

CSCI156 WireShark

Section 1

- 1) It uses HTTP 1.1 for the browser and version 4 for the server.

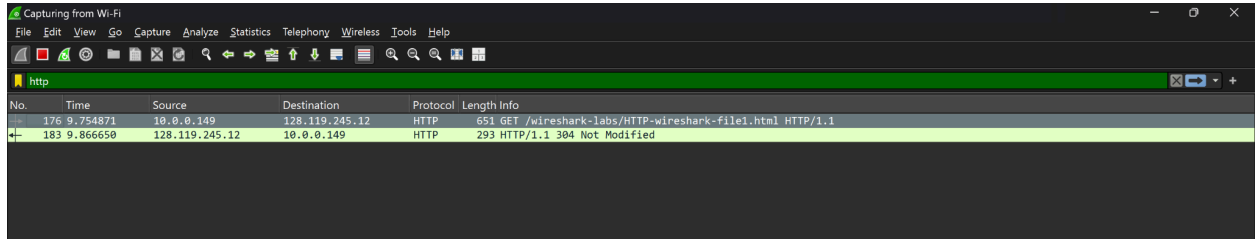


Figure 1. HTTP version for the browser

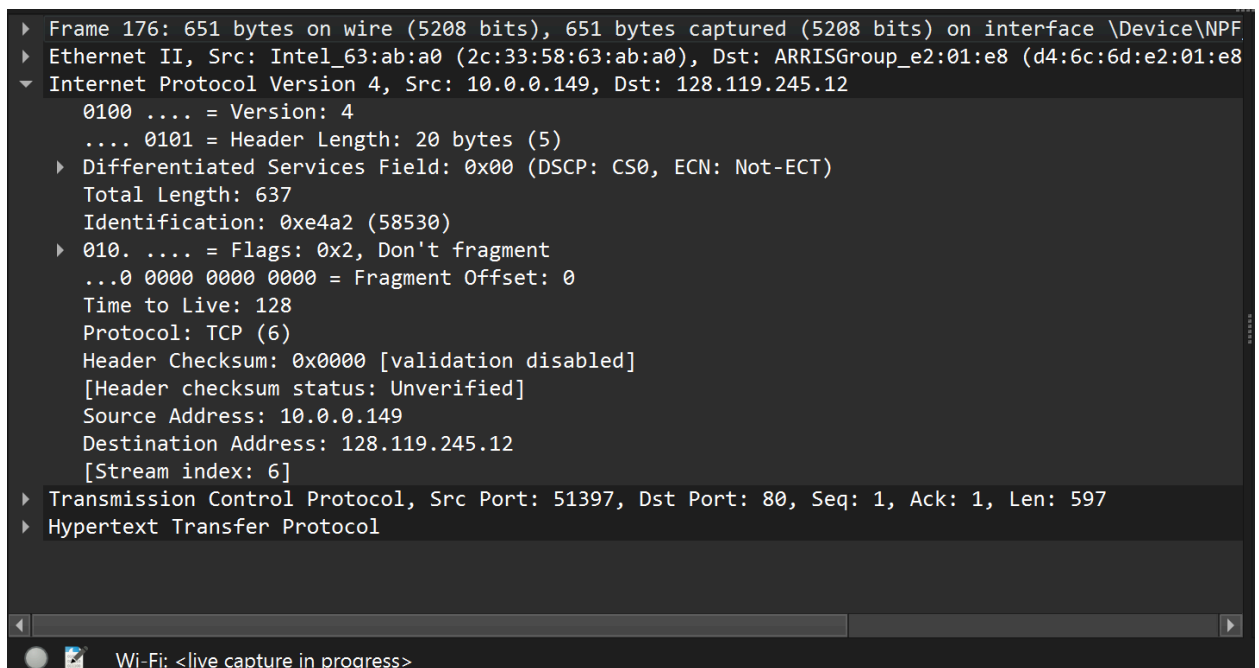
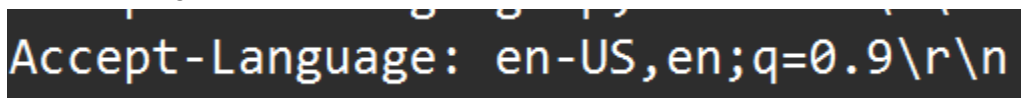


Figure 2. HTTP version for the server

- 2) It accepts English



- 3) The addresses are as indicated

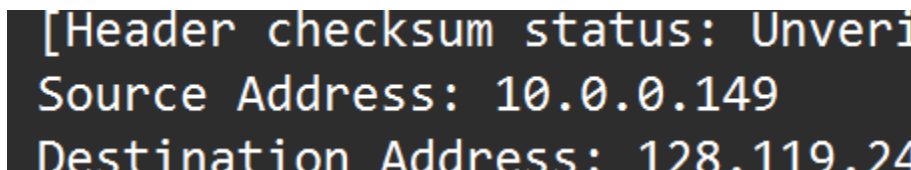


Figure 3. My IP address

Destination Address: 128.119.245.12

Figure 4. Server address

- 4) Status Code was 200.

Status Code: 200

- 5) Last modification:

Last-Modified: Sun, 27 Oct 2024 05:59:02 GMT\r\n

- 6) Content Length: 128 Bytes

[Content length: 128]

- 7) I did not see any headers.

Section 2

- 8) No, I do not see the modified since line.

```
▼ Hypertext Transfer Protocol
  ▼ GET /favicon.ico HTTP/1.1\r\n
    Request Method: GET
    Request URI: /favicon.ico
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
```

- 9) Yes, it does return the contents of the file.

```
File Data: 571 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
    \n
    </html>\n
```

- 10) Also do not see this line.

```

▼ Hypertext Transfer Protocol
  ▼ 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
    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)
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Response in frame: 766]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

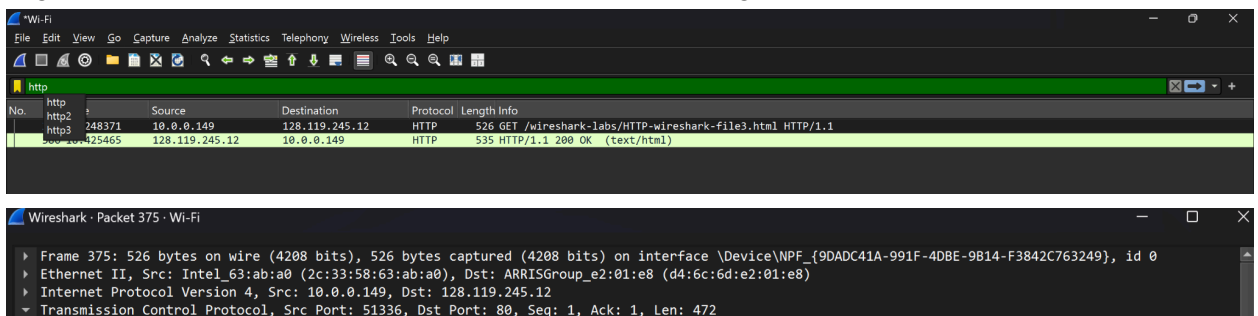
- 11) Status code is 404 and the phrase is: Not Found. It did not return the contents of the file because it was not able to find them.

Status Code: 404

Response Phrase: Not Found

Section 3

- 12) It got one GET request. Packet 375 has the GET message.



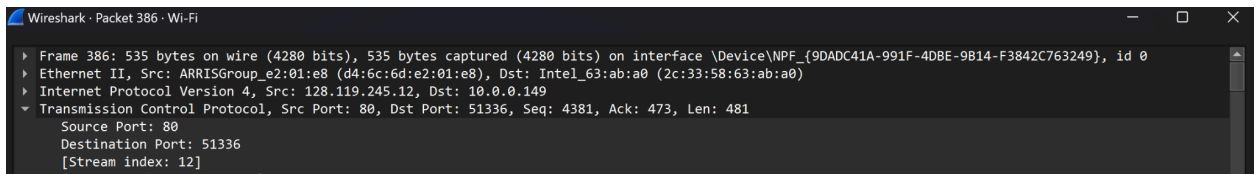
The image shows two screenshots from Wireshark. The top screenshot is the packet list pane, showing a table of captured packets. The bottom screenshot is the packet details pane for packet 375, showing the protocol stack and frame information.

No.	Time	Source	Destination	Protocol	Length	Info
http2	248371	10.0.0.149	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
http3	425465	128.119.245.12	10.0.0.149	HTTP	535	HTTP/1.1 200 OK (text/html)

Wireshark · Packet 375 · Wi-Fi

- Frame 375: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{9DADC41A-991F-4DBE-9B14-F3842C763249}, id 0
- Ethernet II, Src: ARRISGroup_e2:01:e8 (d4:6c:6d:e2:01:e8), Dst: Intel_63:ab:a0 (2c:33:58:63:ab:a0)
- Internet Protocol Version 4, Src: 10.0.0.149, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 51336, Dst Port: 80, Seq: 1, Ack: 1, Len: 472

- 13) Packet 386.



The image shows the packet details pane for packet 386 in Wireshark, displaying the protocol stack and frame information.

Wireshark · Packet 386 · Wi-Fi

- Frame 386: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{9DADC41A-991F-4DBE-9B14-F3842C763249}, id 0
- Ethernet II, Src: ARRISGroup_e2:01:e8 (d4:6c:6d:e2:01:e8), Dst: Intel_63:ab:a0 (2c:33:58:63:ab:a0)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.149
- Transmission Control Protocol, Src Port: 80, Dst Port: 51336, Seq: 4381, Ack: 473, Len: 481
- Source Port: 80
- Destination Port: 51336
- [Stream index: 12]

- 14) Status Code is 200, and Response Phrase is 'OK'.

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK

```

15) 4 TCP Segments.

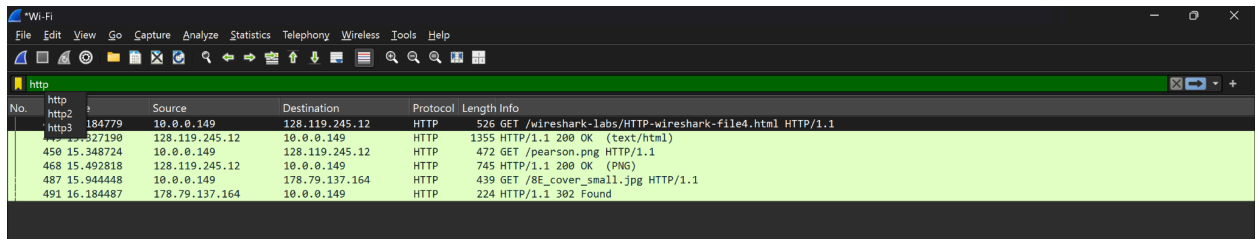
```

[4 Reassembled TCP Segments (4861 bytes): #382(1460), #383(1460), #384(1460), #386(481)]

```

Section 4

16) It sent 4 GET requests. They were sent to destination address of the GET protocol.



The image shows a Wireshark packet capture window with the 'http' filter applied. The packet list shows four GET requests, all with the same timestamp (15.348724) and destination IP (128.119.245.12). The first request is for /wireshark-labs/HTTP-wireshark-file4.html, the second for /pearson.png, the third for /8E_cover_small.jpg, and the fourth for /8E_cover_small.jpg. The packet details pane shows the first packet's structure: GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1.

No.	Time	Source	Destination	Protocol	Length	Info
1	15.348724	10.0.0.149	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
2	15.348724	10.0.0.149	128.119.245.12	HTTP	1355	HTTP/1.1 200 OK (text/html)
3	15.348724	10.0.0.149	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
4	15.348724	10.0.0.149	128.119.245.12	HTTP	745	HTTP/1.1 200 OK (PNG)
5	15.944448	10.0.0.149	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
6	16.184487	178.79.137.164	10.0.0.149	HTTP	224	HTTP/1.1 302 Found

17) I can tell they were downloaded in parallel since they had the same timestamp and not differing ones.

Section 5

18) Status Code: 401 and Response Phrase: Unauthorized.

```

404 11.790841 128.119.245.12 10.0.0.149 HTTP 771 HTTP/1.1 401 Unauthorized (text/html)
Hypertext Transfer Protocol
  HTTP/1.1 401 Unauthorized\r\n
    Response Version: HTTP/1.1
    Status Code: 401
    [Status Code Description: Unauthorized]
    Response Phrase: Unauthorized

```

19) Authorization field is included.

```

  Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5=\r\n

```