Mustafa Alawadi

40217764

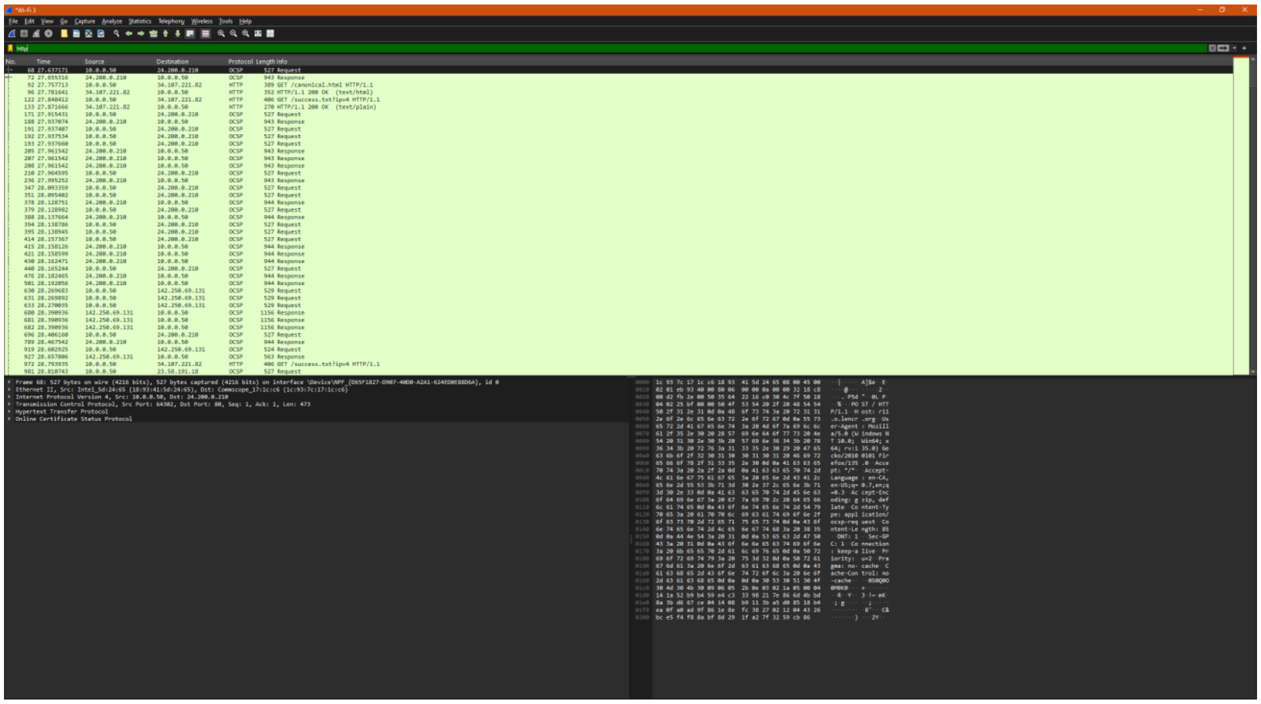
Lab2

Dr Aiman Hanna

2025-02-25

Task 1

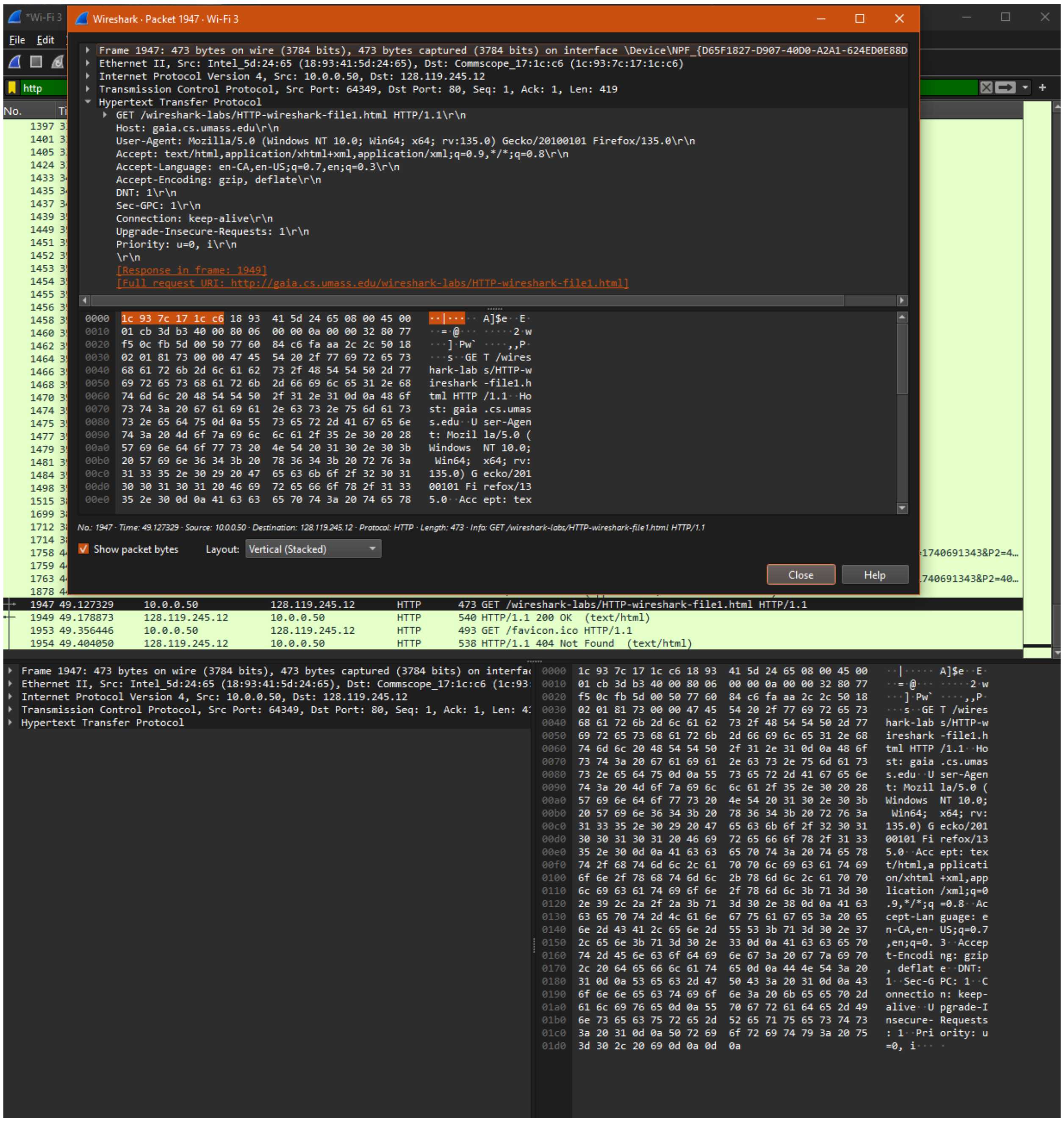
1.


*Wi-Fi 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time       Source           Destination      Protocol Length Info
    68 27.637171  10.0.0.50        24.200.0.210     OCSP      527 Request
    72 27.655316  24.200.0.210     10.0.0.50        OCSP      943 Response
    92 27.757713  10.0.0.50        34.107.221.82    HTTP      389 GET /canonical.html HTTP/1.1
    96 27.781641  34.107.221.82    10.0.0.50        HTTP      352 HTTP/1.1 200 OK  (text/html)
   122 27.848412  10.0.0.50        34.107.221.82    HTTP      406 GET /success.txt?ipv4 HTTP/1.1
   133 27.871666  34.107.221.82    10.0.0.50        HTTP      270 HTTP/1.1 200 OK  (text/plain)
   171 27.915431  10.0.0.50        24.200.0.210     OCSP      527 Request
   188 27.937074  24.200.0.210     10.0.0.50        OCSP      943 Response
   191 27.937407  10.0.0.50        24.200.0.210     OCSP      527 Request
   192 27.937534  10.0.0.50        24.200.0.210     OCSP      527 Request
   193 27.937660  10.0.0.50        24.200.0.210     OCSP      527 Request
   205 27.961542  24.200.0.210     10.0.0.50        OCSP      943 Response
   207 27.961542  24.200.0.210     10.0.0.50        OCSP      943 Response
   208 27.961542  24.200.0.210     10.0.0.50        OCSP      943 Response
   210 27.964595  10.0.0.50        24.200.0.210     OCSP      527 Request
   236 27.995252  24.200.0.210     10.0.0.50        OCSP      943 Response
   347 28.093359  10.0.0.50        24.200.0.210     OCSP      527 Request
   351 28.095402  10.0.0.50        24.200.0.210     OCSP      527 Request
   378 28.128751  24.200.0.210     10.0.0.50        OCSP      944 Response
   379 28.128982  10.0.0.50        24.200.0.210     OCSP      527 Request
   388 28.137664  24.200.0.210     10.0.0.50        OCSP      944 Response
   394 28.138786  10.0.0.50        24.200.0.210     OCSP      527 Request
   395 28.138945  10.0.0.50        24.200.0.210     OCSP      527 Request
   414 28.157367  10.0.0.50        24.200.0.210     OCSP      527 Request
   415 28.158126  24.200.0.210     10.0.0.50        OCSP      944 Response
   421 28.158599  24.200.0.210     10.0.0.50        OCSP      944 Response
   430 28.162471  24.200.0.210     10.0.0.50        OCSP      944 Response
   440 28.165244  10.0.0.50        24.200.0.210     OCSP      527 Request
   476 28.182465  24.200.0.210     10.0.0.50        OCSP      944 Response
   501 28.192056  24.200.0.210     10.0.0.50        OCSP      944 Response
   630 28.269683  10.0.0.50        142.250.69.131   OCSP      529 Request
   631 28.269892  10.0.0.50        142.250.69.131   OCSP      529 Request
   633 28.270035  10.0.0.50        142.250.69.131   OCSP      529 Request
   680 28.390936  142.250.69.131   10.0.0.50        OCSP     1156 Response
   681 28.390936  142.250.69.131   10.0.0.50        OCSP     1156 Response
   682 28.390936  142.250.69.131   10.0.0.50        OCSP     1156 Response
   696 28.406160  10.0.0.50        24.200.0.210     OCSP      527 Request
   789 28.467542  24.200.0.210     10.0.0.50        OCSP      944 Response
   919 28.602925  10.0.0.50        142.250.69.131   OCSP      524 Request
   927 28.657806  142.250.69.131   10.0.0.50        OCSP      563 Response
   972 28.793935  10.0.0.50        34.107.221.82    HTTP      406 GET /success.txt?ipv4 HTTP/1.1
   981 28.810743  10.0.0.50        23.58.191.18     OCSP      527 Request
```

```
> Frame 68: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{D65F1827-D907-40D0-A2A1-624ED0E88D6A}, id 0
> Ethernet II, Src: Intel_5d:24:65 (18:93:41:5d:24:65), Dst: Commscope_17:1c:c6 (1c:93:7c:17:1c:c6)
> Internet Protocol Version 4, Src: 10.0.0.50, Dst: 24.200.0.210
> Transmission Control Protocol, Src Port: 64302, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
> Hypertext Transfer Protocol
> Online Certificate Status Protocol
```

```
0000  1c 93 7c 17 1c c6 18 93  41 5d 24 65 08 00 45 00   ··|·····A]$e··E·
0010  02 01 eb 93 40 00 80 06  00 00 0a 00 00 32 18 c8   ····@········2··
0020  00 d2 fb 2e 00 50 35 64  22 16 c0 30 4c 7f 50 18   ···.·P5d"··0L·P·
0030  04 02 25 bf 00 00 50 4f  53 54 20 2f 20 48 54 54   ··%···POST / HTT
0040  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 72 31 31   P/1.1··Host: r11
0050  2e 6f 2e 6c 65 6e 63 72  2e 6f 72 67 0d 0a 55 73   .o.lencr.org··Us
0060  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent: Mozill
0070  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (Windows N
0080  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0; Win64; x
0090  36 34 3b 20 72 76 3a 31  33 35 2e 30 29 20 47 65   64; rv:135.0) Ge
00a0  63 6b 6f 2f 32 30 31 30  30 31 30 31 20 46 69 72   cko/20100101 Fir
00b0  65 66 6f 78 2f 31 33 35  2e 30 0d 0a 41 63 63 65   efox/135.0··Acce
00c0  70 74 3a 20 2a 2f 2a 0d  0a 41 63 63 65 70 74 2d   pt: */*··Accept-
00d0  4c 61 6e 67 75 61 67 65  3a 20 65 6e 2d 43 41 2c   Language: en-CA,
00e0  65 6e 2d 55 53 3b 71 3d  30 2e 37 2c 65 6e 3b 71   en-US;q=0.7,en;q
00f0  3d 30 2e 33 0d 0a 41 63  63 65 70 74 2d 45 6e 63   =0.3··Accept-Enc
0100  6f 64 69 6e 67 3a 20 67  7a 69 70 2c 20 64 65 66   oding: gzip, def
0110  6c 61 74 65 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   late··Content-Ty
0120  70 65 3a 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   pe: application/
0130  6f 63 73 70 2d 72 65 71  75 65 73 74 0d 0a 43 6f   ocsp-request··Co
0140  6e 74 65 6e 74 2d 4c 65  6e 67 74 68 3a 20 38 35   ntent-Length: 85
0150  0d 0a 44 4e 54 3a 20 31  0d 0a 53 65 63 2d 47 50   ··DNT: 1··Sec-GP
0160  43 3a 20 31 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   C: 1··Connection
0170  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 50 72   : keep-alive··Pr
0180  69 6f 72 69 74 79 3a 20  75 3d 32 0d 0a 50 72 61   iority: u=2··Pra
0190  67 6d 61 3a 20 6e 6f 2d  63 61 63 68 65 0d 0a 43   gma: no-cache··C
01a0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6e 6f   ache-Control: no
01b0  2d 63 61 63 68 65 0d 0a  0d 0a 30 53 30 51 30 4f   -cache····0S0Q0O
01c0  30 4d 30 4b 30 09 06 05  2b 0e 03 02 1a 05 00 04   0M0K0···+·······
01d0  14 1a 52 b9 b4 59 e4 c3  33 98 21 7e 86 6d 4b bd   ··R··Y··3·!~·mK·
01e0  8a 3b d6 67 ce 04 14 00  b9 11 3b a5 d0 85 18 b4   ·;·g······;·····
01f0  ea 0f a0 ad 9f 86 1e 8e  fc 38 27 02 12 04 43 26   ·········8'···C&
0200  bc e5 f4 f8 8a bf 8d 29  1f a2 7f 32 59 cb 86      ·······)···2Y··
```



```
Frame 1947: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{D65F1827-D907-40D0-A2A1-624ED0E88D
Ethernet II, Src: Intel_5d:24:65 (18:93:41:5d:24:65), Dst: Commscope_17:1c:c6 (1c:93:7c:17:1c:c6)
Internet Protocol Version 4, Src: 10.0.0.50, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64349, Dst Port: 80, Seq: 1, Ack: 1, Len: 419
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-CA,en-US;q=0.7,en;q=0.3\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Sec-GPC: 1\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i\r\n
  \r\n
  [Response in frame: 1949]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

```
0000  1c 93 7c 17 1c c6 18 93  41 5d 24 65 08 00 45 00   ··|···· A]$e··E·
0010  01 cb 3d b3 40 00 80 06  00 00 0a 00 00 32 80 77   ··=·@··· ·····2·w
0020  f5 0c fb 5d 00 50 77 60  84 c6 fa aa 2c 2c 50 18   ···]·Pw` ····,,P·
0030  02 01 81 73 00 00 47 45  54 20 2f 77 69 72 65 73   ···s··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
00b0  20 57 69 6e 36 34 3b 20  78 36 34 3b 20 72 76 3a    Win64;  x64; rv:
00c0  31 33 35 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   135.0) G ecko/201
00d0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 31 33   00101 Fi refox/13
00e0  35 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   5.0··Acc ept: tex
```

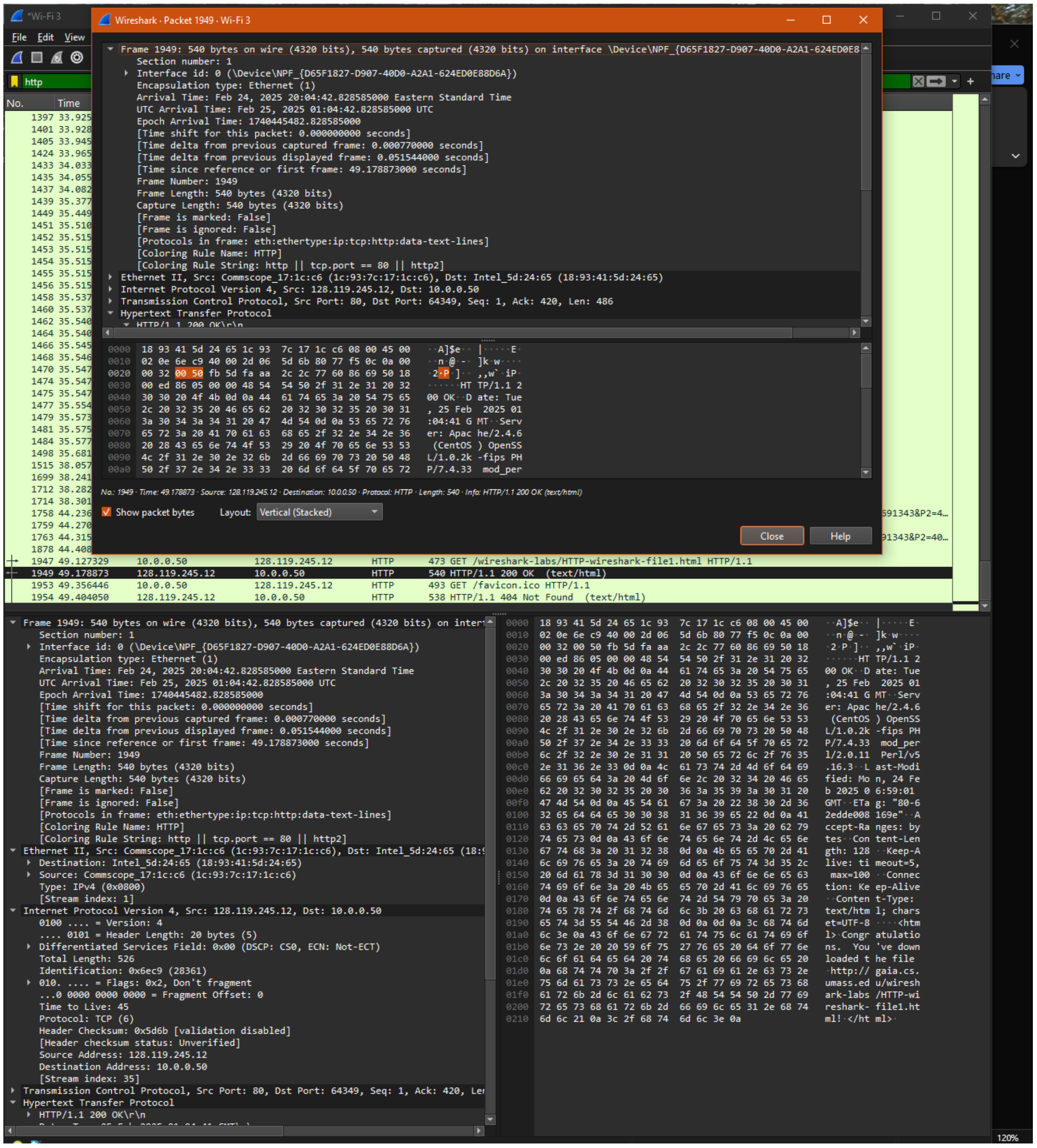
No.: 1947 · Time: 49.127329 · Source: 10.0.0.50 · Destination: 128.119.245.12 · Protocol: HTTP · Length: 473 · Info: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Layout: Vertical (Stacked)

```
No.   Ti
1947 49.127329   10.0.0.50        128.119.245.12   HTTP   473 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1949 49.178873   128.119.245.12   10.0.0.50        HTTP   540 HTTP/1.1 200 OK  (text/html)
1953 49.356446   10.0.0.50        128.119.245.12   HTTP   493 GET /favicon.ico HTTP/1.1
1954 49.404050   128.119.245.12   10.0.0.50        HTTP   538 HTTP/1.1 404 Not Found  (text/html)
```

```
Frame 1947: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interfac
Ethernet II, Src: Intel_5d:24:65 (18:93:41:5d:24:65), Dst: Commscope_17:1c:c6 (1c:93
Internet Protocol Version 4, Src: 10.0.0.50, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64349, Dst Port: 80, Seq: 1, Ack: 1, Len: 41
Hypertext Transfer Protocol
```

```
0000  1c 93 7c 17 1c c6 18 93  41 5d 24 65 08 00 45 00   ··|····· A]$e··E·
0010  01 cb 3d b3 40 00 80 06  00 00 0a 00 00 32 80 77   ··=·@··· ·····2·w
0020  f5 0c fb 5d 00 50 77 60  84 c6 fa aa 2c 2c 50 18   ···]·Pw` ····,,P·
0030  02 01 81 73 00 00 47 45  54 20 2f 77 69 72 65 73   ···s··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
00b0  20 57 69 6e 36 34 3b 20  78 36 34 3b 20 72 76 3a    Win64;  x64; rv:
00c0  31 33 35 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   135.0) G ecko/201
00d0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 31 33   00101 Fi refox/13
00e0  35 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   5.0··Acc ept: tex
00f0  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
0100  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
0110  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
0120  2e 39 2c 2a 2f 2a 3b 71  3d 30 2e 38 0d 0a 41 63   .9,*/*;q =0.8··Ac
0130  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 65   cept-Lan guage: e
0140  6e 2d 43 41 2c 65 6e 2d  55 53 3b 71 3d 30 2e 37   n-CA,en- US;q=0.7
0150  2c 65 6e 3b 71 3d 30 2e  33 0d 0a 41 63 63 65 70   ,en;q=0. 3··Accep
0160  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi ng: gzip
0170  2c 20 64 65 66 6c 61 74  65 0d 0a 44 4e 54 3a 20   , deflat e··DNT: 
0180  31 0d 0a 53 65 63 2d 47  50 43 3a 20 31 0d 0a 43   1··Sec-G PC: 1··C
0190  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
01a0  61 6c 69 76 65 0d 0a 55  70 67 72 61 64 65 2d 49   alive··U pgrade-I
01b0  6e 73 65 63 75 72 65 2d  52 65 71 75 65 73 74 73   nsecure- Requests
01c0  3a 20 31 0d 0a 50 72 69  6f 72 69 74 79 3a 20 75   : 1··Pri ority: u
01d0  3d 30 2c 20 69 0d 0a 0d  0a                        =0, i····
```



```
Frame 1949: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{D65F1827-D907-40D0-A2A1-624ED0E8
    Section number: 1
    Interface id: 0 (\Device\NPF_{D65F1827-D907-40D0-A2A1-624ED0E88D6A})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 24, 2025 20:04:42.828585000 Eastern Standard Time
    UTC Arrival Time: Feb 25, 2025 01:04:42.828585000 UTC
    Epoch Arrival Time: 1740445482.828585000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000770000 seconds]
    [Time delta from previous displayed frame: 0.051544000 seconds]
    [Time since reference or first frame: 49.178873000 seconds]
    Frame Number: 1949
    Frame Length: 540 bytes (4320 bits)
    Capture Length: 540 bytes (4320 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Commscope_17:1c:c6 (1c:93:7c:17:1c:c6), Dst: Intel_5d:24:65 (18:93:41:5d:24:65)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.50
Transmission Control Protocol, Src Port: 80, Dst Port: 64349, Seq: 1, Ack: 420, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n

0000  18 93 41 5d 24 65 1c 93  7c 17 1c c6 08 00 45 00   ··A]$e·· |·····E·
0010  02 0e 6e c9 40 00 2d 06  5d 6b 80 77 f5 0c 0a 00   ··n·@·-· ]k·w····
0020  00 32 00 50 fb 5d fa aa  2c 2c 77 60 86 69 50 18   ·2·P·]·· ,,w`·iP·
0030  00 ed 86 05 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 54 75 65   00 OK··D ate: Tue
0050  2c 20 32 35 20 46 65 62  20 32 30 32 35 20 30 31   , 25 Feb  2025 01
0060  3a 30 34 3a 34 31 20 47  4d 54 0d 0a 53 65 72 76   :04:41 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

No.: 1949 · Time: 49.178873 · Source: 128.119.245.12 · Destination: 10.0.0.50 · Protocol: HTTP · Length: 540 · Info: HTTP/1.1 200 OK (text/html)
```

✓ Show packet bytes   Layout: Vertical (Stacked)

```
No.   Time
1397 33.925
1401 33.928
1405 33.945
1424 33.965
1433 34.033
1435 34.055
1437 34.082
1439 35.377
1449 35.449
1451 35.510
1452 35.515
1453 35.515
1454 35.515
1455 35.515
1456 35.515
1458 35.537
1460 35.537
1462 35.540
1464 35.540
1466 35.545
1468 35.546
1470 35.547
1474 35.547
1475 35.547
1477 35.554
1479 35.573
1481 35.575
1484 35.577
1498 35.681
1515 38.057
1699 38.241
1712 38.282
1714 38.301
1758 44.236                                                                        691343&P2=4…
1759 44.270
1763 44.315                                                                        91343&P2=40…
1878 44.408
1947 49.127329   10.0.0.50        128.119.245.12   HTTP    473 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1949 49.178873   128.119.245.12   10.0.0.50        HTTP    540 HTTP/1.1 200 OK  (text/html)
1953 49.356446   10.0.0.50        128.119.245.12   HTTP    493 GET /favicon.ico HTTP/1.1
1954 49.404050   128.119.245.12   10.0.0.50        HTTP    538 HTTP/1.1 404 Not Found  (text/html)
```

```
Frame 1949: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on inter
    Section number: 1
    Interface id: 0 (\Device\NPF_{D65F1827-D907-40D0-A2A1-624ED0E88D6A})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 24, 2025 20:04:42.828585000 Eastern Standard Time
    UTC Arrival Time: Feb 25, 2025 01:04:42.828585000 UTC
    Epoch Arrival Time: 1740445482.828585000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000770000 seconds]
    [Time delta from previous displayed frame: 0.051544000 seconds]
    [Time since reference or first frame: 49.178873000 seconds]
    Frame Number: 1949
    Frame Length: 540 bytes (4320 bits)
    Capture Length: 540 bytes (4320 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Commscope_17:1c:c6 (1c:93:7c:17:1c:c6), Dst: Intel_5d:24:65 (18:9
    Destination: Intel_5d:24:65 (18:93:41:5d:24:65)
    Source: Commscope_17:1c:c6 (1c:93:7c:17:1c:c6)
    Type: IPv4 (0x0800)
    [Stream index: 1]
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.50
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 526
    Identification: 0x6ec9 (28361)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 45
    Protocol: TCP (6)
    Header Checksum: 0x5d6b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 10.0.0.50
    [Stream index: 35]
Transmission Control Protocol, Src Port: 80, Dst Port: 64349, Seq: 1, Ack: 420, Len
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
```

```
0000  18 93 41 5d 24 65 1c 93  7c 17 1c c6 08 00 45 00   ··A]$e·· |·····E·
0010  02 0e 6e c9 40 00 2d 06  5d 6b 80 77 f5 0c 0a 00   ··n·@·-· ]k·w····
0020  00 32 00 50 fb 5d fa aa  2c 2c 77 60 86 69 50 18   ·2·P·]·· ,,w`·iP·
0030  00 ed 86 05 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 54 75 65   00 OK··D ate: Tue
0050  2c 20 32 35 20 46 65 62  20 32 30 32 35 20 30 31   , 25 Feb  2025 01
0060  3a 30 34 3a 34 31 20 47  4d 54 0d 0a 53 65 72 76   :04:41 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 4d 6f  6e 2c 20 32 34 20 46 65   fied: Mo n, 24 Fe
00e0  62 20 32 30 32 35 20 30  36 3a 35 39 3a 30 31 20   b 2025 0 6:59:01 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 36   GMT··ETa g: "80-6
0100  32 65 64 64 65 30 30 38  31 36 39 65 22 0d 0a 41   2edde008 169e"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54 50 2d 77 69   ark-labs /HTTP-wi
0200  72 65 73 68 61 72 6b 2d  66 69 6c 65 31 2e 68 74   reshark- file1.ht
0210  6d 6c 21 0a 3c 2f 68 74  6d 6c 3e 0a               ml!·</ht ml>·
```

It is important to access the HTTP version and not the HTPPS version because we're using Wireshark to capture and analyze HTTP messages. Wireshark monitors the network traffic where HTTP traffic is transmitted in plaintext. This process makes it easy for Wireshark to capture and display the GET request and the HTTP response along with other headers and messages. HTTPS has a secure connection (SSL), which means that it is encrypted. Therefore, capturing traffic in HTTPS is futile since even if we can capture it, the packets won't be available for view. In everyday use, however, HTTPS is preferable because it encrypts the communication between the browser and the web server. Thu, all sensitive information such as payments or login credentials are protected. In HTTP connection it's known that anyone can monitor the network and can have a look at the data.

2. My browser is running HTTP version 1.1. The server is running version 1.1.

3. My browser indicates that it can accept Canadian and American languages.

4. 20:04:42.777041000 and 20:04:42.828585000

   RTT = 0.051544000 seconds or 51.544 milliseconds.

5. The status code returned is 200 OK.

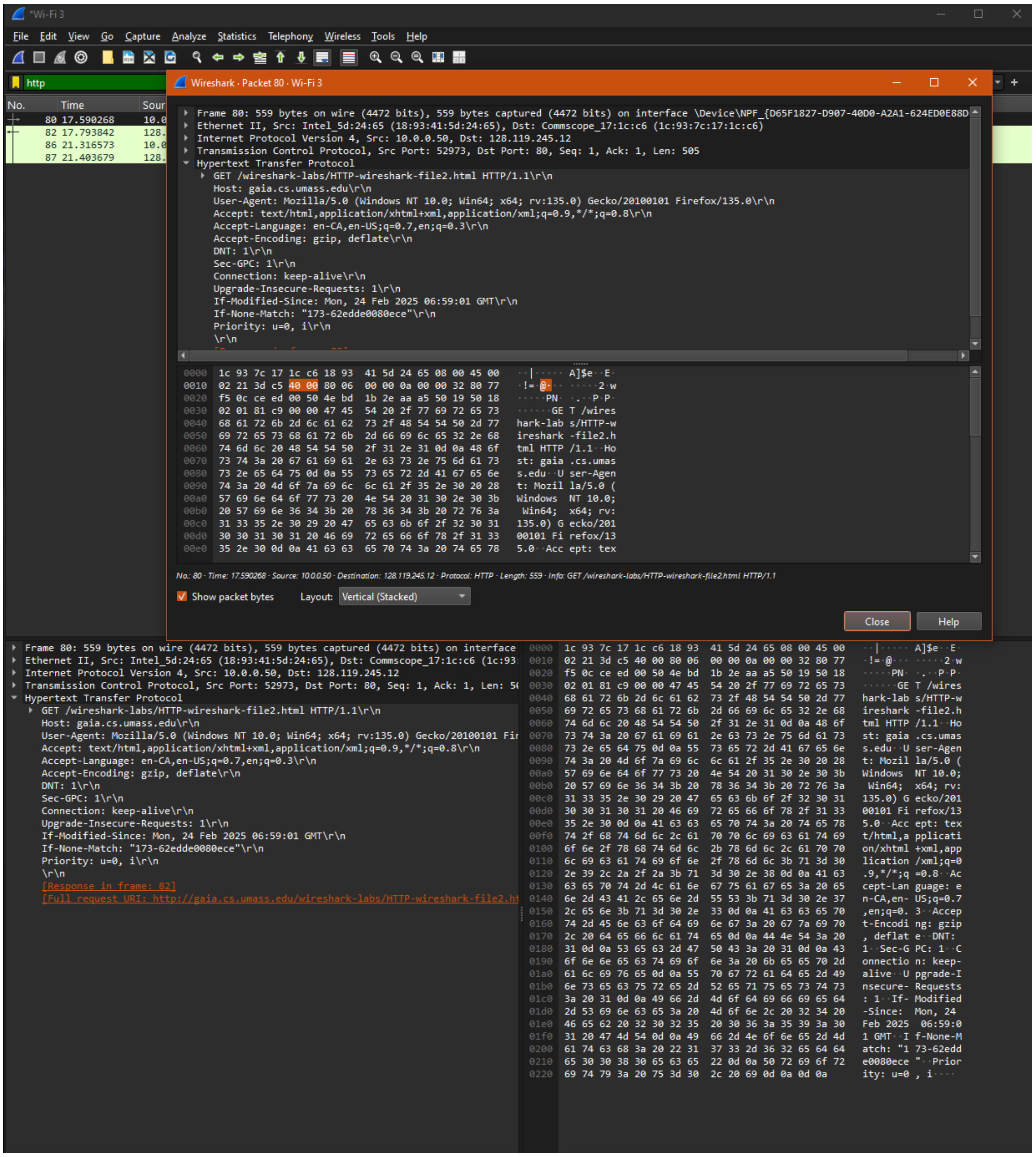
6. Last modified : Mon, 24 Feb 2025 06:59:01 GMT.

7. 540 bytes are being returned.

8. Header missing is TCP segment data (#bytes)

TASK 2

9. I see it when not removing the cache, If-Modified-Since: Mon, 24 Feb 2025 06:59:01 GMT


*Wi-Fi 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Wireshark · Packet 80 · Wi-Fi 3

```
No.   Time       Sour
 80 17.590268    10.0
 82 17.793842    128.
 86 21.316573    10.0
 87 21.403679    128.
```

```
Frame 80: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{D65F1827-D907-40D0-A2A1-624ED0E88D
Ethernet II, Src: Intel_5d:24:65 (18:93:41:5d:24:65), Dst: Commscope_17:1c:c6 (1c:93:7c:17:1c:c6)
Internet Protocol Version 4, Src: 10.0.0.50, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52973, Dst Port: 80, Seq: 1, Ack: 1, Len: 505
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-CA,en-US;q=0.7,en;q=0.3\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Sec-GPC: 1\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  If-Modified-Since: Mon, 24 Feb 2025 06:59:01 GMT\r\n
  If-None-Match: "173-62edde0080ece"\r\n
  Priority: u=0, i\r\n
  \r\n
```

```
0000  1c 93 7c 17 1c c6 18 93  41 5d 24 65 08 00 45 00   ··|····· A]$e··E·
0010  02 21 3d c5 40 00 80 06  00 00 0a 00 00 32 80 77   ·!=·@··· ·····2·w
0020  f5 0c ce ed 00 50 4e bd  1b 2e aa a5 50 19 50 18   ·····PN· ·.··P·P·
0030  02 01 81 c9 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
00b0  20 57 69 6e 36 34 3b 20  78 36 34 3b 20 72 76 3a    Win64;  x64; rv:
00c0  31 33 35 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   135.0) G ecko/201
00d0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 31 33   00101 Fi refox/13
00e0  35 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   5.0··Acc ept: tex
```

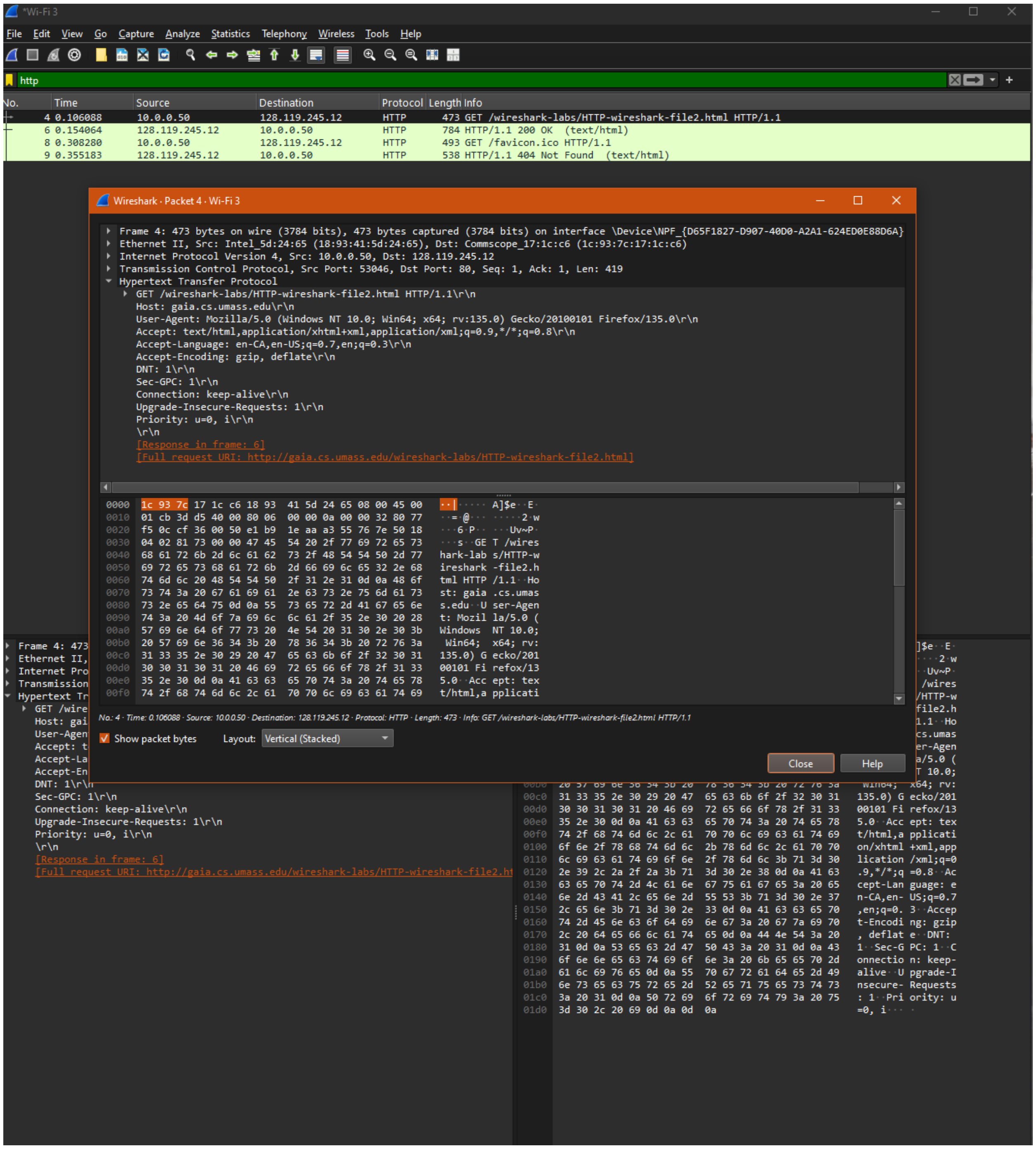
No.: 80 · Time: 17.590268 · Source: 10.0.0.50 · Destination: 128.119.245.12 · Protocol: HTTP · Length: 559 · Info: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

✓ Show packet bytes   Layout: Vertical (Stacked)

```
Frame 80: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface
Ethernet II, Src: Intel_5d:24:65 (18:93:41:5d:24:65), Dst: Commscope_17:1c:c6 (1c:93
Internet Protocol Version 4, Src: 10.0.0.50, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52973, Dst Port: 80, Seq: 1, Ack: 1, Len: 5
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Fir
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-CA,en-US;q=0.7,en;q=0.3\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Sec-GPC: 1\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  If-Modified-Since: Mon, 24 Feb 2025 06:59:01 GMT\r\n
  If-None-Match: "173-62edde0080ece"\r\n
  Priority: u=0, i\r\n
  \r\n
  [Response in frame: 82]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.ht
```

```
0000  1c 93 7c 17 1c c6 18 93  41 5d 24 65 08 00 45 00   ··|····· A]$e··E·
0010  02 21 3d c5 40 00 80 06  00 00 0a 00 00 32 80 77   ·!=·@··· ·····2·w
0020  f5 0c ce ed 00 50 4e bd  1b 2e aa a5 50 19 50 18   ·····PN· ·.··P·P·
0030  02 01 81 c9 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
00b0  20 57 69 6e 36 34 3b 20  78 36 34 3b 20 72 76 3a    Win64;  x64; rv:
00c0  31 33 35 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   135.0) G ecko/201
00d0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 31 33   00101 Fi refox/13
00e0  35 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   5.0··Acc ept: tex
00f0  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
0100  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
0110  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
0120  2e 39 2c 2a 2f 2a 3b 71  3d 30 2e 38 0d 0a 41 63   .9,*/*;q =0.8··Ac
0130  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 65   cept-Lan guage: e
0140  6e 2d 43 41 2c 65 6e 2d  55 53 3b 71 3d 30 2e 37   n-CA,en- US;q=0.7
0150  2c 65 6e 3b 71 3d 30 2e  33 0d 0a 41 63 63 65 70   ,en;q=0. 3··Accep
0160  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi ng: gzip
0170  2c 20 64 65 66 6c 61 74  65 0d 0a 44 4e 54 3a 20   , deflat e··DNT: 
0180  31 0d 0a 53 65 63 2d 47  50 43 3a 20 31 0d 0a 43   1··Sec-G PC: 1··C
0190  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
01a0  61 6c 69 76 65 0d 0a 55  70 67 72 61 64 65 2d 49   alive··U pgrade-I
01b0  6e 73 65 63 75 72 65 2d  52 65 71 75 65 73 74 73   nsecure- Requests
01c0  3a 20 31 0d 0a 49 66 2d  4d 6f 64 69 66 69 65 64   : 1··If- Modified
01d0  2d 53 69 6e 63 65 3a 20  4d 6f 6e 2c 20 32 34 20   -Since:  Mon, 24 
01e0  46 65 62 20 32 30 32 35  20 30 36 3a 35 39 3a 30   Feb 2025  06:59:0
01f0  31 20 47 4d 54 0d 0a 49  66 2d 4e 6f 6e 65 2d 4d   1 GMT··I f-None-M
0200  61 74 63 68 3a 20 22 31  37 33 2d 36 32 65 64 64   atch: "1 73-62edd
0210  65 30 30 38 30 65 63 65  22 0d 0a 50 72 69 6f 72   e0080ece "··Prior
0220  69 74 79 3a 20 75 3d 30  2c 20 69 0d 0a 0d 0a      ity: u=0 , i····
```

When I delete the cache, I do not see it.



```
No.  Time        Source          Destination     Protocol Length Info
   4 0.106088    10.0.0.50       128.119.245.12  HTTP     473 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   6 0.154064    128.119.245.12  10.0.0.50       HTTP     784 HTTP/1.1 200 OK  (text/html)
   8 0.308280    10.0.0.50       128.119.245.12  HTTP     493 GET /favicon.ico HTTP/1.1
   9 0.355183    128.119.245.12  10.0.0.50       HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
Frame 4: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{D65F1827-D907-40D0-A2A1-624ED0E88D6A}
Ethernet II, Src: Intel_5d:24:65 (18:93:41:5d:24:65), Dst: Commscope_17:1c:c6 (1c:93:7c:17:1c:c6)
Internet Protocol Version 4, Src: 10.0.0.50, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53046, Dst Port: 80, Seq: 1, Ack: 1, Len: 419
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-CA,en-US;q=0.7,en;q=0.3\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Sec-GPC: 1\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i\r\n
  \r\n
  [Response in frame: 6]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

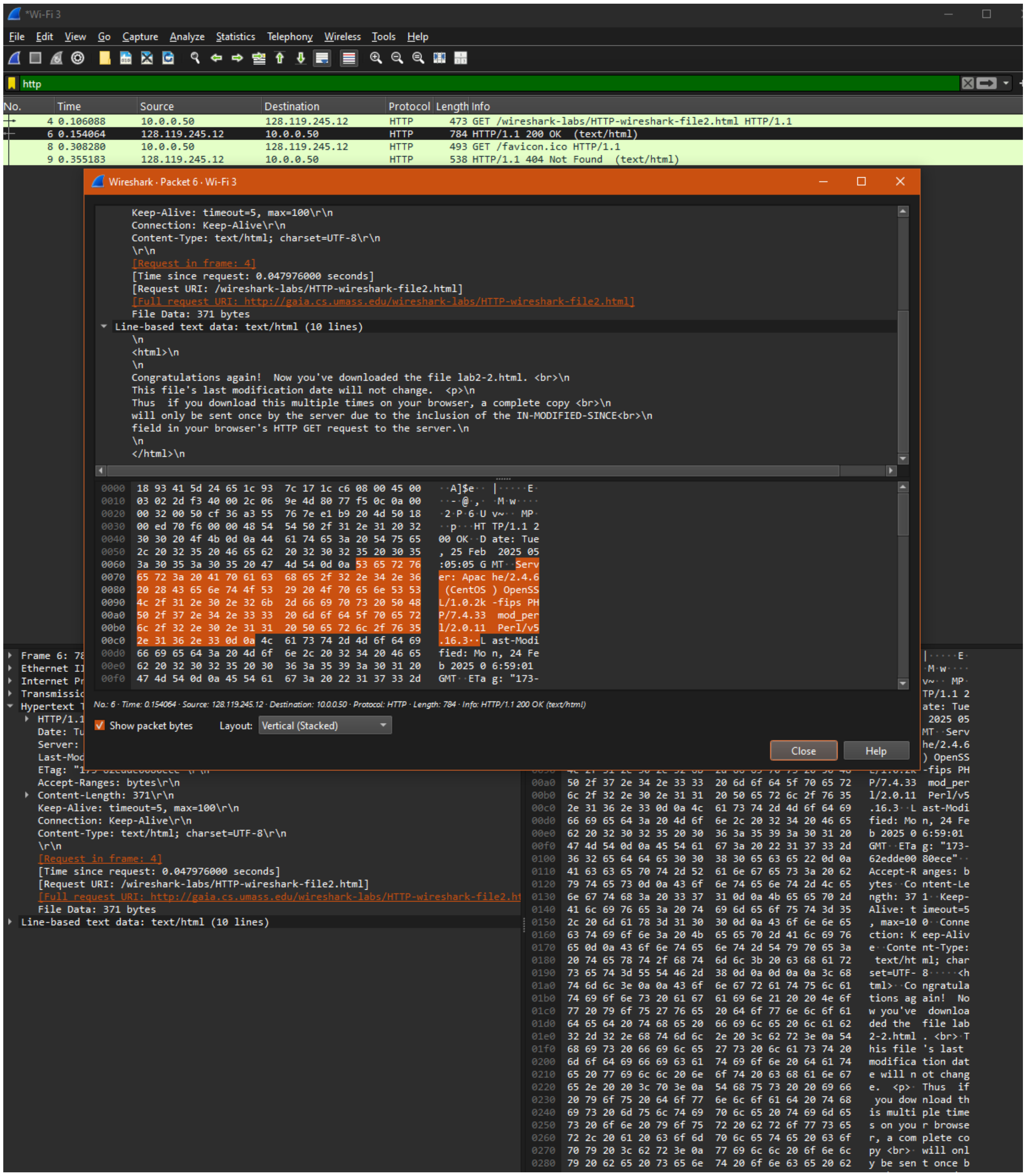
```
0000  1c 93 7c 17 1c c6 18 93  41 5d 24 65 08 00 45 00   ··|····· A]$e··E·
0010  01 cb 3d d5 40 00 80 06  00 00 0a 00 00 32 80 77   ··=·@··· ·····2·w
0020  f5 0c cf 36 00 50 e1 b9  1e aa a3 55 76 7e 50 18   ···6·P·· ···Uv~P·
0030  04 02 81 73 00 00 47 45  54 20 2f 77 69 72 65 73   ···s··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
00b0  20 57 69 6e 36 34 3b 20  78 36 34 3b 20 72 76 3a    Win64;  x64; rv:
00c0  31 33 35 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   135.0) G ecko/201
00d0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 31 33   00101 Fi refox/13
00e0  35 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   5.0··Acc ept: tex
00f0  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
```

No.: 4 · Time: 0.106088 · Source: 10.0.0.50 · Destination: 128.119.245.12 · Protocol: HTTP · Length: 473 · Info: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Show packet bytes ✓   Layout: Vertical (Stacked)

```
0100  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
0110  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
0120  2e 39 2c 2a 2f 2a 3b 71  3d 30 2e 38 0d 0a 41 63   .9,*/*;q =0.8··Ac
0130  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 65   cept-Lan guage: e
0140  6e 2d 43 41 2c 65 6e 2d  55 53 3b 71 3d 30 2e 37   n-CA,en- US;q=0.7
0150  2c 65 6e 3b 71 3d 30 2e  33 0d 0a 41 63 63 65 70   ,en;q=0. 3··Accep
0160  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi ng: gzip
0170  2c 20 64 65 66 6c 61 74  65 0d 0a 44 4e 54 3a 20   , deflat e··DNT: 
0180  31 0d 0a 53 65 63 2d 47  50 43 3a 20 31 0d 0a 43   1··Sec-G PC: 1··C
0190  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
01a0  61 6c 69 76 65 0d 0a 55  70 67 72 61 64 65 2d 49   alive··U pgrade-I
01b0  6e 73 65 63 75 72 65 2d  52 65 71 75 65 73 74 73   nsecure- Requests
01c0  3a 20 31 0d 0a 50 72 69  6f 72 69 74 79 3a 20 75   : 1··Pri ority: u
01d0  3d 30 2c 20 69 0d 0a 0d  0a                        =0, i····
```

10. When I open the content-length and line-based text data, I can see all the details.



*Wi-Fi 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.  Time       Source          Destination     Protocol Length Info
   4 0.106088   10.0.0.50       128.119.245.12  HTTP     473 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   6 0.154064   128.119.245.12  10.0.0.50       HTTP     784 HTTP/1.1 200 OK  (text/html)
   8 0.308280   10.0.0.50       128.119.245.12  HTTP     493 GET /favicon.ico HTTP/1.1
   9 0.355183   128.119.245.12  10.0.0.50       HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

Wireshark · Packet 6 · Wi-Fi 3

```
        Keep-Alive: timeout=5, max=100\r\n
        Connection: Keep-Alive\r\n
        Content-Type: text/html; charset=UTF-8\r\n
        \r\n
        [Request in frame: 4]
        [Time since request: 0.047976000 seconds]
        [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
        [Full 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
```

```
0000  18 93 41 5d 24 65 1c 93  7c 17 1c c6 08 00 45 00   ··A]$e·· |·····E·
0010  03 02 2d f3 40 00 2c 06  9e 4d 80 77 f5 0c 0a 00   ··-·@·,· ·M·w····
0020  00 32 00 50 cf 36 a3 55  76 7e e1 b9 20 4d 50 18   ·2·P·6·U v~·· MP·
0030  00 ed 70 f6 00 00 48 54  54 50 2f 31 2e 31 20 32   ··p···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK··D ate: Tue
0050  2c 20 32 35 20 46 65 62  20 32 30 32 35 20 30 35   , 25 Feb  2025 05
0060  3a 30 35 3a 30 35 20 47  4d 54 0d 0a 53 65 72 76   :05:05 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 4d 6f  6e 2c 20 32 34 20 46 65   fied: Mo n, 24 Fe
00e0  62 20 32 30 32 35 20 30  36 3a 35 39 3a 30 31 20   b 2025 0 6:59:01
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 37 33 2d   GMT··ETa g: "173-
```

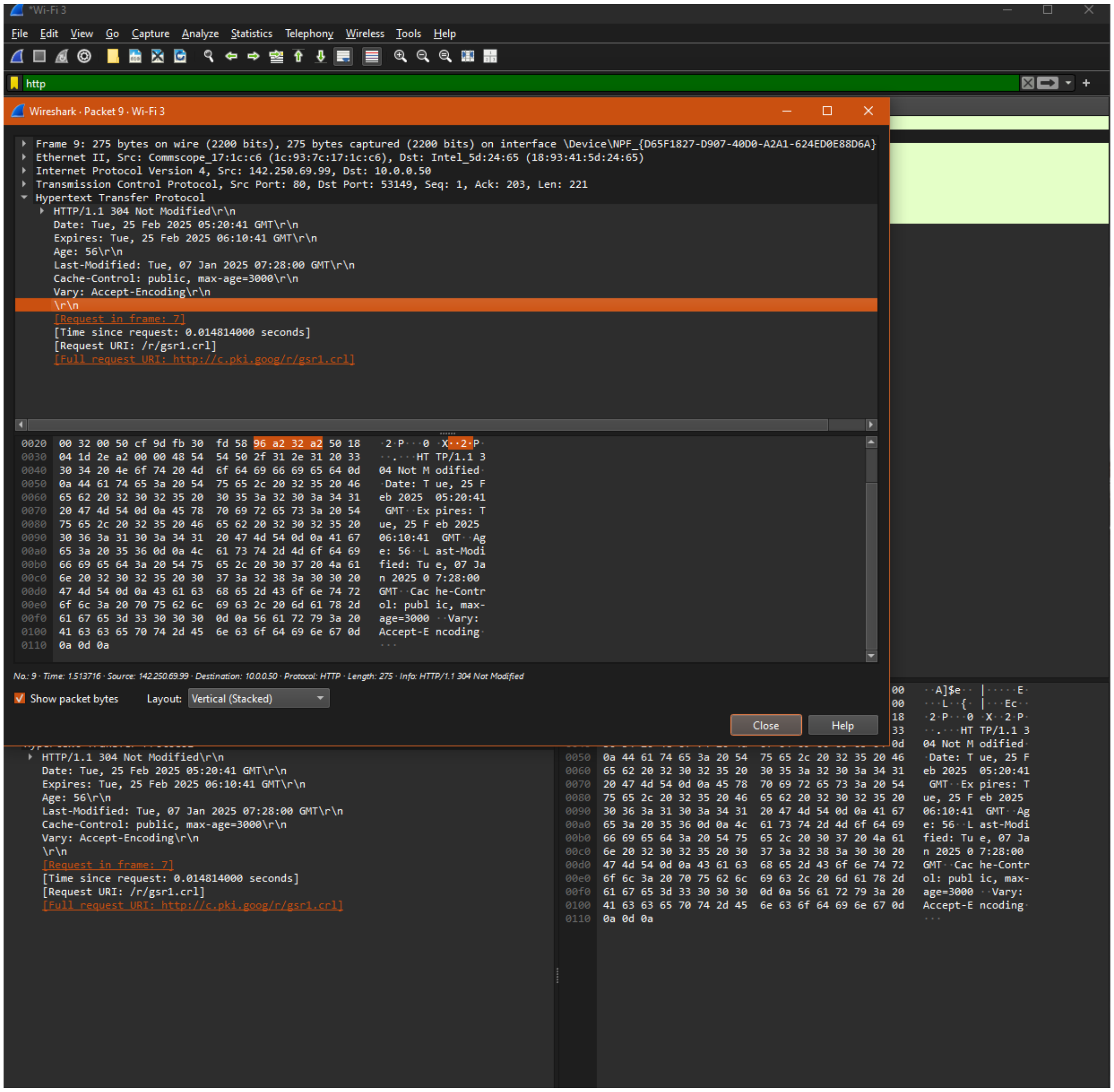
No.: 6 · Time: 0.154064 · Source: 128.119.245.12 · Destination: 10.0.0.50 · Protocol: HTTP · Length: 784 · Info: HTTP/1.1 200 OK (text/html)

```
Frame 6: 78
Ethernet II
Internet Pr
Transmissic
Hypertext T
    HTTP/1.1
    Date: Tu
    Server:
    Last-Moc
    ETag: "1
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 4]
    [Time since request: 0.047976000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.ht
    File Data: 371 bytes
Line-based text data: text/html (10 lines)
```

```
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 4d 6f  6e 2c 20 32 34 20 46 65   fied: Mo n, 24 Fe
00e0  62 20 32 30 32 35 20 30  36 3a 35 39 3a 30 31 20   b 2025 0 6:59:01
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 37 33 2d   GMT··ETa g: "173-
0100  36 32 65 64 64 65 30 30  38 30 65 63 65 22 0d 0a   62edde00 80ece"··
0110  41 63 63 65 70 74 2d 52  61 6e 67 65 73 3a 20 62   Accept-R anges: b
0120  79 74 65 73 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   ytes··Co ntent-Le
0130  6e 67 74 68 3a 20 33 37  31 0d 0a 4b 65 65 70 2d   ngth: 37 1··Keep-
0140  41 6c 69 76 65 3a 20 74  69 6d 65 6f 75 74 3d 35   Alive: t imeout=5
0150  2c 20 6d 61 78 3d 31 30  30 0d 0a 43 6f 6e 6e 65   , max=10 0··Conne
0160  63 74 69 6f 6e 3a 20 4b  65 65 70 2d 41 6c 69 76   ction: K eep-Aliv
0170  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
0180  20 74 65 78 74 2f 68 74  6d 6c 3b 20 63 68 61 72    text/ht ml; char
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8·····<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>··Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
01e0  32 2d 32 2e 68 74 6d 6c  2e 20 3c 62 72 3e 0a 54   2-2.html . <br>·T
01f0  68 69 73 20 66 69 6c 65  27 73 20 6c 61 73 74 20   his file 's last
0200  6d 6f 64 69 66 69 63 61  74 69 6f 6e 20 64 61 74   modifica tion dat
0210  65 20 77 69 6c 6c 20 6e  6f 74 20 63 68 61 6e 67   e will n ot chang
0220  65 2e 20 20 3c 70 3e 0a  54 68 75 73 20 20 69 66   e.  <p>· Thus  if
0230  20 79 6f 75 20 64 6f 77  6e 6c 6f 61 64 20 74 68    you dow nload th
0240  69 73 20 6d 75 6c 74 69  70 6c 65 20 74 69 6d 65   is multi ple time
0250  73 20 6f 6e 20 79 6f 75  72 20 62 72 6f 77 73 65   s on you r browse
0260  72 2c 20 61 20 63 6f 6d  70 6c 65 74 65 20 63 6f   r, a com plete co
0270  70 79 20 3c 62 72 3e 0a  77 69 6c 6c 20 6f 6e 6c   py <br>· will onl
0280  79 20 62 65 20 73 65 6e  74 20 6f 6e 63 65 20 62   y be sen t once b
```

11. Like question 9, it only shows when the cache is not cleared. Otherwise, I can see it with those details If-Modified-Since: Mon, 24 Feb 2025 06:59:01.

12. The packet info reads “not modified” and the status code is 304. The server did not explicitly return the contents of the file this time as it was mentioned previously that if the cache is not cleared, the server will only send one copy of the file due to the inclusion of the If-Modified-Since.



Wireshark · Packet 9 · Wi-Fi 3

```
Frame 9: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits) on interface \Device\NPF_{D65F1827-D907-40D0-A2A1-624ED0E88D6A}
Ethernet II, Src: Commscope_17:1c:c6 (1c:93:7c:17:1c:c6), Dst: Intel_5d:24:65 (18:93:41:5d:24:65)
Internet Protocol Version 4, Src: 142.250.69.99, Dst: 10.0.0.50
Transmission Control Protocol, Src Port: 80, Dst Port: 53149, Seq: 1, Ack: 203, Len: 221
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Tue, 25 Feb 2025 05:20:41 GMT\r\n
    Expires: Tue, 25 Feb 2025 06:10:41 GMT\r\n
    Age: 56\r\n
    Last-Modified: Tue, 07 Jan 2025 07:28:00 GMT\r\n
    Cache-Control: public, max-age=3000\r\n
    Vary: Accept-Encoding\r\n
    \r\n
    [Request in frame: 7]
    [Time since request: 0.014814000 seconds]
    [Request URI: /r/gsr1.crl]
    [Full request URI: http://c.pki.goog/r/gsr1.crl]
```

```
0020  00 32 00 50 cf 9d fb 30  fd 58 96 a2 32 a2 50 18   ·2·P···0 ·X··2·P·
0030  04 1d 2e a2 00 00 48 54  54 50 2f 31 2e 31 20 33   ··.···HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 44 61 74 65 3a 20 54  75 65 2c 20 32 35 20 46   ·Date: T ue, 25 F
0060  65 62 20 32 30 32 35 20  30 35 3a 32 30 3a 34 31   eb 2025  05:20:41
0070  20 47 4d 54 0d 0a 45 78  70 69 72 65 73 3a 20 54    GMT··Ex pires: T
0080  75 65 2c 20 32 35 20 46  65 62 20 32 30 32 35 20   ue, 25 F eb 2025
0090  30 36 3a 31 30 3a 34 31  20 47 4d 54 0d 0a 41 67   06:10:41  GMT··Ag
00a0  65 3a 20 35 36 0d 0a 4c  61 73 74 2d 4d 6f 64 69   e: 56··L ast-Modi
00b0  66 69 65 64 3a 20 54 75  65 2c 20 30 37 20 4a 61   fied: Tu e, 07 Ja
00c0  6e 20 32 30 32 35 20 30  37 3a 32 38 3a 30 30 20   n 2025 0 7:28:00
00d0  47 4d 54 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72   GMT··Cac he-Contr
00e0  6f 6c 3a 20 70 75 62 6c  69 63 2c 20 6d 61 78 2d   ol: publ ic, max-
00f0  61 67 65 3d 33 30 30 30  0d 0a 56 61 72 79 3a 20   age=3000 ··Vary:
0100  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 0d   Accept-E ncoding·
0110  0a 0d 0a                                            ···
```

No.: 9 · Time: 1.513716 · Source: 142.250.69.99 · Destination: 10.0.0.50 · Protocol: HTTP · Length: 275 · Info: HTTP/1.1 304 Not Modified

Show packet bytes ✓ Layout: Vertical (Stacked)

```
    HTTP/1.1 304 Not Modified\r\n
    Date: Tue, 25 Feb 2025 05:20:41 GMT\r\n
    Expires: Tue, 25 Feb 2025 06:10:41 GMT\r\n
    Age: 56\r\n
    Last-Modified: Tue, 07 Jan 2025 07:28:00 GMT\r\n
    Cache-Control: public, max-age=3000\r\n
    Vary: Accept-Encoding\r\n
    \r\n
    [Request in frame: 7]
    [Time since request: 0.014814000 seconds]
    [Request URI: /r/gsr1.crl]
    [Full request URI: http://c.pki.goog/r/gsr1.crl]
```

```
0050  0a 44 61 74 65 3a 20 54  75 65 2c 20 32 35 20 46   ·Date: T ue, 25 F
0060  65 62 20 32 30 32 35 20  30 35 3a 32 30 3a 34 31   eb 2025  05:20:41
0070  20 47 4d 54 0d 0a 45 78  70 69 72 65 73 3a 20 54    GMT··Ex pires: T
0080  75 65 2c 20 32 35 20 46  65 62 20 32 30 32 35 20   ue, 25 F eb 2025
0090  30 36 3a 31 30 3a 34 31  20 47 4d 54 0d 0a 41 67   06:10:41  GMT··Ag
00a0  65 3a 20 35 36 0d 0a 4c  61 73 74 2d 4d 6f 64 69   e: 56··L ast-Modi
00b0  66 69 65 64 3a 20 54 75  65 2c 20 30 37 20 4a 61   fied: Tu e, 07 Ja
00c0  6e 20 32 30 32 35 20 30  37 3a 32 38 3a 30 30 20   n 2025 0 7:28:00
00d0  47 4d 54 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72   GMT··Cac he-Contr
00e0  6f 6c 3a 20 70 75 62 6c  69 63 2c 20 6d 61 78 2d   ol: publ ic, max-
00f0  61 67 65 3d 33 30 30 30  0d 0a 56 61 72 79 3a 20   age=3000 ··Vary:
0100  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 0d   Accept-E ncoding·
0110  0a 0d 0a                                            ···
```

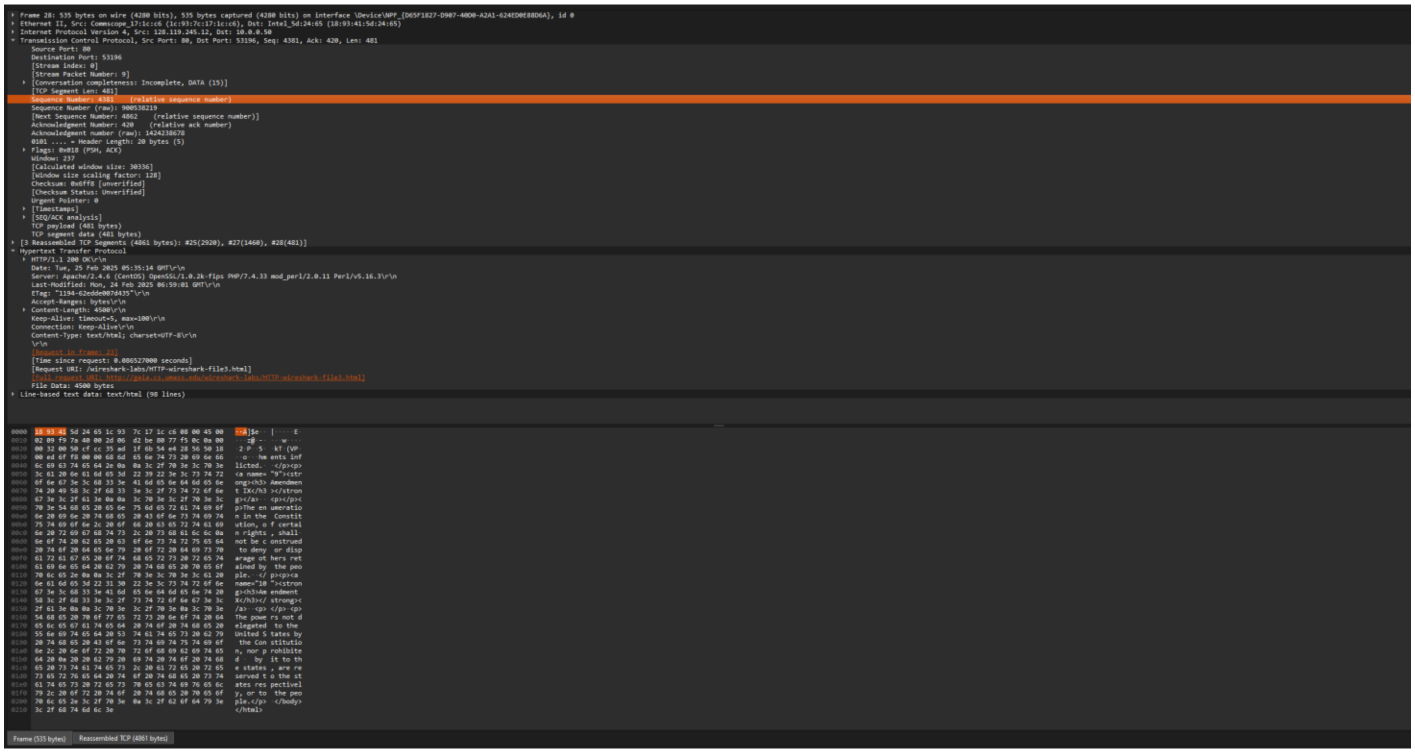
TASK 3

13. My browser sent 2 HTTP GET requests.

14. For the first request it's 200 OK, for the second 404 Not Found.

15. 4381 segments were needed to carry the single HTTP response.

16. Overhead refers to the additional resources used in a network protocol. Examples are TCP, HTTP, etc. Every TCP segment contains a header that holds a certain number of bytes. Those headers contain crucial information to manage and maintain the connection. Some headers are destination port or sequence numbers.



```
Frame 28: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{D65F1827-D907-40D0-A2A1-624ED0E88D6A}, id 0
Ethernet II, Src: Commscope_17:1c:c6 (1c:93:7c:17:1c:c6), Dst: Intel_5d:24:65 (18:93:41:5d:24:65)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.50
Transmission Control Protocol, Src Port: 80, Dst Port: 53196, Seq: 4381, Ack: 420, Len: 481
    Source Port: 80
    Destination Port: 53196
    [Stream index: 0]
    [Stream Packet Number: 9]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 481]
    Sequence Number: 4381    (relative sequence number)
    Sequence Number (raw): 900538219
    [Next Sequence Number: 4862    (relative sequence number)]
    Acknowledgment Number: 420    (relative ack number)
    Acknowledgment number (raw): 1424238678
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x6ff8 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (481 bytes)
    TCP segment data (481 bytes)
[3 Reassembled TCP Segments (4861 bytes): #25(2920), #27(1460), #28(481)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 25 Feb 2025 05:35:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 24 Feb 2025 06:59:01 GMT\r\n
    ETag: "1194-62edde007d435"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 23]
    [Time since request: 0.086527000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file3.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
Line-based text data: text/html (98 lines)
```

```
0000  18 93 41 5d 24 65 1c 93  7c 17 1c c6 08 00 45 00   ··A]$e·· |·····E·
0010  02 09 f9 7a 40 00 2d 06  d2 be 80 77 f5 0c 0a 00   ···z@·-· ···w····
0020  00 32 00 50 cf cc 35 ad  1f 6b 54 e4 28 56 50 18   ·2·P··5· ·kT·(VP·
0030  00 ed 6f f8 00 00 68 6d  65 6e 74 73 20 69 6e 66   ··o···hm ents inf
0040  6c 69 63 74 65 64 2e 0a  0a 3c 2f 70 3e 3c 70 3e   licted.· ·</p><p>
0050  3c 61 20 6e 61 6d 65 3d  22 39 22 3e 3c 73 74 72   <a name= "9"><str
0060  6f 6e 67 3e 3c 68 33 3e  41 6d 65 6e 64 6d 65 6e   ong><h3> Amendmen
0070  74 20 49 58 3c 2f 68 33  3e 3c 2f 73 74 72 6f 6e   t IX</h3 ></stron
0080  67 3e 3c 2f 61 3e 0a 0a  3c 70 3e 3c 2f 70 3e 3c   g></a>·· <p></p><
0090  70 3e 54 68 65 20 65 6e  75 6d 65 72 61 74 69 6f   p>The en umeratio
00a0  6e 20 69 6e 20 74 68 65  20 43 6f 6e 73 74 69 74   n in the  Constit
00b0  75 74 69 6f 6e 2c 20 6f  66 20 63 65 72 74 61 69   ution, o f certai
00c0  6e 20 72 69 67 68 74 73  2c 20 73 68 61 6c 6c 0a   n rights , shall·
00d0  6e 6f 74 20 62 65 20 63  6f 6e 73 74 72 75 65 64   not be c onstrued
00e0  20 74 6f 20 64 65 6e 79  20 6f 72 20 64 69 73 70    to deny  or disp
00f0  61 72 61 67 65 20 6f 74  68 65 72 73 20 72 65 74   arage ot hers ret
0100  61 69 6e 65 64 20 62 79  20 74 68 65 20 70 65 6f   ained by  the peo
0110  70 6c 65 2e 0a 0a 3c 2f  70 3e 3c 70 3e 3c 61 20   ple.··</ p><p><a 
0120  6e 61 6d 65 3d 22 31 30  22 3e 3c 73 74 72 6f 6e   name="10 "><stron
0130  67 3e 3c 68 33 3e 41 6d  65 6e 64 6d 65 6e 74 20   g><h3>Am endment 
0140  58 3c 2f 68 33 3e 3c 2f  73 74 72 6f 6e 67 3e 3c   X</h3></ strong><
0150  2f 61 3e 0a 0a 3c 70 3e  3c 2f 70 3e 0a 3c 70 3e   /a>··<p> </p>·<p>
0160  54 68 65 20 70 6f 77 65  72 73 20 6e 6f 74 20 64   The powe rs not d
0170  65 6c 65 67 61 74 65 64  20 74 6f 20 74 68 65 20   elegated  to the 
0180  55 6e 69 74 65 64 20 53  74 61 74 65 73 20 62 79   United S tates by
0190  20 74 68 65 20 43 6f 6e  73 74 69 74 75 74 69 6f    the Con stitutio
01a0  6e 2c 20 6e 6f 72 20 70  72 6f 68 69 62 69 74 65   n, nor p rohibite
01b0  64 20 0a 20 20 62 79 20  69 74 20 74 6f 20 74 68   d ·  by  it to th
01c0  65 20 73 74 61 74 65 73  2c 20 61 72 65 20 72 65   e states , are re
01d0  73 65 72 76 65 64 20 74  6f 20 74 68 65 20 73 74   served t o the st
01e0  61 74 65 73 20 72 65 73  70 65 63 74 69 76 65 6c   ates res pectivel
01f0  79 2c 20 6f 72 20 74 6f  20 74 68 65 20 70 65 6f   y, or to  the peo
0200  70 6c 65 2e 3c 2f 70 3e  0a 3c 2f 62 6f 64 79 3e   ple.</p> ·</body>
0210  3c 2f 68 74 6d 6c 3e                               </html>
```

Total TCP Overhead = number of TCP segments x TCP header size

Total TCP Overhead = 4381 x 20 = 87620 bytes

HTTP Response Data is 4500 bytes, from the content-length.

Total Data Transmitted is HTTP Response Data + TCP Overhead

Total Data Transmitted is then 4500 bytes + 87620 bytes = 92120 bytes.

To calculate the percentage of TCP Overhead:

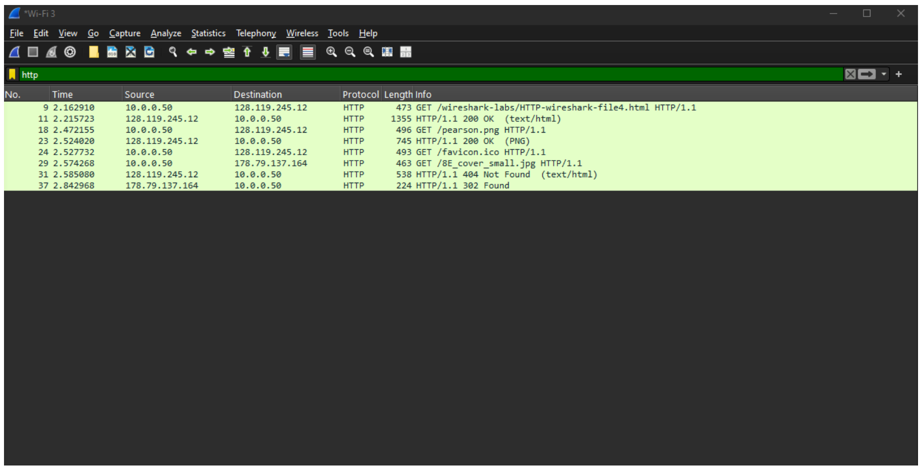
(TCP Overhead / Total Data Transmitted) x 100 = 95.1%

Therefore, TCP Overhead makes 95.1% of the total transmitted data which includes both HTTP response and the TCP headers. This number seem a bit high since data transfer is usually lower than that, but in this example it's normal since our HTML file is rather long and 4500 bytes is too large.

TASK 4

17. My browser sent 4 GET requests. They were sent to 128.119.245.12 and 178.79.137.164.

18.


*Wi-Fi 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time      Source          Destination     Protocol Length Info
   9 2.162910  10.0.0.50       128.119.245.12  HTTP      473 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  11 2.215723  128.119.245.12  10.0.0.50       HTTP     1355 HTTP/1.1 200 OK  (text/html)
  18 2.472155  10.0.0.50       128.119.245.12  HTTP      496 GET /pearson.png HTTP/1.1
  23 2.524020  128.119.245.12  10.0.0.50       HTTP      745 HTTP/1.1 200 OK  (PNG)
  24 2.527732  10.0.0.50       128.119.245.12  HTTP      493 GET /favicon.ico HTTP/1.1
  29 2.574268  10.0.0.50       178.79.137.164  HTTP      463 GET /8E_cover_small.jpg HTTP/1.1
  31 2.585080  128.119.245.12  10.0.0.50       HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  37 2.842968  178.79.137.164  10.0.0.50       HTTP      224 HTTP/1.1 302 Found
```

My browser downloaded the two images in parallel. After the browser sent the first GET request to the server at the 128 address, another GET request to the same address followed shortly after. Then, almost at the same time, a GET request was sent to the 178 address. This shows that the browser was requesting the images from two different servers at the same time. GET request to the 178 address was made quickly after the one to the 128 address, indicating that both requests were made almost simultaneously. This suggests that the browser didn’t wait for one image to finish downloading before it started requesting the next. Instead, it fetched them in parallel, which is a common practice to speed up page loading by getting resources from different servers at once.