An Examination of Digital Forensic Models

Mark Reith, Clint Carr, Gregg Gunsch
Department of Electrical and Computer Engineering
Graduate School of Engineering and Management
Air Force Institute of Technology
Wright-Patterson AFB, OH 45433-7765

Abstract

Law enforcement is in a perpetual race with criminals in the application of digital technologies, and requires the development of tools to systematically search digital devices for pertinent evidence. Another part of this race, and perhaps more crucial, is the development of a methodology in digital forensics that encompasses the forensic analysis of all genres of digital crime scene investigations. This paper explores the development of the digital forensics process, compares and contrasts four particular forensic methodologies, and finally proposes an abstract model of the digital forensic procedure. This model attempts to address some of the shortcomings of previous methodologies, and provides the following advantages: a consistent and standardized framework for digital forensic tool development; a mechanism for applying the framework to future digital technologies; a generalized methodology that judicial members can use to relate technology to non-technical observers; and, the potential for incorporating non-digital electronic technologies within the abstraction

Introduction

The digital age can be characterized as the application of computer technology as a tool that enhances traditional methodologies. The incorporation of computer systems as a tool into private, commercial, educational, governmental, and other facets of modern life has improved

the productivity and efficiency of these entities. In the same manner, the introduction of computers as a criminal tool has enhanced the criminal's ability to perform, hide, or otherwise aid unlawful or unethical activity. In particular, the surge of technical adeptness by the general population, coupled with anonymity, seems to encourage crimes using computer systems since there is a small chance of being prosecuted, let alone being caught [Maher00]. These "cyber-crimes" are not necessarily new crimes, but rather classic crimes exploiting computing power and accessibility to information. They are a consequence of excessive availability and user proficiency of computer systems in unethical hands. To catch and prosecute criminals involved with digital crime, investigators must employ consistent and well-defined forensic procedures. This paper explores the development of the digital forensics process, compares and contrasts four particular forensic methodologies, and finally proposes an abstract model of the digital forensic procedure. This model will attempt to address some of the shortcomings of previous methodologies.

Digital Forensics

Digital forensics is a relatively new science. Derived as a synonym for computer forensics, its definition has expanded to include the forensics of all digital technology. Whereas computer forensics is defined as "the collection of techniques and tools used to find evidence in a computer" [Calo01], digital forensics has been defined 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" [Digi01].

Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity, not just computer

systems. While 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, including future digital technologies. Unfortunately, there does not exist a standard or consistent digital forensic methodology, but rather a set of procedures and tools built from the experiences of law enforcement, system administrators, and hackers. Palmer suggests that the evolution of digital forensics has proceeded from ad hoc tools and techniques, rather than from the scientific community, where many of the other traditional forensic sciences have originated [Palmer02]. This is problematic because evidence must be obtained using methods that are proven to reliably extract and analyze evidence without bias or modification.

Lack Of Digital Forensic Standarization

In many digital crimes, the procedures for accomplishing forensics are neither consistent nor standardized. A number of people have attempted to create rudimentary guidelines over the last few years, but they were written with a focus on the details of the technology and without consideration for a generalized process. For example, Farmer and Venema outline some basic steps in their Computer Forensics Analysis Class notes [Farmer99]. Their guidelines include steps such as "secure and isolate, record the scene, conduct a systematic search for evidence, collect and package evidence, and maintain chain of custody" [Farmer99]. While these guidelines were an appropriate foundation, the remaining portion of class notes focused on specific UNIX forensic procedures. Their definition of the forensics process as well as their ideas on specific methods for achieving each of these steps could have been abstracted to become applicable to general computer systems; however, the lack of software tools precluded the exploration of non-UNIX systems. In fact, the lack of software tools on UNIX platforms prompted Farmer and Venema to construct their own suite of tools known as The Coroner's

Toolkit. These tools assist in accomplishing some of their forensic steps, primarily the systematic search for evidence. While a step in the right direction, this procedure is too focused on one platform, and not the most appropriate model for digital forensics.

Another attempt to outline a viable digital forensics process is described by Mandia and Prosise as an incident response methodology. This methodology is comprised of such steps as "pre-incident preparation, detection of incidents, initial response, response strategy formulation, duplication, investigation, security measure implementation, network monitoring, recovery, reporting, and follow-up" [Mandia01]. No doubt a well thought out methodology, they also provide detailed directions for specific platforms such as Windows NT/2000, UNIX and Cisco Routers. Their methodology serves their intended purpose of providing the depth and breadth of investigating computer crime, and is abstract in the sense that it can be applied to general computer systems. However, since their focus is purely computer crime, they do not address the forensics process in terms of other digital devices such as personal digital assistants, peripheral devices, cell phones, or even future digital technology, computer or otherwise. Their process does begin to develop a more detailed procedure in that it addresses pre-incident preparation as an explicit step to professionally organize the forensic process prior to responding to an incident. Pre-incident preparation is the process of preparing tools and equipment, honing forensic skills and continuing to educate oneself on new technologies that might be useful in dealing with an incident. This is a key step for distinguishing a professional methodology from an amateur one.

The U.S. Department of Justice (DOJ) also attempts to describe the computer forensics process, but has intelligently realized the benefits of abstracting the process from specific technologies. This abstract process includes the phases of "collection, examination, analysis, and reporting" [Tech01]. They do significantly better at identifying the core aspects of the

forensic process and then building steps to support it, rather than becoming entangled in the details of a particular technology or methodology. This is commendable because it allows traditional physical forensic knowledge to be applied to electronic evidence. In addition, the DOJ does not make a distinction between forensics applied to computers or other electronic devices. Instead, it attempts to build a generalized process that will be applicable to most electronic devices. The DOJ also lists the types of evidence that may be found on electronic devices, potential locations it may be found, as well as the types of crime that may be associated with the evidence. For example, it lists the commonly cited hidden evidence locations such as deleted files, hidden partitions and slack space, but also lists what type of information may be stored there such as social security numbers, source code or images. This information is crosschecked against a list of suspected crimes such as identification theft, computer intrusion, or child exploitation, respectively. The identification of the types of potential evidence and the possible hiding locations on different electronic devices is a positive step for forensic practitioners to develop a generalized process that can be instantiated with a particular technology to produce meaningful results to a court of law.

Finally, the Digital Forensics Research Workshop (DFRW) is another significant participant in developing the forensics process. The unique aspect of DFRW is that it is one of the first large-scale consortiums lead by academia rather than law enforcement. This is an important distinction because it will help define and focus the direction of the scientific community towards the challenges of digital forensics. The most significant challenge is that "analytical procedures and protocols are not standardized nor do practitioners and researchers use standard terminology" [Digi01]. The DFRW has worked to develop a forensics framework that includes such steps as "identification, preservation, collection, examination, analysis,

presentation, and decision" [Digi01]. Based on this framework, the scientific community may further the development and refinement this model.

An Abstract Digital Forensics Model

Drawing from the previous forensic protocols, there exist common steps that can be abstractly defined to produce a model that is not dependent on a particular technology or electronic crime. The basis of this model is to determine the key aspects of the aforementioned protocols as well as ideas from traditional forensics, in particular the protocol for an FBI physical crime scene search [FBI02]. This proposed model can be thought of as an enhancement of the DFRW model since it is inspired from it. The key components of this model include the following:

1. Identification – recognizing an incident from indicators and determining its type. This is not explicitly within the field of forensics, but significant because it impacts other steps.

2. Preparation – preparing tools, techniques, search warrants, and monitoring authorizations and management support.

3. Approach strategy – dynamically formulating an approach based on potential impact on bystanders and the specific technology in question. The goal of the strategy should be to maximize the collection of untainted evidence while minimizing impact to the victim.

4. Preservation – isolate, secure and preserve the state of physical and digital evidence. This includes preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius.

5. Collection – record the physical scene and duplicate digital evidence using standardized and accepted procedures.

6. Examination – in-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence, possibly within unconventional locations. Construct detailed documentation for analysis.

7. Analysis – determine significance, reconstruct fragments of data and draw conclusions based on evidence found. It may take several iterations of examination and analysis to support a crime theory. The distinction of analysis is

that it may not require high technical skills to perform and thus more people can work on this case.

8. Presentation – summarize and provide explanation of conclusions. This should be written in a layperson's terms using abstracted terminology. All abstracted terminology should reference the specific details.

9. Returning evidence – ensuring physical and digital property is returned to proper owner as well as determining how and what criminal evidence must be removed. Again not an explicit forensics step, however any model that seizes evidence rarely addresses this aspect.

Note that these steps are not unlike traditional methods used to collect physical evidence, but in fact the abstraction of current practices applied to crimes that involve digital evidence [FBI02]. "A large body of proven investigative techniques and methods exists in more traditional forensics disciplines. Most are applicable in cyberspace, but are not yet considered strongly" [Digi01]. Also observe that the type of digital technology involved in these steps can be abstractly defined up to this point. This is important because it allows a standardized process to be defined without specifying the exact technology involved. This allows a consistent methodology for dealing with past, present, or future digital devices in a well-understood and widely accepted manner. For example, this methodology can be applied to a range of digital devices from calculators to desktop computers, or even unrealized digital devices of the future. Using this model, future technologies and the technical details required to forensically analyze them can be instantiated to provide a consistent and standardized methodology for providing electronic evidence. This would enhance the science of forensics because it provides a basis for analyzing new digital/electronic technology while at the same time providing a common framework for law enforcement and the judicial system to feasibly work within a court of law.

Additional sub-procedures would be necessary to define the different classes of digital technology under this model. Consider a particular sub-procedure called Examine Non-Volatile

Storage that might be included under Examination. This would include the examination of all digital technologies that maintain stable states of their own accord. These technologies are analogous to paper documents, videotape and audio recordings, and are already well accepted evidentiary items. Using the definition of this category, a judicial member may use this abstraction to assign more credibility to it than perhaps technology within the Volatile Storage category. Of course there are many details specific to a particular technology that must be addressed, but this model allows for the introduction of those details. Using this model, methods of collection can be developed for each sub-category of technology, and then scrutinized and refined within the scope of that sub-procedure. Ideally, one developed and refined method may influence the development of methods for other technologies. The fact that the particular method of collection was added to the model gives the category credibility and assures non-technical observers that experience gathering similar evidence was applied to a particular case in the same category.

Continuing with the permanent storage example, consider the membership of fixed hard drives (used generally in traditional computer systems) and embedded non-volatile flash memory (used in personal digital assistants, digital cameras, MP3 players). In this pedagogical example, both technologies could contain evidence useful to judicial members, and by viewing it as permanent digital storage, allows them to sustain a sense of credibility as to the contents found. Of course the actual extraction of the data would be technology dependent, but the examination of the contents may again follow a standardized procedure since it is generally of a binary format. The advantage of the abstraction is that most digital devices, whether they are computer systems, personal digital assistants, digital cameras, or other devices, contain some type of non-volatile storage that can be analyzed for potential evidence. Realizing that commonality,

supporting procedures and tools can be identified for development and previously defined approaches may be used as a starting point for new technologies.

No model is complete without discussing the advantages and disadvantages of it. Having already discussed the advantages, it is important to mention any shortcomings. First, this model has not been tested nor proven to be a silver bullet for a digital forensics framework. It has attempted to provide a point of view that may enhance the development of digital forensic practices by identifying the commonalities of digital technologies and working backwards to establish a solid forensics process that applies to many digital technologies rather than a handful. Consideration must be made to prevent the abstraction of steps that add no value to the process because no practical use can be made of them. Secondly, this model was meant to be applied to digital technologies. Non-digital technologies were not considered in this paper, but may also require forensic analysis. The following is a summary of the model advantages and disadvantages:

Proposed Model Advantages

- Create consistent and standardized framework for digital forensic development.
- Mechanism for applying the same framework to future digital technologies.
- Generalized methodology that judicial members can use to relate technology to non-technical observers.
- Identifies the need for specific technology-dependent tools while providing insight from previously defined tools of the same category.
- Potential for incorporating non-digital, electronic technologies within the abstraction

Proposed Model Disadvantages

- Categories may be defined as too general for practical use.

- No easy or obvious method for testing the model
- Each sub-category added to the model will make it more cumbersome to use.

One obvious area not touched upon in our model is the chain of custody. Of course this is an important facet of any forensic or investigative work. This model assumes that a strong chain of custody will be maintained throughout the duration of the investigation. The absence of it on the model above makes no presumptions that it is not important, only that it is implied in any discussion of forensics.

Conclusion

Each year, there is an increase in the number of digital crimes worldwide. As technology evolves, software changes, and users become digitally savvy, the crimes they commit are becoming more sophisticated. Law enforcement is in a perpetual race with these criminals to ensure that the playing field remains level. Part of this race includes developing tools that have the ability to systematically search digital devices for pertinent evidence. As more devices become digitalized, the tool development should also progress to include these as well. Another part of this race, and perhaps more crucial, is the development of a methodology in digital forensics that encompasses the forensic analysis of all genres of digital crime scene investigations. This methodology must be applicable to all current digital crimes, as well as any unrealized crimes of the future. Many current methods are simply too technology specific. The proposed model attempts to improve upon existing models through the amalgamation of common techniques while trying to ensure method shortfalls are addressed.

References

[Calo01] Caloyannides, Michael A. *Computer Forensics and Privacy*. Artech House, Inc. 2001.

[Digi01] Digital Forensics Research Workshop. "A Road Map for Digital Forensics Research" 2001. www.dfrws.org

[Farmer99] Farmer, D., Venema, W. "Computer Forensics Analysis Class Handouts." http://www.fish.com/forensics/class.html. 1999.

[FBI02] FBI Crime Scene Search. http://www.fbi.gov/hq/lab/handbook/scene1.htm. 6 Jun 02.

[Maher00] Maher, Heather. "Online and Out of Line: Why is Cybercrime on the Rise, and Who's Responsible?" Article dated December 17, 2000. http://abcnews.go.com/sections/us/DailyNews/cybercrime_000117.html. 24 Jun 02.

[Mandia01] Mandia, K., Prosise, C. *Incident Response*. Osborne/McGraw-Hill. 2001.

[Palmer02] Palmer, Gary. "Forensic Analysis in a Digital World." 2002.

[Tech01] Technical Working Group for Electric Crime Scene Investigation. "Electronic Crime Scene Investigation: A Guide for First Responders." 2001.

About the Authors

Mark Reith graduated from the University of Portland in 1999 with a B.S. in Computer Science and was immediately commissioned as a second lieutenant in the United States Air Force. His first assignment was to MacDill Air Force Base, FL where he worked as officer in charge of Network Security for the MacDill wide area network. Following his assignment to MacDill, he was selected to attend the Air Force Institute of Technology at Wright-Patterson Air Force Base, OH where he is currently pursuing his M.S. in Computer Science with a focus on information systems security/assurance (information warfare).

Clinton Carr graduated from the Alabama State University in 1999 with a B.S. in Computer Science and was immediately commissioned as a second lieutenant in the United States Air Force. His first assignment was to Scott Air Force Base, IL where he worked as officer in charge of Information Protection Office for the Scott wide area network. Following his assignment to Scott, he was selected to attend the Air Force Institute of Technology at Wright-Patterson Air

Force Base, OH where he is currently pursuing his M.S. in Computer Systems with a focus on information systems security/assurance (information warfare).

Gregg Gunsch (Lt Col, USAF, ret.) has a BSEE from the University of North Dakota (1979), a MSEE from the Air Force Institute of Technology (1983) specializing in human and automated information processing, and a Ph.D. in Electrical Engineering from the University of Illinois at Urbana-Champaign (1991) specializing in artificial intelligence and machine learning. He has over eighteen years of experience in developing synergistic computer-human systems through the application of artificial intelligence techniques. He is currently an Assistant Professor of Computer Engineering, bearing the primary responsibility for the information systems security/assurance (information warfare) curriculum at the Air Force Institute of Technology. Contact: Gregg.Gunsch@afit.edu, (937) 255-6565 x4281, http://en.afit.edu/ggunsch/