Experiment No.6
To perform Network packet forensics using Network Miner
Date of Performance:
Date of Submission:

Aim: To perform network traffic forensics using network miner

Objective: To extract the artifact from the network traffic using network miner tool

Theory:

Packet Capture or PCAP (also known as libpcap) is an application programming interface (API) that captures live network packet data from OSI model Layers 2-7. Network analyzers like Wireshark create .pcap files to collect and record packet data from a network. PCAP comes in a range of formats including Libpcap, WinPcap, and PCAPng.

These PCAP files can be used to view TCP/IP and UDP network packets. If you want to record network traffic then you need to create a .pcapfile. You can create a .pcapfile by using a network analyzer or packet sniffing tool like Wireshark or tcpdump.

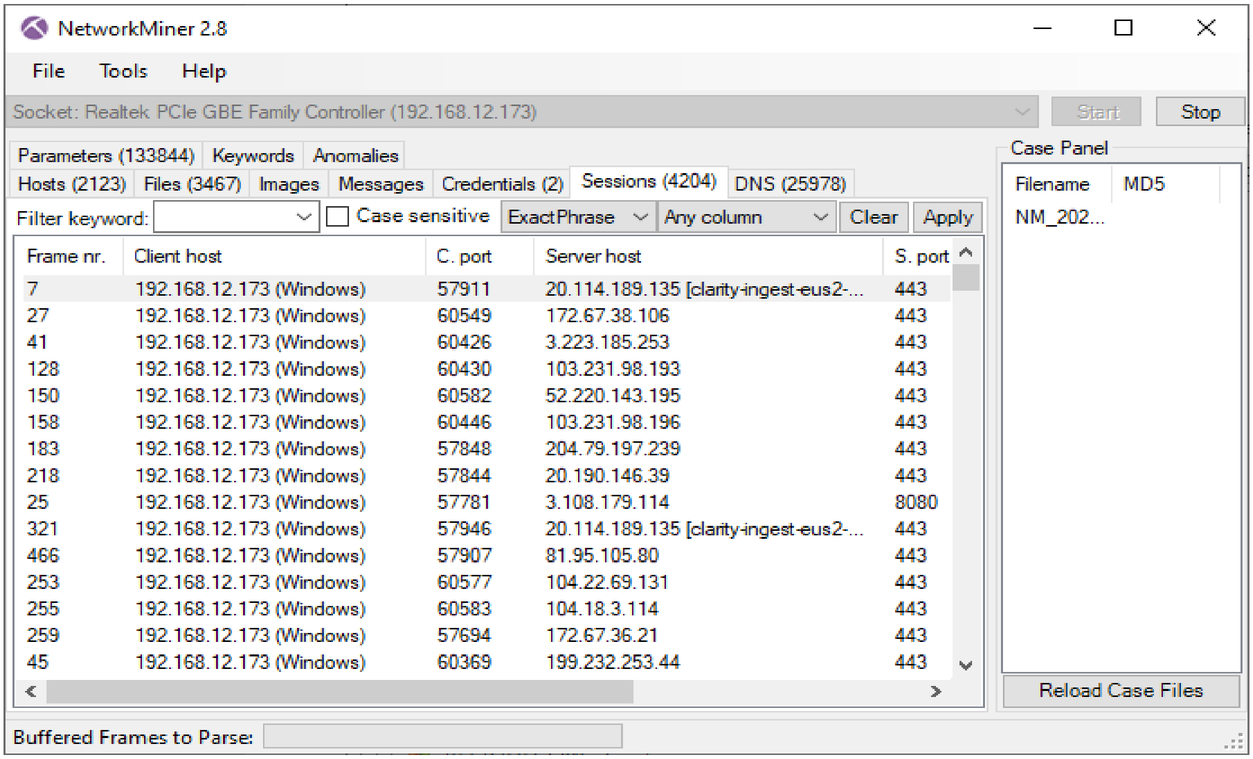
PCAP is a valuable resource for file analysis and to monitor your network traffic. Packet collection tools like Wireshark allow you to collect network traffic and translate it into a format that's human-readable. There are many reasons why PCAP is used to monitor networks. Some of the most common include monitoring bandwidth usage, identifying rogue DHCP servers, detecting malware, DNS resolution, and incident response.

For network administrators and security researchers, packet file analysis is a good way to detect network intrusions and other suspicious activity. For example, if a source is sending the network lots of malicious traffic, you can identify that on the software agent and then take action to remediate the attack.

Network Miner

Network Miner is an open source network forensics tool that extracts artifacts, such as files, images, emails and passwords, from captured network traffic in PCAP files. Network Miner can also be used to capture live network traffic by sniffing a network interface. Detailed information about each IP address in the analyzed network traffic is aggregated to a network host inventory, which can be used for passive asset discovery as well as to get an overview of which devices that are communicating. Network Miner is primarily designed to run in Windows, but can also be used in Linux.

Network Miner has, since the first release in 2007, become a popular tool among incident response teams as well as law enforcement. Network Miner is today used by companies and organizations all over the world. Figure below shows the screenshot of the network miner tool.


NetworkMiner 2.8
File Tools Help
Socket: Realtek PCIe GBE Family Controller (192.168.12.173)
Start
Stop
Parameters (133844) Keywords Anomalies
Hosts (2123) Files (3467) Images Messages Credentials (2) Sessions (4204) DNS (25978)
Filter keyword:
□ Case sensitive
ExactPhrase
Any column
Clear
Apply
Case Panel
Filename MD5
NM_202...
Reload Case Files
Buffered Frames to Parse:

Frame nr.	Client host	C. port	Server host	S. port
7	192.168.12.173 (Windows)	57911	20.114.189.135 [clarity-ingest-eus2-...	443
27	192.168.12.173 (Windows)	60549	172.67.38.106	443
41	192.168.12.173 (Windows)	60426	3.223.185.253	443
128	192.168.12.173 (Windows)	60430	103.231.98.193	443
150	192.168.12.173 (Windows)	60582	52.220.143.195	443
158	192.168.12.173 (Windows)	60446	103.231.98.196	443
183	192.168.12.173 (Windows)	57848	204.79.197.239	443
218	192.168.12.173 (Windows)	57844	20.190.146.39	443
25	192.168.12.173 (Windows)	57781	3.108.179.114	8080
321	192.168.12.173 (Windows)	57946	20.114.189.135 [clarity-ingest-eus2-...	443
466	192.168.12.173 (Windows)	57907	81.95.105.80	443
253	192.168.12.173 (Windows)	60577	104.22.69.131	443
255	192.168.12.173 (Windows)	60583	104.18.3.114	443
259	192.168.12.173 (Windows)	57694	172.67.36.21	443
45	192.168.12.173 (Windows)	60369	199.232.253.44	443

Network Miner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. Network Miner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.

Process:

Step 1. Download the network Miner tool from the website NetworkMiner - The NSM and Network Forensics Analysis Tool ↖ (netresec.com)

Step 2. Install the tool onto your system

Step 3. Connect your system to the internet connection

Step 4. Open the Network Miner tool

Step 5. Extract the Network traffic artefact using Network Miner tool

Step 6. Create a report based on the artefact extracted

Conclusion:

Network Miner enables forensic investigators to extract and analyze critical artifacts from captured network traffic such as files, credentials, host details, and communication sessions.

These artifacts help uncover the nature and source of malicious activities, trace unauthorized access, and identify compromised systems. By reassembling transmitted files and examining session data, investigators can reconstruct the attack timeline and methods used. Thus, Network Miner plays a vital role in digital forensics by providing deep insights into network behavior and aiding in evidence collection for cybercrime investigations.