

# **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.

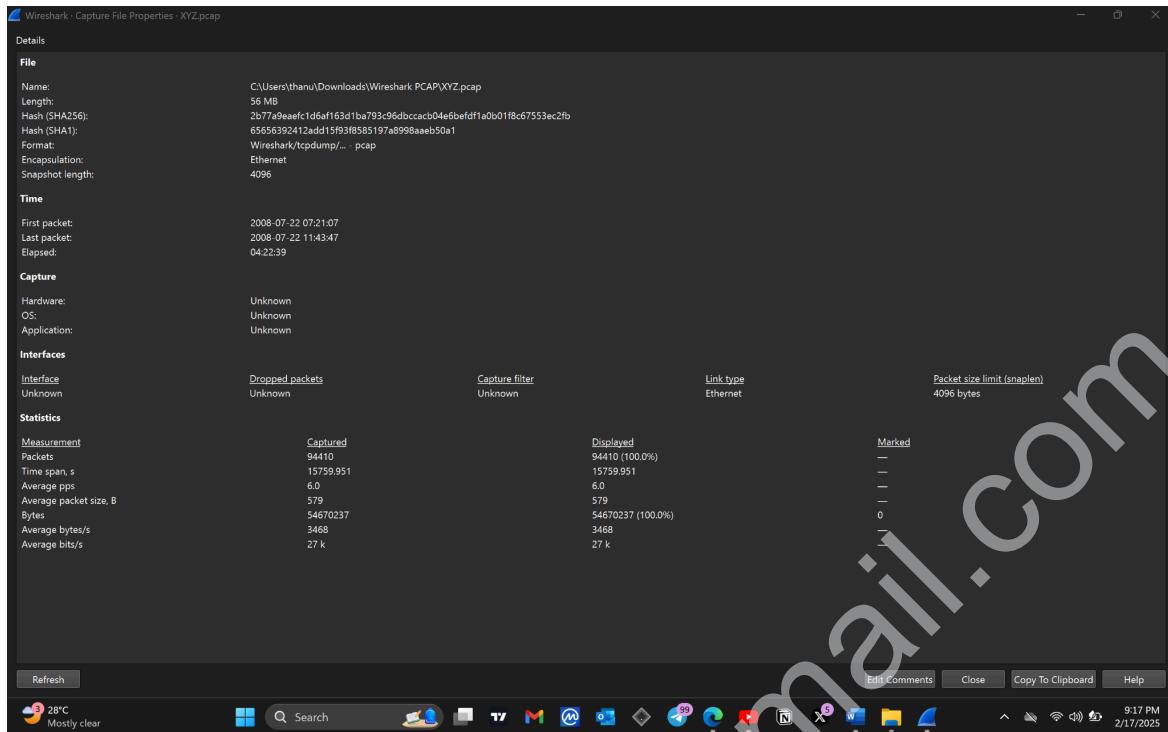
---

## 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	<b>MD5</b> 9981827f11968773ff815e39f5458ec8 <b>SHA1</b> 65656392412add15f93f8585197a8998aaeb50a1 <b>SHA256</b> 2b77a9eaefc1d6af163d1ba793c96dbccacb04e6befdf1a0b01f8c67553ec2fb



Wireshark version 4.2.2 . Capture File Properties . XYZ.pcap

## 2.1 Network Components identified

There are 17 distinct Ethernet Components identified. 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.*

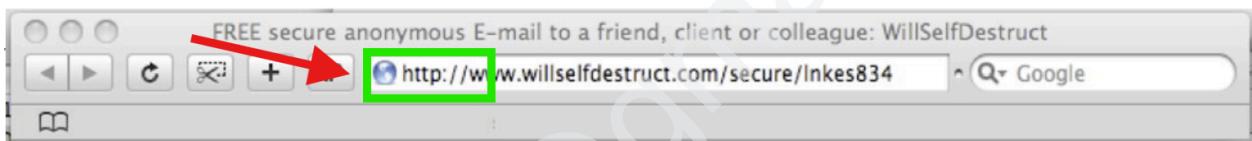
### 3. Methodology

#### 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"*

A screenshot of the Wireshark application interface. The title bar says "XYZ.pcap". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help. The packet list pane shows a large number of rows, each representing a network packet. A pink box highlights the first few columns: No., Time, Source, Destination, Protocol, Length, TCP Segments, Stream, and Hwd Src. The "Protocol" column shows mostly "HTTP". The "Time" column shows timestamps like "82897 15156.433365". The "Source" and "Destination" columns show IP addresses like "192.168.15.4" and "192.168.15.4". The "Length" column shows values like "746" and "688". The "TCP Segments" column shows values like "142" and "84". The "Stream" column shows values like "1060" and "1060". The "Hwd Src" column shows values like "788" and "788". A pink box also highlights the filter bar at the top of the packet list, which contains the text "http contains \"willselfdestruct.com\"".

No.	Time	Source	Destination	Protocol	Length	TCP Segments	Stream	Hwd Src
82897	15156.433365	192.168.15.4	208.185.127.33	HTTP	746	688	1672	GET /?zi=1/Xj&sdn=email&cdn=compute&t=17&gps=101_1829_788_511&f=00&su=p284.9.336.ip.p504.1.336.ip.&tt=48b
82898	15156.453938	208.185.127.33	192.168.15.4	HTTP	142	84	1672	Continuation
82896	15156.473994	192.168.15.4	208.185.127.40	HTTP	793	735	1645	GET /gi/dynamic/offsite.htm?zi=1/Xj&sdn=email&cdn=compute&t=17&gps=101_1829_788_511&f=00&su=p284.9.336.ip
82911	15156.520565	192.168.15.4	208.185.127.40	HTTP	1118	1060	1645	GET /gi/dynamic/zoffsitetopad.htm?zi=1/Xj&sdn=email&cdn=compute&t=17&gps=101_1829_788_511&f=00&su=p284.9.336.ip
82925	15156.662329	192.168.15.4	208.185.127.35	HTTP	842	784	1646	GET /6/j5/b/txt?&email HTTP/1.1
82930	15156.703578	192.168.15.4	208.185.127.35	HTTP	840	782	1647	GET /6/g/email/b/b.js HTTP/1.1
82936	15156.730593	192.168.15.4	69.25.94.22	HTTP	596	526	1680	GET /secure/submit HTTP/1.1
82939	15156.753120	192.168.15.4	208.185.127.35	HTTP	836	778	1648	GET /f/ig/a/f1.gif HTTP/1.1
82940	15156.774485	192.168.15.4	64.236.76.160	HTTP	800	742	1652	GET /rtx/-js?cmd=ADN&s=i11775&x=2&v=3.12&cb=59094 HTTP/1.1
82942	15156.775673	192.168.15.4	64.236.76.160	HTTP	790	732	1651	GET /dastat/ping.js?ADN&s=i11775&cb=37601 HTTP/1.1
82945	15156.777736	192.168.15.4	208.185.127.35	HTTP	831	773	1647	GET /f/a.gif HTTP/1.1
82947	15156.786011	192.168.15.4	208.185.127.35	HTTP	834	776	1646	GET /f/bt/b.gif HTTP/1.1
82968	15156.852648	192.168.15.4	64.236.76.160	HTTP	771	713	1651	GET /opt/r_js?cb=56910 HTTP/1.1
82984	15157.029377	192.168.15.4	192.217.199.107	HTTP	116	58	1653	GET /tte/blank.gif?61083w=1.128=r=http%3A//email.about.com/gi/dynamic/offsite.htm%3Fz1%3D1/Xj%26sdn%3Demai
82985	15157.030671	192.168.15.4	69.25.94.22	HTTP	355	285	1681	GET /images/spacer.gif HTTP/1.1
82986	15157.030887	192.168.15.4	74.125.19.167	HTTP	1167	1097	1638	GET /pagead/ads?client=ca-pub-1121722574718853&dt=1216706648250&lt=1216706648&format=728x15_0ads_a1_sout
82998	15157.115668	69.25.94.22	192.168.15.4	HTTP	75	5	1680	HTTP/1.1 200 OK (text/html)
83011	15157.140244	192.168.15.4	74.125.19.167	HTTP	1188	1118	1639	GET /pagead/ads?client=ca-pub-1121722574718853&dt=1216706648359&lt=1216706648&prev_mts=728x15_0ads_a1_s&u
83025	15157.238976	192.168.15.4	69.25.94.22	HTTP	356	286	1683	GET /images/sm-logo.gif HTTP/1.1
83027	15157.240349	192.168.15.4	74.125.19.127	HTTP	877	807	1684	GET /_utn.gif?utmwv=1.3&utmtn=949193979&utmc=iso-8859-1&utnsr=1050x778&utmc=32-bit&utmul=en-us&utmje=1&ut
83037	15157.270395	192.168.15.4	69.25.94.22	HTTP	361	291	1688	GET /images/warning-home.gif HTTP/1.1
83038	15157.280107	192.168.15.4	66.98.172.25	HTTP	914	856	1685	GET /t.php?&project=1496345&resolution=1050&h=778&camefrom=http%3A//email.about.com/gi/dynamic/offsite.h
83072	15157.435074	192.168.15.4	69.25.94.22	HTTP	356	286	1687	GET /images/body-bk.gif HTTP/1.1
83087	15157.503801	192.168.15.4	69.25.94.22	HTTP	358	288	1688	GET /images/btn-send.gif HTTP/1.1
83162	15157.756987	192.168.15.4	69.25.94.22	HTTP	361	291	1689	GET /images/bridge_small.gif HTTP/1.1
83601	15197.216422	192.168.15.4	69.25.94.22	HTTP	719	649	1707	POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)
83604	15197.373891	192.168.15.4	69.25.94.22	HTTP	359	289	1707	HTTP/1.1 302 Moved Temporarily
83614	15197.468887	192.168.15.4	69.25.94.22	HTTP	461	391	1708	GET /secure/success HTTP/1.1
83632	15197.697852	192.168.15.4	74.125.19.167	HTTP	958	888	1638	GET /pagead/ads?client=ca-pub-1121722574718853&dt=1216706688906&lt=1216706688&format=728x15_0ads_a1_s&out
83641	15197.756153	69.25.94.22	192.168.15.4	HTTP	1189	1119	1708	HTTP/1.1 200 OK (text/html)
83651	15197.800718	192.168.15.4	74.125.19.96	HTTP	359	289	1710	GET /pagead/conversion.js HTTP/1.1
83654	15197.806879	192.168.15.4	69.25.94.22	HTTP	360	290	1708	GET /images/bk-message.gif HTTP/1.1
83662	15197.878133	192.168.15.4	74.125.19.96	HTTP	685	615	1710	GET /pagead/conversion/10/1654845/?random=1216706689093&cv=1&ft=1216706689093&num=1&fmt=1&value=1&label=P
83663	15197.894308	192.168.15.4	74.125.19.167	HTTP	979	909	1639	GET /pagead/ads?client=ca-pub-1121722574718853&dt=1216706689109&lt=1216706689109&format=728x15_0ads_a1_s&
83672	15197.918405	192.168.15.4	74.125.19.127	HTTP	674	600	1688	GET /_utn.gif?utmwv=1.3&utmtn=579691114&utmc=iso-8859-1&utnsr=1050x778&utmc=32-bit&utmul=en-us&utmje=1&ut
83679	15197.968469	192.168.15.4	66.98.172.25	HTTP	740	682	1711	GET /t.php?sc_project=1496345&resolution=1050&h=778&camefrom=http%3A//www.willselfdestruct.com/secure/subm
83747	15207.004838	192.168.15.4	208.185.127.35	HTTP	834	776	1647	GET /f/bt/b.gif HTTP/1.1
83756	15207.032684	192.168.15.4	208.185.127.35	HTTP	834	776	1646	GET /f/bt/b.gif HTTP/1.1

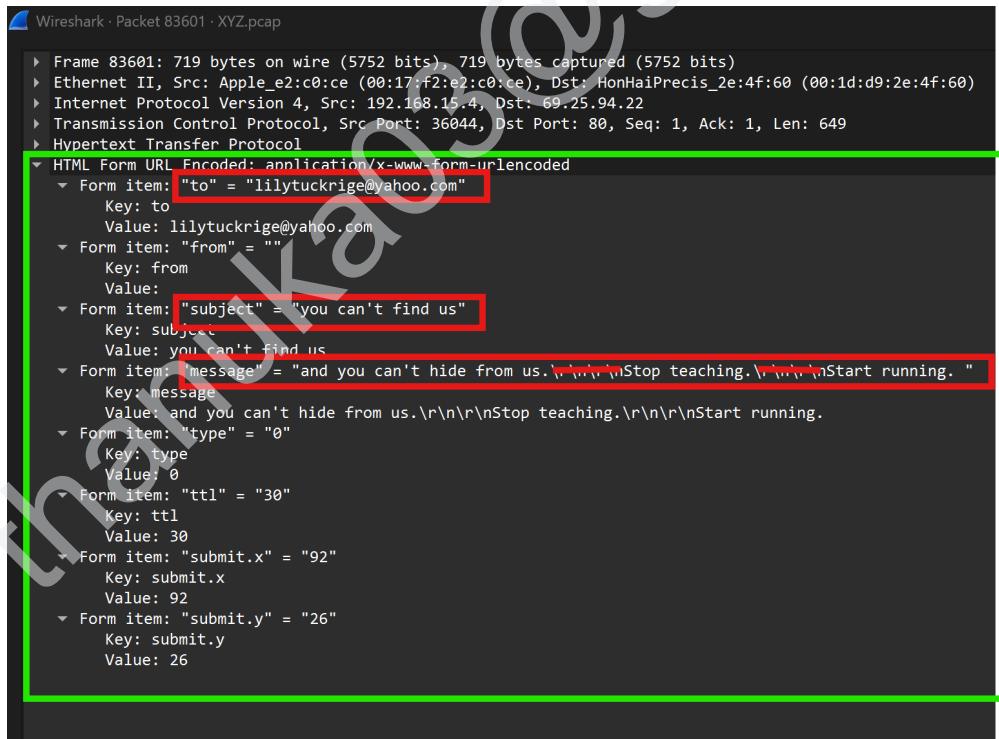
*http packets only contains willselfdestruct.com . XYZ.pcap*

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.

82897 15156.433365	192.168.15.4	208.185.127.33	HTTP	746	688	1672 GET /?zi=1/X&sdn=email&cdn=compute&tm=17&gps=101_1829_788_511&f=00&su=p284.9.336.ip_p504.1.33
82899 15156.453938	208.185.127.33	192.168.15.4	HTTP	142	84	1672 Continuation
82906 15156.473994	192.168.15.4	208.185.127.40	HTTP	793	735	1645 GET /g1/dynamic/offsite.htm?zi=1/X&sdn=email&cdn=compute&tm=17&gps=101_1829_788_511&f=00&su=p
82911 15156.520565	192.168.15.4	208.185.127.40	HTTP	1118	1068	1645 GET /g1/dynamic/offsite.htm?zi=1/X&sdn=email&cdn=compute&tm=17&gps=101_1829_788_511&f=0
82925 15156.662329	192.168.15.4	208.185.127.35	HTTP	842	784	1646 GET /6/j5/b.txt?z=email HTTP/1.1
82930 15156.703578	192.168.15.4	208.185.127.35	HTTP	840	782	1647 GET /6/g/email/b/b.js HTTP/1.1
82936 15156.730593	192.168.15.4	69.25.94.22	HTTP	596	526	1688 GET /secure/submit/HTTP/1.1
82939 15156.753120	192.168.15.4	208.185.127.35	HTTP	836	778	1646 GET /f/lg/afl1.gif HTTP/1.1
82940 15156.774485	192.168.15.4	64.236.76.160	HTTP	800	742	1652 GET /rtx/r.r.js?cd=ADN&s=i+11775&x=s=2&v=3.128cb=50904 HTTP/1.1
82942 15156.775673	192.168.15.4	64.236.76.160	HTTP	790	732	1651 GET /datat/ping.js?ADN&s=i+11775&c=37601 HTTP/1.1
82945 15156.777736	192.168.15.4	208.185.127.35	HTTP	831	773	1647 GET /f/a.gif HTTP/1.1
82947 15156.786011	192.168.15.4	208.185.127.35	HTTP	834	776	1646 GET /f/b/b.gif HTTP/1.1
82966 15156.852648	192.168.15.4	64.236.76.160	HTTP	771	713	1651 GET /opt/r.r.js?cb=56910 HTTP/1.1
82984 15157.029377	192.168.15.4	192.217.199.107	HTTP	116	58	1653 GET /tte/blank.gif?i+10838+v=3.12&r=http%3A//email.about.com/gi/dynamic/offsite.htm?zi=1/X&
82985 15157.030671	192.168.15.4	69.25.94.22	HTTP	356	285	1681 GET /images/spacer.gif HTTP/1.1
82986 15157.030807	192.168.15.4	74.125.19.167	HTTP	1167	1097	1638 GET /pagead/ad?ad?client=ca-pub-1112722574718853&dt=1216706648250&lt=1216706648&format=728x1_0
82998 15157.115668	69.25.94.22	192.168.15.4	HTTP	75	5	1680 HTTP/1.1 200 OK (text/html)
83011 15157.140244	192.168.15.4	74.125.19.167	HTTP	1188	1118	1639 GET /pagead/ad?ad?client=ca-pub-1112722574718853&dt=1216706648359&lt=1216706648&prev_fmts=728x1
83025 15157.238976	192.168.15.4	69.25.94.22	HTTP	356	326	1683 GET /images/sm-logo.gif HTTP/1.1
83027 15157.240349	192.168.15.4	74.125.19.127	HTTP	877	807	1686 GET /_utm.gif?utmwv=1.3&utmn=949193979&utmc=iso-8859-1&utmsr=1050x778&utmsc=32-bit&utmul=en-
83037 15157.279305	192.168.15.4	69.25.94.22	HTTP	361	291	1684 GET /images/warning-home.gif HTTP/1.1
83038 15157.280107	192.168.15.4	66.98.172.25	HTTP	914	856	1685 GET /t.php?sc_project=1496345&resolution=1050x778&camefrom=http%3A//email.about.com/gi/dynam
83072 15157.435074	192.168.15.4	69.25.94.22	HTTP	356	286	1687 GET /images/body-bl.gif HTTP/1.1
83087 15157.503801	192.168.15.4	69.25.94.22	HTTP	358	288	1689 GET /images/button-send.gif HTTP/1.1
83162 15157.756987	192.168.15.4	69.25.94.22	HTTP	361	291	1690 GET /images/bridge_small.gif HTTP/1.1
83601 15197.216422	192.168.15.4	69.25.94.22	HTTP	719	649	17 7 POST /secure/submit/HTTP/1.1 (application/x-www-form-urlencoded)
83604 15197.373891	69.25.94.22	192.168.15.4	HTTP	359	289	17 7 1.1 302 Moved Temporarily
83614 15197.468887	192.168.15.4	69.25.94.22	HTTP	461	391	1708 GET /secure/success/HTTP/1.1
83632 15197.697852	192.168.15.4	74.125.19.167	HTTP	958	888	1638 GET /pagead/ad?client=ca-pub-1112722574718853&dt=1216706688906&lt=1216706688&format=728x1_0
83641 15197.756153	69.25.94.22	192.168.15.4	HTTP	1189	1119	1708 HTTP/1.1 200 OK (text/html)
83651 15197.800718	192.168.15.4	74.125.19.96	HTTP	359	289	1710 GET /pagead/conversion.js HTTP/1.1
83654 15197.806879	192.168.15.4	69.25.94.22	HTTP	360	298	1709 GET /images/bk-message.gif HTTP/1.1
83662 15197.878133	192.168.15.4	74.125.19.96	HTTP	685	615	1710 GET /pagead/conversion/1071654845/?random=1216706689093&c=v=1&fst=1216706689093&num=1&fmt=1&val
83663 15197.894308	192.168.15.4	74.125.19.167	HTTP	979	909	1639 GET /pagead/ad?client=ca-pub-1112722574718853&dt=121670668910981&lt=1216706689&prev_fmts=728x1
83672 15197.918405	192.168.15.4	74.125.19.127	HTTP	674	604	1686 GET /_utm.gif?utmwv=1.3&utmn=57969111&utmc=iso-8859-1&utmsr=1050x778&utmsc=32-bit&utmul=en-
83679 15197.968469	192.168.15.4	66.98.172.25	HTTP	740	682	1711 GET /t.php?sc_project=1496345&resolution=1050x778&camefrom=http%3A//www.willselfdestruct.com
83747 15207.004838	192.168.15.4	208.185.127.35	HTTP	834	776	1647 GET /f/b/b.gif HTTP/1.1
83756 15207.032684	192.168.15.4	208.185.127.35	HTTP	834	776	1646 GET /f/b/b.gif HTTP/1.1

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.

The screenshot shows a web page with a header "WILL SELF-DESTRUCT" and a navigation bar with links like "Send Message", "FAQ", "Blog", "Feedback", "B2B", and "Legal". Below the header, there's a banner for "Ads by Google" and other links for "Free Proxy Server", "Anonymous Surfing", "Anonymous Proxy", "Anonymous Browsing", and "Anonymous Email". The main content area features a large "WILL SELF-DESTRUCT" logo with a bomb icon. A message box displays an email from an undisclosed sender to "lillytuckrige@yahoo.com" with the subject "you can't find us". The message body contains the text: "and you can't hide from us. Stop teaching. Start running." To the right, a sidebar titled "Will Self-Destruct is For Sale" says: "We've had a lot of fun with this over the years but we are moving to pastures greener. If you are interested in buying it you can either visit [eBay](#) or contact us directly." Below this is another sidebar for "Mission Impossible VII" with links to "Ads by Google" and "Tom Cruise in MI: The Site You Have Been Waiting For - TomCruise.com. The Official Site. TomCruise.com".

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.

```

▶ 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:d9:2e: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)
      [Stream index: 19]
      Frame check sequence: 0x60c8d0a3 [unverified]
      [FCS Status: Unverified]
  ▶ Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.25.94.22
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 701
      Identification: 0x02ca (714)
    010.... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: TCP (6)
    Header Checksum: 0xc395 [validation disabled]
      [Header checksum status: Unverified]
    Source Address: 192.168.15.4
    Destination Address: 69.25.94.22
    [Stream index: 447]
  
```

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.

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

ip.addr==192.168.15.4 && http

Packet details String @gmail.com

Options: Narrow & Wide Case sensitive Backwards Multiple occurrences

No.	Time	Source	Destination	Protocol	Length	TCP Segmer Stream	Hwd Src
77454	14973. 327716	192.168.15.4	66.151.146.194	HTTP	482	412	1606 GET /b/ss/e-n.Y-1sHZ2PrBmdj6wVnY-1sEZ2PrA2dJ6wGk4KjCpeAqQ6dj6x9nY-1seQ-2-2/1/wtf/s8559787489126?AQ;
77456	14973. 343543	66.151.146.194	192.168.15.4	HTTP	982	912	1606 HTTP/1.1 200 OK (GIF89a)
77508	14977. 001168	192.168.15.4	74.125.19.184	HTTP	177	107	1607 GET /calendar/render?utm_campaign=en&utm_source=en-ha-na-us-bk&utm_medium=ha&utm_term=google+calendar
77510	14977. 163151	74.125.19.184	192.168.15.4	HTTP	938	868	1607 HTTP/1.1 302 Moved Temporarily (text/html)
77512	14977. 171894	192.168.15.4	74.125.19.184	HTTP	1381	1311	1607 GET /calendar/render?utm_campaign=en&utm_source=en-ha-na-us-bk&utm_medium=ha&utm_term=google+calendar
77521	14977. 358832	74.125.19.184	192.168.15.4	HTTP	498	428	1607 HTTP/1.1 200 OK (text/html)
77528	14977. 375246	192.168.15.4	74.125.19.184	HTTP	1463	1393	1608 GET /calendar/ebe03af5825c752884a3d23978e83cabdozercompiled.css HTTP/1.1
77544	14977. 546272	74.125.19.184	192.168.15.4	HTTP	898	828	1608 HTTP/1.1 200 OK (text/css)
77547	14977. 571296	192.168.15.4	74.125.19.184	HTTP	81	11	1607 GET /calendar/ebe03af5825c752884a3d23978e83cabcalendarjs_doozercompiled_en.js HTTP/1.1
77670	14977. 941598	74.125.19.184	192.168.15.4	HTTP	266	196	1607 HTTP/1.1 200 OK (application/x-javascript)
77676	14978. 072492	192.168.15.4	74.125.19.182	HTTP	932	852	1609 GET /googlecalendar/images/calendar_sm2_en.gif HTTP/1.1
77679	14978. 081762	192.168.15.4	74.125.19.182	HTTP	922	842	1610 GET /googlecalendar/images/blank.gif HTTP/1.1
77686	14978. 185366	74.125.19.182	192.168.15.4	HTTP	345	27	1611 HTTP/1.1 200 OK (GIF89a)
77688	14978. 111047	74.125.19.182	192.168.15.4	HTTP	790	728	1609 HTTP/1.1 200 OK (GIF89a)
77690	14978. 117526	192.168.15.4	74.125.19.182	HTTP	931	861	1609 GET /googlecalendar/images/card_button_m2.gif HTTP/1.1
77691	14978. 121304	192.168.15.4	74.125.19.182	HTTP	929	859	1611 GET /googlecalendar/images/combined_2_0.gif HTTP/1.1
77698	14978. 157924	74.125.19.182	192.168.15.4	HTTP	385	315	1609 HTTP/1.1 200 OK (GIF89a)
77704	14978. 170154	74.125.19.182	192.168.15.4	HTTP	446	376	1610 HTTP/1.1 200 OK (GIF89a)
77718	14978. 265471	192.168.15.4	74.125.19.184	HTTP	151	81	1608 POST /calendar/caldetails HTTP/1.1 (application/x-www-form-urlencoded)
77719	14978. 265791	192.168.15.4	74.125.19.184	HTTP	336	266	1607 POST /calendar/load HTTP/1.1 (application/x-www-form-urlencoded)
77714	14978. 382322	74.125.19.184	192.168.15.4	HTTP	875	805	1607 HTTP/1.1 200 OK (text/javascript)
77717	14978. 521174	74.125.19.184	192.168.15.4	HTTP	712	642	1607 HTTP/1.1 200 OK (text/javascript)
77719	14979. 452905	192.168.15.4	74.125.19.182	HTTP	779	709	1609 GET /googlecalendar/images/bubble_combined.png HTTP/1.1
77721	14979. 476689	74.125.19.182	192.168.15.4	HTTP	878	808	1609 GET /googlecalendar/images/bubble_combined.png HTTP/1.1
77727	14983. 288082	192.168.15.4	74.125.19.182	HTTP	84	14	1609 GET /calendar/ebe03af5825c752884a3d23978e83cabcalendarjs_eventformcompiled_en.js HTTP/1.1
77785	14983. 566397	74.125.19.184	192.168.15.4	HTTP	318	248	1608 GET /calendar/ebe03af5825c752884a3d23978e83cabcalendarjs_eventformcompiled_en.js HTTP/1.1
77793	14986. 328072	192.168.15.4	74.125.19.17	HTTP	899	829	1611 GET /mail/?tab=cm (application/x-javascript)
77795	14986. 389515	74.125.19.17	192.168.15.4	HTTP	1098	1038	1611 GET /mail/?tab=cmb (text/html)
77798	14987. 119352	192.168.15.4	204.2.133.48	HTTP	619	549	1612 GET /hi/73/73292/chocolate_swatch.jpg HTTP/1.1
77805	14987. 792422	192.168.15.4	204.2.133.48	HTTP	707	717	1501 [TCP ACKed seen segment 1 [tcp_rv]] GET /hi/73/73292/roycebluelogo.jpg HTTP/1.1
77828	14987. 844717	192.168.15.4	216.154.205.51	HTTP	826	768	1504 GET /mail/bin/1/counter.asp?sid=319807263 HTTP/1.1
77840	14987. 857911	204.2.133.48	192.168.15.4	HTTP	1350	1280	1501 HTTP/1.1 200 OK (JPEG/JFIF image)
77847	14987. 864286	192.168.15.4	204.2.133.48	HTTP	625	555	1613 GET /hi/73/73292/639_5from_redbackpack.jpg HTTP/1.1
77860	14987. 994348	192.168.15.4	204.2.133.41	HTTP	650	580	1615 GET /hi/73/73292/royce_black_leather_backpack_purse_handbag_639-5.jpg HTTP/1.1
77862	14987. 995326	192.168.15.4	204.2.133.41	HTTP	655	585	1616 GET /hi/73/73292/royce_black_leather_backpack_purse_handbag_back_639-5.jpg HTTP/1.1
77896	14987. 981258	216.154.206.51	192.168.15.4	HTTP	471	413	1504 HTTP/1.1 302 Object moved (text/html)
78038	14988. 178944	204.2.133.41	192.168.15.4	HTTP	579	509	1615 HTTP/1.1 200 OK (JPEG/JFIF image)

- 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**.

```
[...]
Cookie pair: __utma=173272373.890237978.1216706402.1216706402.1216706402
Cookie pair: __utmb=173272373
Cookie pair: __utmc=173272373
Cookie pair: __utmx=173272373.00000983192309928271:2
Cookie pair: __utmz=173272373.1216706402.1.1.utmccn=(organic)|utmcsr=go
Cookie pair: S=calendar-NUITTfir-lug9a7c8ElnG1HA
Cookie pair: OL_SESSION:jcoachj@gmail.com-cal
Cookie pair: CAL=DQAAAG4AAAAypruk1sPpiwr1wiw1iowqnpAerq-KS7yto_wd6bxSP
Cookie pair: secid=708511d04431b1dbce35563e903f2854
Cookie pair: PREF=ID=8fc081df5e738a3c:TM=1210743469:LM=1210743469:S=Pib
Cookie pair: NID=13=tJ7LtEc6z12iH4BP_IPyV0gGhi4aLcZoJcjAf71-9JQ2AeoD8ow
Cookie pair: __utmx=173272373.00000983192309928271:2
Cookie pair: __utmxx=173272373.00000983192309928271:1216706401:2592000
Cookie pair: SID=DQAAAGwAAACH8Y_j5izp1fdbDJzwdRFDGtU3aaeZKlgZ7DwUjYpLoc
\r\n
```

### 3.2 Handling Data

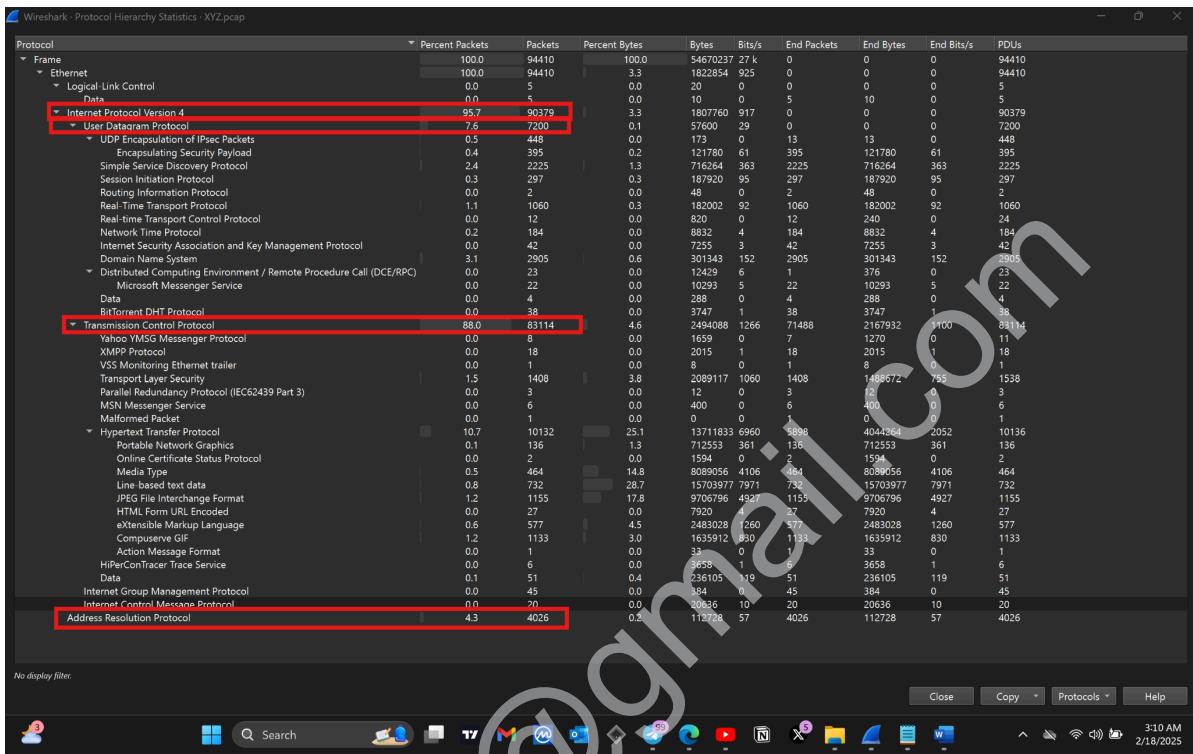


Figure 2.1.2 Wireshark version 4.2.2 . Protocol Hierarchy Statistics . XYZ.pcap

Packet Type	Number of Packets	Request s	Technique	Response s	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

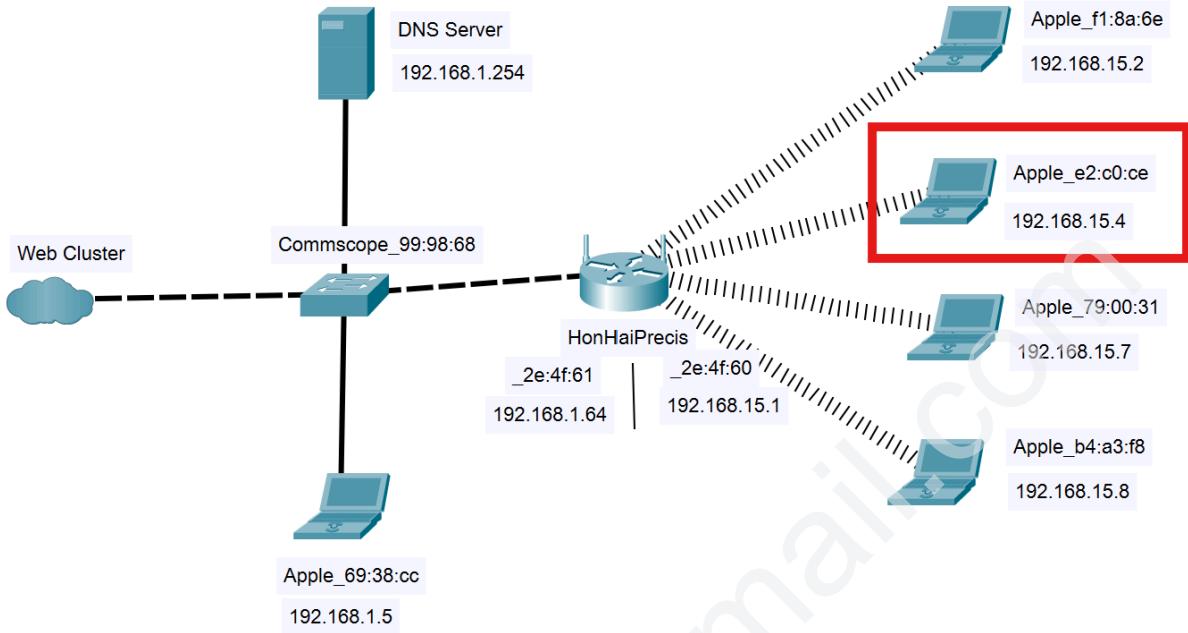


Figure 2.1.2 Possible Network Structure based on reconstruction from xyz.pcap

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 `www.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](http://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	<a href="#">ARP packet contents.txt</a>
2	Ethernet Endpoint	Wireshark version 4.2.2	<a href="#">Endpoints.txt.txt</a>
3	Ethernet Conversation	Wireshark version 4.2.2	<a href="#">Ethernet Conversations.txt</a>
4	HTTP Responses from the suspect	Wireshark version 4.2.2	<a href="#">HTTP Responses_Suspect.txt</a>
5	IPV4 conversation	Wireshark version 4.2.2	<a href="#">IPV4 conversations.txt</a>
6	IPV4 Endpoint	Wireshark version 4.2.2	<a href="#">IPV4 Endpoints.txt</a>
7	TCP conversation	Wireshark version 4.2.2	<a href="#">TCP conversations.txt</a>
8	TCP Endpoints	Wireshark version 4.2.2	<a href="#">TCP Endpoints.txt</a>
9	UDP Conversation	Wireshark version 4.2.2	<a href="#">UDP conversations.txt</a>
10	HTTP Request from the suspect	Wireshark version 4.2.2	<a href="#">HTTP Requests - From Suspect.txt</a>
11	UDP Conversation	Wireshark version 4.2.2	<a href="#">UDP conversations.txt</a>

---

## 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.

---