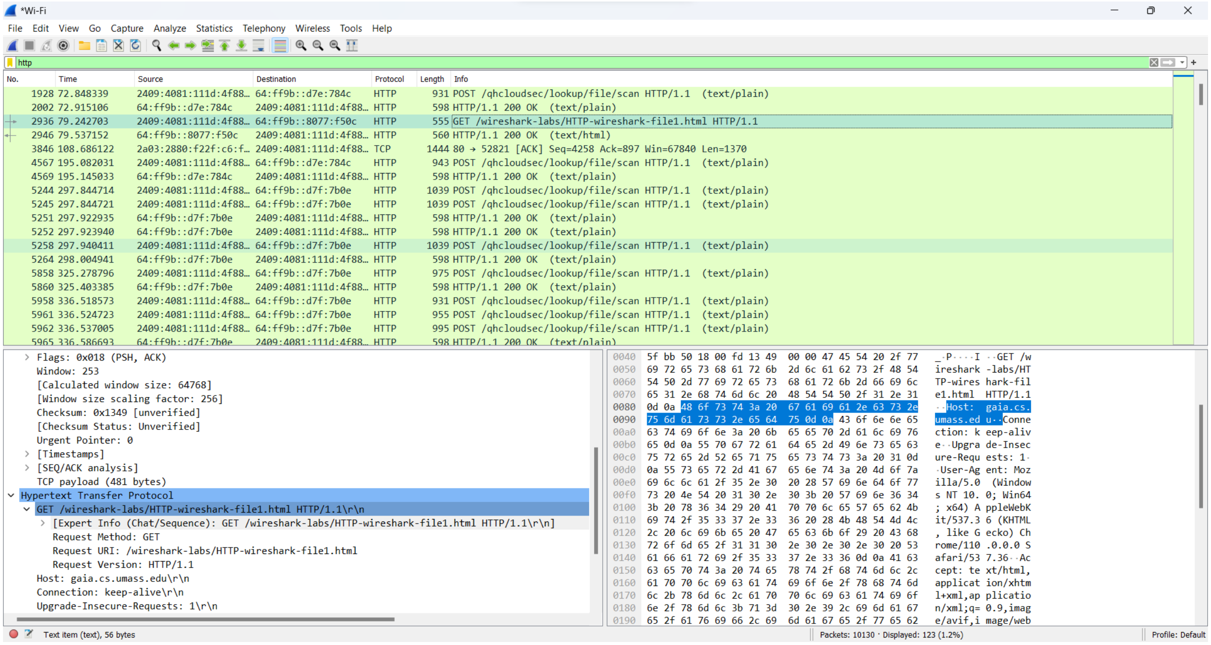
CN ASSIGNMENT 1 - BT20CSE031

HTTP:

1. My browser is running HTTP 1.1


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

```
No.   Time        Source                     Destination                Protocol Length Info
 1928 72.848339   2409:4081:111d:4f88…       64:ff9b::d7e:784c          HTTP      931 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 2002 72.915106   64:ff9b::d7e:784c          2409:4081:111d:4f88…       HTTP      598 HTTP/1.1 200 OK  (text/plain)
 2936 79.242703   2409:4081:111d:4f88…       64:ff9b::8077:f50c         HTTP      555 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 2946 79.537152   64:ff9b::8077:f50c         2409:4081:111d:4f88…       HTTP      560 HTTP/1.1 200 OK  (text/html)
 3846 108.686122  2a03:2880:f22f:c6:f…       2409:4081:111d:4f88…       TCP      1444 80 → 52821 [ACK] Seq=4258 Ack=897 Win=67840 Len=1370
 4567 195.082031  2409:4081:111d:4f88…       64:ff9b::d7e:784c          HTTP      943 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 4569 195.145033  64:ff9b::d7e:784c          2409:4081:111d:4f88…       HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5244 297.844714  2409:4081:111d:4f88…       64:ff9b::d7f:7b0e          HTTP     1039 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5245 297.844721  2409:4081:111d:4f88…       64:ff9b::d7f:7b0e          HTTP     1039 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5251 297.922935  64:ff9b::d7f:7b0e          2409:4081:111d:4f88…       HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5252 297.923940  64:ff9b::d7f:7b0e          2409:4081:111d:4f88…       HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5258 297.940411  2409:4081:111d:4f88…       64:ff9b::d7f:7b0e          HTTP     1039 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5264 298.004941  64:ff9b::d7f:7b0e          2409:4081:111d:4f88…       HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5858 325.278796  2409:4081:111d:4f88…       64:ff9b::d7f:7b0e          HTTP      975 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5860 325.403385  64:ff9b::d7f:7b0e          2409:4081:111d:4f88…       HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5958 336.518573  2409:4081:111d:4f88…       64:ff9b::d7f:7b0e          HTTP      931 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5961 336.524723  2409:4081:111d:4f88…       64:ff9b::d7f:7b0e          HTTP      955 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5962 336.537005  2409:4081:111d:4f88…       64:ff9b::d7f:7b0e          HTTP      995 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5965 336.586693  64:ff9b::d7f:7b0e          2409:4081:111d:4f88…       HTTP      598 HTTP/1.1 200 OK  (text/plain)
```

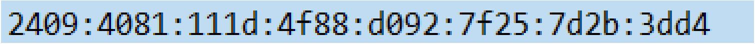
```
  > Flags: 0x018 (PSH, ACK)
    Window: 253
    [Calculated window size: 64768]
    [Window size scaling factor: 256]
    Checksum: 0x1349 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (481 bytes)
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
```

```
0040  5f bb 50 18 00 fd 13 49  00 00 47 45 54 20 2f 77   _·P····I ··GET /w
0050  69 72 65 73 68 61 72 6b  2d 6c 61 62 73 2f 48 54   ireshark -labs/HT
0060  54 50 2d 77 69 72 65 73  68 61 72 6b 2d 66 69 6c   TP-wires hark-fil
0070  65 31 2e 68 74 6d 6c 20  48 54 54 50 2f 31 2e 31   e1.html  HTTP/1.1
0080  0d 0a 48 6f 73 74 3a 20  67 61 69 61 2e 63 73 2e   ··Host:  gaia.cs.
0090  75 6d 61 73 73 2e 65 64  75 0d 0a 43 6f 6e 6e 65   umass.ed u··Conne
00a0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00b0  65 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   e··Upgra de-Insec
00c0  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
00d0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00e0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
00f0  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0100  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
0110  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
0120  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
0130  72 6f 6d 65 2f 31 31 30  2e 30 2e 30 2e 30 20 53   rome/110 .0.0.0 S
0140  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0150  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0160  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
0170  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0180  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0190  65 2f 61 76 69 66 2c 69  6d 61 67 65 2f 77 65 62   e/avif,i mage/web
```

Text item (text), 56 bytes   Packets: 10130 · Displayed: 123 (1.2%)   Profile: Default

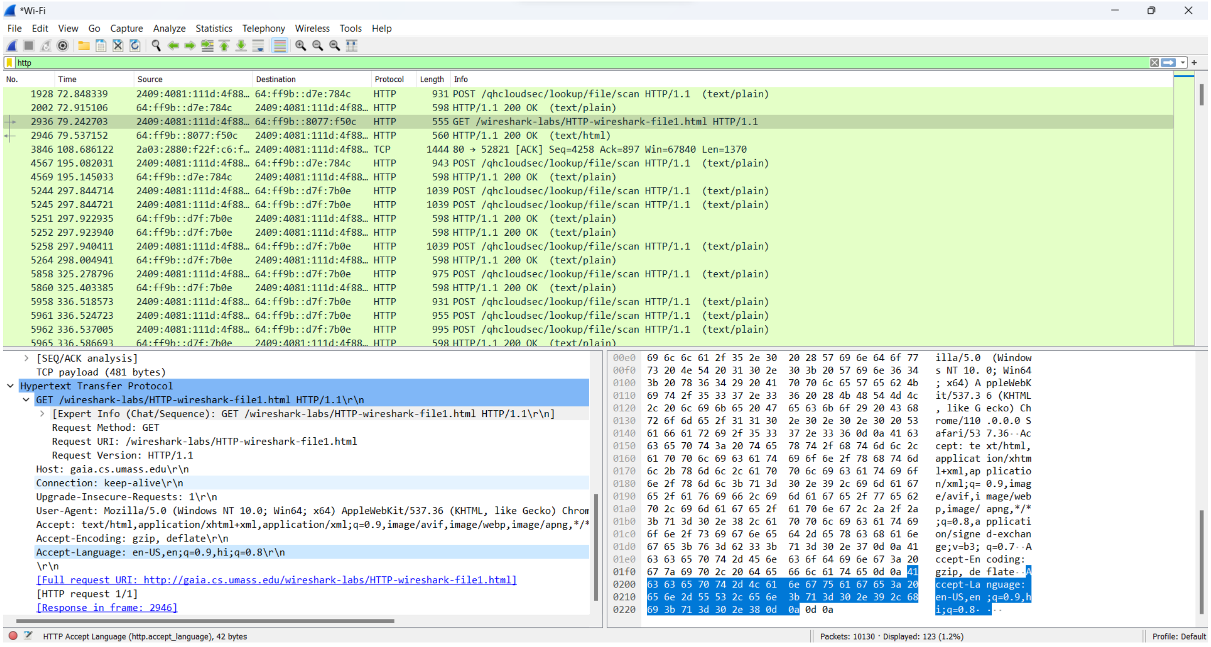
2. Languages supported as indicated are en-US (English) and hi (Hindi)

3. The IP address of my computer is



2409:4081:111d:4f88:d092:7f25:7d2b:3dd4

4. The status code returned to the browser is 200 OK


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

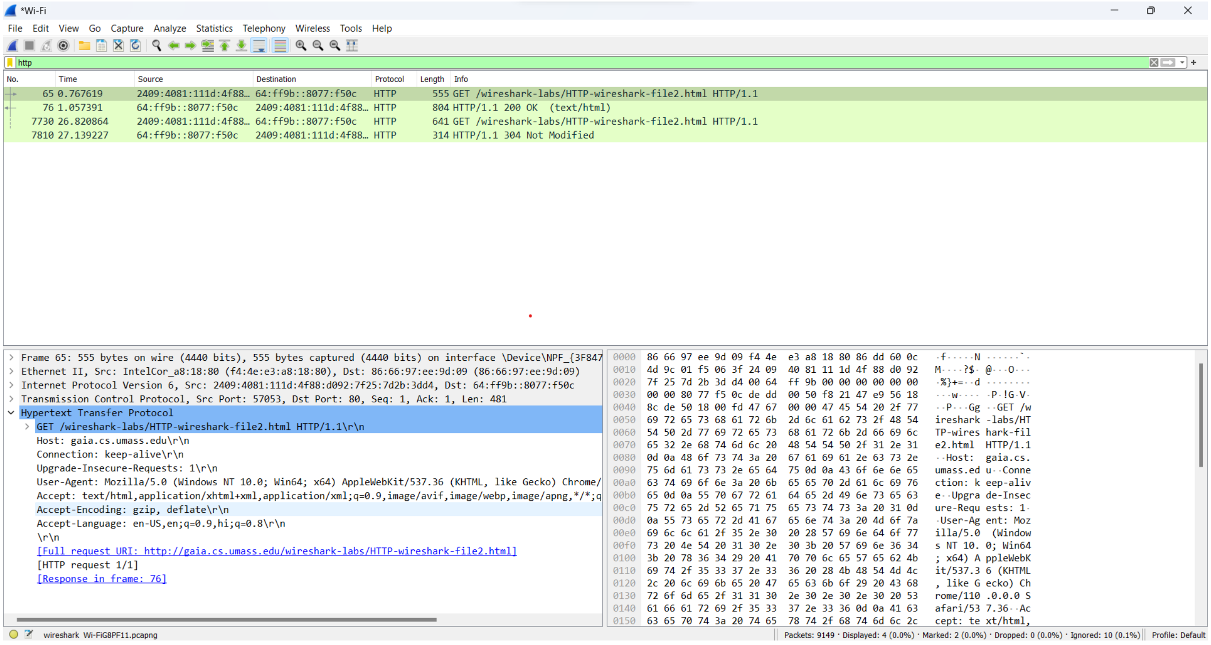
```
No.   Time        Source                Destination           Protocol Length Info
 1928 72.848339   2409:4081:111d:4f88…  64:ff9b::d7e:784c     HTTP      931 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 2002 72.915106   64:ff9b::d7e:784c     2409:4081:111d:4f88…  HTTP      598 HTTP/1.1 200 OK  (text/plain)
 2936 79.242703   2409:4081:111d:4f88…  64:ff9b::8077:f50c    HTTP      555 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 2946 79.537152   64:ff9b::8077:f50c    2409:4081:111d:4f88…  HTTP      560 HTTP/1.1 200 OK  (text/html)
 3846 108.686122  2a03:2880:f22f:c6:f…  2409:4081:111d:4f88…  TCP      1444 80 → 52821 [ACK] Seq=4258 Ack=897 Win=67840 Len=1370
 4567 195.082031  2409:4081:111d:4f88…  64:ff9b::d7e:784c     HTTP      943 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 4569 195.145033  64:ff9b::d7e:784c     2409:4081:111d:4f88…  HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5244 297.844714  2409:4081:111d:4f88…  64:ff9b::d7f:7b0e     HTTP     1039 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5245 297.844721  2409:4081:111d:4f88…  64:ff9b::d7f:7b0e     HTTP     1039 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5251 297.922935  64:ff9b::d7f:7b0e     2409:4081:111d:4f88…  HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5252 297.923940  64:ff9b::d7f:7b0e     2409:4081:111d:4f88…  HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5258 297.940411  2409:4081:111d:4f88…  64:ff9b::d7f:7b0e     HTTP     1039 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5264 298.004941  64:ff9b::d7f:7b0e     2409:4081:111d:4f88…  HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5858 325.278796  2409:4081:111d:4f88…  64:ff9b::d7f:7b0e     HTTP      975 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5860 325.403385  64:ff9b::d7f:7b0e     2409:4081:111d:4f88…  HTTP      598 HTTP/1.1 200 OK  (text/plain)
 5958 336.518573  2409:4081:111d:4f88…  64:ff9b::d7f:7b0e     HTTP      931 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5961 336.524723  2409:4081:111d:4f88…  64:ff9b::d7f:7b0e     HTTP      955 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5962 336.537005  2409:4081:111d:4f88…  64:ff9b::d7f:7b0e     HTTP      995 POST /qhcloudsec/lookup/file/scan HTTP/1.1  (text/plain)
 5965 336.586693  64:ff9b::d7f:7b0e     2409:4081:111d:4f88…  HTTP      598 HTTP/1.1 200 OK  (text/plain)
```

```
  > [SEQ/ACK analysis]
    TCP payload (481 bytes)
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,hi;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 2946]
```

```
00e0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
00f0  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0100  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
0110  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
0120  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
0130  72 6f 6d 65 2f 31 31 30  2e 30 2e 30 2e 30 20 53   rome/110 .0.0.0 S
0140  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0150  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0160  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
0170  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0180  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0190  65 2f 61 76 69 66 2c 69  6d 61 67 65 2f 77 65 62   e/avif,i mage/web
01a0  70 2c 69 6d 61 67 65 2f  61 70 6e 67 2c 2a 2f 2a   p,image/ apng,*/*
01b0  3b 71 3d 30 2e 38 2c 61  70 70 6c 69 63 61 74 69   ;q=0.8,a pplicati
01c0  6f 6e 2f 73 69 67 6e 65  64 2d 65 78 63 68 61 6e   on/signe d-exchan
01d0  67 65 3b 76 3d 62 33 3b  71 3d 30 2e 37 0d 0a 41   ge;v=b3; q=0.7··A
01e0  63 63 65 70 74 2d 45 6e  63 6f 64 69 6e 67 3a 20   ccept-En coding: 
01f0  67 7a 69 70 2c 20 64 65  66 6c 61 74 65 0d 0a 41   gzip, de flate··A
0200  63 63 65 70 74 2d 4c 61  6e 67 75 61 67 65 3a 20   ccept-La nguage: 
0210  65 6e 2d 55 53 2c 65 6e  3b 71 3d 30 2e 39 2c 68   en-US,en ;q=0.9,h
0220  69 3b 71 3d 30 2e 38 0d  0a 0d 0a                  i;q=0.8· ···
```

HTTP Accept Language (http.accept_language), 42 bytes | Packets: 10130 · Displayed: 123 (1.2%) | Profile: Default

5. No, as the browser cache was just cleared, there is no “IF-MODIFIED-SINCE” line in the HTTP GET.


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

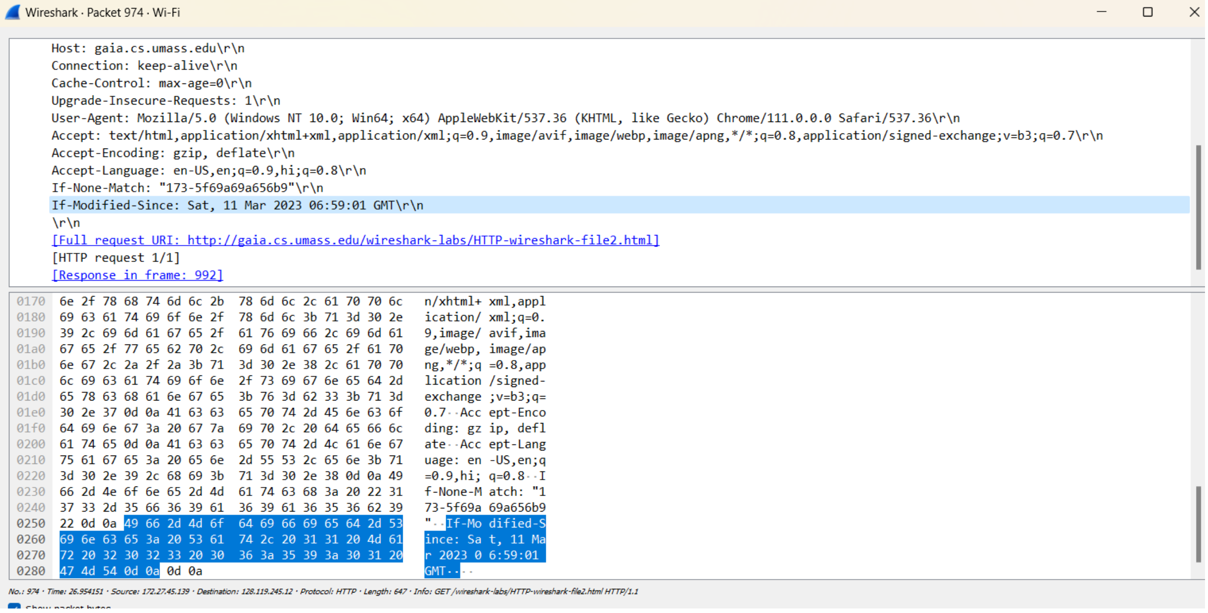
```
No.   Time        Source                Destination           Protocol Length Info
   65 0.767619    2409:4081:111d:4f88…  64:ff9b::8077:f50c    HTTP      555 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   76 1.057391    64:ff9b::8077:f50c    2409:4081:111d:4f88…  HTTP      804 HTTP/1.1 200 OK  (text/html)
 7730 26.820864   2409:4081:111d:4f88…  64:ff9b::8077:f50c    HTTP      641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 7810 27.139227   64:ff9b::8077:f50c    2409:4081:111d:4f88…  HTTP      314 HTTP/1.1 304 Not Modified
```

```
> Frame 65: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface \Device\NPF_{3F847
> Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
> Internet Protocol Version 6, Src: 2409:4081:111d:4f88:d092:7f25:7d2b:3dd4, Dst: 64:ff9b::8077:f50c
> Transmission Control Protocol, Src Port: 57053, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,hi;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 76]
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 86 dd 60 0c   ·f·····N ······`·
0010  4d 9c 01 f5 06 3f 24 09  40 81 11 1d 4f 88 d0 92   M····?$· @···O···
0020  7f 25 7d 2b 3d d4 00 64  ff 9b 00 00 00 00 00 00   ·%}+=··d ········
0030  00 00 80 77 f5 0c de dd  00 50 f8 21 47 e9 56 18   ···w···· ·P·!G·V·
0040  8c de 50 18 00 fd 47 67  00 00 47 45 54 20 2f 77   ··P···Gg ··GET /w
0050  69 72 65 73 68 61 72 6b  2d 6c 61 62 73 2f 48 54   ireshark -labs/HT
0060  54 50 2d 77 69 72 65 73  68 61 72 6b 2d 66 69 6c   TP-wires hark-fil
0070  65 32 2e 68 74 6d 6c 20  48 54 54 50 2f 31 2e 31   e2.html  HTTP/1.1
0080  0d 0a 48 6f 73 74 3a 20  67 61 69 61 2e 63 73 2e   ··Host:  gaia.cs.
0090  75 6d 61 73 73 2e 65 64  75 0d 0a 43 6f 6e 6e 65   umass.ed u··Conne
00a0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00b0  65 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   e··Upgra de-Insec
00c0  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
00d0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00e0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
00f0  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0100  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
0110  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
0120  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
0130  72 6f 6d 65 2f 31 31 30  2e 30 2e 30 2e 30 20 53   rome/110 .0.0.0 S
0140  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0150  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
```

wireshark Wi-FiG8PF11.pcapng | Packets: 9149 · Displayed: 4 (0.0%) · Marked: 2 (0.0%) · Dropped: 0 (0.0%) · Ignored: 10 (0.1%) | Profile: Default

IF-MODIFIED-SINCE” line in the HTTP GET after refreshing.

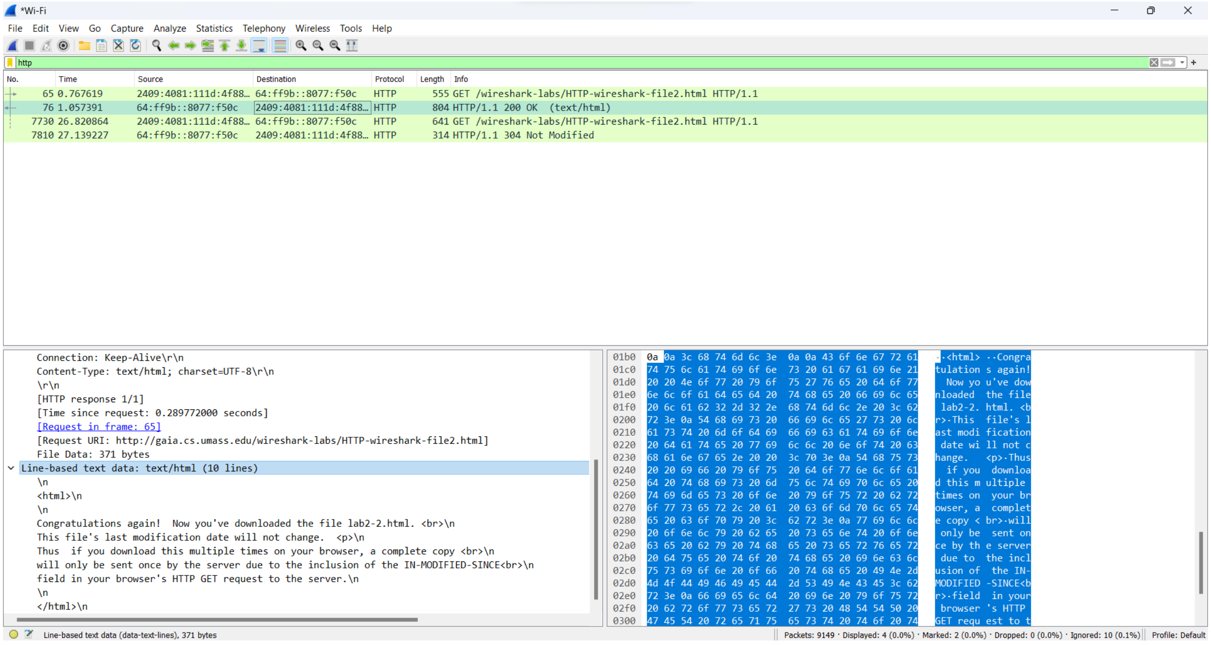


```
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,hi;q=0.8\r\n
    If-None-Match: "173-5f69a69a656b9"\r\n
    If-Modified-Since: Sat, 11 Mar 2023 06:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 992]
```

```
0170  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
0180  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
0190  39 2c 69 6d 61 67 65 2f  61 76 69 66 2c 69 6d 61   9,image/ avif,ima
01a0  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
01b0  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 2c 61 70 70   ng,*/*;q =0.8,app
01c0  6c 69 63 61 74 69 6f 6e  2f 73 69 67 6e 65 64 2d   lication /signed-
01d0  65 78 63 68 61 6e 67 65  3b 76 3d 62 33 3b 71 3d   exchange ;v=b3;q=
01e0  30 2e 37 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.7··Acc ept-Enco
01f0  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
0200  61 74 65 0d 0a 41 63 63  65 70 74 2d 4c 61 6e 67   ate··Acc ept-Lang
0210  75 61 67 65 3a 20 65 6e  2d 55 53 2c 65 6e 3b 71   uage: en -US,en;q
0220  3d 30 2e 39 2c 68 69 3b  71 3d 30 2e 38 0d 0a 49   =0.9,hi; q=0.8··I
0230  66 2d 4e 6f 6e 65 2d 4d  61 74 63 68 3a 20 22 31   f-None-M atch: "1
0240  37 33 2d 35 66 36 39 61  36 39 61 36 35 36 62 39   73-5f69a 69a656b9
0250  22 0d 0a 49 66 2d 4d 6f  64 69 66 69 65 64 2d 53   "··If-Mo dified-S
0260  69 6e 63 65 3a 20 53 61  74 2c 20 31 31 20 4d 61   ince: Sa t, 11 Ma
0270  72 20 32 30 32 33 20 30  36 3a 35 39 3a 30 31 20   r 2023 0 6:59:01 
0280  47 4d 54 0d 0a 0d 0a                               GMT····
```

No.: 974 · Time: 26.954151 · Source: 172.27.45.139 · Destination: 128.119.245.12 · Protocol: HTTP · Length: 647 · Info: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

6. Yes, the contents of the file were visible in the packet capture



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

```
No.   Time       Source                Destination           Protocol Length Info
   65 0.767619   2409:4081:111d:4f88…  64:ff9b::8077:f50c    HTTP      555 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   76 1.057391   64:ff9b::8077:f50c    2409:4081:111d:4f88…  HTTP      804 HTTP/1.1 200 OK  (text/html)
 7730 26.820864  2409:4081:111d:4f88…  64:ff9b::8077:f50c    HTTP      641 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 7810 27.139227  64:ff9b::8077:f50c    2409:4081:111d:4f88…  HTTP      314 HTTP/1.1 304 Not Modified
```

```
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.289772000 seconds]
    [Request in frame: 65]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
  Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

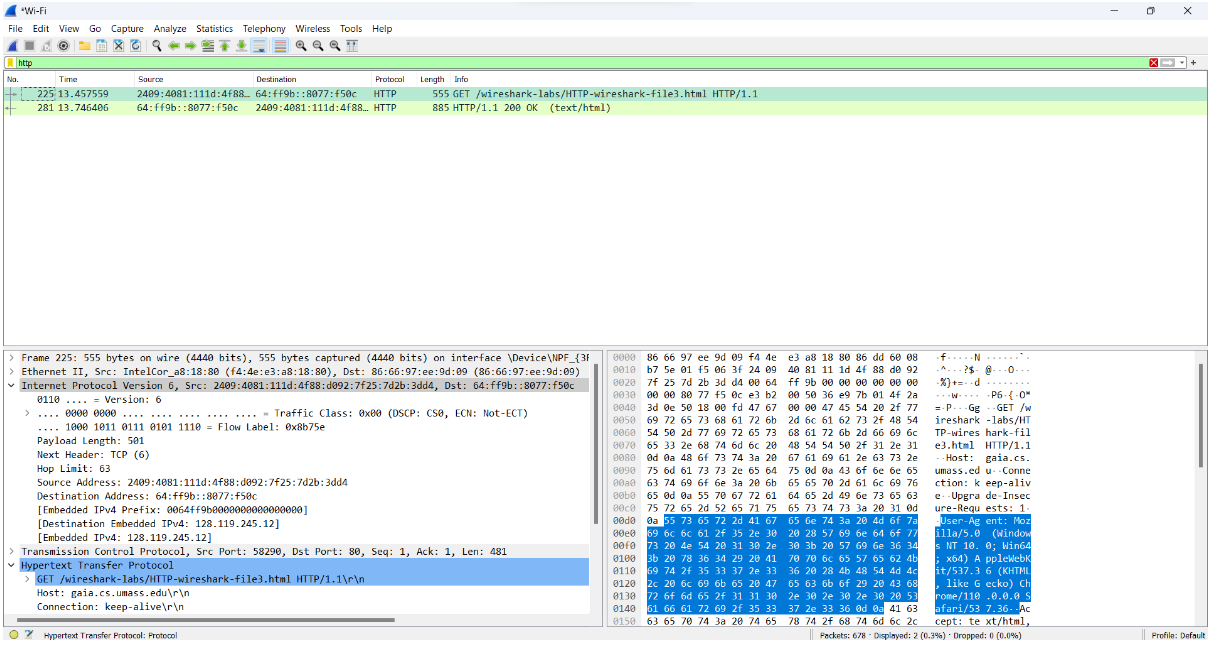
```
01b0  0a 0a 3c 68 74 6d 6c 3e  0a 0a 43 6f 6e 67 72 61   ··<html> ··Congra
01c0  74 75 6c 61 74 69 6f 6e  73 20 61 67 61 69 6e 21   tulation s again!
01d0  20 20 4e 6f 77 20 79 6f  75 27 76 65 20 64 6f 77     Now yo u've dow
01e0  6e 6c 6f 61 64 65 64 20  74 68 65 20 66 69 6c 65   nloaded  the file
01f0  20 6c 61 62 32 2d 32 2e  68 74 6d 6c 2e 20 3c 62    lab2-2. html. <b
0200  72 3e 0a 54 68 69 73 20  66 69 6c 65 27 73 20 6c   r>·This  file's l
0210  61 73 74 20 6d 6f 64 69  66 69 63 61 74 69 6f 6e   ast modi fication
0220  20 64 61 74 65 20 77 69  6c 6c 20 6e 6f 74 20 63    date wi ll not c
0230  68 61 6e 67 65 2e 20 20  3c 70 3e 0a 54 68 75 73   hange.   <p>·Thus
0240  20 20 69 66 20 79 6f 75  20 64 6f 77 6e 6c 6f 61     if you  downloa
0250  64 20 74 68 69 73 20 6d  75 6c 74 69 70 6c 65 20   d this m ultiple 
0260  74 69 6d 65 73 20 6f 6e  20 79 6f 75 72 20 62 72   times on  your br
0270  6f 77 73 65 72 2c 20 61  20 63 6f 6d 70 6c 65 74   owser, a  complet
0280  65 20 63 6f 70 79 20 3c  62 72 3e 0a 77 69 6c 6c   e copy < br>·will
0290  20 6f 6e 6c 79 20 62 65  20 73 65 6e 74 20 6f 6e    only be  sent on
02a0  63 65 20 62 79 20 74 68  65 20 73 65 72 76 65 72   ce by th e server
02b0  20 64 75 65 20 74 6f 20  74 68 65 20 69 6e 63 6c    due to  the incl
02c0  75 73 69 6f 6e 20 6f 66  20 74 68 65 20 49 4e 2d   usion of  the IN-
02d0  4d 4f 44 49 46 49 45 44  2d 53 49 4e 43 45 3c 62   MODIFIED -SINCE<b
02e0  72 3e 0a 66 69 65 6c 64  20 69 6e 20 79 6f 75 72   r>·field  in your
02f0  20 62 72 6f 77 73 65 72  27 73 20 48 54 54 50 20    browser 's HTTP 
0300  47 45 54 20 72 65 71 75  65 73 74 20 74 6f 20 74   GET requ est to t
```

Line-based text data (data-text-lines), 371 bytes

Packets: 9149 · Displayed: 4 (0.0%) · Marked: 2 (0.0%) · Dropped: 0 (0.0%) · Ignored: 10 (0.1%) | Profile: Default

Server didn’t explicitly return the contents of the file for the after refreshing as the earlier response got cached

7. My browser sent 1 GET request. The packet number is 225


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

http

```
No.   Time        Source                Destination          Protocol  Length  Info
  225 13.457559   2409:4081:111d:4f88…  64:ff9b::8077:f50c   HTTP         555  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  281 13.746406   64:ff9b::8077:f50c    2409:4081:111d:4f88… HTTP         885  HTTP/1.1 200 OK  (text/html)
```

```
> Frame 225: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface \Device\NPF_{3F
> Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
v Internet Protocol Version 6, Src: 2409:4081:111d:4f88:d092:7f25:7d2b:3dd4, Dst: 64:ff9b::8077:f50c
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1000 1011 0111 0101 1110 = Flow Label: 0x8b75e
    Payload Length: 501
    Next Header: TCP (6)
    Hop Limit: 63
    Source Address: 2409:4081:111d:4f88:d092:7f25:7d2b:3dd4
    Destination Address: 64:ff9b::8077:f50c
    [Embedded IPv4 Prefix: 0064ff9b0000000000000000]
    [Destination Embedded IPv4: 128.119.245.12]
    [Embedded IPv4: 128.119.245.12]
> Transmission Control Protocol, Src Port: 58290, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 86 dd 60 08   ·f·····N ······`·
0010  b7 5e 01 f5 06 3f 24 09  40 81 11 1d 4f 88 d0 92   ·^···?$· @···O···
0020  7f 25 7d 2b 3d d4 00 64  ff 9b 00 00 00 00 00 00   ·%}+=··d ········
0030  00 00 80 77 f5 0c e3 b2  00 50 36 e9 7b 01 4f 2a   ···w···· ·P6·{·O*
0040  3d 0e 50 18 00 fd 47 67  00 00 47 45 54 20 2f 77   =·P···Gg ··GET /w
0050  69 72 65 73 68 61 72 6b  2d 6c 61 62 73 2f 48 54   ireshark -labs/HT
0060  54 50 2d 77 69 72 65 73  68 61 72 6b 2d 66 69 6c   TP-wires hark-fil
0070  65 33 2e 68 74 6d 6c 20  48 54 54 50 2f 31 2e 31   e3.html  HTTP/1.1
0080  0d 0a 48 6f 73 74 3a 20  67 61 69 61 2e 63 73 2e   ··Host:  gaia.cs.
0090  75 6d 61 73 73 2e 65 64  75 0d 0a 43 6f 6e 6e 65   umass.ed u··Conne
00a0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00b0  65 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   e··Upgra de-Insec
00c0  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
00d0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00e0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
00f0  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0100  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
0110  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
0120  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
0130  72 6f 6d 65 2f 31 31 30  2e 30 2e 30 2e 30 20 53   rome/110 .0.0.0 S
0140  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0150  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
```

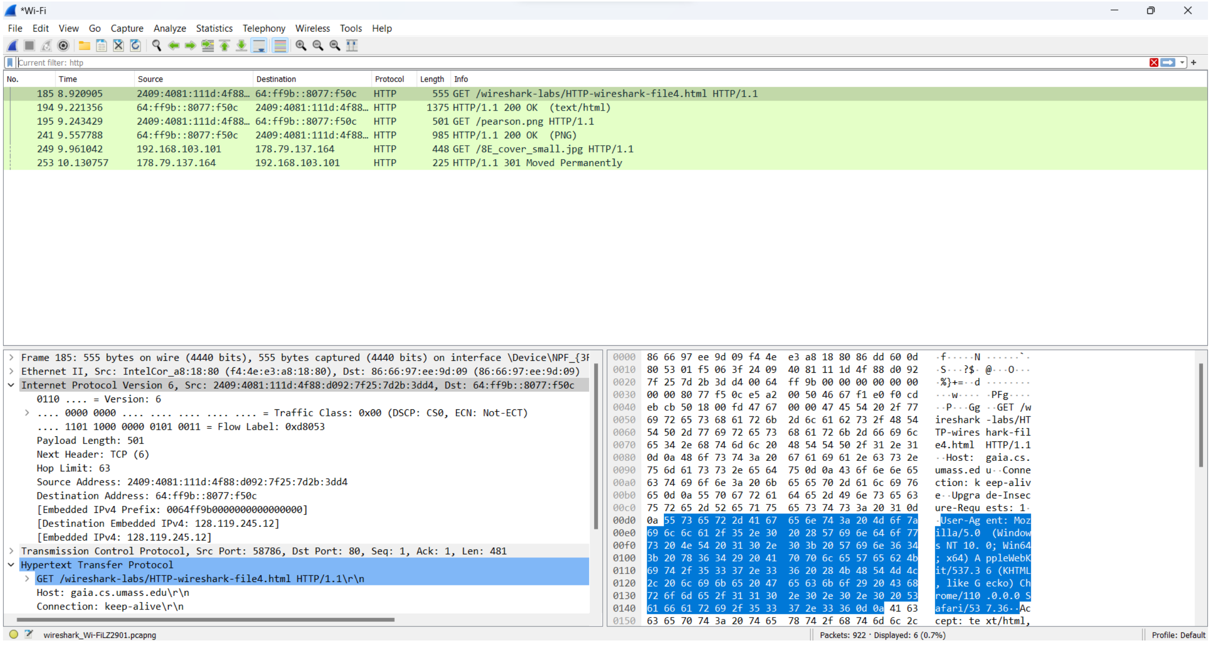
Hypertext Transfer Protocol: Protocol

Packets: 678 · Displayed: 2 (0.3%) · Dropped: 0 (0.0%)

Profile: Default

8. The response is in packet number 281

9. My browser sent 3 GET requests to 64:ff9b::8077:f50c , 64:ff9b::8077:f50c , 178.79.137.164


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

Current filter: http

```
No.   Time        Source                Destination          Protocol  Length  Info
  185 8.920905    2409:4081:111d:4f88…  64:ff9b::8077:f50c   HTTP         555  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  194 9.221356    64:ff9b::8077:f50c    2409:4081:111d:4f88… HTTP        1375  HTTP/1.1 200 OK  (text/html)
  195 9.243429    2409:4081:111d:4f88…  64:ff9b::8077:f50c   HTTP         501  GET /pearson.png HTTP/1.1
  241 9.557788    64:ff9b::8077:f50c    2409:4081:111d:4f88… HTTP         985  HTTP/1.1 200 OK  (PNG)
  249 9.961042    192.168.103.101       178.79.137.164       HTTP         448  GET /8E_cover_small.jpg HTTP/1.1
  253 10.130757   178.79.137.164        192.168.103.101      HTTP         225  HTTP/1.1 301 Moved Permanently
```

```
> Frame 185: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface \Device\NPF_{3F
> Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
v Internet Protocol Version 6, Src: 2409:4081:111d:4f88:d092:7f25:7d2b:3dd4, Dst: 64:ff9b::8077:f50c
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1101 1000 0000 0101 0011 = Flow Label: 0xd8053
    Payload Length: 501
    Next Header: TCP (6)
    Hop Limit: 63
    Source Address: 2409:4081:111d:4f88:d092:7f25:7d2b:3dd4
    Destination Address: 64:ff9b::8077:f50c
    [Embedded IPv4 Prefix: 0064ff9b0000000000000000]
    [Destination Embedded IPv4: 128.119.245.12]
    [Embedded IPv4: 128.119.245.12]
> Transmission Control Protocol, Src Port: 58786, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 86 dd 60 0d   ·f·····N ······`·
0010  80 53 01 f5 06 3f 24 09  40 81 11 1d 4f 88 d0 92   ·S···?$· @···O···
0020  7f 25 7d 2b 3d d4 00 64  ff 9b 00 00 00 00 00 00   ·%}+=··d ········
0030  00 00 80 77 f5 0c e5 a2  00 50 46 67 f1 e0 f0 cd   ···w···· ·PFg····
0040  eb cb 50 18 00 fd 47 67  00 00 47 45 54 20 2f 77   ··P···Gg ··GET /w
0050  69 72 65 73 68 61 72 6b  2d 6c 61 62 73 2f 48 54   ireshark -labs/HT
0060  54 50 2d 77 69 72 65 73  68 61 72 6b 2d 66 69 6c   TP-wires hark-fil
0070  65 34 2e 68 74 6d 6c 20  48 54 54 50 2f 31 2e 31   e4.html  HTTP/1.1
0080  0d 0a 48 6f 73 74 3a 20  67 61 69 61 2e 63 73 2e   ··Host:  gaia.cs.
0090  75 6d 61 73 73 2e 65 64  75 0d 0a 43 6f 6e 6e 65   umass.ed u··Conne
00a0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00b0  65 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   e··Upgra de-Insec
00c0  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
00d0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00e0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
00f0  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0100  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
0110  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
0120  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
0130  72 6f 6d 65 2f 31 31 30  2e 30 2e 30 2e 30 20 53   rome/110 .0.0.0 S
0140  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0150  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
```

wireshark_Wi-FiLZ2901.pcapng

Packets: 922 · Displayed: 6 (0.7%)

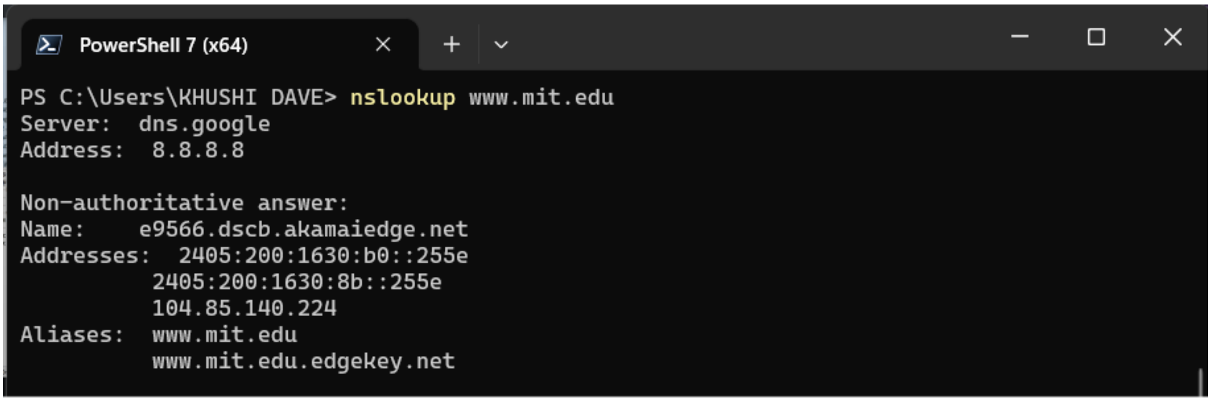
Profile: Default

10. The browser downloaded the two images in serially. I believe this to be the case because the first image was requested and sent before the second image was requested by the browser. Had they been running in parallel, both files would have been

requested then would have returned in the same time period. In this case however, the second image was only requested after the first image came back.

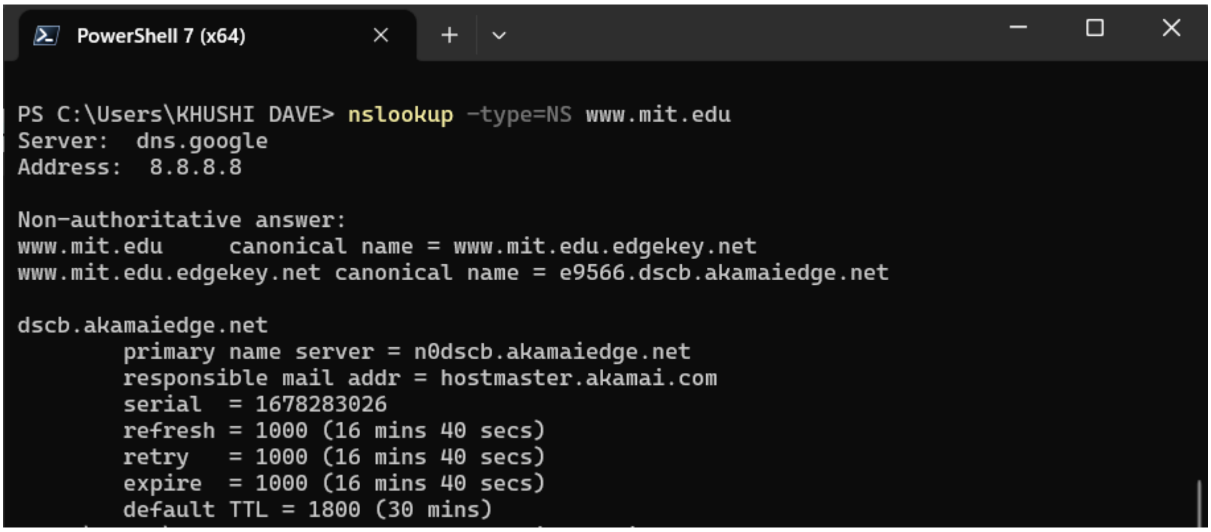
DNS

1. The default DNS server is dns.google with IP address 8.8.8.8



```
PS C:\Users\KHUSHI DAVE> nslookup www.mit.edu
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    e9566.dscb.akamaiedge.net
Addresses:  2405:200:1630:b0::255e
          2405:200:1630:8b::255e
          104.85.140.224
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

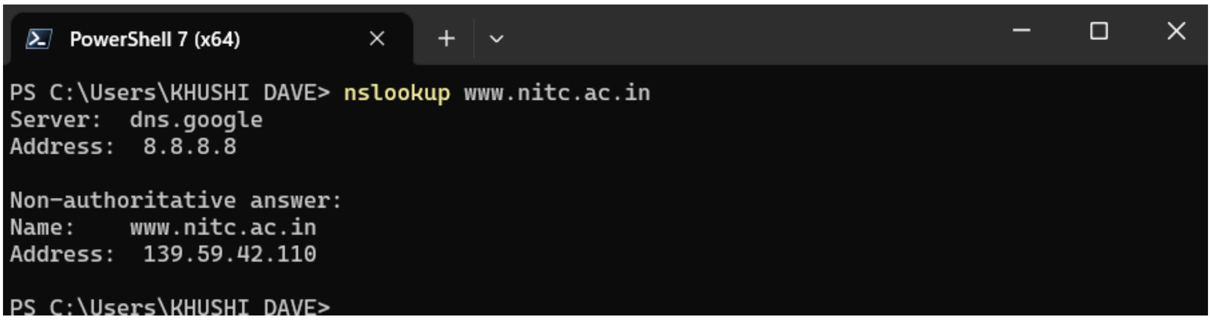
2. n0dscb.akamaiedge.net



```
PS C:\Users\KHUSHI DAVE> nslookup -type=NS www.mit.edu
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net

dscb.akamaiedge.net
        primary name server = n0dscb.akamaiedge.net
        responsible mail addr = hostmaster.akamai.com
        serial  = 1678283026
        refresh = 1000 (16 mins 40 secs)
        retry   = 1000 (16 mins 40 secs)
        expire  = 1000 (16 mins 40 secs)
        default TTL = 1800 (30 mins)
```

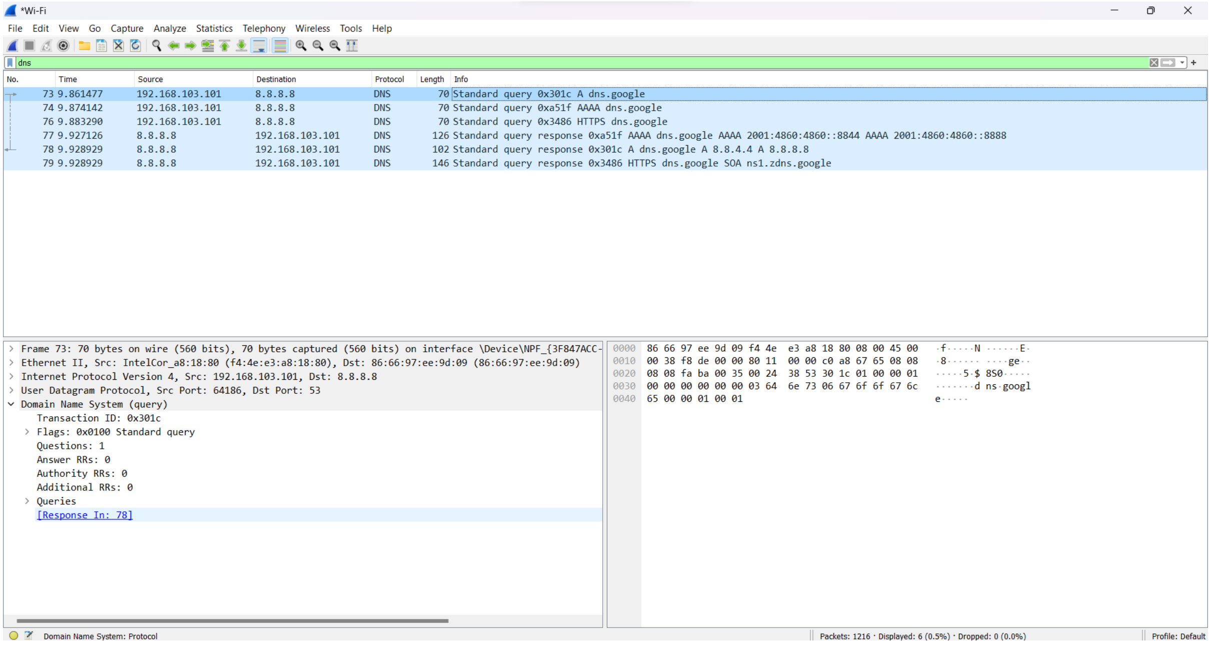
3. I queried the webpage for NIT Calicut

The IP address of that server was 139.59.42.110



```
PS C:\Users\KHUSHI DAVE> nslookup www.nitc.ac.in
Server:   dns.google
Address:   8.8.8.8

Non-authoritative answer:
Name:     www.nitc.ac.in
Address:   139.59.42.110

PS C:\Users\KHUSHI DAVE>
```

4. 4. The DNS query and response messages are sent over UDP



dns

```
No.     Time         Source            Destination       Protocol  Length Info
     73 9.861477     192.168.103.101   8.8.8.8           DNS           70 Standard query 0x301c A dns.google
     74 9.874142     192.168.103.101   8.8.8.8           DNS           70 Standard query 0xa51f AAAA dns.google
     76 9.883290     192.168.103.101   8.8.8.8           DNS           70 Standard query 0x3486 HTTPS dns.google
     77 9.927126     8.8.8.8           192.168.103.101   DNS          126 Standard query response 0xa51f AAAA dns.google AAAA 2001:4860:4860::8844 AAAA 2001:4860:4860::8888
     78 9.928929     8.8.8.8           192.168.103.101   DNS          102 Standard query response 0x301c A dns.google A 8.8.4.4 A 8.8.8.8
     79 9.928929     8.8.8.8           192.168.103.101   DNS          146 Standard query response 0x3486 HTTPS dns.google SOA ns1.zdns.google
```

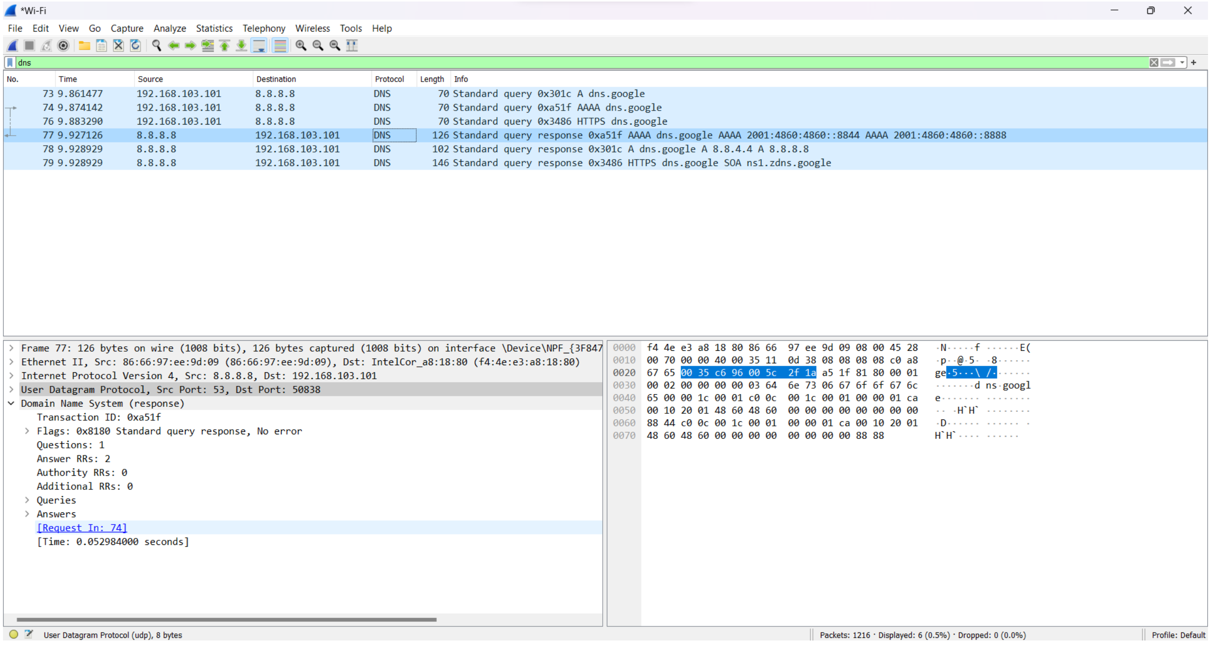
```
> Frame 73: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{3F847ACC-
> Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
> Internet Protocol Version 4, Src: 192.168.103.101, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 64186, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x301c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 78]
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 08 00 45 00   ·f·····N ······E·
0010  00 38 f8 de 00 00 80 11  00 00 c0 a8 67 65 08 08   ·8······ ····ge··
0020  08 08 fa ba 00 35 00 24  38 53 30 1c 01 00 00 01   ·····5·$ 8S0·····
0030  00 00 00 00 00 00 03 64  6e 73 06 67 6f 6f 67 6c   ·······d ns·googl
0040  65 00 00 01 00 01                                  e·····
```

Domain Name System: Protocol

Packets: 1216 · Displayed: 6 (0.5%) · Dropped: 0 (0.0%)

Profile: Default



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

```
dns
```

```
No.   Time      Source           Destination      Protocol Length Info
   73 9.861477  192.168.103.101  8.8.8.8          DNS       70 Standard query 0x301c A dns.google
   74 9.874142  192.168.103.101  8.8.8.8          DNS       70 Standard query 0xa51f AAAA dns.google
   76 9.883290  192.168.103.101  8.8.8.8          DNS       70 Standard query 0x3486 HTTPS dns.google
   77 9.927126  8.8.8.8          192.168.103.101  DNS      126 Standard query response 0xa51f AAAA dns.google AAAA 2001:4860:4860::8844 AAAA 2001:4860:4860::8888
   78 9.928929  8.8.8.8          192.168.103.101  DNS      102 Standard query response 0x301c A dns.google A 8.8.4.4 A 8.8.8.8
   79 9.928929  8.8.8.8          192.168.103.101  DNS      146 Standard query response 0x3486 HTTPS dns.google SOA ns1.zdns.google
```

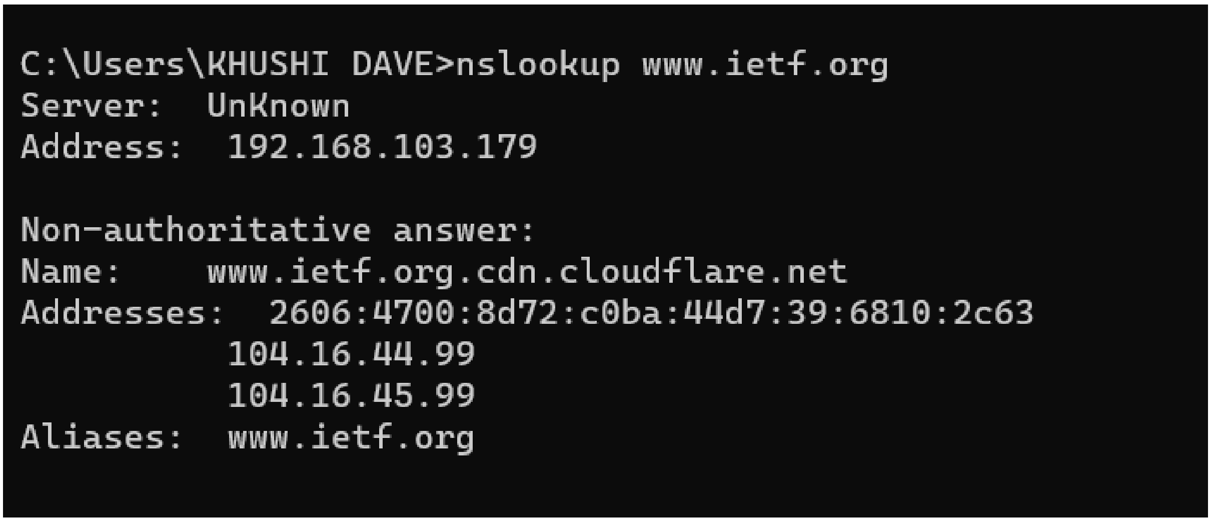
```
> Frame 77: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{3F847
> Ethernet II, Src: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09), Dst: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.103.101
> User Datagram Protocol, Src Port: 53, Dst Port: 50838
v Domain Name System (response)
    Transaction ID: 0xa51f
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 74]
    [Time: 0.052984000 seconds]
```

```
0000  f4 4e e3 a8 18 80 86 66  97 ee 9d 09 08 00 45 28   ·N·····f ······E(
0010  00 70 00 00 40 00 35 11  0d 38 08 08 08 08 c0 a8   ·p··@·5· ·8······
0020  67 65 00 35 c6 96 00 5c  2f 1a a5 1f 81 80 00 01   ge·5···\ /·······
0030  00 02 00 00 00 00 03 64  6e 73 06 67 6f 6f 67 6c   ·······d ns·googl
0040  65 00 00 1c 00 01 c0 0c  00 1c 00 01 00 00 01 ca   e······· ········
0050  00 10 20 01 48 60 48 60  00 00 00 00 00 00 00 00   ·· ·H`H` ········
0060  88 44 c0 0c 00 1c 00 01  00 00 01 ca 00 10 20 01   ·D······ ······ ·
0070  48 60 48 60 00 00 00 00  00 00 00 00 88 88         H`H`···· ······
```

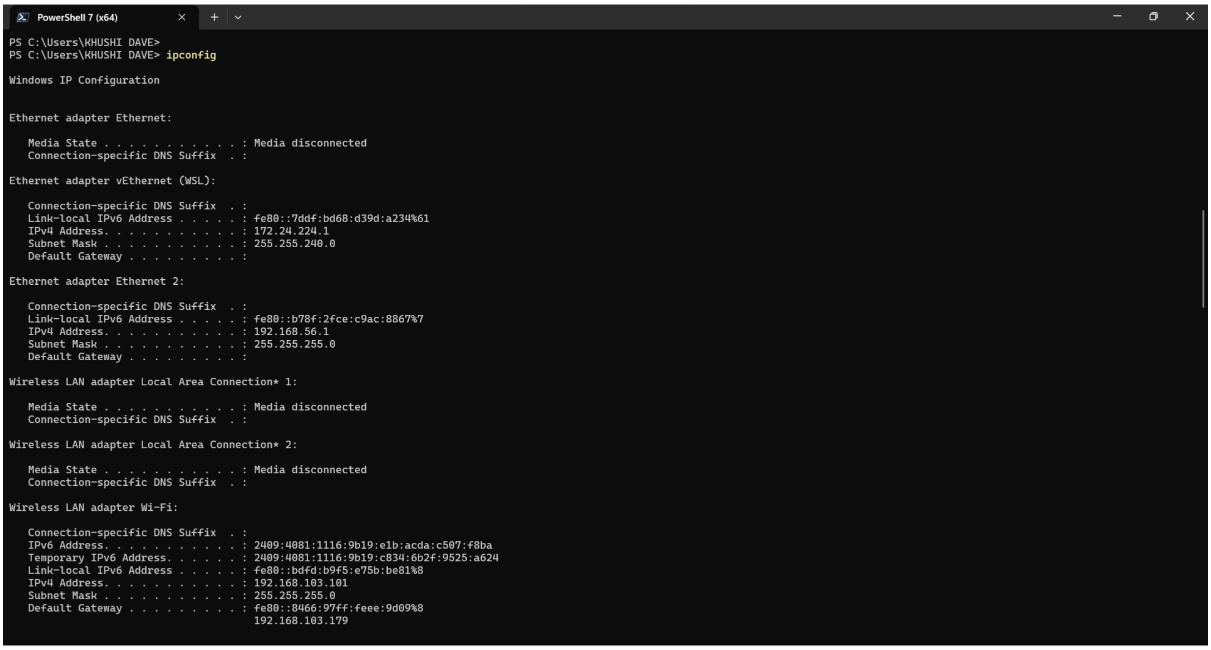
User Datagram Protocol (udp), 8 bytes | Packets: 1216 · Displayed: 6 (0.5%) · Dropped: 0 (0.0%) | Profile: Default

5. The destination port in the DNS query and the source port in the response is 53

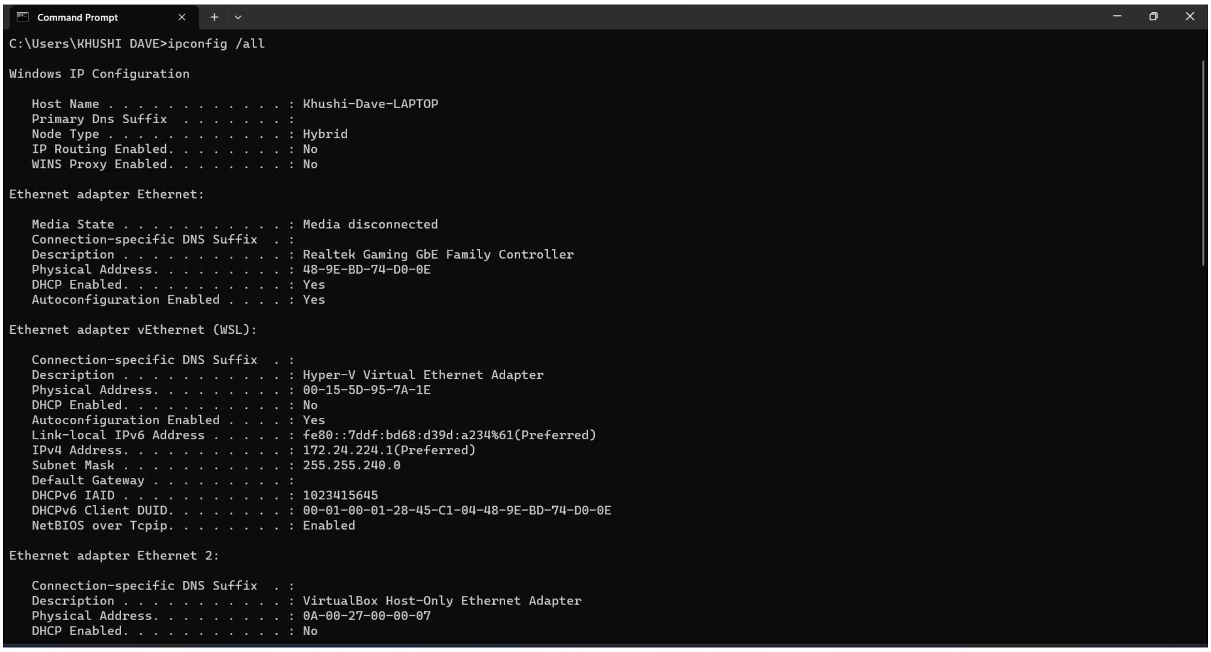
6. The DNS query message was sent to IP address 192.168.103.179 which is the same IP obtained using ipconfig



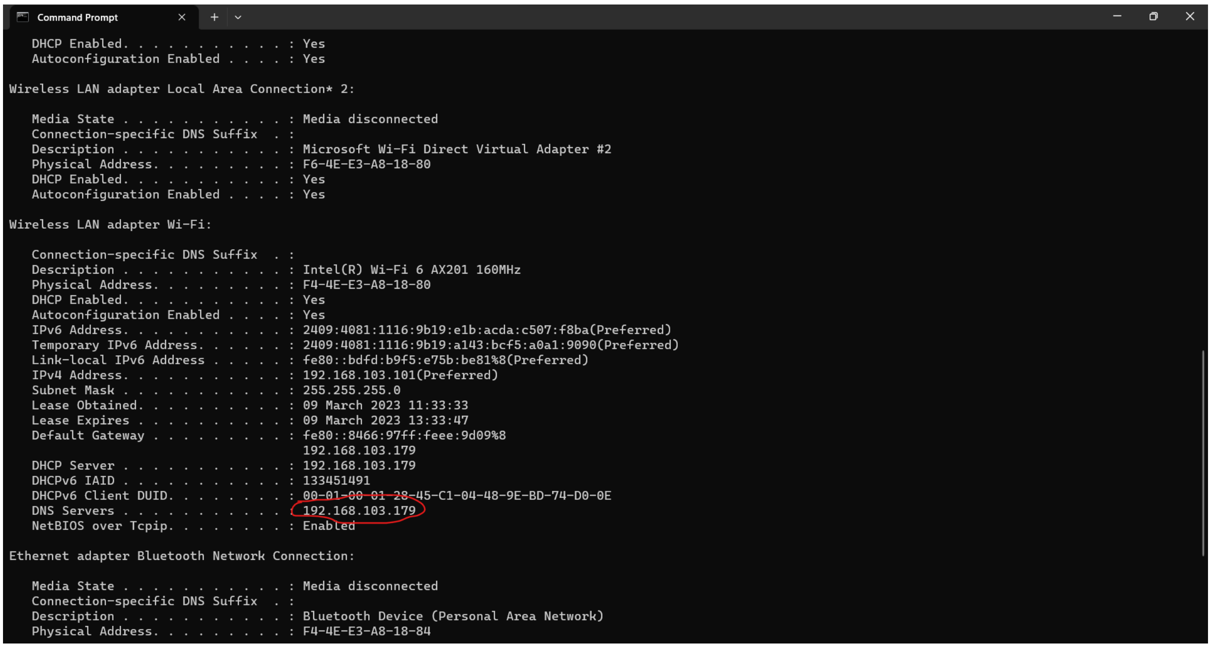
```
C:\Users\KHUSHI DAVE>nslookup www.ietf.org
Server:  UnKnown
Address:  192.168.103.179

Non-authoritative answer:
Name:    www.ietf.org.cdn.cloudflare.net
Addresses:  2606:4700:8d72:c0ba:44d7:39:6810:2c63
          104.16.44.99
          104.16.45.99
Aliases:  www.ietf.org
```



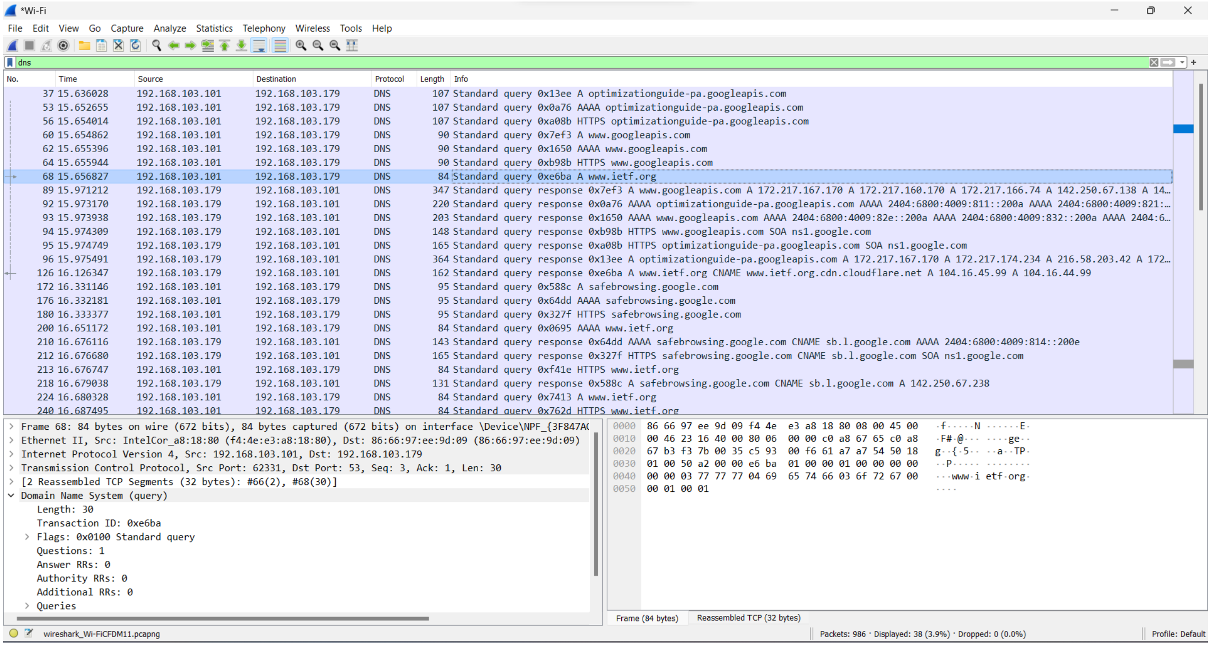
```
PS C:\Users\KHUSHI DAVE>
PS C:\Users\KHUSHI DAVE> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7ddf:bd68:d39d:a234%61
   IPv4 Address. . . . . . . . . . . : 172.24.224.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b78f:2fce:c9ac:8867%7
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4081:1116:9b19:e1b:acda:c507:f8ba
   Temporary IPv6 Address. . . . . . : 2409:4081:1116:9b19:c834:6b2f:9525:a624
   Link-local IPv6 Address . . . . . : fe80::bdfd:b9f5:e75b:be81%8
   IPv4 Address. . . . . . . . . . . : 192.168.103.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::8466:97ff:feee:9d09%8
                                       192.168.103.179
```



```
C:\Users\KHUSHI DAVE>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Khushi-Dave-LAPTOP
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek Gaming GbE Family Controller
   Physical Address. . . . . . . . . : 48-9E-BD-74-D0-0E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter
   Physical Address. . . . . . . . . : 00-15-5D-95-7A-1E
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7ddf:bd68:d39d:a234%61(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.24.224.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 1023415645
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-45-C1-04-48-9E-BD-74-D0-0E
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-07
   DHCP Enabled. . . . . . . . . . . : No
```



```
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : F6-4E-E3-A8-18-80
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : F4-4E-E3-A8-18-80
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2409:4081:1116:9b19:e1b:acda:c507:f8ba(Preferred)
   Temporary IPv6 Address. . . . . . : 2409:4081:1116:9b19:a143:bcf5:a0a1:9090(Preferred)
   Link-local IPv6 Address . . . . . : fe80::bdfd:b9f5:e75b:be81%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.103.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 09 March 2023 11:33:33
   Lease Expires . . . . . . . . . . : 09 March 2023 13:33:47
   Default Gateway . . . . . . . . . : fe80::8466:97ff:feee:9d09%8
                                       192.168.103.179
   DHCP Server . . . . . . . . . . . : 192.168.103.179
   DHCPv6 IAID . . . . . . . . . . . : 133451491
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-45-C1-04-48-9E-BD-74-D0-0E
   DNS Servers . . . . . . . . . . . : 192.168.103.179
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : F4-4E-E3-A8-18-84
```


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

```
No.     Time       Source           Destination      Protocol Length Info
     37 15.636028  192.168.103.101  192.168.103.179  DNS       107 Standard query 0x13ee A optimizationguide-pa.googleapis.com
     53 15.652655  192.168.103.101  192.168.103.179  DNS       107 Standard query 0x0a76 AAAA optimizationguide-pa.googleapis.com
     56 15.654014  192.168.103.101  192.168.103.179  DNS       107 Standard query 0xa08b HTTPS optimizationguide-pa.googleapis.com
     60 15.654862  192.168.103.101  192.168.103.179  DNS        90 Standard query 0x7ef3 A www.googleapis.com
     62 15.655396  192.168.103.101  192.168.103.179  DNS        90 Standard query 0x1650 AAAA www.googleapis.com
     64 15.655944  192.168.103.101  192.168.103.179  DNS        90 Standard query 0xb98b HTTPS www.googleapis.com
     68 15.656827  192.168.103.101  192.168.103.179  DNS        84 Standard query 0xe6ba A www.ietf.org
     89 15.971212  192.168.103.179  192.168.103.101  DNS       347 Standard query response 0x7ef3 A www.googleapis.com A 172.217.167.170 A 172.217.160.170 A 172.217.166.74 A 142.250.67.138 A 14…
     92 15.973170  192.168.103.179  192.168.103.101  DNS       220 Standard query response 0x0a76 AAAA optimizationguide-pa.googleapis.com AAAA 2404:6800:4009:811::200a AAAA 2404:6800:4009:821:…
     93 15.973938  192.168.103.179  192.168.103.101  DNS       203 Standard query response 0x1650 AAAA www.googleapis.com AAAA 2404:6800:4009:82e::200a AAAA 2404:6800:4009:832::200a AAAA 2404:6…
     94 15.974309  192.168.103.179  192.168.103.101  DNS       148 Standard query response 0xb98b HTTPS www.googleapis.com SOA ns1.google.com
     95 15.974749  192.168.103.179  192.168.103.101  DNS       165 Standard query response 0xa08b HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
     96 15.975491  192.168.103.179  192.168.103.101  DNS       364 Standard query response 0x13ee A optimizationguide-pa.googleapis.com A 172.217.167.170 A 172.217.174.234 A 216.58.203.42 A 172…
    126 16.126347  192.168.103.179  192.168.103.101  DNS       162 Standard query response 0xe6ba A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
    172 16.331146  192.168.103.101  192.168.103.179  DNS        95 Standard query 0x588c A safebrowsing.google.com
    176 16.332181  192.168.103.101  192.168.103.179  DNS        95 Standard query 0x64dd AAAA safebrowsing.google.com
    180 16.333377  192.168.103.101  192.168.103.179  DNS        95 Standard query 0x327f HTTPS safebrowsing.google.com
    200 16.651172  192.168.103.101  192.168.103.179  DNS        84 Standard query 0x0695 AAAA www.ietf.org
    210 16.676116  192.168.103.179  192.168.103.101  DNS       143 Standard query response 0x64dd AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2404:6800:4009:814::200e
    212 16.676680  192.168.103.179  192.168.103.101  DNS       165 Standard query response 0x327f HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
    213 16.676747  192.168.103.101  192.168.103.179  DNS        84 Standard query 0xf41e HTTPS www.ietf.org
    218 16.679038  192.168.103.179  192.168.103.101  DNS       131 Standard query response 0x588c A safebrowsing.google.com CNAME sb.l.google.com A 142.250.67.238
    224 16.680328  192.168.103.101  192.168.103.179  DNS        84 Standard query 0x7413 A www.ietf.org
    240 16.687495  192.168.103.101  192.168.103.179  DNS        84 Standard query 0x762d HTTPS www.ietf.org
```

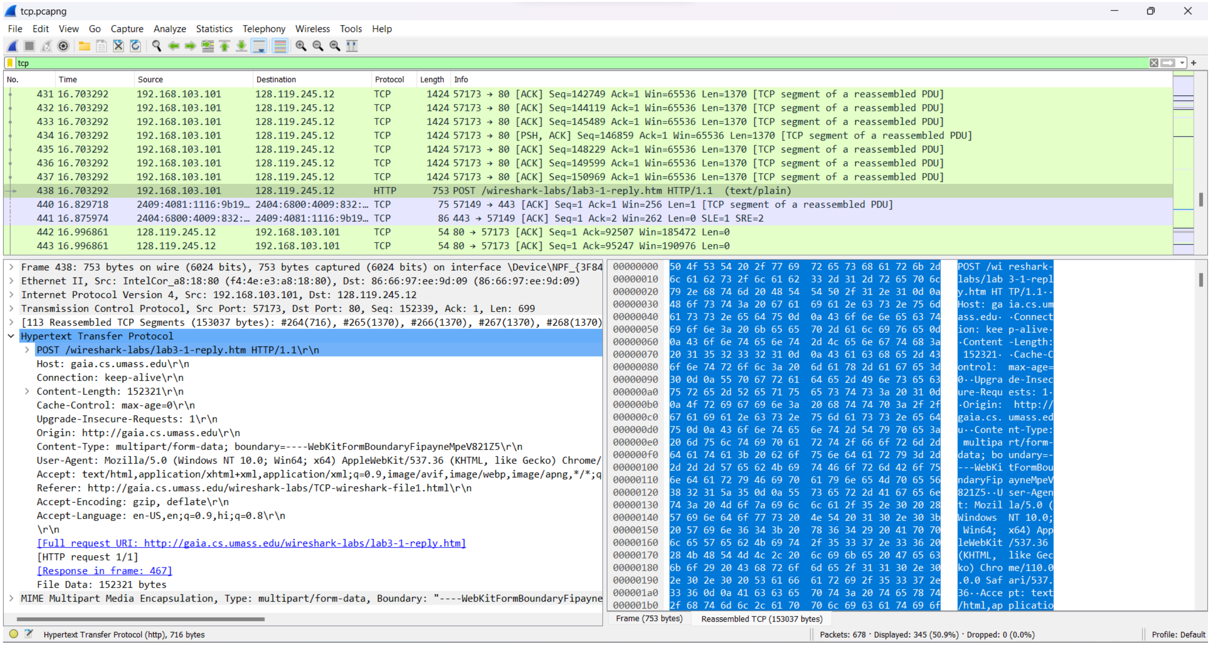
```
> Frame 68: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{3F847A(
> Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
> Internet Protocol Version 4, Src: 192.168.103.101, Dst: 192.168.103.179
> Transmission Control Protocol, Src Port: 62331, Dst Port: 53, Seq: 3, Ack: 1, Len: 30
> [2 Reassembled TCP Segments (32 bytes): #66(2), #68(30)]
v Domain Name System (query)
    Length: 30
    Transaction ID: 0xe6ba
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 08 00 45 00   ·f·····N ······E·
0010  00 46 23 16 40 00 80 06  00 00 c0 a8 67 65 c0 a8   ·F#·@··· ····ge··
0020  67 b3 f3 7b 00 35 c5 93  00 f6 61 a7 a7 54 50 18   g··{·5·· ··a··TP·
0030  01 00 50 a2 00 00 e6 ba  01 00 00 01 00 00 00 00   ··P····· ········
0040  00 00 03 77 77 77 04 69  65 74 66 03 6f 72 67 00   ···www·i etf·org·
0050  00 01 00 01                                        ····
```

Frame (84 bytes)
Reassembled TCP (32 bytes)
wireshark_Wi-FiCFDM11.pcapng
Packets: 986 · Displayed: 38 (3.9%) · Dropped: 0 (0.0%)
Profile: Default

TCP

1. The source (client) IP address is 192.168.103.101 and port number is 57173



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

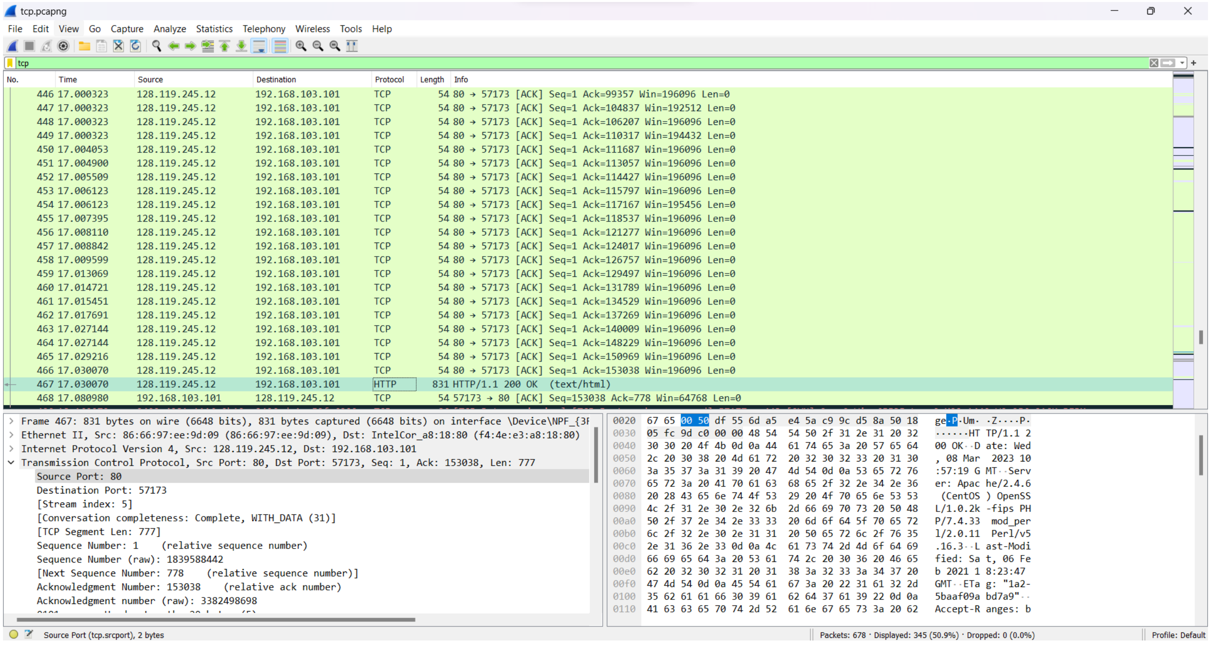
```
tcp
No.  Time       Source                Destination           Protocol Length Info
 431 16.703292  192.168.103.101       128.119.245.12        TCP      1424 57173 → 80 [ACK] Seq=142749 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 432 16.703292  192.168.103.101       128.119.245.12        TCP      1424 57173 → 80 [ACK] Seq=144119 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 433 16.703292  192.168.103.101       128.119.245.12        TCP      1424 57173 → 80 [ACK] Seq=145489 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 434 16.703292  192.168.103.101       128.119.245.12        TCP      1424 57173 → 80 [PSH, ACK] Seq=146859 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 435 16.703292  192.168.103.101       128.119.245.12        TCP      1424 57173 → 80 [ACK] Seq=148229 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 436 16.703292  192.168.103.101       128.119.245.12        TCP      1424 57173 → 80 [ACK] Seq=149599 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 437 16.703292  192.168.103.101       128.119.245.12        TCP      1424 57173 → 80 [ACK] Seq=150969 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 438 16.703292  192.168.103.101       128.119.245.12        HTTP      753 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
 440 16.829718  2409:4081:1116:9b19…  2404:6800:4009:832:…  TCP        75 57149 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
 441 16.875974  2404:6800:4009:832:…  2409:4081:1116:9b19…  TCP        86 443 → 57149 [ACK] Seq=1 Ack=2 Win=262 Len=0 SLE=1 SRE=2
 442 16.996861  128.119.245.12        192.168.103.101       TCP        54 80 → 57173 [ACK] Seq=1 Ack=92507 Win=185472 Len=0
 443 16.996861  128.119.245.12        192.168.103.101       TCP        54 80 → 57173 [ACK] Seq=1 Ack=95247 Win=190976 Len=0
```

```
> Frame 438: 753 bytes on wire (6024 bits), 753 bytes captured (6024 bits) on interface \Device\NPF_{3F84
> Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
> Internet Protocol Version 4, Src: 192.168.103.101, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 57173, Dst Port: 80, Seq: 152339, Ack: 1, Len: 699
> [113 Reassembled TCP Segments (153037 bytes): #264(716), #265(1370), #266(1370), #267(1370), #268(1370)
v Hypertext Transfer Protocol
  > POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
  > Content-Length: 152321\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Origin: http://gaia.cs.umass.edu\r\n
    Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFipayneMpeV821Z5\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
    Referer: http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,hi;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm]
    [HTTP request 1/1]
    [Response in frame: 467]
    File Data: 152321 bytes
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryFipayne
```

```
00000000  50 4f 53 54 20 2f 77 69  72 65 73 68 61 72 6b 2d   POST /wi reshark-
00000010  6c 61 62 73 2f 6c 61 62  33 2d 31 2d 72 65 70 6c   labs/lab 3-1-repl
00000020  79 2e 68 74 6d 20 48 54  54 50 2f 31 2e 31 0d 0a   y.htm HT TP/1.1··
00000030  48 6f 73 74 3a 20 67 61  69 61 2e 63 73 2e 75 6d   Host: ga ia.cs.um
00000040  61 73 73 2e 65 64 75 0d  0a 43 6f 6e 6e 65 63 74   ass.edu· ·Connect
00000050  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
00000060  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
00000070  20 31 35 32 33 32 31 0d  0a 43 61 63 68 65 2d 43    152321· ·Cache-C
00000080  6f 6e 74 72 6f 6c 3a 20  6d 61 78 2d 61 67 65 3d   ontrol:  max-age=
00000090  30 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   0··Upgra de-Insec
000000a0  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
000000b0  0a 4f 72 69 67 69 6e 3a  20 68 74 74 70 3a 2f 2f   ·Origin:  http://
000000c0  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
000000d0  75 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   u··Conte nt-Type:
000000e0  20 6d 75 6c 74 69 70 61  72 74 2f 66 6f 72 6d 2d    multipa rt/form-
000000f0  64 61 74 61 3b 20 62 6f  75 6e 64 61 72 79 3d 2d   data; bo undary=-
00000100  2d 2d 2d 57 65 62 4b 69  74 46 6f 72 6d 42 6f 75   ---WebKi tFormBou
00000110  6e 64 61 72 79 46 69 70  61 79 6e 65 4d 70 65 56   ndaryFip ayneMpeV
00000120  38 32 31 5a 35 0d 0a 55  73 65 72 2d 41 67 65 6e   821Z5··U ser-Agen
00000130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00000140  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
00000150  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;  x64) App
00000160  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36
00000170  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
00000180  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 31 30 2e 30   ko) Chro me/110.0
00000190  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
000001a0  33 36 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   36··Acce pt: text
000001b0  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
Frame (753 bytes)   Reassembled TCP (153037 bytes)
```

```
Hypertext Transfer Protocol (http), 716 bytes    Packets: 678 · Displayed: 345 (50.9%) · Dropped: 0 (0.0%)    Profile: Default
```

2. The IP address of gaia.cs.umass.edu is 128.119.245.12 (IPv4) It is sending to port 57173 (of client) and receiving over port 80



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

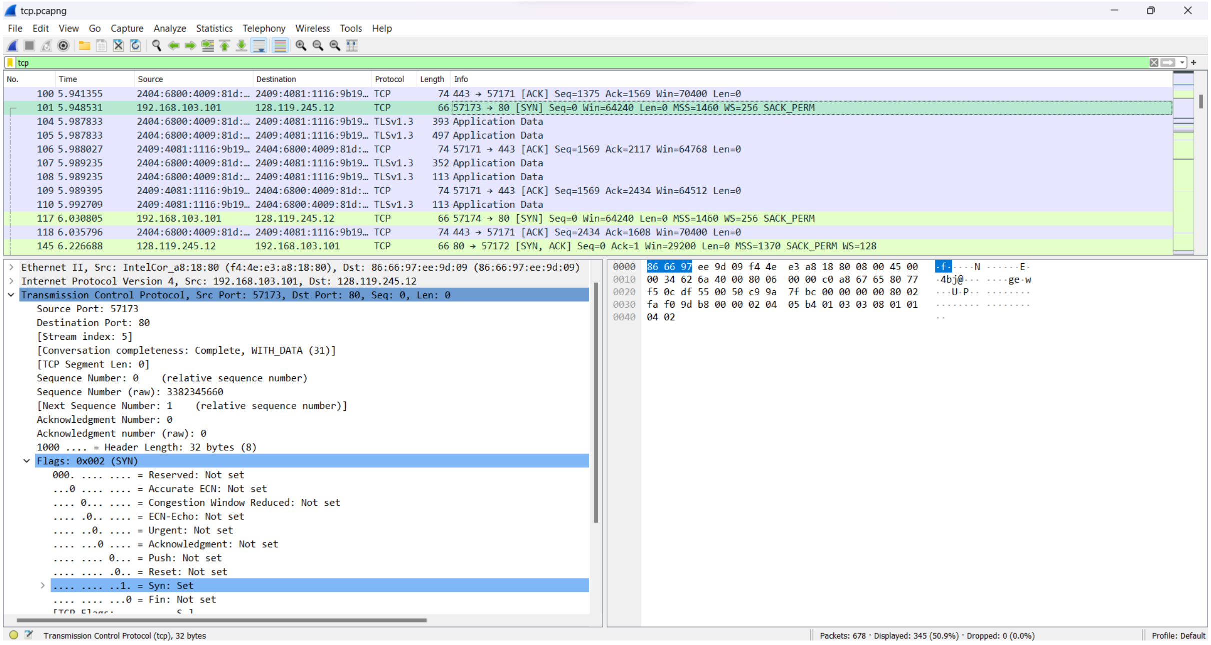
```
tcp
No.  Time       Source           Destination      Protocol Length Info
 446 17.000323  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=99357 Win=196096 Len=0
 447 17.000323  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=104837 Win=192512 Len=0
 448 17.000323  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=106207 Win=196096 Len=0
 449 17.000323  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=110317 Win=194432 Len=0
 450 17.004053  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=111687 Win=196096 Len=0
 451 17.004900  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=113057 Win=196096 Len=0
 452 17.005509  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=114427 Win=196096 Len=0
 453 17.006123  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=115797 Win=196096 Len=0
 454 17.006123  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=117167 Win=195456 Len=0
 455 17.007395  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=118537 Win=196096 Len=0
 456 17.008110  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=121277 Win=196096 Len=0
 457 17.008842  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=124017 Win=196096 Len=0
 458 17.009599  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=126757 Win=196096 Len=0
 459 17.013069  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=129497 Win=196096 Len=0
 460 17.014721  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=131789 Win=196096 Len=0
 461 17.015451  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=134529 Win=196096 Len=0
 462 17.017691  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=137269 Win=196096 Len=0
 463 17.027144  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=140009 Win=196096 Len=0
 464 17.027144  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=148229 Win=196096 Len=0
 465 17.029216  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=150969 Win=196096 Len=0
 466 17.030070  128.119.245.12   192.168.103.101  TCP        54 80 → 57173 [ACK] Seq=1 Ack=153038 Win=196096 Len=0
 467 17.030070  128.119.245.12   192.168.103.101  HTTP      831 HTTP/1.1 200 OK  (text/html)
 468 17.080980  192.168.103.101  128.119.245.12   TCP        54 57173 → 80 [ACK] Seq=153038 Ack=778 Win=64768 Len=0
```

```
> Frame 467: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface \Device\NPF_{3F
> Ethernet II, Src: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09), Dst: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.103.101
v Transmission Control Protocol, Src Port: 80, Dst Port: 57173, Seq: 1, Ack: 153038, Len: 777
    Source Port: 80
    Destination Port: 57173
    [Stream index: 5]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 777]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1839588442
    [Next Sequence Number: 778    (relative sequence number)]
    Acknowledgment Number: 153038    (relative ack number)
    Acknowledgment number (raw): 3382498698
```

```
0020  67 65 00 50 df 55 6d a5  e4 5a c9 9c d5 8a 50 18   ge·P·Um· ·Z····P·
0030  05 fc 9d c0 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 57 65 64   00 OK··D ate: Wed
0050  2c 20 30 38 20 4d 61 72  20 32 30 32 33 20 31 30   , 08 Mar  2023 10
0060  3a 35 37 3a 31 39 20 47  4d 54 0d 0a 53 65 72 76   :57:19 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.33  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 61  74 2c 20 30 36 20 46 65   fied: Sa t, 06 Fe
00e0  62 20 32 30 32 31 20 31  38 3a 32 33 3a 34 37 20   b 2021 1 8:23:47
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 61 32 2d   GMT··ETa g: "1a2-
0100  35 62 61 61 66 30 39 61  62 64 37 61 39 22 0d 0a   5baaf09a bd7a9"··
0110  41 63 63 65 70 74 2d 52  61 6e 67 65 73 3a 20 62   Accept-R anges: b
```

```
Source Port (tcp.srcport), 2 bytes    Packets: 678 · Displayed: 345 (50.9%) · Dropped: 0 (0.0%)    Profile: Default
```

3. The sequence number of the TCP SYN segment is 0 since it is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu. In the flags section, the SYN flag is set to 1



tcp.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time      Source               Destination          Protocol Length Info
 100 5.941355  2404:6800:4009:81d:… 2409:4081:1116:9b19… TCP        74 443 → 57171 [ACK] Seq=1375 Ack=1569 Win=70400 Len=0
 101 5.948531  192.168.103.101      128.119.245.12       TCP        66 57173 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 104 5.987833  2404:6800:4009:81d:… 2409:4081:1116:9b19… TLSv1.3   393 Application Data
 105 5.987833  2404:6800:4009:81d:… 2409:4081:1116:9b19… TLSv1.3   497 Application Data
 106 5.988027  2409:4081:1116:9b19… 2404:6800:4009:81d:… TCP        74 57171 → 443 [ACK] Seq=1569 Ack=2117 Win=64768 Len=0
 107 5.989235  2404:6800:4009:81d:… 2409:4081:1116:9b19… TLSv1.3   352 Application Data
 108 5.989235  2404:6800:4009:81d:… 2409:4081:1116:9b19… TLSv1.3   113 Application Data
 109 5.989395  2409:4081:1116:9b19… 2404:6800:4009:81d:… TCP        74 57171 → 443 [ACK] Seq=1569 Ack=2434 Win=64512 Len=0
 110 5.992709  2409:4081:1116:9b19… 2404:6800:4009:81d:… TLSv1.3   113 Application Data
 117 6.030805  192.168.103.101      128.119.245.12       TCP        66 57174 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 118 6.035796  2404:6800:4009:81d:… 2409:4081:1116:9b19… TCP        74 443 → 57171 [ACK] Seq=2434 Ack=1608 Win=70400 Len=0
 145 6.226688  128.119.245.12       192.168.103.101      TCP        66 80 → 57172 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1370 SACK_PERM WS=128
```

```
> Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
> Internet Protocol Version 4, Src: 192.168.103.101, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 57173, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 57173
    Destination Port: 80
    [Stream index: 5]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3382345660
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 08 00 45 00   ·f····N ······E·
0010  00 34 62 6a 40 00 80 06  00 00 c0 a8 67 65 80 77   ·4bj@··· ····ge·w
0020  f5 0c df 55 00 50 c9 9a  7f bc 00 00 00 00 80 02   ···U·P·· ········
0030  fa f0 9d b8 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Transmission Control Protocol (tcp), 32 bytes

Packets: 678 · Displayed: 345 (50.9%) · Dropped: 0 (0.0%)

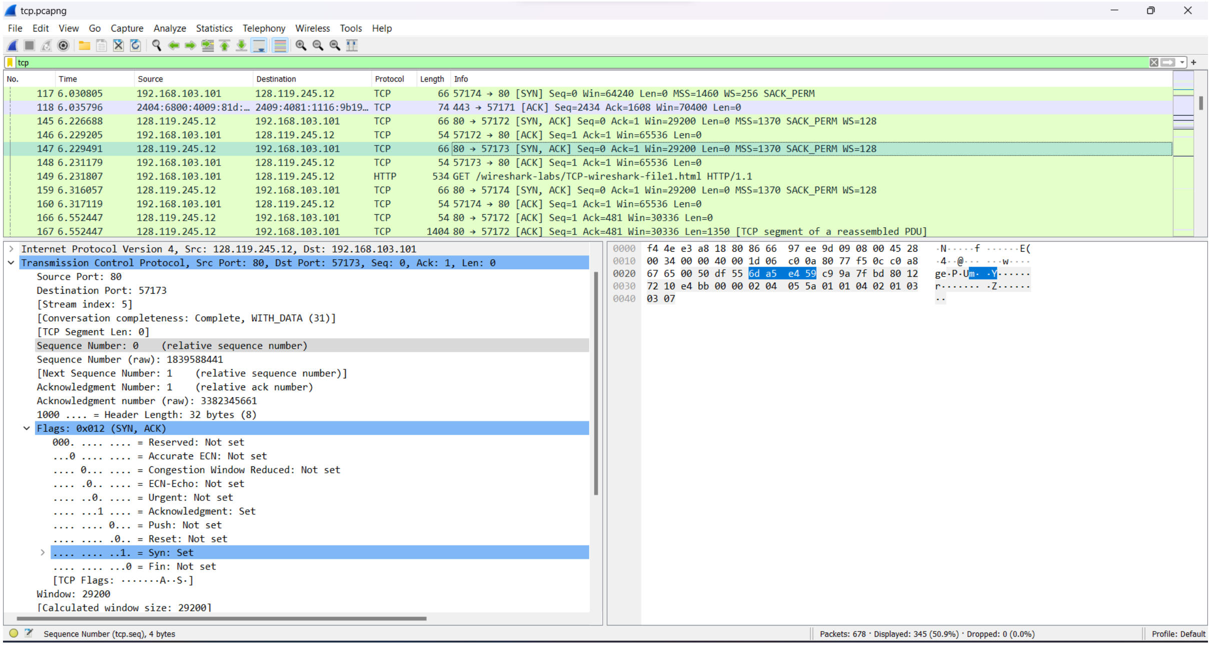
Profile: Default

4 a. The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0

b. The value of the acknowledgement field in the SYNACK segment is 1

c. The server (gaia.cs.umass.edu) adds 1 to the initial sequence number of SYN segment from the client computer (which was 0 in our case)

d. A segment will be identified as a SYNACK segment if both SYN flag and acknowledgement in the segment are set to 1



tcp.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time      Source               Destination          Protocol Length Info
 117 6.030805  192.168.103.101      128.119.245.12       TCP        66 57174 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 118 6.035796  2404:6800:4009:81d:… 2409:4081:1116:9b19… TCP        74 443 → 57171 [ACK] Seq=2434 Ack=1608 Win=70400 Len=0
 145 6.226688  128.119.245.12       192.168.103.101      TCP        66 80 → 57172 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1370 SACK_PERM WS=128
 146 6.229205  192.168.103.101      128.119.245.12       TCP        54 57172 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 147 6.229491  128.119.245.12       192.168.103.101      TCP        66 80 → 57173 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1370 SACK_PERM WS=128
 148 6.231179  192.168.103.101      128.119.245.12       TCP        54 57173 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 149 6.231807  192.168.103.101      128.119.245.12       HTTP      534 GET /wireshark-labs/TCP-wireshark-file1.html HTTP/1.1
 159 6.316057  128.119.245.12       192.168.103.101      TCP        66 80 → 57174 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1370 SACK_PERM WS=128
 160 6.317119  192.168.103.101      128.119.245.12       TCP        54 57174 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 166 6.552447  128.119.245.12       192.168.103.101      TCP        54 80 → 57172 [ACK] Seq=1 Ack=481 Win=30336 Len=0
 167 6.552447  128.119.245.12       192.168.103.101      TCP      1404 80 → 57172 [ACK] Seq=1 Ack=481 Win=30336 Len=1350 [TCP segment of a reassembled PDU]
```

```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.103.101
v Transmission Control Protocol, Src Port: 80, Dst Port: 57173, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 57173
    [Stream index: 5]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1839588441
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3382345661
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A··S·]
    Window: 29200
    [Calculated window size: 29200]
```

```
0000  f4 4e e3 a8 18 80 86 66  97 ee 9d 09 08 00 45 28   ·N·····f ······E(
0010  00 34 00 00 40 00 1d 06  c0 0a 80 77 f5 0c c0 a8   ·4··@··· ···w····
0020  67 65 00 50 df 55 6d a5  e4 59 c9 9a 7f bd 80 12   ge·P·Um· ·Y······
0030  72 10 e4 bb 00 00 02 04  05 5a 01 01 04 02 01 03   r······· ·Z······
0040  03 07                                              ··
```

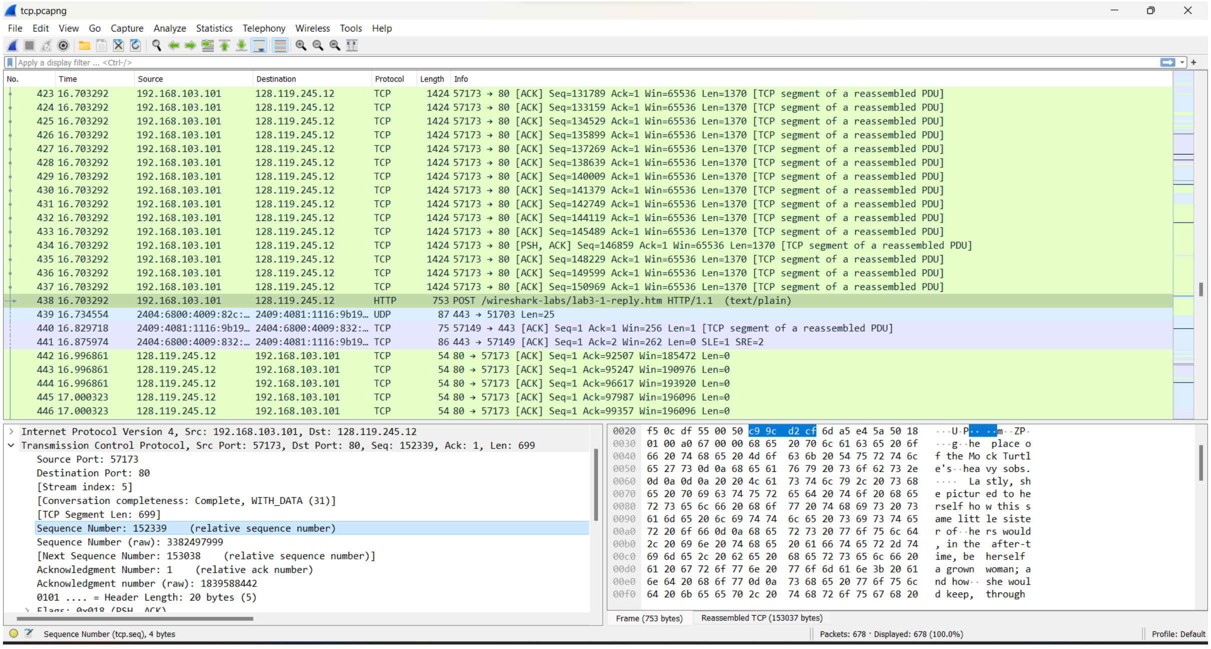
Sequence Number (tcp.seq), 4 bytes

Packets: 678 · Displayed: 345 (50.9%) · Dropped: 0 (0.0%)

Profile: Default

5. The TCP segment that contains the HTTP POST command

has sequence number 152339


tcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

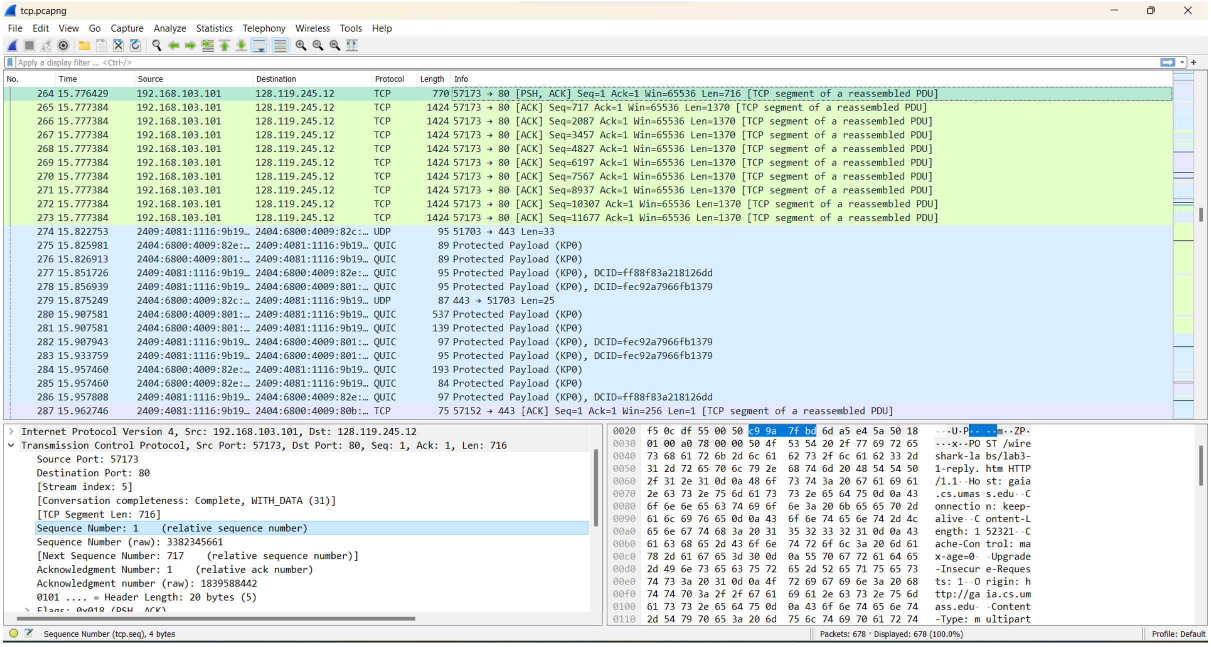
```
No.  Time       Source              Destination         Protocol Length Info
 423 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=131789 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 424 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=133159 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 425 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=134529 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 426 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=135899 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 427 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=137269 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 428 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=138639 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 429 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=140009 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 430 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=141379 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 431 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=142749 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 432 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=144119 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 433 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=145489 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 434 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [PSH, ACK] Seq=146859 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 435 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=148229 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 436 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=149599 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 437 16.703292  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=150969 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 438 16.703292  192.168.103.101     128.119.245.12      HTTP      753 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
 439 16.734554  2404:6800:4009:82c:… 2409:4081:1116:9b19… UDP       87 443 → 51703 Len=25
 440 16.829718  2409:4081:1116:9b19… 2404:6800:4009:832:… TCP       75 57149 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
 441 16.875974  2404:6800:4009:832:… 2409:4081:1116:9b19… TCP       86 443 → 57149 [ACK] Seq=1 Ack=2 Win=262 Len=0 SLE=1 SRE=2
 442 16.996861  128.119.245.12      192.168.103.101     TCP        54 80 → 57173 [ACK] Seq=1 Ack=92507 Win=185472 Len=0
 443 16.996861  128.119.245.12      192.168.103.101     TCP        54 80 → 57173 [ACK] Seq=1 Ack=95247 Win=190976 Len=0
 444 16.996861  128.119.245.12      192.168.103.101     TCP        54 80 → 57173 [ACK] Seq=1 Ack=96617 Win=193920 Len=0
 445 17.000323  128.119.245.12      192.168.103.101     TCP        54 80 → 57173 [ACK] Seq=1 Ack=97987 Win=196096 Len=0
 446 17.000323  128.119.245.12      192.168.103.101     TCP        54 80 → 57173 [ACK] Seq=1 Ack=99357 Win=196096 Len=0
```

```
> Internet Protocol Version 4, Src: 192.168.103.101, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 57173, Dst Port: 80, Seq: 152339, Ack: 1, Len: 699
    Source Port: 57173
    Destination Port: 80
    [Stream index: 5]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 699]
    Sequence Number: 152339    (relative sequence number)
    Sequence Number (raw): 3382497999
    [Next Sequence Number: 153038    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1839588442
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

```
0020  f5 0c df 55 00 50 c9 9c  d2 cf 6d a5 e4 5a 50 18   ···U·P·· ··m··ZP·
0030  01 00 a0 67 00 00 68 65  20 70 6c 61 63 65 20 6f   ···g··he  place o
0040  66 20 74 68 65 20 4d 6f  63 6b 20 54 75 72 74 6c   f the Mo ck Turtl
0050  65 27 73 0d 0a 68 65 61  76 79 20 73 6f 62 73 2e   e's··hea vy sobs.
0060  0d 0a 0d 0a 20 20 4c 61  73 74 6c 79 2c 20 73 68   ····  La stly, sh
0070  65 20 70 69 63 74 75 72  65 64 20 74 6f 20 68 65   e pictur ed to he
0080  72 73 65 6c 66 20 68 6f  77 20 74 68 69 73 20 73   rself ho w this s
0090  61 6d 65 20 6c 69 74 74  6c 65 20 73 69 73 74 65   ame litt le siste
00a0  72 20 6f 66 0d 0a 68 65  72 73 20 77 6f 75 6c 64   r of··he rs would
00b0  2c 20 69 6e 20 74 68 65  20 61 66 74 65 72 2d 74   , in the  after-t
00c0  69 6d 65 2c 20 62 65 20  68 65 72 73 65 6c 66 20   ime, be  herself
00d0  61 20 67 72 6f 77 6e 20  77 6f 6d 61 6e 3b 20 61   a grown  woman; a
00e0  6e 64 20 68 6f 77 0d 0a  73 68 65 20 77 6f 75 6c   nd how·· she woul
00f0  64 20 6b 65 65 70 2c 20  74 68 72 6f 75 67 68 20   d keep,  through
```

Frame (753 bytes)
Reassembled TCP (153037 bytes)
Sequence Number (tcp.seq), 4 bytes
Packets: 678 · Displayed: 678 (100.0%)
Profile: Default

TCP segment having post as a data field has sequence no. 1.


tcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source              Destination         Protocol Length Info
 264 15.776429  192.168.103.101     128.119.245.12      TCP       770 57173 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=716 [TCP segment of a reassembled PDU]
 265 15.777384  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=717 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 266 15.777384  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=2087 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 267 15.777384  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=3457 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 268 15.777384  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=4827 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 269 15.777384  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=6197 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 270 15.777384  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=7567 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 271 15.777384  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=8937 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 272 15.777384  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=10307 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 273 15.777384  192.168.103.101     128.119.245.12      TCP      1424 57173 → 80 [ACK] Seq=11677 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 274 15.822753  2409:4081:1116:9b19… 2404:6800:4009:82c:… UDP       95 51703 → 443 Len=33
 275 15.825981  2404:6800:4009:82e:… 2409:4081:1116:9b19… QUIC      89 Protected Payload (KP0)
 276 15.826913  2404:6800:4009:801:… 2409:4081:1116:9b19… QUIC      89 Protected Payload (KP0)
 277 15.851726  2409:4081:1116:9b19… 2404:6800:4009:82e:… QUIC      95 Protected Payload (KP0), DCID=ff88f83a218126dd
 278 15.856939  2409:4081:1116:9b19… 2404:6800:4009:801:… QUIC      95 Protected Payload (KP0), DCID=fec92a7966fb1379
 279 15.875249  2404:6800:4009:82c:… 2409:4081:1116:9b19… UDP       87 443 → 51703 Len=25
 280 15.907581  2404:6800:4009:801:… 2409:4081:1116:9b19… QUIC     537 Protected Payload (KP0)
 281 15.907581  2404:6800:4009:801:… 2409:4081:1116:9b19… QUIC     139 Protected Payload (KP0)
 282 15.907943  2409:4081:1116:9b19… 2404:6800:4009:801:… QUIC      97 Protected Payload (KP0), DCID=fec92a7966fb1379
 283 15.933759  2409:4081:1116:9b19… 2404:6800:4009:801:… QUIC      95 Protected Payload (KP0), DCID=fec92a7966fb1379
 284 15.957460  2404:6800:4009:82e:… 2409:4081:1116:9b19… QUIC     193 Protected Payload (KP0)
 285 15.957460  2404:6800:4009:82e:… 2409:4081:1116:9b19… QUIC      84 Protected Payload (KP0)
 286 15.957808  2409:4081:1116:9b19… 2404:6800:4009:82e:… QUIC      97 Protected Payload (KP0), DCID=ff88f83a218126dd
 287 15.962746  2409:4081:1116:9b19… 2404:6800:4009:80b:… TCP       75 57152 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
```

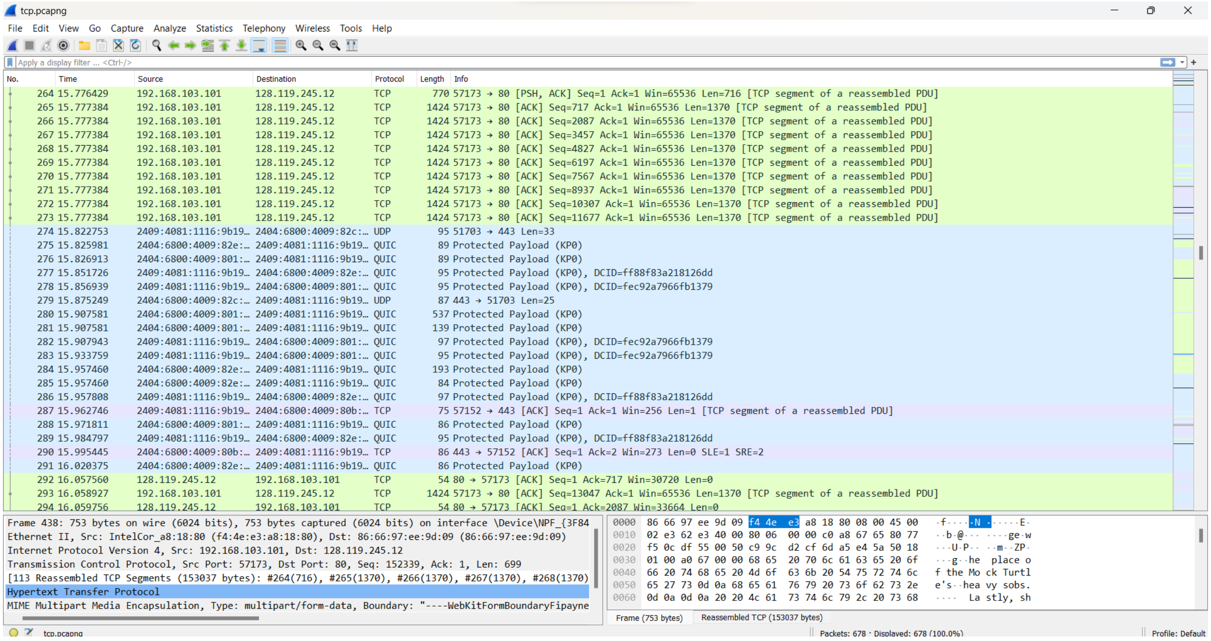
```
> Internet Protocol Version 4, Src: 192.168.103.101, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 57173, Dst Port: 80, Seq: 1, Ack: 1, Len: 716
    Source Port: 57173
    Destination Port: 80
    [Stream index: 5]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 716]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3382345661
    [Next Sequence Number: 717    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1839588442
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

```
0020  f5 0c df 55 00 50 c9 9a  7f bd 6d a5 e4 5a 50 18   ···U·P·· ··m··ZP·
0030  01 00 a0 78 00 00 50 4f  53 54 20 2f 77 69 72 65   ···x··PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 67 61 69 61   /1.1··Ho st: gaia
0070  2e 63 73 2e 75 6d 61 73  73 2e 65 64 75 0d 0a 43   .cs.umas s.edu··C
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
0090  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   alive··C ontent-L
00a0  65 6e 67 74 68 3a 20 31  35 32 33 32 31 0d 0a 43   ength: 1 52321··C
00b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00c0  78 2d 61 67 65 3d 30 0d  0a 55 70 67 72 61 64 65   x-age=0· ·Upgrade
00d0  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
00e0  74 73 3a 20 31 0d 0a 4f  72 69 67 69 6e 3a 20 68   ts: 1··O rigin: h
00f0  74 74 70 3a 2f 2f 67 61  69 61 2e 63 73 2e 75 6d   ttp://ga ia.cs.um
0100  61 73 73 2e 65 64 75 0d  0a 43 6f 6e 74 65 6e 74   ass.edu· ·Content
0110  2d 54 79 70 65 3a 20 6d  75 6c 74 69 70 61 72 74   -Type: m ultipart
```

Sequence Number (tcp.seq), 4 bytes
Packets: 678 · Displayed: 678 (100.0%)
Profile: Default

6.

a. Sequence numbers for segments 1-6 are 1, 717, 2087, 3457, 7567, 8937


tcp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source               Destination          Protocol Length Info
  264 15.776429  192.168.103.101      128.119.245.12       TCP       770 57173 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=716 [TCP segment of a reassembled PDU]
  265 15.777384  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=717 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  266 15.777384  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=2087 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  267 15.777384  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=3457 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  268 15.777384  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=4827 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  269 15.777384  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=6197 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  270 15.777384  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=7567 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  271 15.777384  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=8937 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  272 15.777384  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=10307 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  273 15.777384  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=11677 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  274 15.822753  2409:4081:1116:9b19… 2404:6800:4009:82c:… UDP        95 51703 → 443 Len=33
  275 15.825981  2404:6800:4009:82e:… 2409:4081:1116:9b19… QUIC       89 Protected Payload (KP0)
  276 15.826913  2404:6800:4009:801:… 2409:4081:1116:9b19… QUIC       89 Protected Payload (KP0)
  277 15.851726  2409:4081:1116:9b19… 2404:6800:4009:82e:… QUIC       95 Protected Payload (KP0), DCID=ff88f83a218126dd
  278 15.856939  2409:4081:1116:9b19… 2404:6800:4009:801:… QUIC       95 Protected Payload (KP0), DCID=fec92a7966fb1379
  279 15.875249  2404:6800:4009:82c:… 2409:4081:1116:9b19… UDP        87 443 → 51703 Len=25
  280 15.907581  2404:6800:4009:801:… 2409:4081:1116:9b19… QUIC      537 Protected Payload (KP0)
  281 15.907581  2404:6800:4009:801:… 2409:4081:1116:9b19… QUIC      139 Protected Payload (KP0)
  282 15.907943  2409:4081:1116:9b19… 2404:6800:4009:801:… QUIC       97 Protected Payload (KP0), DCID=fec92a7966fb1379
  283 15.933759  2409:4081:1116:9b19… 2404:6800:4009:801:… QUIC       95 Protected Payload (KP0), DCID=fec92a7966fb1379
  284 15.957460  2404:6800:4009:82e:… 2409:4081:1116:9b19… QUIC      193 Protected Payload (KP0)
  285 15.957460  2404:6800:4009:82e:… 2409:4081:1116:9b19… QUIC       84 Protected Payload (KP0)
  286 15.957808  2409:4081:1116:9b19… 2404:6800:4009:82e:… QUIC       97 Protected Payload (KP0), DCID=ff88f83a218126dd
  287 15.962746  2409:4081:1116:9b19… 2404:6800:4009:80b:… TCP        75 57152 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
  288 15.971811  2404:6800:4009:801:… 2409:4081:1116:9b19… QUIC       86 Protected Payload (KP0)
  289 15.984797  2409:4081:1116:9b19… 2404:6800:4009:82e:… QUIC       95 Protected Payload (KP0), DCID=ff88f83a218126dd
  290 15.995445  2404:6800:4009:80b:… 2409:4081:1116:9b19… TCP        86 443 → 57152 [ACK] Seq=1 Ack=2 Win=273 Len=0 SLE=1 SRE=2
  291 16.020375  2404:6800:4009:82e:… 2409:4081:1116:9b19… QUIC       86 Protected Payload (KP0)
  292 16.057560  128.119.245.12       192.168.103.101      TCP        54 80 → 57173 [ACK] Seq=1 Ack=717 Win=30720 Len=0
  293 16.058927  192.168.103.101      128.119.245.12       TCP      1424 57173 → 80 [ACK] Seq=13047 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
  294 16.059756  128.119.245.12       192.168.103.101      TCP        54 80 → 57173 [ACK] Seq=1 Ack=2087 Win=33664 Len=0
```

```
Frame 438: 753 bytes on wire (6024 bits), 753 bytes captured (6024 bits) on interface \Device\NPF_{3F84
Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
Internet Protocol Version 4, Src: 192.168.103.101, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57173, Dst Port: 80, Seq: 152339, Ack: 1, Len: 699
[113 Reassembled TCP Segments (153037 bytes): #264(716), #265(1370), #266(1370), #267(1370), #268(1370)
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryFipayne
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 08 00 45 00   ·f·····N ······E·
0010  02 e3 62 e3 40 00 80 06  00 00 c0 a8 67 65 80 77   ··b·@··· ····ge·w
0020  f5 0c df 55 00 50 c9 9c  d2 cf 6d a5 e4 5a 50 18   ···U·P·· ··m··ZP·
0030  01 00 a0 67 00 00 68 65  20 70 6c 61 63 65 20 6f   ···g··he  place o
0040  66 20 74 68 65 20 4d 6f  63 6b 20 54 75 72 74 6c   f the Mo ck Turtl
0050  65 27 73 0d 0a 68 65 61  76 79 20 73 6f 62 73 2e   e's··hea vy sobs.
0060  0d 0a 0d 0a 20 20 4c 61  73 74 6c 79 2c 20 73 68   ····  La stly, sh
```

Frame (753 bytes)
Reassembled TCP (153037 bytes)
tcp.pcapng
Packets: 678 · Displayed: 678 (100.0%)
Profile: Default

b.

Segment	Sent time	ACK received time	RTT
1	15.774281	16.05756	0.283279
2	15.777384	16.05756	0.281131
3	15.777384	16.059756	0.282372
4	15.777384	16.059756	0.282372
5	15.777384	16.060372	0.282988
6	15.777384	16.061363	0.283979

C.

Equation : EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT

SEG 1 : ERTT = RTT = 0.283279

SEG 2 : ERTT = 0.875 * 0.283279 + 0.125 * 0.281131 = 0.2830105

SEG 3 : ERTT = 0.875 * 0.2830105 + 0.125 * 0.282372 = 0.2829307

SEG 4 : ERTT = 0.875 *0.2829307 + 0.125 * 0.282372 = 0.282860

SEG 5 : ERTT = 0.875 * 0.282860 + 0.125 * 0.282988 = 0.282876

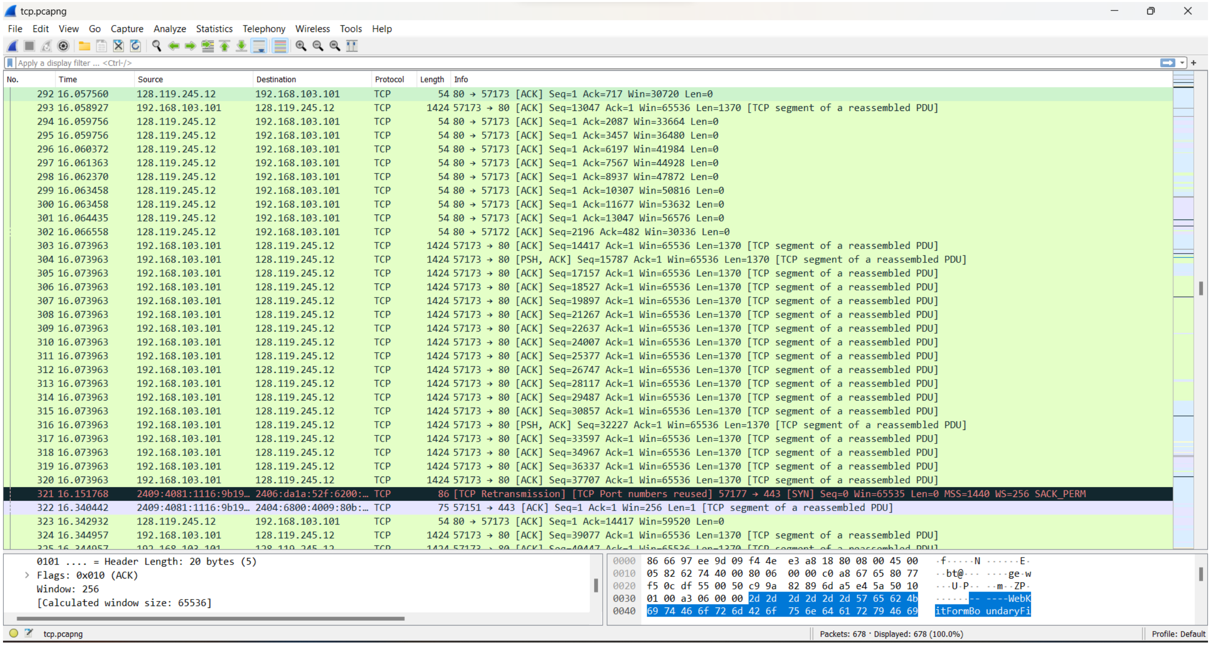
SEG 6 : ERTT = 0.875 * 0.282876 + 0.125 *0.283979 = 0.283013

D.

Segment	Packet Number	Packet Size
1	264	716
2	265	1370
3	266	1370
4	267	1370
5	268	1370
6	269	1370

E.

Total data transmitted = sequence number of last ACK - sequence number of first TCP segment = 10307 - 1 = 10306 bytes Transmission time = time of last ACK - time of first TCP segment = 16.061363 - 15.774281= 0.287082 seconds Therefore, the throughput for the TCP connection is computed as bytes 10306/0.287082 seconds = 35.899 kBps

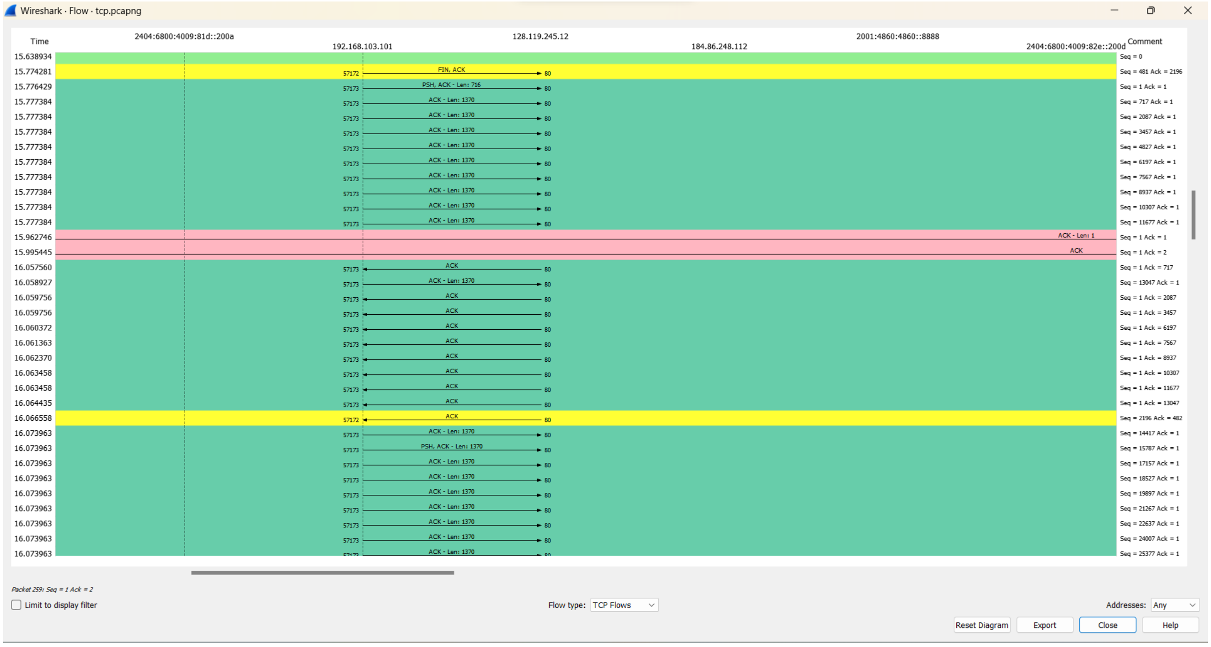


```
No.  Time       Source             Destination        Protocol Length Info
 292 16.057560  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=717 Win=30720 Len=0
 293 16.058927  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=13047 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 294 16.059756  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=2087 Win=33664 Len=0
 295 16.059756  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=3457 Win=36480 Len=0
 296 16.060372  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=6197 Win=41984 Len=0
 297 16.061363  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=7567 Win=44928 Len=0
 298 16.062370  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=8937 Win=47872 Len=0
 299 16.063458  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=10307 Win=50816 Len=0
 300 16.063458  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=11677 Win=53632 Len=0
 301 16.064435  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=13047 Win=56576 Len=0
 302 16.066558  128.119.245.12     192.168.103.101    TCP        54 80 → 57172 [ACK] Seq=2196 Ack=482 Win=30336 Len=0
 303 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=14417 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 304 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [PSH, ACK] Seq=15787 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 305 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=17157 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 306 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=18527 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 307 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=19897 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 308 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=21267 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 309 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=22637 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 310 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=24007 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 311 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=25377 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 312 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=26747 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 313 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=28117 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 314 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=29487 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 315 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=30857 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 316 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [PSH, ACK] Seq=32227 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 317 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=33597 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 318 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=34967 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 319 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=36337 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 320 16.073963  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=37707 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 321 16.151768  2409:4081:1116:9b19… 2406:da1a:52f:6200:… TCP   86 [TCP Retransmission] [TCP Port numbers reused] 57177 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
 322 16.340442  2409:4081:1116:9b19… 2404:6800:4009:80b:… TCP   75 57151 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
 323 16.342932  128.119.245.12     192.168.103.101    TCP        54 80 → 57173 [ACK] Seq=1 Ack=14417 Win=59520 Len=0
 324 16.344957  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=39077 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
 325 16.344957  192.168.103.101    128.119.245.12     TCP      1424 57173 → 80 [ACK] Seq=40447 Ack=1 Win=65536 Len=1370 [TCP segment of a reassembled PDU]
```

```
   0101 .... = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)
   Window: 256
   [Calculated window size: 65536]
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 08 00 45 00   ·f·····N ······E·
0010  05 82 62 74 40 00 80 06  00 00 c0 a8 67 65 80 77   ··bt@··· ····ge·w
0020  f5 0c df 55 00 50 c9 9a  82 89 6d a5 e4 5a 50 10   ···U·P·· ··m··ZP·
0030  01 00 a3 06 00 00 2d 2d  2d 2d 2d 2d 57 65 62 4b   ······-- ----WebK
0040  69 74 46 6f 72 6d 42 6f  75 6e 64 61 72 79 46 69   itFormBo undaryFi
```

tcp.pcapng   Packets: 678 · Displayed: 678 (100.0%)   Profile: Default



Wireshark · Flow · tcp.pcapng

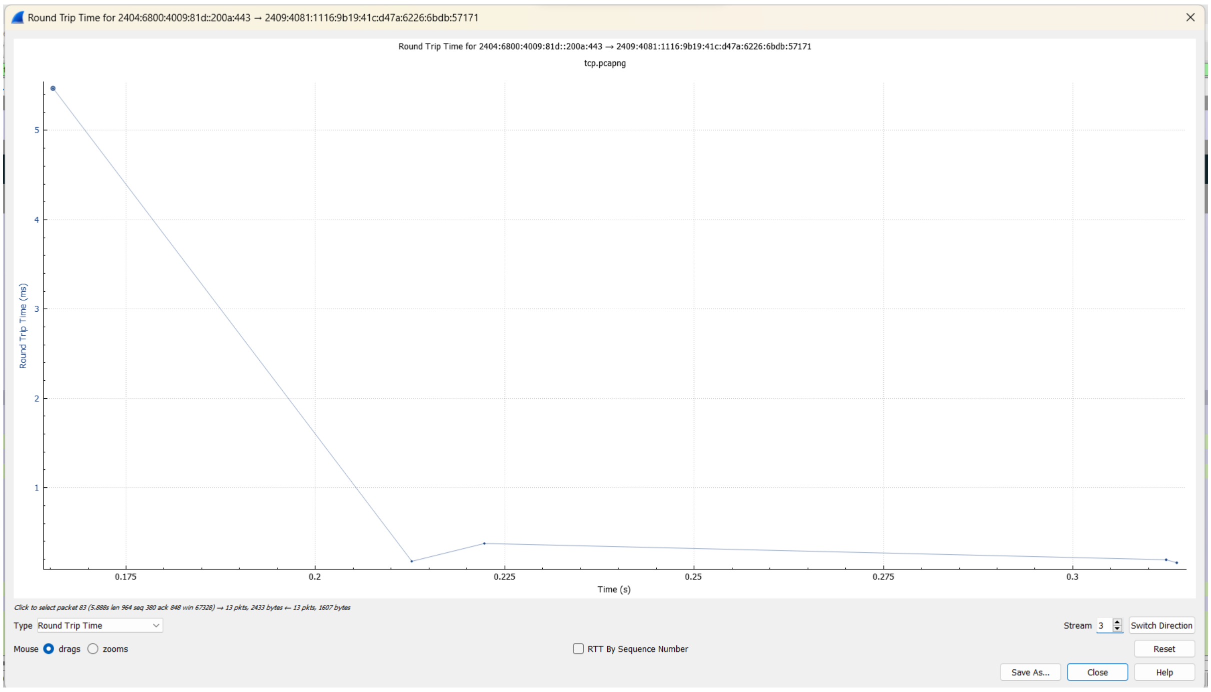
```
Time       2404:6800:4009:81d::200a  192.168.103.101  128.119.245.12  184.86.248.112  2001:4860:4860::8888  2404:6800:4009:82e::200d  Comment
15.638934                                                                                                                           Seq = 0
15.774281                            57172 ---FIN, ACK--------------> 80                                                            Seq = 481 Ack = 2196
15.776429                            57173 ---PSH, ACK - Len: 716---> 80                                                            Seq = 1 Ack = 1
15.777384                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 717 Ack = 1
15.777384                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 2087 Ack = 1
15.777384                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 3457 Ack = 1
15.777384                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 4827 Ack = 1
15.777384                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 6197 Ack = 1
15.777384                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 7567 Ack = 1
15.777384                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 8937 Ack = 1
15.777384                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 10307 Ack = 1
15.777384                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 11677 Ack = 1
15.962746                                                                                                     ACK - Len: 1          Seq = 1 Ack = 1
15.995445                                                                                                     ACK                   Seq = 1 Ack = 2
16.057560                            57173 <--ACK-------------------- 80                                                            Seq = 1 Ack = 717
16.058927                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 13047 Ack = 1
16.059756                            57173 <--ACK-------------------- 80                                                            Seq = 1 Ack = 2087
16.059756                            57173 <--ACK-------------------- 80                                                            Seq = 1 Ack = 3457
16.060372                            57173 <--ACK-------------------- 80                                                            Seq = 1 Ack = 6197
16.061363                            57173 <--ACK-------------------- 80                                                            Seq = 1 Ack = 7567
16.062370                            57173 <--ACK-------------------- 80                                                            Seq = 1 Ack = 8937
16.063458                            57173 <--ACK-------------------- 80                                                            Seq = 1 Ack = 10307
16.063458                            57173 <--ACK-------------------- 80                                                            Seq = 1 Ack = 11677
16.064435                            57173 <--ACK-------------------- 80                                                            Seq = 1 Ack = 13047
16.066558                            57172 <--ACK-------------------- 80                                                            Seq = 2196 Ack = 482
16.073963                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 14417 Ack = 1
16.073963                            57173 ---PSH, ACK - Len: 1370--> 80                                                            Seq = 15787 Ack = 1
16.073963                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 17157 Ack = 1
16.073963                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 18527 Ack = 1
16.073963                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 19897 Ack = 1
16.073963                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 21267 Ack = 1
16.073963                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 22637 Ack = 1
16.073963                            57173 ---ACK - Len: 1370-------> 80                                                            Seq = 24007 Ack = 1
16.073963                                  ---ACK - Len: 1370-------> 80                                                            Seq = 25377 Ack = 1
```

Packet 259: Seq = 1 Ack = 2

☐ Limit to display filter

Flow type: TCP Flows

Addresses: Any



Round Trip Time for 2404:6800:4009:81d::200a:443 → 2409:4081:1116:9b19:41c:d47a:6226:6bdb:57171

Round Trip Time for 2404:6800:4009:81d::200a:443 → 2409:4081:1116:9b19:41c:d47a:6226:6bdb:57171

tcp.pcapng

Click to select packet 83 (5.888s len 964 seq 380 ack 848 win 67328) → 13 pkts, 2433 bytes ← 13 pkts, 1607 bytes

Type: Round Trip Time

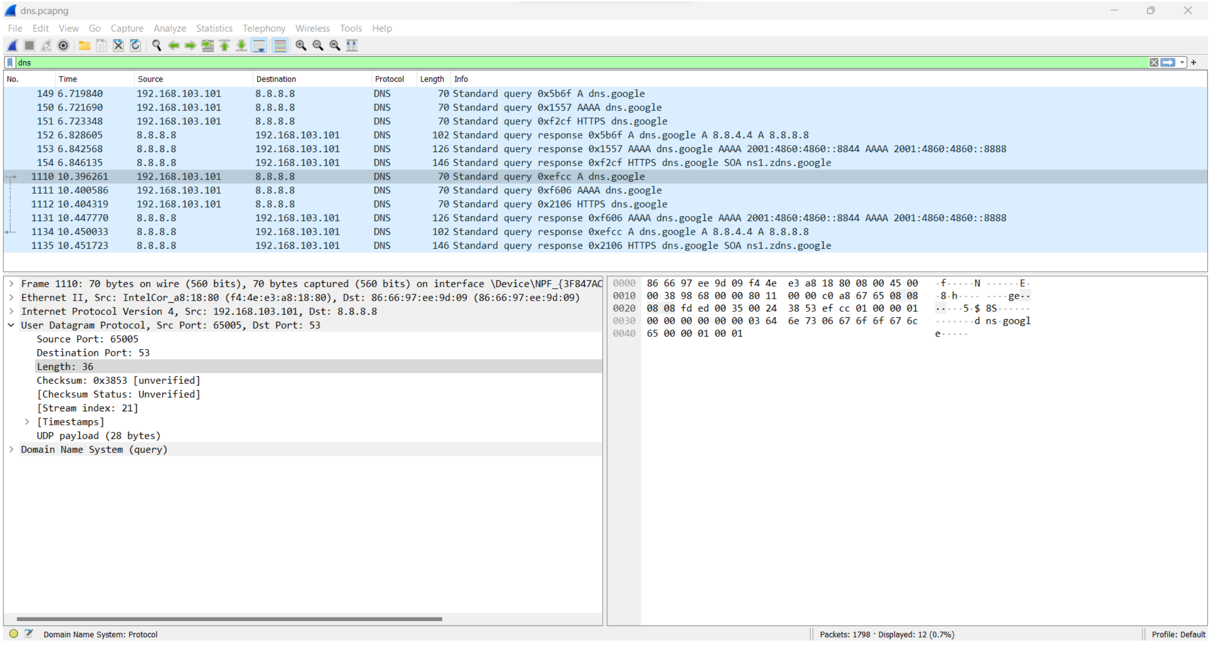
Stream 3

Mouse ● drags ○ zooms

☐ RTT By Sequence Number

UDP

1. Source Port, Destination Port, Length, CheckSum



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

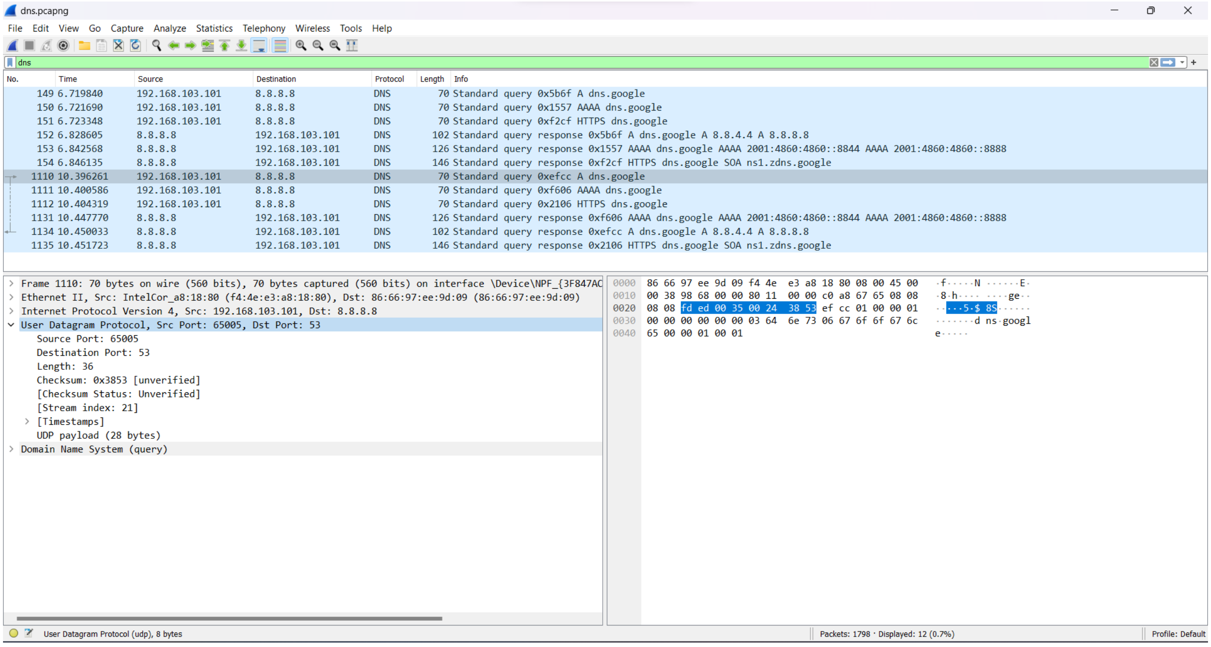
```
No.   Time        Source           Destination      Protocol Length Info
  149 6.719840    192.168.103.101  8.8.8.8          DNS        70 Standard query 0x5b6f A dns.google
  150 6.721690    192.168.103.101  8.8.8.8          DNS        70 Standard query 0x1557 AAAA dns.google
  151 6.723348    192.168.103.101  8.8.8.8          DNS        70 Standard query 0xf2cf HTTPS dns.google
  152 6.828605    8.8.8.8          192.168.103.101  DNS       102 Standard query response 0x5b6f A dns.google A 8.8.4.4 A 8.8.8.8
  153 6.842568    8.8.8.8          192.168.103.101  DNS       126 Standard query response 0x1557 AAAA dns.google AAAA 2001:4860:4860::8844 AAAA 2001:4860:4860::8888
  154 6.846135    8.8.8.8          192.168.103.101  DNS       146 Standard query response 0xf2cf HTTPS dns.google SOA ns1.zdns.google
 1110 10.396261   192.168.103.101  8.8.8.8          DNS        70 Standard query 0xefcc A dns.google
 1111 10.400586   192.168.103.101  8.8.8.8          DNS        70 Standard query 0xf606 AAAA dns.google
 1112 10.404319   192.168.103.101  8.8.8.8          DNS        70 Standard query 0x2106 HTTPS dns.google
 1131 10.447770   8.8.8.8          192.168.103.101  DNS       126 Standard query response 0xf606 AAAA dns.google AAAA 2001:4860:4860::8844 AAAA 2001:4860:4860::8888
 1134 10.450033   8.8.8.8          192.168.103.101  DNS       102 Standard query response 0xefcc A dns.google A 8.8.4.4 A 8.8.8.8
 1135 10.451723   8.8.8.8          192.168.103.101  DNS       146 Standard query response 0x2106 HTTPS dns.google SOA ns1.zdns.google
```

```
> Frame 1110: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{3F847AC
> Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
> Internet Protocol Version 4, Src: 192.168.103.101, Dst: 8.8.8.8
v User Datagram Protocol, Src Port: 65005, Dst Port: 53
    Source Port: 65005
    Destination Port: 53
    Length: 36
    Checksum: 0x3853 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 21]
  > [Timestamps]
    UDP payload (28 bytes)
> Domain Name System (query)
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 08 00 45 00   ·f·····N ······E·
0010  00 38 98 68 00 00 80 11  00 00 c0 a8 67 65 08 08   ·8·h···· ····ge··
0020  08 08 fd ed 00 35 00 24  38 53 ef cc 01 00 00 01   ·····5·$ 8S······
0030  00 00 00 00 00 00 03 64  6e 73 06 67 6f 6f 67 6c   ·······d ns·googl
0040  65 00 00 01 00 01                                  e·····
```

Domain Name System: Protocol | Packets: 1798 · Displayed: 12 (0.7%) | Profile: Default

2. The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long. Highlighting the field will highlight the corresponding hex value. Each hex value corresponds to 1 byte.



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

```
No.   Time        Source           Destination      Protocol Length Info
  149 6.719840    192.168.103.101  8.8.8.8          DNS        70 Standard query 0x5b6f A dns.google
  150 6.721690    192.168.103.101  8.8.8.8          DNS        70 Standard query 0x1557 AAAA dns.google
  151 6.723348    192.168.103.101  8.8.8.8          DNS        70 Standard query 0xf2cf HTTPS dns.google
  152 6.828605    8.8.8.8          192.168.103.101  DNS       102 Standard query response 0x5b6f A dns.google A 8.8.4.4 A 8.8.8.8
  153 6.842568    8.8.8.8          192.168.103.101  DNS       126 Standard query response 0x1557 AAAA dns.google AAAA 2001:4860:4860::8844 AAAA 2001:4860:4860::8888
  154 6.846135    8.8.8.8          192.168.103.101  DNS       146 Standard query response 0xf2cf HTTPS dns.google SOA ns1.zdns.google
 1110 10.396261   192.168.103.101  8.8.8.8          DNS        70 Standard query 0xefcc A dns.google
 1111 10.400586   192.168.103.101  8.8.8.8          DNS        70 Standard query 0xf606 AAAA dns.google
 1112 10.404319   192.168.103.101  8.8.8.8          DNS        70 Standard query 0x2106 HTTPS dns.google
 1131 10.447770   8.8.8.8          192.168.103.101  DNS       126 Standard query response 0xf606 AAAA dns.google AAAA 2001:4860:4860::8844 AAAA 2001:4860:4860::8888
 1134 10.450033   8.8.8.8          192.168.103.101  DNS       102 Standard query response 0xefcc A dns.google A 8.8.4.4 A 8.8.8.8
 1135 10.451723   8.8.8.8          192.168.103.101  DNS       146 Standard query response 0x2106 HTTPS dns.google SOA ns1.zdns.google
```

```
> Frame 1110: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{3F847AC
> Ethernet II, Src: IntelCor_a8:18:80 (f4:4e:e3:a8:18:80), Dst: 86:66:97:ee:9d:09 (86:66:97:ee:9d:09)
> Internet Protocol Version 4, Src: 192.168.103.101, Dst: 8.8.8.8
v User Datagram Protocol, Src Port: 65005, Dst Port: 53
    Source Port: 65005
    Destination Port: 53
    Length: 36
    Checksum: 0x3853 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 21]
  > [Timestamps]
    UDP payload (28 bytes)
> Domain Name System (query)
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 08 00 45 00   ·f·····N ······E·
0010  00 38 98 68 00 00 80 11  00 00 c0 a8 67 65 08 08   ·8·h···· ····ge··
0020  08 08 fd ed 00 35 00 24  38 53 ef cc 01 00 00 01   ·····5·$ 8S······
0030  00 00 00 00 00 00 03 64  6e 73 06 67 6f 6f 67 6c   ·······d ns·googl
0040  65 00 00 01 00 01                                  e·····
```

User Datagram Protocol (udp), 8 bytes | Packets: 1798 · Displayed: 12 (0.7%) | Profile: Default

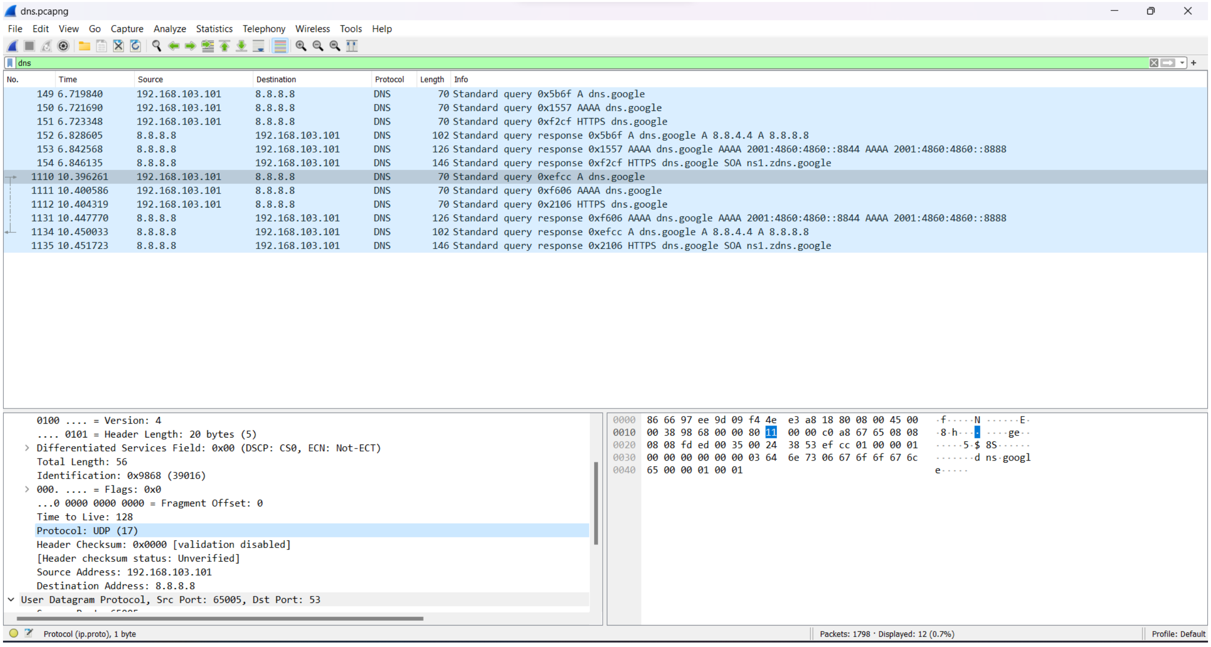
3. **The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.**

The length of UDP payload for selected packet is 36 bytes.
36 bytes - 8 bytes = 28 bytes.

4. **The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.**

5. **The largest possible source port number is (2^16 – 1) = 65535.**

6. **The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.**



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

```
No.     Time       Source            Destination       Protocol  Length  Info
   149  6.719840   192.168.103.101   8.8.8.8           DNS        70 Standard query 0x5b6f A dns.google
   150  6.721690   192.168.103.101   8.8.8.8           DNS        70 Standard query 0x1557 AAAA dns.google
   151  6.723348   192.168.103.101   8.8.8.8           DNS        70 Standard query 0xf2cf HTTPS dns.google
   152  6.828605   8.8.8.8           192.168.103.101   DNS       102 Standard query response 0x5b6f A dns.google A 8.8.4.4 A 8.8.8.8
   153  6.842568   8.8.8.8           192.168.103.101   DNS       126 Standard query response 0x1557 AAAA dns.google AAAA 2001:4860:4860::8844 AAAA 2001:4860:4860::8888
   154  6.846135   8.8.8.8           192.168.103.101   DNS       146 Standard query response 0xf2cf HTTPS dns.google SOA ns1.zdns.google
  1110  10.396261  192.168.103.101   8.8.8.8           DNS        70 Standard query 0xefcc A dns.google
  1111  10.400586  192.168.103.101   8.8.8.8           DNS        70 Standard query 0xf606 AAAA dns.google
  1112  10.404319  192.168.103.101   8.8.8.8           DNS        70 Standard query 0x2106 HTTPS dns.google
  1131  10.447770  8.8.8.8           192.168.103.101   DNS       126 Standard query response 0xf606 AAAA dns.google AAAA 2001:4860:4860::8844 AAAA 2001:4860:4860::8888
  1134  10.450033  8.8.8.8           192.168.103.101   DNS       102 Standard query response 0xefcc A dns.google A 8.8.4.4 A 8.8.8.8
  1135  10.451723  8.8.8.8           192.168.103.101   DNS       146 Standard query response 0x2106 HTTPS dns.google SOA ns1.zdns.google
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x9868 (39016)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.103.101
    Destination Address: 8.8.8.8
v User Datagram Protocol, Src Port: 65005, Dst Port: 53
```

```
0000  86 66 97 ee 9d 09 f4 4e  e3 a8 18 80 08 00 45 00   ·f·····N ······E·
0010  00 38 98 68 00 00 80 11  00 00 c0 a8 67 65 08 08   ·8·h···· ····ge··
0020  08 08 fd ed 00 35 00 24  38 53 ef cc 01 00 00 01   ·····5·$ 8S······
0030  00 00 00 00 00 00 03 64  6e 73 06 67 6f 6f 67 6c   ·······d ns·googl
0040  65 00 00 01 00 01                                  e·····
```

Protocol (ip.proto), 1 byte   Packets: 1798 · Displayed: 12 (0.7%)   Profile: Default