

Student: Kanchan Chopde

Email: hq0656@wayne.edu

Time on Task: 3 hours, 17 minutes

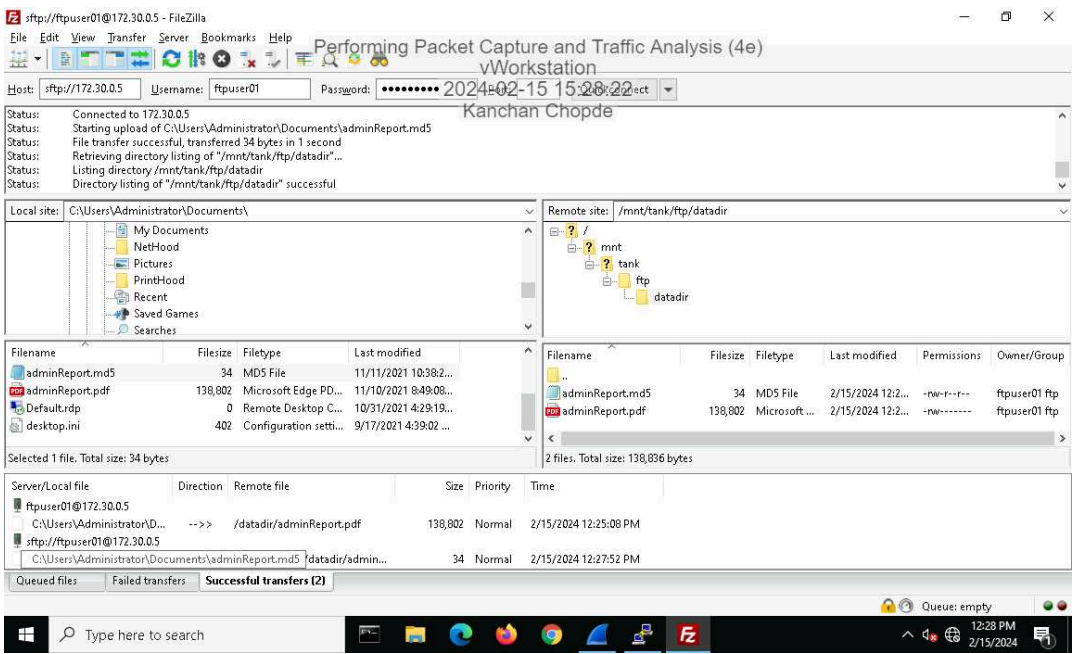
Progress: 100%

Report Generated: Friday, February 16, 2024 at 10:45 PM

Section 1: Hands-On Demonstration

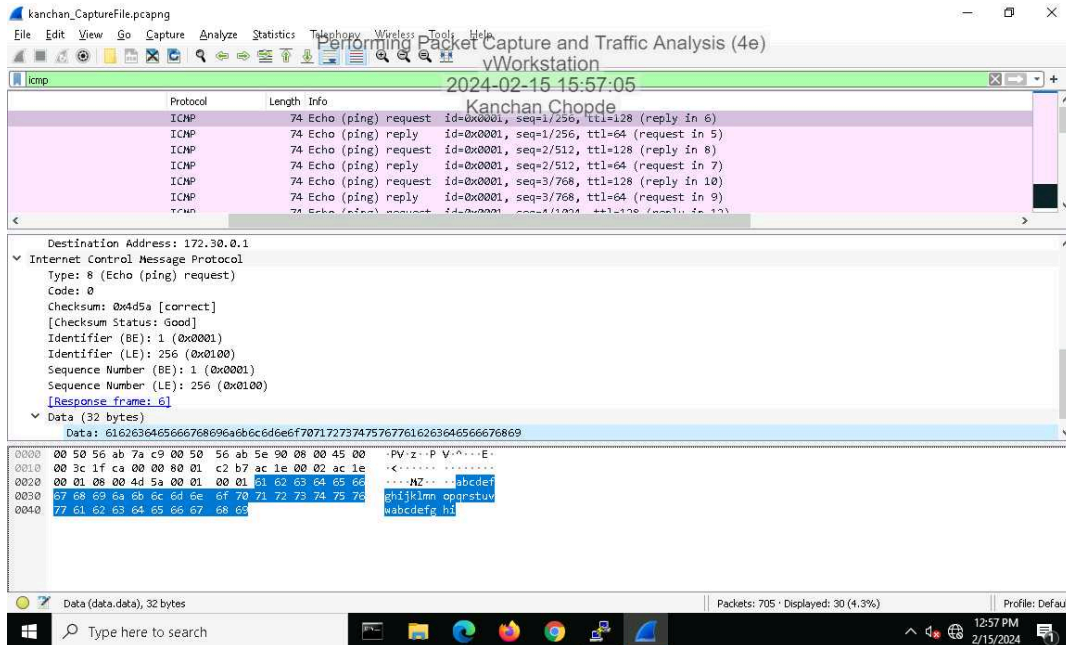
Part 1: Configure Wireshark and Generate Network Traffic

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

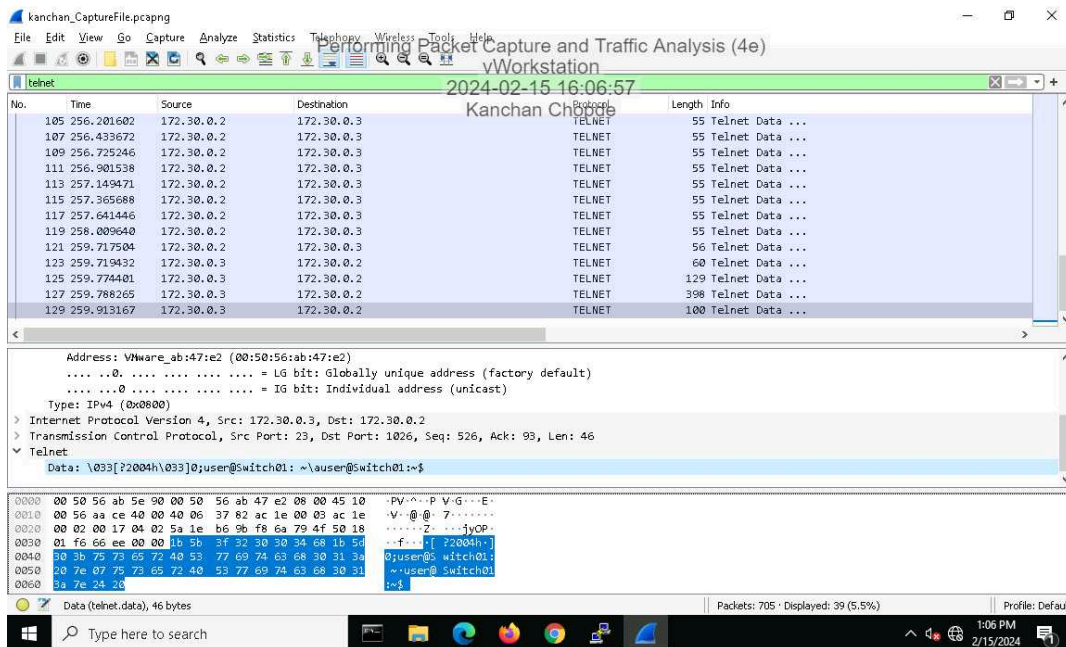


Part 2: Analyze Traffic Using Wireshark

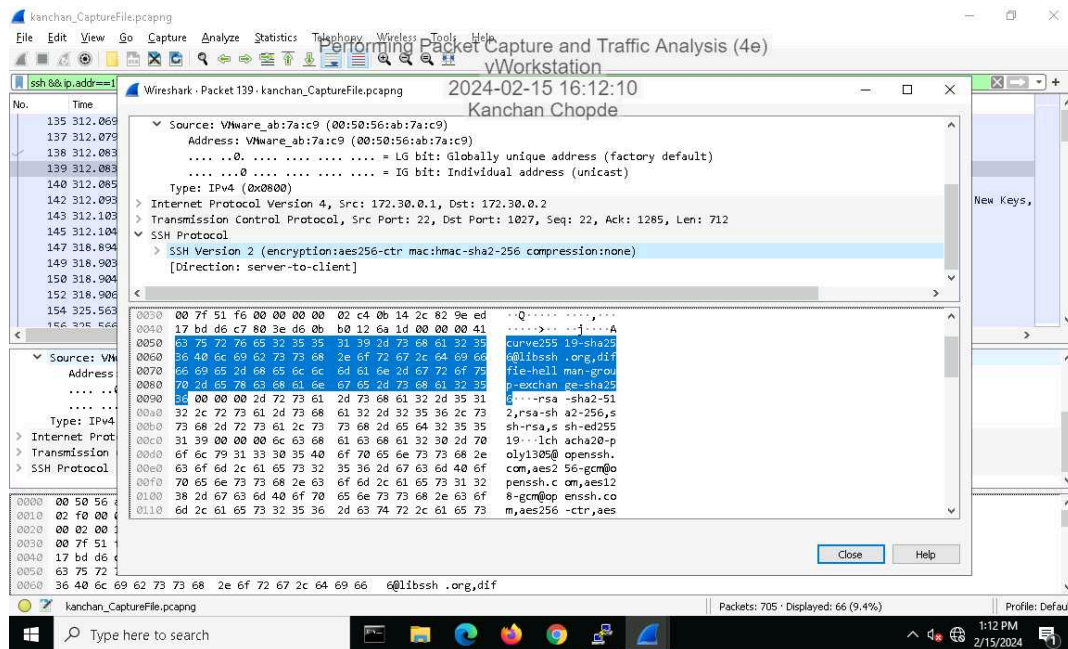
7. Make a screen capture showing the ICMP payload.



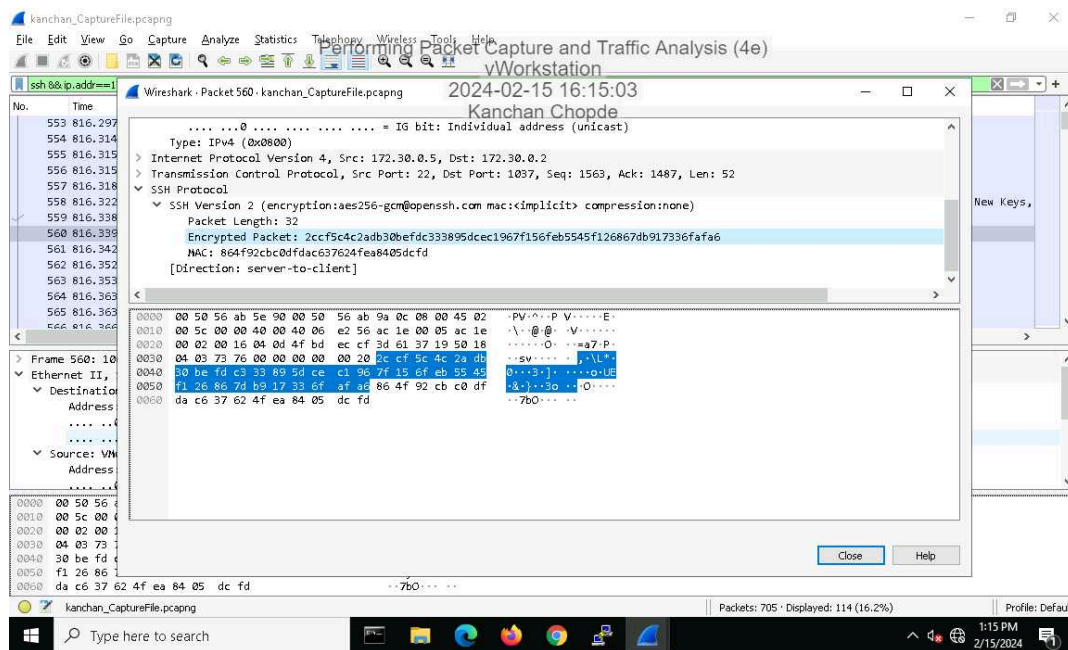
15. Make a screen capture showing the **Last Login** information in the Packet Details pane.



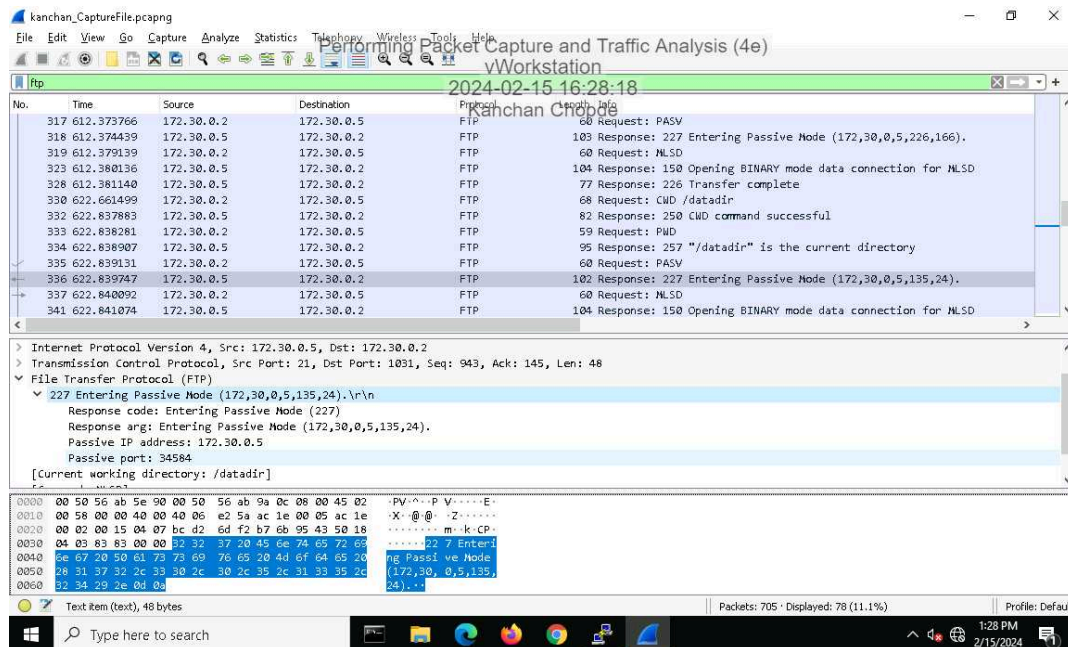
21. Make a screen capture showing the **SSHv2** encryption and mac selections for the SSH connection.



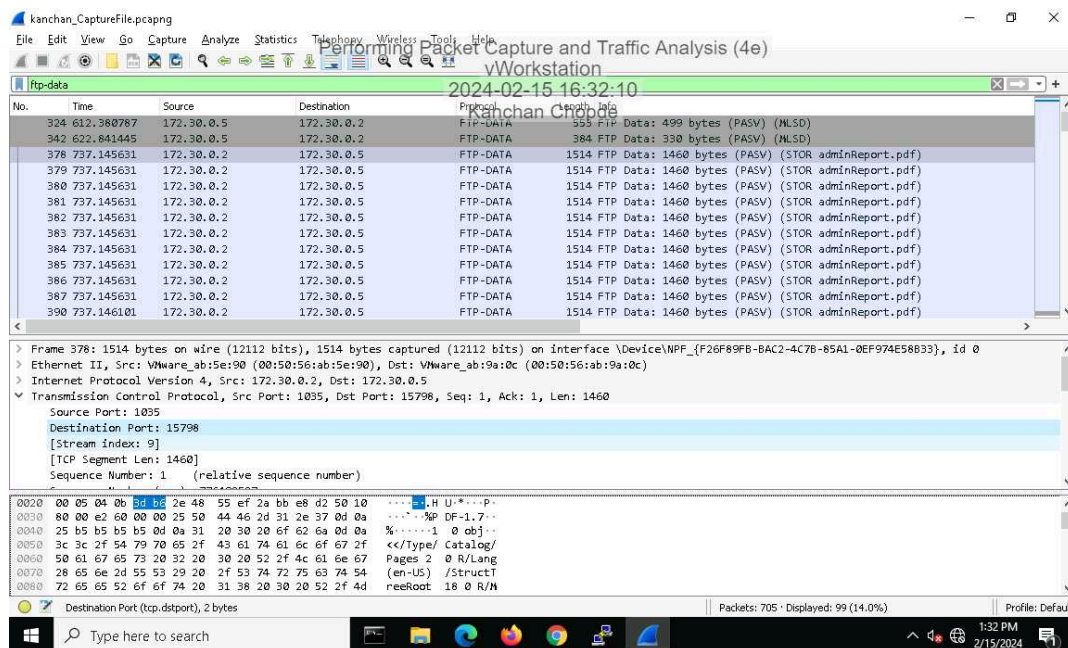
26. Make a screen capture showing the **highlighted (encrypted) data** in the **Packet Bytes** pane.



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



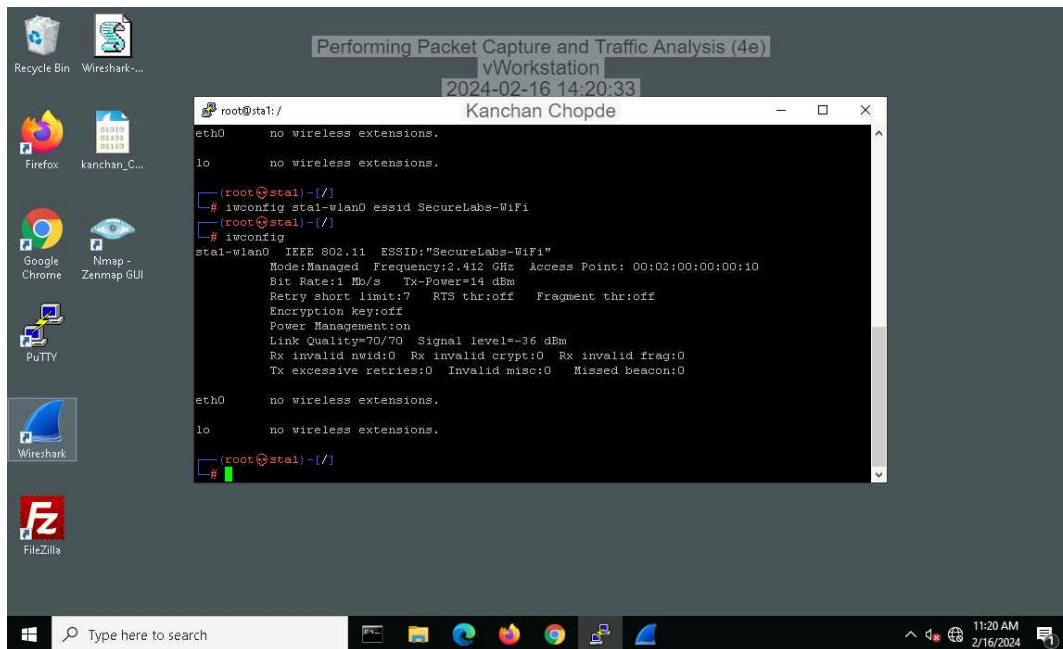
35. Make a screen capture showing the **Destination Port** field value in the **Packet Details** pane.



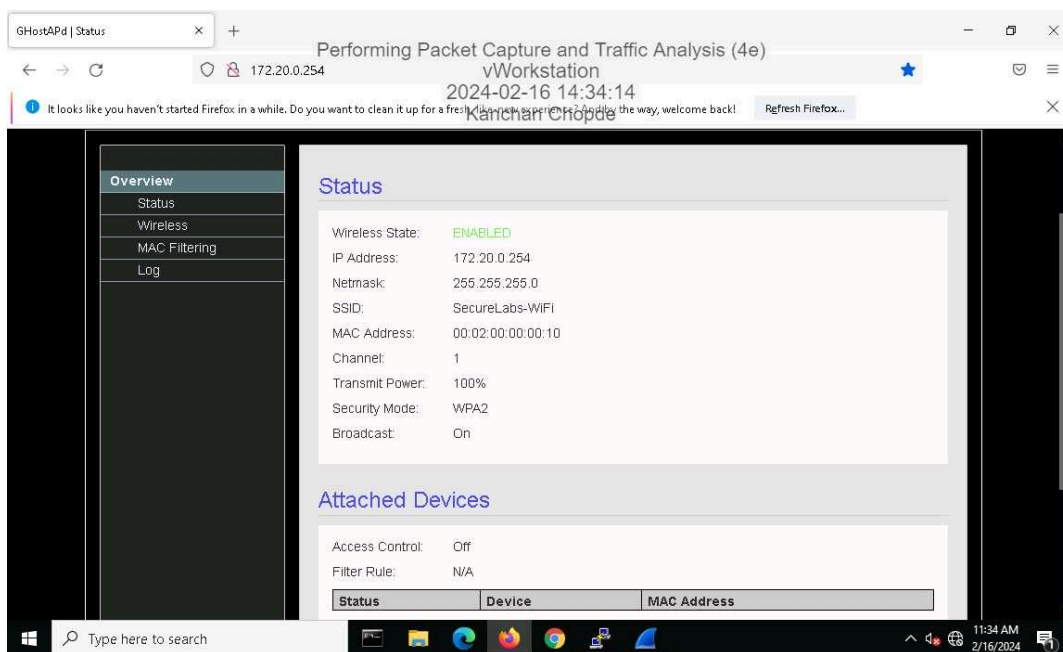
Section 2: Applied Learning

Part 1: Configure Wireshark and Generate Network Traffic

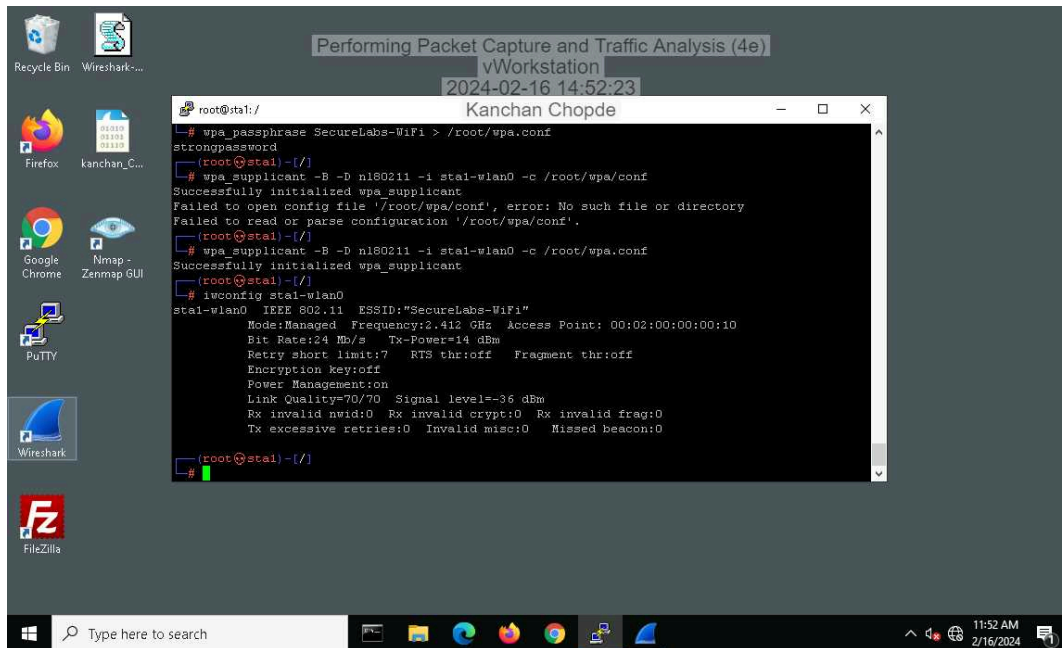
11. Make screen capture showing sta1-wlan0 connected to the SecureLabs-WiFi network.



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

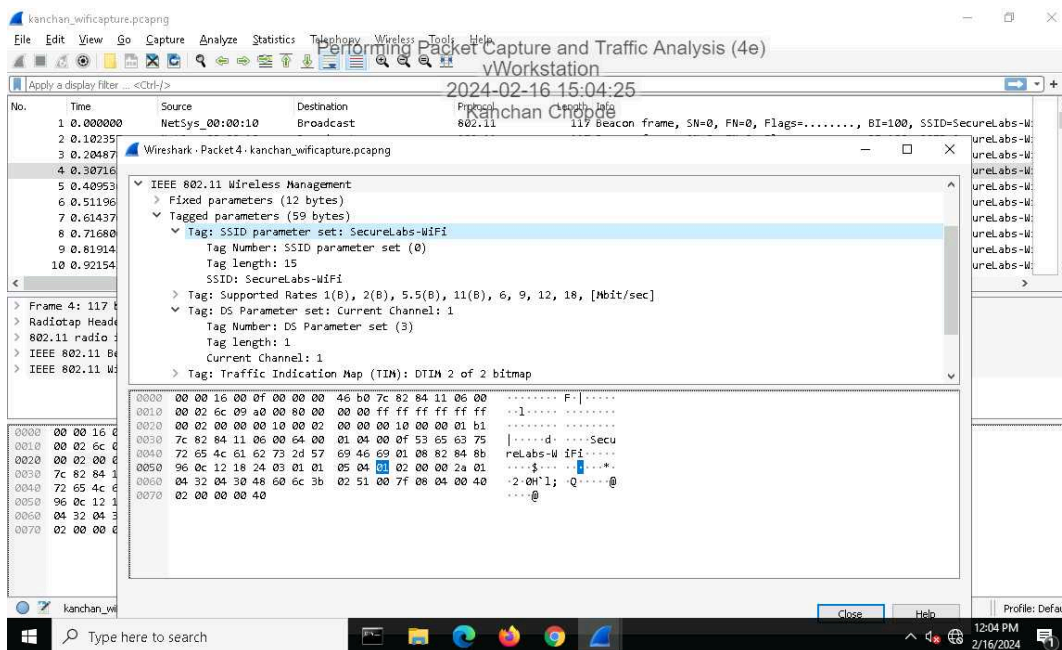


24. Make a screen capture showing the connection to the now-encrypted WLAN.



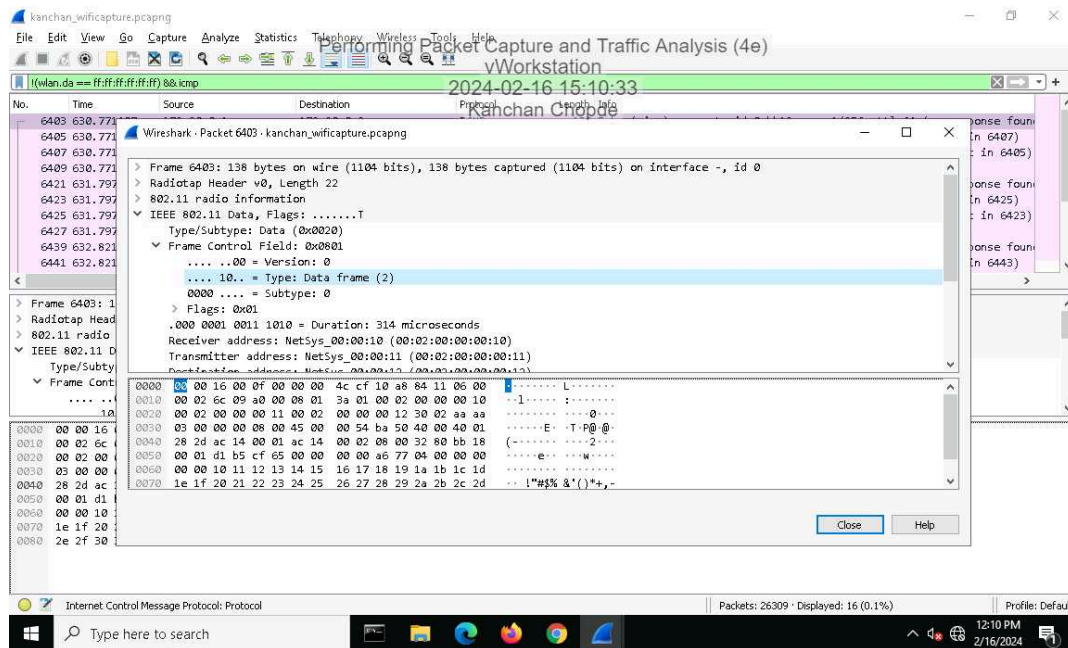
Part 2: Analyze Traffic Using Wireshark

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

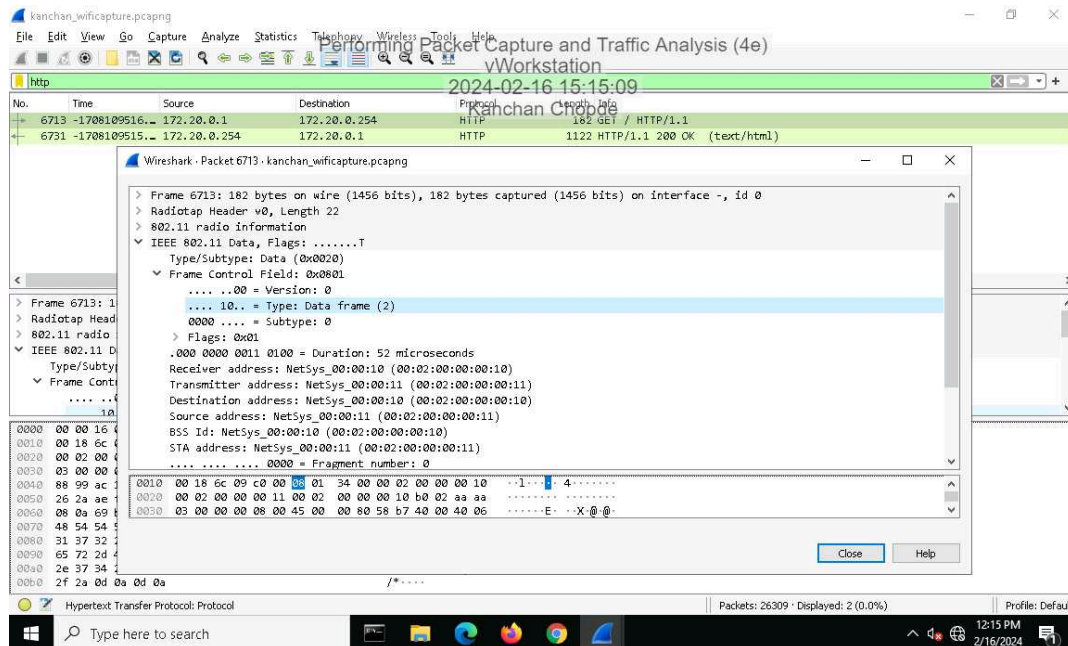


Fundamentals of Information Systems Security, Fourth Edition - Lab 03

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

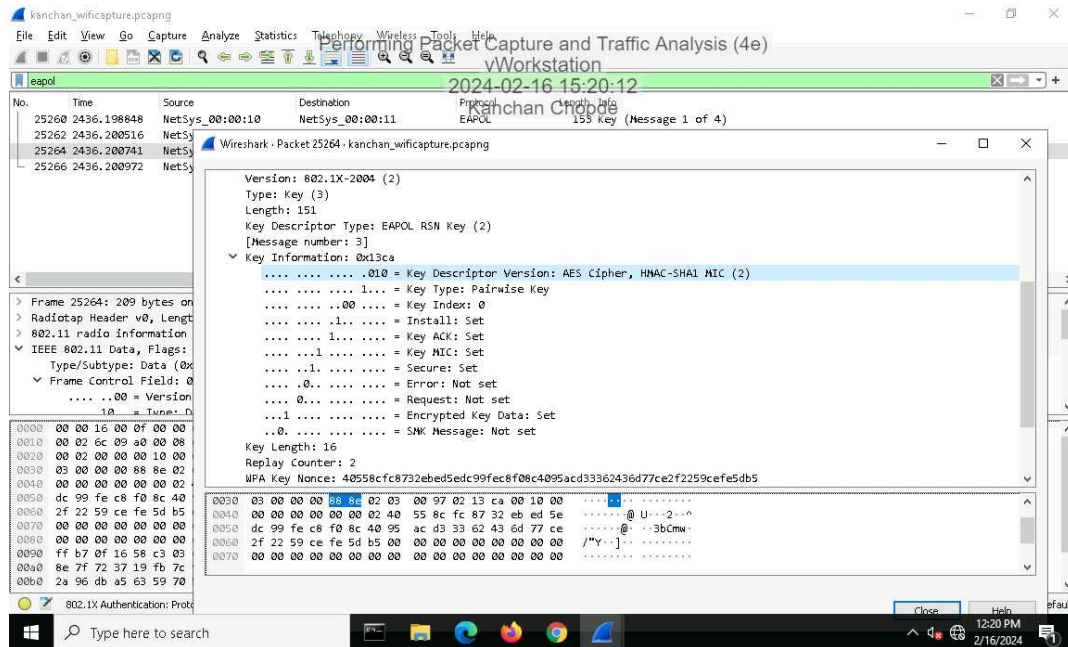


14. **Make a screen capture** showing the **Packet Details** for the **HTTP** packet.



Fundamentals of Information Systems Security, Fourth Edition - Lab 03

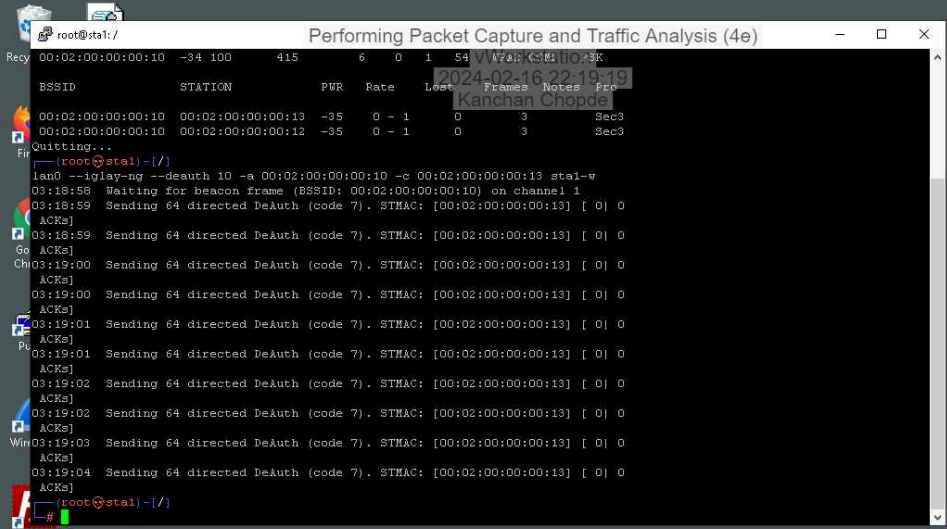
18. **Make a screen capture** showing the **key information for Message 3** in the four-way handshake.



Section 3: Challenge and Analysis

Part 1: Generate Malicious Network Traffic

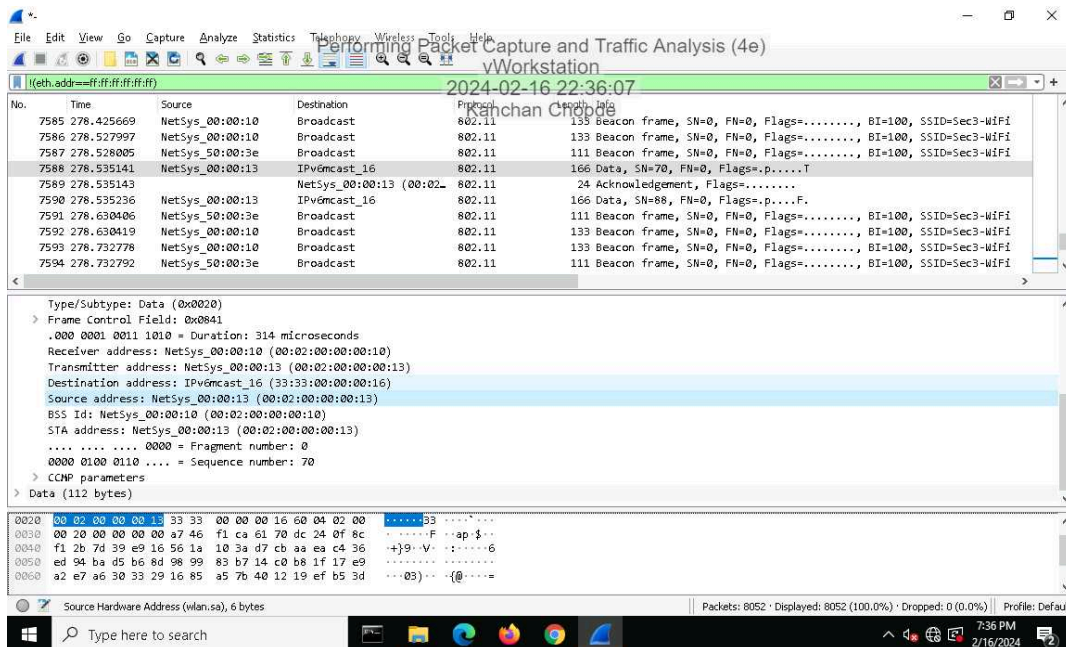
Make a screen capture showing the `aireplay-ng --deauth` output.



```
Recy 00:02:00:00:00:10 -34 100 415 6 0 1 54 V Wlan: CMI 10:3K
BSSID STATION PWR Rate Lost Frames Notes Pri
00:02:00:00:00:10 00:02:00:00:00:13 -35 0 - 1 0 3 Sec3
00:02:00:00:00:10 00:02:00:00:00:12 -35 0 - 1 0 3 Sec3
Quitting...
Fr (root@stali)-[/]
lan0 --igmp --deauth 10 -a 00:02:00:00:00:10 -c 00:02:00:00:00:13 stali-w
03:18:58 Waiting for beacon frame (BSSID: 00:02:00:00:00:10) on channel 1
03:18:59 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
03:18:59 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
03:19:00 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
03:19:00 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
03:19:01 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
03:19:01 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
03:19:02 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
03:19:02 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
Win03:19:03 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
03:19:04 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:13] [ 0] 0
ACKs]
Fr (root@stali)-[/]
```

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.

