# **Assignment 2: Getting started with Wireshark**

Name: Hrishikesh Ravindra Karande

Roll No: 210010020

**Part-I**

1. A packet highlighted in black means that it has some errors or problems. For example, it could have been delivered out of order, or it could have a checksum mismatch.
2. Using filter http and http.request we can list all outgoing traffic.
3. DNS use Follow UDP Stream:
   1. is smaller than TCP and faster. Since UDP does not require 3 way handshaking nor does it require establishing a connection.
   2. DNS is small and fit within the UDP segments.
   3. There are lot of DNS requests, UDP is more scalable than TCP so can handle requests better.

HTTP uses follow TCP stream:

1. TCP establishes connection by 3 way Handshaking, also is more reliable than UDP.
2. TCP ensures that packets have also been received by using checksum mechanism and in case of packet loss uses retransmission.

**Part-II**

1. Different protocols listed in the unfiltered packet-listing window are:

* ARP
* MDNS
* ICMPv6
* MDNS
* TCP
* UDP
* DNS
* TLSv1.3
* HTTP

1. Message was sent at: 5.937999 and OK was received at 5.966720. Therefore the it took roughly 0.02873s

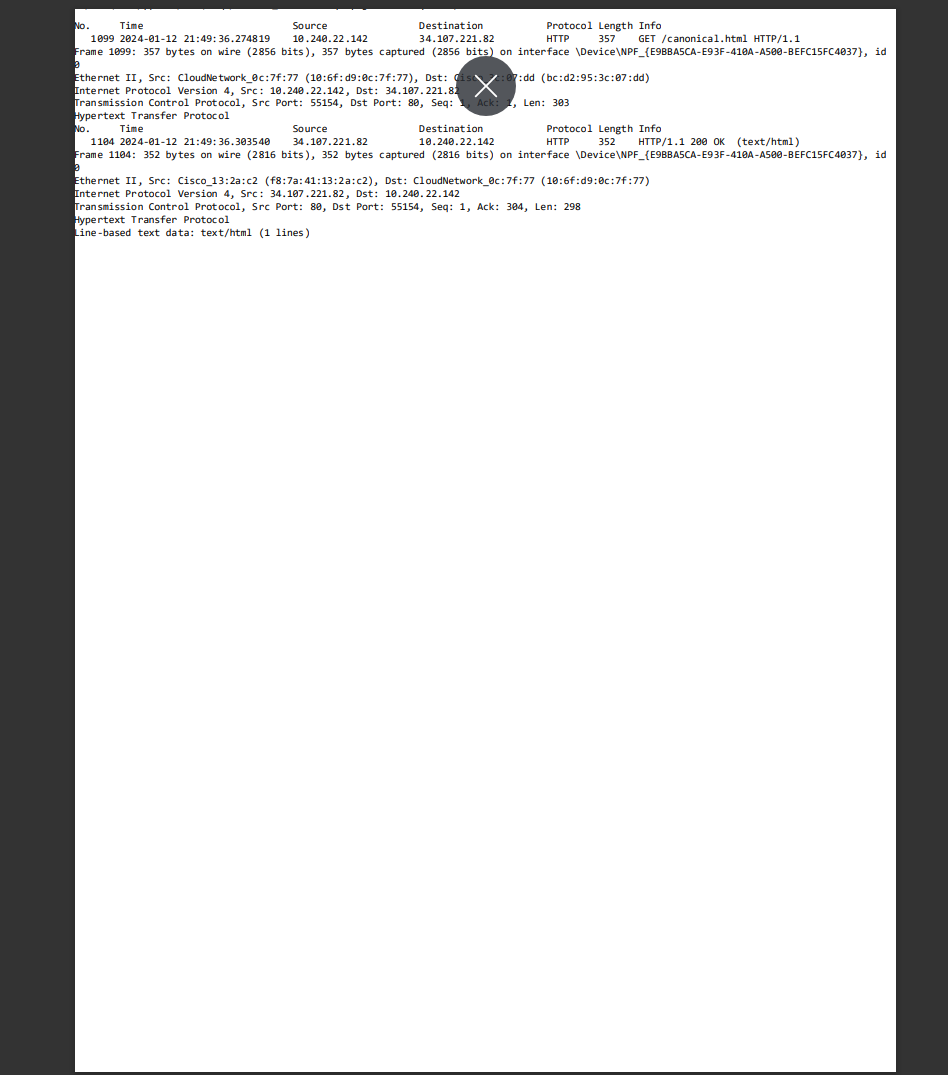
GET Sent :2024-01-12 21:49:36.274819

OKAY Received :2024-01-12 21:49:36.303540

1. The address of source (my Machine) is :10.240.22.142

The destination (URL visited) is : 34.107.221.82

1. **Note:Attaching screenshot of the pdf file that was directed to be generated.**



1. After Executing the above steps on Microsoft Edge, when http was used with filter there wasn’t any packet found. One reason for this might be the browser extensions that I am using microsoft edge. Also firewall or antivirus software settings. They might be blocking the capture or affecting network traffic.