

## Nitroba University Harassment Scenario Analysis

In the scenario it was mentioned that the mail header shows the mail message originated from Nitroba student dorm room with IP address *140.247.62.34*.

Using tshark to isolate the activity done using the IP address and filtering the activity to another pcap file.

```
tshark -r nitroba.pcap -Y "ip.src==140.247.62.34 or ip.dst==140.247.62.34" -w 140_247_62_34.pcap
```

-r nitroba.pcap reads the nitroba.pcap file

-Y "ip.src==*140.247.62.34* or ip.dst== "*140.247.62.34*" filters the packets that have IP address as *140.247.62.34* in the source or destination.

```
C:\Program Files\Wireshark>tshark -r "C:\Users\sunandha\Desktop\forensics\nw forensics\ass3\nitroba.pcap" -T fields -e ip.src > "C:\Users\sunandha\Desktop\forensics\nw forensics\ass3\ip-src.txt"
```

Figure 1

The above tshark command redirect the output to a text file.

-T fields set the output to that of fields.

Figure 2

```
sunandha@DESKTOP-FGHE60A MINGW64 ~  
$ cat "C:\Users\sunandha\Desktop\forensics\nw forensics\ass3\ip-src.txt" | sort  
| uniq -c | sort -n | grep -e " 172\." -e " 192\." -e " 10\."  
 2 192.168.15.2  
 3 192.168.15.7  
 6 192.168.15.8  
 8 10.0.1.5  
14 192.168.15.5  
16 192.168.1.5  
1486 192.168.1.254  
2154 192.168.15.1  
6818 192.168.1.64  
34554 192.168.15.4
```

-e ip.src defines which fields to output.

The above command output the source IP addresses that are sorted into a list. The number of instances that every IP address has is also counted.

Observing the output, we can infer that *192.168.15.4* is the busiest device.

Since there are many IP addresses, if we can determine the MAC address of the device then it may give us the clue to find out who sent those emails.

```
C:\Program Files\Wireshark>tshark -r "C:\Users\sunandha\Desktop\forensics\nw forensics\ass3\nitroba.pcap" -T fields -e ip.p.src -e eth.src > "C:\Users\sunandha\Desktop\forensics\nw forensics\ass3\ip-src-and-mac-src.txt"
```

Figure 3

```
sunandha@DESKTOP-FGHE60A MINGW64 ~
$ cat "C:\Users\sunandha\Desktop\forensics\nw forensics\ass3\ip-src-and-mac-src.txt" | sort | uniq -c | sort -rn | grep -e " 172\." -e " 192\." -e " 10\."

34554 192.168.15.4      00:17:f2:e2:c0:ce
 6814 192.168.1.64      00:1d:d9:2e:4f:61
 2154 192.168.15.1      00:1d:d9:2e:4f:60
 1161 192.168.1.254      00:1d:d9:2e:4f:60
   325 192.168.1.254      00:1d:6b:99:98:68
   16 192.168.1.5       00:0a:95:69:38:cc
   14 192.168.15.5      00:14:d1:44:a0:f1
    8 10.0.1.5          00:1c:b3:79:00:31
    6 192.168.15.8      00:16:cb:b4:a3:f8
    4 192.168.1.64      00:1f:f3:5a:77:9b
    3 192.168.15.7      00:1c:b3:79:00:31
    2 192.168.15.2      00:1b:63:f1:8a:6e
```

Figure 4

Observing the above output, there are two IP addresses with more than one MAC address associated with it.

- *192.168.1.254*-- 00:1d:d9:2e:4f:60

*192.168.1.254*-- 00:1d:6b:99:98:68

- *192.168.1.64* -- 00:1d:d9:2e:4f:61

*192.168.1.64* -- 00:1f:f3:5a:77:9b

Now, in wireshark, use ctrl+F and find the packets that has lily

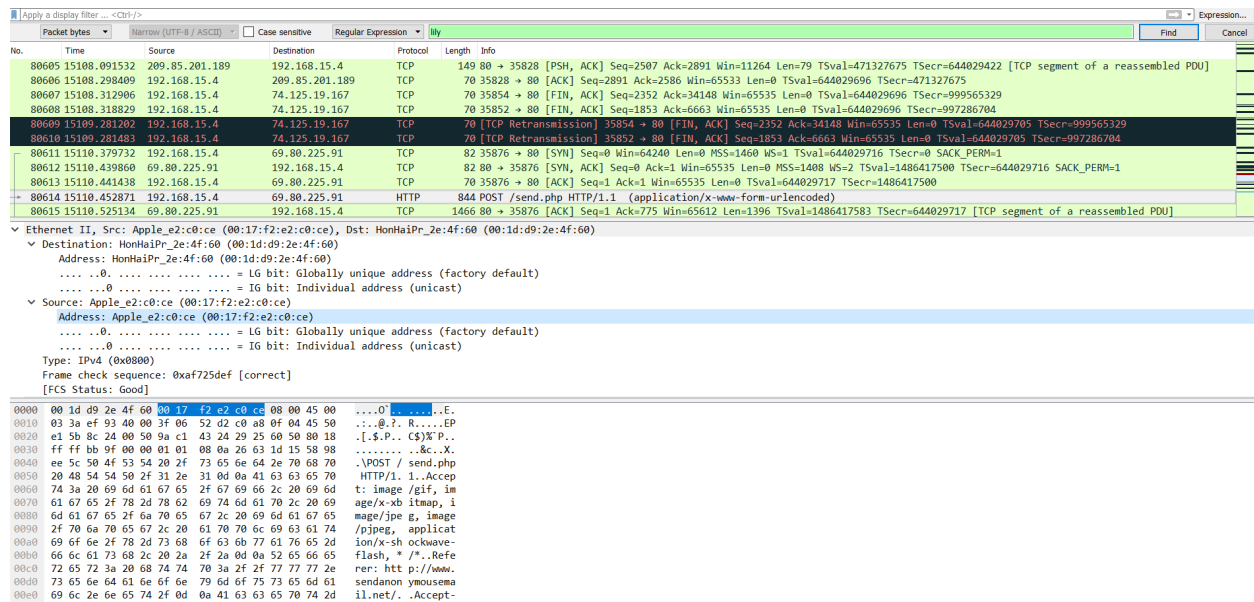


Figure 5

It shows the MAC address of the source as 00:17:f2:e2:c0:ce.

Now filtering the packets with the above IP and MAC address and export them into another new\_pcap file.

Loading this new\_pcap file in network miner, it can be observed that there is an email associated with the IP address. The email ID looks like it belongs one of the students in Lily’s class named ‘Johnny couch’.

Email id: [jcouchj@gmail.com](mailto:jcouchj@gmail.com)

Hosts (590) Files (3943) Images (2295) Messages (2) Credentials (2) Sessions (1720) DNS (2148) Parameters (89882) Keywords Anomalies					
<input type="checkbox"/> Show Cookies <input checked="" type="checkbox"/> Show NTLM challenge-response <input type="checkbox"/> Mask Passwords					
Client	Server	Protocol	Username	Password	Valid login Login timestamp
192.168.15.4 (Apple_iOS)	209.85.201.189 [googlemail.l.google.com]	HTTP Cookie parameter	jcouchj@gmail.com/475090	N/A (unknown Google password)	Unknown 2008-07-22 06:01:02 U
192.168.15.4 (Apple_iOS)	74.125.19.17 [googlemail.l.google.com]	HTTP Cookie parameter	jcouchj@gmail.com/475090	N/A (unknown Google password)	Unknown 2008-07-22 06:01:02 U

Figure 6

Loading the same new\_pcap file in wireshark, it can be noted that some packets contain different email ID that belongs to another person in Lily’s class named ‘Amy smith’.

Email id: [amy789smith@yahoo.com](mailto:amy789smith@yahoo.com)

Another email in some of the packets were found which is

[mylady.ixchel@gmail.com](mailto:mylady.ixchel@gmail.com)

however, this email does appears to be related to any of the students' email.

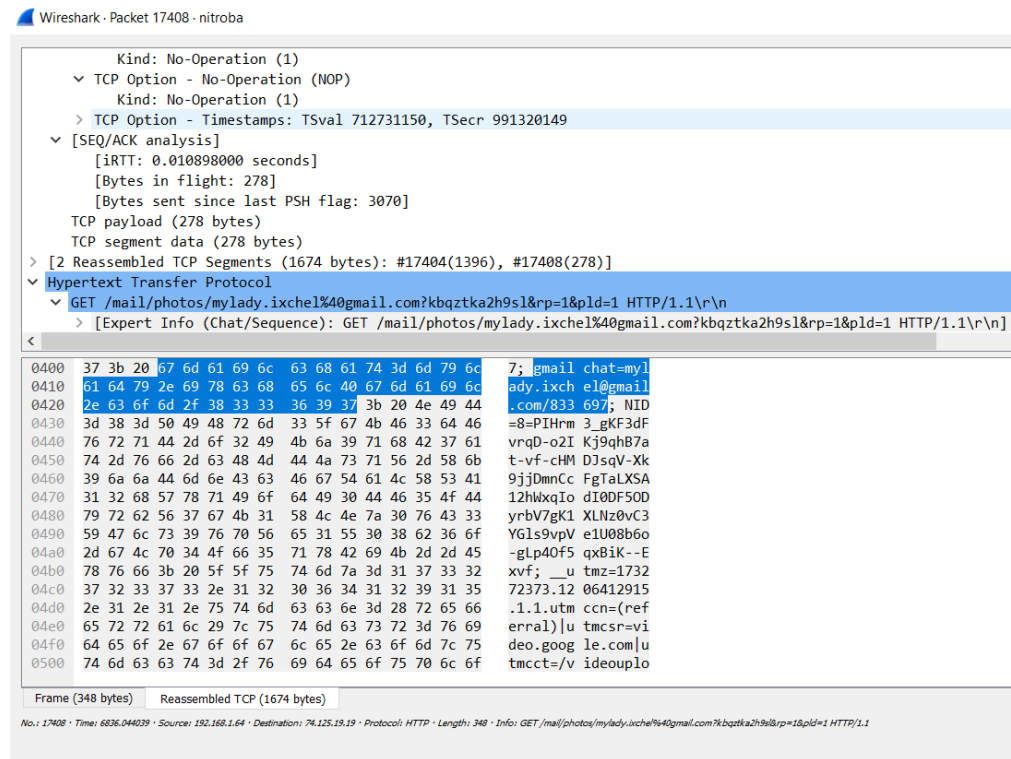


Figure 7

Using ctrl+F and searching all the packets that contain 'amy', it was found that 'Lily' and 'Amy' are buddies in Yahoo.

The following packet with frame number 90426 shows that 'Buddies lilytuckridge YMSG amy789 smith YMSG' (highlighted in the screenshot).

```

[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
▼ Ethernet II, Src: HonHaiPr_2e:4f:60 (00:1d:d9:2e:4f:60), Dst: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
  ▼ Destination: 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)
  ▼ Source: HonHaiPr_2e:4f:60 (00:1d:d9:2e:4f:60)
    Address: HonHaiPr_2e:4f:60 (00:1d:d9:2e:4f:60)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  Frame check sequence: 0x85ae5dda [correct]
  [FCS Status: Good]

```

Figure 8

Wireshark · Packet 90426 · nitroba

▼ Frame 90426: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Jul 22, 2008 01:09:59.227031000 Central Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1216706999.227031000 seconds
[Time delta from previous captured frame: 0.009271000 seconds]
[Time delta from previous displayed frame: 0.009271000 seconds]
[Time since reference or first frame: 15532.131753000 seconds]
Frame Number: 90426
Frame Length: 375 bytes (3000 bits)
Capture Length: 375 bytes (3000 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:ymsg]
[Coloring Rule Name: TCP]

0050	00 00 00 50 6b fb 33 30 32 c0 80 33 31 38 c0 80	...Pk.30 2..318..
0060	33 30 30 c0 80 33 31 38 c0 80 36 35 c0 80 42 75	300..318 ..65..Bu
0070	64 64 69 65 73 c0 80 33 30 32 c0 80 33 31 39 c0	ddies..3 02..319.
0080	80 33 30 30 c0 80 33 31 39 c0 80 37 c0 80 6c 69	.300..31 9..7..li
0090	6c 79 74 75 63 6b 72 69 67 65 c0 80 33 30 31 c0	lytuckri ge..301.
00a0	80 33 31 39 c0 80 33 30 33 c0 80 33 31 39 c0 80	.319..30 3..319..
00b0	33 30 31 c0 80 33 31 38 c0 80 33 30 33 c0 80 33	301..318 ..303..3
00c0	31 38 c0 80 59 4d 53 47 00 0f 00 00 00 29 00 f0	18..YMSG .....)
00d0	00 00 00 00 00 50 6b fb 30 c0 80 61 6d 79 37 38	....Pk. 0..amy78
00e0	39 73 6d 69 74 68 c0 80 31 c0 80 61 6d 79 37 38	9smith.. 1..amy78
00f0	39 73 6d 69 74 68 c0 80 32 34 31 c0 80 30 c0 80	9smith.. 241..0..
0100	00 59 4d 53 47 00 0f 00 00 00 39 00 ef 00 00 00	.YMSG... ..9....
0110	01 00 50 6b fb 33 30 32 c0 80 33 31 32 c0 80 33	..Pk.302 ..312..3
0120	30 30 c0 80 33 31 32 c0 80 33 31 33 c0 80 32 c0	00..312. .313..2.
0130	80 33 31 34 c0 80 30 c0 80 33 30 31 c0 80 33 31	.314..0. .301..31
0140	32 c0 80 33 30 33 c0 80 33 31 32 c0 80 00 59 4d	2..303.. 312...YM
0150	53 47 00 0f 00 00 00 11 00 12 00 00 00 01 00 50	SG..... .....P
0160	6b fb 31 34 33 c0 80 36 30 c0 80 31 34 34 c0 80	k.143..6 0..144..
0170	31 c0 80 85 ae 5d da	1....].

No.: 90426 · Time: 15532.131753 · Source: 66.163.181.179 · Destination: 192.168.15.4 · Protocol: YMSG · Length: 375 · Info: List V15 (status=Default) Status V15 (status=Default) Unknown Service: 239 (status=Server Ack) Ping (status=Server Ack)

Figure 9

Now, searching for jcoachj in wireshark, I found one packet

- ▼ Ethernet II, Src: HonHaiPr\_2e:4f:60 (00:1d:d9:2e:4f:60), Dst: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce)
  - ▼ Destination: 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)
  - ▼ Source: HonHaiPr\_2e:4f:60 (00:1d:d9:2e:4f:60)
    - Address: HonHaiPr\_2e:4f:60 (00:1d:d9:2e:4f:60)
      - .... ..0. .... = LG bit: Globally unique address (factory default)
      - .... ..0 .... = IG bit: Individual address (unicast)
  - Type: IPv4 (0x0800)
  - Frame check sequence: 0x484c32bd [correct]
  - [FCS Status: Good]
- ▼ Internet Protocol Version 4, Src: 74.125.19.104, Dst: 192.168.15.4
  - 0100 .... = Version: 4

Figure 10

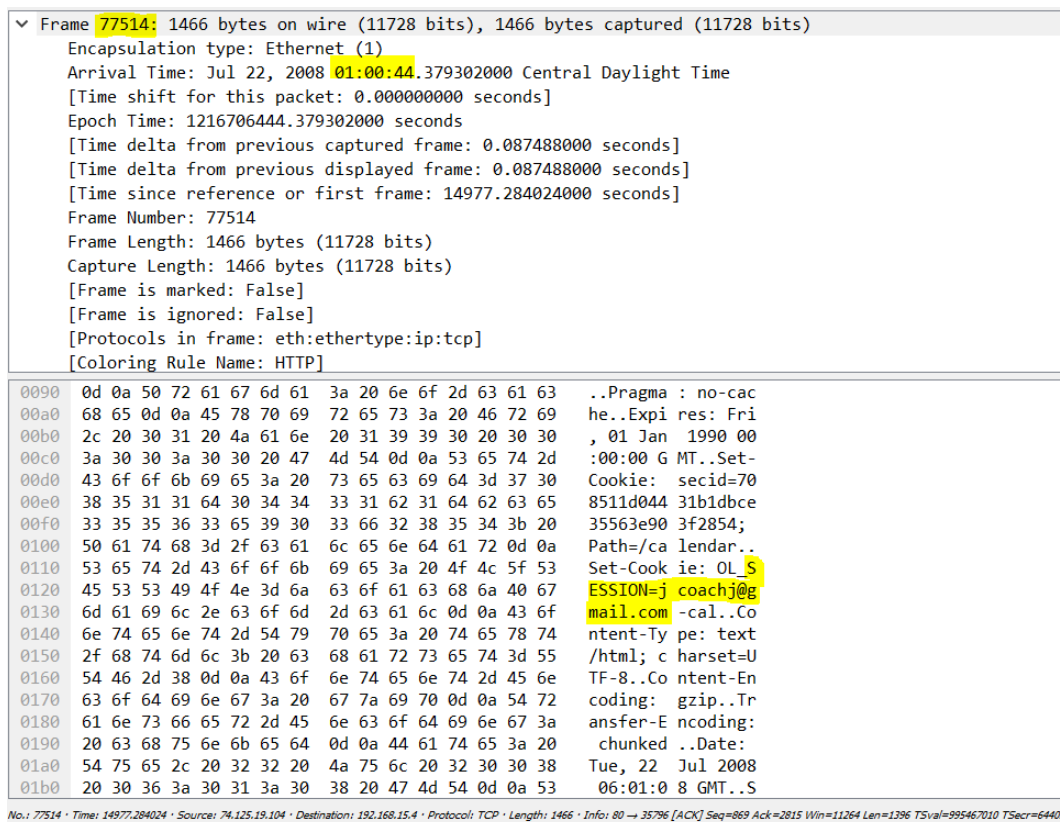


Figure 11

Observe the source and destination MAC address of the devices used in the packet associated with jcoachj gmail id. In the screenshot shown above, ‘Lily’ and ‘Amy’ are buddies on YMSG has common source and destination address. Thus, it can be concluded that ‘Jhonny Couch’ and ‘Amy Smith’ might have done it together.

Also, there is one more packet associated with ‘Jhonny Couch’ mail,

[Coloring Rule String: http || tcp.port == 80 || http2]

- ▼ Ethernet II, Src: Apple\_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPr\_2e:4f:60 (00:1d:d9:2e:4f:60)
  - ▼ Destination: HonHaiPr\_2e:4f:60 (00:1d:d9:2e:4f:60)
    - Address: HonHaiPr\_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: 0xc91ae53f [correct]
  - [FCS Status: Good]
- ▼ Internet Protocol Version 4, Src: 192.168.15.4, Dst: 74.125.19.17

02d0	6d 70 72 6f 78 79 3d 36	75 61 74 4e 63 5a 5a 6d	mproxy=6 uatNcZZm
02e0	42 38 3a 67 6d 70 72 6f	78 79 5f 79 6a 3d 46 52	B8:gmpo xy_yj=FR
02f0	56 31 37 5a 79 57 6e 68	38 3a 67 6d 70 72 6f 78	V17ZyWnh 8:gmpo
0300	79 5f 79 6a 5f 73 75 62	3d 62 7a 67 6f 57 4f 79	y_yj_sub =bzgoWoy
0310	62 41 52 41 3b 20 47 4d	41 49 4c 5f 41 54 3d 78	bARA; GM AIL_AT=x
0320	6e 33 6a 33 32 6f 6b 74	66 32 61 30 71 36 6f 61	n3j32okt f2a0q6oa
0330	33 6b 39 73 66 72 36 64	30 39 79 7a 66 3b 20 47	3k9sfr6d 09yzf; G
0340	4d 41 49 4c 5f 53 55 3d	31 3b 20 67 6d 61 69 6c	MAIL_SU= 1; gmail
0350	63 68 61 74 3d 6a 63 6f	61 63 68 6a 40 67 6d 61	chat=jco achj@ma
0360	69 6c 2e 63 6f 6d 2f 34	37 35 30 39 30 3b 20 50	il.com/4 75090; P
0370	52 45 46 3d 49 44 3d 38	66 63 30 38 31 64 66 35	REF=ID=8 fc081df5
0380	65 37 33 38 61 33 63 3a	54 4d 3d 31 32 31 30 37	e738a3c: TM=12107
0390	34 33 34 36 39 3a 4c 4d	3d 31 32 31 30 37 34 33	43469:LM =1210743
03a0	34 36 39 3a 53 3d 50 69	42 73 79 4a 6b 53 36 63	469:S=Pi BsyJkS6c
03b0	75 2d 55 45 58 56 3b 20	4e 49 44 3d 31 33 3d 74	u-UEXV; NID=13=t
03c0	4a 37 4c 74 45 63 36 7a	31 32 69 48 34 42 50 5f	J7LtEc6z 12iH4BP_
03d0	49 50 79 56 30 67 47 68	69 34 61 4c 63 5a 6f 4a	IPyV0gGh i4aLcZoJ
03e0	63 6a 41 66 37 6c 2d 39	4a 51 32 41 65 6f 44 38	cjAf71-9 JQ2AeoD8
03f0	6f 57 47 39 4e 4a 74 4f	70 37 54 35 74 75 73 6b	owG9NJt0 p7T5tusk

No.: 78968 · Time: 14995.019816 · Source: 192.168.15.4 · Destination: 74.125.19.17 · Protocol: HTTP · Length: 1391 · Info: GET /mail/?ui=1&view=page&name=gp&ver=sh3fb53pgpk&auto=1 HTTP/1.1

Figure 12

This shows that ‘Jhonny Couch’ used Apple\_e2:c0:ce(00:17:f2:e2:c0:ce) also. Even ‘Amy Smith’ used this device (shown in previous screenshots) which also tells us both of them tried to do it together.