

Name =

Abubaker Attique

Roll no =

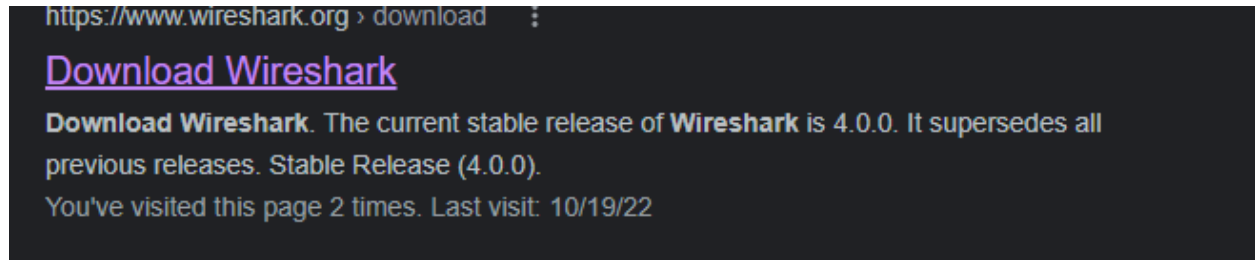
P20-0560

Section =

5-A

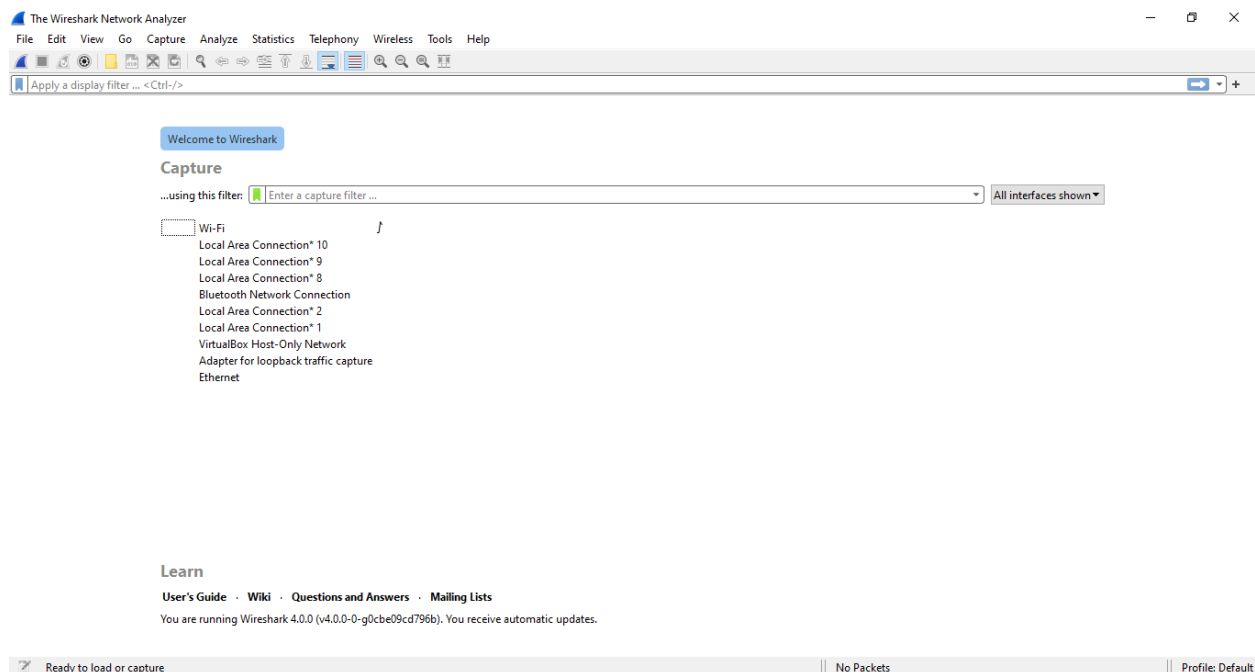
Lab 8

INSTALLATION PROCESS:



Install this setup :

After installation



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
612	7.205797	fe80::7de6:b2a9:409...	ff02::fb	MDNS	136	Standard query response 0x0000 AAAA fe80::7de6:b2a9:4099:f22f A 172.17.2.24
613	7.207285	fe80::7de6:b2a9:409...	ff02::1:3	LLMNR	92	Standard query 0xd5b1 ANY MAQ500D-LPTP
614	7.210254	172.17.2.24	224.0.0.252	LLMNR	72	Standard query 0xd5b1 ANY MAQ500D-LPTP
615	7.210254	172.17.2.114	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
616	7.213704	172.17.2.114	224.0.0.251	MDNS	136	Standard query 0x0001 PTR _X9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast...
617	7.213704	172.17.2.114	224.0.0.251	MDNS	136	Standard query 0x0001 PTR _X9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast...
618	7.213704	172.17.2.222	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
619	7.261545	213.136.74.178	172.17.0.104	TCP	56	61449 → 55922 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
620	7.317728	172.17.0.104	172.217.18.138	UDP	75	64687 → 443 Len=33
621	7.318029	172.17.0.104	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
622	7.357947	172.217.18.138	172.17.0.104	UDP	1167	443 → 64687 Len=1125
623	7.375753	172.17.0.104	172.217.18.138	UDP	75	64687 → 443 Len=33
624	7.392274	Routerbo_1e:0c:99	Broadcast	ARP	56	Who has 172.17.1.97? Tell 172.17.0.2

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \N
 > Ethernet II, Src: Chongqin_93:f8:3b (5c:3a:45:93:f8:3b), Dst: Routerbo_1e:0c:99 (5c:3a:45:93:f8:3b)
 > Internet Protocol Version 4, Src: 172.17.0.104, Dst: 223.233.70.18
 > Transmission Control Protocol, Src Port: 55931, Dst Port: 15636, Seq: 0, Len: 0

0000 cc 2d e0 1e 0c 99 5c 3a 45 93 f8 3b 08 00 45 00: E-;-E-
 0010 00 34 12 38 40 00 80 06 16 17 ac 11 00 68 df e9 -4 8@... ..h..
 0020 46 12 da 7b 3d 14 8f 50 f4 3b 00 00 00 00 80 02 F-{-P ;.....
 0030 fa f0 06 8e 00 00 02 04 05 b4 01 03 03 08 01 01
 0040 04 02 ..

Task: By looking at the information in the HTTP GET and response messages, answer the following questions

1. Is your browser running HTTP version 1.0, 1.1, or 2?

Answer :

Browser is running on HTTP version 1.1.

Wireshark packet capture showing an HTTP GET request and response. The packet list shows packet 617 as the GET request and packet 643 as the 200 OK response. The packet details for packet 617 show the request line: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1. The packet bytes show the raw data of the request.

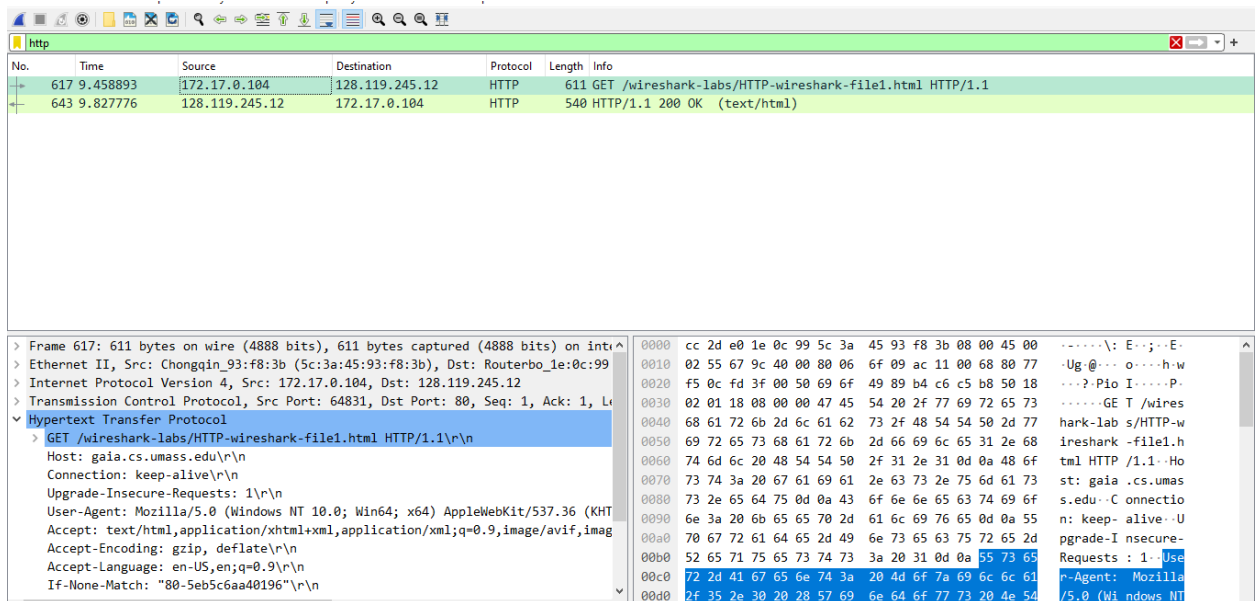
2. What version of HTTP is the server running?

Answer :

Server is running on Http 1.1.

Wireshark packet capture showing an HTTP 200 OK response. The packet list shows packet 643 as the 200 OK response. The packet details for packet 643 show the response line: HTTP/1.1 200 OK. The packet bytes show the raw data of the response.

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



The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows two packets: a GET request (No. 617) and an OK response (No. 643). The packet details pane shows the structure of the GET request, including the Host, Connection, User-Agent, Accept, Accept-Encoding, Accept-Language, and If-None-Match headers. The packet bytes pane shows the raw data of the request, including the GET method, the URL, and the headers.

No.	Time	Source	Destination	Protocol	Length	Info
617	9.458893	172.17.0.104	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
643	9.827776	128.119.245.12	172.17.0.104	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 617: 611 bytes on wire (4888 bits), 611 bytes captured (4888 bits) on interface 0
> Ethernet II, Src: Chongqin_93:f8:3b (5c:3a:45:93:f8:3b), Dst: Routerbo_1e:0c:99
> Internet Protocol Version 4, Src: 172.17.0.104, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64831, Dst Port: 80, Seq: 1, Ack: 1, Len: 611
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.183 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "80-5eb5c6aa40196"

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

Answer : To know about the ip address of our computer will we open our command prompt and write ipconfig.....from there we will know about the ip address of the computer.

Ip of my computer :

IPV4 Address = 172.17.0.104

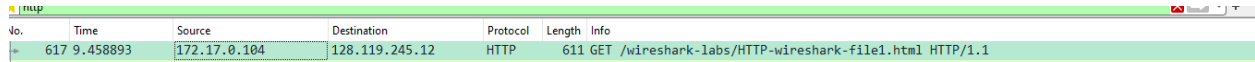
Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::bc68:e3f:aa37:a679%16
IPv4 Address. . . . . : 172.17.0.104
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 172.17.0.2
```

IP address of the gaia.cs.umass.edu server

In the wireshark here we can see the ip addresss

172.17.0.104

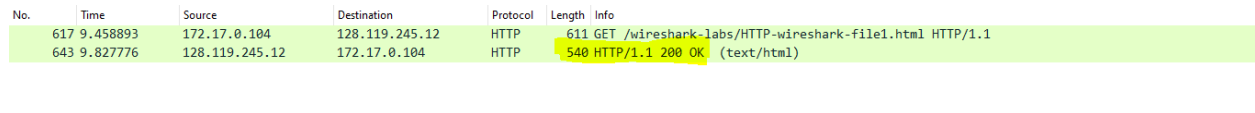


No.	Time	Source	Destination	Protocol	Length	Info
617	9.458893	172.17.0.104	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

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

Answer :

The status code returned from the server to browser is 200 OK.

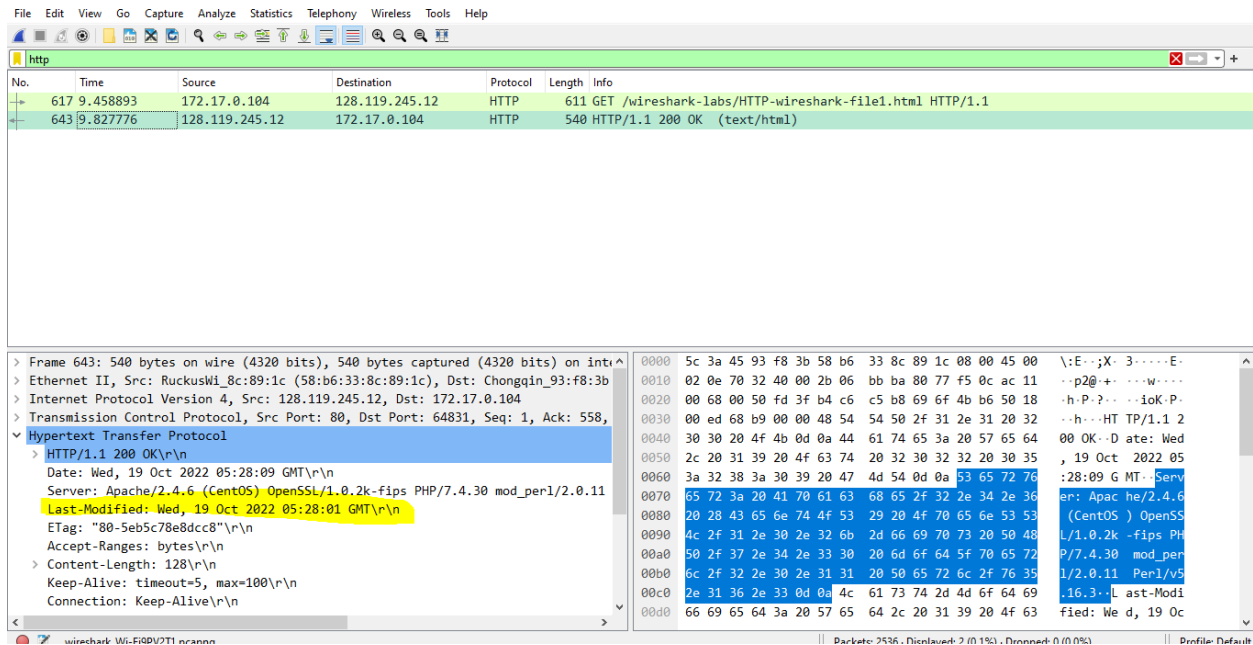


No.	Time	Source	Destination	Protocol	Length	Info
617	9.458893	172.17.0.104	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
643	9.827776	128.119.245.12	172.17.0.104	HTTP	540	HTTP/1.1 200 OK (text/html)

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

Answer :

Here in the Wireshark we can see the last modify as shown in the pic below.



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

Answer :

In this we can see the file size in bits

http

No.	Time	Source	Destination	Protocol	Length	Info
617	9.458893	172.17.0.104	128.119.245.12	HTTP	611	GET /wi
643	9.827776	128.119.245.12	172.17.0.104	HTTP	540	HTTP/1.

```

    ETag: "80-5eb5c78e8dcc8"\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 1/1]
    [Time since request: 0.368883000 seconds]
    [Request in frame: 617]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.ht
    File Data: 128 bytes
  > Line-based text data: text/html (4 lines)
  
```

8. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one

Answer :

No there is no header within the data that are not displayed in the packet-listing window.

Task 2: Answer the following questions:

No.	Time	Source	Destination	Protocol	Length	Info
4287	61.101855	172.17.0.104	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4308	61.397227	128.119.245.12	172.17.0.104	HTTP	784	HTTP/1.1 200 OK (text/html)
4443	62.898495	172.17.0.104	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4455	63.195470	128.119.245.12	172.17.0.104	HTTP	293	HTTP/1.1 304 Not Modified

1. 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?

Answer :

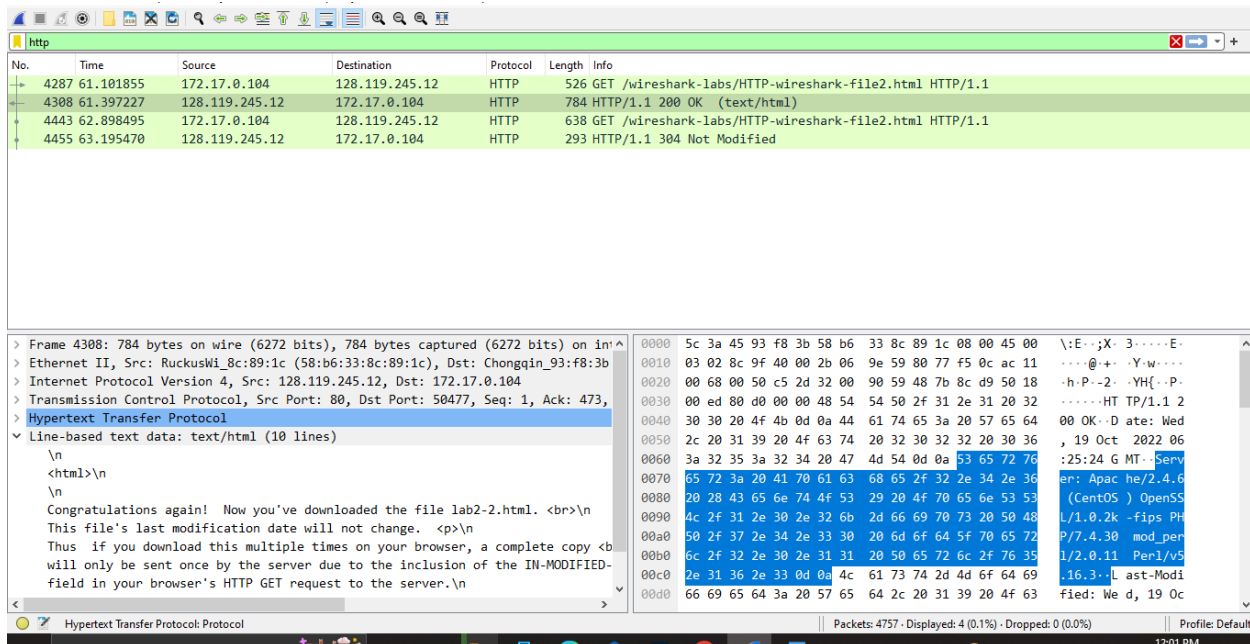
There is no “IF-MODIFIED-SINCE” in the first HTTP GET request because the request for the server is for first time.

No.	Time	Source	Destination	Protocol	Length	Info
4287	61.101855	172.17.0.104	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4308	61.397227	128.119.245.12	172.17.0.104	HTTP	784	HTTP/1.1 200 OK (text/html)
4443	62.898495	172.17.0.104	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4455	63.195470	128.119.245.12	172.17.0.104	HTTP	293	HTTP/1.1 304 Not Modified

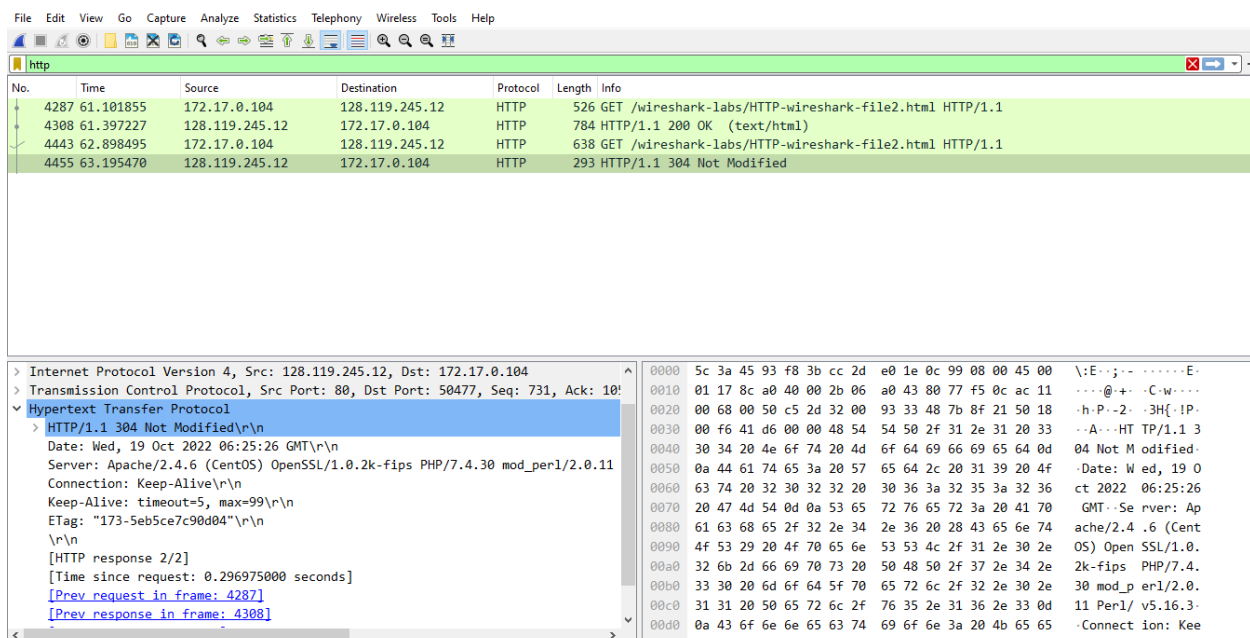
2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer :

When we inspect the contents of the server response, the contents of the file were returned by the server explicitly. But in the second response it did not give the explicit result.



This give the result explicity.



This did not give the result explicity.

3.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 GET6 ? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer : After inspection the content of HTTP GET request from your browser to the server , we see an “IF-MOBIIFIED-SINCE” , we get the date , time, day this is because we refresh the page.

No.	Time	Source	Destination	Protocol	Length	Info
4287	61.101855	172.17.0.104	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4308	61.397227	128.119.245.12	172.17.0.104	HTTP	784	HTTP/1.1 200 OK (text/html)
4443	62.898495	172.17.0.104	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4455	63.195470	128.119.245.12	172.17.0.104	HTTP	293	HTTP/1.1 304 Not Modified

Host: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\nIf-None-Match: "173-5eb5ce7c90d04"\r\nIf-Modified-Since: Wed, 19 Oct 2022 05:59:01 GMT\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]\r\n[HTTP request 2/2]\r\n[Prev request in frame: 4287]

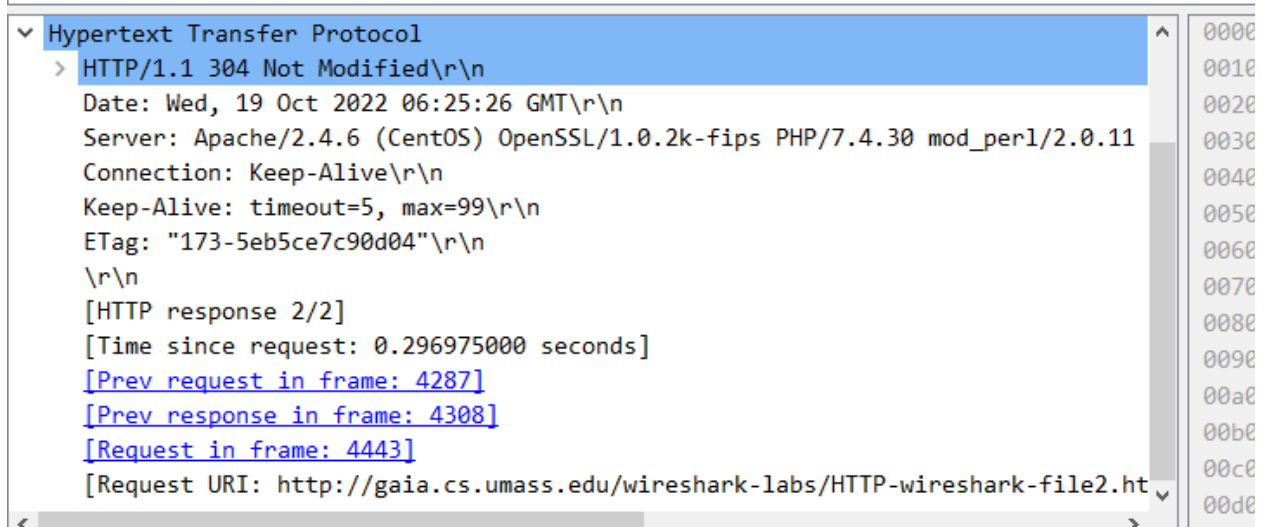
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu..C connectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 n: keep-alive..C
00a0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 ache-Con trol: ma
00b0 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 65 x-age=0- .Upgrade
00c0 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 -Insecur e-Reques
00d0 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e ts: 1..U ser-Agen
00e0 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
00f0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
0100 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70 Win64; x64) App
0110 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 leWebKit /537.36
0120 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 (KHTML, like Gec
0130 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 30 36 2e 30 ko) Chro me/106.0
0140 2e 30 2e 30 20 53 61 66 61 72 69 2f 35 33 37 2e .0.0 Saf ari/537.
0150 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 36- -Acce pt: text

HTTP Connection (http.connection). 24 bytesPackets: 4757 · Disallowed: 4 (0.1%) · Dropped: 0 (0.0%)Profile: Default

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.

Answer

:



The image shows a Wireshark packet capture of an HTTP response. The packet list on the left shows a selected packet of type 'Hypertext Transfer Protocol'. The packet details pane on the right shows the following information:

```
> HTTP/1.1 304 Not Modified\r\n
Date: Wed, 19 Oct 2022 06:25:26 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=99\r\n
ETag: "173-5eb5ce7c90d04"\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.296975000 seconds]
[Prev request in frame: 4287]
[Prev response in frame: 4308]
[Request in frame: 4443]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.ht
```

The packet bytes pane on the right shows the raw data of the packet, starting with 0000.

It is NOT MODIFIED because when the request is done for the first time it will from the server when we again refresh the page this time it will not give from server this time it will be from cache.