CUMULATIVE ASSIGNMENT – 3

Section – K19AP

Coarse Code – INT301

OPEN-SOURCE TECHNOLOGIES

Topic: Implement a network miner tool to detect the operating system, sessions and open ports through packet sniffing and investigate the network traffic.

Submitted By -	**Submitted To -**
Himanshu Dixit	Rajeshwar Sharma
(11904892)	(29484)
Roll No - 51	

CONTENT

1: Introduction

1.1 Objective:

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 Features:

- To appeal to a larger audience, the network miner programme should be made to run on many operating systems, including Windows, macOS, and Linux.
- The tool should have the ability to filter network traffic so that it only collects the relevant packets that include the data needed for the analysis.
- This can enhance the functionality of the instrument and lessen the amount of data that has to be analysed.
- To give a thorough analysis of the network traffic, the tool should be able to recognise and analyse the various protocols used in network traffic, such as TCP, UDP, and ICMP.
- The programme must be able to recognise encrypted communication, such as SSL/TLS, and make an effort to decode it in order to obtain the necessary data.
- This tool should be able to produce reports that list the findings of the network analysis and offer suggestions for resolving any security issues.
- This can assist users in taking the necessary steps to protect their network and fend off any assaults.

1.3 How tools work:

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.

2: System/ Tool Description

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.

Finally document our study and any vulnerabilities or security concerns you have found, finalise your conclusions and offer recommendations. Make sure to include any patches or updates that need be deployed, network configuration modifications that should be made, or extra security tools that should be introduced in your suggestions for strengthening the network's security posture.

2.1 Assumptions and Dependency

There are a few presumptions and dependencies that need to be taken into account before implementing a network miner programme to analyse network traffic and determine the operating system, sessions, and open ports using packet sniffing. These consist of:

Assumptions:

1. The packet sniffing is being done on a network that the target system is connected to.
2. The network miner tool may record and examine network traffic produced by the target system.
3. The target system's network communication is not encrypted and can be read in plaintext.
4. The network miner tool has the required access and authorizations to record and examine network traffic.

Dependencies:

1. In order to record and examine network traffic, the network miner programme needs a computer or server with adequate processing and storage capabilities.

2. To record network traffic, the network miner programme uses a packet capture library, such as libpcap or WinPcap.

3. The completeness and correctness of the packet capture data are necessary for the network miner tool's analysis to be accurate.

4. To parse and examine various network protocols, the network miner programme can need particular software libraries or frameworks.

All things considered, it is crucial to take into account these presumptions and dependencies when putting into practise a network miner tool to make sure that it is successful in identifying the operating system, sessions, and open ports through packet sniffing and network traffic analysis.

2.2 Functional and Non-functional Dependency

Functional dependencies are the specifications and characteristics that a network mining tool must offer to serve the goal for which it was designed. In the context of this assignment, the functional dependencies refer to the specific characteristics that the network mining tool must possess in order to analyse network traffic and determine the operating system, sessions, and open ports using packet sniffing.

Functional prerequisites for the task of developing a network miner programme to examine network traffic and packet-sniff the operating system, sessions, and open ports might include:

1. The capacity to record network traffic from numerous sources, including pcap files and live network interfaces.
2. The capacity to decipher and examine recorded network traffic in order to identify the operating system, open ports, and network sessions of the target machine.
3. The capability of reconstructing files transported over the network, enabling investigators to recover files and other material that could be concealed inside network traffic.
4. The capability of offering an easy-to-use interface for seeing and assessing network traffic.
5. The capability to export data from analysis and network traffic capture in a range of formats for further analysis

Non-functional dependencies for the assignment may include:

On the other hand, non-functional dependencies relate to the qualities that the network miner tool must have to guarantee that it functions effectively, efficiently, and securely. Non-functional dependencies in this assignment refer to the performance, reliability, security, and compatibility criteria that the network miner tool must satisfy in order to successfully carry out its intended role.

1. Performance: The network miner programme should be able to process and manage a lot of network traffic quickly.
2. Reliability: The network miner tool should provide accurate data and be dependable.

3. Security: The network miner tool must be safe and not endanger the network or the monitored devices.
4. Compatibility: The assignment's software and operating system should be compatible with the network miner programme.

In general, dependencies that are both functional and non-functional must be taken into account when using a network miner tool for network forensics study. By taking into account these requirements, the programme may be created to quickly and precisely identify open ports, sessions, and the operating system of the target machine via packet sniffing.

In summary, functional dependencies define the specific features and capabilities required of the network miner tool, while non-functional dependencies specify the general operational characteristics that the tool must possess to perform its intended function adequately.

2.3 Target System Description

Here the target system considers to do this project are 2 machines, they are-

- First one is host window the software is running on i.e., my laptop
- Second one is the host from the Trojan infected window machine in traffic analysis prebuild PCA file

2.4 Dataset

PCAP FILE

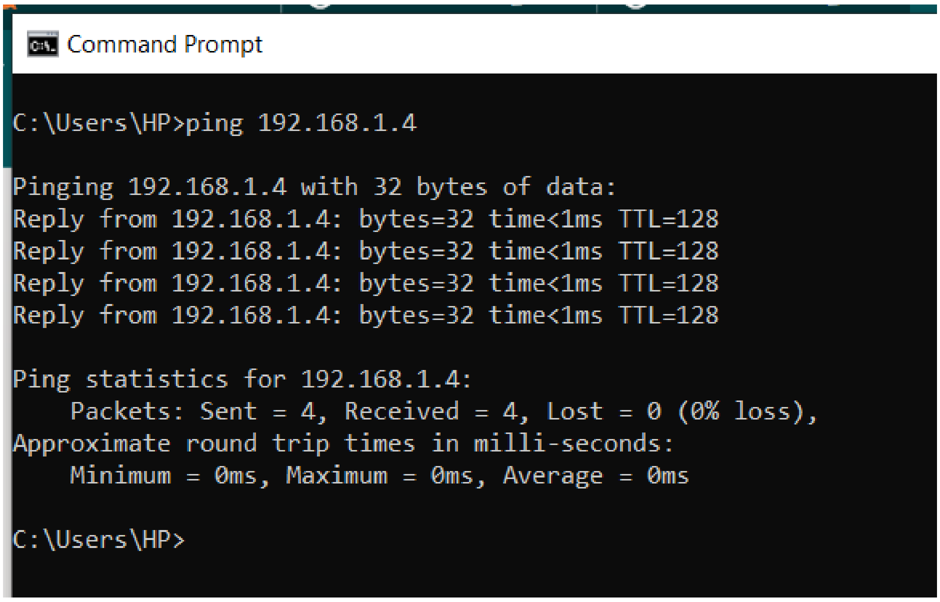
2017-07-22 - TRAFFIC ANALYSIS EXERCISE - WHERE DREAMS ARE MADE

https://www.malware-traffic-analysis.net/2017/07/22/index.html

3: ANALYSIS REPORT

HOST 1: WINDOW LAPTOP(SELF)

First, we will send packet to the host window machine of IP address shown in the picture using ping command, after confirming the packet send, we move to next part



Command Prompt

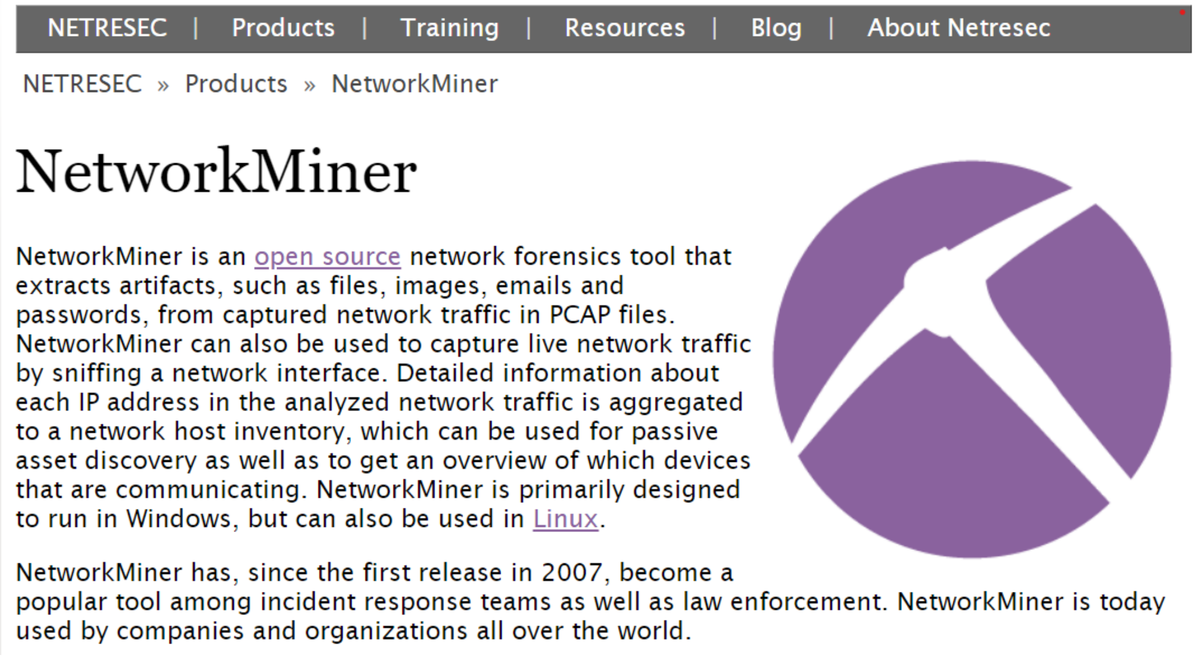
```
C:\Users\HP>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\HP>
```

While setting up in NETRESEC choose network minor



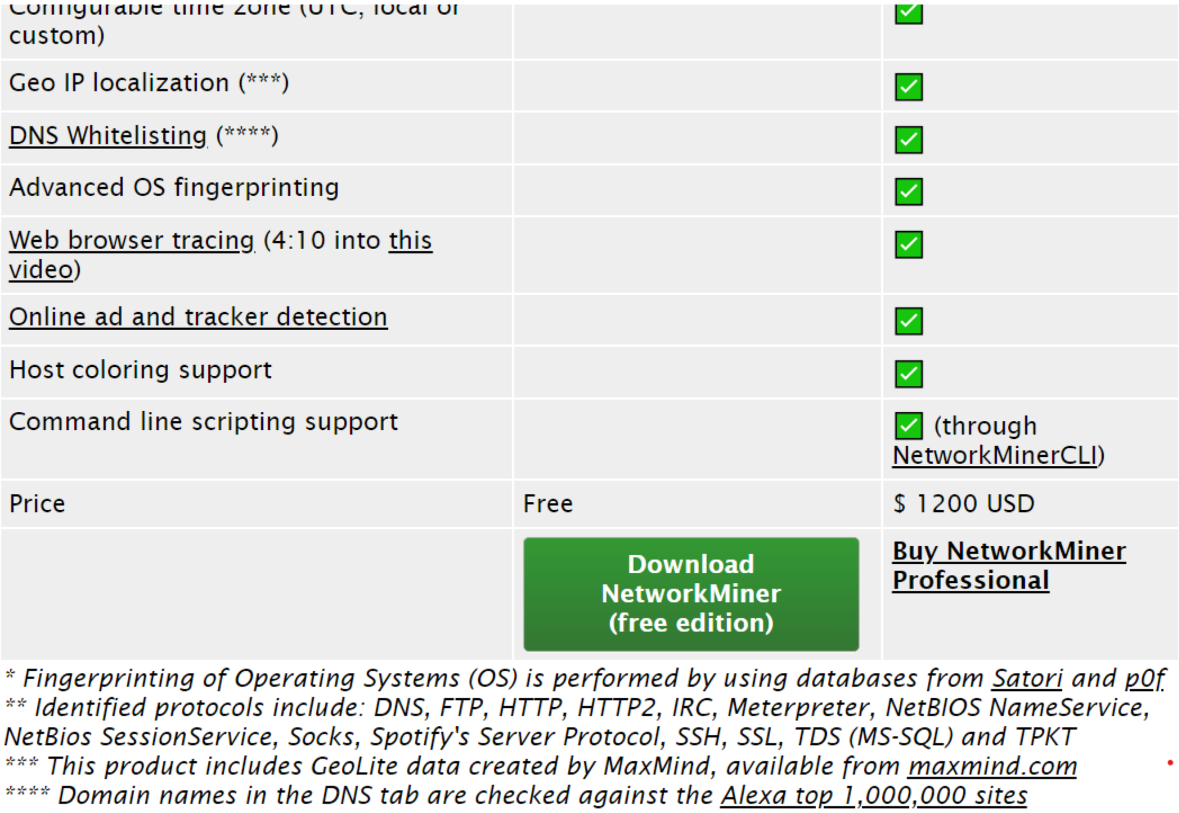
NETRESEC | Products | Training | Resources | Blog | About Netresec
NETRESEC » Products » NetworkMiner

NetworkMiner

NetworkMiner is an open source network forensics tool that extracts artifacts, such as files, images, emails and passwords, from captured network traffic in PCAP files. NetworkMiner 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. NetworkMiner is primarily designed to run in Windows, but can also be used in Linux.

NetworkMiner has, since the first release in 2007, become a popular tool among incident response teams as well as law enforcement. NetworkMiner is today used by companies and organizations all over the world.

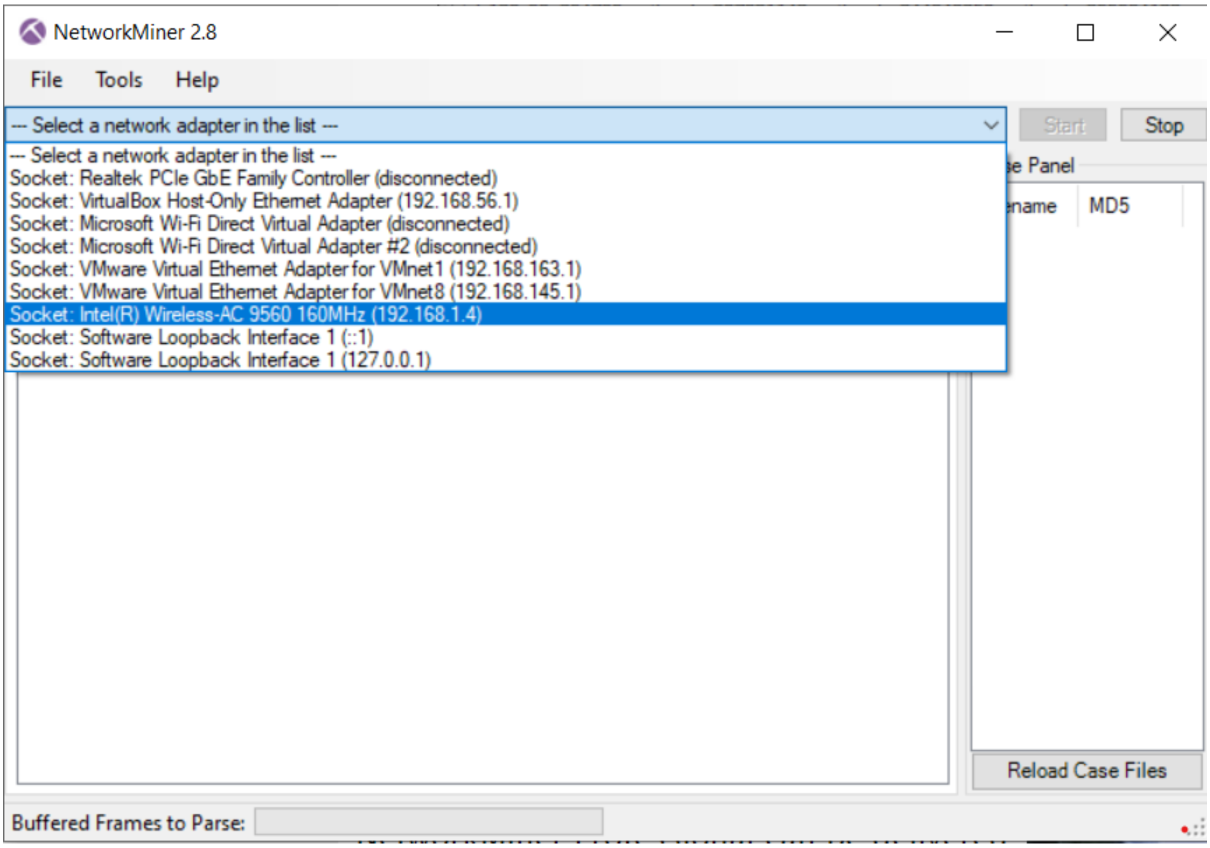
Download the network minor community version



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*

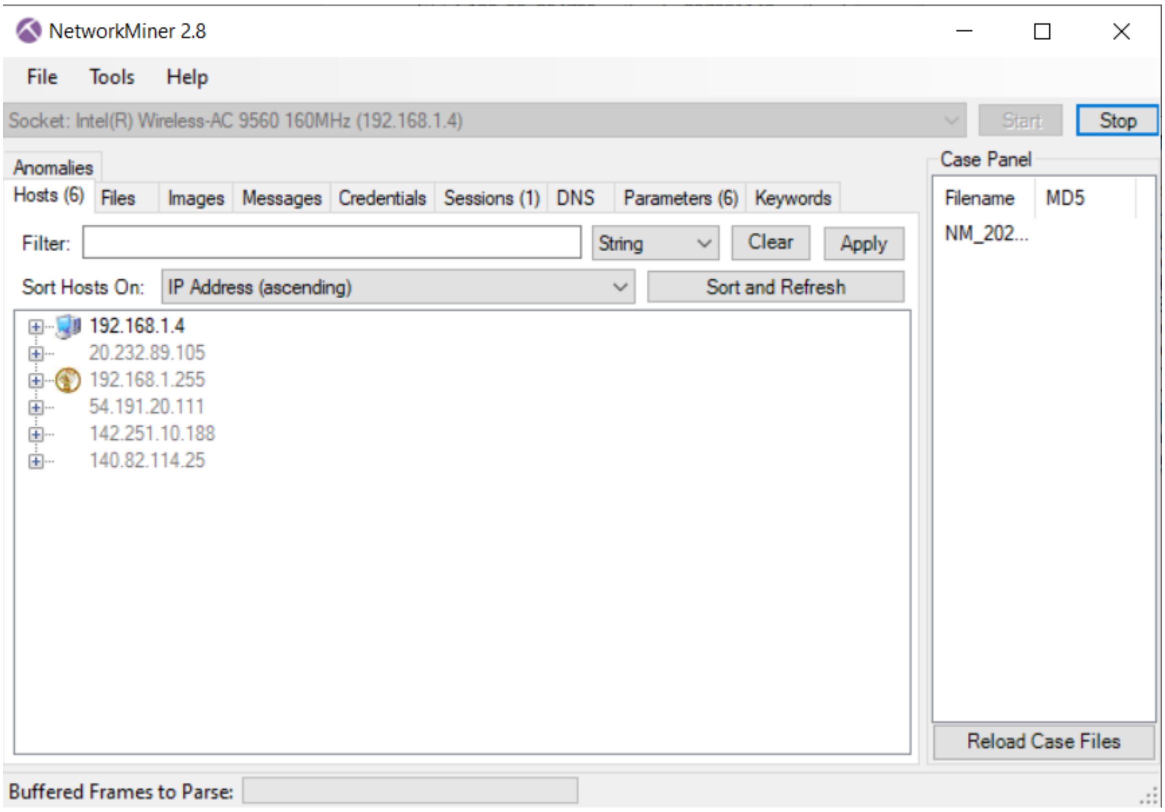
Run the network minor tool in run the administrative privileges and choose the desired adapter to capture the host and machines



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

--- Select a network adapter in the list ---
Socket: Realtek PCIe GbE Family Controller (disconnected)
Socket: VirtualBox Host-Only Ethernet Adapter (192.168.56.1)
Socket: Microsoft Wi-Fi Direct Virtual Adapter (disconnected)
Socket: Microsoft Wi-Fi Direct Virtual Adapter #2 (disconnected)
Socket: VMware Virtual Ethernet Adapter for VMnet1 (192.168.163.1)
Socket: VMware Virtual Ethernet Adapter for VMnet8 (192.168.145.1)
Socket: Intel(R) Wireless-AC 9560 160MHz (192.168.1.4)
Socket: Software Loopback Interface 1 (::1)
Socket: Software Loopback Interface 1 (127.0.0.1)

Most of the IP captured by the tool have a strong firewall. So, for analysis you can stop the firewall if host is known or choose the host with on local machine.



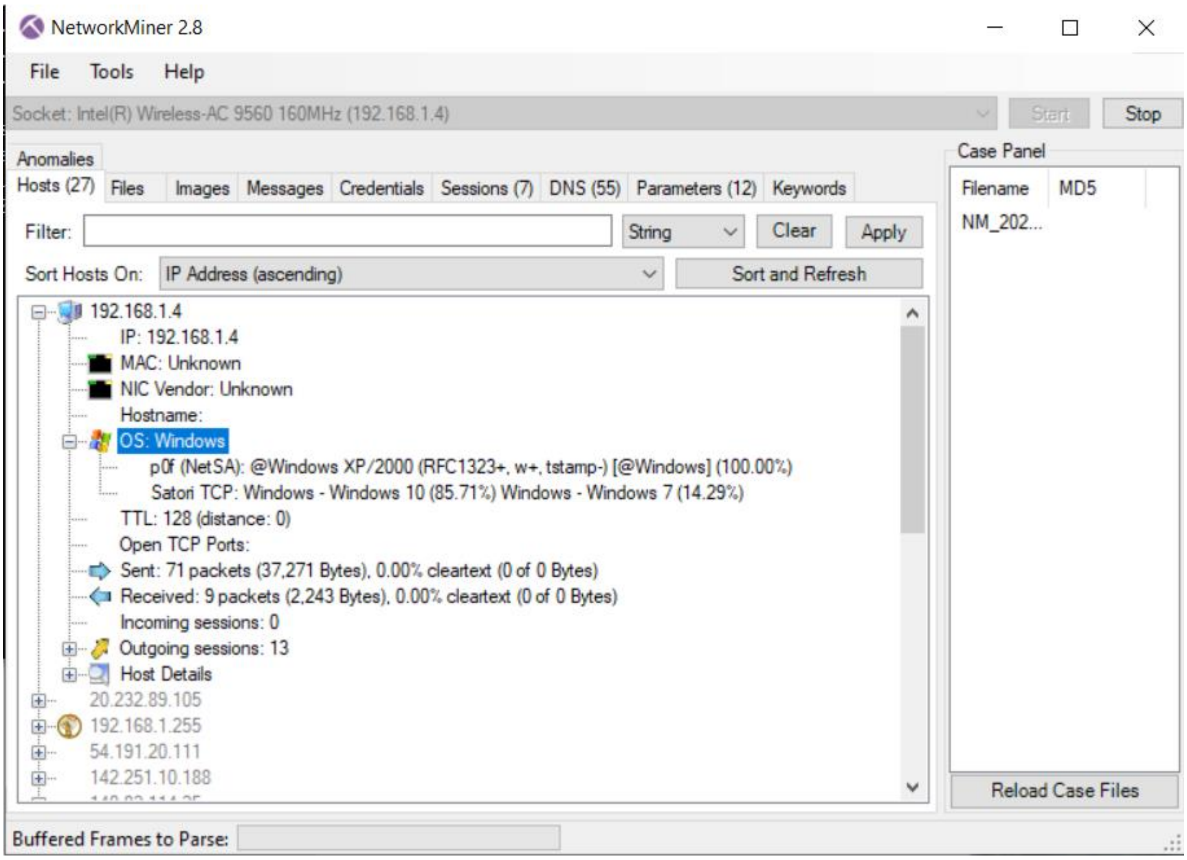
Socket: Intel(R) Wireless-AC 9560 160MHz (192.168.1.4)

Sort Hosts On: IP Address (ascending)

```
192.168.1.4
20.232.89.105
192.168.1.255
54.191.20.111
142.251.10.188
140.82.114.25
```

NM_202...

Select the local machine as host and click the IP to check for details capture of OS, sessions and etc.



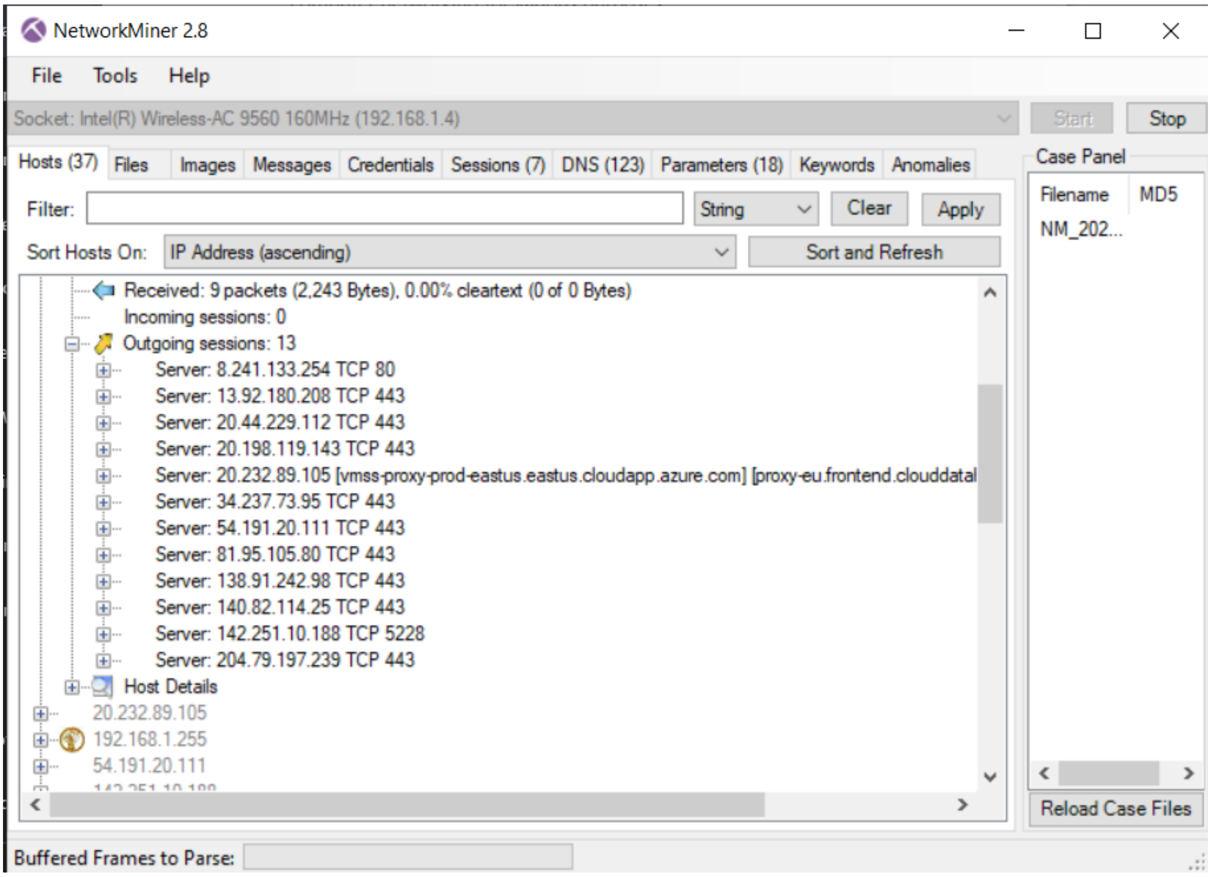
Socket: Intel(R) Wireless-AC 9560 160MHz (192.168.1.4)

Sort Hosts On: IP Address (ascending)

```
192.168.1.4
    IP: 192.168.1.4
    MAC: Unknown
    NIC Vendor: Unknown
    Hostname:
    OS: Windows
        p0f (NetSA): @Windows XP/2000 (RFC1323+, w+, tstamp-) [@Windows] (100.00%)
        Satori TCP: Windows - Windows 10 (85.71%) Windows - Windows 7 (14.29%)
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 71 packets (37,271 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 9 packets (2,243 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 13
    Host Details
20.232.89.105
192.168.1.255
54.191.20.111
142.251.10.188
```

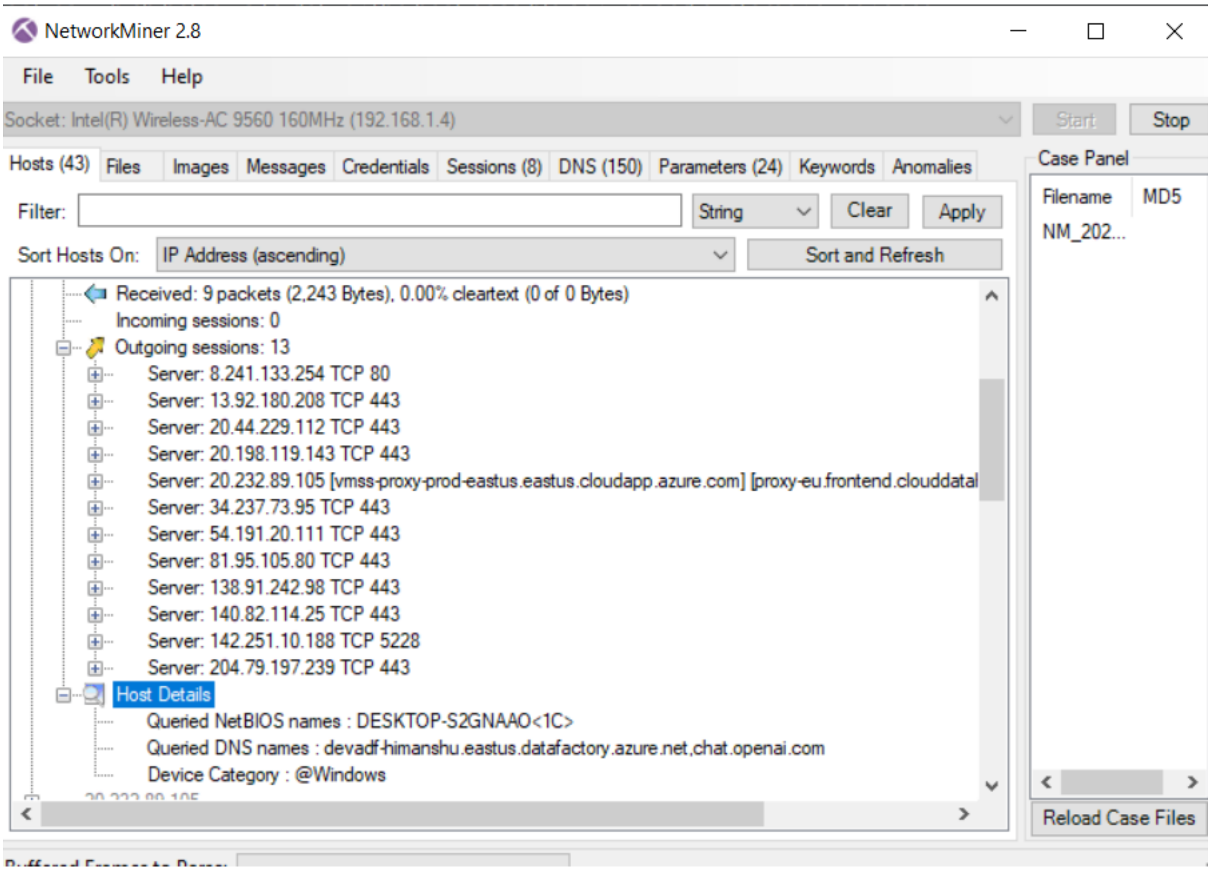
NM_202...

After opening various webpages local machine, check the total packet we send or received by using the internet and ping command we used earlier



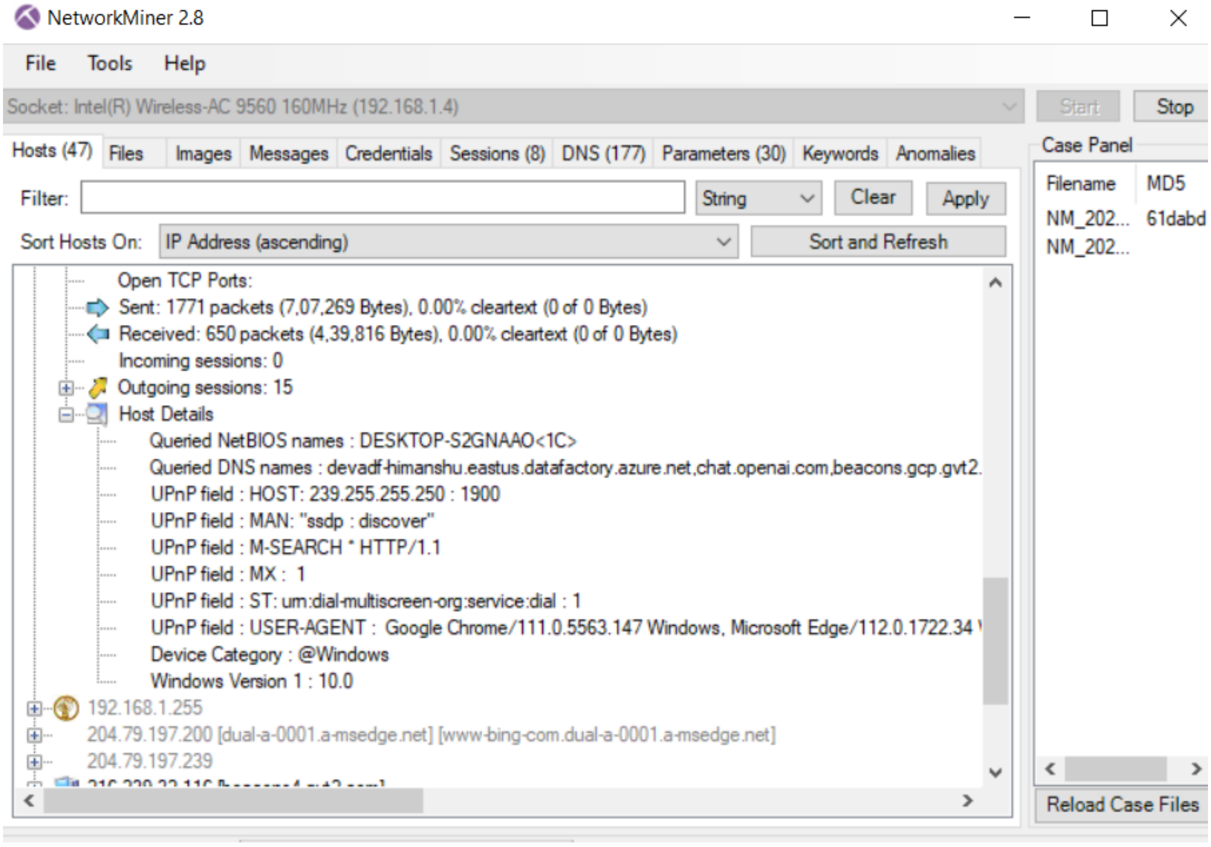
```
Received: 9 packets (2,243 Bytes), 0.00% cleartext (0 of 0 Bytes)
Incoming sessions: 0
Outgoing sessions: 13
    Server: 8.241.133.254 TCP 80
    Server: 13.92.180.208 TCP 443
    Server: 20.44.229.112 TCP 443
    Server: 20.198.119.143 TCP 443
    Server: 20.232.89.105 [vmss-proxy-prod-eastus.eastus.cloudapp.azure.com] [proxy-eu.frontend.clouddatal
    Server: 34.237.73.95 TCP 443
    Server: 54.191.20.111 TCP 443
    Server: 81.95.105.80 TCP 443
    Server: 138.91.242.98 TCP 443
    Server: 140.82.114.25 TCP 443
    Server: 142.251.10.188 TCP 5228
    Server: 204.79.197.239 TCP 443
Host Details
20.232.89.105
192.168.1.255
54.191.20.111
```

Cross- verify the outgoing sessions and incoming sessions and analyze the sessions and ports connected, usually it is TPC as we connected to webpages



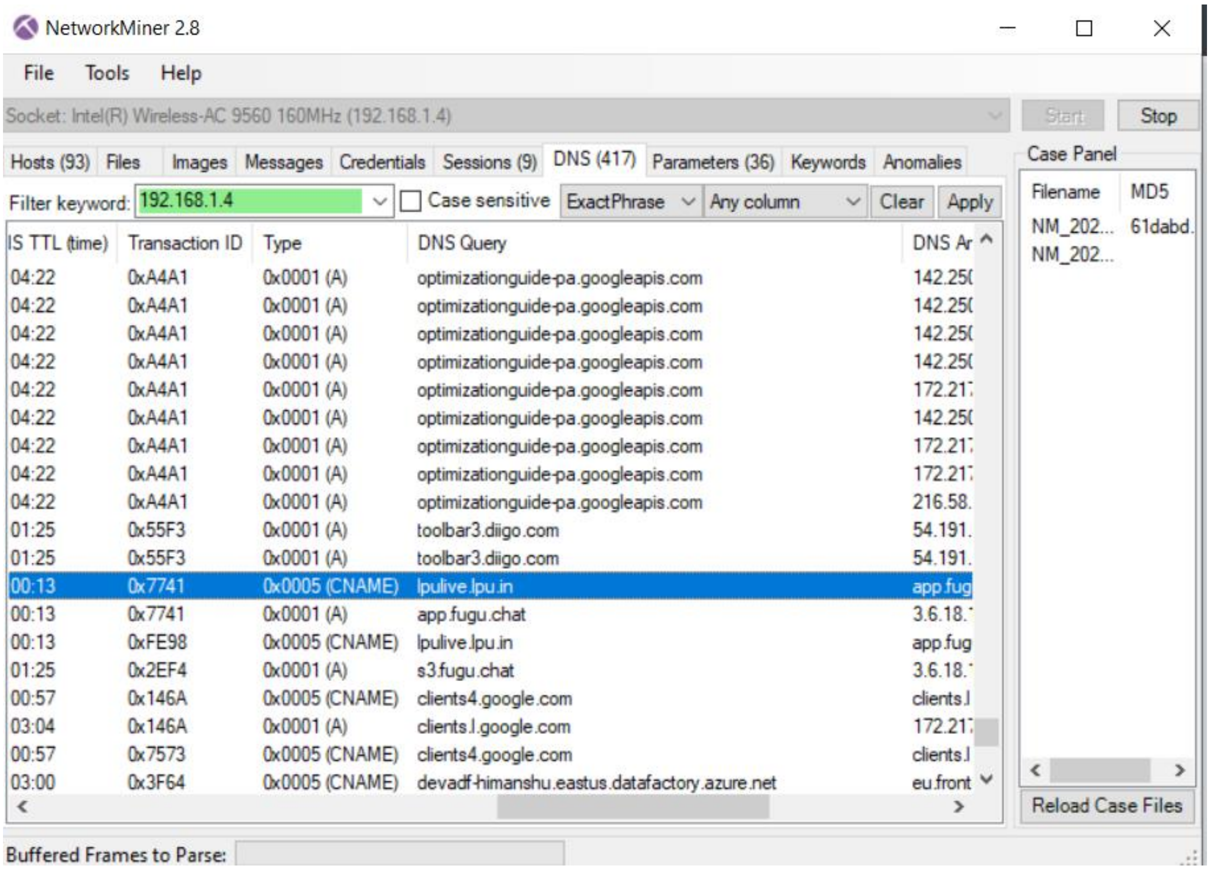
```
Received: 9 packets (2,243 Bytes), 0.00% cleartext (0 of 0 Bytes)
Incoming sessions: 0
Outgoing sessions: 13
    Server: 8.241.133.254 TCP 80
    Server: 13.92.180.208 TCP 443
    Server: 20.44.229.112 TCP 443
    Server: 20.198.119.143 TCP 443
    Server: 20.232.89.105 [vmss-proxy-prod-eastus.eastus.cloudapp.azure.com] [proxy-eu.frontend.clouddatal
    Server: 34.237.73.95 TCP 443
    Server: 54.191.20.111 TCP 443
    Server: 81.95.105.80 TCP 443
    Server: 138.91.242.98 TCP 443
    Server: 140.82.114.25 TCP 443
    Server: 142.251.10.188 TCP 5228
    Server: 204.79.197.239 TCP 443
Host Details
    Queried NetBIOS names : DESKTOP-S2GNAAO<1C>
    Queried DNS names : devadf-himanshu.eastus.datafactory.azure.net,chat.openai.com
    Device Category : @Windows
```

Check the host detail of selected host and cross verify the OS of the machine and see DNS query


NetworkMiner 2.8
File Tools Help
Socket: Intel(R) Wireless-AC 9560 160MHz (192.168.1.4)
Start Stop
Hosts (47) Files Images Messages Credentials Sessions (8) DNS (177) Parameters (30) Keywords Anomalies
Case Panel
Filter:
String Clear Apply
Sort Hosts On: IP Address (ascending)
Sort and Refresh
Filename MD5
NM_202... 61dabd
NM_202...
Reload Case Files

```
Open TCP Ports:
Sent: 1771 packets (7,07,269 Bytes), 0.00% cleartext (0 of 0 Bytes)
Received: 650 packets (4,39,816 Bytes), 0.00% cleartext (0 of 0 Bytes)
Incoming sessions: 0
Outgoing sessions: 15
Host Details
    Queried NetBIOS names : DESKTOP-S2GNAAO<1C>
    Queried DNS names : devadf-himanshu.eastus.datafactory.azure.net,chat.openai.com,beacons.gcp.gvt2.
    UPnP field : HOST: 239.255.255.250 : 1900
    UPnP field : MAN: "ssdp : discover"
    UPnP field : M-SEARCH * HTTP/1.1
    UPnP field : MX : 1
    UPnP field : ST: urn:dial-multiscreen-org:service:dial : 1
    UPnP field : USER-AGENT : Google Chrome/111.0.5563.147 Windows, Microsoft Edge/112.0.1722.34
    Device Category : @Windows
    Windows Version 1 : 10.0
192.168.1.255
204.79.197.200 [dual-a-0001.a-msedge.net] [www-bing-com.dual-a-0001.a-msedge.net]
204.79.197.239
```

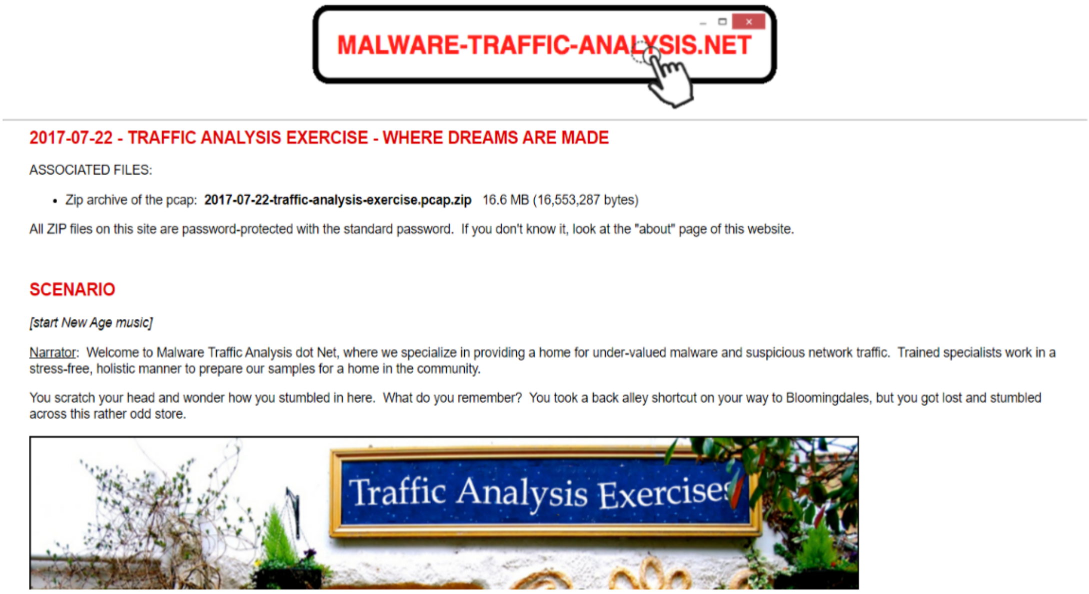
You can see all the DNS query by this host in the DNS section by selecting the desired IP of the target system and see which website we are using, here it is LPU LIVE


NetworkMiner 2.8
File Tools Help
Socket: Intel(R) Wireless-AC 9560 160MHz (192.168.1.4)
Start Stop
Hosts (93) Files Images Messages Credentials Sessions (9) DNS (417) Parameters (36) Keywords Anomalies
Case Panel
Filter keyword: 192.168.1.4
□ Case sensitive
ExactPhrase Any column Clear Apply
Filename MD5
NM_202... 61dabd.
NM_202...
Reload Case Files
Buffered Frames to Parse:

IS TTL (time)	Transaction ID	Type	DNS Query	DNS Ar
04:22	0xA4A1	0x0001 (A)	optimizationguide-pa.googleapis.com	142.25
04:22	0xA4A1	0x0001 (A)	optimizationguide-pa.googleapis.com	142.25
04:22	0xA4A1	0x0001 (A)	optimizationguide-pa.googleapis.com	142.25
04:22	0xA4A1	0x0001 (A)	optimizationguide-pa.googleapis.com	142.25
04:22	0xA4A1	0x0001 (A)	optimizationguide-pa.googleapis.com	172.21
04:22	0xA4A1	0x0001 (A)	optimizationguide-pa.googleapis.com	142.25
04:22	0xA4A1	0x0001 (A)	optimizationguide-pa.googleapis.com	172.21
04:22	0xA4A1	0x0001 (A)	optimizationguide-pa.googleapis.com	172.21
04:22	0xA4A1	0x0001 (A)	optimizationguide-pa.googleapis.com	216.58.
01:25	0x55F3	0x0001 (A)	toolbar3.diigo.com	54.191.
01:25	0x55F3	0x0001 (A)	toolbar3.diigo.com	54.191.
00:13	0x7741	0x0005 (CNAME)	lpulive.lpu.in	app.fug
00:13	0x7741	0x0001 (A)	app.fugu.chat	3.6.18.
00:13	0xFE98	0x0005 (CNAME)	lpulive.lpu.in	app.fug
01:25	0x2EF4	0x0001 (A)	s3.fugu.chat	3.6.18.
00:57	0x146A	0x0005 (CNAME)	clients4.google.com	clients.l
03:04	0x146A	0x0001 (A)	clients.l.google.com	172.21
00:57	0x7573	0x0005 (CNAME)	clients4.google.com	clients.l
03:00	0x3F64	0x0005 (CNAME)	devadf-himanshu.eastus.datafactory.azure.net	eu.front

HOST 2: TARGET HOST WILL BE THE TROJAN INFECTED PC FROM PCAP FILE

download the pcap file from malware traffic analysis.net of name where dream comes true. Unzip it using password INFECTED.



MALWARE-TRAFFIC-ANALYSIS.NET

2017-07-22 - TRAFFIC ANALYSIS EXERCISE - WHERE DREAMS ARE MADE

ASSOCIATED FILES:

- Zip archive of the pcap: **2017-07-22-traffic-analysis-exercise.pcap.zip** 16.6 MB (16,553,287 bytes)

All ZIP files on this site are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

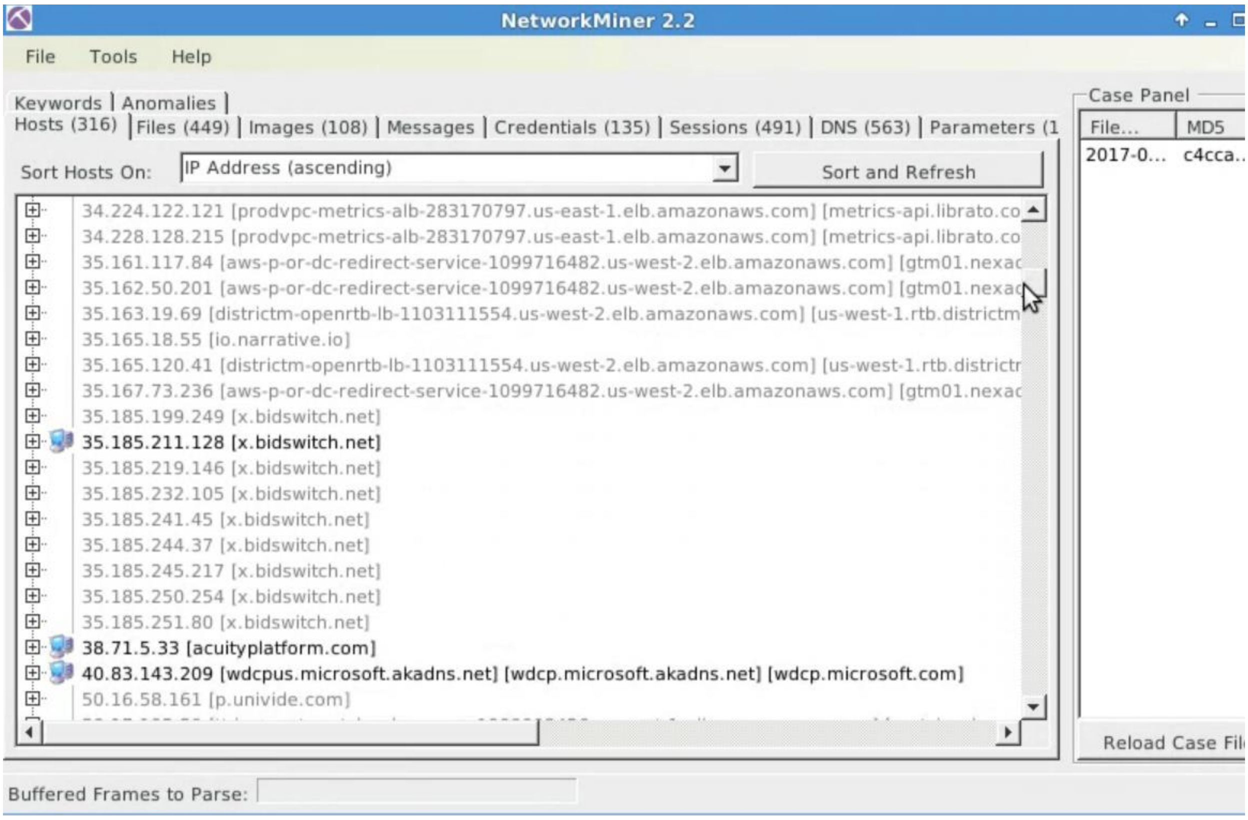
SCENARIO

[start New Age music]

Narrator: Welcome to Malware Traffic Analysis dot Net, where we specialize in providing a home for under-valued malware and suspicious network traffic. Trained specialists work in a stress-free, holistic manner to prepare our samples for a home in the community.

You scratch your head and wonder how you stumbled in here. What do you remember? You took a back alley shortcut on your way to Bloomingdales, but you got lost and stumbled across this rather odd store.

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



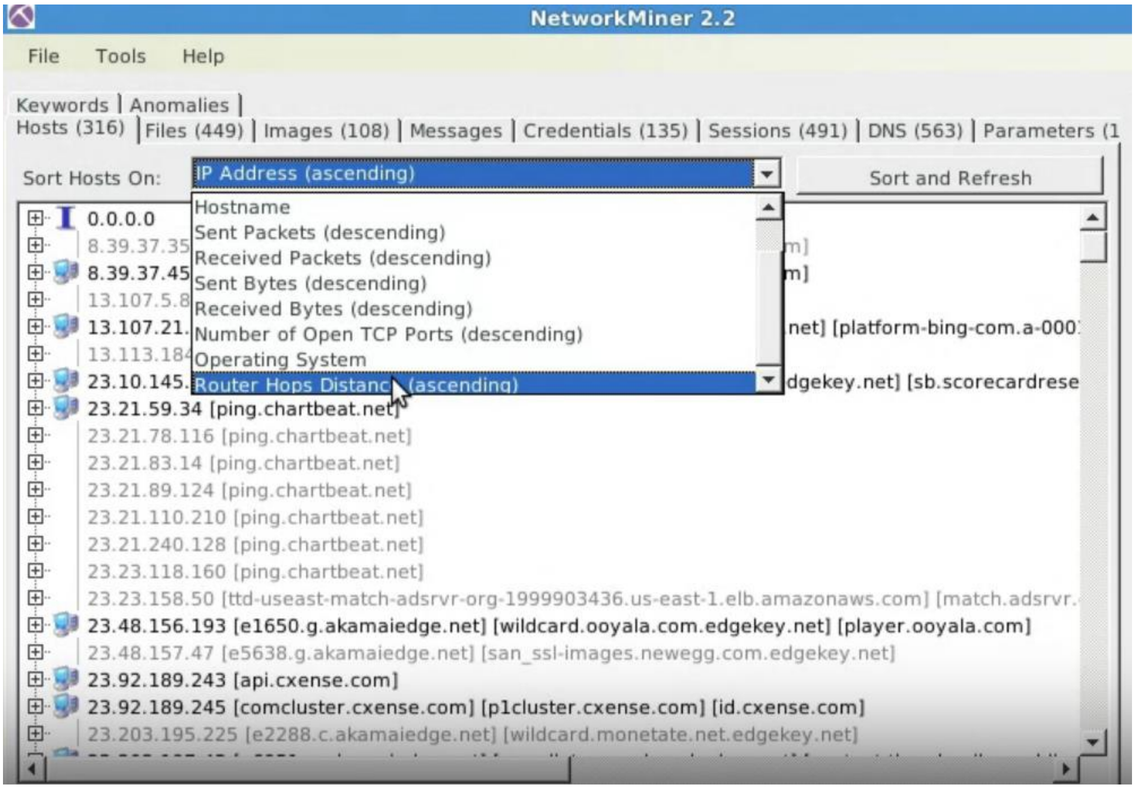
Sort Hosts On: IP Address (ascending)

```
34.224.122.121 [prodvpc-metrics-alb-283170797.us-east-1.elb.amazonaws.com] [metrics-api.librato.co
34.228.128.215 [prodvpc-metrics-alb-283170797.us-east-1.elb.amazonaws.com] [metrics-api.librato.co
35.161.117.84 [aws-p-or-dc-redirect-service-1099716482.us-west-2.elb.amazonaws.com] [gtm01.nexac
35.162.50.201 [aws-p-or-dc-redirect-service-1099716482.us-west-2.elb.amazonaws.com] [gtm01.nexac
35.163.19.69 [districtm-openrtb-lb-1103111554.us-west-2.elb.amazonaws.com] [us-west-1.rtb.districtm
35.165.18.55 [io.narrative.io]
35.165.120.41 [districtm-openrtb-lb-1103111554.us-west-2.elb.amazonaws.com] [us-west-1.rtb.districtr
35.167.73.236 [aws-p-or-dc-redirect-service-1099716482.us-west-2.elb.amazonaws.com] [gtm01.nexac
35.185.199.249 [x.bidswitch.net]
35.185.211.128 [x.bidswitch.net]
35.185.219.146 [x.bidswitch.net]
35.185.232.105 [x.bidswitch.net]
35.185.241.45 [x.bidswitch.net]
35.185.244.37 [x.bidswitch.net]
35.185.245.217 [x.bidswitch.net]
35.185.250.254 [x.bidswitch.net]
35.185.251.80 [x.bidswitch.net]
38.71.5.33 [acuityplatform.com]
40.83.143.209 [wdcpus.microsoft.akadns.net] [wdcp.microsoft.akadns.net] [wdcp.microsoft.com]
50.16.58.161 [p.univide.com]
```

File...	MD5
2017-0...	c4cca..

Buffered Frames to Parse:

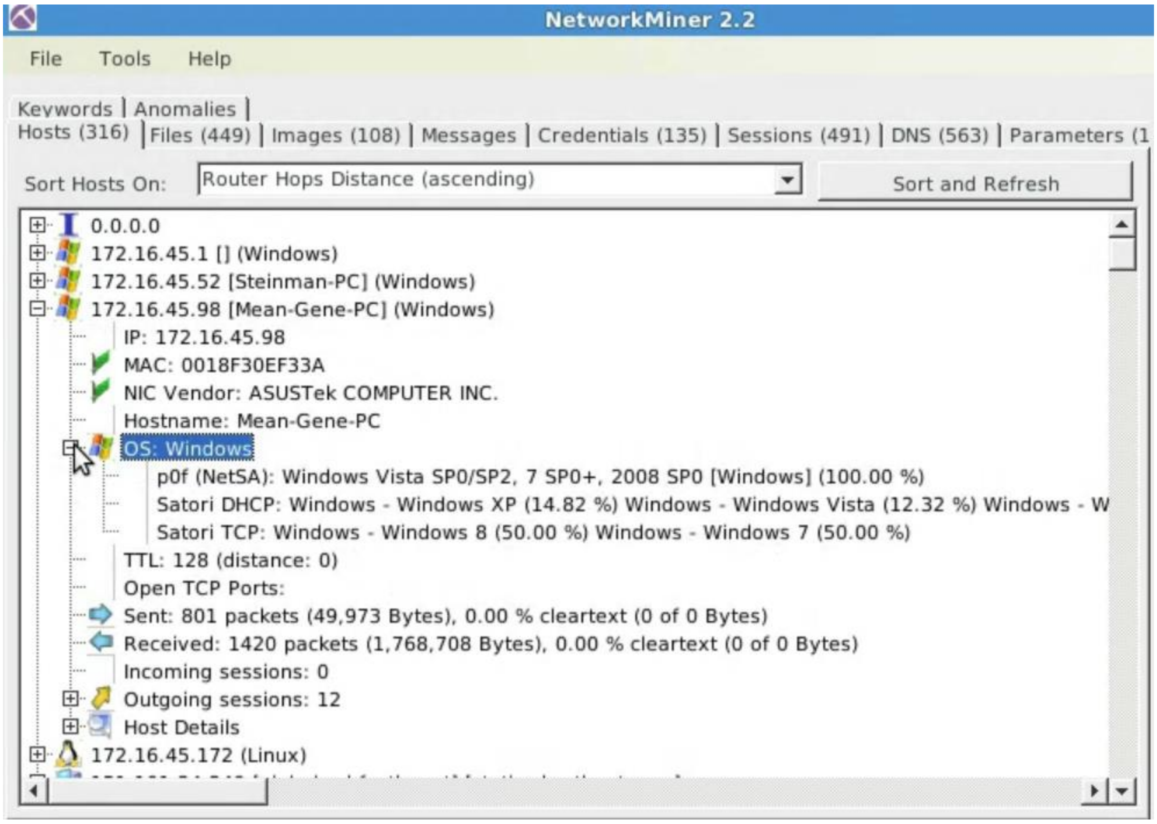
Because infected and target host will be from RFC1918 private network range, we can sort the ip address in router hops distance rather than in ascending order, so that we get host which are closest to sniffing point because there are machines which are several hops away i.e., they on same subnet on packet capturing device.


NetworkMiner 2.2
File
Tools
Help
Keywords | Anomalies |
Hosts (316) | Files (449) | Images (108) | Messages | Credentials (135) | Sessions (491) | DNS (563) | Parameters (1
Sort and Refresh
Hostname
Sent Packets (descending)
Received Packets (descending)
Sent Bytes (descending)
Received Bytes (descending)
Number of Open TCP Ports (descending)
Operating System
Router Hops Distance (ascending)

Sort Hosts On: IP Address (ascending)

```
0.0.0.0
8.39.37.35                                  m]
8.39.37.45                                  m]
13.107.5.8
13.107.21.                                  net] [platform-bing-com.a-000
13.113.184
23.10.145.                                  dgekey.net] [sb.scorecardrese
23.21.59.34 [ping.chartbeat.net]
23.21.78.116 [ping.chartbeat.net]
23.21.83.14 [ping.chartbeat.net]
23.21.89.124 [ping.chartbeat.net]
23.21.110.210 [ping.chartbeat.net]
23.21.240.128 [ping.chartbeat.net]
23.23.118.160 [ping.chartbeat.net]
23.23.158.50 [ttd-useast-match-adsrvr-org-1999903436.us-east-1.elb.amazonaws.com] [match.adsrvr.
23.48.156.193 [e1650.g.akamaiedge.net] [wildcard.ooyala.com.edgekey.net] [player.ooyala.com]
23.48.157.47 [e5638.g.akamaiedge.net] [san_ssl-images.newegg.com.edgekey.net]
23.92.189.243 [api.cxense.com]
23.92.189.245 [comcluster.cxense.com] [p1cluster.cxense.com] [id.cxense.com]
23.203.195.225 [e2288.c.akamaiedge.net] [wildcard.monetate.net.edgekey.net]
```

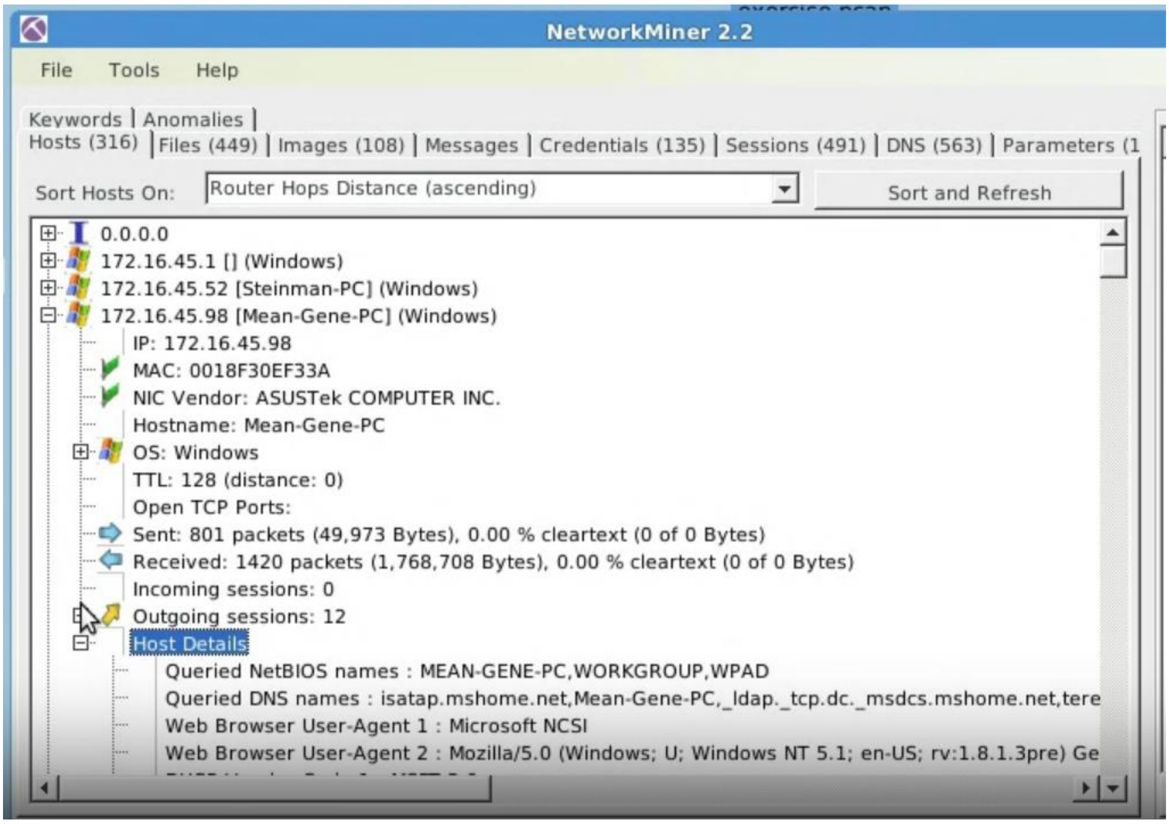
Check the first 5 IP address. Fist ip will be from the client that request the ip address because they have sent the first tpc request from ip address before they assign ip address. Second on is the default gateway address to the other machine in same subnet


NetworkMiner 2.2
File
Tools
Help
Keywords | Anomalies |
Hosts (316) | Files (449) | Images (108) | Messages | Credentials (135) | Sessions (491) | DNS (563) | Parameters (1
Sort and Refresh

Sort Hosts On: Router Hops Distance (ascending)

```
0.0.0.0
172.16.45.1 [] (Windows)
172.16.45.52 [Steinman-PC] (Windows)
172.16.45.98 [Mean-Gene-PC] (Windows)
    IP: 172.16.45.98
    MAC: 0018F30EF33A
    NIC Vendor: ASUSTek COMPUTER INC.
    Hostname: Mean-Gene-PC
    OS: Windows
        p0f (NetSA): Windows Vista SP0/SP2, 7 SP0+, 2008 SP0 [Windows] (100.00 %)
        Satori DHCP: Windows - Windows XP (14.82 %) Windows - Windows Vista (12.32 %) Windows - W
        Satori TCP: Windows - Windows 8 (50.00 %) Windows - Windows 7 (50.00 %)
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 801 packets (49,973 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 1420 packets (1,768,708 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 12
    Host Details
172.16.45.172 (Linux)
```

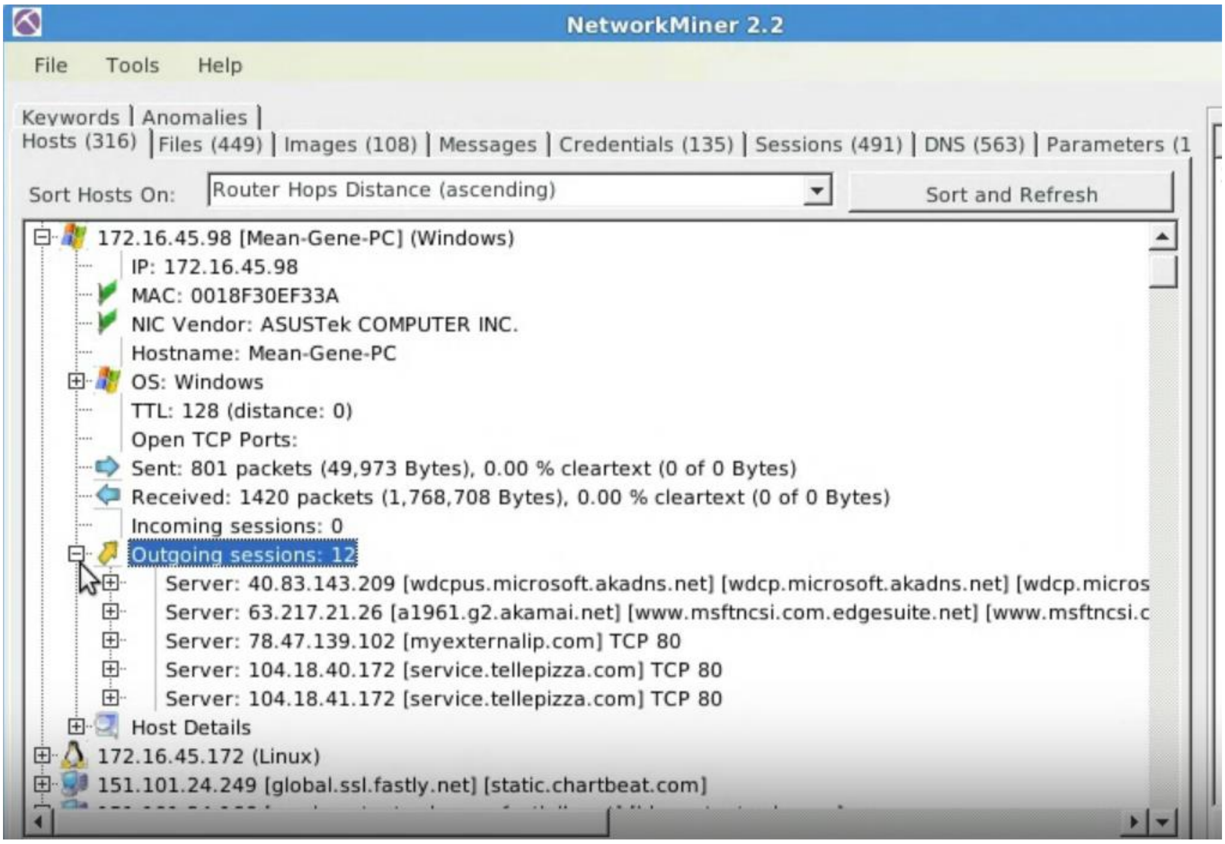
Third machine is the window machine and fourth will be also a window machine as we Expand the OS fingerprint. Seeing host detail tab, we will see it is WINDOW XP or window 5.1.


NetworkMiner 2.2
File Tools Help
Keywords | Anomalies |
Hosts (316) | Files (449) | Images (108) | Messages | Credentials (135) | Sessions (491) | DNS (563) | Parameters (1
Sort and Refresh

Sort Hosts On: Router Hops Distance (ascending)

```
0.0.0.0
172.16.45.1 [] (Windows)
172.16.45.52 [Steinman-PC] (Windows)
172.16.45.98 [Mean-Gene-PC] (Windows)
    IP: 172.16.45.98
    MAC: 0018F30EF33A
    NIC Vendor: ASUSTek COMPUTER INC.
    Hostname: Mean-Gene-PC
    OS: Windows
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 801 packets (49,973 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 1420 packets (1,768,708 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 12
    Host Details
        Queried NetBIOS names : MEAN-GENE-PC,WORKGROUP,WPAD
        Queried DNS names : isatap.mshome.net,Mean-Gene-PC,_ldap._tcp.dc._msdcs.mshome.net,tere
        Web Browser User-Agent 1 : Microsoft NCSI
        Web Browser User-Agent 2 : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.3pre) Ge
```

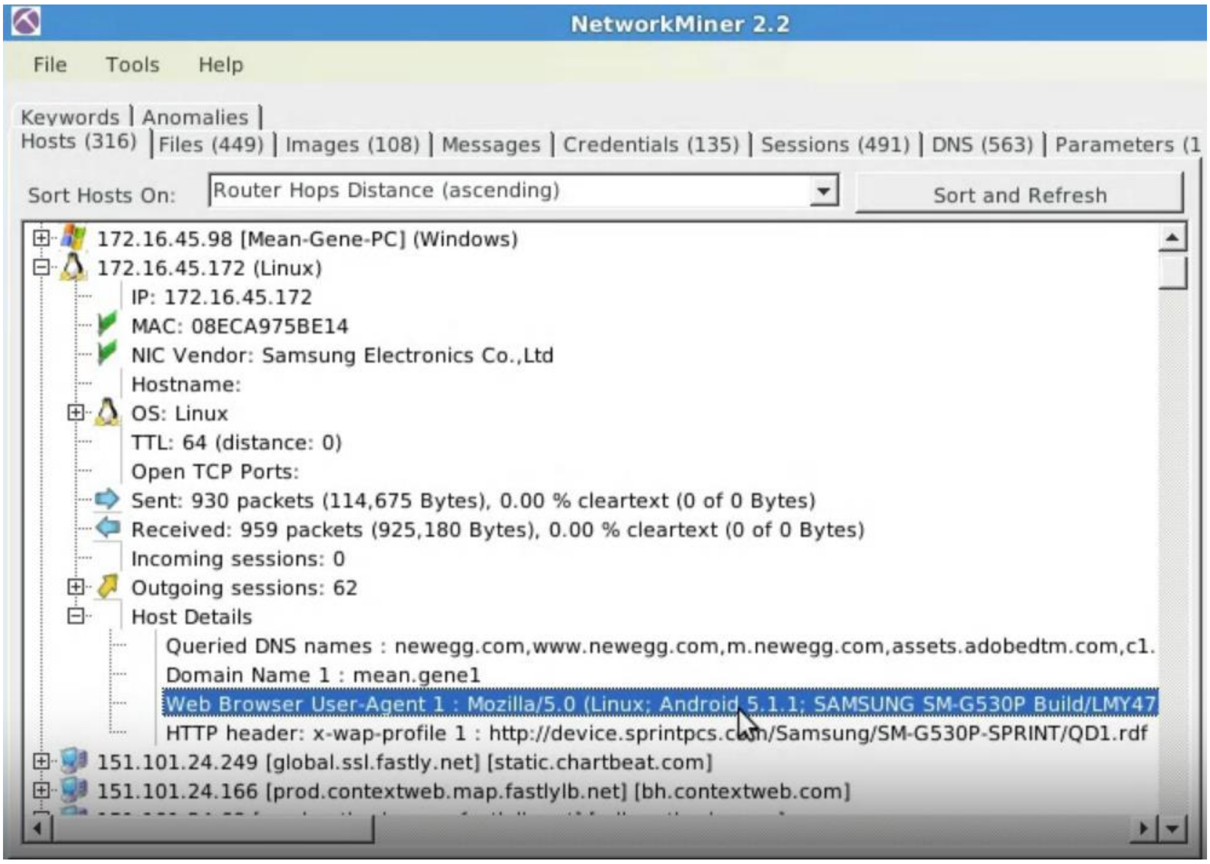
Note that this ip address also communicated to relatively less no of ip address in outgoing session tab.


NetworkMiner 2.2
File Tools Help
Keywords | Anomalies |
Hosts (316) | Files (449) | Images (108) | Messages | Credentials (135) | Sessions (491) | DNS (563) | Parameters (1
Sort and Refresh

Sort Hosts On: Router Hops Distance (ascending)

```
172.16.45.98 [Mean-Gene-PC] (Windows)
    IP: 172.16.45.98
    MAC: 0018F30EF33A
    NIC Vendor: ASUSTek COMPUTER INC.
    Hostname: Mean-Gene-PC
    OS: Windows
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 801 packets (49,973 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 1420 packets (1,768,708 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 12
        Server: 40.83.143.209 [wdcpus.microsoft.akadns.net] [wdcp.microsoft.akadns.net] [wdcp.micros
        Server: 63.217.21.26 [a1961.g2.akamai.net] [www.msftncsi.com.edgesuite.net] [www.msftncsi.c
        Server: 78.47.139.102 [myexternalip.com] TCP 80
        Server: 104.18.40.172 [service.tellepizza.com] TCP 80
        Server: 104.18.41.172 [service.tellepizza.com] TCP 80
    Host Details
172.16.45.172 (Linux)
151.101.24.249 [global.ssl.fastly.net] [static.chartbeat.com]
```

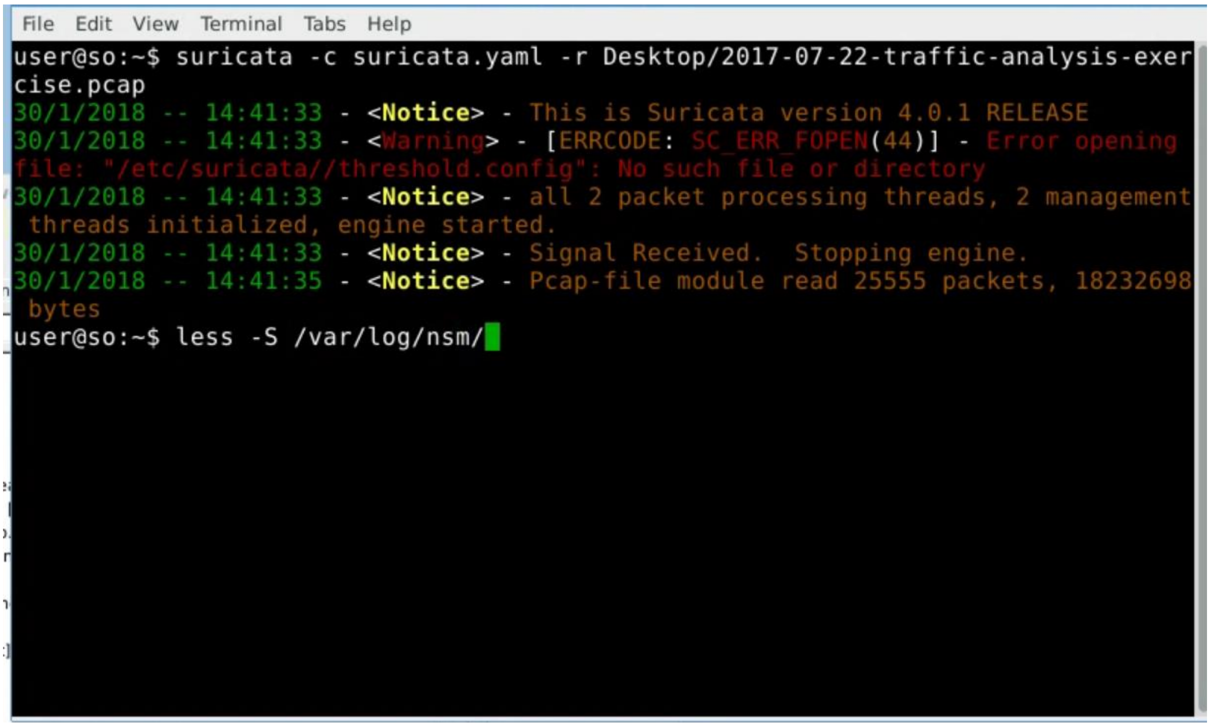
The next machine is the Linux machine based on OS fingerprint with NIC vendor is Samsung with host detail we can conclude it is Samsung galaxy phone.


NetworkMiner 2.2
File Tools Help
Keywords | Anomalies |
Hosts (316) | Files (449) | Images (108) | Messages | Credentials (135) | Sessions (491) | DNS (563) | Parameters (1
Sort and Refresh

Sort Hosts On: Router Hops Distance (ascending)

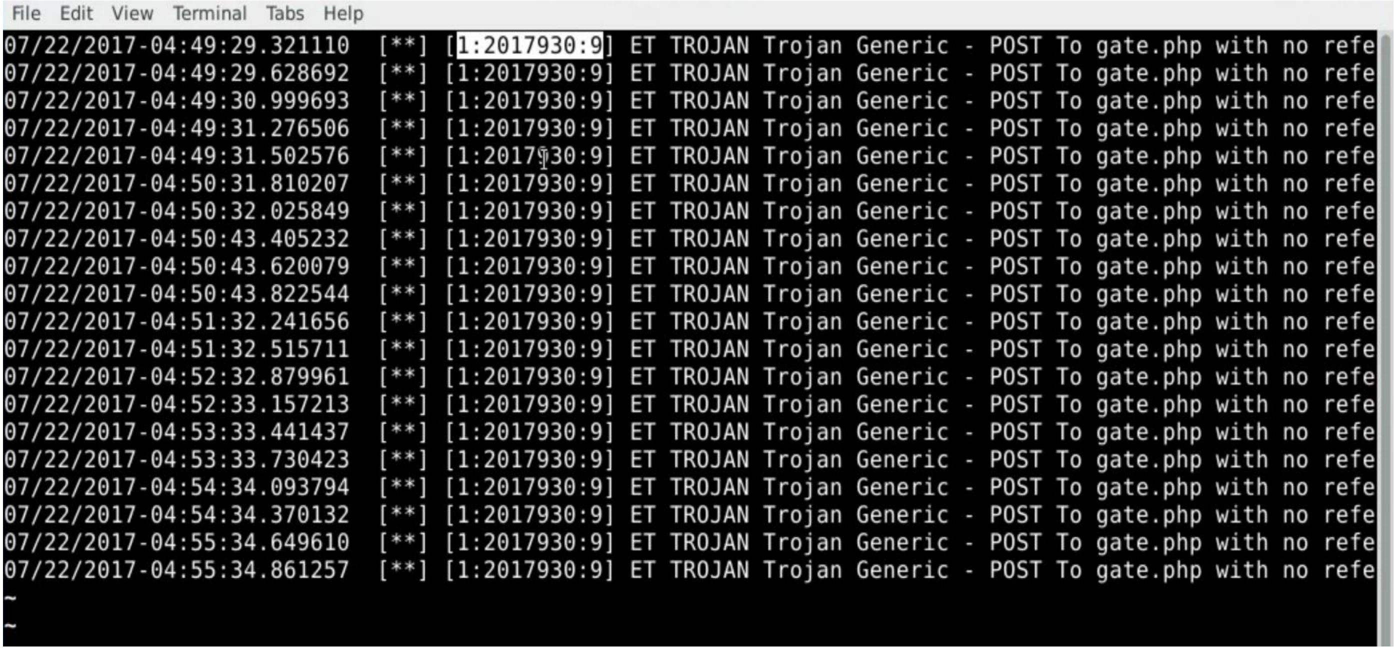
```
172.16.45.98 [Mean-Gene-PC] (Windows)
172.16.45.172 (Linux)
    IP: 172.16.45.172
    MAC: 08ECA975BE14
    NIC Vendor: Samsung Electronics Co.,Ltd
    Hostname:
    OS: Linux
    TTL: 64 (distance: 0)
    Open TCP Ports:
    Sent: 930 packets (114,675 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 959 packets (925,180 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 62
    Host Details
        Queried DNS names : newegg.com,www.newegg.com,m.newegg.com,assets.adobedtm.com,c1.
        Domain Name 1 : mean.gene1
        Web Browser User-Agent 1 : Mozilla/5.0 (Linux; Android 5.1.1; SAMSUNG SM-G530P Build/LMY47
        HTTP header: x-wap-profile 1 : http://device.sprintpcs.com/Samsung/SM-G530P-SPRINT/QD1.rdf
151.101.24.249 [global.ssl.fastly.net] [static.chartbeat.com]
151.101.24.166 [prod.contextweb.map.fastlylb.net] [bh.contextweb.com]
```

Install the SURFICATA tool and type the following command to search through the PCAP file to get any ideal alerts



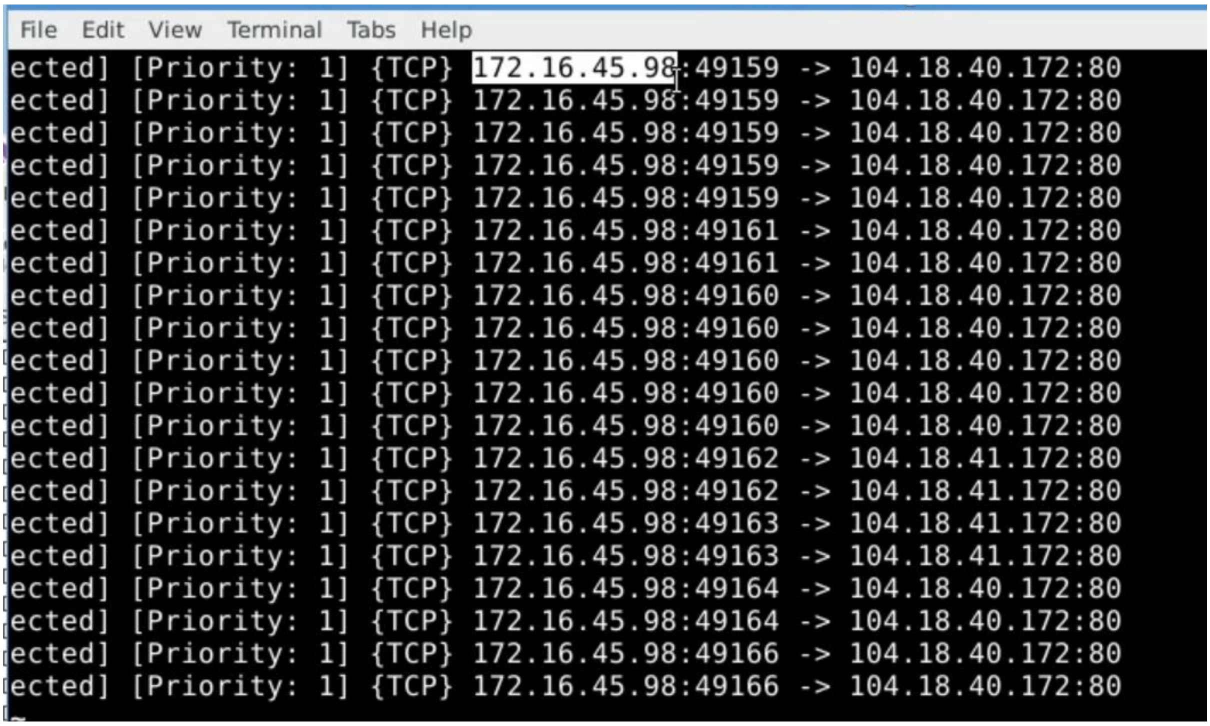
```
user@so:~$ suricata -c suricata.yaml -r Desktop/2017-07-22-traffic-analysis-exer
cise.pcap
30/1/2018 -- 14:41:33 - <Notice> - This is Suricata version 4.0.1 RELEASE
30/1/2018 -- 14:41:33 - <Warning> - [ERRCODE: SC_ERR_FOPEN(44)] - Error opening
file: "/etc/suricata//threshold.config": No such file or directory
30/1/2018 -- 14:41:33 - <Notice> - all 2 packet processing threads, 2 management
 threads initialized, engine started.
30/1/2018 -- 14:41:33 - <Notice> - Signal Received.  Stopping engine.
30/1/2018 -- 14:41:35 - <Notice> - Pcap-file module read 25555 packets, 18232698
 bytes
user@so:~$ less -S /var/log/nsm/
```

We can see multiple alerts from same signature triggering all the time i.e., 1:2017930:9 and altering the detection of generic trojan.



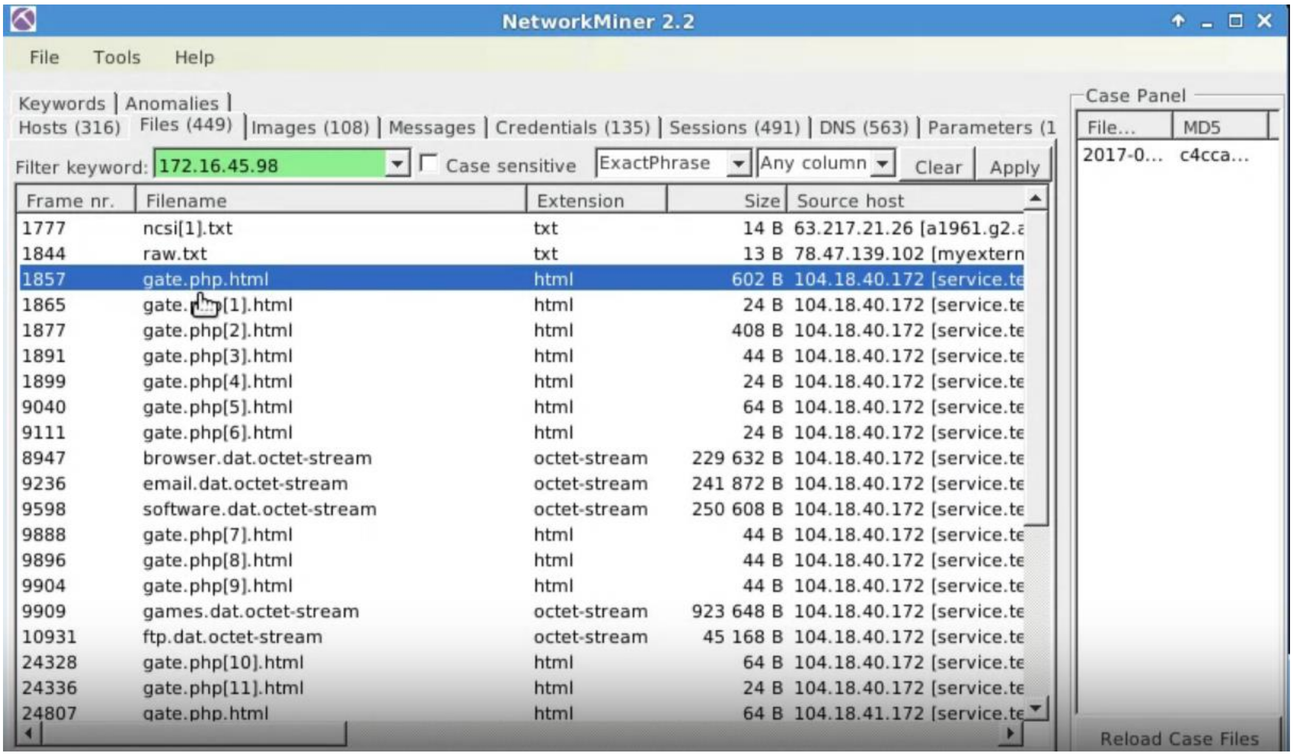
```
07/22/2017-04:49:29.321110  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:49:29.628692  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:49:30.999693  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:49:31.276506  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:49:31.502576  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:50:31.810207  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:50:32.025849  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:50:43.405232  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:50:43.620079  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:50:43.822544  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:51:32.241656  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:51:32.515711  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:52:32.879961  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:52:33.157213  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:53:33.441437  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:53:33.730423  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:54:34.093794  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:54:34.370132  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:55:34.649610  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
07/22/2017-04:55:34.861257  [**] [1:2017930:9] ET TROJAN Trojan Generic - POST To gate.php with no refe
~
~
```

The ip address of machine where trojan is detected by SURFICATA tool is 172.16.45.98 i.e., 4th window target machine. SURFICATA alert is not specific it displays the probable machine to be infected. Thus, helps in further analysis on that host.



```
ected] [Priority: 1] {TCP} 172.16.45.98:49159 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49159 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49159 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49159 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49159 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49161 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49161 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49160 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49160 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49160 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49160 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49160 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49162 -> 104.18.41.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49162 -> 104.18.41.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49163 -> 104.18.41.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49163 -> 104.18.41.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49164 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49164 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49166 -> 104.18.40.172:80
ected] [Priority: 1] {TCP} 172.16.45.98:49166 -> 104.18.40.172:80
~
```

open file tab to see all the file uploaded and downloaded in this network, to see files/traffic from specific network search the file in search bar based on its ip. First file traffic for windows checking its network connectivity, second one is seen as external ip txt of this sandbox usually initiated by malware.

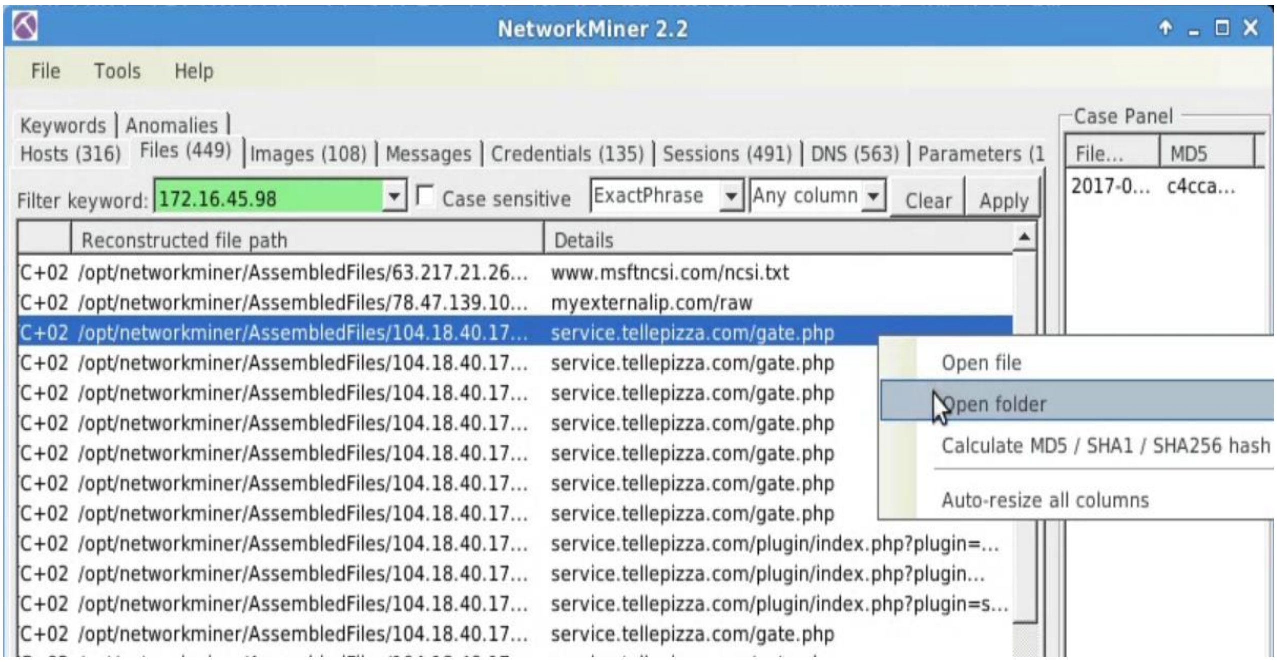


Filter keyword: 172.16.45.98 □ Case sensitive ExactPhrase Any column

Frame nr.	Filename	Extension	Size	Source host
1777	ncsi[1].txt	txt	14 B	63.217.21.26 [a1961.g2.a
1844	raw.txt	txt	13 B	78.47.139.102 [myextern
1857	gate.php.html	html	602 B	104.18.40.172 [service.te
1865	gate.php[1].html	html	24 B	104.18.40.172 [service.te
1877	gate.php[2].html	html	408 B	104.18.40.172 [service.te
1891	gate.php[3].html	html	44 B	104.18.40.172 [service.te
1899	gate.php[4].html	html	24 B	104.18.40.172 [service.te
9040	gate.php[5].html	html	64 B	104.18.40.172 [service.te
9111	gate.php[6].html	html	24 B	104.18.40.172 [service.te
8947	browser.dat.octet-stream	octet-stream	229 632 B	104.18.40.172 [service.te
9236	email.dat.octet-stream	octet-stream	241 872 B	104.18.40.172 [service.te
9598	software.dat.octet-stream	octet-stream	250 608 B	104.18.40.172 [service.te
9888	gate.php[7].html	html	44 B	104.18.40.172 [service.te
9896	gate.php[8].html	html	44 B	104.18.40.172 [service.te
9904	gate.php[9].html	html	44 B	104.18.40.172 [service.te
9909	games.dat.octet-stream	octet-stream	923 648 B	104.18.40.172 [service.te
10931	ftp.dat.octet-stream	octet-stream	45 168 B	104.18.40.172 [service.te
24328	gate.php[10].html	html	64 B	104.18.40.172 [service.te
24336	gate.php[11].html	html	24 B	104.18.40.172 [service.te
24807	gate.php.html	html	64 B	104.18.41.172 [service.te

File...	MD5
2017-0...	c4cca...

Open the folder for third request service.teelepizza.com and check all the folders downloaded

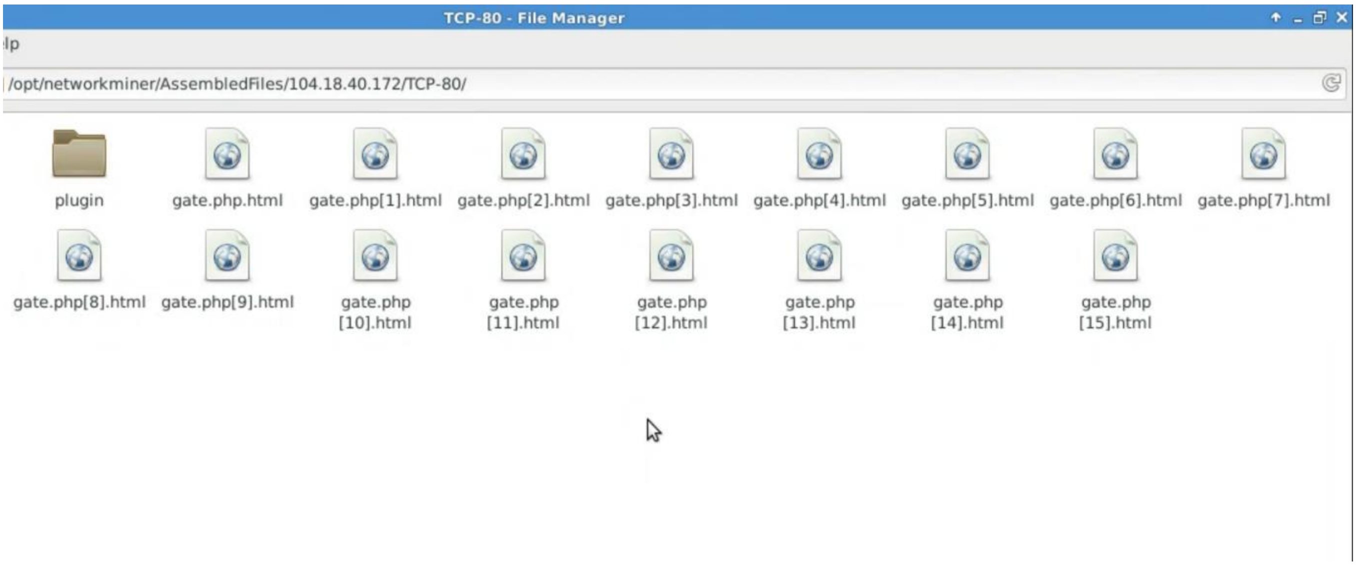


Filter keyword: 172.16.45.98 □ Case sensitive ExactPhrase Any column

	Reconstructed file path	Details
C+02	/opt/networkminer/AssembledFiles/63.217.21.26...	www.msftncsi.com/ncsi.txt
C+02	/opt/networkminer/AssembledFiles/78.47.139.10...	myexternalip.com/raw
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/gate.php
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/gate.php
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/gate.php
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/gate.php
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/gate.php
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/gate.php
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/gate.php
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/plugin/index.php?plugin=...
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/plugin/index.php?plugin...
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/plugin/index.php?plugin=s...
C+02	/opt/networkminer/AssembledFiles/104.18.40.17...	service.tellepizza.com/gate.php

File...	MD5
2017-0...	c4cca...

These are the file downloaded by this particular ip on port 80. We further analysis the file and its content to check for trojan. Like file gate.php.html have a certificate number which can be parse with OPENSSL. If search the certificate we will find that the certificate no will match in the zyklon http trojan with information of http user agent used by trojan which will match with the user agent of our host target machine i.e., BON ECHO (Firefox 2) confirming its infection with zyklon trojan



/opt/networkminer/AssembledFiles/104.18.40.172/TCP-80/

plugin
gate.php.html
gate.php[1].html
gate.php[2].html
gate.php[3].html
gate.php[4].html
gate.php[5].html
gate.php[6].html
gate.php[7].html
gate.php[8].html
gate.php[9].html
gate.php[10].html
gate.php[11].html
gate.php[12].html
gate.php[13].html
gate.php[14].html
gate.php[15].html

4: REFERENCE

- 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

LOVELY PROFESSIONAL UNIVERSITY

THANK U