

Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

10 hours, 3 minutes

Progress:

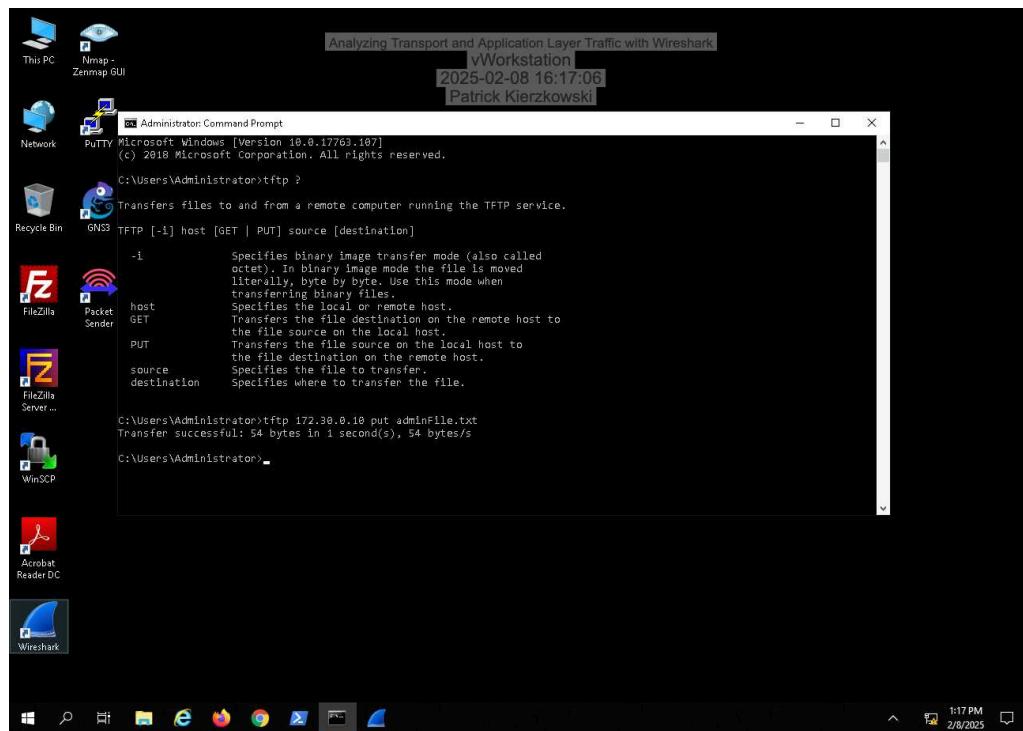
100%

Report Generated: Monday, July 7, 2025 at 9:45 PM

Section 1: Hands-On Demonstration

Part 1: Configure Wireshark and Generate Network Traffic

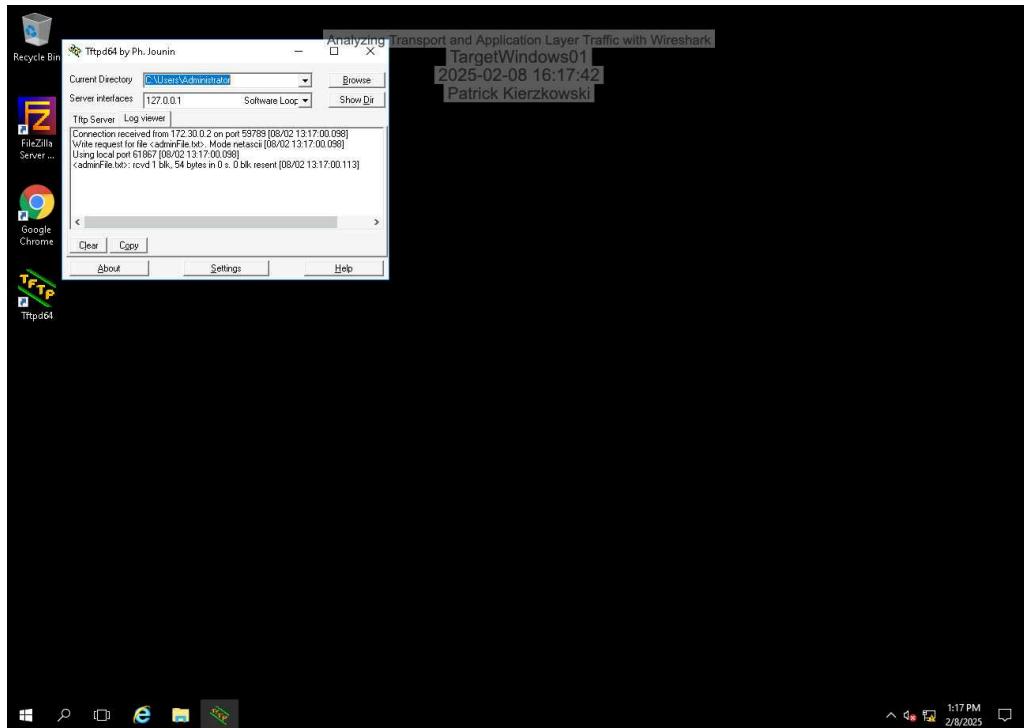
28. Make a screen capture showing the **successful tftp file transfer message in the Command Prompt.**



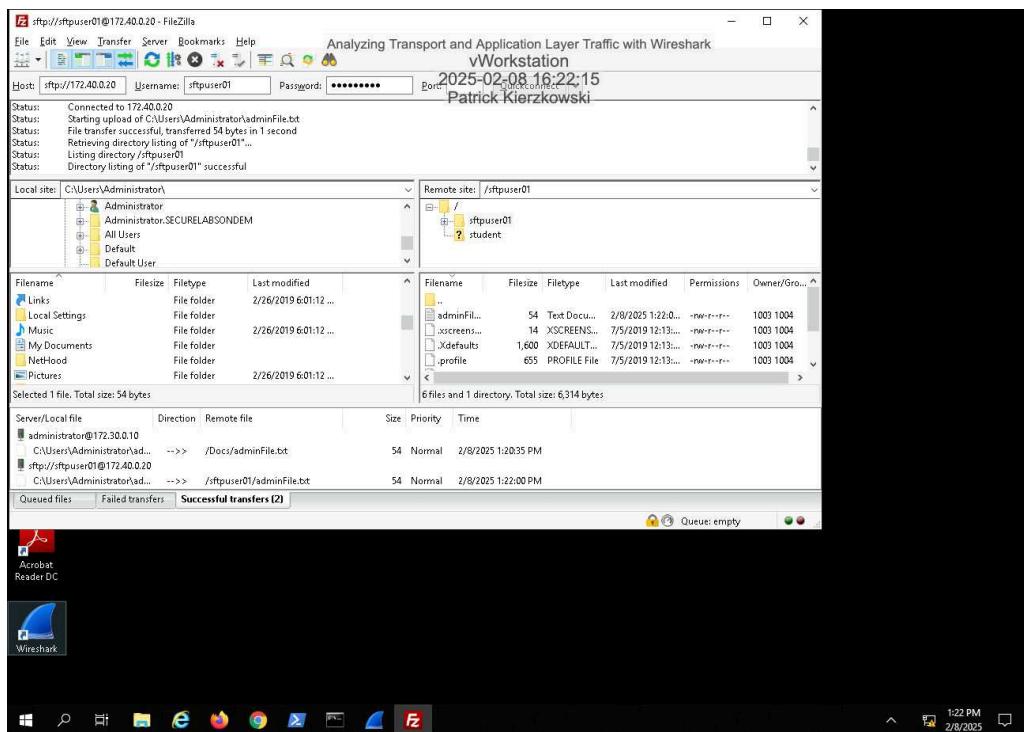
Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

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



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

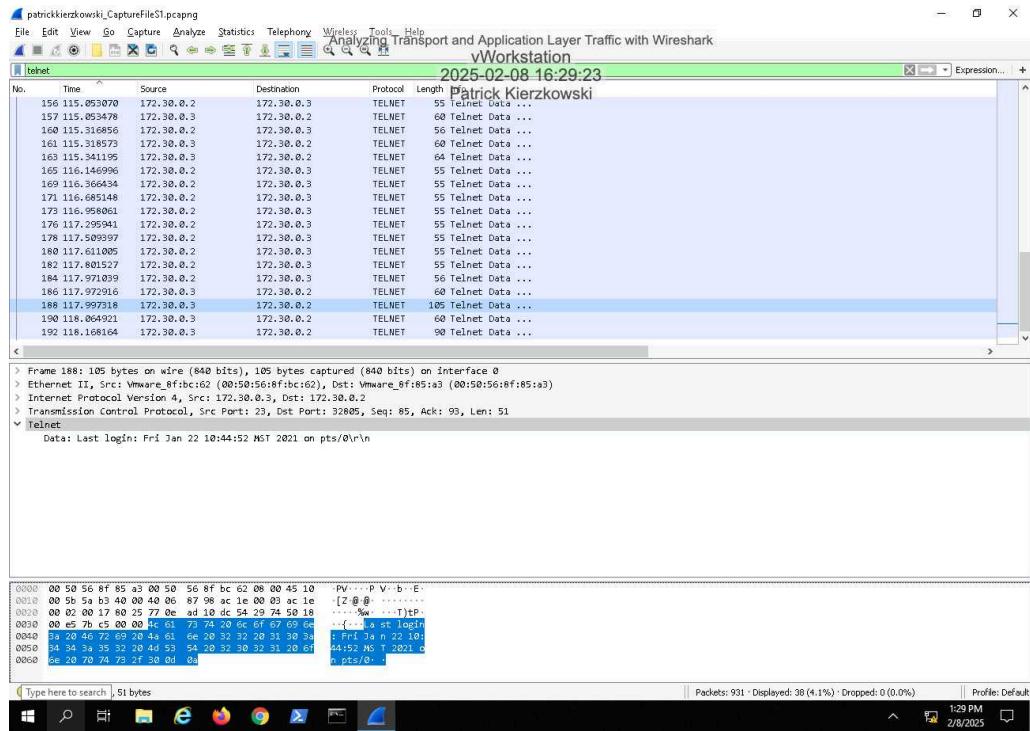


Part 2: Perform Protocol Analysis using Wireshark

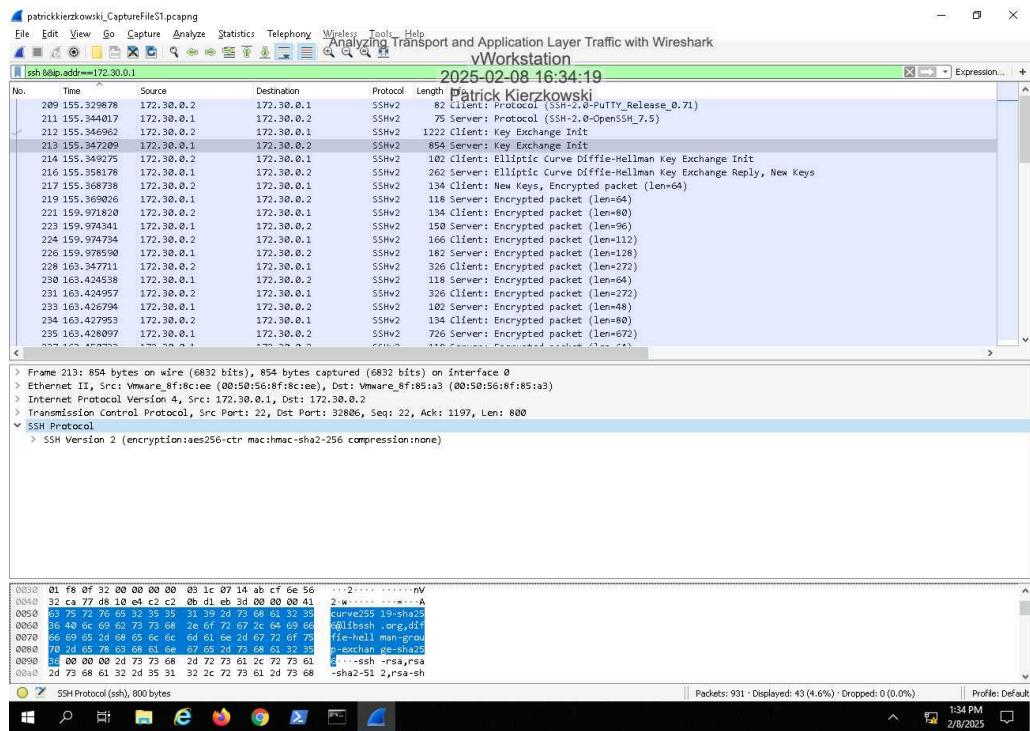
Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

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



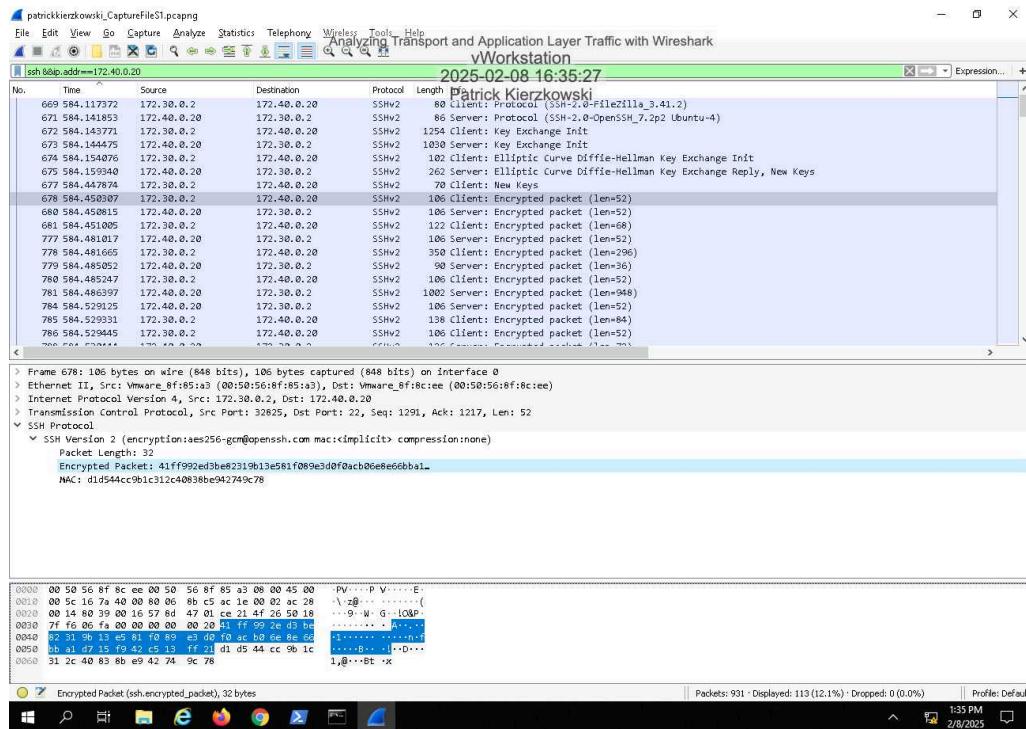
11. Make a screen capture showing the **SSHv2 encryption and mac selections** for the SSH connection.



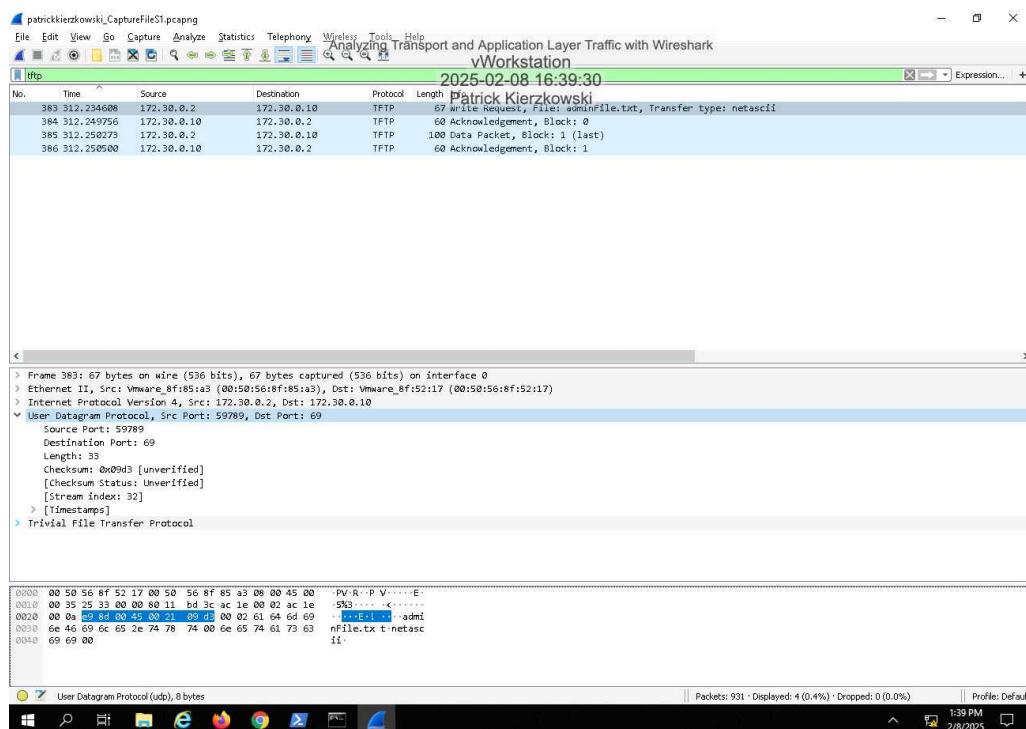
Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

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



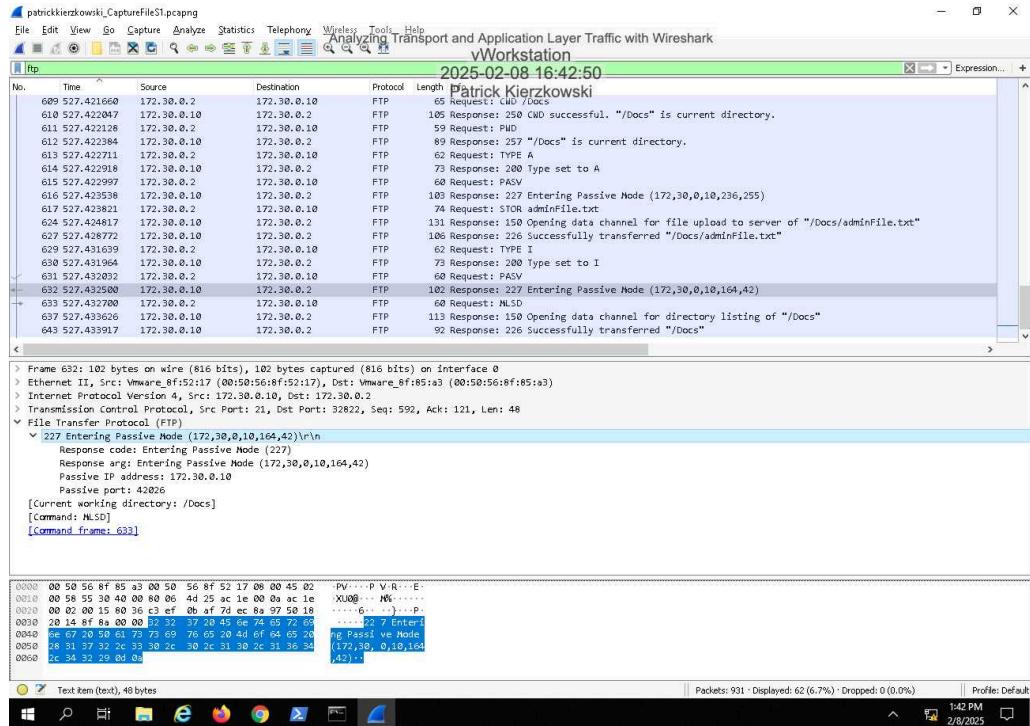
20. Make a screen capture showing the Destination Port used for the initial TFTP transfer request.



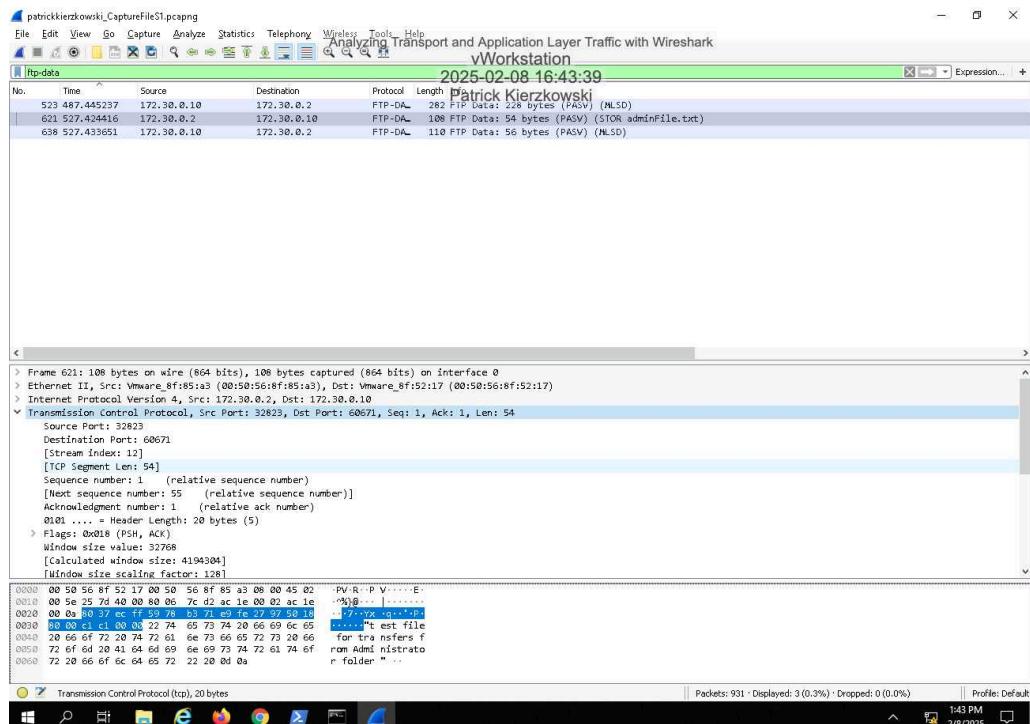
Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

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.



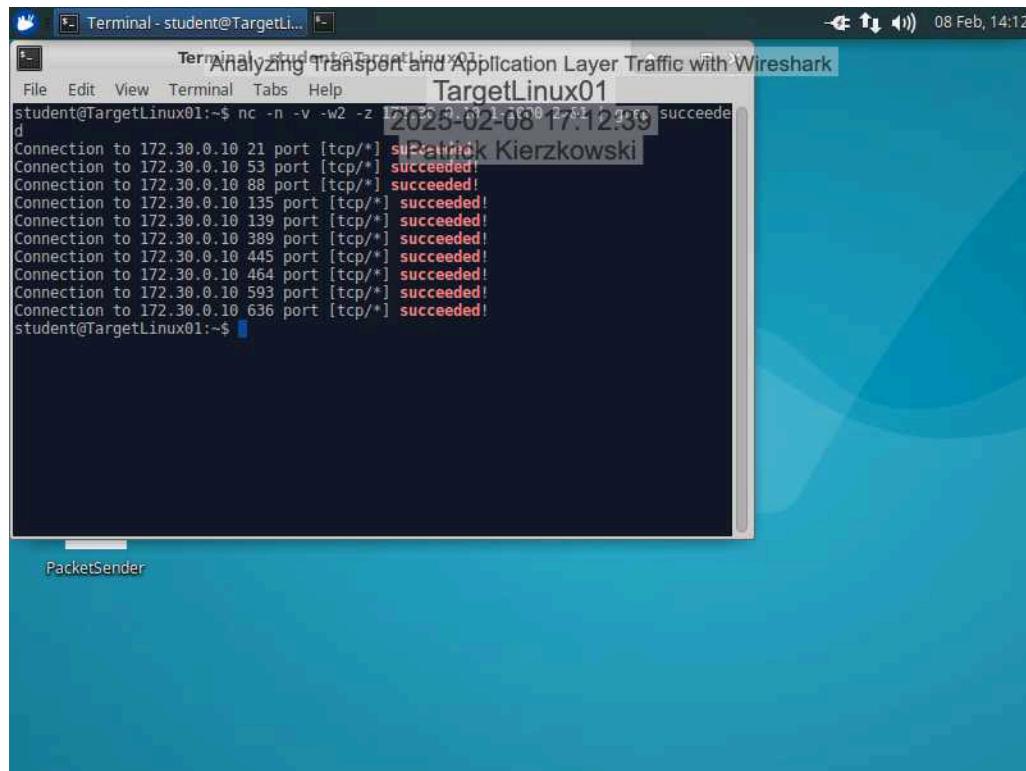
Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

Section 2: Applied Learning

Part 1: Configure Wireshark and Generate Network Traffic

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



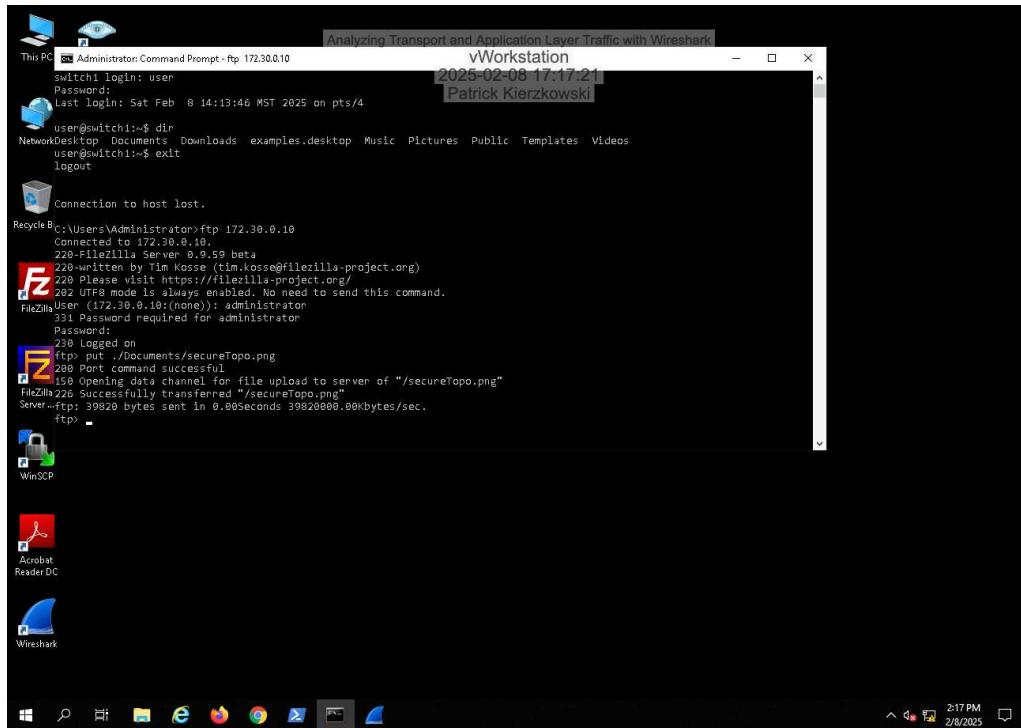
The screenshot shows a terminal window titled "Terminal - student@TargetLinux01" running on a Linux desktop environment. The window displays the command "student@TargetLinux01:~\$ nc -n -v -w2 -z 172.30.0.10 21-636" followed by a timestamp "2025-02-08 17:12:39". Below the timestamp, the output of the netcat scan is shown, listing various ports from 21 to 636 that were successfully connected to on the target host. The desktop background is blue with a wavy pattern, and the window has a standard Linux window border.

```
student@TargetLinux01:~$ nc -n -v -w2 -z 172.30.0.10 21-636
2025-02-08 17:12:39 succeeded!
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:~$
```

Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

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

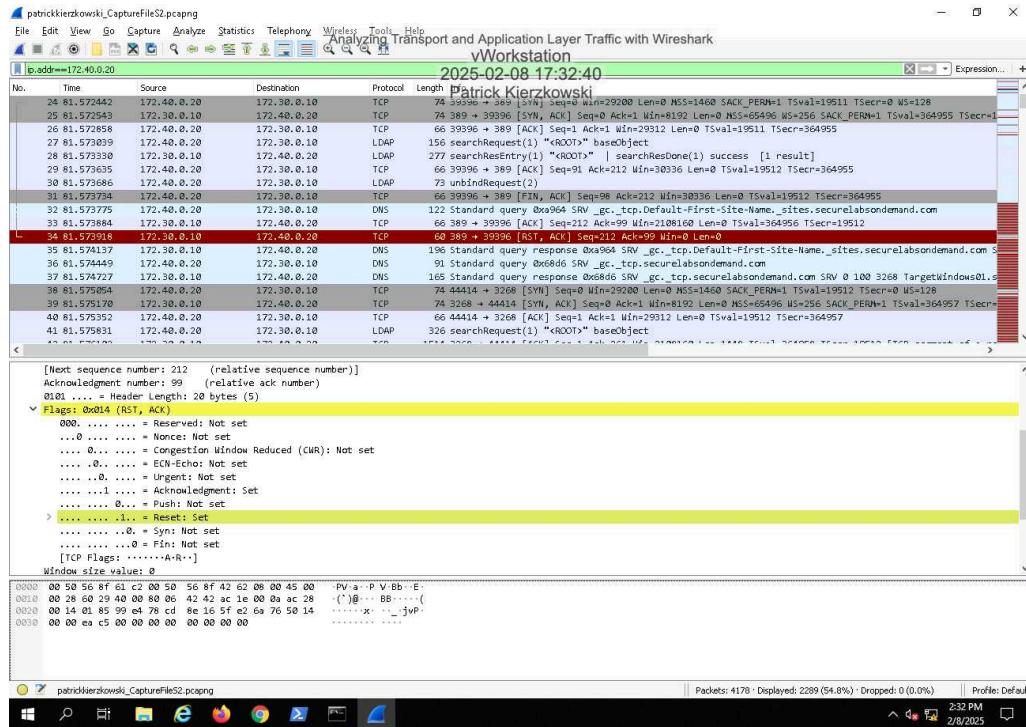


Part 2: Perform Protocol Analysis using Wireshark

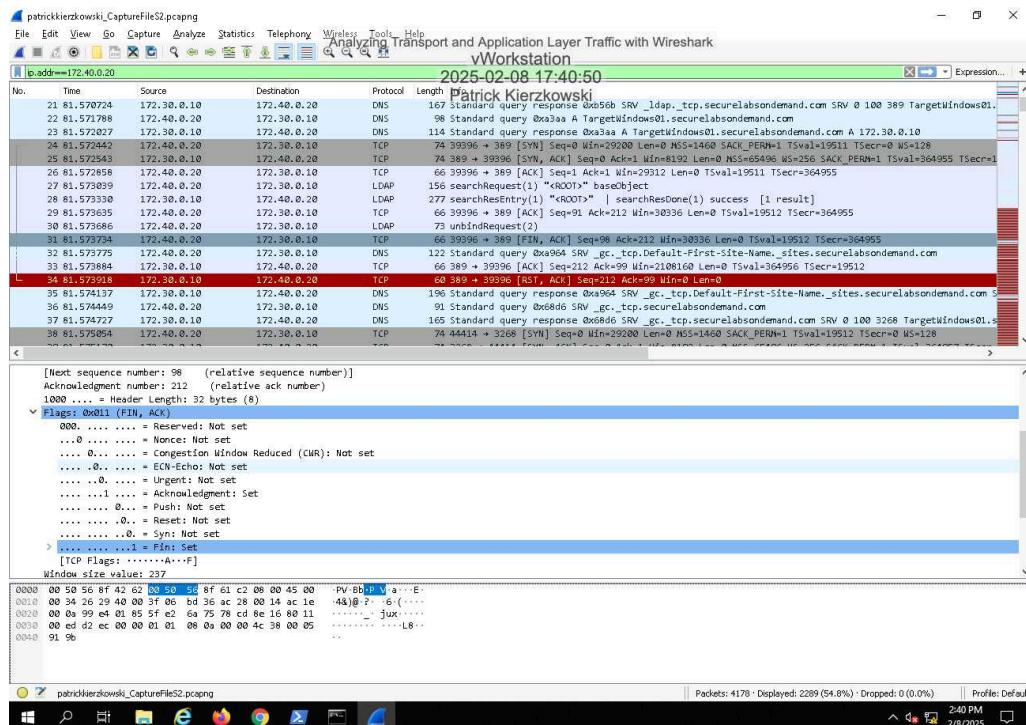
Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

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



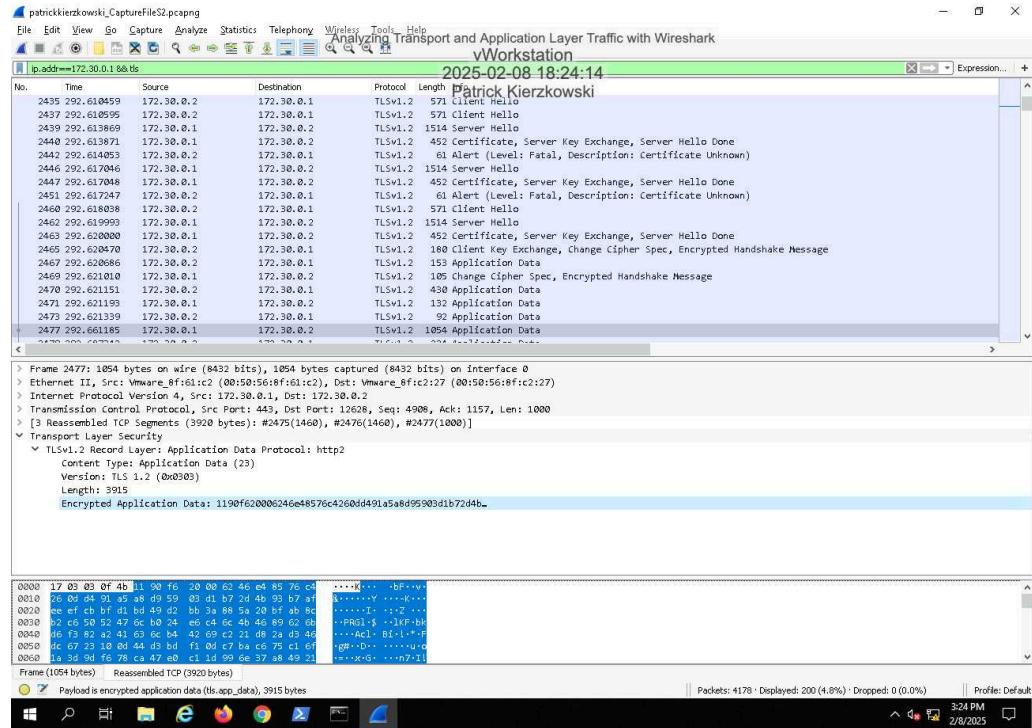
10. Make a screen capture showing the FIN and ACK flags set in the Packet Details View.



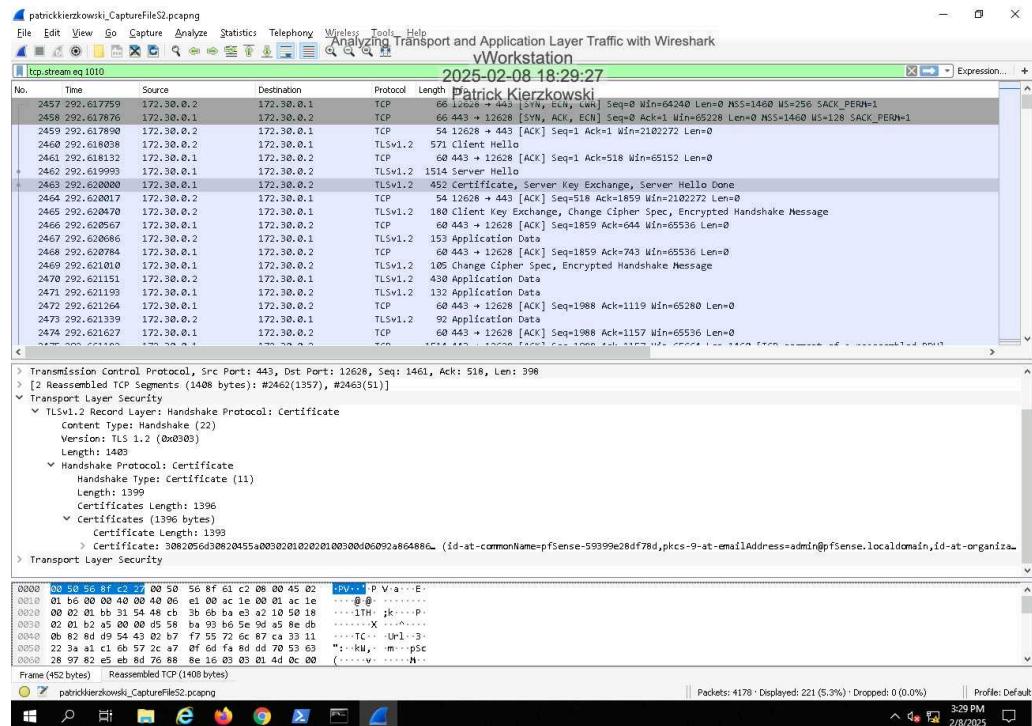
Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

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



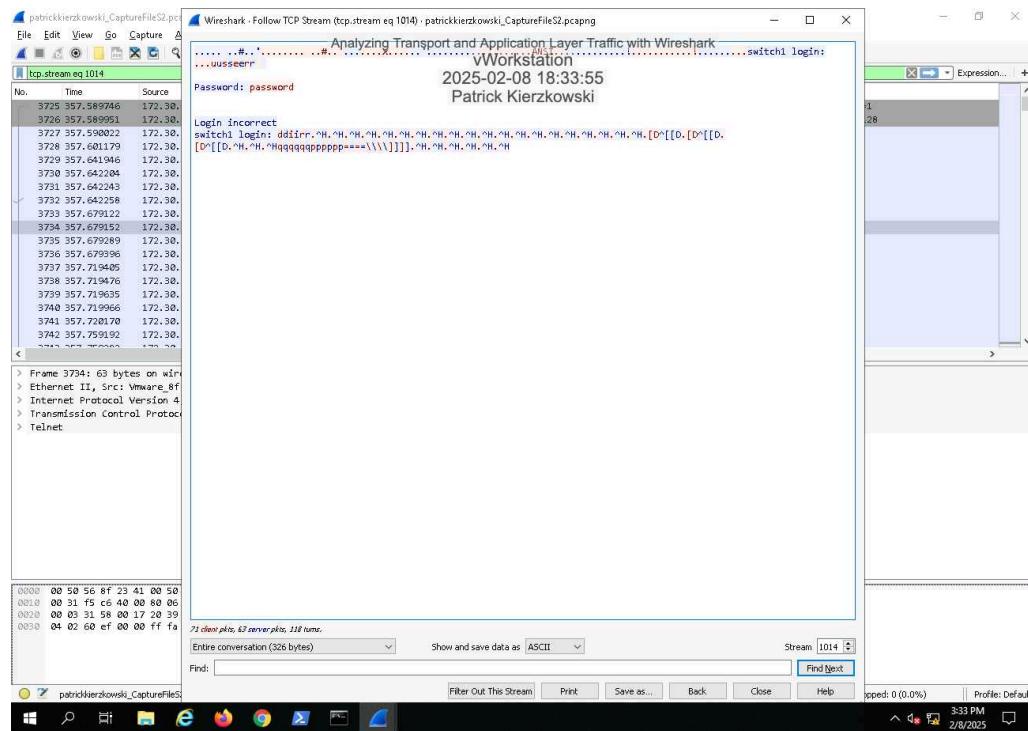
22. Make a screen capture showing the certificate details in the Packet Details pane.



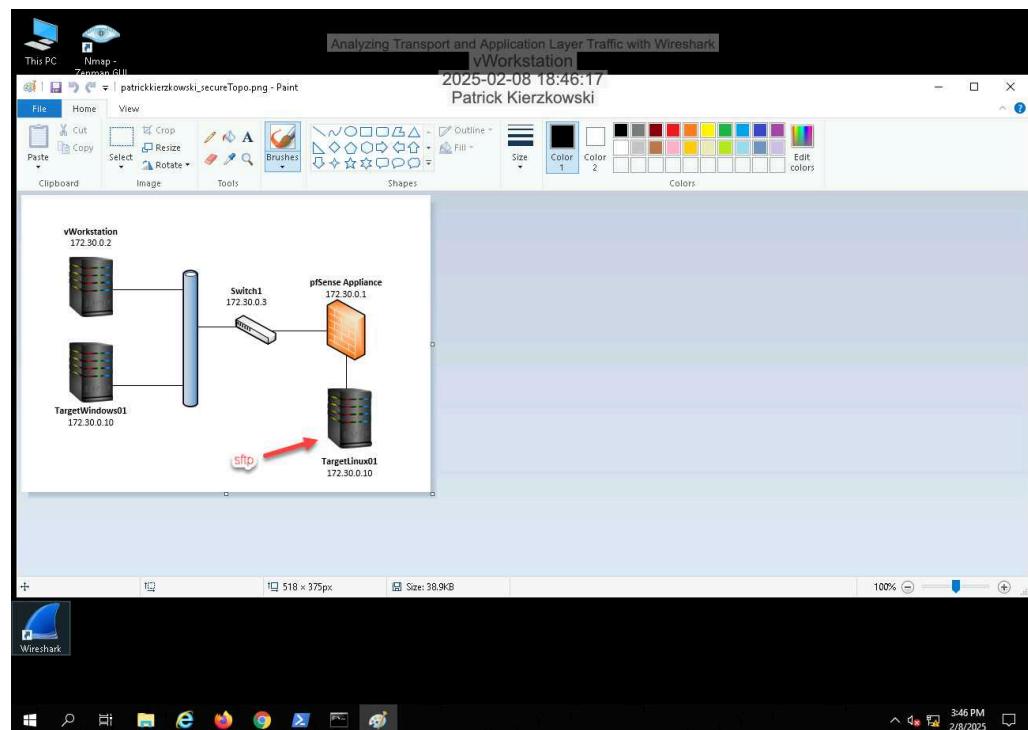
Analyzing Transport and Application Layer Traffic with Wireshark

Fundamentals of Communications and Networking, Third Edition - Lab 03

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.

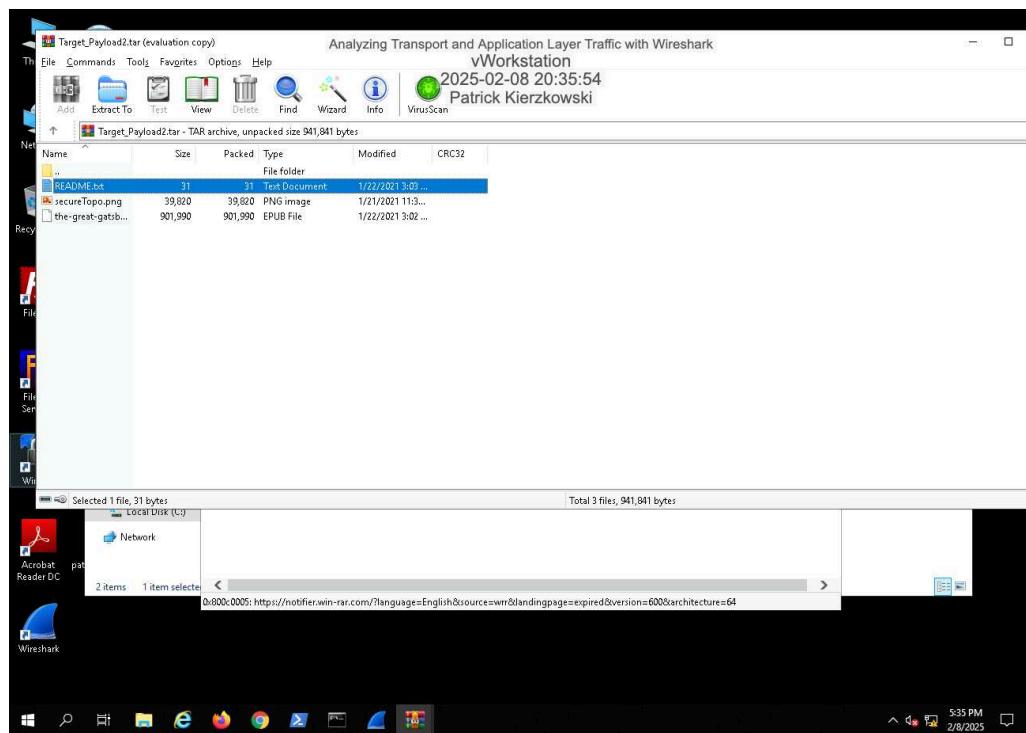
52 61 72 21 1A 07 01 00

Record the name of the correct RAR archive file.

Target_Payload2.rar

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.

The code is {JBL-80802600-SaaS}