CS39006: Computer Networks Lab

Assignment 1 Report

Use Wireshark for Analyzing Network Packet Traces

Report by:

NISARG SHAH (15CS10030)

MAYANK BHUSHAN (15CS30019)

Objective:

The objective of this assignment is to understand some of the application layer protocols and use Wireshark tool to analyse their network packet traces. You have to use Wireshark for answering the questions.

PART I

Observing the packet traces obtained by accessing the HTTP server answer the following:

a. Classify the different ports of the HTTP (i.e., 8100, 8110 and 8111) into these classes namely, (i) HTTP 1.1 - with persistent connections, (ii) HTTP 1.1 - without persistent connections and (iii) HTTP 1.0. Justify your answer from the observations.

Solution:

Port: 8111
Type: HTTP 1.1 - with persistent connections

Port: 8110
Type: HTTP 1.1 - with non-persistent connections

Port: 8100
Type: HTTP 1.0

Justification:

HTTP 1.1 and HTTP 1.0 were distinguished using details provided by Wireshark.

The distinction between persistent and non-persistent connections were realised by observing the number of FIN messages. In persistent connection, we observed only one FIN message at the end to close the connection. Whereas in non-persistent connection, we observed FIN messages after each GET request.

b. How many GET requests were issued to access each of the three HTTP server instances?

Solutions:

17 get requests in each of the HTTP server instances.

Justification:

The number of get requests depend on the data being transferred and not on the server instance. Thus the number of requests remain the same.

c. Obtain the amount of time elapsed between the HTTP GET requests and their corresponding responses, while accessing each of these three HTTP server instances?

Solution:

File name	HTTP 1.0 (8100)	HTTP 1.1(Non Persistent) (8110)	HTTP 1.1(persistent) (8111)
Root	3	28	8
style.css	15	10	34
mobile.css	14	9	34

mobile.js	15	7	36
logo.png	7	17	7
satellite.png	108	131	251
project-image1.jpg	33	38	56
project-image2.jpg	28	31	92
project-image3.jpg	45	44	111
project-image4jpg	44	44	110
mars-rover.jpg	105	94	135
finding-planet.jpg	97	85	118
new-satellitedish.jpg	97	86	150
bg-home.jpg	262	321	393
bg-transparent1.png	116	20	71
icons.png	47	20	135
audiowide-regular-webfont.woff	74	96	68

d. What is the total page download time from each of these three HTTP server instances?

Solution:

HTTP 1.0 Total page download time: 673ms [8100]
HTTP 1.1 Non persistent Total page download time: 832ms [8110]
HTTP 1.1 persistent Total page download time: 810ms [8111]

Justification:

In general, the total page download time using HTTP 1.1 persistent connection should be the least, which was not observed above. This could be due to different loads in the network.

e. Check the user-agent field in the HTTP headers. What information regarding the OS and Browser can you infer from the user-agent field?

Solution:

User Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:57.0) Gecko/20100101 Firefox/57:.0

Justification:

This suggests that we were using Mozilla Firefox browser, version 5.0, Ubuntu, Linux having x86_64 architecture with Gecko as the browser driver.

PART II

Observe the packet traces by accessing the FTP server and answer the following:

a. What are the sequences of FTP messages exchanged between the server and the client for (i) active mode connection, (ii) passive mode connection? Note down the message type, FTP header fields, source IP, destination IP, source port and destination port corresponding to those messages.

Solution:

i) Active mode connection:

The list of FTP messages exchanged is as follows:
1.
Message Type: Response
Source IP: 10.5.20.222
Source port: 21
Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
Response code: Service ready for new user (220)
Response arg: ProFTPD 1.3.5a Server (Debian) [::ffff:10.5.20.222]

2.
Message Type: Request
Source IP: 10.145.238.91
Source port: 46732
Destination IP: 10.5.20.222
Destination port: 21

FTP Header Fields:
Request command:User
Response arg: anonymous

3.
Message Type: Response
Source IP: 10.5.20.222
Source port: 21
Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
Response code: User name okay, need password (331)
Response arg: Anonymous login ok, send your complete email address as your password

4.
Message Type: Request
Source IP: 10.145.238.91
Source port: 46732
Destination IP: 10.5.20.222
Destination port: 21
FTP Header Fields:
Request command: PASS

5.
Message Type: Response
Source IP: 10.5.20.222
Source port: 21
Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
Response code: User logged in, proceed (230)
Response arg: Welcome, archive user anonymous@10.145.238.91 !

6.
Message Type: Response
Source IP: 10.5.20.222
Source port: 21
Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
Response code: User logged in, proceed (230)

7.
Message Type: Request
Source IP: 10.145.238.91
Source port: 46732
Destination IP: 10.5.20.222
Destination port: 21
FTP Header Fields:
Request command: SYST

8.
Message Type: Response
Source IP: 10.5.20.222
Source port: 21
Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
Response code: NAME system type (215)
Response arg: UNIX Type: L8

After running a command,

1.
Source IP: 10.145.238.91
Source port: 46732
Destination IP: 10.5.20.222
Destination port: 21
FTP Header Fields:
PORT 10,145,238,91,225,39\r\n
Request command: PORT
Request arg: 10,145,238,91,225,39
Active IP address: 10.145.238.91
Active port: 57639

2.
Source IP: 10.5.20.222
Source port: 21
Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
200 PORT command successful\r\n
Response code: Command okay (200)
Response arg: PORT command successful

3.
Source IP: 10.145.238.91
Source port: 46732
Destination IP: 10.5.20.222
Destination port: 21
FTP Header Fields:
Request command: LIST

4.
Source IP: 10.5.20.222
Source port: 21

Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
150 Opening ASCII mode data connection for file list\r\n
Response code: File status okay; about to open data connection (150)
Response arg: Opening ASCII mode data connection for file list

5.
Source IP: 10.5.20.222
Source port: 21
Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
226 Transfer complete\r\n
Response code: Closing data connection (226)
Response arg: Transfer complete

ii) Passive mode:

After running a command,

1.
Source IP: 10.145.238.91
Source port: 46732
Destination IP: 10.5.20.222
Destination port: 21
FTP Header Fields:
Request command: PASV

2.
Source IP: 10.5.20.222
Source port: 21

Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
Response code: Entering Passive Mode (227)
Response arg: Entering Passive Mode (10,5,20,222,174,81).
Passive IP address: 10.5.20.222
Passive port: 44625

3.
Source IP: 10.145.238.91
Source port: 46732
Destination IP: 10.5.20.222
Destination port: 21
FTP Header Fields:
Request command: LIST

4.
Source IP: 10.5.20.222
Source port: 21
Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
Response code: File status okay; about to open data connection (150)
Response arg: Opening ASCII mode data connection for file list

5.
Source IP: 10.5.20.222
Source port: 21
Destination IP: 10.145.238.91
Destination port: 46732
FTP Header Fields:
Response code: Closing data connection (226)
Response arg: Transfer complete

b. Distinguish between the command channel and data channel of the communication for active and passive mode TCP. Who initiates the data channel connection for (i) active mode, (ii) passive mode of FTP?

Solution:

The **command channel** is used for sending **FTP requests** and **responses** to and from the server. The **data channel** is used for **transfer** of files/data only.

i. In **active mode**, the client establishes the command channel (from client port X to server port 21) but the server establishes the data channel (from server port 20 to client port Y, where Y has been supplied by the client).

ii. In **passive mode**, the client establishes both channels. In that case, the server tells the client which port should be used for the data channel after the client issues the PASV command.

c. What is the port used for data communication (for both the active mode and passive mode FTP connections)? What is the difference when the passive mode is enabled by the client

Solution:

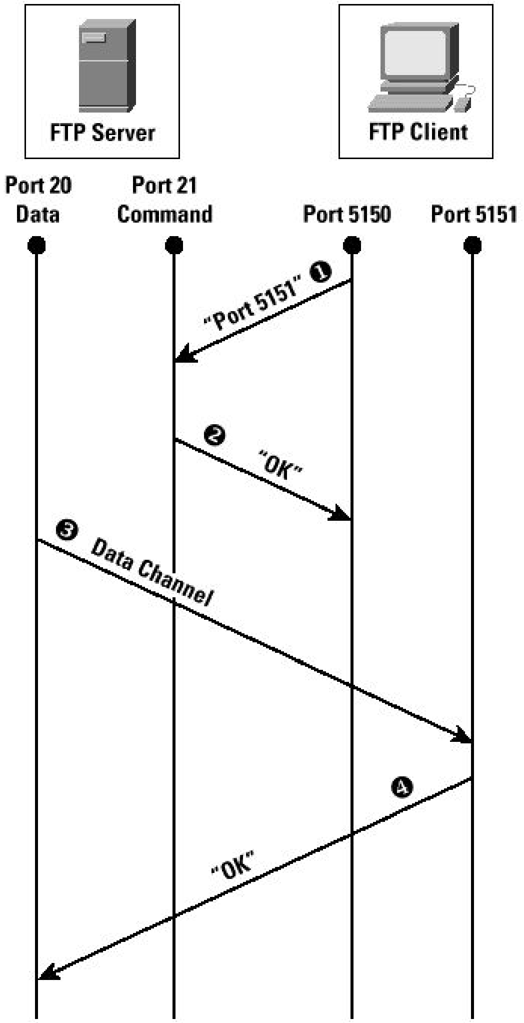
Data Port used for **Active Connection: 20**
Data Port used for **Passive Connection**: **44625**

In active mode, the client establishes the command channel (from client port X to server port 21) but the server establishes the data channel (from server port 20 to client port Y, where Y has been supplied by the client).

In passive mode, the client establishes both channels. In that case, the server tells the client which port should be used for the data channel after the client issues the PASV command.

Procedure applied for Active Mode :

- The client opens a control channel (port 21) to the server and tells the server the port number to respond on. This port number is a randomly determined port greater than 1023.
- The server receives this information and sends the client an acknowledgement "OK" (ack). The client and server exchange commands on this control connection.
- When the user requests a directory listing or initiates the sending or receiving of a file, the client software sends a "PORT" command that includes a port number > 1023 that the client wishes the server to use for the data connection.
- The server then opens a data connection from port 20 to the client's port number, as provided to it in the "PORT" command.
- The client acknowledges and data flows.



❶ FTP Client opens command channel to server; tells server second port number to use

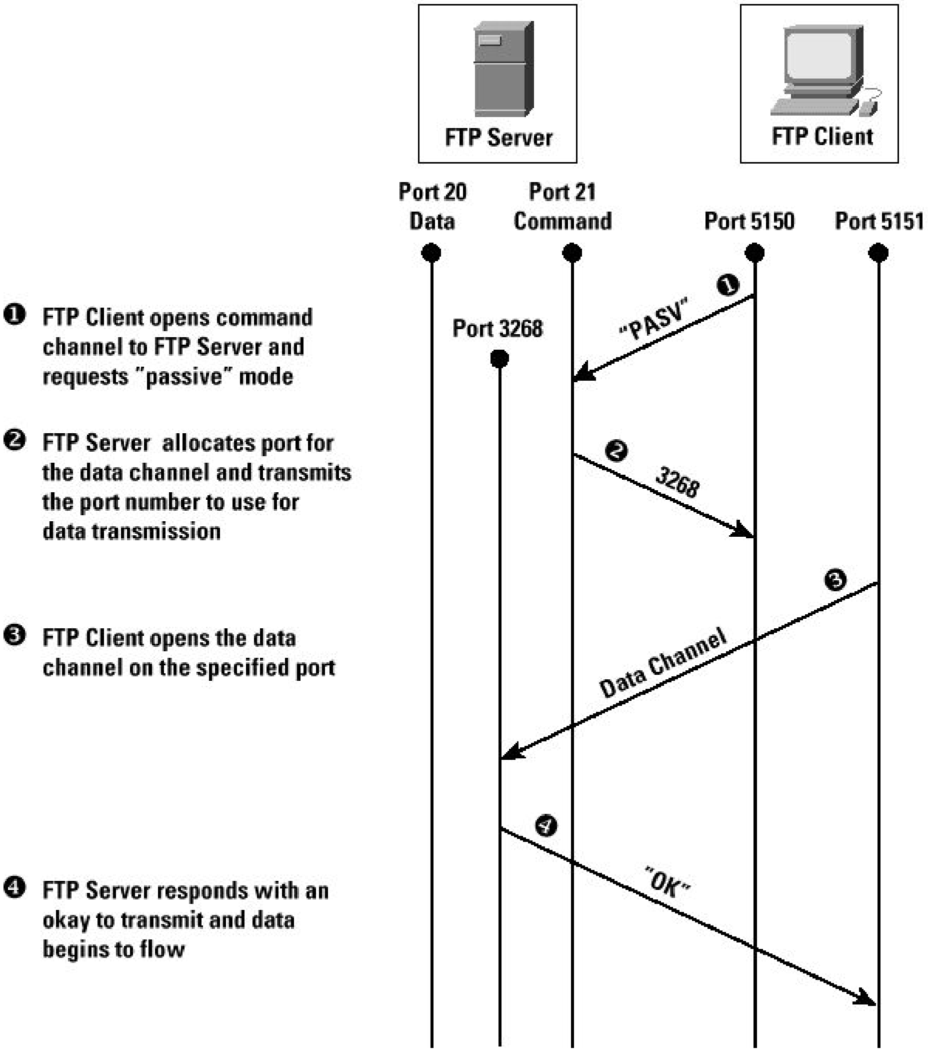
❷ FTP Server acknowledges

❸ FTP Server opens data channel to clients second port as instructed

❹ Client acknowledges and data flows

Procedure applied for Passive Mode :

- In passive FTP, the client opens a control connection on port 21 to the server, and then requests passive mode through the use of the "PASV" command.
- The server agrees to this mode, and then selects a random port number (>1023). It supplies this port number to the client for data transfer.
- The client receives this information and opens a data channel to the server assigned port.



❶ FTP Client opens command channel to FTP Server and requests "passive" mode

❷ FTP Server allocates port for the data channel and transmits the port number to use for data transmission

❸ FTP Client opens the data channel on the specified port

❹ FTP Server responds with an okay to transmit and data begins to flow