

1.0 BACKGROUND INFORMATION	2
2.0 INVESTIGATION SUMMARY	2
3.0 EVENT TIMELINE :	7
4.0 REMEDIATION AND RECOVERY:	8

Cyber Harassment Incident Investigation and Remediation Report at Nitroba University using Wireshark

1.0 BACKGROUND INFORMATION

Nitroba's IT department received an email from Lily Tuckrige, a teacher in the Chemistry Department. Tuckrige has been receiving harassing emails and she suspects that they are being sent by a student in her class Chemistry 109, which she is teaching this summer. The email was received at Tuckrige's personal email account, lilytuckrige@yahoo.com. She took a screenshot of the web browser and sent it in.

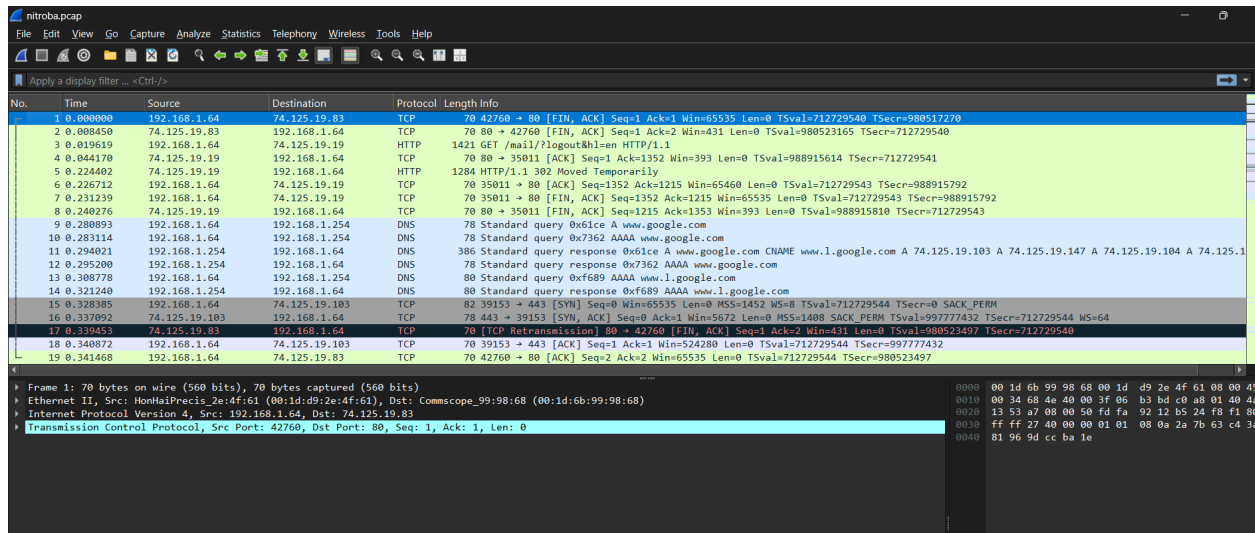
The system administrator who received the complaint wrote back to Tuckrige that Nitroba needed the full headers of the email message. Tuckrige responded by clicking the "Full message headers" button in Yahoo Mail and sent in another screen shot, this one with mail headers.

The mail header shows that the mail message originated from the IP address [140.247.62.34](#), which is a Nitroba student dorm room. Three women share the dorm room. Nitroba provides an Ethernet connection in every dorm room but not Wi-Fi access, so one of the women's friends installed a Wi-Fi router in the room. There is no password on the Wi-Fi.

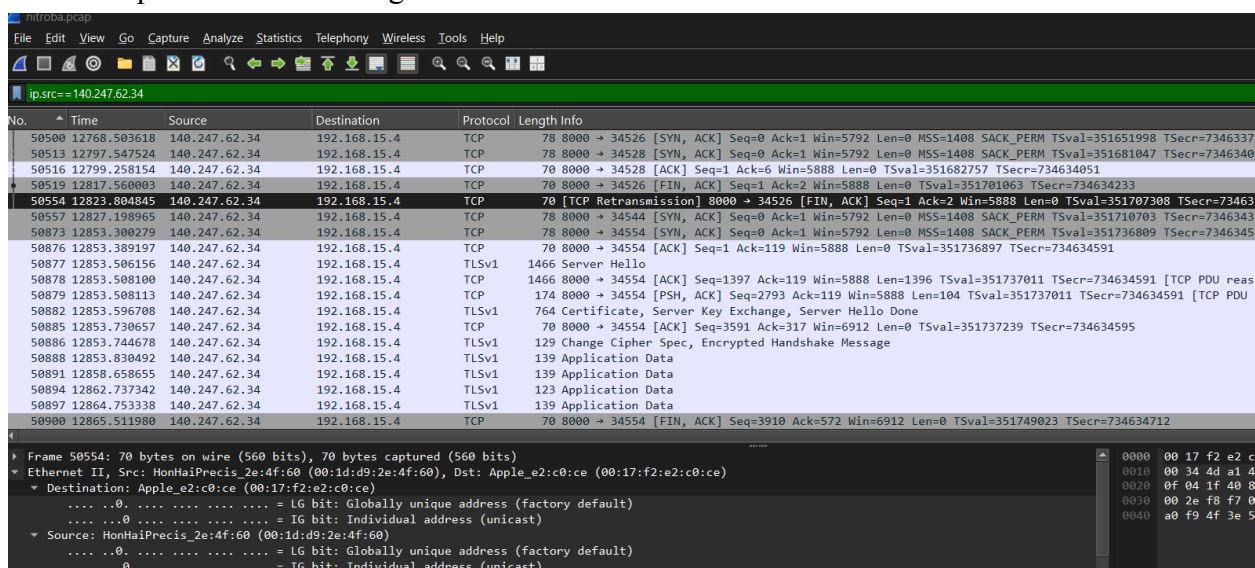
Because several email messages appear to come from the IP address, Nitroba decides to place a network sniffer on the ethernet port. All of the packets are logged. On Monday 7/21 Tuckrige received another harassing email. But this time instead of receiving it directly, the perpetrator sent it through a web-based service called "[willselfdestruct.com](#)." The website briefly shows the message to Tuckrige, and then the website reports that the "Message Has Been Destroyed."

2.0 INVESTIGATION SUMMARY

Step 01 : Opening the pcap file in wireshark



Step 2. Filtering the packets coming from source IP address 140.247.62.34 as the email came from this ip address to tuckridge



Now we have found the ip address that used to send the email and the destination address.

Step 03: Lets check the source and destination mac address , we can see the source used apple device and the mac address is also stated below from the finding

```

▶ 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)
    .... 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)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0 .... = IG bit: Individual address (unicast)
  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

```

Step 04: Now we will check the email message frames that have mentioned the mail id of the teacher. We will use “lilytuckridge”. And we got the source mail address as **192.168.15.4**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame contains "lilytuckridge"

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	Buddy List (status=Ok) Buddy Info (status=Ok) Preference (status=Notify) Ping (status=No)

```

▶ Frame 80614: 844 bytes on wire (6752 bits), 844 bytes captured (6752 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)
    .... 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)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 19]
  Frame check sequence: 0xaf725def [unverified]
  [FCS Status: Unverified]
▼ Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.80.225.91
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 826

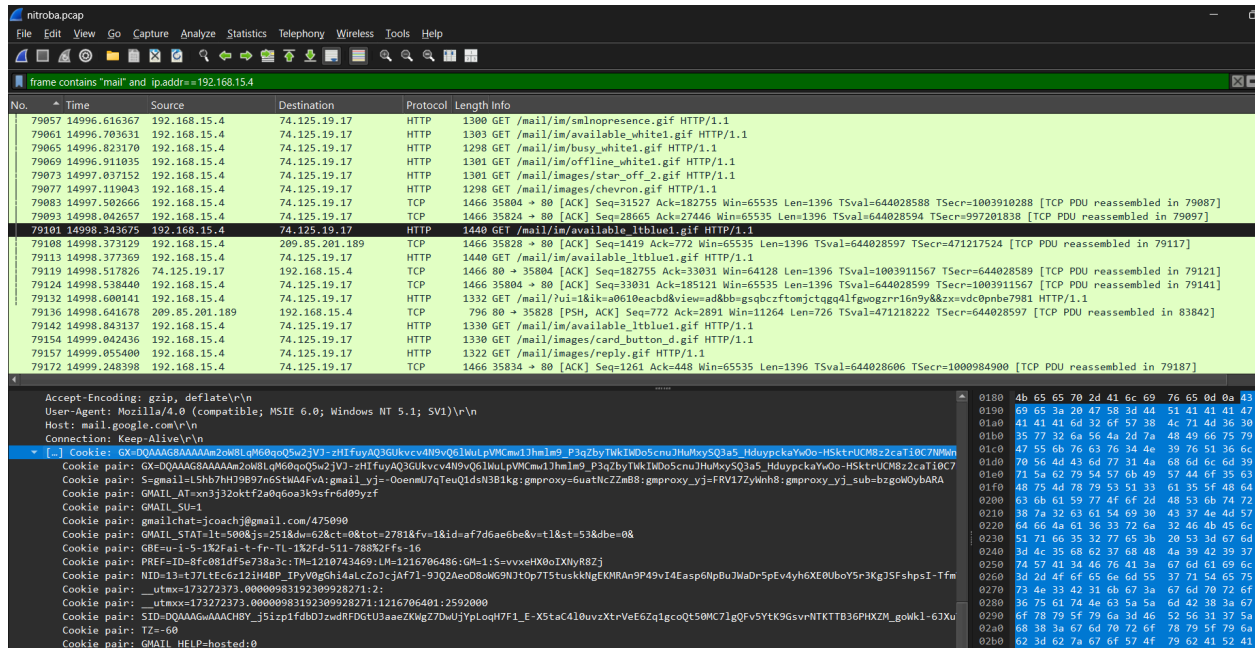
```

Step 05: Here we can observe the mail packets and find out the packet that has been sent to the teacher by threatening her

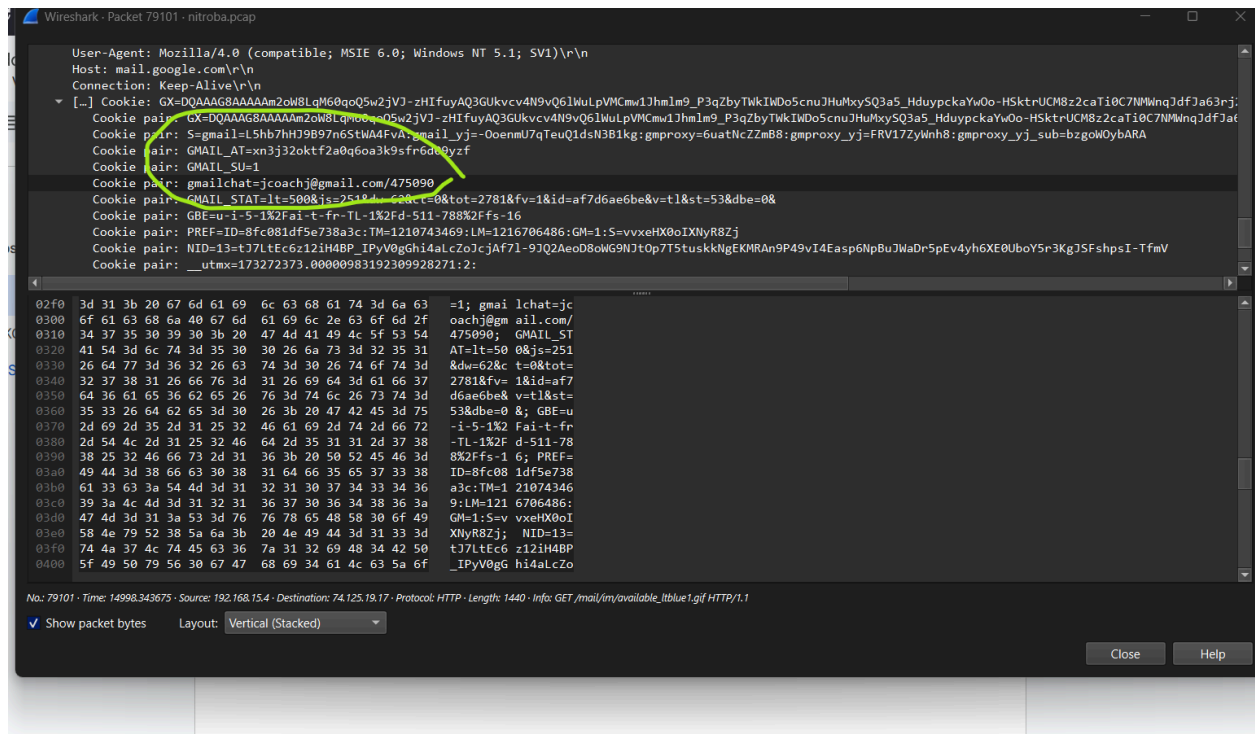
```
Content-Length: 275\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
Cookie: PHPSESSID=762adba03236142ccec305f6a20aaffa\r\n
\r\n
[Response in frame: 80617]
[Full request URI: http://www.sendanonymousemail.net/send.php]
File Data: 275 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "email" = "lilytuckrige@yahoo.com"
  Form item: "sender" = "the_whole_world_is_watching@nitroba.org"
  Form item: "subject" = "Your class stinks"
    Key: subject
    Value: Your class stinks
0230 61 0d 0a 0d 0a 65 6d 61 69 6c 3d 6c 69 6c 79 74 a...ema il=lilyt
0240 75 63 6b 72 69 67 65 40 79 61 68 6f 6f 2e 63 6f uckrige@ yahoo.co
0250 6d 26 73 65 6e 64 65 72 3d 74 68 65 5f 77 68 6f m&sender =the_who
0260 6c 65 5f 77 6f 72 6c 64 5f 69 73 5f 77 61 74 63 le_world _is_watc
0270 68 69 6e 67 40 6e 69 74 72 6f 62 61 2e 6f 72 67 hing@nit roba.org
0280 26 73 75 62 6a 65 63 74 3d 59 6f 75 72 2b 63 6c &subject =Your+cl
0290 61 73 73 2b 73 74 69 6e 6b 73 26 6d 65 73 73 61 ass+stin ks&messa
02a0 67 65 3d 57 68 79 2b 64 6f 2b 79 6f 75 2b 70 65 ge=Why+d otyou+pe
02b0 72 73 69 73 74 2b 69 6e 2b 74 65 61 63 68 69 6e rsist+in +teachin
02c0 67 2b 61 2b 62 6f 72 69 6e 67 2b 63 6c 61 73 73 g+a+bori ng+class
02d0 25 33 46 25 30 44 25 30 41 25 30 44 25 30 41 57 %3F%0D%0 A%0D%0AW
02e0 65 2b 64 6f 6e 25 32 37 74 2b 6c 69 6b 65 2b 69 e+don%27 t+like+i
02f0 74 2e 25 30 44 25 30 41 25 30 44 25 30 41 57 65 t.%0D%0A %0D%0AWe
0300 2b 64 6f 6e 25 32 37 74 2b 6c 69 6b 65 2b 79 6f +don%27t +like+yo
0310 75 2e 25 30 44 25 30 41 25 30 44 25 30 41 26 73 u.%0D%0A %0D%0A&s
0320 65 63 75 72 69 74 79 5f 63 6f 64 65 3d 78 6b 70 ecurity_ code=xkp
0330 6d 6b 62 26 73 75 62 6d 69 74 3d 2b 2b 2b 53 45 mkb&subm it=+++SE
0340 4e 44 25 32 31 2b 2b 2b af 72 5d ef ND%21+++ -r]
```

```
Wireshark - Packet 83601 - nitroba.pcap
Key: from
Value:
  Form item: "subject" = "you can't find us"
  Key: subject
  Value: you can't find us
  Form item: "message" = "and you can't hide from us.\r\n\r\nStop teaching.\r\n\r\nStart running. "
  Key: message
  Value: and you can't hide from us.\r\n\r\nStop teaching.\r\n\r\nStart running.
  Form item: "type" = "0"
  Key: type
  Value: 0
  Form item: "ttl" = "30"
  Key: ttl
  Value: 30
  Form item: "submit.x" = "92"
0000 00 1d d9 2e 4f 60 00 17 f2 e2 c0 ce 08 00 45 00 ...O`... ..E
0010 02 bd 02 ca 40 00 3f 06 c3 95 c0 a8 0f 04 45 19 ...@.?.. ..E
0020 5e 16 8c cc 00 50 fc 72 02 f0 75 b8 f4 26 80 18 ^...P.r ..u. &..
0030 fb 28 fa c7 00 00 01 01 08 0a 26 63 20 78 73 00 (. ... ..&c xs
0040 cb 95 50 4f 53 54 20 2f 73 65 63 75 72 65 2f 73 ..POST / secure/s
0050 75 62 6d 69 74 20 48 54 54 50 2f 31 2e 31 0d 0a ubmit HT TP/1.1..
0060 41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 67 69 Accept: image/gi
0070 66 2c 20 69 6d 61 67 65 2f 78 2d 78 62 69 74 6d f, image /x-xbitm
0080 61 70 2c 20 69 6d 61 67 65 2f 6a 70 65 67 2c 20 ap, imag e/jpeg,
0090 69 6d 61 67 65 2f 70 6a 70 65 67 2c 20 61 70 70 image/pj peg, app
```

Step 06: Now we will filter out the packet with the suspicious email address as 192. and the packet that contains the “mail “



Step 07 : Opening the HTTP frame. Inside the HTTP section there is a cookie section. In that cookie section where the original mail id is mentioned that used to send the message .



And Boom !! We have found out the mail address that has been used to send message to the teacher from the student list jcoach@gmail.com its actually johnny coach

Chemistry 109 class list:

Teacher: Lily Tuckrige

Students:

Amy Smith
Burt Greedom
Tuck Gorge
Ava Book
Johnny Coach
Jeremy Ledvkin
Nancy Colburne
Tamara Perkins
Esther Pringle
Asar Misrad
Jenny Kant

3.0 EVENT TIMELINE :

Date	Event Description
Before 7/21	Lily Tuckrige (Chemistry teacher) begins receiving harassing emails at her personal Yahoo email account. She suspects a student from her Chemistry 109 class.
Complaint Filed	Tuckrige emails the Nitroba IT department with a screenshot of the email.
Follow-up	IT requests full email headers to trace the source. Tuckrige complies and sends the headers.
Header Analysis	Email found to originate from IP address 140.247.62.34 , linked to a student dorm room shared by three women. Dorm uses unsecured Wi-Fi (no password).
Network Monitoring	IT sets up a network sniffer on the dorm's Ethernet port to capture all packets for further

	investigation.
Incident on 7/21	Another harassing message is received, but this time via the web-based ephemeral messaging service “willselfdestruct.com.”
PCAP Analysis	Investigators analyze packet captures using Wireshark . They trace HTTP traffic and identify: - Device type: Apple device - Local IP address: 192.168.15.4 - Destination: lilytuckrige@yahoo.com
Final Discovery	By filtering HTTP packets and inspecting cookies, they find the originating email used: jcoach@gmail.com . This account belongs to Johnny Coach , a student in the class.

4.0 REMEDIATION AND RECOVERY:

Identify and Sanction the Perpetrator:

- Confirm the identity of Johnny Coach using university records.
- Notify academic and disciplinary boards for appropriate academic or legal action based on harassment policies.

Network Security Hardening:

- Remove or disable the unauthorized Wi-Fi router in the dorm room.
- Enforce policies that prohibit personal, unsecured network equipment in university housing.

Awareness and Policy Enforcement:

- Conduct cybersecurity awareness workshops for students about:
 - Responsible digital behavior.
 - Dangers of anonymous harassment tools.
 - Importance of securing personal networks.
- Update dormitory IT usage policies to include penalties for misuse.

Technical Monitoring Enhancements:

- Consider deploying intrusion detection systems (IDS) and network activity logging in sensitive areas like dormitories.
- Create a reporting mechanism for faculty and staff to flag suspicious student activity anonymously.

Support for the Victim:

- Offer counseling and support to Lily Tuckrige.
- Reassure her of Nitroba's commitment to ensuring a safe work environment.

Review and Audit:

- Conduct a post-mortem analysis and internal audit to evaluate the incident response process.
- Create a standard operating procedure (SOP) for similar future incidents.