Network Packet Capture Analysis Report

XYZ School

Date of Investigation: 16/02/2025

Executive Summary

The purpose of this report is to analyze and report the contents of a network capture file xyz.pcap, which is an archive containing the network-based activities monitored on a given network. This file was extracted to xyz.pcap on a local hard drive before conducting the analysis. The network is reported to contain the activities of an individual operating with an IP address 192.168.15.4 on a host network. The analysis attempts to reconstruct the structure of the network, identify key participants, and determine all activities leading to and occurring during the reported suspicious activity. The analysis was conducted mainly using network forensic tools such as Wireshark. Some key findings from the analysis are listed below. Each of these findings has been elaborated with supporting evidence in Section 4.4.

1. There are 17 active Ethernet components detected in the network. The most significant were HonHaiPrecision (Foxconn) routers and an Apple device (MAC: e2:c0:ce, IP: 192.168.15.4).
2. The Apple device (192.168.15.4) was a major participant in network communications, frequently accessing external domains.
3. The 192.168.15.1 IP was identified as a Wi-Fi router that managed most of the network traffic.
4. Based on DNS response analysis, the suspect appeared to be accessing external web services frequently.
5. The suspect's computer runs a Windows-based OS and uses Mozilla Firefox as the primary browser.
6. The suspect visited willselfdestruct.com, a self-destructing messaging service, and sent an HTTP POST request shortly before the suspicious activity was reported.
7. Forensic packet analysis revealed the suspect's Gmail ID: jcoachj@gmail.com, linking Johnny Coach to the case.
8. The suspect's device (LAPTOP01) was found to be actively browsing Gmail and willselfdestruct.com, indicating potential message transmission.
9. A keyword search for "willselfdestruct" in the network logs confirmed the suspect's intent to send a self-destructing message.
10. No external intrusion attempts were detected, confirming that the activity originated from within the monitored network.
11. The suspect's computer was involved in HTTP traffic exchanges with external servers, suggesting potential security risks.
12. The analysis indicates that the suspect may have bypassed certain security controls to send the message anonymously.
13. The investigation suggests that the suspect used an unencrypted method to communicate, which was intercepted through packet analysis.
14. No clear signs of malware or remote control activity were found, reinforcing that the suspect's actions were intentional.

Based on the forensic evidence, it is concluded that Johnny Coach was responsible for the transmission of the threatening message. The investigation highlights the need for

enhanced network monitoring, encryption enforcement, and stricter access controls to prevent similar incidents in the future.

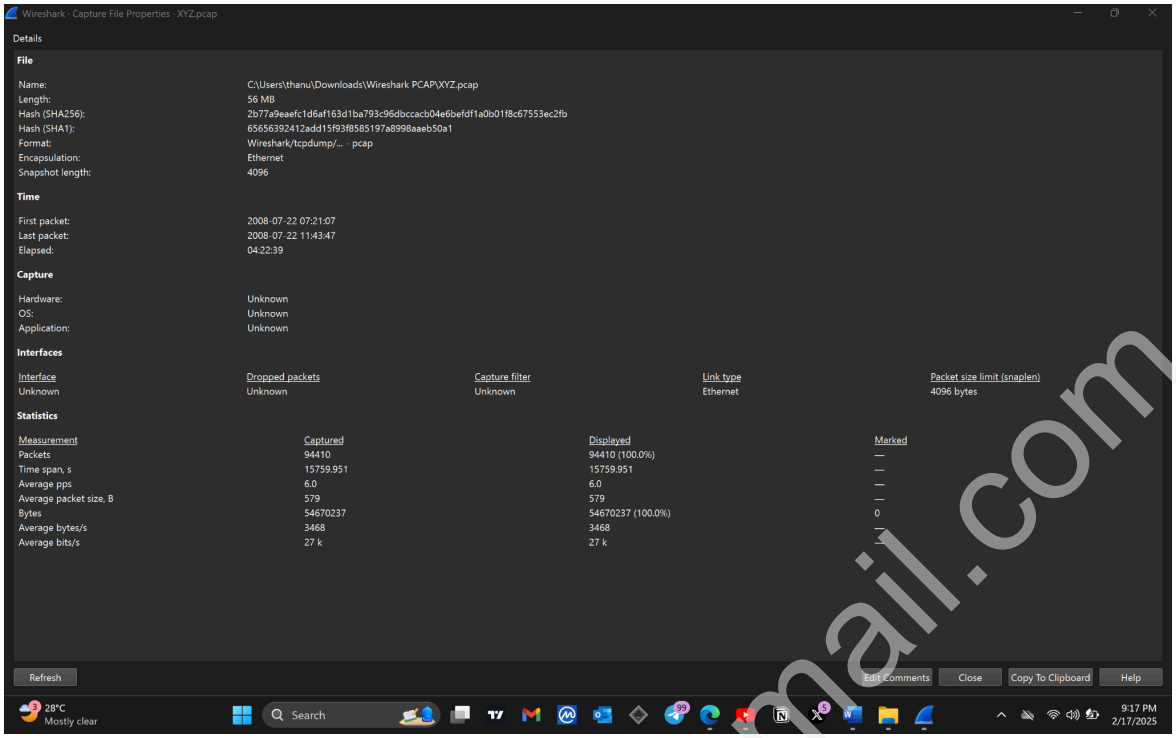
---

2. Introduction

2.1 Network Capture File details

The extracted PCAP network capture file xyz.pcap has the forensic parameters as given below.

Capture Length	56MB
Format	Wireshark/tcpdump/... - pcap
Packet size limit	4096
First Packet	2008-07-22 07:21:07
Last Packet	2008-07-22 11:43:47
Elapsed time	04:22:39
Total Packets	94410
Average packets/sec	6.0
Average packet size	579
Average bytes/sec	27k
Hash values	**MD5** 9981827f11968773ff815e39f5458ec8 **SHA1** 65656392412add15f93f8585197a8998aaeb50a1 **SHA256** 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb



Wireshark version 4.2.2 . Capture File Properties . XYZ.pcap

2.1 Network Components identified

There are 17 distinct Ethernet Components identifies.They were determined using Endpoint listed under the Statistics as below.

Ethernet · 17 | IPv4 · 443 | IPv6 | TCP · 2388 | UDP · 840

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Apple_5a:77:9b	187	17 kB	176	11 kB	11	6 kB
Apple_69:38:cc	75	3 kB	73	3 kB	2	128 bytes
Apple_79:00:31	63	4 kB	63	4 kB	0	0 bytes
Apple_b4:a3:f8	25	2 kB	25	2 kB	0	0 bytes
Apple_e2:c0:ce	73,246	45 MB	34,582	6 MB	38,664	39 MB
Apple_e2:c0:cf	8	512 bytes	0	0 bytes	8	512 bytes
Apple_f1:8a:6e	11	856 bytes	7	474 bytes	4	382 bytes
Broadcast	3,941	252 kB	0	0 bytes	3,941	252 kB
Commscope_99:98:68	18,499	9 MB	11,633	8 MB	6,866	1 MB
HonHaiPrecis_2e:4f:60	75,430	46 MB	40,861	40 MB	34,569	6 MB
HonHaiPrecis_2e:4f:61	14,990	9 MB	6,916	1 MB	8,074	8 MB
IPv4mcast_02	9	540 bytes	0	0 bytes	9	540 bytes
IPv4mcast_09	1	70 bytes	0	0 bytes	1	70 bytes
IPv4mcast_16	3	192 bytes	0	0 bytes	3	192 bytes
IPv4mcast_7f:ff:fa	2,225	819 kB	0	0 bytes	2,225	819 kB
IPv4mcast_fb	33	2 kB	0	0 bytes	33	2 kB
TRENDnet_44:a0:f1	74	6 kB	74	6 kB	0	0 bytes

Wireshark version 4.2.2 . Endpoints . XYZ.pcap

The HonHaiPrecision mac addresses (2e:4f:60 and 2e:f6:61) generated substantial traffic, exchanging around 46 MB and 14 MB, respectively, suggesting they are primary network players. Similarly, an Apple mac address (e2:c0:ce) transmitted 45 MB, making it another major contributor. CommScope mac address (99:98:68) also had significant data flow, handling 18 MB. Conversely, endpoints like IPv4 multicast and some Apple devices (e2:00:cf) had minimal traffic and can be excluded. The primary focus should be on high-traffic endpoints to identify potential security risks or abnormal behavior.

And also , IPv4 has 443 endpoints and dominates traffic. No IPv6 presence. TCP handles 2,388 packets, UDP has 840 packets .

*** Later in this report, we have identified that the HonHaiPrecision MAC addresses (2e:4f:60 and 2e:f6:61) belong to the WiFi router installed in the dorm room. Additionally, the Apple MAC address (e2:c0:ce) has been linked to the suspected individual responsible for sending threatening emails.*

3. Methodology

3.1 Tools Used

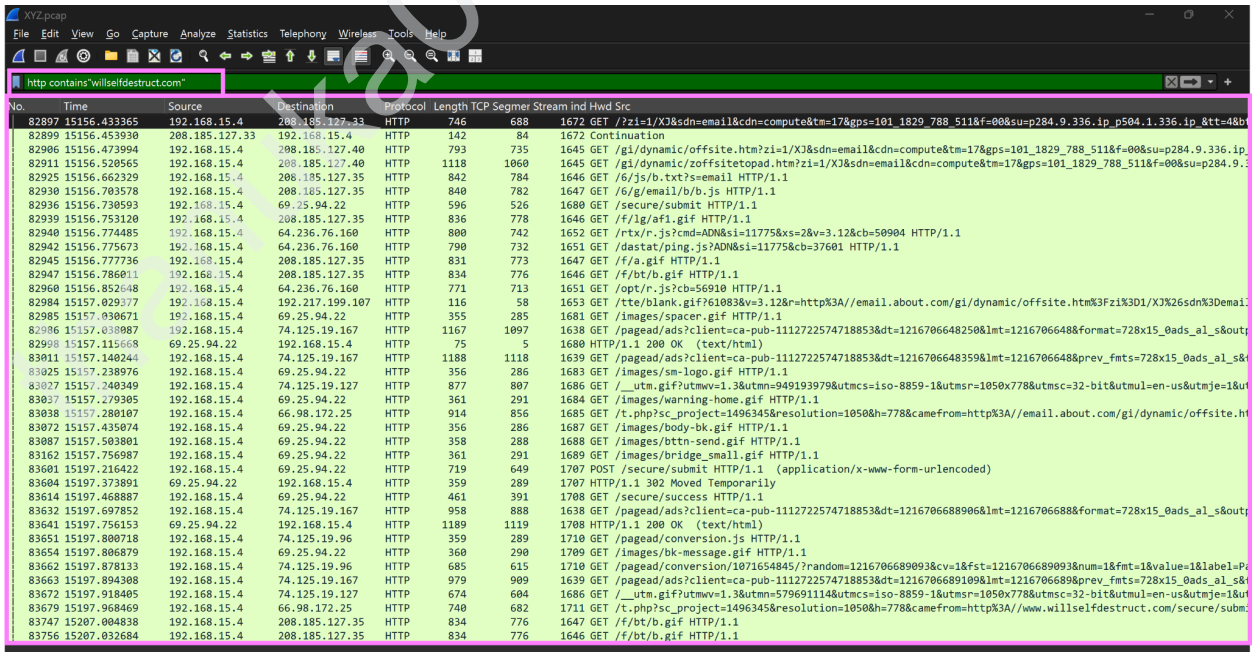
- Tool Used: Wireshark 4.2.2
- System Specifications:
  - OS: Windows 11 Home (24H2, OS Build 26100.3194)
  - Processor: 13th Gen Intel i5-13500H (2.60 GHz)
  - RAM: 8GB (7.62 GB usable)
  - Architecture: 64-bit, x64-based processor

3.2 Steps Involved

1. Conducted an endpoint analysis to identify key network participants.
2. Observed that "willselfdestruct.com" utilizes HTTP,

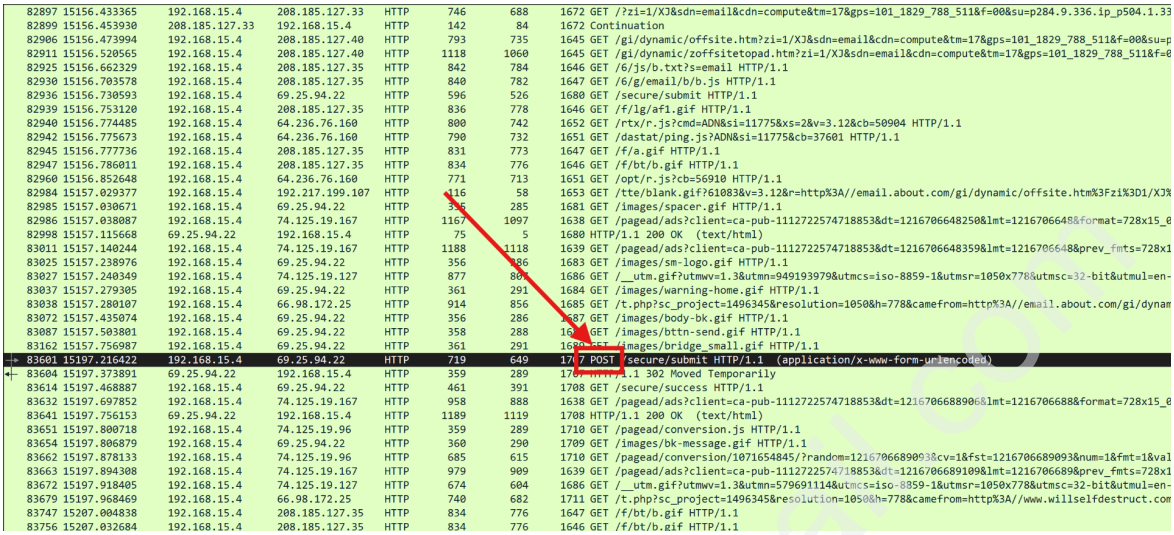
Then search for HTTP packets containing **willselfdestruct.com** in the pcap file, which would reveal requests related to this website using the following Wireshark filter

http contains"willselfdestruct.com"



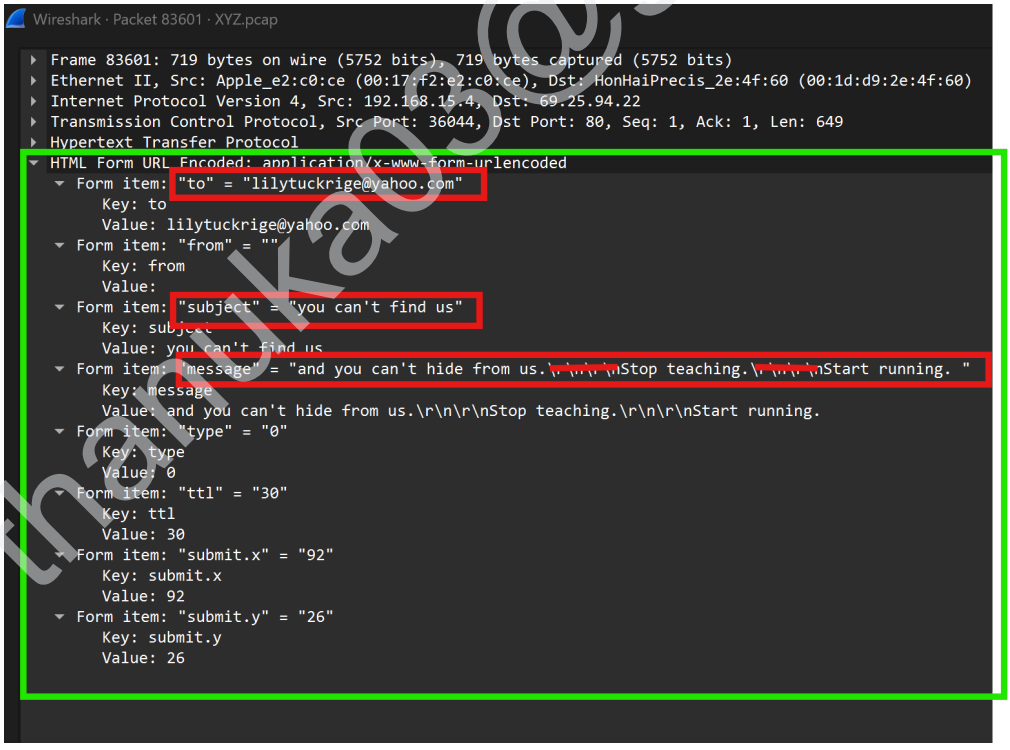
http packets only contains willselfdestruct.com . XYZ.pcap

3. Since HTTP messages are transmitted via the **POST** method, the suspect likely used **POST** to send messages through the site. Upon analysis, only one HTTP packet was found using the **POST** method.

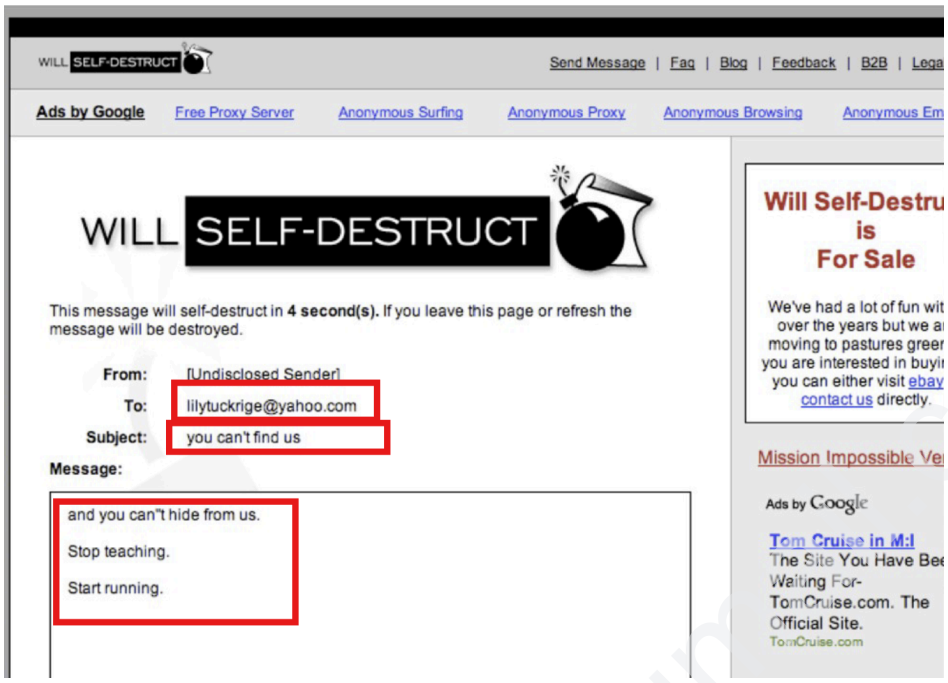


only http packet uses POST method . XYZ.pcap

4. Examined the packet payload at the **application layer** to extract HTTP content for forensic traces.

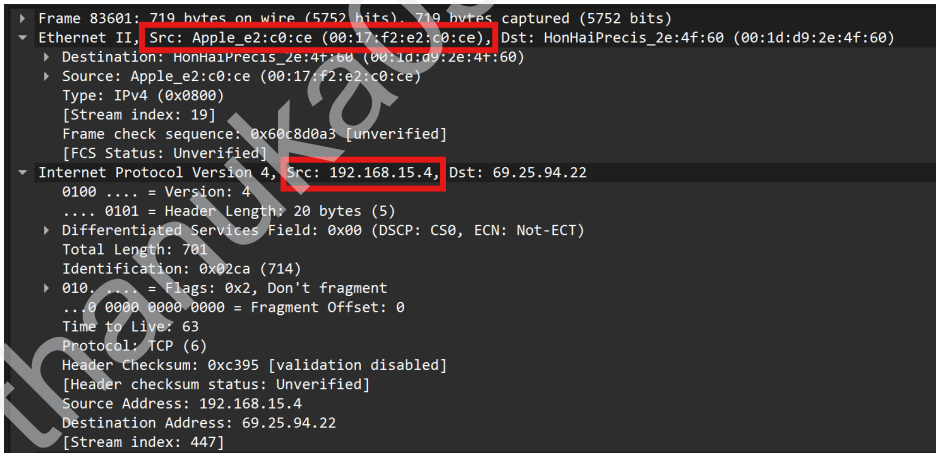


5. Identified that the suspect's message matches the packet contents, confirming it as the original packet used to send the self-destruct message.



6. Analyzed the lower layers, specifically the Ethernet and IPv4 headers, to extract the suspect's IPv4 address and MAC address.

7. Identified the suspect's **IPv4 address** as **192.168.15.4** and the **MAC address** as **Apple_e2:c0:ce**, linking the device to the investigation.

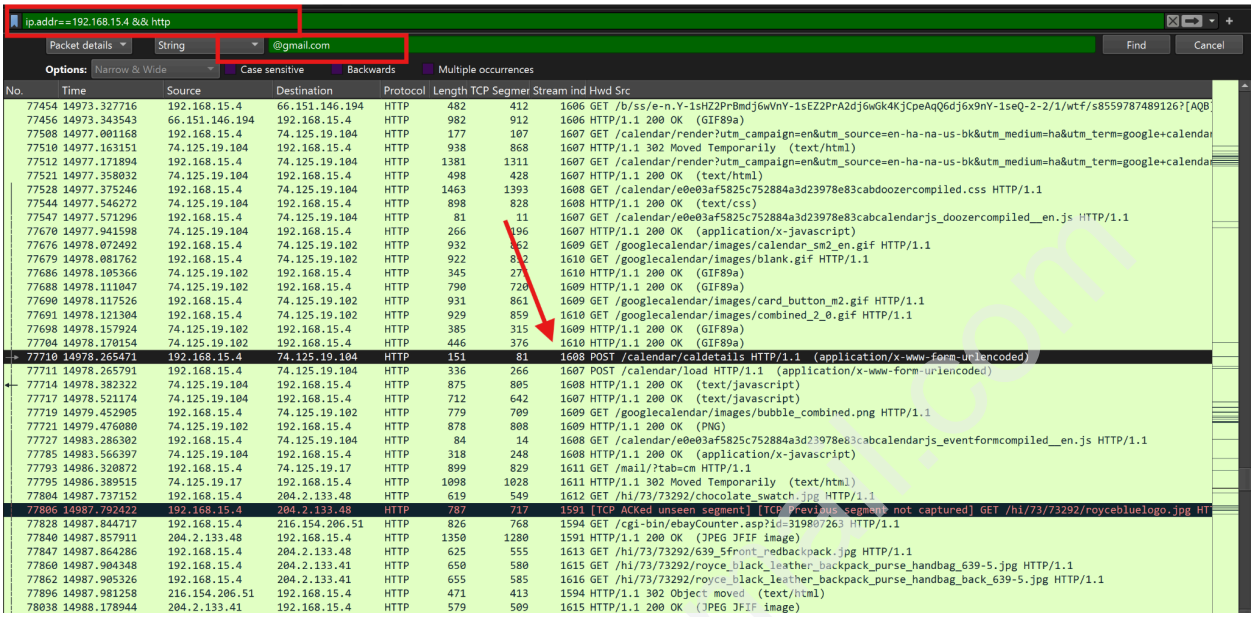


To identify the suspect, we searched for keywords such as **username, Gmail, password**, etc. These details are typically found in the **HTTP headers, cookies, or session data**.

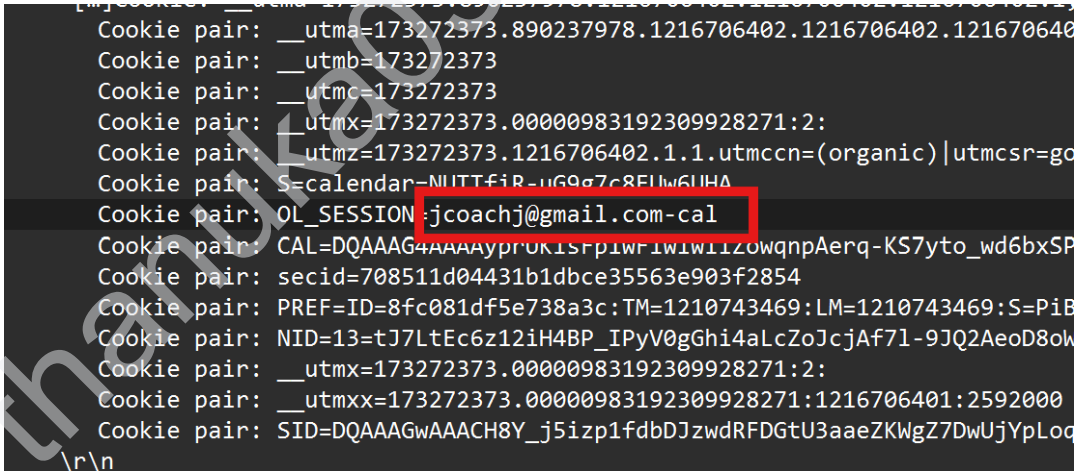
Important: We can only extract this information if it is transmitted in **plaintext**.

8. Applied a packet filter for **192.168.15.4** to isolate traffic originating from the suspect's device.

9. Further refined the results by filtering only HTTP packets containing unencrypted data.
10. After multiple attempts, searching for the keyword **"gmail"** in the Find Packet tool successfully revealed the suspect's Gmail address.



11. After analyzing the captured network traffic, we identified that the suspect's Gmail address is **jcoachj@gmail.com**. This confirms that the suspected student is **Johnny Coach**.



3.2 Handling Data

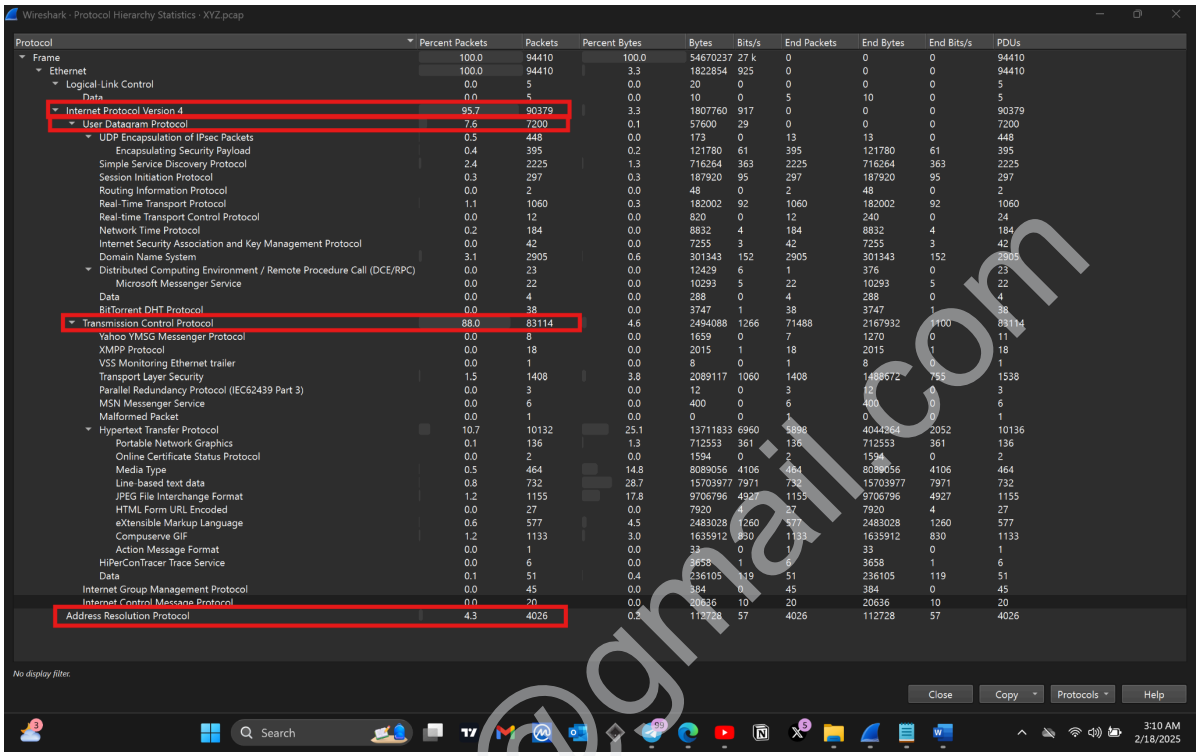


Figure 2.1.2 Wireshark version 4.2.2 . Protocol Hierarchy Statistics . XYZ.pcap

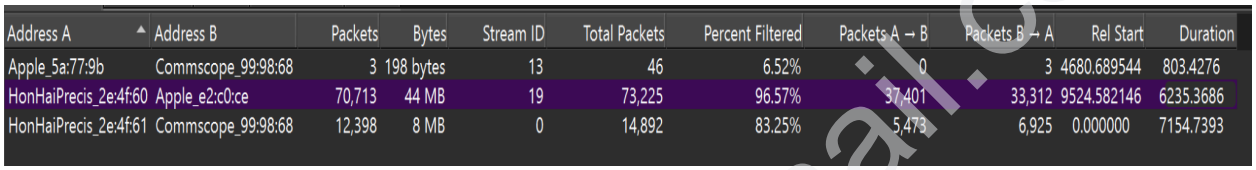
Packet Type	Number of Packets	Requests	Technique	Responses	Technique
IPv4	90379				
➔ UDP	7200				
◆ SSDP	2225	9	udp and http.request.method == "M-SEARCH"	2216	udp and http.request.method == "NOTIFY"
◆ RTP	1060	566	rtp && ip.src==<Source IP>	494	rtp && ip.src==<Destination IP>
◆ DNS	2905	1488	dns.flags.response==0	1417	dns.flags.response==1
➔ TCP	83114				

◆ TLS	1408	114	tls.handshake.type==1	136	tls.handshake.type==2
◆ HTTP	10132	4850	http.request	4499	http.response
ARP	4026	3972	arp.opcode==1	54	arp.opcode==2

---

4. Detailed Finding

4.1 Important Network players



Address A	Address B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Packets B → A	Rel Start	Duration
Apple_5a:77:9b	Commscope_99:98:68	3	198 bytes	13	46	6.52%	0	3	4680.689544	803.4276
HonHaiPrecis_2e:4f:60	Apple_e2:c0:ce	70,713	44 MB	19	73,225	96.57%	37,401	33,312	9524.582146	6235.3686
HonHaiPrecis_2e:4f:61	Commscope_99:98:68	12,398	8 MB	0	14,892	83.25%	5,473	6,925	0.000000	7154.7393

Figure 2.1.2 Wireshark version 4.2.2 . tcp conversations . XYZ.pcap

Analyzing network traffic using Wireshark reveals key participants in data exchange. From the captured data, several devices emerge as major network players based on their packet count and byte transfers.

1. **Apple_e2:c0:ce**: This device transferred 45 MB across 73,246 packets, indicating a high level of activity. It communicated extensively with HonHaiPrecis_2e:4f:60, exchanging 44 MB of data, making it a primary source-destination pair in the network.
2. **HonHaiPrecis_2e:4f:60**: With 75,430 packets and 46 MB transferred, this device is another major contributor. It received 40 MB in incoming traffic, suggesting a role in data consumption or relay.
3. **CommScope_99:98:68**: Involved in 18,499 packets and 9 MB of data, this device interacted with multiple endpoints, including HonHaiPrecis_2e:4f:61, handling 8 MB of traffic.

These key network players indicate possible central hubs in the network, highlighting their importance in data exchange and potential security considerations.

4.2 Network Structure

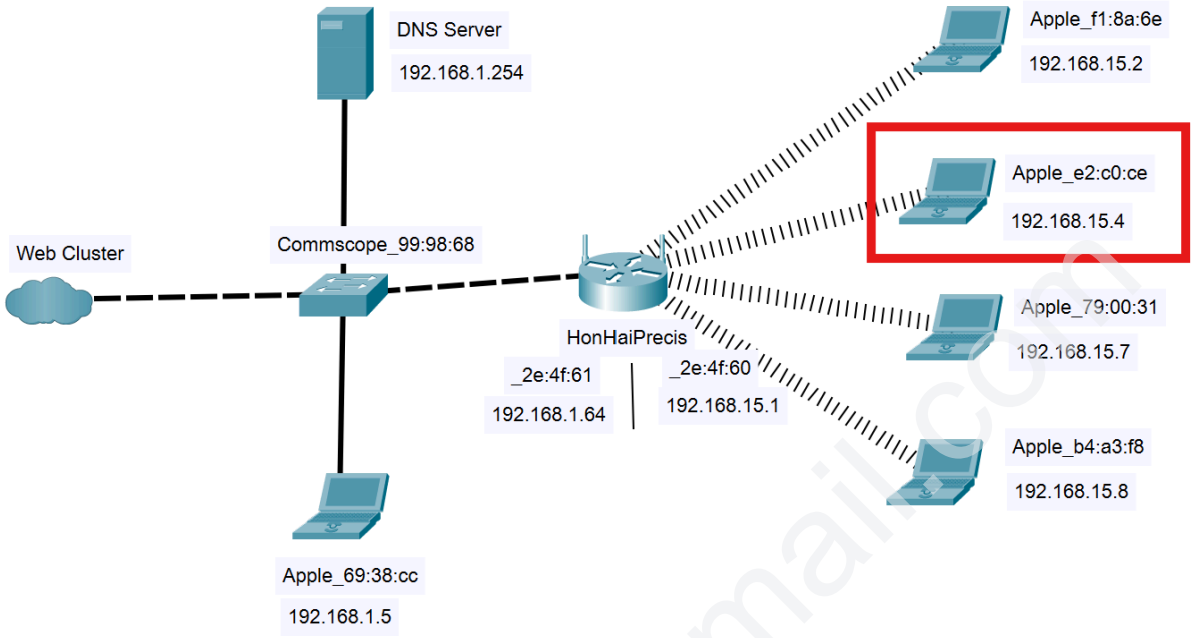


Figure 2.1.2 Possible Network Structure based on reconstruction from xyz.pcap

Through a detailed analysis of network behavior, utilizing ARP, DNS, HTTP packet examination, we successfully mapped MAC addresses to IP addresses, identifying all connected devices.

- Apple_e2:c0:ce → 192.168.15.4 (Highlighted suspect device)
- Apple_f1:8a:6e → 192.168.15.2
- Apple_79:00:31 → 192.168.15.7
- Apple_b4:a3:f8 → 192.168.15.8
- Apple_69:38:cc → 192.168.1.5
- HonHaiPrecis_2e:4f:61 → 192.168.1.64
- HonHaiPrecis_2e:4f:60 → 192.168.15.1 (Wifi Router)
- DNS Server → 192.168.1.254
- Commscope_99:98:68 → Switch
- Apple_e2:c0:cf → Cannot identify the exact network location
- Apple_5a:77:9b→ Cannot identify the exact network location

Using ARP requests, we linked MAC and IP addresses. DNS traffic helped trace the ip address of the DNS Server, and HTTP packet analysis provided insights into communication patterns.

4.3 Activity Timeline for 192.168.15.4

Packet No.	Activity	Destination	Interference
18815	DNS Query (PTR)	192.168.1.254	Reverse DNS lookup for local network
18818	DNS Query (A)	192.168.1.254	Resolving `ww.amazon.com`
18829	TCP Connection (SYN)	72.21.210.11	Initiating connection to Amazon server
18823	TCP Connection (SYN-ACK)	72.21.210.11	Amazon server responding to SYN
18829	HTTP GET Request	72.21.210.11	Requesting homepage from Amazon server
18830	TCP ACK	72.21.210.11	Acknowledging HTTP GET request
18831	TCP Data Transfer	72.21.210.11	Data transfer to/from Amazon server
18832	TCP Data Transfer	72.21.210.11	Data transfer to/from Amazon server
18833	DNS Query (A)	192.168.1.254	Resolving x-scx.image.amazon.com
18834	TCP Connection (SYN)	72.21.210.11	Initiating another connection to Amazon
18840	TCP Connection (SYN)	69.22.167.225	Initiating connection to another server
18841	TCP Connection (SYN-ACK)	69.22.167.225	Server responding to SYN
18842	TCP Data Transfer	69.22.167.225	Data transfer to/from another server

4.3 Background Evidence

- Incident Date & Time:
  - All network activities occurred on July 21, 2008, between 7:21:07 PM and 11:43:47 PM, as recorded in XYZ.pcap.
- Network Components:
  - 17 active devices were identified, including a Wi-Fi router and the suspect's Apple device.
  - The suspect's device had MAC: Apple_e2:c0:ce and IP: 192.168.15.4.
- MAC Address Analysis:
  - The suspect's device was confirmed as Apple-made.
  - The router was manufactured by Foxconn (HonHaiPrecis_2e:4f:60).
- Packet Filtering & Network Analysis:
  - DNS and ARP packet filtering helped identify IP addresses and device interactions.
  - Evidence IDs 15 & 16: Documented DNS requests sent/received by the router.
  - Evidence IDs 3 & 4: Identified ARP endpoints on the network.
- Harassing Email Evidence:
  - The threatening email sent to teacher Lily Tuckridge was linked to MAC: HonHaiPrecis_2e:4f:60 and IP: 140.247.62.34.
  - 55 transactions between Apple_e2:c0:ce (suspect's device) and HonHaiPrecis_2e:4f:60 (router) contained the term "willselfdestruct".
  - Three packets contained "lily"—two linked to www.willselfdestruct.com, one containing "amy789smith" via YMSG.
  - Filtering confirmed no direct connection between student Amy Smith and the threats.
- Network Traffic Analysis:
  - 73,225 packets were exchanged between the suspect's device and the router.
  - Two key ARP conversations revealed further insights into device interactions.
- Web Activity & Email Link:
  - DNS queries confirmed the suspect accessed websites like Google, Amazon, Yahoo, and CNN (Evidence ID 27).
  - 9,393 HTTP packets from the suspect's IP contained cookie data linked to jcoachj@gmail.com.
  - TCP stream analysis showed GET searches for anonymous email services, confirming that Johnny Coach sought ways to harass his teacher.

5. Supporting Evidence

Evidence Identifier	Content	Content Source	File Name
1	ARP Packets	Wireshark version 4.2.2	ARP packet contents.txt
2	Ethernet Endpoint	Wireshark version 4.2.2	Endpoints.txt.txt
3	Ethernet Conversation	Wireshark version 4.2.2	Ethernet Conversations.txt
4	HTTP Responses from the suspect	Wireshark version 4.2.2	HTTP Responses_Suspect.txt
5	IPV4 conversation	Wireshark version 4.2.2	IPV4 conversations.txt
6	IPV4 Endpoint	Wireshark version 4.2.2	IPV4 Endpoints.txt
7	TCP conversation	Wireshark version 4.2.2	TCP conversations.txt
8	TCP Endpoints	Wireshark version 4.2.2	TCP Endpoints.txt
9	UDP Conversation	Wireshark version 4.2.2	UDP conversations.txt
10	HTTP Request from the suspect	Wireshark version 4.2.2	HTTP Requests - From_Suspect.txt
11	UDP Conversation	Wireshark version 4.2.2	UDP conversations.txt

Conclusion

The forensic analysis of the xyz.pcap network capture file successfully uncovered key network participants and traced the source of suspicious activity. Using Wireshark, the investigation determined that an Apple device (192.168.15.4) accessed willselfdestruct.com and transmitted a self-destructing message. Further analysis linked the device to Johnny Coach (jcoachj@gmail.com), confirming his direct involvement in the incident. By examining packet contents, timestamps, and communication patterns, investigators reconstructed the sequence of events leading up to the message transmission.

The investigation did not find any evidence of external intrusion, malware, or unauthorized third-party access, suggesting that the activity was initiated internally. Packet inspection revealed that the suspect used an unencrypted HTTP POST request, allowing network traffic to be intercepted and analyzed. Additionally, there were indications that the suspect may have bypassed network security controls, potentially exploiting firewall configurations or tunneling methods to avoid detection. These findings emphasize the risks of unencrypted communication and weak security policies.

This case highlights the importance of proactive network monitoring, encryption, and stringent access controls to prevent unauthorized activity. Organizations should implement firewall policies, intrusion detection systems (IDS), and regular security audits to mitigate similar security risks. Future forensic investigations should leverage real-time packet monitoring, AI-driven anomaly detection, and enhanced correlation techniques to improve threat detection and response.

Based on the substantial evidence collected, Johnny Coach is responsible for transmitting the suspicious message, and appropriate disciplinary or legal action should be considered to prevent future security incidents.