



## Department of Computer Science & Engineering

### Lab Report #2

Course Code : CSE-3634

Course Title : Computer Network Lab

#### Submitted To:

Abdul Kayum

Adj. Faculty, Dept. Of CSE

International Islamic University Chittagong.

#### Submitted By:

Name : Shahariar Nafiz

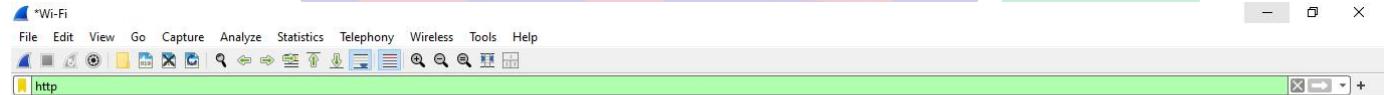
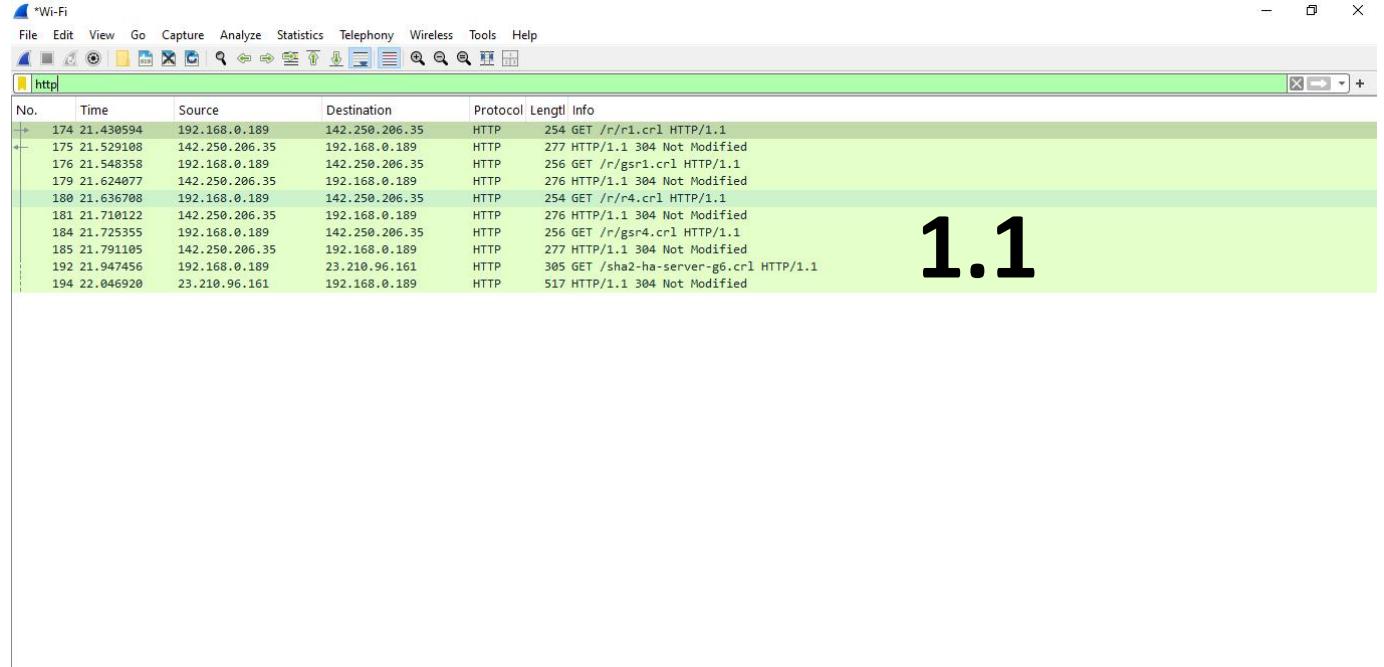
ID : C221361

Section : 7DM

Semester : 7<sup>th</sup>

# The Basic HTTP GET/response interaction

## 1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?



> Frame 174: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF\_{...}

> Ethernet II, Src: LiteonTechno\_13:7b:37 (ac:b5:7d:13:7b:37), Dst: zte\_7c:61:6e (b0:0a:d5:7c:61)

Internet Protocol Version 4, Src: 192.168.0.189, Dst: 142.250.206.35

.... 0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 240

Identification: 0x934c (37708)

> 010. .... = Flags: 0x2, Don't Fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x4838 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.0.189

Destination Address: 142.250.206.35

[Stream index: 12]

> Transmission Control Protocol, Src Port: 61037, Dst Port: 80, Seq: 1, Ack: 1, Len: 200

> Hypertext Transfer Protocol

Version : 4

0000 b0 0a d5 7c 61 6e ac b5 7d 13 7b 37 08 00 45 00 ...|an...}{7..E

0010 00 f0 93 4c 40 00 80 06 48 38 c0 a8 00 bd 8e fa ...L@...H8.....

0020 ce 23 ee 6d 00 5a e8 50 7b 90 64 fc 75 6d 50 18 ...#m:P P {d umP

0030 02 02 62 e9 00 47 45 54 20 2f 72 2f 72 31 2e ..b...GE T /r/1.

0040 63 72 6c 20 48 54 54 50 2f 31 2e 31 00 0a 43 61 cr1 HTTP /1.1..Ca

0050 63 68 65 2d 43 6f 6e 74 72 6f 66 3a 20 6d 178 che-Cont rol: max

0060 2d 61 67 65 26 3d 20 33 38 30 38 0d 0a 43 6f 6e -age = 3 000 'Con

0070 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a nection: Keep-Al

0080 0d 00 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 69 ive. Acc ept: \*/

0090 66 63 65 3a 20 54 68 75 2c 20 32 35 20 48 75 6c If-Mad ified-Si

00a0 20 32 36 32 34 20 31 34 3a 34 38 3a 30 38 20 47 nce: Thu , 25 Jul 2024 14 :48:00 G

00b0 4d 54 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 MT>User-Agent:

00c0 4d 69 63 72 6f 73 6f 66 74 2d 43 72 79 70 74 6f Microsoft t-Crypto

00d0 41 50 49 2f 31 30 2e 30 0d 0a 48 6f 73 74 3a 20 API/10.0 .Host:

00e0 63 2e 70 6b 69 2e 67 6f 6f 67 60 0a 0d 0a c.pki.go og...

## 2. What languages (if any) does your browser indicate that it can accept to the server?

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
174	21.430594	192.168.0.189	142.250.206.35	HTTP	254	GET /r1.crl HTTP/1.1
175	21.529108	142.250.206.35	192.168.0.189	HTTP	277	HTTP/1.1 304 Not Modified
176	21.548358	192.168.0.189	142.250.206.35	HTTP	256	GET /r/gsr1.crl HTTP/1.1
179	21.624077	142.250.206.35	192.168.0.189	HTTP	276	HTTP/1.1 304 Not Modified
180	21.636708	192.168.0.189	142.250.206.35	HTTP	254	GET /r/r4.crl HTTP/1.1
181	21.710122	142.250.206.35	192.168.0.189	HTTP	276	HTTP/1.1 304 Not Modified
184	21.725355	192.168.0.189	142.250.206.35	HTTP	256	GET /r/gsr4.crl HTTP/1.1
185	21.791105	142.250.206.35	192.168.0.189	HTTP	277	HTTP/1.1 304 Not Modified
192	21.947456	192.168.0.189	23.210.96.161	HTTP	305	GET /sha2-ha-server-g6.crl HTTP/1.1
194	22.046920	23.210.96.161	192.168.0.189	HTTP	517	HTTP/1.1 304 Not Modified

```
> Frame 174: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: zte_7c:61:6e (b0:0a:d5:7c:61)
> Internet Protocol Version 4, Src: 192.168.0.189, Dst: 142.250.206.35
> Transmission Control Protocol, Src Port: 61037, Dst Port: 80, Seq: 1, Ack: 1, Len: 200
  Hypertext Transfer Protocol
    GET /r1.crl HTTP/1.1\r\n
      Request Method: GET
      Request URI: /r1.crl
      Request Version: HTTP/1.1
      Cache-Control: max-age = 3000\r\n
      Connection: Keep-Alive\r\n
      Accept: */*\r\n
      If-Modified-Since: Thu, 25 Jul 2024 14:48:00 GMT\r\n
      User-Agent: Microsoft-CryptoAPI/10.0\r\n
      Host: c.pki.google\r\n
      \r\n
    [Response in frame: 175]
    [Full request URI: http://c.pki.google/r1.crl]
```

b0 0a d5 7c 61 6e ac b5 7d 13 7b 37 08 00 45 00 ...|an... }{7·E·
 00 0f 93 4c 40 00 80 06 48 38 c0 a8 00 bd 8e fa ...|L@... H8...·
 ce 23 ee 6d 00 50 e8 50 7b 90 64 fc 75 6d 50 18 #·m·P·P { d·um·P·
 0030 02 02 62 e9 00 00 47 45 54 20 2f 72 2f 72 31 2e ·b··GE T /r/r1.
 0040 63 72 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 43 61 crl HTTP /1.1·Ca
 0050 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 che-Cont rol: max
 0060 2d 61 67 65 20 3d 20 33 30 30 0d 0a 43 6f 6e -age = 3 000·Con
 0070 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nnection: Keep-Al
 0080 69 75 65 0d 0a 41 63 63 65 70 74 3a 20 2f 2a iive·Acc ept: "/"
 0090 0d 0a 49 6d 2d 44 6f 64 69 66 65 64 2d 53 69 .If-Mod ified-Si
 00a0 6e 63 65 3d 28 5d 68 75 2c 20 32 35 20 4a 75 6c nce: Thu , 25 Jul
 00b0 20 32 30 32 34 20 31 34 3a 34 33 3a 30 20 47 2024 14 :48:00 G
 00c0 4d 54 0d 00 55 73 65 72 2d 41 67 65 6e 74 3a 20 MT·User -Agent:
 00d0 4d 69 63 72 6f 73 6f 66 74 2d 43 72 79 70 74 6f Microsoft t·Crypto
 00e0 41 50 49 2f 31 30 2e 30 0d 0a 48 6f 73 74 3a 20 API/10.0 ..Host:
 00f0 63 2e 70 6b 69 2e 67 6f 6f 67 0d 0a 0d 0a c.pki.go og ::::

## 3. What is the IP address of your computer? Of the gaia.cs.umass.edu server

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
174	21.430594	192.168.0.189	142.250.206.35	HTTP	254	GET /r1.crl HTTP/1.1
175	21.529108	142.250.206.35	192.168.0.189	HTTP	277	HTTP/1.1 304 Not Modified
176	21.548358	192.168.0.189	142.250.206.35	HTTP	256	GET /r/gsr1.crl HTTP/1.1
179	21.624077	142.250.206.35	192.168.0.189	HTTP	276	HTTP/1.1 304 Not Modified
180	21.636708	192.168.0.189	142.250.206.35	HTTP	254	GET /r/r4.crl HTTP/1.1
181	21.710122	142.250.206.35	192.168.0.189	HTTP	276	HTTP/1.1 304 Not Modified
184	21.725355	192.168.0.189	142.250.206.35	HTTP	256	GET /r/gsr4.crl HTTP/1.1
185	21.791105	142.250.206.35	192.168.0.189	HTTP	277	HTTP/1.1 304 Not Modified
192	21.947456	192.168.0.189	23.210.96.161	HTTP	305	GET /sha2-ha-server-g6.crl HTTP/1.1
194	22.046920	23.210.96.161	192.168.0.189	HTTP	517	HTTP/1.1 304 Not Modified

```
> Frame 174: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: zte_7c:61:6e (b0:0a:d5:7c:61)
> Internet Protocol Version 4, Src: 192.168.0.189, Dst: 142.250.206.35
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 240
  Identification: 0x934c (37708)
  Flags: 0x0000 (Don't fragment)
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x4838 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.189
  Destination Address: 142.250.206.35
  [Stream index: 12]
> Transmission Control Protocol, Src Port: 61037, Dst Port: 80, Seq: 1, Ack: 1, Len: 200
  Hypertext Transfer Protocol
    GET /r1.crl HTTP/1.1\r\n
      Request Method: GET
      Request URI: /r1.crl
      Request Version: HTTP/1.1
      Cache-Control: max-age = 3000\r\n
      Connection: Keep-Alive\r\n
      Accept: */*\r\n
      If-Modified-Since: Thu, 25 Jul 2024 14:48:00 GMT\r\n
      User-Agent: Microsoft-CryptoAPI/10.0\r\n
      Host: gaia.cs.umass.edu\r\n
      \r\n
    [Response in frame: 175]
    [Full request URI: http://gaia.cs.umass.edu/r1.crl]
```

b0 0a d5 7c 61 6e ac b5 7d 13 7b 37 08 00 45 00 ...|an... }{7·E·
 0010 00 f0 93 4c 40 00 80 06 48 38 c0 a8 00 bd 8e fa ...|L@... H8...·
 ce 23 ee 6d 00 50 e8 50 7b 90 64 fc 75 6d 50 18 #·m·P·P { d·um·P·
 0020 02 02 62 e9 00 00 47 45 54 20 2f 72 2f 72 31 2e ·b··GE T /r/r1.
 0030 63 72 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 43 61 crl HTTP /1.1·Ca
 0040 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 che-Cont rol: max
 0050 2d 61 67 65 20 3d 20 33 30 30 0d 0a 43 6f 6e -age = 3 000·Con
 0060 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nnection: Keep-Al
 0070 69 75 65 0d 0a 41 63 63 65 70 74 3a 20 2f 2a iive·Acc ept: "/"
 0080 0d 0a 49 6d 2d 44 6f 64 69 66 65 64 2d 53 69 .If-Mod ified-Si
 0090 6e 63 65 3d 28 5d 68 75 2c 20 32 35 20 4a 75 6c nce: Thu , 25 Jul
 00a0 20 32 30 32 34 20 31 34 3a 34 33 3a 30 20 47 2024 14 :48:00 G
 00b0 4d 54 0d 00 55 73 65 72 2d 41 67 65 6e 74 3a 20 MT·User -Agent:
 00c0 4d 69 63 72 6f 73 6f 66 74 2d 43 72 79 70 74 6f Microsoft t·Crypto
 00d0 41 50 49 2f 31 30 2e 30 0d 0a 48 6f 73 74 3a 20 API/10.0 ..Host:
 00e0 63 2e 70 6b 69 2e 67 6f 6f 67 0d 0a 0d 0a c.pki.go og ::::

Source address is my ip addresss

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
174	21.430594	192.168.0.189	142.250.206.35	HTTP	254	GET /r1.crl HTTP/1.1
175	21.529188	142.250.206.35	192.168.0.189	HTTP	277	HTTP/1.1 304 Not Modified
176	21.548358	192.168.0.189	142.250.206.35	HTTP	256	GET /r/gsr1.crl HTTP/1.1
179	21.624077	142.250.206.35	192.168.0.189	HTTP	276	HTTP/1.1 304 Not Modified
180	21.636708	192.168.0.189	142.250.206.35	HTTP	254	GET /r/cr1.crl HTTP/1.1
181	21.710122	142.250.206.35	192.168.0.189	HTTP	276	HTTP/1.1 304 Not Modified
184	21.725355	192.168.0.189	142.250.206.35	HTTP	256	GET /r/gsr4.crl HTTP/1.1
185	21.791105	142.250.206.35	192.168.0.189	HTTP	277	HTTP/1.1 304 Not Modified
192	21.947456	192.168.0.189	23.210.96.161	HTTP	305	GET /sha2-ha-server-g6.crl HTTP/1.1
194	22.046920	23.210.96.161	192.168.0.189	HTTP	517	HTTP/1.1 304 Not Modified

```

> Frame 174: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: zte_7c:61:6e (b0:0a:d5:7c:61)
> Internet Protocol Version 4, Src: 192.168.0.189, Dst: 142.250.206.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 240
    Identification: 0x934c (37708)
> 010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x4838 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.189
    Destination Address: 142.250.206.35
    [Stream index: 12]
> Transmission Control Protocol, Src Port: 61037, Dst Port: 80, Seq: 1, Ack: 1, Len: 200
> Hypertext Transfer Protocol

```

```

0000 b0 0a d5 7c 61 6e ac b5 7d 13 7b 37 08 00 45 00 ...|an... }{7..E.
0010 00 f0 93 4c 40 00 80 06 48 38 c0 a8 00 bd Bc 10 ...L@... H8...*
0020 ce 28 ee 6d 00 50 e8 50 7b 98 64 fc 75 6d 50 18 .4m P.P { dump...
0030 02 02 62 e0 00 07 47 45 54 20 2f 72 2f 72 31 2e ..b...GE T /r/r1.
0040 63 72 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 43 61 crl HTTP /1.1 -Ca
0050 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 che-Cont rol: max
0060 2d 61 67 65 20 3d 20 33 30 30 30 0d 0a 43 6f 6e -age = 3 000-Con
0070 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nnection: Keep-Al
0080 69 76 65 0d 0a 41 6c 63 65 70 34 3a 20 2a 2f 2a iv-Ac es/*/
0090 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 69 ..If-Mod ified-Si
00a0 6e 63 65 3a 20 54 68 75 2c 20 32 35 20 4a 75 6c nce: Thu , 25 Jul
00b0 20 32 30 32 34 20 31 34 3a 34 38 3a 30 30 20 47 2024 14 :48:00 G
00c0 4d 54 0d 0e 55 73 65 72 2d 41 67 65 6e 74 3a 20 MT-User-Agent:
00d0 4d 69 63 72 6f 73 6f 66 74 2d 43 72 79 70 74 6f Microsoft t-Crypto
00e0 41 50 49 2f 31 2e 30 0d 0a 48 6f 73 74 3a 20 API/10.0 -Host:
00f0 63 2e 70 6b 69 2b 67 6f 6f 67 0d 0a 0d 0a c.pkl.go og...

```

Destination Address (ip.dst), 4 bytes

Packets: 4035 - Displayed: 10 (0.2%) - Dropped: 0 (0.0%)

Profile: Default

## 4. What is the status code returned from the server to your browser?

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
148	9.047408	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
161	9.369946	128.119.245.12	192.168.0.189	HTTP	539	HTTP/1.1 404 Not Found (text/html)
454	33.308241	192.168.0.189	34.104.35.123	HTTP	314	HEAD /edged1/diffgen-puffin/jflchccmpkfebkiaminagehmchikm/ba938eed54a876b59dd675921ee7c09a7c206c9bdbf68baaf960...
455	33.389533	34.104.35.123	192.168.0.189	HTTP	643	HTTP/1.1 200 OK
458	33.434170	192.168.0.189	34.104.35.123	HTTP	386	GET /edged1/diffgen-puffin/jflchccmpkfebkiaminagehmchikm/ba938eed54a876b59dd675921ee7c09a7c206c9bdbf68baaf960...
460	33.506432	34.104.35.123	192.168.0.189	HTTP	410	HTTP/1.1 206 Partial Content
540	36.377974	192.168.0.189	34.104.35.123	HTTP	389	GET /edged1/diffgen-puffin/jflchccmpkfebkiaminagehmchikm/ba938eed54a876b59dd675921ee7c09a7c206c9bdbf68baaf960...
542	36.466523	34.104.35.123	192.168.0.189	HTTP	267	HTTP/1.1 206 Partial Content

```

> Frame 455: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: zte_7c:61:6e (b0:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37)
> Internet Protocol Version 4, Src: 34.104.35.123, Dst: 192.168.0.189
> Transmission Control Protocol, Src Port: 80, Dst Port: 61451, Seq: 1, Ack: 261, Len: 589
> Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
        accept-ranges: bytes\r\n
        content-disposition: attachment\r\n
        content-length: 2133\r\n
        content-security-policy: default-src 'none'\r\n
        server: Google-Edge-Cache\r\n
        x-content-type-options: nosniff\r\n
        x-frame-options: SAMEORIGIN\r\n
        x-xss-protection: 0\r\n
        x-request-id: 7cab20cd-19b6-48e4-b9c3-c830034bd065\r\n
        date: Mon, 24 Mar 2025 04:37:56 GMT\r\n

```

```

0030 04 1a 99 ab 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 61 63 63 65 70 74 2d 72 61 00 OK-a ccept-ra
0050 6e 67 65 73 3a 20 26 62 79 74 65 73 0d 0a 63 6f 6e nges: by tes::con
0060 74 65 6e 74 2d 64 69 73 20 67 73 69 74 69 6f 6e tent-dis position
0070 3a 20 61 74 74 61 63 68 6d 65 6e 74 0a 0a 63 6f : attach ment::co
0080 64 74 65 74 2d 64 65 66 67 74 68 3a 20 32 31 ntent-l ngth: 21
0090 33 33 0d 0a 63 6f 6e 74 65 6e 74 2d 73 65 63 75 33::cont ent-secu
00a0 72 69 74 79 2d 70 6f 6c 69 63 79 3a 20 64 65 66 rity-pol icy: def
00b0 61 75 6c 74 2d 73 72 63 20 27 6e 6f 6e 65 2d 0d autl-src 'none'.
00c0 0a 73 65 72 76 65 72 3a 20 47 6f 6f 67 6c 65 2d serv: Google-
00d0 45 64 67 65 2d 43 61 63 68 69 6d 0d 0a 78 26 63 6f Edge-Ca he--x-co
00e0 6e 74 65 6e 74 2d 74 79 70 65 2d 6f 70 74 69 6f ntent-t pe-optio
00f0 6e 73 3a 20 66 6f 73 6e 69 66 66 0d 0a 78 2d 66 ns: nosn iff-x-f
0100 72 61 6d 65 2d 6f 70 74 69 6f 6e 73 3a 20 53 41 rame-op ions: SA
0110 4d 45 4f 52 49 47 49 4e 0d 0a 78 2d 78 73 73 2d MEOIRGIN ::x-xss-
0120 70 72 6f 74 65 63 74 69 6f 6e 3a 20 30 0d 0a 78 protecti on: 0-x
0130 2d 72 65 71 75 63 73 74 2d 69 64 3a 20 37 63 61 -request -id: 7ca
0140 62 32 30 63 64 62 31 39 62 36 2d 34 38 65 34 2d b20cd-19 b6-48e4-
0150 62 39 63 33 2d 63 38 33 30 30 33 34 62 64 30 36 b9c3-c83 0034bd06
0160 35 0d 0a 64 61 74 65 3a 20 4d 6f 6e 2c 20 32 34 5::date: Mon, 24
0170 20 4d 61 72 20 32 30 32 35 20 30 34 3a 33 37 3a Mar 202 5 04:37:
0180 35 36 20 47 4d 54 0d 0a 61 67 65 3a 20 34 33 37 56 GMT.. age: 437
0190 33 39 0d 0a 6c 61 73 74 2d 6d 6f 64 69 66 69 65 39..last -modifie

```

HTTP Response Status Code (http.response.code), 3 bytes

Packets: 881 - Displayed: 8 (0.9%)

Profile: Default

## 5. When was the HTML file that you are retrieving last modified at the server?

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
3325	162.131553	142.250.206.35	192.168.0.189	HTTP	276	HTTP/1.1 304 Not Modified
3333	162.227010	192.168.0.189	23.211.193.54	HTTP	281	GET / HTTP/1.1
3334	162.276515	23.211.193.54	192.168.0.189	HTTP	317	HTTP/1.1 304 Not Modified
3337	162.293712	192.168.0.189	142.250.206.35	HTTP	256	GET /r/gsrl.crl HTTP/1.1
3338	162.371723	142.250.206.35	192.168.0.189	HTTP	276	HTTP/1.1 304 Not Modified
3339	162.382303	192.168.0.189	142.250.206.35	HTTP	254	GET /r/f4.crl HTTP/1.1
3340	162.457533	142.250.206.35	192.168.0.189	HTTP	276	HTTP/1.1 304 Not Modified
3348	162.588448	192.168.0.189	146.75.46.172	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?92ce8942a0f7fc0d HTTP/1.1
3349	162.674857	146.75.46.172	192.168.0.189	HTTP	252	HTTP/1.1 304 Not Modified
6222	162.687311	192.168.0.189	23.212.164.114	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/authrootst1.cab?adb33ab316f33bb2 HTTP/1.1
6223	162.694236	23.212.164.114	192.168.0.189	HTTP	322	HTTP/1.1 304 Not Modified
6226	162.667800	192.168.0.189	23.212.164.114	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/pinrulesst1.cab?fb49c5c0ac8e7bfd HTTP/1.1
6227	162.714538	23.212.164.114	192.168.0.189	HTTP	322	HTTP/1.1 304 Not Modified

```

accept-ranges: bytes\r\n
content-disposition: attachment\r\n
> content-length: 2133\r\n
content-security-policy: default-src 'none'\r\n
server: Google-Edge-Cache\r\n
x-content-type-options: nosniff\r\n
x-frame-options: SAMEORIGIN\r\n
x-xss-protection: 0\r\n
x-request-id: 7cab20cd-19b6-48e4-b9c3-c830034bd065\r\n
date: Mon, 24 Mar 2025 04:37:56 GMT\r\n
age: 43739\r\n
last-modified: Mon, 24 Mar 2025 04:35:52 GMT\r\n
etag: "40ef9ad"\r\n
content-type: application/octet-stream\r\n
alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000\r\n
cache-control: public,max-age=86400\r\n
coprocessor-response: download-server\r\n
\r\n
[Request in frame: 454]
[Time since request: 0.081292000 seconds]

```

Mon, 24 mar 2025

0128 70 72 6f 74 65 63 74 69 6f 6e 3a 20 30 0d 0a 78 protecti on: 0..x
0129 2d 72 65 71 75 75 63 74 69 64 6a 3a 20 37 63 61 -request -id: 7ca
0140 62 32 30 63 64 2d 31 39 62 36 2d 34 38 65 34 2d b2cd-19 b6-48e4-
0140 62 32 30 63 64 2d 31 39 62 36 2d 34 38 65 34 2d b9c3-c83 0034bd06
0140 62 32 30 63 64 2d 31 39 62 36 2d 34 38 65 34 2d b9c3-c83 0034bd06
0178 20 40 61 72 26 32 38 33 30 33 34 62 64 30 36 5 -date: Mon, 24
0180 35 36 20 47 4d 54 6d 3a 20 61 67 65 3a 20 34 33 37 3a Mar 2025 04:37:
0180 35 36 20 47 4d 54 6d 3a 20 61 67 65 3a 20 34 33 37 3a 56 GMT.. age: 437
0190 33 39 0d 0a 6c 61 73 74 2d 66 67 64 69 56 69 65 39 -last-modifie
0190 33 39 0d 0a 6c 61 73 74 2d 66 67 64 69 56 69 65 d: Mon, 24 Mar 2
01a0 64 3a 20 4d 6f 6e 2c 20 32 34 3a 33 35 32 20 47 4d 54 025 04:33: 5:52 GMT
01b0 30 32 35 20 30 34 3a 33 35 3a 35 32 20 47 4d 54
01c0 0d 65 74 61 67 3a 20 22 34 30 65 66 39 61 64 ..-etag: "40ef9ad
01d0 22 0d 0a 63 6f 6e 74 65 6e 74 2d 74 79 65 3a ..-conte nt-type:
01e0 65 74 61 67 3a 20 22 34 30 65 66 39 61 64 applica tion/oct
01f0 65 74 2d 73 74 72 65 61 6d 60 0d 0a 61 6c 74 2d 73 et-strea m-alt-s
0200 76 63 3a 20 68 33 3d 22 3a 34 33 22 3b 20 6d vc: h3=":443"; m
0218 61 3d 32 35 39 32 30 38 30 2c 20 68 33 32 39 32 a=2592000, h3-29
0228 3d 22 3a 34 33 22 3b 20 6d 61 3d 32 35 39 32 ="443"; ma=2592
0230 30 30 0d 0a 63 61 63 68 65 2d 63 6f 6e 74 72 000..-cac he-contr
0240 6f 6c 3a 20 70 75 62 6c 69 63 2c 6d 61 78 2d 61 ol: publ ic,max-a
0250 67 65 3d 38 36 34 30 30 0d 0a 63 6f 70 72 61 63 ge=86400 ..-coproc
0260 65 73 73 6f 72 2d 72 65 73 70 6f 6e 73 65 3a 20 essor-re sponse:
0270 64 6f 77 6e 6f 61 64 2d 73 65 72 76 65 72 0d download -server...
0280 0a 0d 0a ...

HTTP Last Modified (http.last\_modified), 46 bytes

Packets: 7044 - Displayed: 28 (0.4%)

Profile: Default

## 6. How many bytes of content are being returned to your browser?

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
148	9.047408	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
161	9.369946	128.119.245.12	192.168.0.189	HTTP	539	HTTP/1.1 404 Not Found (text/html)
454	33.308241	34.104.35.123	192.168.0.189	HTTP	314	HEAD /edged1/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/ba938eed54a876b59dd675921ee7c09a7c206c9bdf68baaf9...
455	33.389533	34.104.35.123	192.168.0.189	HTTP	643	HTTP/1.1 200 OK
458	33.434170	192.168.0.189	34.104.35.123	HTTP	386	GET /edged1/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/ba938eed54a876b59dd675921ee7c09a7c206c9bdf68baaf96...
460	33.506432	34.104.35.123	192.168.0.189	HTTP	410	HTTP/1.1 204 Partial Content
540	36.377974	192.168.0.189	34.104.35.123	HTTP	389	GET /edged1/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/ba938eed54a876b59dd675921ee7c09a7c206c9bdf68baaf96...
542	36.466523	34.104.35.123	192.168.0.189	HTTP	267	HTTP/1.1 206 Partial Content
941	60.763930	192.168.0.189	18.239.151.62	HTTP	274	GET //MEnsDBGMQWQjAJBgUrDgMCggUABBSLwZ6EW5gdyc9uSAeaaljjETNTktAQUv1%2B30c7dH4b0w1Ws3NcQwg6pi0cCCQnDkpMNI3fwK...
944	60.855927	18.239.151.62	192.168.0.189	OCSP	719	Response
953	60.984931	192.168.0.189	108.158.49.186	HTTP	304	GET /MFQwUjBQME4wTDAJ8gUrDgMCggUABBRPw0AUu0%2B5VZ5%2Fa9jFTaU9pkK3FAQUhBjMHTsvAyJlc4INzzHshB0CggCEwdzEjgLnIaIoz...
955	61.081154	108.158.49.186	192.168.0.189	HTTP	824	Response
964	61.263920	192.168.0.189	108.158.49.186	HTTP	307	GET /MFQwUjBQME4wTDAJ8gUrDgMCggUABBRPw0AUu0%2B5VZ5%2Fa9jFTaU9pkK3FAQUhBjMHTsvAyJlc4INzzHshB0CggCEwdzEjgLnIaIoz...

```

Transmission Control Protocol, Src Port: 80, Dst Port: 61451, Seq: 1, Ack: 261, Len: 589
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
accept-ranges: bytes\r\n
content-disposition: attachment\r\n
content-length: 2133\r\n
content-security-policy: default-src 'none'\r\n
server: Google-Edge-Cache\r\n
x-content-type-options: nosniff\r\n
x-frame-options: SAMEORIGIN\r\n
x-xss-protection: 0\r\n
x-request-id: 7cab20cd-19b6-48e4-b9c3-c830034bd065\r\n
date: Mon, 24 Mar 2025 04:37:56 GMT\r\n
age: 43739\r\n
last-modified: Mon, 24 Mar 2025 04:35:52 GMT\r\n
etag: "40ef9ad"\r\n
content-type: application/octet-stream\r\n
alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000\r\n
cache-control: public,max-age=86400\r\n
Content length (http.content_length), 22 bytes

```

2133 bytes

0070 3a 20 61 74 74 61 63 68 6d 65 6e 74 0d 0a 3d 6f : attachment:co
0080 6e 74 65 6e 74 2d 74 6d 65 6e 74 68 3a 20 32 31 intent-le ngth: 21
0090 33 33 0d 0b 63 6f 74 65 6e 74 6d 74 73 65 75 33 33:cont ent-secu
00a0 72 69 74 79 2d 70 6f 6c 69 63 79 3a 20 64 65 66 rity-pol icy: def
00b0 61 75 6c 74 2d 73 72 63 20 27 6f 6e 65 27 0d aut-src: 'none'
00c0 0a 73 65 72 6f 76 65 72 3a 20 47 6f 67 6c 65 2d -server: Google-
00d0 45 64 67 65 2d 43 61 63 68 65 0d 0a 78 2d 63 6f Edge-Cac he-cc
00e0 6e 74 65 66 2d 43 61 63 68 65 0d 0a 78 2d 63 6f ent-typ e-optio
00f0 6e 73 3a 20 6e 6f 73 6a 69 66 60 0d 0a 78 2d 66 ns: nosn iff: x-f
0100 72 61 6d 65 2d 6f 70 74 69 6f 6e 73 3a 20 53 41 rame-opt ions: SA
0110 4d 45 4f 52 49 47 49 4d 0d 0a 78 2d 78 73 73 2d MEORIGIN ..xx-xss-
0120 70 72 6f 74 65 63 74 69 6f 6e 3a 20 30 0d 0a 78 protection: 0..x
0130 2d 72 65 71 75 65 73 74 2d 69 3a 20 37 63 61 -request -id: 7ca
0140 62 32 30 63 64 2d 31 39 62 36 2d 34 38 65 34 2d b2cd-19 b6-48e4-
0150 62 39 63 33 2d 63 38 33 30 33 34 62 64 30 36 b9c3-c83 0034bd06
0160 35 0d 0a 64 61 74 65 3a 20 4d 6f 6e 2c 20 32 34 5 -date: Mon, 24
0170 20 4d 61 72 20 32 30 32 35 20 30 34 3a 33 37 3a Mar 2025 04:37:
0180 35 36 20 47 4d 54 0d 0a 61 67 65 3a 20 34 33 37 3a 56 GMT.. age: 437
0190 33 39 0d 0a 6c 61 73 74 2d 66 6f 64 69 66 69 65 39 -last-modifie
01a0 64 3a 20 4d 6f 6e 2c 20 32 34 20 40 61 72 20 32 0: Mon, 24 Mar 2
01b0 30 32 35 20 30 34 3a 33 35 3a 35 32 20 47 4d 54 025 04:33: 5:52 GMT
01c0 0d 0a 65 74 61 67 3a 20 22 34 30 65 66 39 61 64 ..-etag: "40ef9ad
01d0 22 0d 0a 63 6f 6e 74 65 6e 74 2d 74 79 70 65 3a ..-conte nt-type:

Packets: 10837 - Displayed: 28 (0.3%)

Profile: Default

**7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.**

Screenshot of Wireshark showing network traffic analysis. The main pane displays a list of captured packets, and the bottom pane shows the raw hex and ASCII data for selected packets. A large watermark in the center of the image reads "I don't see any headers".

The packet list shows various HTTP requests and responses, including:

- HTTP GET /favicon.ico
- HTTP 404 Not Found (text/html)
- HTTP HEAD /edged1/difffgen-puffin/jflchccmpkfebkiaminageehmchikm/ba938eed54a876b59dd675921ee7c09a7c206c9bdbf68baaf9..
- HTTP 643 OK
- HTTP 386 GET /edged1/difffgen-puffin/jflchccmpkfebkiaminageehmchikm/ba938eed54a876b59dd675921ee7c09a7c206c9bdbf68baaf9..
- HTTP 419 Partial Content
- HTTP 389 GET /edged1/difffgen-puffin/jflchccmpkfebkiaminageehmchikm/ba938eed54a876b59dd675921ee7c09a7c206c9bdbf68baaf9..
- HTTP 267 Partial Content
- HTTP 274 GET //NeowSDBGM[EQWQ]AJBgUrDg%CGgUABSLwZ6EWsgdYc9uaSEaaLjjETNtkaQUv1%2B30c7dH4b0b1ws3NCQng6p1oCCQnkpMNIK3fvK..
- OCSP 719 Response
- HTTP 304 GET /MFQoUjBQME4wTDAJBgUrDg%CGgUABBSIfaRExmfqfJR3TkMyD705MhzEgQUnF8A36oB1zArOIIiuG1KnPIkYMCewZ%2F1EoqJ83%2B8..
- OCSP 824 Response
- HTTP 307 GET /MFQoUjBQME4wTDAJBgUrDg%CGgUABBRPw0U8%2B5V25%2Fa9jFTaU9pkK3FAQUhBjMhTTsvAyUIC4IWZzMshB0CggCewdEJgLnWaIo..

The details pane shows the structure of a selected packet, highlighting the header checksum status as "Unverified".

The bottom status bar indicates "Packets: 15174 - Displayed: 28 (0.2%)".

# The HTTP CONDITIONAL GET/response interaction

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

no

```
> Frame 254: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{...}\Wi-Fi
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: zte_7c:61:6e (b0:0a:d5:7c:61:6e)
> Internet Protocol Version 4, Src: 192.168.0.189, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61685, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
  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/134.0.0.0 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\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
    \r\n
  [Response in frame: 264]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

0000 b0 0a d5 7c 61 6e ac b5 7d 13 7b 37 08 00 45 00 ...|an... }{7..E...
0010 00 00 04 26 40 00 08 06 bd e8 c0 a8 00 bd 00 77 ...
0020 f5 0c 00 00 50 56 52 56 dd a6 5d 69 dd 40 50 18 ...@...-----w
0030 00 02 02 b1 00 00 47 45 54 20 2f 77 69 72 65 73 ...PVR V-j@P...
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 ...GE T /wireshark-lab...
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68 ...s/HTTP-wireshark-file2.h...
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 08 48 6f ...fml HTTP/1.1-Ho...
0070 73 74 3c 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 ...st gaia.cs.umass.edu-connectio...
0080 73 2e 65 64 75 0d 0a 43 6f 6e 66 65 63 74 69 6f ...n: keep alive-U...
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 00 0a 55 ...pgrade-Insecure-...
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d ...Requests : 1-Use...
00b0 52 65 71 75 63 73 74 73 3e 20 31 0d 0a 55 73 65 ...p-Agent: Mozilla...
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 61 5d .../5.0 (Wi ndows NT...
00d0 2f 35 2e 30 20 28 57 59 6e 64 6f 77 73 29 4e 54 ...10.0; W in64; x64) Apple Webkit/5...
00e0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 ...37.36 (K HTML, li...
00f0 54 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 ...ke Gecko ) Chrome/134.0.0.0 Safar...
0100 53 37 2e 33 36 20 28 48 4b 54 4d 4c 2c 2d 6c 69 .../134.0.0.0 Safari/134.0.0.0...
0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ...1/537.36 .Accept...
0120 2f 31 33 2e 30 2e 30 2e 30 2e 30 20 53 61 66 61 72 ...text/html,application/xhtml+xml...
0130 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 ...application/xm...
0140 3a 20 74 65 78 74 2f 68 74 6d 6c 2b 78 6d ...l,application/xm...
0150 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d ...l,application/xm...
0160 6c 2c 61 70 70 6c 63 61 74 69 6f 6e 2f 78 6d ...l,application/xm...

\_packets: 3462 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) || Profile: Default

8. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

yes it return

```
> Frame 264: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{...}\Wi-Fi
> Ethernet II, Src: zte_7c:61:6e (b0:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189
> Transmission Control Protocol, Src Port: 80, Dst Port: 61685, Seq: 1, Ack: 473, Len: 730
  Hypertext Transfer Protocol
    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 ac b5 7d 13 7b 37 b8 0a d5 7c 61 6e 00 00 45 00 ...|...|an... E...
0010 03 02 d3 eb 40 00 25 06 48 21 80 77 f5 0c c0 a8 00 ...@%... Hi w...
0020 00 bd 00 50 f0 f5 5d 69 dd 49 56 52 58 7c 50 18 ...P...j@nx-p...
0030 00 ed 20 e1 00 00 44 54 54 50 27 31 2e 31 20 32 ...-P- HT/1.1.2
0040 30 30 20 4f 4b 0d 0a 44 71 64 75 3a 20 4d 6f 6e 00 OK Date: Mon ...
0050 2c 20 32 34 29 4d 61 72 20 32 30 32 35 28 31 37 , 24 Mar 2025 17
0060 3a 31 34 3a 34 33 20 47 4d 54 0d 0a 53 65 72 76 :14:43 G MT-Serv...
0070 65 72 3a 28 41 70 61 63 66 65 2f 32 2e 34 2e 36 er: Apache/2.4.6
0080 20 28 43 65 6e 74 4f 53 28 4f 70 65 6e 53 53 (CentOS ) OpenSS...
0090 4c 2f 31 2e 30 2e 32 6b 26 66 69 70 73 20 58 48 L/1.0.2k -fips PH...
00a0 50 2f 37 32 34 32 33 28 6d 6f 64 5f 70 65 72 P/2.4.33 mod\_per...
00b0 6c 2f 32 2e 30 2e 31 31 28 50 65 72 6c 2f 76 35 1/2.0.11 Perl/5
00c0 2e 31 26 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3 - Last-Modi...
00d0 66 69 65 64 3a 20 4d 6f 6c 2c 20 32 34 20 4d 61 fied: Mon, 24 Ma...
00e0 72 20 32 30 32 20 30 35 3a 35 39 3a 30 31 20 r 2025 05:59:01
00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 37 33 2d GMT-ETag: "173...
0100 36 33 31 31 30 34 64 30 38 31 32 33 66 22 0d 0a 63110ad8 8123F...
0110 41 63 63 65 70 74 2d 52 61 6e 67 65 73 30 20 62 Accept-Ranges: b
0120 79 74 65 73 0d 0a 43 6f 74 65 74 2d 4c 65 ytes: Content-Le...
0130 6e 67 74 68 3a 20 33 37 31 0d 0a 4b 65 65 70 2d ngrth: 37 1-Keep...
0140 41 6c 69 76 65 30 20 74 69 6d 65 6f 75 74 3d 35 Alive: timeout=5
0150 2c 20 6d 61 78 3d 31 38 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: Keep-Alive

\_packets: 3462 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) || Profile: Default

**9. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?**

also don't see

```

> Frame 278: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: zte_zc:61:6e (b0:0a:d5:7c:61)
> Internet Protocol Version 4, Src: 192.168.0.189, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61685, Dst Port: 80, Seq: 473, Ack: 731, Len: 418
  Hypertext Transfer Protocol
    > GET /favicon.ico HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
      Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*;q=0.8\r\n
      Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
    \r\n
  [Response in frame: 278]
  [Full request URI: http://gaia.cs.umass.edu/favicon.ico]

```

Packets: 3462 - Displayed: 4 (0.1%) - Dropped: 0 (0.0%) || Profile: Default

**10. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.**

Status code: 404

```

> Frame 278: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: zte_zc:61:6e (b0:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189
> Transmission Control Protocol, Src Port: 80, Dst Port: 61685, Seq: 731, Ack: 891, Len: 484
  Hypertext Transfer Protocol
    > HTTP/1.1 404 Not Found\r\n
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
      Date: Mon, 24 Mar 2025 17:14:43 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.1
      Content-Length: 209\r\n
      Keep-Alive: timeout=5, max=99\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
  [Request in frame: 278]
  [Time since request: 0.500186000 seconds]
  [Request URI: /favicon.ico]

```

Packets: 3462 - Displayed: 4 (0.1%) - Dropped: 0 (0.0%) || Profile: Default

```

> Frame 278: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: zte_zc:61:6e (b0:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189
> Transmission Control Protocol, Src Port: 80, Dst Port: 61685, Seq: 731, Ack: 891, Len: 484
  Hypertext Transfer Protocol
    > HTTP/1.1 404 Not Found\r\n
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
      Date: Mon, 24 Mar 2025 17:14:43 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.1
      Content-Length: 209\r\n
      Keep-Alive: timeout=5, max=99\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
  [Request in frame: 278]
  [Time since request: 0.500186000 seconds]
  [Request URI: /favicon.ico]

```

Packets: 3462 - Displayed: 4 (0.1%) - Dropped: 0 (0.0%) || Profile: Default

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
277	16.713315	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
254	16.242652	192.168.0.189	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
264	16.535193	128.119.245.12	192.168.0.189	HTTP	784	HTTP/1.1 200 OK (text/html)
278	17.213501	128.119.245.12	192.168.0.189	HTTP	538	HTTP/1.1 404 Not Found (text/html)

phrase: not found

```

> Frame 278: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: zte_7c:61:6e (00:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189
> Transmission Control Protocol, Src Port: 80, Dst Port: 61685, Seq: 731, Ack: 891, Len: 484
  Hypertext Transfer Protocol
    HTTP/1.1 404 Not Found\n
      Response Version: HTTP/1.1
      Status Code: 404
        [Status Code Description: Not Found]
          Response Phrase: Not Found
        Date: Mon, 24 Mar 2025 17:14:43 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
        Content-Length: 209\r\n
        Keep-Alive: timeout=5, max=99\r\n
        Connection: Keep-Alive\r\n
        Content-Type: text/html; charset=iso-8859-1\r\n
        \r\n
      [Request in frame: 277]
      [Time since request: 0.500186000 seconds]
      [Request URI: /favicon.ico]
    
```

Packets: 3462 - Displayed: 4 (0.1%) - Dropped: 0 (0.0%) || Profile: Default

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
277	16.713315	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
254	16.242652	192.168.0.189	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
264	16.535193	128.119.245.12	192.168.0.189	HTTP	784	HTTP/1.1 200 OK (text/html)
278	17.213501	128.119.245.12	192.168.0.189	HTTP	538	HTTP/1.1 404 Not Found (text/html)

not return

```

> Frame 278: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: zte_7c:61:6e (00:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189
> Transmission Control Protocol, Src Port: 80, Dst Port: 61685, Seq: 731, Ack: 891, Len: 484
  Hypertext Transfer Protocol
    Line-based text data: text/html (7 lines)
      <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
      <html><head>\n
        <title>404 Not Found</title>\n
      </head><body>\n
        <h1>Not Found</h1>\n
        <p>The requested URL /favicon.ico was not found on this server.</p>\n
      </body></html>\n
    
```

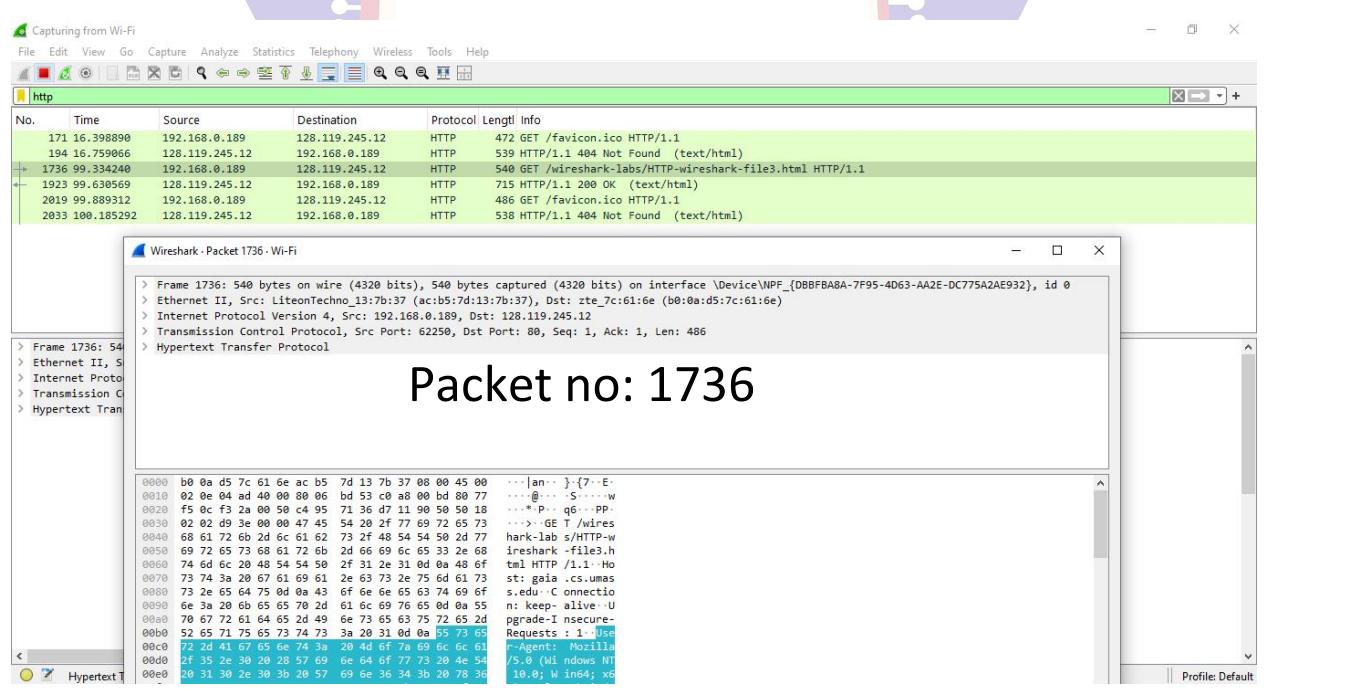
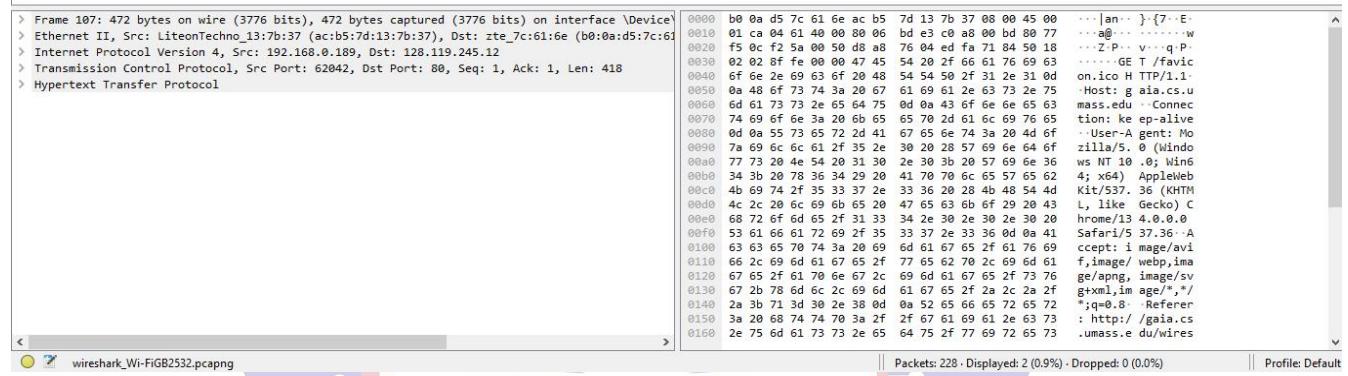
Packets: 3462 - Displayed: 4 (0.1%) - Dropped: 0 (0.0%) || Profile: Default

# Retrieving Long Documents:

11. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?



1



## 12. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Wi-Fi

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
171	16.398890	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
194	16.759066	128.119.245.12	192.168.0.189	HTTP	539	HTTP/1.1 404 Not Found (text/html)
+ 1736	99.334240	192.168.0.189	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+ 1923	99.630569	128.119.245.12	192.168.0.189	HTTP	715	HTTP/1.1 200 OK (text/html)
2019	99.889312	192.168.0.189	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
2033	100.185292	128.119.245.12	192.168.0.189	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Wireshark · Packet 1923 · Wi-Fi

> Frame 1923: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface \Device\NPF\_{DBBFBA8A-7F95-4D63-AA2E-DC775A2AE932}, id 0

> Ethernet II, Src: zte\_7c:61:6e (b0:0:a:d5:7c:61:6e), Dst: LiteonTechno\_13:7b:37 (ac:b5:7d:13:7b:37)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189

> Transmission Control Protocol, Src Port: 80, Dst Port: 62250, Seq: 4201, Ack: 487, Len: 661

> [4 Reassembled TCP Segments (4861 bytes): #1919(1400), #1920(1400), #1921(1400), #1923(661)]

> Hypertext Transfer Protocol

> Line-based text data: text/html (98 lines)

1923

0000 ac b5 7d 13 7b 37 b0 0a d5 7c 61 6e 08 00 45 00 ...{7...·an· E·  
0018 02 b2 97 fd 40 00 25 06 84 54 80 77 f5 0c c0 a8 ...@%·T·w···  
0028 00 ed 00 50 f3 2a d7 11 a0 b3 c4 95 73 1c 50 18 ...P\*·s P·  
0030 00 ed 02 cd 00 60 6d 6f 6e 20 6c 61 77 2e 0a .....mm on law·  
0040 0a 3c 2f 70 3e 3c 70 3e 3c 61 20 6e 61 6d 65 3d </p><p> <name=·  
0058 22 38 22 3e 3c 73 72 72 6f 6e 67 3e 3c 68 33 3e "8"><str ong><h3>·  
0066 41 64 65 6e 64 6d 65 6e 74 20 56 49 49 49 3c 2f Amendmen t VIII</·  
0078 68 33 3e 3c 2f 73 75 72 6f 6e 67 3e 3c 2f 61 3e h3><str ong></a>  
0080 0a 0a 3c 70 3e 3c 2f 70 3e 3c 70 3e 45 78 63 65 </p></p><p>Exce  
0090 73 73 69 76 65 20 62 61 69 6c 20 73 68 61 6c ssive ba il shall  
00a0 20 6e 6f 74 20 62 65 0a 72 65 71 75 69 72 65 64 not be required  
00b0 2c 20 6e 6f 72 20 65 78 63 65 73 73 69 76 65 20 , nor ex cessive  
00c0 66 69 6e 65 73 0a 69 6d 70 6f 73 65 64 2c 20 6e fines im posed, n  
00d0 6f 72 20 63 72 75 65 6c 20 61 6e 64 20 75 6e 75 or cruel and unu

Frame (715 bytes) | Reassembled TCP (4861 bytes)

Profile: Default

## 13. What is the status code and phrase in the response?

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
171	16.398890	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
194	16.759066	128.119.245.12	192.168.0.189	HTTP	539	HTTP/1.1 404 Not Found (text/html)
+ 1736	99.334240	192.168.0.189	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+ 1923	99.630569	128.119.245.12	192.168.0.189	HTTP	715	HTTP/1.1 200 OK (text/html)
2019	99.889312	192.168.0.189	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
2033	100.185292	128.119.245.12	192.168.0.189	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Status code: 200

> Frame 1923: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface \Dev

> Ethernet II, Src: zte\_7c:61:6e (b0:0:a:d5:7c:61:6e), Dst: LiteonTechno\_13:7b:37 (ac:b5:7d:13:7b:37)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189

> Transmission Control Protocol, Src Port: 80, Dst Port: 62250, Seq: 4201, Ack: 487, Len: 661

> [4 Reassembled TCP Segments (4861 bytes): #1919(1400), #1920(1400), #1921(1400), #1923(661)]

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Mon, 24 Mar 2025 18:10:23 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.1

Last-Modified: Mon, 24 Mar 2025 05:59:01 GMT\r\n

ETag: "1194-631104d07d3bf"\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

0000 48 54 50 2f 31 2e 31 20 52 30 30 20 4f 4b 0d HTTP/1.1 200 OK·  
0010 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 32 34 20 4d ·Date: Mon, 24 M  
0020 61 72 28 32 30 32 20 31 38 3a 31 38 3a 32 33 ar 2025 18:10:23  
0030 20 47 40 54 0d 0s 65 65 72 76 65 72 3a 20 41 70 GHT-Se rver: Ap  
0040 61 63 68 65 65 65 32 2e 34 2e 36 20 28 43 65 66 74 achiv 2.4 .6 cent  
0050 47 53 29 20 4f 0d 66 65 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0.  
0060 52 6b 28 66 69 70 28 50 4f 50 2f 37 2e 34 2e 2K-fips PHP/7.4.  
0070 33 33 28 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 33\_mod\_p er1/2.0.  
0080 31 31 28 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 17\_Per/1 v5.16.3·  
0090 0a 4c 61 73 74 2d 4d 67 64 69 66 69 64 3a 20 ·Last-Mo dified:  
00a0 4d 6f 6e 2c 20 32 34 2d 4d 61 72 2d 32 30 32 35 Mon, 24 Mar 2025  
00b0 20 30 35 3c 35 39 3a 30 31 2d 47 4d 54 0d 0a 45 05:59:0 1 GMT+E  
00c0 54 61 67 3a 20 22 31 31 39 3d 2d 36 33 31 31 30 Tag: "11 94-63110  
00d0 34 64 38 37 64 33 62 66 22 0a 0a 43 63 63 65 78 4d07d3bf" ..Accp  
00e0 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d t-Ranges : bytes·  
00f0 0a 43 6f 74 65 6e 74 2d 4c 65 66 67 74 68 3a ·Content -Length:  
0100 20 34 35 30 30 0d 0a 4b 65 65 70 2d 41 6c 69 76 4500 ·Keep-Aliv  
0110 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 e: timeo ut5, m  
0120 78 3d 31 3a 30 0d 0a 43 6f 6e 66 65 63 74 69 6f x=100 ·C onnectio  
0130 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 n: Keep- Alive+C  
0140 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 ontent-T ype: tex  
0150 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d t/html; charset=

Frame (715 bytes) | Reassembled TCP (4861 bytes)

Packets: 4596 - Displayed: 6 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

The figure shows a screenshot of a Wi-Fi network monitoring application. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations and analysis. The main window has a title bar "http" and a status bar at the bottom indicating "HTTP Response Reason Phrase (http.response.phrase), 2 bytes" and "Packets: 4596 - Displayed: 6 (0.1%) - Dropped: 0 (0.0%)".

The central pane displays a table of network traffic. The columns are No., Time, Source, Destination, Protocol, Length, Info, and a large green highlighted area containing the text "phrase: OK".

No.	Time	Source	Destination	Protocol	Length	Info
171	16.398890	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
194	16.759066	128.119.245.12	192.168.0.189	HTTP	539	HTTP/1.1 404 Not Found (text/html)
1736	99.334240	192.168.0.189	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1923	99.630569	128.119.245.12	192.168.0.189	HTTP	715	HTTP/1.1 200 OK (text/html)
2019	99.889312	192.168.0.189	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
2033	100.185292	128.119.245.12	192.168.0.189	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The bottom right corner of the application window says "Profile: Default".

**14. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?**

The figure shows a Wi-Fi interface window at the top and the NetworkMiner tool below it. The NetworkMiner interface has tabs for 'http' and 'tcp'. The 'tcp' tab is active, displaying a list of captured TCP segments. A large watermark '4 tcp' is overlaid on the center of the NetworkMiner window.

**Wi-Fi**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
171	16. 3.98890	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
194	16. 759066	128.119.245.12	192.168.0.189	HTTP	539	HTTP/1.1 404 Not Found (text/html)
+ 1739	99. 334240	192.168.0.189	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
- 1923	99. 630569	128.119.245.12	192.168.0.189	HTTP	715	HTTP/1.1 200 OK (text/html)
2019	99. 889312	192.168.0.189	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
2033	100. 185292	128.119.245.12	192.168.0.189	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 1923: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface \Device\NPF\_{...}  
> Ethernet II, Src: zte\_7c:61:6e (08:0a:d5:7c:61:6e), Dst: LiteonTechno\_13:7b:37 (ac:b5:7d:13:7b:  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189  
> Transmission Control Protocol, Src Port: 80, Dst Port: 62250, Seq: 4201, Ack: 487, Len: 661  
+ [4 Reassembled TCP Segments (4861 bytes): #1919(1400), #1920(1400), #1921(1400), #1923(661)]  
[Frame: 1919, payload: 0-1399 (1400 bytes)]  
[Frame: 1920, payload: 1400-2799 (1400 bytes)]  
[Frame: 1921, payload: 2800-4199 (1400 bytes)]  
[Frame: 1923, payload: 4200-4860 (661 bytes)]  
[Segment count: 4]  
[Reassembled TCP length: 4861]  
[Reassembled TCP Data ...]: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c203234204c  
> Hypertext Transfer Protocol  
> Line-based text data: text/html (98 lines)

Frame (715 bytes) Reassembled TCP (4861 bytes)

Packets: 4596 - Displayed: 6 (0.1%) - Dropped: 0 (0.0%)

Profile: Default

# HTML Documents with Embedded Objects

15. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

6 http get

No.	Time	Source	Destination	Protocol	Length	Info
645	34.094873	192.168.0.189	23.58.31.18	HTTP	308	GET /DigicertGlobalRootG2.crl HTTP/1.1
648	34.168488	23.58.31.18	192.168.0.189	HTTP	517	HTTP/1.1 304 Not Modified
923	36.338269	192.168.0.189	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
969	36.768949	128.119.245.12	192.168.0.189	HTTP	1355	HTTP/1.1 200 OK (text/html)
1077	37.691934	192.168.0.189	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
1118	38.102859	128.119.245.12	192.168.0.189	HTTP	865	HTTP/1.1 200 OK (PNG)
1158	38.577112	192.168.0.189	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
1198	38.793487	178.79.137.164	192.168.0.189	HTTP	225	HTTP/1.1 301 Moved Permanently
1652	41.723760	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
1688	42.172821	128.119.245.12	192.168.0.189	HTTP	539	HTTP/1.1 404 Not Found (text/html)
1833	49.243843	192.168.0.189	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1838	49.610494	128.119.245.12	192.168.0.189	HTTP	294	HTTP/1.1 304 Not Modified

```

> Frame 645: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: zte_7c:61:6e (b0:0a:d5:7c:61)
> Internet Protocol Version 4, Src: 192.168.0.189, Dst: 23.58.31.18
> Transmission Control Protocol, Src Port: 62434, Dst Port: 80, Seq: 1, Ack: 1, Len: 254
> Hypertext Transfer Protocol
    
```

```

0000 b0 0a d5 7c 61 6e ac b5 7d 13 7b 37 08 00 45 00 ...[an... ] {7-E-
0010 01 26 cd 45 40 00 08 06 34 db c0 a8 00 bd 17 3a & E@... 4-----:
0020 0f 12 f3 e2 00 50 33 52 f2 f9 63 f5 bb 50 18 .....P3R -Yc -P
0030 02 02 9a c1 00 00 47 45 54 28 2f 44 69 67 69 43 .....GE T /DigIC
0040 65 72 74 47 6f 62 61 52 6f 6f 74 47 32 2e ergloba lRootG2.
0050 63 72 6c 28 48 54 54 50 2f 31 2e 31 0d 0a 43 61 crt HTTP /1.1 - Ca
0060 63 68 65 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 che-Cont rol: max
0070 2d 61 67 65 2d 3d 20 31 34 32 33 0d 0a 43 6f 6e -age = 1 423; Con
0080 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nnection: Keep-Al
0090 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a ive; Acc ept: */*
00a0 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 69 If-Mod ified-Si
00b0 6e 63 65 3a 20 54 75 65 20 31 38 20 4d 61 72 nce: Tue , 18 Mar
00c0 20 32 30 32 35 20 32 32 3a 31 35 3a 30 36 20 47 2022 22 :15:06 G
00d0 4d 54 0d 0a 49 66 2d 4d 6f 6e 65 2d 4d 61 74 63 MT - If-N one-Matc
00e0 68 3a 20 22 36 37 64 39 63 30 36 61 2d 34 39 33 h: "67d9 f06a-493
00f0 22 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d ".User-Agent: M
0100 59 63 72 6f 73 6f 66 74 2d 43 72 79 70 74 6f 41 icrosoft -Crypto
0110 50 49 2f 31 30 2e 39 0d 0e 48 6f 73 74 3a 20 63 PI/10.0 - Host: c
0120 72 6c 33 2e 64 69 67 69 63 65 72 74 2e 63 6f 6d r13.digi cert.com
0130 0d 0a 0d 0a
    
```

Packets: 2197 · Displayed: 12 (0.5%) · Dropped: 0 (0.0%) · Profile: Default

Destination address of get protocol

No.	Time	Source	Destination	Protocol	Length	Info
645	34.094873	192.168.0.189	23.58.31.18	HTTP	308	GET /DigicertGlobalRootG2.crl HTTP/1.1
648	34.168488	23.58.31.18	192.168.0.189	HTTP	517	HTTP/1.1 304 Not Modified
923	36.338269	192.168.0.189	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
969	36.768949	128.119.245.12	192.168.0.189	HTTP	1355	HTTP/1.1 200 OK (text/html)
1077	37.691934	192.168.0.189	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
1118	38.102859	128.119.245.12	192.168.0.189	HTTP	865	HTTP/1.1 200 OK (PNG)
1158	38.577112	192.168.0.189	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
1198	38.793487	178.79.137.164	192.168.0.189	HTTP	225	HTTP/1.1 301 Moved Permanently
1652	41.723760	192.168.0.189	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
1688	42.172821	128.119.245.12	192.168.0.189	HTTP	539	HTTP/1.1 404 Not Found (text/html)
1833	49.243843	192.168.0.189	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1838	49.610494	128.119.245.12	192.168.0.189	HTTP	294	HTTP/1.1 304 Not Modified

```

> Frame 923: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: LiteonTechno_13:7b:37 (ac:b5:7d:13:7b:37), Dst: zte_7c:61:6e (b0:0a:d5:7c:61)
> Internet Protocol Version 4, Src: 192.168.0.189, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 62437, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
> Hypertext Transfer Protocol
    
```

```

0000 b0 0a d5 7c 61 6e ac b5 7d 13 7b 37 08 00 45 00 ...[an... ] {7-E-
0010 02 00 04 f3 40 00 08 06 bd 1b c0 a8 00 bd 08 77 ....@... .w
0020 f5 0c f3 e2 00 50 33 52 f2 f9 63 f5 bb 50 18 .....P3R -Yc -P
0030 02 02 9a c1 00 00 47 45 54 28 2f 44 69 67 69 43 .....GE T /DigIC
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 50 2d 77 ergloba lRootG2.
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 34 2e 68 crt HTTP /1.1 - Ca
0060 74 6d 6c 28 48 54 50 2f 31 2e 31 0d 0a 43 61 che-Cont rol: max
0070 73 74 3a 20 67 63 69 61 2e 63 73 2e 75 6d 61 73 -age = 1 423; Con
0080 73 26 6d 75 0d 0a 43 6f 6e 65 63 74 69 6f nnection: Keep-Al
0090 6e 3a 20 6b 65 75 0d 0a 43 6f 6c 69 76 65 0d 0a 55 ike-Alive :U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-Requests : 1 -Use
00b0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 r-Agent: Mozilla
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 61 61 /5.0 (Wi ndows NT
00d0 2f 35 3e 20 28 57 69 6e 64 6f 77 73 20 4e 54 10.0; W in64; x6
00e0 28 31 3e 20 38 3b 20 57 69 6e 36 3b 2b 78 36 4) Apple WebKit/5
00f0 34 29 20 41 78 6c 65 57 65 62 4b 69 74 2f 35 37.36 (KHTML, li
0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 2b 6c 69 ke Gecko ) Chrome
0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 65 2d /134.0.0 .0 Safar
0120 2f 31 33 34 2e 30 2e 30 2e 30 20 53 61 66 61 72 1/537.36 - Accept
0130 69 62 2f 35 33 37 2e 33 36 0d 0a 41 63 63 70 74 : text/h tmlappl
0140 3a 20 74 65 78 74 2f 68 74 6d 6c 61 70 70 6c ication/ xhtml+xm
0150 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d l,application/xm
0160 6c 2c 61 70 70 69 63 61 74 69 6f 6e 2f 78 6d 
```

Packets: 2197 · Displayed: 12 (0.5%) · Dropped: 0 (0.0%) · Profile: Default

## 18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
706	19.339849	192.168.0.189	128.119.245.12	HTTP	556	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
778	19.622638	128.119.245.12	192.168.0.189	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
4182	71.172068	192.168.0.189	128.119.245.12	HTTP	582	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
4187	71.449420	128.119.245.12	192.168.0.189	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

**Status code: 401**

```
> Frame 778: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: zte_7c:61:6e (00:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189
> Transmission Control Protocol, Src Port: 80, Dst Port: 62563, Seq: 1, Ack: 503, Len: 717
  Hypertext Transfer Protocol
    HTTP/1.1 401 Unauthorized
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
      Date: Mon, 24 Mar 2025 18:41:42 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.1
      WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
  \r\n
  [Request in frame: 706]
  [Time since request: 0.28278900 seconds]
```

Packets: 4278 - Displayed: 4 (0.1%) - Dropped: 0 (0.0%) ||| Profile: Default

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

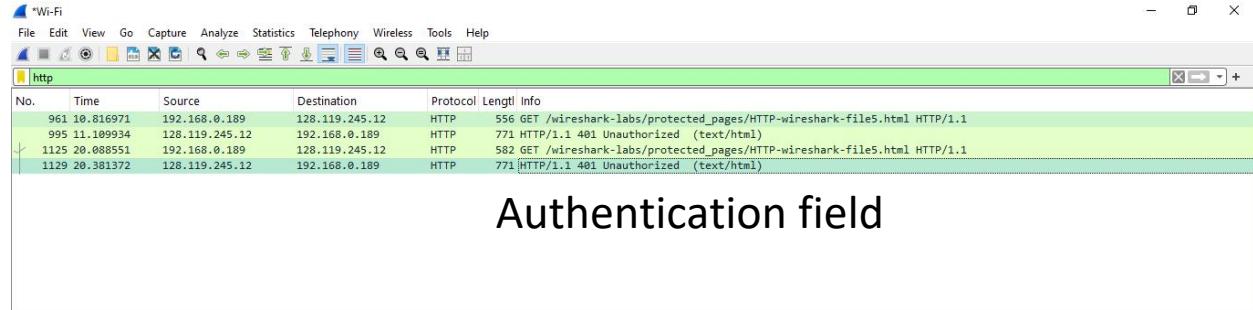
No.	Time	Source	Destination	Protocol	Length	Info
706	19.339849	192.168.0.189	128.119.245.12	HTTP	556	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
778	19.622638	128.119.245.12	192.168.0.189	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
4182	71.172068	192.168.0.189	128.119.245.12	HTTP	582	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
4187	71.449420	128.119.245.12	192.168.0.189	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

**Phrase: unauthorized**

```
> Frame 778: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: zte_7c:61:6e (00:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189
> Transmission Control Protocol, Src Port: 80, Dst Port: 62563, Seq: 1, Ack: 503, Len: 717
  Hypertext Transfer Protocol
    HTTP/1.1 401 Unauthorized
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
      Date: Mon, 24 Mar 2025 18:41:42 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.1
      WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
  \r\n
  [Request in frame: 706]
  [Time since request: 0.28278900 seconds]
```

Packets: 4278 - Displayed: 4 (0.1%) - Dropped: 0 (0.0%) ||| Profile: Default

## 19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?



### Authentication field

```
> Frame 1129: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Dev ^  
> Ethernet II, Src: zte_7c:61:6e (b0:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189  
> Transmission Control Protocol, Src Port: 80, Dst Port: 62711, Seq: 1, Ack: 529, Len: 717  
HTTP/1.1 401 Unauthorized\r\n  Response Version: HTTP/1.1  
  Status Code: 401  
  [Status Code Description: Unauthorized]  
  Response Phrase: Unauthorized  
  Date: Mon, 24 Mar 2025 18:55:12 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..  
  WWW-Authenticate: Basic realm="wireshark-students only"\r\nContent-Length: 381\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=iso-8859-1\r\n\r\n[Request in frame: 1125]  
[Time since request: 0.292821000 seconds]
```

```
0030 00 ed 30 ec 00 00 48 54 54 50 2f 31 2e 31 20 34 .-0-- HT TP/1.1 4  
0040 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 0d 01 Unauth orized  
0050 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 32 34 20 4d Date: M on, 24 M  
0060 61 72 20 32 30 32 35 20 31 38 3a 35 3a 31 32 ar 2025 18:55:12  
0070 20 47 4d 54 0a 0a 53 65 72 76 65 72 3a 20 41 70 GMT-S e rver: Ap  
0080 61 63 68 65 2f 32 2a 34 23 36 20 28 43 65 6e 74 ace/2.4 .6 (Cent  
0090 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0.  
0100 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e 2k-fips PHP/7.4.  
0101 33 33 20 6d 64 5f 70 65 72 6c 2f 32 2e 30 2e 33 mod_p erl/2.0.  
0102 31 31 20 50 65 72 62 2f 78 35 2e 31 36 2e 33 0d 11 Perl/ v5.16.3  
0103 0a 57 57 42 41 75 74 68 65 6e 74 69 63 61 74 .MM-Aut henticat  
0104 65 3a 20 42 61 73 65 63 72 65 61 6c 6d 3d 22 e: Basic realm="wireshar k-studen  
0105 77 69 72 65 73 68 61 72 6b 2d 73 74 75 64 65 6e ts only" - Conten  
0106 74 73 20 6f 6e 79 72 0d 0a 43 6f 6e 74 65 6e t-Length : 381 - K  
0107 65 65 70 2d 41 6c 69 76 65 3a 20 33 38 31 0a 04 b  
0108 75 74 3d 35 2c 20 6d 61 78 3d 31 30 0d 0a 43 eep-Aliv e: timeo  
0109 6f 6e 65 63 74 69 6f 63 3a 20 4b 65 65 78 2d ut=5, ma x=100 C  
0110 41 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 onnection: Keep-  
0111 79 70 65 3a 28 74 65 78 74 2f 68 74 6d 6e 3b 20 Alive: C ontent-T  
0112 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 ype: tex t/html;  
0113 2d 31 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 28 charset= iso-8859  
0114 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f -1---<!DOCTYPE HTML PUB LIC "-//"
```



### no authorization

```
> Frame 1129: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Dev ^  
> Ethernet II, Src: zte_7c:61:6e (b0:0a:d5:7c:61:6e), Dst: LiteonTechno_13:7b:37 (ac:b5:7d:13)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.189  
> Transmission Control Protocol, Src Port: 80, Dst Port: 62711, Seq: 1, Ack: 529, Len: 717  
HTTP/1.1 401 Unauthorized\r\n  Response Version: HTTP/1.1  
  Status Code: 401  
  [Status Code Description: Unauthorized]  
  Response Phrase: Unauthorized  
  Date: Mon, 24 Mar 2025 18:55:12 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..  
  WWW-Authenticate: Basic realm="wireshark-students only"\r\nContent-Length: 381\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=iso-8859-1\r\n\r\n[Request in frame: 1125]  
[Time since request: 0.292821000 seconds]
```

```
0030 00 ed 30 ec 00 00 48 54 54 50 2f 31 2e 31 20 34 .-0-- HT TP/1.1 4  
0040 30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 0d 01 Unauth orized  
0050 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 32 34 20 4d Date: M on, 24 M  
0060 61 72 20 32 30 32 35 20 31 38 3a 35 3a 31 32 ar 2025 18:55:12  
0070 20 47 4d 54 0a 0a 53 65 72 76 65 72 3a 20 41 70 GMT-S e rver: Ap  
0080 61 63 68 65 2f 32 2a 34 23 36 20 28 43 65 6e 74 ace/2.4 .6 (Cent  
0090 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0.  
0100 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e 2k-fips PHP/7.4.  
0101 33 33 20 6d 64 5f 70 65 72 6c 2f 32 2e 30 2e 33 mod_p erl/2.0.  
0102 31 31 20 50 65 72 62 2f 78 35 2e 31 36 2e 33 0d 11 Perl/ v5.16.3  
0103 0a 57 57 42 41 75 74 68 65 6e 74 69 63 61 74 .MM-Aut henticat  
0104 65 3a 20 42 61 73 65 63 72 65 61 6c 6d 3d 22 e: Basic realm="wireshar k-studen  
0105 77 69 72 65 73 68 61 72 6b 2d 73 74 75 64 65 6e ts only" - Conten  
0106 74 73 20 6f 6e 79 72 0d 0a 43 6f 6e 74 65 6e t-Length : 381 - K  
0107 65 65 70 2d 41 6c 69 76 65 3a 20 33 38 31 0a 04 b  
0108 75 74 3d 35 2c 20 6d 61 78 3d 31 30 0d 0a 43 eep-Aliv e: timeo  
0109 6f 6e 65 63 74 69 6f 63 3a 20 4b 65 65 78 2d ut=5, ma x=100 C  
0110 41 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 onnection: Keep-  
0111 79 70 65 3a 28 74 65 78 74 2f 68 74 6d 6e 3b 20 Alive: C ontent-T  
0112 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 ype: tex t/html;  
0113 2d 31 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 28 charset= iso-8859  
0114 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f -1---<!DOCTYPE HTML PUB LIC "-//"
```

Thank You