

Business Horizons (2016) **59**, 593—604

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY
www.elsevier.com/locate/bushor

A multidisciplinary digital forensic investigation process model

Raymond Lutui

Auckland University of Technology, 55 Wellesley Street East, Auckland 1142, New Zealand

KEYWORDS
Forensic investigation models;
Smart devices;
Mobile forensics;
Network forensics;
Cloud forensics

Abstract Worldwide usage of mobile smart devices has increased dramatically over the past two decades. The popularity of these devices has grown as a result of their increased processing power, storage capacity, and memory; they can now hold enormous amounts of both personal and private business data. In addition to the consideration of mobile devices, the scope of any forensic investigation has also grown to include cloud environments. Previously, we proposed a working model that can improve the effectiveness and efficiency of an investigation in a multidisciplinary environment. The study presented herein, however, evaluates a straw man model derived from current practice models to identify the required improvements. The study also proposes a new improved process model known as a multidisciplinary digital forensic investigation process model.

1. The current state of digital forensics

The term 'digital forensics' originated as a synonym for computer forensics, but later expanded to encompass forensic examination of all digital technologies. Reith, Carr, and Gunsch (2002, p. 2) define *computer forensics* as "the collection of techniques and tools used to find evidence in a computer." The same authors, however, explain *digital forensics* as a broader concept to include (p. 2):

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

Digital forensics can be broken down into categories, including computer forensics and mobile forensics. *Mobile forensics* is used to deal with forensic investigation of crimes that involve mobile smart devices, such as smartphones and tablets. Types of data that can be retrieved from these smart devices

E-mail address: raymond.lutui@aut.ac.nz

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.08.001

include call logs, text messages, and contact lists (Da-Yu, Shiuh-Jeng, Sharma, & Huang, 2009; Mellars, 2004).

Due to the omnipresent nature of mobile smart devices, they play a substantial role in digital crime. Regardless of their differences, they all carry precious information that can be vital to an investigation (Mohtasebi & Dehghantanha, 2013). To obtain data from a mobile device for forensic analysis, the investigator needs the help of a tool—and often more than one. Due to the differences in terms of technologies employed, investigators will have to engage different methods and tools depending on the devices involved (Albano, Castiglione, Cattaneo, & de Santis, 2011). The most challenging part is data acquisition, especially when it comes to acquiring data from volatile memory (Dezfouli et al., 2012). As described in the NIST Special Publication 800-101, *mobile device forensics* is the art of employing science to extract digital evidence from a mobile device under forensically compliant conditions while employing accepted techniques (Jansen & Ayers, 2007).

1.1. Digital forensics: Existing standards and guidelines

Digital data on mobile devices has three known properties: it is easy to copy, easy to modify, and difficult to acquire (Lin, Han-Chieh, & Shih-Hao, 2011; Yadav, Ahmad, & Shekhar, 2011). Therefore, prior to acquiring data from a mobile smart device, extra precautions must be taken and standard procedures and base practices must be followed carefully. This process is purposely implemented in order to preserve the integrity of the data or change the state of the device (Jansen & Ayers, 2007). Figure 1 shows the relationship of various fields of digital forensics.

As illustrated, there are four main areas: computer forensics, network forensics, cloud forensics, and mobile forensics (Lin et al., 2011). Regardless of the relevant area, the first step in every investigation is identification. To satisfy the identification phase, data will be extracted from the target device. However, the four areas of digital forensics require different techniques with regard to data acquisitions.

Extracting data from mobile smart devices is different from obtaining data from a computer. In the case of a computer, the hard disk can be isolated. For that reason, the forensic investigator will only work with a clone and not the actual data. However, extracting data from a smartphone's internal memory is more challenging (Fang et al., 2012; Jansen & Ayers, 2007). The most important component of this practice is to preserve the integrity of potential evidence. Certain principles and standards must be met so the findings can be admissible in a court of law (Jansen & Ayers, 2007). Therefore, there is a need to maintain the integrity and credibility of digital evidence. Reputable organizations, such as the ACPO in the United Kingdom and NIST in the United States, have made efforts to develop guidelines to help investigators.

In the NIST Special Publication 800-101, Wayne Jansen and Rick Ayers (2007) explained the purpose of their guidelines is divided into two parts. The guidelines are designed to help organizations properly navigate evolving policies and procedures for dealing with mobile phones. Also, the guidelines aim to prepare digital forensic experts for dealing with

Figure 1. Various fields of digital forensics

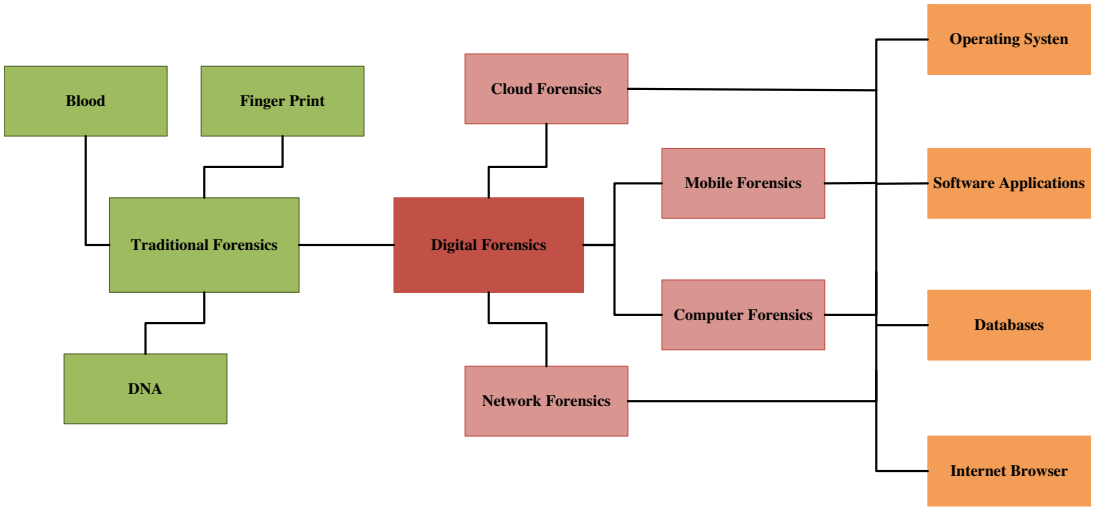


Table 1. ACPO guidelines four principles*

Principle 1	No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
Principle 2	In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3	An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4	The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

* Source: ACPO (2007)

new circumstances when they arise. These recommendations were created to facilitate efficient and effective digital forensic investigations on mobile devices. The NIST guidelines for mobile device forensics are:

- Organizations should ensure that their policies contain clear statements about forensic considerations involving cell phones.
- Organizations should create and maintain procedures and guidelines for performing forensic tasks on cell phones.
- Organizations should ensure that their policies and procedures support the reasonable and appropriate use of forensic tools for cell phones.
- Organizations should ensure that their forensic professionals are prepared to conduct activities in cell phone forensics.

These recommendations do not define how law enforcement and investigators handle mobile devices in an investigation, which must also be considered. Acquiring digital evidence while trying to maintain its integrity may seem a challenge. However, if it is done correctly then it will produce evidence that is irrefutable and cost effective (ACPO, 2007). The ACPO argued that the digital world has evolved but the principles of preserving evidence are still highly relevant. The following in Table 1 are the four ACPO principles from the ACPO guidelines.

In addition to the principles outlined in Table 1, there are other issues to consider, especially when working with mobile devices. The investigator must consider other forensic evidence such as DNA and fingerprints that can be obtained from the device. In this regard, examining the device without considering other forensic data may destroy vital evidence (ACPO, 2007).

2. Existing investigation procedures

The investigator is required to use standardized and formalized investigation procedures when handling digital evidence in order for these findings to be admissible in a court of law. A number of methods, frameworks, and investigation process models have been proposed and can be dated back as far as 1995. International standards are still being developed to formalize and provide digital forensic practitioners with a set of standardized guidelines.

In this section, 12 investigation process models are reviewed. The first model reviewed is the computer forensic investigation process by Mark Pollitt (1995). This model focused on the investigation processes beginning with data acquisition. The model does not define how the investigator could approach the crime scene. In 2001, the first Digital Forensic Research Workshop (DFRWS) extended the computer forensic investigation process by adding three extra processes emphasizing the evaluation stage (Palmer, 2001). This model determined the path the digital evidence took, starting from its physical, logical, and legal context. This approach was debatable because digital evidence must be gathered by employing approved and reliable methods (Reith et al., 2002). The six-phase investigative model from the DFRWS was developed for computer and network forensics (Palmer, 2001).

The DFRWS investigative model (Palmer, 2001) addressed the shortcomings of the model from Mark Pollitt in 1995. The DFRWS model was developed to cover not only forensic investigation on computers but networks too. However, the DFRWS model's identification phase was underdeveloped, as it left out pre-incident preparation in order to organize the forensic processes prior to responding to an incident. Pre-incident processes outline detailed procedures to help investigators deal with digital and physical evidence (Reith et al., 2002).

Reith et al. proposed the abstract digital forensic model in 2002. The model was comprised of nine investigation phases with an iterative feature implemented between the examination and the analysis phase. This model was open for critique as some of the phases could duplicate to a certain extent. For instance, when responding to an incident, identifying the appropriate procedure is likely to involve also determining the technique to be employed (Baryamureeba & Tushabe, 2004).

Carrier and Spafford (2003) introduced a new forensic investigation model known as an integrated digital investigation process. This model was comprised of 17 phases organized into five main groups. The authors outlined the weaknesses of the model. First, the model's classifications may be defined as too general for practical use. Second, there was no easy method for testing the model, and third, all of the subcategories added to the model would make it problematic to utilize. This model failed to define the process of handling the evidence's chain of custody, which is an important aspect of any investigative work (Perumal, 2009).

The computer forensic field triage process model (CFFTPM) (Rogers et al., 2006) suggested that the evidence triage—user's profile, internet usages, and the chronological timeline activities—depended on the type of investigation. The CFFTPM proposed an onsite or field approach to help an investigator in identifying, analyzing, and interpreting the evidence in a very short time frame. However, the CFFTPM model had no requirement for taking the compromised system or media back to the lab to obtain a complete image for further examination. Thus, the CFFTPM framework was not applicable for all investigative situations (Selamat, Yusof, & Sahib, 2008).

The common process model for incident and computer forensics was proposed by Freiling and Schwittay in 2007. This model focused significantly on analysis, consisting of pre-incident preparation, pre-analysis, analysis, and post-analysis. The digital forensic model based on Malaysian investigation process was proposed by Perumal. According to Perumal (2009), the previous models do not show the information process flow focusing on issues such as chain of custody, attention to fragile evidence, and data acquisition processes.

A generic process model for network forensics was proposed by Pilli, Joshi, and Niyogi (2010). The main purpose of this model was to formalize a methodology specifically for network-based investigations. A new feature that this generic model provided was a connection to the incident response through its second phase—the detection phase. The digital forensic model for digital forensic investigation was proposed by Ademu, Imafidon, and Preston in 2011. In this model, the entire investigation process was iterative and conceptualized into four different phases. Yusoff, Ismail, and Hassan (2011) proposed a new generic computer forensic investigation model (GCFIM). In this study, the authors investigated previous forensic investigation process models and found that each of the previously proposed models recommended phases could be placed in at least one of their own proposed generic phases.

With regard to forensic investigation in the cloud environment, this new technology has presented opportunities for criminal activities and challenges to law enforcement agencies. Martini and Choo (2012) proposed a new digital forensic investigation framework for cloud computing. This framework was based on the frameworks developed by McKemmish in 1999 and Kent, Chevalier, Grance, and Dang in 2006. The key difference is the iteration feature implemented on the evidence source identification, preservation phase, examination, and analysis phase. The decentralized nature of how data is processed in the cloud creates new disruptive challenges to investigators. As a result, traditional ways of acquiring data are no longer practical (Birk & Wegener, 2011).

When identifying and extracting evidence in a cloud environment with multitenant architecture, current forensic procedures cannot be applied (Almulla, Iraqi, & Jones, 2013; Sharma & Sabharwal, 2012). An outline of mapping processes of the digital forensic investigation framework was proposed by Selamat, Yusof, and Sahib in 2008. The mapping process model was a result of reviewing the existing investigation frameworks and models. It was evident that each proposed framework was built on the experience of the previous publications. The authors also noted that the processes or activities were slightly different in terms of their orders.

3. A multidisciplinary investigation process model

Figure 1 highlights the fact that digital forensics consists of four main types of technology that all run on various operating systems. They can access the internet and contain third-party software applications, which may host various databases. It is evident in the literature analysis in Section 2 that none of the existing models were designed for an investigation that involved more than one subfield of digital forensics. We previously introduced a working model called the straw man model

Table 2. Features of the straw man model

Features	Straw Man Investigation Process Model
Attributes	Completeness, consistency, accuracy, reliability, usability, fit with the organization
Properties	Efficiency, effectiveness, efficacy, ethicality, elegance, performance

(Cusack & Lutui, 2014). This section is designed to evaluate the performance of the straw man model in order to identify the required improvements.

Our study was guided by design science (DS) research methodology for information systems research. DS is the design and investigation of artifacts in context. The DS research methodology phases incorporate processes for the production of the artifact. The theory for design and action, in particular, concerns the principles of form and function, methods, and justificatory theoretical knowledge that are used in the development of IS. The artifact is emphasized as the prime contribution of design science (Gregor, 2006). Additionally, Hevner, March, Park, and Ram (2004) outlined some criteria that the authors believe are effective due to their contributions to the novelty of the artifacts. That is, the models and methods designed under design science can be evaluated for completeness, simplicity, consistency, ease of use, and the quality of results obtained through use of the method.

Evaluation is the fifth phase of the DS research methodology, which involves observing and evaluating the effectiveness and efficiency of the artifact in solving a problem. The evaluation and observation results from the client/context-centered initiation will be compared with the objectives of a solution. A satisfaction survey result, client feedback, and data from a system performance, such as availability and response time, will be included in the evaluation. In this case, data from the case study and the current standards and guidelines outlined in Section 1 will be used to evaluate the straw man model.

DS research considers the identified problems from the environment and organizational requirements as a significant part of developing the solution. This includes peoples' roles, skills, and characteristics. DS research method also views the organization's structure, culture, processes, and strategies as relevant in a new solution design and development. Another significant and relevant part of this process is the technology, its existing communication infrastructure, applications, and skills development. DS research requires analyzing the existing knowledge base rigorously and exploring the literature in both academic and professional areas to adopt applicable knowledge.

3.1. The straw man model

An artifact should hold the attributes and properties outlined in Table 2; this is evident in the current literature. These attributes can be the design goal, the expected performance measure. DS research methodology can use the attributes and properties during the iteration process in reevaluating and refining the artifact. The artifact in this study is the aforementioned straw man model. The straw man model consists of three different subfields of the digital forensics domain: smart device forensics, network forensics, and cloud forensics. Each of these subfields are different in scope, characteristics, and nature in terms of risks, security, challenges, etc. (Cusack & Lutui, 2013). Investigating network forensics differs in scope and objective from one perspective to another.

For this work, a second case study was set up, in which the initial test-bed and software tools were also used to process and analyze the second case study (Cusack & Lutui, 2014). In the second case study, the tool extracted the deleted data located in the unallocated partitions. A piece of code was found in the unallocated space where potential evidence may be located. A list of users was also found with only one legitimate username. Inside this user's document directory, a text document named 'contacts.txt' was found containing three names, their street addresses, mobile numbers, and email addresses.

Another text document named 'final announcement.txt' was also found. The information in this document indicated that some kind of important event was going to take place. Another text document named 'new cloud.txt' was found containing a username and password. A software tool known as the iPhone Extractor was used to extract the backup image from the iPad. A directory named 'SystemConfiguration' was created and a file named 'preferences.plist' was found. This file contained information about the name of the device and the name of the wi-fi networks to which that the device was connected. A '.plist' file named 'com.apple.lsdidentifiers' was also found on the iPad. Three applications from a company known as Synology Inc. were used to access the cloud. This file contained login information to a private cloud that was found in the hard disk image.

Table 3. Evaluation method

Evaluation Methods	Attributes	Properties
Observational	• Completeness • Consistency • Accuracy • Reliability • Usability • Fit with the organization	• Efficiency • Effectiveness • Efficacy • Ethicality • Elegance • Performance
Analytical		
Experimental		
Testing		

3.2. Straw man model improvements

The case study in our previous article (Cusack & Lutui, 2014) was designed to confirm the problem identified in the literature: the ever-changing character of digital forensic investigations on mobile smart devices and the need of forensic practitioners to adapt. As a result, a multidisciplinary digital forensic investigation process model was developed under the name of the straw man model. The model was tested on fictitious case studies, which showed the model's performance can be optimized and improved. Investigation process models serve as boundary objects. The model represents aspects of forensic investigations for various purposes, to predict and explain the operation and mechanism of the investigation.

3.3. Effectiveness and efficiency evaluation

There are various types of wireless networks that mobile smart devices utilize and there are various areas of knowledge in the digital forensics arena. In comparison to existing investigation process models, a new model should have the ability to define the relationships between various subfields in the digital forensic arena. In order for the model to successfully define these relationships and optimize its performance, the features of each process must be understood. In this subsection, the findings of the straw man model's evaluation for effectiveness and efficiency are reported. Efficiency can be informally defined as 'doing things right.' It can also be referred to as completing a task at minimal time. Effectiveness, on the other hand, can be described as 'doing the right things.' Effectiveness can add value to processes; it enhances innovation. Effectiveness is the scope within which objectives are met and an activity fulfills its purpose. Table 3 shows a combination of the evaluation method used together with the attributes and properties of the model. They are used in the evaluation of the effectiveness and the efficiency of the straw man model.

There are key influences of effectiveness and efficiency that can be identified in the literature, including: speed/movement of the processes, structure of the model that synchronizes the whole process, and space created. Providing a transferable space is a critical factor in terms of task management, especially important in order to avoid any bottlenecks. In the following subsections, the straw man model is evaluated based on the results gathered from the case studies. The straw man design and its features are assessed according to the model's expected attributes and properties as outlined in Table 3. The final evaluation is for relevance and rigor. The data from the case scenarios are used to evaluate the effectiveness and efficiency of the straw man model.

It can be seen in the results listed in Table 4 that the observational and analytical results for processes movement were still rated medium. The observational and analytical results for the structure of the straw man mode also yielded a medium rating while the rest of the evaluation results were rated high. The results from the straw man's efficiency evaluation are outlined in Table 5.

The results for the straw man model's efficiency evaluation results were similar to the effectiveness evaluation results. The observational and analytical results for processes movement among the phases of the model were rated at medium. The structure of the model also rated medium under the analytical and observational test results, while the rest

Table 4. Effectiveness evaluation result

Key Factors	Observational	Analytical	Experimental	Testing	Descriptive
Speed/Movement	Medium	Medium	High	High	High
Model Structure	Medium	Medium	High	High	High
Space	High	High	High	High	High

Table 5. Efficiency evaluation result

Key Factors	Observational	Analytical	Experimental	Testing	Descriptive
Speed/Movement	Medium	Medium	High	High	High
Model Structure	Medium	Medium	High	High	High
Space	High	High	High	High	High

Table 6. The model's design evaluation result

Attributes/ Properties	Observational	Analytical	Experimental	Testing	Descriptive
Completeness	Medium	Medium	High	High	High
Consistency	Medium	Medium	Low	Low	High
Accuracy	Medium	Medium	High	High	High
Performance	Medium	Medium	Medium	Medium	High
Reliability	Medium	Medium	Medium	Medium	High
Usability	High	High	High	High	High
Efficiency	Medium	Medium	High	High	High
Effectiveness	Medium	Medium	High	High	High
Ethicality	High	High	High	High	High

yielded high ratings. Following in subsection the design of the straw man model is evaluated and the findings are outlined.

3.4. Design evaluation

The evaluation method was also applied in the evaluation of the design of the straw man model. The evaluation results of the design of the straw man model yielded interesting information, showing that there is still room for improvement. The majority of the attributes and properties of the straw man were rated medium for observational and analytical factors except for usability and ethicality, which yielded high ratings. Under experimental and testing, the model rated high for most of the attributes and properties while performance and reliability were rated at medium. However, consistency yielded a low rating on both approaches—experimental and testing. All of the attributes and properties of the straw man model were rated high when evaluated under the descriptive approach (Table 6).

3.5. Relevance and rigor evaluation

Design science research methodology is the approach employed to guide this study. DS puts its focuses on the artifact created as a result of a study, from the development stage to its creation, optimization, and communication. To support and justify the development, creation, and evaluation activities of the new artifact, the existing knowledge base needs to be employed.

The existing knowledge base consists of well-informed bases and methods that are recognized among both academic and professional communities. These methods support evaluation activities of a new artifact and the results can be used for improvements. Dresch, Lacerda, and Atntunes (2015) outlined seven benchmarks of conducting DS research. However, according to their fifth, the study should be based on an application of rigors techniques in both the construction and the evaluation of the straw man model. The purpose is to validate the study and expose its reliability. It is important that this is conducted with an appropriate amount of rigor to demonstrate the suitability of the straw man model for its proposed application. See Table 7 for the results yielded when the artifact is evaluated under the same evaluation methodology.

This evaluation is designed to evaluate the relevance of the problem identified in the literature and the rigor of the applicable knowledge employed from the knowledge base. However, when the relevance and rigor of the straw man model is evaluated under the same evaluation methodology, the results indicated that improvements are required. Under observational and analytical, completeness and consistency were both rated low while accuracy, reliability, and performance, together with effectiveness and efficiency, were all rated medium.

Table 7. The model's relevance and rigor evaluation result

Attributes/ Properties	Observational	Analytical	Experimental	Testing	Descriptive
Completeness	Low	Low	Medium	Medium	High
Consistency	Low	Low	Medium	Medium	High
Accuracy	Medium	Medium	Medium	Medium	High
Performance	Medium	Medium	Medium	Medium	High
Reliability	Medium	Medium	Medium	Medium	High
Usability	High	High	High	High	High
Efficiency	Medium	Medium	Medium	Medium	High
Effectiveness	Medium	Medium	Medium	Medium	High
Ethicality	High	High	High	High	High

Along with such approaches as experimental and testing, the majority of the artifact's attributes and properties were rated medium except for usability and ethicality, which were rated high.

3.6. Summary of required improvements

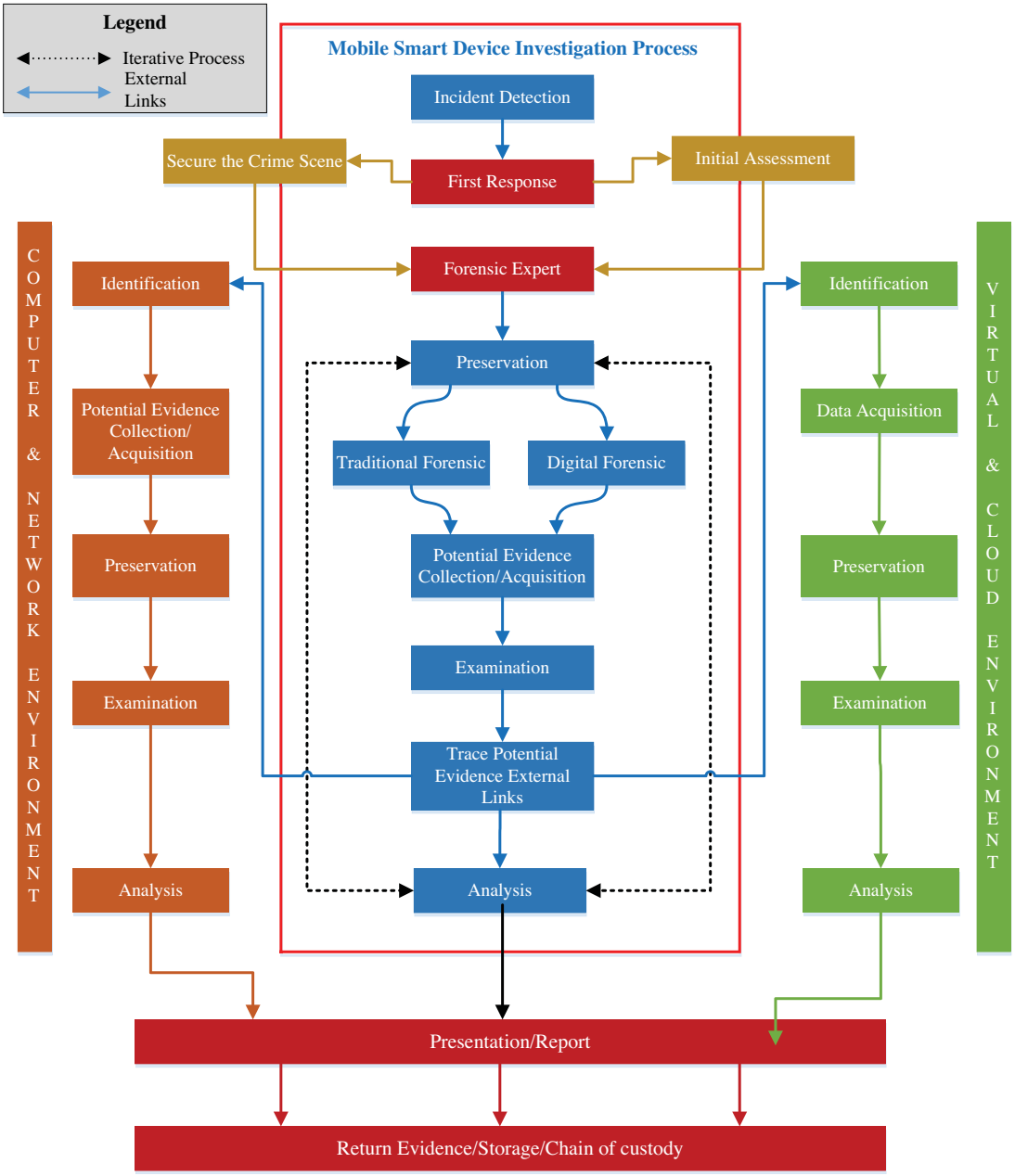
Following in Table 8 is a summary of the results of the evaluation conducted on the straw man model. Based on the summary provided, Table 7 highlighted the weaknesses of the straw man model and areas where improvements are imminent. As a result, Figure 2 showed the improved straw man model, now known as the multidisciplinary digital forensics investigation process model (MDFIPM). The key indicators for improvements were the areas with a low rating: consistency and completeness. Consistency was rated low in the design evaluation and also the relevance and rigor evaluation.

The report flagged that either the model design is weak or the structure is incomplete and inconsistent. As a result, the knowledge base was consulted

Table 8. Areas in which improvements are required

EFFECTIVENESS AND EFFICIENCY					
Key Factors	**Observational**	**Analytical**	**Experimental**	**Testing**	**Descriptive**
Speed/Movement	Medium	Medium			
Model Structure	Medium	Medium			
DESIGN EVALUATION					
Attributes/Properties					
Completeness	Medium	Medium			
Consistency	Medium	Medium	Low	Low	
Accuracy	Medium	Medium			
Performance	Medium	Medium	Medium	Medium	
Reliability	Medium	Medium	Medium	Medium	
Efficiency	Medium	Medium			
Effectiveness	Medium	Medium			
RELEVANCE AND RIGOR					
Completeness	Low	Low	Medium	Medium	
Consistency	Low	Low	Medium	Medium	
Accuracy	Medium	Medium	Medium	Medium	
Performance	Medium	Medium	Medium	Medium	
Reliability	Medium	Medium	Medium	Medium	
Efficiency	Medium	Medium	Medium	Medium	
Effectiveness	Medium	Medium	Medium	Medium	

Figure 2. The multi-disciplinary digital forensic investigation process model



and brought in again. The standards and principles developed by organizations such as ISO/IEC, ACPO, NIST, NIJ were reviewed again against the model's areas of weaknesses. Following in Tables 9 and 10 are the outlined recommendations for improvements made to the straw man model.

The straw man model promotes preparation, preservation, and collection. However, in the literature, identification is more suitable in a network environment. For collection, on the other hand, it is recommended that a logical acquisition of data should be taken before investigators start disconnecting devices in a network environment. A decision should be made based on the situation and the environment depending on whether potential evidence is to be collected or acquired.

Table 10 shows recommendations for improvement regarding investigation in cloud environment. In this environment, there are various service models; however, there are three fundamental service models in particular known as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). One of the recommendations found in the literature is to identify any data

Table 9. Recommendation for improvements in network forensics

Straw Man's Network/Cloud	
Preparation	Identification by observing physical characteristics such as device design elements, power connector, or device labels.
Preservation	Preserve the status of digital device (don't switch on/off) unless transport is required and it cannot be done while the device is operating.
Collection	Devices with one physical network connection might be connected to several logical and/or virtual networks. Thus, before disconnecting, should conduct a logical acquisition of data related to logical connections. Make a decision on whether to collect or acquire potential evidence.

Table 10. Recommendation for improvements in cloud forensics

Straw Man's Network/Cloud	
Preparation	It is recommended that customers identify the additional data sources unique to the cloud service model.
Preservation	Preservation is the protection of the integrity of potential digital evidence. Potential digital evidence and digital devices must be safeguarded from tampering or spoliation.
Collection	Due to the multitenant nature of cloud infrastructures, acquisition should usually be preferred over collection to avoid impacts to parties not involved in the matter

that is unique to the cloud service model. In addition, potential evidence and digital devices need to be secured properly to avoid further tampering or spoliation. There is a need to consider the multitenant nature of cloud technology. It is recommended that acquiring the data should always be considered rather than collecting potential evidence. This is to avoid impacts to other tenants of the cloud.

After comparing the recommendations found in the knowledge base and the results of the straw man model's evaluations, the required improvements were evident. The straw man model's phases for network forensics were the same as the phases for cloud forensics. The evaluation results showed that these two types of digital forensics are completely different, with different investigation environments and requirements. As a result, for network environment investigations, identification should be implemented instead of preparation and collection/acquisitions, while cloud environment investigations should implement acquisition. The new and improved straw man model is now known as the multidisciplinary digital forensic investigation process model (MDFIPM), as illustrated in Figure 2.

Table 11. Summary of improvements for the straw man model

Straw Man's Network/Cloud	MDFIPM Network	MDFIPM Cloud
Preparation	Identification	Identification
Preservation	Collection/ Acquisition	Data Acquisition
Collection	Preservation	Preservation
Examination	Examination	Examination

As reflected in the name, the MDFIPM is designed for an investigation in a multidisciplinary environment. The main investigation path of the MDFIPM is the mobile forensics investigation path. Section 1.1. discusses the ACPO's principles of digital evidence as it showed in Table 1. The purpose of these principles is to preserve the integrity of the evidence. A similar model was proposed by the U.S Department of Justice (2001) with advice on how to handle electronic evidence in the crime scene. Table 12 compares instructions developed by the DoJ and ACPO (2007) on how to handle digital evidence.

To contextualize the context and the scope of the artifacts, this study endeavored to build a set of artifacts that can be applied in any jurisdiction and interpreted by the digital forensic experts to fit their requirements. The digital forensic experts can pick up the artifacts and apply the local legal frameworks, such as the 1995 Evidence Act in Australia, in order to preserve the integrity of the evidence. The model and the framework have been developed to guide a digital forensic investigator through a complex and difficult problem: how to execute a digital investigation that is compliant of the law, up-to-date, and efficient enough to address the information technology and the problem of cost to conduct the investigation.

Table 12. Handling electronic evidence at the crime scene*

DoJ - Standards	ACPO - Instructions
Recognition and identification of the evidence	Any interaction with the handset on a mobile phone could result in loss of evidence.
Documentation of the crime scene	Before handling, decide if any other evidence is required from the phone (such as DNA/fingerprints/drugs/accelerants).
Collection and preservation of the evidence	General advice is to switch the handset OFF due to the potential for loss of data if the battery fails or new network traffic overwrites call logs or recoverable deleted areas (e.g., SMS); there is also potential for sabotage.
Packaging and transportation of the evidence	However, investigating officers (OIC) may require the phone to remain on for monitoring purposes while live inquiries continue. If this is the case, ensure the unit is kept charged and not tampered with. In all events, power-down the unit prior to transport.

* Source: Ashcroft (2001). Available at https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

In the model (Figure 2), for instance, there are three divisions: the mobile device process, which is the main investigation path, and two other paths, network forensics on one side and cloud forensics on the other. The mobile device forensics investigation path can be used on its own, used together with one of the two secondary paths, or all three may be used together in an investigation.

4. Conclusion

The straw man model has been evaluated and reviewed in order to identify its strengths, weaknesses, and opportunities for improvements. The straw man has been put through a number of evaluations: effectiveness and efficiency evaluation, design evaluation and relevance, and rigor evaluation. These evaluations were run against the DS evaluation method together with the straw man attributes and properties.

The evaluation results clearly showed the weaknesses of the straw man model and the required improvements to be made as summarized in Table 11. Figure 2 shows the improved straw man model with its new name, the multidisciplinary digital forensics investigation process model. As shown in the literature, the digital forensic investigation has a complex nature, so it requires multidisciplinary skills and abilities. The professional significance of the multidisciplinary digital forensic investigation process model is that of greater efficiency and effectiveness in digital investigations.

References

ACPO. (2007). *Good practice guide for computer-based evidence* (Official release version 4). Retrieved from https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A new approach of digital forensic model for digital forensic investigation. *International Journal of Advanced Computer Science and Applications, 2*(12), 175–178.

Albano, P., Castiglione, A., Cattaneo, G., & de Santis, A. (2011). A novel anti-forensics technique for the Android OS. In *Proceedings of the 2011 International Conference on Broadband and Wireless Computing, Communication and Applications* (pp. 380–385). Piscataway, NJ: IEEE.

Almulla, S., Iraqi, Y., & Jones, A. (2013). Cloud forensics: A research perspective. In *Proceedings of the 2013 9th International Conference on Innovations in Information Technology* (pp. 66–71). Piscataway, NJ: IEEE.

Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. In *Proceedings of the Fourth Digital Forensic Research Workshop* (pp. 1–9). Available at http://www.dfrws.org/sites/default/files/session-files/paper-the_enhanced_digital_investigation_process_model.pdf

Birk, D., & Wegener, C. (2011). Technical Issues of Forensic Investigations in Cloud Computing Environments. In *Proceedings of the 2011 IEEE Sixth International Workshop on the Systematic Approaches to Digital Forensic Engineering* (pp. 1–10). Piscataway, NJ: IEEE.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence, 2*(2), 1–20.

Cusack, B., & Lutui, R. (2014). Up-dating investigation models for smart phone procedures. In *Proceedings of the 12th Australian Digital Forensics Conference* (pp. 53–63). Joondalup, Australia: Edith Cowan University Research. Online. Conference titles available at http://ro.ecu.edu.au/adf/143

Da-Yu, K., Shiuh-Jeng, W., Sharma, A., & Huang, F.F-Y. (2009). A case-oriented model of digital forensics on infected zombie computers. In *Proceedings of the 2009 2nd International Conference on Computer Science and Its Applications* (pp. 1–6). Piscataway, NJ: IEEE.

Dezfouli, F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F. B. M., & bin Shamsuddin, S. (2012). Volatile memory acquisition using backup for forensic investigation. In *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic* (pp. 186–189). Piscataway, NJ: IEEE.

Dresch, A., Lacerda, D., & Antunes, J., Jr. (2015). Design science research. In *Design science research: A method for science and technology advancement* (pp. 67–102). Cham, Switzerland: Springer.

Fang, J., Jiang, Z., Chow, K-P., Yiu, S-M., Hui, L., Zhou, G., et al. (2012). Forensic analysis of pirated Chinese Shanzhai mobile phones. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics VIII, 8th IFIP WG 11.9 International Conference on Digital Forensics, Revised Selected Papers: Vol. 383* (pp. 129—142). Heidelberg: Springer.

Freiling, F. C., & Schwittay, B. (2007). A common process model for incident response and computer forensics. *IMF, 7*, 19—40.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly, 30*(3), 611—642.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75—105.

Jansen, W., & Ayers, R. (2007). *Guidelines on cell phone forensics (NIST Special Publication 800-101)*. Gaithersburg, MD: US Dept of Commerce Technology Administration National Institute of Standards and Technology.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86)*. Gaithersburg, MD: US Dept of Commerce Technology Administration National Institute of Standards and Technology.

Lin, I. L., Han-Chieh, C., & Shih-Hao, P. (2011). Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone. In *Proceedings of the 2011 International Conference on Broadband and Wireless Computing Communication and Applications* (pp. 386—391). Piscataway, NJ: IEEE.

Martini, B., & Choo, K-K.R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation, 9*(2), 71—80.

McKemmish, R. (1999). What is forensic computing? *Trends & Issues in Crime and Criminal Justice, 118*, 1—6.

Mellars, B. (2004). Forensic examination of mobile phones. *Digital Investigation, 1*(4), 266—272.

Mohtasebi, S., & Dehghantanha, A. (2013). Towards a unified forensic investigation framework of smartphones. *International Journal of Computer Theory and Engineering, 5*(2), 351—355.

Palmer, G. (2001). *A road map for digital forensic research*. Retrieved July 6, 2014, from http://isis.poly.edu/kulesh/forensics/docs/DFRWS_RM_Final.pdf

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), 14—27.

Pollitt, M. (1995). Computer forensics: An approach to evidence in cyberspace. In *Proceedings of the National Information Systems Security Conference* (pp. 487—491). Available at http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA302547

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

Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. In *Proceedings of the 2006 Conference on Digital Forensics, Security and Law* (pp. 27—40). Maidens, VA: ADFSL.

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.

Sharma, H., & Sabharwal, N. (2012). Investigating the implications of virtual forensics. In *Proceedings of the 2012 International Conference on the Advances in Engineering, Science and Management* (pp. 617—620). Piscataway, NJ: IEEE.

United States Department of Justice National Institute of Justice. (2001). *Electronic crime scene investigation: A guide for first responders* (NCJ 187736). Washington, DC: U.S. Government Printing Office.

Yadav, S., Ahmad, K., & Shekhar, J. (2011). Analysis of digital forensic tools and investigation process. In A. Mantri, S. Nandi, G. Kumar, & S. Kumar (Eds.), *High performance architecture and grid computing* (pp. 435—441). Heidelberg: Springer.

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology, 3*(3), 17—32.