Network Forensic Report

PCAP Network Packet Capture Analysis

Sanithu Methnuka - s8170551

Laseya Wimalasiri - s8170583

Table of Contents

[1. Executive Summary 2](#_Toc190794246)

[2. Introduction 3](#_Toc190794249)

[3. Methodology 9](#_Toc190794253)

[4. Detailed Findings 12](#_Toc190794277)

[5. Supporting Evidence Presented 19](#_Toc190794280)

[6. Conclusion 21](#_Toc190794281)

[7. Self - Review 21](#_Toc190794282)

[7.1 Sanithu Methnuka (s8170551) 21](#_Toc190794283)

[7.2 Laseya Wimalasiri (s8170583) 22](#_Toc190794284)

# 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:

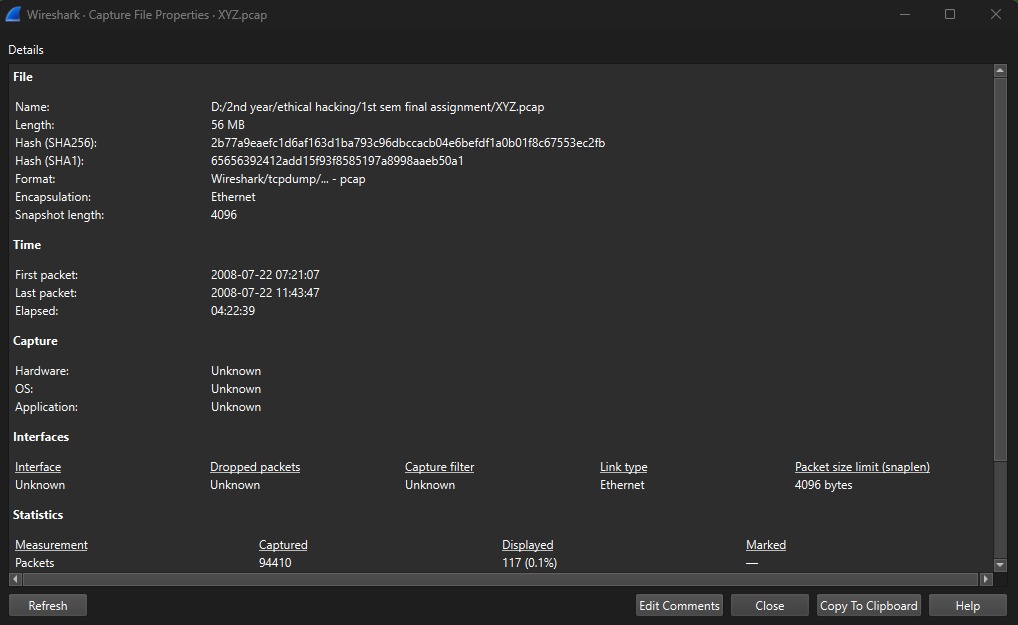
* 9981827f11968773ff815e39f5458ec8

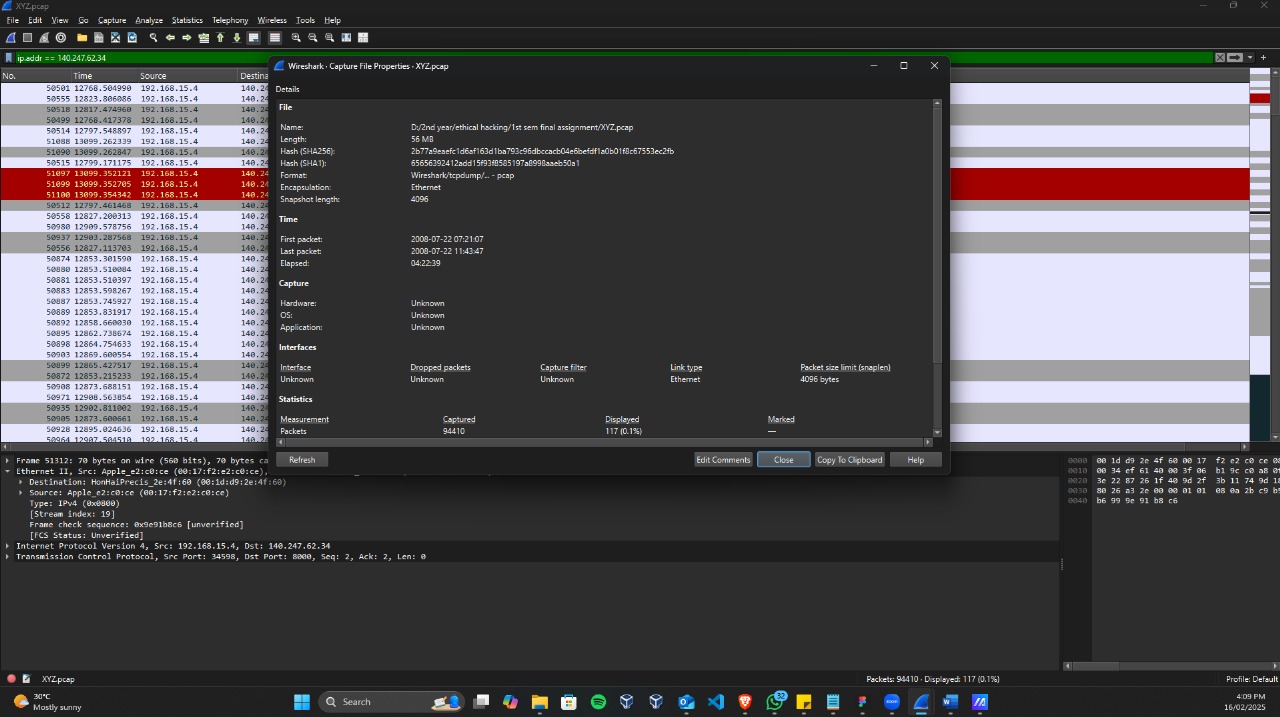
SHA1:

* 65656392412add15f93f8585197a8998aaeb50a1

SHA256 :

* 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb
* Packet capture summary from Wireshark Version 4.4.2





**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

1. 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](mailto: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.

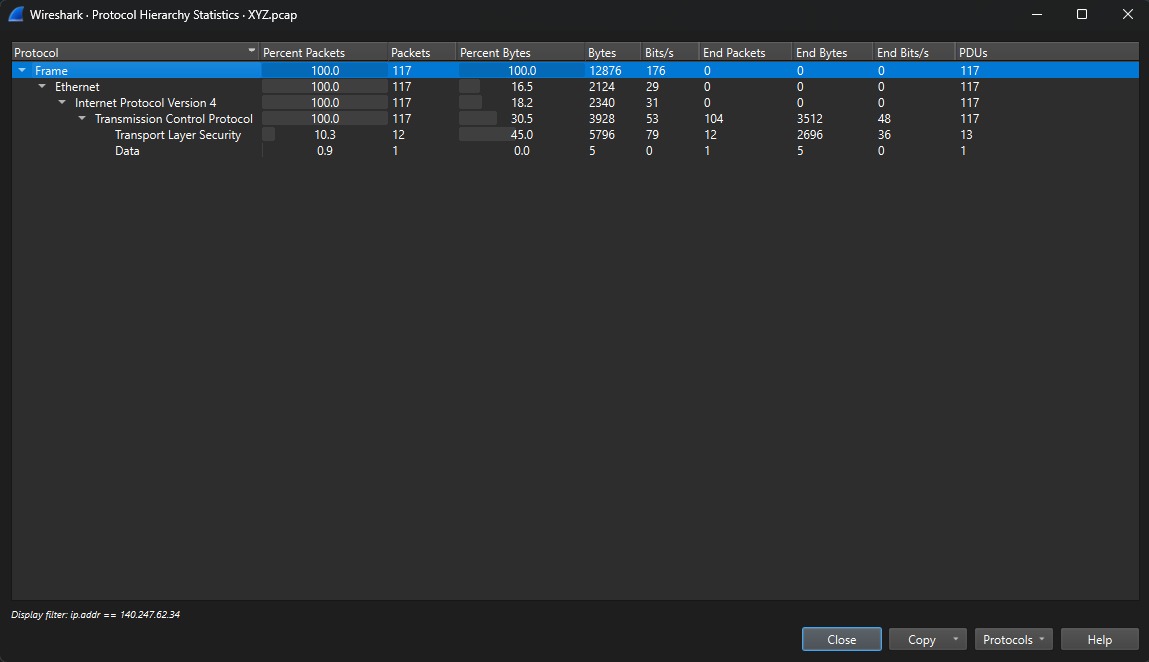
**Step 4: Cross-Referencing with Chemistry 109 Student Records**

* 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**

****

### 

### ****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

1. 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

192.168.1.254

Yahoo

Internet

192.168.1.64

192.168.15.7

192.168.15.5

192.168.15.4

willselfdestruct.com

Google

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 |

* 1. Background Evidence

Evidence 01A computer screen shot of a computer

AI-generated content may be incorrect.

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:

A screenshot of a computer

AI-generated content may be incorrect.

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:

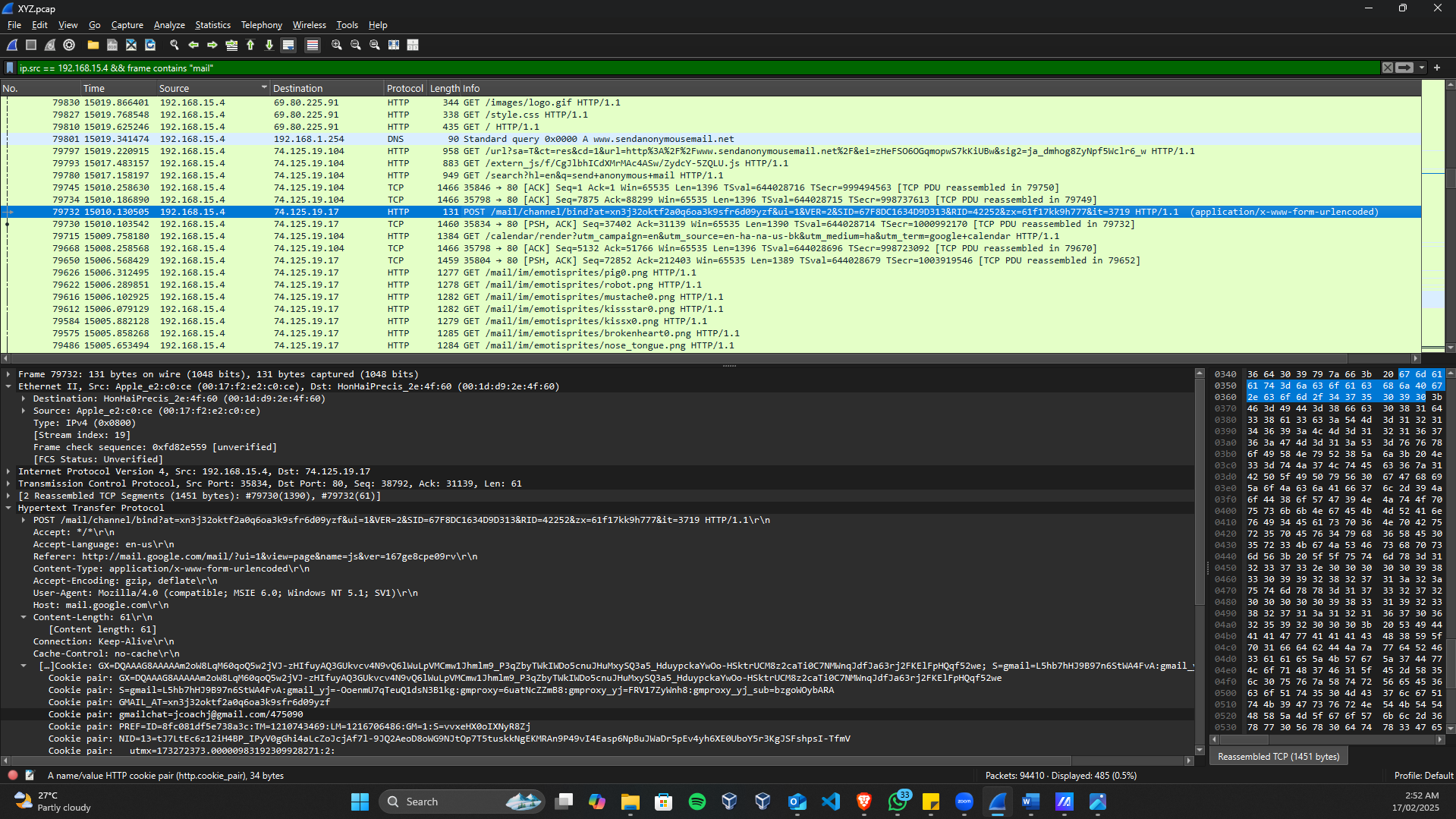
A screenshot of a computer

AI-generated content may be incorrect.

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



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 Conversations | Wireshark ver4.4.2 | EthernetConversations.yml | c0974788abbdbabdf7fb8ecfad8a8c6d | | 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 from the suspect | Wireshark ver4.4.2 | ymsgPacketsFrom192.168.15.4.txt | 16769bcaa757baf427225bb8ee110ddd | | 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.