COMPUTER NETWORK (CS F303)
Second Semester 2018-2019
LAB-SHEET – 1

Objectives:

- **To learn packet sniffing using Wireshark.**
- **To understand HTTP protocol and its working.**
- **To understand DNS protocol and its working**

(References: Wikipedia, Computer Networking: A Top Down Approach by Kurose and Ross)

One's understanding of network protocols can often be greatly deepened by "seeing protocols in action" and by "playing around with protocols" – observing the sequence of messages exchanged between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences. In the Wireshark labs you'll be doing in this course, you'll be running various network applications in different scenarios using your own computer. You'll observe the network protocols in your computer "in action," interacting and exchanging messages with protocol entities executing elsewhere in the Internet. Thus, you and your computer will be an integral part of these "live" labs. You'll observe, and you'll learn, by doing.

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a *copy* of packets that are sent/received from/by application and protocols executing on your machine.

Figure 1 shows the structure of a packet sniffer. At the right of Figure 1 are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Figure 1 is an addition to the usual software in your computer, and consists of two parts. The **packet capture library** receives a copy of every link-layer frame that is sent from or received by your computer. You know that that messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In Figure 1, the assumed physical media is an Ethernet, and so all upper-layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.

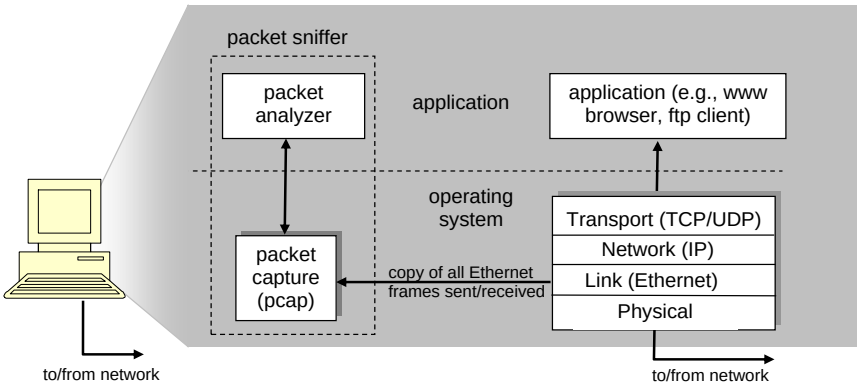

Figure 1: Packet sniffer structure

The second component of a packet sniffer is the **packet analyzer**, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol in Figure 1. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment (as HTTP uses TCP as underlying transport layer protocol) within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol.

There are many packet sniffers available, for example Wireshark packet sniffer, Ethereal Network Analyzer, Snoop Analyzer Standard, Network Probe, etc. We will be using the Wireshark packet sniffer [http://www.wireshark.org/].

Running Wireshark

When you run the Wireshark program, you'll get a startup screen, as shown in Figure-2:

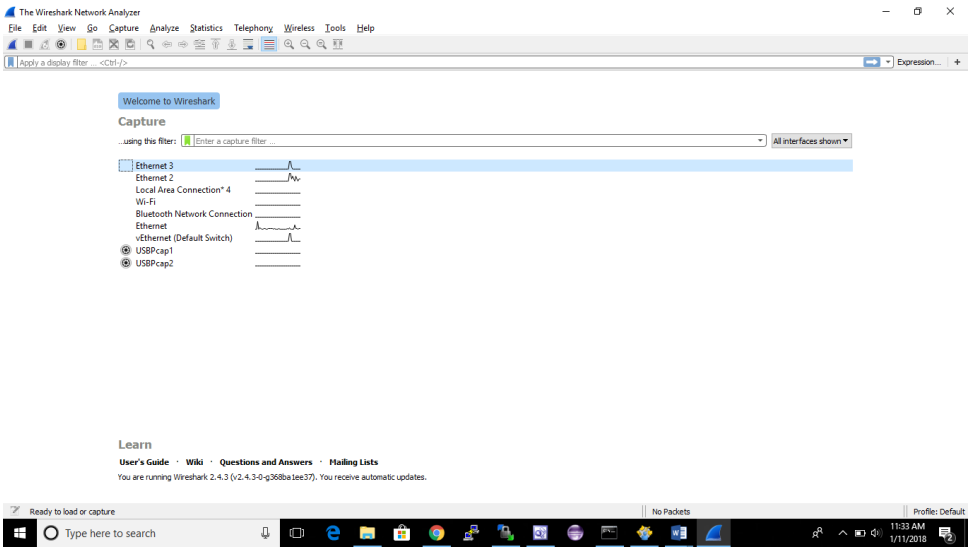

Figure-2: Start up screen of Wireshark.

Take a look at the screen – you'll see an "Interface list". This is the list of network interfaces on your computer. Once you choose an interface, Wireshark will capture all packets on that interface. In the example above, there is an Ethernet interface (Gigabit network Connection) along with some other. Click on "Ethernet" interface to start packet capture (i.e., for Wireshark to begin capturing all packets being sent to/from that interface), a screen like the one shown in Figure-3 will be displayed, showing information about the packets being captured. Once you start packet capture, you can stop it by using the Capture pull down menu and selecting Stop.

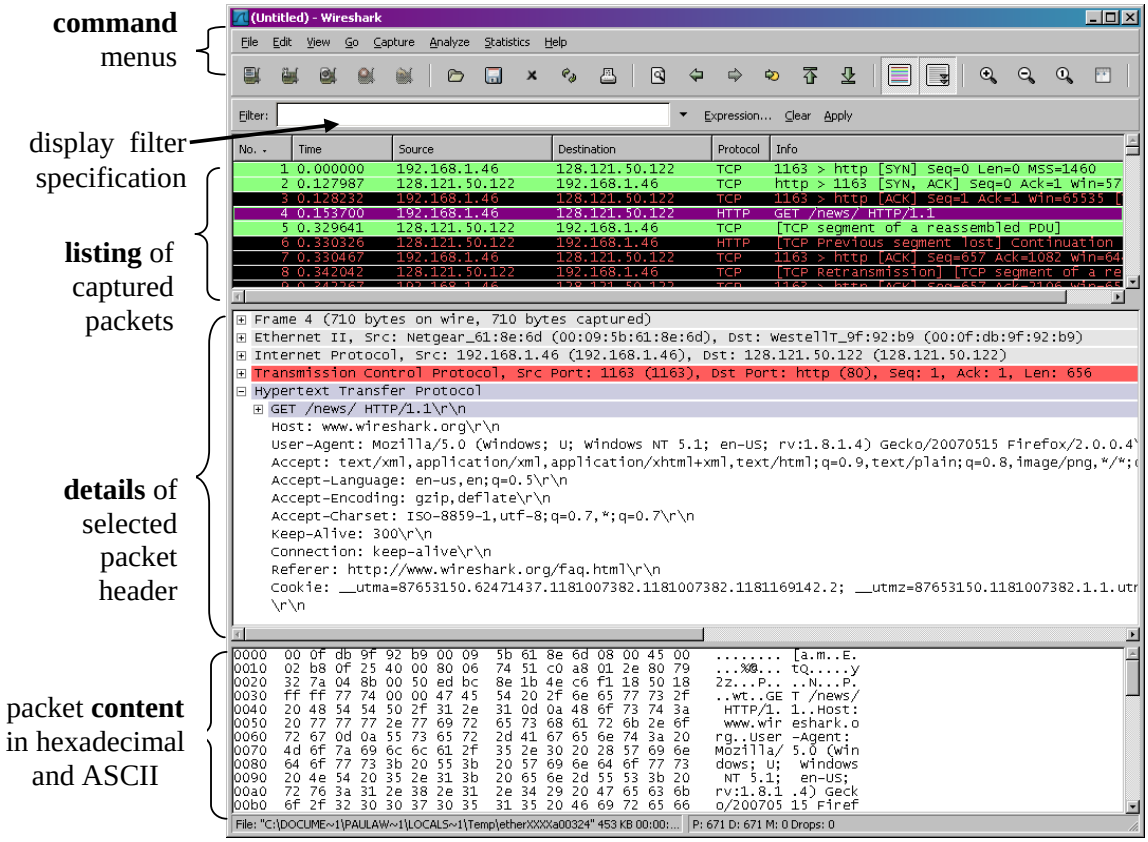

Figure 3: Wireshark Graphical User Interface, during packet capture and analysis

The Wireshark interface has five major components:

- The **command menus** are standard pulldown menus located at the top of the window. Of interest to us now are the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Wireshark application. The Capture menu allows you to begin packet capture.
- The **packet-listing window** displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is *not* a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type

field lists the highest-level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.

- The **packet-header details window** provides details about the packet selected (highlighted) in the packet-listing window. (To select a packet in the packet-listing window, place the cursor over the packet's one-line summary in the packet-listing window and click with the left mouse button.). These details include information about the Ethernet frame (assuming the packet was sent/received over an Ethernet interface) and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the plus minus boxes to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest-level protocol that sent or received this packet are also provided.
- The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

Towards the top of the Wireshark graphical user interface, is the **packet display filter field,** into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark hide (not display) packets except those that correspond to HTTP messages.

Taking Wireshark for a Test Run

Experiment-1

The best way to learn about any new piece of software is to try it out! Do the following

1. Start up your favorite web browser.

2. Start up the Wireshark software. You will initially see a window similar to that shown in Figure 2. Wireshark has not yet begun capturing packets. Select the desired network interface. Packet capture will now begin - Wireshark is now capturing all packets being sent/received from/by your computer!

3. Once you begin packet capture, a window similar to that shown in Figure 3 will appear. This window shows the packets being captured. By selecting *Capture* pulldown menu and selecting *Stop*, you can stop packet capture. But don't stop packet capture yet. Let's capture some interesting packets first. To do so, we'll need to generate some network traffic. Let's do so using a web browser, which will use the HTTP protocol.

4. While Wireshark is running, enter the URL:
   http://ipclabbooking/CSF303/lab1_first_page.htm
   and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at host ***ipclabbooking*** and exchange HTTP messages with the server in order to download this page. The Ethernet frames containing these HTTP messages (as well as all other frames passing through your Ethernet adapter) will be captured by Wireshark.

5. After your browser has displayed the lab1_first_page.htm, stop Wireshark packet capture by selecting stop in the Wireshark capture window. The main Wireshark window should now look similar to Figure 3. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the ***ipclabbooking*** web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well (see, e.g., the many different protocol types shown in the *Protocol* column in Figure 3). Even though the only action you took was to download a web page, there were evidently many other protocols running on your computer that are unseen by the user. We'll learn much more about these protocols as we progress through the text!

6. Type in "http" (without the quotes, and in lower case – all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select *Apply* (to the right of where you entered "http"). This will cause only HTTP message to be displayed in the packet-listing window.

7. Find the HTTP GET message that was sent from your computer to the webserver. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window. Recall that the HTTP GET message that is sent to the http://ipclabbooking/CSF303/lab1_first_page.htm web server is contained within a TCP segment, which is contained (encapsulated) in an IP datagram, which is encapsulated in an Ethernet frame. By clicking on '+' and '-' right-pointing and down-pointing arrowheads to the left side of the packet details window, *minimize* the amount of Frame, Ethernet, Internet Protocol, and Transmission Control Protocol information displayed. *Maximize* the amount information displayed about the HTTP protocol. Your Wireshark display should now look roughly as shown in Figure 4. (Note, in particular, the minimized amount of protocol information for all protocols except HTTP, and the maximized amount of protocol information for HTTP in the packet-header window).

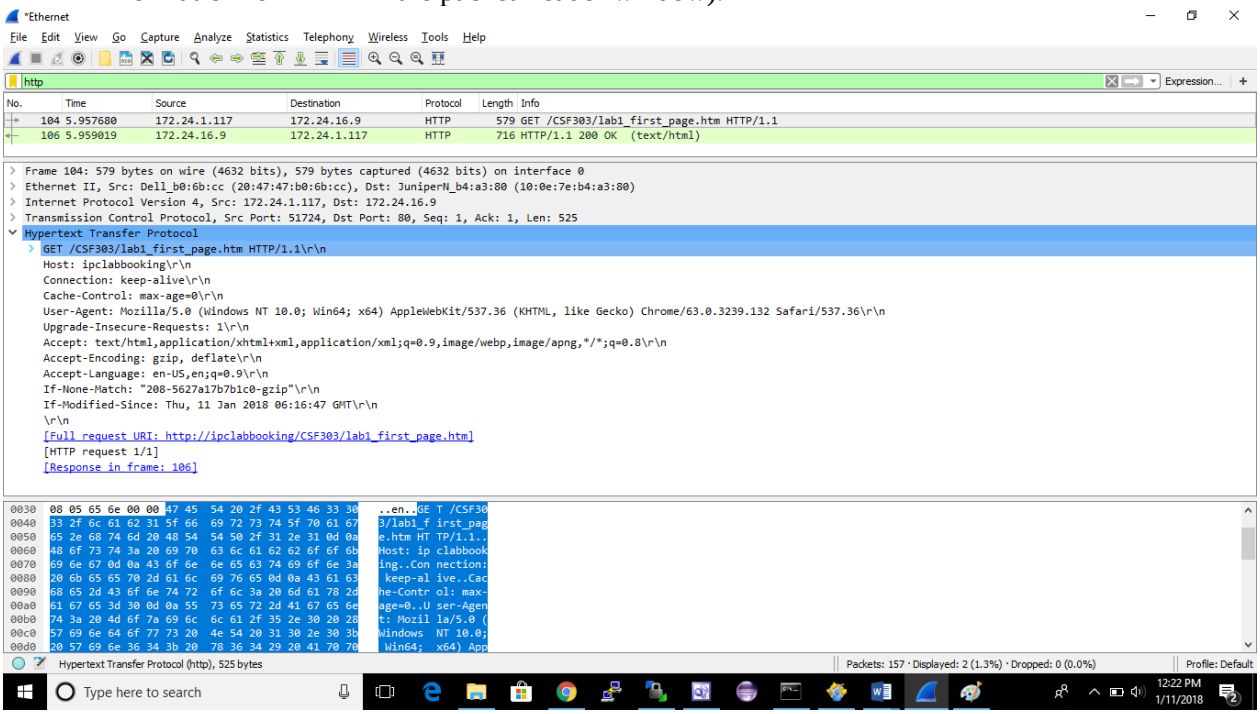

Figure-4: GET message details

8. Save the packet capture and Exit Wireshark

Now try to answer following questions:

1. What does \r\n mean after each line?
2. What indicates the end of HTTP message?
3. What is the version of HTTP used? Is it necessary to pass it in message? Why?
4. What type of connection it is: persistent or non-persistent?
5. What is the source IP address and destination IP address?
6. Which transport layer protocol does HTTP use?
7. What is the source and destination port number?
8. How long did it take from when the HTTP GETT message was sent until HTTP OK reply was received?
9. What is the difference between date header and Last-modified header in HTTP OK reply.?
10. Although URL specifies the host (i.e. "***ipclabbooking***"), why do you think that it is again the part of HTTP GET message?
11. Does HTTP work on specific port? How can it be verified from GET and OK messages?
12. You can see a line "Response in Frame: *some_number*". What does it mean? Verify your answer.

Experiment-2

1. Clear browsing history. You can do it using tools menu of your Brower.
2. Start Wireshark and apply filter "http" (without quotes) as we are interested in http packets.
3. Type the following URL in your web browser and press enter: http://ipclabbooking/CSF303/lab1_second_page.htm
4. Stop capturing packets and observe different HTTP packets. Observe that there are two embedded images in the web page.
   Q1. How many HTTP GET requests are generated?
   Q2. What can be concluded from your answer of Q1 above?
   Q3. What is the status code returned in all HTTP response packets?
   Q4. When were the objects embedded in web page last modified at the server?
   Q5. How many bytes of content are being returned to your browser in each HTTP response packet?
5. Now, start Wireshark packet capture again and refresh the webpage, i.e. enter URL: http://ipclabbooking/CSF303/lab1_second_page.htm
6. Stop capturing packets and observe different HTTP packets again.
   Q1. What is the date header value and Last Modified value in HTTP response packets?
   Q2. Are two embedded images fetched from the server or were locally cached? How to verify it?
7. Now, start Wireshark packet capture again and enter the following URL: http://ipclabbooking/CSF303/lab1_third_page.htm
   Stop capturing packets and observe different HTTP packets again.
   Q1. You will observe that one image is not displayed. Why so?

Q2. Does path of first image (corresponding to "sixth edition") is same as that mentioned in step-7?

Experiment 3

1. Clear browsing history.
2. Start Wireshark and apply filter "http" (without quotes) as we are interested in http packets.
3. Type the following two URL's in your web browser and press enter:
   http://ipclabbooking/CSF303/lab1_forth_page.htm
   http://ipclabbooking/CSF303/lab1_fifth_page.htm
4. Again observe the http packets exchanged in above two cases.
   Q1. You must have observed that in "fifth_page" the size of two images is more than that with respect to "fourth_page". In "fifth_page" the images are the one which is cached or the one which are brought from the server? What can be concluded from your observation?

In all the above experiments see whether response from the server was in one single packet or multiple packets. You will have to observe TCP packets for it in each case.

DOMAIN NAME SERVICE (DNS)

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet, that has been in use since 1985.

The Domain Name System also specifies the technical functionality of the database service that is at its core. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in the DNS, as part of the Internet Protocol Suite. Historically, other directory services preceding DNS were not scalable to large or global directories as they were originally based on text files, prominently the hosts file. A DNS name server is a server that stores the DNS records for a domain; a DNS name server responds with answers to queries against its database.

The most common types of records stored in the DNS database are for Start of Authority (SOA), IP addresses (A and AAAA), SMTP mail exchangers (MX), name servers (NS), pointers for reverse DNS lookups (PTR), and domain name aliases (CNAME).

In this experiment you will sniff DNS packets.

Experiment 4

1. Clear Browsing history.
2. Start Wireshark and type filter name "dns" to see DNS packets.
3. Start browser and type URL: http://ipclabbooking/CSF303/lab1_second_page.htm
4. Understand that the first task to be done by your system is to get IP address corresponding to host name ipclabbooking. See if there is any DNS packet shown in Wireshark to resolve hostname ipclabbooking. Chances are that no DNS packet is shown in Wirehasrk. WHY ?? *Think before reading ahead.*
5. Probably you must have thought that DNS resource records are cached locally and clearing browsing history does not clear DNS records. *You were right!* So, now follow the following steps.
6. Open command prompt (or terminal) and type

   C:\ ipconfig/displaydns

   You will see all the cached DNS resource records. Now you need to clear all this. So type

   C:\ ipconfig/flushdns
7. Now, repeat steps 2 to 4 above and observe DNS packets exchanged. Answer the following questions with respect to DNS query message:

   Q1. Which transport layer protocol is used?

   Q2. What is the transaction ID of the message?

   Q3. What is the query section? What is the type of query and what does it signify about the type of query? Is there any other type of query you can recall?

   Q4. What is the IP address of DNS server?

   Q5. What is the destination port number? Remember that it is fixed for all DNS messages.

8. See the DNS response message and answer the following:

   Q1. What is the transport layer protocol?

   Q2. What is the transaction ID of this message? Is it same as that of corresponding DNS query message?

   Q3. Along with the answer, is there any authoritative name server also. What is its type and what does it signifies?

   Q4. Is there any other field (for example additional records, etc.)? What it signifies?
9. Verify that when the webpage in step 3 above was fetched, DNS query and response was generated first then HTTP query and response.

******