

Date-August 30,2022

Name-Divya Kirtikumar Patel

Student ID-202001420

Lab Group- 6

**[2] The Basic HTTP GET/response interaction**

Questions:

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

Both my browser and server are running on HTTP version 1.1.

Server: 1.1

Host: 1.1

No.	Time	Source	Destination	Protocol	Length	Info
322	14.811008	10.100.77.74	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
266	14.319769	10.100.77.74	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
321	14.782465	128.119.245.12	10.100.77.74	HTTP	578	HTTP/1.1 200 OK (text/html)
328	15.043821	128.119.245.12	10.100.77.74	HTTP	598	HTTP/1.1 404 Not Found (text/html)

```

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 524
  Identification: 0xd066 (53350)
> Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.100.77.74
  Destination: 128.119.245.12
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
> Transmission Control Protocol, Src Port: 53772, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
  Hypertext Transfer Protocol
    > GET /wireshark-labs/HTTP-wireshark-file1.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/104.0.5112.102 Safari/537.36 Edg/104.0.1293.63\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;q=0.9\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      [HTTP request 1/2]
      [Response in frame: 321]
      [Next request in frame: 322]

```

```

0000  00 00 5e 00 01 2f a8 a1 59 da c8 bb 06 00 45 00  ..^... Y.....E.
0010  02 0c d0 66 40 00 80 06 00 00 0a 64 4d 4a 80 77  ...f... dM.w
0020  f5 0c d2 0c 00 50 3d 43 dd 6a b4 49 c8 ed 50 18  ....P=C .j.I..P.
0030  20 14 cf 30 00 00 47 45 54 20 2f 77 69 72 65 73  ...0..GE T/wires
0040  68 61 72 6b 20 6c 61 62 73 2f a8 54 54 50 2d 77  hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68  reshark -file1.h

```

Frame (frame), 538 bytes

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

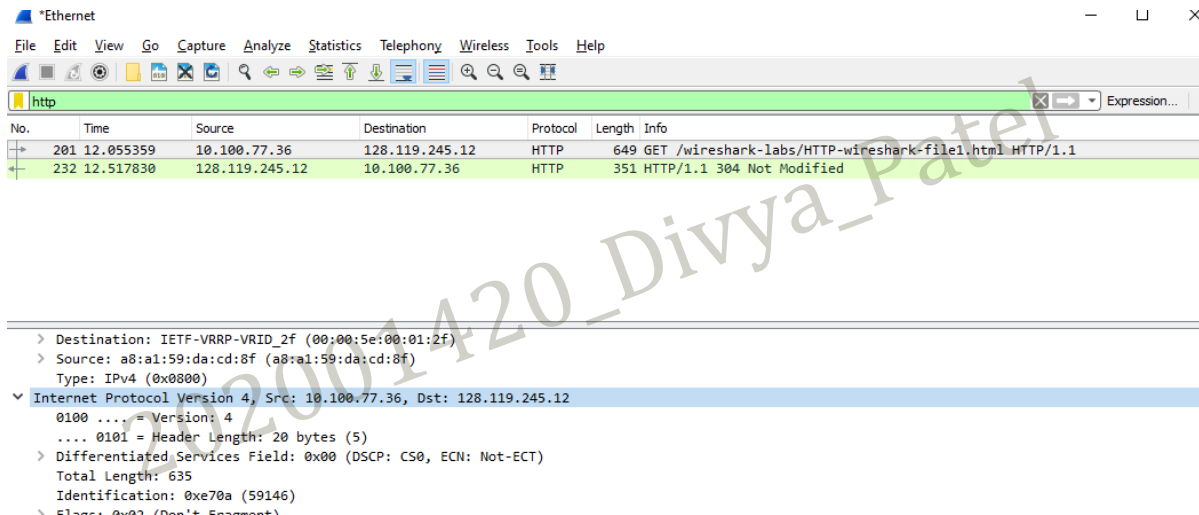
Accept – language to the server : en-US

```

> Ethernet II, Src: a8:a1:59:da:cd:8f (a8:a1:59:da:cd:8f), Dst: IETF-VRRP-VRID_2f (00:00:5e:00:01:2f)
> Internet Protocol Version 4, Src: 10.100.77.36, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64532, Dst Port: 80, Seq: 1, Ack: 1, Len: 595
  Hypertext Transfer Protocol
    > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 Edg/104.0.1293.70\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;q=0.9\r\n
      If-None-Match: "80-5e76f13b236a8"\r\n
      If-Modified-Since: Tue, 30 Aug 2022 05:59:01 GMT\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: 232]

```

Q3. What is the IP address of your computer? and the gaia.cs.umass.eduServer?



The image shows a Wireshark packet capture window titled '\*Ethernet'. The packet list pane shows two packets. Packet 232 is an HTTP GET request from 10.100.77.36 to 128.119.245.12. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
201	12.055359	10.100.77.36	128.119.245.12	HTTP	649	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
232	12.517830	128.119.245.12	10.100.77.36	HTTP	351	HTTP/1.1 304 Not Modified

The packet details pane for packet 232 shows the following information:

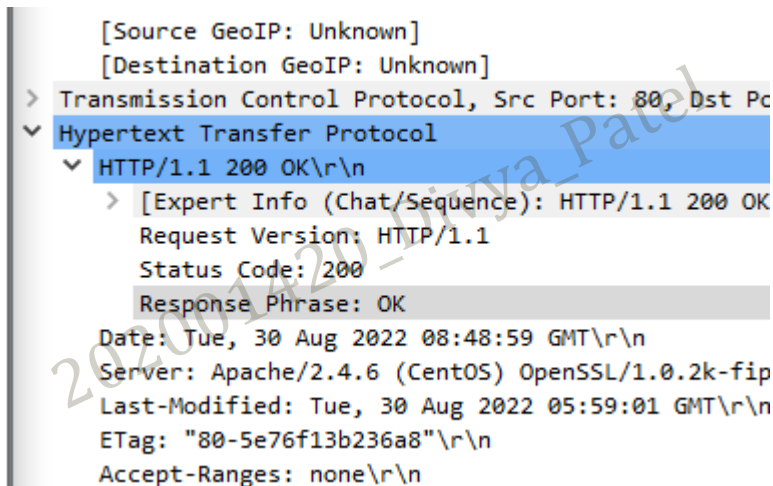
- Destination: IETF-VRRP-VRID\_2f (00:00:5e:00:01:2f)
- Source: a8:a1:59:da:cd:8f (a8:a1:59:da:cd:8f)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 10.100.77.36, Dst: 128.119.245.12
  - 0100 ... = Version: 4
  - ... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 635
  - Identification: 0xe70a (59146)
  - Flags: 0x00 (Don't Fragment)

Internet Protocol Version 4, Src: 10.100.77.36, Dst: 128.119.245.12

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

Status Code: 200

Response Phrase: OK

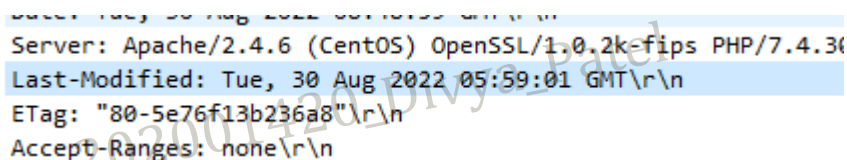


The image shows a Wireshark packet capture window titled '\*Ethernet'. The packet list pane shows two packets. Packet 232 is an HTTP 200 OK response from 128.119.245.12 to 10.100.77.36. The packet details pane shows the following information:

- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 80, Dst Port: 59146
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
    - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK
    - Request Version: HTTP/1.1
    - Status Code: 200
    - Response Phrase: OK
  - Date: Tue, 30 Aug 2022 08:48:59 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30\r\n
  - Last-Modified: Tue, 30 Aug 2022 05:59:01 GMT\r\n
  - ETag: "80-5e76f13b236a8"\r\n
  - Accept-Ranges: none\r\n

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

Last – Modified: Tue, 30 Aug 2022 05:59:01 GMT (At the server)



The image shows a Wireshark packet capture window titled '\*Ethernet'. The packet list pane shows two packets. Packet 232 is an HTTP 200 OK response from 128.119.245.12 to 10.100.77.36. The packet details pane shows the following information:

- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30\r\n
- Last-Modified: Tue, 30 Aug 2022 05:59:01 GMT\r\n
- ETag: "80-5e76f13b236a8"\r\n
- Accept-Ranges: none\r\n

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

```
▼ Frame 321: 578 bytes on wire (4624 bits), 578 bytes captured (4624 bits) on interface 0
  Interface id: 0 (\Device\NPF_{1E9396D9-8471-40CA-88BE-03592A85A9E9})
  Encapsulation type: Ethernet (1)
  Arrival Time: Aug 30, 2022 14:18:59.108309000 India Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1661849339.108309000 seconds
  [Time delta from previous captured frame: 0.081667000 seconds]
  [Time delta from previous displayed frame: 0.462696000 seconds]
  [Time since reference or first frame: 14.782465000 seconds]
  Frame Number: 321
  Frame Length: 578 bytes (4624 bits)
  Capture Length: 578 bytes (4624 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

### [3] The HTTP CONDITIONAL GET/response interaction

Questions:

Q1. 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, I don't see an "IF-MODIFIED-SINCE" line in the HTTP GET.

```
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/104.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/3]
[Response in frame: 81]
[Next request in frame: 82]
```

Q2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes. As we can see the content returned by server in *Line-based text data* field.

The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets, with the selected packet being an HTTP GET request (packet 135) and its corresponding 200 OK response (packet 166). The middle pane shows the details of the selected packet, which is an HTTP response. The 'Line-based text data' field is expanded, showing the HTML content of the response, which includes a congratulatory message and information about the file's last modification date.

No.	Time	Source	Destination	Protocol	Length	Info
135	9.987043	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
166	10.450852	128.119.245.12	10.100.77.36	HTTP	822	HTTP/1.1 200 OK (text/html)
166	10.474711	10.100.77.36	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
170	10.707588	128.119.245.12	10.100.77.36	HTTP	598	HTTP/1.1 404 Not Found (text/html)
247	16.011800	10.100.77.36	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
276	16.471525	128.119.245.12	10.100.77.36	HTTP	352	HTTP/1.1 304 Not Modified

```
Connection: keep-alive\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.463809000 seconds]
[Request in frame: 135]
[Next request in frame: 166]
[Next response in frame: 170]
File Data: 371 bytes
Line-based text data: text/html
  \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 IF-MODIFIED-SINCE<br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
```

Q3. 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?

If-Modified-Since: Tue, 30 Aug 2022 05:59:01 GMT\r\n (the timestamps is the information following the header)

No.	Time	Source	Destination	Protocol	Length	Info
135	9.987043	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
165	10.450852	128.119.245.12	10.100.77.36	HTTP	822	HTTP/1.1 200 OK (text/html)
166	10.474711	10.100.77.36	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
170	10.707588	128.119.245.12	10.100.77.36	HTTP	598	HTTP/1.1 404 Not Found (text/html)
247	16.011800	10.100.77.36	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
276	16.471525	128.119.245.12	10.100.77.36	HTTP	352	HTTP/1.1 304 Not Modified

[Group: Sequence]

Request Method: GET

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

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 Edg/104.0.1293

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

If-None-Match: "173-5e76f13b22ed8"\r\n

If-Modified-Since: Tue, 30 Aug 2022 05:59:01 GMT\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

[HTTP request 1/1]

Q4. 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: 304

Response Phrase: Not Modified

No, the server didn't return the contents of the file.

No.	Time	Source	Destination	Protocol	Length	Info
135	9.987043	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
165	10.450852	128.119.245.12	10.100.77.36	HTTP	822	HTTP/1.1 200 OK (text/html)
166	10.474711	10.100.77.36	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
170	10.707588	128.119.245.12	10.100.77.36	HTTP	598	HTTP/1.1 404 Not Found (text/html)
247	16.011800	10.100.77.36	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
276	16.471525	128.119.245.12	10.100.77.36	HTTP	352	HTTP/1.1 304 Not Modified

Urgent pointer: 0

> [SEQ/ACK analysis]

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 304 Not Modified\r\n

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

[HTTP/1.1 304 Not Modified\r\n]

[Severity level: chat]

[Group: Sequence]

Request Version: HTTP/1.1

Status Code: 304

Response Phrase: Not Modified

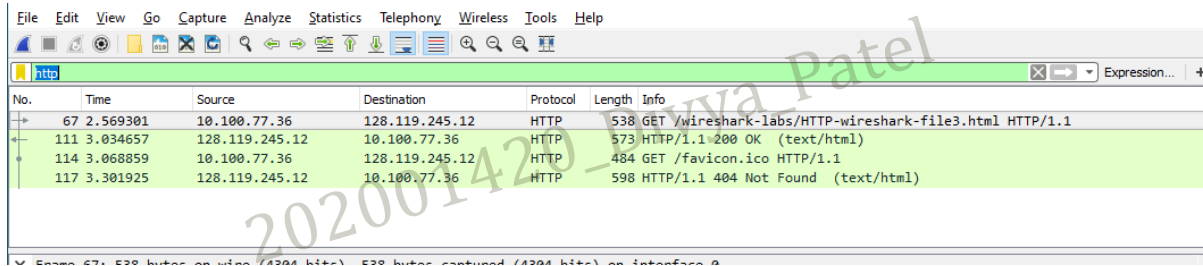
Date: Tue, 30 Aug 2022 09:25:20 GMT\r\n

## [4] Retrieving Long Documents

Questions:

Q1. How many HTTP GET request messages were sent by your browser?

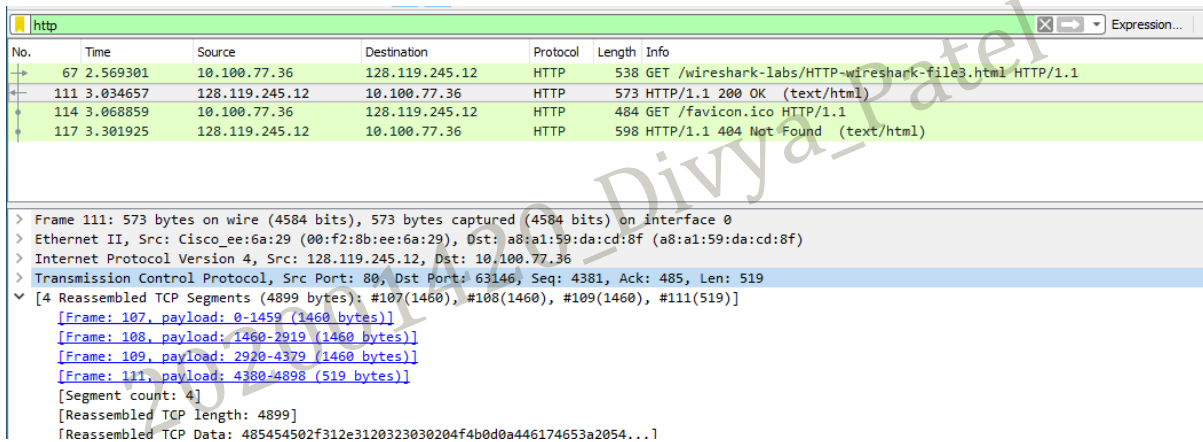
2 HTTP GET request messages were sent.



Wireshark packet capture showing HTTP GET requests. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
67	2.569301	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
111	3.034657	128.119.245.12	10.100.77.36	HTTP	573	HTTP/1.1 200 OK (text/html)
114	3.068859	10.100.77.36	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
117	3.301925	128.119.245.12	10.100.77.36	HTTP	598	HTTP/1.1 404 Not Found (text/html)

Q2. How many data-containing TCP segments were needed to carry the single HTTP response?



Wireshark packet capture showing TCP segments for the HTTP response. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
67	2.569301	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
111	3.034657	128.119.245.12	10.100.77.36	HTTP	573	HTTP/1.1 200 OK (text/html)
114	3.068859	10.100.77.36	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
117	3.301925	128.119.245.12	10.100.77.36	HTTP	598	HTTP/1.1 404 Not Found (text/html)

Below the packet list, the details pane shows the structure of the HTTP response:

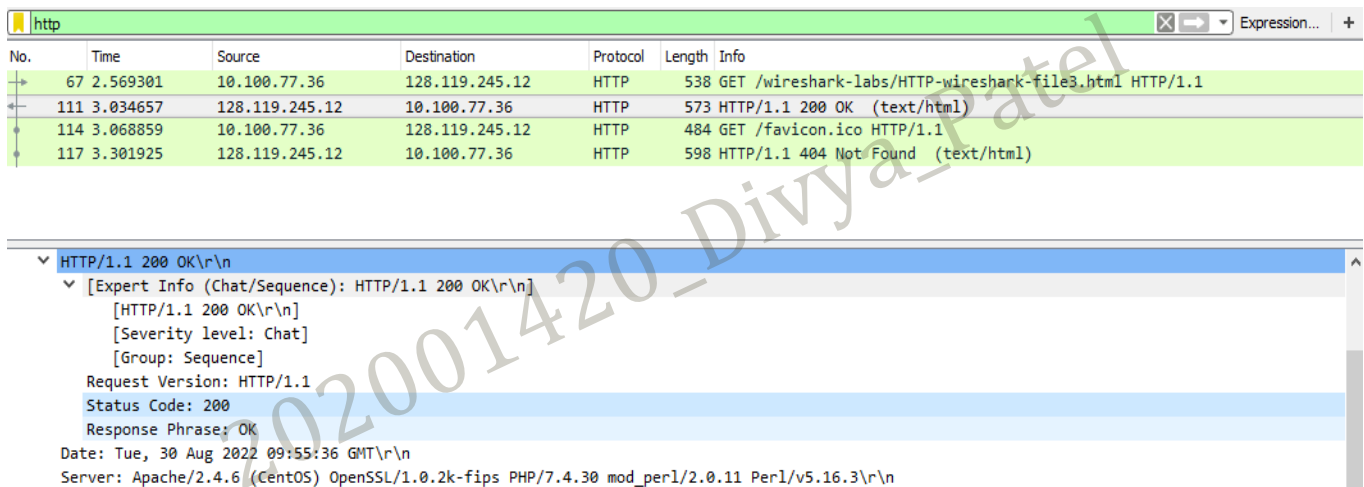
- Frame 111: 573 bytes on wire (4584 bits), 573 bytes captured (4584 bits) on interface 0
- Ethernet II, Src: Cisco\_ee:6a:29 (00:f2:8b:ee:6a:29), Dst: a8:a1:59:da:cd:8f (a8:a1:59:da:cd:8f)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.100.77.36
- Transmission Control Protocol, Src Port: 80, Dst Port: 63146, Seq: 4381, Ack: 485, Len: 519
- 4 Reassembled TCP Segments (4899 bytes): #107(1460), #108(1460), #109(1460), #111(519)
  - Frame 107, payload: 0-1459 (1460 bytes)
  - Frame 108, payload: 1460-2919 (1460 bytes)
  - Frame 109, payload: 2920-4379 (1460 bytes)
  - Frame 111, payload: 4380-4898 (519 bytes)
- Segment count: 4
- Reassembled TCP length: 4899
- Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054...

Four data-containing TCP segments were needed.

Q3. What is the status code and phrase associated with the response to the HTTP GET request?

Status Code: 200

Response Phrase: OK



Wireshark packet capture showing the HTTP response details. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
67	2.569301	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
111	3.034657	128.119.245.12	10.100.77.36	HTTP	573	HTTP/1.1 200 OK (text/html)
114	3.068859	10.100.77.36	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
117	3.301925	128.119.245.12	10.100.77.36	HTTP	598	HTTP/1.1 404 Not Found (text/html)

Below the packet list, the details pane shows the structure of the HTTP response:

- HTTP/1.1 200 OK\r\n
  - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  - [HTTP/1.1 200 OK\r\n]
  - [Severity level: Chat]
  - [Group: Sequence]
  - Request Version: HTTP/1.1
  - Status Code: 200
  - Response Phrase: OK
  - Date: Tue, 30 Aug 2022 09:55:36 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod\_perl/2.0.11 Perl/v5.16.3\r\n

## [5] HTML Documents with Embedded Objects

Questions:

Q1. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

Destination: 128.119.245.12

Destination: 128.119.245.12

Destination: 178.79.137.164

No.	Time	Source	Destination	Protocol	Length	Info
49	3.152502	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
88	3.933342	128.119.245.12	10.100.77.36	HTTP	1393	HTTP/1.1 200 OK (text/html)
89	3.940125	10.100.77.36	128.119.245.12	HTTP	484	GET /pearson.png HTTP/1.1
96	3.943368	10.100.77.36	178.79.137.164	HTTP	451	GET /8E_cover_small.jpg HTTP/1.1
101	4.172706	128.119.245.12	10.100.77.36	HTTP	783	HTTP/1.1 200 OK (PNG)
103	4.309015	178.79.137.164	10.100.77.36	HTTP	288	HTTP/1.1 301 Moved Permanently

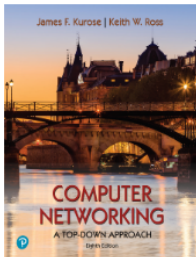
Q2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

The images were downloaded serially. This is confirmed in two ways.

The timestamp for both GET requests is different and the Stream Index is also different for both the requests.



This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.cslash.net in France:



And while we have your attention, you might want to take time to check out the available open resources for this book at [http://gaia.cs.umass.edu/kurose\\_ross](http://gaia.cs.umass.edu/kurose_ross).

*Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
49	3.152502	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
88	3.933342	128.119.245.12	10.100.77.36	HTTP	1393	HTTP/1.1 200 OK (text/html)
89	3.940125	10.100.77.36	128.119.245.12	HTTP	484	GET /pearson.png HTTP/1.1
96	3.943368	10.100.77.36	178.79.137.164	HTTP	451	GET /8E_cover_small.jpg HTTP/1.1
101	4.172706	128.119.245.12	10.100.77.36	HTTP	783	HTTP/1.1 200 OK (PNG)
103	4.309015	178.79.137.164	10.100.77.36	HTTP	288	HTTP/1.1 301 Moved Permanently



http						
No.	Time	Source	Destination	Protocol	Length	Info
49	3.152502	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
88	3.933342	128.119.245.12	10.100.77.36	HTTP	1393	HTTP/1.1 200 OK (text/html)
89	3.940125	10.100.77.36	128.119.245.12	HTTP	484	GET /pearson.png HTTP/1.1
96	3.943368	10.100.77.36	178.79.137.164	HTTP	451	GET /8E_cover_small.jpg HTTP/1.1
101	4.172706	128.119.245.12	10.100.77.36	HTTP	783	HTTP/1.1 200 OK (PNG)
103	4.309015	178.79.137.164	10.100.77.36	HTTP	288	HTTP/1.1 301 Moved Permanently

> Frame 89: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface 0  
 > Ethernet II, Src: a8:a1:59:da:cd:8f (a8:a1:59:da:cd:8f), Dst: IETF-VRRP-VRID\_2f (00:00:5e:00:01:2f)  
 > Internet Protocol Version 4, Src: 10.100.77.36, Dst: 128.119.245.12  
 > Transmission Control Protocol, Src Port: 59714, Dst Port: 80, Seq: 485, Ack: 1340, Len: 430  
   Source Port: 59714  
   Destination Port: 80  
   [Stream index: 5]  
   [TCP Segment Len: 430]  
   Sequence number: 485 (relative sequence number)  
   [Next sequence number: 915 (relative sequence number)]  
   Acknowledgment number: 1340 (relative ack number)  
   Header length: 20 bytes

http						
No.	Time	Source	Destination	Protocol	Length	Info
49	3.152502	10.100.77.36	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
88	3.933342	128.119.245.12	10.100.77.36	HTTP	1393	HTTP/1.1 200 OK (text/html)
89	3.940125	10.100.77.36	128.119.245.12	HTTP	484	GET /pearson.png HTTP/1.1
96	3.943368	10.100.77.36	178.79.137.164	HTTP	451	GET /8E_cover_small.jpg HTTP/1.1
101	4.172706	128.119.245.12	10.100.77.36	HTTP	783	HTTP/1.1 200 OK (PNG)
103	4.309015	178.79.137.164	10.100.77.36	HTTP	288	HTTP/1.1 301 Moved Permanently

> Frame 96: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface 0  
 > Ethernet II, Src: a8:a1:59:da:cd:8f (a8:a1:59:da:cd:8f), Dst: IETF-VRRP-VRID\_2f (00:00:5e:00:01:2f)  
 > Internet Protocol Version 4, Src: 10.100.77.36, Dst: 178.79.137.164  
 > Transmission Control Protocol, Src Port: 59718, Dst Port: 80, Seq: 1, Ack: 1, Len: 397  
   Source Port: 59718  
   Destination Port: 80  
   [Stream index: 7]  
   [TCP Segment Len: 397]  
   Sequence number: 1 (relative sequence number)  
   [Next sequence number: 398 (relative sequence number)]  
   Acknowledgment number: 1 (relative ack number)  
   Header Length: 20 bytes

## [6] HTTP Authentication

Questions:

Q1. What is the servers response (status code and phrase) in response to the initial HTTP GET message from your browser?

http						
No.	Time	Source	Destination	Protocol	Length	Info
50	2.873115	10.100.77.36	128.119.245.12	HTTP	554	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
88	3.639034	128.119.245.12	10.100.77.36	HTTP	876	HTTP/1.1 401 Unauthorized (text/html)
1182	21.832731	10.100.77.36	128.119.245.12	HTTP	639	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1218	22.295665	128.119.245.12	10.100.77.36	HTTP	582	HTTP/1.1 200 OK (text/html)

> Frame 88: 876 bytes on wire (7008 bits), 876 bytes captured (7008 bits) on interface 0  
 > Ethernet II, Src: Cisco\_ee:6a:29 (00:f2:8b:ee:6a:29), Dst: a8:a1:59:da:cd:8f (a8:a1:59:da:cd:8f)  
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.100.77.36  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 56432, Seq: 1, Ack: 501, Len: 822  
 > Hypertext Transfer Protocol  
   HTTP/1.1 401 Unauthorized\r\n
   [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
   [HTTP/1.1 401 Unauthorized\r\n]
   [Severity level: Chat]
   [Group: Sequence]
   Request Version: HTTP/1.1
   Status Code: 401
   Response Phrase: Unauthorized
   Date: Tue, 30 Aug 2022 10:55:26 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod\_perl/2.0.11 Perl/v5.16.3\r\n
   WWW-Authenticate: Basic realm="wireshark-students only"\r\n
   Content-Length: 381\r\n
   [Content length: 381]

Status Code: 401

Response Phrase: Unauthorized

Q2. When your browsers sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

First Request --

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Date: Tue, 30 Aug 2022 10:12:09 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    Proxy-Support: Session-Based-Authentication\r\n
    Accept-Ranges: none\r\n
    Via: HTTP/1.1 forward.http.proxy:3128\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.469594000 seconds]
    [Request in frame: 17]
    [Next request in frame: 39]
    [Next response in frame: 44]
    File Data: 381 bytes
```

Second Request --

```
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  > Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5z\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/104.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-excl\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/2]
    [Response in frame: 624]
    [Next request in frame: 629]
```