Task 1:

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

- 19 <ip.src == 172.16.31.221>

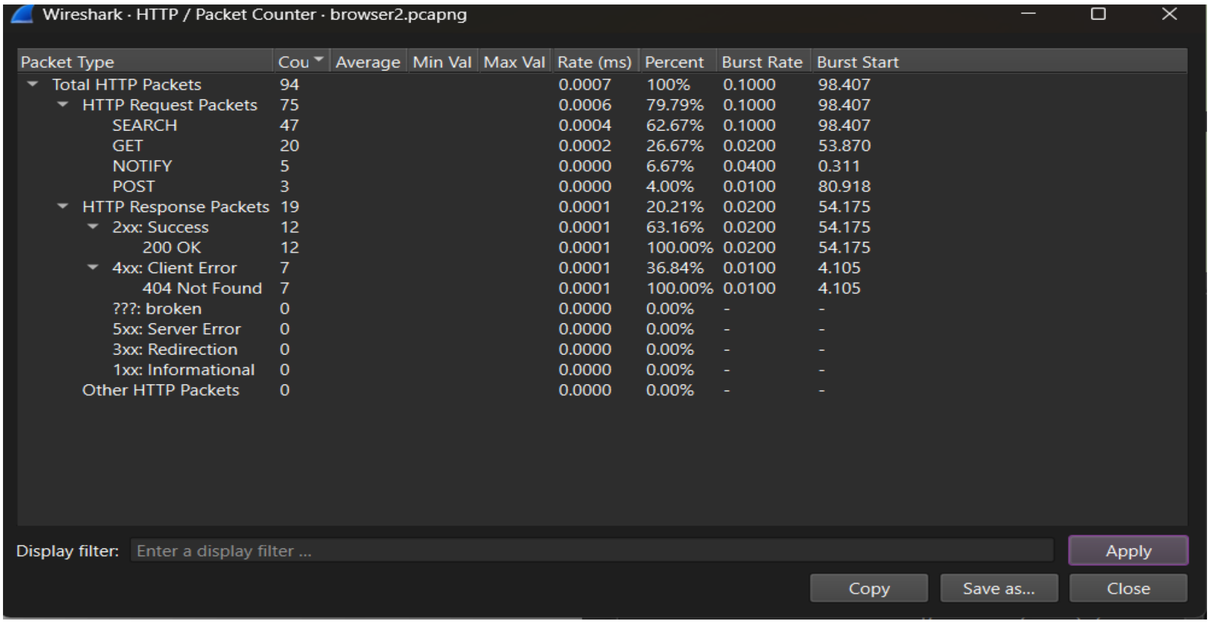
2.How many DNS servers are involved?

- 3 <dns && dns.flags.response == 1>

3.Do all DNS servers respond?

No

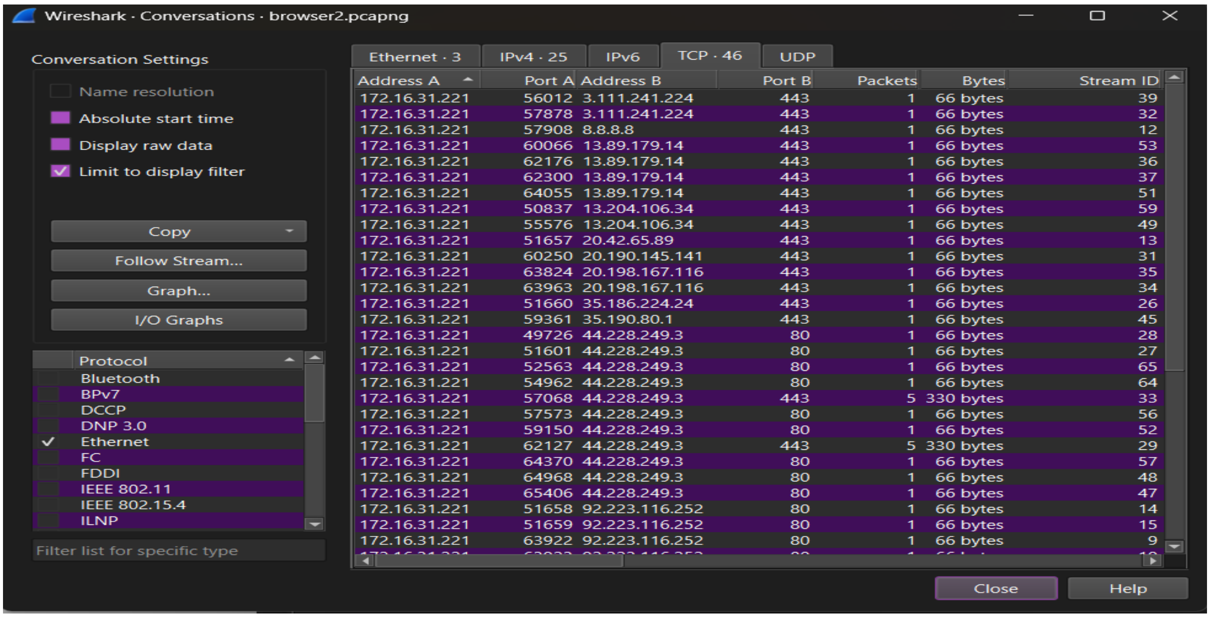
2. How many HTTP requests (Type and respective count of requests), responses (status code and phrase of each of the responses) did the browser send and receive?



Packet Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	94				0.0007	100%	0.1000	98.407
HTTP Request Packets	75				0.0006	79.79%	0.1000	98.407
SEARCH	47				0.0004	62.67%	0.1000	98.407
GET	20				0.0002	26.67%	0.0200	53.870
NOTIFY	5				0.0000	6.67%	0.0400	0.311
POST	3				0.0000	4.00%	0.0100	80.918
HTTP Response Packets	19				0.0001	20.21%	0.0200	54.175
2xx: Success	12				0.0001	63.16%	0.0200	54.175
200 OK	12				0.0001	100.00%	0.0200	54.175
4xx: Client Error	7				0.0001	36.84%	0.0100	4.105
404 Not Found	7				0.0001	100.00%	0.0100	4.105
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
3xx: Redirection	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
Other HTTP Packets	0				0.0000	0.00%	-	-

Display filter: Enter a display filter ...

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



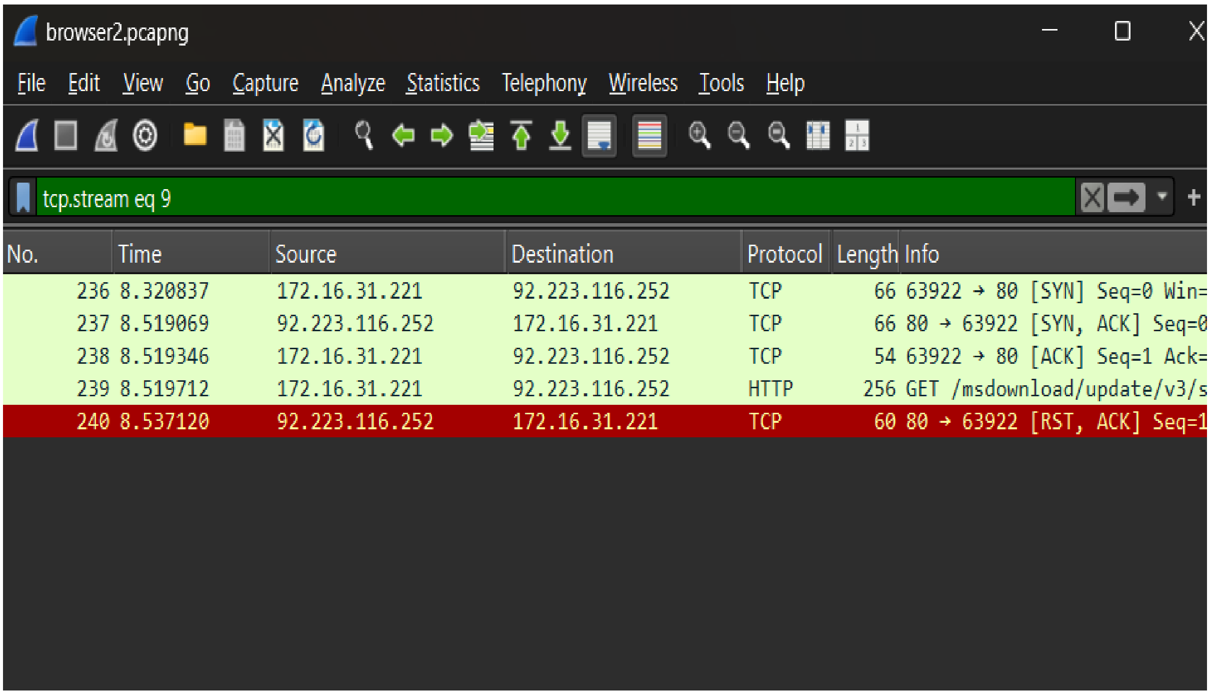
□ Name resolution
■ Absolute start time
■ Display raw data
☑ Limit to display filter

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

Filter list for specific type

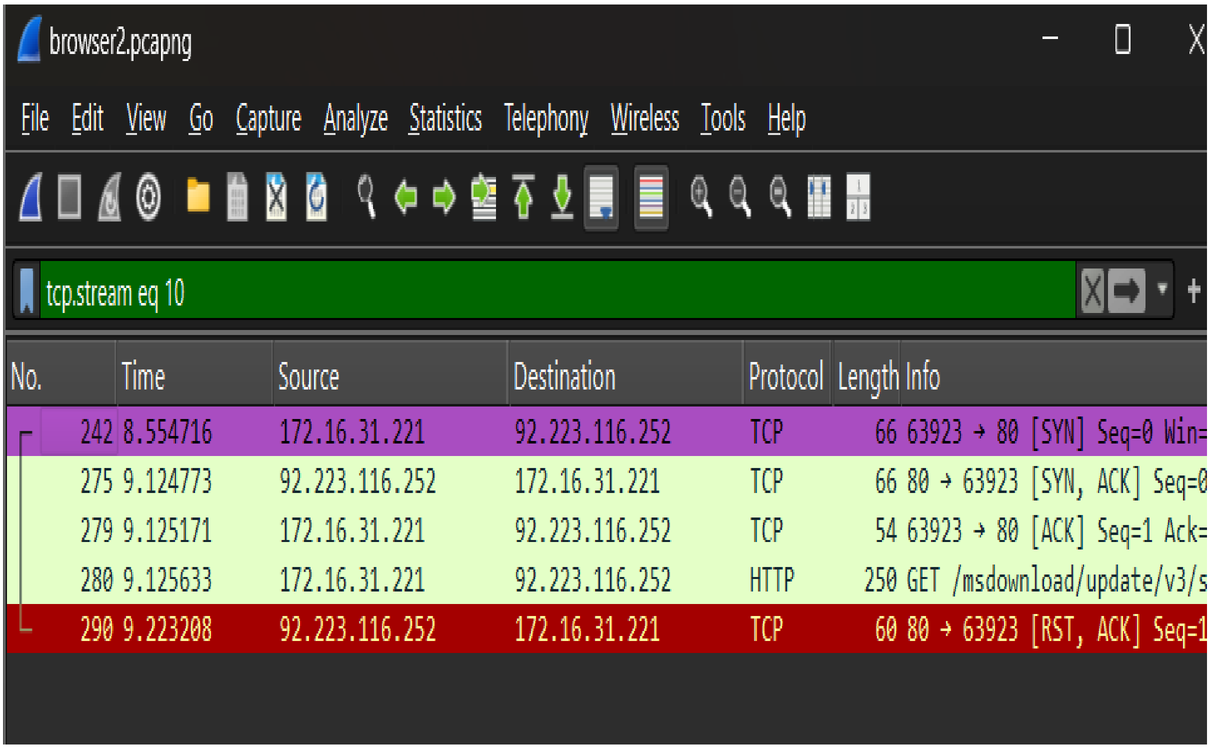
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID
172.16.31.221	56012	3.111.241.224	443	1	66 bytes	39
172.16.31.221	57878	3.111.241.224	443	1	66 bytes	32
172.16.31.221	57908	8.8.8.8	443	1	66 bytes	12
172.16.31.221	60066	13.89.179.14	443	1	66 bytes	53
172.16.31.221	62176	13.89.179.14	443	1	66 bytes	36
172.16.31.221	62300	13.89.179.14	443	1	66 bytes	37
172.16.31.221	64055	13.89.179.14	443	1	66 bytes	51
172.16.31.221	50837	13.204.106.34	443	1	66 bytes	59
172.16.31.221	55576	13.204.106.34	443	1	66 bytes	49
172.16.31.221	51657	20.42.65.89	443	1	66 bytes	13
172.16.31.221	60250	20.190.145.141	443	1	66 bytes	31
172.16.31.221	63824	20.198.167.116	443	1	66 bytes	35
172.16.31.221	63963	20.198.167.116	443	1	66 bytes	34
172.16.31.221	51660	35.186.224.24	443	1	66 bytes	26
172.16.31.221	59361	35.190.80.1	443	1	66 bytes	45
172.16.31.221	49726	44.228.249.3	80	1	66 bytes	28
172.16.31.221	51601	44.228.249.3	80	1	66 bytes	27
172.16.31.221	52563	44.228.249.3	80	1	66 bytes	65
172.16.31.221	54962	44.228.249.3	80	1	66 bytes	64
172.16.31.221	57068	44.228.249.3	443	5	330 bytes	33
172.16.31.221	57573	44.228.249.3	80	1	66 bytes	56
172.16.31.221	59150	44.228.249.3	80	1	66 bytes	52
172.16.31.221	62127	44.228.249.3	443	5	330 bytes	29
172.16.31.221	64370	44.228.249.3	80	1	66 bytes	57
172.16.31.221	64968	44.228.249.3	80	1	66 bytes	48
172.16.31.221	65406	44.228.249.3	80	1	66 bytes	47
172.16.31.221	51658	92.223.116.252	80	1	66 bytes	14
172.16.31.221	51659	92.223.116.252	80	1	66 bytes	15
172.16.31.221	63922	92.223.116.252	80	1	66 bytes	9

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


browser2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

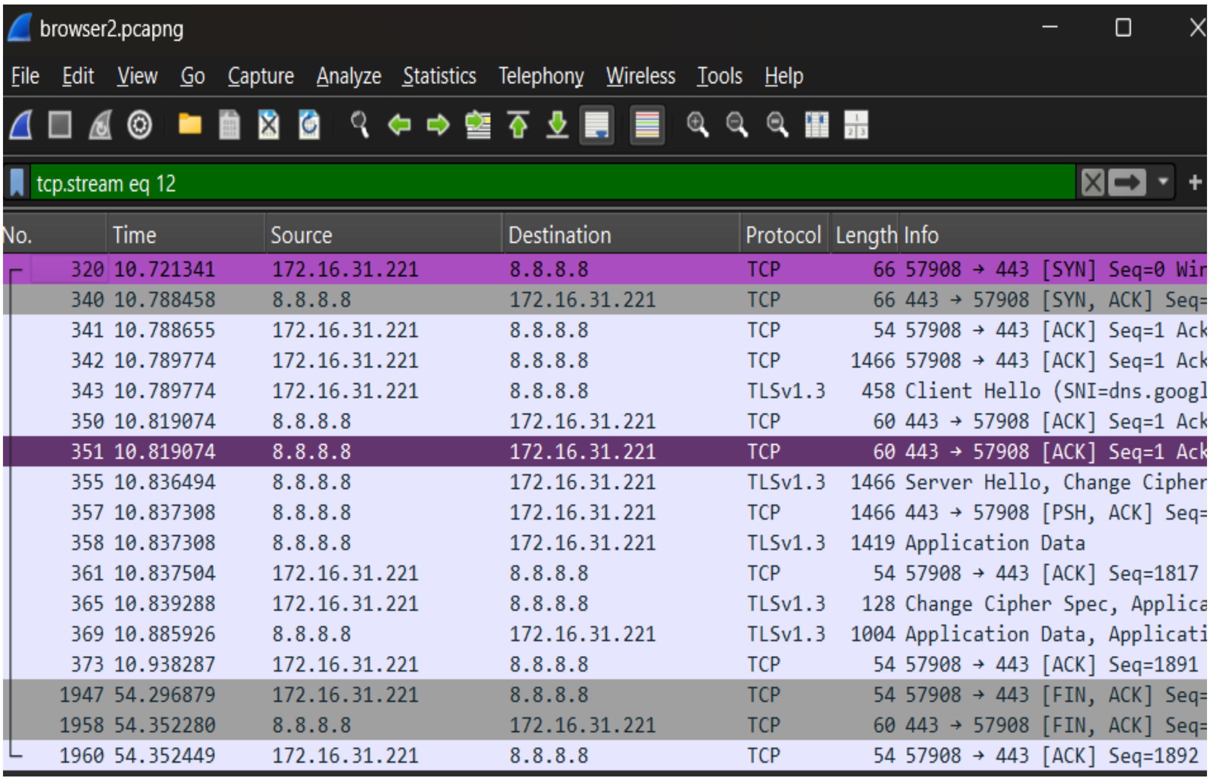
tcp.stream eq 9

No.	Time	Source	Destination	Protocol	Length	Info
236	8.320837	172.16.31.221	92.223.116.252	TCP	66	63922 → 80 [SYN] Seq=0 Win=
237	8.519069	92.223.116.252	172.16.31.221	TCP	66	80 → 63922 [SYN, ACK] Seq=0
238	8.519346	172.16.31.221	92.223.116.252	TCP	54	63922 → 80 [ACK] Seq=1 Ack=
239	8.519712	172.16.31.221	92.223.116.252	HTTP	256	GET /msdownload/update/v3/s
240	8.537120	92.223.116.252	172.16.31.221	TCP	60	80 → 63922 [RST, ACK] Seq=1


browser2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 10

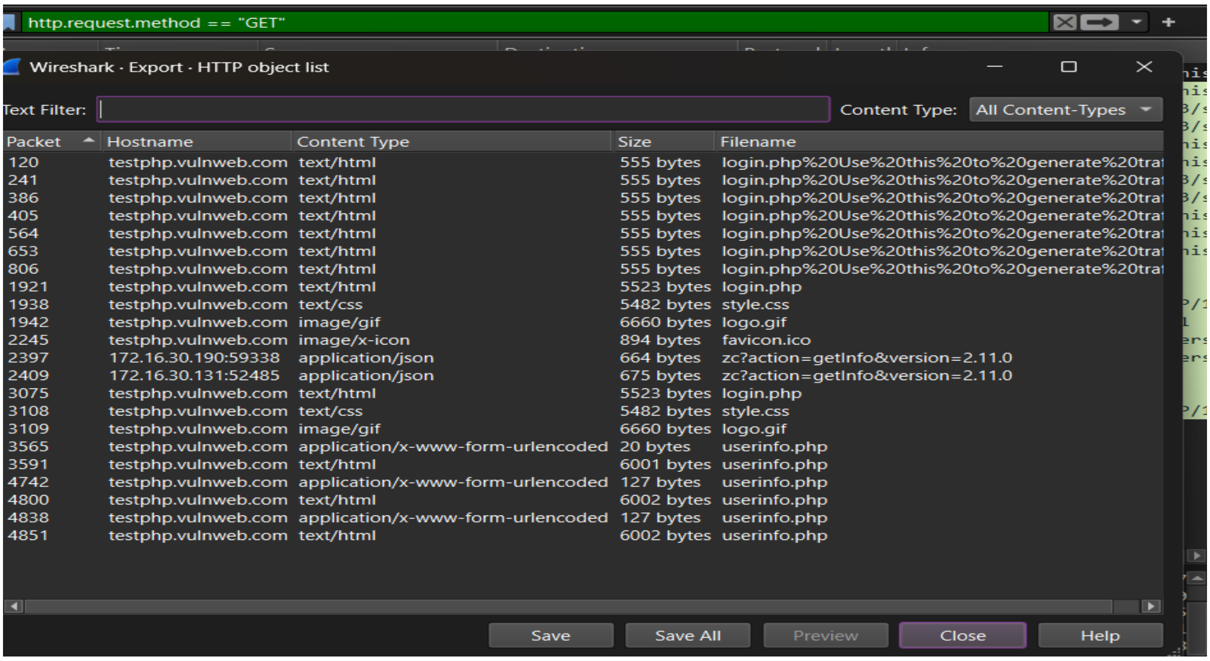
No.	Time	Source	Destination	Protocol	Length	Info
242	8.554716	172.16.31.221	92.223.116.252	TCP	66	63923 → 80 [SYN] Seq=0 Win=
275	9.124773	92.223.116.252	172.16.31.221	TCP	66	80 → 63923 [SYN, ACK] Seq=0
279	9.125171	172.16.31.221	92.223.116.252	TCP	54	63923 → 80 [ACK] Seq=1 Ack=
280	9.125633	172.16.31.221	92.223.116.252	HTTP	250	GET /msdownload/update/v3/s
290	9.223208	92.223.116.252	172.16.31.221	TCP	60	80 → 63923 [RST, ACK] Seq=1



tcp.stream eq 12

No.	Time	Source	Destination	Protocol	Length	Info
320	10.721341	172.16.31.221	8.8.8.8	TCP	66	57908 → 443 [SYN] Seq=0 Wir
340	10.788458	8.8.8.8	172.16.31.221	TCP	66	443 → 57908 [SYN, ACK] Seq=
341	10.788655	172.16.31.221	8.8.8.8	TCP	54	57908 → 443 [ACK] Seq=1 Ack
342	10.789774	172.16.31.221	8.8.8.8	TCP	1466	57908 → 443 [ACK] Seq=1 Ack
343	10.789774	172.16.31.221	8.8.8.8	TLSv1.3	458	Client Hello (SNI=dns.googl
350	10.819074	8.8.8.8	172.16.31.221	TCP	60	443 → 57908 [ACK] Seq=1 Ack
351	10.819074	8.8.8.8	172.16.31.221	TCP	60	443 → 57908 [ACK] Seq=1 Ack
355	10.836494	8.8.8.8	172.16.31.221	TLSv1.3	1466	Server Hello, Change Cipher
357	10.837308	8.8.8.8	172.16.31.221	TCP	1466	443 → 57908 [PSH, ACK] Seq=
358	10.837308	8.8.8.8	172.16.31.221	TLSv1.3	1419	Application Data
361	10.837504	172.16.31.221	8.8.8.8	TCP	54	57908 → 443 [ACK] Seq=1817
365	10.839288	172.16.31.221	8.8.8.8	TLSv1.3	128	Change Cipher Spec, Applica
369	10.885926	8.8.8.8	172.16.31.221	TLSv1.3	1004	Application Data, Applicati
373	10.938287	172.16.31.221	8.8.8.8	TCP	54	57908 → 443 [ACK] Seq=1891
1947	54.296879	172.16.31.221	8.8.8.8	TCP	54	57908 → 443 [FIN, ACK] Seq=
1958	54.352280	8.8.8.8	172.16.31.221	TCP	60	443 → 57908 [FIN, ACK] Seq=
1960	54.352449	172.16.31.221	8.8.8.8	TCP	54	57908 → 443 [ACK] Seq=1892

6. How many objects/files are downloaded?


http.request.method == "GET"

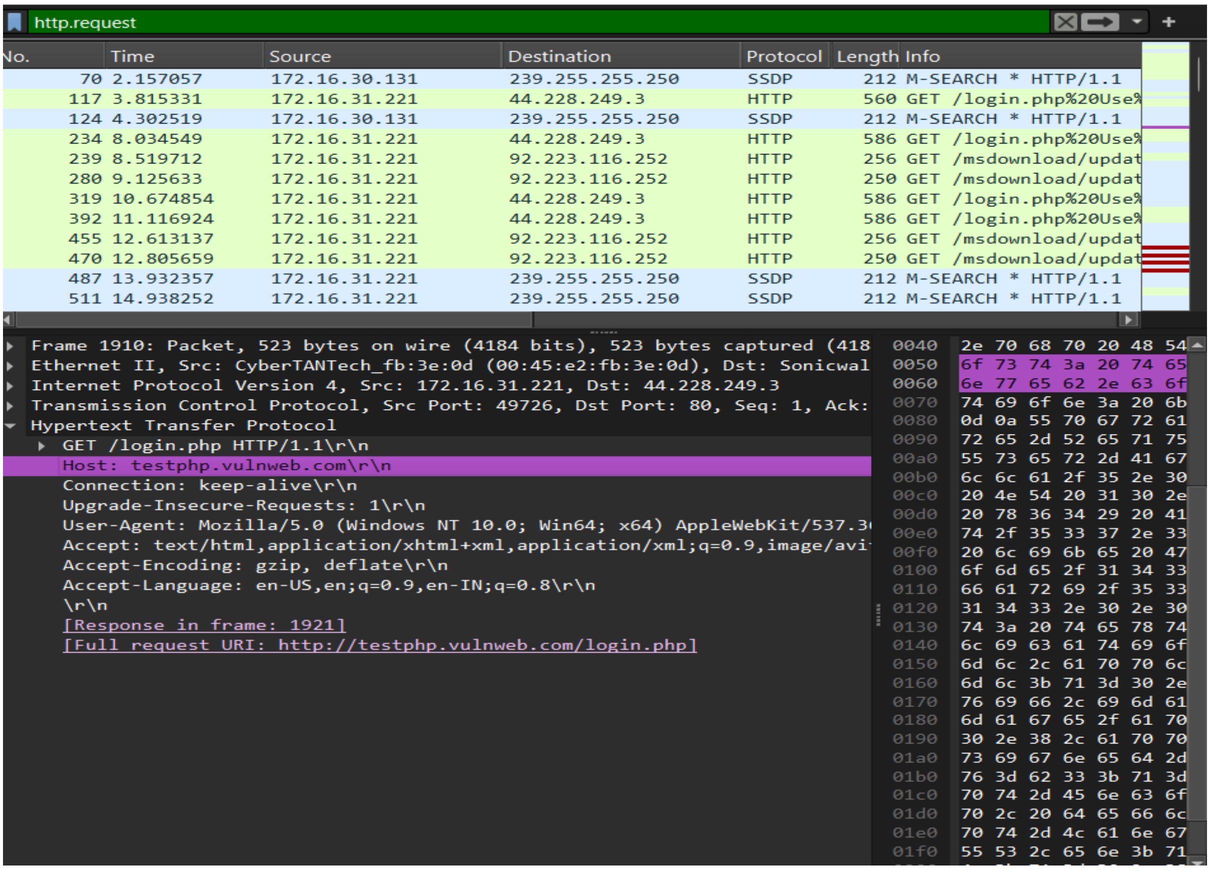
Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
120	testphp.vulnweb.com	text/html	555 bytes	login.php%20Use%20this%20to%20generate%20trai
241	testphp.vulnweb.com	text/html	555 bytes	login.php%20Use%20this%20to%20generate%20trai
386	testphp.vulnweb.com	text/html	555 bytes	login.php%20Use%20this%20to%20generate%20trai
405	testphp.vulnweb.com	text/html	555 bytes	login.php%20Use%20this%20to%20generate%20trai
564	testphp.vulnweb.com	text/html	555 bytes	login.php%20Use%20this%20to%20generate%20trai
653	testphp.vulnweb.com	text/html	555 bytes	login.php%20Use%20this%20to%20generate%20trai
806	testphp.vulnweb.com	text/html	555 bytes	login.php%20Use%20this%20to%20generate%20trai
1921	testphp.vulnweb.com	text/html	5523 bytes	login.php
1938	testphp.vulnweb.com	text/css	5482 bytes	style.css
1942	testphp.vulnweb.com	image/gif	6660 bytes	logo.gif
2245	testphp.vulnweb.com	image/x-icon	894 bytes	favicon.ico
2397	172.16.30.190:59338	application/json	664 bytes	zc?action=getInfo&version=2.11.0
2409	172.16.30.131:52485	application/json	675 bytes	zc?action=getInfo&version=2.11.0
3075	testphp.vulnweb.com	text/html	5523 bytes	login.php
3108	testphp.vulnweb.com	text/css	5482 bytes	style.css
3109	testphp.vulnweb.com	image/gif	6660 bytes	logo.gif
3565	testphp.vulnweb.com	application/x-www-form-urlencoded	20 bytes	userinfo.php
3591	testphp.vulnweb.com	text/html	6001 bytes	userinfo.php
4742	testphp.vulnweb.com	application/x-www-form-urlencoded	127 bytes	userinfo.php
4800	testphp.vulnweb.com	text/html	6002 bytes	userinfo.php
4838	testphp.vulnweb.com	application/x-www-form-urlencoded	127 bytes	userinfo.php
4851	testphp.vulnweb.com	text/html	6002 bytes	userinfo.php

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

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



```
http.request
```

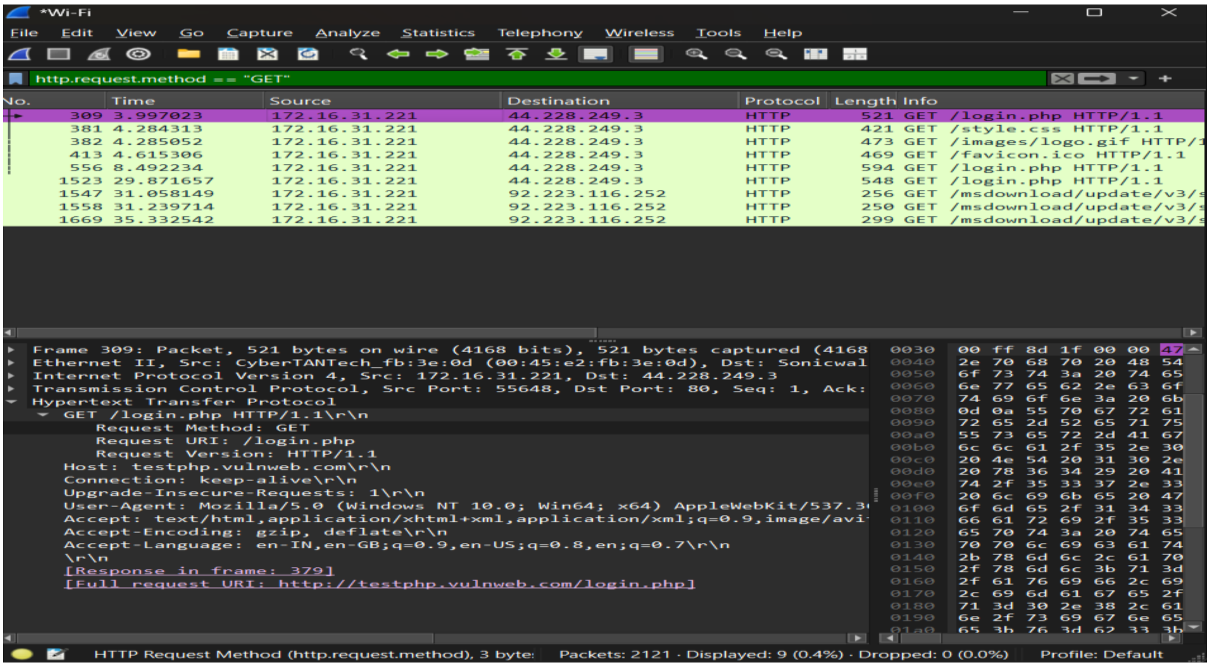
```
No.       Time        Source          Destination       Protocol  Length Info
     70  2.157057    172.16.30.131   239.255.255.250   SSDP         212 M-SEARCH * HTTP/1.1
    117  3.815331    172.16.31.221   44.228.249.3      HTTP         560 GET /login.php%20Use%
    124  4.302519    172.16.30.131   239.255.255.250   SSDP         212 M-SEARCH * HTTP/1.1
    234  8.034549    172.16.31.221   44.228.249.3      HTTP         586 GET /login.php%20Use%
    239  8.519712    172.16.31.221   92.223.116.252    HTTP         256 GET /msdownload/updat
    280  9.125633    172.16.31.221   92.223.116.252    HTTP         250 GET /msdownload/updat
    319 10.674854    172.16.31.221   44.228.249.3      HTTP         586 GET /login.php%20Use%
    392 11.116924    172.16.31.221   44.228.249.3      HTTP         586 GET /login.php%20Use%
    455 12.613137    172.16.31.221   92.223.116.252    HTTP         256 GET /msdownload/updat
    470 12.805659    172.16.31.221   92.223.116.252    HTTP         250 GET /msdownload/updat
    487 13.932357    172.16.31.221   239.255.255.250   SSDP         212 M-SEARCH * HTTP/1.1
    511 14.938252    172.16.31.221   239.255.255.250   SSDP         212 M-SEARCH * HTTP/1.1
```

```
▸ Frame 1910: Packet, 523 bytes on wire (4184 bits), 523 bytes captured (418
▸ Ethernet II, Src: CyberTANTech_fb:3e:0d (00:45:e2:fb:3e:0d), Dst: Sonicwal
▸ Internet Protocol Version 4, Src: 172.16.31.221, Dst: 44.228.249.3
▸ Transmission Control Protocol, Src Port: 49726, Dst Port: 80, Seq: 1, Ack:
▾ Hypertext Transfer Protocol
  ▸ GET /login.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,en-IN;q=0.8\r\n
    \r\n
    [Response in frame: 1921]
    [Full request URI: http://testphp.vulnweb.com/login.php]
```

```
0040  2e 70 68 70 20 48 54
0050  6f 73 74 3a 20 74 65
0060  6e 77 65 62 2e 63 6f
0070  74 69 6f 6e 3a 20 6b
0080  0d 0a 55 70 67 72 61
0090  72 65 2d 52 65 71 75
00a0  55 73 65 72 2d 41 67
00b0  6c 6c 61 2f 35 2e 30
00c0  20 4e 54 20 31 30 2e
00d0  20 78 36 34 29 20 41
00e0  74 2f 35 33 37 2e 33
00f0  20 6c 69 6b 65 20 47
0100  6f 6d 65 2f 31 34 33
0110  66 61 72 69 2f 35 33
0120  31 34 33 2e 30 2e 30
0130  74 3a 20 74 65 78 74
0140  6c 69 63 61 74 69 6f
0150  6d 6c 2c 61 70 70 6c
0160  6d 6c 3b 71 3d 30 2e
0170  76 69 66 2c 69 6d 61
0180  6d 61 67 65 2f 61 70
0190  30 2e 38 2c 61 70 70
01a0  73 69 67 6e 65 64 2d
01b0  76 3d 62 33 3b 71 3d
01c0  70 74 2d 45 6e 63 6f
01d0  70 2c 20 64 65 66 6c
01e0  70 74 2d 4c 61 6e 67
01f0  55 53 2c 65 6e 3b 71
```

Task 2:

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



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == "GET"
```

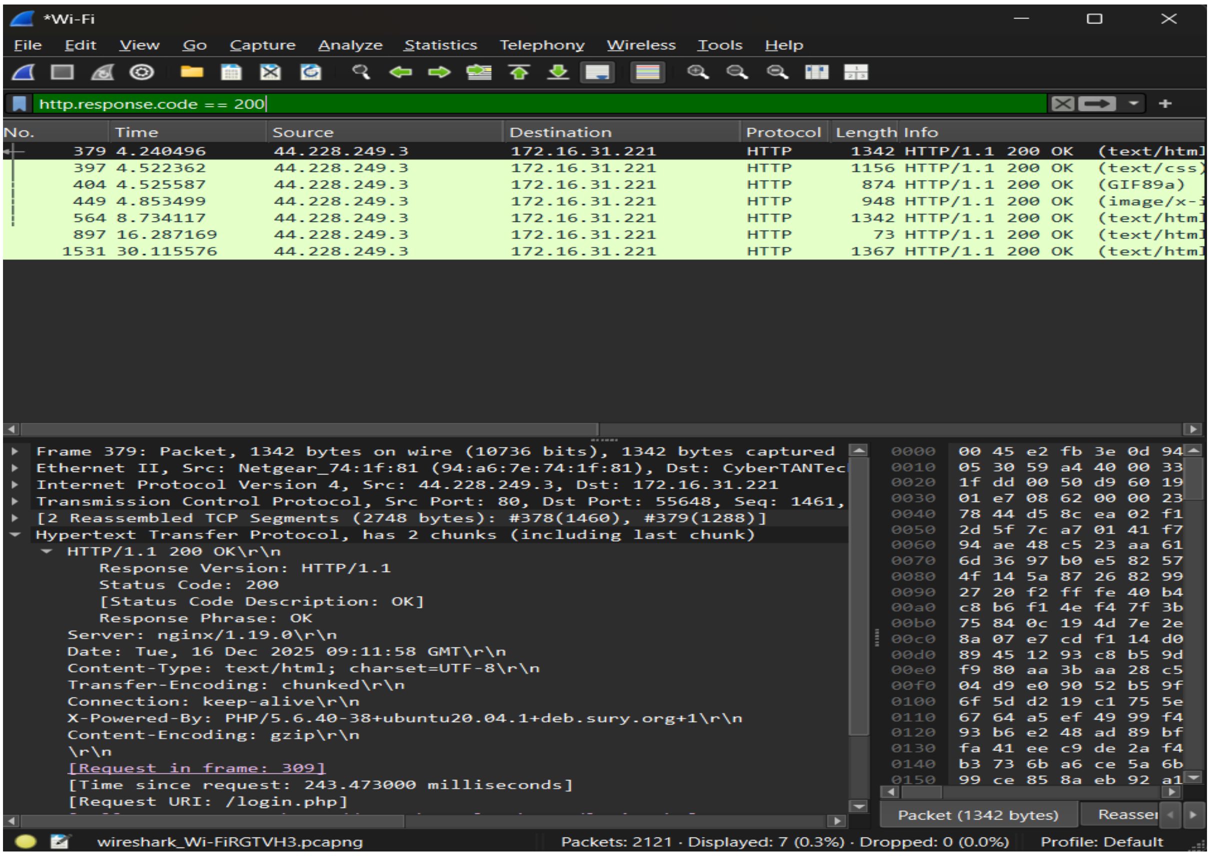
```
No.       Time        Source          Destination       Protocol  Length Info
    309  3.997023    172.16.31.221   44.228.249.3      HTTP         521 GET /login.php HTTP/1.1
    381  4.284313    172.16.31.221   44.228.249.3      HTTP         421 GET /style.css HTTP/1.1
    382  4.285052    172.16.31.221   44.228.249.3      HTTP         473 GET /images/logo.gif HTTP/1
    413  4.615306    172.16.31.221   44.228.249.3      HTTP         469 GET /favicon.ico HTTP/1.1
    556  8.492234    172.16.31.221   44.228.249.3      HTTP         594 GET /login.php HTTP/1.1
   1523 29.871657    172.16.31.221   44.228.249.3      HTTP         548 GET /login.php HTTP/1.1
   1547 31.058149    172.16.31.221   92.223.116.252    HTTP         256 GET /msdownload/update/v3/s
   1558 31.239714    172.16.31.221   92.223.116.252    HTTP         250 GET /msdownload/update/v3/s
   1669 35.332542    172.16.31.221   92.223.116.252    HTTP         299 GET /msdownload/update/v3/s
```

```
▸ Frame 309: Packet, 521 bytes on wire (4168 bits), 521 bytes captured (4168
▸ Ethernet II, Src: CyberTANTech_fb:3e:0d (00:45:e2:fb:3e:0d), Dst: Sonicwal
▸ Internet Protocol Version 4, Src: 172.16.31.221, Dst: 44.228.249.3
▸ Transmission Control Protocol, Src Port: 55648, Dst Port: 80, Seq: 1, Ack:
▾ Hypertext Transfer Protocol
  ▾ GET /login.php HTTP/1.1\r\n
        Request Method: GET
        Request URI: /login.php
        Request Version: HTTP/1.1
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-IN,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Response in frame: 379]
    [Full request URI: http://testphp.vulnweb.com/login.php]
```

```
0030  00 ff 8d 1f 00 00 47
0040  2e 70 68 70 20 48 54
0050  6f 73 74 3a 20 74 65
0060  6e 77 65 62 2e 63 6f
0070  74 69 6f 6e 3a 20 6b
0080  0d 0a 55 70 67 72 61
0090  72 65 2d 52 65 71 75
00a0  55 73 65 72 2d 41 67
00b0  6c 6c 61 2f 35 2e 30
00c0  20 4e 54 20 31 30 2e
00d0  20 78 36 34 29 20 41
00e0  74 2f 35 33 37 2e 33
00f0  20 6c 69 6b 65 20 47
0100  6f 6d 65 2f 31 34 33
0110  66 61 72 69 2f 35 33
0120  65 70 74 3a 20 74 65
0130  70 70 6c 69 63 61 74
0140  2b 78 6d 6c 2c 61 70
0150  2f 78 6d 6c 3b 71 3d
0160  2f 61 76 69 66 2c 69
0170  2c 69 6d 61 67 65 2f
0180  71 3d 30 2e 38 2c 61
0190  6e 2f 73 69 67 6e 65
01a0  65 3b 76 3d 62 33 3b
```

```
HTTP Request Method (http.request.method), 3 byte:   Packets: 2121 · Displayed: 9 (0.4%) · Dropped: 0 (0.0%)   Profile: Default
```

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?


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

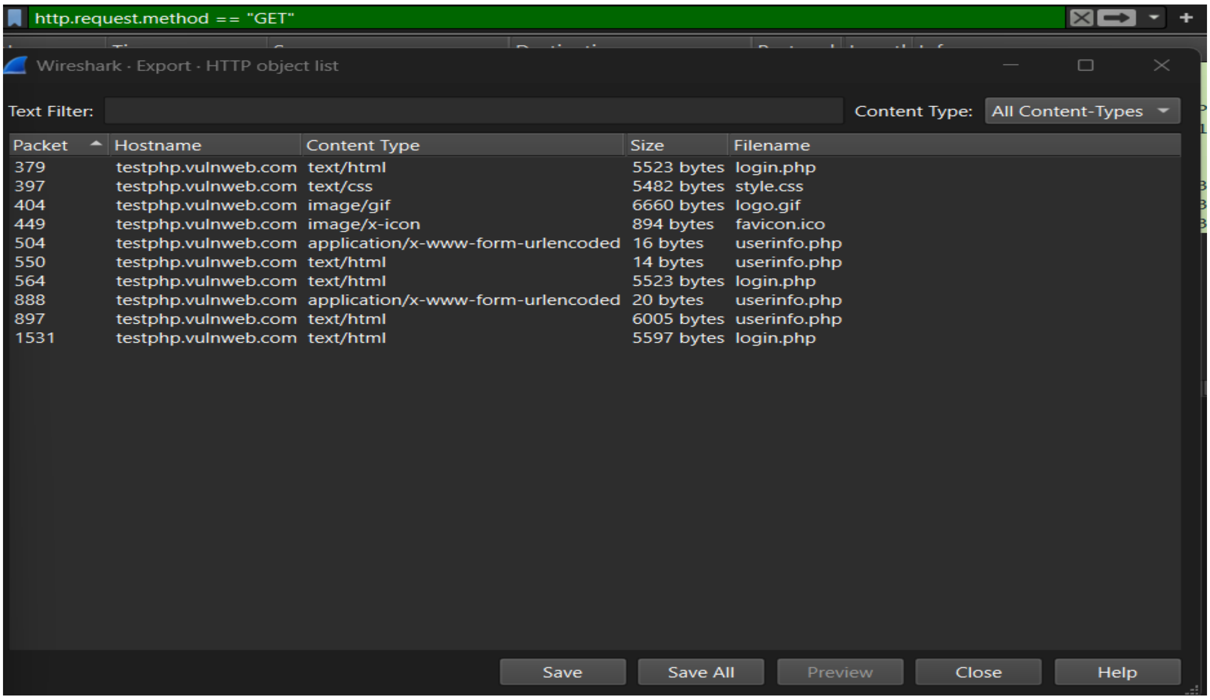
http.response.code == 200

```
No.    Time          Source          Destination     Protocol Length Info
   379 4.240496      44.228.249.3    172.16.31.221   HTTP       1342 HTTP/1.1 200 OK  (text/htm]
   397 4.522362      44.228.249.3    172.16.31.221   HTTP       1156 HTTP/1.1 200 OK  (text/css)
   404 4.525587      44.228.249.3    172.16.31.221   HTTP        874 HTTP/1.1 200 OK  (GIF89a)
   449 4.853499      44.228.249.3    172.16.31.221   HTTP        948 HTTP/1.1 200 OK  (image/x-i
   564 8.734117      44.228.249.3    172.16.31.221   HTTP       1342 HTTP/1.1 200 OK  (text/htm]
   897 16.287169     44.228.249.3    172.16.31.221   HTTP         73 HTTP/1.1 200 OK  (text/htm]
  1531 30.115576     44.228.249.3    172.16.31.221   HTTP       1367 HTTP/1.1 200 OK  (text/htm]
```

```
▸ Frame 379: Packet, 1342 bytes on wire (10736 bits), 1342 bytes captured
▸ Ethernet II, Src: Netgear_74:1f:81 (94:a6:7e:74:1f:81), Dst: CyberTANTec
▸ Internet Protocol Version 4, Src: 44.228.249.3, Dst: 172.16.31.221
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 55648, Seq: 1461,
▸ [2 Reassembled TCP Segments (2748 bytes): #378(1460), #379(1288)]
▾ Hypertext Transfer Protocol, has 2 chunks (including last chunk)
  ▾ HTTP/1.1 200 OK\r\n
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Server: nginx/1.19.0\r\n
    Date: Tue, 16 Dec 2025 09:11:58 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: 309]
    [Time since request: 243.473000 milliseconds]
    [Request URI: /login.php]
```

```
0000  00 45 e2 fb 3e 0d 94
0010  05 30 59 a4 40 00 33
0020  1f dd 00 50 d9 60 19
0030  01 e7 08 62 00 00 23
0040  78 44 d5 8c ea 02 f1
0050  2d 5f 7c a7 01 41 f7
0060  94 ae 48 c5 23 aa 61
0070  6d 36 97 b0 e5 82 57
0080  4f 14 5a 87 26 82 99
0090  27 20 f2 ff fe 40 b4
00a0  c8 b6 f1 4e f4 7f 3b
00b0  75 84 0c 19 4d 7e 2e
00c0  8a 07 e7 cd f1 14 d0
00d0  89 45 12 93 c8 b5 9d
00e0  f9 80 aa 3b aa 28 c5
00f0  04 d9 e0 90 52 b5 9f
0100  6f 5d d2 19 c1 75 5e
0110  67 64 a5 ef 49 99 f4
0120  93 b6 e2 48 ad 89 bf
0130  fa 41 ee c9 de 2a f4
0140  b3 73 6b a6 ce 5a 6b
0150  99 ce 85 8a eb 92 a1
```

wireshark_Wi-FiRGTVH3.pcapng   Packets: 2121 · Displayed: 7 (0.3%) · Dropped: 0 (0.0%)   Profile: Default


http.request.method == "GET"

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
379	testphp.vulnweb.com	text/html	5523 bytes	login.php
397	testphp.vulnweb.com	text/css	5482 bytes	style.css
404	testphp.vulnweb.com	image/gif	6660 bytes	logo.gif
449	testphp.vulnweb.com	image/x-icon	894 bytes	favicon.ico
504	testphp.vulnweb.com	application/x-www-form-urlencoded	16 bytes	userinfo.php
550	testphp.vulnweb.com	text/html	14 bytes	userinfo.php
564	testphp.vulnweb.com	text/html	5523 bytes	login.php
888	testphp.vulnweb.com	application/x-www-form-urlencoded	20 bytes	userinfo.php
897	testphp.vulnweb.com	text/html	6005 bytes	userinfo.php
1531	testphp.vulnweb.com	text/html	5597 bytes	login.php

3. **First Request (Cold Cache):**

- Browser: Sends a standard GET request. It has no copy of the file.
- Server: Responds with HTTP 200 OK and delivers the entire file payload. It also attaches a Last-Modified date or an ETag (Entity Tag) to signature the file.

Second Request (Warm Cache):

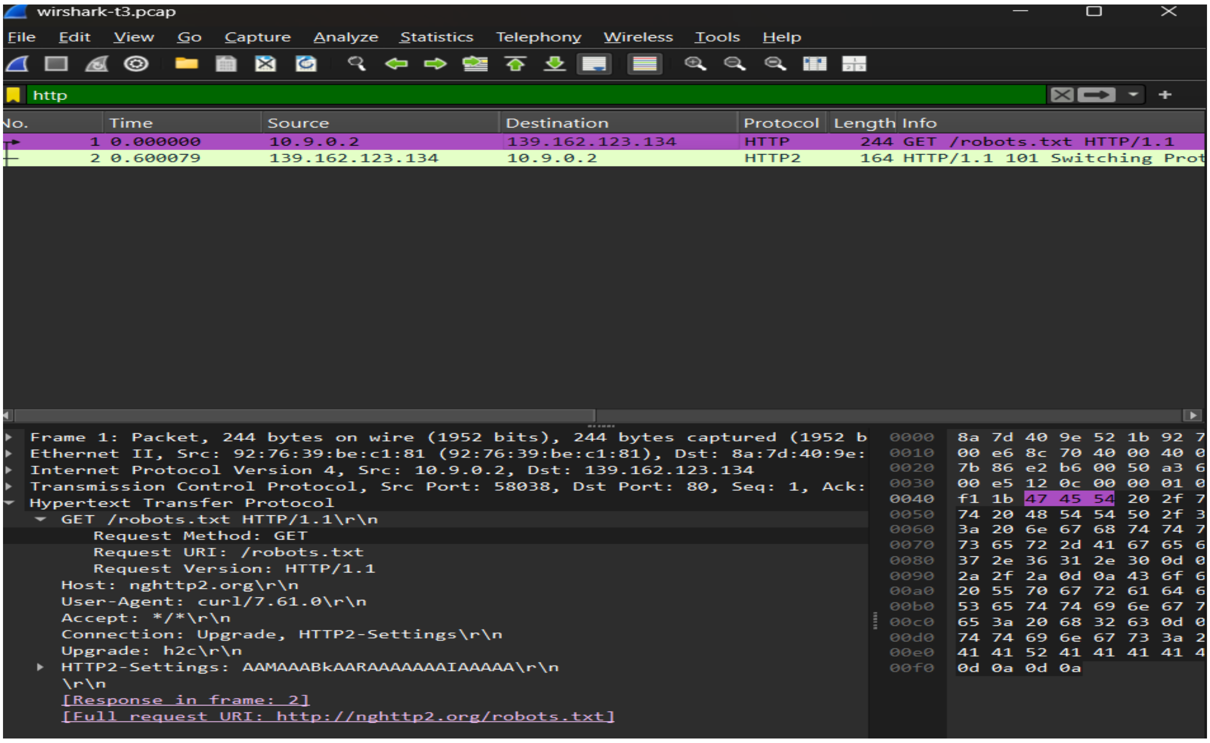
- **Browser:** Detects it has a copy of the file. It sends a Conditional GET. It looks at the previous Last-Modified date and sends it back to the server in a header called If Modified-Since.
- **Server**: Compares the If-Modified-Since date with the file's current date on the server.
  - If match: It sends HTTP 304 Not Modified. It sends no file data, saving bandwidth.
  - If different: It sends HTTP 200 OK with the new file.

4. Request Headers (Sent by Browser):

- If-Modified-Since: The date of the cached version the browser holds.
- If-None-Match: The ETag (hash) of the cached version. • Cache-Control: (e.g., max-age=0 forces a check). Response Headers (Sent by Server):
- Last-Modified: The date the file was last changed on the server.
- ETag: A unique identifier for that specific version of the file.
- Expires: A date after which the cache is considered stale.

Task 3:

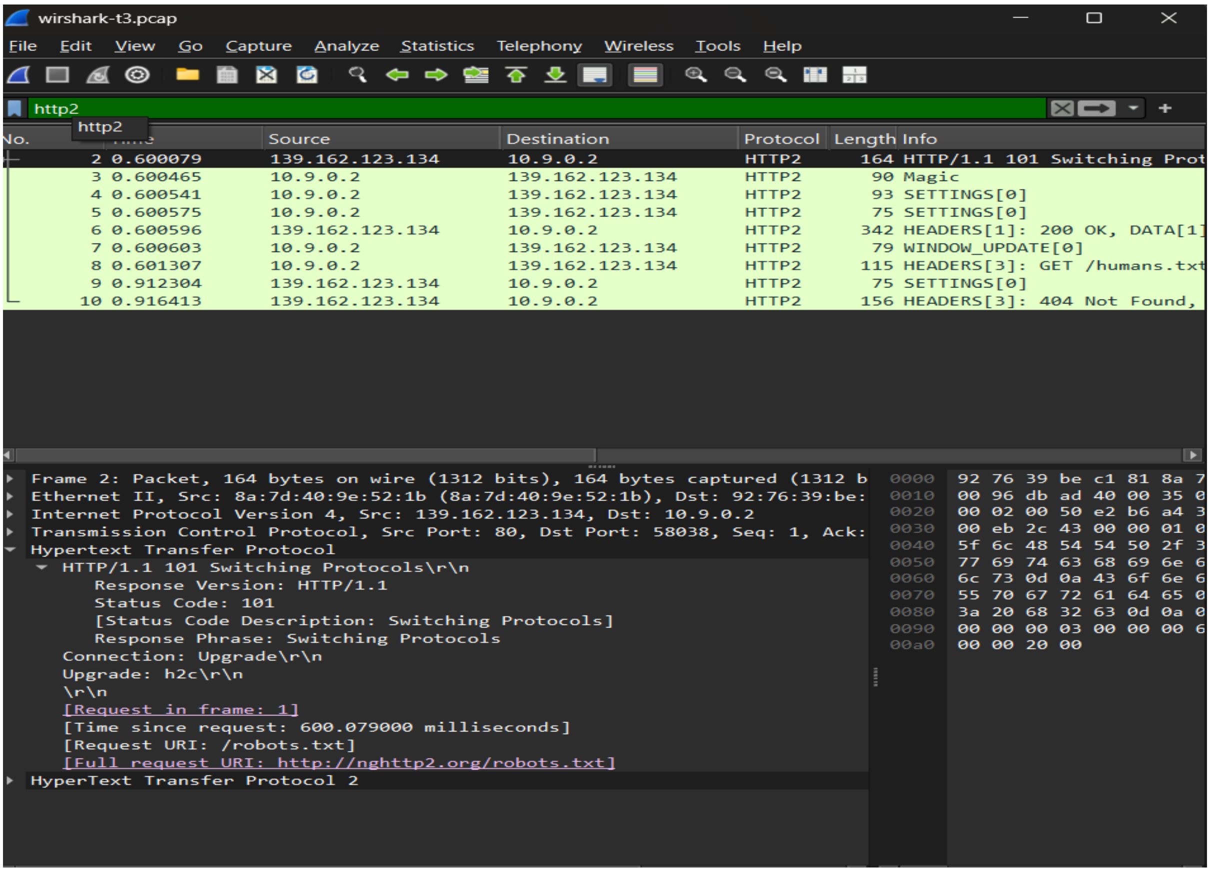
1. How many HTTP/2 and HTTP/1.1 packets are present?



```
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 Prot
```

```
Frame 1: Packet, 244 bytes on wire (1952 bits), 244 bytes captured (1952 b
Ethernet II, Src: 92:76:39:be:c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9e:
Internet Protocol Version 4, Src: 10.9.0.2, Dst: 139.162.123.134
Transmission Control Protocol, Src Port: 58038, Dst Port: 80, Seq: 1, Ack:
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: AAMAAABkAARAAAAAAAIAAAAA\r\n
  \r\n
  [Response in frame: 2]
  [Full request URI: http://nghttp2.org/robots.txt]
```

```
0000  8a 7d 40 9e 52 1b 92 7
0010  00 e6 8c 70 40 00 40 0
0020  7b 86 e2 b6 00 50 a3 6
0030  00 e5 12 0c 00 00 01 0
0040  f1 1b 47 45 54 20 2f 7
0050  74 20 48 54 54 50 2f 3
0060  3a 20 6e 67 68 74 74 7
0070  73 65 72 2d 41 67 65 6
0080  37 2e 36 31 2e 30 0d 0
0090  2a 2f 2a 0d 0a 43 6f 6
00a0  20 55 70 67 72 61 64 6
00b0  53 65 74 74 69 6e 67 7
00c0  65 3a 20 68 32 63 0d 0
00d0  74 74 69 6e 67 73 3a 2
00e0  41 41 52 41 41 41 41 4
00f0  0d 0a 0d 0a
```


wirshark-t3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

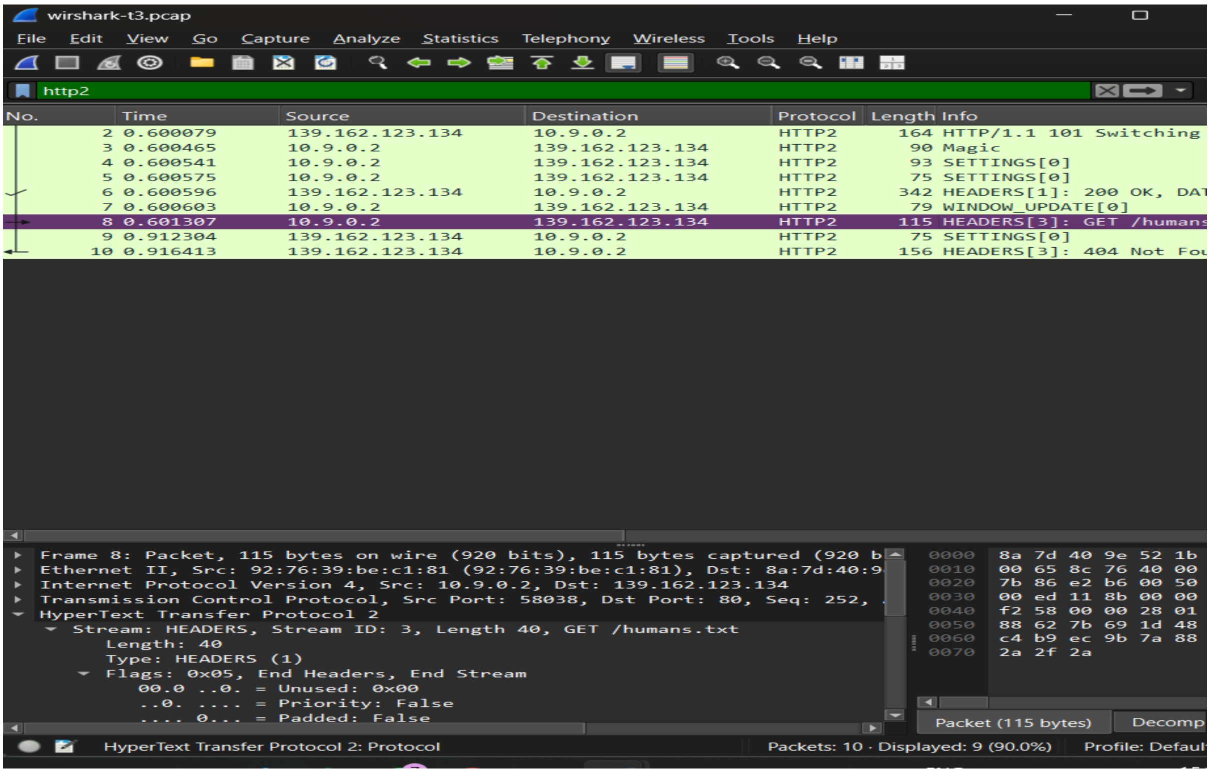
```
http2
```

```
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 Prot
    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]
    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 0.912304   139.162.123.134   10.9.0.2          HTTP2     75 SETTINGS[0]
   10 0.916413   139.162.123.134   10.9.0.2          HTTP2    156 HEADERS[3]: 404 Not Found,
```

```
▸ Frame 2: Packet, 164 bytes on wire (1312 bits), 164 bytes captured (1312 b
▸ Ethernet II, Src: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b), Dst: 92:76:39:be:
▸ Internet Protocol Version 4, Src: 139.162.123.134, Dst: 10.9.0.2
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 58038, Seq: 1, Ack:
▾ Hypertext Transfer Protocol
   ▾ HTTP/1.1 101 Switching Protocols\r\n
        Response Version: HTTP/1.1
        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: 600.079000 milliseconds]
     [Request URI: /robots.txt]
     [Full request URI: http://nghttp2.org/robots.txt]
▸ HyperText Transfer Protocol 2
```

```
0000  92 76 39 be c1 81 8a 7
0010  00 96 db ad 40 00 35 0
0020  00 02 00 50 e2 b6 a4 3
0030  00 eb 2c 43 00 00 01 0
0040  5f 6c 48 54 54 50 2f 3
0050  77 69 74 63 68 69 6e 6
0060  6c 73 0d 0a 43 6f 6e 6
0070  55 70 67 72 61 64 65 0
0080  3a 20 68 32 63 0d 0a 0
0090  00 00 00 03 00 00 00 6
00a0  00 00 20 00
```

2. HowmanyHTTP/2packetsareexchangedbetweenclientandserverherebeforethe first object is fetched?


wirshark-t3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http2
```

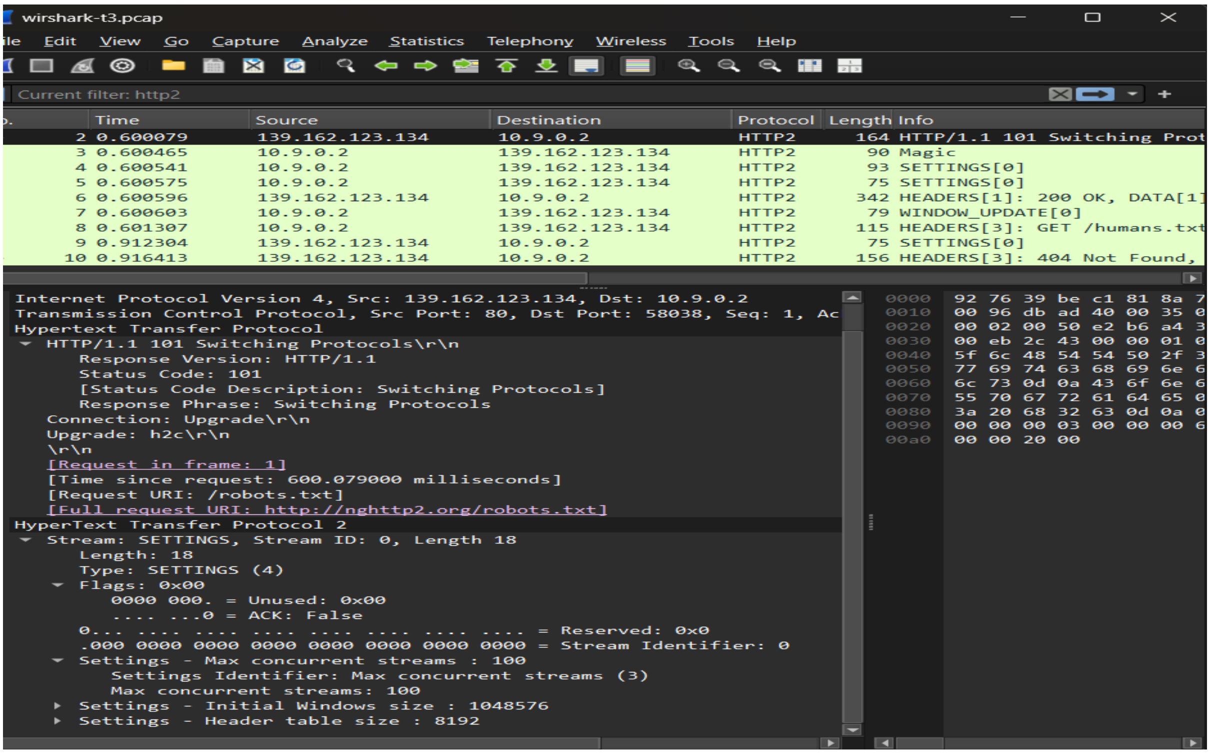
```
No.   Time       Source            Destination       Protocol Length Info
    2 0.600079   139.162.123.134   10.9.0.2          HTTP2    164 HTTP/1.1 101 Switching
    3 0.600465   10.9.0.2          139.162.123.134   HTTP2     90 Magic
    4 0.600541   10.9.0.2          139.162.123.134   HTTP2     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, DAT
    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
    9 0.912304   139.162.123.134   10.9.0.2          HTTP2     75 SETTINGS[0]
   10 0.916413   139.162.123.134   10.9.0.2          HTTP2    156 HEADERS[3]: 404 Not Fou
```

```
▸ Frame 8: Packet, 115 bytes on wire (920 bits), 115 bytes captured (920 b
▸ Ethernet II, Src: 92:76:39:be:c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9
▸ 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,
▾ HyperText Transfer Protocol 2
   ▾ Stream: HEADERS, Stream ID: 3, Length 40, GET /humans.txt
        Length: 40
        Type: HEADERS (1)
      ▾ Flags: 0x05, End Headers, End Stream
           00.0 ..0. = Unused: 0x00
           ..0. .... = Priority: False
           .... 0... = Padded: False
```

```
0000  8a 7d 40 9e 52 1b
0010  00 65 8c 76 40 00
0020  7b 86 e2 b6 00 50
0030  00 ed 11 8b 00 00
0040  f2 58 00 00 28 01
0050  88 62 7b 69 1d 48
0060  c4 b9 ec 9b 7a 88
0070  2a 2f 2a
```

```
HyperText Transfer Protocol 2: Protocol    Packets: 10 · Displayed: 9 (90.0%)    Profile: Defaul
```

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



```
o.     Time        Source            Destination       Protocol Length Info
     2 0.600079    139.162.123.134   10.9.0.2          HTTP2      164 HTTP/1.1 101 Switching Prot
     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]
     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 0.912304    139.162.123.134   10.9.0.2          HTTP2       75 SETTINGS[0]
    10 0.916413    139.162.123.134   10.9.0.2          HTTP2      156 HEADERS[3]: 404 Not Found,
```

```
Internet Protocol Version 4, Src: 139.162.123.134, Dst: 10.9.0.2
Transmission Control Protocol, Src Port: 80, Dst Port: 58038, Seq: 1, Ac
Hypertext Transfer Protocol
  HTTP/1.1 101 Switching Protocols\r\n
      Response Version: HTTP/1.1
      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: 600.079000 milliseconds]
  [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
        0000 000. = Unused: 0x00
        .... ...0 = ACK: False
      0... .... .... .... .... .... .... .... = Reserved: 0x0
      .000 0000 0000 0000 0000 0000 0000 0000 = Stream Identifier: 0
    Settings - Max concurrent streams : 100
        Settings Identifier: Max concurrent streams (3)
        Max concurrent streams: 100
    Settings - Initial Windows size : 1048576
    Settings - Header table size : 8192
```

```
0000   92 76 39 be c1 81 8a 7
0010   00 96 db ad 40 00 35 0
0020   00 02 00 50 e2 b6 a4 3
0030   00 eb 2c 43 00 00 01 0
0040   5f 6c 48 54 54 50 2f 3
0050   77 69 74 63 68 69 6e 6
0060   6c 73 0d 0a 43 6f 6e 6
0070   55 70 67 72 61 64 65 0
0080   3a 20 68 32 63 0d 0a 0
0090   00 00 00 03 00 00 00 6
00a0   00 00 20 00
```