Cyber Forensics and Incident Handling

- Sohrab Ardeshar Vakharia

What is Forensic Science?

- **Forensic science**, also known as criminalistics, is the application of **science** to criminal and civil laws, mainly—on the criminal side—during criminal investigation, as governed by the legal standards of admissible evidence and criminal procedure.

Computer Forensics

- **Computer forensics** involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases.

- Computer Forensics is a part of Incident response in an organization.

Types of Computer Forensic Investigations

- Private investigations
- Public Investigations

Few important terms to be considered during investigation process

- The Warrant
- Company Policies
- Corporate investigations vs non-corporate investigations
- Warnings (warning banners)
- Personal and Company property
- Maintaining the professional conduct

Preparing a Computer Investigation

- Role of computer forensics professional is to gather evidence to prove that a suspect committed a crime or violated a company policy
- Collect evidence that can be offered in court or at a corporate inquiry
  - Investigate the suspect's computer
  - Preserve the evidence on a different computer
- Follow an accepted procedure to prepare a case
- **Chain of custody**
  - Route the evidence takes from the time you find it until the case is closed or goes to court

An Overview of a Computer Crime

- Computers can contain information that helps law enforcement determine:
  - Chain of events leading to a crime
  - Evidence that can lead to a conviction
- Law enforcement officers should follow proper procedure when acquiring the evidence
  - Digital evidence can be easily altered by an overeager investigator
- Information on hard disks might be **password protected**

An Overview of a Company Policy Violation

- Employees misusing resources can cost companies millions of dollars
- Misuse includes:
  - Surfing the Internet
  - Sending personal e-mails
  - Using company computers for personal tasks

Taking a Systematic Approach

- Steps for problem solving
  - Make an initial assessment about the type of case you are investigating
  - Determine a preliminary design or approach to the case
  - Create a detailed checklist
  - Determine the resources you need
  - Obtain and copy an evidence disk drive

Taking a Systematic Approach (continued)

- Steps for problem solving (continued)
  - Analyze and recover the digital evidence
  - Investigate the data you recover
  - Complete the case report
  - Critique the case

Assessing the Case

- Systematically outline the case details
  - Situation
  - Nature of the case
  - Specifics of the case
  - Type of evidence
  - Operating system
  - Known disk format
  - Location of evidence

Assessing the Case (continued)

- Based on case details, you can determine the case requirements
  - Type of evidence
  - Computer forensics tools
  - Special operating systems

Few types of corporate cases

- Employee termination cases (example of s/w company's disgruntled employee)
- Internet Abuse
- Email Abuse
- Media leak
- Industrial Espionage
- Interviews and Interrogations

Understanding Forensic Copy (image/ bit-stream copy)

- A bit-stream copy is a bit-by-bit copy (also known as a sector copy) of the original drive or storage medium and is an exact duplicate. The more exact the copy, the better chance you have of retrieving the evidence you need from the disk. This process is usually referred to as “acquiring an image” or “making an image” of a suspect drive. A bit-stream copy is different from a simple backup copy of a disk. Backup software can only copy or compress files that are stored in a folder or are of a known file type. Backup software can’t copy deleted files and e-mails or recover file fragments.

Computer Forensic Softwares

- ProDiscover Basic
- Autopsy (sleuth kit)
- FTK imager
- Encase
- Mobile edit
- CAINE (OS)

Example case of Company policy Violation

- Manager Steve Billings has been receiving complaints from customers about the job performance of one of his sales representatives, George Montgomery. George has worked as a representative for several years. He's been absent from work for two days but hasn't called in sick or told anyone why he wouldn't be at work. Another employee, Martha, is also missing and hasn't informed anyone of the reason for her absence. Steve asks the IT Department to confiscate George's hard drive and all storage media in his work area. He wants to know whether there's any information on George's computer and storage media that might offer a clue to George's whereabouts and job performance concerns. To help determine George and Martha's whereabouts, you must take a systematic approach, described in the following section, to examining and analyzing the data found on George's desk. (Taking a systematic approach…)

Assessing the case

- In the company-policy violation case, you have been asked to investigate George Montgomery. Steve Billings had the IT Department confiscate all of George's storage media that might contain information about his whereabouts. After talking to George's co-workers, Steve learned that George has been conducting a personal business on the side using company computers. Therefore, the focus of the case has changed from a missing person to a possible employee abuse of corporate resources.

(from the book: Guide to Computer Forensics and Investigations)

Selecting a Basic Forensic Workstation

- Depends on budget and needs
- Use less powerful workstations for mundane tasks
- Use multipurpose workstations for high-end analysis tasks

Stocking Hardware Peripherals

- Any lab should have in stock:
  - IDE cables
  - Ribbon cables for floppy disks
  - SCSI cards, preferably ultra-wide
  - Graphics cards, both PCI and AGP types
  - Power cords
  - Hard disk drives
  - At least two 2.5-inch Notebook IDE hard drives to standard IDE/ATA or SATA adapter
  - Computer hand tools

Maintaining Operating Systems and Software Inventories

- Maintain licensed copies of software like:
  - Microsoft Office
  - Quicken
  - Programming languages
  - Specialized viewers
  - Corel Office Suite
  - StarOffice/OpenOffice
  - Accounting applications

Using a Disaster Recovery Plan

- Restore your workstation and investigation files to their original condition
  - Recover from catastrophic situations, virus contamination, and reconfigurations
- Includes backup tools for single disks and RAID servers
- **Configuration management**
  - Keep track of software updates to your workstation

Thank you!
Any Questions?

-Sohrab Ardeshar Vakharia

www.sohrabvakharia.in