

Computer Forensics: The Need has Arrived

Article

By

Daniel Perez

Salinas Police Department

Command College Class XXXVII

Sacramento, California

October 2005

Computer Forensics: The Need has Arrived

Is Your Department On-Line with Computer Forensic Technology?

Computer forensics, the field of investigating and analyzing evidence that may reside inside computer systems, is growing at such a pace that your local police agency may not be able to keep up with the demand. If local law enforcement cannot recover electronic evidence, who can? Whether it is to identify perpetrators in thefts, fraud, embezzlement or child pornography, every policing agency in the nation needs people on staff with an expertise in computer forensics. Those chiefs and sheriffs who fail to recognize this reality are failing to acknowledge the future of criminal investigations.

With the increasing need for law enforcement personnel with computer forensic expertise, police agencies must find ways to secure this necessary resource. This can be a challenge, especially for smaller agencies that already struggle to meet existing demands for their services. These agencies would be forced to take officers away from the streets or other assignments to complete a demanding training regimen to gain the necessary computer crimes expertise.

“As more criminals utilize technology to achieve their goals and avoid apprehension, there is a developing need for individuals who can analyze and utilize evidence stored on and transmitted using computers”

(Casey, Eoghan, 2001). Many law enforcement agencies are lucky to have one computer expert among their rank and file, often someone who has had the initiative to enhance their hi-tech knowledge more through personal interest than because of crime trends. Although these “experts” may know more than their peers, it does not necessarily mean they have the requisite skills to conduct or assist with crimes committed through automated means.

Computer forensics will have a place in law enforcement investigations units, much like other special assignments such as Persons Crimes, Property Crimes, Sex Crimes, etc. Not every department or organization, however, has the resources to have a trained computer forensics specialist on staff. Even if an agency does not have a member of staff who is qualified to conduct a forensic exam of a seized PC, it is vitally important for any investigator to know the basics of computer seizure and to know where to go for help once high-tech equipment has been seized.

Every crime committed using a computer leaves tracks; you just have to know where to find them. For police purposes, “The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in criminal proceedings” (Heiser, Jay, 2001). As in other criminal investigations, the computer detective must collect and analyze the digital evidence left behind in a digital crime scene. Lacking such a resource, the modern hi-tech criminal

might otherwise elude capture, avoid prosecution and continue to victimize those who otherwise would see justice served as redress for the crimes committed against them.

Today, more people than ever before own personal computers. According to the 2000 census, more than 54 million households in the United States own at least one computer. In 2002, it was estimated that more than 159 million people in the United States have Internet access. Consequently, more potential lawbreakers see opportunities to commit crimes electronically through their own computer and Internet access. There is a “new breed of criminals who use computers to steal money and identities” (Callahan, Rick, 2005). These criminals use computers to commit a wide variety of crimes. With computer equipment becoming more commonplace and affordable, there is no reason to believe this trend will not continue into the foreseeable future. The question is; will law enforcement be able to keep a reasonable pace? The public demands complete and competent investigations and computer forensics will ultimately be seen as an integral part of almost any investigation leading to a successful prosecution.

Cops and Cyber-Criminals

The field of computer forensics is keeping law enforcement and security experts on the trail of cyber criminals. “We’re arming ourselves with software and techniques to catch the bad guys where they work: on their hard drives” (Radcliff, Deborah, 1998). Computer forensic experts dissect hard drives,

diskettes, and other storage media to find evidence of crime or employee misuse. “Computers and other high-tech gadgets have become an indispensable part of many people’s lives, both at work and home. Unfortunately, computers can make it easier for criminals to break the law” (Reeves, Steve, 2005).



Increasingly, investigators are faced with the fact that crime scenes are no more than a computer on someone’s desk. That desktop may hold evidence of peer-to-peer trading of child pornography, it may contain check writer programs to scan, print and forge checks. The computer may contain evidence of identity theft, or it may have been used to launch e-mail scams and conspiracies reaching long distances. It takes a specially trained investigator to know how to look for and recover evidence on a computer hard drive or other storage media. Evidence that might help prosecutors put away a child predator, a forger or an identify thief will go unrecovered without this level of expertise. Sometimes, “Looking for evidence on computers is like trying to find a needle in a haystack. Incriminating data can reside in snippets on swap files, in slack and unallocated

space, or even in bad clusters or boot sectors” (Radcliff, Deborah, 1998). Computer forensics, much like traditional criminal investigation training, is designed to help investigators follow the basic rules of evidence recovery that would hold up to scrutiny in a court of law.

The Work of the Computer Detective

Computer forensics experts use a variety of methods for locating data that may exist in a computer system. Most commonly, computer detectives work from a mirror copy of the suspect’s hard drive, which includes all data hidden in ambient space and “slack space.” Slack space is generated by the computer between various files. It is the remnant area at the end of a file, in the last assigned disk cluster, that is unused by current file data. Slack space may be a possible site for previously created and relevant evidence. The original drive remains unchanged and is preserved for evidence in its original condition. This is done to preserve the original evidence in the event that further examination is required or a completely new and independent exam is needed. The suspect media is copied onto clean media; another hard drive, zip drive or CD-ROM, then the forensic recovery process can begin.

Computer forensic software analyzes all possibly relevant data found in special (and typically inaccessible) areas of a disk. This includes but is not limited to what is called ‘unallocated’ space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence). “Computer specialists can draw on an array of

methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information” (Robbins, Judd, 2004).

No matter what method the computer forensic detective may use, there are core requirements that must be met for each and every case. To look inside a computer crime investigation, one would see the high-tech methods mixed with good old-fashioned policing and a lot of common sense in an electronic setting. “This is a living process that must allow for changes and updates, as well as flexibility and room for decision making on the part of the media analyst to fit particular requirements of each case” (Pueblo High-Tech Crimes Unit, 2004).

Increasingly, criminals are raiding corporate servers, electronically transferring intellectual property, committing frauds or monetary solicitations or harassing employees via e-mail. “They’re using PC’s and Macs to commit felonies such as embezzlement, drug trafficking, money laundering, or distributing child pornography” (Radcliff, Deborah, 1998). Some other conventional examples of law enforcement investigations that would use computer forensics include, fraud, forgery, counterfeiting, stalking, sexual harassment, arson and homicide. Fortunately for investigators, these and all other computer crimes leave evidence. “Far more information is retained on a computer than most people realize. Computer forensics can often find evidence of, or even completely recover, lost or deleted information, even if it was intentionally deleted”

(Berryhill Computer Forensics, 2004). Fortunately for investigators, the technology for recovering that deleted information continues to improve.

Hackers, Terrorists and Encryption – Tools of the Trade

In the field of homeland security, computer forensics is an invaluable tool. Planning for international and domestic terrorism is often conducted on computers via the World-Wide Web (the www...in your website name). The interception and recovery of electronic communications is an essential defense element of the war on terror. Electronic mail is a common means of communications for terrorists and other outlaw groups. With the Internet and networks as vast as they are today, cases involving computers and other electronic devices are borderless. With all the wireless and peripherals out there, (in 2003 there was estimated to be 158.722 million cellular phones in use in the U.S. alone), evidence may be spread over numerous locations. These types of investigations may involve multiple jurisdictions and investigators. “The proliferation of handheld devices connected to wireless networks has ushered in an era of pervasive computing. One of the most significant challenges of investigating criminal activity in the context of pervasive computing is obtaining all the evidence” (Casey, Eoghan 2001).

Just as high-tech cops, agents, and corporate security folks get smarter; hackers will challenge them with new tricks. Being able to find hidden data is a crucial investigative skill, and a necessary component to any successful

computer crime prosecution. “A child pornographer might be adept at hiding photographs disguised as normal text documents” (Reeves, Steve, 2005). One of the latest hacker tricks is called steganography. Steganography is the art of hiding information by embedding covert messages within other messages such as “gif.” and other types of image files, making the data very difficult to recognize and locate. Being aware that steganography exists can help the investigator to explore other forensic options, if primary examinations fail to turn up evidence they know to exist on that storage media.

Criminals may also use cryptography, the process of converting information to a disguised form in order to send it across a potentially open or unsafe channel. Traditionally used by governments during times of war to prevent enemies from learning tactics, cryptography has become one of the main tools for privacy, trust, access control, electronic payments and corporate security in today’s wireless world. The use of cryptography is no longer a privilege reserved for governments and highly skilled specialists, but is readily available for anyone skilled enough to Google the term in their PC’s search engine and pay for one of several encryption programs. A skilled investigator must have a solid understanding of the technology and goals of modern cryptography to uncover evidence to crimes and successfully prosecute cyber-criminals.

The High Tech Investigation - New Tools, New Partners

Computer forensic investigations share many characteristics with most other professional investigative practices and techniques. For example, protecting the integrity of the electronic “crime scene” is paramount. “If there is a computer on the premises of a crime scene, the chances are very good that there is valuable evidence on that computer” (Berryhill Computer Forensics, 2004). Protection of evidence is critical. A knowledgeable computer forensics professional will ensure that a subject computer system is carefully handled to ensure that no possible computer virus is introduced to a subject computer during the analysis process, and a continuing chain of custody is established and maintained” (Robbins, Judd, 2004). Law enforcement and other public safety agencies are increasingly partnering with universities to combat computer crime. These partnerships focus not only on education, but also on certification of forensic training and methodology, forensic software, hardware development and research projects. They can also assist in the development of standards and protocols for investigators.

Examples of research projects that help computer forensics experts are those that develop techniques for profiling the behavior of offenders based on their computer-use habits. The goal of this type of research is to study the human-computer interaction and query level of Web search behavior. “Web search context can be examined at many levels, including: the information environment/social level, organizational level, information seeking level, human-computer interaction level and query

level” (Spink, A., 2004). This information becomes useful because in many instances, more than one person has access to a computer. If this research can help develop user profiles, those profiles can help determine whom the suspect may be if access is an issue. For example, Internet activity that appears threatening may fit the profile of a terrorist or a teen-ager.



The Impact on Your Pocketbook

Theft of intellectual property is costing U.S. businesses more than \$250 billion annually, according the American Society of Industrial Security (ASIS), in Alexandria, Virginia. “Part of the problem is you’re dealing with a more knowledgeable criminal, and electronically speaking, the bad guys are usually one step ahead of the law” (Radcliff, Deborah, 1998). The FBI estimates that more than 80 percent of computer crime goes unreported, often because business leaders think law enforcement agencies will lack the resources and expertise to effectively

combat it. Although the threat of cyberterrorism exists, some believe the greatest risks to Internet communication, commerce and security is from cyber-crime motivated by profit. According to FBI estimates, “cyber crime costs businesses and the government more than \$10 billion a year, with computer-aided identity theft costing individuals and businesses an additional \$1 billion each year” (Callahan, Rick, 2005).

Identity theft is becoming one of the more common offenses reported to law enforcement. “Identity theft has cost consumers, finance and credit card companies about \$11.7 billion in one year up to April 2004” (Chin, Rosalind, 2005). If the mission of policing is to protect the public and bring justice to those victimized by crime, can we succeed unless we are capable of creating the sense of confidence necessary in our community to allow us to patrol our cyber-community as well as the streets of our cities?

Seventy percent of organizations surveyed by CSO magazine, a publication for security executives, reported at least one crime or attack during 2003. The estimated damage from these crimes is believed to be \$666 million. “Forty-three percent of the organizations reported they had more intrusions in 2003 than during the previous year” (Coren, Michael, 2005). Computers have always been susceptible to unwanted intrusions. As the sophistication of computer technology increases so does the need to predict, and safeguard against the corresponding rise in computer related crime. Billions of dollars are lost annually to crime, and

computers are increasingly involved. “Bad things are happening on computers and to computers, and the organizations responsible for these computers have a need to find out what exactly happened” (Heiser, Jay, 2001).



Industrial Espionage - from Company Secrets to Personnel Records

As computers become more prevalent in businesses, employers must safeguard critical business information. “An unfortunate concern today is the possibility that data could be damaged, destroyed or misappropriated by a discontented individual” (Berryhill Computer Forensics, 2004). For instance, before an individual is informed of their termination, a computer forensic specialist would come on-site and create an exact duplicate of the data on the individual’s computer. In this way, should the employee choose to do anything to that data before leaving, the employer is protected.

Damaged or deleted data can be replaced, and evidence can be recovered to show what occurred. This method can

also be used to bolster an employer's case showing the removal of proprietary information, or to protect the employer from false charges made by the employee. "Computer forensic tools and procedures are also used to identify computer security weaknesses and the leakage of sensitive computer data" (New Technologies, Inc., 2004).

Computers can contain evidence in many types of human resources proceedings, including sexual harassment suits, allegations of discrimination, wrongful termination claims, and others. Evidence can be found in electronic mail systems, on network servers, and on individual employee's computers. However, due to the ease with which computer data can be manipulated, if the search and analysis is not performed by a trained computer forensics specialist, it could likely be thrown out of court. Corporations often hire computer forensic specialists to ascertain evidence relating to embezzlement, theft, or misappropriation of trade secrets and other internal confidential information. Private individuals sometimes hire computer forensic specialists in support of possible claims of wrongful termination, sexual harassment, or discrimination. Civil litigators use computer evidence for fraud, divorce, discrimination, and harassment cases. Insurance companies need it to mitigate costs on insurance fraud, accident, and worker's compensation cases.

Conclusion

It is evident that both the public and private sectors are increasing their use of computer forensics to combat

crime, protect company secrets and ensure the integrity of financial records. The uses for computer forensic technology are vast and experts believe this trend will continue. Computer forensics specialists are in short supply and high demand, especially in policing. Law enforcement agencies will no doubt have an increasing need for computer forensic technology and those with the expertise to apply it. Computer forensics is fast becoming a basic component of an increasing number of criminal investigations. Small to midsize police agencies will have no choice but to keep up with the needs of the communities they serve. That service will have to include the ability to provide computer forensics as a component of their major investigations.



After seizing computer evidence, many police agencies must rely on resources outside their agencies to process that evidence due to a lack of expertise in their own ranks. The wait for such a forensic review can be many weeks to months, an unacceptable delay in a world where millions can be transferred by the click of a mouse. Law enforcement will undoubtedly have an

increasing need for computer forensics technology and experts in the field who know how to apply them. Where will police agencies get the computer forensic expertise to meet their future investigative needs? Many small to medium size agencies currently designate one or more investigators to receive computer forensic training and serve as the department resource. A more common alternative chosen by numerous police agencies is to rely on Regional Computer Forensic Labs (county, regional, state).

In spite of regionalization, even the best-equipped and supported agencies will sometimes experience high caseloads or exceptional investigation requirements that may overwhelm their resources. In such circumstances, policing may be forced to look externally for solutions. This may require contracting out for computer forensic services through private

companies. Does the private sector have the capacity, or the interest, to tackle this issue? With readily available services such as forensic software, training, and technical support, perhaps cops should knowledge the reality of the emerging landscape and contract for help.

If the current computer crime trends continue, many more in the United States may become victims of cyber-crime. Preparing your agency to use available computer forensics expertise to investigate these crimes is critical. As a result, your agency will be able to respond quickly to victims and offer an invaluable and timely service to the community. Police executives should search for the best and brightest investigators in their agencies, and then equip them to aid in the resolution of this proliferating crime trend. Remember, it may only be a matter of time until you become a victim. How would you want the police to act?

WORKS CITED

Berryhill Computer Forensics, LLC. "Computer Forensics in Law Enforcement." [On-line]. Available: <http://www.computerforensics.com/lawenforce.htm>

Brantley, A.C. Gangs: A National Perspective F.B.I. Law Enforcement Bulletin, May 1994, Vol. 63, No. 5. pgs. 1-6.

Business Wire. "Computer Forensics International Helps Inkjet Win Court Case." Dallas: Business Wire [On-line], August 25, 2004.

Callahan, Rick (Associated Press). "Officers Schooled to Handle Evidence in Cyberworld Crimes." [On-line]. Available: <http://www.fortwayne.com/news/local.html>

- Casey, Eoghan. (2001). Handbook of Computer Crime Investigation: Forensic Tools and Technology. New York, New York: Penguin Books
- Chin, Rosalind. (CNN). "ID Theft Joins List of Travel Scams." [On-line]. Available: <http://www.cnn.com/2005/Travel/06/27/bf.id.fraud/index.html>
- Coren, Michael. (CNN). "Experts: Cyber-crime Bigger Threat than Cyber-Terror." [On-line]. Available: <http://www.cnn.com/2005/tech/internet/01/18/cyber.security/index.html>
- Heiser, Jay G. (2001). Computer Forensics: Incident Response Essentials. New Jersey: Prentice Hall.
- International Association of Computer Investigative Specialists, The. "Forensic Procedures." [On-line]. Available: <http://www.cops.org/htmlforensicprocedures.htm>
- New Technologies, Inc. "Computer Forensics Defined." [On-line]. Available: <http://www.forensics-intl.com/def4.html>
- Pueblo High-Tech Crimes Unit, The. "Computer Forensics Processing Checklist." [On-line]. Available: <http://www.crimes-research.org/library/forensics.htm>
- Radcliff, Deborah. "Crime in the 21st Century." [On-line]. Available: <http://www.infoworld.com/cgi-bin/displaystory.981214crime.htm>
- Reeves, Steve. Cyber Detectives Put Criminals On Notice. [On-line]. Available: <http://www.charleston.net/cgi-bin/printme.pl>
- Robbins, Judd. "An Explanation of Computer Forensics." [On-line]. Available: <http://www.computerforensics.net/forensics.html>
- Spink, A., & Jansen, B.J. (2004). "A Study of Web Search Trends." *Webology*, 1(2) Article 4. [On-line]. Available: <http://www.webology.ir/2004/v1n2/a4.html>
- Tobias, Zachary. Getting Started in Computer Forensics, Computerworld Magazine [On-line], July 9, 2001.