

Student:John Monteiro

Email:jmonteiro48@bristolcc.edu

Time on Task:6 hours, 22 minutes

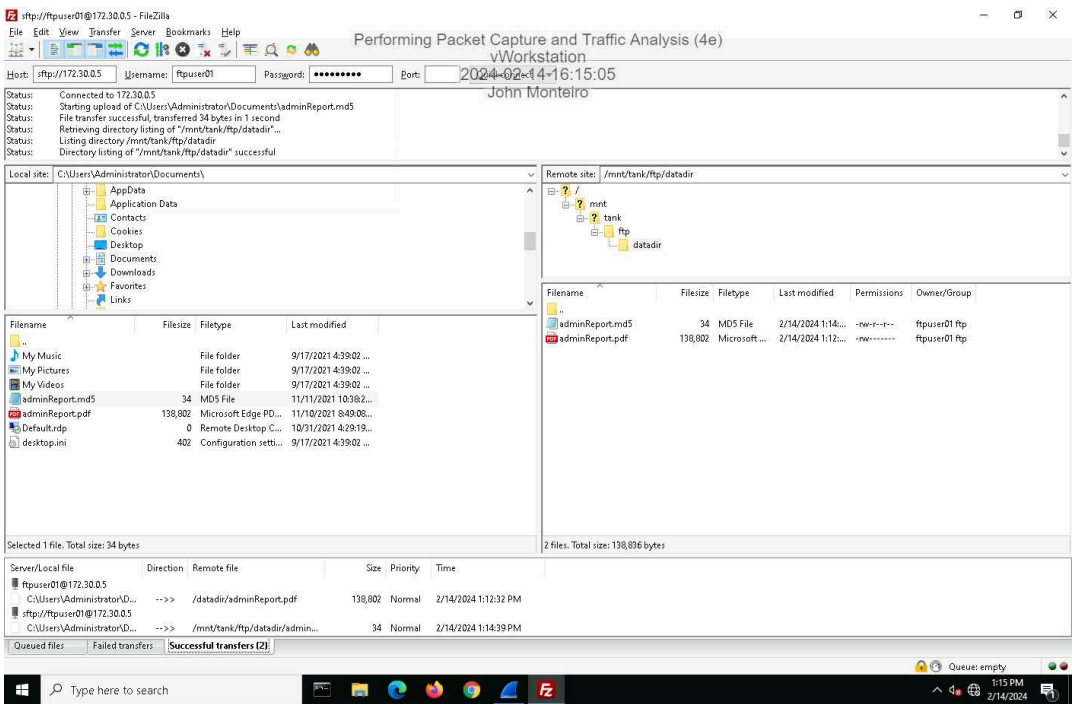
Progress:100%

Report Generated: Thursday, February 15, 2024 at 12:49 PM

Section 1: Hands-On Demonstration

Part 1: Configure Wireshark and Generate Network Traffic

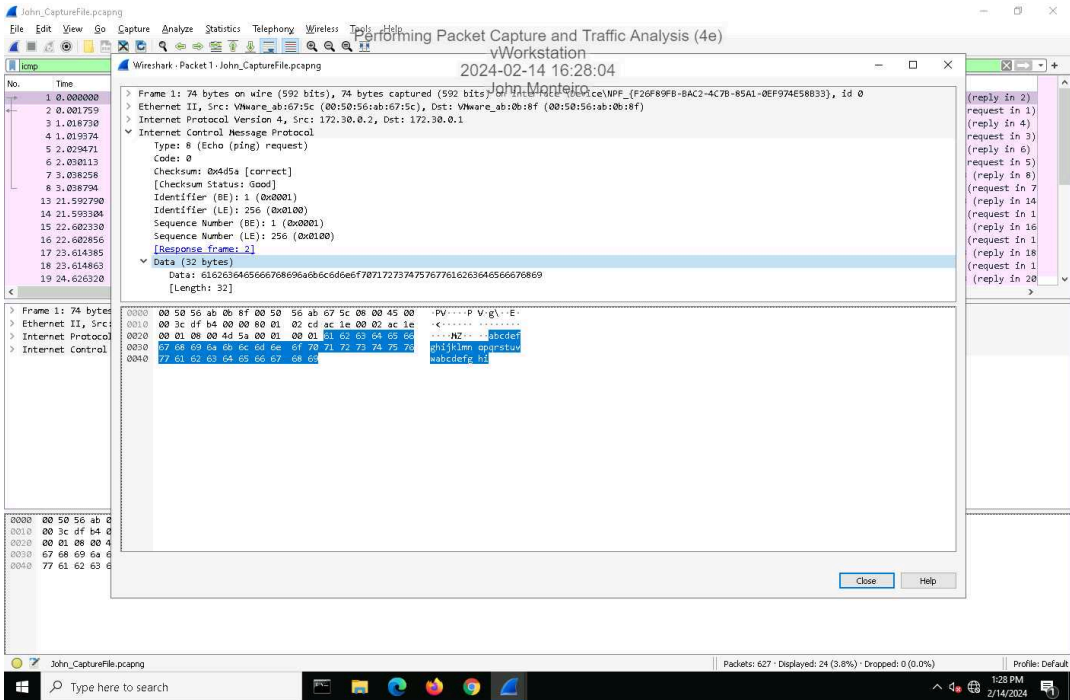
29. Make a screen capture showing the successful FTP and SFTP file transfers.



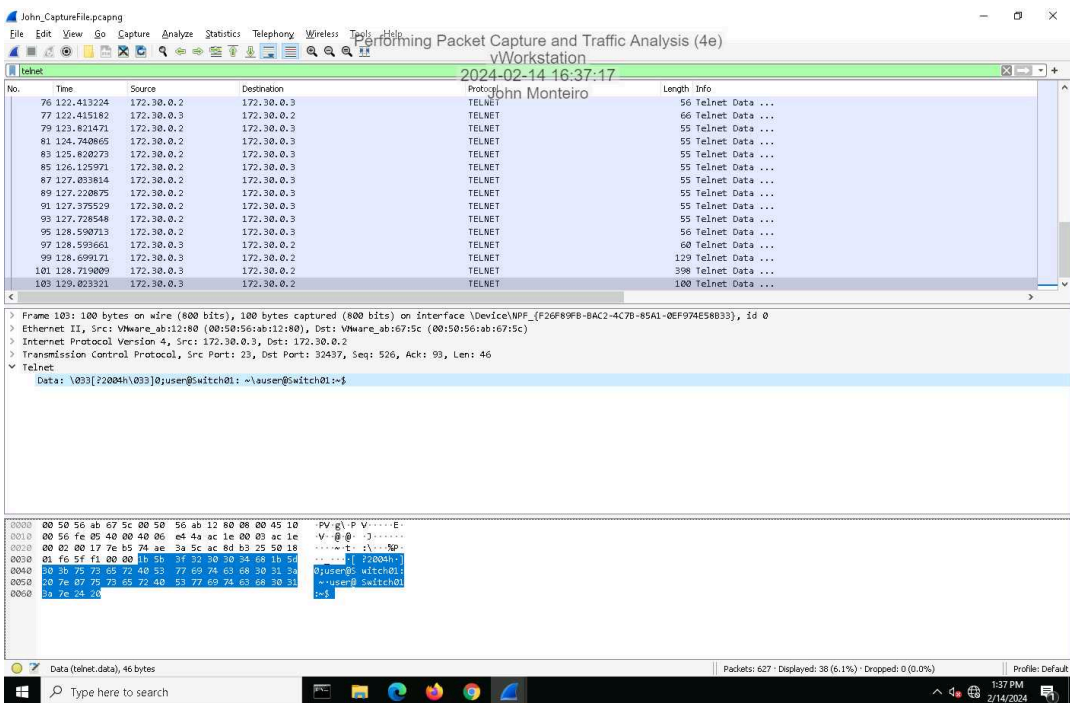
Part 2: Analyze Traffic Using Wireshark

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

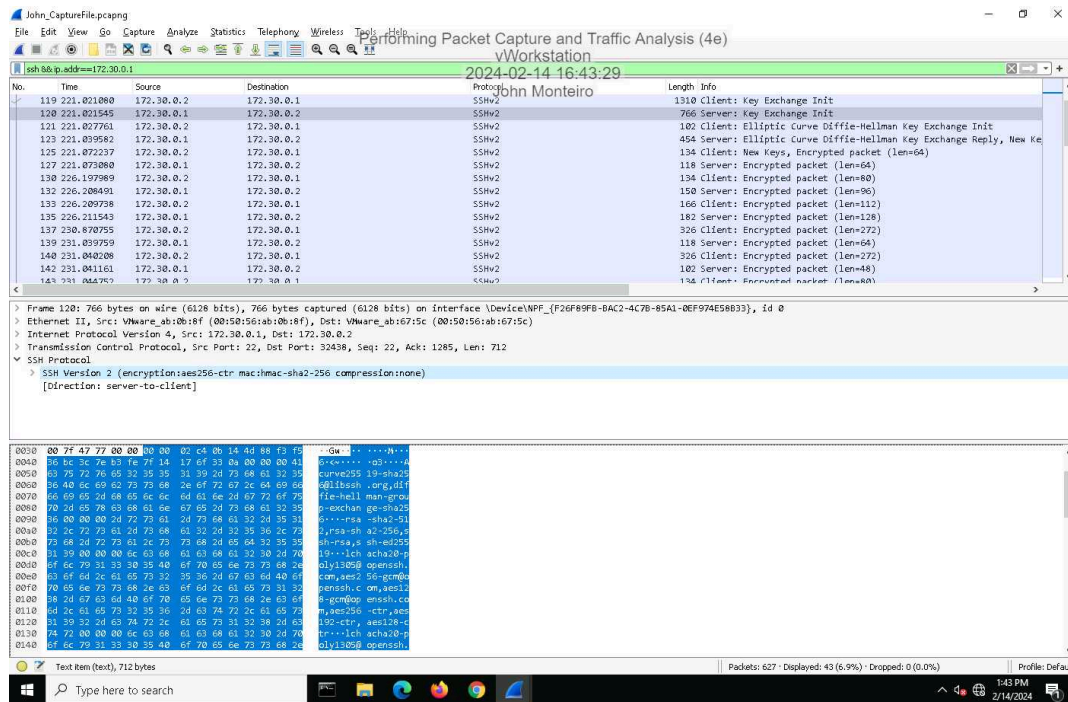
7. **Make a screen capture** showing the **ICMP payload**.



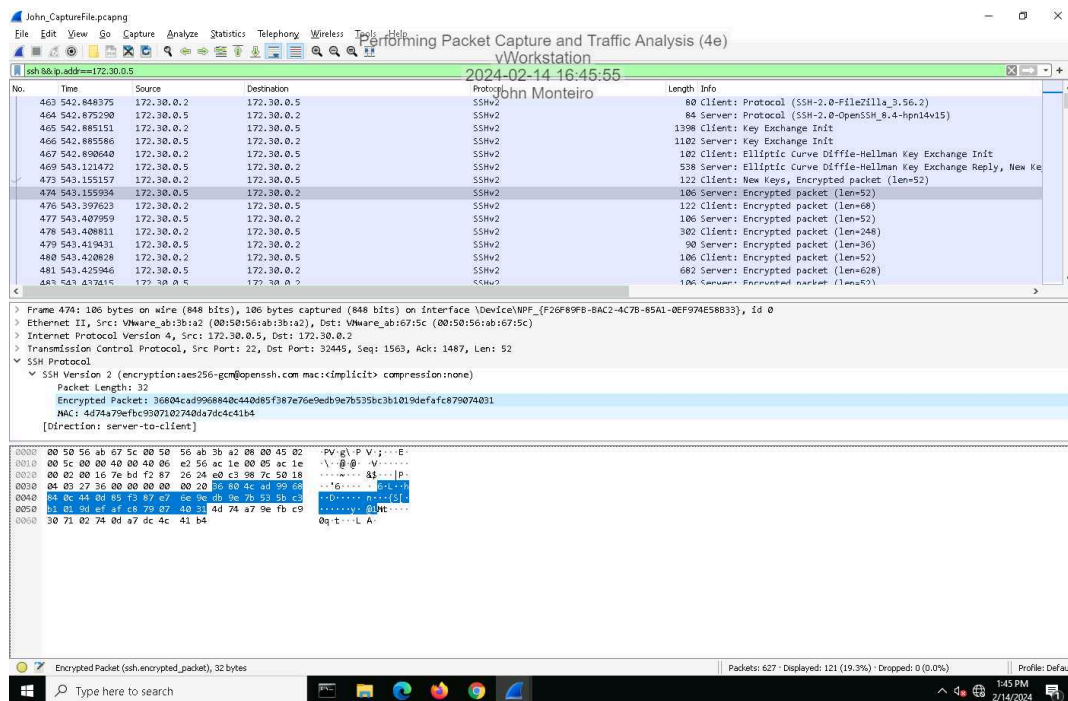
15. **Make a screen capture** showing the *Last Login:* information in the Packet Details pane.



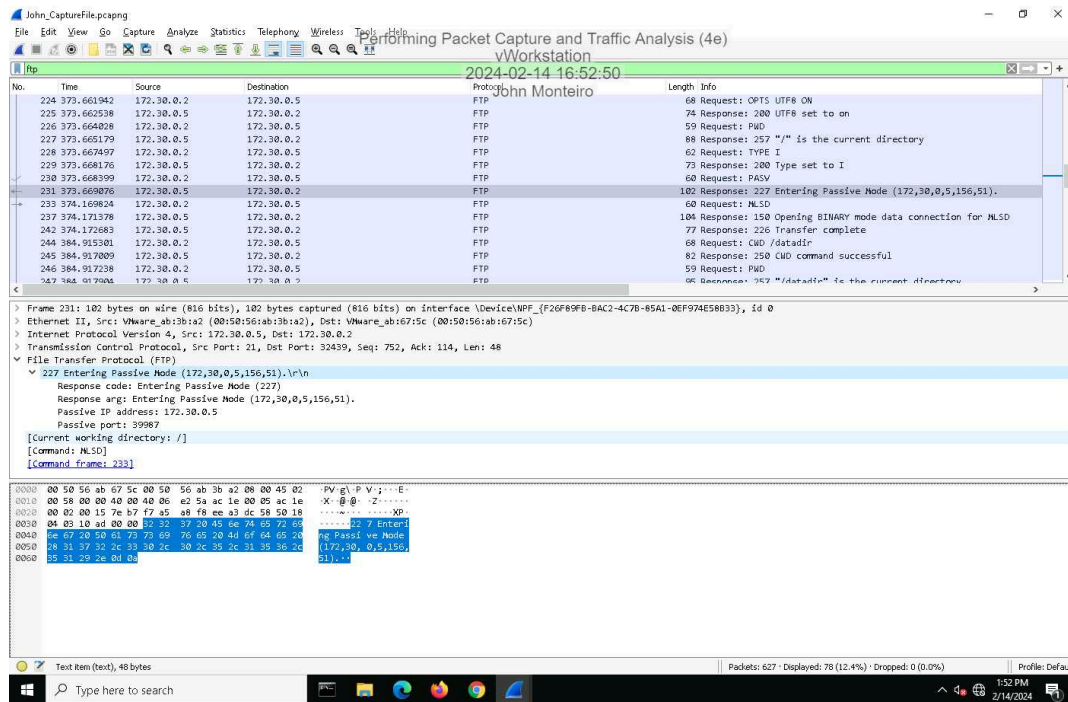
21. Make a screen capture showing the SSHv2 encryption and mac selections for the SSH connection.



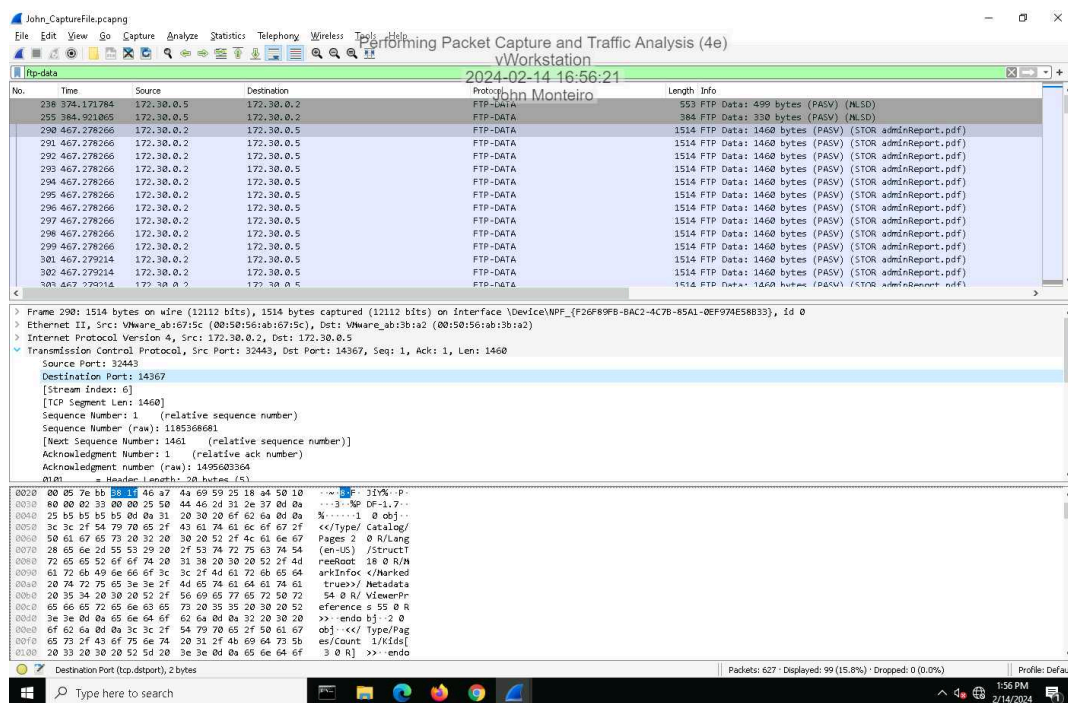
26. Make a screen capture showing the highlighted (encrypted) data in the Packet Bytes pane.



31. Make a screen capture showing the passive port specified by the FTP server in the Packet Details pane.



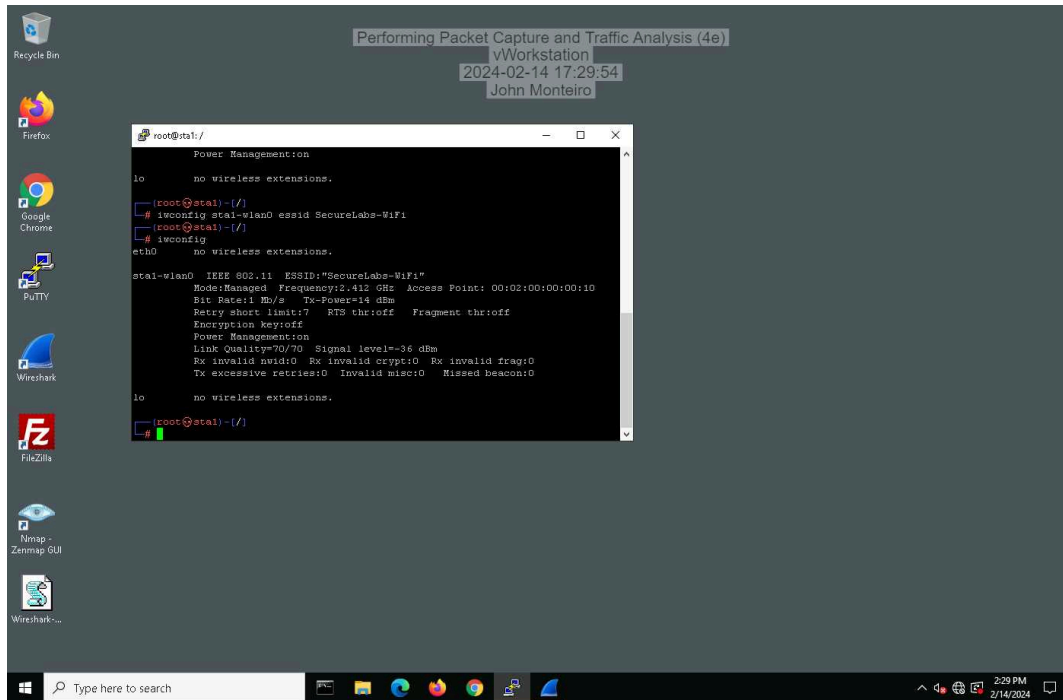
35. Make a screen capture showing the Destination Port field value in the Packet Details pane.



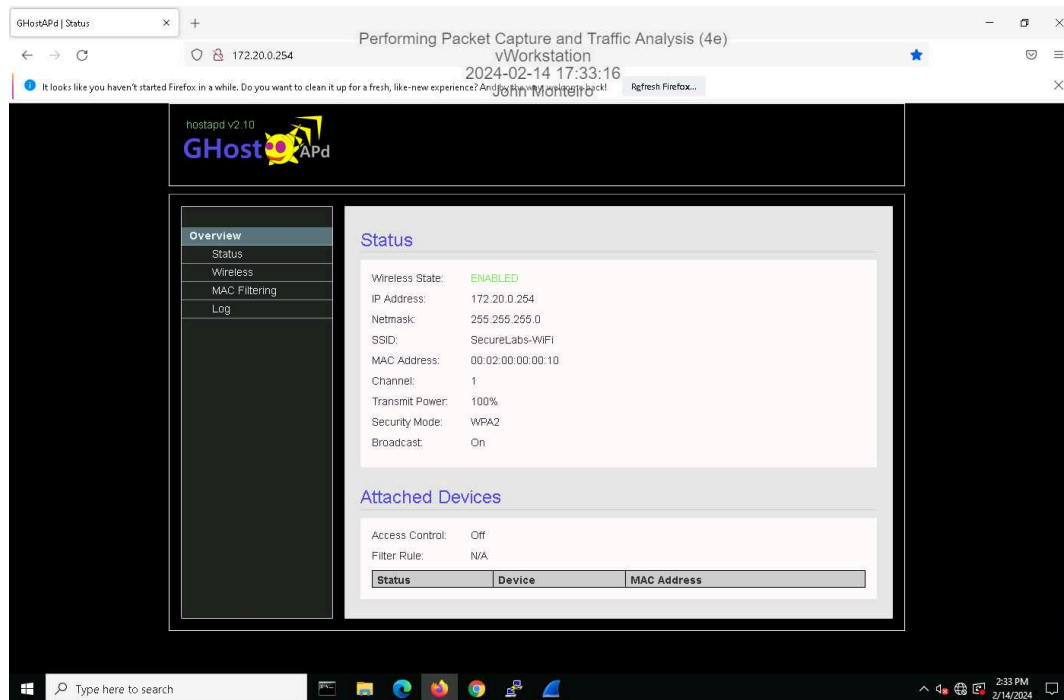
Section 2: Applied Learning

Part 1: Configure Wireshark and Generate Network Traffic

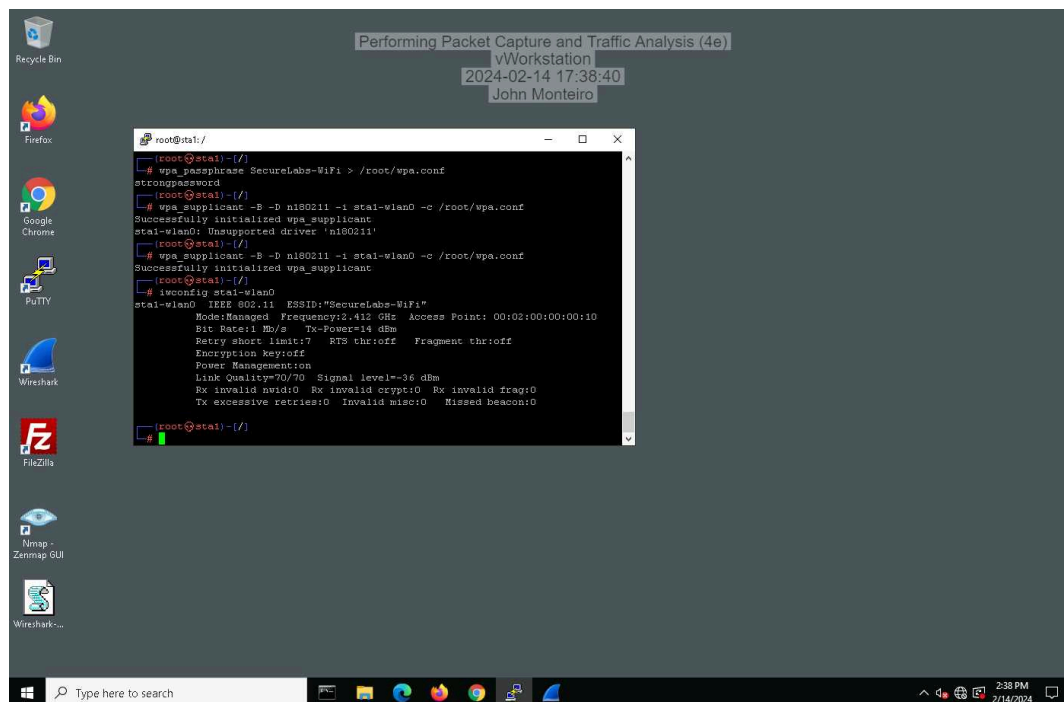
11. Make screen capture showing `sta1-wlan0` connected to the SecureLabs-WiFi network.



18. Make a screen capture showing the updated security mode on the Status page.

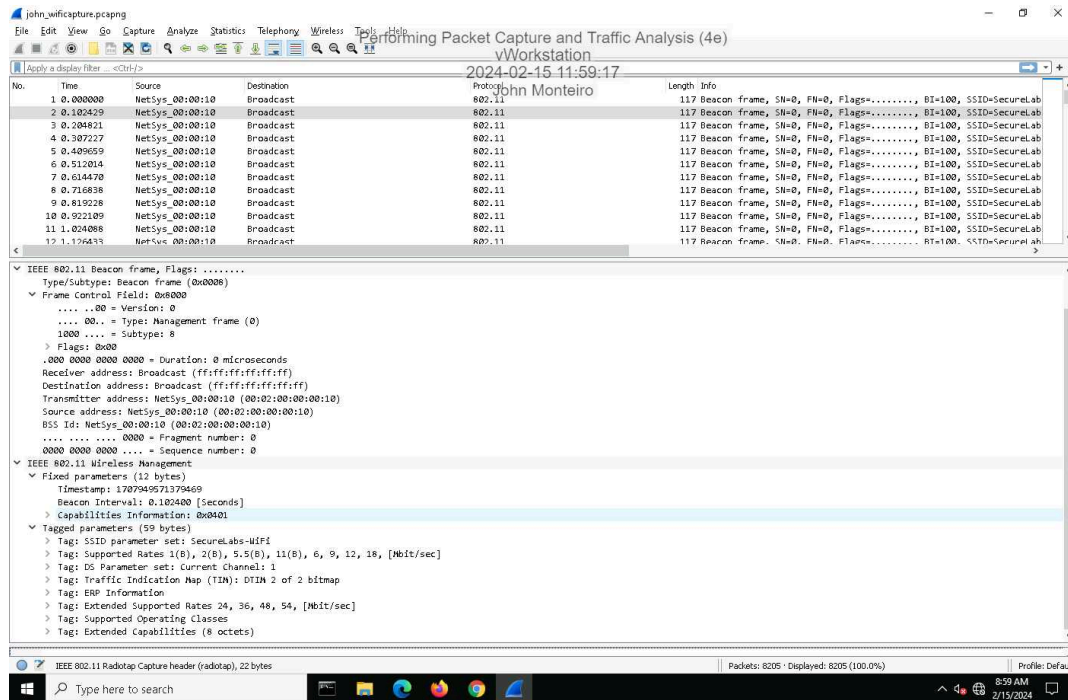


24. Make a screen capture showing the connection to the now-encrypted WLAN.

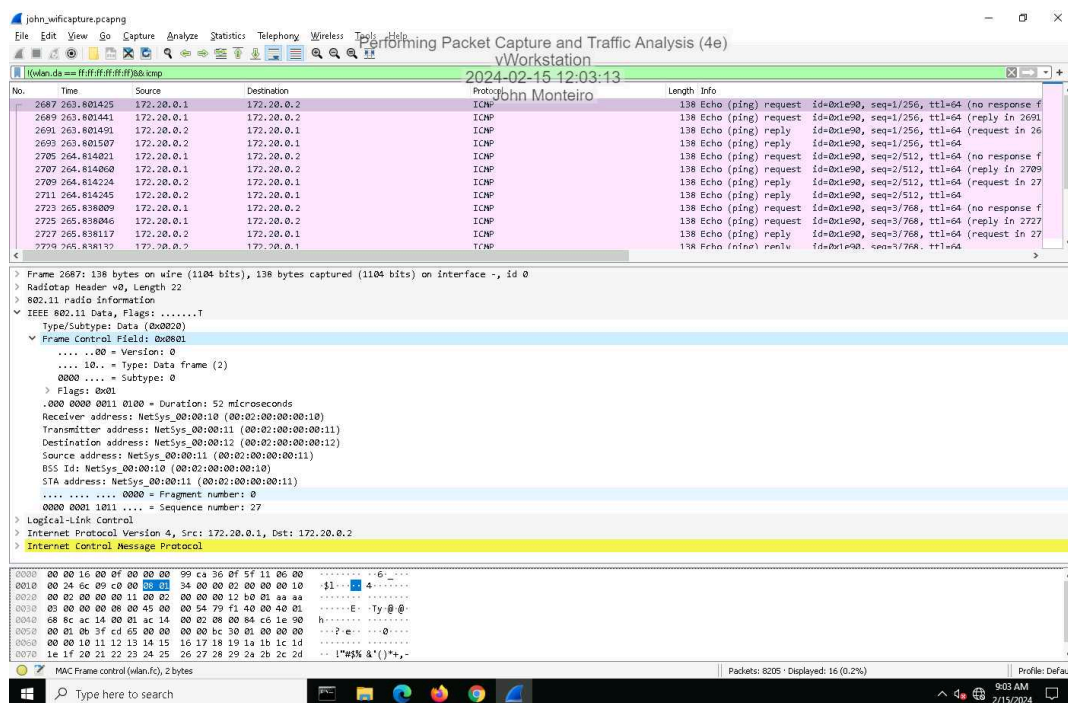


Part 2: Analyze Traffic Using Wireshark

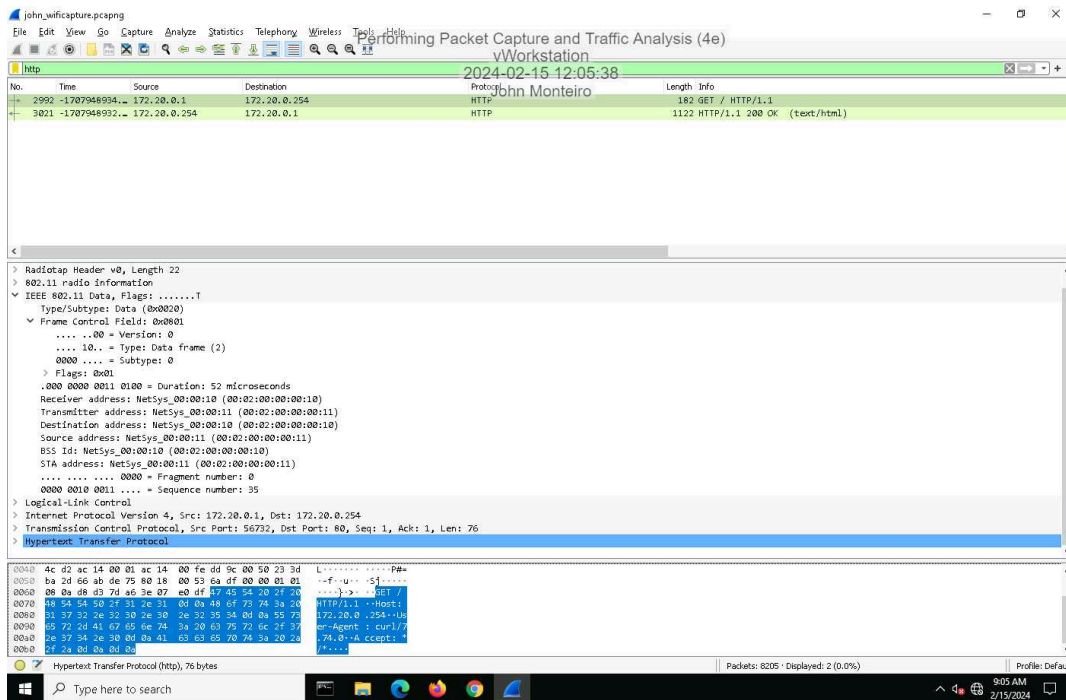
5. Make a screen capture showing the SSID and channel in the Packet Details pane.



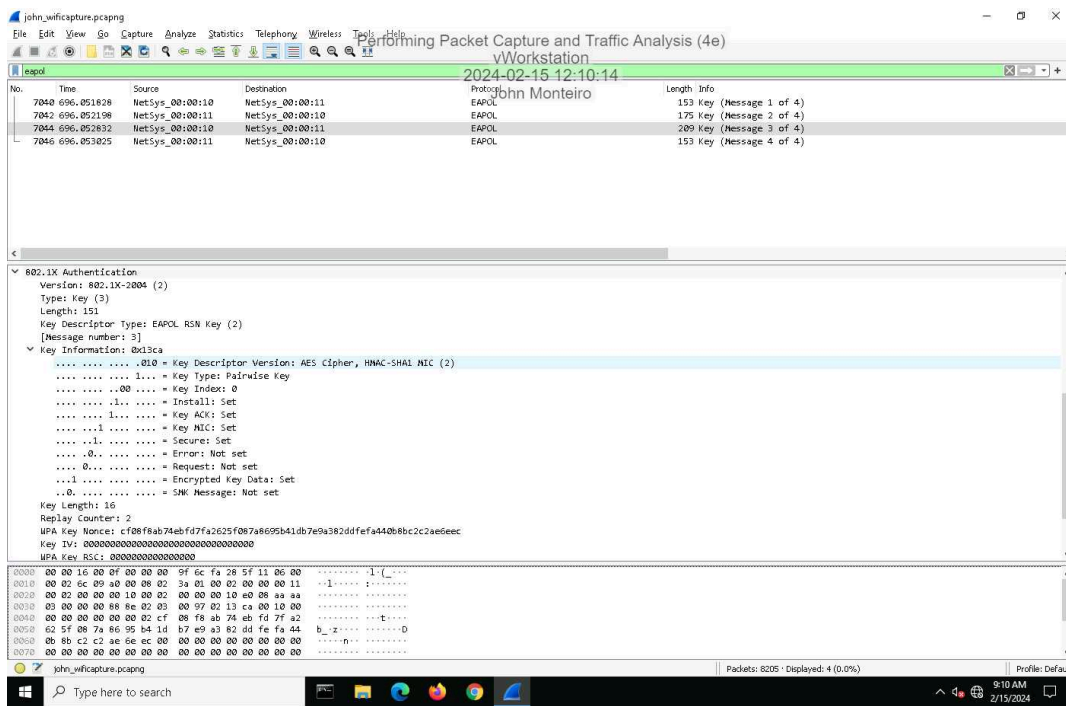
11. Make a screen capture showing the Packet Details for the ICMP packet.



14. Make a screen capture showing the Packet Details for the HTTP packet.



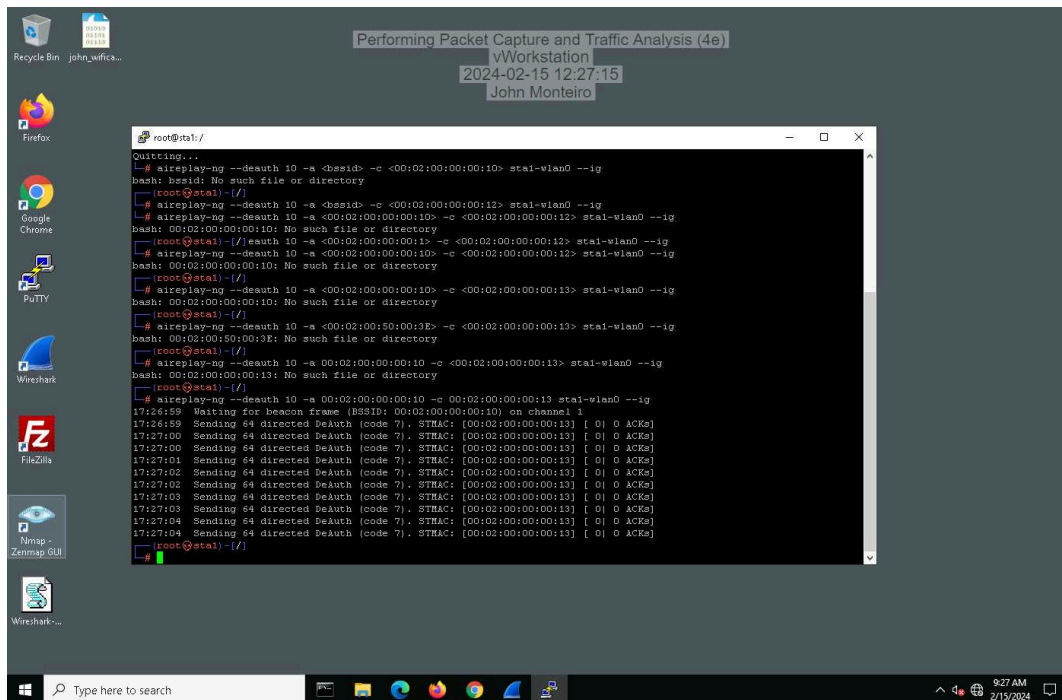
18. Make a screen capture showing the key information for Message 3 in the four-way handshake.



Section 3: Challenge and Analysis

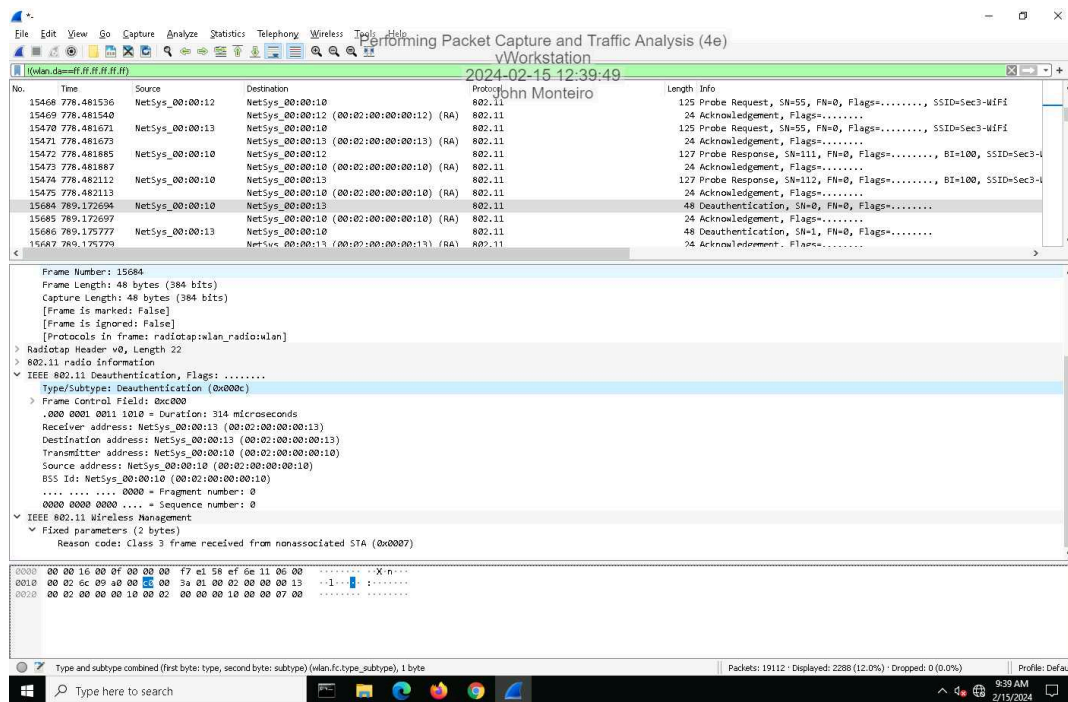
Part 1: Generate Malicious Network Traffic

Make a screen capture showing the `aireplay-ng --deauth` output.



Part 2: Analyze Malicious Network Traffic

Make a screen capture showing one of the deauth packets that you generated between the BSSID and your selected station.



Make a screen capture showing the packets related to the four-way handshake.

