

Student:

Sadam Hashi

Email:

smhashi@asu.edu

Time on Task:

10 hours, 20 minutes

Progress:

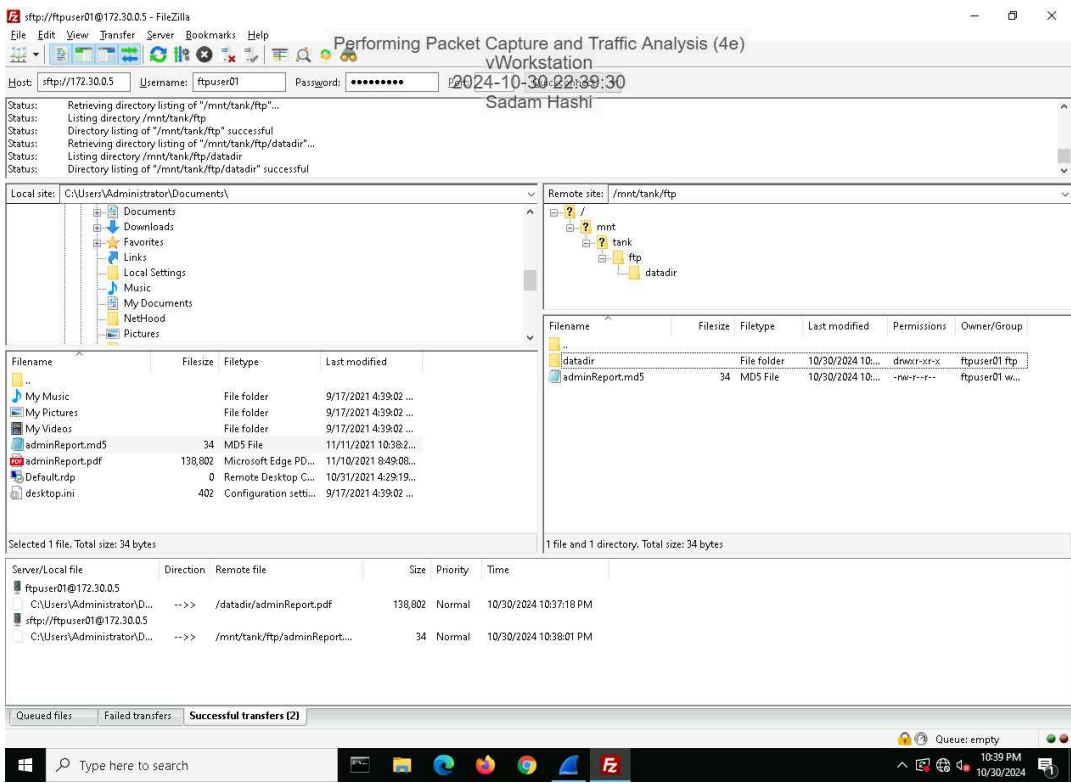
100%

Report Generated: Friday, November 1, 2024 at 1:43 AM

Section 1: Hands-On Demonstration

Part 1: Configure Wireshark and Generate Network Traffic

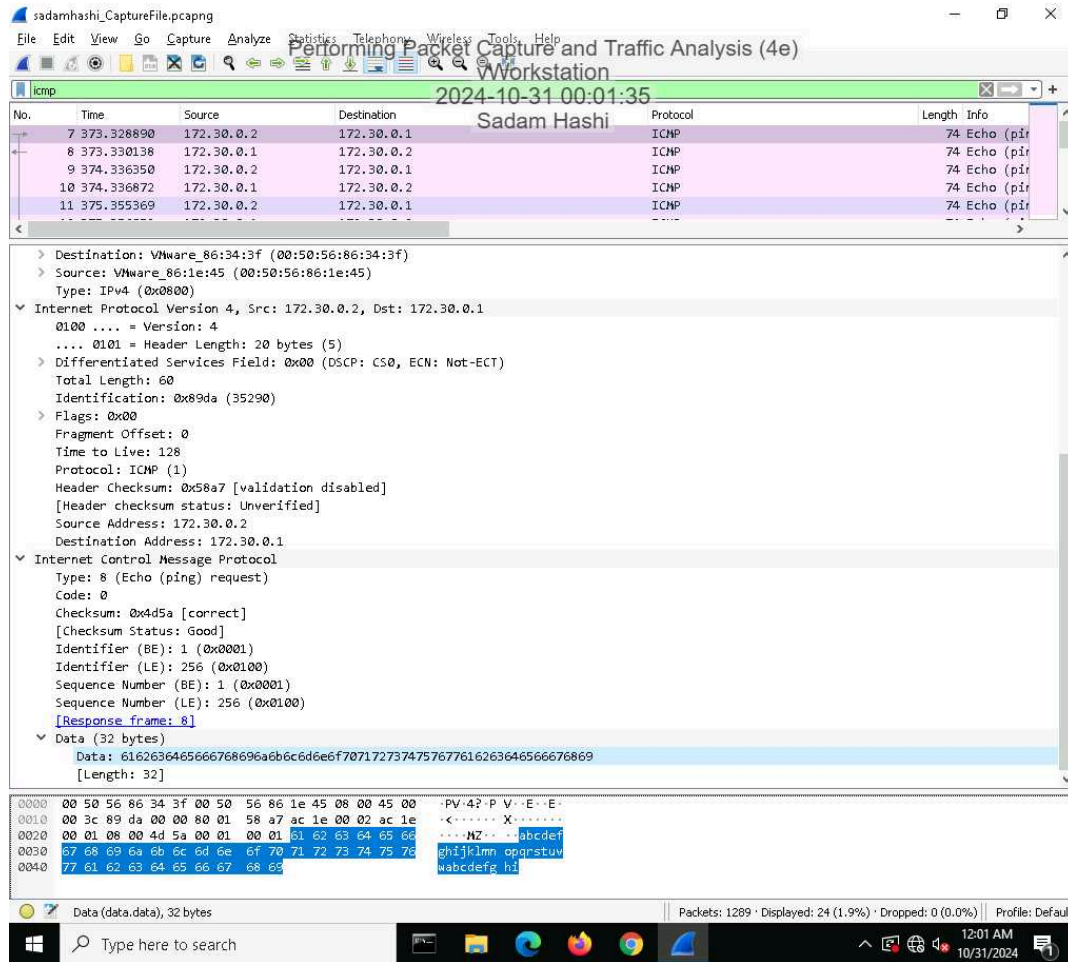
29. Make a screen capture showing the successful FTP and SFTP file transfers.



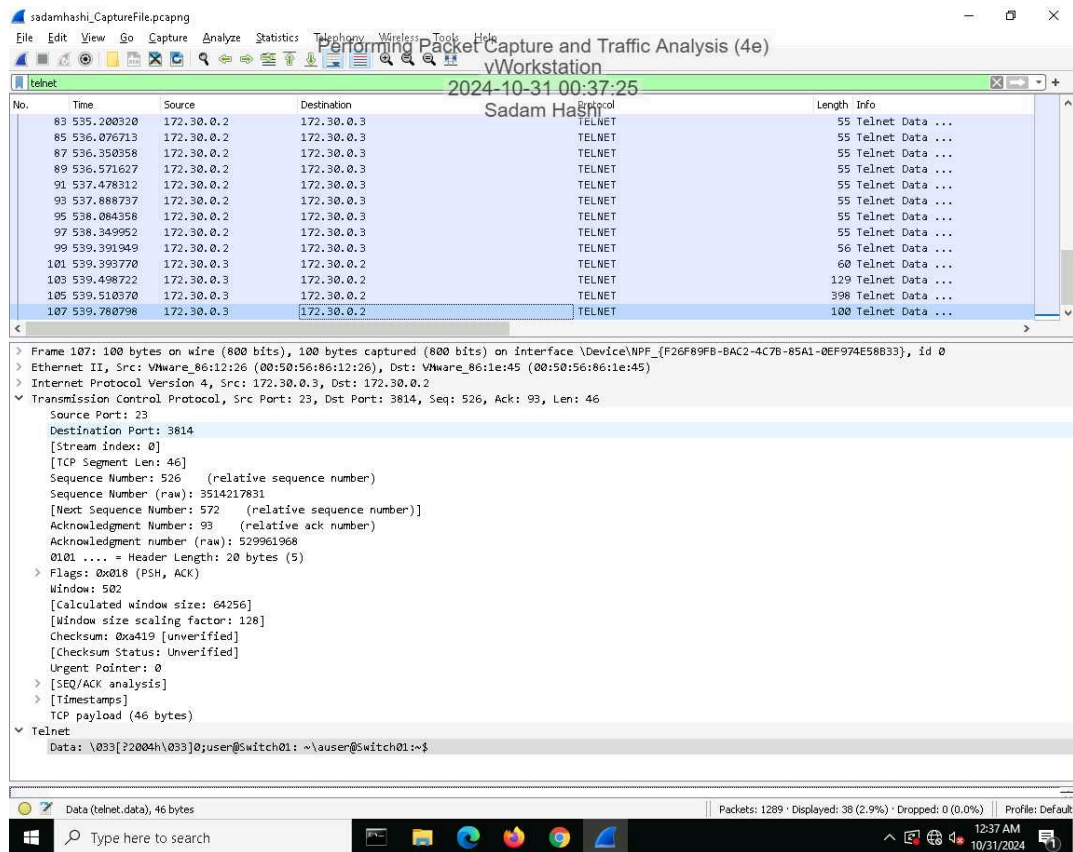
Part 2: Analyze Traffic Using Wireshark

## 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.

The screenshot displays a Wireshark packet capture of an SSHv2 connection. The top pane shows a list of packets, with packet 154 selected. The middle pane shows the details of the selected packet, which is a TCP segment from source port 22 to destination port 3816. The bottom pane shows the raw packet data in hexadecimal and ASCII. The packet is an SSHv2 message, specifically a 'New Keys, Encrypted packet' (len=64). The details pane shows the SSH Protocol section, indicating the encryption algorithm is aes256-ctr and the MAC algorithm is hmac-sha2-256. The packet is labeled as 'Server-to-client'.

No.	Time	Source	Destination	Length	Info
120	697.971747	172.30.0.2	172.30.0.1	82	Client: Protocol (SSH-2.0-PuTTY_Release
122	697.989004	172.30.0.1	172.30.0.2	75	Server: Protocol (SSH-2.0-OpenSSH_7.9)
123	698.002947	172.30.0.2	172.30.0.1	1310	Client: Key Exchange Init
124	698.003366	172.30.0.1	172.30.0.2	766	Server: Key Exchange Init
125	698.009823	172.30.0.2	172.30.0.1	102	Client: Elliptic Curve Diffie-Hellman K
127	698.021685	172.30.0.1	172.30.0.2	454	Server: Elliptic Curve Diffie-Hellman K
129	698.054443	172.30.0.2	172.30.0.1	134	Client: New Keys, Encrypted packet (len=64)
131	698.055448	172.30.0.1	172.30.0.2	118	Server: Encrypted packet (len=64)
145	756.729026	172.30.0.2	172.30.0.1	82	Client: Protocol (SSH-2.0-PuTTY_Release
147	756.739870	172.30.0.1	172.30.0.2	75	Server: Protocol (SSH-2.0-OpenSSH_7.9)
148	756.748319	172.30.0.2	172.30.0.1	1310	Client: Key Exchange Init
149	756.748772	172.30.0.1	172.30.0.2	766	Server: Key Exchange Init
150	756.755624	172.30.0.2	172.30.0.1	102	Client: Elliptic Curve Diffie-Hellman K
152	756.766668	172.30.0.1	172.30.0.2	454	Server: Elliptic Curve Diffie-Hellman K
154	756.788870	172.30.0.2	172.30.0.1	134	Client: New Keys, Encrypted packet (len=64)

Transmission Control Protocol, Src Port: 22, Dst Port: 3816, Seq: 22, Ack: 1285, Len: 712

Source Port: 22  
Destination Port: 3816  
[Stream index: 2]  
[TCP Segment Len: 712]  
Sequence Number: 22 (relative sequence number)  
Sequence Number (raw): 3225456981  
[Next Sequence Number: 734 (relative sequence number)]  
Acknowledgment Number: 1285 (relative ack number)  
Acknowledgment number (raw): 4034498647  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window: 127  
[Calculated window size: 65024]  
[Window size scaling factor: 512]  
Checksum: 0xe258 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[SEQ/ACK analysis]  
[Timestamps]  
TCP payload (712 bytes)

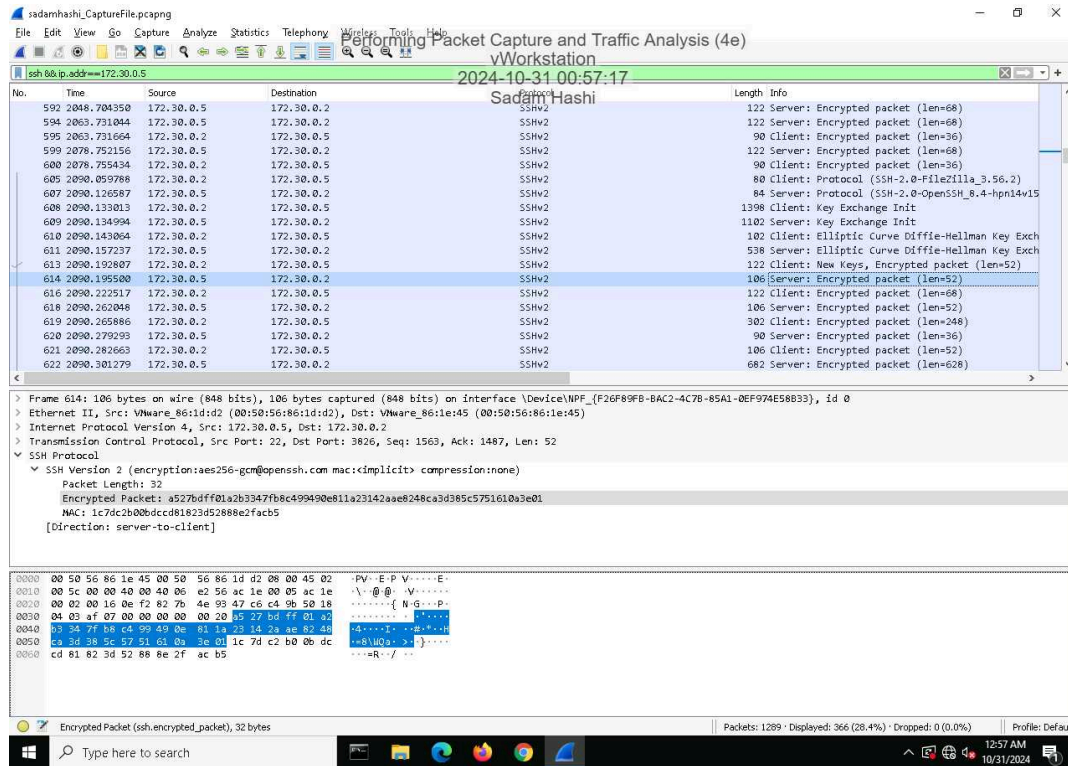
SSH Protocol  
SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)  
[Direction: server-to-client]

0000 00 50 56 86 1e 45 00 50 56 86 34 3f 08 00 45 02 -PV- E P V-4? E-

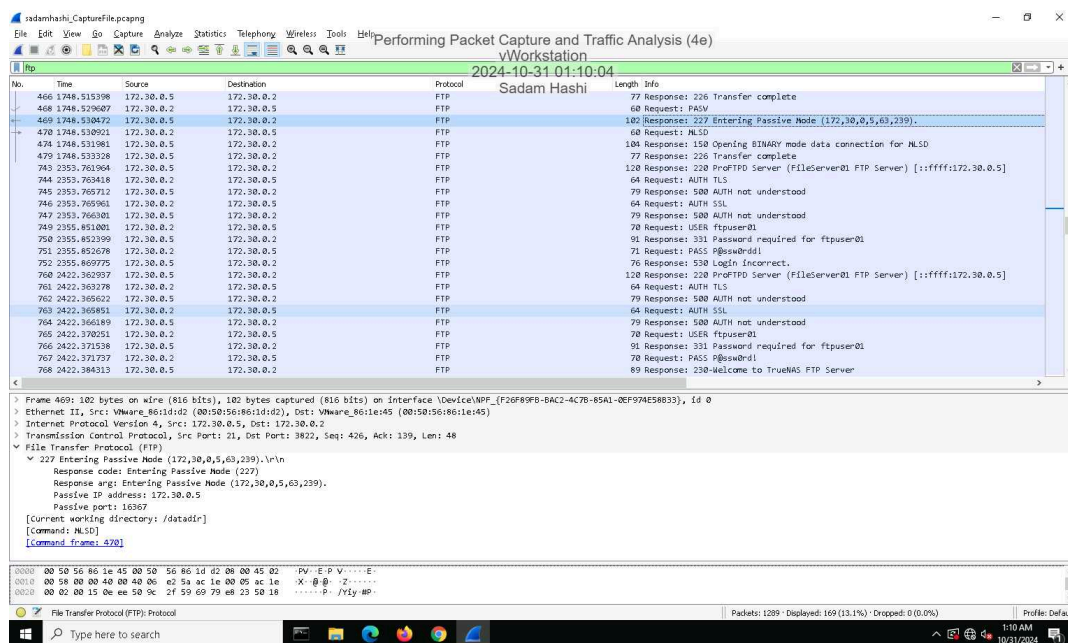
Packets: 1289 • Displayed: 51 (4.0%) • Dropped: 0 (0.0%) • Profile: Default

12:50 AM 10/31/2024

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

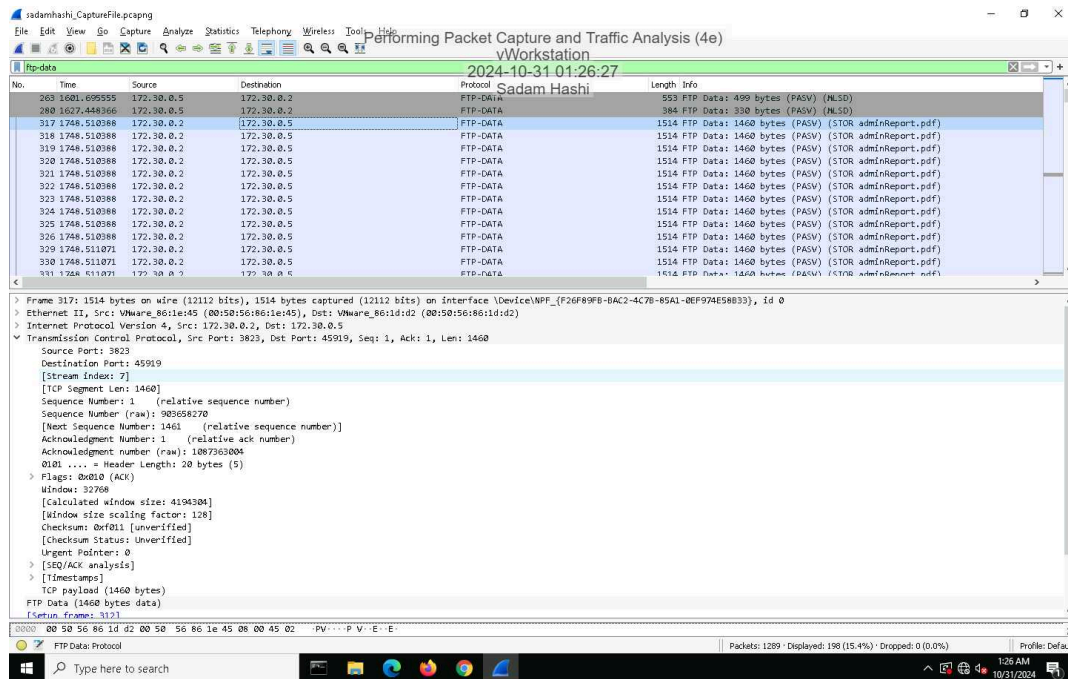


### 31. Make a screen capture showing the passive port specified by the FTP server in the Packet Details pane.





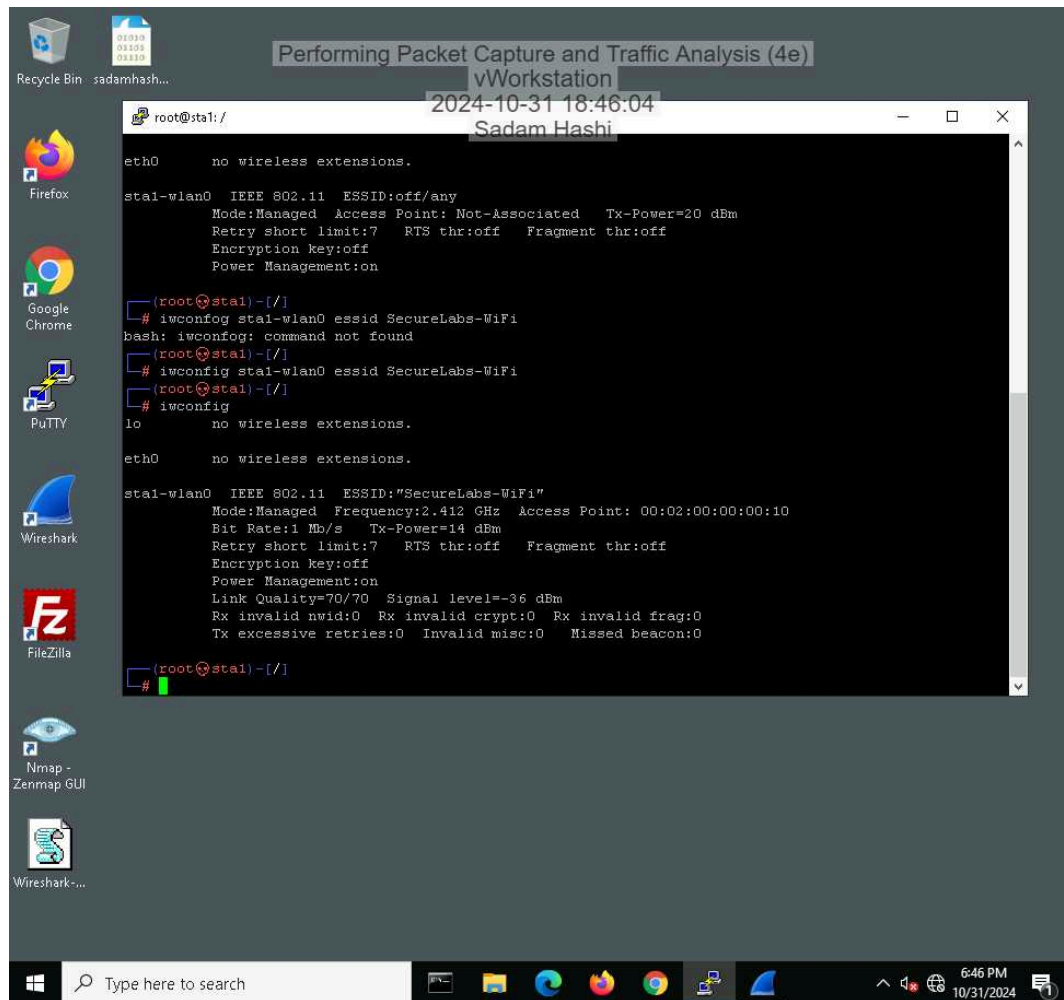
## 35. Make a screen capture showing the Destination Port field value in the Packet Details pane.



## 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.



## Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

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

The screenshot shows a web browser window titled "Performing Packet Capture and Traffic Analysis (4e)" displaying the GHostAPd Status page. The browser's address bar shows the URL "172.20.0.254". A notification at the top of the browser states: "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, better user experience? And by the way, welcome back! Refresh Firefox...".

The GHostAPd interface has a dark theme. On the left is a sidebar with a menu containing "Overview", "Status", "Wireless", "MAC Filtering", and "Log". The "Status" page is active, showing the following 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 information is the "Attached Devices" section, which includes:

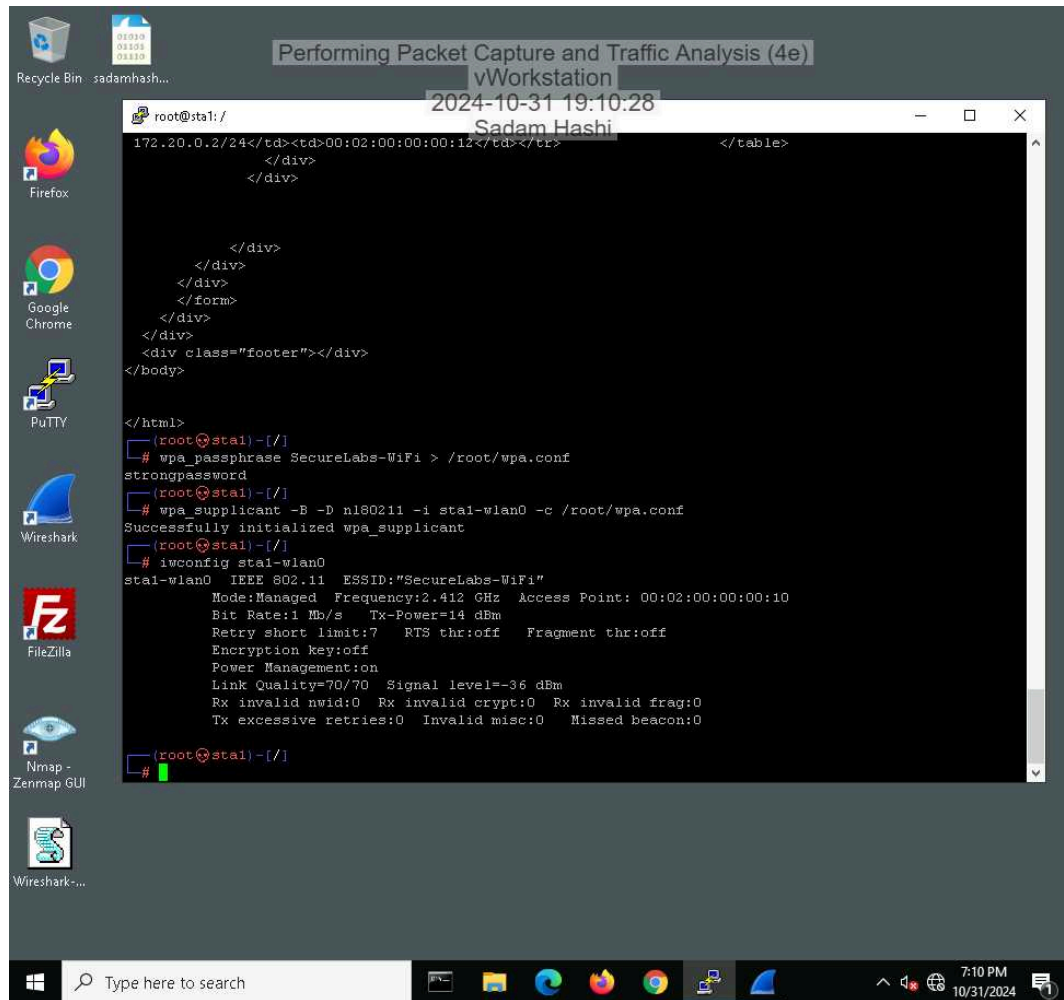
- Access Control: Off
- Filter Rule: N/A

A table for attached devices is shown with the following headers: Status, Device, and MAC Address. The table is currently empty.

The bottom of the screenshot shows the vWorkstation taskbar with a search bar and several application icons. The system clock in the bottom right corner indicates the time is 6:53 PM on 10/31/2024.

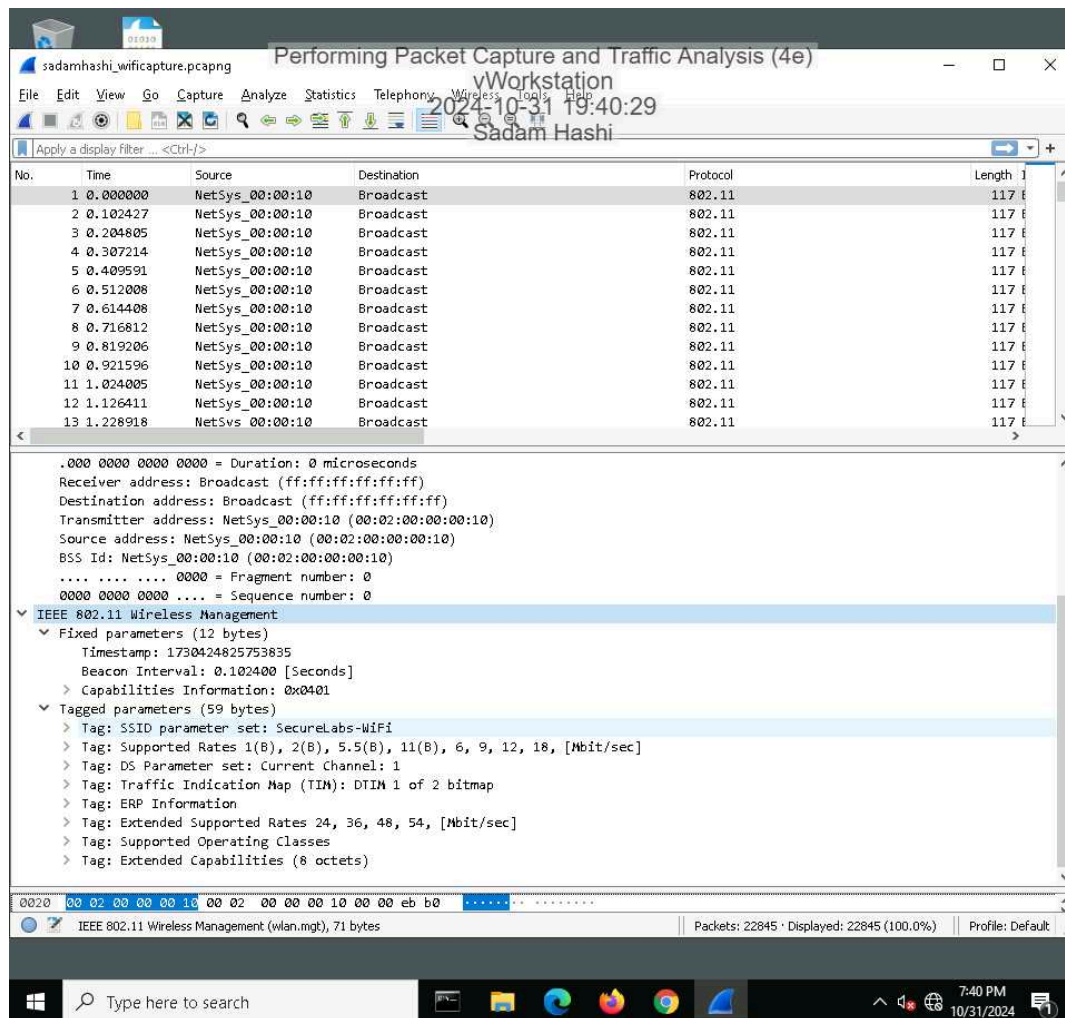


### 24. Make a screen capture showing the connection to the now-encrypted WLAN.



## Part 2: Analyze Traffic Using Wireshark

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



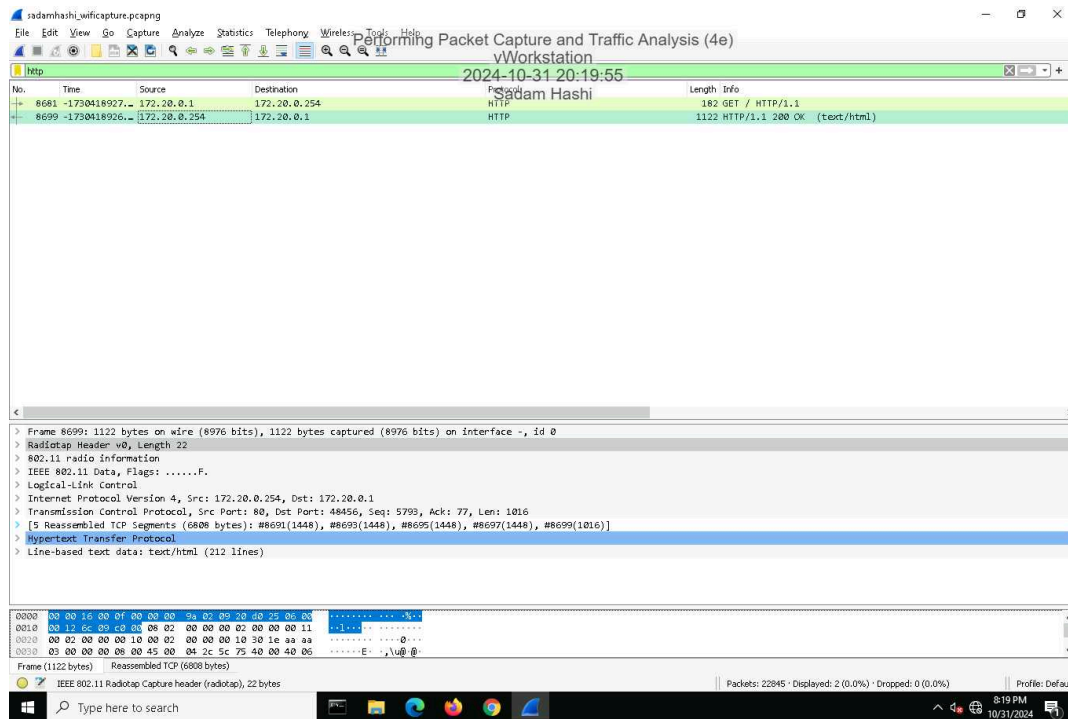
## 11. Make a screen capture showing the Packet Details for the ICMP packet.

The screenshot shows a Wireshark packet capture window titled "Performing Packet Capture and Traffic Analysis (4e)". The capture filter is set to "!(wlan.da == ff:ff:ff:ff:ff:ff) && icmp". The packet list shows several ICMP Echo requests. The selected packet (No. 8065) is an ICMP Echo request from 172.20.0.1 to 172.20.0.2. The packet details pane shows the following information:

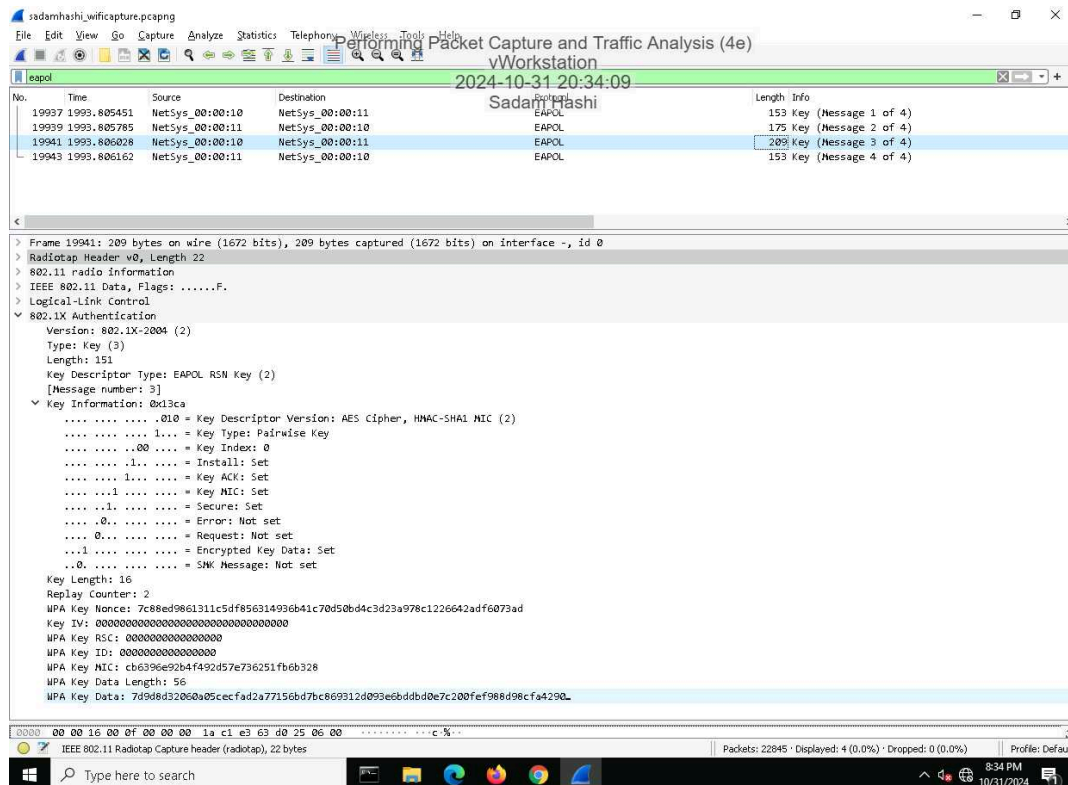
- Frame 8065: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface -, id 0
- Radiotap Header v0, Length 22
- 802.11 radio information
- IEEE 802.11 Data, Flags: .....T
- Logical-Link Control
- Internet Protocol Version 4, Src: 172.20.0.1, Dst: 172.20.0.2
- Internet Control Message Protocol
  - Type: 8 (Echo (ping) request)
  - Code: 0
  - Checksum: 0xd32e [correct]
  - [Checksum Status: Good]
  - Identifier (BE): 51623 (0xc9a7)
  - Identifier (LE): 42953 (0xa7c9)
  - Sequence Number (BE): 1 (0x0001)
  - Sequence Number (LE): 256 (0x0100)
- [No response seen]
- Timestamp from icmp data: Oct 31, 2024 18:47:04.000000000 Pacific Daylight Time
- [Timestamp from icmp data (relative): 0.310709000 seconds]
- Data (48 bytes)
  - Data: 5bbb040000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...
  - [Length: 48]

The packet bytes pane shows the raw data in hexadecimal and ASCII format. The status bar at the bottom indicates "Packets: 22645 • Displayed: 16 (0.1%) • Dropped: 0 (0.0%)".

## 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.

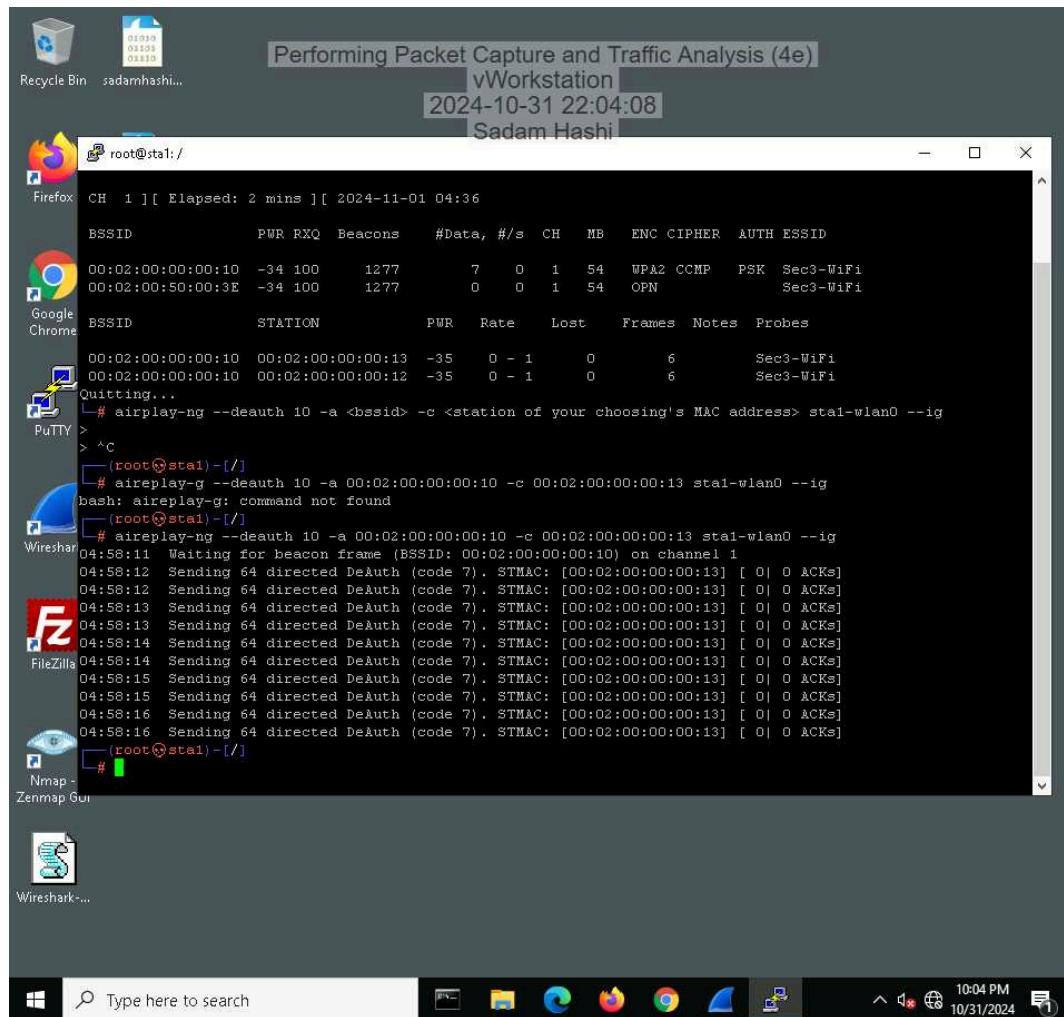




## Section 3: Challenge and Analysis

### Part 1: Generate Malicious Network Traffic

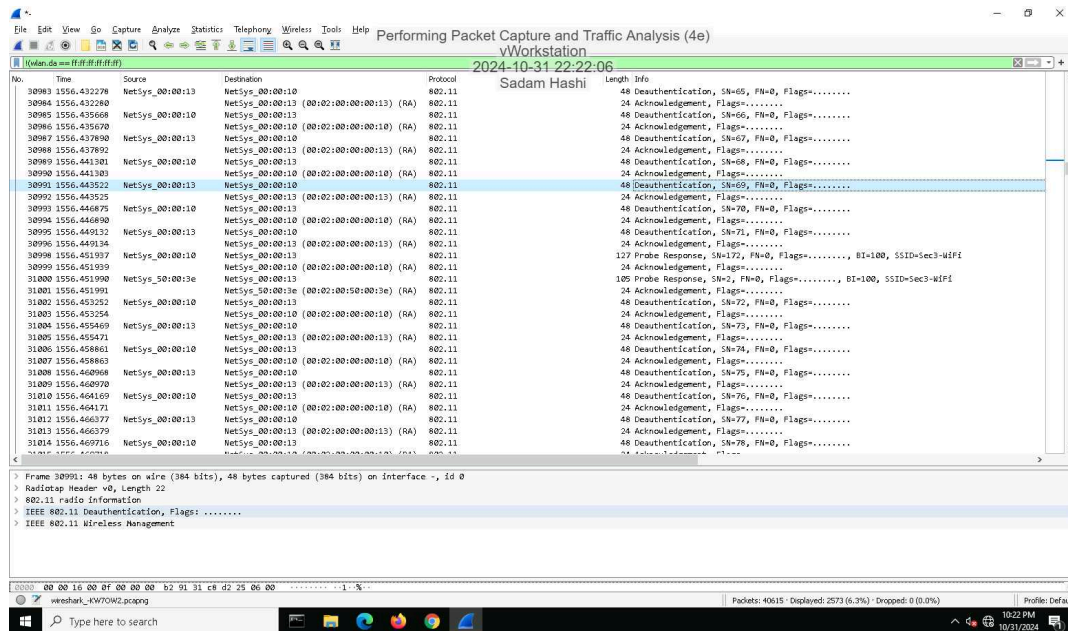
Make a screen capture showing the `aireplay-ng --deauth` output.



### 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.

