Johnny Zhong
Week 2 Write-Up
CS373 – Defense Against the Dark Arts

Week2 – Advanced Forensics

Focus: Incident Response

Remove threat, determine remaining issues, collect evidence.

Timeline:

Can we replicate the sequence of events? Can we explain what happened?
Analysis of memory is on the rise.

Cliff Stohl (The Cuckoo's Nest) – administrator who discovered missing money. First recorded incident response.

When do we conduct Forensic Investigations?

- Fraud
- Intellectual Property Theft
- Inappropriate Use of Internet
- Child Exploitation
- E-discovery (Litigation)

Forensic Computing describes a method to determine what happened on a system. This is done through 3 steps: evidence acquisition, investigation and analysis, then reporting results.

Legality

Forensic Investigators do not determine if an individual is guilty. An Investigator is only responsible for demonstrating what happened on the system.
In addition, Investigators look into only what the case involves, nothing further. Isolation of data, such that it does not intrude on the privacy of others, is often necessary.

Evidence Acquisition

In the past, forensics was performed post-physical system acquisition. This would commonly involve impromptu shutdown of the machine. Now, much of the forensics is performed live, referred to as "live forensics". Live Forensics allows Investigators to obtain a memory dump to evaluate later.

Investigation and Analysis

The memory dump, if acquired, and other files are evaluated using analysis tools and techniques. This includes, but is not limited to, replication of behavior and evaluation of file checksums.

Reporting Results

The evidence must be presented in such a way that a layman is able to understand what had transpired and what was found. The report should be solid. It's commonly reviewed by a colleague and then an attorney.

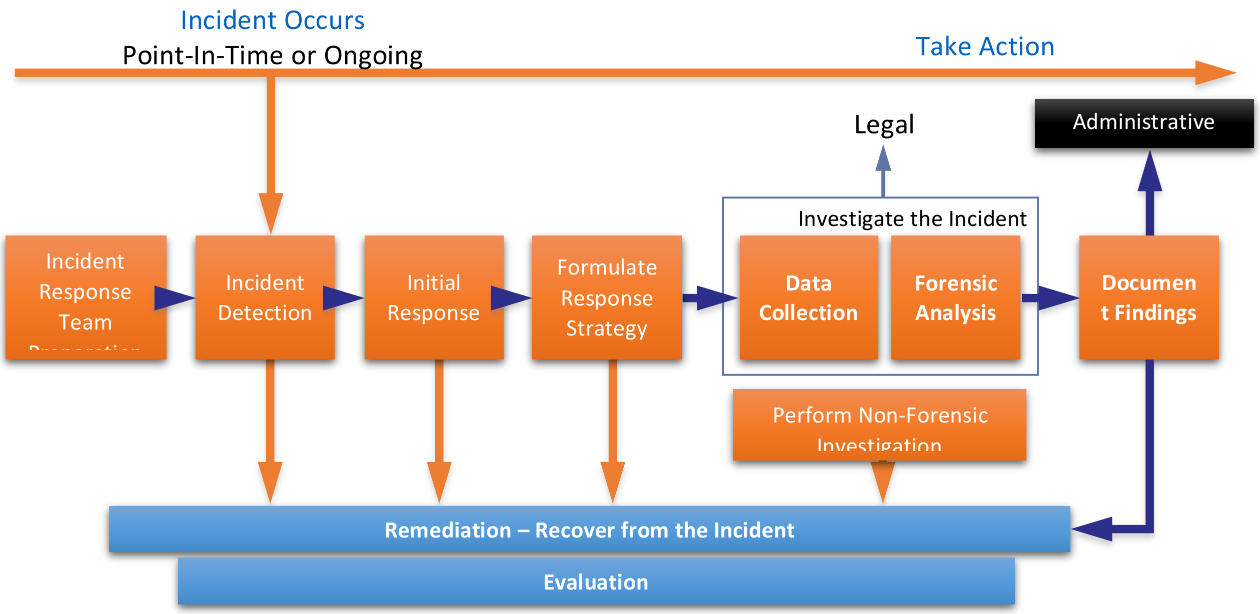
Forensics in a Nutshell:

- Identify Evidence
    -
- Preserve Evidence
- Analyze Evidence
- Present Results

Some tips:

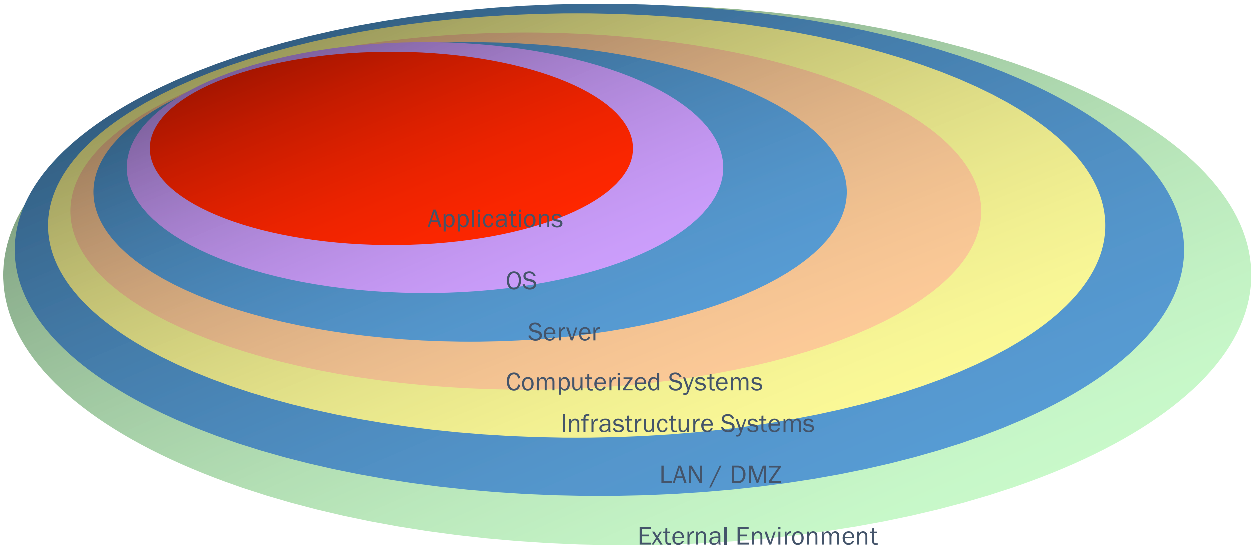
- Minimize data loss
- Record everything done during analysis
    - start with time, physical and system time
    - if a team is used, generally one person is designed by a writer
    - paper and pen is still commonly used
- Analyze all the data
    - can be any source (smart TV, GPS)
    - most education is based around desktops, hard disk drives
    - may require physical override in order to bypass security
    - security can be bypassed using GPUs (as a password cracker)
- Report Findings
    - Evidence is anything you can prove or disprove
    - Much evidence comes in registry, files, memory, databases (physical evidence like CDs and flash drives)
        - Challenge can be in how much data there is to analyze
        - can be mitigated by searching checksums
        - SSDs represent a new challenge for forensic analysis
    - Triage: the ability to prove or disprove an event in multiple ways
        - Look in the registry
        - OS log files
        - Sql log files
        - Database (user added)

Incident Response Process



- Dependent on the situation, first action might be to stop the incident or monitor.
- Incident response team is oftentimes ad-hoc, generally untrained and unpracticed. Training can be performed with a red team/blue team practice

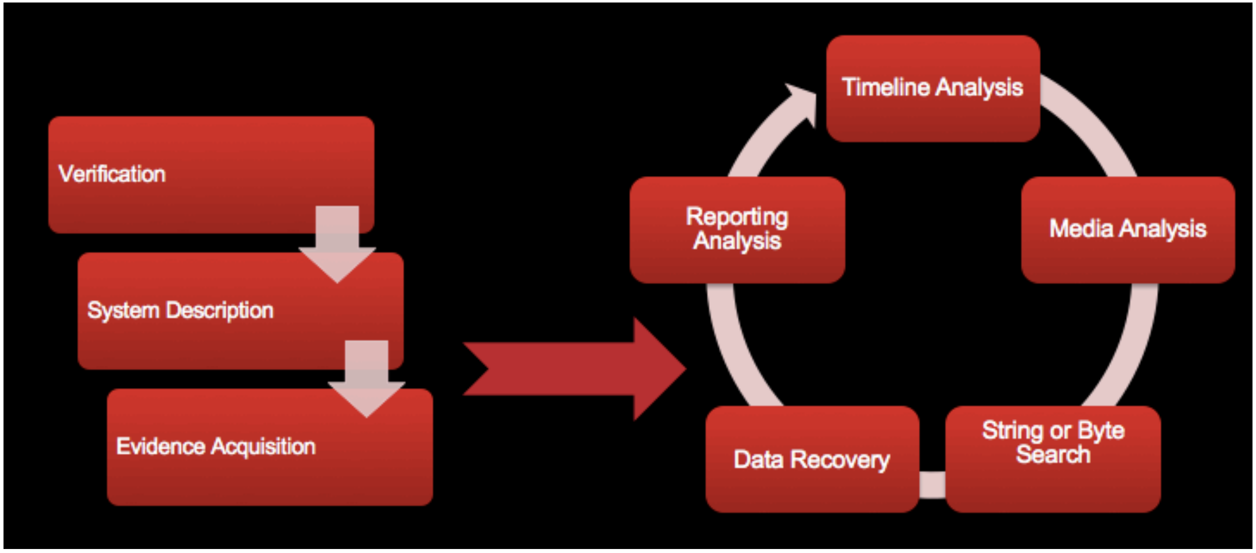
Evidence Lifetime



Evidence in the central circle tends disappear quickly, as opposed to the other environments. Data quickly disappears inside inner circles.
Issues that happen when investigating systems further out in the circle:

- Data is less specific to the case at hand, privacy (logs that have nothing to do with your case)
- Amount of data is huge
- Normalized timelines
- Skills of investigators, dependent on all systems in place
- Tools necessary, dependent on how many systems are investigated

Forensics Lifecycle (of Reporting)



Locard's Exchange Principle

When two objects are in contact with each other, they will leave evidence.

"Once contaminated, it stays contaminated and remains compromised evidence."

Because of this, investigator actions must be recorded in order to comprise a chain of custody of the evidence.

Order of Volatility

When collecting evidence, we should proceed from most volatile to least volatile, in order to gather the most amount of data. (RFC 3227)

A typical ordering looks like:

1. System Memory
2. Temp files
3. Process Table and Network Connections
4. Network Routing Information/ARP Cache
5. Forensics Acquisition of Disks
6. Remote Logging and Monitoring Data
7. Physical Configuration and Network Topology
8. Backups

Between steps 4 and 5, we can begin to disconnect the machine.

FTKImager Lab Notes

Use a toolkit (in the form of a write protected USB or CD) to run forensic applications.

Write results and other files to a location outside of the machine (network shares, other USB sticks).

Memory dump applications do not ignore themselves, this can be a risk if memory is swapped out. Many specialized tools use very little memory to help mitigate this risk.

FTK Imager – a data preview and imaging tool to acquire data.

Instructions and notes from the lab:

File -> Create Image -> Select Format

DD – compatible with linux

E01 – Encase is the preferred format for law enforcement agencies

Volatility Lab Notes

- basic syntax: volatility.exe (or .py) –f <memory_dump_filename> <plugin>
- Memory dump analysis (and can create memory dumps, but there are other smaller tools)
- OS agnostic
- First step: determine configuration (Windows version) using imageinfo:
  - plugin that determines the configuration of the source of the memory dump based on format and file structure from the memory dump
  - provides information to other plugins (some plugins don’t work with certain configs)

  - takes a while, dependent on size
  - provides suggested profile, image date and time (from the machine that took the memory dump)
- Can be run from cmd
- Many plugins available (like tools in a toolkit)
- Second step: psscan
  - Syntax: volatility.exe –f <filename> --profile=<profile_string> psscan
  - Looks in the memory dump to determine what processes were running on the system at the time of the memory dump.
  - Suggested that we write process IDs down. This is to track the behavior of processes, parent and child.
  - Recommended to send output to a txt file.
- Other critical plugins: dlllist (get list of dlls provided process was using), netscan (look at network activity), deskscan (look at desktop activity), getsids (determine which user rights the malware used)

Advanced Forensic Methods and Tools

- USB and peripheral devices have signatures which are recorded to the registry upon insertion. This can be used to determine if and when a device was plugged in.
  - These things can be pulled using a “RegRipper”, which pulls registry information in a similar fashion to memory dumps.
  - RegEdit is the default tool in Windows.
- Registry Investigation
  - autorun location in registry commonly altered, as malware wants to survive a reboot and does not want to depend on user input or alert a user to its existence.
  - Provides when files were accessed, created, deleted,
- Page Files, Index files
  - Internet explorer files
  - Firefox runs a SQLite server for history
- Application, Configuration, and Logfiles, Prefetch Files
  - Event logs are a good source of information
  - Firewall logs
  - Crash dump logs
  - Anti-virus log files
- Prefetch folder (Windows Prefetch, C:\Windows\Prefetch):
  - Contains the last 128 run files
  - Contains part of of the program
  - Contains information on what drivers/dlls were used by the last used programs
  - The whole folder is copied during an investigation

Data Recovery

- Commonly referred to as “Data Carving”: a file is deleted or a media is removed.

- When a file occupies a hard disk, the position of the data is recorded. When the data is removed, flags for the data is removed and the data is still present until it’s overwritten.
- A carving program like (PhotoRec) uses headers and footers to find files that are “deleted” in hard disk to recover files.
- Allows Investigators to find files that were “deleted”.
- “Sleuthkit” is a tool used by Investigators to manually pull files.

Lab Notes – OSFMount

- Purpose: Mount an image and use PhotoRec to recover files.
- Using OSFMount, mount the image.
- PhotoRec is located inside of a folder “testdisk”.
- Upon launch, a cmdline interface is started. Select the appropriate drive and specify the partition if known.
- Next steps include specifying what types of files are to be searched and where to store the found files.