

## Lab 9

### Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Both Browser running on 1.0

No.	Time	Source	Destination	Protocol	Length	Info
684	6.391018000	10.102.110.7	34.107.221.82	HTTP	357	GET /canonical.html HTTP/1.1
685	6.391018000	10.102.110.7	34.107.221.82	HTTP	357	GET /success.txt?ip=10.102.110.7
704	6.422909000	34.107.221.82	10.102.110.7	HTTP	352	HTTP/1.1 200 OK (text/html)
710	6.424432000	34.107.221.82	10.102.110.7	HTTP	270	HTTP/1.1 200 OK (text/plain)
719	6.456313000	10.102.110.7	34.107.221.82	HTTP	374	GET /success.txt?ip=HTTP/1.1
742	6.489656000	34.107.221.82	10.102.110.7	HTTP	270	HTTP/1.1 200 OK (text/plain)
2084	24.7701000	10.102.110.30	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
2118	22.132190000	10.102.110.30	150.121.21.11	HTTP	704	GET /brackettime/time/current?cup2key=2:8GL3cpnprivl1-ON2QD3-D1s3nua7fGhtrMyvq0BY2M&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4
2286	22.657170000	150.171.27.11	10.102.110.7	HTTP	917	HTTP/1.1 200 OK (application/json)
8657	24.247701000	10.102.110.30	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
11134	27.271268000	10.102.110.30	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
11635	30.281541000	10.102.110.30	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
11933	33.282812000	10.102.110.30	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
12110	36.283630000	10.102.110.30	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

```
[@] Frame 684: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface 0
[@] Ethernet II, Src: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4), Dst: Cisco_Oc:10:ff (00:01:9e:0c:10:ff)
[@] Internet Protocol Version 4, Src: 10.102.110.7 (10.102.110.7), Dst: 34.107.221.82 (34.107.221.82)
[@] Transmission Control Protocol, Src Port: 37907 (37907), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 303
[@] Hypertext Transfer Protocol
[+] GET /canonical.html HTTP/1.1\r\n
Host: detectportal.firefox.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0\r\n
Accept: */*\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Cache-Control: no-cache\r\n
Pragma: no-cache\r\n
Connection: keep-alive\r\n
\r\n
[+] Full request URL: http://detectportal.firefox.com/canonical.html
[HTTP request 1/1]
[Response in frame: 704]
```

### Q2: What languages (if any) does your browser indicate that it can accept to the server?

The languages the browser indicating accepted to the server are:

En-us

No.	Time	Source	Destination	Protocol	Length	Info
549	5.923809000	10.102.110.7	34.107.221.82	HTTP	357	GET /canonical.html HTTP/1.1
557	5.938680000	34.107.221.82	10.102.110.7	HTTP	352	HTTP/1.1 200 OK (text/html)
662	6.157136000	10.102.110.7	34.107.221.82	HTTP	374	GET /success.txt?tpv4 HTTP/1.1
676	6.192321000	34.107.221.82	10.102.110.7	HTTP	270	HTTP/1.1 200 OK (text/plain)

```

Frame 549: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface 0
Ethernet II, Src: Cisco_Or10:ff:00 (e8:cf:83:42:53:cd), Dst: Cisco_Or10:ff (00:0f:9e:0c:10:ff)
Internet Protocol Version 4, Src: 10.102.110.7 (10.102.110.7), Dst: 34.107.221.82 (34.107.221.82)
Transmission Control Protocol, src Port: 33323 (33323), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 303
HyperText Transfer Protocol
GET /canonical.html HTTP/1.1\r\n
Host: detectportal.firefox.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0\r\n
Accept: */*\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Cache-Control: no-cache\r\n
Pragma: no-cache\r\n
Connection: keep-alive\r\n
Via:\r\n
[Full request URL: http://detectportal.firefox.com/canonical.html]
[HTTP request 1/1]
[Response in frame: 557]
```

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

200 OK

### 4. When was the HTML file that last modified at the server? (http 200 ok server side)

Thu, 30 Oct 2025 time14:18:56 GMT\r\n

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

Content-Length: 8\r\n

### 7. 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.

There are not such headers displayed

First you clear the cache, ctrl+shift+delete on firfox

**8. 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?**

No, I don't see an “IF-MODIFIED-SINCE” line in the HTTP GET. Because server retrieve the data

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

No, because it was sent by cache, the server did not open up the page again.

**10. Close the browser and open the link again. Capture this packet. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIEDSINCE?” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?**

Both time are same after reload the page and first

IF-Modified\_since: Tue, 28 Oct 2025 5:59:01 GMT\r\n

1244 44.23.65.2400010.102.110.5	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
2942 41.204.94.60010.102.110.7	128.119.245.12	HTTP	527 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2953 41.42143200128.119.245.12	10.102.110.7	HTTP	365 HTTP/1.1 304 Not Modified
3270 46.171.66.50010.102.110.7	128.119.245.12	HTTP	527 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
3294 46.388.10.800128.119.245.12	10.102.110.7	HTTP	364 HTTP/1.1 304 Not Modified

```
Frame 2942: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface 0
Ethernet II, Src: e8:cf:83:42:53:c4 (e8:cf:83:42:53:c4), Dst: Cisco_Oc10:ff (00:1f:9e:0c:10:ff)
Internet Protocol Version 4, Src: 10.102.110.7 (10.102.110.7), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 20167 (20167), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 473
HyperText Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Tue, 28 Oct 2025 05:59:01 GMT\r\n
If-None-Match: "173-64231b67176b7"\r\n
Priority: u=0, i=\r\n
\r\n
[Full request URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/2]
[Response in frame: 2953]
[Next request in frame: 3270]
```

## **12. How many HTTP GET request messages were sent by your browser?**

There are two get request.

No.	Time	Source	Destination	Protocol	Length	Info
6273	18.066652	10.102.110.7	128.119.245.12	HTTP	441	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
6301	18.291591	128.119.245.12	10.102.110.7	HTTP	538	HTTP/1.1 200 OK (text/html)
6320	18.311314	10.102.110.7	128.119.245.12	HTTP	461	GET /favicon.ico HTTP/1.1
6347	18.535158	128.119.245.12	10.102.110.7	HTTP	636	HTTP/1.1 301 Moved Permanently (text/html)

## **13. How many data-containing TCP segments were needed to carry the single HTTP response?**

387 TCP segment were added to carry single HTTP segment

No.	Time	Source	Destination	Protocol	Length	Info
6273	18.066652	10.102.110.7	128.119.245.12	HTTP	441	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
6301	18.291591	128.119.245.12	10.102.110.7	HTTP	538	HTTP/1.1 200 OK (text/html)
6320	18.311314	10.102.110.7	128.119.245.12	HTTP	461	GET /favicon.ico HTTP/1.1
6347	18.535158	128.119.245.12	10.102.110.7	HTTP	636	HTTP/1.1 301 Moved Permanently (text/html)

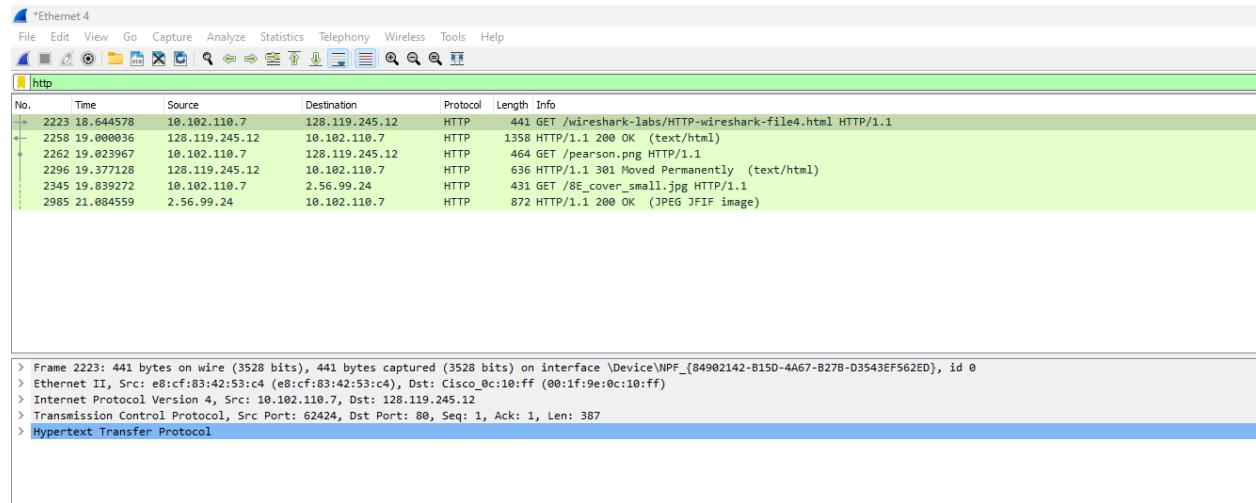
```
> Frame 6273: 441 bytes on wire (3528 bits), 441 bytes captured (3528 bits) on interface \Device\NPF_{84902142-B15D-4A67-B278-D3543EF562ED}, id 0
> Ethernet II, Src: e8:c8:83:42:53:c4 (e8:c8:83:42:53:c4), Dst: Cisco_0c:10:ff (00:1f:9e:0c:10:ff)
> Internet Protocol Version 4, Src: 10.102.110.7, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 8396, Dst Port: 80, Seq: 1, Ack: 1, Len: 387
    Source Port: 8396
    Destination Port: 80
    [Stream index: 64]
    [TCP Segment Len: 387]
    Sequence number: 1 (relative sequence number)
    Sequence number (raw): 4201296922
    [Next sequence number: 388 (relative sequence number)]
    Acknowledgment number: 1 (relative ack number)
    Acknowledgment number (raw): 2473300439
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x0108 (PSH, ACK)
    Window size value: 1026
    [Calculated window size: 262656]
    [Window size scaling factor: 256]
    Checksum: 0xeef8e [unverified]
```

0000: f5 4c 20 cc 00 50 f0 6a h4 1a 93 6b 91 d7 50 1a ...-p..i ...k..p...

**14. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?**

Three GET request, and their destination address are followed:

1. 128.102.110.7
2. 128.102.110.7 see destination address from below pic
3. 10.102.110.7



**15. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**

Two images send serially. As only one request was sent to which response come in.

See JPEG image last command