

Task 1:

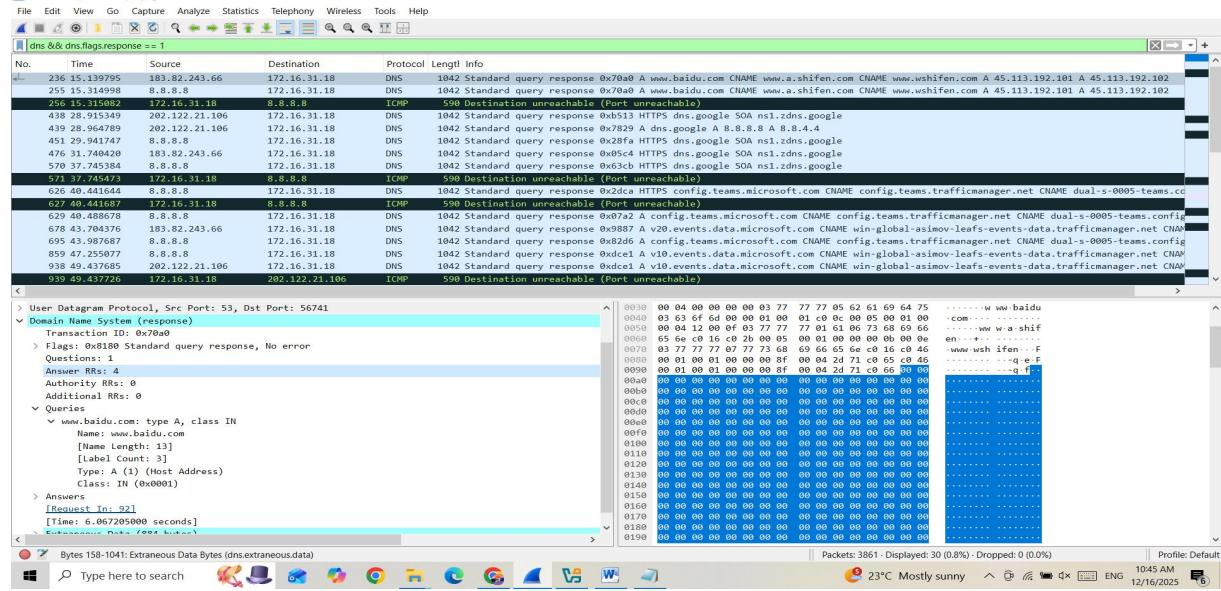
1.1 How many DNS queries are sent from your browser (host machine) to DNS Server(s) ? >DNS/Query-Response:

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate
<hr/>							
Total	104		0.0005	100%	0.0600	66.160	

1.2. How many DNS servers are involved ?

Filter: dns && ip.src == 172.16.31.18 && dns.flags.response == 1

Ans=4



1.3. Which DNS Server replies with actual IP Address(es). Do all DNS servers respond ?

→ no

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

Packet Type	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	178				0.0009	100%	0.0500	89.061
HTTP Request Packets	131				0.0006	73.60%	0.0500	89.061
SEARCH	58				0.0003	44.27%	0.0200	31.159
NOTIFY	46				0.0002	35.11%	0.0400	66.082
GET	17				0.0001	12.98%	0.0100	14.859
POST	10				0.0000	7.63%	0.0100	14.600
HTTP Response Packets	46				0.0002	25.84%	0.0300	155.871
2xx: Success	45				0.0002	97.83%	0.0300	155.871
200 OK	45				0.0002	100.00%	0.0300	155.871
3xx: Redirection	1				0.0000	2.17%	0.0100	14.854
302 Found	1				0.0000	100.00%	0.0100	14.854
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
Other HTTP Packets	1				0.0000	0.56%	0.0100	50.189

Display filter: Apply

Copy Save as... Close

3. How many TCP Connections has the browser established overall ?

Filter: `tcp.flags.syn == 1 && tcp.flags.ack == 0 && ip.src == 172.16.31.18`

Conversation Settings	Ethernet - 1	IPv4 - 14	IPv6	TCP - 40	UDP											
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	Bits/s A → B	Bits/s B → A
172.16.31.18	58745	8.8.8.8	53	1	66 bytes	37	9	11.11%	1	66 bytes	0	0 bytes	66.165981	0.0912	5787 bits/s	0 bits/s
172.16.31.18	58760	13.107.139.11	443	1	66 bytes	57	33	3.03%	1	66 bytes	0	0 bytes	167.497245	0.9253	570 bits/s	0 bits/s
172.16.31.18	57560	44.228.249.3	443	1	66 bytes	5	2	50.00%	1	66 bytes	0	0 bytes	7.293329	30.4521	17 bits/s	0 bits/s
172.16.31.18	57574	44.228.249.3	80	1	66 bytes	32	9	11.11%	1	66 bytes	0	0 bytes	61.832188	72.7122	7 bits/s	0 bits/s
172.16.31.18	57575	44.228.249.3	80	1	66 bytes	33	14	7.14%	1	66 bytes	0	0 bytes	61.832660	72.7116	7 bits/s	0 bits/s
172.16.31.18	57576	44.228.249.3	80	1	66 bytes	34	9	11.11%	1	66 bytes	0	0 bytes	62.064369	72.4801	7 bits/s	0 bits/s
172.16.31.18	58752	44.228.249.3	80	1	66 bytes	46	9	11.11%	1	66 bytes	0	0 bytes	134.308814	61.8103	8 bits/s	0 bits/s
172.16.31.18	58753	44.228.249.3	80	1	66 bytes	47	78	1.28%	1	66 bytes	0	0 bytes	134.309046	80.4810	6 bits/s	0 bits/s
172.16.31.18	58764	44.228.249.3	80	1	66 bytes	61	3	33.33%	1	66 bytes	0	0 bytes	196.113934	0.2386	2229 bits/s	0 bits/s
172.16.31.18	57563	45.113.192.101	80	1	66 bytes	12	3	33.33%	1	66 bytes	0	0 bytes	15.141148	0.0589	8965 bits/s	0 bits/s
172.16.31.18	57564	45.113.192.101	80	1	66 bytes	13	10	10.00%	1	66 bytes	0	0 bytes	15.142232	18.9834	27 bits/s	0 bits/s
172.16.31.18	57565	45.113.192.101	80	1	66 bytes	15	10	10.00%	1	66 bytes	0	0 bytes	25.200184	19.0044	27 bits/s	0 bits/s
172.16.31.18	57567	45.113.192.101	80	1	66 bytes	20	10	10.00%	1	66 bytes	0	0 bytes	35.268874	19.0017	27 bits/s	0 bits/s
172.16.31.18	57570	45.113.192.101	80	1	66 bytes	27	10	10.00%	1	66 bytes	0	0 bytes	45.358859	19.0295	27 bits/s	0 bits/s
172.16.31.18	57572	45.113.192.101	80	1	66 bytes	29	10	10.00%	1	66 bytes	0	0 bytes	55.435818	19.0113	27 bits/s	0 bits/s
172.16.31.18	57578	45.113.192.101	80	1	66 bytes	36	10	10.00%	1	66 bytes	0	0 bytes	65.505161	21.5798	24 bits/s	0 bits/s
172.16.31.18	58766	45.113.192.101	80	1	66 bytes	63	8	12.50%	1	66 bytes	0	0 bytes	214.623888	4.5733	115 bits/s	0 bits/s
172.16.31.18	58746	45.113.192.102	80	1	66 bytes	39	10	10.00%	1	66 bytes	0	0 bytes	79.905902	18.9848	27 bits/s	0 bits/s
172.16.31.18	58746	45.113.192.102	80	1	66 bytes	40	10	10.00%	1	66 bytes	0	0 bytes	89.957158	26.1856	20 bits/s	0 bits/s
172.16.31.18	58748	45.113.192.102	80	1	66 bytes	41	10	10.00%	1	66 bytes	0	0 bytes	100.128416	19.0135	27 bits/s	0 bits/s
172.16.31.18	58749	45.113.192.102	80	1	66 bytes	42	10	10.00%	1	66 bytes	0	0 bytes	110.193923	18.9774	27 bits/s	0 bits/s
172.16.31.18	58750	45.113.192.102	80	1	66 bytes	43	10	10.00%	1	66 bytes	0	0 bytes	120.238714	18.9910	27 bits/s	0 bits/s
172.16.31.18	58751	45.113.192.102	80	1	66 bytes	45	10	10.00%	1	66 bytes	0	0 bytes	130.270871	19.0182	27 bits/s	0 bits/s
172.16.31.18	58757	45.113.192.102	80	1	66 bytes	51	3	33.33%	1	66 bytes	0	0 bytes	150.758256	0.0619	8523 bits/s	0 bits/s
172.16.31.18	58758	45.113.192.102	80	1	66 bytes	52	10	10.00%	1	66 bytes	0	0 bytes	150.758888	19.0096	27 bits/s	0 bits/s
172.16.31.18	58759	45.113.192.102	80	2	132 bytes	55	11	18.18%	2	132 bytes	0	0 bytes	160.812700	20.1254	52 bits/s	0 bits/s
172.16.31.18	58761	45.113.192.102	80	1	66 bytes	59	10	10.00%	1	66 bytes	0	0 bytes	172.025126	19.0005	27 bits/s	0 bits/s

Protocol: Bluetooth BPv7 DCCP DNP 3.0 Ethernet FC FDDI IEEE 802.11 IEEE 802.15.4 ILNP

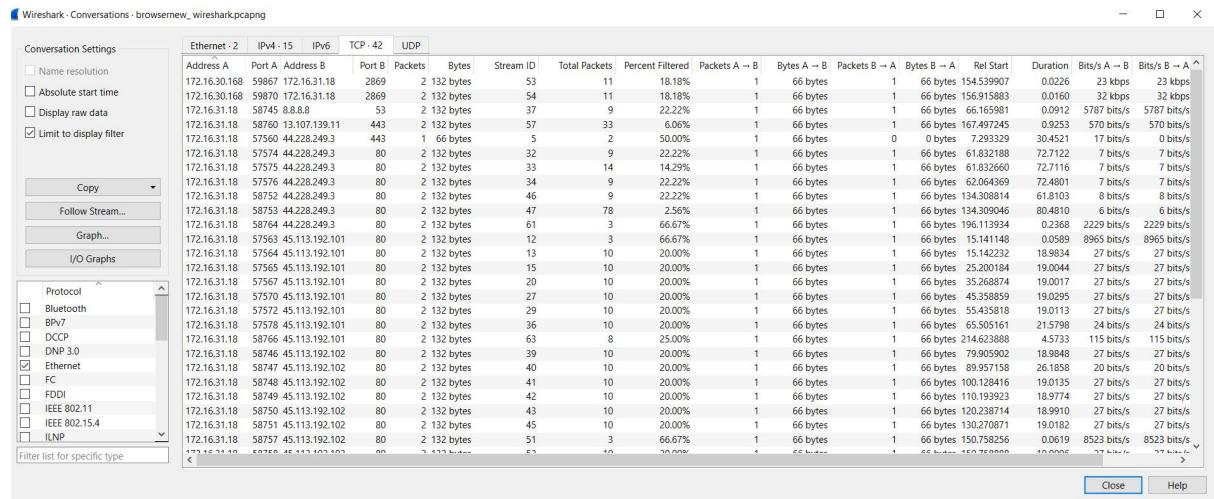
Filter list for specific type:

Close Help

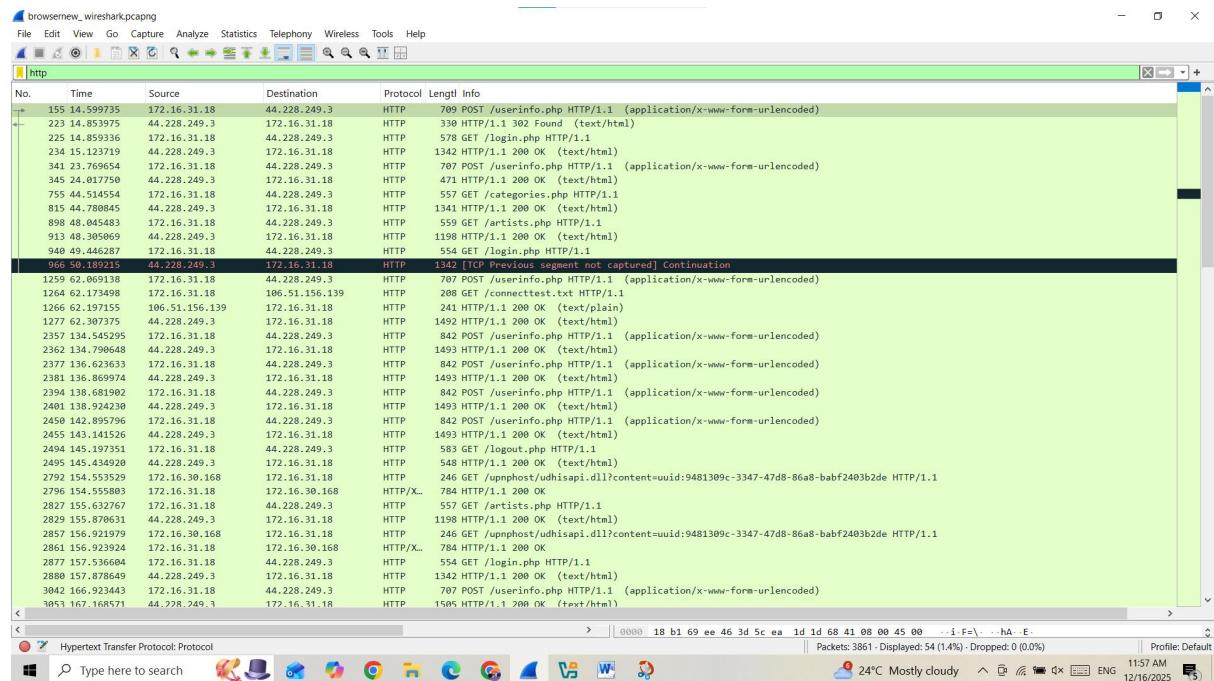
Packets: 3861 - Displayed: 41 (1.1%) - Dropped: 0 (0.0%) Profile: Default

Type here to search 23°C Mostly cloudy 11:39 AM ENG 12/16/2025

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



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



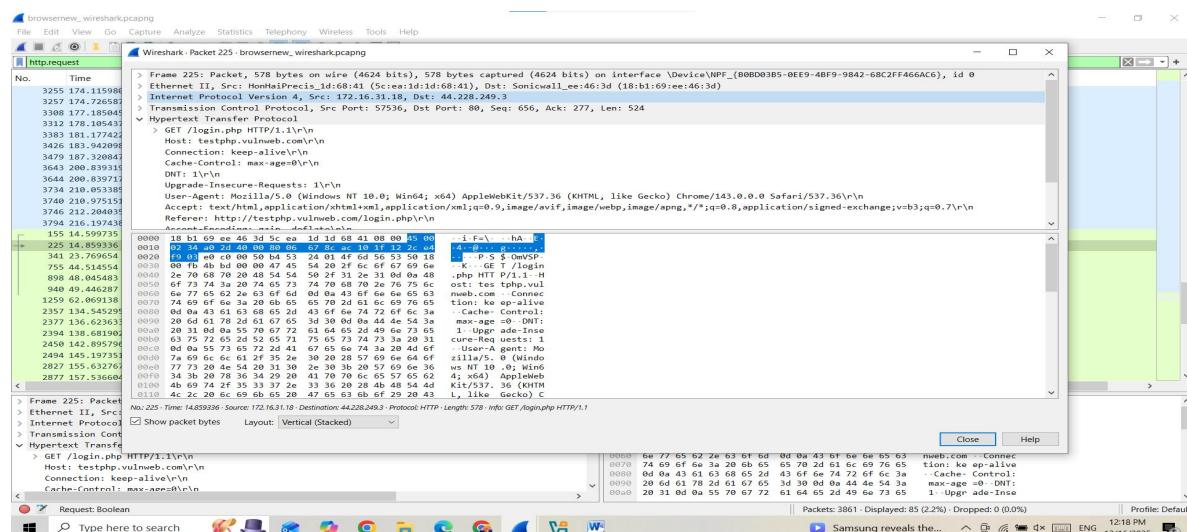
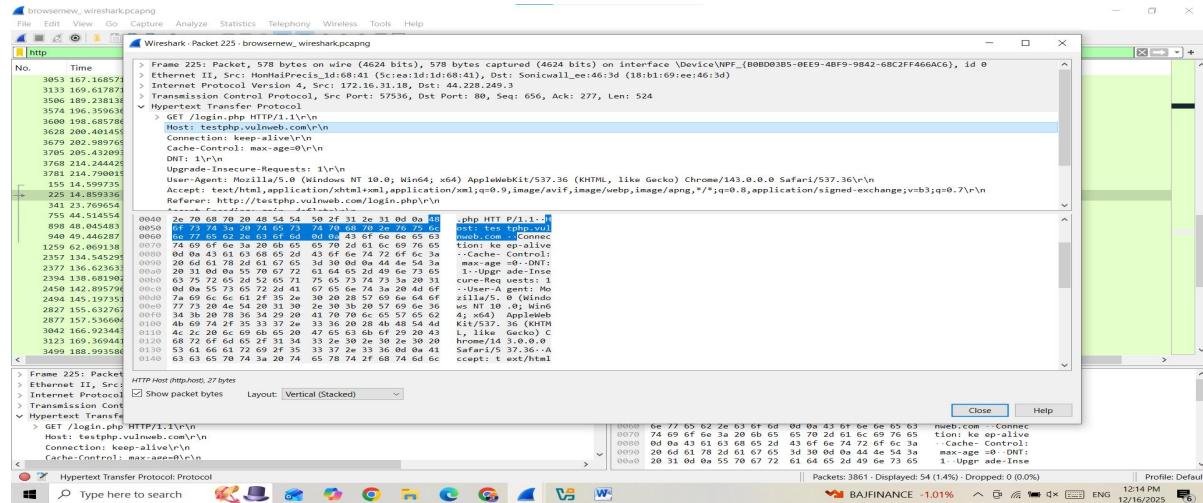
6. How many objects/files are downloaded?

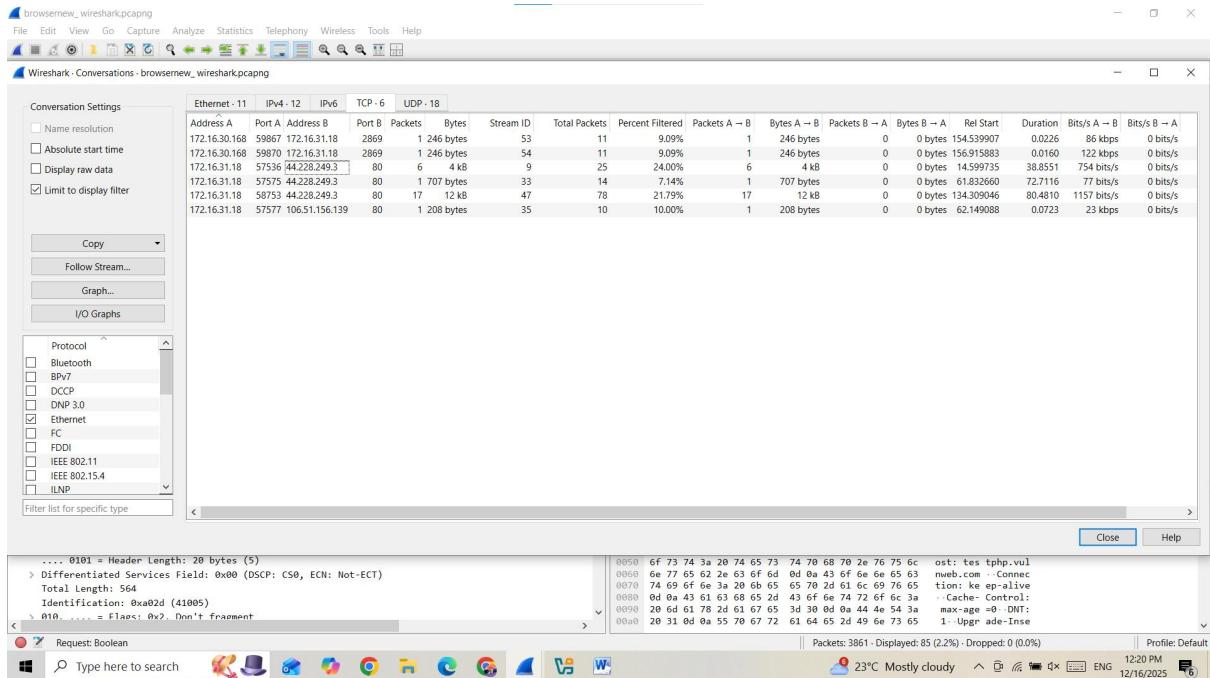
No.	Time	Source	Destination	Protocol	Length	Info
225	14.859336	172.16.31.18	44.228.249.3	HTTP	578	GET /login.php HTTP/1.1
755	44.514554	172.16.31.18	44.228.249.3	HTTP	557	GET /categories.php HTTP/1.1
898	48.045483	172.16.31.18	44.228.249.3	HTTP	559	GET /artists.php HTTP/1.1
940	49.446287	172.16.31.18	44.228.249.3	HTTP	554	GET /login.php HTTP/1.1
1264	62.173498	172.16.31.18	106.51.156.139	HTTP	208	GET /connecttest.txt HTTP/1.1
2494	145.197351	172.16.31.18	44.228.249.3	HTTP	583	GET /logout.php HTTP/1.1
2792	154.553529	172.16.30.168	172.16.31.18	HTTP	246	GET /upnphost/udhisapi.dll?content=uuid:9481309c-3347-47d8-86a8-babf2403b2de HTTP/1.1
2827	155.632767	172.16.31.18	44.228.249.3	HTTP	557	GET /artists.php HTTP/1.1
2857	156.921979	172.16.30.168	172.16.31.18	HTTP	246	GET /upnphost/udhisapi.dll?content=uuid:9481309c-3347-47d8-86a8-babf2403b2de HTTP/1.1
2877	157.536604	172.16.31.18	44.228.249.3	HTTP	554	GET /login.php HTTP/1.1
3557	196.118388	172.16.31.18	44.228.249.3	HTTP	581	GET /cart.php HTTP/1.1
3595	198.445953	172.16.31.18	44.228.249.3	HTTP	583	GET /disclaimer.php HTTP/1.1
3625	200.162572	172.16.31.18	44.228.249.3	HTTP	586	GET /artists.php HTTP/1.1
3674	202.749357	172.16.31.18	44.228.249.3	HTTP	586	GET /categories.php HTTP/1.1
3697	205.190650	172.16.31.18	44.228.249.3	HTTP	584	GET /index.php HTTP/1.1
3764	214.007265	172.16.31.18	44.228.249.3	HTTP	610	GET /index.php HTTP/1.1
3774	214.552770	172.16.31.18	44.228.249.3	HTTP	610	GET /index.php 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

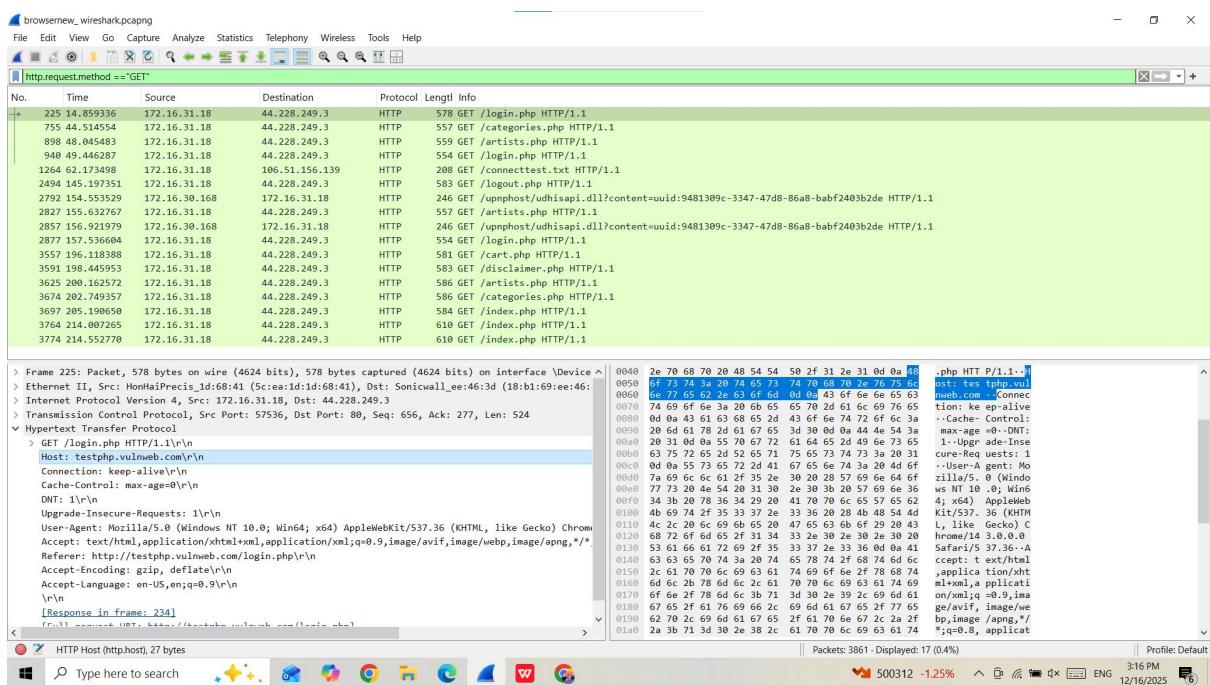
Conversation Settings	Ethernet - 2	IPv4 - 3	IPv6	TCP - 5	UDP												
<input type="checkbox"/> Name resolution	Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
<input type="checkbox"/> Absolute start time	172.16.30.168	59867	172.16.31.18	2869	1	246 bytes	53	11	9.09%	1	246 bytes	0	0 bytes	154.539907	0.0226	86 kbps	0 bits/s
<input type="checkbox"/> Display raw data	172.16.30.168	59870	172.16.31.18	2869	1	246 bytes	54	11	9.09%	1	246 bytes	0	0 bytes	156.915883	0.0160	122 kbps	0 bits/s
<input checked="" type="checkbox"/> Limit to display filter	172.16.31.18	57536	44.228.249.3	80	4	2 kB	9	25	16.00%	4	2 kB	0	0 bytes	14.599735	38.8551	462 bits/s	0 bits/s
	172.16.31.18	58753	44.228.249.3	80	10	6 kB	47	78	12.82%	10	6 kB	0	0 bytes	134.309046	80.4810	579 bits/s	0 bits/s
	172.16.31.18	57577	106.51.156.139	80	1	208 bytes	35	10	10.00%	1	208 bytes	0	0 bytes	62.149088	0.0723	23 kbps	0 bits/s

8. How many other websites are visited from this site, by clicking on to various possible links which take you to the other sites





9. When http://testphp.vulnweb.com/login.php is entered, is there any embedded object shown/downloaded from different site(s) (other than <http://testphp.vulnweb.com/login.php>)?



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

Screenshot of Wireshark showing network traffic. The packet list shows multiple HTTP requests from port 127.0.0.1 (localhost) to port 80 (vulnweb.com). The most recent request (Frame 155) is highlighted.

```

No. Time Source Destination Protocol Length Info
155 14.599735 172.16.31.18 44.228.249.3 HTTP 709 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
223 14.853975 44.228.249.3 172.16.31.18 HTTP 338 HTTP/1.1 302 Found (text/html)
225 14.859336 172.16.31.18 44.228.249.3 HTTP 578 GET /login.php HTTP/1.1
234 15.123719 44.228.249.3 172.16.31.18 HTTP 1342 HTTP/1.1 200 OK (text/html)
341 23.769654 172.16.31.18 44.228.249.3 HTTP 707 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
345 24.017750 44.228.249.3 172.16.31.18 HTTP 471 HTTP/1.1 200 OK (text/html)
755 44.514554 172.16.31.18 44.228.249.3 HTTP 557 GET /categories.php HTTP/1.1
815 44.789845 44.228.249.3 172.16.31.18 HTTP 1341 HTTP/1.1 200 OK (text/html)
898 48.045483 172.16.31.18 44.228.249.3 HTTP 559 GET /artists.php HTTP/1.1
913 48.305069 44.228.249.3 172.16.31.18 HTTP 1198 HTTP/1.1 200 OK (text/html)
940 49.446287 172.16.31.18 44.228.249.3 HTTP 554 GET /login.php HTTP/1.1
96 50.189215 44.228.249.3 172.16.31.18 HTTP 1342 [TCP Previous Segment not captured] Continuation
1259 62.069138 172.16.31.18 44.228.249.3 HTTP 707 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
1264 62.173498 172.16.31.18 106.51.156.139 HTTP 208 GET /connecttest.txt HTTP/1.1
1266 62.197155 106.51.156.139 172.16.31.18 HTTP 241 HTTP/1.1 200 OK (text/plain)
1277 62.307375 44.228.249.3 172.16.31.18 HTTP 1492 HTTP/1.1 200 OK (text/html)
2357 134.545295 172.16.31.18 44.228.249.3 HTTP 842 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

```

Frame 155 details:

```

> Frame 155: Packet, 709 bytes on wire (5672 bits), 709 bytes captured (5672 bits) on interface \Device\NPF_{...} (vulnweb.com)
> Ethernet II, Src: HonhaiPrecis_1d:68:41 (5c:ea:id:1d:68:41), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
> Internet Protocol Version 4, Src: 172.16.31.18, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 57536, Dst Port: 80, Seq: 1, Ack: 1, Len: 655
> Hypertext Transfer Protocol
  > POST /userinfo.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Content-Length: 22\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://testphp.vulnweb.com\r\n
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
  
```

Packet details and bytes panes are visible at the bottom.

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

Screenshot of Wireshark showing network traffic. The packet list shows multiple HTTP requests from port 127.0.0.1 (localhost) to port 80 (vulnweb.com). The most recent request (Frame 155) is highlighted.

```

No. Time Source Destination Protocol Length Info
155 14.599735 172.16.31.18 44.228.249.3 HTTP 709 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
223 14.853975 44.228.249.3 172.16.31.18 HTTP 338 HTTP/1.1 302 Found (text/html)
225 14.859336 172.16.31.18 44.228.249.3 HTTP 578 GET /login.php HTTP/1.1
234 15.123719 44.228.249.3 172.16.31.18 HTTP 1342 HTTP/1.1 200 OK (text/html)
341 23.769654 172.16.31.18 44.228.249.3 HTTP 707 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
345 24.017750 44.228.249.3 172.16.31.18 HTTP 471 HTTP/1.1 200 OK (text/html)
755 44.514554 172.16.31.18 44.228.249.3 HTTP 557 GET /categories.php HTTP/1.1
815 44.789845 44.228.249.3 172.16.31.18 HTTP 1341 HTTP/1.1 200 OK (text/html)
898 48.045483 172.16.31.18 44.228.249.3 HTTP 559 GET /artists.php HTTP/1.1
913 48.305069 44.228.249.3 172.16.31.18 HTTP 1198 HTTP/1.1 200 OK (text/html)
940 49.446287 172.16.31.18 44.228.249.3 HTTP 554 GET /login.php HTTP/1.1
96 50.189215 44.228.249.3 172.16.31.18 HTTP 1342 [TCP Previous Segment not captured] Continuation
1259 62.069138 172.16.31.18 44.228.249.3 HTTP 707 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
1264 62.173498 172.16.31.18 106.51.156.139 HTTP 208 GET /connecttest.txt HTTP/1.1
1266 62.197155 106.51.156.139 172.16.31.18 HTTP 241 HTTP/1.1 200 OK (text/plain)
1277 62.307375 44.228.249.3 172.16.31.18 HTTP 1492 HTTP/1.1 200 OK (text/html)
2357 134.545295 172.16.31.18 44.228.249.3 HTTP 842 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

```

Frame 155 details:

```

> Frame 155: Packet, 709 bytes on wire (5672 bits), 709 bytes captured (5672 bits) on interface \Device\NPF_{...} (vulnweb.com)
> Ethernet II, Src: HonhaiPrecis_1d:68:41 (5c:ea:id:1d:68:41), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
> Internet Protocol Version 4, Src: 172.16.31.18, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 57536, Dst Port: 80, Seq: 1, Ack: 1, Len: 655
> Hypertext Transfer Protocol
  > POST /userinfo.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Content-Length: 22\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://testphp.vulnweb.com\r\n
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
  
```

Packet details and bytes panes are visible at the bottom.

Task 2:

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

Screenshot of Wireshark showing network traffic. A search filter is applied: http.request.method == "GET". The list of captured packets shows various HTTP requests, primarily conditional GETs (HTTP 1.1) from the browser to the server. Key examples include:

- Packet 225: 14.859336, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 578 bytes. GET /login.php HTTP/1.1.
- Packet 895: 48.045483, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 557 bytes. GET /categories.php HTTP/1.1.
- Packet 1077: 14.859336, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 559 bytes. GET /artists.php HTTP/1.1.
- Packet 1264: 62.173408, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 520 bytes. GET /connecttest.txt HTTP/1.1.
- Packet 2494: 145.197351, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 559 bytes. GET /logout.php HTTP/1.1.
- Packet 2792: 154.553529, Source: 172.16.30.168, Destination: 172.16.31.18, Protocol: HTTP, Length: 246 bytes. GET /upphost/udhisapi.dll?content=uuid:9481309c-3347-47d8-86a8-babf2403b2de HTTP/1.1.
- Packet 2827: 155.632767, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 557 bytes. GET /artists.php HTTP/1.1.
- Packet 2857: 156.921979, Source: 172.16.30.168, Destination: 172.16.31.18, Protocol: HTTP, Length: 246 bytes. GET /upphost/udhisapi.dll?content=uuid:9481309c-3347-47d8-86a8-babf2403b2de HTTP/1.1.
- Packet 3557: 199.188188, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 549 bytes. GET /login.php HTTP/1.1.
- Packet 3591: 198.445953, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 583 bytes. GET /disclaimer.php HTTP/1.1.
- Packet 3625: 200.162572, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 586 bytes. GET /artists.php HTTP/1.1.
- Packet 3674: 202.749357, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 586 bytes. GET /categories.php HTTP/1.1.
- Packet 3697: 205.190658, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 584 bytes. GET /index.php HTTP/1.1.
- Packet 3704: 214.807265, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 610 bytes. GET /index.php HTTP/1.1.
- Packet 3774: 214.552778, Source: 172.16.31.18, Destination: 44.228.249.3, Protocol: HTTP, Length: 610 bytes. GET /index.php HTTP/1.1.

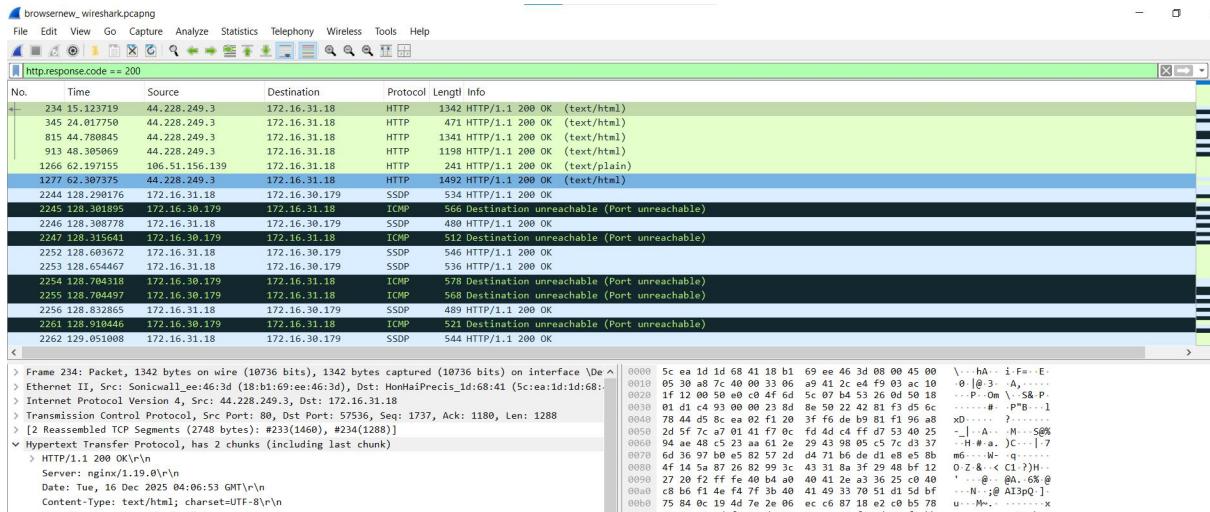
The screenshot also shows the browser's address bar with "HTTP Connection (http.connection)" and the status bar indicating "Packets: 3861 - Displayed: 17 (0.4%)".

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 ?

Screenshot of Wireshark showing the "HTTP object list" table. The table lists various files and objects downloaded, including their content type, size, and filename. The "Content Type" column is set to "All Content-Types".

Packet	Hostname	Content Type	Size	Filename
155	testphp.vulnweb.com	application/x-www-form-urlencoded	22 bytes	userinfo.php
223	testphp.vulnweb.com	text/html	14 bytes	userinfo.php
234	testphp.vulnweb.com	text/html	5523 bytes	login.php
341	testphp.vulnweb.com	application/x-www-form-urlencoded	20 bytes	userinfo.php
345	testphp.vulnweb.com	text/html	170 bytes	userinfo.php
815	testphp.vulnweb.com	text/html	6115 bytes	categories.php
913	testphp.vulnweb.com	text/html	5328 bytes	artists.php
966			1288 bytes	
1259	testphp.vulnweb.com	application/x-www-form-urlencoded	20 bytes	userinfo.php
1266	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt
1277	testphp.vulnweb.com	text/html	5995 bytes	userinfo.php
2357	testphp.vulnweb.com	application/x-www-form-urlencoded	124 bytes	userinfo.php
2362	testphp.vulnweb.com	text/html	6007 bytes	userinfo.php
2377	testphp.vulnweb.com	application/x-www-form-urlencoded	124 bytes	userinfo.php
2381	testphp.vulnweb.com	text/html	6007 bytes	userinfo.php
2394	testphp.vulnweb.com	application/x-www-form-urlencoded	124 bytes	userinfo.php
2401	testphp.vulnweb.com	text/html	6007 bytes	userinfo.php
2450	testphp.vulnweb.com	application/x-www-form-urlencoded	124 bytes	userinfo.php
2455	testphp.vulnweb.com	text/html	6007 bytes	userinfo.php
2495	testphp.vulnweb.com	text/html	170 bytes	logout.php
2796	172.16.31.18:2869	text/xml	3650 bytes	udhisapi.dll?content=uuid:9481309c-3347-47d8-86a8-babf2403b2de
2829	testphp.vulnweb.com	text/html	5328 bytes	artists.php

The screenshot also shows the bottom of the Wireshark interface with buttons for "Save", "Save All", "Preview", "Close", and "Help".



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

->First Request

During the first request, the browser cache is empty. The browser sends normal HTTP GET requests for the main HTML page and all embedded objects. Since the server has no information about any cached copies at the client side, it unconditionally sends the full content of every requested resource.

http method – 200 Ok – full content will be delivered

Second Request

During the second request, the browser already has cached copies of the previously downloaded resources. Instead of requesting the full content again, the browser sends conditional GET requests that include cache validation headers.

http method – 304 not modified – where it will not send any content if it was same.

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

->List of HTTP method Headers

For 200

If modified since

If none match

Cache control

For 304

Last modified

Etag

Task-3:

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

Wireshark capture of http2-h2c.pcap showing two total 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]

Wireshark capture of http2-h2c.pcap showing a detailed view of the HTTP/2 exchange:

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	0.600596	139.162.123.134	10.9.0.2	HTTP2	342	HEADERS[1]: 200 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	0.512304	139.162.123.134	10.9.0.2	HTTP2	75	SETTINGS[0]
10	0.516413	139.162.123.134	10.9.0.2	HTTP2	156	HEADERS[3]: 404 Not Found, DATA[3] (text/plain)

Packet details for frame 8 (115 bytes):

```
> Frame 8: Packet, 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
> Ethernet II, Src: c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b)
> Internet Protocol Version 4, Src: 10.9.0.2, Dst: 139.162.123.134
> Transmission Control Protocol, Src Port: 58038, Dst Port: 80, Seq: 252, Ack: 375, Len: 49
> HyperText Transfer Protocol 2
  > Stream: HEADERS, Stream ID: 3, Length 40, GET /humans.txt
```

Hex dump for frame 8:

```
0000  8a 7d 40 9e 52 1b 92 76 39 be c1 81 08 45 00 7@ R- v 9-----E-
0001  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e v@ -----
0002  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 { - P- 2- 1-
0003  00 ed 11 8b 00 00 01 01 08 0a 44 e5 61 c5 d4 bc .-.-. -D A- -
0004  f2 58 00 00 28 01 05 00 00 00 03 3f e1 1f 82 04 X-(-.-?-
0005  88 62 7b 69 1d 48 5d 3e 53 86 41 88 aa 69 d2 9a b-[H]> S A- i-
0006  c4 b9 ec 9b 7a 88 25 b6 50 c3 ab b8 15 c1 53 03 -----z% P-----S-
0070  2a 2f 2a */*
```

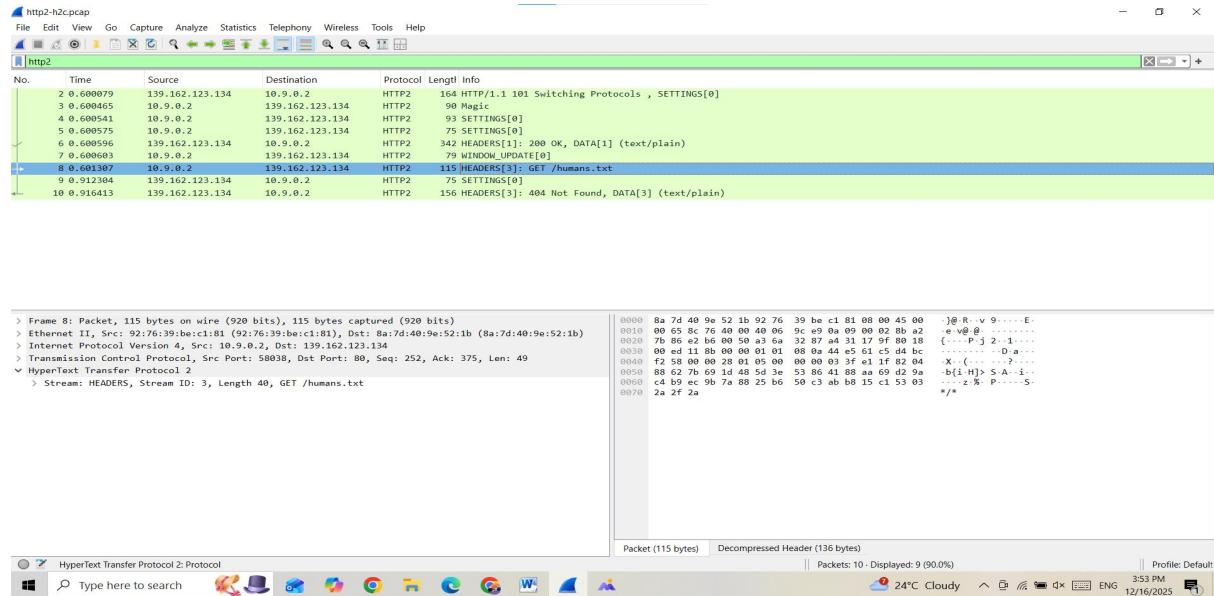
Decompressed Header (136 bytes):

```
Packet (115 bytes) | Decompressed Header (136 bytes)
```

Windows Taskbar:

- HyperText Transfer Protocol 2: Protocol
- Type here to search
- Icons for File Explorer, Mail, Photos, Task View, Google Chrome, Microsoft Edge, File Explorer, and File Explorer
- System tray icons: Battery (24%), Cloudy, 24°C, ENG, 3:53 PM, 12/16/2025

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



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

