# Assignment 2

**Part-1**

1)

Black identifies TCP packets with problems - for example, they could have been delivered out-of-order.

2)

Type **http** in the filtering field of Wireshark to list all the **http** traffic on the connected on the network.

3)

DNS uses "Follow UDP Stream" because DNS operates over the User Datagram Protocol (UDP) whereas HTTP uses the Transmission Control Protocol (TCP), which is a connection-oriented protocol, hence it uses "Follow TCP Stream".

**Part-2**

1)

**TCP, DNS, TLS, DHCP, ARP, QUIC, MDNS** are the different protocols that appear in the protocol column in the unfiltered packet-listing window in Wireshark GUI

2)

0.23745 seconds is the amount of time it took between the **GET** message was sent and the **OK** reply was obtained.

3)

My computer **IP** is **10.240.22.74**

Destination **IP** is **15.197.142.173**

1. The data which was printed is as follows:-

**No. Time Source Destination Protocol Length Info**

**1077 18:11:53.665470597 15.197.142.173 10.240.22.74 HTTP 417 HTTP/1.1**

**301 Moved Permanently (text/html)**

**Frame 1077: 417 bytes on wire (3336 bits), 417 bytes captured (3336 bits) on interface**

**wlp0s20f3, id 0**

**Ethernet II, Src: Cisco\_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: Intel\_aa:e1:aa (98:8d:46:aa:e1:aa)**

**Internet Protocol Version 4, Src: 15.197.142.173, Dst: 10.240.22.74**

**0100 .... = Version: 4**

**.... 0101 = Header Length: 20 bytes (5)**

**Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)**

**Total Length: 403**

**Identification: 0xe413 (58387)**

**010. .... = Flags: 0x2, Don't fragment**

**...0 0000 0000 0000 = Fragment Offset: 0**

**Time to Live: 241**

**Protocol: TCP (6)**

**Header Checksum: 0xe4a4 [validation disabled]**

**[Header checksum status: Unverified]**

**Source Address: 15.197.142.173**

**Destination Address: 10.240.22.74**

**Transmission Control Protocol, Src Port: 80, Dst Port: 45148, Seq: 1, Ack: 348, Len: 351**

**Hypertext Transfer Protocol**

**HTTP/1.1 301 Moved Permanently\r\n**

**Date: Sun, 14 Jan 2024 12:41:54 GMT\r\n**

**Content-Type: text/html; charset=utf-8\r\n**

**Content-Length: 58\r\n**

**Connection: keep-alive\r\n**

**Location: http://www.flipkart.com\r\n**

**Server: ip-100-74-2-26.eu-west-2.compute.internal\r\n**

**X-Request-Id: 24b9cc4f-e6c0-4181-ad26-61d06ca49c9e\r\n**

**\r\n**

**[HTTP response 1/1]**

**[Time since request: 0.237443444 seconds]**

**[Request in frame: 1057]**

**[Request URI: http://www.flipkart.in/]**

**File Data: 58 bytes**

**Line-based text data: text/html (2 lines)**

**No. Time Source Destination Protocol Length Info**

**1136 18:11:53.964172009 103.243.32.90 10.240.22.74 HTTP 547 HTTP/1.1**

**301 Moved Permanently (text/html)**

**Frame 1136: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface**

**wlp0s20f3, id 0**

**Ethernet II, Src: Cisco\_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: Intel\_aa:e1:aa (98:8d:46:aa:e1:aa)**

**Internet Protocol Version 4, Src: 103.243.32.90, Dst: 10.240.22.74**

**0100 .... = Version: 4**

**.... 0101 = Header Length: 20 bytes (5)**

**Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)**

**Total Length: 533**

**Identification: 0xb8c2 (47298)**

**010. .... = Flags: 0x2, Don't fragment**

**...0 0000 0000 0000 = Fragment Offset: 0**

**Time to Live: 55**

**Protocol: TCP (6)**

**Header Checksum: 0xdf99 [validation disabled]**

**[Header checksum status: Unverified]**

**Source Address: 103.243.32.90**

**Destination Address: 10.240.22.74**

**Transmission Control Protocol, Src Port: 80, Dst Port: 33282, Seq: 1, Ack: 349, Len: 481**

**Hypertext Transfer Protocol**

**HTTP/1.1 301 Moved Permanently\r\n**

**server: nginx\r\n**

**date: Sun, 14 Jan 2024 12:41:54 GMT\r\n**

**content-type: text/html\r\n**

**content-length: 162\r\n**

**location: https://www.flipkart.com/\r\n/Users/omdeshmukh/Downloads/Sem VI/Computer Networks Lab/Lab2/om-mozilla.pcapng 6081 total packets, 62 shown**

**accept-ch: Sec-CH-UA,Sec-CH-UA-Arch,Sec-CH-UA-Full-Version,Sec-CH-UA-Full-Version-List,Sec-**

**CH-UA-Model,Sec-CH-UA-Platform,Sec-CH-UA-Platform-Version\r\n**

**\r\n**

**[HTTP response 1/1]**

**[Time since request: 0.050048454 seconds]**

**[Request in frame: 1135]**

**[Request URI: http://www.flipkart.com/]**

**File Data: 162 bytes**

**Line-based text data: text/html (7 lines)**

5)

All the values were output same as before, however instead of a **OK** message, I got a **MOVED PERMANENTLY** message.

Screenshot 2024-01-14 at 7.49.39 PM