Week 10: Introduction to Digital Forensics

Ayman El Hajjar

Email: a.elhajjar@westminster.ac.uk
Twitter: @azelhajjar

6COSC002W - Security and Forensics

22 March 2021

University of Westminster

Session Overview

1. Digital Forensics
2. Identifying file, program and storage anomalies
   - Evidence Gathering Measures
   - Physical & Logical Analysis
3. Forensics imaging
4. Learning to handle the evidence
   - Shutting Down the computer
   - Transport
   - Preparation
   - Documentation
   - Mathematical Authentication of Data
5. Learning to handle the evidence

Computer Forensics

What is digital forensics

Digital forensics is generally held to be about retrieving and using Digital Evidence. This might be data recovered from a computer hard drive. It might also include data from:

- Computer/laptops/tablets/mobile phones
- External storage devices such as usb pendrive, sd cards, etc..
- Network devices
- Any other device that stores data

Several Reasons for conducting a forensic investigation such as:

- To find evidence where a crime has been committed
- To find out how a system was compromised (Hacked)
- To identify inappropriate user access to a system

What is digital forensics (Cont.)

Intro

Data can be either

- Hidden from normal users but available if you know where to look
- deleted but recoverable given the right expertise and tools

- A wide variety of forensic tools available to help with the process of data recovery from devices where the data has been logically deleted from the device.
- Data is rarely physically deleted unless it is overwritten by some other data.
- This is true even if partitions are deleted or disks are formatted.

Identifying file, program and storage anomalies

- Encrypted, compressed and graphics files stored data in binary format.
- As a result text search programs cant identify text data stored in these file formats.
- These files require manual evaluation, which may involve a lot of work especially with encrypted files.
- Reviewing the partition on seized hard drives is also important.
- Evaluating hidden partitions for evidence and document their existence.

Evidence Gathering Measures

- Avoid changing the evidence: Forensic specialists should also make exact bit by bit copies,storing the copies on an unalterable medium such as a CD Rom or DVD Rom.
- Determine when evidence was created: Timelines of computer usage and file accesses can be valuable sources of computer evidence.
- Search throughout a device: this includes emails, temporary files, swap files, logical file structure and slack and free space.

Evidence Gathering Measures

- Determine information about encrypted and stegnized files: Investigators should usually not attempt to decode files at first. Rather should look for evidence in a computer that tells them what is in the encrypted files.
- Present the evidence well: Investigators must present computer evidence in a logical compelling and persuasive manner.

Logical Analysis

- Logical Analysis involves using the native Operating System, on the evidence disk or a forensic duplicate, to pursue the data.
- Logical analysis is looking for things that are visible, known about, and possibly controlled by user.
- Logical file and directory structure must be examined to reconstruct what the user was doing with his/her computer.

Logical Analysis

- Logical analysis will not give you a signed confession but it can give you an idea of what the computer has been set up for.
- For example a programmer optimize computer for speed, a pornographer for storage and a stalker for messaging.
- Divide the data into layers and try to find information at each layer that can be used as evidence.
- Look for peculiarities on each layer and then choose the right extraction tool.

Physical Analysis

- Physical analysis is looking for things that are looking for things that may have been overlooked or are invisible to the user.
- The user may have attempted to delete files and you want to reconstruct those files.
- You should index the different kind of file formats.

Physical Analysis

- The file format you start with depends on the type of case.
- For example you might want to start with graphics file format if the case is a forgery case.
- Forgery criminals rarely go into trouble of removing header information, so it is an easy matter of finding for example one graphics header at the beginning of a JPEG file and doing a string search for all other graphics of that type.

Physical Analysis: SWAP file and Unallocated space

- swap file
  - Swap file is a place where an investigator should physically analyse
  - A swap file is the most important type of ambient data.
  - A swap file is like a scratch pad to write data to when additional RAM is needed.
- Unallocated space
  - Unallocated space or free space is the area of a hard drive that has never been allocated for file storage.
  - The only way to clear unallocated old fragments is with cleansing devices known as sweepers or scrubbers.

Storage Formats

- Once you have acquired a physical storage medium of some type, you need to image it.
- You should always work with an image.
- it is possible to create a forensic image utilizing open source tools, specifically Linux commands.
- You must forensically wipe the target drive to ensure there is no residual data left from a previous case.

Storage Formats: DD tool

- you can use dd command to zero bit the target drive
  - dd if=dev/zero of=/dev/hdb1 bs=2048
- It is now time to copy the victim/criminal hard drive bit by by bit to your target drive
  - dd if=dev/sda1 of=/dev/sdb1 bs=2048
  - Where sda1 is the hard drive you are copying and sdb1 is your target drive

Handling evidence procedures

- It is important to follow proper procedure when examining a suspect machine.
- In this section we will cover specific details on the proper procedure to follow when collecting, seizing and protecting evidence.
- Below are the main procedures.
  - Shutting Down
  - Transport
  - Preparation
  - Documentation

Shutting Down the computer

- At some time, it was recommended that the first step to analyse the computer was to switch it off to avoid further damage.
- This now perceived as not advisable.
- It is now apparent that valuable evidence can be lost if computer is switched off.

Shutting Down the computer

- At some time, it was recommended that the first step to analyse the computer was to switch it off to avoid further damage.
- This now perceived as not advisable.
- It is now apparent that valuable evidence can be lost if computer is switched off. Why ?

Shutting Down the computer

- At some time, it was recommended that the first step to analyse the computer was to switch it off to avoid further damage.
- This now perceived as not advisable.
- It is now apparent that valuable evidence can be lost if computer is switched off. Why ?

Shutting Down the computer

- At some time, it was recommended that the first step to analyse the computer was to switch it off to avoid further damage.
- This now perceived as not advisable.
- It is now apparent that valuable evidence can be lost if computer is switched off. Why ?
  - Important data /evidence can be located in a process or several processes running or in memory.

Shutting Down the computer

- At some time, it was recommended that the first step to analyse the computer was to switch it off to avoid further damage.
- This now perceived as not advisable.
- It is now apparent that valuable evidence can be lost if computer is switched off. Why ?
  - Important data /evidence can be located in a process or several processes running or in memory.or

Shutting Down the computer

- At some time, it was recommended that the first step to analyse the computer was to switch it off to avoid further damage.
- This now perceived as not advisable.
- It is now apparent that valuable evidence can be lost if computer is switched off. Why ?
  - Important data /evidence can be located in a process or several processes running or in memory.or
  - It may be the case that he computer is using drive encryption.
- Steps to shut down computer are shown in next slide.

Steps to shut Down the computer

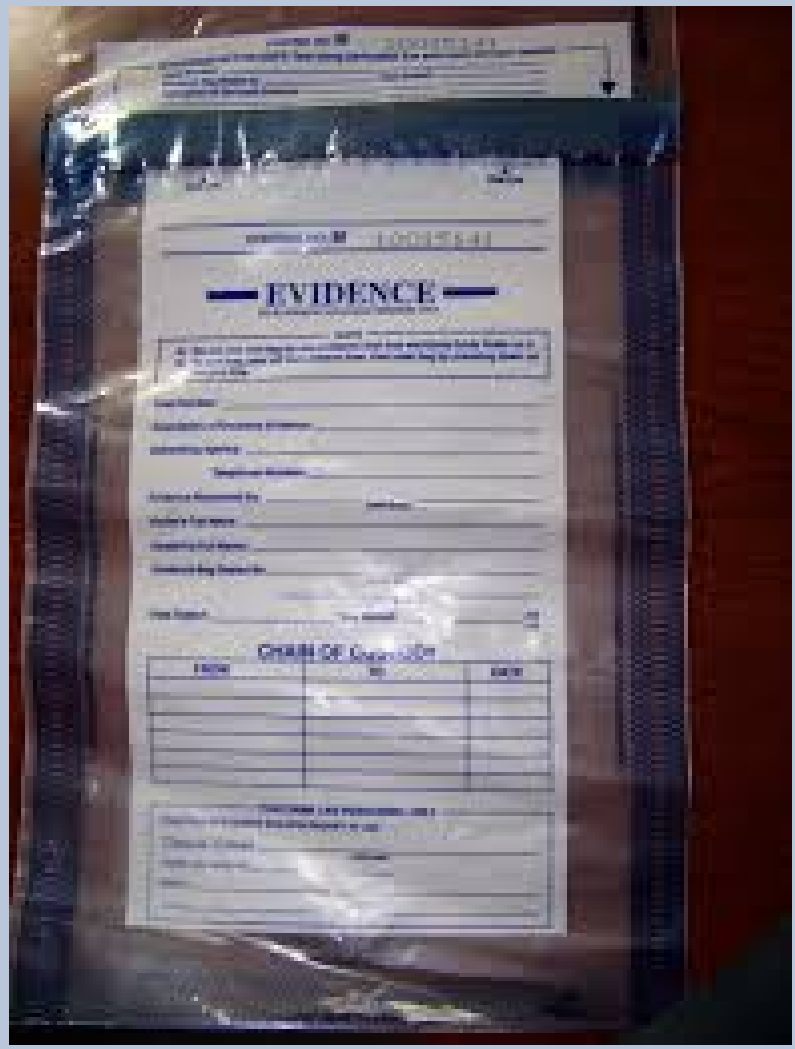
1. Check for running processes.
   - For Windows: press **ctrl+alt+Delete** then select task manager.
   - For Linux: In command line, type **top** or **ps -aux**
2. Take a picture of all your running processes output.
3. Check if live connections to this computer are running
   - Using **netstat**, we can obtain network statistics and any current connections
   - using **net sessions** command is more useful than netstat. net sessions only shows established network communication sessions. **net sessions** alternative for Linux is **who**
   - **openfiles** command tells you if any shared files or folders are open and who has them open.
4. Take a copy of the system memory contents in case it is needed at a later time.Magnet RAM memory capture tool

Transport

- Seized computers or victims computers are often stored in less than secure location.
- A computer that is left unattended can easily be compromised
- Anyone could plant evidence or destroy crucial evidence.
- During the transport, you must be aware that this seized computer is evidence.
- Any period of time that you cannot account for the evidence is a break in the chain of custody.

Preparation

- If the device you have seized is a computer, you need to remove the drive(s) from the suspect machine.
- Prepare a chain of custody form for removed devices. Example of chain custody form is shown in the figure to the right.



Documentation

- It is important to take pictures of the computer from all angles to document the system hardware components and how they are connected.
- You should also record BIOS (**B**asic **I**nput/**O**utput **S**ystem) information or UEFI (**U**nified **E**xtensible **F**irmware **I**nterface) in newer systems.
- It is important to record specifically the time and date of the system.
- File system is also important as different file systems use different timing zone. NTFS stores Greenwich mean time.

Mathematical Authentication of Data

- You must be able to prove that you did not alter any of the evidence after taking possession of a suspect computer.
- After imaging any drive, you must always create a **hash** of the original copy.
- Compare hashes before you take any work on the image.

Mathematical Authentication of Data

- You must be able to prove that you did not alter any of the evidence after taking possession of a suspect computer.
- After imaging any drive, you must always create a **hash** of the original copy.
- Compare hashes before you take any work on the image. They should match.
- You must document what hashing algorithm you used (SHA2 is the most used one nowadays).
- Most forensic tools can record the hash of drives.
- Linux has a built in a hashing command.

Mathematical Authentication of Data

- You must be able to prove that you did not alter any of the evidence after taking possession of a suspect computer.
- After imaging any drive, you must always create a **hash** of the original copy.
- Compare hashes before you take any work on the image. They should match.
- You must document what hashing algorithm you used (SHA2 is the most used one nowadays).
- Most forensic tools can record the hash of drives.
- Linux has a built in a hashing command. The command is **md5sum /dev/hda1**
- You can also send your hash to a target machine such as "Forensic Server", you can use **md5sum /dev/hda1 | nc 192.168.0.2 8888 -w 3**
  - NOTE: IP address, port number and partition name are

Learning to handle the evidence

- Digital evidence is fragile.
- Can be destroyed or tampered with easily.
- For evidence, a simple opening a file can cause it to change.
- Digital evidence may also degrade over time.
- A single out-of-place bit can raise questions about its authenticity and its admissibility.
- To ensure that this does not happen, as investigators, we need to adhere to a set of fundamental rules.
  - Rule 1: Never mishandle the evidence
  - Rule 2: never work on the original evidence or system
  - Rule 3: document everything

Handling evidence- Rule 1: Never mishandle the evidence

- Evidence has to be handled with extreme care.
- The objective is to minimize any disruptive contact with the evidence.
- When it is essential for the investigator to interact with the evidence, it must be done in a manner that is least intrusive and completely documented.

Handling evidence- Rule 2: never work on the original evidence or system

- Any interaction with the original evidence in digital form causes the evidence to be compromised.
- Metadata such as dates and time stamps on files change almost instantly.
- The suspect system should never be used to carry out an investigation.
- Not only does that compromise the evidence, but it also adds to the risk of the evidence being manipulated / deleted / damaged / destroyed.
- The recommended process is:
  - Create a forensic copy of the digital evidence
  - Ensure its authenticity vis-à-vis the original
  - Carry out your investigations in a write-protected manner

Handling evidence- Rule 2: never work on the original evidence or system

- Any interaction with the original evidence in digital form causes the evidence to be compromised.
- Metadata such as dates and time stamps on files change almost instantly.
- The suspect system should never be used to carry out an investigation.
- Not only does that compromise the evidence, but it also adds to the risk of the evidence being manipulated / deleted / damaged / destroyed.
- The recommended process is:
  - Create a forensic copy of the digital evidence
  - Ensure its authenticity vis-à-vis the original
  - Carry out your investigations in a write-protected manner

Handling evidence-Rule 3: document everything

- In forensics, any evidence is only as good as the process followed to obtain it.
- Unless proper processes with the correct precautions are followed the process of acquiring and authenticating the evidence may be flawed until we have a clear-cut documentation attesting to the fact.
- A comprehensive chain of custody, or CoC as it is known, has to be followed, where a detailed record is to be maintained vis-à-vis every exhibit and who had it in custody at any specific period of time.
- Hash values should be maintained and rechecked every time the exhibit changes hands.

References

- Lecture notes were compiled (Texts and figures) from the System Forensics, investigation and response book for by Chuck Easttom
- Contents compiled from Recommended book **Network forensics by Ric Messier** chapter 4 and 5
- Some slides are compiled from the further reading book **Assessing Network Security** By Ben Smith, Kevin Lam, David LeBlanc- Penetration testing for Intrusive attacks chapter.
- you can find those books in the reading list of the module on Blackboard.