



תקשורת

מטלה 1



WIRESHARK

INTRO

1) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

2) How long did it take from when the HTTP GET message was sent until the HTTP

OK reply was received? (By default, the value of the Time column in the packet-

listing window is the amount of time, in seconds, since Wireshark tracing began.

To display the Time field in time-of-day format, select the Wireshark View pull

down menu, then select Time Display Format, then select Time-of-day.)

3). What is the Internet address of the `gaia.cs.umass.edu` (also known as `www-`

`net.cs.umass.edu`)? What is the Internet address of your computer?)

4). Print the two HTTP messages (GET and OK) referred to in question 2 above. To

do so, select Print from the Wireshark File command menu, and select the

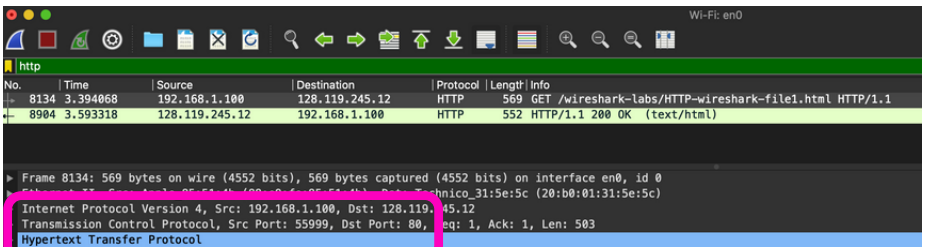
"Selected Packet Only" and "Print as displayed" radial buttons, and then click

OK.

Question 1

List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Answer 1



Here we can clearly see 3 different protocols

- Internet Protocol Version 4. "IPV4"
- Transmission Control Protocol "TCP"
- Hypertext Transfer Protocol "HTTP"

Question 2

How long did it take from when the HTTP GET message was sent until the HTTP

OK reply was received? (By default, the value of the Time column in the packet-

listing window is the amount of time, in seconds, since Wireshark tracing began.

To display the Time field in time-of-day format, select the Wireshark View pull

down menu, then select Time Display Format, then select Time-of-day.)

Answer 2

Time
3.394068
3.593318

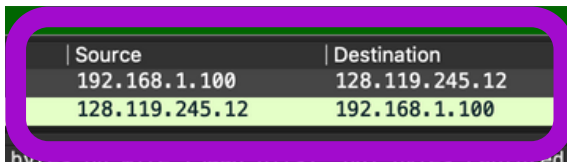
Time To execute 3.394068

Question 3

3). What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)?

What is the Internet address of your computer?

Answer 3



Source	Destination
192.168.1.100	128.119.245.12
128.119.245.12	192.168.1.100

Computer Internet address :

- Source Address "**192.168.1.100**"

gaia.cs.umass.edu Internet address :

- Destination Address "**128.119.245.12**"

Question 4

Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.

Answer 4

/var/folders/2h/_cqqmpms0k91t9rl27l22nph0000gn/T/wireshark_Wi-Fi2QUU0.pcapng 14279 total packets, 2 shown

No.	Time	Source	Destination	Protocol	Length	Info
8134	3.394068	192.168.1.100	128.119.245.12	HTTP	569	GET /

wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 8134: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits) on interface en0, id 0
Ethernet II, Src: Apple_85:51:4b (88:e9:fe:85:51:4b), Dst: Technico_31:5e:5c (20:b0:01:31:5e:5c)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55999, Dst Port: 80, Seq: 1, Ack: 1, Len: 503
Hypertext Transfer Protocol

WIRESHARK

HTTP

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. What languages (if any) does your browser indicate that it can accept to the server?
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
4. What is the status code returned from the server to your browser?
5. When was the HTML file that you are retrieving last modified at the server?
6. How many bytes of content are being returned to your browser?
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.
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?
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
10. 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 GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?
11. 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.
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
14. What is the status code and phrase in the response?
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Question 1

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

Answer 1

```
552 HTTP/1.1 200 OK (text/html)
```

My browser running HTTP version 1.1

Question 2

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

Answer 2

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,  
Accept-Encoding: gzip, deflate\r\n  
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
```

French & English (US)

Question 3

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

Answer 3

Source	Destination
192.168.1.100	128.119.245.12

Computer Internet address :

- Source Address **"192.168.1.100"**

gaia.cs.umass.edu Internet address :

- Destination Address **"128.119.245.12"**

Question 4

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

Answer 4

552 HTTP/1.1 200 OK (text/html)

200 OK

Question 5

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

Answer 5

```
Last-Modified: Sat, 14 Nov 2020 06:59:02 GMT\r\n
```

Saturday 14 Novembre 2020 at 06:59:02

Question 6

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

Answer 6

```
Accept-Ranges: bytes\r\n
▼ Content-Length: 128\r\n
    [Content length: 128]
Keep-Alive: timeout=5, max=1
```

Content-Length 128 Bytes

Question 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. No. The raw data appears to match up exactly with what is shown in the packet-listing window.

Answer 7

No, i don't see any header

Question 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?

Answer 8

No, i don't see any "IF-MODIFIED-SINCE

Question 9

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

Answer 9

```
\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
```

Yes i can clearly see the contain html :
"Congratulation. Again! ..."

Question 10

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 GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

Answer 10

```
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If-None-Match: "80-5b40bae1a9518"\r\n
If-Modified-Since: Sat, 14 Nov 2020 06:59:02 GMT\r\n
\r\n
```

Sat, 14 Nov 2020

06:59:02

Question 11

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 11

```
304 HTTP/1.1 304 Not Modified
```

```
Hypertext Transfer Protocol
```

```
HTTP/1.1 304 Not Modified\r\n
```

The second HTTP GET returned 304 Not Modified because the request don't have to be renew the cash well know this adress so it can be signified that nothing was modified since my last request .

Question 12

How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Answer 12

645	192.168.1.100	128.119.245.12	HTTP	569	GET /wireshark-labs/HTTP-wireshark-file3.ht
652	128.119.245.12	192.168.1.100	HTTP	883	HTTP/1.1 200 OK (text/html)

My browser send 1 HTTP GET request message

Question 13

Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer 13

43	6	336645	192.168.1.100	128.119.245.12	HTTP	569	GET /wireshark-labs/HT
55	6	533652	128.119.245.12	192.168.1.100	HTTP	883	HTTP/1.1 200 OK (text/

No. 43

Question 14

What is the status code and phrase in the response?

Answer 14

```
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
```

GET /wireshark-labs/HTPP-wireshark-file3.html HTTP/1.1

Question 15

How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Answer 15

```
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
HTTP/1.1 200 OK (text/html)
```

2 TCP segments (1GET)(1 OK).

Question 16

How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer 16

No.	Time	Source	Destination	Protocol	Length	Info
52	2.834963	192.168.1.100	128.119.245.12	HTTP	569	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
75	3.838690	128.119.245.12	192.168.1.100	HTTP	1139	HTTP/1.1 200 OK (text/html)
77	3.067043	192.168.1.100	128.119.245.12	HTTP	501	GET /pearson.png HTTP/1.1
106	3.269795	128.119.245.12	192.168.1.100	HTTP	981	HTTP/1.1 200 OK (PNG)
133	3.478382	192.168.1.100	128.119.245.12	HTTP	475	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
278	4.309361	128.119.245.12	192.168.1.100	HTTP	284	HTTP/1.1 200 OK (JPEG JFIF image)

1 destinations :

- 128.119.245.12

Question 17

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

Answer 17

Picture 1

[3 Reassembled TCP Segments (3611 bytes): #103(1348), #104(1348), #106(915)]

Picture 2

▶ [77 Reassembled TCP Segments (101318 bytes): #137(1348), #138(1348

both images have been downloaded in series

Question 18

What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer 18

68	3.848689	192.168.1.100	128.119.245.12	HTTP	601	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
74	4.841381	128.119.245.12	192.168.1.100	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
319	32.771244	192.168.1.100	128.119.245.12	HTTP	668	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
324	33.791718	128.119.245.12	192.168.1.100	HTTP	586	HTTP/1.1 404 Not Found (text/html)

The server's response in the initial HTTP GET is the N°68 GET/wireshark-labs/protected_pages/HTTP-wireshark-HTTP/1.1

Question 19

When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer 19

68	3.848689	192.168.1.100	128.119.245.12	HTTP	601	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
74	4.841381	128.119.245.12	192.168.1.100	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
319	32.771244	192.168.1.100	128.119.245.12	HTTP	668	GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1
324	33.791718	128.119.245.12	192.168.1.100	HTTP	586	HTTP/1.1 404 Not Found (text/html)

Unauthorized