Student:	Email:
Enrique Mejia	enriquem2260@gmail.com

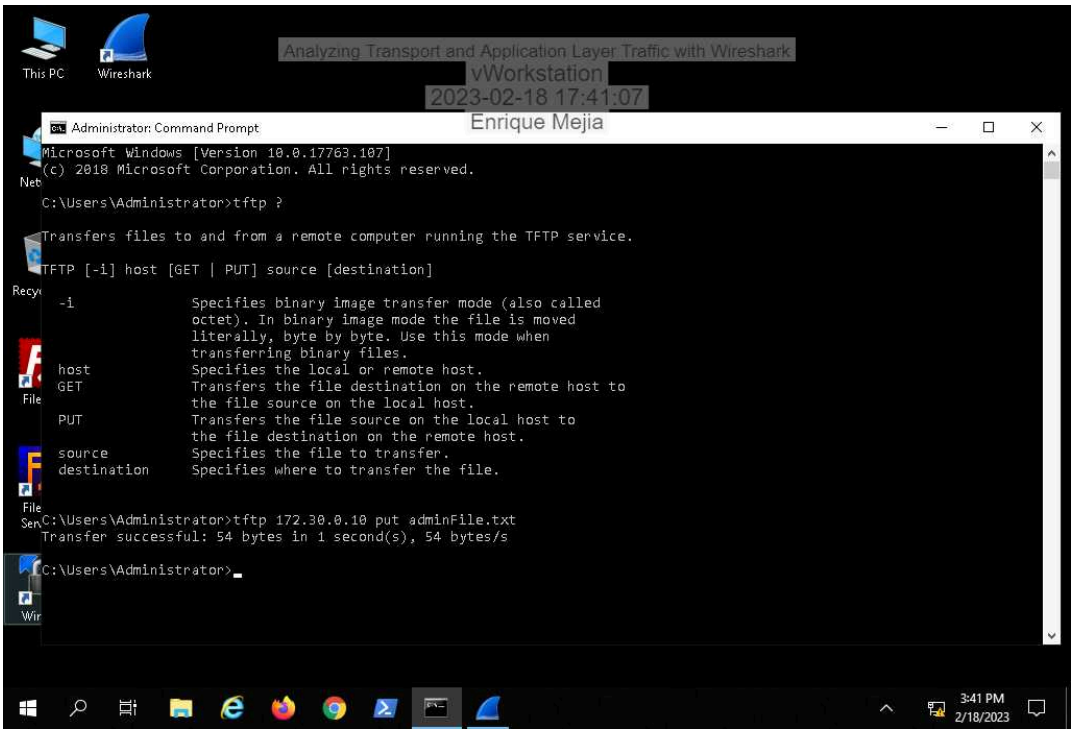
Time on Task:	Progress:
1 hour, 33 minutes	100%

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

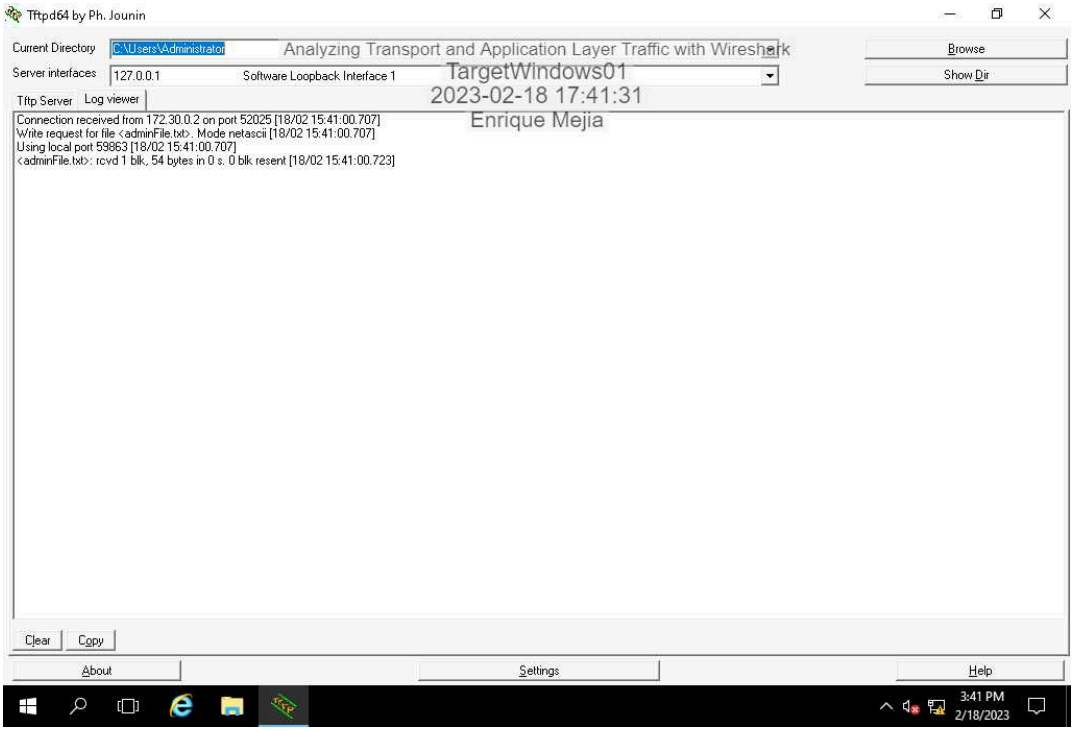
Section 1: Hands-On Demonstration

Part 1: Configure Wireshark and Generate Network Traffic

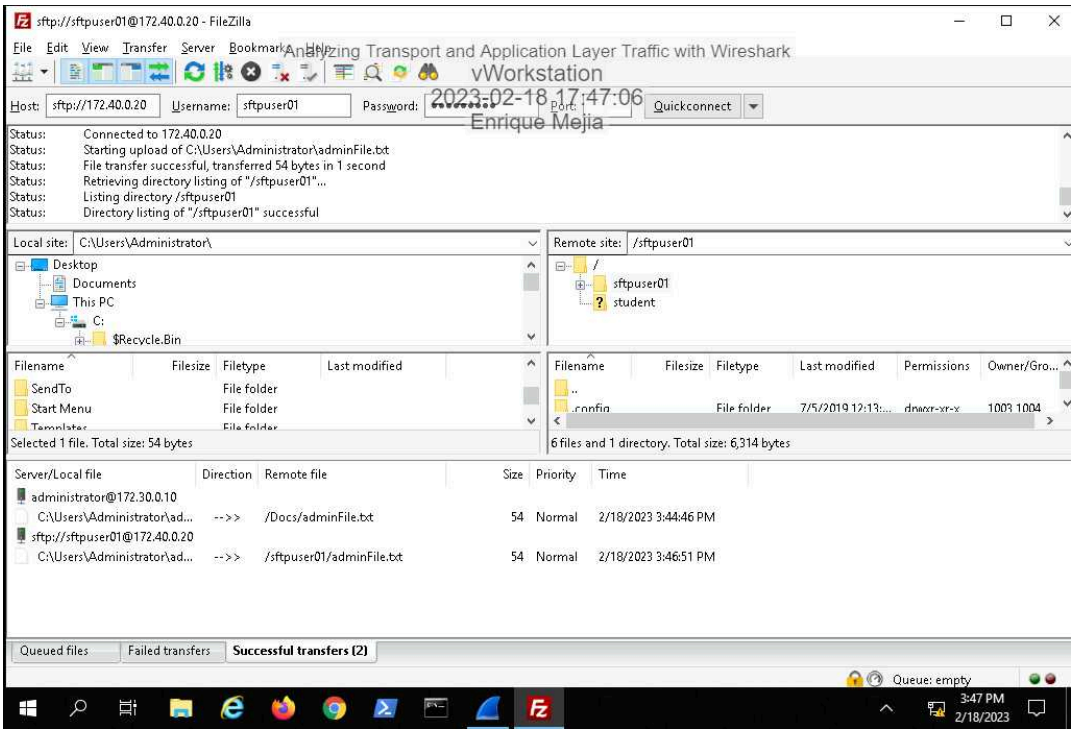
28. **Make a screen capture** showing the **successful tftp file transfer message in the Command Prompt**.



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

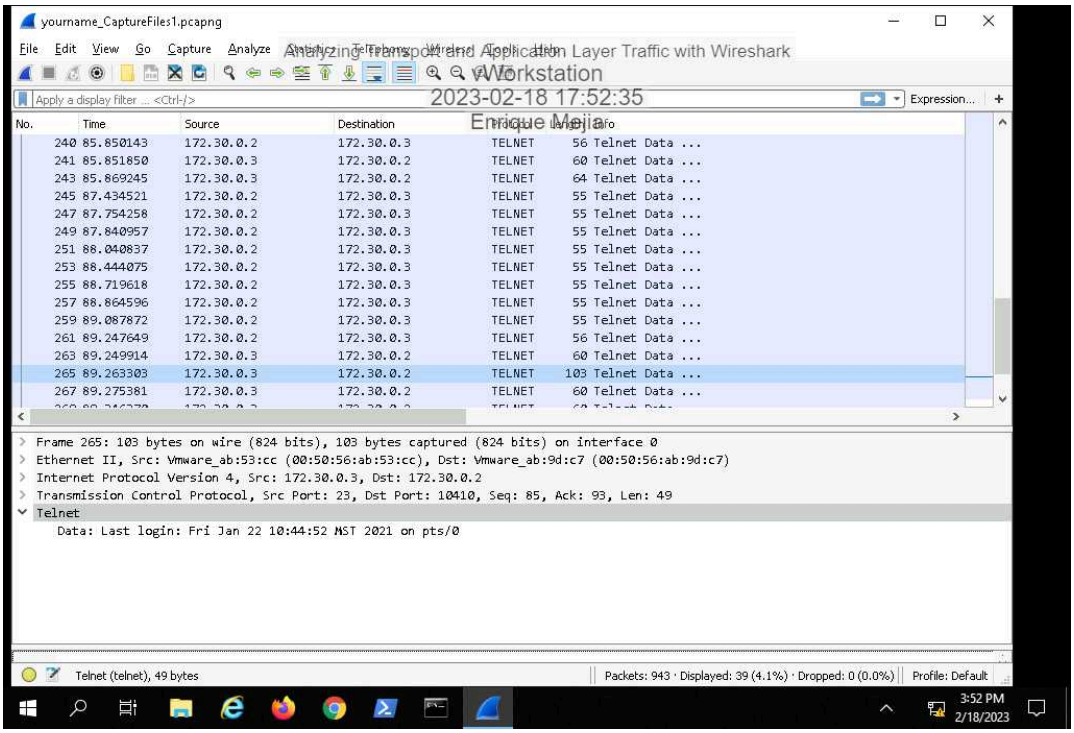


45. **Make a screen capture** showing the **successful SFTP file transfer**.

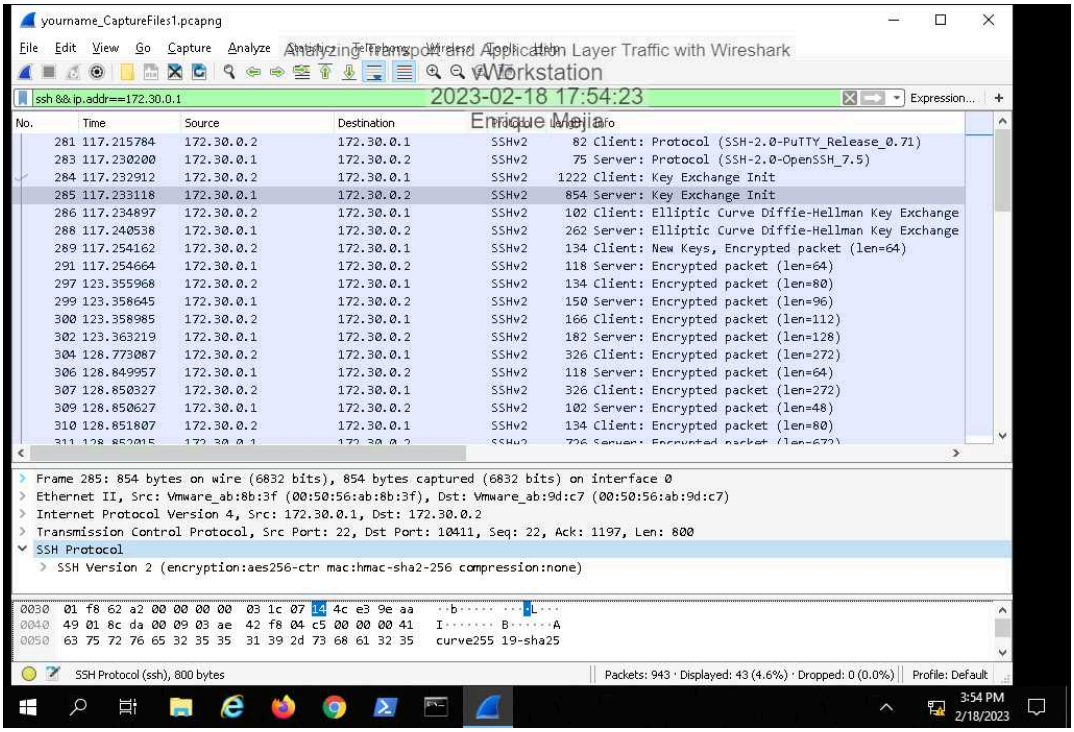


Part 2: Perform Protocol Analysis using Wireshark

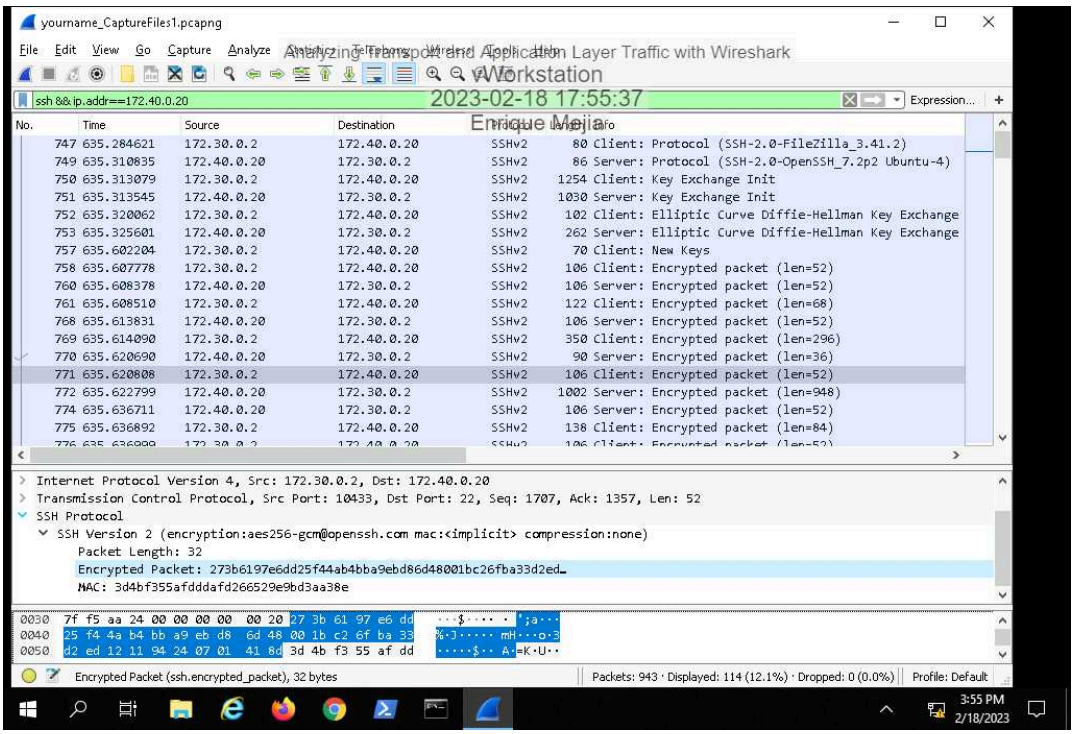
5. **Make a screen capture** showing the ***Last Login:*** **information in the Packet Details pane**.



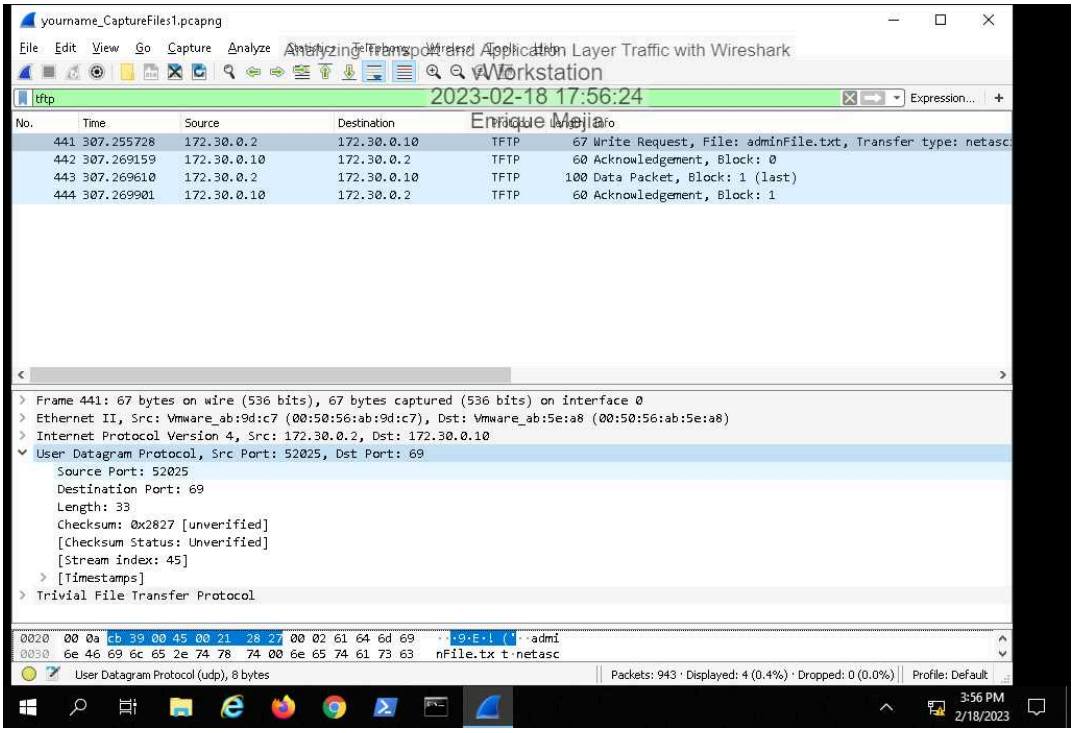
11. **Make a screen capture** showing the **SSHv2 encryption and mac selections for the SSH connection**.



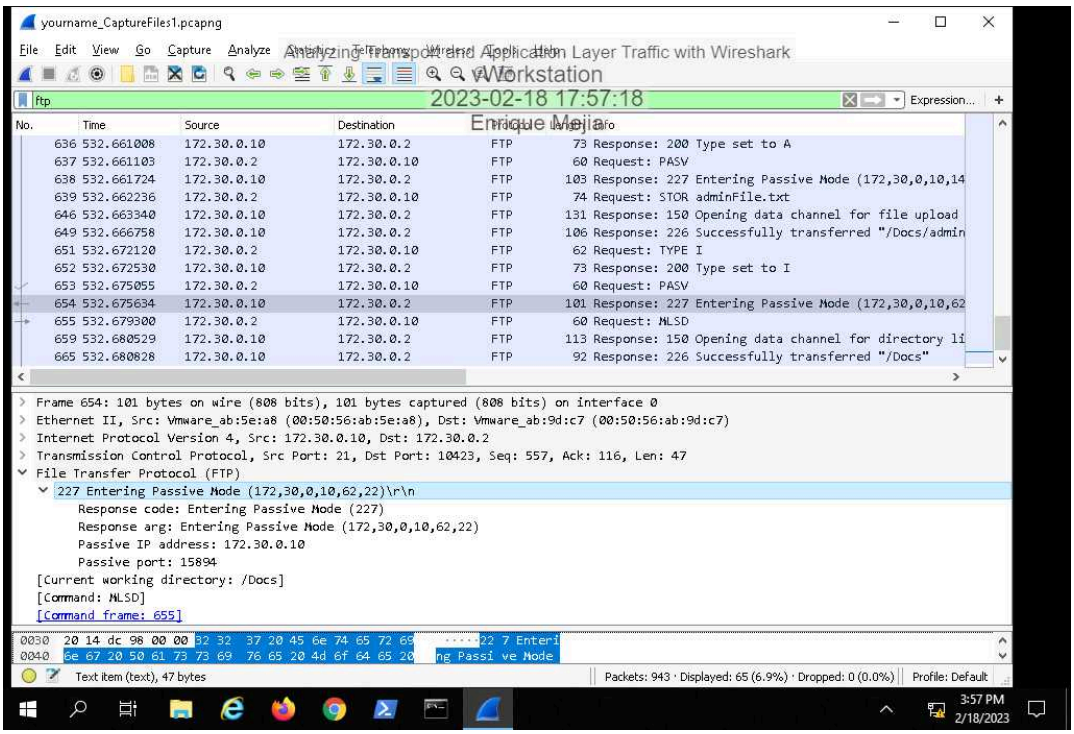
16. **Make a screen capture** showing the **highlighted (encrypted) data in the Packet Bytes pane**.



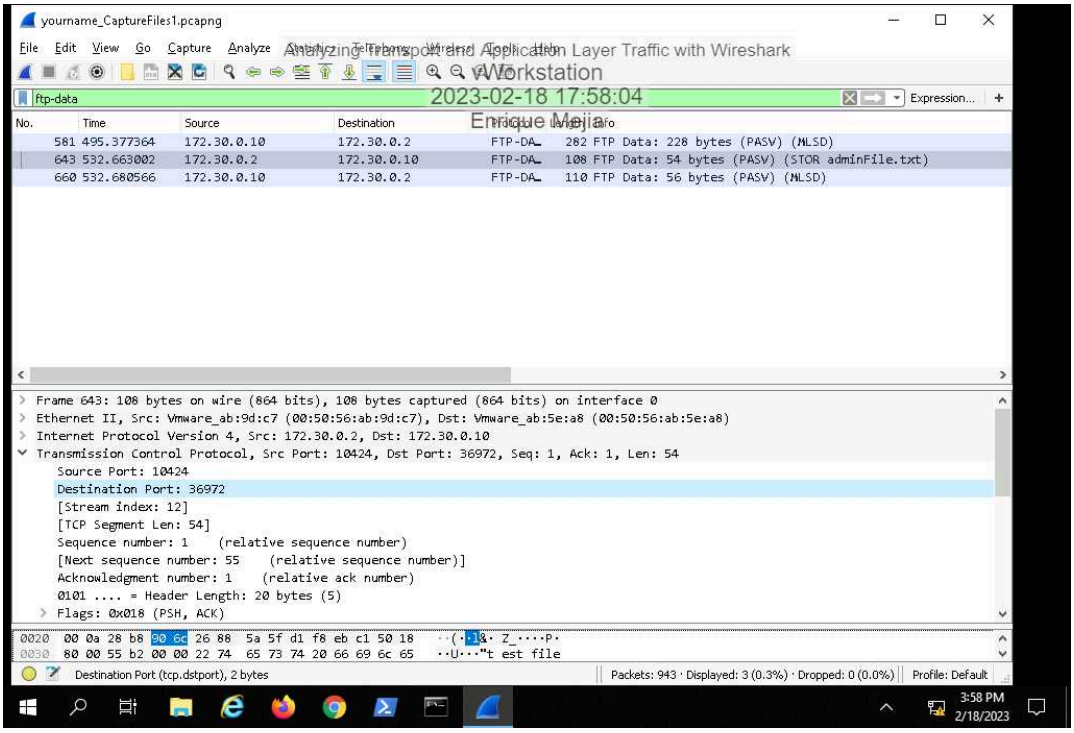
20. **Make a screen capture** showing the **Destination Port used for the initial TFTP transfer request**.



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



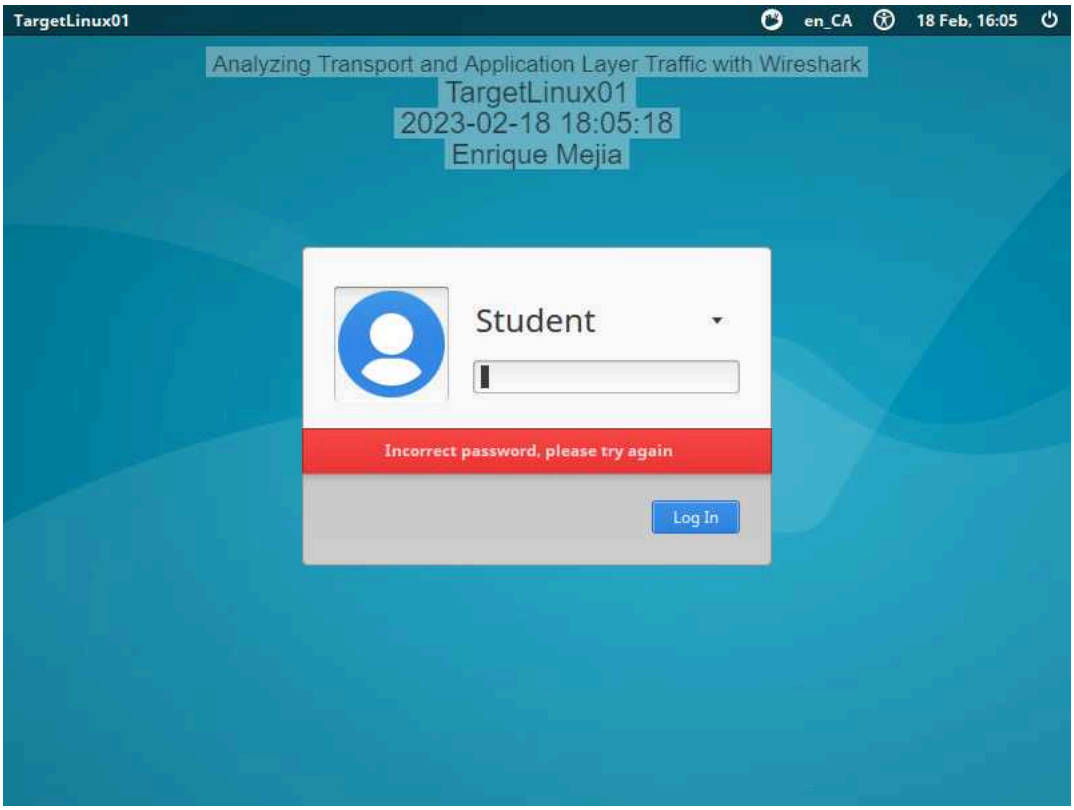
29. **Make a screen capture** showing the **Destination Port field value in the Packet Details pane**.



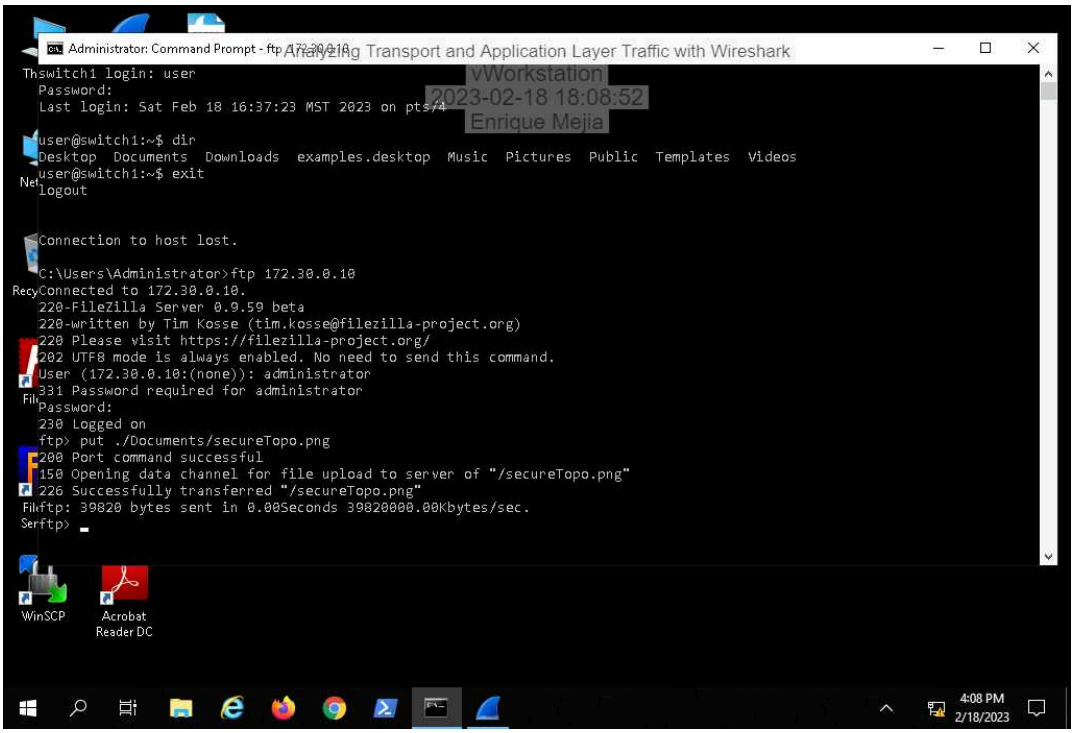
Section 2: Applied Learning

Part 1: Configure Wireshark and Generate Network Traffic

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

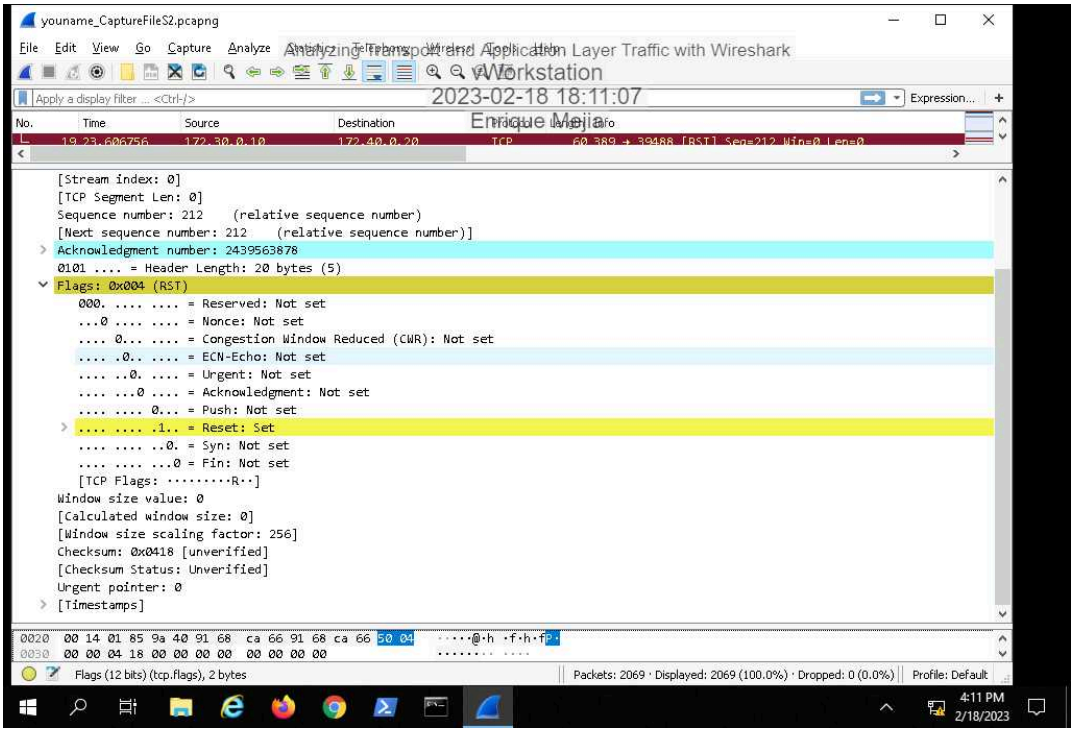


20. **Make a screen capture** showing the **successful transfer in the Command Prompt output**.

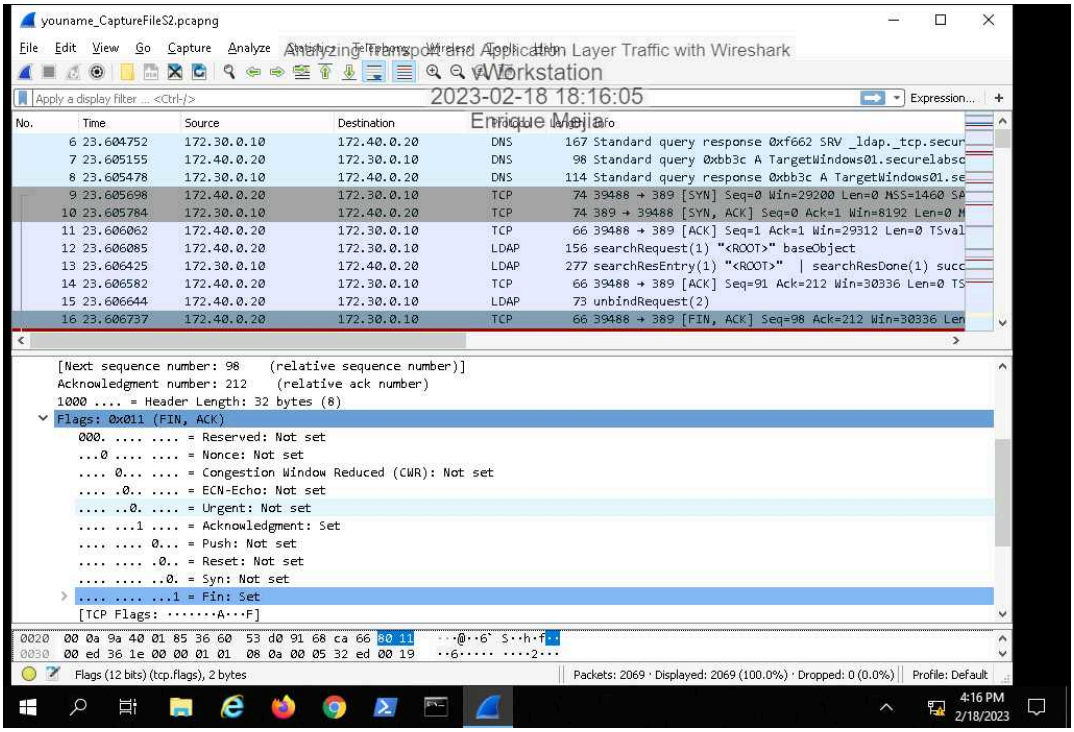


Part 2: Perform Protocol Analysis using Wireshark

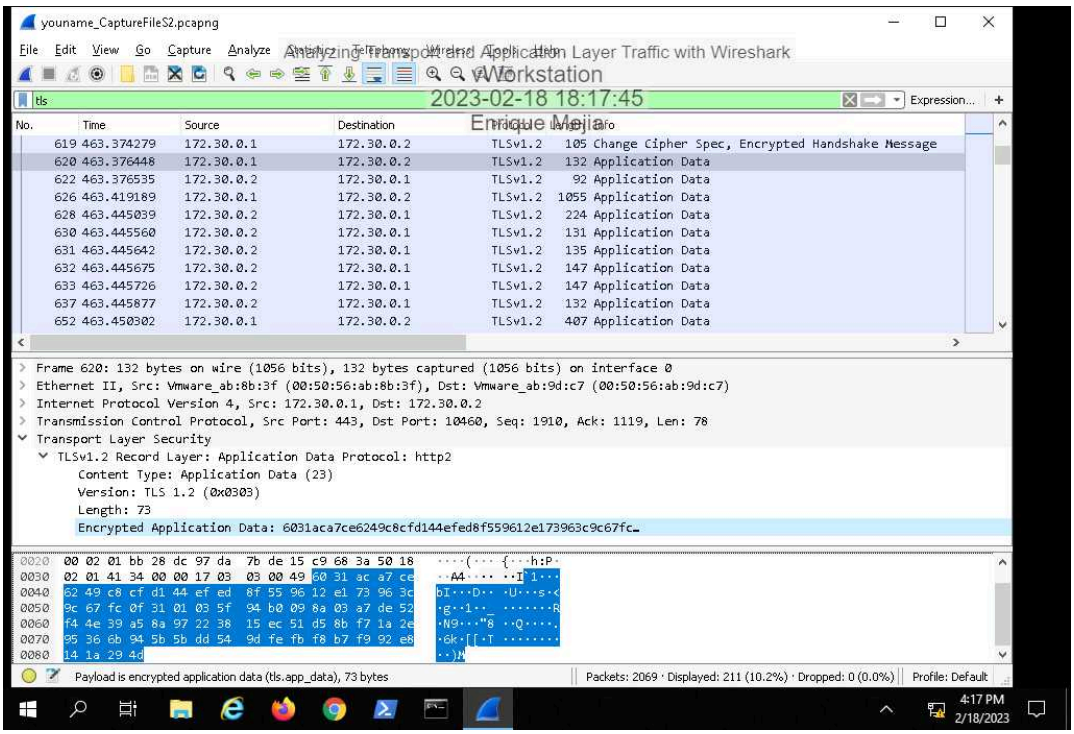
5. **Make a screen capture** showing the **TCP flags set in the Packet Details pane for the first RST packet**.



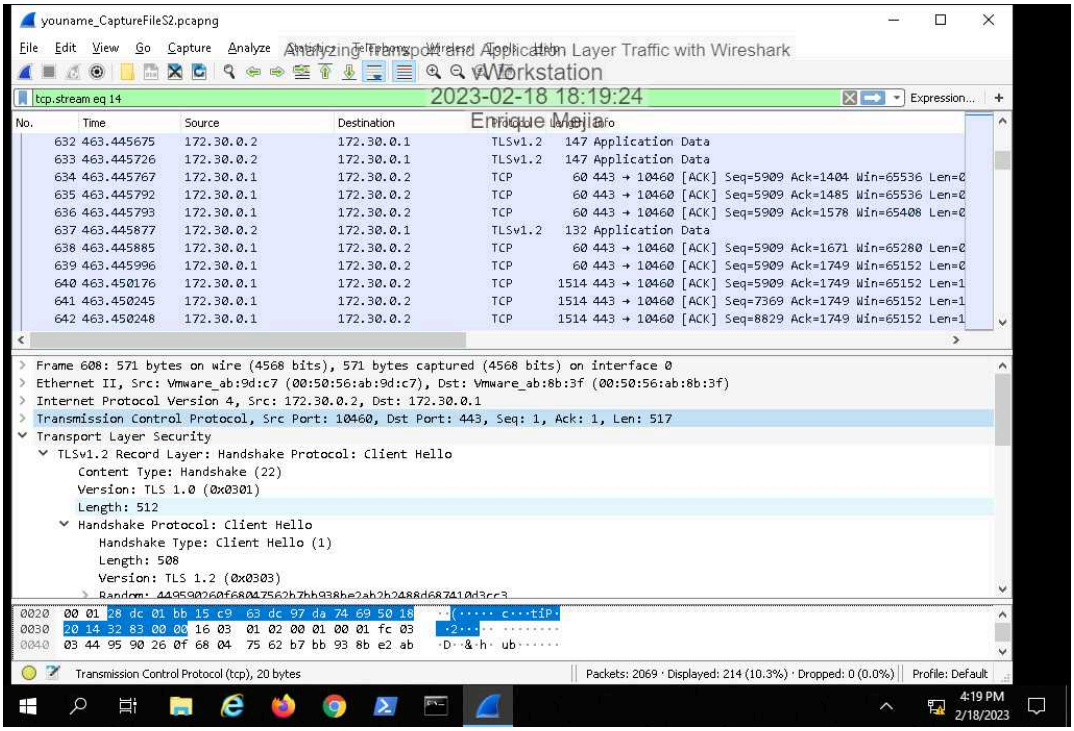
10. **Make a screen capture** showing the **FIN and ACK flags set in the Packet Details View**.



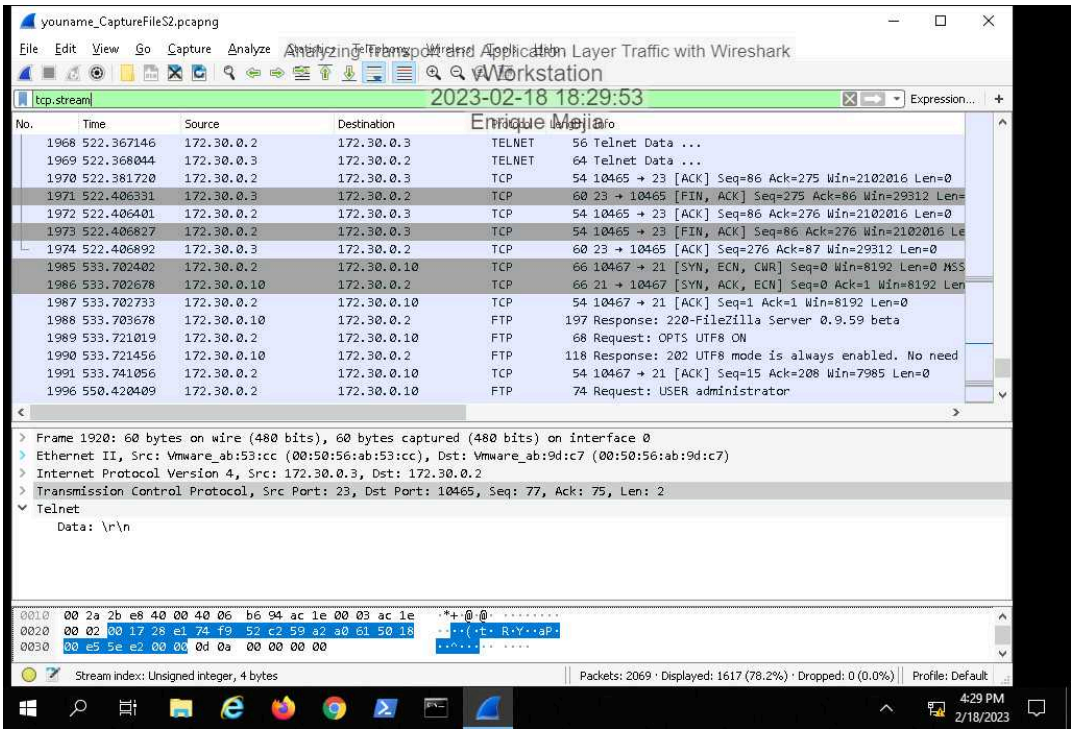
16. **Make a screen capture** showing the **highlighted Encrypted Application Data in the Packet Bytes pane**.



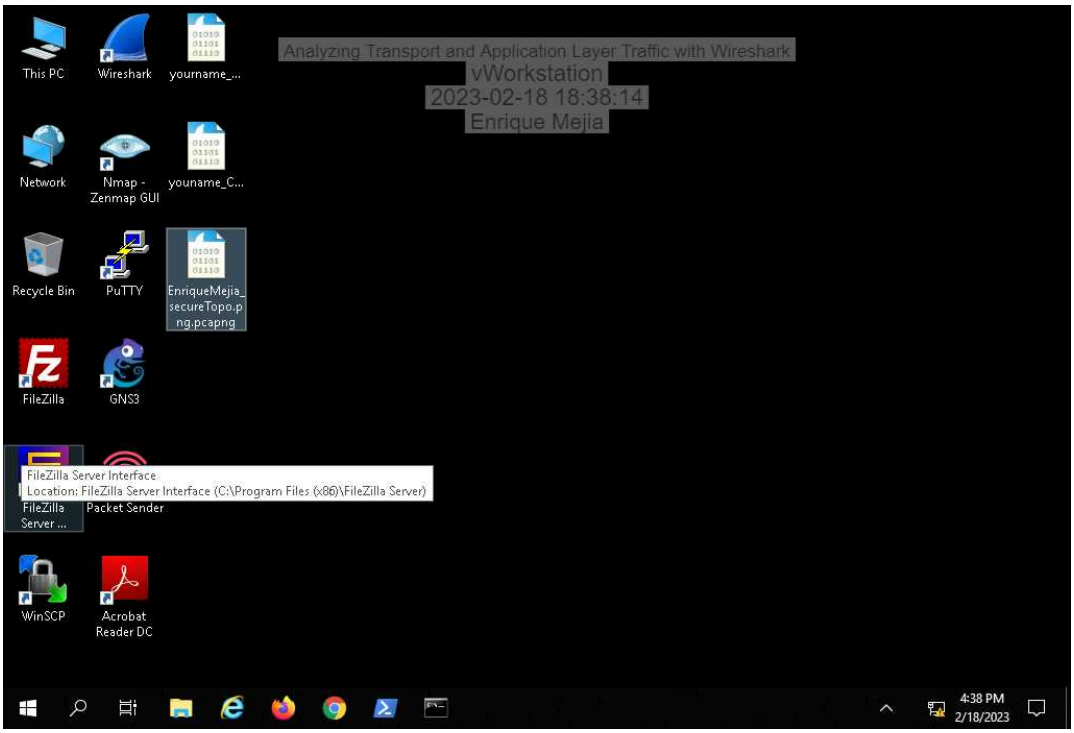
22. **Make a screen capture** showing the **certificate details in the Packet Details pane**.



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.

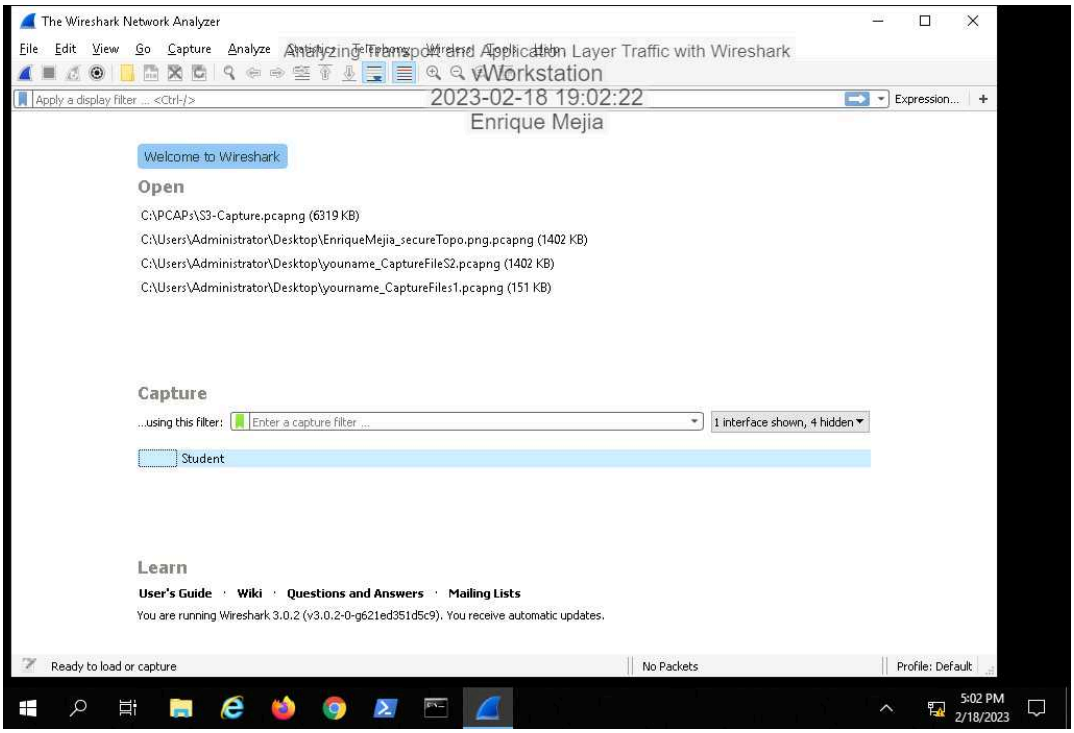
The correct signature to find the RAR archive is though the Ctrl+Host command

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