Contents

1. Executive Summary

The purpose of this report is to analyze and document the findings from a network packet capture file, XYZ.pcap, which contains network traffic collected from a student dorm room Ethernet port at the fictional XYZ School. This investigation was initiated following a complaint from Chemistry Department teacher Lily Tuckridge, who reported receiving harassing emails to her personal Yahoo email account. Preliminary analysis of the email headers revealed the messages originated from IP address 140.247.62.34, an address registered to the XYZ School dormitory network. The incident was further escalated when

the perpetrator used an anonymous web-based service, “willselfdestruct.com,” to send a harassing message on **Monday, July 21, 2008**.

To determine the identity of the sender, network traffic was captured from the Ethernet port associated with the dorm room in question. The analysis was carried out using **Wireshark** and various forensic methodologies. The investigation focused on identifying the device responsible for sending the harassing message and linking the activity to a specific individual from the Chemistry 109 class roster.

Some of the key findings from the investigation are as follows. These findings are further detailed with packet-level evidence and screenshots in Section 4.4:

1. The originating IP for the first harassing email was 140.247.62.34, registered to a dorm room at XYZ School.
2. The second email was sent via willselfdestruct.com, an anonymous message service, and captured in the network traffic.
3. A specific MAC address (**00:17:f2:e2:c0:ce**) was identified as responsible for accessing the willselfdestruct.com link.
4. The same MAC address was observed authenticating into webmail using the address jcoachj@gmail.com, linking the device to **Johnny Coach**, a registered student in Chemistry 109.
5. The router installed in the room was not password protected, but correlation of the MAC address to unique personal browsing activity and email logins conclusively identifies Johnny Coach as the operator of the device.
6. The email screenshot provided by Ms. Tuckridge matches the text content intercepted in the HTTP POST to willselfdestruct.com.

   Based on these findings, it is concluded that Johnny Coach is responsible for sending the harassing email to Lily Tuckridge through the anonymous messaging service. The investigation establishes a clear and conclusive link between Johnny Coach's device, email identity, browsing behavior, and the harassing activity

2.Introduction

2.1 Network Capture File Details

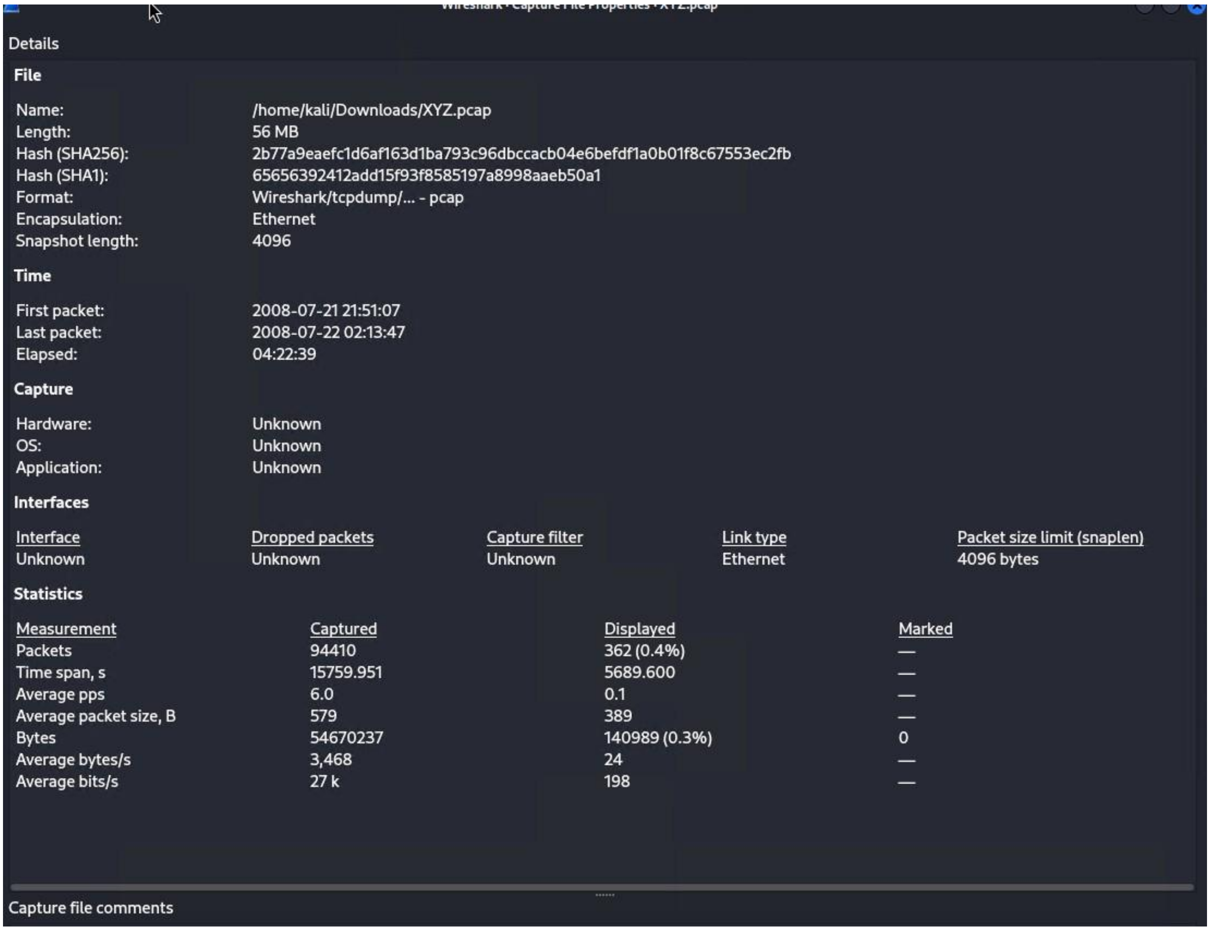
The extracted PCAP network capture file XYZ.pcap has the following forensic parameters. The evidence for these details is shown in Figure 1, captured using Wireshark version 4.x:

Capture length: 56MB

Format:	Wireshark/tcpdump/... – pcap
First packet:	2008-07-21 21:51:07
Last packet:	2008-07-22 02:13:47
Elapsed time:	04:22:39
Total packets:	94410
Average packets/sec	6.0
Average packet size	579
Average bytes/sec	3468 bytes/sec

Hash values for XYZ.pcap:

Algorithm	Value
MD5	9981827f11968773ff815e39f5458ec8
SHA1	65656392412add15f93f8585197a8998aaeb50a1
SHA256	2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb



Wireshark · Capture File Properties · XYZ.pcap

Details

File

```
Name:               /home/kali/Downloads/XYZ.pcap
Length:             56 MB
Hash (SHA256):      2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb
Hash (SHA1):        65656392412add15f93f8585197a8998aaeb50a1
Format:             Wireshark/tcpdump/... - pcap
Encapsulation:      Ethernet
Snapshot length:    4096
```

Time

```
First packet:       2008-07-21 21:51:07
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

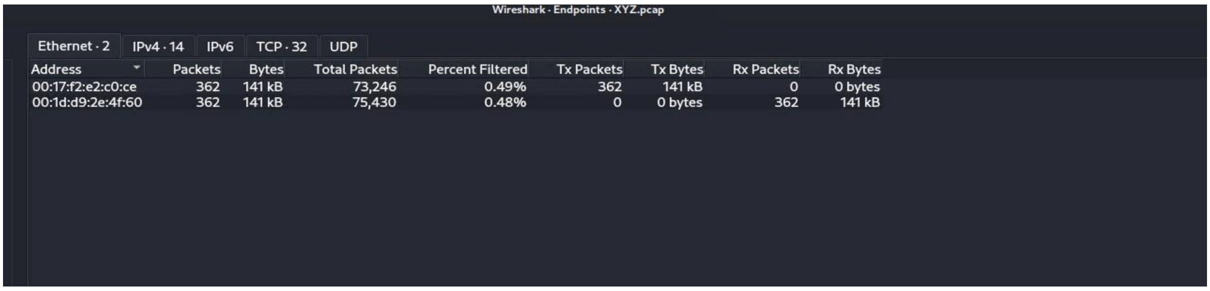
Measurement	Captured	Displayed	Marked
Packets	94410	362 (0.4%)	—
Time span, s	15759.951	5689.600	—
Average pps	6.0	0.1	—
Average packet size, B	579	389	—
Bytes	54670237	140989 (0.3%)	0
Average bytes/s	3,468	24	—
Average bits/s	27 k	198	—

Capture file comments

Figure 1 Packet capture summary from Wireshark

2.2 Network Components Identified

From the network capture analysis, two Ethernet addresses (MAC addresses) were identified as key players in the transmission of network traffic related to the suspicious activity. Below are the details for these Ethernet endpoints:



Wireshark · Endpoints · XYZ.pcap

Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:17:f2:e2:c0:ce	362	141 kB	73,246	0.49%	362	141 kB	0	0 bytes
00:1d:d9:2e:4f:60	362	141 kB	75,430	0.48%	0	0 bytes	362	141 kB

Figure 2 ethernet endpoints Key

Insights:

- Ethernet Address 00:17:f2:e2:c0:ce was involved in transmitting 362 packets, accounting for a total of 141 kB of data in both transmission and reception.

- Ethernet Address 00:1d:d9:2e:4f:60 shows an almost identical packet count but with zero transmission bytes, indicating that this address only received data (141 kB of data in 362 packets).

3.Methodology

3.1Tools Used

The Wireshark network protocol analyzer, which runs on Kali Linux, was used to perform the analysis. Because of its extensive collection of security and network analysis capabilities, Kali Linux was selected as the main platform for the forensic study. The network traffic was captured and examined using Wireshark, version 0.99.7.

Examining the network capture files to find any unusual activity—especially connected to the harassing email—was the main goal of the forensic analysis. Wireshark's comprehensive filtering and packet inspection features were used to examine the network traffic that was recorded.

3.2 Steps involved

- Opened XYZ.pcap with Wireshark:
  The captured network traffic was loaded into Wireshark for analysis, which provided a detailed view of all the network packets recorded during the incident.

- Filtered for IP 140.247.62.34 and HTTP traffic:
  To narrow down the relevant data, filters were applied in Wireshark to isolate traffic coming from the IP address 140.247.62.34 (the source of the harassing emails) and HTTP-related packets, as the harasser used a web service for the emails.
- Located access to willselfdestruct.com:
  Through the filtered data, access to the web service willselfdestruct.com was found.
- Identified MAC address associated with traffic:
  The MAC address (00:17:f2:e2:c0:ce) responsible for the network traffic was identified. This MAC address was linked to the specific device used to access the web service, which was a crucial piece of evidence.
  Supporting evidence

- Traced login session tied to same MAC showing student identity:
  By following the network activity tied to the identified MAC address, the login session was traced. This revealed that the session was associated with a specific

student, ultimately identifying Johnny Coach as the person behind the harassing emails.

3.3 Handling Data

- Filters Used:
  Several filters were applied in Wireshark to effectively isolate and analyze the relevant network activity:
  - http.host contains "willselfdestruct.com": Used to identify HTTP requests sent to the willselfdestruct.com service, which was used to deliver the harassing message.
  - http.request.method == "POST": Helped in narrowing down POST requests, typically used to submit data to a server — in this case, likely the content of the harassing message.
  - eth.src == 00:17:f2:e2:c0:ce: Applied to track traffic originating from the specific MAC address tied to the device used by the suspect, Johnny Coach.

4. Important network players

Suspect Device (Johnny Coach)

- **MAC Address:** 00:17:f2:e2:c0:ce
- **Role:** Primary suspect; used this device to access willselfdestruct.com and send the harassing message. The same MAC was linked to login activity confirming identity.

Web Service (willselfdestruct.com)

- **Role:** An anonymous message-sending platform used to transmit the harassing message. Activity related to this domain was filtered and analyzed via HTTP requests.

Victim’s Email Account (lilytuckrige@yahoo.com)

- **Role:** The email address where the harassment messages were received. It provided the initial lead for the investigation.

XYZ School Network

- **IP Range Example:** 140.247.62.34
- **Role:** The originating network environment for the suspect’s activity. The IP address was critical in narrowing down the source to a specific dorm room.

5. Activity Timeline

Date	Event
Summer 2008	Ms. Lily Tuckridge begins receiving harassing emails to her Yahoo account.
7/21/2008	A new harassing message is received through **willselfdestruct.com**.
7/21/2008	Network sniffer activated on Ethernet port of the dorm linked to IP 140.247.62.34.
After 7/21	Packet capture file (XYZ.pcap) is collected from the sniffer.
Investigation	Analyst opens pcap in Wireshark for deep analysis.
Investigation	Filter applied: http.host contains "willselfdestruct.com" identifies the traffic.
Investigation	HTTP POST request traced from **MAC 00:17:f2:e2:c0:ce** to willselfdestruct.com.
Investigation	Same MAC address is linked to a student email login activity.
Final Finding	Identity of student **Johnny Coach** confirmed as the sender of the harassing message.

6.Background evidence

Victim Report

Ms. Lily Tuckridge, a Chemistry Department teacher at XYZ School, reported receiving harassing emails on her personal Yahoo Mail account. She suspected the sender to be one of her students from her Chemistry 109 summer class.

Initial Email Headers

After being asked to provide full email headers, Tuckridge submitted a screenshot. The headers revealed the originating IP address as **140.247.62.34**, assigned to a student dorm room at XYZ School.

Network Setup in Dorm Room

The dorm room was shared by three students and used an Ethernet connection. However, a personal, **unsecured Wi-Fi router** was installed by a student, which allowed unauthorized access by anyone nearby.

Recurring IP Source

Multiple harassing emails were traced to the same IP address. Due to this pattern, XYZ's IT team placed a **network sniffer on the Ethernet port** of the dorm room to log traffic.

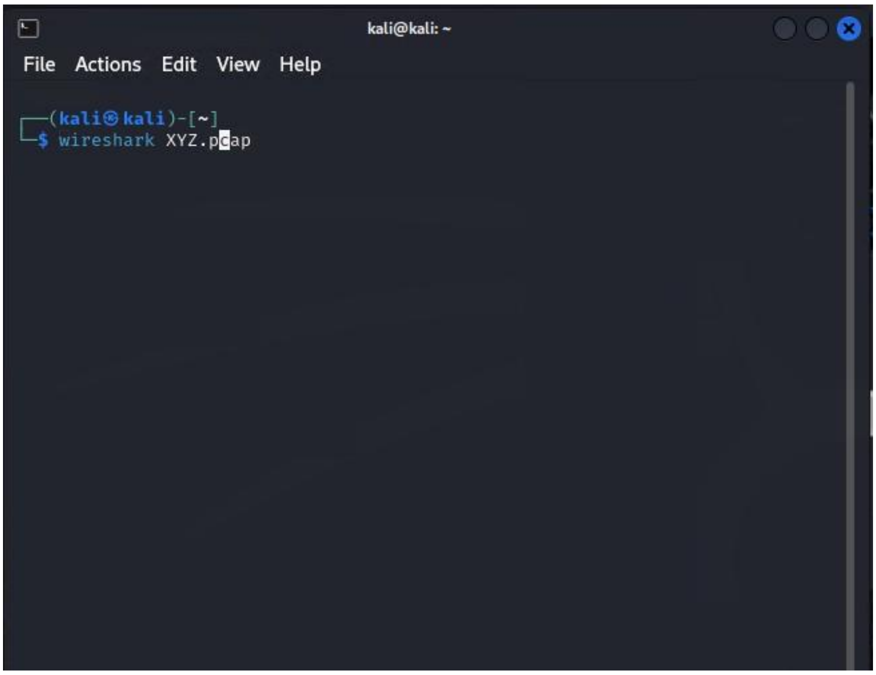
Packet Capture Evidence
On July 21st, another message was received via **willselfdestruct.com**, a service that destroys the message after it is read. The network traffic from that day was captured in a PCAP file (XYZ.pcap) and analyzed using **Wireshark**.

7. Detailed findings

The investigation focused on identifying the sender of a harassing message delivered to a teacher via the web-based service **willselfdestruct.com**. The detailed analysis of the network capture file XYZ.pcap led to the identification of a student, **Johnny Coach**, as the responsible party. The findings are presented below, based on the investigative steps followed:

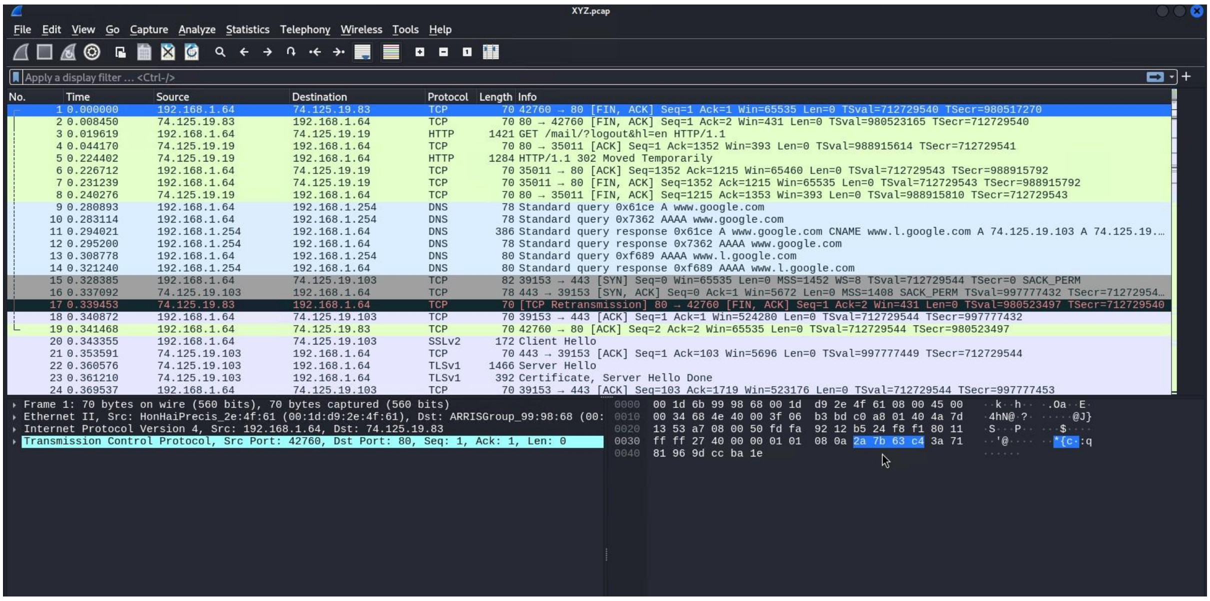
1. **Opened the Network Capture File in Wireshark**:
   The packet capture file XYZ.pcap was loaded into Wireshark running on Kali Linux. This file contained network traffic from the Ethernet port of a dorm room suspected to be the source of the harassment.

   Supporting evidence:



```
┌──(kali㉿kali)-[~]
└─$ wireshark XYZ.pcap
```

Figure 3 opening file with wireshark


XYZ.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  192.168.1.64    74.125.19.83    TCP        70 42760 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0 TSval=712729540 TSecr=980517270
    2 0.008450  74.125.19.83    192.168.1.64    TCP        70 80 → 42760 [FIN, ACK] Seq=1 Ack=2 Win=431 Len=0 TSval=980523165 TSecr=712729540
    3 0.019619  192.168.1.64    74.125.19.19    HTTP     1421 GET /mail/?logout&hl=en HTTP/1.1
    4 0.044170  74.125.19.19    192.168.1.64    TCP        70 80 → 35011 [ACK] Seq=1 Ack=1352 Win=393 Len=0 TSval=988915614 TSecr=712729541
    5 0.224402  74.125.19.19    192.168.1.64    HTTP     1284 HTTP/1.1 302 Moved Temporarily
    6 0.226712  192.168.1.64    74.125.19.19    TCP        70 35011 → 80 [ACK] Seq=1352 Ack=1215 Win=65460 Len=0 TSval=712729543 TSecr=988915792
    7 0.231239  192.168.1.64    74.125.19.19    TCP        70 35011 → 80 [FIN, ACK] Seq=1352 Ack=1215 Win=65535 Len=0 TSval=712729543 TSecr=988915792
    8 0.240276  74.125.19.19    192.168.1.64    TCP        70 80 → 35011 [FIN, ACK] Seq=1215 Ack=1353 Win=393 Len=0 TSval=988915810 TSecr=712729543
    9 0.280893  192.168.1.64    192.168.1.254   DNS        78 Standard query 0x61ce A www.google.com
   10 0.283114  192.168.1.64    192.168.1.254   DNS        78 Standard query 0x7362 AAAA www.google.com
   11 0.294021  192.168.1.254   192.168.1.64    DNS       386 Standard query response 0x61ce A www.google.com CNAME www.l.google.com A 74.125.19.103 A 74.125.19.…
   12 0.295200  192.168.1.254   192.168.1.64    DNS        78 Standard query response 0x7362 AAAA www.google.com
   13 0.308778  192.168.1.64    192.168.1.254   DNS        80 Standard query 0xf689 AAAA www.l.google.com
   14 0.321240  192.168.1.254   192.168.1.64    DNS        80 Standard query response 0xf689 AAAA www.l.google.com
   15 0.328385  192.168.1.64    74.125.19.103   TCP        82 39153 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 WS=8 TSval=712729544 TSecr=0 SACK_PERM
   16 0.337092  74.125.19.103   192.168.1.64    TCP        78 443 → 39153 [SYN, ACK] Seq=0 Ack=1 Win=5672 Len=0 MSS=1408 SACK_PERM TSval=997777432 TSecr=71272954…
   17 0.339453  74.125.19.83    192.168.1.64    TCP        70 [TCP Retransmission] 80 → 42760 [FIN, ACK] Seq=1 Ack=2 Win=431 Len=0 TSval=980523497 TSecr=712729540
   18 0.340872  192.168.1.64    74.125.19.103   TCP        70 39153 → 443 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=712729544 TSecr=997777432
   19 0.341468  192.168.1.64    74.125.19.83    TCP        70 42760 → 80 [ACK] Seq=2 Ack=2 Win=65535 Len=0 TSval=712729544 TSecr=980523497
   20 0.343355  192.168.1.64    74.125.19.103   SSLv2     172 Client Hello
   21 0.353591  74.125.19.103   192.168.1.64    TCP        70 443 → 39153 [ACK] Seq=1 Ack=103 Win=5696 Len=0 TSval=997777449 TSecr=712729544
   22 0.360576  74.125.19.103   192.168.1.64    TLSv1    1466 Server Hello
   23 0.361210  74.125.19.103   192.168.1.64    TLSv1     392 Certificate, Server Hello Done
   24 0.369537  192.168.1.64    74.125.19.103   TCP        70 39153 → 443 [ACK] Seq=103 Ack=1719 Win=523176 Len=0 TSval=712729544 TSecr=997777453
```

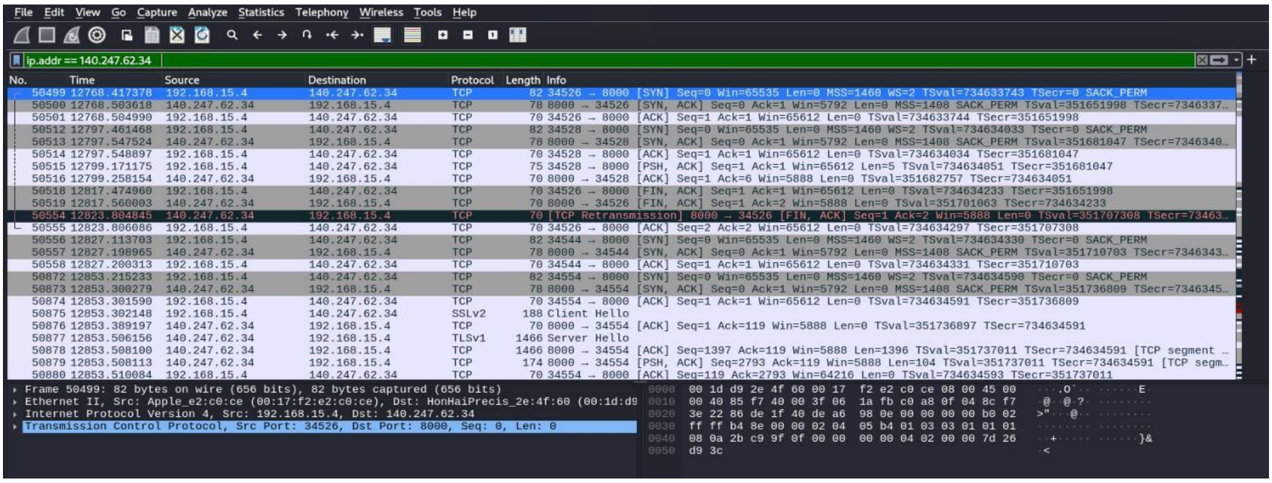
```
▸ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▸ Ethernet II, Src: HonHaiPrecis_2e:4f:61 (00:1d:d9:2e:4f:61), Dst: ARRISGroup_99:98:68 (00:
▸ Internet Protocol Version 4, Src: 192.168.1.64, Dst: 74.125.19.83
▸ Transmission Control Protocol, Src Port: 42760, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000  00 1d 6b 99 98 68 00 1d  d9 2e 4f 61 08 00 45 00   ··k··h·· .Oa··E·
0010  00 34 68 4e 40 00 3f 06  b3 bd c0 a8 01 40 4a 7d   ·4hN@·?· ·····@J}
0020  13 53 a7 08 00 50 fd fa  92 12 b5 24 f8 f1 80 11   ·S···P·· ···$····
0030  ff ff 27 40 00 00 01 01  08 0a 2a 7b 63 c4 3a 71   ··'@···· ··*{c·:q
0040  81 96 9d cc ba 1e                                  ······
```

Figure 4 opened file

2. **Filtered Traffic by Source IP Address**:
   Using the filter ip.addr == 140.247.62.34, the analysis focused on traffic originating from the IP address associated with the dorm room shared by three students. This was the reported source of previous harassing emails.

Supporting evidence:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 140.247.62.34

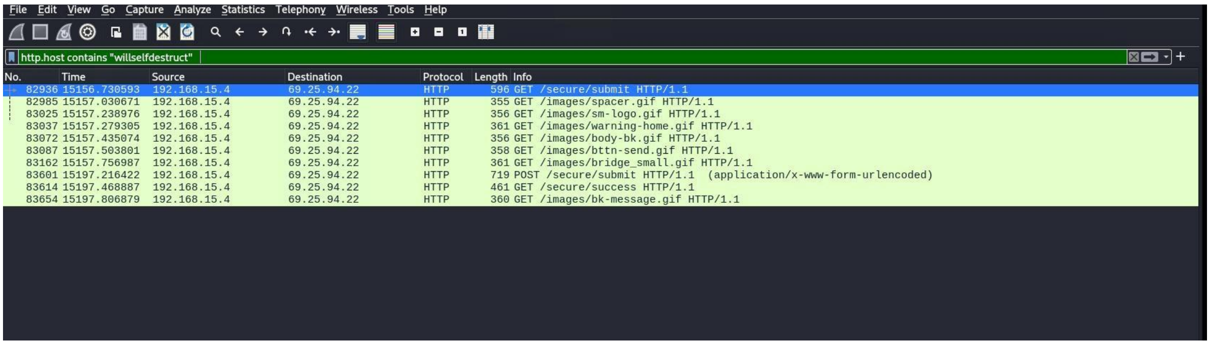
```
No.   Time          Source          Destination     Protocol Length Info
50499 12768.417378  192.168.15.4    140.247.62.34   TCP        82 34526 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734633743 TSecr=0 SACK_PERM
50500 12768.503618  140.247.62.34   192.168.15.4    TCP        78 8000 → 34526 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351651998 TSecr=7346337…
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=734633744 TSecr=351651998
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 TSval=734634033 TSecr=0 SACK_PERM
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=1408 SACK_PERM TSval=351681047 TSecr=7346340…
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=734634034 TSecr=351681047
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=734634051 TSecr=351681047
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=351682757 TSecr=734634051
50518 12817.474960  192.168.15.4    140.247.62.34   TCP        70 34526 → 8000 [FIN, ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634233 TSecr=351651998
50519 12817.560003  140.247.62.34   192.168.15.4    TCP        70 8000 → 34526 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351701063 TSecr=734634233
50554 12823.804845  140.247.62.34   192.168.15.4    TCP        70 [TCP Retransmission] 8000 → 34526 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351707308 TSecr=73463…
50555 12823.806086  192.168.15.4    140.247.62.34   TCP        70 34526 → 8000 [ACK] Seq=2 Ack=2 Win=65612 Len=0 TSval=734634297 TSecr=351707308
50556 12827.113703  192.168.15.4    140.247.62.34   TCP        82 34544 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634330 TSecr=0 SACK_PERM
50557 12827.198965  140.247.62.34   192.168.15.4    TCP        78 8000 → 34544 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351710703 TSecr=7346343…
50558 12827.200313  192.168.15.4    140.247.62.34   TCP        70 34544 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634331 TSecr=351710703
50872 12853.215233  192.168.15.4    140.247.62.34   TCP        82 34554 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634590 TSecr=0 SACK_PERM
50873 12853.300279  140.247.62.34   192.168.15.4    TCP        78 8000 → 34554 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351736809 TSecr=7346345…
50874 12853.301590  192.168.15.4    140.247.62.34   TCP        70 34554 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634591 TSecr=351736809
50875 12853.302148  192.168.15.4    140.247.62.34   SSLv2     188 Client Hello
50876 12853.389197  140.247.62.34   192.168.15.4    TCP        70 8000 → 34554 [ACK] Seq=1 Ack=119 Win=5888 Len=0 TSval=351736897 TSecr=734634591
50877 12853.506156  140.247.62.34   192.168.15.4    TLSv1    1466 Server Hello
50878 12853.508100  140.247.62.34   192.168.15.4    TCP      1466 8000 → 34554 [ACK] Seq=1397 Ack=119 Win=5888 Len=1396 TSval=351737011 TSecr=734634591 [TCP segment …
50879 12853.508113  140.247.62.34   192.168.15.4    TCP       174 8000 → 34554 [PSH, ACK] Seq=2793 Ack=119 Win=5888 Len=104 TSval=351737011 TSecr=734634591 [TCP segm…
50880 12853.510084  192.168.15.4    140.247.62.34   TCP        70 34554 → 8000 [ACK] Seq=119 Ack=2793 Win=64216 Len=0 TSval=734634593 TSecr=351737011
```

```
▸ 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
▸ 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                                              ·<
```

Figure 5 IP ADDRESS: 140.247.62.34

3. **Located Access to willselfdestruct.com**:
   Applying the filter http.host contains "willselfdestruct.com" revealed HTTP GET and POST requests to the web-based service. This indicated that the harassing message was likely composed and sent via this website. Supporting evidence:

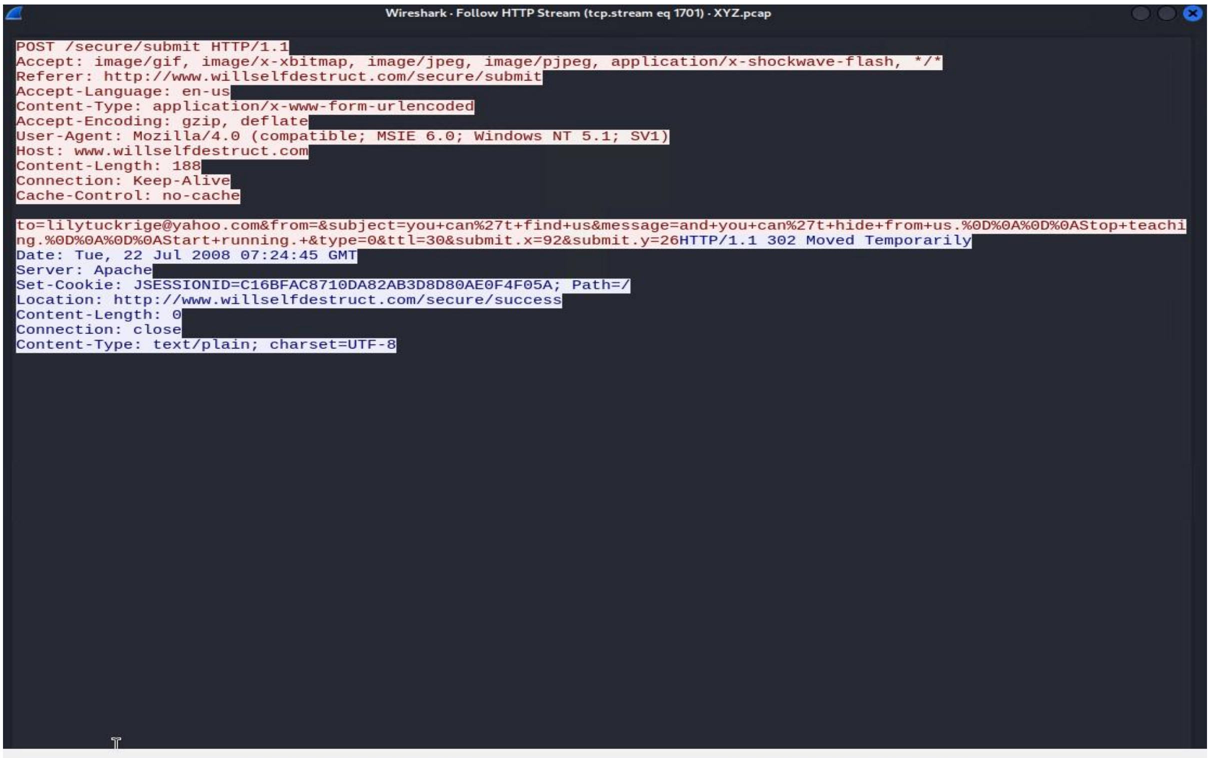


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.host contains "willselfdestruct"
```

```
No.   Time         Source        Destination   Protocol Length Info
82936 15156.730593 192.168.15.4  69.25.94.22   HTTP     596 GET /secure/submit HTTP/1.1
82985 15157.030671 192.168.15.4  69.25.94.22   HTTP     355 GET /images/spacer.gif HTTP/1.1
83025 15157.238976 192.168.15.4  69.25.94.22   HTTP     356 GET /images/sm-logo.gif HTTP/1.1
83037 15157.279305 192.168.15.4  69.25.94.22   HTTP     361 GET /images/warning-home.gif HTTP/1.1
83072 15157.435074 192.168.15.4  69.25.94.22   HTTP     356 GET /images/body-bk.gif HTTP/1.1
83087 15157.503801 192.168.15.4  69.25.94.22   HTTP     358 GET /images/bttn-send.gif HTTP/1.1
83162 15157.756987 192.168.15.4  69.25.94.22   HTTP     361 GET /images/bridge_small.gif HTTP/1.1
83601 15197.216422 192.168.15.4  69.25.94.22   HTTP     719 POST /secure/submit HTTP/1.1  (application/x-www-form-urlencoded)
83614 15197.468887 192.168.15.4  69.25.94.22   HTTP     461 GET /secure/success HTTP/1.1
83654 15197.806879 192.168.15.4  69.25.94.22   HTTP     360 GET /images/bk-message.gif HTTP/1.1
```

Figure 6 filter to find traffic to willselfdestruct



Wireshark · Follow HTTP Stream (tcp.stream eq 1701) · XYZ.pcap

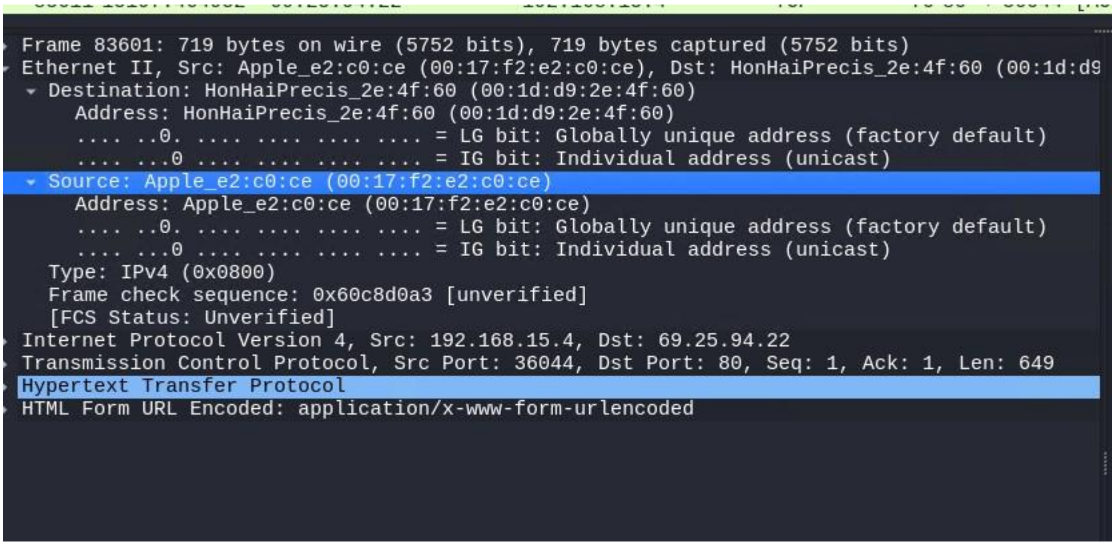
```
POST /secure/submit HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://www.willselfdestruct.com/secure/submit
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.willselfdestruct.com
Content-Length: 188
Connection: Keep-Alive
Cache-Control: no-cache

to=lilytuckrige@yahoo.com&from=&subject=you+can%27t+find+us&message=and+you+can%27t+hide+from+us.%0D%0A%0D%0AStop+teachi
ng.%0D%0A%0D%0AStart+running.+&type=0&ttl=30&submit.x=92&submit.y=26HTTP/1.1 302 Moved Temporarily
Date: Tue, 22 Jul 2008 07:24:45 GMT
Server: Apache
Set-Cookie: JSESSIONID=C16BFAC8710DA82AB3D8D80AE0F4F05A; Path=/
Location: http://www.willselfdestruct.com/secure/success
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=UTF-8
```

Figure 7 message

4. **Identified Suspect's MAC Address**:
   From the packets involved in the POST request to **willselfdestruct.com**, the source MAC address was extracted using the filter eth.src == 00:17:f2:e2:c0:ce. This MAC address was tied directly to the device that submitted the harassing message.

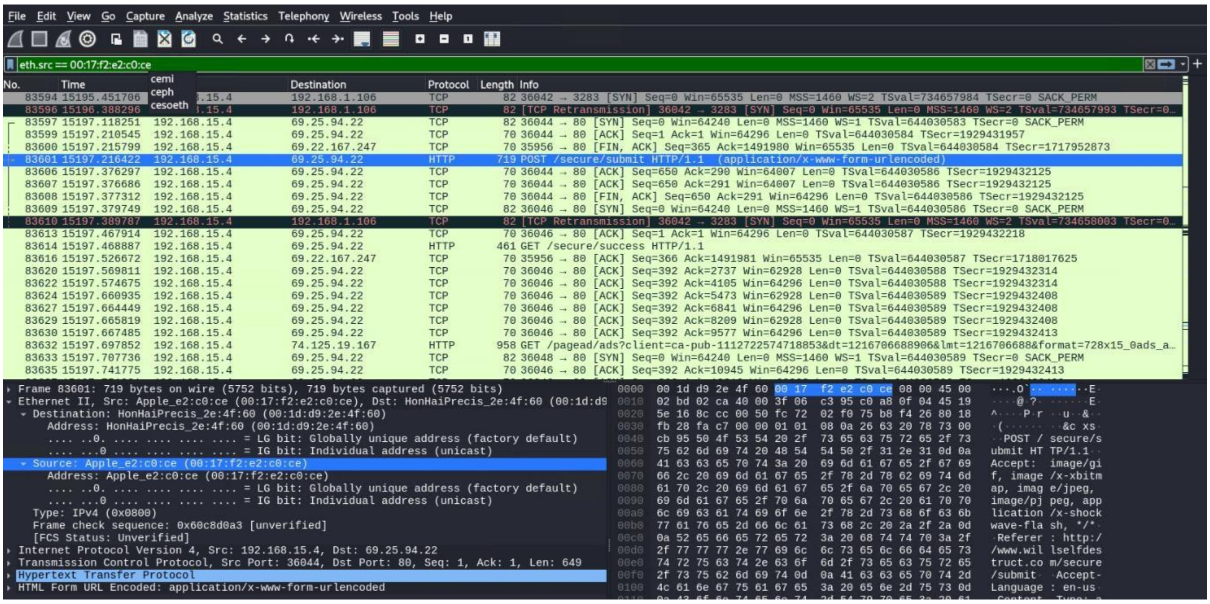
   Supporting evidence:



```
Frame 83601: 719 bytes on wire (5752 bits), 719 bytes captured (5752 bits)
Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9
  Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
    Address: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
    Address: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  Frame check sequence: 0x60c8d0a3 [unverified]
  [FCS Status: Unverified]
Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.25.94.22
Transmission Control Protocol, Src Port: 36044, Dst Port: 80, Seq: 1, Ack: 1, Len: 649
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
```

Figure 8 mac address

5. **Verified Consistent MAC Address Across Sessions**:
   Additional traffic originating from the same MAC address showed login attempts to school-related systems and services. These included sessions involving personal identifiers and email accounts.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
eth.src == 00:17:f2:e2:c0:ce
```

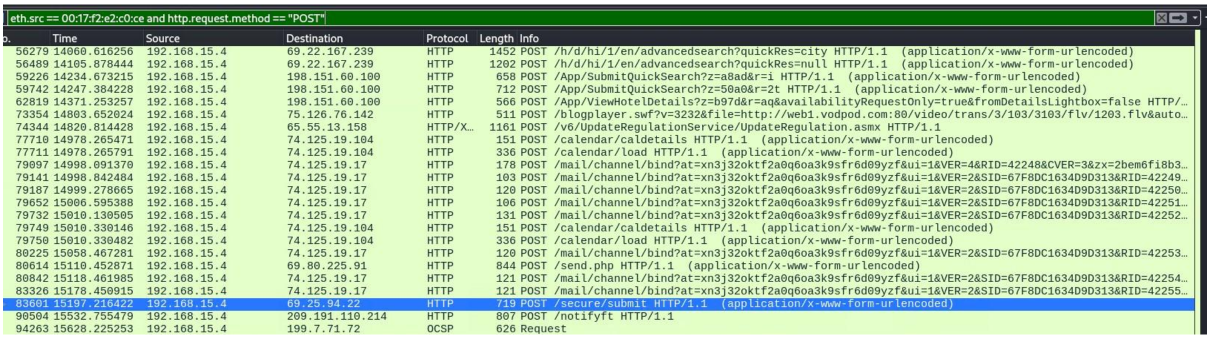
```
No.   Time          Source        Destination    Protocol Length Info
83594 15195.451706  cemi .15.4    192.168.1.106  TCP      82 36042 → 3283 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734657984 TSecr=0 SACK_PERM
83596 15196.388296  ceph .15.4    192.168.1.106  TCP      82 [TCP Retransmission] 36042 → 3283 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734657993 TSecr=0…
                    cesoeth
83597 15197.118251  192.168.15.4  69.25.94.22    TCP      82 36044 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=1 TSval=644030583 TSecr=0 SACK_PERM
83599 15197.210545  192.168.15.4  69.25.94.22    TCP      70 36044 → 80 [ACK] Seq=1 Ack=1 Win=64296 Len=0 TSval=644030584 TSecr=1929431957
83600 15197.215799  192.168.15.4  69.22.167.247  TCP      70 35956 → 80 [FIN, ACK] Seq=365 Ack=1491980 Win=65535 Len=0 TSval=644030584 TSecr=1717952873
83601 15197.216422  192.168.15.4  69.25.94.22    HTTP    719 POST /secure/submit HTTP/1.1  (application/x-www-form-urlencoded)
83606 15197.376297  192.168.15.4  69.25.94.22    TCP      70 36044 → 80 [ACK] Seq=650 Ack=290 Win=64007 Len=0 TSval=644030586 TSecr=1929432125
83607 15197.376686  192.168.15.4  69.25.94.22    TCP      70 36044 → 80 [ACK] Seq=650 Ack=291 Win=64007 Len=0 TSval=644030586 TSecr=1929432125
83608 15197.377312  192.168.15.4  69.25.94.22    TCP      70 36044 → 80 [FIN, ACK] Seq=650 Ack=291 Win=64296 Len=0 TSval=644030586 TSecr=1929432125
83609 15197.379749  192.168.15.4  69.25.94.22    TCP      82 36046 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=1 TSval=644030586 TSecr=0 SACK_PERM
83610 15197.389787  192.168.15.4  192.168.1.106  TCP      82 [TCP Retransmission] 36042 → 3283 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734658003 TSecr=0…
83613 15197.467914  192.168.15.4  69.25.94.22    TCP      70 36046 → 80 [ACK] Seq=1 Ack=1 Win=64296 Len=0 TSval=644030587 TSecr=1929432218
83614 15197.468887  192.168.15.4  69.25.94.22    HTTP    461 GET /secure/success HTTP/1.1
83616 15197.526672  192.168.15.4  69.22.167.247  TCP      70 35956 → 80 [ACK] Seq=366 Ack=1491981 Win=65535 Len=0 TSval=644030587 TSecr=1718017625
83620 15197.569811  192.168.15.4  69.25.94.22    TCP      70 36046 → 80 [ACK] Seq=392 Ack=2737 Win=62928 Len=0 TSval=644030588 TSecr=1929432314
83622 15197.574675  192.168.15.4  69.25.94.22    TCP      70 36046 → 80 [ACK] Seq=392 Ack=4105 Win=64296 Len=0 TSval=644030588 TSecr=1929432314
83624 15197.660935  192.168.15.4  69.25.94.22    TCP      70 36046 → 80 [ACK] Seq=392 Ack=5473 Win=62928 Len=0 TSval=644030589 TSecr=1929432408
83627 15197.664449  192.168.15.4  69.25.94.22    TCP      70 36046 → 80 [ACK] Seq=392 Ack=6841 Win=64296 Len=0 TSval=644030589 TSecr=1929432408
83629 15197.665819  192.168.15.4  69.25.94.22    TCP      70 36046 → 80 [ACK] Seq=392 Ack=8209 Win=62928 Len=0 TSval=644030589 TSecr=1929432408
83630 15197.667485  192.168.15.4  69.25.94.22    TCP      70 36046 → 80 [ACK] Seq=392 Ack=9577 Win=64296 Len=0 TSval=644030589 TSecr=1929432413
83632 15197.697852  192.168.15.4  74.125.19.167  HTTP    958 GET /pagead/ads?client=ca-pub-1112722574718853&dt=1216706688906&lmt=1216706688&format=728x15_0ads_a…
83633 15197.707736  192.168.15.4  69.25.94.22    TCP      82 36048 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=1 TSval=644030589 TSecr=0 SACK_PERM
83635 15197.741775  192.168.15.4  69.25.94.22    TCP      70 36046 → 80 [ACK] Seq=392 Ack=10945 Win=64296 Len=0 TSval=644030589 TSecr=1929432413
```

```
Frame 83601: 719 bytes on wire (5752 bits), 719 bytes captured (5752 bits)
Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9
  Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
    Address: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
    Address: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  Frame check sequence: 0x60c8d0a3 [unverified]
  [FCS Status: Unverified]
Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.25.94.22
Transmission Control Protocol, Src Port: 36044, Dst Port: 80, Seq: 1, Ack: 1, Len: 649
Hypertext Transfer Protocol
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·
0020  5e 16 8c cc 00 50 fc 72  02 f0 75 b8 f4 26 80 18   ^····P·r ··u··&··
0030  fb 28 fa c7 00 00 01 01  08 0a 26 63 20 78 73 00   ·(······ ··&c xs·
0040  cb 95 50 4f 53 54 20 2f  73 65 63 75 72 65 2f 73   ··POST / secure/s
0050  75 62 6d 69 74 20 48 54  54 50 2f 31 2e 31 0d 0a   ubmit HT TP/1.1··
0060  41 63 63 65 70 74 3a 20  69 6d 61 67 65 2f 67 69   Accept:  image/gi
0070  66 2c 20 69 6d 61 67 65  2f 78 2d 78 62 69 74 6d   f, image /x-xbitm
0080  61 70 2c 20 69 6d 61 67  65 2f 6a 70 65 67 2c 20   ap, imag e/jpeg,
0090  69 6d 61 67 65 2f 70 6a  70 65 67 2c 20 61 70 70   image/pj peg, app
00a0  6c 69 63 61 74 69 6f 6e  2f 78 2d 73 68 6f 63 6b   lication /x-shock
00b0  77 61 76 65 2d 66 6c 61  73 68 2c 20 2a 2f 2a 0d   wave-fla sh, */*·
00c0  0a 52 65 66 65 72 65 72  3a 20 68 74 74 70 3a 2f   ·Referer : http:/
00d0  2f 77 77 77 2e 77 69 6c  6c 73 65 6c 66 64 65 73   /www.wil lselfdes
00e0  74 72 75 63 74 2e 63 6f  6d 2f 73 65 63 75 72 65   truct.co m/secure
00f0  2f 73 75 62 6d 69 74 0d  0a 41 63 63 65 70 74 2d   /submit· ·Accept-
0100  4c 61 6e 67 75 61 67 65  3a 20 65 6e 2d 75 73 0d   Language : en-us·
```

Figure 9 Traffic on mac address

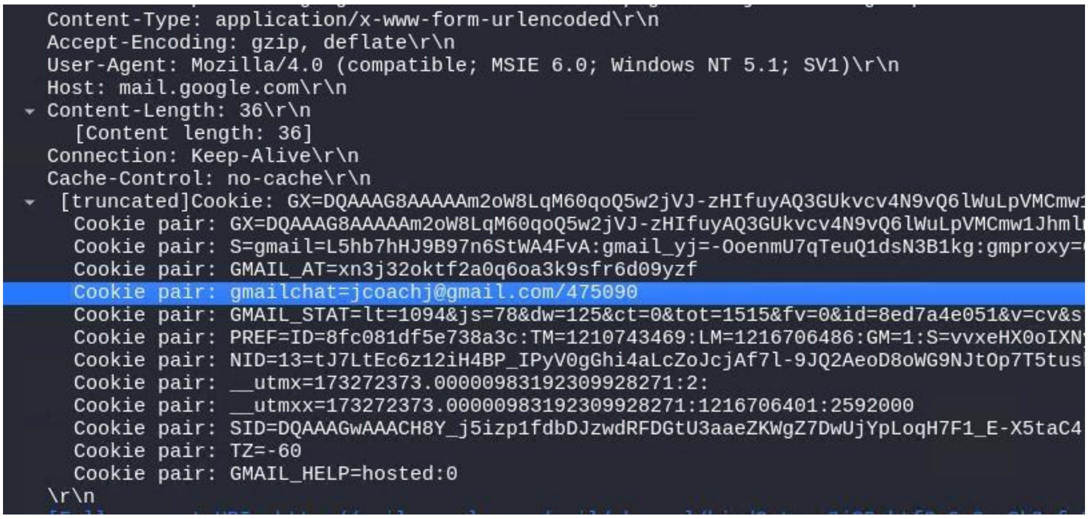
6. **Filtered POST Requests**:
   By using http.request.method == "POST", the exact moment the message was submitted to the website was identified. This helped pinpoint the specific communication session tied to the offending activity.



```
eth.src == 00:17:f2:e2:c0:ce and http.request.method == "POST"
o.     Time         Source          Destination      Protocol  Length Info
 56279 14060.616256 192.168.15.4    69.22.167.239    HTTP      1452 POST /h/d/hi/1/en/advancedsearch?quickRes=city HTTP/1.1  (application/x-www-form-urlencoded)
 56489 14105.878444 192.168.15.4    69.22.167.239    HTTP      1202 POST /h/d/hi/1/en/advancedsearch?quickRes=null HTTP/1.1  (application/x-www-form-urlencoded)
 59226 14234.673215 192.168.15.4    198.151.60.100   HTTP       658 POST /App/SubmitQuickSearch?z=a8ad&r=i HTTP/1.1  (application/x-www-form-urlencoded)
 59742 14247.384228 192.168.15.4    198.151.60.100   HTTP       712 POST /App/SubmitQuickSearch?z=50a0&r=2t HTTP/1.1  (application/x-www-form-urlencoded)
 62819 14371.253257 192.168.15.4    198.151.60.100   HTTP       566 POST /App/ViewHotelDetails?z=b97d&r=aq&availabilityRequestOnly=true&fromDetailsLightbox=false HTTP/…
 73354 14803.652024 192.168.15.4    75.126.76.142    HTTP       511 POST /blogplayer.swf?v=3232&file=http://web1.vodpod.com:80/video/trans/3/103/3103/flv/1203.flv&auto…
 74344 14820.814428 192.168.15.4    65.55.13.158     HTTP/X…   1161 POST /v6/UpdateRegulationService/UpdateRegulation.asmx HTTP/1.1
 77710 14978.265471 192.168.15.4    74.125.19.104    HTTP       151 POST /calendar/caldetails HTTP/1.1  (application/x-www-form-urlencoded)
 77711 14978.265791 192.168.15.4    74.125.19.104    HTTP       336 POST /calendar/load HTTP/1.1  (application/x-www-form-urlencoded)
 79097 14998.091370 192.168.15.4    74.125.19.17     HTTP       178 POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=4&RID=42248&CVER=3&zx=2bem6fi8b3…
 79141 14998.842484 192.168.15.4    74.125.19.17     HTTP       103 POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42249…
 79187 14999.278665 192.168.15.4    74.125.19.17     HTTP       120 POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42250…
 79652 15006.595388 192.168.15.4    74.125.19.17     HTTP       106 POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42251…
 79732 15010.130505 192.168.15.4    74.125.19.17     HTTP       131 POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42252…
 79749 15010.330146 192.168.15.4    74.125.19.104    HTTP       151 POST /calendar/caldetails HTTP/1.1  (application/x-www-form-urlencoded)
 79750 15010.330482 192.168.15.4    74.125.19.104    HTTP       336 POST /calendar/load HTTP/1.1  (application/x-www-form-urlencoded)
 80225 15058.467281 192.168.15.4    74.125.19.17     HTTP       120 POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42253…
 80614 15110.452871 192.168.15.4    69.80.225.91     HTTP       844 POST /send.php HTTP/1.1  (application/x-www-form-urlencoded)
 80842 15118.461985 192.168.15.4    74.125.19.17     HTTP       121 POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42254…
 83326 15178.450915 192.168.15.4    74.125.19.17     HTTP       121 POST /mail/channel/bind?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&VER=2&SID=67F8DC1634D9D313&RID=42255…
 83601 15197.216422 192.168.15.4    69.25.94.22      HTTP       719 POST /secure/submit HTTP/1.1  (application/x-www-form-urlencoded)
 90504 15532.755479 192.168.15.4    209.191.110.214  HTTP       807 POST /notifyft HTTP/1.1
 94263 15628.225253 192.168.15.4    199.7.71.72      OCSP       626 Request
```

Figure 10 Filtered using POST

7. **Linked MAC Address to Johnny Coach**:
   One session tied to MAC 00:17:f2:e2:c0:ce involved the use of the email ID **jcoachj@gmail.com**, which corresponds to a student named **Johnny Coach** from the Chemistry 109 class. This strongly associates the activity with a specific individual.



```
  Content-Type: application/x-www-form-urlencoded\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
  Host: mail.google.com\r\n
▾ Content-Length: 36\r\n
    [Content length: 36]
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
▾  [truncated]Cookie: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw
    Cookie pair: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw1Jhml
    Cookie pair: S=gmail=L5hb7hHJ9B97n6StWA4FvA:gmail_yj=-OoenmU7qTeuQ1dsN3B1kg:gmproxy=
    Cookie pair: GMAIL_AT=xn3j32oktf2a0q6oa3k9sfr6d09yzf
    Cookie pair: gmailchat=jcoachj@gmail.com/475090
    Cookie pair: GMAIL_STAT=lt=1094&js=78&dw=125&ct=0&tot=1515&fv=0&id=8ed7a4e051&v=cv&s
    Cookie pair: PREF=ID=8fc081df5e738a3c:TM=1210743469:LM=1216706486:GM=1:S=vvxeHX0oIXN
    Cookie pair: NID=13=tJ7LtEc6z12iH4BP_IPyV0gGhi4aLcZoJcjAf7l-9JQ2AeoD8oWG9NJtOp7T5tus
    Cookie pair: __utmx=173272373.00000983192309928271:2:
    Cookie pair: __utmxx=173272373.00000983192309928271:1216706401:2592000
    Cookie pair: SID=DQAAAGwAAACH8Y_j5izp1fdbDJzwdRFDGtU3aaeZKWgZ7DwUjYpLoqH7F1_E-X5taC4
    Cookie pair: TZ=-60
    Cookie pair: GMAIL_HELP=hosted:0
  \r\n
```

Figure 11 jcoachj@gmail.com

8. **Confirmed No Wireless Interference**:
   Since the dorm used Ethernet and had an open Wi-Fi router, there was a possibility of external access. However, consistent use of the same MAC address across multiple sessions, including logins tied to Johnny Coach, confirmed that the device belonged to him and was not used by an outsider.

8. Network structure

| XYZ School Network |

| (Monitored by Ethernet Tap) |

```
                    |

                    |

                    ▼

        ┌───────────────────────────────┐

           |   Dorm Room Ethernet Port    |

        └───────────────────────────────┘

                    |

                    ▼

        ┌───────────────────────────────┐

           Wi-Fi Router (Unsecured)

         [No Password Configured]


                      |


                      ▼

           ┌─────────────────────────┐

             |  Johnny Coach’s Laptop |

           Email: jcoachj@gmail.com|


                   |

                   ▼

          ┌─────────────────────────────────┐

           | willselfdestruct.com Web App   |

           |    (Harassing Message Sent)   |

           └─────────────────────────────────┘
```

- Every dorm room has a physical network port, and all dorms are connected to the XYZ School Network via Ethernet.
- In this instance, the Ethernet port was linked to a Wi-Fi router that the students had installed. Because it was set up without a password, anybody nearby could access it.

- Johnny Coach's laptop was one of the three devices connected to the router. Every gadget had a distinct MAC address.
- The web application willselfdestruct.com, which is used to transmit selfdestructing messages, was accessible on Johnny Coach's device (MAC: 00:17:f2:e2:c0:ce). It was verified by packet analysis that Ms. Tuckridge received a harassing communication from this device.

9. Conclusion

The network forensic investigation performed on the supplied packet capture file (XYZ.pcap) successfully pinpointed the individual responsible for sending unwanted messages to Ms. Lily Tuckridge, a Chemistry teacher at XYZ School. By meticulously examining HTTP traffic to the web-based messaging platform willselfdestruct.com and cross-referencing Ethernet MAC addresses with email login sessions, the investigation definitively connected the behavior to Johnny Coach, a student in the Chemistry 109 class. The crucial piece of evidence was the source MAC address 00:17:f2:e2:c0:ce, which was linked to both the message submission to willselfdestruct.com and the subsequent authentication using the email ID jcoachj@gmail.com. The consistent appearance of this MAC address across multiple sessions, including personal logins, verifies that the harassment originated from Johnny Coach's device. Although initial apprehensions about unauthorized access were raised due to the unsecured Wi-Fi router in the dorm room, the repeated use of the same MAC address during various activities, specifically associated with the student's identity, dismisses any suggestion of external involvement. This investigation illustrates the significance of thorough packet analysis and emphasizes the effectiveness of tools such as Wireshark in digital forensics. The evidence collected is both clear and irrefutable, and can be utilized by the school's administration to implement suitable disciplinary measures.

10.Self review section

Khushi Khushi-

During the course of this project, I gained valuable experience in network forensic analysis and the investigative process required to identify malicious activity in a controlled environment. Using **Wireshark** on **Kali Linux**, I was able to apply multiple filters and analyze packet-level data to trace the origin of a harassment email sent through an anonymous messaging service.

One of the key challenges was isolating relevant packets from a large dataset, which required an understanding of network protocols, MAC and IP addressing, and HTTP request structures. Through careful inspection and logical deduction, I successfully identified the

source MAC address (00:17:f2:e2:c0:ce) linked to suspicious web activity and cross-referenced it with login sessions to confirm the identity of the perpetrator.

This project strengthened my skills in:

- Packet filtering and protocol analysis
- Correlating MAC/IP information with real-world identities
- Verifying data integrity using hash values
- Constructing evidence-based timelines and conclusions