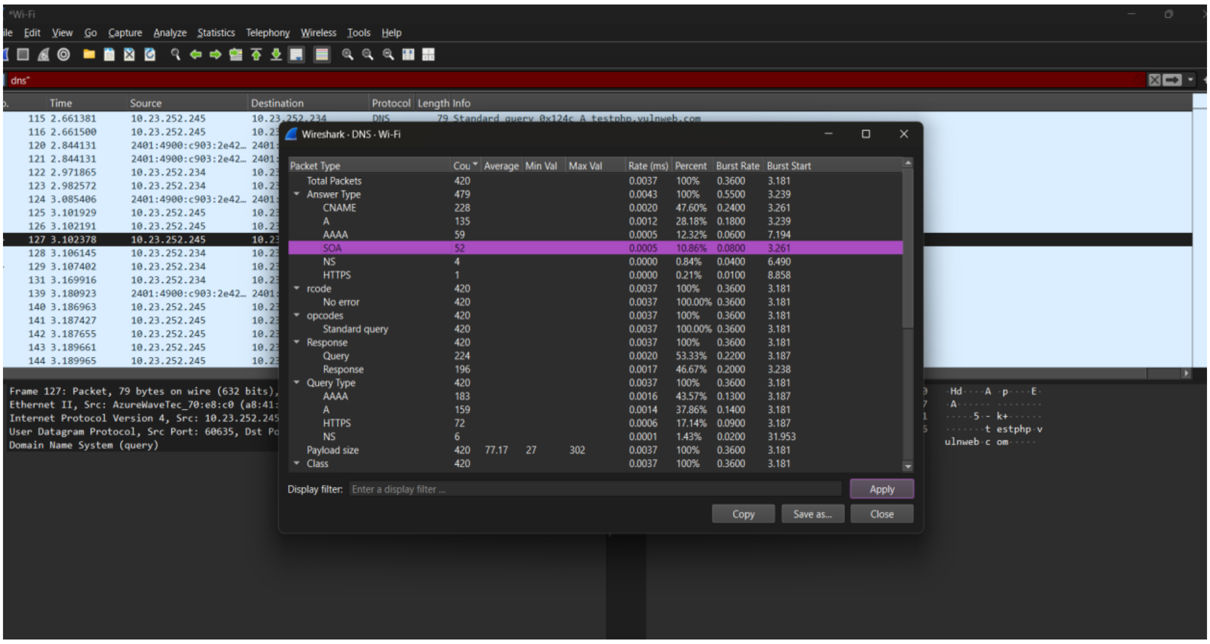
TASK 1

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



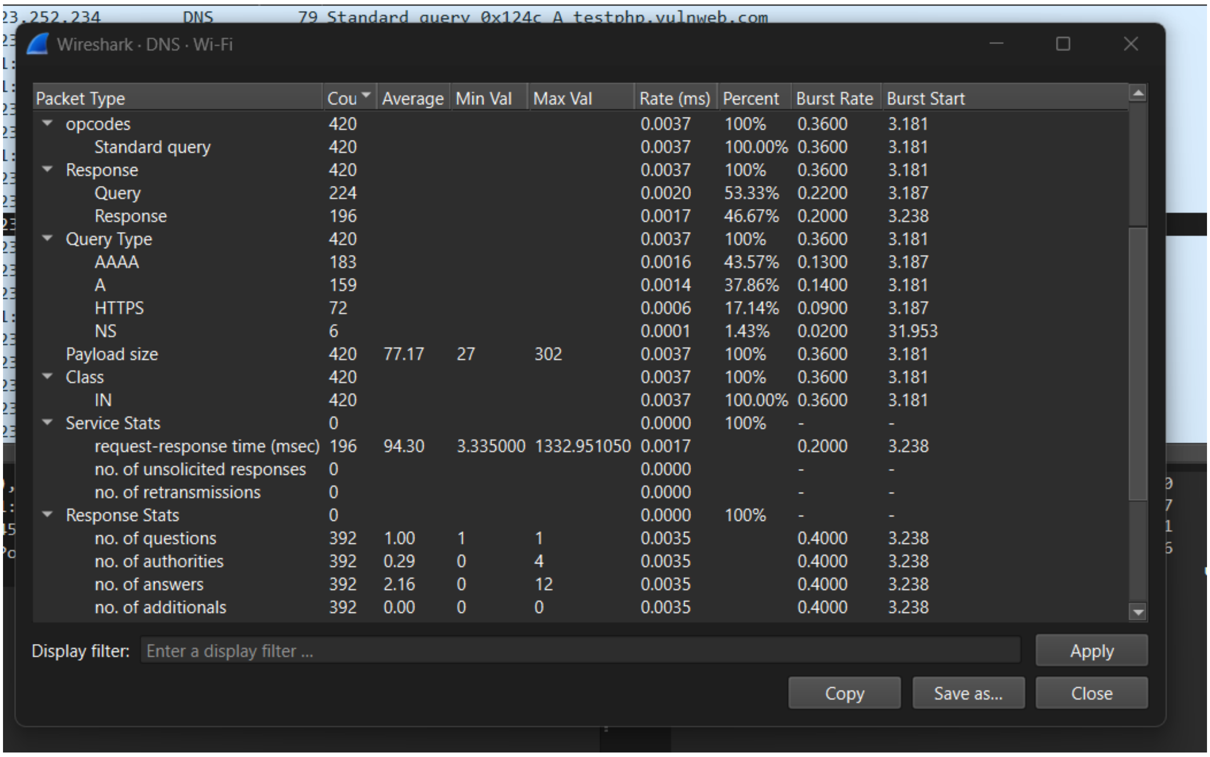
```
*Wi-Fi
. Time        Source                    Destination     Protocol Length Info
115 2.661381  10.23.252.245             10.23.252.234   DNS      79 Standard query 0x124c A testphp.vulnweb.com
116 2.661500  10.23.252.245             10.23
120 2.844131  2401:4900:c903:2e42…      2401
121 2.844131  2401:4900:c903:2e42…      2401
122 2.971865  10.23.252.234             10.23
123 2.982572  10.23.252.234             10.23
124 3.085406  2401:4900:c903:2e42…      2401
125 3.101929  10.23.252.245             10.23
126 3.102191  10.23.252.245             10.23
127 3.102378  10.23.252.245             10.23
128 3.106145  10.23.252.234             10.23
129 3.107402  10.23.252.234             10.23
131 3.169916  10.23.252.234             10.23
139 3.180923  2401:4900:c903:2e42…      2401
140 3.186963  10.23.252.245             10.23
141 3.187427  10.23.252.245             10.23
142 3.187655  10.23.252.245             10.23
143 3.189661  10.23.252.245             10.23
144 3.189965  10.23.252.245             10.23

Frame 127: Packet, 79 bytes on wire (632 bits),
Ethernet II, Src: AzureWaveTec_70:e8:c0 (a8:41:
Internet Protocol Version 4, Src: 10.23.252.245
User Datagram Protocol, Src Port: 60635, Dst Po
Domain Name System (query)
```

Wireshark · DNS · Wi-Fi

Packet Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total Packets	420				0.0037	100%	0.3600	3.181
Answer Type	479				0.0043	100%	0.5500	3.239
CNAME	228				0.0020	47.60%	0.2400	3.261
A	135				0.0012	28.18%	0.1800	3.239
AAAA	59				0.0005	12.32%	0.0600	7.194
SOA	52				0.0005	10.86%	0.0800	3.261
NS	4				0.0000	0.84%	0.0400	6.490
HTTPS	1				0.0000	0.21%	0.0100	8.858
rcode	420				0.0037	100%	0.3600	3.181
No error	420				0.0037	100.00%	0.3600	3.181
opcodes	420				0.0037	100%	0.3600	3.181
Standard query	420				0.0037	100.00%	0.3600	3.181
Response	420				0.0037	100%	0.3600	3.181
Query	224				0.0020	53.33%	0.2200	3.187
Response	196				0.0017	46.67%	0.2000	3.238
Query Type	420				0.0037	100%	0.3600	3.181
AAAA	183				0.0016	43.57%	0.1300	3.187
A	159				0.0014	37.86%	0.1400	3.181
HTTPS	72				0.0006	17.14%	0.0900	3.187
NS	6				0.0001	1.43%	0.0200	31.953
Payload size	420	77.17	27	302	0.0037	100%	0.3600	3.181
Class	420				0.0037	100%	0.3600	3.181

Display filter: Enter a display filter ...

How many DNS servers are involved



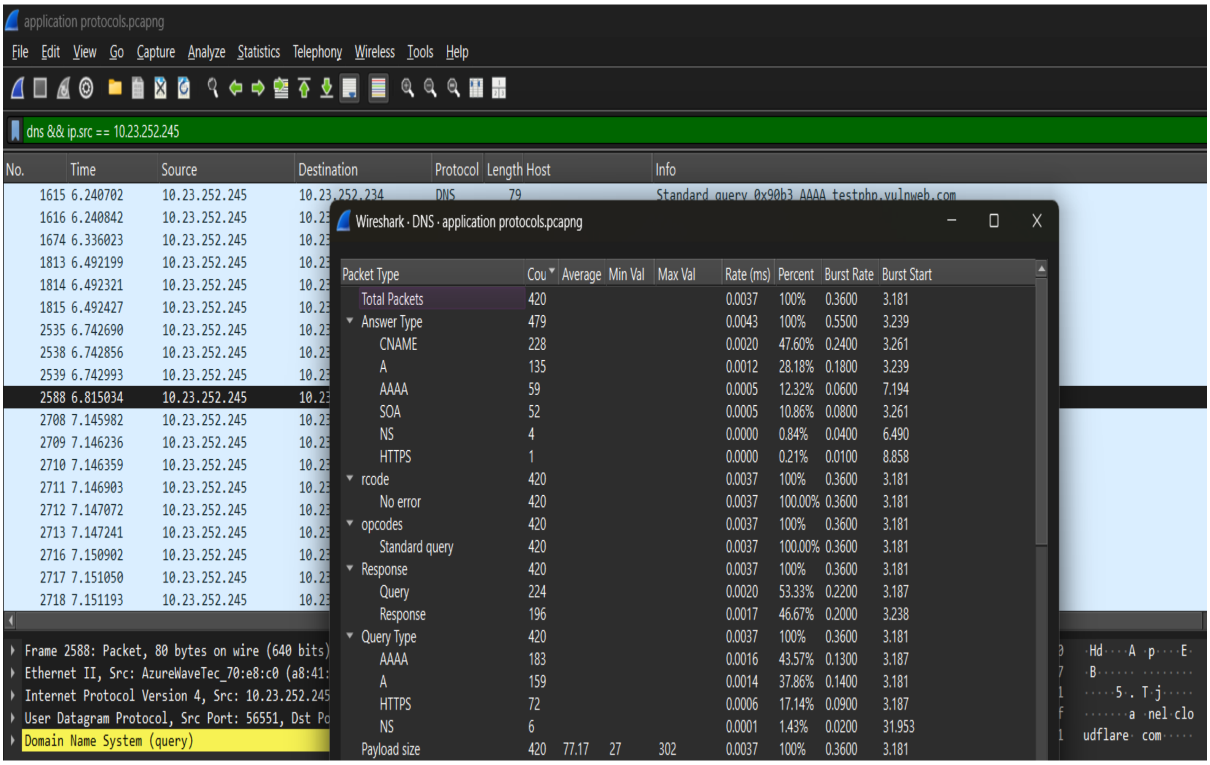
```
23.252.234          DNS          79 Standard query 0x124c A testphp.vulnweb.com
```

Wireshark · DNS · Wi-Fi

Packet Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
opcodes	420				0.0037	100%	0.3600	3.181
Standard query	420				0.0037	100.00%	0.3600	3.181
Response	420				0.0037	100%	0.3600	3.181
Query	224				0.0020	53.33%	0.2200	3.187
Response	196				0.0017	46.67%	0.2000	3.238
Query Type	420				0.0037	100%	0.3600	3.181
AAAA	183				0.0016	43.57%	0.1300	3.187
A	159				0.0014	37.86%	0.1400	3.181
HTTPS	72				0.0006	17.14%	0.0900	3.187
NS	6				0.0001	1.43%	0.0200	31.953
Payload size	420	77.17	27	302	0.0037	100%	0.3600	3.181
Class	420				0.0037	100%	0.3600	3.181
IN	420				0.0037	100.00%	0.3600	3.181
Service Stats	0				0.0000	100%	-	-
request-response time (msec)	196	94.30	3.335000	1332.951050	0.0017		0.2000	3.238
no. of unsolicited responses	0				0.0000		-	-
no. of retransmissions	0				0.0000		-	-
Response Stats	0				0.0000	100%	-	-
no. of questions	392	1.00	1	1	0.0035		0.4000	3.238
no. of authorities	392	0.29	0	4	0.0035		0.4000	3.238
no. of answers	392	2.16	0	12	0.0035		0.4000	3.238
no. of additionals	392	0.00	0	0	0.0035		0.4000	3.238

Display filter: Enter a display filter ...

Which DNS Server replies with actual IP Address(es).



application protocols.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns && ip.src == 10.23.252.245

```
No.   Time      Source          Destination    Protocol Length Host  Info
1615 6.240702  10.23.252.245   10.23.252.234  DNS      79          Standard query 0x90b3 AAAA testphp.vulnweb.com
1616 6.240842  10.23.252.245   10.23
1674 6.336023  10.23.252.245   10.23
1813 6.492199  10.23.252.245   10.23
1814 6.492321  10.23.252.245   10.23
1815 6.492427  10.23.252.245   10.23
2535 6.742690  10.23.252.245   10.23
2538 6.742856  10.23.252.245   10.23
2539 6.742993  10.23.252.245   10.23
2588 6.815034  10.23.252.245   10.23
2708 7.145982  10.23.252.245   10.23
2709 7.146236  10.23.252.245   10.23
2710 7.146359  10.23.252.245   10.23
2711 7.146903  10.23.252.245   10.23
2712 7.147072  10.23.252.245   10.23
2713 7.147241  10.23.252.245   10.23
2716 7.150902  10.23.252.245   10.23
2717 7.151050  10.23.252.245   10.23
2718 7.151193  10.23.252.245   10.23
```

```
Frame 2588: Packet, 80 bytes on wire (640 bits)
Ethernet II, Src: AzureWaveTec_70:e8:c0 (a8:41:
Internet Protocol Version 4, Src: 10.23.252.245
User Datagram Protocol, Src Port: 56551, Dst Po
Domain Name System (query)
```

Wireshark · DNS · application protocols.pcapng

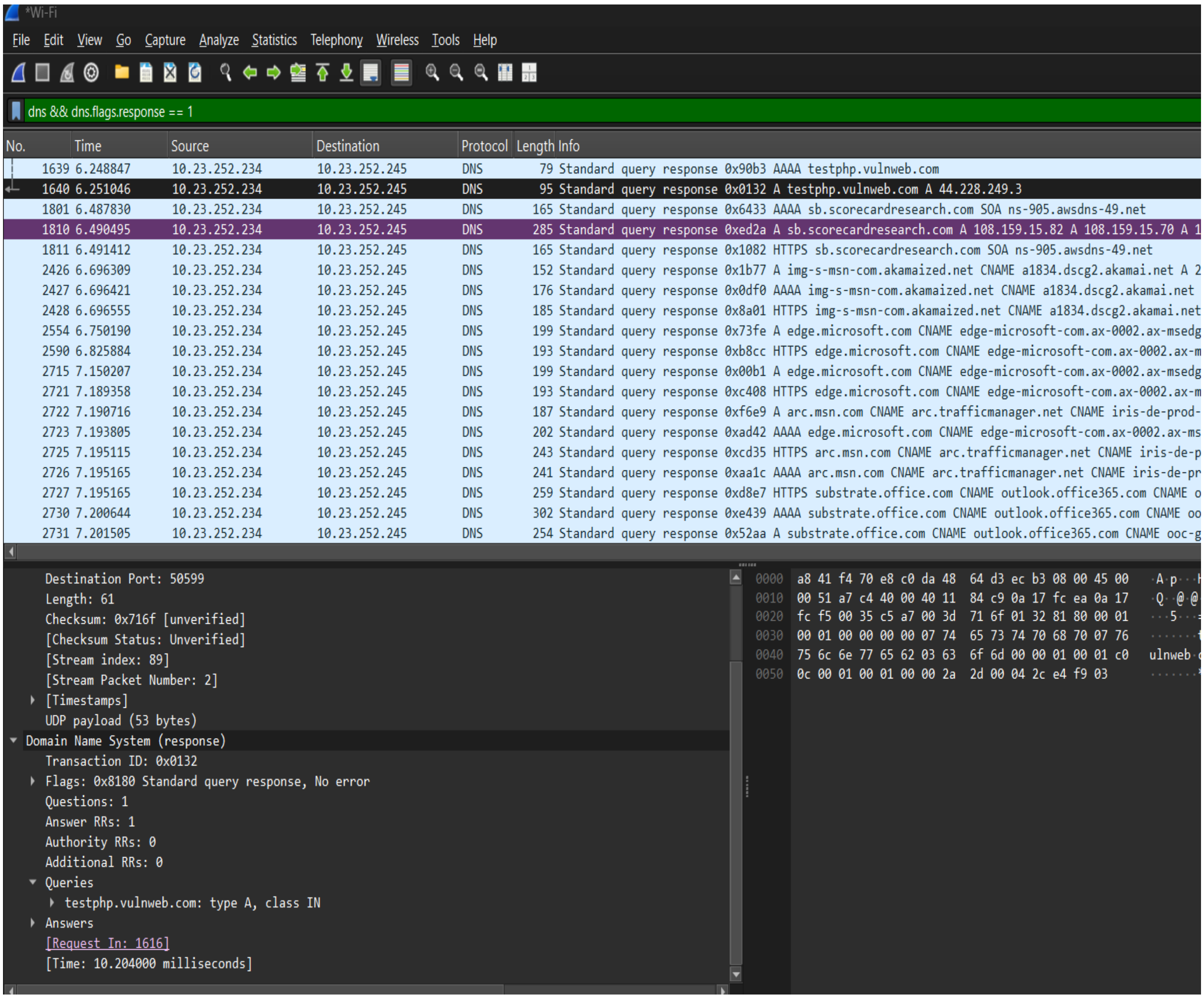
Packet Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total Packets	420				0.0037	100%	0.3600	3.181
Answer Type	479				0.0043	100%	0.5500	3.239
CNAME	228				0.0020	47.60%	0.2400	3.261
A	135				0.0012	28.18%	0.1800	3.239
AAAA	59				0.0005	12.32%	0.0600	7.194
SOA	52				0.0005	10.86%	0.0800	3.261
NS	4				0.0000	0.84%	0.0400	6.490
HTTPS	1				0.0000	0.21%	0.0100	8.858
rcode	420				0.0037	100%	0.3600	3.181
No error	420				0.0037	100.00%	0.3600	3.181
opcodes	420				0.0037	100%	0.3600	3.181
Standard query	420				0.0037	100.00%	0.3600	3.181
Response	420				0.0037	100%	0.3600	3.181
Query	224				0.0020	53.33%	0.2200	3.187
Response	196				0.0017	46.67%	0.2000	3.238
Query Type	420				0.0037	100%	0.3600	3.181
AAAA	183				0.0016	43.57%	0.1300	3.187
A	159				0.0014	37.86%	0.1400	3.181
HTTPS	72				0.0006	17.14%	0.0900	3.187
NS	6				0.0001	1.43%	0.0200	31.953
Payload size	420	77.17	27	302	0.0037	100%	0.3600	3.181

```
·Hd···A ·p···E·
·B······ ········
·····5·. T·j·····
·······a ·nel·clo
udflare· com·····
```

Do all DNS servers respond

Ans: NO

Clearly list the resource records involved in resolving the IP address of the site, mentioning, Name, value, type, TTL appropriately in the complete resolving process of this DNS conversation including query/queries and response/answer(s).



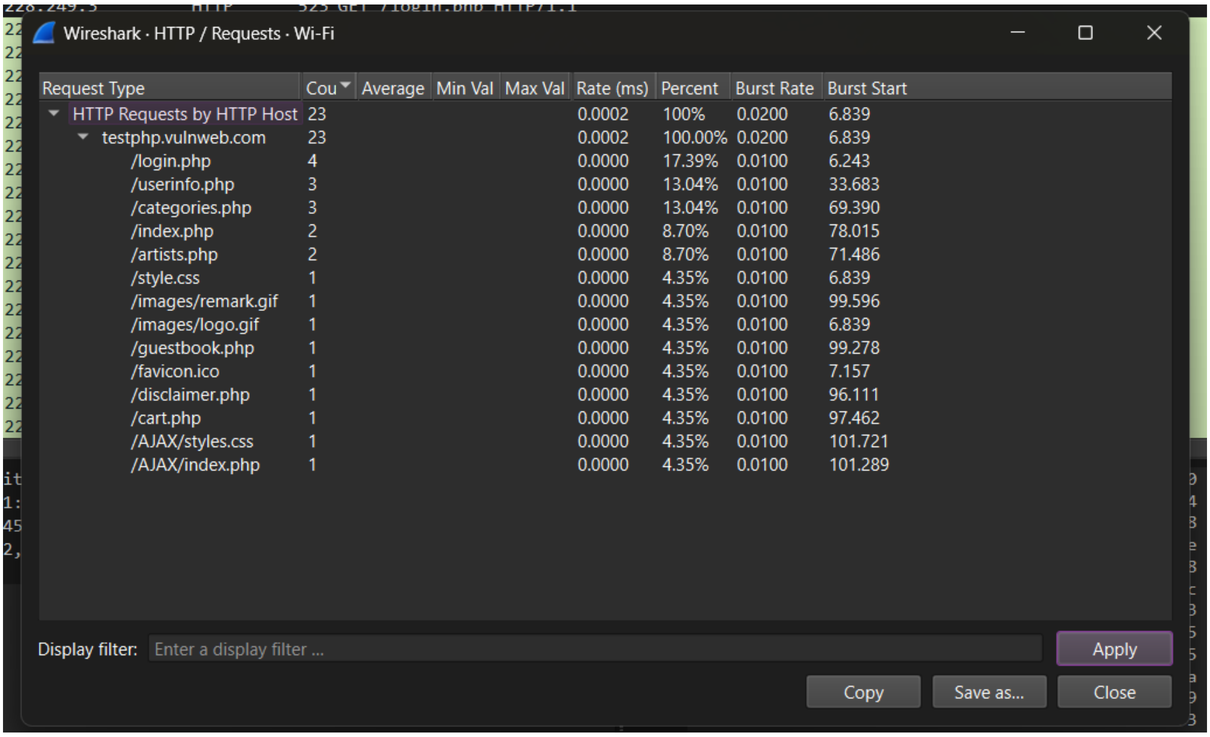
dns && dns.flags.response == 1

No.	Time	Source	Destination	Protocol	Length	Info
1639	6.248847	10.23.252.234	10.23.252.245	DNS	79	Standard query response 0x90b3 AAAA testphp.vulnweb.com
1640	6.251046	10.23.252.234	10.23.252.245	DNS	95	Standard query response 0x0132 A testphp.vulnweb.com A 44.228.249.3
1801	6.487830	10.23.252.234	10.23.252.245	DNS	165	Standard query response 0x6433 AAAA sb.scorecardresearch.com SOA ns-905.awsdns-49.net
1810	6.490495	10.23.252.234	10.23.252.245	DNS	285	Standard query response 0xed2a A sb.scorecardresearch.com A 108.159.15.82 A 108.159.15.70 A 1
1811	6.491412	10.23.252.234	10.23.252.245	DNS	165	Standard query response 0x1082 HTTPS sb.scorecardresearch.com SOA ns-905.awsdns-49.net
2426	6.696309	10.23.252.234	10.23.252.245	DNS	152	Standard query response 0x1b77 A img-s-msn-com.akamaized.net CNAME a1834.dscg2.akamai.net A 2
2427	6.696421	10.23.252.234	10.23.252.245	DNS	176	Standard query response 0x0df0 AAAA img-s-msn-com.akamaized.net CNAME a1834.dscg2.akamai.net
2428	6.696555	10.23.252.234	10.23.252.245	DNS	185	Standard query response 0x8a01 HTTPS img-s-msn-com.akamaized.net CNAME a1834.dscg2.akamai.net
2554	6.750190	10.23.252.234	10.23.252.245	DNS	199	Standard query response 0x73fe A edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedg
2590	6.825884	10.23.252.234	10.23.252.245	DNS	193	Standard query response 0xb8cc HTTPS edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-m
2715	7.150207	10.23.252.234	10.23.252.245	DNS	199	Standard query response 0x00b1 A edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedg
2721	7.189358	10.23.252.234	10.23.252.245	DNS	193	Standard query response 0xc408 HTTPS edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-m
2722	7.190716	10.23.252.234	10.23.252.245	DNS	187	Standard query response 0xf6e9 A arc.msn.com CNAME arc.trafficmanager.net CNAME iris-de-prod-
2723	7.193805	10.23.252.234	10.23.252.245	DNS	202	Standard query response 0xad42 AAAA edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-ms
2725	7.195115	10.23.252.234	10.23.252.245	DNS	243	Standard query response 0xcd35 HTTPS arc.msn.com CNAME arc.trafficmanager.net CNAME iris-de-p
2726	7.195165	10.23.252.234	10.23.252.245	DNS	241	Standard query response 0xaa1c AAAA arc.msn.com CNAME arc.trafficmanager.net CNAME iris-de-pr
2727	7.195165	10.23.252.234	10.23.252.245	DNS	259	Standard query response 0xd8e7 HTTPS substrate.office.com CNAME outlook.office365.com CNAME o
2730	7.200644	10.23.252.234	10.23.252.245	DNS	302	Standard query response 0xe439 AAAA substrate.office.com CNAME outlook.office365.com CNAME oo
2731	7.201505	10.23.252.234	10.23.252.245	DNS	254	Standard query response 0x52aa A substrate.office.com CNAME outlook.office365.com CNAME ooc-g

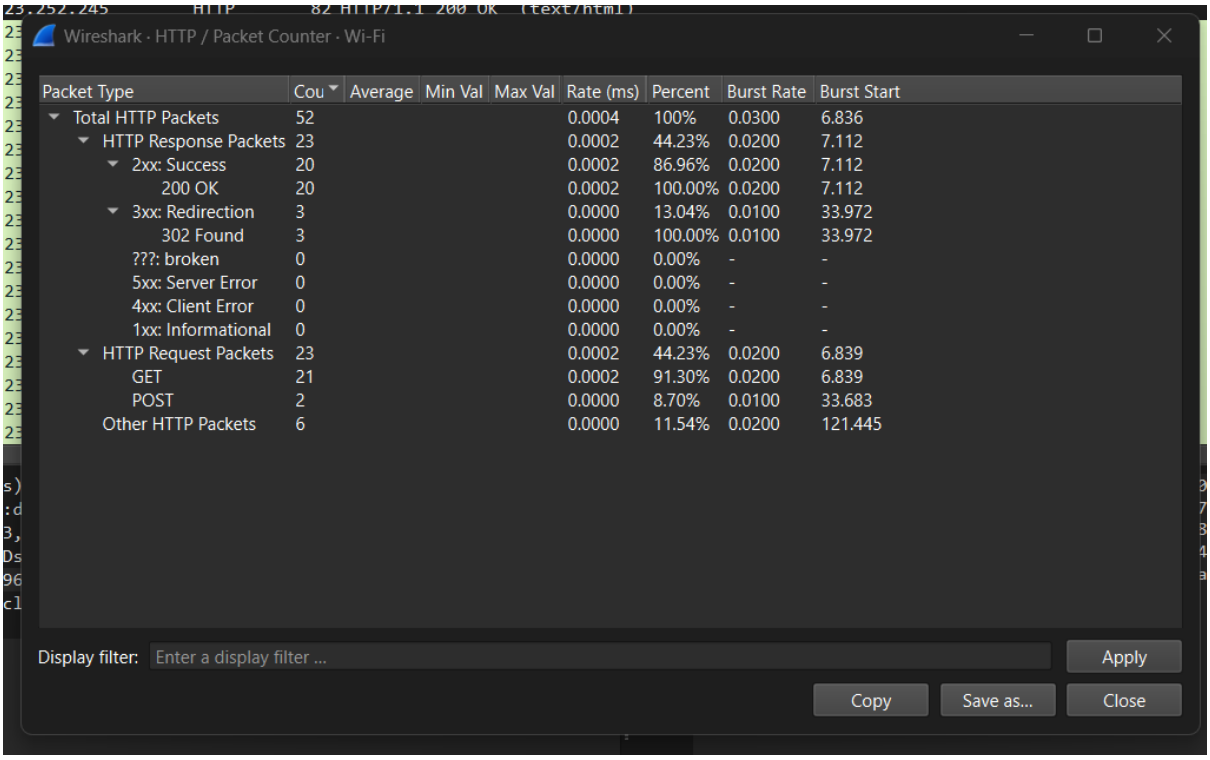
```
    Destination Port: 50599
    Length: 61
    Checksum: 0x716f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 89]
    [Stream Packet Number: 2]
  > [Timestamps]
    UDP payload (53 bytes)
v Domain Name System (response)
    Transaction ID: 0x0132
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > testphp.vulnweb.com: type A, class IN
  > Answers
    [Request In: 1616]
    [Time: 10.204000 milliseconds]
```

```
0000  a8 41 f4 70 e8 c0 da 48  64 d3 ec b3 08 00 45 00   ·A·p···H
0010  00 51 a7 c4 40 00 40 11  84 c9 0a 17 fc ea 0a 17   ·Q··@·@
0020  fc f5 00 35 c5 a7 00 3d  71 6f 01 32 81 80 00 01   ···5···
0030  00 01 00 00 00 00 07 74  65 73 74 70 68 70 07 76   ·······t
0040  75 6c 6e 77 65 62 03 63  6f 6d 00 00 01 00 01 c0   ulnweb·
0050  0c 00 01 00 01 00 00 2a  2d 00 04 2c e4 f9 03      ·······
```

2nd:

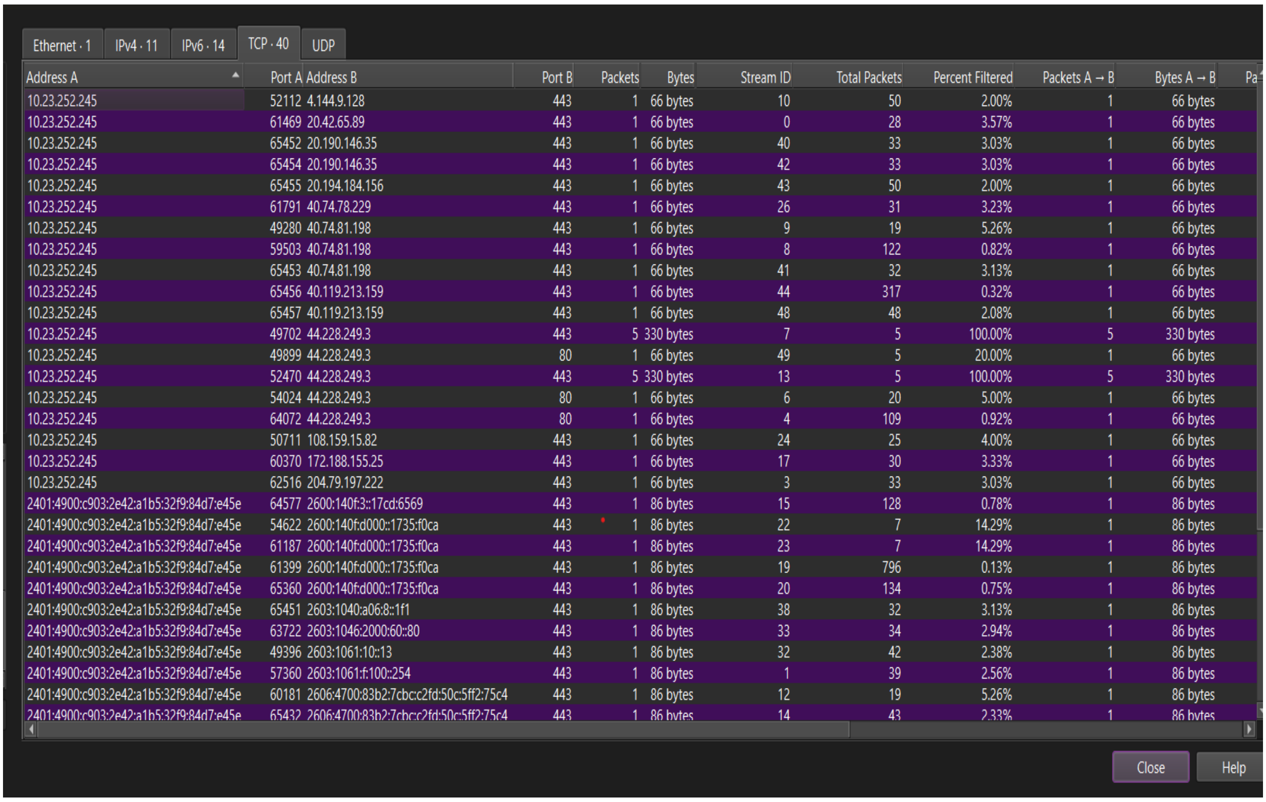

Wireshark · HTTP / Requests · Wi-Fi
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

Request Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Requests by HTTP Host	23				0.0002	100%	0.0200	6.839
testphp.vulnweb.com	23				0.0002	100.00%	0.0200	6.839
/login.php	4				0.0000	17.39%	0.0100	6.243
/userinfo.php	3				0.0000	13.04%	0.0100	33.683
/categories.php	3				0.0000	13.04%	0.0100	69.390
/index.php	2				0.0000	8.70%	0.0100	78.015
/artists.php	2				0.0000	8.70%	0.0100	71.486
/style.css	1				0.0000	4.35%	0.0100	6.839
/images/remark.gif	1				0.0000	4.35%	0.0100	99.596
/images/logo.gif	1				0.0000	4.35%	0.0100	6.839
/guestbook.php	1				0.0000	4.35%	0.0100	99.278
/favicon.ico	1				0.0000	4.35%	0.0100	7.157
/disclaimer.php	1				0.0000	4.35%	0.0100	96.111
/cart.php	1				0.0000	4.35%	0.0100	97.462
/AJAX/styles.css	1				0.0000	4.35%	0.0100	101.721
/AJAX/index.php	1				0.0000	4.35%	0.0100	101.289


Wireshark · HTTP / Packet Counter · Wi-Fi
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

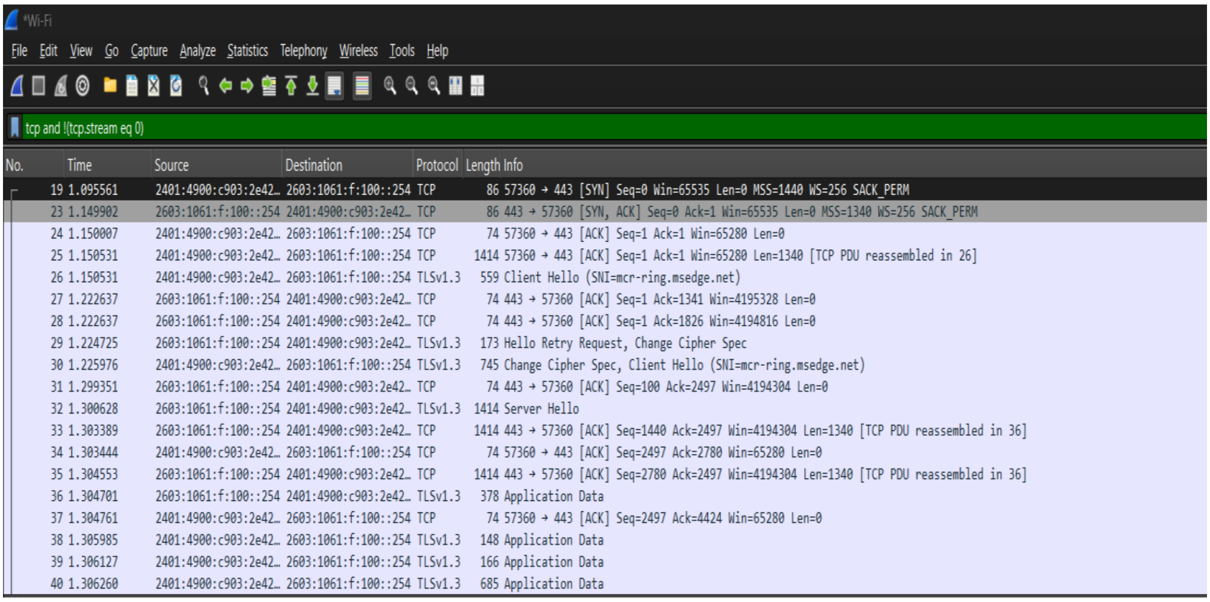
Packet Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	52				0.0004	100%	0.0300	6.836
HTTP Response Packets	23				0.0002	44.23%	0.0200	7.112
2xx: Success	20				0.0002	86.96%	0.0200	7.112
200 OK	20				0.0002	100.00%	0.0200	7.112
3xx: Redirection	3				0.0000	13.04%	0.0100	33.972
302 Found	3				0.0000	100.00%	0.0100	33.972
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	23				0.0002	44.23%	0.0200	6.839
GET	21				0.0002	91.30%	0.0200	6.839
POST	2				0.0000	8.70%	0.0100	33.683
Other HTTP Packets	6				0.0000	11.54%	0.0200	121.445

3rd:



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Pa
10.23.252.245	52112	4.144.9.128	443	1	66 bytes	10	50	2.00%	1	66 bytes	
10.23.252.245	61469	20.42.65.89	443	1	66 bytes	0	28	3.57%	1	66 bytes	
10.23.252.245	65452	20.190.146.35	443	1	66 bytes	40	33	3.03%	1	66 bytes	
10.23.252.245	65454	20.190.146.35	443	1	66 bytes	42	33	3.03%	1	66 bytes	
10.23.252.245	65455	20.194.184.156	443	1	66 bytes	43	50	2.00%	1	66 bytes	
10.23.252.245	61791	40.74.78.229	443	1	66 bytes	26	31	3.23%	1	66 bytes	
10.23.252.245	49280	40.74.81.198	443	1	66 bytes	9	19	5.26%	1	66 bytes	
10.23.252.245	59503	40.74.81.198	443	1	66 bytes	8	122	0.82%	1	66 bytes	
10.23.252.245	65453	40.74.81.198	443	1	66 bytes	41	32	3.13%	1	66 bytes	
10.23.252.245	65456	40.119.213.159	443	1	66 bytes	44	317	0.32%	1	66 bytes	
10.23.252.245	65457	40.119.213.159	443	1	66 bytes	48	48	2.08%	1	66 bytes	
10.23.252.245	49702	44.228.249.3	443	5	330 bytes	7	5	100.00%	5	330 bytes	
10.23.252.245	49899	44.228.249.3	80	1	66 bytes	49	5	20.00%	1	66 bytes	
10.23.252.245	52470	44.228.249.3	443	5	330 bytes	13	5	100.00%	5	330 bytes	
10.23.252.245	54024	44.228.249.3	80	1	66 bytes	6	20	5.00%	1	66 bytes	
10.23.252.245	64072	44.228.249.3	80	1	66 bytes	4	109	0.92%	1	66 bytes	
10.23.252.245	50711	108.159.15.82	443	1	66 bytes	24	25	4.00%	1	66 bytes	
10.23.252.245	60370	172.188.155.25	443	1	66 bytes	17	30	3.33%	1	66 bytes	
10.23.252.245	62516	204.79.197.222	443	1	66 bytes	3	33	3.03%	1	66 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	64577	2600:140f:3::17cd:6569	443	1	86 bytes	15	128	0.78%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	54622	2600:140f:d000::1735:f0ca	443	1	86 bytes	22	7	14.29%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	61187	2600:140f:d000::1735:f0ca	443	1	86 bytes	23	7	14.29%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	61399	2600:140f:d000::1735:f0ca	443	1	86 bytes	19	796	0.13%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	65360	2600:140f:d000::1735:f0ca	443	1	86 bytes	20	134	0.75%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	65451	2603:1040:a06:8::1f1	443	1	86 bytes	38	32	3.13%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	63722	2603:1046:2000:60::80	443	1	86 bytes	33	34	2.94%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	49396	2603:1061:10::13	443	1	86 bytes	32	42	2.38%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	57360	2603:1061:f:100::254	443	1	86 bytes	1	39	2.56%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	60181	2606:4700:83b2:7cbc:c2fd:50c:5ff2:75c4	443	1	86 bytes	12	19	5.26%	1	86 bytes	
2401:4900:c903:2e42:a1b5:32f9:84d7:e45e	65432	2606:4700:83b2:7cbc:c2fd:50c:5ff2:75c4	443	1	86 bytes	14	43	2.33%	1	86 bytes	

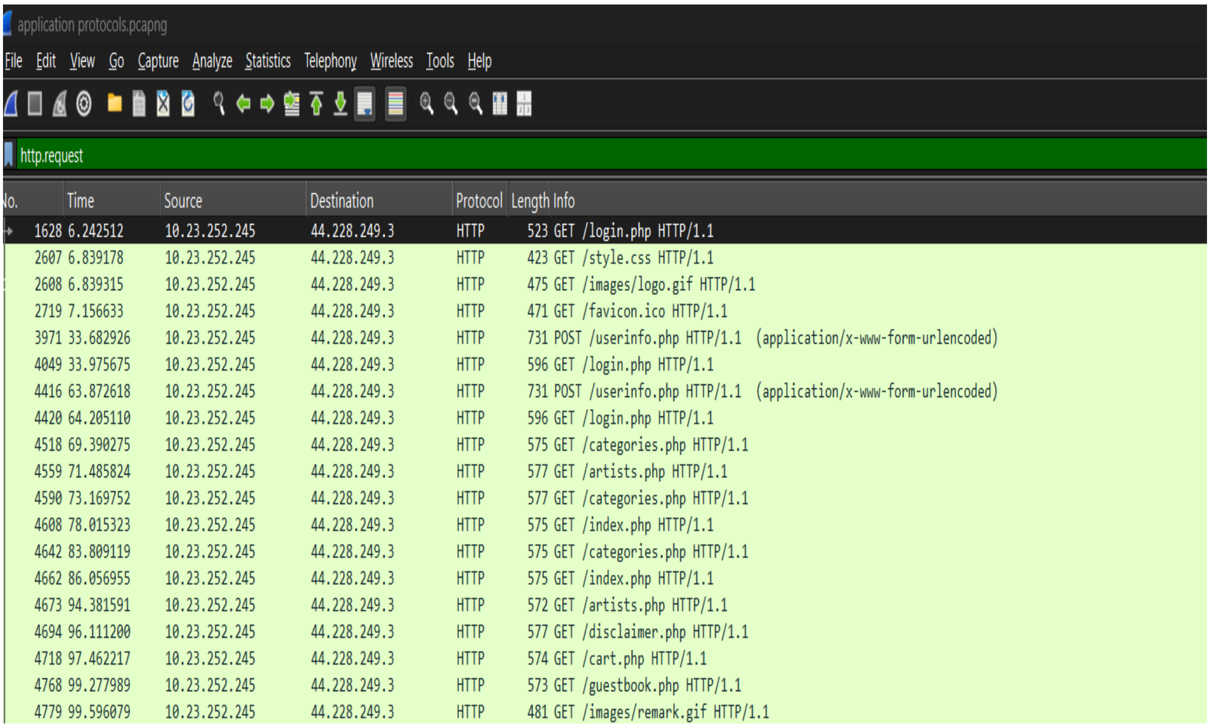
4th:


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

tcp and !(tcp.stream eq 0)

No.	Time	Source	Destination	Protocol	Length	Info
19	1.095561	2401:4900:c903:2e42…	2603:1061:f:100::254	TCP	86	57360 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
23	1.149902	2603:1061:f:100::254	2401:4900:c903:2e42…	TCP	86	443 → 57360 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM
24	1.150007	2401:4900:c903:2e42…	2603:1061:f:100::254	TCP	74	57360 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
25	1.150531	2401:4900:c903:2e42…	2603:1061:f:100::254	TCP	1414	57360 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1340 [TCP PDU reassembled in 26]
26	1.150531	2401:4900:c903:2e42…	2603:1061:f:100::254	TLSv1.3	559	Client Hello (SNI=mcr-ring.msedge.net)
27	1.222637	2603:1061:f:100::254	2401:4900:c903:2e42…	TCP	74	443 → 57360 [ACK] Seq=1 Ack=1341 Win=4195328 Len=0
28	1.222637	2603:1061:f:100::254	2401:4900:c903:2e42…	TCP	74	443 → 57360 [ACK] Seq=1 Ack=1826 Win=4194816 Len=0
29	1.224725	2603:1061:f:100::254	2401:4900:c903:2e42…	TLSv1.3	173	Hello Retry Request, Change Cipher Spec
30	1.225976	2401:4900:c903:2e42…	2603:1061:f:100::254	TLSv1.3	745	Change Cipher Spec, Client Hello (SNI=mcr-ring.msedge.net)
31	1.299351	2603:1061:f:100::254	2401:4900:c903:2e42…	TCP	74	443 → 57360 [ACK] Seq=100 Ack=2497 Win=4194304 Len=0
32	1.300628	2603:1061:f:100::254	2401:4900:c903:2e42…	TLSv1.3	1414	Server Hello
33	1.303389	2603:1061:f:100::254	2401:4900:c903:2e42…	TCP	1414	443 → 57360 [ACK] Seq=1440 Ack=2497 Win=4194304 Len=1340 [TCP PDU reassembled in 36]
34	1.303444	2401:4900:c903:2e42…	2603:1061:f:100::254	TCP	74	57360 → 443 [ACK] Seq=2497 Ack=2780 Win=65280 Len=0
35	1.304553	2603:1061:f:100::254	2401:4900:c903:2e42…	TCP	1414	443 → 57360 [ACK] Seq=2780 Ack=2497 Win=4194304 Len=1340 [TCP PDU reassembled in 36]
36	1.304701	2603:1061:f:100::254	2401:4900:c903:2e42…	TLSv1.3	378	Application Data
37	1.304761	2401:4900:c903:2e42…	2603:1061:f:100::254	TCP	74	57360 → 443 [ACK] Seq=2497 Ack=4424 Win=65280 Len=0
38	1.305985	2401:4900:c903:2e42…	2603:1061:f:100::254	TLSv1.3	148	Application Data
39	1.306127	2401:4900:c903:2e42…	2603:1061:f:100::254	TLSv1.3	166	Application Data
40	1.306260	2401:4900:c903:2e42…	2603:1061:f:100::254	TLSv1.3	685	Application Data

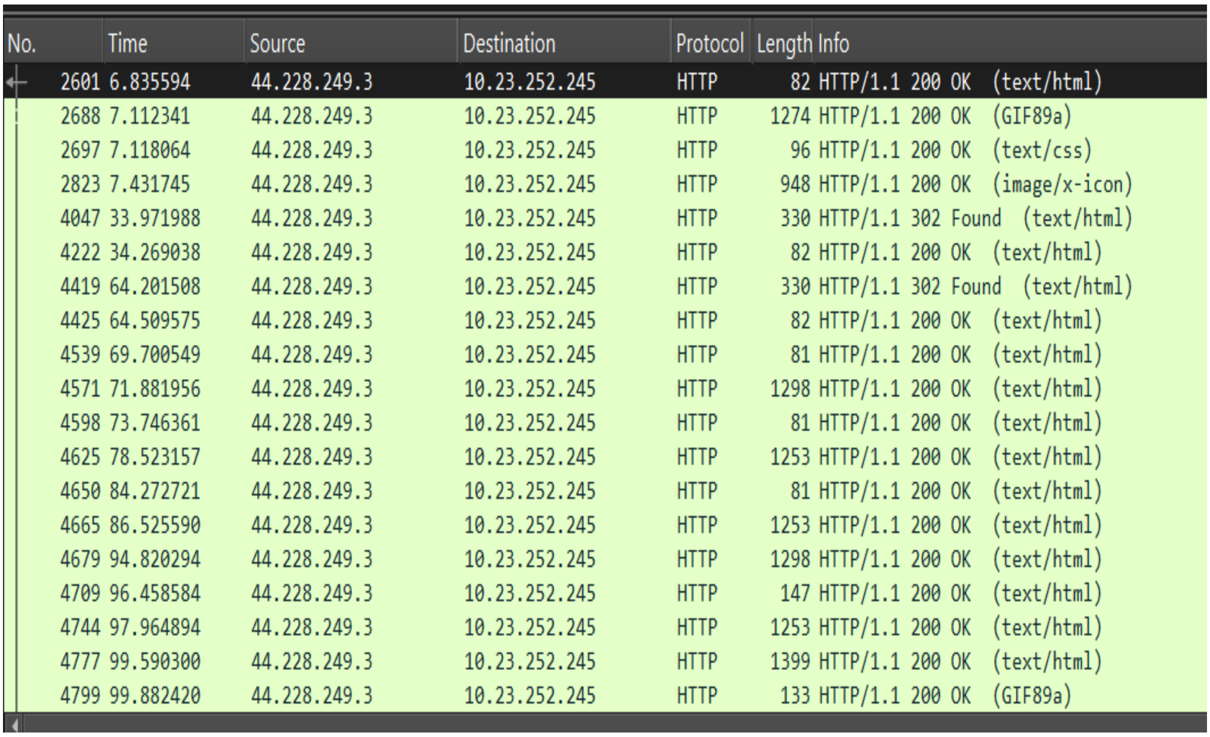
5th:


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

http.request

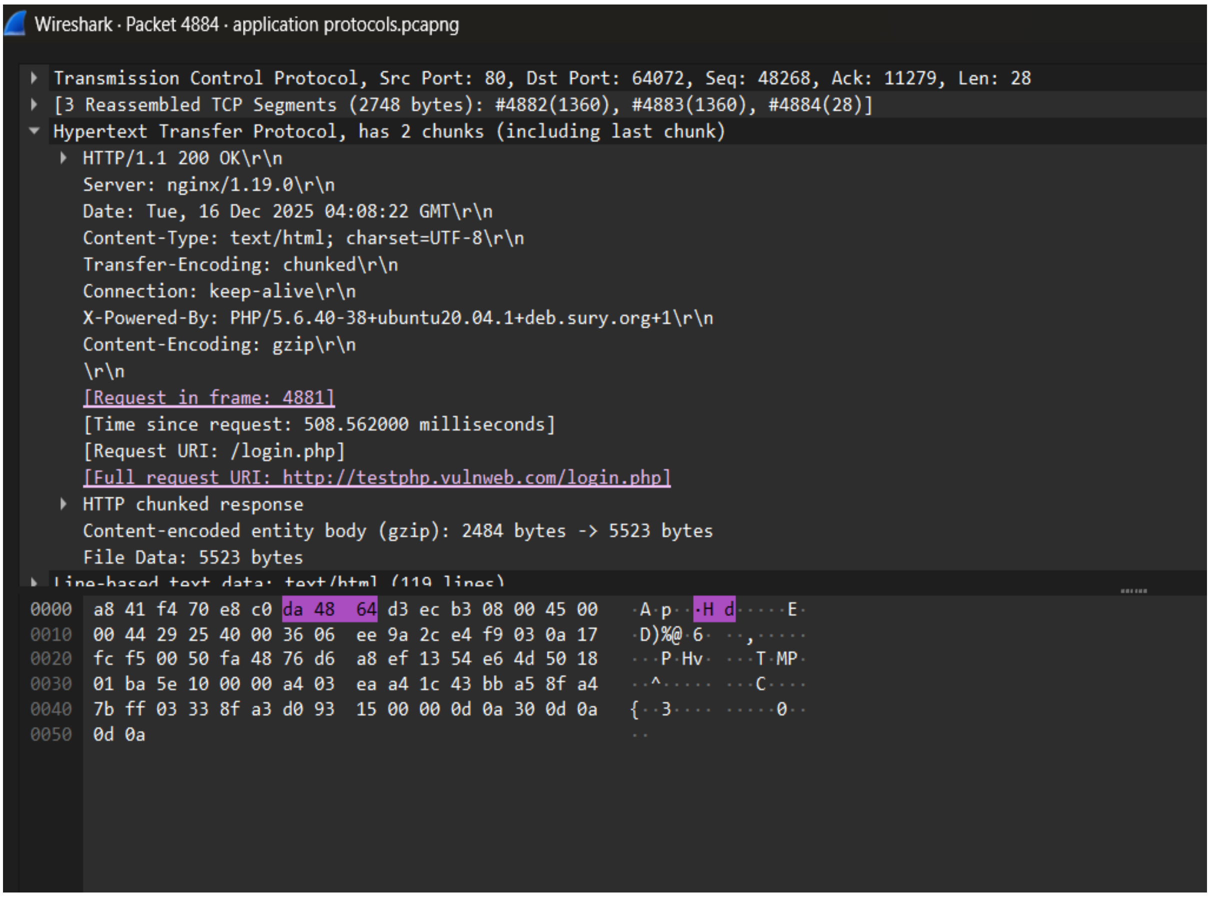
No.	Time	Source	Destination	Protocol	Length	Info
1628	6.242512	10.23.252.245	44.228.249.3	HTTP	523	GET /login.php HTTP/1.1
2607	6.839178	10.23.252.245	44.228.249.3	HTTP	423	GET /style.css HTTP/1.1
2608	6.839315	10.23.252.245	44.228.249.3	HTTP	475	GET /images/logo.gif HTTP/1.1
2719	7.156633	10.23.252.245	44.228.249.3	HTTP	471	GET /favicon.ico HTTP/1.1
3971	33.682926	10.23.252.245	44.228.249.3	HTTP	731	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
4049	33.975675	10.23.252.245	44.228.249.3	HTTP	596	GET /login.php HTTP/1.1
4416	63.872618	10.23.252.245	44.228.249.3	HTTP	731	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
4420	64.205110	10.23.252.245	44.228.249.3	HTTP	596	GET /login.php HTTP/1.1
4518	69.390275	10.23.252.245	44.228.249.3	HTTP	575	GET /categories.php HTTP/1.1
4559	71.485824	10.23.252.245	44.228.249.3	HTTP	577	GET /artists.php HTTP/1.1
4590	73.169752	10.23.252.245	44.228.249.3	HTTP	577	GET /categories.php HTTP/1.1
4608	78.015323	10.23.252.245	44.228.249.3	HTTP	575	GET /index.php HTTP/1.1
4642	83.809119	10.23.252.245	44.228.249.3	HTTP	575	GET /categories.php HTTP/1.1
4662	86.056955	10.23.252.245	44.228.249.3	HTTP	575	GET /index.php HTTP/1.1
4673	94.381591	10.23.252.245	44.228.249.3	HTTP	572	GET /artists.php HTTP/1.1
4694	96.111200	10.23.252.245	44.228.249.3	HTTP	577	GET /disclaimer.php HTTP/1.1
4718	97.462217	10.23.252.245	44.228.249.3	HTTP	574	GET /cart.php HTTP/1.1
4768	99.277989	10.23.252.245	44.228.249.3	HTTP	573	GET /guestbook.php HTTP/1.1
4779	99.596079	10.23.252.245	44.228.249.3	HTTP	481	GET /images/remark.gif HTTP/1.1

6th:



No.	Time	Source	Destination	Protocol	Length	Info
2601	6.835594	44.228.249.3	10.23.252.245	HTTP	82	HTTP/1.1 200 OK (text/html)
2688	7.112341	44.228.249.3	10.23.252.245	HTTP	1274	HTTP/1.1 200 OK (GIF89a)
2697	7.118064	44.228.249.3	10.23.252.245	HTTP	96	HTTP/1.1 200 OK (text/css)
2823	7.431745	44.228.249.3	10.23.252.245	HTTP	948	HTTP/1.1 200 OK (image/x-icon)
4047	33.971988	44.228.249.3	10.23.252.245	HTTP	330	HTTP/1.1 302 Found (text/html)
4222	34.269038	44.228.249.3	10.23.252.245	HTTP	82	HTTP/1.1 200 OK (text/html)
4419	64.201508	44.228.249.3	10.23.252.245	HTTP	330	HTTP/1.1 302 Found (text/html)
4425	64.509575	44.228.249.3	10.23.252.245	HTTP	82	HTTP/1.1 200 OK (text/html)
4539	69.700549	44.228.249.3	10.23.252.245	HTTP	81	HTTP/1.1 200 OK (text/html)
4571	71.881956	44.228.249.3	10.23.252.245	HTTP	1298	HTTP/1.1 200 OK (text/html)
4598	73.746361	44.228.249.3	10.23.252.245	HTTP	81	HTTP/1.1 200 OK (text/html)
4625	78.523157	44.228.249.3	10.23.252.245	HTTP	1253	HTTP/1.1 200 OK (text/html)
4650	84.272721	44.228.249.3	10.23.252.245	HTTP	81	HTTP/1.1 200 OK (text/html)
4665	86.525590	44.228.249.3	10.23.252.245	HTTP	1253	HTTP/1.1 200 OK (text/html)
4679	94.820294	44.228.249.3	10.23.252.245	HTTP	1298	HTTP/1.1 200 OK (text/html)
4709	96.458584	44.228.249.3	10.23.252.245	HTTP	147	HTTP/1.1 200 OK (text/html)
4744	97.964894	44.228.249.3	10.23.252.245	HTTP	1253	HTTP/1.1 200 OK (text/html)
4777	99.590300	44.228.249.3	10.23.252.245	HTTP	1399	HTTP/1.1 200 OK (text/html)
4799	99.882420	44.228.249.3	10.23.252.245	HTTP	133	HTTP/1.1 200 OK (GIF89a)

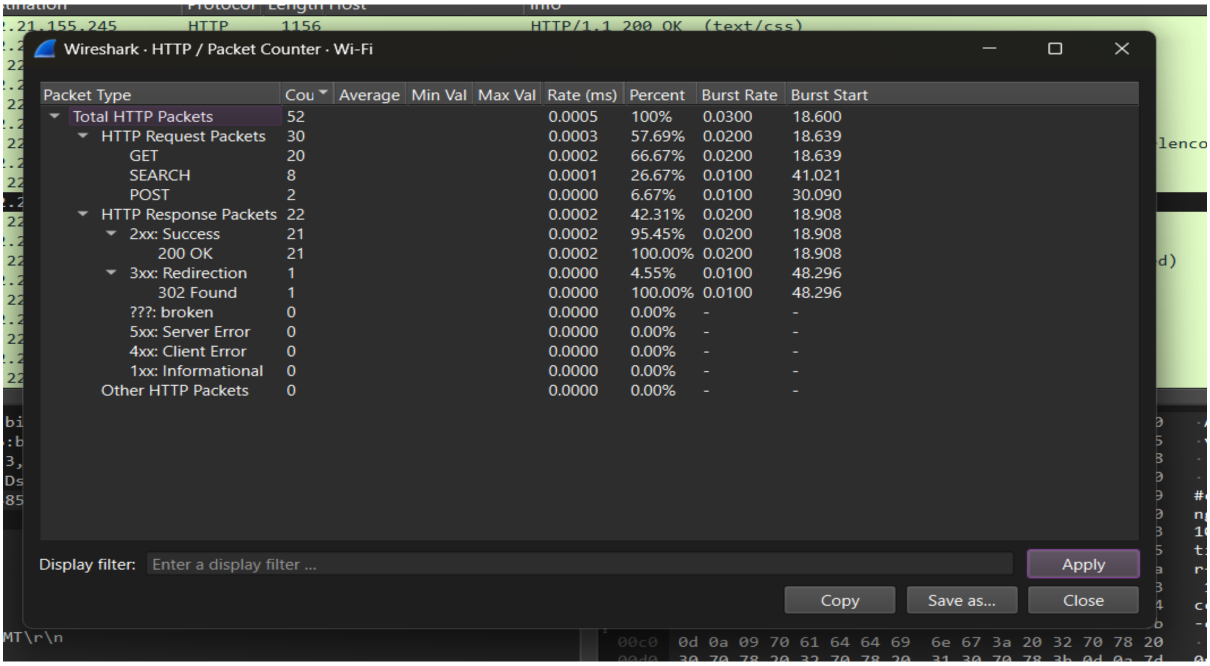
7th:



```
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 64072, Seq: 48268, Ack: 11279, Len: 28
▸ [3 Reassembled TCP Segments (2748 bytes): #4882(1360), #4883(1360), #4884(28)]
▾ 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 04:08:22 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: 4881]
    [Time since request: 508.562000 milliseconds]
    [Request URI: /login.php]
    [Full request URI: http://testphp.vulnweb.com/login.php]
  ▸ HTTP chunked response
    Content-encoded entity body (gzip): 2484 bytes -> 5523 bytes
    File Data: 5523 bytes
▸ Line-based text data: text/html (119 lines)

0000  a8 41 f4 70 e8 c0 da 48  64 d3 ec b3 08 00 45 00   ·A·p··H d·····E·
0010  00 44 29 25 40 00 36 06  ee 9a 2c e4 f9 03 0a 17   ·D)%@·6· ··,·····
0020  fc f5 00 50 fa 48 76 d6  a8 ef 13 54 e6 4d 50 18   ···P·Hv· ···T·MP·
0030  01 ba 5e 10 00 00 a4 03  ea a4 1c 43 bb a5 8f a4   ··^····· ···C····
0040  7b ff 03 33 8f a3 d0 93  15 00 00 0d 0a 30 0d 0a   {··3···· ·····0··
0050  0d 0a                                              ··
```

Task-2

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

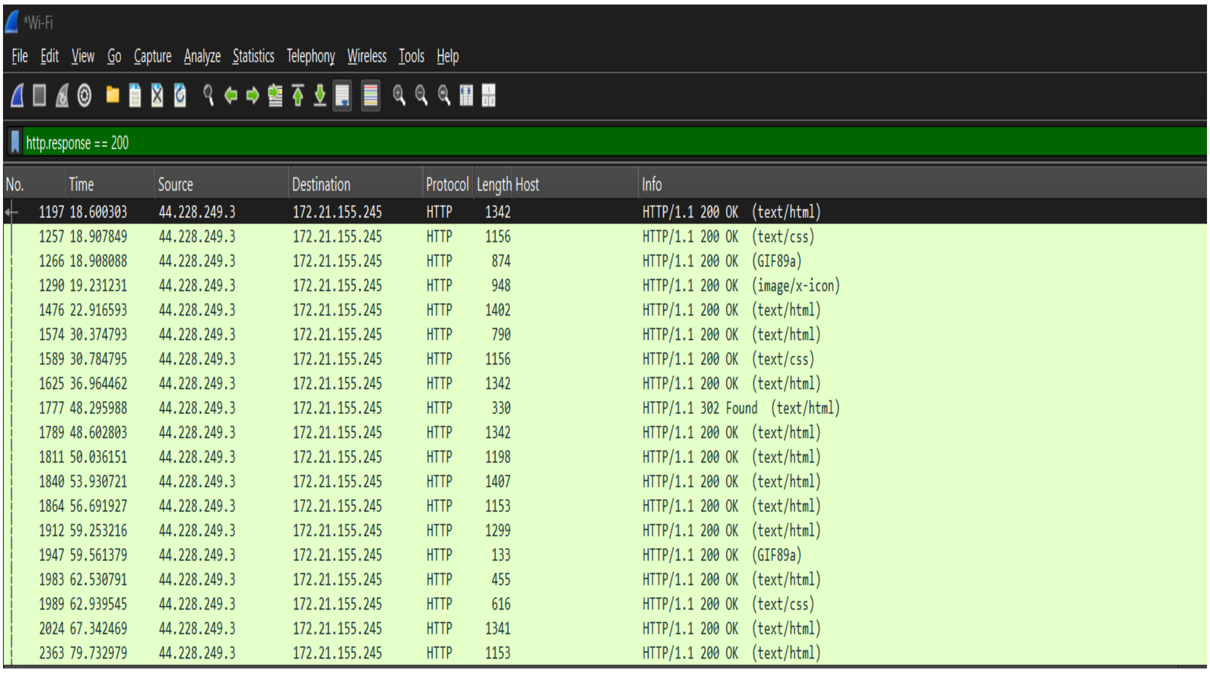


Wireshark · HTTP / Packet Counter · Wi-Fi

Packet Type	Cou	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	52				0.0005	100%	0.0300	18.600
HTTP Request Packets	30				0.0003	57.69%	0.0200	18.639
GET	20				0.0002	66.67%	0.0200	18.639
SEARCH	8				0.0001	26.67%	0.0100	41.021
POST	2				0.0000	6.67%	0.0100	30.090
HTTP Response Packets	22				0.0002	42.31%	0.0200	18.908
2xx: Success	21				0.0002	95.45%	0.0200	18.908
200 OK	21				0.0002	100.00%	0.0200	18.908
3xx: Redirection	1				0.0000	4.55%	0.0100	48.296
302 Found	1				0.0000	100.00%	0.0100	48.296
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	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 ...

Make a list for each of the file/object downloaded, how many times the server sends the full contents of the respective file/object ?

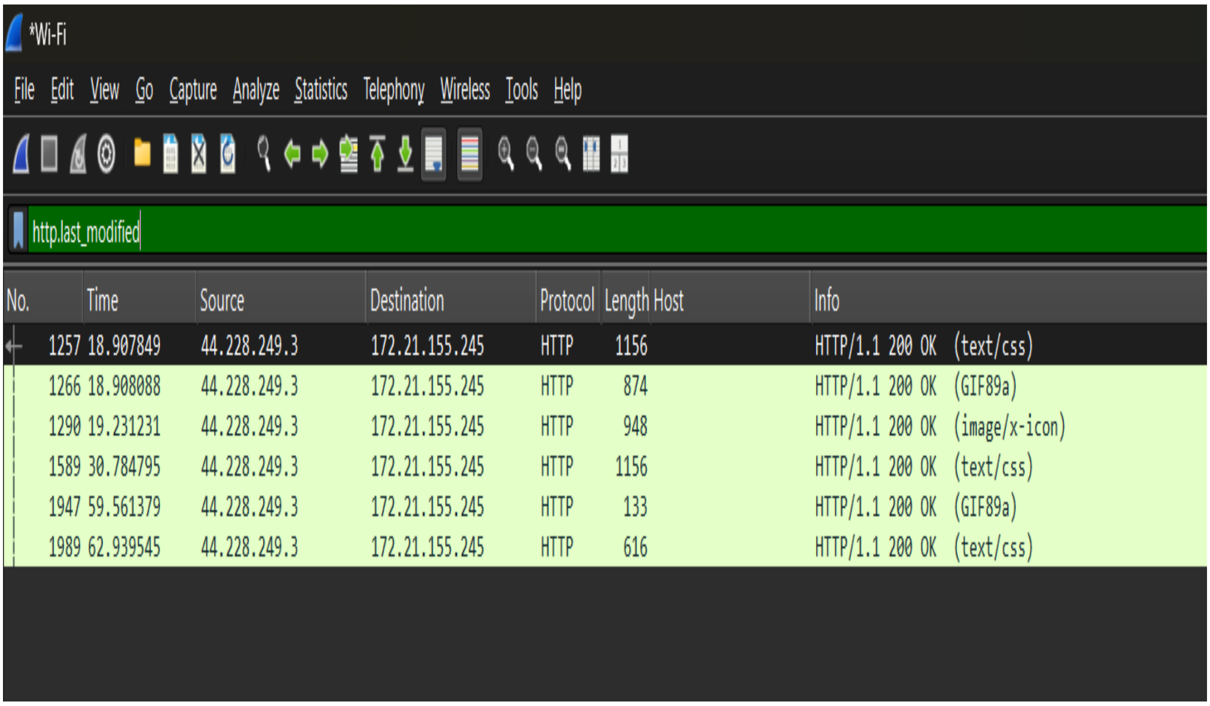


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response == 200

No.	Time	Source	Destination	Protocol	Length	Host	Info
1197	18.600303	44.228.249.3	172.21.155.245	HTTP	1342		HTTP/1.1 200 OK (text/html)
1257	18.907849	44.228.249.3	172.21.155.245	HTTP	1156		HTTP/1.1 200 OK (text/css)
1266	18.908088	44.228.249.3	172.21.155.245	HTTP	874		HTTP/1.1 200 OK (GIF89a)
1290	19.231231	44.228.249.3	172.21.155.245	HTTP	948		HTTP/1.1 200 OK (image/x-icon)
1476	22.916593	44.228.249.3	172.21.155.245	HTTP	1402		HTTP/1.1 200 OK (text/html)
1574	30.374793	44.228.249.3	172.21.155.245	HTTP	790		HTTP/1.1 200 OK (text/html)
1589	30.784795	44.228.249.3	172.21.155.245	HTTP	1156		HTTP/1.1 200 OK (text/css)
1625	36.964462	44.228.249.3	172.21.155.245	HTTP	1342		HTTP/1.1 200 OK (text/html)
1777	48.295988	44.228.249.3	172.21.155.245	HTTP	330		HTTP/1.1 302 Found (text/html)
1789	48.602803	44.228.249.3	172.21.155.245	HTTP	1342		HTTP/1.1 200 OK (text/html)
1811	50.036151	44.228.249.3	172.21.155.245	HTTP	1198		HTTP/1.1 200 OK (text/html)
1840	53.930721	44.228.249.3	172.21.155.245	HTTP	1407		HTTP/1.1 200 OK (text/html)
1864	56.691927	44.228.249.3	172.21.155.245	HTTP	1153		HTTP/1.1 200 OK (text/html)
1912	59.253216	44.228.249.3	172.21.155.245	HTTP	1299		HTTP/1.1 200 OK (text/html)
1947	59.561379	44.228.249.3	172.21.155.245	HTTP	133		HTTP/1.1 200 OK (GIF89a)
1983	62.530791	44.228.249.3	172.21.155.245	HTTP	455		HTTP/1.1 200 OK (text/html)
1989	62.939545	44.228.249.3	172.21.155.245	HTTP	616		HTTP/1.1 200 OK (text/css)
2024	67.342469	44.228.249.3	172.21.155.245	HTTP	1341		HTTP/1.1 200 OK (text/html)
2363	79.732979	44.228.249.3	172.21.155.245	HTTP	1153		HTTP/1.1 200 OK (text/html)

List the headers of HTTP which influence this functionality.



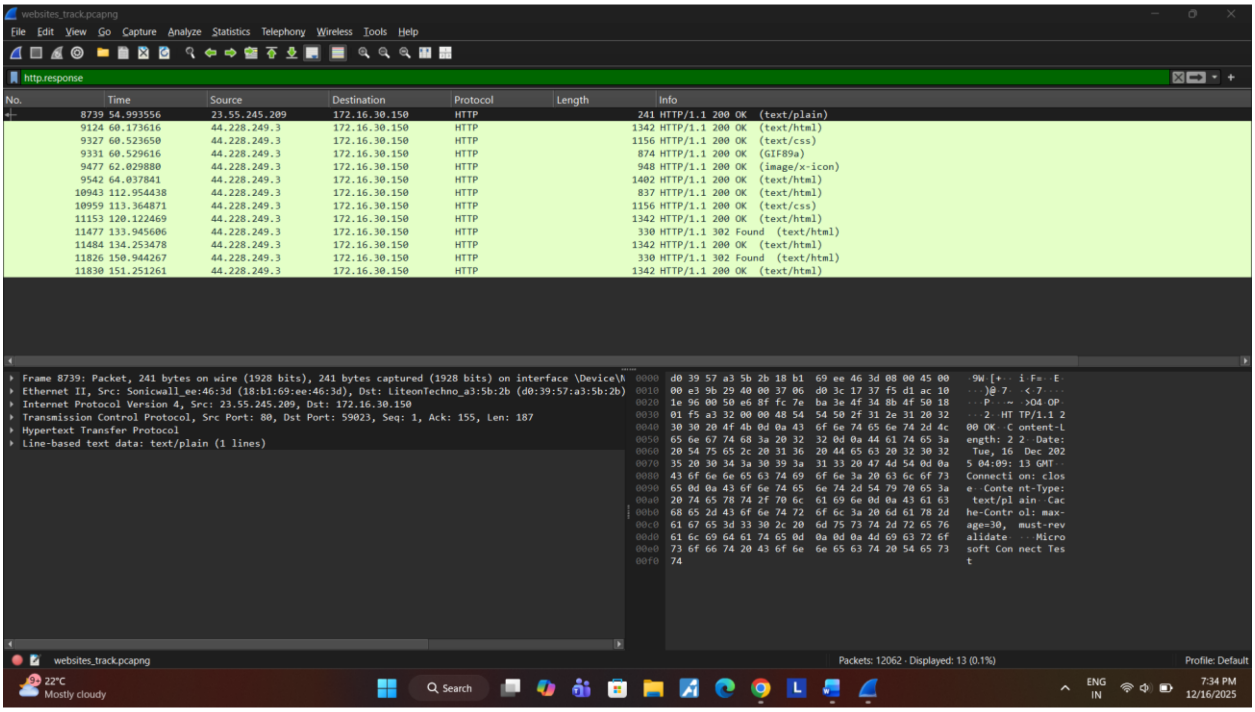
http.last_modified

No.	Time	Source	Destination	Protocol	Length	Host	Info
1257	18.907849	44.228.249.3	172.21.155.245	HTTP	1156		HTTP/1.1 200 OK (text/css)
1266	18.908088	44.228.249.3	172.21.155.245	HTTP	874		HTTP/1.1 200 OK (GIF89a)
1290	19.231231	44.228.249.3	172.21.155.245	HTTP	948		HTTP/1.1 200 OK (image/x-icon)
1589	30.784795	44.228.249.3	172.21.155.245	HTTP	1156		HTTP/1.1 200 OK (text/css)
1947	59.561379	44.228.249.3	172.21.155.245	HTTP	133		HTTP/1.1 200 OK (GIF89a)
1989	62.939545	44.228.249.3	172.21.155.245	HTTP	616		HTTP/1.1 200 OK (text/css)

Task-3

Analyze the attached HTTP/2 packet (http2-h2c.pcap: Included in zip file) capture using Wireshark to answer the following (Hint : Use Statistics->HTTP, HTTP2 windows).

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



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

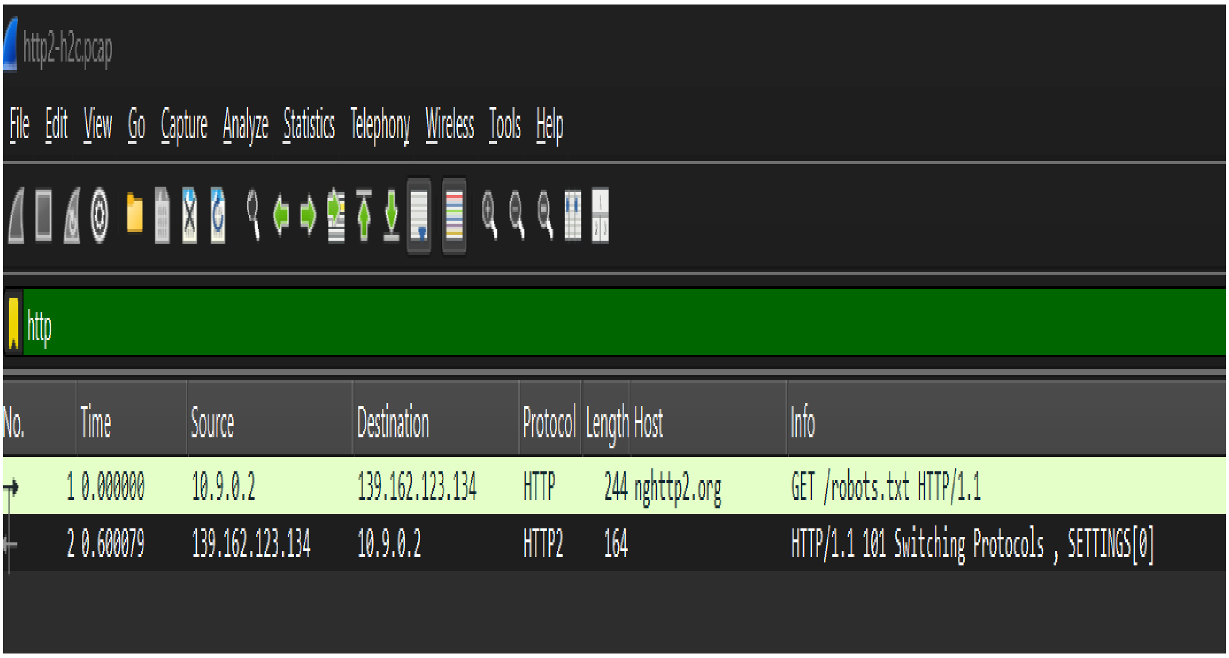
http.response

```
No.         Time          Source           Destination      Protocol   Length   Info
     8739 54.993556     23.55.245.209    172.16.30.150    HTTP         241 HTTP/1.1 200 OK  (text/plain)
     9124 60.173616     44.228.249.3     172.16.30.150    HTTP        1342 HTTP/1.1 200 OK  (text/html)
     9327 60.523650     44.228.249.3     172.16.30.150    HTTP        1156 HTTP/1.1 200 OK  (text/css)
     9331 60.529616     44.228.249.3     172.16.30.150    HTTP         874 HTTP/1.1 200 OK  (GIF89a)
     9477 62.029880     44.228.249.3     172.16.30.150    HTTP         948 HTTP/1.1 200 OK  (image/x-icon)
     9542 64.037841     44.228.249.3     172.16.30.150    HTTP        1402 HTTP/1.1 200 OK  (text/html)
    10943 112.954438    44.228.249.3     172.16.30.150    HTTP         837 HTTP/1.1 200 OK  (text/html)
    10959 113.364871    44.228.249.3     172.16.30.150    HTTP        1156 HTTP/1.1 200 OK  (text/css)
    11153 120.122469    44.228.249.3     172.16.30.150    HTTP        1342 HTTP/1.1 200 OK  (text/html)
    11477 133.945606    44.228.249.3     172.16.30.150    HTTP         330 HTTP/1.1 302 Found  (text/html)
    11484 134.253478    44.228.249.3     172.16.30.150    HTTP        1342 HTTP/1.1 200 OK  (text/html)
    11826 150.944267    44.228.249.3     172.16.30.150    HTTP         330 HTTP/1.1 302 Found  (text/html)
    11830 151.251261    44.228.249.3     172.16.30.150    HTTP        1342 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 8739: Packet, 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\N
› Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: LiteonTechno_a3:5b:2b (d0:39:57:a3:5b:2b)
› Internet Protocol Version 4, Src: 23.55.245.209, Dst: 172.16.30.150
› Transmission Control Protocol, Src Port: 80, Dst Port: 59023, Seq: 1, Ack: 155, Len: 187
› Hypertext Transfer Protocol
› Line-based text data: text/plain (1 lines)
```

```
0000  d0 39 57 a3 5b 2b 18 b1  69 ee 46 3d 08 00 45 00   ·9W·[+·· i·F=··E·
0010  00 e3 9b 29 40 00 37 06  d0 3c 17 37 f5 d1 ac 10   ···)@·7· ·<·7····
0020  1e 96 00 50 e6 8f fc 7e  ba 3e 4f 34 8b 4f 50 18   ···P···~ ·>O4·OP·
0030  01 f5 a3 32 00 00 48 54  54 50 2f 31 2e 31 20 32   ···2··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK··C ontent-L
0050  65 6e 67 74 68 3a 20 32  32 0d 0a 44 61 74 65 3a   ength: 2 2··Date:
0060  20 54 75 65 2c 20 31 36  20 44 65 63 20 32 30 32    Tue, 16  Dec 202
0070  35 20 30 34 3a 30 39 3a  31 33 20 47 4d 54 0d 0a   5 04:09: 13 GMT··
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 63 6c 6f 73   Connecti on: clos
0090  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
00a0  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 43 61 63    text/pl ain··Cac
00b0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78 2d   he-Contr ol: max-
00c0  61 67 65 3d 33 30 2c 20  6d 75 73 74 2d 72 65 76   age=30,  must-rev
00d0  61 6c 69 64 61 74 65 0d  0a 0d 0a 4d 69 63 72 6f   alidate· ···Micro
00e0  73 6f 66 74 20 43 6f 6e  6e 65 63 74 20 54 65 73   soft Con nect Tes
00f0  74                                                 t
```

Packets: 12062 · Displayed: 13 (0.1%)

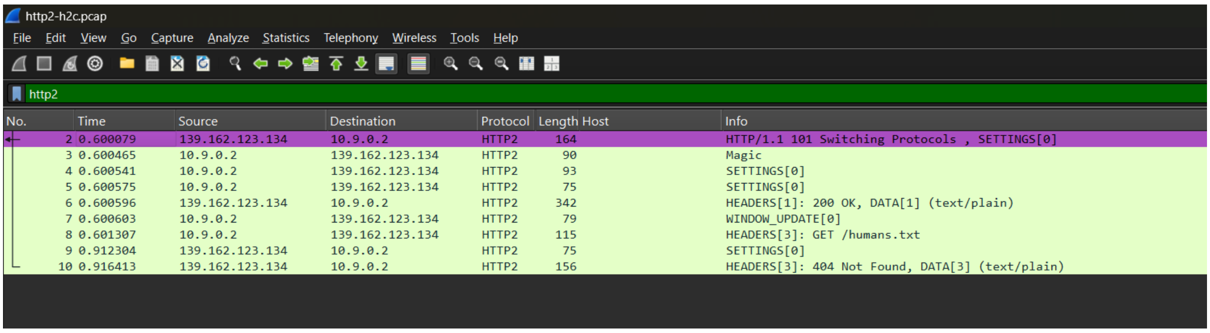


http2-h2c.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

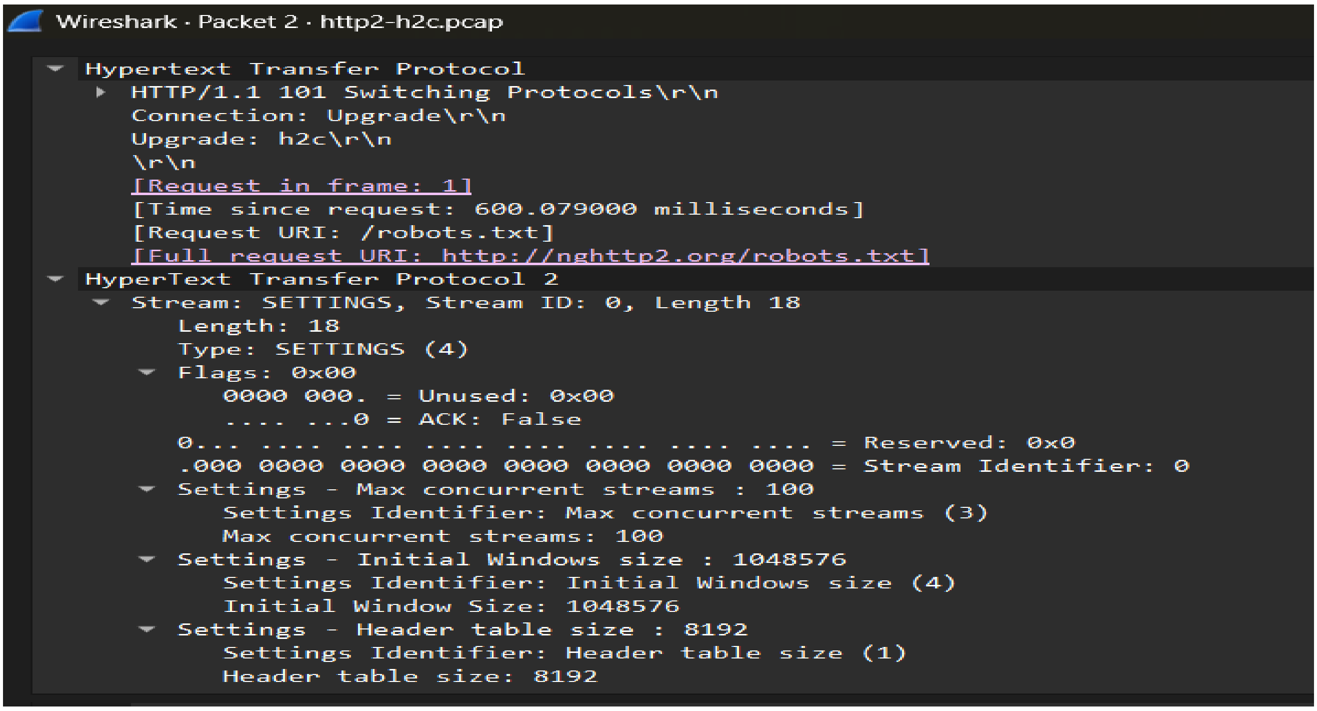
```
No.  Time       Source            Destination       Protocol  Length  Host          Info
  1  0.000000   10.9.0.2          139.162.123.134   HTTP      244     nghttp2.org   GET /robots.txt HTTP/1.1
  2  0.600079   139.162.123.134   10.9.0.2          HTTP2     164                   HTTP/1.1 101 Switching Protocols , SETTINGS[0]
```

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


http2-h2c.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http2

```
No.    Time      Source           Destination      Protocol Length Host  Info
     2 0.600079  139.162.123.134  10.9.0.2         HTTP2    164          HTTP/1.1 101 Switching Protocols , SETTINGS[0]
     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] (text/plain)
     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, DATA[3] (text/plain)
```

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



```
Hypertext Transfer Protocol
  HTTP/1.1 101 Switching Protocols\r\n
  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 Identifier: Initial Windows size (4)
      Initial Window Size: 1048576
    Settings - Header table size : 8192
      Settings Identifier: Header table size (1)
      Header table size: 8192
```