Unit 9 Final Project

By Michelle Hoffmann

CJ215: Exploration of Computer Crime
Professor: David Makin
February 13, 2012

Over the past few years, the incidences of cybercrime have become more and more common. With the availability of cell phones and smartphones, the advent of social networking sites such as Facebook and MySpace, and the increase in computer use, those whose intent it is to break the law have found more and more opportunity to perpetrate money scams and other insidious cons via electronic means. This has caused renewed concerns about computer security among computer users worldwide. The vice president of SophosLabs, http://www.sophos.com/, Mark Harris stated recently, "As cybercriminals expand their focus, organizations are challenged to keep their security capabilities from backsliding as they adopt new technologies," (Smith, 2012).

Current trends in cybercrime

An investigative news team recently did a story in St. Paul, MN on the hacking of Wi-Fi having become a big problem in the area. Criminals would set up shop at coffee shops, gas stations, the University and other places, and proceed to set up false networks so that unsuspecting computer users would use them and thereby grant access to their computers to the criminal.

Also becoming more common place, is the rash of malware and viruses being used to usernames and passwords to sensitive websites. Banks and other companies have the latest and greatest security in place, but hackers and other cyber criminals seem to keep one step ahead of them. It's a never ending race.

One of the newest cybercrimes focuses on those who own timeshares.

According to the Internet Crime Complaint Center (ic3), “Timeshare owners across the country are being scammed out of millions of dollars by unscrupulous companies that promise to sell or rent the unsuspecting victims' timeshares. “ (Internet Crime, 2012)

Based on the information above and recent events within the company, it is evident that less and less technologically knowledgeable people now have access to and the ability to commit computer related crimes.

The Latest Laws Relevant To Computer Crime

Prior to being able to make any recommendations or policies on computer access and usage, it is important to understand how the law interprets computer crime.

In response to the growing problem of computer crime, the108th session of Congress has introduced over 150 bills that are related to the privacy of individuals and companies. The 109th congress has also introduced over 60 more

So far, over 35 states have created laws requiring that companies not only protect sensitive information but also notify customers should the information be compromised. (Mark, 2006)

In an attempt to stop computer crime in the United States, the Federal Government passed the Computer Fraud and Abuse Act (CFAA) of the US Criminal Code (18 U.S.C . §1030) in 1984. This act makes it illegal to knowingly attempt to breach another’s computer network or system (Mark, 2006).

Rules for Seizing Electronic Devices (Hart, 2004)

1. Policy and Procedure Development: Create a training program for the examiners focusing on how to recover digital evidence safely and securely.

2. Evidence Assessment: All digital evidence should be thoroughly assessed. The search warrant should be reviewed as to the details of the case. The officers involved in the gathering of evidence need to know nature of hardware and software and what other potential evidence to look for. Make sure that the scene is properly secured before and during the search. If necessary, take note of the following while at the scene:

- Identify the number and type of computers.
- Determine if a network is present.
- Interview the system administrator and users.
- Identify and document the types and volume of media, including all *removable media such as external drives*.
- Document the location from which the media was removed.
- Identify any offsite storage areas and/or remote computing locations.
- Identify any *proprietary software, i.e. software that is owned by the company*.
- Evaluate the general conditions of the site.
- Determine the operating system in question.

3. Evidence Acquisition:

- First you will secure digital evidence. This must be done by following certain guidelines as set up by the department.
- Document the hardware and the software configuration of the examiner's system.

■ Verify that the search warrant includes all available hardware and software.

■ Disassemble the case of the computer to be examined to permit physical access to the storage devices.

—Take care to ensure equipment is protected from static electricity and magnetic fields.

■ Identify what storage devices will need to be acquired. These devices can be internal, external, or both.

■ Document the internal storage devices and hardware configuration. Write down:

■ Drive information (e.g., make, model, geometry, size, jumper settings, location, drive interface).

■ What internal components are connected to the computer (e.g., sound card; video card; network card, including *media access control (MAC)* address – a hardware address that uniquely identifies each node of a network; personal computer memory card international association (PCMCIA) cards).

■ Disconnect the storage devices using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data.

■ Retrieve configuration information from the suspect's system through controlled boots.

■ Perform a controlled boot to capture ***CMOS/BIOS*** information and test functionality.

■ Boot sequence (this may mean changing the BIOS to ensure the system boots

from the floppy or CD-ROM drive).

■ Times and dates of computer operation.

■ Passwords used to power the computer on.

■ Perform a second controlled boot to test the computer's functionality and the forensic boot disk.

■ Ensure the power and data cables are properly connected to the floppy or CDROM drive, and ensure the power and data cables to the storage devices are still disconnected.

■ Place the forensic boot disk into the floppy or CD-ROM drive. Boot the computer and ensure the computer will boot from the forensic boot disk.

■ Reconnect the storage devices and perform a third controlled boot to capture the drive configuration information from the CMOS/BIOS.

■ Ensure there is a forensic boot disk in the floppy or CD-ROM drive to prevent the computer from accidentally booting from the storage devices.

■ Drive configuration information includes logical block addressing (LBA); large disk; cylinders, heads, and sectors (CHS); or auto-detect.

■ Power the system down.

■ Whenever possible, remove the subject storage device and acquire the data using the examiner's system. When attaching the subject device to the examiner's system, be sure to configure the storage device so that it will be recognized.

■ Exceptional circumstances, including the following, may result in a decision not to remove the storage devices from the subject system:

■ RAID (redundant array of inexpensive disks). Removing the disks and

acquiring them individually may not yield usable results.

■ Laptop systems. The system drive may be difficult to access or may be unusable when detached from the original system.

■ Hardware dependency (legacy equipment). Older drives may not be readable in newer systems.

■ Equipment availability. When the examiner does not have access to the necessary equipment

4. Evidence Examination: The process of evidence examination can be broken down into three basic steps.

#1: Back up the files to a separate drive so that they can be later recovered.

#2: Extract the evidence from the computer. This can be done in one of two ways.

a) Physical Extraction:

- extract the data from the drive by using keyword searches, examine the partition. This could identify the systems and tell you if the whole drive is accounted for or if it has been partitioned.

- Use a file carving utility. This could help to recover and extract usable data and files that are not evident on the system

b) 'Logical Extraction':

-■ Extraction of the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location.

■ Data reduction to identify and eliminate known files through the comparison of calculated hash values to authenticated hash values.

- The extraction of files pertinent to the examination. Methods to accomplish this may be based on file name and extension, file header, file content, and location on the drive.
- The recovery of deleted files.
- Extraction of *password-protected*, encrypted, and compressed data.
- Extraction of file slack.
- Extraction of the *unallocated space*.

#3: Analyze the data that has been extracted. This means that you will interpret the data to determine how significant it is to the case. There are three ways to accomplish an analysis:

TimeFrame analysis: This can be done by reviewing the computer's Meta data to determine when the computer was last used, what changes were made on the computer and when or if files had been modified or deleted. It would also be helpful to go over any logs that are available on the computer.

Data Hiding Analysis: This can help in detecting and recovering data that has been hidden on the computer. It can help by pointing at who the owner is and what his/her intent was. Some ways to perform this type of analysis are by accessing all of the password protected, encrypted and compressed files. If they are present, it could mean that there is something that the user is trying to hide from anyone who is not authorized on the computer. Even just the password itself could lend a clue to the file's contents.

Sometimes, there may be evidence of what is called '***Steganography***', or the hiding of information within information. (Steganography, 2001) These can be as

simple as hidden text within a document or website, the use of “covert channels” such as denial-of-service tools that use the ICMP (Internet Control Message Protocol) as a way of “talking” to compromised systems. (Steganography, 2001)

Application and File Analysis: By performing this type of analysis, one can gain information about the capability of both the computer itself and the person using it. By performing this type of analysis, it may lead to the necessity of further steps to be taken in order to extract and analyze the data.

These steps include: “

- *Reviewing file names for relevance and patterns.*
- *Examining file content.*
- *Identifying the number and type of operating system(s).*
- *Correlating the files to the installed applications.*
- *Considering relationships between files. For example, correlating Internet history to cache files and e-mail files to e-mail attachments.*
- *Identifying unknown file types to determine their value to the investigation.*
- *Examining the users’ default storage location(s) for applications and the file structure of the drive to determine if files have been stored in their default or an alternate location(s).*
- *Examining user-configuration settings.*
- *Analyzing file metadata, the content of the user-created file containing data additional to that presented to the user, typically viewed through the application*

that created it. For example, files created with word processing applications may include authorship, time last edited, number of times edited, and where they were printed or saved" (Hart,2004)

The metadata contents may reveal information about Ownership and possession: In some instances it may be important to find out the identity of the person who created, modified or accessed a file. (Hart, 2004) This type of analysis may be dependent on other factors which may be part of any of the other types of analysis as defined above.

5. Documenting and Reporting: It is the responsibility of the person performing the examination to completely document all digital evidence throughout the investigation. Each step is to be accurately recorded and the final report should be written up as comprehensively as possible. (Hart, 2004) Use the following list as a guide:

■ Take notes when consulting with the case investigator and/or prosecutor. (Hart, 2004)

■ Keep a copy of the search warrant with the case notes. (Hart, 2004)

■ Maintain the initial request for assistance with the case file. (Hart, 2004)

■ Maintain a copy of chain of custody documentation. (Hart, 2004)

■ Take notes detailed enough to allow complete duplication of actions. (Hart, 2004)

■ Include in the notes dates, times, and descriptions and results of actions taken. (Hart, 2004)

■ Document any irregularities encountered and any actions taken regarding the irregularities during the examination. (Hart, 2004)

■ Include additional information, such as network topology, list of authorized users, user agreements, and/or passwords. (Hart, 2004)

■ Document changes made to the system or network by or at the direction of law enforcement or the examiner. (Hart, 2004)

■ Document the operating system and relevant software version and current, installed patches. (Hart, 2004)

■ Document information obtained at the scene regarding remote storage, remote user access, and offsite backups. (Hart, 2004)

CopperMine Heavy Industries. Acceptable Use Policy

At it's sole discretion, CopperMine Heavy Industries reserves the right at any time to edit, change or modify in whole or in part the contents of this document.

A third party posting may not contain or be linked to any "Prohibited Content". Prohibited Content shall be identified as any content that:

1. Does not have the legal right to use any copyrighted, trademarked, or patented references

2. Violates any confidentiality agreements;

3. is Defamatory, libelous or slanderous conduct;

4. Consists of anything of a personal, private or non-business related nature;

5. Is illegal, obscene or promotes hatred or bigotry based on sex, race, religion, race,

nationality, or any other differentiating criteria;

6. Can be seen as harassment, stalking or otherwise threatening towards a person.

7. Is misleading, false, or intended to misrepresent.

8. Any corporate or business information that is classified as secret, proprietary and unique to CopperMine Heavy Industries.

CopperMine Heavy Industries, in its sole discretion, will determine what constitutes "Prohibited Content" under this AUP. Any violations of this Acceptable Use Policy should be sent to *abuse@coppermine.com*

The usage of computers and other electronic media by criminals to access both personal and company information and create havoc increases exponentially every time a technological advancement is made. Security companies try to stay on top of new developments, but because the criminal element seems to stay one step ahead, other ways are put into place to deter theft.

References

Hart, Sarah V. Forensic Examination of Digital Evidence. 2004. NIJ DOJ.pdf

Internet Crime Complaint Center. Joint FBI and DHS Puclic Service Announcement. 2012. http://www.ic3.gov/media/2012/120120.aspx

Internet Crime Complaint Center. TimeShare Marketing Scams. 2012. http://www.ic3.gov/media/2012/120125.aspx

Kessler, Gary L. Steganography. 2001. http://www.garykessler.net/library/steganography.html

Mark, Heather. The Wild West Information Security. 2006. http://ww.transactionworld.net/articles/2006/January/security1.asp

Smith, Tineka. Mobile and social media to dominate cybercrime trends in 2012. 26 January, 2012. http://security.cbronline.com/news/a-look-back-at-2011-trends-in-cybercrime-260112