CIS 457: Data Communications
Week 06 Assignment: Working with FTP Protocol
Point Value: 13 Pts, late submission policy (20%/day for up to 5 days)
Due Date: 2/23/2024 by 12:00 AM EST
Submission format:

The following reports will be submitted on Blackboard (BB) using each group member's account.
(1) The entire assignment's solution in a PDF format (your contribution to the assignment)
(2) Group's Agreed-upon solution in a PDF format.
(3) Group Code as requested in the assignment.
Note: Missing an individual's contribution leads to receiving **NO** credit for the assignment.

Objectives:

The purpose of this lab is to:

- Understand how the FTP protocol works
- Explore the format of the FTP commands and responses

Use Wireshark and download the Wireshark trace ftpRFC959.cap from Blackboard. The FTP Wireshark trace is captured between a local FTP machine with the IP address 192.168.0.101 and an FTP server machine with the IP address 128.9.176.20. Answer the following questions using the packet info listed in the ftpRFC959.cap

1. When this trace was captured, we specified a capture limit of 100 seconds. Give a possible reason for the trace to report less than 100 seconds.
2. How many packets appear in this trace?
3. Use the seventh packet (# 7) in the trace and answer the following questions:
    a. How large is the *Ethernet header*? How large is the entire *Ethernet frame*?
    b. How large is the *IP header*? the *IP datagram*/*Pkt*?
    c. How large is the *TCP header*? The *TCP segment*? You may consider drawing a picture of the packet with each piece identified.
4. Apply the following Wireshark string filters to the **ftpRFC959.cap**. Then, describe the output of each filter. How many packets are in each case?
   Filter #1: ftp.request.command
   Filter #2: ftp.response.code
5. Write a filter to capture only traffic sent from the IP address 192.168.0.101. What filter is used?
6. Record the packet number, source port number, and destination port number for all the TCP SYN packets for each of the four connections in the trace. (Hint: you may use the filter **tcp.flags.syn==1 && tcp.flags.ack==0** to display the SYN packets).
7. Draw a timeline showing when the control channel and each data channel begin and end. (Hint: Here, it is probably best to isolate each stream one at a time using its port numbers (e.g. tcp.dstport == 1932) and record the time of the first and last packet.)). Organize your answer in a tabular format such as shown below:

	Port on local machine	Port on server machine 128.9.176.20	Time 1st packet (SYN packet)	Time of Last packet
Control channel	1931	21		
Data channel 1 Directory listing for /	1932	34178		
Data channel 2 Directory listing for in-notes	1933	34188		
Data channel 3 Retrieve file	1934	34247		

8. On which connection (Control connection or Data connection):
   a. Is the ftp command (list) sent over??
   b. Is the list of files and directories sent over??

9. How long (approximately) did it take to transfer the file in **data connection 3**?

10. How can you determine the size of the file?

11. Compute the transfer rate (file size in (MB)/ time to send the file in (sec))?
(Hint: use this filter tcp.dstport == 1934. Then, select any packet that belongs to this connection and do a right mouse click and select Follow → TCP stream). Use the drop box on the bottom left corner of the obtained screen to determine the file size).