LAB(3)

Report 3

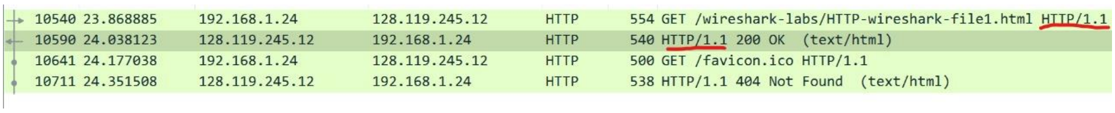
Abdullah khalid Alharbi STD/420166 COE331

Introduction:

After we knew how "Wireshark" works in the previous lab, now we'll start using the program to catch more packets and see the protocols used in the operations. One of these protocols is (HTTP) protocol and we will cover the most important aspects of this protocol.

1. What version of HTTP is your browser running? What version of HTTP is the server running?

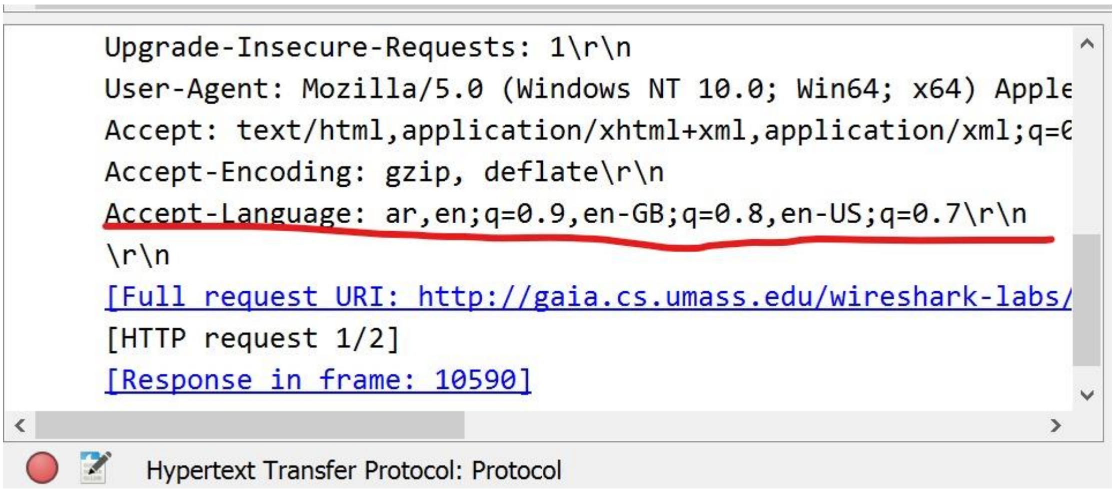
Answer: both of them are HTTP 1.1



```
10540 23.868885   192.168.1.24     128.119.245.12   HTTP   554 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
10590 24.038123   128.119.245.12   192.168.1.24     HTTP   540 HTTP/1.1 200 OK  (text/html)
10641 24.177038   192.168.1.24     128.119.245.12   HTTP   500 GET /favicon.ico HTTP/1.1
10711 24.351508   128.119.245.12   192.168.1.24     HTTP   538 HTTP/1.1 404 Not Found  (text/html)
```

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

Answer:

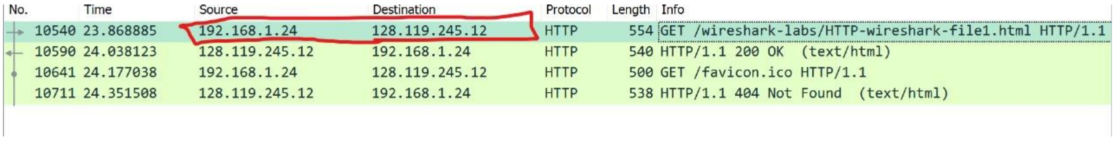


```
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
Accept: text/html,application/xhtml+xml,application/xml;q=0
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ar,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/
[HTTP request 1/2]
[Response in frame: 10590]
```

Hypertext Transfer Protocol: Protocol

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

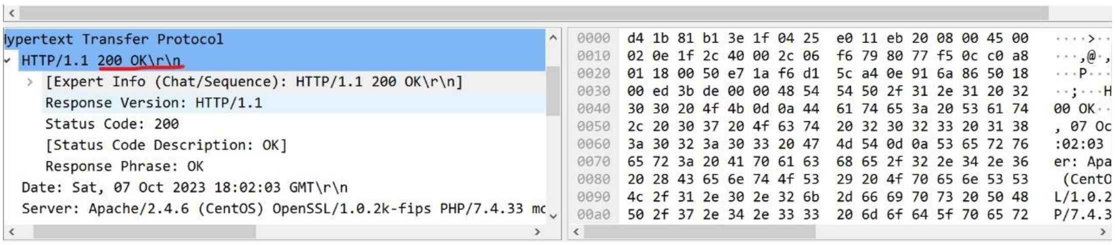
Answer: My computer's IP is 192.168.1.24 and the site is 128.119.245.12



```
No.    Time       Source          Destination      Protocol  Length Info
10540 23.868885   192.168.1.24    128.119.245.12   HTTP       554 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
10590 24.038123   128.119.245.12  192.168.1.24     HTTP       540 HTTP/1.1 200 OK  (text/html)
10641 24.177038   192.168.1.24    128.119.245.12   HTTP       500 GET /favicon.ico HTTP/1.1
10711 24.351508   128.119.245.12  192.168.1.24     HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

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

Answer:

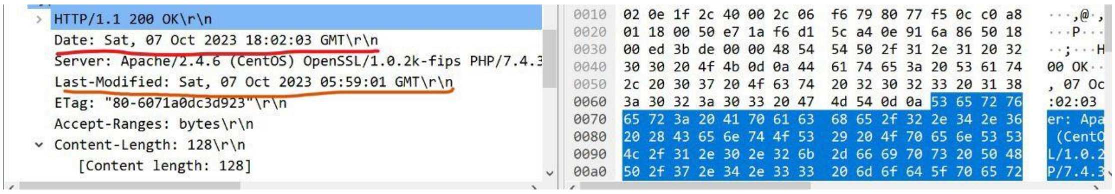


```
ypertext Transfer Protocol
 HTTP/1.1 200 OK\r\n
   [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
   Response Version: HTTP/1.1
   Status Code: 200
   [Status Code Description: OK]
   Response Phrase: OK
 Date: Sat, 07 Oct 2023 18:02:03 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mc
```

```
0000  d4 1b 81 b1 3e 1f 04 25  e0 11 eb 20 08 00 45 00   ····>··
0010  02 0e 1f 2c 40 00 2c 06  f6 79 80 77 f5 0c c0 a8   ···,@·,
0020  01 18 00 50 e7 1a f6 d1  5c a4 0e 91 6a 86 50 18   ···P···
0030  00 ed 3b de 00 00 48 54  54 50 2f 31 2e 31 20 32   ··;···H
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··
0050  2c 20 30 37 20 4f 63 74  20 32 30 32 33 20 31 38   , 07 Oc
0060  3a 30 32 3a 30 33 20 47  4d 54 0d 0a 53 65 72 76   :02:03 
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apa
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentO
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.3
```

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

Answer:

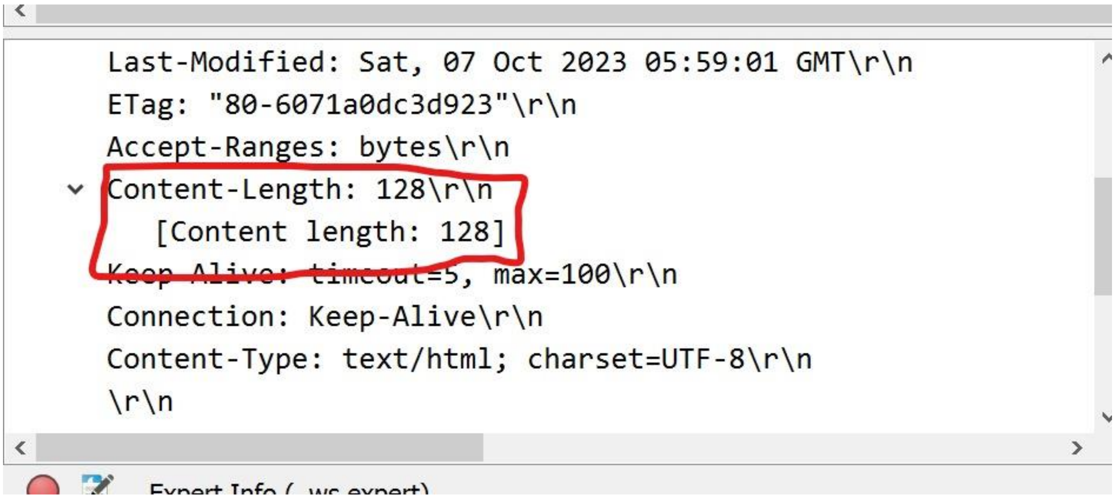


```
 HTTP/1.1 200 OK\r\n
 Date: Sat, 07 Oct 2023 18:02:03 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.3
 Last-Modified: Sat, 07 Oct 2023 05:59:01 GMT\r\n
 ETag: "80-6071a0dc3d923"\r\n
 Accept-Ranges: bytes\r\n
 Content-Length: 128\r\n
   [Content length: 128]
```

```
0010  02 0e 1f 2c 40 00 2c 06  f6 79 80 77 f5 0c c0 a8   ···,@·,
0020  01 18 00 50 e7 1a f6 d1  5c a4 0e 91 6a 86 50 18   ···P···
0030  00 ed 3b de 00 00 48 54  54 50 2f 31 2e 31 20 32   ··;···H
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··
0050  2c 20 30 37 20 4f 63 74  20 32 30 32 33 20 31 38   , 07 Oc
0060  3a 30 32 3a 30 33 20 47  4d 54 0d 0a 53 65 72 76   :02:03 
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apa
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentO
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70 65 72   P/7.4.3
```

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

Answer:



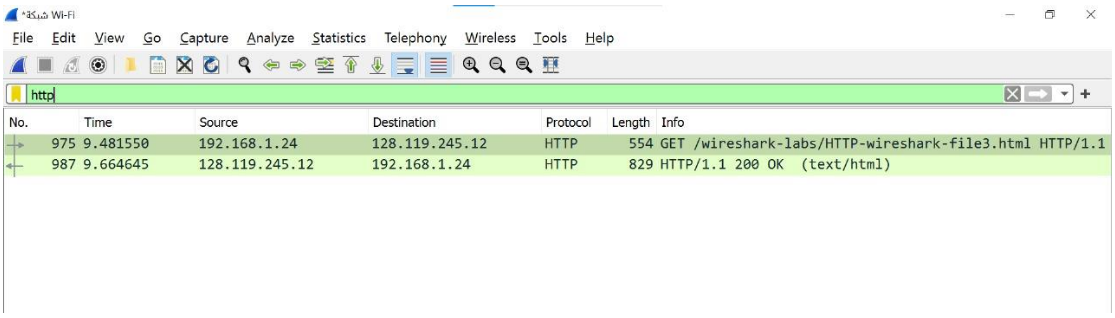
```
 Last-Modified: Sat, 07 Oct 2023 05:59:01 GMT\r\n
 ETag: "80-6071a0dc3d923"\r\n
 Accept-Ranges: bytes\r\n
 Content-Length: 128\r\n
   [Content length: 128]
 Keep-Alive: timeout=5, max=100\r\n
 Connection: Keep-Alive\r\n
 Content-Type: text/html; charset=UTF-8\r\n
 \r\n
```

Expert Info (_ws.expert)

Part (2):

1. How many HTTP GET request messages did your browser send?

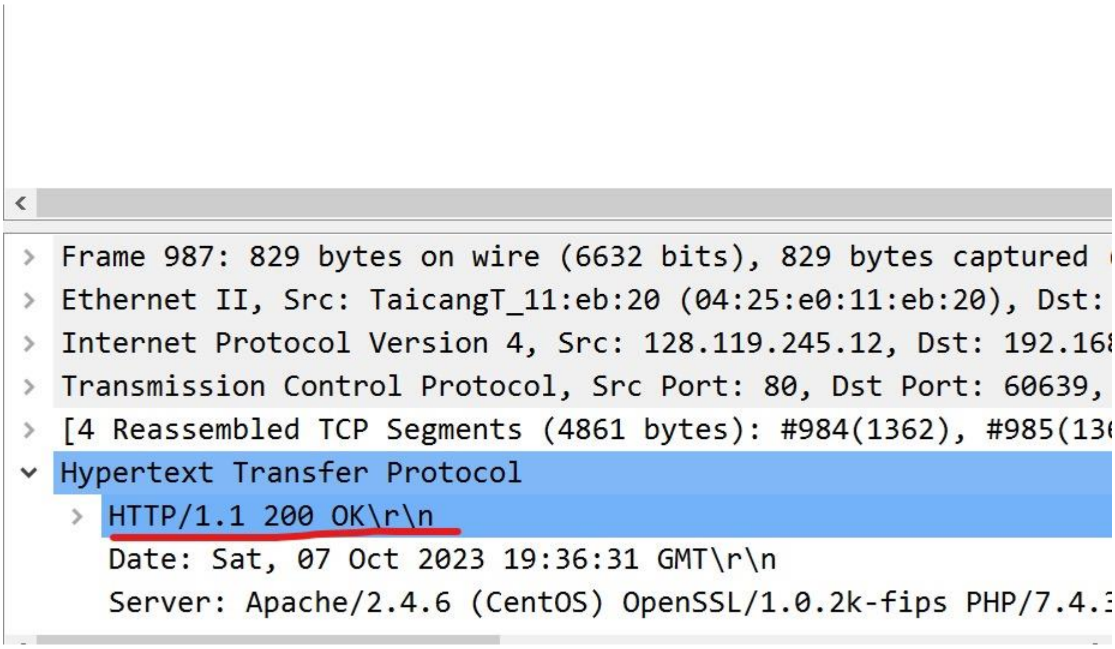
Answer: only 1 get



No.	Time	Source	Destination	Protocol	Length	Info
975	9.481550	192.168.1.24	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
987	9.664645	128.119.245.12	192.168.1.24	HTTP	829	HTTP/1.1 200 OK (text/html)

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

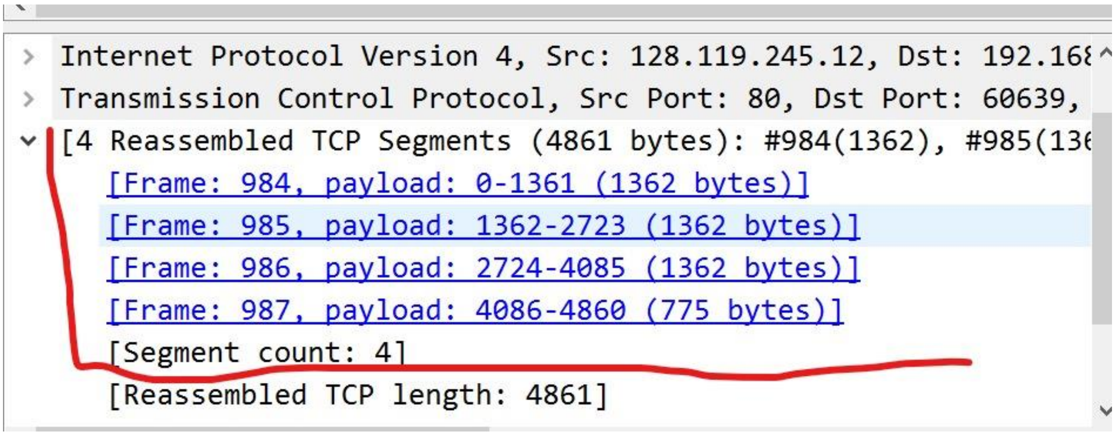
Answer:



```
> Frame 987: 829 bytes on wire (6632 bits), 829 bytes captured
> Ethernet II, Src: TaicangT_11:eb:20 (04:25:e0:11:eb:20), Dst:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.16
> Transmission Control Protocol, Src Port: 80, Dst Port: 60639,
> [4 Reassembled TCP Segments (4861 bytes): #984(1362), #985(13
v Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Sat, 07 Oct 2023 19:36:31 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.
```

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

Answer: 4 TCP segments



```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168
> Transmission Control Protocol, Src Port: 80, Dst Port: 60639,
v [4 Reassembled TCP Segments (4861 bytes): #984(1362), #985(136
      [Frame: 984, payload: 0-1361 (1362 bytes)]
      [Frame: 985, payload: 1362-2723 (1362 bytes)]
      [Frame: 986, payload: 2724-4085 (1362 bytes)]
      [Frame: 987, payload: 4086-4860 (775 bytes)]
      [Segment count: 4]
      [Reassembled TCP length: 4861]
```

Conclusion(including what I have learned):

at the end, we've tried retrieving both short and long html files. We learned how to see each packet information, like knowing when the packet was requested and when it was retrieved. And the HTTP version for both source and destination, also after the packet has been requested(GET request message) you will get the response status. Finally each packet include a body that shows your IP and and the site's IP, and the language your browser using, how many bytes of content being returned to you, and number of TCP segments.