CS315 : Computer Networks Lab

Assignment 2

Sourabh Bhosale (200010004)

January 10, 2023

1 Part 1

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

Black identifies TCP packets with problems, ICMP errors, OSPF State Change, HSRP State Change.

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

Filter command : http

3. Why does DNS use Follow UDP Stream while http use Follow TCP Stream?

DNS uses the User Datagram Protocol (UDP) on port 53 to serve DNS queries. UDP is preferred because it is fast and has low overhead. A DNS query is a single UDP request from the DNS client followed by a single UDP reply from the server.

Between TCP and UDP, TCP is reliable and UDP isn't. HTTP therefore relies on the TCP standard, which is connection-based. Before a client and server can exchange an HTTP request/response pair, they must establish a TCP connection, a process which requires several round-trips.

2 Part 2

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

MDNS, ARP, ICMP, ARP, QUIC, UDP, TCP, TLS, HTTP, SSDP, NTP

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.)

Time in seconds : 0.029133

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

IP address of URL : 10.250.200.15
IP address of computer : 10.196.6.255

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.

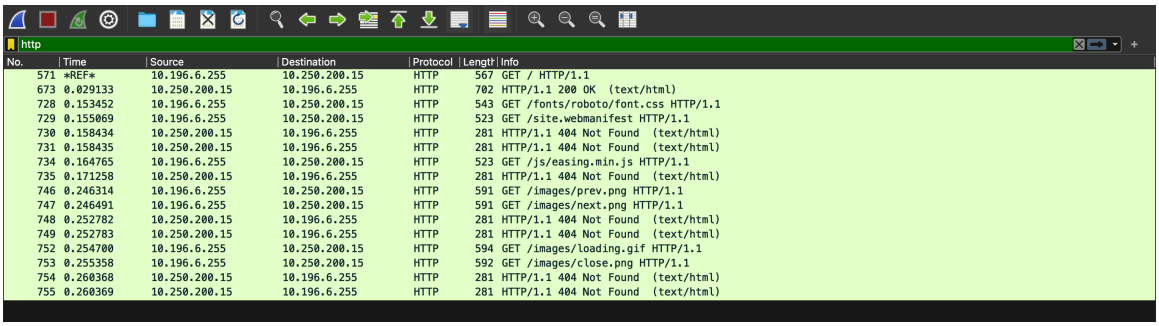
```
/var/folders/hy/jwrrl0ld76gghnkgv8yv_6040000gn/T/wireshark_Wi-FiWWQGY1.pcapng 1736 total packets, 16 shown

No.     Time           Source                Destination           Protocol Length Info
    571 *REF*          10.196.6.255          10.250.200.15         HTTP     567    GET / HTTP/
1.1
Frame 571: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface en0, id 0
Ethernet II, Src: Apple_ad:cf:45 (14:7d:da:ad:cf:45), Dst: ExtremeNetworks_9a:82:e8
(02:04:96:9a:82:e8)
Internet Protocol Version 4, Src: 10.196.6.255, Dst: 10.250.200.15
Transmission Control Protocol, Src Port: 59465, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    673 0.029133       10.250.200.15         10.196.6.255          HTTP     702    HTTP/1.1 200
OK  (text/html)
Frame 673: 702 bytes on wire (5616 bits), 702 bytes captured (5616 bits) on interface en0, id 0
Ethernet II, Src: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8), Dst: Apple_ad:cf:45
(14:7d:da:ad:cf:45)
Internet Protocol Version 4, Src: 10.250.200.15, Dst: 10.196.6.255
Transmission Control Protocol, Src Port: 80, Dst Port: 59465, Seq: 114014, Ack: 502, Len: 636
[80 Reassembled TCP Segments (114649 bytes): #573(1448), #574(1448), #575(1448), #576(1448),
#577(1448), #578(1069), #579(1448), #580(1448), #581(1448), #582(1448), #590(1448), #591(1448),
#592(1448), #593(1448), #594(1448), #595(1448), #59]
Hypertext Transfer Protocol
Line-based text data: text/html (1993 lines)
```

Figure 1: `HTTP messages`

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

For Safari browser, I was able to see http protocol results as shown below :

Figure 2: `iitdh.ac.in of Safari`



http

No.	Time	Source	Destination	Protocol	Length	Info
571	*REF*	10.196.6.255	10.250.200.15	HTTP	567	GET / HTTP/1.1
673	0.029133	10.250.200.15	10.196.6.255	HTTP	702	HTTP/1.1 200 OK (text/html)
728	0.153452	10.196.6.255	10.250.200.15	HTTP	543	GET /fonts/roboto/font.css HTTP/1.1
729	0.155069	10.196.6.255	10.250.200.15	HTTP	523	GET /site.webmanifest HTTP/1.1
730	0.158434	10.250.200.15	10.196.6.255	HTTP	281	HTTP/1.1 404 Not Found (text/html)
731	0.158435	10.250.200.15	10.196.6.255	HTTP	281	HTTP/1.1 404 Not Found (text/html)
734	0.164765	10.196.6.255	10.250.200.15	HTTP	523	GET /js/easing.min.js HTTP/1.1
735	0.171258	10.250.200.15	10.196.6.255	HTTP	281	HTTP/1.1 404 Not Found (text/html)
746	0.246314	10.196.6.255	10.250.200.15	HTTP	591	GET /images/prev.png HTTP/1.1
747	0.246491	10.196.6.255	10.250.200.15	HTTP	591	GET /images/next.png HTTP/1.1
748	0.252782	10.250.200.15	10.196.6.255	HTTP	281	HTTP/1.1 404 Not Found (text/html)
749	0.252783	10.250.200.15	10.196.6.255	HTTP	281	HTTP/1.1 404 Not Found (text/html)
752	0.254700	10.196.6.255	10.250.200.15	HTTP	594	GET /images/loading.gif HTTP/1.1
753	0.255358	10.196.6.255	10.250.200.15	HTTP	592	GET /images/close.png HTTP/1.1
754	0.260368	10.250.200.15	10.196.6.255	HTTP	281	HTTP/1.1 404 Not Found (text/html)
755	0.260369	10.250.200.15	10.196.6.255	HTTP	281	HTTP/1.1 404 Not Found (text/html)

Figure 3: `http result for Safari`

For Google Chrome and Brave browser, I was not able to see any http protocol results.