Computer Forensics

COMP620

"Certainly going back to Sherlock Holmes we have a tradition of forensic science featured in detective stories."

Jeffery Deaver

What is Computer Forensics?

- Scientific process of preserving, identifying, extracting, documenting, and interpreting data on computer

- Used to obtain potential legal evidence

What does Dr. Williams know about Computer Forensics?

A. He has seen some CSI *(**C**omputer **S**cience **I**nvestigator)* on TV
B. He has read Wikipedia
C. He may have done something long ago

Use of Computer Forensics

- Dr. Conrad Murray, the doctor of Michael Jackson, was convicted partially by digital evidence including medical documentation showing lethal amounts of propofol
- The BTK serial killer, Dennis Rader, sent letters to the police on a floppy disk. Metadata within the documents implicated an author named "Dennis“
- A murderer in Durham dumped the body of his wife in a lake. A search of his computer showed maps of the lake depth

Background

- The Dean of Students at Purdue University estimates that 25% of all disciplinary cases involve some sort of computer evidence
- The Director of the FBI now expects 50% of all cases handled by the FBI to involve at least one computer forensic examination
- Local law enforcement agencies and prosecutors expect 20-40% of all cases will require information forensics

Computers in Crime

- A computer can hold data of a crime
  - child pornography
- The computer could be stolen property
- The computer could hold evidence of a crime
  - spreadsheet of drug transactions
- A computer can be the instrument of a crime
  - hacking
  - distribute copyrighted videos

Computers Role in Crime

- Computer as ***Target*** of the incident
  - Get to instructor's test preparation
  - Access someone else's homework
  - Access/Change a grade
  - Access financial information
  - "Denial of Service"
- Computer as ***Tool*** of the incident
  - Word processing used to create plagiarized work
  - E-mail sent as threat or harassment
  - Printing used to create counterfeit material
- Computer as ***Incidental*** to the incident
  - E-mail/file access used to establish date/timelines
  - Stored names and addresses of contacts or others potentially involved in the incident

Forensic Use

Computer forensics is used for

- Law enforcement
- Enforce employee policies
- To gather evidence against an employee that an organization wishes to terminate
- Recover data in the event of a hardware or software failure
- Understand how a system works

Wikipedia

Law Enforcement

- Computer forensics is often used to gather evidence to prosecute a crime
- Computer forensics professionals must be careful to follow the legal requirements for handling evidence
- The evidence can be dismissed if it cannot be shown that it was not tampered, either accidently or intentionally

Preparing an Investigation

- Role of computer forensics professional: gather evidence to prove 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

The 3 As

The basic methodology consists of the 3 As:

- **A**cquire the evidence without altering or damaging the original
- **A**uthenticate the image
- **A**nalyze the data without modifying it

Computer Forensic Activities

Activities commonly include:

- the **secure** collection of computer data
- the **identification** of suspect data
- the **examination** of suspect data to determine details such as origin and content
- the **presentation** of computer-based information
- the **application** of a country's laws to computer practice

The Process

- The primary activities of a computer forensics specialist are investigative in nature.
- The investigative process encompasses
  - Identification
  - Preservation
  - Collection
  - Examination
  - Analysis
  - Presentation
  - Decision

Chain of Custody

- Protects integrity of the evidence
- Effective process of documenting the complete journey of the evidence during the life of the case
- Allows you to answer the following questions:
  - Who collected it?
  - How & where?
  - Who took possession of it?
  - How was it stored & protected in storage?
  - Who took it out of storage & why?

General Types of Digital Forensics

- Network Analysis
  - Communication analysis
  - Log analysis
  - Path tracing
- Media Analysis
  - Disk imaging
  - Content analysis
  - Slack space analysis
  - Steganography
- Code Analysis
  - Reverse engineering
  - Malicious code review
  - Exploit Review

5 Rules of Evidence

- Admissible
  - Must be able to be used in court or elsewhere
- Authentic
  - Evidence relates to incident in relevant way
- Complete (no tunnel vision)
  - Exculpatory evidence for alternative suspects
- Reliable
  - No question about authenticity & veracity
- Believable
  - Clear, easy to understand, and believable by a jury

General Evidence Dos & Don’ts

1. Minimize Handling/Corruption of Original Data
2. Account for Any Changes and Keep Detailed Logs of Your Actions
3. Comply with the Five Rules of Evidence
4. Do Not Exceed Your Knowledge
5. Follow Your Local Security Policy and Obtain Written Permission
6. Capture as Accurate an Image of the System as Possible
7. Be Prepared to Testify
8. Ensure Your Actions are Repeatable
9. Work Fast
10. Proceed From Volatile to Persistent Evidence
11. Don't Run Any Programs on the Affected System
12. Document Document Document!!!!

Scott L. Ksander Source: AusCERT 2003 (www.auscert.org)

Creating Disk Images

- Care must be taken not to change the evidence.
- Most media are “magnetic based” and the data is volatile:
  - Registers & Cache
  - Process tables, ARP Cache, Kernel stats
  - Contents of system memory
  - Temporary File systems
  - Data on the disk
- Examining a live file system changes the state of the evidence
- The computer/media is the “crime scene”
- Protecting the crime scene is paramount as once evidence is contaminated it cannot be decontaminated.
- **Really only one chance to do it right!**

Why Create a Duplicate Image?

- A file copy does not recover all data areas of the device for examination
- Working from a duplicate image
  - Preserves the original evidence
  - Prevents inadvertent alteration of original evidence during examination
  - Allows recreation of the duplicate image if necessary

Bitstream vs. Backups

- Forensic Copies (Bitstream) are bit for bit copies capturing all the data on the copied media including hidden and residual data (e.g., free space, swap, residue, deleted files etc.)
- Often the “smoking gun” is found in the residual data
- Logical vs. physical image

Make Two Copies

- Make 2 copies of the original media
  - 1 copy becomes the working copy
  - 1 copy is a library/control copy
  - Verify the integrity of the copies to the original
- The working copy is used for the analysis
- The library copy is stored for disclosure purposes or in the event that the working copy becomes corrupted
- If performing a drive to drive imaging (not an image file) use clean media to copy to
  - Shrink wrapped new drives
  - Next best, zero another drive

Volatile Data

- Data in the RAM disappears when the computer is turned off
- There may be evidence in RAM that is no longer part of a running program
- There are tools that can copy the RAM to a USB file
- Running a program overwrites some RAM

- Moving a desktop computer to a forensic lab can be challenging involving connecting a UPS and a mouse jiggler

Computer Forensics Certification

There are several professional groups and companies that offer forensic certification

- International Association of Computer Investigative Specialist (IACIS) offers
  - Certified Electronic Evidence Collection Specialist Certification (CEECS)
  - Certified Forensic Computer examiner (CFCE)
- Global Information Assurance Certification Certified Forensic Analyst