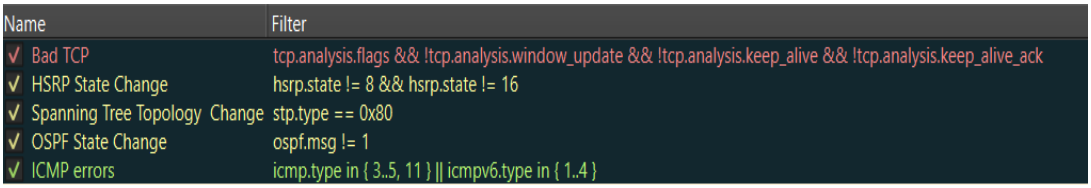
Computer Networks Lab

ASSIGNMENT – 2

Rahul Cheryala, 210010012

PART – 1

1. In Wireshark, if a packet is highlighted in black, it typically means that there is an issue with the TCP packet. Black highlighting often indicates TCP packets with problems, such as out-of-order delivery. Out-of-order delivery means that the packets did not arrive at the destination in the expected order, which can happen in certain network conditions.



Name	Filter
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }

2. The filter command for listing all outgoing HTTP traffic is:

   http.request.method == "GET" || http.request.method == "POST"

   This filter selects packets where the HTTP request method is either "GET" or "POST," indicating outgoing HTTP traffic.

3. DNS uses the User Datagram Protocol (UDP) for communication. UDP is a connectionless protocol that does not establish a persistent connection before transmitting data. DNS queries and responses are typically small and can fit within a single UDP packet.

   HTTP, on the other hand, uses the Transmission Control Protocol (TCP), which is a connection-oriented protocol. HTTP requires a reliable, ordered, and stream-oriented connection for the exchange of data between the client (browser) and the server. TCP provides mechanisms for error

recovery, retransmission of lost packets, and ensuring that data is received in the correct order.

When following a stream in Wireshark, "Follow UDP Stream" is used for UDP-based protocols, and "Follow TCP Stream" is used for TCP-based protocols. This allows you to see the entire conversation or data exchange between the client and server for the respective protocol.

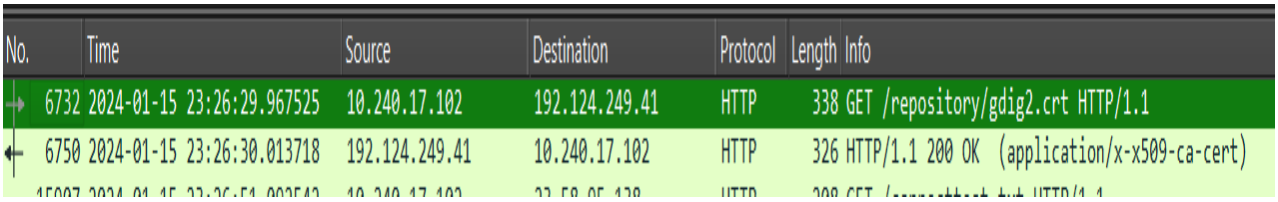
PART – 2

http://iitdh.ac.in/

1. In the unfiltered packet-listing window in Wireshark, we may see various protocols depending on the network activity. Common protocols include:

- HTTP
- TCP
- DNS
- TLS/SSL
- ARP
- ICMP
- UDP and others.

2. In Wireshark, you can filter for HTTP traffic using the display filter 'http'.
Look for the HTTP GET request and the corresponding HTTP OK reply.
Check the Time column for the time duration between the two messages.



No.	Time	Source	Destination	Protocol	Length	Info
6732	2024-01-15 23:26:29.967525	10.240.17.102	192.124.249.41	HTTP	338	GET /repository/gdig2.crt HTTP/1.1
6750	2024-01-15 23:26:30.013718	192.124.249.41	10.240.17.102	HTTP	326	HTTP/1.1 200 OK (application/x-x509-ca-cert)

The time it took from HTTP GET message to HTTP OK reply is:

30.013718 - 29.967525 = 0.046193 seconds

3. Identify the destination IP address for the URL you visited by looking at the HTTP GET request.
Determine your computer's IP address by checking the source IP address in the same HTTP GET request.

Internet Address of my computer: **10.240.17.102**
Internet (IP) Address of the URL: **192.124.249.41**

4.

```
No.     Time                           Source                Destination           Protocol Length Info
   2080 2024-01-15 23:29:39.295310    10.240.17.102         49.44.136.170         HTTP     208    GET /connecttest.txt HTTP/1.1
Frame 2080: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id
0
Ethernet II, Src: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf), Dst: Cisco_0a:9a:e1 (44:b6:be:0a:9a:e1)
Internet Protocol Version 4, Src: 10.240.17.102, Dst: 49.44.136.170
Transmission Control Protocol, Src Port: 4720, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
Hypertext Transfer Protocol
No.     Time                           Source                Destination           Protocol Length Info
   2082 2024-01-15 23:29:39.344650    49.44.136.170         10.240.17.102         HTTP     241    HTTP/1.1 200 OK  (text/plain)
Frame 2082: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id
0
Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf)
Internet Protocol Version 4, Src: 49.44.136.170, Dst: 10.240.17.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4720, Seq: 1, Ack: 155, Len: 187
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)
```

5.

Brave:

```
No.     Time                           Source                Destination           Protocol Length Info
   4894 2024-01-15 23:28:01.766245    10.240.17.102         23.58.95.138          HTTP     208    GET /connecttest.txt HTTP/1.1
Frame 4894: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id
0
Ethernet II, Src: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf), Dst: Cisco_0a:9a:e1 (44:b6:be:0a:9a:e1)
Internet Protocol Version 4, Src: 10.240.17.102, Dst: 23.58.95.138
Transmission Control Protocol, Src Port: 4594, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
Hypertext Transfer Protocol
No.     Time                           Source                Destination           Protocol Length Info
   4897 2024-01-15 23:28:01.817567    23.58.95.138          10.240.17.102         HTTP     241    HTTP/1.1 200 OK  (text/plain)
Frame 4897: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id
0
Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf)
Internet Protocol Version 4, Src: 23.58.95.138, Dst: 10.240.17.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4594, Seq: 1, Ack: 155, Len: 187
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)
```

Mozilla Firefox:

```
No.     Time                           Source                Destination           Protocol Length Info
   1327 2024-01-15 23:40:06.072400    10.240.17.102         34.107.221.82         HTTP     357    GET /canonical.html HTTP/1.1
Frame 1327: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id
0
Ethernet II, Src: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf), Dst: Cisco_0a:9a:e1 (44:b6:be:0a:9a:e1)
Internet Protocol Version 4, Src: 10.240.17.102, Dst: 34.107.221.82
Transmission Control Protocol, Src Port: 3389, Dst Port: 80, Seq: 1, Ack: 1, Len: 303
Hypertext Transfer Protocol
No.     Time                           Source                Destination           Protocol Length Info
   1329 2024-01-15 23:40:06.092821    34.107.221.82         10.240.17.102         HTTP     352    HTTP/1.1 200 OK  (text/html)
Frame 1329: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface \Device\NPF_{8F3B6709-9739-4955-9F08-FBF0EC1F870B}, id
0
Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: ASUSTekCOMPU_02:43:cf (04:42:1a:02:43:cf)
Internet Protocol Version 4, Src: 34.107.221.82, Dst: 10.240.17.102
Transmission Control Protocol, Src Port: 80, Dst Port: 3389, Seq: 1, Ack: 304, Len: 298
Hypertext Transfer Protocol
Line-based text data: text/html (1 lines)
```

Time taken from HTTP GET to HTTP OK in Brave browser is around 0.051322 seconds and for Firefox browser is around 0.020421 seconds.
Port number for Brave is: 4594

Port number for Firefox is: 3389