# CS212 : Computer Networks Lab
# Assignment 2

T Satwik
190030043

## 1 Part 1

### 1.1 Question 1

If a packet is highlighted by black, it means that the packet is identified to be TCP **packet with problems**, for example the packet could have been delivered out of order.

### 1.2 Question 2

we can simply use http as a filter command to get all the traffic with http protocol, but we can use the command:
ip.src ==(computer ip address) and http
With this command, we can get all the protocols with http and the packets with source as our own computer's ip address, so that we get only the outgoing packets from out compouter.

### 1.3 Question 3

DNS uses Follow UDP Stream while http use Follow TCP Stream, because UDP is faster compared to TCP and DNS requests are small and hence fit into the UDP segments. Thought UDP is less reliable when compared to TCP, extra protection can be added in the application layer of DNS. Hence DNS uses UDP instead of TCP.
However, HTTP uses TCP instead of UDP, as the packets are larger in size, and TCP is more reliable and secure(due to the handshaking protocol), Hence HTTP uses TCP protocol

# 2 Part 2

I have used http://info.cern.ch/, because it is one of the websites that is still using http and hence all the packets are displayed in the wireshark UI and I have used mozilla firefox browser.

## 2.1 Question 1

The different protocols that appear in the protocol column in the unfiltered packet-listing window in wireshark GUI are listed below:

- TCP
- TLSv1.2
- DNS
- HTTP
- OSCP
- TLSv1.3
- ARP

## 2.2 Question 2

Arrival time fort the HTTP GET request packet is : 17:56:49.119447257 IST
and the Arrival time fort the HTTP OK request packet is : 17:56:49.296067269 IST
Hence the time taken in between is

$$.296067269 - .119447257 = 0.176620012 \; seconds$$

These values can also present in the print file of the two messages, attached with this report.

## 2.3 Question 3

IP address of the URL(http://info.cern.ch/): 188.184.21.108
IP address of my computer: 192.168.1.12
This was obtained from the Internet Protocol section of the HTTP GET packet(can be checked in the print file of HTTP messages).

## 2.4 Question 4

The pdf of the print file is also attached with this report.

## 2.5 Question 5

The screenshots corresponding to Chrome (Figure 1) and Brave (Figure 2) browsers are attached with this report. As we can see, we get the HTTP GET and HTTP OK packets, with their other details just like we got with firefox browser, hence we are able to see HTTP protocol. However, the times taken between the GET and OK packets are lower for brave browser when compared to chrome.

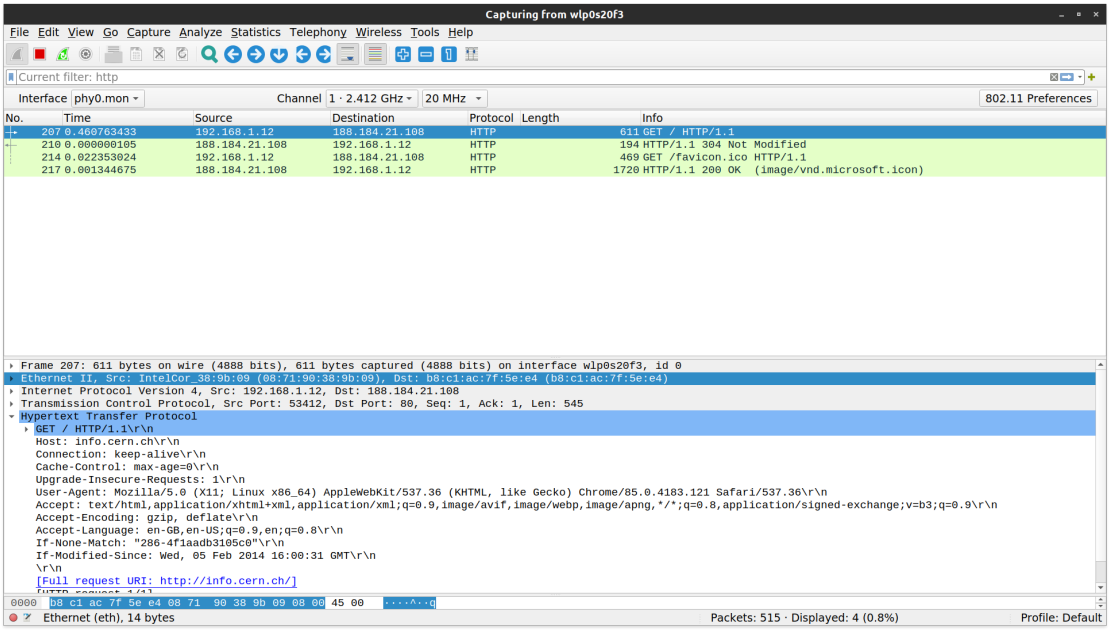


Figure 1: Chrome Browser

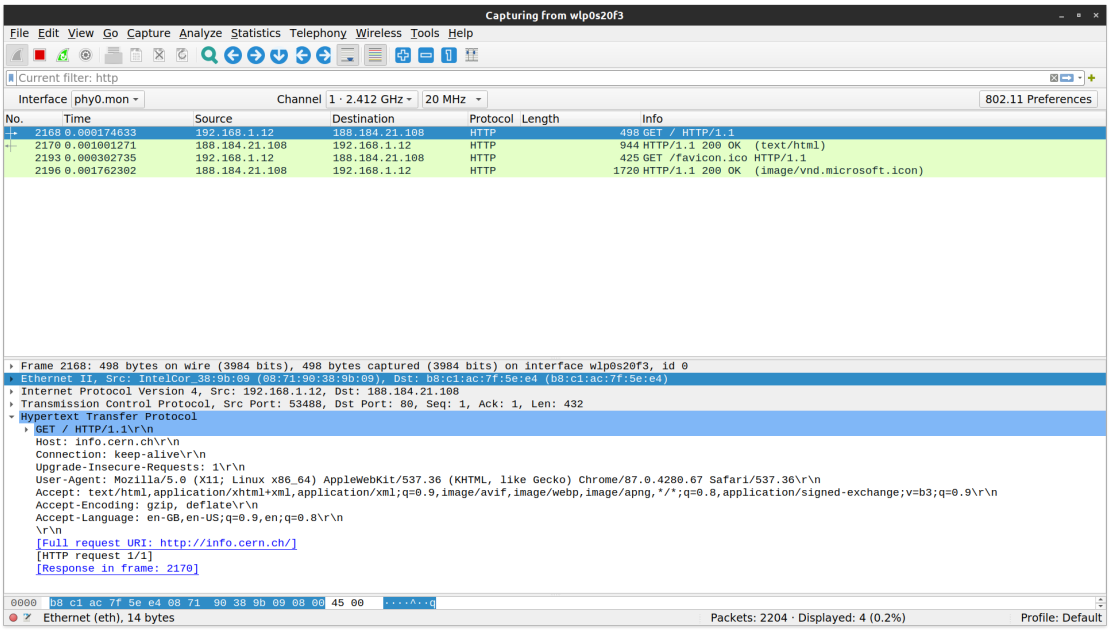


Figure 2: Brave Browser