Global Information Assurance Certification Paper

Computer Forensics

By James J. Dougherty

The basic nature of Internet technology offers criminals many ways to hide their tracks and disguise their crimes. Computer crimes are borderless; the crime can be committed over a modem from next door or from ten thousand miles away, with equally effective outcomes. However, at the same time, technology provides many clues as to the nature of the crime, how it was committed, and who was behind it. In computer forensics, things are not always as they seem. The criminals tend to stay a few steps ahead of law enforcement, and often come up with the most inventive means of protecting themselves and destroying evidence. It is the job of the computer forensics expert to work with law enforcement to preserve evidence, reconstruct crimes, and ensure that the evidence collected is usable in court. Only after extensive analysis is there any hope of finding out who is responsible for computer crimes.

The science of forensics is a highly technical and detailed discipline. Computer forensics experts are hackers in their own right. They have to know the technology inside and out, understand the daily activities of the criminals, forage into a computer used in the commission of a crime, and develop a case that prosecutors can use in court. So much of what occurs on a computer is invisible to the user that special tools are needed to reconstruct data. The computer forensics expert has to possess a wide variety of skills, own or develop a suite of software forensic tools, and maintain the integrity of the chain of evidence according to accepted legal practices.

The forensics examiner's tool kit should contain the tools and techniques to collect and analyze the data. Some of these are tcpdump, Argus, NFR, tcpwrapper, sniffers, nstat, tripwire, and DOS commands diskcopy (version 6.22) with the /v switch turned on and the DD copy command in Unix, and a printer. Lawyers believe that bits are easier to tamper with than paper. In one sensitive case a bitstream copy of the hard drive and a memory dump of the RAM needed to be done by a qualified specialist before examination. The rule needs to be "preserve and then examine."

The tools used by the forensic expert have to be established as working properly and must not alter the data

in any way. The computer forensic community must accept the tools and the results must be repeatable. These same tools are sometimes also used to monitor and audit a network. So, in a way, a good system administrator should provide a staring point for the investigation of the network by providing the installation information about the network and updates as each new application or change was completed, in addition to the backup and log files. This gives the investigators a baseline of the system to work with. Any unauthorized activity can be identified and examined.

Forensics experts can collect only the data specified in the documentation, such as a warrant. Obtaining a warrant can be very tricky. It needs to specify what needs to be looked at and possibly seized. The local authorities can be helpful in this regard. Some police departments have computer crime units, can refer you to the local F.B.I. office, or can call (202) 324-9168 for the F.B.I. computer crime unit in Washington, D.C. If you want to maintain a low profile on the incident until you are sure of what actually took place you can have a local police investigator, if they have computer crime unit, come in as a consultant. Consultants can verify what happened and help specify what needs to be in the warrant as long as the equipment and data involved belong to you or your company.

The methodology of a forensics professional is that of an expert who has a wide range of computer hardware and software expertise. They can identify the intrusion by knowing where to look, what to look for, and what other evidence may be needed. He should gather enough information to decide if law enforcement should be involved. The protection of evidence is crucial. Evidence should not be damaged or altered in the recovery and analysis process. It should also be protected from viruses and mechanical and electromechanical damage. The chain of custody has to be established and maintained. Forensics professionals should also try not to disrupt the business. A checklist of the procedures to follow will accompany the forensics team and be analyzed after the incident is completed to determine what procedures worked and what procedures need to be revised. This should be done as soon as possible after the incident so that details are fresh in the memories of the personnel involved.

A forensics investigation is a very costly procedure, often ranging from $500,000 and higher, so it may be a good

idea to bring in an investigator to determine if there is sufficient evidence to proceed with a full-fledged investigation and possibly a trial.

The first person on the scene may not be a forensics specialist or a system administrator. This is where the security policy determines which procedures are taken. The security policy should be considered a living document; that is, it should be reviewed on a regular basis. A good security policy must start with the CEO and senior management. It should define what an organization looks like from a risk management perspective. It can assist an organization in setting security expectations and outlining the proper procedures for a response should a security incident occur. The security policy should be easy to implement and understand. It should be concise; some experts recommend the document be no more than twenty pages per department. This will make it easier for everyone to read, review, or update. The legal department should review the policy to make sure it is enforceable. If the plan has been written, the individual will know what steps to take to preserve the scene and maintain the chain of evidence. If the company has CERT (Computer Emergency Response Team) they should respond and have written procedures to follow. They should clear everyone away from the affected computer, examine the connections, and observe the screen display. Try to photograph or draw picture of the scene. Do not turn the computer off or disconnect it from the network. It is an ongoing problem whether to disconnect the computer from the network or just turn it off. Perform a normal shutdown, disconnect the modem from the phone line, and do not use the phone. Document and label all connections to the computer. Do not write on the evidence; use a separate note pad, a spiral pad is preferred because these notes can and will be used in court. Write everything down as precisely as possible because it could be six months to a year or more before this goes to court.

Most companies today depend on the IT department to do all the security investigations. Most are not prepared or equipped to handle a proper investigation because they don't have the training to handle and examine evidence. They may change or delete evidence without realizing it. They may disregard password protected or encrypted data. Also, they can destroy a suspect's computer or diskettes without knowing it. They can subject you, your agency and themselves to a huge lawsuit. They lack the credentials to

get the data admitted into evidence. They also lack the expertise to withstand cross-examination by an astute defense attorney.

Proper procedure may include videotaping your arrival on the scene and your entrance into the crime scene to establish what equipment the forensics team brought. This may help stop claims of planting evidence. You should also videotape and document the packing and loading for transport of all the evidence that was seized. This will include the handling of evidence leaving the scene to the transport vehicle and leaving the transport vehicle going into the forensics lab. Unpack and document the evidence, noting any unusual visual details or configurations. Now you have to make a decision as to what to use to image the hard drive. It should be a new media if possible. If not new it should be documented and certified as clean. You would not want to do all this work just to have it thrown out of court because of a technicality. You have to remove the hard drive or drives before proceeding. You don't want to boot the machine you should boot from a floppy to record the time of the CMOS because the examination might be taking place in a different time zone than the computer was seized. The tool you use to image the storage media should only copy not access or change the data in any way. It also should be documented not only who accessed the data, but the date and time and the tool used. After you have made the image, make a copy and place both into a secure area where everyone that handles the evidence has to sign for it and initial the container the evidence is in. It should be an electrostatic container for computer data evidence.

I quote from a study by the Electronic Privacy Information Center (EPIC). "Since 1992 the number of computer crime cases sent to federal prosecutors has tripled, while the number of cases actually prosecuted has remained the same. Of the 419 cases referred to prosecutors, only 83 were prosecuted. The rest were dismissed due to lack of evidence. Even when such cases are prosecuted, they can take more than five years to bring to trial. Part of the reason for this delay is that the evidence collected in computer crime cases is complicated, and prosecutors are ill-prepared to sift through reams of technical data and piece together an iron-clad trail of evidence. At the same time, defense attorneys are quick to challenge the reliability of today's evidence-collection methods." Copies of computer files are now as good as the

original electronic document. Because of this and the strict rules that are applied to forensic examinations, lawyers will need to call upon the expertise of the computer specialist on an ever-increasing basis. They are asking the courts for orders, compelling the production of the original electronic document and all ambient data. This documentary evidence has broadened the horizon for legal discovery. It is an excellent reason for computer experts to be formally trained with recognized training providers and receive a recognized international qualification.

A good investigator typically is easy to talk to and can carry on a conversation with anyone. He also can be very nosy--questioning things and never taking "because" as an answer. He is very precise about everything he does. Logical thinking is an industry trait. Every IT professional has to be a logical thinker to succeed in this business. He has to be objective and unbiased to get the investigation to a conclusion without controversy. He should not lead anyone to his conclusion but rather let them lead him to the proper one. Allegations of bias cast a certain pall over any investigation. He has to have excellent written and verbal skills to write the reports so that everyone understands what happened and what should be done about it. Pay particular attention to leaps of logic that aren't supported by evidence because this may lead to questions about impartiality. He should be able to ask for advice and expertise when it is needed.

Many security professionals have a very difficult time when assigned to investigate a colleague. They find that they are totally unprepared for the personal and professional problems they experience. You should be prepared to remove yourself from any investigation where your personal feelings are involved. You should also be prepared for an investigation to turn into something a lot larger than you first thought. Another personal problem to be aware of is that people who work for a long time in investigation sometimes are accused of being very cynical and suspicious, even with the people they care most about. This can lead to a lot of stress both in the personal and public lives of investigators.

I think of computer forensics as just an extension of good network management. You use a lot of the same tools and investigative skills to solve the same problems. A good system administrator knows his network inside and out so

that any anomalies should be apparent very quickly. A good investigator seeks expertise from other experts in an investigation. According to a recent survey (Dec. 2000) the greatest threats to a computer network are as follows: 68% employees, 17% hackers, 9% competitors, and 6% customers. The conclusion I draw from this is that we have to protect the network from both the inside and outside.

Works Sited

1. Chappell, Michael "Computer Forensics and Litigation Support" 6 Jan 2001. URL:http//www.sinch.com.au/articles/2000/computer_forensics.htm

2. Armstrong,Illena "Computer Forensics 16 Sept. 2000 URL:http//www.scmagazine.com/scmagazine/2000_04/cover/cover.html

3. Mendell,Ronald "Working The Big Computer Crime Case" 24 Oct 2000 URL:httpsecurityportal.com/articles/crime20001019.htm

4. Mendell,Ronald "Computer Crime Investigator's Toolkit" 9 Jan 2000 URL:http//www.securityportal.com/articles/toolkit200010102.htm

5. Rude,Thomas "Evidence Seizure Methodology for Computer Forensics" 6 Jan 2001. URL:http//www.crazytrain.com/seizure.html

6. Betts,Bill "Crime Seen" 3 Sept. 2000 URL:http//www.infosecuritymag.com/march20000/forensics.html

7. Author Unknown "Computer Forensics and Law Enforcement" 28 Dec 2000 URL:http//www.teleport.com/~peterc/law.html

8. Rude,Thomas "DD and Computer Forensics" 28 Dec. 2000 URL:http//www.crazytrain.com/dd.html

9. Morrow,David "The It Security Professional as An Investigator" 3 Sept. 2000
URL:http//www.gocsi.com/sec.pro.htm

10. Ranum,Marcus "Some Tips on Network Forensics" 28 Dec. 2000.
URL:htttp//www.gocsi.com/sometips.htm

11. Sommer,Peter "Computer Forensics an introduction" 28 Dec. 2000
URL:http//www.virtualcity.co.uk/vcaforens.htm

12. Robbins,Judd "An Explanation of Computer Forensics" 28 Dec. 2000
URL:htttp//www.computerforensics.net/forensics.htm