

CS 39006: Networks Lab

Assignment 2: Understanding the Protocols of Application Layer

Date: 18th January, 2018

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.

Submission Instructions:

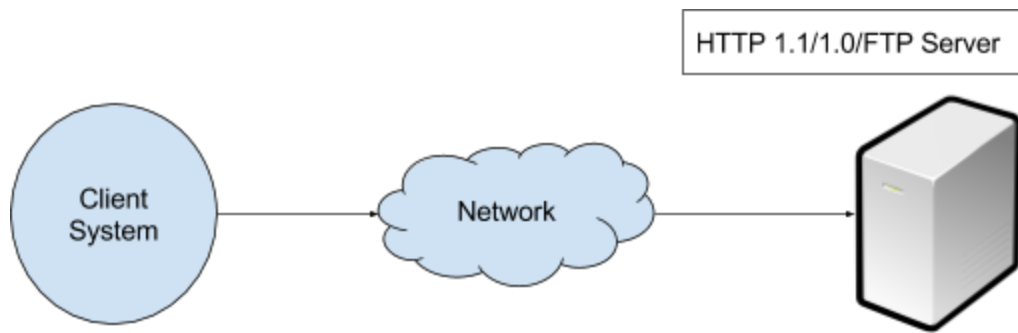
You need to prepare a report that will contain the followings.

1. **Steps** followed in executing the experiments.
2. **Observations** from the experiments.
3. Intuitive **justification** behind the observations

You need to submit the report in a single compressed (tar.gz) file. Rename the compressed file as **Assignment_1_Roll1_Roll2.tar.gz**, where Roll1 and Roll2 are the roll numbers of the two members in the group. Submit the compressed file through Moodle by the submission deadline. The submission deadline is: **January 25, 2018 02:00 PM**. Please note that this is a strict deadline and no extension will be granted.

Please note that your submission will be awarded zero marks without further consideration, if it is found to be copied. In such cases, all the submissions will be treated equally, without any discrimination to figure out who has copied from whom.

Assignment Statement:



The client system (representing your system) is connected through the network to an HTTP (1.1 and 1.0) and an FTP server running at **10.5.20.222**.

HTTP Server

The HTTP server used an **Apache 2.4.18 Web Server**. There are three instances of this same server running on this host system.

1. At port **8111**
2. At port **8110**
3. At port **8100**

The three instances are corresponding to (not in this order) - (a) HTTP 1.0 server, (b) HTTP 1.1 server with persistent connections (keep-alive is on), (c) HTTP 1.1 server with non-persistent connections (keep-alive is off). However, your task would be to find out which server corresponds to which version of HTTP.

Note : The default port 80 for HTTP has been blocked and you can access the web server only using the ports mentioned above.

To access the server open a browser and enter the following url (uniform resource locator):
http://10.5.20.222:8111 (or 8110 or 8100)
and then observe the packet traces using Wireshark.

Note :

- You have to bypass the proxy to access the above mentioned url. To bypass use the address **10.0.0.0/8** in the proxy settings of your browser.
- You need to “Disable Cache” before accessing the web page. To do that go to the network panel of the developer options of the browser and check disable cache (Open Menu -> Web Developer -> Network or Ctrl+Shift+E for Firefox).

FTP Server

The FTP server for this system **ProFTPD 1.3.5a**. The server can be connected to via its default port 21. As you know, the FTP server can work either in active mode (the server initiates the data channel socket towards the client) or in passive mode (the client initiates the data channel socket towards the server). The objective of this assignment would be to

explore the active mode and passive mode operations of FTP. The FTP server can be accessed using the following commands:

`ftp -d -A` (This command starts the FTP server **under active mode** with debug functionalities enabled)

`open 10.5.20.222` (**Username:** anonymous. **Password:** Blank, just hit enter)

To access the FTP in passive mode, use the following command:

`passive`

To see the list of other commands available, use the following command:

`help`

For this assignment, you don't need to transfer any file to the FTP server. You can check the data model operations of the FTP via simple FTP commands like `ls`.

Note : You might not be authorised to perform all the available operations over the FTP server.

Tips : To check your IP use the command `ifconfig` from the terminal. You may use the open source utility `gnuplot` (<http://www.gnuplot.info/>) to plot the graph.



Deeper inspection with Wireshark

1. Start Wireshark
2. In the menu bar, go to Capture -> Options
3. In the Input tab, select the interface `em1`
4. Enter the following **capture filter**
 - a. **host 10.5.20.222 and host <your IP>**
 - b. This will force wireshark to capture only the packets between the hosts
5. Enter the ftp commands and watch the packet trace
6. After the capture completes, right click on any packet and click Follow -> TCP stream
 - a. You should see the data that was sent in the current TCP stream
7. In the capture filter you should see something like **tcp.stream eq 1** which indicates stream number 1
 - a. By changing the stream number, we can see the various data that was sent in each stream

Assignments

Answer the following questions by observing the packet traces in Wireshark and the network panel of the web developer of the browser.

1. 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.

-  b. How many GET requests were issued to access each of the three HTTP server instances?
 -  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?
 - d. What is the total page download time from each of these three HTTP server instances? (total page download time = time of last response message received - time of first GET request message sent)
 - 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?
2. 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.
 - 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?
 - 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?