2010

Generating System Requirements for a Mobile Digital Evidence Collection System: A Preliminary Step Towards Enhancing the Forensic Collection of Digital Devices

Ibrahim Baggili
University of New Haven, ibaggili@newhaven.edu

Publisher Citation

Baggili, I. (2010). Generating system requirements for a mobile digital evidence collection system: a preliminary step towards enhancing the forensic collection of digital devices. European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS2010)

Comments

Dr. Baggili was appointed to the University of New Haven’s Elder Family Endowed Chair in 2015.

Posted with permission. More information and proceedings from EMCIS are at emcis.eu. Dr. Baggili was appointed to the University of New Haven's Elder Family Endowed Chair in 2015.

GENERATING SYSTEM REQUIREMENTS FOR A MOBILE DIGITAL DEVICE COLLECTION SYSTEM: A PRELIMINARY STEP TOWARDS ENHANCING THE FORENSIC COLLECTION OF DIGITAL DEVICES

Ibrahim Baggili (PhD), College of Information Technology, Zayed University,
Ibrahim.Baggili@zu.ac.ae

Abstract

Collecting digital devices in a forensically sound manner is becoming more critical since 80% of all cases have some sort of digital evidence involved in them (Rogers, 2006, p. 1) .The process of documenting and tagging digital devices is cumbersome and involves details that might not apply to other types of evidence, since each evidence item has unique physical characteristics (Hesitis & Wilbon, 2005, p. 17). The process becomes less manageable when a large number of digital devices are seized. This paper examines the information and issues investigators should be aware of when collecting digital devices at crime scenes. Furthermore, this paper proposes a mobile solution that can potentially improve the process of forensic digital device collection, by keeping track of what has been collected at a crime scene.

Keywords: Forensics, Mobile Devices, Mobile Systems, Information systems, System requirements.

1 EVIDENCE COLLECTION

Crime scene documentation is the most important part of processing a forensic scene (Lee, Palmach & Miller, 2001; James, Nordby, 2003) because it is the only medium the crime scene will be retained after it has been processed. The collection of evidence is a crucial part of the crime scene documentation process. Paul Huff, an experienced detective and crime scene investigator explained that it is important to collect evidence items in a systematic and orderly manner in an attempt to minimize the amount of errors that might happen while processing the crime scene (personal communication, November 01, 2006).

Weston and Lushbaugh (2003) explained that evidence found at crime scenes fall into seven major categories: (a) weapons (b) blood (c) imprints or impressions, (d) tool marks (e) dust and dirt traces (f) questioned documents and (g) miscellaneous trace or transfer. No where in that list do we see them mention digital devices. However, personnel in charge of collecting evidence are starting to realize the importance of collecting digital devices as a form of evidence items as cases are becoming prominent.

The evidence categories mentioned by Weston & Lushbaugh (2003) may be found on digital devices. Computer evidence in the past has been used in cases that dealt with child pornography, fraud, and stalking, just to name a few. Evidence found on computers and digital devices have enabled investigators to incriminate suspects without reasonable doubt in numerous cases. Therefore, leaving digital devices as a non-recognizable form of evidence may result in a lost repository of evidence. As we enter the digital age, the seizure of digital devices is becoming more important. Organizations such as Department of Justice in the U.S., the RCMP in Canada, the Australian National Police and Scotland Yard are “literally scrambling trying to develop new procedures and checklists to allow investigators to effectively deal with digital evidence and digital crime scenes” (Rogers, 2006, p. 1). Research papers have been published to help create theoretical models to help law enforcement and other organizations in dealing with digital evidence. Rogers (2006) explains that these initiatives are "still lacking is an applied/practical approach to dealing with digital crime scenes and the digital evidence contained there in" (p.1). Our intention is to examine and improve the practical approach of digital device collection at crime scenes that pertain to digital devices.

Henry Lee's model for crime scene analysis and documentation is applicable even in the case of digital devices (Lee, Palmach & Miller, 2001). An important rule that is followed in all forensic disciplines is that evidence should always be handled with care and should not to be altered. The proper documentation, packaging and tagging of evidence needs to be performed to retain the original state of the evidence and the crime scene. In the case of digital devices, the digital evidence found on them is considered fragile (Kornblum, 2002). Furthermore, Rogers (2006) explained "Digital/Electronic evidence is usually more volatile than physical evidence and should be "keyed" on first" (p. 23). Understanding the proper procedures for collecting devices is crucial so that "fragile evidence's" original state is maintained after the collection process has occurred. The physical characteristics and functionality that shape a digital device can play a role in its collection procedure. For example, cellular phones are treated differently at a crime scene, when compared to desktop computers, since cellular phones have a live cellular connection to the service provider. In this scenario, the use of cellular signal jamming equipment, such as a faraday bag, would be useful in blocking the phone's signal during the collection phase.

When collecting other types of physical evidence such as news papers, shoes, clothing, knives or pictures, they are not usually in an operational state. Digital devices can be in a variety of modes. For instance, they can be networked, switched on, switched off, hibernating etc. Understanding the proper procedures for seizing digital devices can aid in minimizing the loss of important digital evidence. It is important to note that forensic professionals should always adhere to the second G8 forensic principle that reads "Upon seizing digital evidence, taken should not change that evidence" ("G8 Proposed principles.", 2002, p1.). Environmental factors may also change the digital evidence being acquired therefore; studying the various environmental conditions may help in delineating the evidence collection process at the crime scene.

To tackle the problem of properly seizing digital devices, the Cyber Forensics community has established a set of recommended guidelines for the seizure of digital devices. Documents have been published by organizations such as the Scientific Working Group on Digital Evidence (SWGDE), the National White Color Crime Center (NW3C), the United States Secret Service (USSS) and the National Institute of Justice (NIJ). These documents however, are mostly technical in nature. All of the guidelines present technical procedures about the seizure of digital devices, but they do not discuss the laws associated with the seizure of evidence. To be able to effectively collect evidence at the crime scene, one should understand the laws associated with them, to ensure that forensic analysis is being performed in a law abiding manner.

2 LAW OVERVIEW

Examining case laws can assure that forensic professionals are following the right steps and documenting the right information when collecting evidence. The process of evidence seizure usually starts with the release of a legal document, one of which is a search warrant.

A typical search warrant should entail what can be seized in a format that is clearly defined (Kerr, 2005). Also some search warrants contain restrictions on when the seized items need to be returned (Clifford, p. 163). In the digital world, search and seizure of digital devices is being applied based on search and seizure laws used in other contexts (Clifford, p. 163).

When collecting a digital device, one can be seizing evidence that relates to numerous other crimes. A single computer can have evidence that relates to drugs, child pornography, credit card theft etc and other offenses. The State v. Townsend (2001) case helps illustrate that digital evidence needs to be collected in a manner that abides by the law. Also the Privacy Protection Act and the Electronic Communications Privacy Act need to be taken into consideration when collecting digital evidence, starting with the physical collection of the devices. Clifford (2006) also argues that the law should distinguish between three computers types 1) Victim's computer 2) Suspect's computer & 3) Third party computer (Clifford, 2006, p. 124). With that said, when searching for a computer system, one has to deal with certain legal limits.

Legal limits on searches stem from a) Constitutional limits b) Statutory limits and c) Limits imposed by court rule or issuing magistrate (Clifford, 2006, p. 125). Kerr (2005) also explains that under federal constitutional limits, the Fourth Amendment protects against unreasonable search and seizure. Furthermore, case law helps in showing that different categories of digital devices identify the expectation of privacy one should have. The location of the device is also important to note as was shown in the case of Welsh v. Wisconsin (1984) the highest privacy is usually attached to private dwellings. When a computer is not located in a residence, the level of expectation of privacy is not as clear. Therefore, the physical location of a computer when seized is an important factor and should be noted. A computer should be identified in one of four categories 1) A stand alone computer at home 2) Laptop computer 3) Employer-provided computers and 4) Public access computers (Clifford, 2006, p. 126). So based on the mobility of the technology and the physical location of the computer system, the level of expectation of privacy is determined.

For an employment provided computer, it should be noted whether the employer is a public or a private employer. In O'connor v. Ortegea (1987) for instance, it was shown that in public employment settings, the expectation of privacy is diminished or sometimes eliminated. It is also important to know who uses the computer. Generally case laws have aided in the categorization of users as 1) Parents 2) Spouses 3) Co-users 4) Others (Clifford, 2006, p. 139).

3 ALTERATION OF DIGITAL EVIDENCE

Research has been performed on how to destroy data on computers, and various ways to destroy digital information on hard drives. Rutter (2005) identified various ways of destroying a computer such as the use of electrostatic discharge (ESD) as he explained "A discharge as low as 200 volts is sufficient to destroy a chip, and this level of charge can easily be accumulated in just a few steps on carpet." Data on hard drives can also be deleted by sanitizing the hard drive. Garfinkel & Shelat (2003) explain that the most common methods of properly sanitizing hard drives include a)Physically destroying the drive, rendering it unusable b)Degaussing the drive to randomize the magnetic domains—most likely rendering the drive unusable in the process and c)Overwriting the drive's data so that it cannot be recovered (pg. 19).

Forensic personnel at crime scenes should be aware of the threats that can potentially damage digital devices, whether they are intentional or not. An intended threat is one that is performed deliberately by the suspect, such as degaussing or sanitizing a hard drive. A non-intended threat is one that can be caused by the environment or can simply be due to the nature of the technology itself. Environmental factors are things like temperature and humidity. These are related to the sensitivity of the digital devices (Rogers, 2006, p. 24), meaning, how susceptible the device is to its surroundings. With these factors in mind, properly trained personnel seizing digital devices should take protective measures when seizing them. Suitable containers should be used (e.g. anti-static bags and bubble wrap) (Rogers, 2006, pg. 25). Other considerations that forensic investigators should take into account include:

1. The use of antistatic bags for seizing digital devices to help in preventing ESD
2. The use antistatic gloves to help in preventing ESD
3. The use of faraday bags to jam the signal on cellular phones
4. The understanding of the proper procedures of handling an online-live system

5. The understanding of how to capture the volatile memory of a computer system
6. The understanding of the various hard drive degaussing techniques

Consequently, when documenting the evidence collection process, an investigator should note any items used to seize the device, the procedure that was used and any possible intentional and non-intentional threats. However, simply understanding how digital evidence is altered is not sufficient. We need to also examine the issues related to the evidence collection process.

4 OTHER ISSUES RELATED TO EVIDENCE COLLECTION

The problem with evidence being collected is that each evidence item has unique properties and in many cases should be handled differently (Huesitis & Wilbon, 2005, p. 17). In fact, (Huesitis & Wilbon, 2005, p. 17) state:

Evidence associated with any crime can be so varied in type, physical structure, etc, and it is so susceptible to change that no set of standard rules or procedures can adequately describe how each and every item should be packaged and submitted (Huesitis & Wilbon, 2005, p. 17). Huestis & Wilbon (2005) identified the following as common problems that require corrections by officers when collecting evidence:

1. Incorrect report numbers
2. Failure to attach a Property Report to item
3. Failure to list all items on envelope or bag
4. Property Report not completed properly
5. Failure to identify items as found, personal property or evidence
6. Incorrect status codes
7. Improperly packaged items
8. Packaging money and jewellery together

As shown in the above list, the process of collecting evidence can result in mistakes. This paper intends to propose a solution for these problems through the implementation of a mobile system that can help automate part of the evidence collection process.

Another concern that comes up when collecting evidence is during the collection of a large amount of evidence items. In an interview, James Adriansen, the head of the IRS Internet Crimes Desk explained that he was involved in cases where they had to seize 200-300 digital devices at a single crime scene. He also explained that the process becomes tedious, and that keeping track of all the digital devices is hectic. To solve this problem, he stated their department took the initiative in building a program that helps them print a label for the evidence items at the crime scene (personal communication, October 24, 2006).

To support that claim, detective Paul Huff of the Lafayette Police Department gave the example of September 11th. One can only imagine the number of evidence items that would be related to that incident. He explained that in disaster related situations, it would be difficult for evidence collection personnel to properly and systematically package all the evidence items without any mistakes, because of the number of evidence items found on the scene (personal communication, November 01, 2006).

By examining the results of both the interviews and Hesitis & Wilbon (2005), one may conclude that there are problems in the process of collecting evidence items. Some of these problems may be mitigated through an applied systematic mobile approach, with the implementation of a semi-automated, user entry based mobile system. The mobile system's proposed requirements will be discussed in the later section.

5 PROPOSED SOLUTION

This paper proposes the creation of mobile software that runs on a mobile device. The software's main goal is to aid crime scene personnel in the collection of digital devices during the course of an investigation. In order to achieve that goal, the system requirements are outlined in the system requiremensts section.

6 METHODOLOGY

The methodology used to generate the system requirements consisted of two parts. The first part included two interviews, the first with an experienced crime scene investigator, and the second with a director of a governmental forensic laboratory. The second part included surveying the available literature, and extracting the system requirements from the literature. In specific, the following steps were followed to generate the system requirements:

1. Conducting two interviews with expert crime scene investigators.
2. Surveying the guides for first responders issued by the National Institute of Justice, and other law enforcement agencies that were gathered throughout the life of the project (Nolan, O'Sullivan, Branson, & Waits, 2005; Ashcroft, 2001).
3. Surveying and adopting the framework introduced in the paper Forensic scene documentation using mobile technology (Baggili, 2006).

7 RESULTING SYSTEM REQUIREMENTS

This section presents a mobile system's minimum requirements when used in the collection phase of digital devices. As described in the methodology, these requirements were formulated by examining various computer evidence work sheets from various agencies and law enforcement departments, through personal communication with various forensic investigators and a review of the forensic literature. This list is by no means exhaustive, and may be used as a guide for building a future mobile system that can be used for the collection of digital devices.

1. The mobile device software shall enable the user to enter data
2. The mobile device shall enable the user to print a bar-coded evidence tag, even if it has to connect wirelessly to a mobile printer
3. The mobile device shall enable the user to take photographs of the digital devices
4. The mobile device shall enable the user to take videos of the crime scene
5. The mobile software shall ask the user to enter his/her name and ID number
6. The mobile software shall enable the user to enter case information as follows
    a. Incident number, Incident name, Incident description, Incident location, when to return evidence items, other people involved in collecting the digital evidence items
7. The mobile software shall enable the user to add an infinite number of digital device evidence items to an incident
8. The mobile software shall enable the user to enter the following information about the digital device
    a. Device Type, Device Color, Device Description, Device State, Device Location, Device Pictures, Device distinguishing marks, Manufacturer, Model, Serial Number, Markings, Condition, Number of hard drives, collection Date and Time, Internal

Peripherals, External Peripherals, Running programs, Operating System, System Date, System Time, Processor, Description of shutdown method, Part number, Intentional Threat, Non-intentional threat

9. If a stand alone storage device was being seized the software shall enable the user to enter the following information
    a. Storage device type
    b. Disk size, disk model, serial number, CHS, LBA, Intentional Threat, Non-intentional threat
10. If a forensic image was taken at the scene, the software shall enable the user to document that. The following information shall be documented about the forensic imaging process:
    a. Storage device type
    b. Disk size, disk model, serial number, CHS, Software used to image, Software version, Imaging start time, Imaging end time, Image verification method, compression, Drive used to store the image, serial number of that drive, disk model of that drive, CHS of that drive, Intentional Threat, Non-intentional threat
11. The mobile software shall enable the user to document all the items used to collect the device, such as anti-static bags, rubber gloves etc
12. The user shall be able to print out a uniquely identifying bar-coded label, to label the digital device. Bar codes are used as military standard (MIL-STD 230 UID). The label shall also include various other information that could be added at the user's discretion such as a signature line, the incident number and incident's date and time
13. The server shall sync up all the information from the mobile device.
14. The server software module shall enable the user to check in and out evidence items using the bar-coded tag
15. The server software module shall enable the user to accurately search through the evidence items and show their related information respectively

8 ARCHITECTURAL CHALLENGES

There are some potential challenges with the proposed mobile system. One of the major challenges is that there isn't an agreed upon ontological model for digital devices. There are numerous digital devices that exist today and new devices are continuously released. Another issue is that the process of digital device collection might change. Both of these concerns related to digital device collection can impact the system requirements and may introduce new data fields that investigators need to acknowledge during the evidence collection process. To keep up with the changes, the mobile software has to be robust and dynamic to support these changes; therefore the mobile system needs to be easily updatable.

9 CONCLUSION

When forensic personnel are at a crime scene they have to systematically collect evidence by labelling, packaging and documenting evidence items. Proper measures should be taken during any forensic process to ensure that evidence is not tampered with. Digital devices contain volatile data. The proper documentation of seized digital devices is crucial for retaining their original state information at a later part of an investigation. Currently there are challenges with the collection of evidence items. These challenges may be more problematic in digital investigations since the process of digital device collection is modern and not standardized. A mobile system can help in semi-automating the process of digital device collection at a crime scene. The mobile system can also generate tags, with barcodes that are used as a military standard (MIL-STD 230 UID). A properly developed mobile system geared towards digital devices can potentially ameliorate the process of evidence collection and enhance the retention of the original state information of the digital devices, as well as their chain of custody.

References

Ashcroft, J. (2001, July). *National Criminal Justice Reference Service.* Retrieved March 25, 2010, from National Criminal Justice Reference Service: http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

Baggili, I. (2006). Forensic Scene Documentation Using Mobile Technology. *Conference on Digital Forensics Security and Law* (pp. 41-54). Las Vegas: Association of Digital Forensics Security and Law.

Clifford, R. D. (2006). Cybercrime: The Investigation, Prosecution and defence of a computer-related crime. Durham, California Academic Press.

G8 Proposed principles for procedures relating to digital evidence. (2002). Retrieved December 7, 2006, from http://ncfs.org/documents/ioce2002/reports/g8ProposedPrinciples.pdf

Garfinkel, S., Shelat, S (2003). Remembrance of data passed: a study of disk sanitization practices.

Security & Privacy Magazine, IEEE. 1: 17-27.

Huestis, B., & Wilbon, T. (2005). *Colorado Association of Property and Evidence Technicians.* Retrieved March 22, 2010, from Colorado Association of Property and Evidence Technicians: http://capet.com/images/CAPET%20Evidence%20Class_1.ppt

James, S., H, Nordby, Jon, J (2003). Forensic Science: An Introduction to Scientific and Investigative Techniques, CRC Press.

Kerr, O. S. (2005). "Searches and Seizures in a Digital World." Retrieved December 7, 2006, from http://www.harvardlawreview.org/issues/119/Dec05/Kerr.pdf

Kornblum, J. (2002). Preservation of Fragile Digital Evidence by First Responders. Digital Forensics Research Workshop, Syracuse, NY, DFRWS.

Lee, H., Palmbach, T, Miller, Marilyn (2001). Henry Lee's Crime Scene Handbook, Academic Press.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005, March). *CERT.* Retrieved March 25, 2010, from CERT: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf

O'connor v. Orteaga. (1987). 480 709.

Paul B. Weston, C. A. L. (2006). Criminal Investigation: Basic Perspectives. Upper Saddle River, Prentice Hall Publishing Co.

Rogers, M. (2006). DCSA: A Practical Approach to Digital Crime Scene Analysis. West Lafayette, Purdue University.

Rutter, D. (2005). How To Destroy Your Computer. Retrieved December 7, 2006, from http://www.dansdata.com/sbs3.htm

Welsh v. Wisconsin. (1984). 446: 740.