Global Information Assurance Certification Paper

Legal Aspects of Collecting and Preserving Computer Forensic Evidence

Franklin Witter
GSEC Practical v1.2c
SANS Triangle Park Security Essentials Course
April 20, 2001

Companies are spending millions each year to ensure that their networks and data are properly protected against intrusion. Operating systems are hardened, firewalls are installed, intrusion detection systems are put in place, honeypots are implemented, security policies and procedures are established, security awareness programs are rolled out and systems are monitored. This defense-in-depth approach is used because companies know that people will try to gain unauthorized access to their systems. When unauthorized access does occur, the last line of defense is legal action against the intruder. However, if evidence of an intrusion is not properly handled, it becomes inadmissible in a court of law. It is important to remember one of the basic rules of our legal system: if there is no evidence of a crime, there is no crime in the eyes of the law. Therefore, it is of paramount importance that utmost care is taken in the collection and preservation of evidence.

Some of the most common reasons for improper evidence collection are poorly written policies, lack of an established incident response plan, lack of incident response training, and a broken chain of custody. For the purposes of this paper, the reader should assume that policies have been clearly defined and have been reviewed by legal counsel, an incident response plan is in place, and necessary personnel have been properly trained. The remainder of this paper focuses on the procedure a private organization should follow in collecting computer forensic evidence in order to maintain chain of custody.

Definition

What is a chain of custody? In simple terms, a chain of custody is a roadmap that shows how evidence was collected, analyzed, and preserved in order to be presented as evidence in court. Establishing a clear chain of custody is crucial because electronic evidence can be easily

altered. A clear chain of custody demonstrates that electronic evidence is trustworthy.

In their article, "Top Ten Things To Do When Collecting Forensic Evidence", Joan Feldman and Rodger Kohn state, "Preserving a chain of custody for electronic evidence, at a minimum, requires proving: (a) no information has been added or changed, (b) a complete copy was made, (c) a reliable copying process was used, and (d) all media was secured." Proving this chain is unbroken is a prosecutor's primary tool in authenticating electronic evidence.

Legal Requirements

In order to collect evidence, certain legal requirements must be met. These legal requirements are vast, complex and vary from country to country. However, there are certain requirements that are generally agreed upon within the United States. US Code Title 28, Section 1732 provides that log files are admissible as evidence if they are collected "in the regular course of business." Also, Rule 803(6) of the Federal Rules of Evidence provides that logs, which might otherwise be considered hearsay, are admissible as long as they are collected "in the course of regularly conducted business activity." Robert Ferrell, in his article, "Calling the Cybercops: Law Enforcement and Incident Handling", gives the following summary of these rules, "This means you'd be much safer to log everything all the time and deal with the storage issues, rather than try to turn on logging only after [an incident] is suspected. Not only is this a bit like closing the barn door after the horse has fled, it may render your logs inadmissible in court."

Another factor in the admissibility of log files is the ability to prove that they have not been subject to tampering. Whenever possible, digital signatures should be used to verify log authenticity. Other protective measures include, but are not limited to, storing logs on a dedicated logging server and/or encrypting log files. Log files are often one of the best, if not only, sources of evidence available. Therefore, due diligence should be applied in protecting them.

One other generally accepted requirement of evidence collection is a user's expectation of privacy. A key to establishing that a user has no right to privacy when using corporate networks and/or computer systems is the implementation of a logon banner. CERT Advisory CA-1992-19 suggests the following text be tailored to a corporation's specific needs under the guidance of legal counsel:

> This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
>
> In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.
>
> Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Furthermore, security policy can play a key role in establishing a user's expectation of privacy. The Supreme Court ruling in O'Connor v. Ortega, 480 U.S. 709 (1987), implies that the legality of workplace monitoring depends primarily upon whether employment policies exist that authorize monitoring and whether that policy has been clearly communicated to employees. In order to prove that policy has been communicated, employees should sign a statement indicating that the employee has read, understood and agreed to comply with corporate policy and consents to system monitoring.

Evidence Collection Procedure

When the time arrives to begin collection of evidence, the first rule that must be followed is do not rush. Tensions will probably be high and people will want to find answers as quickly as possible. However, if the investigators rush through these procedures, mistakes will be made and evidence will be lost.

The investigation team will need to bring certain tools with them to the incident site. They will need a copy of their incident handling procedure, an evidence collection notebook, and evidence identification tags. Depending on the type of incident and whether the team will be able to

retrieve an entire system or just the data, they may also need to bring tools to produce reliable copies of electronic evidence including media to use in the copying process. In some cases, legal counsel will want photographs of the system(s) prior to search and seizure. If this is something your legal counsel wants as part of the evidence, then also include a Polaroid camera in the list of tools.

Policy and procedure should indicate who is to act as Incident Coordinator. When an incident is reported, this individual will contact the other members of the response team as outlined in the Incident Response Policy. Upon arrival at the incident site, this individual will be responsible for ensuring that every detail of the incident handling procedure is followed. The Incident Coordinator will also assign team members the various tasks outlined in the incident handling procedure and will serve as the liaison to the legal team, law enforcement officials, management and public relations personnel. Ultimate responsibility for ensuring that evidence is properly collected and preserved and that the chain of custody is properly maintained belongs to the Incident Coordinator.

One team member will be assigned the task of maintaining the evidence notebook. (Please note: a separate notebook should be used for each investigation. Also, the notebook should not be spiral bound. It should be bound in such a way that it is obvious if a page or pages have been removed.) This person will record the who, what, where, when, and how of the investigation process. At a minimum, items to be recorded in the notebook include:

- Who initially reported the suspected incident along with time, date and circumstances surrounding the suspected incident.
- Details of the initial assessment leading to the formal investigation.
- Names of all persons conducting the investigation.
- The case number of the incident.
- Reasons for the investigation.
- A list of all computer systems included in the investigation along with complete system specifications. Also include identification tag numbers assigned to the systems or individual parts of the system.
- Network Diagrams

- Applications running on the computers systems listed above.
- A copy of the policy or policies that relate to accessing and using the systems listed above.
- A list of administrators responsible for the routine maintenance of the system.
- A detailed list of steps used in collecting and analyzing evidence. Specifically this list needs to identify the date and time each task was performed, a description of the task, who performed the task, where the task was performed and the results of the analysis.
- An access control list of who had access to the collected evidence at what date and time.

This notebook is a crucial element in maintaining chain of custody. Therefore, it must be as detailed as possible to assist in maintaining this chain.

Another team member or members will be assigned the task of evidence collection. In order to avoid confusion, the number of people assigned this task should be kept to a minimum. This member or members should also be highly proficient with the copying and analysis tools listed below. This person will tag all evidence and work with the person responsible for the evidence notebook to ensure that this information is properly recorded. This person will also be responsible for making a reliable copy of all data to be used as evidence. This data will include complete copies of drives on compromised or suspect systems as well as all relevant log files. This can either be done on-site or the entire system can be moved to a forensics lab, as needs dictate.

A simple file copy is not sufficient to serve as evidence in the case of compromised or suspect systems. A binary copy of the data is the proper way to preserve evidence. According to Feldman and Kohn:

> A reliable copy process has three critical characteristics. First the process must meet industry standards for quality and reliability. This includes the software used to create the copy and the media on which the copy is made. A good benchmark is whether the software is used and relied on by law enforcement agencies. Second, the copies made must be capable of independent verification. . . Third, the copies must be tamper proof.

The Unix dd command and the product Encase are two examples of acceptable tools. Two copies of the data should be made using an acceptable tool. The original should be placed in a sealed container. One copy will be used for analysis and the other copy can be put back in the system so the system can be returned to service as quickly as possible. (Please note: in certain cases it is necessary to keep the entire system or certain pieces of hardware as part of evidence. The investigation coordinator will work with the legal team to determine requirements for a given case.)

Once all evidence is collected and logged, it can be securely transported to the forensics lab. A detailed description of how data was transported and who was responsible for the transport along with date, time and route should be included in the log. It is required that the evidence be transported under dual control.

Storage and Analysis of Data

The chain of custody must be maintained throughout the analysis process. One of the keys to maintaining the chain is a secure storage location. If the corporation uses access control cards and/or video surveillance in other parts of the building, consider using these devices in the forensics lab. Access control cards for entering and exiting the lab will help verify who had access to the lab at what time. The video cameras will help to determine what they did once they were inside the lab. At a minimum, the lab must provide some form of access control and a log should be kept detailing entrance and exit times of all individuals. It is important that evidence never be left in an unsecured area. If a defense lawyer can show that unauthorized persons had access to the evidence, it could easily be declared inadmissible.

Pieces of evidence should be grouped and stored by case along with the evidence notebook. In an effort to be as thorough as possible, investigators should follow a clearly documented analysis plan. A detailed plan will help to prevent mistakes during analysis that could lead to the evidence becoming inadmissible. As analysis of evidence is performed, investigators must log the details of their actions in the evidence notebook. The following should be included as a minimum:

- The Date and Time of Analysis
- Tools Used in Performing the Analysis
- Detailed Methodology of the Analysis
- Results of the Analysis

Again, the information recorded in the evidence notebook must be as detailed as possible in order to demonstrate the trustworthiness of the evidence. According to David Movius in Section VIII Part D of the "Supplement to Federal Guidelines for Searching and Seizing Computers", "[A] trial lawyer well versed in the technological world who knows how to ask the right questions may find that the 'method or circumstances of preparation indicate lack of trustworthiness,' under Fed. R. Evid. 803(6), to such a degree that a court will sustain, or at least consider, a challenge to the admissibility of the evidence." A properly prepared evidence notebook will help defeat such a challenge.

Once all evidence has been analyzed and all results have been recorded in the evidence notebook, a copy of the notebook should be made and given to the legal team. If the legal team finds sufficient evidence exists to take legal action, it will be important to maintain the chain of custody until the evidence is handed over to the proper legal authorities. Legal officials should provide a receipt detailing all of the items received for entry into evidence.

Conclusions

As stated earlier, the laws surrounding the collection and preservation of evidence are vast and complex. A solid relationship should be established with local law enforcement, as they will be a valuable resource in the evidence collection process. Even if local law enforcement does not have a computer forensics expert on staff, they will know the basic rules of evidence collection and should have contacts within the law enforcement community who are experts in computer forensics.

A clearly documented plan is essential in order for an investigation team to be successful in collecting admissible evidence. The plan should be designed with the assistance of legal counsel and law enforcement agencies in order to ensure compliance with all applicable local, state and federal laws.

Once a plan has been drafted and the incident team is assembled, practice should begin. Configure a test network in a lab environment and invite members of the IT staff to attempt to circumvent the security measures installed in the lab network. Treat the intrusion as an actual incident and follow the incident handling and evidence collection procedures. Review the results with the team and evaluate whether or not evidence collected would be admissible based on the procedures followed and the analysis results. Again, when possible, include legal staff and local law enforcement in these practice sessions.

Finally, when in doubt, hire an expert. If resident security staff members are not equipped to perform the investigation, do not hesitate to bring in outside assistance. It is in the best interest of the company to ensure that the investigation is handled properly. The goal is to collect and preserve evidence in such a way that it will be admissible in a court of law.

References

Banisar, Dave. "EPIC Analysis of New Justice Department Draft Guidelines on Searching and Seizing Computers." January 1995. URL: http://www-swiss.ai.mit.edu/6095/assorted-short-pieces/doj-seizure-guidelines-jan95.txt. (15 Apr. 2001).

Brockman, Belinda. "A Forensic Argument for Network Time Synchronization." Information Security Reading Room. November 20, 2000. URL: http://www.sans.org/infosecFAQ/legal/time_synch.htm (15 Apr. 2001).

CERT Coordination Center. "CERT Advisory CA-1992-19: Keystroke Logging Banner." September 19, 1997. URL: http://www.cert.org/advisories/CA-1992-19.html (15 Apr. 2001).

CERT Coordination Center. "Collect and Protect Information Associated with an Intrusion." CERT Security Improvement Practices. Undated. URL: http://www.cert.org/security-improvement/practices/p048.html (15 Apr. 2001).

CERT Coordination Center. "Establish a Policy and Procedures That Prepare Your Organization to Detect Signs of Intrusion." CERT Security Improvement Practices. October 18, 2000. URL: http://www.cert.org/security-improvement/practices/p090.html (15 Apr 2001).

CERT Coordination Center. "Establish Policies and Procedures for Responding to Intrusions." CERT Security Improvement Practices. Undated. URL: http://www.cert.org/security-improvement/practices/p044.html (15 Apr. 2001).

CERT Coordination Center. "How the FBI Investigates Computer Crime." July 17, 2000. URL: http://www.cert.org/tech_tips/FBI_investigates_crime.html (15 Apr. 2001).

CERT Coordination Center. "Steps for Recovering from a UNIX or NT System Compromise." April 17, 2000. URL: http://www.cert.org/tech_tips/root_compromise.html (15 Apr. 2001).

Feldman, Joan E. & Kohn, Rodger I. "Top Ten Things to do when Collecting Electronic Evidence." Reprinted from The Essentials of Computer Discover Seminar. 1999. URL: http://library.lp.findlaw.com/scripts/getfile.pl?file=/legpub/glass/glass000013.html (17 Apr. 2001).

Ferrell, Robert G. "Calling the CyberCops: Law Enforcement and Incident Handling." April 25, 2000. URL: http://www.securityfocus.com/focus/ih/articles/cybercop.html (17 Apr. 2001).

Kerr, Orin S. "Computer Records and the Federal Rules of Evidence." USA Bulletin. March 2001. URL: http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm (15 Apr. 2001).

McMillan, Jim. "Importance of a Standard Methodology in Computer Forensics." Information Security Reading Room. May 2, 2000. URL: http://www.sans.org/infosecFAQ/incident/methodology.htm (15 Apr. 2001).

Movius, David. "Supplement to Federal Guidelines for Searching and Seizing Computers." Computer Crime and Intellectual Property Section: Criminal Division. May 9, 1999. URL: http://www.usdoj.gov/criminal/cybercrime/supplement/ssgsup.htm. (15 Apr. 2001).

Staggs, Jimmy. "Computer Security and the Law." Information Security Reading Room. December 1, 2000. URL: http://www.sans.org/infosecFAQ/legal/law.htm (15 Apr. 2001).

United States Department of Justice. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." Computer Crime and Intellectual Property Section. January 2001. http://www.usdoj.gov/criminal/cybercrime/searchmanual.htm (15 Apr. 2001).