# GHARDA FOUNDATION

**GHARDA INSTITUTE OF TECHNOLOGY, LAVEL**

#### Department of Computer Engineering

**Evaluation Sheet**

Class: TE-Computer Engineering Sem: V Subject: **Computer Networks**

#### Experiment No: 7

#### Title of Experiment: [Study](https://drive.google.com/file/d/1uQMn8WeCWn0VEWeEtmYb4FUtzgDM8wVN/view?usp=sharing) of [Packets Capturing using Wireshark](https://drive.google.com/file/d/1vBGNh8WhvANugl53VRIoCSY8FaKCPdn4/view?usp=sharing)

#### Name of Student: Harvande Sanket Chandrashekhar Roll No: 19

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No. | Evaluation Criteria | Max Marks | Marks Obtained |
| 1 | Practical Performance | 8 |  |
| 2 | Oral | 5 |  |
| 3 | Timely Submission | 2 |  |
|  | Total | 15 |  |

Signature of Subject Teacher (Mr. S. S. Tathare)

#### **Aim**: To study [the](https://drive.google.com/file/d/1uQMn8WeCWn0VEWeEtmYb4FUtzgDM8wVN/view?usp=sharing) [packets capturing using Wireshark](https://drive.google.com/file/d/1vBGNh8WhvANugl53VRIoCSY8FaKCPdn4/view?usp=sharing).

**Apparatus**: Wireshark software

**Procedure**:

Step1: Install Wireshark & Select the interface on which packets will be captured

Step2: Start capturing and check for the fields viewed: Time(packet was received/sent;view-time display format), Source Ip, Destination IP, Protocol, Length, Information

Step3: Click on any TCP packet from your IP to other and check the frame info, ethernet info, IP(src and destn addr), TCP info(src port(temp),destn port no, seq no and ack no)

Step4: Click on capture again and continue without saving

Step5: Open GIT website on browser and now stop capturing packets on packet tracer and then check for http GET packet; you can see large packets captured in seconds

Step6: We can use filter and type HTTP and open the http packet and you will see the http section below TCP, which u can explore and see the 1) host as the website name visited 2)User-agent as Windows 10 and Chrome

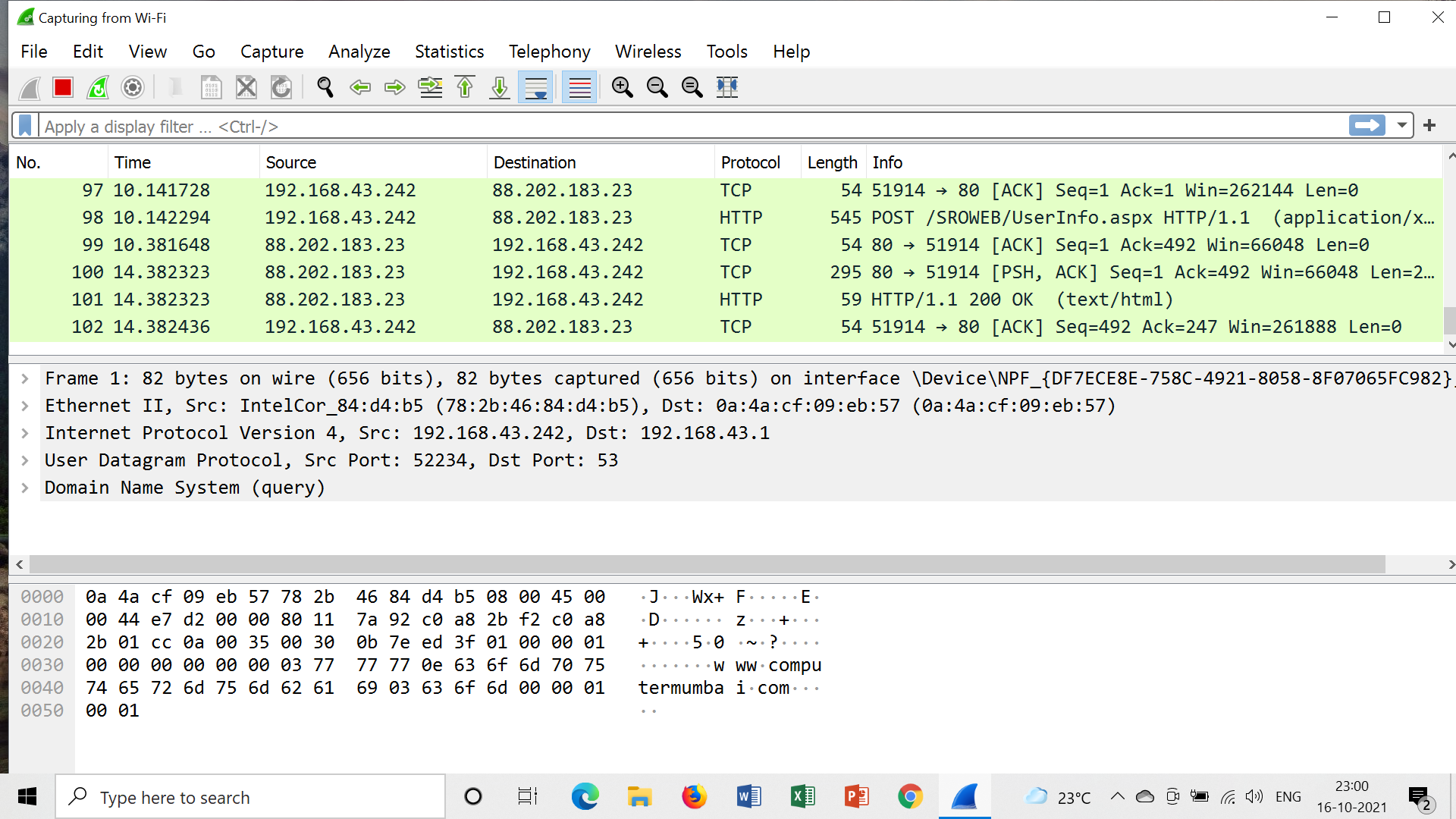
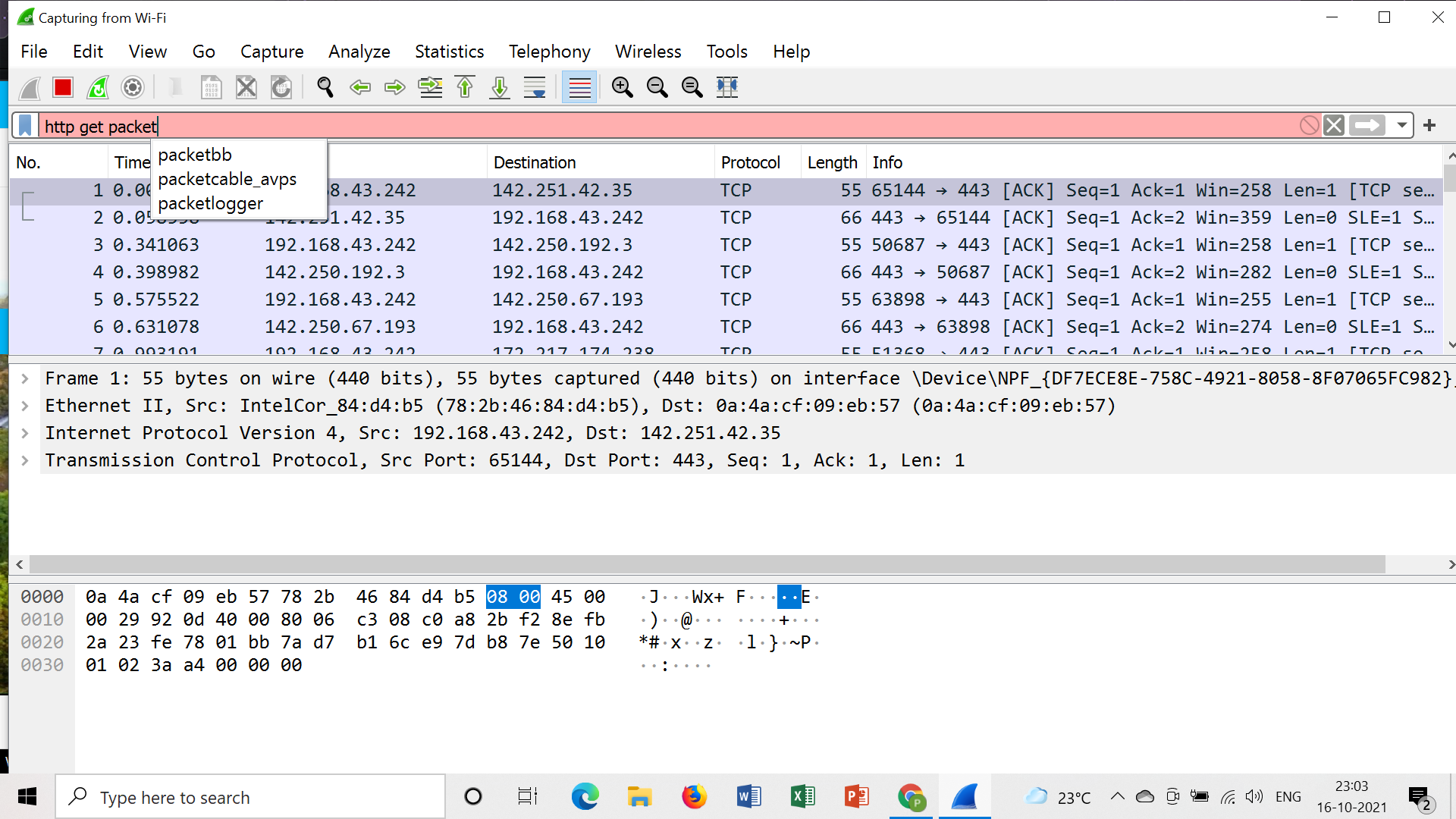
Step 7: If you want to check for the packets from certain source IP, click on that IP, right click and click on Apply as Filter and selected; “and selected” is for the filter to be applied for the given source IP along-with http

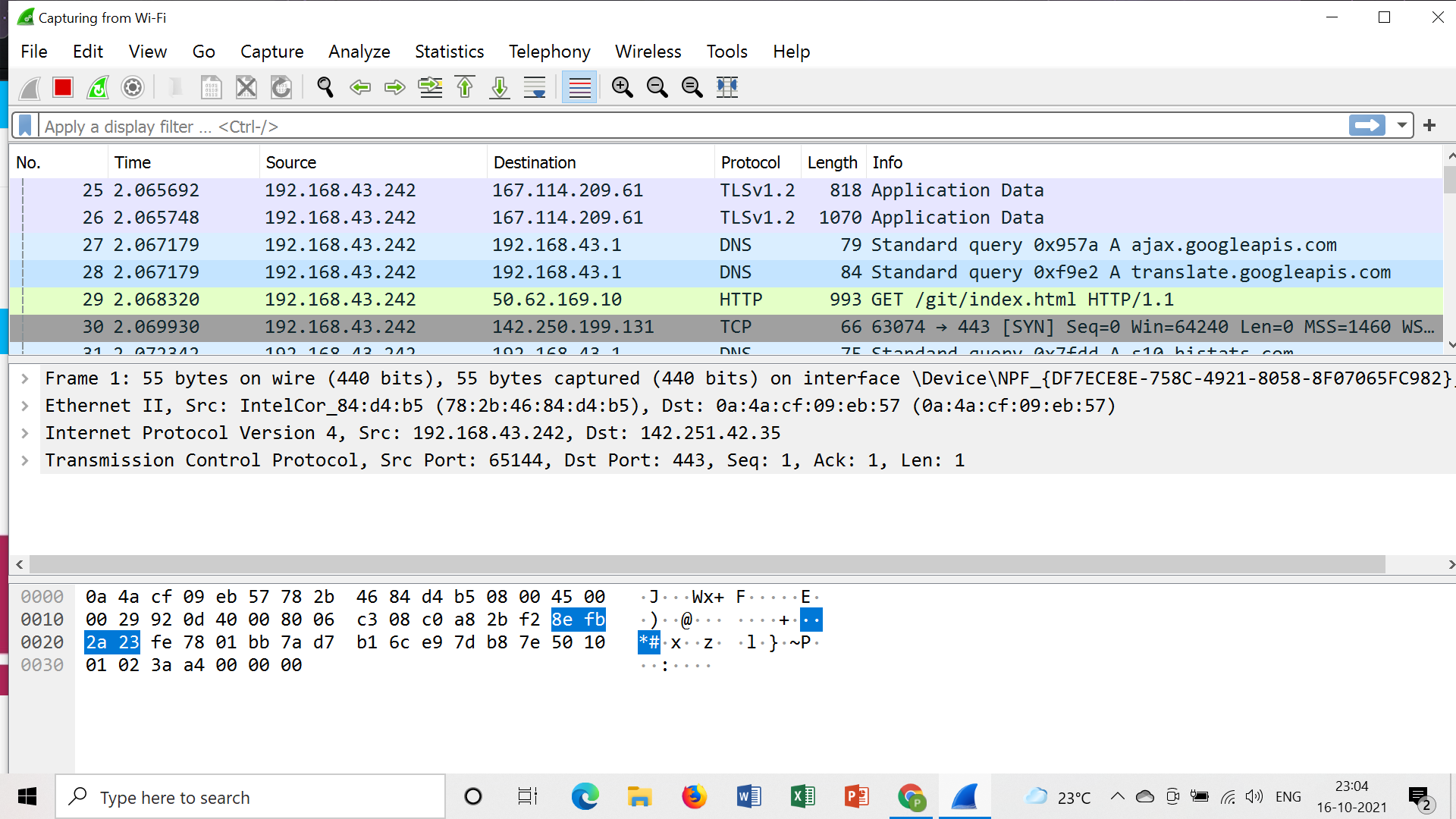
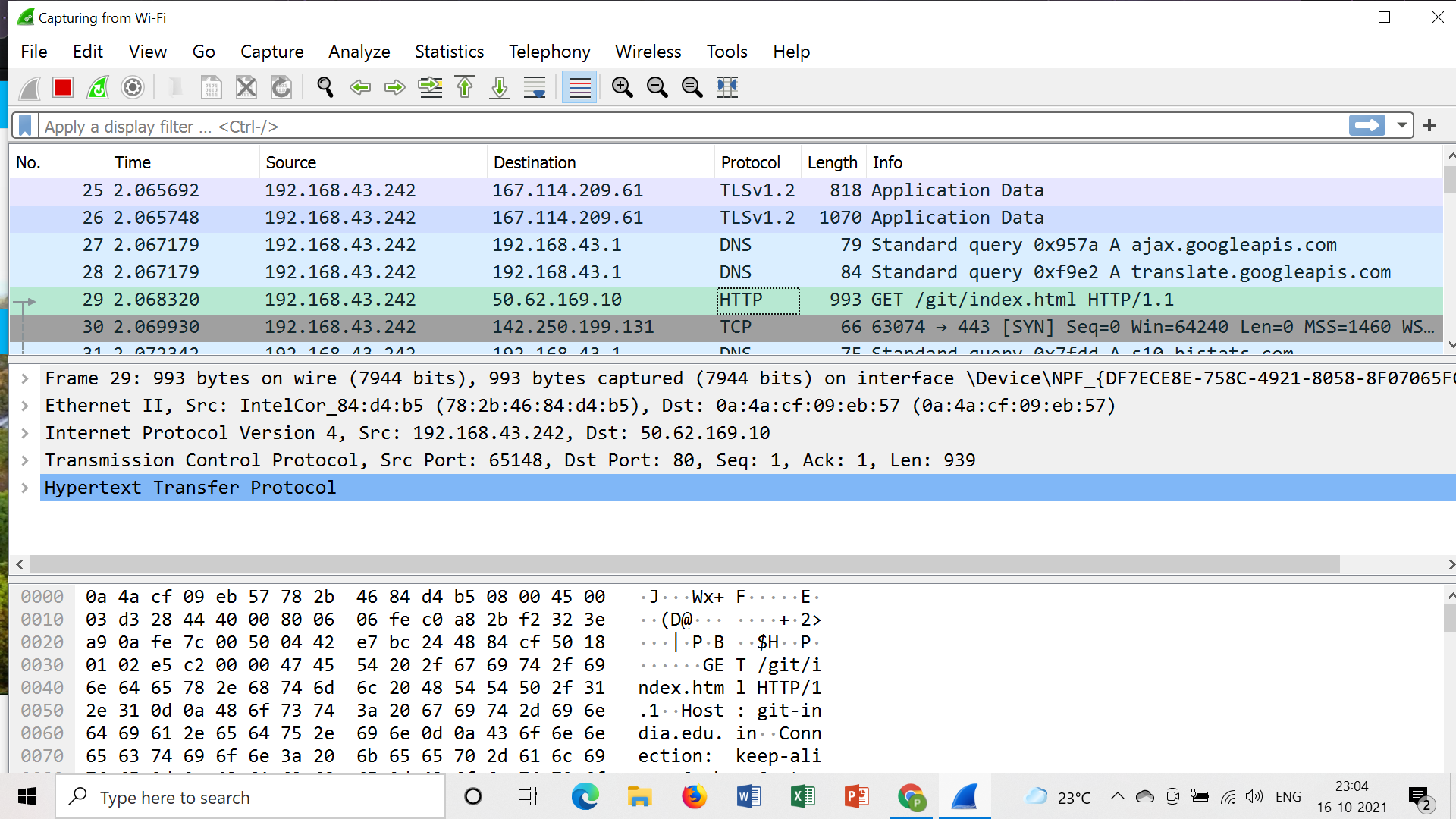
Step 8: Check for the http packets captured intended to us from webserver to us, which shows text/html OR text/css, and we can also see the corresponding html code.

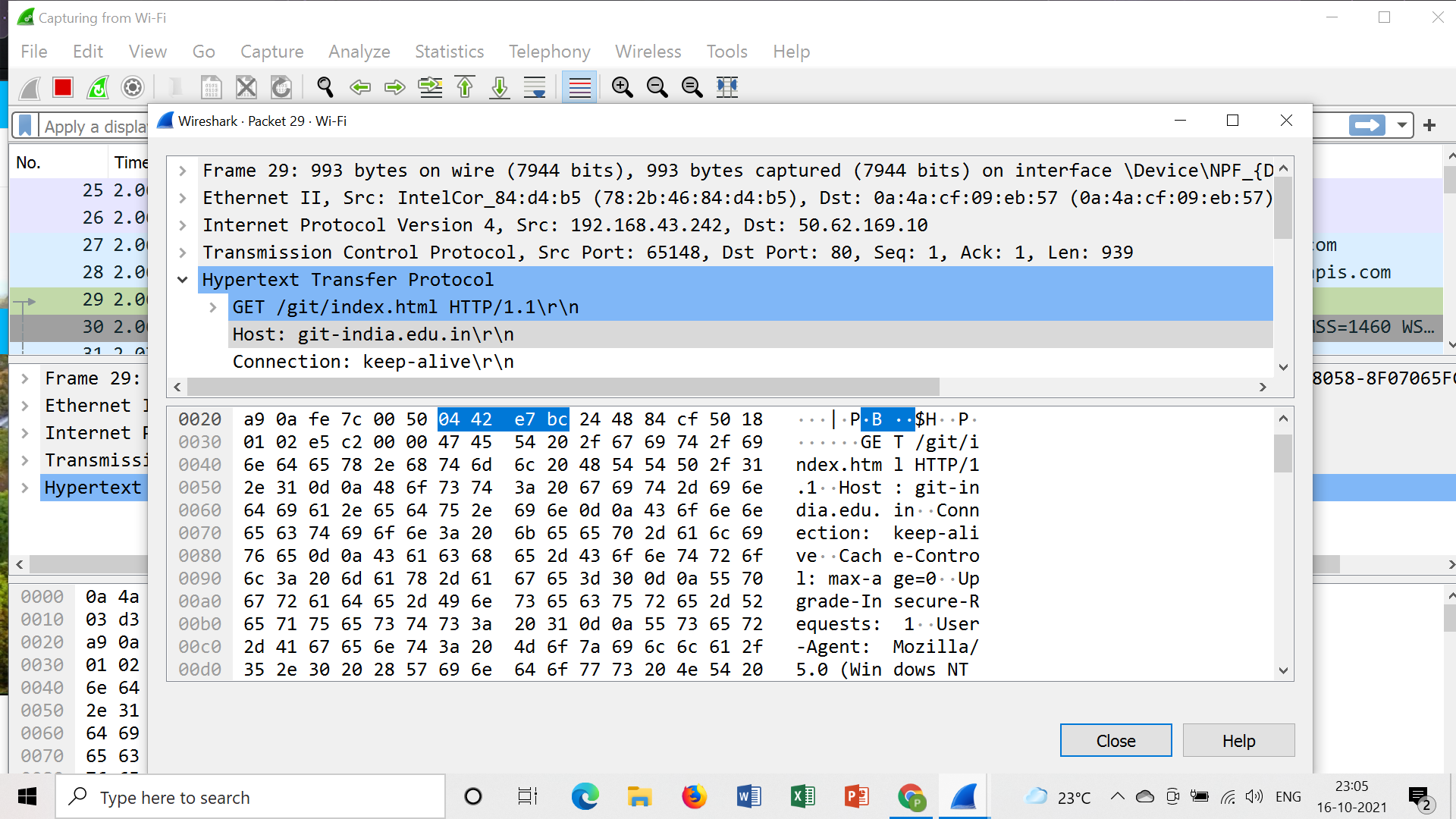
Step 9: Check for the ARP packet which is used to check for the MAC address at the initial stage, till it gets discovered, which can also be shown.

Step 10: Check for the Port no 53 for DNS by filtering the corresponding packet.

**Screenshots**:







#### **Conclusion**: Thus the study of [packets capturing](https://drive.google.com/file/d/1vBGNh8WhvANugl53VRIoCSY8FaKCPdn4/view?usp=sharing) is done using Wireshark software.