

Student:

Fernando Parra

Email:

fparra1@msudenve.edu

Time on Task:

4 hours, 20 minutes

Progress:

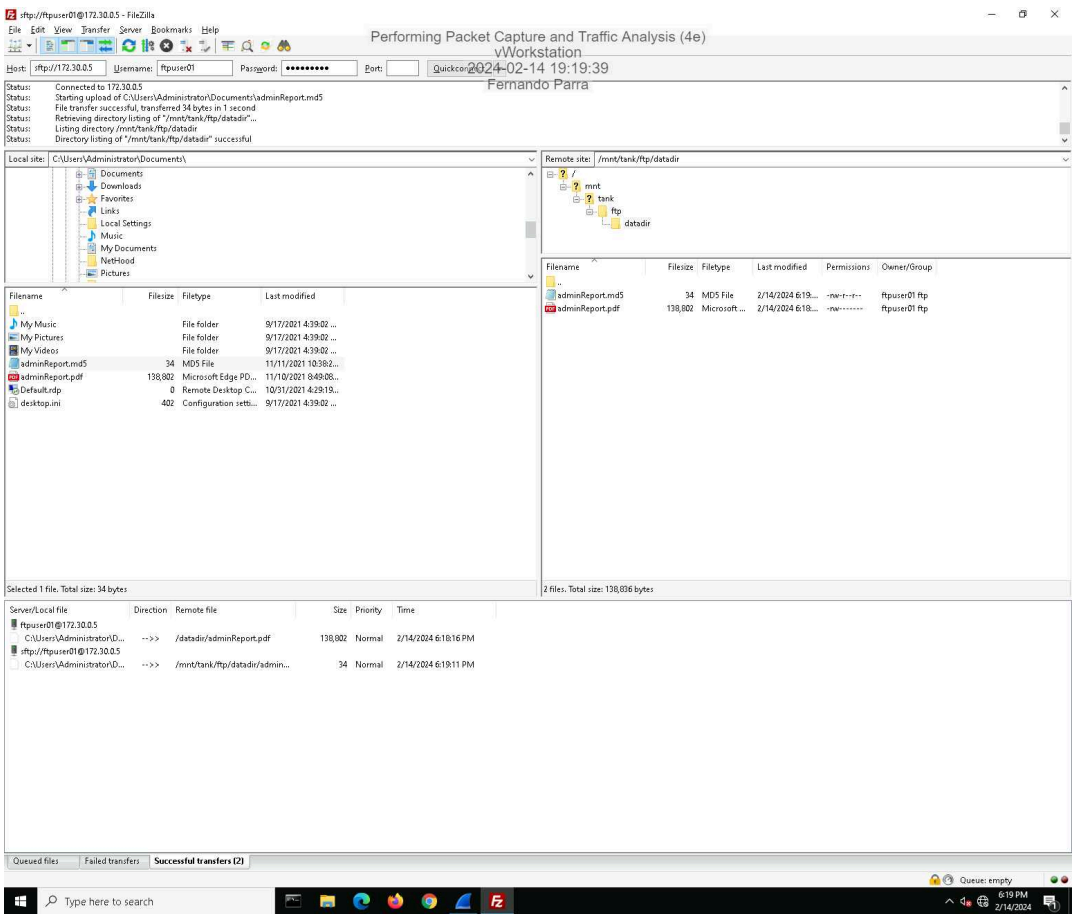
100%

Report Generated: Wednesday, February 21, 2024 at 10:22 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

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

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The title bar reads "Performing Packet Capture and Traffic Analysis (4e)".

The packet list pane shows a list of captured packets. Packet 1 is an ICMP Echo (ping) request from 172.30.0.2 to 172.30.0.1. The packet details pane for packet 1 shows the following information:

- Internet Control Message Protocol
- Type: 8 (echo (ping) request)
- Code: 0
- Checksum: 0x555a [correct]
- [Checksum status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Request frame: 1]
- [Response time: 0.950 ms]

The packet bytes pane shows the raw data of the ICMP Echo request. The data is displayed in hexadecimal and ASCII. The ASCII column shows the following text:

```
PV-X.P.V.v...E-
<g-@:.....
-UD-
ah1Kjmn seqistua
abcdedfg h1
```

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

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The title bar reads "Performing Packet Capture and Traffic Analysis (4e)".

The packet list pane (top) shows a list of captured packets. The selected packet is 101, which is a Telnet packet from 172.30.0.3 to 172.30.0.2. The packet details pane (middle) shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Telnet. The packet bytes pane (bottom) shows the raw data of the selected packet, with the Telnet data field highlighted.

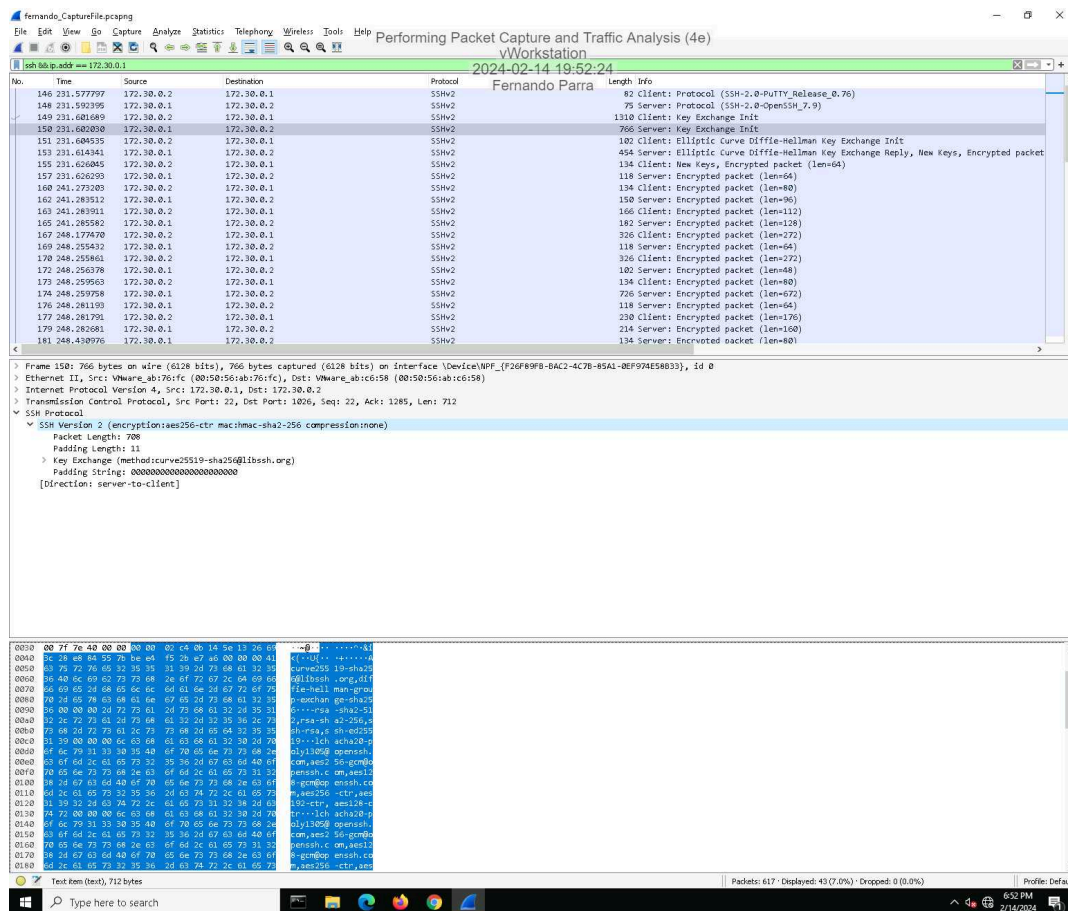
The packet details pane shows the following information:

- Frame 101: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\NPF\_{F26F80FB-BAC2-4C7B-85A1-DEP974E58833}, Id 0
- Ethernet II, Src: VMware\_ahb6:95 (00:50:56:ab:c6:95), Dst: VMware\_ahc6:58 (00:50:56:ab:c6:58)
- Internet Protocol Version 4, Src: 172.30.0.3, Dst: 172.30.0.2
- Transmission Control Protocol, Src Port: 23, Dst Port: 1025, Seq: 526, Ack: 99, Len: 46
- Telnet

The packet bytes pane shows the raw data of the selected packet, with the Telnet data field highlighted. The data is shown in hexadecimal and ASCII format.

## 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.

The screenshot displays the Wireshark interface with a packet capture named 'fermando\_CaptureFile.pcapng'. The main packet list shows an SSH session between 172.30.0.5 and 172.30.0.2. Packet 497 is selected, showing an 'SSH Version 2' packet. The packet details pane shows the 'Encrypted Packet' field with a length of 32 bytes. The packet bytes pane at the bottom shows the raw data of the encrypted packet, which is highlighted in blue. The status bar at the bottom indicates 'Packets: 617 · Displayed: 106 (17.2%) · Dropped: 0 (0.0%)'.

No.	Time	Source	Destination	Protocol	Length	Info
490	469.215606	172.30.0.2	172.30.0.5	SSHv2	80	Client: Protocol (SSH-2.0-FileZilla_3.56.2)
491	469.230785	172.30.0.5	172.30.0.2	SSHv2	84	Server: Protocol (SSH-2.0-OpenSSH_8.4-pnl4v15)
492	469.232083	172.30.0.2	172.30.0.5	SSHv2	1308	Client: Key Exchange Init
493	469.232351	172.30.0.5	172.30.0.2	SSHv2	1102	Server: Key Exchange Init
494	469.235008	172.30.0.2	172.30.0.5	SSHv2	102	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
495	469.239377	172.30.0.5	172.30.0.2	SSHv2	538	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet
496	469.255361	172.30.0.2	172.30.0.5	SSHv2	122	Client: New Keys, Encrypted packet (len=52)
497	469.255751	172.30.0.5	172.30.0.2	SSHv2	106	Server: Encrypted packet (len=52)
498	469.257848	172.30.0.2	172.30.0.5	SSHv2	122	Client: Encrypted packet (len=68)
499	469.267813	172.30.0.5	172.30.0.2	SSHv2	100	Server: Encrypted packet (len=52)
500	469.268212	172.30.0.2	172.30.0.5	SSHv2	302	Client: Encrypted packet (len=248)
501	469.278314	172.30.0.5	172.30.0.2	SSHv2	90	Server: Encrypted packet (len=36)
502	469.279229	172.30.0.2	172.30.0.5	SSHv2	100	Client: Encrypted packet (len=52)
503	469.281161	172.30.0.5	172.30.0.2	SSHv2	682	Server: Encrypted packet (len=628)
505	469.295133	172.30.0.5	172.30.0.2	SSHv2	106	Server: Encrypted packet (len=52)
506	469.295590	172.30.0.2	172.30.0.5	SSHv2	190	Client: Encrypted packet (len=136)
507	469.296357	172.30.0.5	172.30.0.2	SSHv2	126	Server: Encrypted packet (len=72)
508	469.297217	172.30.0.2	172.30.0.5	SSHv2	100	Client: Encrypted packet (len=52)
509	469.305878	172.30.0.5	172.30.0.2	SSHv2	250	Server: Encrypted packet (len=196)
510	469.306226	172.30.0.2	172.30.0.5	SSHv2	100	Client: Encrypted packet (len=52)
511	469.306469	172.30.0.5	172.30.0.2	SSHv2	154	Server: Encrypted packet (len=100)
512	469.308447	172.30.0.2	172.30.0.5	SSHv2	122	Client: Encrypted packet (len=68)

Frame 497: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF\_{F26F89FB-BAC2-4C7B-85A1-DEFA94E58B33}, id 0

Ethernet II, Src: VMware, ab:13:2a:00:50:56:ab:13:2a, Dst: VMware, ab:c6:58:00:50:56:ab:c6:58

Internet Protocol Version 4, Src: 172.30.0.5, Dst: 172.30.0.2

Transmission Control Protocol, Src Port: 22, Dst Port: 1033, Seq: 1563, Ack: 1487, Len: 52

SSH Protocol

SSH Version 2 (encryption=aes256-gcm@openssh.com mac=implicit compression=none)

Packet Length: 32

Encrypted Packet: 40b9e0d96e551e217e71b2407238409f2200930c3075a6981a33a4c715c8733

MAC: ebc3d97e427957597c14d990bb994faa

[Direction: server-to-client]

0000 00 50 56 ab c6 58 00 50 56 ab 13 2a 00 00 45 02 PV X P V . . . E .

0010 00 5c 00 00 40 40 00 05 e2 56 ac 1e 00 05 ac 1e \ . @ . V . . . . .

0020 00 02 00 16 04 09 98 47 af 7d ce 1a e6 46 50 18 . . . . . G . . . . .

0030 01 03 4b 7b 00 00 00 00 20 40 47 40 70 70 70 . . . . .

0040 23 6c 17 67 1b 58 97 33 b4 00 42 50 00 39 03 07 . . . . .

0050 28 68 81 15 76 4c 71 5c 07 33 eb c3 09 7e 42 73 . . . . .

0060 57 59 7c 14 d9 90 bb 99 4f aa . . . . .

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

The screenshot shows a Wireshark packet capture of an FTP session. The top pane displays a list of packets, with packet 258 selected. The middle pane shows the details of this packet, which is an FTP response (227) indicating the server is entering passive mode. The response code is '227', the response arg is 'Entering Passive Mode (172,30,0,5,98,163)', and the passive IP address is 172.30.0.5. The bottom pane shows the raw packet data in hexadecimal and ASCII, with the response code '227' and the response arg 'Entering Passive Mode' highlighted.

fermando.CaptureFile.pcapng

Performing Packet Capture and Traffic Analysis (4e)

vWorkstation

2024-02-14 20:04:30

Fernando Parra

No.	Time	Source	Destination	Protocol	Length	Info
240	377.854186	172.30.0.5	172.30.0.2	FTP	61	Response: NFMT
241	377.854186	172.30.0.5	172.30.0.2	FTP	163	Response: NLST modify*perm*size*type*unique*UNIX.group*UNIX.m
242	377.854186	172.30.0.5	172.30.0.2	FTP	68	Response: REST STREAM
243	377.854186	172.30.0.5	172.30.0.2	FTP	61	Response: SIZE
245	377.854389	172.30.0.5	172.30.0.2	FTP	61	Response: TVPS
246	377.854389	172.30.0.5	172.30.0.2	FTP	61	Response: UTF8
247	377.854389	172.30.0.5	172.30.0.2	FTP	63	Response: 211 End
249	377.854590	172.30.0.2	172.30.0.5	FTP	70	Request: CLNT FileZilla
250	377.854877	172.30.0.5	172.30.0.2	FTP	62	Response: 200 OK
251	377.854979	172.30.0.2	172.30.0.5	FTP	60	Request: OPTS UTF8 ON
252	377.855259	172.30.0.5	172.30.0.2	FTP	74	Response: 200 UTF8 set to on
253	377.855969	172.30.0.2	172.30.0.5	FTP	59	Request: PWD
254	377.856240	172.30.0.5	172.30.0.2	FTP	88	Response: 257 "/" is the current directory
255	377.857755	172.30.0.2	172.30.0.5	FTP	62	Request: TYPE I
256	377.858124	172.30.0.5	172.30.0.2	FTP	73	Response: 200 Type set to I
257	377.858262	172.30.0.2	172.30.0.5	FTP	60	Request: PASV
258	377.858585	172.30.0.5	172.30.0.2	FTP	102	Response: 227 Entering Passive Mode (172,30,0,5,98,163).
259	377.864254	172.30.0.2	172.30.0.5	FTP	60	Request: NLSD
263	377.865204	172.30.0.2	172.30.0.2	FTP	104	Response: 150 Opening BINARY mode data connection for NLSD
268	377.866130	172.30.0.5	172.30.0.2	FTP	77	Response: 226 Transfer complete
270	481.828248	172.30.0.2	172.30.0.5	FTP	67	Request: CWD detailir
271	481.840257	172.30.0.5	172.30.0.2	FTP	82	Response: 250 CWD command successful

Frame 258: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF\_{F26F89F8-BAC2-4C7B-85A1-DEFA94E58B33}, id 0

Ethernet II, Src: VMware\_abi13:2a (00:50:56:ab:c6:15), Dst: VMware\_abic6:58 (00:50:56:ab:c6:58)

Internet Protocol Version 4, Src: 172.30.0.5, Dst: 172.30.0.2

Transmission Control Protocol, Src Port: 21, Dst Port: 1027, Seq: 752, Ack: 114, Len: 48

File Transfer Protocol (FTP)

227 Entering Passive Mode (172,30,0,5,98,163).\r\n

Response code: Entering Passive Mode (227)

Response arg: Entering Passive Mode (172,30,0,5,98,163).

Passive IP address: 172.30.0.5

Passive port: 25951

[Current working directory: /]

[Command: NLSD]

[Command frame: 259]

0000 00 50 56 ab c6 58 00 50 56 ab 13 2a 00 00 05 02 PV X P V : P : E :

0010 00 58 00 00 40 00 40 05 e2 5a ac 1e 00 05 ac 1e X : @ : Z : : : :

0020 00 02 00 15 04 03 dc ba 92 13 eb 09 4a d5 5b 18 : : : : : : : : : : : : : :

0030 04 03 53 15 00 00 00 00 00 00 00 00 00 00 00 : : : : : : : : : : : : : :

0040 54 67 28 58 63 73 73 69 76 05 20 44 6f 54 65 24 ng Passi ve Mode

0050 36 11 32 3c 33 30 2c 30 2c 35 2c 39 38 2c 31 (172,30,0,5,98,1

0060 35 35 25 3c 00 04 55),\r\n

Test Item (text), 48 bytes

Packets: 617 · Displayed: 80 (13.0%) · Dropped: 0 (0.0%)

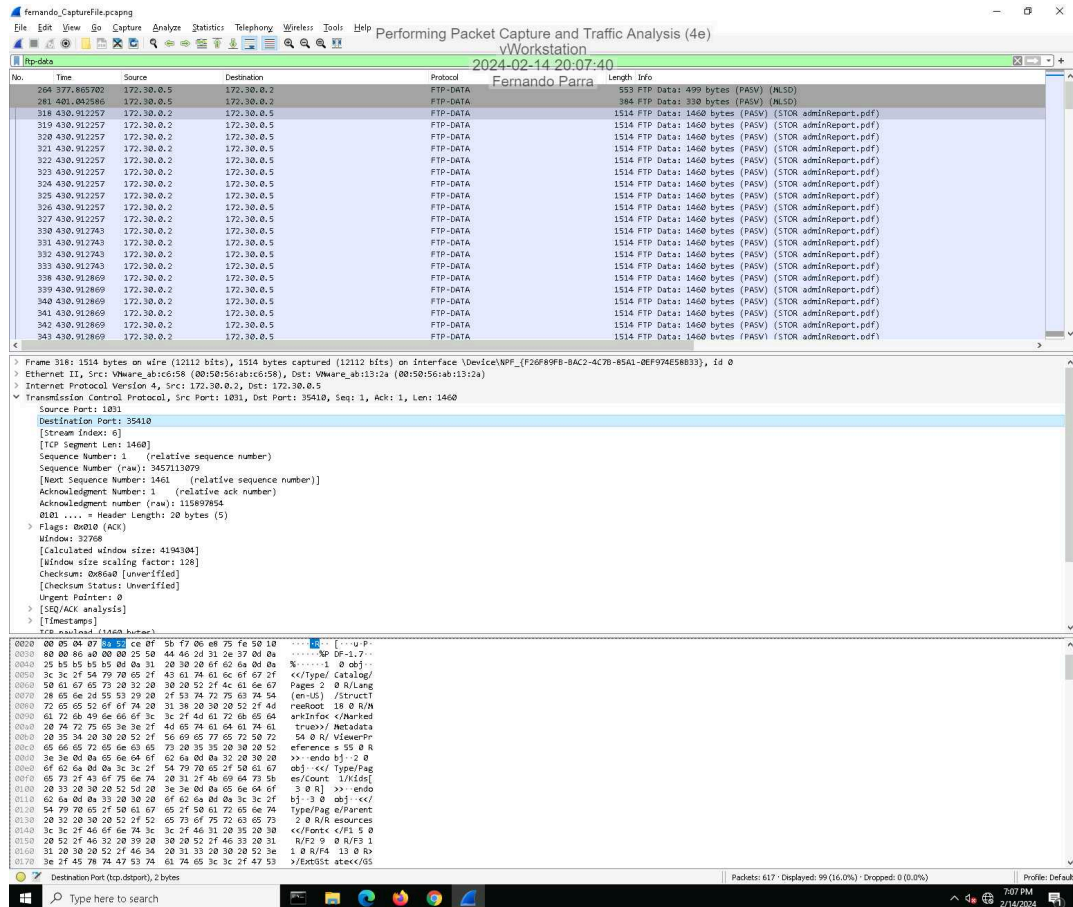
Profile: Default

Type here to search

7:04 PM 2/14/2024

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

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

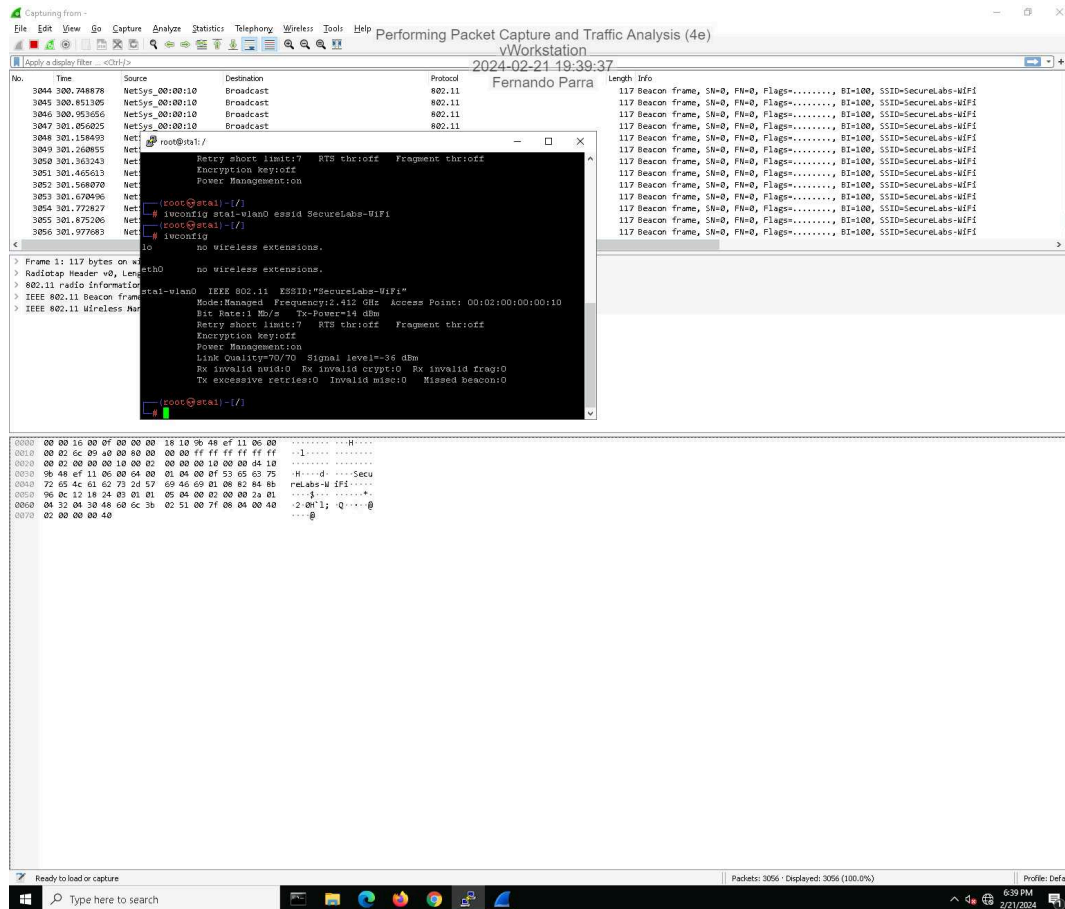




## Section 2: Applied Learning

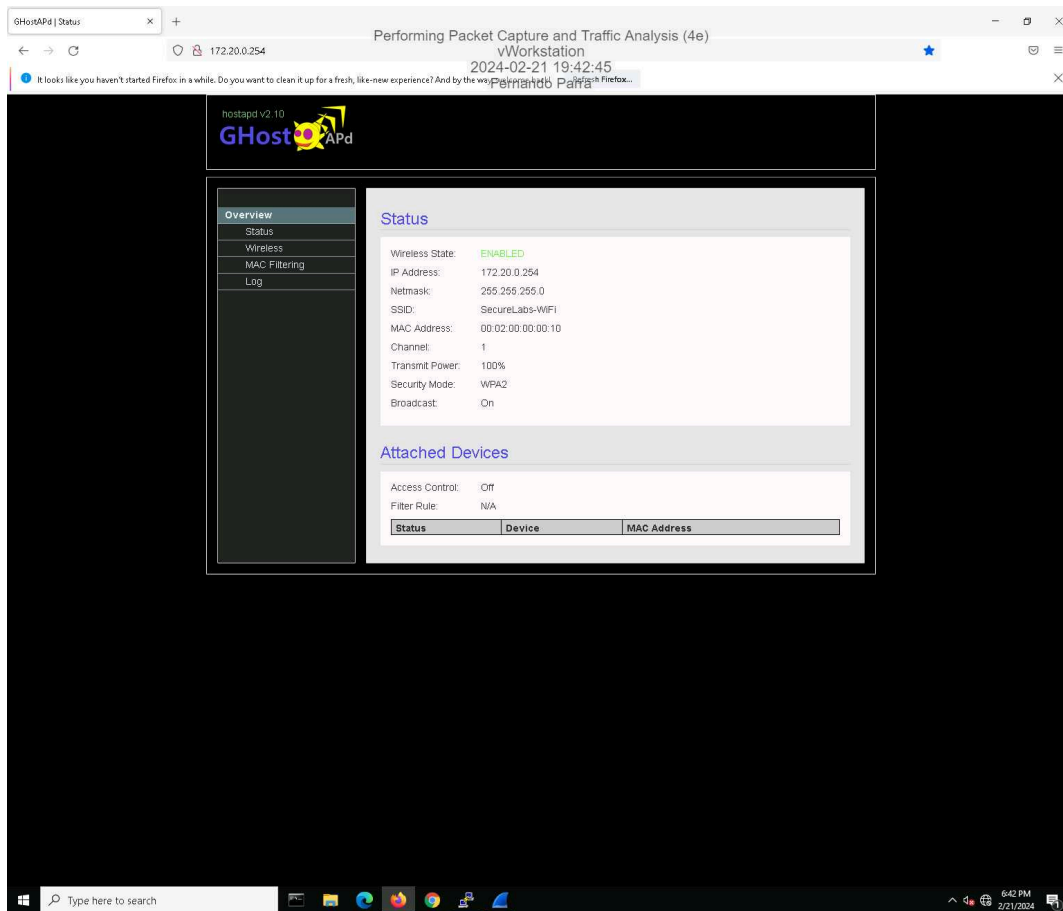
### Part 1: Configure Wireshark and Generate Network Traffic

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

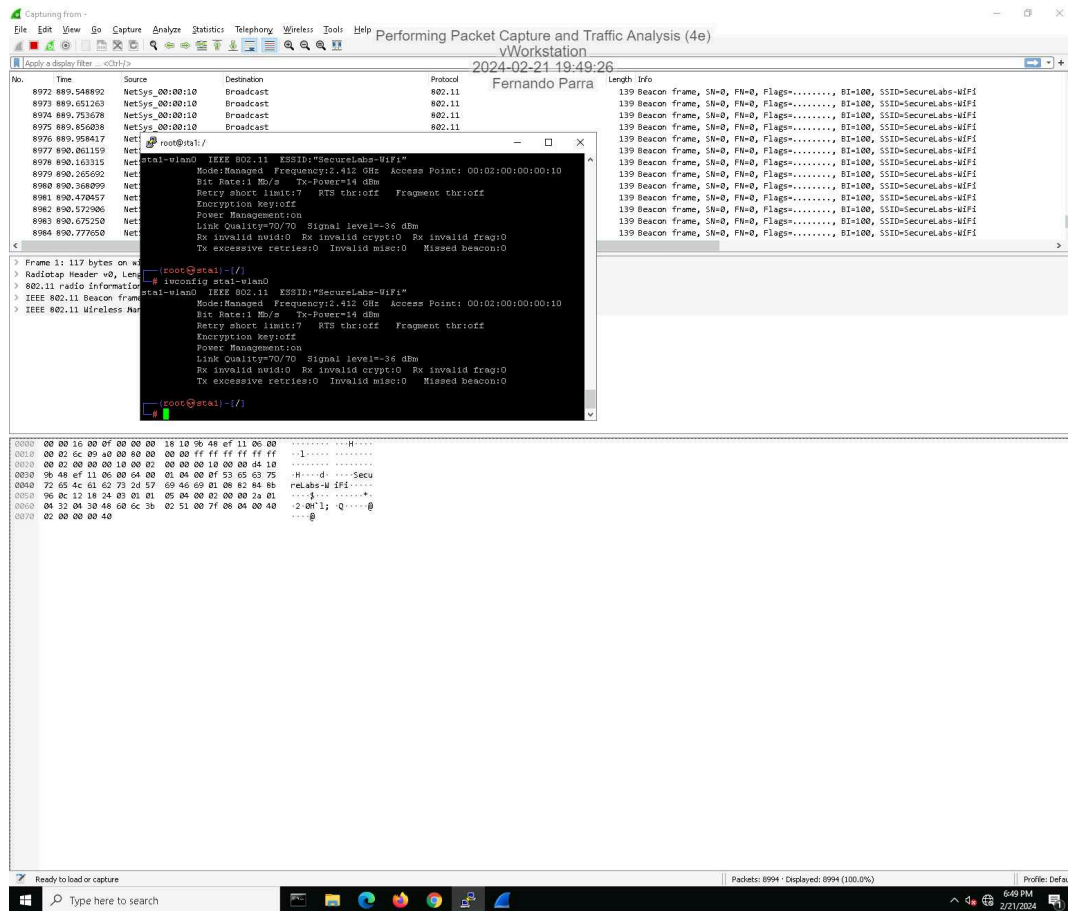




18. Make a screen capture showing the **updated security mode** on the **Status** page.

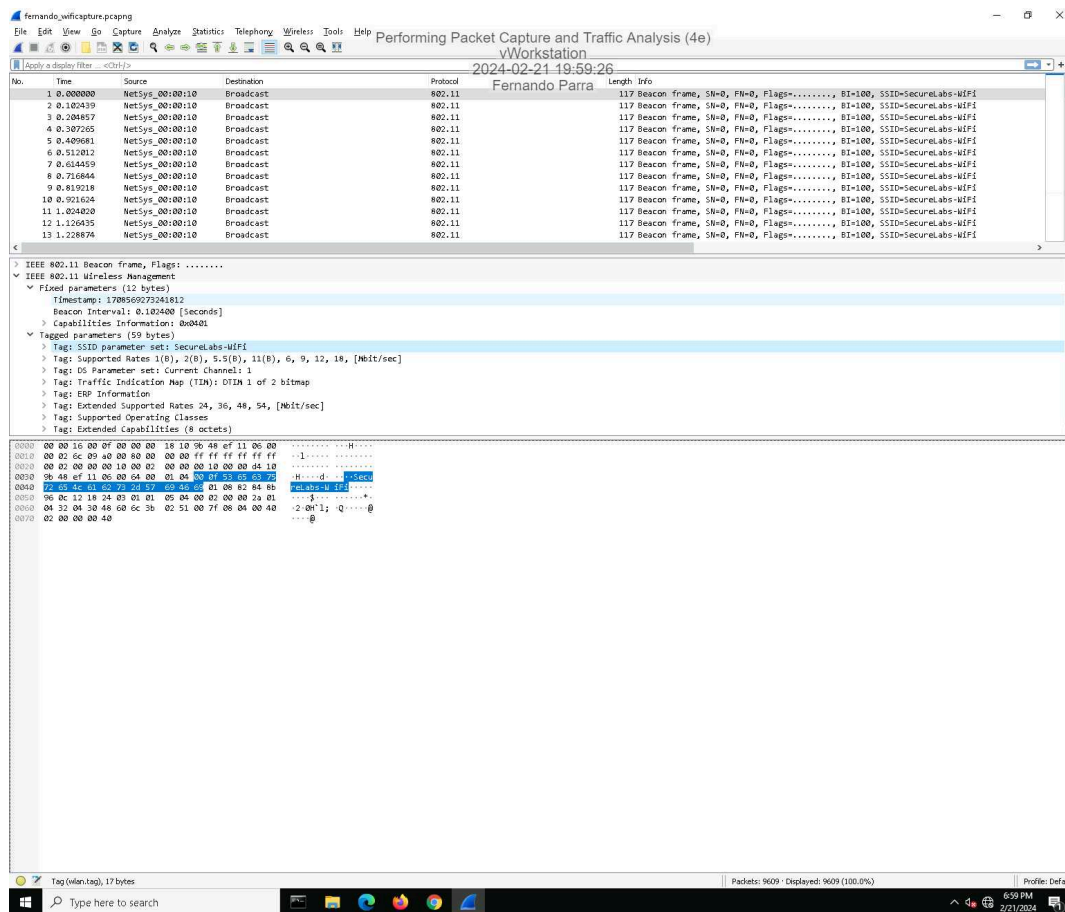


## 24. Make a screen capture showing the connection to the now-encrypted WLAN.



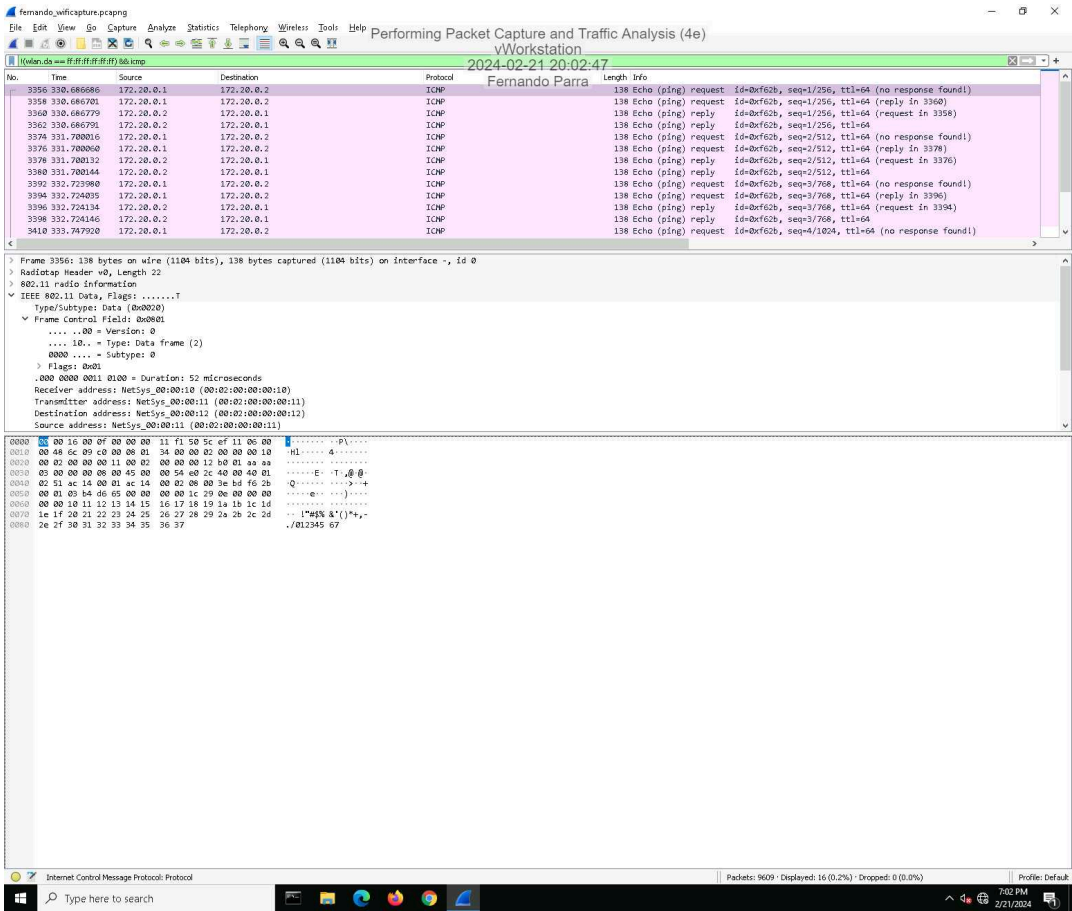
## Part 2: Analyze Traffic Using Wireshark

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

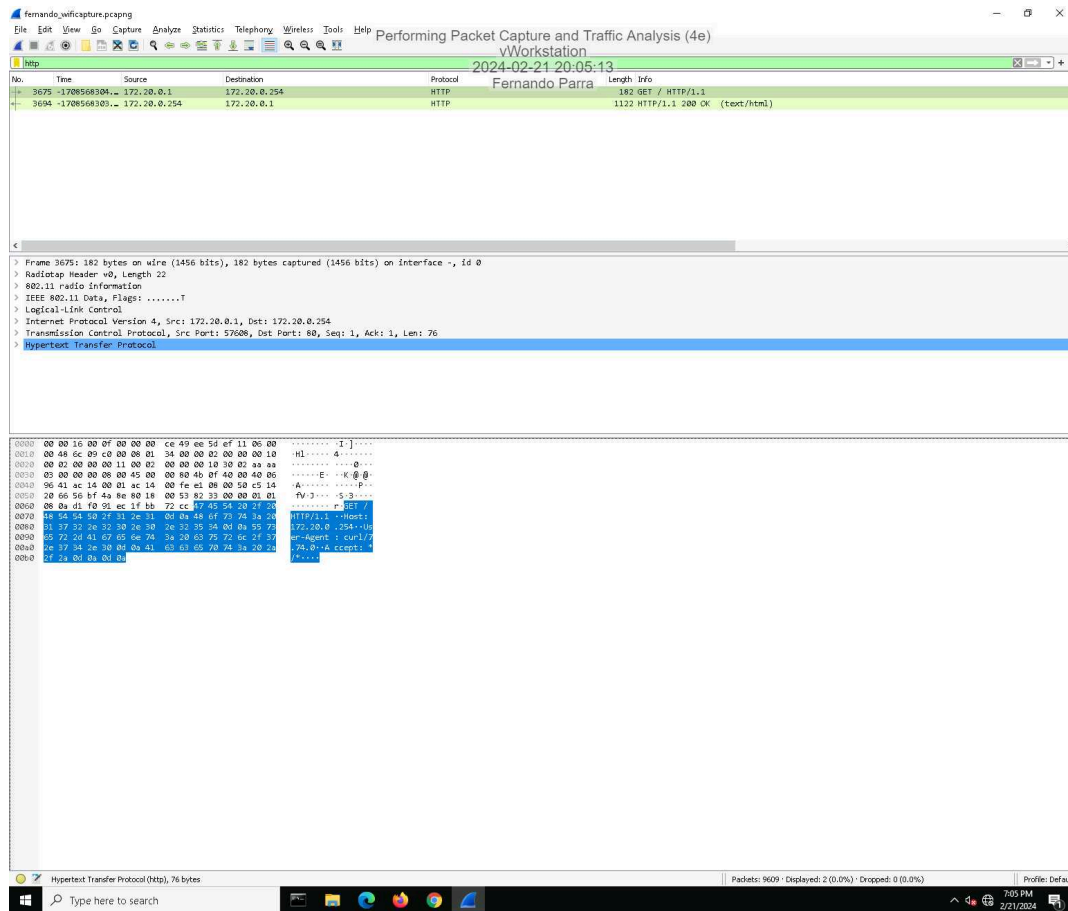


## Fundamentals of Information Systems Security, Fourth Edition - Lab 03

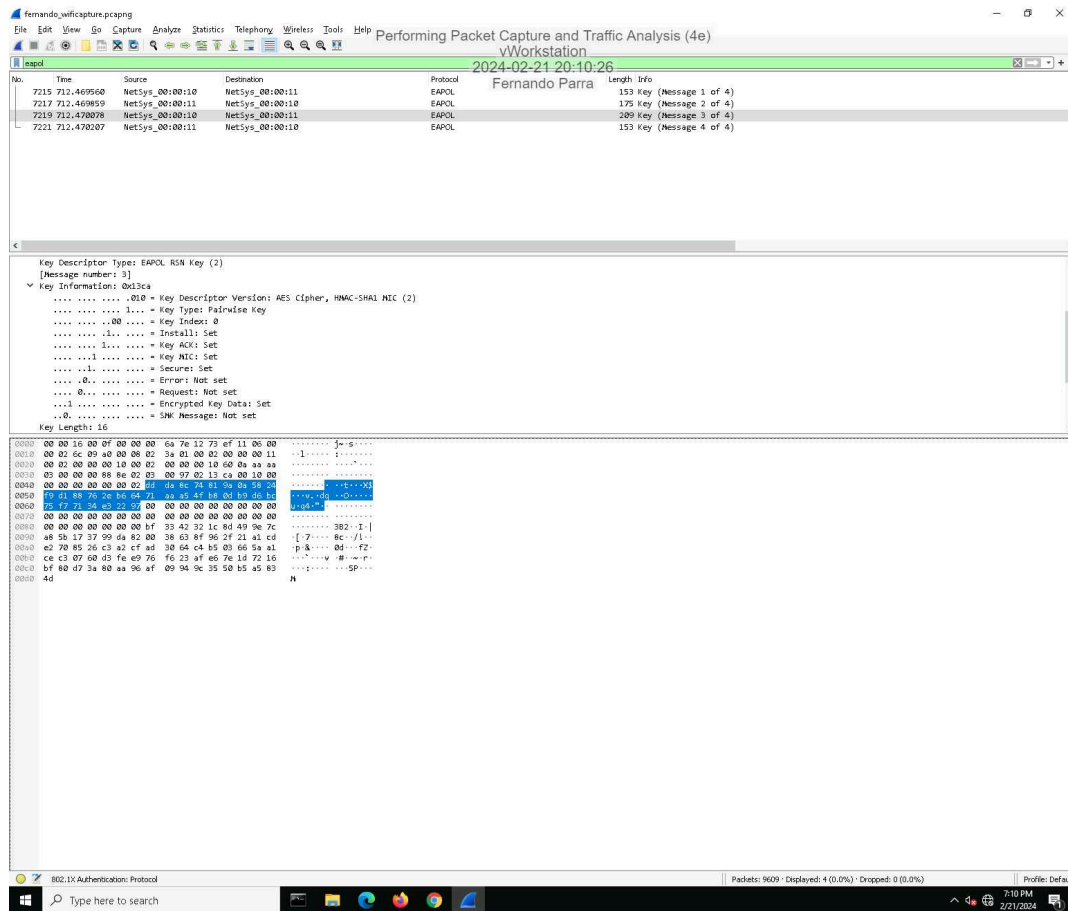
11. **Make a screen capture** showing the **Packet Details for the ICMP packet**.



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



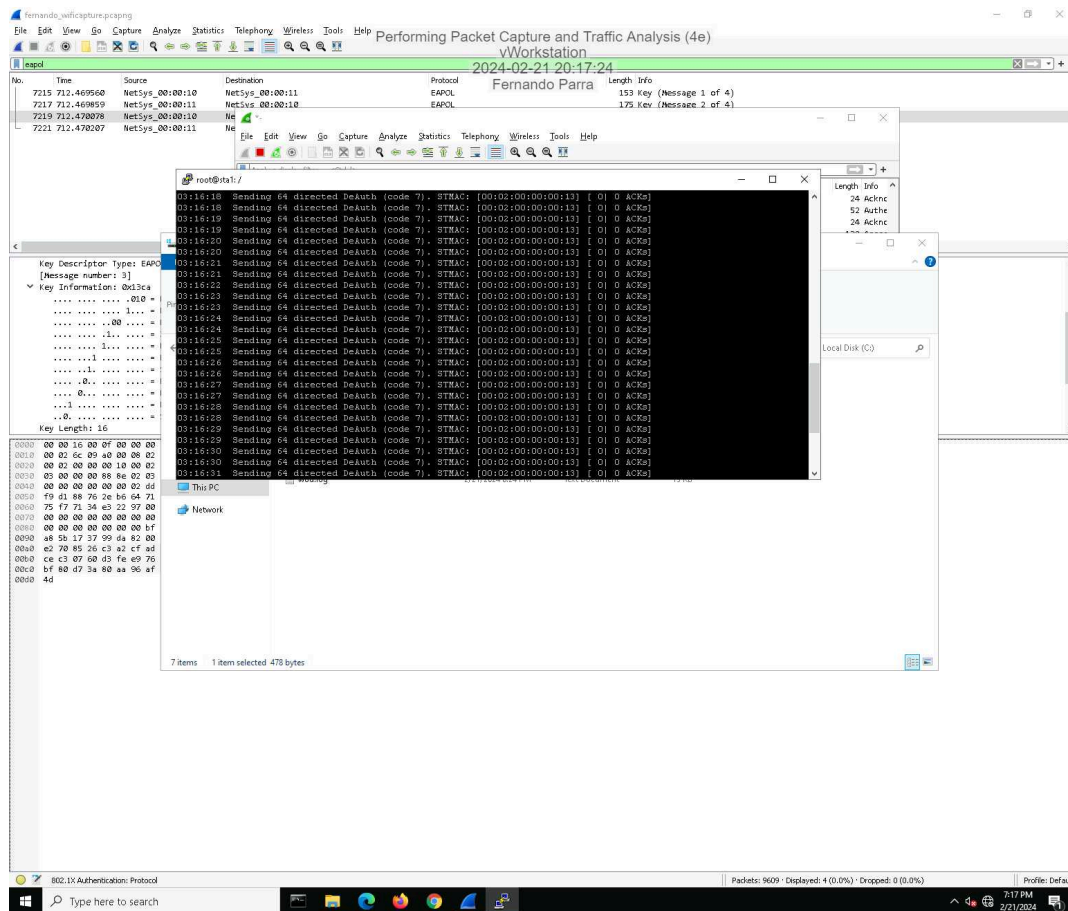
## 18. Make a screen capture showing the key information for Message 3 in the four-way handshake.



## Section 3: Challenge and Analysis

### Part 1: Generate Malicious Network Traffic

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



### 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.

The screenshot shows the Wireshark interface with a packet capture of a deauthentication packet. The packet list on the left shows a deauthentication packet (No. 15072) from NetSys\_00:00:10 to NetSys\_00:00:13. The packet details pane on the right shows the deauthentication packet structure, including the IEEE 802.11 header and the deauthentication frame. The packet bytes pane at the bottom shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
15072	248.865113	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2532, FN=0, Flags=.....
15073	248.867299	NetSys_00:00:13	NetSys_00:00:10	802.11	48	Deauthentication, SN=2533, FN=0, Flags=.....
15074	248.867296	NetSys_00:00:13	NetSys_00:00:13 (00:02:00:00:00:13) (RA)	802.11	24	Acknowledgment, Flags=.....
15075	248.870542	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2534, FN=0, Flags=.....
15076	248.872721	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2535, FN=0, Flags=.....
15078	248.872722	NetSys_00:00:13	NetSys_00:00:13 (00:02:00:00:00:13) (RA)	802.11	24	Acknowledgment, Flags=.....
15079	248.875900	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2536, FN=0, Flags=.....
15079	248.878148	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2537, FN=0, Flags=.....
15080	248.878149	NetSys_00:00:13	NetSys_00:00:13 (00:02:00:00:00:13) (RA)	802.11	24	Acknowledgment, Flags=.....
15081	248.881399	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2538, FN=0, Flags=.....
15082	248.883523	NetSys_00:00:10	NetSys_00:00:10	802.11	48	Deauthentication, SN=2539, FN=0, Flags=.....
15083	248.883525	NetSys_00:00:13	NetSys_00:00:13 (00:02:00:00:00:13) (RA)	802.11	24	Acknowledgment, Flags=.....
15084	248.886785	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2540, FN=0, Flags=.....
15085	248.888941	NetSys_00:00:13	NetSys_00:00:10	802.11	48	Deauthentication, SN=2541, FN=0, Flags=.....
15086	248.888942	NetSys_00:00:13	NetSys_00:00:13 (00:02:00:00:00:13) (RA)	802.11	24	Acknowledgment, Flags=.....
15087	248.892247	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2542, FN=0, Flags=.....
15088	248.894440	NetSys_00:00:13	NetSys_00:00:10	802.11	48	Deauthentication, SN=2543, FN=0, Flags=.....
15089	248.894442	NetSys_00:00:13	NetSys_00:00:13 (00:02:00:00:00:13) (RA)	802.11	24	Acknowledgment, Flags=.....
15090	248.897789	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2544, FN=0, Flags=.....
15091	248.899995	NetSys_00:00:13	NetSys_00:00:10	802.11	48	Deauthentication, SN=2545, FN=0, Flags=.....
15092	248.899998	NetSys_00:00:13	NetSys_00:00:13 (00:02:00:00:00:13) (RA)	802.11	24	Acknowledgment, Flags=.....
15093	248.902182	NetSys_00:00:10	NetSys_00:00:13	802.11	48	Deauthentication, SN=2546, FN=0, Flags=.....
15115	249.931042	NetSys_50:00:3e	NetSys_00:00:13	802.11	105	Probe Response, SN=8, FN=0, Flags=....., B1=100, SSID=Sec3-WiFi
15116	249.931043	NetSys_50:00:3e	NetSys_50:00:13e (00:02:00:50:00:3e) (RA)	802.11	24	Acknowledgment, Flags=.....

Frame 15072: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface -, id 0  
RadioTap Header v0, Length 22  
802.11 radio information  
IEEE 802.11 Deauthentication, Flags: .....

0000 00 00 16 00 0f 00 00 00 6c 52 12 df ef 11 00 00 .....1R.....  
0010 00 02 6c 09 a0 00 c0 00 3a 01 00 02 00 00 00 13 .....:.....  
0020 00 02 00 00 00 10 00 02 00 00 00 10 40 9e 07 00 .....@.....

Wireshark - 15072.pcapng | Packets: 17350 | Displayed: 10261 (59.1%) | Cropped: 0 (0.0%) | Profile: Default

Make a screen capture showing the packets related to the four-way handshake.

The screenshot shows a Wireshark packet capture window titled "Performing Packet Capture and Traffic Analysis (4e)". The capture was taken on the "vWorkstation" interface at 2024-02-21 20:20:18. The packet list shows several EAPOL (Extensible Authentication Protocol over LAN) frames between NetSys\_00:00:110 and NetSys\_00:00:113. The selected packet is frame 11409, which is 153 bytes long and contains a Key (Message 1 of 4). The packet details pane shows the following structure:

- Frame 11409: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface -, id 0
- RadioTap Header v0, Length 22
- 802.11 radio Information
- IEEE 802.11 Data, Flags: .....F.
- Logical-Link Control
- 802.1X Authentication

The packet bytes pane shows the raw data of the selected packet, starting with 0000 00 00 16 00 0f 00 00 00 9f 13 82 de ef 11 00 00.