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-FGHE6OA MINGW64 ~
$ cat "C:\Users\sunandha\Desktop\forensics\nw forensics\ass3\ip-src.txt" | sort
| uniq -c | sort -n | grep -e " 172\." -e " 192\.168\." -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 i
p.src -e eth.src > "C:\Users\sunandha\Desktop\forensics\nw forensics\ass3\ip-src-and-mac-src.txt"
```

Figure 3

```
sunandha@DESKTOP-FGHE6OA 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\.168\." -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

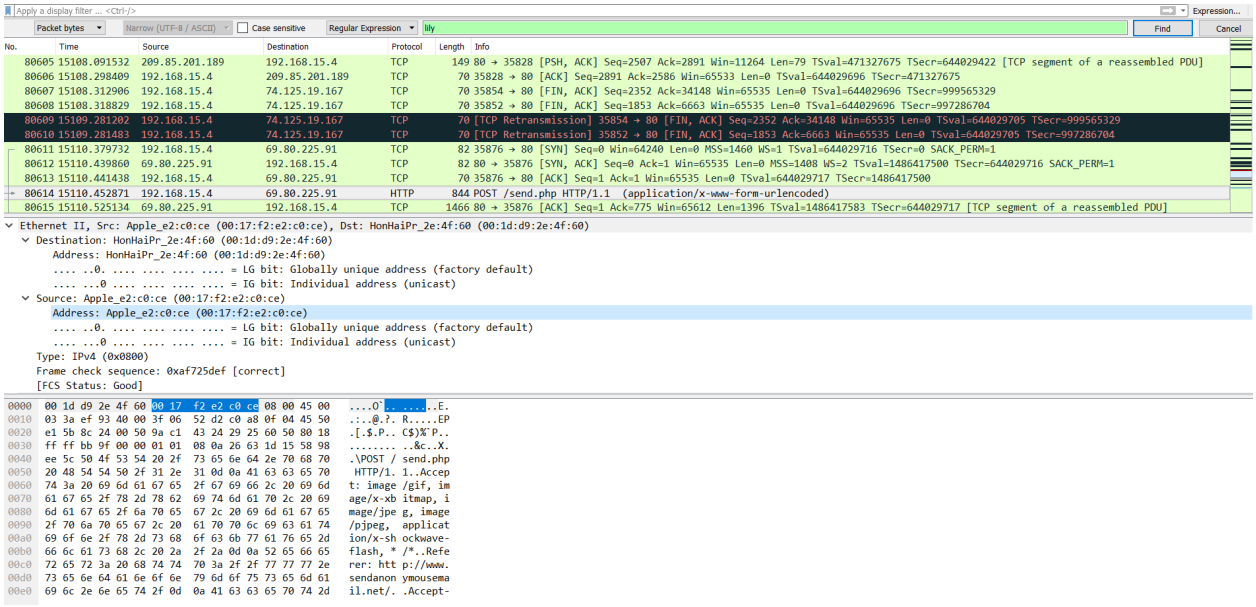

Figure 5

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

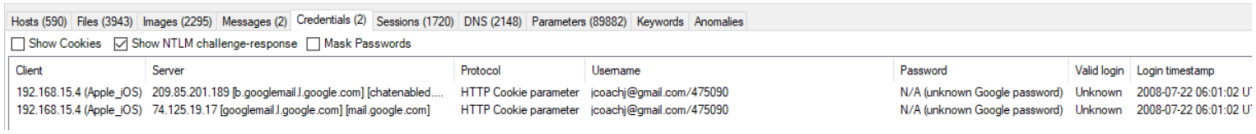

Figure 6

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

Another email in some of the packets were found which is

mylady.ixchel@gmail.com

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

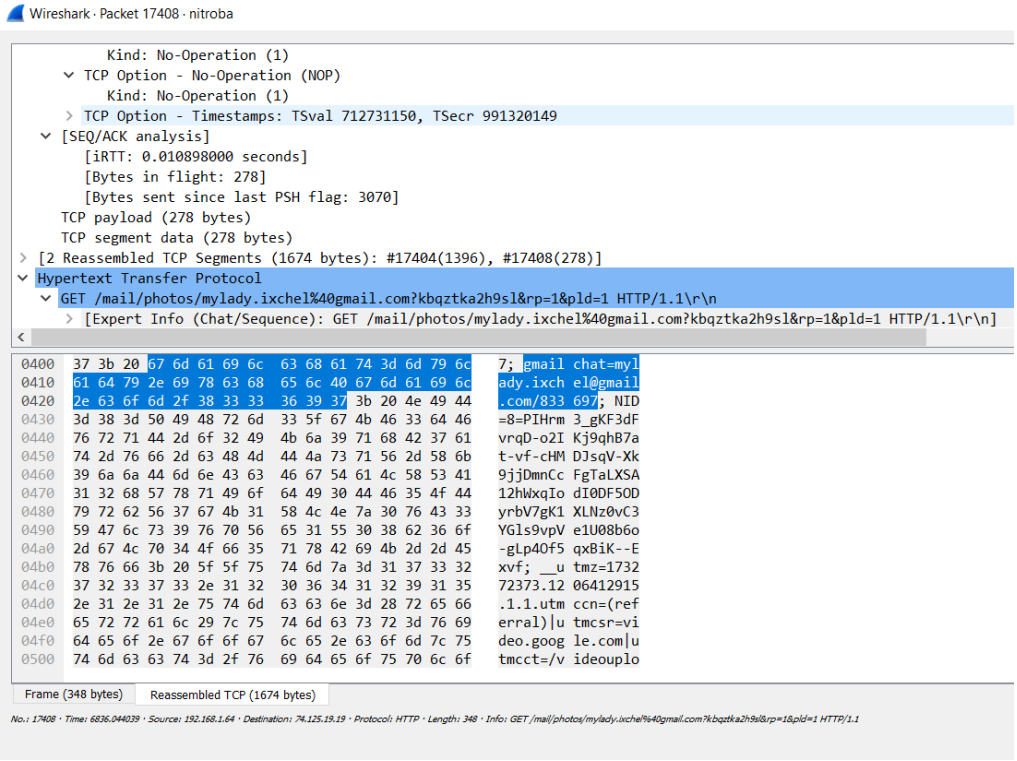

Figure 7

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

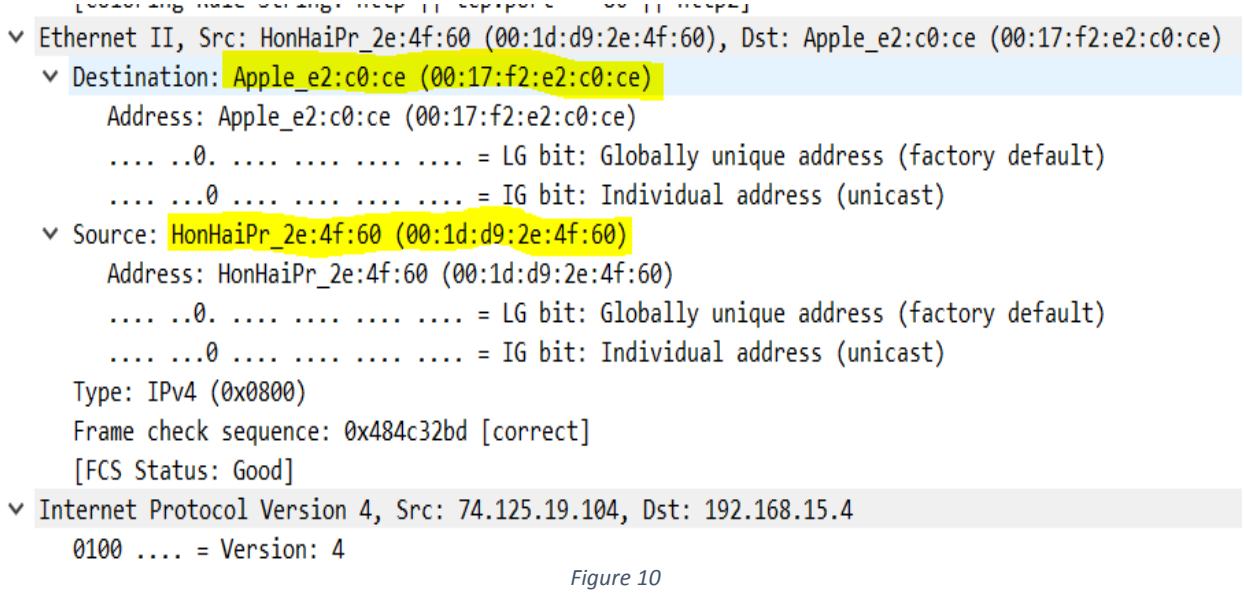

Figure 10

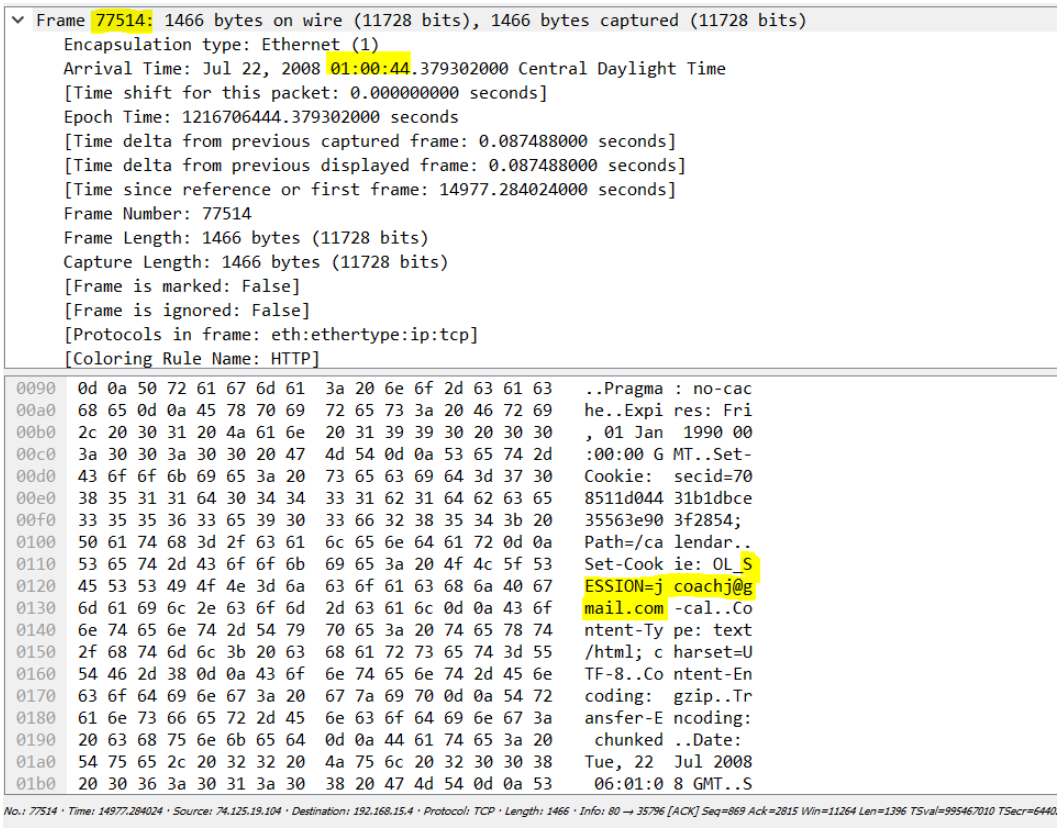

Figure 11

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,

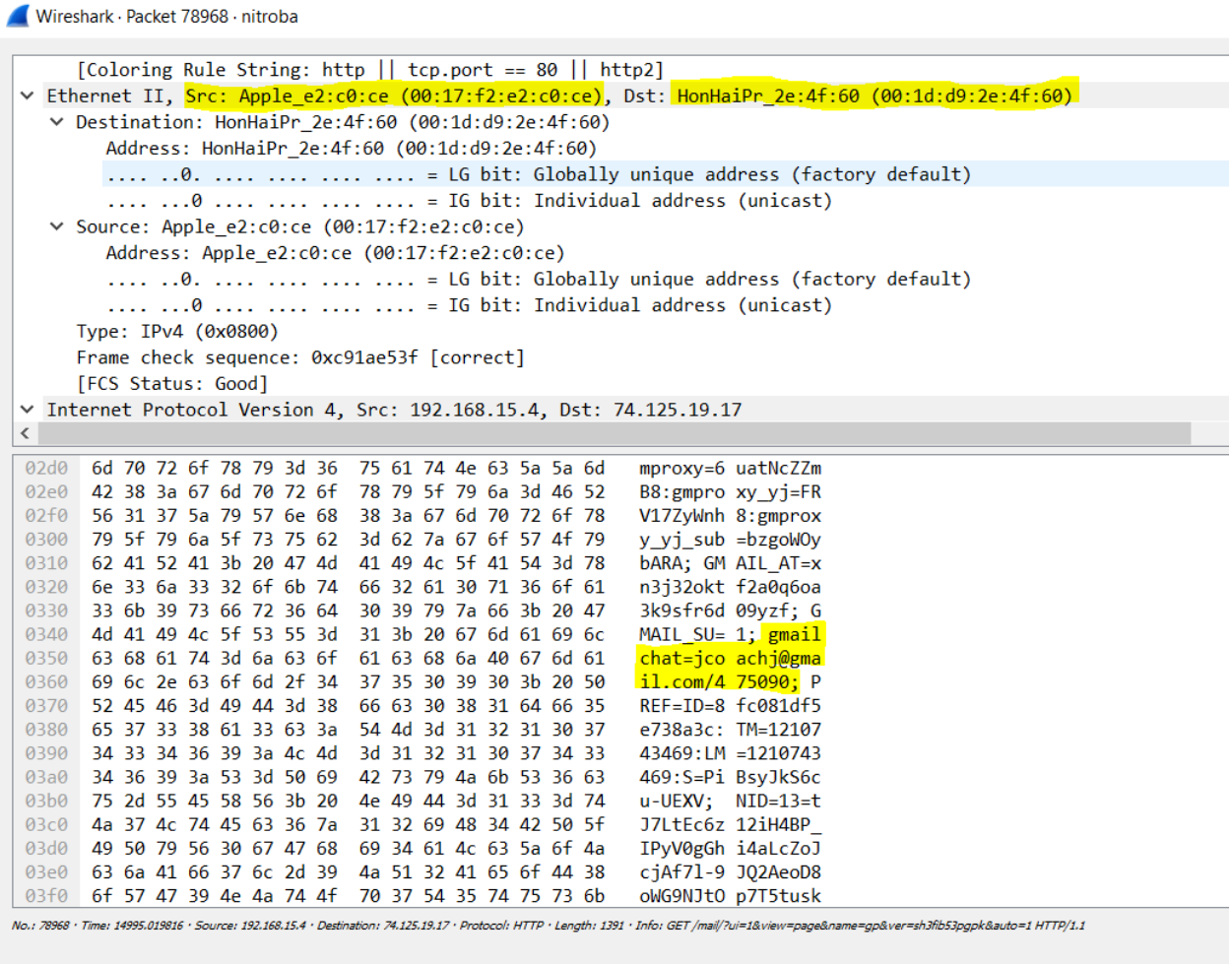

Figure 12

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.