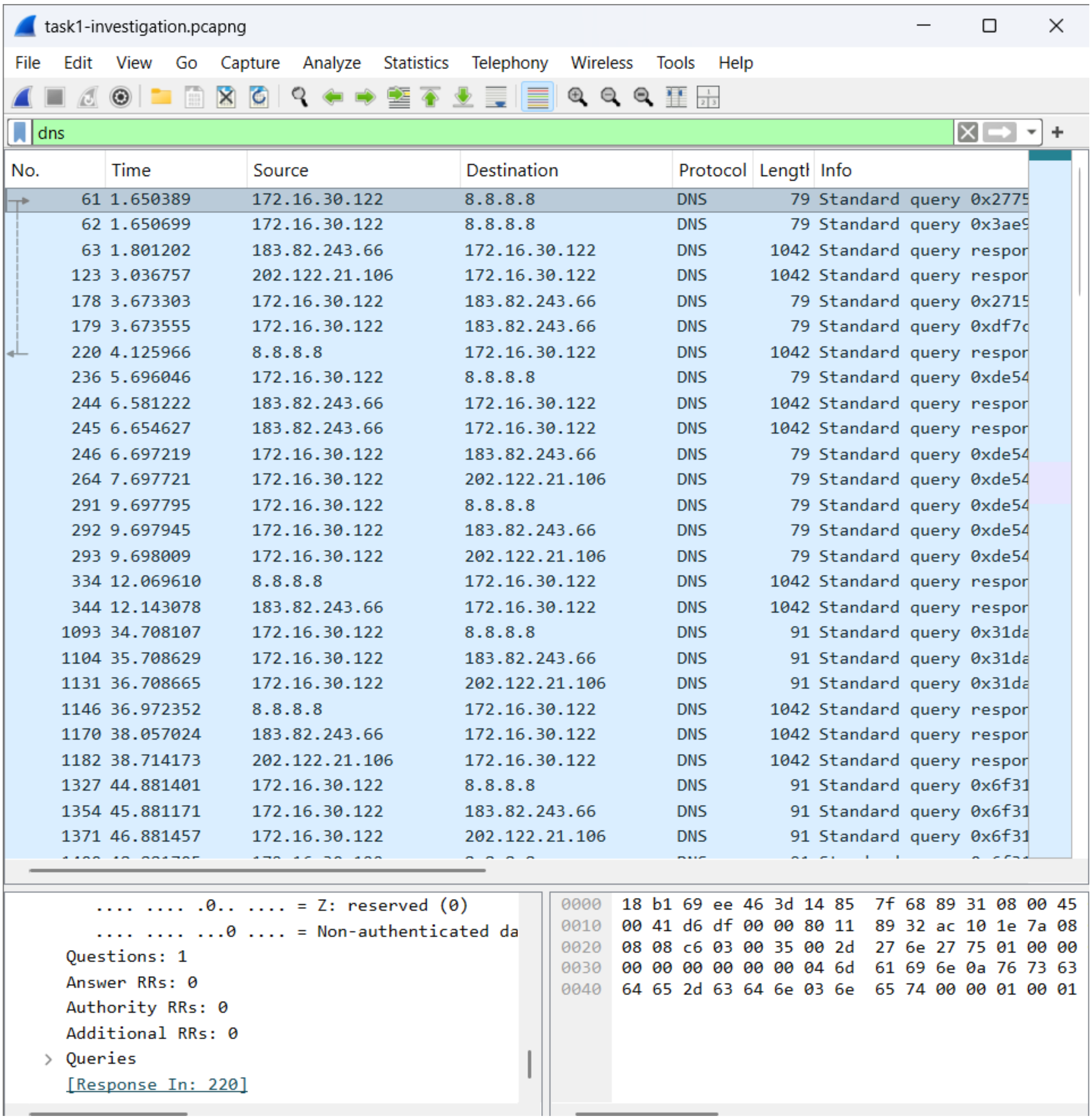
TASK – 1

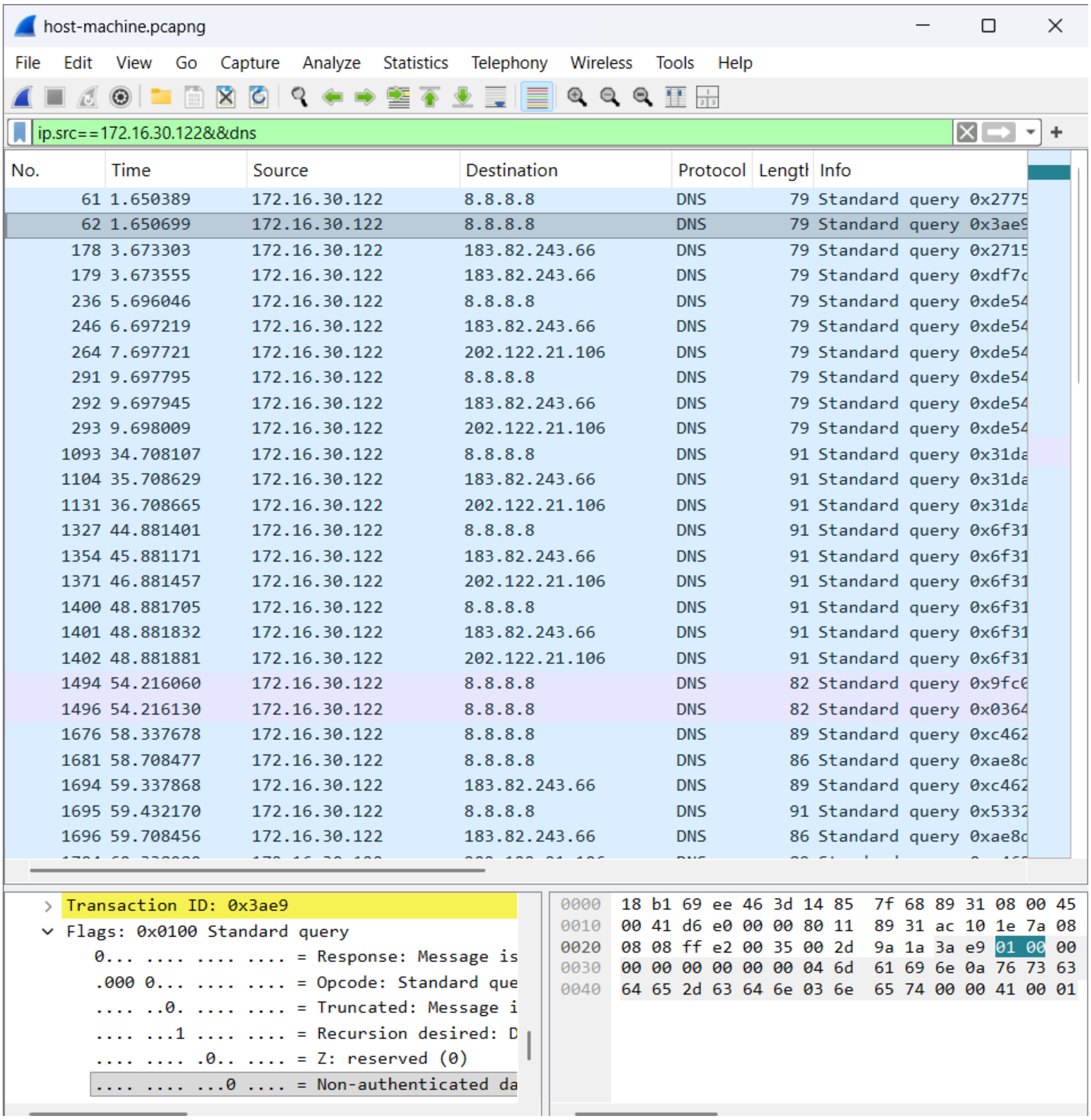


dns

```
No.     Time         Source           Destination      Protocol Lengtl Info
     61 1.650389     172.16.30.122    8.8.8.8          DNS        79 Standard query 0x2775
     62 1.650699     172.16.30.122    8.8.8.8          DNS        79 Standard query 0x3ae9
     63 1.801202     183.82.243.66    172.16.30.122    DNS      1042 Standard query respor
    123 3.036757     202.122.21.106   172.16.30.122    DNS      1042 Standard query respor
    178 3.673303     172.16.30.122    183.82.243.66    DNS        79 Standard query 0x2715
    179 3.673555     172.16.30.122    183.82.243.66    DNS        79 Standard query 0xdf7c
    220 4.125966     8.8.8.8          172.16.30.122    DNS      1042 Standard query respor
    236 5.696046     172.16.30.122    8.8.8.8          DNS        79 Standard query 0xde54
    244 6.581222     183.82.243.66    172.16.30.122    DNS      1042 Standard query respor
    245 6.654627     183.82.243.66    172.16.30.122    DNS      1042 Standard query respor
    246 6.697219     172.16.30.122    183.82.243.66    DNS        79 Standard query 0xde54
    264 7.697721     172.16.30.122    202.122.21.106   DNS        79 Standard query 0xde54
    291 9.697795     172.16.30.122    8.8.8.8          DNS        79 Standard query 0xde54
    292 9.697945     172.16.30.122    183.82.243.66    DNS        79 Standard query 0xde54
    293 9.698009     172.16.30.122    202.122.21.106   DNS        79 Standard query 0xde54
    334 12.069610    8.8.8.8          172.16.30.122    DNS      1042 Standard query respor
    344 12.143078    183.82.243.66    172.16.30.122    DNS      1042 Standard query respor
   1093 34.708107    172.16.30.122    8.8.8.8          DNS        91 Standard query 0x31da
   1104 35.708629    172.16.30.122    183.82.243.66    DNS        91 Standard query 0x31da
   1131 36.708665    172.16.30.122    202.122.21.106   DNS        91 Standard query 0x31da
   1146 36.972352    8.8.8.8          172.16.30.122    DNS      1042 Standard query respor
   1170 38.057024    183.82.243.66    172.16.30.122    DNS      1042 Standard query respor
   1182 38.714173    202.122.21.106   172.16.30.122    DNS      1042 Standard query respor
   1327 44.881401    172.16.30.122    8.8.8.8          DNS        91 Standard query 0x6f31
   1354 45.881171    172.16.30.122    183.82.243.66    DNS        91 Standard query 0x6f31
   1371 46.881457    172.16.30.122    202.122.21.106   DNS        91 Standard query 0x6f31
```

```
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated da
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 220]
```

```
0000  18 b1 69 ee 46 3d 14 85  7f 68 89 31 08 00 45
0010  00 41 d6 df 00 00 80 11  89 32 ac 10 1e 7a 08
0020  08 08 c6 03 00 35 00 2d  27 6e 27 75 01 00 00
0030  00 00 00 00 00 00 04 6d  61 69 6e 0a 76 73 63
0040  64 65 2d 63 64 6e 03 6e  65 74 00 00 01 00 01
```

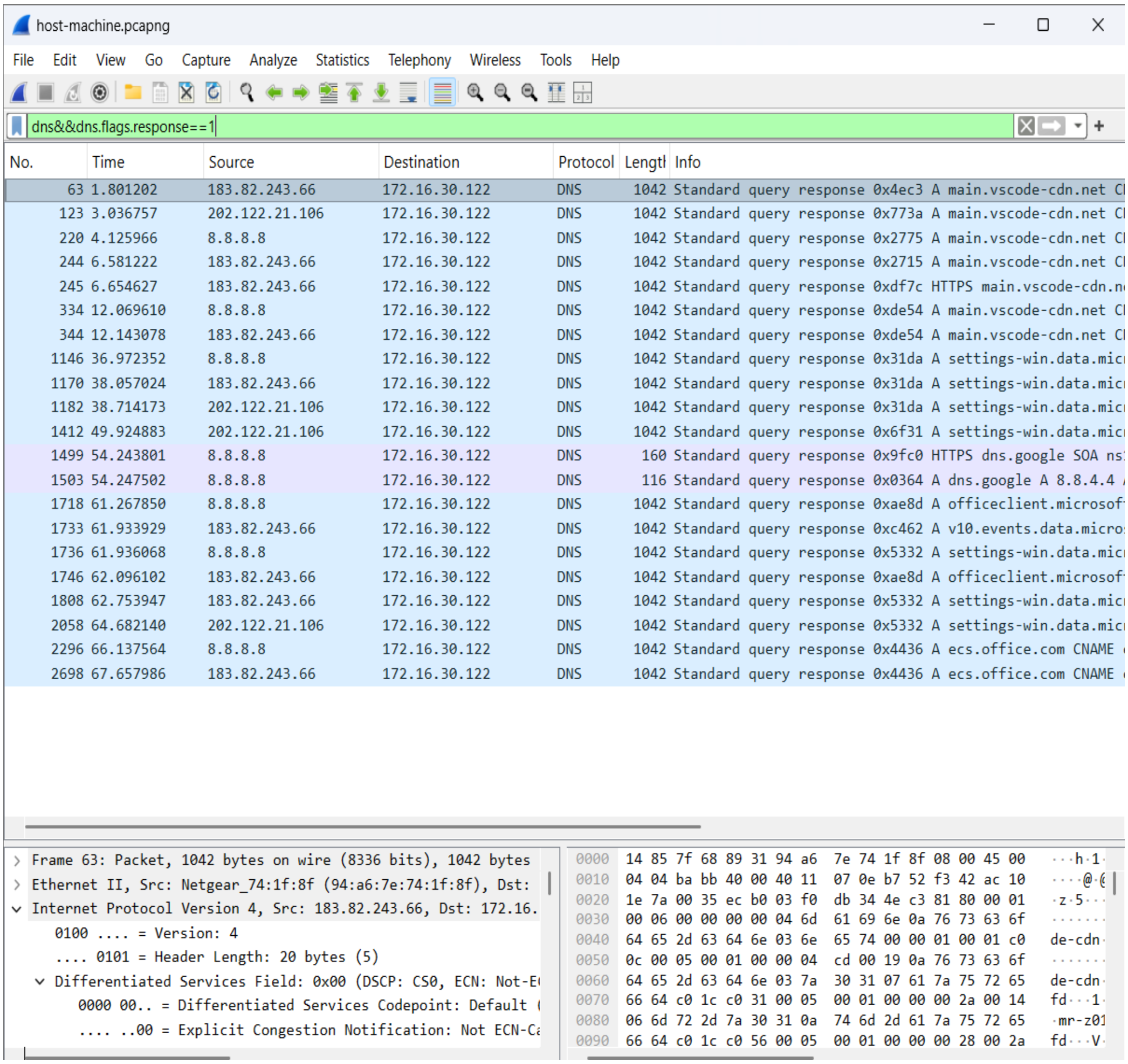


ip.src==172.16.30.122&&dns

No.	Time	Source	Destination	Protocol	Length	Info
61	1.650389	172.16.30.122	8.8.8.8	DNS	79	Standard query 0x2775
62	1.650699	172.16.30.122	8.8.8.8	DNS	79	Standard query 0x3ae9
178	3.673303	172.16.30.122	183.82.243.66	DNS	79	Standard query 0x2715
179	3.673555	172.16.30.122	183.82.243.66	DNS	79	Standard query 0xdf7c
236	5.696046	172.16.30.122	8.8.8.8	DNS	79	Standard query 0xde54
246	6.697219	172.16.30.122	183.82.243.66	DNS	79	Standard query 0xde54
264	7.697721	172.16.30.122	202.122.21.106	DNS	79	Standard query 0xde54
291	9.697795	172.16.30.122	8.8.8.8	DNS	79	Standard query 0xde54
292	9.697945	172.16.30.122	183.82.243.66	DNS	79	Standard query 0xde54
293	9.698009	172.16.30.122	202.122.21.106	DNS	79	Standard query 0xde54
1093	34.708107	172.16.30.122	8.8.8.8	DNS	91	Standard query 0x31da
1104	35.708629	172.16.30.122	183.82.243.66	DNS	91	Standard query 0x31da
1131	36.708665	172.16.30.122	202.122.21.106	DNS	91	Standard query 0x31da
1327	44.881401	172.16.30.122	8.8.8.8	DNS	91	Standard query 0x6f31
1354	45.881171	172.16.30.122	183.82.243.66	DNS	91	Standard query 0x6f31
1371	46.881457	172.16.30.122	202.122.21.106	DNS	91	Standard query 0x6f31
1400	48.881705	172.16.30.122	8.8.8.8	DNS	91	Standard query 0x6f31
1401	48.881832	172.16.30.122	183.82.243.66	DNS	91	Standard query 0x6f31
1402	48.881881	172.16.30.122	202.122.21.106	DNS	91	Standard query 0x6f31
1494	54.216060	172.16.30.122	8.8.8.8	DNS	82	Standard query 0x9fc6
1496	54.216130	172.16.30.122	8.8.8.8	DNS	82	Standard query 0x0364
1676	58.337678	172.16.30.122	8.8.8.8	DNS	89	Standard query 0xc462
1681	58.708477	172.16.30.122	8.8.8.8	DNS	86	Standard query 0xae8c
1694	59.337868	172.16.30.122	183.82.243.66	DNS	89	Standard query 0xc462
1695	59.432170	172.16.30.122	8.8.8.8	DNS	91	Standard query 0x5332
1696	59.708456	172.16.30.122	183.82.243.66	DNS	86	Standard query 0xae8c

```
> Transaction ID: 0x3ae9
v Flags: 0x0100 Standard query
    0... .... .... .... = Response: Message is
    .000 0... .... .... = Opcode: Standard que
    .... ..0. .... .... = Truncated: Message i
    .... ...1 .... .... = Recursion desired: D
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated da
```

```
0000  18 b1 69 ee 46 3d 14 85  7f 68 89 31 08 00 45
0010  00 41 d6 e0 00 00 80 11  89 31 ac 10 1e 7a 08
0020  08 08 ff e2 00 35 00 2d  9a 1a 3a e9 01 00 00
0030  00 00 00 00 00 00 04 6d  61 69 6e 0a 76 73 63
0040  64 65 2d 63 64 6e 03 6e  65 74 00 00 41 00 01
```

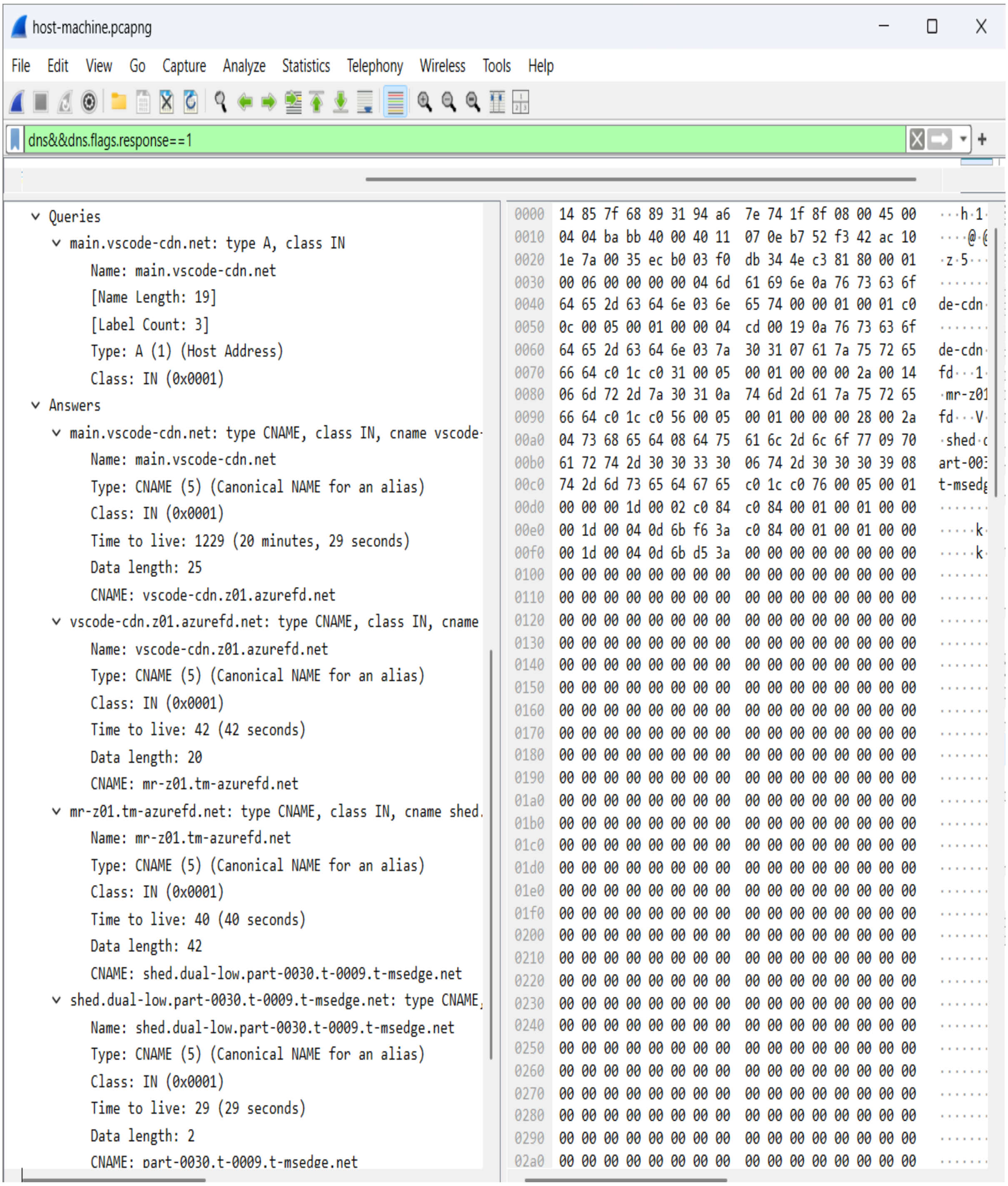


dns&&dns.flags.response==1

No.	Time	Source	Destination	Protocol	Lengtl	Info
63	1.801202	183.82.243.66	172.16.30.122	DNS	1042	Standard query response 0x4ec3 A main.vscode-cdn.net C
123	3.036757	202.122.21.106	172.16.30.122	DNS	1042	Standard query response 0x773a A main.vscode-cdn.net C
220	4.125966	8.8.8.8	172.16.30.122	DNS	1042	Standard query response 0x2775 A main.vscode-cdn.net C
244	6.581222	183.82.243.66	172.16.30.122	DNS	1042	Standard query response 0x2715 A main.vscode-cdn.net C
245	6.654627	183.82.243.66	172.16.30.122	DNS	1042	Standard query response 0xdf7c HTTPS main.vscode-cdn.n
334	12.069610	8.8.8.8	172.16.30.122	DNS	1042	Standard query response 0xde54 A main.vscode-cdn.net C
344	12.143078	183.82.243.66	172.16.30.122	DNS	1042	Standard query response 0xde54 A main.vscode-cdn.net C
1146	36.972352	8.8.8.8	172.16.30.122	DNS	1042	Standard query response 0x31da A settings-win.data.mic
1170	38.057024	183.82.243.66	172.16.30.122	DNS	1042	Standard query response 0x31da A settings-win.data.mic
1182	38.714173	202.122.21.106	172.16.30.122	DNS	1042	Standard query response 0x31da A settings-win.data.mic
1412	49.924883	202.122.21.106	172.16.30.122	DNS	1042	Standard query response 0x6f31 A settings-win.data.mic
1499	54.243801	8.8.8.8	172.16.30.122	DNS	160	Standard query response 0x9fc0 HTTPS dns.google SOA ns
1503	54.247502	8.8.8.8	172.16.30.122	DNS	116	Standard query response 0x0364 A dns.google A 8.8.4.4
1718	61.267850	8.8.8.8	172.16.30.122	DNS	1042	Standard query response 0xae8d A officeclient.microsof
1733	61.933929	183.82.243.66	172.16.30.122	DNS	1042	Standard query response 0xc462 A v10.events.data.micro
1736	61.936068	8.8.8.8	172.16.30.122	DNS	1042	Standard query response 0x5332 A settings-win.data.mic
1746	62.096102	183.82.243.66	172.16.30.122	DNS	1042	Standard query response 0xae8d A officeclient.microsof
1808	62.753947	183.82.243.66	172.16.30.122	DNS	1042	Standard query response 0x5332 A settings-win.data.mic
2058	64.682140	202.122.21.106	172.16.30.122	DNS	1042	Standard query response 0x5332 A settings-win.data.mic
2296	66.137564	8.8.8.8	172.16.30.122	DNS	1042	Standard query response 0x4436 A ecs.office.com CNAME
2698	67.657986	183.82.243.66	172.16.30.122	DNS	1042	Standard query response 0x4436 A ecs.office.com CNAME

```
> Frame 63: Packet, 1042 bytes on wire (8336 bits), 1042 bytes
> Ethernet II, Src: Netgear_74:1f:8f (94:a6:7e:74:1f:8f), Dst:
v Internet Protocol Version 4, Src: 183.82.243.66, Dst: 172.16.
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-E
      0000 00.. = Differentiated Services Codepoint: Default (
      .... ..00 = Explicit Congestion Notification: Not ECN-Ca
```

```
0000  14 85 7f 68 89 31 94 a6  7e 74 1f 8f 08 00 45 00   ···h·1·
0010  04 04 ba bb 40 00 40 11  07 0e b7 52 f3 42 ac 10   ····@·@
0020  1e 7a 00 35 ec b0 03 f0  db 34 4e c3 81 80 00 01   ·z·5···
0030  00 06 00 00 00 00 04 6d  61 69 6e 0a 76 73 63 6f   ·······
0040  64 65 2d 63 64 6e 03 6e  65 74 00 00 01 00 01 c0   de-cdn·
0050  0c 00 05 00 01 00 00 04  cd 00 19 0a 76 73 63 6f   ·······
0060  64 65 2d 63 64 6e 03 7a  30 31 07 61 7a 75 72 65   de-cdn·
0070  66 64 c0 1c c0 31 00 05  00 01 00 00 00 2a 00 14   fd···1·
0080  06 6d 72 2d 7a 30 31 0a  74 6d 2d 61 7a 75 72 65   ·mr-z01
0090  66 64 c0 1c c0 56 00 05  00 01 00 00 00 28 00 2a   fd···V·
```

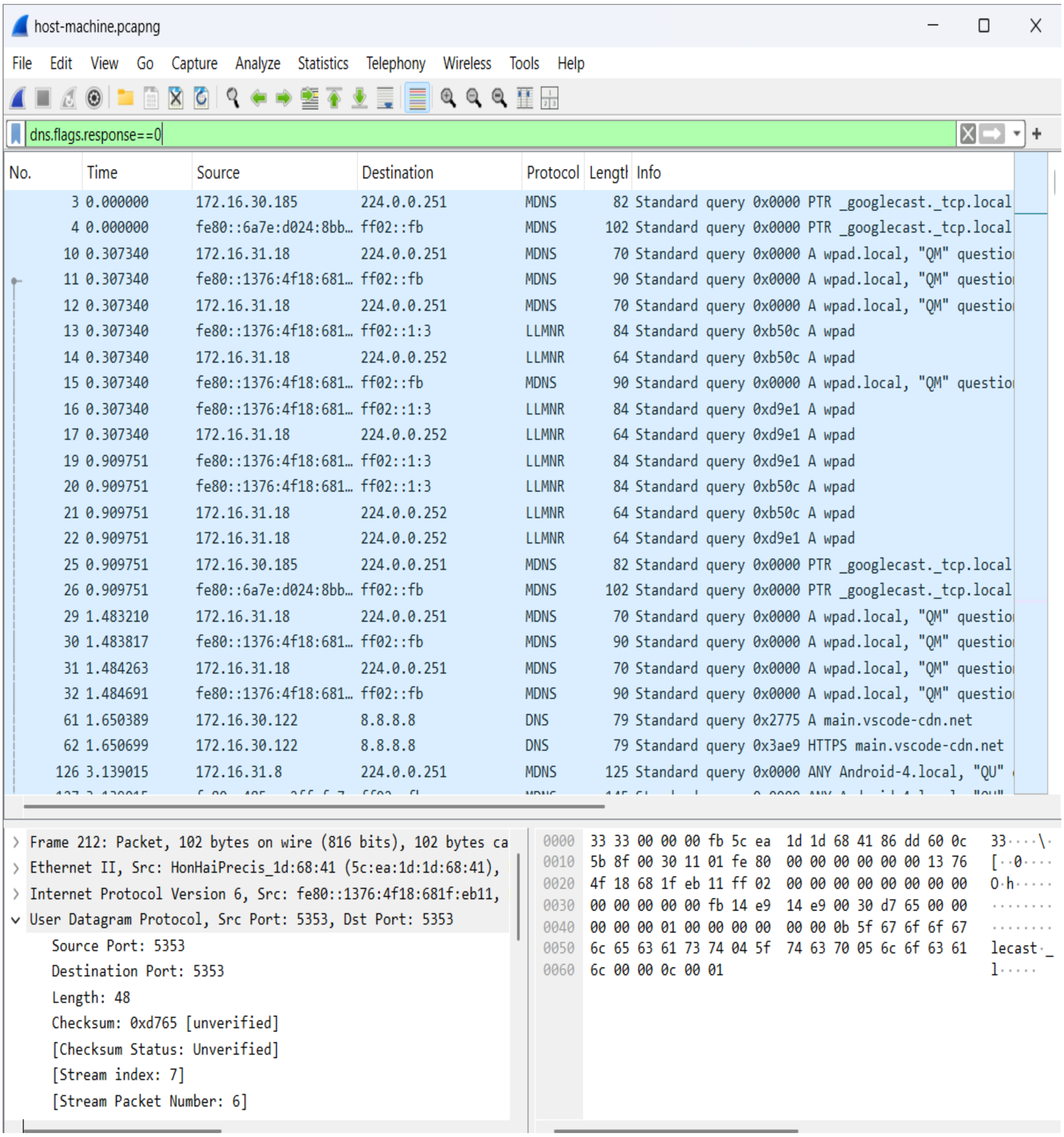


host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns&&dns.flags.response==1

```
  ∨ Queries
    ∨ main.vscode-cdn.net: type A, class IN
        Name: main.vscode-cdn.net
        [Name Length: 19]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ∨ Answers
    ∨ main.vscode-cdn.net: type CNAME, class IN, cname vscode-
        Name: main.vscode-cdn.net
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 1229 (20 minutes, 29 seconds)
        Data length: 25
        CNAME: vscode-cdn.z01.azurefd.net
    ∨ vscode-cdn.z01.azurefd.net: type CNAME, class IN, cname
        Name: vscode-cdn.z01.azurefd.net
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 42 (42 seconds)
        Data length: 20
        CNAME: mr-z01.tm-azurefd.net
    ∨ mr-z01.tm-azurefd.net: type CNAME, class IN, cname shed.
        Name: mr-z01.tm-azurefd.net
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 40 (40 seconds)
        Data length: 42
        CNAME: shed.dual-low.part-0030.t-0009.t-msedge.net
    ∨ shed.dual-low.part-0030.t-0009.t-msedge.net: type CNAME,
        Name: shed.dual-low.part-0030.t-0009.t-msedge.net
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 29 (29 seconds)
        Data length: 2
        CNAME: part-0030.t-0009.t-msedge.net
```

```
0000  14 85 7f 68 89 31 94 a6  7e 74 1f 8f 08 00 45 00   ···h·1·
0010  04 04 ba bb 40 00 40 11  07 0e b7 52 f3 42 ac 10   ····@·@
0020  1e 7a 00 35 ec b0 03 f0  db 34 4e c3 81 80 00 01   ·z·5···
0030  00 06 00 00 00 00 04 6d  61 69 6e 0a 76 73 63 6f   ·······
0040  64 65 2d 63 64 6e 03 6e  65 74 00 00 01 00 01 c0   de-cdn·
0050  0c 00 05 00 01 00 00 04  cd 00 19 0a 76 73 63 6f   ·······
0060  64 65 2d 63 64 6e 03 7a  30 31 07 61 7a 75 72 65   de-cdn·
0070  66 64 c0 1c c0 31 00 05  00 01 00 00 00 2a 00 14   fd···1·
0080  06 6d 72 2d 7a 30 31 0a  74 6d 2d 61 7a 75 72 65   ·mr-z01
0090  66 64 c0 1c c0 56 00 05  00 01 00 00 00 28 00 2a   fd···V·
00a0  04 73 68 65 64 08 64 75  61 6c 2d 6c 6f 77 09 70   ·shed·c
00b0  61 72 74 2d 30 30 33 30  06 74 2d 30 30 30 39 08   art-003
00c0  74 2d 6d 73 65 64 67 65  c0 1c c0 76 00 05 00 01   t-msedg
00d0  00 00 00 1d 00 02 c0 84  c0 84 00 01 00 01 00 00   ·······
00e0  00 1d 00 04 0d 6b f6 3a  c0 84 00 01 00 01 00 00   ·····k·
00f0  00 1d 00 04 0d 6b d5 3a  00 00 00 00 00 00 00 00   ·····k·
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
01a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
01b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
01c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
01d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
01e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
01f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0240  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0250  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0260  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0270  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0280  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
0290  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
02a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······
```

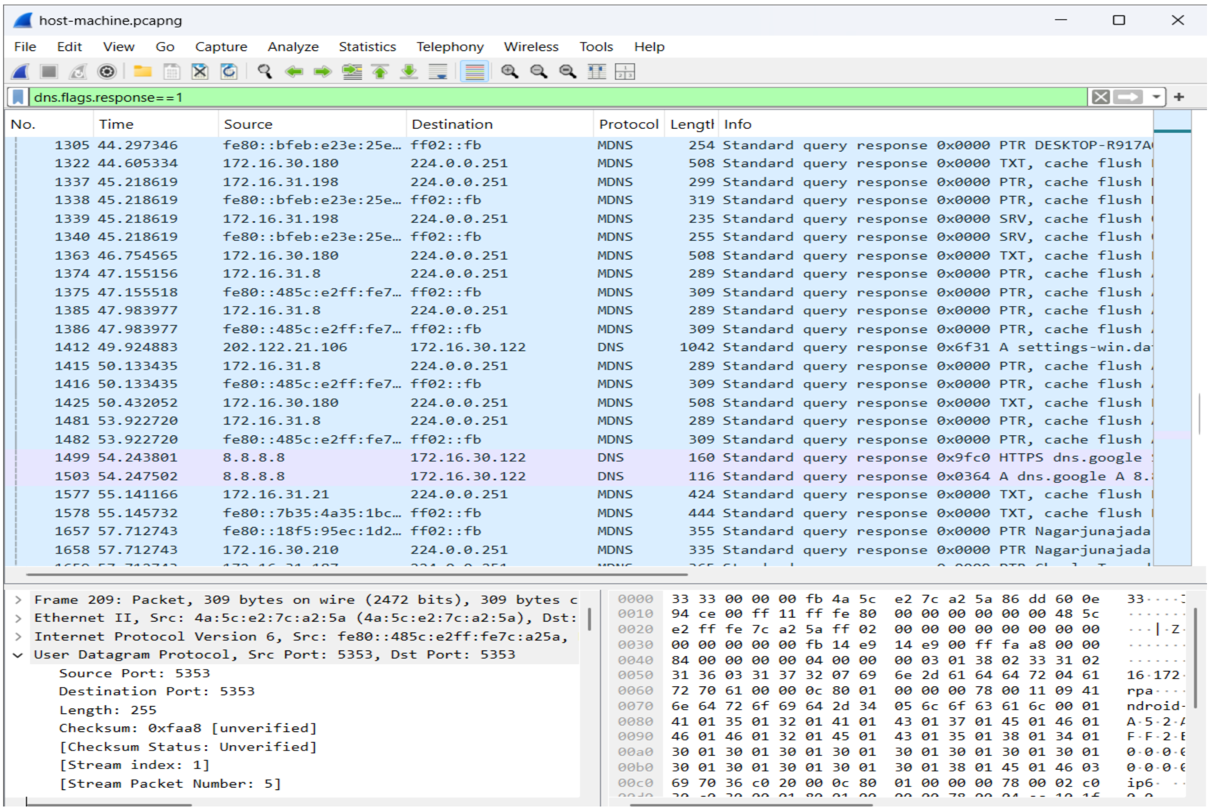

host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.flags.response==0

```
No.   Time     Source                    Destination   Protocol Lengtl Info
    3 0.000000 172.16.30.185             224.0.0.251   MDNS      82 Standard query 0x0000 PTR _googlecast._tcp.local
    4 0.000000 fe80::6a7e:d024:8bb…      ff02::fb      MDNS     102 Standard query 0x0000 PTR _googlecast._tcp.local
   10 0.307340 172.16.31.18              224.0.0.251   MDNS      70 Standard query 0x0000 A wpad.local, "QM" questio
   11 0.307340 fe80::1376:4f18:681…      ff02::fb      MDNS      90 Standard query 0x0000 A wpad.local, "QM" questio
   12 0.307340 172.16.31.18              224.0.0.251   MDNS      70 Standard query 0x0000 A wpad.local, "QM" questio
   13 0.307340 fe80::1376:4f18:681…      ff02::1:3     LLMNR     84 Standard query 0xb50c A wpad
   14 0.307340 172.16.31.18              224.0.0.252   LLMNR     64 Standard query 0xb50c A wpad
   15 0.307340 fe80::1376:4f18:681…      ff02::fb      MDNS      90 Standard query 0x0000 A wpad.local, "QM" questio
   16 0.307340 fe80::1376:4f18:681…      ff02::1:3     LLMNR     84 Standard query 0xd9e1 A wpad
   17 0.307340 172.16.31.18              224.0.0.252   LLMNR     64 Standard query 0xd9e1 A wpad
   19 0.909751 fe80::1376:4f18:681…      ff02::1:3     LLMNR     84 Standard query 0xd9e1 A wpad
   20 0.909751 fe80::1376:4f18:681…      ff02::1:3     LLMNR     84 Standard query 0xb50c A wpad
   21 0.909751 172.16.31.18              224.0.0.252   LLMNR     64 Standard query 0xb50c A wpad
   22 0.909751 172.16.31.18              224.0.0.252   LLMNR     64 Standard query 0xd9e1 A wpad
   25 0.909751 172.16.30.185             224.0.0.251   MDNS      82 Standard query 0x0000 PTR _googlecast._tcp.local
   26 0.909751 fe80::6a7e:d024:8bb…      ff02::fb      MDNS     102 Standard query 0x0000 PTR _googlecast._tcp.local
   29 1.483210 172.16.31.18              224.0.0.251   MDNS      70 Standard query 0x0000 A wpad.local, "QM" questio
   30 1.483817 fe80::1376:4f18:681…      ff02::fb      MDNS      90 Standard query 0x0000 A wpad.local, "QM" questio
   31 1.484263 172.16.31.18              224.0.0.251   MDNS      70 Standard query 0x0000 A wpad.local, "QM" questio
   32 1.484691 fe80::1376:4f18:681…      ff02::fb      MDNS      90 Standard query 0x0000 A wpad.local, "QM" questio
   61 1.650389 172.16.30.122             8.8.8.8       DNS       79 Standard query 0x2775 A main.vscode-cdn.net
   62 1.650699 172.16.30.122             8.8.8.8       DNS       79 Standard query 0x3ae9 HTTPS main.vscode-cdn.net
  126 3.139015 172.16.31.8               224.0.0.251   MDNS     125 Standard query 0x0000 ANY Android-4.local, "QU"
```

```
> Frame 212: Packet, 102 bytes on wire (816 bits), 102 bytes ca
> Ethernet II, Src: HonHaiPrecis_1d:68:41 (5c:ea:1d:1d:68:41),
> Internet Protocol Version 6, Src: fe80::1376:4f18:681f:eb11,
v User Datagram Protocol, Src Port: 5353, Dst Port: 5353
    Source Port: 5353
    Destination Port: 5353
    Length: 48
    Checksum: 0xd765 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
    [Stream Packet Number: 6]
```

```
0000  33 33 00 00 00 fb 5c ea  1d 1d 68 41 86 dd 60 0c   33····\·
0010  5b 8f 00 30 11 01 fe 80  00 00 00 00 00 00 13 76   [··0····
0020  4f 18 68 1f eb 11 ff 02  00 00 00 00 00 00 00 00   O·h·····
0030  00 00 00 00 00 fb 14 e9  14 e9 00 30 d7 65 00 00   ········
0040  00 00 00 01 00 00 00 00  00 00 0b 5f 67 6f 6f 67   ········
0050  6c 65 63 61 73 74 04 5f  74 63 70 05 6c 6f 63 61   lecast·_
0060  6c 00 00 0c 00 01                                  l·····
```



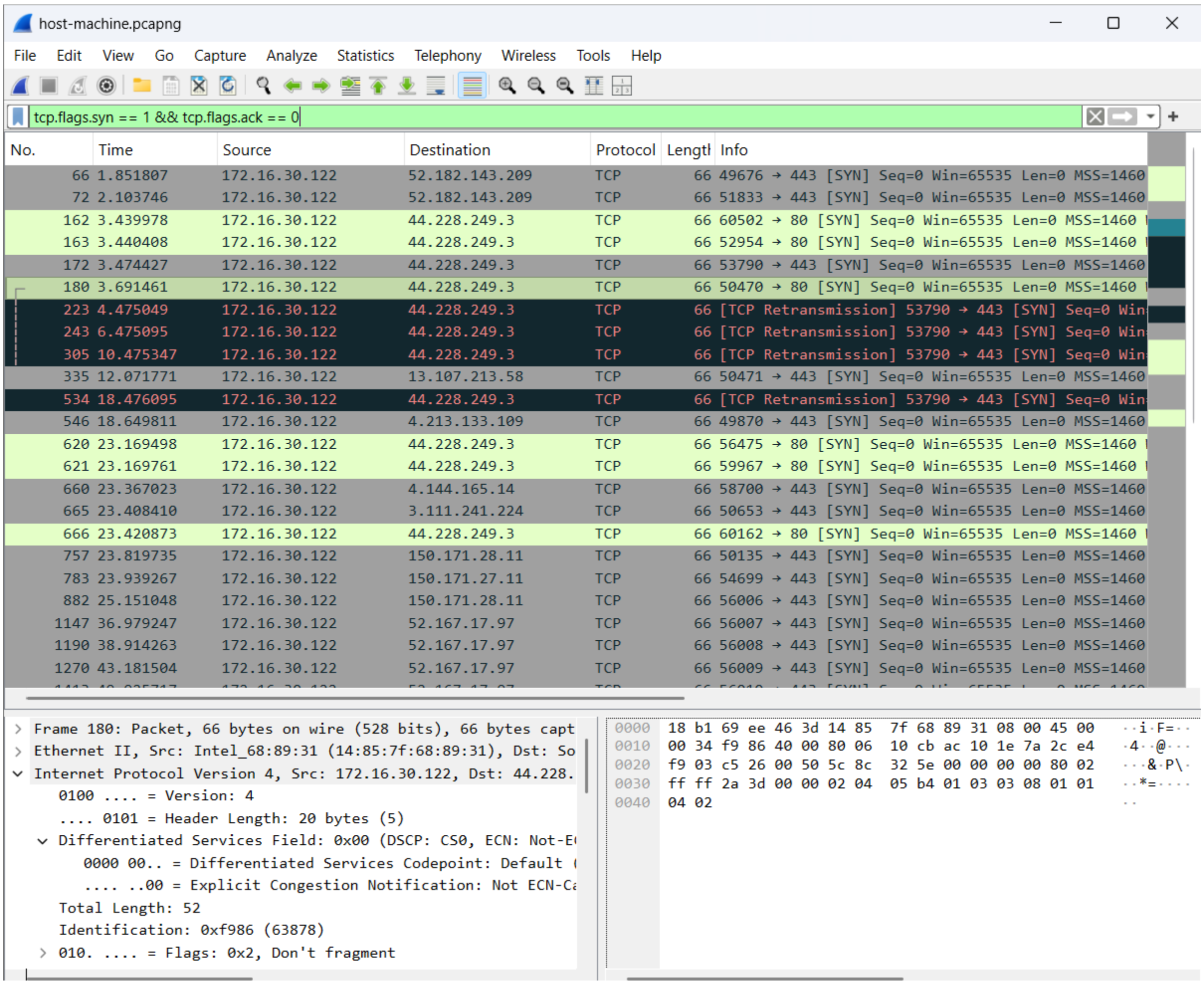
host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.flags.response==1

```
No.     Time       Source                Destination     Protocol Lengtl Info
   1305 44.297346  fe80::bfeb:e23e:25e…  ff02::fb        MDNS     254 Standard query response 0x0000 PTR DESKTOP-R917A
   1322 44.605334  172.16.30.180         224.0.0.251     MDNS     508 Standard query response 0x0000 TXT, cache flush
   1337 45.218619  172.16.31.198         224.0.0.251     MDNS     299 Standard query response 0x0000 PTR, cache flush
   1338 45.218619  fe80::bfeb:e23e:25e…  ff02::fb        MDNS     319 Standard query response 0x0000 PTR, cache flush
   1339 45.218619  172.16.31.198         224.0.0.251     MDNS     235 Standard query response 0x0000 SRV, cache flush
   1340 45.218619  fe80::bfeb:e23e:25e…  ff02::fb        MDNS     255 Standard query response 0x0000 SRV, cache flush
   1363 46.754565  172.16.30.180         224.0.0.251     MDNS     508 Standard query response 0x0000 TXT, cache flush
   1374 47.155156  172.16.31.8           224.0.0.251     MDNS     289 Standard query response 0x0000 PTR, cache flush
   1375 47.155518  fe80::485c:e2ff:fe7…  ff02::fb        MDNS     309 Standard query response 0x0000 PTR, cache flush
   1385 47.983977  172.16.31.8           224.0.0.251     MDNS     289 Standard query response 0x0000 PTR, cache flush
   1386 47.983977  fe80::485c:e2ff:fe7…  ff02::fb        MDNS     309 Standard query response 0x0000 PTR, cache flush
   1412 49.924883  202.122.21.106        172.16.30.122   DNS     1042 Standard query response 0x6f31 A settings-win.da
   1415 50.133435  172.16.31.8           224.0.0.251     MDNS     289 Standard query response 0x0000 PTR, cache flush
   1416 50.133435  fe80::485c:e2ff:fe7…  ff02::fb        MDNS     309 Standard query response 0x0000 PTR, cache flush
   1425 50.432052  172.16.30.180         224.0.0.251     MDNS     508 Standard query response 0x0000 TXT, cache flush
   1481 53.922720  172.16.31.8           224.0.0.251     MDNS     289 Standard query response 0x0000 PTR, cache flush
   1482 53.922720  fe80::485c:e2ff:fe7…  ff02::fb        MDNS     309 Standard query response 0x0000 PTR, cache flush
   1499 54.243801  8.8.8.8               172.16.30.122   DNS      160 Standard query response 0x9fc0 HTTPS dns.google
   1503 54.247502  8.8.8.8               172.16.30.122   DNS      116 Standard query response 0x0364 A dns.google A 8.
   1577 55.141166  172.16.31.21          224.0.0.251     MDNS     424 Standard query response 0x0000 TXT, cache flush
   1578 55.145732  fe80::7b35:4a35:1bc…  ff02::fb        MDNS     444 Standard query response 0x0000 TXT, cache flush
   1657 57.712743  fe80::18f5:95ec:1d2…  ff02::fb        MDNS     355 Standard query response 0x0000 PTR Nagarjunajada
   1658 57.712743  172.16.30.210         224.0.0.251     MDNS     335 Standard query response 0x0000 PTR Nagarjunajada
```

```
> Frame 209: Packet, 309 bytes on wire (2472 bits), 309 bytes c
> Ethernet II, Src: 4a:5c:e2:7c:a2:5a (4a:5c:e2:7c:a2:5a), Dst:
> Internet Protocol Version 6, Src: fe80::485c:e2ff:fe7c:a25a,
v User Datagram Protocol, Src Port: 5353, Dst Port: 5353
    Source Port: 5353
    Destination Port: 5353
    Length: 255
    Checksum: 0xfaa8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    [Stream Packet Number: 5]
```

```
0000  33 33 00 00 00 fb 4a 5c  e2 7c a2 5a 86 dd 60 0e   33····:
0010  94 ce 00 ff 11 ff fe 80  00 00 00 00 00 00 48 5c   ·······
0020  e2 ff fe 7c a2 5a ff 02  00 00 00 00 00 00 00 00   ···|·Z·
0030  00 00 00 00 00 fb 14 e9  14 e9 00 ff fa a8 00 00   ·······
0040  84 00 00 00 00 04 00 00  00 03 01 38 02 33 31 02   ·······
0050  31 36 03 31 37 32 07 69  6e 2d 61 64 64 72 04 61   16·172·
0060  72 70 61 00 00 0c 80 01  00 00 00 78 00 11 09 41   rpa····
0070  6e 64 72 6f 69 64 2d 34  05 6c 6f 63 61 6c 00 01   ndroid-
0080  41 01 35 01 32 01 41 01  43 01 37 01 45 01 46 01   A·5·2·A
0090  46 01 46 01 32 01 45 01  43 01 35 01 38 01 34 01   F·F·2·E
00a0  30 01 30 01 30 01 30 01  30 01 30 01 30 01 30 01   0·0·0·0
00b0  30 01 30 01 30 01 30 01  30 01 38 01 45 01 46 03   0·0·0·0
00c0  69 70 36 c0 20 00 0c 80  01 00 00 00 78 00 02 c0   ip6·  ·
```



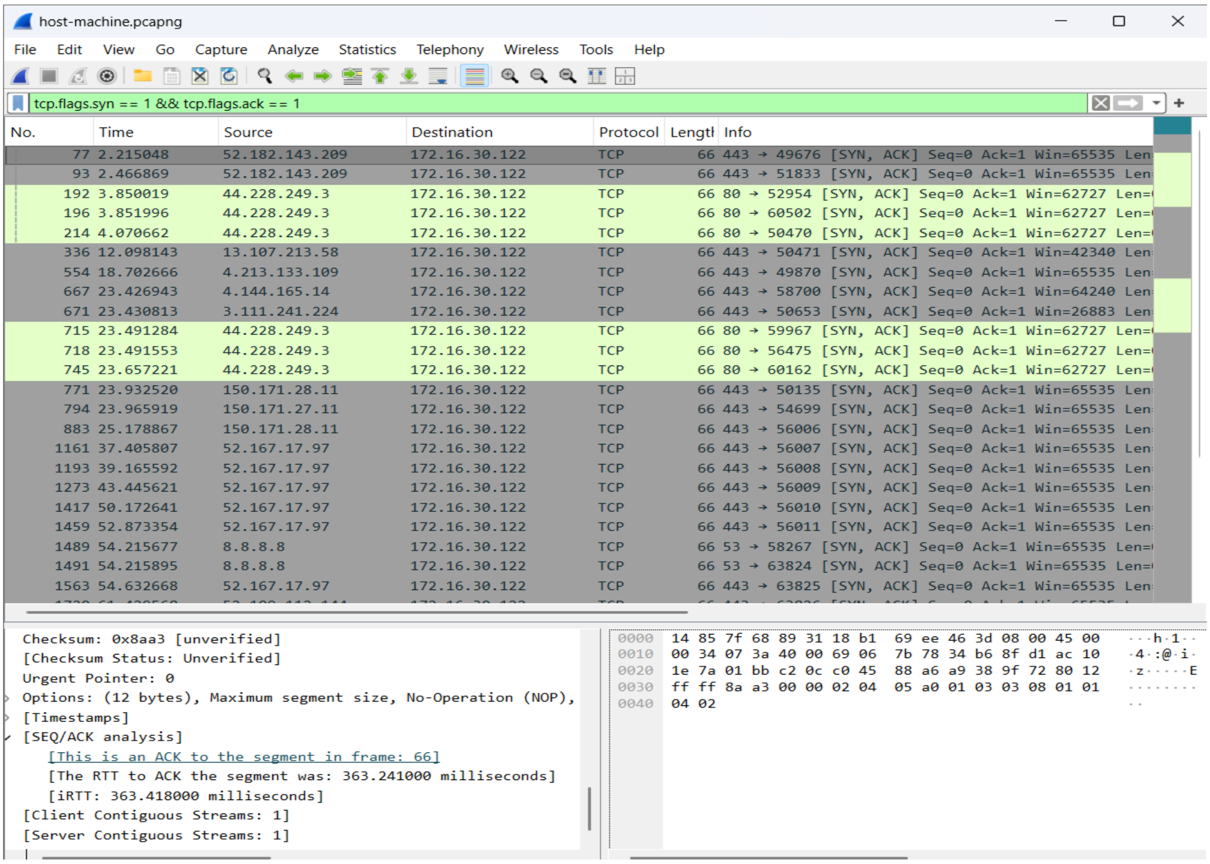
host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 && tcp.flags.ack == 0

```
No.     Time       Source          Destination      Protocol Lengtl Info
     66 1.851807   172.16.30.122   52.182.143.209   TCP      66 49676 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
     72 2.103746   172.16.30.122   52.182.143.209   TCP      66 51833 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    162 3.439978   172.16.30.122   44.228.249.3     TCP      66 60502 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    163 3.440408   172.16.30.122   44.228.249.3     TCP      66 52954 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    172 3.474427   172.16.30.122   44.228.249.3     TCP      66 53790 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    180 3.691461   172.16.30.122   44.228.249.3     TCP      66 50470 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    223 4.475049   172.16.30.122   44.228.249.3     TCP      66 [TCP Retransmission] 53790 → 443 [SYN] Seq=0 Win
    243 6.475095   172.16.30.122   44.228.249.3     TCP      66 [TCP Retransmission] 53790 → 443 [SYN] Seq=0 Win
    305 10.475347  172.16.30.122   44.228.249.3     TCP      66 [TCP Retransmission] 53790 → 443 [SYN] Seq=0 Win
    335 12.071771  172.16.30.122   13.107.213.58    TCP      66 50471 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    534 18.476095  172.16.30.122   44.228.249.3     TCP      66 [TCP Retransmission] 53790 → 443 [SYN] Seq=0 Win
    546 18.649811  172.16.30.122   4.213.133.109    TCP      66 49870 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    620 23.169498  172.16.30.122   44.228.249.3     TCP      66 56475 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    621 23.169761  172.16.30.122   44.228.249.3     TCP      66 59967 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    660 23.367023  172.16.30.122   4.144.165.14     TCP      66 58700 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    665 23.408410  172.16.30.122   3.111.241.224    TCP      66 50653 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    666 23.420873  172.16.30.122   44.228.249.3     TCP      66 60162 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    757 23.819735  172.16.30.122   150.171.28.11    TCP      66 50135 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    783 23.939267  172.16.30.122   150.171.27.11    TCP      66 54699 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
    882 25.151048  172.16.30.122   150.171.28.11    TCP      66 56006 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
   1147 36.979247  172.16.30.122   52.167.17.97     TCP      66 56007 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
   1190 38.914263  172.16.30.122   52.167.17.97     TCP      66 56008 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
   1270 43.181504  172.16.30.122   52.167.17.97     TCP      66 56009 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
```

```
> Frame 180: Packet, 66 bytes on wire (528 bits), 66 bytes capt
> Ethernet II, Src: Intel_68:89:31 (14:85:7f:68:89:31), Dst: So
v Internet Protocol Version 4, Src: 172.16.30.122, Dst: 44.228.
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-E
      0000 00.. = Differentiated Services Codepoint: Default (
      .... ..00 = Explicit Congestion Notification: Not ECN-Ca
    Total Length: 52
    Identification: 0xf986 (63878)
  > 010. .... = Flags: 0x2, Don't fragment
```

```
0000  18 b1 69 ee 46 3d 14 85  7f 68 89 31 08 00 45 00   ··i·F=··
0010  00 34 f9 86 40 00 80 06  10 cb ac 10 1e 7a 2c e4   ·4··@···
0020  f9 03 c5 26 00 50 5c 8c  32 5e 00 00 00 00 80 02   ···&·P\·
0030  ff ff 2a 3d 00 00 02 04  05 b4 01 03 03 08 01 01   ··*=····
0040  04 02                                              ··
```

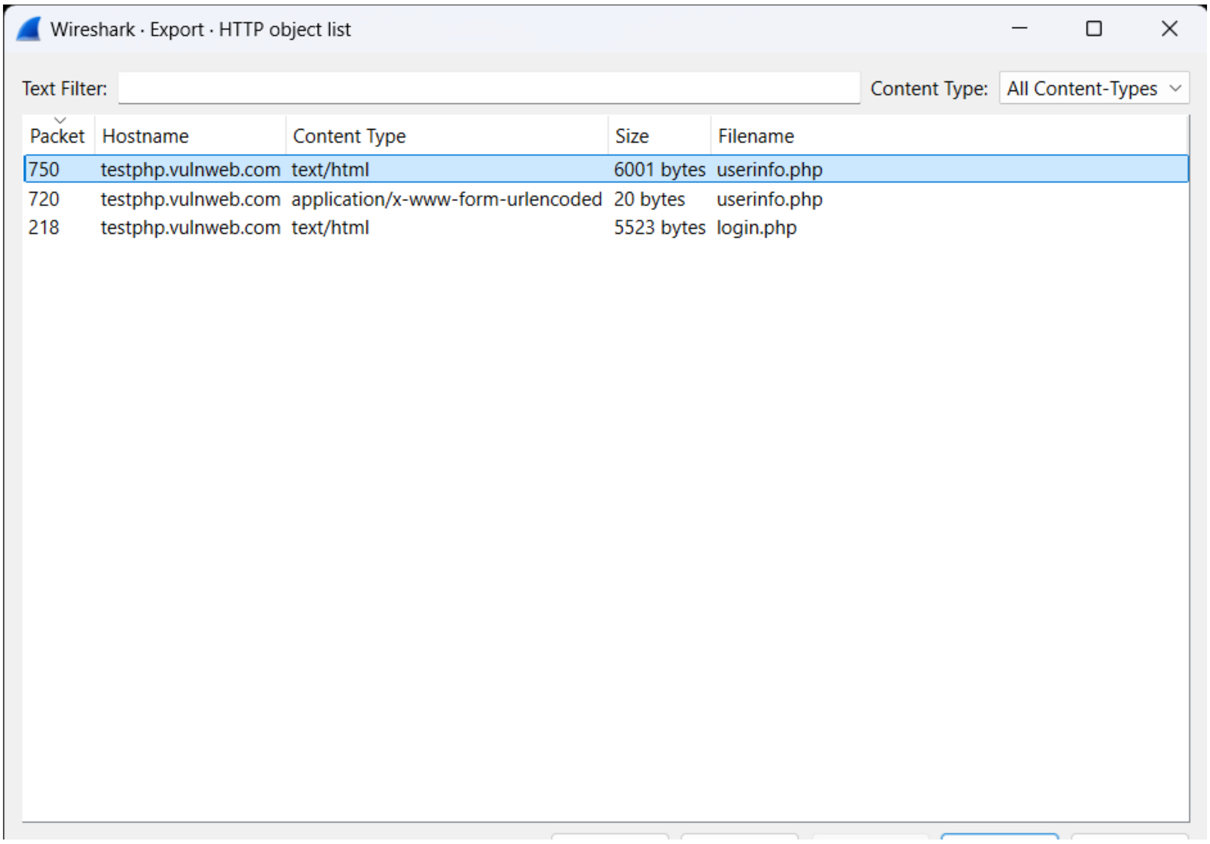


```
tcp.flags.syn == 1 && tcp.flags.ack == 1
```

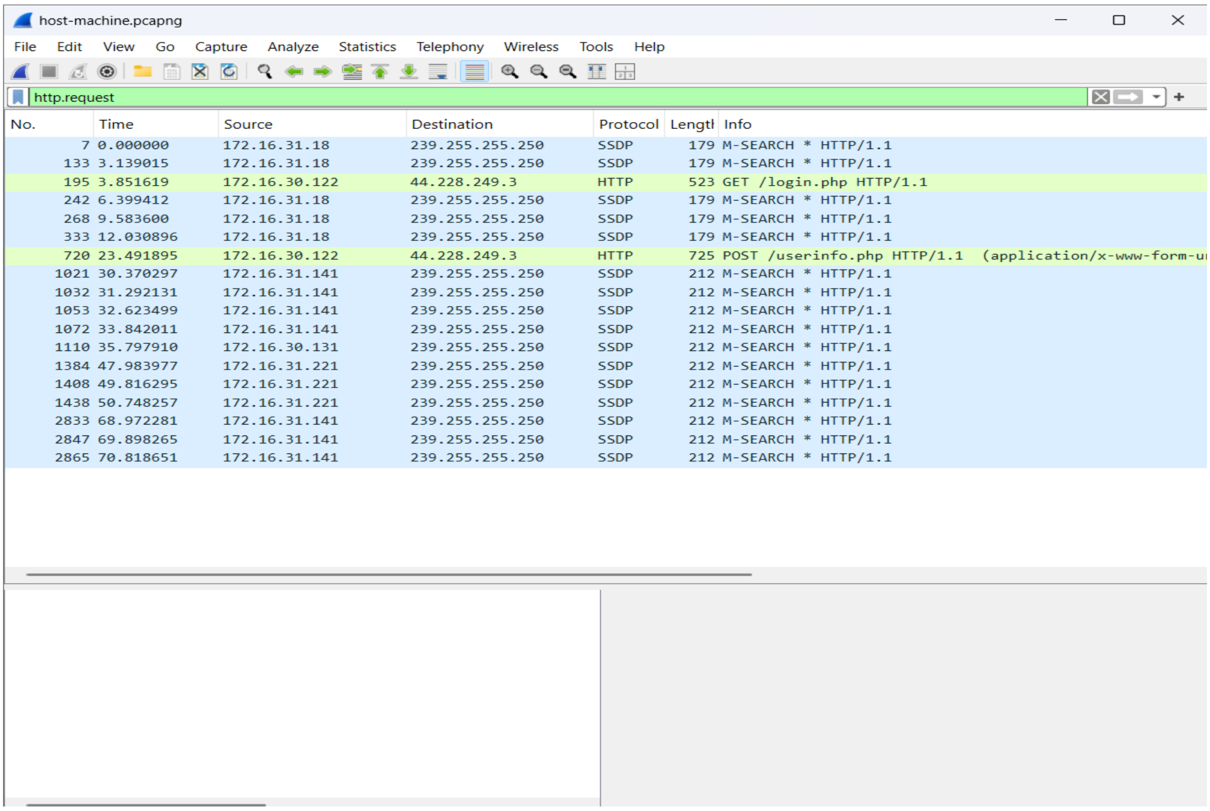
```
No.    Time        Source           Destination     Protocol Lengtl Info
  77 2.215048     52.182.143.209   172.16.30.122   TCP      66 443 → 49676 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
  93 2.466869     52.182.143.209   172.16.30.122   TCP      66 443 → 51833 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
 192 3.850019     44.228.249.3     172.16.30.122   TCP      66 80 → 52954 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=
 196 3.851996     44.228.249.3     172.16.30.122   TCP      66 80 → 60502 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=
 214 4.070662     44.228.249.3     172.16.30.122   TCP      66 80 → 50470 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=
 336 12.098143    13.107.213.58    172.16.30.122   TCP      66 443 → 50471 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len
 554 18.702666    4.213.133.109    172.16.30.122   TCP      66 443 → 49870 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
 667 23.426943    4.144.165.14     172.16.30.122   TCP      66 443 → 58700 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len
 671 23.430813    3.111.241.224    172.16.30.122   TCP      66 443 → 50653 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len
 715 23.491284    44.228.249.3     172.16.30.122   TCP      66 80 → 59967 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=
 718 23.491553    44.228.249.3     172.16.30.122   TCP      66 80 → 56475 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=
 745 23.657221    44.228.249.3     172.16.30.122   TCP      66 80 → 60162 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=
 771 23.932520    150.171.28.11    172.16.30.122   TCP      66 443 → 50135 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
 794 23.965919    150.171.27.11    172.16.30.122   TCP      66 443 → 54699 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
 883 25.178867    150.171.28.11    172.16.30.122   TCP      66 443 → 56006 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
1161 37.405807    52.167.17.97     172.16.30.122   TCP      66 443 → 56007 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
1193 39.165592    52.167.17.97     172.16.30.122   TCP      66 443 → 56008 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
1273 43.445621    52.167.17.97     172.16.30.122   TCP      66 443 → 56009 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
1417 50.172641    52.167.17.97     172.16.30.122   TCP      66 443 → 56010 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
1459 52.873354    52.167.17.97     172.16.30.122   TCP      66 443 → 56011 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
1489 54.215677    8.8.8.8          172.16.30.122   TCP      66 53 → 58267 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
1491 54.215895    8.8.8.8          172.16.30.122   TCP      66 53 → 63824 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
1563 54.632668    52.167.17.97     172.16.30.122   TCP      66 443 → 63825 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len
```

```
  Checksum: 0x8aa3 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operation (NOP),
> [Timestamps]
v [SEQ/ACK analysis]
     [This is an ACK to the segment in frame: 66]
     [The RTT to ACK the segment was: 363.241000 milliseconds]
     [iRTT: 363.418000 milliseconds]
  [Client Contiguous Streams: 1]
  [Server Contiguous Streams: 1]
```

```
0000  14 85 7f 68 89 31 18 b1  69 ee 46 3d 08 00 45 00   ···h·1··
0010  00 34 07 3a 40 00 69 06  7b 78 34 b6 8f d1 ac 10   ·4·:@·i·
0020  1e 7a 01 bb c2 0c c0 45  88 a6 a9 38 9f 72 80 12   ·z·····E
0030  ff ff 8a a3 00 00 02 04  05 a0 01 03 03 08 01 01   ········
0040  04 02                                              ··
```

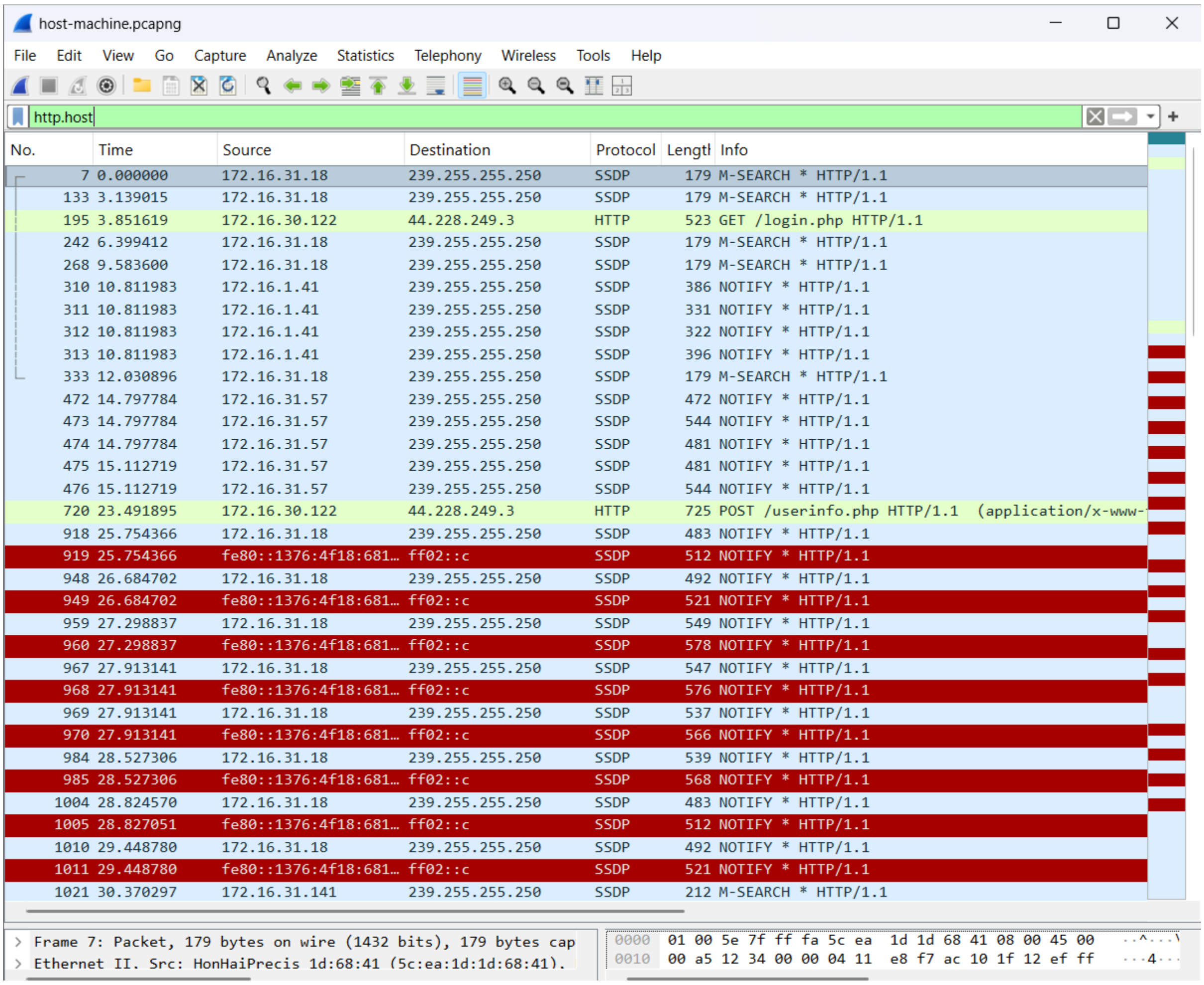


Packet	Hostname	Content Type	Size	Filename
750	testphp.vulnweb.com	text/html	6001 bytes	userinfo.php
720	testphp.vulnweb.com	application/x-www-form-urlencoded	20 bytes	userinfo.php
218	testphp.vulnweb.com	text/html	5523 bytes	login.php


host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

```
No.    Time          Source            Destination        Protocol Lengtl Info
     7 0.000000      172.16.31.18      239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   133 3.139015      172.16.31.18      239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   195 3.851619      172.16.30.122     44.228.249.3       HTTP     523 GET /login.php HTTP/1.1
   242 6.399412      172.16.31.18      239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   268 9.583600      172.16.31.18      239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   333 12.030896     172.16.31.18      239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   720 23.491895     172.16.30.122     44.228.249.3       HTTP     725 POST /userinfo.php HTTP/1.1  (application/x-www-form-u
  1021 30.370297     172.16.31.141     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  1032 31.292131     172.16.31.141     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  1053 32.623499     172.16.31.141     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  1072 33.842011     172.16.31.141     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  1110 35.797910     172.16.30.131     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  1384 47.983977     172.16.31.221     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  1408 49.816295     172.16.31.221     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  1438 50.748257     172.16.31.221     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  2833 68.972281     172.16.31.141     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  2847 69.898265     172.16.31.141     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
  2865 70.818651     172.16.31.141     239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
```

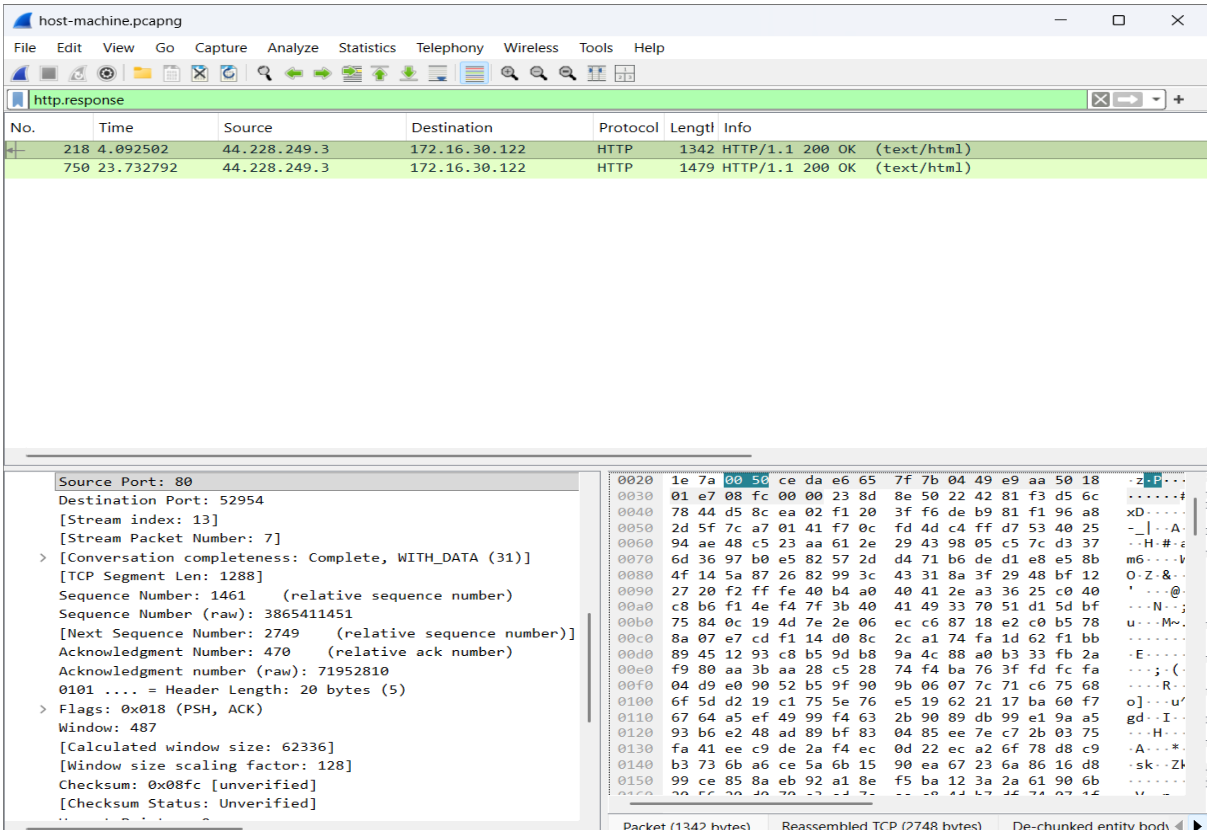

host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.host

```
No.    Time          Source                  Destination        Protocol Lengtl Info
     7 0.000000      172.16.31.18            239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   133 3.139015      172.16.31.18            239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   195 3.851619      172.16.30.122           44.228.249.3       HTTP     523 GET /login.php HTTP/1.1
   242 6.399412      172.16.31.18            239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   268 9.583600      172.16.31.18            239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   310 10.811983     172.16.1.41             239.255.255.250    SSDP     386 NOTIFY * HTTP/1.1
   311 10.811983     172.16.1.41             239.255.255.250    SSDP     331 NOTIFY * HTTP/1.1
   312 10.811983     172.16.1.41             239.255.255.250    SSDP     322 NOTIFY * HTTP/1.1
   313 10.811983     172.16.1.41             239.255.255.250    SSDP     396 NOTIFY * HTTP/1.1
   333 12.030896     172.16.31.18            239.255.255.250    SSDP     179 M-SEARCH * HTTP/1.1
   472 14.797784     172.16.31.57            239.255.255.250    SSDP     472 NOTIFY * HTTP/1.1
   473 14.797784     172.16.31.57            239.255.255.250    SSDP     544 NOTIFY * HTTP/1.1
   474 14.797784     172.16.31.57            239.255.255.250    SSDP     481 NOTIFY * HTTP/1.1
   475 15.112719     172.16.31.57            239.255.255.250    SSDP     481 NOTIFY * HTTP/1.1
   476 15.112719     172.16.31.57            239.255.255.250    SSDP     544 NOTIFY * HTTP/1.1
   720 23.491895     172.16.30.122           44.228.249.3       HTTP     725 POST /userinfo.php HTTP/1.1  (application/x-www-
   918 25.754366     172.16.31.18            239.255.255.250    SSDP     483 NOTIFY * HTTP/1.1
   919 25.754366     fe80::1376:4f18:681…    ff02::c            SSDP     512 NOTIFY * HTTP/1.1
   948 26.684702     172.16.31.18            239.255.255.250    SSDP     492 NOTIFY * HTTP/1.1
   949 26.684702     fe80::1376:4f18:681…    ff02::c            SSDP     521 NOTIFY * HTTP/1.1
   959 27.298837     172.16.31.18            239.255.255.250    SSDP     549 NOTIFY * HTTP/1.1
   960 27.298837     fe80::1376:4f18:681…    ff02::c            SSDP     578 NOTIFY * HTTP/1.1
   967 27.913141     172.16.31.18            239.255.255.250    SSDP     547 NOTIFY * HTTP/1.1
   968 27.913141     fe80::1376:4f18:681…    ff02::c            SSDP     576 NOTIFY * HTTP/1.1
   969 27.913141     172.16.31.18            239.255.255.250    SSDP     537 NOTIFY * HTTP/1.1
   970 27.913141     fe80::1376:4f18:681…    ff02::c            SSDP     566 NOTIFY * HTTP/1.1
   984 28.527306     172.16.31.18            239.255.255.250    SSDP     539 NOTIFY * HTTP/1.1
   985 28.527306     fe80::1376:4f18:681…    ff02::c            SSDP     568 NOTIFY * HTTP/1.1
  1004 28.824570     172.16.31.18            239.255.255.250    SSDP     483 NOTIFY * HTTP/1.1
  1005 28.827051     fe80::1376:4f18:681…    ff02::c            SSDP     512 NOTIFY * HTTP/1.1
  1010 29.448780     172.16.31.18            239.255.255.250    SSDP     492 NOTIFY * HTTP/1.1
  1011 29.448780     fe80::1376:4f18:681…    ff02::c            SSDP     521 NOTIFY * HTTP/1.1
  1021 30.370297     172.16.31.141           239.255.255.250    SSDP     212 M-SEARCH * HTTP/1.1
```

```
> Frame 7: Packet, 179 bytes on wire (1432 bits), 179 bytes cap
> Ethernet II. Src: HonHaiPrecis 1d:68:41 (5c:ea:1d:1d:68:41).
```

```
0000  01 00 5e 7f ff fa 5c ea  1d 1d 68 41 08 00 45 00   ··^···\
0010  00 a5 12 34 00 00 04 11  e8 f7 ac 10 1f 12 ef ff   ···4···
```


host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

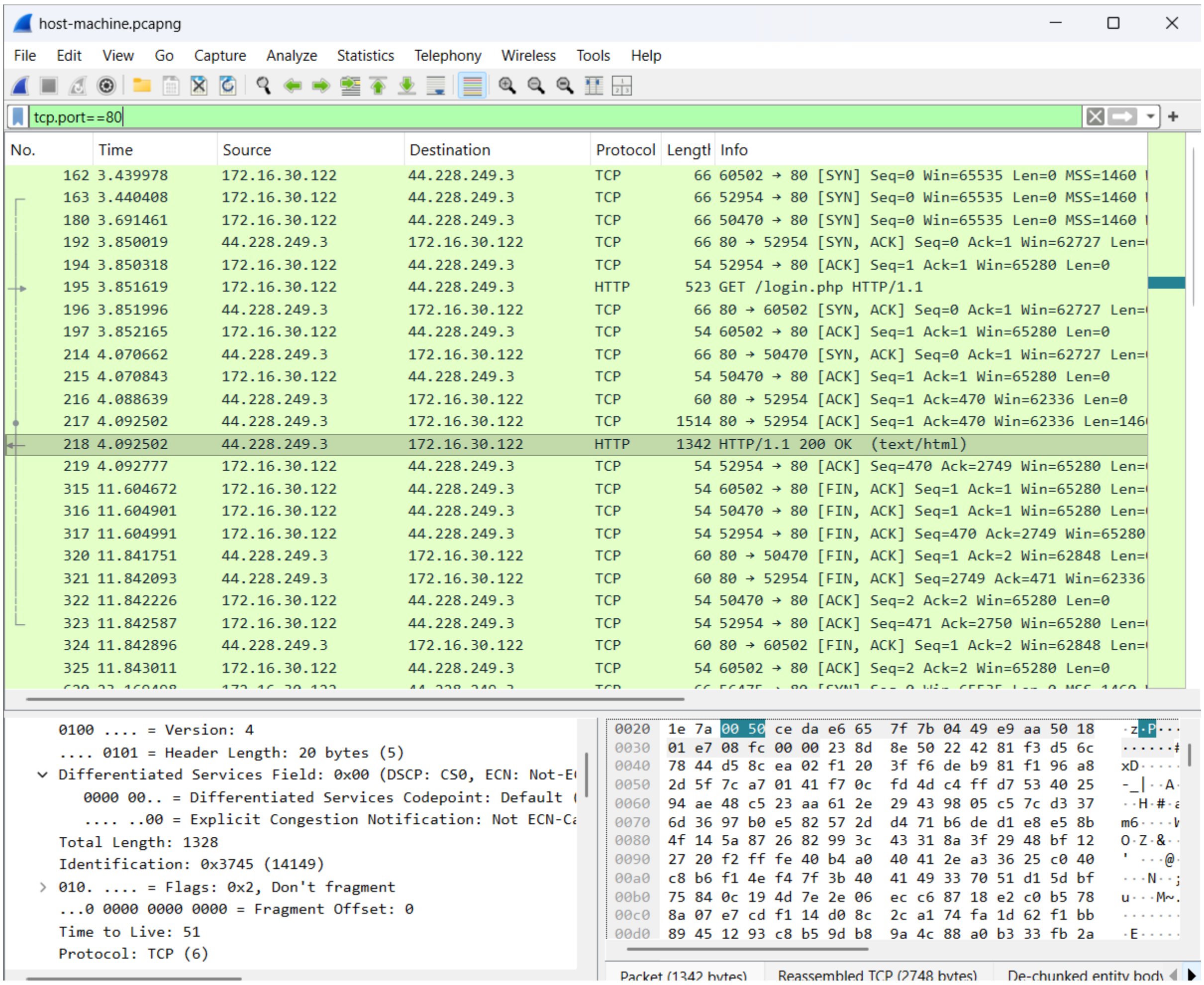
http.response

```
No.   Time        Source         Destination    Protocol Lengtl Info
  218 4.092502    44.228.249.3   172.16.30.122  HTTP     1342 HTTP/1.1 200 OK  (text/html)
  750 23.732792   44.228.249.3   172.16.30.122  HTTP     1479 HTTP/1.1 200 OK  (text/html)
```

```
      Source Port: 80
      Destination Port: 52954
      [Stream index: 13]
      [Stream Packet Number: 7]
    > [Conversation completeness: Complete, WITH_DATA (31)]
      [TCP Segment Len: 1288]
      Sequence Number: 1461    (relative sequence number)
      Sequence Number (raw): 3865411451
      [Next Sequence Number: 2749    (relative sequence number)]
      Acknowledgment Number: 470    (relative ack number)
      Acknowledgment number (raw): 71952810
      0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x018 (PSH, ACK)
      Window: 487
      [Calculated window size: 62336]
      [Window size scaling factor: 128]
      Checksum: 0x08fc [unverified]
      [Checksum Status: Unverified]
```

```
0020  1e 7a 00 50 ce da e6 65  7f 7b 04 49 e9 aa 50 18   ·z·P···
0030  01 e7 08 fc 00 00 23 8d  8e 50 22 42 81 f3 d5 6c   ······#
0040  78 44 d5 8c ea 02 f1 20  3f f6 de b9 81 f1 96 a8   xD·····
0050  2d 5f 7c a7 01 41 f7 0c  fd 4d c4 ff d7 53 40 25   -_|··A·
0060  94 ae 48 c5 23 aa 61 2e  29 43 98 05 c5 7c d3 37   ··H·#·a
0070  6d 36 97 b0 e5 82 57 2d  d4 71 b6 de d1 e8 e5 8b   m6····W
0080  4f 14 5a 87 26 82 99 3c  43 31 8a 3f 29 48 bf 12   O·Z·&··
0090  27 20 f2 ff fe 40 b4 a0  40 41 2e a3 36 25 c0 40   ' ···@·
00a0  c8 b6 f1 4e f4 7f 3b 40  41 49 33 70 51 d1 5d bf   ···N··;
00b0  75 84 0c 19 4d 7e 2e 06  ec c6 87 18 e2 c0 b5 78   u···M~.
00c0  8a 07 e7 cd f1 14 d0 8c  2c a1 74 fa 1d 62 f1 bb   ·······
00d0  89 45 12 93 c8 b5 9d b8  9a 4c 88 a0 b3 33 fb 2a   ·E·····
00e0  f9 80 aa 3b aa 28 c5 28  74 f4 ba 76 3f fd fc fa   ···;·(·
00f0  04 d9 e0 90 52 b5 9f 90  9b 06 07 7c 71 c6 75 68   ····R··
0100  6f 5d d2 19 c1 75 5e 76  e5 19 62 21 17 ba 60 f7   o]···u^
0110  67 64 a5 ef 49 99 f4 63  2b 90 89 db 99 e1 9a a5   gd··I··
0120  93 b6 e2 48 ad 89 bf 83  04 85 ee 7e c7 2b 03 75   ···H···
0130  fa 41 ee c9 de 2a f4 ec  0d 22 ec a2 6f 78 d8 c9   ·A···*·
0140  b3 73 6b a6 ce 5a 6b 15  90 ea 67 23 6a 86 16 d8   ·sk··Zk
0150  99 ce 85 8a eb 92 a1 8e  f5 ba 12 3a 2a 61 90 6b   ·······
```

Packet (1342 bytes)   Reassembled TCP (2748 bytes)   De-chunked entity body


host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

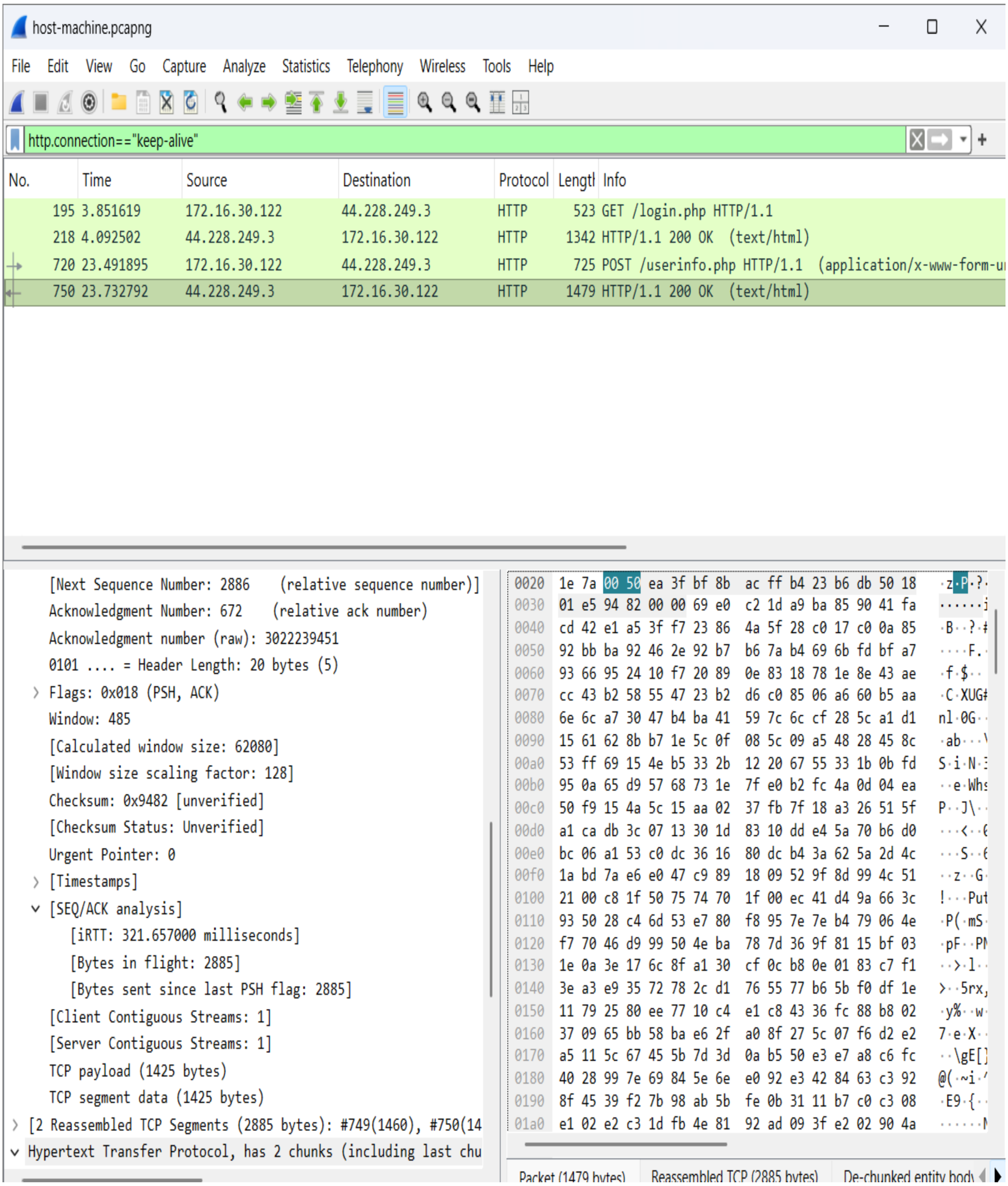
tcp.port==80

```
No.   Time        Source         Destination    Protocol Lengtl Info
  162 3.439978    172.16.30.122  44.228.249.3   TCP        66 60502 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
  163 3.440408    172.16.30.122  44.228.249.3   TCP        66 52954 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
  180 3.691461    172.16.30.122  44.228.249.3   TCP        66 50470 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
  192 3.850019    44.228.249.3   172.16.30.122  TCP        66 80 → 52954 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=
  194 3.850318    172.16.30.122  44.228.249.3   TCP        54 52954 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
  195 3.851619    172.16.30.122  44.228.249.3   HTTP      523 GET /login.php HTTP/1.1
  196 3.851996    44.228.249.3   172.16.30.122  TCP        66 80 → 60502 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=
  197 3.852165    172.16.30.122  44.228.249.3   TCP        54 60502 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
  214 4.070662    44.228.249.3   172.16.30.122  TCP        66 80 → 50470 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=
  215 4.070843    172.16.30.122  44.228.249.3   TCP        54 50470 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
  216 4.088639    44.228.249.3   172.16.30.122  TCP        60 80 → 52954 [ACK] Seq=1 Ack=470 Win=62336 Len=0
  217 4.092502    44.228.249.3   172.16.30.122  TCP      1514 80 → 52954 [ACK] Seq=1 Ack=470 Win=62336 Len=146
  218 4.092502    44.228.249.3   172.16.30.122  HTTP     1342 HTTP/1.1 200 OK  (text/html)
  219 4.092777    172.16.30.122  44.228.249.3   TCP        54 52954 → 80 [ACK] Seq=470 Ack=2749 Win=65280 Len=
  315 11.604672   172.16.30.122  44.228.249.3   TCP        54 60502 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65280 Len=
  316 11.604901   172.16.30.122  44.228.249.3   TCP        54 50470 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65280 Len=
  317 11.604991   172.16.30.122  44.228.249.3   TCP        54 52954 → 80 [FIN, ACK] Seq=470 Ack=2749 Win=65280
  320 11.841751   44.228.249.3   172.16.30.122  TCP        60 80 → 50470 [FIN, ACK] Seq=1 Ack=2 Win=62848 Len=
  321 11.842093   44.228.249.3   172.16.30.122  TCP        60 80 → 52954 [FIN, ACK] Seq=2749 Ack=471 Win=62336
  322 11.842226   172.16.30.122  44.228.249.3   TCP        54 50470 → 80 [ACK] Seq=2 Ack=2 Win=65280 Len=0
  323 11.842587   172.16.30.122  44.228.249.3   TCP        54 52954 → 80 [ACK] Seq=471 Ack=2750 Win=65280 Len=
  324 11.842896   44.228.249.3   172.16.30.122  TCP        60 80 → 60502 [FIN, ACK] Seq=1 Ack=2 Win=62848 Len=
  325 11.843011   172.16.30.122  44.228.249.3   TCP        54 60502 → 80 [ACK] Seq=2 Ack=2 Win=65280 Len=0
```

```
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ∨ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-E
        0000 00.. = Differentiated Services Codepoint: Default (
        .... ..00 = Explicit Congestion Notification: Not ECN-C
      Total Length: 1328
      Identification: 0x3745 (14149)
    > 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 51
      Protocol: TCP (6)
```

```
0020  1e 7a 00 50 ce da e6 65  7f 7b 04 49 e9 aa 50 18   ·z·P···
0030  01 e7 08 fc 00 00 23 8d  8e 50 22 42 81 f3 d5 6c   ······#
0040  78 44 d5 8c ea 02 f1 20  3f f6 de b9 81 f1 96 a8   xD·····
0050  2d 5f 7c a7 01 41 f7 0c  fd 4d c4 ff d7 53 40 25   -_|··A·
0060  94 ae 48 c5 23 aa 61 2e  29 43 98 05 c5 7c d3 37   ··H·#·a
0070  6d 36 97 b0 e5 82 57 2d  d4 71 b6 de d1 e8 e5 8b   m6····W
0080  4f 14 5a 87 26 82 99 3c  43 31 8a 3f 29 48 bf 12   O·Z·&··
0090  27 20 f2 ff fe 40 b4 a0  40 41 2e a3 36 25 c0 40   ' ···@·
00a0  c8 b6 f1 4e f4 7f 3b 40  41 49 33 70 51 d1 5d bf   ···N··;
00b0  75 84 0c 19 4d 7e 2e 06  ec c6 87 18 e2 c0 b5 78   u···M~.
00c0  8a 07 e7 cd f1 14 d0 8c  2c a1 74 fa 1d 62 f1 bb   ·······
00d0  89 45 12 93 c8 b5 9d b8  9a 4c 88 a0 b3 33 fb 2a   ·E·····
```

Packet (1342 bytes)   Reassembled TCP (2748 bytes)   De-chunked entity body


host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

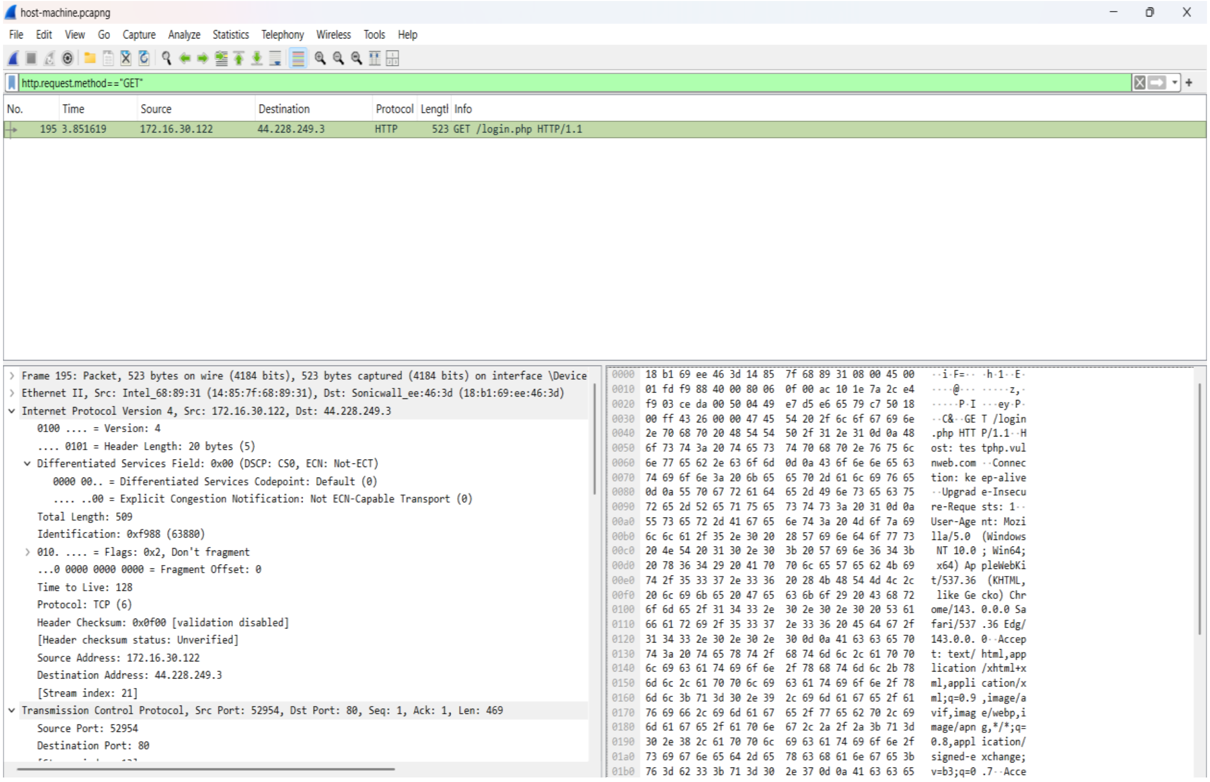
http.connection=="keep-alive"

```
No.   Time        Source          Destination     Protocol Lengtl Info
  195 3.851619    172.16.30.122   44.228.249.3    HTTP      523 GET /login.php HTTP/1.1
  218 4.092502    44.228.249.3    172.16.30.122   HTTP     1342 HTTP/1.1 200 OK  (text/html)
  720 23.491895   172.16.30.122   44.228.249.3    HTTP      725 POST /userinfo.php HTTP/1.1  (application/x-www-form-u
  750 23.732792   44.228.249.3    172.16.30.122   HTTP     1479 HTTP/1.1 200 OK  (text/html)
```

```
      [Next Sequence Number: 2886    (relative sequence number)]
      Acknowledgment Number: 672    (relative ack number)
      Acknowledgment number (raw): 3022239451
      0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x018 (PSH, ACK)
      Window: 485
      [Calculated window size: 62080]
      [Window size scaling factor: 128]
      Checksum: 0x9482 [unverified]
      [Checksum Status: Unverified]
      Urgent Pointer: 0
    > [Timestamps]
    v [SEQ/ACK analysis]
        [iRTT: 321.657000 milliseconds]
        [Bytes in flight: 2885]
        [Bytes sent since last PSH flag: 2885]
      [Client Contiguous Streams: 1]
      [Server Contiguous Streams: 1]
      TCP payload (1425 bytes)
      TCP segment data (1425 bytes)
> [2 Reassembled TCP Segments (2885 bytes): #749(1460), #750(14
v Hypertext Transfer Protocol, has 2 chunks (including last chu
```

```
0020  1e 7a 00 50 ea 3f bf 8b  ac ff b4 23 b6 db 50 18   ·z·P·?·
0030  01 e5 94 82 00 00 69 e0  c2 1d a9 ba 85 90 41 fa   ······i
0040  cd 42 e1 a5 3f f7 23 86  4a 5f 28 c0 17 c0 0a 85   ·B··?·#
0050  92 bb ba 92 46 2e 92 b7  b6 7a b4 69 6b fd bf a7   ····F.·
0060  93 66 95 24 10 f7 20 89  0e 83 18 78 1e 8e 43 ae   ·f·$··
0070  cc 43 b2 58 55 47 23 b2  d6 c0 85 06 a6 60 b5 aa   ·C·XUG#
0080  6e 6c a7 30 47 b4 ba 41  59 7c 6c cf 28 5c a1 d1   nl·0G··
0090  15 61 62 8b b7 1e 5c 0f  08 5c 09 a5 48 28 45 8c   ·ab···\
00a0  53 ff 69 15 4e b5 33 2b  12 20 67 55 33 1b 0b fd   S·i·N·3
00b0  95 0a 65 d9 57 68 73 1e  7f e0 b2 fc 4a 0d 04 ea   ··e·Whs
00c0  50 f9 15 4a 5c 15 aa 02  37 fb 7f 18 a3 26 51 5f   P··J\··
00d0  a1 ca db 3c 07 13 30 1d  83 10 dd e4 5a 70 b6 d0   ···<··0
00e0  bc 06 a1 53 c0 dc 36 16  80 dc b4 3a 62 5a 2d 4c   ···S··6
00f0  1a bd 7a e6 e0 47 c9 89  18 09 52 9f 8d 99 4c 51   ··z··G·
0100  21 00 c8 1f 50 75 74 70  1f 00 ec 41 d4 9a 66 3c   !···Put
0110  93 50 28 c4 6d 53 e7 80  f8 95 7e 7e b4 79 06 4e   ·P(·mS·
0120  f7 70 46 d9 99 50 4e ba  78 7d 36 9f 81 15 bf 03   ·pF··PN
0130  1e 0a 3e 17 6c 8f a1 30  cf 0c b8 0e 01 83 c7 f1   ··>·l··
0140  3e a3 e9 35 72 78 2c d1  76 55 77 b6 5b f0 df 1e   >··5rx,
0150  11 79 25 80 ee 77 10 c4  e1 c8 43 36 fc 88 b8 02   ·y%··w·
0160  37 09 65 bb 58 ba e6 2f  a0 8f 27 5c 07 f6 d2 e2   7·e·X··
0170  a5 11 5c 67 45 5b 7d 3d  0a b5 50 e3 e7 a8 c6 fc   ··\gE[}
0180  40 28 99 7e 69 84 5e 6e  e0 92 e3 42 84 63 c3 92   @(·~i·^
0190  8f 45 39 f2 7b 98 ab 5b  fe 0b 31 11 b7 c0 c3 08   ·E9·{··
01a0  e1 02 e2 c3 1d fb 4e 81  92 ad 09 3f e2 02 90 4a   ······N
```

TASK – 2

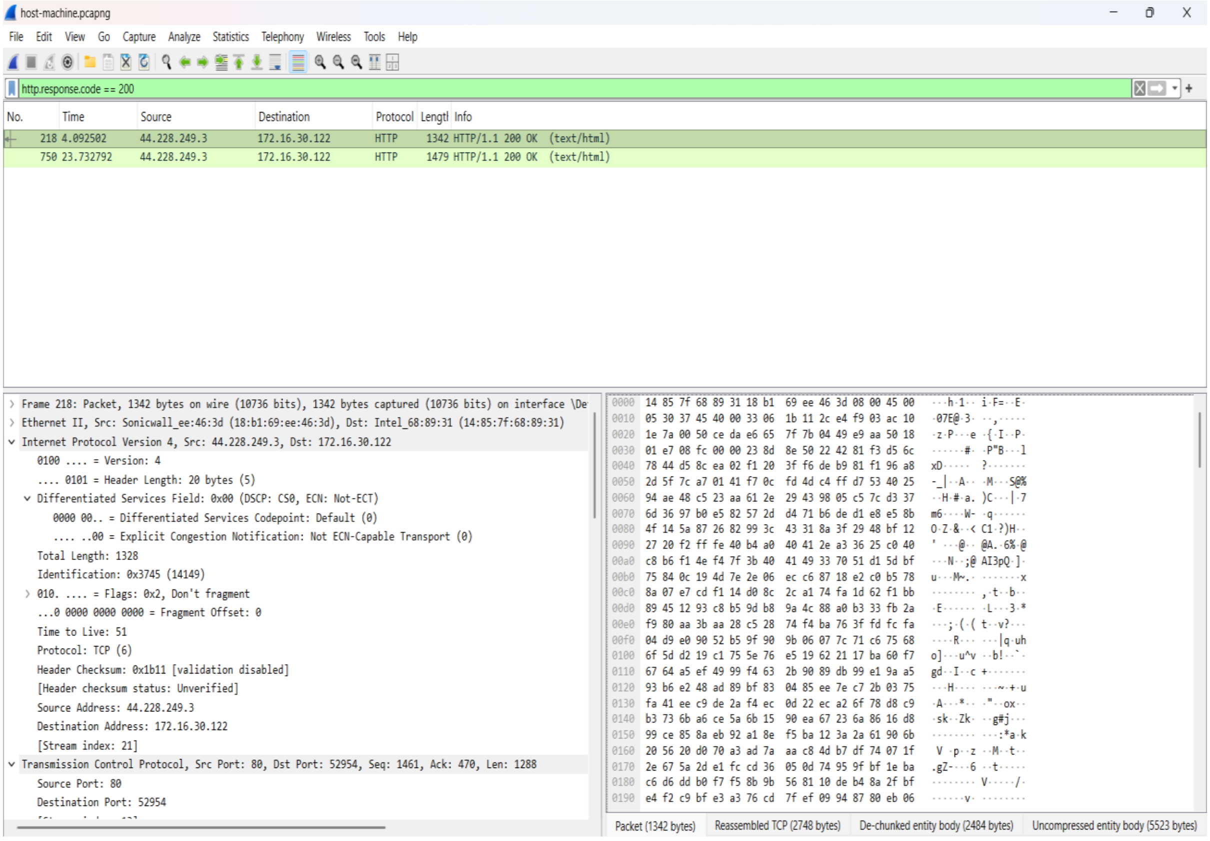

host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method=="GET"

```
No.   Time      Source         Destination    Protocol Lengtl Info
  195 3.851619  172.16.30.122  44.228.249.3   HTTP      523 GET /login.php HTTP/1.1
```

```
> Frame 195: Packet, 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits) on interface \Device
> Ethernet II, Src: Intel_68:89:31 (14:85:7f:68:89:31), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d)
v Internet Protocol Version 4, Src: 172.16.30.122, Dst: 44.228.249.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 509
    Identification: 0xf988 (63880)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0f00 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.30.122
    Destination Address: 44.228.249.3
    [Stream index: 21]
v Transmission Control Protocol, Src Port: 52954, Dst Port: 80, Seq: 1, Ack: 1, Len: 469
    Source Port: 52954
    Destination Port: 80
```

```
0000  18 b1 69 ee 46 3d 14 85  7f 68 89 31 08 00 45 00   ··i·F=·· ·h·1··E·
0010  01 fd f9 88 40 00 80 06  0f 00 ac 10 1e 7a 2c e4   ····@··· ·····z,·
0020  f9 03 ce da 00 50 04 49  e7 d5 e6 65 79 c7 50 18   ·····P·I ···ey·P·
0030  00 ff 43 26 00 00 47 45  54 20 2f 6c 6f 67 69 6e   ··C&··GE T /login
0040  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··H
0050  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vul
0060  6e 77 65 62 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   nweb.com ··Connec
0070  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0080  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0090  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
00a0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
00b0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
00c0  20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b    NT 10.0 ; Win64;
00d0  20 78 36 34 29 20 41 70  70 6c 65 57 65 62 4b 69    x64) Ap pleWebKi
00e0  74 2f 35 33 37 2e 33 36  20 28 4b 48 54 4d 4c 2c   t/537.36  (KHTML,
00f0  20 6c 69 6b 65 20 47 65  63 6b 6f 29 20 43 68 72    like Ge cko) Chr
0100  6f 6d 65 2f 31 34 33 2e  30 2e 30 2e 30 20 53 61   ome/143. 0.0.0 Sa
0110  66 61 72 69 2f 35 33 37  2e 33 36 20 45 64 67 2f   fari/537 .36 Edg/
0120  31 34 33 2e 30 2e 30 2e  30 0d 0a 41 63 63 65 70   143.0.0. 0··Accep
0130  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
0140  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0150  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0160  6d 6c 3b 71 3d 30 2e 39  2c 69 6d 61 67 65 2f 61   ml;q=0.9 ,image/a
0170  76 69 66 2c 69 6d 61 67  65 2f 77 65 62 70 2c 69   vif,imag e/webp,i
0180  6d 61 67 65 2f 61 70 6e  67 2c 2a 2f 2a 3b 71 3d   mage/apn g,*/*;q=
0190  30 2e 38 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   0.8,appl ication/
01a0  73 69 67 6e 65 64 2d 65  78 63 68 61 6e 67 65 3b   signed-e xchange;
01b0  76 3d 62 33 3b 71 3d 30  2e 37 0d 0a 41 63 63 65   v=b3;q=0 .7··Acce
```

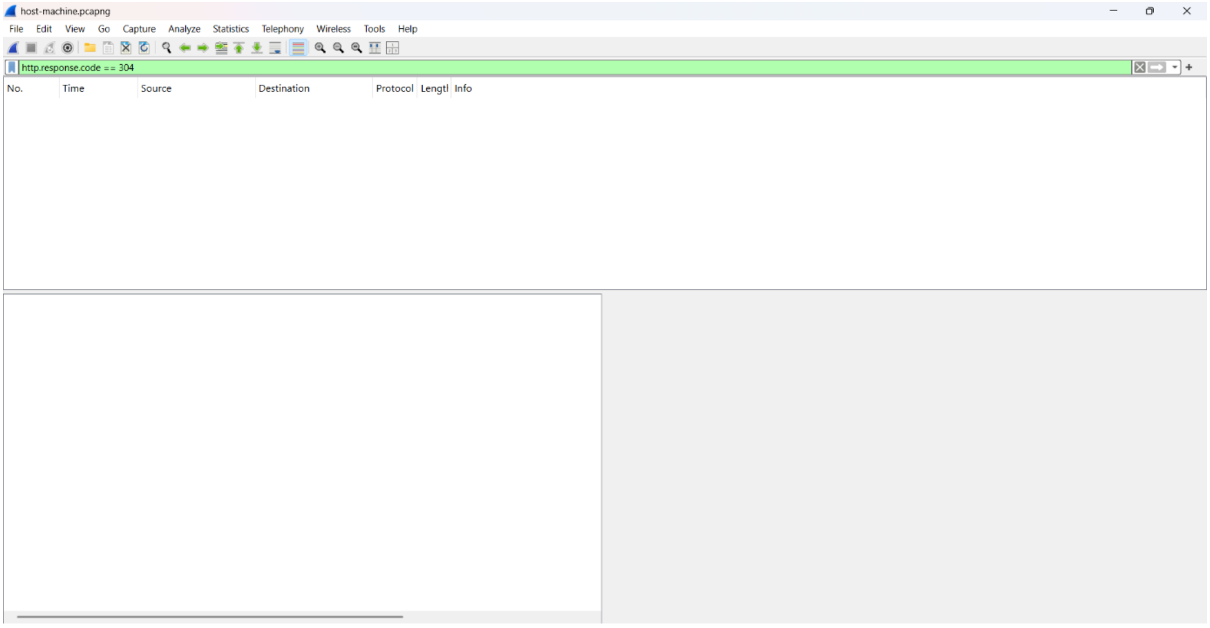

host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet (1342 bytes)
Reassembled TCP (2748 bytes)
De-chunked entity body (2484 bytes)
Uncompressed entity body (5523 bytes)

http.response.code == 200

```
No.   Time       Source        Destination    Protocol Lengtl Info
  218 4.092502   44.228.249.3  172.16.30.122  HTTP     1342 HTTP/1.1 200 OK  (text/html)
  750 23.732792  44.228.249.3  172.16.30.122  HTTP     1479 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 218: Packet, 1342 bytes on wire (10736 bits), 1342 bytes captured (10736 bits) on interface \De
> Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: Intel_68:89:31 (14:85:7f:68:89:31)
v Internet Protocol Version 4, Src: 44.228.249.3, Dst: 172.16.30.122
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1328
    Identification: 0x3745 (14149)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 51
    Protocol: TCP (6)
    Header Checksum: 0x1b11 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 44.228.249.3
    Destination Address: 172.16.30.122
    [Stream index: 21]
v Transmission Control Protocol, Src Port: 80, Dst Port: 52954, Seq: 1461, Ack: 470, Len: 1288
    Source Port: 80
    Destination Port: 52954
```

```
0000  14 85 7f 68 89 31 18 b1  69 ee 46 3d 08 00 45 00   ···h·1·· i·F=··E·
0010  05 30 37 45 40 00 33 06  1b 11 2c e4 f9 03 ac 10   ·07E@·3· ··,·····
0020  1e 7a 00 50 ce da e6 65  7f 7b 04 49 e9 aa 50 18   ·z·P···e ·{·I··P·
0030  01 e7 08 fc 00 00 23 8d  8e 50 22 42 81 f3 d5 6c   ······#· ·P"B···l
0040  78 44 d5 8c ea 02 f1 20  3f f6 de b9 81 f1 96 a8   xD·····  ?·······
0050  2d 5f 7c a7 01 41 f7 0c  fd 4d c4 ff d7 53 40 25   -_|··A·· ·M···S@%
0060  94 ae 48 c5 23 aa 61 2e  29 43 98 05 c5 7c d3 37   ··H·#·a. )C···|·7
0070  6d 36 97 b0 e5 82 57 2d  d4 71 b6 de d1 e8 e5 8b   m6····W- ·q······
0080  4f 14 5a 87 26 82 99 3c  43 31 8a 3f 29 48 bf 12   O·Z·&··< C1·?)H··
0090  27 20 f2 ff fe 40 b4 a0  40 41 2e a3 36 25 c0 40   ' ···@·· @A.·6%·@
00a0  c8 b6 f1 4e f4 7f 3b 40  41 49 33 70 51 d1 5d bf   ···N··;@ AI3pQ·]·
00b0  75 84 0c 19 4d 7e 2e 06  ec c6 87 18 e2 c0 b5 78   u···M~.· ·······x
00c0  8a 07 e7 cd f1 14 d0 8c  2c a1 74 fa 1d 62 f1 bb   ········ ,·t··b··
00d0  89 45 12 93 c8 b5 9d b8  9a 4c 88 a0 b3 33 fb 2a   ·E······ ·L···3·*
00e0  f9 80 aa 3b aa 28 c5 28  74 f4 ba 76 3f fd fc fa   ···;·(·( t··v?···
00f0  04 d9 e0 90 52 b5 9f 90  9b 06 07 7c 71 c6 75 68   ····R··· ···|q·uh
0100  6f 5d d2 19 c1 75 5e 76  e5 19 62 21 17 ba 60 f7   o]···u^v ··b!··`·
0110  67 64 a5 ef 49 99 f4 63  2b 90 89 db 99 e1 9a a5   gd··I··c +·······
0120  93 b6 e2 48 ad 89 bf 83  04 85 ee 7e c7 2b 03 75   ···H···· ···~·+·u
0130  fa 41 ee c9 de 2a f4 ec  0d 22 ec a2 6f 78 d8 c9   ·A···*·· ·"··ox··
0140  b3 73 6b a6 ce 5a 6b 15  90 ea 67 23 6a 86 16 d8   ·sk··Zk· ··g#j···
0150  99 ce 85 8a eb 92 a1 8e  f5 ba 12 3a 2a 61 90 6b   ········ ···:*a·k
0160  20 56 20 d0 70 a3 ad 7a  aa c8 4d b7 df 74 07 1f    V ·p··z ··M··t··
0170  2e 67 5a 2d e1 fc cd 36  05 0d 74 95 9f bf 1e ba   .gZ-···6 ··t·····
0180  c6 d6 dd b0 f7 f5 8b 9b  56 81 10 de b4 8a 2f bf   ········ V·····/·
0190  e4 f2 c9 bf e3 a3 76 cd  7f ef 09 94 87 80 eb 06   ······v· ········
```


host-machine.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 304

No. Time Source Destination Protocol Lengtl Info

2.3

First Request

During the first request, the browser cache is empty. The browser sends normal HTTP GET requests for the main HTML page and all embedded objects. Since the server has no information about any cached copies at the client side, it unconditionally sends the full content of every requested resource.

http method – 200 Ok – full content will be delivered

Second Request

During the second request, the browser already has cached copies of the previously downloaded resources. Instead of requesting the full content again, the browser sends conditional GET requests that include cache validation headers.

http method – 304 not modified – where it will not send any content if it was same.

2.4

List of HTTP method Headers

For 200

If modified since

If none match

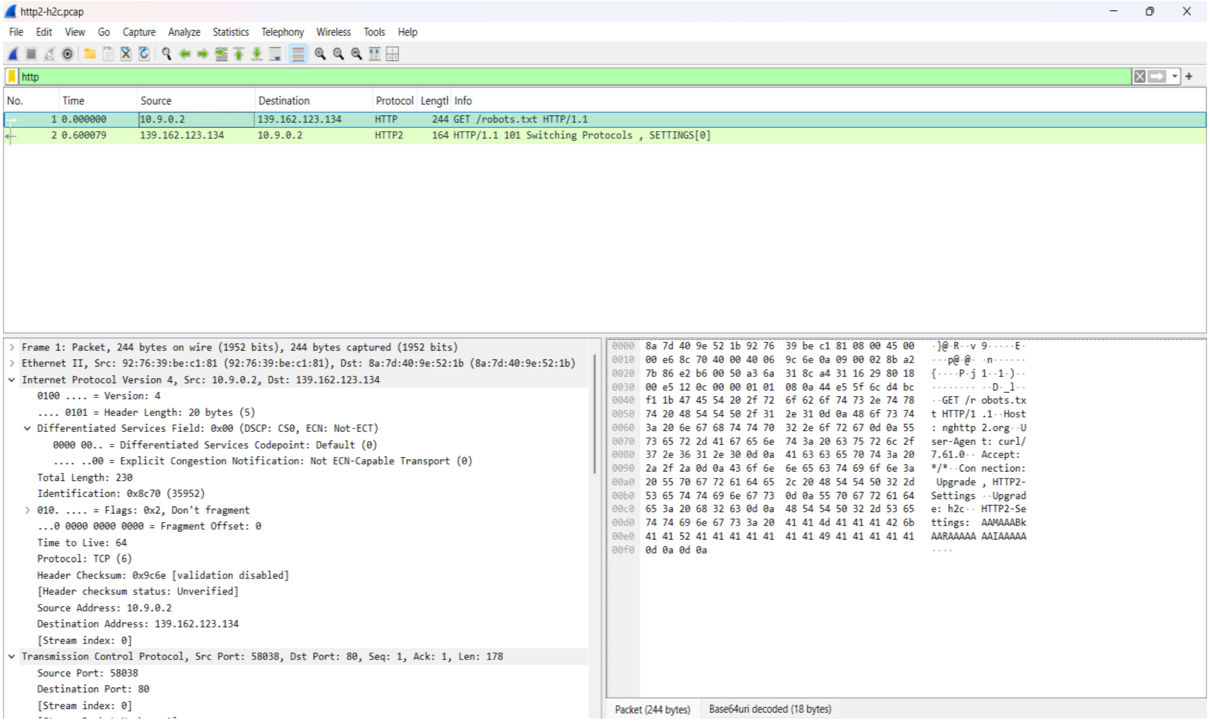
Cache control

For 304

Last modified

Etag

TASK – 3

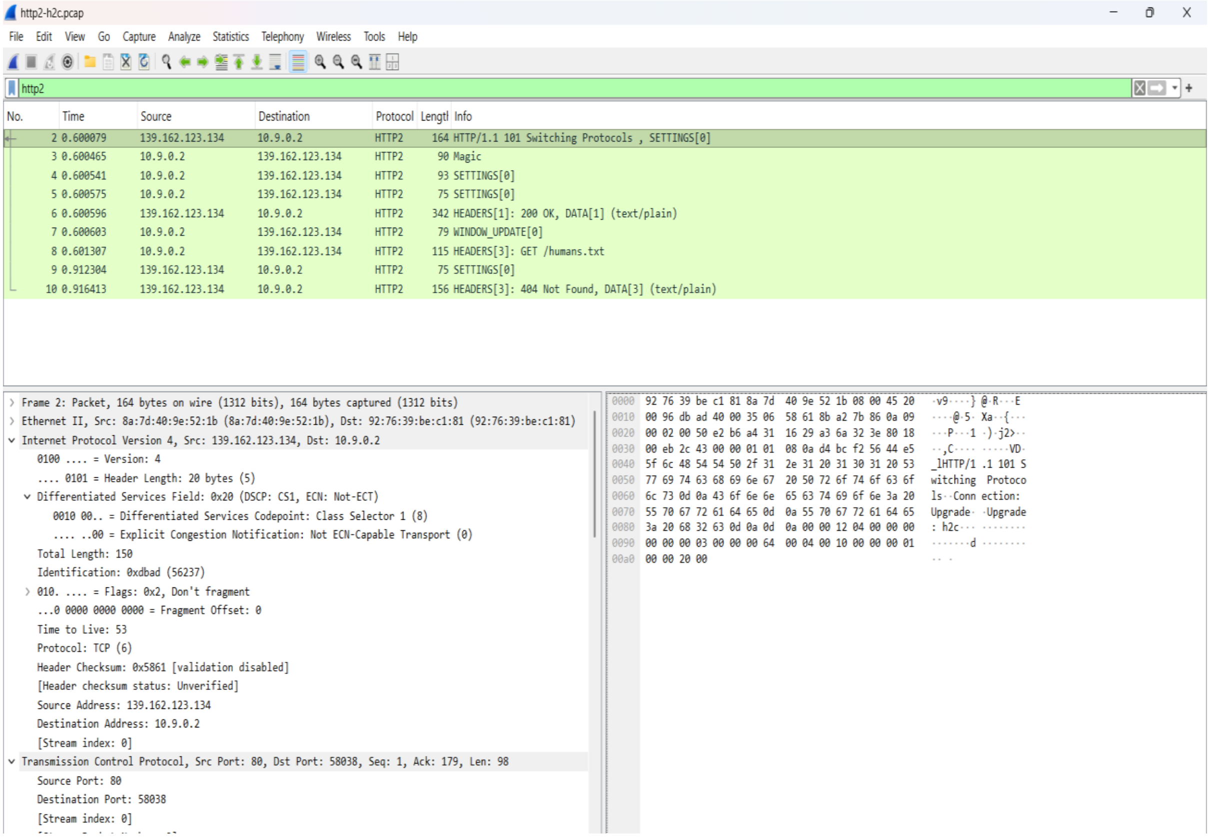


```
http
```

No.	Time	Source	Destination	Protocol	Lengtl	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 Protocols , SETTINGS[0]

```
> Frame 1: Packet, 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
> Ethernet II, Src: 92:76:39:be:c1:81 (92:76:39:be:c1:81), Dst: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b)
v Internet Protocol Version 4, Src: 10.9.0.2, Dst: 139.162.123.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 230
    Identification: 0x8c70 (35952)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x9c6e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.9.0.2
    Destination Address: 139.162.123.134
    [Stream index: 0]
v Transmission Control Protocol, Src Port: 58038, Dst Port: 80, Seq: 1, Ack: 1, Len: 178
    Source Port: 58038
    Destination Port: 80
    [Stream index: 0]
```

```
0000  8a 7d 40 9e 52 1b 92 76  39 be c1 81 08 00 45 00   ·}@·R··v 9·····E·
0010  00 e6 8c 70 40 00 40 06  9c 6e 0a 09 00 02 8b a2   ···p@·@· ·n······
0020  7b 86 e2 b6 00 50 a3 6a  31 8c a4 31 16 29 80 18   {····P·j 1··1·)··
0030  00 e5 12 0c 00 00 01 01  08 0a 44 e5 5f 6c d4 bc   ········ ··D·_l··
0040  f1 1b 47 45 54 20 2f 72  6f 62 6f 74 73 2e 74 78   ··GET /r obots.tx
0050  74 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   t HTTP/1 .1··Host
0060  3a 20 6e 67 68 74 74 70  32 2e 6f 72 67 0d 0a 55   : nghttp 2.org··U
0070  73 65 72 2d 41 67 65 6e  74 3a 20 63 75 72 6c 2f   ser-Agen t: curl/
0080  37 2e 36 31 2e 30 0d 0a  41 63 63 65 70 74 3a 20   7.61.0·· Accept: 
0090  2a 2f 2a 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   */*··Con nection:
00a0  20 55 70 67 72 61 64 65  2c 20 48 54 54 50 32 2d    Upgrade , HTTP2-
00b0  53 65 74 74 69 6e 67 73  0d 0a 55 70 67 72 61 64   Settings ··Upgrad
00c0  65 3a 20 68 32 63 0d 0a  48 54 54 50 32 2d 53 65   e: h2c·· HTTP2-Se
00d0  74 74 69 6e 67 73 3a 20  41 41 4d 41 41 41 42 6b   ttings:  AAMAAABk
00e0  41 41 52 41 41 41 41 41  41 41 49 41 41 41 41 41   AARAAAAA AAIAAAAA
00f0  0d 0a 0d 0a                                        ····
```

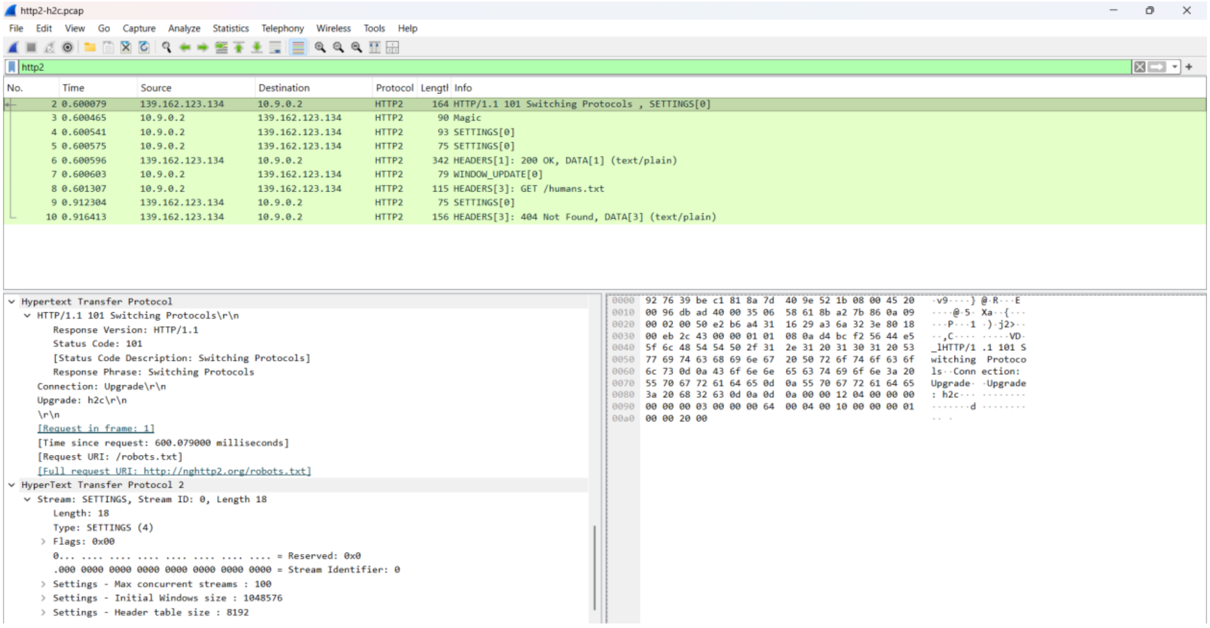


```
http2
```

No.	Time	Source	Destination	Protocol	Lengtl	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)

```
> Frame 2: Packet, 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
> Ethernet II, Src: 8a:7d:40:9e:52:1b (8a:7d:40:9e:52:1b), Dst: 92:76:39:be:c1:81 (92:76:39:be:c1:81)
v Internet Protocol Version 4, Src: 139.162.123.134, Dst: 10.9.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
      0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 150
    Identification: 0xdbad (56237)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 53
    Protocol: TCP (6)
    Header Checksum: 0x5861 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 139.162.123.134
    Destination Address: 10.9.0.2
    [Stream index: 0]
v Transmission Control Protocol, Src Port: 80, Dst Port: 58038, Seq: 1, Ack: 179, Len: 98
    Source Port: 80
    Destination Port: 58038
    [Stream index: 0]
```

```
0000  92 76 39 be c1 81 8a 7d  40 9e 52 1b 08 00 45 20   ·v9····} @·R···E 
0010  00 96 db ad 40 00 35 06  58 61 8b a2 7b 86 0a 09   ····@·5· Xa··{···
0020  00 02 00 50 e2 b6 a4 31  16 29 a3 6a 32 3e 80 18   ···P···1 ·)·j2>··
0030  00 eb 2c 43 00 00 01 01  08 0a d4 bc f2 56 44 e5   ··,C···· ·····VD·
0040  5f 6c 48 54 54 50 2f 31  2e 31 20 31 30 31 20 53   _lHTTP/1 .1 101 S
0050  77 69 74 63 68 69 6e 67  20 50 72 6f 74 6f 63 6f   witching  Protoco
0060  6c 73 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   ls··Conn ection: 
0070  55 70 67 72 61 64 65 0d  0a 55 70 67 72 61 64 65   Upgrade· ·Upgrade
0080  3a 20 68 32 63 0d 0a 0d  0a 00 00 12 04 00 00 00   : h2c··· ········
0090  00 00 00 03 00 00 00 64  00 04 00 10 00 00 00 01   ·······d ········
00a0  00 00 20 00                                        ·· ·
```



```
http2
```

```
No.     Time      Source            Destination       Protocol Lengtl 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)
```

```
v Hypertext Transfer Protocol
  v 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]
v HyperText Transfer Protocol 2
  v Stream: SETTINGS, Stream ID: 0, Length 18
      Length: 18
      Type: SETTINGS (4)
    > Flags: 0x00
      0... .... .... .... .... .... .... .... = Reserved: 0x0
      .000 0000 0000 0000 0000 0000 0000 0000 = Stream Identifier: 0
    > Settings - Max concurrent streams : 100
    > Settings - Initial Windows size : 1048576
    > Settings - Header table size : 8192
```

```
0000  92 76 39 be c1 81 8a 7d  40 9e 52 1b 08 00 45 20   ·v9····} @·R···E
0010  00 96 db ad 40 00 35 06  58 61 8b a2 7b 86 0a 09   ····@·5· Xa··{···
0020  00 02 00 50 e2 b6 a4 31  16 29 a3 6a 32 3e 80 18   ···P···1 ·)·j2>··
0030  00 eb 2c 43 00 00 01 01  08 0a d4 bc f2 56 44 e5   ··,C···· ·····VD·
0040  5f 6c 48 54 54 50 2f 31  2e 31 20 31 30 31 20 53   _lHTTP/1 .1 101 S
0050  77 69 74 63 68 69 6e 67  20 50 72 6f 74 6f 63 6f   witching  Protoco
0060  6c 73 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   ls··Conn ection: 
0070  55 70 67 72 61 64 65 0d  0a 55 70 67 72 61 64 65   Upgrade· ·Upgrade
0080  3a 20 68 32 63 0d 0a 0d  0a 00 00 12 04 00 00 00   : h2c··· ········
0090  00 00 00 03 00 00 00 64  00 04 00 10 00 00 00 01   ·······d ········
00a0  00 00 20 00                                        ·· ·
```