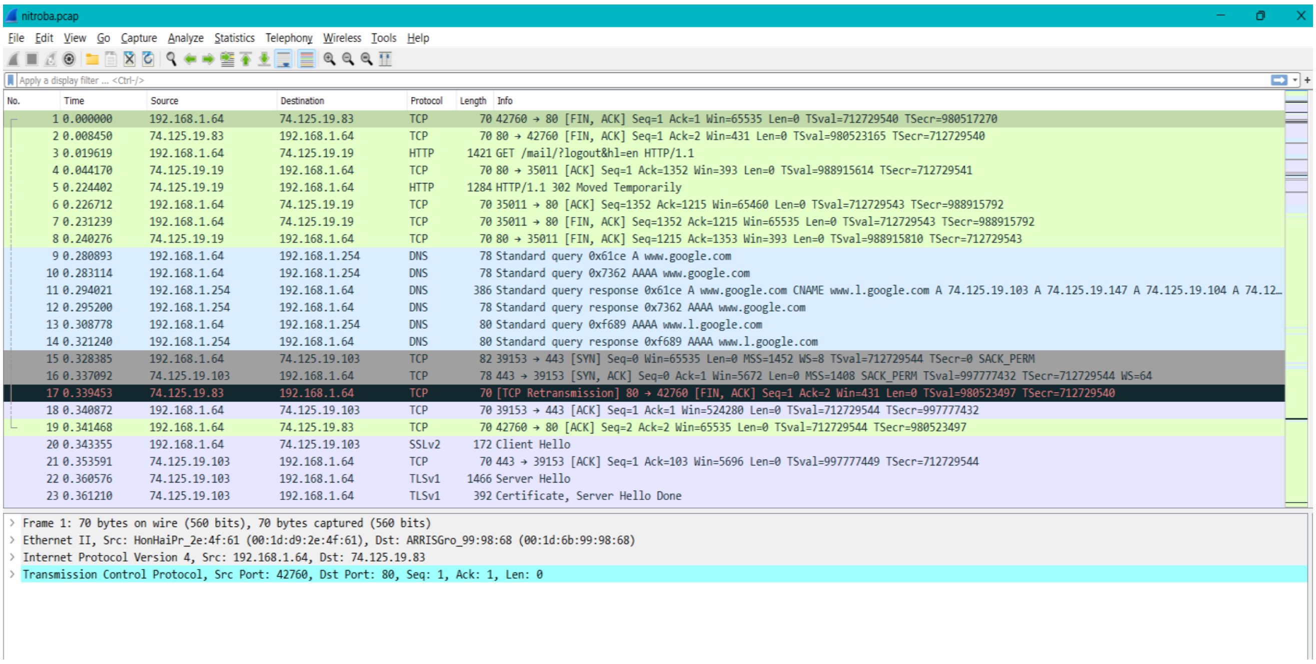
Project3 – Network Forensics

Observation of the PCAP file: After I open the packet capture (PCAP) file in Wireshark, I got a long list of packets captured. The packets are captured in the order of Time, Source, Destination IP`s, Protocol, Length, and information of the packets.


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

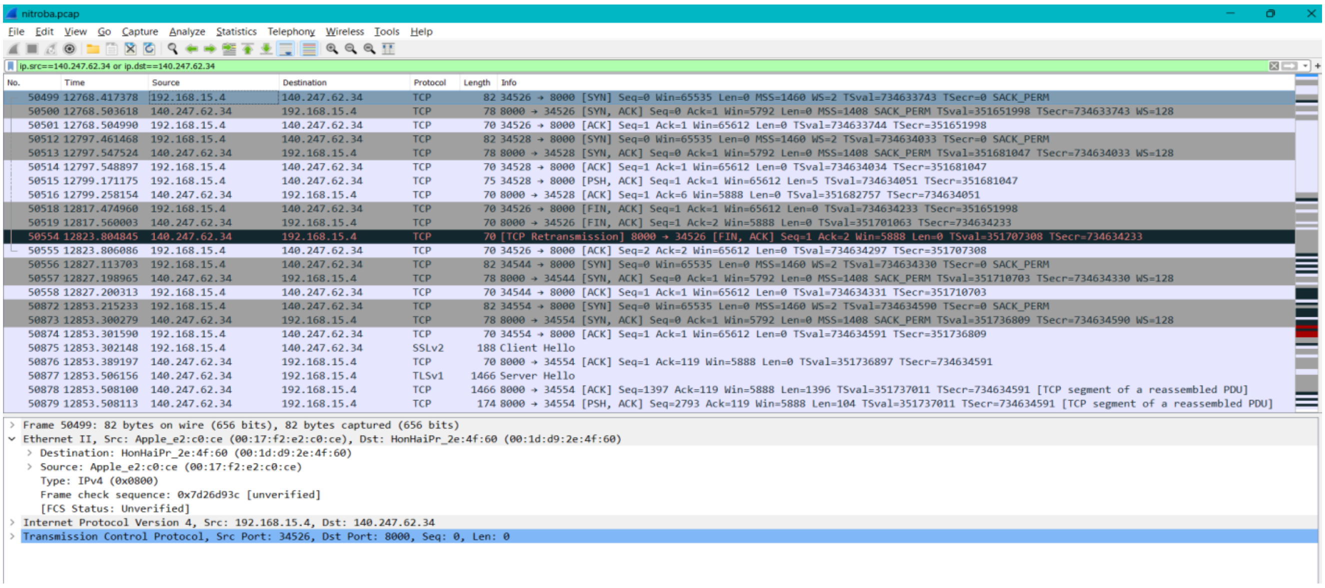
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.64	74.125.19.83	TCP	70	42760 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0 TSval=712729540 TSecr=980517270
2	0.008450	74.125.19.83	192.168.1.64	TCP	70	80 → 42760 [FIN, ACK] Seq=1 Ack=2 Win=431 Len=0 TSval=980523165 TSecr=712729540
3	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 74.125.19.147 A 74.125.19.104 A 74.12…
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=712729544 WS=64
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

```
> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: HonHaiPr_2e:4f:61 (00:1d:d9:2e:4f:61), Dst: ARRISGro_99:98:68 (00:1d:6b:99:98:68)
> 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
```

PCAP File

Map out the Nitroba dorm room network: I am mapping out the dorm room network because the first spoofed email was sent using this network, and the proof for this was seen in the PowerPoint of the challenge slides, where the professor gets the mail from the IP: 140.247.62.34 (which was seen in the email header) and this IP points to the dorm room.

Now, in order to find out who sent the threatening mail, first I will filter the PCAP file using the IP address used in the first email. The filter is written as **ip.src==140.247.62.34 or ip.dst==140.247.62.34** to filter out the IP address.


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src==140.247.62.34 or ip.dst==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=734633743 WS=128
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=734634033 WS=128
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=734634233
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=734634330 WS=128
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=734634590 WS=128
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 of a reassembled PDU]
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 segment of a reassembled PDU]
```

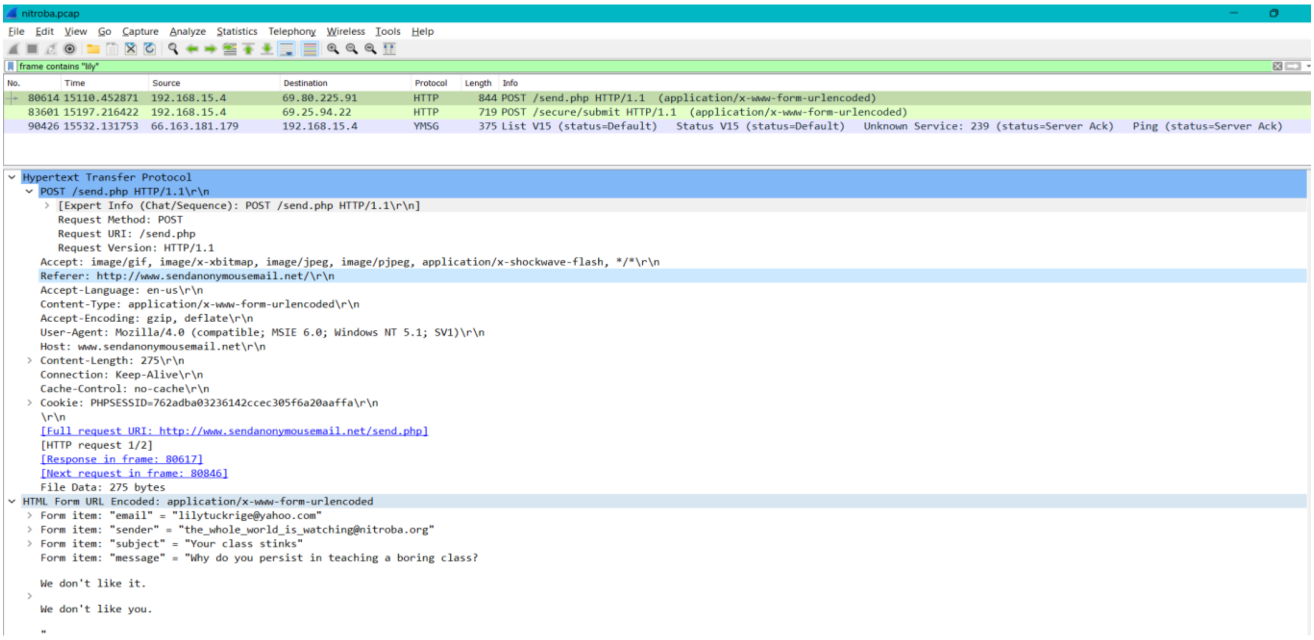
```
> Frame 50499: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
v Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPr_2e:4f:60 (00:1d:d9:2e:4f:60)
  > Destination: HonHaiPr_2e:4f:60 (00:1d:d9:2e:4f:60)
  > Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
    Type: IPv4 (0x0800)
    Frame check sequence: 0x7d26d93c [unverified]
    [FCS Status: Unverified]
> 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
```

PCAP with filtering IP: 140.247.62.34

Now taking a closer look at the screenshot above, the **IP: 192.168.15.4**, plays a central role as it is the only IP bridging with the **IP: 140.247.62.34**. And also, the information of the two IP`s like hardware and MAC addresses of the two physical devices pointed by these IP`s.

Finding who sent the email to lilytuckrige@yahoo.com:

Now, I am using the filter to map out the email address of the professor with the name. The filter is written as **frame contains "lily";** this filter narrows down the list of packets with the name lily. And then I got the packets as below.


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
frame contains "lily"

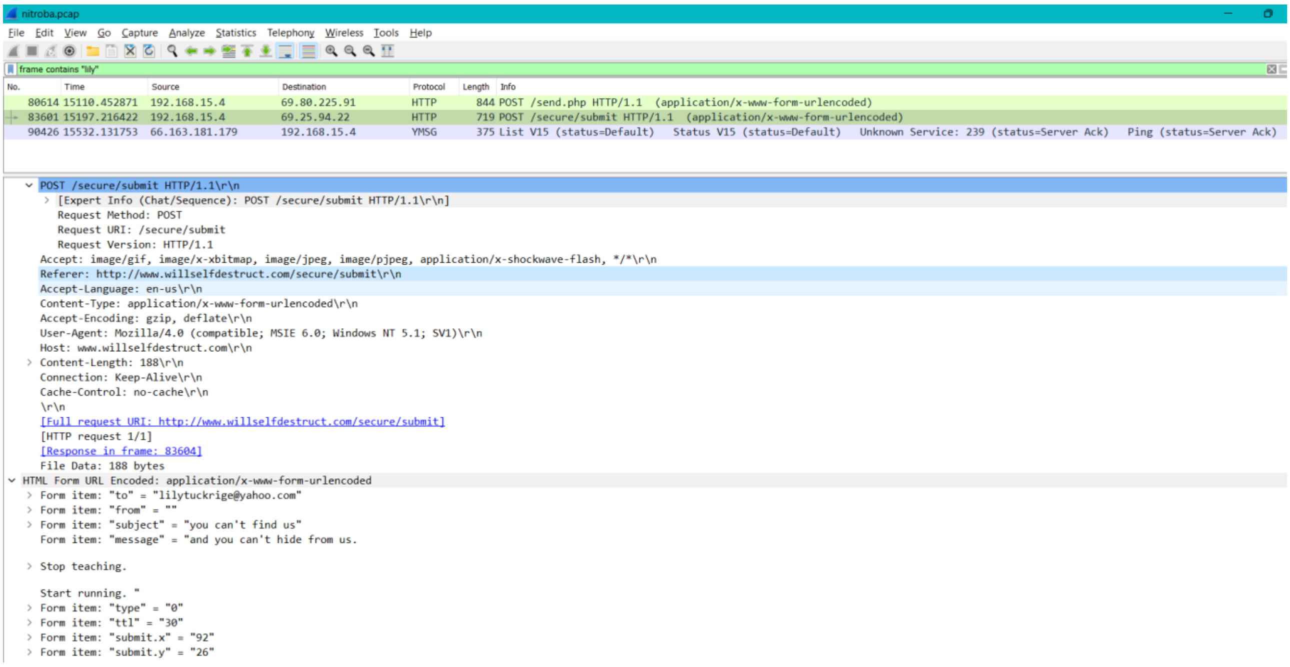
```
No.   Time         Source         Destination    Protocol Length Info
80614 15110.452871 192.168.15.4   69.80.225.91   HTTP      844 POST /send.php HTTP/1.1  (application/x-www-form-urlencoded)
83601 15197.216422 192.168.15.4   69.25.94.22    HTTP      719 POST /secure/submit HTTP/1.1  (application/x-www-form-urlencoded)
90426 15532.131753 66.163.181.179 192.168.15.4   YMSG      375 List V15 (status=Default)   Status V15 (status=Default)   Unknown Service: 239 (status=Server Ack)   Ping (status=Server Ack)
```

```
v Hypertext Transfer Protocol
  v POST /send.php HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): POST /send.php HTTP/1.1\r\n]
      Request Method: POST
      Request URI: /send.php
      Request Version: HTTP/1.1
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
    Referer: http://www.sendanonymousemail.net/\r\n
    Accept-Language: en-us\r\n
    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: www.sendanonymousemail.net\r\n
  > Content-Length: 275\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
  > Cookie: PHPSESSID=762adba03236142ccec305f6a20aaffa\r\n
    \r\n
    [Full request URI: http://www.sendanonymousemail.net/send.php]
    [HTTP request 1/2]
    [Response in frame: 80617]
    [Next request in frame: 80846]
    File Data: 275 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "email" = "lilytuckrige@yahoo.com"
  > Form item: "sender" = "the_whole_world_is_watching@nitroba.org"
  > Form item: "subject" = "Your class stinks"
    Form item: "message" = "Why do you persist in teaching a boring class?

    We don't like it.
  >
    We don't like you.

    "
```

PCAP filtering the email address with the name (Packet1).

As, we can see the first packet contains the harassing message and was sent using sendanonymousemail.net.

I can also say that the message was sent from a particular web browser, and that is Mozilla version-4 (from the screenshot above).


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame contains "lily"

```
No.   Time             Source           Destination     Protocol  Length Info
80614 15110.452871     192.168.15.4     69.80.225.91    HTTP      844 POST /send.php HTTP/1.1  (application/x-www-form-urlencoded)
83601 15197.216422     192.168.15.4     69.25.94.22     HTTP      719 POST /secure/submit HTTP/1.1  (application/x-www-form-urlencoded)
90426 15532.131753     66.163.181.179   192.168.15.4    YMSG      375 List V15 (status=Default)   Status V15 (status=Default)   Unknown Service: 239 (status=Server Ack)   Ping (status=Server Ack)
```

```
  POST /secure/submit HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /secure/submit HTTP/1.1\r\n]
    Request Method: POST
    Request URI: /secure/submit
    Request Version: HTTP/1.1
  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
  Referer: http://www.willselfdestruct.com/secure/submit\r\n
  Accept-Language: en-us\r\n
  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: www.willselfdestruct.com\r\n
  Content-Length: 188\r\n
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  \r\n
  [Full request URI: http://www.willselfdestruct.com/secure/submit]
  [HTTP request 1/1]
  [Response in frame: 83604]
  File Data: 188 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "to" = "lilytuckrige@yahoo.com"
  Form item: "from" = ""
  Form item: "subject" = "you can't find us"
  Form item: "message" = "and you can't hide from us.

  Stop teaching.

  Start running. "
  Form item: "type" = "0"
  Form item: "ttl" = "30"
  Form item: "submit.x" = "92"
  Form item: "submit.y" = "26"
```

PCAP filtering the email address with the name (Packet2).

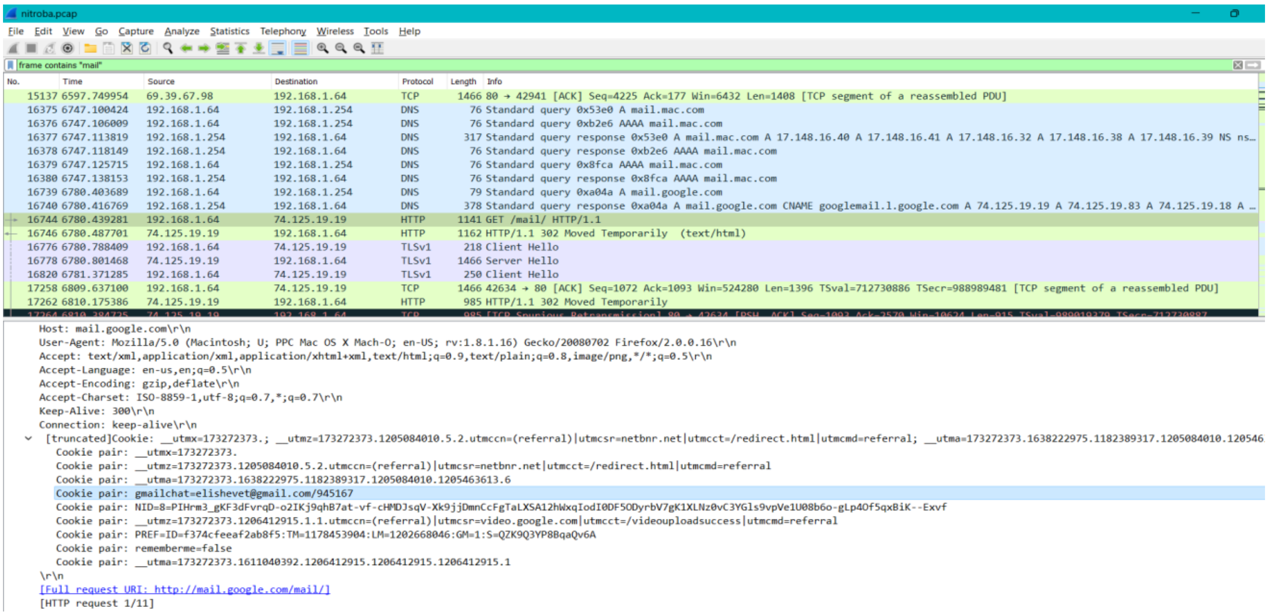
And the second packet contains the harassing message and was sent using willselfdestruct.com with the email header: “you can`t find us” which is exactly the same as shown in the challenge slides.

From this, we can say that the **IP: 192.168.15.4** plays a central role in the threatening email attacks and the harassment faced by the professor Lily Tuckrige.

I can also say that the message was sent from a particular web browser, and that is Mozilla version-4 (from the screenshot above).

<u>Finding information in one of the TCP connections that ID`s the attacker</u>: Now, I will use the filter to try to find the email address of the attacker. I will use the filter **frame contains “mail”** . This filter helps narrow down the search with the mail. And as the packets are displayed, I looked for the packets with frames titled “GET/mail/HTTP/1.1”. They revealed some interesting information like email address used and email platform used.

Before trying to see if we can find the email address of the attacker, first lets find to see if we can identify other TCP connections that below to the attacker.


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame contains "mail"

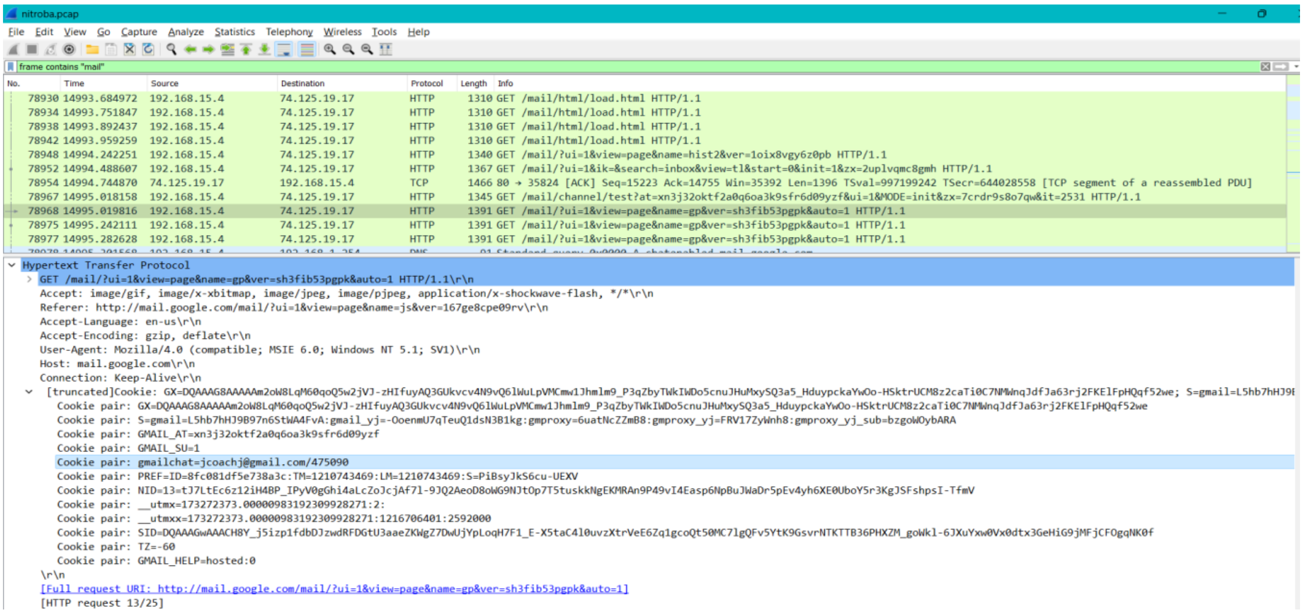
```
No.   Time          Source          Destination     Protocol Length Info
15137 6597.749954   69.39.67.98     192.168.1.64    TCP      1466 80 → 42941 [ACK] Seq=4225 Ack=177 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
16375 6747.100424   192.168.1.64    192.168.1.254   DNS        76 Standard query 0x53e0 A mail.mac.com
16376 6747.106009   192.168.1.64    192.168.1.254   DNS        76 Standard query 0xb2e6 AAAA mail.mac.com
16377 6747.113819   192.168.1.254   192.168.1.64    DNS       317 Standard query response 0x53e0 A mail.mac.com A 17.148.16.40 A 17.148.16.41 A 17.148.16.32 A 17.148.16.38 A 17.148.16.39 NS ns…
16378 6747.118149   192.168.1.254   192.168.1.64    DNS        76 Standard query response 0xb2e6 AAAA mail.mac.com
16379 6747.125715   192.168.1.64    192.168.1.254   DNS        76 Standard query 0x8fca AAAA mail.mac.com
16380 6747.138153   192.168.1.254   192.168.1.64    DNS        76 Standard query response 0x8fca AAAA mail.mac.com
16739 6780.403689   192.168.1.64    192.168.1.254   DNS        79 Standard query 0xa04a A mail.google.com
16740 6780.416769   192.168.1.254   192.168.1.64    DNS       378 Standard query response 0xa04a A mail.google.com CNAME googlemail.l.google.com A 74.125.19.19 A 74.125.19.83 A 74.125.19.18 A …
16744 6780.439281   192.168.1.64    74.125.19.19    HTTP     1141 GET /mail/ HTTP/1.1
16746 6780.487701   74.125.19.19    192.168.1.64    HTTP     1162 HTTP/1.1 302 Moved Temporarily  (text/html)
16776 6780.788409   192.168.1.64    74.125.19.19    TLSv1     218 Client Hello
16778 6780.801468   74.125.19.19    192.168.1.64    TLSv1    1466 Server Hello
16820 6781.371285   192.168.1.64    74.125.19.19    TLSv1     250 Client Hello
17258 6809.637100   192.168.1.64    74.125.19.19    TCP      1466 42634 → 80 [ACK] Seq=1072 Ack=1093 Win=524280 Len=1396 TSval=712730886 TSecr=988989481 [TCP segment of a reassembled PDU]
17262 6810.175386   74.125.19.19    192.168.1.64    HTTP      985 HTTP/1.1 302 Moved Temporarily
```

```
    Host: mail.google.com\r\n
    User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.1.16) Gecko/20080702 Firefox/2.0.0.16\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
  ⌄ [truncated]Cookie: __utmx=173272373.; __utmz=173272373.1205084010.5.2.utmccn=(referral)|utmcsr=netbnr.net|utmcct=/redirect.html|utmcmd=referral; __utma=173272373.1638222975.1182389317.1205084010.120546
      Cookie pair: __utmx=173272373.
      Cookie pair: __utmz=173272373.1205084010.5.2.utmccn=(referral)|utmcsr=netbnr.net|utmcct=/redirect.html|utmcmd=referral
      Cookie pair: __utma=173272373.1638222975.1182389317.1205084010.1205463613.6
      Cookie pair: gmailchat=elishevet@gmail.com/945167
      Cookie pair: NID=8=PIHrm3_gKF3dFvrqD-o2IKj9qhB7at-vf-cHMDJsqV-Xk9jjDmnCcFgTaLXSA12hWxqIodI0DF5ODyrbV7gK1XLNz0vC3YGls9vpVe1U08b6o-gLp4Of5qxBiK--Exvf
      Cookie pair: __utmz=173272373.1206412915.1.1.utmccn=(referral)|utmcsr=video.google.com|utmcct=/videouploadsuccess|utmcmd=referral
      Cookie pair: PREF=ID=f374cfeeaf2ab8f5:TM=1178453904:LM=1202668046:GM=1:S=QZK9Q3YP8BqaQv6A
      Cookie pair: rememberme=false
      Cookie pair: __utma=173272373.1611040392.1206412915.1206412915.1206412915.1
    \r\n
    [Full request URI: http://mail.google.com/mail/]
    [HTTP request 1/11]
```

PCAP file to find the email address of the sender.

Now, if we look at the above screenshot, we can look into the cookie pair, where it says **gmailchat=elishevet@gmail.com/945167** and the full request URI is **http://mail.google.com/mail/** .

Now that since we can identify the email address of the sender and the http address. Now, we can find the attackers email address using the same filter.


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame contains "mail"

```
No.   Time           Source          Destination     Protocol Length Info
78930 14993.684972   192.168.15.4    74.125.19.17    HTTP     1310 GET /mail/html/load.html HTTP/1.1
78934 14993.751847   192.168.15.4    74.125.19.17    HTTP     1310 GET /mail/html/load.html HTTP/1.1
78938 14993.892437   192.168.15.4    74.125.19.17    HTTP     1310 GET /mail/html/load.html HTTP/1.1
78942 14993.959259   192.168.15.4    74.125.19.17    HTTP     1310 GET /mail/html/load.html HTTP/1.1
78948 14994.242251   192.168.15.4    74.125.19.17    HTTP     1340 GET /mail/?ui=1&view=page&name=hist2&ver=1oix8vgy6z0pb HTTP/1.1
78952 14994.488607   192.168.15.4    74.125.19.17    HTTP     1367 GET /mail/?ui=1&ik=&search=inbox&view=tl&start=0&init=1&zx=2uplvqmc8gmh HTTP/1.1
78954 14994.744870   74.125.19.17    192.168.15.4    TCP      1466 80 → 35824 [ACK] Seq=15223 Ack=14755 Win=35392 Len=1396 TSval=997199242 TSecr=644028558 [TCP segment of a reassembled PDU]
78967 14995.018158   192.168.15.4    74.125.19.17    HTTP     1345 GET /mail/channel/test?at=xn3j32oktf2a0q6oa3k9sfr6d09yzf&ui=1&MODE=init&zx=7crdr9s8o7qw&it=2531 HTTP/1.1
78968 14995.019816   192.168.15.4    74.125.19.17    HTTP     1391 GET /mail/?ui=1&view=page&name=gp&ver=sh3fib53pgpk&auto=1 HTTP/1.1
78975 14995.242111   192.168.15.4    74.125.19.17    HTTP     1391 GET /mail/?ui=1&view=page&name=gp&ver=sh3fib53pgpk&auto=1 HTTP/1.1
78977 14995.282628   192.168.15.4    74.125.19.17    HTTP     1391 GET /mail/?ui=1&view=page&name=gp&ver=sh3fib53pgpk&auto=1 HTTP/1.1
```

```
⌄ Hypertext Transfer Protocol
  > GET /mail/?ui=1&view=page&name=gp&ver=sh3fib53pgpk&auto=1 HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
    Referer: http://mail.google.com/mail/?ui=1&view=page&name=js&ver=167ge8cpe09rv\r\n
    Accept-Language: en-us\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
    Connection: Keep-Alive\r\n
  ⌄ [truncated]Cookie: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw1Jhmlm9_P3qZbyTWkIWDo5cnuJHuMxySQ3a5_HduypckaYwOo-HSktrUCM8z2caTi0C7NMWnqJdfJa63rj2FKElFpHQqf52we; S=gmail=L5hb7hHJ9I
      Cookie pair: GX=DQAAAG8AAAAAm2oW8LqM60qoQ5w2jVJ-zHIfuyAQ3GUkvcv4N9vQ6lWuLpVMCmw1Jhmlm9_P3qZbyTWkIWDo5cnuJHuMxySQ3a5_HduypckaYwOo-HSktrUCM8z2caTi0C7NMWnqJdfJa63rj2FKElFpHQqf52we
      Cookie pair: S=gmail=L5hb7hHJ9B97n6StWA4FvA:gmail_yj=-OoenmU7qTeuQ1dsN3B1kg:gmproxy=6uatNcZZmB8:gmproxy_yj=FRV17ZyWnh8:gmproxy_yj_sub=bzgoWOybARA
      Cookie pair: GMAIL_AT=xn3j32oktf2a0q6oa3k9sfr6d09yzf
      Cookie pair: GMAIL_SU=1
      Cookie pair: gmailchat=jcoachj@gmail.com/475090
      Cookie pair: PREF=ID=8fc081df5e738a3c:TM=1210743469:LM=1210743469:S=PiBsyJkS6cu-UEXV
      Cookie pair: NID=13=tJ7LtEc6z12iH4BP_IPyV0gGhi4aLcZoJcjAf7l-9JQ2AeoD8oWG9NJtOp7T5tuskkNgEKMRAn9P49vI4Easp6NpBuJWaDr5pEv4yh6XE0UboY5r3KgJSFshpsI-TfmV
      Cookie pair: __utmx=173272373.00000983192309928271:2:
      Cookie pair: __utmxx=173272373.00000983192309928271:1216706401:2592000
      Cookie pair: SID=DQAAAGwAAACH8Y_j5izp1fdbDJzwdRFDGtU3aaeZKWgZ7DwUjYpLoqH7F1_E-X5taC4l0uvzXtrVeE6Zq1gcoQt50MC7lgQFv5YtK9GsvrNTKTTB36PHXZM_goWkl-6JXuYxw0Vx0dtx3GeHiG9jMFjCFOgqNK0f
      Cookie pair: TZ=-60
      Cookie pair: GMAIL_HELP=hosted:0
    \r\n
    [Full request URI: http://mail.google.com/mail/?ui=1&view=page&name=gp&ver=sh3fib53pgpk&auto=1]
    [HTTP request 13/25]
```

PCAP file to find the email address of the attacker.

Now, if we look at the above screenshot, we can look into the cookie pair, where it says **gmailchat=jcoach@gmail.com/475090**. Now that we identified the attackers email address, we just have to prove that this is the attacker, so in order to do that, we can check the IP address of the sender to the IP address of the previously observed IP address. Since the IP address (192.168.15.4) is matching with the previous IP address, we can say that **jcoach@gmail.com** is the attacker. Since, now that we have a potential name "jcoach", we can compare it with the list of names of the students in the classroom and conclude. We have a match **with Johnny Coach**.