# Department of Computer Science

**EE353: Computer Networks**

**Class: BSCS7AB**

# Lab 6: Analysis of FTP in Wireshark

# Date: 23 OCT 2019

**Lab Engineer: Kaleem Ullah**

# Instructor: Dr. Arsalan Ahmed

**Name: Hassan Shahzad Regn. No.: 211798**

***IP Screen Shot:***

***Lab Title:*** *Analysis of FTP in Wireshark*

***Objective of this lab:***

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

***Instructions:***

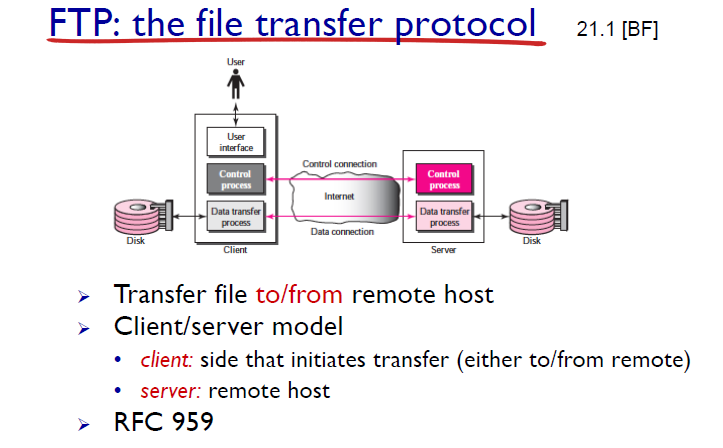
* *Read carefully before starting the lab.*
* *These exercises are to be done individually.*
* *You are supposed to provide the answers to the questions listed at the end of this document (substantiate your answers with screen shots of your Wireshark captures) and upload the completed report to your 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.*

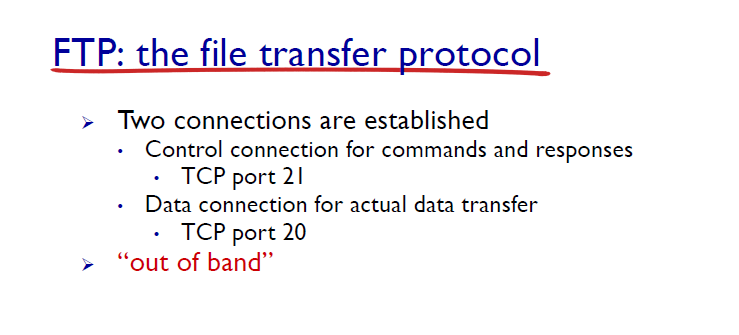
***Background:***

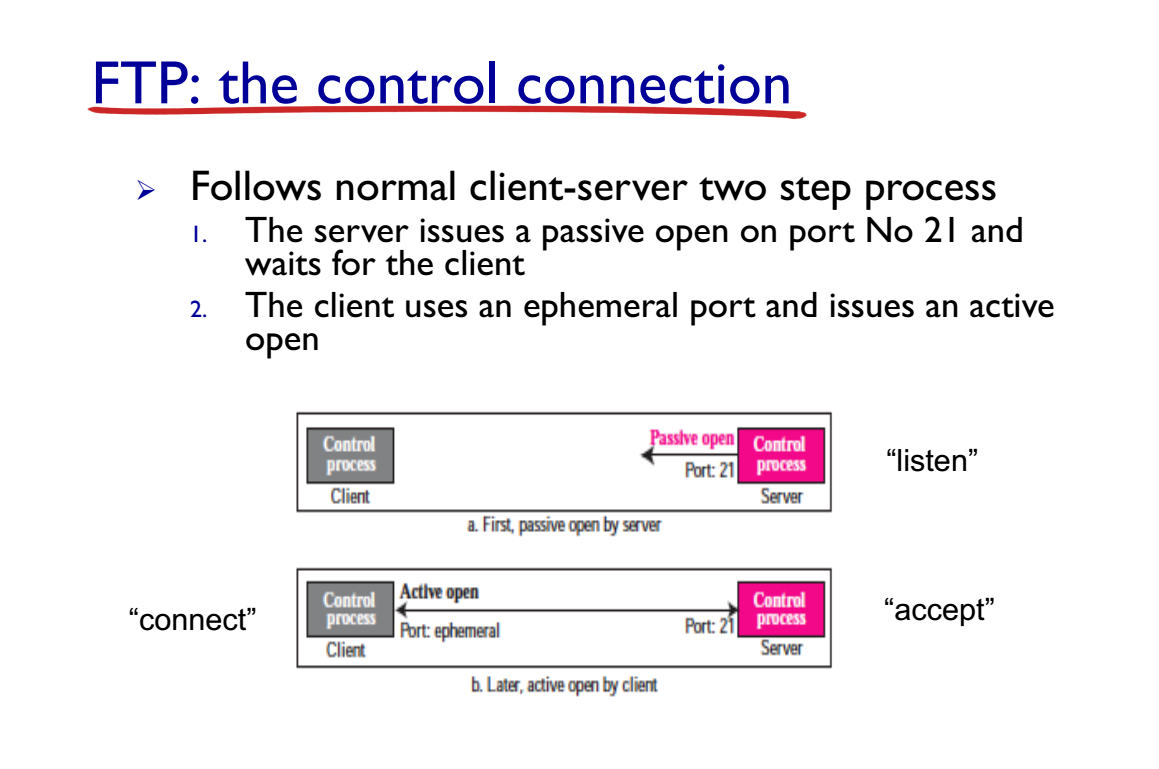
FTP (File Transfer Protocol) is a simple application layer protocol (based on client/server network architecture). FTP is primarily used for transfer of files between the client and server.

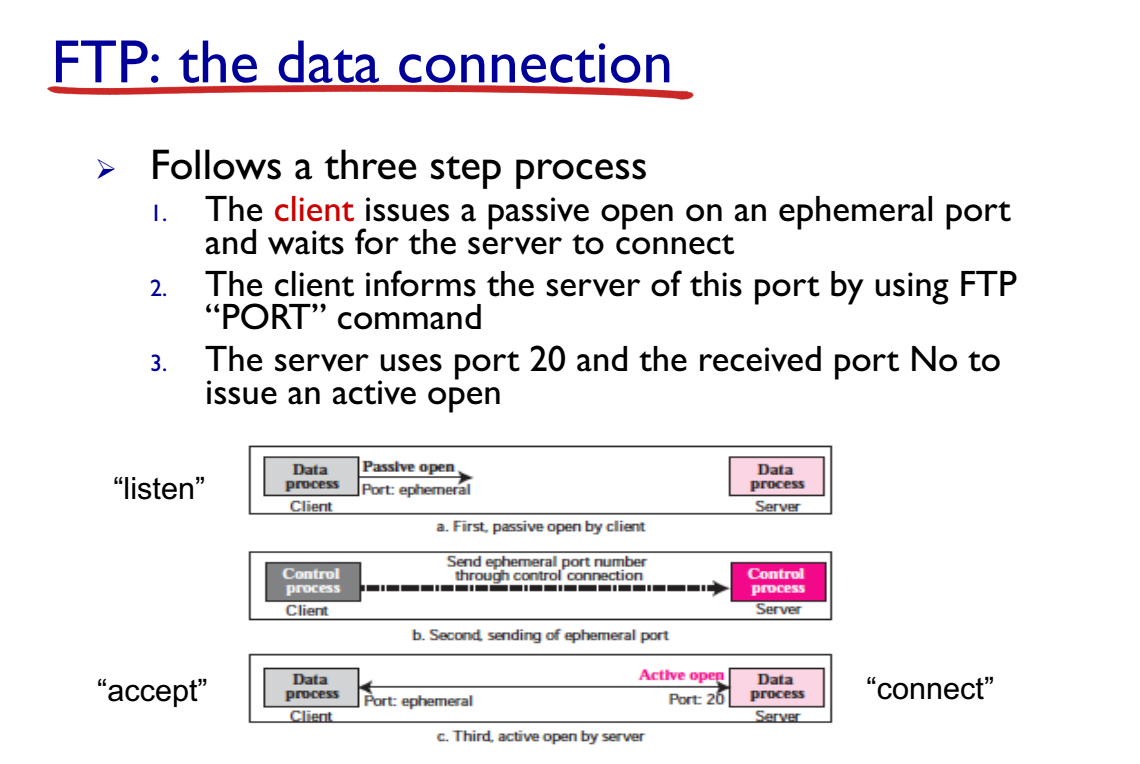
Pl go through the lecture slides to revise the following important concepts regarding FTP:

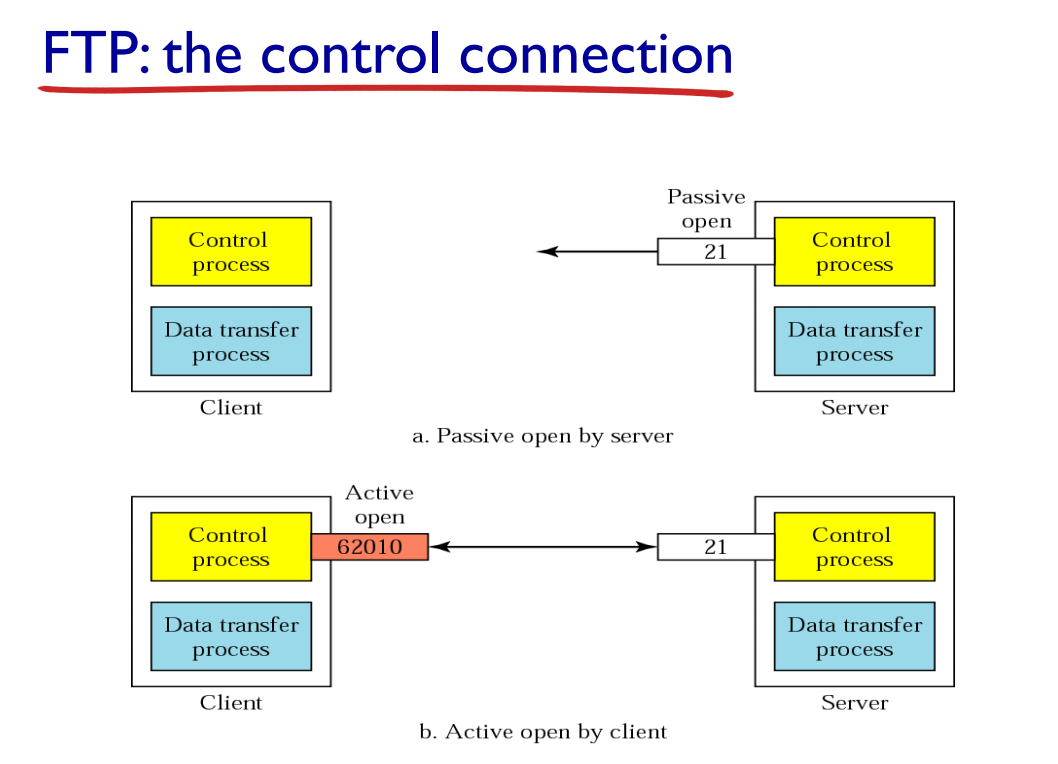
1. FTP uses out of band signaling
2. FTP uses two separate TCP connections, one for control and the other one for data
3. FTP control connection is persistent, while the data connection is non-persistent
4. FTP can work in either active or passive mode
5. There are several commands and responses available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

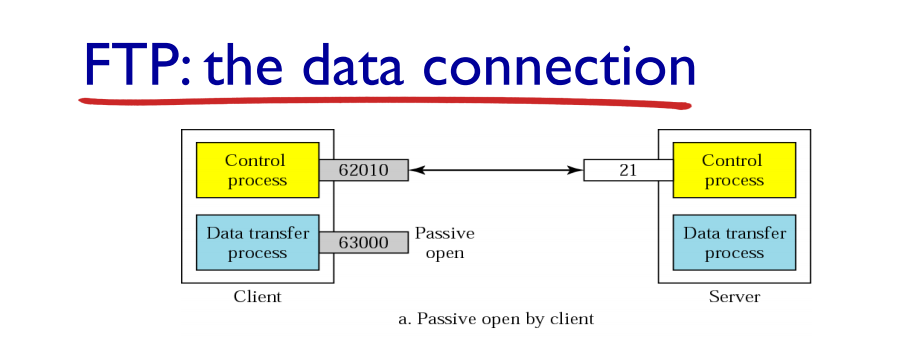


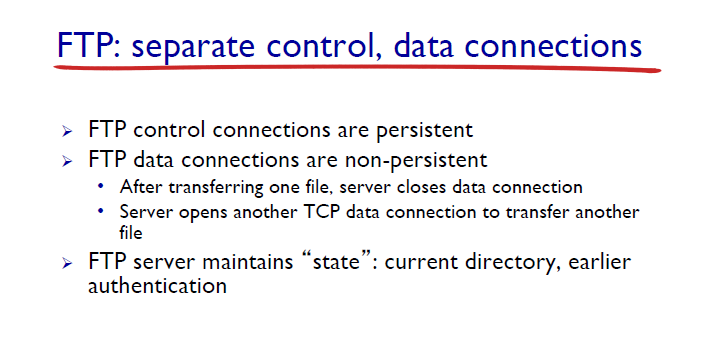


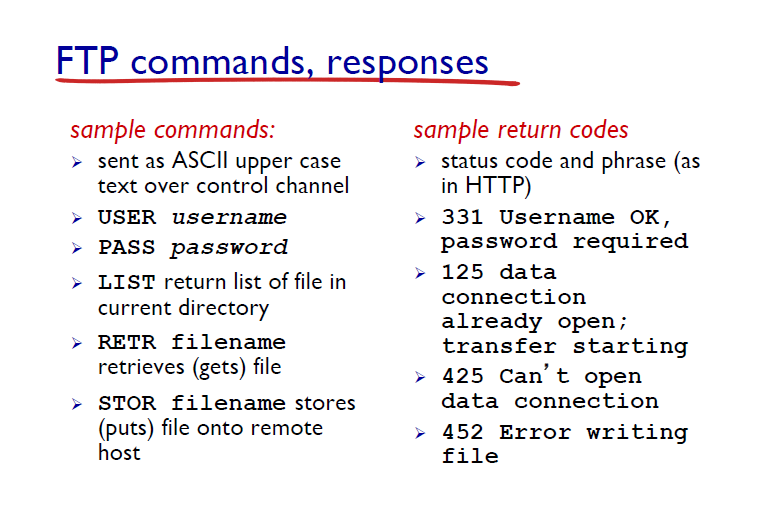


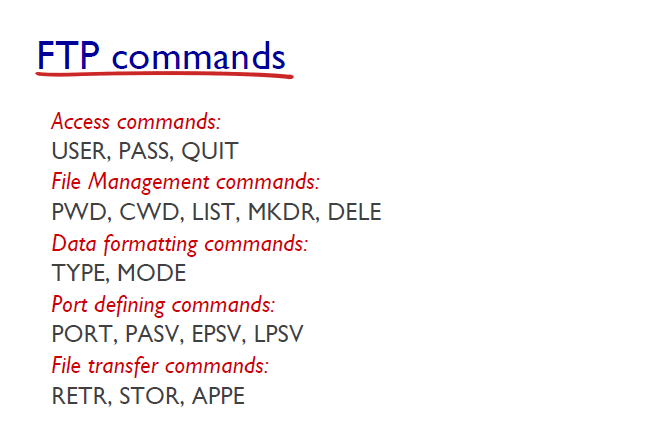


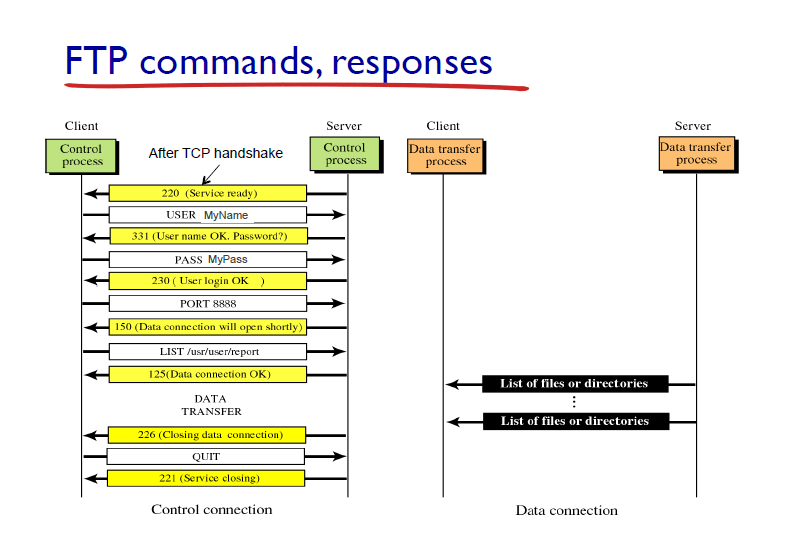










***Steps for performing this lab:***

*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*](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?*

***Ans: The other protocol FTP uses is:***

***Transmission Control Protocol***



1. *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?*

***Ans: Only One connection of TCP is formed by FTP in this transaction.***

***Source IP: 198.246.117.106***

***Destination IP: 10.3.93.216***

***Sort Port: 21***

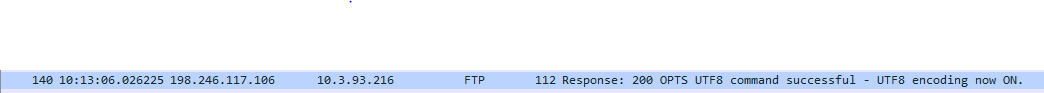
***Destination port: 54765***



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

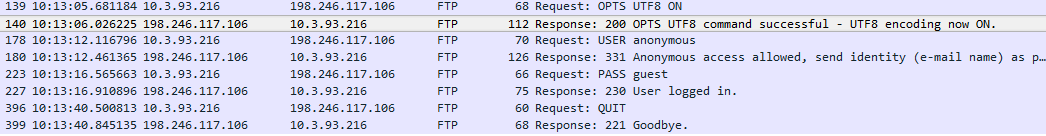
***Ans: The first response code and message received from FTP Server is:***

***112 Response: 200 OPTS UTF8 command successful – UTF encoding now ON.***



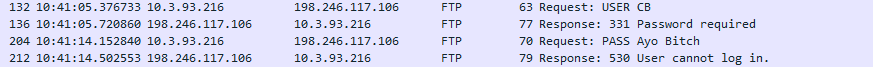
1. *How many requests/responses are involved for authentication between the client and server? What response code and message does the server return when the authentication fails?*

***Ans: The number of requests involved for authentication between server and client is: 4***



***The authentication fails when either username or password is incorrect or unknown. And the response code and message returned is:***

***530 User cannot log in.***



1. *What is the response code and message from server when the client sent ‘QUIT’?*

***Ans: The response code and message from the server when client sent ‘QUIT’ is:***

***221 Goodbye***



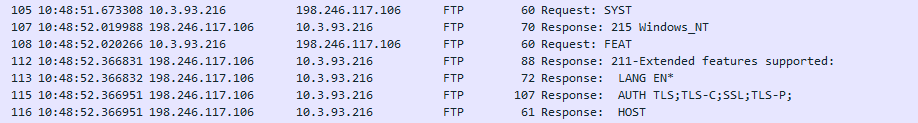
***B.*** *Do the following:*

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*](ftp://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?*

***Ans: The client asks ‘SYST’ and ‘FEAT’ one after the other respectively. The following responses are returned by the server:***



***SYST: In response the server displays the client operating system.***

***FEAT: In response the server shows info. Like the language, the AUTH TLS, HOST etc. on the client system***

1. *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?*

***Only one TCP Connection is established***



*Src: 198.246.117.106*

*Dst: 10.3.93.216*

*Src Port: 21*

*Dst Port: 54930*

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

***67 Request: RETR Readme***

***96 Response: 150 Opening BINARY mode data connection.***

***78 Response: 226 Transfer complete.***



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

***Session is terminated by pressing F10 button. So no connection is closed because we do not type ‘Quit’***

***Conclusion:***

***This lab taught us to learn and analyze with FTP.***