

Junhyeok Jeong

Bill Pfeil

CS 372-X001

10/27/2019

Lab 2

1. 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?

The image shows a Wireshark packet capture window titled "*Ethernet". The packet list pane displays several HTTP packets. Packet 453 is selected, showing a GET request for "/wireshark-labs/INTRO-wireshark-file1.html" from 10.0.0.24 to 128.119.245.12. The packet details pane shows the request method as GET, the request URI as "/wireshark-labs/INTRO-wireshark-file1.html", and the request version as HTTP/1.1. The packet bytes pane shows the raw data of the request, including the Host, Connection, and Upgrade-Insecure-Requests headers.

No.	Time	Source	Destination	Protocol	Length	Info
91	01:40:50.167905	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
93	01:40:50.269884	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
107	01:40:54.539004	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
108	01:40:54.645250	128.119.245.12	10.0.0.24	HTTP	292	HTTP/1.1 304 Not Modified
453	01:41:11.966660	10.0.0.24	128.119.245.12	HTTP	709	GET /wireshark-labs/INTRO-wireshark-file1.html
457	01:41:12.078213	128.119.245.12	10.0.0.24	HTTP	492	HTTP/1.1 200 OK (text/html)

[Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
[GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/INTRO-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n

0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTTP/1.1 · H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gaia.cs.uma
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 ss.edu · Connecti
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep-alive ·
00a0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade-Insecure
00b0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Request s: 1 · Us
00c0 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
00d0 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (Windows M
00e0 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64; x
00f0 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 64) AppleWebKit/
0100 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 537.36 (KHTML, l
0110 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d ike Gecko) Chrom

HTTP Request HTTP-Version (http.request.version), 8 bytes | Packets: 4450 · Displayed: 6 (0.1%) | Profile: Default

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
91	01:40:50.167905	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
93	01:40:50.269884	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
107	01:40:54.539004	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
108	01:40:54.645250	128.119.245.12	10.0.0.24	HTTP	292	HTTP/1.1 304 Not Modified
453	01:41:11.966660	10.0.0.24	128.119.245.12	HTTP	709	GET /wireshark-labs/INTRO-wireshark-file1.html
457	01:41:12.078213	128.119.245.12	10.0.0.24	HTTP	492	HTTP/1.1 200 OK (text/html)

< >

> Transmission Control Protocol, Src Port: 80, Dst Port: 54995, Seq: 1, Ack: 656, Len: 438

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Sun, 20 Oct 2019 08:41:12 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Last-Modified: Sun, 20 Oct 2019 05:59:01 GMT\r\n

0030 00 ef 8a 20 00 00 48 54 54 50 2f 31 2e 31 20 32 ... HTTP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 75 6e 00 OK-D ate: Sun

0050 2c 20 32 30 20 4f 63 74 20 32 30 31 39 20 30 38 , 20 Oct 2019 08

0060 3a 34 31 3a 31 32 20 47 4d 54 0d 0a 53 65 72 76 :41:12 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 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per

00b0 6c 2f 32 2e 30 2e 31 30 20 50 65 72 6c 2f 76 35 1/2.0.10 Perl/v5

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3-L ast-Modi

00d0 66 69 65 64 3a 20 53 75 6e 2c 20 32 30 20 4f 63 fied: Su n, 20 Oc

00e0 74 20 32 30 31 39 20 30 35 3a 35 39 3a 30 31 20 t 2019 0 5:59:01

- both my computer and server's HTTP version are 1.1(above screenshot)

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

The screenshot shows a Wireshark packet capture on an Ethernet interface. The packet list pane displays several HTTP packets. Packet 453 is selected, showing an HTTP GET request to `/wireshark-labs/INTRO-wireshark-file1.html` from source IP `10.0.0.24` to destination IP `128.119.245.12`. The packet details pane shows the HTTP message structure, including the request line, headers, and the full request URI. The headers include `Upgrade-Insecure-Requests: 1`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9`, `Accept-Encoding: gzip, deflate`, and `Accept-Language: en-US,en;q=0.9`. The status bar at the bottom indicates the selected packet is an HTTP Accept Language request, 33 bytes in size.

No.	Time	Source	Destination	Protocol	Length	Info
91	01:40:50.167905	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
93	01:40:50.269884	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
107	01:40:54.539004	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
108	01:40:54.645250	128.119.245.12	10.0.0.24	HTTP	292	HTTP/1.1 304 Not Modified
453	01:41:11.966660	10.0.0.24	128.119.245.12	HTTP	709	GET /wireshark-labs/INTRO-wireshark-file1.html
457	01:41:12.078213	128.119.245.12	10.0.0.24	HTTP	492	HTTP/1.1 200 OK (text/html)

```
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
> Cookie: _ga=GA1.2.543059244.1569647008; _gcl_aud=1.1.531762234.1569647008; _fbp=fb.1.1569647008255.1466163930\r\n
If-None-Match: "51-593e72a62308e"\r\n
If-Modified-Since: Wed, 02 Oct 2019 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

01d0 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 gzip, deflate-A
01e0 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 ccept-La nguage:
01f0 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d 0a en-US,en ;q=0.9-
0200 43 6f 6f 6b 69 65 3a 20 5f 67 61 3d 47 41 31 2e Cookie: _ga=GA1.
0210 32 2e 35 34 33 30 35 39 32 34 34 2e 31 35 36 39 2.543059 244.1569
0220 36 34 37 30 30 38 3b 20 5f 67 63 6c 5f 61 75 3d 647008; _gcl_aud=
0230 31 2e 31 2e 35 33 31 37 36 32 32 33 34 2e 31 35 1.1.5317 62234.15
0240 36 39 36 34 37 30 30 38 3b 20 5f 66 62 70 3d 66 69647008 ; _fbp=f
0250 62 2e 31 2e 31 35 36 39 36 34 37 30 30 38 32 35 b.1.1569 64700825
0260 35 2e 31 34 36 36 31 36 33 39 33 30 0d 0a 49 66 5.146616 3930-If
0270 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a 20 22 35 31 -None-Ma tch: "51
0280 2d 35 39 33 65 37 32 61 36 32 33 30 38 65 22 0d -593e72a 62308e".

HTTP Accept Language (http.accept_language), 33 bytes | Packets: 4969 · Displayed: 6 (0.1%) | Profile: Default

- US English (en-US) is accepted

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

- my computer's IP address is 10.0.0.24 and gaia.cs.umass.edu server's IP address is 128.119.245.12 (above screenshot)

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

- 200 OK (check the screenshot of Q1)

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

The screenshot shows a Wireshark packet capture of an HTTP response. The packet list at the top shows a GET request from 10.0.0.24 to 128.119.245.12. The packet details pane shows the response headers, including Last-Modified: Sun, 20 Oct 2019 05:59:01 GMT and Content-Length: 81. The packet bytes pane shows the raw data of the response, which is a 46-byte HTML document.

No.	Time	Source	Destination	Protocol	Length	Info
91	01:40:50.167905	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
93	01:40:50.269884	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
107	01:40:54.539004	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
108	01:40:54.645250	128.119.245.12	10.0.0.24	HTTP	292	HTTP/1.1 304 Not Modified
453	01:41:11.966660	10.0.0.24	128.119.245.12	HTTP	709	GET /wireshark-labs/INTRO-wireshark-file1.html
457	01:41:12.078213	128.119.245.12	10.0.0.24	HTTP	492	HTTP/1.1 200 OK (text/html)
148...	01:56:11.270141	10.0.0.24	96.6.139.222	HTTP	267	GET /en-US/livetile/preinstall?region=US&appid=...
148...	01:56:11.309387	96.6.139.222	10.0.0.24	HTTP/...	286	HTTP/1.1 200 OK

Packet Details:

```

Date: Sun, 20 Oct 2019 08:41:12 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Sun, 20 Oct 2019 05:59:01 GMT\r\n
ETag: "51-5955143908cc1"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
[Content length: 81]
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n

```

Packet Bytes:

```

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..Last-Modi
00d0 66 69 65 64 3a 20 53 75 6e 2c 20 32 30 20 4f 63 fied: Sun, 20 Oc
00e0 74 20 32 30 31 39 20 30 35 3a 35 39 3a 30 31 20 t 2019 0 5:59:01
00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 35 31 2d 35 GMT..ETag: "51-5
0100 39 35 35 31 34 33 39 30 38 63 63 31 22 0d 0a 41 95514390 8cc1"..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 38 31 0d 0a 4b 65 65 70 2d 41 6c gth: 81. ·Keep-Al
0140 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 ive: tim eout=5,
0150 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 max=100. ·Connect
0160 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d ion: Kee p-Alive.
0170 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 ·Content -Type: t

```

HTTP Last Modified (http.last_modified), 46 bytes

Packets: 17734 · Displayed: 8 (0.0%)

Profile: Default

- The last modified time is Sun, 20 October 2019 05:59:01 GMT (above screenshot)

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

- 81 bytes (above screenshot)

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.

The screenshot shows the Wireshark interface with a packet capture on the 'http' filter. The packet list displays several HTTP packets, including a GET request and a 200 OK response. The packet details pane for the selected packet (No. 457) shows the response body as HTML text. The packet bytes pane shows the raw hex and ASCII data of the response body.

No.	Time	Source	Destination	Protocol	Length	Info
91	01:40:50.167905	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
93	01:40:50.269884	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
107	01:40:54.539004	10.0.0.24	128.119.245.12	HTTP	734	GET /wireshark-labs/HTTP-wireshark-file1.html
108	01:40:54.645250	128.119.245.12	10.0.0.24	HTTP	292	HTTP/1.1 304 Not Modified
453	01:41:11.966660	10.0.0.24	128.119.245.12	HTTP	709	GET /wireshark-labs/INTRO-wireshark-file1.html
457	01:41:12.078213	128.119.245.12	10.0.0.24	HTTP	492	HTTP/1.1 200 OK (text/html)
148...	01:56:11.270141	10.0.0.24	96.6.139.222	HTTP	267	GET /en-US/livetile/preinstall?region=US&appid=...
148...	01:56:11.309387	96.6.139.222	10.0.0.24	HTTP/...	286	HTTP/1.1 200 OK

Packet Details (Selected Packet: 457):

- Line-based text data: text/html (3 lines)
 - <html>\n
 - Congratulations! You've downloaded the first Wireshark lab file!\n
 - </html>\n

Packet Bytes (Selected Packet: 457):

```

0130  67 74 68 3a 20 38 31 0d 0a 4b 65 65 70 2d 41 6c  gth: 81- -Keep-Al
0140  69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20  ive: tim eout=5,
0150  6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74  max=100- -Connect
0160  69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d  ion: Kee p-Alive-
0170  0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74  -Content -Type: t
0180  65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65  ext/html ; charse
0190  74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c  t=UTF-8- ...<html
01a0  3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f 6e  >.Congra tulation
01b0  73 21 20 20 59 6f 75 27 76 65 20 64 6f 77 6e 6c  s! You' ve downl
01c0  6f 61 64 65 64 20 74 68 65 20 66 69 72 73 74 20  oaded th e first
01d0  57 69 72 65 73 68 61 72 6b 20 6c 61 62 20 66 69  Wireshar k lab fi
01e0  6c 65 21 0a 3c 2f 68 74 6d 6c 3e 0a              le!</ht ml>-

```

- Line-base text data isn't displayed on packet-listing window

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?

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
167	02:42:33.072664	10.0.0.24	128.119.245.12	HTTP	481	GET /wireshark-labs/HTTP-wireshark-file2.
179	02:42:33.181705	128.119.245.12	10.0.0.24	HTTP	784	HTTP/1.1 200 OK (text/html)
277	02:42:34.836857	10.0.0.24	128.119.245.12	HTTP	593	GET /wireshark-labs/HTTP-wireshark-file2.
278	02:42:34.943122	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
284	02:42:35.055201	10.0.0.24	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
288	02:42:35.162044	128.119.245.12	10.0.0.24	HTTP	539	HTTP/1.1 404 Not Found (text/html)
291	02:42:36.550447	10.0.0.24	128.119.245.12	HTTP	593	GET /wireshark-labs/HTTP-wireshark-file2.
292	02:42:36.652408	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
294	02:42:36.659186	10.0.0.24	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1

> Frame 167: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface 0

> Ethernet II, Src: AsustekC_91:eb:e8 (04:d4:c4:91:eb:e8), Dst: CiscoSpv_b0:00:40 (f4:4b:2a:b0:00:40)

> Internet Protocol Version 4, Src: 10.0.0.24, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 53952, Dst Port: 80, Seq: 1, Ack: 1, Len: 427

> Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file2.html

Request Version: HTTP/1.1

0000 f4 4b 2a b0 00 40 04 d4 c4 91 eb e8 08 00 45 00 .K*..@.. ..E-

0010 01 d3 bf 7f 40 00 80 06 00 00 0a 00 00 18 80 77 ...@... ..w

0020 f5 0c d2 c0 00 50 bb 94 a6 a2 74 8b ac d9 50 18P... ..t...P-

0030 04 00 81 61 00 00 47 45 54 20 2f 77 69 72 65 73 ...a...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 41 63 tml HTTP /1.1-Ac

0070 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: te xt/html,

0080 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d applicat ion/xhtm

0090 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml,ap plicatio

00a0 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b n/xml;q= 0.9,*/;

00b0 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 q=0.8-A ccept-La

Ethernet (eth), 14 bytes

Packets: 335 · Displayed: 10 (3.0%) · Dropped: 0 (0.0%) Profile: Default

- I can't find "IF-MODIFIED-SINCE:" line in the first HTTP GET

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

Wireshark packet capture showing an HTTP GET request and response. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file2.html. The packet details pane shows the request URI and the response body as line-based text data. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
167	02:42:33.072664	10.0.0.24	128.119.245.12	HTTP	481	GET /wireshark-labs/HTTP-wireshark-file2.html
179	02:42:33.181705	128.119.245.12	10.0.0.24	HTTP	784	HTTP/1.1 200 OK (text/html)
277	02:42:34.836857	10.0.0.24	128.119.245.12	HTTP	593	GET /wireshark-labs/HTTP-wireshark-file2.html
278	02:42:34.943122	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
284	02:42:35.055201	10.0.0.24	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
288	02:42:35.162044	128.119.245.12	10.0.0.24	HTTP	539	HTTP/1.1 404 Not Found (text/html)
291	02:42:36.550447	10.0.0.24	128.119.245.12	HTTP	593	GET /wireshark-labs/HTTP-wireshark-file2.html
292	02:42:36.652408	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
294	02:42:36.659186	10.0.0.24	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1

[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

```

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

Packets: 335 · Displayed: 10 (3.0%) · Dropped: 0 (0.0%) · Profile: Default

- the server explicitly returned the contents of the file as the Line-based text data (above screenshot)

10. 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?

Wireshark packet capture showing an HTTP GET request and response. The packet list shows a GET request for a file, followed by a 200 OK response. The packet details show the request line and headers. The packet bytes show the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
167	02:42:33.072664	10.0.0.24	128.119.245.12	HTTP	481	GET /wireshark-labs/HTTP-wireshark-file2.
179	02:42:33.181705	128.119.245.12	10.0.0.24	HTTP	784	HTTP/1.1 200 OK (text/html)
277	02:42:34.836857	10.0.0.24	128.119.245.12	HTTP	593	GET /wireshark-labs/HTTP-wireshark-file2.
278	02:42:34.943122	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
284	02:42:35.055201	10.0.0.24	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
288	02:42:35.162044	128.119.245.12	10.0.0.24	HTTP	539	HTTP/1.1 404 Not Found (text/html)
291	02:42:36.550447	10.0.0.24	128.119.245.12	HTTP	593	GET /wireshark-labs/HTTP-wireshark-file2.
292	02:42:36.652408	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
294	02:42:36.659186	10.0.0.24	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1

Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.10
 Accept-Encoding: gzip, deflate\r\n
 Host: gaia.cs.umass.edu\r\n
 If-Modified-Since: Sun, 20 Oct 2019 05:59:02 GMT\r\n
 If-None-Match: "173-595514390bf89"\r\n
 Connection: Keep-Alive\r\n
 \r\n
[\[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html\]](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html)
 [HTTP request 2/3]

01a0 2e 31 38 33 36 32 0d 0a 41 63 63 65 70 74 2d 45 .18362·
 01b0 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d
 01c0 65 66 6c 61 74 65 0d 0a 48 6f 73 74 3a 20 67 61 eflate·
 01d0 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d Host: ga
 01e0 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 69 6e ia.cs.um ass.edu·
 01f0 63 65 3a 20 53 75 6e 2c 20 32 30 20 4f 63 74 20 ·If-Modi fied-Sin
 0200 32 30 31 39 20 30 35 3a 35 39 3a 30 32 20 47 4d ce: Sun, 20 Oct
 0210 54 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 2019 05: 59:02 GM
 0220 3a 20 22 31 37 33 2d 35 39 35 35 31 34 33 39 30 T·If-No ne-Match
 0230 62 66 38 39 22 0d 0a 43 6f 6e 6e 65 63 74 69 6f : "173-5 95514390
 0240 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d bf89"··C onnectio
 0250 0a · n: Keep- Alive··

Request line (http.request.line), 50 bytes | Packets: 335 · Displayed: 10 (3.0%) · Dropped: 0 (0.0%) | Profile: Default

- Yes, the second HTTP GET has “IF-MODIFIED-SINCE:”. It followed the time stamp (Sun, 20 Oct 2019 05:59:02 GMT\r\n)

11. 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.

The screenshot shows a Wireshark packet capture on an Ethernet interface. The packet list displays several HTTP requests and responses. The selected packet is an HTTP 304 Not Modified response. The packet details pane shows the response structure, including the status code and phrase. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
167	02:42:33.072664	10.0.0.24	128.119.245.12	HTTP	481	GET /wireshark-labs/HTTP-wireshark-file2.
179	02:42:33.181705	128.119.245.12	10.0.0.24	HTTP	784	HTTP/1.1 200 OK (text/html)
277	02:42:34.836857	10.0.0.24	128.119.245.12	HTTP	593	GET /wireshark-labs/HTTP-wireshark-file2.
278	02:42:34.943122	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
284	02:42:35.055201	10.0.0.24	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
288	02:42:35.162044	128.119.245.12	10.0.0.24	HTTP	539	HTTP/1.1 404 Not Found (text/html)
291	02:42:36.550447	10.0.0.24	128.119.245.12	HTTP	593	GET /wireshark-labs/HTTP-wireshark-file2.
292	02:42:36.652408	128.119.245.12	10.0.0.24	HTTP	293	HTTP/1.1 304 Not Modified
294	02:42:36.659186	10.0.0.24	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1

Transmission Control Protocol, Src Port: 80, Dst Port: 53952, Seq: 731, Ack: 967, Len: 239

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]

Response Version: HTTP/1.1

Status Code: 304

[Status Code Description: Not Modified]

Response Phrase: Not Modified

Date: Sun, 20 Oct 2019 09:42:35 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Connection: Keep-Alive\r\n

0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT- Se rver: Ap
0080 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 ache/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.
00a0 32 6b 2d 66 69 70 73 20 50 48 50 2f 35 2e 34 2e 2k-fips PHP/5.4.
00b0 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 16 mod_p erl/2.0.
00c0 31 30 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 10 Perl/ v5.16.3.
00d0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 -Connect ion: Kee
00e0 70 2d 41 6c 69 76 65 0d 0a 4b 65 65 70 2d 41 6c p-Alive -Keep-Al
00f0 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 ive: tim eout=5,
0100 6d 61 78 3d 39 39 0d 0a 45 54 61 67 3a 20 22 31 max=99 ETag: "1
0110 37 33 2d 35 39 35 35 31 34 33 39 30 62 66 38 39 73-59551 4390bf89
0120 22 0d 0a 0d 0a "....

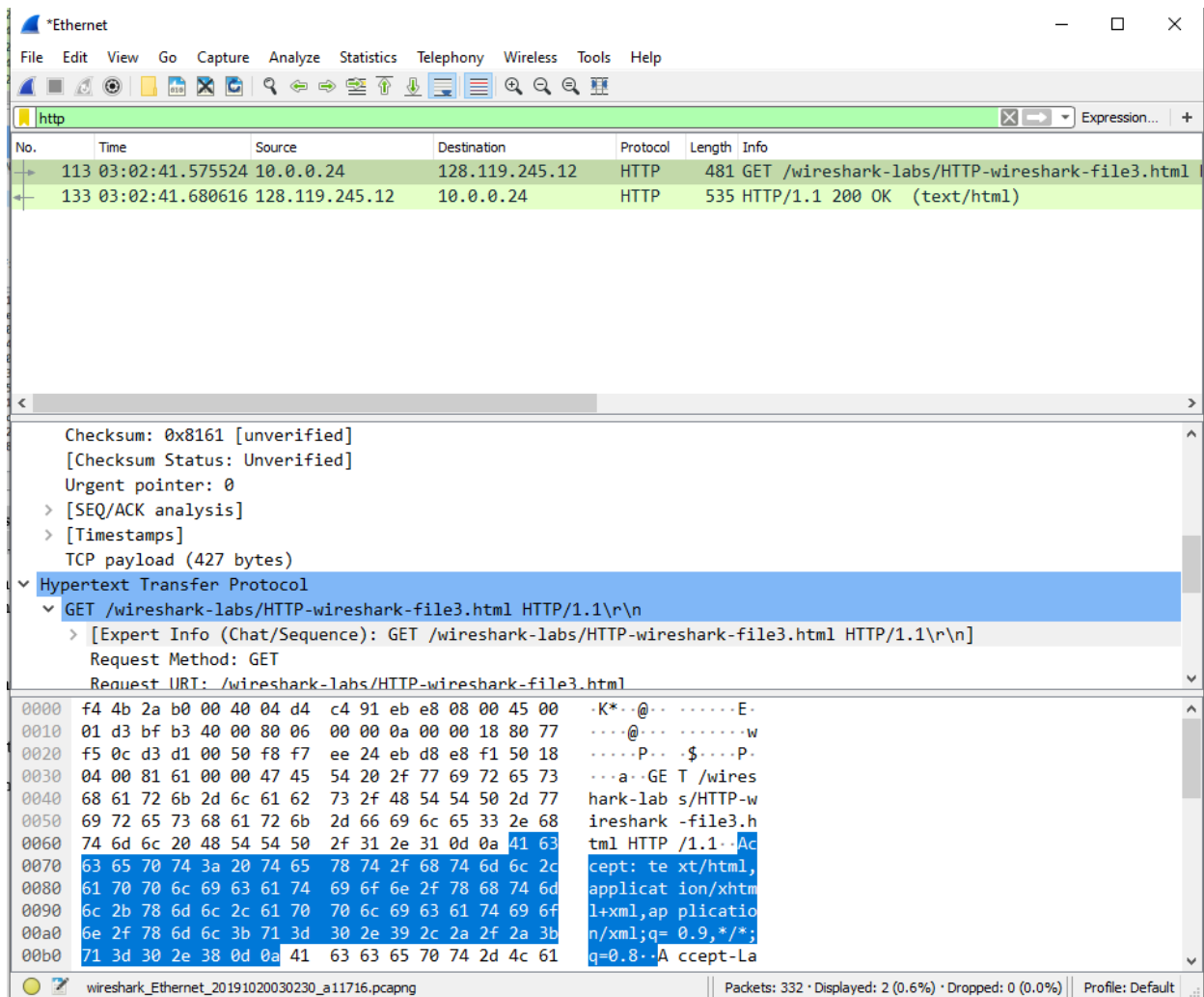
HTTP Response Status Code (http.response.code), 3 bytes

Packets: 335 · Displayed: 10 (3.0%) · Dropped: 0 (0.0%) Profile: Default

- The second HTTP GET returned status code and phrase, “304 Not Modified” and the packet is shorter than the first one. In addition, it didn’t include the Line-based text data.

3. Retrieving Long Documents

12. 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?



- There is only one HTTP GET request message with packet number 113

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

- The packet number 133 contains the status code and phrase (above screenshot)

14. What is the status code and phrase in the response?

- “200 OK” on the packet number 133 (above screenshot)

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

Wireshark interface showing a packet capture on the Ethernet interface. The packet list shows two HTTP packets:

No.	Time	Source	Destination	Protocol	Length	Info
113	03:02:41.575524	10.0.0.24	128.119.245.12	HTTP	481	GET /wireshark-labs/HTTP-wireshark-file3.html
133	03:02:41.680616	128.119.245.12	10.0.0.24	HTTP	535	HTTP/1.1 200 OK (text/html)

The packet details pane shows the structure of the HTTP response (packet 133):

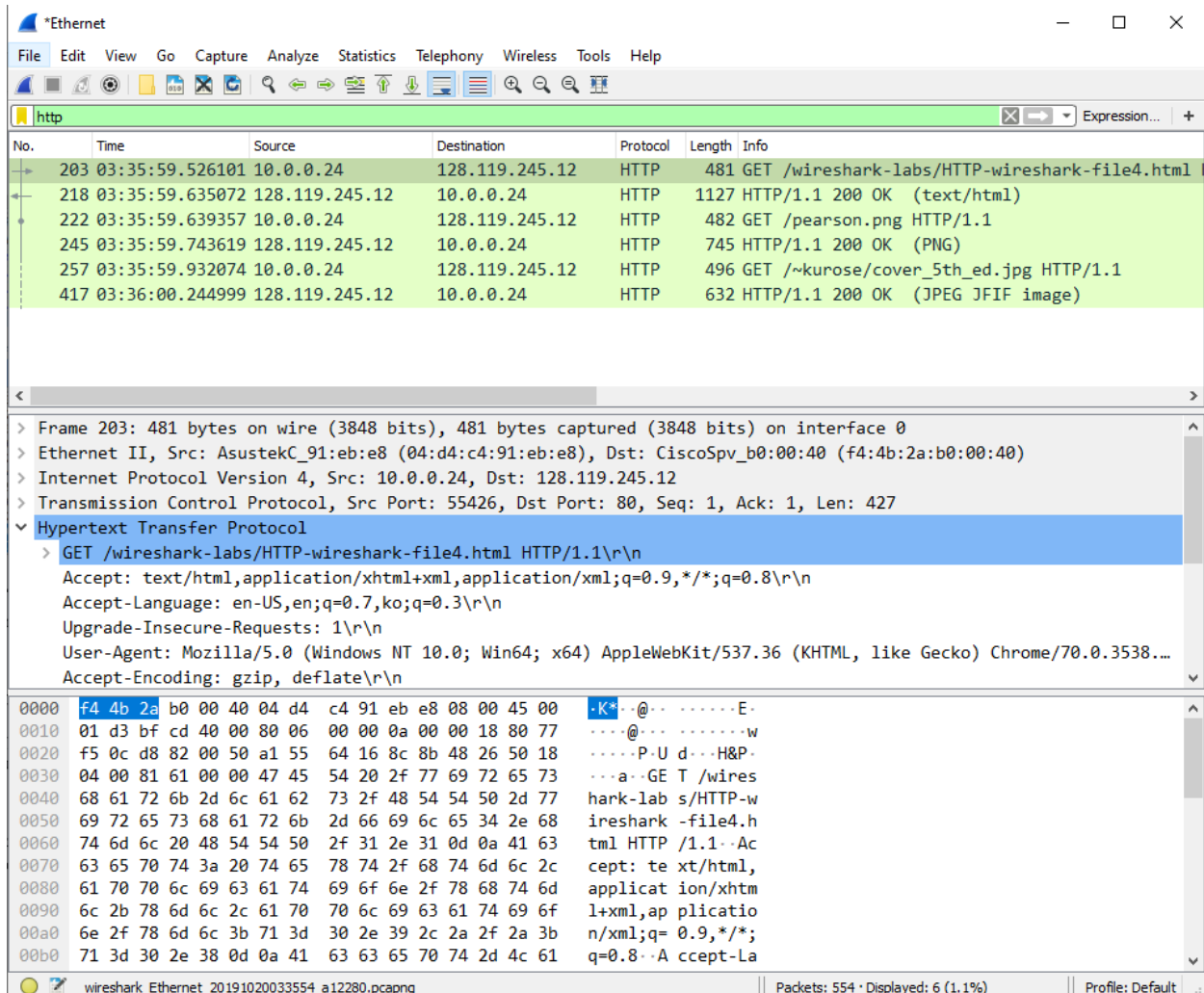
- Transmission Control Protocol, Src Port: 80, Dst Port: 54225, Seq: 4381, Ack: 428, Len: 481
 - [4 Reassembled TCP Segments (4861 bytes): #127(1460), #129(1460), #131(1460), #133(481)]
 - [Frame: 127, payload: 0-1459 (1460 bytes)]
 - [Frame: 129, payload: 1460-2919 (1460 bytes)]
 - [Frame: 131, payload: 2920-4379 (1460 bytes)]
 - [Frame: 133, payload: 4380-4860 (481 bytes)]
 - [Segment count: 4]
 - [Reassembled TCP length: 4861]
 - [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a2053...]
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK
 - 0a 44 61 74 65 3a 20 53 75 6e 2c 20 32 30 20 4f .Date: Sun, 20 Oct 2019 10:02:41
 - 63 74 20 32 30 31 39 20 31 30 3a 30 32 3a 34 31 ct 2019 10:02:41
 - 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT Server: Apache/2.4.6 (Cent
 - 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 OS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3
 - 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3
 - 32 6b 2d 66 69 70 73 20 50 48 50 2f 35 2e 34 2e 2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3
 - 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 16 mod_perl/2.0.10 Perl/v5.16.3
 - 31 30 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 10 Perl/v5.16.3
 - 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 .Last-Modified: Sun, 20 Oct 2019
 - 53 75 6e 2c 20 32 30 20 4f 63 74 20 32 30 31 39 Sun, 20 Oct 2019

The packet bytes pane shows the raw data of the HTTP response, including the status line and headers.

- There are 4 TCP segments carried the single HTTP response

4. HTML Documents with Embedded Objects

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



- There are 3 HTTP GET request messages which are for requesting http page, pearson logo as png file, and a textbook cover image as jpg file.

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain

- I think my browser (Microsoft Edge) downloaded the two images serially because the first image file (logo) completed the request and send process first and then the second image file (textbook cover) completed. If the process did parallelly, both HTTP GET request messages would be in the same time line.

5. HTTP Authentication

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

Wireshark interface showing a packet capture on the Ethernet interface. The filter is set to http. The packet list shows several HTTP GET requests to /wireshark-labs/protected_pages/HTTP-wires. The packet details pane shows the selected packet (No. 210) as an HTTP 1.1 401 Unauthorized response. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
198	03:54:33.660328	10.0.0.24	128.119.245.12	HTTP	496	GET /wireshark-labs/protected_pages/HTTP-wires
210	03:54:33.766076	128.119.245.12	10.0.0.24	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
212	03:54:33.766624	10.0.0.24	128.119.245.12	HTTP	555	GET /wireshark-labs/protected_pages/HTTP-wires
214	03:54:33.869372	128.119.245.12	10.0.0.24	HTTP	582	HTTP/1.1 404 Not Found (text/html)
310	03:54:40.036740	10.0.0.24	128.119.245.12	HTTP	497	GET /wireshark-labs/protected_pages/HTTP-wires
322	03:54:40.141916	128.119.245.12	10.0.0.24	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
476	03:54:52.467426	10.0.0.24	128.119.245.12	HTTP	556	GET /wireshark-labs/protected_pages/HTTP-wires
480	03:54:52.590855	128.119.245.12	10.0.0.24	HTTP	544	HTTP/1.1 200 OK (text/html)

Packet Details:

- Transmission Control Protocol, Src Port: 80, Dst Port: 56032, Seq: 1, Ack: 443, Len: 717
- Hypertext Transfer Protocol
 - HTTP/1.1 401 Unauthorized\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 401
 - [Status Code Description: Unauthorized]
 - Response Phrase: Unauthorized
 - Date: Sun, 20 Oct 2019 10:54:33 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
 - WWW-Authenticate: Basic realm="wireshark-students only"\r\n

Packet Bytes:

```

0030  00 ed 2b 21 00 00 48 54 54 50 2f 31 2e 31 20 34  ..+!..HT TP/1.1 4
0040  30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 0d  01 Unaut horized
0050  0a 44 61 74 65 3a 20 53 75 6e 2c 20 32 30 20 4f  .Date: S un, 20 0
0060  63 74 20 32 30 31 39 20 31 30 3a 35 34 3a 33 33  ct 2019 10:54:33
0070  20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70  GMT..Se rver: Ap
0080  61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74  ache/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.
00a0  32 6b 2d 66 69 70 73 20 50 48 50 2f 35 2e 34 2e  2k-fips PHP/5.4.
00b0  31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e  16 mod_p erl/2.0.
00c0  31 30 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d  10 Perl/ v5.16.3
00d0  0a 57 57 57 2d 41 75 74 68 65 6e 74 69 63 61 74  .WWW-Aut henticat
00e0  65 3a 20 42 61 73 69 63 20 72 65 61 6c 6d 3d 22  e: Basic realm="

```

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

Packets: 521 · Displayed: 8 (1.5%) · Dropped: 0 (0.0%) | Profile: Default

- The server's response is "401 Unauthorized" as the initial HTTP GET message

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

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
198	03:54:33.660328	10.0.0.24	128.119.245.12	HTTP	496	GET /wireshark-labs/protected_pages/HTTP-wires
210	03:54:33.766076	128.119.245.12	10.0.0.24	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
212	03:54:33.766624	10.0.0.24	128.119.245.12	HTTP	555	GET /wireshark-labs/protected_pages/HTTP-wires
214	03:54:33.869372	128.119.245.12	10.0.0.24	HTTP	582	HTTP/1.1 404 Not Found (text/html)
310	03:54:40.036740	10.0.0.24	128.119.245.12	HTTP	497	GET /wireshark-labs/protected_pages/HTTP-wires
322	03:54:40.141916	128.119.245.12	10.0.0.24	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
476	03:54:52.467426	10.0.0.24	128.119.245.12	HTTP	556	GET /wireshark-labs/protected_pages/HTTP-wires
480	03:54:52.590855	128.119.245.12	10.0.0.24	HTTP	544	HTTP/1.1 200 OK (text/html)

Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102\r\n
 Accept-Encoding: gzip, deflate\r\n
 Host: gaia.cs.umass.edu\r\n
 Connection: Keep-Alive\r\n
 Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
 \r\n
[\[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html\]](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html)
 [HTTP request 2/2]
[\[Prev request in frame: 198\]](#)

0170 65 2f 37 30 2e 30 2e 33 35 33 38 2e 31 30 32 20 e/70.0.3 538.102
 0180 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45 64 Safari/5 37.36 Ed
 0190 67 65 2f 31 38 2e 31 38 33 36 32 0d 0a 41 63 63 ge/18.18 362 Acc
 01a0 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a ept-Enco ding: gz
 01b0 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 48 6f 73 ip, defl ate Hos
 01c0 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 t: gaia. cs.umass
 01d0 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e .edu Co nnection
 01e0 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 75 : Keep-A live Au
 01f0 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 thorizat ion: Bas
 0200 69 63 20 64 32 6c 79 5a 58 4e 6f 59 58 4a 72 4c ic d2lyZ XNoYXJrL
 0210 58 4e 30 64 57 52 6c 62 6e 52 7a 4f 6d 35 6c 64 XN0dWRlbn RzM5ld
 0220 48 64 76 63 6d 73 3d 0d 0a 0d 0a Hdvcms= - - -

HTTP Authorization header (http.authorization), 59 bytes

Packets: 521 · Displayed: 8 (1.5%) · Dropped: 0 (0.0%) Profile: Default

- The new field is included the authorization with the key (Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=) because I sent username and password to the server when I requested to access

Extra credit #3

Socket programming in c

1. Code screenshots

```
ec_lab2.c
1  #include<stdio.h>
2  #include<string.h> //strlen
3  #include<sys/socket.h>
4  #include<arpa/inet.h> //inet_addr
5
6  int main(int argc , char *argv[])
7  {
8      int socket_desc;
9      struct sockaddr_in server;
10     char *message , server_reply[2000];
11
12     //Create socket
13     socket_desc = socket(AF_INET , SOCK_STREAM , 0);
14     if (socket_desc == -1)
15     {
16         printf("Could not create socket");
17     }
18
19     server.sin_addr.s_addr = inet_addr("172.217.14.196");
20     server.sin_family = AF_INET;
21     server.sin_port = htons( 80 );
22
23     //Connect to remote server
24     if (connect(socket_desc , (struct sockaddr *)&server , sizeof(server)) < 0)
25     {
26         puts("connect error");
27         return 1;
28     }
29
30     puts("Connected\n");
31
32     //Send some data
33     message = "GET / HTTP/1.1\r\n\r\n";
34     if( send(socket_desc , message , strlen(message) , 0) < 0)
35     {
36         puts("Send failed");
37         return 1;
38     }
39     puts("Data Send\n");
```



```

41 //Receive a reply from the server
42 if( recv(socket_desc, server_reply , 2000 , 0) < 0)
43 {
44     puts("recv failed");
45 }
46 puts("Reply received\n");
47 puts(server_reply);
48
49 return 0;
50 }
51

```

2. www.google.com

```

[jeongju@flip3 ~/cs372]$ gcc ec_lab2.c -o lab2
[jeongju@flip3 ~/cs372]$ ./lab2
Connected

Data Send

Reply received

HTTP/1.1 200 OK
Date: Mon, 21 Oct 2019 00:13:54 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2019-10-21-00; expires=Wed, 20-Nov-2019 00:13:54 GMT; path=/; domain=.google.com; SameSite=none
Set-Cookie: NID=189=qubg9poojHXP9neVmK2ioR06XT_1Z9rc1j94d9Q-Lw035eCIb3N0676s6khcE9A_Dt6uU9vpSbbgeHtHfx_1lzmQqzh3EMXJ9nxHpdjdfriGNn9UnQq2I6tuf8c16eTh6_UhupZPEfbq83BT61qHvXe6H0qfN2IBvBW8LJIEGFM; expires=Tue, 21-Apr-2020 00:13:54 GMT; path=/; domain=.google.com; HttpOnly
Accept-Ranges: none
Vary: Accept-Encoding
Transfer-Encoding: chunked

5e09
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en"><head><meta content="Se
arch the world's information, including webpages, images, videos and more. Google has many special featu

```

3. <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

```
[jeongju@flip3 ~/cs372]$ gcc ec_lab2.c -o lab2
[jeongju@flip3 ~/cs372]$ ./lab2
Connected
Data Send
Reply received
HTTP/1.1 400 Bad Request
Date: Mon, 21 Oct 2019 00:19:52 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
</body></html>

[jeongju@flip3 ~/cs372]$ █
```

- The ip address of <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html> is 128.119.245.12. However, I tried to run with that ip address, always got 400 bad request status and code.