Wireshark to investigate application protocols in operation

Analyze the packet captured using the Wireshark to answer all the questions. Browse **http://goidirectory.nic.in/** as the website for **Task1** and **Task2.** Use appropriate filters, helper windows, properties in Wireshark. Place the screenshots of wireshark and browser where appropriate inline to answers, as a proof of analysis in answering the question.

Task1

Start the Wireshark packet sniffer and start capturing.
Enter the following URL into your browser http://goidirectory.nic.in/.
Stop the packet capture when you have all the information captured, which is required to answer all the questions below.

1. How many DNS queries are sent from your browser (host machine) to DNS Server(s) ? How many DNS servers are involved ? Which DNS Server replies with actual IP Address(es). Do all DNS servers respond ? Clearly list the resource records involved in resolving the IP address of the site, mentioning, Name, value, type, TTL appropriately in the complete resolving process of this DNS conversation including query/queries and response/answer(s).
2. How many HTTP requests (Type and respective count of requests), responses (status code and phrase of each of the responses) did the browser send and receive ?
3. How many TCP Connections has the browser established overall ?
4. What is the time taken to establish TCP connection(s) ?. List this time taken value for each of the TCP connection(s).
5. Browse the website by moving to various sub links, embedded objects listed in the site.
6. How many objects/files are downloaded?
7. Make a detailed list including for each object/file downloaded what is the time taken for downloading the objects, the size of the object downloaded, object name, last modified time at the server.
8. How many other websites are visited from this site, by clicking on to various possible links which take you to the other sites (other than http://goidirectory.nic.in/)
9. When http://goidirectory.nic.in/ is entered, is there any embedded object shown/downloaded from different site(s) (other than http://goidirectory.nic.in/) ?
10. How many times does the browser ask the site to keep the connection alive ?
11. Which version of the HTTP is your browser running ?

Task2

Before starting the steps below, make sure your browser's cache is empty.

Steps
Start the Wireshark packet sniffer and start capturing..
Enter the following URL into your browser http://goidirectory.nic.in/.
Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)
Stop Wireshark packet capture.

1. How many conditional GETs are sent by browser to the server ?
2. Make a list for each of the file/object downloaded, how many times the server sends the full contents of the respective file/object ?
3. Explain in detail what is the difference in server's behaviour between first and second request/browsing ?
4. List the headers of HTTP which influence this functionality.

Task3

Analyse the attached HTTP/2 packet (**http2-h2c.pcap**: Included in zip file) capture using Wireshark to answer the following (Hint : Use Statistics->HTTP, HTTP2 windows).

1. How many HTTP/2 and HTTP/1.1 packets are present?
2. How many HTTP/2 packets are exchanged between client and server here before the first object is fetched ?
3. What main difference do you observe in headers of HTTP/2 packets displayed here, compared to the headers of HTTP/1.1 packets ?

Submission

Prepare a detailed observation and analysis report including Task1, Task2 and Task3 with specific details asked in individual tasks. Submit it to google classroom in the posted assignment section.

PLAGIARISM STATEMENT <Include it in your report>

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or

personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.

Name of the student
Roll No