

Task 1.1 How many DNS queries are sent from your browser (host machine) to DNS Server(s)?

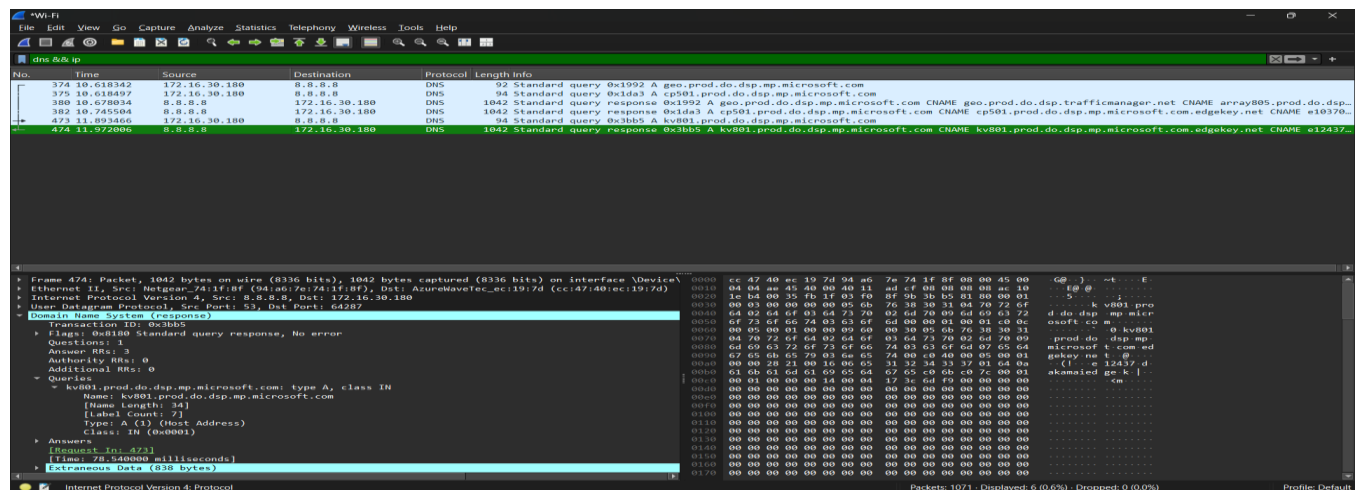
DNS/Query-Response:

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst
--------------	-------	---------	---------	---------	-----------	---------	-------

Total	27	0.0003	100%	0.0300	13.444		
-------	----	--------	------	--------	--------	--	--

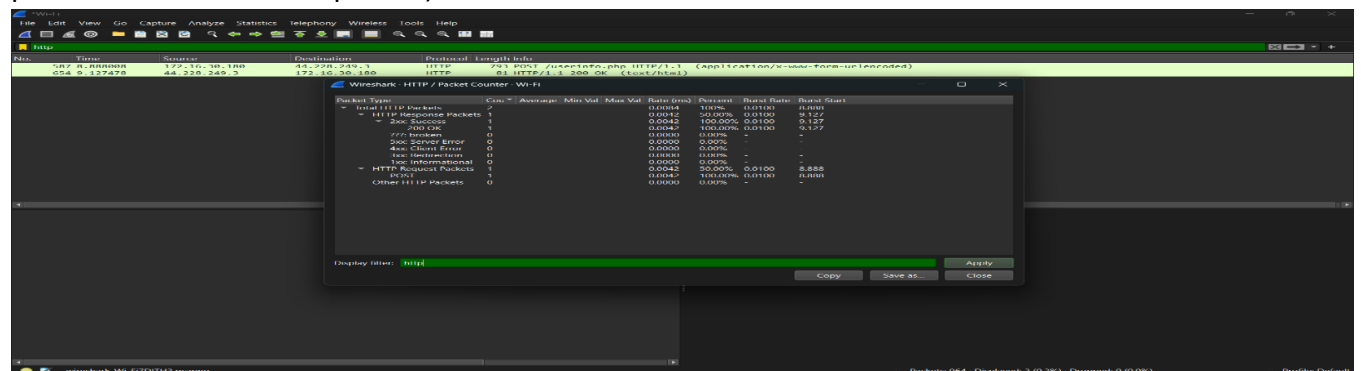
1.2 How many DNS servers are involved ?

Ans:3



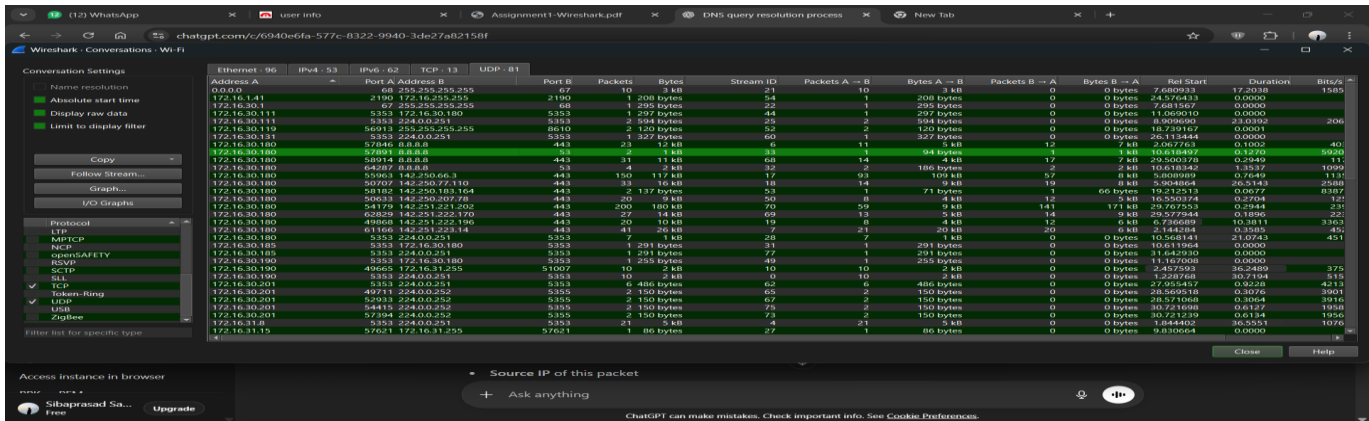
1.3 NO

2.1 How many HTTP requests (Type and respective count of requests), responses(status and phrase of each of the responses) did the browser send and receive ?



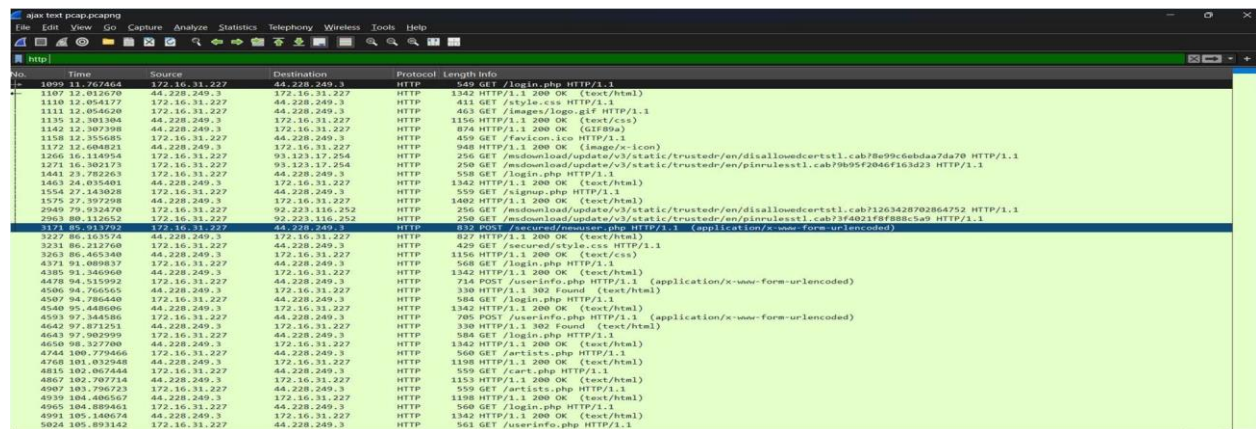
3 and 4) How many TCP Connections has the browser established overall ?

4) What is the time taken to establish TCP connection(s)? List the time taken value for each of the TCP connection(s).



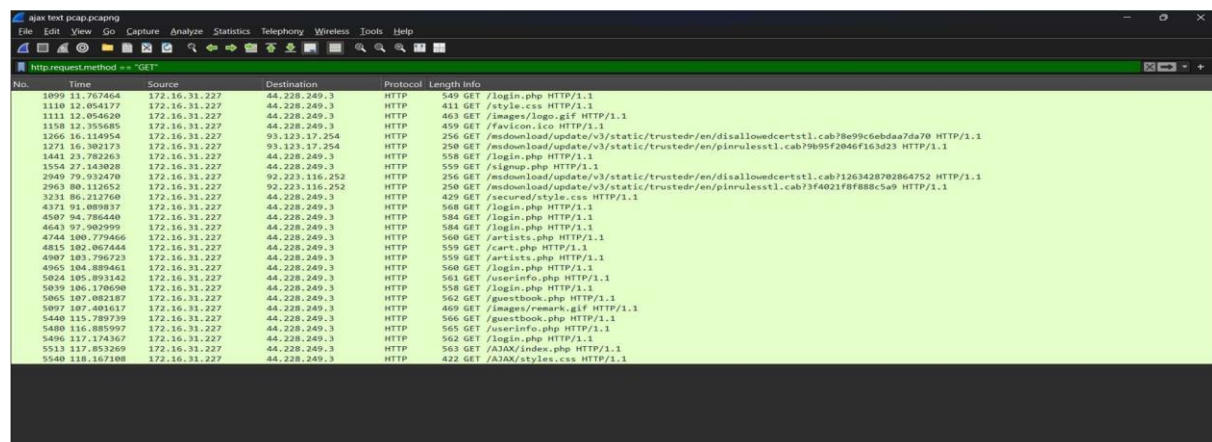
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel. Start	Duration	Bits/s
172.16.1.41	2190	172.16.255.255	2190	67	10 KB	21	10	3 KB	0	0 bytes	7.689933	17.2038	1585
172.16.30.1	67	255.255.255.255	67	1	208 bytes	54	1	208 bytes	0	0 bytes	24.576433	0.0000	—
172.16.30.111	5353	172.16.30.180	5353	1	297 bytes	44	1	297 bytes	0	0 bytes	11.069010	0.0000	—
172.16.30.110	56911	255.255.255.255	8610	2	120 bytes	52	2	120 bytes	0	0 bytes	18.739167	0.0001	206
172.16.30.131	5353	224.0.0.251	5353	1	327 bytes	66	1	327 bytes	0	0 bytes	24.115444	0.0003	—
172.16.30.180	57446	8.8.8.8	443	23	12 KB	8	11	5 KB	12	7 KB	2.067763	0.1002	40
172.16.30.180	57446	8.8.8.8	443	2	1 KB	31	1	94 bytes	1	3 KB	10.618467	0.3270	1000
172.16.30.180	58914	8.8.8.8	443	31	11 KB	68	14	4 KB	12	7 KB	20.500378	0.2949	111
172.16.30.180	56707	142.250.77.110	443	31	10 KB	16	14	9 KB	19	8 KB	5.908464	20.5143	2500
172.16.30.180	58182	142.250.183.164	443	2	137 bytes	53	1	71 bytes	1	66 bytes	19.212513	0.0677	6307
172.16.30.180	56003	142.250.207.76	443	20	10 KB	50	8	4 KB	12	5 KB	16.500374	0.2704	121
172.16.30.180	54179	142.251.221.202	443	200	100 KB	70	59	9 KB	141	171 KB	29.707553	0.2144	231
172.16.30.180	62828	142.251.222.170	443	27	14 KB	69	13	5 KB	14	9 KB	29.277944	0.1896	42
172.16.30.180	49866	142.251.222.196	443	20	10 KB	19	8	4 KB	12	6 KB	6.736689	10.3811	3303
172.16.30.180	61566	142.251.222.14	443	41	20 KB	7	21	20 KB	20	8 KB	2.144284	0.3585	45
172.16.30.180	5353	224.0.0.251	5353	7	1 KB	28	7	1 KB	0	0 bytes	10.568141	21.0743	451
172.16.30.180	5353	172.16.30.180	5353	41	291 bytes	31	1	291 bytes	0	0 bytes	11.618064	0.0000	—
172.16.30.185	5353	224.0.0.251	5353	1	291 bytes	77	1	291 bytes	0	0 bytes	31.642030	0.0000	—
172.16.30.190	40665	172.16.31.255	51007	10	2 KB	10	10	2 KB	0	0 bytes	2.857593	36.2489	372
172.16.30.201	5353	224.0.0.251	5353	9	4 KB	10	2	4 KB	0	0 bytes	3.587460	30.7194	915
172.16.30.201	49711	224.0.0.252	5355	2	150 bytes	65	2	150 bytes	0	0 bytes	27.051457	0.3228	4211
172.16.30.201	54415	224.0.0.252	5355	2	150 bytes	67	2	150 bytes	0	0 bytes	26.569516	0.3076	3901
172.16.30.201	57394	224.0.0.252	5355	2	150 bytes	75	2	150 bytes	0	0 bytes	30.721698	0.6127	3916
172.16.31.8	5353	224.0.0.251	5353	21	5 KB	4	21	5 KB	0	0 bytes	30.721239	0.5114	1856
172.16.31.15	57621	172.16.31.255	57621	1	80 bytes	27	1	80 bytes	0	0 bytes	9.830664	36.5551	1076

5) Browse the website by moving to various sub links, embedded objects listed in the site.



No.	Time	Source	Destination	Protocol	Length	Info
1099	11.767464	172.16.31.227	44.228.249.3	HTTP	549	GET /login.php HTTP/1.1
1107	12.054177	172.16.31.227	44.228.249.3	HTTP	1342	HTTP/1.1 200 OK (text/html)
1110	12.054177	172.16.31.227	44.228.249.3	HTTP	411	GET /style.css HTTP/1.1
1111	12.054620	172.16.31.227	44.228.249.3	HTTP	403	GET /images/logo.gif HTTP/1.1
1130	12.355685	172.16.31.227	44.228.249.3	HTTP	1156	HTTP/1.1 200 OK (text/css)
1132	12.355685	44.228.249.3	172.16.31.227	HTTP	874	HTTP/1.1 200 OK (text/html)
1134	12.355685	44.228.249.3	172.16.31.227	HTTP	458	GET /favicon.ico HTTP/1.1
1172	12.604821	44.228.249.3	172.16.31.227	HTTP	948	HTTP/1.1 200 OK (image/x-icon)
1206	16.14054	172.16.31.227	93.123.17.254	HTTP	256	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?9b95f2046f163d23 HTTP/1.1
1271	16.302173	172.16.31.227	93.123.17.254	HTTP	256	GET /login.php HTTP/1.1
1441	23.782263	172.16.31.227	44.228.249.3	HTTP	558	GET /login.php HTTP/1.1
1463	24.035481	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
1554	27.143028	172.16.31.227	44.228.249.3	HTTP	559	GET /ajax.php HTTP/1.1
1575	27.397098	44.228.249.3	172.16.31.227	HTTP	1402	HTTP/1.1 200 OK (text/html)
1949	79.932478	172.16.31.227	92.223.116.252	HTTP	256	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?1263428702864752 HTTP/1.1
2963	80.112652	172.16.31.227	92.223.116.252	HTTP	256	GET /msdownload/update/v3/static/trusted/en/pirulesstl.cab?3640218f8885c9 HTTP/1.1
3171	85.931792	172.16.31.227	44.228.249.3	HTTP	832	POST /secured/userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
3221	86.212760	172.16.31.227	44.228.249.3	HTTP	429	GET /secured/style.css HTTP/1.1
3231	86.212760	172.16.31.227	44.228.249.3	HTTP	429	GET /secured/style.css HTTP/1.1
3261	86.465348	44.228.249.3	172.16.31.227	HTTP	1156	HTTP/1.1 200 OK (text/css)
3371	91.089837	172.16.31.227	44.228.249.3	HTTP	568	GET /login.php HTTP/1.1
3385	91.346968	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
4470	94.315992	172.16.31.227	44.228.249.3	HTTP	714	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
4506	94.766565	44.228.249.3	172.16.31.227	HTTP	330	HTTP/1.1 302 Found (text/html)
4507	94.766440	172.16.31.227	44.228.249.3	HTTP	584	GET /login.php HTTP/1.1
4540	95.448606	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
4593	97.348806	172.16.31.227	44.228.249.3	HTTP	795	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
4642	97.873251	44.228.249.3	172.16.31.227	HTTP	330	HTTP/1.1 302 Found (text/html)
4643	97.982999	172.16.31.227	44.228.249.3	HTTP	584	GET /login.php HTTP/1.1
4650	98.127700	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
4744	100.779466	172.16.31.227	44.228.249.3	HTTP	560	GET /artists.php HTTP/1.1
4761	101.032548	44.228.249.3	172.16.31.227	HTTP	1198	HTTP/1.1 200 OK (text/html)
4815	102.067444	172.16.31.227	44.228.249.3	HTTP	559	GET /cart.php HTTP/1.1
4867	102.707714	172.16.31.227	44.228.249.3	HTTP	1153	HTTP/1.1 200 OK (text/html)
4907	103.796723	172.16.31.227	44.228.249.3	HTTP	559	GET /artists.php HTTP/1.1
4939	104.486567	44.228.249.3	172.16.31.227	HTTP	1198	HTTP/1.1 200 OK (text/html)
4963	104.889461	172.16.31.227	44.228.249.3	HTTP	560	GET /login.php HTTP/1.1
4991	105.140674	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
5024	105.893142	172.16.31.227	44.228.249.3	HTTP	561	GET /userinfo.php HTTP/1.1

6) How many objects/files are downloaded?



No.	Time	Source	Destination	Protocol	Length	Info
1099	11.767464	172.16.31.227	44.228.249.3	HTTP	549	GET /login.php HTTP/1.1
1110	12.054177	172.16.31.227	44.228.249.3	HTTP	411	GET /style.css HTTP/1.1
1111	12.054620	172.16.31.227	44.228.249.3	HTTP	403	GET /images/logo.gif HTTP/1.1
1130	12.355685	172.16.31.227	44.228.249.3	HTTP	1156	HTTP/1.1 200 OK (text/css)
1132	12.355685	44.228.249.3	172.16.31.227	HTTP	874	HTTP/1.1 200 OK (text/html)
1134	12.355685	44.228.249.3	172.16.31.227	HTTP	458	GET /favicon.ico HTTP/1.1
1206	16.14054	172.16.31.227	93.123.17.254	HTTP	256	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?9b95f2046f163d23 HTTP/1.1
1271	16.302173	172.16.31.227	93.123.17.254	HTTP	256	GET /login.php HTTP/1.1
1441	23.782263	172.16.31.227	44.228.249.3	HTTP	558	GET /login.php HTTP/1.1
1463	24.035481	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
1554	27.143028	172.16.31.227	44.228.249.3	HTTP	559	GET /ajax.php HTTP/1.1
1575	27.397098	44.228.249.3	172.16.31.227	HTTP	1402	HTTP/1.1 200 OK (text/html)
1949	79.932478	172.16.31.227	92.223.116.252	HTTP	256	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?1263428702864752 HTTP/1.1
2963	80.112652	172.16.31.227	92.223.116.252	HTTP	256	GET /msdownload/update/v3/static/trusted/en/pirulesstl.cab?3640218f8885c9 HTTP/1.1
3171	85.931792	172.16.31.227	44.228.249.3	HTTP	429	GET /secured/style.css HTTP/1.1
3221	86.212760	172.16.31.227	44.228.249.3	HTTP	429	GET /secured/style.css HTTP/1.1
3261	86.465348	44.228.249.3	172.16.31.227	HTTP	1156	HTTP/1.1 200 OK (text/css)
3371	91.089837	172.16.31.227	44.228.249.3	HTTP	568	GET /login.php HTTP/1.1
3385	91.346968	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
4470	94.315992	172.16.31.227	44.228.249.3	HTTP	714	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
4506	94.766565	44.228.249.3	172.16.31.227	HTTP	330	HTTP/1.1 302 Found (text/html)
4507	94.766440	172.16.31.227	44.228.249.3	HTTP	584	GET /login.php HTTP/1.1
4540	95.448606	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
4593	97.348806	172.16.31.227	44.228.249.3	HTTP	795	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
4642	97.873251	44.228.249.3	172.16.31.227	HTTP	330	HTTP/1.1 302 Found (text/html)
4643	97.982999	172.16.31.227	44.228.249.3	HTTP	584	GET /login.php HTTP/1.1
4650	98.127700	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
4744	100.779466	172.16.31.227	44.228.249.3	HTTP	560	GET /artists.php HTTP/1.1
4761	101.032548	44.228.249.3	172.16.31.227	HTTP	1198	HTTP/1.1 200 OK (text/html)
4815	102.067444	172.16.31.227	44.228.249.3	HTTP	559	GET /cart.php HTTP/1.1
4867	102.707714	172.16.31.227	44.228.249.3	HTTP	1153	HTTP/1.1 200 OK (text/html)
4907	103.796723	172.16.31.227	44.228.249.3	HTTP	559	GET /artists.php HTTP/1.1
4939	104.486567	44.228.249.3	172.16.31.227	HTTP	1198	HTTP/1.1 200 OK (text/html)
4963	104.889461	172.16.31.227	44.228.249.3	HTTP	560	GET /login.php HTTP/1.1
4991	105.140674	44.228.249.3	172.16.31.227	HTTP	1342	HTTP/1.1 200 OK (text/html)
5024	105.893142	172.16.31.227	44.228.249.3	HTTP	561	GET /userinfo.php HTTP/1.1
5039	106.170690	172.16.31.227	44.228.249.3	HTTP	558	GET /login.php HTTP/1.1
5065	107.082187	172.16.31.227	44.228.249.3	HTTP	562	GET /guestbook.php HTTP/1.1
4907	107.481617	172.16.31.227	44.228.249.3	HTTP	409	GET /images/remark.gif HTTP/1.1
5440	115.789739	172.16.31.227	44.228.249.3	HTTP	566	GET /guestbook.php HTTP/1.1
5480	116.885997	172.16.31.227	44.228.249.3	HTTP	565	GET /userinfo.php HTTP/1.1
5496	117.174167	172.16.31.227	44.228.249.3	HTTP	562	GET /login.php HTTP/1.1
5513	117.853269	172.16.31.227	44.228.249.3	HTTP	563	GET /AJAX/index.php HTTP/1.1
5540	118.167108	172.16.31.227	44.228.249.3	HTTP	432	GET /AJAX/styles.css HTTP/1.1

7) Make a detailed list including for each object/file downloaded what is the time taken for downloading the objects, the size of the object downloaded, object name, last modified time at the server.

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
172.16.31.227	57962	44.228.249.3	80	2	960 bytes	19	20	10.00%	2	960 bytes	0	0 bytes	8.499940	7
172.16.31.227	63844	44.228.249.3	80	21	11 kB	20	124	16.94%	21	11 kB	0	0 bytes	8.737862	10
172.16.31.227	52709	92.223.116.252	80	1	256 bytes	45	5	20.00%	1	256 bytes	0	0 bytes	79.761036	1
172.16.31.227	52710	92.223.116.252	80	1	250 bytes	46	5	20.00%	1	250 bytes	0	0 bytes	79.953368	1
172.16.31.227	55232	93.123.17.254	80	1	256 bytes	32	5	20.00%	1	256 bytes	0	0 bytes	15.944550	1
172.16.31.227	55233	93.123.17.254	80	1	250 bytes	33	5	20.00%	1	250 bytes	0	0 bytes	16.135342	1

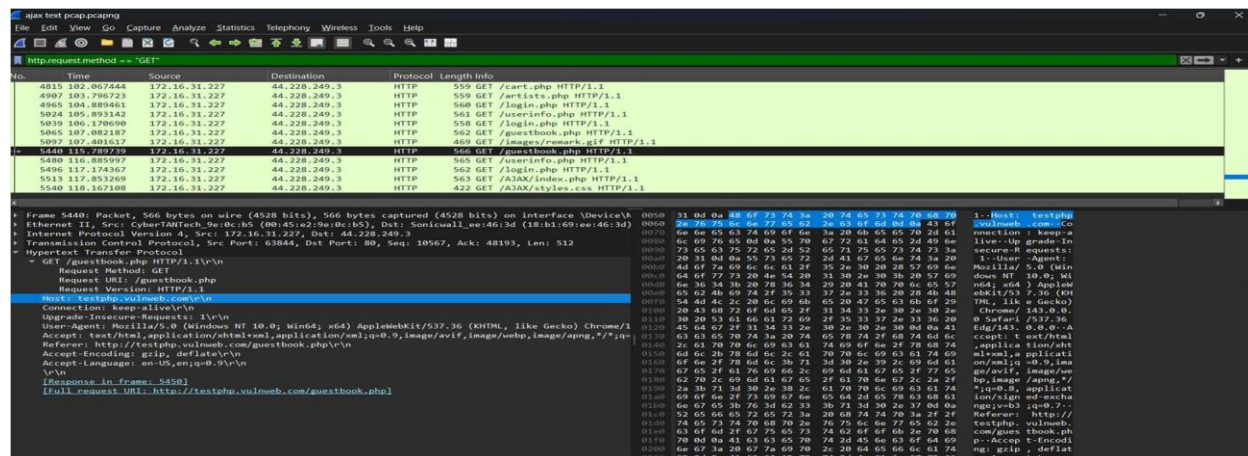
8) How many other websites are visited from this site, by clicking on to various possible links which take you to the other sites (other than <http://goidirectory.nic.in/>)

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
172.16.30.100	1234	44.228.249.3	80	5	4 kB	4	13	38.46%	3	1 kB	2	3 kB	2.933483	6
172.16.30.100	21620	44.228.249.3	80	4	4 kB	9	14	28.57%	2	1 kB	2	3 kB	12.021180	12
172.16.30.100	28706	44.228.249.3	80	1	4 kB	6	14	28.57%	2	1 kB	2	3 kB	8.503481	7
172.16.30.100	40771	44.228.249.3	80	6	4 kB	10	19	31.58%	3	2 kB	3	2 kB	16.873094	6
172.16.30.100	40770	44.228.249.3	80	4	4 kB	12	14	30.77%	2	1 kB	2	3 kB	24.981161	2
172.16.30.100	61162	44.228.249.3	80	5	4 kB	3	13	26.46%	3	1 kB	2	3 kB	2.909552	9

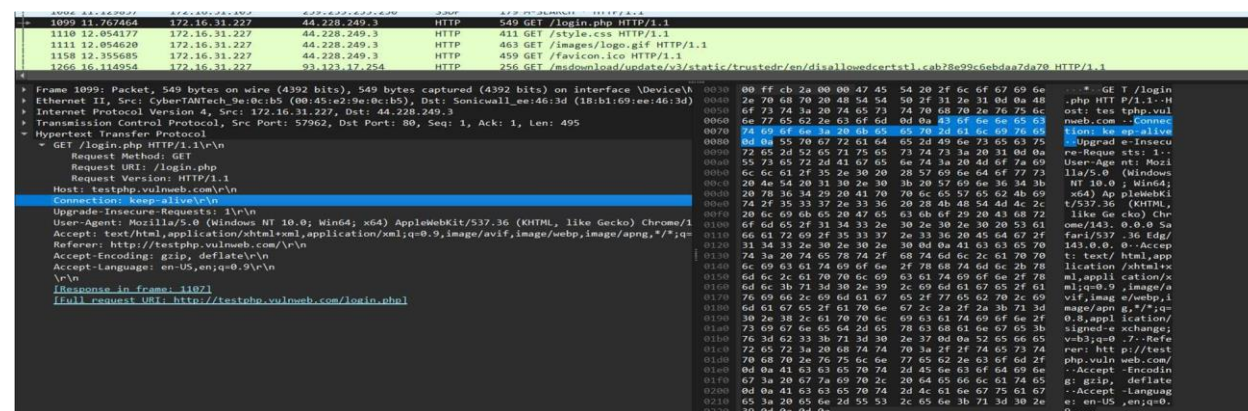
HTTP Request (HTTP-Version: 1.0) 0 bytes

Packets: 695 - Displayed: 20 (4.0%) - Drropped: 0 (0.0%)

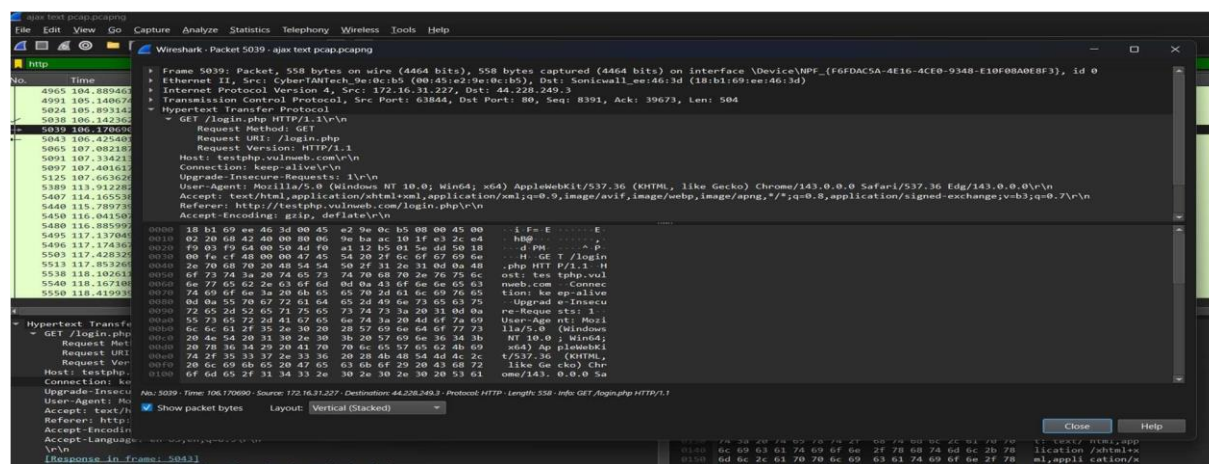
9) When `http://goidirectory.nic.in/` is entered, is there any embedded object shown/downloaded from different site(s) (other than `http://goidirectory.nic.in/`) ?



10) How many times does the browser ask the site to keep the connection alive?



11) Which version of the HTTP is your browser running ?



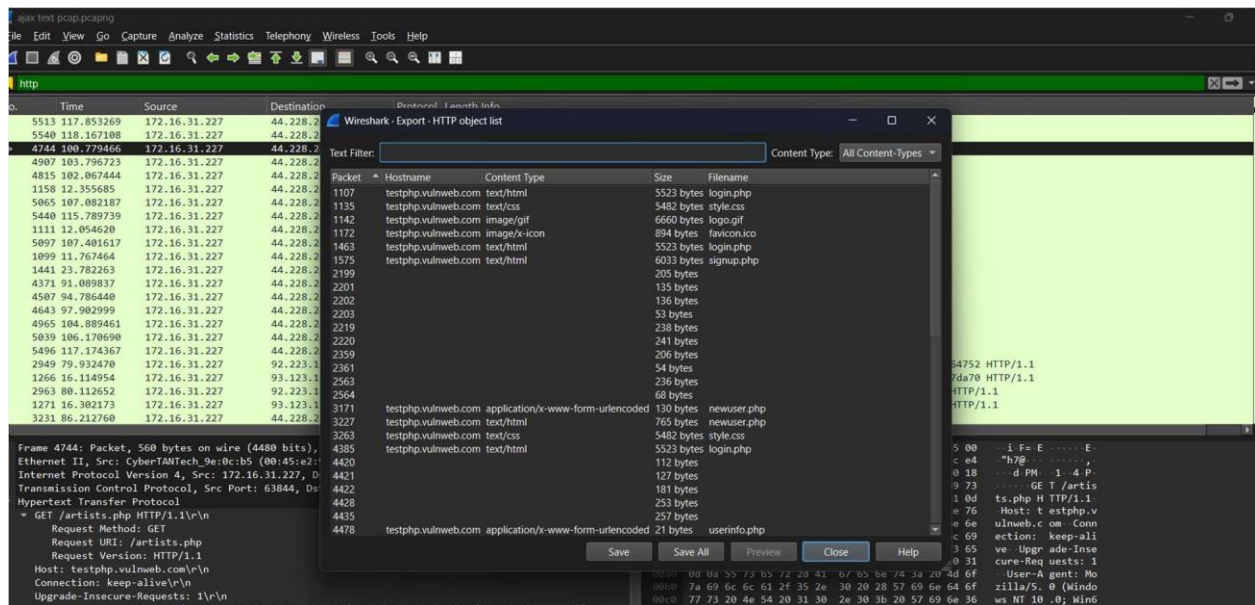
TASK 2

1) How many conditional GETs are sent by browser to the server?

The screenshot shows a Wireshark packet capture of an HTTP session. The top pane displays a list of packets, with packet 5440 selected. The middle pane shows the details of this packet, which is an HTTP GET request for /guestbook.php. The bottom pane shows the raw packet data in hexadecimal and ASCII. The request includes headers such as Host: testphp.vulnweb.com, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36, and Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8. The request is a conditional GET, as indicated by the 'If-None-Match' header.

2) Make a list for each of the file/object downloaded, how many times the server sends the full contents of the respective file/object?

The screenshot shows a Wireshark packet capture of an HTTP session. The top pane displays a list of packets, with packet 1142 selected. The middle pane shows the details of this packet, which is an HTTP 200 OK response for /guestbook.php. The bottom pane shows the raw packet data in hexadecimal and ASCII. The response includes headers such as Server: nginx/1.19.0, Date: Tue, 16 Dec 2025 04:09:46 GMT, and Content-Type: image/gif. The response is a full content response, as indicated by the 'Content-Length' header.



3) Explain in detail what is the difference in server's behaviour between first and second request/browsing ?

4) List the headers of HTTP which influence this functionality.

First Request (Cold Cache)

- **Browser:**
Sends a normal **HTTP GET** request because it does not have a cached copy of the file.
- **Server:**
Responds with **HTTP 200 OK** and sends the **entire file payload**.
The response includes caching metadata such as:
 - **Last-Modified** (timestamp of last change)
 - **ETag** (unique identifier for the file version)

2. Second Request (Warm Cache)

- **Browser:**
Detects that a cached copy of the file exists and sends a **Conditional GET** request.
It includes validation headers such as:
 - **If-Modified-Since** (based on Last-Modified)
 - **If-None-Match** (based on ETag)
- **Server:**
Compares the conditional headers with the current file state:
 - **If unchanged:**
Responds with **HTTP 304 Not Modified** and sends **no file data**, saving bandwidth.
 - **If modified:**
Responds with **HTTP 200 OK** and sends the **updated file**.

3. Request Headers (Sent by Browser)

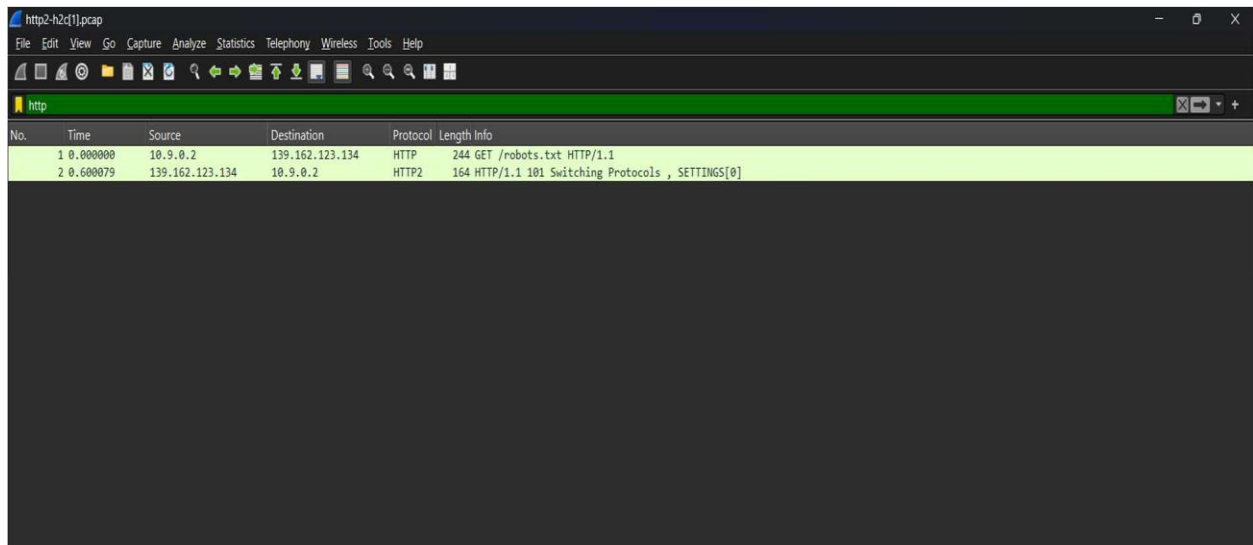
- **If-Modified-Since:** Date of the cached file version.
- **If-None-Match:** ETag value of the cached version.
- **Cache-Control:** (e.g., max-age=0 forces revalidation).

4. Response Headers (Sent by Server)

- **Last-Modified:** Last modification time of the file.
- **ETag:** Unique identifier for the file version.
- **Expires:** Time after which the cached copy becomes stale.

TASK 3

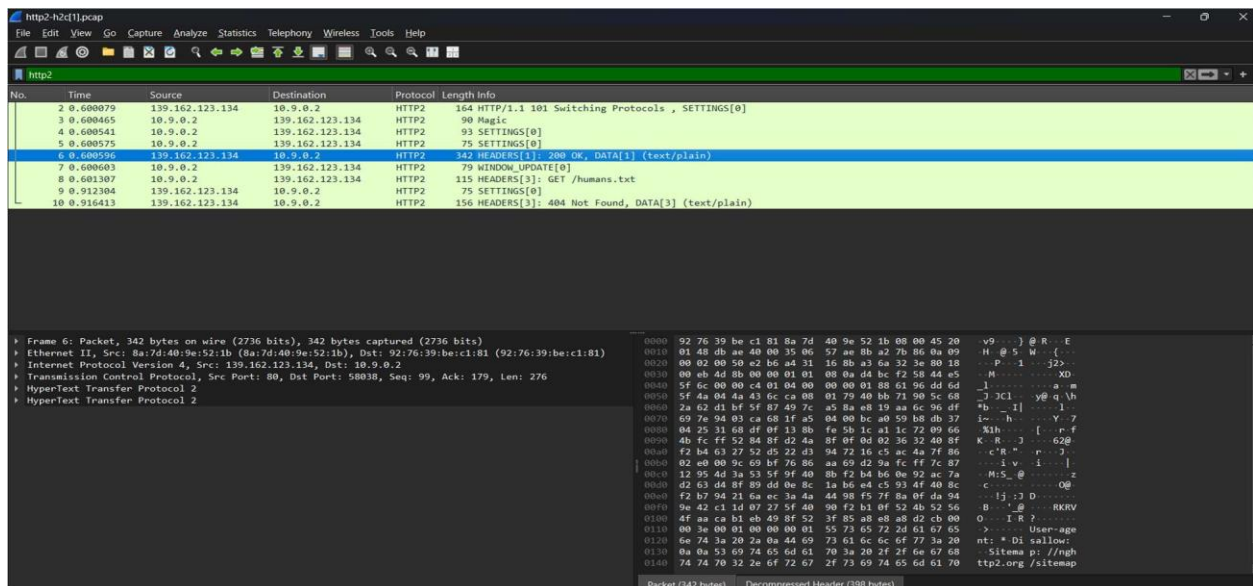
1) How many HTTP/2 and HTTP/1.1 packets are present?



The screenshot shows a Wireshark packet capture window titled 'http2-h2c[1].pcap'. The packet list pane shows two packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.9.0.2	139.162.123.134	HTTP	244	GET /robots.txt HTTP/1.1
2	0.600079	139.162.123.134	10.9.0.2	HTTP2	164	HTTP/1.1 101 Switching Protocols , SETTINGS[0]

2) How many HTTP/2 packets are exchanged between client and server here before the first object is fetched?



The screenshot shows a Wireshark packet capture window titled 'http2-h2c[1].pcap'. The packet list pane shows the first 10 packets:

No.	Time	Source	Destination	Protocol	Length	Info
2	0.600079	139.162.123.134	10.9.0.2	HTTP2	164	HTTP/1.1 101 Switching Protocols , SETTINGS[0]
3	0.600465	10.9.0.2	139.162.123.134	HTTP2	90	Magic
4	0.600541	10.9.0.2	139.162.123.134	HTTP2	93	SETTINGS[0]
5	0.600575	10.9.0.2	139.162.123.134	HTTP2	75	SETTINGS[0]
6	0.600295	139.162.123.134	10.9.0.2	HTTP2	122	HTTP2 SETTINGS OK, DATA[1] (text/plain)
7	0.600603	10.9.0.2	139.162.123.134	HTTP2	79	WINDOW_UPDATE[0]
8	0.601307	10.9.0.2	139.162.123.134	HTTP2	115	HEADERS[3]: GET /humans.txt
9	0.912304	139.162.123.134	10.9.0.2	HTTP2	75	SETTINGS[0]
10	0.916413	139.162.123.134	10.9.0.2	HTTP2	156	HEADERS[3]: 404 Not Found, DATA[3] (text/plain)

The packet details pane for packet 6 shows:

- Frame 6: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bytes)
- Ethernet II, Src: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b), Dst: 92:76:39:be:c1:81 (92:76:39:be:c1:81)
- Internet Protocol Version 4, Src: 139.162.123.134, Dst: 10.9.0.2
- Transmission Control Protocol, Src Port: 80, Dst Port: 58038, Seq: 99, Ack: 179, Len: 276
- HyperText Transfer Protocol 2
- HyperText Transfer Protocol 2

The packet bytes pane shows the raw data of the packet, including the decompressed header (398 bytes).

2) What main difference do you observe in headers of HTTP/2 packets displayed here, compared to the headers of HTTP/1.1 packets ?

