

# Introduction to Security Forensics and Incident Handling

Ming Chow ([mchow@cs.tufts.edu](mailto: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

APPLICATION FOR SEARCH WARRANT G.L. c. 276, §§ 1-7		TRIAL COURT OF MASSACHUSETTS 
NAME OF APPLICANT		COURT DEPARTMENT
POSITION OF APPLICANT		DIVISION
		SEARCH WARRANT DOCKET NUMBER
<p>I, the undersigned <b>APPLICANT</b>, being duly sworn, depose and say that:</p> <p>1. I have the following information based upon the attached affidavit(s), consisting of a total of _____ pages, which is (are) incorporated herein by reference.</p> <p>2. Bases upon this information, there is <b>PROBABLE CAUSE</b> to believe that the property described below:</p> <p><input type="checkbox"/> has been stolen, embezzled, or obtained by false pretenses.</p> <p><input type="checkbox"/> is intended for use or has been used as the means of committing a crime.</p> <p><input type="checkbox"/> has been concealed to prevent a crime from being discovered.</p> <p><input type="checkbox"/> is unlawfully possessed or concealed for an unlawful purpose.</p> <p><input type="checkbox"/> is evidence of a crime or is evidence of criminal activity.</p> <p><input type="checkbox"/> other (specify) _____</p> <p>3. I am seeking the issuance of a warrant to search for the following property (describe the property to be searched for as particularly as possible):</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>4. Based upon this information, there is also probable cause to believe that the property may be found (check as may as apply):</p> <p><input type="checkbox"/> at (identify the exact location or description of the place(s) to be searched):</p> <p>_____</p> <p>_____</p> <p>which is occupied by and/or in possession of:</p> <p>_____</p> <p><input type="checkbox"/> on the person or in the possession of (identify any specific person(s) to be searched):</p> <p>_____</p> <p><input type="checkbox"/> on 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.</p> <p>THEREFORE, I respectfully request that the court issue a Warrant and order of seizure, authorizing the search of the above described place(s) and person(s), if any, to be searched, and directing that such property or evidence or any part thereof, if found, be seized and brought before the court, together with such other and further relief that the court may deem proper.</p> <p><input type="checkbox"/> have previously submitted the same application.</p> <p><input type="checkbox"/> Have <b>not</b> previously submitted the same application.</p>		
PRINTED NAME OF APPLICANT		SIGNED UNDER THE PENALTIES OF PERJURY
		<b>X</b> _____ Signature of Applicant
SWORN AND SUBSCRIBED TO BEFORE		
<b>X</b> _____ Signature of Justice, Clerk-Magistrate or Assistant Clerk		DATE

# Example of a Search Warrant

<b>SEARCH WARRANT</b> G.L. c. 276, §§ 1-7	<b>TRIAL COURT OF MASSACHUSETTS</b> _____ COURT DEPARTMENT _____ DIVISION
	SEARCH WARRANT DOCKET NUMBER _____
<p><b>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:</b></p> <p>Proof by affidavit, which is hereby incorporated by reference, has been made this day and I find that there is <b>PROBABLE CAUSE</b> to believe that the property described below:</p> <p> <input type="checkbox"/> has been stolen, embezzled, or obtained by false pretenses.  <input type="checkbox"/> is intended for use or has been used as the means of committing a crime.  <input type="checkbox"/> has been concealed to prevent a crime from being discovered.  <input type="checkbox"/> is unlawfully possessed or concealed for an unlawful purpose.  <input type="checkbox"/> is evidence of a crime or is evidence of criminal activity.  <input type="checkbox"/> other (specify) _____         </p> <p><b>YOU ARE THEREFORE COMMANDED</b> 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:</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p><input type="checkbox"/> at:</p> <p>_____</p> <p>_____</p> <p>which is occupied by and/or in possession of:</p> <p>_____</p> <p><input type="checkbox"/> on the person or in the possession of (identify any specific person(s) to be searched):</p> <p>_____</p> <p>You <input type="checkbox"/> are <input type="checkbox"/> are not also authorized to conduct the search at any time during the night.</p> <p>You <input type="checkbox"/> are <input type="checkbox"/> are not also authorized to enter the premises without announcement.</p> <p>You <input type="checkbox"/> are <input type="checkbox"/> 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.</p> <p><b>YOU ARE FURTHER COMMANDED</b> 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.</p>	
DATE ISSUED _____	SIGNATURE OF JUSTICE, CLERK-MAGISTRATE OR ASSISTANT CLERK <b>X</b> _____
FIRST OR ADMINISTRATIVE JUSTICE <b>WITNESS:</b> _____	PRINTED NAME OF JUSTICE, CLERK-MAGISTRATE OR ASSISTANT CLERK _____



# Example of a Search Warrant (continued)

**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.

<small>SIGNATURE OF PERSON MAKING SEARCH</small> <b>X</b> _____	<small>DATE AND TIME OF SEARCH</small> _____	<small>SWORN AND SUBSCRIBED TO BEFORE</small> <b>X</b> _____ <small>Signature of Justice, Clerk-Magistrate or Assistant Clerk</small>
<small>PRINTED NAME OF PERSON MAKING SEARCH</small> _____	<small>TITLE OF PERSON MAKING SEARCH</small> _____	<small>DATE SWORN AND SUBSCRIBED TO</small> _____



SCHOOL OF ENGINEERING  
Computer Science



# 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 "cradle-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](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](http://forensicswiki.org/wiki/Write_Blockers)
2. <http://exforensis.blogspot.com/2009/09/how-is-computer-forensics-different.html>