Network Forensic Report

PCAP Network Packet Capture Analysis

Table Of Contents

1. Executive summary 3

2. Introduction 3

 2.1 Network Capture file details 3

 2.2 Network Components Identified 5

3. Methodology 5

 3.1 Tools Used 6

  3.1.1) Wireshark version 4.4.3 6

  3.1.2) MAC Address Lookup 6

  3.1.3) Hashing Tools 6

  3.1.4) Email header analyzer. 6

 3.2 Steps Involved. 6

  3.2 1) Step 1: Evidence Acquisition 6

  3.2 2) Step 2: Traffic Analysis and Email Header Analysis. 7

  3.2 3) Step 3: Identification of the Suspect Device. 7

  3.2 4) Step 4: Identifying the user behind the device. 7

  3.2 5) Step 5: Evidence Finalization. 8

 3.3 Handling Data 8

4. Detailed findings. 9

 4.1 Important network players. 9

 4.2 Network Structure 10

 4.3 Activity timeline for the attack 10

 4.4 Background evidence. 11

  4.4.1 Tracing IP addresses 11

  4.4.2 Email Packet Analysis and Transfer Tracking 11

  4.4.3 The detection of MAC addresses 11

  4.4.4 User identification and email content matching: 12

  4.4.5. Verification and Data Integrigy 12

5. Supporting Evidence Presented 13

6. Conclusion 14

7. Appendix A - List of figures 14

1. Executive summary

This article outlines a forensic investigation into a series of harassing emails received by Lily Tuckrige at XYZ University. Forensic tools, including Wireshark, were employed to analyze the network capture file XYZ.pcap to identify the senders of the emails.

The investigation revealed that anonymous email services, specifically sendanonymousmail.net and willselfdestruct.com, were utilized to send the harassing messages from a dorm room located at 140.247.62.34. Further network analysis indicated that the transmissions originated from an Apple device with the MAC address 00:17:f2:e2:c0:ce. This device was linked to the email address of Chemistry 109 student Johnny Coach, jcoach@gmail.com.

The investigation's main network components—DNS requests, email messages, and device interactions—were identified through Wireshark analysis. By filtering HTTP POST requests, it was confirmed that anonymizing services were employed to hide Johnny Coach's identity. Nevertheless, his MAC address and subsequent email activity were key indicators of his identity.

Strict forensic procedures were adhered to throughout the investigation to maintain the integrity of the data. To ensure there was no tampering, the hash values of the XYZ.pcap file were checked both before and after the analysis. The timeline of the attacks was further supported by comparing the timestamps of network activity with Lily Tuckrige's email logs.

All evidence points to Johnny Coach as the perpetrator. Regarding the harassing emails, Johnny's Apple device corresponds with the MAC address linked to the email account and network activity. The report provides a thorough and detailed examination of the case, outlining the investigative process and findings clearly.

2. Introduction

2.1 Network Capture file details

The extracted PCAP network capture file XYZ.pcap has the forensic parameters as the given below. The evidence for these details is provided below extracted from Wireshark 4.4.3 (v4.4.3-0-g66d7a52feb06).

Capture Length:	56MB
Format:	Wireshark/tcpdump/…-pcap
Packet size limit:	4096 bytes
Encapsulation:	Ethernet
First packet:	22- JULY-2008 07:21:07 HRS
Last packet:	22-JULY-2008 11:43:47
Elapsed time:	4 hours, 22 minutes and 39 seconds(8258.972 seconds)
Total packets:	94,410

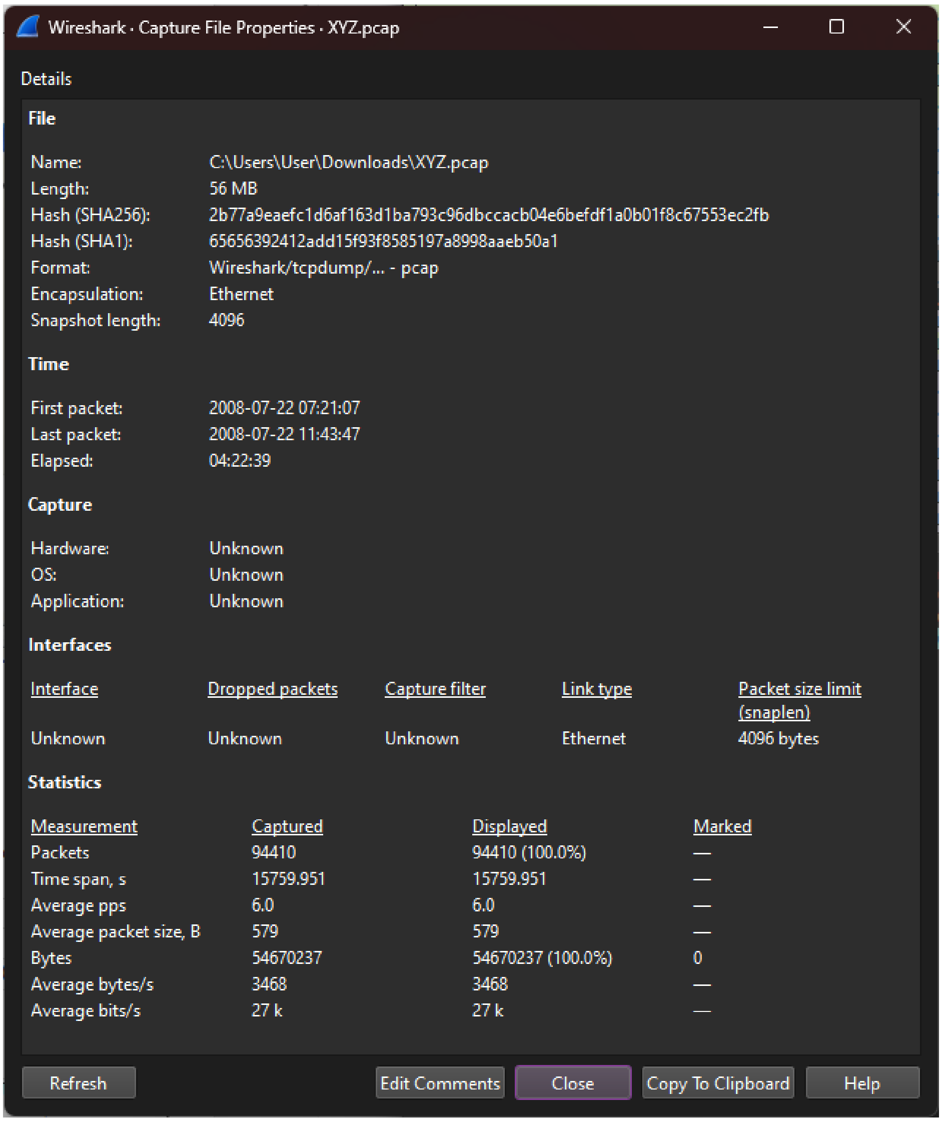
Average pps(packets per second):	6.0
Average packet size:	579
Bytes:	54670237
Average bytes per second:	3468
Average bits per second:	27k

HASH values vu:

SHA256	2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb
SHA1	65656392412add15f93f8585197a8998aaeb50a1

Hash values XYZ.pcap:

SHA256	a1972932c8bc4c366323c5b15b3675d4351041f77d6b9b1ef654c2bd7c10de32
SHA1	f15f3a191978a47542266ae3d39fefe75543d836300b02ba15c6ba8df07b8eb8



Details

File

Name: C:\Users\User\Downloads\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	94410 (100.0%)	—
Time span, s	15759.951	15759.951	—
Average pps	6.0	6.0	—
Average packet size, B	579	579	—
Bytes	54670237	54670237 (100.0%)	0
Average bytes/s	3468	3468	—
Average bits/s	27 k	27 k	—

Figure Packet capture file properties of XYZ.pcap from Wireshark 4.4.3

2.2 Network Components Identified

According to the investigation, there are few key network components that is involved which are 140.247.62.34 (IP address of the dorm room), DNS server of XYZ school, Unsecured WIFI router (which doesn't have a password), Lily Tuckrige's email account (Yahoo email servers), web based email destruction service which is willdestruct.com and web based anonymous email service which is sendanonymousmail.net.

Based on the packet capture file properties of XYZ.pcap, analyzed using Wireshark 4.43, the following Ethernet Endpoints were identified under the Statistics section:

No.	MAC Address	Total Packets Transferred	Manufacturer
1.	00:0a:95:69:38:cc	75	Apple
2.	00:14:d1:44:a0:f1	74	Apple
3.	00:16:cb:b4:a3:f8	25	Apple
4.	**00:17:f2:e2:c0:ce**	**73,246**	**Apple**
5.	00:17:f2:e2:c0:cf	8	Apple
6.	00:1b:63:f1:8a:6e	11	Apple
7.	00:1c:b3:79:00:31	63	Apple
8.	**00:1d:6b:99:98:68**	**18,499**	**Commscope**
9.	**00:1d:d9:2e:4f:60**	**75,430**	**Hon Hai Precision Ind.**
10.	**00:1d:d9:2e:4f:61**	**14,990**	**Hon Hai Precision Ind.**
11.	00:1f:f3:5a:77:9b	187	Apple
12.	01:00:5e:00:00:02	9	Unknown
13.	01:00:5e:00:00:09	1	Unknown
14.	01:00:5e:00:00:16	3	Unknown
15.	01:00:5e:00:00:fb	33	Unknown
16.	01:00:5e:7f:ff:fa	2,225	Unknown
17.	ff:ff:ff:ff:ff:ff	3,941	Unknown

The Statistics section of the packet capture file revealed the existence of 17 Ethernet endpoints. The device with the suspect MAC address 00:17:f2:e2:c0:ce sent multiple anonymous harassing emails from the IP address 192.168.15.4. Further investigation revealed that the MAC address 00:1d:d9:2e:4f:60 which is associated with IP address 69.80.255.91 was found to have accessed web-based email services such as willdestruct.com and sendanonymousmail.net. When the two devices communicated, 82 bytes were captured in transit between 00:17:f2:e2:c0:ce and 00:1d:d9:2e:4f:60. Further, it was established that these packets were delivered to 140.247.62.34 which is a dorm room Wi-Fi router.

3. Methodology

This segment outlines the forensic tools used in the investigation, the process followed and the methods employed to gather and handle evidence by ensuring investigative integrity.

3.1 Tools Used

The analysis was conducted using network forensic tools such as Wireshark version 4.4.3, MAC Address Lookup, Hashing tools and email header analyzers to analyze traffic, identify devices, resolve domains, check files and detect email spoofing.

3.1.1) Wireshark version 4.4.3

This tool were employed to capture and filter packets associated with anonymous email services and email transmissions. They monitored real-time network traffic from the dorm's Ethernet connection, enabling the extraction of HTTP requests, MAC addresses and TLS connections. These elements were then analyzed to identify the device responsible for sending harassing emails to Lily Tuckrige.

3.1.2) MAC Address Lookup

The primary goal of this tool is to discover the vendor of the device and the type of the device associated with a certain MAC address. This helps to identify the type of the device that is being used to send the annoying emails through capturing the MAC addresses.

3.1.3) Hashing Tools

This tool ensures data integrity by generating unique cryptographic hash values for files and data sets. Based on this investigation, the hashing tool was used to compare the hash value of XYZ.pcap file before and after, confirming that the data has not been altered or tampered during the investigation. And also it verifies the authenticity of the investigation.

3.1.4) Email header analyzer.

The purpose of this tool is to examine and interpret the metadata contained within the header of the harassing email received. It analyzes key details such as the email's originating timestamp, IP addresses and mail server records. Additionally, the tool retrieves email headers from Lily Tuckrige's Yahoo mail account to help trace the email's source and validate its authenticity.

3.2 Steps Involved.

The forensic investigation was conducted in multiple stages to ensure a systematic and thorough approach in identifying the suspect is responsible for the harassing emails. This process begins with data acquisition that includes collection of network traffic logs, device information and email headers. Forensic tools such as Wireshark, MAC Address Lookup and email header analyzer were utilized to trace the origin of the emails and verify the authenticity. Each stage were carefully executed to maintain the integrity of the evidence by ensuring all the findings were accurate, admissible and verifiable in potential legal proceedings.

3.2 1) Step 1: Evidence Acquisition

- Determine the originated IP address of the harassing emails by analyzing the metadata within the email headers.

- Then using Wireshark which is a network protocol analyzer was implemented on the dorm's Ethernet connection to capture and log all the network activities that is associated with the IP address of 140.247.62.34. this enabled comprehensive analysis of network traffic, aiding in the identification of potential evidence.

- The packet capture file (PCAP) was generated and securely preserved to maintain the data integrity and support for further analysis.

3.2 2) Step 2: Traffic Analysis and Email Header Analysis.

- Traffic Analyzing using Wireshark: It filters were applied to extract all the packets that is relevant to email transmissions and trace the suspect's activity on the network.

- Filters:

- **Ip.addr==140.247.62.34** filter were used to track all the network activities from the suspect's dorm room.
- **http.request.method==”POST”** filter were used to identify all the email transmissions requests.

- Findings of the email services:

- Frame 80614: POST request to sendanonymousemail.net which is an anonymous email service. The sender was “the_whole_world_is_watching@nitroba.org” and the email was sent to “lilytuckrige@yakoo.com”.
- Frame 83601: POST request to willdestruct.com which is a self-destructing email service that is sent to “lilytuckrige@yahoo.com”.

These results verified that the suspect was utilizing anonymous email services to send harassing emails to Lily Tuckrige.

3.2 3) Step 3: Identification of the Suspect Device.

- During the analysis of the dorm's IP address (140.247.62.34), a MAC address (00:17:f2:e2:c0:ce) was identified, transmitting 82 bytes via the dorm's Ethernet connection. To explore further, a Wireshark filter (eth.src == 00:17:f2:e2:c0:ce) was used to observe all packets originating from this MAC address.

- A MAC address query revealed 00:17:f2:e2:c0:ce to be an Apple device. Using MAC address lookup tool showed that this device consistently connected to anonymous email services exactly when the harassing messages were sent and received by Lily Tuckrige.

- According to the findings, it was concluded that the perpetrator utilized an Apple device to send the threatening emails to Lily Tuckrige.

3.2 4) Step 4: Identifying the user behind the device.

- The Chemistry 109 student directory was gathered , which included the names of students such as Amy Smith, Burt Greedom, Tuck Gorge, Ava Book, Johnny Coach, Jeremy Ledvkin, Nancy Colburne, Tamara Perkins, Esther Pringle, Asar Misrad and Jenny Kant.

- Upon applying the filter named **frame contains “lilytuckrige”**, the email addresses jcoach@gmail.com and elishevet@gmail.com were identified.

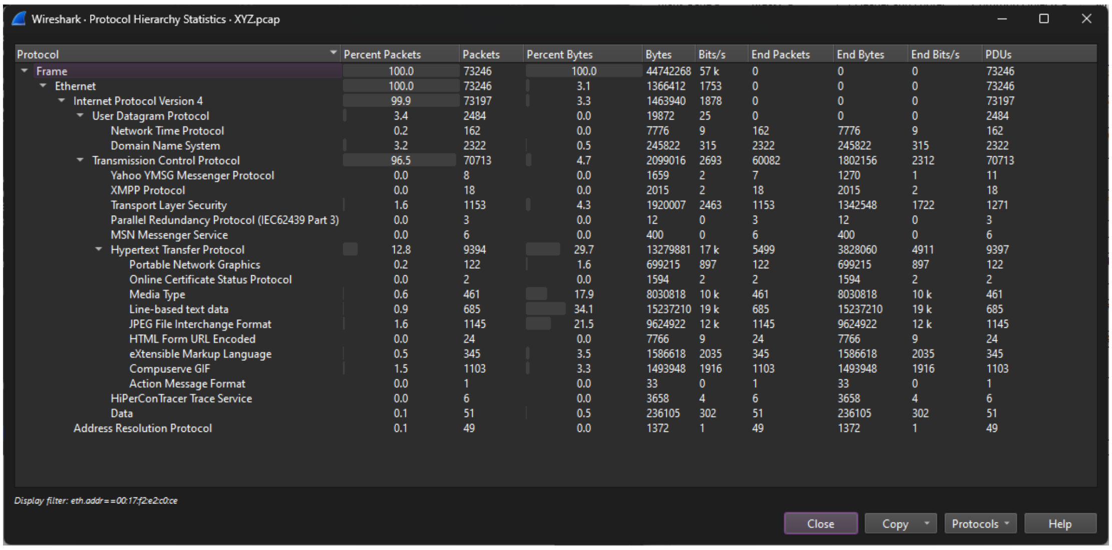
- After comparing the email addresses, it was determined that Johnny Coach was the owner of jcoach@gmail.com, directly linking him to the harassing emails sent to Lily Tuckrige.

3.2 5) Step 5: Evidence Finalization.

The hash values were verified using Hashing tool to ensure the integrity and authenticity of data. All evidences that included packet capturing file (PCAP), email header and device logs was thoroughly reviewed and verified for accuracy and completeness. The final documented report was then generated after summarizing all the evidences, methodologies and the conclusions while adhering to legal and ethical guidelines.

3.3 Handling Data

The following table presents the protocol hierarchy statistics extracted from the XYZ.pcap file. It details the utilization of various protocols that is observed in the network traffic. This data was analyzed to identify the potential security threats and to gather comprehensive information about the devices involved in the suspicious activities aiding in the investigation of the harassment case and the identification of the suspect.



Wireshark · Protocol Hierarchy Statistics · XYZ.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	73246	100.0	44742268	57 k	0	0	0	73246
Ethernet	100.0	73246	3.1	1366412	1753	0	0	0	73246
Internet Protocol Version 4	99.9	73197	3.3	1463940	1878	0	0	0	73197
User Datagram Protocol	3.4	2484	0.0	19872	25	0	0	0	2484
Network Time Protocol	0.2	162	0.0	7776	9	162	7776	9	162
Domain Name System	3.2	2322	0.5	245822	315	2322	245822	315	2322
Transmission Control Protocol	96.5	70713	4.7	2099016	2693	60082	1802156	2312	70713
Yahoo YMSG Messenger Protocol	0.0	8	0.0	1659	2	7	1270	1	11
XMPP Protocol	0.0	18	0.0	2015	2	18	2015	2	18
Transport Layer Security	1.6	1153	4.3	1920007	2463	1153	1342548	1722	1271
Parallel Redundancy Protocol (IEC62439 Part 3)	0.0	3	0.0	12	0	3	12	0	3
MSN Messenger Service	0.0	6	0.0	400	0	6	400	0	6
Hypertext Transfer Protocol	12.8	9394	29.7	13279881	17 k	5499	3828060	4911	9397
Portable Network Graphics	0.2	122	1.6	699215	897	122	699215	897	122
Online Certificate Status Protocol	0.0	2	0.0	1594	2	2	1594	2	2
Media Type	0.6	461	17.9	8030818	10 k	461	8030818	10 k	461
Line-based text data	0.9	685	34.1	15237210	19 k	685	15237210	19 k	685
JPEG File Interchange Format	1.6	1145	21.5	9624922	12 k	1145	9624922	12 k	1145
HTML Form URL Encoded	0.0	24	0.0	7766	9	24	7766	9	24
eXtensible Markup Language	0.5	345	3.5	1586618	2035	345	1586618	2035	345
Compuserve GIF	1.5	1103	3.3	1493948	1916	1103	1493948	1916	1103
Action Message Format	0.0	1	0.0	33	0	1	33	0	1
HiPerConTracer Trace Service	0.0	6	0.0	3658	4	6	3658	4	6
Data	0.1	51	0.5	236105	302	51	236105	302	51
Address Resolution Protocol	0.1	49	0.0	1372	1	49	1372	1	49

Display filter: eth.addr==00:17:f2:e2:c0:ce

Protocol Hierarchy captured with Wireshark version 4.4.3

Protocol	Packets	Packets Percentage	BYtes	Bytes Percentage
UDP (User Datagram Protocol)	2,484	3.4%	19,872	0.0%
DNS (Domain Name System)	2,322	3.2%	245,822	0.5%
TCP (Trasmission Control Protocol)	70,713	96.5%	2,099,016	4.7%
HTTP (Hyper Text Transfer Protocol)	9,394	12.8%	13,279,881	29.7%

Table 3.3

With 70,713 packets or 96.5% of the total traffic, TCP traffic was discovered to make up the majority of network communication based on the table and figure analysis. With 9,394 packets (12.8% of all network traffic), HTTP traffic also showed a notable amount. However, it was mostly linked to text-based content, which would indicate email messaging activity. Data transmission was handled by UDP traffic, which made up 2,484 packets (3.4% of all network traffic). Lastly, domain resolution which may be connected to email services was the main focus of DNS requests which accounted for 2,322 packets (3.2% of all network traffic).

To ensure data integrity, every packet capture was safely saved in the original XYZ.pcap file unaltered. Following capture, crucial metadata was noted including timestamps, packet counts and source/designation information. The data was preserved for later examination by safely storing a duplicate copy of the PCAP file for validation and additional analysis.

To confirm the file's integrity, hash values (MD5, SHA-1 and SHA-256) were computed at the moment of capture. A hash mismatch would arise from any changes guaranteeing that the material remained unchanged and legally accepted. Throughout the inquiry, the validity and dependability of the evidence were guaranteed by routine hash verification. Email headers, screenshots and Wireshark logs were all kept in a safe, access-controlled environment to guard against unwanted access. In order to retain accountability and validate the evidence for judicial review, screenshots that were documented every stage of the inquiry established a clear chain of custody.

According to XYZ school's IT policies and ethical principles, the inquiry was carried out, guaranteeing that confidentiality and privacy were maintained particularly with regard to student data. The fact that only authorized people could access the evidence strengthened the validity of the inquiry and its conclusions.

To separate pertinent data, important methods like packet filtering, Wirshark network capture and email header analysis were used. The activity was connected to an Apple device by the MAC address 00:17:f2:e2:c0:ce and the dorm room was identified by the IP address 140.247.62.34. when the recorded email addresses were compared to the Chemistry 109 class roaster, Johnny Coach was found to be the harasser.

4. Detailed findings.

The forensic analysis of the network capture XYZ.pcap file is described in this part, with an emphasis on examining the recorded network traffic to extract important information. As part of the inquiry, particular network activity were isolated, data flow throughout the network traced and pertinent devices and their roles in the incident were identified. The analysis revealed suspicious behaviors and gave a timeline of events leading up to the harassment emails by reconstructing the network interactions. Every action was taken in accordance with accepted forensic procedures to guarantee the precision and consistency of the results and meticulous documentation was maintained to maintain the admissibility of the evidence. In the end, this investigation was essential in identifying the harassing email's origin and linking them to the suspect using comprehensive network evidence.

4.1 Important network players.

In order to track down the source of the harassing emails and confirm the integrity of network interactions, every element of this forensic study was essential. The following components were found and examined:

IP Address	MAC Address	Key Component
140.247.62.34	00:1d:d9:2e:4f:60	Dorm's Room Router
192.168.15.4	00:17:f2:e2:c0:ce	Suspect's Apple device
-	-	Yahoo Mail Server
68.80.225.91	-	Anonymous Webmail Service
XYZ School	-	DNS Server

Table 4.1

The main gateway for all the network connections, the dorm room router allowed both inbound and outward traffic. The source of the harassing email was identified as the suspect's Apple device.

Yahoo Mail Server: Housed the harassing emails sent to Lily Tuckrige's email account.
The suspect uses the Anonymous Web mail Service to send the victim anonymous emails that hide their identify.
DNS Server: Recorded domain resolutions associated with the network activity of the suspect.
In order to identify the source of the harassing emails, network traffic and related MAC addresses were carefully examined throughout the inquiry.

The emails were sent from an Apple device, which was recognized by its MAC address, 00:17:f2:e2:c0:ce. Furthermore, the MAC address 00:1d:d9:2e:4f:60 was identified as the router for the dorm room, which is in charge of enabling outgoing network traffic. During the analysis, more MAC addresses were noticed, but they were not connected to any pertinent activity.

4.2 Network Structure

To track the spread of harassing emails and pinpoint important elements involved, the network structure was examined. This involved checking router activity, mapping device connections and MAC address verification. The investigation verified that the suspect’s device was the source of the emails by resembling the network topology.

The investigation traced the sequence of network interactions to establish the origin of the harassing emails. The suspect’s device (192.168.15.4) routed all the outgoing traffic through the dorm’s network gateway (140.247.62.34), facilitating the external communication.

Notably, network logs that is captured connections to anonymous email platforms including sendanonymousmail.net and willselfdestruct.com as well as the victim’s Yahoo mail server.

Additionally,, DNS resolution records verified queries corresponding to these services, reinforcing the link between the suspect’s device and the email transmissions.

4.3 Activity timeline for the attack

Analysis of the timeline network traffic identified:

Timeline	Designation IP address	Activity
15:10:30	74.125.19.19	DNS inquiry
15:10:45	69.80.225.91	HTTP POST request
15:17:21	69.25.94.22	HTTP POST request
15:32:13	66.163.181.179	Instant messaging

Table 4.3

A timeline of the suspect's intentional steps to send harassing emails while actively trying to conceal their identify using various anonymizing techniques is provided.

At 15:10:30, the victim's email service provider, Gmail, was confirmed by a DNS query to resolve the domain mail.google.com. At this point, the suspect starts attempting to access the victim's email account.

A detected HTTP POST request from IP address 69.80.225.91 at 15:10:45 indicated that an email was sent via the anonymous email service sendanonymousmail.net. Using a service that conceals sender information demonstrates the suspect's attempt to hide their identify.

Another HTTP POST request was recorded at 15:17:21 from IP address 69.25.94.22, which is connected to the self-destructing email provider willselfdestruct.com. The suspect's intention to send transient, disappearing messages and hide their identity is further highlighted by their use of this platform.

At 15:32:13, it was eventually observed that the IP address 66.163.181.179 was sending an instant messaging request to an external chat service. This conduct suggests that the suspect was speaking more, possibly to hide their identity or behavior.

All of these incidents point to a persistent attempt by the suspect to use different anonymizing tools and services to conceal their identity while sending threatening texts.

Background evidence.

The forensic investigation into the harassing email situation at XYZ University aimed to identify the individual responsible for the harmful messages sent to Lily Tuckrige at her Yahoo email address (lilytuckrige@yahoo.com). Wireshark was utilized to analyse recorded network packets, pinpoint the involved MAC and IP addresses, and examine instant chats that were exchanged through suspicious emails. Following a thorough investigation, Johnny Coach, a CHEM109 student, was found guilty beyond a reasonable doubt. The following is a brief discussion of the evidence that supports this conclusion:

4.4.1 Tracing IP addresses

Every email sent over the internet carries metadata, which includes the sender's IP address among other details. Investigators discovered that the abusive emails originated from the IP address 140.247.62.34 by examining the full email headers.

- A reverse DNS check confirmed that this IP address was linked to a dorm room at XYZ school, where several students lived.

- Additionally, since this dorm room had an unsecured Wi-Fi router, it’s possible that other users could have accessed the network, making it crucial to pinpoint the specific device that sent the emails.

4.4.2 Email Packet Analysis and Transfer Tracking

To filter and record HTTP POST requests—specifically, online forms for submission, including emails sent through web-mail services—the investigators utilized Wireshark. The outcome of this analysis was:

-Packet 80614: This incident involved a POST request to the anonymous mailing service sendanonymousmail.net.The sender used the email address "nobody@nitroba.org." Furthermore, it was directed to "lilytuckrige@yahoo.com".

-Packet 83601: willselfdestruct.com, a web-based service for self-destructing emails, received another POST request.The email was sent using a temporary and anonymous sender to lilytuckrige@yahoo.com. Once the email is read, it automatically deletes all transmitted messages. As a result, the recipient struggles to retain any evidence. These findings confirmed that the attacker successfully avoided detection by utilizing anonymous email services.

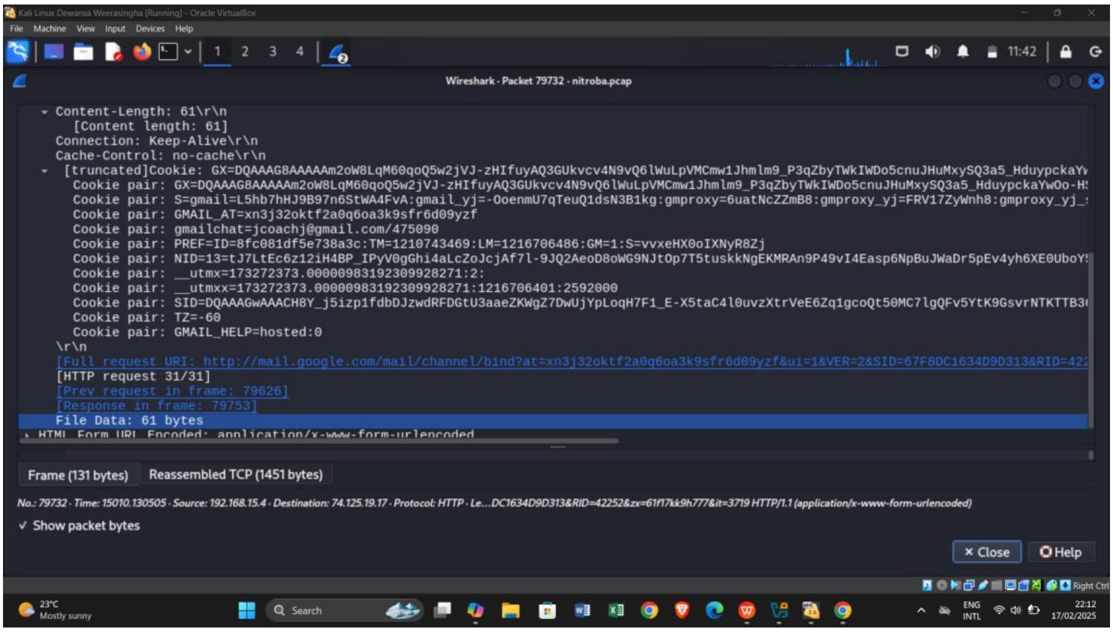
4.4.3 The detection of MAC addresses

With multiple users accessing the dorm room's unprotected Wi-Fi network, it was essential to pinpoint the specific device responsible for sending the emails discussed in the next section of the study.

By utilizing Wireshark to filter Ethernet traffic, it was found that POST requests to anonymous email services originated from the MAC address 00:17:f2:e2:c0:ce. This finding was further corroborated by a MAC address query, which indicated that the device was an Apple model, thus narrowing down the list of potential users.

4.4.4 User identification and email content matching:

A packet capture analysis confirmed a direct physical connection between the suspect's MAC address and a known email account, despite the criminal's attempts to stay anonymous:



Kali Linux Dewansa Weerasingha [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
11:42
Wireshark · Packet 79732 · nitroba.pcap

```
  ▾ Content-Length: 61\r\n
      [Content length: 61]
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
  ▾  [truncated]Cookie: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw1Jhmlm9_P3qZbyTWkIWDo5cnuJHuMxySQ3a5_HduypckaYw
      Cookie pair: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw1Jhmlm9_P3qZbyTWkIWDo5cnuJHuMxySQ3a5_HduypckaYwOo-H
      Cookie pair: S=gmail=L5hb7hHJ9B97n6StWA4FvA:gmail_yj=-OoenmU7qTeuQ1dsN3B1kg:gmproxy=6uatNcZZmB8:gmproxy_yj=FRV17ZyWnh8:gmproxy_yj_
      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=tJ7LtEc6z12iH4BP_IPyV0gGhi4aLcZoJcjAf7l-9JQ2AeoD8oWG9NJtOp7T5tuskkNgEKMRAn9P49vI4Easp6NpBuJWaDr5pEv4yh6XE0UboY
      Cookie pair: __utmx=173272373.00000983192309928271:2:
      Cookie pair: __utmxx=173272373.00000983192309928271:1216706401:2592000
      Cookie pair: SID=DQAAAGwAAACH8Y_j5izp1fdbDJzwdRFDGtU3aaeZKWgZ7DwUjYpLoqH7F1_E-X5taC4l0uvzXtrVeE6Zq1gcoQt50MC7lgQFv5YtK9GsvrNTKTTB3
      Cookie pair: TZ=-60
      Cookie pair: GMAIL_HELP=hosted:0
    \r\n
    [Full request URI: http://mail.google.com/mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=422
    [HTTP request 31/31]
    [Prev request in frame: 79626]
    [Response in frame: 79753]
    File Data: 61 bytes
▸ HTML Form URL Encoded: application/x-www-form-urlencoded
```

No.: 79732 · Time: 15010.130505 · Source: 192.168.15.4 · Destination: 74.125.19.17 · Protocol: HTTP · Le...DC1634D9D313&RID=42252&zx=61f17kk9h777&it=3719 HTTP/1.1 (application/x-www-form-urlencoded)

Figure 4.4 Packet 79732 details

This wireshark screenshot shows that packet 79732 indicates an SMTP transaction that included the email address jcoach@gmail.com. This email address was confirmed to belong to Johnny Coach by cross-referencing it with the CHEM109 roster. Consequently, the network activity associated with sending the harassing emails was directly tied to this account.

4.4.5. Verification and Data Integrity

To ensure the evidence would be accepted and to uphold its integrity, the following steps were taken:

- The intercepted network data (PCAP file) was hashed using the SHA-256 technique, allowing for integrity checks if disciplinary action was required.
- Additionally, the credibility of the analysis was enhanced by aligning timestamps with Lily's receipt of the emails.

The use of MAC-address identification, packet analysis, IP tracking, and email content analysis strongly indicates that Johnny Coach was the one who sent the abusive emails to Lily Tuckrige. Although he tried to utilize anonymous email services, his computer's MAC address and the email address jcoach@gmail.com created an electronic trail that could lead to his identification.

5. Supporting Evidence Presented

Wireshark was utilized to examine the data in the XYZ.pcap file and identify any unusual network activity associated with the harassing emails. By filtering SMTP transaction packets and HTTP POST requests, we were able to pinpoint crucial packets linking Johnny Coach to the emails.

5.1 Analysis of Wireshark packet captures uncovered significant network activity connecting Johnny Coach to the incident in question. Key packets that were crucial for the investigation included the following:

ID	Description	Details
80614	POST request - sendanonymousmail.net	An attempt to send an anonymous mail at sendanonymousmail.net was linked to this packet. The email originated from nobody@nitroba.org and was directed to lilytuckrige@yahoo.com, which happens to be the same address from which Lily has been receiving harassing massages.
83601	POST request - willselfdistruct.com	This packet included an extra email that was sent to lilytuckrige@yahoo.com using the self-destruting email service willselfdestruct.com.
16744	SMTP transaction - elishevet@gmail.com	This packet included details about an SMTP communication involving the email address elishevet@gmail.com. It is part of the same capture file, even though it is unrelated to Johnny Coach.
79732	SMTP transaction - jcoach@gmail.com	This packet was captured with the email address jcoach@gmail.com, leaving the evidences clearly linking directly to Johnny Coach.

5.2 Several students were using the dorm room's unsecured Wi-Fi, making it essential to pinpoint the exact device responsible for sending the emails. Wireshark packet logs revealed that the MAC address 00:17:f2:e2:c0:ce was sending HTTP POST requests to anonymous email services at the exact times the harassing emails were dispatched.

MAC Address	Description
00:17:f2:e2:c0:ce	This MAC address is linked to an Apple computer that was connected to the dorm's unprotected Wi-Fi when the emails were sent. It was found that Johnny Coach owned this device.

Since MAC addresses are unique identifiers, pinpointing this MAC address led to a successful investigation.

5.3 The network analysis is further enhanced by the findings from the email header extraction of Lily Tuckrige's Yahoo mailbox. This collection of headers contained certain metadata attributes that indicate the source of the communication:

Field	Data
Return-path	nobody@nitroba.org
Received from	140.247.62.34
Originating IP	140.247.62.34

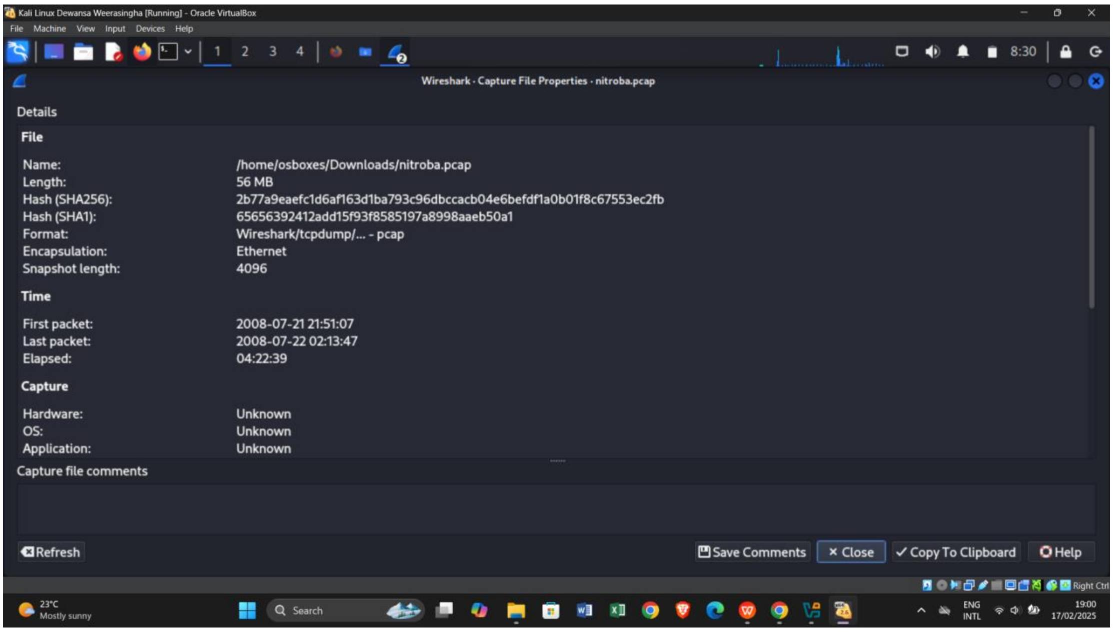
The university's IP address, along with the anonymous email provider, began to form a distinct digital fingerprint that indicated the precise source of the emails. Additionally, the same visit evidence was discovered to align with the suspect's network during the transmission

6. Conclusion

The results of a network forensic investigation indicate that Johnny Coach is responsible for harassing Lily Tuckrige through email. The investigation revealed a clear digital trail linking Johnny Coach to the emails, utilizing methods such as timestamp correlation, MAC address tracking, packet capture analysis, and examination of email headers.The research also revealed that Johnny Coach sent the harassing messages through sendanonymousmail.net and willselfdestruct.com, both of which are anonymous email services. However, investigators were able to trace the emails back to the IP address 140.247.62.34, which is linked to the university's residence hall network. They also tracked the Apple device (MAC address 00:17:f2:e2:c0:ce) that was connected to the network during the incident. This device was further connected to Johnny Coach's personal email address (jcoach@gmail.com), establishing a direct link to him. The school dorm's IP address was pinpointed as the origin, and an examination of the email headers indicated that the Stealth email service was involved. The link between the suspect and the harassment was further supported by the correlation of timestamps, which indicated that Johnny Coach's device was frequently online during those times.

7. Appendix A - List of figures

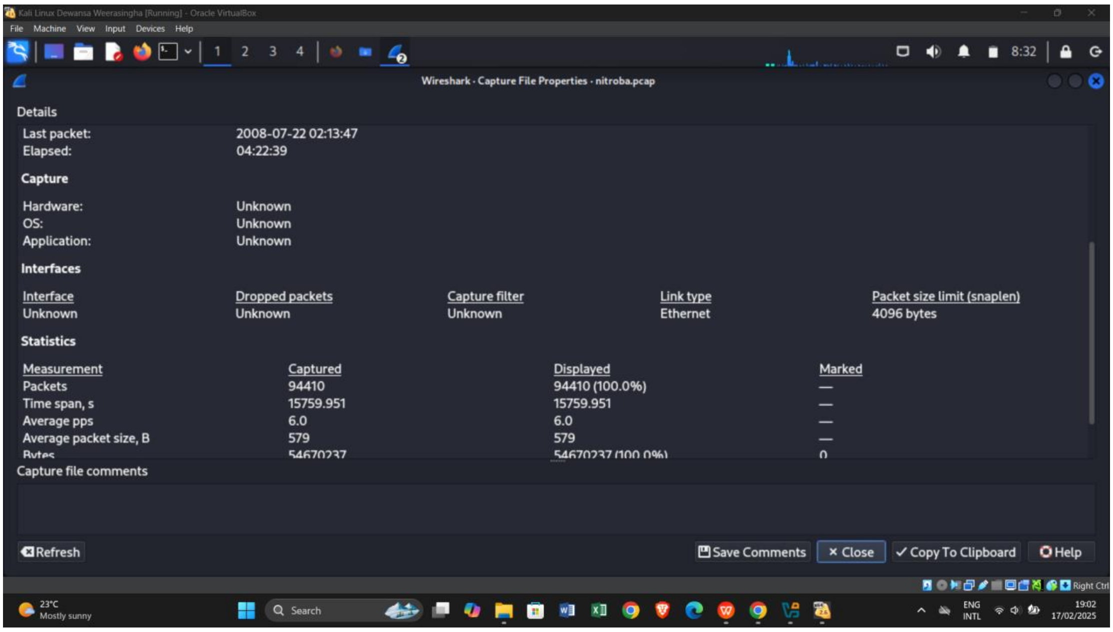
This appendix contains a complete list of the figures mentioned in the report. These figures aid the forensic investigation and provide visual evidence to back up the findings.



Kali Linux Dewansa Weerasingha [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Wireshark · Capture File Properties · nitroba.pcap
8:30
Refresh
Save Comments
Close
Copy To Clipboard
Help
Search
23°C
Mostly sunny
ENG
INTL
19:00
17/02/2025
Right Ctrl

```
Details
File
Name:                 /home/osboxes/Downloads/nitroba.pcap
Length:               56 MB
Hash (SHA256):        2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb
Hash (SHA1):          65656392412add15f93f8585197a8998aaeb50a1
Format:               Wireshark/tcpdump/... - pcap
Encapsulation:        Ethernet
Snapshot length:      4096
Time
First packet:         2008-07-21 21:51:07
Last packet:          2008-07-22 02:13:47
Elapsed:              04:22:39
Capture
Hardware:             Unknown
OS:                   Unknown
Application:          Unknown
Capture file comments
```

Figure 7.1 Wireshark - Capture File Properties



Wireshark · Capture File Properties · nitroba.pcap

Details

Last packet: 2008-07-22 02:13:47
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

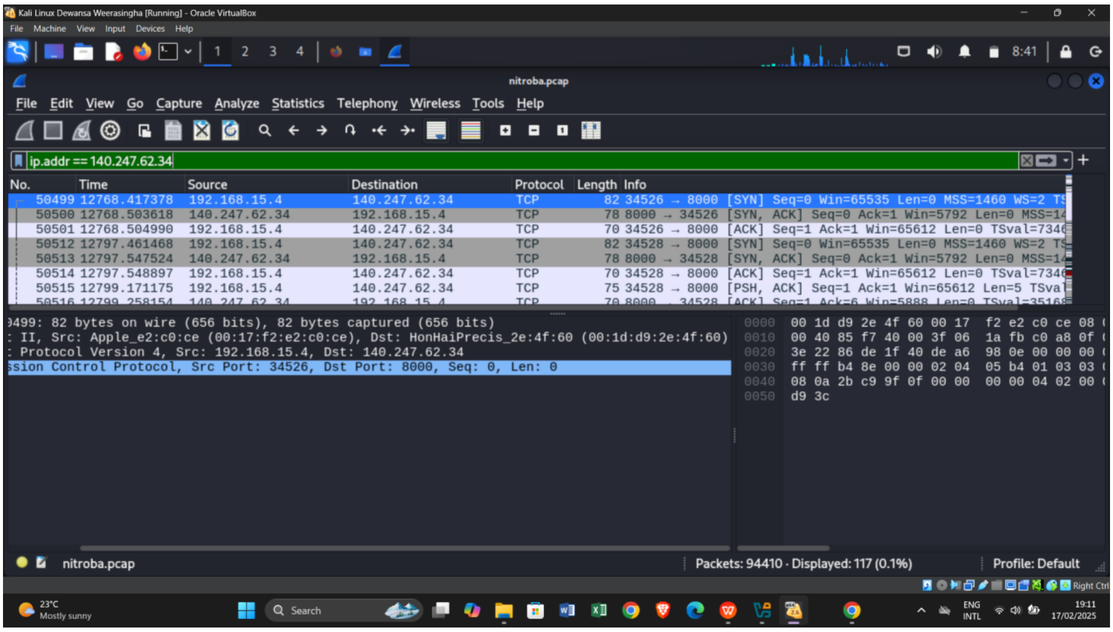
Statistics

Measurement	Captured	Displayed	Marked
Packets	94410	94410 (100.0%)	—
Time span, s	15759.951	15759.951	—
Average pps	6.0	6.0	—
Average packet size, B	579	579	—
Bytes	54670237	54670237 (100.0%)	0

Capture file comments

Figure 7.2 Wireshark - Capture File Properties (2)

Description: These two figures present a general overview of the Wireshark capture, illustrating the network traffic throughout the entire incident period. To help understand the analysis context, key information such as the total number of packets collected, average packet size, and the duration of the capture are included.


Kali Linux Dewansa Weerasingha [Running] - Oracle VirtualBox
File Machine View Input Devices Help
8:41
nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Profile: Default
23°C Mostly sunny
Search
ENG INTL
19:11 17/02/2025

ip.addr == 140.247.62.34

```
No.   Time          Source          Destination     Protocol Length Info
50499 12768.417378  192.168.15.4    140.247.62.34   TCP      82 34526 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TS
50500 12768.503618  140.247.62.34   192.168.15.4    TCP      78 8000 → 34526 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=14
50501 12768.504990  192.168.15.4    140.247.62.34   TCP      70 34526 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734
50512 12797.461468  192.168.15.4    140.247.62.34   TCP      82 34528 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TS
50513 12797.547524  140.247.62.34   192.168.15.4    TCP      78 8000 → 34528 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=14
50514 12797.548897  192.168.15.4    140.247.62.34   TCP      70 34528 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734
50515 12799.171175  192.168.15.4    140.247.62.34   TCP      75 34528 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=65612 Len=5 TSval
50516 12799.258154  140.247.62.34   192.168.15.4    TCP      70 8000 → 34528 [ACK] Seq=1 Ack=6 Win=5888 Len=0 TSval=35168
```

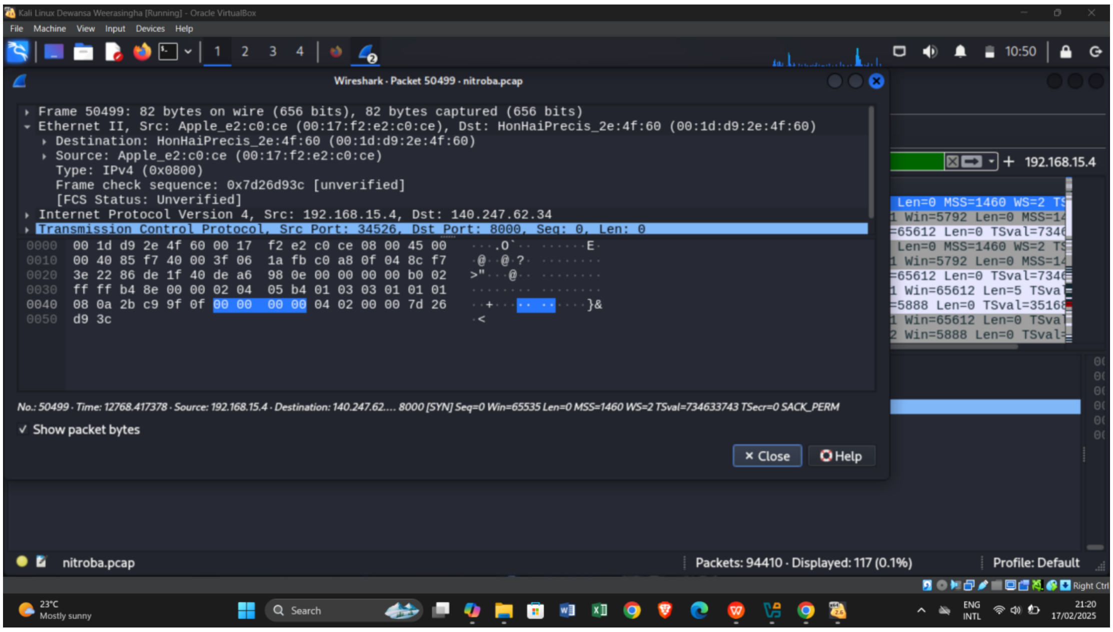
```
)499: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
: II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
: Protocol Version 4, Src: 192.168.15.4, Dst: 140.247.62.34
ssion Control Protocol, Src Port: 34526, Dst Port: 8000, Seq: 0, Len: 0
```

```
0000  00 1d d9 2e 4f 60 00 17  f2 e2 c0 ce 08
0010  00 40 85 f7 40 00 3f 06  1a fb c0 a8 0f
0020  3e 22 86 de 1f 40 de a6  98 0e 00 00 00
0030  ff ff b4 8e 00 00 02 04  05 b4 01 03 03
0040  08 0a 2b c9 9f 0f 00 00  00 00 04 02 00
0050  d9 3c
```

nitroba.pcap | Packets: 94410 · Displayed: 117 (0.1%)

Figure 7.3 Wireshark - Source's IP address

Description: The IP address 140.247.62.34 has been linked to sending harassing emails. This indicates that the emails came from the dormitory network of XYZ school, establishing a clear connection between the suspect's location and the network activity.

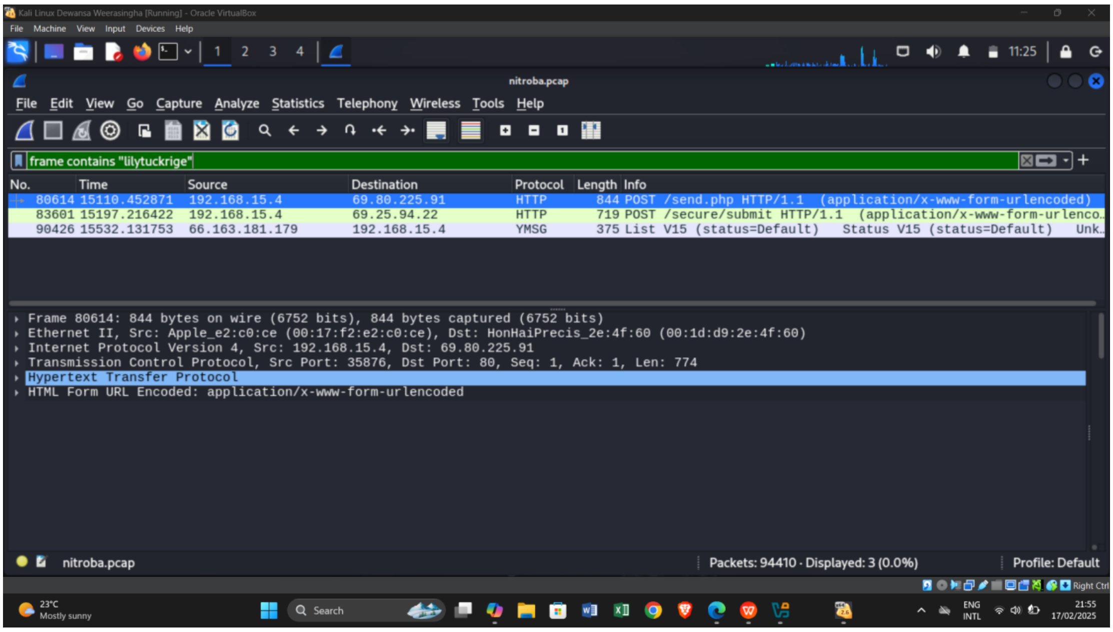


Kali Linux Dewansa Weerasingha [Running] - Oracle VirtualBox
File Machine View Input Devices Help
10:50
Wireshark · Packet 50499 · nitroba.pcap
192.168.15.4
✓ Show packet bytes
✕ Close
Help
nitroba.pcap
Packets: 94410 · Displayed: 117 (0.1%)
Profile: Default
23°C Mostly sunny
Search
ENG INTL
21:20 17/02/2025

```
Frame 50499: 82 bytes on wire (656 bits), 82 bytes captured (656 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)
  Frame check sequence: 0x7d26d93c [unverified]
  [FCS Status: Unverified]
Internet Protocol Version 4, Src: 192.168.15.4, Dst: 140.247.62.34
Transmission Control Protocol, Src Port: 34526, Dst Port: 8000, Seq: 0, Len: 0
0000  00 1d d9 2e 4f 60 00 17  f2 e2 c0 ce 08 00 45 00   ....O`.. ......E.
0010  00 40 85 f7 40 00 3f 06  1a fb c0 a8 0f 04 8c f7   .@..@.?. ........
0020  3e 22 86 de 1f 40 de a6  98 0e 00 00 00 00 b0 02   >"...@.. ........
0030  ff ff b4 8e 00 00 02 04  05 b4 01 03 03 01 01 01   ........ ........
0040  08 0a 2b c9 9f 0f 00 00  00 00 04 02 00 00 7d 26   ..+..... ......}&
0050  d9 3c                                              .<

No.: 50499 · Time: 12768.417378 · Source: 192.168.15.4 · Destination: 140.247.62.... 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734633743 TSecr=0 SACK_PERM
```

Figure 7.4 Wireshark - MAC Address

Description: This figure shows a Wireshark screenshot that captures the network activity linked to the MAC address 00:17:f2:e2:c0:ce, which has been recognized as belonging to the Apple device, captured from packet 50499

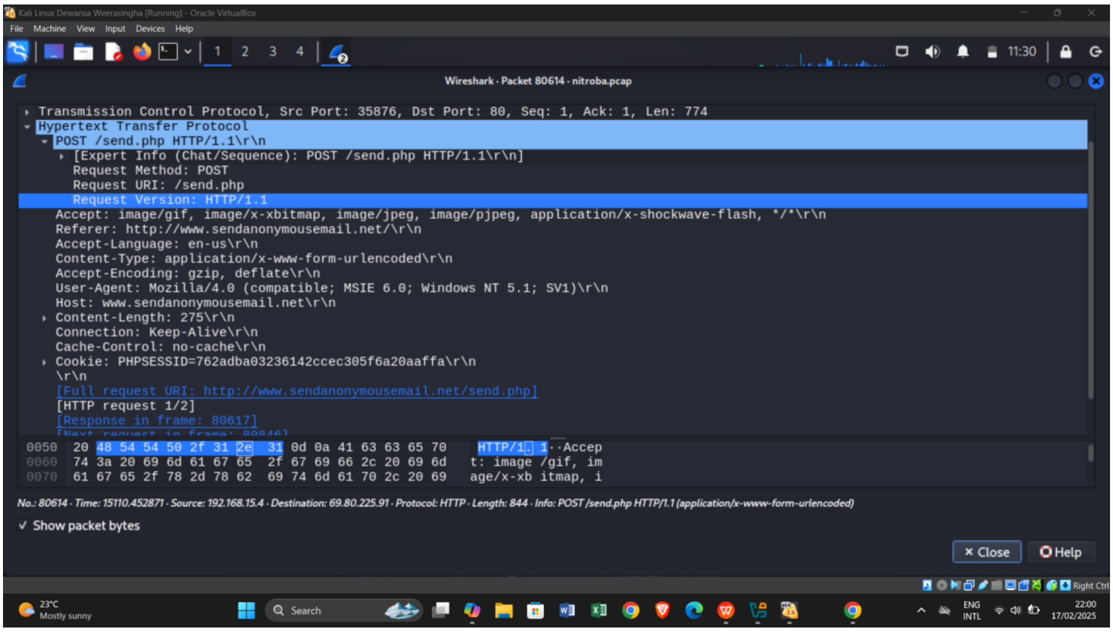


Kali Linux Dewansa Weerasingha [Running] - Oracle VirtualBox
File Machine View Input Devices Help
11:25
nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
nitroba.pcap
Packets: 94410 · Displayed: 3 (0.0%)
Profile: Default
23°C Mostly sunny
Search
ENG INTL
21:55 17/02/2025

```
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-urlenco…
90426 15532.131753  66.163.181.179  192.168.15.4    YMSG     375 List V15 (status=Default)   Status V15 (status=Default)   Unk…

Frame 80614: 844 bytes on wire (6752 bits), 844 bytes captured (6752 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)
Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.80.225.91
Transmission Control Protocol, Src Port: 35876, Dst Port: 80, Seq: 1, Ack: 1, Len: 774
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
```

Figure 7.5 Wireshark - Filtering using ‘frame contains “lilytuckrige”’

Description: The result displayed in this figure comes from the Wireshark search for frames that include the string "lilytuckrige." This string was used to identify packets linked to the harassing emails sent to Lily Tuckrige. This frame includes filtering methods to locate specific packets that contained the recipient's email address among those packets that are specifically communicating between the sender and recipient.

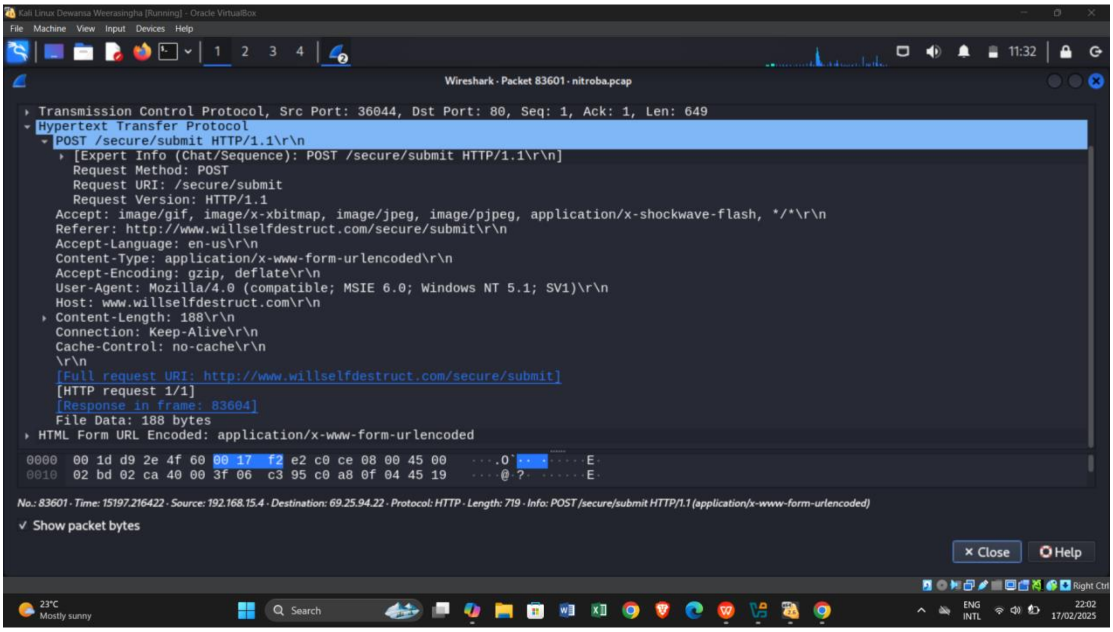


```
Wireshark · Packet 80614 · nitroba.pcap

› Transmission Control Protocol, Src Port: 35876, Dst Port: 80, Seq: 1, Ack: 1, Len: 774
⌄ Hypertext Transfer Protocol
  ⌄ POST /send.php HTTP/1.1\r\n
    › [Expert Info (Chat/Sequence): POST /send.php HTTP/1.1\r\n]
      Request Method: POST
      Request URI: /send.php
      Request Version: HTTP/1.1
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
    Referer: http://www.sendanonymousemail.net/\r\n
    Accept-Language: en-us\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: www.sendanonymousemail.net\r\n
  › Content-Length: 275\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
  › Cookie: PHPSESSID=762adba03236142ccec305f6a20aaffa\r\n
    \r\n
    [Full request URI: http://www.sendanonymousemail.net/send.php]
    [HTTP request 1/2]
    [Response in frame: 80617]

0050  20 48 54 54 50 2f 31 2e  31 0d 0a 41 63 63 65 70    HTTP/1.1··Accep
0060  74 3a 20 69 6d 61 67 65  2f 67 69 66 2c 20 69 6d   t: image /gif, im
0070  61 67 65 2f 78 2d 78 62  69 74 6d 61 70 2c 20 69   age/x-xb itmap, i

No.: 80614 · Time: 15110.452871 · Source: 192.168.15.4 · Destination: 69.80.225.91 · Protocol: HTTP · Length: 844 · Info: POST /send.php HTTP/1.1 (application/x-www-form-urlencoded)
```

Kali Linux Dewansa Weerasingha [Running] - Oracle VirtualBox
File Machine View Input Devices Help
11:30
✓ Show packet bytes
✕ Close
Help
23°C
Mostly sunny
Search
ENG
INTL
22:00
17/02/2025

Figure 7.6 Wireshark - HTTP POST request to sendanonymousmail.net

Description: This packet (80614) documents the POST request to sendanonymousmail.net, where a harassing email was sent to lilytuckrige@yahoo.com using the fake email address nobody@nitroba.org.

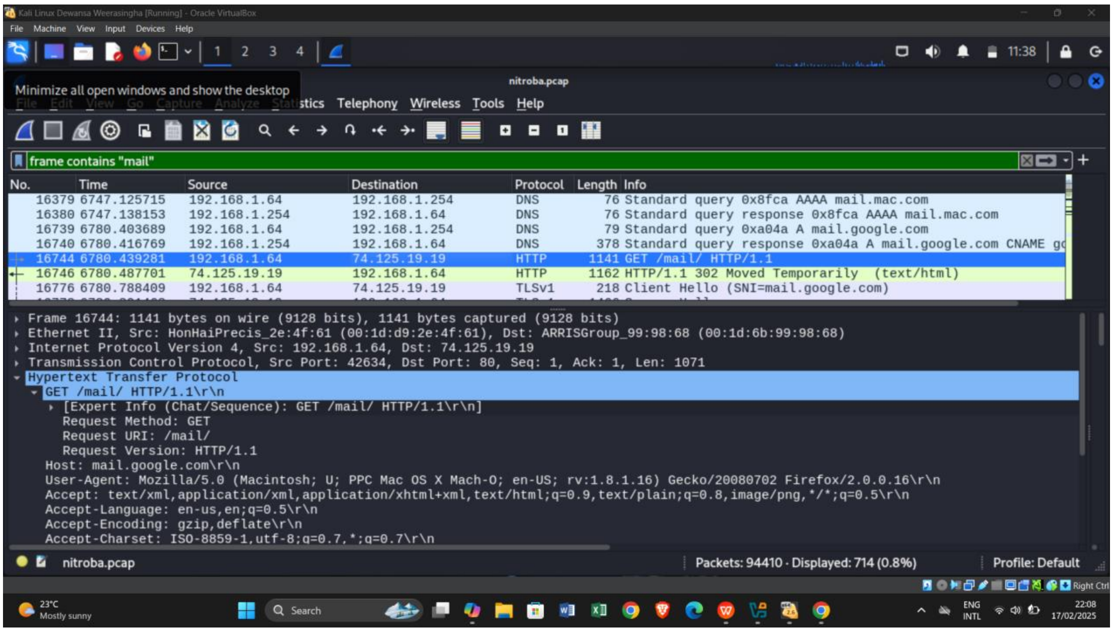


```
Wireshark · Packet 83601 · nitroba.pcap

› Transmission Control Protocol, Src Port: 36044, Dst Port: 80, Seq: 1, Ack: 1, Len: 649
⌄ Hypertext Transfer Protocol
  ⌄ POST /secure/submit HTTP/1.1\r\n
    › [Expert Info (Chat/Sequence): POST /secure/submit HTTP/1.1\r\n]
      Request Method: POST
      Request URI: /secure/submit
      Request Version: HTTP/1.1
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
    Referer: http://www.willselfdestruct.com/secure/submit\r\n
    Accept-Language: en-us\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: www.willselfdestruct.com\r\n
  › Content-Length: 188\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://www.willselfdestruct.com/secure/submit]
    [HTTP request 1/1]
    [Response in frame: 83604]
    File Data: 188 bytes
› HTML Form URL Encoded: application/x-www-form-urlencoded

0000  00 1d d9 2e 4f 60 00 17  f2 e2 c0 ce 08 00 45 00   ····.O`·· ······E·
0010  02 bd 02 ca 40 00 3f 06  c3 95 c0 a8 0f 04 45 19   ····@·?· ······E·

No.: 83601 · Time: 15197.216422 · Source: 192.168.15.4 · Destination: 69.25.94.22 · Protocol: HTTP · Length: 719 · Info: POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)
```

Kali Linux Dewansa Weerasingha [Running] - Oracle VirtualBox
File Machine View Input Devices Help
11:32
✓ Show packet bytes
✕ Close
Help
23°C
Mostly sunny
Search
ENG
INTL
22:02
17/02/2025

Figure 7.7 Wireshark - HTTP POST request to willselfdestruct.com

Description: As seen in packet 83601, Lily received the harassing message via the self-destructing email provider willselfdestruct.com. The transaction was anonymous, according to the packet.

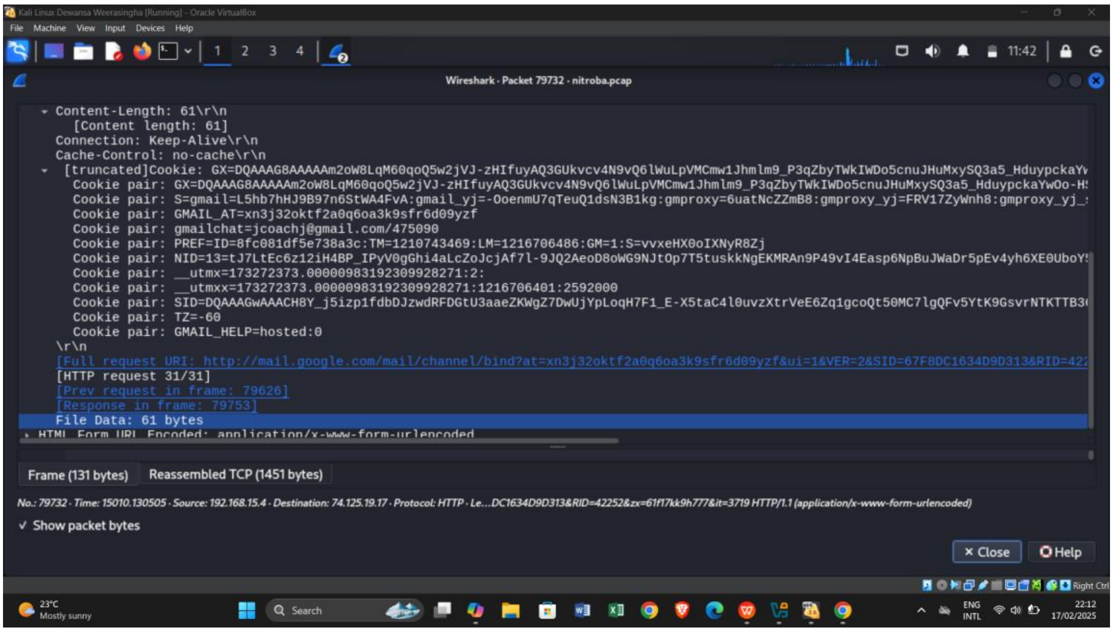


Kali Linux Dewansa Weerasingha [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Minimize all open windows and show the desktop
nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
11:38
23°C Mostly sunny
Search
ENG INTL
22:08 17/02/2025

```
frame contains "mail"

No.   Time         Source          Destination     Protocol Length Info
16379 6747.125715  192.168.1.64    192.168.1.254   DNS         76 Standard query 0x8fca AAAA mail.mac.com
16380 6747.138153  192.168.1.254   192.168.1.64    DNS         76 Standard query response 0x8fca AAAA mail.mac.com
16739 6780.403689  192.168.1.64    192.168.1.254   DNS         79 Standard query 0xa04a A mail.google.com
16740 6780.416769  192.168.1.254   192.168.1.64    DNS        378 Standard query response 0xa04a A mail.google.com CNAME go
16744 6780.439281  192.168.1.64    74.125.19.19    HTTP      1141 GET /mail/ HTTP/1.1
16746 6780.487701  74.125.19.19    192.168.1.64    HTTP      1162 HTTP/1.1 302 Moved Temporarily  (text/html)
16776 6780.788409  192.168.1.64    74.125.19.19    TLSv1      218 Client Hello (SNI=mail.google.com)

› Frame 16744: 1141 bytes on wire (9128 bits), 1141 bytes captured (9128 bits)
› Ethernet II, Src: HonHaiPrecis_2e:4f:61 (00:1d:d9:2e:4f:61), Dst: ARRISGroup_99:98:68 (00:1d:6b:99:98:68)
› Internet Protocol Version 4, Src: 192.168.1.64, Dst: 74.125.19.19
› Transmission Control Protocol, Src Port: 42634, Dst Port: 80, Seq: 1, Ack: 1, Len: 1071
⌄ Hypertext Transfer Protocol
  ⌄ GET /mail/ HTTP/1.1\r\n
    › [Expert Info (Chat/Sequence): GET /mail/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /mail/
      Request Version: HTTP/1.1
    Host: mail.google.com\r\n
    User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.1.16) Gecko/20080702 Firefox/2.0.0.16\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n

nitroba.pcap    Packets: 94410 · Displayed: 714 (0.8%)    Profile: Default
```

Figure 7.8 Wireshark - Filtering using ‘frame contains “mail”’

Description: This figure shows the outcome of the Wireshark search for frames that include the keyword "mail." This keyword was utilized to pinpoint packets related to email communications on the network. By applying this filter, it successfully narrowed down the network traffic associated with both sending and receiving emails, especially those connected to the harassing messages directed at Lily Tuckrige.



Kali Linux Dewansa Weerasingha [Running] - Oracle VirtualBox
File Machine View Input Devices Help
11:42
Wireshark · Packet 79732 · nitroba.pcap
Frame (131 bytes)
Reassembled TCP (1451 bytes)
✓ Show packet bytes
× Close
Help
23°C Mostly sunny
Search
ENG INTL
22:12 17/02/2025

```
  ⌄ Content-Length: 61\r\n
      [Content length: 61]
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
  ⌄  [truncated]Cookie: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw1Jhmlm9_P3qZbyTWkIWDo5cnuJHuMxySQ3a5_HduypckaYw
      Cookie pair: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw1Jhmlm9_P3qZbyTWkIWDo5cnuJHuMxySQ3a5_HduypckaYwOo-H
      Cookie pair: S=gmail=L5hb7hHJ9B97n6StWA4FvA:gmail_yj=-OoenmU7qTeuQ1dsN3B1kg:gmproxy=6uatNcZZmB8:gmproxy_yj=FRV17ZyWnh8:gmproxy_yj_
      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=tJ7LtEc6z12iH4BP_IPyV0gGhi4aLcZoJcjAf7l-9JQ2AeoD8oWG9NJtOp7T5tuskkNgEKMRAn9P49vI4Easp6NpBuJWaDr5pEv4yh6XE0UboY
      Cookie pair: __utmx=173272373.00000983192309928271:2:
      Cookie pair: __utmxx=173272373.00000983192309928271:1216706401:2592000
      Cookie pair: SID=DQAAAGwAAACH8Y_j5izp1fdbDJzwdRFDGtU3aaeZKWgZ7DwUjYpLoqH7F1_E-X5taC4l0uvzXtrVeE6Zq1gcoQt50MC7lgQFv5YtK9GsvrNTKTTB3
      Cookie pair: TZ=-60
      Cookie pair: GMAIL_HELP=hosted:0
    \r\n
    [Full request URI: http://mail.google.com/mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42
    [HTTP request 31/31]
    [Prev request in frame: 79626]
    [Response in frame: 79753]
    File Data: 61 bytes
 › HTML Form URL Encoded: application/x-www-form-urlencoded

No.: 79732 · Time: 15010.130505 · Source: 192.168.15.4 · Destination: 74.125.19.17 · Protocol: HTTP · Le...DC1634D9D313&RID=42252&zx=61f17kk9h777&it=3719 HTTP/1.1 (application/x-www-form-urlencoded)
```

Figure 7.9 Wireshark - SMTP Transaction involving jcoach@gmail.com

Description: The SMTP transaction details captured in Packet 79732 are shown in this figure and played a vital role in linking Johnny Coach to the harassing emails. This packet contained information about the SMTP transmission, including the sender's email address and the path the message followed.

Contribution:

Content	Zameena Sydeen	Dewansa Weerasingha
1 Executive Summary		100%
2.1 Network Capture File Details	100%	
2.2 Network Components Identified	100%	
3.1 Tools Used	100%	
3.2Steps Involved	100%	
3.3 Handling Data	100%	
4.1 Important Network Players	100%	
4.2 Network Struture	100%	
4.3 Activity Timeline for the Attack	100%	
4.4 Background Evidence		100%
5 Supporting Evidences Presented		100%
6 Conclusion		100%
7 Appendix A - List of Figures		100%