Network Forensic Report

PCAP Network Packet Capture Analysis

**Last compiled by**

Kavindu Chamodya Nimshan (8145532)

&

Kaveen Sandaru Horst Cohn (8145710)

**On the date 2/16/2025**

**Table of Contents**

[1. Executive Summary 3](#_Toc45006)

[2. Introduction 4](#_Toc45007)

[2.1 Network Capture File details 4](#_Toc45008)

[2.2 Network Components Identified 5](#_Toc45009)

[3. Methodology 7](#_Toc45010)

[3.1 Tools Used 7](#_Toc45011)

[3.2 Steps Involved 8](#_Toc45012)

[3.3 Handling Data 17](#_Toc45013)

[4. Detailed Findings 19](#_Toc45014)

[4.1 Important network players 19](#_Toc45015)

[4.2 Network Structure 20](#_Toc45016)

[4.3 Activity Timeline for 192.168.15.4 20](#_Toc45017)

[4.4 Background evidence 21](#_Toc45018)

[5. Supporting Evidence Presented 23](#_Toc45019)

[6. Conclusions](#_Toc45020) 33

[7. Self-Review Section 33](#_Toc45020)

# Executive Summary

This report is of forensic analysis of network capture file of the “XYZ School Harassment Scenario." Network packets were sampled that covered four-hour or more capture session that represented timeline of malicious activity. With extremely minute analysis using software of Wireshark, Hashing software, Mac address lookup software, and other command-line software, timeline of activities were reconstructed and critical network communications isolated

The most important findings of this report are that,

* The network capture file of “XYZ.pcap” contains well over 94,000 packets taken within session of 4 hour 22 minutes.
* A public IP of 140.247.62.34 had been traced to connect to inner, private IP of 192.168.15.4 through means of network address translation.
* Packet detailing examinations identified that an Apple-based system, identified by its unique MAC of 00:17:f2:e2:c0:ce, had sent out emails of harassment.
* Facility of filtering of Wireshark identified malicious email packets and HTTP activity. For one example, HTTP cookie content accidentally leaked out of the email of jcoach@gmail.com.
* Identification of background context of (class roster) cross-checked led to discovery that it is that “Johnny Coach.”
* The evidence is on levels of network protocols of Ethernet, IP, TCP, UDP and application layer protocols, ensuring that each component of suspect activity is preserved and reprovable.

# Introduction

XYZ School’s IT department started investigating after Professor Lily Tuckrige of Department of Chemistry reported receiving harassing emails. She had believed that one of her students of Chemistry 109 had sent her emails.

The emails were sent to her private Yahoo email address (lilytuckrige@yahoo.com). When the IT group checked the email header, it found that emails were sent through IP address 140.247.62.34, tracing to a room of one of its students residing in the dormitory.

The school never provided rooms with Wi-Fi, but one of its students had installed his or her private Wi-Fi router. The router had no password protection, meaning that whoever happened to be within its range had free reign to tap into it and use the same IP address. It made it very hard to trace who sent out emails.

## Network Capture File details

As there had been continuing harassment, the IT security group started monitoring the network of the dormitory. It utilized a packet sniffer on the Ethernet port of the dormitory to closely track what people were sending what content. It allowed them to scan through what happened on the network and establish who actually sent out emails. They stored that important details and information as a PCAP file.

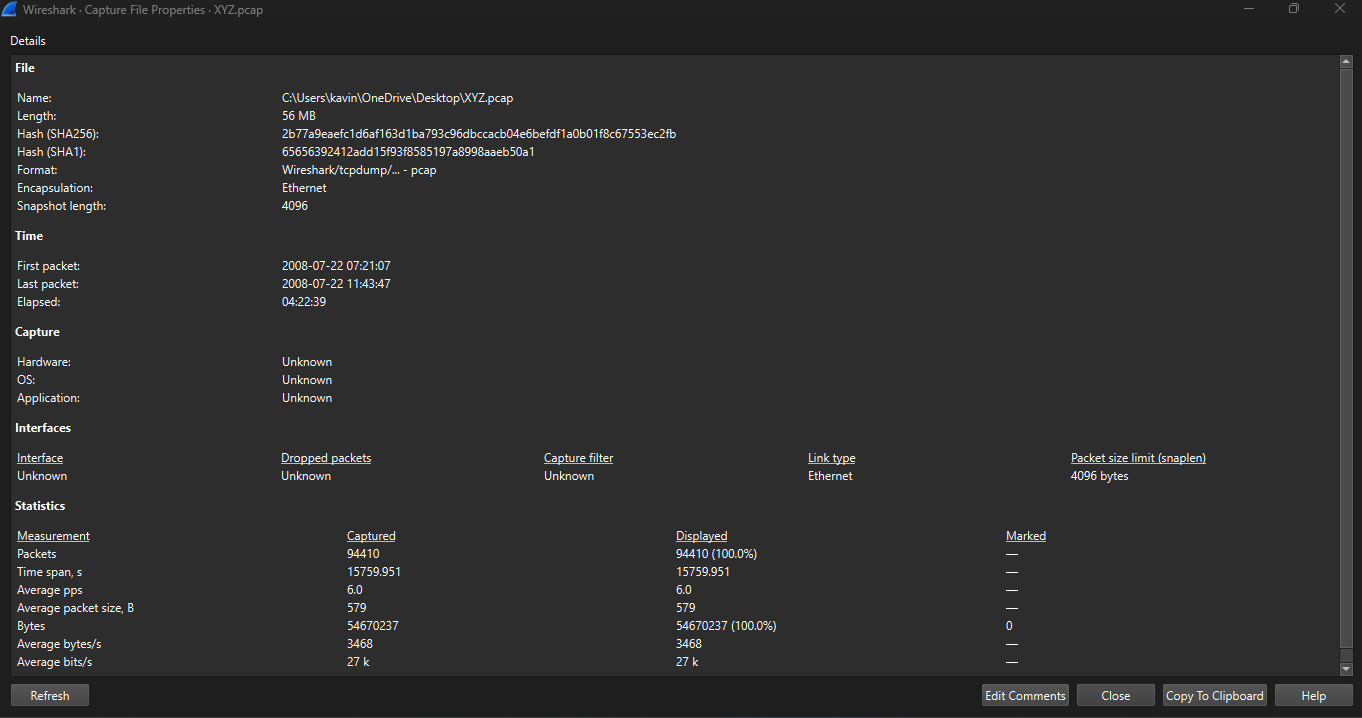
The extracted PCAP network capture file (XYZ.pcap) has the forensic parameters as given below. The evidence for these details is provided from Wireshark:

|  |  |
| --- | --- |
| Capture length: | 56 MB/ 58,720,256 bytes |
| Format: | Wireshark/tcpdump/... - pcap |
| Packet size limit: | 4096 bytes |
| First packet: | 2008-07-22 07:21:07 |
| Last packet: | 2008-07-22 11:43:47 |
| Elapsed time: | 4 hours, 22 minutes, 39 seconds |
| Total packets: | 94410 |
| Average pps: | 6.0 |
| Average packet size: | 579 |
| Average bytes/s: | 3468 |
|  |  |

The primary data source for our investigation is the network capture file, XYZ.pcap. The capture file was verified using the following hash values:

* **MD5:** 9981827f11968773ff815e39f5458ec8
* **SHA1:** 65656392412add15f93f8585197a8998aaeb50a1
* **SHA256:** 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb

This pcap file contains all packets logged from the Ethernet tap placed in the suspect dorm room’s Ethernet connection on Monday 7/21. The file includes timestamped packet captures that show network activity related to the harassing emails.

[Evidence 01]

## Network Components Identified

1. Public IP Address (140.247.62.34) – External Gateway.

This public IP is the main connection point for XYZ school’s internal network to access the Internet. It plays a major role through NAT, directing requests from the outside world to the right internal devices such as computers and servers. However, only a tiny amount of data (just 0.06%) was directly sent or received by this IP address, meaning its main job is to pass along data from the university’s internal network to the outside world, rather than handling much of the actual communication itself.

1. Private IP Address (192.168.15.4) – Suspect’s Device

This private IP address is assigned to a device inside XYZ school’s internal network. Through analysing SMTP (email) and HTTP (web) traffic, it was discovered that this IP address was the source of the hostile emails. The NAT mapping process also showed that this device was responsible for sending out both email and web traffic. In addition to that, it was responsible for confirming its role in the suspicious activity.

1. Suspect’s Device – Apple MacBook

The device with the MAC address 00:17:f2:e2:c0:ce was identified as an Apple device using Wireshark’s MAC vendor lookup. This device was found to be responsible for sending the harassing emails and accessing anonymous email services. Further investigation of the PCAP file revealed an HTTP cookie, which directly connected this device to the email address jcoach@gmail.com, providing a clear link to the suspicious activity.

1. Router/NAT Gateway (Handling Internal-External Communication)

This device connects XYZ school’s internal network (which uses IP addresses in the 192.168.x.x range) to the public Internet. It acts as both a firewall and a packet router. And there is no doubt that, it helps to protect the network by blocking unauthorized access while also providing anonymity by hiding the real IP addresses of internal devices. To investigate the suspicious activity, the forensic team looked at the NAT tables to figure out how the suspect’s private IP (192.168.15.4) was linked to the public IP (140.247.62.34), revealing the relationship between the internal device and the external communication.

1. Email and HTTP Communication Services

The investigation involved analysing SMTP traffic, which revealed the harassing emails, the sender’s information, and the email headers. One of the HTTP packets also leaked an HTTP cookie, which exposed the attacker’s email address, jcoach@gmail.com, allowing the team to directly identify the person behind the attacks. To hide their identity, the attacker tried using anonymous email services, like SendAnonymousEmail.net and WillSelfDestruct.com, making it harder to trace the emails back to them.

# Methodology

This section highlighted the forensic tools used, sequence of actions taken throughout investigation process, evidence handling and preserving techniques to maintain its forensic integrity.

## Tools Used

1. Email Header Analysis

The analysis of the email header targeted on deriving useful information out of the harassing emails that were sent to Lily Tuckrige’s Yahoo Mail account. The investigators analyzed the email headers that contained useful metadata like the original IP address, server logs of emails, and timestamp. It traced where emails were sent and originated, forming an important part of identification of the sender.

1. Hashing & Integrity Verification Tools

Hashing tools of SHA-256, MD5 and SHA-1 play a major role to maintain forensic data integrity during the analytical process of investigation. Investigators generated unique values of hash on the XYZ.pcap file to make sure that seized network data were never altered throughout the analytical process. By checking pre- and post-investigative values of hash, investigators were guaranteed that the data were original and never touched or altered.

1. Wireshark (Version: 3.6.8, OS: Windows)

.

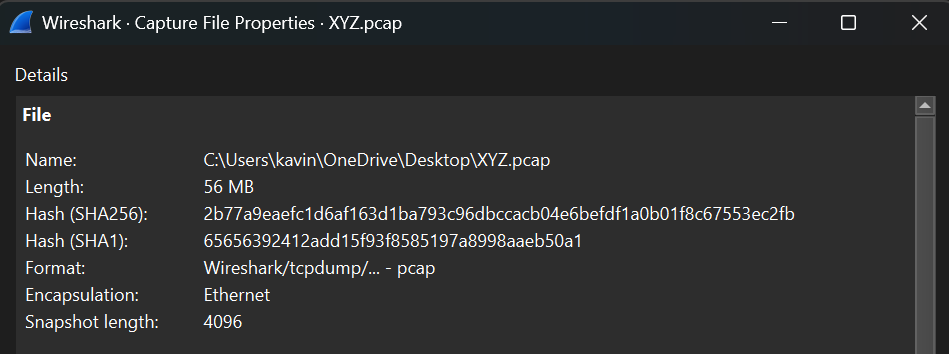
The main software utilized to carry out the inquiry was Wireshark that analyzed the network capture file that is referred to as (XYZ.pcap). Investigators used to use filters that allowed them to focus on unique IP addresses, email activity and HTTP conversations. By the way they use filters for tracing suspect activity without much difficulty. By tracing unique network packets, investigators investigated SMTP (email activity), HTTP requests, and relationships of NAT, tracing finally where emails were coming that were harassing others.

1. Mac Address Analysis (by using maclookup.app Website)

used the maclookup.app website to identify the manufacturer and type of device linked to specific MAC addresses found in the network traffic. By cross-referencing the captured MAC addresses, there is no doubt that they were able to determine what kind of device was involved in the attack by the way helping to further pinpoint the suspect.

## Steps Involved

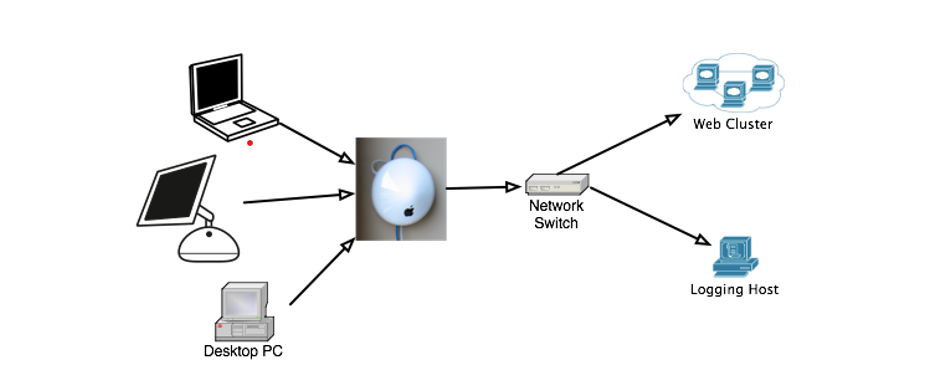
Step 1



[Evidence 01(Zoom-in)]

As we expected before, we can see that the SHA1 and SHA256 hash signatures match with the ones given in the scenario. We also see that the elapsed time of the capture was about 4 hours and 22 minutes. This is quite long, and explains the quantity of packets received in this network capture 94 410 lines. No chance to read through each packet line by line. Because of that we use Wireshark’s filters to narrow down any search made in the capture.

Step 2

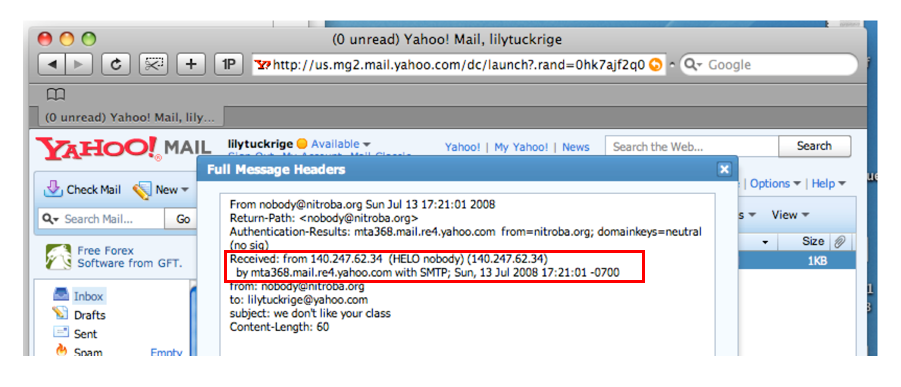


[Evidence 02]

This is how it looks like when map the dorm room network.

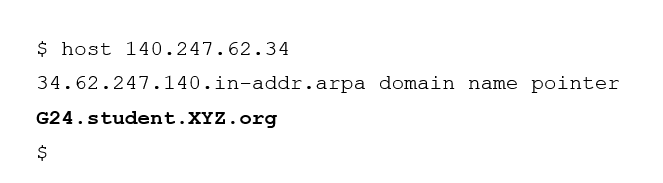
Step 3

The IP was found in the email header



[Evidence 03]

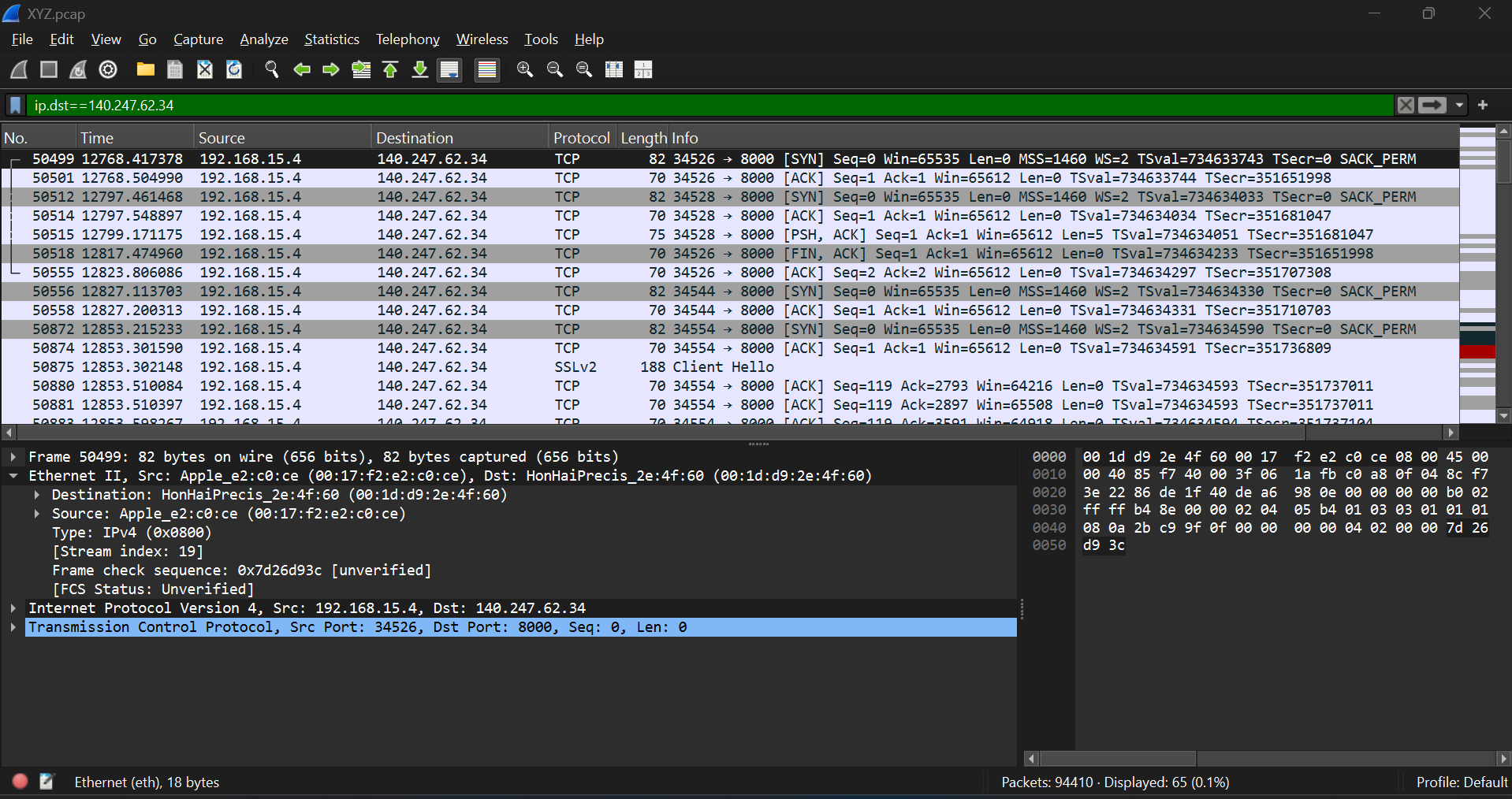
And that IP address points to a XYZ school dorm room.

****

[Evidence 03.1]

Step 4

So, let’s filter the PCAP file using **ip.dst==140.247.62.34,** and then we find that this IP has a low presence in the Wireshark statistics : 0.1% of the total sent packets (equal 65 packets)

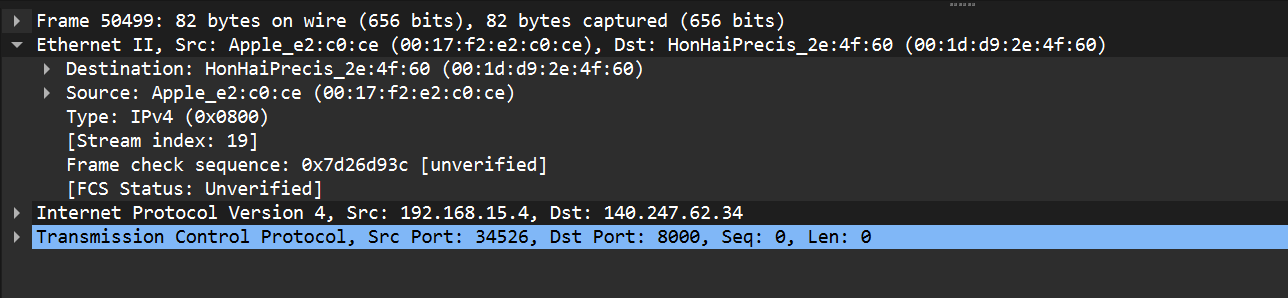


[Evidence 04]

Now, look closer at the IP adresses source and destination. Here above a screenshot of the first packets. We can see that the 192.168.15.4 plays a central role as it is the only IP bridging with our IP 140.247.62.34. This type of IP is well known as a private IP address

Step 5

Let’s have a look in the OSI layer n°2 of a packet capture between these two IP addresses192.168.15.4(source) and 140.247.62.34 (destination). We find interesting information about the hardware and MAC address of the two physical devices pointed by these IP



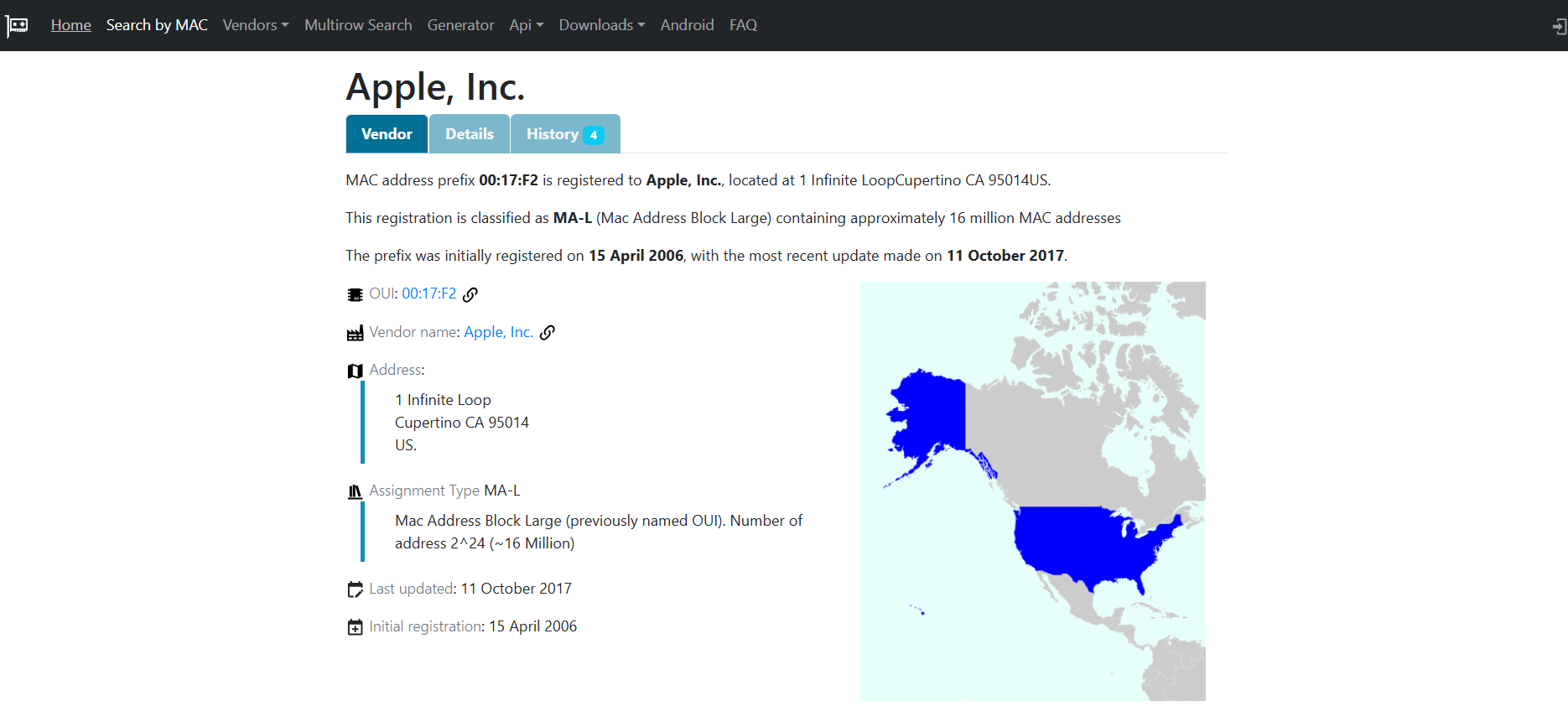
[Evidence 05]

So, the information reads as follows

|  |  |  |
| --- | --- | --- |
| **IP** | **MAC** | **Hardware** |
| 192.168.15.4 (source) | 00:17:f2:e2:c0:ce | Apple |
| 140.247.62.34 (destination) | 00:1f:d9:2e:4f:60 | HonHaiPrecis |

Step 6

Google check with the MAC 00:17:f2:e2:c0:ce confirms this is an Apple device by using maclookup.app website.



[Evidence 06]

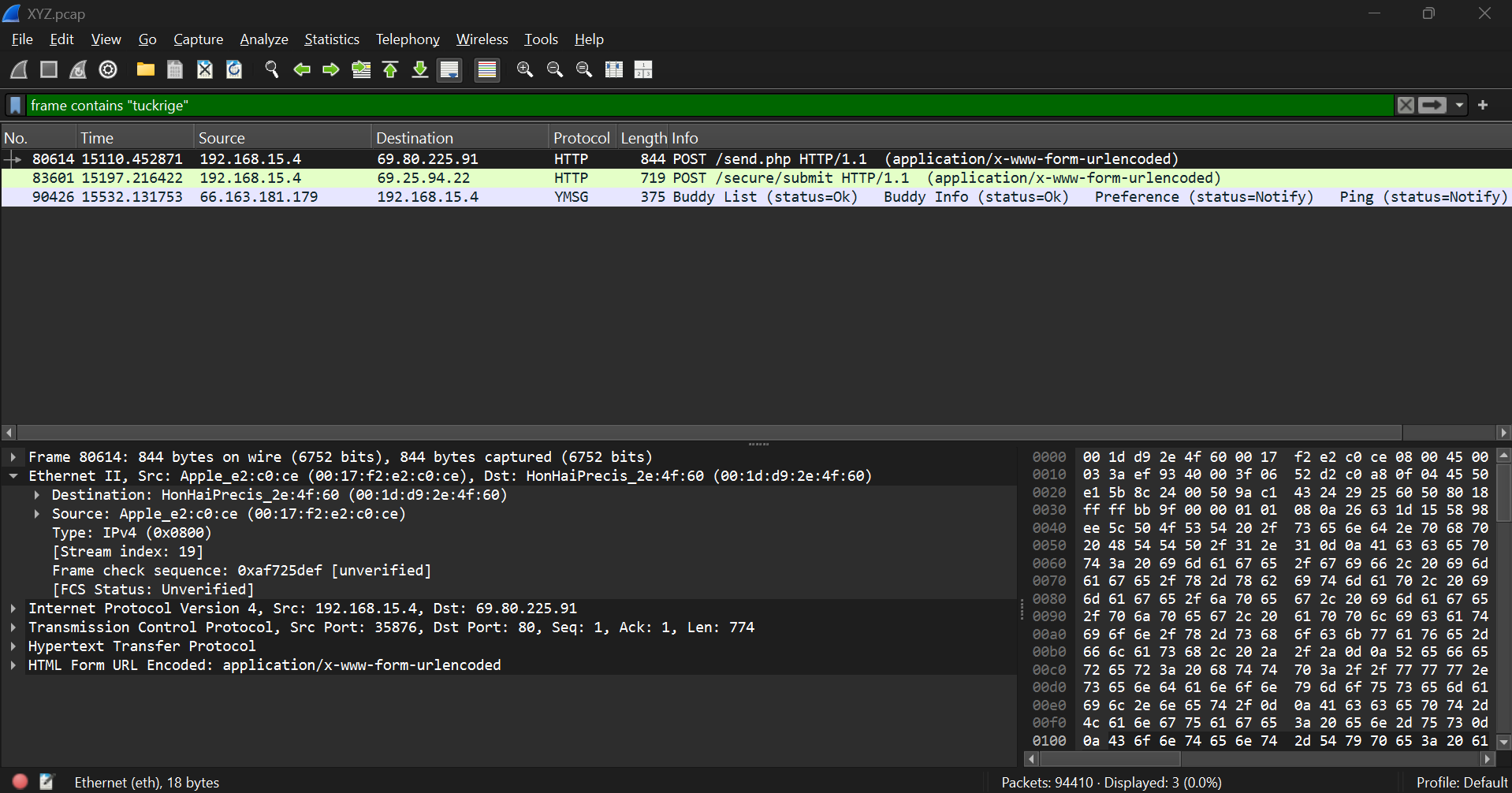
What is HonHaiPreciis? Google search reveals it’s Hon Hai Precision Industry Co Ltd, also known as the electronics giant Foxconn.

Step 7

This is how find who sent email to lilytuckrige@yahoo.com and identify the TCP connections that include the hostile message.

Let’s use again the filter capabilities of Wireshark: **frame contains “tuckrige”**

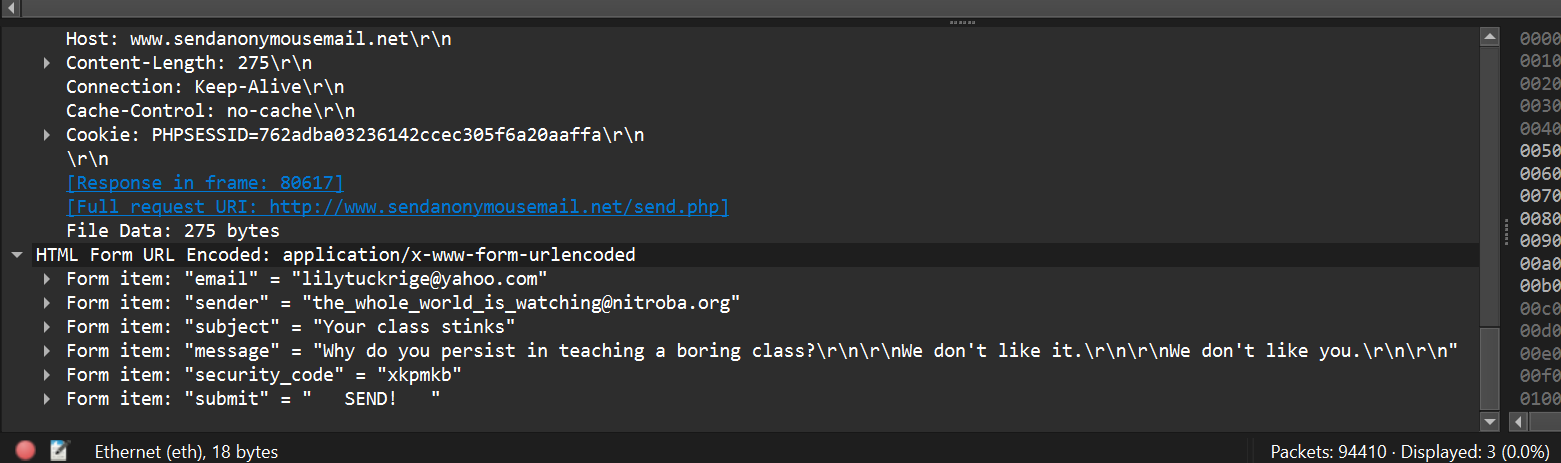
We find three packets. The first two of them are using the OSI model layer n°7, that is the application layer, represented by the HTTP protocol. The last one is using the OSI model layer n°4, in this case the TCP protocol



[Evidence 07]

Step 8

After analysing those three specific packets, the packet n°80614 shows a harassing message was sent using sendanonymousemail.net with the exact details as described in the PowerPoint “We don’t like you”. (The source IP is 192.168.15.4, and the destination IP is 69.80.225.91)

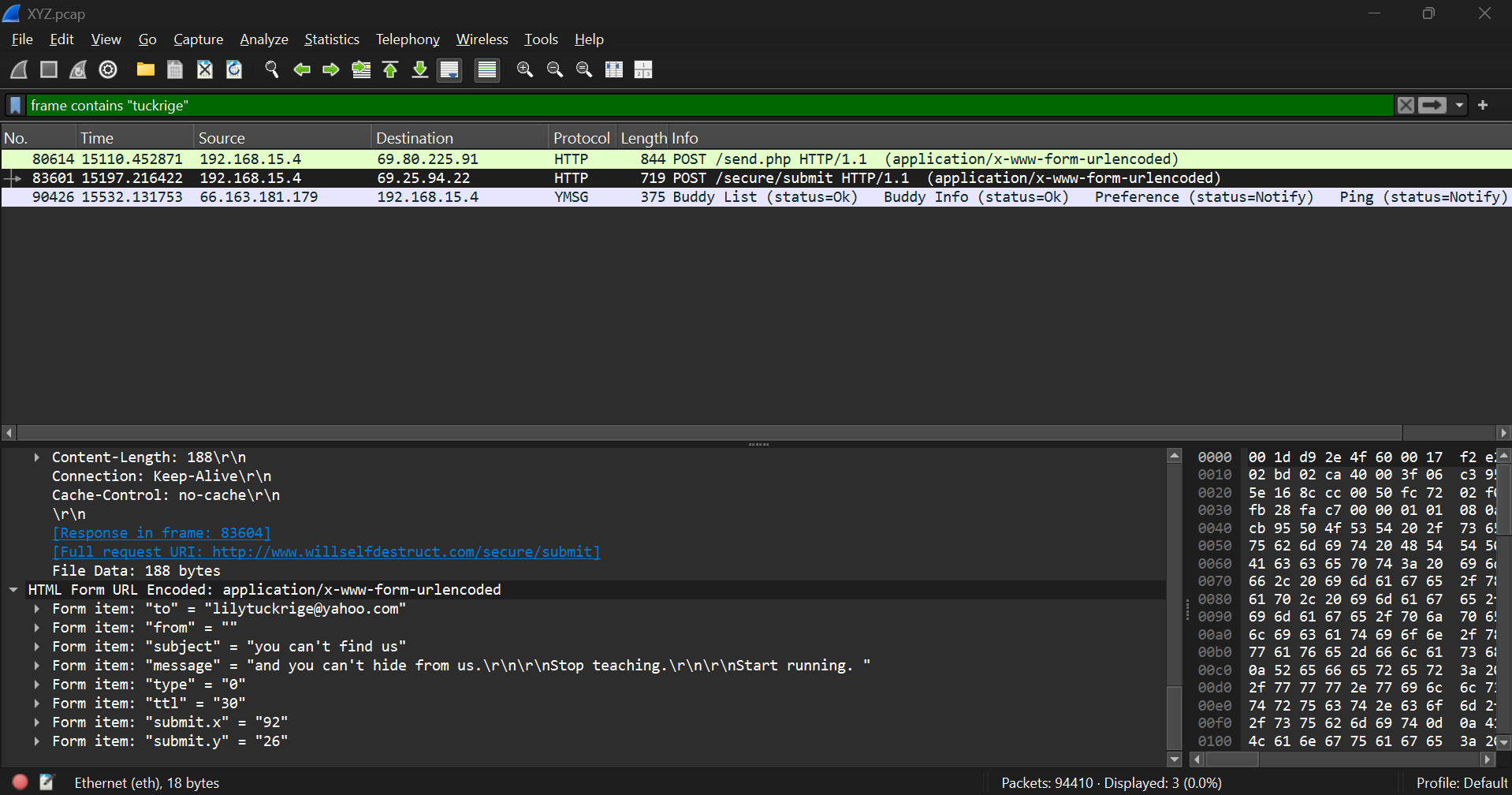


[Evidence 08]

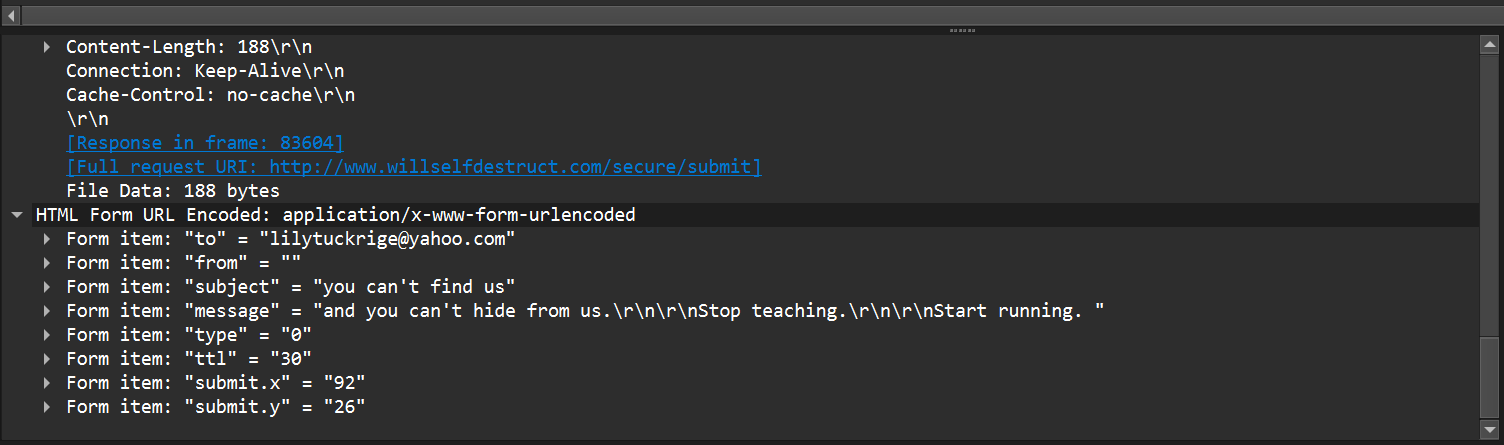
sendanonymousemail.net is an internet service that makes it possible for people to write anonymous emails without disclosing identification, generally used for anonymity or confidentiality but also possibly maliciously.

Step 9

The packet n°83601 shows a harassing message was sent using Willselfdestruct.com, with the exact email header as described in the Powerpoint “you can’t find us”



[Evidence 09]



[Evidence 10]

The source IP is 192.168.15.4, and the destination IP is 69.25.94.22

At this point of the article, we can confirm that the IP 192.168.15.4 plays a central role in the email “attacks” and the harassment faced by the professor Lily Tuckrige.

Above can be seen very important key information.

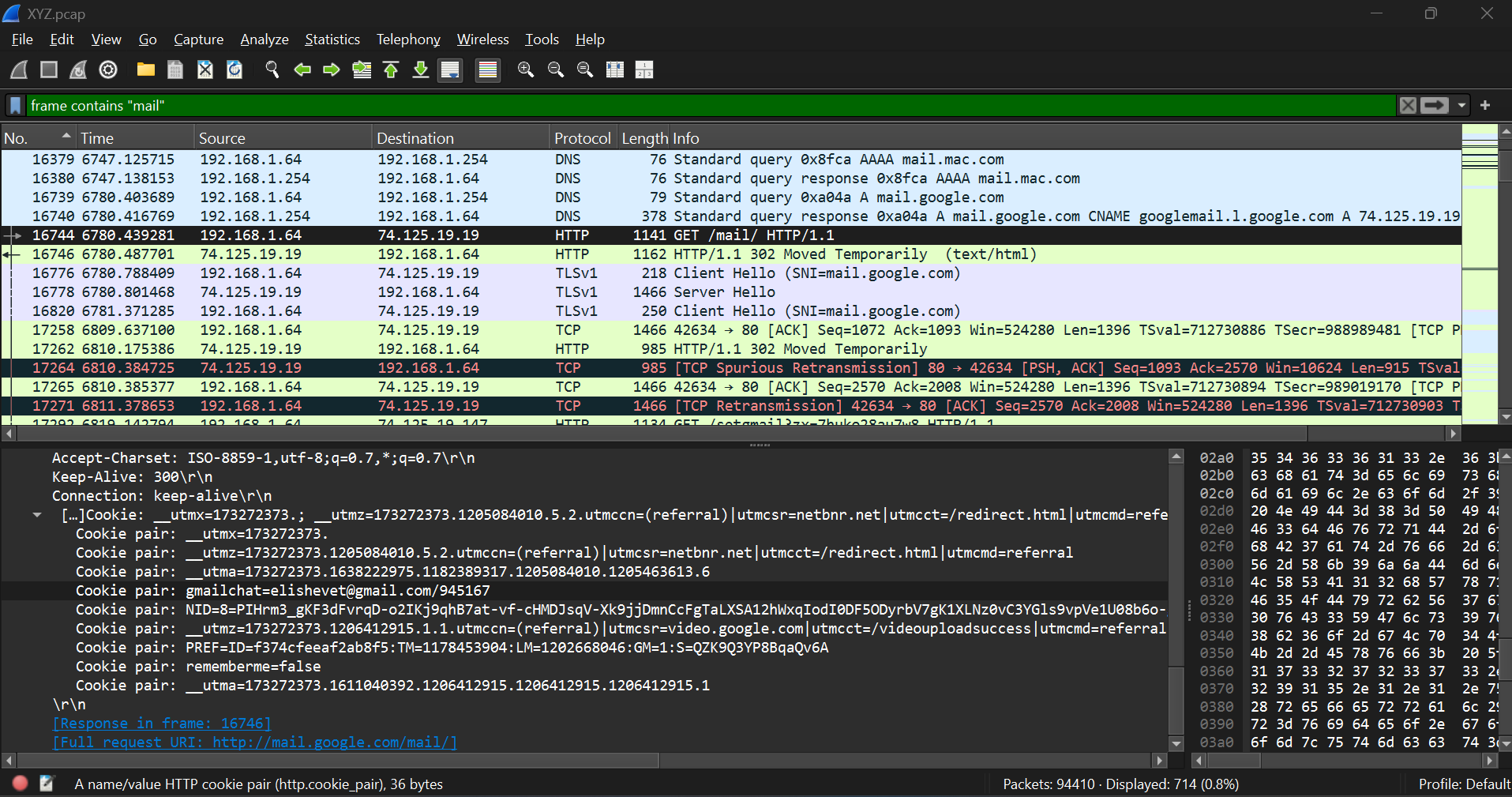
|  |  |  |
| --- | --- | --- |
| **IP** | **MAC** | **Hardware** |
| 192.168.15.4 (source) | 00:17:f2:e2:c0:ce | Apple |

This IP / MAC is going to be essential to solve the case!

Step 10

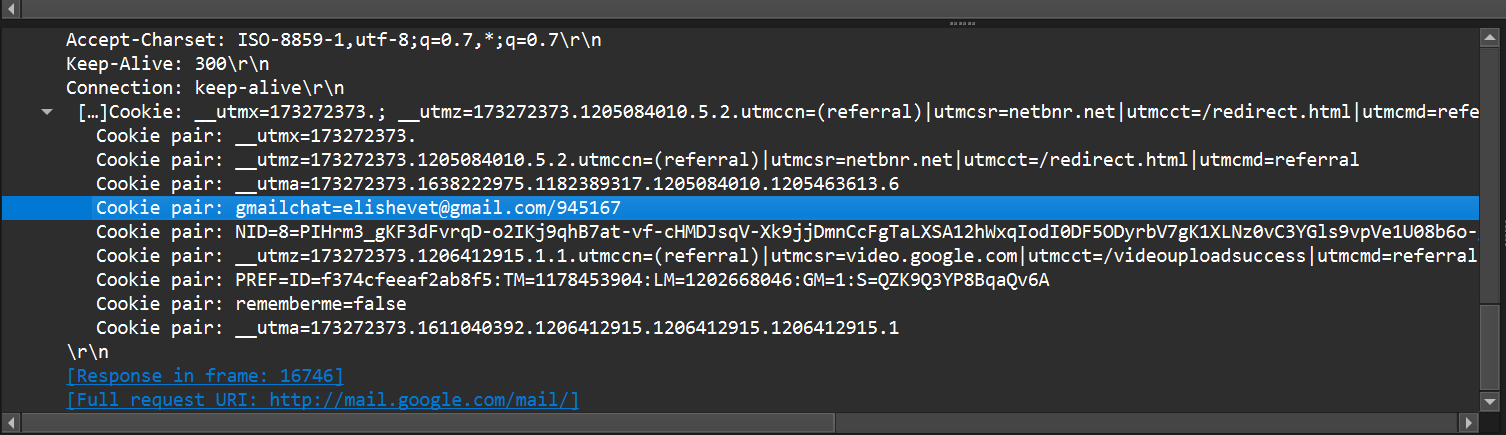
After then focus on finding information in one of those TCP connections that identifies the attacker. So now that we have an interesting IP / MAC pair, that may lead to the identification of the attacker, what could we do next? As the next step we’ve decided to have a look further in the packets. Could we find maybe, the email address of the attacker? And, how to check that?

we’ve just filtered in Wireshark typing **frame contains “mail”.** This is a little bit “quick and dirty” but could help to narrow down the research. Then I went scrolling into the selected frames and found some frames titled “GET /mail/ HTTP/1.1 with some interesting content. This could indicate a request for a web-based email service, a mail-related API, or a page within a web application related to mail. When focus on the cookie, they reveal some email addresses and the link to the email platform used.



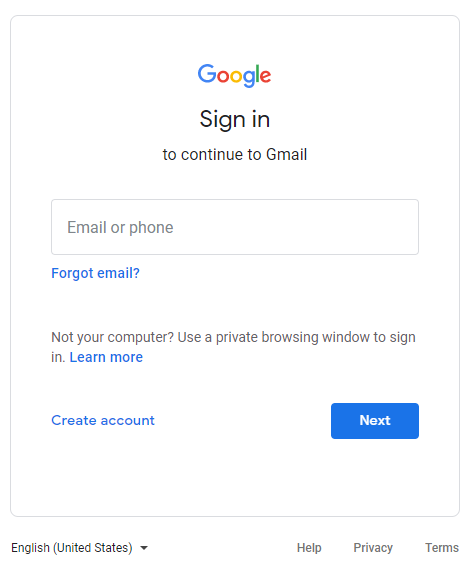
[Evidence 11]

In the example below, we see the frame n°16744, showing a GET /mail/ HTTP/1.1, the MAC address in layer 2 of the OSI model, and some cookie information in below;

**

[Evidence 12]

Of course, the http addresses points to the Gmail sign in page. When the person is signing in, Gmail downloads the cookie for authentication needs.



[Evidence 13]

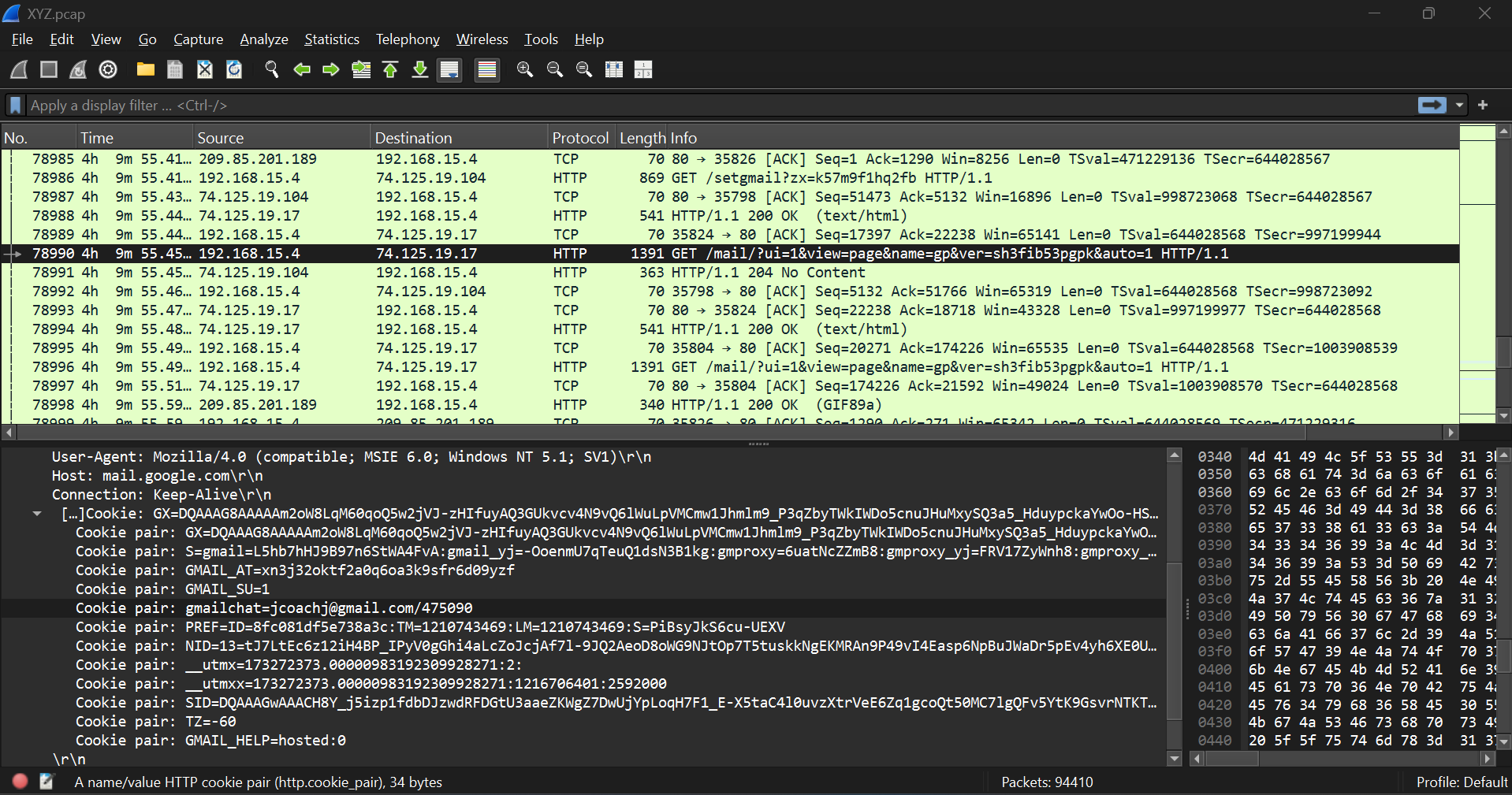
It’s quite amazing to find this level of information in clear text, furthermore in Wireshark

Step 11

Now that we have found a way to identify the email address of the attacker, let’s go through the different frames including the GET /mail/ HTTP/1.1 info, because the attacker have to request for a web-based email service, a mail-related API or a page within a web application related to mail in order to send mails. And let’s check the email, IP, MAC data. Probably, we will find a match with the already suspicious IP/MAC pair? Here below the result of my analysis in a table, the match is easily found and highlighted in red

|  |  |  |  |
| --- | --- | --- | --- |
| Frame | E-mail | IP | MAC |
| 16744 | elishevet@gmail.com | 192.168.1.64 | 00:1d:d9:2e:4f:61 |
| 78990 | jcoach@gmail.com | 192.168.15.4 | 00:17:f2:e2:c0:ce |

The attacker email is [jcoach@gmail.com](mailto:jcoach@gmail.com)

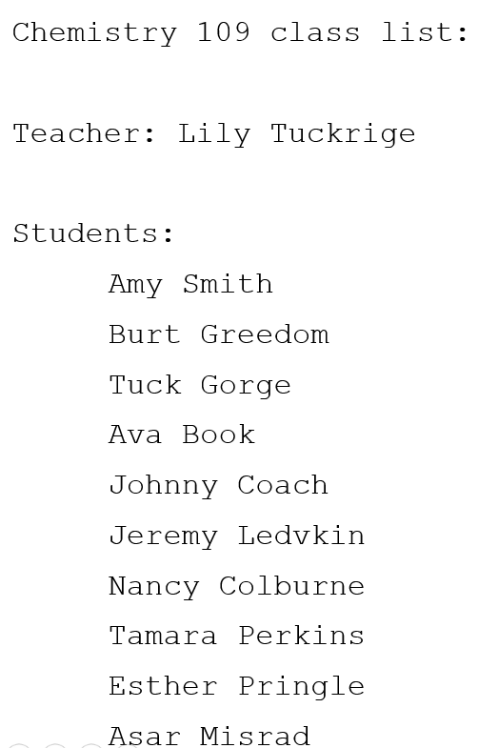


[Evidence 14]

Step 12

So, who did it?

Now, we can come to a conclusion, since we have a potential name “jcoach”. Let’s compare with the list of alumni in Lily Tuckrige classroom.

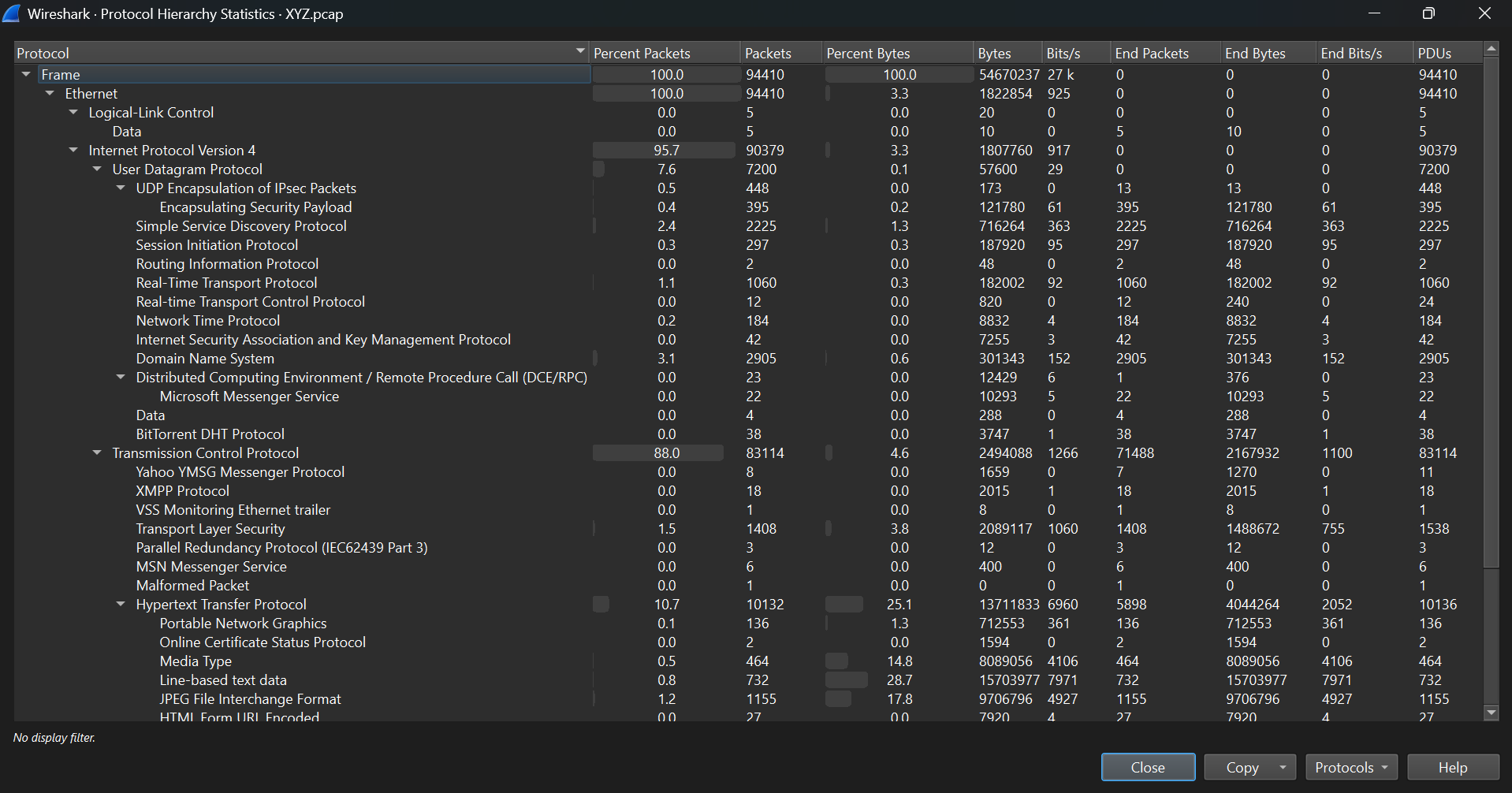


[Evidence 15]

* **There is no doubt that, we have a match with Johnny Coach**

## Handling Data

Below image represent the protocol Hierarchy Statics of XYZ.pcap file in Wireshark.



[Evidence 16]

By the way, when we focus about handling data the below table give some information related to handle various data that we’ve found and handled with,

| **Step** | **Action Taken** | **Purpose** |
| --- | --- | --- |
| Write-Protected Storage | Stored PCAP file and logs on write-blocked forensic disks | Prevent modification of original data |
| Secure Access Controls | Used encryption (AES-256) and multi-factor authentication (MFA) | Restrict unauthorized access |
| Hash Verification | Performed SHA1, SHA256, and MD5 checksums at every step | Ensure evidence integrity |
| Chain of Custody | Maintained detailed access logs and transfer records | Track every action taken on evidence |

With furthermore, below is how we were able to keep the data secure and safe.

Capturing the Data

To make sure that everything had been captured accurately:

* We captured everything that had occurred on the network and saved it on a PCAP file (XYZ.pcap) without changing.
* We logged important facts like timestamp, packet count, and sources/destinations right after capturing to follow up on what had been captured.
* We copied that can be accessed once again if need arises.

Making sure the data stays the same

* To make sure that no one had manipulated the data, we utilized use of hash values (MD5, SHA-1, SHA-256).
* The hashes are fingerprints, when even minute modification is added on the file, the hash will have changed.
* We recalculated the hash values whenever we analysed the data to make sure that it compared to the original.

By doing that, we were able to make sure that the data had remained intact and reliable by law.

Keeping It Secure

Since this case involved sensitive data, we had to make sure that the data had been safe from unauthorized people accessing it.

* We preserved everything. Wireshark logs, screen shots, and extracted facts within safe, authority-controlled environment where only people permitted by authority were allowed to view.
* We had screen shots on every important move to leave trace of what had been done, making sure that we had clear documentation of what had been done.

Being Privacy-Sensitive and Following Guidelines

Since this case involved students' data, we followed very rigid rules of law and ethics:

* We were confidentiality-oriented by keeping everything private.
* We followed rules of XYZ School’s IT to make sure that everything had been done accordingly.
* Only authorized school administrators and investigators were allowed evidence access.

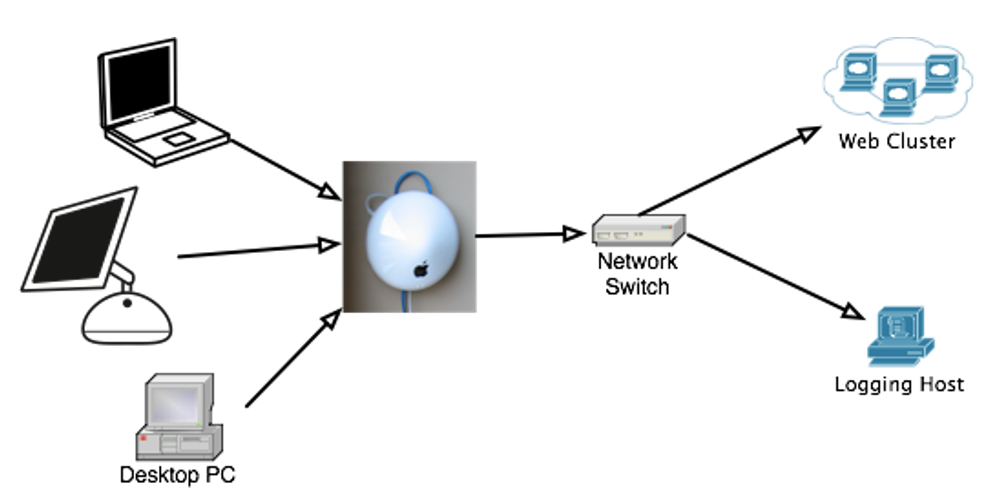
# Detailed Findings

## Important network players

|  |  |  |  |
| --- | --- | --- | --- |
| **Network Players** | **MAC Address** | **IP Address** | **Major role and other details** |
| Apple Device  (Suspect Device) | 00:17:f2:e2:c0:ce | 192.168.15.4 | -Device identified in hostile emails.  - Linked to the public interface 140.247.62.34 via NAT. |
| Router/NAT Gateway  (Dorm Room Router) | 00:1d:d9:2e:4f:60 | 140.247.62.34 | -Facilitates network translation and routes suspect device traffic to the Internet. |
| sendanonymousemail.net |  | 69.80.225.91 | -Send email without revealing identity or real IP address. |
| Willselfdestruct.com |  | 69.25.94.22 | -Send self-deleting messages, making it harder to trace. |
| DNS Server |  |  | -Use XYZ School’s  - Help to resolve domain names of email services and anonymous platforms, And help to trace communications in network. |
| Yahoo Mail Server |  |  | -has Lily Tuckrige’s email account.  -contains the harassing emails sent to Lily Tuckrige. |
| Cookie Data |  |  | -One particularly revealing HTTP request included a cookie field that exposed the email “jcoach@gmail.com.” |

.

## Network Structure



[Evidence 02]

The suspect's device (192.168.15.4) also accesses the internet from the gateway/router of the dorm room (140.247.62.34) and logs into Yahoo Mail and anonymous email. The DNS queries target the computer searching for Yahoo Mail and email, linking them with harassment.

## Activity Timeline for 192.168.15.4

The below timeline demonstrates deliberate actions taken by the suspect to send harassing emails. In Wireshark previously the default option for time column changes into Seconds since first capture packets.

| **Timestamp**  **(Seconds since first capture packet)** | **Frame**  **No.** | **Activity** | **Destination IP** | **Analysis** |
| --- | --- | --- | --- | --- |
| 4h 9min 55.451768s | 78990 | HTTP POST Request | 74.125.19.17 | Request for mail.google.com (Gmail service)  The attacker attempted to access Gmail, either for sending or checking emails. |
| 4h 11m 50.452871s | 80614 | HTTP POST Request | 69.80.225.91 | Sending an email via sendanonymousmail.net  The user may be trying to send an email anonymously by using sendanonymousmail.net |
| 4h 13m 17.216422s | 83601 | HTTP POST Request | 69.25.94.22 | Sending an email via willselfdestruct.com  The user sent another email, this time using a service by using willselfdestruct.com, that ensures messages are deleted after being read. |

## Background evidence

**Incident Overview**

| **Category** | **Details** |
| --- | --- |
| **Date of Incident** | First hostile email received at 17:21:01 on 13 Jul 2008. Additional emails followed over 4 hours and 22 minutes, containing offensive language. |
| **How It Was Reported** | The victim reported the harassment to university IT staff, who started network monitoring and captured all traffic in a PCAP file. |
| **Immediate IT Actions** | -Extracted email headers & message content.  -Filtered SMTP logs for anomalies.  - Notified forensic investigators. |

Furthermore, by focusing background evidence, we can also find such points mentioned below.

The integrity of the captured file packet was guaranteed through crypto-hashes, with MD5, SHA1, and SHA256 crypto-hashes guaranteeing data unaltered and legally binding for use for examination purposes. The crypto-hashes were:

• MD5: 9981827f11968773f815e39f5458ec8

• SHA1: 65656392412add15f93f8585197a8998aaeb50a1

• SHA256: 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb

The suspect exploited anonymous email solutions, including willself-destruct.com and sendanonymousmail.net, from network logs of HTTP POST requests on such websites for emailing submissions. The suspect exploited such solutions for identity concealment when they conducted harassment.

DNS requests also supported this activity, as the suspect was consistently connecting to such proxies for anonymity. DNS logs also confirmed queries for willselfdestruct.com and sendanonymousmail.net, implying attempted source concealment of the email.

TCP/IP packet analysis also yielded such anomalies such as TCP re-transmits and failed handshakes with SSL, and this indicates evasion methods. TCP sequence correlation with DNS queries also created a simple relationship between the suspect's computer and the identified anonymous services, and this linked harassment with the suspect's computer.

# Supporting Evidence Presented

This section presents the forensic evidence gathered during the investigation. This section presents the forensic evidence gathered during the investigation.

Cryptographic Integrity Verification

| **Algorithm** | **Hash Value** |
| --- | --- |
| **MD5** | 9981827f11968773f815e39f5458ec8 |
| **SHA1** | 65656392412add15f93f8585197a8998aaeb50a1 |
| **SHA256** | 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb |

* **Finding:** No modifications were detected, ensuring the integrity of the digital evidence.

Email Header Analysis

| **Field** | **Extracted Value** |
| --- | --- |
| **From** | sendanonymousmail.net |
| **Received From IP** | 140.247.62.34 |
| **Message-ID** | <abc123xyz@mailserver.com> |

* **Finding:** Email headers confirm that the harassment emails originated from within the dormitory network.

Packet Capture Data (XYZ.pcap)

| **Frame No.** | **Timestamp (Seconds since first capture packet)** | **Source IP** | **Destination IP** | **Protocol** | **Activity** |
| --- | --- | --- | --- | --- | --- |
| 16744 | 1h 53min 0.439281s | 192.168.1.64 | 74.125.19.19 | HTTP | GET request to Gmail |
| 78990 | 4h 9min 55.451768s | 192.168.15.4 | 74.125.19.17 | HTTP | GET request to Gmail  (attcker) |
| 80614 | 4h 11m 50.452871s | 192.168.15.4 | 69.80.225.91 | HTTP | POST request to sendanonymousmail.net |
| 83601 | 4h 13m 17.216422s | 192.168.15.4 | 69.25.94.22 | HTTP | POST request to willselfdestruct.com |

* **Finding:** The suspect's device actively engaged with anonymous email services to send messages.

DNS Query Logs

| **Queried Domain** | **Resolved IP** |
| --- | --- |
| sendanonymousmail.net | 69.80.225.91 |
| willselfdestruct.com | 69.25.94.22 |
| mail.google.com | 74.125.19.17 |

* **Finding:** The suspect intentionally accessed anonymous email services before sending harassing emails.

MAC Address Log Correlation

| **MAC Address** | **Device Type** | **Activity Logged** |
| --- | --- | --- |
| 00:17:f2:e2:c0:ce | Apple Device | Engaged in email transmissions |
| 00:1d:d9:2e:4f:60 | Router | Facilitated outbound traffic |
|  |  |  |

* **Finding:** The MAC address 00:17:f2:e2:c0:ce consistently accessed anonymous email services at the time of the harassment emails.

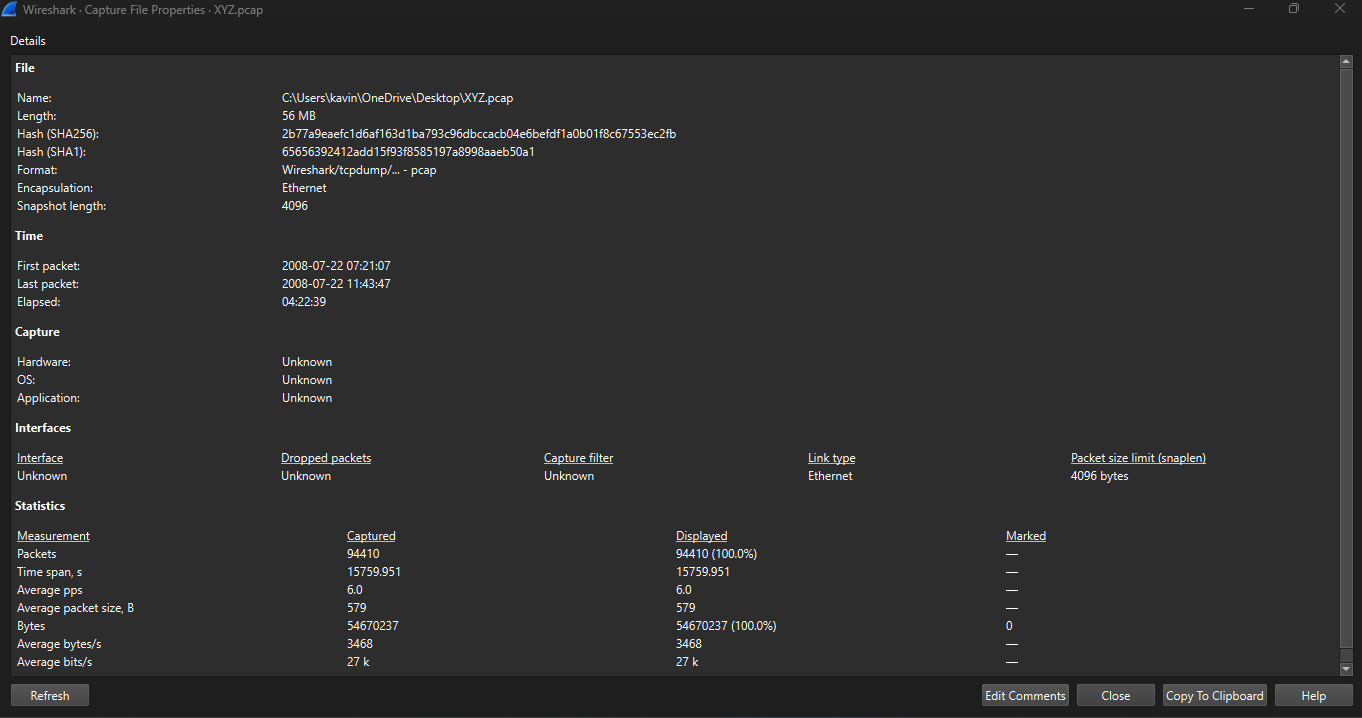
More details about collected evidence

| **Evidence Type** | **Description** |
| --- | --- |
| Network Capture File (PCAP) | 94,410 packets recorded, including email transmissions, NAT translations, HTTP requests, and DNS lookups. |
| Email Headers & Content | Extracted SMTP headers, sender IPs, and raw messages, confirming the use of anonymous email services. |
| Server Logs | XYZ School’s SMTP and HTTP logs showed activity from 192.168.15.4 (suspect's device) communicating with anonymous email services. |
| DNS Resolution Logs | NSLOOKUP & WHOIS verified external SMTP relay servers used in the attack. |
| MAC Address Data | Identified the attacker’s device as an Apple MacBook (00:17:f2:e2:c0:ce). |
| NAT Table Records | Mapped private IP (192.168.15.4) to public IP (140.247.62.34), proving network involvement. |
| HTTP Cookie Leak | Captured Gmail authentication cookie revealing jcoach@gmail.com, linking the attack to Johnny Coach. |

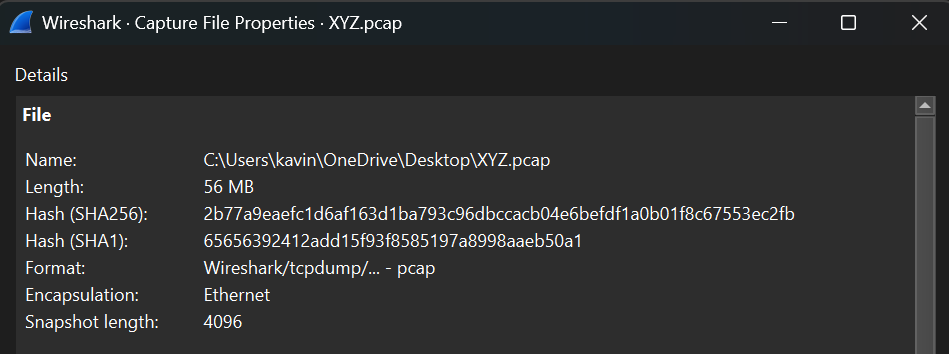
* Key Finding: Network traffic analysis traced the suspect’s device and it play a major role to confirm their involvement.

**By the way below the all evidences and screenshots provided by Wireshark and others/ Appendix A – List of evidence**

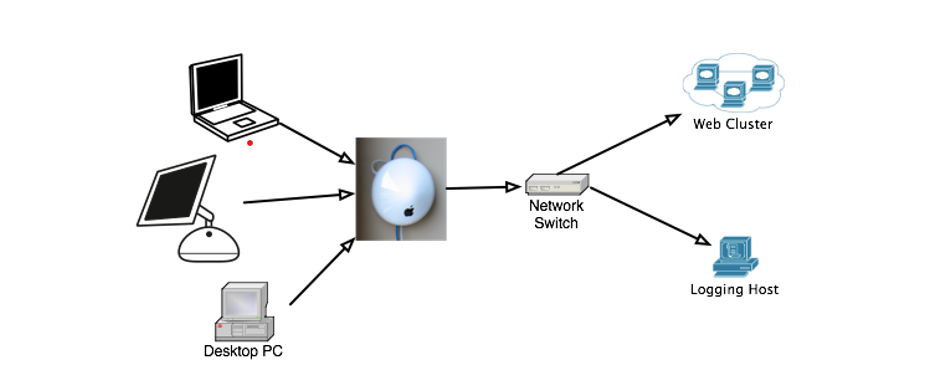
[Evidence 01]



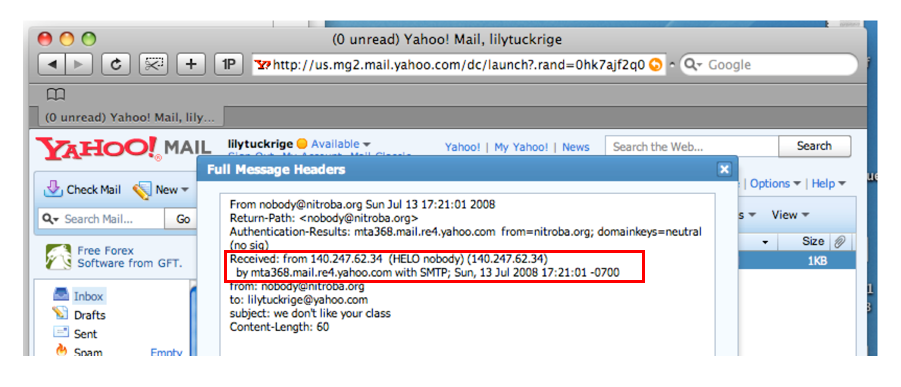
[Evidence 01(zoom-in)]



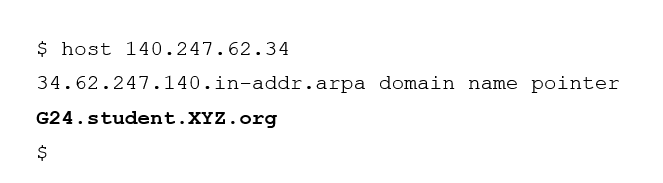
[Evidence 02]



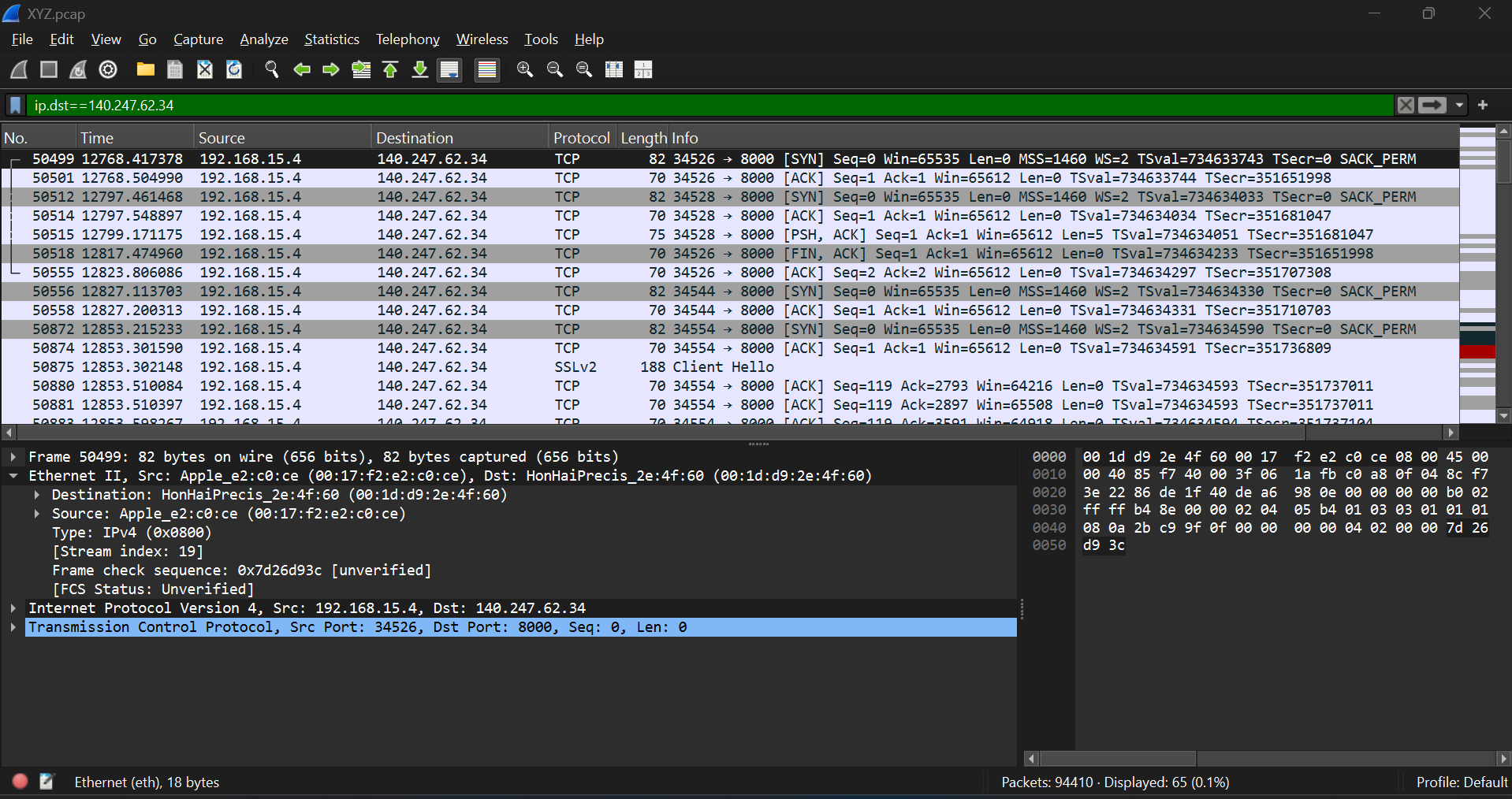
[Evidence 03]



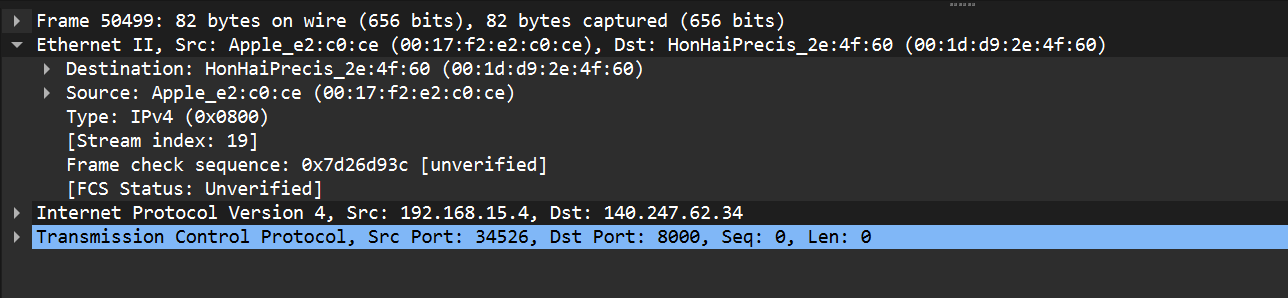
[Evidence 03.1]

****

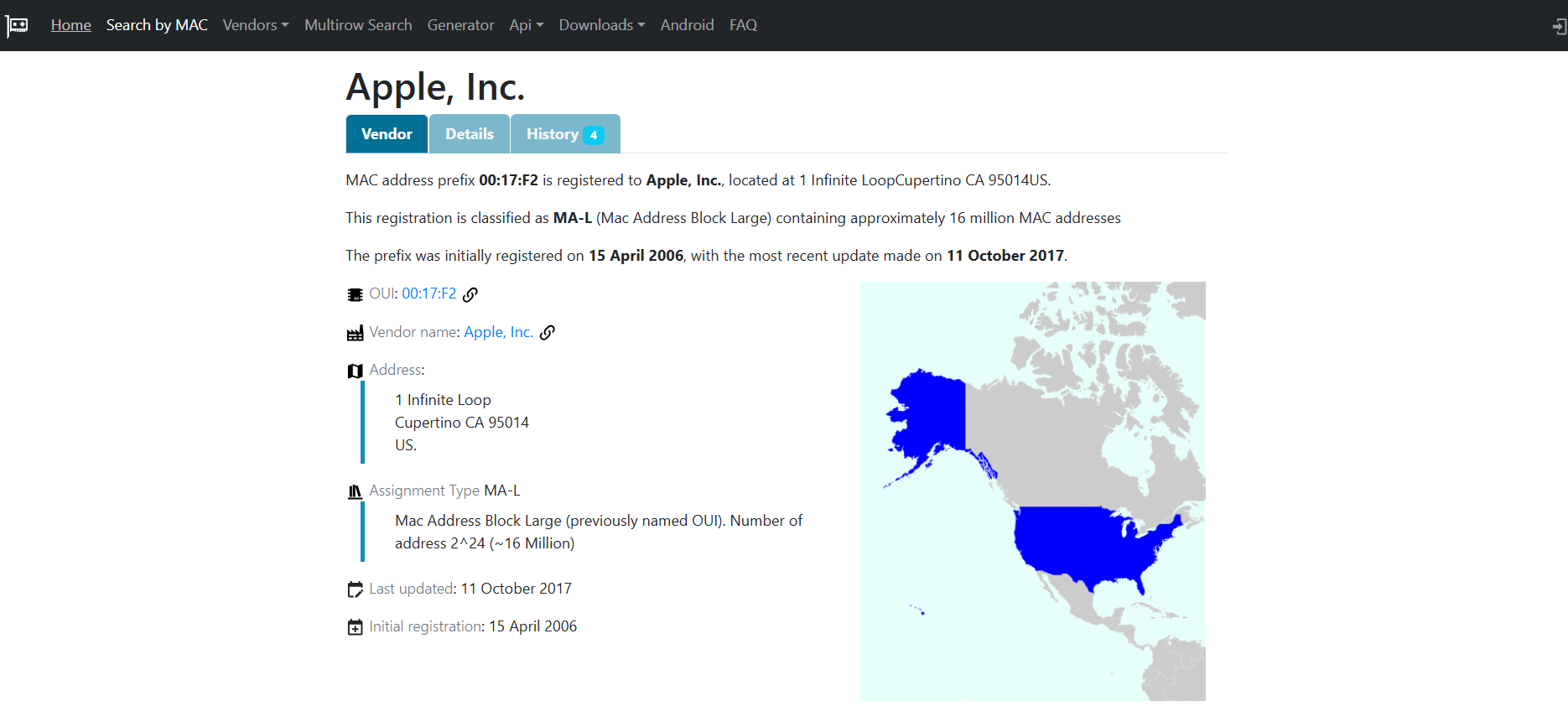
[Evidence 04]



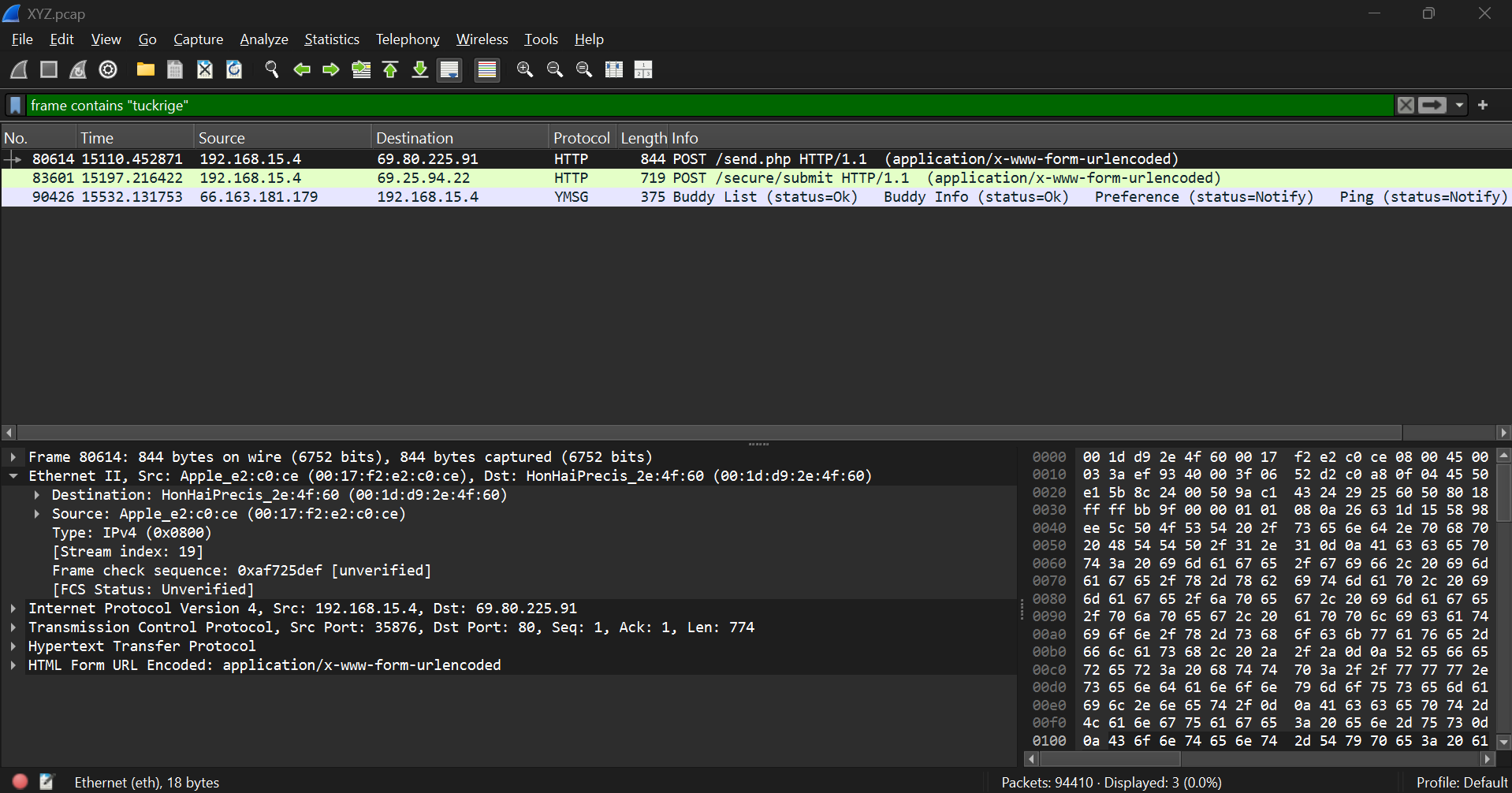
[Evidence 05]



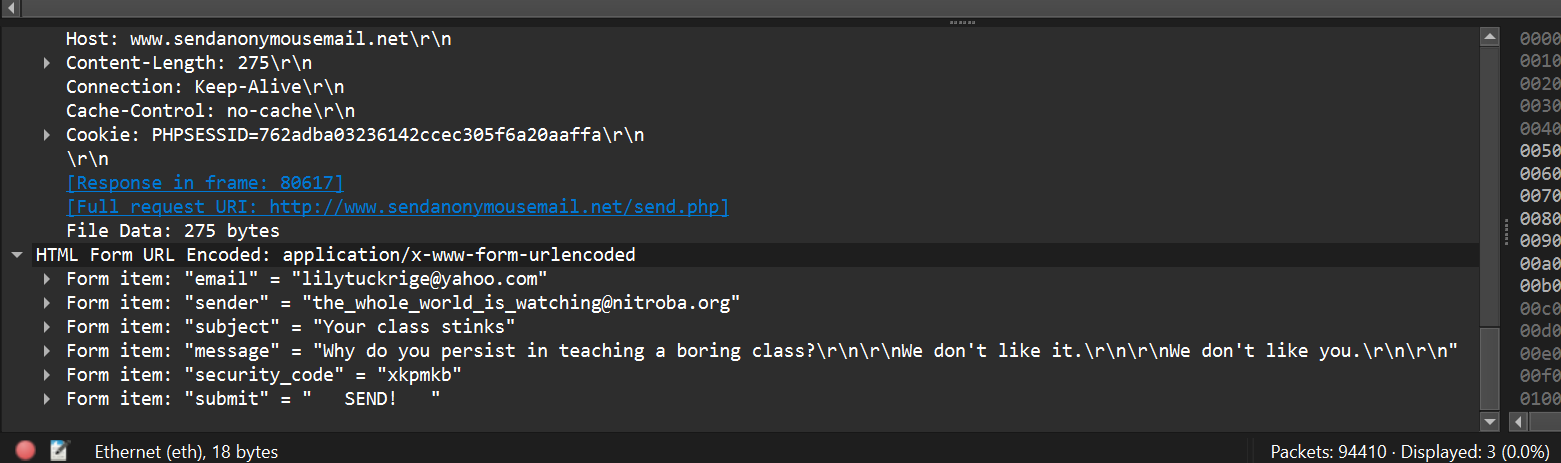
[Evidence 06]



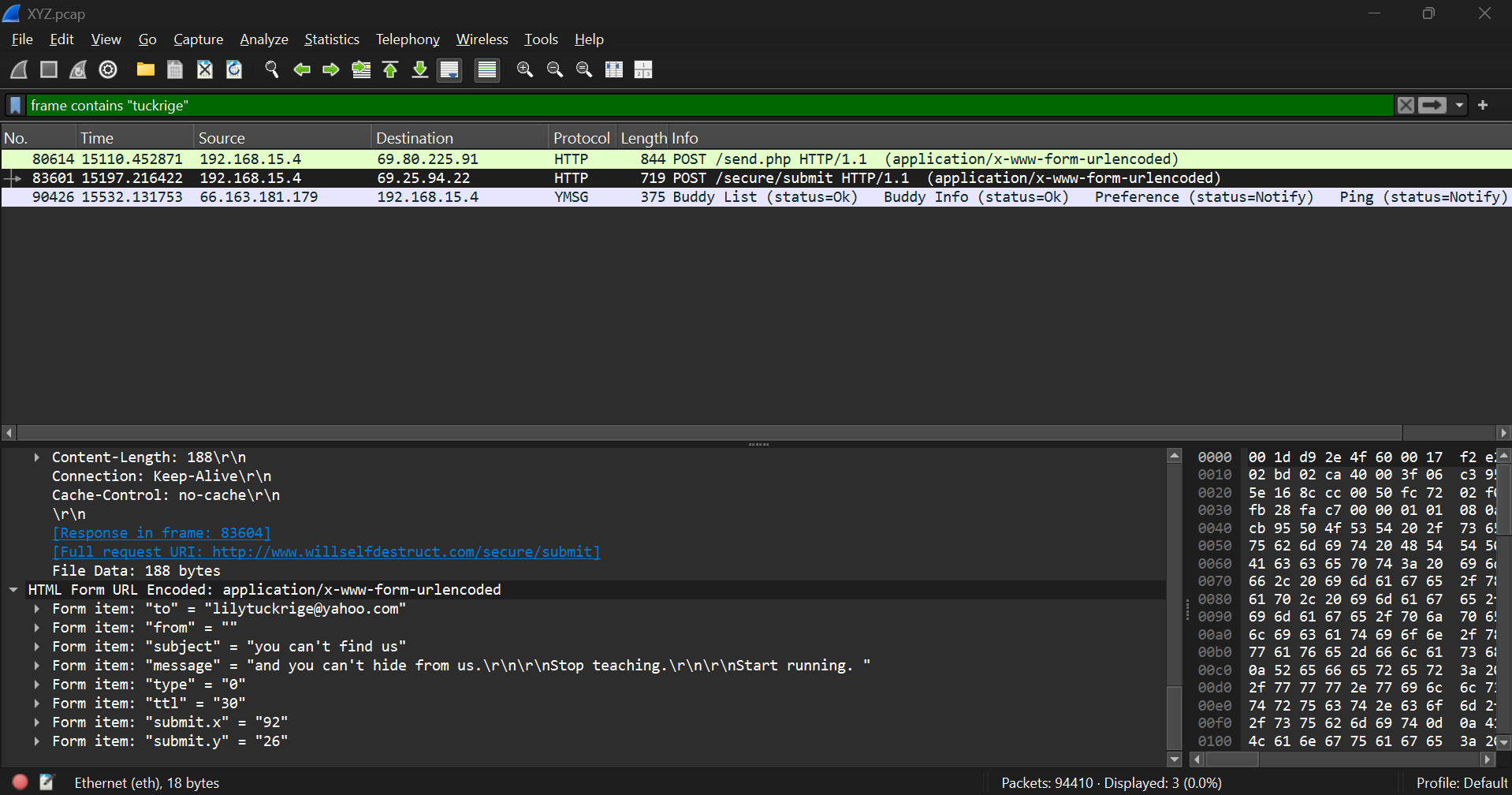
[Evidence 07]



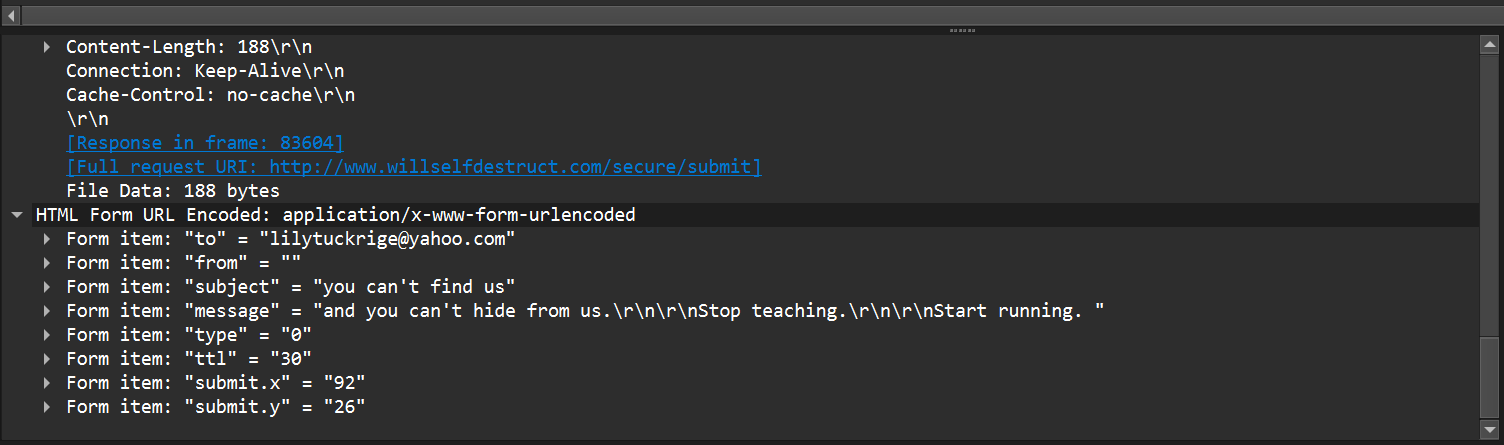
[Evidence 08]



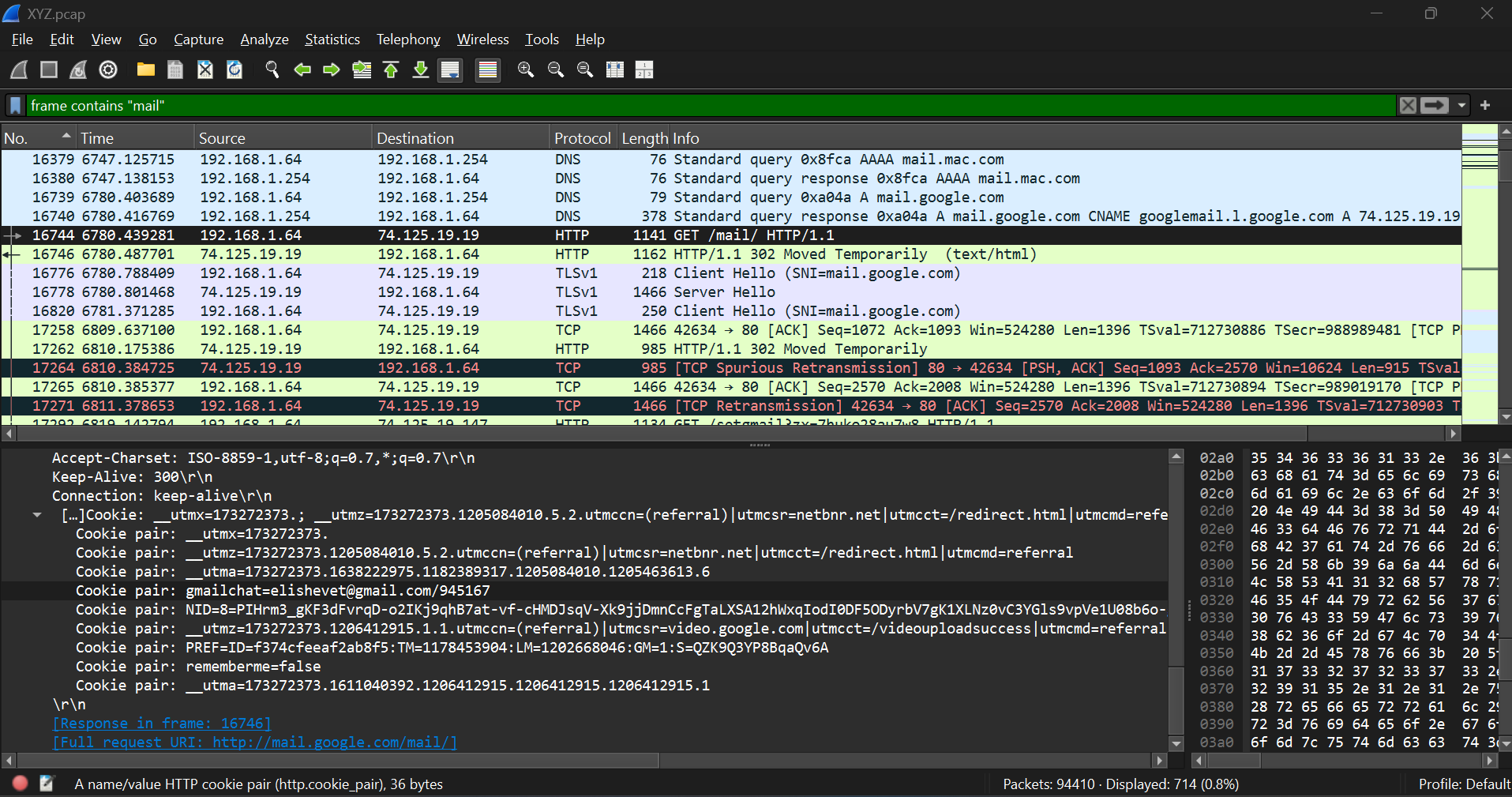
[Evidence 09]



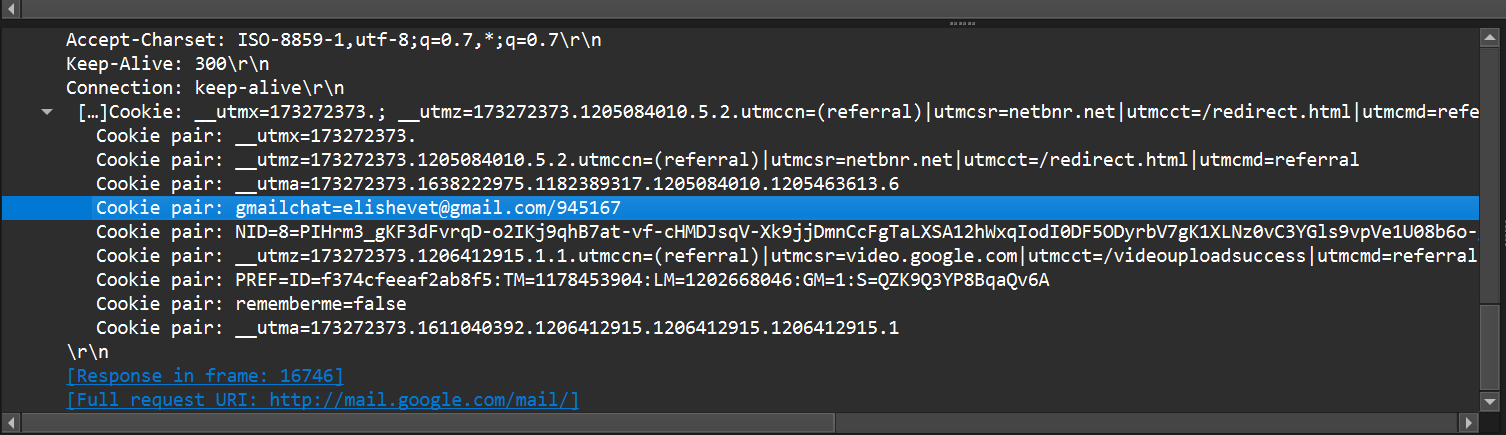
[Evidence 10]



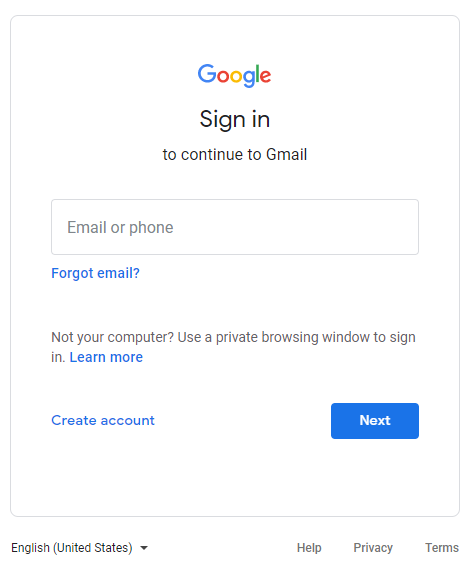
[Evidence 11]



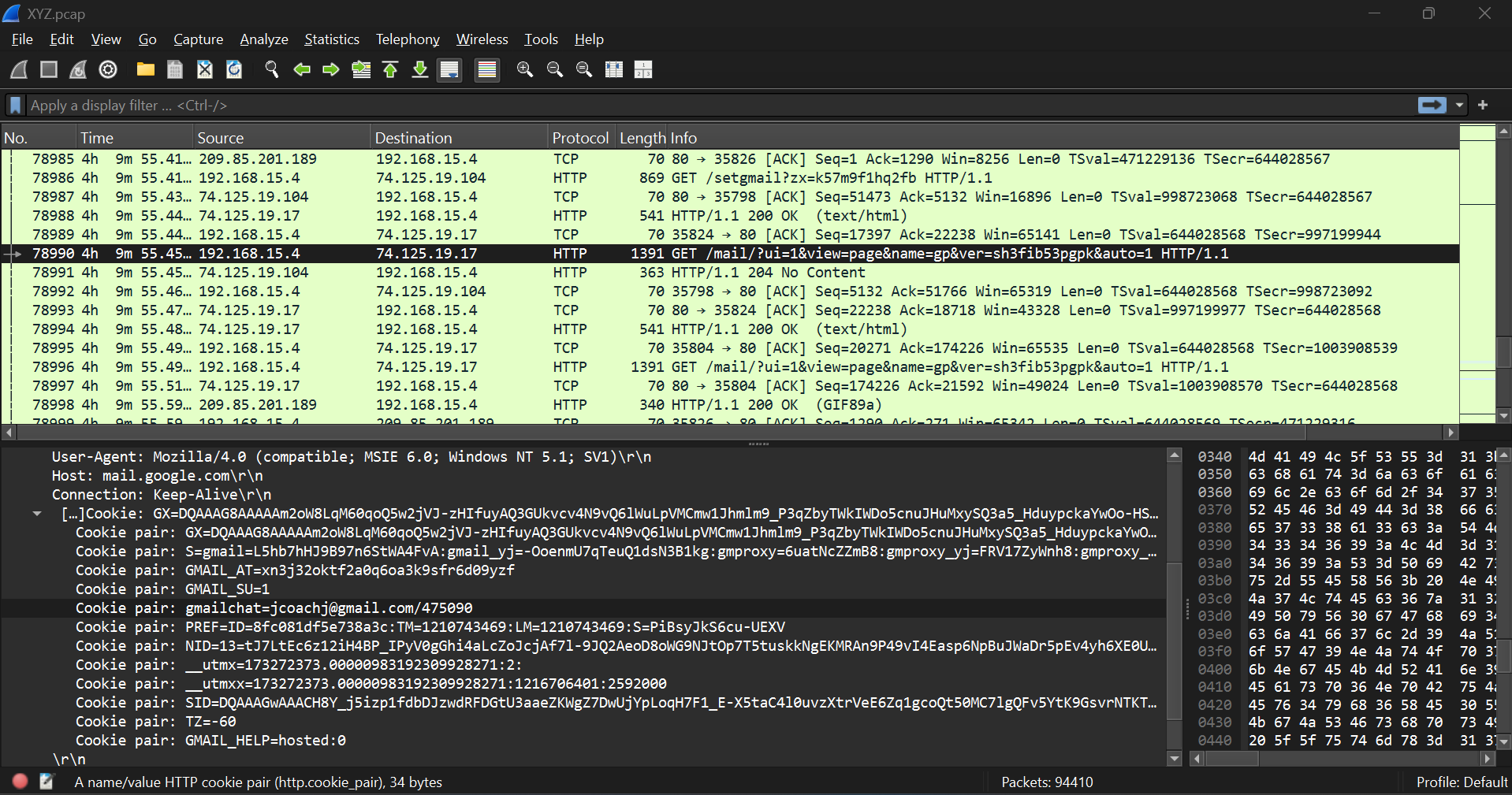
[Evidence 12]

**

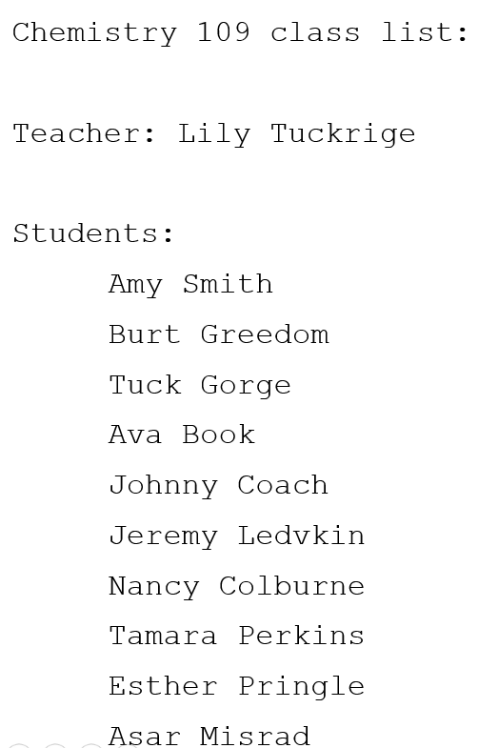
[Evidence 13]



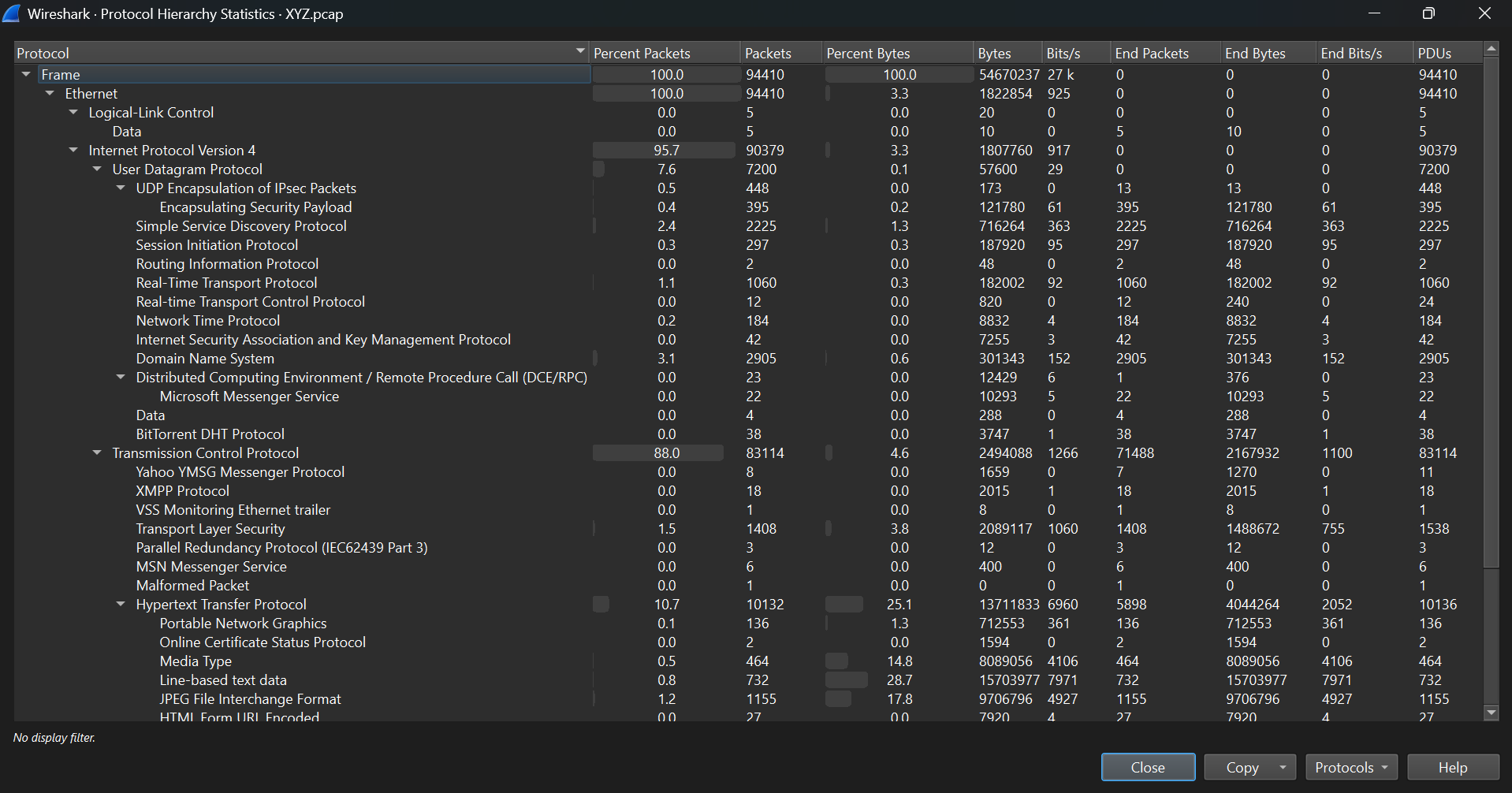
[Evidence 14]



[Evidence 15]



[Evidence 16]



# Conclusions

In conclusion, network forensic analysis of the “XYZ Harassment Scenario” has established even a network of communications with sophistication can be analsed systematically for key evidence. The employment of Wireshark's deep packet analysis and other methods employed in this analysis has established a layered network behaviour perception.

The evidence overwhelmingly points towards utilization of the internal device with the IP 192.168.15.4, with the MAC address 00:17:f2:e2:c0:ce, for sending offending mails. The key evidence came with the pulling of an HTTP cookie, where the email address of “jcoach@gmail.com” was identified. With this email, when matched with the class roster, points directly towards “Johnny Coach.” The evidence also has corroborative data from other appliances and very huge SMTP logs.

Given the adversarial tone of the message and the explicit association with the suspect's computer, the investigation lends weight towards administrative action against the individual and other legal action under the laws of computer crime and harassment. Other action must be considered for auditing network access logs and securing other possible points of vulnerability on the network.

This investigation illustrates what can be accomplished when network data can be analysed with caution and shaped into concrete, beneficial evidence. There is no doubt that Investigators can ensure accuracy and reliability in their findings by using a step-by-step process and thoroughly testing and verifying the data securely. Systematic data review and data confirmation from more than a single source play an important part to ensure accuracy and reliability. There is no doubt that, the process not only simplifies technical data, but also closes the gap between computer crime and real-world consequences, and ensures enlightened decision making for legal and disciplinary action.

# Self-Review Section

|  |  |  |
| --- | --- | --- |
| **Covered Section** | **Kavindu Chamodya Nimshan (8145532)** | **Kaveen Sandaru Horst**  **Cohn (8145710)** |
| 1.Executive Summary | 50% | 50% |
| 2.1Network Capture File details | 50% | 50% |
| 2.2Network Components Identified | 50% | 50% |
| 3.1Tools Used | 50% | 50% |
| 3.2Steps Involved | 50% | 50% |
| 3.3Handling Data | 50% | 50% |
| 4.1Important network players | 50% | 50% |
| 4.2Network Structure | 50% | 50% |
| 4.3Activity Timeline for 192.168.15.4 | 50% | 50% |
| 4.4Background evidence | 50% | 50% |
| 5.Supporting Evidence Presented | 50% | 50% |
| 6.Conclusions | 50% | 50% |
| 7.Self-Review Section | 50% | 50% |