1-1-2012

# A Platform Independent Investigative Process Model for Smartphones

Frances Chevonne Dancer

# A platform independent investigative process model for smartphones

By

Frances Chevonne Dancer

A Dissertation
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
in Computer Science
in the Department of Computer Science and Engineering

Mississippi State, Mississippi

December 2012

A platform independent investigative process model for smartphones

By

Frances Chevonne Dancer

Approved:

| | |
|---|---|
| David A. Dampier<br>Professor of Computer Science and Engineering<br>(Director of Dissertation) | Rayford Vaughn<br>William L. Giles Distinguished Professor of Computer Science and Engineering<br>(Committee Member) |
| J. Edward Swan II<br>Professor of Computer Science and Engineering<br>(Committee Member) | Yoginder Dandass<br>Associate Professor of Computer Science and Engineering<br>(Committee Member) |
| Edward Allen<br>Associate Professor of Computer Science and Engineering<br>(Graduate Coordinator) | Sarah A. Rajala<br>Dean of the Bagley College of Engineering |

Name: Frances Chevonne Dancer

Date of Degree: December 15, 2012

Institution: Mississippi State University

Major Field: Computer Science

Major Professor: Dr. David A. Dampier

Title of Study: A platform independent investigative process model for smartphones

Pages of Study: 181

Candidate for Degree of Doctor of Philosophy

A properly conducted forensic examination is one of the most fundamental aspects of a digital investigation. Examiners are obligated to obtain the skills necessary to use forensic tools and methodologies and rely on sound judgment when analyzing a digital device. Anytime during this process, the quality of the methods, skills, and expertise of the examiner may be challenged, thus, placing the forensic value of the evidence collected during the process in jeopardy. In order to combat the potential challenges posed as a result of the forensic examination process, the digital forensics community must ensure that suitable protocols are used throughout the analysis process.

Currently, there is no standard methodology forensic examiners use to analyze a digital device. Examiners have made use of a model derived from the Digital Forensic Research Workshop in 2001 and the application of ad-hoc techniques has become routine. While these approaches may reveal potential data of evidentiary value when applying them to digital devices, their core purpose specifically involves the analysis of computers. It is not clear how effective these methods have been when examining other digital technologies, in particular Small Scale Digital Devices (SSDDs). Due to these

mitigating factors, it is critical to develop standard scientifically sound methodologies in the area of digital forensics that allow us to evaluate various digital technologies while considering their distinctive characteristics. This research addresses these issues by introducing the concept of an extendable forensic process model applicable to smartphones regardless of platform. The model has been developed using the property of invariance to construct a core components list which serves as the foundation of the proposed methodology. This dissertation provides a description of the forensic process, the models currently used, the developed model, and experiments to show its usefulness.

DEDICATION

First and foremost, I would like to give thanks to my Lord and Savior Jesus Christ, for with Him all things are possible. This research is dedicated to my family and the late Mr. Earl Thomas.

ACKNOWLEDGMENTS

The author wishes to express gratitude to the many people for all of their support and guidance throughout this process. Beginning with my husband, Mr. Daniel Keith Lopez Dancer, I would like to say thank you for all of the support and encouragement you have given me throughout the years. You never made it seem as if I neglected my family obligations, even though I did at times. Next, I would like to thank my entire family; you all have been my rock since the beginning of this process and without you, this would never have come to fruition. Dr. Dave A. Dampier, I would like to tell you how much I really appreciate you for supporting and guiding me through my educational, professional, and personal challenges. I would also like to thank Dr's Vaughn, Swan, and Dandass for serving as my committee members and offering invaluable advice regarding this research. This section would not be complete without thanking the following people: Dr. Gordon Skelton, Director of the Center for Defense Integrated Data and Chair of the Department of Computer Science at Jackson State University; Mr. Chris Staten, mentor, Dr. Peggy West, Instructor of Mathematics and Computer Science at Mississippi Gulf Coast Community College Jefferson Davis Campus and mentor; Dr. Ora Rawls, Security Officer at Jackson State University and mentor; Dr. Evelyn Leggette, Dean of Undergraduate Studies at Jackson State University and mentor. I would also like to thank all of my colleagues, past and present at the following state agencies: the Mississippi

Department of Environmental Quality (MDEQ), Mississippi Gulf Coast Community College, Jackson State University, and the Center for Defense Integrated Data.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

# CHAPTER I

# INTRODUCTION

The digital forensic discipline is considered to be in its infancy in comparison to its siblings and is uniquely evolving in that it must account for the recurrent changes in technology in order to preserve its progressive state. Over the past ten years, this area has made advancements toward developing standards, tools, and methodologies in order to object a similar formalism to the discipline as its predecessors. This has been made apparent in the recent increase in publications, conferences and research efforts focused around digital forensics.

Among these advancements is the division of the discipline into sub-disciplines. Researchers deemed this separation necessary due to the varying size and functionality of technological devices. These sub-disciplines are depicted in Figure 1.2. Of these, Small Scale Digital Device Forensics (SSDDF) demands the most rigor in that technological advances versus standards do not trend similarly, the demand for high performance compact devices has risen over the past decade, and the speed at which new models are released is inconsistent to the rate at which humans acquire the necessary skill set to perform analyses on these models adequately.

For these reasons, there is a need for a forensic process model customized for SSDDs, more particularly the smartphone. A vast number of forensic examiners have used the DFRWS forensic process model based solely on its immense acceptance or have

applied a similar ad-hoc approach to analyze SSDDs. Though these techniques have resulted in the discovery of data of evidentiary value, a model developed primarily for SSDDs is fundamental for the discipline to continue to advance. The forensic investigative process has been used since the induction of the digital forensic field and given the age of the discipline, this is not peculiar. Another reason researchers and forensic examiners are supportive of this detailed process is because it has not been shown to be ineffective. The objective of this research is not to demonstrate that this process is unsuccessful, but to build upon this process to construct a platform independent process model specific to smartphones. The need for different methodologies and tools to handle the dissimilar technologies within each sub-discipline has been recognized, and the use of Mathematics, Software Engineering, Digital Forensics, and Software Engineering will assist in supporting this hypothesis. Specific topics within these disciplines which will be useful are: the property of invariance, related research, experimentation with SSDD technologies, and human subject studies.

This chapter discusses the usage of specific terms in digital forensics literature by comparing and contrasting them and suggests a revised framework for the category of devices under the umbrella of the digital forensics discipline. The activities that define any digital forensic investigation are presented in Section 1.2 and the motivation for the direction of this research is discussed in Section 1.3. The initial proposed plan of research detailing the questions, goals and hypotheses is described in Section 1.4.

## 1.1 Digital Forensics

Computer forensics is an innovative area of computer science that is also referred to as digital forensics in various literatures. Due to its infancy, researchers, law enforcement, and those tenured in the field have faced significant issues developing standards and methodologies effectively. One of those struggles has been the development of a standard vocabulary. As a result, we find that "computer forensics" and "digital forensics" are often used synonymously due to their similar definitions. The author believes that this is done in error because by definition, as well as they are alike, they are dissimilar. Kruse and Heiser define computer forensics as

> " involving the preservation, identification, extraction, documentation, and interpretation of computer data" [27].

Digital forensics is defined by Palmer as

> "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" [34].

As can be seen, the definition for digital forensics has advanced over time to include potential evidentiary data from all electronic devices, not just computers. Proven scientific methods are also an important part of the process because the integrity of the digital data extracted may be questioned due to its volatile nature as well as the validity

of the results of the investigation [27]. It is also noticed that the activities involved in conducting a digital forensic investigation have been expanded to include key processes that were not included in Kruse's definition of computer forensics. Collection, validation, analysis, and presentation are all imperative components of the forensics progression. For these reasons, "computer forensics" has been encompassed as a category of "digital forensics".

The author agrees with Carrier and Spafford [9] on how the area of digital forensics should be divided with one exception, the addition of SSDDF. Digital forensics includes any investigative technique applied to any technology and is therefore divided into four major areas:

- Computer forensics: Collecting, analyzing, and preserving evidence on computers, laptops, notebooks, etc.
- Small Scale Digital Device Forensics: Collecting, analyzing, and preserving evidence on small digital devices
- Network forensics: Collecting, analyzing, and preserving evidence that is spread throughout a network
- Software forensics: Linking software or malicious code to its author.

The addition of SSDDF is vital and the significance of its addition is detailed in Section 1.1.2.

### 1.1.1 Computer Crime vs. Digital Crime

Just as "digital forensics" and "computer forensics" are used interchangeably throughout forensics literature, "digital crime" and "computer crime" are as well. The author believes that these words, although similar, are not synonymous. There has been debate over the definition of "computer crime". The Department of Justice (DOJ) defines computer crime as:

> "any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution"[16].

Some see this definition as too abstract because it could potentially include crimes that have nothing to do with computers being used or targeted for the commission of a crime. As an example, a criminal could use the computer to assist in locating potential victims with the intention of committing a heinous act against them. Under the DOJ definition, this crime would be categorized as a computer crime whether it is a terrorist bombing, stalking, or assault. But this classification would not be accurate because neither of the crimes mentioned above uses a computer to commit the act. In this situation, the computer would contain vital evidentiary data that would assist in proving that the suspected party had specific knowledge of the location of each victim. So this definition of computer crime is not as thorough as is needed for this discipline.

Kruse and Heiser defined computer crime by categorizing it in two different classes, either the computer itself is the object of the offense, or the computer is used to commit the offense. If the computer is the object of the offense, it is the target of the aggressor. Examples of this would be a user deliberately destroying the monitor by

defacing it, pouring liquid in the chassis, physically misusing the peripherals, or physically taking a weapon and damaging it. The destruction of the computer does not always have to be physical in nature. One could embed malicious code on the computer with the intentions of causing some unexpected action to occur. Although these acts are against the law, the author believes that they fall under the category of willful and malicious destruction of property and should not necessarily be classified as computer crimes. The intent of the perpetrator could also be to steal information from a specific computer. In this case, a particular computer is targeted and this action would also be categorized as an offense committed against the computer.

When a computer is used to commit an offense, then the target is one other than that physical computer itself. Because of this, various legal issues may arise. For instance, one could use the computer to launder money, spread viruses, commit software piracy, unlawfully copy media, participate in child pornography, blackmail victims, sabotage individuals, or recreate legal documents which are all illegal activities. No matter what resources are used to accomplish these tasks, they are illegal. As an example, one can send a threatening email over the network using a specific computer which is against the law. But it would still be illegal if the same person was to write the threatening note and personally deliver it to the intended victim. Although there may not be laws pertaining to computers in place to assist in deterring these types of crimes, there are punishments in place for the illegal actions committed using computers such as blackmail, money laundering, and forging documents.

There are instances where the computer is used as an avenue to gain information that will assist the suspect in the commission of a crime. Although it is not against the law to conduct research via the Internet, a well-developed forensic investigation can uncover these actions and extract evidence that can support or refute the position of the prosecutor. Following are several cases involving the use of computers to assist in committing a criminal act [14]. One will notice that the charges against each suspect are not considered computer crimes, but a computer assisted each in the commission of their crimes.

On September 26, 2007, Lan Lee and Yuefi Ge were indicted on charges of conspiracy to commit economic espionage. Their plan was to steal trade secrets related to computer chip design from their employer and pass them off as their own creations. The two formed a company called SICO Microsystems in order to develop the products and market them to other companies for compensation. Neither suspect has been prosecuted, but they both face up to 15 years in prison and a fine of $500,000.

Mark Wayne Miller faces a minimum of 35 years to life in prison for one count of the Sexual Exploitation of Children in Dayton, OH. Miller successfully persuaded minors to conduct themselves inappropriately on a webcam for his viewing pleasure. Without the knowledge of the minors, Miller would also eavesdrop on them by obtaining their passwords through phishing and then using the password to access their webcam through special software. In order to lure the girls, he would assume the identity of a teenage male in chat rooms and engage them in conversation. He was arrested on November 28, 2005 by the U.S. Marshals and remains in their custody.

In 2004, Larry Lee Ropp was indicted on charges of federal wiretapping for installing an electronic device on a company computer that recorded every key stroke taken by an employee. This was the first of such a case in the United States. Ropp faced a maximum of 5 years in federal prison.

Although these crimes are not considered computer crimes, they are still a part of the digital forensic process because evidence was located on a computer that supported the indictment of each suspect. With that, the author believes that there are three types of computer crime: crimes against computers, crimes committed using computers, and crimes committed with the assistance of computers. The definition of a computer-assisted crime is when a computer is used to aide in the commission of a crime by performing information searches and storing information pertinent to the crime in memory either actively or passively. The idea of computer-assisted crimes is vital to this research mainly because of the technology chosen as the focus.

"Digital crime" is not as often used in literature as "computer crime", but the author feels this is due to the non-standard vocabulary. At its infancy, researchers in this area of computer science developed preliminary definitions that did not keep pace with the evolving technologies. As technology advances, these definitions must be altered to accommodate those changes. Surprisingly, in the systematic review process, the author found no sufficient definition for "digital crime", so an attempt to provide clarity is as follows:

Digital crime

- Involves the use of any digital technology to commit a criminal offense.
- Involves any digital technology that is the target of a crime.
- Involves the use of any digital technology to obtain or store information for the exclusive purpose of committing a crime.
- Involves the unauthorized access, unauthorized use, dishonest manipulation or theft of information from any digital technology.

Following the same logic used when comparing definitions of "computer forensics" and "digital forensics", "digital crime" would encompass "computer crime" because the first three statements are derived from the definition of "computer forensics". The difference is the word "computer" is changed to "digital technology" in order to encompass *all* technologies whether past, present, or future.

### 1.1.2 Small Scale Digital Device Forensics

Due to the vast number of digital devices with the ability to perform various functionalities, digital forensics further categorizes devices by their physical size and operability as follows: computers, storage devices, and obscure devices. Examples of devices that are classified as computers are laptops, tablet PCs, desktop computers, and notebooks. A storage device would be a peripheral that stores digital data such as a flash drive, iPod, or external hard drive. An obscure device would be a Play Station Portable (PSP), Nintendo Gameboy, and any other portable gaming device [27].

Harrill and Mislan refined the device categories above by introducing the SSDD category described as

> "a small form factor device which utilizes permanent or temporary memory in conjunction with embedded chips to perform a variety of tasks" [19].

He established that the SSDD category would contain five sub-categories assisting in determining which device belonged in which category. The five sub-categories are Embedded Chip Devices, PDAs, Cellular Telephones, Audio/Video Devices, and Gaming Devices. These devices are all small and dynamic in nature which has made them difficult to evaluate and examine. From this category comes a sub-area of digital forensics called Small Scale Digital Device Forensics (SSDDF), which was established in order to provide the examiner with the capability to investigate technologies developed after the invention of the computer and future devices. This area focuses on the five sub-categories of SSDD. To provide a starting point for investigations, the devices in each category have to be classified with respect to the internal components of each.

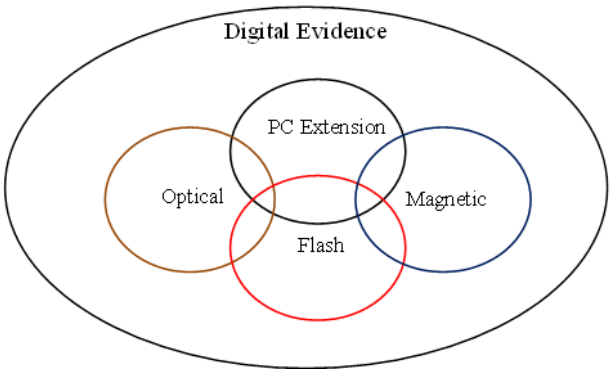


Figure 1.1 SSDD Framework and devices by type

Figure 1.1 is a revised version of the Harrill et al. classification of the SSDD Framework showing how devices store information. The difference is that based upon device breakdown, PC extension devices, flash devices, and magnetic drives can overlap. In the illustration by Harrill et al., the device categories only overlap with PC Extension devices [19]. The authors would also like to point out that Harrill et al. classify notebook computers and tablet computers as SSDD. The digital forensic framework suggested in this research by definition does not contain any devices that are considered computers, as can be seen in Figure 1.2. A computer can be categorized in all four groups: magnetic, PC extension, flash, and optical. This would mean that all four categories would overlap each other. However, the illustration depicts PC extension and flash devices overlapping while magnetic and optical devices never relate. This is not to say that the topology of the framework will remain the same. Allowances for future devices will have to be considered.

Harrill states that in order to be effective, the field of SSDDF will have to be handled differently depending upon the internal components of each device. These

devices can then be categorized and the type of forensics applied to each device depends upon how it is grouped. From this, it is obvious that a separate category for small scale digital devices is necessary due to the unique attributes of each. If separation from computers and the creation of a unique category was necessary for these types of devices, then a different framework for investigating them must be necessary as well. The key processes that define a digital investigation will still have to be present in the process model, but approached in a different manner [19].

Figure 1.2 depicts the digital forensic hierarchy as proposed by the author. The sub-disciplines are depicted in the rounded rectangles and the devices belonging to each are shown in the ovals. Software and network forensics are defined as sub-disciplines of digital forensics, however, defining any devices or processes belonging to each lies outside the scope of this research. Because there are aspects of each that may be categorized as part of another discipline, these rounded ovals are not fully contained by the digital forensic discipline.

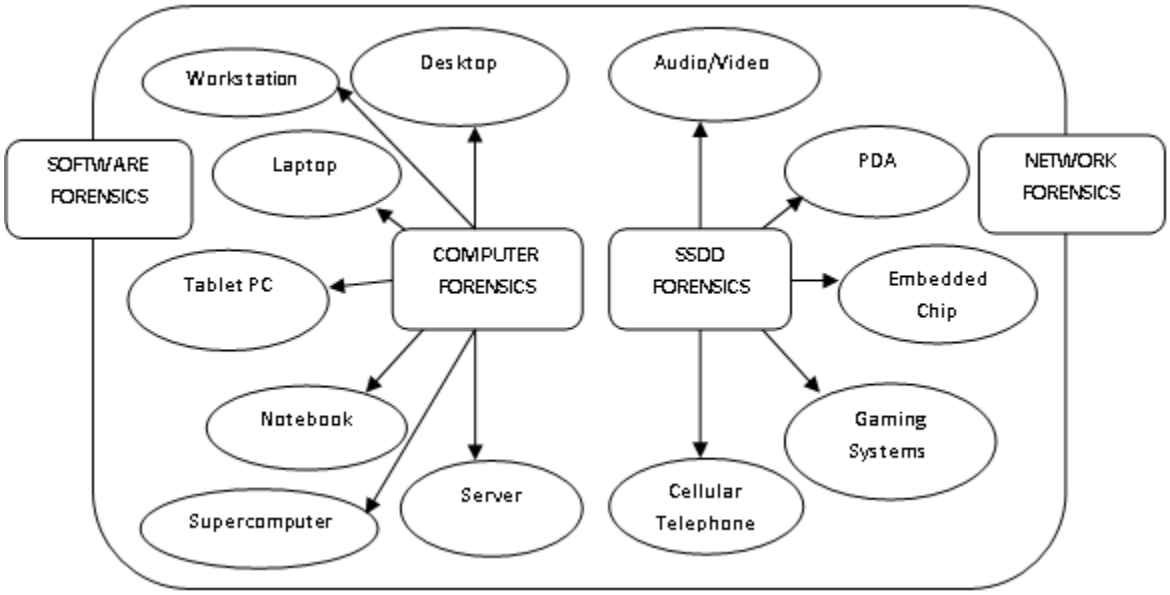


Figure 1.2 Digital Forensic Hierarchy and Devices

## 1.2 Digital Forensic Investigative Process

In order to be characterized as a digital forensic investigation, there are important aspects of the definition that must be considered. The definition mentions the following processes and activities that should be included in any digital investigative framework if not directly, indirectly: preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation. Their order has been altered to show the logical progression of an investigation from start to finish as depicted in Figure 1.3 and is influenced by the Digital Forensics Research Workshop (DFRWS) model. The DFRWS model is discussed in more detail in Section 2.1.

The processes are depicted as elongated rectangles at the top, and the activities are shown as rounded rectangles encapsulated by the processes. Every activity should include documentation, and therefore it is shown that this process encompasses all activities and

processes. The next process in the hierarchy is validation. It is our belief that validation should take place in every aspect of the investigation and should be documented, hence its place in the hierarchy. Considering preservation, the evidence should be accounted for in every core activity in the investigation so that validity can be shown, which is why all the activities are packaged directly under this process.

The following is the order of activities of digital forensics: identification, collection, analysis, interpretation, and presentation respectively. The results from the identification activity are passed along to the collection activity, which is shown by the arrow. The next three activities are shown as overlapping because performing the analysis and interpretation activities may lead the examiner to back track to the previous activity. Once this sequence of events has occurred, the results of the interpretation activity are provided to the presentation activity. After the key elements of the presentation activity are executed, the investigation is considered complete.

The following sections will discuss the processes and activities of a digital forensic investigation in detail. The author uses “activity” and “phase” interchangeably. There are some issues with the framework as is defined that will conflict with an investigation based on smartphones that are noteworthy. Some of these concerns are discussed briefly.

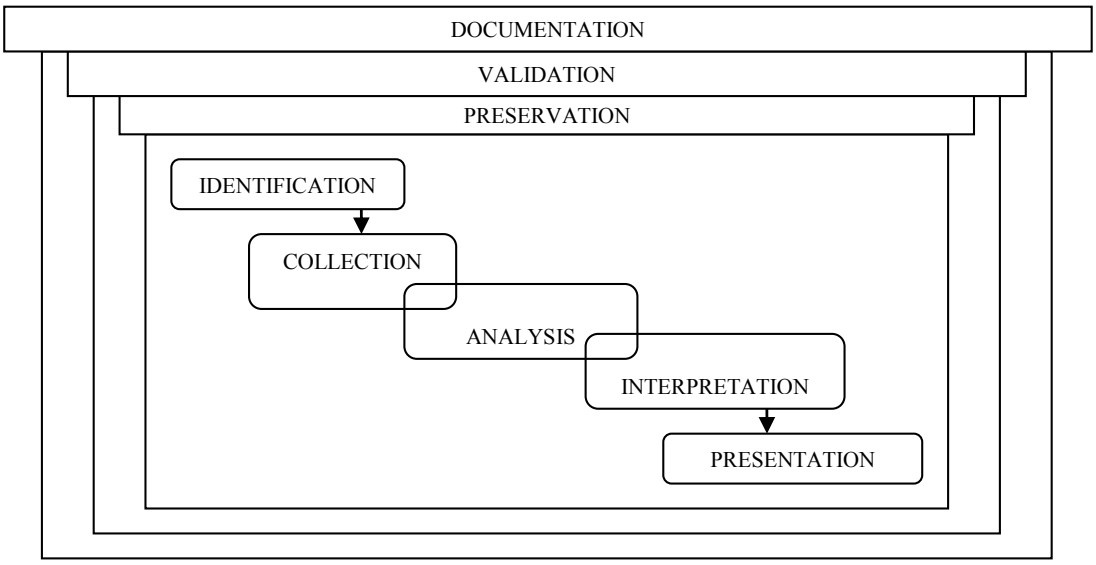


Figure 1.3 The Digital Forensic Process

### 1.2.1 Documentation

Documentation is not a stand-alone activity. It should be done throughout the progression of the investigation and is directly correlated to how successful the prosecutor assigned to each particular case will be. Labeling evidence, taking notes, sketching the crime scene, taking photographs, and using voice recording software are all categorized as documentation activities. These actions are all used in order to capture important details of the scene such as the types of software, version numbers, collection tools, the methodology used to collect the evidence, and explanations as to why certain things were done [27].

Taking photographs of the scene is as important as note-taking because when reviewed, a picture can reveal an important detail that the investigator would have otherwise missed. There have been many documented physical crime scene

investigations where the investigator analyzed photos of the crime scene in order to glean information that ultimately led them to new evidence in order to solve the case. Sketches are equally important to photograph-taking, but some believe it unnecessary. Sketches are essential because the investigation is seen from the viewpoint of another person. They may also depict elements of the scene not captured by a photograph. Voice-recording software can also be useful because it is more convenient for the investigator to record their thoughts real-time than to write word for word every idea that comes to mind. Emphasis is also apparent in a voice recording as opposed to written notes where it can only be implied [15].

Throughout every activity discussed in this section, it is noticeable that documentation is an essential part of each. In order to be able to provide an accurate account of the occurrences throughout the investigation, sufficiently documenting each action taken plays a key role. No matter which combination of documentation methods are chosen, as long as every action is accounted for in sufficient detail, the results of the investigation can never be discounted due to the methodology followed by the digital forensic team.

### 1.2.2 Validation

This activity, like documentation, is not a stand-alone phase. Validation occurs throughout the investigation because evidence is processed many times which increases the likelihood for errors to be introduced into the process. Contamination of evidence can be introduced several different ways. Environmental factors, nature, and human error can

all cause the composition of evidence to change. This lays the foundation for the integrity of the evidence to be questioned. Mold and dust are two environmental factors that can affect evidence by either altering the way it operates or its physical appearance. Insects, weather, and other elements of nature can not only alter evidence but damage it to a point where extracting meaningful data from the media is unlikely if not impossible. These circumstances can displace or even destroy the device as well as anything that has been extracted from it. If contamination is present, human error is the most likely culprit. Improper storage and inappropriate evidence handling are two factors that are controlled by humans. If evidence is mishandled, the chances that any of the factors mentioned can taint the evidence are probable. If tainted evidence reaches the court, reasonable doubt can be injected into the trial. The defense can suggest that the evidence was in a tainted state when extracted from the device due to mishandling or the methodology used by the examiner. If there is not sufficient documentation showing the state of the evidence before, during, and after extraction, the examiner will have nothing to refute the allegations of the defense.

There are several techniques that can be used to validate digital evidence, the most popular being hashing algorithms and time-stamping. A hash value of the original media can be created and then compared to the hash value of the copy. If the copy has been changed in any way, the hash will have a different value. Otherwise, the values will be the same. Time-stamping can be used to prove that a particular piece of evidence existed at a specific point in time. It can also be used to assist examiners in maintaining the chain of custody.

### 1.2.3 Preservation

The preservation process is conducted over the entire life of the investigation. The examiners are interested in conducting activities that will ensure the evidence is being handled properly in order to guarantee that little to no contamination has been introduced. These activities include but are not limited to maintaining the chain of custody, handling data sufficiently, transporting and storing evidence in the proper manner, and disposing of the evidence appropriately.

Digital evidence is processed by many different entities within a department. Not only does the digital forensic examiner have to process it, a different forensic specialist may have to inspect the device for traces of latent fingerprints. Evidence passes from hand to hand countless times throughout an investigation not only internally, but externally as well. This is where the chain of custody plays a major role. It pertains to documenting who handled the evidence at each point of the investigation. This is helpful because if an incident occurs, it would be known who had custody of the evidence before and after the incident. As long as there is documentation concerning every action that is taken which answers the questions of "who, when, what why, and how" as they pertain to the evidence, if contamination has been introduced into the process it should not hinder the investigation from proceeding.

### 1.2.4 Identification

Once a crime or suspicious incident has been detected, it is reported to the appropriate authorities. Depending on the severity of the offense and the interests of the

victim, law enforcement may become involved. Although legal involvement may not be imminent, those involved should proceed as if the results of the investigation will lead to the successful prosecution of the alleged suspect. After reviewing the preliminary findings, the investigation continues as authorities see fit for the specific circumstances.

When dealing with smartphones, more than likely, law enforcement will have initiated the investigation because it is their belief that the device may have taken part in the conduct of a crime or contains information such as the whereabouts of the person of interest at a particular time, known acquaintances, or communication between two people of interest. It is important to mention that an investigation on a smartphone is not always initiated due to a digital crime being committed. In a case such as this, the identification of an incident would have taken place before the investigator is aware that there will be a digital forensic investigation, and the smartphone is being examined to uncover information that may support or refute certain testimony. This also means that the physical investigation will be underway before the digital device is encountered. Due to this exception, the identification phase should take on a different meaning in a smartphone investigative process model.

### 1.2.5 Collection

The goal of this activity is to legally seize the devices involved and image the data from the devices. If the evidence will be used to prove or disprove a hypothesis in a legal setting, the investigator must ensure that all legal documents necessary for the seizure of the devices is in place. If the owner gives his consent those documents are unnecessary,

but consent can be withdrawn at any time and therefore it is safer not to rely on consent. If an investigator has neither the legal documents nor the consent of the owner and evidence is collected, it could be unusable in a court of law because the seizure was unlawful. There is no way the investigator will have knowledge of whether the case will be tried in a court of law, so it is important to obtain permission in every case whether it be from the suspect or the court. When dealing with digital devices such as smartphones, a search warrant will more than likely already be attained because these types of devices are usually discovered in the process of searching for evidence at a physical crime scene. If evidence is collected at the crime scene that may lead law enforcement to focus in a different direction, then the process repeats itself. In order to gain access to the belongings of another person, a search warrant has to be in place.

There are two legal exceptions to the warrant rule referred to as "a search incident to arrest" and "a search justified by exigent circumstances". The search incident to arrest rule states that law enforcement can conduct a search of the arrestee's person and their immediate wingspan at the time of the arrest without any suspicion whatsoever. This type of search is legal as long as the arrest is a valid one and the search is contemporaneous with the arrest [40]. An example of this exception can be found in case law. In the case of the United States v. Finley, the United States Court of Appeals for the 5$^{th}$ Circuit considered disallowing the search of a cellular phone that was seized upon the arrest of a suspected drug dealer. While a search warrant was being executed at the home of the suspect, a law enforcement officer examined the phone and found evidence that ultimately convicted the suspect. The defense attorney appealed the decision stating that

the evidence seized from the cellular phone was unlawful. The United States Court of Appeals for the 5th Circuit concluded the search lawful based upon the premise that the search was incident to the arrest of the suspect [48].

The second exception to the warrant rule is a search that is justified by exigent circumstances. This type of search is based on probable cause that the device or item contains evidence that may be lost if not retrieved immediately [40]. In the case of the United States v. Young, evidence linking the suspect to a drug ring was discovered on the cellular phone belonging to the defendant. Young appealed the decision of the court to allow the evidence collected to be presented to the jury. A law enforcement officer testified that the text messages and call logs contained valuable data that could be erased or overwritten by incoming text messages and calls. He also argued that some model phones empty the contents of its memory if its power source is depleted. The Fourth Circuit Court found that this argument was feasible and that the conditions surrounding the evidence collected on the phone were justified by exigent circumstances [49].

Both of these exceptions have only been applied in case law as there are no actual laws concerning digital devices such as these. These case laws are referenced by many court cases and the same conclusion is not always reached. This area is still developing and there are still many unanswered questions as protocol is concerned, Ryan suggests that if unsure, consulting the local prosecutor may be the best avenue when attempting to make decisions of lawful seizures when dealing with digital devices [40].

After the technicalities are handled, the investigator can proceed with seizure. Once the identification of potential evidence has occurred, the investigator will have to

make the decision as to whether he/she will image the device on site or whether the device must be taken back to the lab. Currently, there is no way to create a forensically sound image of a smartphone that would include the entire memory space due to issues specific to smartphones that are discussed in Section 1.3. Because this is a standard activity in the collection phase of a computer, different techniques will have to be used for this type of device. Currently, there are only a couple of ways a smartphone can be transported from place to place in the same state that it was in upon seizure. Smartphones have wireless antennas which cause changes to be logged upon receiving different signals from towers, other devices, or antennas. These changes could jeopardize an investigation and can be prevented by turning of the antenna capability of the phone. Another way to preserve the state of the device is to use a Faraday Cage. A lower cost alternative would be a shielding box [20]. The primary function of these is to prevent any outgoing communication from the phone by jamming the radio frequency. Incoming radio frequencies are not as important since there is a two-way handshake protocol used for two devices to communicate. If one is prevented from communicating then the connection will not occur. Smartphones should be seized and transported in a proper manner to the forensic examiner unless there is a mobile forensic unit equipped with the suitable tools. Throughout this entire process, documentation of every action is required.

### 1.2.6 Analysis

The analysis phase deals with actively examining each piece of evidence after it has been lawfully collected. If possible, it should begin with the examiner creating a

backup of the forensic image of the hard drive acquired in the collection phase in case something unexpected occurs to the original image. An experienced examiner will more than likely have a specific method by which he/she analyzes the drive for data pertaining to the investigation. If this is not the case, an analysis plan should be generated. Modern devices have a vast memory capacity and the capability to store more data continues to cultivate. We have seen this trend continue and as forensic examiners, we should expect it to in the future. For example, some smartphones have the capacity to store upwards of 160 GB of data. This is a vast amount of data to consider without having some systematic plan as to how the analysis will take place. Because these situations are time sensitive, there must be a practical approach to sifting through this amount of data to find the pertinent information.

Literature suggests that the success of any investigation relies heavily on the evidence discovered in this activity, which is why this phase seems to be the main focus of most forensic process models [12]. There has been much debate on whether exhaustive or constrained search methods will better suit examiners as well as the type of key word searches that should be used in order to search for evidence pertinent to the specific investigation. What steps should be done first when searching has been investigated as well, but no specific model detailing the order of activities is available. Most examiners use personal experience and the facts surrounding each particular case to decide in which order certain activities will be performed.

Bogen presents a methodology that models the computer forensics case environment in order to glean information from the facts available. From this domain

model, a structured method for extracting keywords to assist in planning an investigation was developed. In this methodology, concepts, relationships, and attributes are identified. Concepts are identified as high level entities that are relevant to the case and are described by zero or more attributes. Each concept is related to at least one other concept. Relationships are realized between concepts by understanding the associations between them and attributes are the characteristics that define a concept. Once these elements are identified, the model is assigned actual values. This process results in a structured list of keyword search terms that may increase the likelihood of the investigator successfully discovering evidence pertinent to a particular case. Several experimental trials and a pilot study show the methodology to be successful in the attempt to increase the quality of computer forensics investigations without significantly increasing the effort of planning [6]. This is one of many options available to the forensic examiner. Due to the numerous choices available, documentation becomes increasingly important.

### 1.2.7 Interpretation

This activity is closely related to the analysis phase and involves event reconstruction. Once the collection and analysis activities are performed, the evidence has to be interpreted in a way that will assist the investigator in building a case against the suspect based on what is found. In order to interpret it, the evidence has to be pieced together in a way that will prove a particular sequence of events took place in a specific order and left behind digital traces of data. Piecing together fragments of data will help to prove or disprove any hypotheses formulated by the investigator. The process can also

lead to the formation of new hypotheses that support how a sequence of events occurred and potentially tie the reconstructed event sequence to the identity of the suspect. There is no formal process model describing how the reconstruction of events should occur, but this area of research has seen increasing popularity.

### 1.2.8 Presentation

Investigators review their notes and prepare reports based on the conclusions of each investigation. Expert testimony may be necessary in which case the forensic examiner may have to testify based on the notes taken during the process. This is the reason documentation is extremely vital because the circumstances are too important to rely on memory, especially if the court hearing is delayed. Depending on the situation, hearings can be postponed for months, sometimes years. Human memory is not infallible, so it will be necessary for the examiner to refer back to his notes during preparation for the legal hearing. The defense will test the knowledge of the examiner as well as the methodology used during cross examination.

Tanner suggests using concept mappings throughout every phase of a forensic investigation. Making use of concept maps in the presentation phase allows the hierarchical relationships between the concepts of a court case to be presented in a more attractive and organized manner. Additionally, the physical documents and images can be attached to the concept maps where applicable. For example, if a search warrant was obtained, a copy of the search warrant can be added to the concept map in the preservation phase and made easily accessible. An advantage to using concept maps in

this phase allows law enforcement to present the case in a way that allows the court to know exactly what tasks were performed, when and why they were performed, what evidence was found, and the steps taken to ensure the chain of custody was maintained. Concept mappings would be very useful in court cases that are postponed. Because each person within the judicial system is faced with new cases containing vast amounts of evidence and information almost daily, it is difficult for them to pick up a cold case and effectively handle it with the same understanding as when they were actively dealing with the case on a daily basis. Concept mappings would alleviate any misunderstanding and refresh the memory of the investigator because of the story line presentation [45].

Not all investigations reach a courtroom, so results should be provided in a manner that can be understood by a person that is not fluent in the digital forensics area. It is not always appropriate to present the results formally. Oral and visual presentations may be more suitable in certain situations. An example of where these types of presentations may be used is if a company has an internal digital forensic team that discovered and investigated an incident. The board of directors may request a special meeting where the team communicates its findings. In this case, the team may decide that it is more appropriate to describe the events orally using visual presentation software.

## 1.3 Motivation

The number of mobile phones has grown exponentially over the last decade, and it is estimated that they will be the primary connection to the Internet and the principal means of communication by the year 2020 [11]. Evidence of this is apparent because we

have seen these devices replace the landline phone which has been a permanent fixture in households for decades. Mobile phones have also begun to substitute personal computers due to the incorporated functionality and comparable affordability with no loss of application, usability, convenience, and portability.

There are three types of mobile phones: basic, intermediate, and smartphone/personal digital assistant (PDA) [17]. Of these, we are particularly interested in the latter. Although more expensive compared to other types of mobile phones available, sales in smartphones during 2008 grew 75% from the previous year [11]. People have become increasingly fascinated with the smartphone due to its "all-in-one" capability which usually includes functions such as Bluetooth, Wi-Fi, multimedia messaging, instant messaging, PC syncing, data sharing, data streaming, document editing, gaming and GPS capabilities.

Three of the most popular smartphones are the RIM Blackberry, outfitted with the unique ability of pin-to-pin messaging; the Apple iPhone, equipped with a distinctive display capable of automatic toggling from portrait to landscape orientation; and the G1 with the Android OS manufactured by T-Mobile, capable of obtaining applications such as bar code scanners at no cost by downloading them from the exclusive Android market [39]. With the significant increase in sales, the growing popularity, and the prediction of growth for the future, the smartphone is most appropriate for the direction of this research. The rising use of smartphones is the reason forensic examiners must acquire and analyze these devices for evidentiary value when any criminal activity is suspected to have occurred. Attributable to the multiplicity of functions available, there is an array of

information to be obtained from the analysis of smartphones such as the identity of the owner, locale at specific times, habits, interests, call logs, contacts, text messages, emails, web browsing history, network information, and images [13, 17, 24, 25, 39, 41].

In order to obtain this information as evidence, the forensic examiner has to extract the data in a way that can be documented, is repeatable and testable so that his/her methodology is acceptable by the forensic community as well as law enforcement [1]. The examiner typically either follows the investigative process model presented by the Digital Forensics Research Workshop (DFRWS) that has become a widely accepted methodology amongst the forensic community, or uses an ad-hoc approach when attempting to analyze a smartphone [34, 35]. The dilemma with these approaches is that they are not well-matched for the forensic examination of such a device.

When developed, the DFRWS process model focused on the state of digital forensics in 2001, so mobile devices were not specifically considered in this process although there is mention of emerging technologies in its description [34]. This model could be used as a general guide for mobile devices, but there are some issues that have to be considered when dealing with these devices that this model does not consider. The major drawback of examiners using an ad-hoc approach is that the model may be subject to scrutiny when viewed by academia, law enforcement, and the judicial system due to the lack of peer-review, rigorous testing, and general acceptance. Therefore, the use of either approach may lead to non-discovery of data, questionable integrity and validity of results, or the loss of pertinent information when applying them to mobile device forensics.

Some of the issues unique to the examination of smartphones are as follows [8, 24, 36, 37, 41]:

- **Memory Type**: Data can be lost if an adequate power source is not available due to flash memory.
- **States**: A smartphone can be in any one of the following states: nascent, active, quiescent, or semi-active. The device is qualified as being in an off state only if the battery is removed.
- **Remote Communication**: Data can be altered due to wireless communication capabilities.
- **Proprietary Information**: The framework of the device is considered a trade secret and therefore not publicly available which makes it difficult for examiners to thoroughly understand the system.
- **Data-sharing**: Communication with other mobile devices via applications such as Bluetooth, pin-to-pin, and beaming can introduce uncertainties.
- **Lack of Standardization**: There are approximately 56 different manufacturers that produce a variety of phones with different platforms.
- **Technological Advances**: A different model smartphone is released about once every two years.
- **Grandfathered Model Support**: Older models are almost never phased out so the lack of standardization seems inevitable.
- **Connectors and Accessories**: A standard connector for all smartphones is not yet in existence so the examiner must obtain every accessory that accompanies the

device upon purchase. The investigation can be done wirelessly, but there is an increased security risk in doing so.

- **Tool Validity**: There is no mobile forensic tool that is widely accepted due to validity issues.

These, and other underlying factors, are why there is no investigative process model widely accepted that is independent of platform, manufacturer, or functionality for forensically examining a smartphone. The lack of standardization and the rise in the use of smartphones serve as the main motivations for this research. The author believes that utilizing the functionality of the hardware components of smartphones that have remained unchanged over the decades will assist in developing a methodology that overcomes some of the impediments previously mentioned. In the context of this research, anything that remains unchanged or anything that remains unchanged for long periods of time is said to contain the property of invariance. Invariance as it relates to smartphones is found in Section 3.1.

## 1.4 The Initial Proposal Plan

This section describes the initial questions this research will attempt to answer as well as the initial goals and hypotheses. The overall question that this research focuses on answering is:

*Will the Platform Independent Forensic Process Model (PIFPM) be more effective at identifying evidence when inspecting smartphones than the use of existing process models?*

This question will be answered by systematically reviewing the literature concerning the investigative process models in existence and conducting experiments based upon research. Models that are more likely to coincide with the unique issues concerning smartphones will be further examined to discover whether or not one is well-suited to analyze a smartphone. The following detailed questions help to motivate this research:

- As defined currently, is computer forensics the appropriate term to describe the forensic examination of all digital devices?
- Under what hierarchical category should smartphones fall?
- To what extent does invariance play a role in current frameworks?
- Are current process models sufficient for the examination of any digital device?
- Should devices be examined based on the components and capabilities of each?
- Should each category of devices under the proposed digital forensic framework have its own investigative model?
- Is there a direct correlation between the use of the platform independent model and the amount of evidentiary data found when applied to smartphones?
- Does the use of the proposed model significantly affect an investigator's capability to find data on a smartphone?
- Compared to the proposed model, do current models negatively affect an investigation dealing with smartphones?
- Do examiners familiar with smartphones perform significantly better than examiners that are not familiar with the devices when using the proposed model?

The high-level goal of this research is:

> *To provide forensic examiners and law enforcement with an extendable framework for the purpose of analyzing any model smartphone despite its characteristics using the property of invariance.*

This goal contains three areas of focus which include examining and understanding computer forensic investigative process models, examining and characterizing smartphone properties, and applying the property of invariance to the smartphone characterization. These three approaches will assist in the development of a platform independent smartphone forensic investigative model. The steps performed to accomplish this goal are as follows:

1. Review investigative process models and related computer forensics literature.
2. Identify candidate devices and obtain them for analysis.
3. Compare the characteristics of each device to identify the invariant properties.
4. Conduct experiments using the devices obtained.
    a. Obtain appropriate forensic tools
5. Construct PIFPM for smartphones
6. Evaluate the effectiveness of the proposed model
    a. Conduct case studies
7. Publish the findings.

Section 4.1 gives an overview of the refined research questions, goals, and hypotheses.

### 1.4.1 Methodology and Key Elements

#### 1.4.1.1 Review investigative process models and related computer forensics literature.

A systematic literature review has been completed in the area of digital forensics. This review focuses on investigative process models, the unique characteristics of smartphones including functionality and architecture, and the property of invariance. The reasons for the systematic review is to ensure the author is not performing studies that have already been completed and to apply what is learned to this research in order to assist in attaining the main goal.

#### 1.4.1.2 Identify candidate devices and obtain them for analysis.

This step is completed and a variety of smartphones and accompanying accessories are being received from several different sources including but not limited to family, friends, co-workers, E-bay, and devices donated by companies whether they are refurbished, malfunctioned, broken, or new. The reason all types of phones are acceptable is because the examiner may find himself or herself in a similar situation and the process model will need to acknowledge this. So far, the literature review has shown that no model currently exists that deals with these issues. The donors are guaranteed anonymity when publishing the results of the content found on the devices.

#### 1.4.1.3 Compare the characteristics of each device to identify the invariant properties.

In order to develop the platform independent process model, a baseline for the characteristics of smartphones was established. This basis concerns the properties of the devices that will not change. The knowledge gained from the portion of the systematic review that focuses on the architecture and functionality of different smartphones is

applicable at this stage. A model is an abstract construct that assists us in accomplishing a task. In order to be abstract, the model needs to be applicable to the majority, if not all, of the smartphones available. To accomplish this, a grouping of the devices must occur that separates them based on their internal components. This will allow the invariant properties each smartphone has in common to be incorporated into the proposed framework.

#### 1.4.1.4 Conduct experiments using the devices obtained.

The smartphones were examined using XRY to obtain information about how the OS of each reacts to certain user functions. The statistics obtained from each smartphone was compared and contrasted to the other devices in order to construct a manual model for examination.

#### 1.4.1.5 Construct new process model for smartphones

The next step in the methodology is to construct a process model that is platform independent using a combination of processes in other models as well as the results obtained in the previous steps. There is one precursor phase that the proposed model addresses that no other model has: Classification Phase. This phase contains two activities called Case Classification and Device Classification. Considering Case Classification, the examiner will need to be familiar with the type of criminal act that is suspected to have been committed. Once understood, it is more probable that the examiner will locate data pertinent to that particular case at a better rate than if not understood. If proven to be a more successful approach, this method could be injected into every examination of a digital device. As for Device Classification, the examiner will undoubtedly have to be familiar with the device. If not, the examiner could

potentially damage, overlook, or lose data of evidentiary substance. Particularly, smartphones will be classified based upon the functionality of their internal components. This classification may lead to an improved understanding of the device, which could cause the investigation to run more smoothly and the knowledge base of the examiner will be enhanced readying him for the next case involving smartphones.

#### 1.4.1.6 Evaluate the potential effectiveness of the proposed model

The next step is to conduct qualitative studies involving forensic examiners in order to gauge how effective this model could be in the field of practice. The results are recorded for future comparison to case study data. In order to ensure that the new investigative process model is an acceptable scientific methodology, further experimentation is needed.

#### 1.4.1.7 Publish the findings.

Using the results gathered from the case studies, forms, and surveys given to the participants, the author was able to gather metrics to assist in answering the research questions posed. From this data, observations for improving the proposed model are realized because the advantages and disadvantages of using this model as opposed to other models can be discussed. If the new process model is found to be a feasible approach, further discussion in the forensic community can ensue as well as the development of a forensically sound tool.

### 1.4.2 Hypotheses

The following hypotheses were formulated upon the start of this research:

1. *By refining investigative process models already in existence and examining smartphones of various platforms, a platform independent investigative process model can be developed using the property of invariance that will aid examiners in retrieving evidence while minimizing the potential for contamination.*
2. *By categorizing a device based on its internal components, the type of forensics that should be applied to the device will be obvious and an understanding of the device itself will be achieved.*

After the Initial Proposal Plan shown in Section 1.4 was discussed with the researcher's committee, it was decided that this research will give more information to us from a qualitative stand point and that the focus should be on understanding how useful and feasible it may be to inject PIFPM into a smartphone investigation and simultaneously attempting to learn as much about the current process as possible than carrying out the initial proposal plan. The original plan was to conduct experiments with forensic examiners to discover how much data they may find using PIFPM. Due to this shift in the research methods approach, a new specifically refined set of research questions and hypothesis were generated and can be found in Section 4.1.

# CHAPTER II

# RELATED WORK

There has been an increased interest in the theory involving forensic investigative frameworks over the last decade and with this interest has come various process models based on different techniques. This chapter presents an overview of the different investigative process models and frameworks, the origins of the invariance property and its relation to computer forensics, the characteristics and architecture of the most popular smartphones, as well as the challenges examiners face when dealing with smartphones.

## 2.1 Digital Investigative Process Models

Modeling is a comparatively new undertaking in computer forensic investigations, but it has been a critical part of several different areas of technology including computer security, networking, software engineering, high performance computing, visualization, and bioinformatics. Although the concept of using models in the area of technology is not newly realized, applying this theory to computer forensics has been distinguished as an innovative technique. The first widely accepted modeling technique developed for a digital forensic investigation was produced in 2001 at the Digital Forensics Research Workshop consisting of a conglomerate of academia, computer forensic examiners, analysts, and law enforcement. This investigative framework, deemed the DFRWS

model, has served as the basis for all forensic frameworks published since. The model, depicted in Table 1, consists of a linear process containing six categories each with a list of methods belonging to each category. The group believed that the items in gray were less confusing than the others and that this framework should serve as a basis to researchers to further revise the model and/or develop other process models [34].

Table 2.1 DFRWS Framework

| Identification | Preservation | Collection | Examination | Analysis | Presentation | Decision |
|---|---|---|---|---|---|---|
| Event/Crime Detection | Case Management | Preservation | Preservation | Preservation | Documentation | |
| Resolve Signture | Imaging Technologies | Approved Methods | Traceability | Traceability | Expert Testimony | |
| Profile Detection | Chain of Custody | Approved Software | Validation Techniques | Statistical | Clarification | |
| Anomalous Detection | Time Synch. | Approved Hardware | Filtering Techniques | Protocols | Mission Impact Statement | |
| Complaints | | Legal Authority | Pattern Matching | Data Mining | Recommended Countermeasure | |
| System Monitoring | | Lossless Compression | Hidden Data Discovery | Timeline | Statistical Interpretation | |
| Audit Analysis | | Sampling | Hidden Data Extraction | Link | | |
| Etc. | | Data Reduction | | Spacial | | |
| | | Recovery Techniques | | | | |

The definitions for each category are as follows [43]:

- Identification – An incident or crime has been reported to have occurred against a computer system, where a computer is used as an instrument, or a non-related computer crime where evidentiary information has been stored in digital form. From here, it is determined by interested entities whether it is feasible to continue with a computer forensic investigation.

- Preservation – Consists of a set of activities that are continuous throughout every category in the framework. These activities ensure that evidence maintains the chain of custody and is handled in a proper manner in order to withstand any analysis of validity that may be encountered in a court room.

- Collection – Deals with physically confiscating the computer and imaging the data from it using a computer forensic tool that makes a bit-for-bit image of the hard drive of the computer. There may also be other media that should be seized such as floppy disks, compact disks, flash drives, external hard drives, digital cameras, game stations,

- Examination – Focuses primarily on investigating the image created in the previous phase. Sometimes the forensic analyst may have to revert to examining the original data source as well in order to obtain relevant or other interesting data of evidentiary value that the bit-for-bit image lacks.

- Analysis – The output from the previous phase is analyzed in order to relate the digital evidence to the physical evidence and the events that occurred during the commission of the crime.

- Presentation – The last phase consists of the reporting process, whether it is formal or informal. Every investigation does not result in legal action occurring, but if so, the forensic investigator will have taken all the necessary steps in previous phases to account for this possibility. This process ends with written

documentation, oral presentations, and/or testimony submitted to the proper entities. These reporting procedures should be in a format that could be understood by the computer forensic community as well as those of different professions.

Although the framework is presented as a linear model, the investigative forensic process is non-linear. Every investigation is unique in some way so investigators may have to retrace a previous step in order to gain more insight, or because new information has been realized that would require the investigator to repeat a phase in the framework. Some of the concepts the DFRWS framework lacks are flexibility, iteration support, identification of information flows, obvious methods for testing, consideration of different digital architectures, and applicability to advanced technological devices [3, 7, 12, 37, 38]. Given this, the model was meant to be a basis for future work and has served as such. The models that will be discussed attempt to improve upon the DFRWS framework while using it as a baseline.

The following sections provide an overview of the investigative frameworks reviewed by the author. The frameworks are grouped based on the technique used to develop each model.

### 2.1.2 Objectives Based Approach

Beebe and Clark propose a model that focuses on theory and practice that includes lower order objectives-based sub-phases for each higher order phase. They argue that because previous models are single-tier higher order models that focus on the

abstract rather than the more concrete principles, the models fail to support inclusion of additional layers of detail.

In the proposed framework, the phases and sub-phases are distinct, discrete steps that suggest a sequential and sometimes iterative approach. Principles are guidelines and methodological approaches that overlap some or all phases. Principles represent goals and objectives throughout the entire process. This is applied to each objective and a six first-tier phase framework was developed with each phase containing several second-tier phases (sub-phases). The sub-phases were included so that this framework would be applicable to all possible types of crime and digital evidence. The sub-phases are meant to remain mostly consistent, but the activities within each sub-phase are detailed to the particular investigation. Figure 1 shows the overall structure of the proposed framework [3].

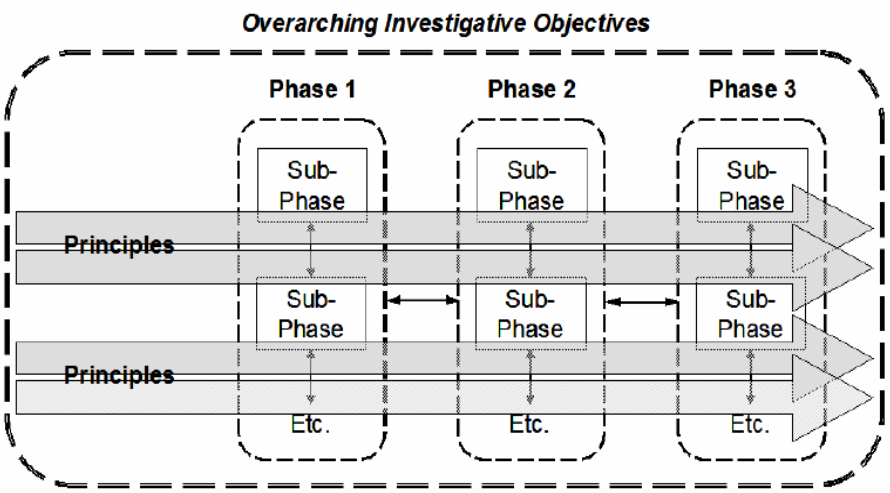


Figure 2.1 Beebe and Clark Framework

The first-tier phases are distinct, clearly defined, sequentially ordered phases that are a function of time and support loose iteration within an investigation. The six phases are presented as follows [3]:

- Preparation Phase: This phase includes any steps taken by an investigating entity

  > "to maximize the availability of evidence in support of deterrence, detection, response, investigation, and prosecution related to computer security incidents".

  There are several activities under this phase which are all focused on the target of the computer crime such as assessing risks, developing a retention plan, developing an Incident Response Plan, developing technical capabilities, training personnel, etc.

- Incident Response Phase: The detection and initial investigation of a suspected computer crime related incident. This phase is meant to detect, validate, assess, and determine a strategy to respond to the threat detected. Some of the routine activities of this phase are detecting the activity, reporting the detection, validating that the incident occurred, assessing the damage, etc.

- Data Collection Phase: The purpose of this phase is to collect digital evidence to support the strategy formalized in the previous phase. The Data Collection Phase activities are to complete a "live response" data collection, obtain evidentiary data from networks, hosts, and removable media, ensure the integrity of the data, and package, transport, and store the evidence, etc.

- Data Analysis Phase: The output of this phase will either confirm or refute whether an incident occurred, and answer the key questions that link the physical evidence to the digital evidence collected in previous phases. The activities of this phase are to perform some type of data synthesis in order to manage the volume of data collected, survey the evidence collected and profile the suspect skill-wise, use data extraction techniques, and reconstruct the data, etc.

- Presentation of Findings Phase: The purpose of this phase is to present the findings of the previous phase to all applicable parties. Depending upon who the findings are reported to will dictate how the information will be relayed. No matter how the information is communicated, it will have to be detailed, accurate, and comprehensible in order to be useful to the company, management, legal personnel, or law enforcement. There are no activities specifically defined in this phase.

- Incident Closure Phase: This phase focuses on the end of the investigation and the retention of knowledge and lessons learned in order to perform the next investigation more smoothly. The activities in this phase are to conduct a review of the process, act upon decisions from those findings, dispose of evidence properly, and collect all information related to the incident, etc.

Although a robust, flexible, and iterative alternative to the DFRWS framework, this model focuses on traditional computer and network forensics, there is uncertainty

about the applicability across all abstraction layers, OS specific renditions of the task hierarchy may be needed, and the model has not been rigorously reviewed by the computer forensic community.

### 2.1.3 Physical Crime Scene Based Approach

Carrier and Spafford propose the Integrated Digital Investigation Model (IDIP), a framework based on the process model that is used at physical crime scene investigations. The hypothesis is that using that process model as a basis, they can show that investigating a digital crime is more similar to investigating a physical crime scene than using the process for conducting a biological forensic analysis [10].

The model is composed of five categories of phases: Readiness Phases, Deployment Phases, Physical Crime Scene Investigation Phases, Digital Crime Scene Investigation Phases, and the Presentation Phase, of which the authors focused on the Digital Crime Scene Investigation Phases. This category consists of three major phases, the System Preservation & Documentation Phase, Evidence Searching & Documentation Phase, and the Event Reconstruction & Documentation Phase. The latter two phases contain sub-phases.

The System Preservation & Documentation Phase focuses on taking the proper measures to preserve the digital crime scene and documenting the state of the crime scene so that references can be made at a later time to ensure that nothing has been modified. If something has been modified, due to the documentation, it can be shown that a certain piece of evidence existed in the original state of the digital crime scene. The Digital

Evidence Searching and Documentation Phase deals with what digital devices contain information. This phase consists of four sub-phases described below:

- Target Definition: This phase defines a target to be used in order to locate evidence on the digital devices in question.

- Data Extraction and Interpretation: This phase deals with using a search pattern in order to extract data from the devices.

- Data Comparison: This phase compares the data extracted from the devices to the target set in the first sub-phase.

- Knowledge Update: Updates about the general knowledge of the investigation take place in this phase which allows more targets to be defined.

The goal of the Digital Event Reconstruction and Documentation phase is to develop hypotheses about the events that occurred in order to determine the underlying causes of these events. Thus, each piece of evidence is examined and a determination made as to what events that evidence was involved in to determine what events were a part of the digital crime scene. This phase contains five sub-phases presented below:

- Evidence Examination Phase: In this phase, each of the digital evidence objects obtained from the previous phase is categorized using their class properties and individualized using their individual properties. Any additional examination that needs to be conducted is done in this phase.

- Role Classification Phase: This phase deals with the hypothesis creation of the roles each digital evidence object was involved in based on the characteristics identified in the previous phase.

- Event Construction and Testing Phase: In this phase, cause and effect roles are grouped together in order to try to reconstruct the order of events in the digital crime. If other objects have to exist in order for an event to have happened, then the investigator searches for this object.

- Event Sequencing Phase: The goal of this phase is to place the series of events in order based on when they occurred.

- Hypothesis Testing Phase: The final phase deals with testing the hypotheses of the digital incident using the knowledge gained from the event sequencing phase. If the event sequence does not support the hypothesis then the conclusion must be that there is insufficient evidence to support that hypothesis.

The IDIP succeeded in its attempt to expound upon all earlier models, model the computer forensic process, and emphasize the process of event reconstruction which will provide researchers with insight on developing tools to help speed forensic examinations. The authors believe this model to be a more intuitive and flexible framework when compared with the DFRWS model even though most of the ideas are the same. Although they feel this model is of better quality, the authors agree that choosing a model to use is

a subjective process and mainly depends on the type of technology being considered as well as the type of investigation.

Nevertheless, this model has its disadvantages as well. It was pointed out by Baryamureeba and Tushabe that the model attempts to confirm an incident in the deployment phase even though a preliminary investigation has yet to be carried out. The framework can also be seen as too general and it is not clear how the investigator is to distinguish between the crime scene of the victim and that of the suspect [2].

Baryamureeba and Tushabe propose the Enhanced Digital Investigation Process Model (EDIP) which is based on the IDIP framework. The main difference is that it expands the deployment phase of the IDIP model to include both the physical and digital crime scenes in order to overcome one of the disadvantages of the previously proposed model. A new phase is also introduced that deals with tracing back to the device at the crime scene of the suspect that was used to commit the offense. Instead of having two different reconstructions, this model only deals with the reconstruction of events after all investigations have occurred.

The EDIP model consists of five major phases, each containing sub-phases with the exception of the Review Phase: Readiness Phases, Deployment Phases, Traceback Phases, Dynamite Phases, and lastly the Review Phase. The authors saw no need to alter the Readiness and Review Phases of the IDIP model, and thus remain unchanged in the EDIP framework. The goal of the Deployment Phases is to provide a way for an incident to be detected and confirm that the incident did indeed occur. These phases take place where the incident was detected. The Traceback Phases deal with identifying the devices

of interest after the primary crime scene is located. The Dynamite Phases seek to seize the devices found in the previous phase and analyze them. A description of each sub-phase belonging to the major phases is detailed below [2].

- Deployment Phases
    - Detection and Notification Phase: Deals with detecting the incident and reporting it to the suitable entities.
    - Physical Crime Scene Investigation Phase: Potential evidence is identified during the physical examination of the secondary crime scene.
    - Digital Crime Scene Investigation Phase: Potential digital evidence is identified during a digital examination of the secondary crime scene and if possible an assessment as to the extent of damage.
    - Confirmation Phase: The incident is confirmed and approval is given to contact the proper authorities in order to obtain any legal documents needed to further inspect the primary crime scene.
    - Submission Phase: The physical and digital evidence collected in the previous sub-phases are passed on to the proper individuals.
- Traceback Phases
    - Digital Crime Scene Investigation Phase: The primary crime scene is traced from the information obtained in the previous phase.

- Authorization Phase: Permission is given to further investigate and obtain more information.

- Dynamite Phases
  - Physical Crime Scene Investigation Phase: Potential evidence is identified during the physical examination of the primary crime scene.
  - Digital Crime Scene Investigation Phase: Potential digital evidence is identified during a digital examination of the primary crime scene and if possible time stamps of the incident.
  - Reconstruction Phase: Deals with identifying the most likely investigation hypotheses by reconstructing the events using the evidence gathered in the previous phases.
  - Communication Phase: Interpretations and conclusions of the evidence gathered in all previous phases are reached and presented to the appropriate entities.

### 2.1.4 Technology Specific Approach

Ramabhdran proposes the first investigative process model that is technology specific, the Windows Mobile Device (WMD) model, which consists of twelve stages. The goal of the model is to help organizations develop the appropriate procedures to follow when investigating a Windows Mobile Device while considering the unique

processes involved. Currently no other proposed model deals with the specific information flow of these types of devices. The twelve stages are presented below as well as a brief description of the events in each [37]:

- Preparation: Involves understanding the nature of the crime, preparing the necessary tools needed in order to examine the devices, forming a team and assigning roles to each member. Being knowledgeable of the different types of Windows Mobile Devices would be a favorable advantage.

- Securing the Scene: Deals with preserving the crime scene and ensuring that only those with authorized admission are allowed.

- Survey and Recognition: An initial survey of the scene is conducted as well as identifying potential sources of evidence. Once these activities have been accomplished, a search plan is formulated.

- Documenting the Scene: Involves documenting the crime scene properly which includes photographing the scene, sketching, and crime-scene mapping.

- Communication Shielding: Deals with ensuring that all possible network communication between the device(s) and any other device is severed and will not be re-established at any point during the investigation.

- Volatile Evidence Collection: A decision must be made at this point as to whether the volatile evidence will be collected on site or in the forensic laboratory. This is a unique issue to Windows Mobile Devices because they

are mobile which means that in order to operate they must run off battery power. Another issue is that these types of devices can be in more than one state at the time of collection. Depending on each individual situation, this decision must be made by the investigator.

- Non-Volatile Evidence Collection: Deals with collecting possible evidentiary information from supporting storage media such as flash drives, floppy disks, compact discs, digital video discs, external hard drives, etc.

- Preservation: Entails the procedures for the packaging, transportation, and storage of the all potential evidence.

- Examination: The contents of the evidence collected in the previous phase is examined in a forensic setting in order to acquire digital evidence from the devices and/or supporting media. Several sustainable activities must be incorporated in order to examine a manageable amount of information such as data filtering, validation techniques, pattern matching techniques and key word searches.

- Analysis: Deals with identifying how fragments of data relate to each other by determining the significance of the information obtained in the previous phase. A reconstruction of events takes place and conclusions are reached as a result.

- Presentation: This phase is no different from the Presentation Phase of the DFRWS model discussed previously.

- Review: This phase is similar to the Review phase in the IDIP and EDIP models discussed previously.

The advantages of this model are that it can be applied to any Windows Mobile Device; it is the first model to suggest that an investigation separate from the typical forensic investigation of a computer would be beneficial for smartphones due to their unique nature; and it offers a standard for the entire category of Windows Mobile Devices.

With every advantage, there are always disadvantages. The set of activities proposed in this model are incomplete. Although it serves as a standard for Windows Mobile Devices, future work is needed in order for the model to be applicable to the entire category of smartphones as well as other portable devices. Another disadvantage is that the model lacks rigorous testing in the computer forensic community and therefore practicality of its incorporation in a real–world investigation is questionable. Because the model is constrained to a specific technology, some may see this as a weakness. The author suggests that future work should be done by researchers to add procedures to the model and extend it in order to improve upon some of its limitations [37].

### 2.1.5 Based on Information Flows

Ciardhuain proposes the Extended Model of Cybercrime Investigations Model (EMCI) which explicitly represents the information flows of an investigation. Ciardhuain discusses two flaws in existing models: 1) None of them explicitly identify the information flows of an entire investigation; 2) The middle phases of a forensic investigation tend to be the main focus instead of the entire process. EMCI exhibits the waterfall technique in that activities two through twelve are permitted to backtrack to the previous phase if need be. There are thirteen activities which are described below [12].

- Awareness: This step alerts the organization that an investigation is needed and is usually initiated externally.

- Authorization: Approval is obtained in order to proceed with the investigation by acquiring the necessary legal documentation if needed.

- Planning: External to the organization, regulations and legislature will determine how the investigation will move forward as well as input from the policies and procedures of the organization.

- Notification: Alerting the suspect, victim, and other concerned parties that an investigation will proceed from this point.

- Search for and identify evidence: Locating evidence and classifying what data should continue to the next activity occurs in this step.

- Collection of evidence: Deals with the seizure of the evidence in a form that can be analyzed in a forensic manner.

- Transport of evidence: Evidence is transported in a proper manner to a location in order to be examined at a later time in.

- Storage of evidence: After transportation, the evidence must be stored in a suitable fashion.

- Examination of evidence: This step entails the same steps as all previous models.

- Hypothesis: A hypothesis of the events that occurred at the secondary crime scene should be constructed based on the evidentiary knowledge gained from the examination step.

- Presentation of hypothesis: The hypothesis formulated in the previous step is presented externally while internally, it will be provided to management so that a decision can be made concerning what action the company wishes to take.

- Proof/Defense of hypothesis: Validity of the hypothesis presented in the previous step will have to be proven using the appropriate methods.

- Dissemination of information: The distribution of information from the investigation occurs internally as well as externally. All data may not be

released due to the confidential nature of the information collected. Collecting this information and maintaining it for later is also a supporting activity in this step of the model.

Although the model is a general representation of the forensic investigative process focusing on the information flows of the entire investigation, it does have a few drawbacks. The model is constructed in the context of an organization so it must be applied in that fashion in order to gauge its usefulness. This means that the model has not been rigorously tested by a vast number of organizations or the computer forensic community.

### 2.1.6 Cost-Effective Based Approach

Overill et al. propose a framework that determines whether it is feasible to conduct a forensic examination of computers which will be referenced here as the Cost Effective Digital Forensics Investigation Model (CEDFIM). This model is based on establishing the costs to retrieve individual traces of digital evidence. Once these costs are established, it can be determined whether or not it is feasible to continue with the investigative process by comparing the total weight of each digital trace of evidence with the value **α** [33].

The overall concept involves the intuition of the digital forensic examiner whom would be responsible for ranking the relative costs of investigating each piece of digital trace evidence according to their resource requirements (man-hours, availability of tools,

etc.). This cost ranking is referred to as $\mathbf{T_1 \leq T_2 \leq \ldots T_{m-1} \leq T_m}$. From this cost ranking, the minimum cost path for the entire investigation can be defined as the permutation of $\mathbf{[T_1\ T_2\ \ldots\ T_{m-1}\ T_m\ ]}$ if all of the digital traces can be found and ranked. In order to determine whether the investigation should proceed, the weight ($\mathbf{W_i}$) of each trace of evidence ($\mathbf{T_i}$) is assigned by peer review or by default is set to $\boldsymbol{\alpha/m}$ where the value of $\boldsymbol{\alpha}$ is $0 < \boldsymbol{\alpha} < 1$. Then the weight ($\mathbf{W}$) of the entire investigation can be calculated by summing the weights of each trace of evidence. This value is then compared to $\boldsymbol{\alpha}$. If W is adequately close to α, this would show that the case is probably feasible. Else, the digital traces of evidence are likely insufficient to support the case.

From this, the authors developed the CEDFIM which encompasses a two-phase schema for executing the type of examination described above.

- **Phase 1:**
    - Enumerate the set of traces that are expected to be present in the seized computer based on the type of computer crime that is suspected of having been committed.
    - Assign investigation costs to each of the expected traces.
    - Rank the expected traces in order of increasing investigation costs.
    - Set up a Bayesian Network model for the hypothesis of the digital crime and run it with all expected traces present to get $\boldsymbol{\alpha}$, the evidential threshold value.
    - Set $\mathbf{W}$, the evidential weight estimate, equal to zero.
    - Set $\mathbf{W_{rem}}$, the remaining total of available weights, to $\boldsymbol{\alpha}$.

- For each expected trace, taken in ranked order:
  - Search for the expected trace.
  - Subtract the importance weight $w_i$ of the expected trace from $\mathbf{W}_{\mathbf{rem.}}$
  - If the expected trace is present add its importance weight $w_i$ to **W.**
  - If **W** is sufficiently close to **α** then proceed immediately to Phase 2.
  - If ($\mathbf{W}$ + $W_{rem)}$ is insufficiently close to **α** then abandon the forensic investigation.

- **Phase 2**
  - Run and analyze the full Bayesian Network model for the hypothesis of the digital crime as described by Kwan et al [28].

The CEDFIM is meant to be executed in tandem with the data collection phase of any forensic investigative process model. The advantages of this model is that it offers the ability for the forensic examiners to create templates of the traces of digital evidence that are expected to be found in a specific type of digital crime which could be used as a starting point for less experienced examiners, and organizations the ability to determine whether or not it is feasible to pursue the investigation cost-wise. One of the disadvantages of the model is that the judgment of the forensic examiner plays a major part in assigning values for ranking in Phase 1. If the examiner is not experienced or makes an error, then the results of the investigation are questionable. Another

disadvantage is that its performance depends upon the distribution of importance and cost. It performs best in cases where the cost is low than in cases when the cost is high, although the authors mention that this model should not perform considerably worse than an exhaustive search for digital traces.

### 2.1.7 Legal Approach

Andrew and Hailey present a process model for the analysis phase of the forensic process that focuses on the legal and technical aspects of the events in this process phase. This model contains two qualifying concepts: Level of Proof and Certainty of the occurrence of an Event. The "level of proof" states that all evidence should be scaled using a proof scale to determine the level of certainty reached regarding the crime and the culprit. Table 1 shows the different levels of proof. The "certainty of the occurrence of an event" deals with reconstructing the events that took place on the device. There are four possible outcomes to performing this reconstruction:

- The event can be shown to have occurred in a given manner
- The event can be shown to have likely occurred in a given manner
- It can be shown to be unlikely that the event occurred in a given manner
- It can be shown that the event did not occur in a given manner

Table 2.2 Levels of Proof

| Proof | Intuition | Probable Cause | Preponder-ance of Evi-dence | Clear and Convincing | Reasonable Doubt | Scientific Certainty |
|---|---|---|---|---|---|---|
| Evidence | Hunch, guess | Reasonable-ness of facts | Corroborated facts, eyewitness testimony, physical evidence, evidence interpreted by an expert | | | Precise facts, known accuracy |

Coupled with the two qualifying concepts are two principles, which serve as the foundation of the model, and five areas of examination, called "Laws". The five laws are not executed in sequence because some will have to be done simultaneously. The principles and laws are defined as follows [1]:

- Principle of Consistent Results: "A well designed system will produce consistent results from any given action unless corrupted by an outside force." This statement says that all processes applied properly should produce accurate results.

- Principle of Static Storage: "Data at rest will remain at rest unless accessed for a directed purpose." This statement says that the data saved in a system will not subjectively be changed by the system.

- Law of Association: "Data must be correctly associated with both the processes that created it and the source that initiated those processes." This law says that data should correlate with the process and the source that created it. The Law of Association has two parts, Process Association and Source Association.

- Process Association: Relates to associating the data with the process that created it.

- Source Association: Relates to associating the data with the source that created it.

- Law of Context: "Data can only be interpreted correctly in context." This law says that data can only be deduced in the overall context of the investigation. There are two categories of context defined in this model: Internal and External.

  - Internal Context: Relates to the context retrieved from data limited to the system environment.

  - External Context: Relates to all other information not defined by the Internal Context.

- Law of Access: "If must be demonstrated that the individual had access to the device at the time the data was created." This law says that the evidence must show that the suspect had access to the device by either general or specific accessibility. The two levels are General Access and Specific Access.

- General Access: Relates to the examiner obtaining evidence that the suspect had an opportunity to physically access the device when the data was created.

- Specific Access: Relates to correlating a specific user to a specific time to the device the data was created on.

- Law of Intent: "It must be demonstrated that the data was created as the result of an intentional action taken by the user. Conversely, the analyst must be able to refute any claims that the system was corrupted and controlled by an unknown agent." This law says that the evidence must or must not show that data exists on the device in question due to a deliberate action by the user.

- Law of Validation: "The integrity, authenticity, and accuracy of the data must be validated before it can be presented as evidence in support of conclusions and opinions." This law says that before data can be considered evidence, it has to be validated in the areas of integrity, authenticity, and accuracy.

The advantages of this model are that it provides a common terminology and helps to further promote the standardization of digital forensics and that it is broad and flexible enough so that other technologies can be incorporated into its framework. There are a few disadvantages that can be seen by the author. It is not clear how this phase will

tie into the other phases of the forensic investigative process and the model has not been rigorously tested by the forensic community.

Kohn et al. propose a three phase framework with a legal base as its foundation in order to produce forensically sound evidence to support in a successful prosecution. The framework incorporates many of the concepts of previous models and it claims that all phases in previous models can be incorporated into one of the three phases presented. The authors mention that these phases are no different from phases detailed in previous models. The activities belonging to each high level phase are defined as seen below:

- Preparation:
    - Standards used in the organization
    - Policies and procedures in place to assist in the investigation
    - Training
    - Legal advice
    - Notification to the correct authorities
    - Documentation of previous incidents
    - Planning
- Investigation:
    - Searching for and identifying evidence on a computer
    - Collection of the evidence from the computer
    - Transportation of the evidence to a secure environment
    - Storage of evidence collected at the scene
    - Examination of the evidence using the proper tools

- Analysis

- Presentation:
  - Presenting the analysis
  - Proving the analysis

The advantages of this model are that it offers a legal basis for the framework in order to focus on an examination that may result in being presented in a court room, and it is the most basic of all the models previously presented allowing adequate room for additions. The main disadvantages that the author realizes is that the straightforward three phase concept may be too basic to be utilized in a real-world environment and this model, as well as many others, has not been rigorously tested in the forensic community [26].

### 2.1.8 Technologically and Crime Independent Approach

Reith et al. present a framework that is abstractly defined from the previously presented models and boasts to be technology and specific crime independent while incorporating ideas from traditional forensics as well as the protocol for an FBI physical crime scene search. The components of the model and their definitions are as follows:

- Identification: Deals with recognizing an incident from indicators and determining its type.

- Preparation: Deals with the preparation of tools, techniques, search warrants, monitoring authorizations, and management support.

- Approach strategy: Deals with formulating an approach based on the potential impact of bystanders and the type of technology in question.

- Preservation: Deals with the isolation, security, and preservation of the state of physical and digital evidence.

- Collection: Deals with recording the physical scene and duplicating the digital evidence using accepted practices and procedures.

- Examination: Deals with locating and identifying potential evidence and documenting the process throughout.

- Analysis: Deals with the reconstruction of the evidence from the previous phase in order to draw conclusions about the events that took place.

- Presentation: Deals with the summary and explanation of the conclusions reached written for an audience of laymen.

- Returning Evidence: Deals with ensuring that all property is returned to its rightful owner.

The authors suggest that the model is advantageous in that it creates a consistent framework, can be applied to future technologies, uses a generalized methodology that can be used to relate technology to non-forensic examiners, and the potential for incorporating non-digital technologies is available. The disadvantages are that the model

may be too general for real-world usefulness, each sub-category of the model adds to its intricacy which could make it difficult to follow, and the model has not been rigorously tested by the forensic community [38].

## 2.2 Invariance

This section provides readers with information on the origins of invariant theory as well as how the concept of invariance applies to the fields of Mathematics and computer science. Section 2.2.3 describes how invariance has been used in digital forensics, how it will be useful in this research, and how it can be applied to assist in developing a digital forensic process model.

### 2.2.1 Invariants in Mathematics

Invariant theory was discovered in the nineteenth century by a German mathematician named David Hillbert [21]. His discovery helped to develop a branch of mathematics called abstract algebra and is one of the most important concepts in applied physics and mathematics. Invariant theory studies the symmetry of objects on algebraic varieties depending on how the effect functions. If an object is invariant, it is said to possess the property of invariance. For example, invariance of power means that after some transformation has occurred due to a surge of electricity and the power remains the same. Symons et al. define invariance in the physical context as follows [44]:

> "...after some transformation is performed, the result of a certain operation remains unchanged."

Invariant theory as it applies to mathematics exists in two forms: Classical invariant theory (CIT) and Geometric invariant theory (GIT). Classical invariant theory is the study of polynomials and their intrinsic properties. Below is an example of how invariants are used in polynomials [31].

The simplest example of a polynomial is the binary form. More accurately, the binary form is a homogeneous function of the variables $\mathbf{x} = (x,y)$, which can be either real or complex:

$$\mathrm{Q}(\mathbf{x}) = \mathrm{Q}(x,y) = \sum_{i=0}^{n} a_i \binom{n}{i} x^{n-i} y^i \tag{2.1}$$

The integer *n* is the degree of the form. Under the general transformation of variables: $(x,y) \to (a\tilde{x} + b\tilde{y}, c\tilde{x} + d\tilde{y})$, the polynomial (I) is mapped to a new polynomial, given by:

$$\tilde{\mathrm{Q}}(\tilde{x},\tilde{y}) = \mathrm{Q}(a\tilde{x} + b\tilde{y}, c\tilde{x} + d\tilde{y}) \tag{2.2}$$

An **invariant** of the binary form Q(**x**) is a function:

$$I(\tilde{\mathbf{a}}) = (\det \mathrm{A})^g I(\mathbf{a}), \mathrm{A} \in \mathrm{GL}(2) \tag{2.3}$$

depending on the coefficients of Q, which, up to a determinantal factor (detA), does not change (is invariant) under the action (II) of the general linear group, where:

$$\mathrm{A} = \begin{bmatrix} ab \\ cd \end{bmatrix} = ad - bc \tag{2.4}$$

is nonsingular, i.e. an element of some general linear group GL(2). A **covariant** is a function, depending both on its coefficients and on the independent variables

**x** = $(x, y)$. Therefore:

$$J(\tilde{\mathbf{a}},\tilde{\mathbf{x}}) = \det(\mathrm{A})^g J(\mathbf{a},\mathbf{x}), \mathrm{A} \in \mathrm{GL}(2). \tag{2.5}$$

where $g$ is the weight of the invariant (or covariant). The degree of $J$ is its degree in the independent variables, the order of $J$ or $I$ is its degree in the coefficients **a** of the equation.

CIT has several important applications including but not limited to dynamical systems, solution of non-convex variational problems, elasticity, molecular physics, modular forms, and computer vision [42].

GIT originated from the ideas of CIT and was developed in 1965 by David Mumford. It is used to construct quotients by group actions in algebraic geometry which are in turn used to construct moduli spaces. A moduli space is a geometric space usually referred to as a scheme containing rings, or an algebraic stack which defines the space for genus curves, whose points represent algebro-geometric objects of some fixed kind. The can also represent the isomorphism classes of algebro-geometric objects.

The author takes from this research the physical context of invariance and will be using the general definition to apply to the current research.

### 2.2.2 Invariants in Computer Science

The definition of an invariant as it pertains to computer science is based upon the same basic concept, 'change'. A predicate is said to be invariant to a sequence of operations if it remains unaltered by the transformation [46]. A predicate is a property that all elements of a set have in common. So the application of invariance in this sense says that after some operations have been performed on the set, the property has the same value as it did before the operations were performed on the set. In other words, the value of the predicate remains unchanged.

Invariants play a major part in reasoning about programs in terms of what they do not change. The theory of optimizing compilers, the methodology of design by contract, and formal methods for determining the correctness of programs all use invariants decisively. An example of the usefulness of invariants in a Post canonical system is the MU puzzles given below [22]:

> Suppose there are the symbols M, I, and U which can be combined to produce strings of symbols called words. The puzzle asks one to start with the axiomatic work MI and transform it into the word MU using in each step of the transformation one of the following rules:
>
> 1. Add a U to the end of any string ending in I.
> 2. Double any string after the M.
> 3. Replace any III with a U.
> 4. Remove any UU.

Using these four rules, is it possible to change MI into MU in a finite number of steps?

This question can be answered using invariance while applying the four rules above. We can look at the total number of I's in a string. Only the second and third rules change this number because rule two will double it and rule three will reduce it by 3. Now, the invariant property is that the number of I's is not divisible by 3.

In the beginning, the number of I's is 1 which is not divisible by 3. Doubling a number that is not divisible by 3 does not make it divisible by 3. Subtracting 3 from a number that is not divisible by 3 does not make it divisible by 3. Therefore, changing MU to MI cannot be achieved because 0 is not divisible by 3.

Much time could be spent applying the transformation rules given in the puzzle without considering using the invariant property. From the rules, we can see that the only way to get rid of any I's is to have three of them together, which is why our invariant property ended up being that the number of I's is not divisible by 3.

### 2.2.3 Applying Invariants to Digital Forensics

Currently, the author has found no research directly connecting invariants to any aspect of digital forensics. Although not documented or published, the idea of invariance has played a major part in the development of digital forensics. In order to develop a forensic process model, one has to study the invariant properties of the technologies in question as well as having a clear understanding of the software and architecture. The phases of the framework should be based on technological invariants, or details of the technology that are less likely to change than others. As an example, one of the activities

belonging to the examination phase of the DFRWS framework is to make a bit-for-bit image of the hard drive of the computer. From this framework, a forensic tool for imaging hard drives was developed. This leads the author to assume that the developers of the DFRWS model were dependent upon the fact that the hard drive of the computer will be an invariant property, that is, the composition and functionality of the hard drive will remain the same no matter the make or model. Otherwise, the framework as well as the forensic imaging tool would have to be redrafted every time the functionality and composition of the hard drive changed, which is not feasible.

Section 3.1 will show the importance of the invariant property in this research and will demonstrate its use in assisting with the development of the proposed framework.

## 2.3 Smartphone OS Architectures

The most popular smartphones are manufactured with Linux, Windows, Palm, Symbian, and RIM operating systems. This section gives a brief overview of each manufacturer including the characteristics of the devices and provides an illustration of the architectures of each as well as the generic hardware design for any smartphone [23].

### 2.3.1 Linux

Linux is popular mainly due to its open source operating system which can come preinstalled on the PDA or can be installed by the user. The platform is responsible for allocating and managing memory, creating and processing threads, ensuring communication between processes, interrupt handling, execute-in-place (SIP) ROM file

systems, RAM file systems, flash management and TCP/IP networking. The most popular Linux PDA is called the Sharp Zaurus. These devices have a Strong or ARM processor, a lithium-ion battery as the power source, built-in support for Wi-Fi and blue tooth, and security/encryption modules. The devices have Compact Flash and SD slots that also accept MMCs which is typically a standard of all modern PDAs.

The Linux architecture contains five layers: Application Programs, Utility Programs, System Call Interface Library, Kernel, and Hardware shown in Figure 2.2.

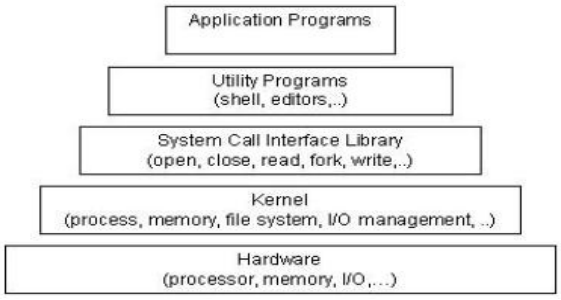


Figure 2.2 Linux Architecture

Security features that Linux offers include user identification and authentication, access controls on files that are permission based, logging activities, network encryption, separation of processes to prevent interference, and the ability to incorporate third party applications to help assist in the security of the data stored on the device.

### 2.3.1 Windows

Windows CE (WinCE) is the initial operating system for Windows Mobile Devices (WMDs). The functionality of WinCE was updated and the new OS was made

available called PocketPC (PPC). PPC runs on numerous processors but most WMDs either have XScale, ARM, or SHx processors. Most of the devices rely on lithium-ion batteries to maintain their power. When the power begins to deplete, the battery has to be recharged via the docking cradle or a power cable. The operating system and the applications are stored in ROM, and RAM contains the user data. If need be, RAM can be backed up to a space in ROM that has not been allocated. The kernel and other modules can be ported to a different processor by recompiling the code for a specific hardware and deploying it to that device. PPC also allows developers to decide whether certain services are included in the device.

There are four types of memory installed on a WMD: RAM, Expansion RAM, ROM, and Persistent Storage. Readers are already familiar with RAM and ROM so they will not be included in this discussion. Expansion RAM serves as extra storage or a backup to RAM. If the device has been powered completely off, Expansion RAM is mapped into virtual memory and is identical to the contents of RAM. Persistent storage is storage that is mapped into memory from removable media such as storage cards.

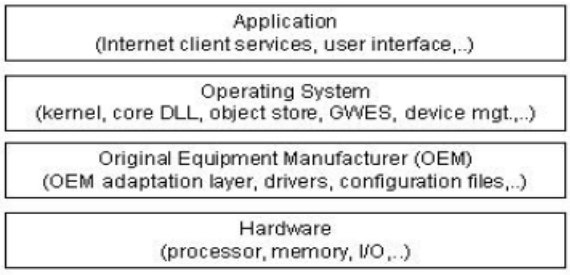


Figure 2.3 Pocket PC Architecture

The architecture of WMDs is categorized in four layers as can be seen in Figure 2.3: the Application Layer, the Operating System Layer, the Original Equipment Manufacturer (OEM) Layer, and the Hardware Layer. The OS Layer contains the kernel, the core DLL, the object store, the graphics, windowing, and events subsystem (GWES), and the device management. The GWES is the interface between the user, the application and the platform, and the object store contains the file system, the registry, and property databases. Property databases can serve as a valuable resource to forensic examiners because properties about certain applications are stored here. The OEM Layer writes functions for system startup, interrupt handling, power management, profiling, and the timer and clock. The hardware drivers and configuration files are also located in this layer. If any of the modules are ported to another device, the OEM Layer will have to write these functions in order for the OS to be operable.

The PPC offers several security features including the user ability to set a password between 4 and 29 characters long to be triggered once a cold boot has occurred. The user also has the ability to set a timeout that will lock the device once a specific time has elapsed. Biometrics has been coupled with some WMDs to be used in tandem with the set password, for example fingerprint technology. If implemented, only the fingerprint of the owner and the correct password set by the owner will allow access to the applications on the device.

### 2.3.2 Palm

Palm OS is the operating system offered by Palm PDAs and was for the most part based on the Motorola DragonBall MC68328 microprocessors and used alkaline batteries as their main power source. Newer models use StrongArm and XScale microprocessors and their power source is maintained using a lithium-ion battery. Similar to PPC, the operating system and the built in applications are located in ROM and the application and user data are located in RAM. There are also backups in place that copy the PIM data to parts of available ROM when requested or triggered. RAM and ROM are both organized by the OS onto one or more memory cards. The OS and the applications can be replaced by removing the memory cards and reinstalling new ones.

RAM is divided into two categories: dynamic RAM and storage RAM. Dynamic RAM is temporary storage and operates equivalent to RAM on a desktop computer while storage RAM is equivalent to disk storage on a desktop computer. Power is continuously applied to the memory of a PDA so if it is in low power mode, the contents of RAM remain intact. If the device has been reset, the equivalent of a warm boot, storage RAM is preserved but dynamic RAM is lost. If a cold boot is performed, both dynamic and storage RAM are lost.

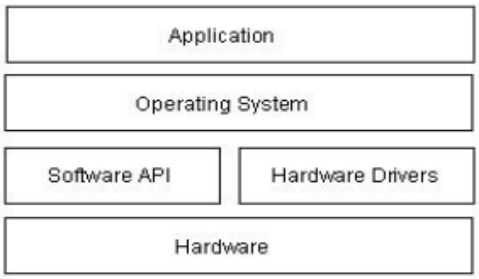


Figure 2.4 Palm Architecture

Figure 2.4 shows that the architecture of Palm PDAs contains four different layers: The Application Layer, the Operating System layer, the Software API and Hardware Drivers, and Hardware. The API allows applications to execute using different hardware and also allows a developer to directly access the processor by circumventing the API. This means that any application can gain access to the data stored on the device and modify it. This capability is a breeding ground for malicious code writers because the OS does not employ permissions on code or data.

There are several security features built-in to the OS to try to facilitate the protection of data stored on the device from unauthorized access. Users are able to lock individual records as private and they cannot be accessed unless the correct password is given. There is also the ability for the device to automatically lock when it is turned off. This would mean that no individual could use the device once it is powered on unless the correct password is given. Third party encryption applications can be installed on the device to help strengthen security.

### 2.3.3 Symbian

As of November 2008, Symbian is said to be the leader in the mobile phone industry with more than 46% of smartphone users. The Symbian OS supports a variety of interfaces from several different devices and was developed by Symbian Ltd. It also runs exclusively on the ARM microprocessors. As most smartphones to date, its power source is the lithium-ion based battery. These devices typically have 3 on-board memory types and one expandable option: RAM, ROM, Internal Flash Disk, and removable memory cards.

A Symbian device consists of a five tier architecture as seen in Figure 2.5. The UI Framework consists of applications for UI support and the UI Application Framework. The Application Services layer consists of multimedia protocols, internet and web application, content handling, client provisioning, messaging subsystem, PIM, and data synchronization. Both of these layers are driven by Java. The OS Services layer contains the core system services such as the generic OS services, communications services, multimedia and graphics services, and connectivity services. The generic OS services would be items such as event logging and task scheduling. The communications services deal with tasks such as telephony, short link, and networking. The multimedia and graphics services are the drivers for images, sounds, and video as well as printing. Lastly, the connectivity services deal with connecting the device to different devices and servers. The fourth layer is Base Services. This is the last layer that is reachable by the user and is referred to as the user side of the OS. This layer consists of low level libraries, character conversion, XML, persistent storage, user library, and a user side hardware abstraction.

The last layer is the Kernel and Hardware Interface layer which contains the kernel and the driver for the screen as well as other device drivers [29].

The Symbian OS has adopted a model that uses permissions per process instead of permissions per object. This means that software installed on the phone will not be able to change anything without being digitally signed and granted permission. Data caging is also used which means users can access a certain area of the file system. Third party anti-virus software can be integrated into the security model of a Symbian device strengthening it to withstand attacks [33].

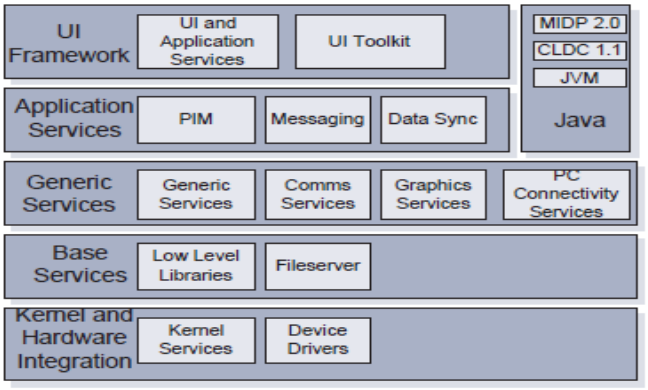


Figure 2.5 Symbian Architecture

### 2.3.4 RIM

Research in Motion (RIM) offers the Blackberry OS for its smartphone models with the latest series using the Intel XScale 624 MHz processor making them the fastest models to date. Older model smartphones used the Intel-80386 based processors. All current Blackberrys use a lithium-ion battery as their power source whereas in the past, some have used nickel-metal hydride batteries. These devices contain two types of

memory aside from expandable memory: flash and SRAM memory. All the applications of the device are stored in flash memory. Once the device is powered on, the OS and the modules take up a minimum of 10 to 15 MB depending on which version OS the device is running on. Flash memory also stores PIM as well as emails and data from the Java Application [4].

Figure 2.6 depicts the architecture of a RIM Blackberry device. The top layer is the Applications Layer which contains the Java ME applications (MIDlets) and the Blackberry IT applications. The next layer is the Java Classes and Frameworks which resembles the Java ME platform. The classes that manage the user interface are located here as well as the CLDC classes. This layer is also responsible for implementing Java Specification Request (JSR) API packages that deal with PIM, capture and playback, Bluetooth, and wireless messaging. The classes from this layer and the Applications Layer are loaded and executed by the Blackberry JVM which belongs to the Runtime Layer. The OS Layer then listens to the threads created to monitor device events [47].

RIM has included in its design several security features such as authentication controls, code signing, APIs with controlled access, an IT policy support, application controls, and file encryption on SD cards. They have also designed the Java Development Environment in a way that inhibits applications from accidentally or maliciously causing problems in other places on the device. Blackberry applications are only allowed to write to the device memory that the JVM uses. They cannot access virtual memory or persistent storage unless they are specifically granted that right.

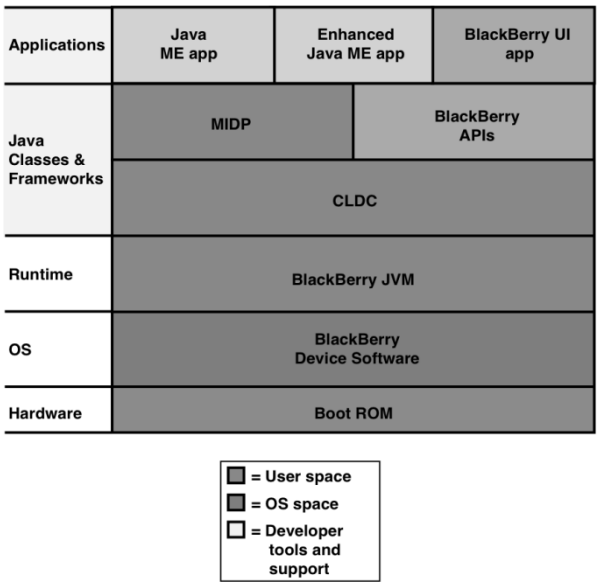


Figure 2.6 RIM Architecture

### 2.3.5 Generic Hardware Architecture

The hardware architecture is as equally important as the architecture of the operating system. [23] suggests that a generic design of a smartphone is as shown in Figure 2.7. The components in this figure are important to this research because it seems to support the list of smartphone core components the author suggests in Section 3.1. Some components are not a part of the list because the goal is to support past, present, and future technologies. As an example, all smartphones do not have cradle connectors. If this item were added to the smartphone core components, then the list would not be applicable across all model smartphones. But in order to support those models that do have cradles, the proposed process model will have to be extendable which means the smartphone core components list will not change but will have make allowances for innovative components.

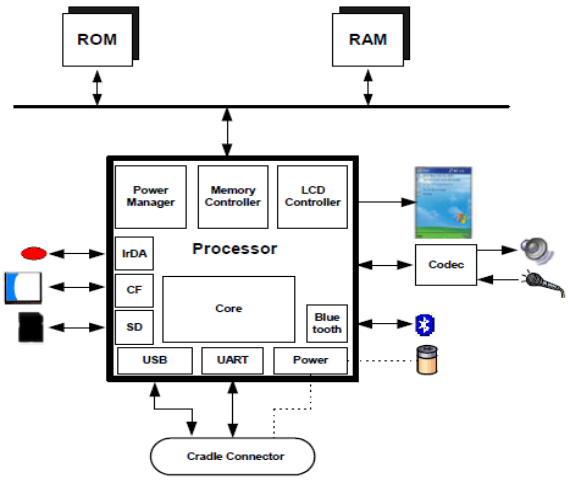


Figure 2.7Generic Hardware Architecture

CHAPTER III

THE PROPOSED MODEL

This chapter describes the methods used to develop the platform independent model as well as the model itself and is organized as follows: Section 3.1 describes the role invariant properties have in this research; and Section 3.2 presents the Platform Independent Forensic Process Model (PIFPM) and discusses its phases and sub-phases.

## 3.1 Invariance in Smartphone Forensics

In order to identify the role invariance will have when developing a framework for smartphones, the definition of a smartphone has to be understood. The following list will define what the author believes a mobile device must contain in order to be categorized as a smartphone:

- A connection to CDMA or GSM networks
- LCD
- Processor
- OS
- Personal Information Management (PIM)
- RAM and ROM
- File system
- Internet capability

- SIM/USIM
- Radio capability (Bluetooth, Wi-Fi, etc.)

The number of smartphones available today and the different functionality offered by each makes it impossible to develop a model specific to each device specification but applicable to all smartphones. Every model of smartphone undergoes changes at some point in its lifecycle due to technological advances and newer models being introduced at an alarming rate. Because of this, the features and functionality of the devices are very likely to evolve, but these changes do not affect the components of the device that classify it as a smartphone. To combat the lack of standardization, the proposition is to use the smartphone core components above to develop a model independent of functionality.

The researcher believes that the core components will be the same regardless of make, model, or functionality. To help support this idea, the Verizon Samsung Omnia and the RIM Blackberry Storm are compared to see if the specifications of each could be synthesized to the list of smartphone core components. Table 4.1 and Table 4.2 list the specifications of each device respectively.

Table 3.1 Omnia Specifications

| ***Verizon Samsung Omnia*** | | |
|---|---|---|
| **Software and Features** | **Hardware** | **Connectivity** |
| Operating System | Processor | Bluetooth |
| Microsoft Outlook Mobile | Display | Wi-Fi |
| Microsoft Office Mobile | Keyboard | 3G network |
| Microsoft Internet Explorer Mobile | Touch Screen | CMDA/ EVDO Rev A |
| Push E-Mail | Camera | |
| Windows Media Player | RAM/ROM | |
| Voice Recognition | Expandable memory | |
| Live Search | GPS | |
| Microsoft Auto | | |

Table 3.2 Storm Specifications

| ***Blackberry Storm*** | | |
|---|---|---|
| **Software and Features** | **Hardware** | **Connectivity** |
| Operating System | Processor | Bluetooth |
| Organizer | LCD Display | Wi-Fi |
| Corporate Data Access | QWERTY Keyboard | CMDA/EVDO Rev A |
| Browser | Touch Screen | UMTS/HSPA |
| E-Mail | Camera | GSM/GPRS |
| Media Player | RAM/ROM | |
| SMS/MMS | Expandable memory | |
| Speakerphone | Blackberry Maps | |
| | Video Recorder | |
| | GPS | |

To develop a rough standard architecture of the two, we can begin by comparing the devices to see what they have in common so that we can obtain our core components list. In the Software and Features category, the differences are mainly software applications. The Blackberry Storm does not have Microsoft software because it is a RIM device so we would not expect Microsoft Office, Outlook, Live Search and Auto to be a part of its specifications. As such, we do not expect Corporate Data Access to be a feature of a Windows Mobile Device. In the Hardware category, the only true differences are a video recorder and Blackberry Maps which are offered with the Blackberry Storm. As far as Connectivity, both offer Bluetooth and Wi-Fi capabilities as well as the CDMA and GSM (3G) networks. The difference is that the Blackberry Storm can connect to the UMTS network. After this comparison, the core components list is compiled as follows:

- OS
- Browser
- Email
- Media Player

- SMS/MMS
- Processor
- LCD touch screen
- PIM
- File System (not mentioned in specifications because the consumer would more than likely not be interested in this component)
- SIM (not necessary if phone is on CDMA network)
- Keyboard
- Camera
- RAM/ROM
- Expandable memory
- GPS
- Connection to a network
- Bluetooth and Wi-Fi

If the two lists are compared, it is noticeable that every element in the smartphone core components list has been included here. This list contains some components that are not in the core components list, which would allow the proposed model to be a more flexible model than those in existence in that it will be extendable. It will have the ability to include unique features of individual devices even though these characteristics are not present in the smartphone core components list. This means that even as future devices are developed with cutting edge capabilities, the proposed model will still be applicable. By comparing and contrasting the specifications of these two devices, the invariant

properties were recognized. In realizing this, the proposed model will be developed given the invariants of each model smartphone examined.

## 3.2 PIFPM

The Platform Independent Forensics Process Model (PIFPM) consists of five phases, each with its own set of sub-phases with the exception of the last phase. A similarity shared between PIFPM and the most popular forensic model, DFWRS, is that a Documentation Phase does not exist where as other forensic models include this as a standalone phase [34, 43]. Rather, documentation is an activity that takes place within each phase in the model and therefore should not be a standalone activity in any forensics examination. The phases of the model are as follows: Transportation, Classification, Analysis, Interpretation, and Retention.

The first phase of this model is the Transportation Phase. Of all the process models reviewed, only Ciardhuain outlines this as a standalone phase called the Transport Phase [12]. The Windows Mobile Device (WMD) model lists this as an activity to be completed within another phase, while most other process models omit it mainly because they were developed for the sole purpose of analyzing PCs [35]. Due to the nature of this research, transportation is necessary as an individual phase. Unlike a typical forensic investigation on a computer, an examination of a smartphone brings with it unique challenges that are difficult to manage for most examiners due to a lack of familiarity. Currently, there is no way to create a bit-for-bit image of a smartphone so the device will almost always require transportation from one location to another. Because of the ability

of these devices to communicate via radio waves, there is a chance for the contamination of evidence. Before the need to forensically analyze Wi-Fi capable mobile devices, this was not an issue. The following activities must take place in the Transportation Phase and are therefore referred to as sub-phases: Accessibility and Isolation.

The Accessibility Sub-phase deals with the investigator or examiner gaining access to the mobile device. Several smartphones are password protected and some are programmed to wipe the memory of the device if a password is guessed incorrectly a certain number of times. In this phase, the concern of the examiner is gaining access to the device in order to prevent the contamination of evidence from outside devices and to be able to perform analysis with a fair amount of ease. If the examiner is unable to obtain the password from the owner of the device or ascertain it some other way, conducting a proper analysis may be inhibited. The Isolation Sub-phase contains activities related to preventing any outside mechanism from manipulating the contents of the mobile device. This is usually accomplished by disabling the radio functionality of the device which can be achieved by locating the capability on the interface of the device and performing the task manually, or by using a Faraday bag or cage to render the Wi-Fi capability inoperable.

The purpose of the Classification Phase is to catalog the facts about the investigation and the mobile device in order to assist in determining the type of forensic tools needed for the analysis phase. The Classification Phase contains three sub-phases: Case, Device, and Tool. Details are gathered from several sources in the Case Sub-phase including but not limited to logs, reports, photographs, and investigators. Examples of

information that may be gathered here are the type of investigation, data about the suspect or person of interest such as physical addresses, known aliases, prior criminal history, education level, relationship to the victim, list of electronic devices owned, and any other personal information that may assist the examiner in his efforts. It may also be helpful to obtain details about the victim. This information is valuable for several reasons. If the forensic examiner knows the type of case the mobile device is suspected to be involved in, it is easier for him to determine what data found is potential evidence. Having a list of other electronic devices allows the examiner to make certain assumptions. For example, if the suspect has a notebook cataloged as one of his belongings, the examiner could assume that a backup of the data on the mobile device could exist on the computer and request that it be seized accordingly. As previously mentioned, part of the Case Sub-phase is collecting facts about the suspect. This type of information can be used to assist examiners in determining the type of rigor that should be applied to the investigation of a mobile device.

Next in the Classification Phase is the Device Sub-phase. This sub-phase compiles detailed information about the actual mobile device under examination. A modern smartphone usually has a SIM card, a battery, and sometimes a memory card. At the least, these things should be cataloged and stored separately from the device. The following is a list of all the information that should be gathered from the mobile device and its supporting components:

- Make and model of device or removable component
- Carrier

- Version number of OS
- Type of memory
- Amount of memory (used and free)
- Type of SIM
- Integrated Circuit Card Identification (ICCID)
- International Mobile Subscriber Identity (IMSI)
- Mobile Station International Subscriber Directory Number (MSISDN)
- PIN number if applicable
- International Mobile Equipment Identifier (IMEI)
- Mobile Equipment ID (MEID)
- Electronic Serial Number (ESN)
- Mobile Identification Number (MIN)
- Mobile Directory Number (MDN)
- MAC address
- List of all installed apps

The first six items in the list are standard for examiners to document and can usually be found with a fair amount of ease under "Preferences" or "Phone Information" on the device. If the investigator has subpoenaed the phone carrier, this information will be supplied within it. The ICCID is 10 byte number located on the SIM card uniquely identifying it. The IMSI can be up to 15 digits long and is used to uniquely identify the network of a mobile device user. The MSISDN is the assigned telephone number of the mobile device user. The PIN number is the Personal Identification Number and is most

easily obtained by requesting it from the owner of the mobile device. The IMEI number is a number that uniquely identifies the device itself and can usually be found on the underside of the battery. The MEID number replaced the ESN number on phones connected to the CDMA network and both uniquely identify a mobile device on the network. There are some hybrid devices that contain both an IMEI number and a MEID number. On the CDMA network, the MDN is the 10digit number assigned by the carrier to the mobile device user, and the MIN is the 10 digit number that uniquely identifies the mobile device to the mobile station and is derived from the MDN.

Documenting this information allows each device to be compared to the CCL and the ascertainment of items not on the list. The items not on the list are categorized as extendable items. By compiling a list of items non-similar to those on the CCL, a property that no other model can claim is afforded this one, extendibility. In order for any model to handle any device regardless of platform, it will have to be able to adjust with the incessant revolution in technology. Without this distinctive quality, any attempt at achieving that goal will fail.

The last sub-phase in the Classification phase is the Tool Sub-phase. It entails the examiner choosing the tool that he believes will be most effective when examining this particular device given the information collected in the case and device sub-phases and the lessons learned from previous examinations. In future experiments, the researchers hope to construct a list of tools that most suits a particular operating system from the least effective to the most effective based on the smartphone category tests presented in Table 4.5.

The Analysis Phase contains two activities: the Preliminary sub-phase and the Primary sub-phase. The purpose of this phase is no different from its purpose in existing models. The goal is to use forensic tools to gather evidentiary data from the smartphone that can be verified using reliable methods. In other models, verification is recognized as a phase. This model treats verification as it does documentation but with one distinct difference. Whereas documentation is required throughout each phase, verification is only required in the Analysis Phase. It is designed in this way because when dealing with smartphones, the focus of the examiner is on extracting data with the lowest possible probability for contamination and being able to show the process repeatable. Since this is the main focus of the examiner and this model, verification methods are discussed in this phase. The purpose of the Preliminary Sub-phase is to perform a non-invasive examination of the smartphone to reveal as much data of probable evidentiary value as possible. To begin, the examiner obtains the Preliminary Toolset generated in the Tool Sub-phase of the Classification Phase and follows the order given. Depending on the goal of the investigator and/or victim, the evidence uncovered using these tools may be all that is necessary to prove or refute a position. If it is proven or if the desire of the interested party is to continue with the forensic investigation, the examiner proceeds to the Primary Sub-phase. Conversely, if the need of the interested party has been met in the Preliminary Sub-phase, the examiner will proceed to the Interpretation Phase. At this point, the examiner could also make educated guesses to assist the interested party as to which path would most likely produce the desired results.

Verification techniques must be incorporated after each of these sub-phases. Because of the differences in the rigor of analyses conducted, the techniques must differ as well. Examples of the verification techniques for the Preliminary Sub-phase would be hashing methods, recreating the process and repeating the analysis using the same procedures on a different smartphone of the same make/model with the same internal components, or using a different forensic tool to obtain the same results. Only the latter two of these techniques would prove useful in the Primary Sub-phase. Using those techniques, the examiner can verify that the same results can be obtained. But because this sub-phase is more invasive than the prior sub-phase, additional precautions must be taken. Hashing methods will not assist in this situation because files have more than likely been altered. One way to combat this is to locate the log files on the smartphone before the analysis of the device. Once the log files have been duplicated, the analysis can proceed. After the analysis, the log files can be copied again and compared to the initial reproduction. Some manufacturers have specifications publicly available that provide information about how altering a file or application affects the log files kept in memory. Other companies consider this data a trade secret and can only be discovered through extensive experimentation. If these specifications are available, the log file behavior can be compared to the behavior described to determine adherence.

The next phase in the model is called the Interpretation Phase. The goal of the activities here is to establish a narrative that shows a link between the potential evidence passed from the Analysis Phase to the facts gathered in the Case sub-phase of the Classification Phase. More appealing to the investigator of the case would be the

establishment of a timeline of events which would link the evidence with a specific date and time stamp as well as location. Once the evidence has been associated with these elements, it is the responsibility of the investigator to interpret the results as he deems necessary. These activities constitute the Synthesis Sub-phase. The last sub-phase of this phase is called the Presentation Sub-phase and is similar to the last phase in most process models. This sub-phase will generate a report that takes the facts given in the Classification Phase, describes the sequence of events conducted in the Analysis Phase, and shows how the evidence is linked to locations and particular dates/times and presents it to the investigator or stakeholder.

The Retention Phase is the final phase in the model. At this point, the forensic examination of the mobile device has ended and the findings provided to the appropriate parties. The goal of this phase is to retain any lessons learned that can advance the examination process by making it more efficient at allowing the examiner to locate pertinent data in the least possible amount of time. By improving the examination process, this process model will progress as well. These enhancements can be documented in a number of ways, but the suggestion would be that each law enforcement agency create or maintain a wiki with a segment dedicated to mobile device forensics that can be revised accordingly after each examination.

Figure 3.1 depicts the PIFPM model. The five phases are shown in rectangles each encompassing the sub-phases shown in rounded rectangles. The order in which the sub-phases are entered is from left to right. The block arrows represent the flow of information from one phase to another and the dashed arrows represent one of two paths

that can be taken. The only instance of dashed arrows is in the Analysis Phase. Once the preliminary analysis has taken place, a choice can be made as to whether to enter the Primary Sub-phase or continue to the Interpretation Phase. The figure also depicts a solid arrow that initiates at the Interpretation Phase and terminates at the Analysis Phase. Once the evidence has been interpreted in the Synthesis Sub-phase, the examiner may find the need to revisit the Analysis Phase to repeat an analysis for verifiability of a result. It is also possible that the synthesis of information leads the examiner to another mobile device in need of analysis.

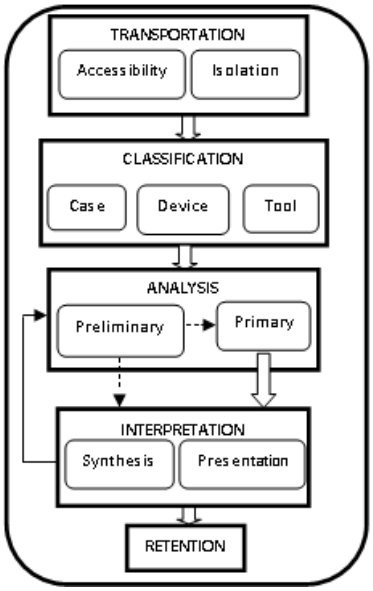


Figure 3.1 Platform Independent Process Model

# CHAPTER IV

# RESEARCH DESIGN

This chapter describes the proposed work which involves collecting data from a case study and experiments in order to determine the feasibility and usefulness of the proposed model as compared to other models. A survey has been developed and will be distributed to practicing forensic examiners in order to assess the feasibility of the logic flow and the order of the proposed phases as well as the necessity of each. In an effort to tailor the proposed model to the forensic examination of any smartphone, the researcher has conducted experiments in order to glean any trends in the data that will assist investigators in their efforts during the examination and analysis phases. Another focus is to determine whether there is a need for forensic process models specific to a certain category of devices. The remainder of the chapter is organized as follows: Section 4.1 discusses the research questions, the design, and analysis plan for the qualitative study and the experiments; and Sections 4.1.1, 4.1.3, and 4.1.6 describe the results.

## 4.1 Research Questions

The main goal of these studies is to gain insight into the feasibility and usefulness of the proposed model. Stated in GQM format, the goal is to:

*Analyze the Platform Independent Forensic Investigative Process Model in order to understand it with respect to usability and feasibility from the point of view of the forensic examiner.*

The studies focus on usability and feasibility because these qualities are correlated with helping us realize how successful the proposed model will be in assisting examiners with analyzing a smartphone. A collection of measurements from surveys, interviews, and observations involving these qualities will allow some basic comparisons between models to be performed in order to realize whether one model better suits the forensic examination of a smartphone as opposed to another. The questions and hypotheses that address this goal are:

1. *How useful is PIFPM in a smartphone examination?*

   **Hypothesis 1a**: Examiners with little to no experience will find PIFPM to be at least somewhat useful.

   **Hypothesis 1b:** Examiners with more experience will find PIFPM to be at least slightly useful.

   **Hypothesis 1c:** Examiners with little to no experience will be more likely to incorporate PIFPM into their forensic examination process than examiners with more experience.

   **Hypothesis 1d:** Examiners with more experience will be less likely to incorporate PIFPM into their forensic examination process than examiners with more experience.

2. *Is it feasible to include PIFPM in the current process for examining smartphones?*

**Hypothesis 2a:** Most examiners will find PIFPM to be at least somewhat feasible.

**Hypothesis 2b:** Most examiners will find that all the proposed phases fit the logical progression of a smartphone forensic examination.

**Hypothesis 2c:** Examiners, regardless of experience, will find that PIFPM is not difficult.

3. *Does PIFPM offer anything to a smartphone investigation that other models do not?*

**Hypothesis 3a:** Examiners with little to no experience will find that PIFPM has more strengths than weaknesses.

**Hypothesis 3b:** Examiners with more experience will find that PIFPM has more weaknesses than strengths.

4. *Is it logical to suggest that every category of technological device should assume a unique forensic process model?*

**Hypothesis 4:** Examiners, regardless of experience, will not find that it is very logical to use the same process model to examine smartphones and computers.

5. *Do examiners, whether intentional manually manipulate current process models in order to suit specific model smartphones?*

**Hypothesis 5a:** Examiners with little to no experience do not manipulate current process models often.

**Hypothesis 5b:** Examiners with more experience do manipulate current process models somewhat often.

The answers to these questions will assist in identifying the strengths and weaknesses of the proposed model while providing useful values to metrics that communicate the feasibility and usefulness of the model. Described in Sections 4.1.1, 4.1.2 and 4.1.5 are the Qualitative Case Study, the Quantitative Experimental Design, and the Qualitative Study Design respectively.

### 4.1.1 Qualitative Case Study

Because of what we do know about smartphone modeling, or the lack thereof, we have decided to use a mixed methods approach which will allow the researchers to explore the idea of how or if the development of an independent smartphone forensic process model will assist investigators in analyzing smartphones while providing some quantitative data about how specific model smartphones fair under certain conditions. The researchers will perform several different quantitative experiments on 5 different model smartphones of the following operating systems: Palm, Apple, RIM, Windows Mobile, and Android. These tests will allow the researchers to recognize patterns, if any, in the data and the proposed model can be tailored to include any themes that emerge.

The qualitative study reflects the genre of society and culture because the researchers are focusing on a particular group in order to develop a deeper understanding of their experiences as smartphone forensic examiners. Using interviews and surveys,

examiners' unique experiences, and personal interpretations of the current models, opinions on the feasibility and usefulness of the proposed model can be captured.

To begin the qualitative study, a pre-survey was disseminated to 115 forensic practitioners and researchers from various universities, governmental organizations, local and state law enforcement in Mississippi, federal law enforcement organizations, and one special task force group using internet ethnography that gleaned information such as gender, affiliation to digital forensics, and the number of years as a researcher or practitioner. From this method of dissemination, 20% of the total responded without any prior knowledge of receipt or prior contact from the researcher. Following the general inquiry are questions situated around smartphone forensics. The results of each question are given below.

The results of Questions 1 – 4 are detailed by participant in Table 4.1. Of the 23 respondents, 61% were male and 39% were female. The group of participants is almost equally divided into two groups, forensic examiners, instructors, or researchers and forensic students, at 48% and 52% respectively. Although the majority of the group has less than 2 years researching or practicing forensics, 44% of the entire group has at least 71 years of forensic experience combined. The participants have experience in examining or researching multiple devices including computers, laptops, smartphones, iPods, gaming systems, external hard drives, and thumb drives. At least 65% of the group has experience dealing with smartphones.

Table 4.1 Pre Survey Participants by Gender, Years Experience, and Devices Examined

| | *Gender* | | | *Device Examination* | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Partici-pant Type | Male | Female | Years Experience | Notebook | Computer | Smartphone/ Cellphone | iPod/ MP3 | Gaming System | Other |
| FE1 | | x | 7 – 9 | x | x | X | | | |
| FE2 | x | | 10+ | x | x | X | x | x | |
| FE3 | x | | 7 – 9 | x | x | | | | |
| FE4 | x | | 10+ | x | x | X | x | x | |
| FE5 | x | | 3- 6 | x | x | X | x | x | |
| FE6 | x | | 10+ | x | x | X | x | | |
| FR1 | x | | 0 - 2 | x | x | | | | |
| FI1 | x | | 7 – 9 | x | x | X | | | x |
| FI2 | x | | 3 - 6 | x | x | X | | | |
| FI3 | x | | 7 - 9 | x | x | X | x | x | |
| FI4 | | x | 7 - 9 | x | x | X | x | x | x |
| FS1 | | x | 0 – 2 | x | x | | | | |
| FS2 | | x | 0 – 2 | | x | X | | | |
| FS3 | | x | 0 – 2 | | x | | | | |
| FS4 | | x | 0 – 2 | x | x | | | | |
| FS5 | | x | 0 – 2 | | x | X | | | |
| FS6 | | x | 0 – 2 | x | x | | | | |
| FS7 | | x | 0 – 2 | x | x | | | | |
| FS8 | x | | 0 – 2 | x | x | X | x | | |
| FS9 | x | | 0 – 2 | x | x | X | | | |
| FS10 | x | | 0 – 2 | x | x | | | | |
| FS11 | x | | 0 – 2 | x | x | X | x | | |
| FS12 | x | | 0 – 2 | x | x | X | | | |
| Total | 14/ 60.9% | 9/ 39.1% | >71 | 20/ 86.9% | 23/ 100% | 15/ 65.2% | 8/ 34.8% | 5/ 21.7% | 2/ 9% |

Next, Question 5 asks the participants to place the activities of the proposed model in order as it pertains to which is performed first. If they felt that an activity did not fit the logical progression of a smartphone investigation, this would be denoted by "NA". On the other hand, if the participant believed the activity should be done throughout the investigation, this would be denoted by "TO". It was not revealed to the participants where these activities were derived so as not to introduce bias to the study. The activities were presented to the participants in random order. Although the participants were given the option to answer with "NA" or "TO", the given answers will first be compared to the list below. Then, the answers from the participants will be compared to the list below with Activities D and K listed as activities to be done

throughout the examination. Below, each activity is presented in the order in which the authors believe each should be performed and will be referred to in this section as its corresponding letter assigned to it.

ACTIVITIES

A. Gaining Access to the device
B. Omitting wireless communication capability
C. Transporting the device
D. Gathering supporting evidence such as case logs, files, suspect info, etc.
E. Recording device specific information such as make/model, IMEI, etc.
F. Determining a tool for forensic examination
G. Verifying the preliminary findings
H. Verifying the primary findings
I. Interpreting the findings
J. Presenting the findings
K. Retaining information about what was successful/unsuccessful about the investigation

With respect to the order that the activities in the proposed model should occur, at least 22% of the participants agreed with the authors ordering in 6 of the 11 activities presented with the highest percentage agreeing that Activities A, G, H, and J should be the first, seventh, eighth, and tenth activities performed, respectively at 26%. The activity with the least amount of participants agreeing with the authors concerning where it should lie in terms of order was Activity E.

Given that a significant amount of participants listed activities D and K as items that should be performed throughout an investigation, the authors decided to deviate from the proposed list and oblige the participants. In doing so, the participants agreed with the authors ordering in 9 of the 11 activities at a rate of 22% or above with the highest percentage agreeing that Activity I should be the eighth activity performed at a rate of 39%. Similarly, 35% of the participants agreed that Activity H should be performed seventh and that Activity D should be performed throughout the investigation. The activity with the least amount of participants agreeing with its order is Activity E. 9% of the participants agreed that this activity should be performed fourth. Refer to Figures 4.1 and 4.2.

The purpose of Question 6 is to ascertain whether or not the participants believe that the phases of the proposed smartphone forensics model fit within the confines of the DFRWS model. The participants were not told that the column headers were phases of the DFRWS model and neither were they told that the row headers corresponded with the phases of the proposed model. The definition of each activity and phase was provided to the participant. It has been concluded by the authors that the participants believe that two activities should occur throughout the examination: Documentation and Chain of Custody. At least 52% of the participants believe that documentation and chain of custody should occur in every phase.

As for the remaining activities, the authors believe that the DFRWS model is not well suited for examining smartphones because the activities are not clear as to how digital devices, particularly smartphones, other than computers should be handled:

Accessibility, Isolation, Device, Preliminary, Primary, Retention, and Validation. Of the 23 participants, 4% agree with the authors in that Accessibility and Device are not properly handled in the DFRWS model. 9% believe that the Preliminary phase is not represented in the DFRWS model; 13%, 22%, and 22% agree about Validation, Primary, and Retention.

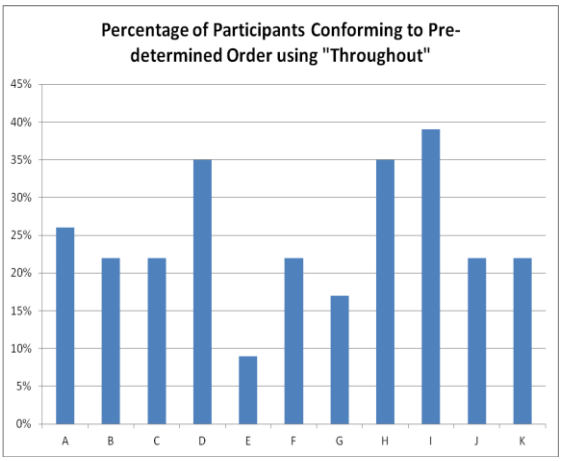


Figure 4.1 Percentage of Participants Agreeing with Authors' Altered Progression of Activities using throughout

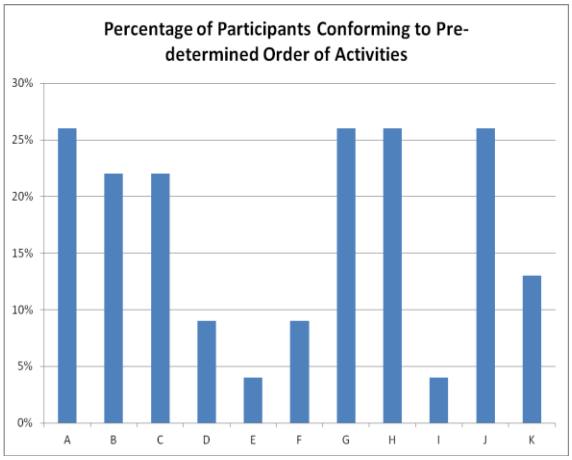


Figure 4.2 Percentage of Participants Agreeing with Authors' Original Progression of Activities

If certain information had been disclosed to the participants, the authors believe that more would have agreed that certain activities would not belong in certain phases. Because the DFRWS model was created specifically for computers, some of the language, such as "computer", was removed from the definition of the phases as not to present the element of bias.

Question 7, as seen in Table 4.2, dealt with the logical progression of a smartphone examination. The participants were asked to identify which phase in the DFRWS model did not fit the logical progression. The phases were listed in the order in which they are presented in the model. At least 83% of the respondents believe that each of these phases should be accounted for in some way in a smartphone model.

Table 4.2 Question 7 Frequency/Percent Table by Group

| **Q7. Of the phases listed, are there one or more phases that do not fit the logical progression of a smartphone examination? Is so, please choose all that apply.** | | | | |
|---|---|---|---|---|
| Option | FE Group Distribution Frequency/Percent | FR Group Distribution Frequency/Percent | FI Group Distribution Frequency/Percent | FS Group Distribution Frequency/Percent |
| Identification | 0/0% | 0/0% | 0/0% | 2/16.6% |
| Preservation | 0/0% | 0/0% | 0/0% | 3/25.0% |
| Collection | 0/0% | 1/100% | 0/0% | 2/16.6% |
| Examination | 0/0% | 0/0% | 0/0% | 2/16.6% |
| Analysis | 0/0% | 0/0% | 0/0% | 2/16.6% |
| Presentation | 0/0% | 0/0% | 0/0% | 2/16.6% |
| No Response | 6/100% | 0/0% | 4/100% | 9/75% |

Table 4.3 Question 8 Frequency/Percent Table by Group

| **Q8. Of the phases listed, are there one or more phases not listed that should be added in order to better fit the logical progression of a smartphone examination?** | | | | |
|---|---|---|---|---|
| Option | FE Group Distribution Frequency/Percent | FR Group Distribution Frequency/Percent | FI Group Distribution Frequency/Percent | FS Group Distribution Frequency/Percent |
| Yes | 0/0% | 0/0% | 0/0% | 2/16.6% |
| No | 1/16.6% | 1/100% | 2/50% | 3/25.0% |
| No Response | 5/83.3% | 0/0% | 2/50% | 7/58.3% |

Question 8, as seen in Table 4.3, dealt with phases that may be missing and should be added to better fit the logical progression of a smartphone. One participant answered, “Transporting”. Another participant answered, “The biggest problem with cellular phone forensic examinations is the multitude of devices on the market (both) current and previous. Not every, or any, forensics device has the capability to capture every phone, resulting in most examiners needing access to multiple tools…” 26% of the responses were either “no” or “n/a” and the remainder of the participants did not respond.

Since this study focuses on the experiences and thoughts of the forensic examiner, there are several different settings that are appropriate. In particular, conferences that

focus on topics related to forensics, law enforcement agencies (both state and nationwide), colleges and universities. These sites are realistic for the researcher because entry will not be difficult, there is a rich mix of people and experiences present at each particular site, some of the examiners are familiar with the researchers so a trusting relationship has already somewhat been established, there will be no issue in the study being conducted ethically, and the chance that the quality of data collected credibly is highly likely given the reasons listed previously [30]. Potential examiners will receive a formal letter requesting their voluntary participation. A sample of the letter can be found in Appendix C.

Regarding sample size, qualitative research case studies have been performed using one person and others have been performed using an entire organization. The sample size of this case study was determined according to the number of participants who fit the criteria of being a professional smartphone forensic examiner and were willing to take part in the study. Because of these reasons and other issues such as timing, the sample size will be no more than 5. Based on the exploratory research being conducted, the researchers have decided to use a mixed sampling type strategy of maximum variation and combination sampling. Maximum variation will allow the research to document the different variations observed during data gathering and allow any common patterns to be realized. Using a combination approach will allow the researchers to be flexible and use triangulation to verify some results or underlying themes observed. The researchers are mindful to be reasonable when considering size, strategy, and complexity due to the resources available [5, 18].

The role of the qualitative researcher is to consider technical and interpersonal considerations. Of the technical aspects of the study, the researchers have decided that their roll will be as complete observers/interviewers. They will not interfere or engage the participants in any way while in their environment. This has been decided so as not to project the beliefs of the observer onto the participant. Another technical aspect that has to be decided is how much about the study the researcher will reveal to the participant. In this case, the researcher would not be able to conceal that there is a study being conducted because some of the settings require special permission to gain access. In being provided this entry, the researcher will have to give legitimate reasons for wanting to gain entry. It has been decided that the participants as well as the agencies will be aware of this study. The problem with full disclosure is that people tend to behave unnaturally which may skew the results of the study. In order to defend this, the researchers will have to note when such behaviors present themselves. In doing so, results that are determined to be outliers may be explained by the unnatural behavior of the participant.

As far as role intensiveness/extensiveness, the researchers will be as minimally intrusive as possible and will only be present at the setting for a short period of time. We estimate that the longest period of time spent at one setting will be no longer than two days depending on the schedule of the participant. As mentioned earlier, the researchers are already familiar with some of the participants in the study from previous interactions and have already built a rapport with them. Because of these reasons, gaining access to

the sites will be less problematic than usual and there will also be less chance for tension between researcher and participant.

Some of the interpersonal considerations of a qualitative study include building trust and rapport, reciprocity, and ethics. Trust and rapport have been discussed previously. Reciprocity usually presents itself whether formally or informally. It can come in the form of volunteering for a cause of interest to the participant, providing feedback, tutoring, and other forms. Because this research is an area of extreme interest to the researchers, volunteering to assist would be of no issue. The researchers could also include other small tokens of appreciation. Regarding ethics, the participants will be provided with an informed consent document detailing that their participation in the study is entirely voluntary and that they will be allowed to exit the study at any point. The participants will also be informed that any information given by them will be guarded as sensitive and that the informants' privacy will be protected. They will also be provided the contact information of both researchers as well as the IRB contact for Mississippi State University in case any questions may arise. Appendix D gives an example of the informed consent form given to the participants in the study. As far as risks taken by the participants, the researchers anticipate that the issue in which we will have to deal with the most is anonymity. This may create an issue due to the sensitive nature of the participants' profession and the sensitivity of the data collected by each. To alleviate this, pseudonyms will be used in the place of actual names and organizations.

The researchers plan to use a variety of data collection methods which include note-taking, in-depth interviewing, and surveys. In conducting field interviews, the

researcher will go to each participant and task them with answering a series of questions concerning their forensic routine when examining a mobile device. Then the participant will be given an overview of PIFPM model and allowed to ask questions. The researcher will take note of the questions. Upon completion of the interview, the researcher will provide each participant with a survey. If there are an abundance of unanswered questions, the researcher will conduct an in-depth interview. The topical interview approach will be used so that the participants' views about the topic should unfold unbiased by how the researchers feel about the topic.

The benefits of using this approach are that the researchers gain immediate clarification, they can follow-up with the participant instantaneously, and the researcher can understand the meanings of the examiners' everyday activities. The limitations to this approach are that the participants may be uncomfortable, the interviewer may not ask the questions that are reflective of the insight she would like to gain, the interviewer may not interpret responses correctly when analyzing the data, the participants may choose to be untruthful, and scheduling will have to be done around the participants daily routine [30].

In order to manage the data collected, there will be coding processes used, such as abbreviated key words and color coding, as well as data organization techniques. The researcher will list on note cards the data gathered, perform minor editing, and log the data according to dates/times, places, and people observed/interviewed.

Table 4.4 provides a list of themes in two categories: theory-generated and in vivo. The theory-generated codes contain those themes that have been derived from the review of the literature. In reviewing the literature available on the subject, the researcher

has realized three themes: There is a lack of standards for mobile technology; there is a lack of standard analysis methodologies for smartphones; each technology should belong to a unique forensic process, depending on which hardware category in which it is classified.

The in vivo codes are those themes realized during data collection and after data analysis. During data collection and analysis, the researcher realized three themes: In practice, forensic examiners do not follow any forensic model available when examining a mobile device whether it be computer or smartphone and therefore follow their own ad-hoc approach; the ad-hoc approach is specific to each organization and is passed on to new employees; a smartphone process model would be accepted without much opposition in an actual forensic setting.

The researcher will use comparative analysis, analytic induction, and triangulation methods in order to edit the proposed model under the grounded theory method. As data are collected and themes are revealed, the model can be iteratively changed to demonstrate these new underlying themes.

Table 4.4 Theory-generated/In vivo themes

| Theory Generated Themes | In Vivo Themes |
|---|---|
| There is a lack of standards for mobile technology | In practice, forensic examiners do not follow any forensic model available when examining a mobile device whether it be computer or smartphone and therefore follow their own ad-hoc approach |
| Each technology should belong to a unique forensic process | The ad-hoc approach is specific to each organization and is passed on to new employees |
| Depending on which hardware category in which it is classified | A smartphone process model would be accepted without much opposition in an actual forensic setting |

### 4.1.2 Experimental Study Design

In an effort to realize interesting and unique forensic patterns in the operations of different model smartphones, the researcher designed two experiments in an effort to reveal any if they exist. Six different mobile devices with the following 5 OS platforms are used: Windows, RIM, Apple, Symbian, and Android. The experimental logic is described below.

Because many mobile OS devices contain proprietary software, the full operation of each has not been realized by forensic examiners. In most cases, without the needed equipment and software for each, the kernel is unreachable. In others, the kernel may still be inaccessible. In order to help combat this issue, an experiment was designed that can reveal how the kernel deals with file stores, edits, and deletes after certain operations. Knowing this information may help an examiner at certain points in the examination. It may even help to negate or support the testimony of a potential witness, victim, or offender.

The following categories are studied: browser operations, call operations, voicemail operations (only applicable to the Apple iPhone), messaging operations, contact operations, and camera operations. Table 4.5 provides the specific tests performed and the categories in which they belong. There are six smartphones used in this experiment with varying levels of operation. The Apple iPhone 3G A1241 is functional and currently under contract with AT&T®. The Blackberry 8530 (CDMA) RIM v5.0.0.654 is functional and previously under contract with Alltel®. The Blackberry 7130e (CDMA) can be powered on, but with an error on the screen which reads, “Device

Error: 348 Reset". After researching this error, the suggestion was to reinstall the OS. The researcher attempted to reinstall the OS twice, but the installation failed. The OS originally installed on the device was RIM v4.1. The Blackberry 8703e (CDMA) RIM v4.10.344 is functional and previously under contract with Verizon®. The HTC Touch Pro 6850 had to be hard reset in order to function correctly and was previously under contract with Sprint®. The OS is WM OS v6.1. The HTC Aria was previously under contract with AT&T® with an Android OS v2.1. The Nokia 5230 Nuron was previously under contract with T-Mobile® with a Symbian OS v9.4. Table 4.6 shows a breakdown of devices examined by carrier and OS.

Table 4.5 Experimental Smartphone Tests

| | **CATEGORIES** | | | | | | |
|---|---|---|---|---|---|---|---|
| | *Call* | *Contacts* | *Voicemail** | *SMS Messaging* | *MMS Messaging* | *Browser* | *Camera* |
| **TESTS** | Placed an answered outgoing | Created contact | Received a new voicemail | Received a new sms | Received a new mms | Opened a browser window | Snapped a picture |
| | Received and answered an incoming | Altered contact | Listened to voicemail | Opened a new sms | Opened a new mms | Closed a browser window | Deleted a picture |
| | Received an unanswered incoming | Deleted contact | Received a new voicemail and deleted it. | Deleted sms | Deleted mms | Google searched for rare disease | |
| | Deleted missed call | | Deleted an old voicemail | Sent an sms | Sent an mms | Deleted browser history | |
| | Deleted all calls | | Deleted all voicemails/call logs | | Deleted all messages | Deleted browser history + bookmarks | |

Table 4.6 Device Breakdown by Platform and Carrier

| | | Carrier | | | | |
|---|---|---|---|---|---|---|
| **Platform** | | *Alltel* | *AT&T* | *Sprint* | *T-Mobile* | *Verizon* |
| | *Android* | | HTC Aria | | | |
| | *Apple* | | Apple iPhone | | | |
| | *RIM* | Blackberry 8530 | | | | Blackberry 8703e |
| | *Symbian* | | | | Nokia 5230 Nuron | |
| | *Windows Mobile* | | | HTC Touch Pro 6850 | | |

The limitations of the experiments were that every test could not be performed on every phone. The only phone that is activated through a carrier is the Apple iPhone 3G. Even though the other devices are not activated, the researcher still conducted the experiments as though they were when possible. The logic behind this is that the file being edited or created concerning that experimental category should still log some sort of error, therefore creating a change in the state of the device. Another issue is that the forensic tool used can only read all information from the Apple iPhone 3G if it is jailbroken. That is, the OS has to be hacked and a new one installed on the device. In doing so, the researcher found that email and IM no longer operated correctly. Before the jailbreak, emails could be automatically pushed to the device by the network carrier. One more limitation is that one of the devices does not have a camera. According to our CCL, the camera is an extendable feature of a smartphone, so it is not required.

In order to capture the data, a spreadsheet for each device was created. In each spreadsheet, the name of the experiment conducted is listed on the left and the

corresponding filename is in the cell next to it. The column headings contain the different modes in which the device was processed. For example, the first column heading reads, "Unlocked w/SIM", which means the passcode for access to the phone was either known or was not set and that there was a SIM card in the phone upon processing. The subsequent headings are as follows: Locked w/SIM, Unlocked wo/SIM, Locked wo/SIM. Each filename contains the snapshot of the state of the device after each experiment is performed.

The goal of each experiment is to assist in determining the path with the smallest possibility of contamination when examining a device manually. This path is determined by computing the percent of change with respect to file size and the number of files that change between states. This will reveal how much the memory of the device changes between states thus, divulging which category and/or activity in Table 4.7 alters memory most significantly. Each category will be ranked with respect to percent difference from least to greatest. Ordering the categories in this fashion allows the proposed model to be edited in a way that considers how much the examiner will change the devices' memories during a manual examination.

The first experiment involves securing the files generated by XRY and capturing the size of each at the byte level. The files will be compared to others in 40 separate tests within their particular smartphone category with respect to the size, carrier, OS, and device. Doing so enables the author to compute the differences in size by test as well as by category. This affords us the knowledge of discovering which categories offer the least and most file size change. When dealing with the changes in file size, the results can

only take on one of three options. Either the size will increase, decrease, or have no change. Given these options, the researcher was able to provide projections of how each XRY file would be affected by each test.

In the second experiment, the XRY file from the first experiment is exported to the hard drive as a hierarchical folder containing all the files and folders extracted from each device. The number of files within the folder structure that differ from one state to the next are compared by inputting the two folders that compose a test into the SourceForge DiffMerge version 3.3.2 software. The number of identical, different, and unique files, as well as the number of folders will be identified. From these experiments, each test within each category can be ranked from least to greatest amount of change with respect to the percentage of change reported.

These experiments can add substance to a forensic examination by providing an examiner data which informs him on how to proceed when analyzing a smartphone manually. As mentioned earlier, some investigations may not reach a court of law because that is not what the victim desires. Also, in smaller more rural areas, investigators may not be equipped with the tools needed to handle a smartphone examination in a manner that is acceptable in a court of a law. This portion of the research will allow these examiners to know which category the examination should begin with in order to lessen the amount of contamination that will take place within the file system of the device. With repeat experiments, examiners may be able to track the changes applied and show that the change is standard across all devices containing that

specific operating system. The following section provides an analysis of the experiments performed and the results of each.

### 4.1.3 Experimental Analysis Results

#### 4.1.4.1 Experiment 1: File Size Difference

In this experiment, the files are compared to others within their smartphone category with respect to the size, carrier, and platform. Before experimentation began, the author coded each test using a unique ID and developed projections regarding the outcome of each test. The unique IDs are decoded in Table 4.7. Table 4.8 reflects these data coupled with the actual results. There were a total of 40 tests over 7 categories conducted. All categories coincide with those in Table 4.5 with the exception of the Miscellaneous Category. This group was added because there are some tests conducted that are unique to a specific device. For example, only RIM devices are required to activate via the enterprise server and no device with a different platform can attempt to do so. Therefore, Test E-IE and Test E-ELAN belong to the Miscellaneous Category and are only applicable to RIM devices.

Of the 40 tests conducted, at least one or more of the devices conform to 83% of the projected results. 20% of the tests are not predicted due to an uncertainty by the author and therefore, the projected resulted is coded as undecided (U). There are four other codes in the table, I, D, NC, and N/A, which are acronyms for the following: increased in file size, decreased in file size, no change in file size, and not applicable. Some of the entries in the table have a red font. These are the actual results that contradict

the projected results given by the author. Test V-IP is the only test in which every device performs similarly and as projected with the exception of the Nokia 5230. The call category is not applicable to the Nokia 5230 in this experiment and therefore cannot be included in the analysis of that category. In the remainder of the tests, none of the devices perform as predicted.

The actual results show the relationship between devices based on how similar or dissimilar they perform. Across the battery of tests, the Apple iPhone performs most similarly to the HTC TouchPro 6850 where 20% of the tests are equivalent. The iPhone is least akin to the HTC Aria matching 7.5% of the time. The Blackberry 8530 performs most similarly to the Blackberry 8703e where 27.5% of the tests are equivalent whereas it is least akin to the Nokia 5230 performing similarly in only 2.5% of the tests. The Blackberry 8703e performs most similarly to the Blackberry 8530 and is least akin to the Nokia 5230 matching only 2.5% of the time. The HTC TouchPro 6850 is most like the Blackberry 8530 and the Apple iPhone performing similarly in 20% of the tests whereas the Nokia 5230 is least akin to it performing similarly in only 2.5% of the tests. The HTC Aria performs in parallel to the Blackberry 8530 in 17% of the tests but is least like the Nokia 5230 in that it performs the same only 5% of the time. Lastly, the Nokia 5230 performs most similarly to the Apple iPhone 10% of the time and least similarly to the HTC TouchPro 6850, the Blackberry 8530, and the Blackberry 8703e with a percentage of 2.5% of matching results. Three of six devices tested are the most compatible with the Blackberry 8530 and four of the six devices are the least compatible with the Nokia 5230.

In addition to evaluating how the devices perform to each other throughout the entire experiment, the researcher also observed how the devices performed to one another with respect to the smartphone categories. Table 4.9 shows which devices are most/least like others with respect to file size performance by category. The devices are listed with a number that corresponds to each. The table references the numbers when reporting the least and most like device. Some devices were not able to be tested in certain categories and therefore the entire category is marked N/A. Table 4.9 shows this in two ways. An asterisk follows the category name in which one or more devices are not applicable and each device that was not considered in a specific category is recognized as such with an N/A in the corresponding cell for that particular category.

Table 4.7 Unique ID Lookup Table

| Category | Unique ID | Test State 1 to Test State 2 |
|---|---|---|
| Browser | B-IO | Initial to Open Browser Window |
| | B-OG | Open Browser Window to Google Search |
| | B-GC | Google Search to Close Browser Window |
| | B-OC | Open Browser Window to Close Browser Window |
| | B-GD | Google Search to Delete History and Bookmarks |
| | B-CD | Close Browser Window to Delete History |
| Contact | C-IN | Initial to New Contact |
| | C-NA | New Contact to Altered Contact |
| | C-AD | Altered Contact to Deleted Contact |
| MMS | M-IR | Initial to Received MMS message |
| | M-IS | Initial to Sent MMS message |
| | M-RO | Received MMS message to Opened MMS message |
| | M-RD | Received MMS message to Deleted MMS message |
| | M-SD | Sent MMS message to Deleted MMS message |
| Picture | P-IN | Initial to New Picture |
| | P-ND | New Picture to Deleted Picture |
| SMS | S-IR | Initial to Received SMS message |
| | S-IS | Initial to Sent SMS message |
| | S-RO | Received SMS message to Opened SMS message |
| | S-OD | Received SMS message to Deleted SMS message |
| | S-SD | Sent SMS message to Deleted SMS message |
| Call | V-IP | Initial to Placed Call |
| | V-IRA | Initial to Received Answered Call |
| | V-IRU | Initial to Received Unanswered Call |
| | V-IDC | Initial to Deleted Call log |
| | V-PDC | Placed Call to Deleted Call log |
| | V-RUDM | Received Unanswered Call to Deleted Missed Call |
| Miscellaneous | A-ISA | Initial to Stop All Apps (TouchPro 6850 only) |
| | E-IE | Initial to Connect to Enterprise Server (BB only) |
| | E-ELAN | Connect to Enterprise Server to Disconnect from WLAN (BB only) |
| | J-IJB | Initial to Jailbreak (iPhone only) |
| | J-JBDM | Jailbreak to Delete SMS (iPhone only) |
| | L-IL | Initial to Passcode Enabled (iPhone only) |
| | L-LnS | Passcode Enabled to no SIM (iPhone only) |
| | N-IDN | Initial to Deleted Network Info (BB only) |
| | Vmail-IR | Initial to Received Voicemail (iPhone only) |
| | Vmail-RL | Received Voicemail to Listened to Voicemail (iPhone only) |
| | Vmail-LD | Listened to Voicemail to Deleted Voicemail (iPhone only) |
| | W-ILAN | Initial to Connected to WLAN (BB only) |
| | W-LAN | Connect to WLAN to Disconnect from WLAN (BB only) |

Table 4.8 Projected Result vs. Actual Result

| | | Actual Result | | | | | |
|---|---|---|---|---|---|---|---|
| TEST ID | Projected Result | Apple iPhone | RIM BB 8530 | RIM BB8703 | HTC TouchPro 6850 | HTC Aria | Nokia 5230 |
| B-IO | I | D | I | N/A | I | NC | N/A |
| B-OG | I | D | NC | N/A | I | I | N/A |
| B-GC | D | I | NC | N/A | I | D | N/A |
| B-OC | U | I | NC | N/A | I | NC | N/A |
| B-GD | D | I | NC | N/A | I | D | N/A |
| B-CD | D | I | NC | N/A | D | D | N/A |
| C-IN | I | I | I | I | D | I | I |
| C-NA | U | I | I | I | NC | D | D |
| C-AD | D | I | D | D | D | D | I |
| M-IR | I | I | N/A | N/A | N/A | N/A | N/A |
| M-IS | I | D | I | N/A | I | N/A | D |
| M-RO | U | I | N/A | N/A | N/A | N/A | N/A |
| M-RD | D | I | N/A | N/A | N/A | N/A | N/A |
| M-SD | D | I | D | N/A | N/A | N/A | N/A |
| P-IN | I | I | NC | N/A | I | N/A | I |
| P-ND | D | I | NC | N/A | I | N/A | D |
| S-IR | I | I | D | NC | N/A | N/A | N/A |
| S-IS | I | I | I | I | I | I | D |
| S-RO | U | I | NC | NC | N/A | N/A | N/A |
| S-OD | D | I | NC | NC | N/A | N/A | N/A |
| S-SD | D | I | D | D | I | D | N/A |
| V-IP | I | I | I | I | I | I | N/A |
| V-IRA | I | D | N/A | N/A | N/A | N/A | N/A |
| V-IRU | I | I | N/A | N/A | N/A | N/A | N/A |
| V-IDC | D | I | D | D | D | NC | N/A |
| V-PDC | D | I | D | D | D | D | N/A |
| V-RUDM | D | I | N/A | N/A | N/A | N/A | N/A |
| A-ISA | D | N/A | N/A | N/A | I | N/A | N/A |
| E-IE | I | N/A | N/A | NC | N/A | N/A | N/A |
| E-ELAN | U | N/A | N/A | NC | N/A | N/A | N/A |
| J-IJB | I | I | N/A | N/A | N/A | N/A | N/A |
| J-JBDM | D | D | N/A | N/A | N/A | N/A | N/A |
| L-IL | U | D | N/A | N/A | N/A | N/A | N/A |
| L-LnS | U | D | N/A | N/A | N/A | N/A | N/A |
| N-IDN | D | N/A | NC | N/A | N/A | N/A | N/A |
| Vmail-IR | I | I | N/A | N/A | N/A | N/A | N/A |
| Vmail-RL | U | D | N/A | N/A | N/A | N/A | N/A |
| Vmail-LD | D | D | N/A | N/A | N/A | N/A | N/A |
| W-ILAN | I | N/A | I | NC | N/A | N/A | N/A |
| W-LAN | D | N/A | NC | NC | N/A | N/A | N/A |

In some instances, all tests in a category were not able to be performed but one or more was. In these instances, comparisons were done considering the amount of test

results available. For example, when finding out which devices are most and least like the HTC TouchPro 6850 in the MMS Category the HTC Aria and the Blackberry 8703e cannot be considered because no results are available. All results are available for the Apple iPhone; two are available for the Blackberry 8530, and one for the Nokia 5230. Since more results are available for the Apple iPhone, the comparison of the two devices takes precedence over the remainder of the devices followed by the Blackberry 8530 and then the Nokia 5230.

In the Browser Category, the Apple iPhone performs most similarly to the HTC TouchPro 6850 and least similarly to the Blackberry 8530 and the HTC Aria whereas in the Contact Category, the Apple iPhone performs most similarly to the Blackberry 8530, the Blackberry 8703e, and the Nokia 5230 and least similarly to the HTC TouchPro 6850. Comparably, the Apple iPhone performs the least similarly to the Blackberry 8530 in the MMS and Picture Categories. The Nokia 5230 is most akin to the Apple iPhone in the MMS Category and in tandem with the HTC TouchPro 6850 in the Picture Category. In the SMS Category, the Apple iPhone performs most like the HTC TouchPro 6850. Regarding the Call Category, all the devices perform similarly in that only one test matches the results of the Apple iPhone with the exception of the Nokia 5230 with no results available in this category.

Table 4.9 Device Comparison by Category

| Device | | Browser* | Contact | MMS* | Picture* | SMS | Call* |
|---|---|---|---|---|---|---|---|
| Apple iPhone (1) | Most Like | 4 | 2, 3, 6 | 6 | 4 | 4 | 2-5 |
| | Least Like | 2, 5 | 4 | 2 | 2 | 6 | 2-5 |
| BB 8530 (2) | Most Like | 4, 5 | 3 | 4 | -- | 3 | 3, 4 |
| | Least Like | 1 | 4, 6 | 1 | 1,4,6 | 1 | 1 |
| BB 8703e (3) | Most Like | N/A | 2 | N/A | N/A | 2 | 2, 4 |
| | Least Like | N/A | 6 | N/A | N/A | 1 | 1 |
| HTC 6850 (4) | Most Like | 1 | 2, 3, 5 | 2 | 1 | 1 | 2, 3 |
| | Least Like | 2 | 1, 6 | 1 | 2 | 2, 3 | 1 |
| HTC Aria (5) | Most Like | 4 | 2, 3, 6 | N/A | N/A | 2, 3 | 2,3,4 |
| | Least Like | 1 | 1, 4 | N/A | N/A | 1 | 1 |
| Nokia 5230 (6) | Most Like | N/A | 1, 5 | 1 | 1, 4 | -- | N/A |
| | Least Like | N/A | 4 | 2 | 2 | 1, 2 | N/A |

The Blackberry 8530 is most similar to the HTC TouchPro 6850 and the HTC Aria with respect to the Browser Category and is less like the Apple iPhone. As in this category, the Blackberry 8530 is also less like the Apple iPhone in the MMS, SMS, and Call Categories. The SMS and Contact Categories find the Blackberry 8703e most akin to the Blackberry 8530 but the Contact Category shows the HTC TouchPro 6850 and the Nokia 5230 least like the device. The HTC TouchPro 6850 is most like the Blackberry 8530 in the MMS Category and is also most like the device in tandem with the Blackberry 8703 in the Call Category. None of the devices share similarities with the HTC TouchPro 6850 in the Picture Category, however, given the fact that some devices did not have results for each test in this category, there are devices that perform least like the HTC TouchPro 6850 and are as follows: the Apple iPhone, HTC TouchPro 6850, and the Nokia.

The HTC TouchPro 6850 is most similar to the Apple iPhone in the Browser and SMS Categories as well as the Picture Category. The device is least similar to the Blackberry 8530 in the Brower and Picture Categories. The HTC TouchPro 6850 is also most similar to the Blackberry 8530 in the MMS Category and least like the Apple iPhone. In addition to the Blackberry 8530, the Blackberry 8703e is most like the device in the Call Category and the HTC TouchPro 6850 is least like the Apple iPhone. The Contact Category shows that both Blackberrys and the HTC Aria perform most like the HTC TouchPro 6850 and that the device is least akin to the Apple iPhone and the Nokia 5230.

The Blackberry 8703e was not considered in the Browser, MMS, or Picture Categories. In the Contact and SMS Categories, the Blackberry 8530 is the most akin to Blackberry 8703e whereas in the Contact Category, the device is least like the Nokia 5230. The device is less like the Apple iPhone in the SMS Category. Regarding the Call Category, the HTC TouchPro 6850 and the Blackberry 8530 are most like the device whereas the Apple iPhone is least akin to the Blackberry 8703e.

The HTC Aria was not considered in the MMS and Picture Categories. The Browser Category shows that the device has the most in common with the Blackberry 8530 and the HTC TouchPro 6850 and the least in common with the Apple iPhone. Actually, all the categories applicable to the HTC Aria are the least akin to the Apple iPhone in tandem with the HTC TouchPro 6850 in the Contact Category. The Contact Category also shows that the HTC Aria has the most in common with three devices: Blackberry 8530, Blackberry 8703e, and the Nokia 5230. The device also has the most in

common with both Blackberrys in the SMS Category coupled with the HTC TouchPro 6850 in the Call Category.

The Nokia 5230 was not considered in the Browser Category. The Contact Category shows that the device has the most in common with the HTC Aria and the Apple iPhone and the least in common with the HTC TouchPro 6850. The Category shows that the Nokia 5230 is the most akin to the Apple iPhone and the least akin to the Blackberry 8530. The Picture category almost mirrors the MMS Category in that the Nokia 5230 performs most like the Apple iPhone coupled with the HTC TouchPro and is least like the Blackberry 8530. The SMS Category shows that this device has nothing in common with any of its competitors in that it does not perform as any other device does. Due to the lack of applicability of some devices, the Nokia 5230 does have devices that it is least like in the SMS Category; Apple iPhone and the Blackberry 8530.

Table 4.10 Device Performance Comparison by Carrier/Platform Based on File Size Change

| | | Carrier |
|---|---|---|
| AT&T (Apple) (iPhone) | Most Like | Sprint (6850) (WMD) |
| | Least Like | AT&T (Aria) (Android) |
| Alltel (RIM) (Blackberry 8530) | Most Like | Verizon (8703e) (RIM) |
| | Least Like | T-Mobile (5230) (Symbian) |
| Verizon (RIM) (Blackberry 8703e | Most Like | Alltel (8530) (RIM) |
| | Least Like | T-Mobile (5230) (Symbian) |
| Sprint (WMD) (HTC TouchPro 6850) | Most Like | Alltel (8530) (RIM), AT&T (iPhone) |
| | Least Like | T-Mobile (5230) (Symbian) |
| AT&T (Android) (HTC Aria) | Most Like | Alltel (8530) (RIM) |
| | Least Like | T-Mobile (5230) (Symbian) |
| T-Mobile (Symbian) (Nokia 5230) | Most Like | AT&T (iPhone) |
| | Least Like | Sprint (6850) (WMD), Verizon (8703e) (RIM), Alltel (8530) (RIM) |

Considering how the devices compare regarding carrier, it can be deduced that these six categories perform independently. This is shown by looking at two devices with the same carrier and observing the relationship between the two. The HTC Aria and the Apple iPhone are both under the AT&T carrier and the Apple iPhone is the least related to the HTC Aria. The Blackberry 8530 and the Blackberry 8703e are the most compatible of all the devices but are handled by two different carriers, Alltel and Verizon respectively. Table 4.10 shows the most and least similar devices by carrier and platform.

Regarding platform, the least astonishing result is that both RIM devices are most like each other and they both share the same platform that each is dislike; Symbian. More telling were the remaining results. Like the RIM devices, the Android shares the same compatibilities. The Apple OS is shown to perform more like the Windows OS and less

like the Android OS. The Windows OS is shown to be compatible with the broadest range of available OSs; RIM and Apple, whereas it is least compatible with Symbian. Lastly, the Symbian OS has the most in common with the Apple OS, but is the only device with more than one incompatible OS; RIM and Windows OS.

Overall, the devices can be ranked by which device performs the most like all the other devices to which device performs the least like all the others. Of all the tests, the Blackberry 8530 performs like one or more of the devices over the battery of tests 12.5% of the time, the HTC TouchPro 6850 11.7% of the time, the Blackberry 8703e 10.8% of the time, the HTC Aria 10% of the time, the Apple iPhone 9.7% of the time, and the Nokia 5230 3.8% of the time.

Analyzing Table 4.10 allows one to evaluate which devices are more like others regarding smartphone category. Given these results, the Preliminary Toolset of PIFPM can be designed with respect to the amount of change that takes place within each category. To assist in this effort, the average percent of change by category is computed in Table 4.11.

Ranking the devices by the average amount of change that takes place in each category allows us to name the area of each device where file size will be affected the least and the most by manual manipulation. Only the order of examination for the Apple iPhone is stated with the most confidence given that it is the only device that contained results for each test. The following results are based solely on change to file size and the results shown in Table 4.11. When examining the Apple iPhone manually, data from pictures or calls should be extracted first. The order of examination for the remainder of

the data is as follows: browser, SMS, MMS, contacts. When examining the Blackberry 8530, the order should be as follows: picture, contact, browser, call, MMS, and SMS. The data provide an order as follows for the Blackberry 8703e: contact, call, and SMS. The remainder of the categories contains no results. The author believes that if the device yielded results for each test as did the Blackberry 8530, the order would be the same. This will be taken under consideration when manipulating PIFPM. The order of examination for the HTC TouchPro should be as follows: SMS, call, browser, MMS, contact, and Picture. Both the HTC Aria and the Nokia 5230 have categories that contain no results and both therefore show four of the six categories in their order of examination. Contact, call, browser, and SMS is the order in which the HTC Aria should be examined while the Nokia 5230 should be examined as follows: SMS or MMS, picture, and contact.

Table 4.11 Categorical Percent Difference

| Category | TEST ID | Apple iPhone | | RIM BB8530 | | RIM BB8703 | | HTC TouchPro 6850 | | HTC Aria | | Nokia 5230 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | %Δ | Avg. | %Δ | Avg. | %Δ | Avg. | %Δ | Avg. | %Δ | Avg. | %Δ | Avg. |
| Browser | B-IO | .0001 | .0006 | .087 | .086 | N/A | N/A | .004 | .0374 | 0 | .856 | N/A | N/A |
| | B-OG | .0001 | | 0 | | N/A | | .054 | | 1.211 | | N/A | |
| | B-GC | .001 | | 0 | | N/A | | .031 | | 1.196 | | N/A | |
| | B-OC | .0009 | | 0 | | N/A | | .085 | | 0 | | N/A | |
| | B-GD | .0012 | | 0 | | N/A | | .031 | | 2.701 | | N/A | |
| | B-CD | .0002 | | 0 | | N/A | | .019 | | .002 | | N/A | |
| Contact | C-IN | .0001 | .0024 | .106 | .079 | .904 | .673 | 11.348 | 4.092 | .348 | .232 | 315.96 | 141.3 |
| | C-NA | .0005 | | .013 | | .111 | | 0 | | .022 | | 70.486 | |
| | C-AD | .0064 | | .119 | | 1.006 | | .0001 | | .325 | | 238.82 | |
| MMS | M-IR | .0016 | .0013 | N/A | 2.06 | N/A | N/A | N/A | .195 | N/A | N/A | N/A | .058 |
| | M-IS | .0008 | | 2.02 | | N/A | | .195 | | N/A | | .058 | |
| | M-RO | .0003 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | M-RD | .001 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | M-SD | .0026 | | 2.103 | | N/A | | N/A | | N/A | | N/A | |
| Pic | P-IN | .0006 | .0004 | 0 | 0 | N/A | N/A | .075 | 6.4 | N/A | N/A | 50.66 | 40.86 |
| | P-ND | .0002 | | 0 | | N/A | | 12.721 | | N/A | | 34.35 | |
| SMS | S-IR | .0015 | .0007 | 11.21 | 4.15 | 0 | 1.187 | N/A | .00006 | N/A | .774 | N/A | .058 |
| | S-IS | .00004 | | .126 | | 1.194 | | .001 | | .777 | | .058 | |
| | S-RO | .0002 | | 0 | | 0 | | N/A | | N/A | | N/A | |
| | S-OD | .0001 | | 0 | | 0 | | N/A | | N/A | | N/A | |
| | S-SD | .0018 | | .218 | | 1.18 | | .00001 | | .771 | | N/A | |
| Call | V-IP | .0002 | .0004 | .157 | .183 | 1.032 | 1.025 | .002 | .002 | .623 | .621 | N/A | N/A |
| | V-IRA | .0005 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | V-IRU | .0003 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | V-IDC | .0003 | | .197 | | 1.022 | | .002 | | .619 | | N/A | |
| | V-PDC | .0003 | | .197 | | 1.022 | | .002 | | .619 | | N/A | |
| | V-RUDM | .0004 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| Miscellaneous | A-ISA | N/A | 13.53 | N/A | .092 | N/A | | .873 | .873 | N/A | N/A | N/A | N/A |
| | E-IE | N/A | | N/A | | 0 | | N/A | | N/A | | N/A | |
| | E-ELAN | N/A | | N/A | | 0 | | N/A | | N/A | | N/A | |
| | J-IJB | 94.49 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | J-JBDM | .0017 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | L-IL | .0001 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | L-LnS | .0004 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | N-IDN | N/A | | 0 | | N/A | | N/A | | N/A | | N/A | |
| | Vmail-IR | .001 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | Vmail-RL | .001 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | Vmail-LD | .001 | | N/A | | N/A | | N/A | | N/A | | N/A | |
| | W-ILAN | N/A | | .092 | | 0 | | N/A | | N/A | | N/A | |
| | W-LAN | N/A | | 0 | | 0 | | N/A | | N/A | | N/A | |

#### 4.1.4.2 Experiment 2: Average Change in File Content

In both experiments, XRY writes a specific set of information to each examination file. The difference is that in Experiment 2, this information is arranged in the form of files at the root of the folder which alter the outcome of the experiment. As an aside, these files were counted in the analysis of the results. XRY also alters the state of most of the devices or instructs the examiner to do so before experimentation began. Following is an outline of the extraction media, the data limitations, and the changes made to each device.

The recommended media connection for the Apple iPhone is by microUSB cable. XRY v6.1 is unable to support the extraction of SIM calls, sms, or contacts, tasks, PC & device clock, retrieval of the phone number of the device, and any data from the memory card. Email extraction is partially supported, but only if the device is jailbroken and MMS is only supported on an iPhone OS of 3.0 or later. XRY makes no changes to memory, but in order to extract the maximum amount of data from the device, the state of memory has to be altered by jailbreaking the device. The Apple iPhone used in this experiment was examined both pre and post jailbreak so that the results of each could be compared.

The Blackberry 8530 has a recommended media connection of a microUSB cable. Data such as SIM contacts, calls, and SMS, bookmarks, IMSI, phone number of the device, PC & device clock, and the SMS service center number are not available. Files and MMS are only partially supported. XRY makes no changes to memory, but before any information can be retrieved, the state of the device has to be altered to ensure that

“media card support” is set to “on”, “encryption mode” is set to “none”, “mass storage mode support" is set to "on", and "auto enable mass storage mode when connected" is set to "yes".

The recommended media connection for the Blackberry 8703e is microUSB cable. The support of SIM contacts, calls, and SMS, bookmarks, IMSI, phone number of the device, PC & device clock are not available in this version of XRY. Files are only partially supported. Although, XRY makes no changes to memory and the device does not have to be altered in any way in order for extraction to begin, this device has only been tested as a Verizon operator. Being as such, XRY does not guarantee all functionality when examining devices with different carriers.

The HTC Aria has the same recommended connection as all the other devices; microUSB cable. The following items for data extraction are not supported: pictures, audio, video, files, tasks, and notes. XRY partially supports email, but fully extracts SIM contacts and SMS, device contacts, calls, SMS, MMS, calendar events, and memory card data. XRY makes no changes to memory but before extraction can begin, the examiner must ensure that "USB debugging" is enabled which will alter the current state of the device.

The HTC TouchPro 6850 is not listed as a supported device, but is recognized as a Windows Mobile 6 device upon connecting it to XRY using a mediaUSB cable. There are three other TouchPro devices reported to be supported that extract all features except SIM calls and device notes. Due to security settings, IMEI, IMSI, and SIM SMS may not be extracted. XRY makes changes to the device by installing an XRY plug-in to the root

of the memory of the phone and is executed from there. There is an option to install the plug-in on a memory card in order to avoid altering the state of the device. Regardless of installation choice, the plug-in is said to be uninstalled automatically.

The Nokia Nuron 5230 has a recommended connection of microUSB cable. SIM contacts, calls, or SMS are not supported but extraction of all other data is. XRY alters the state of the device by installing a connectivity assistant in memory. There is also an option to install the program on a memory card but uninstalling it is a manual task done by the user. Before XRY writes to the device, the examiner is advised to alter the state of the device in order to ensure that the certificate check is disabled and that the software installation option is set to "all".

In order to compute the difference in the number of files where the content differs, each folder structure representing each test was inputted into the DiffMerge software along with its comparison test folder structure. DiffMerge returned the number of identical and different files, the number of files without peers, and the number of folders. The percent difference in the number of files where the content changed was computed by adding the number of different files and files without peers and dividing by the total number of files within the folder structure. This number is then divided by 100.

The Apple iPhone is the only device where the total number of folders per test fluctuates between 2,550 and 4,833 seen in Table 4.12. The number of folders throughout all other tests for every other device remains the same. Given the limitations of extraction by XRY, it is not surprising that the Nokia Nuron 5230, the HTC Aria, and the Blackberry 8703e only contain 1 folder for each of the forty tests. These results can be

reviewed in Tables 4.17, 4.16, and 4.14 respectively. Tables 4.13 and 4.15 respectively show that the Blackberry 8530 contains 8 folders throughout the experiment and the HTC TouchPro 6850 contains 0 folders.

Since the HTC TouchPro 6850 is not listed as a supported device, not much data was extracted from the device. Throughout all 40 tests, there were a total of 4 files found listed under the different category. There were 0 identical and 0 without peers. When examining these 4 files, it was discovered that they were all generated by XRY and are all types of log files: Case Data.txt, Device-General Information.txt, Summary.txt, and XRY System-Log.txt. When examining the 4 files to discover the differences, it was found that they are minor changes such as date and time of extraction. Looking at Experiment 1, one can deduce that since the size of the XRY file changed with every category except the Call Category that the HTC TouchPro 6850 is somewhat supported by XRY v6.1. With that said, it is not known what types of files are being manipulated. It is possible that only the size of the log files are changing, therefore providing results as seen in the first experiment. Therefore, the amount of change in the number of files per test gives us an average change percentage of 100% for each smartphone category as follows: Picture, Contact, and Browser.

Table 4.12 Apple iPhone: % Change in Folder Content by Test and Category

| | | Number of Differences | | | | |
|---|---|---|---|---|---|---|
| Unique Test ID | Identical | Different | Without Peers | # Folders | % Δ | Categorical % Δ |
| J-IJB | 1 | 9 | 71023 | 4430 | 99.999% | 62.7% |
| J-JBDM | 54784 | 6410 | 14645 | 4355 | 27.763% | |
| M-IS | 55041 | 16484 | 19345 | 4743 | 39.429% | 34.0% |
| M-SR | 64563 | 7626 | 17901 | 4833 | 28.335% | |
| M-RO | 64394 | 8101 | 17354 | 4800 | 28.331% | |
| M-OD | 54869 | 16644 | 19404 | 4774 | 39.649% | |
| S-IS | 66276 | 7096 | 15628 | 4731 | 25.533% | 25.3% |
| S-SR | 65933 | 7407 | 15714 | 4728 | 25.963% | |
| S-RO | 66815 | 6679 | 15464 | 4769 | 24.892% | |
| S-OD | 66750 | 6802 | 15431 | 4743 | 24.986% | |
| Vmail-IR | 55774 | 7520 | 14409 | 2590 | 28.222% | 27.9% |
| Vmail-RL | 56215 | 7557 | 13601 | 2550 | 27.345% | |
| Vmail-LD | 55599 | 8125 | 13581 | 2611 | 28.078% | |
| V-RUDM | 55796 | 7770 | 13636 | 2648 | 27.727% | 28.2% |
| V-DMR | 55745 | 7630 | 14054 | 2648 | 28.005% | |
| V-IP | 56133 | 7553 | 13620 | 2587 | 27.389% | |
| V-PDC | 56496 | 7168 | 13596 | 2637 | 26.875% | |
| P-IN | 56298 | 7332 | 13772 | 2644 | 27.265% | 27.3% |
| P-ND | 56257 | 7539 | 13609 | 2614 | 27.321% | |
| B-DBO | 39193 | 23142 | 16021 | 2686 | 49.981% | 46.6% |
| B-OG | 37100 | 24862 | 17000 | 2656 | 53.015% | |
| B-GC | 53427 | 9142 | 16024 | 2577 | 32.021% | |
| B-CD | 38285 | 24222 | 16124 | 2679 | 51.311% | |
| C-IN | 38529 | 24032 | 16044 | 2679 | 50.984% | 61.1% |
| C-NA | 53619 | 9008 | 15976 | 2679 | 31.785% | |
| C-AD | 1 | 61678 | 18030 | 2680 | 99.999% | |
| L-IL | 1 | 61942 | 17607 | 2637 | 99.999% | 75.0% |
| L-LnS | 39531 | 23567 | 15284 | 2637 | 49.566% | |

Table 4.13 Blackberry 8530: % Change in Folder Content by Device and Category

| | | Number of Differences | | | | |
|---|---|---|---|---|---|---|
| Unique Test ID | Identical | Different | Without Peers | # Folders | % Δ | Categorical % Δ |
| S-IR | 8 | 5 | 2 | 8 | 46.667% | 40.7% |
| S-RO | 8 | 5 | 0 | 8 | 38.462% | |
| S-OD | 8 | 5 | 0 | 8 | 38.462% | |
| S-IS | 8 | 5 | 0 | 8 | 38.462% | |
| P-IN | 8 | 5 | 0 | 8 | 38.462% | 38.5% |
| P-ND | 8 | 5 | 0 | 8 | 38.462% | |
| C-IN | 8 | 5 | 0 | 8 | 38.462% | 41.5% |
| C-NA | 8 | 5 | 1 | 8 | 42.857% | |
| C-AD | 8 | 5 | 1 | 8 | 42.857% | |
| W-ILAN | 8 | 5 | 0 | 8 | 38.462% | 38.5% |
| W-LAN | 8 | 5 | 0 | 8 | 38.462% | |
| N-IDN | 8 | 5 | 0 | 8 | 38.462% | 38.5% |
| M-SMSMMS | 8 | 5 | 0 | 8 | 38.462% | 38.5% |
| M-SD | 8 | 5 | 0 | 8 | 38.462% | |
| V-IP | 8 | 5 | 0 | 8 | 38.462% | 38.5% |
| V-PDC | 8 | 5 | 0 | 8 | 38.462% | |
| B-IO | 8 | 5 | 0 | 8 | 38.462% | 38.5% |
| B-OG | 8 | 5 | 0 | 8 | 38.462% | |
| B-GD | 8 | 5 | 0 | 8 | 38.462% | |
| B-DDC | 8 | 5 | 0 | 8 | 38.462% | |

Both the Blackberry 8703e and the HTC Aria report 1 file as identical, 4 files as different, and 0 files as being without peers. These four files listed as different are the same log files found in the HTC TouchPro 6850 file structure. The 1 file on the Blackberry 8703e that is identical to all the other tests is a JPG file containing a picture of a Blackberry 8703e. The 1 file on the HTC Aria that is identical to all the other tests is also a JPG file containing a picture of an HTC Aria. Examination of the 4 files revealed the same results as did looking at the 4 HTC TouchPro 6850 files being reported as different. The amount of change in the number of files per test on the Blackberry 8703e

gives us an average change percentage of 80% for each smartphone category as follows: SMS, Contact, and Call. The percentage is the same for the HTC Aria with smartphone categories of SMS, Call, Contact, and Browser.

Of the 40 tests, 3 resulted in files without peers when examining the Blackberry 8530. Test S-IR lists 8 files as identical, 5 different, and 2 without peers. Tests C-NA and C-AD lists 8 files as identical, 5 as different and 1 file without a peer. The remainder of the tests lists 8 files as identical, 5 files as different and 0 files without peers. Examining the folder structure resulted in the discovery of another log file written by XRY, "Files-Unrecognized.txt". This is a log file generated by XRY that contains the name of the file, the path of the file on the device, the date and time created and modified, and four hash values of the file. Consequently, the Blackberry 8530 reports an average change percentage of 38.5% for each of the following smartphone categories: Picture, Call, MMS, and Browser. The Contact Category has an average contents change of 41.5% and the SMS Category an average change of 40.7%.

Table 4.14 Blackberry 8703e: % Change in Folder Content by Device and Category

| | | Number of Differences | | | | |
|---|---|---|---|---|---|---|
| Unique Test ID | Identical | Different | Without Peers | # Folders | % Δ | Categorical % Δ |
| S-IR | 1 | 4 | 0 | 1 | 80% | 80% |
| S-RO | 1 | 4 | 0 | 1 | 80% | |
| S-IS | 1 | 4 | 0 | 1 | 80% | |
| C-IN | 1 | 4 | 0 | 1 | 80% | 80% |
| C-NA | 1 | 4 | 0 | 1 | 80% | |
| C-AD | 1 | 4 | 0 | 1 | 80% | |
| W-ILAN | 1 | 4 | 0 | 1 | 80% | 80% |
| W-ELAN | 1 | 4 | 0 | 1 | 80% | |
| V-IP | 1 | 4 | 0 | 1 | 80% | 80% |
| V-PDC | 1 | 4 | 0 | 1 | 80% | |
| E-IE | 1 | 4 | 0 | 1 | 80% | 80% |

XRY writes a total of 13 log files to each folder representing each test for the Apple iPhone as follows: Calls.txt, Case Data.txt, Device-General Information.txt, Device-Keyboard Cache.txt, Files-Archives.txt, Files-Audio.txt, Files-Documents.txt, Files-Pictures.txt, Files-Unrecognized.txt, Files-Videos.txt, Messages-SMS.txt, Summary.txt, and XRY System-Log.txt. Due to the amount of data retrieved from the Apple iPhone tests, it is infeasible to discuss each. Therefore, only the most interesting tests will be mentioned in the text and readers can refer to Table 4.12 for further review. According to XRY, if the Apple iPhone is jailbroken, XRY is able to extract more data. Test J-IJB which compares the Apple iPhone in its pre-jailbroken and post jailbroken state, reveals that 99.99% of the files contained different content. 1 of the files is identical, 9 of the files are different, and 71,023 of the files did not have peers. With only 1 file identical, and 9 different, it can be concluded that the remainder of the files did not exist in the pre-jailbreak folder structure. Therefore, the claim that XRY can extract more

data from a jailbroken device seems to be supported. Of the 6 smartphone categories, the greatest amount of content change takes place in the Contact Category, and the least amount of content change takes place in the SMS Category. On average, The Contact Category reports 30,716 files as identical, 31,573 files as different, and 16,683 files without peers. This means that 61.1% of the contents of the files in this category change. On average, the SMS Category reports 66,444 files as identical, 6,996 files as different, and 15,559 files without peers. This means that 25.3% of the content of the files in this category change. Following is the remainder of the categories coupled with the average amount of change per category from least amount of change to most: Picture-27.3%, Call-28.2%, MMS-34%, and Browser-46.6%.

As in the first experiment, an order of examination can be deduced based on these results. The Blackberry 8703e, HTC TouchPro 6850, and the HTC Aria all have the same amount of categorical change and therefore this experiment does not assist in devising an order of examination for these devices. However, this order can be realized for the remaining devices. Table 4.12 shows that the categorical order of manual examination for the Apple iPhone that will result in the least file manipulation is as follows: SMS, Picture, Voicemail, Call, MMS, Browser, and Contact. The Miscellaneous Tests all result in the greatest amount of content change to the XRY folder structure of the Apple iPhone. Table 4.13 shows that several of the smartphone categories result in the same percent of content change which happens to be the lowest amount of average change: MMS, Call, Browser, and Picture. Either of these categories can be examined resulting at the beginning of a Blackberry 8530 examination. The remaining categories should be

examined in the following order: SMS, Contact. Table 4.17 shows that the order of manual examination for the Nokia Nuron 5230 is as follows: SMS, Contact, Picture, and lastly MMS.

Table 4.15 HTC TouchPro 6850: % Change in Folder Content by Device and Category

| | | Number of Differences | | | | |
|---|---|---|---|---|---|---|
| Unique Test ID | Identical | Different | Without Peers | # Folders | % Δ | Categorical % Δ |
| P-IN | 0 | 4 | 0 | 0 | 100% | 100% |
| P-ND | 0 | 4 | 0 | 0 | 100% | |
| C-IN | 0 | 4 | 0 | 0 | 100% | 100% |
| C-AD | 0 | 4 | 0 | 0 | 100% | |
| W-ILAN | 0 | 4 | 0 | 0 | 100% | 100% |
| B-IO | 0 | 4 | 0 | 0 | 100% | 100% |
| B-OG | 0 | 4 | 0 | 0 | 100% | |
| B-GD | 0 | 4 | 0 | 0 | 100% | |
| B-DBO | 0 | 4 | 0 | 0 | 100% | |
| B-CD | 0 | 4 | 0 | 0 | 100% | |
| V-IP | 0 | 4 | 0 | 0 | 100% | 100% |
| V-PDC | 0 | 4 | 0 | 0 | 100% | |
| S-IS | 0 | 4 | 0 | 0 | 100% | 100% |
| S-SD | 0 | 4 | 0 | 0 | 100% | |
| A-ISA | 0 | 4 | 0 | 0 | 100% | 100% |
| M-IS | 0 | 4 | 0 | 0 | 100% | 100% |

Table 4.16 HTC Aria: % Change in Folder Content by Device and Category

| | | Number of Differences | | | | |
|---|---|---|---|---|---|---|
| Unique Test ID | Identical | Different | Without Peers | # Folders | % Δ | Categorical % Δ |
| S-IS | 1 | 4 | 0 | 1 | 80% | 80% |
| S-SD | 1 | 4 | 0 | 1 | 80% | |
| V-IP | 1 | 4 | 0 | 1 | 80% | 80% |
| V-PDC | 1 | 4 | 0 | 1 | 80% | |
| C-IN | 1 | 4 | 0 | 1 | 80% | 80% |
| C-NA | 1 | 4 | 0 | 1 | 80% | |
| C-AD | 1 | 4 | 0 | 1 | 80% | |
| B-IO | 1 | 4 | 0 | 1 | 80% | 80% |
| B-OC | 1 | 4 | 0 | 1 | 80% | |
| B-GD | 1 | 4 | 0 | 1 | 80% | |
| B-DDB | 1 | 4 | 0 | 1 | 80% | |

Table 4.17 Nokia Nuron 5230: % Change in Folder Content by Device and Category

| | | Number of Differences | | | | |
|---|---|---|---|---|---|---|
| Unique Test ID | Identical | Different | Without Peers | # Folders | % Δ | Categorical % Δ |
| P-IN | 3 | 4 | 7 | 1 | 78.571% | 82.1% |
| P-ND | 1 | 4 | 2 | 1 | 85.714% | |
| P-DE | 1 | 4 | 2 | 1 | 85.714% | |
| S-IS | 3 | 4 | 1 | 1 | 62.5% | 62.5% |
| M-SMSMMS | 1 | 4 | 3 | 1 | 87.5% | 87.5% |
| C-IN | 1 | 4 | 0 | 1 | 80% | 80% |
| C-NA | 1 | 4 | 0 | 1 | 80% | |
| C-AD | 1 | 4 | 0 | 1 | 80% | |

### 4.1.4 Modified PIFPM

Given the results from Experiments 1 & 2, the preliminary model presented in Figure 3.1 has been modified to incorporate a model for manual examination. The altered design is derived with the results from Experiment 2 superseding those of Experiment 1 unless there is only 1 test result available in one specific smartphone category. If this is

the case, the results from Experiment 1 will take precedence. If there are several categories in Experiment 2 that result in the same average percentage of content change, Experiment 1 will take precedence as well. The rule of thumb is that the more files available for comparison in Experiment 2, the stronger the results.

The categorical examination order of each smartphone is given in Table 4.18. It shows the examination orders from Experiments 1 & 2 and also the actual examination order. In three instances, the order placement of categories matches from Experiment 1 and Experiment 2. Both experiments found that manual manipulation of the Contact Category results in the greatest amount of file size change as well as the greatest amount of content change to the Apple iPhone. Also, both experiments show that the Nokia Nuron 5230 has the least amount of change regarding the SMS Category and the second most amount of change in the Picture Category. Given that the Blackberry 8703e did not have results for several categories, it is deduced that since it performs most like the Blackberry 8530 that it will have an examination order similar to the device as well. This explains why the final order of the Blackberry 8703e does not mirror the order from Experiment 1. Figure 4.3 shows the resulting changes to PIFPM.

PIFPM has been modified to allow examiners a choice in how to proceed in the examination after the Classification Phase by producing a Manual Examination Phase along path one. Following this path, the forensic examiner will choose the platform of the device being examined and follow the order of manual examination given. Once this has been achieved, the examiner can proceed to the Interpretation Phase or revisit the Manual

Examination Phase. Path two consists of the Automated Examination Phase as presented in Section 3.2.

Table 4.18 Manual Examination Order

| Device | Experiment 1 Order | Experiment 2 Order | Final Order |
|---|---|---|---|
| Apple iPhone | Picture, Call | SMS | SMS |
| | Browser | Picture | Picture |
| | SMS | Call | Call |
| | MMS | MMS | MMS |
| | Contact | Browser | Browser |
| | | Contact | Contact |
| | | | |
| Blackberry 8530 | Picture | MMS, Call, Browser, Picture | Picture |
| | Contact | SMS | Browser |
| | Browser | Contact | Call |
| | Call | | MMS |
| | MMS | | SMS |
| | SMS | | Contact |
| | | | |
| Blackberry 8703e | Contact | -- | Picture |
| | Call | -- | Browser |
| | SMS | -- | Call |
| | | | MMS |
| | | | SMS |
| | | | Contact |
| | | | |
| HTC TouchPro 6850 | SMS | -- | SMS |
| | Call | -- | Call |
| | Browser | -- | Browser |
| | MMS | -- | MMS |
| | Contact | -- | Contact |
| | Picture | -- | Picture |
| | | | |
| HTC Aria | Contact | -- | Contact |
| | Call | -- | Call |
| | Browser | -- | Browser |
| | SMS | -- | SMS |
| Nokia Nuron 5230 | SMS | SMS | SMS |
| | MMS | Contact | Contact |
| | Picture | Picture | Picture |
| | Contact | MMS | MMS |

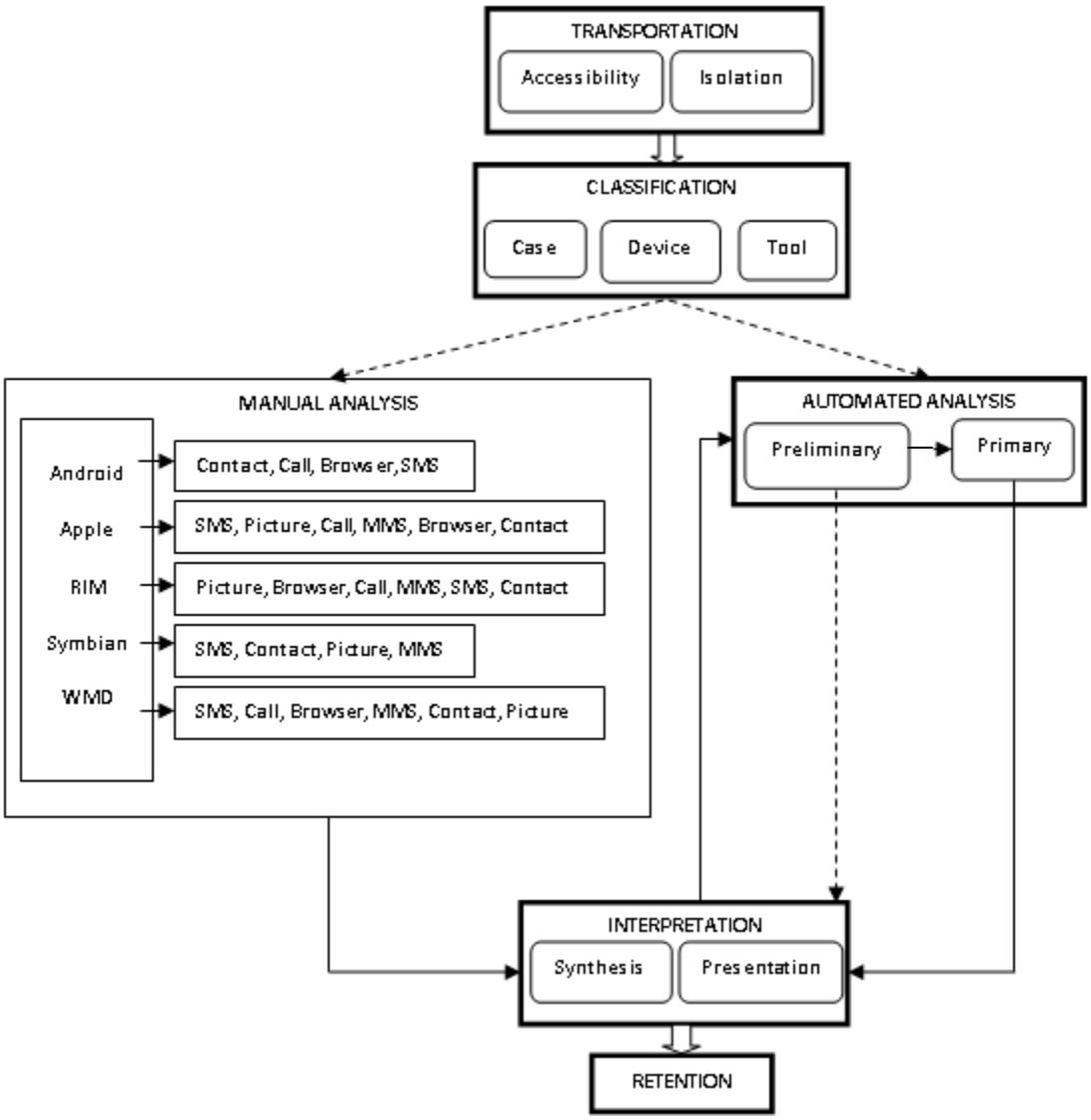


Figure 4.3 PIFPM

### 4.1.5 Qualitative Study Design

The observable population consists of three professional forensic examiners with varying years of experience examining many different devices including smartphones. The researcher traveled to each participant in his perspective location. The participants

were interviewed concerning their current process when examining mobile devices as well as the usage of any equipment. Then, the participant examined the proposed model while a presentation was given about PIFPM. After the presentation was completed, the participants were allowed to ask any questions they had about the model. A follow-up survey was given that captured qualitative data regarding usefulness, feasibility, weaknesses, and strengths of PIFPM.

### 4.1.6 Qualitative Analysis Results

Each participant was interviewed separately in an effort to maintain an unbiased environment. Tables 4.19 – 4.21 contain the interview notes from each participant. Each person was asked the same four questions in an attempt for uniformity, but each examiner was also asked one or more follow-up questions. The answers to the interview questions allowed the researcher to discover a theme that could possibly be verified through interviews with a larger population set. Examiners ME-A and ME-B, from the same organization, almost follow the same process from beginning to end. They also use the same tool, almost never deviating. On the other hand, Examiner SE-A uses a more ad-hoc process where he adapts to his environment depending on the type of OS being dealt with. ME-A and SE-A were both asked the same follow-up question after the researcher inquired about their specific process which was, "What happens if [your process] does not work?". ME-A said that they return the phone to its owner without trying any other tool other than Cellebrite. When asked about XRY in particular, he said that anything XRY can read, Cellebrite can read and if Cellebrite cannot read the device, XRY cannot

read the device either. On the other hand, SE-A said that they go on to the other tools in their arsenal to see if any of those can extract the data. If none of the other tools comply, the examiner returns the phone to the user. He also added that if the client still wants the information to be extracted without the use of tools, they usually return the phone to them and instruct them to look for the information manually.

While mapping the interviewees with their particular responses, it was discovered that each examiner had once before manually examined a device. In every case, with each examiner, the process used in these instances was the same. They take photographs of every action taken by the examiner on the device. SE-A was then asked another follow-up question concerning whether or not he has ever examined a device manually for a reason other than to be used in a court of law. His answer was, "Sure".

The next question was purely a question that stemmed from curiosity. The researcher asked them whether or not they ever examined two phones of the same make/model and compared them to see what affect their actions had on the OS. The answers from each examiner were that they had not done so either because they had not had the opportunity or that they never had a reason to.

Next, the examiners were asked whether or not there was a particular model smartphone that they feel more confident in examining over others. SE-A and ME-A both said no, but ME-B said that he likes examining anything but a Samsung Galaxy or an iPhone. When inquiring why, the examiner mentioned that no tool in his organization could break into the phone if it were passcode protected. The only thing they would be

able to do is extract the SIM card and get whatever information is available there or ask a federal agency for the tool that can break into the phones.

Table 4.19 Recorded Observations and Interview Notes for Participant SE-A

| *The National Center for Forensics Mississippi State University, MS September 19, 2012 1:15 PM SE-A* | *Interviewee's Response* | *Interviewer's Follow-up Question* | *Interviewee's Response* |
|---|---|---|---|
| Question 1: Do you follow a particular process when examining a mobile device? | "Not really. Well, it really depends on the OS. If it is a feature/flip phone [not Android or IOS], we start with XRY." | FUQuestion 1: What happens if that does not work? | We go on to the other tools that we have until one works. If it doesn't work, we return the device to its owner and suggest that they find it manually. |
| Question 2: Have you ever had to manually examine a mobile device? | Yes. We take photos of the screen when doing so, but this does not happen often. | FUQuestion 2: Have you ever manually examined a device for reasons not law related? | Yes, for example, there was a lady whose son committed suicide and she just wanted to know if there were any texts, pics, etc. on the device that could shed some light as to why he did what he did. |
| Question 3: Have you ever examined two phones of the same make/model and compared the results of how the OS is affected? | No. We have never had two clients come in with the exact same phones so we have never thought of doing so because we have never had that chance. | | |
| Question 4: Is there one device that you feel more confident in examining than others? | No. Not particularly | | |

Table 4.20 Recorded Observations and Interview Notes for Participant B

| *Attorney General's Office*<br>*Jackson, MS*<br>*September 20, 2012*<br>*10:25 AM*<br>*ME-A* | *Interviewee's Response* | *Interviewer's Follow-up Question* | *Interviewee's Response* |
|---|---|---|---|
| Question 1: Do you follow a particular process when examining a mobile device? | "Yes. We take pictures, power the device on, hook it up to Cellebrite once we know that it is passcode free, extract the data, and make an html report." | FUQuestion 1: What happens if that does not work? | We don't examine it. |
| Question 2: Have you ever had to manually examine a mobile device? | Yes. We take pictures of the process | | |
| Question 3: Have you ever examined two phones of the same make/model and compared the results of how the OS is affected? | No. We never have had a reason to. | | |
| Question 4: Is there one device that you feel more confident in examining than others? | Not really | | |

Table 4.21 Recorded Observations and Interview Notes for Participant C

| *Attorney General's Office*<br>*Jackson, MS*<br>*September 20, 2012*<br>*10:45 AM*<br>*ME-B* | *Interviewee's Response* | *Interviewer's Follow-up Question* | *Interviewee's Response* |
|---|---|---|---|
| Question 1: Do you follow a particular process when examining a mobile device? | "Yes. We check to see where it came from, after a search warrant has been obtained; we use Cellebrite due to its simplicity." | FUQuestion 1: Why don't you particularly care to examine Galaxies or iPhones? | If it is passcode protected, nothing in this office can break into it. |
| Question 2: Have you ever had to manually examine a mobile device? | Yes. This sometimes happens when we are in the field. We photograph the process. | FUQuestion 2: What do you do if it is passcode protected? | The FBI has software that will extract the passcode, but it will not break the Galaxy code. So we take out the SIM card and extract as much as possible from it. |
| Question 3: Have you ever examined two phones of the same make/model and compared the results of how the OS is affected? | No. I have never had the opportunity to do so. | | |
| Question 4: Is there one device that you feel more confident in examining than others? | Anything but the iPhone or the Samsung Galaxy | | |

Table 4.22 Participant Comments

| | | |
|---|---|---|
| *SE-A* | "I think it's cool. It would be great for examiners to use because there would be something out there to follow." | Overall, the model looks good. As far as the manual examination path, I would look at the browser information on an Android device last. Every time the browser is loaded, all the windows that were opened during its last use reload in the browser. There are also different browsers that can be downloaded and used. As a matter of fact, to be on the safe side, it would not hurt to look at the browser information on all the devices last, despite the type of OS. |
| *ME-A* | In my opinion, you can't perform a forensic examination on a smartphone because it alters the entire makeup of a phone when you examine it. I testify in court often and the prosecutor or DA could eat me for lunch for calling an examination on a smartphone a forensic examination. When saying that [you are conducting a forensic examination], you assume that it can be repeated and the device can be verified by hashing. But we know that if we take a hash value of the phone in one state and conduct an examination, the hash value will be different after the conclusion of the examination. For this reason, I refer to it as a smartphone examination. | |
| *ME-B* | This is a logical model. The only thing I would change is the order of manual examination for the iPhone. I would look at the browser information last. | |

After the presentation of PIFPM was given, the participants were allowed to ask any questions or make any comments about the model. Each comment made by each participant can be found in Table 4.22.

Table 4.23 gives us a breakdown of the interview information as well as the participants' affiliations. All participants were males with two having 3 – 4 years of experience and the other having 2 – 3. Given this information, the researcher created two categories pertaining to experience since some of the research questions deal with that in particular. The categories are More Experience (ME) and Some Experience (SE). Using this information, eight frequency/percent tables were created outlining each question that deals with the hypotheses as well as a Rankings and Medians Table. To follow is a discussion of the responses to the questions found on the post survey.

In this study, the sampling method used was convenience sampling. In using this method, there is a possibility of bias but this method was selected due to ease of collection and the nature of the careers of the participants. This resulted in a sample size insufficient to support this work with great confidence. In determining the confidence interval of the survey data given here, it can be stated with 95% confidence that if the same population is sampled on numerous occasions and interval estimates are made on each occasion, the resulting intervals would bracket the true population in approximately 56.58% of the cases [18]. Tables 4.24 – 4.32 are reported based upon this data.

Given this, the margin of error is well beyond what is acceptable by the researchers. In order to alleviate this, the study will have to be repeated in order to obtain a sample size of at least 24. We will then be able to state that the margin of error is 20%

that the answers will represent those reported 95% of the time. In order to absolve all doubt, as part of future work, the researchers plan to survey a total of 384 forensic examiners in order to obtain a confidence interval of 5% [18].

Question 2 asked the participants how difficult PIFPM was to understand. The response frequency and percents are broken down by group and mapped to each response given on the survey as seen in Table 4.24. The SE Group and 50% of the ME Group feel that PIFPM is not at all difficult to understand and the other half of the ME Group feel that it was somewhat difficult to understand.

Question 3 asked the participants to rate how feasible PIFPM would be in its application to the forensic processing of smartphones. Table 4.25 shows that the SE group and 50% of the ME Group feel that it is extremely feasible. The remaining 50% of the ME Group feel that PIFPM is somewhat feasible.

Table 4.23 Post Survey Participant/Interview Information

| Participant | Location | Date/Time | M/F | Years' Experience |
|---|---|---|---|---|
| ME-A | Attorney General's Office<br>Sillers Building<br>Jackson, MS | 9/20/12<br>10:25 AM | M | 3-4 |
| ME-B | Attorney General's Office<br>Sillers Building<br>Jackson, MS | 9/20/12<br>10:45 AM | M | 3-4 |
| SE-A | The National Center for Forensics<br>Mississippi State University, MS | 9/19/12<br>1:15 PM | M | 2-3 |

Table 4.24 Question 2 Frequency/Percent Distribution by Group

| **Q2. How difficult is PIFPM to understand?** | | |
|---|---|---|
| Option | SE Group Distribution Frequency/Percent | ME Group Distribution Frequency/Percent |
| Not Difficult | 1/100% | 1/50% |
| Slightly Difficult | 0/0% | 0/0% |
| Somewhat Difficult | 0/0% | 1/50% |
| Very Difficult | 0/0% | 0/0% |
| Extremely Difficult | 0/0% | 0/0% |

Table 4.25 Question 3 Frequency/Percent Distribution by Group

| **Q3. Rate how feasible PIFPM would be in its application to the forensic processing of smartphones?** | | |
|---|---|---|
| Option | SE Group Distribution Frequency/Percent | ME Group Distribution Frequency/Percent |
| Not at all feasible | 0/0% | 0/0% |
| Slightly feasible | 0/0% | 0/0% |
| Somewhat feasible | 0/0% | 1/50% |
| Very feasible | 0/0% | 0/0% |
| Extremely feasible | 1/100% | 1/50% |

Question 4 asked each participant how likely he would be to incorporate PIFPM into his forensic examination process and Table 4.26 shows the frequency and percentage of the responses from each group. The SE Group reported that it would be extremely likely to incorporate PIFPM into their forensic process. The ME Group is split. Half of the group reported to be very likely to incorporate the model whereas the other half reported that it would be somewhat likely to use PIFPM in their examination process.

Question 5 asked the examiners which phases do not fit the logical progression of a forensic examination out of the following: Transportation, Classification, Analysis, and Interpretation. If they felt that all of the phases are logical, they had the opportunity to circle that choice as well. 100% of both groups feel that all of these phases seem logical as shown in Table 4.27.

Question 6, as seen in Table 4.28, asked each participant how useful PIFPM would be in a smartphone examination. The SE Group feels that PIFPM would be extremely useful. The ME Group is split. 50% of the group feels that PIFPM would be very useful, whereas the other half feel that the model would be somewhat useful.

Table 4.26 Question 4 Frequency/Percent Distribution by Group

| **Q4. How likely would you be to incorporate PIFPM into your forensic examination process?** | | |
|---|---|---|
| Option | SE Group Distribution Frequency/Percent | ME Group Distribution Frequency/Percent |
| Not likely | 0/0% | 0/0% |
| Slightly likely | 0/0% | 0/0% |
| Somewhat likely | 0/0% | 1/50% |
| Very likely | 0/0% | 1/50% |
| Extremely likely | 1/100% | 0/0% |

Table 4.27 Question 5 Frequency/Percent Distribution by Group

| **Q5. Of the phases listed below, which one(s) do not fit the logical progression of a forensic examination?** | | |
|---|---|---|
| Option | SE Group Distribution Frequency/Percent | ME Group Distribution Frequency/Percent |
| Transportation | 0/0% | 0/0% |
| Classification | 0/0% | 0/0% |
| Analysis | 0/0% | 0/0% |
| Interpretation | 0/0% | 0/0% |
| All seem logical | 1/100% | 2/100% |

Table 4.29 shows the frequency and percent of the responses given for Question 8. This question asked the participants whether it is logical for smartphones to use the same forensic process model as computers. The SE Group and half of the ME Group feel that it is somewhat logical to use the same forensic process model as computers. The remainder of the ME Group feels that it is very logical.

Table 4.28 Question 6 Frequency/Percent Distribution by Group

| **Q6. How useful is PIFPM in a smartphone examination?** | | |
|---|---|---|
| Option | SE Group Distribution Frequency/Percent | ME Group Distribution Frequency/Percent |
| Not useful at all | 0/0% | 0/0% |
| Slightly useful | 0/0% | 0/0% |
| Somewhat useful | 0/0% | 1/50% |
| Very useful | 0/0% | 1/50% |
| Extremely useful | 1/100% | 0/0% |

Table 4.29 Question 8 Frequency/Percent Distribution by Group

| **Q8. Is it logical for smartphones to use the same forensic process model as computers?** | | |
|---|---|---|
| Option | SE Group Distribution Frequency/Percent | ME Group Distribution Frequency/Percent |
| Not logical | 0/0% | 0/0% |
| Slightly logical | 0/0% | 0/0% |
| Somewhat logical | 1/100% | 1/50% |
| Very logical | 0/0% | 1/50% |
| Extremely logical | 0/0% | 0/0% |

Question 9 asked each participant how often he manipulates the process he uses to examine smartphones. Table 4.30 shows that the SE Group changes the process somewhat often. Half of the ME Group reported that its process does not change often when examining smartphones and the remainder of the group reported that change occurs slightly often.

Table 4.31 reports the frequency and percent of the responses for Question 14 on the survey. Each examiner was asked whether he believed that incorporating PIFPM into smartphone examinations would change the confidence level of the investigator. The SE Group feels that using PIFPM would elevate the confidence level of the investigator greatly and the ME Group feels that using the model would elevate the confidence level of the investigator slightly.

Table 4.30 Question 9 Frequency/Percent Distribution by Group

| **Q9. How often do you manipulate the process you frequently use to examine smartphones, whether intentionally or unintentionally?** | | |
|---|---|---|
| Option | SE Group Distribution Frequency/Percent | ME Group Distribution Frequency/Percent |
| Not often | 0/0% | 1/50% |
| Slightly often | 0/0% | 1/50% |
| Somewhat often | 1/100% | 0/0% |
| Very often | 0/0% | 0/0% |
| Extremely often | 0/0% | 0/0% |

Table 4.31 Question 14 Frequency/Percent Distribution by Group

| **Q14. Do you believe that incorporating PIFPM into phone examinations will change the confidence level of the investigator?** | | |
|---|---|---|
| Option | SE Group Distribution Frequency/Percent | ME Group Distribution Frequency/Percent |
| Yes, it will lower the confidence level greatly | 0/0% | 0/0% |
| Yes, it will lower the confidence level slightly | 0/0% | 0/0% |
| No, the confidence level will not change | 0/0% | 0/0% |
| Yes, it will elevate the confidence level slightly | 0/0% | 2/100% |
| Yes, it will elevate the confidence level greatly | 1/100% | 0/0% |

The survey also contained two questions that asked each examiner to list any strengths and weaknesses they could discern from evaluating the model during the presentation. Table 4.32 reports the number of weaknesses and strengths outlined by the examiners. The SE Group reported one weakness and one strength. The ME Group reported 1 weakness and 3 strengths.

Table 4.33 shows the three discussion questions asked to the examiners as shown on the survey. The first discussion question asked each participant whether PIFPM offered anything to an examination that other models do not. One examiner had no response because he said that he could not answer it. Another examiner reported that he had no model for comparison, and the last examiner reported, “Not that I am aware of”.

The second discussion question asked the examiners what strengths PIFPM offers to the examination of a smartphone. One examiner reported that it offers good guidelines on the next step to take in most situations. Another examiner reported that it gives them an orderly process to follow and it also ensures the same process is followed each time. The last examiner reported that the model offers them diversity.

The final discussion question asked the examiners what weaknesses PIFPM offers to a forensic examiner in a smartphone investigation. One examiner reported that it will need to adapt as [smartphone] OS's change. Another examiner reported that given the amount and frequency of updates on phones, inconsistency would be an issue. The last examiner had no weaknesses to report.

Table 4.34 contains the responses for each question that relates to our hypotheses and ranks the answers from 1 – 5 using a mapping created from the available responses labeled a – e. The median values are the values used to either support or refute our hypotheses and assist in answering Research Question 2 (R2) and Research Question 4 (R4). Table 4.35 shows a mapping of the research questions to the hypotheses and to the survey questions.

Table 4.32 Number of Reported PIFPM Weaknesses vs. Strengths

| | SE Group Distribution Frequency | ME Group Distribution Frequency |
|---|---|---|
| Strengths | 1 | 3 |
| Weaknesses | 1 | 1 |

Table 4.33 Post Survey Discussion Questions

| | |
|---|---|
| Q1 | Does PIFPM offer anything to an examination that other models do not? |
| Q2 | What strengths does PIFPM offer to a forensic examiner in a smartphone investigation? |
| Q3 | What weaknesses does PIFPM offer to a forensic examiner in a smartphone investigation? |

R2 maps to Hypothesis 2a (H2a), Hypothesis 2b (H2b), and Hypothesis 2c (H2c) in Table 4.35. H2a states that "Most examiners will find PIFPM to be at least somewhat feasible". Table 4.34 shows that the median answer for survey Q3 is "Extremely feasible". As a result, the qualitative data is shown to support H2a. H2b states that "Most examiners will find that all the proposed phases fit the logical progression of a smartphone forensic examination". Table 4.34 shows that the median answer for survey Q5 is "All seem logical". As a result, the qualitative data is shown to support H2b. H2c states that "Examiners regardless of experience will find that PIFPM is not difficult". Table 4.34 shows that the median answer for Q2 is "Not difficult". As a result, the qualitative data is shown to support H2c. Given that all the hypotheses derived for Research Question 2 are supported by the qualitative data, it is reasonable to believe that it is feasible to include PIFPM in the current process to examine smartphones.

Table 4.34 Post Survey Response Rankings and Medians

| **Question** | **Q2** | **Q3** | **Q4** | **Q5** | **Q6** | **Q8** | **Q9** | **Q14** |
|---|---|---|---|---|---|---|---|---|
| AGO-A | 3 | 5 | 4 | 5 | 3 | 4 | 1 | 4 |
| AGO-B | 1 | 3 | 3 | 5 | 4 | 3 | 2 | 4 |
| NCF-A | 1 | 5 | 5 | 5 | 5 | 3 | 3 | 5 |
| *Median* | 1 | 5 | 4 | 5 | 4 | 3 | 2 | 4 |

Table 4.35 Research Questions, Hypotheses, and Survey Questions Mapping

| Research Question | Hypothesis | Initially Supported Y or N | Post Survey Question |
|---|---|---|---|
| R1. How useful is PIFPM in a smartphone examination? | H1a. Examiners with less experience will find PIFPM to be at least somewhat useful. | Y | Q6 |
| | H1b. Examiners with more experience will find PIFPM to be at least slightly useful. | N | |
| | H1c. Examiners with less experience will be more likely to incorporate PIFPM into their forensic examination process than examiners with more experience. | Y | Q4 |
| | H1d. Examiners with more experience will be less likely to incorporate PIFPM into their forensic examination process than examiners with less experience. | Y | |
| R2. Is it feasible to include PIFPM in the current process for examining smartphones? | H2a. Most examiners will find PIFPM to be at least somewhat feasible. | Y | Q3 |
| | H2b. Most examiners will find that all the proposed phases fit the logical progression of a smartphone forensic examination. | Y | Q5 |
| | H2c. Examiners, regardless of experience will find that PIFPM is not difficult. | Y | Q2 |
| R3. Does PIFPM offer anything to a smartphone investigation that other models do not? | H3a. Examiners with less experience will find that PIFPM has more strengths than weaknesses. | N | Q12, Q13, Q7 |
| | H3b. Examiners with more experience will find that PIFPM has more weaknesses than strengths. | N | |
| R4. Is it logical to suggest that every category of technological device should assume a unique forensic process model? | H4. Examiners, regardless of experience, will not find that it is very logical to use the same process model to examine smartphones and computers. | Y | Q8 |
| R5. Do examiners, whether intentional or not, manually manipulate current process models in order to suit specific model smartphones? | H5a. Examiners with less experience do not manipulate current process models often. | N | Q9 |
| | H5b. Examiners with more experience do manipulate current process models often. | N | |

R4 maps to Hypothesis 4 (H4). H4 states that "Examiners, regardless of experience, will not find that it is very logical to use the same process model to examine smartphones and computers". Table 4.34 shows that the median answer for survey Q8 is

"Somewhat logical". As a result, the qualitative data is shown to support H4. Given that the hypothesis derived for Research Question 4 is supported by the qualitative data, it is reasonable to suggest that every category of technological device should assume a unique forensic process model.

In order to support or refute Research Questions 1 and 5, the researcher has to refer back to the frequency and percent tables shown earlier because these questions are based on experience. Research Question 1 (R1) maps to Hypothesis 1a (H1a), Hypothesis 1b (H1b), Hypothesis 1c (H1c), and Hypothesis 1d (H1d). H1a states that "Examiners with less experience will find PIFPM to be at least somewhat useful". Table 4.28 shows that the SE Group reported to find PIFPM very useful. Since the SE Group is the group with less experience than the ME Group, H1a is supported by the qualitative data. H1b states that "Examiners with more experience will find PIFPM to be at least slightly useful". Table 4.28 shows that the median response maps between "Somewhat useful" and "Very useful". The researcher believed that a more experienced examiner may not be as open to change as a less experienced examiner, but this was not the case in this instance. As a result, H1b is not supported by the qualitative data. H1c states that "Examiners with less experience will be more likely to incorporate PIFPM into their forensic examination process". H1d states that "Examiners with more experience will be less likely to incorporate PIFPM into their forensic examination process". Table 4.26 shows that the SE Group reported to find that it is extremely likely that they would incorporate PIFPM into their examination whereas the ME Group reported that their likelihood of incorporating PIFPM into their examination would be the median of "Very

likely" and "Somewhat likely". Given our mapping scale, the data shows that the group with the least amount of experience would be more likely to incorporate the model into the daily examination than the group with the most experience. As a result, both H1c and H1d are supported by the qualitative data. Given that three of the four hypotheses derived for Research Question 1 are supported by the qualitative data, that Table 4.34 reports the median response of the usefulness of PIFPM as being "very useful", and the likelihood of the examiner incorporating the model into the daily routine as being "very likely", it is reasonable to believe that PIFPM would be at least somewhat useful in a smartphone examination.

Research Question 5 (R5) maps to Hypothesis 5a (H5a) and Hypothesis 5b (H5b). H5a states that "Examiners with less experience do not manipulate current process models often" and H5b states that "Examiners with more experience do manipulate current process models often". Table 4.30 shows that the SE Group reported that it manipulates its process somewhat often whereas the ME Group reported that its frequency of manipulation would be the median of "Not often" and "Slightly often". As a result, both H5a and H5b are not supported by the qualitative data. In deriving these hypotheses, the researcher believed that the less experienced examiner would be less likely to change their routine and skew from the norm. It was also the belief of the researcher that the more experienced examiner would be more likely to change their process mainly due to lessons learned. Even though the hypotheses are not supported by the data, Table 4.34 shows that the median response for all participants is that they manipulate their process slightly often, which answers R5.

Lastly, Research Question 3 (R3) was answered by using the frequencies reported in Table 4.32. R3 maps to Hypothesis 3a (H3a) and Hypothesis 3b (H3b). H3a states that "Examiners with less experience will find that PIFPM has more strengths than weaknesses". H3b states that "Examiners with more experience will find that PIFPM has more weaknesses than strengths". Table 4.32 shows that the SE Group reported the same amount of weaknesses and strengths, and the ME Group reported more strengths than weaknesses. Given this, the qualitative data refutes both H3a and H3b. This question was also asked to the participants verbatim in Question 7 on the survey. As mentioned previously, the participants had no answer for this question for various reasons. Therefore, the researcher is not able to answer R3 which asks whether PIFPM offers anything to a smartphone investigation that other models do not based on the qualitative data in this study.

Although the results given in the surveys are not statistically significant, there were several lessons that can be taken away from the qualitative portion of the study based on whether or not they would actually apply PIFPM, instances in which they would or would not use the model, what they would change about PIFPM, and their overall opinion of the model.

The author asked the participants, after they experienced the model and its uses, if and how they would incorporate PIFPM into their examinations and the response was unanimously positive. No participant reported that they would decline to incorporate it into their work. For example, Participant A reported that he would be very open to incorporating it into his normal process because the model is not difficult to understand

and it seems logical. He would first test the model out by using it after using his normal process to compare procedures several times. If he felt comfortable with the process and results, he would then begin to incorporate it in his normal processes. Alternatively, Participant B also feels that the model is not difficult to understand, and he would feel more comfortable incorporating PIFPM if a workshop was conducted that will assist in directing examiners on how to actually approach each phase and sub-phase in the model.

When asked of any instance they could think of that they would not feel comfortable incorporating PIFPM, Participant C stated that because he does not feel comfortable examining Android and Apple mobile devices, he would more than likely not use the model on these devices. Participant B felt that he may not feel comfortable testifying in a court of law based on this model without some experience.

The participants were asked what aspects of PIFPM they would change given the fact that they are practicing examiners, Participant A would change the order of manual examination. Given that the browser of most smartphones reloads all the windows last used, he would change this category to the last category viewed on an Android device. After further thought, he also decided that this should probably be the case for every OS smartphone. Participant C also mentioned that the browser information for the Android and Apple mobile devices should be listed last. Other than that, he said that he would not change anything from this initial introduction. Participant B felt that he could not decide what he would change in theory, but after he has been able to apply the practices of the model, he could give a more accurate response to this question.

The researcher inquired how the participants felt about the model overall. Participant A felt that the model was "cool" and that it would be great because there would be something out there to follow. Participant B did not have any negative feedback of the model itself. He questioned the use of the word 'forensics' when referring to the examination of a smartphone due to the fact that smartphone examinations always change the state of the device and forensic examinations are not supposed to make changes. This is true in general, but there is no method in general that is guaranteed to preserve the state of a smartphone or any cell phone during examination. This is accepted practice and can be explained in court. Participant C felt that the model seemed to be an overall logical one and that he would have more of an opinion after being able to apply the model.

# CHAPTER V

# CONCLUSIONS

This chapter gives a summary of the contributions offered by this research and possible avenues of future work.

## 5.1 Contributions

The extendable framework, PIFPM, presented will provide examiners with a process model for the purpose of inspecting any model smartphone conscious of the unique qualities belonging to each. After reviewing the models already established, it was discovered that no such model existed. After its development, a qualitative study was disseminated in an effort to gauge the openness of forensic researchers, examiners, and scholars to a model designed only for smartphones. The researcher then conducted several quantitative studies in an effort to reveal any new information about the different smartphones. After this study, the researcher modified the design of PIFPM to include a path for manual examination based on the information discerned in the File Size Difference and the Average Change in Content experiments. After the change in design, the researcher conducted one more qualitative study. The data gathered through interviews and surveys in this study were used to help initially support or not support the hypotheses derived. Conclusions about the research questions were drawn based on the results of the data gathered through analyses, the interpretation of the qualitative data in

the post interviews and surveys, the experiences of practicing examiners, and the outcome of each hypothesis. The researcher plans to conduct future studies that will result in statistical significance.

PIFPM contributes to the area of Digital Forensics in several ways. Firstly, it is unique in that it is the only model of its kind that offers any type of process for examiners to follow when dealing with any model smartphone. There is no way we can standardize mobile device OS development so that there will never be another mobile OS to emerge. Because the model has been designed to be extendable in an effort to account for any make/model smartphone, it will not be obsolete when new operating systems are introduced. Secondly, PIFPM provides a standard process for all examiners to follow. Utilizing this model will provide a specific roadmap for smartphone examiners to follow just as computer forensic examiners have the DFWRS model. In the words of one of the participants on the post survey, "At least there'll be *something* out there to follow". Thirdly, the smartphone examiners will now feel more confident in examining smartphones knowing that there is a standard model that others will be following as well that has been tailored to the unique issues that limit smartphone forensics. Lastly, although in its infancy, the model presents the opportunity for the refinement of smartphone forensic processes and may assist in launching the development of a forensically sound tool for any model smartphone.

## 5.2 Publications

The papers that have been published from this research are as follows:

Refereed Journal Paper

*Dancer, F. Chevonne Thomas and Dampier, David A, "Refining the Digital Device Hierarchy," Journal of the Academy of Sciences, vol. 55, no. 4, October 2010.*

Refereed Conference Paper

*Dancer, F. Chevonne Thomas and Dampier, David A., "A Platform Independent Process Model for Smartphones Based on Invariants," Proceedings: 2010 Fifth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, 20, May, 2010.*

Refereed Journal Paper

*Dancer, F. Chevonne Thomas; Dampier, David A.; Jackson, Jacqueline M.; and Meghanathan, Natarajan, "A Theoretical Process Model for Smartphones," Proceedings: 2012 Second International Conference on Artificial Intelligence, Soft Computing and Applications, Chennai, India, 13-15, July 2012.*

## 5.3 Recommendations for Future Work

There are several avenues for future work. The researcher plans to experiment with several more model smartphones. Even though all the phones in the experiments were not activated through a carrier and information was still gleaned from the experiments, the researcher would like to perform similar studies using devices that have been activated through the carrier that manufactured the device as well as different carriers in an effort to contrast the functionality of each. Another avenue of experimentation would be comparing the influence each activity has on the operating system to every other activity belonging in its category. In the same token, the researcher

could also try and determine whether one activity causes the same number of files to change or not change as the next activity. The same can be done regarding file size. Similarly, the researcher could compare the influence each activity has on the operating system to every other activity belonging to a different category. An experiment could also be conducted in order to determine the types of files changed by certain activities whether they are log file, word processing files, data files, etc. A similar experiment may be able to tell us whether certain functions cause certain areas of memory to be populated sporadically or in some sort of methodical fashion. Additionally, more experimental trials will be run to strengthen the statistical observations in the use of the model.

REFERENCES


1. M. W. Andrew, "Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media," *Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2007, pp. 16-30.

2. V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model," *Digital Forensics Research Workshop*, August 2004.

3. N. L. Beebe and J. G. Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process," *Digital Investigation*, vol. 2, no. 2, 2005, pp. 146-166.

4. Blackberry, "Fundamentals Guide - Blackberry Java Development Environment: Blackberry device memory," http://docs.blackberry.com/en/developers/deliverables/5827/BB_device_memory_447111_11.jsp (Current Sep. 15, 2010).

5. R. C. Bogdan and S. K. Biklen, *Qualitative research in education: An introduction to theory and methods* (3rd ed.), Needham Heights, MA: Allyn & Bacon (1998).

6. A. C. Bogen, "Selecting Keyword Search Terms in Computer Forensics Examinations Using Domain Analysis and Modeling," Dissertation, Department of Computer Science and Engineering, Mississippi State University, Mississippi State, 2006.

7. D. Bradford, A. Ray, and G. Phillip, "Models of Models: Digital Forensics and Domain-Specific Languages," 2007; http://www.ioc.ornl.gov/csiirw/07/abstracts/Bradford-Abstract.pdf(Current Sep. 15, 2010).

8. M. Breeuwsma, M. de Jongh, C. Klaver, R. vander Knijff, and M. Roeloffs, "Forensic Data Recovery From Flash Memory," *Small Scale Digital Forensics Journal*, vol. 1, no. 1, 2007.

9. B. Carrier, "A Hypothesis-Based Approach to Digital Forensic Investigations," *International Journal of Digital Evidence*, vol. 2, no. 2, 2006.

10. B. D. Carrier and E. H. Spafford, "An Event-Based Digital Forensic Investigation Framework," *Book An Event-Based Digital Forensic Investigation Framework*, Series An Event-Based Digital Forensic Investigation Framework, ed., 2004, pp.

11. S. Choney, "2009: Cell phone sales will be down but not out," 2009; http://www.msnbc.msn.com/id/28316931/(Current Sep. 15, 2010).

12. S. O. Ciardhuain, "An Extended Model of Cybercrime Investigations," *International Journal of Digital Evidence*, vol. 3, no. 1, 2004, pp. 1-22.

13. A. Distefano and G. Me, "An overall assessment of Mobile Internal Acquistion Tool," *Digital Investigation*, 2008, pp. 121-127.

14. DOJ, "United States Department of Justice: Computer Crime Cases," www.cybercrime.gov/cccases.html(Current Sep. 15, 2010).

15. S. A. C. Doyle, "Methodical Approach to Processing the Crime Scene," *An Introduction to Crime Scene Investigation*, Jones and Bartlett Publishers, 2010, pp. 103 - 133.

16. M. Goodman, "Making Computer Crime Count," *FBI Law Enforcement Bulletin*, vol. 70, no. 8, 2001, pp. 10-17.

17. V.Gratzer, D. Naccache, and D. Znaty, "Law Enforcement, Forensics and Mobile Communications," *Proc. The 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, 2006, pp. 67-70.

18. A. Graziano, *Research Methods: AProcess of Inquiry*, Pearson, 1993.

19. D. C. Harrill and R. P. Mislan, "A Small Scale Digital Device Forensics ontology," *Small Scale Digital Forensics Journal*, vol. 1, no. 1, 2007, pp. 1-6.

20. L. W. Hill, "An Inexpensive Method to Shield Wireless Devices During Hardware Forensic Investigation in a Laboratory Setting," *Book An Inexpensive Method to Shield Wireless Devices During Hardware Forensic Investigation in a Laboratory Setting*, Series An Inexpensive Method to Shield Wireless Devices During Hardware Forensic Investigation in a Laboratory Setting, ed., ACM, 2007, pp. 239-244.

21. D. Hillbert, "Über die vollen Invariantensysteme," *Math*, vol. 42, 1893, pp. 313.

22. D. Hofstadter, *Gödel, Escher, Back: An Eternal Golden Braid*, Basic Books, 1979.

23. W. Jansen and K. Scarfone, "Guidelines on PDA Forensics; Recommendations of the National Institute of Standards and Technology," *Book Guidelines on PDA Forensics; Recommendations of the National Institute of Standards and Technology*, Series Guidelines on PDA Forensics; Recommendations of the

National Institute of Standards and Technology, ed., National Institue of Standards and Technology, 2004, pp.

24. W. Jansen, A. Delaitre, and L. Moenner, "Overcoming Impediments to Cell Phone Forensics," 2008; http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/Impediments-formatted-final-post.pdf (Current Sep. 15, 2010).

25. W. Jansen and K. Scarfone, "Forensic Software Tools for Cell Phone Subscriber Identity Modules," *Proc. Conference on Digital Forensics, Association of Digital Forensics Security, and Law*, 2006, pp. 101- 113.

26. J. H. P. Eloff, M. Kohn, and M. S. Oliver, "Framework for a Digital Forensic Investigation," *Information Security South Africa (ISSA)*, 2005.

27. W. G. Kruse II and J. G. Heiser, *Computer Forensics: Incident Response Essentials*, 2001, p. 398.

28. M. Kwan, K.P. Chow, F. Law, and P. Lai, "Reasoning About Evidence using Bayesian Network," *Advances in Digital Forensics IV, International Federation for Information Processing (IFIP)*, 2008, pp. 141-155.

29. Lance Li, "Symbian OS Architecture," 2007; http://download.farsight.com.cn/download/pdf/Farsight071117Symbian02.pdf (Current Sep. 15, 2010).

30. C. Marshall and G. Rossman, *Designing Qualitative Research Fifth Edition*, Thousand Oaks, CA, Sage Publications.

31. E. V. Mavrodiev, "Classical Morphology of Plants as an Elementary Instance of Classical Invariant Theory," *PLoS One*, vol. 4, no. 9, 2009.

32. B. Morris, "Platform Security and Symbian Signed: Foundation for a Secure Platform," 2008; http://developer.symbian.com/main/downloads/papers/PlatSec_and_Symbian_Signed.pdf (Current Sep. 15, 2010).

33. R. E. Overill, M. Y. K. Kwan, K. P. Chow, Pierre K. Y. Lai, and Frank Y. W. Law, "A Cost-Effective Digital Forensics Investigation Model," *Book A Cost-Effective Digital Forensics Investigation Model*, Series A Cost-Effective Digital Forensics Investigation Model, ed., 2009, pp.

34. G. Palmer, *A Road Map for Digital Forensic Research*, First Digital Forensics Research Workshop (DFWRS), 2001.

35. M. M. Pollitt, "An Ad Hoc Review of Digital Forensic Models," *Book An Ad Hoc Review of Digital Forensic Models*, Series An Ad Hoc Review of Digital Forensic Models, ed., 2007, pp. 43 - 52.

36. S. G. Punja and R. P. Mislan, "Mobile Device Analysis," *Small Scale Digital Forensics Journal*, vol. 2, no. 1, 2008, pp. 1-16.

37. A. Ramabhadran, "Forensic Investigation Process Model for Windows Mobile Devices," http://www.forensicfocus.com/downloads/windows-mobile-forensic-process-model.pdf (Current Sep. 15, 2010).

38. M. Reith, C. Carr, and G. Gunsch, "An Examination of Digital Forensic Models," *International Journal of Digital Evidence*, vol. 1, no. 3, 2002, pp. 1-12.

39. Research In Motion, "Erasing file systems on Blackberry devices," 2008; http://na.blackberry.com/eng/deliverables/4322/Erasing%filesystems%on%Blackberry%devices%-%4.1.6%-Technical%Overview.pdf (Current Sep. 15, 2010).

40. J. Ryan, "Cellular Phones/Digital Devices and Search Incident to Arrest," August 31, 2010 2007; http://policelink.monster.com/training/articles/4921-cellular-phonesdigital-devices-and-search-incident-to-arrest (Current Sep. 15, 2010).

41. A. Savoldi and P. Gubian, "SIM and USIM Filesystem: a Forensics Perspective," *Proc. Proceedings of the 2008 ACM Symposium on Applied Computing (SAC'07)*, 2007, pp. 181-187.

42. C. Shakiban and P. Olver, "Computations in Classical Invariant Theory of Binary Forms," http://www.google.com/url?sa=t&source=web&ct=res&cd=1&ved=0CBMQFjAA&url=http%3A%2F%2Fwww.ima.umn.edu%2F2006-2007%2Fseminars%2Fshakiban%2FInvarant2.ppt&rct=j&q=Computations+in+Classical+Invariant+Theory+of+Binary+Forms+Cheri&ei=q7_lSp2YM42l8QaouNyIBw&usg=AFQjCNE0NMw33Zx8-vLLesZetamHPzP3rA (Current Sep. 15, 2010).

43. P. Stephenson, "Modeling of Post-Incident Root Cause Analysis," *International Journal of Digital Evidence*, vol. 2, no. 2, 2003.

44. J. Symons, J. Urenda, and V. Kreinovich, "Towards a General Description of Physical Invariance in Category Theory," www.johnfsymons/invariance.pdf (Current Sep. 15, 2010).

45. A. Tanner and D. Dampier, “Concept Mapping for Digital Forensic Investigations,” *Advances in Digital Forensics V*306, 2009.

46. “The International Dictionary of Applied Mathematics,”*Book The International Dictionary of Applied Mathematics*, Series The International Dictionary of Applied Mathematics, ed., Van Nostrand, 1960, pp. 1173.

47. T. Thompson, “Smartphone Operating Systems: A Developer's Perspective,” 2009; www.ddj.com/mobile/216300179?pgno=3 (Current Sep. 15, 2010).

48. *U.S. v. Finley,* 2007 (477 F.3d 250).

49. *U.S. v. Young,* 2006 (U.S. Dist W. Va.).

APPENDIX A

PRE SURVEY

Exit this survey

*1. Please choose the answer that best describes you.

○ Male ○ Female

*2. Please choose the answer that best describes your affiliation to digital forensics.

Other (please specify)

*3. Please choose the answer that best describes how long you have been researching digital forensics or practicing as a forensic examiner.

*4. From the list below, please check all the devices that you have experience examining or researching.

☐ laptops/notebooks ☐ iPods/MP3s

☐ computers ☐ gaming systems

☐ smartphones/cellphones

Other (please specify)

*5. Please rank the following from 1 to 11 with respect to order as it pertains to a smartphone investigation. If you find that one activity should take place throughout the investigation please denote that by choosing "TO". If you find that one activity does not address a smartphone investigation, please denote that by choosing "NA".

| | Order from 1 - 11 |
|---|---|
| Presenting the findings | |
| Retaining information about what was successful/unsuccessful about the investigation | |
| Interpreting the findings | |
| Verifying the preliminary findings | |
| Transporting the device | |

Definitions: Phases
Analysis – Deals with actively examining each piece of evidence after it has been lawfully collected.
Collection – Deals with legally seizing the devices involved and imaging the data from the devices.
Examination – Deals with recognizing and locating the potential evidence from the collected data, using a systematic approach.
Identification – Deals with profile detection, system analysis, and audit monitoring.
Presentation – Deals with preparing reports based on the conclusions of each investigation.
Preservation – Ensures the evidence is being handled properly in order to guarantee that little to no contamination has been introduced.

**7. Of the 6 phases listed above, are there one or more phases that do not fit the logical progression of a smartphone examination? If so please choose all that apply.**

- ☐ Identification
- ☐ Preservation
- ☐ Collection
- ☐ Examination
- ☐ Analysis
- ☐ Presentation

**8. Of the phases listed above, are there one or more phases not listed that should be added in order to better fit the logical progression of a smartphone examination?**

Thank you for taking the time to participate in this survey!

Done

APPENDIX B

POST SURVEY

**Post Survey**

| | |
|---|---|
| Q1 | What is your level of experience in performing forensic tasks on smartphones?<br>a. No experience (0-1 years)<br>b. Little experience (1 – 2 years)<br>c. Some experience (2 – 3 years)<br>d. More experience (3 – 4 years)<br>e. Very experienced (5+ years) |
| Q2 | How difficult is PIFPM to understand?<br>a. Not difficult<br>b. Slightly difficult<br>c. Somewhat difficult<br>d. Very difficult<br>e. Extremely difficult |
| Q3 | Rate how feasible PIFPM would be in its application to the forensic processing of smartphones.<br>a. Not at all feasible<br>b. Slightly feasible<br>c. Somewhat feasible<br>d. Very feasible<br>e. Extremely feasible |
| Q4 | How likely would you be to incorporate PIFPM into your forensic examination process?<br>a. Not likely<br>b. Slightly likely<br>c. Somewhat likely<br>d. Very likely<br>e. Extremely likely |
| Q5 | Of the phases listed below, which one(s) do not fit the logical progression of a forensic examination?<br>a. Transportation<br>b. Classification<br>c. Analysis<br>d. Interpretation<br>e. Retention<br>f. All seem logical |
| Q6 | How useful is PIFPM in a smartphone examination?<br>a. Not useful at all<br>b. Slightly useful<br>c. Somewhat useful<br>d. Very useful<br>e. Extremely useful |
| Q7 | Does PIFPM offer anything to an examination that other models do not? |

| | |
|---|---|
| Q8 | Is it logical for smartphones to use the same forensic process model as computers?<br>a. Not logical<br>b. Slightly logical<br>c. Somewhat logical<br>d. Very logical<br>e. Extremely logical |
| Q9 | How often do you manipulate the process you frequently use to examine smartphones, whether intentionally or unintentionally?<br>a. Not often<br>b. Slightly often<br>c. Somewhat often<br>d. Very often<br>e. Extremely often |
| Q10 | Have you ever manually examined a device using no external equipment such as XRY, FTK, etc?<br>a. Yes<br>b. No |
| Q11 | If you answered yes to Q10, what was your reason for examining the mobile device manually? If you answered no, please mark N/A.<br>a. No forensic equipment available<br>b. No tool available for that specific OS<br>c. Research purposes<br>d. Other_____<br>e. N/A |
| Q12 | What strengths does PIFPM offer to a forensic examiner in a smartphone investigation? |
| Q13 | What weaknesses does PIFPM offer to a forensic examiner in a smartphone investigation? |
| Q14 | Do you believe that incorporating PIFPM into phone examinations will change the confidence level of the investigator?<br>a. Yes, it will lower the confidence level greatly<br>b. Yes, it will lower the confidence level slightly<br>c. No, the confidence level will not change<br>d. Yes, it will elevate the confidence level slightly<br>e. Yes, it will elevate the confidence level greatly |

APPENDIX C

QUALITATIVE STUDY PARTICIPANT FORM

**Qualitative Study Participant Form**

Prospective Smartphone Forensic Examiner Participant

I, Frances Chevonne Dancer, am conducting a study that calls for forensic examiner volunteers with experience in processing smartphones under the direction of my major professor, Dr. Dave A. Dampier, Professor of Computer Science in the Bagley College of Engineering at Mississippi State University.

I would like your permission to observe you in your setting while examining a smartphone as you normally would or interviewing you in order to gather information about your current process. I will then provide you with another model so that you may compare and contrast it to your regular forensic process. Afterwards, I would interview you in case there are any questions I have after the observation. Lastly, you will be provided a survey that will assist me in assessing some of the qualitative information needed for the study.

In conducting this study, we hope to gain a better understanding of how forensic examiners process smartphones in an effort to move closer towards a golden standard for all smartphones regardless of make, model, and functionality.

_____ _____

Participant signature Date

APPENDIX D

INFORMED CONSENT FORM

**Mississippi State University**
**Informed Consent Form for Participation in Research**

**Title of Research Study:** A Platform Independent Forensic Process Model for Smartphones

**Study Site:** Mississippi State University's Forensic Training Center

**Researchers:** Frances Chevonne Dancer and David A. Dampier

**Purpose**

The purpose of this project is to understand whether a platform independent forensic process model will aid in searching, identifying, and analyzing digital evidence on various models of smartphones during a computer forensic investigation in a more effective manner than methods currently used.

**Procedures**

The subjects will examine and analyze a smartphone using either an ad hoc approach or/and one of the presented forensic process models. The control group will be using the ad hoc or the more commonly used approach during the experiment. The experimental group will use the proposed forensic model to locate and identify digital evidence during the experiment. To initiate the study, the subjects will be given a 30-45 minute lecture on the functionality of a basic smartphone. After questions are answered, the subjects will be given a brief 30 – 45 minute presentation on the key activities that should take place in a digital forensic investigation by definition. Lastly, one hour will be allotted to allow the participants to experiment with different model smartphones so that they will be familiar with the devices. At the beginning of sessions 2 – 4, a lecture on the specific modeling approach to be used in that session will be presented. Next, the subjects will be presented with a fictitious case and will use their respective approaches to examine, analyze, and locate date of evidentiary value. Lastly, the subjects will be given a questionnaire to assess their experience with using each approach. The experiment will take 2 hours to complete.

***Risks or Discomforts***

Procedures in the experiment are similar to and pose no more risk than those of the seminar or a real digital forensic examination (as stated in the IRB application).

***Benefits***

The potential benefits of this project are as follows: the examiner will be able to locate more digital forensic evidence with less effort and time, the impact that the technological skill/experience of an examiner has on locating potential evidentiary information will be realized as well as the precision of accuracy to which an examiner locates actual evidence. This study will provide a new method for examining and analyzing smartphones, increase the quality of digital forensics investigations, and potentially impact the architecture of future small scale digital devices.

***Incentive to participate***

An incentive of five additional training hours will be given to those subjects who complete the experiment.

***Confidentiality***

***The data will be collected via computer software, forms, and questionnaires. Once all of the data are collected, each subject's name will be replaced with a code to facilitate tracing the relationships between sets of data. Once the names are removed, data will not be distinguishable as to who provided it.***

*Questions*

If you have any questions about this research project, please feel free to contact Chevonne Dancer at 601-750-3638. You may also contact Mrs. Dancer's faculty advisor, Dr. David A. Dampier, at 662-325-8923.

For questions regarding your rights as a research participant, or to express concerns or complaints, please feel free to contact the MSU Regulatory Compliance Office by phone at 662-325-3994, by e-mail at irb@research.msstate.edu, or on the web at http://orc.msstate.edu/*participant/*.

***Voluntary Participation***

Please understand that your **participation is voluntary. You have the right to refuse to answer any specific question asked of you.** Your **refusal to participate will**

**involve no penalty or loss** of benefits to which you are otherwise entitled. You **may**

Please take all the time you need to read through this document and decide whether you would like to participate in this research study.

If you agree to participate in this research study, please sign below. You will be given a copy of this form for your records.

| | |
|---|---|
| _____ | _____ |
| Participant Signature | Date |
| _____ | _____ |
| Investigator Signature | Date |

**discontinue your participation** at any time without penalty or loss of benefits.