Hassel Stacy Jr.
Dr. Philip Lunsford
ICTN4040 601
04/16/06

Computer Forensics For Law Enforcement

The Internet, data systems and growing computer networks provide many opportunities for computer crimes. Computers are increasingly used to commit, enable or support crimes perpetrated against business, people and property. Computers can be used to commit the crime, may contain evidence from a crime and could be targets of crime. Understanding the role and nature of evidence that might be found, how to process a crime scene containing potential forensic evidence, and how an agency might respond to such experiences of the law enforcement community, the public sector, and the private sector in the recognition, collection and preservation of computer forensic evidence in a variety of crime scenes will be defined in the following paragraphs.

A phrase often heard in computer technology is "computer forensics". Computer forensics is process of collecting, analyzing and preserving computer related data. I am going to examine computer forensics for law enforcement. I will provide the reader with a better understanding of computer forensics, I will reference specific laws dealing with cybercrime. Finally, I will discuss the tools and techniques to gather evidence from a cybercrime.

The are many laws which deal with cybercrime and provide precedence for law enforcement personnel. The Computer Fraud and Abuse Act of 1986 (as amended in 1994 and 1996) makes it illegal to knowingly access a computer without authorization or exceeding authorized access, and to intentionally, without authorization, access any nonpublic computer of a department or agency of the Government of the United States. The US Patriot Act of 2001 modified a wide range of existing laws to provide law enforcement with broader control in order to combat terrorism. These laws provide stiff penalities of up to 20 years in prison. There are many types of cybercrime. Some examples are:

online auction fraud, child exploitation/abuse, computer intrusion, death investigation, domestic violence, economic fraud such as online fraud and counterfeiting, email threats/harassment/stalking, extortion, online gambling, identity theft, narcotics, prostitution, software piracy and telecommunication fraud.

Many of these crimes don't go to trial, especially those in business areas, where computer forensic evidence often evokes out of court settlements. Another reason these crimes may not go to trial would be "tainting" of forensic evidence. If a computer involved in a crime and its contents are examined by anyone other than a trained and experienced computer forensics specialist, the usefulness and credibility of that evidence will be compromised. Always follow this rule if you suspect you network has been breached and a cybercrime has been committed: If the suspect computer or computers are off, leave them off, if they are on, leave them on. Contact your local law enforcement agency. The agency will send and officer and if deemed necessary a trained computer forensic examiner.

The examiner will use special tools and follow certain evidence collection procedures. The forensic examiner's tools usually include operating system utilities (for backups, disk manipulation, string searches, etc.), data recovery software (to thwart file deletion attempts) file viewers and Hex editors (to perform Win/Mac data conversion and reveal information contents and patterns) and commercial firewalls (for network sniffing and port scanning during investigations). There are also packages which provide assistance for forensic examinations, complete with case management tracking for procedures, reports and billing. These useful forensic products can be can be obtained from Danny Mares and Company @ www.dmares.com/maresware/linksto_forensic_tools.htm, from Computer Crime Research Center and from University of Western Sidney's School of Computing and Information Technology

Most law enforcement departments use the following criteria when collecting evidence from a cybercrime. There should be access to tools and equipment necessary to document, disconnect, remove, package, and transport digital evidence. Preparations should be made to acquire the equipment needed to collect forensic evidence. Actions taken to secure and collect computer forensic evidence should not change the evidence. Persons conducting the examination of electronic evidence should be trained for the purpose. Activity relating to the seizure, examination, storage, or transfer of electronic evidence should be fully documented, preserved, and available for review.

What is digital evidence? Digital evidence is information and data of investigative value that is stored on or transmitted by an electronic device. Such evidence is acquired when data or physical items are collected and stored for examination purposes. Computer forensic evidence is often latent in the same sense as fingerprints or DNA evidence. It can cross borders with ease and speed, is fragile an and can be easily altered, damaged, or destroyed, it is sometimes time sensitive. User created files, on computers involved in computer forensic investigations, may contain important evidence of criminal activity such as address books and database files that prove criminal association, still or moving pictures that may be evidence of pedophile activity, and communications between criminals such as email or letters. Other files which may contain useful forensic evidence are address books, audio/video files, calendars, database files, documents or text files, email files, image/graphic files, Internet bookmarks/favorites, and spreadsheets. Some other useful information might be Internet protocol addresses, keyword lists, ,nicknames, passwords, points of contact, and supporting documents.

Computer forensic evidence, like all other evidence must be handled carefully and in a manner that preserves its evidentiary value. Certain types of computer evidence, requires special collection, packaging, and transportation procedure. Thoughtfulness should be given to protect computer data that

may be susceptible to damage or alteration from electromagnetic fields such as those generated by static electricity, magnets, radio transmitters and other devices. Keep electronic evidence away from magnetic sources. Avoid storing forensic evidence in vehicles for prolonged periods of time. Excessive heat, cold, or humidity can damage forensic evidence. Verify that computers and other electronic components that are not packaged in containers are secured in the vehicle to prevent shock and potentially damaging vibrations.

In response to the need to analyze, preserve, protect and defend forensic evidence, an initiative was begun in 1999 to build and staff Regional Computer Forensic Laboratories (RCFLs) Thirteen RCFLs are available for use by more than 1,000 law enforcement agencies, spanning fifteen states. The New Jersey RCFL provides free computer forensic training services for law enforcement investigators and computer forensic specialists, who can also receive FBI digital forensic examiner certification through participation in a twelve to eighteen month training regiment that includes coursework, backed by forensic labs and on the job training.

Computer forensic investigations may involve dead or live analysis techniques. Live analysis techniques use software which existed on the system during the time slot being investigated This is in comparison to dead analysis techniques, which uses no software which existed on the system during that time slot. "Rootkits" provide the most common source of false data during live analysis. Rootkits are backdoor tools which modify existing operating system software so an attacker can keep access to and hide on a computer. There are several countermeasures which exist to deal with rootkits. To counter application level rootkits, an investigator can us a CD of trusted tools that he or she knows have not been modified. Library level rootkits, may be countered by an investigator using a CD of trusted tools which are statically compiled so they do not use Trojan libraries. Live analysis may not produce reliable results, but is useful in some cases. Some computer forensic investigations will be too

important to risk using live analysis techniques, as such incidents that involve sensitive data may result in legal action. To date, there is more legal precedence dealing with digital evidence from dead analysis than live analysis.

Sophisticated hackers operate by attempting to conceal or remove evidence of an intrusion by deleting logs, altering date timestamps, and installing their own utilities to bypass the operating system. Programs like Hacker Defender (hxdef.czweb.org) alter the kernel and return information to systems calls. In addition, tools are being developed specifically to make forensic examination more difficult (http://www.metasploit.com/projects/antiforensics/). Increasingly, cybercriminals are using strong

encryption to cloak their activities by encrypting data before stealing it. Careful intruders use covert channel techniques to conceal their mailicious activities within legitimate network activities such as DNS or HTML traffic.

Recovering from compromised hosts is only half the battle. Locating the criminals is also becoming more challenging. Skilled intruders hide their location and work around firewall restrictions using time activated backdoors that periodically "phone home" initiating a connection from inside the compromised network tunnel through firewalls that the intruder uses to communicate with compromised hosts, evening establishing a Windows Terminal Service session when this protocol is blocked by a firewall.

A multidisciplinary team with a wide range of skills is usually needed to apprehend sophisticated attackers. The ideal investigative team has expertise in information security, digital forensics, penetration testing, reverse engineering, programming and behavior profiling. Record keeping and case management are critical to monitor the flow of information. A successful forensic investigation is heavily dependent on the logging and backup systems an organization has in place, and how quickly sources of evidence are located and preserved. Integration of forensic principles into

security tools will improve the ability of law enforcement agencies to conduct network investigations. Furthermore, there is a need to improve training, tools, techniques, and intelligence gathering to help investigators determine when hackers gained access, their methods, what information was exposed, their intent, and how to intruders can be apprehended or at least mitigated.

Computer forensics is a rapidly changing field, which means that computer crime is also rapidly evolving. Furthermore, the computer systems under investigation evolve more rapidly that the tools to examine them. The increasing usage of computers in today's society means that computer crimes occur in all jurisdictions, from large metropolitan cities to small towns that lack the resources to train computer forensic investigators. These combined factors often force inexperienced investigators to examine computer crimes with inadequate and outdated tools. As cybercrime increases, there will be an increased demand for professionally trained law enforcement personnel.

REFERENCES

Leigland Ryan, Krings Axel W., "A Formation of Digital Forensics", International Journal of Digital Evidence", Fall 2004, Volume 3, Issue 2
http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B8472C-D1D2-8F98-8F7597844CF74DF8.pdf

Harrison Warren, Aucsmith David, Heuston George, Mocas Sarah, Morrisey Mark, Russell Steve, "A Lessons Repository for Computer Forensics", International Journal of Digital Evidence, Fall 2002, Volume 1, Issue 3 *
http://www.utica.edu/academic/institutes/ecii/publications/articles/A049D6C7-93E9-51F2-A468BF90038985DB.pdf

Radcliff Deborah, "Cybersleuthing solves the case" Computerworld, 14 January 2002
http://www.computerworld.com/securitytopics/security/story/0,10801,67299,00.html

Carrier Brian D., Spafford Eugene H., "Defining Event Reconstruction of Digital Crime Scenes", CERIAS Tech Report 2004-37
https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2004-37.pdf

US Department of Justice, "Electronic Crime Scene Investigation, A Guide To First Responders"
http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

The Computer Fraud and Abuse Act
http://www.panix.com/~eck/computer-fraud-act.html

The USA Patriot Act
http://www.epic.org/privacy/terrorism/usapatriot/default.html

Richard III Golden G., Roussev Vassil, "Next-Generation Digital Forensics", Communications of the ACM, February 2006, Volume 49, No. 2 *
http://portal.acm.org/citation.cfm?id=1113034.1113074&coll=GUIDE&dl=GUIDE&idx=J79&part=periodical&WantType=periodical&title=Communications%20of%20the%20ACM

Carrier Brian D., "Risks of Live Digital Forensic Analysis", Communications of the ACM, February 2006, Volume 49, No. 2
http://portal.acm.org/citation.cfm?id=1113034.1113069&coll=GUIDE&dl=GUIDE&idx=J79&part=periodical&WantType=periodical&title=Communications%20of%20the%20ACM

Casey Eoghan, "Investigating Sophisticated Security Breaches", Communications Of The ACM, February 2006, Volume 49, No. 2
http://www.strozllc.com/docs/pdf/Casey-CACM-Sophisticated-Intruders.pdf

Schweitzer Douglas, "Incident Response" Wiley Publishing Inc., 2003

Whitman Michael E., Mattord Herbert J., " Principles of Information Security" Thomson Course Technology, 2005