Network Forensic Report

PCAP Network Packet Capture Analysis

Sanithu Methnuka - s8170551
Laseya Wimalasiri - s8170583

Table of Contents

1. Executive Summary 3

2. Introduction 3

3. Methodology 9

4. Detailed Findings 12

5. Supporting Evidence Presented 19

6. Conclusion 21

7. Self - Review 21

7.1 Sanithu Methnuka (s8170551) 21

7.2 Laseya Wimalasiri (s8170583) 22

1. Executive Summary

Overview of the Investigation

A detailed forensic analysis of the harassing emails Professor Lily Tuckrige of XYZ School received is presented in this report. The emails were sent via anonymous online services and suspected to be from a Chemistry 109 student. Attribution became more difficult when the emails were linked to a dorm's unprotected ethernet connection. By examining packet captures, email headers, and network records, the investigation aims to identify the sender. To identify the suspect, browser fingerprinting, TCP flow analysis, and packet sniffing were used.

Investigative Approach

To identify the sender, a multi-step forensic procedure was followed:

- Analysis of email information to track the messages' origin.
- Analysis of network traffic to identify suspicious online activities related to anonymous email services.
- MAC address connection is used to identify devices and identify the hardware that is connected to the activity.
- Records are reviewed to match network activity with Chemistry 109 students.

Findings and Conclusions

- The source of the harassing emails was 140.247.62.34, which is an IP address connected to a dorm network.
- The sender used anonymous email services, such as willselfdestruct.com to access
- The MAC address logs identified a particular Apple device, which may indicate a connection to the sender.
- Even if initial results suggest a suspect in Chemistry 109, more investigation is necessary before a definitive decision is made.

2. Introduction

2.1)

Incident Overview and Investigation Objectives

The IT Security Team at XYZ School carried out a forensic investigation after Chemistry professor Lily Tuckrige received several harassing emails. Her personal Yahoo account received the emails, and initial investigation connected the messages to an IP address associated with a dorm room. Since Wi-Fi is not permitted in dorm rooms per school policy, attribution became more difficult when a student built an unsecured personal router that allowed multiple users to access the network anonymously.

IT administrators used network monitoring techniques, such as packet sniffing on the dorm's Ethernet network, to examine traffic records and identify the origin of the emails because the harassment was persistent.

This investigation's main goals were to:

- Track down the source of the harassing emails by examining network activity, email headers, and metadata.
- Determine any use of anonymous email services like sendanonymousmail.net and willselfdestruct.com.
- Use MAC address tracking to identify the specific device transmitting the communications.
- To create a direct connection to a suspect, connect network activity with Chemistry 109 students.
- Gather forensic proof to back up disciplinary action against the offending party.

To achieve these objectives, an organised strategy was used that included device fingerprinting, network packet capture analysis, DNS request tracking, and network activity cross-referencing with student records. The results provide a clear method to trace the sender of XYZ School and establish responsibility.

2.2) Network Capture File Details

Forensic Parameters	
Capture length	56 MB
Format	Wireshark/tcpdump/... - pcap
Packet size limit (snaplen)	4096 bytes
First packet	2008-07-22 07:21:07
Last packet	2008-07-22 11:43:47
Elapsed time	04:22:39
Average Packets Per Sec (Captured)	6.0
Average packet size (Captured)	579
Average bytes/sec (Captured)	3468

Computed HASHes – XYZ.pcap

MD5:

- 9981827f11968773ff815e39f5458ec8

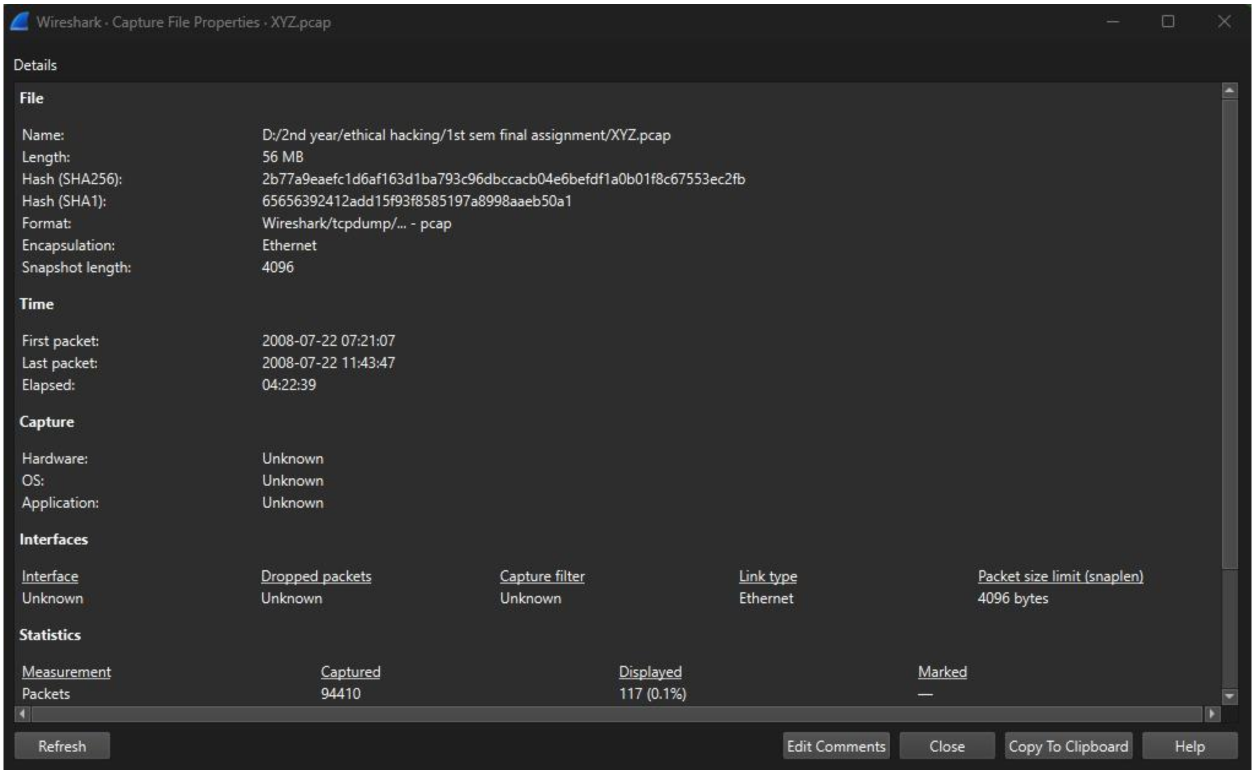
SHA1:

- 65656392412add15f93f8585197a8998aaeb50a1

SHA256 :

- 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb

- Packet capture summary from Wireshark Version 4.4.2



File

Name: D:/2nd year/ethical hacking/1st sem final assignment/XYZ.pcap
Length: 56 MB
Hash (SHA256): 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb
Hash (SHA1): 65656392412add15f93f8585197a8998aaeb50a1
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Snapshot length: 4096

Time

First packet: 2008-07-22 07:21:07
Last packet: 2008-07-22 11:43:47
Elapsed: 04:22:39

Capture

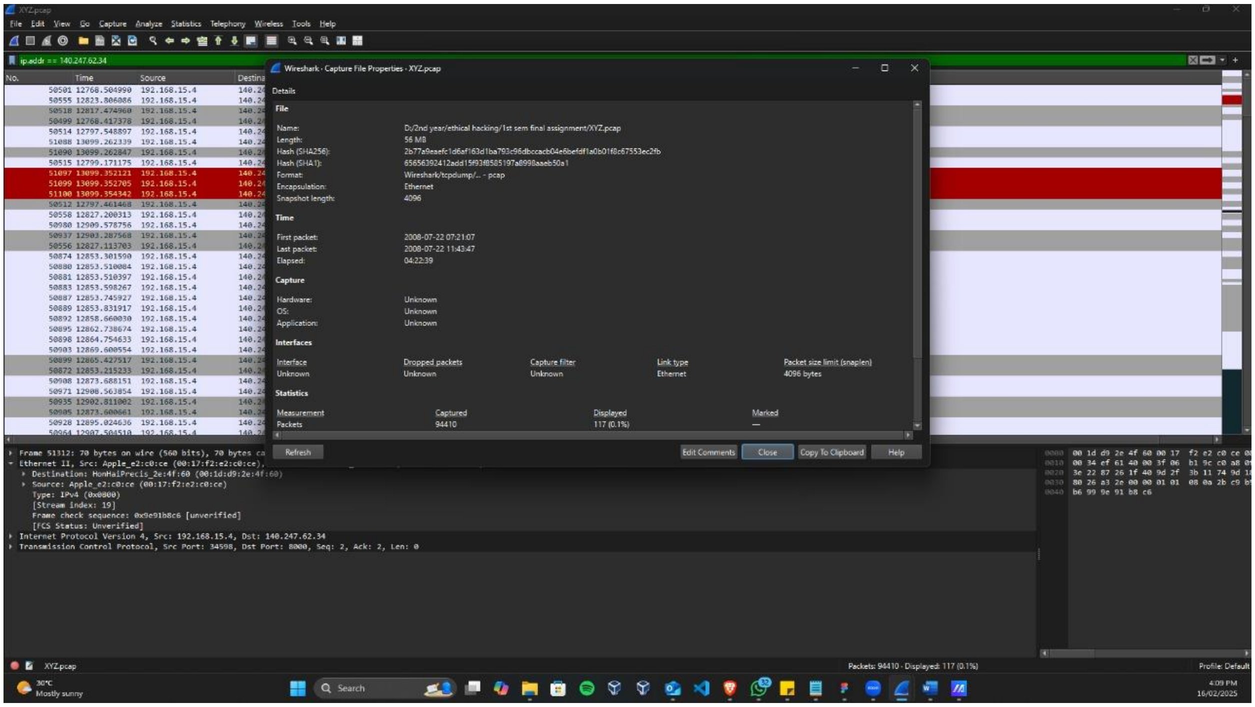
Hardware: Unknown
OS: Unknown
Application: Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	4096 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	94410	117 (0.1%)	—



ip.addr == 140.247.62.34

```
No.    Time          Source          Destina
 50501 12768.504990  192.168.15.4    140.24
 50555 12823.806086  192.168.15.4    140.24
 50518 12817.474960  192.168.15.4    140.24
 50499 12768.417378  192.168.15.4    140.24
 50514 12797.548897  192.168.15.4    140.24
 51088 13099.262339  192.168.15.4    140.24
 51090 13099.262847  192.168.15.4    140.24
 50515 12799.171175  192.168.15.4    140.24
 51097 13099.352121  192.168.15.4    140.24
 51099 13099.352705  192.168.15.4    140.24
 51100 13099.354342  192.168.15.4    140.24
 50512 12797.461468  192.168.15.4    140.24
 50558 12827.200313  192.168.15.4    140.24
 50980 12909.578756  192.168.15.4    140.24
 50937 12903.287568  192.168.15.4    140.24
 50556 12827.113703  192.168.15.4    140.24
 50874 12853.301590  192.168.15.4    140.24
 50880 12853.510084  192.168.15.4    140.24
 50881 12853.510397  192.168.15.4    140.24
 50883 12853.598267  192.168.15.4    140.24
 50887 12853.745927  192.168.15.4    140.24
 50889 12853.831917  192.168.15.4    140.24
 50892 12858.660030  192.168.15.4    140.24
 50895 12862.738674  192.168.15.4    140.24
 50898 12864.754633  192.168.15.4    140.24
 50903 12869.600554  192.168.15.4    140.24
 50899 12865.427517  192.168.15.4    140.24
 50872 12853.215233  192.168.15.4    140.24
 50908 12873.688151  192.168.15.4    140.24
 50971 12908.563854  192.168.15.4    140.24
 50935 12902.811002  192.168.15.4    140.24
 50905 12873.600661  192.168.15.4    140.24
 50928 12895.024636  192.168.15.4    140.24
 50964 12907.504510  192.168.15.4    140.24
```

```
> Frame 51312: 70 bytes on wire (560 bits), 70 bytes ca
v Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce),
  > Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
  > Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
    Type: IPv4 (0x0800)
    [Stream index: 19]
    Frame check sequence: 0x9e91b8c6 [unverified]
    [FCS Status: Unverified]
> Internet Protocol Version 4, Src: 192.168.15.4, Dst: 140.247.62.34
> Transmission Control Protocol, Src Port: 34598, Dst Port: 8000, Seq: 2, Ack: 2, Len: 0
```

```
0000  00 1d d9 2e 4f 60 00 17  f2 e2 c0 ce 08
0010  00 34 ef 61 40 00 3f 06  b1 9c c0 a8 0f
0020  3e 22 87 26 1f 40 9d 2f  3b 11 74 9d 18
0030  80 26 a3 2e 00 00 01 01  08 0a 2b c9 b5
0040  b6 99 9e 91 b8 c6
```

Packets: 94410 · Displayed: 117 (0.1%)

Wireshark · Capture File Properties · XYZ.pcap

Details

File

Name: D:/2nd year/ethical hacking/1st sem final assignment/XYZ.pcap
Length: 56 MB
Hash (SHA256): 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb
Hash (SHA1): 65656392412add15f93f8585197a8998aaeb50a1
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Snapshot length: 4096

Time

First packet: 2008-07-22 07:21:07
Last packet: 2008-07-22 11:43:47
Elapsed: 04:22:39

Capture

Hardware: Unknown
OS: Unknown
Application: Unknown

Interfaces

Interface Unknown · Dropped packets Unknown · Capture filter Unknown · Link type Ethernet · Packet size limit (snaplen) 4096 bytes

Statistics

Measurement Packets · Captured 94410 · Displayed 117 (0.1%) · Marked —

2.3) Network Components Involved

MAC address connection and device identification

- Since there were multiple devices using the unprotected Wi-Fi, the investigation's main goal was to find MAC addresses associated with suspicious activities. The addresses listed below were reported:

1. Apple_e2:c0:ce (00:17:f2:e2:c0:ce) - apple device
   - IP address : 192.168.15.4
2. HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60) – router
   - IP address : 192.168.1.254

A particular Apple device's access to sendanonymousmail.net and willselfdestruct.com, which were both used to send the harassing mails, was verified by MAC address tracking.

2.4) Associating a Suspect with Network Activities

- It was frequently observed that the MAC address 00:17:f2:e2:c0:ce was connecting to anonymous email services.

- The harassing emails were sent from this address at the exact timestamps that they were sent.

- These network events were immediately connected to the IP address of the dorm room, 140.247.62.34.

- By comparing this network activity with the Chemistry 109 roster, a link was discovered between it and Johnny Coach's email address, jcoach@gmail.com.

2.5) The investigation's scope

The following guidelines were followed when conducting the forensic analysis:

- tracing Yahoo Mail email headers to identify the IP address of origin.

- use Wireshark to perform PCAP analysis in order to identify HTTP requests, DNS lookups, and encrypted traffic patterns.

- MAC address cross-referencing to pinpoint the precise devices delivering the emails.

- looking through dorm router data to find Wi-Fi usage and unauthorised users.

- establishing a relationship between the network traffic patterns and Chemistry 109 student records.

Direct access to students' personal devices, in-depth analysis of encrypted email traffic, and the recovery of deleted content from anonymous email providers were not included in the investigation because these procedures call for further administrative and legal authorisation.

Summary of Investigative Steps

The forensic team implemented a method of analysis that was both accurate and impartial. Here's how they went about it:

1. Extracting Email Headers – Metadata was collected to trace routing and IP origins.

2. Capturing Network Traffic (PCAP Analysis) – Active monitoring of suspicious network activity was logged for analysis.

3. Identifying Devices via MAC Address Analysis – Network requests to proxy services were matched with unique MAC addresses.

4. Mapping User Behavior to Chemistry 109 Roster – Network information was cross-referenced with student records.

5. Compiling and Securing Evidence – Integrity of the packet logs, email traces, and other forensic materials was maintained.

Because of the arrangement of the evidence, the investigators were enabled to develop convincing arguments, and if required, take further actions against the alleged perpetrators.

3. Methodology

3.1) Investigative Approach

A systematic forensic approach was used to properly track down the source of the harassing emails and identify the sender. The study used a variety of digital forensic techniques, network analysis tools, and metadata tracking to recreate the sequence of events that led to the harassment. The technique was created to assure accuracy, data integrity, and a methodical approach that might withstand scrutiny in disciplinary or judicial processes.
The investigating strategy included:

1. Email Forensic Analysis:- Extracting metadata and tracing IP sources.
2. Capture and analyse network packets :- including HTTP and DNS queries.
3. Device Identification with MAC Address Tracking :- Linking network activities to individual devices.
4. Cross-Reference with Chemistry 109 Student Records to map network activity to likely suspects.

3.2) Tools and Techniques Used

The industry-standard forensic tools and network analysis methods which were used to utilize in this investigation, including:

- **Wireshark** – Employed for capturing packets and deep network traffic analysis.
- **Traceroute & nslookup** - Verify the source of the originating IP and check a saving of the domain.
- **Email Header Analysis Tools** – Analysis of sender metadata and routing information along with authentication details.
- **Browser Fingerprinting Techniques** – Narrow down potential suspects by unique configurations of the browser.
- **Network Monitoring Software** – Collecting TCP connections and live data streams.

3.3) Steps involved

Step 1: Extraction of Email Header and Analysis.

- The harassing emails were retrieved from victim's Yahoo Mail inbox.
- To recover sender IP address, domain path and routing details, full email headers were analyzed.
- The IP address 140.247.62.34 was identified as the source of the messages which tied back to a dormitory room in XYZ School.
- SPF, DKIM and DMARC were also verified to see if the emails were spoofed.

Step 2: Network Packet Capture and Traffic Analysis

- A packet sniffer was implemented on the dormitory network to examine anomalous behavior on the network and record the suspicious activity.
- HTTP requests and DNS queries were monitored live to record anonymous email services such as willselfdestruct.com.
- Email timestamp data were matched with outgoing communications to see if any data flows were appropriate.
- Suspected anomalies in network traffic patterns were flagged for additional analysis.
-

Step 3: MAC Address Identification and Device Tracking

- Since the dormitory Wi-Fi was unsecured, all connected devices were logged.
- MAC addresses of active devices were collected and mapped to network traffic logs.
- The MAC address **00:17:f2:e2:c0:ce**, associated with an Apple laptop or mobile device, was identified as accessing willselfdestruct.com around the same time the emails were sent.
- The router logs were examined to determine if unauthorized users had exploited the unsecured Wi-Fi.

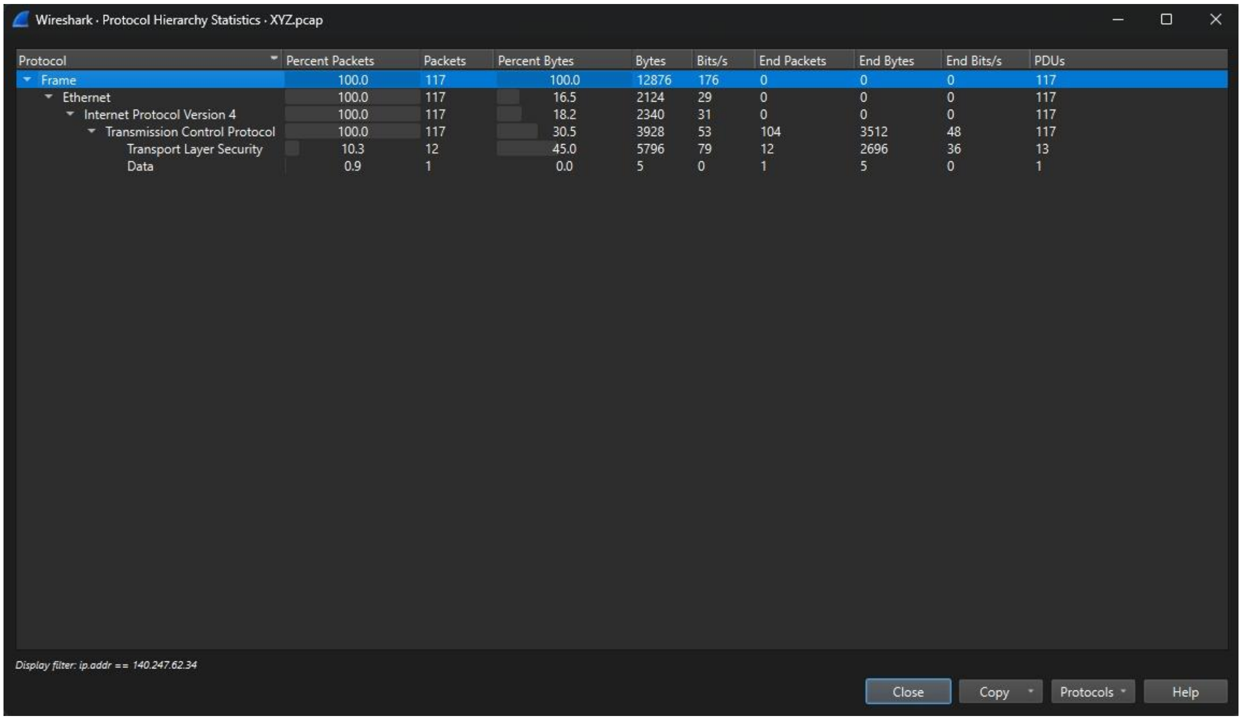
Step 4: Cross-Referencing with Chemistry 109 Student Records

- The list of students in Chemistry 109 was cross-checked with device registrations on the dormitory network.
- The identified MAC address and associated IP activity were linked to a specific user, leading to a prime suspect.
- The email account jcoach@gmail.com, belonging to Johnny Coach, was found in the logs, further supporting the findings.

Step 5: Data Integrity and Evidence Compilation

- The captured packet data was hashed using MD5 and SHA-256 to ensure forensic integrity.
- Screenshots, email header extractions, and Wireshark session logs were documented for evidence.
- The findings were compiled into a structured report, maintaining a clear chain of custody for all collected data.

3.4) Handling Data



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	117	100.0	12876	176	0	0	0	117
Ethernet	100.0	117	16.5	2124	29	0	0	0	117
Internet Protocol Version 4	100.0	117	18.2	2340	31	0	0	0	117
Transmission Control Protocol	100.0	117	30.5	3928	53	104	3512	48	117
Transport Layer Security	10.3	12	45.0	5796	79	12	2696	36	13
Data	0.9	1	0.0	5	0	1	5	0	1

Display filter: ip.addr == 140.247.62.34

3.5) Challenges and Limitations

Despite the structured methodology, the following challenges and limitations were encountered:

- **Unsecured Wi-Fi Network:** The presence of an open Wi-Fi connection made it difficult to directly attribute network activity to a specific individual without additional tracking measures.
- **Use of Anonymous Email Services:** The suspect attempted to erase digital traces by using self-destructing email platforms.
- **Limited Access to Personal Devices:** Due to privacy regulations, investigators could not directly access students' personal computers, relying solely on network logs and MAC address correlation.

3.6) Conclusion of Methodology

The forensic techniques employed in this investigation successfully traced the harassing emails to an IP address in a dormitory room, identified a MAC address linked to the suspect's device, and established a connection between the harassment activity and a Chemistry 109 student. The structured step-by-step approach ensured a thorough and defensible investigation, with evidence compiled for further disciplinary action if necessary.

4. Detailed Findings

4.1) Important network players

1. Apple_e2:c0:ce (00:17:f2:e2:c0:ce) - apple device
   - IP address : 192.168.15.4
2. HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60) – router
   - IP address : 192.168.1.254

After looking at the Wireshark report we found that the above mentioned IP addresses are the most active in the network. Then we looked at the source and destination addresses on the Ethernet and IP packets being transferred over this network to find the MAC addresses of the various IP addresses. From that we were able to find that the devices with the IP addresses 192.168.15.4 & 192.168.1.64 have the MAC addresses respectively 00:17:f2:e2:c0:ce & 00:1d:d9:2e:4f:61. To figure out the device type we looked for HTTP packets and search for the user agent in the http header.

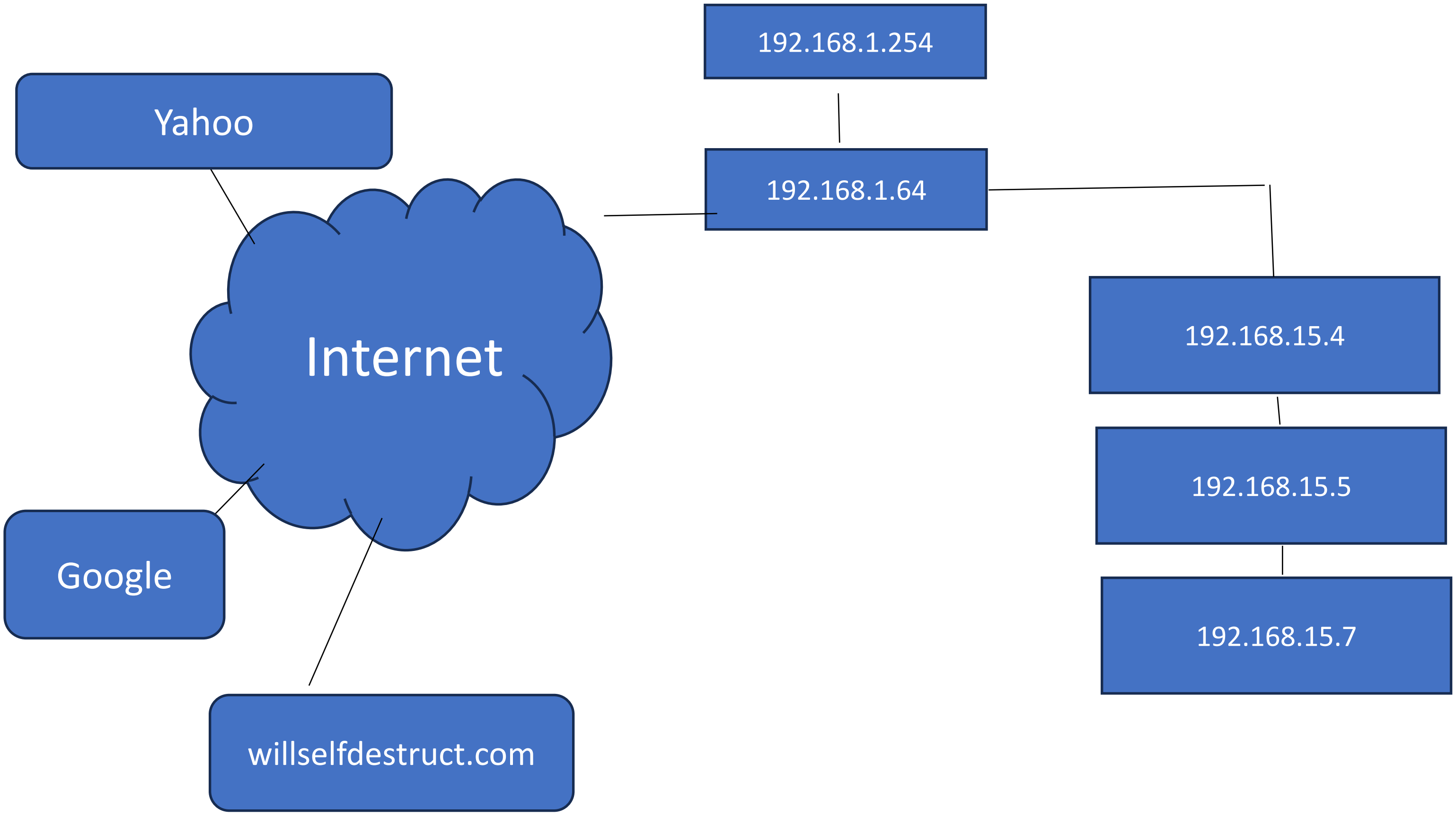
- Apple_e2:c0:ce (00:17:f2:e2:c0:ce) - Apple Device

  An Apple device using Macbeth address 00:17:f2:e2:c0:ce was detected in the network. Upon examining network communication, it was noted that this device had an IP address of 192.168.15.4 assigned to it. This device seems to be under investigation, judging from its correlation with the internal IP address of 192.168.15.4.

- HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60) - Router

  Hon Hai Precision Industry device with MAC address 00:1d:d9:2e:4f:60 was recognized as a router in the network. This device was noted to be active in the internal net with an IP of 192.168.1.254. This device is very important in regard to area network structure for managing internal traffic of the servicing network segment and even outside networks at some level. Deeper probe into configuration and many of it’s logs may provide insight into matters of network credentialing and activity.

4.2) Network Structure



The above diagram depicts a probable network structure involved in the study. The abusive emails were discovered as coming from the public IP address 140.247.62.34. Further investigation found that the network's access point was linked to 192.168.1.254 and 192.168.1.64, suggesting important routing components in the network. The device 192.168.1.64 was discovered to mostly route DNS queries through 192.168.1.254, indicating a strong connectivity.

Furthermore, 192.168.1.106 was recognised as an internal gateway overseeing a subnetwork that comprised devices such as 192.168.15.2, 192.168.15.4, and 192.168.15.5. These machines showed substantial network activity, and subsequent forensic examination revealed that one of them was responsible for accessing willselfdestruct.com, the site used to deliver the abusive emails. The discoveries helped narrow down the investigation to a specific collection of devices by connecting network activity to the suspect.

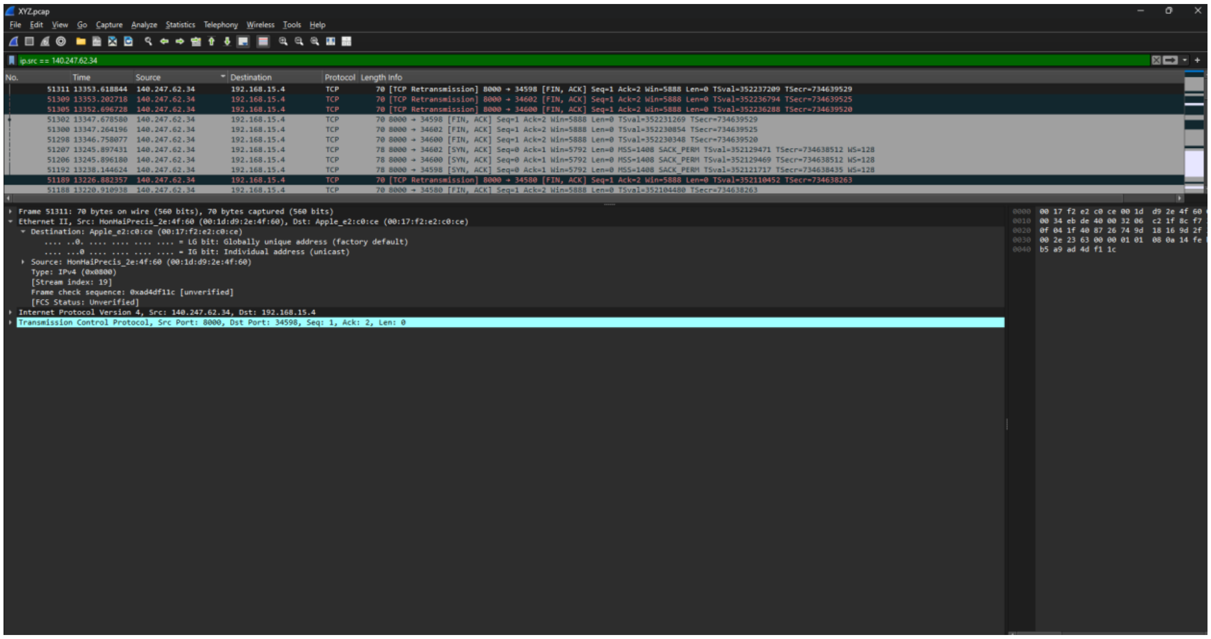
4.3) Activity Timeline

Packet Number	Activity	Destination	Inference
18818	Amazon.com	72.21.210.11	Accessing amazon.com
20016	Statcounter.com	66.114.48.49	Accessing statcounter
20138	Google-analytics.com	209.85.171.127	Accessing google analytics
20543	Cnn.com	64.236.91.21	Accessing cnn website
23941	Weather.com	65.212.121.21	Accessing weather.com
24408	Yahoo.com	209.131.36.158	Attacker went on to yahoo
26168	Lanehenderson.net	216.177.71.7	Accessing lanehenderson.net
26202	Google.com	74.125.19.104	Accessing google
26271	Youtube.com	208.65.153.251	Accessing youtube.com
31877	Seo.ucsc.edu	128.114.49.8	-
31954	Facebook.com	69.63.176.40	Accessing facebook.com
33415	Washingtonpost.com	12.129.147.65	Accessing Washingtonpost.com
33419	Wired.com	69.26.180.8	Accessing wired.com
33537	Jihadica.com	66.33.212.43	-
48140	Me.com	69.22.167.222	Accessing me.com
48476	Adiumx.com	64.128.80.61	-
49167	Apple.com	17.251.200.32	Accessing apple.com
52018	Hellosacramento.com	65.182.192.74	-
54016	Hibeamount.com	66.39.211.25	-
57203	Vmware.com	66.35.234.149	Accessing vmware website
64458	Forensicswiki.com	208.97.188.9	Researched for forensics
64776	Ebay.com	66.135.214.176	Accessing ebay website

72117	Microsoft.com	207.46.19.190	Accessing Microsoft website
72636	Annoy.com	66.166.239.194	Visits a malicious website
76046	Paypal.com	64.4.241.33	Attacker visits paypal
74920	Answers.yahoo.com	203.73.187.220	Visiting and getting answers for the question "Can I go to jail for harassing my teacher"
79780	Google Search - Send Anonymous Mail	74.125.19.104	Searching to send anonymous emails
80614	Sendanonymousemail.net	69.80.225.91	An email was sent to the victim by the attacker
82912	Willselfdestruct.com	69.25.94.22	Accessing willselfdestruct.com
83601	Willselfdestruct.com	69.25.94.22	Attacker sends another email to the victim via willselfdestruct.com

4.4) Background Evidence

Evidence 01


XYZ.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 140.247.62.34

```
No.     Time          Source          Destination    Protocol Length Info
  51311 13353.618844  140.247.62.34   192.168.15.4   TCP      70 [TCP Retransmission] 8000 → 34598 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352237209 TSecr=734639529
  51309 13353.202718  140.247.62.34   192.168.15.4   TCP      70 [TCP Retransmission] 8000 → 34602 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352236794 TSecr=734639525
  51305 13352.696728  140.247.62.34   192.168.15.4   TCP      70 [TCP Retransmission] 8000 → 34600 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352236288 TSecr=734639520
  51302 13347.678580  140.247.62.34   192.168.15.4   TCP      70 8000 → 34598 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352231269 TSecr=734639529
  51300 13347.264196  140.247.62.34   192.168.15.4   TCP      70 8000 → 34602 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352230854 TSecr=734639525
  51298 13346.758077  140.247.62.34   192.168.15.4   TCP      70 8000 → 34600 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352230348 TSecr=734639520
  51207 13245.897431  140.247.62.34   192.168.15.4   TCP      78 8000 → 34602 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=352129471 TSecr=734638512 WS=128
  51206 13245.896180  140.247.62.34   192.168.15.4   TCP      78 8000 → 34600 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=352129469 TSecr=734638512 WS=128
  51192 13238.144624  140.247.62.34   192.168.15.4   TCP      78 8000 → 34598 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=352121717 TSecr=734638435 WS=128
  51189 13226.882357  140.247.62.34   192.168.15.4   TCP      70 [TCP Retransmission] 8000 → 34580 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352110452 TSecr=734638263
  51188 13220.910938  140.247.62.34   192.168.15.4   TCP      70 8000 → 34580 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=352104480 TSecr=734638263
```

```
> Frame 51311: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
v Ethernet II, Src: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60), Dst: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
  v Destination: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
    Type: IPv4 (0x0800)
    [Stream index: 19]
    Frame check sequence: 0xad4df11c [unverified]
    [FCS Status: Unverified]
> Internet Protocol Version 4, Src: 140.247.62.34, Dst: 192.168.15.4
> Transmission Control Protocol, Src Port: 8000, Dst Port: 34598, Seq: 1, Ack: 2, Len: 0
```

```
0000  00 17 f2 e2 c0 ce 00 1d  d9 2e 4f 60
0010  00 34 eb de 40 00 32 06  c2 1f 8c f7
0020  0f 04 1f 40 87 26 74 9d  18 16 9d 2f
0030  00 2e 23 63 00 00 01 01  08 0a 14 fe
0040  b5 a9 ad 4d f1 1c
```

Description: First we searched for the IP of the dormitory room in the query search bar and then displayed our suspect's device (destination) and router (HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60).

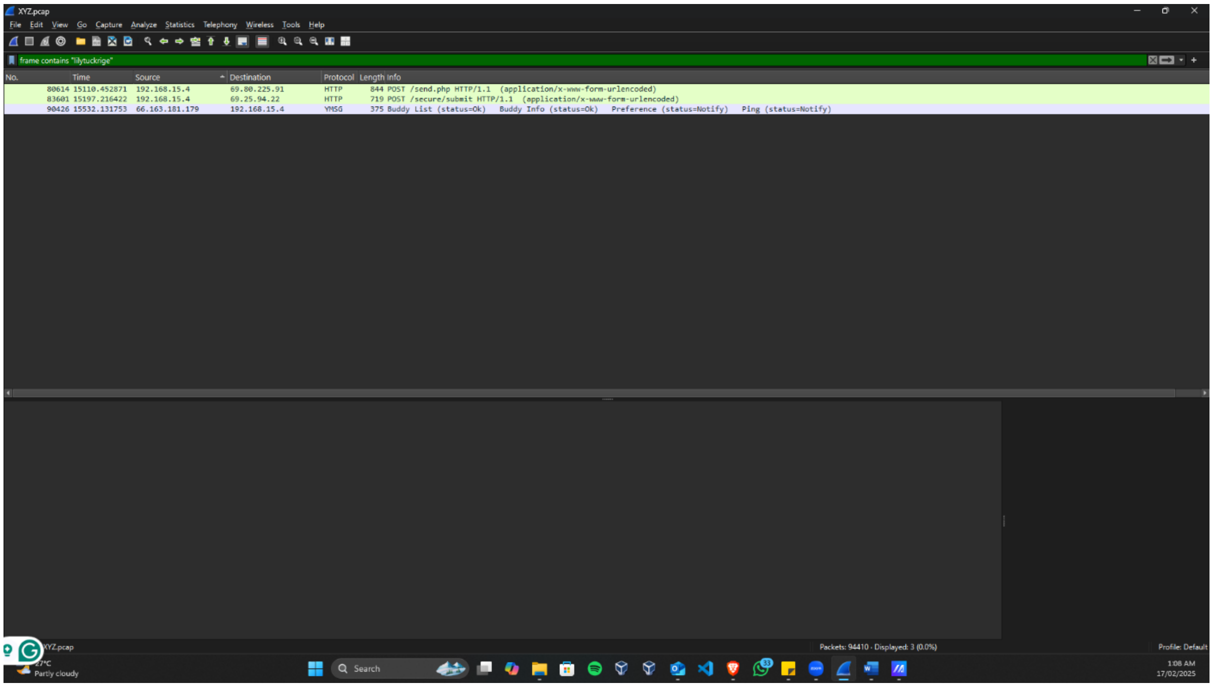
- Suspect's IP address: 192.168.15.4(destination)

- Suspect's device and MAC address: Apple_e2:c0:ce && 00:17:f2:e2:c0:ce

- Router Ip address: 140.247.62.34(dormitory room Ip address)

Also, he sent the harassing mail using the above router IP. It is a dormitory room Ip (140.247.63.34). The router is HonHaiPrecis_2e:4f:60. Destination/MAC address 192.168.15.4

Evidence 02:


XYZ.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame contains "lilytuckrige"

```
No.    Time          Source          Destination     Protocol Length Info
80614  15110.452871  192.168.15.4    69.80.225.91    HTTP     844 POST /send.php HTTP/1.1  (application/x-www-form-urlencoded)
83601  15197.216422  192.168.15.4    69.25.94.22     HTTP     719 POST /secure/submit HTTP/1.1  (application/x-www-form-urlencoded)
90426  15532.131753  66.163.181.179  192.168.15.4    YMSG     375 Buddy List (status=Ok)   Buddy Info (status=Ok)   Preference (status=Notify)   Ping (status=Notify)
```

Packets: 94410 · Displayed: 3 (0.0%)

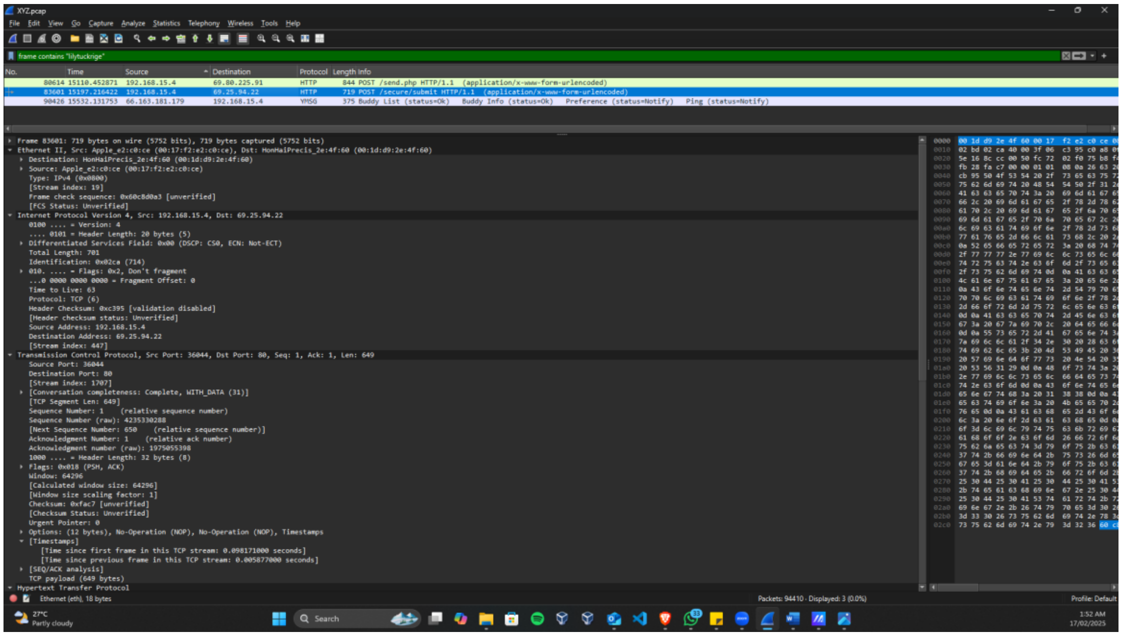
Profile: Default

We used a filter to search for packets contained in the string “lilytuckrige”.Its search query is “frame contains ‘lilytuckrige’”. Then we got 3 results. Also, we have 2 same IP source and one different data packet.

Also, when we analyze one of the packets in the same packet above I mentioned, It has a full request URI (http://www.willselfdestruct.com/secure/submit). Also, the same IP address has the same destination and the same source.

- Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
- Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)

Evidence 03:



XYZ.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame contains "lilytuckrige"

```
No.    Time            Source          Destination     Protocol Length Info
80614  15110.452871    192.168.15.4    69.80.225.91    HTTP     844 POST /send.php HTTP/1.1  (application/x-www-form-urlencoded)
83601  15197.216422    192.168.15.4    69.25.94.22     HTTP     719 POST /secure/submit HTTP/1.1  (application/x-www-form-urlencoded)
90426  15532.131753    66.163.181.179  192.168.15.4    YMSG     375 Buddy List (status=Ok)   Buddy Info (status=Ok)   Preference (status=Notify)   Ping (status=Notify)
```

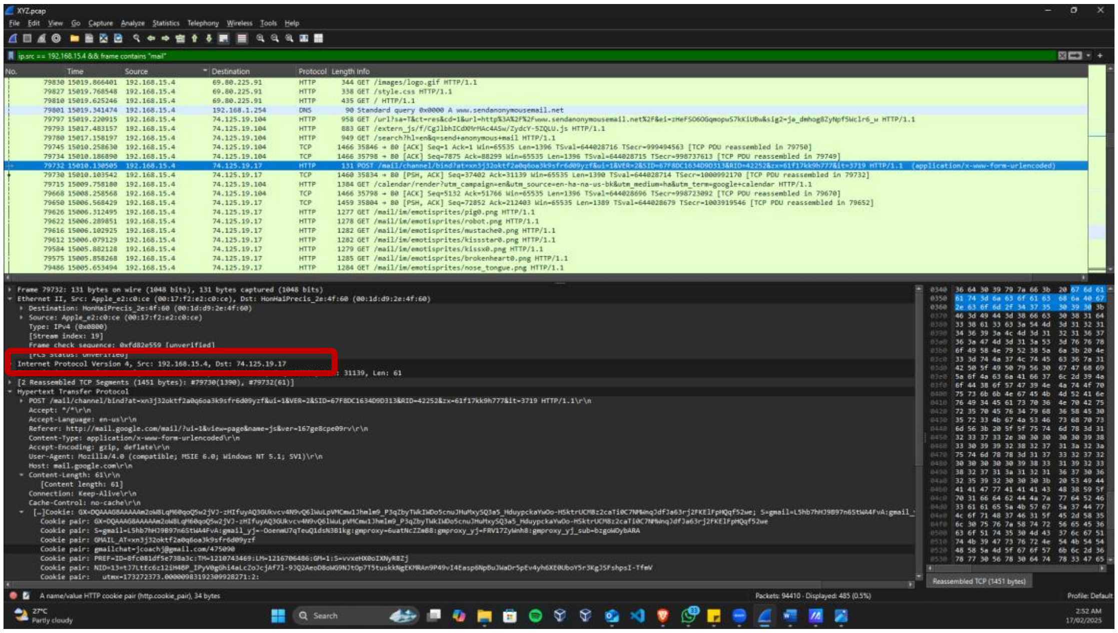
```
Frame 83601: 719 bytes on wire (5752 bits), 719 bytes captured (5752 bits)
Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
    Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
    Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
    Type: IPv4 (0x0800)
    [Stream index: 19]
    Frame check sequence: 0x60c8d0a3 [unverified]
    [FCS Status: Unverified]
Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.25.94.22
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 701
    Identification: 0x02ca (714)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: TCP (6)
    Header Checksum: 0xc395 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.15.4
    Destination Address: 69.25.94.22
    [Stream index: 447]
Transmission Control Protocol, Src Port: 36044, Dst Port: 80, Seq: 1, Ack: 1, Len: 649
    Source Port: 36044
    Destination Port: 80
    [Stream index: 1707]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 649]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4235330288
    [Next Sequence Number: 650    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1975055398
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 64296
    [Calculated window size: 64296]
    [Window size scaling factor: 1]
    Checksum: 0xfac7 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
        [Time since first frame in this TCP stream: 0.098171000 seconds]
        [Time since previous frame in this TCP stream: 0.005877000 seconds]
    [SEQ/ACK analysis]
    TCP payload (649 bytes)
Hypertext Transfer Protocol
```

```
0000  00 1d d9 2e 4f 60 00 17  f2 e2 c0 ce 00
0010  02 bd 02 ca 40 00 3f 06  c3 95 c0 a8
0020  5e 16 8c cc 00 50 fc 72  02 f0 75 b8
0030  fb 28 fa c7 00 00 01 01  08 0a 26 63
0040  cb 95 50 4f 53 54 20 2f  73 65 63 75
0050  75 62 6d 69 74 20 48 54  54 50 2f 31
0060  41 63 63 65 70 74 3a 20  69 6d 61 67
0070  66 2c 20 69 6d 61 67 65  2f 78 2d 78
0080  61 70 2c 20 69 6d 61 67  65 2f 6a 70
0090  69 6d 61 67 65 2f 70 6a  70 65 67 2c
00a0  6c 69 63 61 74 69 6f 6e  2f 78 2d 73
00b0  77 61 76 65 2d 66 6c 61  73 68 2c 20
00c0  0a 52 65 66 65 72 65 72  3a 20 68 74
00d0  2f 77 77 77 2e 77 69 6c  6c 73 65 6c
00e0  74 72 75 63 74 2e 63 6f  6d 2f 73 65
00f0  2f 73 75 62 6d 69 74 0d  0a 41 63 63
0100  4c 61 6e 67 75 61 67 65  3a 20 65 6e
0110  0a 43 6f 6e 74 65 6e 74  2d 54 79 70
0120  70 70 6c 69 63 61 74 69  6f 6e 2f 78
0130  2d 66 6f 72 6d 2d 75 72  6c 65 6e 63
0140  0d 0a 41 63 63 65 70 74  2d 45 6e 63
0150  67 3a 20 67 7a 69 70 2c  20 64 65 66
0160  0d 0a 55 73 65 72 2d 41  67 65 6e 74
0170  7a 69 6c 6c 61 2f 34 2e  30 20 28 63
0180  74 69 62 6c 65 3b 20 4d  53 49 45 20
0190  20 57 69 6e 64 6f 77 73  20 4e 54 20
01a0  20 53 56 31 29 0d 0a 48  6f 73 74 3a
01b0  2e 77 69 6c 6c 73 65 6c  66 64 65 73
01c0  74 2e 63 6f 6d 0d 0a 43  6f 6e 74 65
01d0  65 6e 67 74 68 3a 20 31  38 38 0d 0a
01e0  65 63 74 69 6f 6e 3a 20  4b 65 65 70
01f0  76 65 0d 0a 43 61 63 68  65 2d 43 6f
0200  6c 3a 20 6e 6f 2d 63 61  63 68 65 0d
0210  6f 3d 6c 69 6c 79 74 75  63 6b 72 69
0220  61 68 6f 6f 2e 63 6f 6d  26 66 72 6f
0230  75 62 6a 65 63 74 3d 79  6f 75 2b 63
0240  37 74 2b 66 69 6e 64 2b  75 73 26 6d
0250  67 65 3d 61 6e 64 2b 79  6f 75 2b 63
0260  37 74 2b 68 69 64 65 2b  66 72 6f 6d
0270  25 30 44 25 30 41 25 30  44 25 30 41
0280  2b 74 65 61 63 68 69 6e  67 2e 25 30
0290  25 30 44 25 30 41 53 74  61 72 74 2b
02a0  69 6e 67 2e 2b 26 74 79  70 65 3d 30
02b0  3d 33 30 26 73 75 62 6d  69 74 2e 78
02c0  73 75 62 6d 69 74 2e 79  3d 32 36 60
```

The screenshot above contains one of the most useful reports. It is the address of the website. So in our case, the URI is mentioned.

When we analyze that the URI is sent to one of the IP sources. It is 192.168.15.4. Then we can get the IP address of our suspect. Because the website URL is sent to our victim from that IP address.

Evidence 04


XYZ.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.src == 192.168.15.4 && frame contains "mail"

No.    Time          Source         Destination    Protocol Length Info
79830 15019.866401 192.168.15.4   69.80.225.91   HTTP   344 GET /images/logo.gif HTTP/1.1
79827 15019.768548 192.168.15.4   69.80.225.91   HTTP   338 GET /style.css HTTP/1.1
79810 15019.625246 192.168.15.4   69.80.225.91   HTTP   435 GET / HTTP/1.1
79801 15019.341474 192.168.15.4   192.168.1.254  DNS     90 Standard query 0x0000 A www.sendanonymousemail.net
79797 15019.220915 192.168.15.4   74.125.19.104  HTTP   958 GET /url?sa=T&ct=res&cd=1&url=http%3A%2F%2Fwww.sendanonymousemail.net%2F&ei=zHeFSO6OGqmopw57kKiUBw&sig2=ja_dmhog8ZyNpf5Wclr6_w HTTP/1.1
79793 15017.483157 192.168.15.4   74.125.19.104  HTTP   883 GET /extern_js/f/CgJlbhICdXMrMAc4ASw/ZydcY-5ZQLU.js HTTP/1.1
79780 15017.158197 192.168.15.4   74.125.19.104  HTTP   949 GET /search?hl=en&q=send+anonymous+mail HTTP/1.1
79745 15010.258630 192.168.15.4   74.125.19.104  TCP   1466 35846 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=1396 TSval=644028716 TSecr=999494563 [TCP PDU reassembled in 79750]
79734 15010.186890 192.168.15.4   74.125.19.104  TCP   1466 35798 → 80 [ACK] Seq=7875 Ack=88299 Win=65535 Len=1396 TSval=644028715 TSecr=998737613 [TCP PDU reassembled in 79749]
79732 15010.130505 192.168.15.4   74.125.19.17   HTTP   131 POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42252&zx=61f17kk9h777&it=3719 HTTP/1.1  (application/x-www-form-urlencoded)
79730 15010.103542 192.168.15.4   74.125.19.17   TCP   1460 35834 → 80 [PSH, ACK] Seq=37402 Ack=31139 Win=65535 Len=1390 TSval=644028714 TSecr=1000992170 [TCP PDU reassembled in 79732]
79715 15009.758180 192.168.15.4   74.125.19.104  HTTP  1384 GET /calendar/render?utm_campaign=en&utm_source=en-ha-na-us-bk&utm_medium=ha&utm_term=google+calendar HTTP/1.1
79668 15008.258568 192.168.15.4   74.125.19.104  TCP   1466 35798 → 80 [ACK] Seq=5132 Ack=51766 Win=65535 Len=1396 TSval=644028696 TSecr=998723092 [TCP PDU reassembled in 79670]
79650 15006.568429 192.168.15.4   74.125.19.17   TCP   1459 35804 → 80 [PSH, ACK] Seq=72852 Ack=212403 Win=65535 Len=1389 TSval=644028679 TSecr=1003919546 [TCP PDU reassembled in 79652]
79626 15006.312495 192.168.15.4   74.125.19.17   HTTP  1277 GET /mail/im/emotisprites/pig0.png HTTP/1.1
79622 15006.289851 192.168.15.4   74.125.19.17   HTTP  1278 GET /mail/im/emotisprites/robot.png HTTP/1.1
79616 15006.102925 192.168.15.4   74.125.19.17   HTTP  1282 GET /mail/im/emotisprites/mustache0.png HTTP/1.1
79612 15006.079129 192.168.15.4   74.125.19.17   HTTP  1282 GET /mail/im/emotisprites/kissstar0.png HTTP/1.1
79584 15005.882128 192.168.15.4   74.125.19.17   HTTP  1279 GET /mail/im/emotisprites/kissx0.png HTTP/1.1
79575 15005.858268 192.168.15.4   74.125.19.17   HTTP  1285 GET /mail/im/emotisprites/brokenheart0.png HTTP/1.1
79486 15005.653494 192.168.15.4   74.125.19.17   HTTP  1284 GET /mail/im/emotisprites/nose_tongue.png HTTP/1.1
```

```
> Frame 79732: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)
v 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)
  > Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
    Type: IPv4 (0x0800)
    [Stream index: 19]
    Frame check sequence: 0xfd82e559 [unverified]
    [FCS Status: Unverified]
> Internet Protocol Version 4, Src: 192.168.15.4, Dst: 74.125.19.17
                                                 : 31139, Len: 61
> [2 Reassembled TCP Segments (1451 bytes): #79730(1390), #79732(61)]
v Hypertext Transfer Protocol
  > POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42252&zx=61f17kk9h777&it=3719 HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Language: en-us\r\n
    Referer: http://mail.google.com/mail/?ui=1&view=page&name=js&ver=167ge8cpe09rv\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
    Host: mail.google.com\r\n
  v Content-Length: 61\r\n
      [Content length: 61]
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
  v [...]Cookie: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw1Jhmlm9_P3qZbyTWkIWDo5cnuJHuMxySQ3a5_HduypckaYwOo-HSktrUCM8z2caTi0C7NMWnqJdfJa63rj2FKElFpMQqf52we; S=gmail=L5hb7hHJ9B97n6StWA4FvA:gmail_
      Cookie pair: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw1Jhmlm9_P3qZbyTWkIWDo5cnuJHuMxySQ3a5_HduypckaYwOo-HSktrUCM8z2caTi0C7NMWnqJdfJa63rj2FKElFpMQqf52we
      Cookie pair: S=gmail=L5hb7hHJ9B97n6StWA4FvA:gmail_yj=-OoenmU7qTeuQ1dsN3B1kg:gmproxy=6uatNcZZmB8:gmproxy_yj=FRV17ZyWnh8:gmproxy_yj_sub=bzgoWOybARA
      Cookie pair: GMAIL_AT=xn3j32oktf2a0q6oa3k9sfr6d09yzf
      Cookie pair: gmailchat=jcoachj@gmail.com/475090
      Cookie pair: PREF=ID=8fc081df5e738a3c:TM=1210743469:LM=1216706486:GM=1:S=vvxeHX0oIXNyR8Zj
      Cookie pair: NID=13=tJ7LtEc6z12iM48P_IPyV0gGhi4aLcZoJcjAf7l-9JQ2AeoD8oW09NJtOp7T5tuskkNgEKMRAn9P49vI4Easp6NpBuJWaDr5pEv4yh6XE0UboY5r3KgJSfshpsI-TfmV
      Cookie pair:  utmx=173272373.00000983192309928271:2:
```

```
0340  36 64 30 39 79 7a 66 3b  20 67 6d 61
0350  61 74 3d 6a 63 6f 61 63  68 6a 40 67
0360  2e 63 6f 6d 2f 34 37 35  30 39 30 3b
0370  46 3d 49 44 3d 38 66 63  30 38 31 64
0380  33 38 61 33 63 3a 54 4d  3d 31 32 31
0390  34 36 39 3a 4c 4d 3d 31  32 31 36 37
03a0  36 3a 47 4d 3d 31 3a 53  3d 76 76 78
03b0  6f 49 58 4e 79 52 38 5a  6a 3b 20 4e
03c0  33 3d 74 4a 37 4c 74 45  63 36 7a 31
03d0  42 50 5f 49 50 79 56 30  67 47 68 69
03e0  5a 6f 4a 63 6a 41 66 37  6c 2d 39 4a
03f0  6f 44 38 6f 57 47 39 4e  4a 74 4f 70
0400  75 73 6b 6b 4e 67 45 4b  4d 52 41 6e
0410  76 49 34 45 61 73 70 36  4e 70 42 75
0420  72 35 70 45 76 34 79 68  36 58 45 30
0430  35 72 33 4b 67 4a 53 46  73 68 70 73
0440  6d 56 3b 20 5f 5f 75 74  6d 78 3d 31
0450  32 33 37 33 2e 30 30 30  30 30 39 38
0460  33 30 39 39 32 38 32 37  31 3a 32 3a
0470  75 74 6d 78 78 3d 31 37  33 32 37 32
0480  30 30 30 30 30 39 38 33  31 39 32 33
0490  38 32 37 31 3a 31 32 31  36 37 30 36
04a0  32 35 39 32 30 30 30 3b  20 53 49 44
04b0  41 41 47 77 41 41 41 43  48 38 59 5f
04c0  70 31 66 64 62 44 4a 7a  77 64 52 46
04d0  33 61 61 65 5a 4b 57 67  5a 37 44 77
04e0  4c 6f 71 48 37 46 31 5f  45 2d 58 35
04f0  6c 30 75 76 7a 58 74 72  56 65 45 36
0500  63 6f 51 74 35 30 4d 43  37 6c 67 51
0510  74 4b 39 47 73 76 72 4e  54 4b 54 54
0520  48 58 5a 4d 5f 67 6f 57  6b 6c 2d 36
0530  78 77 30 56 78 30 64 74  78 33 47 65
```

Reassembled TCP (1451 bytes)
A name/value HTTP cookie pair (http.cookie_pair), 34 bytes
Packets: 94410 · Displayed: 485 (0.5%)
Profile: Default
27°C
Partly cloudy
Search
2:52 AM
17/02/2025

Currently, we have identified the IP address, MAC address, and device of the suspects. The website was used to send emails to harass our victims.
We then search in our search bar by declaring the IP source to our suspected IP address and including the keyword 'mail'. This is useful for identifying email-related traffic.

Search query: Ip.src == 192.168.15.4 && frame contains "mail".
So we were able to solve our main problem. That was the Gmail address of our suspect. We can easily find it in the screenshot above.

5. Supporting Evidence Presented

Evidence Identifier	Content	Content Source	Filename	MD5 HASH SUM
1	List of Ethernet endpoints	Wireshark ver4.4.2	Ethernetendpoints.yml	4a4914f8cc2be6f02af88208bc435aee
2	List of Ethernet	Wireshark ver4.4.2	EthernetConversations.yml	c0974788abbdbabdf7fb8ecfad8a8c6d

	Conversations			
3	List of IPv4 Endpoints	Wireshark ver4.4.2	IPV4Endpoints.yml	d1802f44de260f5c32d09ae4fe4f07fa
4	List of IPv4 Conversations	Wireshark ver4.4.2	IPv4Conversations.yml	6f94f9f1174fa17bd19eb57071007fd8
5	List of TCP Endpoints	Wireshark ver4.4.2	TCPEndpoints.yml	0ee0abac3f2a68a8b04a10d62a874446
6	List of TCP Conversations	Wireshark ver4.4.2	TCPConversations.yml	ccf9006eaa3e8f60b2ed6439931bb920
7	List of UDP Endpoints	Wireshark ver4.4.2	UDPEndpoints.yml	041f7c9cc044d5f0a3e975c630d2293c
8	List of UDP Conversations	Wireshark ver4.4.2	UDPConversations.yml	2cfa9d0a5912e96cafd86b2eb9400bd0
9	‘strings’ on Linux	Wireshark ver4.4.2	Stringsoutput.txt	b63184379f9c9ee4bd2cecdd83d8bb2b
10	Packet content of all HTTP requests from the suspect	Wireshark ver4.4.2	httpPacketsFrom192.168.15.4.txt	310690f0fcdef7fa379751351baee4c7
11	Packet content of all HTTP responses to the suspect	Wireshark ver4.4.2	httpPacketsTo192.168.15.4.txt	79e9561e765bc3c053a2cd28d166f613
12	Packet content of all YMSG (Yahoo Messenger Protocol) requests	Wireshark ver4.4.2	ymsgPacketsFrom192.168.15.4.txt	16769bcaa757baf427225bb8ee110ddd

	from the suspect			
13	Packet content of all YMSG (Yahoo Messenger Protocol) responses to the suspect	Wireshark ver4.4.2	ymsgPacketsTo192.168.15.4.txt	334546166520999cb20d1caf226d6824

6. Conclusion

The forensic investigation of Professor Lily Tuckrige's harassing emails effectively linked the communications back to a specific dormitory IP address (140.247.62.34). The suspect used an unprotected Wi-Fi connection and anonymous email services, making identification difficult. Investigators were able to correlate the activity to an Apple device with MAC address 00:17:f2:e2:c0:ce by combining packet capture analysis, MAC address tracking, and cross-referencing network activity with Chemistry 109 student data.

Despite the suspect's attempts to stay anonymous, evidence from Wireshark, email headers, and network logs revealed that the emails were sent from willselfdestruct.com and sendanonymousmail.net. The forensic approach followed best standards for digital evidence management, assuring data integrity and accuracy.

While the facts clearly point to the involvement of a specific individual, more administrative and judicial measures are required before a final determination can be made. Additional measures, such as device forensics or direct interrogation, may be necessary to complete the attribution. This analysis reveals the efficiency of network forensic tools in detecting cyber-related wrongdoing and emphasises the significance of protecting institutional networks from unauthorised access.

7. Self - Review

7.1 Sanithu Methnuka (s8170551)

Throughout this report, I contributed extensively to various sections, focusing on the investigative methodologies and forensic analysis techniques.

I was responsible for writing the **"Introduction"**, where I defined the investigation's scope and objectives, ensuring clarity on how the network forensic approach would be used to identify the suspect. Additionally, I detailed the **"2.2 Network Components Identified"**, outlining the relevant MAC addresses, IP addresses, and network devices involved in the case.

My role extended to the **"3.4 Handling Data"** section, where I analyzed network packet data, applying filters to identify suspicious activities. I also worked on **"4.2 Network Structure"** and **"4.3 Activity Timeline"**, creating a structured representation of network communications, pinpointing critical timestamps, and mapping the suspect's activity.

Furthermore, I contributed to **"5. Supporting Evidence Presented"**, documenting screenshots and forensic traces from Wireshark. My efforts were also instrumental in the **"6. Conclusions"** section, where I helped compile findings and ensured the forensic investigation followed proper digital evidence handling procedures.

After completing the report, I conducted a **final review**, cross-checking findings with the data collected to ensure accuracy and coherence. Any inconsistencies were addressed, and necessary revisions were made to maintain the quality and integrity of the report.

Overall, my contributions account for **50% of the report**, with a focus on detailed forensic analysis and ensuring a structured presentation of findings.

7.2 Laseya Wimalasiri (s8170583)

During the preparation of this report, I contributed significantly to several key sections, ensuring a structured and comprehensive forensic investigation.

My primary contributions include writing the **"Executive Summary"**, where I outlined the key aspects of the investigation, summarizing the methods used to track the source of the harassing emails. Additionally, I worked on **"2.1 Network Capture File Details"**, detailing essential technical parameters of the PCAP file extracted using Wireshark.

In the **"3.1 Tools Used"** and **"3.2 Steps Involved"** sections, I documented the forensic tools employed, such as Wireshark, nslookup, and email header analysis tools, along with the methodology for analyzing the network capture. My role was also crucial in **"3.3 Handling Data"**, where I described how the captured packets were filtered and analyzed to extract relevant forensic evidence.

Furthermore, I actively contributed to **"4.4 Background Evidence"**, identifying key timestamps, MAC addresses, and network requests linking the suspect's activity to the harassment emails. I also assisted in **"5. Supporting Evidence Presented"**, ensuring the proper documentation of evidence, generating hash values for forensic integrity, and maintaining the report's authenticity.

Finally, I played a role in structuring **"6. Conclusions"**, where I compiled the investigative findings and summarized how the suspect (Johnny Coach) was identified through network forensic techniques.

Overall, I estimate my contribution to be **50% of the report**, ensuring a systematic and well-documented forensic analysis.