CA – 3 (Project)

Name: Divyam Sharyan

Registration no.: 11904871

Roll no.: 17

Section: KE009

Submitted to: Rajeshwar Sharma

School of Computer Science

CONTENT

1. Introduction

Digital forensics investigations are becoming increasingly important in today's world as more criminal activities are being carried out online. One crucial aspect of digital forensics investigations is the extraction deleted file from disk. By analysing these artifacts, digital forensic investigators can track the suspect's online activities, identify any criminal behavior, and build a solid case against them.

Autopsy forensic tool is an open-source digital forensic tool that can be used to extract or restore images from disk, phone or any other flash drive. It provides various modules and tools that can help investigators search for specific keywords, analyse file metadata, and extract various types of files from disk images. In this task, we will focus on using Autopsy forensic tool to extract deleted image from disk

By leveraging Autopsy's powerful keyword search capabilities, digital forensic investigators can search for specific search terms such as illegal activities, pornography, child exploitation, hacking, and terrorism, among others. By analysing the search results, investigators can identify potentially incriminating evidence and use it to build a solid case against the suspect.

1.1 Objective of the project

The objective of this project is to employ a network miner tool capable of capturing network packets, decoding the information within them, and identifying open ports, operating systems, and active network sessions. The tool must be able to extract relevant details such as the source and destination IP addresses, protocols, and data payloads.

By analyzing this information, the tool will determine the operating system, open ports, and active network sessions. The findings of the network analysis will be presented in a comprehensible manner.

The primary goal of the project is to scrutinize network traffic, uncover potential security risks and vulnerabilities, and pre-emptively address any issues that could be exploited by attackers.

1.2 Description of the project

A network forensics analysis programme called Network Miner is intended to assist investigators in deciphering recorded packets of data and analysing network traffic. Here is a description of how the tool functions:

1. Capture network traffic: Network Miner can capture network traffic from a variety of sources, including pcap files, live network interfaces, and Network Miner's proprietary pcap-over-IP protocol.
2. Parse network traffic: After NetworkMiner has recorded the network traffic, it

analyses the packets to extract data about different network protocols, such as file transfers, DNS inquiries, and HTTP requests and answers.
3. Reassemble files that are transported over the network: NetworkMiner can also put together files that are moved over the network, enabling investigators to pull out files and other information that could be concealed inside network traffic.
4. Examine network traffic: For viewing and examining network traffic, NetworkMiner offers a user-friendly interface. The programme may be used by investigators to find network abnormalities, monitor particular network device behavior, and spot possible security risks.
5. Export data: NetworkMiner gives investigators the option to export network traffic and analysis data in a number of formats, including as CSV, JSON, and HTML, allowing for additional investigation using other programmes and platforms.
Overall, Network security experts, incident responders, and law enforcement organisations frequently utilise NetworkMiner as a strong tool for network forensics investigation.
It has a number of functions, such as the capacity to parse files and extract metadata from different network protocols, that enable investigators to locate and examine network activity.

1.3 Scope of the project

The scope of the project is to demonstrate the process of extracting deleted image from disk The project also includes searching for specific search terms on diskimages or phone images using Network Miner tool.

The project focuses on using Autopsy forensic tool as the primary digital forensic tool for extracting data from disk. It does not cover other digital forensic tools or techniques that can be used for similar purposes.

The specific search terms used in the project are intended to provide general examples of potentially incriminating evidence that can be found on the disk. The project does not cover the investigation of specific criminal cases or provide legal advice.

The project assumes that the disk images or phone images used as evidence are legally obtained and within the boundaries of applicable laws and regulations.

It also assumes that the investigation is conducted by trained and authorized digitalforensic investigators.

Overall, the scope of the project is to introduce digital forensicsinvestigations and demonstrate how Autopsy forensic tool can be used to extract deleted images from flash disk and how we can extract important information from website.

2. System Description

- The following is a system description for using Autopsy:
    - Operating System: Windows, macOS, or Linux
    - Autopsy Tool: Download the latest version of Autopsy from the official website and install it on your system.
- The following is a system description for using the Harvester:
    - Operating System: macOS or Linux
    - The Harvester tool: updated with API

2.1 Target system description

- For website I am using lpu.in domain.
- For Autopsy, I am using a flash drive or pen drive which contains 8GB of storage.

1. Utilizing the packet sniffing library, start by collecting network traffic on the target network. You will be able to record every packet that moves via the network, along with its data and metadata.

2. To determine the operating system that the network's devices are using, analyse the packets that were recorded. This may be achieved by looking at several packet header information, including TTL values, packet flags, and TCP/IP fingerprinting methods.

3. To find on the network active sessions, use the packets that were collected. This may be achieved by identifying requests and answers exchanged across network devices by looking at the packet contents and headers. Additionally, you might want to keep an eye out for network traffic abnormalities that might point to nefarious or suspicious conduct.

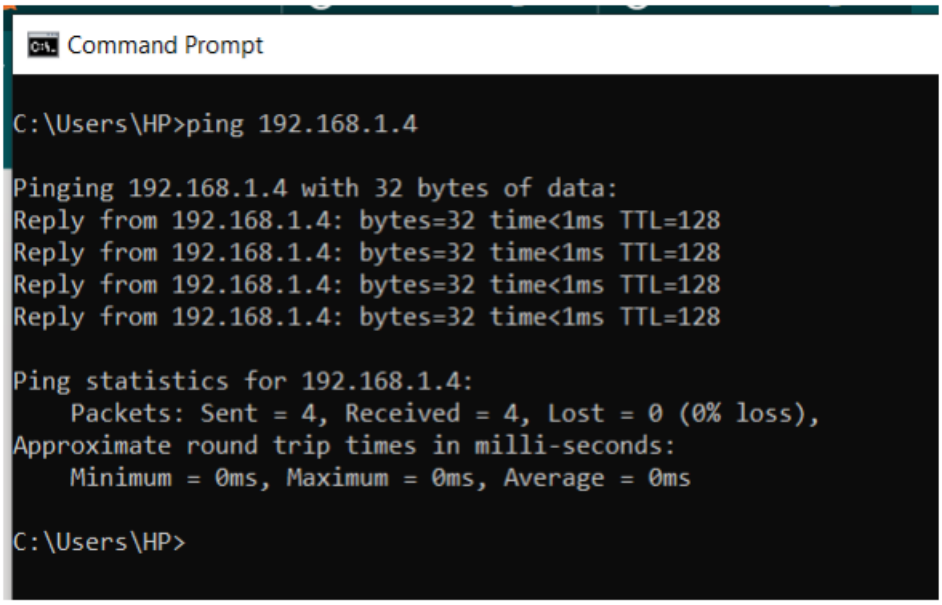
4. By looking for TCP SYN packets and answers in the packet headers, you may find open ports on the network. You may use this to find out which ports are open and which services are using them.

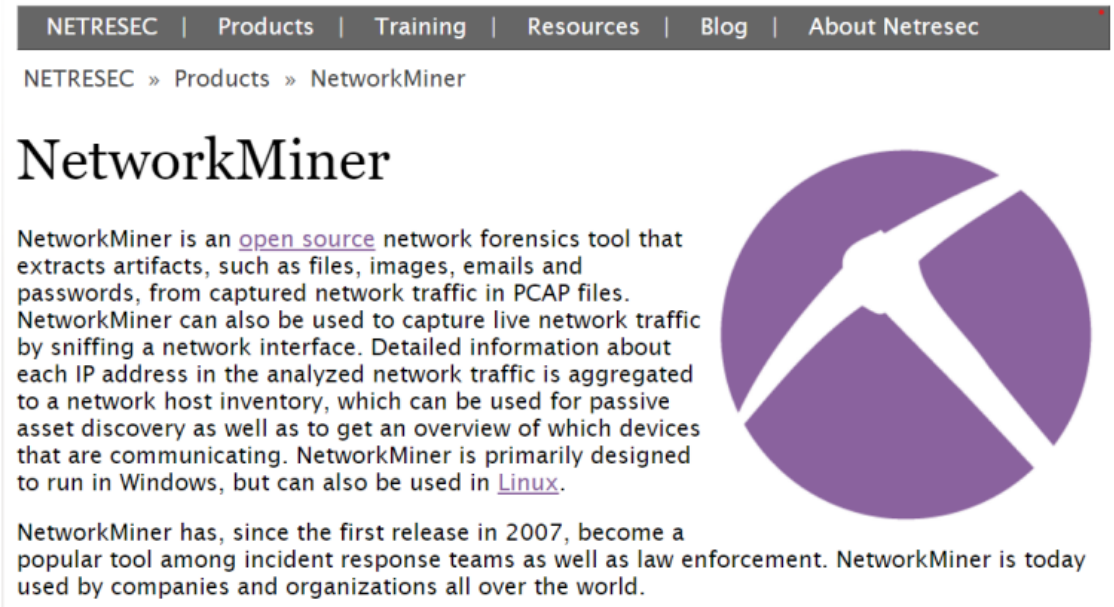
5. Using additional network security tools and techniques, you may look into the network further after determining the operating system, sessions, and open ports. This might involve executing penetration tests, running vulnerability scans, or continuously monitoring network traffic to spot patterns or behavioural changes.

3. Analysis Report

3.1 System snapshots and full analysis report

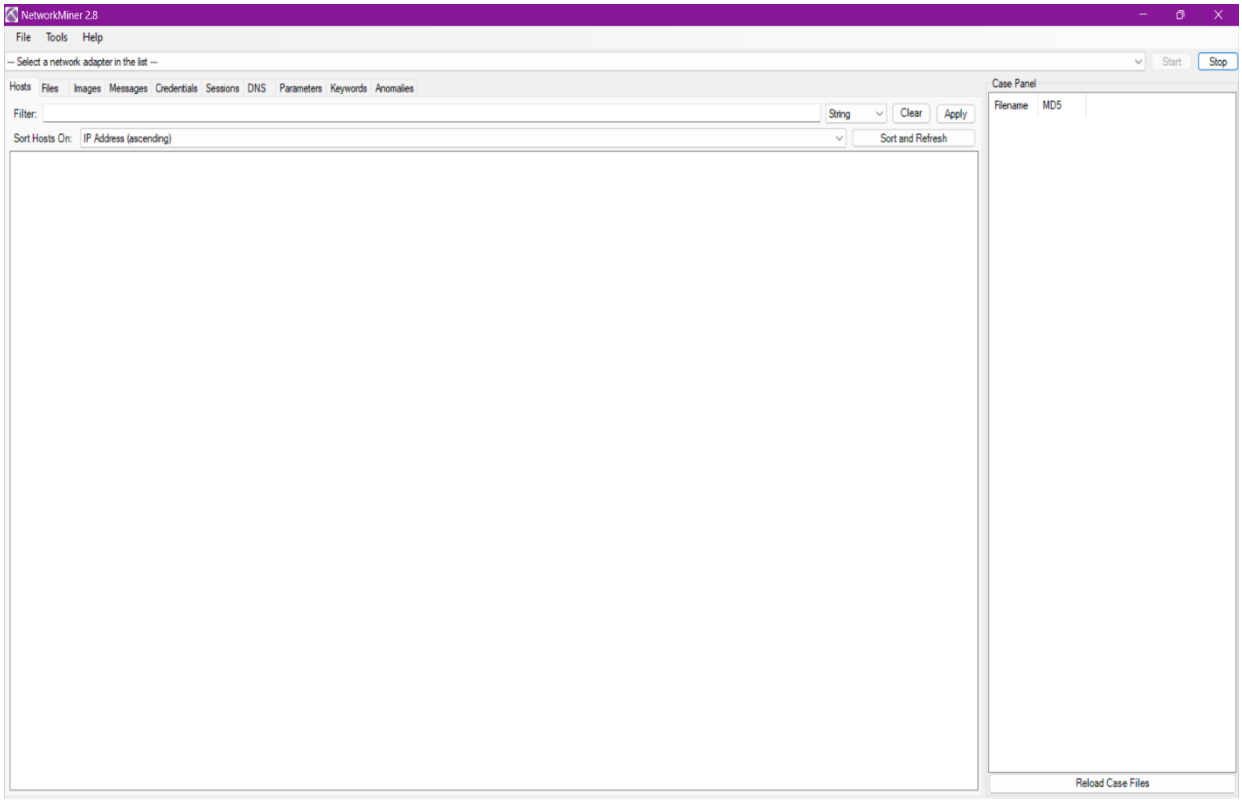
- Find out the specific search terms on disk and phone using Autopsy forensic tool.

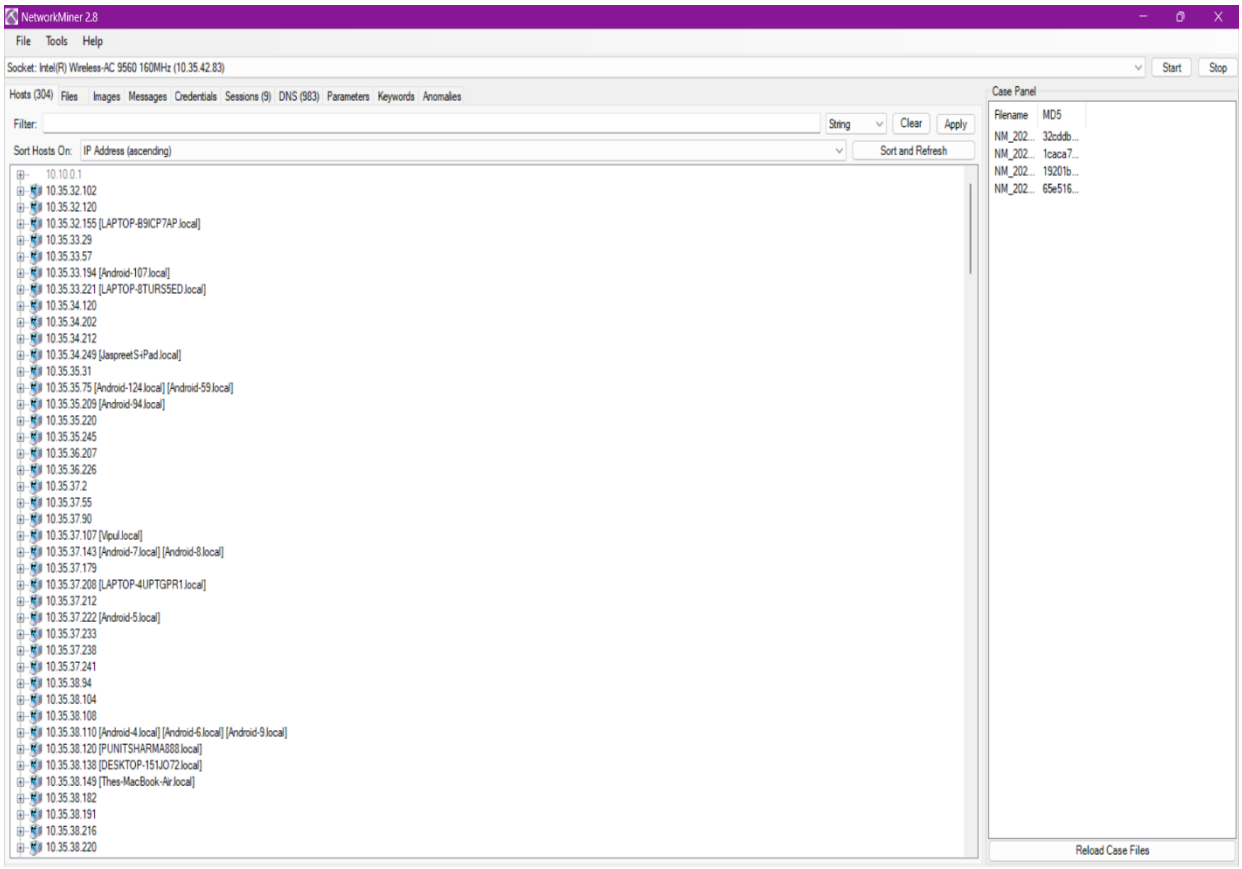


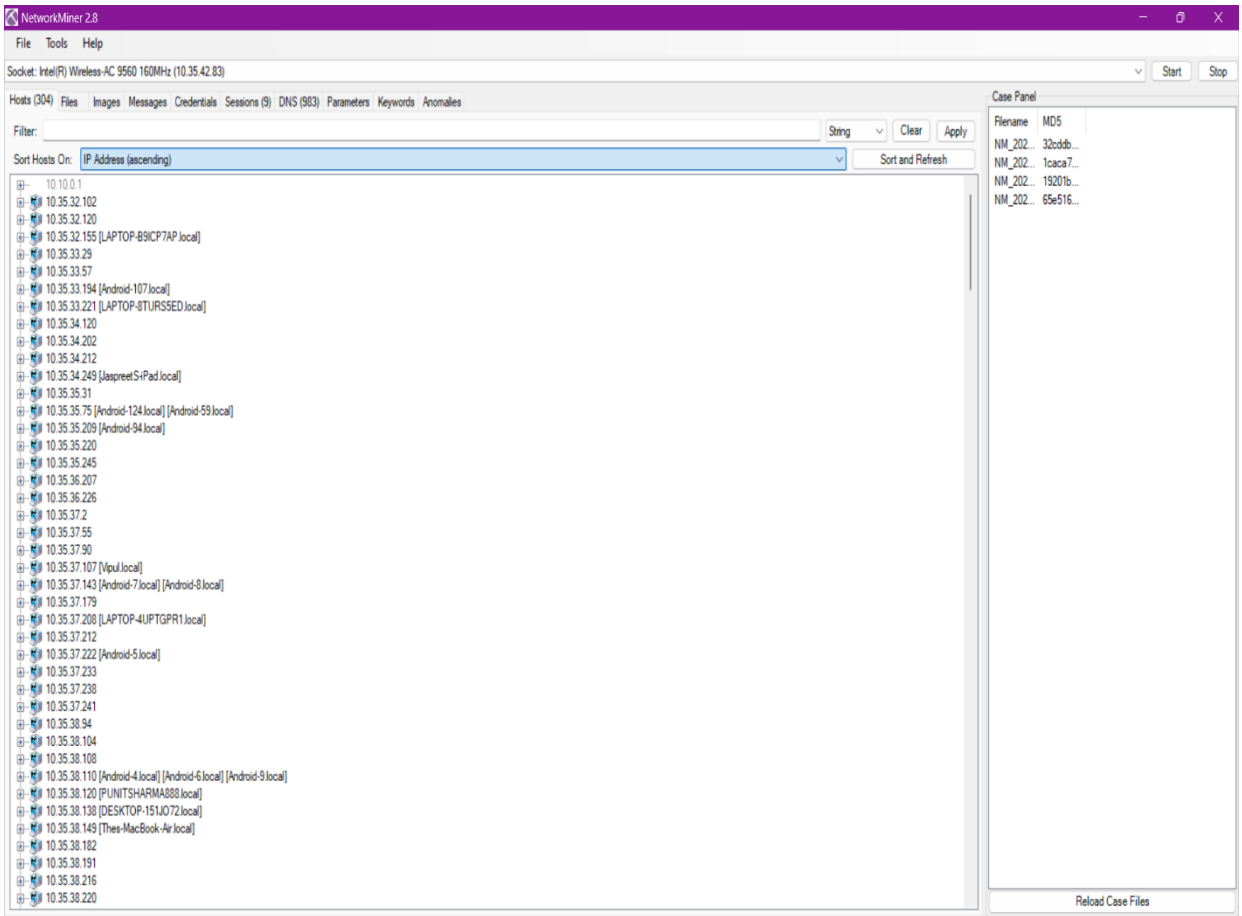


Configurable time zone (UTC, local or custom)		✅
Geo IP localization (***)		✅
DNS Whitelisting (****)		✅
Advanced OS fingerprinting		✅
Web browser tracing (4:10 into this video)		✅
Online ad and tracker detection		✅
Host coloring support		✅
Command line scripting support		✅ (through NetworkMinerCLI)
Price	Free	$ 1200 USD
	Download NetworkMiner (free edition)	**Buy NetworkMiner Professional**

** Fingerprinting of Operating Systems (OS) is performed by using databases from Satori and p0f*
*** Identified protocols include: DNS, FTP, HTTP, HTTP2, IRC, Meterpreter, NetBIOS NameService, NetBios SessionService, Socks, Spotify's Server Protocol, SSH, SSL, TDS (MS-SQL) and TPKT*
**** This product includes GeoLite data created by MaxMind, available from maxmind.com*
***** Domain names in the DNS tab are checked against the Alexa top 1,000,000 sites*




NetworkMiner 2.8
File Tools Help
Socket: Intel(R) Wireless-AC 9560 160MHz (10.35.42.83)
Start
Stop
Hosts (304) Files Images Messages Credentials Sessions (9) DNS (983) Parameters Keywords Anomalies
Filter:
String
Clear
Apply
Sort Hosts On: IP Address (ascending)
Sort and Refresh
10.10.0.1
10.35.32.102
10.35.32.120
10.35.32.155 [LAPTOP-B9ICP7AP.local]
10.35.33.29
10.35.33.57
10.35.33.194 [Android-107.local]
10.35.33.221 [LAPTOP-8TURS5ED.local]
10.35.34.120
10.35.34.202
10.35.34.212
10.35.34.249 [JaspreetS-iPad.local]
10.35.35.31
10.35.35.75 [Android-124.local] [Android-59.local]
10.35.35.209 [Android-94.local]
10.35.35.220
10.35.35.245
10.35.36.207
10.35.36.226
10.35.37.2
10.35.37.55
10.35.37.90
10.35.37.107 [Vipul.local]
10.35.37.143 [Android-7.local] [Android-8.local]
10.35.37.179
10.35.37.208 [LAPTOP-4UPTGPR1.local]
10.35.37.212
10.35.37.222 [Android-5.local]
10.35.37.233
10.35.37.238
10.35.37.241
10.35.38.94
10.35.38.104
10.35.38.108
10.35.38.110 [Android-4.local] [Android-6.local] [Android-9.local]
10.35.38.120 [PUNITSHARMA888.local]
10.35.38.138 [DESKTOP-151JO72.local]
10.35.38.149 [Thes-MacBook-Air.local]
10.35.38.182
10.35.38.191
10.35.38.216
10.35.38.220
Case Panel
Filename MD5
NM_202... 32cddb...
NM_202... 1caca7...
NM_202... 19201b...
NM_202... 65e516...
Reload Case Files


NetworkMiner 2.8
File Tools Help
Socket: Intel(R) Wireless-AC 9560 160MHz (10.35.42.83)
Start
Stop
Hosts (304) Files Images Messages Credentials Sessions (9) DNS (983) Parameters Keywords Anomalies
Filter:
String
Clear
Apply
Sort Hosts On: IP Address (ascending)
Sort and Refresh
10.10.0.1
10.35.32.102
10.35.32.120
10.35.32.155 [LAPTOP-B9ICP7AP.local]
10.35.33.29
10.35.33.57
10.35.33.194 [Android-107.local]
10.35.33.221 [LAPTOP-8TURS5ED.local]
10.35.34.120
10.35.34.202
10.35.34.212
10.35.34.249 [JaspreetS-iPad.local]
10.35.35.31
10.35.35.75 [Android-124.local] [Android-59.local]
10.35.35.209 [Android-94.local]
10.35.35.220
10.35.35.245
10.35.36.207
10.35.36.226
10.35.37.2
10.35.37.55
10.35.37.90
10.35.37.107 [Vipul.local]
10.35.37.143 [Android-7.local] [Android-8.local]
10.35.37.179
10.35.37.208 [LAPTOP-4UPTGPR1.local]
10.35.37.212
10.35.37.222 [Android-5.local]
10.35.37.233
10.35.37.238
10.35.37.241
10.35.38.94
10.35.38.104
10.35.38.108
10.35.38.110 [Android-4.local] [Android-6.local] [Android-9.local]
10.35.38.120 [PUNITSHARMA888.local]
10.35.38.138 [DESKTOP-151JO72.local]
10.35.38.149 [Thes-MacBook-Air.local]
10.35.38.182
10.35.38.191
10.35.38.216
10.35.38.220
Case Panel
Filename MD5
NM_202... 32cddb...
NM_202... 1caca7...
NM_202... 19201b...
NM_202... 65e516...
Reload Case Files

NetworkMiner 2.8

File Tools Help

Socket: Intel(R) Wireless-AC 9560 160MHz (10.35.42.83) Start Stop

Hosts (304) Files Images Messages Credentials Sessions (9) DNS (983) Parameters Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
170	10.35.42.83	51514	103.10.124.123	443	Ssl	2023-04-13 08:54:33 UTC
490	10.35.42.83 (Windows)	53055	52.167.249.196	443	Ssl	2023-04-13 08:57:48 UTC
498	10.35.42.83 (Windows)	53050	52.119.187.0	443	Ssl	2023-04-13 08:57:48 UTC
535	10.35.42.83 (Windows)	53037	13.33.79.163	443	Ssl	2023-04-13 08:57:48 UTC
544	10.35.42.83 (Windows)	53036	10.10.0.1	443		2023-04-13 08:57:48 UTC
553	10.35.42.83 (Windows)	53039	209.191.163.209	443		2023-04-13 08:57:48 UTC
555	10.35.42.83 (Windows)	53045	147.28.129.37	443		2023-04-13 08:57:48 UTC
552	10.35.42.83 (Windows)	53044	209.191.163.209	443		2023-04-13 08:57:48 UTC
560	10.35.42.83 (Windows)	53040	147.28.129.37	443		2023-04-13 08:57:48 UTC

Case Panel

Filename	MD5
NM_202...	32cddb...
NM_202...	1caca7...
NM_202...	19201b...
NM_202...	65e516...

Reload Case Files

NetworkMiner 2.8

File Tools Help

Socket: Intel(R) Wireless-AC 9560 160MHz (10.35.42.83) Start Stop

Hosts (304) Files Images Messages Credentials Sessions (9) DNS (983) Parameters Keywords Anomalies

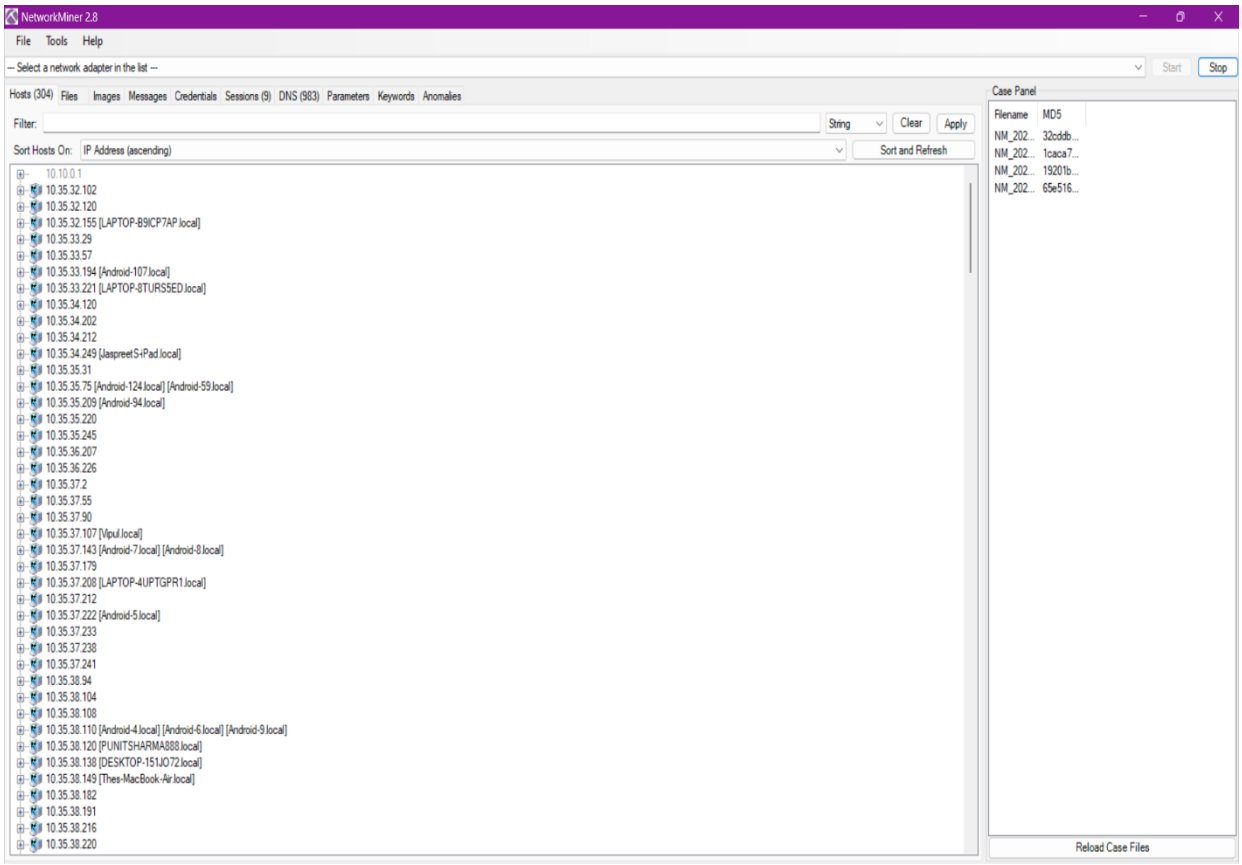
Filter keyword: 10.35.42.83 Case sensitive ExactPhrase Any column Clear Apply

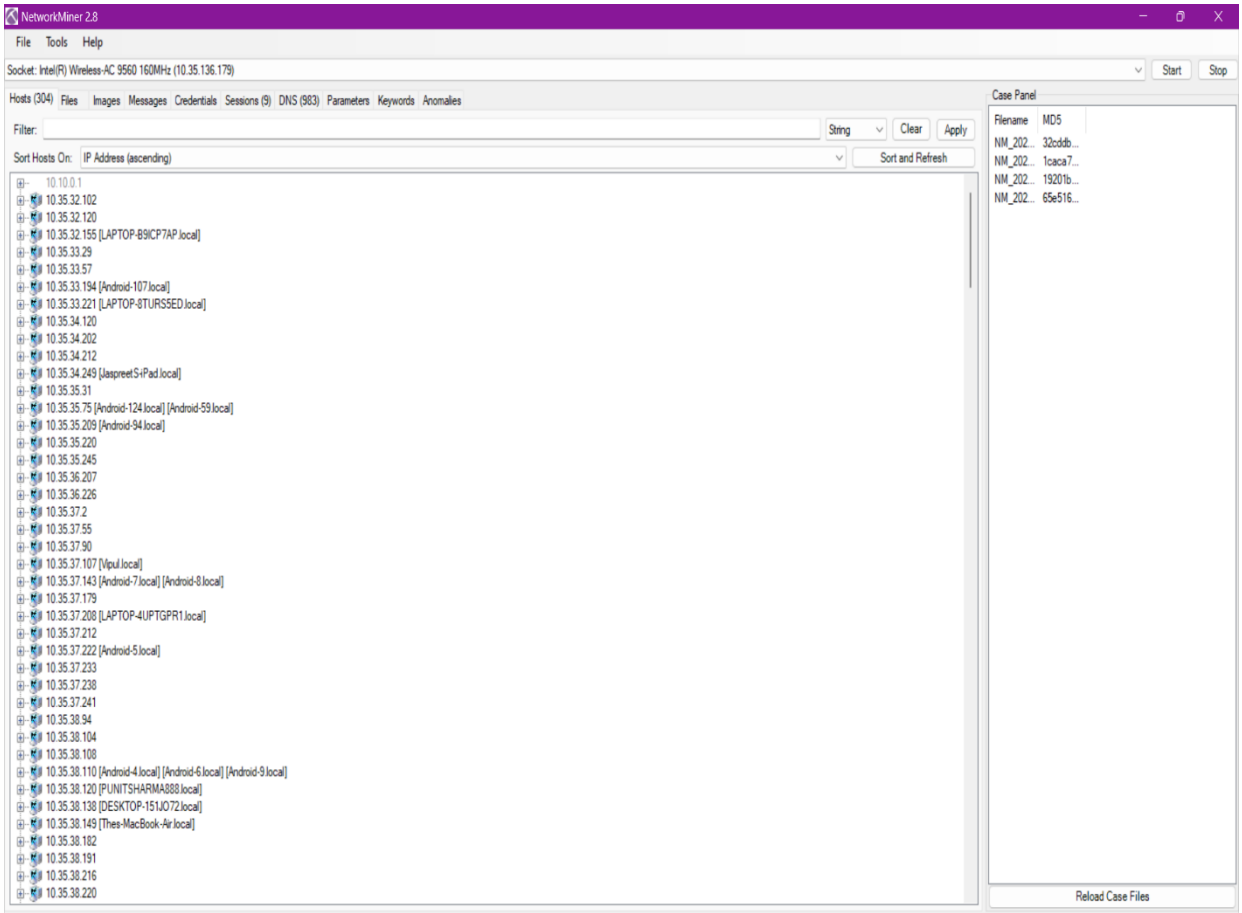
Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DNS Answer	Alexa Top 1M
2023-04-13 08:54:40 UTC	10.35.42.83 (Windows)	52242	172.19.2.254	53	125	00:25:40	0xA37B	0x0005 (CNAME)	www.msftconnecttest.com	ncsi-geo.trafficmanager.net	N/A (Pro version only)
2023-04-13 08:54:40 UTC	10.35.42.83 (Windows)	52242	172.19.2.254	53	125	02:41:16	0xA37B	0x0005 (CNAME)	ncsi-geo.trafficmanager.net	v4ncsi.msedge.net	N/A (Pro version only)
2023-04-13 08:54:40 UTC	10.35.42.83 (Windows)	52242	172.19.2.254	53	125	00:00:59	0xA37B	0x0005 (CNAME)	v4ncsi.msedge.net	ncsi.4-c-0003.c-msedge.net	N/A (Pro version only)
2023-04-13 08:54:40 UTC	10.35.42.83 (Windows)	52242	172.19.2.254	53	125	00:00:09	0xA37B	0x0005 (CNAME)	ncsi.4-c-0003.c-msedge.net	4-c-0003.c-msedge.net	N/A (Pro version only)
2023-04-13 08:54:40 UTC	10.35.42.83 (Windows)	52242	172.19.2.254	53	125	00:00:07	0xA37B	0x0001 (A)	4-c-0003.c-msedge.net	13.107.4.52	N/A (Pro version only)
2023-04-13 09:01:40 UTC	10.35.42.83 (Windows)	55588	172.19.2.252	53	125	00:00:00	0xAAE7	0x0000	ade.googlesyndication.com	No error condition (flags 0x8180)	N/A (Pro version only)
2023-04-13 09:01:40 UTC	10.35.42.83 (Windows)	58624	172.19.2.252	53	125	00:02:30	0x934F	0x0001 (A)	ade.googlesyndication.com	142.251.42.2	N/A (Pro version only)
2023-04-13 09:01:40 UTC	10.35.42.83 (Windows)	50528	172.19.2.252	53	125	00:00:53	0x54A9	0x0005 (CNAME)	beacons.gcp.gvt2.com	beacons-handoff.gcp.gvt2.com	N/A (Pro version only)
2023-04-13 09:01:40 UTC	10.35.42.83 (Windows)	55105	172.19.2.252	53	125	00:00:53	0x88DB	0x0005 (CNAME)	beacons.gcp.gvt2.com	beacons-handoff.gcp.gvt2.com	N/A (Pro version only)
2023-04-13 09:01:40 UTC	10.35.42.83 (Windows)	55105	172.19.2.252	53	125	00:00:33	0x88DB	0x0001 (A)	beacons-handoff.gcp.gvt2.com	172.217.160.163	N/A (Pro version only)
2023-04-13 09:01:41 UTC	10.35.42.83 (Windows)	58286	172.19.2.254	53	125	00:18:39	0x51AD	0x0005 (CNAME)	www.msftconnecttest.com	ncsi-geo.trafficmanager.net	N/A (Pro version only)
2023-04-13 09:01:41 UTC	10.35.42.83 (Windows)	58286	172.19.2.254	53	125	02:34:15	0x51AD	0x0005 (CNAME)	ncsi-geo.trafficmanager.net	v4ncsi.msedge.net	N/A (Pro version only)
2023-04-13 09:01:41 UTC	10.35.42.83 (Windows)	58286	172.19.2.254	53	125	00:00:13	0x51AD	0x0005 (CNAME)	v4ncsi.msedge.net	ncsi.4-c-0003.c-msedge.net	N/A (Pro version only)
2023-04-13 09:01:41 UTC	10.35.42.83 (Windows)	58286	172.19.2.254	53	125	00:00:31	0x51AD	0x0005 (CNAME)	ncsi.4-c-0003.c-msedge.net	4-c-0003.c-msedge.net	N/A (Pro version only)
2023-04-13 09:01:41 UTC	10.35.42.83 (Windows)	58286	172.19.2.254	53	125	00:00:06	0x51AD	0x0001 (A)	4-c-0003.c-msedge.net	13.107.4.52	N/A (Pro version only)

Case Panel

Filename	MD5
NM_202...	32cddb...
NM_202...	1caca7...
NM_202...	19201b...
NM_202...	65e516...

Reload Case Files


NetworkMiner 2.8
File Tools Help
-- Select a network adapter in the list --
Start
Stop
Hosts (304) Files Images Messages Credentials Sessions (9) DNS (983) Parameters Keywords Anomalies
Filter:
String
Clear
Apply
Sort Hosts On: IP Address (ascending)
Sort and Refresh
10.10.0.1
10.35.32.102
10.35.32.120
10.35.32.155 [LAPTOP-B9ICP7AP.local]
10.35.33.29
10.35.33.57
10.35.33.194 [Android-107.local]
10.35.33.221 [LAPTOP-8TURS5ED.local]
10.35.34.120
10.35.34.202
10.35.34.212
10.35.34.249 [JaspreetS-iPad.local]
10.35.35.31
10.35.35.75 [Android-124.local] [Android-59.local]
10.35.35.209 [Android-94.local]
10.35.35.220
10.35.35.245
10.35.36.207
10.35.36.226
10.35.37.2
10.35.37.55
10.35.37.90
10.35.37.107 [Vipul.local]
10.35.37.143 [Android-7.local] [Android-8.local]
10.35.37.179
10.35.37.208 [LAPTOP-4UPTGPR1.local]
10.35.37.212
10.35.37.222 [Android-5.local]
10.35.37.233
10.35.37.238
10.35.37.241
10.35.38.94
10.35.38.104
10.35.38.108
10.35.38.110 [Android-4.local] [Android-6.local] [Android-9.local]
10.35.38.120 [PUNITSHARMA888.local]
10.35.38.138 [DESKTOP-151JO72.local]
10.35.38.149 [Thes-MacBook-Air.local]
10.35.38.182
10.35.38.191
10.35.38.216
10.35.38.220
Case Panel
Filename MD5
NM_202... 32cddb...
NM_202... 1caca7...
NM_202... 19201b...
NM_202... 65e516...
Reload Case Files


NetworkMiner 2.8
File Tools Help
Socket: Intel(R) Wireless-AC 9560 160MHz (10.35.136.179)
Start
Stop
Hosts (304) Files Images Messages Credentials Sessions (9) DNS (983) Parameters Keywords Anomalies
Filter:
String
Clear
Apply
Sort Hosts On: IP Address (ascending)
Sort and Refresh
10.10.0.1
10.35.32.102
10.35.32.120
10.35.32.155 [LAPTOP-B9ICP7AP.local]
10.35.33.29
10.35.33.57
10.35.33.194 [Android-107.local]
10.35.33.221 [LAPTOP-8TURS5ED.local]
10.35.34.120
10.35.34.202
10.35.34.212
10.35.34.249 [JaspreetS-iPad.local]
10.35.35.31
10.35.35.75 [Android-124.local] [Android-59.local]
10.35.35.209 [Android-94.local]
10.35.35.220
10.35.35.245
10.35.36.207
10.35.36.226
10.35.37.2
10.35.37.55
10.35.37.90
10.35.37.107 [Vipul.local]
10.35.37.143 [Android-7.local] [Android-8.local]
10.35.37.179
10.35.37.208 [LAPTOP-4UPTGPR1.local]
10.35.37.212
10.35.37.222 [Android-5.local]
10.35.37.233
10.35.37.238
10.35.37.241
10.35.38.94
10.35.38.104
10.35.38.108
10.35.38.110 [Android-4.local] [Android-6.local] [Android-9.local]
10.35.38.120 [PUNITSHARMA888.local]
10.35.38.138 [DESKTOP-151JO72.local]
10.35.38.149 [Thes-MacBook-Air.local]
10.35.38.182
10.35.38.191
10.35.38.216
10.35.38.220
Case Panel
Filename MD5
NM_202... 32cddb...
NM_202... 1caca7...
NM_202... 19201b...
NM_202... 65e516...
Reload Case Files

NetworkMiner 2.8

File Tools Help

Socket: Intel(R) Wireless-AC 9560 160MHz (10.35.136.179) Start Stop

Hosts (304) Files Images Messages Credentials Sessions (9) DNS (983) Parameters Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
170	10.35.42.83	51514	103.10.124.123	443	Ssl	2023-04-13 08:54:33 UTC
490	10.35.42.83 (Windows)	53055	52.167.249.196	443	Ssl	2023-04-13 08:57:48 UTC
498	10.35.42.83 (Windows)	53050	52.119.187.0	443	Ssl	2023-04-13 08:57:48 UTC
535	10.35.42.83 (Windows)	53037	13.33.79.163	443	Ssl	2023-04-13 08:57:48 UTC
544	10.35.42.83 (Windows)	53036	10.10.0.1	443		2023-04-13 08:57:48 UTC
553	10.35.42.83 (Windows)	53039	209.191.163.209	443		2023-04-13 08:57:48 UTC
555	10.35.42.83 (Windows)	53045	147.28.129.37	443		2023-04-13 08:57:48 UTC
552	10.35.42.83 (Windows)	53044	209.191.163.209	443		2023-04-13 08:57:48 UTC
560	10.35.42.83 (Windows)	53040	147.28.129.37	443		2023-04-13 08:57:48 UTC

Case Panel

Filename	MD5
NM_202...	32cddb...
NM_202...	1caca7...
NM_202...	19201b...
NM_202...	65e516...

Reload Case Files

NetworkMiner 2.8

File Tools Help

Socket: Intel(R) Wireless-AC 9560 160MHz (10.35.136.179) Start Stop

Hosts (304) Files Images Messages Credentials Sessions (9) DNS (983) Parameters Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DNS Answer	Alexa Top 1M
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.43.3...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-9.local	fe80::606d:34ff:fe6b:614f	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.43.3...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-9.local	10.35.43.30	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.41.1...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-103.local	10.35.41.198	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.41.1...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-103.local	fe80::7e6b:9cff:fe26:72b	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.40.1...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-10.local	10.35.40.146	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.40.1...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-10.local	fe80::4dce:4e54:d05c:39f6	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.39.1...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-3.local	10.35.39.165	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.39.1...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-3.local	fe80::cf61:1443:ba95:96bb	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.43.2...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-6.local	fe80::f41e:e7ff:fea0:42e8	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.47.129	5353	255	01:15:00	0x0000	0x0010 (TXT)	{"nm":"Sofia","as":"[8194],...	idHash=MDI0dev=1sec=2app...	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.47.129	5353	255	00:02:00	0x0000	0x0021 (SRV)	{"nm":"Sofia","as":"[8194],...	Android-2.local	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.41.1...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-90.local	10.35.41.133	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.41.1...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-90.local	fe80::72bb:e9ff:fe6d:d928	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.37.2...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-5.local	10.35.37.222	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.37.2...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-5.local	fe80::68d9:85ff:fe4e:59f4	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.43.8...	5353	255	01:15:00	0x0000	0x0010 (TXT)	I0JPRVH8n14AAA_FC9F5E...	f=5220n=MpVUma1qKHDgSl...	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.43.8...	5353	255	00:02:00	0x0000	0x0021 (SRV)	I0JPRVH8n14AAA_FC9F5E...	Android-7.local	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.41.2...	5353	255	01:15:00	0x0000	0x0010 (TXT)	{"nm":"Redmi Note 9 Pro Ma...	idHash=MDA5dev=1sec=2ap...	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.41.2...	5353	255	00:02:00	0x0000	0x0021 (SRV)	{"nm":"Redmi Note 9 Pro Ma...	Android-51.local	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.41.2...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-51.local	10.35.41.22	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.41.2...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-51.local	fe80::e002:f7ff:feaa:1376	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.43.2...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-6.local	10.35.43.26	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.43.2...	5353	255	00:02:00	0x0000	0x0021 (SRV)	{"nm":"Redmi Note 10 Pro M...	Android-6.local	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.40.5...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-109.local	10.35.40.55	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.40.5...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-109.local	fe80::acee:b6ff:fea5:5cb5	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.37.179	5353	255	01:15:00	0x0000	0x0010 (TXT)	Dharshanâs MacBook Air _d...	model=MacBookAir10,1osxver...	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.42.2...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-8.local	10.35.42.215	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.42.2...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-8.local	fe80::c8d3:b48a:56c1:4ac7	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.37.1...	5353	255	00:02:00	0x0000	0x0021 (SRV)	{"nm":"Rampure Rahul","as"...	Android-7.local	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.37.1...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-7.local	10.35.37.143	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.37.1...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-7.local	fe80::4cfb:cbff:fec4:50de	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.43.8...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-7.local	10.35.43.81	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.43.8...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-7.local	fe80::f4c1:66ff:fee3:a5f5	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.42.47	5353	255	01:15:00	0x0000	0x0010 (TXT)	de18e6c8-dda7-4b5c-afb0-a...	txtvers=1host=LAPTOP-3SIN...	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.42.47	5353	255	00:02:00	0x0000	0x0021 (SRV)	de18e6c8-dda7-4b5c-afb0-a...	LAPTOP-3SINS5US.local	N/A (Pro version on
2023-04-13 08:54:29 UTC	224.0.0.251	5353	10.35.39.209	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-5.local	fe80::7aa9:98a8:d62e:458f	N/A (Pro version on
2023-04-13 08:54:30 UTC	224.0.0.251	5353	10.35.39.1...	5353	255	00:02:00	0x0000	0x0001 (A)	Android-4.local	10.35.39.132	N/A (Pro version on
2023-04-13 08:54:30 UTC	224.0.0.251	5353	10.35.39.1...	5353	255	00:02:00	0x0000	0x001C (AAAA)	Android-4.local	fe80::98d9:2fff:fe3d:ef1c	N/A (Pro version on
2023-04-13 08:54:30 UTC	224.0.0.251	5353	10.35.37.1...	5353	255	00:02:00	0x0000	0x0021 (SRV)	{"nm":"Rampure Rahul","as"...	Android-7.local	N/A (Pro version on

Case Panel

Filename	MD5
NM_202...	32cddb...
NM_202...	1caca7...
NM_202...	19201b...
NM_202...	65e516...

Reload Case Files

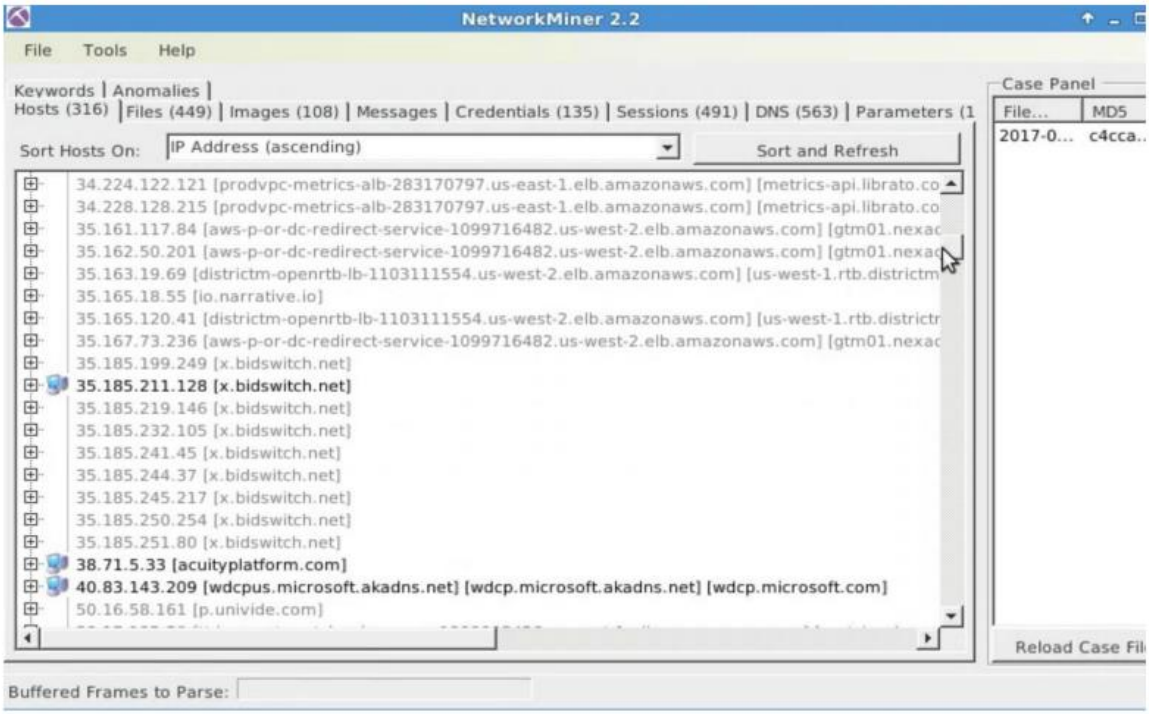
2. For recovery of deleted emails from your email account:

Firstly create pst file: A PST file (Personal Storage Table) is a file format used by Microsoft Outlook to store email messages, contacts, calendar items, and other data. It is a type of data file used by Microsoft Outlook to store messages and other data on your computer's hard drive. PST files are used to create archives of email messages or to backup email messages from an email account.

Secondly install Recover My Email tool: This tool can recover deleted or lost emails from your computer's hard drive, external drives, and other storage devices. It supports Microsoft Outlook email client.

TARGET HOST WILL BE TROJAN INJECTED PC FROM PCAP FILE:

Drag and drop pcap file in network minor tools and u will see the host tab will get populated with various IP.



NetworkMiner Professional 2.8

File Tools Help

--- Select a network adapter in the list --- Start Stop

VoIP (6) Sessions (34951) DNS (16559) Parameters (381771) Keywords Anomalies

Hosts (1376) Browsers (393) Files (14517) Images (72) Messages (170) Credentials (2589)

Filter: Android String Clear Apply

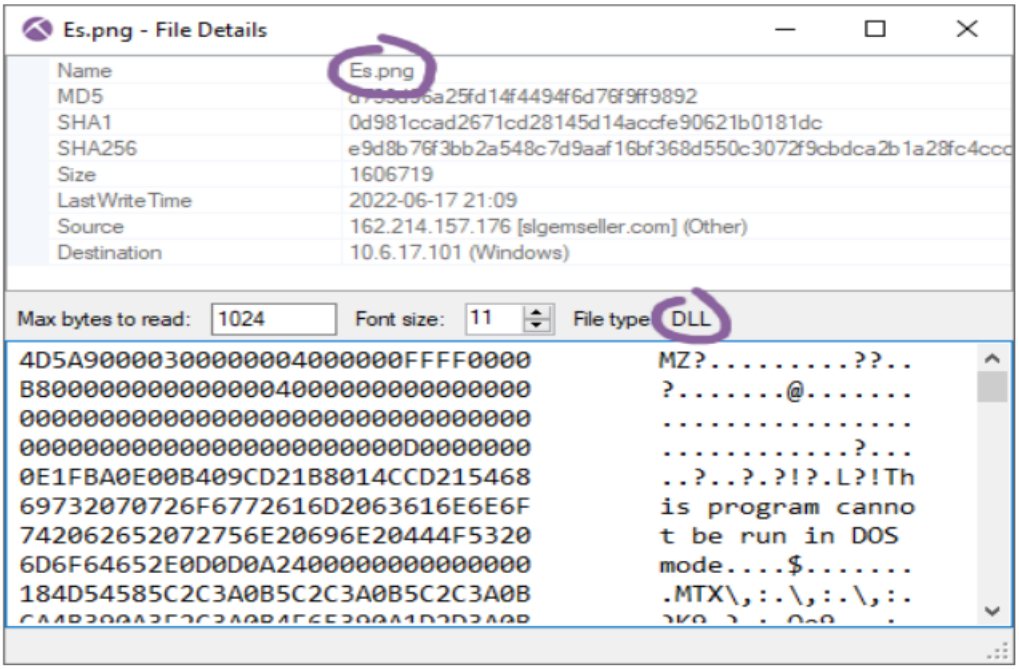
Sort Hosts On: IP Address (ascending) Sort and Refresh

- 114.119.162.196
  - IP: 114.119.162.196
  - MAC: 260206496B31
  - NIC Vendor: Unknown
  - Hostname:
  - GeoIP: SG Singapore
  - OS: Unknown
  - TTL: 41 (distance: 23)
  - Open TCP Ports:
  - Sent: 5 packets (680 Bytes), 0.00% cleartext (0 of 0 Bytes)
  - Received: 5 packets (552 Bytes), 0.00% cleartext (0 of 0 Bytes)
  - Incoming sessions: 0
  - Outgoing sessions: 1
  - Host Details
    - Web Browser User-Agent 1 : Mozilla/5.0 (Linux; Android 7.0;) AppleWebKit/537.36 (
    - Accept-Language 1 : en,zh;q=0.1
    - HTTP header: X-Forwarded-For 1 : 10.179.4.42
- 114.119.165.49
- 192.168.4.25 [android-6d9fdb566158404] [Android.local] (Android)
  - IP: 192.168.4.25
  - MAC: 98FFD096DE2A
  - NIC Vendor: Lenovo Mobile Communication Technology Ltd.
  - MAC Age: 2013-09-21
  - Hostname: android-6d9fdb566158404, Android.local
  - OS: Android
    - Advanced DHCP: Android - Android [SmartDevice] [Android] (100.00%)
    - Satori DHCP: Linux - Linux 2.6 (13.64%) Linux - Linux 3.4 [eBook Reader] [Amazon]
    - Satori TCP: BrightSign HD223 (50.00%) Android - Android 7 (50.00%)
  - TTL: 64 (distance: 0)
  - Open TCP Ports:
  - Sent: 105950 packets (13,951,000 Bytes), 0.00% cleartext (0 of 0 Bytes)
  - Received: 104058 packets (32,955,357 Bytes), 0.00% cleartext (0 of 0 Bytes)
  - Incoming sessions: 0
  - Outgoing sessions: 20071
  - Host Details
    - Queried DNS names : asia.pool.ntp.org,www.googleapis.com,android.googleapis.co
    - Web Browser User-Agent 1 : Dalvik/1.6.0 (Linux; U; Android 4.4.2; Lenovo A7600-F

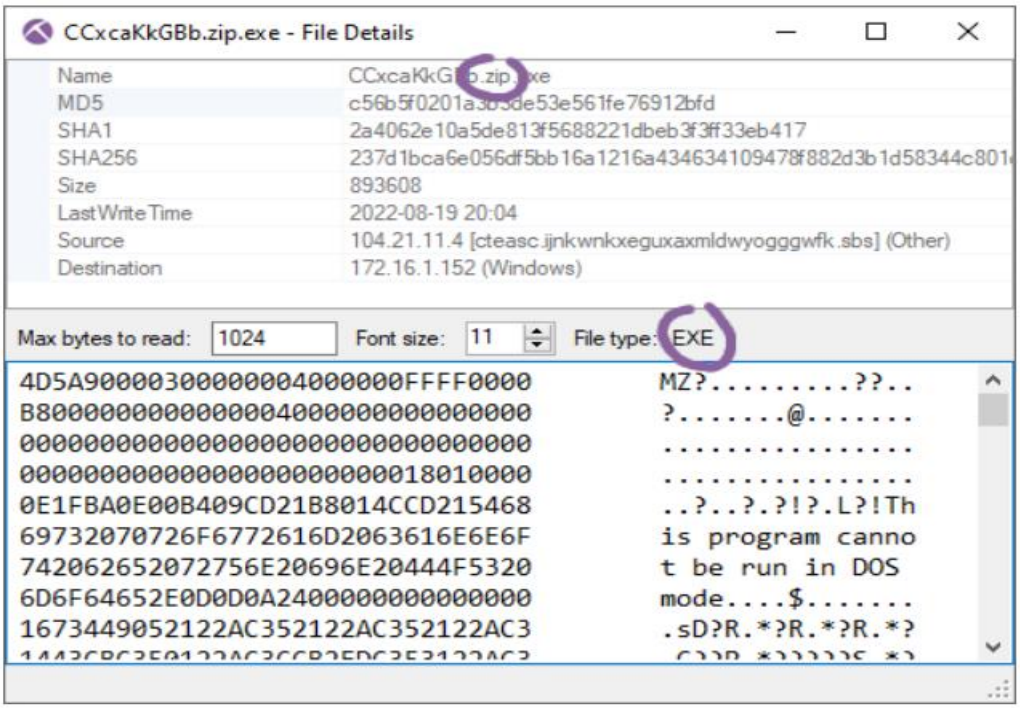
Buffered Frames to Parse:

It's now also possible to copy text from most tabs in NetworkMiner with Ctrl+C or by right-clicking and selecting "Copy selected rows". A maximum of 10 rows can be copied at a time using the free version of NetworkMiner, while the Professional version allows all rows to be copied in one go.

The content based file type identification introduced in NetworkMiner 2.7 has been improved to also differentiate between EXE and DLL files as of version 2.8.



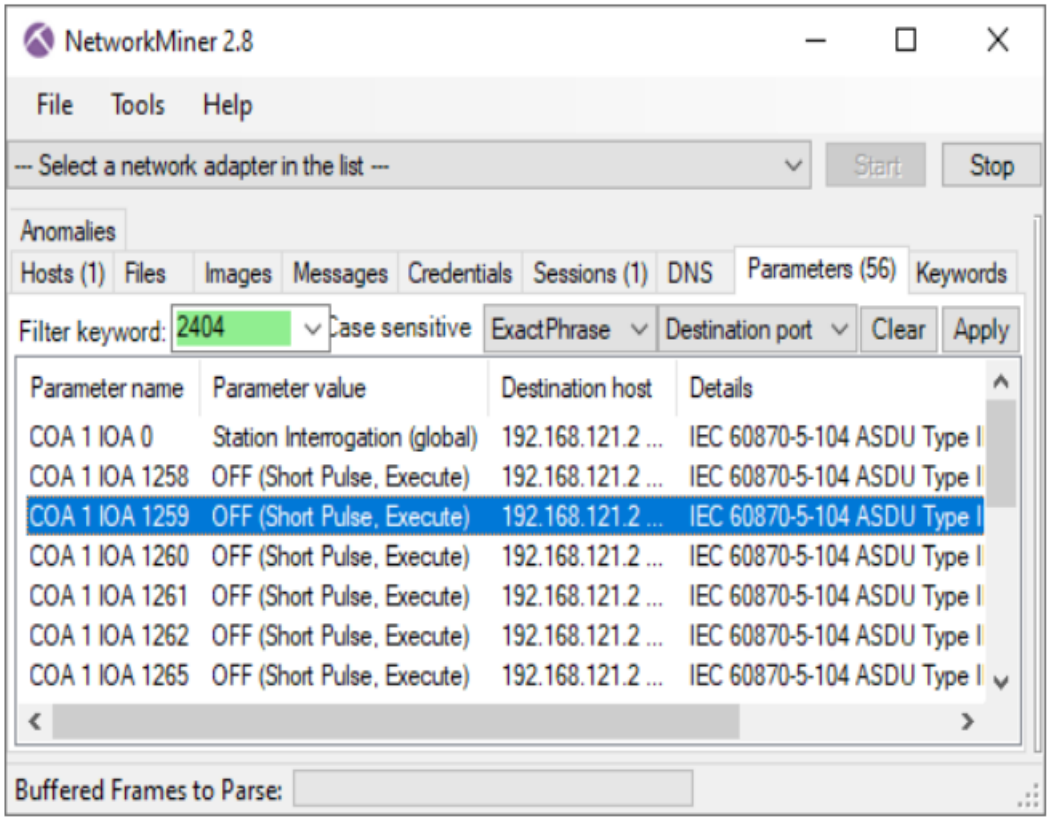
- Matanbuchus malware DLL disguised as PNG
- MD5: d733d96a25fd14f4494f6d76f9ff9892
- Source: 2022-06-17-Matanbuchus-with-Cobalt-Strike.pcap



- AutoIt EXE disguised as ZIP file
- MD5: c56b5f0201a3b3de53e561fe76912bfd
- Source: 2022-08-19-Astaroth-Guildma-infection-traffic.pcap

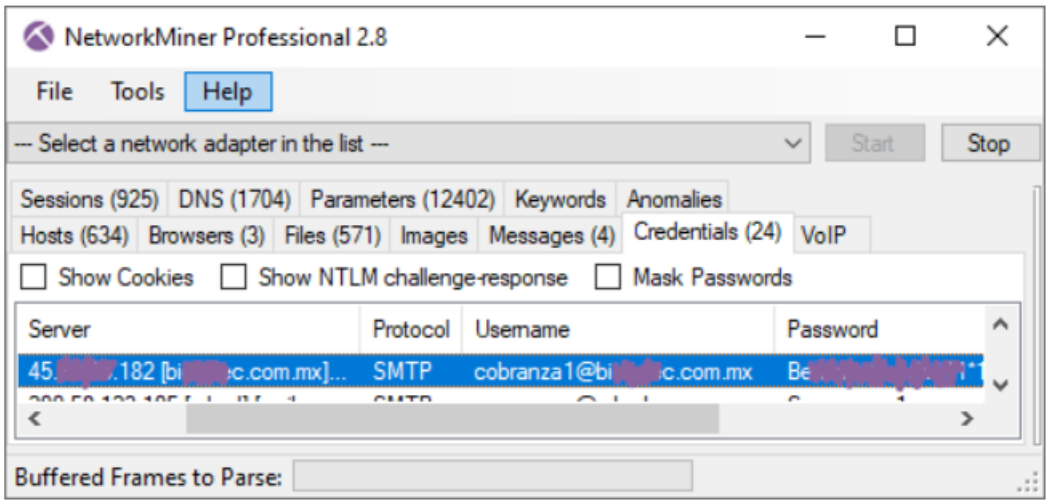
IEC 60870-5-104

NetworkMiner's parser for the SCADA protocol IEC 60870-5-104 (IEC-104) has been significantly improved in version 2.8. NetworkMiner now supports more IEC-104 commands and the commands are presented on the Parameters tab in a clearer way than before.

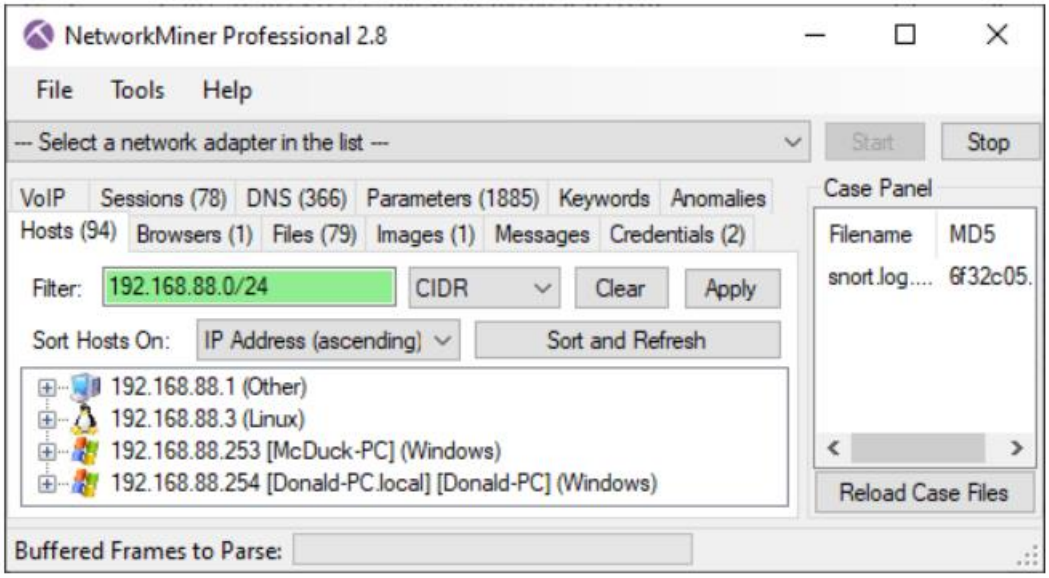


CAPWAP Decapsulation

NetworkMiner 2.8 can read IEEE 802.11 packets inside CAPWAP tunnels between WLAN Controllers and Access Points. This feature allows WiFi traffic to be analyzed without having to capture packets in the air.



In addition to allowing hosts to be filtered using string and regex matching, NetworkMiner Professional also allows the discovered hosts to be filtered on IP address using CIDR notation, such as “192.168.1.0/24” or “10.0.0.0/8”.



- 224.0.0.0/4 = IPv4 multicast (224/4 is also supported)
- 127.0.0.0/8 = IPv4 loopback (127/8 is also supported)
- fe80::/10 = IPv6 link-local addresses
- ff00::/8 = IPv6 multicast
- 0.0.0.0/0 = IPv4 hosts (0/0 is also supported)
- 0::/0 = IPv6 hosts

Reference/ Bibliography

- https://www.autopsy.com/
- https://www.malware-traffic analysis.net/2017/07/22/index.html
- https://github.com/Security-Onion Solutions/security-onion
- https://www.arbornetworks.com/blog/asert/wp content/uploads/2017/05/zyklon_season.pdf
- https://www.netresec.com/?page=NetworkMiner
- https://www.kali.org/tools/theharvester/#:~:text=The%20package%20contains%20a%20tool,Installed%20size%3A%201.72%20MB
- https://www.youtube.com/watch?v=S6V66G2tVr8
- https://www.youtube.com/watch?v=cDryilcK39c
- https://en.wikipedia.org/wiki/Autopsy_(software)
- https://www.oreilly.com/library/view/web-penetration-testing/9781788623377/71203ba9-3894-4192-af66-1003405ab8ed.xhtml
- https://youtu.be/behDv6HEIrk
- https://www.igi-global.com/dictionary/introduction-to-email-web-and-messageforensics/82333