Computer Crimes and Forensics

Professor Stephen S. Yau

Computer Involvement with a Crime

- Three types :
  - Computer assisted a crime: child pornography, credit card fraud, intellectual property theft in corporate environment, etc.
  - Computer was the target of a crime: DoS attack against an e-commerce website, etc.
  - Computer contains information that is incidental to the crime: “pay and owe” list from drug trafficker’s computer

Who Need Computer Forensics?

- The victims
- Law enforcement agencies
- Insurance carriers
- Ultimately the legal system
- Who are the victims?
  - Corporations (profit or non-profit)
  - Government
  - Individuals

Why Is Evidence Important?

- Evidence is used to establish facts
- Forensic examiner is not biased.
- If you cannot present undeniable evidence, bad guys may walk away free
- In the legal world, evidence is ***EVERYTHING***

What is Computer Forensics?

- Investigation of a computer system or any device

  that contains a processor and memory in order to determine computer-related conduct:
  - ***who, what, when, where***, and ***how*** computer systems or devices are used.
- Goal: ***collect, preserve, filter***, and ***present*** computer system artifacts of potential evidentiary value
- Most challenges of computer forensics surround ***authenticity***.
  - Was the data altered?
  - What was the identity of the author?
  - Was the program that generated the data reliable?

Two Main Types of Requests

- ***Intrusion Analysis***
  - Who gained entry?
  - What did they do?
  - When did this happen?
  - Where did they go?
  - How did they do this?

Two Main Types of Requests (Cont.)

- ***Damage Assessment***
  - What was available for the intruder to see?
  - What did the intruder take?
  - What did the intruder leave behind?
  - Where did the intruder go?

Electronic Crime Scene Investigation

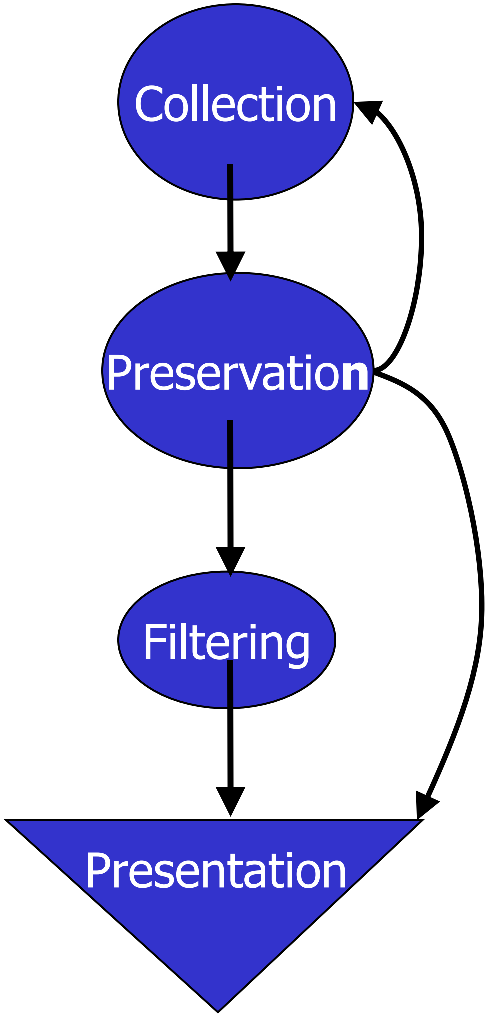
- Basic law enforcement training in crime scene investigation has long been limited to ***documentation and collection of physical evidence.***
- Computer forensics investigators focus on ***using computer knowledge and forensics techniques to identify evidence and generate leads*** to assist investigators to solve a criminal case.

Practitioners of Computer Forensics

- Federal, state and local law enforcement agents for criminal cases
- Legal service providers
- Corporate IT security personnel for criminal and civil cases
- Corporate HR investigators for workplace investigations
- Private investigators for various investigations
- Outside computer security consultants in incident response

Phases of Computer Forensics

- Four phases:
  - Collection
  - Preservation
  - Filtering
  - Presentation



Five Key Properties of Evidence

- ***Admissible*:** Evidence can be used in court
- ***Authentic*:** Able to show that the evidence relates to the incident in a relevant way.
- ***Complete*:** Collect not only evidence that can prove the attacker’s actions, but also evidence that may prove their innocence.
    - If you show the attacker was logged in at time of incident, you also need to show who else were logged in that time and why they did not do it.
- ***Reliable*:** Evidence collection and analysis procedures must not cast doubt on authenticity and veracity of the evidence.
- ***Believable*:** Evidence should be clearly understandable and believable to a jury.

Evidence Collection Guidelines

- Minimize handling and corruption of original data
  - Always work with secondary
- Account for any changes and keep detailed logs of your actions
  - Sometimes evidence alteration is unavoidable, then changes must be recorded in detailed logs
- Maintain the five key properties of the evidence
- Do not exceed your knowledge
  - If you are not sure what to do with the evidence, ***do not do it***. Either learn more before continue, or ask someone more knowledgeable for help

Evidence Collection Guidelines (cont.)

- Follow your local security policy
  - Failure to comply with local evidence collection policies may not only get you in trouble, but also the evidence you have collected may not be admissible
- Capture as accurate an image of the system as possible
  - Difference between original system and master copy should be minimized. Able to explain why the changes, if any, will not affect the case
- Be prepared to testify
  - Always remember you may need to testify later when you collect the evidence.

Evidence Collection Guidelines (cont.)

- Work ***fast***
- Proceed from volatile to persistent evidence
- Do ***not shutdown*** computer before collecting evidence
  - Shutting down computer may not only cause loss of volatile evidence, but also trigger startup/shutdown scripts to alter system configuration attacker put on the system before
  - Rebooting is even worse.
- Do not run any program on affected systems
  - May trigger some Trojan programs left by attacker to change or destroy the evidence.

Order of Volatility

Many evidence sources may be involved -- example of order of volatility list:

1. Registers and cache
2. Routing tables
3. ARP (**A**ddress **R**esolution **P**rotocol) cache
4. Process table
5. Kernel statistics [e.g., system call statistics] and modules [e.g., processors]
6. Main memory
7. Temporary file systems
8. Secondary memory
9. Router configuration
10. Network topology

Evidence Preservation

- Requires to show at least the following:
  - No information has been added or changed
  - A complete copy was made
  - A reliable copying process was used
  - All media was secured
- Pieces of evidence should be grouped and stored by cases along with the evidence notebook, where investigators log details of their actions, including at least the following:
  - Date and time of analysis
  - Tools used
  - Detailed methodology of analysis
  - Results of analysis

Digital Forensics Tools

- **SANS Investigative Forensics Toolkit – SIFT:** Multi-purpose forensic operating system http://computer-forensics.sans.org/
- **Digital Forensics Framework:** DFF is both a digital investigation tool and a development platform http://www.digital-forensic.org/
- **Open Computer Forensics Architecture:** Computer forensics framework for CF-Lab environment http://sourceforge.net/apps/trac/ocfa/wiki
- **The Sleuth Kit:** A library of tools for both Unix and Windows http://www.sleuthkit.org/
- **The Coroner's Toolkit:** A suite of programs for Unix analysis http://www.porcupine.org/forensics/tct.html

References

- Bill Nelson, Amelia Phillips, Frank Enfinger, and Christopher Steuart, *Guide to Computer Forensics and Investigations, 4th Edition*, Course Technology, Cengage Learning, 2009
- Michael E. Whitman, Herbert J. Mattord , *Principles of Information Security, 4th edition*, Course Technology, 2011
- Mark Stamp, *Information Security: Principles and Practice*, Wiley, May 2011, 606 pages, ISBN-10 0470626399
- Robert Beverly; Simson Garfinkel; Gregory Cardwell;, "Forensic Carving of Network Packets and Associated Data Structures,“ *Digital Investigation, 2011 the Eleventh Annual DFRWS Conference on*, vol. 8; 2011
- Hunt, R.; Slay, J.; , "Achieving critical infrastructure protection through the interaction of computer security and network forensics," *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on* , vol., no., pp.23-30, 17-19 Aug. 2010