Muhammad Rizwan Khalid
BSCS - 6A
180459

Lab Title: *Analysis of FTP in Wireshark*

Objective of this lab:

In this lab, we will analyze the behavior of FTP in detail.

Instructions:

Read carefully before starting the lab.

These exercises are to be done individually.

You are supposed to provide the answers to the questions listed at the end of this document (substantiate your answers with screen shots of your Wireshark captures) and upload the completed report to your course's LMS site.

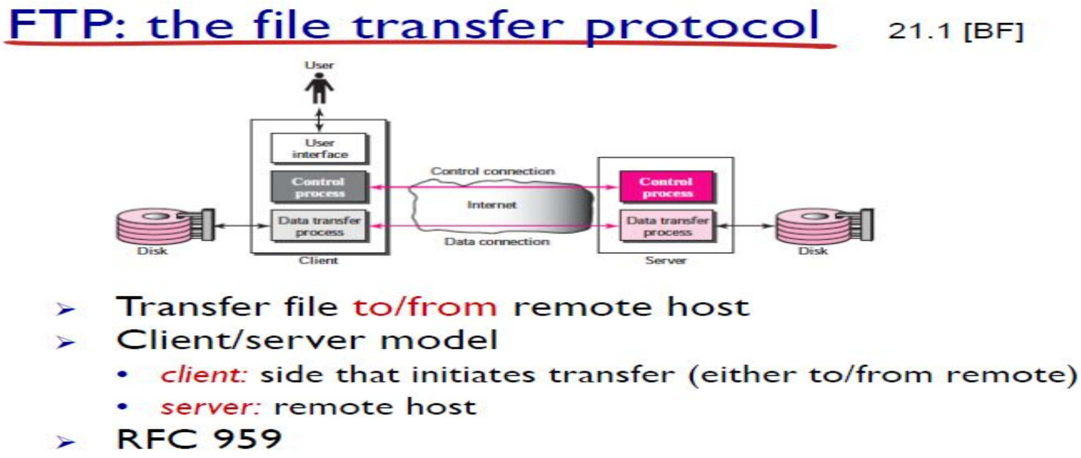
Avoid plagiarism by copying from the Internet or from your peers. You may refer to source/ text but you must paraphrase the original work.

Background:

FTP (File Transfer Protocol) is a simple application layer protocol (based on client/server network architecture). FTP is primarily used for transfer of files between the client and server.

Pl go through the lecture slides to revise the following important concepts regarding FTP:

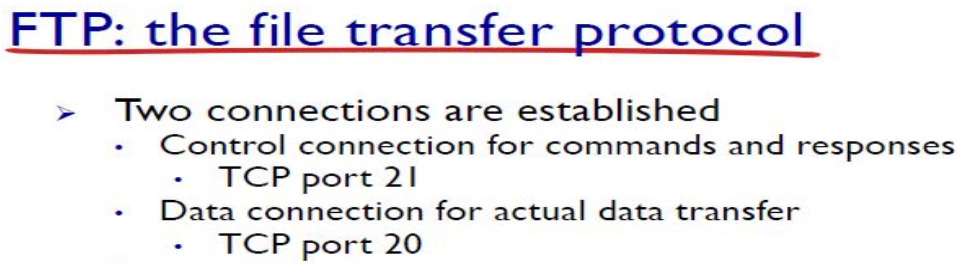
1. FTP uses out of band signaling
2. FTP uses two separate TCP connections, one for control and the other one for data
3. FTP control connection is persistent, while the data connection is non-persistent
4. FTP can work in either active or passive mode
5. There are several commands and responses available in FTP protocol



FTP: the file transfer protocol

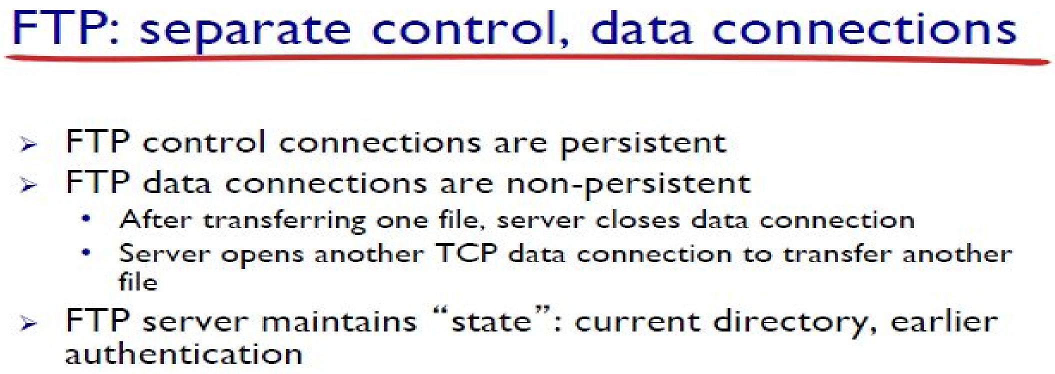
21.1 [BF]

- Transfer file to/from remote host
- Client/server model
  - *client:* side that initiates transfer (either to/from remote)
  - *server:* remote host
- RFC 959



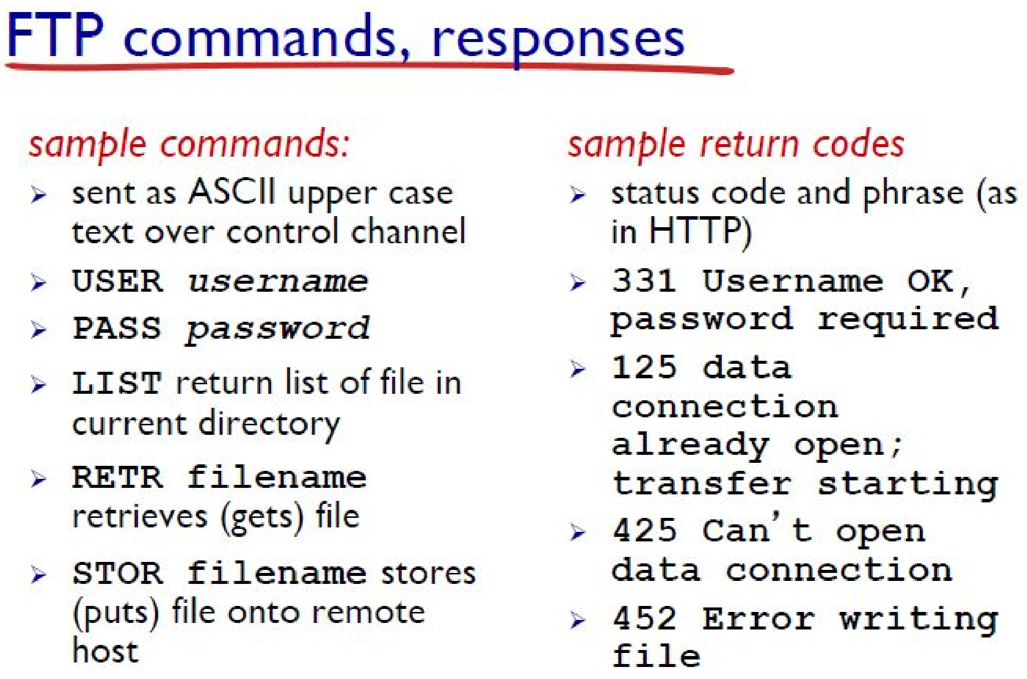
FTP: the file transfer protocol

- Two connections are established
  - Control connection for commands and responses
    - TCP port 21
  - Data connection for actual data transfer
    - TCP port 20



FTP: separate control, data connections

- FTP control connections are persistent
- FTP data connections are non-persistent
  - After transferring one file, server closes data connection
  - Server opens another TCP data connection to transfer another file
- FTP server maintains “state”: current directory, earlier authentication



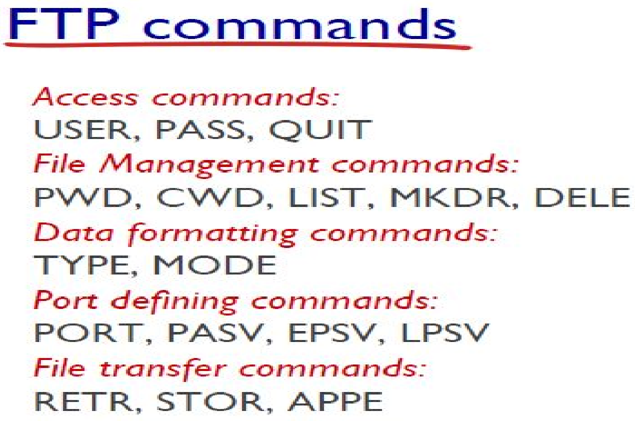
FTP commands, responses

sample commands:

- sent as ASCII upper case text over control channel
- `USER` *`username`*
- `PASS` *`password`*
- `LIST` return list of file in current directory
- `RETR filename` retrieves (gets) file
- `STOR filename` stores (puts) file onto remote host

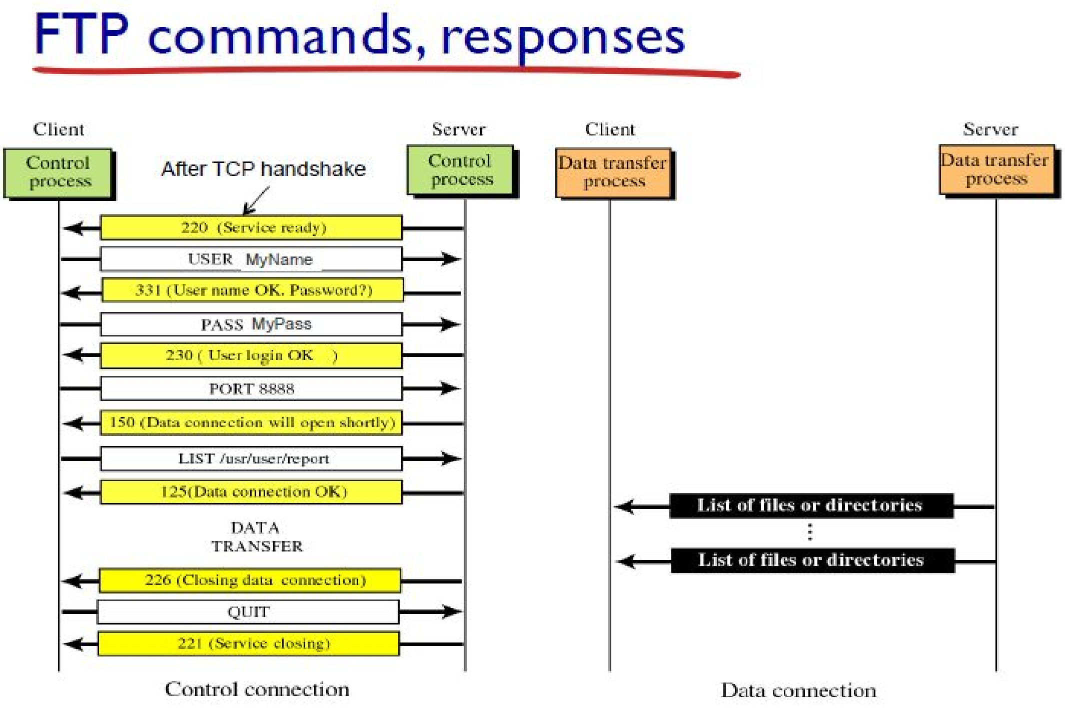
sample return codes

- status code and phrase (as in HTTP)
- `331 Username OK, password required`
- `125 data connection already open; transfer starting`
- `425 Can't open data connection`
- `452 Error writing file`



FTP commands

Access commands:
USER, PASS, QUIT
File Management commands:
PWD, CWD, LIST, MKDR, DELE
Data formatting commands:
TYPE, MODE
Port defining commands:
PORT, PASV, EPSV, LPSV
File transfer commands:
RETR, STOR, APPE



Steps for performing this lab:

There are 2 parts of this lab. A and B.

A. *Do the following:*

1. ***Start up the Wireshark software.***
2. ***Begin packet capture,*** *select the Capture pull down menu and select Options.*
3. ***Selecting the network interface on which packets would be captured:*** *You can use most of the default values in this window. The network interfaces (i.e., the physical connections) that your computer has to the network will be shown in the Interface pull down menu at the top of the Capture Options window. Click Start. Packet capture will now begin*
4. ***Open command prompt*** *and use command ftp ftp.cdc.gov*
5. ***Use anonymous as username and guest as password***
6. ***Type 'exit'***
7. ***Stop the wireshark capture***

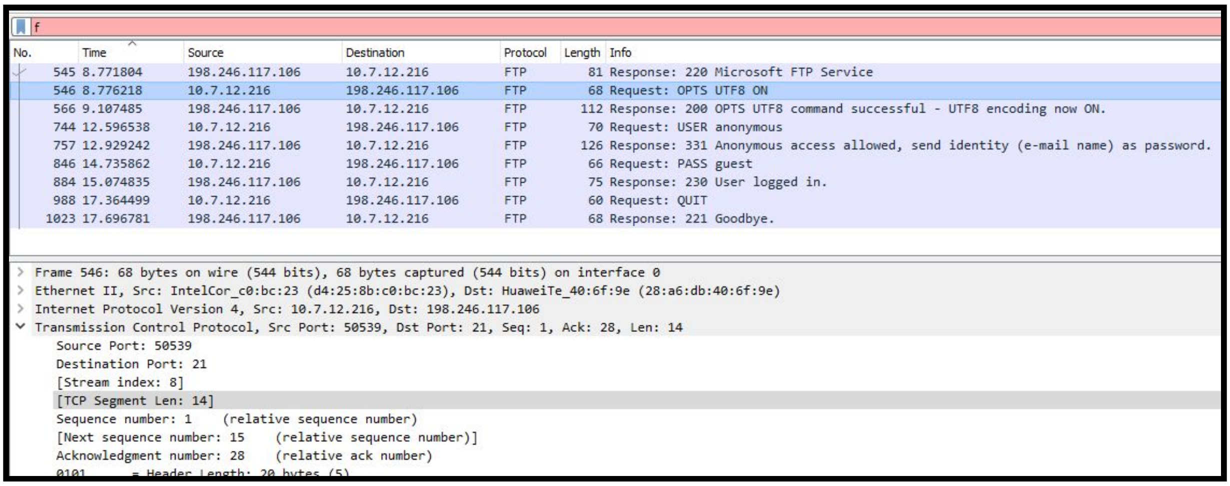
Questions:

1. *What other protocols does FTP require for its working?*

Answer: *FTP itself uses the TCP transport protocol. It never uses UDP for its transport needs.*

2. *How many TCP connections are formed by FTP in this transaction? What is the source IP, source port No, destination IP and destination port No for the "Control connection" of FTP for this interaction?*

Answer: *As we did not transfer any data so only one TCP connection as a control connection is formed when we connect to FTP transaction. Source ip is* ***10.7.12.216*** *with port no* ***50539.*** *The destination ip is* ***198.246.117.106.*** *and port is* ***21.]***

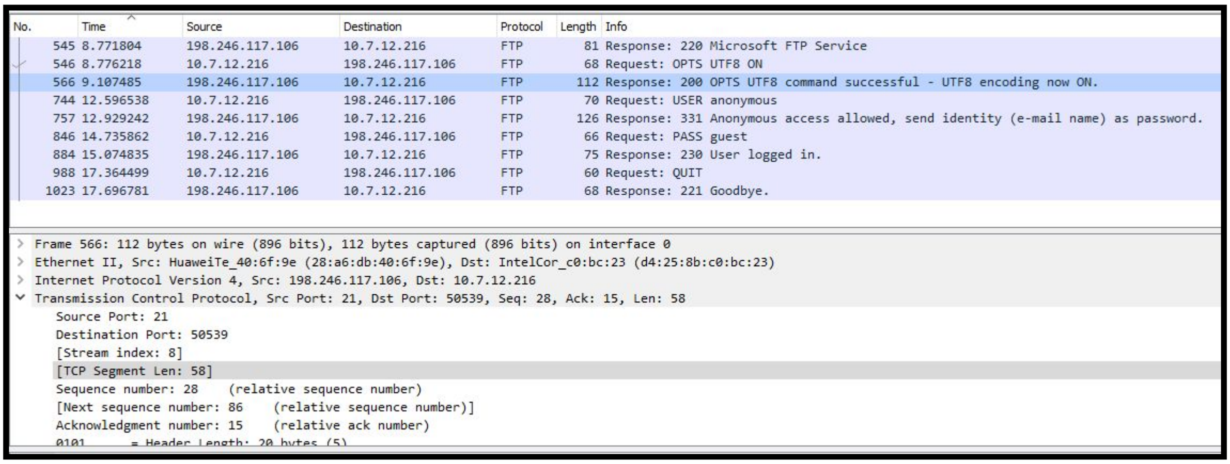


```
f
No.   Time        Source           Destination      Protocol Length Info
  545 8.771804    198.246.117.106  10.7.12.216      FTP         81 Response: 220 Microsoft FTP Service
  546 8.776218    10.7.12.216      198.246.117.106  FTP         68 Request: OPTS UTF8 ON
  566 9.107485    198.246.117.106  10.7.12.216      FTP        112 Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
  744 12.596538   10.7.12.216      198.246.117.106  FTP         70 Request: USER anonymous
  757 12.929242   198.246.117.106  10.7.12.216      FTP        126 Response: 331 Anonymous access allowed, send identity (e-mail name) as password.
  846 14.735862   10.7.12.216      198.246.117.106  FTP         66 Request: PASS guest
  884 15.074835   198.246.117.106  10.7.12.216      FTP         75 Response: 230 User logged in.
  988 17.364499   10.7.12.216      198.246.117.106  FTP         60 Request: QUIT
 1023 17.696781   198.246.117.106  10.7.12.216      FTP         68 Response: 221 Goodbye.

> Frame 546: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
> Ethernet II, Src: IntelCor_c0:bc:23 (d4:25:8b:c0:bc:23), Dst: HuaweiTe_40:6f:9e (28:a6:db:40:6f:9e)
> Internet Protocol Version 4, Src: 10.7.12.216, Dst: 198.246.117.106
v Transmission Control Protocol, Src Port: 50539, Dst Port: 21, Seq: 1, Ack: 28, Len: 14
    Source Port: 50539
    Destination Port: 21
    [Stream index: 8]
    [TCP Segment Len: 14]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 15    (relative sequence number)]
    Acknowledgment number: 28    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
```

3. *What is the first response code and message received from the FTP server on the control connection?*

Answer: *The response code is 200 while the message says "OPTS UTF8 command successful – UTF8 encoding now ON."*



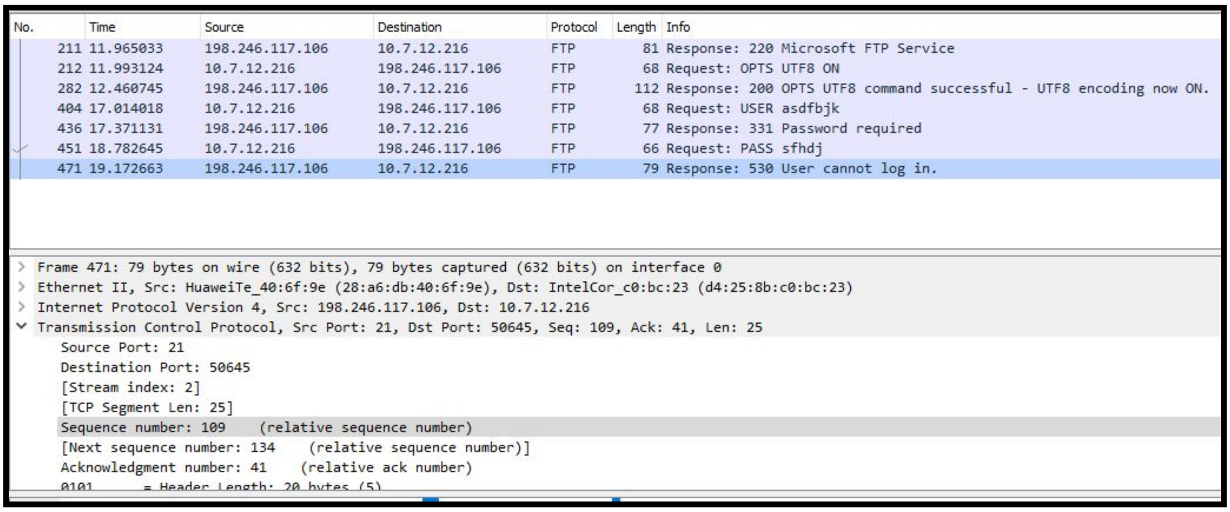
```
No.   Time        Source           Destination      Protocol Length Info
  545 8.771804    198.246.117.106  10.7.12.216      FTP         81 Response: 220 Microsoft FTP Service
  546 8.776218    10.7.12.216      198.246.117.106  FTP         68 Request: OPTS UTF8 ON
  566 9.107485    198.246.117.106  10.7.12.216      FTP        112 Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
  744 12.596538   10.7.12.216      198.246.117.106  FTP         70 Request: USER anonymous
  757 12.929242   198.246.117.106  10.7.12.216      FTP        126 Response: 331 Anonymous access allowed, send identity (e-mail name) as password.
  846 14.735862   10.7.12.216      198.246.117.106  FTP         66 Request: PASS guest
  884 15.074835   198.246.117.106  10.7.12.216      FTP         75 Response: 230 User logged in.
  988 17.364499   10.7.12.216      198.246.117.106  FTP         60 Request: QUIT
 1023 17.696781   198.246.117.106  10.7.12.216      FTP         68 Response: 221 Goodbye.

> Frame 566: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
> Ethernet II, Src: HuaweiTe_40:6f:9e (28:a6:db:40:6f:9e), Dst: IntelCor_c0:bc:23 (d4:25:8b:c0:bc:23)
> Internet Protocol Version 4, Src: 198.246.117.106, Dst: 10.7.12.216
v Transmission Control Protocol, Src Port: 21, Dst Port: 50539, Seq: 28, Ack: 15, Len: 58
    Source Port: 21
    Destination Port: 50539
    [Stream index: 8]
    [TCP Segment Len: 58]
    Sequence number: 28    (relative sequence number)
    [Next sequence number: 86    (relative sequence number)]
    Acknowledgment number: 15    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
```

4. *How many requests/responses are involved for authentication between the client and*

server? What response code and message does the server return when the authentication fails?

Answer: *There are three requests and responses involved in authentication between client and server as seen in the above pictures. If somehow authentication fails then response code 530 is returned saying "User cannot login". This is displayed in picture below:*

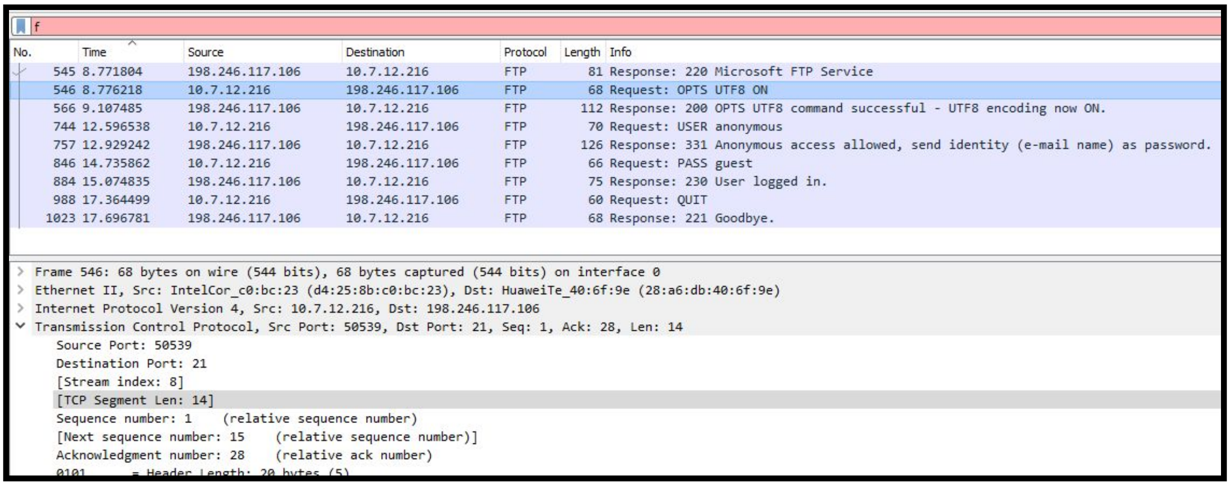


No.	Time	Source	Destination	Protocol	Length	Info
211	11.965033	198.246.117.106	10.7.12.216	FTP	81	Response: 220 Microsoft FTP Service
212	11.993124	10.7.12.216	198.246.117.106	FTP	68	Request: OPTS UTF8 ON
282	12.460745	198.246.117.106	10.7.12.216	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
404	17.014018	10.7.12.216	198.246.117.106	FTP	68	Request: USER asdfbjk
436	17.371131	198.246.117.106	10.7.12.216	FTP	77	Response: 331 Password required
451	18.782645	10.7.12.216	198.246.117.106	FTP	66	Request: PASS sfhdj
471	19.172663	198.246.117.106	10.7.12.216	FTP	79	Response: 530 User cannot log in.

```
> Frame 471: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
> Ethernet II, Src: HuaweiTe_40:6f:9e (28:a6:db:40:6f:9e), Dst: IntelCor_c0:bc:23 (d4:25:8b:c0:bc:23)
> Internet Protocol Version 4, Src: 198.246.117.106, Dst: 10.7.12.216
v Transmission Control Protocol, Src Port: 21, Dst Port: 50645, Seq: 109, Ack: 41, Len: 25
    Source Port: 21
    Destination Port: 50645
    [Stream index: 2]
    [TCP Segment Len: 25]
    Sequence number: 109    (relative sequence number)
    [Next sequence number: 134    (relative sequence number)]
    Acknowledgment number: 41    (relative ack number)
    0101       = Header Length: 20 bytes (5)
```

5. *What is the response code and message from server when the client sent 'QUIT'?*

Answer: *Response code is 221 while the message "Good Bye is returned." It is the last response as seen in the picture below.*



f

No.	Time	Source	Destination	Protocol	Length	Info
545	8.771804	198.246.117.106	10.7.12.216	FTP	81	Response: 220 Microsoft FTP Service
546	8.776218	10.7.12.216	198.246.117.106	FTP	68	Request: OPTS UTF8 ON
566	9.107485	198.246.117.106	10.7.12.216	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
744	12.596538	10.7.12.216	198.246.117.106	FTP	70	Request: USER anonymous
757	12.929242	198.246.117.106	10.7.12.216	FTP	126	Response: 331 Anonymous access allowed, send identity (e-mail name) as password.
846	14.735862	10.7.12.216	198.246.117.106	FTP	66	Request: PASS guest
884	15.074835	198.246.117.106	10.7.12.216	FTP	75	Response: 230 User logged in.
988	17.364499	10.7.12.216	198.246.117.106	FTP	60	Request: QUIT
1023	17.696781	198.246.117.106	10.7.12.216	FTP	68	Response: 221 Goodbye.

```
> Frame 546: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
> Ethernet II, Src: IntelCor_c0:bc:23 (d4:25:8b:c0:bc:23), Dst: HuaweiTe_40:6f:9e (28:a6:db:40:6f:9e)
> Internet Protocol Version 4, Src: 10.7.12.216, Dst: 198.246.117.106
v Transmission Control Protocol, Src Port: 50539, Dst Port: 21, Seq: 1, Ack: 28, Len: 14
    Source Port: 50539
    Destination Port: 21
    [Stream index: 8]
    [TCP Segment Len: 14]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 15    (relative sequence number)]
    Acknowledgment number: 28    (relative ack number)
    0101       = Header Length: 20 bytes (5)
```

B. *Do the following:*

1. ***Start up the Wireshark software.***

2. ***Begin packet capture,*** *select the Capture pull down menu and select Options.*

3. ***Selecting the network interface on which packets would be captured:*** *You can use most of the default values in this window. The network interfaces (i.e., the physical connections) that your computer has to the network will be shown in the Interface pull*

down menu at the top of the Capture Options window. Click Start. Packet capture will now begin

4. ***Open winscp and change the file protocol to FTP. Enter*** *ftp.cdc.gov in the Host name.*

5. ***Use anonymous as username and guest as password***

6. ***Drag and drop 'Readme' file from the FTP server to your local drive.***

7. ***Drag and drop 'welcome.msg' file from the FTP server to your local drive.***

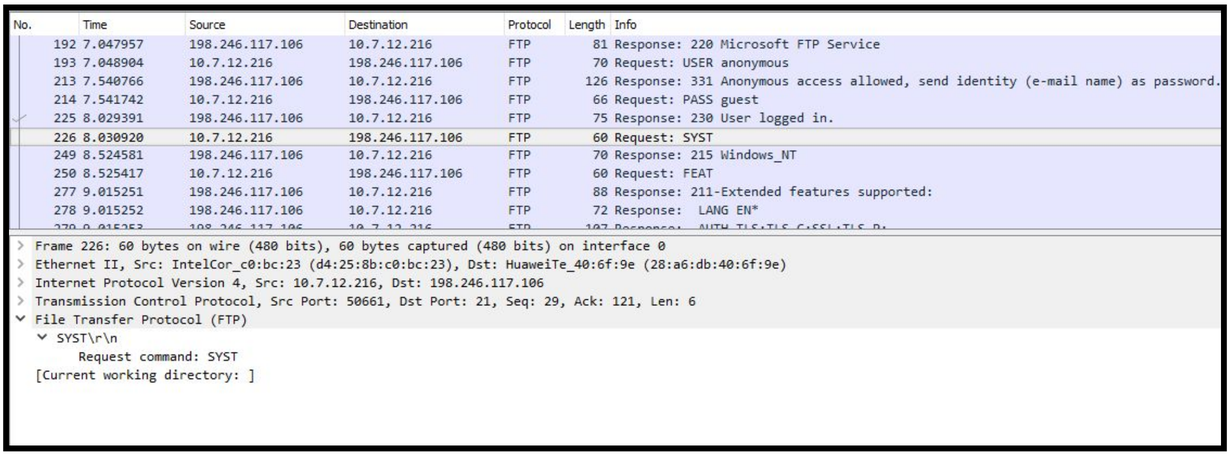
8. ***Type 'F10' to terminate the application.***

9. ***Stop the Wireshark capture.***

Questions:

1. *Once the user is authenticated, the client asks for 'SYST' and 'FEAT'. What is being asked and what are the responses by the server?*

Answer: *Client asks for SYST and FEAT after the authentication. SYST request asks the information about the server's operating system. The server gives response with response code of **215** saying that its os is **Windows_NT.** FEAT command asks the server if it supports the extended features. The server gives response with response code of **211** saying "**Extended features supported**".*



No.	Time	Source	Destination	Protocol	Length	Info
192	7.047957	198.246.117.106	10.7.12.216	FTP	81	Response: 220 Microsoft FTP Service
193	7.048904	10.7.12.216	198.246.117.106	FTP	70	Request: USER anonymous
213	7.540766	198.246.117.106	10.7.12.216	FTP	126	Response: 331 Anonymous access allowed, send identity (e-mail name) as password.
214	7.541742	10.7.12.216	198.246.117.106	FTP	66	Request: PASS guest
225	8.029391	198.246.117.106	10.7.12.216	FTP	75	Response: 230 User logged in.
226	8.030920	10.7.12.216	198.246.117.106	FTP	60	Request: SYST
249	8.524581	198.246.117.106	10.7.12.216	FTP	70	Response: 215 Windows_NT
250	8.525417	10.7.12.216	198.246.117.106	FTP	60	Request: FEAT
277	9.015251	198.246.117.106	10.7.12.216	FTP	88	Response: 211-Extended features supported:
278	9.015252	198.246.117.106	10.7.12.216	FTP	72	Response: LANG EN*
279	9.015253	198.246.117.106	10.7.12.216	FTP	107	Response: AUTH TLS;TLS-C;SSL;TLS-P;

```
> Frame 226: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: IntelCor_c0:bc:23 (d4:25:8b:c0:bc:23), Dst: HuaweiTe_40:6f:9e (28:a6:db:40:6f:9e)
> Internet Protocol Version 4, Src: 10.7.12.216, Dst: 198.246.117.106
> Transmission Control Protocol, Src Port: 50661, Dst Port: 21, Seq: 29, Ack: 121, Len: 6
v File Transfer Protocol (FTP)
  v SYST\r\n
      Request command: SYST
  [Current working directory: ]
```

2. *How many TCP connections are formed by FTP in this transaction? What is the source IP, source port No, destination IP and destination port No for the "Control connection" and "Data connection" of FTP for this interaction?*

Answer: *Basically FTP uses two connections of TCP one is a control connection and the other is the data connection. Control connection uses port 21 while data connection uses port 20*

Control connection:

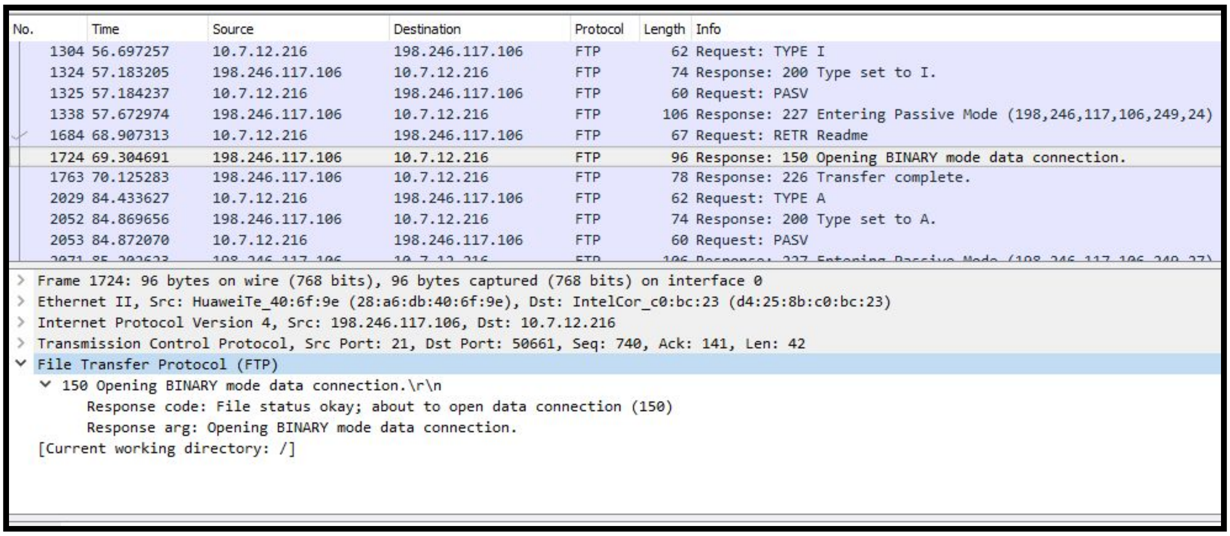
Source IP	***Source port***	***Destination IP***	***Destination port***
10.7.12.216	***50661***	***198.246.117.106***	***21***

Data connection:

Source IP	***Source port***	***Destination IP***	***Destination port***
10.7.12.216	***50661***	***198.246.117.106***	***21***

3. *What happens when you drag and drop ‘Readme’? List the conversation between the client and server (request code/message and response code/message).*

   Answer: *When we drop readme in local drive the request of “RETR readme” is sent. After the complete transfer of file response code of 226 is returned with the message “Transfer complete”.*



```
No.   Time       Source           Destination      Protocol Length Info
 1304 56.697257  10.7.12.216      198.246.117.106  FTP       62 Request: TYPE I
 1324 57.183205  198.246.117.106  10.7.12.216      FTP       74 Response: 200 Type set to I.
 1325 57.184237  10.7.12.216      198.246.117.106  FTP       60 Request: PASV
 1338 57.672974  198.246.117.106  10.7.12.216      FTP      106 Response: 227 Entering Passive Mode (198,246,117,106,249,24)
 1684 68.907313  10.7.12.216      198.246.117.106  FTP       67 Request: RETR Readme
 1724 69.304691  198.246.117.106  10.7.12.216      FTP       96 Response: 150 Opening BINARY mode data connection.
 1763 70.125283  198.246.117.106  10.7.12.216      FTP       78 Response: 226 Transfer complete.
 2029 84.433627  10.7.12.216      198.246.117.106  FTP       62 Request: TYPE A
 2052 84.869656  198.246.117.106  10.7.12.216      FTP       74 Response: 200 Type set to A.
 2053 84.872070  10.7.12.216      198.246.117.106  FTP       60 Request: PASV
 2071 85.203623  198.246.117.106  10.7.12.216      FTP      106 Response: 227 Entering Passive Mode (198,246,117,106,249,27)

> Frame 1724: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
> Ethernet II, Src: HuaweiTe_40:6f:9e (28:a6:db:40:6f:9e), Dst: IntelCor_c0:bc:23 (d4:25:8b:c0:bc:23)
> Internet Protocol Version 4, Src: 198.246.117.106, Dst: 10.7.12.216
> Transmission Control Protocol, Src Port: 21, Dst Port: 50661, Seq: 740, Ack: 141, Len: 42
v File Transfer Protocol (FTP)
  v 150 Opening BINARY mode data connection.\r\n
      Response code: File status okay; about to open data connection (150)
      Response arg: Opening BINARY mode data connection.
  [Current working directory: /]
```

4. *Which connection is closed when you type “Quit”?*

   Answer: *The window is closed by simply pressing F10 because there is no quit option(response) which wireshark can capture.*