# Digital Forensics

- Evidence Volatility (network vs memory vs disk)
- Network Forensics
  - DNS logs / passive DNS
  - Netflow
  - Sampling rate
- Disk Forensics
  - Disk imaging
  - Filesystems (NTFS / ext2/3/4 / AFPS)
  - Logs (Windows event logs, Unix system logs, application logs)
  - Data recovery (carving)
  - Tools
  - plaso / log2timeline
  - FTK imager
  - encase
- Memory Forensics
  - Memory acquisition (footprint, smear, hiberfiles)
  - Virtual vs physical memory
  - Life of an executable
  - Memory structures
  - Kernel space vs user space
  - Tools
  - Volatility
  - Google Rapid Response (GRR) / Rekall
  - WinDbg
- Mobile Forensics
  - Jailbreaking devices, implications
  - Differences between mobile and computer forensics
  - Android vs. iPhone
- Anti Forensics
  - How does malware try to hide?
  - Timestomping
- Chain of Custody
  - Handover notes