

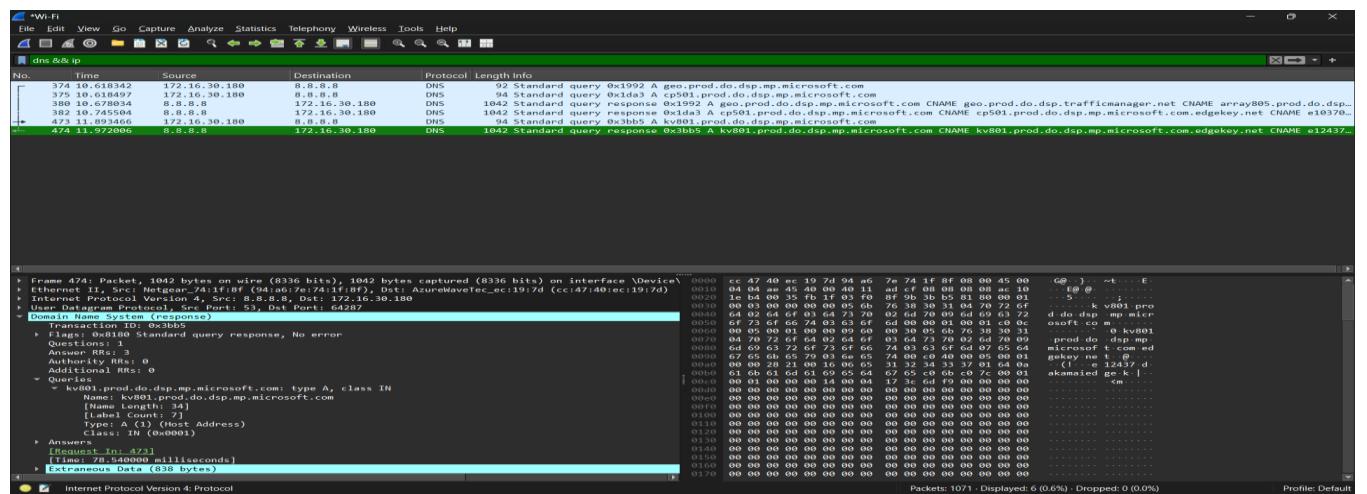
Task 1.1 How many DNS queries are sent from your browser (host machine) to DNS Server(s)?

DNS/Query-Response:

| Topic / Item | Count | Average | Min Val | Max Val | Rate (ms) | Percent | Burst |
|--------------|-------------|---------|---------|---------|-----------|---------|-------|
| Rate | Burst Start | | | | | | |
| <hr/> | | | | | | | |
| Total | 27 | | 0.0003 | 100% | 0.0300 | 13.444 | |

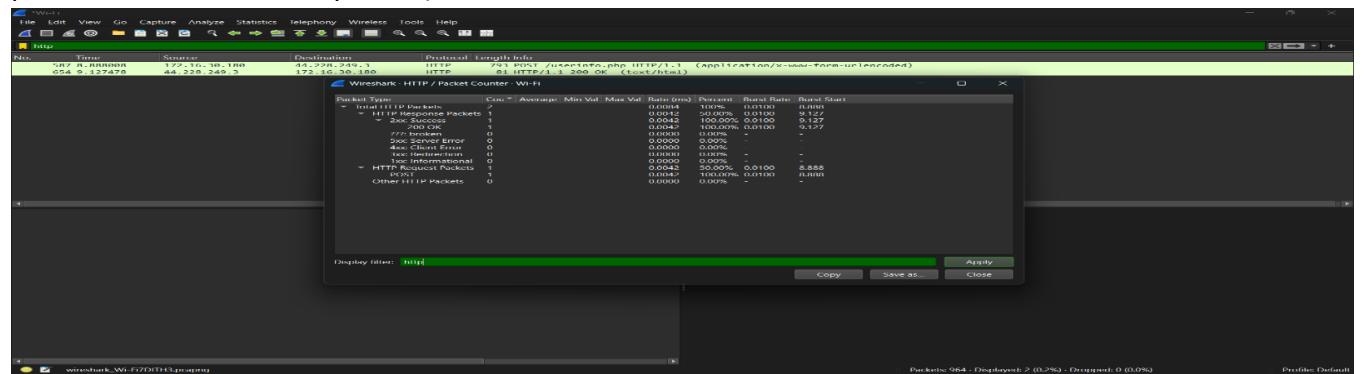
1.2 How many DNS servers are involved ?

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 this time taken value for each of the TCP connection(s).

| Conversation Settings | Ethernet | 96 | IPv4 | 53 | IPv6 | 62 | TCP | 13 | UDP | 81 | 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 |
|-------------------------|----------------|----------------|-------|-----------------|-----------------|-------|-----|-----------|-----------|-------|------------------|-----------|---------|-------------|-----------|---------------|-------------|---------------|--------------|-----------|----------|--------|
| Name resolution | ✓ | 0.0.0.1 | | 68 | 255.255.255.255 | | 67 | 10 | 3 kB | 21 | 10 | 3 kB | 0 | 0 bytes | 208 bytes | 0 | 0 bytes | 1 | 10.11.11.111 | 17.2038 | 1585 | |
| Absolute start time | ✓ | 17.2.16.1.41 | | 219 | 255.255.255.255 | | 219 | 10 | 3 kB | 21 | 10 | 3 kB | 0 | 0 bytes | 208 bytes | 0 | 0 bytes | 1 | 10.11.11.111 | 17.2038 | 1585 | |
| Display raw data | ✓ | 17.2.16.30.11 | | 67 | 255.255.255.255 | | 68 | 1 | 295 bytes | 22 | 1 | 295 bytes | 0 | 0 bytes | 295 bytes | 0 | 0 bytes | 1 | 7.681567 | 0.0000 | | |
| Limit to display filter | ✓ | 17.2.16.30.111 | | 528 | 255.255.255.255 | | 528 | 1 | 295 bytes | 60 | 1 | 295 bytes | 0 | 0 bytes | 295 bytes | 0 | 0 bytes | 1 | 7.681567 | 0.0000 | | |
| | 17.2.16.30.111 | | 5353 | 2.24.0.25 | | 5353 | 2 | 594 bytes | 25 | 2 | 594 bytes | 0 | 0 bytes | 594 bytes | 0 | 0 bytes | 1 | 8.009690 | 23.0392 | 206 | | |
| | 17.2.16.30.119 | | 5062 | 255.255.255.255 | | 5062 | 10 | 2 kB | 52 | 2 | 2 kB | 0 | 0 bytes | 1024 bytes | 0 | 0 bytes | 1 | 10.11.11.111 | 17.2038 | 1585 | | |
| | 17.2.16.30.131 | | 5353 | 2.24.0.25 | | 5353 | 1 | 327 bytes | 60 | 1 | 327 bytes | 0 | 0 bytes | 327 bytes | 0 | 0 bytes | 1 | 26.113444 | 0.0000 | | | |
| | 17.2.16.30.140 | | 57846 | 8.8.8.8 | | 443 | 1 | 12 kB | 6 | 1 | 12 kB | 12 | 1 kB | 12 kB | 0 | 0 bytes | 1 | 10.11.11.111 | 0.0000 | 40 | | |
| | 17.2.16.30.140 | | 7000 | 8.8.8.8 | | 443 | 1 | 12 kB | 31 | 1 | 12 kB | 31 | 1 kB | 12 kB | 0 | 0 bytes | 1 | 10.11.11.111 | 0.0000 | 40 | | |
| | 17.2.16.30.180 | | 56914 | 8.8.8.8 | | 443 | 31 | 11 kB | 68 | 14 | 4 kB | 17 | 7 kB | 29.500728 | 0.2949 | | | | | | | |
| | 17.2.16.30.180 | | 56914 | 8.8.8.8 | | 443 | 31 | 11 kB | 68 | 14 | 4 kB | 17 | 7 kB | 29.500728 | 0.2949 | | | | | | | |
| | 17.2.16.30.180 | | 55961 | 142.250.66.3 | | 443 | 150 | 11 kB | 71 | 93 | 10 kB | 57 | 5 kB | 5.808999 | 0.7649 | | | | | | | |
| | 17.2.16.30.180 | | 55961 | 142.250.66.3 | | 443 | 35 | 11 kB | 103 | 11 | 10 kB | 57 | 5 kB | 5.808999 | 0.7649 | | | | | | | |
| | 17.2.16.30.180 | | 55962 | 142.250.133.164 | | 443 | 1 | 137 bytes | 53 | 1 | 137 bytes | 1 | 1 kB | 137 bytes | 0.137 | 0 bytes | 1 | 10.11.11.111 | 17.2038 | 1585 | | |
| | 17.2.16.30.180 | | 56914 | 8.8.8.8 | | 443 | 1 | 137 bytes | 53 | 1 | 137 bytes | 1 | 1 kB | 137 bytes | 0.137 | 0 bytes | 1 | 60.192153 | 0.0677 | | | |
| | 17.2.16.30.180 | | 54179 | 142.251.221.202 | | 443 | 200 | 18 kB | 70 | 59 | 9 kB | 141 | 17.1 kB | 29.767553 | 0.2944 | | | | | | | |
| | 17.2.16.30.180 | | 56926 | 142.251.221.202 | | 443 | 25 | 10 kB | 123 | 12 | 9 kB | 141 | 17.1 kB | 29.767553 | 0.2944 | | | | | | | |
| | 17.2.16.30.180 | | 56926 | 142.251.221.202 | | 443 | 20 | 10 kB | 119 | 8 | 4 kB | 12 | 6 kB | 7.5636699 | 0.103811 | | | | | | | |
| | 17.2.16.30.180 | | 49664 | 142.251.221.196 | | 443 | 1 | 1 kB | 41 | 26 kB | 19 | 1 kB | 20 | 20 kB | 0 | 0 bytes | 6 kB | 10.562431 | 0.394033 | 45 | | |
| | 17.2.16.30.180 | | 5353 | 17.2.16.30.180 | | 5353 | 1 | 1 kB | 28 | 1 kB | 28 | 1 kB | 0 | 0 bytes | 10.611964 | 0.0000 | | | | | | |
| | 17.2.16.30.185 | | 5353 | 17.2.16.30.180 | | 5353 | 1 | 291 bytes | 31 | 1 | 291 bytes | 0 | 0 bytes | 291 bytes | 0 | 0 bytes | 1 | 10.611964 | 0.0000 | | | |
| | 17.2.16.30.190 | | 5353 | 17.2.16.30.180 | | 5353 | 1 | 137 bytes | 71 | 1 | 137 bytes | 0 | 0 bytes | 137 bytes | 0.137 | 0 bytes | 1 | 10.11.11.111 | 17.2038 | 1585 | | |
| | 17.2.16.30.190 | | 5353 | 17.2.16.30.180 | | 5353 | 1 | 255 bytes | 49 | 1 | 255 bytes | 0 | 0 bytes | 255 bytes | 0 | 0 bytes | 1 | 11.167008 | 0.0000 | | | |
| | 17.2.16.30.190 | | 49664 | 142.251.221.196 | | 5353 | 10 | 10 kB | 10 | 10 | 2 kB | 0 | 0 bytes | 11.167008 | 0.0000 | | | | | | | |
| | 17.2.16.30.190 | | 5353 | 2.24.0.25 | | 5353 | 10 | 2 kB | 0 | 10 | 2 kB | 0 | 0 bytes | 1.2287568 | 0.375 | | | | | | | |
| | 17.2.16.30.190 | | 5353 | 2.24.0.25 | | 5353 | 1 | 8 kB | 65 | 5 | 4 kB | 0 | 0 bytes | 8 kB | 0.0000 | | | | | | | |
| | 17.2.16.30.201 | | 49711 | 2.24.0.25 | | 5355 | 2 | 150 bytes | 65 | 2 | 150 bytes | 0 | 0 bytes | 2.150 bytes | 0 | 0 bytes | 1 | 28.571068 | 0.3076 | 3901 | | |
| | 17.2.16.30.201 | | 52933 | 2.24.0.25 | | 5355 | 2 | 150 bytes | 67 | 2 | 150 bytes | 0 | 0 bytes | 2.150 bytes | 0 | 0 bytes | 1 | 28.571068 | 0.3076 | 3916 | | |
| | 17.2.16.30.201 | | 52933 | 2.24.0.25 | | 5355 | 1 | 150 bytes | 63 | 1 | 150 bytes | 0 | 0 bytes | 1.150 bytes | 0.150 | 0 bytes | 1 | 30.712139 | 0.6134 | 1956 | | |
| | 17.2.16.30.201 | | 52934 | 2.24.0.25 | | 5355 | 2 | 150 bytes | 73 | 2 | 150 bytes | 0 | 0 bytes | 2.150 bytes | 0 | 0 bytes | 1 | 30.712139 | 0.6134 | 1976 | | |
| | 17.2.16.30.201 | | 52934 | 2.24.0.25 | | 5355 | 2 | 150 bytes | 73 | 2 | 150 bytes | 0 | 0 bytes | 2.150 bytes | 0 | 0 bytes | 1 | 30.712139 | 0.6134 | 1976 | | |
| | 17.2.16.31.15 | | 57621 | 17.2.16.31.255 | | 57621 | 1 | 86 bytes | 27 | 1 | 86 bytes | 0 | 0 bytes | 86 bytes | 0.086 | 0 bytes | 1 | 9.036064 | 0.0000 | | | |

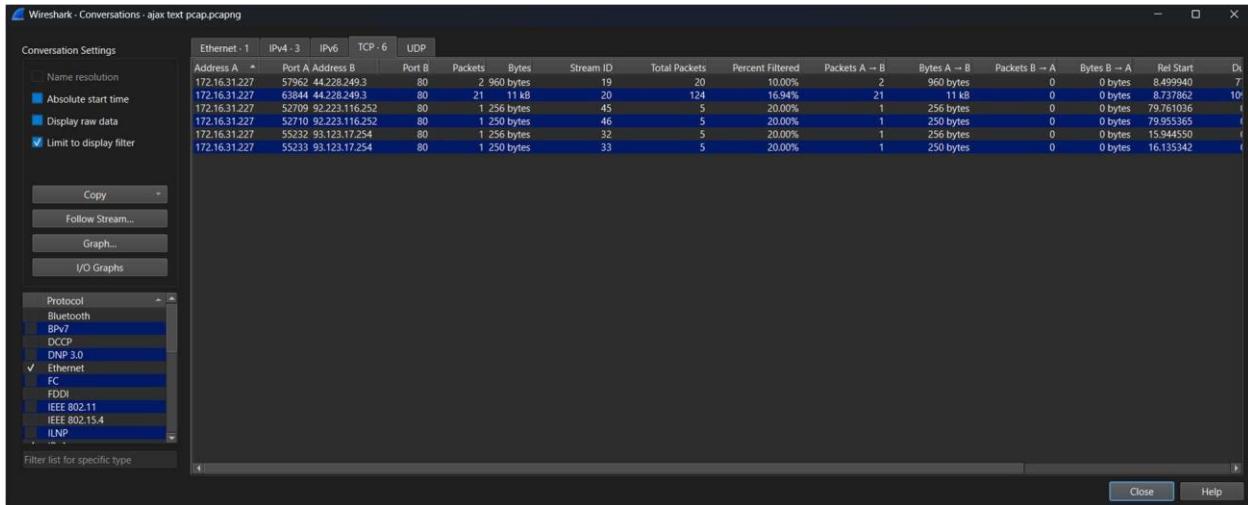
5) Browse the website by moving to various sub links, embedded objects listed in the site.

| No | Time | Source | Destination | Protocol | Length | Info |
|------|------------|---------------|---------------|----------|--------|---|
| 1099 | 11.767464 | 172.16.31.227 | 44.228.249.3 | HTTP | 549 | /login.php HTTP/1.1 |
| 1107 | 12.012670 | 44.228.249.3 | 172.16.31.227 | HTTP | 1342 | HTTP/1.1 200 OK (text/html) |
| 1115 | 12.013777 | 172.16.31.227 | 44.228.249.3 | HTTP | 137 | HTTP/1.1 200 OK (text/css) |
| 1111 | 12.054626 | 172.16.31.227 | 44.228.249.3 | HTTP | 463 | GET /images/logo.gif HTTP/1.1 |
| 1112 | 12.054626 | 172.16.31.227 | 172.16.31.227 | HTTP | 160 | HTTP/1.1 200 OK (text/html) |
| 1142 | 12.307398 | 44.228.249.3 | 172.16.31.227 | HTTP | 874 | HTTP/1.1 200 OK (GIFBMP) |
| 1158 | 12.355685 | 172.16.31.227 | 44.228.249.3 | HTTP | 459 | GET /favicon.ico HTTP/1.1 |
| 1160 | 12.355685 | 172.16.31.227 | 172.16.31.227 | HTTP | 137 | HTTP/1.1 200 OK (text/html) |
| 1266 | 16.114954 | 172.16.31.227 | 93.123.17.254 | HTTP | 256 | GET /msdownload/update/v3/static/trustedr/en/disallowdescertstl.cab?8e99c6ebdaa7d0 HTTP/1.1 |
| 1271 | 16.380213 | 172.16.31.227 | 93.123.17.254 | HTTP | 256 | GET /msdownload/update/v3/static/trustedr/en/pinrulestl.cab?9b95f2046f163d23 HTTP/1.1 |
| 1272 | 16.380213 | 172.16.31.227 | 44.228.249.3 | HTTP | 457 | POST /index.php HTTP/1.1 |
| 1273 | 16.380213 | 172.16.31.227 | 172.16.31.227 | HTTP | 1342 | HTTP/1.1 200 OK (text/html) |
| 1344 | 23.054001 | 44.228.249.3 | 172.16.31.227 | HTTP | 442 | POST /login.php HTTP/1.1 |
| 1353 | 23.054001 | 172.16.31.227 | 44.228.249.3 | HTTP | 1402 | HTTP/1.1 200 OK (text/html) |
| 1575 | 27.397208 | 44.228.249.3 | 172.16.31.227 | HTTP | 526 | GET /msdownload/update/v3/static/trustedr/en/disallowdescertstl.cab?1263428793864752 HTTP/1.1 |
| 2029 | 29.054001 | 172.16.31.227 | 44.228.249.3 | HTTP | 1252 | POST /login.php HTTP/1.1 |
| 3171 | 85.913702 | 172.16.31.227 | 44.228.249.3 | HTTP | 832 | POST /secured/mouse.php HTTP/1.1 (application/x-www-form-urlencoded) |
| 3227 | 86.135974 | 44.228.249.3 | 172.16.31.227 | HTTP | 427 | HTTP/1.1 200 OK (text/html) |
| 3230 | 86.135974 | 172.16.31.227 | 44.228.249.3 | HTTP | 137 | HTTP/1.1 200 OK (text/css) |
| 3263 | 86.465349 | 44.228.249.3 | 172.16.31.227 | HTTP | 1156 | HTTP/1.1 200 OK (text/css) |
| 3437 | 91.346960 | 44.228.249.3 | 172.16.31.227 | HTTP | 463 | GET /index.php HTTP/1.1 |
| 4385 | 91.346960 | 44.228.249.3 | 172.16.31.227 | HTTP | 1342 | HTTP/1.1 200 OK (text/html) |
| 4478 | 94.515929 | 172.16.31.227 | 44.228.249.3 | HTTP | 714 | POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded) |
| 4500 | 94.515929 | 172.16.31.227 | 172.16.31.227 | HTTP | 137 | HTTP/1.1 200 OK (text/html) |
| 4549 | 94.786448 | 172.16.31.227 | 44.228.249.3 | HTTP | 584 | GET /login.php HTTP/1.1 |
| 4550 | 95.484696 | 44.228.249.3 | 172.16.31.227 | HTTP | 1342 | HTTP/1.1 200 OK (text/html) |
| 4551 | 95.484696 | 172.16.31.227 | 44.228.249.3 | HTTP | 451 | POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded) |
| 4642 | 97.871253 | 44.228.249.3 | 172.16.31.227 | HTTP | 338 | HTTP/1.1 302 Found (text/html) |
| 4643 | 97.871253 | 172.16.31.227 | 44.228.249.3 | HTTP | 137 | HTTP/1.1 200 OK (text/html) |
| 4650 | 98.327708 | 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 |
| 4745 | 100.779466 | 44.228.249.3 | 172.16.31.227 | HTTP | 137 | 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 | 44.228.249.3 | 172.16.31.227 | HTTP | 1155 | HTTP/1.1 200 OK (text/html) |
| 4909 | 104.480652 | 172.16.31.227 | 44.228.249.3 | HTTP | 137 | HTTP/1.1 200 OK (text/html) |
| 4934 | 104.480652 | 44.228.249.3 | 172.16.31.227 | HTTP | 1198 | HTTP/1.1 200 OK (text/html) |
| 4991 | 104.140674 | 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 | 361 | GET /userinfo.php HTTP/1.1 |

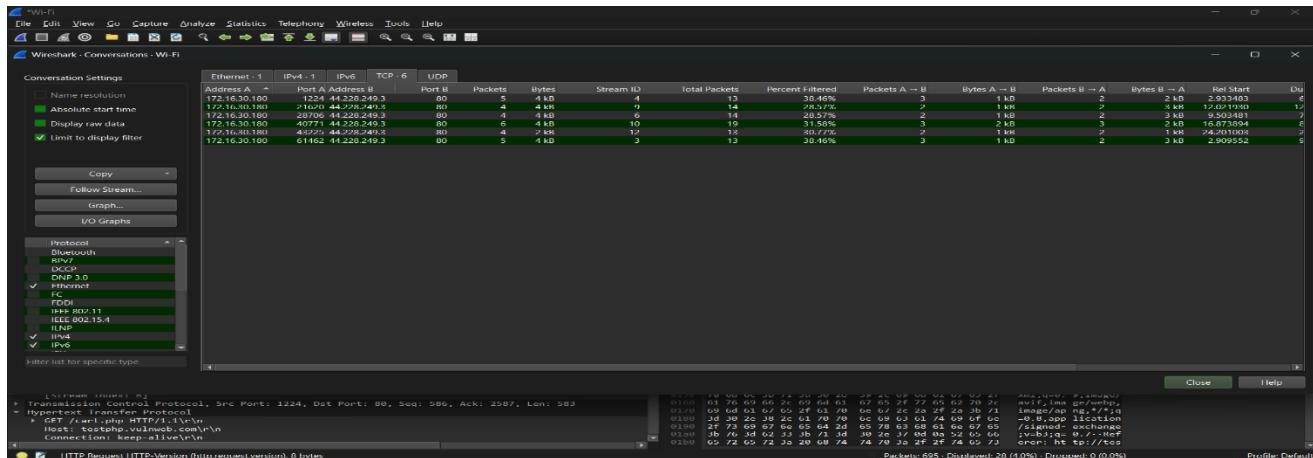
6) How many objects/files are downloaded?

| No. | Time | Source | Destination | Protocol | Length | info |
|---------------------|---------------|----------------|-------------|----------|--------|--|
| 1009 12. 70.47464 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 549 | GET | /login.php HTTP/1.1 |
| 1110 12. 69.41177 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 479 | GET | /style.css HTTP/1.1 |
| 1111 12. 05.46267 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 463 | GET | /images/logo.gif HTTP/1.1 |
| 1158 12. 35.56868 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 459 | GET | /favicon.ico HTTP/1.1 |
| 1206 16. 10.46267 | 172.16.31.227 | 93.123.17.254 | HTTP/1.1 | 299 | GET | /msdownload/update/v3/static/trusted/en/disallowedcertst1.cab?#0x9C6bdaa7d70 HTTP/1.1 |
| 1271 16. 30.2173 | 172.16.31.227 | 93.123.17.254 | HTTP/1.1 | 299 | GET | /msdownload/update/v3/static/trusted/en/pinrulesst1.cab?#0x95f2846f163d23 HTTP/1.1 |
| 1444 23. 782263 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 558 | GET | /login.php HTTP/1.1 |
| 1554 27. 14.50284 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 559 | GET | /sign.php HTTP/1.1 |
| 2949 10. 10.46267 | 172.16.31.227 | 92.233.116.252 | HTTP/1.1 | 299 | GET | /msdownload/update/v3/static/trusted/en/disallowedcertst1.cab?#1263427820864752 HTTP/1.1 |
| 2963 80. 11.2625 | 172.16.31.227 | 92.233.116.252 | HTTP/1.1 | 299 | GET | /msdownload/update/v3/static/trusted/en/pinrulesst1.cab?#f4021f8f888c5a9 HTTP/1.1 |
| 3231 86. 21.27676 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 429 | GET | /secured/style.css HTTP/1.1 |
| 4371 12. 10.46267 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 561 | GET | /index.php HTTP/1.1 |
| 4507 94. 786464 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 584 | GET | /login.php HTTP/1.1 |
| 4644 97. 9029959 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 584 | GET | /login.php HTTP/1.1 |
| 5740 10. 10.46267 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 569 | GET | /index.php HTTP/1.1 |
| 4815 102. 06.67444 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 599 | GET | /cart.php HTTP/1.1 |
| 4907 103. 796273 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 559 | GET | /artists.php HTTP/1.1 |
| 4996 103. 889597 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 560 | GET | /login.php HTTP/1.1 |
| 5024 105. 193.142 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 560 | GET | /index.php HTTP/1.1 |
| 5039 106. 17.70968 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 558 | GET | /login.php HTTP/1.1 |
| 5065 107. 08.92837 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 562 | GET | /guestbook.php HTTP/1.1 |
| 5083 107. 10.889597 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 404 | GET | /index.php HTTP/1.1 |
| 5448 115. 789739 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 565 | GET | /guestbook.php HTTP/1.1 |
| 5449 116. 888597 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 565 | GET | /userinfo.php HTTP/1.1 |
| 5461 117. 12.852869 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 563 | GET | /AJAX/index.php HTTP/1.1 |
| 5513 117. 12.852869 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | 422 | GET | /AJAX/styles.css HTTP/1.1 |
| 5540 118. 167108 | 172.16.31.227 | 44.228.249.3 | HTTP/1.1 | | | |

7) Make a detailed list including foreach 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.



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



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/>) ?

```
ajax test scap-pearing
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http://request.method == "GET"
No. Time Source Destination Protocol Length Info
48815 10.065444 172.16.31.227 44.228.249.3 HTTP 559 GET /cart.php HTTP/1.1
49097 103.796723 172.16.31.227 44.228.249.3 HTTP 559 GET /artists.php HTTP/1.1
4965 104.889641 172.16.31.227 44.228.249.3 HTTP 560 GET /login.php HTTP/1.1
4965 104.889641 172.16.31.227 44.228.249.3 HTTP 560 GET /index.php HTTP/1.1
5033 106.170699 172.16.31.227 44.228.249.3 HTTP 558 GET /login.php HTTP/1.1
5033 106.170699 172.16.31.227 44.228.249.3 HTTP 558 GET /guestbook.php HTTP/1.1
5085 107.891657 172.16.31.227 44.228.249.3 HTTP 569 GET /guestbook-gif.php HTTP/1.1
5440 115.789739 172.16.31.227 44.228.249.3 HTTP 566 GET /guestbook.php HTTP/1.1
5440 115.789739 172.16.31.227 44.228.249.3 HTTP 566 GET /index.php HTTP/1.1
5496 117.743657 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 562 GET /AJAX/index.php HTTP/1.1
5540 118.107858 172.16.31.227 44.228.249.3 HTTP 422 GET /AJAX/styles.css HTTP/1.1

frame 5440: Network traffic on wire (4528 bytes), 566 bytes captured (4528 bytes) on interface \Device\Vlan0
0050 2e 76 75 8c 6e 77 65 62 2e 63 67 6d 6d 0a 43 6f
0050 6c 69 76 65 6d 0a 59 78 67 72 61 64 65 2d 49 6e
0050 6c 69 76 65 6d 0a 59 78 67 72 61 64 65 2d 49 6e
0050 6c 69 76 65 6d 0a 59 78 67 72 61 64 65 2d 49 6e
0050 73 65 63 75 72 05 2d 52 65 73 75 65 73 74 73 6a
0050 6c 69 76 65 6d 0a 59 78 67 72 61 64 65 2d 49 6e
0050 64 6f 7a 69 66 0c 61 2f 35 3e 2e 30 2e 28 57 69 6e
0050 64 6f 7a 69 66 0c 61 2f 35 3e 2e 30 2e 28 57 69 6e
0050 66 36 34 36 29 78 36 34 29 20 41 70 6c 65 65 7a
0050 66 36 34 36 29 78 36 34 29 20 41 70 6c 65 65 7a
0050 65 62 4b 69 74 2f 35 33 2e 31 3e 2e 28 4b 4b
0050 65 62 4b 69 74 2f 35 33 2e 31 3e 2e 28 4b 4b
0050 29 43 68 72 67 6d 65 2f 31 34 33 2e 30 2e 30 2e
0050 29 43 68 72 67 6d 65 2f 31 34 33 2e 30 2e 30 2e
0100 63 65 63 74 2a 3e 29 74 65 78 74 2e 68 74 6d 6c
0100 63 65 63 74 2a 3e 29 74 65 78 74 2e 68 74 6d 6c
0150 6d 62 2b 78 6d 6c 2c 61 70 78 76 69 63 61 74 69
0150 6d 62 2b 78 6d 6c 2c 61 70 78 76 69 63 61 74 69
0170 67 65 2f 61 76 69 66 2e 69 6d 61 67 2f 77 65
0170 67 65 2f 61 76 69 66 2e 69 6d 61 67 2f 77 65
0180 62 70 2e 69 6d 61 67 65 2e 61 79 76 67 2c 24 2e
0180 62 70 2e 69 6d 61 67 65 2e 61 79 76 67 2c 24 2e
0149 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61
0149 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61
0150 65 66 65 72 65 72 3e 20 68 74 74 70 3e 2f 2f
0150 65 66 65 72 65 72 3e 20 68 74 74 70 3e 2f 2f
0109 74 63 73 74 69 70 2e 76 75 66 77 65 62 2e
0109 74 63 73 74 69 70 2e 76 75 66 77 65 62 2e
0170 78 69 69 61 63 65 70 74 72 4d 45 63 67 64 69
0170 78 69 69 61 63 65 70 74 72 4d 45 63 67 64 69
0230 65 69 64 61 63 65 70 74 72 4d 61 66 67 75 61
0230 65 69 64 61 63 65 70 74 72 4d 61 66 67 75 61
```

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

```

#逢送包 1099: 172.16.31.227 44.228.249.3 HTTP/1.1 GET /login.php HTTP/1.1
#逢送包 1100: 172.16.31.227 44.228.249.3 HTTP/1.1 GET /style.css HTTP/1.1
#逢送包 1101: 172.16.31.227 44.228.249.3 HTTP/1.1 GET /logos.gif HTTP/1.1
#逢送包 1102: 172.16.31.227 44.228.249.3 HTTP/1.1 GET /Favicon.ico HTTP/1.1
#逢送包 1266: 172.16.31.227 93.123.17.254 HTTP/1.1 GET /mdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8e99c6ebdaa7da0 HTTP/1.1

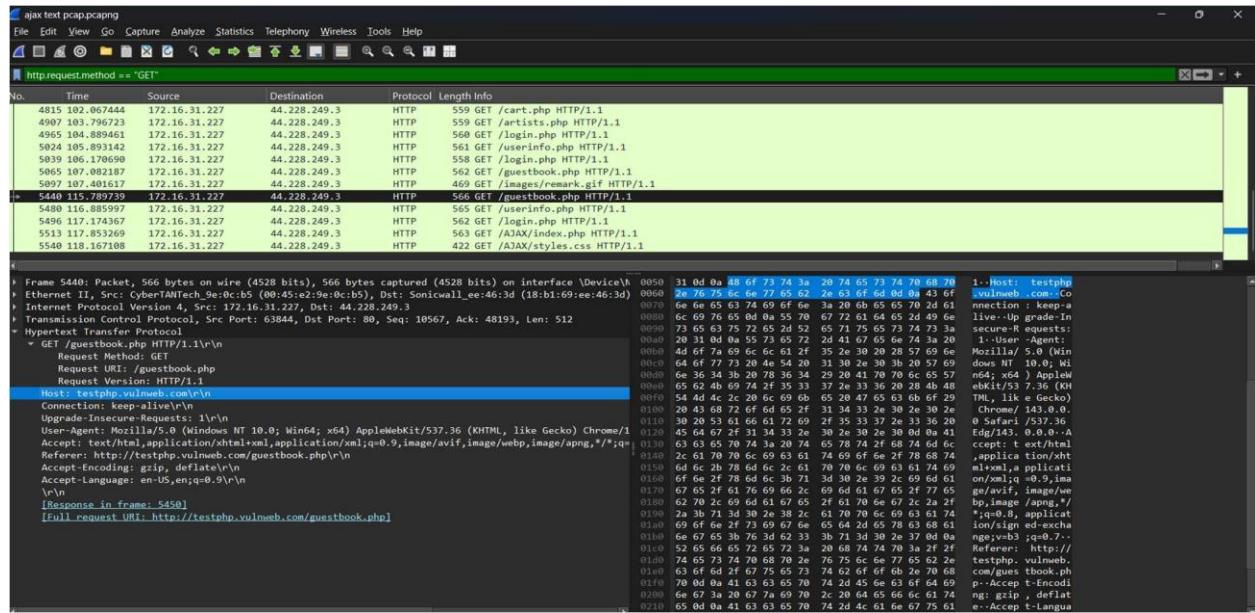
#逢送包 1099: Packet 549 bytes on wire (4392 bits), 549 bytes captured on interface \Device\NPF_{...} at 00:ff:cb:2a:00:00 offset 0 (relative to capture start)
#Ethernet II, Src: CyberTANtech_Weishi (00:ff:cb:2a:00:00), Dst: Sonicwall_eei:46:3d (10:bb:69:e6:46:3d)
#Transmission Control Protocol, Src Port: 57962, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
#HyperText Transfer Protocol
#  GET /login.php HTTP/1.1\n
#    Request Method: GET
#    Request-URI: /login.php
#    Request Version: HTTP/1.1
#    Host: testphp.vulnweb.com\n
#    Connection: keep-alive\n
# Upgrade-Insecure-Requests: 1\n
# User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/14.0.740.116 Safari/537.36 Edg/14.0.740.116
# Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
# Referer: http://testphp.vulnweb.com/\n
# Accept-Encoding: gzip, deflate\n
# Accept-Language: en-US,en;q=0.9\n
# Vary: *\n
# Response in frame: 1107
# Full request URI: http://testphp.vulnweb.com/login.php
```

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

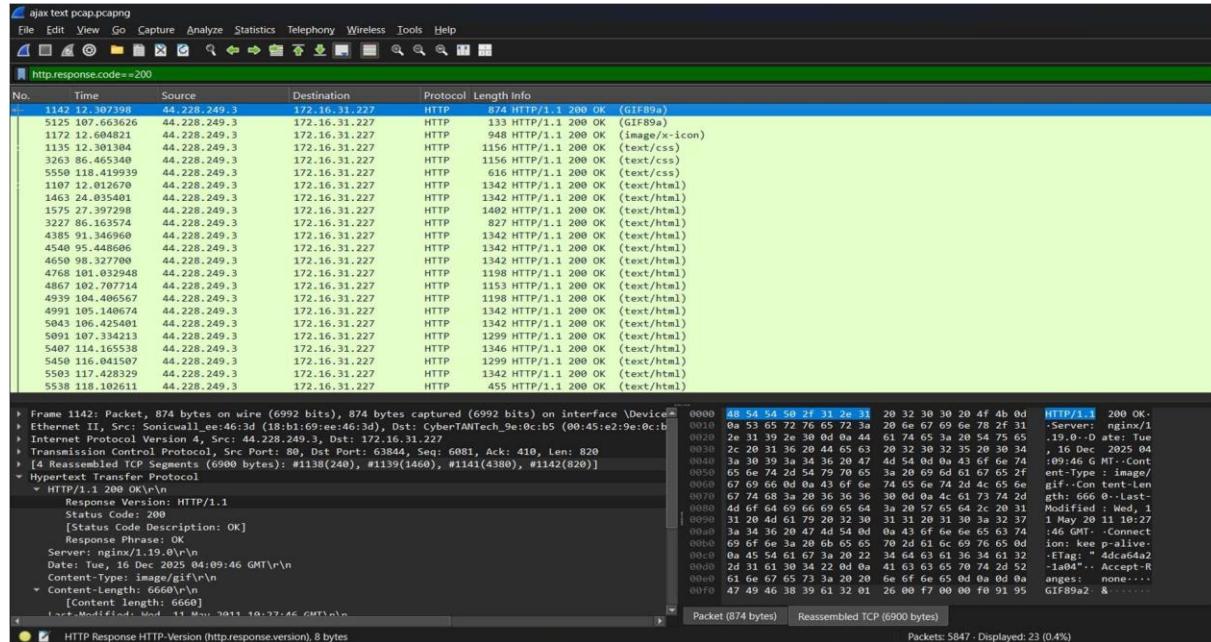
The screenshot shows a Wireshark capture of network traffic. The packet list pane shows a single packet (No. 5039) from a host at 172.16.31.227 to a host at 172.16.31.227, port 80. The packet details pane shows the HTTP request: GET /login.php HTTP/1.1. The bytes pane shows the raw hex and ASCII data of the request. The packet details pane also includes a "Reuest-Header" section with various headers like User-Agent, Accept, and Accept-Encoding. The bottom status bar indicates the packet is number 5039, has a length of 558 bytes, and was captured at 10:06:17.000000. The bottom left shows options for "Show packet bytes" and "Layout: Vertical (Stacked)".

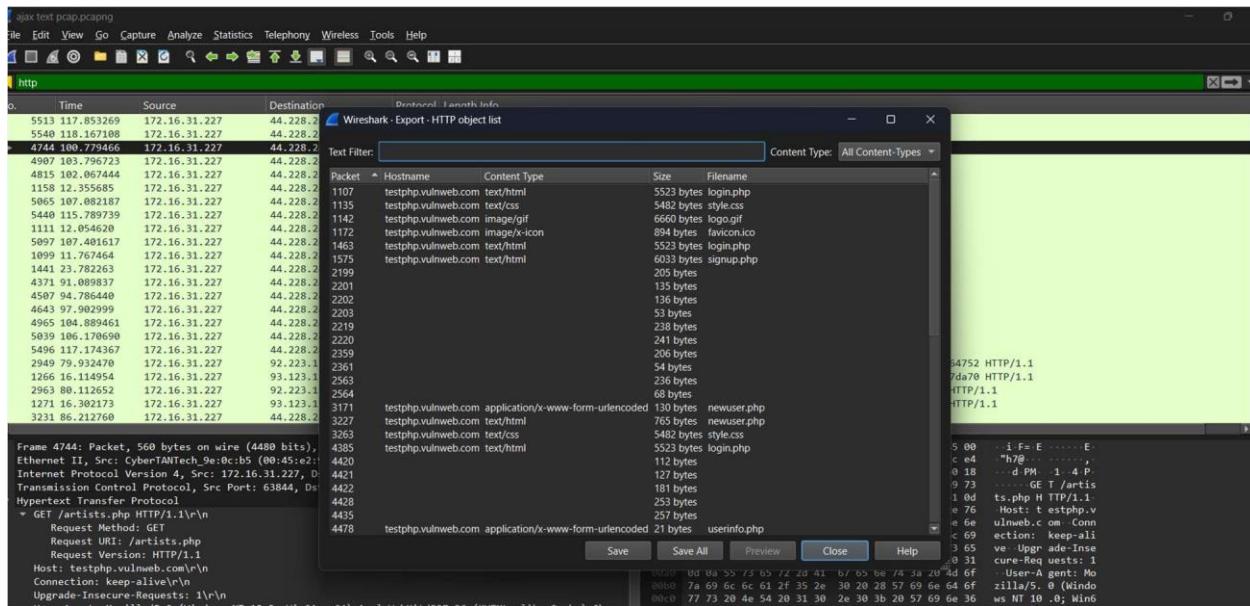
TASK 2

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



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 ?





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)

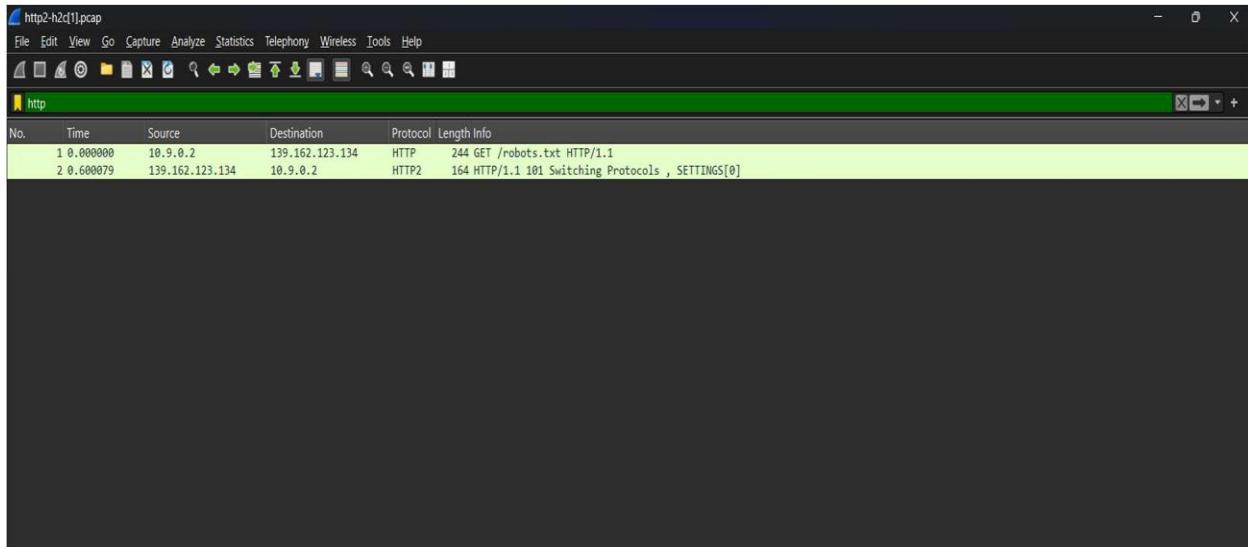
- **If-Modified-Since:** Date of the cached file version.
- **If-None-Match:** ETag value of the cached version.
- **Cache-Control:** (e.g., max-age=0 forces revalidation).

4. Response Headers (Sent by Server)

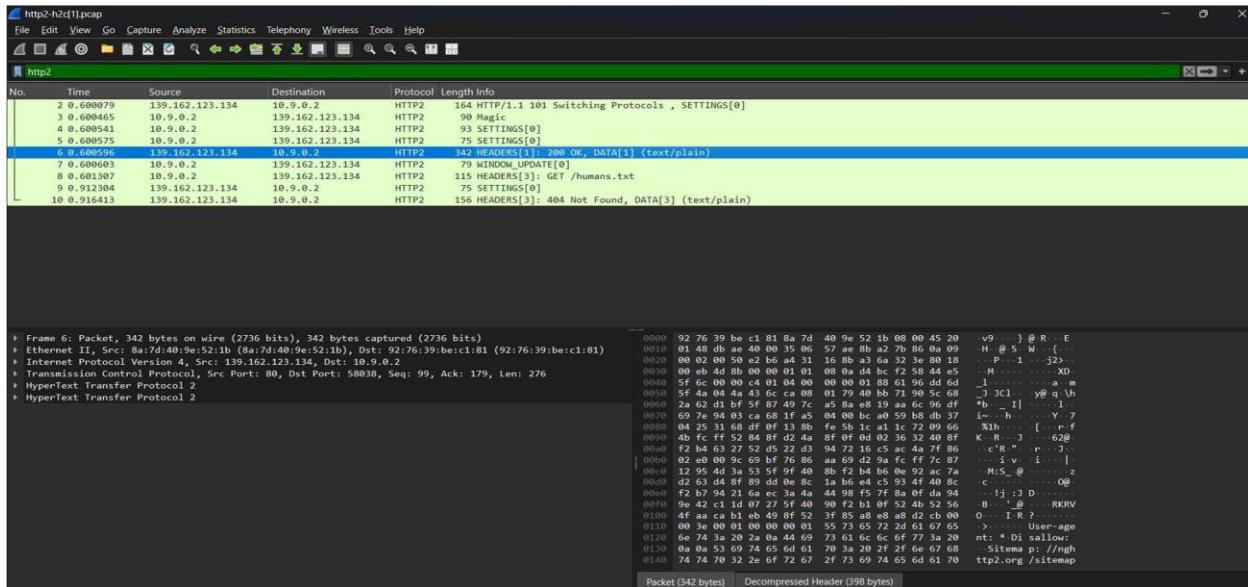
- **Last-Modified:** Last modification time of the file.
- **ETag:** Unique identifier for the file version.
- **Expires:** Time after which the cached copy becomes stale.

TASK 3

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



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



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

