Building Theoretical Underpinnings for Digital Forensics Research

Sarah Mocas
Portland State University

Abstract

In order for technical research in digital forensics to progress a cohesive set of electronic forensics characteristics must be specified. To date, although the need for such a framework has been expressed, with a few exceptions, clear unifying characteristics have not been well laid out. We begin the process of formulating a framework for digital forensics research by identifying fundamental properties and abstractions.

1 Introduction

Research is often done independent of practice, with an aim toward clarifying the terrain or advancing the boundaries of a particular discipline. While this is perfectly acceptable, in the case of digital forensics it is highly useful for researchers to understand the context in which their research may be applied. This is especially true when research leads to the development of forensics tools since tools developed for processing digital evidence may themselves come under scrutiny and their use may be restricted. For example, if digital evidence is presented in court then producing evidence may not be good enough. It may be important to address the admissibility and reliability of the evidence including the methods and tools used to find and process it.

Our goal is to define a set of properties and terms that can be used as organizing principles for the development and evaluation of research in digital forensics. In addition, we see these abstractions as highly useful for the development of forensic tools. In [15] an abstract model of the digital forensic procedure is given with one goal being "a consistent and standardized framework for digital forensic tool development." Their model focuses on key features of the process used to collect, examine, analyze and present digital evidence. Unlike the model in [15], the framework laid out here does not parallel the steps of the investigative process. The model presented is more closely related to that used in computer security research in that we attempt to abstract a context for digital forensics and give properties that are inherent in investigative best practices.

The motivation for this work comes from several sources. The first Digital Forensics Research Workshop (DFRWS), held in 2001, had as a stated goal "to start a meaningful dialog for defining the field of Digital Forensic Science" [14]. To this end, attendees listed five characteristics that digital forensic science must further develop, including the development of theoretic principles that attempt to explain how things work and the development of abstractions and models that can be used to guide research. The efforts carried out by the first DFRWS mark a beginning of a process and demonstrate the need for further work in this area. Both the second meeting of DFRWS in 2002 and a document produced in June 2002 by the Institute for Security Technology Studies at Dartmouth College [3] focus primarily on forensics tools, although the need for foundational work is stressed by both groups. Also in [2], guidelines for presenting digital evidence in the courtroom are given, including a section on evidentiary considerations discussing digital evidence and a section on data integrity. This paper discusses similar issues but from the viewpoint of tools development and research. Both the Scientific Working Group on Digital Evidence and the International Organization on Computer Evidence have also done foundational work especially as it relates to the practice of digital forensics [13, 12].

Section 2 gives an intuitive framework for modeling some of the characteristics of digital forensics. Section 3 expands and refines the concepts used for expressing this framework.

2 Overview

In the same way that system security is evaluated relative to a specific security policy, digital forensics is done in an *investigative context*. In forensics, information is gathered to serve a specific objective, and that objective directly relates to the environment in which the investigation takes place. For example, law enforcement gathers information to serve as evidence in support of a criminal investigation. Within the military community, the same objectives may exist, but the set of laws governing an investigation will differ. The military also relies on digital forensics to build a "conclusive description of cyber-attack activities for the purpose of complete post-attack enterprise and critical infrastructure information restoration" [4]. A national defense interest may be to find evidence that contributes to the decision making process that determines military actions. Finally, investigations in the private sector may be motivated by civil litigation; to determine if grounds exist for dismissing an employee or as part of standard system administrative and security practices. In each case there is an *investigative context*: a set of reasons for initiating the investigation, a set of constraints on the scope of the investigation, and a set of potential outcomes.

To refine our understanding of the area, it is also important to separate the investigative context from the technical environment in which an investigation takes place. The *technical environment* describes the set of devices and relationships between devices from which data is retrieved. For example, imaging a single hard drive and then performing a search on that image provides a *static technical environment*. In contrast, a *dynamic technical environment* is one in which one or more of the components from which data is retrieved has a potential for modification, independent of any system changes that might be introduced during the investigative process. In other words, "live" systems and systems connected to the Internet qualify as dynamic. These two classifications serve only as a starting point for a broader discussion on technical context.

In [8] several arguments are given as to why digital forensic science is different from other types of forensic science. Based on the concepts presented here, what is different, and therefore of interest, are the technological approaches that would be acceptable depending on the investigative context and technical environment.

2.1 Evidence

A natural question arises: *What properties are necessary and/or sufficient for evidence to be viable in a specific investigative context?* Clearly, data integrity or assuring that digital evidence is not modified (either intentionally or accidentally) is primary. Authenticating information is important as is the reproducibility of the processes used to gather and examine evidence. Knowing the seizure of evidence does not substantively change the state of either the evidence or system from which it was taken is also important. Lastly, it is valuable to show that only information relevant to an investigation has been accessed. While these properties may not be feasible in every situation, they do provide desirerable properties over digital evidence and/or the techniques for obtaining evidence.

2.2 Motivation from Research in Computer Security

When considering appropriate abstractions for forensics research, an examination of research in computer security is a logical starting point since properties such as data integrity and authentication are common to both disciplines. Furthermore, the fields are similar in that (1) computer security in practice is developed on top of layers of hardware and software that do not support secure systems and (2) digital forensics is performed on systems that do not explicitly support preserving evidence or promote investigative goals. For an overview of the major concepts and principles of computer security, see [5].

Primary to any discussion of computer security is security policy. A security policy is a set of rules defined to meet a particular goal of securing a computer and the data on it [5]. A security policy is based on the concerns of the system owner and generally aims to preserve properties such as availability, confidentiality, authentication and integrity. The policy implementation will also be influenced by security principles such as accountability, least privilege and defense in depth (to mention a few). These properties and principles are widely used to both design and evaluate systems. Potentially, in digital forensics, the investigative context can play a role similar to that of a security policy and properties outlined in the next section will serve as useful guidelines and measures.

Historically, in computer security, distinctions have been made between the concerns of commercial and military organizations and this is reflected in the overall research. Likewise, in digital forensics, law enforcement and commercial organizations have different concerns. In computer security, clearly articulating the differences has contributed to the successful development of security mechanisms for both communities. In forensics, understanding the investigative objectives (desired set of outcomes) and implied constraints (laws, etc.) of the law enforcement and commercial communities respectively will contribute to the development of more effective and useful tools for both. This is discussed further in Section 3.1.

3 Initial Framework

This section expands on and refines the intuitions presented in Section 2.

3.1 Context

Broadly, an investigation proceeds from the preservation of the state of the technology to the collection of data, to the examination (usually search) of data and then to the analysis [15]. All of these steps are influenced by the following concept of an investigative context.

- *investigative context*: a set of events that initiate the investigation; a set of constraints on the scope of the investigation and a set of potential investigative outcomes.

The first portion of this definition, *a set of events that initiate the investigation*, may or may not be viewed as part of the field of digital forensics but plays a crucial role in determining how an investigation will proceed. The next part, *a set of constraints on the scope of the investigation*, is primarily determined by the set of laws or rules that must be observed for the investigation to proceed to a desirable conclusion. Legal precedent, while typically not motivated by specific technology, may limit the types of technology that can be used effectively in a given context and so determine the scope of useful research. Constraints might also include time, cost and resource limits on the investigative process. The constraint set might also be modeled as multi-level, with legal, technical and other constraints specified. This is an interesting area for research. The set of constraints corresponds nicely to the concept of a security policy in that system security can only be developed/evaluated relative to a particular set of rules [5] and forensic methods are legitimate with respect to an investigative context. It is also useful to abstract *a set of potential investigative outcomes* in order to determine the validity of using particular mechanisms in a fixed context.

For any set of possible investigative outcomes, there is usually a subset of outcomes that interests the investigator. These are the investigator goals. In a legal setting a typical goal is to produce evidence that furthers an investigation and is admissible in a proceeding. This implies that evidence needs to withstand scrutiny. Typically, in a commercial setting, system administrators use investigative methods (1) to help maintain systems or restore crashed systems and (2) to monitor and improve system security.

In a commercial setting, the desired outcome relies on gathering and analyzing information but the information is usually not further presented in support of a case (as it might be in a law enforcement investigation). In some instances, for example if the goal is simply restoring system activity, using relatively incomplete information is acceptable. In other cases a more complete picture is needed so that system weaknesses can be tracked and fixed. In a business environment, less stringent requirements on the information gathered (evidence) implies less rigorous requirements on tools. For example, system logs are frequently used, even though there is no guarantee of data integrity. Likewise, intrusion detection systems contain information that can be used in support of system security even though this information gives an incomplete picture of system activity.

Several things should be noted. First, digital forensics done in any environment can be subject to legal considerations. For example, investigations in a business environment can lead to legal proceedings and so care should be taken when gathering evidence. Further, to gather system information, commercial organization sometimes use mechanisms, like honey pots, where there may be legal ramifications [16]. For example, state or federal laws may restrict the right to monitor some network traffic. Second, as was pointed out in [4], the military is also interested in rigorously carrying out the same tasks we have assigned to the commercial world, particularly post-attack analysis and system restoration. Last, all types of information, including system logs, are currently used in forensics across the board.

In the same way that security research has evolved based on the different interests (security goals) of military and commercial organizations, different perspectives on what are interesting investigative outcomes can be used to distinguish the type of forensics done in support of a criminal or civil case from forensics done in a business environment. In general, different investigative goals influence the set of constraints needed and therefore the set of tools and procedures that are useful. What is important for researchers and the developers of forensic tools is a clear understanding of the different environments in which digital forensics is done.

3.1.1 Additional Considerations

The following three definitions are intended to allow researchers to precisely characterize the technical assumptions they are making. Specifically, this is the environment from which data is collected.

- *technical environment:* the set of devices and the relationships between devices from which data is retrieved in support of the investigation.
- *static technical environment:* only the investigative process has the potential for modifying information related to the investigation.
- *dynamic technical environment:* one or more of the components from which data is retrieved has a potential for modifying information related to the investigation, independent of any changes to the system that might be introduced during the investigative process.

Retrieving information may be done in a dynamic environment like the Internet but another area to consider is what methods can be used in live critical systems and what will be the impact of the investigation on the larger environment. The need to characterize the appropriate environment exists because some desirable properties, like the reproducibility of a process, are closely tied to the type of environment. These categories capture only the most standard cases leaving a need for other useful technical characterizations.

Although currently the courts tend not to distinguish between information that helps to connect (or eliminate) an individual to an offense and evidence of a crime, this distinction is useful since the technical issues that apply to each may be independent. These distinctions are stated as:

- *evidence of an offense:* information of a particular crime or misdeed.
- *associative information:* information that either relates evidence of an offense to a particular person, group or event, or can be used to conclude that a relationship does not exist.

Particularly in the case of associative information, there is a potential to develop new methods for identifying, gathering and preserving this type of information prior to an actual need for it. To date, this is done as a byproduct of some systems, such as those used for intrusion detection, but typically is not done under the assumption that the information will be used to support a criminal investigation.

3.2 Properties

The following properties are not meant to be achievable in all contexts. They are intended to be desirable properties that can be used to frame questions, model behavior and evaluate tools and procedures.

It is worth noting that, in general, these properties are proposed with a legal setting in mind. Although forensics done in a commercial setting, especially if done in support of system security, could benefit from more rigorous requirements on tools, this is of more importance when evidence will potentially be presented in court. An excellent guide for preparing digital evidence for courtroom presentation is [2].

3.2.1 Integrity

In [10] the following procedural principle is given: *Actions taken to secure and collect electronic evidence should not change that evidence.* Digital information is fragile in that it can be easily modified or destroyed. Providing integrity over digital evidence is one way to show that the evidence has not changed.

- *data integrity*: assuring that digital information is not modified (either intentionally or accidentally) without proper authorization [5].

Arguably, this standard definition from computer security is vague and open to interpretation. As stated in [7], it is unclear if a single definition that covers all uses is possible or needed. For our purposes the operational view is that "digital information" refers to a set of bits, and knowing that they are not modified implies that if the bits have a particular state at some point in time, say t_1, then at a future time t_2, it is verifiable that the values of the bits are the same as at t_1. The following companion property is stated to specifically cover the reproduction or copy of a set of bits.

- *duplication integrity*: assuring that, given a data set, the process of creating a duplicate of the data does not modify the data (either intentionally or accidentally) and the duplicate is an exact bit copy of the original data set.

Separating these notions is important because the general notion of integrity is too broad to carefully express the particulars of all situations. For example, it is standard for some imaging tools to create a cryptographic hash during the process of creating a duplicate. The hash can be used to check that, at the time of duplication, the duplicate (image) and the original set of bits are exactly the same, assuring the property of duplication integrity. Further, the hash is used to ensure that, during information processing (search), any copies made from the image are identical to the image.

If the computer (and not just the data) was seized, then procedures given in [10] are used to provide integrity over the evidence. If the system was not seized, then the data on the original system may change. In such a case the hash made of the image can no longer be used to verify that the image is in fact an exact copy of the original data because the image can be changed and rehashed.

It is possible to preserve data integrity over the duplicate, with respect to the original, by using a trusted third party. At the time the image is created, a copy of the hash can be given to a trusted third party to hold in escrow. Now changes to the duplicate can be detected even if the original is modified. One possibility is to have the same technology that is creating the duplicate transmit the hash and a device ID to a trusted database. The escrow device can then acknowledge receipt by returning the same information and adding a time stamp.

It should also be noted that in [6] there is a discussion of the program developed by the National Institute of Standards and Technologies (NIST) for evaluating disk imaging tools. This is only one step in NIST's efforts to build standards for the evaluations of forensic tools. Also in [1] Duren and Hosmer give an in depth discussion on providing integrity over data with regard to time. This includes suggestions on how to achieved this with time stamps and what the underlying system requirements would be.

3.2.2 Authentication

The first definition given below follows the general notion of authentication common in computer security. The second is a rephrasing of a definition used in [11].

- *authentication* (computer security): knowing that the apparent author of text is in fact the true author.
- *authentication* (legal): knowing that the electronic evidence is what its proponent claims.

It is often important to connection a person to a piece of information. This is sometimes established by nontechnical means but technical mechanisms that can be used to make the connection between a person and a machine are biometric identification systems and cryptographic primitives. These are not commonplace. Without such mechanisms, authentication (computer security) can be difficult to positively establish based simply on digital evidence. Still, there is interesting research on ways that digital information can be used to indicate a possible author. For example, there is work on establishing personal characteristics based on document features (see [17]).

The second definition for authentication, taken from federal guidelines for searching and seizing electronic evidence, is broader and might imply integrity or authentication (computer security). If the information is claimed to have been created by a particular person then issues of authentication, as used in computer security, apply. Authentication and integrity are closely related concepts but not the same. In cryptography authenticated typically implies integrity but the opposite is not always true.

The first notion of authentication could also be broadened to include the authentication of systems, possibly based on system identifiers, IP addresses, etc. The desired property might be stated as knowing that the apparent system of origin is in fact the true system of origin.

3.2.3 Reproducibility

The scientific method is the process used by scientist to build an accurate and reliable representation of events. The Daubert ruling [*Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993)], used by federal courts to determine the admissibility of expert opinion testimony, is in part based on being able to reliably test the merits of scientific evidence. A key feature of science is that hypotheses are supported by reproducible experiments. Reproducibility strengthens the belief that a hypothesis is correct. Likewise, the reproducibility of investigative procedures lends credibility to the evidence produced.

- *reproducibility*: assuring that, given a data set or set of devices, the processes used to gather and/or examine evidence from the data set or devices are reproducible.

Currently, not all scientific evidence presented in court successfully meets the criteria implied by the Daubert ruling. But it is still worth considering when developing forensics tools and building it in when possible. In a dynamic technical environment, identifying the state of all systems involved may be impractical or even infeasible. In this case it would be interesting to prove that under certain conditions it is impossible or at least infeasible to reproduce a process.

3.2.4 Non-interference

Quoting from [9] *One of the most important aspects of securing a crime scene is to preserve the scene with minimal contamination and disturbance of physical evidence.* Typically, in any forensics investigation, some trace of the investigator is deposited at the scene. This is also the case in a technical environment. As operations are performed on digital devices, at a minimum some state information is changed and some memory is written to. Ideally, the tools and methods used to gather and evaluate evidence will not change the original data set and in a fixed context, such as a seized hard drive, this may be possible to achieve. In other situations, such as performing forensics analysis over a network connection, changing some data of the target machine may be unavoidable. In this case, we are interested in the extent to which the changes can be identified and potentially disregarded as unimportant information. The following two properties attempt to capture the essence of the interaction of the investigation on the data under examination.

- *non-interference*: assuring that the method (or tool) used to gather and/or analyze digital evidence does not change the original data set.
- *identifiable interference* : assuring that when the method (or tool) used to gather and/or analyze digital evidence does change the original data set that the changes are identifiable.

3.2.5 Minimalization

In some cases, such as those governed by Federal laws, *the law does not authorize the government to seize items which do not have evidentiary value, and generally agents cannot take things from a search site when their non-evidentiary nature is apparent at the time of the search* [11]. It is acknowledged that this is not always possible with digital evidence. Still, for legal and practical considerations, it is desirable to limit the information seized when possible.

- *minimization*: assuring that the minimum amount of data was processed (seized and/or examined).

This overly broad definition is included as an important property with potentially interesting questions and research. For example, specific Internet traffic can be targeted so, in some cases, it is possible to limit the amount of information seized, but it is currently difficult to reduce the amount of data processes from a hard disk and as sensor networks develop new research areas will emerge. By eliminating known "good" and "bad" files from a search, the amount of data processed is reduced. Still as the amount of investigative data increases, tools that reduce the size of the search space or more effectively identify useful evidence will be highly useful. Further, minimization supports 4^{th} Amendment guarantees based on privacy considerations by limiting the intrusiveness of an investigation.

3.3 What's the Point

The intention of this paper is to show that researchers can now ask questions such as:

- Under what constraints (rules, laws, resources, etc.) can a specific tool be used?
- For a particular tool or circumstance, can integrity (or any other property) be provided over the data that is processed? If so, is this provable? If not, is this provably so?
- Are the results obtained by using a tool reproducible? If not, is it possible or provably impossible to get reproducibility.

The goal is to frame requirements that are desirable in a forensics context and that can be used to measure the applicability and reliability of forensic tools and methods. We have introduced concepts that can be used by researchers working in the field of digital forensics but see this as only the beginning of a discussion. The challenge is to further refine these abstractions so that they create a useful framework.

Acknowledgments

Thanks goes to Special Agent Mark Pollitt for his insight on digital forensics, especially legal concepts (although any errors are mine) and for his knowledge of the history of the field.

References

[1] M. Duren and C. Hosmer. Can digital evidence endure the test of time? In *Proc. 2^{nd} Digital Forensic Research Workshop 2002*, 2002.

[2] National Center for Forensic Science. Digital evidence in the courtroom: A guide for preparing digital evidence for courtroom presentation. U.S. Department of Justice, National Institute of Justice, Washington D.C., 2003. Draft Document at http://www.ncfs.org/DE_courtroomdraft.pdf.

[3] Institute for Security Technology Study. Law enforcement tools and technologies for investigating cyber attacks: A national needs assessment. ISTS, Dartmouth College, Hanover, NH 03755, 2002.

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

[5] C. E. Landwehr. Computer security. *International Journal of Information Security*, 1:3–13, 2001.

[6] James Lyle. NIST CFTT: Testing disk imaging tools. In *Proc. 2^{nd} Digital Forensic Research Workshop 2002*, 2002.

[7] T. Mayfield, J. E. Roskos, S. R. Welkeand, and J. M. Boone. Integrity in automated information systems. Technical Report 79-91, National Computer Security Center (NCSC), Institute for Defense Analyses, 1801 N. Beauregard Street, Alexandria, Virginia 22311, September 1991.

[8] Michael G. Noblett, Mark M. Pollitt, and Lawrence A. Presley. Recovering and examining computer forensic evidence. *Forensic Science Communications*, 2(4), Oct. 2000.

[9] National Institute of Justice. Crime scene investigation: A guide for law enforcement. U.S. Department of Justice, National Institute of Justice, Washington D.C., 2000. NCJ 178280.

[10] National Institute of Justice. Electronic crime scene investigation: A guide for law enforcement. U.S. Department of Justice, National Institute of Justice, Washington D.C., 2000. NCJ 187736.

[11] U.S. Department of Justice. Searching and seizing computers and related electronic evidence issues. In *Computer Crime and Intellectual Property Section*. U.S. Department of Justice, Criminal Division, Washington D.C., 2002. http://www.usdoj.gov/criminal/cybercrime/searching.htm.

[12] International Organization on Computer Evidence. International principles for computer evidence. *Forensic Science Communications*, 2(2), April 2000.

[13] Scientific Working Group on Digital Evidence. Proposed standards for the exchange of digital evidence. *Forensic Science Communications*, 2(2), April 2000.

[14] G. Palmer. A road map for digital forensics research, report from the first Digital Forensics Research Workshop (DFRWS). Technical Report DTR-T001-01, Air Force Research Laboratory, Rome Research Site, 2001.

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

[16] Richard Salgado. The legal ramifications of operating a honeypot. *IEEE Security & Privacy*, 1(2):18–19, 2003.

[17] Olivier De Vel, Malcolm Corney, Alsion Anderson, and George Mohay. Language and gender analysis of e-mail authorship for computer forensics. In *Proc. 2^{nd} Digital Forensic Research Workshop 2002*, 2002.