# Department of Computer Science

**EE353: Computer Networks**

**Submitted by:** M. Hasnain Naeem

**Registration No. :** 212728

**Class:** BSCS-7B

# Lab 8: *Analysis of FTP in Wireshark*

# Date: 4th Nov, 2019

**Lab Engineer: Engr. Kaleem Ullah**

# Instructor: Dr. Muhammad Zeeshan

***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.

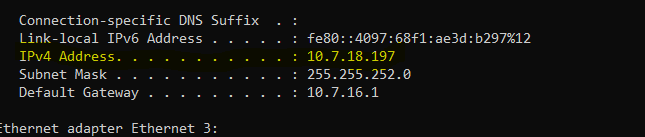
Pl go through the lecture slides to revise the following important concepts regarding FTP:

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

***Objectives:***

* *Getting familiar with FTP.*
* *Analyzing FTP packets using Wireshark.*

***IP Address:***



***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.org*](ftp://ftp.cdc.org)
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?*

*TCP transport layer protocol and IP network layer 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?*

*1 3-way-handshake connection is formed in this transaction to transfer control information. No connection is formed for the files.*

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

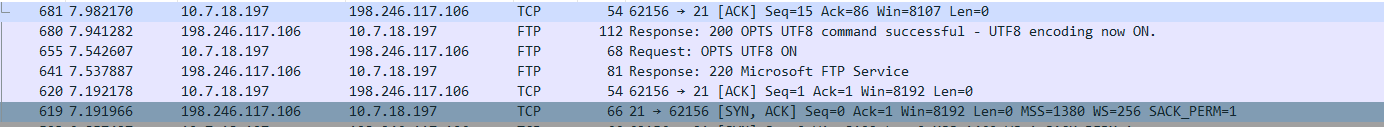
*Response Code: 220*

*Message: Microsoft FTP service.*



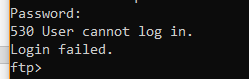
1. *How many requests/responses are involved for authentication between the client and server? What response code and message does the server return when the authentication fails?*

*6 connections are involved in authentication purpose.*



*Response code on authentication failure: 530*

*Message on authentication failure: User cannot log in.*



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

*Code: 221*

*Message: 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:***

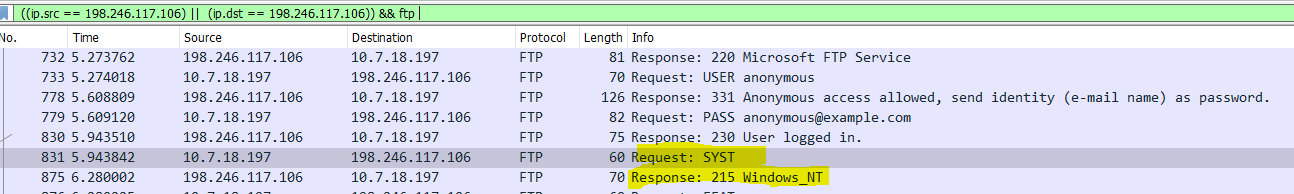
1. *Once the user is authenticated, the client asks for ‘SYST’ and ‘FEAT’. What is being asked and what are the responses by the server?*

***Purpose:***

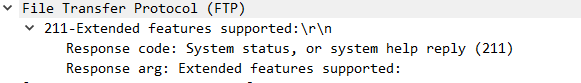
* ***SYST:*** *client is asking the server for its sytem type.*
* ***FEAT:*** *ask for the list of features implemented on server.*

***Responses:***

* ***SYST:*** *Windows\_NT*



* ***FEAT:*** *Empty body.*



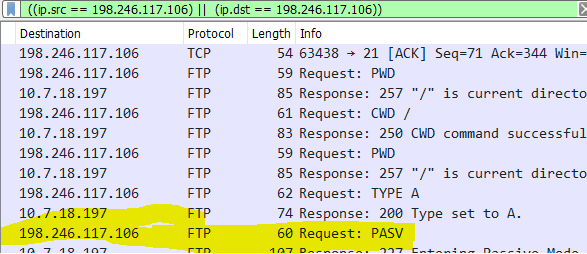
1. *How many TCP connections are formed by FTP in this transaction? What is the source IP, source port No, destination IP and destination port No for the “Control connection” and “Data connection” of FTP for this interaction?*

|  |  |
| --- | --- |
| ***Control Connection*** | **Data Connection** |
| *Source (Client):*  *10.7.18.197 : 63438*  *Destination (Server):*  *198.246.117.106 : 21* | *Source (Server):*  *198.246.117.106 : 54136*  *Destination(Client):*  *10.7.18.197 : 63550* |

1. *Who does the ‘passive open’ for the data connection, client or server? Which mode the FTP is working in (ACTIVE, PASSIVE, EPSV, LPSV)? Why?*

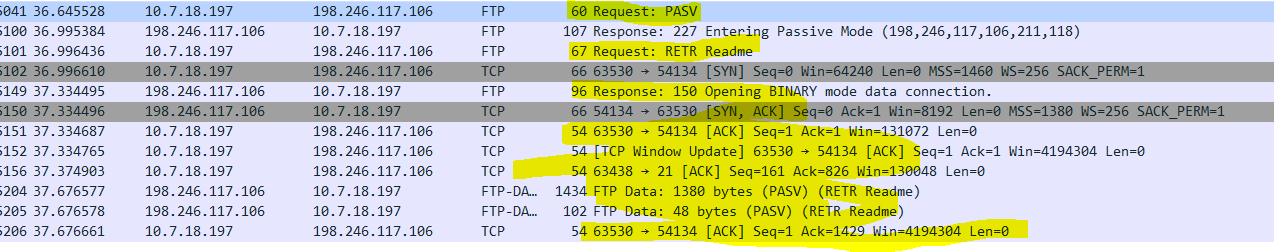
*Client does the passive open in FTP.*

*FTP is working in Passive mode because the client is requesting for the list of files. Moreover, it requests for files when we drag “readme” and “welcome.msg” files.*



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

* *Client requests to set the mode to “PASV”*
* *Server sets the mode to passive.*
* *Client asks requests for the “Readme” file using the RETR command.*
* *Server opens a binary mode data connection (TCP).*
* *Client acknowledges the connection.*
* *Then the data transfer begins.*
* *Client acknowledges the end of file.*



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

* *Both, control and data connections are closed when “Quit” is sent to the server. Hence, all the connections between server and client terminate, which ends the session.*

**Conclusion:**

FTP application layer protocol utilize the TCP transport layer protocol and IP network layer protocol to transfer files from one machine to another. We can analyze the FTP packets sent from the client to the server using Wireshark. We can look up the control information sent by client and server, plus, the data transferred between them.