**Forensic Assignment**

**Group Members:** Sarah Kaunain Syeda (30220873)

                                           Abigail Brown (30214975)

                                         Nina Onwuachi (10190678)

**Forensic Analysis**

1. **Packet search for the string “lily”**

A screenshot of a computer

Description automatically generated

*Figure 1: String search for lily*

*A screenshot of a computer

Description automatically generated*

*Figure 2: TCP Stream for packet 80614*

Filters were applied to display packets with the string “lily”. The packet details pane contained the following information of probative value:

* Source MAC address 00:17:f2:e2:c0:ce, which is associated with Apple.
* Source IP address 192.168.15.4 identified. The IP address is a private IP. *See Appendix E*
* Lily’s personal email can be seen in the HTML packet details.
* A malicious email is observed in the HTTP packet details by the name of the\_whole\_world\_is\_watching@nitroba.org
* Contents of the HTML section corresponds with the harassment emails.
* User-agent used states Mozilla/4.0.

1. **Packet search for students in Lily’s Chemistry class**

Filters were applied for the first names and last names for all the students in Lily’s class. The packet filters displayed results for:

* Amy Smith’s first and last name
* Ava Book’s first and last name
* Johnny Coach’s last name

1. **Packet search for suspected user-agent and IP address**

The investigators began with filtering by the suspected user-agent and IP address of the harasser along with the last names of each of the students who appeared in the network traffic. There were no results for Amy Smith and Ava Book, however, Johnny Coach’s last name produced 94 packets.

A screenshot of a computer

Description automatically generated

*Figure 3: Filter on Amy Smith with suspected harasser’s user-agent and IP*

*A screenshot of a computer

Description automatically generated*

*Figure 4: Filter on Ava Book with suspected harasser’s user-agent and IP*

*A screenshot of a computer

Description automatically generated*

*Figure 5: Filter on Johnny Coach with suspected harasser’s user-agent and IP*

*A screenshot of a computer

Description automatically generated*

*Figure 6: Identification of Johnny's email*

* Analysis of the filtered results revealed the email address “jcoach@gmail.com”

**Conclusion**

The network traffic containing the harassing emails do not specifically name a student in Lily’s class. However, based on analysis of user-agent and IP address, the only student whose name had packet results was Johnny Coach.

It was observed that multiple persons were assigned to the same IP address ( 192.168.15.4 ) as a result only the IP is not reliable to justify one particular person sent the email

It can be assumed that the harasser is Johnny Coach. <edit>

**APPENDIX**

**A. First email to Lily Tuckrige**

A computer screen with a message

Description automatically generated

**B. First email headers**

A computer screen shot of a website

Description automatically generated

**C. Lily Tuckrige Class List**

A white paper with black text

Description automatically generated

**D. Second email to Lily Tuckrige**

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A computer screen shot of a message

Description automatically generated

**E. Google research on suspected IP**

A screenshot of a computer

Description automatically generated