

Computer Security and Forensics

Prem Uppuluri, PhD

Dept of Information Technology

Radford University

Material in these slides is based on the book: Brian Carrier, File System Forensic Analysis, Addison Wesley, 2005 (ISBN: 0-32-126817-2) or other resources (when noted).

Examples of where digital forensics is used.

- Civil and criminal prosecutions.
- Computer crime vs. using a computer to help in a crime.
- **Computer crime examples:**
 - Performed a digital event that violated a law (e.g., sending a threatening email/IM message or accessing data without authorization).
 - Launching a computer attack.
- **Using a computer to help a crime**
 - User researches Internet to commit a crime.
 - Fraud
 - E.g., Tax evasion.
 - Child exploitation/abuse
 - Gambling
 - Identity Theft

So how does digital forensics help?

Pre-requisites.

- Computer Security and Digital Forensics are closely tied fields.
- Some pre-requisites
 - An understanding of the web.
 - Concept of an Operating System (OS)
 - Using general purpose OSes
 - Windows, Linux
 - Basic concepts of computer networking.

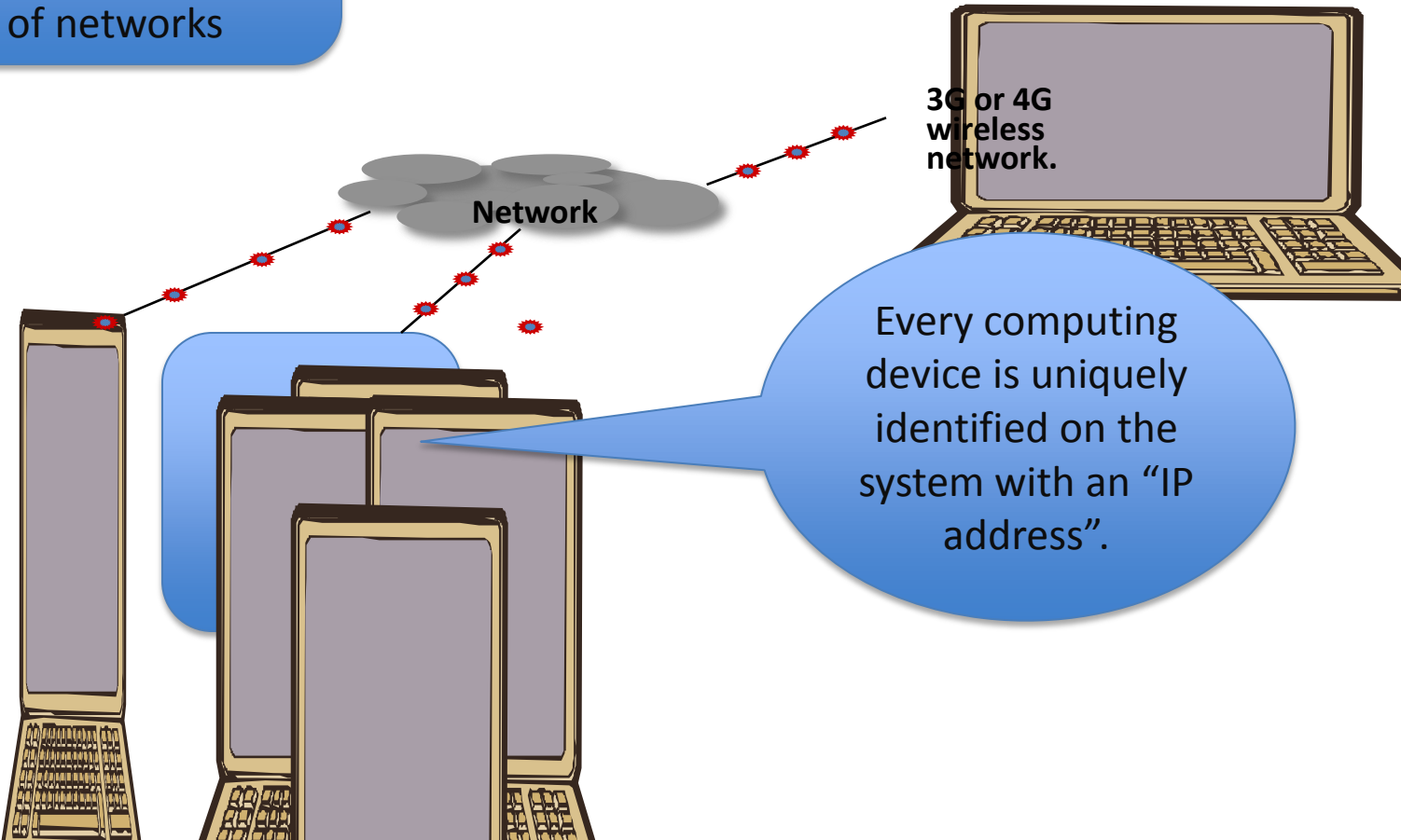
Some pre-requisites.

- Concept of files on a computer.
- Concepts of networking:
 - How do programs on our computers connect to programs on another computer across the Internet?

High level big picture of the internet

Internet is a large network connecting a variety of individual computing devices, LANs and other forms of networks

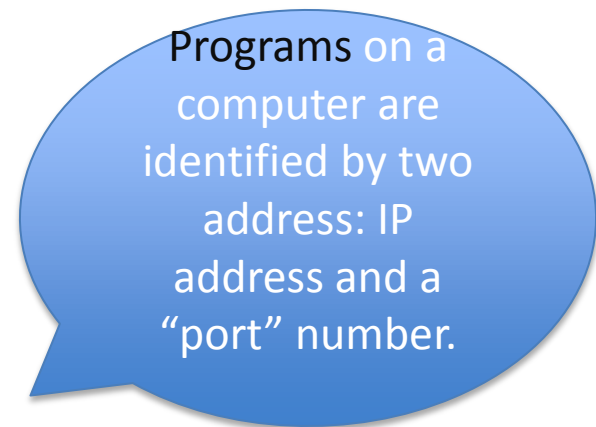
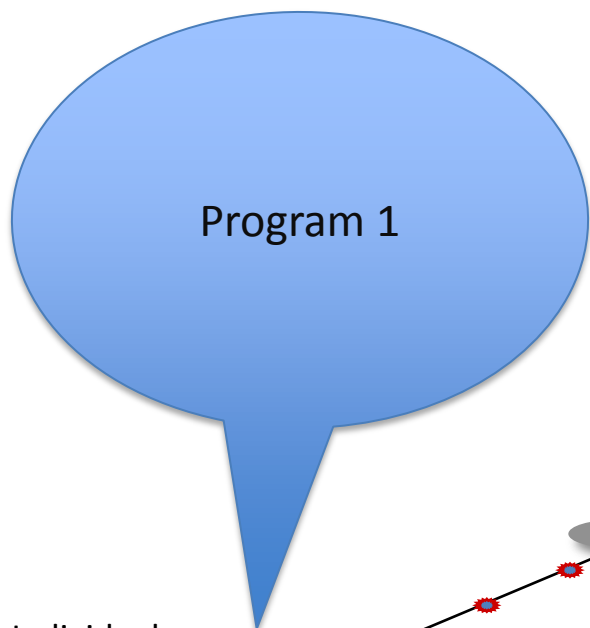
Individual desktops or devices



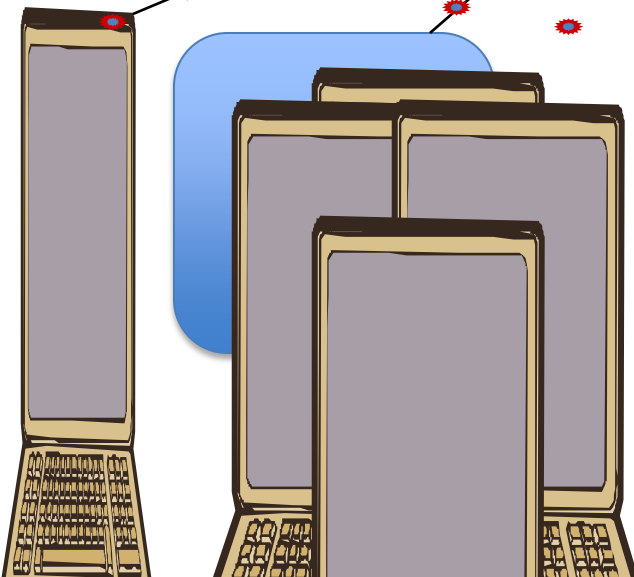
3G or 4G wireless network.

Every computing device is uniquely identified on the system with an "IP address".

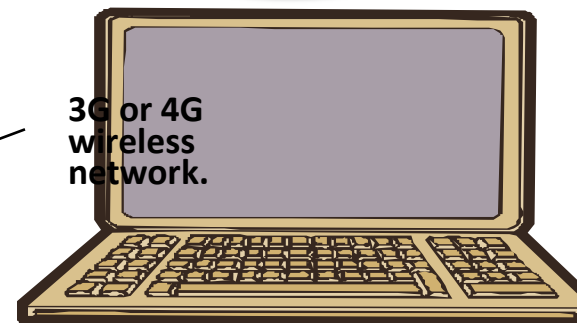
High-level view of how two programs communicate over the network.



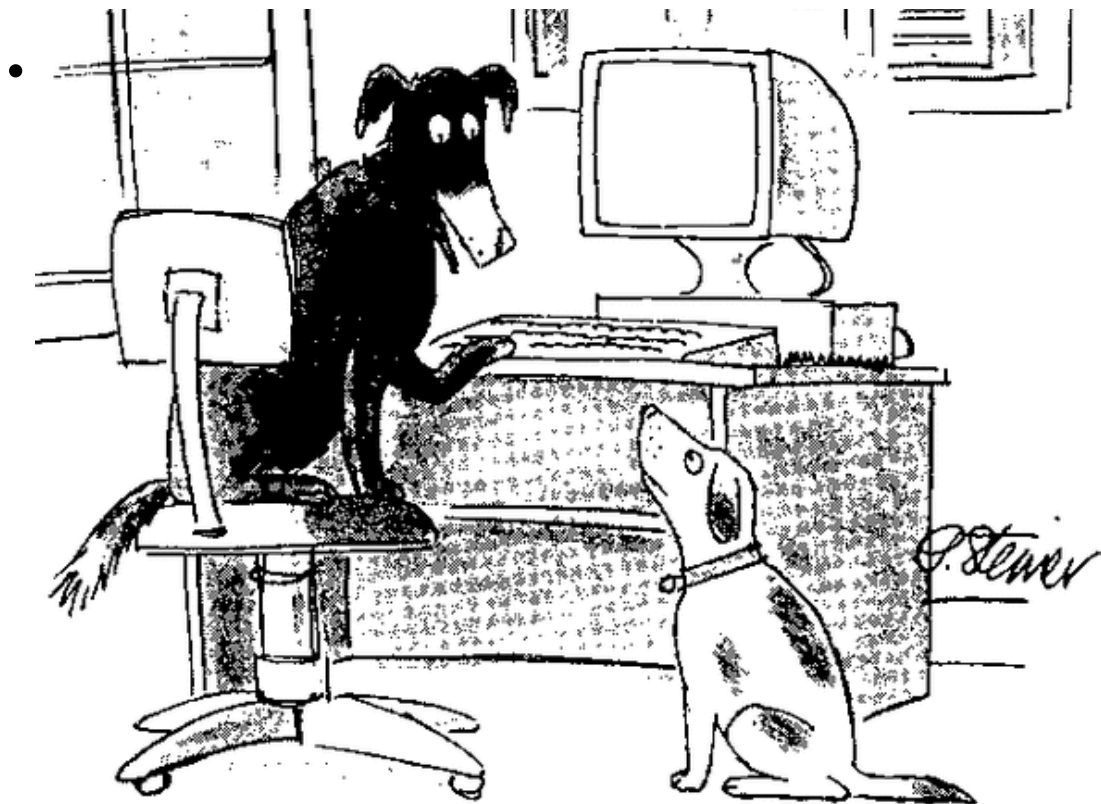
Individual desktops or devices



3G or 4G wireless network.



How does digital forensics work?



"On the Internet, nobody knows you're a dog."

A popular myth.

All activity on digital equipment (computers, smart-phones etc), leave **traces!**

Forensics is the art of finding these traces.

Cartoon © Peter Steiner, The New Yorker, 1994. Used here for educational purposes as per the fair use clause of the copyright law.

What traces? Some examples.

- Traces on the Internet:

- When you browse the Internet – what traces do you leave?

- An example: Go to the website: www.privacy.net to analyze information being leaked to the Internet.

- **Class exercise idea: See how much information is being shared about your computer by your web-browser?**



- File Traces:

- When a file is deleted, it is not “really” deleted!

- When we use the computer for various tasks – logs are made (to improve our experience and to keep track of last actions.)

- But these logs contain valuable forensics data.

- Next: volatility of traces.

Digital “breadcrumbs”: What are these traces?

- **Less volatile traces:**
 - Files (on the disk in flash ROM or memory cards).
 - Software installed on the system (e.g., used to find DVD pirating etc.).
- **Semi-volatile traces.**
 - Logs (e.g., log of computer network activity).
 - Web browser cache.
 - Web Cookies.
 - Chat message histories.
 - Commands that the user(s) executed on the equipment.
Software that the user(s) executed on the system.
- **Volatile**
 - Physical memory – usually lost if the device is powered down.
 - E.g., traces of spyware.
 - Network connections (e.g., to bittorrent websites)
 - Processes currently being executed.
 - Users currently logged in.

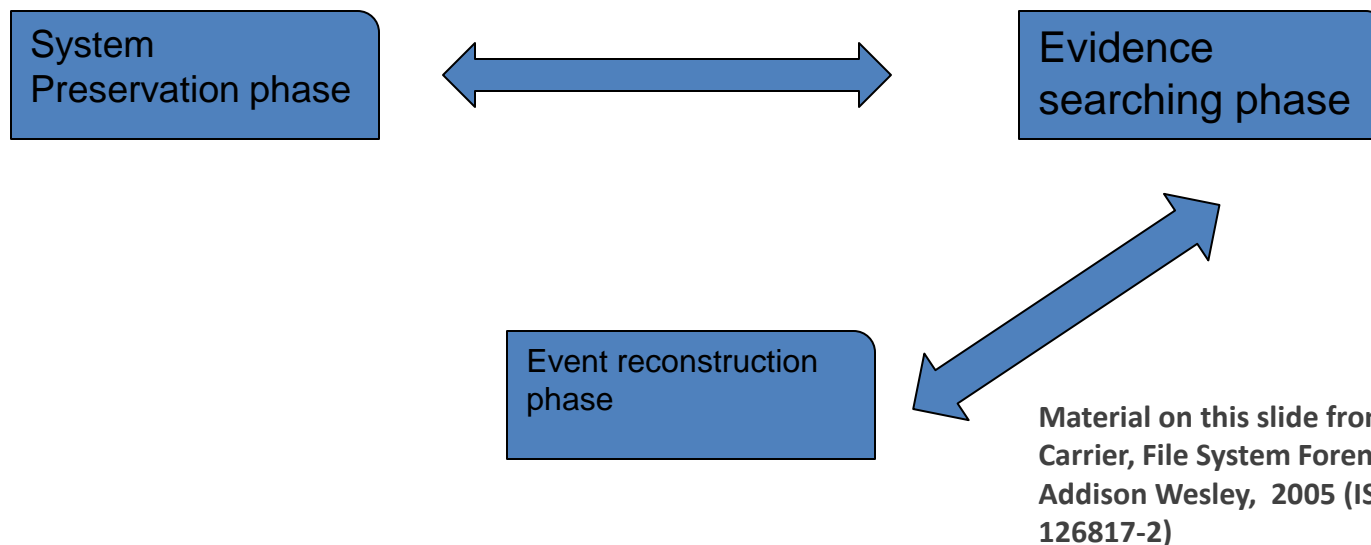
Material on this slide from: Brian Carrier, File System Forensic Analysis, Addison Wesley, 2005 (ISBN: 0-32-126817-2)

Rest of this session.

- Digital forensics process
- Traces on the
 - Web
 - Email
- Log files on computers.
- Dealing with deletion.
- Copying files and their attributes.
- Tracing network connections.

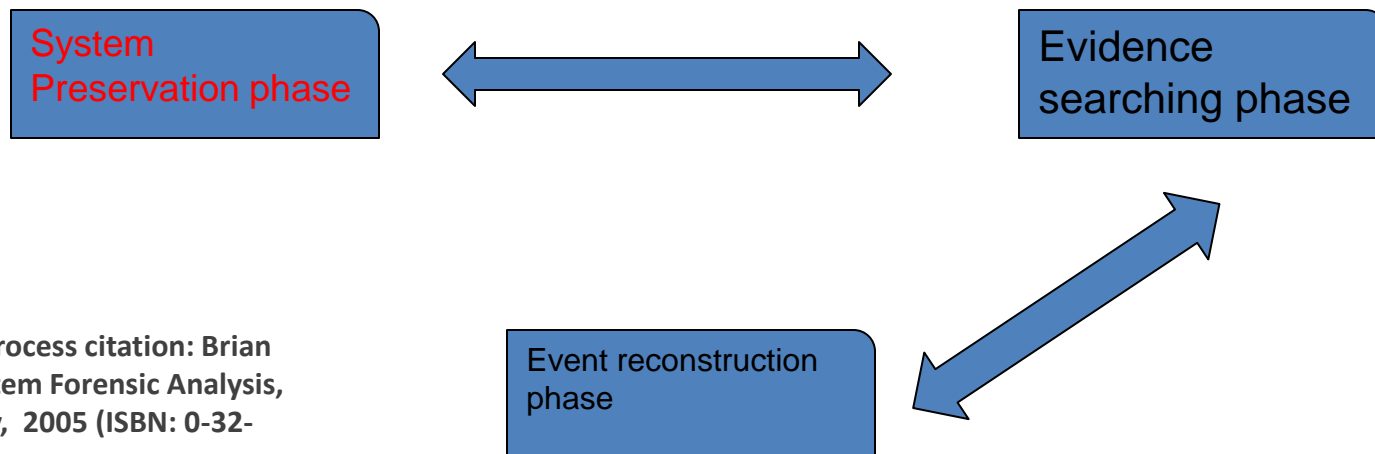
Overview of the Digital Forensics process

- Several approaches.
- Very similar to crime scene investigation.



Overview: system preservation.

- What needs to be preserved during the preservation phase? What is evidence?
 - Depends on the crime.
 - Examples (citation: “Best Practices” pocket guide by the Dept. of Homeland Security)
 - stand alone home computer
 - Location of the cables
 - PDA cell phones
 - Memory cards (e.g., SD card), phone cards (e.g., SIMM cards).



Evidence that may need to be preserved.

- Physical aspects
 - Number of network connections.
 - Type of network connections (Wireless/Wired)
 - Cables – location of cables.
 - Access restrictions (physical).
 - Current content of the computer screen.
- Why is this evidence important?
 - Who has access to the computer?
 - How does the computer connect to the net?
 - Are there any external devices?
 - Printers?
 - For some crimes – what was being done on the system?
- **Class exercise idea:** A walk-through of a computer lab



Example: Open Wi-Fi connections

- War driving and piggybacking of Wi-Fi connections is quite common.
- Criminals can use open wi-fi to access internet.

Evidence that may need to be preserved (2).

- Technological aspects
 - Volatile evidence:
 - Programs currently running on the computer.
 - Class exercise: using software such as: Windows Task Manager, identify different programs.
 - E.g., Press Ctrl + Alt + Del to invoke task manager
 - Network connections made by the computer.
 - Run the program **netstat** as follows:
 - » On Windows → Start → Run
 - » Type cmd.
 - » Type netstat -aen
- Class exercise: take snapshots of
 - processes currently executing.
 - network connections currently being made by the computer.
- Example resource: www.hackerhighschool.org
- Free lessons available for teaching high school students.



The exercise ideas on this slide and others are from hackerhighschool.org (Lesson 8: digital forensics – with some modifications by Prem Uppuluri).

Evidence that may need to be preserved (3).

- Technological aspects

- Non volatile data.

- Preserving Files

- Class Exercise: Make a copy of the hard drive.

- Why is a simple copy and paste operation on file not enough to preserve it?

- » Files contain certain “meta” attributes: who created it, when was it first created, when was it last modified etc.

- » Such data will be lost in a copy-paste operation.

- Solution: use forensic tools that preserve such meta-data.

- Examples: http://www.cftt.nist.gov/disk_imaging.htm



The exercise ideas on this slide and others are from hackerhighschool.org (Lesson 8: digital forensics – with some modifications by Prem Uppuluri).

Evidence preservation challenges.

- Challenge 1: To shutdown or not to shutdown.
- How to shutdown?
 - Clean vs. Dirty
 - e.g., through shutdown menu option or by pulling the power source?.

Evidence preservation challenges (2).

- Challenge 1: To shutdown or not to shutdown.
 - Depends on the context.
 - E.g., Dept. of homeland security (DHS) recommendation:
 - Desktops/laptops etc. – shutdown after photographing the screen.
 - Cell phones/PDAs/smart phones: do not shutdown.
- How to shutdown?
 - Clean vs. Dirty
 - e.g., through shutdown menu option or by pulling the power source.
 - In some contexts, DHS Recommendation: pull the power cable.
- Challenge 2: How to ensure evidence is not tampered with?
 - Use cryptographic hashes – mathematical functions that generate a condensed signature of electronic data. If the data is tampered, signature will not match.

Evidence preservation?

- Challenge 2: Preserving evidence
- Use of cryptographic sums.
- Free tools available to compute the cryptographic sums.
 - E.g.,: <http://www.fastsum.com/support/md5-checksum-utility-faq/md5-checksum.php>

The exercise ideas are from hackerhighschool.org (Lesson 8: digital forensics – with some modifications by Prem Uppuluri).

Evidence searching and acquisition phase

- Where can we search for evidence?
 - Depends on what we are looking for.
- Here are some common data to look for:
 - Documents on the computer
 - E.g.,
 - Documents used to store financial data.
 - Meta-data on the documents.
 - E.g., when was the file created? Who created it?
 - Log files (log of activities)
 - E.g.,
 - Email cache – to get the specific email sent.
 - Chat history cache – if IM was used.
 - Temporary files from the Internet
 - Web browser cache – to identify a user's internet activity.
 - Web Cookies

The exercise ideas are from hackerhighschool.org (Lesson 8: digital forensics – with some modifications by Prem Uppuluri).



Evidence searching and acquisition phase (2): Documents on the computer.



- Documents to look for include:
 - PDF files, .doc(x), .txt, .xls etc...
 - Class exercise: Ask students to identify files based on their extensions.
- Sometimes documents are “hidden”. Examples
 - by changing their extension – trying to trick someone.
 - Solution: Files have sig
- Look at meta-data on files in question to get idea about time-lines and ownerships.
 - E.g., when did a person visit a specific website?
 - Files on electronic equipment have lot of “attributes”.
 - Not always easily visible to user.
 - Example attributes:
 - Modification time of a file.
 - Creation time of a file.
 - Size.
 - Ownership (who created the file – in a multi user environment).
 - Access rights (who can access a file and with what permissions).
 - Many of these attributes are lost when files are copied!

The exercise ideas are from hackerhighschool.org (Lesson 8: digital forensics – with some modifications by Prem Uppuluri).

Evidence searching and acquisition phase (2): Documents on the computer.

- 
- Documents to look for include:
 - PDF files, .doc(x), .txt, .xls etc...
 - Class exercise: Ask students to identify files based on their extensions.
 - Sometimes documents are “hidden”. Examples
 - by changing their extension – trying to trick someone.
 - Solution: Files have signatures.
 - Class exercise: Ask students to find the signature of a Microsoft Word document.
 - By giving them strange file names.
 - E.g., in UNIX (Mac OS, Linux): Files with a “.” (dot) in front become hidden files.
 - Solution: Use the “search” tool to find such files
 - Needle in a haystack issue: what if there are too many files.
 - Use “search” effectively. E.g., the “find” program in UNIX.
 - What if the files were deleted?
 - Files are hard to “actually” delete.
 - Use file restoration software: Class exercise: students try to recover deleted files using “Directory snoop”: <http://www.briggsoft.com/dsnoop.htm>
- 

Evidence searching and acquisition phase (3): Meta-data on files

- Look at meta-data on files in question to get idea about time-lines and ownerships.
 - E.g., when did a person visit a specific website?
 - Files on electronic equipment have lot of “attributes”.
 - Not always easily visible to user.
 - Example attributes:
 - Modification time of a file.
 - Creation time of a file.
 - Size.
 - Ownership (who created the file – in a multi user environment).
 - Access rights (who can access a file and with what permissions).

The exercise ideas are from hackerhighschool.org (Lesson 8: digital forensics – with some modifications by Prem Uppuluri.)

Evidence search and preservation phase (4):

Log Files

- Every operating system, maintains several logs
 - Examples:
 - Log of past commands executed
 - Log of web history.
 - Log of accesses to the computer.
- Example logs:
 - Web site histories
 - Not only sites visited.
 - But can be used to re-construct what was visited.
 - Histories are also stored by search engines.
 - Chat histories (e.g., using a chat engine – history of chat messages).



Evidence search and preservation phase (5): Temporary files from the Internet

- Examples: Cookies.
 - What is an Internet cookie?
 - Help track websites visited.
 - Class exercise: identifying cookies and along with them websites visited.



The exercise ideas are from hackerhighschool.org (Lesson 8: digital forensics – with some modifications by Prem Uppuluri).

Event reconstruction.

- Similar to crime scene investigation.
 - List of programs
 - List of network connections
- Example: Operation Aurora.

Event reconstruction example:

Operation Aurora.

- Name given by McAfee Inc.
- Attack on various companies (Google, Adobe and 20 or more companies etc.) (citation for attack description: Dennis Fisher, January 19 2010, Threatpost.com)
 - **Objective:** gain access to google accounts (among other things) of human rights activists (speculation at this point).
 - Attack initiation traced to hackers in China by VeriSign.
 - Attack used **Malware**
 - Stands for “**Malicious software**”. E.g., Viruses, Spyware.

Event reconstruction of Operation Aurora.

- Please note:
 - This may or may not be exactly how the events were reconstructed.
 - I pieced these based on my expertise and information available from VeriSign Inc. and McAfee Inc (two companies involved with investigating this attack).

Example of how traces are used:

Operation Aurora (2).

- Once attack was detected, here is the evidence found:
 - Step 1: Users within company (Google) visited certain suspicious websites.
 - Conclusion: Maybe a “Phished” website (a fake website that has the look and feel of the real one).
 - Step 2: Why did the users visit the phished website?
 - Evidence: users got an email from a colleague with a link to the phished website.
 - Conclusion: Must have been a spoofed email!

Example of how traces are used:

Operation Aurora (3).

- Step 3: Phished websites usually download some malicious software.
 - Evidence: malicious software found on the computer.
- Step 4: Analyzing the malicious software (based on information from McAfee):
 - Run the malicious software in test lab.
 - See the network connections it makes.
 - Trace the connections to the destination computers.
 - Sniff the data being sent over the network connections – will tell us the payload being sent.

Example of how traces are used:

Operation Aurora (4).

- Step 5: Continue evidence collection on the destinations identified and finally trace the perpetrator.
 - E.g., by tracing ip addresses.
 - Having IP address also gives other information:
 - E.g., route to reach that computer.
 - Class exercise: have students find the route taken to reach a specific computer.

So what does someone study to get into digital forensics?

- Many options, here is what I recommend:
- A diploma in Information Technology or Computer Science.
- Knowledge of computer networking.
- A certificate in Forensics.

Resources to teach Security/Forensics

- National Cyber security alliance:
www.staysafeonline.org
- Cyber patriot www.highschoolcdc.com
- Hacker High School:
www.hackerhighschool.org