Computer Forensics:

History, Tools and Outlooks

By John Burns

IT-103-002

Research Paper

02/25/2012

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://academicintegrity.gmu.edu/honorcode/ . I am fully aware of the following sections of the Honor Code: Extent of the Honor Code, Responsibility of the Student and Penalty. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://universitypolicy.gmu.edu/1301gen.html web site."

The information age has forever changed the way people connect with each other and our world as a whole. From the creation of the internet in the 1950's to the use of smart phones, the world is empowered with information. Any person with an Internet service provider (ISP) can search anything using any number of search engines, including Google. Because of the availability of this information, the saying, "it is not what you know it is how fast you can find out." Is truer than ever. Whether they realize it or not, most people are walking around with a very powerful computer/phone in their hands. This allows people to go about the day with all the information the Internet has to offer at their fingertips. Yet, with all the positives of the information age, new categories of crime have emerged as a very large negative. These computer crimes, include the gaining and manipulation of information, is available to us. (Solomon p.4) There is very specific branch of law enforcement, computer forensics, that deals specifically with these new computer crimes. These computer forensic professionals are people whom use computers to hunt, investigate, and present evidence of computer crimes. Most Internet crimes can be classified into black hat hacking, internet scams, corporate fraud, and security concerns such as viruses, worms, and trojan horses. It is important to know the functions and behaviors of each to protect your computer and your data from these threats.

First, black hat hacking is the unethical use of computer knowledge and skills to gain access to data used to commit crimes or for personal gain. The term black hat is used to classify the hacker as a bad guy. The term originates from old west movies where the "good guys" wore white hats and the villains wore black hats. This type of hacker is not motivated to improve or build anything, but rather to destroy and plunder. I think of black hackers as the pirates of the internet - they may employ a variety of scams, viruses, worms, and trojan horses to acheive their desired means. They are also known for Internet scams.

Our second type of crime is Internet scams, which can be defined by the social engineering of a story via email, chat sites, or other messaging services. There are many types of social engineering techniques, most are centered around convincing the mark (target) to give up some sensitive information. Hackers do this by convincing marks that they are authorized to receive the information.. This sensitive information can then be use to steal money, commit computer crimes using your computer and infecting other computers with a virus.

Next, corporate fraud is the manipulation and/ or destruction of papers that may incriminate a company's management/owners. Everyone is familiar with ENRON, the world's largest business failure. Enron was the world's largest communication and energy trading company that filed for bankruptcy. As a result, millions of dollars were lost and all of Enron's employees lost their jobs. Law enforcers found most of the evidence was the various communications on Enron executives' computers and in their E-mails. Computer forensics teams have been created to deal with this type of investigation.

Wikipedia.com defines computer forensics as *" a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.*" I think of it as the practice of finding and preserving data from multiple sources, including lost, deleted and corrupted files, that is pertinent to a criminal case. Computer forensics is an imperative resource for collecting evidence to present in court for computer crimes. Computer Forensics must follow a thorough and systemic searching procedure to ensure the protection and authenticity of evidence. The job of a computer forensics team is to search, preserve, collect, and present the data in a court. Computer forensics is a profession that encompasses the

computer science and elements of law that collects and analyzes data off of a computer, storage device, or network that is important to a case (Marcella P.5). Computer forensics professionals can be hired for many reasons, including aiding criminal prosecutions, aiding law enforcement officials, assisting with insurance company verification, and identifying corporate wrongdoing (Bauchner p.11-12).

In the instance of gathering criminal evidence in cyber crimes, the computer forensics professionals follow a specific set of procedures. First, law enforcement must obtain a special warrant for seizing a computer. Once the warrant is presented to the accused, the investigators will physically take pictures of the room and the layout of the electronics. Next the officers will secure the electronics and any storage devices that are believed to have data important to the case (Strickland). The storage devices are sent to the labs to be analyzed. Once the evidence is delivered to the computer lab, the forensic investigator will then create a full back up image and second copy of the device. This is for the protection of the evidence and it also allows the investigator to manipulate the disk to find files without compromising the original data. to the investigators look for are electronic tampering, viruses, and worms. There are numerous tools at the investigators' disposal. The most current ones are Prodiscovery, AccessData FTX and Mandiant First Response , just to list a few. The Encase suite and Mandiant First Response are the most common and easy to use (Marcella p.113). Through the introduction of powerful soft ware and the experience of the investigator, the analysis of the data can be quickly and accurately sorted and collected. Most computer forensic labs have a standard operating procedure checklist in place. The purposes of these standards are to ensure quality documentation for the computer forensic technician. Every crime lab should have these standard

operating procedures or best practices in place to ensure quality. Yet, even with standard operation, there are some challenges that may arise when the technician does their investigation.

Computer forensics investigation techniques and operation procedures are not perfect. Technicians face many challenges, including anti-forensics software, viruses, and improper chain of custody of the evidence.

First, we will learn about anti-Forensics. Anti-forensic software is any software used to hide, encrypt or falsify data that is being investigated (Wikipedia). Anti-forensics has gained more popularity because of the increased use of computer forensics in criminal investigations. Hiding information is done by encrypting data with a program or cipher

Next we have viruses. A virus is a code that cannot spread on its own and needs to piggy-back on other programs. There are a lot of similarities between computer viruses and biological viruses. Both need a host to live, both are contagious, and both are not easily spotted without using precautions. Viruses can install a back door to the computer for hackers, record key logs to steal passwords, or just to delete or tamper with data files on the computers infected with the virus. So it is important to check for viruses before starting the computer investigations.

The destroying or tampering of evidence on a hard drive is very easy and can be hard to track if not monitored. The destruction of a hard drive can be as easy as smashing it, exposing it to an electromagnet, or reformatting the hard drive.

In conclusion, the positives of the creation of computer forensics investigation far outweigh the negatives. It is a great field that benefits everyone. Computer forensics technicians are the unseen detectives that collect, access, and present evidence and data. This is a great comfort for anyone who uses the Internet at home or in his or her business.

I learned about security and IT hardening. We brushed the importance of computer forensics and the pros and cons of the trade. The Internet is not going anywhere, and as a result we will always have a need for computer forensics. Now you are empowered with the information to learn more about the tools and maybe join the ranks of other computer forensic investigators (Reuuscher). There is plenty of schooling available in the Northern Virginia area to become a computer forensic technician.

Resources

Reuuscher, D. (n.d.). How to Become a Cyber-Investigator. Retrieved February 19, 2012, from http://certification.about.com/cs/securitycerts/a/compforensics.htm

Strickland, J. (n.d.). HowStuffWorks "How Computer Forensics Works." Retrieved February 19, 2012, from http://computer.howstuffworks.com/computer-forensic.htm

Solomon, Michael. (n.d.). Computer Forensics Jumpstart- *google books*. Retrieved February 19, 2012, from http://books.google.com/books?id=ETgIaxAygQAC&pg=PA1&source=gbs_toc_r&cad=4#v=onepage&q&f=false

Computer forensics - Wikipedia, the free encyclopedia. (n.d.). Retrieved February 19, 2012, from http://en.wikipedia.org/wiki/Computer_forensics

Marcella, A & Mendendez , D. (2008) *Cyber Forensics: a field manual for collecting and examining and presenting Evidence of Computer crimes.*. Botan Roca, FL: Aurbach Publishing

Bauchner, Elizabeth, 2006, *Computer Investigation: forensics the science of crime solving*.

Broomall, PA : Mason crest Publisher