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

***Name: Mujtaba Shahid Faizi***

***Regn No: 131818***

***Current IP Address: 10.99.7.201***

***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* www.taru2.com
5. ***Use ‘none’ as username and ‘none’ as password***
6. ***Type ‘quit’***
7. ***Stop the wireshark capture***

***Questions:***

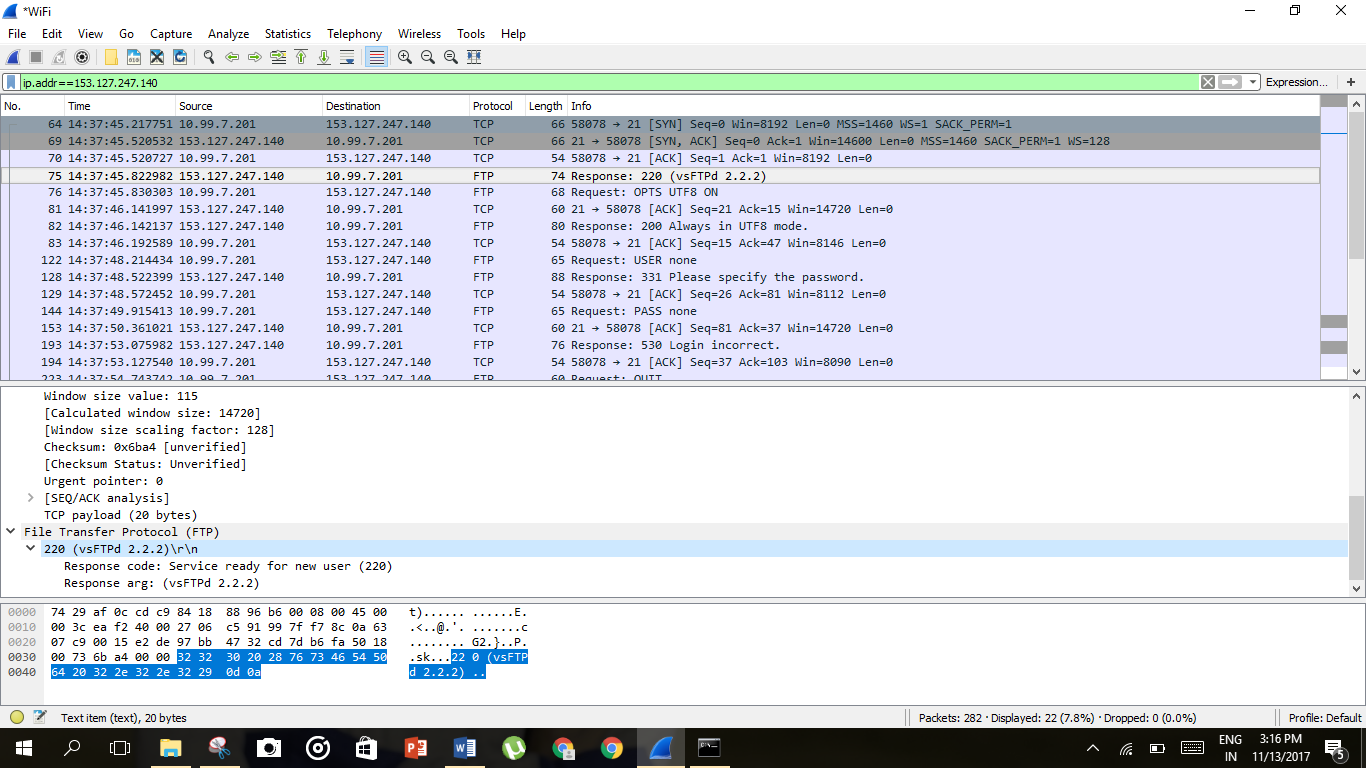
1. *How many TCP connections are formed by FTP in this transaction? What is the source IP, source port No, destination IP and destination port No for the “Control connection” of FTP for this interaction?*

*1 TCP connection.*

*SourceIP:*10.99.7.201 *Source Port no:21*

*Dest Port no: 58078*

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

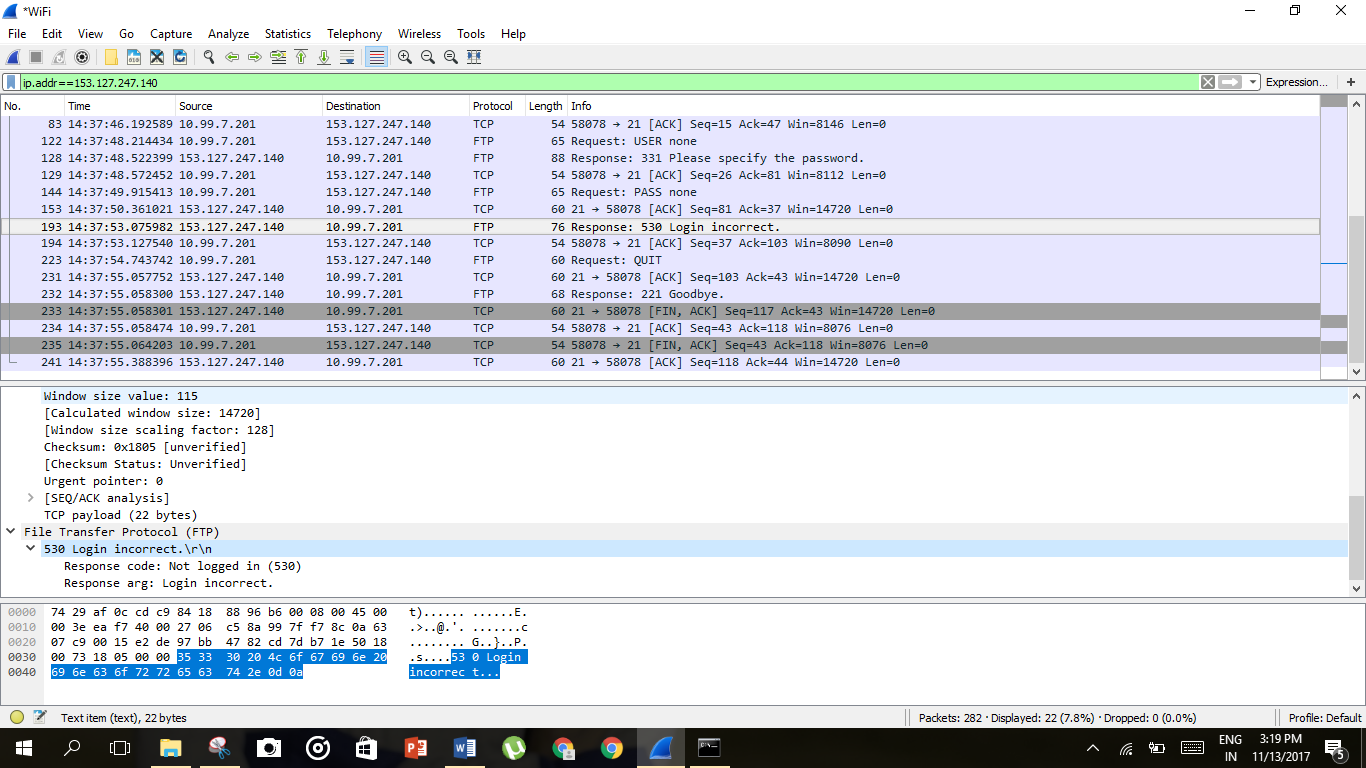




1. *How many requests/responses are involved for authentication between the client and server? What response code and message does the server return when the authentication fails?*

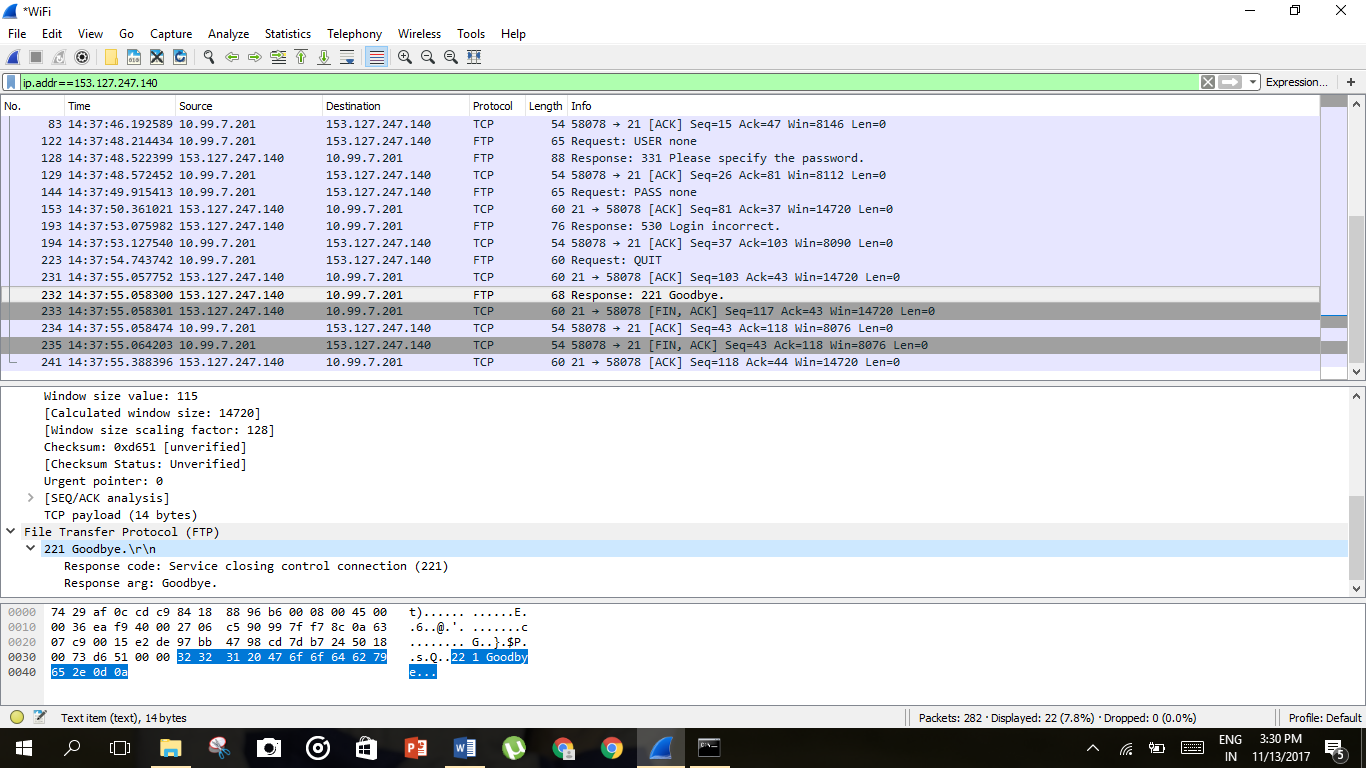
*5 responses, 4 requests*







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





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

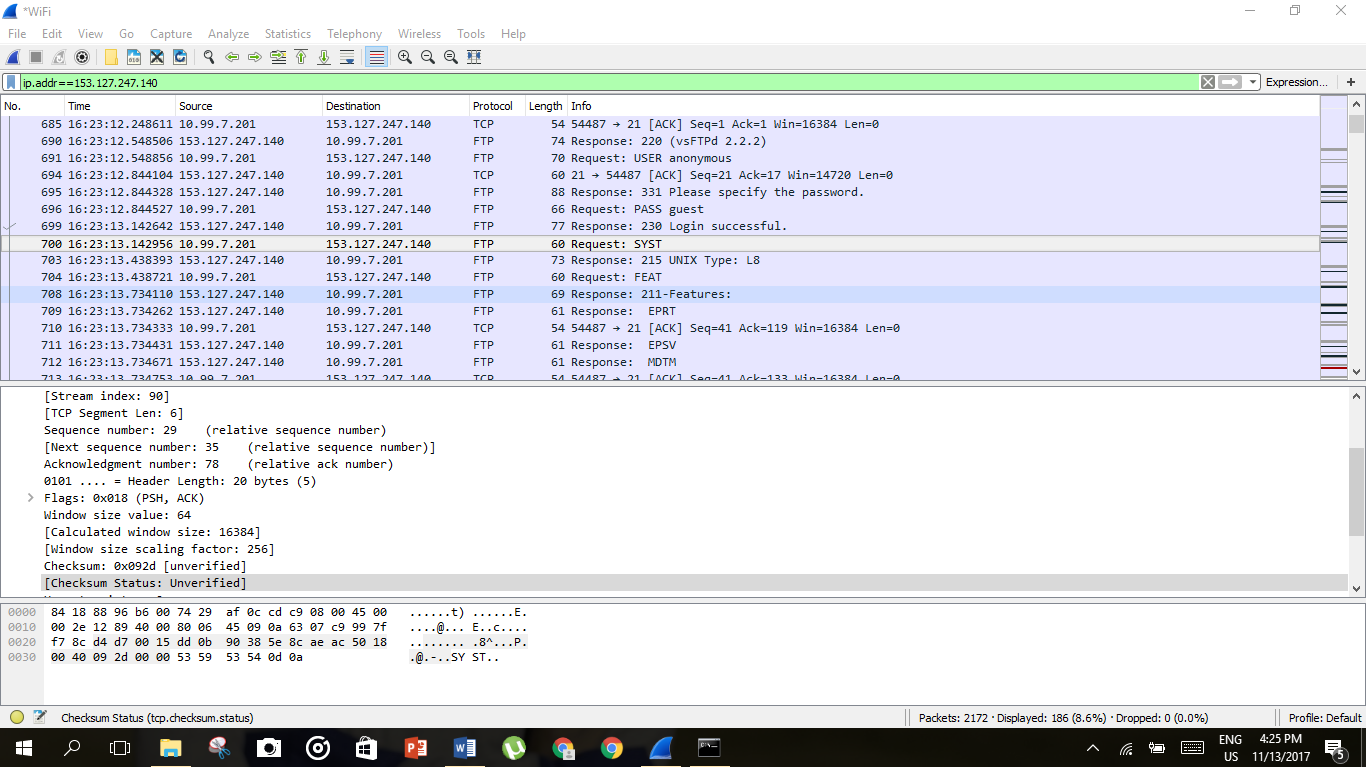
1. ***Start up the Wireshark software.***
2. ***Begin packet capture,*** *select the Capture pull down menu and select Options.*
3. ***Selecting the network interface on which packets would be captured:*** *You can use most of the default values in this window. The network interfaces (i.e., the physical 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***153.127.247.140 *in the Host name.*
5. ***Use anonymous as username and guest as password***
6. ***Locate the file ‘print.gif’ and Drag and drop this file from the FTP server to your local drive.***
7. ***Drag and drop ‘warning.gif’ 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?*

*SYST returns the system type of ftp server*

*FEAT returns the features implemented by server.*





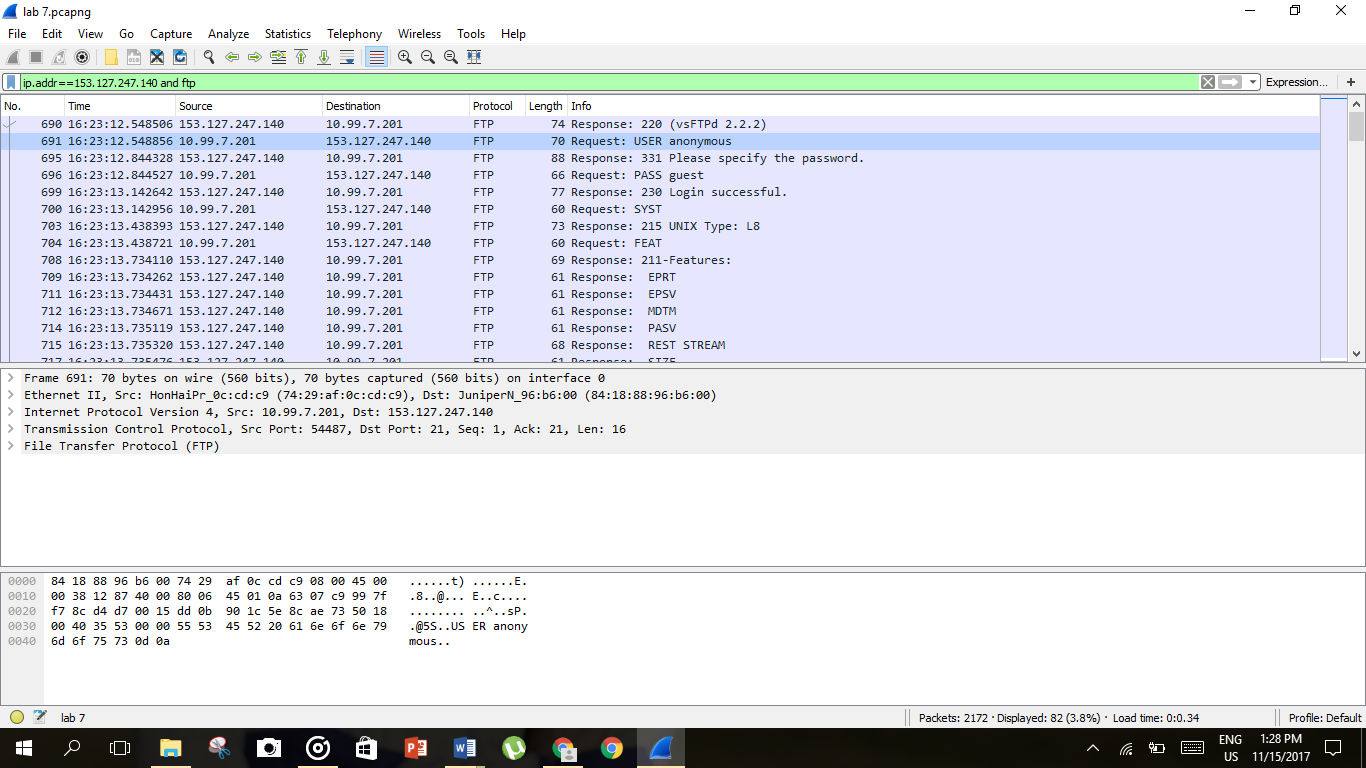
1. *How many TCP connections are formed by FTP in this transaction? What is the source IP, source port No, destination IP and destination port No for the “Control connection” and “Data connection” of FTP for this interaction?*

***Control connection:***

*Source IP:**10.99.7.201*

*Dest IP:* *153.127.247.140*

*SourcePort:54487  
Dest Port:21*



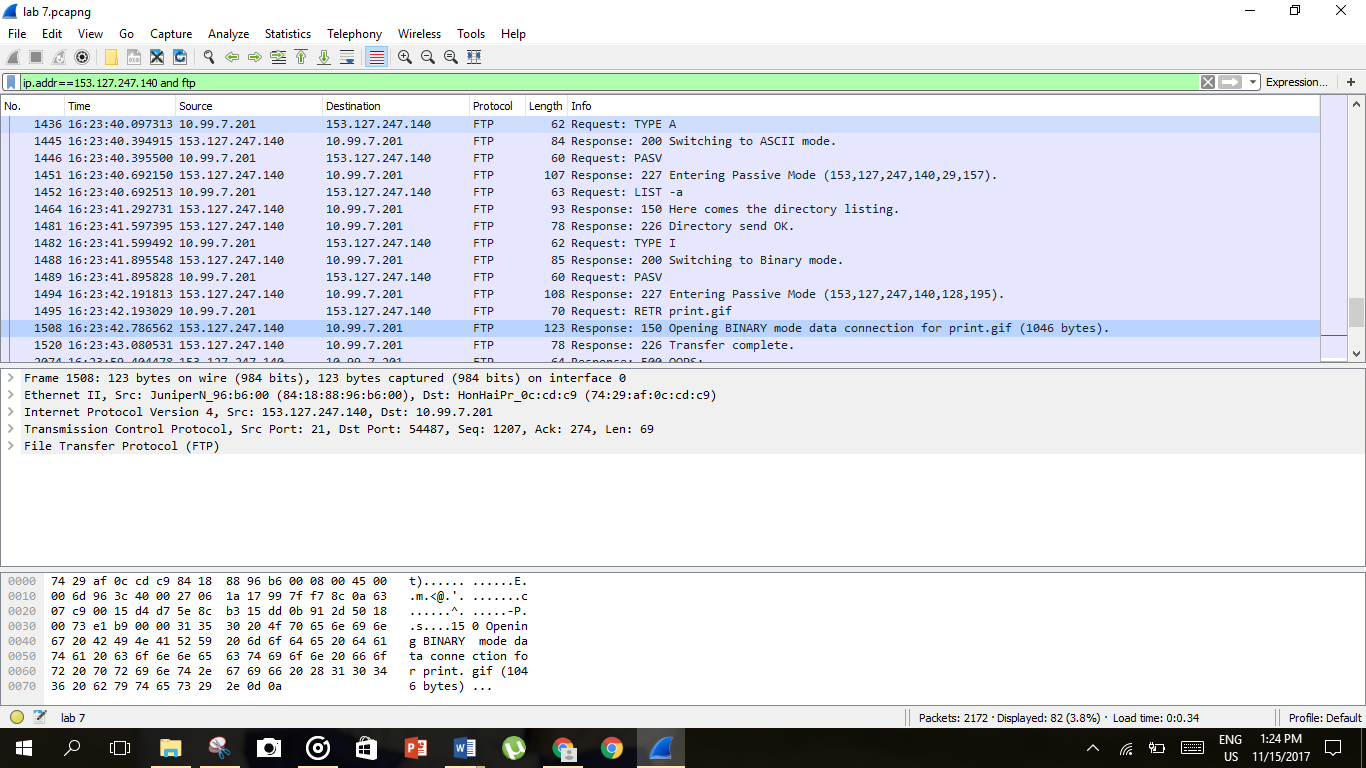


***Data connection:***

*Source IP:* *153.127.247.140*

*Dest IP:**10.99.7.201*

*SourcePort:21   
Dest Port:54487*





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?*

*In a passive connection* ***server opens a listening server*** *and* ***client initiates a connection****. The server is operating in a* ***PASSIVE mode*** *because the client establishes a connection for file retrieval. Client would need port forwarding for active connection to work.*

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

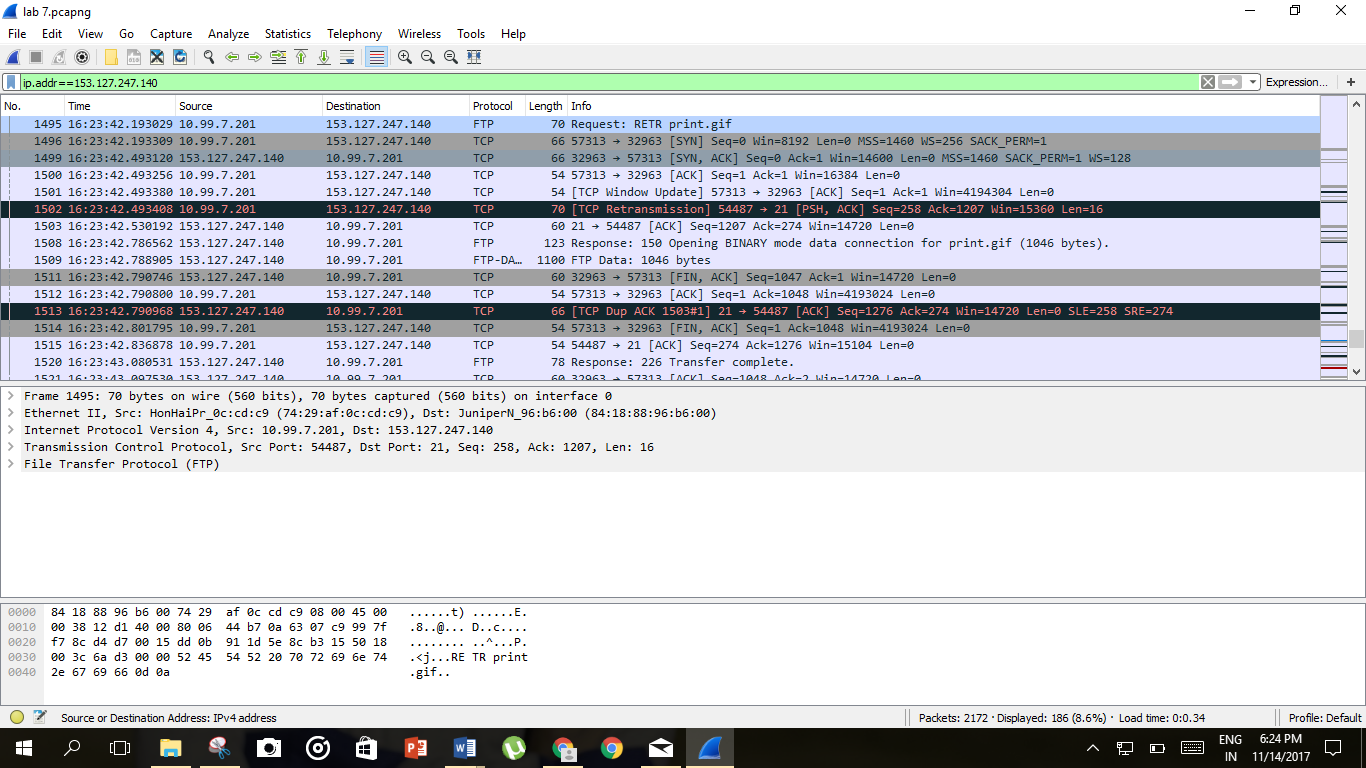
*Request Message: RETR print.gif*

*Response Code: 150*

*Response Message: Opening BINARY mode data connection.*

*Response Code: 226*

*Response Message: Transfer complete.*





1. *Which connection is closed when you type “F10”?*

*Control connection*