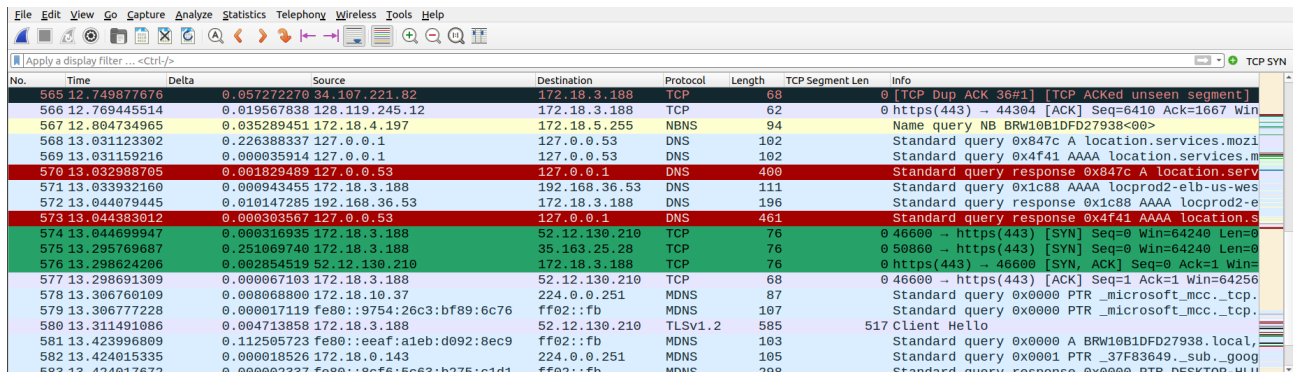


Lab- 1

-Sanyam Kaul
-CS23MTECH14011

Q1.

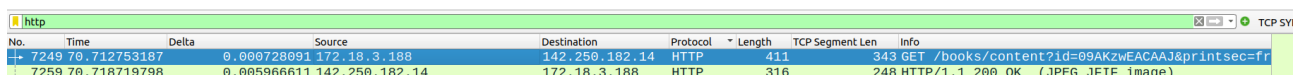
I can see many protocols in my packet capture. Some of them are: -
TCP, OCSP, MDNS, UDP, T:SV1.2. ARP, NBNS, ICMPv6, DNS



No.	Time	Delta	Source	Destination	Protocol	Length	TCP Segment Len	Info
565	12.749877676	0.057272270	34.107.221.82	172.18.3.188	TCP	68		0 [TCP Dup ACK 36#1] [TCP ACKED unseen segment]
566	12.769445514	0.019567838	128.119.245.12	172.18.3.188	TCP	62		0 https(443) → 44304 [ACK] Seq=6410 Ack=1667 Win=
567	12.804734965	0.035289451	172.18.4.197	172.18.5.255	NBNS	94		Name query NB BRW10B1DFD27938<00>
568	13.031123302	0.226388337	127.0.0.1	127.0.0.53	DNS	102		Standard query 0x847c A location.services.mozil
569	13.031159216	0.000035914	127.0.0.1	127.0.0.53	DNS	102		Standard query 0x4f41 AAAA location.services.m
570	13.032988705	0.001829489	127.0.0.53	127.0.0.1	DNS	400		Standard query response 0x847c A location.serv
571	13.033932160	0.000943455	172.18.3.188	192.168.36.53	DNS	111		Standard query 0x1c88 AAAA locprod2-elb-us-wes
572	13.044079445	0.010147285	192.168.36.53	172.18.3.188	DNS	196		Standard query response 0x1c88 AAAA locprod2-e
573	13.044383012	0.000303567	127.0.0.53	127.0.0.1	DNS	461		Standard query response 0x4f41 AAAA location.s
574	13.044699947	0.000316935	172.18.3.188	52.12.130.210	TCP	76		0 46600 → https(443) [SYN] Seq=0 Win=64240 Len=0
575	13.295769687	0.251069740	172.18.3.188	35.163.25.28	TCP	76		0 50800 → https(443) [SYN] Seq=0 Win=64240 Len=0
576	13.298624206	0.002854519	52.12.130.210	172.18.3.188	TCP	76		0 https(443) → 46600 [SYN, ACK] Seq=9 Ack=1 Win=
577	13.298691309	0.000067103	172.18.3.188	52.12.130.210	TCP	68		0 46600 → https(443) [ACK] Seq=1 Ack=1 Win=64256
578	13.306760109	0.008068000	172.18.10.37	224.0.0.251	MDNS	87		Standard query 0x0000 PTR _microsoft_mcc._tcp.
579	13.306777228	0.000017119	fe80::9754:26c3:bf89:6c76	ff02::fb	MDNS	107		Standard query 0x0000 PTR _microsoft_mcc._tcp.
580	13.311491086	0.004713858	172.18.3.188	52.12.130.210	TLSv1.2	585		517 Client Hello
581	13.423996809	0.112505723	fe80::eaf:a1eb:d092:8ec9	ff02::fb	MDNS	103		Standard query 0x0000 A BRW10B1DFD27938.local
582	13.424015335	0.000018526	172.18.0.143	224.0.0.251	MDNS	105		Standard query 0x0001 PTR _37f83649._sub._goog
583	13.424017672	0.000002337	fe80::8c56:5c63:b275:c1d1	ff02::fb	MDNS	298		Standard query response 0x0000 PTR DESKTOP-HUI

Q2.

I captured packets for harvard.com. There were multiple HTTP GET requests. Below is the snapshot of 1 such request and its response: -



No.	Time	Delta	Source	Destination	Protocol	Length	TCP Segment Len	Info
7249	70.712753187	0.000728091	172.18.3.188	142.250.182.14	HTTP	411	343	GET /books/content?id=09AKZwEACAAJ&printsec=fr
7259	70.718719798	0.005966611	142.250.182.14	172.18.3.188	HTTP	316	248	HTTP/1.1 200 OK (JPEG JFIF image)

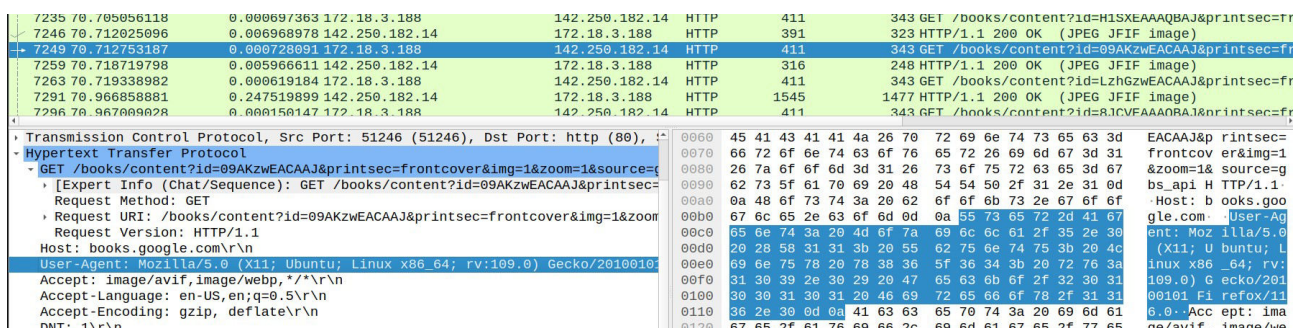
I made a separate column of delta time which shows the total time it took to respond to the GET request.

Q3.

I captured for harvard.com and its destination IP is – 142.250.182.14

Q4.

On selecting one of the HTTP packet, I can see that the user-agent is Mozilla/5.0 in the packet-details window. I am using Firefox browser



No.	Time	Delta	Source	Destination	Protocol	Length	TCP Segment Len	Info
7235	70.705056118	0.000697363	172.18.3.188	142.250.182.14	HTTP	411	343	GET /books/content?id=HISXEAQA&printsec=fr
7246	70.710250996	0.006968978	142.250.182.14	172.18.3.188	HTTP	391	323	HTTP/1.1 200 OK (JPEG JFIF image)
7249	70.712753187	0.000728091	172.18.3.188	142.250.182.14	HTTP	411	343	GET /books/content?id=09AKZwEACAAJ&printsec=fr
7259	70.718719798	0.005966611	142.250.182.14	172.18.3.188	HTTP	316	248	HTTP/1.1 200 OK (JPEG JFIF image)
7263	70.719338982	0.000619184	172.18.3.188	142.250.182.14	HTTP	411	343	GET /books/content?id=LzhGzwEACAAJ&printsec=fr
7291	70.966858881	0.247519899	142.250.182.14	172.18.3.188	HTTP	1545	1477	HTTP/1.1 200 OK (JPEG JFIF image)
7296	70.967089828	0.000150147	172.18.3.188	142.250.182.14	HTTP	411	343	GET /books/content?id=JCVFAA0RA&printsec=fr

Transmission Control Protocol, Src Port: 51246 (51246), Dst Port: http (80), Seq: 343, Win: 64240, Len: 0	
Hypertext Transfer Protocol	
GET /books/content?id=09AKZwEACAAJ&printsec=frontcover&img=1&zoom=1&source=google&bs_api=H HTTP/1.1	
[Expert Info (Chat/Sequence): GET /books/content?id=09AKZwEACAAJ&printsec=frontcover&img=1&zoom=1&source=google&bs_api=H HTTP/1.1]	
Request Method: GET	
Request URI: /books/content?id=09AKZwEACAAJ&printsec=frontcover&img=1&zoom=1&source=google&bs_api=H HTTP/1.1	
Request Version: HTTP/1.1	
Host: books.google.com\r\n	
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0\r\n	
Accept: image/avif,image/webp,*/*\r\n	
Accept-Language: en-US,en;q=0.5\r\n	
Accept-Encoding: gzip, deflate\r\n	
DNT: 1\r\n	

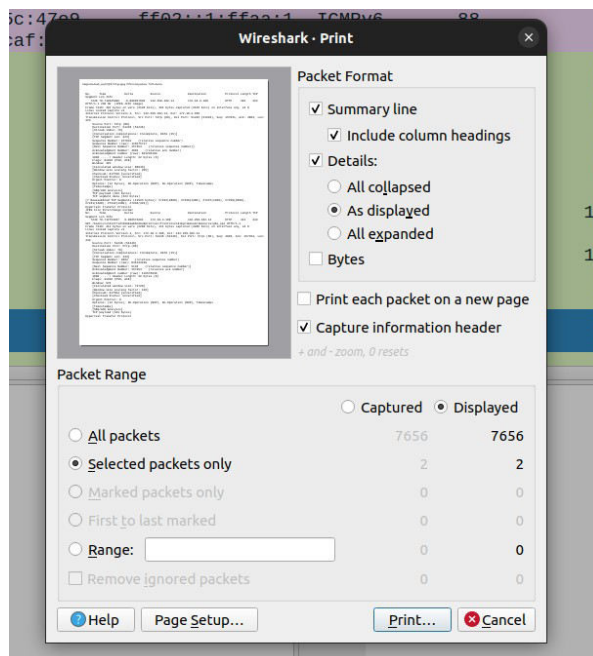
Q5.

Destination Port number is 80

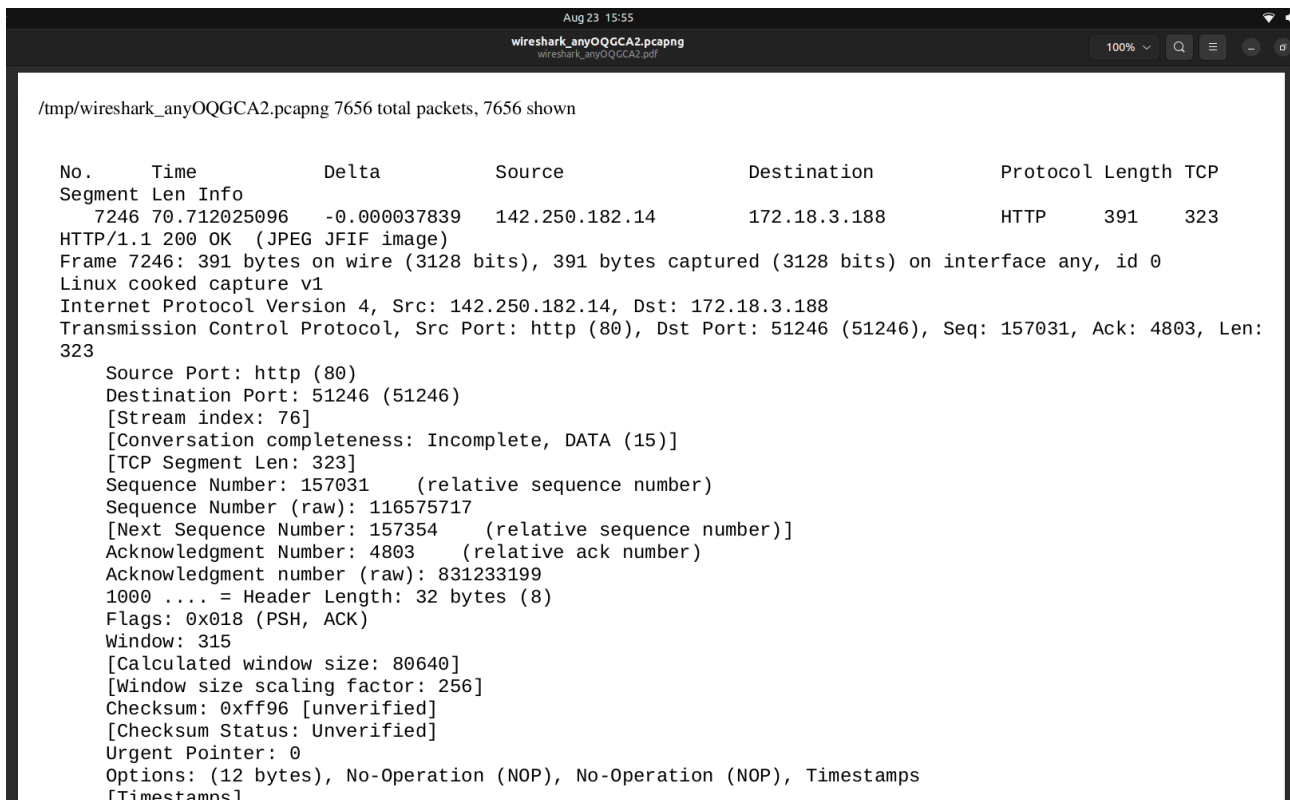
7296 70.967009028	0.000047444	172.18.3.188	142.250.182.14	HTTP	411	343 GET /books/content?id=8JCVEAAQBAJ&printsec=fr
7291 70.966858881	0.000028785	142.250.182.14	172.18.3.188	HTTP	1545	1477 HTTP/1.1 200 OK (JPEG JFIF image)
7263 70.719338982	0.000294956	172.18.3.188	142.250.182.14	HTTP	411	343 GET /books/content?id=LzhGzwEACAAJ&printsec=fr
7259 70.718719798	-0.000022833	142.250.182.14	172.18.3.188	HTTP	316	248 HTTP/1.1 200 OK (JPEG JFIF image)
7249 70.712753187	0.000572091	172.18.3.188	142.250.182.14	HTTP	411	343 GET /books/content?id=09AKzwEACAAJ&printsec=fr
7246 70.712025096	-0.000037839	142.250.182.14	172.18.3.188	HTTP	391	323 HTTP/1.1 200 OK (JPEG JFIF image)
7235 70.705056118	0.000453839	172.18.3.188	142.250.182.14	HTTP	411	343 GET /books/content?id=H1SXFAAA0RAJ&printsec=fr

<ul style="list-style-type: none"> Frame 7249: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on Linux cooked capture v1 Internet Protocol Version 4, Src: 172.18.3.188, Dst: 142.250.182.14 Transmission Control Protocol, Src Port: 51246 (51246), Dst Port: http (80), Source Port: 51246 (51246) Destination Port: http (80) [Stream index: 76] [Conversation completeness: Incomplete, DATA (15)] [TCP Segment Len: 343] Sequence Number: 4803 (relative sequence number) Sequence Number (raw): 831233199 [Next Sequence Number: 5146 (relative sequence number)] Acknowledgment Number: 157354 (relative ack number) 	<pre> 0000 00 04 00 01 00 06 34 c9 3d 19 fb ef 00 00 08 00 4..... 0010 45 00 01 8b 98 fb 40 00 40 06 ab 9a ac 12 03 bc E.....@..... 0020 8e fa b6 0e c8 2e 00 50 31 8b 9c af 06 f2 cf 28 P1..... 0030 80 18 02 40 f6 54 00 00 01 01 08 0a 8a d4 23 51 ...@T.....#Q 0040 dd c4 cb 68 47 45 54 20 2f 62 6f 6f 6b 73 2f 63 ...hGET /books/c 0050 6f 6e 74 65 6e 74 3f 69 64 3d 30 39 41 4b 7a 77 ontent?id=09AKzw 0060 45 41 43 41 41 4a 26 70 72 69 6e 74 73 65 63 3d EACAAJ&p rintsec= 0070 66 72 6f 6e 74 63 6f 76 65 72 26 69 6d 67 3d 31 frontcov er&img=1 0080 26 7a 6f 6f 6d 3d 31 26 73 6f 75 72 63 65 3d 67 &zoom=1& source=g 0090 62 73 5f 61 70 69 20 48 54 54 50 2f 31 2e 31 0d bs_api H TTP/1.1. 00a0 0a 48 6f 73 74 3a 20 62 6f 6f 6b 73 2e 67 6f 6f .Host: books.goo 00b0 67 6c 65 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 gle.com. User-Ag 00c0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Mozilla/5.0 </pre>
---	--

Q6.



Printed file snapshot: -



Q7.

In case of youtube: -

protocols - TCP, OCSP, MDNS, UDP, T:Sv1.2. ARP, NBNS, ICMPv6, DNS

Since the web site is already cached I am not able to capture any HTTP packets. When I am filtering for http, I can see only the OCSP packets which I think is related to the web site certificate.

The packet capture is not stopping. I think this is because the web site is dynamic of there are constant http request and responses for use cases like ads, video auto play etc

Destination IP address is – 142.250.195.69

In case of iith.ac.in: -

protocols - TCP, OCSP, T:Sv1.2. ARP, ICMPv6, DNS

Again, I am getting OCSP packets only as the web site is already cached: -

No.	Time	Delta	Source	Destination	Protocol	Length	TCP Segment Len	Info
360	10.019030027	0.000000000	172.18.3.188	104.95.97.33	OCSP	491		423 Request
376	10.340287890	0.321257863	104.95.97.33	172.18.3.188	OCSP	957		889 Response
758	10.794876030	0.454588140	172.18.3.188	142.250.182.99	OCSP	494		426 Request
759	10.795103361	0.000227331	172.18.3.188	142.250.182.99	OCSP	495		427 Request
762	10.800108486	0.005005125	172.18.3.188	142.250.182.99	OCSP	495		427 Request
769	10.866533505	0.066425019	142.250.182.99	172.18.3.188	OCSP	770		702 Response
774	10.872085804	0.005552299	142.250.182.99	172.18.3.188	OCSP	769		701 Response
776	10.874126954	0.002041150	142.250.182.99	172.18.3.188	OCSP	770		702 Response

In case of example.com :-

Protocols – DNS, ARP, UDP, MDNS, TLSv1.2, TCP

No.	Time	Delta	Source	Destination	Protocol	Length	TCP Segment Len	Info
549	5.005288140	0.000000000	172.18.3.188	93.184.216.34	HTTP	411		343 GET / HTTP/1.1
573	5.220715238	0.223427158	93.184.216.34	172.18.3.188	HTTP	1090		1022 HTTP/1.1 200 OK (text/html)
603	5.293813621	0.065098323	172.18.3.188	93.184.216.34	HTTP	362		294 GET /favicon.ico HTTP/1.1
665	5.543407830	0.249594209	93.184.216.34	172.18.3.188	HTTP	1081		1013 HTTP/1.1 404 Not Found (text/html)

We can see that we have received 404 no found in the final HTTP response.

In case of Washington.edu :-

protocols - TCP, OCSP, UDP, T:sv1.2. ARP, , ICMPv6, DNS

Here I got HTTP packets as I am opening this web site for the first time: -

No.	Time	Delta	Source	Destination	Protocol	Length	TCP Segment Len	Info
776	14.475589628	0.300110563	172.18.3.188	128.95.155.197	HTTP	349		281 GET / HTTP/1.1
873	15.141069197	0.665479569	128.95.155.197	172.18.3.188	HTTP	150		82 HTTP/1.1 200 OK (text/html)
1103	16.371668273	1.230599076	172.18.3.188	142.250.182.99	OCSP	494		426 Request
1122	16.419615571	0.047947298	172.18.3.188	142.250.182.99	OCSP	495		427 Request
1128	16.435220769	0.015605198	172.18.3.188	142.250.182.99	OCSP	495		427 Request
1129	16.436156898	0.000936129	142.250.182.99	172.18.3.188	OCSP	769		701 Response
1158	16.487159139	0.051002241	142.250.182.99	172.18.3.188	OCSP	770		702 Response
1216	16.522051330	0.034892191	142.250.182.99	172.18.3.188	OCSP	770		702 Response
1644	16.863942247	0.341890917	172.18.3.188	13.33.144.60	OCSP	501		433 Request
1649	16.890543550	0.026601303	13.33.144.60	172.18.3.188	OCSP	1011		943 Response
1658	16.892129506	0.001585956	172.18.3.188	13.33.144.60	OCSP	501		433 Request
1683	16.913096415	0.020966909	13.33.144.60	172.18.3.188	OCSP	1012		944 Response
3227	18.552576667	1.639480252	172.18.3.188	13.33.144.60	OCSP	501		433 Request
3245	18.576782232	0.024205565	13.33.144.60	172.18.3.188	OCSP	1012		944 Response
3252	18.577044627	0.000262395	172.18.3.188	13.33.144.60	OCSP	501		433 Request
3264	18.611755121	0.034710494	13.33.144.60	172.18.3.188	OCSP	1012		944 Response
3402	19.908306020	1.296631699	128.95.155.135	172.18.3.188	HTTP	255		187 HTTP/1.0 400 Bad request (text/html)
3437	20.906854276	0.998467456	128.95.155.198	172.18.3.188	HTTP	255		187 HTTP/1.0 400 Bad request (text/html)
3920	35.165376024	14.258521748	172.18.3.188	91.189.91.48	HTTP	155		87 GET / HTTP/1.1

The destination IP for the HTTP request is – 128.95.155.197

The total time it took to load the website completely is arounds 21 ms. I can see that the last HTTP request took 14 ms.

Q8.

In case of web sites like IIT-H and washington.edu the packet capture stopped after everything was loaded in the browser. I

n case of Youtube the packet capture was not getting terminated because the web site was dynamic and there were constant HTTP requests being sent from the browser.

In case of example.com there was 404 not found response because this is not a valid domain name. Also, we can see that there is a GET request made to favicon.ico and this could be related to the message that I am seeing on the browser which is as follows: -

