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 Tuckridge's personal email account, lilytuckrige@yahoo.com. She took a screenshot of the web browser and sent it in.

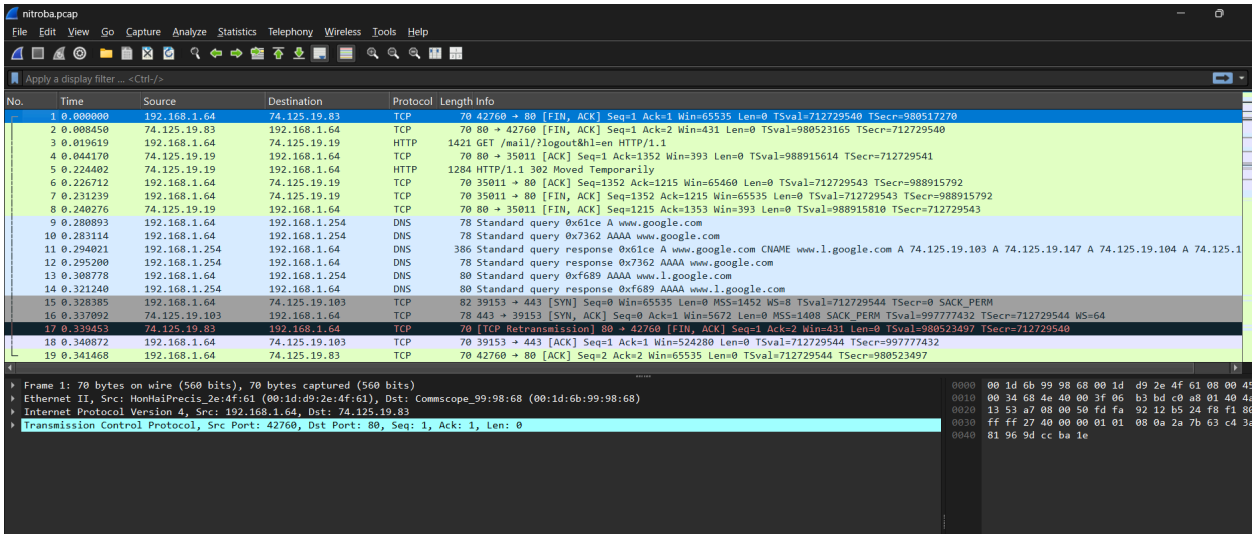
The system administrator who received the complaint wrote back to Tuckridge that Nitroba needed the full headers of the email message. Tuckridge responded by clicking the "Full message headers" button in Yahoo Mail and sent in another screen shot, this one with mail headers.

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.

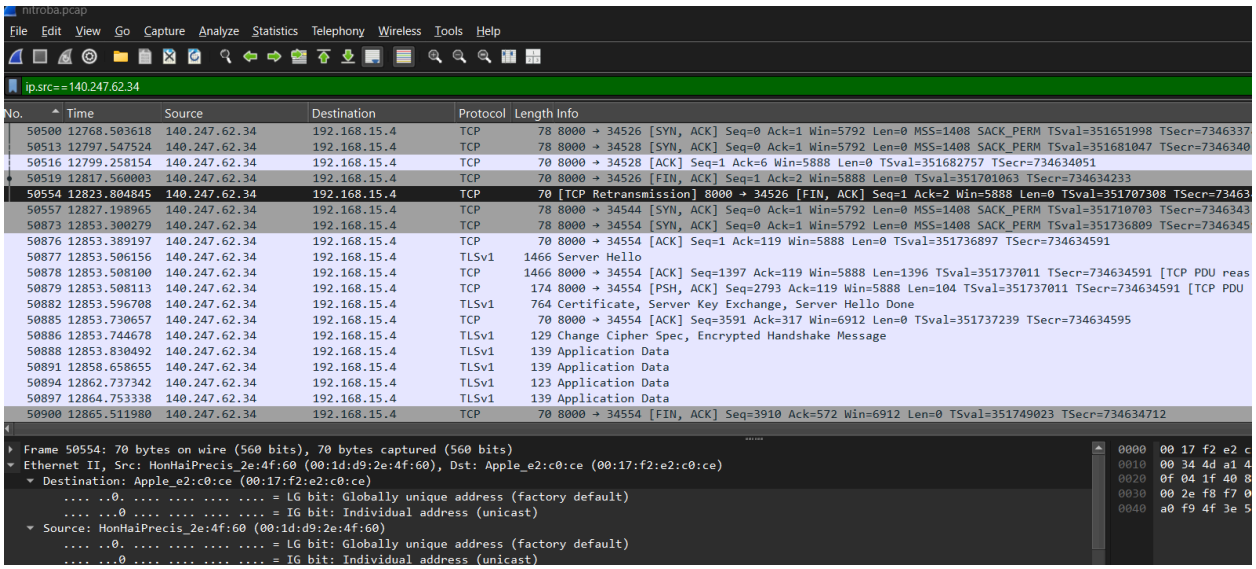
Because several email messages appear to come from the IP address, Nitroba decides to place a network sniffer on the ethernet port. All of the packets are logged. On Monday 7/21 Tuckridge received another harassing email. But this time instead of receiving it directly, the perpetrator sent it through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

2.0 INVESTIGATION SUMMARY

Step 01 : Opening the pcap file in wireshark

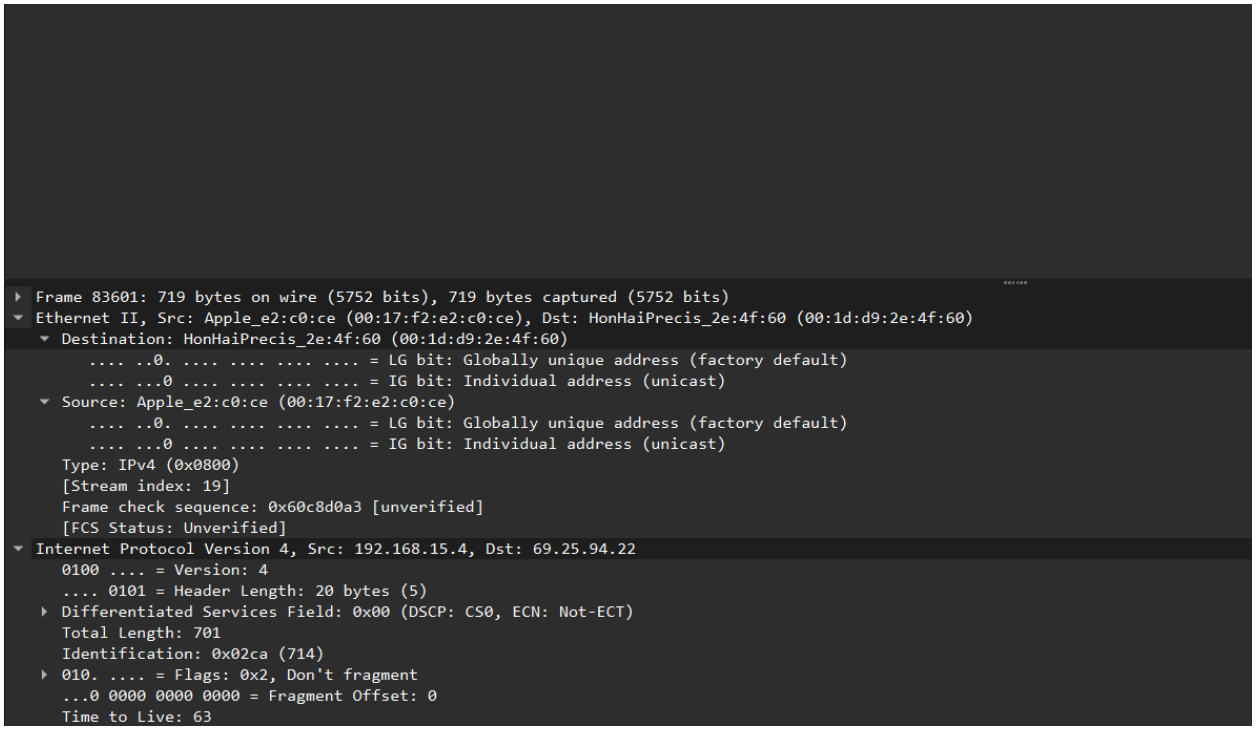


Step 2. Filtering the packets coming from source IP address 140.247.62.34 as the email came from this ip address to tuckridge

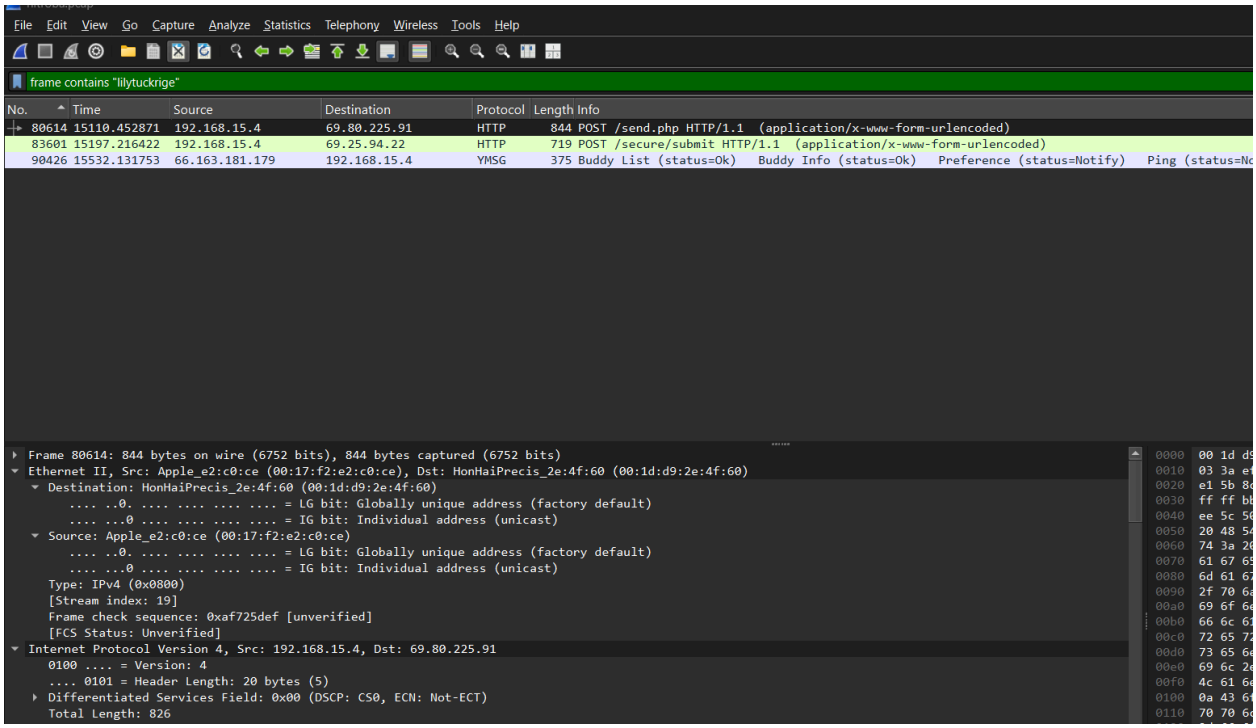


Now we have found the ip address that used to send the email and the destination address.

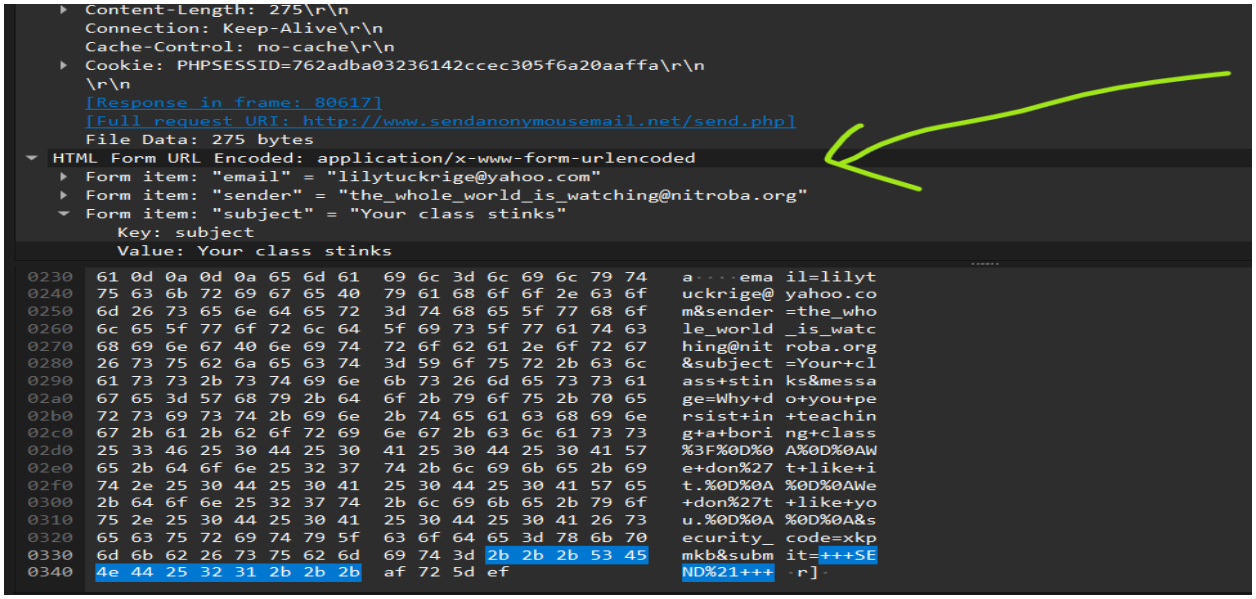
Step 03: Lets check the source and destination mac address , we can see the source used apple device and the mac address is also stated below from the finding

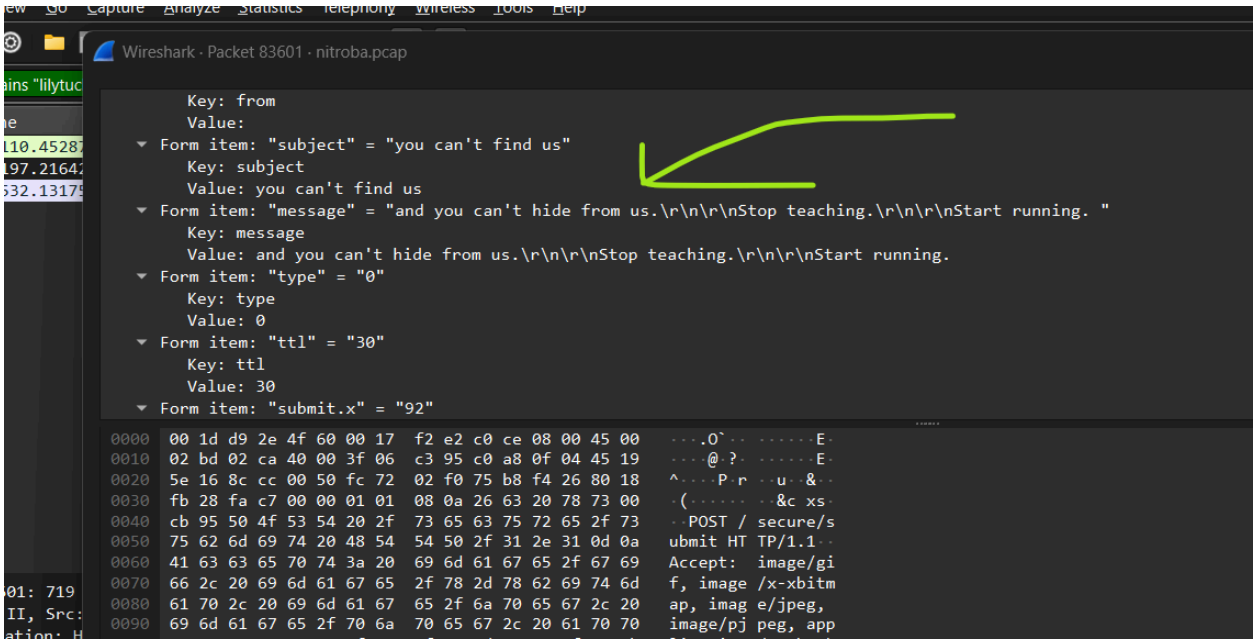


Step 04: Now we will check the email message frames that have mentioned the mail id of the teacher. We will use “liliytuckridge”. And we got the source mail address as **192.168.15.4**

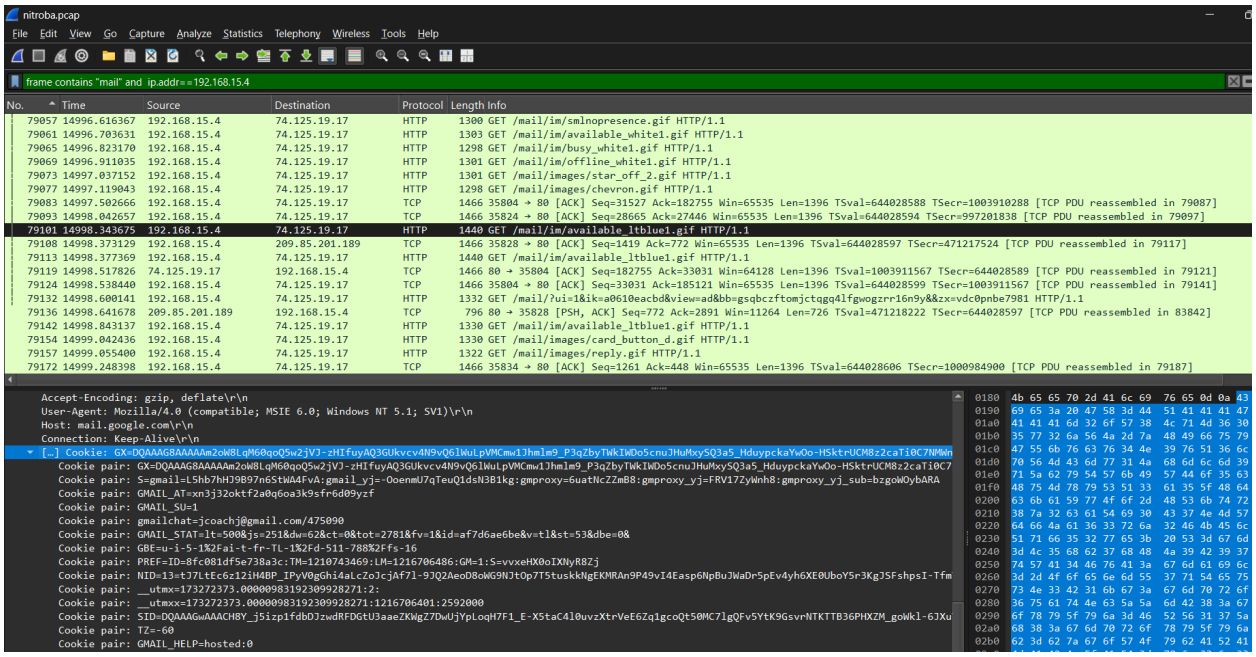


Step 05: Here we can observe the mail packets and find out the packet that has been sent to the teacher by threatening her

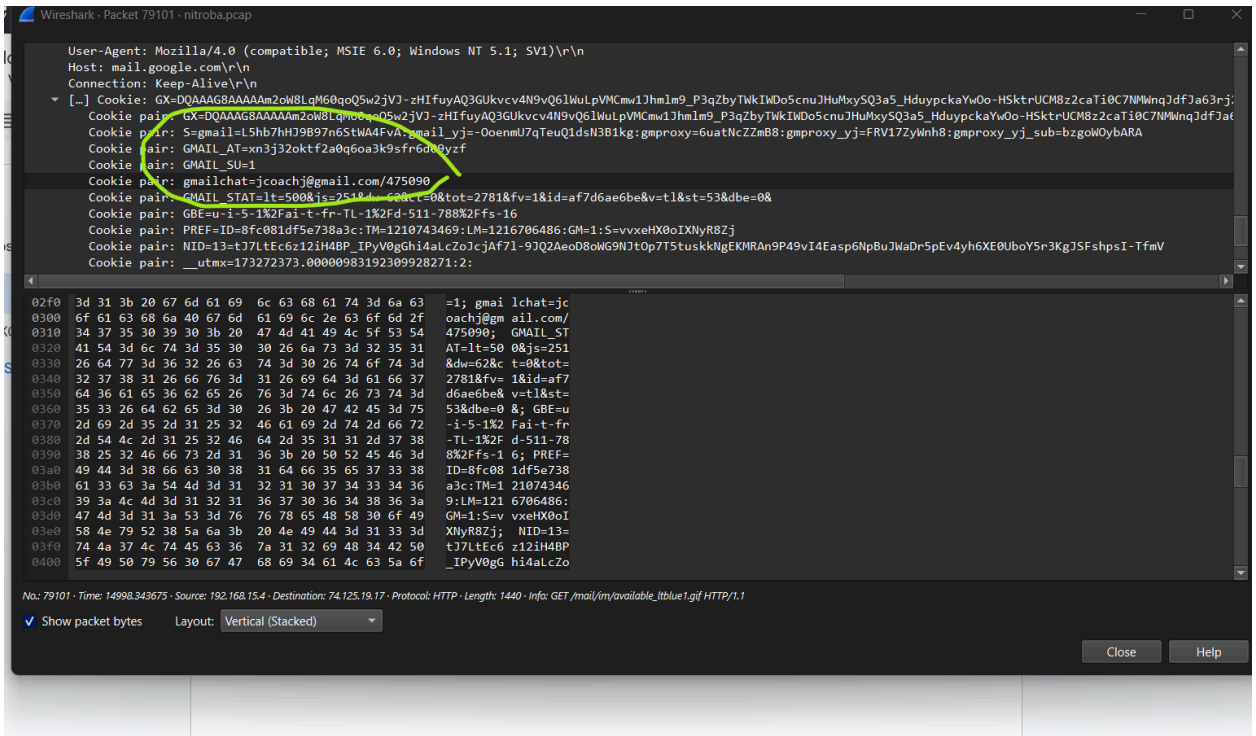




Step 06: Now we will filter out the packet with the suspicious email address as 192. and the packet that contains the “mail “



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.