National University of Computer and Emerging Sciences



**Laboratory Manuals**

*for*

**Computer Networks**

(CL -307)

|  |  |
| --- | --- |
| Course Instructor |  |
| Lab Instructor(s) |  |
| Section | CS- |
| Semester | Spring 2023 |

Department of Computer Science

FAST-NU, Lahore, Pakistan

**Lab Manual 06**

# Objective:

* Analyzing the **FTP** packets using Wireshark
* TCP Socket Programming using Multithreaded Server to handle multiple clients at the same time

**Lab Statement 1: Capturing FTP packets using Wireshark (10)**

**Step 1**: **Start a Wireshark capture.**

**a.** Close all unnecessary network traffic, such as the web browser, to limit the amount traffic during the Wireshark capture.

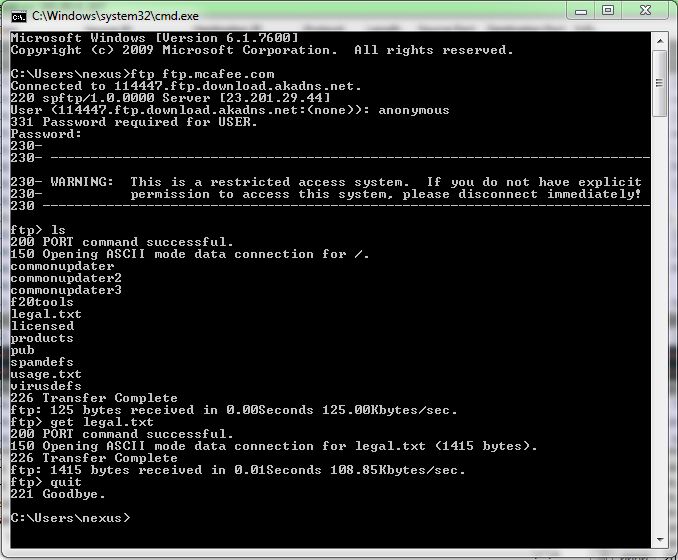
**b.** Start the Wireshark capture.

**Step 2: Download the .txt file.**

**a.** From the command prompt, enter ftp [ftp.mcafee.com](ftp://ftp.mcafee.com)

**b.** Log into the FTP site for mcafee.com with user **anonymous** and no password.

**c.** Locate and download any .txt file.



**Step 3: Stop the Wireshark capture.**

**Step 4: View the Wireshark Main Window**

Wireshark captured many packets during the FTP session to [ftp.mcafee.com](ftp://ftp.mcafee.com). To limit the amount of data for analysis, type **tcp and ip.addr == 195.89.6.167** in the Filter. The IP address, **195.89.6.167**, is the address for [ftp.mcafee.com](ftp://ftp.mcafee.com).

**Step 5: Analyze the packets**

Carefully analyze the packets in Wireshark windows and answer the following question:

**Use the FTP\_Session.pcapng (Wireshark Capture File) to answer the questions below**

1. FTP uses two port numbers: 20 and 21. Apply **tcp.port==20** and **tcp.port==21**. Analyze the result and write down the purposes of these two ports for FTP.

**Ans:**

**Port 20:**  It has been used for data transfer i.e. the original transfer of requested files.

**Port 21:** It has been used for control commands. For example for sending response that file transfer is complete.

1. Filter out each packet using either FTP or FTP-DATA Protocol (using **ftp || ftp-data** filter). Mention each packet number and its purpose with reference to request made and response received in the above mentioned FTP Session in command line to get file legal.txt (screenshot show above). Also look for **Response Code** and **Response Arg** in the FTP Header for each packet

**(**There are **19 such packets** and you have to write one/two lines explanation for each packet, what the packet is doing w.r.t FTP Session (Screenshot shown above) **e.g., Packet 104: Client asks server to send the data on IP:192.168.1.2 and Port:16341** [63(0x3F),213(0xD5) and **(0x3FD5=16341**)**] )**

**Ans:**

* **89**: Response by server which is success code. The sever has the service ready for new user.
* **94**: Request by client sending arguments for User .
* **96**: Response by server telling the client that user name is okay and asking client for password.
* **99**: Request by client sending password against the username
* **100**: Response by server telling client of successful login.
* **104**: Request by client to send data on IP:192.168.1.2 and Port 16341
* **105**: Response by server – a success message.
* **106**: Request by client to give list of files present on the IP address and Port no sent earlier.
* **107**: Server Responds by okay. The server is establishing connection to send the requested list of files.
* **125**: Requested data has been sent. Server is now closing the connection.
* **127**: Requested data(list of files) received in this packet.
* **151**: Client again requests for PORT asking the server to send data on IP: 192.168.1.2 and Port no 16342.
* **152**: Server Responses by success message.
* **153**: Client requests server for downloading a copy of the file ‘legal.txt’.
* **155**: Server responds by positive message and is opening data connection for transfer.
* **160**: Server has sent the file and this packet is sent to inform that it is closing connection now.
* **161**: The file “legal.txt” is received in this packet.
* **173**: Client wished to exit and informing the server by sending QUIT command.
* **175**: Server acknowledges the QUIT command by saying goodbye to client with this packet and closes the control connection.