Law Enforcement Challenges in Digital Forensics

NCISSE 2002 General Track

Prepared by Gal Shpantzer and Ted Ipsen, CISSP with generous contributions by DetectiveGreg Roberts, CISSP

Speaker and contact for correspondence:

Gal Shpantzer
5021 Vernon Ave #174
Edina, MN 55436
Email: gal@visi.com
V-mail: (612) 701 3159

Abstract

Abstract: This paper presents an overview of pressing issues in use of forensic science in the context of high-technology crime investigations, often called computer forensics or digital forensics. It also highlights several existing training programs in computer forensics and attempts a crude estimate of capacity for training in computer forensics.

Law enforcement faces many significant challenges in developing and mastering the skills, tools and techniques of digital forensics. Finding qualified forensics personnel is difficult in the private sector, partly because of the restrictions placed on civilian access to training programs. In law enforcement, additional difficulties arise due to a multitude of structural and cultural factors in that closed community. Even in those cases where trained personnel are available, there may be impediments to successful prosecution, such as the lack of adequate equipment and facilities to process digital evidence, or prosecutorial unfamiliarity with the issues surrounding the seizure and processing of such evidence.

Agencies must tackle these challenges in order to develop digital forensics into a mature and rigorous science, like its peers in other forensic specialties. They must also be willing to dedicate resources to digital forensics in a manner that facilitates the development of specialized personnel who handle this particular type of evidence.

What is Forensic Science?

Forensic science involves the “collection, preservation and validation of evidence” as well as the “investigation and analysis of the data, and the preparation of a report for the authorities.”
(SANS GIAC Forensics track description)

What is *digital* forensics?

(not just desktops and servers)

"*Digital evidence is any information of probative value that is either stored or transmitted in a binary form. This field includes not only computers in the traditional sense but also includes digital audio and video.*"

National Center for Forensic Science at the University of Central Florida

Typology of Digital Crime

- Mark and Mike Menz from HTCIA of California created a classification system for digital crime. Some of the major categories are:
- Computers as targets of crime
- Computers as an instrument of crime
- Computers as an incidental peripheral to a crime
- (expand on this)

Why is digital forensics so important?

As we have seen in Menz' classification, there is a wide variety of digital crime, and we can only expect to see more as society becomes ever more reliant on networked systems. The following are only two documented examples of network-based attacks on critical infrastructure. If ordinary citizens can wreak havoc with infrastructure, what could trained terrorists do?

Teenager hacks airport

- In 1997, a teenager in Massachusetts, using his home computer, shut down Worcester, Mass. Airport and a neighboring small town for six hours.
- Emergency communications nets,landing light control and other services were unavailable.

Angry at being fired, man hacks sewage control system

- March 2000, Australia
- Dumped tons of raw sewage into an environmentally sensitive and economically important “Sunshine Coast” tourist area.

- http://www.newsbytes.com/news/01/171730.html

Cyber attacks on infrastructure: Not just theoretical threat

- Fortunately, this has been successfully demonstrated in only a few instances.
- Law enforcement must be able to investigate and bring to justice people who perpetrate digital crime just as they do in the violent crime or white collar crime arenas. This is especially important in a cyber-terrorism scenario.

Other forensic disciplines are highly developed: What about computer crimes?

- The United States has amazing capabilities to investigate and prosecute all kind of terror-related crimes, partly because of rigorous programs in forensic sciences, able to secure and analyze evidence from such crimes as bombings, poisonings, arsons and shootings.
- What about computer crimes?

Research into digital forensics is crucial

- What are some of the problems that must be tackled in order to expand digital forensics capabilities?
- What are some of the existing training programs?
- What is the capacity for training law enforcement personnel?

Challenges in Law Enforcement Forensics

"A forensics expert must have the investigative skills of a detective, the legal skills of a lawyer, and the computing skills of the criminal." "A forensics expert must have the investigative skills of a detective, the legal skills of a lawyer, and the computing skills of the criminal."

IEEE Institute article, Oct.01

Proof of Scientific Rigor

- Juries, judges, and prosecutors must have confidence in tools and techniques used in digital crime cases. Digital forensics tools and techniques must go through a lengthy process of establishing legitimacy in the courtroom, as other forensic tools had to. These days, DNA evidence, for example, is routinely accepted as powerful and convincing evidence, but this was not always so.

Esoteric Nature of Digital Evidence

- Related to the confidence in tools and techniques is the fact that in order to believe in the evidence, one must first understand it at some level. Digital forensics can be challenging to even technically proficient computer professionals. The technical nature of the evidence and the methods used to collect and preserve it creates an inherent challenge in convincing the various participants in the criminal prosecution process that the evidence is not tainted in any way.

Volatility of Evidence

Digital evidence, by its very nature, is extremely susceptible to damage or destruction by a well meaning investigator during the process of seizure or in subsequent investigation.

Lack of qualified personnel

- Senior agent in federal agency divulged that competition for computer forensics specialists in law enforcement is fierce.
- Agencies often resort to ‘stealing’ personnel from other agencies, especially at the local and state levels.

Lack of qualified personnel (cont)

- Qualified forensics experts are difficult enough to find in the private sector. In the law enforcement arena, the problem compounds.
- Low compensation relative to private sector, and lucrative offers outside of law enforcement are very difficult to resist for all but the most dedicated.

Lack of qualified personnel (cont)

- Even if technically proficient specialists are available, how many of them are trained to deliver convincing, scientifically valid expert-witness testimony?
- How many can perform in the lab *and* in the courtroom, under pressure of cross-examination? Standards and certifications must be established for expert witnesses.

Jurisdiction and related issues

- Who's in charge in a cyber attack from across state lines, or from abroad? FBI? Secret Service? It depends…
- Turf wars between agencies are often the norm rather than the exception. Competition for personnel, facilities, budgets and prestige aggravate the situation, driving a lack of inter-agency, or even intra-agency cooperation.

Admissibility of Tools and Techniques

- Even if the evidence was seized, collected and analyzed in a technically correct manner, the prosecution must still defend the constitutionality of the methods used to obtain the evidence. Picking locks and installing sound and video surveillance is already understood and accepted. What about methods to bypass encryption and other less-proven technical surveillance issues?

Magic Lantern

One example is the case of the FBI's Magic Lantern program, officially acknowledged in the fall of 2001. Magic Lantern is a keystroke logger, surreptitiously installed on a computer in order to defeat a file encryption program (PGP). This is done by obtaining the passphrase to decrypt the files. The computer belonged to alleged organized crime figure Nicodemo Scarfo.

Scarfo's prosecution had heavy cost to FBI's surveillance capabilities

- Scarfo's defense team mounted a lengthy legal challenge to the admissibility of evidence obtained using Magic Lantern. This case destroyed the covert nature of the Magic Lantern program, as the FBI lost its bid to suppress the details of how the evidence was obtained. For full coverage, see http://www.epic.org/crypto/scarfo.html

Cycle-time as a Weapon

Crackers, malicious code writers and other criminals can take advantage of a tremendous number and variety of tools and devices. They don't have to prove their tools in court or defend constitutional challenges like law enforcement agencies do, so there is an inherent problem in keeping up with the black-hats, who routinely share information and cooperate. By the time a DDoS or mass-mailer virus is detected and analyzed, not to mention issued a patch or signature, the black hats are already working on the next project.

Cycle time (continued)

- The problem of cycle-time also applies to the multitude of new devices, operating systems, applications and protocols. Windows experts must know Windows 95, 98, Millennium, NT, etc. What about the different flavors of Unix, and of course the Macintosh? New wireless protocols such as 802.11a/b and Bluetooth present tremendous technical difficulties to forensics researchers. Most recently, the advent of virtual machines (VMWare) has created an additional level of difficulty. (HTCIA.org Dec. 2001 newsletter)

Professional tools, training and facilities can be prohibitively expensive

Tools like EnCase from Guidance Software significantly automate the process of collecting data from a hard drive, but many agencies cannot afford the cost of the software and the training to use it correctly. This leaves them to use free, manual tools to extract evidence. As one investigator told us:

"*For those that don't think they can afford a program like EnCase and are doing it with manual tools, God help them when they have to explain to Johnny Cochran how the(expletive deleted) thing works!*"

Law Enforcement Career Track: Not conducive to long term specialization

- Whereas most forensic examiners are career scientists, law enforcement personnel that work in digital forensics are often unable to develop and mature as specialists.
- Some obstacles to continuous development and maturation process of specialists include rotation in duties (back to patrol, etc) and geographic location.

Law Enforcement Career Track: Not conducive to long term specialization

Since sworn personnel are often subject to rotation out of specialized units, taking their training and experience with them. The staffing of specialty units within a law enforcement agency is often subject to the whim of the executive in the governing body for that political term. And, in the ever present battle over resources to respond to calls for primary service, officers will always be reallocated to patrol cars and foot beats, to the detriment of special investigative units with little public visibility.

You've been trained
to handle this.

What about this?

Image courtesy of
Computerforensics.com

Training programs in Digital Forensics

- In order to estimate the capacity for training digital forensics specialists, we have assembled several programs and examined them for level of sophistication as well as numerical output of students per year. Adding up the individual estimates will give us a crude overall estimate of the number of specialists that can be trained per year.

National White Collar Crime Center (NW3C)

- www.cybercrime.com
- Data Recovery and Analysis Course
- Basic and Advanced Levels
- Estimated about 1,300 people yearly capacity for both levels combined, with about 1,000 people in the basic level.

University of Central Florida

- Post-baccalaureate certificate program hosted at UCF, created by National Center for Forensic Science at the National Institute of Justice.
- Five graduate level courses mixing technical system and network science with ‘softer’ side of forensics such as courtroom testimony and other legal issues.
- www.cs.ucf.edu/csdept/info/gccf/admisReq.htm

SANS Institute's GIAC Certification in Forensics

- www.giac.org
- Five day seminar on Unix and Windows operating systems, and covers legal and technical issues in forensics.
- Unique aspect of GIAC course is the live demonstration of a forensic analysis of a compromised system from the Honeynet Project.
- http://project.honeynet.org/

  Only offered two or three times a year and is only about a year old. Estimate of 300 – 400 people capacity.

IACIS

- http://www.cops.org/training.htm
- International Association of Computer Investigative Specialists
- Offers multi-course training program as well as individual courses. Some courses are vendor specific, such as Guidance Software's Encase or Paraben's palmtop handheld forensics applications.

IACIS (cont.)

- Courses on UNIX and Windows, as well as network forensics.
- Certifications include the two week long training course to become a Certified Electronic Evidence Collection Specialist (CEECS) and further training beyond that may result in a designation of Certified Forensic Computer Examiner (CFCE).

IPTM

- Institute of Police Technology and Management www.iptm.org
- Has an introductory level five-day course entitled Computer Investigations, focusing on Windows. Course includes topics from hard drive imaging to court testimony and establishing a dedicated computer forensics unit.
- Estimated capacity is about 100 people at the basic level, based on three trainings in 2002 calendar, assuming 30 people per course.

Guidance Software (Encase)

- www.encase.com
- Encase is the leading software package in the forensics world. This vendor provides dozens of courses every year at the basic, intermediate and advanced levels.
- Estimated 2,000 attendees per year for all levels. This does not translate to 2,000 unique individuals, as the higher level courses have the basic as a prerequisite, but this vendor is a significant contributor to the corps of forensic specialists.

SEARCH

A program of the Dept. of Justice, SEARCH provides training courses on Seizure and Examination of Microcomputers, as well as Investigation of Computer Crime. There are over a dozen scheduled dates over a one year period, so this suggests that there is a capacity to train several hundred people in these topics.

This list is not exhaustive

- The training programs above are open only to law enforcement, with the exception of the SANS training, which is open to all. The FBI, Secret Service, and other federal law enforcement, intelligence and military agencies may have their own exclusive programs, and these are not considered in the above list.

Some Resources From Federal Law Enforcement Websites

- Some resources for learning more about the federal agencies' forensics programs are the United States Secret Service site, and the FLETC site.
- www.treas.gov/usss/ (Electronic Crimes Branch) This site also has an excellent guide on correct seizure practices for digital evidence, called 'Best Practices for Seizing Electronic Evidence'
- www.fletc.gov and http://www.fletc.gov/tmd/cotp.pdf (Financial Fraud Institute)

Location, Location, Location

- Most of the trainings offered are in California or D.C. area. Obviously there is a need for ‘road show’ type trainings that travel the country and serve the rest of the country. This would greatly enhance the ability of smaller agencies to acquire the skills to perform digital forensics work..
- One example is the National White Collar Crime Center’s program, with trainings all over the country, including areas with no major city nearby, such as Branson, Missouri and Meridian, Mississippi.

Training first, then a place to put skills to work

While forensics software vendors and other entities that provide training can provide an acceptable capacity for training, actual investigations necessitate laboratories, specialized evidence storage locations and other such facilities in order to bring about successful investigations and prosecutions. A holistic approach to digital crime must be undertaken and should include training and facilities for both the investigator and the prosecutor.

Conclusion

Our initial estimates (more detail and methods coming during next few weeks) lead us to believe that there exists a capacity to train at least three to five thousand new digital forensics personnel on a yearly basis. Some of these obviously include people outside of law enforcement, such as some of the SANS or EnCase training volunteers, but the majority of the training opportunities do not allow civilian access, so the bulk of the trainees are sworn personnel.

Government, Academia and Industry

As described in the training section, partnerships and cooperative efforts between government, academia and industry are already bearing fruit in this critical field, providing much needed training opportunities. They must be continually assessed for relevance, timeliness and productivity in terms of providing digital crime investigators and prosecutors with the tools, techniques and skills they need to perform their critical mission.

Government, Academia and Industry

As our nation has been thrust into a harsh new reality of its vulnerability, we struggle to shore up our law enforcement capabilities to respond to new threats. The sworn community needs relevant and timely training in digital forensics, and both academia and industry would do well to cater to this demand.