

Data Communications Laboratory

TCP & FTP

Your Name: Khalid Bakhshi

Your Student ID: 46392459

Documentation Task 1.

1. What is the name and IP address of the FTP server contacted? In which packets can this information be found (hint: you will need to clear the filter and examine the packets just before the first packets on port 21)?

Packet number: 79

Ip address: 156.21.1.54

Name: ftp.ftppplanet.com

2. What is the port used on the server?

Packet number 83

Port 21 is source port

3. What port is being used on the client?

Packet number 83

Port 2011 is the destination port

4. Identify the three-way handshake that established the TCP connection between the client and server. Which packet numbers does the three-way handshake appear in?

No.	Time	Source	Destination	Protocol	Length	Info
79	17.179545	10.46.38.218	156.21.1.54	TCP	62	2011 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
83	17.435715	156.21.1.54	10.46.38.218	TCP	62	21 → 2011 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
84	17.435771	10.46.38.218	156.21.1.54	TCP	54	2011 → 21 [ACK] Seq=1 Ack=1 Win=65535 Len=0

Appears in packet number

79, 83, and 84

5. The TCP connection is set by a SYN message from the FTP client, a SYN/ACK from the FTP server and an ACK from the client. What is happening in each of these messages?

Packet 79 the client send the sequence number 10221884863 to the acknowledgement number 0

Packet 83 the acknowledgement number 1021884863 is being sent to the sequence number 3491910592

Packet 85: the client acknowledges the handshake and accepts the both the sequence number: 1021884863 and the acknowledgement number 3491910593.

This Packet completes the handshake

6. Once the connection is established the FTP server sends a message saying it is ready. What packet carries this message?

Packet 85 carries the response code: Service ready for new user (220)

```
▼ File Transfer Protocol (FTP)
  ▼ 220 ftp.ftpplanet.com X2 WS_FTP Server 7.5(05332327)\r\n
    Response code: Service ready for new user (220)
    Response arg: ftp.ftpplanet.com X2 WS_FTP Server 7.5(05332327)
    [Current working directory: ]
```

7. What information in the packet makes you think you have the correct packet?

The packet contains the standard FTP server greeting: "Service ready for user (220)"

The packet is sent from the FTP server (port 21) to the client which confirms it's a server response

It appears immediately after the three way handshake and it's usually first response from the server, before any login or authentication

8. The user then types a user ID and a password. What packet numbers are involved in this exchange? Are the characters in the user ID sent individually or in a single packet? What is the username?

Packet number 124 and packet number 126 is involved in this exchange.

The username is anonymous. The character in the user ID is sent in a single packet.

```
220 ftp.ftpplanet.com X2 WS_FTP Server 7
USER anonymous
331 Enter password
PASS apassword
230 User logged in
PORT 10,46,38,218,19,137
200 Command PORT succeed
LIST
125 Transferring directory
226 Transfer completed
QUIT
221 bye
```

5 client pkts, 7 server pkts, 10 turns.

Entire conversation (251 bytes) Show as ASC

9. Can you see the password? If so, what is it?

Yes I can see the password. Password is apassword.

10. What is your conclusion about the security of FTP? Isn't packet sniffing fun?

FTP is not secure because it shows usernames and passwords in plaintext. This makes FTP vulnerable to packet sniffing and man in the middle attacks in unsecured wifi networks such as public wifi.

11. Find the single FTP command issued to the server. What is it and what message is it in?

Packet number: 160

The list command is the actual user issued FTP command asking the server to send back a directory listing.

The message:

125 Transferring directory

226 Transfer completed

160	32.371286	10.46.38.218	156.21.1.54	FTP	60 Request: LIST
-----	-----------	--------------	-------------	-----	------------------

12. In what packet(s) is the actual data sent from the server in response to that command? NOTE: that this will be in the FTP-DATA packets sent from the server on port 20.

The actual data was in packets 173 and 175. These contain the response to the LIST command. These packets come from the source port 20 on the FTP server and is directed to destination port 5001.

173	32.900345	156.21.1.54	10.46.38.218	FTP-DA...	113 FTP Data: 59 bytes (PORT) (LIST)
175	32.944431	156.21.1.54	10.46.38.218	FTP-DA...	1007 FTP Data: 953 bytes (PORT) (LIST)

13. Why do FTP and other protocols use a separate channel for command and data communications?

FTP uses separate channels for commands and data to make it more easier and more organized. The command channel stays open for sending instructions like login or file requests, while the data channel is only used when files or directory listing are being transferred. This setup allows better control during transfers.

14. In what packet does the client say it wants to end the FTP session?

Packet number 302

Contains the command QUIT and Server responds with 221 byte in packet number 303

302	58.672038	10.46.38.218	156.21.1.54	FTP	60 Request: QUIT
-----	-----------	--------------	-------------	-----	------------------

15. Which flag is set in this packet?

TCP ACK flag is set to acknowledge previous communication

This is shown in packet number 305

```
305 58.921155 10.46.38.218 156.21.1.54 TCP 54 2011 → 21 [ACK] Seq=71 Ack=183 Win=65354 Len=0
```

16. In what packet does the server respond?

Packet 303 server replies with Reponse: 221 bye

```
303 58.921075 156.21.1.54 10.46.38.218 FTP 63 Response: 221 bye
```

17. What messages are used to close the TCP connection?

Packet no	Flags	Description
304	FIN, ACK	Clients starts termination
305	ACK	Server acknowledges the FIN
306	RST, ACK	Client resets the connection

18. Which end – client or server – actually terminates the TCP connection?

The client terminates the TCP connection.

Packet 302 send the FTP quit command

Packet 304 sends TCP FIN, ACK which is the first step in terminating conneciton

Packet 306 the client sends a RST, ACK, fully closing/resetting the connection.

19. What are the sequence numbers used in these messages?

Packet number 304: Seq= 182

Packet number 305: Seq= 71

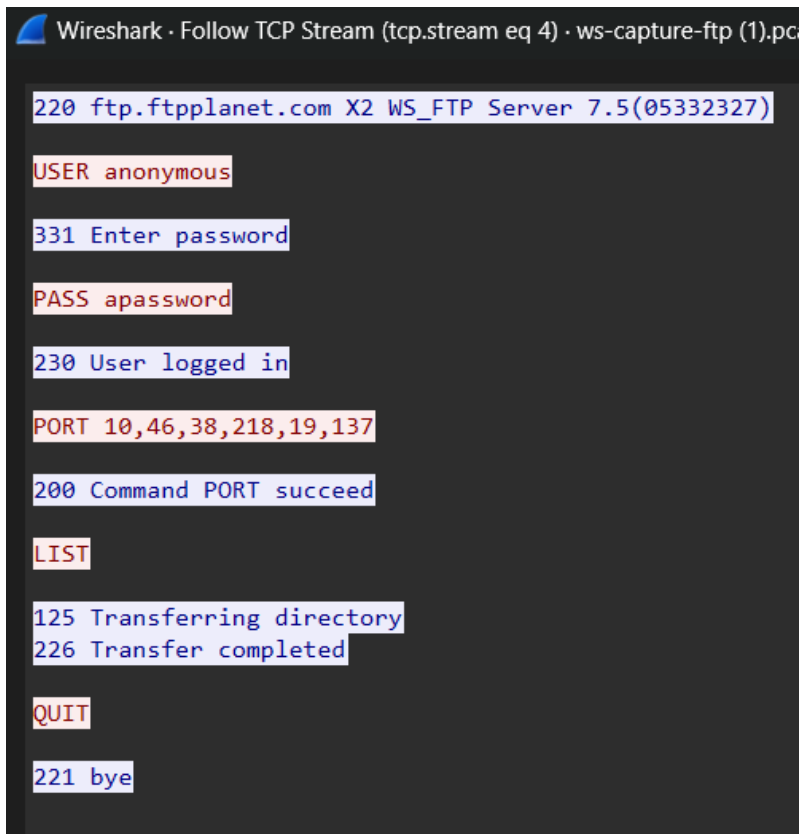
Packet number 306: Seq= 71

20. Compare the sequence numbers displayed in Wireshark's analysis against the actual values shown in the raw packet in the bottom pane – are they the same? Can you suggest why?

No they arent the same. This is due to ease of analysis.

21. Select the first message in the command (port 21) conversation. Use the "Follow TCP Stream" option in the Wireshark Analyze Menu to see a summary of the information that is exchanged between the client and server. Does the result show the password?

Yes it does



```

Wireshark · Follow TCP Stream (tcp.stream eq 4) · ws-capture-ftp (1).pcap

220 ftp.ftpplanet.com X2 WS_FTP Server 7.5(05332327)

USER anonymous

331 Enter password

PASS apassword

230 User logged in

PORT 10,46,38,218,19,137

200 Command PORT succeed

LIST

125 Transferring directory
226 Transfer completed

QUIT

221 bye

```

22. Select the first message on the data port (20). Display it as a stream – what data is being transferred?
 Its part of a directory listing transferred from the server to the client in response to the LIST command. It shows the contents of the server's current directory including file and folder names, sizes, and timestamps.

23. Identify the three-way handshake for this connection – which end is initiating the connection: the client or the server?

Packet no 161: SYN flag

Packet no 162: SYN, ACK flag

Packet no 172: ACK flag

The server initiates the data connection from 20 to the client's port 5001. The three-way handshake occurs in packets 161, 162, 172.

24. Find the PORT command issued by the FTP client. How does the FTP server know where to send the data from this message?

Packet number 157: PORT 10,46,38,218,19,137

FTP client sends PORT command to packet 157

This tells the server to open a data connection to IP address 10.46.38.218 on port 5001. This server then uses this information to send data from port 20 to the client port.

25. In packets 174 and 178, the server sends two messages to the client (“125 Transferring directory” and “226 Transfer complete”) but there is only one ACK message from the client following both of these. Explain why two messages can have only one ACK.

In TCP, data is sent as a continuous stream of bytes. Each message from the server adds more bytes to that stream. When the client sends an ACK, it acknowledges the highest byte number received, not individual messages. So if the server sends two messages back-to-back (packets 174 and 178), and the client receives them without issue, it can send one ACK that confirms both were received. This is more efficient and reduces unnecessary network traffic.