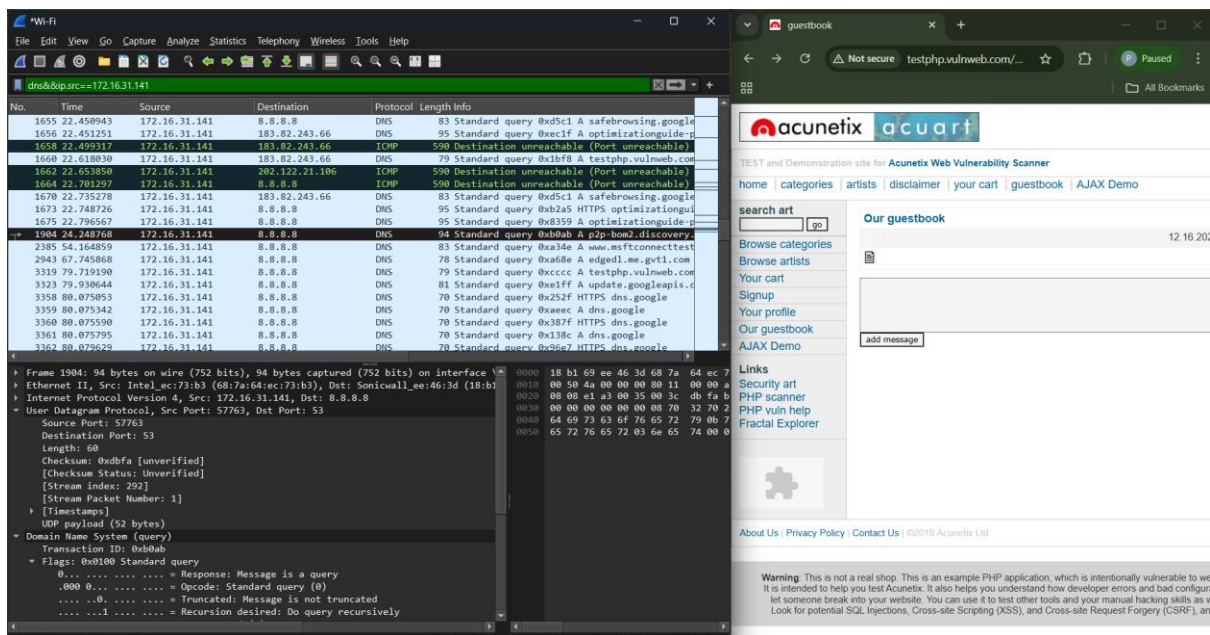
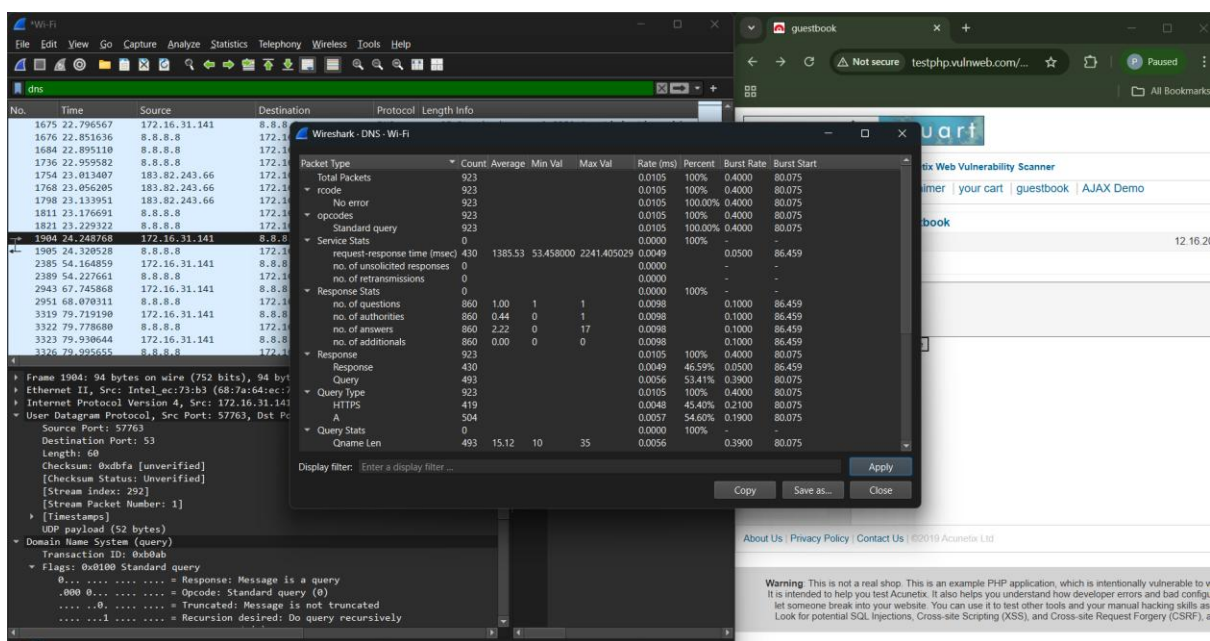


TASK 1



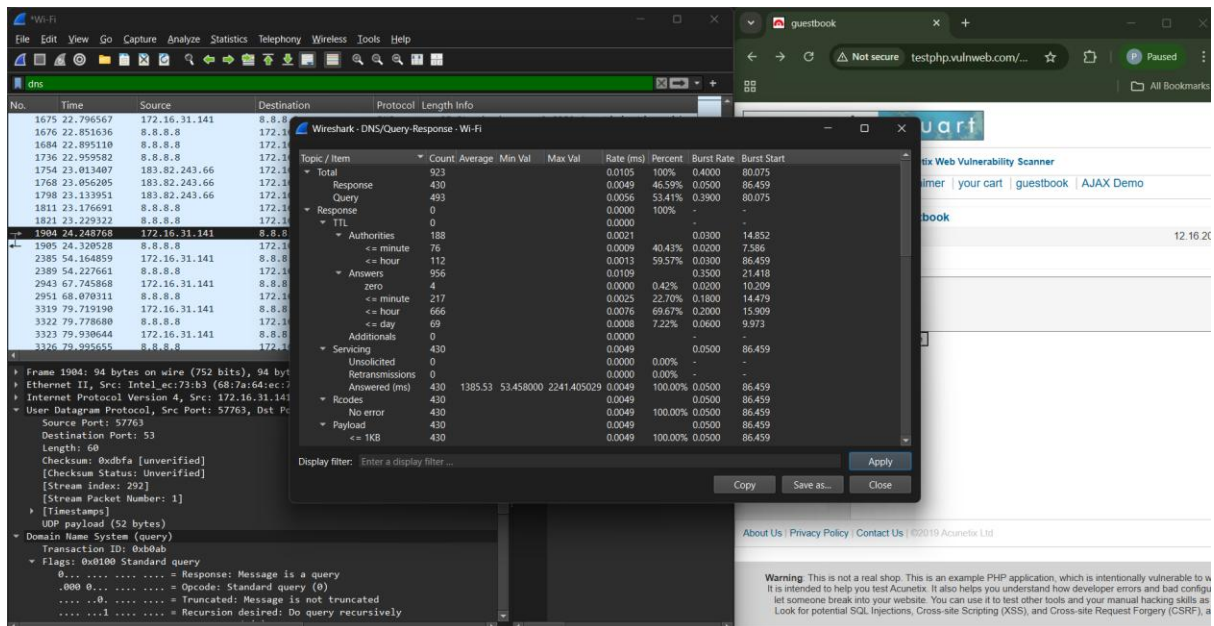
1. DNS Queries and DNS Servers

In the screenshot where the dns filter is applied, DNS query packets are visible from the client machine to the DNS server to resolve testphp.vulnweb.com. Multiple DNS queries are sent before the website is accessed. The DNS response packet contains the A record, which provides the actual IP address of the server along with TTL information. This confirms successful domain name resolution.



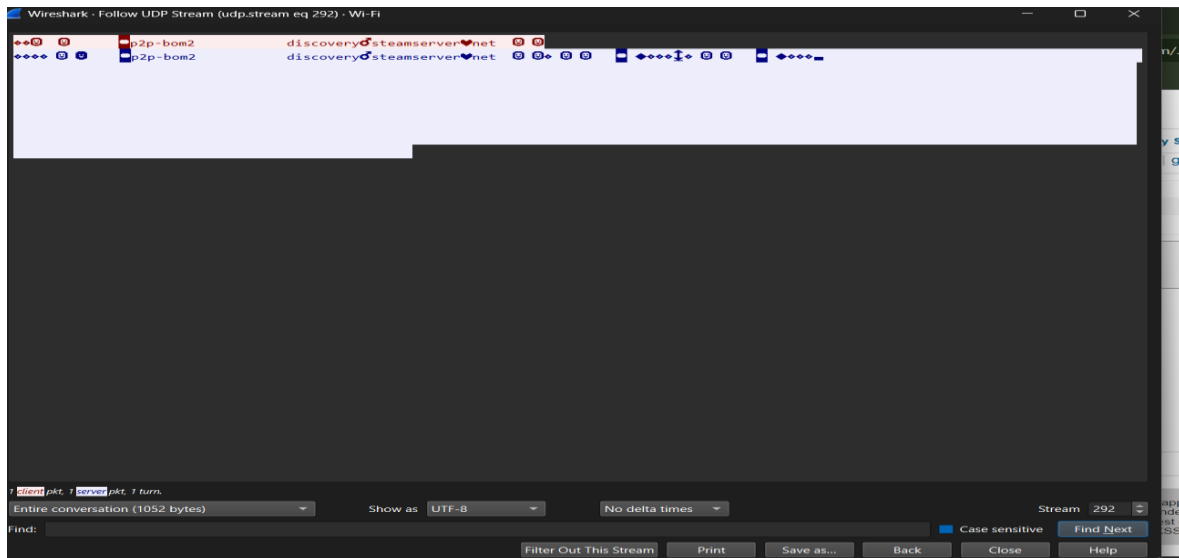
2. HTTP Requests and Responses

Using the http filter, the screenshot shows several HTTP GET requests sent by the browser to fetch the guestbook page and its associated resources. Corresponding HTTP responses with status code 200 OK are received from the server. This indicates that the requested resources were successfully delivered.



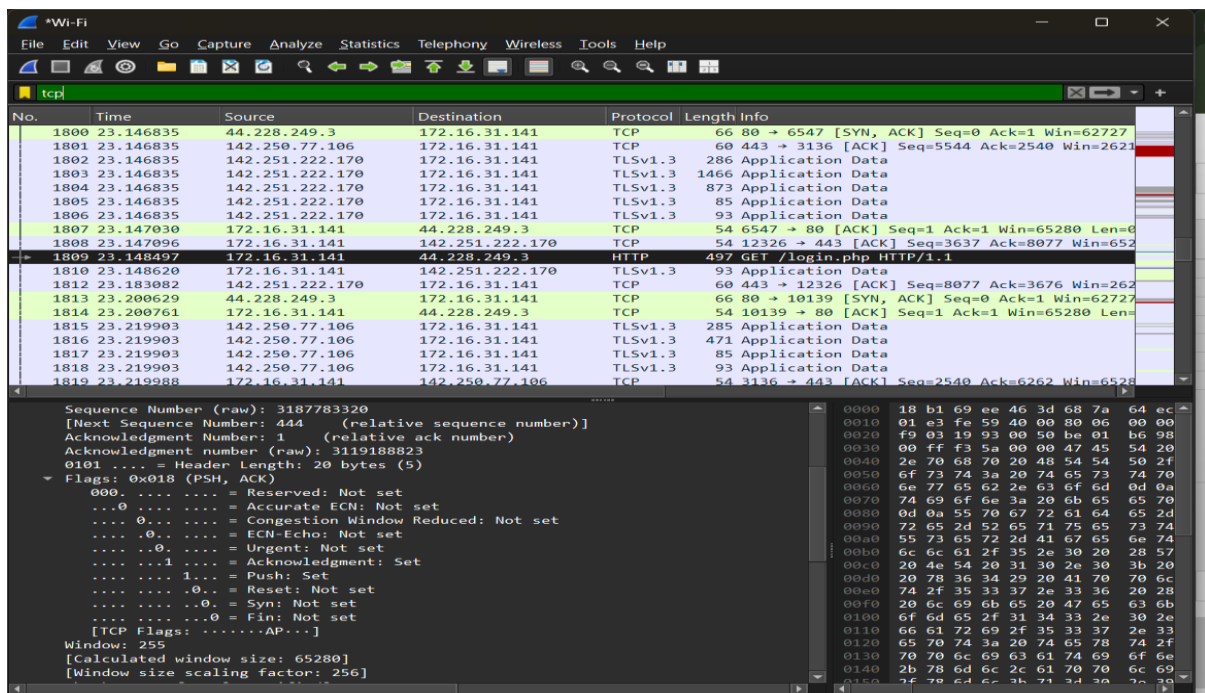
3. TCP Connections Established

From the tcp filtered screenshot, multiple TCP connections are visible between the client and the web server. Each connection is identified by a unique source and destination port number. This shows that the browser establishes TCP connections before transferring HTTP data.



4. TCP Connection Establishment Time

In the TCP handshake packets shown in the screenshot, the **SYN**, **SYN-ACK**, and **ACK** sequence can be observed. The time difference between SYN and ACK packets gives the TCP connection setup time. Each TCP stream shows a slightly different establishment delay.



5. Browsing Embedded Objects

After loading the main guestbook page, the browser automatically requests additional embedded objects. This is visible through multiple HTTP GET

requests for images and page components. These requests confirm normal webpage rendering behavior.

The screenshot shows a Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows a series of QUIC and DNS packets. The selected packet is a DNS response (No. 1798). The packet details pane shows the structure of the DNS response, including the transaction ID, flags, and the answer section.

No.	Time	Source	Destination	Protocol	Length	Info
1746	22.980490	172.16.31.141	8.8.8.8	QUIC	77	Protected Payload (KP0), DCID=fdc5c650d8bb3
1749	22.995985	8.8.8.8	172.16.31.141	QUIC	65	Protected Payload (KP0)
1751	23.006149	172.16.31.141	8.8.8.8	QUIC	74	Protected Payload (KP0), DCID=fcd22994ac9d
1752	23.013407	8.8.8.8	172.16.31.141	QUIC	65	Protected Payload (KP0)
1754	23.013407	183.82.243.66	172.16.31.141	DNS	1042	Standard query response 0xec1f A optimizati
1762	23.043617	8.8.8.8	172.16.31.141	QUIC	66	Protected Payload (KP0)
1768	23.056205	183.82.243.66	172.16.31.141	DNS	1042	Standard query response 0x1bf8 A testphp.vu
1798	23.133951	183.82.243.66	172.16.31.141	DNS	1042	Standard query response 0xd5c1 A safebrowsi
1811	23.176691	8.8.8.8	172.16.31.141	DNS	1042	Standard query response 0xb2a5 HTTPS optimi
1821	23.229322	8.8.8.8	172.16.31.141	DNS	1042	Standard query response 0x8359 A optimizati
1833	23.654448	fe80::27f7:7015:4d6...	ff02::fb	MDNS	202	Standard query response 0x0000 PTR, cache f
1855	23.843269	172.16.31.141	8.8.8.8	QUIC	253	Protected Payload (KP0), DCID=fdc5c650d8bb3
1856	23.843512	172.16.31.141	8.8.8.8	QUIC	253	Protected Payload (KP0), DCID=fdc5c650d8bb3
1857	23.891273	8.8.8.8	172.16.31.141	QUIC	70	Protected Payload (KP0)
1858	23.891273	8.8.8.8	172.16.31.141	QUIC	621	Protected Payload (KP0)
1859	23.891273	8.8.8.8	172.16.31.141	QUIC	64	Protected Payload (KP0)
1860	23.892145	172.16.31.141	8.8.8.8	QUIC	77	Protected Payload (KP0), DCID=fdc5c650d8bb3
1861	23.904317	172.16.31.141	8.8.8.8	QUIC	88	Protected Payload (KP0), DCID=fdc5c650d8bb3
1863	23.910861	8.8.8.8	172.16.31.141	QUIC	571	Protected Payload (KP0)

Packet Details for No. 1798:

- [Checksum Status: Unverified]
- [Stream index: 286]
- [Stream Packet Number: 2]
- [Timestamps]
- UDP payload (1000 bytes)
- Domain Name System (response)
 - Transaction ID: 0xd5c1
 - Flags: 0x8180 Standard query response, No error
 - 1... = Response: Message is a response
 - .000 0... = Opcode: Standard query (0)
 - ... 0... = Authoritative: Server is not an authority for domain
 - ... 0... = Truncated: Message is not truncated
 - ... 1... = Recursion desired: Do query recursively
 - ... 1... = Recursion available: Server can do recursive queries
 - ... 0... = Z: reserved (0)
 - ... 0... = Answer authenticated: Answer/authority portion was not a
 - ... 0... = Non-authenticated data: Unacceptable
 - ... 0000 = Reply code: No error (0)
 - Questions: 1
 - Answer RRs: 2

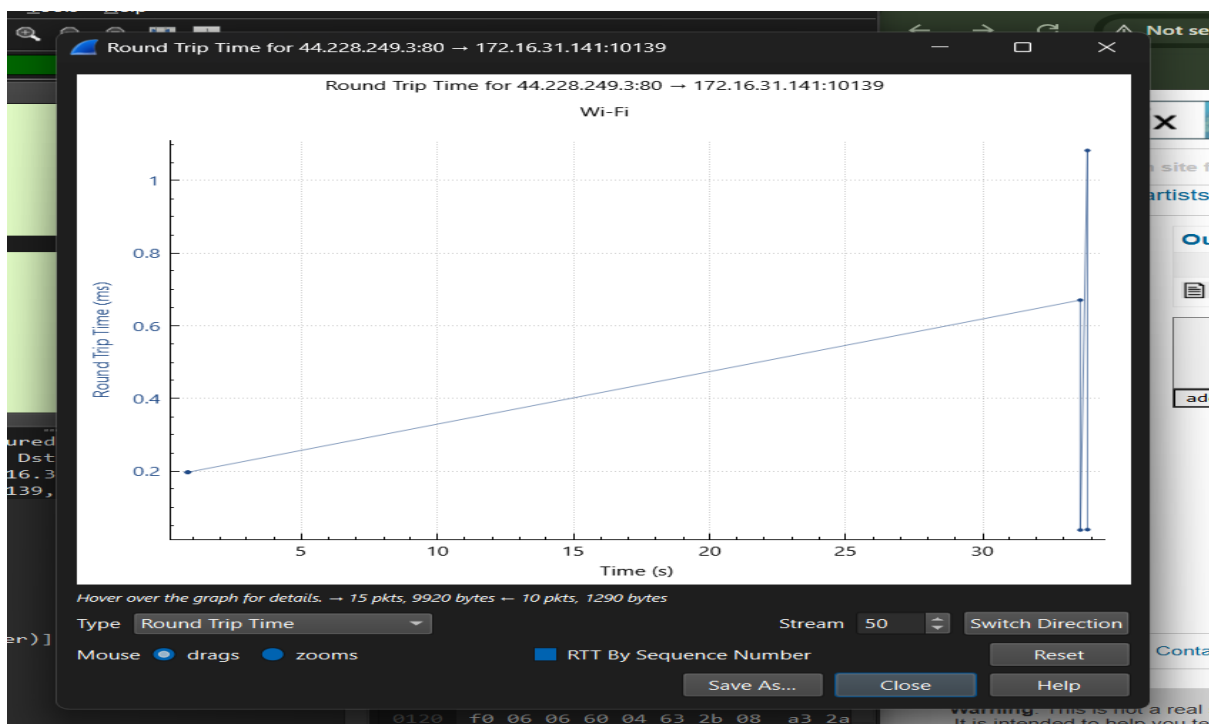
6. Number of Objects Downloaded

From the HTTP packet list in the screenshot, multiple objects are downloaded by the browser. Each object corresponds to a separate HTTP GET request. This includes the main PHP page and supporting resources.

Time	172.16.31.141	92.223.116.252	204.79.197.203	Comment
13.708694	10044	HEAD /filestreamingservice/files/fb6dd03b-99d7-4c...	80	HTTP: HEAD /filestreamingservice/files/fb6dd03b-99d7-4c8...
20.606814	14899	GET /ocsp/MFQwUJBQME4wTDAJBgUrDgMCGGUABBT...	6	HTTP: GET /ocsp/MFQwUJBQME4wTDAJBgUrDgMCGGUABBT...
20.646862				OCSP: Response
23.148497		GET /login.php HTTP/1.1		HTTP: GET /login.php HTTP/1.1
23.453304	6547	HTTP/1.1 200 OK (text/html)		HTTP: HTTP/1.1 200 OK (text/html)
23.523364	6547	GET /style.css HTTP/1.1		HTTP: GET /style.css HTTP/1.1
23.523920	10139	GET /images/logo.gif HTTP/1.1		HTTP: GET /images/logo.gif HTTP/1.1
23.763055	6547	HTTP/1.1 200 OK (text/css)		HTTP: HTTP/1.1 200 OK (text/css)
23.763055	10139	HTTP/1.1 200 OK (GIF89a)		HTTP: HTTP/1.1 200 OK (GIF89a)
31.659199	6547	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)		HTTP: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
31.896821	6547	HTTP/1.1 302 Found (text/html)		HTTP: HTTP/1.1 302 Found (text/html)
31.907593	6547	GET /login.php HTTP/1.1		HTTP: GET /login.php HTTP/1.1
32.145400	6547	HTTP/1.1 200 OK (text/html)		HTTP: HTTP/1.1 200 OK (text/html)
46.989446	6547	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)		HTTP: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
47.314705	6547	HTTP/1.1 302 Found (text/html)		HTTP: HTTP/1.1 302 Found (text/html)
47.320827	6547	GET /login.php HTTP/1.1		HTTP: GET /login.php HTTP/1.1
47.631928	6547	HTTP/1.1 200 OK (text/html)		HTTP: HTTP/1.1 200 OK (text/html)
50.151899	6547	GET /userinfo.php HTTP/1.1		HTTP: GET /userinfo.php HTTP/1.1
50.484519	6547	HTTP/1.1 302 Found (text/html)		HTTP: HTTP/1.1 302 Found (text/html)
50.490114	6547	GET /login.php HTTP/1.1		HTTP: GET /login.php HTTP/1.1

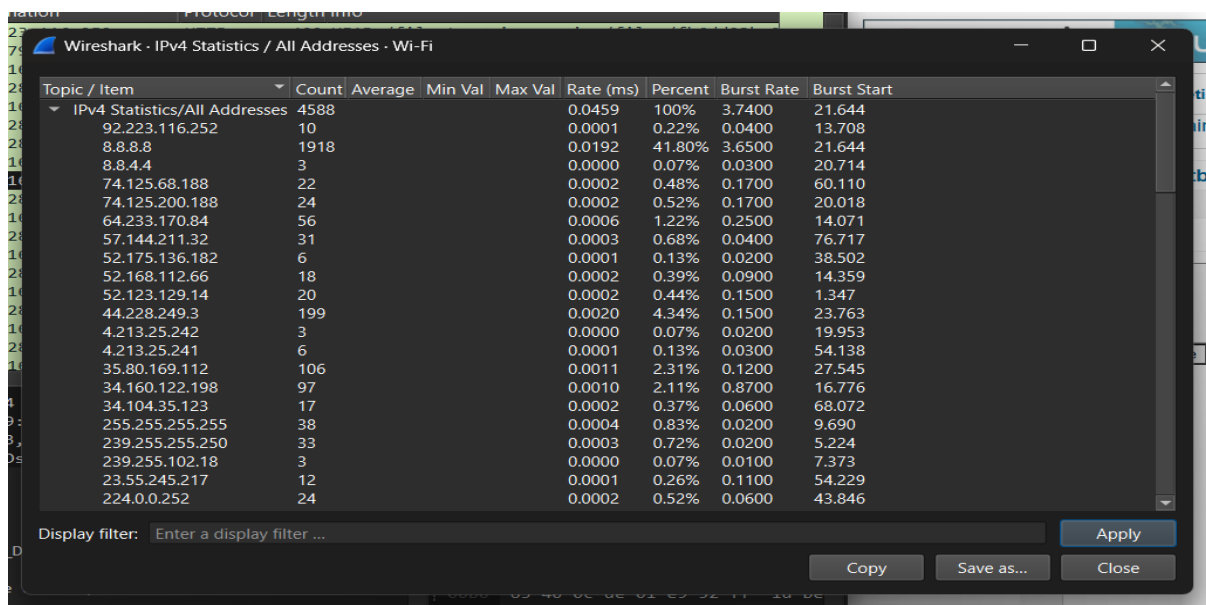
7. Object Details (Time, Size, Name, Last-Modified)

Using Statistics → HTTP → Requests, the screenshot displays details such as object name, size, and download duration. HTTP response headers show the Last-Modified field for some objects. This information helps analyze server response behavior and performance.



8. External Websites Accessed

By observing the Host field in HTTP packets, it is seen that all requests are primarily directed to testphp.vulnweb.com. No significant redirection to other domains is observed during normal browsing of the guestbook page.



The screenshot shows the Wireshark 'IPv4 Statistics / All Addresses - Wi-Fi' window. It displays a table of IP addresses and their associated statistics. The table has columns for Topic / Item, Count, Average, Min Val, Max Val, Rate (ms), Percent, Burst Rate, and Burst Start. The data is sorted by Count in descending order.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IPv4 Statistics/All Addresses	4588				0.0459	100%	3.7400	21.644
92.223.116.252	10				0.0001	0.22%	0.0400	13.708
8.8.8.8	1918				0.0192	41.80%	3.6500	21.644
8.8.4.4	3				0.0000	0.07%	0.0300	20.714
74.125.68.188	22				0.0002	0.48%	0.1700	60.110
74.125.200.188	24				0.0002	0.52%	0.1700	20.018
64.233.170.84	56				0.0006	1.22%	0.2500	14.071
57.144.211.32	31				0.0003	0.68%	0.0400	76.717
52.175.136.182	6				0.0001	0.13%	0.0200	38.502
52.168.112.66	18				0.0002	0.39%	0.0900	14.359
52.123.129.14	20				0.0002	0.44%	0.1500	1.347
44.228.249.3	199				0.0020	4.34%	0.1500	23.763
4.213.25.242	3				0.0000	0.07%	0.0200	19.953
4.213.25.241	6				0.0001	0.13%	0.0300	54.138
35.80.169.112	106				0.0011	2.31%	0.1200	27.545
34.160.122.198	97				0.0010	2.11%	0.8700	16.776
34.104.35.123	17				0.0002	0.37%	0.0600	68.072
255.255.255.255	38				0.0004	0.83%	0.0200	9.690
239.255.255.250	33				0.0003	0.72%	0.0200	5.224
239.255.102.18	3				0.0000	0.07%	0.0100	7.373
23.55.245.217	12				0.0001	0.26%	0.1100	54.229
224.0.0.252	24				0.0002	0.52%	0.0600	43.846

9. Embedded Objects from Other Domains

The screenshot shows that most embedded objects are loaded from the same domain. There are no major embedded resources fetched from third-party websites, indicating minimal external dependency.

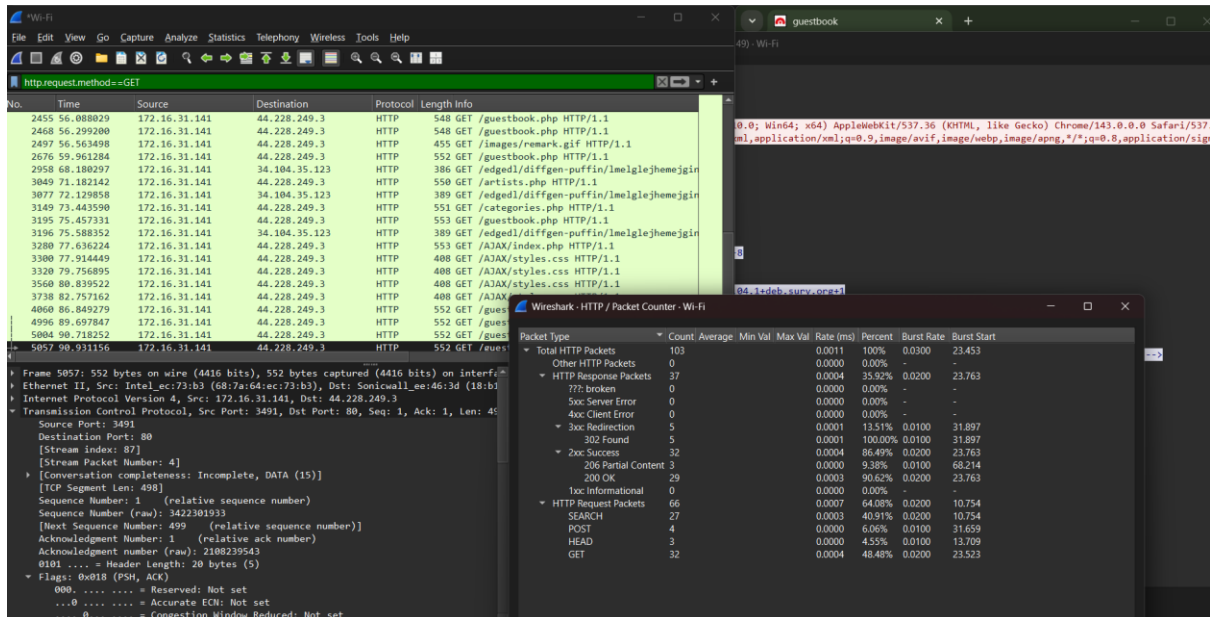
10. Keep-Alive Requests

In the HTTP request headers visible in the screenshot, the Connection: keep-alive field is present multiple times. This shows that the browser requests the server to maintain the same TCP connection for multiple HTTP requests.

11. HTTP Version Used

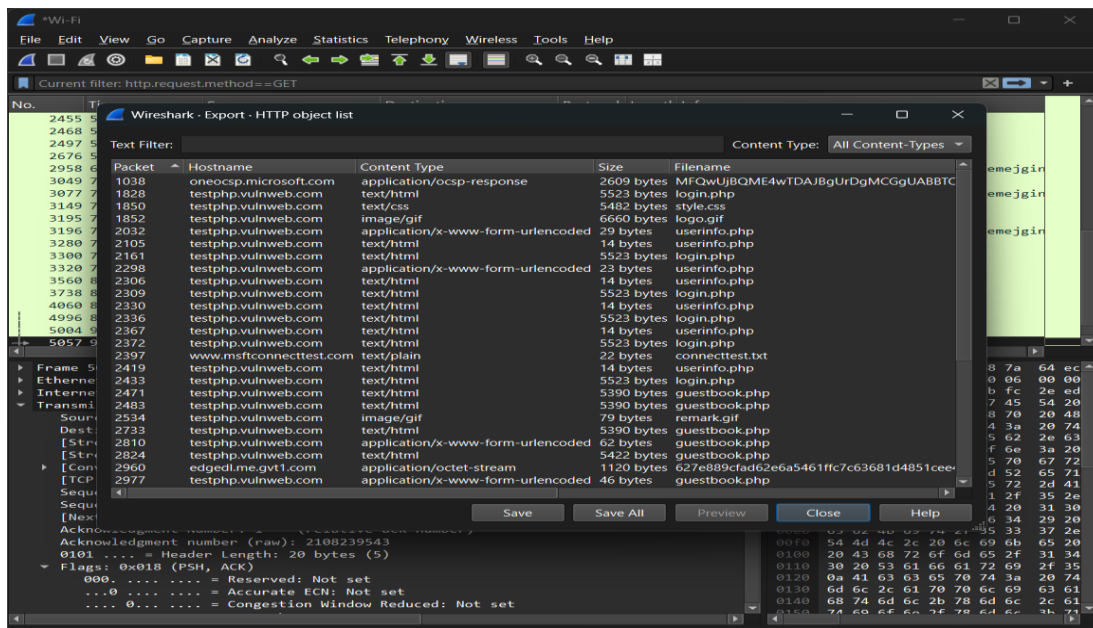
From the HTTP request line in the packet details, the browser is using HTTP/1.1. This is clearly indicated alongside the GET request method.

TASK 2



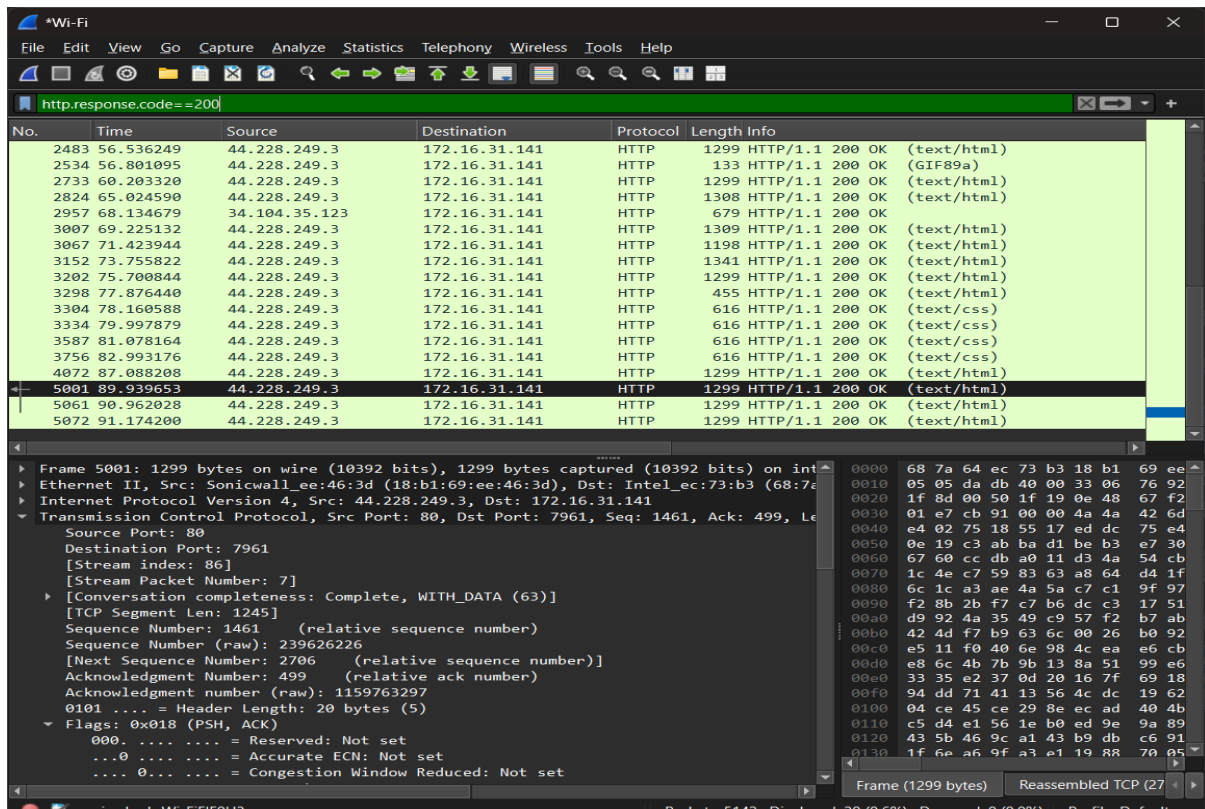
1. Conditional GET Requests

In the second browsing session, HTTP packets contain headers such as If-Modified-Since and If-None-Match, visible in the screenshot. These headers indicate that conditional GET requests were sent by the browser to validate cached content.



2. Full Content Sent by Server

During the first request, the server sends the full content of all requested objects. In the second request, the server does not resend unchanged files completely, showing efficient cache usage. This behavior is visible through response headers.



3. Difference Between First and Second Request

In the first browsing, all objects are downloaded fully from the server. In the second browsing, the browser checks whether resources have changed and avoids re-downloading unchanged files. This reduces network traffic and improves loading speed.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code==200

No.	Time	Source	Destination	Protocol	Length	Info
2483	56.536249	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
2534	56.801095	44.228.249.3	172.16.31.141	HTTP	133	HTTP/1.1 200 OK (GIF89a)
2733	60.203320	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
2824	65.024590	44.228.249.3	172.16.31.141	HTTP	1308	HTTP/1.1 200 OK (text/html)
2957	68.134679	34.104.35.123	172.16.31.141	HTTP	679	HTTP/1.1 200 OK (text/html)
3007	69.225132	44.228.249.3	172.16.31.141	HTTP	1309	HTTP/1.1 200 OK (text/html)
3067	71.423944	44.228.249.3	172.16.31.141	HTTP	1198	HTTP/1.1 200 OK (text/html)
3152	73.755822	44.228.249.3	172.16.31.141	HTTP	1341	HTTP/1.1 200 OK (text/html)
3202	75.700844	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
3298	77.876440	44.228.249.3	172.16.31.141	HTTP	455	HTTP/1.1 200 OK (text/html)
3304	78.160588	44.228.249.3	172.16.31.141	HTTP	616	HTTP/1.1 200 OK (text/css)
3334	79.997879	44.228.249.3	172.16.31.141	HTTP	616	HTTP/1.1 200 OK (text/css)
3587	81.078164	44.228.249.3	172.16.31.141	HTTP	616	HTTP/1.1 200 OK (text/css)
3756	82.993176	44.228.249.3	172.16.31.141	HTTP	616	HTTP/1.1 200 OK (text/css)
4072	87.088208	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
5001	89.939653	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
5061	90.962028	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
5072	91.174200	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)

TCP segment data (1245 bytes)

[2 Reassembled TCP Segments (2705 bytes): #2482(1460), #2483(1245)]

Hypertext Transfer Protocol, has 2 chunks (including last chunk)

HTTP/1.1 200 OK\r\n

Server: nginx/1.19.0\r\n

Date: Tue, 16 Dec 2025 07:33:53 GMT\r\n

Content-Type: text/html; charset=UTF-8\r\n

Transfer-Encoding: chunked\r\n

Connection: keep-alive\r\n

X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n

Content-Encoding: gzip\r\n

\r\n

[Request in frame: 2468]

[Time since request: 0.237049000 seconds]

[Request URI: /guestbook.php]

[Full request URI: http://testphp.vulnweb.com/guestbook.php]

HTTP chunked response

Content-encoded entity body (gzip): 2441 bytes -> 5390 bytes

File Data: 5390 bytes

Line-based text data: text/html (112 lines)

Frame (1299 bytes) Reassembled TCP (2705 bytes)

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code==200

No.	Time	Source	Destination	Protocol	Length	Info
2483	56.536249	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
2534	56.801095	44.228.249.3	172.16.31.141	HTTP	133	HTTP/1.1 200 OK (GIF89a)
2733	60.203320	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
2824	65.024590	44.228.249.3	172.16.31.141	HTTP	1308	HTTP/1.1 200 OK (text/html)
2957	68.134679	34.104.35.123	172.16.31.141	HTTP	679	HTTP/1.1 200 OK (text/html)
3007	69.225132	44.228.249.3	172.16.31.141	HTTP	1309	HTTP/1.1 200 OK (text/html)
3067	71.423944	44.228.249.3	172.16.31.141	HTTP	1198	HTTP/1.1 200 OK (text/html)
3152	73.755822	44.228.249.3	172.16.31.141	HTTP	1341	HTTP/1.1 200 OK (text/html)
3202	75.700844	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
3298	77.876440	44.228.249.3	172.16.31.141	HTTP	455	HTTP/1.1 200 OK (text/html)
3304	78.160588	44.228.249.3	172.16.31.141	HTTP	616	HTTP/1.1 200 OK (text/css)
3334	79.997879	44.228.249.3	172.16.31.141	HTTP	616	HTTP/1.1 200 OK (text/css)
3587	81.078164	44.228.249.3	172.16.31.141	HTTP	616	HTTP/1.1 200 OK (text/css)
3756	82.993176	44.228.249.3	172.16.31.141	HTTP	616	HTTP/1.1 200 OK (text/css)
4072	87.088208	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
5001	89.939653	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
5061	90.962028	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)
5072	91.174200	44.228.249.3	172.16.31.141	HTTP	1299	HTTP/1.1 200 OK (text/html)

TCP payload (79 bytes)

TCP segment data (79 bytes)

[2 Reassembled TCP Segments (315 bytes): #2533(236), #2534(79)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Server: nginx/1.19.0\r\n

Date: Tue, 16 Dec 2025 07:33:53 GMT\r\n

Content-Type: image/gif\r\n

Content-Length: 79\r\n

Last-Modified: Wed, 11 May 2011 10:27:46 GMT\r\n

Connection: keep-alive\r\n

ETag: "4dca64a2-4f"\r\n

Accept-Ranges: none\r\n

\r\n

[Request in frame: 2497]

[Time since request: 0.237597000 seconds]

[Request URI: /images/remark.gif]

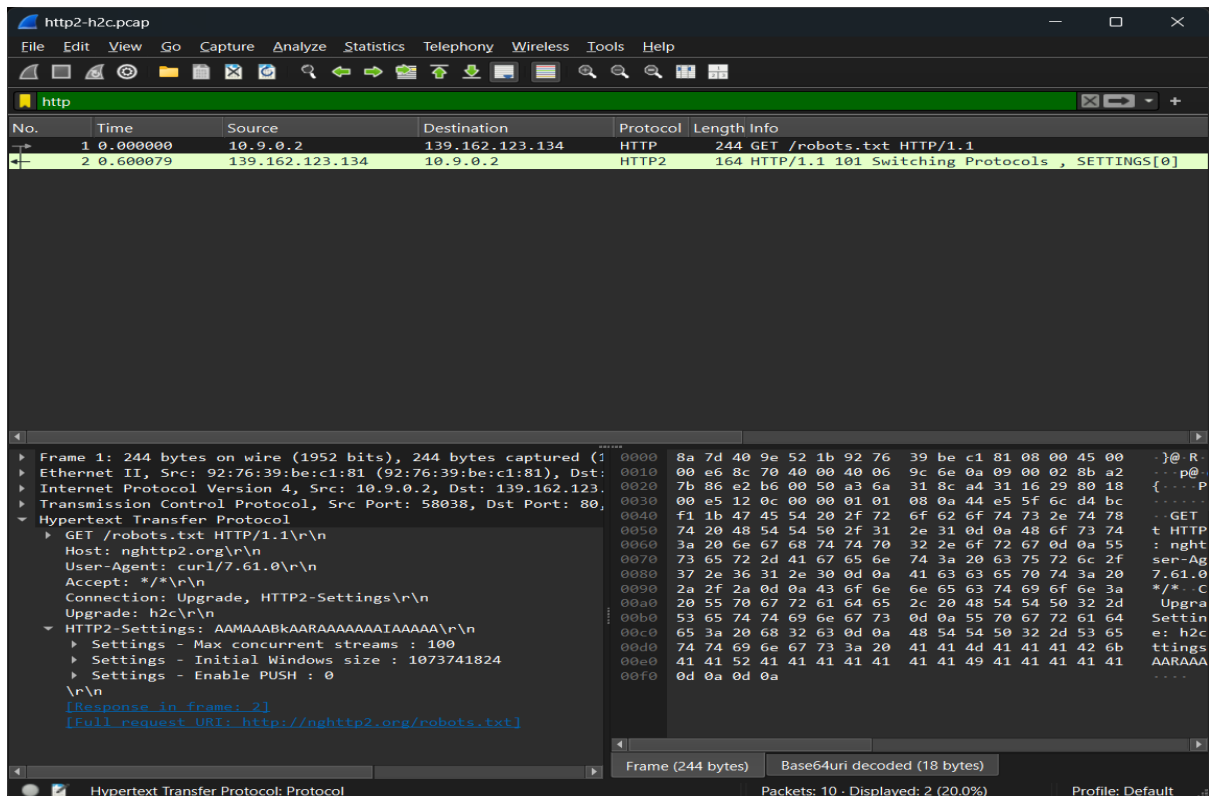
[Full request URI: http://testphp.vulnweb.com/images/remark.gif]

File Data: 79 bytes

Compuserve GIF, Version: GIF89a

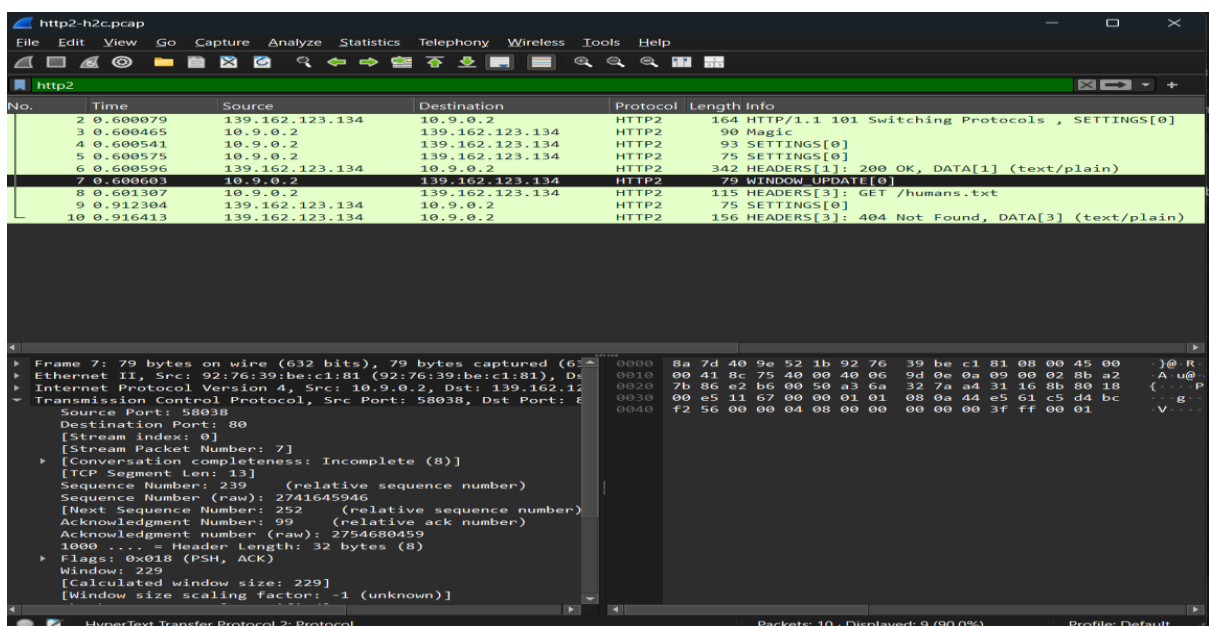
Frame (133 bytes) Reassembled TCP (315 bytes)

TASK 3



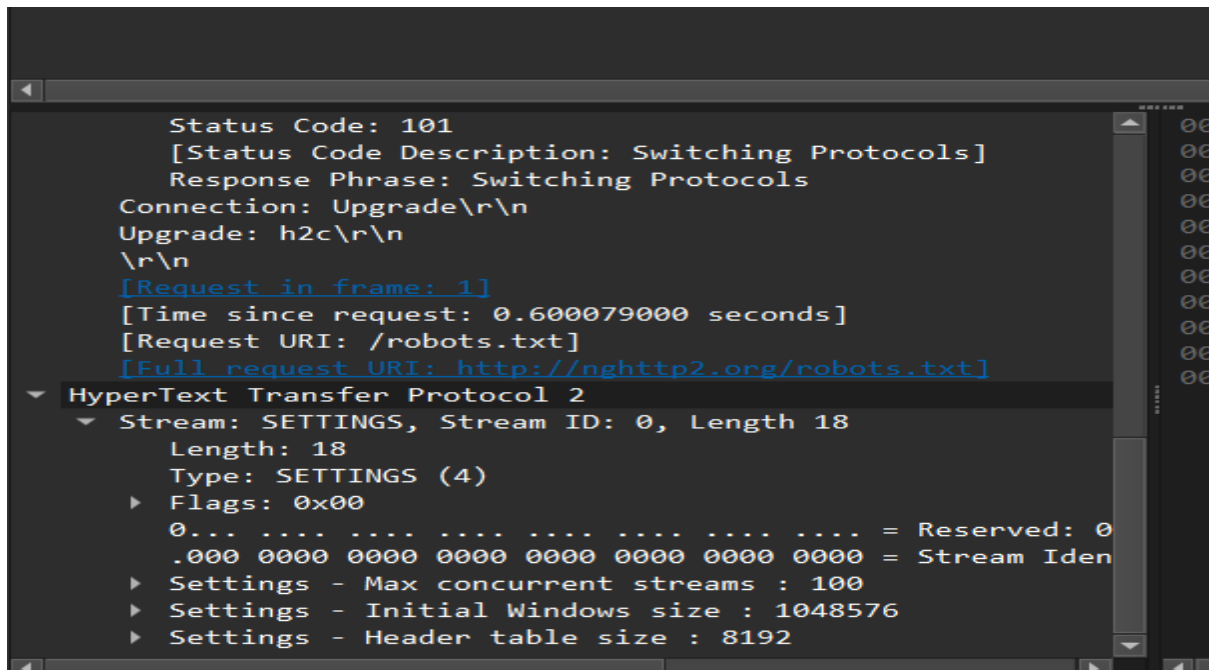
1. HTTP/2 vs HTTP/1.1 Packets

Using Statistics → HTTP / HTTP2, the screenshot shows a higher number of HTTP/2 packets compared to HTTP/1.1 packets. This confirms that most communication in the capture uses HTTP/2.



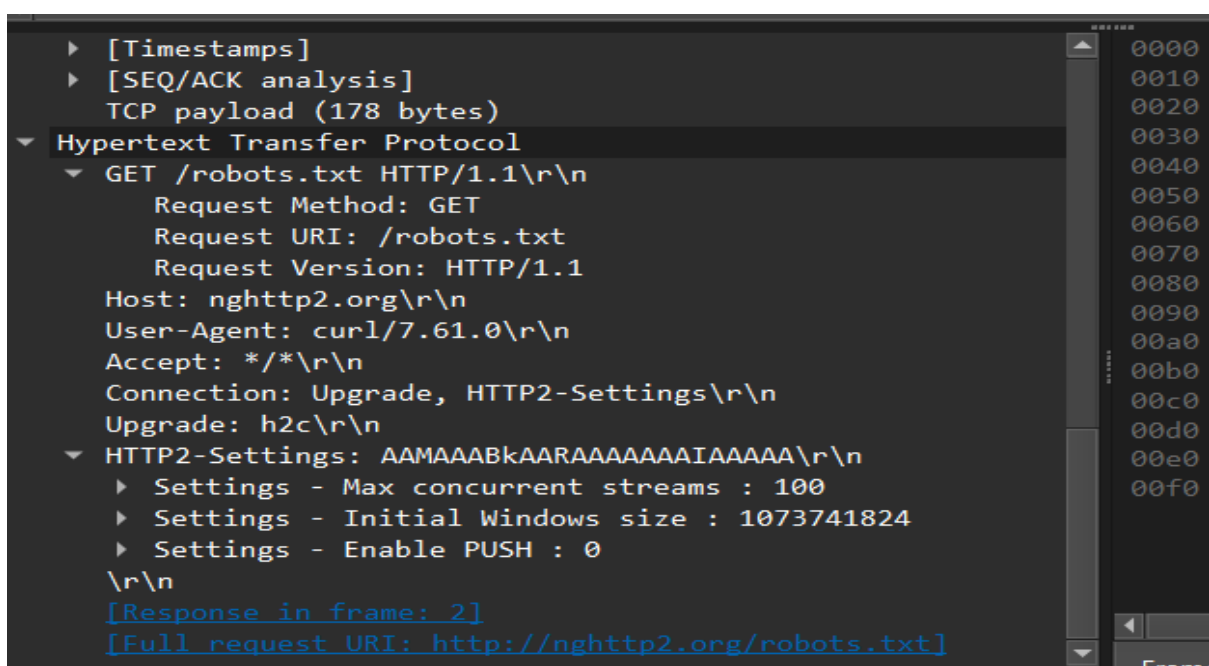
2. HTTP/2 Packets Before First Object

Before the first object is fetched, several HTTP/2 packets such as SETTINGS and HEADERS frames are exchanged. These packets establish protocol parameters between client and server.



A screenshot of a Wireshark packet capture window. The selected packet is an HTTP/2 response with status code 101 (Switching Protocols). The packet details pane shows the following information:

- Status Code: 101
[Status Code Description: Switching Protocols]
Response Phrase: Switching Protocols
- Connection: Upgrade\r\n
- Upgrade: h2c\r\n\r\n
- [Request in frame: 1]
[Time since request: 0.600079000 seconds]
[Request URI: /robots.txt]
[Full request URI: http://nghttp2.org/robots.txt]
- ▼ Hypertext Transfer Protocol 2
 - ▼ Stream: SETTINGS, Stream ID: 0, Length 18
 - Length: 18
 - Type: SETTINGS (4)
 - ▶ Flags: 0x00
 - 0... .. = Reserved: 0
 - .000 0000 0000 0000 0000 0000 0000 0000 = Stream Identifier
 - ▶ Settings - Max concurrent streams : 100
 - ▶ Settings - Initial Windows size : 1048576
 - ▶ Settings - Header table size : 8192



A screenshot of a Wireshark packet capture window showing two packets. The first packet is an HTTP/1.1 GET request, and the second packet is an HTTP/2 upgrade response.

Packet 1: GET /robots.txt HTTP/1.1

- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (178 bytes)
- ▼ Hypertext Transfer Protocol
 - ▼ GET /robots.txt HTTP/1.1\r\n
 - Request Method: GET
 - Request URI: /robots.txt
 - Request Version: HTTP/1.1
 - Host: nghttp2.org\r\n
 - User-Agent: curl/7.61.0\r\n
 - Accept: */*\r\n
 - Connection: Upgrade, HTTP2-Settings\r\n
 - Upgrade: h2c\r\n
 - ▼ HTTP2-Settings: AAMAAABkAARAAAAAIAAAAA\r\n
 - ▶ Settings - Max concurrent streams : 100
 - ▶ Settings - Initial Windows size : 1073741824
 - ▶ Settings - Enable PUSH : 0
- \r\n
- [Response in frame: 2]
- [Full request URI: http://nghttp2.org/robots.txt]

3. Header Differences

HTTP/2 headers appear in compressed binary format, unlike HTTP/1.1 headers which are plain text. This reduces overhead and improves performance, as observed in the packet details.

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.

Name of the student :Priyanka C P

Roll No :TL034

