Lecture Overview

- Introduction
  - Overview of the industry and resources

- Assessing the Case
  - Employee Termination Investigations
  - Media Leak Investigations
  - Industrial Espionage Investigations

- Taking a Systematic Approach

- Securing the Evidence

- Network & Email Forensics

- Digital Image Forensics
Introduction

Real Life Case Studies

- Framed by a virus?
- The Nigerian connection
- Saved by Facebook
- A “hopeful” artist?

- Cracking Stuxnet, a 21st-century cyber weapon (TED video)
Introduction: Digital Forensics

- Computer Forensics: investigates data that can be retrieved from a computer’s hard disk or other storage media

- Computer forensics investigators:
  - focus on retrieving information from the computer and/or its component parts
    - active, archival, latent

- Network Forensics: yields information about how a perpetrator or an attacker gained access to a network

- Network forensics investigators:
  - use log files to determine when users logged on, frequency, URLs visited and for how long, how they logged on, from what location etc.
Introduction: Digital Forensics

- Computer/Network forensics specialists may be (and often are) the same person - they may have a specialized function in investigative group

- Hot career – why?

- Types of cases in which digital forensics is employed …?
  - Child Pornography:
  - And?
Introduction: Digital Forensics

- How is computer forensics different from normal data recovery?
  - Inculpatory or
  - Exculpatory
Brief History

- Relatively new field

- Paradox of Computer/ Network/ Digital Forensics:

  - 1970’s:
    - electronic crimes – mainframe
    - computer users were experts and only certain industries used computers
    - white-collared fraud – banking industry
      - one half-cent crime
Brief History

- **1970’s:**
  - The Federal [Rules of Evidence](#) controlled the use of digital evidence
    - code of evidence law

- **1980s/ 1990s:**
  - Due to increasing number of cases involving digital evidence, the [Computer Analysis and Response Team](#) (CART) was formed
    - provides assistance to FBI field offices

- **Current Examples:**
  - CART teamed up with DoD’s Computer Forensics Laboratory (DCFI)
    - the Philly Division
  - [SANS](#)
  - [CERT @ CMU](#)
  - [ISFCE](#)
### Examples of Crimes Solved Using Forensics

<table>
<thead>
<tr>
<th>Criminal</th>
<th>Type of Crime</th>
<th>Type of E-Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dennis Rader</td>
<td>Serial killer</td>
<td>Deleted files on a floppy disk used by the criminal at his church’s computer</td>
</tr>
<tr>
<td>Lee Boyd Malvo, John Allen Muhammad</td>
<td>Snipers</td>
<td>Laptop computer found in the car, that contained maps with icons pinpointing shooting scenes</td>
</tr>
<tr>
<td>Lisa Montgomery</td>
<td>Murder and fetus-kidnapping</td>
<td>E-mail communication between the victim and criminal—tracing an IP address to a computer at criminal’s home</td>
</tr>
</tbody>
</table>

Let’s not forget one of the most famous corporate cases that has involved a substantial amount of computer forensics ….
<table>
<thead>
<tr>
<th>Criminal</th>
<th>Type of Crime</th>
<th>Type of E-Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peter Chapman (Ashleigh Hall)</td>
<td>FB/ Murder</td>
<td>Used FB to arrange meeting</td>
</tr>
<tr>
<td>Scott Peterson</td>
<td>Murder</td>
<td>GPS data from his car and cell phone; Internet history, currents, map</td>
</tr>
<tr>
<td>Robert Durall (“computer expert”)</td>
<td>Murder</td>
<td>Web browser history “Kill + Spouse,” “Accident + Deaths.” “smothering”</td>
</tr>
<tr>
<td>Neil Entwistle</td>
<td>Murder of wife and baby</td>
<td>Web browser history “how to kill people,” before the murders and various escort services after the murders</td>
</tr>
<tr>
<td>Alejandro Avila</td>
<td>Rape and murder</td>
<td>E-evidence of child pornography on his computer</td>
</tr>
<tr>
<td>Zacarias Moussaouï</td>
<td>Terrorism</td>
<td>E-mail, files from his computers</td>
</tr>
</tbody>
</table>
Below are examples of some widely used digital forensic software companies:

- **EnCase** from Guidance Software (~ $2,500 per user)
- **FTK** from AccessData (~ $600 per user)
- **Digital Intelligence**
- **Paraben**
- **Passware**
- **Further list of tools**
- **List of free forensic tools**
Who Works on Digital Forensics Cases?

- Governmental (NSA, CIA, FBI)
- State/ Local
- International (Interpol, MI5)

- Examples of private security companies
  - www.arcsight.com
  - www.clearswift.com
  - www.datasec.co.uk
  - www.integrais.com
  - www.forensics-intl.com
  - www.pentasafe.com
  - www.savvydata.com
  - www.vestigeltd.com
  - www.vogon-international.com
  - www.vordel.com

- Money contingent on experience and success rate
Some Certifications for Computer/ Digital Forensic Experts

- Global Information Assurance Certification (GIAC)
- Certified Forensics Analyst (CFA)
- Certified Computer Forensics Examiner (CCFE) certification. The test candidate must pass a multiple choice exam with a score of 70% or higher.
- Encase Certified Examiner (EnCE) certification
- Certified Information Systems Auditor (CISA)
- The International Society of Forensic Computer Examiners’ Certified Computer Examiner (CCE)
Some Journals and References of Interest

- Digital Forensics Magazine
- Cryptologia
- International Journal of Digital Evidence
- International Journal of Forensic Computer Science
- International Journal of Digital Crime and Forensics
- Journal of Digital Forensics, Security and Law
- Journal of Digital Investigation
- Journal of Digital Forensic Practice
- Small Scale Digital Device Forensic Journal
- The Journal of Applied Digital Forensics and eDiscovery
Conferences Related to Digital Forensics

- American Academy of Forensic Science
- Conference on Digital Forensics, Security and Law
- Department of Defense CyberCrime Conference
- Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)
- EuSecWest
- EuroForensics-Forensics Sciences Conference and Exhibition
- Computer Security Foundations Symposium
- International Conference on Security and Privacy in Communication Networks
- USENIX Security Symposium
- International Workshop on Security in Cloud Computing
- DEF CON Hacking Conference
Forensics Investigation Methods

Methods used by investigators must achieve many of these objectives:

- Protect the suspect system
- Discover all files (text/ video/ audio/ pictures/ emails etc.)
- Recover deleted files
- Reveal contents of hidden files
- Access protected or encrypted files
- Use steganalysis to identify hidden data
- Analyze data in unallocated and slack space
- Print an analysis of the system
- Provide an opinion of the system layout
- Provide expert testimony or consultation
Assessing the Case

- Imagine that you are the Computer Forensics Specialist... before you start, there are some things to consider

- Situation: corporate employee abuse case, pornography, murder/homicide/suicide ... take copious notes on...
  - types of evidence
  - operating systems
  - locations of evidence
  - descriptions of evidence
  - antistatic bags, tapes, tags, labels and ________________
<table>
<thead>
<tr>
<th>Case No.</th>
<th>Exhibit Ref. No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male:</td>
<td>Model:</td>
</tr>
<tr>
<td>Serial No:</td>
<td>Size:</td>
</tr>
<tr>
<td>Cylinder:</td>
<td>Heads:</td>
</tr>
<tr>
<td>Sectors</td>
<td>Jumper setting:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Volume Label</th>
<th>No of Partitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition Name 1</td>
<td>Partition Name 2</td>
</tr>
<tr>
<td>Partition Name 3</td>
<td>Partition Name 4</td>
</tr>
</tbody>
</table>

### Imaging

<table>
<thead>
<tr>
<th>Software and Version (Image 1)</th>
<th>Write block type used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software and Version (Image 2)</td>
<td>Write block type used</td>
</tr>
<tr>
<td>Time Connected</td>
<td>Time Source</td>
</tr>
</tbody>
</table>

### Notes:

<table>
<thead>
<tr>
<th>Hashed Match Image 1</th>
<th>Hashed Match Image 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash verification attached?</td>
<td>No</td>
</tr>
</tbody>
</table>

### Case Hard Drive Information

<table>
<thead>
<tr>
<th>Original Image located on Disk No (In safe)</th>
<th>Disk Reference No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Image located on Disk No (in safe)</td>
<td>Disk Reference No</td>
</tr>
<tr>
<td>Backup Image located on Disk No (in server)</td>
<td>Disk Reference No</td>
</tr>
<tr>
<td>Work Disk for case</td>
<td>Disk Reference No</td>
</tr>
</tbody>
</table>
Typical Nature of Corporate Cases

- Forensics experts are called in for several types of cases. Some common examples are:
  - Employee Termination Cases
  - Media Leak Investigations
  - Industrial Espionage Investigations

some other examples
Employee Termination Cases

- majority of these involve the abuse of corporate assets

- predominant in contributing to hostile work environment
  - distributing emails/ pictures that are offensive
  - examples at Brooklyn and MU

- 2 main types of Investigations:
  - Internet abuse
  - email/ IM/ text abuse
Employee Termination Cases (see Lab 6)

Headers and IP addresses are common sources of forensic investigations.

What is a header?
To find email headers go to this link:
http://mail.google.com/support/bin/answer.py?hl=en&answer=22454

What is an IP address?
xxxx.xxxx.xxxx.xxxx
E.g. IP address for Millersville University is: 166.66.64.xxxx
To find your IP address or any IP address go to this link:
http://ip-lookup.net/
http://www.hostip.info/
http://whatismyipaddress.com/
cmd
Employee Termination Cases

- Internet Abuse Investigations

- Firstly – what constitutes ‘abuse’- you must be versed with the laws of your state and the corporate policies

- As the forensics expert, you need the following, for starters:
  - your analysis toolkit (ProDiscover, X-Ways Forensics, EnCase, FTK etc.)
  - the organization’s Internet server logs (from the administrator)
  - the suspect computer’s IP address (from the administrator)
  - all the disk drives

- AND??
Employee Termination Cases

- **Email/ IM/ Text Abuse Investigations**
  - most often include emails that are inappropriate, threats, harassments
  - Detroit mayor: [http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503043.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503043.html)

- **As the forensics expert, you need the following:**
  - electronic copies of emails (header data)
  - phone records for texts – what are you looking for here?
  - email server logs – or the server that houses back ups
  - .pst files (Outlook)
  - company policies

- What else?
Media Leak Cases

- Why is the leaking of information a critical problem for many organizations?

  examples:
  - Holder article
  - Citi analyst and FB leak

- As the forensics expert, you need to do the following:
Industrial Espionage

- Involves either previously “trusted” employees or disgruntled employees or seemingly ignorant employees.
  - 60% of employees who leave or are fired from their jobs, steal (?) data
  - Survey
  - Coca-Cola example

- These are most often treated as criminal investigations

- As the forensics expert, you need to do the following:
Motives for Cybercrimes: the 5 W’s

- Finding the motive - answering the 5 Ws helps in criminal investigations:
  - Who?
  - What?
  - Where?
  - When?
  - Why?

- Possible motives:
  - Financial gain, including extortion and blackmail
  - Cover up a crime
  - Remove incriminating information or correspondence
  - Steal goods or services without having to pay for them
  - Industrial espionage
  - Framing
  - Pranksters?

- What else?
The 3 C’s of E-Evidence – some guidelines

- Care
- Control
- Chain of Custody

- These guidelines are more burdensome for easily altered digital data – e.g. e-mail evidence; the investigator would have to establish the origin of the message, the integrity of the system in which the message was transmitted, and the chain of custody of the message.

- E-evidence may be affected by magnetic forces, so they should not be placed in a vehicle of truck that also contains electromagnetic equipment (similar to blood needing to be kept at the proper temperature).

- The operations used to actually collect, copy, analyze, control, and present e-evidence cannot modify the original item being studied in any manner.

- Everyone who touches evidence can contaminate it – therefore a strict chain of custody is essential in computer forensic investigations – each piece of original evidence that is seized should have a chain of custody log associated with it.
Sample of Chain of Custody Form

EVIDENCE

Submitting Agency ____________________________

Date Collected ___________ Time ____________

Item # ______________ Case # ______________

Collected By ____________________________

Description of Evidence ____________________________

Location Where Collected ____________________________

Type of Offense ____________________________

CHAIN OF CUSTODY

Rec. From ___________ By ___________

Date ___________ Time ___________

Rec. From ___________ By ___________

Date ___________ Time ___________

Rec. From ___________ By ___________

Date ___________ Time ___________
Establishing Chain of Custody

During an investigation, the following procedures should be followed to ensure the chain of custody:

1. A record or evidence log should be kept to show when all items of evidence, such as server logs, computers, hard drives, and disk, are received or seized and where they are located.

2. If the items are released to auditors, authorities, or the court, those release dates should be recorded.

3. Access to evidence should be restricted throughout the investigations and any subsequent proceedings.

4. To preserve the chain of custody, the original hard disk should be placed in an evidence locker and appropriate notations should be made in the evidence log.

5. All computer forensics should be performed in the mirror image copy (which should be write-protected) – never on the original.