

Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

Student:

Matias Kun

Email:

rvh4zx@virginia.edu

Time on Task:

18 hours, 46 minutes

Progress:

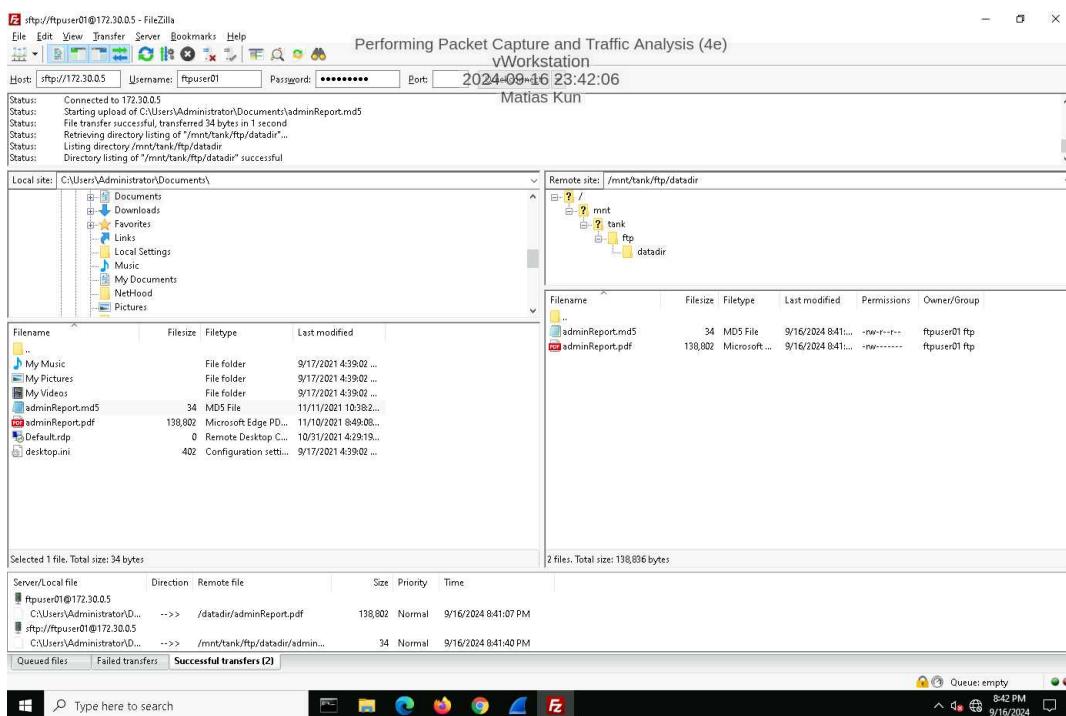
100%

Report Generated: Wednesday, October 2, 2024 at 10:18 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.

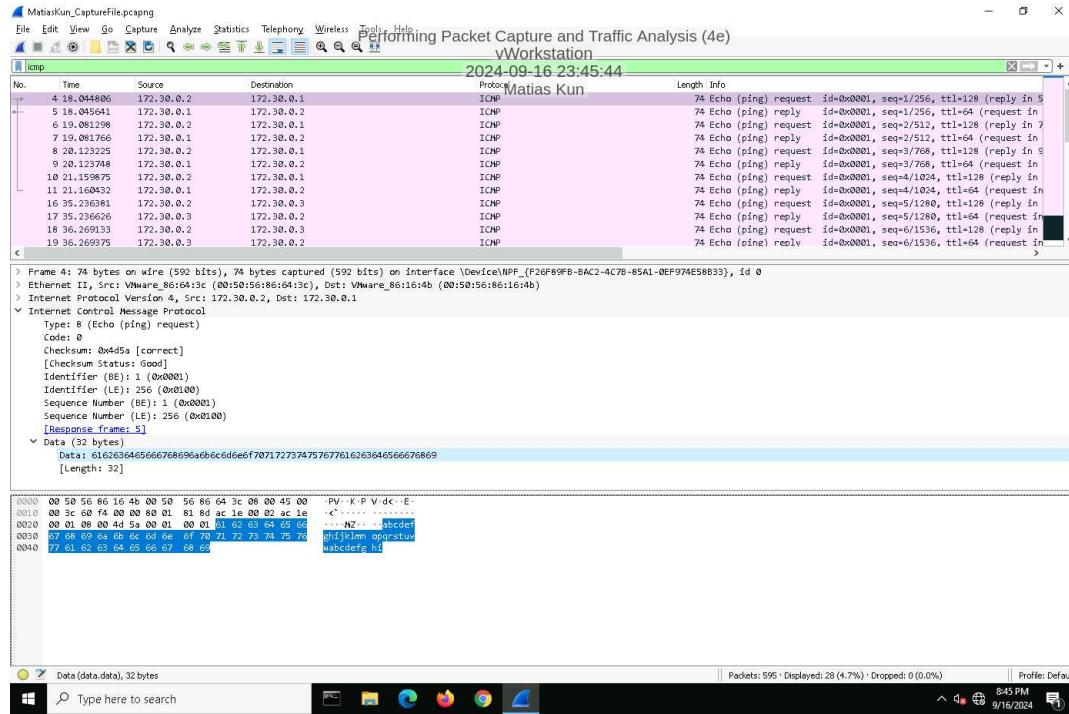


Part 2: Analyze Traffic Using Wireshark

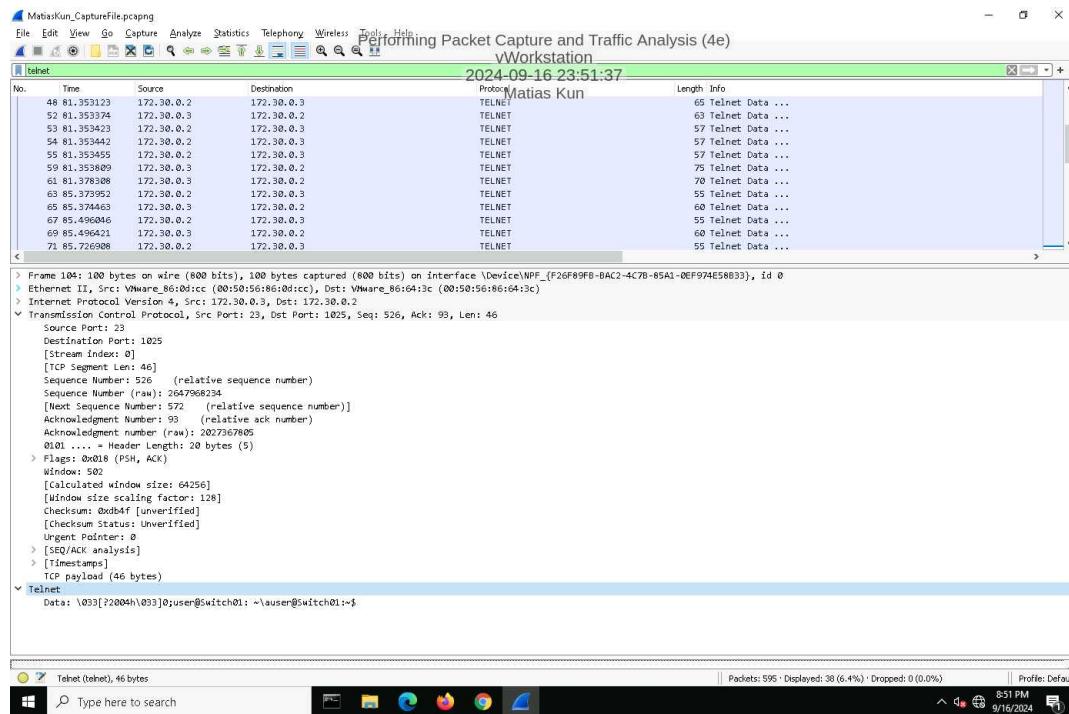
Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

7. Make a screen capture showing the ICMP payload.



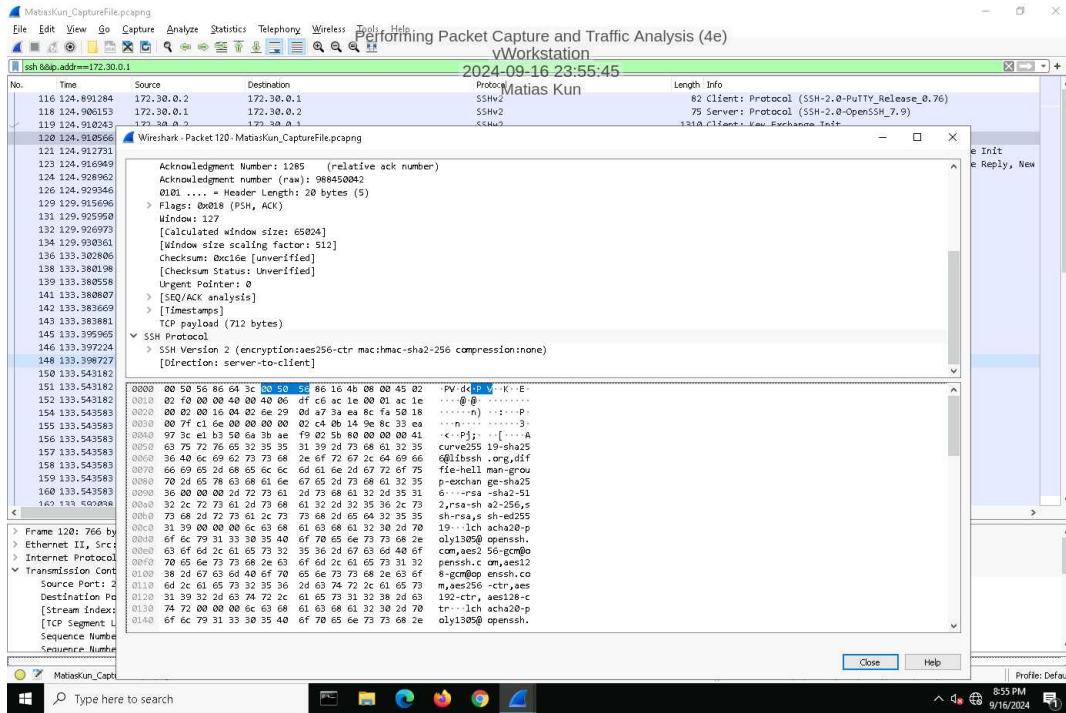
15. Make a screen capture showing the *Last Login:* information in the Packet Details pane.



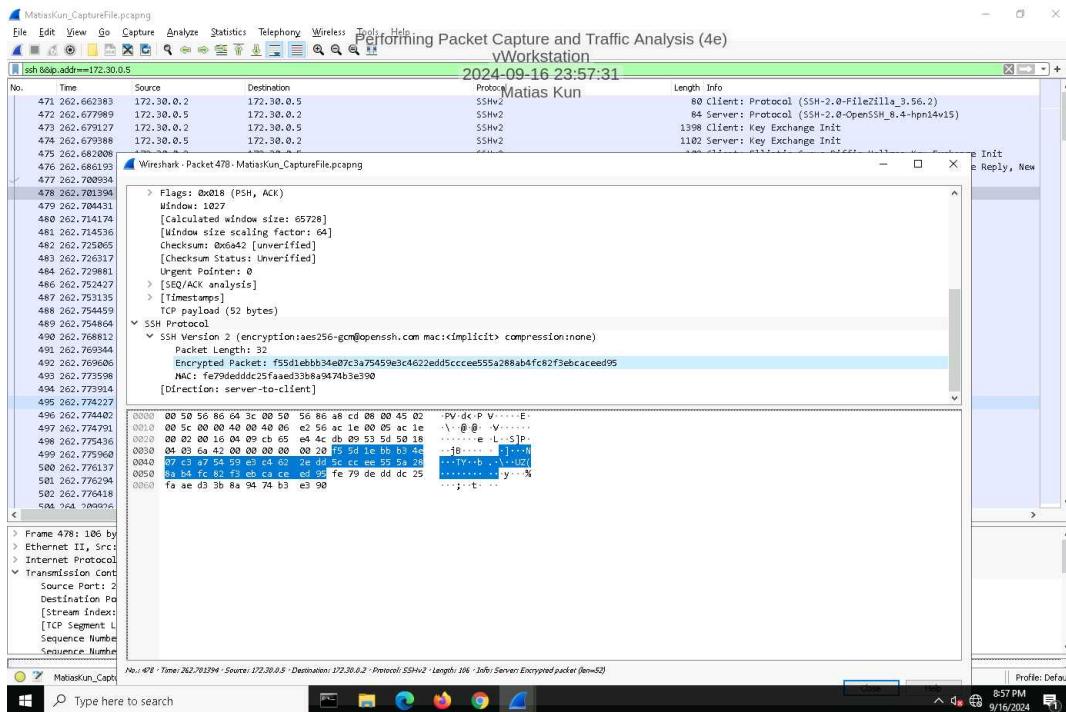
Performing Packet Capture and Traffic Analysis (4e)

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.



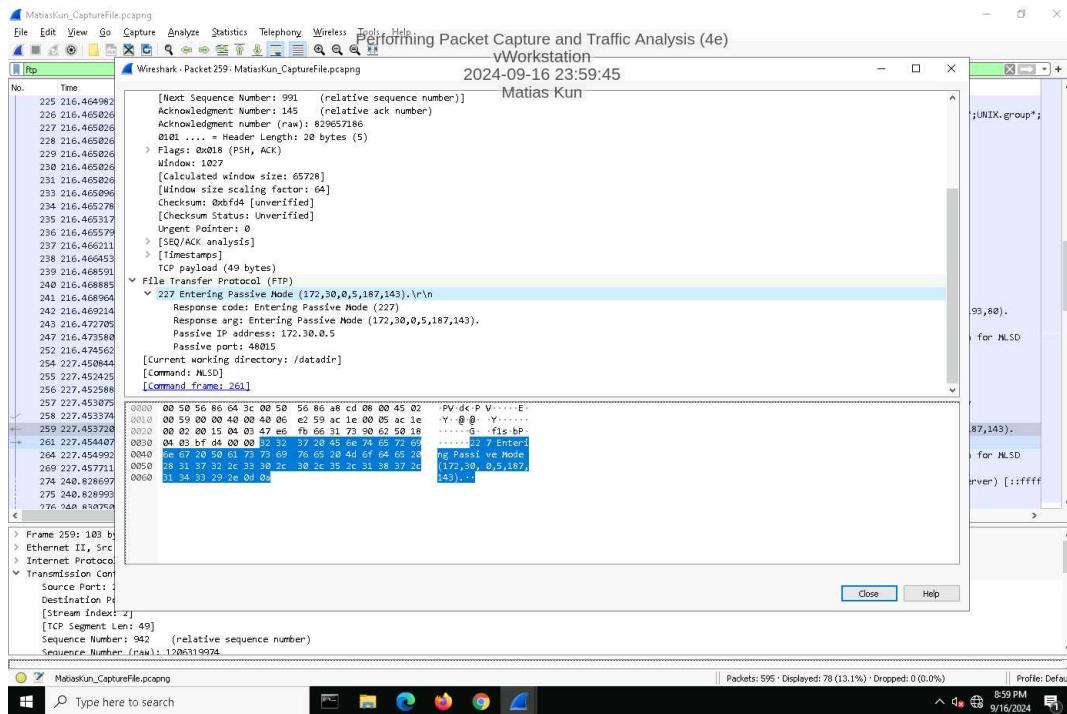
26. Make a screen capture showing the highlighted (encrypted) data in the Packet Bytes pane.



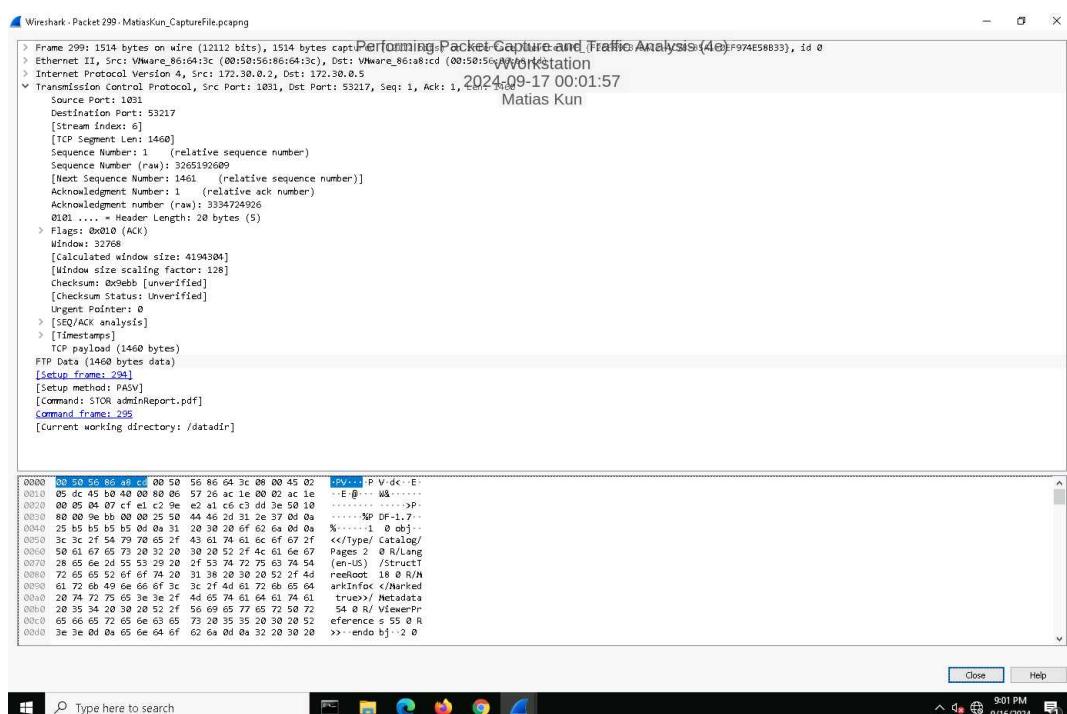
Performing Packet Capture and Traffic Analysis (4e)

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.

The screenshot shows a terminal window titled "Performing Packet Capture and Traffic Analysis (4e)" running on a Windows 10 desktop. The terminal content is as follows:

```
root@sta1:/ 
sta1-wlan0 Scan completed : 
    Cell 01 - Address: 00:02:00:00:00:10 
        Channel: 1 
        Frequency:2.412 GHz (Channel 1) 
        Quality=70/70  Signal level=-36 dBm 
        Encryption key:off 
        ESSID:"SecureLabs-WiFi" 
        Bit Rates:2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s 
          9 Mb/s; 12 Mb/s; 18 Mb/s 
        Bit Rates:12 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s 
        Mode:Master 
        Extra: IEEE 802.11b 
        Extra: Last beacon: 32ms ago 
        IE: Unknown: 000F516563757254C6162732D57694669 
        IE: Unknown: 010882848B960C121824 
        IE: Unknown: 030101 
        IE: Unknown: 2A0104 
        IE: Unknown: 32043048606C 
        IE: Unknown: 38025100 
        IE: Unknown: 7F000400400200000040 

[root@sta1 ~]# 
[root@sta1 ~]# iwconfig 
eth0      no wireless extensions. 
lo       no wireless extensions. 

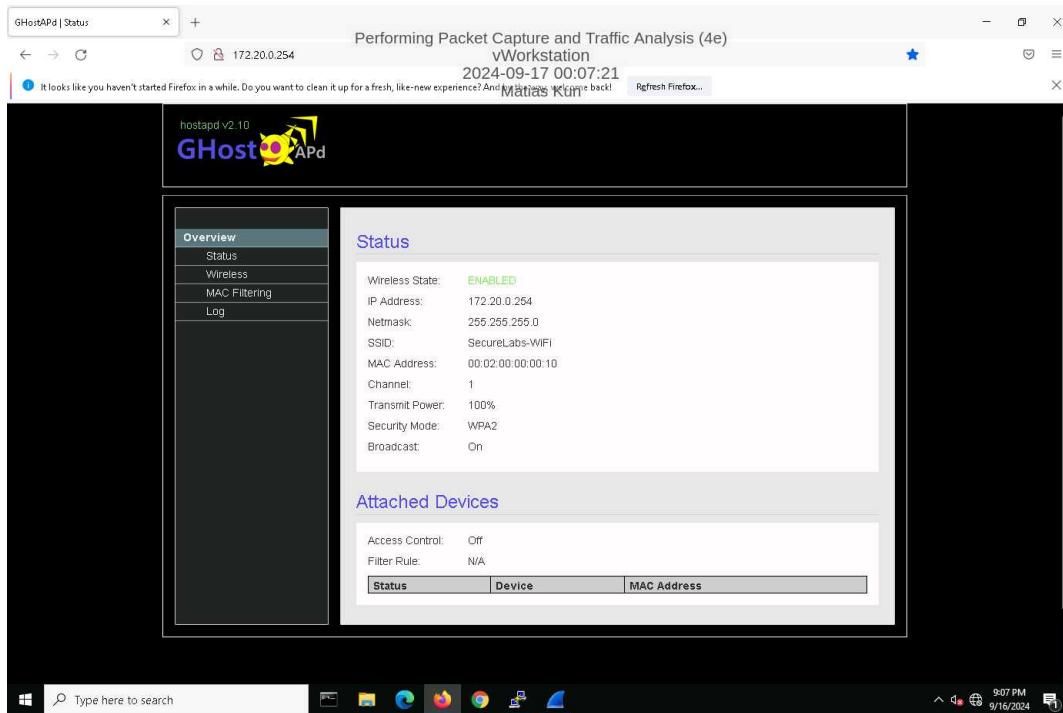
sta1-wlan0  IEEE 802.11  ESSID:"SecureLabs-WiFi" 
          Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm 
          Retry short limit:7  RTS thr:off  Fragment thr:off 
          Encryption key:off 
          Power Management: 
[root@sta1 ~]# 
[root@sta1 ~]# iwconfig sta1-wlan0 essid SecureLabs-WiFi 
[root@sta1 ~]# 
[root@sta1 ~]# iwconfig 
eth0      no wireless extensions. 
lo       no wireless extensions. 

sta1-wlan0  IEEE 802.11  ESSID:"SecureLabs-WiFi" 
          Mode:Managed  Frequency:2.412 GHz  Access Point: 00:02:00:00:00:10 
          Bit Rate:1 Mb/s   Tx-Power:14 dBm 
          Retry short limit:7  RTS thr:off  Fragment thr:off 
          Encryption key:off 
          Power Management: 
          Link Quality=70/70  Signal level=-36 dBm 
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0 
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0 

[root@sta1 ~]# 
```

The terminal shows the root user performing a wireless scan, listing available networks, and then connecting to the "SecureLabs-WiFi" network using the "iwconfig" command. The status bar at the bottom right of the terminal window shows the date and time as 9/16/2024 at 9:05 PM.

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.

A screenshot of a terminal window titled "root@sta1:/". The terminal shows the following command history:

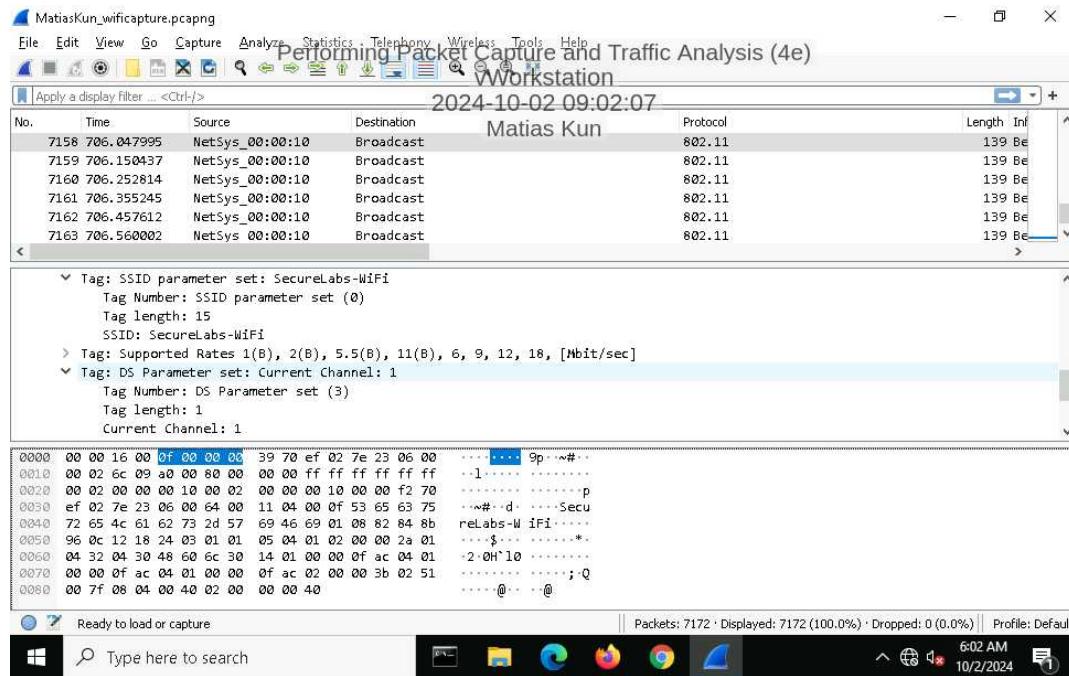
```
</div>
</div>
</div>
</form>
</div>
<div class="footer"></div>
</body>

</html>
[root@sta1]# wpa_passphrase SecureLabs-WiFi > /root/wpa.conf
strongpassword
[root@sta1]# wpa_supplicant -B -D nl80211 -i sta1-wlan0 -c /root/wpa.conf
Successfully initialized wpa_supplicant
[root@sta1]# iwconfig sta1-wlan0
sta1-wlan0 IEEE 802.11 ESSID:"SecureLabs-WiFi"
        Mode:Managed Frequency:2.412 GHz Access Point: 00:02:00:00:00:10
        Bit Rate:1 Mb/s Tx-Power=14 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management
        Link Quality=70/70 Signal level=-36 dBm
        Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
        Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

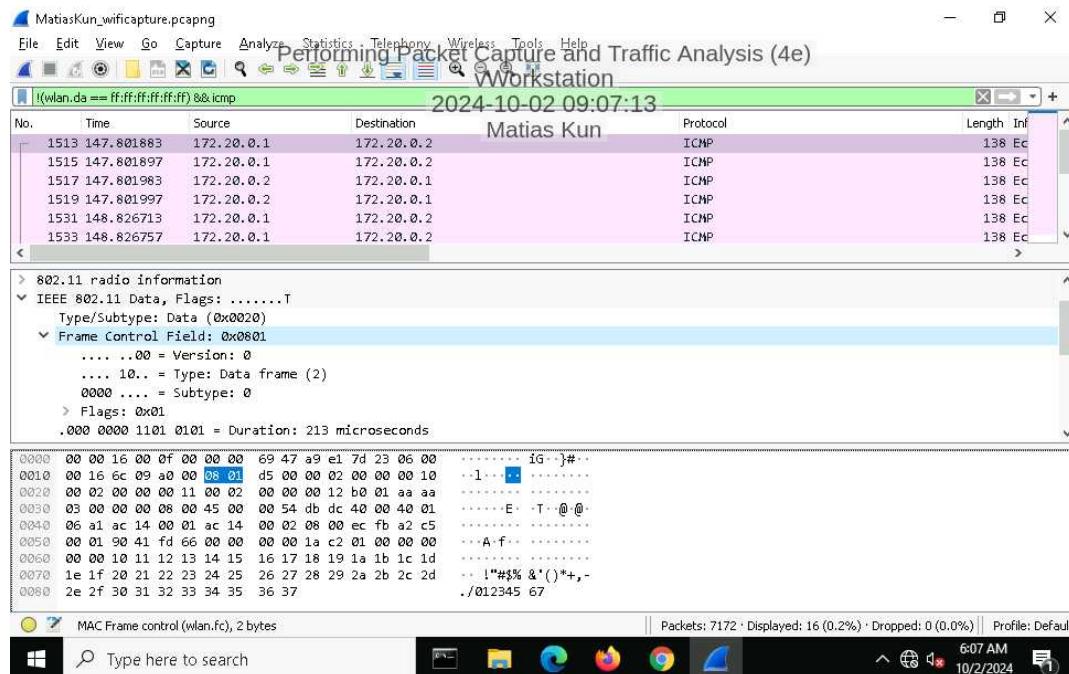
While iwconfig does not display WPA2 encryption status, wpa_supplicant was successfully initialized and is actively handling the encryption in the background.

Part 2: Analyze Traffic Using Wireshark

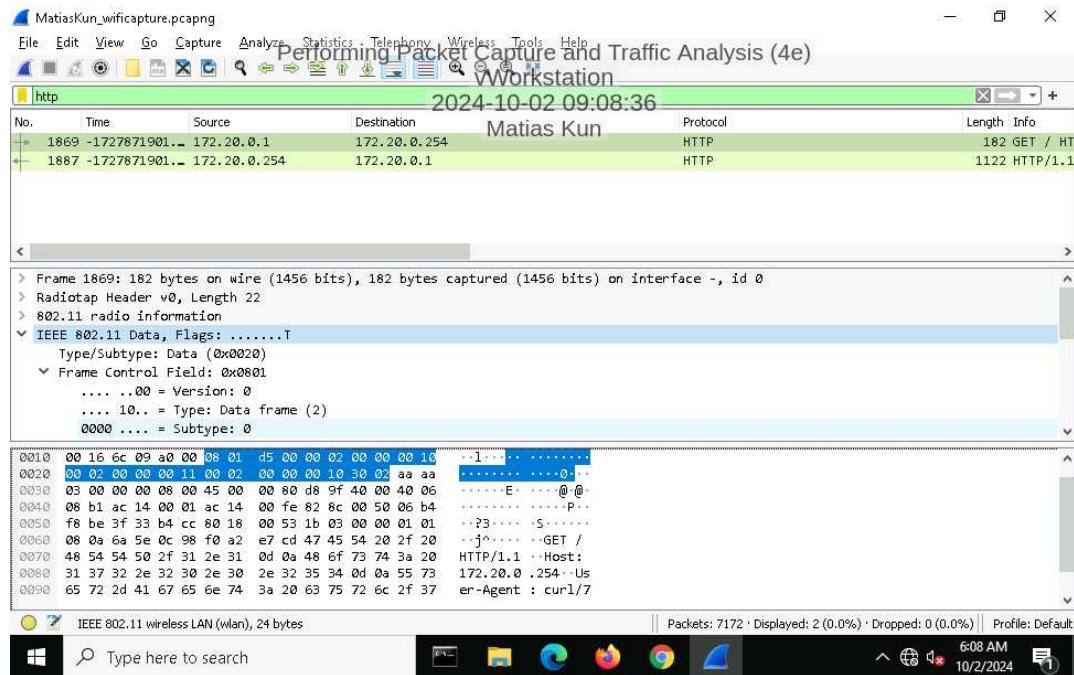
5. Make a screen capture showing the SSID and channel in the Packet Details pane.



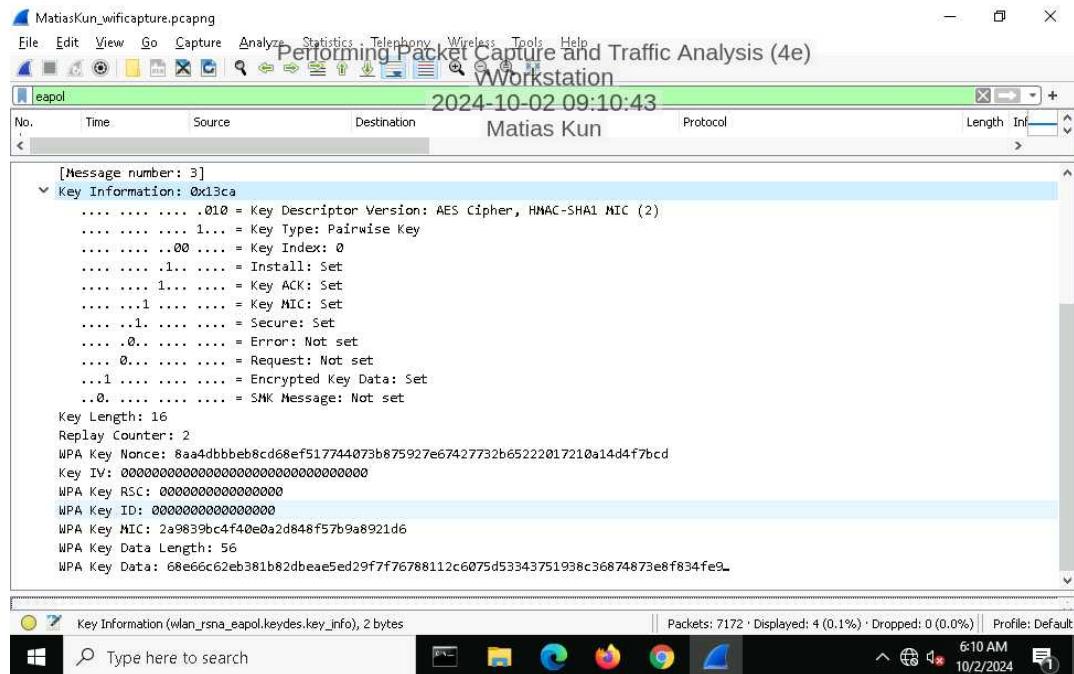
11. Make a screen capture showing the Packet Details for the ICMP packet.



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.



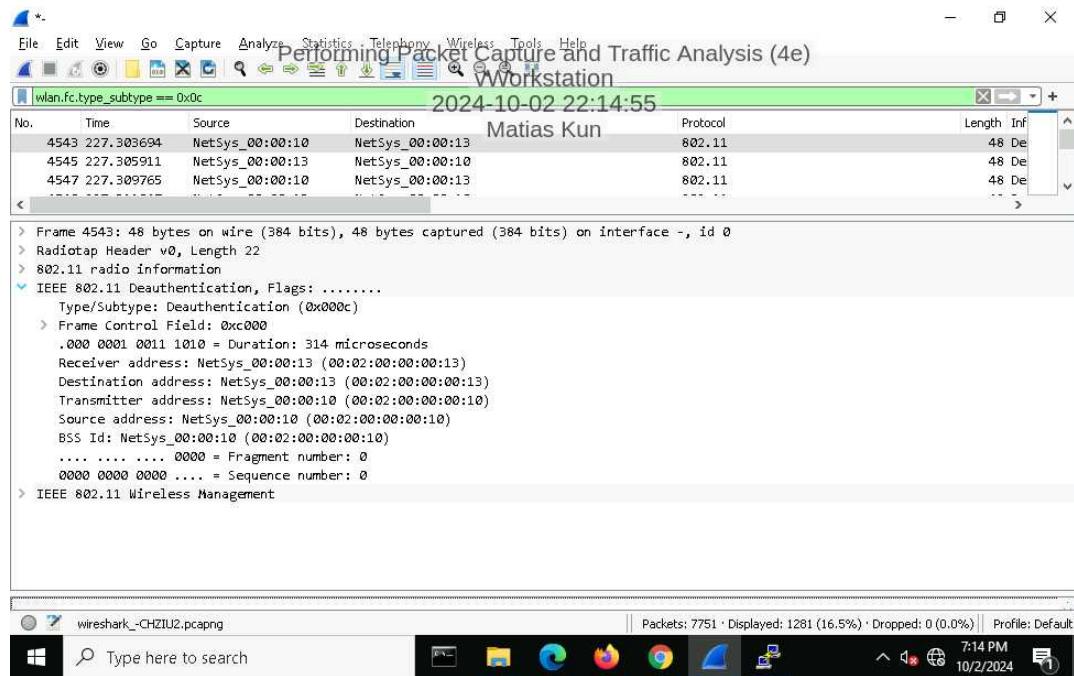
The screenshot shows a terminal window titled "root@sta1:/". The window displays the output of the `aireplay-ng --deauth` command. The command issued was `aireplay-ng --deauth 10 -a 00:02:00:00:00:10 -c 00:02:00:00:00:13 sta1-wlan0`. The output shows the process of sending directed DeAuth frames (code 7) to the target station `00:02:00:00:00:10` on channel 1. The log includes details like ACKs and ACKs received. The terminal window also shows the user's path as `(root@sta1:~)`.

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.

