CERIAS Tech Report 2005-27

DIGITAL MUSIC DEVICE FORENSICS

by Christopher V. Marsico

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

DIGITAL MUSIC DEVICE FORENSICS

A Thesis

Submitted to the Faculty

of

Purdue University

by

Christopher V. Marsico

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

May 2005

TABLE OF CONTENTS

ABSTRACT

Marsico, Christopher V. M.S., Purdue University, May, 2005. Digital Music Device Forensics. Major Professors: Melissa J. Dark, Marcus K. Rogers.

The digital music device has become a common household item. The newest models have become more PDA like than ever before. With this new functionality the digital music device has recently found its way into the criminal world. With the continued growth of the digital music device market, it is possible that their use in criminal activity will only continue to increase. This research analyzed some of the frameworks that offer guidelines of best practice for cyber forensics for their use with the digital music device. Literature review found little or no documentation or discussion on the forensic analysis of these devices. The frameworks were evaluated using a hypothetical scenario involving a digital music device. The guidelines of Reith, Carr and Gunsch (2002) and Carrier and Spafford (2003) were most effective. In the future, a scientific test involving a physical scene and participants separately following each set guidelines would be useful in gaining a better understanding of how each works with the digital music device.

INTRODUCTION

The computer world is changing at a rapid pace. Every day new products and technologies come to market. One of the biggest growing industries in the cyber world is digital music. The digital music revolution, as it has been coined, came about with the development of audio compression technologies, such as the popular MP3, and peer-to-peer file sharing for digital music. These two technological developments gave the average computer user the ability to exchange and trade music digitally across the Internet. This digital music exchange spurred the development of devices similar to portable compact disk players that allow a person to take digital music with them and listen to it.

More recently the popularity of online music stores where digital music can be purchased has made these digital music devices or MP3 players increasing popular. The IDC research firm expects that by 2008 there will be over 50 million of these devices sold to consumers (Guloyan, 2004). Similar to the industry from which they were born, these devices have experienced a rapid evolution. The digital music device of today no longer simply holds several songs for the user's enjoyment. Large storage capacities and personal digital assistant (PDA) functionalities have made the digital music device a technology that should be of interest to the cyber forensic community (Reith, Carr, & Gunsch, 2002).

Forensics is the use of science and technology to investigate fact in the court of law (Saferstein, 2004). Forensics has been around for many years, originally progressing in the hard sciences. Cyber forensics according to Giordano and Maciag (2002), is “The exploration and application of scientifically proven methods to gather, process, interpret, and utilize digital evidence...” (p. 3). With the coming of the digital age, the computer became a common household item and therefore made a natural progression into the criminal world (Rogers & Seigfried, 2004). The digital music revolution has also seen the digital music device become a common household item. It is only a short time until they too make a natural progression into the criminal world. This progression has already begun. One example is the use of, an Apple iPod by a gang of thieves in England to store information related to their crimes (BBC News, 2004). Can the law enforcement community sit idly by while these devices continue to make this progression into the criminal world? An essential step in the extension of cyber forensics into the world of digital music devices is to explore current cyber forensic guidelines for use with digital music devices.

This research focused on frameworks by Carrier and Spafford (2003), the Department of Justice (2001), Noblett, Pollitt and Presley (2000), Beebe and Clark (2004), and Reith, Carr and Gunsch (2002). These frameworks are more than just guidelines; they also contain the beginnings of what may become theories for the field. Cyber forensics is still in an immature state and there are not yet true theories on which the discipline can be based. The frameworks analyzed in this thesis offer some guidelines for practicing cyber forensics.

Statement of the Problem

The problem of this study was to determine if current guidelines for cyber forensic data collection and analysis were able to handle the physical and digital crime scene involving digital music devices. This type of determination has become necessary with the recent advances in digital music technology. The latest digital music devices include large storage capacities as a result of hard drive technology. Some of the hard drive-based devices have capacities upwards of 60GB. With this much storage space for music, developers have branched out and included features like a calendar and contact book ("Apple iPod - Music and more", 2004). These devices are simply a portable hard drive, and have the ability to store other types of files besides music; such as documents or pictures. Thomas (2004) reports that an employee could take sensitive information by using the capabilities of a digital music device. Suspects could potentially store critical evidence on these types of devices. It must be determined if current frameworks of cyber forensic science are applicable and to what extent current guidelines can be applied to digital music device forensics.

According to recent surveys; data collection, education and well-documented techniques are important areas for further research (Rogers & Seigfried, 2004; Stambaugh, Beaupre, Icove, Baker, Cassaday, & Williams, 2001). Rogers and Seigfried (2004) report that tools, technologies and data acquisition are areas needing further development. An earlier study by the National Institute of Justice also contained similar findings (Stambaugh et al., 2001). Forensic practitioners questioned in the survey said that data acquisition

is an area in need of further research and development (Stambaugh et al., 2001). Palmer (2002) states that research must stand behind the techniques and methods employed in cyber forensics. This research focused specifically on guidelines for data acquisition and analysis in a physical and digital crime scene as they pertain to digital music device forensics.

It is important for evidence to be collected in a forensic manner when it is being prepared for possible submission to court proceedings (Kruse & Heiser, 2002). The case of *Daubert* v*. Merrell* (1993) outlines the rules necessary for evidence admissibility. Carrier (2002) discusses the fact that well documented and commonly accepted tools and techniques are necessary for admissibility under the Daubert criteria. These requirements have not been fully met for the collection of evidence from computers, so it must also be true that these requirements are not currently met for the collection of evidence from digital music devices (Marsico, 2004). The applicability of current guidelines to digital music devices is the first step in meeting these documentation and acceptability requirements.

Significance of the Problem

This project is important for the common body of knowledge in the discipline of cyber forensic science. Little research has been to done to determine if these guidelines were sufficient for digital music device forensics and no specific documentation is available. This research helped fill a void in the knowledge of the community on forensic thinking for these and similar devices. It

may also directly benefit law enforcement and corporate incident response teams in their investigation of potential crimes where a digital music or similar device is present.

This analysis exposed any shortcomings of the guidelines when used for forensic analysis of a digital music device. Providing information as to where a current set of guidelines are lacking allowed them to be changed for these and possibly other new devices. If this analysis was not done, the current holes would have continued to grow, the proliferation of the digital music device would continue and forensic practitioners would not have a solid set of guidelines to use for forensic analysis of digital music devices. By correcting the problem now, future practitioners can be sure to consider the digital music device when following one of the guidelines analyzed in this study. When individuals are developing new guidelines, refining old ones or working on a true theory for cyber forensics, digital music devices and other unique devices may now be viewed with greater importance.

In recent years there has been a proliferation of digital music devices. Their increasing capacities and capabilities require that the common body of knowledge in the community address the forensic collection of data from them. The Apple iPod itself, the most popular digital music device, has sold over 4 million units (Thomas, 2004). Additionally, in 2004 all Duke University freshmen were given an Apple iPod as part of a research project to study the use of the device to enhance learning ("Duke iPod", 2004). The students were encouraged to use the device to store their files, academic calendars, contacts, and to input

their homework assignments as tasks (Menzies, 2004). Some devices with proper configuration can run Linux and even contain all the necessary information for a computer system to run effectively (Knaster, 2004). This would allow an individual to carry their entire computer around with them and boot it via their digital music device attached to most any computer.

As stated earlier, many digital music devices have additional functionality besides playing music. Devices are taking on more PDA like characteristics, such as the contact lists and calendar functions. Recently there has been work done by National Institute of Standards and Technology (NIST) to develop guidelines for PDA forensics (Jansen & Ayers, 2004). The knowledge discovered as a result of this analysis may be used to develop more comprehensive forensic frameworks that account for the digital music device.

The digital music device is an interesting challenge for the forensic examiner, especially in terms of collection and analysis, because of their small size and unique technologies. It is necessary to search a physical crime scene and a suspect's personal effects for digital music devices. Many new digital devices have become common in the physical crime scene and the digital music device is one such device that will now be frequently found. With the large variety of these devices available to consumers and an abundance of proprietary operating systems and unique file structures, these new pieces of evidence may cause difficulty for the forensic investigator.

Statement of the Purpose

The purpose of this study was to determine if current guidelines for cyber forensics could be used for digital music device forensics. The setting of the study was a developed hypothetical scenario that included the physical and digital crime scene, as described by Carrier and Spafford (2003). This setting allowed the context of the study to be that of a law enforcement and incident response perspective, especially in the area of investigation and evidence collection for admission into the criminal federal United States court of law by following the guidelines of the Federal Rules of Evidence (FRE) and precedents set in the cases of *Frye* v. *U.S, Daubert* v. *Merrell*, *Kumho Tire Co. Ltd.* v. *Carmichael.*

The question answered in this study was whether or not current cyber forensic guidelines could be used for digital music device forensics. There has been much work done on collection and processing of data in other communities of forensics; such as finger print analysis and DNA. The science of DNA evidence collection went through its maturation process several years ago with tools and techniques being defined by its scientific community (Connors, Lundregan, Miller, & McEwen, 1996). Similar progress needs to be made in the cyber forensic community (Palmer, 2002). Many different organizations have worked to develop guidelines for the forensic analysis of computer evidence. The abundance of similar but different guidelines has almost become a burden to the community by resulting in no one “gold standard” (Rogers & Seigfried, 2004). Specialized areas of digital evidence have also been explored such as the NIST

document on PDA evidence collection (Jansen & Ayers, 2004). Research like this provides specific information for a unique area of digital evidence collection.

Definitions

Digital Music Device- A hardware device containing memory designed to store and play digital music.

Forensics- The use of science and technology to investigate and establish facts in criminal or civil courts of law.

Gigabyte (GB) – A unit of computer memory or data storage capacity equal to one billion bytes.

Hash- the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string (Whatis.com, 2005).

iPod- A hard drive-based digital music device from Apple Computer.

NIST- National Institute of Standards and Technology.

Personal Digital Assistant (PDA)- A handheld device used as a personal organizer usually including clock, date book, address book, task list, memo pad and a simple calculator.

Assumptions

The freely available and open frameworks analyzed in this research have greater distribution and can be easily reviewed by members of the community

from which they came. These will therefore be more accepted than a closed framework that has not been through such a review process.

Delimitations

This research is delimitated in several ways based on external and internal factors. The external forces of money and time were the cause of the delimitations of this study. The following delimitations have been recognized;

- Only guidelines publicly available in October of 2004 were considered in this research.
- Only digital forensic guidelines that are openly available in journals or free publications were used in this research.
- A best practice guide was not developed as a product of this research. Theoretical discussions that could be used in the development of such a guide are presented.
- This study was a one-time look at the current frameworks as they apply to the digital music devices available in 2004. There will be no follow up study but future recommendations are given.
- Lack of methodology for analysis of cyber forensic frameworks required the researcher to develop a descriptive style critical analysis evaluation methodology.

Limitations

The following issues related to validity were identified. First, a physical scene was not created. The scene that was created was a hypothetical one that was intended to be generic enough to allow generalization of findings from the thesis. However, this was not tested and there exists a potential limitation to external validity. Second, the analysis was limited to the thinking of the author. No external participants were used in the analysis. The author assessed each framework using pre-established criteria and the hypothetical situation and then progressed to the next scenario. The continued learning of the author during the investigation is a potential maturation limitation. Lastly, there is the possibility for measurement error. The author developed the criteria for evaluating the guidelines based on a thorough literature review. However, whether or not these are the appropriate criteria was not tested within the larger cyber forensics community.

REVIEW OF LITERATURE

The science of digital forensics is new and growing. There is much to be learned in this field. This makes for a research area that is much too large to study in a single research project. There are many sub-areas under the main branch of digital forensics. Digital forensics according to Palmer (2001) is:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (p. 16).

Practitioners often find that there are several different areas under the main area of digital forensic science:

- Computer Forensics
- Network Forensics
- Video Forensics

Computer forensics, according to Kruse & Heiser (2002), “involves the preservation, identification, extraction, documentation and interpretation of computer data” (p. 2). Network forensics, on the other hand, deals with the

forensic analysis of active network devices (Palmer, 2001). Reith et al. (2002) state that, “computer forensics tends to focus on specific methods for extracting evidence from a particular platform, digital forensics must be modeled such that it can encompass all types of digital devices” (p. 3).

Some practitioners today are starting to include both computer and network forensics into a single grouping called cyber forensics (Palmer, 2001). This is based on the use of the word cyber as it refers to the modern world of computers, Internet, and computer like devices. So in turn, cyber forensics deals with computers and computer like devices. This area of cyber forensics is where this author believes there is a “gaping hole” for new devices such as the digital music device. No research or documentation on forensic analysis of digital music devices was found. The community’s frameworks may have been created without the digital music device in mind and therefore it is believed they may be inadequate to account for such a device.

Background research into basic forensic models from the physical world was necessary for this research. Physical world forensic examinations usually focus on the hard sciences. These include sciences such as chemistry, biology and physics (Saferstein, 2004). Saferstein (2004) reports that physical forensic analysis is usually concerned with the identification of forensic evidence for the purposes of comparison. This identification can be used to link a suspect to the crime scene and reconstruct the events surrounding a crime. The main areas of a physical crime scene forensic theory are recognition, individualization and admissibility (Saferstein, 2004). These are necessary components for a physical

world forensic theory. If cyber forensic frameworks are to be judged on their ability to handle the addition of a digital music device to the physical crime scene, then the frameworks of cyber forensics must also be able to meet the requirements of physical investigations.

The digital music device in the physical world is similar to a corpse. The device is a piece of evidence itself, yet contains latent evidence within it in a digital crime scene. The latent evidence must be carved out of the digital scene using special techniques and tools. The dualistic nature of the device requires that a framework of cyber forensics be able to address the requirements in both the physical and digital sense (Carrier & Spafford, 2003).

The digital crime scene is a conceptual idea that the space on the hard drive or storage media is similar to that of physical space in a real crime scene. In the digital crime scene, evidence could be located in many different places similar to that of a physical scene. The digital crime scene must be sectioned off and protected similar to the physical crime scene; this is to prevent contamination. Evidence collection and location must be clearly documented. This is a necessary component of evidence collection. Palmer (2002) also refers to the concept but uses different terminology. Palmer thinks of it as a virtual crime scene, which is analogous to Carrier & Spafford's (2003) digital crime scene. For this research, the digital crime scene concept was used and the analysis of the guidelines occurred based on the dualistic nature of the digital music device as a physical corpse containing a digital crime scene.

A literature search revealed several articles and books discussing guidelines for cyber forensics. Frameworks of cyber forensics, as opposed to the physical crime scene, involve a process of tracing a user's activity and recovery of latent evidence (Carrier & Spafford, 2003). Frameworks that are peer reviewed and published in journals or government reports were looked at in this research. Frameworks by Carrier and Spafford (2003), the Department of Justice (2001), Noblett, Pollitt and Presley (2000), Beebe and Clark (2004), and Reith, Carr and Gunsch (2002) were considered. These frameworks contain guidelines that make up some of the foundation of cyber forensic practice.

The framework of Carrier and Spafford (2003) outlines the steps they believe are necessary for the digital investigation process. This process takes place both in the physical and digital. The conceptual idea of the digital crime scene is defined as "the digital environment created by the hardware and software" (Carrier & Spafford, 2003, p. 2). Their model is created with the basic forensic science in mind and therefore maybe complete in the three established areas of basic forensic science. Meaning that the criteria of recognition, individualization, and admissibility reported by Saferstein (2004) may be met by this framework . The model they created takes the approach of the computer itself as a crime scene. Their high level model offers five groups of phases with sub-phases for some.

1. Readiness Phases
    a. Operations Readiness Phase
    b. Infrastructure Readiness Phase

2. Deployment Phases
    a. Detection and Notification Phase
    b. Confirmation and Authorization Phase
3. Physical Crime Scene Investigation Phases
    a. Preservation Phase
    b. Survey Phase
    c. Documentation Phase
    d. Search and Collection Phase
    e. Reconstruction Phase
    f. Presentation Phase
4. Digital Crime Scene Investigation Phases
    a. Preservation Phase
    b. Survey Phase
    c. Documentation Phase
    d. Search and Collection Phase
    e. Reconstruction Phase
    f. Presentation Phase
5. Review Phase

All of the phases are important for digital music device forensics; however, the two most important phases are the physical crime scene and the digital crime scene. Some of the authors' assumptions, such as all digital world environments can be easy replicated, fall short with its unique application to some digital devices.

Beebe and Clark's (2004) objective-based framework attempts to add more granularity to the digital investigation process. Their model is a hierarchical, objectives-based framework that hopes to lead practitioners to the proper course of action though objectives. The model takes high level frameworks created by others and adds lower level objectives. They report that many of the other frameworks outline several processes in the digital investigation. These phases include preparation, incident response, data collection, data analysis, presentation and incident closure. The second tier phases they propose are step-by-step processes of what information should be colleted and analyzed from a device.

This research is a step in the right direction for the computer forensic community and would be applicable to specialized devices such as the digital music device. Beebe and Clark (2004) provide a very limited example in their paper, using the model for the computer and admit that additional work is necessary for their model to be applicable to other digital devices. This objective-based framework would be useful in digital music device forensics if proper objectives were outlined and accepted. These objectives should remain open enough to offer guidance to the practitioner but allow them the freedom to investigate what they believe is the necessary evidence. In this paper however, the example they provide becomes very specific and fails to remain open to allow freedom.

Recovering and Examining Computer Forensic Evidence by Noblett, Pollitt, and Presley (2000) is another example of a high level framework of cyber

forensics. This work outlines many of the steps necessary for the community in the coming years. It likens the cyber forensic community to that of DNA and the maturation process that it had to go through to become a recognized and accepted forensic practice. Noblett, Pollitt, and Presley's (2000) paper reports that computer forensics extracts and reports information. This is a key concept in cyber forensics and different than DNA or other forensics.

The authors report that a problem with the computer forensic science is that it was and still is almost completely market driven and they call for the establishment of policies, protocols and procedures. Furthermore, the authors go on to say that one cannot expect computer forensics to fully meet the requirements of repeatability because each forensic examination is unique. The authors attribute this fact to the unique nature of digital evidence. They report that the computer forensics is unique because not only does one have the physical (i.e. chips, boards, hard drives, etc.) but there is also a "metaphysical electronic form" (Noblett et al., 2000, p. 6). This concept is the same as the digital crime scene in that there is digital or as the author's of this framework call it "metaphysical" evidence inside the physical device. For collection and analysis, the authors point to several key concepts in computer forensics. They state the need for unaltered evidence and verification that it is unchanged. This is done by the creation of a copy or image. This may be difficult for digital music device forensics. Creating an exact copy of the device or image is something that may not be easily accomplished. For the analysis, the authors suggest that using a well-documented technique that explains why something is done is sufficient for

admissibility. This works well in cyber forensics and for digital music devices because the openness of their recommendation allows the practitioner to work in whatever way is necessary to extract the latent evidence.

In *An Examination of Digital Forensic Models* by Reith, Carr and Gunsch (2002) the authors make the point that many digital forensic models are too specific and cannot be applied to other devices besides computers. In the paper, the authors compare and contrast four common models and then present their own model they hope will be more applicable to all digital devices, not just computers. The model they present is abstract, high level and the type of model necessary for digital music device forensics. The authors report that digital forensics has become an important topic because "modern day life includes a variety of digital devices that can be exploited for criminal activity" (p. 2). Reith et al. (2002) is critical of computer forensic models of Farmer and Venema, Mandia and Prosise, the U.S. Department of Justice and Digital Forensics Research Workshop (DFRW). The authors report that the first two models are much too technology specific and not applicable across a wide range of digital devices. The DFRW model is more abstract, but fails to provide a distinction between forensics of computers and forensics of other digital devices. The guidelines proposed by the authors are highly abstract and is based on the DFRW model. The nine steps they propose are: "identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and return evidence" (p. 6-7). The guidelines' openness ensures that they will apply to any digital device, which is necessary for digital music device forensics. The author of

this paper agrees their developed guidelines provide “a consistent methodology for dealing with past, present, or future digital devices” (Reith et al., 2002, p. 7). Sub-steps can be created to specifically apply to different devices. The concept of sub-sets is important and the authors even go as far as to say that devices such as MP3 players could contain evidence useful to judicial members. This statement fits directly into line with the research of this thesis. Their framework “identifies commonalities of digital technologies” (Reith et al., 2002, p. 9). This concept is important for the ability of the guidelines of the framework to handle a digital music device and is applicable to digital music device forensics.

Electronic Crime Scene Investigation by the National Institute of Justice (2001) is a guide for first responders to an incident involving possible digital evidence. The paper is an attempt to provide a comprehensive guide for the first responder and others at the crime scene. It provides information on the types of devices and potential evidence, investigative tools, securing a scene, documenting, collection, and packing, transport and storage.

The paper’s first big flaw, but one the authors admit, is that it is not comprehensive. With the changing technology market there would need to be constant updates to respond to the ever-increasing number of devices. There is no mention at all in the types of devices section of this paper of the digital music device as something that a first responder should be interested in collecting. This most likely is a result of the paper’s publication date of 2001. Though digital music devices were available, they were certainly not as ubiquitous as they are now. This being the case, the guide fails to even recognize the digital music

device as an item of interest. The guide makes good discussion on the fact that digital evidence is latent, similar to DNA and fingerprints. At a high level it reports that special precautions need to be made regarding collection and preservation. In the requirements for basic forensics the guide discusses recognition of evidence in both the physical and digital realms. This recognition is one of the cornerstones of this evaluation. The guide offers information on the scene but again limits most of its discussion to computers and their collection. It does offer high-level guidance to immediately secure and document any device containing perishable data. Collection is again limited to computers with a coverall for any other type of device. The packing, transport and storage section of the paper does cover the requirements and procedures for digital devices and they are high-level and abstract enough to be applied to the digital music device. The chain of custody concept and the requirement of documentation are also emphasized. This guide, though biased towards the computer in many aspects, does point out there that are a large number of other devices of which a first responder to a crime scene should be aware. An updated version of the paper should include the digital music device.

Conceptual Framework

A framework of forensic science should be able to recognize forensic evidence, individualize components, and provide for the admissibility of evidence to the court room (Nickell & Fischer, 1999). These components are all necessary for a forensic theory in the physical world. The ability to recognize evidence in the

physical world is the identification of all potential aspects of a crime scene that may contain evidence (Nickell & Fischer, 1999). This is also true in the digital world in the ability to find evidence on a device or system. It is important to be able to recognize evidence in the digital crime scene. Evidence can be any information on the electronic device. Sometimes evidence may require special processing in order to be recovered. This latent evidence can often be identified through the use of a forensic tool. These aspects are necessary for proper identification and it will be important for the forensic guidelines to recognize a digital music device in the physical crime scene. These guidelines must also lead the analysts to search and discover obvious and latent evidence in the digital crime scene.

To individualize the components is to identify and link the evidence collected at the physical scene to the individuals or suspects. In the digital crime scene, evidence collected from the device must also be linked to the suspects (Carrier & Spafford, 2003). This link can be established by showing personal possession of the physical item or by connecting a suspect with the use of the device. In the digital world this is difficult. Digital evidence must be shown that it was created, used or accessed by the suspect. Timelines based on access and creation time of files and device usernames are most effective in this endeavor. The guidelines should lead an analyst to search out these identifiers and offer discussion on their importance.

Finally, all the evidence collected and analyzed both in the physical and digital worlds must be done in a manner that is consistent with the requirements

for admissibility to the courtroom. These admissibility requirements are outlined by such documents as the Federal Rules of Evidence (FRE) and by court cases such as *Frye* v. *US* and *Daubert* v. *Merrell* (Carrier, 2002). Additionally, the case of *Kumho Tire* v. *Carmichael* (1999) extended the application of the criteria outlined from the Daubert case to technological and engineering evidence.

Considerations for chain of custody, preservation of integrity and discovery should be discussed in the framework. Proper documentation and accountability for all time periods after collection are necessary to maintain a proper chain of custody. A key concept in the preservation of integrity is that one should work with a copy of the original data (Palmer, 2001). It is necessary to prove that data was not changed during analysis and only the data that was present at the time of collection remains on the original. This is the quality of authenticity and evidence must be shown to be authentic in order to be accepted by the courts. A framework of cyber forensics must discuss these requirements and offer guidelines for this preservation when applied to any device, including a digital music device.

The three main components of the core of forensics, recognition, individualization, and admissibility, are necessary in both the physical and digital crime scene. These components were used as the basis for the evaluation of the guidelines. The guidelines of each framework should all be able to fulfill the requirements. This may not prove to be true due to the fact that the guidelines evaluated in this research were not created with the digital music device in mind and therefore may not account for the device in the physical or digital crime

scene. The special considerations these devices require are similar to that of a PDA. The researcher believed that the guidelines, though not designed with the digital music device in mind, could be used with the devices. The more granular the guidelines the more difficulty it will have accounting for the devices. Higher-level guidelines would allow more flexibility for the practitioner.

Some considerations needed to be made when looking at guidelines and their applicability to the digital music device. The steps should account for a digital music device. If not, then what steps were missing or are sub-steps merely required to account for these devices similar to the hierarchical framework developed by Beebe and Clark (2004) and the sub-steps proposed by Reith et al. (2002). The guidelines, when applied to digital music device forensics, should meet the three core components of basic forensic theory. The digital crime scene, as described by Carrier and Spafford (2003), is found on the digital music device. The guidelines should be applicable to the digital crime scene of the digital music device as they are to the digital crime scene of the computer. The steps of the guidelines may be affected by the digital music device, so it was necessary to determine what steps were affected and if considerations needed to be made for them.

Based on the above assertions the following questions were addressed in this study:

- Are the guidelines steps adequate to account for digital music devices?
    - Do sub steps need to be created?

    - Does the framework respond in a way that is consistent with recognition, individualization, and admissibility of basic forensic theory?
- Can the frameworks' components and principles transfer from the computer digital crime scene to the digital crime scene of a music device?
- What steps of the guidelines directly relate to digital music devices?

Summary

Needs analysis pointed to data acquisition and theory as key areas in need of further research. Current market trends and research reports anticipate the continued proliferation of the digital music device. The necessity for collection of evidence from these devices led to a review of the frameworks of cyber forensics. The dualistic nature of the digital evidence required guidelines of physical forensics to be understood. The components of physical forensic theory were used to develop the criteria on which cyber forensic guidelines were evaluated.

METHODOLOGY

This evaluation focused on the five frameworks of cyber forensics and their use in collection and analysis of the digital music device. The guidelines were evaluated for their use in digital music device forensics. The following methodology was designed to answer the research questions posed in the previous section. The guidelines were critically analyzed for their foundations in the three-core aspects of the science of forensics; recognition, individualization and admissibility.

The evaluation in this study was of a qualitative nature. It was exploratory and descriptive, and provided a critical analysis of the guidelines. There was neither numerical data collection nor statistical analysis. The analysis focused on the criteria of, recognition, individualization, admissibility, transference, and affected, as defined by the researcher. The operational definitions on the following page were used to define the requirements of each criterion. The guidelines were adjudicated on its fulfillment of these criteria.

A hypothetical scenario was developed involving a digital music device and the guidelines of each framework were judged on their response to the scenario. This response was determined through a hypothetical investigation of the crime scene in the scenario. This research was cross-sectional and only

analyzed guidelines of the selected frameworks. This research can also be considered developmental in that the research provides guidance for future researchers to rework guidelines that fail for digital music devices. This work could also be used in the development of a best practice guide for digital music device forensics.

Scenario

The hypothetical scenario used in this research is that of a fictional crime scene in which there is a physical computer, paper work, CD-ROMs, floppy disks and a digital music device. The location is a home office style room with a desk, chair and shelves. The digital music device is unconnected to any computer and in an off state lying on the desk next to the computer. In the scenario, the scene is being investigated by several hypothetical investigators who are responding to the scene per the company's request because the suspect, who owns the room and its contents, is accused of stealing sensitive corporate data that includes digital photos and documents. The specific location of the data is unknown to the investigators, but it is reasonable to assume that it is stored on digital media in the office, so the investigators are able to gain permission to search the room. For the purposes of this analysis, the digital crime scene where the data is stored is located on the digital music device and it was necessary for the investigators to collect the device to gain access to the digital crime scene within it. Though this scenario is fictional it is based on common scenarios from the author's experience and literature review.

Criteria

Five criteria were used as the variables for the testing. These criteria allowed the researcher to design the testing methodology to analyze the guidelines for their fulfillment of the criteria and use in digital music device forensics. The following list is the operational definitions for the criteria from the research questions in the review of literature section. These definitions were created by the researcher for use in this analysis.

Operational Definitions

Recognition - The ability of forensic guidelines to point the investigator to what should be collected and analyzed.

Individualization – The linking of evidence to a suspect or timeframe.

Admissibility- The ability for the evidence that is colleted to be used in a criminal court of law based on the requirements set forth in FRE 702, and the case of *Daubert* v. *Merrell*. This ideal is judged on almost a case-by-case basis.

Transference- The guidelines can be used for its original intended target, in most cases the personal computer, and the digital music device.

Affected- The steps of the guidelines have unique considerations when they are applied for use with digital music device forensics.

These criteria were explored in the identified guidelines. After this analysis, answers to the research questions were found. These criteria are measured through the use of the developed instrument.

Instrument

The methodology used in the analysis is considered the instrument of testing. This methodology was designed to investigate the guidelines and answer the research questions. It was created by the author with the guidance of members of the thesis committee and is based on the standard methodology used by NIST to test tools for computer forensics.

The NIST computer forensic tool-testing (CFTT) project, tests computer forensics tools and reports on their effectiveness. The methodology they use is described in the document *General Test Methodology for Computer Forensic Tools* (National Institute of Standards and Technology, 2001). This tool testing methodology was used as a design model for the method conducted here. The NIST testing methodology is based on ISO 17025. NIST outlines several aspects that are necessary for testing. The following steps were identified:

- Establish categories of forensic requirements
- Identify requirements for specific categories
- Develop test assertions based on requirements
- Develop test code for assertions
- Identify relevant test cases
- Develop testing procedure and method
- Report results

The NIST (2001) methodology is “based on well-recognized methodologies for conformance and quality testing” (p. 1). Conformity as defined by NIST is the fulfillment by a product, process or service of specific

requirements. In this study, the conformity is the guidelines meeting the requirements of the criteria.

Validity was established for this methodology in several ways. The members of the thesis committee evaluated the method during and after its development to establish face validity. The use of the NIST method as a baseline for the methodology here establishes construct validity.

The frameworks were analyzed in a step-by-step manner. The general guidelines of the framework were extracted by the researcher (see appendix A). They were then individually applied to the developed scenario. This analysis occurred though the use of the hypothetical investigators. These investigators went through the scene as if they had been trained solely on the guidelines of one of the frameworks. The scenario was analyzed five times, once for each framework. The results of the hypothetical collection and analysis by the investigators determined if, by following the guidelines of the framework, it was possible to recognize the digital music device and individualize the device to the suspect. It is necessary that both of these requirements were achieved in a way that would allow for the evidence to be admissible. If these were all met, the guidelines were considered adequate.

The evidence in the scenario was located on the digital music device. The guidelines of the framework should have led to recognition of the pictures and the documents on the device and the individualization of the evidence to the suspect. Both should again be done in a manner that allows for admissibility. These

requirements show that the guidelines can be transferred from computer to the digital music device.

The possible outcomes of the analysis were failure, partial success or success for each guidelines analyzed. A framework may fail in all aspects of digital music device forensics by not meeting any of the basic requirements of forensics when the guidelines are applied to the scenario or by failing to recognize the digital music device at all. Partial success occurred when analysis showed the guidelines met the requirements of some, but failed in others. Finally, success occurred if the guidelines were able to meet all the basic requirements when applied to the scenario. The aspects of the scenario that met the requirements were recorded and the final outcome determined. Guidelines that failed or showed partial success required changes to fulfill the requirements. The aspects of the guidelines that are affected by the digital music device were documented, and recommendations as to how these should change including specific modifications, were given.

DATA ANALYSIS

Each of the identified frameworks in this thesis was broken down into their major categories of guidelines. The guidelines are what the frameworks lead a forensic practitioner to do during, after and sometimes before an investigation. The guidelines were extracted from the framework and the hypothetical analysis was performed to determine how well the guidelines met the requirements of the criteria (recognition, individualization, admissibility, transference, and affected) defined in this thesis (see appendix A). Every framework except *Recovering and Examining Computer Evidence* by Noblett, Pollitt and Presley (2000) had guidelines that could be easily extracted. Noblett, Pollitt and Presley's (2000) guidelines did not specifically outline steps; however they could be determined through critical reading of the text. The rest of the frameworks offered the following number of steps for their guidelines. Each of the guidelines steps are explained in more detail in appendix A.

- *Electronic Crime Scene Investigation* (DoJ, 2001)- Seven
- *An Examination of Digital Forensic Models* (Reith et al., 2002)- Nine
- *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process* (Beebe & Clark, 2004)- Six

- *Getting Physical with the Digital Investigation Process* (Carrier & Spafford, 2003)- Five

The developed scenario was investigated following the guidelines of each framework. Conclusions were made on what the investigators would do in the scenario when following the guidelines. The guidelines used with the scenario were also evaluated based on the requirements of the criteria. Each set of guidelines and its use in the scenario are explained below. For each of the guidelines the steps are identified in italics in the text. Additionally the analysis of the guidelines, when compared to the criteria, is also given.

Results

Electronic crime scene investigation.

Electronic Crime Scene Investigation (DoJ, 2001) has seven steps that were applied to the scenario. *Know devices* provided a list of known devices that might have been at the scene for the investigators of the scenario to reference. The listing in the guidelines is almost completely comprehensive for the time of publication. The device listing helped the investigators recognize the computer, floppy disks, and CDs. The papers were known physical evidence. The digital music device is also almost overlooked except one of the investigators understood that the guidelines point out that there a large number of unique

devices that one should be aware of and the investigator realized that the digital music device would fall into that category.

Have proper tools prepared the investigators to be ready to collect the known digital devices. The investigators were prepared with the proper tools and equipment to collect and analyze evidence in a forensically sound manner. They had write block capability for the computer hard drives but nothing to protect the digital music device when imaging.

The investigators once on the scene worked to s*ecure and evaluate the scene*. The investigators did not allow unauthorized personnel into the area. They left the computer in the state at which it was upon arrival and left all devices in their places. The connections to the computer were documented and then disconnected. The investigators next worked at d*ocumenting the scene.* They took notes on the locations of all the devices and their states upon arrival. The investigators photographed the entire scene.

Evidence *collection* was the important step where the electronic and other physical evidence was collected. The investigators collected the papers and other non electronic evidence. It was important that these physical pieces of evidence be secured. Latent evidence that may have been on the devices, such as fingerprints, were noted and the proper precautions taken not to harm this evidence. The computer was checked to determine if it was on with a shake of the mouse. Both the computer and monitor were off. The investigators unplugged the power cord from the back of the computer, checked the drive for floppy disks, taped the drives shut, recorded the make, model and serial numbers and

photographed and documented the computer connections. The removable media of CDs and floppy disks were colleted and the digital music device was taken as an “other electronic device.”

The main goal of the p*acking, transportation and storage* stage was not to change the evidence in any way. The investigators documented how each device was collected, which was important for the chain of custody. Forensic e*xamination* by crime category was the final step in the scenario investigation. The guidelines were referenced by case type to determine the proper course of action. In this case, the investigators searched for pictures and documents on the digital media and devices. The guidelines are not specific to technology, so there is not any type of guidance on the proper collection from the media, the computer or the digital music device.

These guidelines did well in meeting the requirements of the criteria. They had partial success when applied to the scenario developed in this thesis. It met the requirements of recognition, individualization and transference but fails in regards to admissibility. Additionally, the guidelines’ steps were affected in several ways when applied to the scenario with the digital music device. The guidelines provided the investigators the necessary guidance to recognize all the pertinent evidence on the scene. With regards to the digital music device, a careful understanding of the guidelines would be necessary to recognize that device. The framework makes the point that there are a large number of unique digital devices that are not in the provided list. The framework points out that a practitioner should be aware that there are some devices that will require unique

considerations. With a general knowledge of digital devices it is reasonable to assume that a practitioner would recognize the digital music device as one of these specialized devices. The images and the documents are common in digital investigations and once the digital music device had been collected, an investigator could easy recognize those within the digital crime scene.

The guidelines miss the mark when it comes to linking the digital evidence to the suspect. No discussion on digital evidence linking to the suspect is given, although it does well in linking of the physical evidence to the suspect. This is done thorough the use of photographs and complete documentation of the scene. This documentation can then be used to link the devices to the suspect by proving them to be at the suspect's home office. Additionally, the guidelines discuss the possibility of latent evidence of a non-electronic nature being present on the physical devices. It cautions a practitioner to be aware of fingerprints or other latent evidence that may be on the digital devices that will need to be collected at a later date. This latent evidence would be useful in individualization.

The authors of the framework use evidence protection and documentation as the main methods to ensure admissibility. In the scenario the physical scene would have been well documented and all the steps taken by the investigators would also be recorded. The guidelines make no mention of imaging or duplicating the digital devices. Also there is no method of hashing or CRC to later prove integrity of the digital evidence found on the devices' digital crime scene. This lack of integrity checks and imaging is a major downfall to these guidelines and will hurt evidence admissibility from the digital music device as well as the

other devices because it would be difficult to prove the evidence had not been contaminated.

This guideline's transference is high, simply based on the fact that digital evidence searches are not device specific. As opposed to most other guidelines the authors of this framework propose a methodology that the guides a practitioner based on the type of incident instead of the device type. The target of the digital investigation in this framework is based on incidents. This unique approach allows the guidelines to be easy transferred between different types of devices but also limits to the applicability to the incident types described in the framework. This limitation hurts the guideline's transference but overall, this unique approach is highly transferable to a wide rage of devices including the digital music device.

Many of the guideline's steps are affected by the inclusion of the digital music device in the scenario. In the known devices section, the digital music device should be listed, it is not, though considerations for other digital devices are made. Collection is affected by the digital music device because a practitioner should be aware of these devices and their large storage capacities. Exams listed by device type do not mention imaging or hashing. This should be especially important if the digital music device is collected because it may be difficult to create an image.

An examination of digital forensic models.

Reith, Carr and Gunsch's *An Examination of Digital Forensic Models* (2002) was applied to the scenario through the high level, abstract nine step model they present. *Identification* occurred even before the scene was recognized. This pre-forensic step was when the company realized that data was missing. The *preparation* for the crime involved gathering the tools needed to evaluate the scene and getting the necessary warrants and monitoring permissions to narrow the suspects down to this particular employee. An *approach strategy* was developed based on the preparation and narrowing of the target to the employee in the scenario. The investigators worked to develop a plan that would minimize the impact to the company and other stakeholders.

Preservation began with securing the scene from contamination and the investigators prevented unauthorized personnel from being at the scene. *Collection* documented the physical crime scene. Also, this step is where the devices were duplicated. The computer was duplicated, though no specific instructions were given to the investigators by the guidelines. The digital music device is recognized as an MP3 player by the investigators and is collected and imaged.

The investigators do an e*xamination* and a "systematic search of evidence" in the scenario (Reith et al., 2002). The investigators searched the physical crime scene of the home office for evidence. The digital crime scenes in the computer, media and digital music device were searched electronically. The investigators found the images and documents on the digital music device and

are able to move to the next stage. *Analysis* of the images and documents found on the digital music device allowed the investigators to reconstruct the actions of the employee and develop the crime theory. Finally, the *presentation* of the evidence that was colleted is made to the appropriate authorities. The employee is found to have taken company information and is both criminally and civilly liable for the crime. *Returning evidence* to the company was the final step for the investigators and with the investigation completed, the documents and pictures were returned to the company.

This framework is the only one that directly recognizes the digital music device as an electronic source of potential evidence. These guidelines are a success in all aspects of the criteria. The guidelines have several steps that are affected by the presence of the digital music device and provide high level guidance for them. The framework directly states that the digital music device is something the investigators should be interested in. With the collection of the digital music device, a practitioner would easily recognize the images and documents present on it during the examination. The guidelines also direct the investigators to be aware of future technologies as well as common storage devices such as flash drives and removable hard disks. The guidelines work well to point an investigator to wide range of digital evidence.

This framework uses the preservation and approach strategy to individualize the evidence to the suspect. By isolating the scene for contamination and recording the physical crime scene, the guidelines led the investigators to prevent contamination. Because the evidence is shown to belong

to the suspect, preservation will prove that the investigators did not change the evidence and therefore must have been created by the owner, who is the suspect. For digital evidence, hashing is used by the investigators as a means of proving integrity.

The authors of this framework provide guidelines for several means to accomplish the goal of admissibility. First the scene of the crime was preserved and isolated from any opportunities for contamination. The investigators were even directed to prevent electric devices from coming in contact with other potential sources of electromagnetic interference. During collection, the investigators recorded all evidence and the entire physical crime scene. The digital devices that were collected were duplicated or imaged. Before going to the scene in the scenario, the investigators, following these guidelines, would develop and document an approach strategy, to follow during the investigation. A well documented strategy for the investigation would assist in admissibility because the documentation would allow the investigation to be repeated if necessary to show that the same results will occur. These guidelines provided the investigators with a robust group of techniques to account for potential contamination and fulfilled the requirements of admissibility.

The guidelines are high level and abstract and can be applied to a large number of devices and situations. They are not dependent on a specific technology or crime. The model is designed like this on purpose and lower level guidelines can be created for specific devices. The abstract nature of the framework provided the theoretical guidelines while allowing the opportunity to be

continually applied to current and future technologies. These guidelines worked well in regard to their ability to be transferred between many different devices.

The framework was created with the digital music device and other unique devices in mind. Its high level nature allows it to be general enough to provide guidance when used with the scenario involving the digital music device. Steps of the guidelines do not change when applied to the digital music device, computer or any other digital device. This is due to the fact that the authors planned the guidelines with these and other special devices in mind.

Several steps do have unique consideration none the less when applied to the scenario with the digital music device. The approach strategy in this case would be developed looking for this type of device. The examination would need to have special precautions taken to write block the device for imaging or live analysis.

Recovering and examining computer forensic evidence.

Recovering and Examining Computer Forensic Evidence (Noblett et al., 2000) presents a less formal framework for cyber forensics. The authors outline guidelines of acquiring, preserving, retrieving, and presenting. The framework is general and does not contain specific steps. The guidelines, when applied to the scenario, produced the following results.

Planning for the evidence collection from the suspect occurred well in advance. Upon arrival on the scene the investigators documented the area and colleted evidence. They recognized the digital music device as a unique

electronic device that needed to be collected. During the examination they *preserved* the integrity of the evidence by not analyzing any originals. Copies or images were produced and verified with a cyclic redundancy check (CRC). Both types of evidence, physical and “metaphysical,” were *retrieved* and searched following the organization’s forensic guidelines. The investigators found the images and documents related to the company information and recorded and reported the evidence.

This framework, when evaluated on the criteria, met the requirements of recognition, admissibility, and transference. This makes its guidelines a partial success. The guidelines met the requirements of recognition. The framework provides guidance at a level that is not device specific. The guidelines pointed to the fact that the digital device market is changing at a rapid peace and an investigator must be aware of the ever increasing number of devices. The investigators, when following these guidelines, would not necessarily be led directly to any of the evidence. They must determine what they believe to be evidence on their own, but the recognition of the increasing device market makes it reasonable to assume they would recognize the digital music device along with the other more common physical crime scene components of the computer, papers and media. The framework uses the idea of “metaphysical” evidence as the electronic form found on devices. During a search for the “metaphysical” evidence on the digital music device the images and documents would be recognized and documented as evidence.

In order to individualize the evidence, the guidelines recommend that practitioners follow structured steps. Individualization is the weakest component of these guidelines. In no way do the guidelines lead an investigator to secure the scene or prevent contamination. For “metaphysical” evidence the use of CRC is mentioned to prove that files were not manipulated during the investigation. This is a very minimal effort at individualization. The guidelines do not mention timelines or reconstruction of evidence to link it to the suspect or the incident.

Admissibility requirements are better met than the other criteria when an investigator follows these guidelines. In this case the scene was documented thoroughly and investigators would only work off of a comprehensive organizational plan that was developed in advance of the incident. Steps were taken to prevent the digital evidence from being altered and this integrity was further proved by the use of a CRC on obtained “metaphysical” evidence. Examinations where only conducted on a copy of the digital information on the computer, media, and digital music device. No mention of write block is made by the guidelines, but one is cautioned not to alter the evidence.

The guidelines really do not have a target, so the transference is high. This framework is basically a discussion of what the authors believe is the best practice when conducting computer forensic examination and collection. There is not a specific technology or crime target. The guidelines therefore could be used for a wide rage of technologies and crimes.

The guidelines are affected in several ways by the presence of the digital music device in the scenario. Organizational policy in regards to collected

devices would have to be altered to account for the digital music device. Copies of the digital music device need to be made in order to access the “metaphysical” evidence the framework reports is in a digital device. This may be difficult with a digital music device and recognition of write block capabilities for these devices would have to be made. Investigations should be based on organizational policy and many organizations may not have policies in place for the digital music device.

A hierarchical, objectives-based framework for the digital investigation process.

Beebe and Clark (2004) have developed *A Hierarchical, Objectives-based Framework for the Digital Investigation Process* from which guidelines for cyber forensic analysis of the scenario were determined. Investigators following the guidelines of Beebe and Clark (2004) would have a six step process in their investigation of the stolen corporate data.

Preparation for the events in the scenario started long before the incident. The investigators were trained in cyber forensics and assembled toolkits to take onsite in the event of an investigation. Additionally, planning was done on how to respond to the event. Once the incident occurred, the *incident response* began and the investigators determined the proper course of the investigation. They verified the incident and contacted appropriate authorities. Also the investigators planned what to look for in the investigation.

The investigators then moved to *data collection* and, after identifying the suspect and locations of potential evidence they proceed to the scene to secure the evidence there. The floppy disks and CDs are collected. The computer is collected and integrity is insured with write protection of collection and hashing of images. The digital music device is missed due to the fact that investigators are not guided to be aware of other electronic devices.

The investigators now begin the *data analysis* and search the collected electronic physical evidence for potential digital evidence. Obvious pieces of digital evidence are recognized and then more extensive techniques such as keyword searches are conducted. The investigators miss the documents and images on the digital music device because it was overlooked during the physical collection phase.

Investigators have not found any relevant evidence to the case. They report in the *presentation of findings* phase that no information was found on the suspect's media or computer. They believe that the information must be stored somewhere else. This is detrimental to the company's case against the suspect. In *incident closure* the investigators review their process of investigation. They realize that a critical piece of evidence, the digital music device, was over looked. At this point though all items of physical evidence are returned to the owner and the collected digital evidence has been destroyed.

These guidelines fail when applied to the developed scenario. They do well in areas of transference and admissibility but fall short in regards to recognition and individualization. Overall there are many aspects of the

framework that are affected by the presence of the digital music device. A strict interpretation of the guidelines fails to recognize the digital music device. It is safe to say, had the digital music device been recognized, a practitioner following the guidelines would have easily recognized the digital evidence of the images and the documents, satisfying the criteria recognition for the digital crime scene but not the physical one.

The guidelines are high level but then it specifics specific devices and media types that should be accounted for. In order to provide a more complete framework and satisfy the requirements of the scenario one would need to develop lower abstraction layers for the digital music device, the goal of this framework is just that. While the high level guidance does not provide for a complete evaluation, it should be noted that if the guidelines were developed to the fullest intent then there would be a sub level created especially for the digital music devices, which could have been referenced when one was recognized at the scene. The computer, electronic media and papers are recovered from the home office situation.

This framework is not sufficient to individualize evidence to the suspect. There is no mention of securing the scene and preventing contamination. The guidelines do point to the necessity to use a write block for proper imaging of the devices collected at the scene. This provides integrity of the evidence. During the data analysis the investigator would produce a timeline that could be used to link the evidence to the known times of the incident. These are good steps towards

individualization of the digital evidence, but more consideration should be given to the physical scene.

When evidence is collected following the guidelines, admissibility is met in several ways. Incident response is planned in advance of on scene activity. This planning allowed the investigators to be prepared for the scene and conduct the collection in manner that was consistent with admissible evidence practice. The evidence that is collected is imaged and hashed by investigators. Also the use of a write blocker in imaging makes contamination highly unlikely. Documentation of results and activities is also conducted by the investigators and provides a record of all activities conducted around the evidence.

The framework is abstract so there is no specific target of the general guidelines. The framework hopes to provide the high level guidelines that allow it to be generalized to a number of devices. This makes it highly transferable to a wide range of devices. The guidelines need sub steps to be created for each possible abstraction layer in order to be completely transferable. The framework's guidelines cannot be easily applied without complex work on the part of the practitioner to develop the necessary underlying sub steps.

Several steps of the guidelines are affected by the presence of the digital music device. First in the incident response phase, one should be prepared for the digital music device. This could be done by the preparation of sub steps and technical capabilities for collection and analysis. Second the data collection phase would need to provide guidance that would lead to the recognition of the device. The unique considerations when imaging a digital music device will affect

the data analysis. Write block again may not be achieved without special tools or configurations. Therefore the many aspects of the digital music device make the framework highly affected by its presence.

Getting physical with the digital investigation process.

Getting Physical with the Digital Investigation Process (Carrier & Spafford, 2003) outlines a five step process with multiple sub steps. This multi-tier process is high level and granular. The base five steps lead the investigator with conceptual ideas while the sub steps point the investigator to actual practice. When applied to the scenario the following occurred.

The *readiness* phase had the investigators prepare for the incident long before it occurred. They prepared on two fronts; *operations readiness* and *infrastructure readiness*. The investigators prepared operationally for future investigation by attending training sessions and preparing equipment for an investigation. When an event was recognized, the *deployment* step began. The investigators received notification of the incident and communicated with the appropriate authorities to obtain the necessary approvals to conduct the investigation. The investigators worked with the company and law enforcement to obtain a warrant to search the suspect's home office.

After the recognition of the event, the *physical crime scene investigation* began. Physical evidence and physical devices that may contain digital evidence were *preserved* by limiting access to the scene to only authorized personnel. The scene is then *surveyed* by the investigators for obvious pieces of evidence. The

CDs and floppy disks are *collected*. The computer is unplugged from the network. The entire scene is documented and photographs are taken. The location of all evidence is recorded. A complete search of the scene reveals the digital music device, it too is collected, as the investigators know it may contain digital evidence.

After collection, each physical digital device that is collected contains a digital crime scene with possible evidence, which requires a *digital crime scene investigation*. The investigators created backup images of the computer, digital device, and media in order to *preserve* the evidence. They *survey* the devices and media for any type of evidence and find the images from the company and the documents. They *documented* this by hashing so they can prove that the evidence has not been tampered with at a later date. The device images were also carved and *searched* deeper for other evidence that may not have been obvious, but none was found. Timelines were created based on the images' and documents' creation and access dates. The investigators compiled the discovered evidence and *reconstructed* how the evidence got there. Finally the digital evidence is incorporated with the physical evidence found on the scene.

A report on both the physical evidence and the digital evidence is created by the investigators. They develop the theory of the crime and *reconstruct* what they believe occurred. Finally, they *presented* both the physical and digital evidence to the appropriate authorities. After the presentation, the processes used in the investigation were *reviewed* and the investigators determined ways they could improve in the future.

These guidelines are a success, the digital music device was recognized, evidence collected and requirements of the criteria were met. The guidelines are affected in several ways by the presence of the digital music device in the scenario. The recognition occurred because the investigators performed an in-depth search of the scene for additional digital devices and found the digital music device. The computer and media were easily recognized in the survey phase. The paper was recognized in the survey phase as physical evidence. Because the collection of the digital music device occurred, the digital investigator was able to recognize the pictures and documents on the device during the digital crime scene investigation.

The evidence recognized by the investigators following these guidelines would be individualized to the suspect through several means. The scene would be preserved and access limited to authorized personnel. The scene was photographed and thoroughly documented. The digital crime scene present on each of the collected devices was hashed and chain of custody kept so that integrity could be shown at a later date. The digital evidence was reconstructed in a timeline to link it to the timeframe of the incident and the suspect.

Precautions to provide for admissibility were achieved in several ways. One of which was following a detailed methodology that was developed before the incident. Investigators prepared by training in the readiness phase. They assembled the proper tools for a variety of incidents. The scene was documented and proper authorizations for the search were secured by the investigators. Photographs were taken of the scene and the device locations and connections

were all recorded. Devices and other physical evidence were tagged for chain of custody. The digital crime scenes were all imaged and hashed to show integrity. Also the chain of custody for digital evidence was kept. These aspects make this framework quite robust when it comes to admissibility. It is obvious that this basic forensic requirement was thought though in the development of its guidelines.

The guidelines can be used for the digital music device for several reasons. The guidelines are not technology specific. They are high level in its major five steps and then break down into lower level steps that can be applied to any type of device or incident. These are easily transferred to other devices. The recommendations of hashing and imaging apply to the digital music device and other devices. The idea of a digital crime scene is a common component amongst all digital devices. The digital crime scene phase points to type of evidence to look for, not specific means of looking for it. The actual step of technology specific evidence discovery is left up to the investigators.

Many of the steps of guidelines are affected by the digital music device. The investigators should be prepared for such devices, so in the readiness phase they should receive training for digital music devices as well as other specialty devices. In the physical crime scene phase the investigators look for physical devices there is a cover all for other devices, but the digital music device could be spelled out along with cell phones and PDAs as the digital music device is become more common place. Additionally, in the digital crime scene the investigators would need to make special considerations for digital music device by preparing equipment with proper write block capabilities to image the devices.

DISCUSSION

The guidelines analyzed in this thesis, showed outcomes that covered the entire rage of possible scores (see appendix B). The *Electronic Crime Scene Investigation* (DoJ, 2001) and *Recovering and Examining Computer Evidence* (Noblett et al., 2000) were rated as partial success by meeting some of the criteria but not all. However, both of these guidelines were successful in the scenario. The guidelines of *An Examination of Digital Forensic Models* (Reith et al., 2002) and *Getting Physical with the Digital Investigation Process* (Carrier & Spafford, 2003) were the only ones to be rated as full success. They were able to meet all the criteria when used for the scenario.

Finally, *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process* (Beebe & Clark, 2004) was the only framework to fail. It did meet some of the criteria but a strict interpretation of the guidelines did not effectively complete the scenario and failed to recognize the digital music device. The identified guidelines were more successful for digital music device forensics than was initially believed. None the less, changes in the guidelines would lead to their increased applicability to digital music device forensics. This thesis does not create a new set of guidelines that would only add to the already large number of guidelines to choose from. However the recommendations for modifications to

the guidelines analyzed if implemented would help their success for the scenario and digital music device forensics (see appendix C).

Recommendations

Electronic Crime Scene Investigation (DoJ, 2001) being a partial success would only require minimal change in order to be a full success for digital music device forensics. The main inadequacy with the guidelines was admissibility. The guidelines should offer better guidance on the use of imaging and hashing. These types of recommendations for proper forensic practice would help assure that evidence collected and analyzed would be admissible to the court of law. The use of write block especially through USB or other connections common on unique devices are a necessary addition to these guidelines. In the individualization of collected evidence the guidelines should discuss the use of hashing and imaging for integrity.

The guidelines could also use timeline development to link the evidence discovered on the suspect's devices to the times of the incident. The guidelines should receive an update to its known devices section to include such common devices as the digital music device, Blackberry and other common digital devices of today. The guidelines case by case instructions are also limited by the cases they account for. The creation of additional cases to meet current challenges for the cyber forensic community would be useful for forensics of any device. The steps of the guidelines that were all affected by the digital music device in the scenarios would be accounted for by these recommendations.

An Examination of Digital Forensic Models (Reith et al., 2002) was rated a full success for digital music device forensics. Its guidelines were able to meet all the criteria requirements. It was affected in some ways by the digital music device in the scenario. Modifications to the guidelines could make it even more useable. Information on the special precautions necessary for the use of write block when imaging a digital music device would be helpful to an investigator. The guidelines were designed with these devices in mind, so no other changes to these abstract guidelines are necessary.

Recovering and Examining Computer Evidence (Noblett et al., 2000) was rated as a partial success requiring several changes to be better at digital music device forensics. The guidelines rely heavily on the recommendation to follow organizational policy. The problem being that these policies may not be prepared for a digital music device. The guidelines would be more effective if they offered some guidance for individuals who were attempting to develop organizational policy. The guidelines also fail to account for unique considerations when imaging the device. As with other guidelines, discussion of write block for the device is necessary. The individualization of discovered evidence should also be discussed. The guidelines need to point out that the scene should be secured and the “metaphysical” as well as physical evidence needs to be treated in a way that minimizes or eliminates the possibility of contamination. Construction of a timeline or theory of the crime would also be useful concepts for individualization. With the additions of these components the

guidelines would be more up-to-date and useful for application to the digital music device.

A Hierarchical, Objectives-based Framework for the Digital Investigation Process (Beebe & Clark, 2004) needs a lot of work to be used for digital music device forensics. The investigators following these guidelines did not recognize the device in the scenario. The guidelines should be changed in several ways and sub steps for the digital music device need to be created. The guidelines go too far and attempt to be granular when their initial design is as a high level framework. The guidelines become technology and device specific when they should remain independent and allow a practitioner to create these specifics in lower abstraction levels.

The sub step idea is one that would work well for digital music device forensics. The original six steps should remain high-level. If a practitioner were to follow the guidelines for digital music device forensics, steps for these devices would need to be developed. When one was discovered at a scene, the abstraction layers that were created for the device could be referenced and used in the collection and analysis. These sub steps should account for the use of special software configurations to image the digital music device. Securing the physical scene from contamination is also missed in these guidelines. They should include a recommended practice of limiting access. Write block capability for images of the digital music device is not discussed and would be necessary in the lower levels to properly meet admissibility requirements. The areas that are

affected by the digital music device could all be accounted for by the development of sub steps.

Getting Physical with the Digital Investigation Process (Carrier & Spafford, 2003) was only affected in few ways by the digital music device in the scenario. It scored a success and requires only minimal changes in order to be more effectively used for digital music device forensics. The guidelines point an investigator to look for PDAs, cell phones and other devices. The digital music device should be listed amongst these devices as a device of interest, in addition to having a cover all for other digital devices. As with many of the other guidelines, the use of specialized techniques for write block of USB or other connections should be discussed. Live system collection, which may be necessary for these devices, is listed but no information for precautions when performing a live system analysis is present. Overall these guidelines are highly useable with the digital music device scenario.

Common changes that could occur in all guidelines are the addition of guidelines for use of a write blocker for USB and firewire devices. The use of special software configured to prevent a write to these types of devices when imaging. Guidelines for live system collection, when imaging or write block is not possible, would make all guidelines more complete. Also all the frameworks should follow the lead of Reith et al. (2002) and list the digital music device as a electronic device that may contain digital evidence. The device could be put in the guidelines along with the computer, PDA and whatever other digital devices they are listing. Several of the guidelines also miss the opportunity for collection

of latent evidence off the device. An investigator should be warned that devices may have fingerprints or other valuable non digital latent evidence and the device should be collected in manner that protects this evidence.

Conclusions

The analyzed guidelines lead the investigators adequately in the designed scenario. They performed much better than was anticipated. Most of the guidelines, even without the changes recommended above, provided the necessary instruction to lead the investigators to discover the digital music device and recognized the evidence on it. Many fulfilled the requirements of the criteria, which were based on the basic requirements of forensic science. This is good for the cyber forensic community because it is important that the guidelines of cyber forensics be consistent with the standards of physical forensics. This adds credibility to the guidelines due to the fact that the physical forensics' standards are already well accepted by the courts and forensic practitioners. The results of this thesis showed, that for the most part, the guidelines are based on these standards.

While this by no means is the only test that could be conducted on the guidelines, a hypothetical scenario analysis, like this one, has broader implications than just determining which guidelines are best for digital music device forensics. As Reith et al. (2002) point out in their framework, the future will bring many more devices. Hopefully because of the fact that only minimal changes were necessary to guide the investigators for digital music devices,

these guidelines will also be able to accommodate other new devices as the ever changing digital market evolves.

The best frameworks were Reith et al. (2002) and Carrier and Spafford (2003) their high level and abstract nature allowed them to be applied to the digital music device. Even though the guidelines of Beebe and Clark (2004) failed in this analysis, its ideas are a step in the right direction for the community. High level guidelines with lower abstraction layers, like the one they propose, would be an important foundation for a more complete set of guidelines for the community. The sub steps they propose would work well in combination with Reith et al.'s (2002) abstract guidelines. Finally Carrier and Spafford's (2003) guidelines best embody what general level-two sub steps should look like. Their level two steps provide more detail for a practitioner yet still remain technology natural and provide general guidance.

These observations lead to the realization that a combination of the best aspects of each framework's guidelines would make a new strong foundation for cyber forensic analysis of digital music and other unique devices. This would be an excellent next step for the cyber forensics community. It would create a baseline that could be used to develop lower level guidelines to meet the unique requirements of a given situation. The combined foundation framework should be developed with the inputs of many members of the community while sub steps should be created at an individual organizational, as each situation has requirements that can not be generalized across the whole community.

The results of this research are limited in two separate ways because of the method and instrument employed. There are limitations to both the internal and external validity of the results. The limitations on the internal validity were based on the fact that the hypothetical analysis was done only by the author. The continued learning of the author during the investigation is a potential maturation limitation. The hypothetical scenario was intended to be generic enough to allow generalization of findings from the thesis. However, this was not tested and there exists a potential limitation to external validity. There may exist a scenario, where in, the generalizations made in this thesis's scenario do not meet the requirements of that specific scenario. This being the case, external validity may be challenged if a scenario could be determined where the generalizations made here are not applicable. Additionally, there is the possibility for measurement error. The author developed the criteria for evaluating the guidelines based on a thorough literature review. However, whether or not these are the appropriate criteria was not tested. While these limitations are not exceedingly detrimental to the results or conclusions of this thesis, it is important that they be identified and future work could be done to address these limitations as well as other issues.

Future Research.

As a future work to follow this research, the proposed combination of identified guidelines could be performed to create a hybrid set of guidelines with the best aspects of each. This is similar to what was done by Reith et al. (2002) and not surprisingly those guidelines were found to be one of the best.

Another area that could be explored would be to look at other unique devices and analyze these and other guidelines for use with the devices. On a larger scale a standardized effort to assess these and other cyber forensic guidelines for general use would be of benefit to the community. This would require the development of testing criteria for cyber forensic guidelines and frameworks similar to the criteria developed here. These criteria should be developed with the input of the community to address the potential validity issues identified in this thesis. A standardized effort to assess the frameworks may lead to the development of compendious and useful guidelines. The criteria used to judge the guidelines should be generalizable to any cyber forensic situation and could be based on the core requirements of physical forensics, as done with the identified criteria of this thesis. An instrument similar to the one developed in the analysis for digital music device forensics could be developed for analysis of frameworks for general cyber forensics.

This research could be carried out again in a true scientific test. For this test, participants without prior cyber forensics training could be recruited and trained based on only one set of the guidelines. Participants would then be given the situation of the scenario. As the investigators of the scenario they would visit a true physical space prepared by the researcher to be the scene for the test and would include all the physical devices described in the hypothetical scenario used in this thesis. Participants would have the opportunity to perform actual collection of evidence based on the training they received. Participants would then be able to bring their collected physical evidence into a lab and perform

analysis for digital evidence. This type of test would scientifically show if these guidelines could be used for digital music device forensics.

Having a solid foundation for cyber forensic science to be built upon is important to gain credibility as a true scientific discipline. Evaluations like this which offer a critical analysis of the foundations are necessary for the science. The guidelines created for cyber forensics are currently a continually involving set of ideas. Eventually a solid foundation based on traditional forensic science will come from this continued evolution. As cyber forensics continues to gain more creditability, it is seen not as unique, but as a branch of traditional forensics. Continued development by academia and practitioners is a necessary path for the community. As one should not fail to understand, cyber forensics is still in its infancy, the fields of traditional forensic sciences took many years to mature and there is still a long road ahead for cyber forensics.

REFERENCES

Apple iPod - music and more. (2004). Retrieved September 3, 2004, from *http://www.apple.com/ipod/musicandmore.html*

BBC News. (2004). iPod car theft ringleader jailed. Retrieved September 3, 2004, from *http://news.bbc.co.uk/1/hi/england/london/3932847.stm*

Beebe, N. L., & Clark, J. G. (2004, August). *A hierarchical, objectives-based framework for the digital investigations process.* Paper presented at the DFRWS 2004, Baltimore, MD.

Carrier, B. (2002, October). Open source digital forensics tools: The legal argument. Retrieved October 11, 2004, from *http://www.atstake.com/research/reports/acrobat/atstake_opensource_forensics.pdf*

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

Connors, E., Lundregan, T., Miller, N., & McEwen, T. (1996). Case studies in use of DNA evidence. Retrieved March 11, 2004, 2004, from *http://www.ncjrs.org/txtfiles/dnaevid.txt*

Daubert v. Merrell Dow Pharmaceuticals (509 US 579 1993) Retrieved September 3, 2004, from *http://supct.law.cornell.edu/supct/html/92-102.ZS.html*.

DoJ. (2001). Electronic crime scene investigation - a guide for first responders. In U.S. Department of Justice (Ed.).

Duke iPod first-year experience FAQs. (2004). Retrieved September 3, 2004, from *http://www.duke.edu/ipod/help/faq.html*

Giordano, J., & Maciag, C. (2002). Cyber forensics: A military operations perspective. *International Journal of Digital Evidence, 1*(2).

Guloyan, J. (2004). Booming market for MP3 players according to IDC's latest forecast. Retrieved September 24, 2004, from *http://idc.com/getdoc.jsp?containerId=pr2004_08_23_153832*

Jansen, W., & Ayers, R. (2004). Guidelines on PDA forensics (Special Publication 800-72 ed.): National Institute of Standards and Technology.

Knaster, S. (2004). *Hacking iPod and iTunes*: John Wiley & Sons.

Kruse, W. G., & Heiser, J. G. (2002). *Computer forensics: Incident response essentials*. Boston: Addison-Wesley.

Kumho Tire v. Carmichael (526 US 137 1999) Retrieved September 3, 2004, from http://supct.law.cornell.edu/supct/html/97-1709.ZS.html.

Marsico, C. V. (2004). Computer evidence v. Daubert: The coming conflict. Unpublished manuscript. Retrieved March 1, 2005, from https://*www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-17.pdf*

Menzies, D. (2004). Duke to give apple iPods to first-year students for educational use. Retrieved September 3, 2004, from *http://www.dukenews.duke.edu/news/ipods_0704.html*

National Institute of Standards and Technology. (2001). General test methodology for computer forensic tools. In U.S. Department of Commerce (Ed.) (Vol. 1.9).

Nickell, J., & Fischer, J. F. (1999). *Crime science: Methods of forensic detection*. Lexington: The University Press of Kentucky.

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000, October). Recovering and examining computer forensic evidence. *Forensic Science Communications*, 2, Number 4. Retrieved October 30, 2004, from *http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm*

Palmer, G. L. (2001). A road map for digital forensics research - report from the first digital forensics research workshop (DFRWS) (technical report dtr-t001-01 final): Air Force Research Laboratory, Rome Research Site.

Palmer, G. L. (2002). Forensic analysis in the digital world. *International Journal of Digital Evidence, 1*(1), 6.

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

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers and Security, 23,* 12-16.

Saferstein, R. (2004). *Criminalistics: An introduction to forensic science* (8th ed.). Upper Saddle River: Pearson Education.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassaday, W., & Williams, W. P. (2001). Electronic crime needs assessment for state and local law enforcement. In U.S. Department of Justice (Ed.) (Vol. NCJ 186276): National Institute of Justice.

Thomas, D. (2004). Mobile threat to company data exposed by security experts. Retrieved September 9, 2004, from *http://www.personneltoday.com/pt_news/news_daily_det.asp?liArticleID=25477*

Whatis.com. (2005). Hashing. Retrieved April 9, 2005, from *http://whatis.techtarget.com/definition/0,289893,sid9_gci212230,00.html*

Appendix A. GUIDELINES

Electronic Crime Scene Investigation (DoJ, 2001)

Seven main steps:

1: Know Devices out there- Listed large number of devices (MP3 Player was not among them).

2: Have proper tools and equipment ready- Physical collection of devices.

3: Secure evaluation scene – Protect the evidence.

4: Documentation – Document everything, locations of devices, position of mouse, conditions of devices, photograph entire scene, take written notes on what is on the computer and device screens.

5: Collection- Computer related information, contact expert and unplug computer after documentation. Collect other electronic devices Relies on contact of an expert for special consideration regarding device collection.

6: Packing, Transport, and Storage- Do not modify data, document packing of devices, be aware of latent evidence on devices (fingerprints, etc.).

7: Exams are listed by case type. This outlines what evidence to look for by case, not how to look for the evidence.

An Examination of Digital Forensic Models (Reith et al., 2002)

Abstract model developed to be not specific for a technology or crime. Requires the development of lower levels of abstraction to be made for individual devices. Nine step model:

1: Identification- Recognize the incident.

2: Preparation- Preparing tools and technologies.

3: Approach Strategy- Formulate approach to incident based on impact to maximize collection and minimize impact.

4: Preservation- Isolate the scene, secure the scene, preserve the evidence.

5: Collection- Record physical crime scene and duplicate digital evidence.

6: Examination- Systematic search of evidence, detailed documentation.

7: Analysis- Determine significance, reconstruct data, develop conclusions based on evidence.

8: Presentation- Summarization and explanation of conclusions.

9: Return evidence- Return property to proper owners.

Allows the collection from technologies based on abstraction layers. Technical details would need to be developed for each device. Sub procedures for different technology classes.

Recovering and Examining Computer Forensic Evidence (Noblett et al., 2000)

Acquiring → preserving → retrieving → presenting

Examine only well identified probative info

Information unaltered by the examination process

Document well

Recognizes the fast changing and diverse world of electronic devices

Storage methods unique to devices and media

Two types of evidence

1: Physical: Chips, media, monitors, etc.

2: Metaphysical: electronic form

Should be based on principals, polices, and procedures.

Principles of Examination

Based on organization policy. Should be structured guidance

Exams are: planned, performed, monitored, recorded and reported

Procedures and Techniques

Examination only conducted on copy of original

Verify with CRC

A Hierarchical, Objectives-Based Framework for the Digital Investigations Process (Beebe & Clark, 2004)

Multi-tier phases based on lower abstraction levels for device types. The guidelines outline a first tier high level six phase process. The high level

guidelines are then designed to be broken down into more granular phases or abstraction layers.

1: Preparation- development of technical capabilities, training, pre-forensics.

2: Incident Response- detect activity, validate the incident, formulate investigation plan, develop response strategy.

3: Data collection- obtain evidence (host based, network based, removable media and devices), ensure integrity (hash, write protect), pack & transport evidence.

4: Data Analysis- recognize obvious pieces of digital evidence, employee data extraction techniques, event reconstruction.

5: Presentation of Findings- communicate findings to appropriate audience.

6: Incident Closure- review, dispose of evidence, act upon findings.

Getting Physical with the Digital Investigation Process (Carrier & Spafford, 2003)

Five step process based on the digital investigation being similar to investigation in the physical world.

1: Readiness Phases-

Operations Readiness Phase- Proper training and equipment for investigating incidents.

Infrastructure Readiness Phase- Prepare system for the possibility of a forensic examination (Not applicable to crime scene

investigation because investigators do not have control of the suspects scene before the incident).

2: Deployment Phases-

Detection and Notification Phase- Receive notification of an incident.

Confirmation and Authorization Phase- Obtain proper authorizations to investigate the scene of the incident.

3: Physical Crime Scene Investigation Phases- Physical evidence and physical devices that may contain digital evidence.

Preservation Phase- Preserve evidence, limit access.

Survey Phase- Identify obvious evidence, develop initial theory of crime, collect fragile pieces of evidence (CDs, Computers, PDA, Cell phones), contact computer specialist, unplug computer from network.

Documentation Phase- Photograph entire scene including computer connections and layouts, document devices components (memory, hard drives, etc.), tag all evidence.

Search and Collection Phase- In depth search of scene for additional physical evidence, look for media and additional digital devices, collect evidence.

Reconstruction Phase- Correlates digital and physics evidence to develop theory of the incident.

Presentation Phase- Present the physical and digital evidence and the developed theory.

4: Digital Crime Scene Investigation Phases – The model outlines digital crime scene that exists within a physical device. Each digital device is considered a separate crime scene.

Preservation Phase- isolate system form network, collect volatile data, log files, create backup image.

Survey Phase- search image or live system for obvious piece of digital evidence (pictures, application logs, rootkits, browser history and cache).

Documentation Phase- document evidence based on its abstraction level, hash the evidence to prove its integrity at a later date, chain of custody should also be documented for all digital evidence.

Search and Collection Phase- through analysis of system for evidence (keyword searches, unallocated space, timelines, reverse engineering, encryption analysis).

Reconstruction Phase- group and classify digital evidence, what can be trusted, perform advanced analysis (decryption), how evidence got there and what it means.

Presentation Phase- present the digital evidence found back to the physical investigation team in the reconstruction phase.

5: Review Phase- Review procedures to improve.

Appendix B. RESULTS

Matrix of results listed by criteria vs. guidelines

Framework	Recognition	Individualization	Admissibility	Transference	Affected
Electronic Crime Scene Investigation (DoJ, 2001)	Yes Physical - "Other devices" Digital – Documents and Pictures	Yes Physical-Photographs, document scene, non-digital latent evidence on devices Digital- None!	No Physical- evidence protection & documentation Digital- None!	Yes Not device specific, targeted towards incident so can be used with any incident that's listed	-List digital music device in "known devices" - Imaging & Hashing - Timelines & reconstruction -USB write block
An Examination of Digital Forensic Models (Reith et al., 2002)	Yes Physical- Lists MP3 player Digital- Images and documents common	Yes Physical- preservation & isolation of scene Digital- hashing, event reconstruction	Yes Physical- preservation & isolation, record evidence & physical scene, documented strategy Digital- no electromagnetic contact, hash & image	Yes Technology & crime independent, high level, abstract	- develop approach strategy for digital music devices - USB write block
Recovering and Examining Computer Forensic Evidence (Noblett et al., 2000)	Yes Physical- increasing nbrs of devices Digital – search for "metaphysical"	No Physical- None Digital- CRC check	Yes Physical- document, work from plan Digital- CRC, image, "do not alter"	Yes No specific target, best practice for general forensics	-no organization policy for digital music device - image device - USB write block
A Hierarchical, Objectives-Based Framework for the Digital Investigations Process (Beebe & Clark, 2004)	No Physical- Failed to recognize the digital music device Digital- would have found if device had been collected	No Physical- None Digital- write block, image, timeline	Yes Physical- advance planning, preparation, documentation Digital- image, hashing, documentation	Yes Abstract, no specific target, development of sub steps per device required	-Prepare for a digital music device - recognize device - USB write block
Getting Physical with the Digital Investigation Process (Carrier & Spafford, 2003)	Yes Physical- in depth scene search, additional digital devices, Digital- Digital crime scene investigation	Yes Physical- preservation, limit access, photo & document Digital- hashing, timeline, reconstruction, theory of crime	Yes Physical- detailed method, training, proper tools, documentation, photos, authorizations Digital- images, hashes	Yes Not technology specific, digital crime scene on all digital devices, open to investigator	-prepare for the digital music device -list with other devices of interest -train for special devices

Appendix C. RECOMMENDATIONS

Below is a list of recommended changes and additions for each framework's guidelines. The bullets outline what should be discussed/included in the guidelines to make them more effective for digital music device forensics.

Electronic Crime Scene Investigation (DoJ, 2001)

- guidance on use of imaging and hashing
- use of write blocker for USB and firewire
- use of timeline to link evidence to time of crime and suspect
- update "known devices" section to include the digital music device
- create additional cases to meet more current forensic challenges

An Examination of Digital Forensic Models (Reith et al., 2002)

- use of write blocker for USB and firewire

Recovering and Examining Computer Forensic Evidence (Noblett et al., 2000)

- guidance on development of organizational policy
- use write blocker for all devices including USB and firewire connections
- secure the physical scene
- prevent contamination of "metaphysical" and physical evidence
- development of timeline and theory of the crime

A Hierarchical, Objectives-Based Framework for the Digital Investigations Process (Beebe & Clark, 2004)

- sub steps for the digital music device
- adjust main steps to remain independent
- adjust main steps to remain high level
- use of write blocker for USB and firewire
- secure physical scene from contamination
- limit access to physical scene

Getting Physical with the Digital Investigation Process (Carrier & Spafford, 2003)

- list digital music device with other devices that are listed
- use of write blocker for USB and firewire
- precautions when performing an analysis on a live system

Common recommendations for all frameworks

- use of write blocker for USB and firewire connections
- guidelines for live system collection
- list the digital music device (if guidelines list devices to look for)
- collection of non-digital latent evidence from physical digital devices (fingerprints)
- precautions to protect non-digital latent evidence

REFERENCES

APPENDICES