

Student:

Enrique Mejia

Email:

enriquem2260@gmail.com

Time on Task:

1 hour, 33 minutes

Progress:

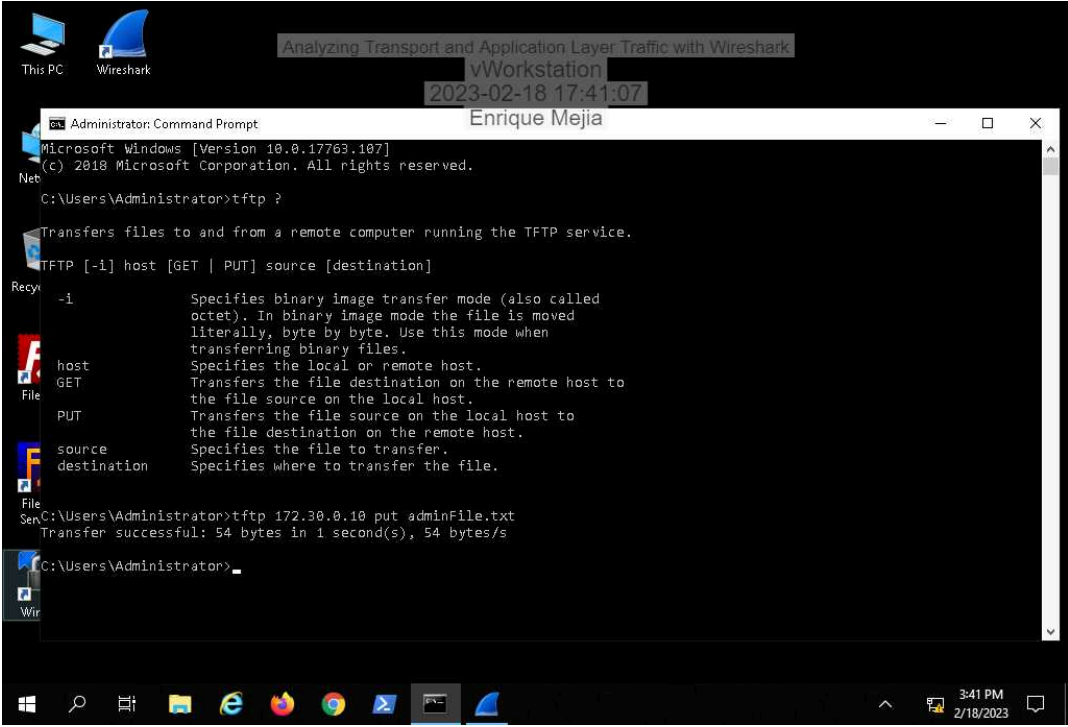
100%

Report Generated: Saturday, February 18, 2023 at 8:04 PM

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**.



The screenshot shows a Windows desktop with a taskbar at the bottom. The taskbar includes icons for This PC, Wireshark, and several web browsers. A Command Prompt window is open, displaying the following text:

```
Administrator: 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.

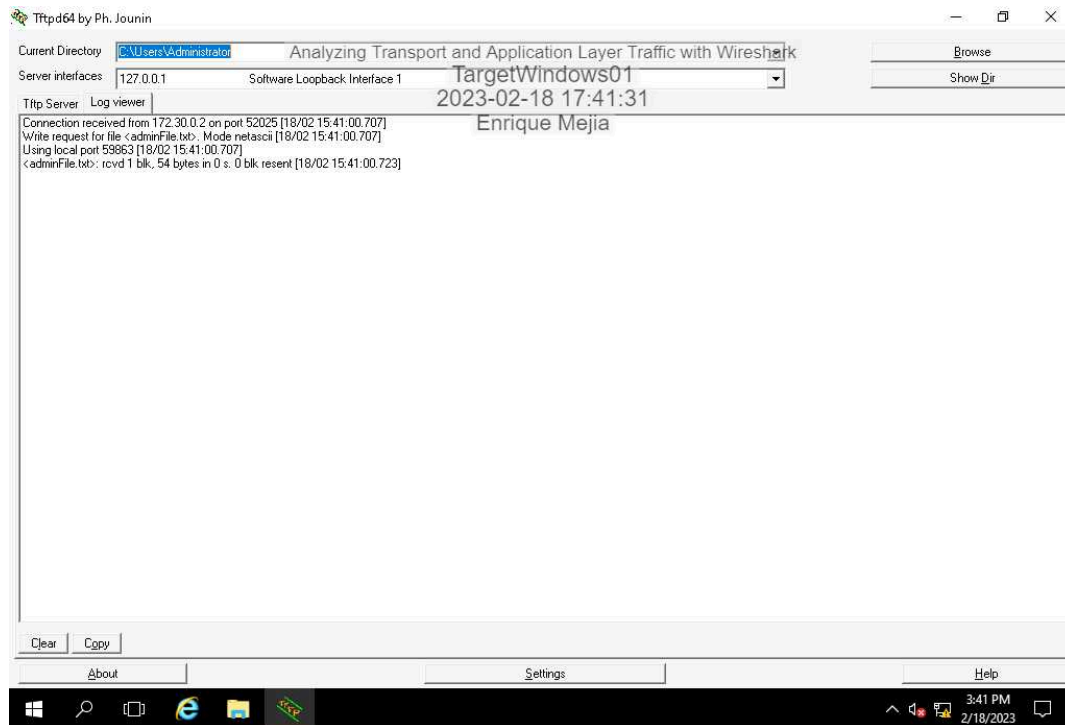
TFTP [-i] host [GET | PUT] source [destination]

-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.

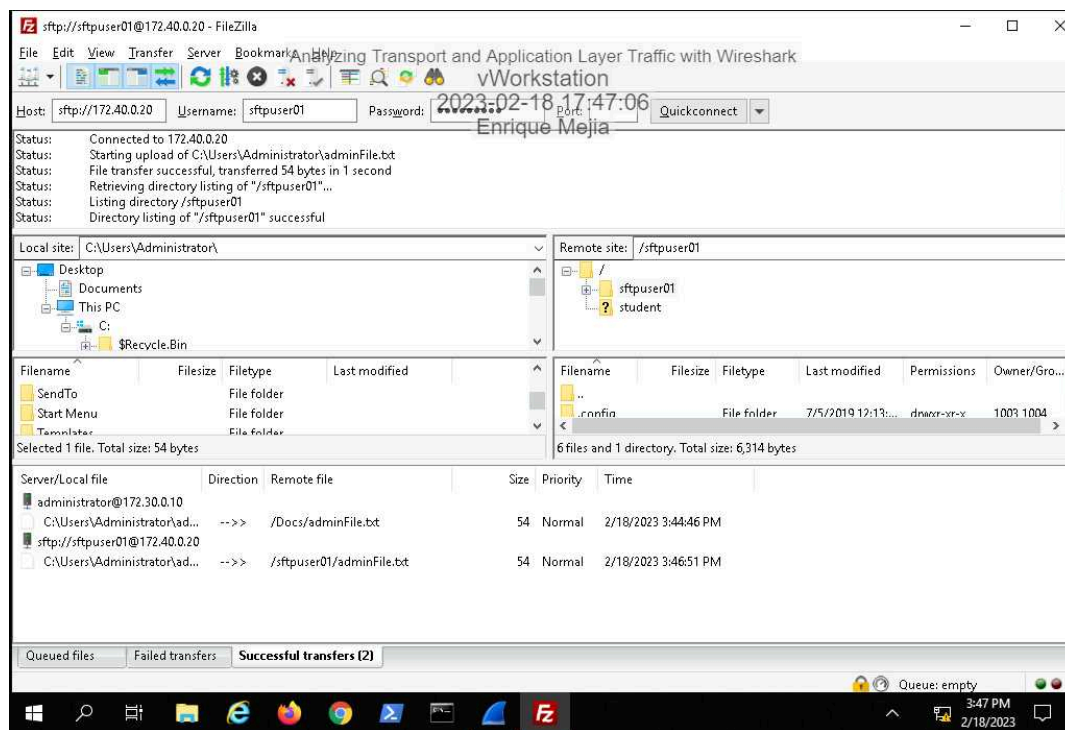
C:\Users\Administrator>tftp 172.30.0.10 put adminFile.txt
Transfer successful: 54 bytes in 1 second(s), 54 bytes/s

C:\Users\Administrator>
```

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

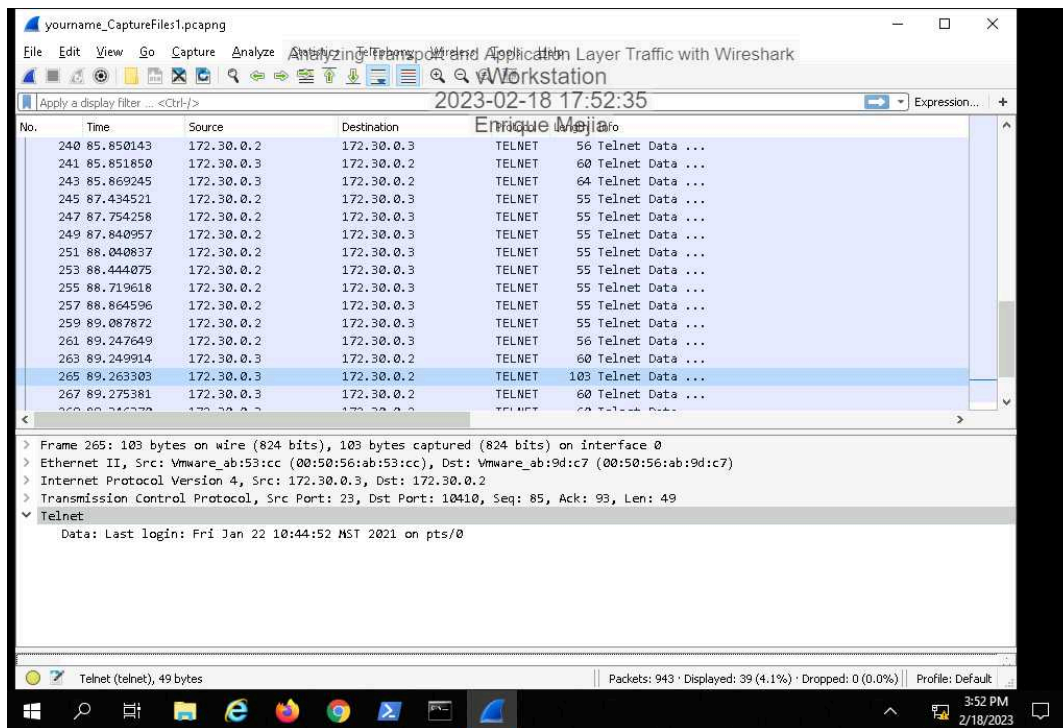


45. Make a screen capture showing the successful SFTP file transfer.

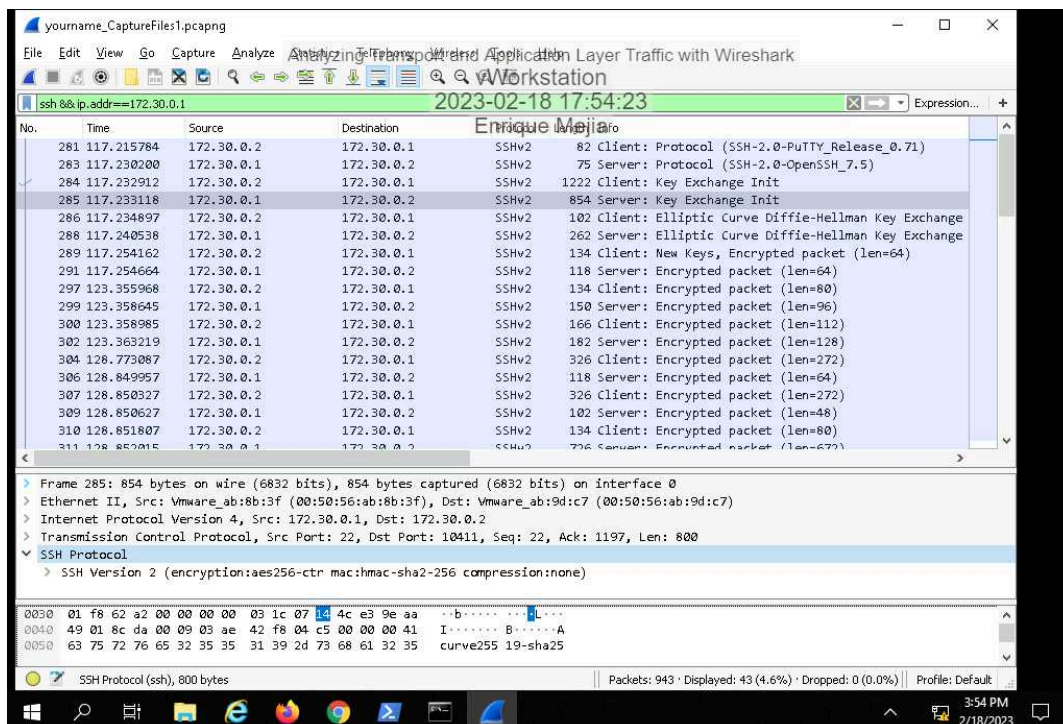


Part 2: Perform Protocol Analysis using Wireshark

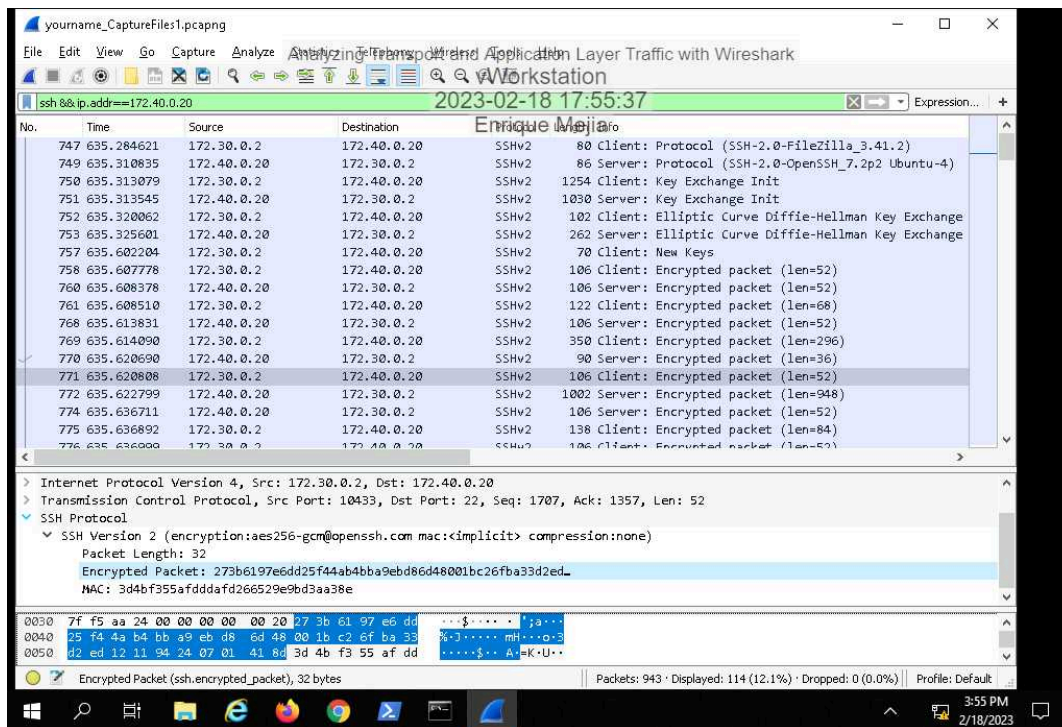
5. Make a screen capture showing the **Last Login** information in the Packet Details pane.



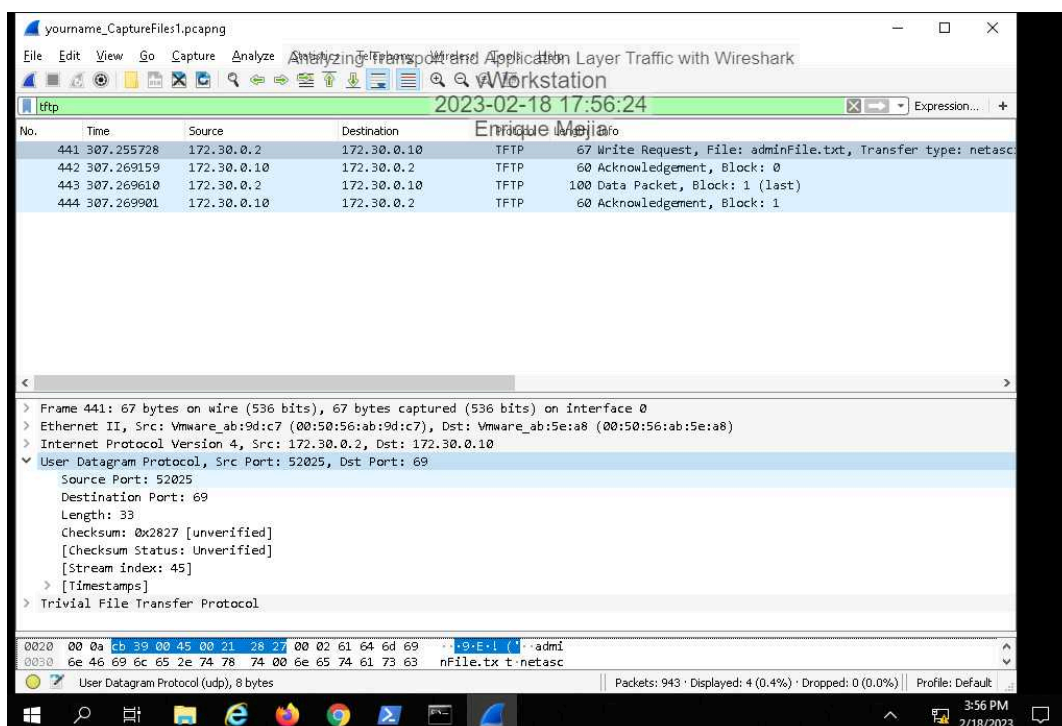
11. Make a screen capture showing the SSHv2 encryption and mac selections for the SSH connection.



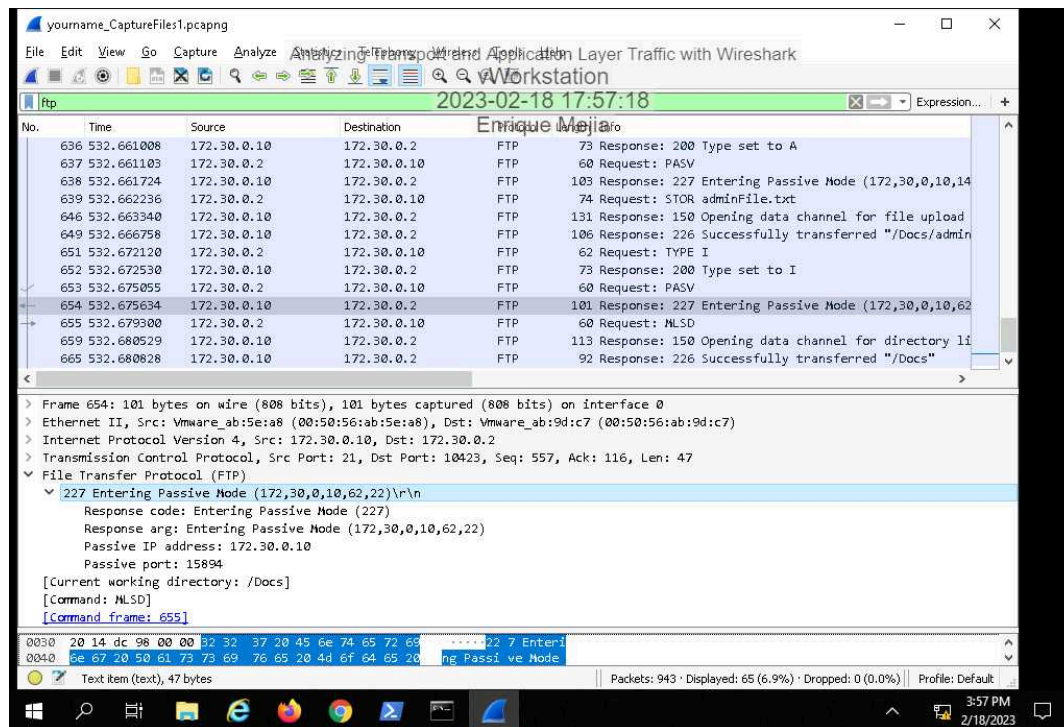
16. Make a screen capture showing the **highlighted (encrypted) data** in the **Packet Bytes** pane.



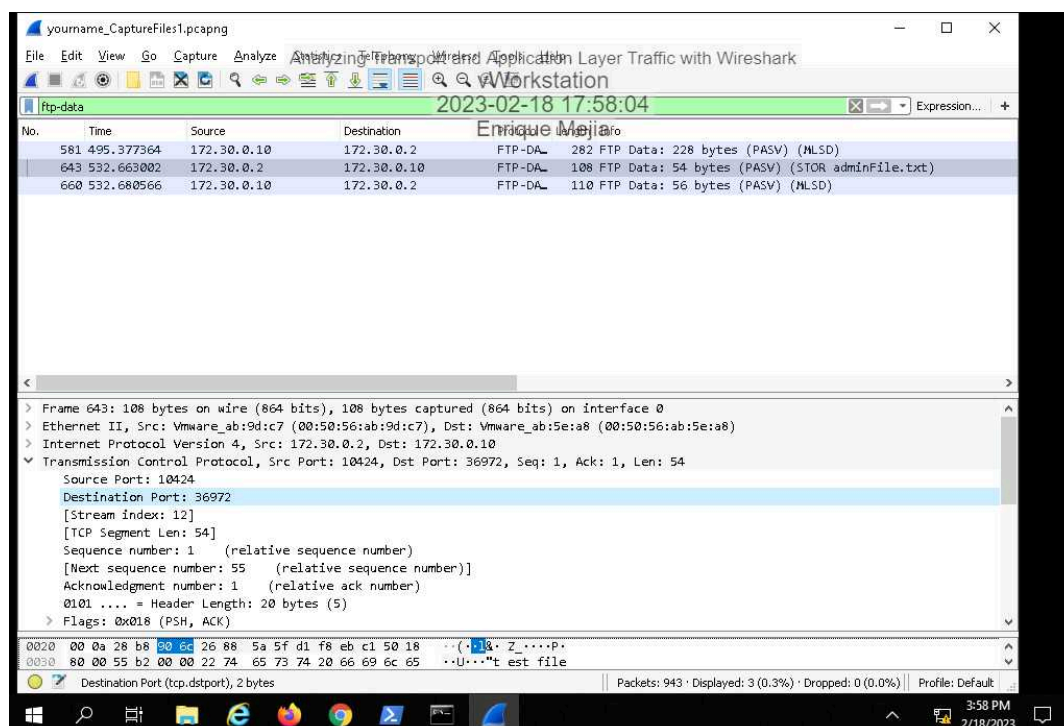
20. Make a screen capture showing the **Destination Port** used for the initial TFTP transfer request.



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



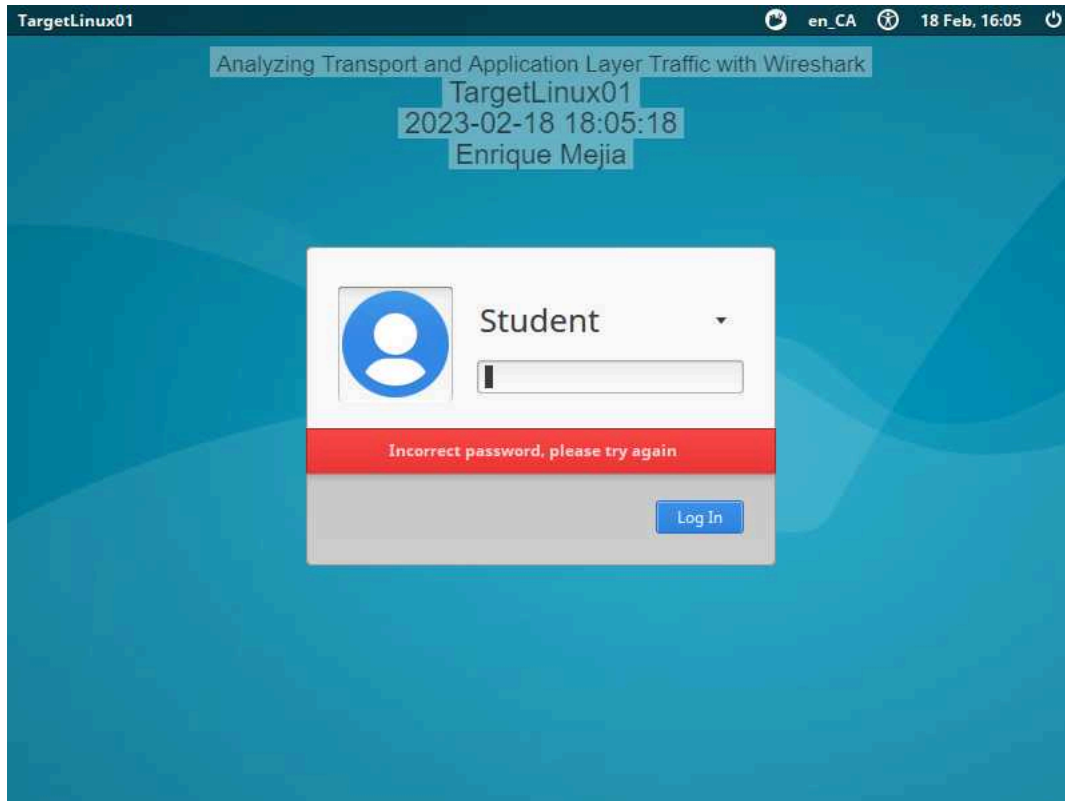
29. Make a screen capture showing the **Destination Port** field value in the **Packet Details** pane.



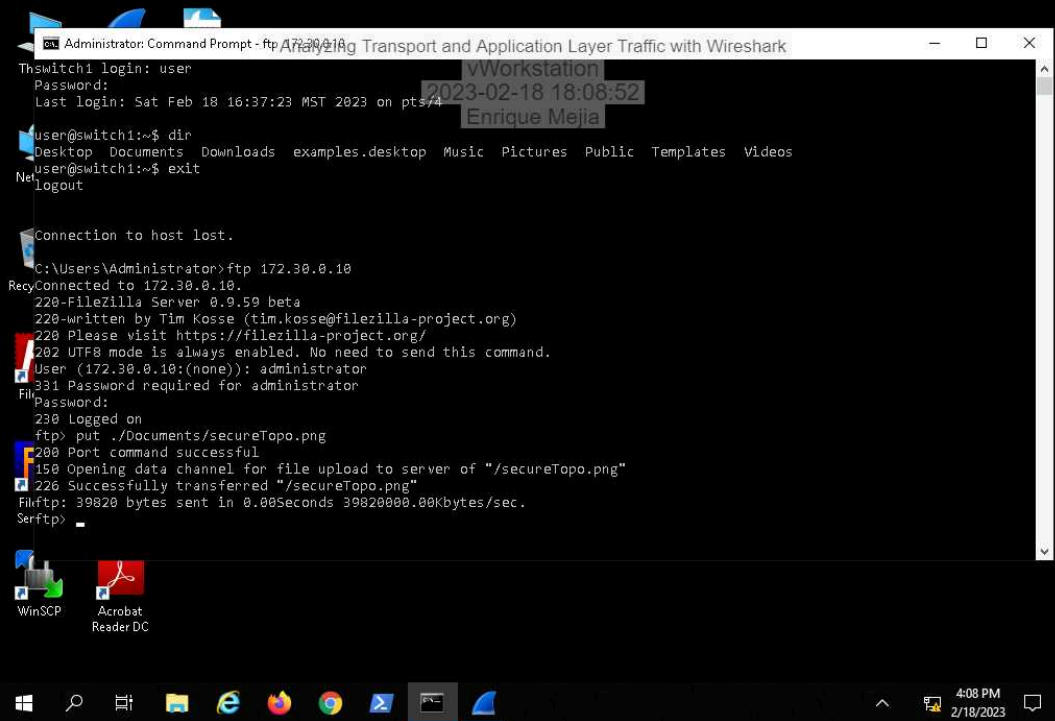
Section 2: Applied Learning

Part 1: Configure Wireshark and Generate Network Traffic

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



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

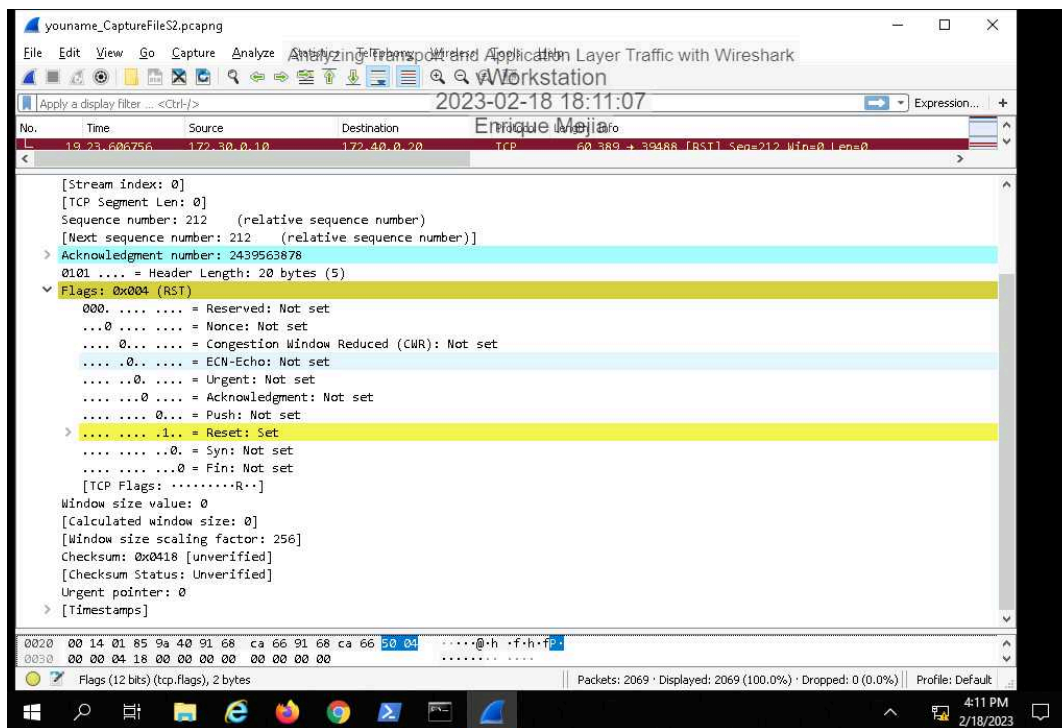


The screenshot shows a Windows desktop with a Command Prompt window open. The window title is "Administrator: Command Prompt - ftp 172.30.0.10". The output shows a login sequence for a user on a switch, followed by an exit. Then, an FTP session is initiated to 172.30.0.10. The user 'administrator' is logged in, and the file 'secureTopo.png' is successfully uploaded to the server. The final output shows the file size (39820 bytes) and the transfer speed (3982000.00kbytes/sec).

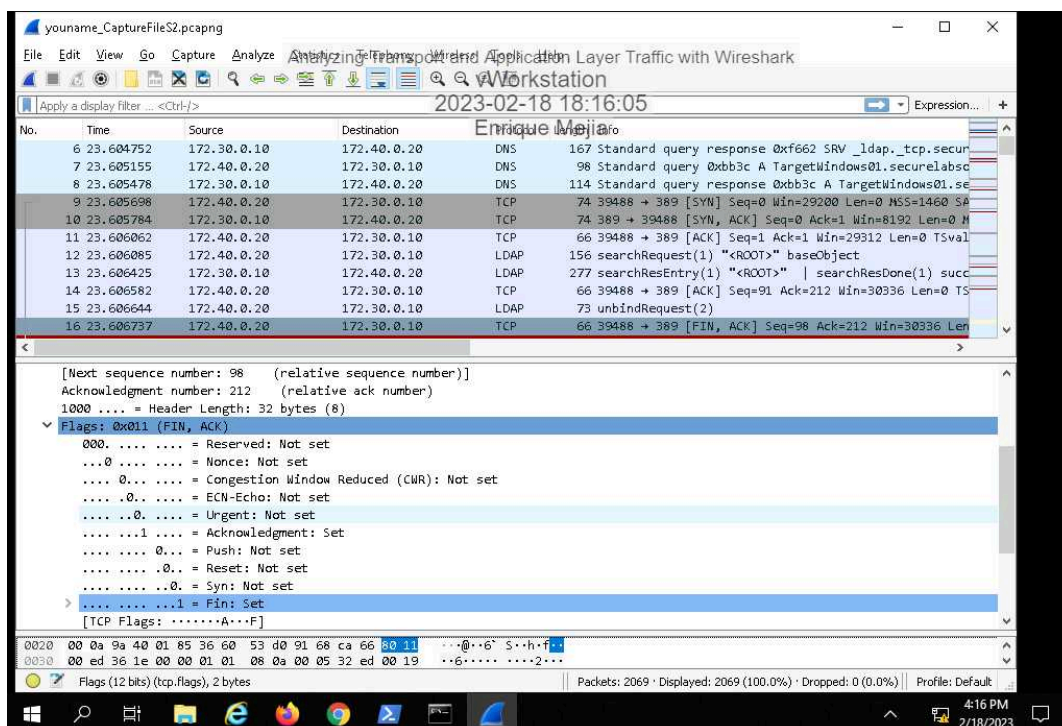
```
Administrator: Command Prompt - ftp 172.30.0.10
The switch1 login: user
Password:
Last login: Sat Feb 18 16:37:23 MST 2023 on pts/4
user@switch1:~$ dir
Desktop Documents Downloads examples.desktop Music Pictures Public Templates Videos
user@switch1:~$ exit
Net
Logout
Connection to host lost.
C:\Users\Administrator>ftp 172.30.0.10
Reconnected to 172.30.0.10.
220-FileZilla Server 0.0.59 beta
220-Written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
220 UTF8 mode is always enabled. No need to send this command.
User (172.30.0.10:(none)): administrator
331 Password required for administrator
File
Password:
230 Logged on
ftp> put ../Documents/secureTopo.png
200 Port command successful
158 Opening data channel for file upload to server of "/secureTopo.png"
226 Successfully transferred "/secureTopo.png"
Fileftp: 39820 bytes sent in 0.00Seconds 3982000.00kbytes/sec.
Serftp>
```

Part 2: Perform Protocol Analysis using Wireshark

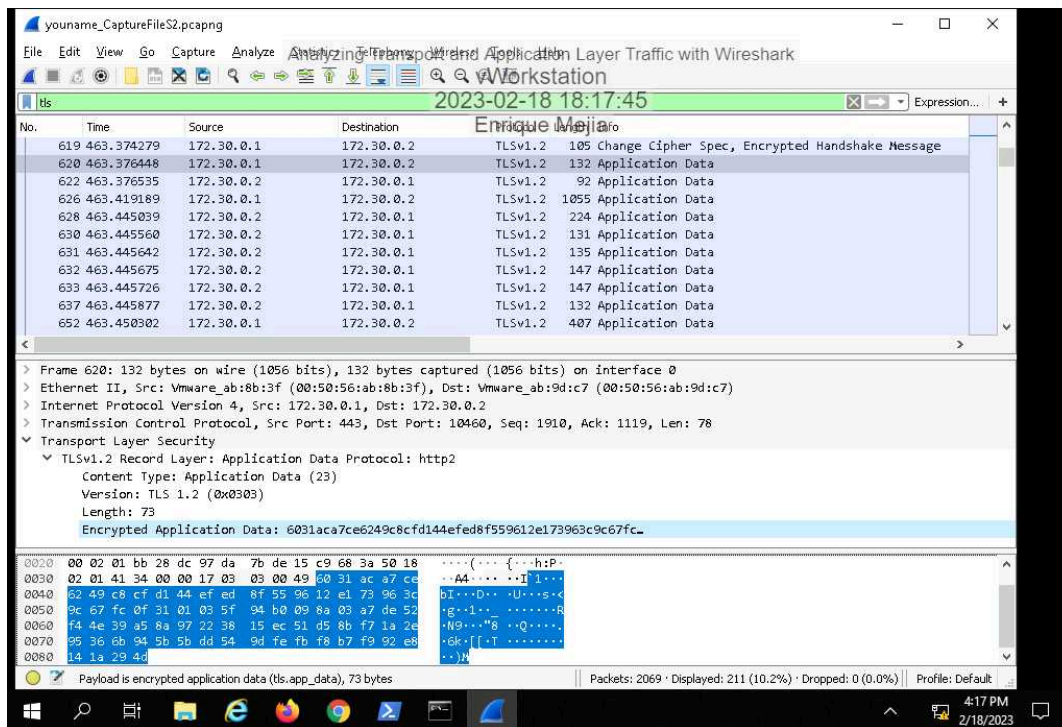
5. Make a screen capture showing the TCP flags set in the Packet Details pane for the first RST packet.



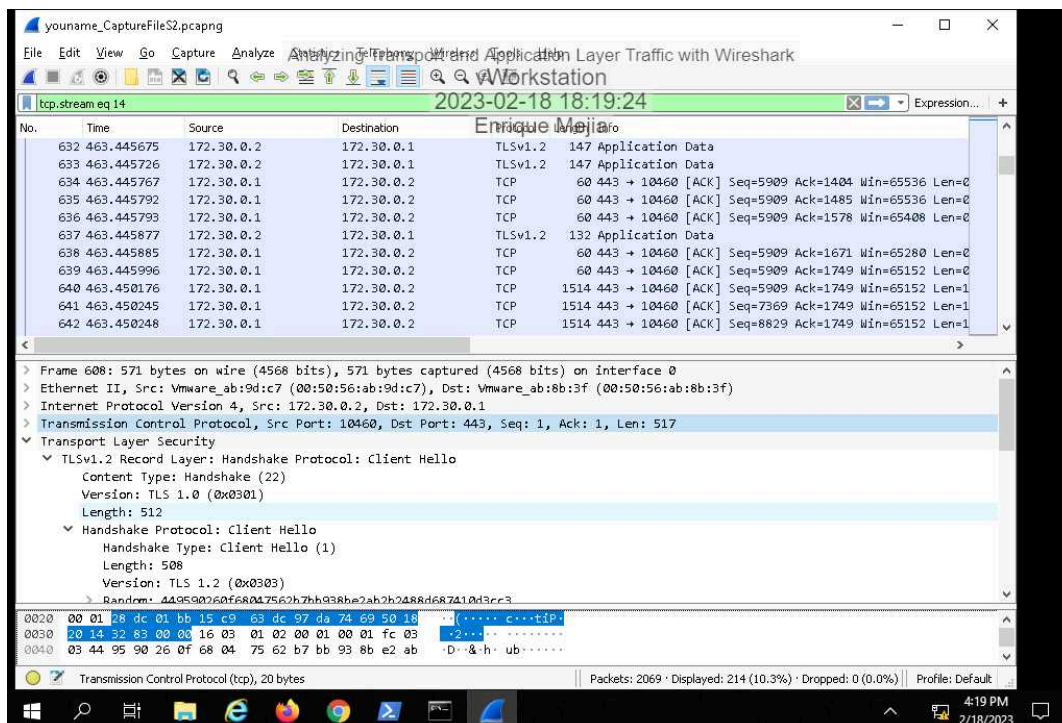
10. Make a screen capture showing the FIN and ACK flags set in the Packet Details View.



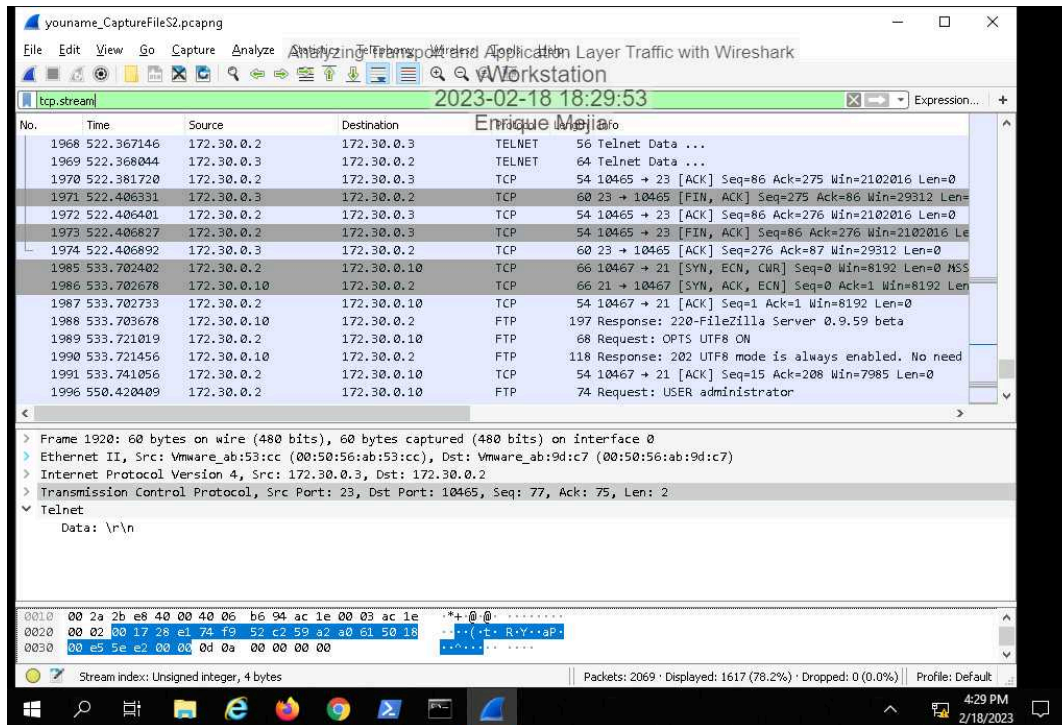
16. Make a screen capture showing the highlighted Encrypted Application Data in the Packet Bytes pane.



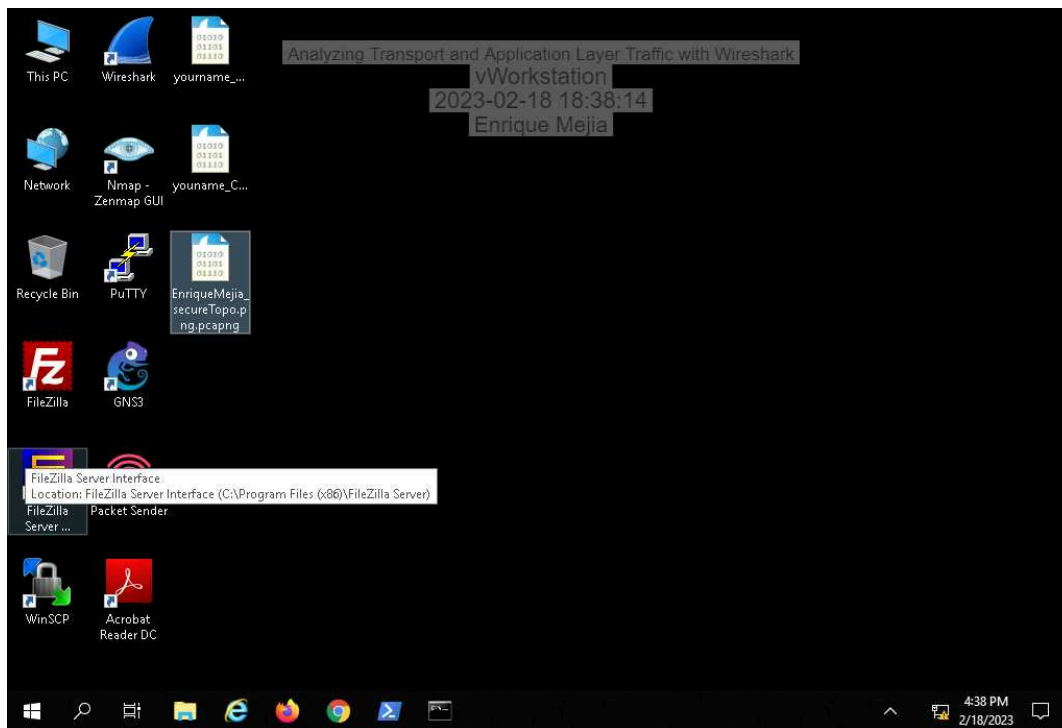
22. Make a screen capture showing the certificate details in the Packet Details pane.



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



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



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.

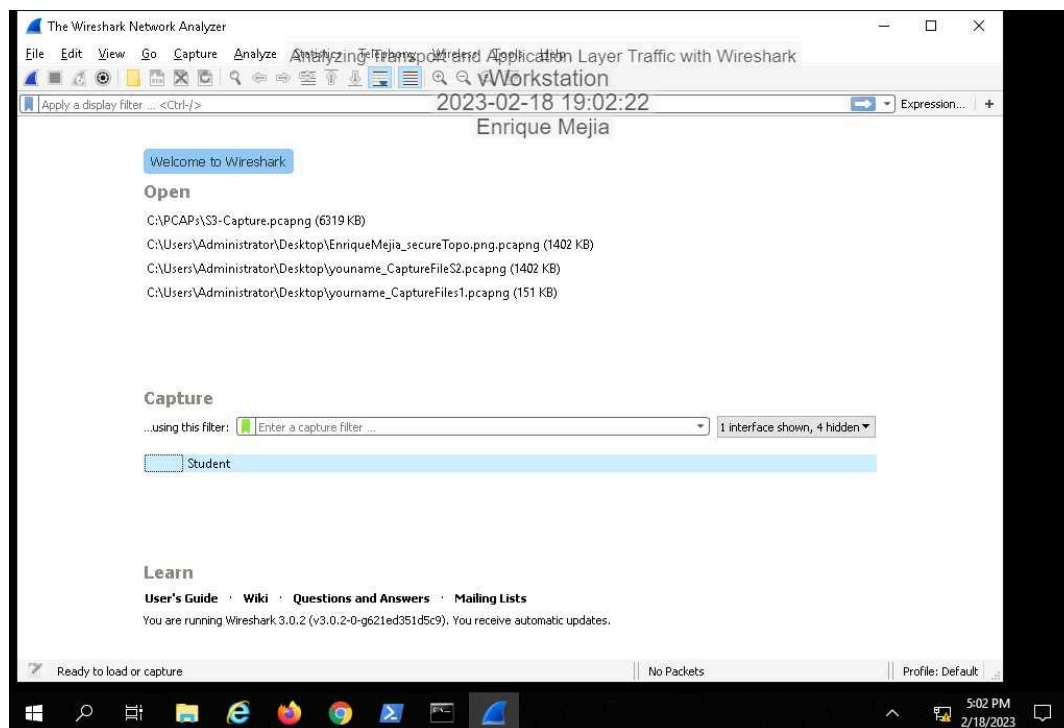
The correct signature to find the RAR archive is though the Ctrl+Host command

Record the name of the correct RAR archive file.

The name of the correct RAR arcvhive is in the http port

Part 2: Reassemble the RAR Archive from its Constituent Bytes

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



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

Was not able to locate due to not finding the README.txt.file