Bridging Differences in Digital Forensics for Law Enforcement and National Security

Stephen D. Burd  
University of New Mexico  
burd@mgt.unm.edu

SSA Darrin E. Jones  
FBI, Albuquerque, NM  
Darrin.Jones@ic.fbi.gov

Alessandro F. Seazzu  
University of New Mexico  
alex@mgt.unm.edu

Abstract

Digital forensics approaches used by national security and law enforcement agencies have evolved along separate lines to serve different purposes. As a result, practices, tools, and techniques used by each agency group differ. The changing nature of national security threats and the increasing sophistication of domestic digital crime necessitates bridging the different approaches. This paper compares and contrasts the historic and current differences between digital forensics and describes how and why those differences must be bridged.

1. Introduction

Digital forensics (DF), sometimes called computer 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 facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.” [1]

Law enforcement agencies use DF as means to further their primary goal, catching and prosecuting criminals. As such, law enforcement DF is primarily concerned with obtaining evidence that can be used in a court of law. Investigators follow well-defined and reproducible procedures for collecting digital evidence and fully document their work as it occurs. The chain of evidence custody from initial seizure to the prosecution stage is also documented so that courts can be certain that there was no opportunity for evidence tampering. [2]

In the realm of national security, agencies such as the National Security Administration (NSA), Department of Defense (DOD), and Department of Energy (DOE) identify, respond to, and mitigate, current and emerging threats to national security. In this realm, DF is often practiced within the context of system and network intrusions. DF approaches are generally biased toward rapid response to intrusions, often at the expense of the ability to prosecute perpetrators. The goals are to prevent breaches before they occur and to stop breaches that do occur as quickly as possible. Ensuring successful prosecution of perpetrators is a secondary consideration, especially when perpetrators are outside of the U.S. and are “beyond reach” of the U.S. legal system. DF in the private corporate realm shares many similarities with DF in the national security realm.

For the remainder of this paper, we’ll use the term forensic examiner (FE) to describe a person or organization within a law enforcement agency, national security agency, or corporation who practices DF. However, keep in mind that DF is often a separate specialty within law enforcement whereas it’s typically combined with other tasks such as security analysis and intrusion detection in national security contexts and the corporate realm.

2. Differences

The following sections describe the most significant differences between current DF practice in law enforcement and national security organizations.

2.1. Privacy rights

An FE within a national security agency usually operates under the legal authority of the U.S. government while protecting government networks, systems, and digital assets. Systems are bannered (see Figure 1) and users have almost no expectation of privacy. In most cases users have to sign very
detailed user agreements. They know well that these systems are closely monitored and virtually all activity logged. As a result, the FE is free to do whatever is best for the protection and administration of their networks. A similar situation exists in the corporate world, where employees have little or no expectation of privacy and DF personnel are free to use whatever methods they choose to protect their networks and computing resources.

You are about to access a United States government computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose, including criminal prosecution.

Figure 1. Sample banner message for a U.S. Government computer system.

In contrast, an FE within a law enforcement agency operates under much more restricted legal authority. Great care must be taken to review and understand under what authority the media may be examined and searched. Citizens are protected against most forms of search and seizure unless they grant consent to search or unless a court of competent jurisdiction has issued a search warrant. When investigating criminal matters in a national security context, the FE may deal with classified authorities such as the U.S. Foreign Intelligence Surveillance Court (FISC).

With standard criminal search warrants, great care must be taken to not exceed the scope of the warrant. Warrants may authorize search of only parts of a system or, specific physical locations. [3] In national security and corporate contexts, the FE is only limited by technical capability—if they can get to the data they can analyze it.

2.2. Data extraction methods

A national security FE is generally free to use whichever methods or technologies are available to them. They can store, copy and share information at their discretion (within appropriate security circles). They may have to consider the external appearance of their actions so as not to telegraph to the adversary that the intrusion has been detected, especially if counterintelligence experts want to allow exploits to remain active to learn more about the adversary's methodology or even to allow exfiltration of controlled or misinformation.

National security FEs often create custom tools for use on their own systems and share tools within a small tightly controlled community of colleagues. The tools are often not perfect, but they don't have to be. If they work most of the time and they're helpful they are used.

A law enforcement FE is at the opposite end of the spectrum. Extraction technology and methodology are at least as important as the extracted digital evidence since “electronic evidence is such that it poses special challenges for its admissibility in court.” [4]

The U.S. Department of Justice (DOJ) provides testing services for domestic law enforcement agencies to ensure that extracted evidence will withstand scrutiny in court. [5] DOJ develops specifications and test methods for computer forensics tools and tests tools to those specifications. The services help toolmakers improve the tools, users make informed choices about acquiring and using computer forensics tools, and the legal community and others to understand the tools' capabilities.

During a DF exam, the FE reviews all media following very strict protocols with complete documentation so that the search or exam can be recreated in the future if necessary. In addition, chain of custody concerns are ever present. These measures ensure that prosecutors can prove that original evidence was not altered or damaged during the investigation.

2.3. Training and skill levels

In 2009 the National Academies of Sciences identified three pressing challenges in the field of digital forensics [6]:

- “The digital evidence community does not have an agreed certification program or list of qualifications for digital forensic examiners
- Some agencies still treat the examination of digital evidence as an investigative rather than a forensic activity; and
- There is wide variability in and uncertainty about the education, experience, and training of those practicing this discipline”

Some progress has been made on all three fronts as evidenced by initiatives sponsored by organizations such as the (ISC)² and the American Society of Digital Forensics & eDiscovery (ASDFED). None-the-less, many law enforcement
FEs are trained and certified on only a limited set of DF tools. Experience and advanced training provide additional skills in such areas as mobile devices, advanced data storage subsystems, and the subtleties of different operating systems. National security and corporate FEs tend to be much more skilled in network-related exploits and defense than the Law enforcement FEs. As discussed in the next few sections, the training gap for law enforcement FEs is an increasing problem as the technology employed by criminals changes.

2.4. Technical sophistication

Traditionally, national security agencies encounter more sophisticated exploits. Perpetrators want to get in, steal secrets, and get out undetected—exploit technology evolves rapidly in an attempt to keep ahead of “the good guys”. Political ramifications can be severe if intrusions can be convincingly attributed to a foreign state or military. Increasingly, more care is taken by foreign infiltrators to ensure that their intrusion attempts are not attributable.

Historically, domestic criminals have used less sophisticated intrusion techniques and haven’t made extensive efforts to avoid attribution. But as law enforcement agencies have improved their technical sophistication and prosecutorial track record, the technical sophistication of domestic criminal attacks has begun to approach that of foreign infiltrators of governmental systems. Very generally speaking, perpetrator technology and techniques seen in the national security arena migrates to the law enforcement arena within a year or two.

2.5. Encryption

In the law enforcement arena, encryption technology is commonly encountered in criminal cases. Encryption technology is often poorly implemented by both legitimate and criminal users. However, encryption used for criminal purposes is increasingly well-implemented due to greater technical sophistication and the trend by manufacturers toward embedding hard-to-crack encryption in software and hardware.

In law enforcement, FEs must often deal with secondary storage devices with either hardware- or operating system-based encryption. Law enforcement FEs can’t always easily derive passwords or keys. National security FEs also encounter encryption but it most commonly occurs as data is encrypted on exfiltration making mitigation and post-intrusion analysis more difficult.

Both scenarios illustrate shortcomings of forensic methods that examine stored data “after-the-fact”. In law enforcement the data may not be recoverable in a usable form and in national security recoverable evidence may have never been stored.

2.6. Live Memory and distributed data

National security intrusions most often deal with live networks so the value of and need to capture live memory has long been recognized by the national security FEs. The importance of capturing live memory is increasing as the sophistication level of intrusions continues to rise. Perpetrators are improving their ability to leave no trace once a system is powered down. Preserving the dynamic memory content of running systems enables an FE to preserve encryption keys and in-memory pointers to static or otherwise less or transient data on a network or individual system.

Law enforcement FEs have historically concerned themselves with static systems and data storage devices. They generally follow a process such as the one shown in Figure 2, with powering down computer systems and other devices as standard practice to preserve the digital crime scene. Devices are powered up in a read-only state for duplication and examined only after they’ve been moved to a DF lab.

![Digital Crime Scene Investigation Phases](image-url)

**Figure 2. Digital Crime Scene Investigation Phases [7]**

In the modern era, such methods are increasingly ineffective. Incriminating evidence and keys and passwords needed for access may be stored in the servers that support desktop and mobile devices or within the live memory of a perpetrator’s laptop, cell phone, home computer, or office workstation. Thus, capturing the live state is increasingly important for law enforcement FEs to preserve any keys or other necessary data that will be needed to view the
evidence later. Search warrants and seizure procedures must often cover targeted areas of servers and network communication among devices. Law enforcement FEs are increasingly required to surgically extract data from live networks.

Comingling of data that evidences a criminal matter with unrelated data protected by privacy laws is a growing challenge. For example, obtaining a search warrant for an entire corporate database server or a Google email server is highly unlikely given the comingling of targeted and legally protected content. Also, there may be laws such as the health insurance portability and accountability act that further limit access to data.

2.7. Persistent malware

The type of malware encountered in each arena also differs. In general, malware retrieved in evidence collected during law enforcement investigation is known or ordinary and has been "in the wild" throughout the Internet. Databases are available to identify the code and mitigate the existing payload. Additionally, the system can be sanitized and restored to operations if needed.

In national security intrusions the code is customized for the target and has a much narrower scope in terms of achievable goals. Further, while it may be detected and even mitigated, it is not always clear that it has been removed or that it did not duplicate itself within the target’s computing and network infrastructure. This creates significant challenges when attempting to restore critical systems to operation as it may remain unknown whether the malware was thoroughly eradicated or even if the system is still vulnerable to the exploit which could, by now, vector in from inside the organization.

3. Convergence

In this section we discuss factors driving the convergence of DF issues within the law enforcement and national security realms, including:

- Rapidly advancing technology used by criminals for attacks and a shorter lag time between its first appearance in the national security realm and its adoption by a wider range of criminals.
- Increasing trend toward national security intrusions launched from within the U.S. and perpetrated or aided by U.S. citizens or resident aliens.

3.1. Pace of technology adoption and change

Historically, advanced technologies used by adversaries in the national security realm took many years to be adopted by criminals. In the modern world, this form of “technology transfer” occurs over a period of months or at most a year or two. In addition, both law enforcement and national security FEs face an accelerating pace of technological change. As a result of these trends, both FE types need to rapidly assimilate new technology trends.

In the national security realm, this need has traditionally been addressed by hiring highly-skilled FEs, conducting ongoing research into emerging trends, and (in the post 9/11 era) sharing that information across the various agencies in the national security community. As the pace of technology change accelerates, these measures become more important and they require additional resources to ensure the ability to keep up.

In the law enforcement realm, the historically slow pace of identifying new criminal methods and developing and standardizing related methods of forensic analysis is no longer adequate.

3.2. Domestic national security intrusions

The historic paradigm of national security intrusions launched exclusively from overseas or by spies within the U.S. is increasingly outdated. In the modern world, intrusions into governmental and other systems containing national security information can be launched from anywhere. Weaknesses in domestic systems can be exploited to make them unwitting agents in national security intrusions.

In addition, the range of potential perpetrators is much larger than in the past. In addition to foreign governments, intelligence services, and militaries, possible perpetrators include domestic and foreign terrorists, U.S. citizens “investigating” alleged illegal acts of their government, and U.S. citizens who knowingly or unknowingly aid domestic terrorists or foreign perpetrators.

Because national security intrusions may now involve assets and persons in the U.S. or within the reach of U.S. law, issues of evidence and prosecution that were formerly ignored in the national security realm must now be considered. Thus, issues such as reproducibility and chain of custody are now as much a part of national security DF as they are of law enforcement DF.
4. Responding to the challenges

The convergence of DF issues in law enforcement and national security necessitates changes in current DF approaches and additional measures, which are described in the sections below.

4.1. Cooperation across agencies

The need for increased cooperation among national security and law enforcement agencies to address the changing nature of cyber-threats has been recognized for at least a decade, “Cooperation among defense, intelligence, and law enforcement must be improved.” [9] Some of the difficulties in achieving improved cooperation were also recognized: “Intelligence and law enforcement agencies have a history of rivalry and very distinct cultures. In particular, they answer to different authorities and use their information in different ways.” [9]

Cooperation has improved in the post-9/11 era and it includes the FBI to the extent it has responsibility for investigating domestic acts of espionage. However, cooperation between national security agencies and other domestic law enforcement agencies is minimal. There are several negative implications including compromising the ability of domestic law enforcement agencies to keep up with rapid technology change.

National security agencies are a reservoir of knowledge concerning newly emerging digital threats. Increased cooperation and communication among national security and law enforcement agencies is needed to enable law enforcement agencies to tap into those resources. As a result, law enforcement FEs will be able to train for new threats and technology before they occur and they can develop related forensic tools and methods that ensure that perpetrators can be prosecuted.

4.2. Improvement in DF training, tools, and methods

Although, the National Academies Report [6] pointed out significant gaps and inconsistencies in law enforcement FE training and the development and certification of DF tools and methods, it did not fully identify the impact of the factors identified earlier in this paper. The report was more backward looking than forward, and thus did not directly address issues such as emerging technology threats and the challenges of collecting and analyzing evidence in the modern digital crime environment. None-the-less, its conclusions are valid though their importance is even greater than stated in the report.

We assert that some of the training problems identified in the report are a symptom of the emerging issues identified in this paper. It isn’t just that training levels are inconsistent, rather they are insufficient to address increasingly more sophisticated types of digital crime and the technology vectors and environment in which they occur. In short, providing better and more consistent training for law enforcement FEs to use tools designed for yesterday’s digital crime does little to address more sophisticated emerging threats.

Addressing the problem requires a combination of more timely development of tools and methods to deal with emerging threats and more rapid FE training in those tools and methods.

There are some in the DF community that hope or assume that more intelligent and automated tools can be developed to identify threats and collect and analyze evidence automatically. While the development of such tools and technologies is a worthy goal, it is unlikely to address the entire range of digital crime. Further, given the role of human judgment in both criminal investigation and prosecution, it is doubtful that improved tools can be substituted for improved FE training and education. Rather, rapid technology advances by digital criminals will require increases in FE education and training levels to adequately address current and emerging threats.

4.3. Cooperative training and research

Regional Computer Forensics Libraries (RCFLs) have served as mechanism to share forensics knowledge between the FBI and state/local law enforcement agencies, provide training for state/local law enforcement FEs, and as a resource for state/local law enforcement agencies without their own FEs. [8] Some newer RCFLs are affiliated with academic institutions which multiple benefits, including:

- Students are provided with access to FE training resources and internships
- Research faculty interact with FBI and local law enforcement FEs to study and improve forensic tools and methods

RCFLs provide one possible platform for increasing cooperation between national security agencies, national and local law enforcement agencies, and related education and research activities within academic institutions. Affiliation of RCFLs with academic institutions enables part of this
increased cooperation but participation by national security agencies is also needed.

Adding academic researchers and national security FEs and researchers to the RCFL mix will improve the speed and effectiveness of knowledge transfer from the national security realm to law enforcement. Participation by national security FEs will also yield benefits as those FEs are exposed to evidence-related issues faced by law enforcement agencies in prosecuting both digital crime.

Integration of corporate and other private sector FEs into cooperative training and research is also desirable though not currently addressed through the RCFLs. The FBI does sponsor other initiatives to engage that community such as Infragard [10] that facilitate two-way information exchange between the law enforcement agencies and the private sector.

5. Summary

The historically separate worlds of law enforcement and national security DF are increasingly intertwined. Advanced intrusion and other criminal technology that emerges in the national security is rapidly adopted in the more traditional realm of law enforcement. In addition, crimes related to national security are increasingly launched from within U.S. borders and often by persons within the reach of U.S. law enforcement. Successfully addressing this reality will require merging the “best practices” of both world.

The path to merging the best of both worlds is not easy or straightforward. It requires:
- A much greater degree of cooperation among national security and law enforcement agencies
- Rapid technology transfer among national security and law enforcement agencies
- Rapid development of DF procedures for emerging technical intrusion and crime challenges that meet standards of evidence expected by courts of law
- Continuing research into more effective means to address emerging threats and crime methods

6. References


