approaches to Digital Forensic Engineering (SADFE)* (pp. 1-10). CA: IEEE. doi:10.1109/SADFE.2011.17

Dezfouli, F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F. B. M., & bin Shamsuddin, S. (2012, 26-28 June 2012). Volatile memory acquisition using backup for forensic investigation. *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* (pp. 186-189). Kuala Lumpur: IEEE. doi:10.1109/CyberSec.2012.6246108

Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. *IMF, 7,* 19-40.

Furht, B. (2010). Cloud Computing Fundamentals. In B. Furht & A. Escalante (Eds.), *Handbook of Cloud Computing* (pp. 3-19): Springer US. Retrieved from http://dx.doi.org/10.1007/978-1-4419-6524-0_1. doi:10.1007/978-1-4419-6524-0_1

Goel, A., Tyagi, A., & Agarwal, A. (2012). Smartphone Forensic Investigation Process Model. *International Journal of Computer Science & Security (IJCSS), 6*(5), 322.

Hankins, R., Uehara, T., & Jigang, L. (2009, 8-10 July 2009). A Comparative Study of Forensic Science and Computer Forensics. *Proceedings of the Third IEEE International Conference on Secure Software Integration and Reliability Improvement, 2009. SSIRI 2009* (pp. 230-239). Shanghai: IEEE. doi:10.1109/ssiri.2009.42

Jansen, W., & Ayers, R. (2007). Guidelines on cell phone forensics. *NIST Special Publication, 800*, 101.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication,* 800-886.

Leavitt, N. (2011). Mobile Security: Finally a Serious Problem? *Computer, 44*(6), 11-14. doi:10.1109/mc.2011.184

Lin, I. L., et al. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. *Proceedings if the 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)* (pp. 386-391). Barcelona IEEE.

Lin, R., Dor-Shifer, D., Rosenberg, S., Kraus, S., & Sarne, D. (2006). Towards the fourth generation of cellular networks: improving performance using distributed negotiation. *Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems*. Terromolinos: ACM.

McKemmish, R. (1999). *What is forensic computing?* : Australian Institute of Criminology.

Martini, B., & Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation, 9*(2), 71-80. doi:http://dx.doi.org/10.1016/j.diin.2012.07.001

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). *NIST Special Publication, 800,* 145.

Mollah, M. B., Islam, K. R., & Islam, S. S. (2012, April 29 2012-May 2 2012). Next generation of computing through cloud computing technology. *Proceedings of the 2012 25th IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)* (pp.1-6). Montreal: IEEE. doi:10.1109/ccece.2012.6334973

Owen, P., & Thomas, P. (2011). An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines. *Digital Investigation, 8*(2), 135-140. doi:http://dx.doi.org/10.1016/j.diin.2011.03.002

Palmer, G., & Corporation, M. (2001). *A Road Map for Digital Forensic Research*. Retrieved from http://isis.poly.edu/kulesh/forensics/docs/DFRWS_RM_Final.pdf doi:citeulike-article-id:1449974

Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security, 9*(8), 38-44.

Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. *Digital Investigation, 7*(1–2), 14-27. doi:http://dx.doi.org/10.1016/j.diin.2010.02.003

Pollitt, M. (1995). Computer forensics: An approach to evidence in cyberspace. *Symposium conducted at the meeting of the Proceedings of the National Information Systems Security Conference* (pp. 487-491).

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3), 1-12.

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Proceedings of the 2006 Conference on Digital Forensics, Security and Law* (pp. 27-40).

Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation, 10*(1), 34-43. doi:http://dx.doi.org/10.1016/j.diin.2013.02.004

Said, H., Yousif, A., & Humaid, H. (2011). IPhone forensics techniques and crime investigation. *Proceedings of the 2011 International Conference and Workshop on Current Trends in Information Technology (CTIT).* Dubai. doi:10.1109/ctit.2011.6107946

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security, 8*(10), 163-169.

Tanner, A., & Dampier, D. (2009). Concept Mapping for Digital Forensic Investigations. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics V* (Vol. 306, pp. 291-300): Springer Berlin Heidelberg. Retrieved from http://dx.doi.org/10.1007/978-3-642-04155-6_22. doi:10.1007/978-3-642-04155-6_22

Valjarevic, A., & Venter, H. S. (2012, 15-17 Aug. 2012). Harmonised digital forensic investigation process model. *Proceedings of the 2012 Information Security for South Africa (ISSA).* (pp. 1-10). Johannesburg: IEEE. doi:10.1109/issa.2012.6320441

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone Security Challenges. *Computer, 45*(12), 52-58. doi:10.1109/mc.2012.288

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases Of Computer Forensics Investigation Models [Article]. *International Journal of Computer Science & Information Technology, 3*(3), 17-31. doi:10.5121/ijcsit.2011.3302