CS315: Assignment-2

Name: Shahil Patel
Roll No.: 200010039

Part-1

1. If a packet is highlighted in black, what does it mean for the packet?

   Ans: If a packet is highlighted in black, it shows a *TCP packet with a problem*, such as a packet that could have been delivered out-of-order.

2. What is the filter command for listing all outgoing HTTP traffic?

   Ans: The filter used to list all the outgoing HTTP traffic is: *http.request.method*

3. Why does DNS use follow UDP Stream while HTTP use follows TCP Stream?

Ans: DNS use follows the UDP (User Datagram Protocol) stream, as most DNS requests are brief and easily fit into UDP segments. At the same time, UDP is faster than TCP. While HTTP follows the TCP stream because TCP is a connection base and thus is more secure than UDP, which is less reliable. Before a client and server can exchange an HTTP request/response, they must establish a TCP connection, which requires several round trips.

Part-2

1. List the different protocols that appear in the protocol column in the unfiltered packet-listing window in wireshark GUI?

Ans: The different protocols that appear in the protocol column in the unfiltered packet-listing window in Wireshark GUI are:

a. TCP
b. OCSP
c. HTTP

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received for the web page you visited in your web browser? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

Ans. The time taken to receive the HTTP OK reply from when the HTTP GET message was sent is **0.085011062 seconds**.

3. What is the Internet (IP) address of the URL you visited and what is the Internet address of your computer?

   Ans: The Internet (IP) address of the URL visited is: **10.250.200.15**
   The Internet (IP) address of my Computer is: **10.196.9.130**

4. Print the two HTTP messages displayed in Wireshark GUI after you had visited the above URL through your web browser. To do so, select Print from the Wireshark File command menu, and select “Selected Packet Only” and then click Print.

   Ans: attached is a screenshot of the PDF printed using the above procedure:

```
No.     Time           Source                Destination           Protocol Length Info
     18 2.696829384    10.196.9.130          10.250.200.15         HTTP     543    GET / HTTP/1.1
Frame 18: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface wlp5s0, id 0
    Interface id: 0 (wlp5s0)
        Interface name: wlp5s0
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 10, 2023 11:16:52.781212044 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1673329612.781212044 seconds
    [Time delta from previous captured frame: 0.000199912 seconds]
    [Time delta from previous displayed frame: 2.339410316 seconds]
    [Time since reference or first frame: 2.696829384 seconds]
    Frame Number: 18
    Frame Length: 543 bytes (4344 bits)
    Capture Length: 543 bytes (4344 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: IntelCor_5b:96:b3 (d8:f2:ca:5b:96:b3), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
    Destination: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
        Address: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: IntelCor_5b:96:b3 (d8:f2:ca:5b:96:b3)
        Address: IntelCor_5b:96:b3 (d8:f2:ca:5b:96:b3)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.196.9.130, Dst: 10.250.200.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 529
    Identification: 0x82dd (33501)
    Flags: 0x40, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xceba [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.196.9.130
    Destination Address: 10.250.200.15
Transmission Control Protocol, Src Port: 34418, Dst Port: 80, Seq: 1, Ack: 1, Len: 477
    Source Port: 34418
    Destination Port: 80
```

```
    [Next request in frame: 40]
No.     Time           Source                Destination           Protocol Length Info
     38 2.781840446    10.250.200.15         10.196.9.130          HTTP     3598   HTTP/1.1 200 OK  (text/
html)
Frame 38: 3598 bytes on wire (28784 bits), 3598 bytes captured (28784 bits) on interface wlp5s0, id 0
    Interface id: 0 (wlp5s0)
        Interface name: wlp5s0
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 10, 2023 11:16:52.866223106 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1673329612.866223106 seconds
    [Time delta from previous captured frame: 0.000075648 seconds]
    [Time delta from previous displayed frame: 0.085011062 seconds]
    [Time since reference or first frame: 2.781840446 seconds]
    Frame Number: 38
    Frame Length: 3598 bytes (28784 bits)
    Capture Length: 3598 bytes (28784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8), Dst: IntelCor_5b:96:b3 (d8:f2:ca:5b:96:b3)
    Destination: IntelCor_5b:96:b3 (d8:f2:ca:5b:96:b3)
        Address: IntelCor_5b:96:b3 (d8:f2:ca:5b:96:b3)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
        Address: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
```

/tmp/wireshark_wlp5s0S8N6X1.pcapng 4326 total packets, 246 shown

```
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory
default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.250.200.15, Dst: 10.196.9.130
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 3584
    Identification: 0x060d (1549)
    Flags: 0x40, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: TCP (6)
    Header Checksum: 0x409c [validation disabled]
```

```
    Time to Live: 63
    Protocol: TCP (6)
    Header Checksum: 0x409c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.250.200.15
    Destination Address: 10.196.9.130
Transmission Control Protocol, Src Port: 80, Dst Port: 34418, Seq: 111118, Ack: 478, Len: 3532
    Source Port: 80
    Destination Port: 34418
    [Stream index: 2]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 3532]
    Sequence Number: 111118    (relative sequence number)
    Sequence Number (raw): 3242162667
    [Next Sequence Number: 114650    (relative sequence number)]
    Acknowledgment Number: 478    (relative ack number)
    Acknowledgment number (raw): 283845472
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····AP···]
    Window: 235
    [Calculated window size: 30080]
    [Window size scaling factor: 128]
    Checksum: 0xf541 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
        TCP Option - No-Operation (NOP)
            Kind: No-Operation (1)
        TCP Option - No-Operation (NOP)
            Kind: No-Operation (1)
        TCP Option - Timestamps: TSval 664388265, TSecr 1424448184
            Kind: Time Stamp Option (8)
            Length: 10
            Timestamp value: 664388265
            Timestamp echo reply: 1424448184
    [Timestamps]
        [Time since first frame in this TCP stream: 0.107056887 seconds]
        [Time since previous frame in this TCP stream: 0.000075648 seconds]
    [SEQ/ACK analysis]
```

5. Execute the above steps on Google Chrome, Safari, or any other browsers. also, check whether you will be able to see the http protocol. Write down your analysis with screenshots.

   Ans: a. The Protocols that appeared by using Google Chrome are:
   - I. MDNS
   - II. ARP
   - III. TCP
   - IV. TLSv1.2
   - V. DHCP

VI. NBNS

2708	28.614898868	216.239.32.116	10.196.9.130	TLSv1.3	97	Application Data
2709	28.614898927	216.239.32.116	10.196.9.130	TLSv1.3	105	Application Data
2710	28.614941073	10.196.9.130	216.239.32.116	TCP	66	53972 → 443 [ACK] Seq=1641 Ack=7144 W
2711	28.614985763	10.196.9.130	216.239.32.116	TLSv1.3	105	Application Data
2712	28.618931887	10.196.9.130	74.125.200.188	TCP	66	38266 → 5228 [ACK] Seq=1 Ack=1 Win=50
2713	28.655125625	216.239.32.116	10.196.9.130	TCP	66	443 → 53972 [ACK] Seq=7144 Ack=1680 W
2714	28.669466825	10.196.9.21	224.0.0.251	MDNS	81	Standard query response 0x0000 A, cac
2715	28.669466979	10.196.4.173	224.0.0.251	MDNS	160	Standard query response 0x0000 PTR, c
2716	28.669468614	10.196.8.34	10.196.255.255	NBNS	92	Name query NB WPAD<00>
2717	28.671754281	10.196.8.11	224.0.0.251	MDNS	103	Standard query 0x000f PTR _233637DE._
2718	28.684094271	142.250.195.206	10.196.9.130	TLSv1.2	349	Application Data
2719	28.684123049	10.196.9.130	142.250.195.206	TCP	66	43342 → 443 [ACK] Seq=813 Ack=1534 Wi
2720	28.684256315	10.196.9.130	142.250.195.206	TLSv1.2	101	Application Data
2721	28.684911500	10.196.9.130	142.250.195.206	TLSv1.2	101	Application Data

The HTTP protocol is unavailable because Google Chrome converts HTTP to HTTPS to secure the connection.

B. The Internet (IP) address of the URL visited is: **10.250.200.15**
The Internet (IP) address of my Computer is: **10.196.9.130**