CS 315 : Computer Networks Lab
Assignment - 2
Getting started with Wireshark

Ayush Mallick
CS22BT008

Part-1

1.

In Wireshark, black-highlighted packets indicate potential problems in the network connection or instability in packet delivery. The errors can be Bad TCP, HSRP State Change, Spanning Tree Topology Change, OSPF State Change, ICMP errors, Checksum Errors as per the default coloring rules (View -> Coloring Rules) in Wireshark.

2.

To list all outgoing HTTP traffic using Wireshark, we can use the filter command *http.request*. This filter shows all HTTP GET and POST requests.

3.

DNS uses Follow UDP Stream because it primarily uses the connectionless UDP protocol for fast, small queries, which is faster and more efficient. HTTP uses Follow TCP Stream since it relies on the connection-oriented TCP protocol for reliable, ordered communication.

Part-2

1.

ARP – resolves IP addresses to MAC addresses.
DNS – used for resolving domain names into IP addresses.
TCP – provides reliable data transfer for communication.
TLS – used for secure HTTPS communication.
HTTP – used for transferring website content over the network.
QUIC – transport layer network protocol designed by Google.
OSPF – dynamic routing protocol for finding the best path between routers.
OCSP – used to check the revocation status of X.509 digital certificates.
etc.

2.

a. **frame contains “iitdh” :** 15
b. **http.request.method==GET :** 26
c. **http.request.method==POST :** 82
d. **tcp :** 4915
e. **tls :** 1887
f. **tcp and tls :** 1608

3.

a.

Domain	Source IP	Destination IP
iitdh.ac.in	10.200.255.153	10.195.250.62
amazon.in	10.200.255.153	52.95.116.115
youtube.com	10.200.255.153	142.250.183.46

b.

Domain	Source Port	Destination Port
iitdh.ac.in	36256	443
amazon.in	43258	443
youtube.com	60858	443

c.

https://iitdh.ac.in

2.133394878 - 2.131930619 = 0.001464259 seconds

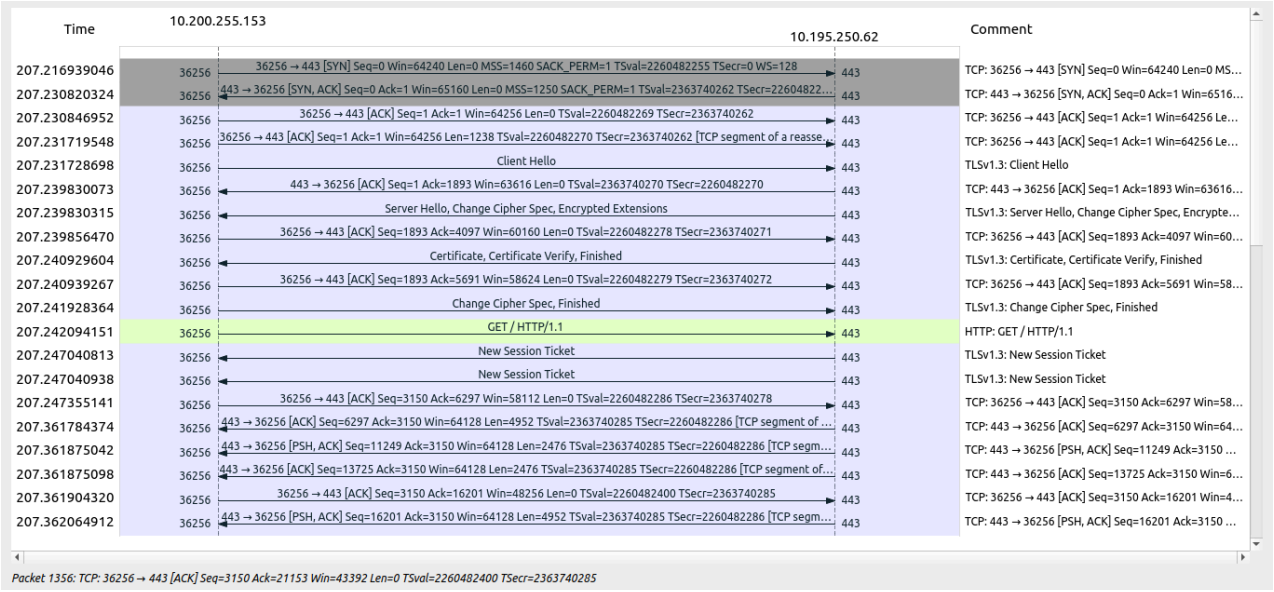
https://www.amazon.in

8.505432567 - 8.314369938 = 0.191062629 seconds

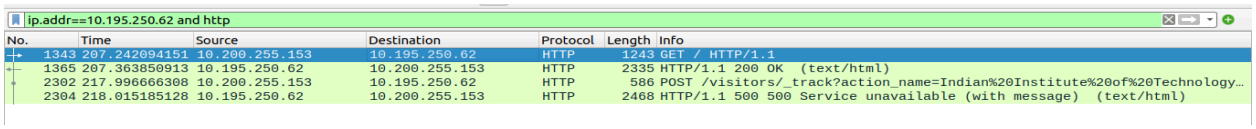
https://youtube.com

4.474375419 - 4.416556382 = 0.057819037 seconds

d.



4.



ip.addr==10.195.250.62 and http

No.	Time	Source	Destination	Protocol	Length	Info
1343	207.242094151	10.200.255.153	10.195.250.62	HTTP	1243	GET / HTTP/1.1
1365	207.363850913	10.195.250.62	10.200.255.153	HTTP	2335	HTTP/1.1 200 OK (text/html)
2302	217.996666308	10.200.255.153	10.195.250.62	HTTP	586	POST /visitors/_track?action_name=Indian%20Institute%20of%20Technology…
2304	218.015185128	10.195.250.62	10.200.255.153	HTTP	2468	HTTP/1.1 500 500 Service unavailable (with message) (text/html)

a. GET

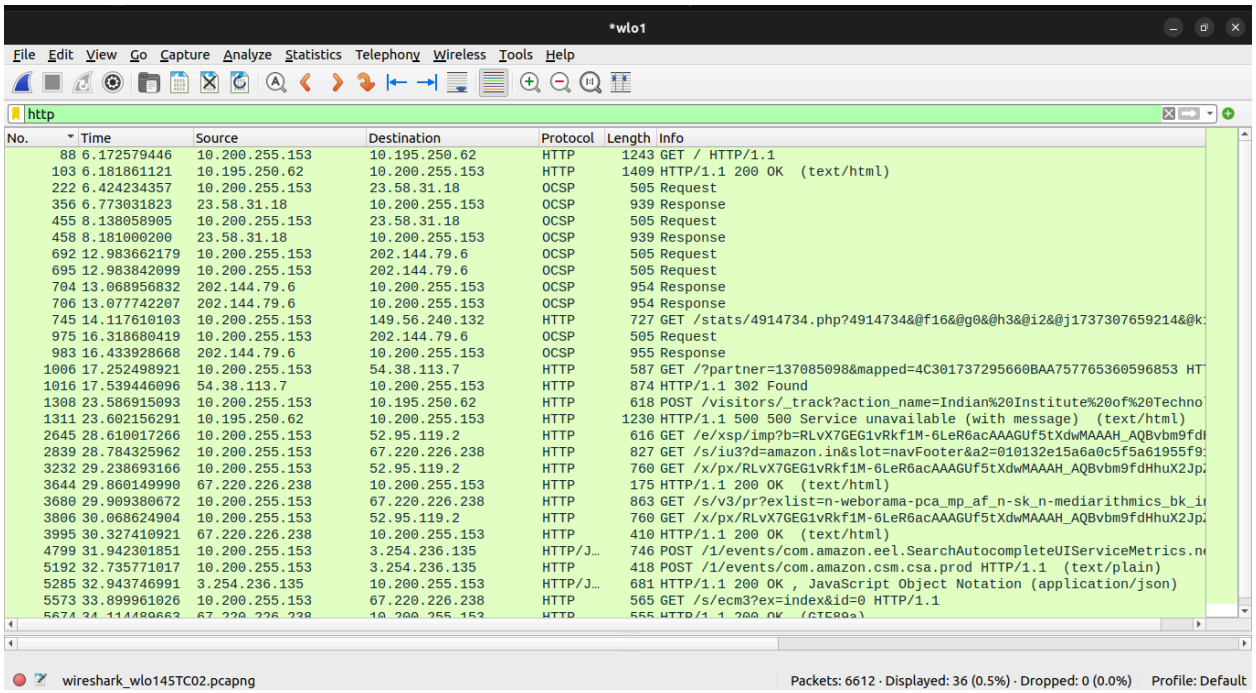
b. HTTP/1.1

c. 200 OK

d. 0.121756762

e. Yes, the IP address remains the same for *iitdh.ac.in*.
However, the IP addresses keep changing for *amazon.in* and *youtube.com*.

5.



*wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
88	6.172579446	10.200.255.153	10.195.250.62	HTTP	1243	GET / HTTP/1.1
103	6.181861121	10.195.250.62	10.200.255.153	HTTP	1409	HTTP/1.1 200 OK (text/html)
222	6.424234357	10.200.255.153	23.58.31.18	OCSP	505	Request
356	6.773031823	23.58.31.18	10.200.255.153	OCSP	939	Response
455	8.138058905	10.200.255.153	23.58.31.18	OCSP	505	Request
458	8.181000200	23.58.31.18	10.200.255.153	OCSP	939	Response
692	12.983662179	10.200.255.153	202.144.79.6	OCSP	505	Request
695	12.983842099	10.200.255.153	202.144.79.6	OCSP	505	Request
704	13.068956832	202.144.79.6	10.200.255.153	OCSP	954	Response
706	13.077742207	202.144.79.6	10.200.255.153	OCSP	954	Response
745	14.117610103	10.200.255.153	149.56.240.132	HTTP	727	GET /stats/4914734.php?4914734&@f16&@g0&@h3&@i2&@j1737307659214&@k:
975	16.318680419	10.200.255.153	202.144.79.6	OCSP	505	Request
983	16.433928668	202.144.79.6	10.200.255.153	OCSP	955	Response
1006	17.252498921	10.200.255.153	54.38.113.7	HTTP	587	GET /?partner=137085098&mapped=4C301737295660BAA757765360596853 HT
1016	17.539446096	54.38.113.7	10.200.255.153	HTTP	874	HTTP/1.1 302 Found
1308	23.586915093	10.200.255.153	10.195.250.62	HTTP	618	POST /visitors/_track?action_name=Indian%20Institute%20of%20Techno
1311	23.602156291	10.195.250.62	10.200.255.153	HTTP	1230	HTTP/1.1 500 500 Service unavailable (with message) (text/html)
2645	28.610017266	10.200.255.153	52.95.119.2	HTTP	616	GET /e/xsp/imp?b=RLvX7GEG1vRkf1M-6LeR6acAAAGUf5tXdwMAAAH_AQBvbm9fdI
2839	28.784325962	10.200.255.153	67.220.226.238	HTTP	827	GET /s/iu3?d=amazon.in&slot=navFooter&a2=010132e15a6a0c5f5a61955f9:
3232	29.238693166	10.200.255.153	52.95.119.2	HTTP	760	GET /x/px/RLvX7GEG1vRkf1M-6LeR6acAAAGUf5tXdwMAAAH_AQBvbm9fdHhuX2Jp:
3644	29.860149990	67.220.226.238	10.200.255.153	HTTP	175	HTTP/1.1 200 OK (text/html)
3680	29.909380672	10.200.255.153	67.220.226.238	HTTP	863	GET /s/v3/pr?exlist=n-weborama-pca_mp_af_n-sk_n-mediarithmics_bk_i
3806	30.068624904	10.200.255.153	52.95.119.2	HTTP	760	GET /x/px/RLvX7GEG1vRkf1M-6LeR6acAAAGUf5tXdwMAAAH_AQBvbm9fdHhuX2Jp:
3995	30.327410921	67.220.226.238	10.200.255.153	HTTP	410	HTTP/1.1 200 OK (text/html)
4799	31.942301851	10.200.255.153	3.254.236.135	HTTP/J…	746	POST /1/events/com.amazon.eel.SearchAutocompleteUIServiceMetrics.n
5192	32.735771017	10.200.255.153	3.254.236.135	HTTP	418	POST /1/events/com.amazon.csm.csa.prod HTTP/1.1 (text/plain)
5285	32.943746991	3.254.236.135	10.200.255.153	HTTP/J…	681	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
5573	33.899961026	10.200.255.153	67.220.226.238	HTTP	565	GET /s/ecm3?ex=index&id=0 HTTP/1.1
5674	34.114489663	67.220.226.238	10.200.255.153	HTTP	555	HTTP/1.1 200 OK (GIF89a)

wireshark_wlo145TC02.pcapng Packets: 6612 · Displayed: 36 (0.5%) · Dropped: 0 (0.0%) Profile: Default

As seen in the screenshot above, the HTTP protocol packets are visible after setting up TLS decryption using SSLKEYLOGGERFILE.