Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

Student:	Email:
Udo Udo Williams	raggg12@gmail.com

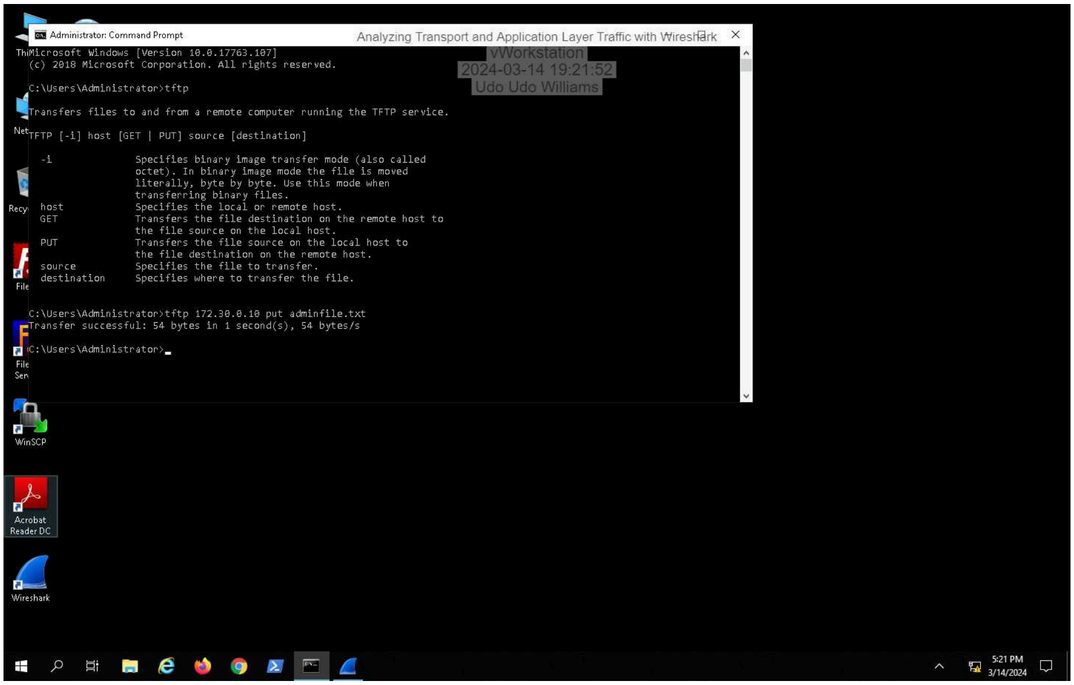
Time on Task:	Progress:
9 hours, 48 minutes	100%

Report Generated: Friday, March 15, 2024 at 12:36 AM

Section 1: Hands-On Demonstration

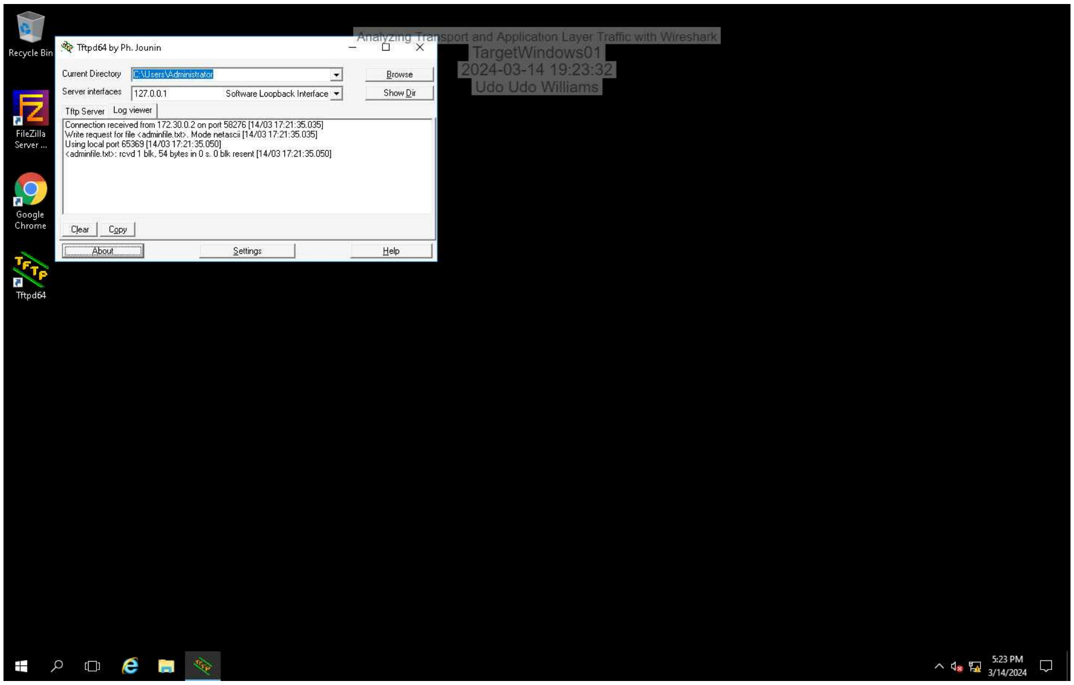
Part 1: Configure Wireshark and Generate Network Traffic

28. **Make a screen capture** showing the **successful tftp file transfer message in the Command Prompt**.



```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>tftp

Transfers files to and from a remote computer running the TFTP service.

TFTP [-i] host [GET | PUT] source [destination]

  -i              Specifies binary image transfer mode (also called
                  octet). In binary image mode the file is moved
                  literally, byte by byte. Use this mode when
                  transferring binary files.
  host            Specifies the local or remote host.
  GET             Transfers the file destination on the remote host to
                  the file source on the local host.
  PUT             Transfers the file source on the local host to
                  the file destination on the remote host.
  source          Specifies the file to transfer.
  destination     Specifies where to transfer the file.


C:\Users\Administrator>tftp 172.30.0.10 put adminfile.txt
Transfer successful: 54 bytes in 1 second(s), 54 bytes/s

C:\Users\Administrator>_
```

32. **Make a screen capture** showing the **Tftpd64 Server log**.

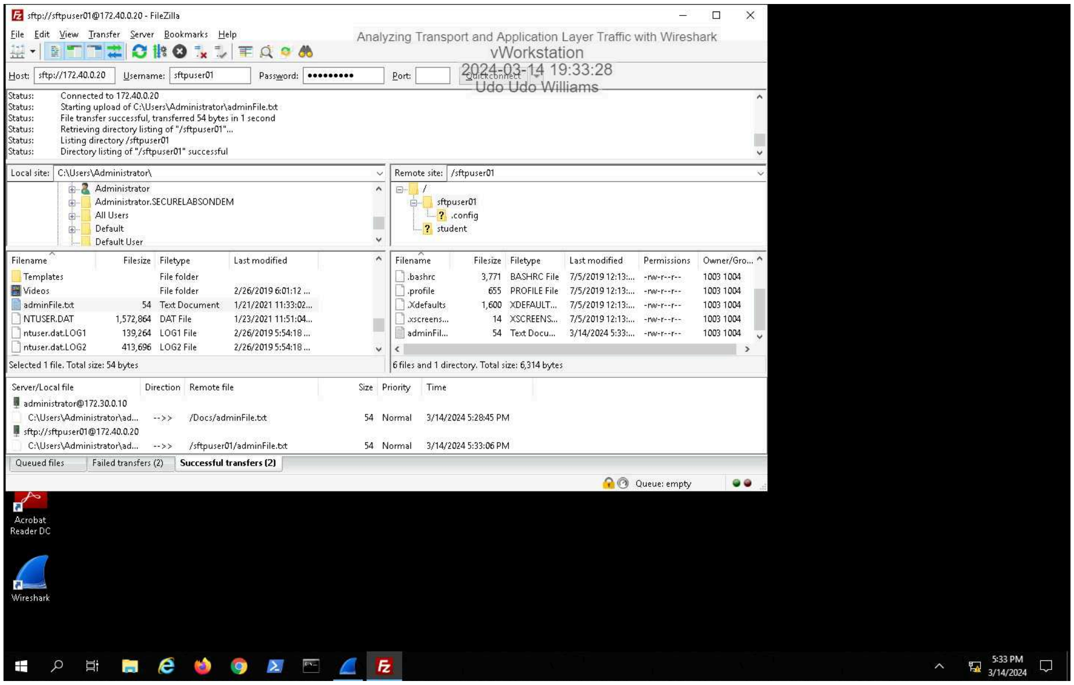


Analyzing Transport and Application Layer Traffic with Wireshark
TargetWindows01
2024-03-14 19:23:32
Udo Udo Williams

Current Directory: C:\Users\Administrator
Server interfaces: 127.0.0.1 Software Loopback Interface

```
Connection received from 172.30.0.2 on port 58276 [14/03 17:21:35.035]
Write request for file <adminfile.txt>. Mode netascii [14/03 17:21:35.035]
Using local port 65369 [14/03 17:21:35.050]
<adminfile.txt>: rcvd 1 blk, 54 bytes in 0 s. 0 blk resent [14/03 17:21:35.050]
```

45. **Make a screen capture** showing the **successful SFTP file transfer**.



Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 19:33:28
Udo Udo Williams

Host: sftp://172.40.0.20 Username: sftpuser01 Password: •••••••••• Port:

```
Status:     Connected to 172.40.0.20
Status:     Starting upload of C:\Users\Administrator\adminFile.txt
Status:     File transfer successful, transferred 54 bytes in 1 second
Status:     Retrieving directory listing of "/sftpuser01"...
Status:     Listing directory /sftpuser01
Status:     Directory listing of "/sftpuser01" successful
```

Local site: C:\Users\Administrator\

- Administrator
- Administrator.SECURELABSONDEM
- All Users
- Default
- Default User

Remote site: /sftpuser01

- /
  - sftpuser01
    - .config
  - student

Filename	Filesize	Filetype	Last modified
Templates		File folder	
Videos		File folder	2/26/2019 6:01:12 ...
adminFile.txt	54	Text Document	1/21/2021 11:33:02...
NTUSER.DAT	1,572,864	DAT File	1/23/2021 11:51:04...
ntuser.dat.LOG1	139,264	LOG1 File	2/26/2019 5:54:18 ...
ntuser.dat.LOG2	413,696	LOG2 File	2/26/2019 5:54:18 ...

Selected 1 file. Total size: 54 bytes

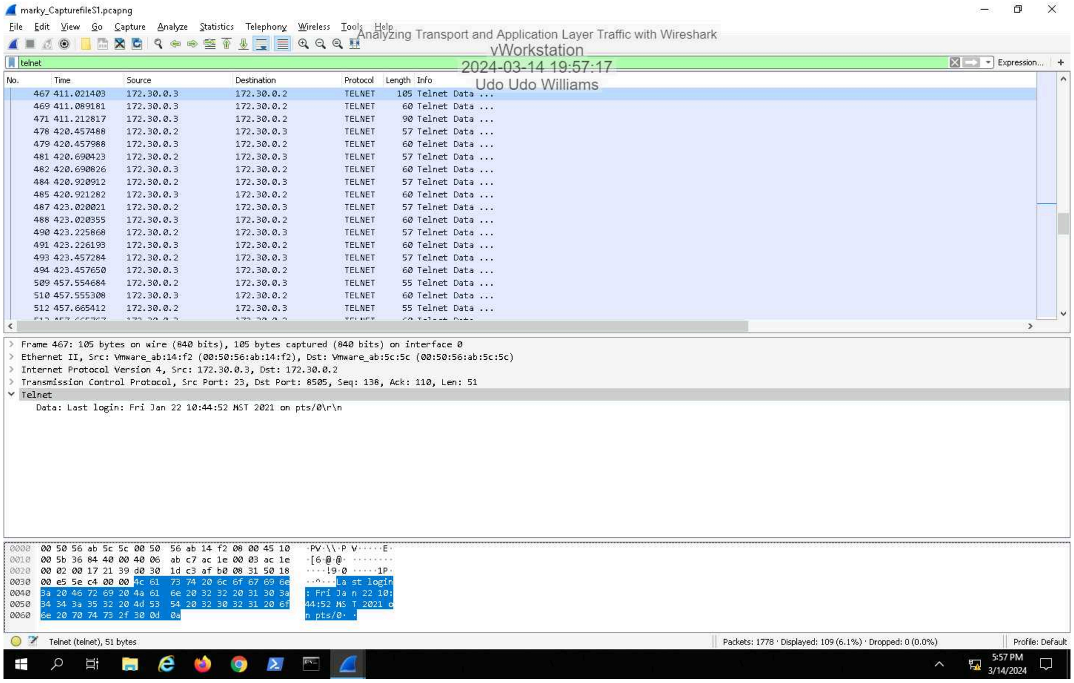
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
.bashrc	3,771	BASHRC File	7/5/2019 12:13:...	-rw-r--r--	1003 1004
.profile	655	PROFILE File	7/5/2019 12:13:...	-rw-r--r--	1003 1004
.Xdefaults	1,600	XDEFAULT...	7/5/2019 12:13:...	-rw-r--r--	1003 1004
.xscreens...	14	XSCREENS...	7/5/2019 12:13:...	-rw-r--r--	1003 1004
adminFil...	54	Text Docu...	3/14/2024 5:33:...	-rw-r--r--	1003 1004

6 files and 1 directory. Total size: 6,314 bytes

Server/Local file	Direction	Remote file	Size	Priority	Time
administrator@172.30.0.10					
C:\Users\Administrator\ad...	-->>	/Docs/adminFile.txt	54	Normal	3/14/2024 5:28:45 PM
sftp://sftpuser01@172.40.0.20					
C:\Users\Administrator\ad...	-->>	/sftpuser01/adminFile.txt	54	Normal	3/14/2024 5:33:06 PM

Part 2: Perform Protocol Analysis using Wireshark

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


marky_CapturefileS1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 19:57:17
Udo Udo Williams
Expression...
5:57 PM
3/14/2024

Filter: telnet

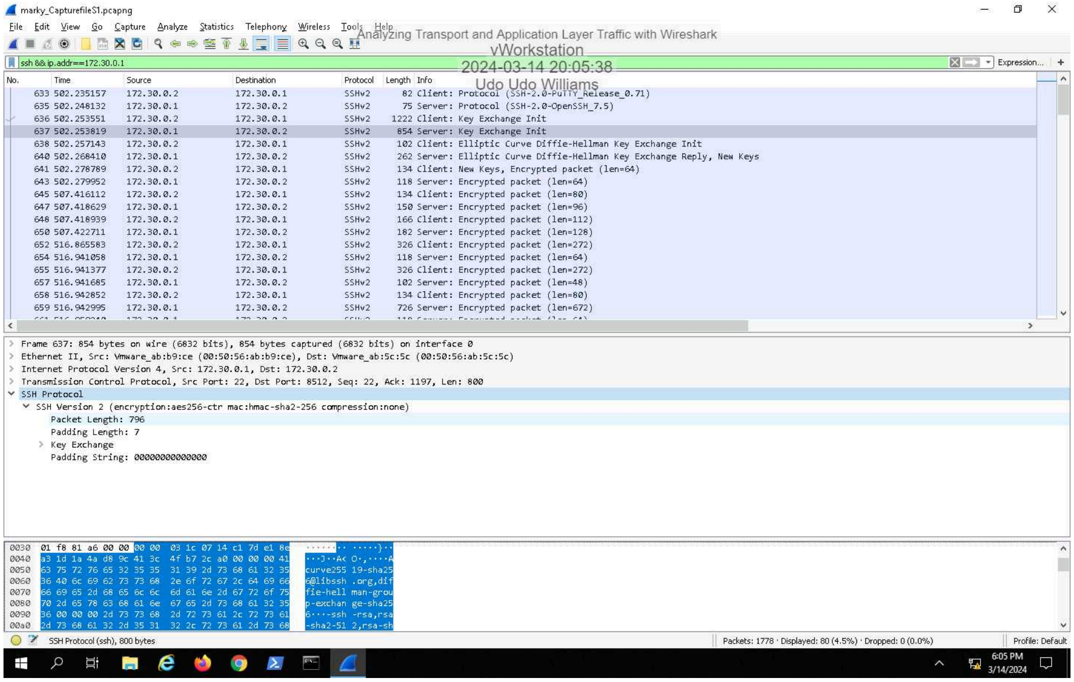
```
No.  Time        Source       Destination  Protocol  Length  Info
467 411.021403  172.30.0.3   172.30.0.2   TELNET    105 Telnet Data ...
469 411.089181  172.30.0.3   172.30.0.2   TELNET     60 Telnet Data ...
471 411.212817  172.30.0.3   172.30.0.2   TELNET     90 Telnet Data ...
478 420.457488  172.30.0.2   172.30.0.3   TELNET     57 Telnet Data ...
479 420.457988  172.30.0.3   172.30.0.2   TELNET     60 Telnet Data ...
481 420.690423  172.30.0.2   172.30.0.3   TELNET     57 Telnet Data ...
482 420.690826  172.30.0.3   172.30.0.2   TELNET     60 Telnet Data ...
484 420.920912  172.30.0.2   172.30.0.3   TELNET     57 Telnet Data ...
485 420.921282  172.30.0.3   172.30.0.2   TELNET     60 Telnet Data ...
487 423.020021  172.30.0.2   172.30.0.3   TELNET     57 Telnet Data ...
488 423.020355  172.30.0.3   172.30.0.2   TELNET     60 Telnet Data ...
490 423.225868  172.30.0.2   172.30.0.3   TELNET     57 Telnet Data ...
491 423.226193  172.30.0.3   172.30.0.2   TELNET     60 Telnet Data ...
493 423.457284  172.30.0.2   172.30.0.3   TELNET     57 Telnet Data ...
494 423.457650  172.30.0.3   172.30.0.2   TELNET     60 Telnet Data ...
509 457.554684  172.30.0.2   172.30.0.3   TELNET     55 Telnet Data ...
510 457.555308  172.30.0.3   172.30.0.2   TELNET     60 Telnet Data ...
512 457.665412  172.30.0.2   172.30.0.3   TELNET     55 Telnet Data ...
```

```
> Frame 467: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0
> Ethernet II, Src: Vmware_ab:14:f2 (00:50:56:ab:14:f2), Dst: Vmware_ab:5c:5c (00:50:56:ab:5c:5c)
> Internet Protocol Version 4, Src: 172.30.0.3, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 23, Dst Port: 8505, Seq: 138, Ack: 110, Len: 51
v Telnet
    Data: Last login: Fri Jan 22 10:44:52 MST 2021 on pts/0\r\n
```

```
0000  00 50 56 ab 5c 5c 00 50  56 ab 14 f2 08 00 45 10   ·PV·\\·P V·····E·
0010  00 5b 36 84 40 00 40 06  ab c7 ac 1e 00 03 ac 1e   ·[6·@·@· ········
0020  00 02 00 17 21 39 d0 30  1d c3 af b0 08 31 50 18   ····!9·0 ·····1P·
0030  00 e5 5e c4 00 00 4c 61  73 74 20 6c 6f 67 69 6e   ··^···La st login
0040  3a 20 46 72 69 20 4a 61  6e 20 32 32 20 31 30 3a   : Fri Ja n 22 10:
0050  34 34 3a 35 32 20 4d 53  54 20 32 30 32 31 20 6f   44:52 MS T 2021 o
0060  6e 20 70 74 73 2f 30 0d  0a                        n pts/0· ·
```

Telnet (telnet), 51 bytes | Packets: 1778 · Displayed: 109 (6.1%) · Dropped: 0 (0.0%) | Profile: Default

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


marky_CapturefileS1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 20:05:38
Udo Udo Williams
Expression...
6:05 PM
3/14/2024

Filter: ssh && ip.addr==172.30.0.1

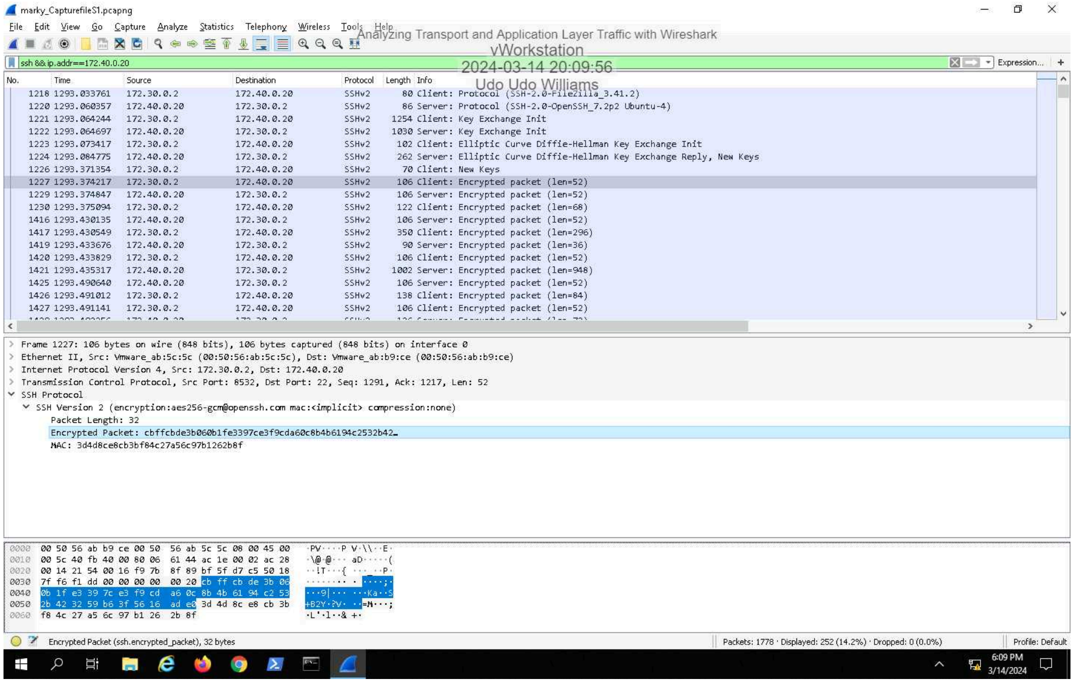
```
No.  Time        Source       Destination  Protocol  Length  Info
633 502.235157  172.30.0.2   172.30.0.1   SSHv2      82 Client: Protocol (SSH-2.0-PuTTY_Release_0.71)
635 502.248132  172.30.0.1   172.30.0.2   SSHv2      75 Server: Protocol (SSH-2.0-OpenSSH_7.5)
636 502.253551  172.30.0.2   172.30.0.1   SSHv2    1222 Client: Key Exchange Init
637 502.253819  172.30.0.1   172.30.0.2   SSHv2     854 Server: Key Exchange Init
638 502.257143  172.30.0.2   172.30.0.1   SSHv2     102 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
640 502.268410  172.30.0.1   172.30.0.2   SSHv2     262 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
641 502.278789  172.30.0.2   172.30.0.1   SSHv2     134 Client: New Keys, Encrypted packet (len=64)
643 502.279952  172.30.0.1   172.30.0.2   SSHv2     118 Server: Encrypted packet (len=64)
645 507.416112  172.30.0.2   172.30.0.1   SSHv2     134 Client: Encrypted packet (len=80)
647 507.418629  172.30.0.1   172.30.0.2   SSHv2     150 Server: Encrypted packet (len=96)
648 507.418939  172.30.0.2   172.30.0.1   SSHv2     166 Client: Encrypted packet (len=112)
650 507.422711  172.30.0.1   172.30.0.2   SSHv2     182 Server: Encrypted packet (len=128)
652 516.865583  172.30.0.2   172.30.0.1   SSHv2     326 Client: Encrypted packet (len=272)
654 516.941058  172.30.0.1   172.30.0.2   SSHv2     118 Server: Encrypted packet (len=64)
655 516.941377  172.30.0.2   172.30.0.1   SSHv2     326 Client: Encrypted packet (len=272)
657 516.941685  172.30.0.1   172.30.0.2   SSHv2     102 Server: Encrypted packet (len=48)
658 516.942852  172.30.0.2   172.30.0.1   SSHv2     134 Client: Encrypted packet (len=80)
659 516.942995  172.30.0.1   172.30.0.2   SSHv2     726 Server: Encrypted packet (len=672)
```

```
> Frame 637: 854 bytes on wire (6832 bits), 854 bytes captured (6832 bits) on interface 0
> Ethernet II, Src: Vmware_ab:b9:ce (00:50:56:ab:b9:ce), Dst: Vmware_ab:5c:5c (00:50:56:ab:5c:5c)
> Internet Protocol Version 4, Src: 172.30.0.1, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 22, Dst Port: 8512, Seq: 22, Ack: 1197, Len: 800
v SSH Protocol
  v SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
      Packet Length: 796
      Padding Length: 7
    > Key Exchange
      Padding String: 00000000000000
```

```
0030  01 f8 81 a6 00 00 00 00  03 1c 07 14 c1 7d e1 8e   ········ ·····}··
0040  a3 1d 1a 4a d8 9c 41 3c  4f b7 2c a0 00 00 00 41   ···J··A< O·,····A
0050  63 75 72 76 65 32 35 35  31 39 2d 73 68 61 32 35   curve255 19-sha25
0060  36 40 6c 69 62 73 73 68  2e 6f 72 67 2c 64 69 66   6@libssh .org,dif
0070  66 69 65 2d 68 65 6c 6c  6d 61 6e 2d 67 72 6f 75   fie-hell man-grou
0080  70 2d 65 78 63 68 61 6e  67 65 2d 73 68 61 32 35   p-exchan ge-sha25
0090  36 00 00 00 2d 73 73 68  2d 72 73 61 2c 72 73 61   6···-ssh -rsa,rsa
00a0  2d 73 68 61 32 2d 35 31  32 2c 72 73 61 2d 73 68   -sha2-51 2,rsa-sh
```

SSH Protocol (ssh), 800 bytes | Packets: 1778 · Displayed: 80 (4.5%) · Dropped: 0 (0.0%) | Profile: Default

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


marky_CapturefileS1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 20:09:56
Udo Udo Williams
Expression...

ssh && ip.addr==172.40.0.20

```
No.  Time         Source       Destination  Protocol  Length Info
1218 1293.033761  172.30.0.2   172.40.0.20  SSHv2       80 Client: Protocol (SSH-2.0-FileZilla_3.41.2)
1220 1293.060357  172.40.0.20  172.30.0.2   SSHv2       86 Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4)
1221 1293.064244  172.30.0.2   172.40.0.20  SSHv2     1254 Client: Key Exchange Init
1222 1293.064697  172.40.0.20  172.30.0.2   SSHv2     1030 Server: Key Exchange Init
1223 1293.073417  172.30.0.2   172.40.0.20  SSHv2      102 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
1224 1293.084775  172.40.0.20  172.30.0.2   SSHv2      262 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
1226 1293.371354  172.30.0.2   172.40.0.20  SSHv2       70 Client: New Keys
1227 1293.374217  172.30.0.2   172.40.0.20  SSHv2      106 Client: Encrypted packet (len=52)
1229 1293.374847  172.40.0.20  172.30.0.2   SSHv2      106 Server: Encrypted packet (len=52)
1230 1293.375094  172.30.0.2   172.40.0.20  SSHv2      122 Client: Encrypted packet (len=68)
1416 1293.430135  172.40.0.20  172.30.0.2   SSHv2      106 Server: Encrypted packet (len=52)
1417 1293.430549  172.30.0.2   172.40.0.20  SSHv2      350 Client: Encrypted packet (len=296)
1419 1293.433676  172.40.0.20  172.30.0.2   SSHv2       90 Server: Encrypted packet (len=36)
1420 1293.433829  172.30.0.2   172.40.0.20  SSHv2      106 Client: Encrypted packet (len=52)
1421 1293.435317  172.40.0.20  172.30.0.2   SSHv2     1002 Server: Encrypted packet (len=948)
1425 1293.490640  172.40.0.20  172.30.0.2   SSHv2      106 Server: Encrypted packet (len=52)
1426 1293.491012  172.30.0.2   172.40.0.20  SSHv2      138 Client: Encrypted packet (len=84)
1427 1293.491141  172.30.0.2   172.40.0.20  SSHv2      106 Client: Encrypted packet (len=52)
```

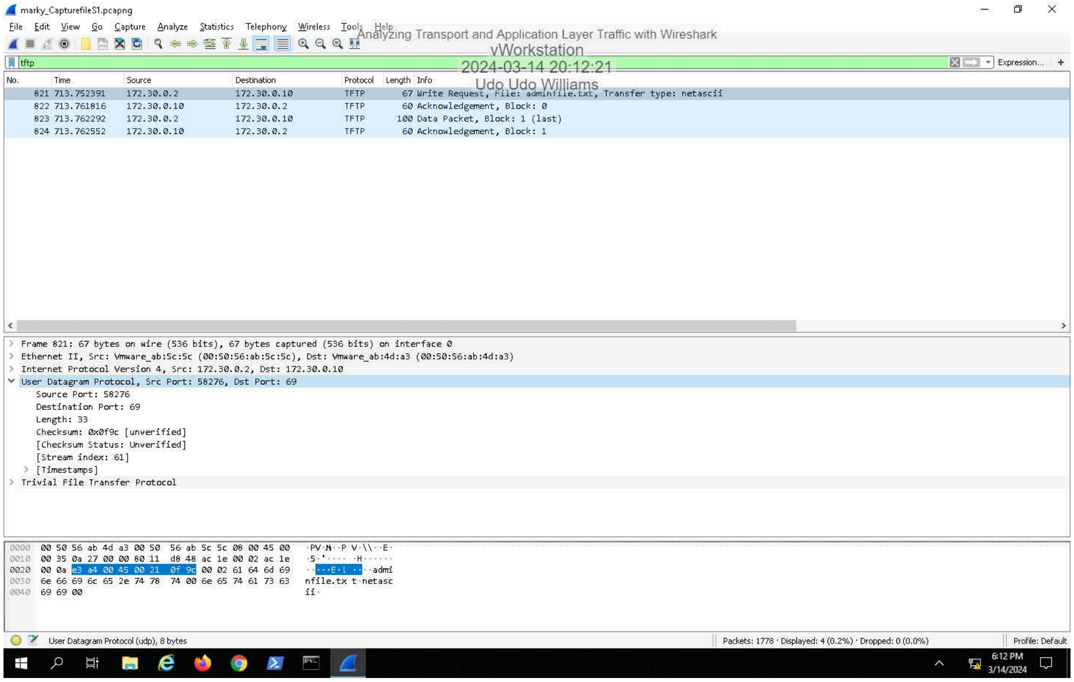
```
> Frame 1227: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Vmware_ab:5c:5c (00:50:56:ab:5c:5c), Dst: Vmware_ab:b9:ce (00:50:56:ab:b9:ce)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.40.0.20
> Transmission Control Protocol, Src Port: 8532, Dst Port: 22, Seq: 1291, Ack: 1217, Len: 52
v SSH Protocol
  v SSH Version 2 (encryption:aes256-gcm@openssh.com mac:<implicit> compression:none)
      Packet Length: 32
      Encrypted Packet: cbffcbde3b060b1fe3397ce3f9cda60c8b4b6194c2532b42…
      MAC: 3d4d8ce8cb3bf84c27a56c97b1262b8f
```

```
0000  00 50 56 ab b9 ce 00 50  56 ab 5c 5c 08 00 45 00   ·PV····P V·\\··E·
0010  00 5c 40 fb 40 00 80 06  61 44 ac 1e 00 02 ac 28   ·\@·@··· aD·····(
0020  00 14 21 54 00 16 f9 7b  8f 89 bf 5f d7 c5 50 18   ··!T···{ ······P·
0030  7f f6 f1 dd 00 00 00 00  00 20 cb ff cb de 3b 06   ········ ·····;·
0040  0b 1f e3 39 7c e3 f9 cd  a6 0c 8b 4b 61 94 c2 53   ···9|··· ···Ka··S
0050  2b 42 32 59 b6 3f 56 16  ad e0 3d 4d 8c e8 cb 3b   +B2Y·?V· ··=M···;
0060  f8 4c 27 a5 6c 97 b1 26  2b 8f                     ·L'·l··& +·
```

Encrypted Packet (ssh.encrypted_packet), 32 bytes | Packets: 1778 · Displayed: 252 (14.2%) · Dropped: 0 (0.0%) | Profile: Default

6:09 PM 3/14/2024

20. **Make a screen capture** showing the **Destination Port used for the initial TFTP transfer request**.


marky_CapturefileS1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 20:12:21
Udo Udo Williams
Expression...

tftp

```
No. Time        Source       Destination  Protocol  Length Info
821 713.752391  172.30.0.2   172.30.0.10  TFTP        67 Write Request, File: adminfile.txt, Transfer type: netascii
822 713.761816  172.30.0.10  172.30.0.2   TFTP        60 Acknowledgement, Block: 0
823 713.762292  172.30.0.2   172.30.0.10  TFTP       100 Data Packet, Block: 1 (last)
824 713.762552  172.30.0.10  172.30.0.2   TFTP        60 Acknowledgement, Block: 1
```

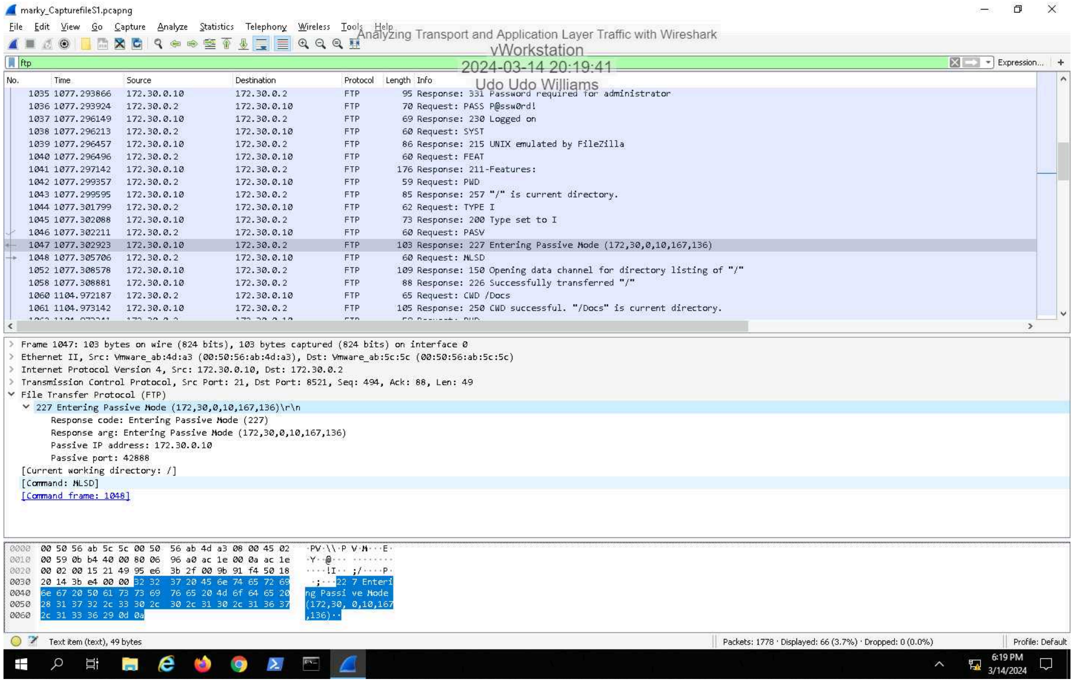
```
> Frame 821: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
> Ethernet II, Src: Vmware_ab:5c:5c (00:50:56:ab:5c:5c), Dst: Vmware_ab:4d:a3 (00:50:56:ab:4d:a3)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.10
v User Datagram Protocol, Src Port: 58276, Dst Port: 69
    Source Port: 58276
    Destination Port: 69
    Length: 33
    Checksum: 0x0f9c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 61]
  > [Timestamps]
> Trivial File Transfer Protocol
```

```
0000  00 50 56 ab 4d a3 00 50  56 ab 5c 5c 08 00 45 00   ·PV·M··P V·\\··E·
0010  00 35 0a 27 00 00 80 11  d8 48 ac 1e 00 02 ac 1e   ·5·'···· ·H······
0020  00 0a e3 a4 00 45 00 21  0f 9c 00 02 61 64 6d 69   ·····E·! ····admi
0030  6e 66 69 6c 65 2e 74 78  74 00 6e 65 74 61 73 63   nfile.tx t·netasc
0040  69 69 00                                           ii·
```

User Datagram Protocol (udp), 8 bytes | Packets: 1778 · Displayed: 4 (0.2%) · Dropped: 0 (0.0%) | Profile: Default

6:12 PM 3/14/2024

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


marky_CaptureFileS1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
ftp
```

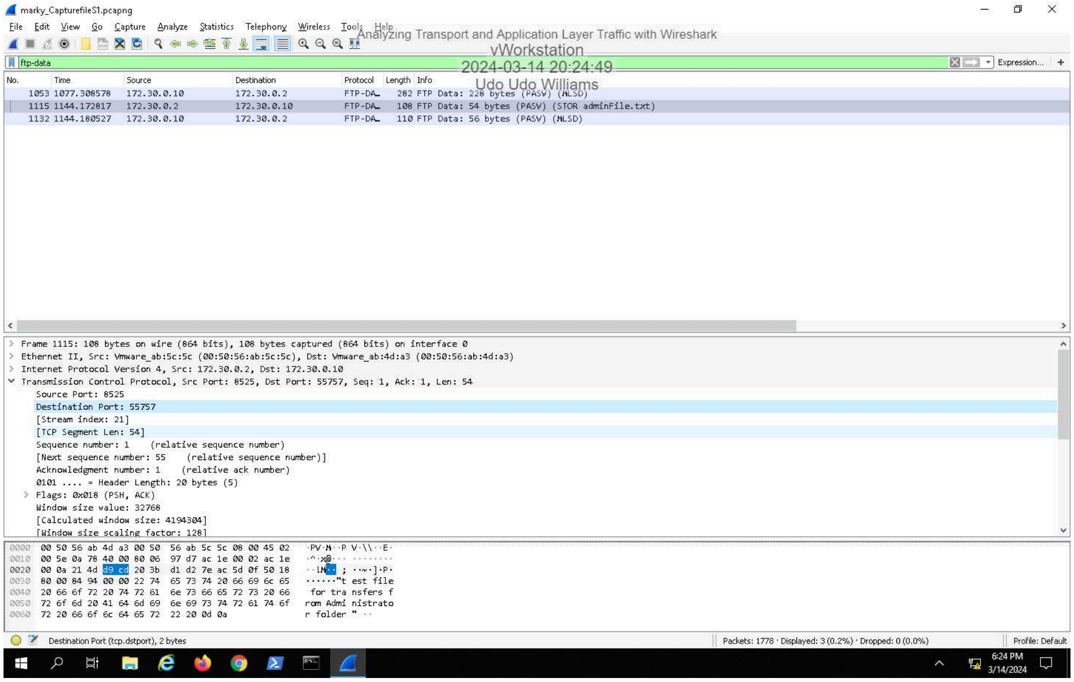
```
No.  Time         Source       Destination  Protocol Length Info
1035 1077.293866  172.30.0.10  172.30.0.2   FTP      95 Response: 331 Password required for administrator
1036 1077.293924  172.30.0.2   172.30.0.10  FTP      70 Request: PASS P@ssw0rd!
1037 1077.296149  172.30.0.10  172.30.0.2   FTP      69 Response: 230 Logged on
1038 1077.296213  172.30.0.2   172.30.0.10  FTP      60 Request: SYST
1039 1077.296457  172.30.0.10  172.30.0.2   FTP      86 Response: 215 UNIX emulated by FileZilla
1040 1077.296496  172.30.0.2   172.30.0.10  FTP      60 Request: FEAT
1041 1077.297142  172.30.0.10  172.30.0.2   FTP     176 Response: 211-Features:
1042 1077.299357  172.30.0.2   172.30.0.10  FTP      59 Request: PWD
1043 1077.299595  172.30.0.10  172.30.0.2   FTP      85 Response: 257 "/" is current directory.
1044 1077.301799  172.30.0.2   172.30.0.10  FTP      62 Request: TYPE I
1045 1077.302088  172.30.0.10  172.30.0.2   FTP      73 Response: 200 Type set to I
1046 1077.302211  172.30.0.2   172.30.0.10  FTP      60 Request: PASV
1047 1077.302923  172.30.0.10  172.30.0.2   FTP     103 Response: 227 Entering Passive Mode (172,30,0,10,167,136)
1048 1077.305706  172.30.0.2   172.30.0.10  FTP      60 Request: MLSD
1052 1077.308578  172.30.0.10  172.30.0.2   FTP     109 Response: 150 Opening data channel for directory listing of "/"
1058 1077.308881  172.30.0.10  172.30.0.2   FTP      88 Response: 226 Successfully transferred "/"
1060 1104.972187  172.30.0.2   172.30.0.10  FTP      65 Request: CWD /Docs
1061 1104.973142  172.30.0.10  172.30.0.2   FTP     105 Response: 250 CWD successful. "/Docs" is current directory.
```

```
> Frame 1047: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
> Ethernet II, Src: Vmware_ab:4d:a3 (00:50:56:ab:4d:a3), Dst: Vmware_ab:5c:5c (00:50:56:ab:5c:5c)
> Internet Protocol Version 4, Src: 172.30.0.10, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 8521, Seq: 494, Ack: 88, Len: 49
v File Transfer Protocol (FTP)
  v 227 Entering Passive Mode (172,30,0,10,167,136)\r\n
      Response code: Entering Passive Mode (227)
      Response arg: Entering Passive Mode (172,30,0,10,167,136)
      Passive IP address: 172.30.0.10
      Passive port: 42888
  [Current working directory: /]
  [Command: MLSD]
  [Command frame: 1048]
```

```
0000  00 50 56 ab 5c 5c 00 50  56 ab 4d a3 08 00 45 02   ·PV·\\·P V·M···E·
0010  00 59 0b b4 40 00 80 06  96 a0 ac 1e 00 0a ac 1e   ·Y··@··· ········
0020  00 02 00 15 21 49 95 e6  3b 2f 00 9b 91 f4 50 18   ····!I·· ;/····P·
0030  20 14 3b e4 00 00 32 32  37 20 45 6e 74 65 72 69    ·;···22 7 Enteri
0040  6e 67 20 50 61 73 73 69  76 65 20 4d 6f 64 65 20   ng Passi ve Mode 
0050  28 31 37 32 2c 33 30 2c  30 2c 31 30 2c 31 36 37   (172,30, 0,10,167
0060  2c 31 33 36 29 0d 0a                               ,136)··
```

```
Text item (text), 49 bytes    Packets: 1778 · Displayed: 66 (3.7%) · Dropped: 0 (0.0%)    Profile: Default
```

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


marky_CaptureFileS1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
ftp-data
```

```
No.  Time         Source       Destination  Protocol Length Info
1053 1077.308578  172.30.0.10  172.30.0.2   FTP-DA…  282 FTP Data: 228 bytes (PASV) (MLSD)
1115 1144.172817  172.30.0.2   172.30.0.10  FTP-DA…  108 FTP Data: 54 bytes (PASV) (STOR adminFile.txt)
1132 1144.180527  172.30.0.10  172.30.0.2   FTP-DA…  110 FTP Data: 56 bytes (PASV) (MLSD)
```

```
> Frame 1115: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0
> Ethernet II, Src: Vmware_ab:5c:5c (00:50:56:ab:5c:5c), Dst: Vmware_ab:4d:a3 (00:50:56:ab:4d:a3)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.10
v Transmission Control Protocol, Src Port: 8525, Dst Port: 55757, Seq: 1, Ack: 1, Len: 54
    Source Port: 8525
    Destination Port: 55757
    [Stream index: 21]
    [TCP Segment Len: 54]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 55    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 32768
    [Calculated window size: 4194304]
    [Window size scaling factor: 128]
```

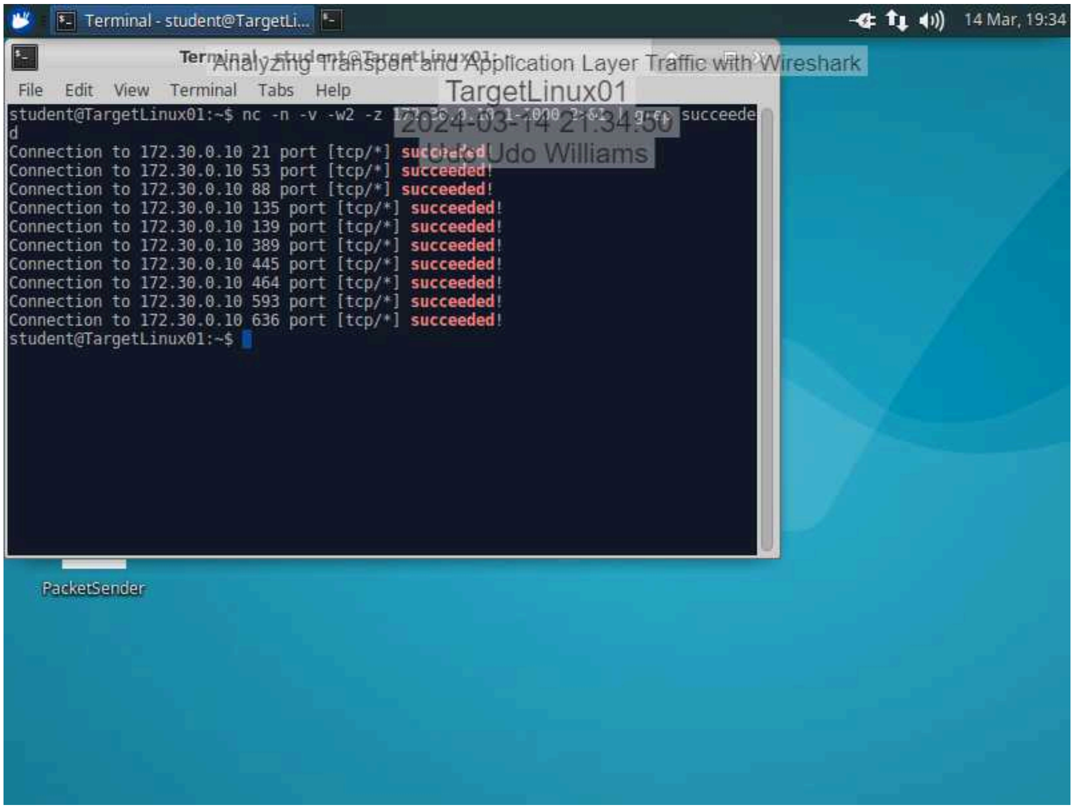
```
0000  00 50 56 ab 4d a3 00 50  56 ab 5c 5c 08 00 45 02   ·PV·M··P V·\\··E·
0010  00 5e 0a 78 40 00 80 06  97 d7 ac 1e 00 02 ac 1e   ·^·x@··· ········
0020  00 0a 21 4d d9 cd 20 3b  d1 d2 7e ac 5d 0f 50 18   ··!M·· ; ··~·]·P·
0030  80 00 84 94 00 00 22 74  65 73 74 20 66 69 6c 65   ······"t est file
0040  20 66 6f 72 20 74 72 61  6e 73 66 65 72 73 20 66    for tra nsfers f
0050  72 6f 6d 20 41 64 6d 69  6e 69 73 74 72 61 74 6f   rom Admi nistrato
0060  72 20 66 6f 6c 64 65 72  22 20 0d 0a               r folder " ··
```

```
Destination Port (tcp.dstport), 2 bytes    Packets: 1778 · Displayed: 3 (0.2%) · Dropped: 0 (0.0%)    Profile: Default
```

Section 2: Applied Learning

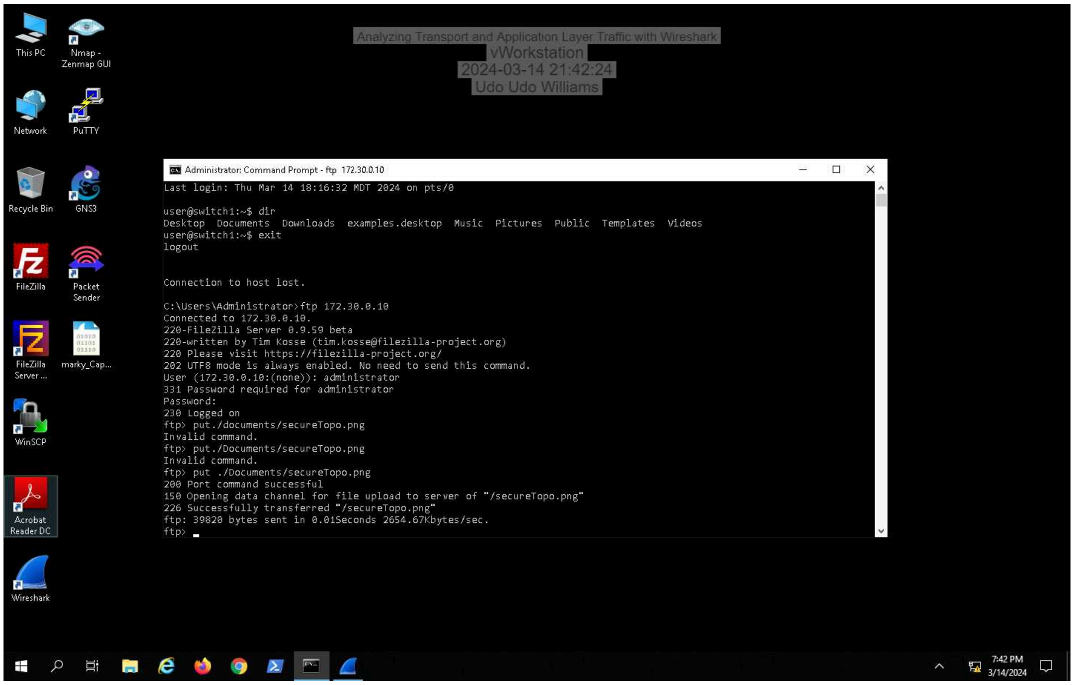
Part 1: Configure Wireshark and Generate Network Traffic

7. **Make a screen capture** showing the **successfully executed netcat command**.


Terminal - student@TargetLi...
14 Mar, 19:34
Terminal - student@TargetLinux01: ~
File
Edit
View
Terminal
Tabs
Help
Analyzing Transport and Application Layer Traffic with Wireshark
TargetLinux01
2024-03-14 21:34:50
Udo Williams
PacketSender

```
student@TargetLinux01:~$ nc -n -v -w2 -z 172.30.0.10 1-1000 2>&1 | grep succeede
d
Connection to 172.30.0.10 21 port [tcp/*] succeeded!
Connection to 172.30.0.10 53 port [tcp/*] succeeded!
Connection to 172.30.0.10 88 port [tcp/*] succeeded!
Connection to 172.30.0.10 135 port [tcp/*] succeeded!
Connection to 172.30.0.10 139 port [tcp/*] succeeded!
Connection to 172.30.0.10 389 port [tcp/*] succeeded!
Connection to 172.30.0.10 445 port [tcp/*] succeeded!
Connection to 172.30.0.10 464 port [tcp/*] succeeded!
Connection to 172.30.0.10 593 port [tcp/*] succeeded!
Connection to 172.30.0.10 636 port [tcp/*] succeeded!
student@TargetLinux01:~$
```

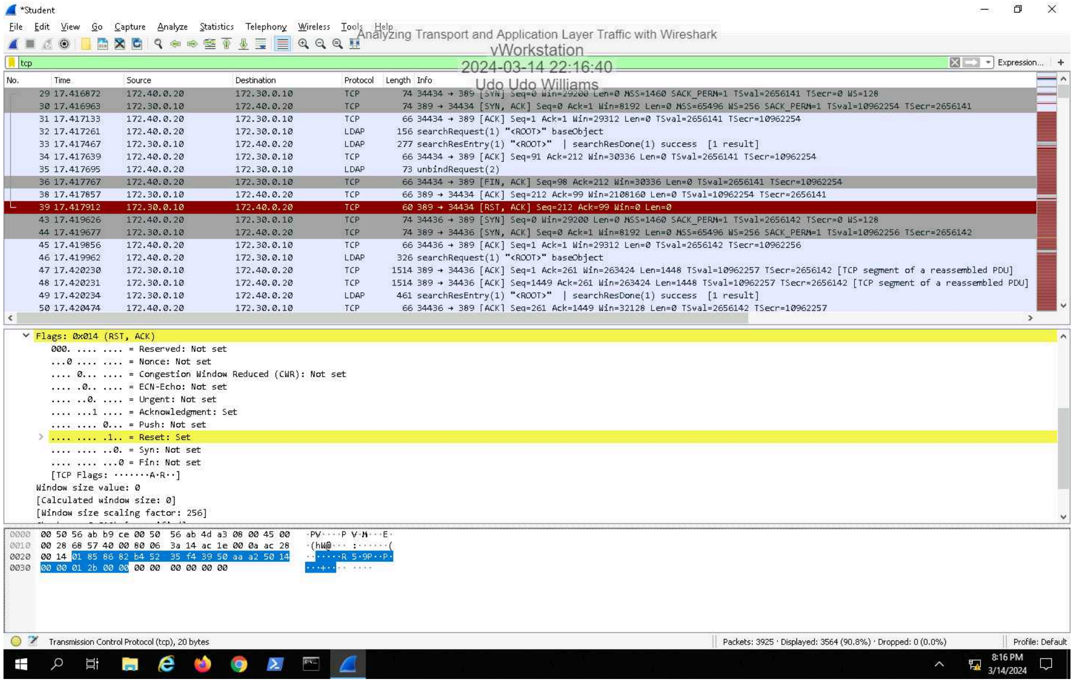
20. **Make a screen capture** showing the **successful transfer in the Command Prompt output**.



```
Last login: Thu Mar 14 18:16:32 MDT 2024 on pts/0

user@switch1:~$ dir
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
user@switch1:~$ exit
logout


Connection to host lost.

C:\Users\Administrator>ftp 172.30.0.10
Connected to 172.30.0.10.
220-FileZilla Server 0.9.59 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
202 UTF8 mode is always enabled. No need to send this command.
User (172.30.0.10:(none)): administrator
331 Password required for administrator
Password:
230 Logged on
ftp> put./documents/secureTopo.png
Invalid command.
ftp> put./Documents/secureTopo.png
Invalid command.
ftp> put ./Documents/secureTopo.png
200 Port command successful
150 Opening data channel for file upload to server of "/secureTopo.png"
226 Successfully transferred "/secureTopo.png"
ftp: 39820 bytes sent in 0.01Seconds 2654.67Kbytes/sec.
ftp>
```

Part 2: Perform Protocol Analysis using Wireshark

5. **Make a screen capture** showing the **TCP flags set in the Packet Details pane for the first RST packet**.


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 22:16:40
Udo Udo Williams
Expression...
+
8:16 PM
3/14/2024

tcp

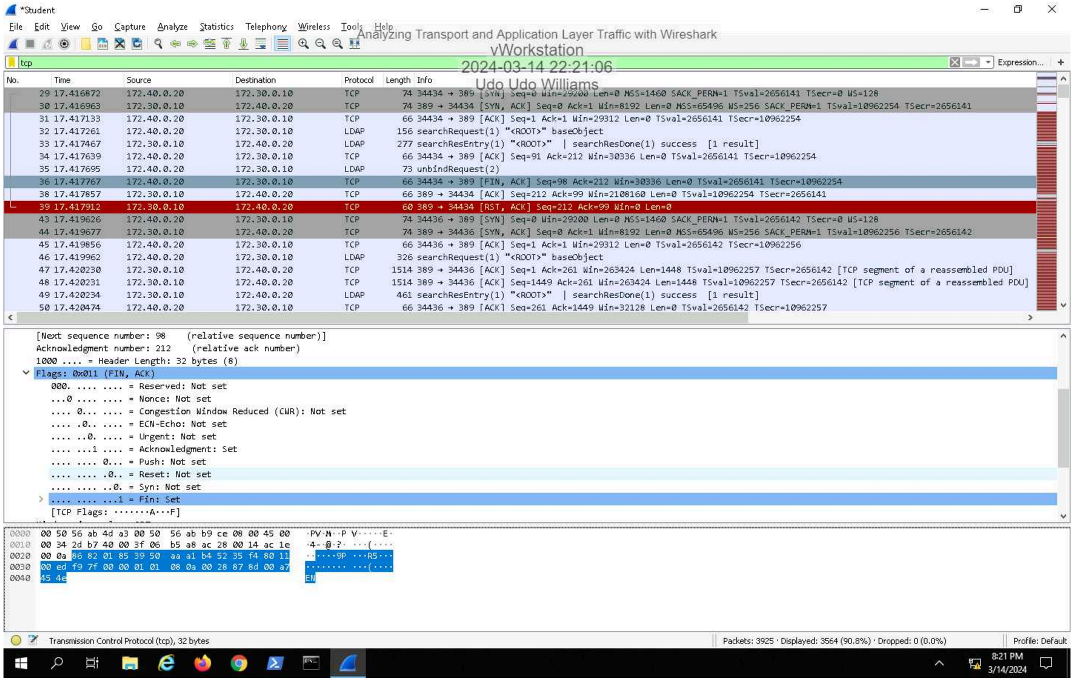
```
No.      Time          Source        Destination   Protocol  Length  Info
     29 17.416872     172.40.0.20   172.30.0.10   TCP        74 34434 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2656141 TSecr=0 WS=128
     30 17.416963     172.30.0.10   172.40.0.20   TCP        74 389 → 34434 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65496 WS=256 SACK_PERM=1 TSval=10962254 TSecr=2656141
     31 17.417133     172.40.0.20   172.30.0.10   TCP        66 34434 → 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2656141 TSecr=10962254
     32 17.417261     172.40.0.20   172.30.0.10   LDAP      156 searchRequest(1) "<ROOT>" baseObject
     33 17.417467     172.30.0.10   172.40.0.20   LDAP      277 searchResEntry(1) "<ROOT>"  | searchResDone(1) success  [1 result]
     34 17.417639     172.40.0.20   172.30.0.10   TCP        66 34434 → 389 [ACK] Seq=91 Ack=212 Win=30336 Len=0 TSval=2656141 TSecr=10962254
     35 17.417695     172.40.0.20   172.30.0.10   LDAP       73 unbindRequest(2)
     36 17.417767     172.40.0.20   172.30.0.10   TCP        66 34434 → 389 [FIN, ACK] Seq=98 Ack=212 Win=30336 Len=0 TSval=2656141 TSecr=10962254
     38 17.417857     172.30.0.10   172.40.0.20   TCP        66 389 → 34434 [ACK] Seq=212 Ack=99 Win=2108160 Len=0 TSval=10962254 TSecr=2656141
     39 17.417912     172.30.0.10   172.40.0.20   TCP        60 389 → 34434 [RST, ACK] Seq=212 Ack=99 Win=0 Len=0
     43 17.419626     172.40.0.20   172.30.0.10   TCP        74 34436 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2656142 TSecr=0 WS=128
     44 17.419677     172.30.0.10   172.40.0.20   TCP        74 389 → 34436 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65496 WS=256 SACK_PERM=1 TSval=10962256 TSecr=2656142
     45 17.419856     172.40.0.20   172.30.0.10   TCP        66 34436 → 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2656142 TSecr=10962256
     46 17.419962     172.40.0.20   172.30.0.10   LDAP      326 searchRequest(1) "<ROOT>" baseObject
     47 17.420230     172.30.0.10   172.40.0.20   TCP      1514 389 → 34436 [ACK] Seq=1 Ack=261 Win=263424 Len=1448 TSval=10962257 TSecr=2656142 [TCP segment of a reassembled PDU]
     48 17.420231     172.30.0.10   172.40.0.20   TCP      1514 389 → 34436 [ACK] Seq=1449 Ack=261 Win=263424 Len=1448 TSval=10962257 TSecr=2656142 [TCP segment of a reassembled PDU]
     49 17.420234     172.30.0.10   172.40.0.20   LDAP      461 searchResEntry(1) "<ROOT>"  | searchResDone(1) success  [1 result]
     50 17.420474     172.40.0.20   172.30.0.10   TCP        66 34436 → 389 [ACK] Seq=261 Ack=1449 Win=32128 Len=0 TSval=2656142 TSecr=10962257
```

```
  Flags: 0x014 (RST, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .1.. = Reset: Set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······A·R··]
  Window size value: 0
  [Calculated window size: 0]
  [Window size scaling factor: 256]
```

```
0000  00 50 56 ab b9 ce 00 50  56 ab 4d a3 08 00 45 00   ·PV····P V·M···E·
0010  00 28 68 57 40 00 80 06  3a 14 ac 1e 00 0a ac 28   ·(hW@··· :······(
0020  00 14 01 85 86 82 b4 52  35 f4 39 50 aa a2 50 14   ·······R 5·9P··P·
0030  00 00 01 2b 00 00 00 00  00 00 00 00               ···+···· ····
```

Transmission Control Protocol (tcp), 20 bytes | Packets: 3925 · Displayed: 3564 (90.8%) · Dropped: 0 (0.0%) | Profile: Default

10. **Make a screen capture** showing the **FIN and ACK flags set in the Packet Details View**.


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 22:21:06
Udo Udo Williams
tcp
Expression...
8:21 PM
3/14/2024

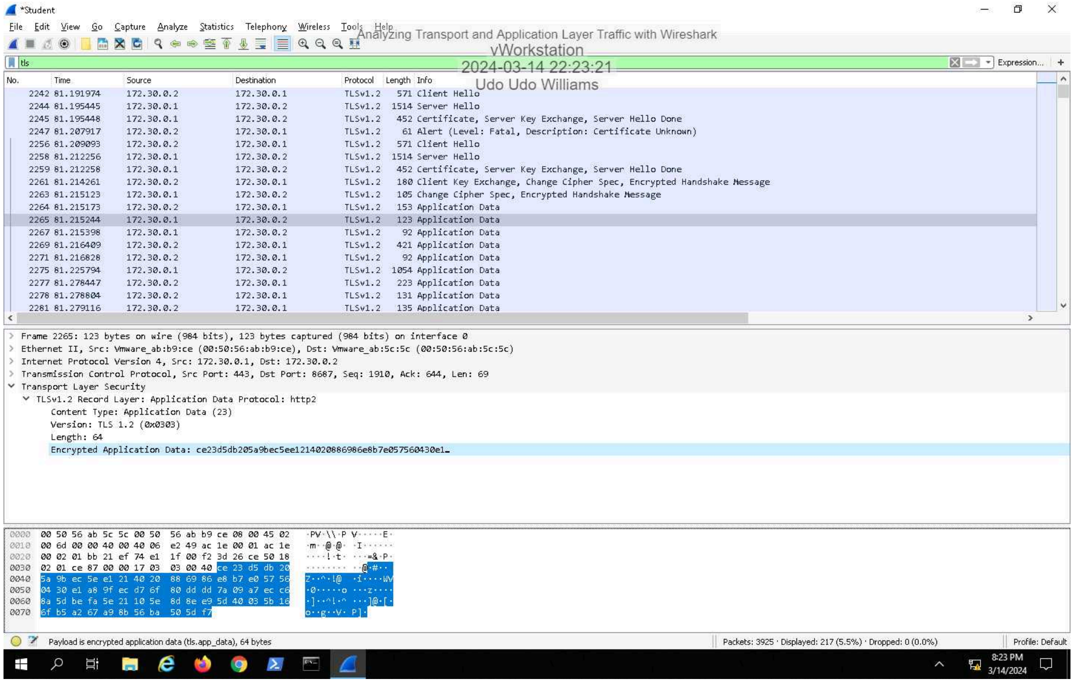
```
No.   Time       Source       Destination  Protocol Length Info
   29 17.416872  172.40.0.20  172.30.0.10  TCP        74 34434 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2656141 TSecr=0 WS=128
   30 17.416963  172.30.0.10  172.40.0.20  TCP        74 389 → 34434 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65496 WS=256 SACK_PERM=1 TSval=10962254 TSecr=2656141
   31 17.417133  172.40.0.20  172.30.0.10  TCP        66 34434 → 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2656141 TSecr=10962254
   32 17.417261  172.40.0.20  172.30.0.10  LDAP      156 searchRequest(1) "<ROOT>" baseObject
   33 17.417467  172.30.0.10  172.40.0.20  LDAP      277 searchResEntry(1) "<ROOT>"  | searchResDone(1) success  [1 result]
   34 17.417639  172.40.0.20  172.30.0.10  TCP        66 34434 → 389 [ACK] Seq=91 Ack=212 Win=30336 Len=0 TSval=2656141 TSecr=10962254
   35 17.417695  172.40.0.20  172.30.0.10  LDAP       73 unbindRequest(2)
   36 17.417767  172.40.0.20  172.30.0.10  TCP        66 34434 → 389 [FIN, ACK] Seq=98 Ack=212 Win=30336 Len=0 TSval=2656141 TSecr=10962254
   38 17.417857  172.30.0.10  172.40.0.20  TCP        66 389 → 34434 [ACK] Seq=212 Ack=99 Win=2108160 Len=0 TSval=10962254 TSecr=2656141
   39 17.417912  172.30.0.10  172.40.0.20  TCP        60 389 → 34434 [RST, ACK] Seq=212 Ack=99 Win=0 Len=0
   43 17.419626  172.40.0.20  172.30.0.10  TCP        74 34436 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2656142 TSecr=0 WS=128
   44 17.419677  172.30.0.10  172.40.0.20  TCP        74 389 → 34436 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65496 WS=256 SACK_PERM=1 TSval=10962256 TSecr=2656142
   45 17.419856  172.40.0.20  172.30.0.10  TCP        66 34436 → 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2656142 TSecr=10962256
   46 17.419962  172.40.0.20  172.30.0.10  LDAP      326 searchRequest(1) "<ROOT>" baseObject
   47 17.420230  172.30.0.10  172.40.0.20  TCP      1514 389 → 34436 [ACK] Seq=1 Ack=261 Win=263424 Len=1448 TSval=10962257 TSecr=2656142 [TCP segment of a reassembled PDU]
   48 17.420231  172.30.0.10  172.40.0.20  TCP      1514 389 → 34436 [ACK] Seq=1449 Ack=261 Win=263424 Len=1448 TSval=10962257 TSecr=2656142 [TCP segment of a reassembled PDU]
   49 17.420234  172.30.0.10  172.40.0.20  LDAP      461 searchResEntry(1) "<ROOT>"  | searchResDone(1) success  [1 result]
   50 17.420474  172.40.0.20  172.30.0.10  TCP        66 34436 → 389 [ACK] Seq=261 Ack=1449 Win=32128 Len=0 TSval=2656142 TSecr=10962257
```

```
    [Next sequence number: 98    (relative sequence number)]
    Acknowledgment number: 212    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x011 (FIN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
    > .... .... ...1 = Fin: Set
      [TCP Flags: ·······A···F]
```

```
0000  00 50 56 ab 4d a3 00 50  56 ab b9 ce 08 00 45 00   ·PV·M··P V·····E·
0010  00 34 2d b7 40 00 3f 06  b5 a8 ac 28 00 14 ac 1e   ·4-·@·?· ···(····
0020  00 0a 86 82 01 85 39 50  aa a1 b4 52 35 f4 80 11   ······9P ···R5···
0030  00 ed f9 7f 00 00 01 01  08 0a 00 28 87 8d 00 a7   ········ ···(····
0040  45 4e                                              EN
```

Transmission Control Protocol (tcp), 32 bytes | Packets: 3925 · Displayed: 3564 (90.8%) · Dropped: 0 (0.0%) | Profile: Default

16. **Make a screen capture** showing the **highlighted Encrypted Application Data in the Packet Bytes pane**.


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 22:23:21
Udo Udo Williams
tls
Expression...
8:23 PM
3/14/2024

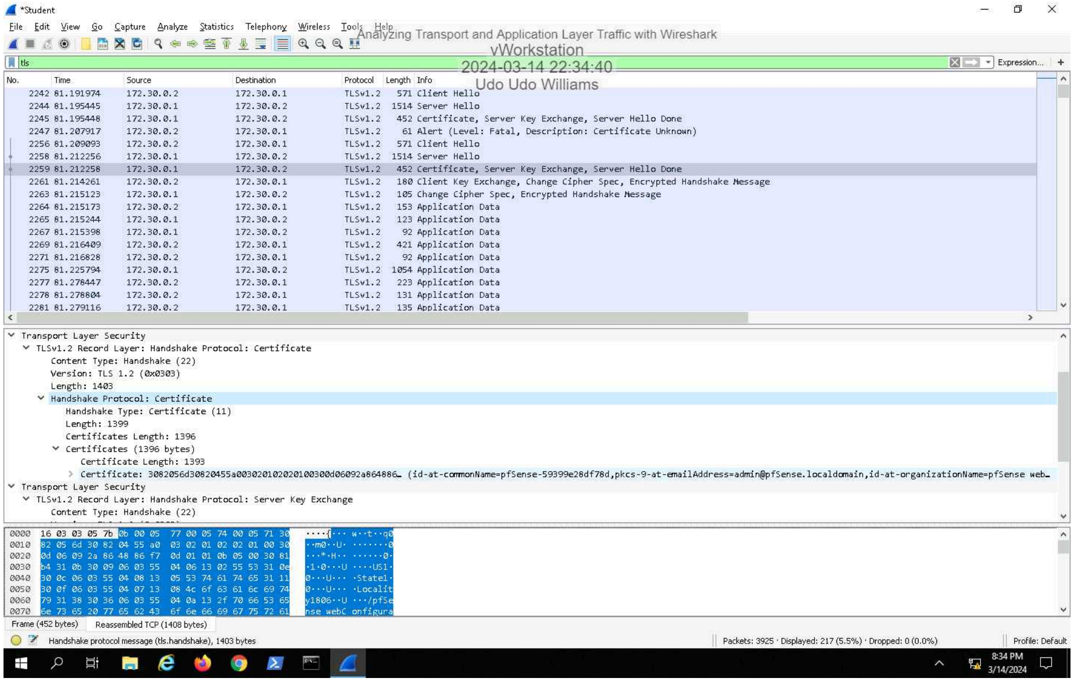
```
No.   Time       Source      Destination Protocol Length Info
 2242 81.191974  172.30.0.2  172.30.0.1  TLSv1.2   571 Client Hello
 2244 81.195445  172.30.0.1  172.30.0.2  TLSv1.2  1514 Server Hello
 2245 81.195448  172.30.0.1  172.30.0.2  TLSv1.2   452 Certificate, Server Key Exchange, Server Hello Done
 2247 81.207917  172.30.0.2  172.30.0.1  TLSv1.2    61 Alert (Level: Fatal, Description: Certificate Unknown)
 2256 81.209093  172.30.0.2  172.30.0.1  TLSv1.2   571 Client Hello
 2258 81.212256  172.30.0.1  172.30.0.2  TLSv1.2  1514 Server Hello
 2259 81.212258  172.30.0.1  172.30.0.2  TLSv1.2   452 Certificate, Server Key Exchange, Server Hello Done
 2261 81.214261  172.30.0.2  172.30.0.1  TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 2263 81.215123  172.30.0.1  172.30.0.2  TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
 2264 81.215173  172.30.0.2  172.30.0.1  TLSv1.2   153 Application Data
 2265 81.215244  172.30.0.1  172.30.0.2  TLSv1.2   123 Application Data
 2267 81.215398  172.30.0.1  172.30.0.2  TLSv1.2    92 Application Data
 2269 81.216409  172.30.0.2  172.30.0.1  TLSv1.2   421 Application Data
 2271 81.216828  172.30.0.2  172.30.0.1  TLSv1.2    92 Application Data
 2275 81.225794  172.30.0.1  172.30.0.2  TLSv1.2  1054 Application Data
 2277 81.278447  172.30.0.2  172.30.0.1  TLSv1.2   223 Application Data
 2278 81.278804  172.30.0.2  172.30.0.1  TLSv1.2   131 Application Data
 2281 81.279116  172.30.0.2  172.30.0.1  TLSv1.2   135 Application Data
```

```
> Frame 2265: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface 0
> Ethernet II, Src: Vmware_ab:b9:ce (00:50:56:ab:b9:ce), Dst: Vmware_ab:5c:5c (00:50:56:ab:5c:5c)
> Internet Protocol Version 4, Src: 172.30.0.1, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 443, Dst Port: 8687, Seq: 1910, Ack: 644, Len: 69
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: http2
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 64
      Encrypted Application Data: ce23d5db205a9bec5ee1214020886986e8b7e057560430e1…
```

```
0000  00 50 56 ab 5c 5c 00 50  56 ab b9 ce 08 00 45 02   ·PV·\\·P V·····E·
0010  00 6d 00 00 40 00 40 06  e2 49 ac 1e 00 01 ac 1e   ·m··@·@· ·I······
0020  00 02 01 bb 21 ef 74 e1  1f 00 f2 3d 26 ce 50 18   ····!·t· ···=&·P·
0030  02 01 ce 87 00 00 17 03  03 00 40 ce 23 d5 db 20   ········ ··@·#··
0040  5a 9b ec 5e e1 21 40 20  88 69 86 e8 b7 e0 57 56   Z··^·!@  ·i····WV
0050  04 30 e1 a8 9f ec d7 6f  80 dd dd 7a 09 a7 ec c6   ·0·····o ···z····
0060  8a 5d be fa 5e 21 10 5e  8d 8e e9 5d 40 03 5b 16   ·]··^!·^ ···]@·[·
0070  6f b5 a2 67 a9 8b 56 ba  50 5d f7                  o··g··V· P]·
```

Payload is encrypted application data (tls.app_data), 64 bytes | Packets: 3925 · Displayed: 217 (5.5%) · Dropped: 0 (0.0%) | Profile: Default

22. **Make a screen capture** showing the **certificate details in the Packet Details pane**.


*Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 22:34:40
Udo Udo Williams
Expression…
8:34 PM
3/14/2024

Filter: tls

```
No.   Time      Source       Destination  Protocol Length Info
 2242 81.191974 172.30.0.2   172.30.0.1   TLSv1.2   571 Client Hello
 2244 81.195445 172.30.0.1   172.30.0.2   TLSv1.2  1514 Server Hello
 2245 81.195448 172.30.0.1   172.30.0.2   TLSv1.2   452 Certificate, Server Key Exchange, Server Hello Done
 2247 81.207917 172.30.0.2   172.30.0.1   TLSv1.2    61 Alert (Level: Fatal, Description: Certificate Unknown)
 2256 81.209093 172.30.0.2   172.30.0.1   TLSv1.2   571 Client Hello
 2258 81.212256 172.30.0.1   172.30.0.2   TLSv1.2  1514 Server Hello
 2259 81.212258 172.30.0.1   172.30.0.2   TLSv1.2   452 Certificate, Server Key Exchange, Server Hello Done
 2261 81.214261 172.30.0.2   172.30.0.1   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 2263 81.215123 172.30.0.1   172.30.0.2   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
 2264 81.215173 172.30.0.2   172.30.0.1   TLSv1.2   153 Application Data
 2265 81.215244 172.30.0.1   172.30.0.2   TLSv1.2   123 Application Data
 2267 81.215398 172.30.0.1   172.30.0.2   TLSv1.2    92 Application Data
 2269 81.216409 172.30.0.2   172.30.0.1   TLSv1.2   421 Application Data
 2271 81.216828 172.30.0.2   172.30.0.1   TLSv1.2    92 Application Data
 2275 81.225794 172.30.0.1   172.30.0.2   TLSv1.2  1054 Application Data
 2277 81.278447 172.30.0.2   172.30.0.1   TLSv1.2   223 Application Data
 2278 81.278804 172.30.0.2   172.30.0.1   TLSv1.2   131 Application Data
 2281 81.279116 172.30.0.2   172.30.0.1   TLSv1.2   135 Application Data
```

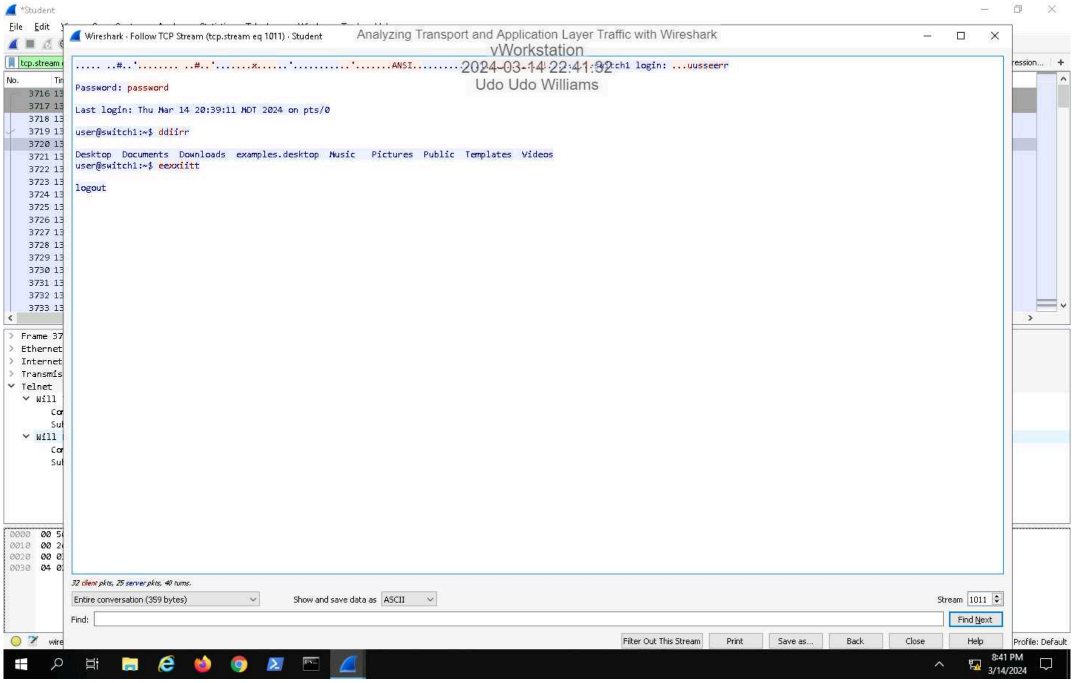
```
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 1403
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1399
        Certificates Length: 1396
      v Certificates (1396 bytes)
          Certificate Length: 1393
        > Certificate: 3082056d30820455a003020102020100300d06092a864886… (id-at-commonName=pfSense-59399e28df78d,pkcs-9-at-emailAddress=admin@pfSense.localdomain,id-at-organizationName=pfSense web…
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
```

```
0000  16 03 03 05 7b 0b 00 05  77 00 05 74 00 05 71 30   ····{··· w··t··q0
0010  82 05 6d 30 82 04 55 a0  03 02 01 02 02 01 00 30   ··m0··U· ·······0
0020  0d 06 09 2a 86 48 86 f7  0d 01 01 0b 05 00 30 81   ···*·H·· ······0·
0030  b4 31 0b 30 09 06 03 55  04 06 13 02 55 53 31 0e   ·1·0···U ····US1·
0040  30 0c 06 03 55 04 08 13  05 53 74 61 74 65 31 11   0···U··· ·State1·
0050  30 0f 06 03 55 04 07 13  08 4c 6f 63 61 6c 69 74   0···U··· ·Localit
0060  79 31 38 30 36 06 03 55  04 0a 13 2f 70 66 53 65   y1806··U ···/pfSe
0070  6e 73 65 20 77 65 62 43  6f 6e 66 69 67 75 72 61   nse webC onfigura
```

Frame (452 bytes) | Reassembled TCP (1408 bytes)

Handshake protocol message (tls.handshake), 1403 bytes | Packets: 3925 · Displayed: 217 (5.5%) · Dropped: 0 (0.0%) | Profile: Default

25. **Make a screen capture** showing the **complete set of data in the TCP Stream window**.



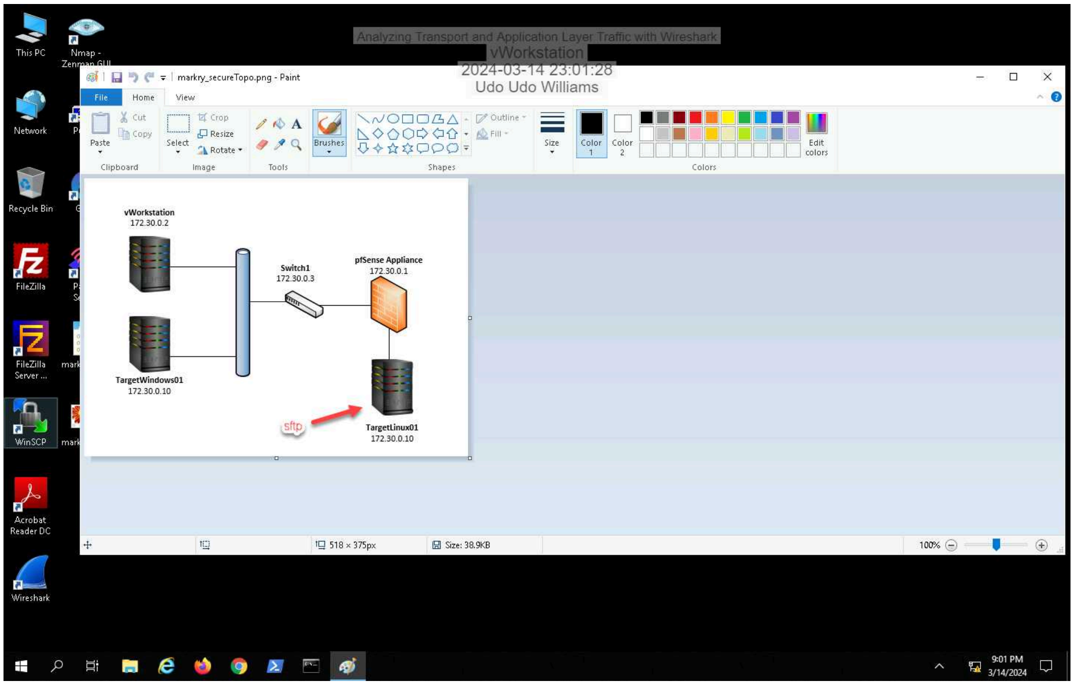
```
..... ..#..'........ ..#..'.......x......'..........'.......ANSI........switch1 login: ...uusseerr

Password: password

Last login: Thu Mar 14 20:39:11 MDT 2024 on pts/0

user@switch1:~$ ddiirr

Desktop  Documents  Downloads  examples.desktop  Music   Pictures  Public  Templates  Videos
user@switch1:~$ eexxiitt

logout
```

32 client pkts, 25 server pkts, 40 turns.

Entire conversation (359 bytes) | Show and save data as: ASCII | Stream: 1011

Find:

36. **Make a screen capture** showing the **reconstituted PNG file**.



Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 23:01:28
Udo Udo Williams

markry_secureTopo.png - Paint

518 × 375px

Size: 38.9KB

100%

Section 3: Challenge and Analysis

Part 1: Locate a Target RAR File Transfer in a Packet Capture

Record the file signature you used to find the RAR archive.

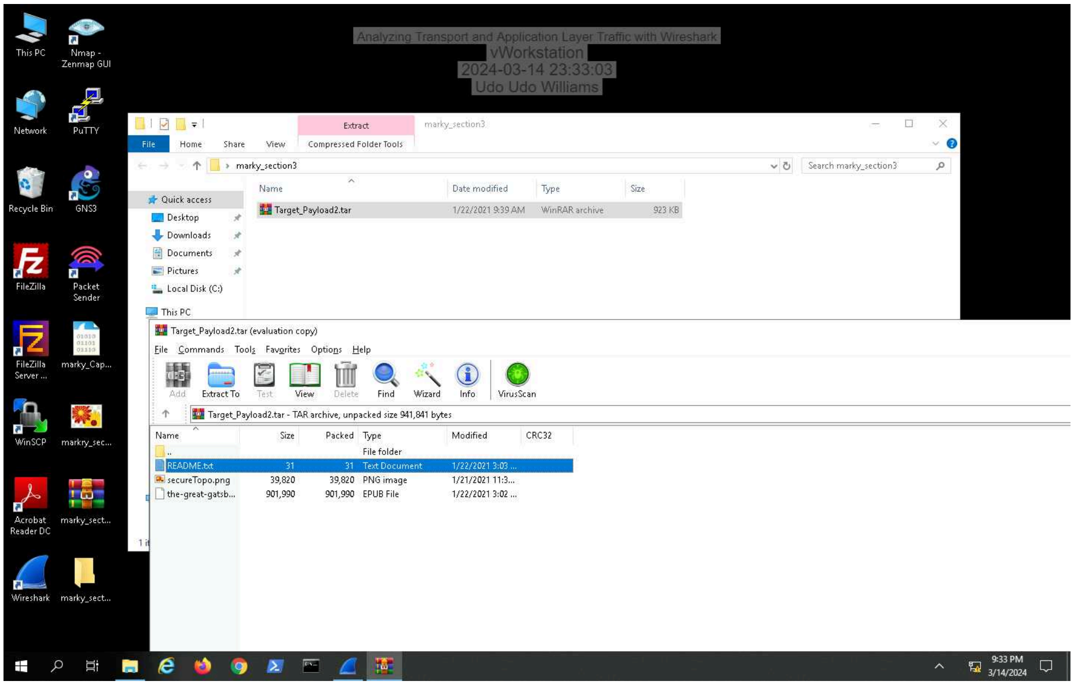
52 61 72 21 1A 07 01 00

Record the name of the correct RAR archive file.

Stor Target_payload2.rar

Part 2: Reassemble the RAR Archive from its Constituent Bytes

Make a screen capture showing the **contents of the tar file**.



Analyzing Transport and Application Layer Traffic with Wireshark
vWorkstation
2024-03-14 23:33:03
Udo Udo Williams

Name	Date modified	Type	Size
Target_Payload2.tar	1/22/2021 9:39 AM	WinRAR archive	923 KB

Target_Payload2.tar (evaluation copy)

Target_Payload2.tar - TAR archive, unpacked size 941,841 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
README.txt	31	31	Text Document	1/22/2021 3:03 ...	
secureTopo.png	39,820	39,820	PNG image	1/21/2021 11:3...	
the-great-gatsb...	901,990	901,990	EPUB File	1/22/2021 3:02 ...	

Record the passphrase discovered in the **README.txt file**.

the code is {JBL-80802600-SaaS}