CS301: Computer Networks

Assignment 1: Application Layer Protocols (HTTP & DNS)

Deadline: 31st August 2022, 11:59PM

Goal of the Assignment: Study and understand application layer protocols (HTTP, DNS) using packer analyzer and other tools.

Part 1

Instruction: Start packet capture just before opening 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 Points]

2. For each HTTP GET requests as you see above, find out (i) the total amount of data being received in the corresponding HTTP response message. [2 Points]

3. For the response to your HTTP GET request, get the image reconstructed by hex editor. [2 Points]

4. Find the total amount of data being received when you access https://www.iitbhilai.ac.in [2 Points]

5. **HTTP Conditional GET:** Answer the following questions. [4 Points]

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.

6. Find the throughput observed while browsing IIT Bhilai site under two cases [3 Points]

   a. When no other traffic in the background

   b. When a large file download is going.

the throughput calculation needs filtering only IIT Bhilai pages (from the get request originated from your browser till the last response has arrived at end of the web page).

7. 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 Points]

   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?

Part 2

1. 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 it took 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? [8 Points]

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

   Use dig to ask the root server 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.)

3. Find all the active TCP port on your system. Identify the ports and PIDs of your web browser. Can you identify the port number and PID of specific TAB in your browser? Find out if any of the services running in your system uses the standard ports of HTTP, DHCP, DNS, SMTP, and FTP. [4 Points]

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 Marks 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.

Check Web sources for more information