Network Forensics

- Analysis and interpretation of network traffic
- Network data
  - either live traffic
  - stored communications, or
  - IDS logs, Firewall logs, Routers, servers logs
- The Role of Network Forensics
  - the **temporal** nature of the network information
  - Only capture **a snap shot** of the current activity

Network Based Forensics

- Network Forensics: Tracking Hackers through Cyberspace, by Sherri Davidoff and Jonathan Harn, ISBN: 0132564718
- Determine what happened on a system **based on network traffic study**
- Post-mortem analysis
  - MAC timeline analysis
  - Discover the reconnaissance, exploitation and covert operations
  - Which vulnerability was exploited
  - Recover the contents of rootkits
  - Where it came from
  - Who (ip addr) did it

Network Forensics (Con't)

- Four basic classes of network information
  - Full content data
  - Session data
  - Alert data
  - Statistical data

wireshark

- Parse, filter and display network traffic
- Interpret network traffics from tcpdump and snort
- Extract specific sessions using Follow TCP Stream – Forensic examiners are interested in
  - Given a single packet, it allows the investigator to view an entire TCP stream

NetworkMiner

- Hjelmvik, E. (2008). Passive network security analysis with NetworkMiner. *Insecure.com, Issue 18, page 18-21*, http://www.net-security.org/dl/insecure/INSECURE-Mag-18.pdf
- Sniffing network traffic
- Perform comprehensive offline analyses
- Groups all the traffic as incoming and outgoing sessions under each host in the network
- Identify systems' abnormal behaviors and examine whether sensitive data is passing through the network