

Student:Patrick Kierzkowski

Email:pxk405@francis.edu

Time on Task:11 hours, 33 minutes

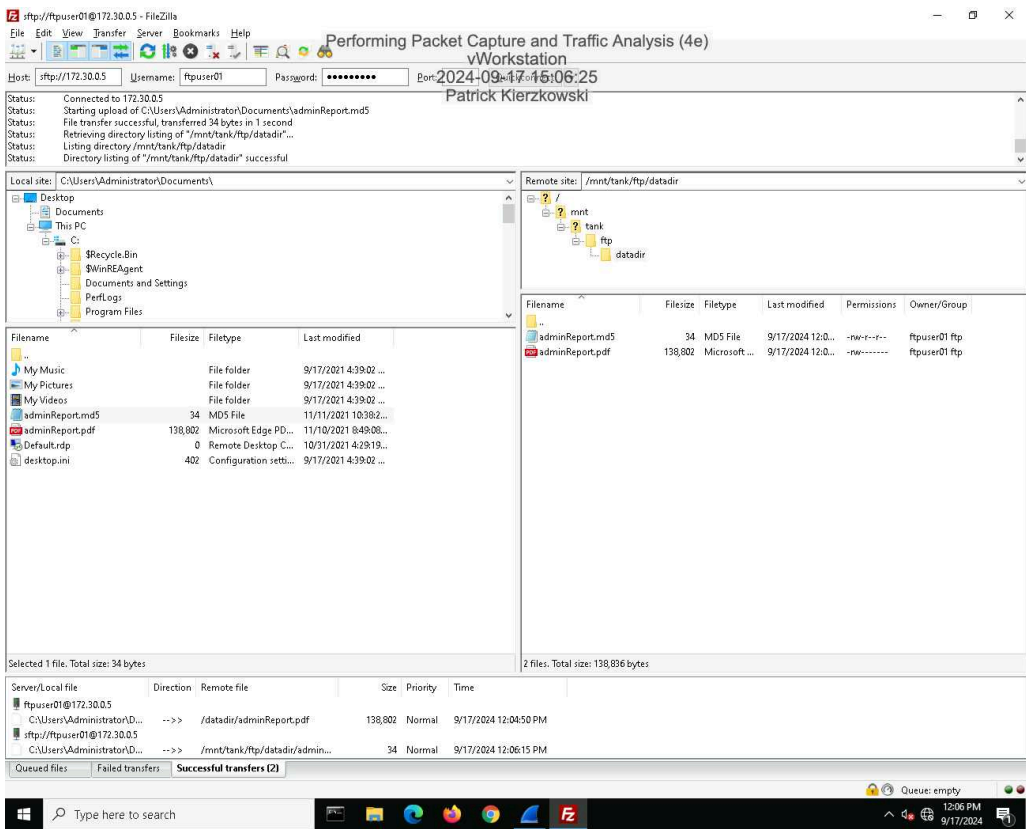
Progress:100%

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

Section 1: Hands-On Demonstration

Part 1: Configure Wireshark and Generate Network Traffic

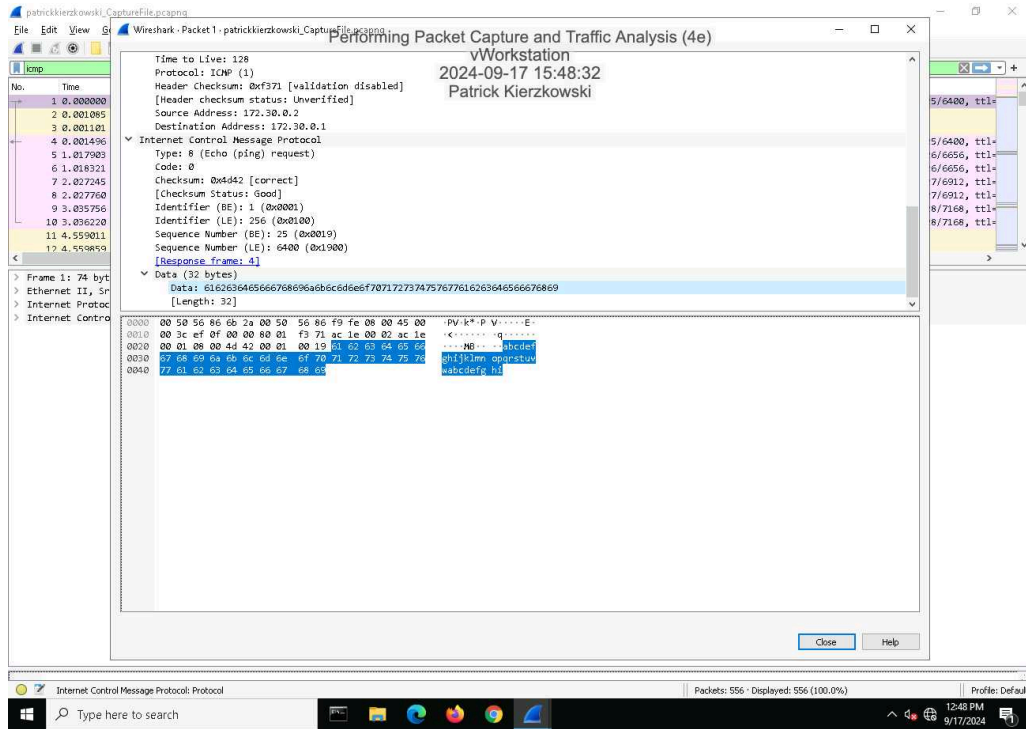
29. Make a screen capture showing the successful FTP and SFTP file transfers.



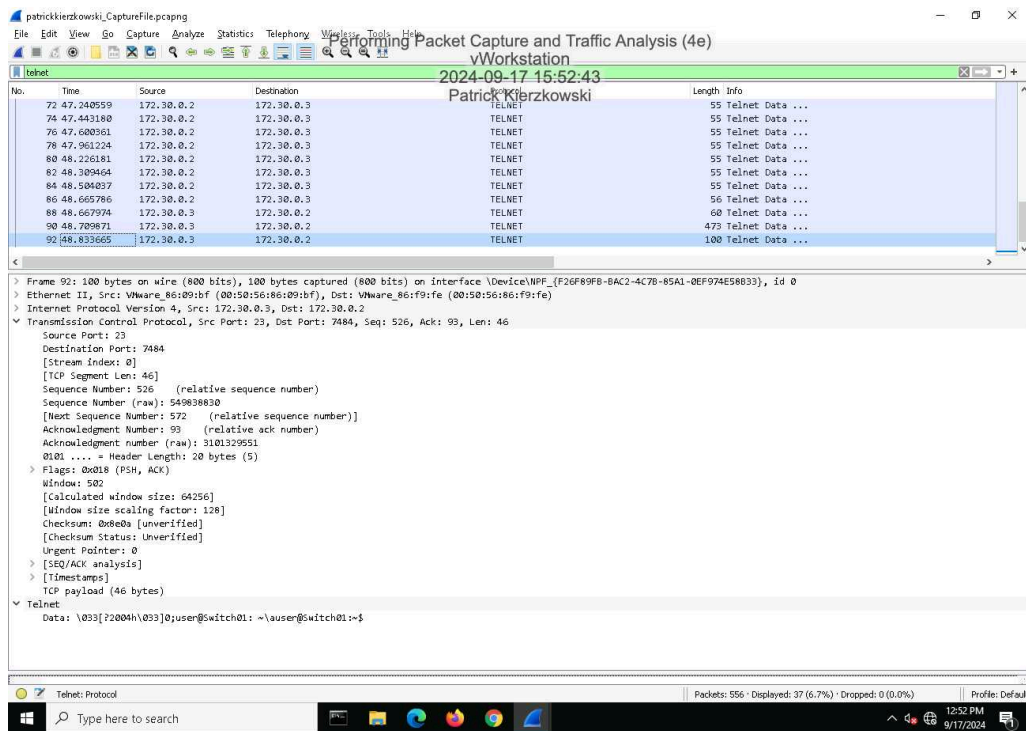
Part 2: Analyze Traffic Using Wireshark

## Fundamentals of Information Systems Security, Fourth Edition - Lab 03

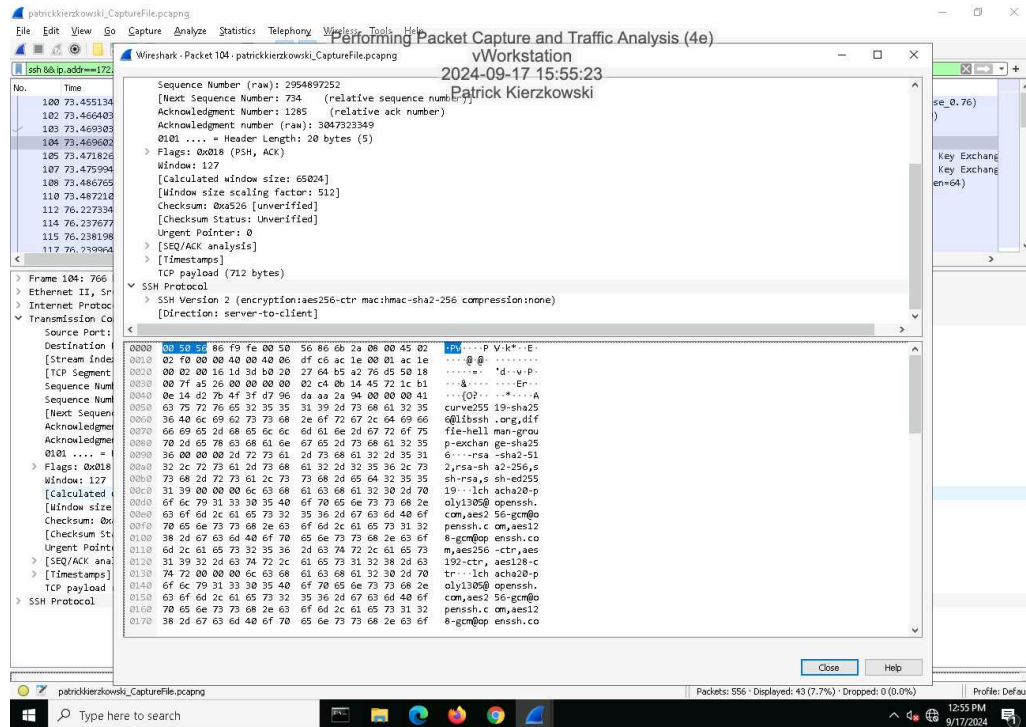
7. **Make a screen capture** showing the **ICMP payload**.



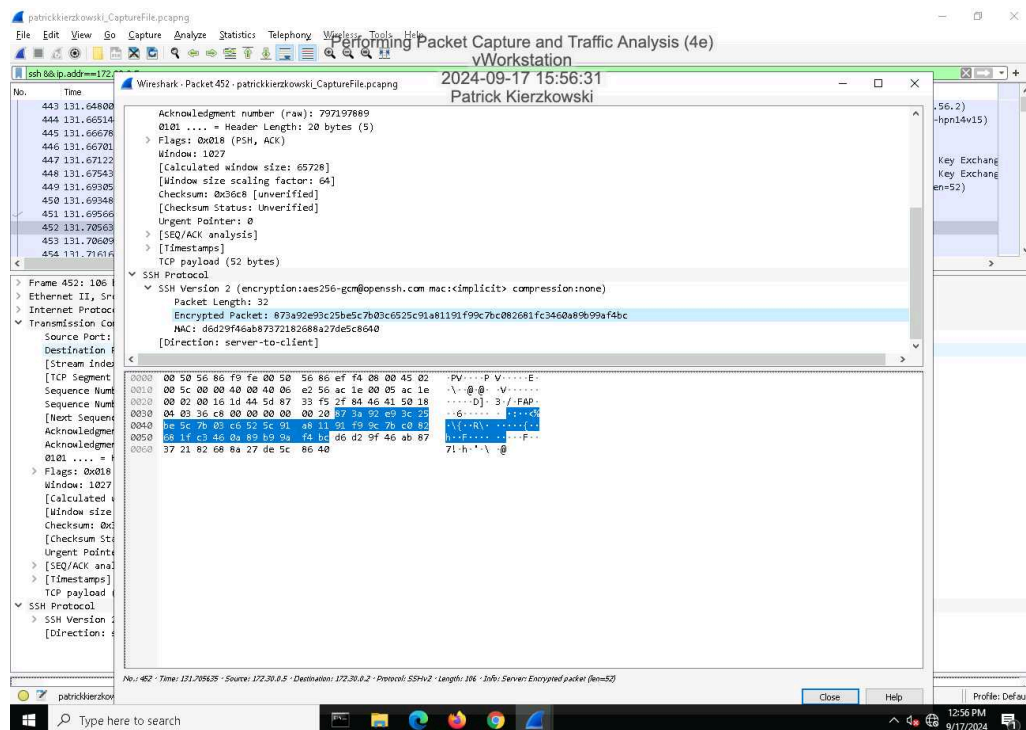
15. **Make a screen capture** showing the ***Last Login:*** information in the **Packet Details** pane.



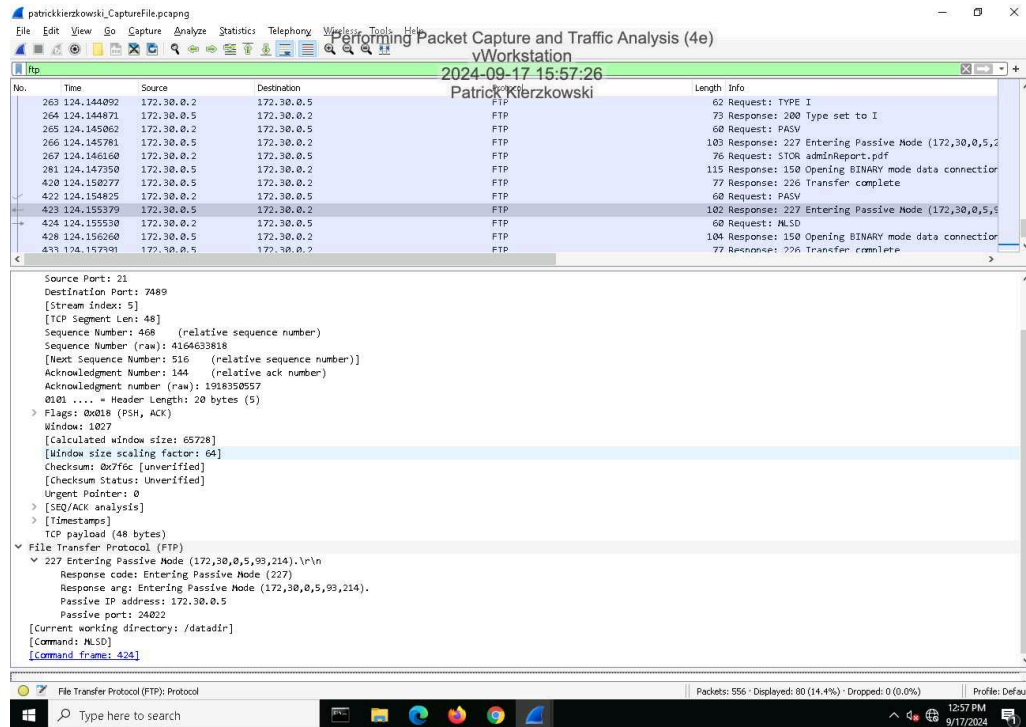
## 21. Make a screen capture showing the SSHv2 encryption and mac selections for the SSH connection.



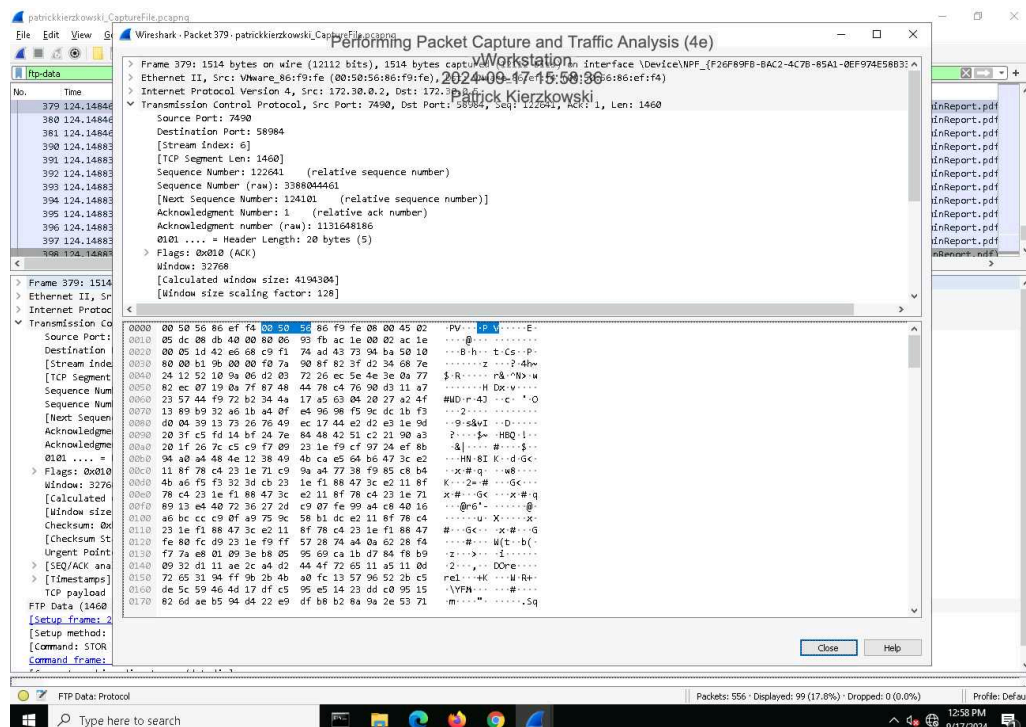
## 26. Make a screen capture showing the highlighted (encrypted) data in the Packet Bytes pane.



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.

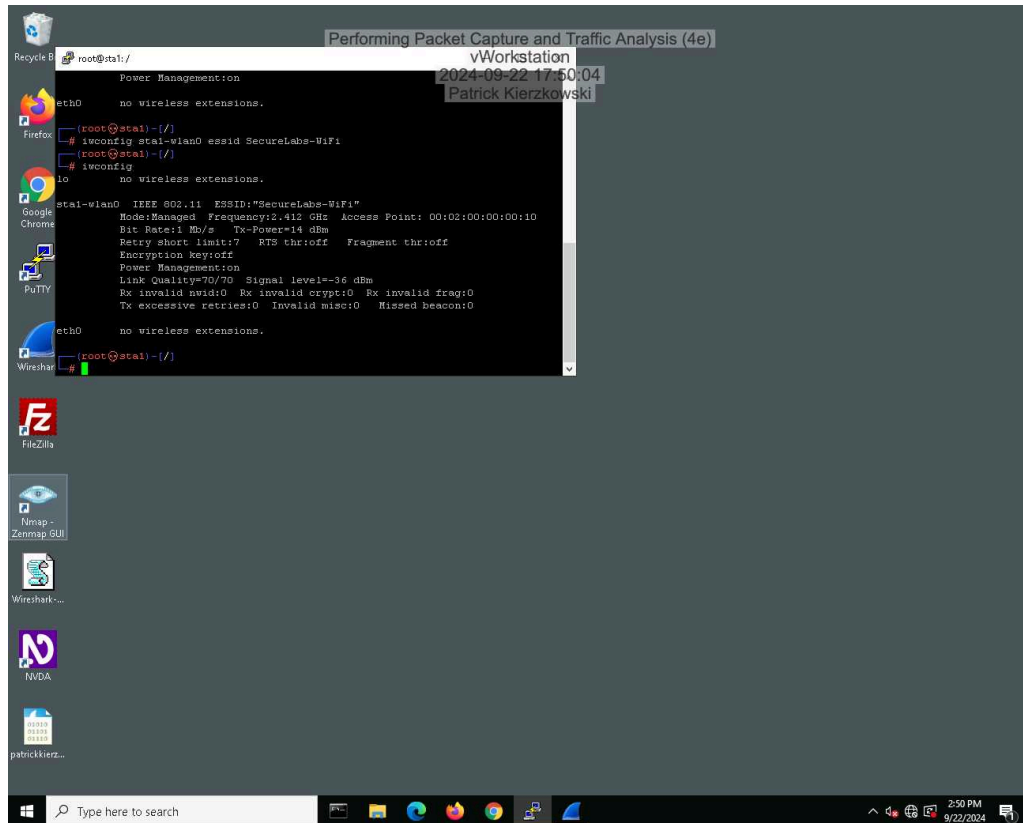




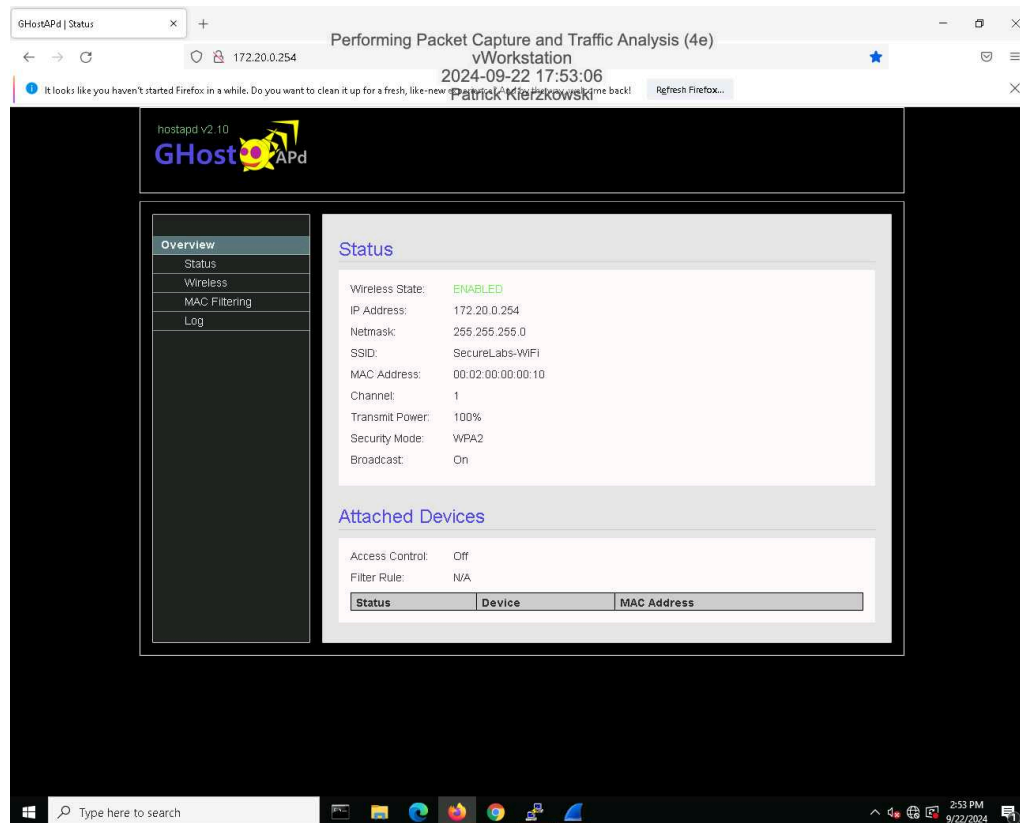
## Section 2: Applied Learning

### Part 1: Configure Wireshark and Generate Network Traffic

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

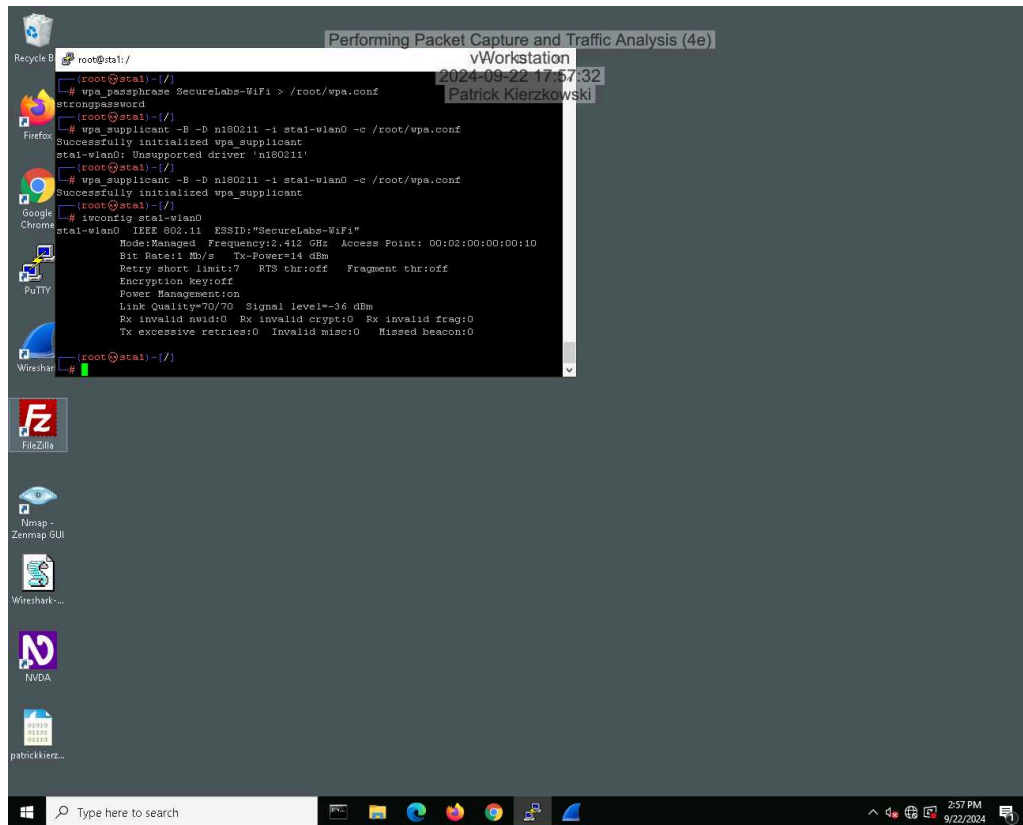


18. Make a screen capture showing the **updated security mode** on the **Status** page.





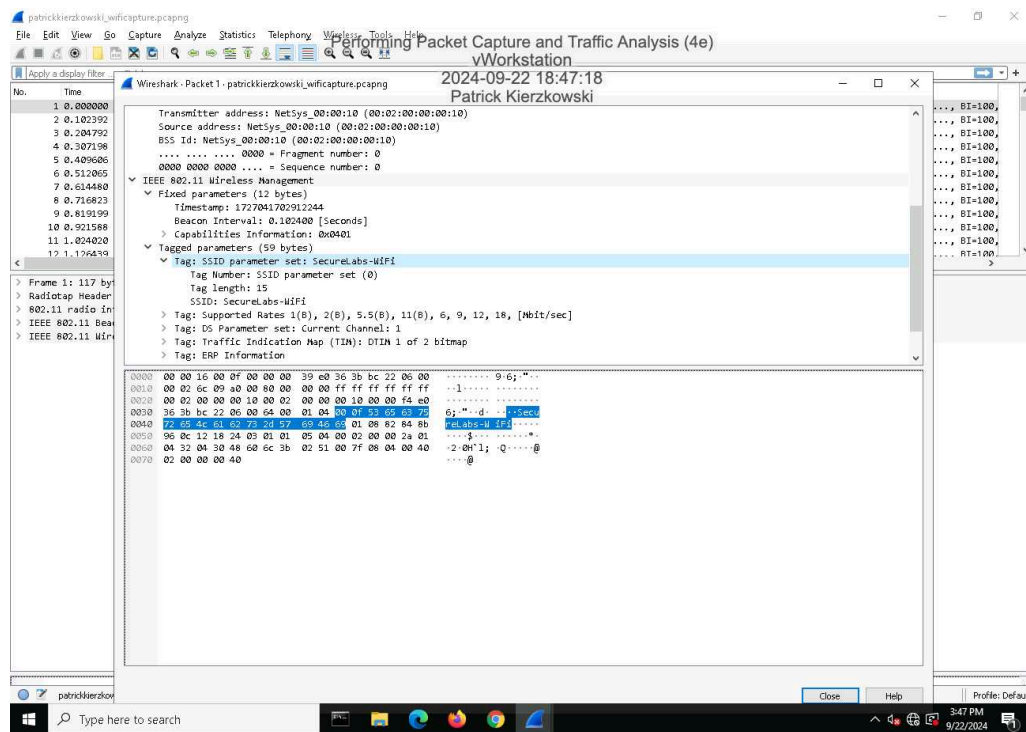
24. Make a screen capture showing the connection to the now-encrypted WLAN.



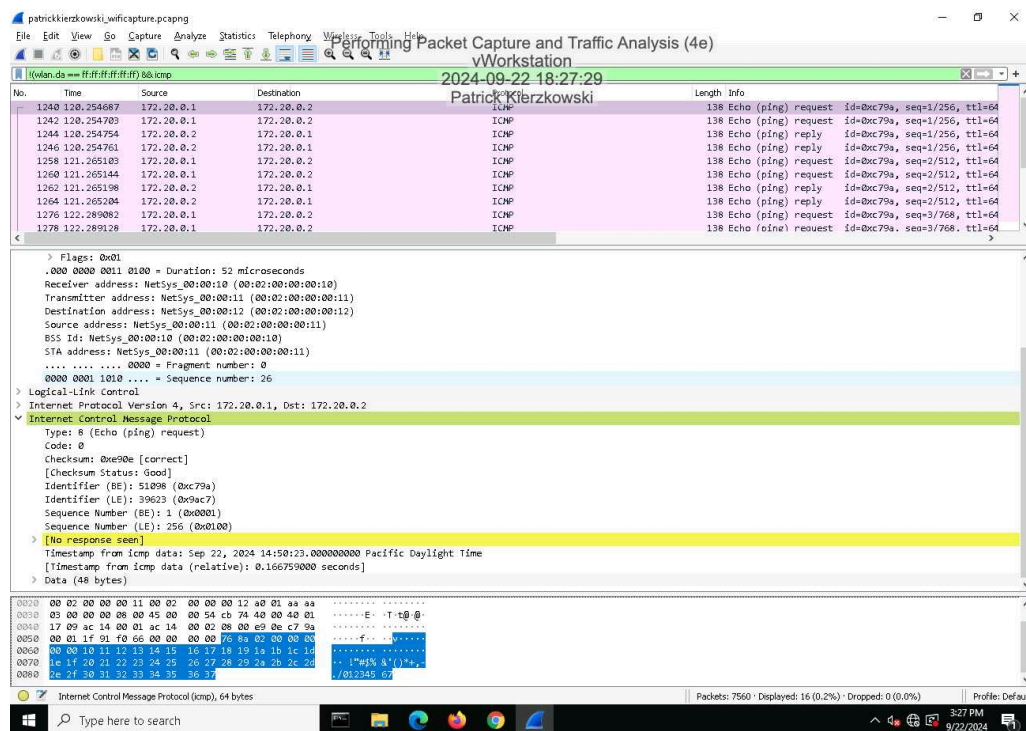
## Part 2: Analyze Traffic Using Wireshark



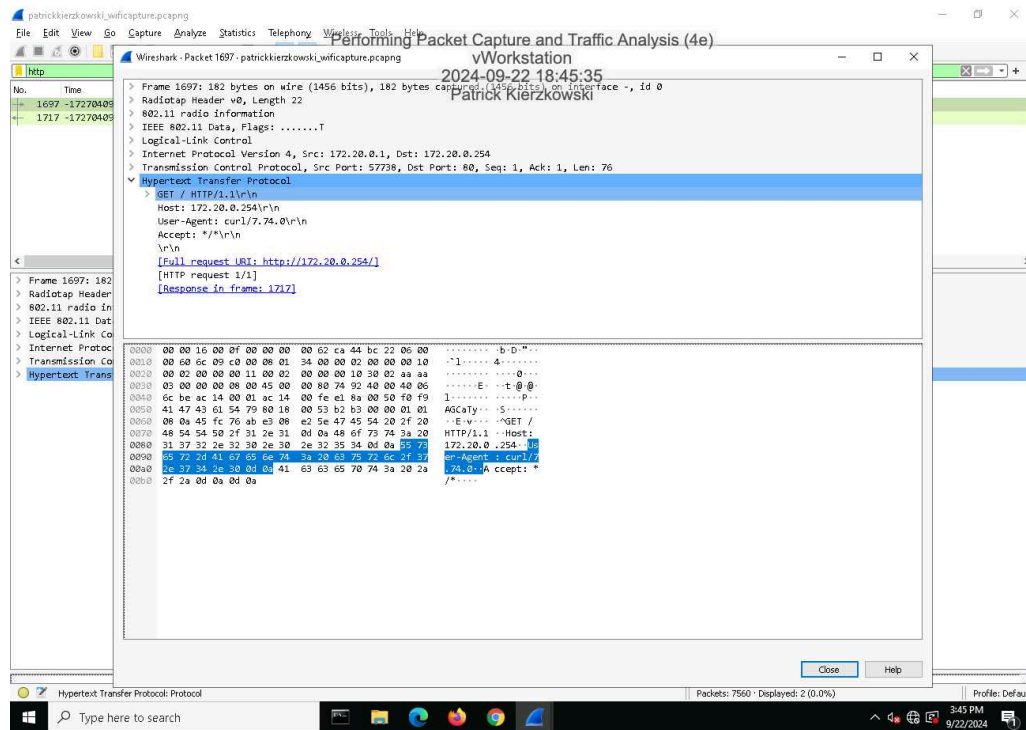
## 5. Make a screen capture showing the SSID and channel in the Packet Details pane.



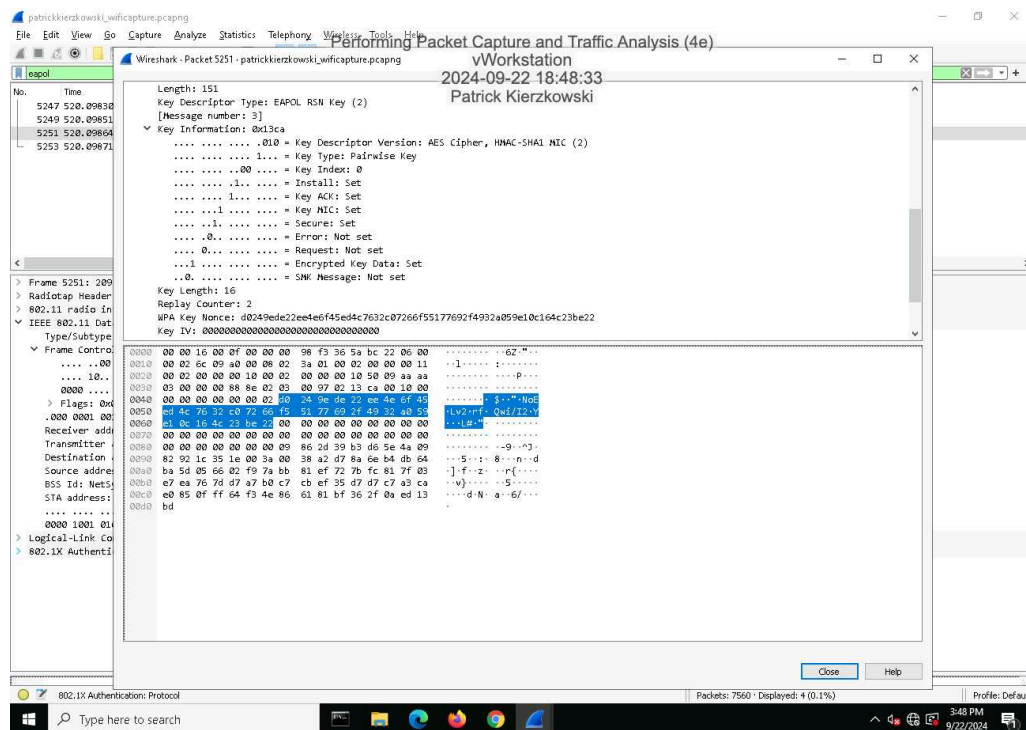
## 11. Make a screen capture showing the Packet Details for the ICMP packet.



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.





## Fundamentals of Information Systems Security, Fourth Edition - Lab 03

The image displays a Wireshark packet capture analysis of IEEE 802.11 wireless LAN traffic. The top pane shows a list of captured packets, with packet 19036 selected. The middle pane shows the packet details, including encapsulation type, arrival time, epoch time, frame number, and frame length. The bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Length	Info
19024	953.733473	NetSys_00:00:10	NetSys_00:00:12	48	Deauthentication, SN=0, FN=0, Flags=.....
19026	953.735662	NetSys_00:00:10	NetSys_00:00:12	48	Deauthentication, SN=1, FN=0, Flags=.....
19028	953.739018	NetSys_00:00:10	NetSys_00:00:12	48	Deauthentication, SN=2, FN=0, Flags=.....
19030	953.741432	NetSys_00:00:10	NetSys_00:00:12	48	Deauthentication, SN=3, FN=0, Flags=.....
19032	953.744736	NetSys_00:00:10	NetSys_00:00:12	48	Deauthentication, SN=4, FN=0, Flags=.....
19034	953.746973	NetSys_00:00:10	NetSys_00:00:10	48	Deauthentication, SN=5, FN=0, Flags=.....
19036	953.750248	NetSys_00:00:12	NetSys_00:00:12	48	Deauthentication, SN=6, FN=0, Flags=.....
19038	953.752424	NetSys_00:00:12	NetSys_00:00:10	48	Deauthentication, SN=7, FN=0, Flags=.....
19042	953.755638	NetSys_00:00:10	NetSys_00:00:12	48	Deauthentication, SN=8, FN=0, Flags=.....
19044	953.757751	NetSys_00:00:12	NetSys_00:00:10	48	Deauthentication, SN=9, FN=0, Flags=.....
19046	953.760927	NetSys_00:00:12	NetSys_00:00:12	48	Deauthentication, SN=10, FN=0, Flags=.....
19048	953.763102	NetSys_00:00:17	NetSys_00:00:10	48	Deauthentication, SN=11, FN=0, Flags=.....

**Packet Details:**

- Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
- Arrival Time: Sep 22, 2024 16:12:19.862323000 Pacific Daylight Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1727046739.862323000 seconds
- [Time delta from previous captured frame: 0.002730000 seconds]
- [Time delta from previous displayed frame: 0.002730000 seconds]
- [Time since reference on first frame: 953.750248000 seconds]
- Frame Number: 19036
- Frame Length: 48 bytes (384 bits)
- Capture Length: 48 bytes (384 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: radiotap;wlan;radio;wlan]
- > Radiotap Header v0, Length 22
- > 802.11 radio information
- > IEEE 802.11 Deauthentication, Flags: .....
- Type/Subtype: Deauthentication (0x000c)
- > Frame control field: 0x0000
  - 0x00 0001 0011 1010 = Duration: 314 microseconds
  - Receiver address: NetSys\_00:00:12 (00:02:00:00:00:12)
  - Destination address: NetSys\_00:00:12 (00:02:00:00:00:12)
  - Transmitter address: NetSys\_00:00:10 (00:02:00:00:00:10)
  - Source address: NetSys\_00:00:10 (00:02:00:00:00:10)
  - BSS Id: NetSys\_00:00:10 (00:02:00:00:00:10)
  - ..... 0000 = Fragment number: 0
  - 0000 0000 0110 .... = Sequence number: 6
- > IEEE 802.11 Wireless Management
- > Fixed parameters (2 bytes)
- Reason code: Class 3 frame received from nonassociated STA (0x0007)

**Raw Data:**

```

IEEE 802.11 wireless LAN (wlan), 24 bytes
Packets: 28130 | Displayed: 2560 (9.1%) | Dropped: 0 (0.0%) | Profile: Default
Type here to search
4:58 PM
9/22/2024

```

The screenshot displays the Wireshark network protocol analyzer interface. The main window is titled "Performing Packet Capture and Traffic Analysis (4e)". The top pane shows a list of 19 packets, all of which are EAPOL Key messages. The bottom pane shows the details of the selected packet (Frame 19), including the Radiotap header, IEEE 802.11 data, and Logical-Link Control. The status bar at the bottom indicates 28130 packets displayed, with 16 (0.1%) dropped.

No.	Time	Source	Destination	Length	Info
19	0.454336	NetSys_00:00:10	NetSys_00:00:12	153	Key (Message 1 of 4)
21	0.454841	NetSys_00:00:12	NetSys_00:00:10	175	Key (Message 2 of 4)
23	0.454900	NetSys_00:00:10	NetSys_00:00:12	209	Key (Message 3 of 4)
25	0.455050	NetSys_00:00:12	NetSys_00:00:10	153	Key (Message 4 of 4)
38	0.457724	NetSys_00:00:10	NetSys_00:00:13	153	Key (Message 1 of 4)
40	0.458136	NetSys_00:00:13	NetSys_00:00:10	175	Key (Message 2 of 4)
42	0.458281	NetSys_00:00:10	NetSys_00:00:13	209	Key (Message 3 of 4)
44	0.458353	NetSys_00:00:13	NetSys_00:00:10	153	Key (Message 4 of 4)
21390	971.665925	NetSys_00:00:10	NetSys_00:00:12	153	Key (Message 1 of 4)
21392	971.666354	NetSys_00:00:12	NetSys_00:00:10	175	Key (Message 2 of 4)
21394	971.666698	NetSys_00:00:10	NetSys_00:00:12	209	Key (Message 3 of 4)
21396	971.666836	NetSys_00:00:12	NetSys_00:00:10	153	Key (Message 4 of 4)

Frame 19: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface -, id 0  
 Radiotap Header v0, Length 22  
 IEEE 802.11 radio information  
 IEEE 802.11 Data, Flags: .....F.  
 Logical-Link Control  
 IEEE 802.1X Authentication

Packets: 28130 · Displayed: 16 (0.1%) · Dropped: 0 (0.0%)

