



Computer Forensics

Steps to Ensure a Successful Outcome in the U.S. Legal System

Prepared for

Norwich University, MSIA
Seminar Five: Computer Forensic Investigations
Final Essay

Report prepared by:

Becki True, CISSP
becki@beckitrue.com

Table of Contents

EXECUTIVE SUMMARY	3
TYPES OF COMPUTER INCIDENTS	4
Detecting Computer Incidents	5
Device Log Data	6
Conclusion	6
INVESTIGATING COMPUTER INCIDENTS	6
Investigation Models and Techniques	7
Analysis	9
Investigators	9
Digital Evidence	10
Collecting and Managing Digital Evidence	12
Expectation to Privacy	14
Computer Forensic Tools and Techniques	14
PRESENTING THE EVIDENCE	15
The Decision to Prosecute	16
Presenting in Court	17
Preparing for Cross Examination	17
CONCLUSION	18
APPENDIX A: RECOMMENDATIONS	19
APPENDIX B: RECOMMENDATIONS BY PRIORITY	20
BIBLIOGRAPHY	21

Computer Forensics

Steps to Ensure a Successful Outcome in the U.S. Legal System

This report will discuss the steps required to ensure a successful outcome for the prosecution of a crime that relies on computer evidence. It is intended to be a good beginning reference for anyone interested in learning what is required to bring a computer incident to a successful resolution in the U.S. legal system.

The report will begin by reviewing some common types of computer incidents. The next section will focus on the response to a computer incident, including the collection and management of digital evidence. As with all evidence, digital evidence must be managed to ensure that it is preserved and admissible in a court of law in the United States (U.S.). The next section of the report will concentrate on the investigation of the incident. In this section, the difference between the investigation techniques for traditional crimes versus those of a cyber crime will be examined. Computer forensics tools and techniques are an important component of the investigation, and will be discussed in this section. The last section will give attention to the presentation of the evidence; first to the company, and then to a court of law.

Note: the author is not a lawyer and the information in this report is not intended as legal advice. Please consult a qualified lawyer if you require legal advice.

Executive Summary

Long before a case that relies on computer evidence reaches the courtroom, its outcome has largely been decided by how the evidence was collected, managed and examined.

Courtrooms are by their very nature adversarial, and every aspect of the investigation is subject to scrutiny by the opposing side. Computer evidence is extremely fragile and can be obliterated or damaged if improperly handled. Ask anyone who has watched a crime drama on TV how they should handle a crime scene, and most people will correctly answer to leave it alone and secure until the authorities arrive. Ask IT professionals the same question about how to properly handle a computer crime scene, and most will not know the answer.

Digital evidence is no magic bullet; it is only one piece of the investigative puzzle. A digital incident is investigated in much the same manner as a conventional crime. Traditional investigative techniques can and do lead to digital evidence, and the converse is also true. Ideally, each type of evidence builds on and supports the other. It is the sum of all of the evidence that is required to bring a case to a successful conclusion.

Although a case will not be won on digital evidence alone, digital evidence can and often does play an important role in the investigation and prosecution of computer crimes. Therefore, it is important to understand the Federal Rules of Evidence as they relate to digital evidence. It is also important to understand that all investigations should begin as if they will result in a criminal or civil case. This ensures that the evidence is collected and managed properly, preventing it from being dismissed when the case does go to court. Having an investigator or lawyer on staff or retainer would be a prudent precaution against losing evidence because it was mishandled.

The organization should decide on an investigative model, and establish processes and procedures. These processes and procedures will come under scrutiny if the incident goes to court. The investigators will be cross-examined against them, so these should be accurate and kept up to date, or the entire case could be discredited.

The organization will be faced with a decision to spend money on expensive software licensing and training, to use open source tools, or to outsource the job to a company specializing in computer forensics. Regardless of the decision, management should be aware that there are legal standards that must be met for computer forensic tools and techniques. Failure to meet these standards will disallow any evidence collected using these tools or methods.

Finally, the well-prepared organization will spend time to develop a compelling and interesting presentation for a jury. They will also prepare their investigators to provide credible testimony, and to be prepared for the tactics used during cross-examination.

Types of Computer Incidents

There are many motivations for criminals to commit computer crimes. These motives range from curiosity and “bragging rights”, to personal financial gain or to cause financial harm to a competitor or to one’s own employer. In fact, insiders can cause considerably more damage to an organization simply because they are inside the security perimeter and are trusted. According to a 2005 FBI Computer Crime Survey¹, of the respondents who experienced unauthorized access to computer systems, insiders committed 44% of them.

“Every digital crime has a source point, a destination point and a path between those two points.”² Almost always, the source and destination points are on different computers, perhaps separated by one or two continents and scores of networks. Obviously, the more computing devices and the more legal jurisdictions that are involved, the more difficult it

¹ FBI, "2005 FBI Computer Crime Survey". <http://www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf> 2005: 7-8.

² Stephenson, Peter. 2006. "The Mechanics of Cyber Attacks". 1.

is to investigate a computer crime. This fact is not lost on those who commit computer crimes, and criminals use this to their advantage.

Computer incidents that span multiple jurisdictions are extremely difficult to investigate and prosecute.

In general, computer criminals follow a seven-step pattern when committing a computer crime³:

1. **Reconnaissance:** locate a victim and learn as much about them as possible. An insider has an obvious advantage here.
2. **Footprinting:** learn more information about the target including Internet Protocol (IP) addresses, and system owners using public databases such as *whois*. Again, an insider has a distinct advantage here.
3. **Enumeration:** learn about the target's systems including Operating Systems (OS) and services running on the computers using tools such as *nmap*. An insider begins to lose their advantage at this stage. Although they may know which OS the organization uses, they may still need to conduct scans.
4. **Probing for weaknesses:** probe the target for known vulnerabilities using tools such as *Nessus*. An insider is not likely to know the specific vulnerabilities of the system, so they will also need to probe for vulnerabilities. They do have an advantage of being able to observe flaws with processes and procedures that might result in the employee gaining elevated access privileges.
5. **Penetration:** the attacker exploits a vulnerability to gain unauthorized access to the target. The insider may exploit a process or procedure vulnerability, which may or may not be easier than a system vulnerability.
6. **Gaining the objective:** the attacker carries out his or her crime. This could be a denial of service, data theft, or to load computer code for future access. There is no real advantage to an insider at this stage.
7. **Cleanup:** the attacker covers his tracks by manipulating logs to remove all evidence of the crime, and may install software known as a *rootkit* to prevent future detection. Depending on the insider's access privileges, this may or may not be easier than it is for an outside attacker.

Detecting Computer Incidents

Obviously, it will be impossible to investigate a computer incident if it is not detected. Preventing attacks is also a good strategy. Detailed discussions of both are out of scope for this document, but it is important for the reader to recognize the role that the devices that

³ Stephenson, Peter. 2006. "The Mechanics of Cyber Attacks". 2-3.

are designed to prevent and detect attacks are excellent sources of information for investigators.

For example, the logs from an Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) can provide a wealth of data for the investigator. According to Dr. Stephenson⁴, “A well-executed IDS is very likely to detect nMap as is a well-executed firewall. It is one of the attacker’s objectives to locate, understand and evade these two devices. During that process it is possible, if not likely, that the attacker will leave footprints of his or her own to be found by the astute investigator.”

Device Log Data

The data from device logs is critical to a successful investigation of a computer crime, or a crime involving a computer. Depending on the number of devices in the attack path, the log data can be overwhelming, and reviewing the data can be extremely labor intensive and impractical. In the case of a large organization, it may be prudent to incorporate the use of Security Information and Event Management (SIEM) software. This software helps collect and correlate log data, reducing the amount of data that an analyst must review.

Because the logs are so critical to digital investigations, they must be protected. Organizations need to implement good management tactics such as least privilege and separation of duties. For example, the people administering systems should not have write access to the log data. If they do, they have the ability to load software on a computer and to cover their tracks by altering the system logs.

Conclusion

As we have seen in this section, a successful digital investigation begins with a well-configured and managed system. Executed correctly, this provides the investigators evidence that can be used to support evidence collected from other sources. The investigators can piece this evidence together to determine exactly when the attack happened, how it was executed, and with some luck, its source.

Investigating Computer Incidents

In many ways, investigating computer incidents is not much different than investigating traditional crimes. All crime scenes must be preserved and evidence must be collected without contaminating it; this is no different with digital evidence. The main difference is that the crime scene either is the computing device itself, or involves one or more computing devices.

⁴ Stephenson, Peter. 2006. "The Mechanics of Cyber Attacks". 4.

What makes digital evidence much different than traditional, physical evidence is that digital evidence is extremely easy to change, manipulate, or destroy. For example, a murder investigation may involve forensic ballistic evidence. The act of collecting the bullet fragments is not often going to destroy them, and it will never turn them into bullet fragments from a weapon of a different caliber. The same cannot be said for digital evidence. Digital evidence can easily be destroyed if it is not collected properly. It can also be manipulated to look as if it came from a source other than its true source. “Stated differently, computer forensics can determine what is on the suspect’s digital storage media at the time of the forensics investigation, but is never able to determine who put it there, when, how, or whether the data has been changed.”⁵

Investigation Models and Techniques

There is currently no established standard method to conduct investigations of digital incidents. The existing process models attempt to incorporate the processes for traditional investigations and to integrate with them.

One investigative model is the framework from the Digital Research Forensics Workshop (DRFW), which is depicted in the diagram below. The DRFW consists of six classes (column headings) and associated elements. “Those elements in **bold** type are required for a complete, structured investigation. The rest may be addressed as applicable.”⁶

IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation
Resolve Signature	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling	Hidden Data Extraction	Link	
		Data Reduction		Spatial	
		Recovery Techniques			

Digital Research Forensics Workshop (DRFW) Framework for Digital Investigations⁷

⁵ Kanellis, Panagiotis, et al (Ed.). 2006. Digital Crime and Forensic Science in Cyberspace. Hershey, PA: Idea Group. 335.

⁶ Stephenson, Peter. A Structured Approach to Incident Post Mortems. 2.

⁷ Stephenson, Peter. A Structured Approach to Incident Post Mortems. 2.

Compare the DRFW to the model proposed by Brian Carrier and Dr. Eugene Spafford. The goals of their model are⁸:

- The model must be based on existing theory for physical crime investigations.
- The model must be practical and follow the same steps that an actual investigation would take.
- The model must be general with respect to technology and not be constrained to current products and procedures.
- The model must be specific enough that general technology requirements for each phase can be developed.
- The model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response.

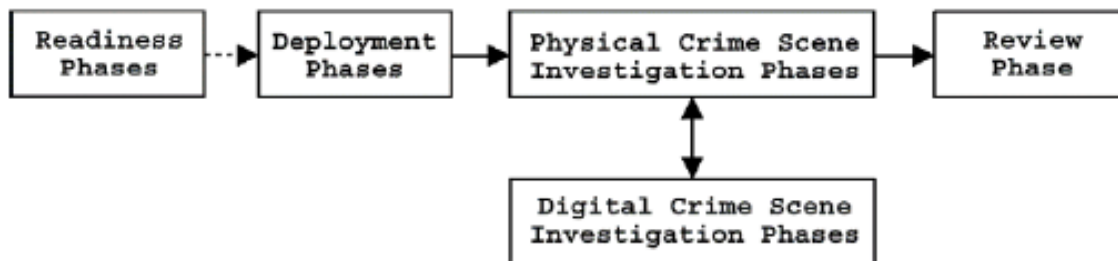
The Carrier / Spafford model compares favorably to the DRFW framework. Their model has five groups, and 17 phases, which compare to the classes in the DRFW⁹:

1. Readiness Phases
 - a. Operations readiness phase – training and equipment needed
 - b. Infrastructure readiness phase – ensures data exists for an investigation
2. Deployment Phases
 - a. Detection and notification phase
 - b. Confirmation and authorization phase
3. Physical Crime Scene Investigation Phases
 - a. Preservation phase
 - b. Survey phase
 - c. Documentation phase
 - d. Search and collection phase
 - e. Reconstruction phase
 - f. Presentation phase
4. Digital Crime Scene Investigation Phases
 - a. Preservation phase
 - b. Survey phase
 - c. Documentation phase
 - d. Search and collection phase
 - e. Reconstruction phase
 - f. Presentation phase
5. Review Phase

The relationship of the five groups can be seen in the diagram below.

⁸ Carrier, Brian and Dr. Eugene Spafford. 2003. Getting Physical with the Digital Investigative Process. 1.

⁹ Carrier, Brian and Dr. Eugene Spafford. 2003. Getting Physical with the Digital Investigative Process. 6-12.



5 Groups of Phases of the Investigation Process¹⁰

Both models attempt to provide a structured approach to the digital investigative process, and both account for the legal requirements for the collection, preservation, management and analysis of digital and physical evidence. However, the DRFW framework provides more detail, especially in the examination and analysis classes. On the other hand, the Carrier / Spafford model accounts for what they call the “readiness phases”, without which, would be gaps in the available data, and there would be no qualified people to perform the investigation. The DRFW assumes these issues exist.

Analysis

The analysis phase or class is an iterative process. Using the End-to-End Digital Investigation (EEDI) approach that is built on the DRFW framework, the investigators form an initial set of theories that are tested against evidence as it is collected. Some theories will be eliminated and some will remain. Duplicate data is normalized, or eliminated. Data that is reported multiple times from the same source is viewed as a single event. This removes much of the clutter and “noise” from the data set. At this point, a timeline is developed and analyzed.

This process continues as new data is collected, and a chain of evidence is built from corroborated evidence. It is extremely unlikely that an entire chain of evidence can be built from digital evidence alone, so analog data will have to fill in the gaps.

Investigators

Experienced, trained investigators are required regardless of the investigation process model that an organization chooses. An organization may choose to hire a company to perform this function, or if they are large enough, they may want to hire investigators on a full-time basis.

Physical security personnel are often retired military or law enforcement, and have the necessary skills to perform the initial incident response and documentation. They also have the skills to conduct the interviews and traditional investigation.

¹⁰ Carrier, Brian and Dr. Eugene Spafford. 2003. Getting Physical with the Digital Investigative Process. 7.

It is probably easier to teach the traditional investigator to conduct an investigation that involves digital evidence than it is to teach a computer technician to conduct an investigation. As Dr Stephenson wrote, “While, to be sure, there may be a place for the stereotypical scientist in the digital forensic world, that place probably is not in the field conducting routine investigations.”¹¹ The best mix might be to have the traditional investigator conduct the investigation and receive information from the computer forensics technician, much in the same way a police detective works with a crime scene investigator.

Digital Evidence

Not all investigations of computer incidents will go to court, but the investigation should be conducted as if it will. Otherwise, potential evidence will be destroyed or mishandled, rendering it as inadmissible in court. Therefore, a familiarity with the rules of evidence is in order.

Digital evidence must comply with the following standards under the Federal Rules of Evidence to be admissible in a US court of law:

Hearsay: evidence that contains hearsay can be excluded. According to the U.S. Department of Justice (USDOJ) document, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, “The courts generally have admitted computer records upon a showing that the records fall within the business records exception, Fed. R. Evid. 803(6):

Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term “business” as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.”¹²

The USDOJ goes on to make a distinction between computer records generated by humans versus computer-generated records such as log data. Human-generated records are subject to

¹¹ Stephenson, Peter. 2003. “A Comprehensive Approach to Digital Incident Investigation” Elsevier Information Security Technical Report. 4.

¹² USDOJ. 2002. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. 142.

the hearsay rule, while computer-generated records are evaluated based on their truthfulness. “The evidentiary issue is no longer whether a human's out-of-court statement was truthful and accurate (a question of hearsay), but instead whether the computer program that generated the record was functioning properly (a question of authenticity).”¹³

A third type of record exists that combines both human-generated and computer-generated data. This hybrid record type must be evaluated on both hearsay and authenticity standards.

Authentication: as stated in the introduction to this section, digital data is very easy to manipulate and made to look completely different than its original form. Therefore, in the author’s opinion, it is even more critical to establish the authenticity of digital records than it is for analog records. However, the current standard is the same.

“The standard for authenticating computer records is the same for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form. See *United States v. Vela*, 673 F.2d 86, 90 (5th Cir. 1982); *United States v. DeGeorgia*, 420 F.2d 889, 893 n.11 (9th Cir. 1969). But see *United States v. Scholle*, 553 F.2d 1109, 1125 (8th Cir. 1977) (stating in dicta that “the complex nature of computer storage calls for a more comprehensive foundation”). For example, witnesses who testify to the authenticity of computer records need not have special qualifications. The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. See *United States v. Salgado*, 250 F.3d 438, 453 (6th Cir. 2001) (stating that “it is not necessary that the computer programmer testify in order to authenticate computer-generated records”); *United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991) (citing cases). Instead, the witness simply must have first-hand knowledge of the relevant facts to which she testifies. See generally *United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997) (FBI agent who was present when the defendant's computer was seized can authenticate seized files); *United States v. Miller*, 771 F.2d 1219, 1237 (9th Cir. 1985) (telephone company billing supervisor can authenticate phone company records); *Moore*, 923 F.2d at 915 (head of bank's consumer loan department can authenticate computerized loan data).”¹⁴

This leaves challenges to the authenticity of the data¹⁵:

1. **Claim that the data has been altered.** The courts have decided, “The mere possibility of tampering does not affect the authenticity of a computer record.”

¹³ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 143.

¹⁴ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 144.

¹⁵ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 144, 145.

¹⁶Instead, the challenger must have some specific evidence that tampering has occurred. “Absent specific evidence of tampering, allegations that computer records have been altered go to their weight, not their admissibility.”¹⁷

2. **Challenge the reliability of the computer-generated data by challenging the reliability of the computer program.** This challenge appears to have more leeway for the challenger: “If the program’s output is inaccurate, the record may not be “what its proponent claims” according to Fed. R. Evid. 901.”¹⁸ Not all is in the challenger’s favor though, “The courts have indicated that the government can overcome this challenge so long as the government provides sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof.”¹⁹ One of the standard arguments for reliability is that the business relies on it on a daily basis. The argument is, that if it is good enough for the business, then it is reliable.

Challenge the authorship of computer-stored records. The courts do not necessarily take authorship at face value, but require supporting circumstantial evidence to establish authorship. Lacking supporting evidence, evidence can be excluded. For example, “St. Clair v. Johnny’s Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999) (holding that evidence from a webpage could not be authenticated, since information from the Internet is “inherently untrustworthy”).”²⁰

Best Evidence Rule: this rule requires the original record, not a copy (See Fed. R. Evid. 1002). Since a computer record is an invisible (to the naked eye at least) set of binary data on a storage medium, viewing it in another form could be considered not to be the original record. The Federal Rules of Evidence addressed this, “if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an “original”.”²¹

Collecting and Managing Digital Evidence

The purpose of collecting evidence in response to a digital incident is to piece together a picture of what happened, how it happened, and who did it. Throughout the investigative process we will be looking for two types of evidence:

¹⁶ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 145.

¹⁷ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 145.

¹⁸ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 146.

¹⁹ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 146.

²⁰ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 148.

²¹ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 152.

1. “Primary evidence that fits directly in the chain and corroborates other evidence and is itself corroborated directly
2. Secondary evidence whose only purpose is corroboration of other evidence without itself being corroborated.”²²

It is important to note that the investigation will not be a linear process. Evidence will be discovered and new information will be learned, leading to more evidence.

No one knows the whole picture when the incident is discovered, so it is best to collect as much information as is available and sort it out later. Log data is very important to collect because many organizations lack large storage devices for log data, and it is overwritten within weeks or even days. Eyewitness accounts also get stale quickly, so getting their statements as close to the event as possible is critical.

The investigators should collect data from all the devices in the attack path. That includes requesting data from the organization’s Internet Service Provider (ISP), as well as any other vendors that might have pertinent data. Data should be collected from devices that are not known to be targets as well.

Only those who have authorization and training to do so should perform data collection. Unauthorized or untrained first responders should secure the scene and notify the appropriate point of contact for their Computer Incident Response Team (CIRT).

Here is a short list of data that should be collected:

- Document the scene(s) by creating a diagram and taking photographs
- Begin an incident timeline
- Create a list of names of people in the area at or near the time of the incident
- If the devices are powered on, leave them on
- If the devices are connected to a network, disconnect them if it will not severely disrupt business operations
- Trained forensics technicians will make a forensic image of the target device(s). This means a bit copy of the drive(s) and ensures that the hash of both the original and the copy are identical.
- Trained administrators will make a copy of the configuration files of the devices in the suspected attack path, and may possibly make a copy of the output of diagnostic commands such as **show tech-support** on devices running Cisco Internetwork Operating System (IOS). These types of commands capture a large amount of diagnostic data including the memory contents.
- Collect logs from all devices in the attack path
- Collect physical access logs

²² Stephenson, Peter. 2002. Collecting Evidence of a Computer Crime. 2.

The evidence must be managed with a controlled chain of custody. The evidence must be locked and access to it is tightly controlled and logged.

Authenticity of the evidence cannot be challenged simply because tampering is possible, but a poor chain of custody could be grounds to disallow the evidence, or raise doubt with a jury. This is one reason why the original media should never be used for analysis. The bit copy is used to make more copies for analysis purposes.

Expectation to Privacy

The Fourth Amendment to the U.S. Constitution limits the government from searching for evidence without a warrant. The U.S. Supreme Court has decided that a warrantless search does not violate the Fourth Amendment if one of two conditions is satisfied:

1. The government's conduct does not violate a person's reasonable expectation to privacy
2. A warrantless search that does violate a person's reasonable expectation to privacy will be considered reasonable if it meets an established exception to the warrant requirement

In the case of a business investigating a computer incident, the law is generally interpreted as favoring the business as the owner of the computing equipment. As the owner, the business has the right to monitor it and search its property. The employee has no expectation to privacy, especially where policies and banners clearly state that the employer monitors communications.²³

Should the business decide to prosecute, the evidence they collected and present to the government is not subject to the Fourth Amendment. "The Fourth Amendment does not apply to searches conducted by private parties who are not acting as agents of the government."²⁴ However, the government cannot "exceed the scope of the private investigation."²⁵ That does not mean that the government is completely limited because the evidence produced by the private investigation may provide probable cause for the government to obtain a search warrant.

Computer Forensic Tools and Techniques

A critically important aspect of the digital evidence collection process is the computer forensic tools and techniques. Computer forensic tools and techniques have to meet a legal

²³ "Privacy in the Workplace". Berkman Center for Internet and Society. 11/21/2009 <http://cyber.law.harvard.edu/privacy/Module3_Intronew.html>.

²⁴ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 7.

²⁵ USDOJ. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 8.

standard known as the Daubert Test. “The U.S. Supreme Court decision Daubert vs. Merrell Dow Pharmaceuticals, Inc. ...found that evidence or opinion derived from scientific or technical activities must come from methods that are proven to be “scientifically valid” to be admissible in a court of law. ...In the context of digital forensics, this means that the tools and techniques used in the collection and analysis of digital evidence must be validated and proven to meet scientific methods.”²⁶

In other words, if the tools and techniques used to conduct the forensic investigation have not been validated, there is a risk that the evidence will not be admissible. Therefore, an organization should strongly consider the risks if they choose not to use validated tools and techniques when performing computer forensics investigations.

A company may choose to use tools or techniques that have not been validated, but they will have to go through the validation process and a Daubert hearing before their evidence will be admitted. A Daubert hearing takes place before a judge before the actual trial begins. “The Daubert process identifies four general categories that are used as guidelines when assessing a procedure:

- **Testing:** Can and has the procedure been tested?
- **Error Rate:** Is there a known error rate of the procedure?
- **Publication:** Has the procedure been published and subject to peer review?
- **Acceptance:** Is the procedure generally accepted in the relevant scientific community?”²⁷

There are few groups that formally test computer forensic tools. One is the National Institute of Standards and Technology’s (NIST) Computer Forensics Tool Testing (CFTT). According to their website, “A vendor may request testing of a tool, however the steering committee makes the decision about which tools to test.”²⁸ Test results can be found on the National Institute of Justice website:

http://nij.ncjrs.gov/publications/Pub_Search.asp?category=99&searchtype=basic&location=top&PSID=55

Given the uncertainty and cost associated with testing a validating tools and techniques, the recommendation is to use approved methods and tools.

Presenting the Evidence

Digital investigations are complex and involve complex, technical concepts and rules of evidence. Explaining the findings so they are understandable to the organization’s leadership

²⁶ Kanellis, Panagiotis, et al (Ed.). 2006. Digital Crime and Forensic Science in Cyberspace. Hershey, PA: Idea Group. 92.

²⁷ Carrier, Brian. 2002. Open Source Digital Forensics Tools. 3.

²⁸ "CFTT Methodology Overview". CFTT. 11/21/2009
<http://www.cftt.nist.gov/Methodology_Overview.htm>.

or to a judge and jury requires a special skill. The best way to explain the findings is to create a timeline and to describe the events, and place the evidence at appropriate point on the timeline. We should be able to establish:

- “An appropriate evidence chain that traces events from attacker to victim
- Proof that we have collected and managed our evidence appropriately”²⁹

We should also be able to demonstrate that we followed whatever investigative process we chose. For example, we should be able to:³⁰

- Explain how we identified the incident
- Explain our incident response process
- Explain who responded to the incident, when and how
- Explain what was discovered referring to the documentation we created
- Explain how we synchronize our log date-time stamps and demonstrate that the devices were properly configured to use a central time source
- Explain how the evidence was collected and demonstrate that it was properly collected using approved tools and techniques, and that it was collected by authorized and trained personnel
- Explain how the evidence was handled and managed, preserving the chain of custody
- Explain how the evidence was analyzed
- Add non-digital evidence to the timeline, especially where it fills in the digital evidence gaps
- Explain your analysis: paint the picture on how you determined the attack source, the attack destination, and the attack path

Graphs, charts and other visual aids are helpful in communicating complex technical concepts to non-technical people. The use of these is strongly recommended.

The Decision to Prosecute

There are valid reasons why an organization might choose not to prosecute. Perhaps the cost outweighs the perceived benefit. For example, an employee may resign when faced with the evidence of an investigation, while the cost to prosecute would be much more than it is worth to the company. On the other hand, there may be regulatory or compliance reasons that basically force the company to prosecute.

Usually the decision whether to prosecute come down to cost, either financial or to the company’s reputation. A company will probably decide to prosecute when the government is paying the financial cost. For example, in the case of credit card theft, the company can pass

²⁹ Stephenson, Peter. 2002. Using Evidence Effectively. 1

³⁰ Stephenson, Peter. 2002. Using Evidence Effectively. 2-3.

the case and the cost onto the government. However, in a wrongful termination case the company would bear the entire burden and costs.

Presenting in Court

Presenting the results of the investigation in court is much the same as presenting to the organization's leadership. The lawyers, judge and jury are not likely to be knowledgeable about computing systems or digital investigations. The main difference between presenting to an internal organization and presenting in court is the inherent adversarial nature of U.S. courtrooms. The opposing council has two things to try to discredit: the evidence, or the person who collected, analyzed or presents it.

Perhaps the most important advice is to keep things simple and to stay cool under pressure. Dr Stephenson offers this advice for those who will be presenting in court³¹:

- “Be yourself
- Simplify but don't talk down
- Confidence, not arrogance
- Rapport with the judge
 - Achieved when the expert is easily understandable
- Rapport with the jury
 - Achieved through confidence, damaged by arrogance
- Prepare to be challenged
- Stay educated
- Enquire as to opposing expert's background
- Prepare before you testify
- Don't go beyond your area of expertise or into areas where you are weak
- Credibility is essential”

You and your lawyer will need to be a team in the courtroom. It is extremely important that you and the lawyer for your side prepare your testimony well ahead of time. It is important that your lawyer understand the information that you are trying to convey, and your lawyer can help you understand what to expect. Your lawyer can also coach you on your testimony and presentation.

Preparing for Cross Examination

The potential witness should prepare for the tactics lawyers use to help them make their case during cross-examination³²:

³¹ Stephenson, Peter. Computer Forensic Investigation: Week 10 Lecture: Expert Testimony

³² Ball, Craig. Cross Examination of the Computer Forensic Expert.

- Use the Federal Rule of Evidence 702, which states that experts are qualified, “by knowledge, skill, experience, training or education.” The opposing lawyer will try to discredit you based on one or more of those criteria.
- Use the Daubert Test to discredit your findings. For example try to demonstrate that the tool or technique used was not tested or has not been generally accepted
- The opposing lawyer will try to push you to testify to something that is beyond your knowledge. The lawyer will use this to raise doubt with the jury about your other testimony.
- Attempt to show that you are not qualified, made a mistake, made inconsistent statements, use methods or come to conclusions that differ from accepted wisdom, or that you are biased.
- They will attempt to discredit you by demonstrating that you did not follow a process, procedure or checklist
- Opposing council will attempt to discredit you using whatever information they can find on you, including social networks.
- They will look for any embellishments to your qualifications.
- They will look for a lack of education, training or certifications
- They will want to know how much time you spend working on computer forensic tasks

Conclusion

A successful conclusion to a digital investigation, especially one that goes to court, depends on several factors including policies, proper device configuration, log data collection, qualified investigators, qualified computer forensics technicians, validated forensic tools, and gifted presenters. Obviously, this requires a team of highly skilled people, which is why the cost of conducting an investigation is high. Cost is a major reason why a relatively low number of digital incidents are investigated and brought to a court of law. Nevertheless, this report should serve as a good primer for those who want to prepare for the possibility of bringing a computer incident to court.

Appendix A: Recommendations

1. Hire or train people that understand computer attack methods
2. Have a means of detecting and preventing reconnaissance probes and scanning
3. Use Network Time Protocol (NTP) to synchronize log date-time stamps
4. Configure devices to use NTP
5. Collect and monitor device logs
6. Purchase SIEM software
7. Enforce “least privilege” and separation of duties
8. Have a lawyer or investigator on staff or on retainer who understands computer law and rules of evidence
9. Establish policies and procedures for a CIRT
10. Establish a CIRT
11. Train CIRT personnel
12. Establish and conduct incident response awareness training
13. Train or hire investigators
14. Establish an investigation process
15. Establish procedures for each process element or phase
16. Train or hire computer forensics technicians, or have a forensics company on retainer
17. Purchase computer forensics software if the decision is to bring forensics investigation in-house
18. Train and certify computer forensics technicians on the forensic tools
19. Establish security policies stating that the organization owns the computing equipment and will monitor its use
20. Display login banners on computing devices stating that the organization owns the computing equipment and will monitor its use
21. Create an incident timeline with charts, graphs and other visual aids when presenting the results of the investigation
22. Prepare to present testimony in court and to be cross examined

Appendix B: Recommendations by Priority

Priority	Recommendation	Capital Cost
1	Collect and monitor device logs	N/A
1	Use Network Time Protocol (NTP) to synchronize log date-time stamps	N/A
1	Configure devices to use NTP	N/A
1	Establish security policies stating that the organization owns the computing equipment and will monitor its use	N/A
1	Display login banners on computing devices stating that the organization owns the computing equipment and will monitor its use	N/A
1	Enforce “least privilege” and separation of duties	N/A
2	Establish policies and procedures for a CIRT	N/A
2	Establish an investigation process	N/A
2	Establish a CIRT	N/A
2	Train CIRT personnel	N/A
3	Have a means of detecting and preventing reconnaissance probes and scanning	TBD
3	Establish procedures for each process element or phase	N/A
4	Hire or train people that understand computer attack methods	N/A
4	Establish and conduct incident response awareness training	N/A
TBD	Have a lawyer or investigator on staff or on retainer who understands computer law and rules of evidence	N/A
TBD	Train or hire computer forensics technicians, or have a forensics company on retainer	N/A
TBD	Purchase computer forensics software if the decision is to bring forensics investigation in-house	TBD
TBD	Train and certify computer forensics technicians on the forensic tools	N/A
TBD	Purchase SIEM software	TBD
TBD	Create an incident timeline with charts, graphs and other visual aids when presenting the results of the investigation	N/A
TBD	Prepare to present testimony in court and to be cross examined	N/A

TBD = To Be Determined. This recommendation depends on the size, business need, and skill level of the organization.

Capital costs are not operational costs such as salaries and training.

Bibliography

Works Cited

Photo on cover page used with the gracious permission of Thom Gould.

Ball, Craig. Cross Examination of the Computer Forensic Expert.

Carrier, Brian and Dr. Eugene Spafford. (2003). "Getting Physical with the Digital Investigative Process". International Journal of Digital Evidence.

Carrier, Brian. 2002. "Open Source Digital Forensics Tools".

FBI, (2005). "2005 FBI Computer Crime Survey". <http://www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf>

Kanellis, Panagiotis, Evangelos Kiountouzis, and Drakoulis Martakos (Ed.). (2006). "Digital Crime and Forensic Science in Cyberspace". Hershey, PA: Idea Group.

"Privacy in the Workplace". Berkman Center for Internet and Society. 11/21/2009 <http://cyber.law.harvard.edu/privacy/Module3_Intronew.html>.

Stephenson, Peter. (2006). "The Mechanics of Cyber Attacks".

Stephenson, Peter. (2002). "Collecting Evidence of a Computer Crime".

Stephenson, Peter. "A Structured Approach to Incident Post Mortems".

Stephenson, Peter. (2003). "A Comprehensive Approach to Digital Incident Investigation" Elsevier Information Security Technical Report.

Stephenson, Peter. 2002. "Using Evidence Effectively".

Stephenson, Peter. Computer Forensic Investigation: Week 10 Lecture: Expert Testimony

USDOJ. (2002). "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations". 142.

"CFTT Methodology Overview". CFTT. 11/21/2009 <http://www.cftt.nist.gov/Methodology_Overview.htm>.