CS301: Computer Networks
Assignment 02: Application Layer Protocols (HTTP & DNS)

Goal:

1. Study and understand application layer protocols (HTTP, DNS) using packet analyzer and other tools.

Instructions:

1. **Deadline: August 31, 2024 11:59 PM.**
2. Any **plagiarism** case will be considered unethical practice, and appropriate action will be taken against them.

Install Wireshark

For installing Wireshark in Ubuntu type the following command in the terminal

```
sudo apt-get install wireshark
```

For further details you can use
(https://www.wireshark.org/download.html)

Wireshark Basics

Here are some basics on how to get started with Wireshark

(https://www.wireshark.org/docs/wsug_html_chunked/)
(http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/)

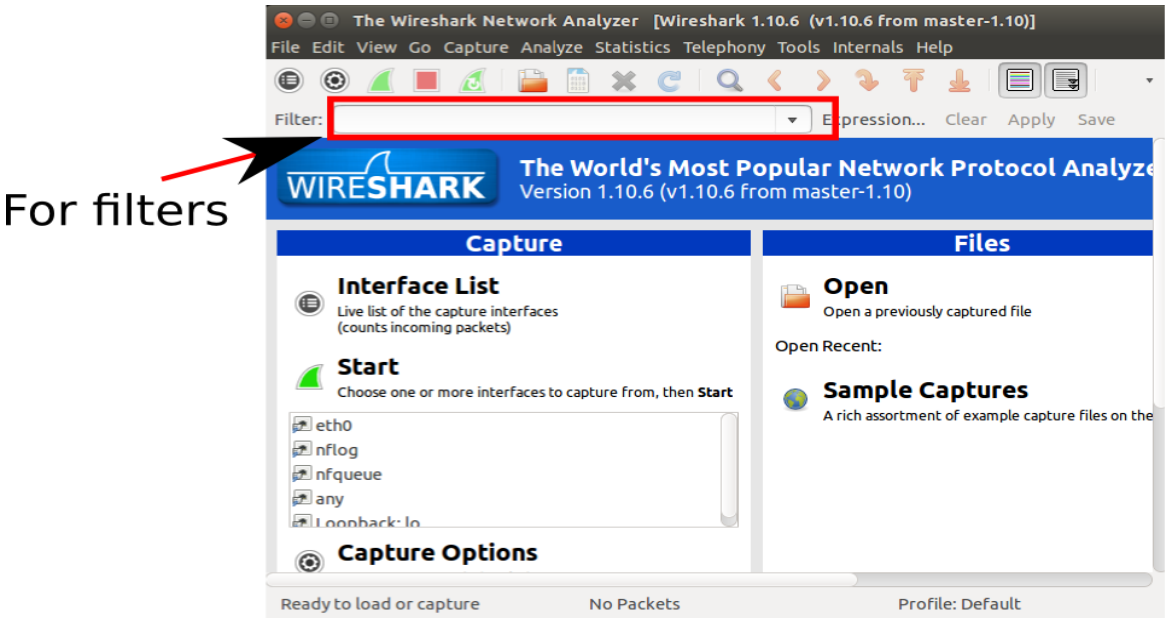
Hands-on Tutorial

1. How to start capture

Run Wireshark with sudo privilege; choose the interface to capture (wlan0 or eth0) from the interface bar

2. How to use filters

Filters are placed at the top of Wireshark tool, Check the below figure. Check some common command (for eg., http)



3. How to obtain the stats in wireshark

After applying filters, statistics (tab) → summary.

4. How to plot the IO graphs based on filters

Find Statistics → IO graph, apply filter in each of the filter column (for eg., ip.addr = = 192.168.0.82)

5. Reconstruct an image from the captured data

For an http GET request you may get a response. Check the response inside which you can find the application layer content. Choose the byte stream which actually contains data for that file. If the image is not shared across multiple chunks then simply export using wireshark (file → export selected bytes). Else copy the image file across multiple files into an hex editor to get back the original image.

Part 1: HTTP

Instruction: Start packet capture just before opening the https://www.iitbhilai.ac.in website and stop the packet capture once the complete page is loaded (or you can wait for 2 minutes and then stop the packet capture). Save the pcap file and answer the following questions by analyzing the packet traces.

1. When you browse IIT Bhilai main page (https://www.iitbhilai.ac.in) how many get request is sent (how many of the GET request are for embedded content and how many get request for the text)? Plot the IO graph for packets sent to iitbhilai.ac.in and packets received from iitbhilai.ac.in **[3]**
2. For each HTTP GET request as you see above, find out (i) the total amount of data being received in the corresponding HTTP response message. **[2]**
3. For the response to your HTTP GET request, get the image reconstructed by hex editor. **[2]**
4. **HTTP Conditional GET:** Answer the following questions. **[4]**
    a. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
    b. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
    c. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?
    d. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
5. Surf a website (other than google.com) of your choice and discuss the end-to-end process of web page loading using Wireshark. How much time did it take to load the page? Find out how many connections are used to download this page. Are these connections persistent or non-persistent? How many objects have been transferred on these connections? Which object took the longest time to download? **[5]**
6. List all the header fields present in HTTP GET request/response header with their usage/purpose for **iitbhilai.ac.in** and for the website used in problem 5. (You can use **Burp Suite** [Installation Guideline)] for this) **[2]**

Part 2: DNS

1. Along with IIT Bhilai website, access one more website of your choice and answer the following questions. How many DNS packets have you observed in total? **[4]**
    a. Create a <Domain Name, IP> table by exploring the queries and the answers in those DNS packets. The Domain Name will be the domain for which you see a query, and the IP address will be the address that is being returned against the corresponding query.
    b. Can you find out the IP of the DNS servers by exploring the DNS packets?

2. The root servers on the Internet are in the domain root-servers.net. You can see the list of all root servers using dig [DNS lookup utility] or any tool/command. **[6]**

    Use dig to ask the root server for the address of www.iitbhilai.ac.in, without recursion. Go through the hierarchy from the root without recursion, following the referrals manually until you have found the address of www.iitbhilai.ac.in

    List all the name servers involved to find out the IP address of the www.iitbhilai.ac.in.

    Do the same exercise for 2 more websites with different top-level domains (.com, .edu, .org, etc.)

Deliverables in a tar ball on GC:

- Submission Guidelines: Upload the Assignment Report, pcap in GC as a tar ball with file name as <your roll no>_<your name>.tar
- Readable Report **[2 Points for report quality]** enumerating steps followed with screenshots for each of the important steps.
    - Pcap trace collected and mention the command/tool used.
    - Put the screenshots (**mandatory**) to validate your answers in the report.
    - Clear and concise writing.

Check Web sources for more information.