Performing Packet Capture and Traffic Analysis (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 03

Student:	Email:
Yengkong Sayaovong	ysayaovo@asu.edu

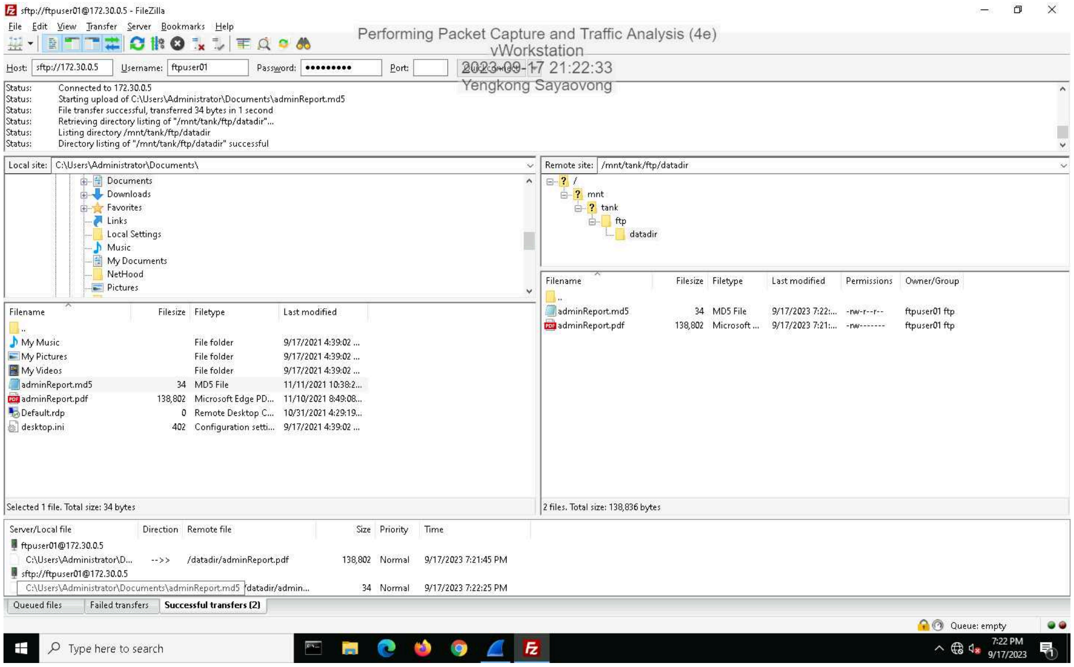
Time on Task:	Progress:
0 hours, 24 minutes	41%

Report Generated: Sunday, September 17, 2023 at 10:39 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**.



sftp://ftpuser01@172.30.0.5 - FileZilla

Performing Packet Capture and Traffic Analysis (4e)
vWorkstation
2023-09-17 21:22:33
Yengkong Sayaovong

Host: sftp://172.30.0.5 Username: ftpuser01 Password: •••••••••• Port:

```
Status:     Connected to 172.30.0.5
Status:     Starting upload of C:\Users\Administrator\Documents\adminReport.md5
Status:     File transfer successful, transferred 34 bytes in 1 second
Status:     Retrieving directory listing of "/mnt/tank/ftp/datadir"...
Status:     Listing directory /mnt/tank/ftp/datadir
Status:     Directory listing of "/mnt/tank/ftp/datadir" successful
```

Local site: C:\Users\Administrator\Documents\

Filename	Filesize	Filetype	Last modified
..			
My Music		File folder	9/17/2021 4:39:02 ...
My Pictures		File folder	9/17/2021 4:39:02 ...
My Videos		File folder	9/17/2021 4:39:02 ...
adminReport.md5	34	MD5 File	11/11/2021 10:38:2...
adminReport.pdf	138,802	Microsoft Edge PD...	11/10/2021 8:49:08...
Default.rdp	0	Remote Desktop C...	10/31/2021 4:29:19...
desktop.ini	402	Configuration setti...	9/17/2021 4:39:02 ...

Selected 1 file. Total size: 34 bytes

Remote site: /mnt/tank/ftp/datadir

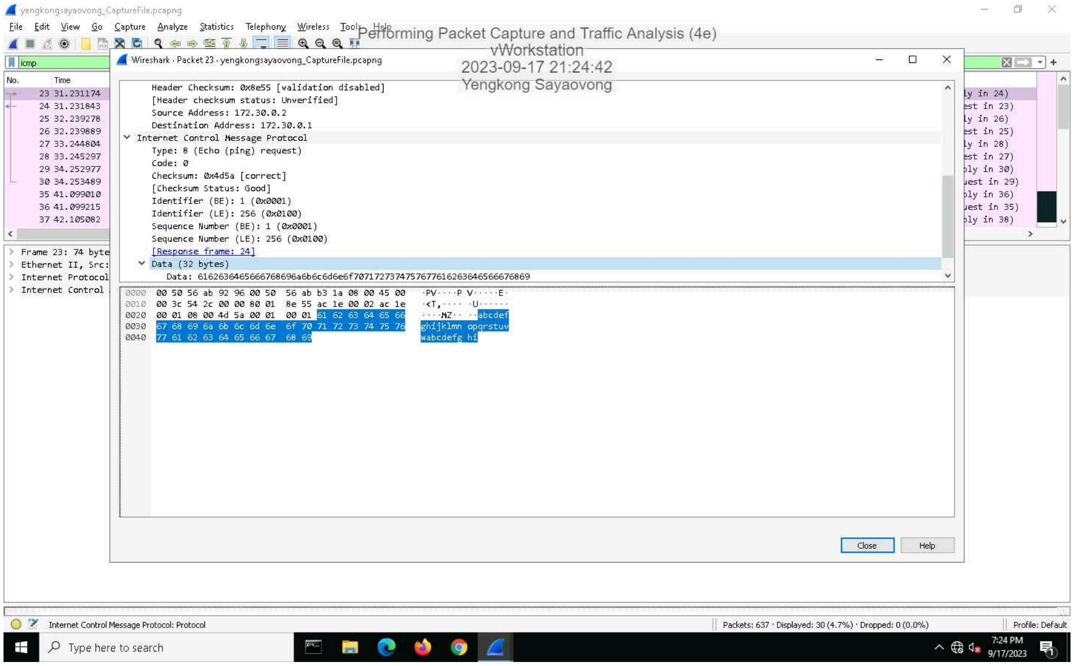
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
..					
adminReport.md5	34	MD5 File	9/17/2023 7:22:...	-rw-r--r--	ftpuser01 ftp
adminReport.pdf	138,802	Microsoft ...	9/17/2023 7:21:...	-rw-------	ftpuser01 ftp

2 files. Total size: 138,836 bytes

Server/Local file	Direction	Remote file	Size	Priority	Time
ftpuser01@172.30.0.5					
C:\Users\Administrator\D...	-->>	/datadir/adminReport.pdf	138,802	Normal	9/17/2023 7:21:45 PM
sftp://ftpuser01@172.30.0.5					
C:\Users\Administrator\Documents\adminReport.md5		/datadir/admin...	34	Normal	9/17/2023 7:22:25 PM

Part 2: Analyze Traffic Using Wireshark

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


yengkongsayaovong_CaptureFile.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Performing Packet Capture and Traffic Analysis (4e)
vWorkstation
2023-09-17 21:24:42
Yengkong Sayaovong
Wireshark · Packet 23 · yengkongsayaovong_CaptureFile.pcapng
No.
Time
Close
Help
Type here to search
7:24 PM
9/17/2023

```
23 31.231174
24 31.231843
25 32.239278
26 32.239889
27 33.244804
28 33.245297
29 34.252977
30 34.253489
35 41.099010
36 41.099215
37 42.105082
```

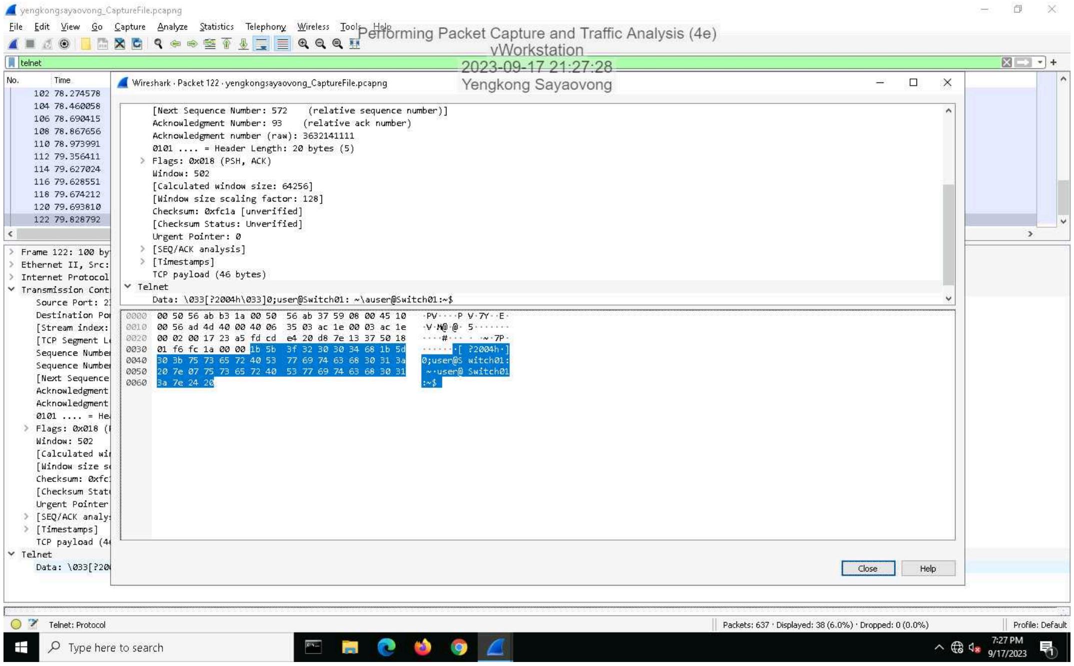
```
> Frame 23: 74 byte
> Ethernet II, Src:
> Internet Protocol
> Internet Control
```

```
    Header Checksum: 0x8e55 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.30.0.2
    Destination Address: 172.30.0.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 24]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
```

```
0000  00 50 56 ab 92 96 00 50  56 ab b3 1a 08 00 45 00   ·PV····P V·····E·
0010  00 3c 54 2c 00 00 80 01  8e 55 ac 1e 00 02 ac 1e   ·<T,···· ·U······
0020  00 01 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ····MZ·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Control Message Protocol: Protocol | Packets: 637 · Displayed: 30 (4.7%) · Dropped: 0 (0.0%) | Profile: Default

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


yengkongsayaovong_CaptureFile.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
Performing Packet Capture and Traffic Analysis (4e)
vWorkstation
2023-09-17 21:27:28
Yengkong Sayaovong
Wireshark · Packet 122 · yengkongsayaovong_CaptureFile.pcapng
No.
Time
Close
Help
Type here to search
7:27 PM
9/17/2023

```
102 78.274578
104 78.460058
106 78.690415
108 78.867656
110 78.973991
112 79.356411
114 79.627024
116 79.628551
118 79.674212
120 79.693810
122 79.828792
```

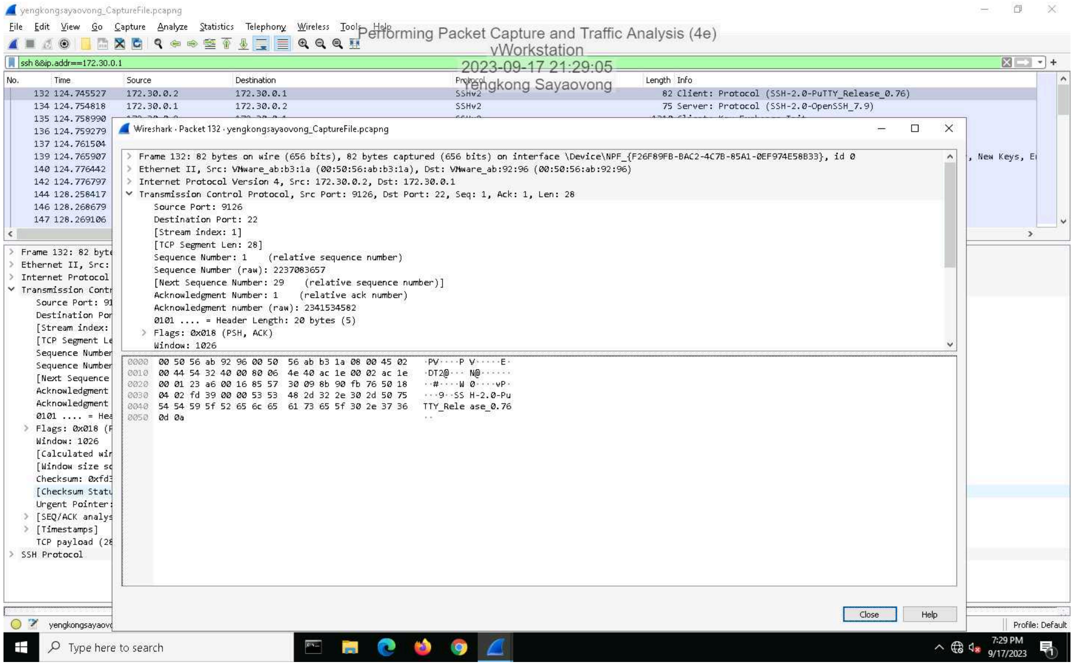
```
> Frame 122: 100 by
> Ethernet II, Src:
> Internet Protocol
v Transmission Cont
    Source Port: 2
    Destination Po
    [Stream index:
    [TCP Segment L
    Sequence Numbe
    Sequence Numbe
    [Next Sequence
    Acknowledgment
    Acknowledgment
    0101 .... = He
  > Flags: 0x018 (
    Window: 502
    [Calculated wi
    [Window size s
    Checksum: 0xfc
    [Checksum Stat
    Urgent Pointer
  > [SEQ/ACK analy
  > [Timestamps]
    TCP payload (4
v Telnet
    Data: \033[?20
```

```
    [Next Sequence Number: 572    (relative sequence number)]
    Acknowledgment Number: 93    (relative ack number)
    Acknowledgment number (raw): 3632141111
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0xfc1a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (46 bytes)
v Telnet
    Data: \033[?2004h\033]0;user@Switch01: ~\auser@Switch01:~$
```

```
0000  00 50 56 ab b3 1a 00 50  56 ab 37 59 08 00 45 10   ·PV····P V·7Y··E·
0010  00 56 ad 4d 40 00 40 06  35 03 ac 1e 00 03 ac 1e   ·V·M@·@· 5·······
0020  00 02 00 17 23 a5 fd cd  e4 20 d8 7e 13 37 50 18   ····#··· · ·~·7P·
0030  01 f6 fc 1a 00 00 1b 5b  3f 32 30 30 34 68 1b 5d   ······[ ?2004h·]
0040  30 3b 75 73 65 72 40 53  77 69 74 63 68 30 31 3a   0;user@S witch01:
0050  20 7e 07 75 73 65 72 40  53 77 69 74 63 68 30 31    ~·user@ Switch01
0060  3a 7e 24 20                                        :~$
```

Telnet: Protocol | Packets: 637 · Displayed: 38 (6.0%) · Dropped: 0 (0.0%) | Profile: Default

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


yengkongsayaovong_CaptureFile.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis (4e)
vWorkstation
2023-09-17 21:29:05
Yengkong Sayaovong
Close
Help
Profile: Default
Type here to search
7:29 PM
9/17/2023

ssh &&ip.addr==172.30.0.1

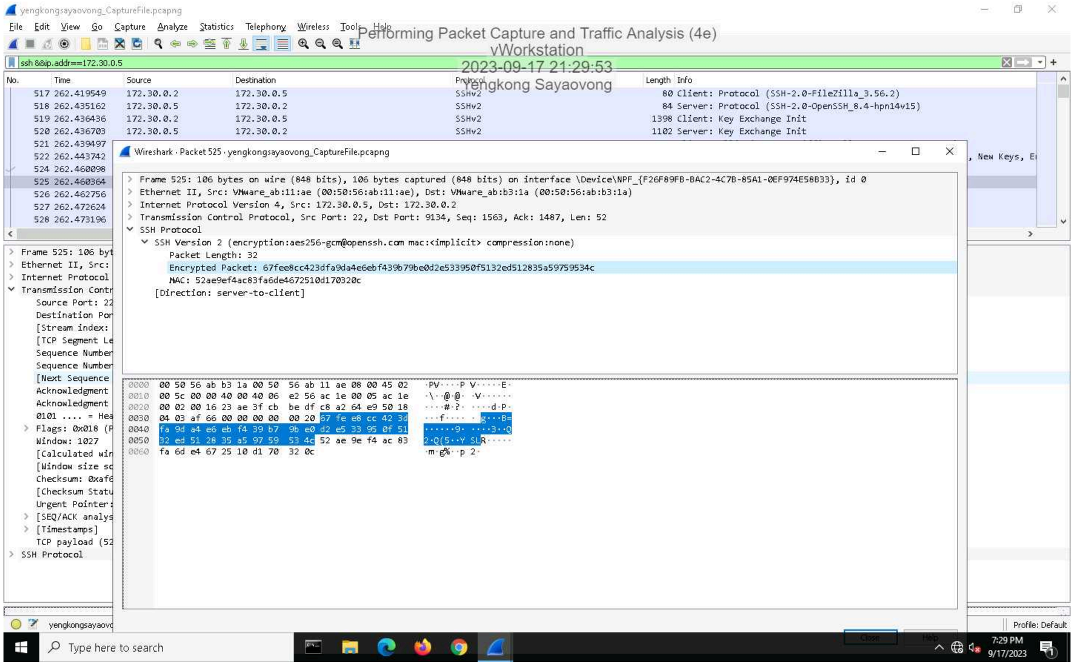
```
No.   Time        Source       Destination  Protocol  Length Info
  132 124.745527  172.30.0.2   172.30.0.1   SSHv2         82 Client: Protocol (SSH-2.0-PuTTY_Release_0.76)
  134 124.754818  172.30.0.1   172.30.0.2   SSHv2         75 Server: Protocol (SSH-2.0-OpenSSH_7.9)
  135 124.758990
  136 124.759279
  137 124.761504
  139 124.765907                                                , New Keys, E
  140 124.776442
  142 124.776797
  144 128.258417
  146 128.268679
  147 128.269106
```

Wireshark · Packet 132 · yengkongsayaovong_CaptureFile.pcapng

```
> Frame 132: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{F26F89FB-BAC2-4C7B-85A1-0EF974E58B33}, id 0
> Ethernet II, Src: VMware_ab:b3:1a (00:50:56:ab:b3:1a), Dst: VMware_ab:92:96 (00:50:56:ab:92:96)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.1
v Transmission Control Protocol, Src Port: 9126, Dst Port: 22, Seq: 1, Ack: 1, Len: 28
    Source Port: 9126
    Destination Port: 22
    [Stream index: 1]
    [TCP Segment Len: 28]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2237083657
    [Next Sequence Number: 29    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2341534582
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1026
```

```
0000  00 50 56 ab 92 96 00 50  56 ab b3 1a 08 00 45 02   ·PV····P V·····E·
0010  00 44 54 32 40 00 80 06  4e 40 ac 1e 00 02 ac 1e   ·DT2@··· N@······
0020  00 01 23 a6 00 16 85 57  30 09 8b 90 fb 76 50 18   ··#····W 0····vP·
0030  04 02 fd 39 00 00 53 53  48 2d 32 2e 30 2d 50 75   ···9··SS H-2.0-Pu
0040  54 54 59 5f 52 65 6c 65  61 73 65 5f 30 2e 37 36   TTY_Rele ase_0.76
0050  0d 0a                                               ··
```

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


yengkongsayaovong_CaptureFile.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis (4e)
vWorkstation
2023-09-17 21:29:53
Yengkong Sayaovong
Profile: Default
Type here to search
7:29 PM
9/17/2023

ssh &&ip.addr==172.30.0.5

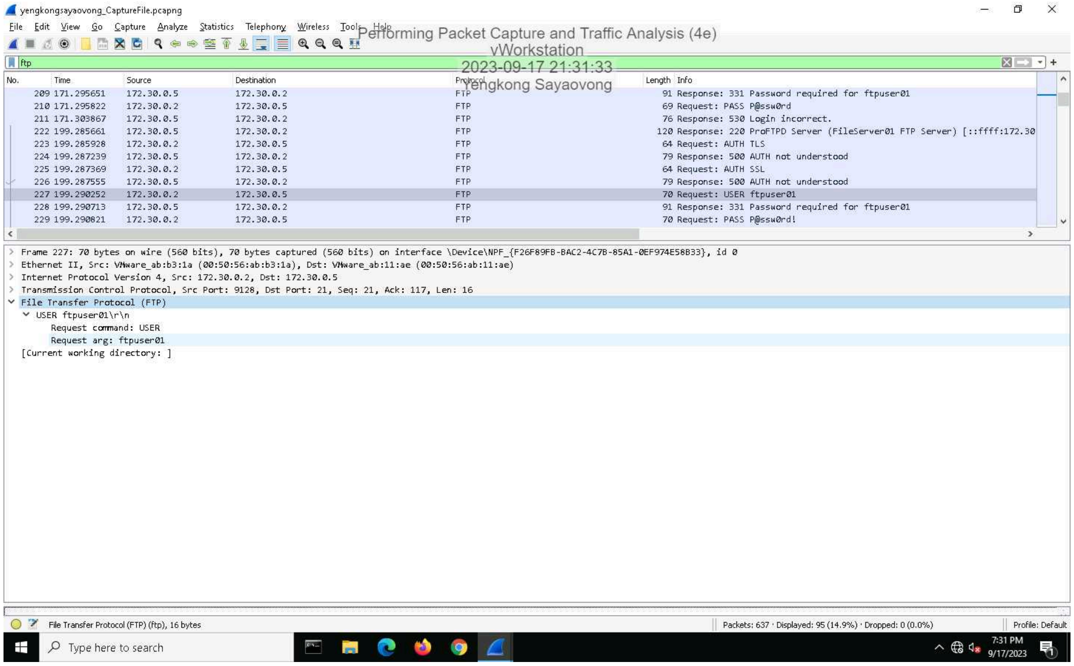
```
No.   Time        Source       Destination  Protocol  Length Info
  517 262.419549  172.30.0.2   172.30.0.5   SSHv2         80 Client: Protocol (SSH-2.0-FileZilla_3.56.2)
  518 262.435162  172.30.0.5   172.30.0.2   SSHv2         84 Server: Protocol (SSH-2.0-OpenSSH_8.4-hpn14v15)
  519 262.436436  172.30.0.2   172.30.0.5   SSHv2       1398 Client: Key Exchange Init
  520 262.436703  172.30.0.5   172.30.0.2   SSHv2       1102 Server: Key Exchange Init
  521 262.439497
  522 262.443742                                                , New Keys, E
  524 262.460098
  525 262.460364
  526 262.462756
  527 262.472624
  528 262.473196
```

Wireshark · Packet 525 · yengkongsayaovong_CaptureFile.pcapng

```
> Frame 525: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{F26F89FB-BAC2-4C7B-85A1-0EF974E58B33}, id 0
> Ethernet II, Src: VMware_ab:11:ae (00:50:56:ab:11:ae), Dst: VMware_ab:b3:1a (00:50:56:ab:b3:1a)
> Internet Protocol Version 4, Src: 172.30.0.5, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 22, Dst Port: 9134, Seq: 1563, Ack: 1487, Len: 52
v SSH Protocol
  v SSH Version 2 (encryption:aes256-gcm@openssh.com mac:<implicit> compression:none)
      Packet Length: 32
      Encrypted Packet: 67fee8cc423dfa9da4e6ebf439b79be0d2e533950f5132ed512835a59759534c
      MAC: 52ae9ef4ac83fa6de4672510d170320c
    [Direction: server-to-client]
```

```
0000  00 50 56 ab b3 1a 00 50  56 ab 11 ae 08 00 45 02   ·PV····P V·····E·
0010  00 5c 00 00 40 00 40 06  e2 56 ac 1e 00 05 ac 1e   ·\··@·@· ·V······
0020  00 02 00 16 23 ae 3f cb  be df c8 a2 64 e9 50 18   ····#·?· ····d·P·
0030  04 03 af 66 00 00 00 00  00 20 67 fe e8 cc 42 3d   ···f···· · g···B=
0040  fa 9d a4 e6 eb f4 39 b7  9b e0 d2 e5 33 95 0f 51   ······9· ····3··Q
0050  32 ed 51 28 35 a5 97 59  53 4c 52 ae 9e f4 ac 83   2·Q(5··Y SLR·····
0060  fa 6d e4 67 25 10 d1 70  32 0c                     ·m·g%··p 2·
```

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

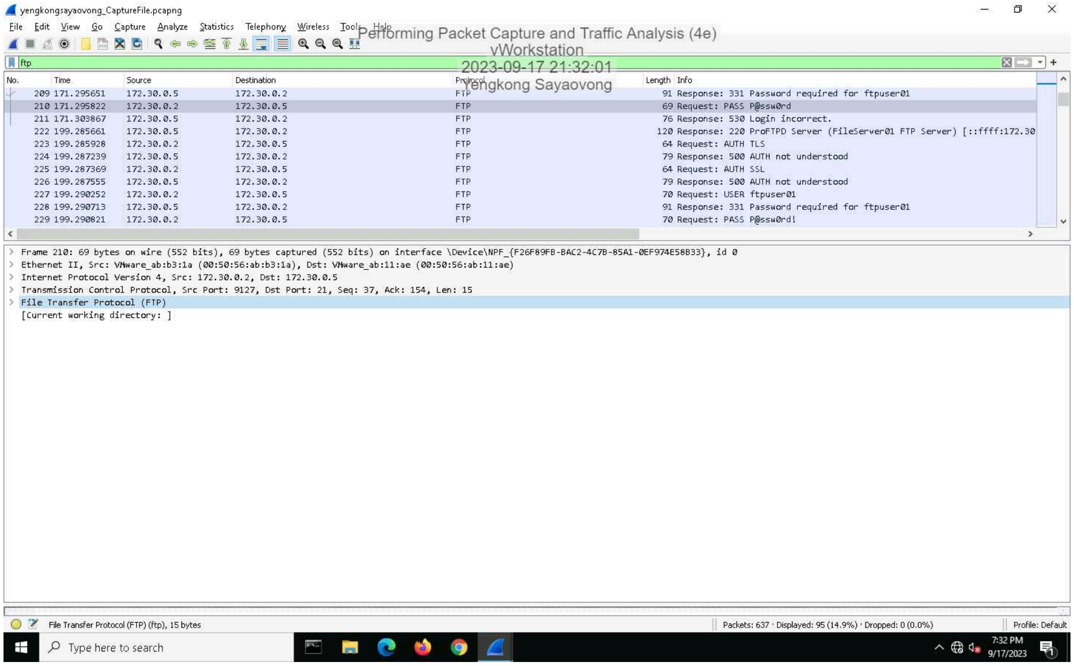

yengkongsayaovong_CaptureFile.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis (4e)
vWorkstation
2023-09-17 21:31:33
Yengkong Sayaovong
ftp
Type here to search
7:31 PM
9/17/2023

```
No.  Time        Source       Destination  Protocol  Length Info
 209 171.295651  172.30.0.5   172.30.0.2   FTP           91 Response: 331 Password required for ftpuser01
 210 171.295822  172.30.0.2   172.30.0.5   FTP           69 Request: PASS P@ssw0rd
 211 171.303867  172.30.0.5   172.30.0.2   FTP           76 Response: 530 Login incorrect.
 222 199.285661  172.30.0.5   172.30.0.2   FTP          120 Response: 220 ProFTPD Server (FileServer01 FTP Server) [::ffff:172.30
 223 199.285928  172.30.0.2   172.30.0.5   FTP           64 Request: AUTH TLS
 224 199.287239  172.30.0.5   172.30.0.2   FTP           79 Response: 500 AUTH not understood
 225 199.287369  172.30.0.2   172.30.0.5   FTP           64 Request: AUTH SSL
 226 199.287555  172.30.0.5   172.30.0.2   FTP           79 Response: 500 AUTH not understood
 227 199.290252  172.30.0.2   172.30.0.5   FTP           70 Request: USER ftpuser01
 228 199.290713  172.30.0.5   172.30.0.2   FTP           91 Response: 331 Password required for ftpuser01
 229 199.290821  172.30.0.2   172.30.0.5   FTP           70 Request: PASS P@ssw0rd!
```

```
> Frame 227: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{F26F89FB-BAC2-4C7B-85A1-0EF974E58B33}, id 0
> Ethernet II, Src: VMware_ab:b3:1a (00:50:56:ab:b3:1a), Dst: VMware_ab:11:ae (00:50:56:ab:11:ae)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.5
> Transmission Control Protocol, Src Port: 9128, Dst Port: 21, Seq: 21, Ack: 117, Len: 16
v File Transfer Protocol (FTP)
  v USER ftpuser01\r\n
      Request command: USER
      Request arg: ftpuser01
  [Current working directory: ]
```

File Transfer Protocol (FTP) (ftp), 16 bytes | Packets: 637 · Displayed: 95 (14.9%) · Dropped: 0 (0.0%) | Profile: Default

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


yengkongsayaovong_CaptureFile.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis (4e)
vWorkstation
2023-09-17 21:32:01
Yengkong Sayaovong
ftp
Type here to search
7:32 PM
9/17/2023

```
No.  Time        Source       Destination  Protocol  Length Info
 209 171.295651  172.30.0.5   172.30.0.2   FTP           91 Response: 331 Password required for ftpuser01
 210 171.295822  172.30.0.2   172.30.0.5   FTP           69 Request: PASS P@ssw0rd
 211 171.303867  172.30.0.5   172.30.0.2   FTP           76 Response: 530 Login incorrect.
 222 199.285661  172.30.0.5   172.30.0.2   FTP          120 Response: 220 ProFTPD Server (FileServer01 FTP Server) [::ffff:172.30
 223 199.285928  172.30.0.2   172.30.0.5   FTP           64 Request: AUTH TLS
 224 199.287239  172.30.0.5   172.30.0.2   FTP           79 Response: 500 AUTH not understood
 225 199.287369  172.30.0.2   172.30.0.5   FTP           64 Request: AUTH SSL
 226 199.287555  172.30.0.5   172.30.0.2   FTP           79 Response: 500 AUTH not understood
 227 199.290252  172.30.0.2   172.30.0.5   FTP           70 Request: USER ftpuser01
 228 199.290713  172.30.0.5   172.30.0.2   FTP           91 Response: 331 Password required for ftpuser01
 229 199.290821  172.30.0.2   172.30.0.5   FTP           70 Request: PASS P@ssw0rd!
```

```
> Frame 210: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{F26F89FB-BAC2-4C7B-85A1-0EF974E58B33}, id 0
> Ethernet II, Src: VMware_ab:b3:1a (00:50:56:ab:b3:1a), Dst: VMware_ab:11:ae (00:50:56:ab:11:ae)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.5
> Transmission Control Protocol, Src Port: 9127, Dst Port: 21, Seq: 37, Ack: 154, Len: 15
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

File Transfer Protocol (FTP) (ftp), 15 bytes | Packets: 637 · Displayed: 95 (14.9%) · Dropped: 0 (0.0%) | Profile: Default

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**.

Incomplete

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

Incomplete

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

Incomplete

Part 2: Analyze Traffic Using Wireshark

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

Incomplete

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

Incomplete

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

Incomplete

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

Incomplete

Section 3: Challenge and Analysis

Part 1: Generate Malicious Network Traffic

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

Incomplete

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**.

Incomplete

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

Incomplete