DEVSECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK SEVEN/ LESSON TWO

Agenda

- Forensic Image Capture
- Taking Forensic Snapshots
- Snapshot Escrow
- Introducing Selfie
- Lab 2

Forensic Image Capture

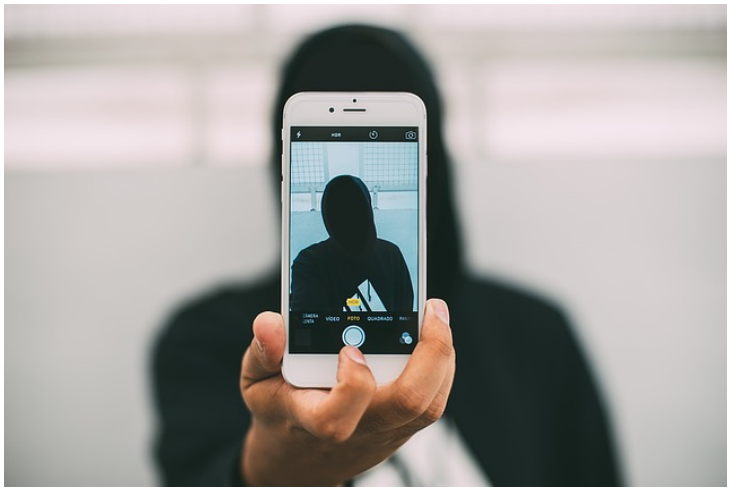
- Source of truth for investigation
- Snapshots of disk images are taken in account where incident took place
- Snapshots only captures disk contents not Memory
  - No: open ports, running processes, logged in users
- Memory capture: roll your own with something like LiME

Snapshot Escrow

- Snapshots are copied to the forensic account
- Forensic investigation should be performed on copies of the snapshots
- Can be done through GUI but is labor intensive and prone to mistakes

Selfie

- DevSecOps tool
- Command line only
- Recently open sourced
- Automates a lot of the previously mentioned manual process
- Needs some love
- https://github.com/devsecops/selfie



Lab 2 - Selfie

- https://github.com/devsecops/bootcamp/blob/master/Week-7/labs/LAB-2.md