Experiment-8

AIM: To capture and analyze HTTP traffic to understand how a basic website operation works, such as request and response between a client (browser) and a server.

Objective: Understand the HTTP protocol, including GET requests, response codes, and the data exchanged between the client and server.

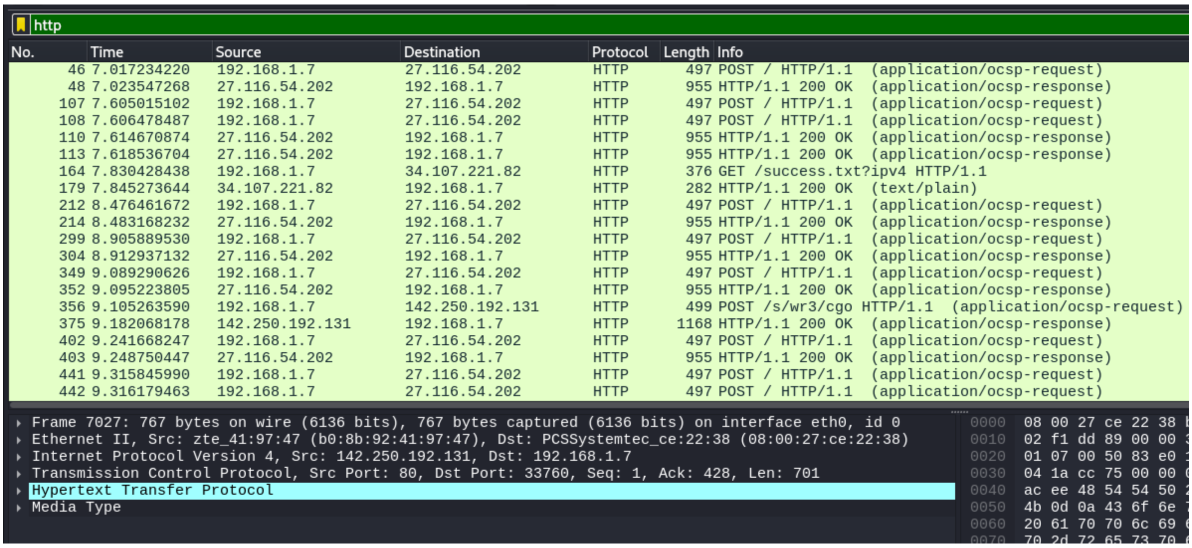
Theory: When you visit a website, your browser sends an HTTP request to the web server to fetch resources (HTML, images, scripts, etc.). The server responds with the requested data. Wireshark can capture these HTTP packets, allowing you to inspect the communication and understand the details of the request-response cycle.

Used **Commands** in Wireshark:

1. Capture HTTP Traffic:

- Start capturing packets (Capture > Start).

- Use the filter http to show only HTTP traffic. This will help you focus on the communication between the client and the server.

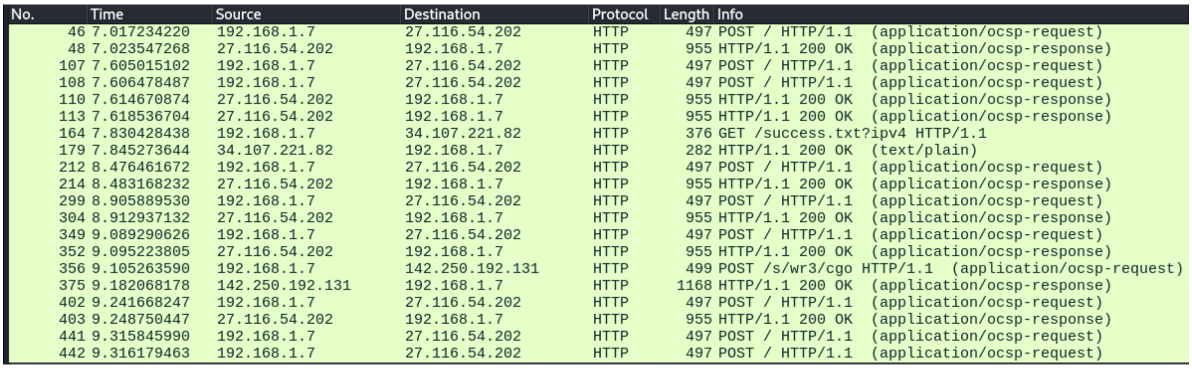


```
http
No.      Time         Source            Destination       Protocol  Length Info
      46 7.017234220  192.168.1.7       27.116.54.202     HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
      48 7.023547268  27.116.54.202     192.168.1.7       HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
     107 7.605015102  192.168.1.7       27.116.54.202     HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
     108 7.606478487  192.168.1.7       27.116.54.202     HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
     110 7.614670874  27.116.54.202     192.168.1.7       HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
     113 7.618536704  27.116.54.202     192.168.1.7       HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
     164 7.830428438  192.168.1.7       34.107.221.82     HTTP       376 GET /success.txt?ipv4 HTTP/1.1
     179 7.845273644  34.107.221.82     192.168.1.7       HTTP       282 HTTP/1.1 200 OK  (text/plain)
     212 8.476461672  192.168.1.7       27.116.54.202     HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
     214 8.483168232  27.116.54.202     192.168.1.7       HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
     299 8.905889530  192.168.1.7       27.116.54.202     HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
     304 8.912937132  27.116.54.202     192.168.1.7       HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
     349 9.089290626  192.168.1.7       27.116.54.202     HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
     352 9.095223805  27.116.54.202     192.168.1.7       HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
     356 9.105263590  192.168.1.7       142.250.192.131   HTTP       499 POST /s/wr3/cgo HTTP/1.1  (application/ocsp-request)
     375 9.182068178  142.250.192.131   192.168.1.7       HTTP      1168 HTTP/1.1 200 OK  (application/ocsp-response)
     402 9.241668247  192.168.1.7       27.116.54.202     HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
     403 9.248750447  27.116.54.202     192.168.1.7       HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
     441 9.315845990  192.168.1.7       27.116.54.202     HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
     442 9.316179463  192.168.1.7       27.116.54.202     HTTP       497 POST / HTTP/1.1  (application/ocsp-request)

▸ Frame 7027: 767 bytes on wire (6136 bits), 767 bytes captured (6136 bits) on interface eth0, id 0    0000  08 00 27 ce 22 38
▸ Ethernet II, Src: zte_41:97:47 (b0:8b:92:41:97:47), Dst: PCSSystemtec_ce:22:38 (08:00:27:ce:22:38)  0010  02 f1 dd 89 00 00
▸ Internet Protocol Version 4, Src: 142.250.192.131, Dst: 192.168.1.7                                 0020  01 07 00 50 83 e0
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 33760, Seq: 1, Ack: 428, Len: 701           0030  04 1a cc 75 00 00
▸ Hypertext Transfer Protocol                                                                          0040  ac ee 48 54 54 50
▸ Media Type                                                                                           0050  4b 0d 0a 43 6f 6e
                                                                                                       0060  20 61 70 70 6c 69
                                                                                                       0070  70 2d 72 65 73 70
```

2. Analyze HTTP Request:

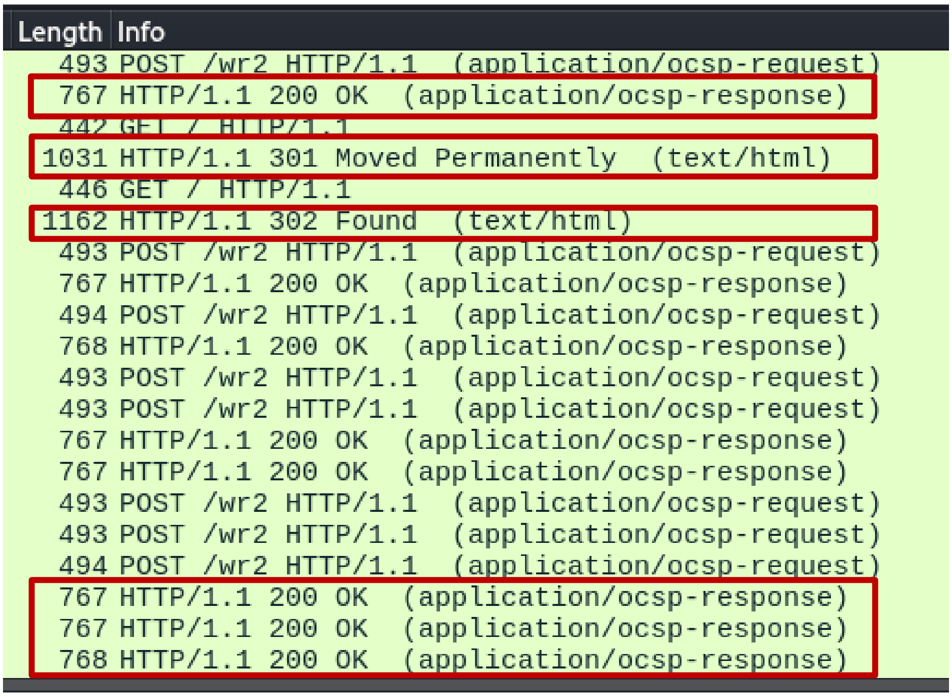
- Look at the packets captured to find HTTP GET/POST requests. For example, you will see GET requests like GET /index.html HTTP/1.1.



```
No.    Time          Source           Destination      Protocol  Length Info
    46 7.017234220   192.168.1.7      27.116.54.202    HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
    48 7.023547268   27.116.54.202    192.168.1.7      HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
   107 7.605015102   192.168.1.7      27.116.54.202    HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
   108 7.606478487   192.168.1.7      27.116.54.202    HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
   110 7.614670874   27.116.54.202    192.168.1.7      HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
   113 7.618536704   27.116.54.202    192.168.1.7      HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
   164 7.830428438   192.168.1.7      34.107.221.82    HTTP       376 GET /success.txt?ipv4 HTTP/1.1
   179 7.845273644   34.107.221.82    192.168.1.7      HTTP       282 HTTP/1.1 200 OK  (text/plain)
   212 8.476461672   192.168.1.7      27.116.54.202    HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
   214 8.483168232   27.116.54.202    192.168.1.7      HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
   299 8.905889530   192.168.1.7      27.116.54.202    HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
   304 8.912937132   27.116.54.202    192.168.1.7      HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
   349 9.089290626   192.168.1.7      27.116.54.202    HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
   352 9.095223805   27.116.54.202    192.168.1.7      HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
   356 9.105263590   192.168.1.7      142.250.192.131  HTTP       499 POST /s/wr3/cgo HTTP/1.1  (application/ocsp-request)
   375 9.182068178   142.250.192.131  192.168.1.7      HTTP      1168 HTTP/1.1 200 OK  (application/ocsp-response)
   402 9.241668247   192.168.1.7      27.116.54.202    HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
   403 9.248750447   27.116.54.202    192.168.1.7      HTTP       955 HTTP/1.1 200 OK  (application/ocsp-response)
   441 9.315845990   192.168.1.7      27.116.54.202    HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
   442 9.316179463   192.168.1.7      27.116.54.202    HTTP       497 POST / HTTP/1.1  (application/ocsp-request)
```

3. HTTP Response:

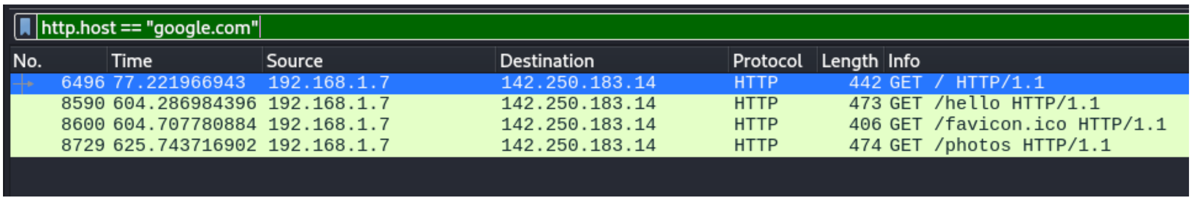
- Find HTTP response packets, which will have status codes like 200 OK, 301 Moved Permanently, 302 Found, etc. The response will include the body of the HTML or other resources.



```
Length Info
  493 POST /wr2 HTTP/1.1  (application/ocsp-request)
  767 HTTP/1.1 200 OK  (application/ocsp-response)
  442 GET / HTTP/1.1
 1031 HTTP/1.1 301 Moved Permanently  (text/html)
  446 GET / HTTP/1.1
 1162 HTTP/1.1 302 Found  (text/html)
  493 POST /wr2 HTTP/1.1  (application/ocsp-request)
  767 HTTP/1.1 200 OK  (application/ocsp-response)
  494 POST /wr2 HTTP/1.1  (application/ocsp-request)
  768 HTTP/1.1 200 OK  (application/ocsp-response)
  493 POST /wr2 HTTP/1.1  (application/ocsp-request)
  493 POST /wr2 HTTP/1.1  (application/ocsp-request)
  767 HTTP/1.1 200 OK  (application/ocsp-response)
  767 HTTP/1.1 200 OK  (application/ocsp-response)
  493 POST /wr2 HTTP/1.1  (application/ocsp-request)
  493 POST /wr2 HTTP/1.1  (application/ocsp-request)
  494 POST /wr2 HTTP/1.1  (application/ocsp-request)
  767 HTTP/1.1 200 OK  (application/ocsp-response)
  767 HTTP/1.1 200 OK  (application/ocsp-response)
  768 HTTP/1.1 200 OK  (application/ocsp-response)
```

4. Filter by Host:

- Use the filter http.host == "google.com" to see the HTTP traffic specifically for a particular website.



```
http.host == "google.com"

No.    Time            Source        Destination      Protocol  Length Info
  6496 77.221966943    192.168.1.7   142.250.183.14   HTTP        442 GET / HTTP/1.1
  8590 604.286984396   192.168.1.7   142.250.183.14   HTTP        473 GET /hello HTTP/1.1
  8600 604.707780884   192.168.1.7   142.250.183.14   HTTP        406 GET /favicon.ico HTTP/1.1
  8729 625.743716902   192.168.1.7   142.250.183.14   HTTP        474 GET /photos HTTP/1.1
```

Conclusion: In this experiment, we successfully captured and analyzed HTTP traffic using Wireshark to understand the fundamental operation of a website. By focusing on the communication between a client (browser) and a server, we observed the **request-response cycle** of the HTTP protocol.