10-2010

Refining the Digital Device Hierarchy

F. Chevonne Dancer

David Dampier

REFINING THE DIGITAL FORENSICS HIERARCHY

F. Chevonne Dancer[1] and David A. Dampier[2]

[1, 2]Department of Computer Science and Engineering, Mississippi State University, Mississippi State University, MS 39762

Abstract

Smartphones are increasing in popularity due to functionality, portability, convenience and affordability. Because of this, examiners must acquire and analyze these devices when criminal activity is suspected to have occurred. In order to obtain this information, it has to be extracted in a way that is repeatable and testable. There are several process models available for use, but the ad-hoc approach is on the rise. The dilemmas are that ad-hoc approaches and the forensic investigative process models available are not well suited for the examination of such devices. These approaches may cause the validity of investigator skill and methods to fall under scrutiny. To address this, there is a need for an investigative framework tailored to the unique qualities of smartphones. To accomplish this, the hierarchy of digital forensics should be understood. "Computer forensics" and "digital forensics" are used synonymously in literature, but wrongfully so. This paper highlights the differences in computer forensics, digital forensics, computer crime, and digital crime while proposing a revised hierarchy of the forensics discipline.

INTRODUCTION

Due to the increase in the use of smartphones, the need has arisen to be able to examine these devices forensically and accurately. In order to accomplish this task, a thorough understanding of the functionality of the devices as well as the methods and tools used is necessary. Before this can be achieved, the forensics community must evaluate the current state of the discipline. The authors believe that this re-evaluation begins with definitively identifying important terms that will assist in understanding where smartphones lie in the hierarchy of the discipline.

Computer Forensics vs. Digital Forensics

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

> " involving the preservation, identification, extraction, documentation, and interpretation of computer data" (Kruse II and Heiser, 2001).

Digital forensics is defined by Palmer as

> "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the

reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Palmer, 2001).

As can be seen, the definition for digital forensics has advanced over time to include potential evidentiary data from all technological devices, not just computers. Scientific proven methods are also an important part of the process because the integrity of the digital data extracted may be questioned due to its volatile nature as well as the validity of the results of the investigation (Kruse II and Heiser, 2001).. It is also noticed that the activities involved in conducting a digital forensic investigation have been expanded to include key processes that were not included in Kruse's definition of computer forensics such as collection, validation, analysis, and presentation which are all imperative components of the forensics progression. For these reasons, "computer forensics" should be a category of forensics encompassed by "digital forensics".

The authors agree with Carrier and Spafford (Carrier, 2006) on how the area of digital forensics should be divided with one exception, the addition of Small Scale Digital Device Forensics (SSDDF). Digital forensics includes any investigative technique applied to any technology and is therefore divided into four major areas:

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

The addition of SSDDF is vital and the significance of its addition is detailed in the section on: **Small Scale Digital Forensics (SSDF)**.

Computer Crime vs. Digital Crime

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

> "any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution" (Goodman, 2001).

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

Kruse and Heiser defined computer crime by categorizing it in two different classes, either the computer itself is the object of the offense, or the computer is used to commit the offense. If the computer is the object of the

offense, it is the target of the aggressor. Examples of this would be a user deliberately destroying the monitor by defacing it, pouring liquid in the chassis, physically misusing the peripherals, or physically taking a weapon and damaging it. The destruction of the computer does not always have to be physical in nature. One could embed malicious code on the computer with the intentions of causing some unexpected action to occur.

When a computer is used to commit an offense, then the target is one other than that physical computer itself. Because of this, various legal issues may arise. For instance, one could use the computer to launder money, spread viruses, commit software piracy, blackmail victims, sabotage individuals, or recreate legal documents which are all illegal activities. No matter what resources are used to accomplish these tasks, they are illegal. As an example, one can send a threatening email over the network using a specific computer which is against the law. But it would still be illegal if the same person was to write the threatening note and personally deliver it to the intended victim. Although there are no laws pertaining to computers in place to assist in deterring these types of crimes, there are punishments in place for the illegal actions committed using computers such as blackmail, money laundering, and forging documents.

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

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

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

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

Although these crimes are not considered computer crimes, they are still a part of the digital forensic process because evidence was located on a computer that supported the indictment of each suspect. With that, the authors believe that there are three types of computer crime: crimes against computers, crimes committed using computers, and crimes committed with the assistance of computers. The definition of a computer-assisted crime is when a computer is used to aide in the

commission of a crime by performing information searches and storing information pertinent to the crime in memory either actively or passively. The idea of computer-assisted crimes is vital to this research mainly because of the technology chosen as the focus.

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

Digital crime

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

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

Small Scale Digital Forensics (SSDF)

Due to the vast number of digital devices with the ability to perform various functionalities, digital forensics further categorizes devices by their physical size and operability as follows: computers, storage devices, and obscure devices. Examples of devices that are classified as computers are laptops, tablet PCs, desktop computers, and notebooks. A storage device would be a peripheral that stores digital data such as a flash drive, iPod, or external hard drive. An obscure device would be a Play Station Portable (PSP), Nintendo Gameboy, and any other portable gaming device (Kruse II and Heiser, 2001).

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

> "a small form factor device which utilizes permanent or temporary memory in conjunction with embedded chips to perform a variety of tasks" (Harrill and Mislan, 2007).

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

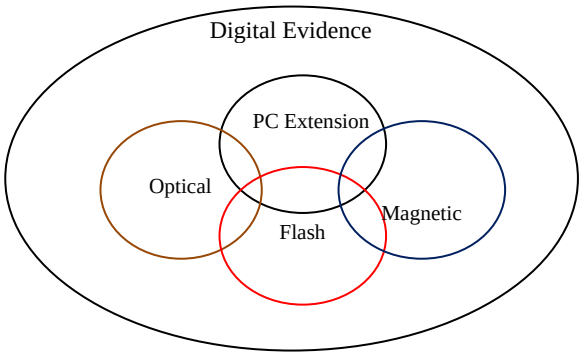

Figure 1. SSDD Framework and devices by type

Figure 1 is a revised version of the Harrill et al. classification of the SSDD Framework showing how devices store information. The difference is that based upon device breakdown, PC extension devices, flash devices, and magnetic drives can overlap. In the illustration by Harrill et al., the device categories only overlap with PC Extension devices (Harrill and Mislan, 2007). The authors would also like to point out that Harrill et. al. classifies notebook computers and tablet computers as SSDD. The digital forensic framework suggested in this research by definition does not contain any devices that are considered computers, as can be seen in Figure 2. A computer can be categorized in all four groups: magnetic, PC extension, flash, and optical. This would mean that all four categories would overlap each other. However, the illustration depicts PC extension and flash devices overlapping while magnetic and optical devices never relate. This is not to say that the topology of the framework will remain the same. Allowances for future devices will have to be considered.

Harrill and Mislan, (2007) states that in order to be effective, the field of SSDDF will have to be handled depending upon the internal components of each device. These devices can then be categorized and the type of forensics applied to each device depends upon how it is grouped. From this, it is obvious that a separate category for small scale digital devices is necessary due to the unique attributes of each. If separation from computers and the creation of a unique category was necessary for these types of devices, then a different framework for investigating them must be necessary as well. The key processes that define a digital investigation will still have to be present in the process model, but approached in a different manner.

Figure 2 depicts the digital forensic hierarchy as proposed by the author. The sub-disciplines are depicted in the rounded rectangles and the devices belonging to each are shown in the ovals. Software and network forensics are defined as sub-disciplines of digital forensics, however, defining any devices or processes belonging to each lies outside the scope of this research. Because there are aspects of each that may be categorized as part of another discipline, these rounded ovals are not fully contained by the digital forensic discipline.

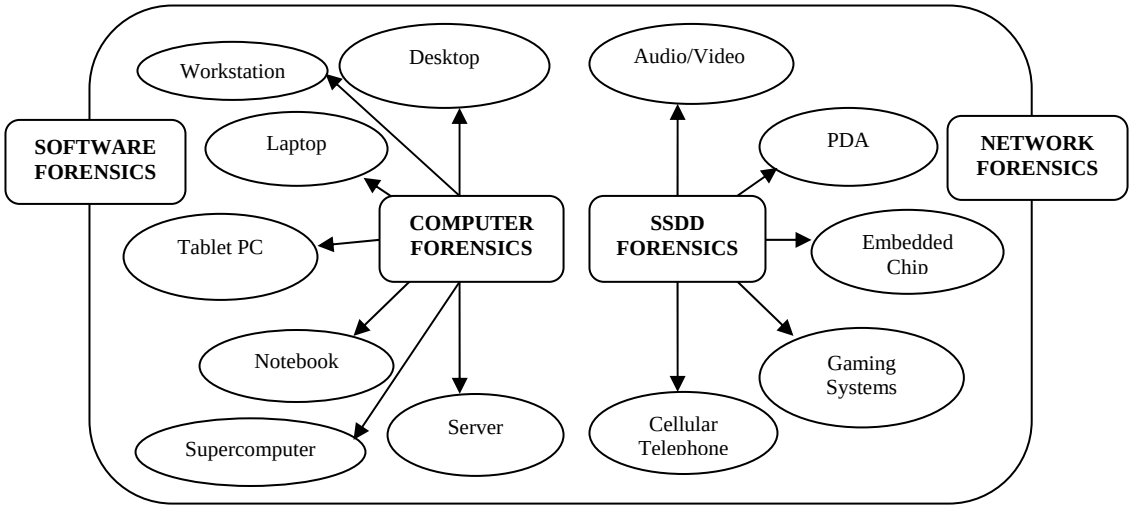

Figure 2. Digital Forensic Hierarchy and Devices

CONCLUSION

A standard terminology in the field of digital forensics is necessary in order for the successful continuation of digital research. The terms "computer forensics" and "digital forensics" are used synonymously and will continue to be used that way until further research eliminates this usage. "Computer forensics" was sufficiently used at the infancy of the discipline because computers were the target device in examinations, however, the term should now be a sub-discipline. Today, interests have expanded to include SSDDs and other types of technologies. SSDDs cannot be categorized as computers and therefore cannot belong to a discipline entitled "Computer Forensics". Simultaneously, all of the devices in question can be categorized as digital devices so the proper name for this field would be "Digital Forensics". The authors are conducting further research in the field of SSDDs targeting the smartphone. A forensic process model is being developed that deals specifically with smartphones due to issues distinct to that device.

LITERATURE CITED

Carrier, B. 2006. A Hypothesis-Based Approach to Digital Forensic Investigations. International Journal of Digital Evidence, 2:2.

Department of Justice (DOJ). United States Department of Justice: Computer Crime Cases. Computer Crime and Intellectual Property Section. [Online], Available: www.cybercrime.gov/cccases.html.

Goodman, M. 2001. Making Computer Crime Count. FBI Law Enforcement Bulletin. 70:8. 10-17.

Harrill, D. C. and Mislan, R. P. 2007. A Small Scale Digital Device Forensics Ontology. Small Scale Digital Forensics Journal. 1:1. 1-6.

Kruse II, W and Heiser, J.G. 2001. Computer Forensics: Incident Response Essentials. Addison Wesley.

Palmer, G. 2001. A Road Map for Digital Forensic Research. First Digital Forensics Research Workshop (DFWRS), Utica, New York, pp. 1-42.