

Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

Student:

Jose Cruz

Email:

jose.cruz2@udc.edu

Time on Task:

7 hours, 51 minutes

Progress:

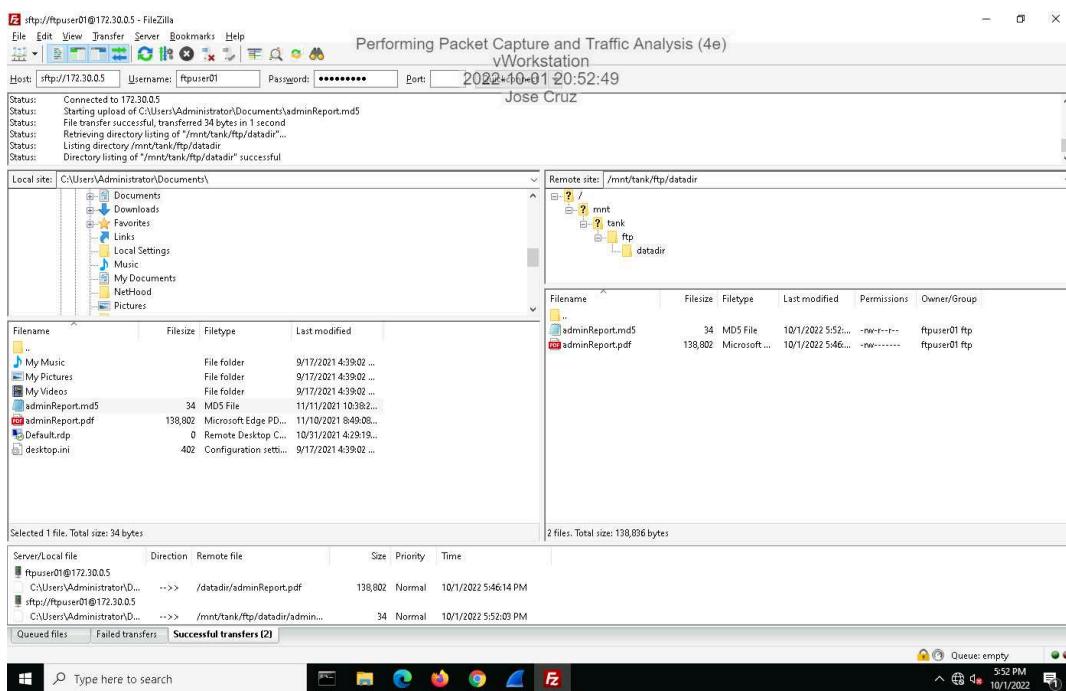
100%

Report Generated: Saturday, October 22, 2022 at 11:17 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.

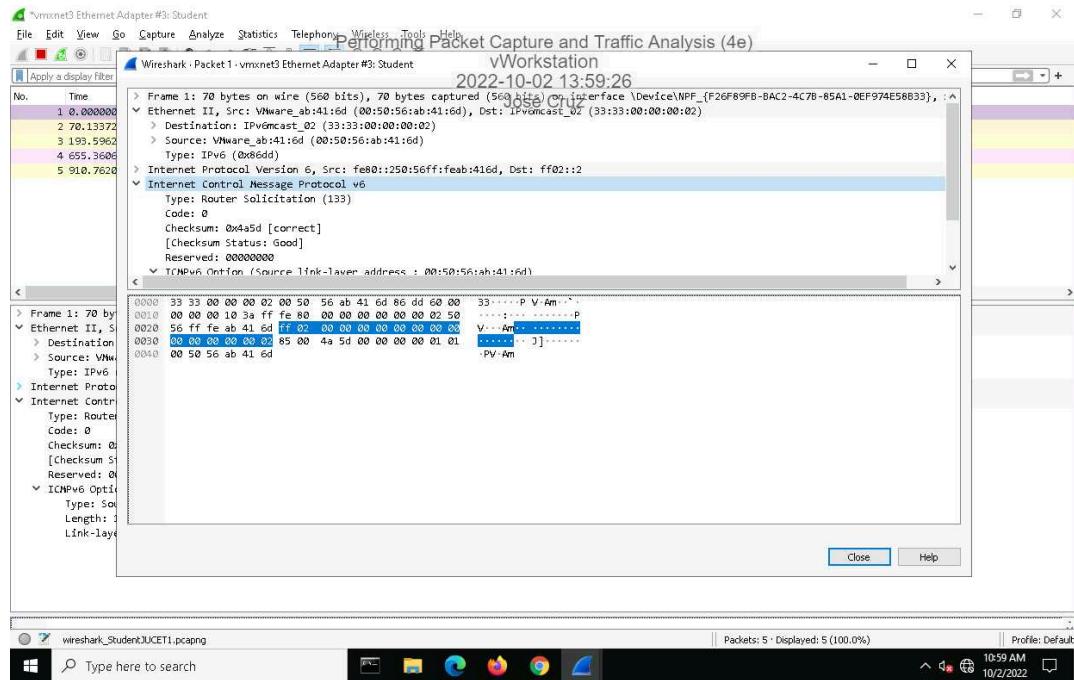


Part 2: Analyze Traffic Using Wireshark

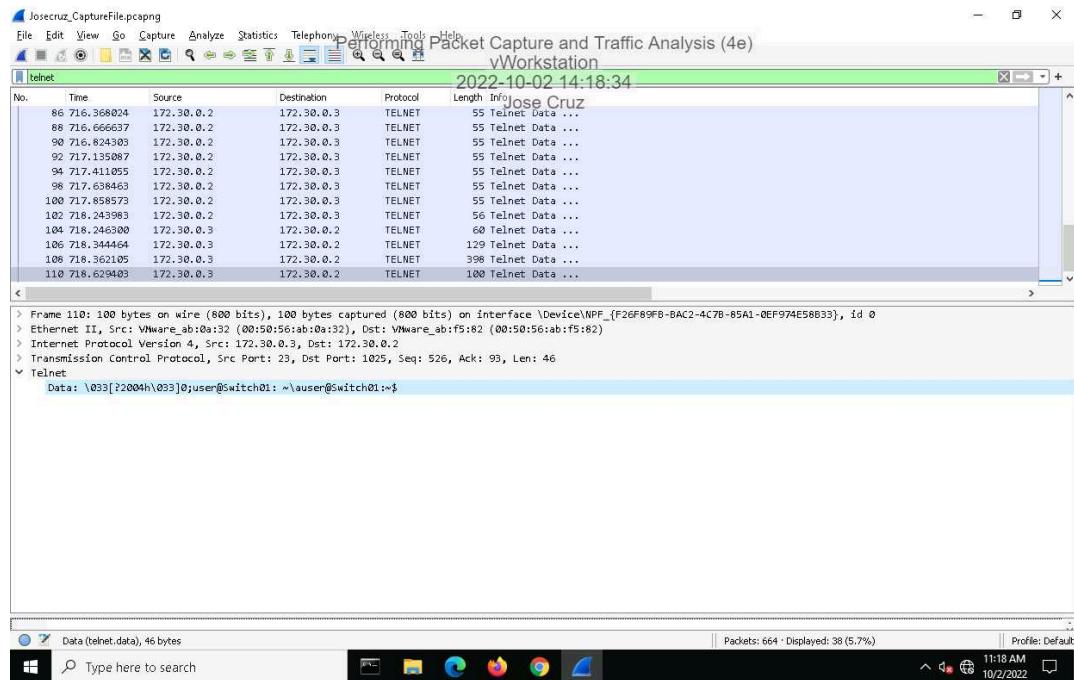
Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

7. Make a screen capture showing the ICMP payload.



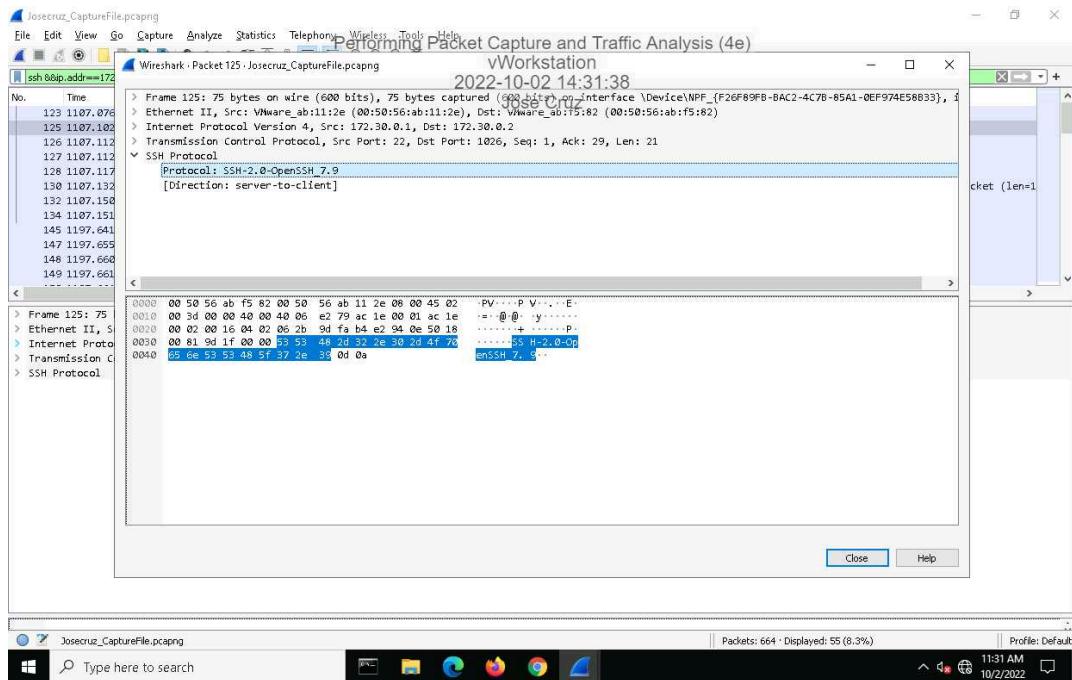
15. Make a screen capture showing the *Last Login:* information in the Packet Details pane.



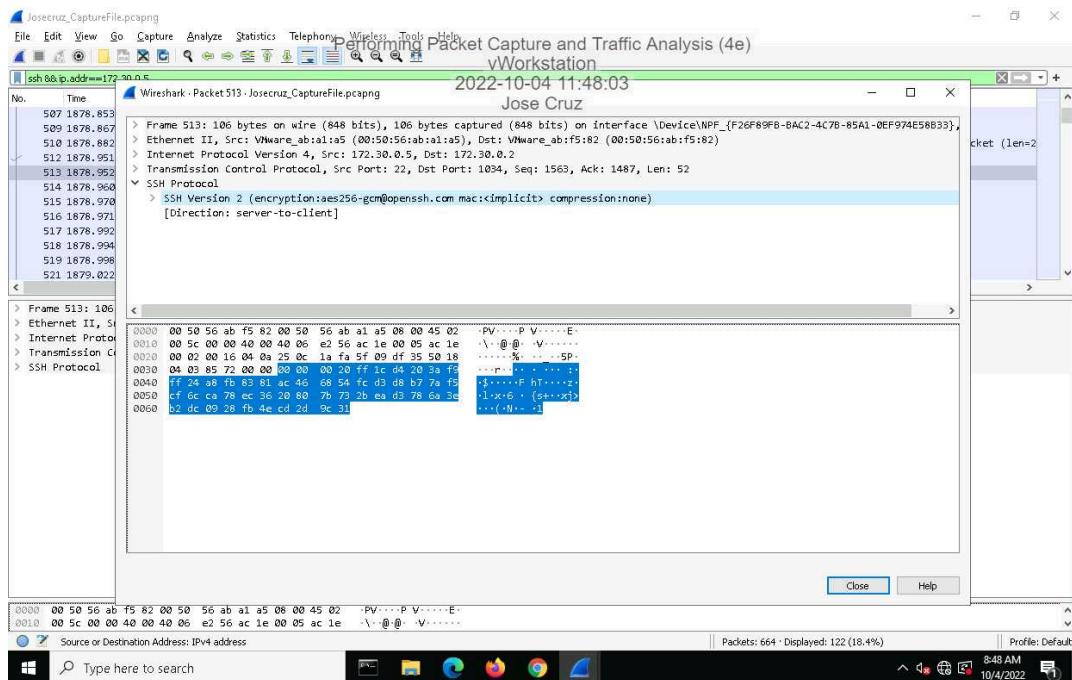
Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

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



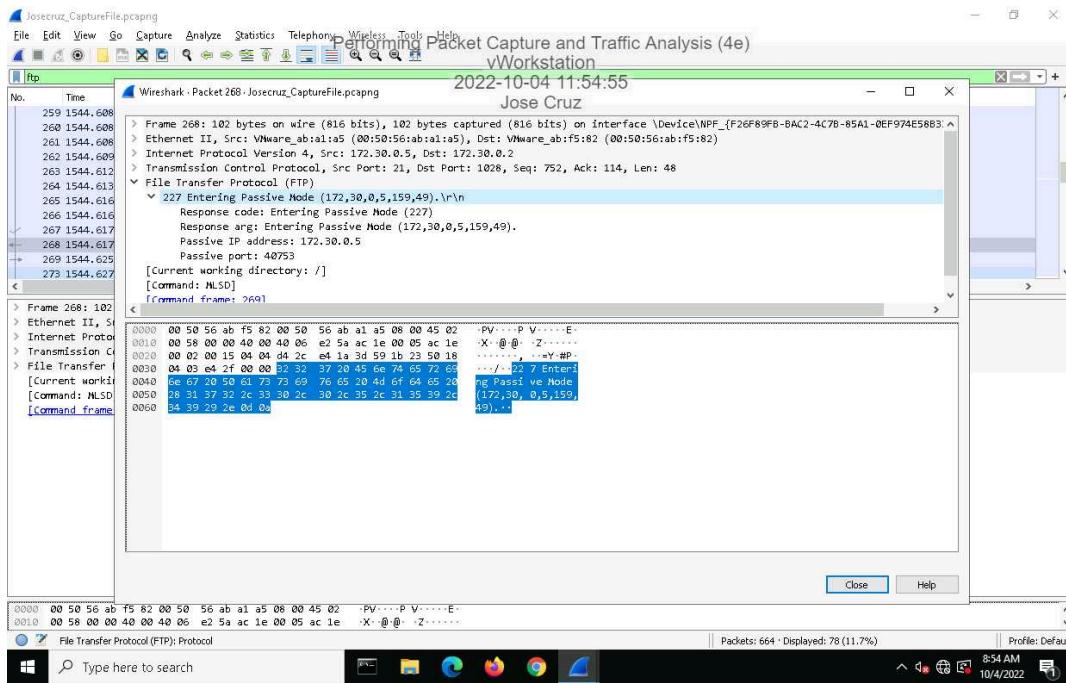
26. Make a screen capture showing the highlighted (encrypted) data in the Packet Bytes pane.



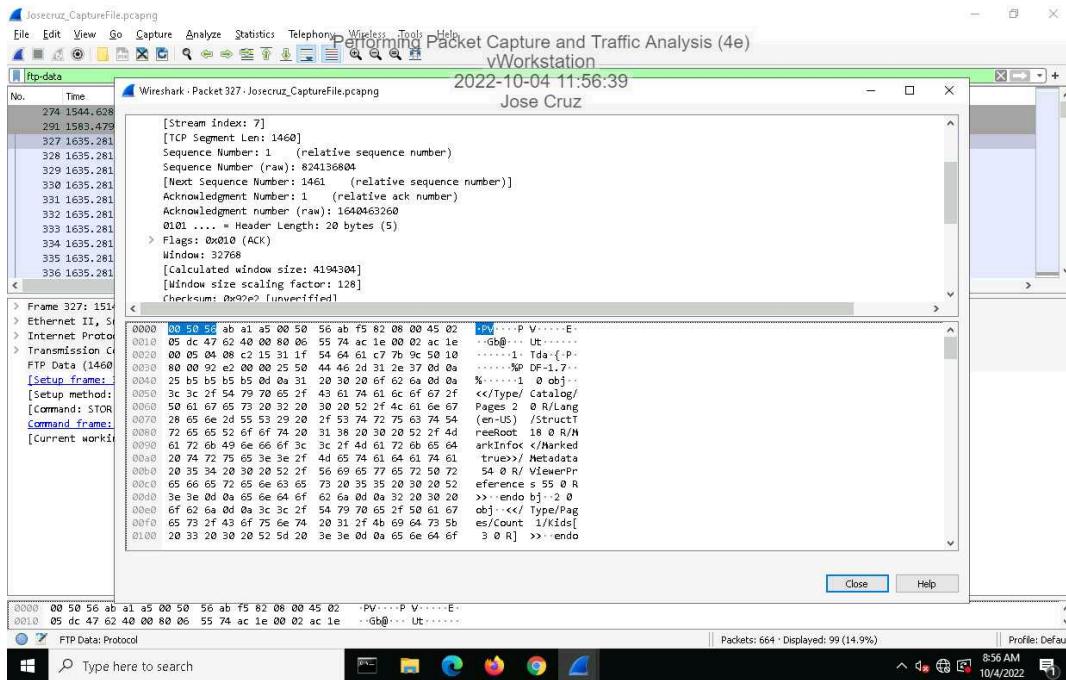
Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

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



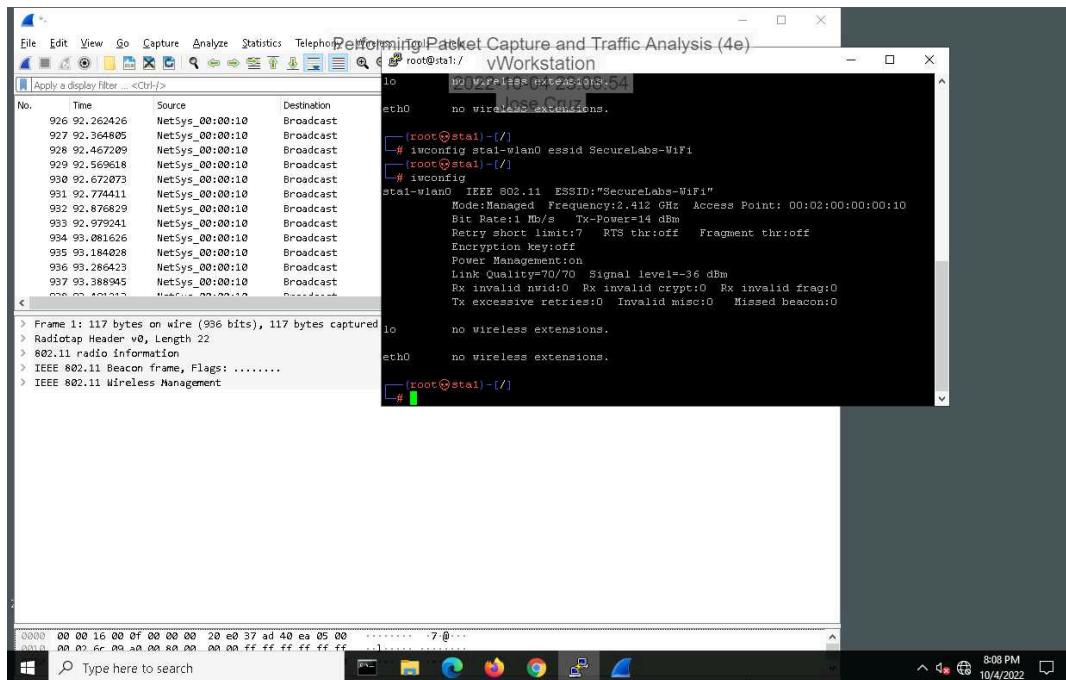
35. Make a screen capture showing the Destination Port field value in the Packet Details pane.



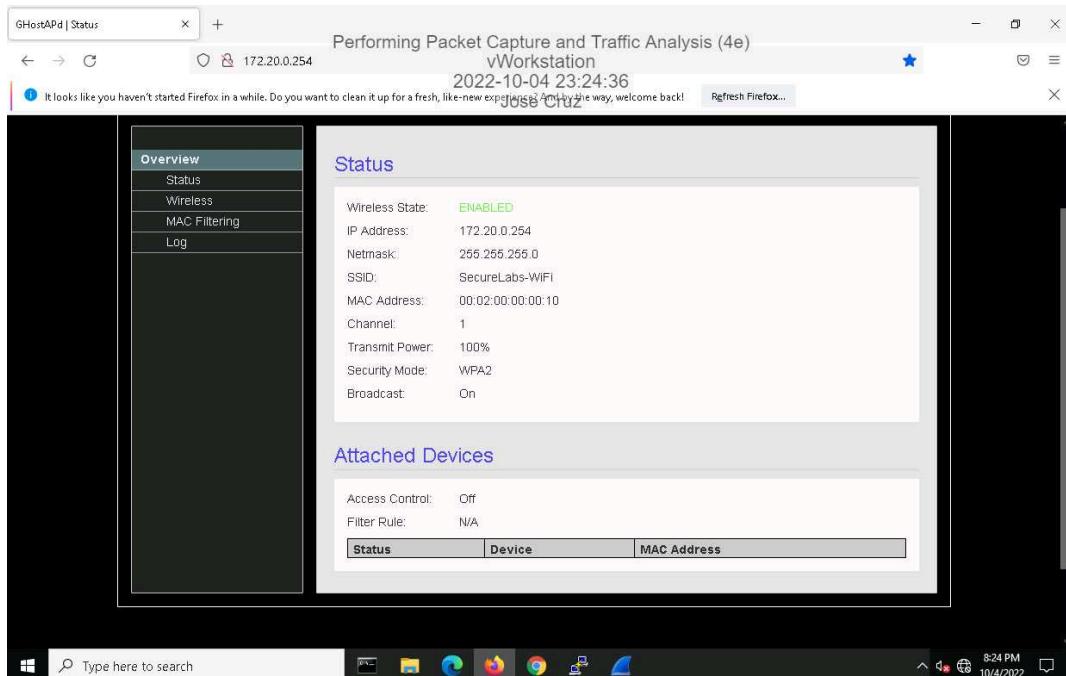
Section 2: Applied Learning

Part 1: Configure Wireshark and Generate Network Traffic

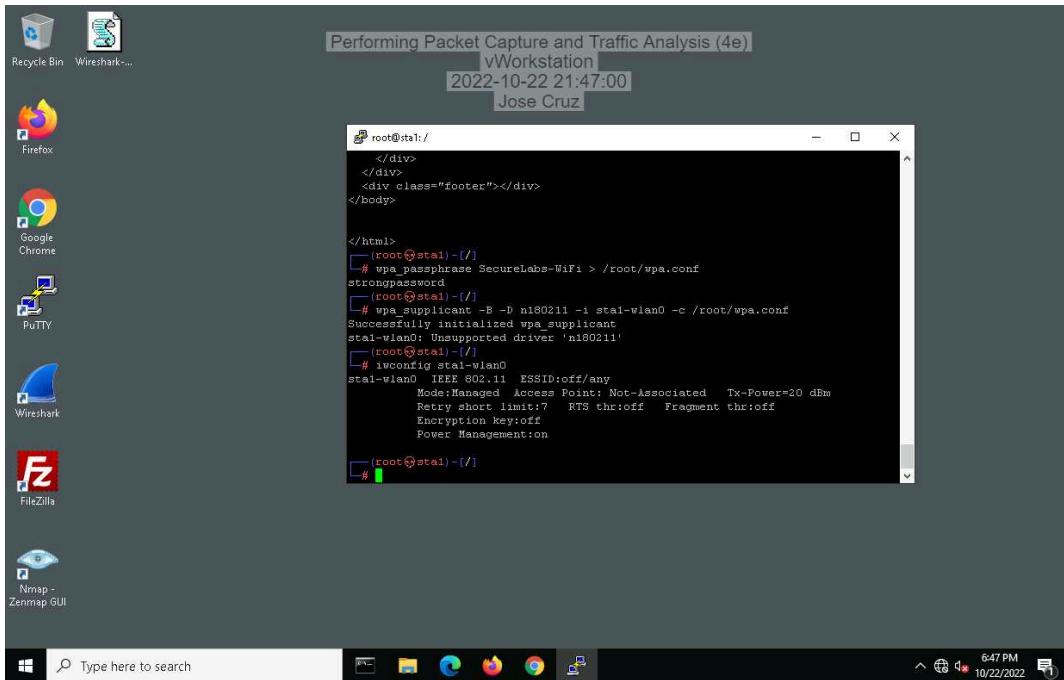
11. Make screen capture showing sta1-wlan0 connected to the SecureLabs-WiFi network.



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

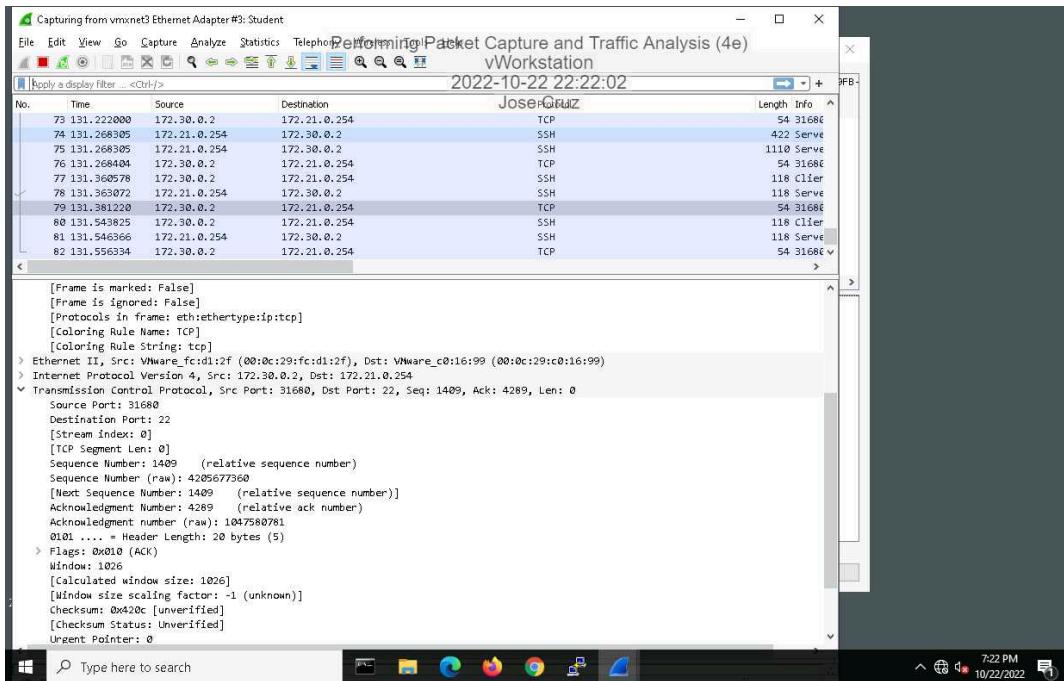


24. Make a screen capture showing the connection to the now-encrypted WLAN.



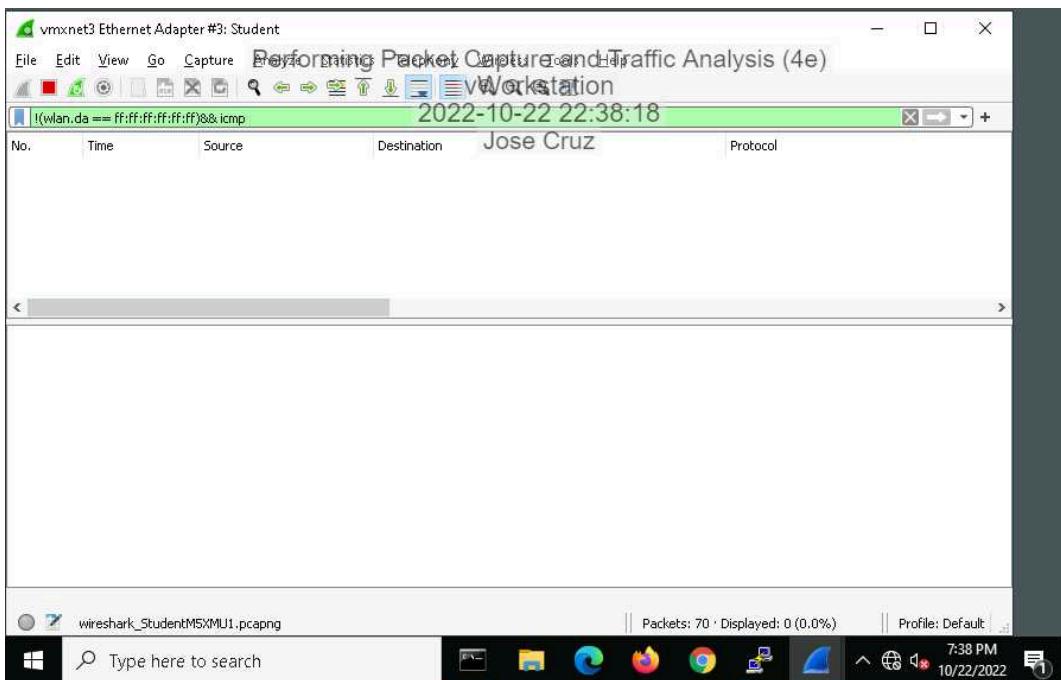
Part 2: Analyze Traffic Using Wireshark

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

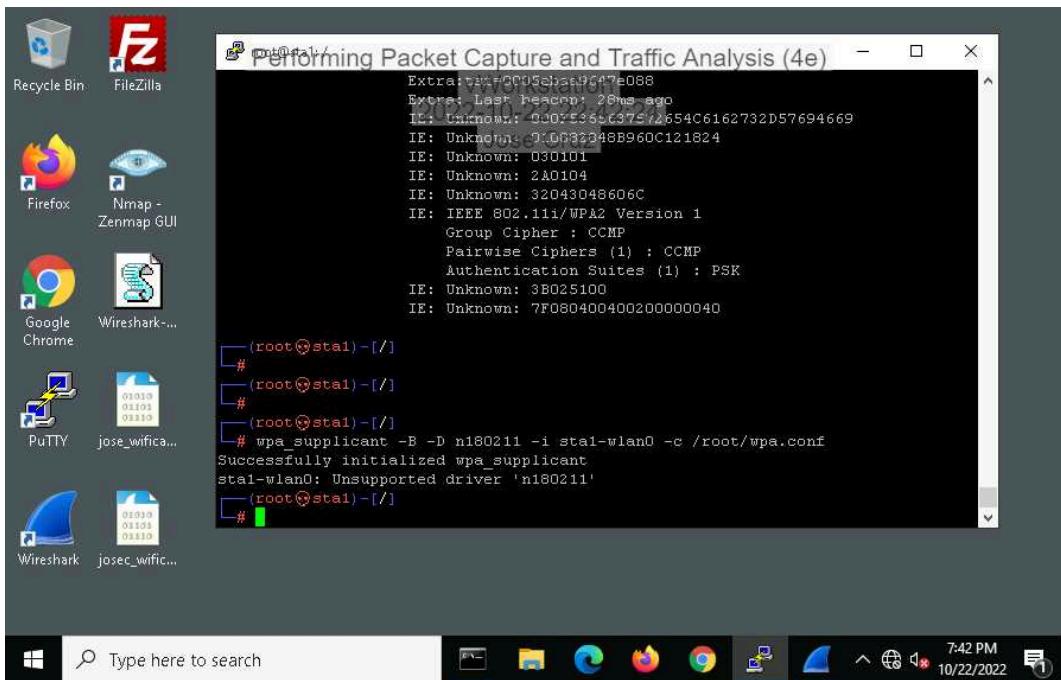


Performing Packet Capture and Traffic Analysis (4e)
Fundamentals of Information Systems Security, Fourth Edition - Lab 03

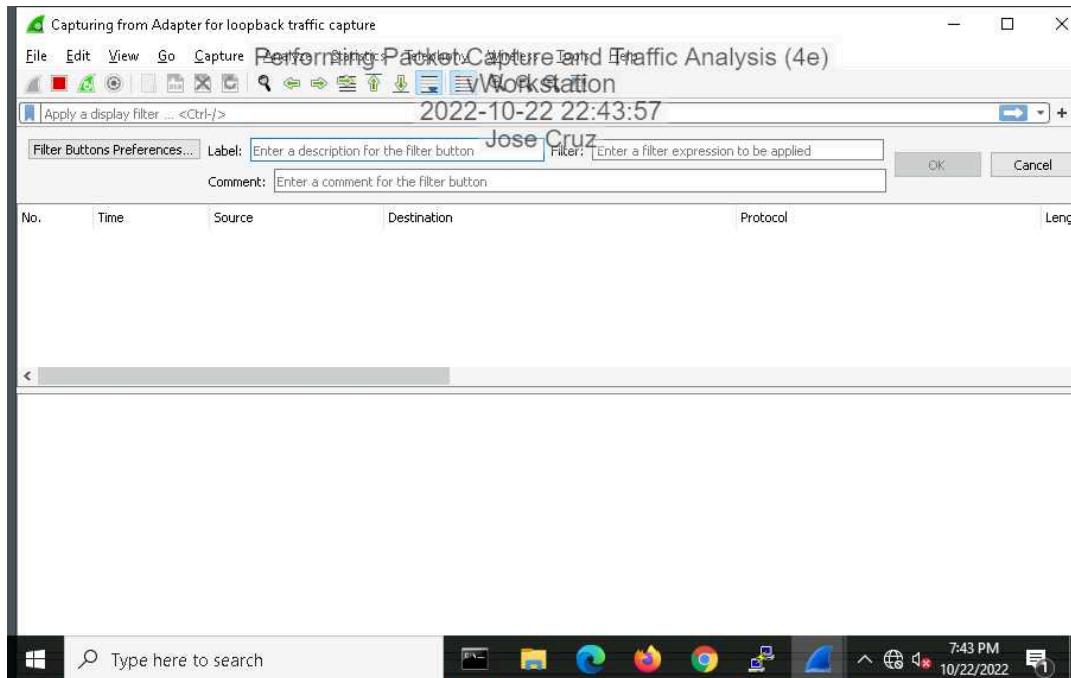
11. Make a screen capture showing the **Packet Details** for the ICMP packet.



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



- 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.

The screenshot shows a Windows desktop environment. In the center is a terminal window titled 'root@sta1:/'. The title bar also displays 'Performing Packet Capture and Traffic Analysis (4e)' and 'vWorkstation' along with a date and time stamp '2022-10-22 22:58:47'. The terminal window contains the following text:

```
CH 1 ][ Elapsed: 2 mins ][ 2022-10-23 00:50:50
root@sta1:/
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH
00:02:00:00:00:10 -34 100    1253      0   0   1   54 WPA2 CCMP  PSK

BSSID          STATION          PWR   Rate Lost   Frames Notes Pro
dress>replay-ng --deauth 10 -a <bssid> -c <station of your choosing's MAC ad
\> aireplay-ng --deauth 10 -a <bssid> -c <station of your choosing's MAC address>
sta1-wlan0 --ig
bash: syntax error near unexpected token `newline'
bash: sta1-wlan0: command not found
\# sta1-wlan0 --ig
bash: sta1-wlan0: command not found
[root@sta1 ~]
\#
[root@sta1 ~]
dress>sta1-wlan0 --iguth 10 -a <bssid> -c <station of your choosing's MAC ad
\>
```

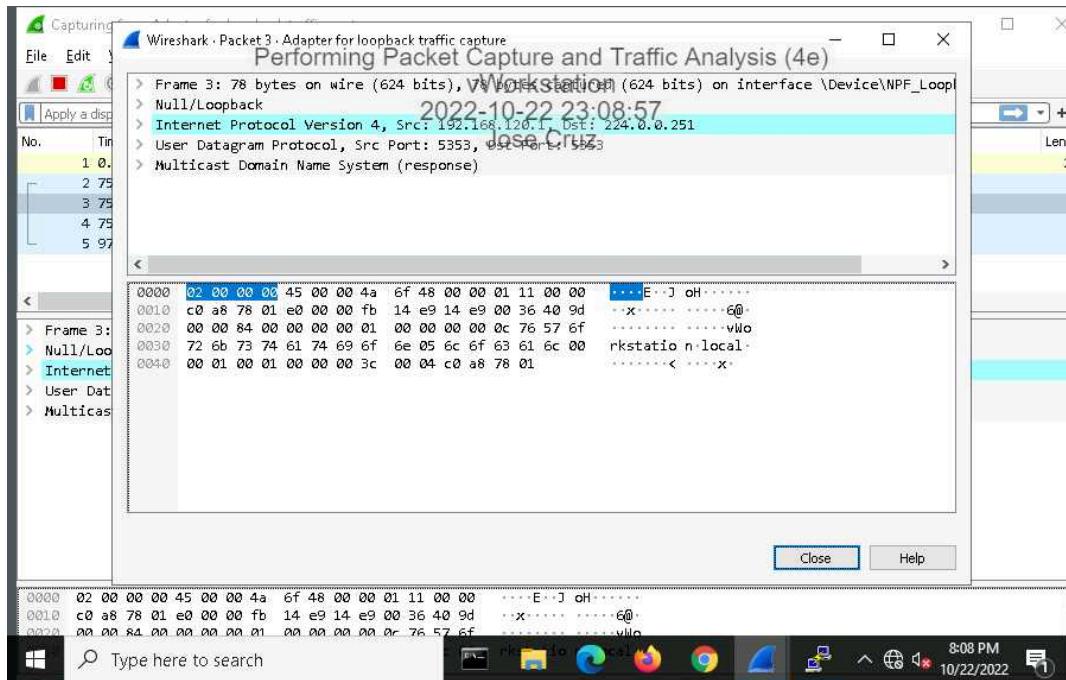
The desktop background is dark grey. On the left, there is a vertical column of icons for 'Recycle Bin', 'FZ', 'root@sta1:/', 'Firefox', 'Google Chrome', 'PuTTY', and 'Wireshark'. At the bottom, the taskbar includes the Start button, a search bar with 'Type here to search', and several pinned application icons: File Explorer, Edge, Firefox, Google Chrome, FileZilla, Task View, and a battery icon. The system tray shows the date '10/22/2022' and the time '7:58 PM'.

Part 2: Analyze Malicious Network Traffic

Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

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.

