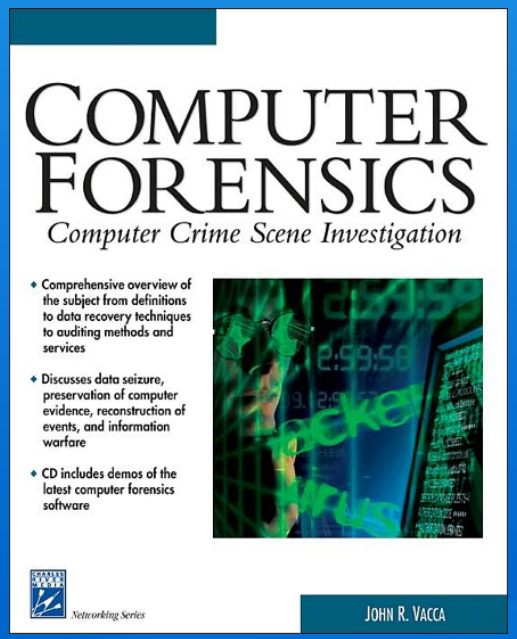
NetworkMiner

Erik Hjelmvik, SecHeads 2008

Network Forensics

Network forensics is the principle of reconstructing the activities leading to an event and determining the answers to "What did they do?" and "How did they do it?"

- John Vacca in:
  Computer Forensics:
  Computer Crime Scene Investigation

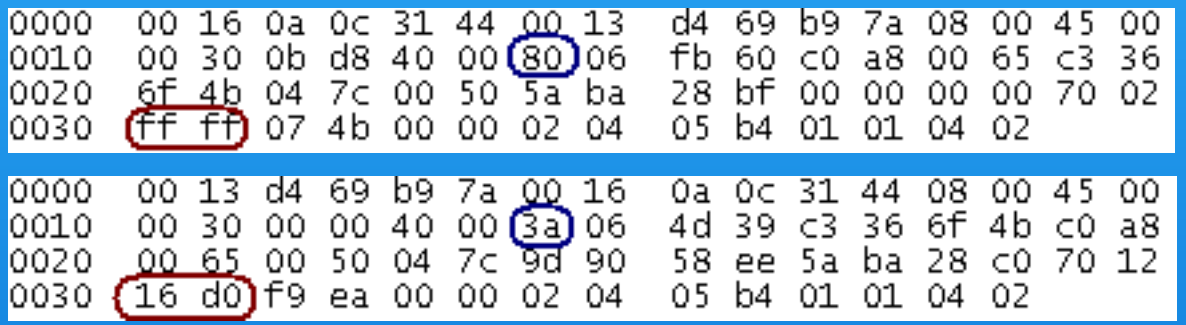


Functionalities

- Passive OS fingerprinting
  - p0f
  - Ettercap
  - Satori TCP
  - Satori DHCP
- File extraction from network stream
  - HTTP GET & POST, FTP, TFTP, SMB
- Credentials extraction (usernames & passwords)
  - HTTP Forms, FTP, SMB/CIFS
- Keyword search and cleartext monitoring
  - Protocol independent

IP Time To Live

TCP Window Size



What is NetworkMiner used for?

- Network intrusion investigations
  - Analysis of PCAP files from IDS / IPS
- Analysis of BotNets
  - Analysis of BotNet C&C traffic
- Honeypot traffic analysis
- Analysis of traffic from a compromised machine
- Passive Network inventory mapping (passive Nmap)
- Criminal Investigation Wiretapping
  - Child abuse (child pornography)

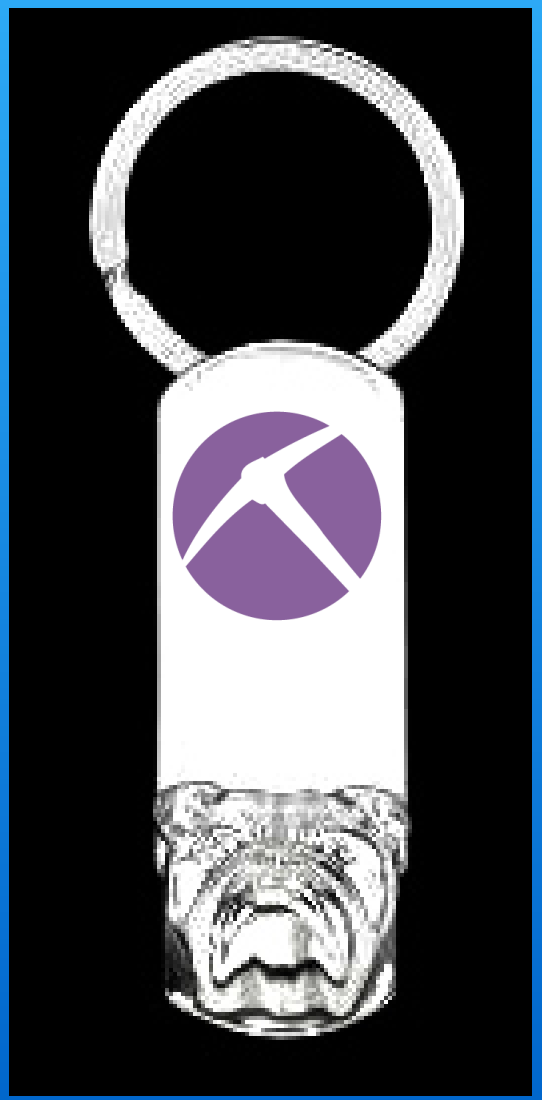
Network traffic sources

Traffic can be captured (sniffed) through:

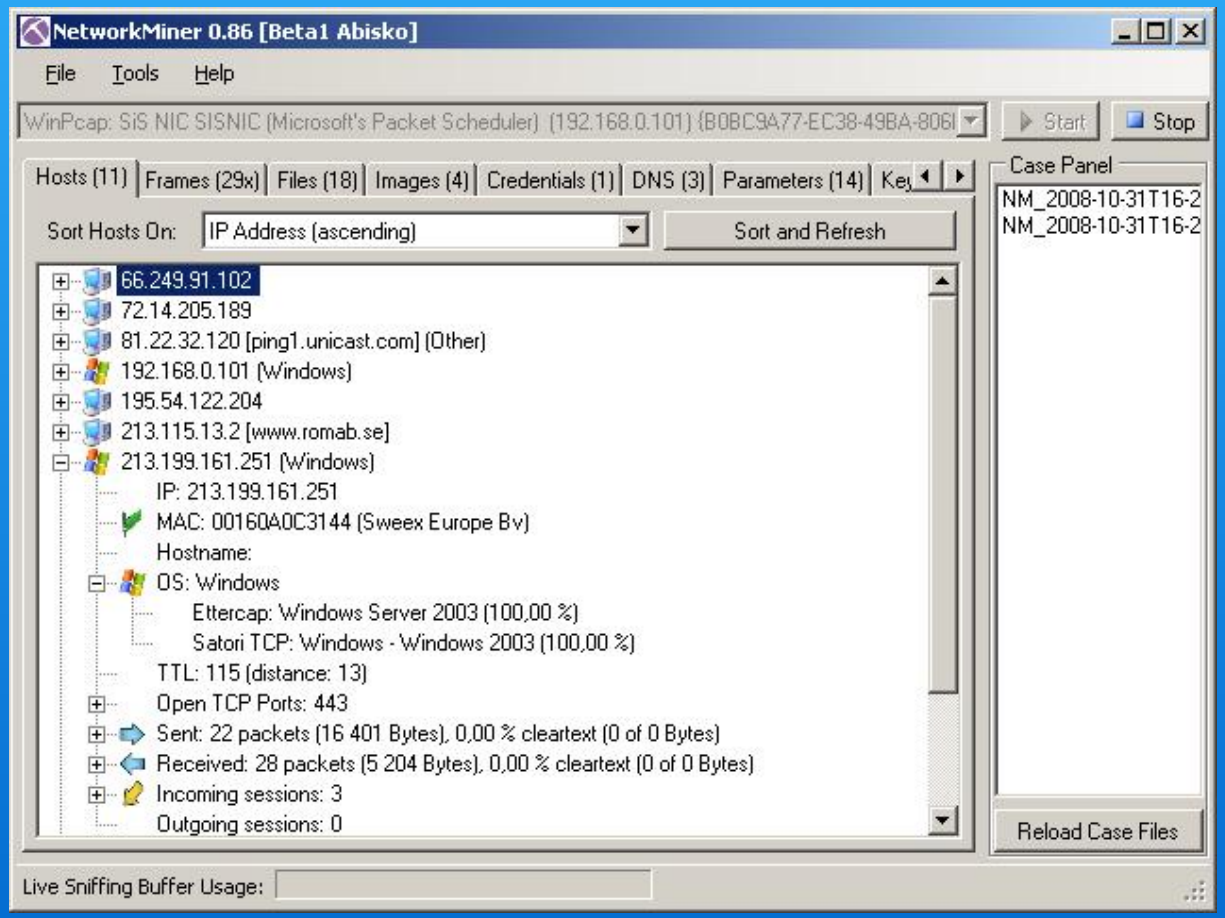
- Raw Sockets (requires admin user rights)
- WinPcap (driver must be installed)
- AirPcap (driver + AirPcap device)

Portable application

- NetworkMiner doesn't require installation
- Can be run from a USB memory stick

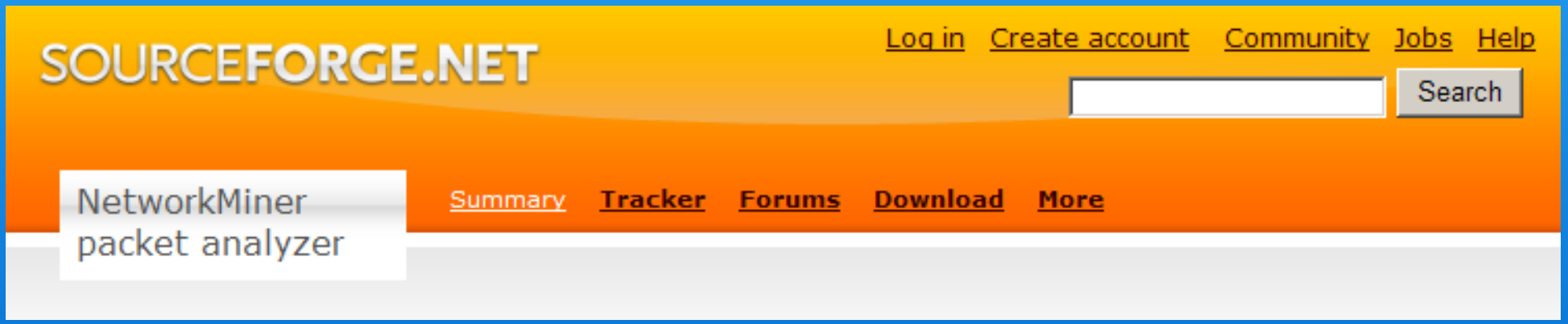


Demo - PCAP file analysis



Warning: Live Sniffing Ahead!

Get NetworkMiner



http://sourceforge.net/projects/networkminer/