

CO222- Wireshark Lab 2

E/19/166

1. Both server and Browser are running HTTP Version 1.1

Wireshark capture showing HTTP 1.1 traffic. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the request structure, including Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language.

No.	Time	Source	Destination	Protocol	Length	Info
67	15:18:05.677100	192.168.1.157	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
95	15:18:05.956908	128.119.245.12	192.168.1.157	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15:18:06.017179	192.168.1.157	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
99	15:18:06.297158	128.119.245.12	192.168.1.157	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 67: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface 0
Ethernet II, Src: HonHaiPr_96:0c:cf (90:32:4b:96:0c:cf), Dst: Guangzho_16:f3:33 (08:00:27:16:f3:33)
Internet Protocol Version 4, Src: 192.168.1.157, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55123, Dst Port: 80, Seq: 1, Ack: 1, Len: 533
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.81 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png; q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n

2. Server accepts English and English-US

Wireshark capture showing HTTP 1.1 traffic. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the request structure, including Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language.

No.	Time	Source	Destination	Protocol	Length	Info
67	15:18:05.677100	192.168.1.157	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
95	15:18:05.956908	128.119.245.12	192.168.1.157	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15:18:06.017179	192.168.1.157	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
99	15:18:06.297158	128.119.245.12	192.168.1.157	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 67: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface 0
Ethernet II, Src: HonHaiPr_96:0c:cf (90:32:4b:96:0c:cf), Dst: Guangzho_16:f3:33 (08:00:27:16:f3:33)
Internet Protocol Version 4, Src: 192.168.1.157, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55123, Dst Port: 80, Seq: 1, Ack: 1, Len: 533
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.81 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png; q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n

3. Source (IP address of my computer) : 128.119.245.12
Destination (IP address of the Server): 192.168.1.157

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list on the left shows four packets. The selected packet (No. 95) is an HTTP GET request from 128.119.245.12 to 192.168.1.157. The packet details pane on the right shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane on the right shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
67	15:18:05.677100	192.168.1.157	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
95	15:18:05.956908	128.119.245.12	192.168.1.157	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15:18:06.017179	192.168.1.157	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
99	15:18:06.297158	128.119.245.12	192.168.1.157	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 95: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
> Ethernet II, Src: Guangzho_16:66:33 (98:a9:42:16:66:33), Dst: HonHaiPr_96:0c:cf (98:0d:11:16:00:00)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.157
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 526
Identification: 0x6a1d (27165)
> 010. = Flags: 0x2, Don't fragment
... 0000 0000 0000 = Fragment Offset: 0
Time to Live: 34
Protocol: TCP (6)
Header Checksum: 0xb503 [validation disabled]
[Header checksum status: Unverified]

Hypertext Transfer Protocol: Protocol

Packets: 133 - Displayed: 4 (3.0%) - Dropped: 0 (0.0%)

4. Status code: 200 OK

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list on the left shows four packets. The selected packet (No. 95) is an HTTP GET request from 128.119.245.12 to 192.168.1.157. The packet details pane on the right shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane on the right shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
67	15:18:05.677100	192.168.1.157	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
95	15:18:05.956908	128.119.245.12	192.168.1.157	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15:18:06.017179	192.168.1.157	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
99	15:18:06.297158	128.119.245.12	192.168.1.157	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 95: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
> Ethernet II, Src: Guangzho_16:66:33 (98:a9:42:16:66:33), Dst: HonHaiPr_96:0c:cf (98:0d:11:16:00:00)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.157
> Transmission Control Protocol, Src Port: 80, Dst Port: 55123, Seq: 1, Ack: 480, Len: 540
> Hypertext Transfer Protocol
> Line-based text data: text/html (4 lines)

Internet Protocol Version 4 (ip), 20 bytes

Packets: 133 - Displayed: 4 (3.0%) - Dropped: 0 (0.0%)

5. Last Modified: Fri, 21 Oct 2022 05:59:02 GMT

Wireshark packet capture showing an HTTP GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane highlights the 'Last-Modified' header value: 'Fri, 21 Oct 2022 05:59:02 GMT'.

No.	Time	Source	Destination	Protocol	Length	Info
67	15:18:05.677100	192.168.1.157	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
95	15:18:05.956908	128.119.245.12	192.168.1.157	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15:18:06.017179	192.168.1.157	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
99	15:18:06.297158	128.119.245.12	192.168.1.157	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Packet 95 details:

- Transmission Control Protocol, Src Port: 80, Dst Port: 55123, Seq: 1, Ack: 480, Win: 0, Len: 0
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Date: Fri, 21 Oct 2022 09:48:02 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11
 - Last-Modified: Fri, 21 Oct 2022 05:59:02 GMT\r\n**
 - ETag: "80-5eb85237d6784"\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 1/2]

6. 128 bytes

Wireshark packet capture showing an HTTP GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane highlights the 'Content-Length' header value: '128'.

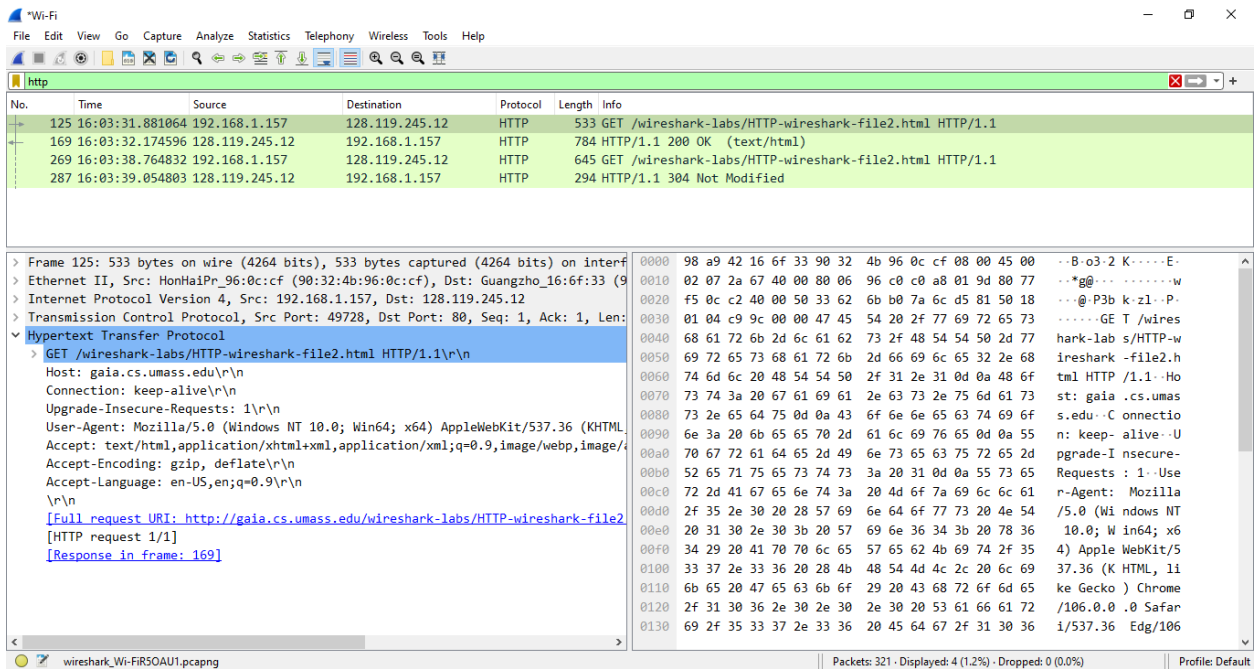
No.	Time	Source	Destination	Protocol	Length	Info
67	15:18:05.677100	192.168.1.157	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
95	15:18:05.956908	128.119.245.12	192.168.1.157	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15:18:06.017179	192.168.1.157	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
99	15:18:06.297158	128.119.245.12	192.168.1.157	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Packet 95 details:

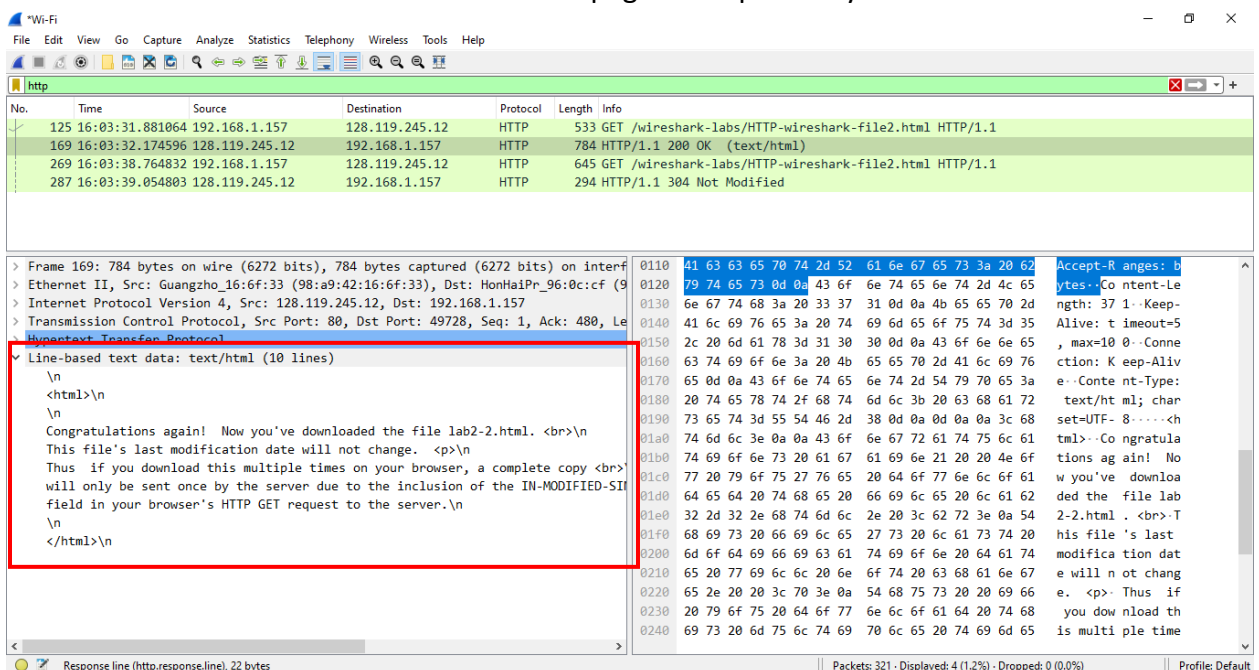
- Transmission Control Protocol, Src Port: 80, Dst Port: 55123, Seq: 1, Ack: 480, Win: 0, Len: 0
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Date: Fri, 21 Oct 2022 09:48:02 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11
 - Last-Modified: Fri, 21 Oct 2022 05:59:02 GMT\r\n
 - ETag: "80-5eb85237d6784"\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 1/2]
 - [Time since request: 0.279808000 seconds]
 - [Request in frame: 67]
 - [Next request in frame: 98]

7. Couldn't see any different headers in both windows.

8. No. I didn't see "IF-MODIFIED-SINCE" in HTTP GET request



9. The server explicitly returned the contents of file. Proof is the “Line-Base Text Data” section. It contains HTML code which matches to the page that opened by browser.



10. Yes. There is a term “IF-MODIFIED-SINCE:”. This header shows the date and time that the website was last accessed.

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows four packets, with the fourth packet (No. 287) selected. The packet details pane on the right shows the Hypertext Transfer Protocol section, which includes the 'If-Modified-Since' header. The header value is 'Fri, 21 Oct 2022 05:59:02 GMT'. The packet bytes pane on the right shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
125	16:03:31.881064	192.168.1.157	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
169	16:03:32.174596	128.119.245.12	192.168.1.157	HTTP	784	HTTP/1.1 200 OK (text/html)
269	16:03:38.764832	192.168.1.157	128.119.245.12	HTTP	645	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
287	16:03:39.054803	128.119.245.12	192.168.1.157	HTTP	294	HTTP/1.1 304 Not Modified

Frame 269: 645 bytes on wire (5160 bits), 645 bytes captured (5160 bits) on interface
> Ethernet II, Src: HonHaiPr_96:0c:cf (90:32:4b:96:0c:cf), Dst: Guangzho_16:f6:33 (9
> Internet Protocol Version 4, Src: 192.168.1.157, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49727, Dst Port: 80, Seq: 1, Ack: 1, Len:
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "173-5eb85237d5fb4"
If-Modified-Since: Fri, 21 Oct 2022 05:59:02 GMT
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2
[HTTP request 1/1]
[Response in frame: 287]

11. Status Code: 304

No file was return by the server because my browser was cached the site in previous request. Therefore, if there isn't any change in the page there is no need to receive file again. So, the page is loaded by cached data.

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows four packets, with the fourth packet (No. 287) selected. The packet details pane on the right shows the Hypertext Transfer Protocol section, which includes the 'If-Modified-Since' header. The header value is 'Fri, 21 Oct 2022 10:33:35 GMT'. The packet bytes pane on the right shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
125	16:03:31.881064	192.168.1.157	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
169	16:03:32.174596	128.119.245.12	192.168.1.157	HTTP	784	HTTP/1.1 200 OK (text/html)
269	16:03:38.764832	192.168.1.157	128.119.245.12	HTTP	645	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
287	16:03:39.054803	128.119.245.12	192.168.1.157	HTTP	294	HTTP/1.1 304 Not Modified

Frame 287: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface
> Ethernet II, Src: Guangzho_16:f6:33 (98:a9:42:16:f6:33), Dst: HonHaiPr_96:0c:cf (9
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.157
> Transmission Control Protocol, Src Port: 80, Dst Port: 49727, Seq: 1, Ack: 592, Le
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified
Date: Fri, 21 Oct 2022 10:33:35 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Per
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "173-5eb85237d5fb4"
[HTTP response 1/1]
[Time since request: 0.289971000 seconds]
[Request in frame: 269]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]