Introduction to Digital Forensics

Lesson 1
Reference: Scott L. Ksander
Purdue University
Assistant Professor, Department of Computer Technology
Now, a few words on looking for things:

- When you go looking for something specific, your chances of finding it are very bad.
- Because, of all the things in the world, you're only looking for one of them.
- When you go looking for anything at all, your chances of finding it are very good.
- Because, of all the things in the world, you're sure to find some of them.

-- Darryl Zero, The Zero Effect
Why are we bothering?

• 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
Myths & Misconceptions

- Cyber-criminals are computer experts with a high technical ability
- Cyber-criminals have higher than average IQs
- All cyber-criminals are introverts
- Cyber-criminals are never violent
- Cyber-criminals are not “real” criminals
- Cyber-criminals fit one “neat” profile
Incident Response Methodology (PDCAERF)

Digital Forensics/Evidence Management

Preparation → Detection → Containment → Analysis → Eradication → Recovery → Follow-up

Feed Back
Remains likely those of missing student

Joe Gerret
Staff
Journal and Courier

By Joe Gerret
jgerret@journalandcourier.com

Police suspect that human remains found in the trunk of a car in Rosemont, Ill., belong to a Purdue University graduate student who has been missing since last week.

The Cook County medical examiner is investigating to determine whether the dismembered body belongs to Lei He, 28, a graduate student in Purdue’s mechanical engineering school.

The officer noticed a large meat cleaver in the kitchen sink.

After the body was discovered Tuesday in Rosemont, police got permission from Magistrate Norris Wang to re-enter the apartment to search for a wide array of physical evidence.

The evidence sought included weapons, hair, blood, bills, receipts, notes, financial records, and computer and telephone records.
Context of Digital / Computer Forensics

- Homeland Security
- Information Security
- Corporate Espionage
- White Collar Crime
- Child Pornography
- Traditional Crime
- Incident Response
- Employee Monitoring
- Privacy Issues
- ????
History & Development of Forensic Science

• Francis Galton (1822-1911)
  – First definitive study of fingerprints
• Sir Arthur Conan Doyle (1887)
  – Sherlock Holmes mysteries
• Leone Lattes (1887-1954)
  – Discovered blood groupings (A,B,AB, & 0)
• Calvin Goddard (1891-1955)
  – Firearms and bullet comparison
• Albert Osborn (1858-1946)
  – Developed principles of document examination
• Hans Gross (1847-1915)
  – First treatise on using scientific disciplines in criminal investigations.
Communities

- There at least 3 distinct communities within Digital Forensics
  - Law Enforcement
  - Military
  - Business & Industry
    - Possibly a 4th – Academia
Digital Forensic Science

- Digital Forensic Research
- Homeland Security
- Information Warfare
- Military Operations
- Business & Industry
- Critical Infrastructure Protection
- Law Enforcement
- Courts

Auburn University Digital Forensics
www.eng.auburn.edu/users/hamilton/security/
The Process of Digital Forensic Science

- The primary activities of DFS are investigative in nature.
- The investigative process encompasses
  - Identification
  - Preservation
  - Collection
  - Examination
  - Analysis
  - Presentation
  - Decision
Computer Forensic Activities

Computer forensics 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 3 As

• The basic methodology consists of the 3 As:
  
  – Acquire the evidence without altering or damaging the original
  – Authenticate the image
  – Analyze the data without modifying it
“The Computer”

• 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
General Types of Digital Forensics

• “Network” Analysis
  – Communication analysis
  – Log analysis
  – Path tracing

• Media Analysis
  – Disk imaging
  – MAC time analysis (Modify, Access, Create)
  – Content analysis
  – Slack space analysis
  – Steganography

• Code Analysis
  – Reverse engineering
  – Malicious code review
  – Exploit Review

• The “puzzle” is a combination of all the above pieces
Locard Principle of Exchange

• “..when a person commits a crime something is always left at the scene of the crime that was not present when the person arrived.”

• (Edmund Locard, 1910)
## Forensic Principles

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An Individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.
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

• Source: AusCERT 2003 (www.auscert.org)
5/16D-3. Computer tampering
(a) A person commits the offense of computer tampering when he knowingly and without the authorization of a computer's owner, or in excess of the authority granted to him
(1) Accesses or causes to be accessed a computer or any part thereof, or a program or data;
(2) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and obtains data or services
(3) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and damages or destroys the computer or alters, deletes or removes a computer program or data.
(b) Sentence
(1) A person who commits the offense of computer tampering as set forth in subsection (a)(1) of this Section shall be guilty of a Class B misdemeanor.
(2) A person who commits the offense of computer tampering as set forth in subsection (a)(2) of this Section shall be guilty of a Class A misdemeanor and a Class 4 felony for the second or subsequent offense.
(3) A person who commits the offense of computer tampering as set forth in subsection (a)(3) of this Section shall be guilty of a Class 4 felony and a Class 3 felony for the second or subsequent offense.
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
Evidence Life Cycle

- Collection & identification
- Storage, preservation, and transportation
- Presentation
- Return to production, owner, or court
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?
Forensic Mindset

• Digital Forensic Mindset – Condensed Definition:
  – Using your skills to determine what has occurred or,
  – What most likely occurred as opposed to what is possible
  – You do NOT work for anyone but the TRUTH!
• The tools used are not nearly as important as the person using them!
• The examination should not occur in a vacuum.
• Find out all you can about what is already known.
Organizing the Investigation

• Use your knowledge to examine the system to answer; could it have happened that way or not?
• Don’t make it more complicated than it has to be – start with the obvious!
• Examples:
  – Check for programs that will cause you aggravation – encryption (PGP, Magic Folders, File Vault, EFS, etc.)
Organizing the Investigation

• MAC information – what was happening on the system during the time frame you are interested in?

• What was being “written”, “changed” or “accessed”? 
Why use images

• In keeping with the second IOCE principle, 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 (MAC times)
• 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?

Computer evidence is fragile
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
Why Create a Duplicate Image?

• Digital evidence can be duplicated with no degradation from copy to copy
  – This is not the case with most other forms of evidence
Bitstream vs. Backups

• Are backups sufficient?
  – Ideally NO!
  – Practically it may be the only method available

• Most O/Ses only pay attention to the live filesystem structure
  – Slack, residue, deleted, etc. are not indexed

• Backups generally do not capture this data and they also modify the timestamps of data, contaminating the timeline.
Bitstream vs. Backups

- Forensic Copies (Bitstream)
  - Bit for Bit copying captures all the data on the copied media including hidden and residual data (e.g., slack space, swap, residue, unused space, deleted files etc.)

- Often the “smoking gun” is found in the residual data.

- Logical vs. physical image
Disk Imaging Tools Requirements

• The tool shall make a bit-stream duplicate or an image of an original disk or partition.
• The tool shall not alter the original disk.
• The tool shall be able to verify the integrity of a disk image file.
• The tool shall log I/O errors.
• The tool’s documentation shall be correct.
MAC Times

• Time attributes (Modified, Accessed, Changed).
• Allow an investigator to develop a time line or Chronology of the incident
• The time line is vital when examining logs, & event files
• Improperly accessing or searching a system can alter the time lines destroying evidence or erasing trails.
Drive Imaging Tools

- SafeBack ([www.forensics-intl.com](http://www.forensics-intl.com))
- Ghost ([www.symantec.com](http://www.symantec.com))
  - Newest version of Ghost has a forensic “switch” now
- DD (standard unix/linux utility)
  - `#dd if=device of=device bs=blocksize`
- Encase ([www.encase.com](http://www.encase.com))
- Mareware
- FTK ([www.accessdata.com](http://www.accessdata.com))
Drive Imaging Hardware

• Forensic mobile field system (MFS)
  – Laptop with NIC
  – Portable workstation
Rules of Thumb

• 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
• Verify the integrity of all images!
Disk Write Blockers

- Prevent data being written to the suspect drive
- Ensure the integrity of the suspect drive
- Software Write Blockers v. Hardware
Normal HD Access

• Using the interrupt 0x13 interface for hard drive
  An application program issues an interrupt 0x13 command.
• The interrupt transfers control to the interrupt 0x13 routine in the BIOS. The BIOS routine issues commands, ATA or SCSI as appropriate, directly to the hard drive controller.
• The device does the requested operation and returns the result to the BIOS and then to the application program.
Software Write Block

- Use of a SWB tool changes the normal operation of the interrupt 0x13 interface.
- The SWB tool is executed. The SWB tool saves the current interrupt 0x13 routine entry address and installs a new interrupt 0x13 routine.
- The application program initiates a drive I/O operation by invoking interrupt 0x13. The replacement routine installed by the SWB tool intercepts the command.
- The SWB tool determines if the requested command should be blocked or if the command should be allowed.
- If a command is blocked, the SWB tool returns to the application program without passing any command to the BIOS I/O routines. Depending on SWB tool configuration either success or error is returned for the command status.
- If the command is allowed (not blocked), the command is passed to the BIOS and the BIOS I/O routine issues required I/O commands (ATA, SCSI or other) to the drive controller so that the desired I/O operation occurs on the hard drive.
- Results are returned to the application program.
Hardware Write Block

• A hardware write blocker (HWB) is a hardware device that attaches to a computer system with the primary purpose of intercepting and preventing (or ‘blocking’) any modifying commands from ever reaching the storage device.
• Physically, the device is connected between the computer and a storage device.
• Some of its functions include monitoring and filtering any activity that is transmitted or received between its interface connections to the computer and the storage device.
Forensic Boot Disk

• General principles:
  – Used to boot suspect systems safely
  – Contains a filesystem and statically linked utilities (e.g., ls, fdisk, ps, nc, dd, ifconfig, etc.)
  – Recognizes large partitions (+2 or +8 Gb)
  – Places the suspect media in a locked or read-only state
  – Does not swap any data to the suspect media
Forensic Boot Disk

• **General principles:**
  – Used to boot suspect systems *safely*
  – Contains a filesystem and statically linked utilities (e.g., `ls`, `fdisk`, `ps`, `nc`, `dd`, `ifconfig`, etc.)
  – Recognizes large partitions (+2 or + 8 Gb)
  – Places the suspect media in a locked or read-only state
  – Does not swap any data to the suspect media
Forensic Boot Disk

• Open source bootable images:

  – **Helix**
    (http://www.e-fense.com/helix/)

  – **Trinux**
    (http://trinux.sourceforge.net/)

  – **BartPE**
    (http://www.nu2.nu/pebuilder/)