

Wireshark Lab 1 -- Getting Started

Jiaying Li
JI10919

Lab environment:

Answer: My PC uses macOS Catalina 10.15.6, shows the following setting with *ifconfig*:

```
(base) JesLeedeMBP:~ jeslee$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xffffffff
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
            nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether ac:bc:32:7b:83
        inet6 fe80::1c81:11c:970e:3b33%en0 prefixlen 64 secured scopeid 0x4
        inet 192.168.1.155 netmask 0xfffffff0 broadcast 192.168.1.255
            nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=460<TS04,TS06,CHANNEL_IO>
    ether 82:13:09:8a:17:40
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=460<TS04,TS06,CHANNEL_IO>
    ether 82:13:09:8a:17:41
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=63<RXCSUM,TXCSUM,TS04,TS06>
    ether 82:13:09:8a:17:40
    Configuration:
        id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
        maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
        root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
        ipfilter disabled flags 0x0
    member: en1 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 5 priority 0 path cost 0
    member: en2 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 6 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    options=400<CHANNEL_IO>
    ether 0e:bc:32:7b:83
        media: autoselect
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
    options=400<CHANNEL_IO>
    ether e2:8b:ae:0c:af:c5
        inet6 fe80::e08b:aeff:fe0c:afc5%awdl0 prefixlen 64 scopeid 0x9
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether e2:8b:ae:0c:af:c5
        inet6 fe80::e08b:aeff:fe0c:afc5%llw0 prefixlen 64 scopeid 0xa
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    inet6 fe80::f58d:6031:ca37:b987%utun0 prefixlen 64 scopeid 0xb
        nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
    inet6 fe80::af3a:6b7e:729f:e148%utun1 prefixlen 64 scopeid 0xc
        nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    inet6 fe80::8888:4408:7f6e:76ea%utun2 prefixlen 64 scopeid 0xd
        nd6 options=201<PERFORMNUD,DAD>
utun3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    inet6 fe80::2b53:b72c:6e42:c414%utun3 prefixlen 64 scopeid 0xe
        nd6 options=201<PERFORMNUD,DAD>
```

The Basic HTTP GET/response interaction. Answer the following questions:

Wi-Fi: en0

No.	Time	Source	Destination	Protocol	Length	Info
904	21:12:42.319016	192.168.1.155	203.205.179.144	HTTP	775	POST /mmtls/2ba97279 HTTP/1.1
906	21:12:42.695121	203.205.179.144	192.168.1.155	HTTP	1245	HTTP/1.1 200 OK
969	21:12:59.813747	192.168.1.155	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
971	21:12:59.840015	128.119.245.12	192.168.1.155	HTTP	552	HTTP/1.1 200 OK (text/html)

Frame 969: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface en0, id 0

Ethernet II, Src: Apple_7b:7f:83 (ac:bc:32:7b:7f:83), Dst: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)

Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 57146, Dst Port: 80, Seq: 1, Ack: 1, Len: 397

Hypertext Transfer Protocol

 ▼ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n

 ► [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]

 Request Method: GET

 Request URI: /wireshark-labs/HTTP-wireshark-file1.html

 Request Version: HTTP/1.1

 Host: gaia.cs.umass.edu\r\n

 Upgrade-Insecure-Requests: 1\r\n

 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15\r\n

 Accept-Language: en-us\r\n

 Accept-Encoding: gzip, deflate\r\n

 Connection: keep-alive\r\n

\r\n

 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

 [HTTP request 1/1]

 [Response in frame: 971]

0070 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ··Host:

0080 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed

0090 75 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 u·Upgra de-Insec

00a0 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d ure-Requ ests: 1·

HTTP Request HTTP-Version (http.request.version), 8 bytes

Packets: 1084 - Displayed: 4 (0.4%) - Dropped: 0 (0.0%) - Profile: Default

Wi-Fi: en0

No.	Time	Source	Destination	Protocol	Length	Info
904	21:12:42.319016	192.168.1.155	203.205.179.144	HTTP	775	POST /mmtls/2ba97279 HTTP/1.1
906	21:12:42.695121	203.205.179.144	192.168.1.155	HTTP	1245	HTTP/1.1 200 OK
969	21:12:59.813747	192.168.1.155	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
971	21:12:59.840015	128.119.245.12	192.168.1.155	HTTP	552	HTTP/1.1 200 OK (text/html)

Frame 971: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0

Ethernet II, Src: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89), Dst: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155

Transmission Control Protocol, Src Port: 80, Dst Port: 57146, Seq: 1, Ack: 398, Len: 486

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, 27 Sep 2020 01:12:59 GMT\r\n

 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n

 Last-Modified: Sat, 26 Sep 2020 05:59:01 GMT\r\n

 ETag: "80-5b0312148b021"\r\n

 Accept-Ranges: bytes\r\n

 Content-Length: 128\r\n

 Keep-Alive: timeout=5, max=100\r\n

 Connection: Keep-Alive\r\n

 Content-Type: text/html; charset=UTF-8\r\n

\r\n

 [HTTP response 1/1]

 [Time since request: 0.026268000 seconds]

0000 ac bc 32 7b 7f 83 b8 f8 53 5e ea 89 08 00 45 02 ..2{.... S^.... E·

0010 02 1a cb 63 40 00 33 06 42 b1 80 77 f5 0c c0 a8 ..c@.3: B·w....

0020 01 9b 00 50 df 3a 50 3c 7e 8d ee 29 7f aa 80 18 ..P:P< ~...)...

0030 00 eb 6f ab 00 00 01 01 08 0a c1 13 b5 f6 2b ca ..o.....+..

wireshark_Wi-Fi_20200926211133.Zho3tk.pcapng

Packets: 1084 - Displayed: 4 (0.4%) - Dropped: 0 (0.0%) - Profile: Default

Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer: As shown in the screenshots for GET and Response above, HTTP get and reply message below, highlighted with yellow, my browser is running HTTP 1.1, and server is running HTTP 1.1

Q2. What languages (if any) does your browser indicate that it can accept to the server?

Answer: As shown in the screenshot for GET above, HTTP get message below, highlighted with gray, my browser indicate that it can accept en-us (US English).

Q3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Answer: As shown in the screenshot for Response above, HTTP reply message below, highlighted with green, the IP address of my computer (shown as destination) is 192.168.1.155, the IP address of gaia.cs.umass.edu server (shown as Source) is 128.119.245.12.

Q4. What is the status code returned from the server to your browser?

Answer: As shown in the screenshot for Response above, HTTP reply message below, highlighted with purple(white in the screenshot), the status code returned from the server to my browser is 200, the phrase is OK.

Q5. When was the HTML file that you are retrieving last modified at the server?

Answer: As shown in the screenshot for Response above, HTTP reply message below, highlighted with blue, the HTML file that I am retrieving last modified at Sat, 26 Sep 2020 05:59:01 GMT at the server.

Q6. How many bytes of content are being returned to your browser?

Answer: As shown in the screenshot for Response above, HTTP reply message below, highlighted with red, the size of content is 128 bytes.

Q7. 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.

Answer: No. All the data that in the headers are in the packet content window. As shown in the screenshot below, the headers of request and response can be checked in the browser and the information of them are circled in red and blue. All the header information is contained in the packet content window.

Congratulations. You've downloaded the file <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>!

The screenshot shows a browser window with the message "Congratulations. You've downloaded the file http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!". Below it, the Network tab of Wireshark is open, displaying an incoming request and an outgoing response for the same URL.

Request:

```

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15.6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive
    
```

Response:

```

HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
ETag: "80-5b0312148b021"
Last-Modified: Sat, 26 Sep 2020 05:59:01 GMT
Accept-Ranges: bytes
Date: Sun, 27 Sep 2020 01:12:59 GMT
Content-Length: 128
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3
    
```

HTTP GET message:

No.	Time	Source	Destination	Protocol	Length	Info
969	21:12:59.813747	192.168.1.155	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 969: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface en0, id 0
 Ethernet II, Src: Apple_7b:7f:83 (ac:bc:32:7b:7f:83), Dst: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)
 Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 57146, Dst Port: 80, Seq: 1, Ack: 1, Len: 397

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file1.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu\r\n

Upgrade-Insecure-Requests: 1\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15\r\n
 Accept-Language: en-us\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
 [HTTP request 1/1]
 [Response in frame: 971]

HTTP REPLY message:

No.	Time	Source	Destination	Protocol	Length	Info
971	21:12:59.840015	128.119.245.12	192.168.1.155	HTTP	552	HTTP/1.1 200 OK (text/html)

Frame 971: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
 Ethernet II, Src: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89), Dst: Apple_7b:7f:83 (ac:be:32:7b:7f:83)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155

Transmission Control Protocol, Src Port: 80, Dst Port: 57146, Seq: 1, Ack: 398, Len: 486
 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, 27 Sep 2020 01:12:59 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sat, 26 Sep 2020 05:59:01 GMT\r\n

ETag: "80-5b0312148b021"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.026268000 seconds]

[Request in frame: 969]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

File Data: 128 bytes

Line-based text data: text/html (4 lines)

The HTTP CONDITIONAL GET/response interaction. Answer the following questions:

Q8. 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?

Answer: As shown in the screenshot below, there is no “IF-MODIFIED-SINCE” line in the first HTTP GET.

The screenshot shows a Wireshark capture window. The packet list pane shows several network packets, with the first one highlighted. The details pane shows the packet structure, and the bytes pane shows the raw binary data. A red box highlights the first HTTP request (packet 48) in the details pane, which is a GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 request. The bytes pane shows the raw hex and ASCII representation of this request, including the host header and user agent.

No.	Time	Source	Destination	Protocol	Length	Info
44	22:04:26.769192	192.168.1.155	128.119.245.12	HTTP	557	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
48	22:04:26.800156	128.119.245.12	192.168.1.155	HTTP	796	HTTP/1.1 200 OK (text/html)
116	22:04:30.505589	192.168.1.155	128.119.245.12	HTTP	669	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
117	22:04:30.528954	128.119.245.12	192.168.1.155	HTTP	305	HTTP/1.1 304 Not Modified

Q9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer: As shown in the screenshot below, we can see that the server explicitly return the contents of the file. We can see the content under the “Line-based text data”. And the content here is exactly the content we can see on the webpage(<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>).

Content-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/2]\n[Time since request: 0.030964000 seconds]\n[Request in frame: 44]\n[Next request in frame: 116]\n[Next response in frame: 117]\n[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]\nFile Data: 371 bytes

```

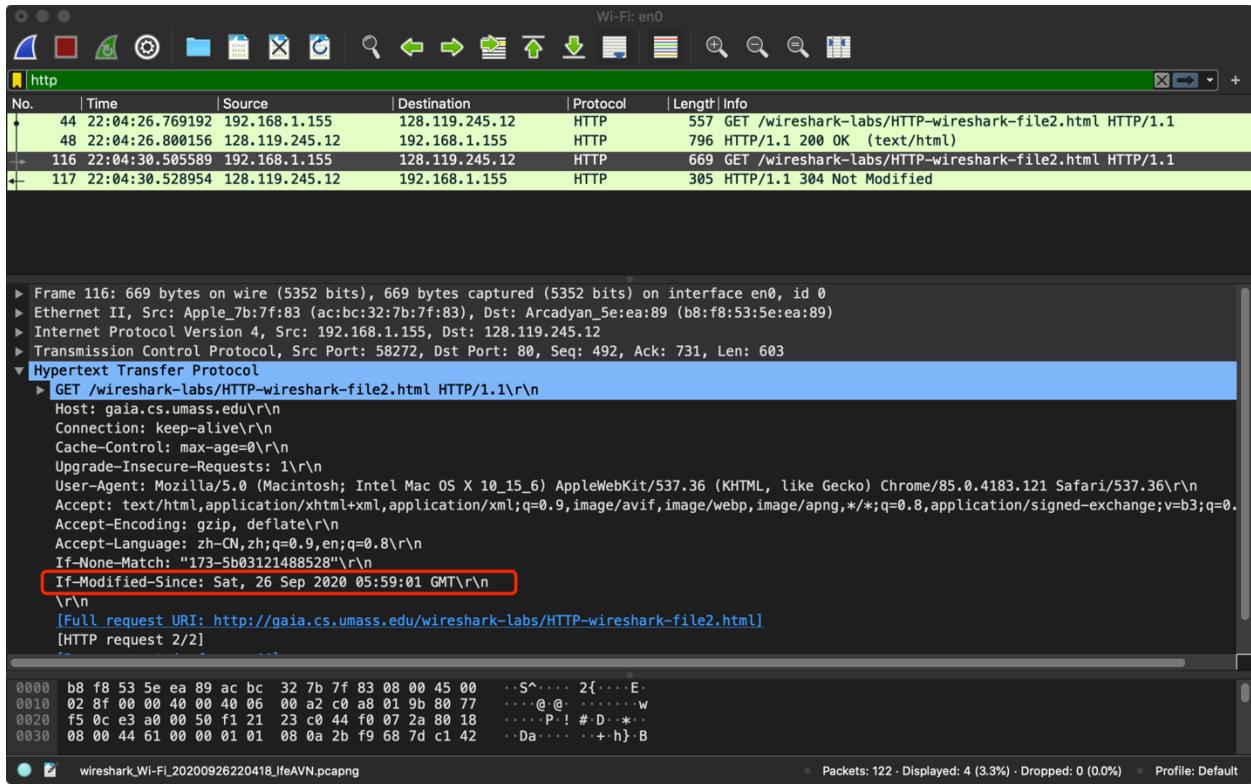
<html>
  <body>
    <p>Congratulations again! Now you've downloaded the file lab2-2.html. This file's last modification date will not change. Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE field in your browser's HTTP GET request to the server.</p>
</body>
</html>

```

0000 ac bc 32 7b 7f 83 b8 f8 53 5e ea 89 08 00 45 00 ..2{... S^... E.
0001 03 0e d4 0b 40 00 34 06 38 17 80 77 f5 0c c0 a8 ...@4.. 8..w...
0020 01 9b 00 50 e3 a0 44 f0 04 50 f1 21 23 c0 80 18 ...P..D.. P.!#...
0030 00 eb b4 cc 00 00 01 01 08 0a c1 42 d0 62 2b f9B.b+.

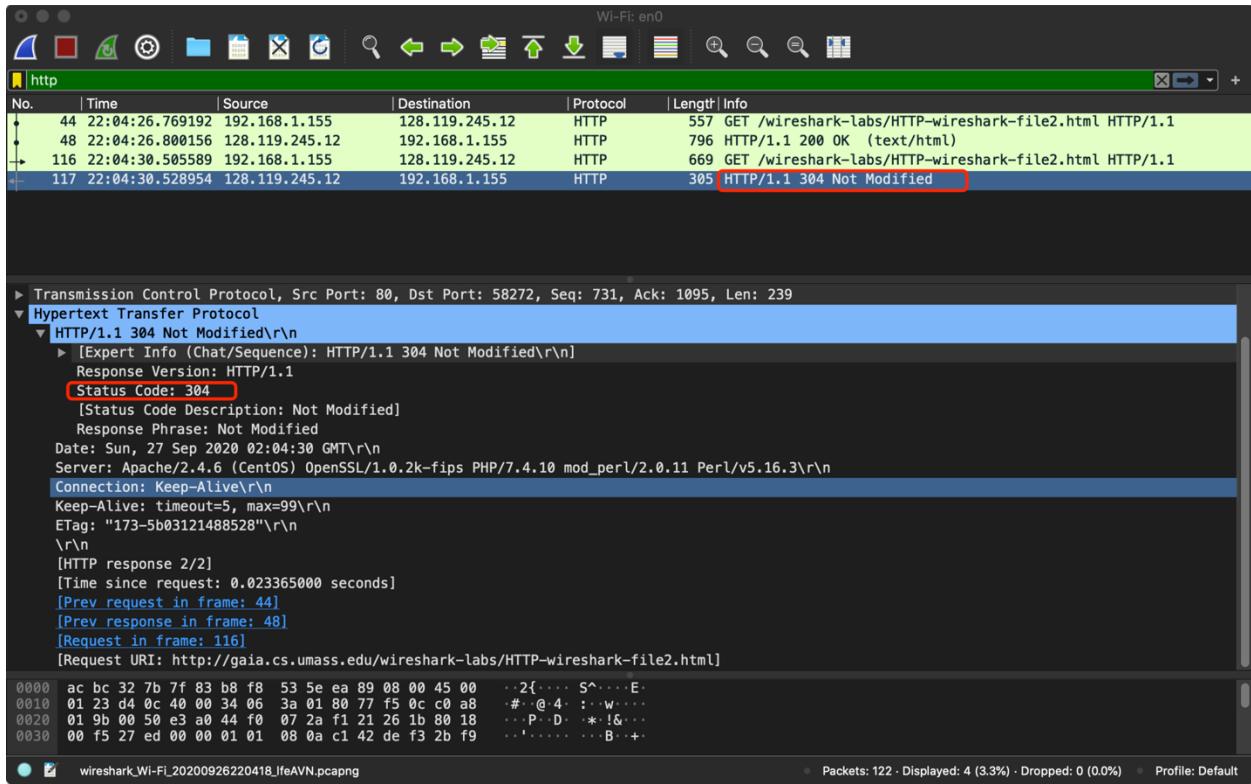
Q10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer: As shown in the screenshot below, there is “IF-MODIFIED-SINCE” line in the second HTTP GET. IF-MODIFIED-SINCE: Sat, 26 Sep 2020 05:50:01 GMT\r\n



Q11. 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.

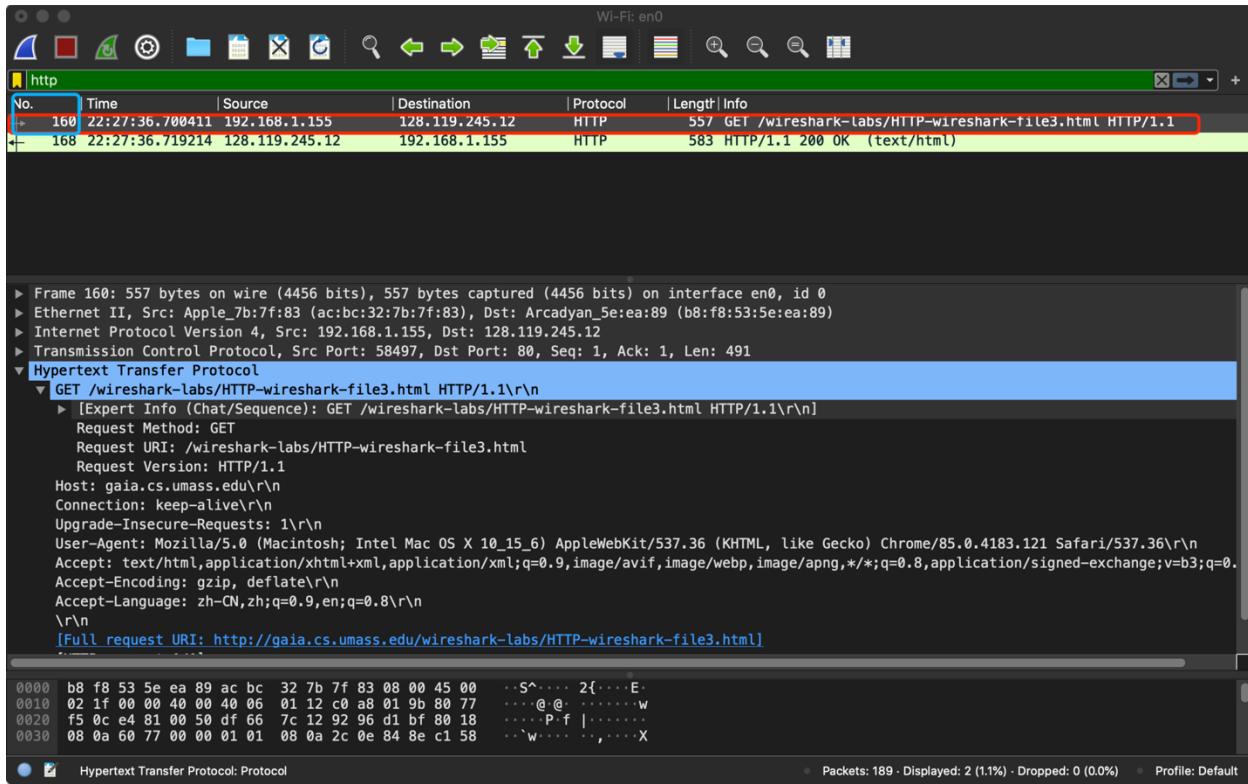
Answer: As shown in the screenshot below, the status code and phrase returned from the server in response to this second HTTP GET is “304” and “Not Modified”. And the server didn’t return the contents of the file. That’s because we already have this file cached so when we request the same file for the second time, server doesn’t need to return the full response packet like it did for the first time.



Retrieving Long Documents. Answer the following questions:

Q12. 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?

Answer: As shown in the screenshot below my browser send one HTTP GET request messages. And the packet No.160 contains the GET message.



Q13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer: As shown in the screenshot below, packet No.168 contains the status code and phrase associated with the response to the HTTP GET request.

Wi-Fi: en0

No.	Time	Source	Destination	Protocol	Length	Info
→ 160	22:27:36.7000411	192.168.1.155	128.119.245.12	HTTP	557	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
168	22:27:36.719214	128.119.245.12	192.168.1.155	HTTP	583	HTTP/1.1 200 OK (text/html)

```

▶ Frame 168: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0
▶ Ethernet II, Src: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89), Dst: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 58497, Seq: 4345, Ack: 492, Len: 517
▶ [4 Reassembled TCP Segments (4861 bytes): #165(1448), #166(1448), #167(1448), #168(517)]
▼ 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, 27 Sep 2020 02:27:36 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Sat, 26 Sep 2020 05:59:01 GMT\r\n
      ETag: "1194-5b03121460484"\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
    Frame (583 bytes) | Reassembled TCP (4861 bytes)
    The reassembled payload (tcp.reassembled.data), 4861 bytes
  Packets: 189 - Displayed: 2 (1.1%) - Dropped: 0 (0.0%) | Profile: Default
  
```

Q14. What is the status code and phrase in the response?

Answer: As shown in the screenshot below, status code is “200”, phrase is “OK”.

Wi-Fi: en0

No.	Time	Source	Destination	Protocol	Length	Info
→ 160	22:27:36.7000411	192.168.1.155	128.119.245.12	HTTP	557	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
168	22:27:36.719214	128.119.245.12	192.168.1.155	HTTP	583	HTTP/1.1 200 OK (text/html)

```

▶ Frame 168: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0
▶ Ethernet II, Src: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89), Dst: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 58497, Seq: 4345, Ack: 492, Len: 517
▶ [4 Reassembled TCP Segments (4861 bytes): #165(1448), #166(1448), #167(1448), #168(517)]
  [Frame: 165, payload: 0-1447 (1448 bytes)]
  [Frame: 166, payload: 1448-2895 (1448 bytes)]
  [Frame: 167, payload: 2896-4343 (1448 bytes)]
  [Frame: 168, payload: 4344-4860 (517 bytes)]
  [Segment count: 4]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053...]
▼ 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, 27 Sep 2020 02:27:36 GMT\r\n
    Frame (583 bytes) | Reassembled TCP (4861 bytes)
    Hypertext Transfer Protocol: Protocol
    Packets: 189 - Displayed: 2 (1.1%) - Dropped: 0 (0.0%) | Profile: Default
  
```

Q15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

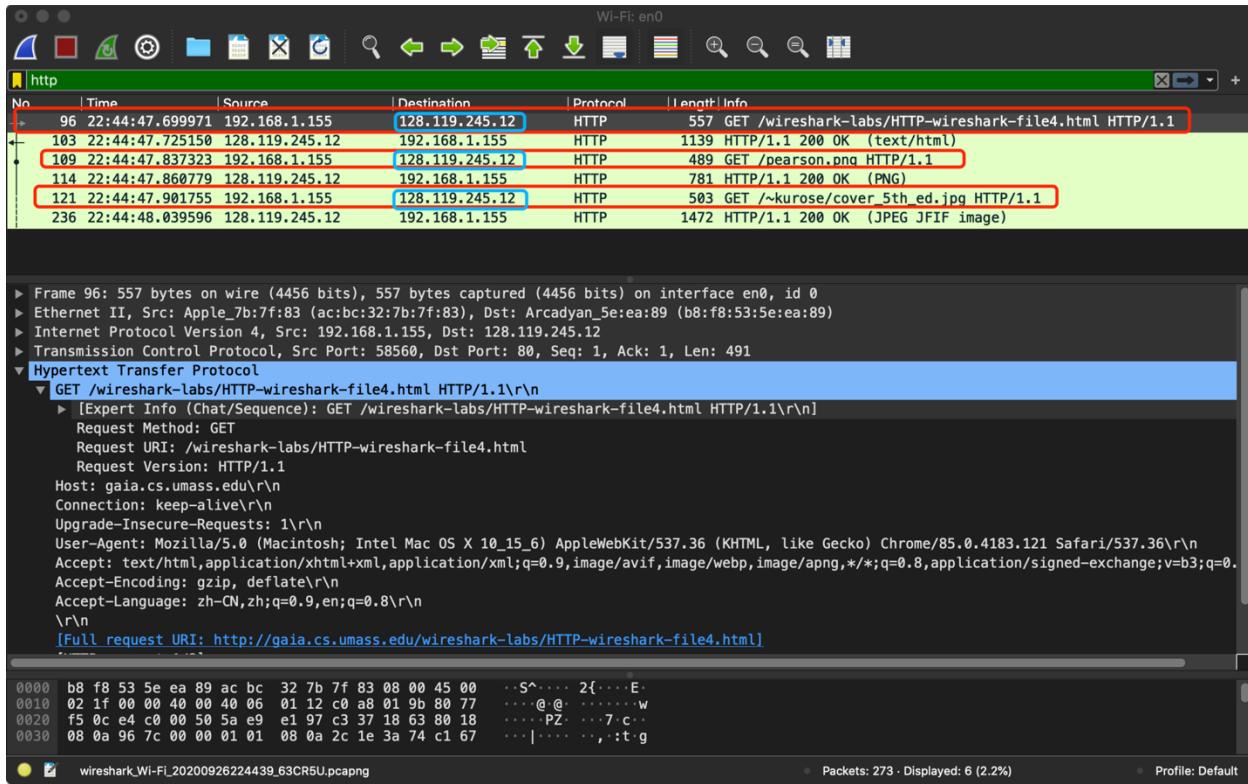
Answer: As shown in the screenshot below, there are 4 TCP segments.

The screenshot shows a Wireshark capture window titled "http" with two frames. Frame 160 is a GET request from 192.168.1.155 to 128.119.245.12. Frame 168 is a response from 128.119.245.12 to 192.168.1.155. The response is expanded to show its four reassembled TCP segments. A red box highlights the reassembly information: "[4 Reassembled TCP Segments (4861 bytes): #165(1448), #166(1448), #167(1448), #168(517)]". Below this, it shows the segment details: [Frame: 165, payload: 0-1447 (1448 bytes)], [Frame: 166, payload: 1448-2895 (1448 bytes)], [Frame: 167, payload: 2896-4343 (1448 bytes)], and [Frame: 168, payload: 4344-4860 (517 bytes)]. It also indicates a segment count of 4 and a total reassembled TCP length of 4861 bytes. The bottom of the window shows the raw hex and ASCII data of the frame, with the ASCII dump showing the HTML content of the Bill of Rights.

HTML Documents with Embedded Objects. Answer the following questions:

Q16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer: As shown in the screenshot below, there are 3 HTTP GET request messages did my browser send. The three Internet address are all 128.119.245.12.



Q17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Answer: As shown in the screenshot below, from the timestamp we can see, two images were downloaded serially—the first image was requested at 22:44:47.837323 and finished download at 22:44:47.860779, the second image was requested at 22:44:47.901755 and finished download at 22:44:48.039596. What's more, the first image is transmitted via source port 58560, and the second image is transmitted via source port 58562. Thus we can know that two images were downloaded serially through two different TCP connections.

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
96	22:44:47.699971	192.168.1.155	128.119.245.12	HTTP	557	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
103	22:44:47.725150	128.119.245.12	192.168.1.155	HTTP	1139	HTTP/1.1 200 OK (text/html)
109	22:44:47.837323	192.168.1.155	128.119.245.12	HTTP	489	GET /pearson.png HTTP/1.1
114	22:44:47.860779	128.119.245.12	192.168.1.155	HTTP	781	HTTP/1.1 200 OK (PNG)
121	22:44:47.901755	192.168.1.155	128.119.245.12	HTTP	503	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
236	22:44:48.039596	128.119.245.12	192.168.1.155	HTTP	1472	HTTP/1.1 200 OK (JPEG/JFIF image)

```

▶ Frame 109: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_7b:7f:83 (ac:bc:32:7b:7f:83), Dst: Arcadyan_5e:ea:89 (08:f8:53:5e:ea:89)
▶ Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 58560, Dst Port: 80, Seq: 492, Ack: 1074, Len: 423
    Source Port: 58560
    Destination Port: 80
    [Stream index: 5]
    [TCP Segment Len: 423]
    Sequence number: 492 (relative sequence number)
    Sequence number (raw): 1525277570
    [Next sequence number: 915 (relative sequence number)]
    Acknowledgment number: 1074 (relative ack number)
    Acknowledgment number (raw): 3275168916
    1000 .... = Header Length: 32 bytes (8)
    ► Flags: 0x018 (PSH, ACK)
    Window size value: 2048
    [Calculated window size: 131072]
    [Window size scaling factor: 64]
    Checksum: 0x6e9f [unverified]
    [Checksum Status: Unverified]

0000 b8 f8 53 5e ea 89 ac bc 32 7b 7f 83 08 00 45 00 ..S^.... 2{...E.
0010 01 db 00 00 40 00 40 06 01 56 c0 a8 01 9b 80 77 ...@:@.V....w
0020 f5 0c e4 c0 00 50 5a e9 e3 82 c3 37 1c 94 80 18 .....PZ....7...
0030 08 00 6e 9f 00 00 01 01 08 0a 2c 1e 3a fc c1 67 ...n.....,..:..g

● wireshark_Wi-Fi_20200926224439_63CR5U.pcapng
● Packets: 273 - Displayed: 6 (2.2%) - Dropped: 0 (0.0%) - Profile: Default

```

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
96	22:44:47.699971	192.168.1.155	128.119.245.12	HTTP	557	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
103	22:44:47.725150	128.119.245.12	192.168.1.155	HTTP	1139	HTTP/1.1 200 OK (text/html)
109	22:44:47.837323	192.168.1.155	128.119.245.12	HTTP	489	GET /pearson.png HTTP/1.1
114	22:44:47.860779	128.119.245.12	192.168.1.155	HTTP	781	HTTP/1.1 200 OK (PNG)
121	22:44:47.901755	192.168.1.155	128.119.245.12	HTTP	503	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
236	22:44:48.039596	128.119.245.12	192.168.1.155	HTTP	1472	HTTP/1.1 200 OK (JPEG/JFIF image)

```

▶ Frame 121: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_7b:7f:83 (ac:bc:32:7b:7f:83), Dst: Arcadyan_5e:ea:89 (08:f8:53:5e:ea:89)
▶ Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 58562, Dst Port: 80, Seq: 1, Ack: 1, Len: 437
    Source Port: 58562
    Destination Port: 80
    [Stream index: 7]
    [TCP Segment Len: 437]
    Sequence number: 1 (relative sequence number)
    Sequence number (raw): 1424784456
    [Next sequence number: 438 (relative sequence number)]
    Acknowledgment number: 1 (relative ack number)
    Acknowledgment number (raw): 1245425989
    1000 .... = Header Length: 32 bytes (8)
    ► Flags: 0x018 (PSH, ACK)
    Window size value: 2058
    [Calculated window size: 131712]
    [Window size scaling factor: 64]
    Checksum: 0xa0c0 [unverified]
    [Checksum Status: Unverified]

0000 b8 f8 53 5e ea 89 ac bc 32 7b 7f 83 08 00 45 00 ..S^.... 2{...E.
0010 01 e9 00 00 40 00 40 06 01 48 c0 a8 01 9b 80 77 ...@:@.H....w
0020 f5 0c e4 c2 00 50 54 ec 7c 48 4a 3b b1 45 80 18 .....PT|HJ;E...
0030 08 0a 0c 00 00 01 01 08 0a 2c 1e 3b 3a c1 67 .....n.....,..:..g

● wireshark_Wi-Fi_20200926224439_63CR5U.pcapng
● Packets: 273 - Displayed: 6 (2.2%) - Dropped: 0 (0.0%) - Profile: Default

```

HTTP Authentication. Answer the following questions:

Q18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer: As shown in the screenshot below, the response to the initial HTTP GET message is “401 Unauthorized”.

Wi-Fi: en0

No. | Time | Source | Destination | Protocol | Length | Info

162	23:07:57.212057	192.168.1.155	128.119.245.12	HTTP	573	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html...
165	23:07:57.230889	128.119.245.12	192.168.1.155	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
310	23:08:24.103454	192.168.1.155	128.119.245.12	HTTP	658	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html...
315	23:08:24.140401	128.119.245.12	192.168.1.155	HTTP	556	HTTP/1.1 200 OK (text/html)

► Frame 165: 783 bytes on wire (6264 bits), 783 bytes captured (6264 bits) on interface en0, id 0
► Ethernet II, Src: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89), Dst: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
► Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
► Transmission Control Protocol, Src Port: 80, Dst Port: 58616, Seq: 1, Ack: 508, Len: 717

▼ Hypertext Transfer Protocol

 ▼ HTTP/1.1 401 Unauthorized\r\n ► [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\nn]
 Response Version: HTTP/1.1
 Status Code: 401
 [Status Code Description: Unauthorized]
 Response Phrase: Unauthorized
 Date: Sun, 27 Sep 2020 03:07:57 GMT\r\nn
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\nn
 WWW-Authenticate: Basic realm="wireshark-students only"\r\nn
 ► Content-Length: 381\r\nn
 Keep-Alive: timeout=5, max=100\r\nn
 Connection: Keep-Alive\r\nn
 Content-Type: text/html; charset=iso-8859-1\r\nn
 \r\nn
 [HTTP response 1/1]

0020 01 9b 00 50 e4 f8 04 66 8d 35 b7 62 bb fc 80 18 ...p...f .5.b...
0030 00 eb 61 23 00 00 01 01 08 0a c1 7c f4 e0 2c 33 ..a#.... . .|. ,3
0040 68 72 48 54 54 50 2f 31 2e 31 20 34 30 31 20 55 hrHTTP/1 .1 401 U
0050 6e 61 75 74 68 6f 72 69 7a 65 64 0d 0a 44 61 74 nauthori zed-Dat

Source Port (tcp.srcport), 2 bytes Packets: 323 - Displayed: 4 (1.2%) · Dropped: 0 (0.0%) Profile: Default

Q19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer: As shown in the screenshots below, the first screenshot shows the data of the first HTTP GET and the second screenshot shows the data of the second HTTP GET. By comparing these two images we can see that the new fields are “Authorization” and “Cache-control”.

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
162	23:07:57.212057	192.168.1.155	128.119.245.12	HTTP	573	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
165	23:07:57.230889	128.119.245.12	192.168.1.155	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
310	23:08:24.103454	192.168.1.155	128.119.245.12	HTTP	658	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
315	23:08:24.140401	128.119.245.12	192.168.1.155	HTTP	556	HTTP/1.1 200 OK (text/html)

► Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12
 ► Transmission Control Protocol, Src Port: 58616, Dst Port: 80, Seq: 1, Ack: 1, Len: 507
 ▼ Hypertext Transfer Protocol
 ▼ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
 ▶ [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
 Request Method: GET
 Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
 Request Version: HTTP/1.1
 Host: gaia.cs.umass.edu\r\n
 Connection: keep-alive\r\n
 Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
 [HTTP request 1/1]
 [Response in frame: 165]

0000 b8 f8 53 5e ea 89 ac bc 32 7b 7f 83 08 00 45 00 ..S^... 2{ ... E.
 0010 02 2f 00 00 40 00 40 06 01 02 c0 a8 01 9b 80 77 ./ @@w
 0020 f5 0c e4 f8 00 50 b7 62 ba 01 04 66 8d 35 80 18P.b ...f 5..
 0030 08 0a e0 6a 00 00 01 01 08 0a 2c 33 68 72 c1 7c ...j3hr..|

● wireshark_Wi-Fi_20200926230748_1RohQE.pcapng ● Packets: 323 - Displayed: 4 (1.2%) - Dropped: 0 (0.0%) ● Profile: Default

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
162	23:07:57.212057	192.168.1.155	128.119.245.12	HTTP	573	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
165	23:07:57.230889	128.119.245.12	192.168.1.155	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
310	23:08:24.103454	192.168.1.155	128.119.245.12	HTTP	658	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
315	23:08:24.140401	128.119.245.12	192.168.1.155	HTTP	556	HTTP/1.1 200 OK (text/html)

► Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12
 ► Transmission Control Protocol, Src Port: 58617, Dst Port: 80, Seq: 1, Ack: 1, Len: 592
 ▼ Hypertext Transfer Protocol
 ▼ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
 ▶ [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
 Request Method: GET
 Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
 Request Version: HTTP/1.1
 Host: gaia.cs.umass.edu\r\n
 Connection: keep-alive\r\n
 Cache-Control: max-age=0\r\n
 ▶ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRz0m5ldHdvcms=\r\n
 Credentials: wireshark-students:network
 Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
 \r\n
 0000 65 3d 30 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 e=0..Aut horizati
 0001 6f 6e 3a 20 42 61 73 69 63 20 64 32 6c 79 5a 58 on: Basi c d2lyZX
 00f0 4e 6f 59 58 4a 72 4c 58 4e 30 64 57 52 6c 62 6e NoYXJrLX N0dWRlbn
 0100 52 7a 4f 6d 35 6c 64 48 64 76 63 6d 73 3d 0d 0a Rz0m5ldH dvcms=..

● HTTP Authorization header (http.authorization), 59 bytes ● Packets: 323 - Displayed: 4 (1.2%) - Dropped: 0 (0.0%) ● Profile: Default