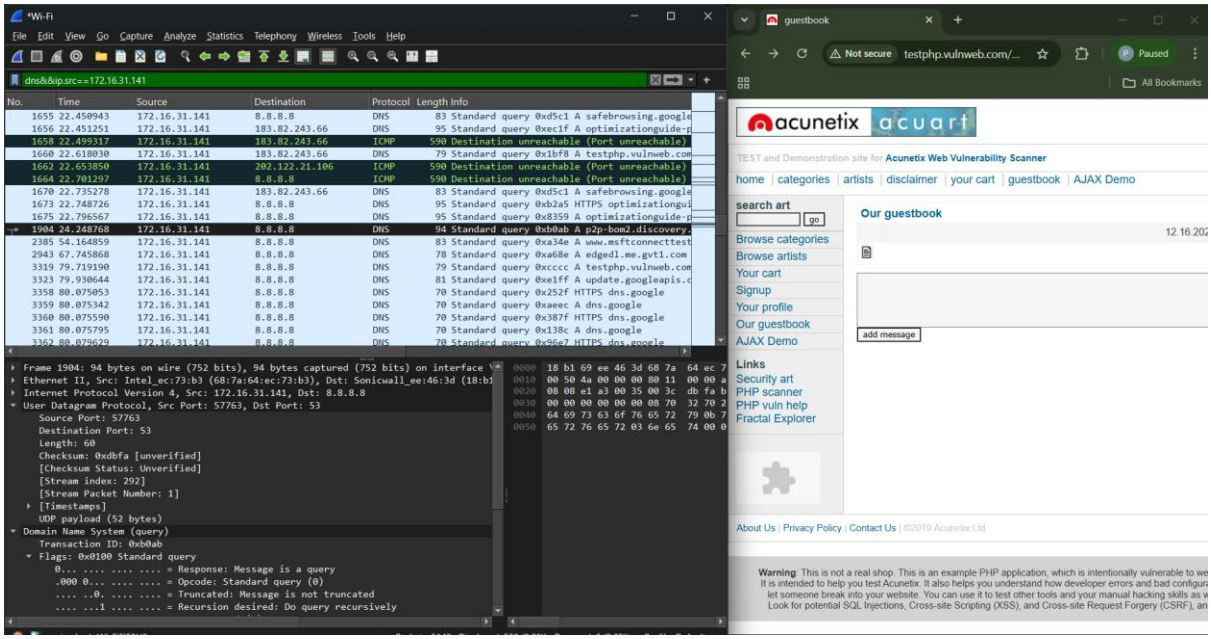
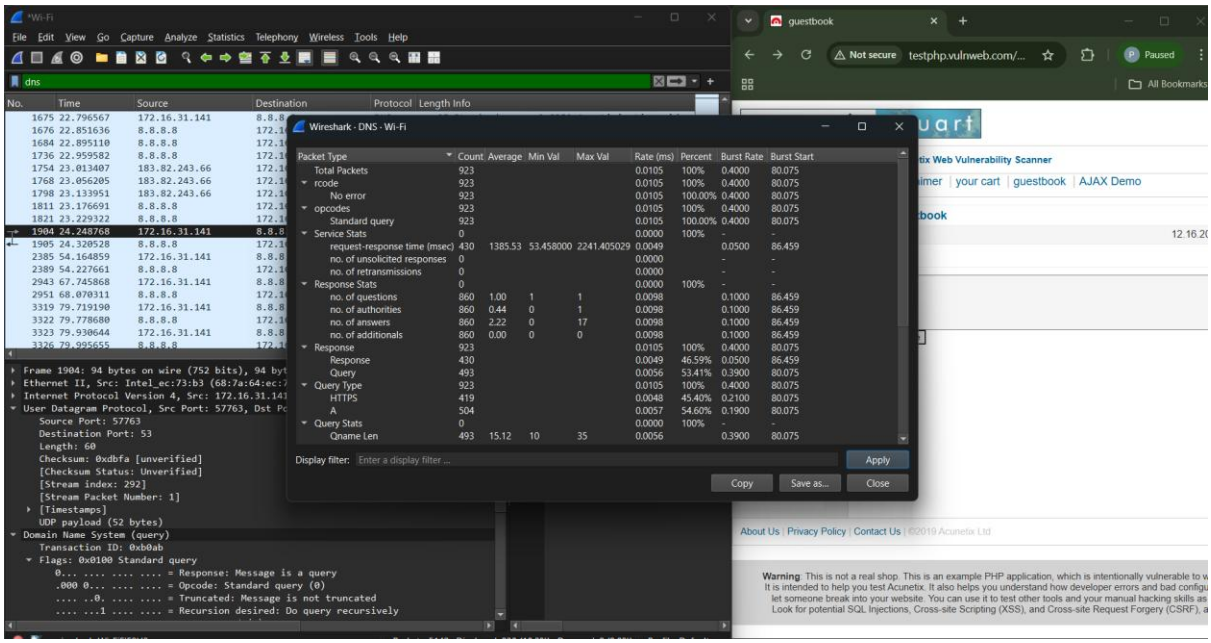
# TASK 1



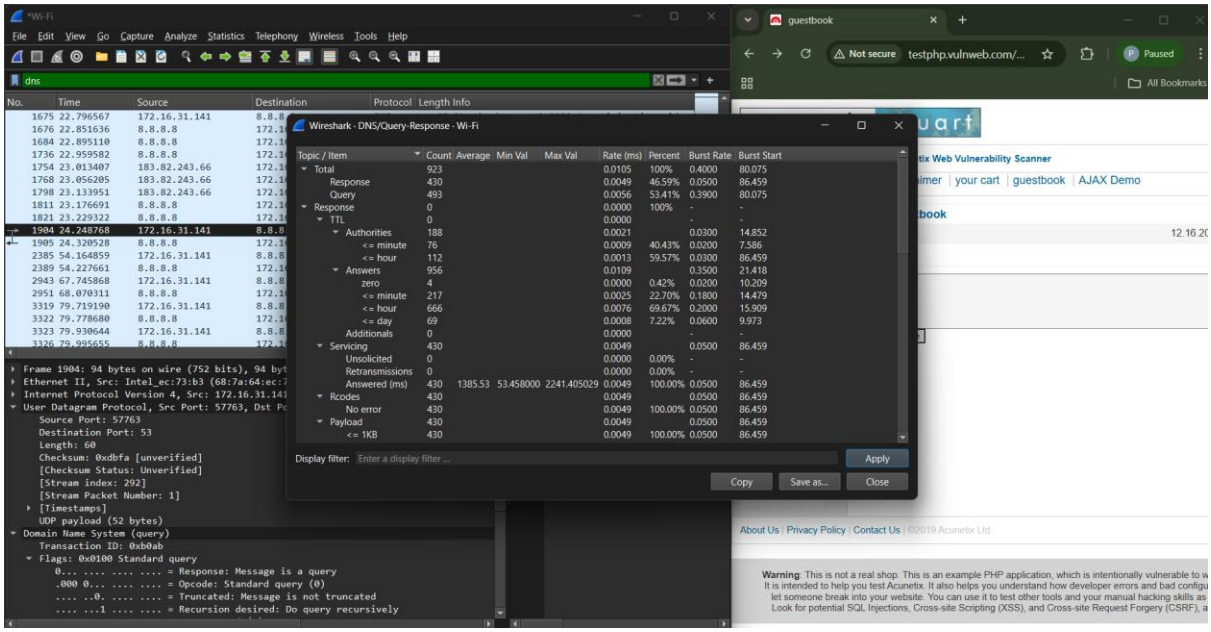
## 1. DNS Queries and DNS Servers

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.



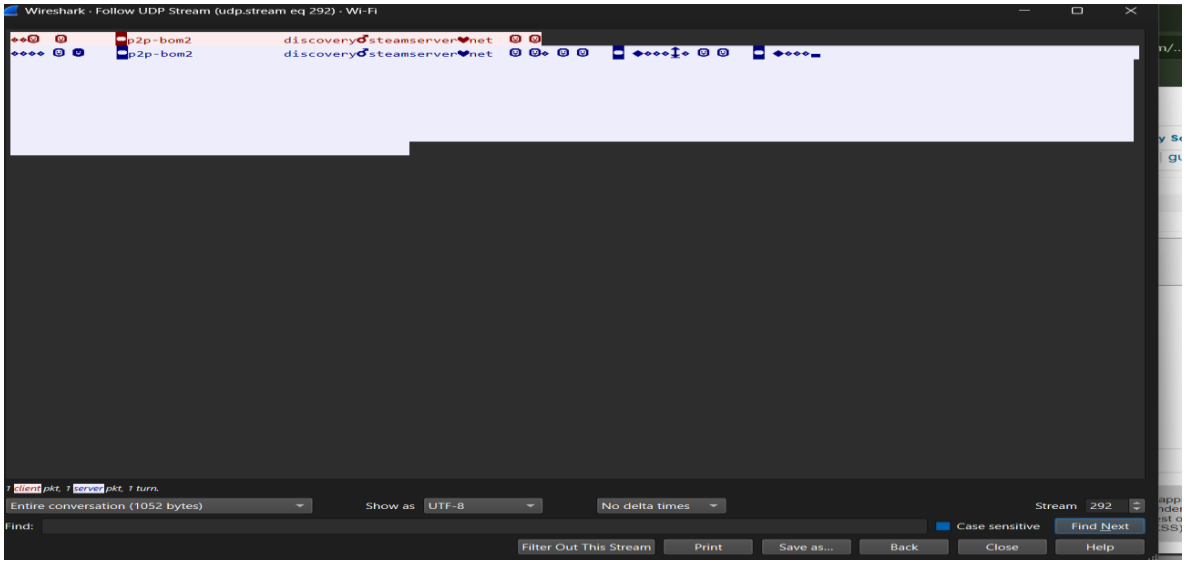
## 2. HTTP Requests and Responses

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.



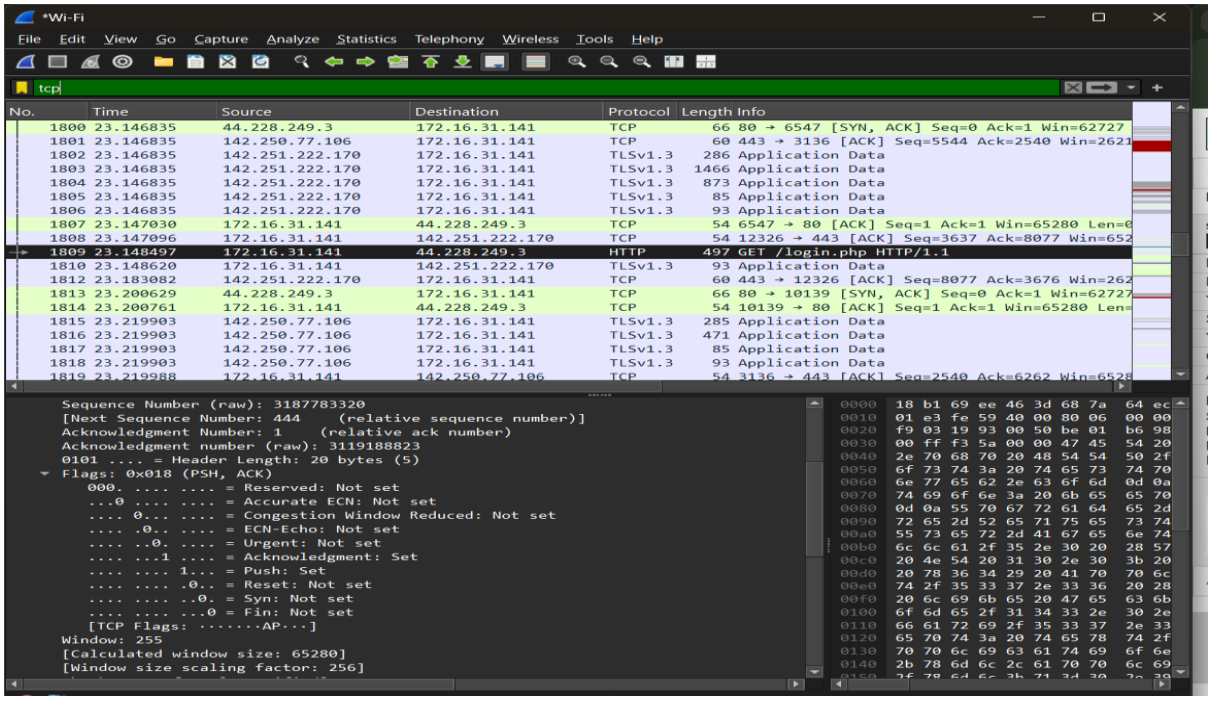

## 3. TCP Connections Established

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

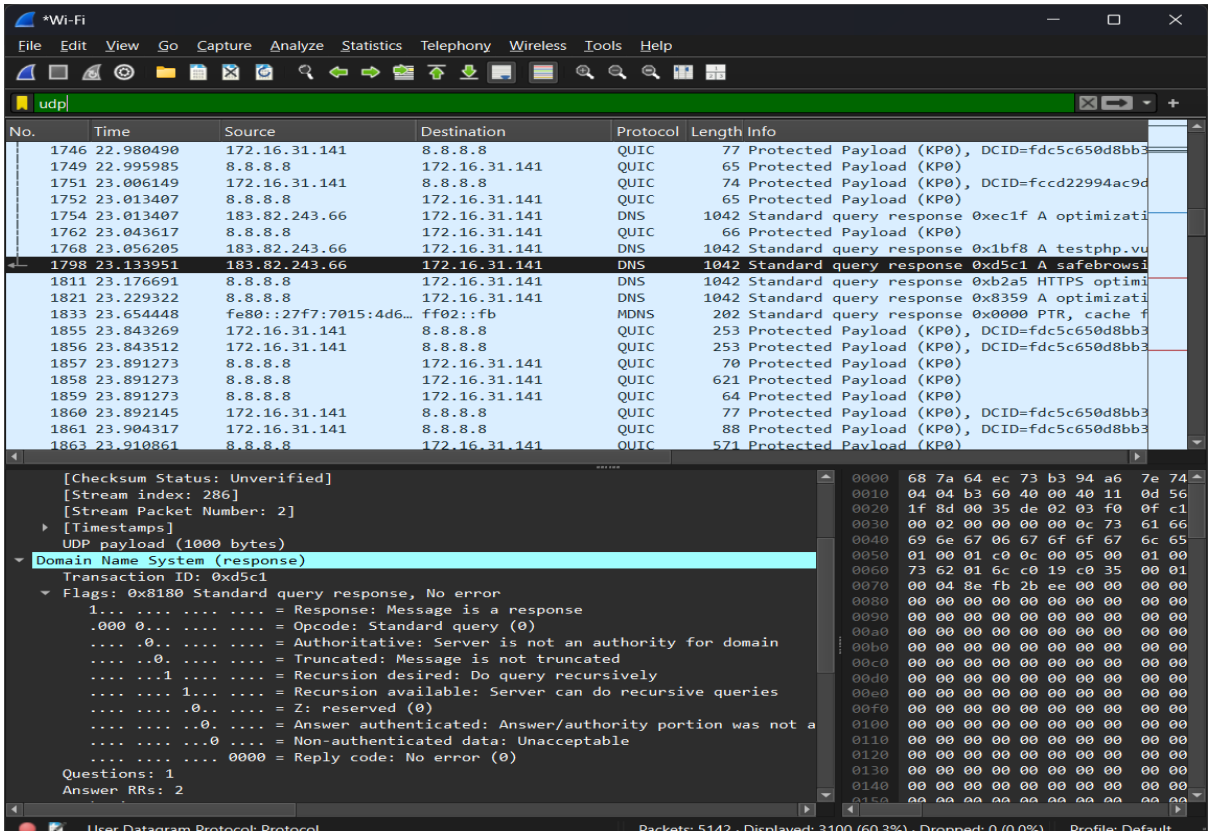
In the TCP handshake packets shown in the screenshot, the **SYN, SYN-ACK, and ACK** sequence can be observed. The time difference between SYN and ACK packets gives the TCP connection setup time. Each TCP stream shows a slightly different establishment delay.




## 5. Browsing Embedded Objects

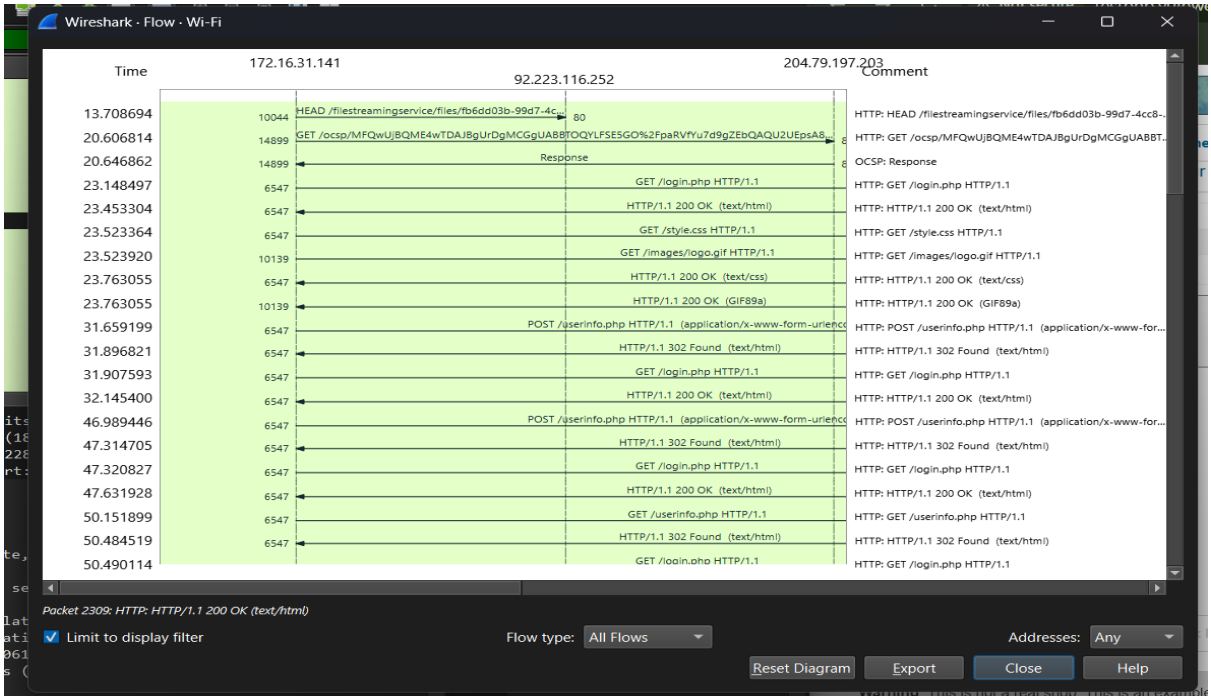
After loading the main guestbook page, the browser automatically requests additional embedded objects. This is visible through multiple HTTP GET

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



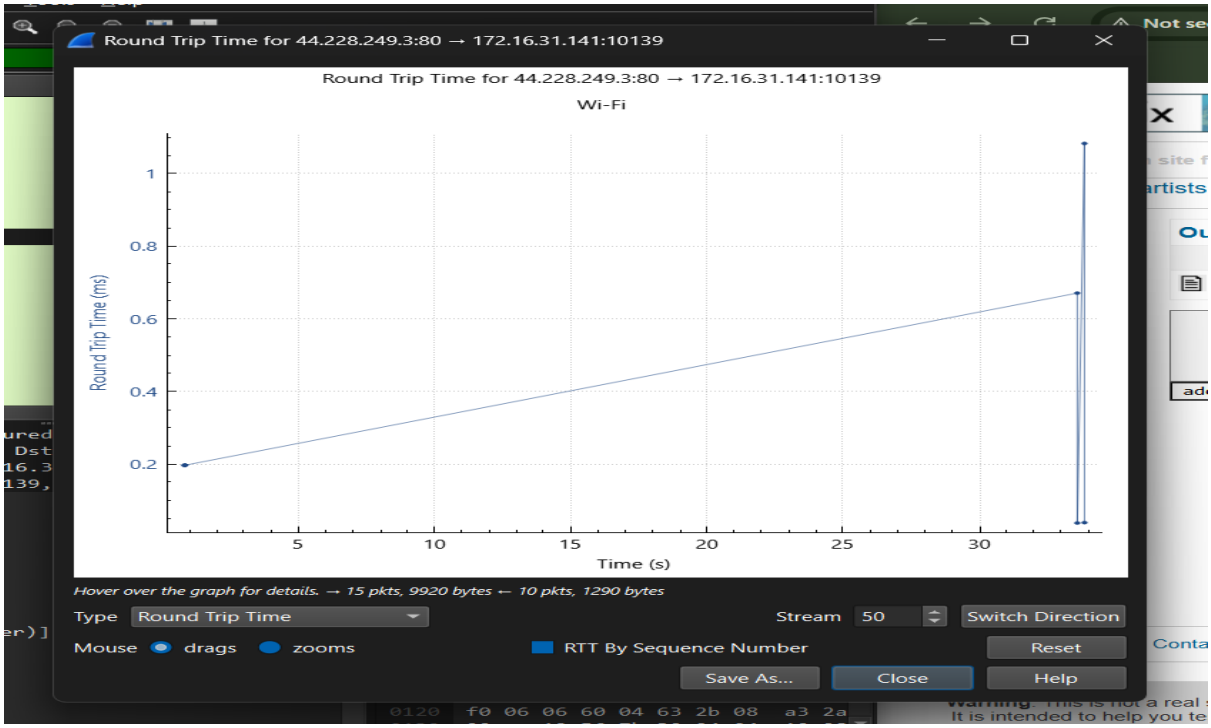

## 6. Number of Objects Downloaded

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.



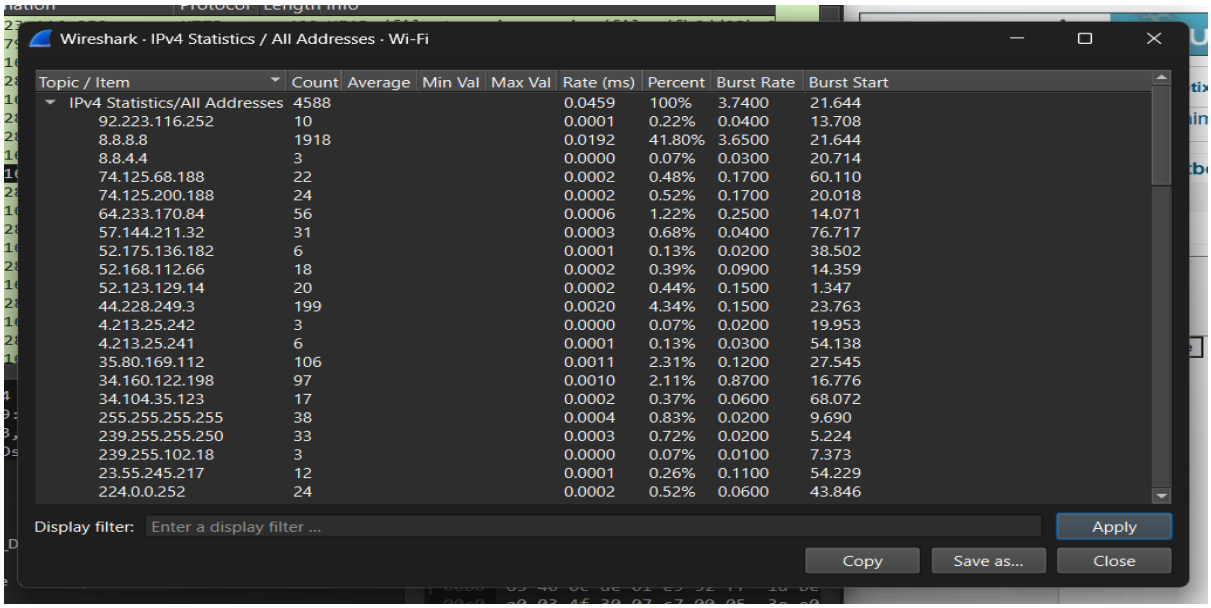

## 7. Object Details (Time, Size, Name, Last-Modified)

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**.**




## 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.

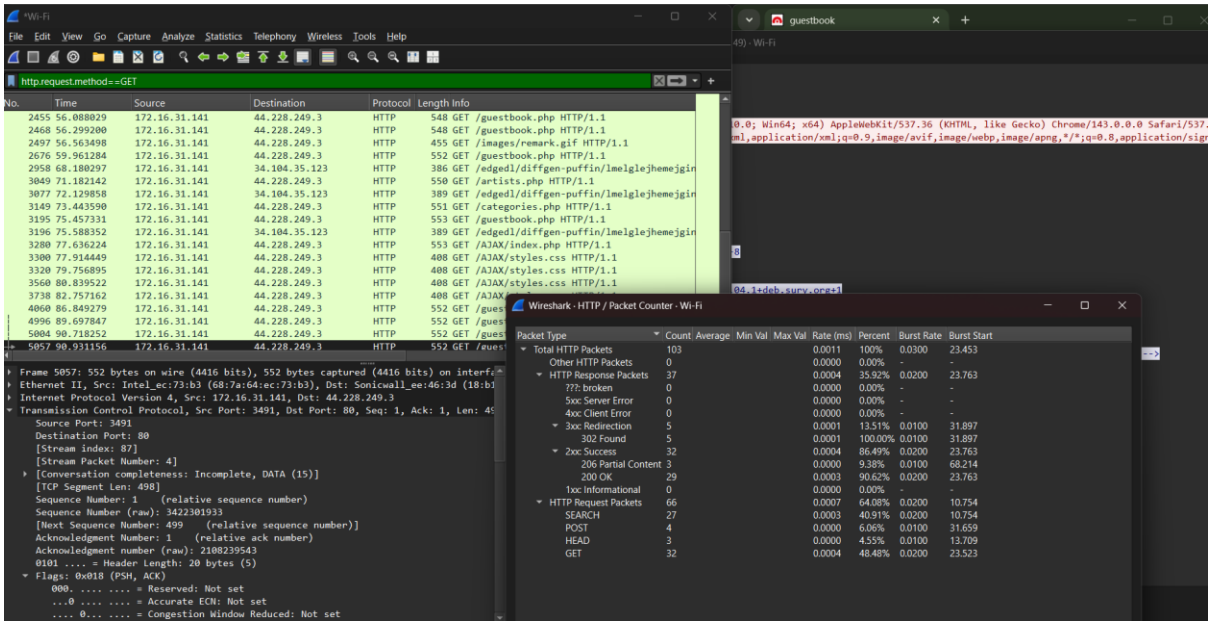
## 10. Keep-Alive Requests

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

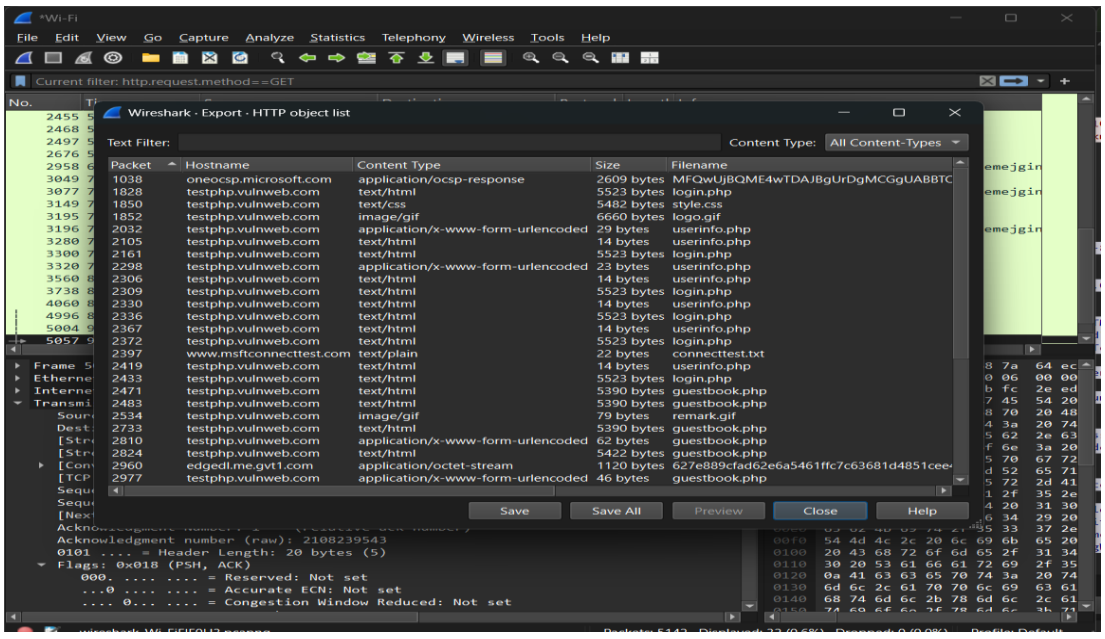
From the HTTP request line in the packet details, the browser is using HTTP/1.1. This is clearly indicated alongside the GET request method.

# TASK 2



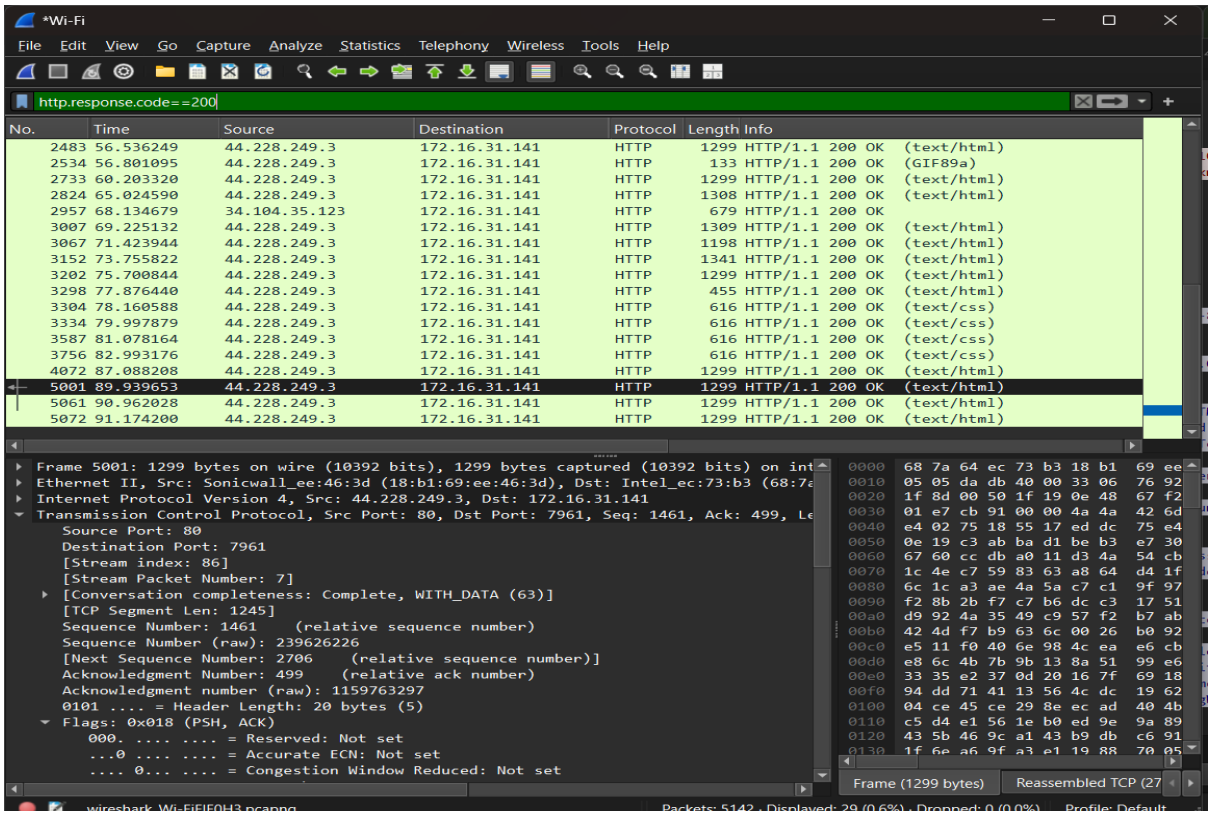

## 1. Conditional GET Requests

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.



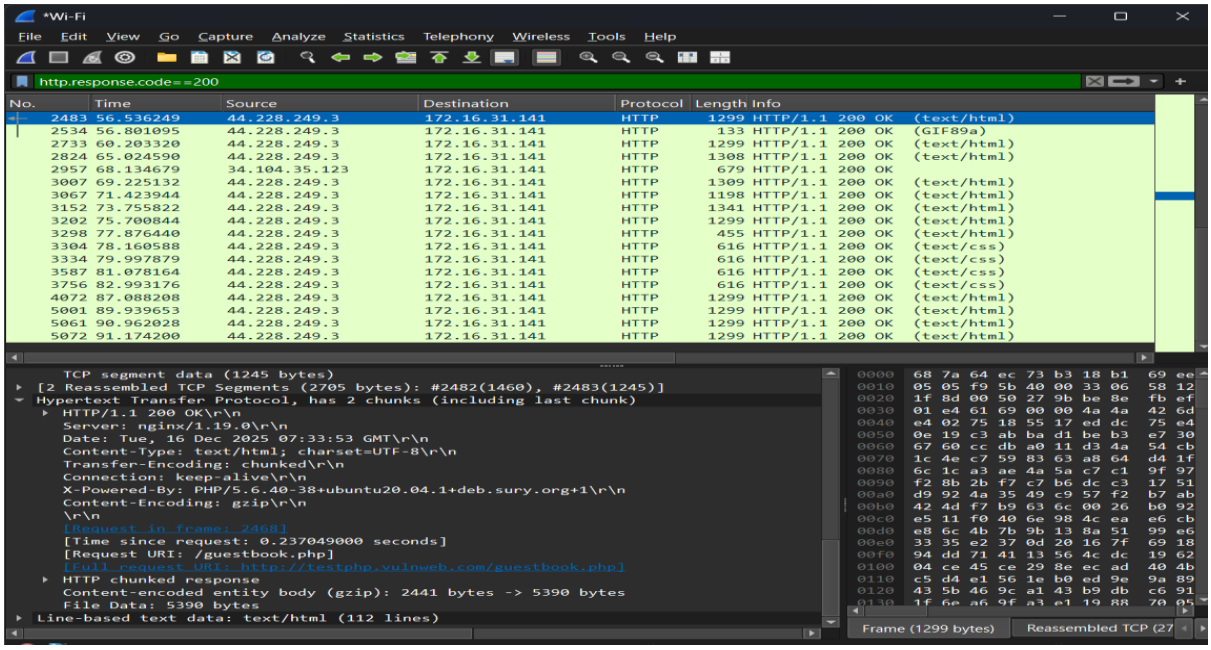
## 2. Full Content Sent by Server

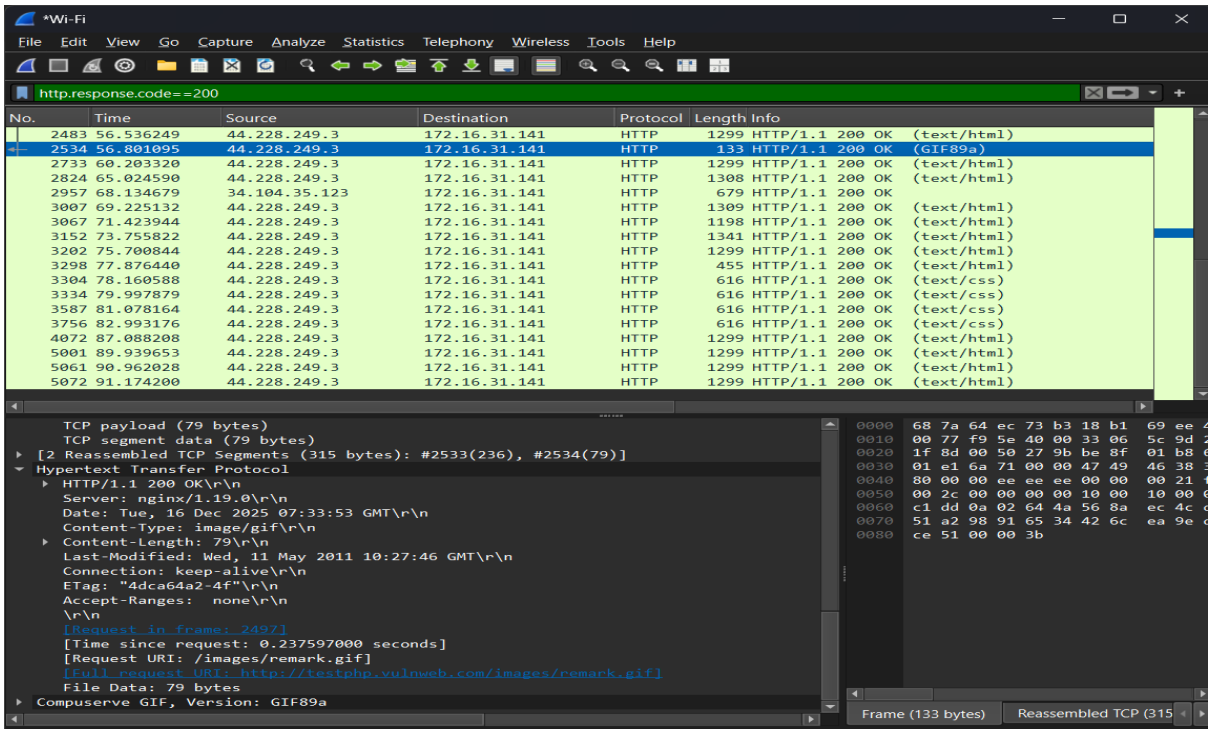
During the first request, the server sends the full content of all requested objects. In the second request, the server does not resend unchanged files completely, showing efficient cache usage. This behavior is visible through response headers.

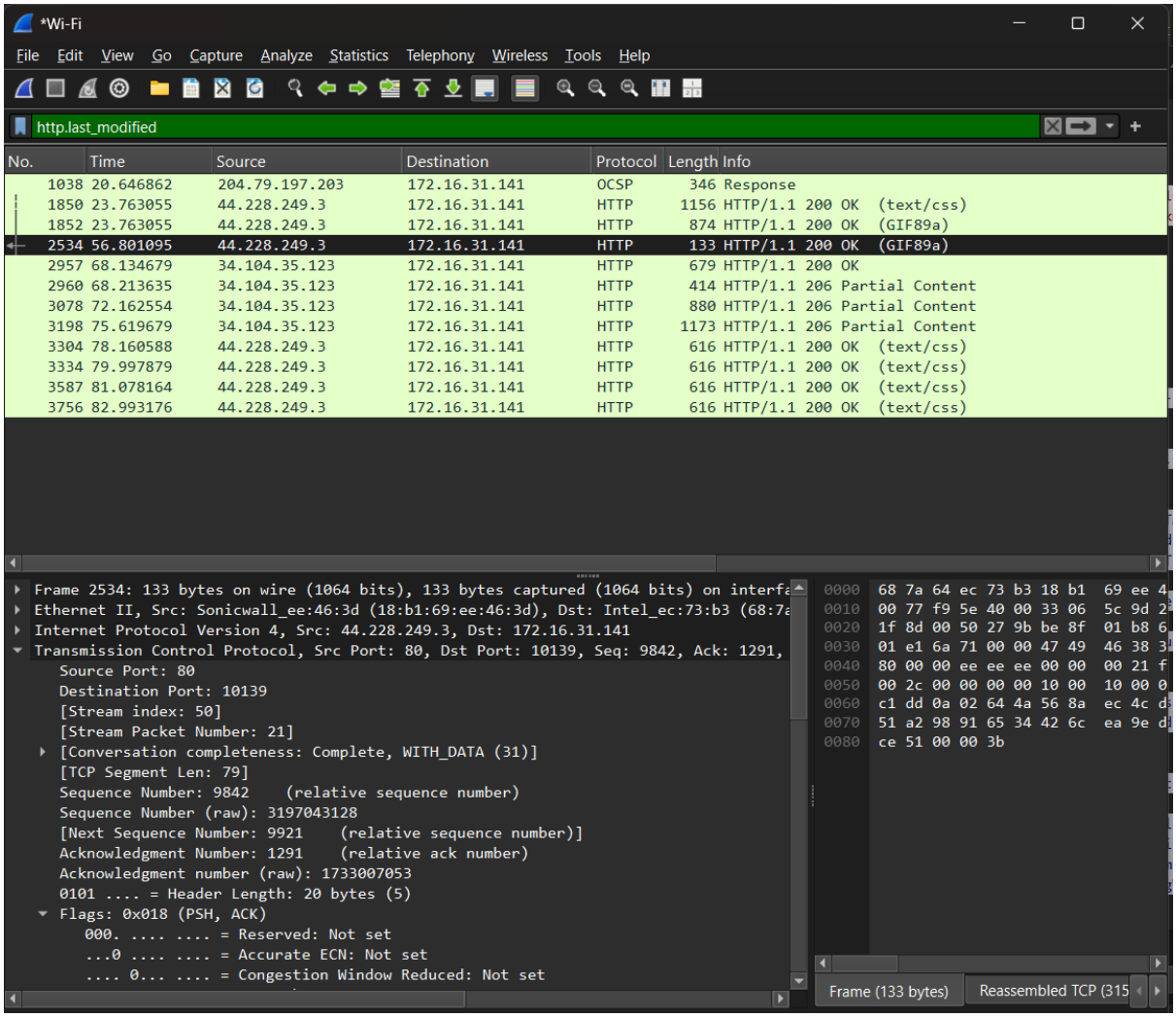



## 3. Difference Between First and Second Request

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
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 (27

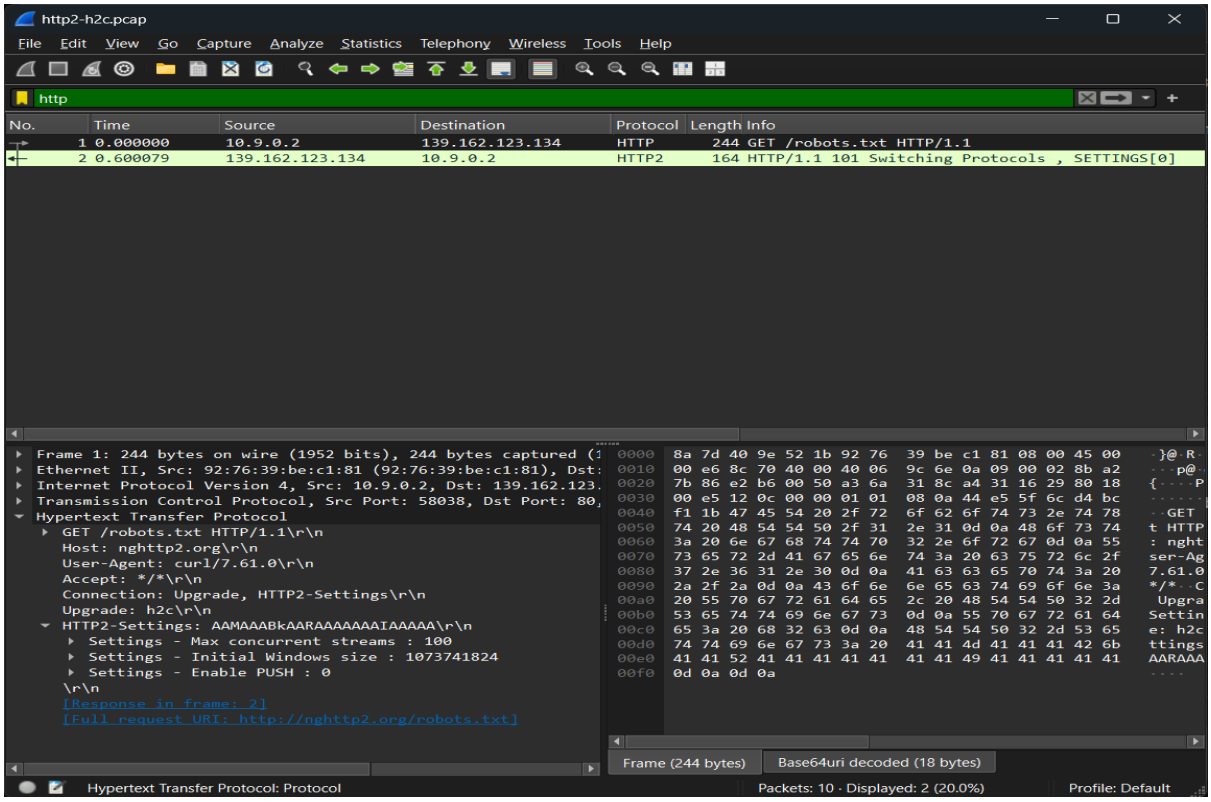

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response.code==200
No. Time Source Destination Protocol Length Info
2483 56.536249 44.228.249.3 172.16.31.141 HTTP 1299 HTTP/1.1 200 OK (text/html)
2534 56.801095 44.228.249.3 172.16.31.141 HTTP 133 HTTP/1.1 200 OK (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
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




## 4. HTTP Headers Responsible

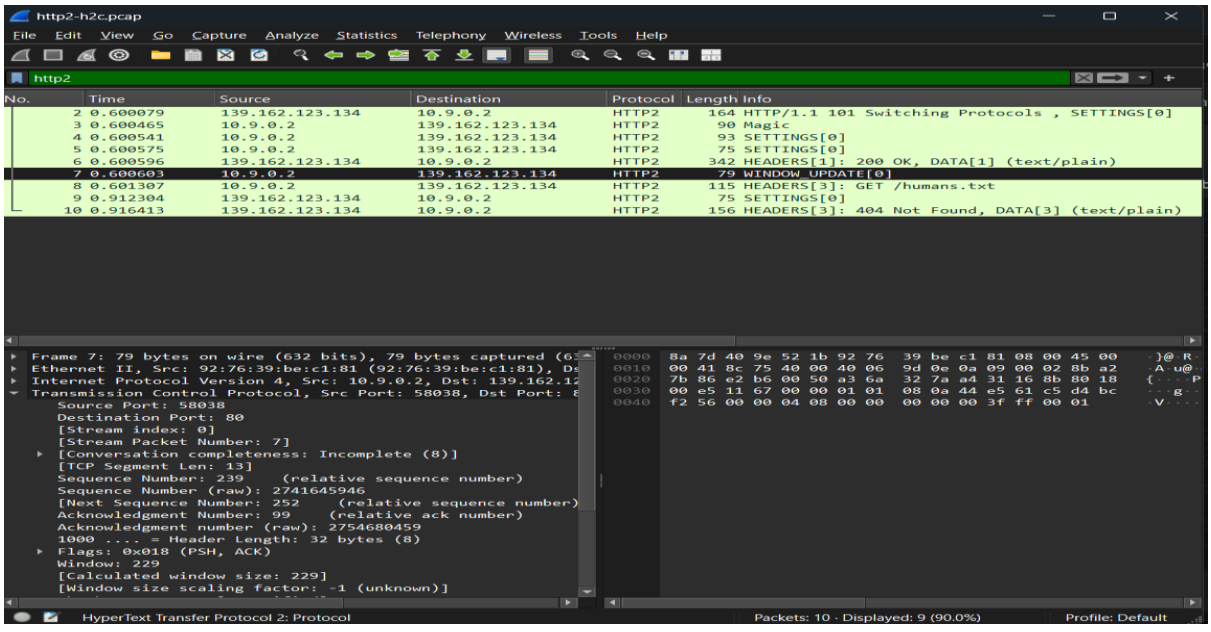
The screenshot shows headers such as If-Modified-Since, If-None-Match, ETag, Last-Modified, and Cache-Control. These headers control caching and conditional requests between the browser and server.

## TASK 3



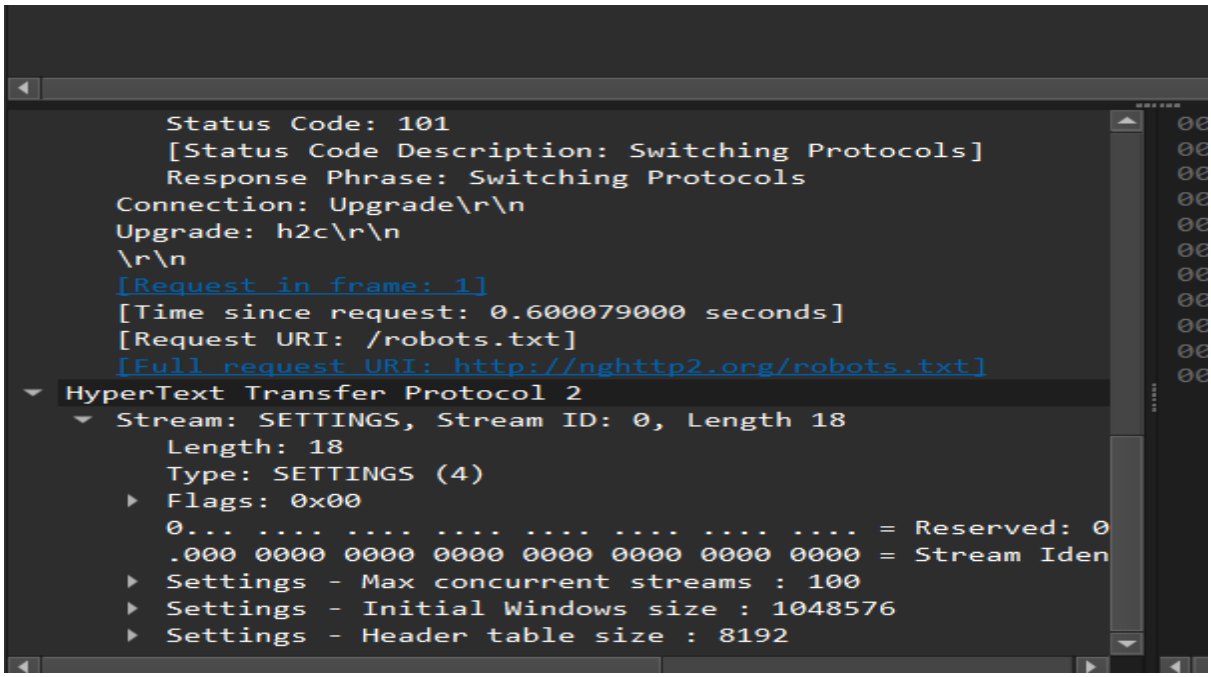

## 1. HTTP/2 vs HTTP/1.1 Packets

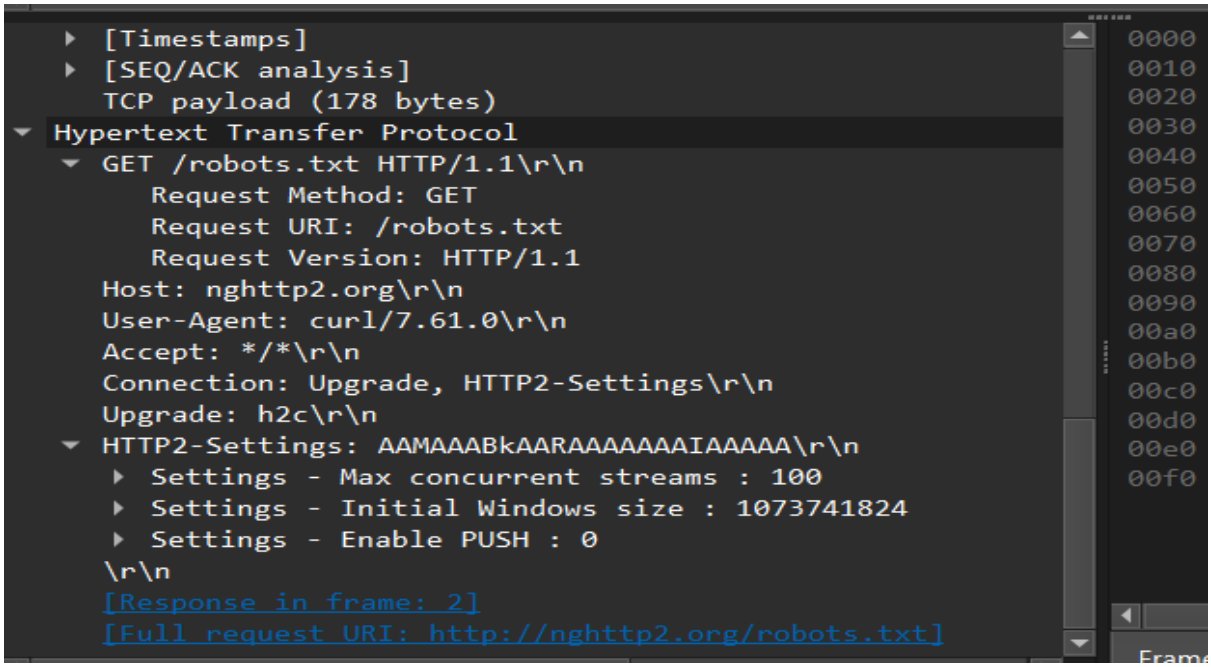
Using Statistics → HTTP / HTTP2, the screenshot shows a higher number of HTTP/2 packets compared to HTTP/1.1 packets. This confirms that most communication in the capture uses HTTP/2.



## 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.



### 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 thework of other students and/or persons. I pledge to up hold the principles of honesty and responsibility at CSE@IITH. Inaddition, 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