**National University of Computer and Emerging Sciences**



**Laboratory Exercise**

**Computer Networks**

*Instructor: Sumaira Mustafa*

Student: Muhammad Abdullah 19F-0916

**FAST School of Computer Science**

## Question#1: The Basic HTTP GET/response interaction

Let’s begin our exploration of HTTP by downloading a very simple HTML file - one that is very short and contains no embedded objects. Do the following:

1. Start up your web browser.
2. Start up the Wireshark packet sniffer, as described in the Introductory lab (but don’t yet begin packet capture). Enter “http” (just the letters, not the quotation marks) in the display-filterspecification window, so that only captured HTTP messages will be displayed later in the packetlisting window. (We’re only interested in the HTTP protocol here, and don’t want to see the clutter of all captured packets).
3. Wait a bit more than one minute (we’ll see why shortly), and then begin Wireshark packet capture.
4. Enter the following to your browser [http://gaia.cs.umass.edu/wireshark-labs/HTTP-wiresharkfile1.html](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html) Your browser should display the very simple, one-line HTML file.
5. Stop Wireshark packet capture.

Answer following questions:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

ANSWER: My Browser is Running HTTP 1.1 Version

Graphical user interface, application

Description automatically generated

1. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?

ANSWER: Language Supported by Browser is:



Other Information is:

Graphical user interface, application, Word

Description automatically generated

1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

ANSWER: IP address of the computer is:

Text

Description automatically generated



1. What is the status code returned from the server to your browser?

ANSWER: Returned Status Code is:



1. When was the HTML file that you are retrieving last modified at the server?

ANSWER: Last HTML file was modified at:



1. How many bytes of content are being returned to your browser?

ANSWER: Number of bytes returned are:

A picture containing text, orange, close

Description automatically generated 

Question#2:

Do the following steps:

1. Start up the Wireshark program (select an interface and press start to capture packets).
2. Start up your favorite browser.
3. In your browser, go to Wayne State homepage by typing www.wayne.edu.
4. After your browser has displayed the http://www.wayne.edu page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture.

Answer these questions:

1. Mention the coloring scheme followed for which type of traffic (protocol).

ANSWER: Following are the Colors:



Black Shows TCP



Light Blue Shows UDP



Green Shows HTTP



Grey Shows Tcp



Red Shows TCP RST

1. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! However, as you will notice the HTTP messages are not clearly shown because there are many other packets included in the packet capture. Even though the only action you took was to open your browser, there are many other programs in your computer that communicate via the network in the background. To filter the connections to the ones we want to focus on, we must use the filtering functionality of Wireshark. **show all the packets that are using HTTP protocol from the captured packet. Attach the snapshot of your filtered packets**.

ANSWER:

Table

Description automatically generated

1. To further filter packets in Wireshark, you need to use a more precise filter. Show all the packet where the HTTP host is: [www.wayne.edu.](http://www.wayne.edu/) Or <http://flexstudents.nu.edu.pk>

ANSWER:

Graphical user interface, text, application

Description automatically generated

1. Show all the packets using sent on 53 port number.

ANSWER: No Data Found on 53 But 80 Shows Following

Text

Description automatically generated

1. Show all the packets that are using TCP protocol.

ANSWER: Following are the TCP protocol:

Table

Description automatically generated with medium confidence

1. Let’s try now to find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button and show the follow stream of the question:5 protocol.

Graphical user interface, text, application

Description automatically generated

1. If a packet is highlighted by black, what does it mean for the packet?

ANSWER: Check Following:

Text

Description automatically generated

1. What is the filter command for listing all outgoing http traffic?

ANSWER: tcp.port==80 || ip.addr== 192.168.1.1 (Here ip.addr can be changed accordingly)

## Question#3: Using Wireshark to capture the FTP password

Do the following steps:

1. Start up the Wireshark program (select an interface and press start to capture packets).
2. Start up your favorite browser.
3. In your browser, go to slate home page by typing <http://slate.nu.edu.pk/>.
4. Login slate with your own roll number. After your browser has displayed the <http://slate.nu.edu.pk/login/>page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture.

Answer these questions:

1. Show all the http packets captured so far.

ANSWER: Following are the Packets

Table

Description automatically generated with low confidence

1. Show the request packets of  [http://slate.nu.edu.pk/.](http://slate.nu.edu.pk/)

Text

Description automatically generated

1. Show all the response packets of [http://slate.nu.edu.pk/.](http://slate.nu.edu.pk/)

Graphical user interface, table

Description automatically generated

1. Explore the response message and find out the password and username. Take screen shot of this and attach.

Graphical user interface, application

Description automatically generated