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:
   a. is smaller than TCP and faster. Since UDP does not require 3 way handshaking nor does it require establishing a connection.
   b. DNS is small and fit within the UDP segments.
   c. There are lot of DNS requests, UDP is more scalable than TCP so can handle requests better.

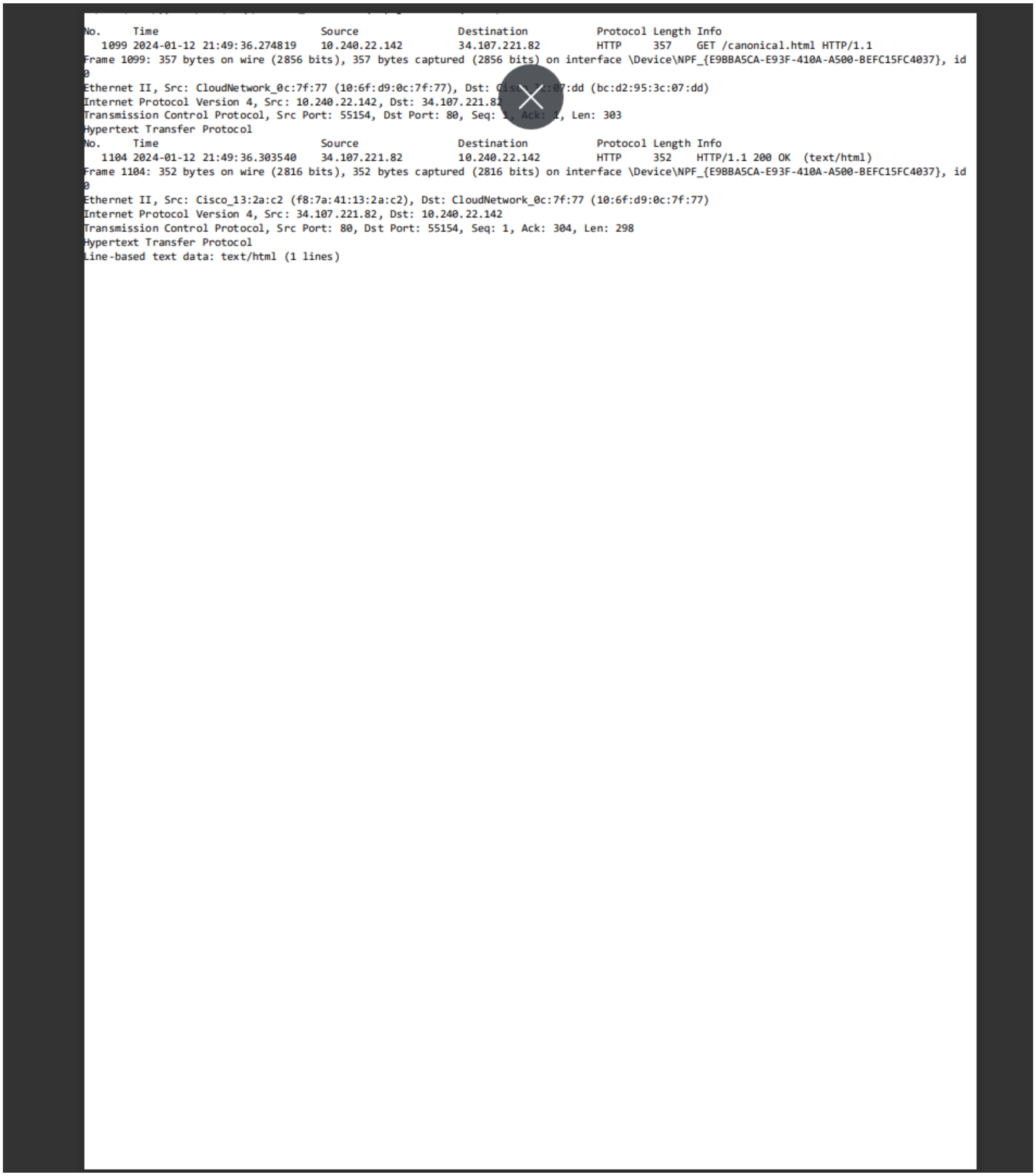
   HTTP uses follow TCP stream:
   a. TCP establishes connection by 3 way Handshaking, also is more reliable than UDP.
   b. TCP ensures that packets have also been received by using checksum mechanism and in case of packet loss uses retransmission.

PART-II

1. Different protocols listed in the unfiltered packet-listing window are:
    - ARP
    - MDNS
    - ICMPv6
    - MDNS
    - TCP
    - UDP
    - DNS
    - TLSv1.3
    - HTTP
2. 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

3. The address of source (my Machine) is :10.240.22.142
   The destination (URL visited) is : 34.107.221.82

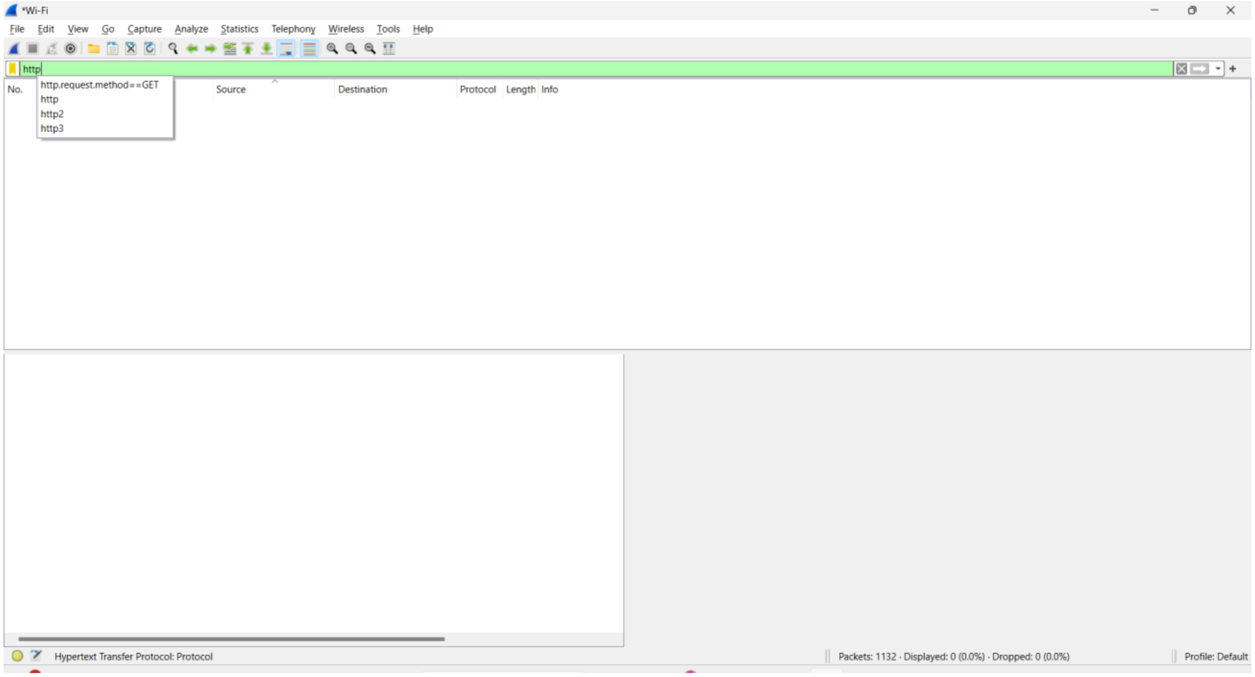
4. **Note:Attaching screenshot of the pdf file that was directed to be generated.**



```
No.     Time                          Source                Destination           Protocol Length Info
   1099 2024-01-12 21:49:36.274819    10.240.22.142         34.107.221.82         HTTP     357    GET /canonical.html HTTP/1.1
Frame 1099: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface \Device\NPF_{E9BBA5CA-E93F-410A-A500-BEFC15FC4037}, id
0
Ethernet II, Src: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77), Dst: Cisco_3c:07:dd (bc:d2:95:3c:07:dd)
Internet Protocol Version 4, Src: 10.240.22.142, Dst: 34.107.221.82
Transmission Control Protocol, Src Port: 55154, Dst Port: 80, Seq: 1, Ack: 1, Len: 303
Hypertext Transfer Protocol
No.     Time                          Source                Destination           Protocol Length Info
   1104 2024-01-12 21:49:36.303540    34.107.221.82         10.240.22.142         HTTP     352    HTTP/1.1 200 OK  (text/html)
Frame 1104: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface \Device\NPF_{E9BBA5CA-E93F-410A-A500-BEFC15FC4037}, id
0
Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: CloudNetwork_0c:7f:77 (10:6f:d9:0c:7f:77)
Internet Protocol Version 4, Src: 34.107.221.82, Dst: 10.240.22.142
Transmission Control Protocol, Src Port: 80, Dst Port: 55154, Seq: 1, Ack: 304, Len: 298
Hypertext Transfer Protocol
Line-based text data: text/html (1 lines)
```

5. 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.



http

http.request.method==GET
http
http2
http3

Hypertext Transfer Protocol: Protocol

Packets: 1132 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%)

Profile: Default