Introduction to Security Forensics and Incident Handling

Ming Chow (mchow@cs.tufts.edu)

Twitter: @0xmchow

Topic Outcomes

- Acquire data (from a disk) using `dd`
- Analyze image of disk from `dd` using forensics tools including Autopsy/Sleuth Kit , Foremost
- Recover deleted files off a disk

Scenario

Imagine you have been attacked, compromised, or is involved in a criminal incident. What's the evidence? What happened? When? Who was involved?

What is Forensics?

- Preservation (of computer media)
- Identification (of computer media)
- Extraction (of computer media)
- Interpretation
- Documentation

The Process

- Assess the situation

- Acquire data

- Analyze data

- Report

Law Enforcement: Before Accessing Situation, Obtain Search Warrant

SEARCH WARRANT

G.L. c. 276, §§ 1-7

TRIAL COURT OF MASSACHUSETTS

_____COURT DEPARTMENT

_____DIVISION

SEARCH WARRANT DOCKET NUMBER

TO THE SHERIFFS OF OUR SEVERAL COUNTIES OR THEIR DEPUTIES, ANY STATE POLICE OFFICER, OR ANY CONSTABLE OR POLICE OFFICER OF ANY CITY OR TOWN, WITHIN OUR COMMONWEALTH:

Proof by affidavit, which is hereby incorporated by reference, has been made this day and I find that there is **PROBABLE CAUSE** to believe that the property described below:

☐ has been stolen, embezzled, or obtained by false pretenses.
☐ is intended for use or has been used as the means of committing a crime.
☐ has been concealed to prevent a crime from being discovered.
☐ is unlawfully possessed or concealed for an unlawful purpose.
☐ is evidence of a crime or is evidence of criminal activity.
☐ other _(specify)_ _____

YOU ARE THEREFORE COMMANDED within a reasonable time and in no event later than seven days from the issuance of this search warrant to search for the following property:

_____
_____
_____
_____
_____

☐ at:

_____
_____

which is occupied by and/or in possession of:

_____
_____

☐ on the person or in the possession of _(identify any specific person(s) to be searched)_:

_____

You ☐ are ☐ are not   also authorized to conduct the search at any time during the night.

You ☐ are ☐ are not   also authorized to enter the premises without announcement.

You ☐ are ☐ are not   also commanded to search any person present who may be found to have such property in his or her possession or under his or her control or to whom such property may have been delivered.

YOU ARE FURTHER COMMANDED if you find such property or any part thereof, to bring it, and when appropriate, the persons in whose possession it is found before the
_____ Division of the _____ Court Department.

DATE ISSUED	SIGNATURE OF JUSTICE, CLERK-MAGISTRATE OR ASSISTANT CLERK
	X _____
FIRST OR ADMINISTRATIVE JUSTICE	PRINTED NAME OF JUSTICE, CLERK-MAGISTRATE OR ASSISTANT CLERK
WITNESS: _____	

RETURN OF OFFICER SERVING SEARCH WARRANT

A search warrant must be executed as soon as reasonably possible after its issuance, and in any case may not be valid executed more than 7 days after its issuance. The executing officer must file his or her return with the court named in the warrant within 7 days after the warrant is issued. G.L. c. 276, §3A.

This search warrant was issued on _____ , 20 _____ , and I have executed it as follows:
                                        DATE

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____

(attach additional pages as necessary)

This inventory was made in the presence of: _____

_____

I swear that this inventory is a true and detailed account of all property taken by me
on this search warrant.

SIGNATURE OF PERSON MAKING SEARCH	DATE AND TIME OF SEARCH	SWORN AND SUBSCRIBED TO BEFORE
X_____		X_____
		Signature of Justice, Clerk-Magistrate or Assistant Clerk
PRINTED NAME OF PERSON MAKING SEARCH	TITLE OF PERSON MAKING SEARCH	DATE SWORN AND SUBSCRIBED TO

Terminology

- **Volatile data**: RAM, processes

- **Non-volatile data**: Hard disks, USB drives

- **Physical acquisition**: Bit-by-bit copy of entire physical store

- **Logical acquisition**: Bit-by-bit copy of directories and files on a file system partition

- **Write blockers**: "Devices that allow acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents. They do this by allowing read commands to pass but by blocking write commands" [1]

- **Chain-of-custody**: Chronological documentation from "crade-to-grave" (i.e., warrant, seizure, custody, control, transfer, analysis, disposal)

To Ponder

- What could possibly go wrong if you don't use a write blocker to acquire evidence, data?

- What are the pros and cons of physical vs logical acquisition? When would you want to use one over the other?

Forensics Tools

- strings
- md5/sha1/sha256/sha512
- dd
- FTK
- Encase
- stegdetect
- Sleuth Kit and Autopsy
- Foremost

Demo Time

- dd
- Sleuth Kit and Autopsy
- Foremost

Incident Handling

- Generalized and broad term
- Incorrect?
  - Incident Handling (IH) is the logistics, communications, coordination, and planning functions needed in order to resolve an incident in a calm and efficient manner.
  - Incident Response (IR) is all of the technical components required in order to analyze and contain an incident.
  - https://isc.sans.edu/forums/diary/Incident+Response+vs+Incident+Handling/6205
- Rebuttal by Richard Bejtlich
  - tl;dr IH and IR are the same
  - https://taosecurity.blogspot.com/2009/04/speaking-of-incident-response.html

Why Incident Handling is Important

- Chaos
- Barking up the wrong trees
- Dead-end investigations
- Hard to accumulate knowledge, experience
- Legal issues
- Cost overruns
- Organization (i.e., do not know who to contact)

Incident Handling vs Forensics

- There are overlaps

- Forensics: "finding and documenting the actions of a person or persons in relation to other people or places or activities. Must have a strong understanding of where and how data is stored, how data is created, how to recover that data in a forensically sound manner and how to analyze the recovered data." [2]

- Incident Handling: generally speaking, must be well versed with many facets of IT and information security.

Incident Handling Phases

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned
- Take SANS' SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling https://www.sans.org/course/hacker-techniques-exploits-incident-handling
- Read: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

For a Deeper Dive into Incident Handling

- Take SANS' SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling https://www.sans.org/course/hacker-techniques-exploits-incident-handling
  - Yours truly is an alumnus of the course back in 2007
  - SANS GCIH certification https://www.giac.org/certification/certified-incident-handler-gcih
- Read: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Anti-Forensics (or countering against forensics)

- Full-disk wipe using DoD 5220.22-M
  - https://www.nispom.org/NISPOM_2006.pdf
- Remove logs
- Steganography
- Encryption (full-disk, VeraCrypt, BitLocker for Windows, FileVault for macOS)
- Put disk into BBQ or fire pit

Forensics

1. http://forensicswiki.org/wiki/Write_Blockers
2. http://exforensis.blogspot.com/2009/09/how-is-computer-forensics-different.html