

# Lab 3

AbdelRahman Adel AbdelFattah

17012296

1. Request Version: HTTP/1.1  
Response Version: HTTP/1.1
2. Accept-Language: en-US,en
3. Server Address: 128.119.245.12  
Computer Address: 192.168.1.7
4. Status Code: 200
5. Last-Modified: Wed, 09 November 2022, 06:59:01 GMT
6. File Data: 128 bytes
7. None was found
8. No there is no "IF-MODIFIED-SINCE"
9. Yes It returned explicitly the contents of the file, wireshark shows a "Line-based text data" drop menu
10. If-Modified-Since: Wed, 09 Nov 2022 06:59:01 GMT\r\n
11. Status Code: 304 - Not Modified, and the server didn't specifically return the content because it wasn't modified so it retrieved it from the cache of the browser.
12. Only one HTTP GET request and packet number was 170
13. packet 180
14. Status Code: 200  
Response Phrase: OK
15. [4 Reassembled TCP Segments (4861 bytes): #177(1420), #178(1420), #179(1420), #180(601)]
16. 4 GET requests, one fore the HTML, 2 for the images, and one for the favicon.ico
17. Both requests were sent in parallel, and then got back in parallel according to wireshark, since it was GET and then another GET and then responses.
18. Status Code: 401  
Response Phrase: Unauthorized
19. Authorization: Basic d2lyZXNoYXJrLXN0dWRIbnRzOm5ldHdvcm5=\r\n  
Credentials: wireshark-students:network

No.	Time	Source	Destination	Protocol
13	2022/313 11:56:41.214055	192.168.1.7	128.119.245.12	HTTP 544

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1  
Frame 13: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface en0, id 0

Section number: 1  
Interface id: 0 (en0)  
Interface name: en0  
Interface description: Wi-Fi  
Encapsulation type: Ethernet (1)  
Arrival Time: Nov 9, 2022 11:56:41.214055000 EET  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1667987801.214055000 seconds  
[Time delta from previous captured frame: 0.000670000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 2.204374000 seconds]  
Frame Number: 13  
Frame Length: 544 bytes (4352 bits)  
Capture Length: 544 bytes (4352 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:http]  
[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: Apple\_24:87:4e (50:ed:3c:24:87:4e), Dst: zte\_b4:e2:25 (24:d3:f2:b4:e2:25)  
Destination: zte\_b4:e2:25 (24:d3:f2:b4:e2:25)  
Address: zte\_b4:e2:25 (24:d3:f2:b4:e2:25)  
.... ..0. .... = LG bit: Globally unique address (factory default)  
.... ..0 .... = IG bit: Individual address (unicast)  
Source: Apple\_24:87:4e (50:ed:3c:24:87:4e)  
Address: Apple\_24:87:4e (50:ed:3c:24:87:4e)  
.... ..0. .... = LG bit: Globally unique address (factory default)  
.... ..0 .... = IG bit: Individual address (unicast)  
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
0000 00.. = Differentiated Services Codepoint: Default (0)  
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)  
Total Length: 530  
Identification: 0x0000 (0)  
010. .... = Flags: 0x2, Don't fragment  
0... .... = Reserved bit: Not set  
.1.. .... = Don't fragment: Set  
..0. .... = More fragments: Not set  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 64  
Protocol: TCP (6)  
Header Checksum: 0x01b3 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 192.168.1.7  
Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 65506, Dst Port: 80, Seq: 1, Ack: 1, Len: 478  
Source Port: 65506  
Destination Port: 80  
[Stream index: 1]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 478]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 3033946166  
[Next Sequence Number: 479 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 2143700587  
1000 .... = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, ACK)  
000. .... = Reserved: Not set  
...0 .... = Accurate ECN: Not set  
.... 0... = Congestion Window Reduced: Not set  
.... .0.. = ECN-Echo: Not set  
.... ..0. = Urgent: Not set  
.... ...1 .... = Acknowledgment: Set  
.... .... 1... = Push: Set  
.... .... .0.. = Reset: Not set  
.... .... ..0. = Syn: Not set  
.... .... ...0 = Fin: Not set  
[TCP Flags: .....AP...]  
Window: 2063  
[Calculated window size: 132032]  
[Window size scaling factor: 64]  
Checksum: 0xaf04 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
TCP Option - No-Operation (NOP)  
Kind: No-Operation (1)  
TCP Option - No-Operation (NOP)  
Kind: No-Operation (1)  
TCP Option - Timestamps  
Kind: Time Stamp Option (8)  
Length: 10  
Timestamp value: 791171842: TSval 791171842, TSecr 1774131279  
Timestamp echo reply: 1774131279  
[Timestamps]  
[Time since first frame in this TCP stream: 0.154220000 seconds]  
[Time since previous frame in this TCP stream: 0.000670000 seconds]  
[SEQ/ACK analysis]  
[iRTT: 0.153550000 seconds]  
[Bytes in flight: 478]  
[Bytes sent since last PSH flag: 478]  
TCP payload (478 bytes)  
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]  
[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]  
[Severity level: Chat]  
[Group: Sequence]  
Request Method: GET  
Request URI: /wireshark-labs/HTTP-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  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML,  
like Gecko) Chrome/107.0.0.0 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-file1.html]  
[HTTP request 1/2]  
[Response in frame: 15]  
[Next request in frame: 17]

No.	Time	Source	Destination	Protocol	
Length	Info				
15	2022/313 11:56:41.350918	128.119.245.12	192.168.1.7	HTTP	552
HTTP/1.1 200 OK (text/html)					
Frame 15: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0					

```
Section number: 1
Interface id: 0 (en0)
  Interface name: en0
  Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Nov  9, 2022 11:56:41.350918000 EET
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1667987801.350918000 seconds
[Time delta from previous captured frame: 0.000001000 seconds]
[Time delta from previous displayed frame: 0.136863000 seconds]
[Time since reference or first frame: 2.341237000 seconds]
Frame Number: 15
Frame Length: 552 bytes (4416 bits)
Capture Length: 552 bytes (4416 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]
Ethernet II, Src: zte_b4:e2:25 (24:d3:f2:b4:e2:25), Dst: Apple_24:87:4e (50:ed:3c:24:87:4e)
  Destination: Apple_24:87:4e (50:ed:3c:24:87:4e)
    Address: Apple_24:87:4e (50:ed:3c:24:87:4e)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ..0. .... = IG bit: Individual address (unicast)
  Source: zte_b4:e2:25 (24:d3:f2:b4:e2:25)
    Address: zte_b4:e2:25 (24:d3:f2:b4:e2:25)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 538
  Identification: 0x5eb4 (24244)
  010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 46
  Protocol: TCP (6)
  Header Checksum: 0xb4f6 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 128.119.245.12
  Destination Address: 192.168.1.7
Transmission Control Protocol, Src Port: 80, Dst Port: 65506, Seq: 1, Ack: 479, Len: 486
  Source Port: 80
  Destination Port: 65506
  [Stream index: 1]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 486]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2143700587
  [Next Sequence Number: 487 (relative sequence number)]
  Acknowledgment Number: 479 (relative ack number)
  Acknowledgment number (raw): 3033946644
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .....0. = Urgent: Not set
```

.... 1.... = Acknowledgment: Set  
.... 1... = Push: Set  
.... .0.. = Reset: Not set  
.... ..0. = Syn: Not set  
.... ...0 = Fin: Not set  
[TCP Flags: .....AP...]

Window: 235

[Calculated window size: 30080]

[Window size scaling factor: 128]

Checksum: 0xcaf1 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

TCP Option - Timestamps

Kind: Time Stamp Option (8)

Length: 10

Timestamp value: 1774131417: TSval 1774131417, TSecr 791171842

Timestamp echo reply: 791171842

[Timestamps]

[Time since first frame in this TCP stream: 0.291083000 seconds]

[Time since previous frame in this TCP stream: 0.000001000 seconds]

[SEQ/ACK analysis]

[iRTT: 0.153550000 seconds]

[Bytes in flight: 486]

[Bytes sent since last PSH flag: 486]

TCP payload (486 bytes)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

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

[HTTP/1.1 200 OK\r\n\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Wed, 09 Nov 2022 09:56:41 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

Last-Modified: Wed, 09 Nov 2022 06:59:01 GMT\r\n

ETag: "80-5ed043103b344"\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

[HTTP response 1/2]

[Time since request: 0.136863000 seconds]

[Request in frame: 13]

[Next request in frame: 17]

[Next response in frame: 18]

[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)

<html>\n

Congratulations. You've downloaded the file \n

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n

</html>\n