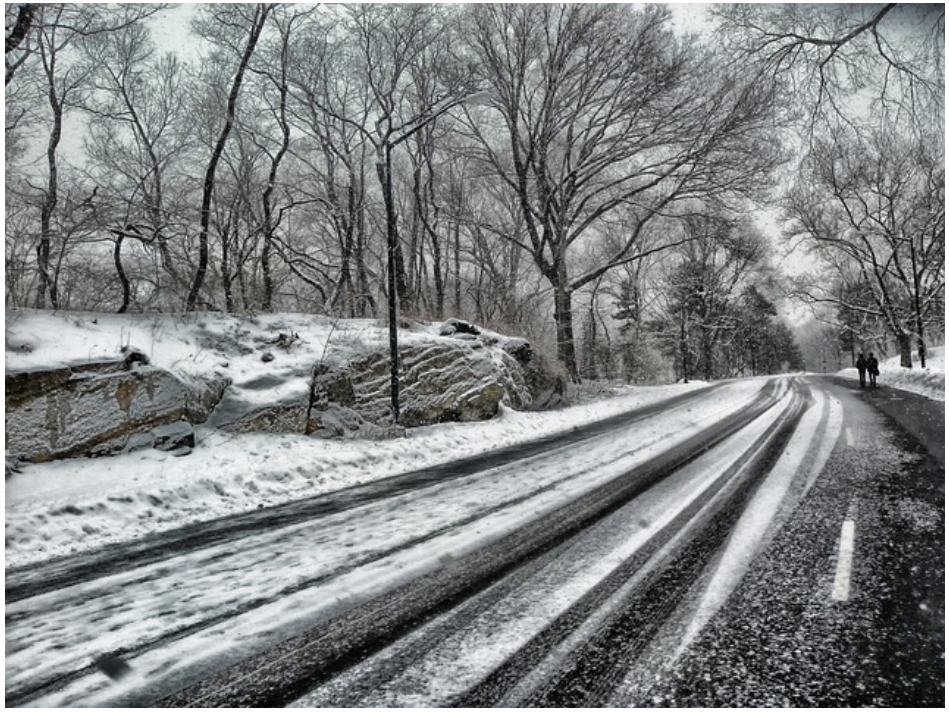
DEVSECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK SEVEN / LESSON THREE

Agenda

- Forensic Investigation Basics
- Enterprise Forensic Analysis
- Memory
- Disk
- Tools



Forensic Investigation Basics

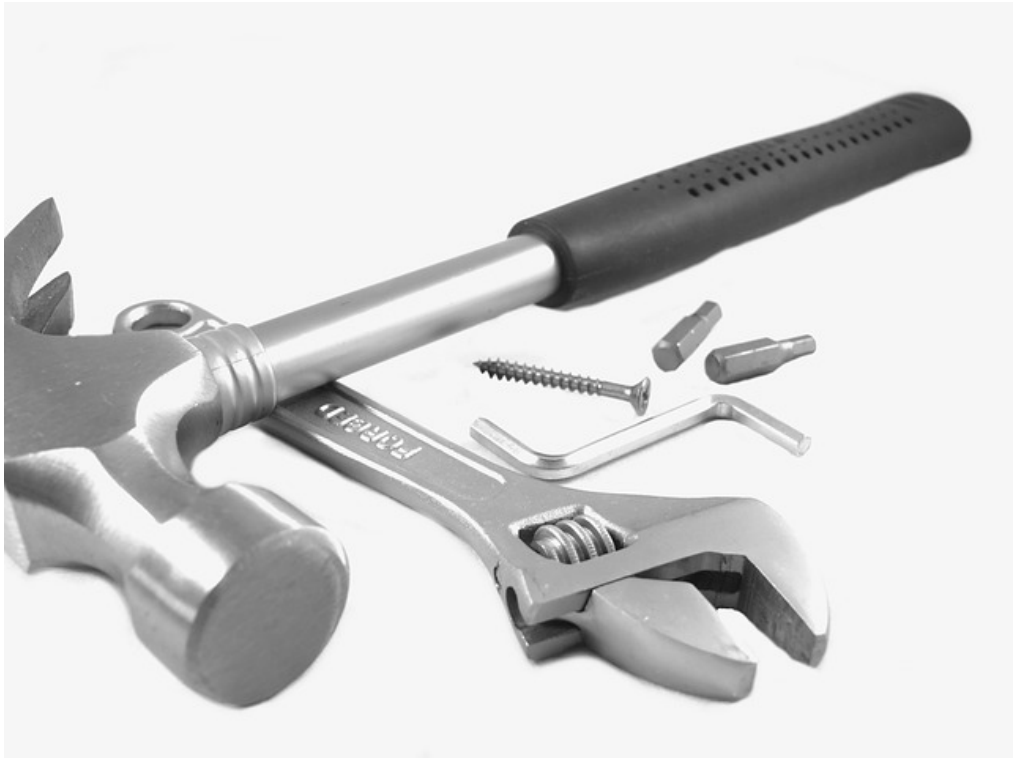
- Collection
  - The methods used to collect evidence should be transparent and documented for reproducibility
- Order of Volatility
  - Collect most volatile first
- Chain of custody
  - Describe how you obtained the evidence, how it was handled and anything that happened to it

Enterprise Forensic Analysis

- Tools
  - EnCase
    - Agents on systems
- Network Taps
- Network IDS
- Packet Capture
- Memory Dump
- Access to physical hardware

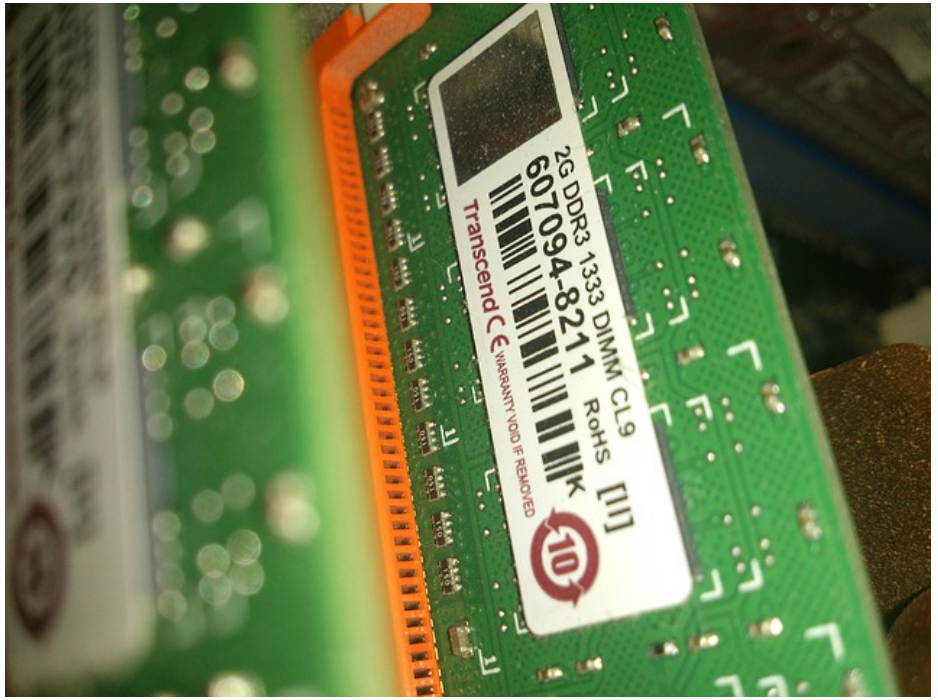
Tools

- Live CDs
  - CAINE
  - Kali Linux
- Tools
  - Autopsy
  - Sleuth Kit
  - Log2timeline
  - dcfl-dd/dd-rescue
  - Tcpdump/wireshark
  - Testdisk/photorec
  - Hashsets
  - volatility



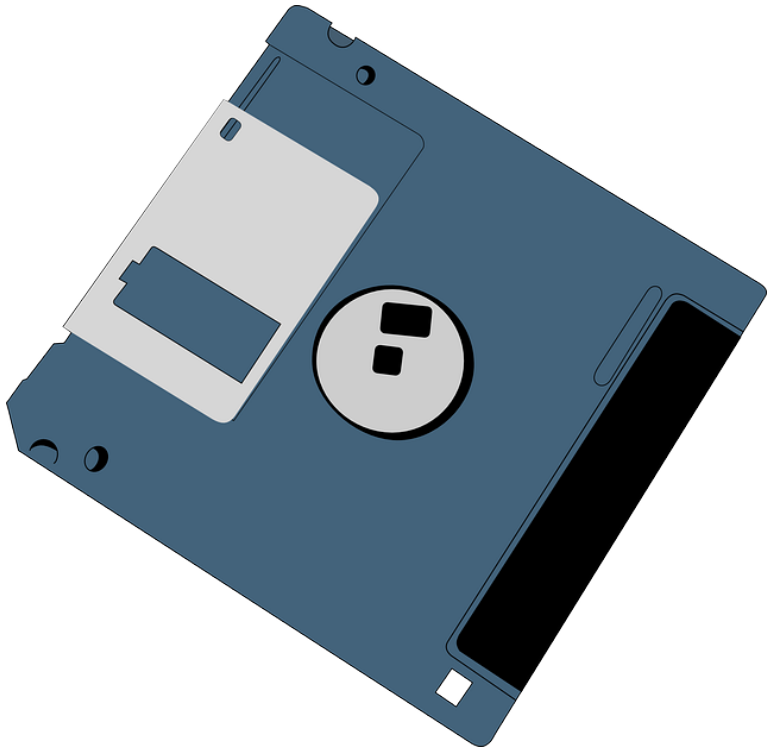
Memory

- Volatility Framework
  - Python based
  - Can extract
    - Process lists
    - Logged in users
    - Tcp connections



Disk

- Acquisition
  - dcfldd
  - ddrescue/dd_rescue
  - dd
- Analysis
  - fdisk
  - testdisk
- Extraction
  - photorec
  - scalpel
  - find/strings/cat



Lab 3

- https://github.com/devsecops/bootcamp/blob/master/Week-7/labs/LAB-3.md