Network Forensic Report

PCAP Network Packet Capture Analysis

Last compiled by T W V Fernando and MDP Induwara

on the date 2/18/2025

This report provides the details of the forensic analysis performed on the network capture file "nforensics.pcap" in Brisbane, Queensland Australia

Table of Contents

1. Executive Summary

This report contains the forensic analysis conducted for the sole purpose of determining whether a student from Chemistry 109 in the XYZ school was responsible for sending harassing emails, one of which was sent with a web-based service called willselfdestruct.com and the other the primary threat focused on Lily Tuckridge, the teacher of said class and department. The investigation primarily focuses on the network traffic captured using a network sniffer placed on the ethernet port at the school, from the IP address of the dormitory 140.247.62.34, which was linked to the harassing emails. For detailed review and investigation, the following pcap file called XYZ.pcap was reviewed using software such as Wireshark and Network Miner.

1. The two routers (00:1d:d9:2e:4f:60, 00:1d:d9:2e:4f:61) were monitored directly by the network sniffer, and all information and packets that were monitored were with the help of that to find the harassment activities.

2. DNS response using frame contains "willselfdestruct" && dns gives us conclusive information about all the searches that were made to that website, within that time.
3. The suspects device runs on a MacOS with (User-Agent: Mozilla/5.0 (Macintosh; PPC Mac OS X)), indicating the use of an apple device for these activities.
4. The email ID jcoachj@gmail.com and MAC address 00:17:f2:e2:c0:ce strongly implicate "jcoachj" as the primary suspect. This was done by filtering based on the public IP to find connection to the private IP, then coming across the MAC address they provide which was the same throughout the packets ensuring the connection to the private IP, and with the TCP stream confirming the device used.
5. We made use of Network Miner and Wireshark to analyze the network traffic, to get the information sufficient to validate our findings.
6. Traffic to sendanonymousmail.net Frame number 80614 and WillSelfDestruct.com Frame number 83601 originated from 192.168.15.4, confirming jcoachj's device as the source.
7. Filtering on keywords such as teacher and Gmail revealed Frame number 74920 a google query containing "can I go to jail for harassing my teacher", and Frame number 79715 a cleartext cookie containing the cookie pair of jcoachj.
8. The DNS requests for harassment domains were resolved to the XYZ campus network, which means any alibi of it being off-campus activity is completely improbable.
9. Another ID was found connecting to the device jcoachj was using, under the alias amy789smith indicating device sharing or an attempt to get the device from the original owner, both this individual and later mentioned elishevet have shown no involved in this harassment attempt, but certain aspects have been monitored with the idea of further proofing the involved of jcoachj.
10. Consider that 73000~ packets out of the 94000~ were strictly communication between MacOS device used by jcoachj and the dorm router.
11. All evidence provided complies with forensics standards for the chain of custody.

2. Introduction

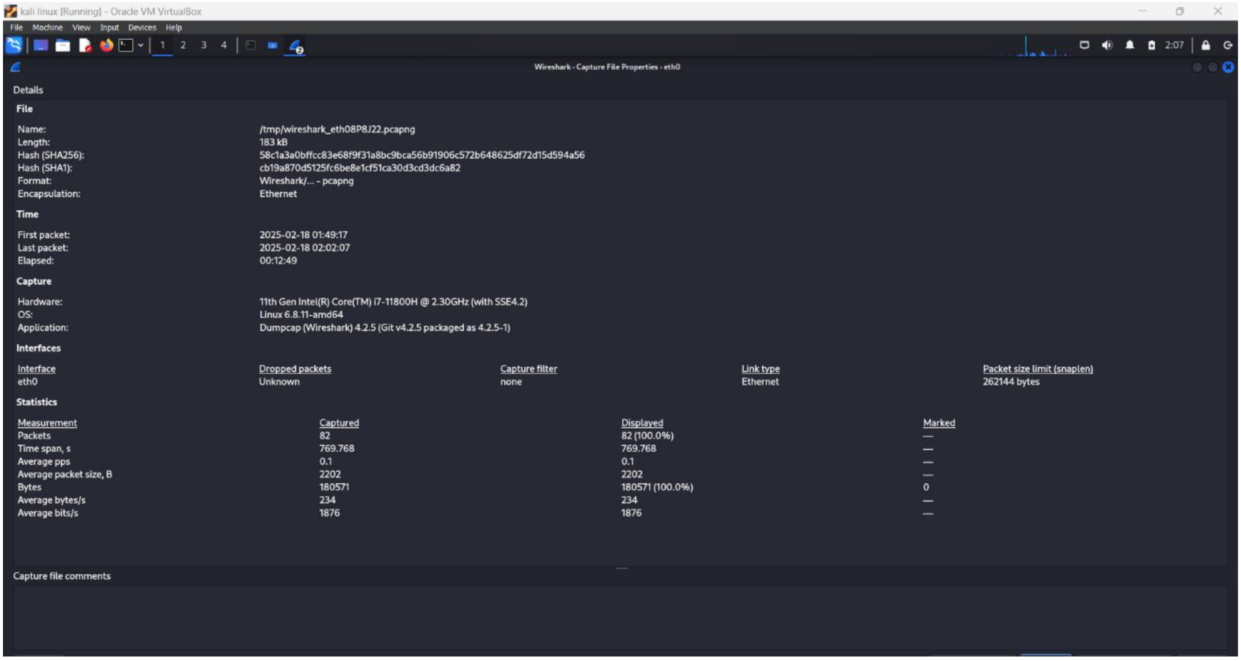
2.1 Network Capture File details

The extracted PCAP network capture file XYZ.pcap has the forensic parameters as given below. The evidence for these details is provided in Figure 1 extracted from Wireshark ver 4.2.5 and Network Miner 2.9.0:

Capture length:	187,392 bytes
Format:	/tmp/Wireshark_eth08p8J22.pcapng
Packet size limit:	65535 bytes
First packet:	18-FEB-2025 01:49:17 HRS
Last packet:	18-FRB-2025 02:02:07 HRS
Elapsed time:	12 minutes, 49 seconds
Total packets:	82
Average packets/sec	0.1 packets/sec
Average packet size	2202bytes
Average bytes/sec	234 bytes/sec

Computed HASHes – XYZ.pcap

MD5:	9981827f119687f3ff815e39f5458ec8
SHA1:	cb198a70d5125fcb6be8efc15ca30d3cd3dc6a82



kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark · Capture File Properties · eth0

Details

File

Name:	/tmp/wireshark_eth08P8J22.pcapng
Length:	183 kB
Hash (SHA256):	58c1a3a0bffcc83e68f9f31a8bc9bca56b91906c572b648625df72d15d594a56
Hash (SHA1):	cb19a870d5125fc6be8e1cf51ca30d3cd3dc6a82
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2025-02-18 01:49:17
Last packet:	2025-02-18 02:02:07
Elapsed:	00:12:49

Capture

Hardware:	11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz (with SSE4.2)
OS:	Linux 6.8.11-amd64
Application:	Dumpcap (Wireshark) 4.2.5 (Git v4.2.5 packaged as 4.2.5-1)

Interfaces

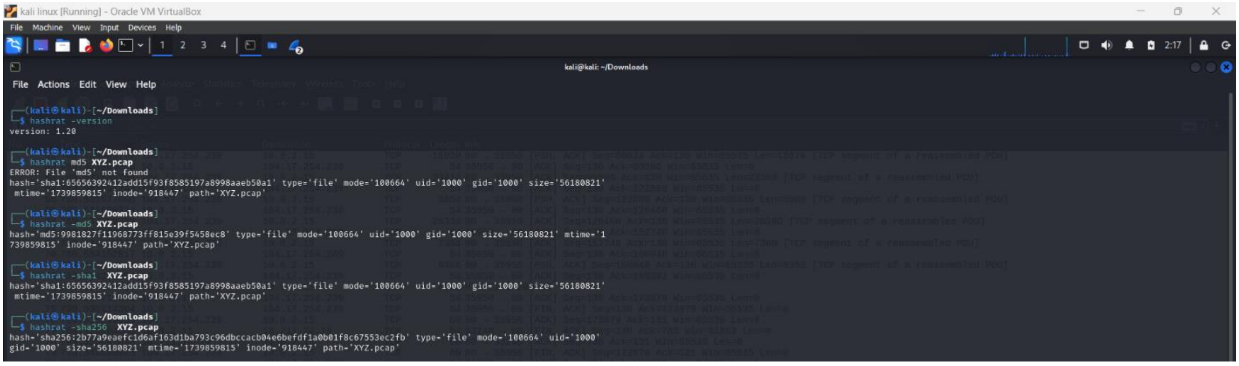
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
eth0	Unknown	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	82	82 (100.0%)	—
Time span, s	769.768	769.768	—
Average pps	0.1	0.1	—
Average packet size, B	2202	2202	—
Bytes	180571	180571 (100.0%)	0
Average bytes/s	234	234	—
Average bits/s	1876	1876	—

Capture file comments

Figure 1. Packet capture summary from Wireshark ver0.99.7



kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Downloads]
└─$ hashrat -version
version: 1.20

┌──(kali㉿kali)-[~/Downloads]
└─$ hashrat md5 XYZ.pcap
ERROR: File 'md5' not found
hash='sha1:65656392412add15f93f8585197a8998aaeb50a1' type='file' mode='100664' uid='1000' gid='1000' size='56180821'
 mtime='1739859815' inode='918447' path='XYZ.pcap'

┌──(kali㉿kali)-[~/Downloads]
└─$ hashrat -md5 XYZ.pcap
hash='md5:9981827f11968773ff815e39f5458ec8' type='file' mode='100664' uid='1000' gid='1000' size='56180821' mtime='1
739859815' inode='918447' path='XYZ.pcap'

┌──(kali㉿kali)-[~/Downloads]
└─$ hashrat -sha1  XYZ.pcap
hash='sha1:65656392412add15f93f8585197a8998aaeb50a1' type='file' mode='100664' uid='1000' gid='1000' size='56180821'
 mtime='1739859815' inode='918447' path='XYZ.pcap'

┌──(kali㉿kali)-[~/Downloads]
└─$ hashrat -sha256  XYZ.pcap
hash='sha256:2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb' type='file' mode='100664' uid='1000'
gid='1000' size='56180821' mtime='1739859815' inode='918447' path='XYZ.pcap'
```

Figure 2. Verifying the hashes of the pcap file and the archive version using hash rat

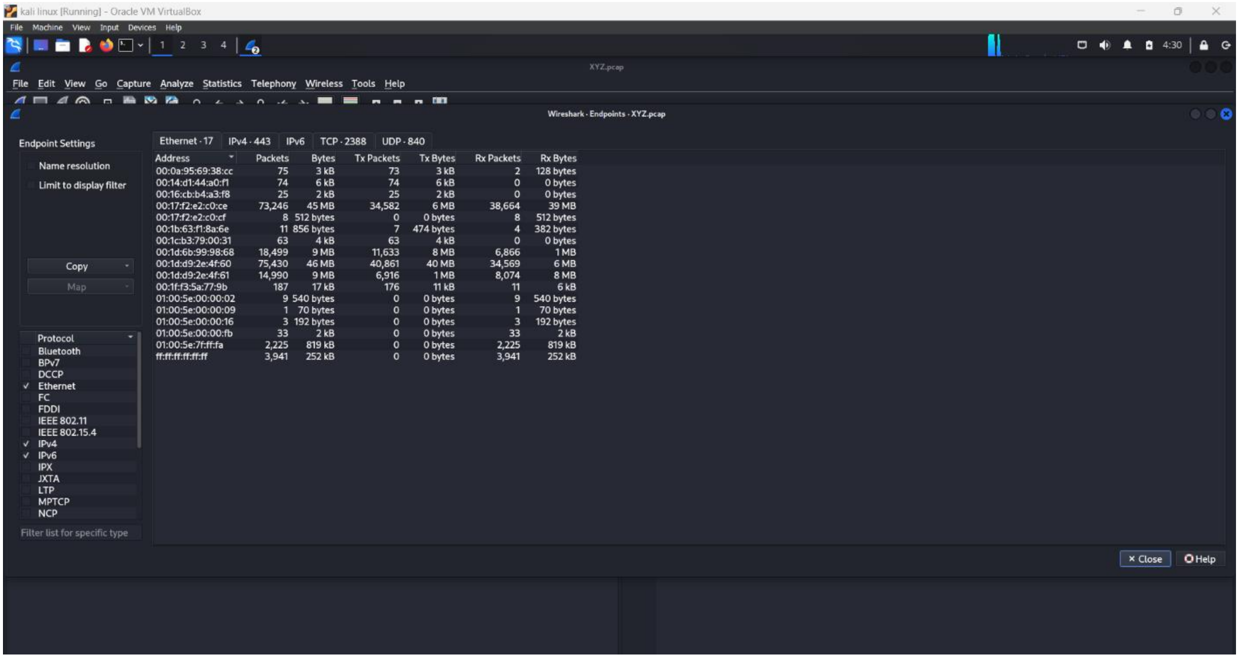
2.2 Network Components Identified

According to the capture summary as provided by Wireshark ver 4.2.5, there are 6 distinct Ethernet components. They were determined using the Ethernet Endpoints listed under Statistics as below:

No	MAC Address	MAC Address with Name Resolution	IP Address	Vendor	Device	OS
1	00:0a:95:69:38:cc	Apple_69:38:cc	192.168.1.5	Apple, Inc.		
	00:14:d1:44:a0:f1	TRENDnet_44:a0:f1	192.168.15.5	TRENDnet, Inc.		
	00:16:cb:b4:a3:f8	Apple_b4:a3:f8	192.168.15.8	Apple, Inc.		
	00:17:f2:e2:c0:ce	Apple_e2:c0:ce	192.168.15.4	Apple, Inc.	Macintosh	Intel Mac OS X 10.5.4
	00:17:f2:e2:c0:cf	Apple_e2:c0:cf	-	Apple, Inc.	-	-
	00:1b:63:f1:8a:6e	Apple_e2:c0:cf	192.168.15.2	Apple, Inc.	-	-
	00:1c:b3:79:00:31	Apple_79:00:31	10.0.1.5	Apple, Inc.	-	-
	00:1d:6b:99:98:68	ARRISGroup_99:98:68 (Commscope_99:98:68)	192.168.1.254	ARRIS Group, Inc.	Router	-

	00:1d:d9:2e:4f:60	HonHaiPrecis_2e:4f:60	192.168.15.1	Hon Hai Precision Ind. Co.,Ltd.	Router	-
	00:1d:d9:2e:4f:61	HonHaiPrecis_2e:4f:61	192.168.1.64	Hon Hai Precision Ind. Co.,Ltd.	Router	-
	00:1f:f3:5a:77:9b	Apple_5a:77:9b	169.254.90.183	Apple, Inc.	-	-
	01:00:5e:00:00:02	IPv4mcast_02	-	-	-	-
	01:00:5e:00:00:09	IPv4mcast_09	-	-	-	-
	01:00:5e:00:00:16	IPv4mcast_16	-	-	-	-
	01:00:5e:00:00:fb	IPv4mcast_fb	-	-	-	-
	01:00:5e:7f:ff:fa	IPv4mcast_7f:ff:fa	-	-	-	-
	ff:ff:ff:ff:ff:ff	Broadcast	-	-	-	-

remaining part of the investigation. The device with a name resolution of Apple b4:a3:f8 and with the MAC address 00:17:f2:e2:c0:ce was found to have the IP address 192.168.15.4 which was our suspicious individual. He accessed 69.80.225.91 and 69.25.94.22 (Destination IP Addresses) from his device through the router with the name resolution as Broadcast with an IP address of 140.247.62.34 and MAC address of 00:1d:d9:2e:4f:60. This could potentially imply that the device was actively communicating with external servers, indicating possible unauthorized access or data exfiltration. Based on the evidence of connections established between 192.168.15.4 and the destination IP addresses 69.80.225.91 and 69.25.94.22, this report concludes that the device was engaged in outbound network activity, which may suggest suspicious or unauthorized behavior.



Wireshark · Endpoints · XYZ.pcap

Endpoint Settings

☐ Name resolution

☐ Limit to display filter

Protocol: Bluetooth, BPv7, DCCP, ✓ Ethernet, FC, FDDI, IEEE 802.11, IEEE 802.15.4, ✓ IPv4, ✓ IPv6, IPX, JXTA, LTP, MPTCP, NCP

Ethernet · 17 | IPv4 · 443 | IPv6 | TCP · 2388 | UDP · 840

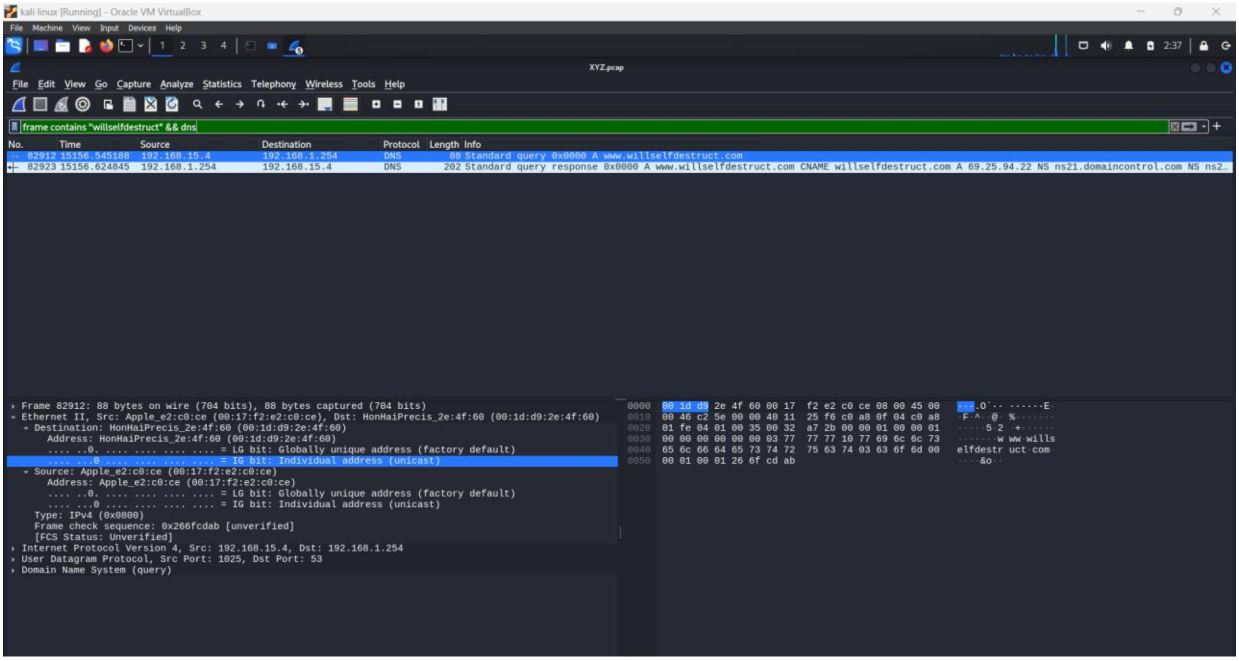
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:0a:95:69:38:cc	75	3 kB	73	3 kB	2	128 bytes
00:14:d1:44:a0:f1	74	6 kB	74	6 kB	0	0 bytes
00:16:cb:b4:a3:f8	25	2 kB	25	2 kB	0	0 bytes
00:17:f2:e2:c0:ce	73,246	45 MB	34,582	6 MB	38,664	39 MB
00:17:f2:e2:c0:cf	8	512 bytes	0	0 bytes	8	512 bytes
00:1b:63:f1:8a:6e	11	856 bytes	7	474 bytes	4	382 bytes
00:1c:b3:79:00:31	63	4 kB	63	4 kB	0	0 bytes
00:1d:6b:99:98:68	18,499	9 MB	11,633	8 MB	6,866	1 MB
00:1d:d9:2e:4f:60	75,430	46 MB	40,861	40 MB	34,569	6 MB
00:1d:d9:2e:4f:61	14,990	9 MB	6,916	1 MB	8,074	8 MB
00:1f:f3:5a:77:9b	187	17 kB	176	11 kB	11	6 kB
01:00:5e:00:00:02	9	540 bytes	0	0 bytes	9	540 bytes
01:00:5e:00:00:09	1	70 bytes	0	0 bytes	1	70 bytes
01:00:5e:00:00:16	3	192 bytes	0	0 bytes	3	192 bytes
01:00:5e:00:00:fb	33	2 kB	0	0 bytes	33	2 kB
01:00:5e:7f:ff:fa	2,225	819 kB	0	0 bytes	2,225	819 kB
ff:ff:ff:ff:ff:ff	3,941	252 kB	0	0 bytes	3,941	252 kB

kali linux [Running] - Oracle VM VirtualBox
XYZ.pcap
Copy
Map
Filter list for specific type
× Close
Help

3. Methodology

3.1 Tools Used

The analysis analysed the contents using network forensic tools such as wireshark Version 4.2.5 executing under kali Linux 64 bit on Single CPU with 4GB RAM in Virtual BOX and Wireshark Version 4.2.5 on a separate windows running on windows 11, with 16gb RAM and a 11th Gen Intel(R) Core™ i7-11800H@2.30GHz, with an RTX 3050 Laptop GPU.Findings were later cross verified on another system using Network Miner Version 2.9.0 executing on windows 11platform with 16GB RAM and a 11th Gen Intel(R) Core™ i7-11800H@2.30GHz, with an RTX 3050 Laptop. The analysis revealed the internal IP which were used to access to willselfdestruct.com (192.168.15.4) and the external which send the response to the login request(192.168.1.254) through DNS.



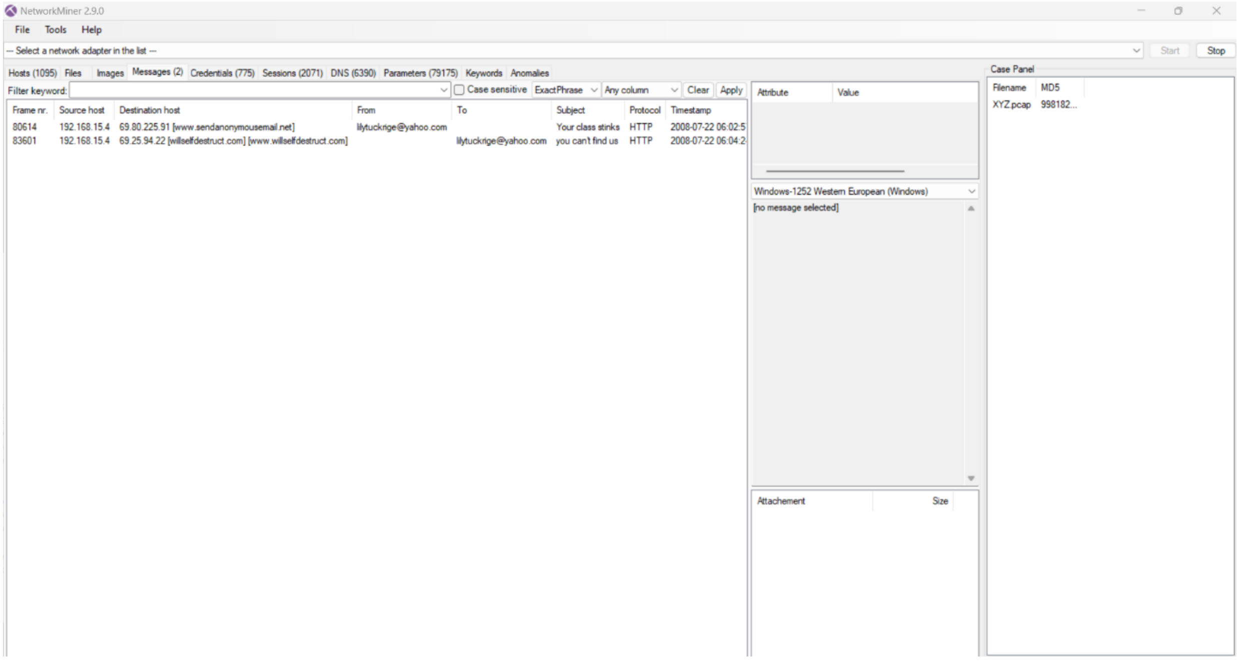
frame contains "willselfdestruct" && dns

```
No.   Time          Source         Destination    Protocol Length Info
82912 15156.545188  192.168.15.4   192.168.1.254  DNS       88 Standard query 0x0000 A www.willselfdestruct.com
82923 15156.624845  192.168.1.254  192.168.15.4   DNS      202 Standard query response 0x0000 A www.willselfdestruct.com CNAME willselfdestruct.com A 69.25.94.22 NS ns21.domaincontrol.com NS ns2…
```

```
› Frame 82912: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
⌄ Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
  ⌄ Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
      Address: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⌄ Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
      Address: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    Frame check sequence: 0x266fcdab [unverified]
    [FCS Status: Unverified]
› Internet Protocol Version 4, Src: 192.168.15.4, Dst: 192.168.1.254
› User Datagram Protocol, Src Port: 1025, Dst Port: 53
› Domain Name System (query)
```

```
0000  00 1d d9 2e 4f 60 00 17  f2 e2 c0 ce 08 00 45 00   ···.O`·· ······E·
0010  00 46 c2 5e 00 00 40 11  25 f6 c0 a8 0f 04 c0 a8   ·F·^··@· %·······
0020  01 fe 04 01 00 35 00 32  a7 2b 00 00 01 00 00 01   ·····5·2 ·+······
0030  00 00 00 00 00 00 03 77  77 77 10 77 69 6c 6c 73   ·······w ww·wills
0040  65 6c 66 64 65 73 74 72  75 63 74 03 63 6f 6d 00   elfdestr uct·com·
0050  00 01 00 01 26 6f cd ab                            ····&o··
```

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
XYZ.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help


NetworkMiner 2.9.0
File Tools Help
--- Select a network adapter in the list ---
Start Stop
Hosts (1095) Files Images Messages (2) Credentials (775) Sessions (2071) DNS (6390) Parameters (79175) Keywords Anomalies
Filter keyword:
□ Case sensitive
ExactPhrase
Any column
Clear Apply

Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Timestamp
80614	192.168.15.4	69.80.225.91 [www.sendanonymousemail.net]	lilytuckrige@yahoo.com		Your class stinks	HTTP	2008-07-22 06:02:5
83601	192.168.15.4	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com]		lilytuckrige@yahoo.com	you can't find us	HTTP	2008-07-22 06:04:2

Attribute	Value

Windows-1252 Western European (Windows)

[no message selected]

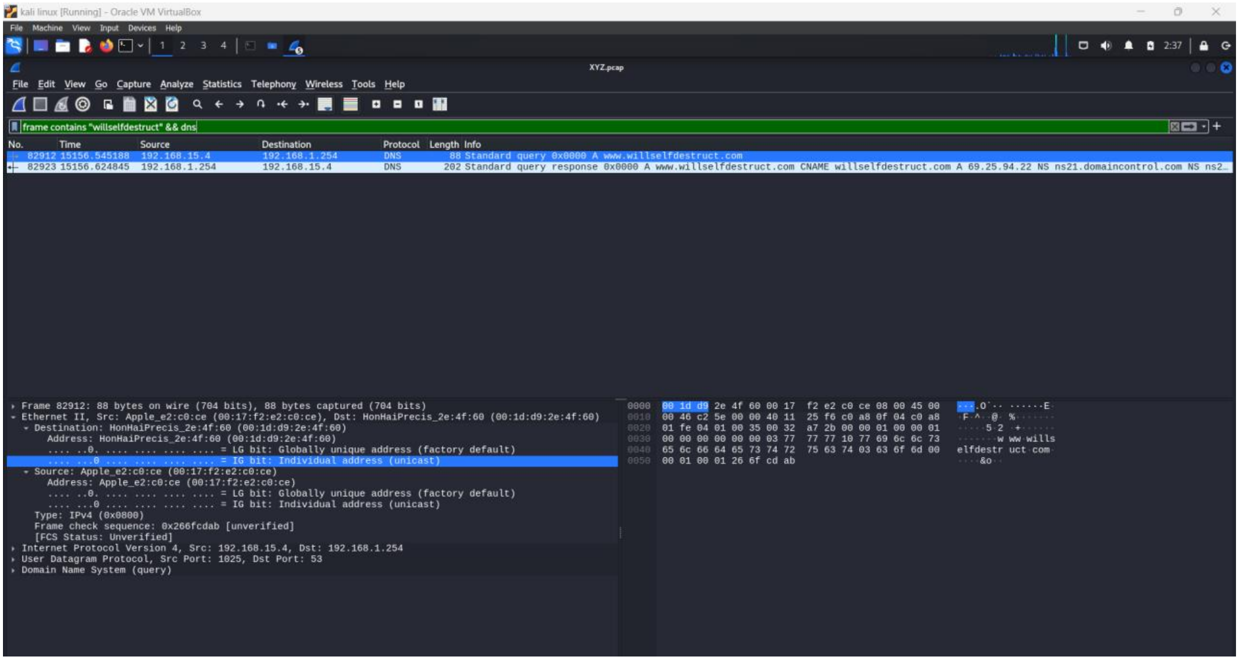
Attachement	Size

Case Panel

Filename	MD5
XYZ.pcap	998182...

3.2 Steps Involved

The archive was extracted to XYZ.pcap and opened using the Wireshark ver 4.2.5 tool and Network Miner v2.9.0 in Windows for analysis. We used the following Cryptographic Hashes; MD5, SHA1, SHA256 to ensure file integrity prior to the giving and examination .Firstly, by extracting the Private IP with the use of content mentioned in the background evidence we can filter based on ip.addr==192.168.15.4 and check the statistics tab provided by Wireshark to get the conversations and endpoints, specifically in endpoints we can see that there’s 73,197 or so packets, while the entire pcap file contains around 94,410 totally.


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
2:37
XYZ.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

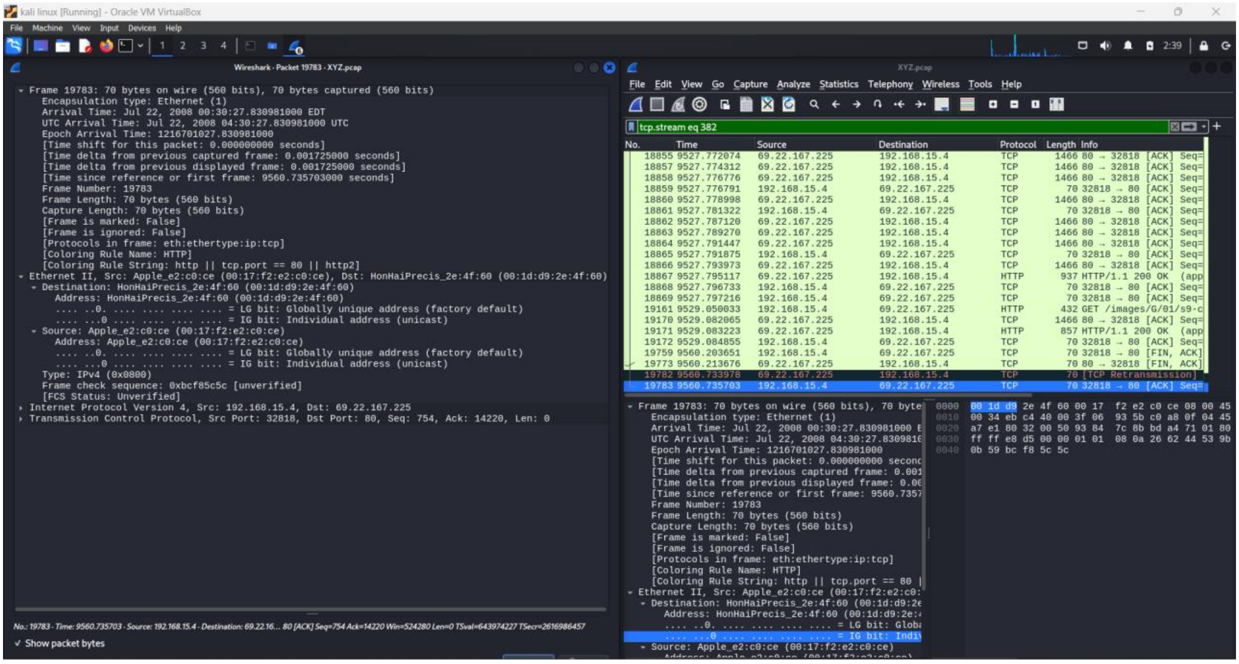
frame contains "willselfdestruct" && dns

```
No.    Time          Source         Destination    Protocol Length Info
 82912 15156.545188  192.168.15.4   192.168.1.254  DNS        88 Standard query 0x0000 A www.willselfdestruct.com
 82923 15156.624845  192.168.1.254  192.168.15.4   DNS       202 Standard query response 0x0000 A www.willselfdestruct.com CNAME willselfdestruct.com A 69.25.94.22 NS ns21.domaincontrol.com NS ns2…
```

```
▸ Frame 82912: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
▾ Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
  ▾ Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
      Address: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
      Address: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    Frame check sequence: 0x266fcdab [unverified]
    [FCS Status: Unverified]
▸ Internet Protocol Version 4, Src: 192.168.15.4, Dst: 192.168.1.254
▸ User Datagram Protocol, Src Port: 1025, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  00 1d d9 2e 4f 60 00 17  f2 e2 c0 ce 08 00 45 00   ···.O`·· ······E·
0010  00 46 c2 5e 00 00 40 11  25 f6 c0 a8 0f 04 c0 a8   ·F·^··@· %·······
0020  01 fe 04 01 00 35 00 32  a7 2b 00 00 01 00 00 01   ·····5·2 ·+······
0030  00 00 00 00 00 00 03 77  77 77 10 77 69 6c 6c 73   ·······w ww·wills
0040  65 6c 66 64 65 73 74 72  75 63 74 03 63 6f 6d 00   elfdestr uct·com·
0050  00 01 00 01 26 6f cd ab                            ····&o··
```

Filtering steps taken include; (eth.addr 00:17:12:e2:c0:ce) for activity on MAC Address, (ip.addr= 192.168.15.4 && http) activity of the HTTP transactions in correlation to the IP address, keyword searches such as (frame contains "gmail.com", and http.host contains "willselfdestruct"), combining filters like (ip.addr 192.168.15.4 && eth.addr 00:17:f2:e2:c0:ce) then following the TCP stream shown in Figure 9. relates to the specific device used, (frame contains "lily") shows those packets set to Lily Tuckridge, (eth.addr = 00:17:f2:e2:c0:ce && frame contains "search result") showing all the searches done by the specific device, and (eth.addr=00:17:f2:e2:c0:ce && frame contains "GET /mail") focusing primarily on the individual and attempting to find their cookie session of their email, focusing entirely on the cookie pairs of the specific MAC address. (eth.addr=00:17:f2:e2:c0:ce && http.cookie_pair).


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
2:39
Wireshark · Packet 19783 · XYZ.pcap
XYZ.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
✓ Show packet bytes

```
▾ Frame 19783: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 22, 2008 00:30:27.830981000 EDT
    UTC Arrival Time: Jul 22, 2008 04:30:27.830981000 UTC
    Epoch Arrival Time: 1216701027.830981000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.001725000 seconds]
    [Time delta from previous displayed frame: 0.001725000 seconds]
    [Time since reference or first frame: 9560.735703000 seconds]
    Frame Number: 19783
    Frame Length: 70 bytes (560 bits)
    Capture Length: 70 bytes (560 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▾ Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
  ▾ Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
      Address: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
      Address: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    Frame check sequence: 0xbcf85c5c [unverified]
    [FCS Status: Unverified]
▸ Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.22.167.225
▸ Transmission Control Protocol, Src Port: 32818, Dst Port: 80, Seq: 754, Ack: 14220, Len: 0
```

No.: 19783 · Time: 9560.735703 · Source: 192.168.15.4 · Destination: 69.22.16… 80 [ACK] Seq=754 Ack=14220 Win=524280 Len=0 TSval=643974227 TSecr=2616986457

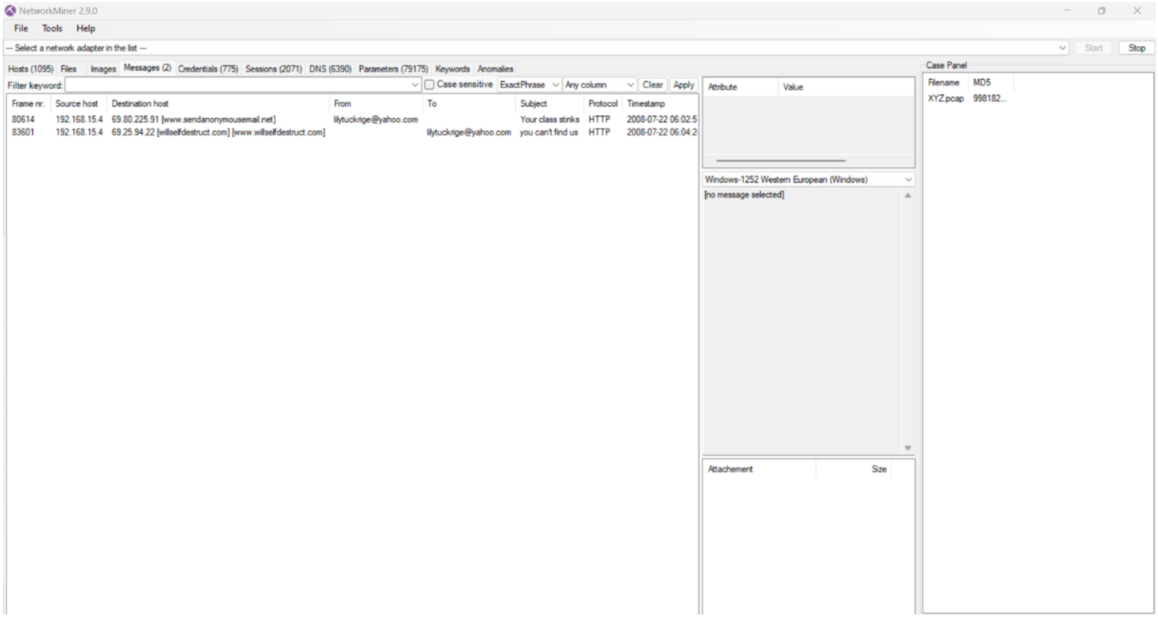
tcp.stream eq 382

```
No.   Time          Source          Destination     Protocol Length Info
18855 9527.772074   69.22.167.225   192.168.15.4    TCP      1466 80 → 32818 [ACK] Seq=
18857 9527.774312   69.22.167.225   192.168.15.4    TCP      1466 80 → 32818 [ACK] Seq=
18858 9527.776776   69.22.167.225   192.168.15.4    TCP      1466 80 → 32818 [ACK] Seq=
18859 9527.776791   192.168.15.4    69.22.167.225   TCP        70 32818 → 80 [ACK] Seq=
18860 9527.778998   69.22.167.225   192.168.15.4    TCP      1466 80 → 32818 [ACK] Seq=
18861 9527.781322   192.168.15.4    69.22.167.225   TCP        70 32818 → 80 [ACK] Seq=
18862 9527.787120   69.22.167.225   192.168.15.4    TCP      1466 80 → 32818 [ACK] Seq=
18863 9527.789270   69.22.167.225   192.168.15.4    TCP      1466 80 → 32818 [ACK] Seq=
18864 9527.791447   69.22.167.225   192.168.15.4    TCP      1466 80 → 32818 [ACK] Seq=
18865 9527.791875   192.168.15.4    69.22.167.225   TCP        70 32818 → 80 [ACK] Seq=
18866 9527.793973   69.22.167.225   192.168.15.4    TCP      1466 80 → 32818 [ACK] Seq=
18867 9527.795117   69.22.167.225   192.168.15.4    HTTP      937 HTTP/1.1 200 OK  (app
18868 9527.796733   192.168.15.4    69.22.167.225   TCP        70 32818 → 80 [ACK] Seq=
18869 9527.797216   192.168.15.4    69.22.167.225   TCP        70 32818 → 80 [ACK] Seq=
19161 9529.050033   192.168.15.4    69.22.167.225   HTTP      432 GET /images/G/01/s9-c
19170 9529.082065   69.22.167.225   192.168.15.4    TCP      1466 80 → 32818 [ACK] Seq=
19171 9529.083223   69.22.167.225   192.168.15.4    HTTP      857 HTTP/1.1 200 OK  (app
19172 9529.084855   192.168.15.4    69.22.167.225   TCP        70 32818 → 80 [ACK] Seq=
19759 9560.203651   192.168.15.4    69.22.167.225   TCP        70 32818 → 80 [FIN, ACK]
19773 9560.213676   69.22.167.225   192.168.15.4    TCP        70 80 → 32818 [FIN, ACK]
19782 9560.733978   69.22.167.225   192.168.15.4    TCP        70 [TCP Retransmission]
19783 9560.735703   192.168.15.4    69.22.167.225   TCP        70 32818 → 80 [ACK] Seq=
```

```
▾ Frame 19783: 70 bytes on wire (560 bits), 70 byte
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 22, 2008 00:30:27.830981000 E
    UTC Arrival Time: Jul 22, 2008 04:30:27.8309810
    Epoch Arrival Time: 1216701027.830981000
    [Time shift for this packet: 0.000000000 seconc
    [Time delta from previous captured frame: 0.001
    [Time delta from previous displayed frame: 0.00
    [Time since reference or first frame: 9560.7357
    Frame Number: 19783
    Frame Length: 70 bytes (560 bits)
    Capture Length: 70 bytes (560 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 |
▾ Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:
  ▾ Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e
      Address: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:
      .... ..0. .... .... .... .... = LG bit: Globa
      .... ...0 .... .... .... .... = IG bit: Indiv
  ▾ Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
```

```
0000  00 1d d9 2e 4f 60 00 17  f2 e2 c0 ce 08 00 45
0010  00 34 eb c4 40 00 3f 06  93 5b c0 a8 0f 04 45
0020  a7 e1 80 32 00 50 93 84  7c 8b bd a4 71 01 80
0030  ff ff e8 d5 00 00 01 01  08 0a 26 62 44 53 9b
0040  0b 59 bc f8 5c 5c
```

Key frame numbers to take note of, 74920 Google search query "can I go to jail for harassing my teacher", 79715 a clear text gmail cookie of (jcoachj@gmail.com) which was tied to the MAC address of the individual, another one to use is 78967 containing another login session done by jcoachj tied down to the MAC address, 80614, and 83601 respectively containing both threat mails sent to Lily Tuckridge connected to the same IP.

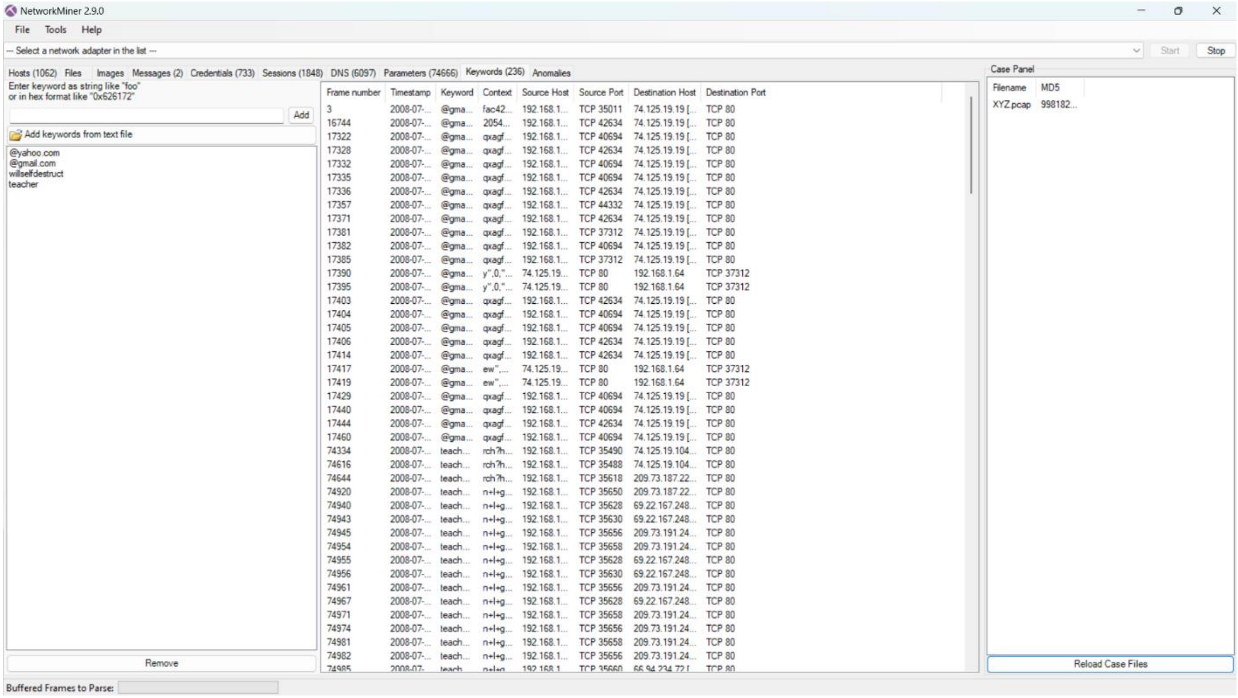


NetworkMiner 2.9.0
File Tools Help
--- Select a network adapter in the list ---
Start
Stop
Hosts (1095) Files Images Messages (2) Credentials (775) Sessions (2071) DNS (6390) Parameters (79175) Keywords Anomalies
Filter keyword:
□ Case sensitive
ExactPhrase
Any column
Clear
Apply
Attribute
Value
Windows-1252 Western European (Windows)
Attachement
Size
Case Panel

Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Timestamp
80614	192.168.15.4	69.80.225.91 [www.sendanonymousemail.net]	lilytuckrige@yahoo.com		Your class stinks	HTTP	2008-07-22 06:02:5
83601	192.168.15.4	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.com]		lilytuckrige@yahoo.com	you can't find us	HTTP	2008-07-22 06:04:2

[no message selected]

Filename	MD5
XYZ.pcap	998182...



NetworkMiner 2.9.0
File Tools Help
--- Select a network adapter in the list ---
Start
Stop
Hosts (1062) Files Images Messages (2) Credentials (733) Sessions (1848) DNS (6097) Parameters (74666) Keywords (236) Anomalies
Add
Add keywords from text file
Remove
Case Panel
Reload Case Files
Buffered Frames to Parse:

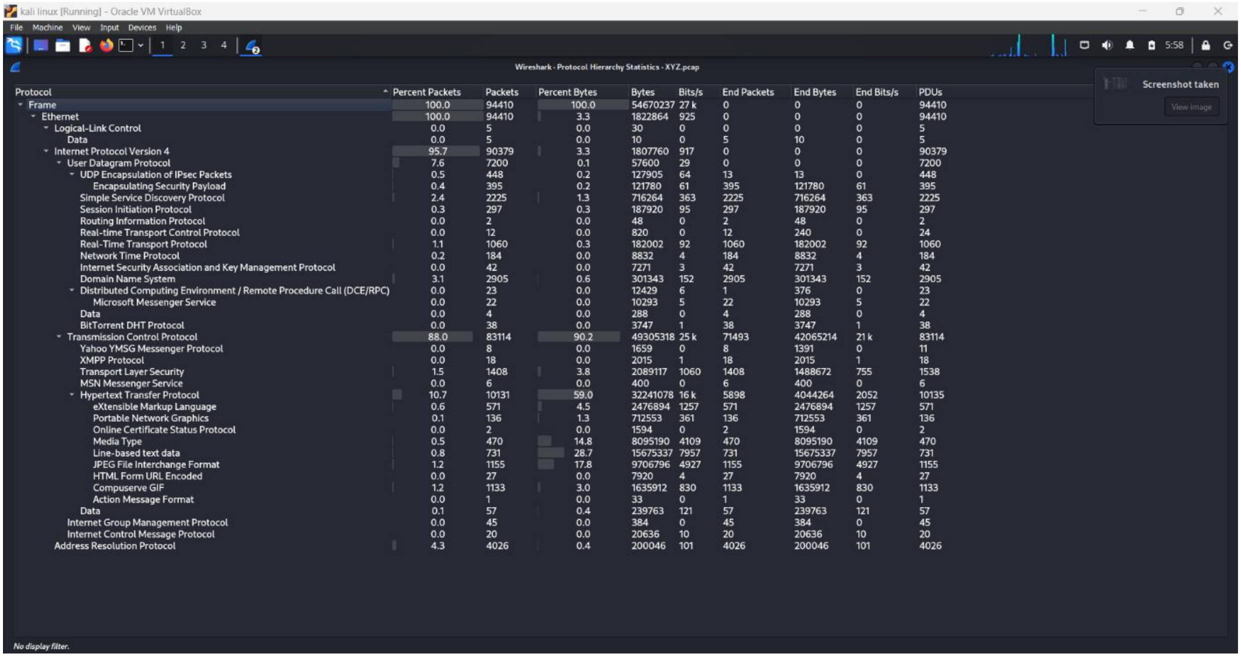
Enter keyword as string like "foo"
or in hex format like "0x626172"

@yahoo.com
@gmail.com
willselfdestruct
teacher

Frame number	Timestamp	Keyword	Context	Source Host	Source Port	Destination Host	Destination Port
3	2008-07-...	@gma...	fac42...	192.168.1...	TCP 35011	74.125.19.19 [...	TCP 80
16744	2008-07-...	@gma...	2054...	192.168.1...	TCP 42634	74.125.19.19 [...	TCP 80
17322	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 40694	74.125.19.19 [...	TCP 80
17328	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 42634	74.125.19.19 [...	TCP 80
17332	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 40694	74.125.19.19 [...	TCP 80
17335	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 40694	74.125.19.19 [...	TCP 80
17336	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 42634	74.125.19.19 [...	TCP 80
17357	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 44332	74.125.19.19 [...	TCP 80
17371	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 42634	74.125.19.19 [...	TCP 80
17381	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 37312	74.125.19.19 [...	TCP 80
17382	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 40694	74.125.19.19 [...	TCP 80
17385	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 37312	74.125.19.19 [...	TCP 80
17390	2008-07-...	@gma...	y",0,"...	74.125.19...	TCP 80	192.168.1.64	TCP 37312
17395	2008-07-...	@gma...	y",0,"...	74.125.19...	TCP 80	192.168.1.64	TCP 37312
17403	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 42634	74.125.19.19 [...	TCP 80
17404	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 40694	74.125.19.19 [...	TCP 80
17405	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 40694	74.125.19.19 [...	TCP 80
17406	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 42634	74.125.19.19 [...	TCP 80
17414	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 42634	74.125.19.19 [...	TCP 80
17417	2008-07-...	@gma...	ew",...	74.125.19...	TCP 80	192.168.1.64	TCP 37312
17419	2008-07-...	@gma...	ew",...	74.125.19...	TCP 80	192.168.1.64	TCP 37312
17429	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 40694	74.125.19.19 [...	TCP 80
17440	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 40694	74.125.19.19 [...	TCP 80
17444	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 42634	74.125.19.19 [...	TCP 80
17460	2008-07-...	@gma...	qxagf...	192.168.1...	TCP 40694	74.125.19.19 [...	TCP 80
74334	2008-07-...	teach...	rch?h...	192.168.1...	TCP 35490	74.125.19.104...	TCP 80
74616	2008-07-...	teach...	rch?h...	192.168.1...	TCP 35488	74.125.19.104...	TCP 80
74644	2008-07-...	teach...	rch?h...	192.168.1...	TCP 35618	209.73.187.22...	TCP 80
74920	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35650	209.73.187.22...	TCP 80
74940	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35628	69.22.167.248...	TCP 80
74943	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35630	69.22.167.248...	TCP 80
74945	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35656	209.73.191.24...	TCP 80
74954	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35658	209.73.191.24...	TCP 80
74955	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35628	69.22.167.248...	TCP 80
74956	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35630	69.22.167.248...	TCP 80
74961	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35656	209.73.191.24...	TCP 80
74967	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35628	69.22.167.248...	TCP 80
74971	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35658	209.73.191.24...	TCP 80
74974	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35656	209.73.191.24...	TCP 80
74981	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35658	209.73.191.24...	TCP 80
74982	2008-07-...	teach...	n+l+g...	192.168.1...	TCP 35656	209.73.191.24...	TCP 80
74985	2008-07-	teach	n+l+g	192.168.1	TCP 35660	66.94.234.72 [	TCP 80

Filename	MD5
XYZ.pcap	998182...

3.3 Handling Data



Wireshark · Protocol Hierarchy Statistics · XYZ.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	94410	100.0	54670237	27 k	0	0	0	94410
Ethernet	100.0	94410	3.3	1822864	925	0	0	0	94410
Logical-Link Control	0.0	5	0.0	30	0	0	0	0	5
Data	0.0	5	0.0	10	0	5	10	0	5
Internet Protocol Version 4	95.7	90379	3.3	1807760	917	0	0	0	90379
User Datagram Protocol	7.6	7200	0.1	57600	29	0	0	0	7200
UDP Encapsulation of IPsec Packets	0.5	448	0.2	127905	64	13	13	0	448
Encapsulating Security Payload	0.4	395	0.2	121780	61	395	121780	61	395
Simple Service Discovery Protocol	2.4	2225	1.3	716264	363	2225	716264	363	2225
Session Initiation Protocol	0.3	297	0.3	187920	95	297	187920	95	297
Routing Information Protocol	0.0	2	0.0	48	0	2	48	0	2
Real-time Transport Control Protocol	0.0	12	0.0	820	0	12	240	0	24
Real-Time Transport Protocol	1.1	1060	0.3	182002	92	1060	182002	92	1060
Network Time Protocol	0.2	184	0.0	8832	4	184	8832	4	184
Internet Security Association and Key Management Protocol	0.0	42	0.0	7271	3	42	7271	3	42
Domain Name System	3.1	2905	0.6	301343	152	2905	301343	152	2905
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.0	23	0.0	12429	6	1	376	0	23
Microsoft Messenger Service	0.0	22	0.0	10293	5	22	10293	5	22
Data	0.0	4	0.0	288	0	4	288	0	4
BitTorrent DHT Protocol	0.0	38	0.0	3747	1	38	3747	1	38
Transmission Control Protocol	88.0	83114	90.2	49305318	25 k	71493	42065214	21 k	83114
Yahoo YMSG Messenger Protocol	0.0	8	0.0	1659	0	8	1391	0	11
XMPP Protocol	0.0	18	0.0	2015	1	18	2015	1	18
Transport Layer Security	1.5	1408	3.8	2089117	1060	1408	1488672	755	1538
MSN Messenger Service	0.0	6	0.0	400	0	6	400	0	6
Hypertext Transfer Protocol	10.7	10131	59.0	32241078	16 k	5898	4044264	2052	10135
eXtensible Markup Language	0.6	571	4.5	2476894	1257	571	2476894	1257	571
Portable Network Graphics	0.1	136	1.3	712553	361	136	712553	361	136
Online Certificate Status Protocol	0.0	2	0.0	1594	0	2	1594	0	2
Media Type	0.5	470	14.8	8095190	4109	470	8095190	4109	470
Line-based text data	0.8	731	28.7	15675337	7957	731	15675337	7957	731
JPEG File Interchange Format	1.2	1155	17.8	9706796	4927	1155	9706796	4927	1155
HTML Form URL Encoded	0.0	27	0.0	7920	4	27	7920	4	27
Compuserve GIF	1.2	1133	3.0	1635912	830	1133	1635912	830	1133
Action Message Format	0.0	1	0.0	33	0	1	33	0	1
Data	0.1	57	0.4	239763	121	57	239763	121	57
Internet Group Management Protocol	0.0	45	0.0	384	0	45	384	0	45
Internet Control Message Protocol	0.0	20	0.0	20636	10	20	20636	10	20
Address Resolution Protocol	4.3	4026	0.4	200046	101	4026	200046	101	4026

Figure 2. Protocol Hierarchy captured with Wireshark ver0.99.7

Protocol/Service	**Percent Packets**	**Packets**	**Percent Bytes**	**Bytes**	**Bits/s**	**End Packets**	**End Bytes**	**End Bits/s**	**PDUs**
Frame	100.0	94410	100.0	54670237	27k	0	0	0	94410
Ethernet	100.0	94410	3.3	1822864	925	0	0	0	94410
Logical-Link Control	0.0	5	0.0	10	0	5	10	0	5
Internet Protocol Version 4	95.7	90379	3.3	1807760	917	0	0	0	90379
User Datagram Protocol	7.6	7200	0.1	57600	29	0	0	0	7200
UDP Encapsulation of IPsec Packets	0.5	448	0.2	127905	64	13	13	0	448
Encapsulating Security Payload	0.4	395	0.2	121780	61	395	121780	61	395

Simple Service Discovery Protocol	2.4	2225	1.3	716264	363	2225	716264	363	2225
Session Initiation Protocol	0.3	297	0.3	187920	95	297	187920	95	297
Routing Information Protocol	0.0	2	0.0	48	0	2	48	0	2
Real-time Transport Control Protocol	0.0	12	0.0	820	0	12	240	0	24
Real-Time Transport Protocol	1.1	1060	0.3	182002	92	1060	182002	92	1060
Network Time Protocol	0.2	184	0.0	8832	4	184	8832	4	184
Internet Security Association and Key Management Protocol	0.0	42	0.0	7271	3	42	7271	3	42
Domain Name System	3.1	2905	0.6	301343	152	2905	301343	152	2905
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.0	23	0.0	12429	6	1	376	0	23
Microsoft Messenger Service	0.0	22	0.0	10293	5	22	10293	5	22
BitTorrent DHT Protocol	0.0	38	0.0	3747	1	38	3747	1	38
Transmission Control Protocol	88.0	83114	90.2	49305318	25k	71493	42065214	21k	83114
Yahoo YMSG Messenger Protocol	0.0	8	0.0	1659	0	8	1391	0	11

XMPP Protocol	0.0	18	0.0	2015	1	18	2015	1	18
Transport Layer Security	1.5	1408	3.8	2089117	1060	1408	1488672	755	1538
MSN Messenger Service	0.0	6	0.0	400	0	6	400	0	6
Hypertext Transfer Protocol	10.7	10131	59.0	32241078	16k	5898	4044264	2052	10135
eXtensible Markup Language	0.6	571	4.5	2476894	1257	571	2476894	1257	571
Portable Network Graphics	0.1	136	1.3	712553	361	136	712553	361	136
Online Certificate Status Protocol	0.0	2	0.0	1594	0	2	1594	0	2
Media Type	0.5	470	14.8	8095190	4109	470	8095190	4109	470
Line-based text data	0.8	731	28.7	15675337	7957	731	15675337	7957	731
JPEG File Interchange Format	1.2	1155	17.8	9706796	4927	1155	9706796	4927	1155
HTML Form URL Encoded	0.0	27	0.0	7920	4	27	7920	4	27
Compuserve GIF	1.2	1133	3.0	1635912	830	1133	1635912	830	1133
Action Message Format	0.0	1	0.0	33	0	1	33	0	1
Internet Group Management Protocol	0.0	45	0.0	384	0	45	384	0	45
Internet Control Message Protocol	0.0	20	0.0	20636	10	20	20636	10	20
Address Resolution Protocol	4.3	4026	0.4	200046	101	4026	200046	101	4026

Table 1. Decomposition of different packet types from capture

Based on the statistics provided in the table, the network traffic was TCP-based, accounting for 88.04% of the total packets. Wireshark TCP filters indicate substantial request-response activity involving IP addresses within the network. A notable portion of the traffic, approximately 10.73% of packets and 25.08% of total bytes, was associated with HTTP communication, suggesting significant web browsing activity. Additionally, a large amount of JPEG and GIF file transfers were observed, making up 17.76% and 2.99% of the total bytes, respectively, which implies the transmission of multimedia content. UDP traffic, particularly DNS queries (3.08% of packets), was also present, indicating active domain name resolution. This analysis is further supported by forensic verification using network monitoring tools, with relevant evidence documented in Evidence File IDs referenced in Section 5, Table 4 of this report.

IP Address	As Sender	As Receiver
192.168.15.4	34554	38643
192.168.1.254	1486	1496
192.168.1.254	12	23
192.168.15.1	2154	0
192.168.1.64	6818	8084

Table 2. Decomposition of IP traffic (Inbound & Outbound)

It is evident from the information presented in the table that 192.168.15.4 was the most prominent player in network activity, with the highest number of packets sent and received. The activity observed on 192.168.15.1 suggests that it did not receive any packets, indicating a role as a broadcasting device or a system primarily focused on outgoing traffic. Additionally, 192.168.1.254 and 192.168.1.64 exhibited moderate network activity, while 192.168.1.254 had minimal engagement, representing an external connection or a low-traffic endpoint.

4. Detailed Findings

4.1 Important network players

No	MAC Address	MAC Address with Name Resolution	IP Address	Vendor	Device
1	Apple_e2:c0:ce	192.168.15.4	Apple, Inc	Macintosh	Intel MAC OS X 10.5.4

2	ARRISGroup_99:98:68 (commscope_99:98:68)	192.168.1.254	ARRIS Group, Inc	Router	
3	HonHaiPrecis_2e:4f:60	192.168.15.1	Hon Hai Precision Ind. Co.,Ltd	Router	
4	HonHaiPrecis_2e:4f:61	192.168.1.64	Hon Hai Precision Ind. Co.,Ltd	Router	
5	WillSelfDestruct.Com	192.168.1.254			

To determine the IP addresses of the different MAC devices on the network, the investigator examined the source and destination addresses on the Ethernet and IP packets being exchanged over this network. This examination was then correlated with the findings between the two layers of the source and destination addresses. This revealed that devices with MAC addresses Apple_e2:c0:c3, ARRISGroup_99:98:68, HonHaiPrecis_2e:4f:60 and HonHaiPrecis_2e:4f:61 owned the IP addresses 192.168.15.4, 192.168.1.254, 192.168.15.1 and 192.168.1.64 respectively.

4.2 Network Structure

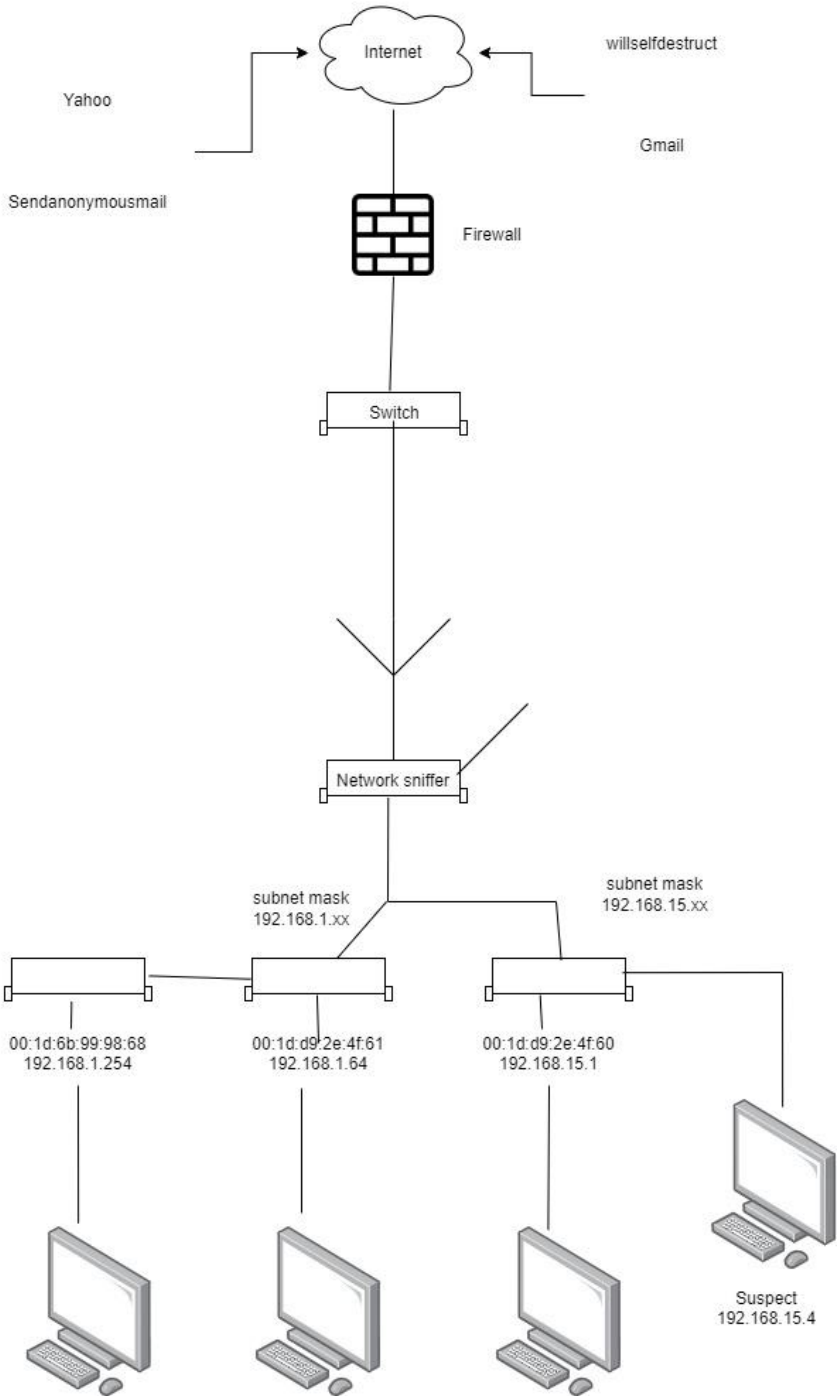

Yahoo
Sendanonymousmail
Internet
willselfdestruct
Gmail
Firewall
Switch
Network sniffer
subnet mask
192.168.1.xx
subnet mask
192.168.15.xx
00:1d:6b:99:98:68
192.168.1.254
00:1d:d9:2e:4f:61
192.168.1.64
00:1d:d9:2e:4f:60
192.168.15.1
Suspect
192.168.15.4

Figure 3. Possible Network Structure based on reconstruction from nforensics.pcap

Here are the sentences from the provided text, with some minor corrections for clarity:

4.2 Network Structure

The internal IP 192.168.1.1 has shown to serve as the network's DNS resolver, evidenced by repeated DNS requests that were sent to this address from the internal devices like 192.168.15.4. With the use of filters like dns && ip.dst == 192.168.1.1 it reveals queries for domains such as WillSelfDestruct.com and sendanonymousmail.net, perfectly aligning with the attackers' activities. The entire network consists of a simple format that follows the essential rules of a switch directing flow of the connection to two routers, one of which is the dorm router, and the other the campus specific one. Both of which are being monitored by the network sniffer for a period of the evidence. The router directly connected to the campus was installed by the boyfriend of one of the dorm students, but the attacker has been using the dorm router connected to their Mac Device.

4.3 Activity Timeline for 192.168.1.103

Packet No.	Activity	Destination	Inference
26211	Google Search	74.125.19.99	Searching for Dark Knight trailer
26249	Visiting news.google.com	74.125.39.99	Going to Google News
51933	Google Search	74.125.19.103	Searching for Sacramento tourist information
52018	Visiting www.hellosacramento.com	65.182.192.74	Just Visiting The Site www.hellosacramento.com
72597	Google Search	74.125.19.104	Searching "how to annoy people"
73157	Visiting annoy.com	66.166.239.194	Visiting Annoy.com
74059	Google Search	74.125.19.104	Searching for anonymous mail services
74334	Google Search	74.125.19.104	Searching "how to harass a teacher"
74920	Yahoo Answers search query	209.73.187.220	Searching for legal consequences of harassment
75852	Google Search	74.125.19.104	Searching for Google Calendar
80614	Visiting www.sendanonymousemail.net	69.80.225.91	Sending first harassment email
83601	Visiting www.willselfdestruct.com	69.25.94.22	Sending a second harassment email

Table 3. Activity Timeline based on network forensic analysis and event reconstruction

Note: Only distinct IP addresses with different time stamps are mentioned on the table. Each IP has a sequence of following TCP/HTTP packets following it which is not captured in this table. Packet numbers provided in the table indicate the first occurrence of the transaction.

4.4 Background evidence

4.4 Background Evidence

1. The original PCAP file was secured using different cryptographic hashing algorithms such as MD5, SHA1, and SHA256 to ensure the chain-of-custody compliance. The hashes have been cross checked multiple times against the scenarios meta data to confirm any signs of tampering or data corruption during said acquisition.
2. The private IP address 192.168.15.4 was found as the origin of the threats sent to Lily Tuckridge, and it correlates to the public IP 140.247.62.34 as shown in Evidence 1, this was further confirmed via MAC address mapping 00:17:f2:e2:c0:ce which was found to be an apple device being used for the attacks.
3. HTTP protocol dissection showed the times Willselfdestruct was accessed by different IP addresses within the network, not limiting to just those by the attacker 192.168.15.4, specifically 192.168.15.7 accessed it as well, but only 192.168.15.4 matched the corresponding MAC address. EV2.
4. Information on the website Willselfdestruct with consideration of the dns, limiting to 2 packets showing us MAC addresses for both the attacker 00:17:f2:e2:c0:ce and the campus router 00:1c:b3:9a:4e:1a this was seen due to the unencrypted TCP handshakes being exposed. EV3.
5. Limiting the MAC addresses to just one (the attacker) and searching for relations with the website will self-destruct, MAC address 00:17:f2:e2:c0:ce being the attackers specific device. This confirmed the use of the apple hardware, and the number of packets is something to note. EV4.
6. Showing all said threats sent to lily, one being the original message sent through sendanonymousmail.net payload containing "Stop teaching. Start running..", and the other from willselfdestruct.com the self-deleting note reads "You can't find us." Packet 80614, and 83601, respectively. EV5.
7. By filtering based on MAC Address we find all searches done with eth.addr 00:17:f2:e2:c0:ce && frame contains "search_result", all of which can be accessed using the file EV6.
8. Under that filter we find the packet 74920 which searches the following "can I go to jail for harassing my teacher", again the exact MAC address we found previously, and with timestamps aligning to the harassment event. EV7.
9. Contains all the email logins done within the network during the packet sniffing allocated time, including the user elishavet@gmail.com and the attacker jcoachj@gmail.com EV8.

10. Using said previous filter we can find elishevet@gmail.com with its relevant cookie pair making use of the boyfriend's router, which was installed into the dorm, this was deduced by the different destination being CommScope EV9.

11. We can now find all the mail logons done from the specific mac address of the attacker eth.addr 00:17:f2:e2:c0:ce && frame contains "GET /mail" EV10.

12. Using that we can find jcoachj@gmail.com being accessed authenticated from that specific Mac Address 00:17:f2:e2:c0:ce in packet 78967 EV11.

13. After finding out that "jcoachj" belongs to the attacker we can find that there's 130~ different packets including Gmail, and Google drive activity from specific email using http.cookie_pair contains "jcoachj" EV12.

14. Now finally using eth.addr 00:17:f2:e2:c0:ce && http.cookie_pair contains "jcoachj" we can test whether the number of packets sent matches that of which sent using the apple device (MAC address) EV13.

15. Now considering a different application we used Network Miner to get more information to further help us with justifying the culprit, by searching keywords in the application such as "Teacher" and "Gmail.com" reveals frame number 74920, again mentioning the "can I go to jail for harassing my teacher", and 79715 which mentions the cleartext cookie of jcoachj tied to the ip address 192.168.15.4.

16. Considering that Wireshark provides a more in-depth analysis, network miner still provided a clear and understanding approach, for example the messages tab directly highlighted both the sendanonymousmail.net and Willselfdetruct.com activities with its corresponding frame numbers. This also confirmed the attacker's activity clustered within a 15-minute window which predated the email deliveries.

17. The attacker's User-Agent was shown multiple times with the help of Network miner, which read Mozilla/5.0 (Macintosh; PPC Mac OS X) indicating an outdated macOS software, with many vulnerabilities.

18. Another thing to consider is the username amy789smith was detected in packet 90471 via Yahoo messenger authentication which was sharing the same IP and MAC address as jcoachj, potentially device sharing between the 2 individuals.

19.

5. Supporting Evidence Presented

Evidence identifier	Content	Content Source	Filename	MD5	SHA1	SHA256
1	Private IP Proof	Wireshark Version 4.4.3	ev_1_privateipproof.txt	e188a19288369b8b4a84edd0995398e3	9f27d994ce8b758932c4ad459237baf65bae65aa	dd8b4e19248b298f5dd53fcfa0611c87615820b301676afe9923991d6937e1cd
2	Will self-Destruct packet capture	Wireshark Version 4.4.3	ev_2_Willselfdestruct.pcap	0babbe4f413c62dd80564925714dc31e	98023a0600ca97ff943192fb09634a985900e6df	84ca4ae37fb42bd401cbae9dcfc45d2e85c6d3e5814dfcce52cfb52cdebfccc7
3	Will self – Destruct with DNS info	Wireshark Version 4.4.3	ev_3_willselfdestructwithednsinfo.txt	c2c16a557433ce10800573937d859396	ee2c1b0e9bef6adb33dba1b34062dfe6ad86630e	98ab5c2a6525a8c8ba92475efcedb33041868134f82542731db64391d0fd625 0
4	Specific MAC address for will self-Destruct	Wireshark Version 4.4.3	ev_4_specificmacaddressforwillselfdestruct.txt	13f4e50ceff2b30a9b5f3146481bce e29	bbc70ce15af18c5e7dc6bdb9a82df9633d13db8d	27bcd2afaf9c938e8fb9d9fb476b75f98bd4ea43e710e747e9c62ecfe9e5e5df
5	All threats sent to Lily	Wireshark Version 4.4.3	ev_5_allthethreatstentolily.pcap	13f4e50ceff2b30a9b5f3146481bce e29	bbc70ce15af18c5e7dc6bdb9a82df9633d13db8d	27bcd2afaf9c938e8fb9d9fb476b75f98bd4ea43e710e747e9c62ecfe9e5e5df
6	Searches Done by Address	Wireshark Version 4.4.3	ev_6_searchesdonebymacaddress.pcap	87f2cef148b663f8f3218e7fe5ca8e2e	0042a562b8a20552339c197850da52dd3ee0bbc2	ce0fd65fff15f7763452ea73bdc540c89cce644dc529052

						f58bdcb348d66c7a85
7	Packet 74920 incrimination	Wireshark Version 4.4.3	ev_7_packet74920incrimination.txt	df8f71207ffbd6e0c087f71d4a26e868	b0e0205f684909a817a83041481eeb761018e267	9d432f7f5133a6872dc62007afc3aa4e4c510783faed61d700729f2d435ab5b a
8	All the logins of the Emails in the Network	Wireshark Version 4.4.3	ev_8_alltheloginsoftheemailsinthenetwork.pcap	23ca932a13dbf9abe53f6c77f40b768a	271cf61f72627044e7863baac1915cbe44b63238	cdf5b78407f87decb1948ac33e994f83f0b5192864f63bd4bccb9a12ed22ea3 0
9	“Elishevet My goat”Note	Wireshark Version 4.4.3	ev_9_elishevetmygoat.txt	b213f46e01f78e507c133d99e96f7b39	fa450908bb2aa7658e853737a0e097ebe3834b14	06f4c7b51825e987f430f9a943a59725368fb4a7d4eabc66d273e19029cf86a 8
10	All mail logons from MAC address	Wireshark Version 4.4.3	ev_10_allmaillogonsfromthemacaddress.pcap	311dae2c80487376c3b2388190719ee2	cc32bf823dfe5eb980fc78881b5021ec4fbb44dd	42fab1319f112da59028b473b605c7406cee6278c394b9b0517fdeb46be0736ef
11	JCoach Email stiff from MAC Address	Wireshark Version 4.4.3	ev_11_jcoachemailstifffrommacaddress.txt	cb5487608dff701a1e0e0d96dd608fa2	3a74e3a14b699239689e2e63dc2ba2e96f9937ee	b3e539f2e6cfcce3d417a4e9dded762f47e2a63b0d9aa747e96479ab1e233a05
12	Jcoach cookie pairs	Wireshark Version 4.4.3	ev_12_jcoachjcookiepairs.pcap	bd69bd8edc339f54bde4d50bf8a4f775	b95c7c33e9bf82161da90ccc3f54dcaff52e4613	085321d65562936aadd5ca2ffb34f05229b618a91c2f69ad2a8984eec0757675

13	Jcoach comparison with MAC address	Wireshark Version 4.4.3	ev_13_jcoachjcomparisonwithmacaddress.pcap	bd69bd8edc339f54bde4d50bf8a4f775	b95c7c33e9bf82161da90ccc3f54dcaff52e4613	085321d65562936aadd5ca2ffb34f05229b618a91c2f69ad2a8984eec0757675
14	TCP Stream proofing	Wireshark Version 4.4.3	ev_14_TCPStreamProofing.txt	813e5df9ba06b9c52c280a3526ef1a2e	95b7fa833a1e00fe96ece1570adfdb91cdcded42	c56595987c85de6e6751441a1533f592ab68b743203ca13bd7419e6c28ca8828

Table 4. Tabulated list of evidence supporting the Forensic report

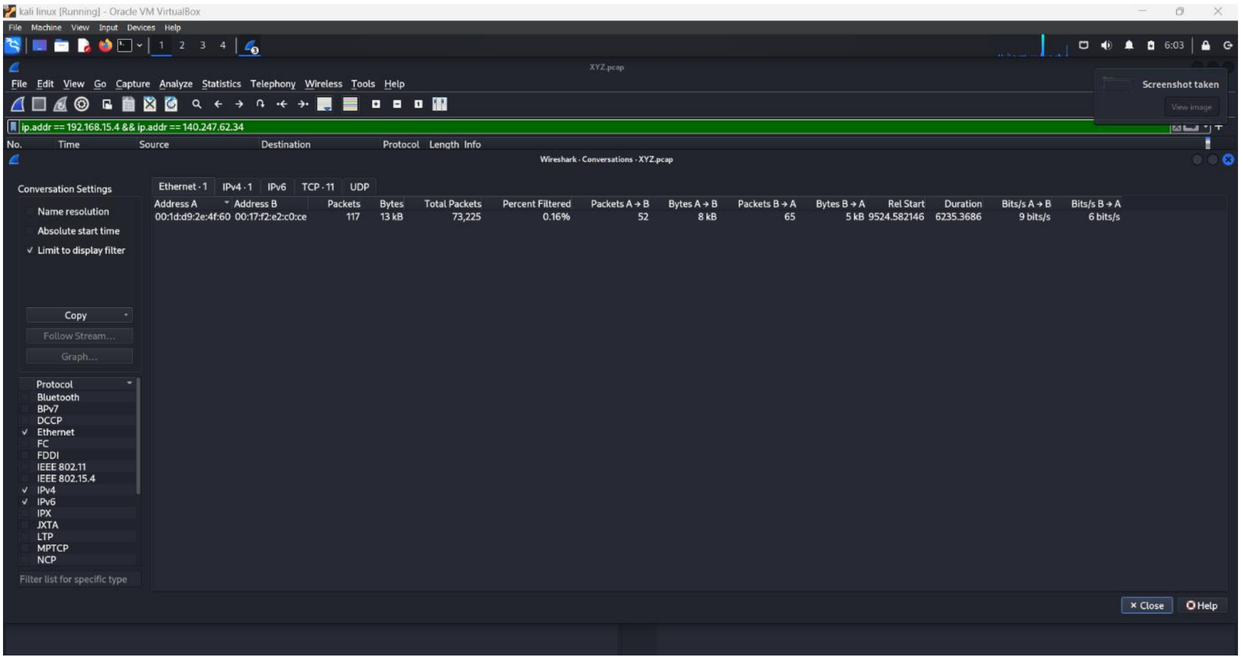
6. Conclusions

7. 5. Conclusions

The forensic analysis of the XYZ.pcap file identifies that JcoachJ who owns the email jcoachj@gmail.com as the perpetrator behind the harassment targeting the teacher Lily Tuckridge, a Chemistry instructor. The investigation was conducted using Wireshark and Network Miner, revealing that the attacker's device (MAC 00:17:12:e2:c0:ce, IP 192.168.15.4), sent harassing emails via the use of services such as sendanonymousmail.net, and willselfdestruct.com with the messages such as "Stop teaching. Start running," and "You can't find us." These emails were routed through the dorm router (00:1d:d9:2e:4f:60), with the help of the network sniffer we were able go over the packets flowing through the network and come up with the following conclusion. The MAC address 00:17:f2:e2:c0:ce, tied to an Apple device, was consistently linked to jcoachj@gmail.com through cleartext HTTP cookies (e.g., gmailchat-jcoachj@gmail.com/945167) found in Google service logins which can be further found in the evidence provided, by following through the TCP stream of the MAC address of the suspect, we found the Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_4; en-us) to be the main device used by said individual, and one other person that has accessed this device but not involved in the harassment. Knowing this Lily Tuckridge is legally capable of acting against the student for these threats if she chooses, furthermore, all evidence provided complies with the standards for the chain of custody, and considering the best practices. All provided evidence has been encrypted with secure hashing algorithms and that will conclude the report.

8. Appendix A – List of figures

Evidence 038



kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
XYZ.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Screenshot taken
View image
No. Time Source Destination Protocol Length Info
Wireshark · Conversations · XYZ.pcap
Copy
Follow Stream…
Graph…
Filter list for specific type
× Close
Help

ip.addr == 192.168.15.4 && ip.addr == 140.247.62.34

Conversation Settings

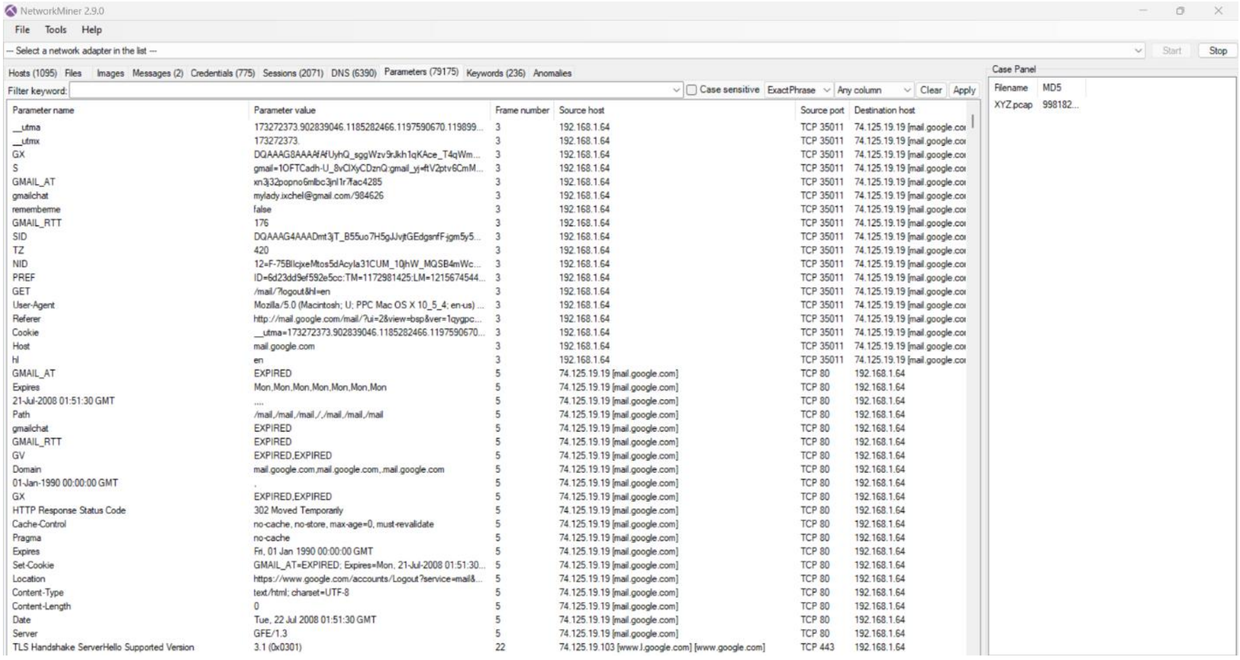
- Name resolution
- Absolute start time
- ✓ Limit to display filter

Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 11 | UDP

Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:1d:d9:2e:4f:60	00:17:f2:e2:c0:ce	117	13 kB	73,225	0.16%	52	8 kB	65	5 kB	9524.582146	6235.3686	9 bits/s	6 bits/s

Protocol

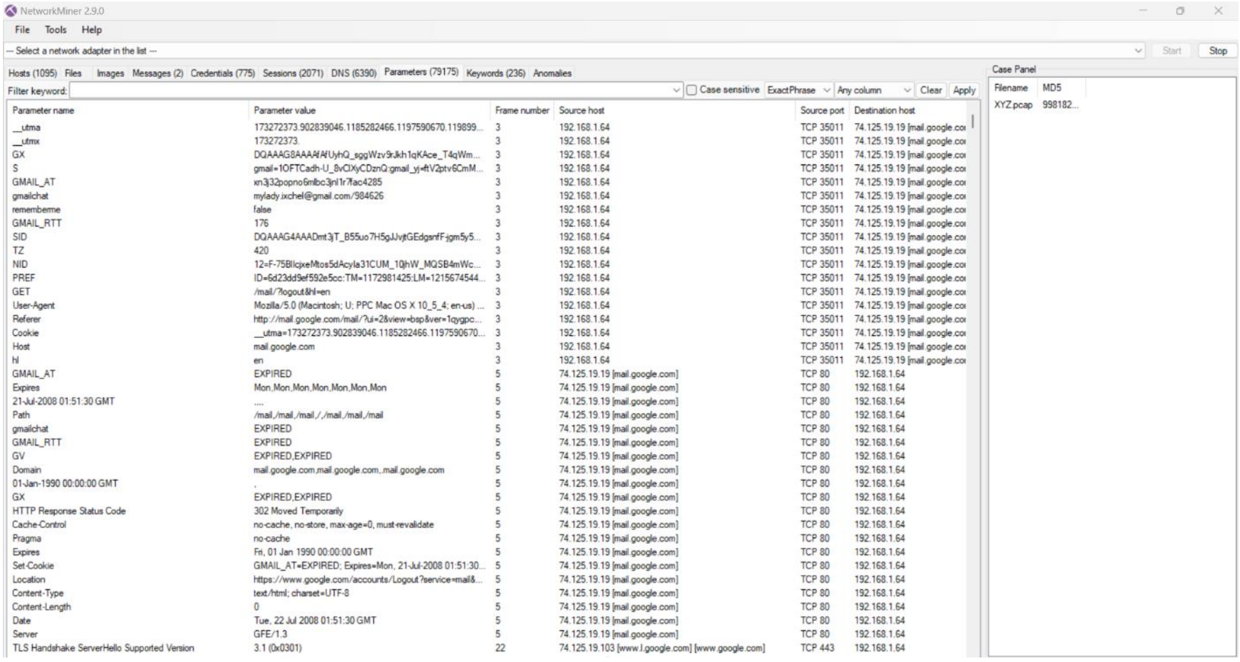
- Bluetooth
- BPv7
- DCCP
- ✓ Ethernet
- FC
- FDDI
- IEEE 802.11
- IEEE 802.15.4
- ✓ IPv4
- ✓ IPv6
- IPX
- JXTA
- LTP
- MPTCP
- NCP



NetworkMiner 2.9.0
File Tools Help
--- Select a network adapter in the list ---
Start
Stop
Hosts (1095) Files Images Messages (2) Credentials (775) Sessions (2071) DNS (6390) Parameters (79175) Keywords (236) Anomalies
Filter keyword:
☐ Case sensitive
ExactPhrase
Any column
Clear
Apply
Case Panel

Filename	MD5
XYZ.pcap	998182...

Parameter name	Parameter value	Frame number	Source host	Source port	Destination host
__utma	173272373.902839046.1185282466.1197590670.119899...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
__utmx	173272373.	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GX	DQAAAG8AAAAfAfUyhQ_sggWzv9rJkh1qKAce_T4qWm...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
S	gmail=1OFTCadh-U_8vClXyCDznQ:gmail_yj=ftV2ptv6CmM...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GMAIL_AT	xn3j32popno6mlbc3jnl1r7fac4285	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
gmailchat	mylady.ixchel@gmail.com/984626	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
rememberme	false	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GMAIL_RTT	176	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
SID	DQAAAG4AAADmt3jT_B55uo7H5gJJvjtGEdgsnfF-jgm5y5...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
TZ	420	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
NID	12=F-75BIlcjxeMtos5dAcyla31CUM_10jhW_MQSB4mWc...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
PREF	ID=6d23dd9ef592e5cc:TM=1172981425:LM=1215674544...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GET	/mail/?logout&hl=en	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
User-Agent	Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_5_4; en-us) ...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
Referer	http://mail.google.com/mail/?ui=2&view=bsp&ver=1qygpc...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
Cookie	__utma=173272373.902839046.1185282466.1197590670...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
Host	mail.google.com	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
hl	en	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GMAIL_AT	EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Expires	Mon,Mon,Mon,Mon,Mon,Mon,Mon	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
21-Jul-2008 01:51:30 GMT	....	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Path	/mail,/mail,/mail,/,/mail,/mail,/mail	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
gmailchat	EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
GMAIL_RTT	EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
GV	EXPIRED,EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Domain	mail.google.com,mail.google.com,.mail.google.com	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
01-Jan-1990 00:00:00 GMT	.	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
GX	EXPIRED,EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
HTTP Response Status Code	302 Moved Temporarily	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Cache-Control	no-cache, no-store, max-age=0, must-revalidate	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Pragma	no-cache	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Expires	Fri, 01 Jan 1990 00:00:00 GMT	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Set-Cookie	GMAIL_AT=EXPIRED; Expires=Mon, 21-Jul-2008 01:51:30...	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Location	https://www.google.com/accounts/Logout?service=mail&...	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Content-Type	text/html; charset=UTF-8	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Content-Length	0	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Date	Tue, 22 Jul 2008 01:51:30 GMT	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Server	GFE/1.3	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
TLS Handshake ServerHello Supported Version	3.1 (0x0301)	22	74.125.19.103 [www.l.google.com] [www.google.com]	TCP 443	192.168.1.64



Filter keyword: □ Case sensitive ExactPhrase Any column

Parameter name	Parameter value	Frame number	Source host	Source port	Destination host
__utma	173272373.902839046.1185282466.1197590670.119899...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
__utmx	173272373.	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GX	DQAAAG8AAAAfAfUyhQ_sggWzv9rJkh1qKAce_T4qWm...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
S	gmail=1OFTCadh-U_8vClXyCDznQ:gmail_yj=ftV2ptv6CmM...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GMAIL_AT	xn3j32popno6mlbc3jnl1r7fac4285	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
gmailchat	mylady.ixchel@gmail.com/984626	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
rememberme	false	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GMAIL_RTT	176	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
SID	DQAAAG4AAADmt3jT_B55uo7H5gJJvjtGEdgsnfF-jgm5y5...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
TZ	420	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
NID	12=F-75BIlcjxeMtos5dAcyla31CUM_10jhW_MQSB4mWc...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
PREF	ID=6d23dd9ef592e5cc:TM=1172981425:LM=1215674544...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GET	/mail/?logout&hl=en	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
User-Agent	Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_5_4; en-us) ...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
Referer	http://mail.google.com/mail/?ui=2&view=bsp&ver=1qygpc...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
Cookie	__utma=173272373.902839046.1185282466.1197590670...	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
Host	mail.google.com	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
hl	en	3	192.168.1.64	TCP 35011	74.125.19.19 [mail.google.co
GMAIL_AT	EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Expires	Mon,Mon,Mon,Mon,Mon,Mon,Mon	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
21-Jul-2008 01:51:30 GMT	.....	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Path	/mail,/mail,/mail,/,/mail,/mail,/mail	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
gmailchat	EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
GMAIL_RTT	EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
GV	EXPIRED,EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Domain	mail.google.com,mail.google.com,.mail.google.com	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
01-Jan-1990 00:00:00 GMT	,	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
GX	EXPIRED,EXPIRED	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
HTTP Response Status Code	302 Moved Temporarily	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Cache-Control	no-cache, no-store, max-age=0, must-revalidate	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Pragma	no-cache	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Expires	Fri, 01 Jan 1990 00:00:00 GMT	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Set-Cookie	GMAIL_AT=EXPIRED; Expires=Mon, 21-Jul-2008 01:51:30...	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Location	https://www.google.com/accounts/Logout?service=mail&...	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Content-Type	text/html; charset=UTF-8	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Content-Length	0	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Date	Tue, 22 Jul 2008 01:51:30 GMT	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
Server	GFE/1.3	5	74.125.19.19 [mail.google.com]	TCP 80	192.168.1.64
TLS Handshake ServerHello Supported Version	3.1 (0x0301)	22	74.125.19.103 [www.l.google.com] [www.google.com]	TCP 443	192.168.1.64

Filename	MD5
XYZ.pcap	998182...

Contribution

T W V Fernando - s8145685

I arranged everything accordingly using Wireshark so that we can understand the behavior of the network

And as well as I used the given Pcap file to analyze & filter the packets by using various techniques.

Did background research that included background evidence and presented it accordingly.

MDP Induwara – s 8145490

I explained the behavior and the things that process inside this network

I diagramed the network structure and found the how data handles in this network as well as provided with the timeline which set things accordingly.

Additionally, I presented the supporting evidence to this report.