תיקשורת ומחשוב

מטלה 1

<u>מגישים</u>

יעקב מילורקובסקי: 207045053

דולב דוגלוף: 207867342

1c קלסן

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

A: HTTP, UDP, TCP

Q: 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*.)

A:

Info	Length	Protocol	Destination	Source	Time	.No
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1	637	HTTP	128.119.245.12	192.168.43.223	10:37:17.308600 2022-03-16	82
HTTP/1.1 200 OK (text/html)	540	HTTP	192.168.43.223	128.119.245.12	10:37:17.493564 2022-03-16	95

17.493564 - 17.308600 = 0.184964 sec

Q: 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?

A: gaia → 128.119.245.12

ME: 192.168.43.223

Q: 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.

```
No.     Time                           Source                Destination           Protocol Length Info
     82 2022-03-16 10:37:17.308600     192.168.43.223        128.119.245.12        HTTP     637    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 82: 637 bytes on wire (5096 bits), 637 bytes captured (5096 bits) on interface \Device\NPF_{7536D27E-1811-46B4-8C42-C5C7E92194CC}, id 0
Ethernet II, Src: CyberTAN_e0:69:0f (28:39:26:e0:69:0f), Dst: 72:1b:45:3e:90:31 (72:1b:45:3e:90:31)
Internet Protocol Version 4, Src: 192.168.43.223, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61231, Dst Port: 80, Seq: 1, Ack: 1, Len: 583
Hypertext Transfer Protocol
No.     Time                           Source                Destination           Protocol Length Info
     95 2022-03-16 10:37:17.493564     128.119.245.12        192.168.43.223        HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 95: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{7536D27E-1811-46B4-8C42-C5C7E92194CC}, id 0
Ethernet II, Src: 72:1b:45:3e:90:31 (72:1b:45:3e:90:31), Dst: CyberTAN_e0:69:0f (28:39:26:e0:69:0f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.223
Transmission Control Protocol, Src Port: 80, Dst Port: 61231, Seq: 1, Ack: 584, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
```

חלק ב

Q: 1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

A:

Info	Length	Protocol	Destination	Source	Time	.No
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1	637	HTTP	128.119.245.12	192.168.43.223	10:37:17.308600 2022-03-16	82
HTTP/1.1 200 OK (text/html)	540	HTTP	192.168.43.223	128.119.245.12	10:37:17.493564 2022-03-16	95

Http 1.1 server

Http 1.1 chrome

Q: 2. What languages (if any) does your browser indicate that it can accept to the server?

A:

```
                                                Connection: keep-alive\r\n
                                                Cache-Control: max-age=0\r\n
                                                Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 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: he,en;q=0.9\r\n
                                                If-None-Match: "173-5da4f9c360102"\r\n
                                                If-Modified-Since: Wed, 16 Mar 2022 05:59:01 GMT\r\n
                                                r\n\
                                                [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
                                                [HTTP request 1/1]
                                                [Response in frame: 703]
```

עברית, אנגלית

Q: 3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

A:

Info	Length	Protocol	Destination	Source	Time	.No
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1	637	HTTP	128.119.245.12	192.168.43.223	10:37:17.308600 2022-03-16	82
HTTP/1.1 200 OK (text/html)	540	HTTP	192.168.43.223	128.119.245.12	10:37:17.493564 2022-03-16	95

me: 192.168.43.223

gaia: 128.119.245.12

Q: 4. What is the status code returned from the server to your browser?

A:

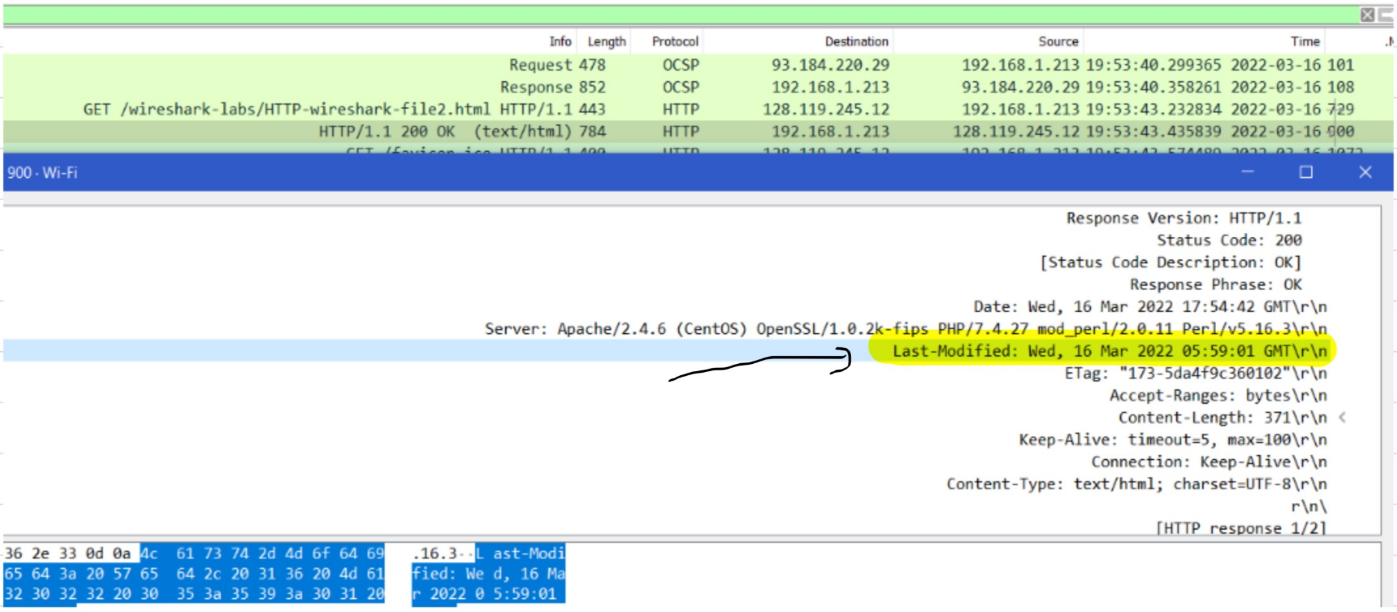
```
        Protocol Length Info
        HTTP     540    HTTP/1.1 200 OK  (text/html)
interface \Device\NPF_{7536D27E-1811-46B4-8C42-C5C7E921
69:0f (28:39:26:e0:69:0f)

584, Len: 486
```

→ 200 OK

Q: 5. When was the HTML file that you are retrieving last modified at the server?

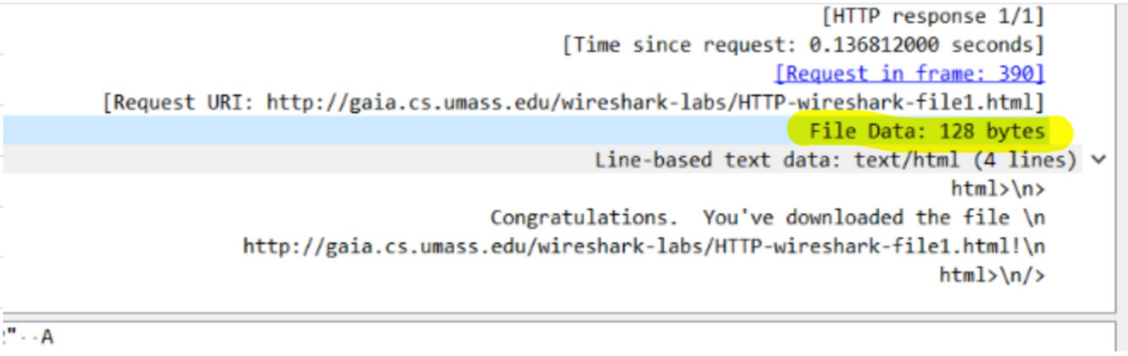
A:



Wed, 16 Mar 2022 05:59:01 GMT

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

A:



128 bytes

Q: 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.

A: לאו, החלון הוא תגובה מורחבת של המידע

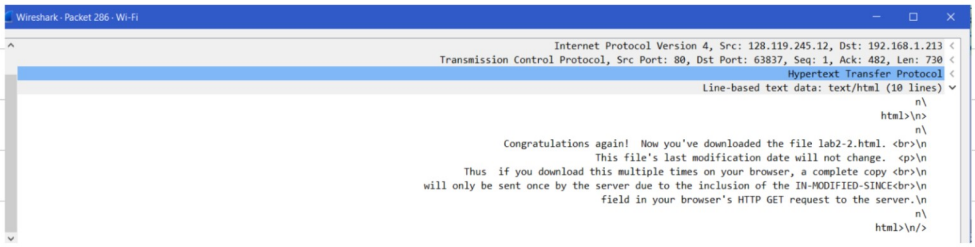
למשל השדה File Data

לא מופיע בתגובה הקטנה.

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?

לא, אין שורה כזו

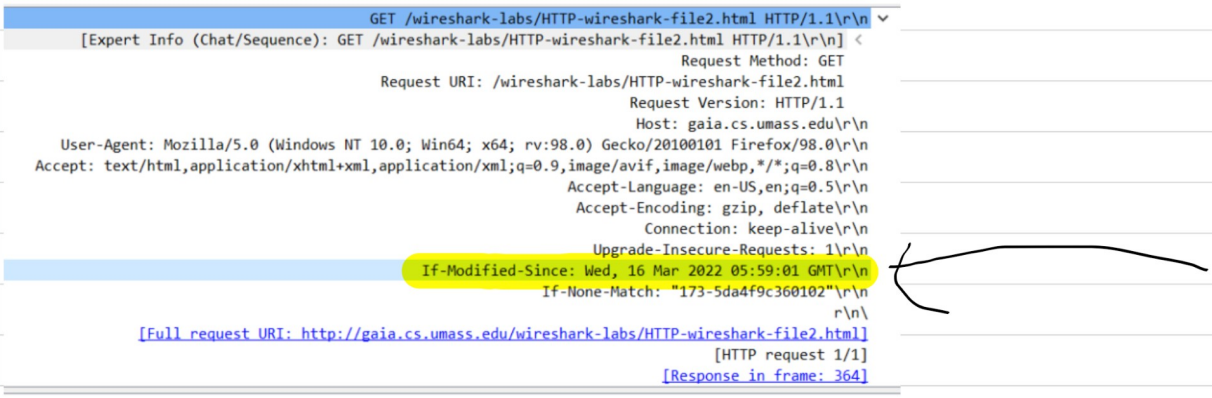
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



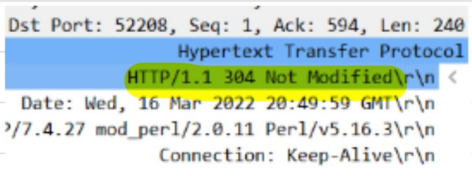
HTML

כן ←

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?



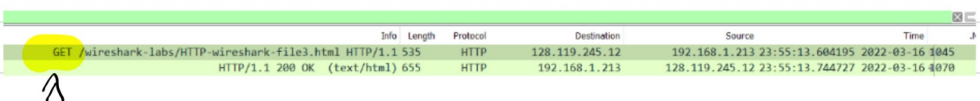
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.



כיוון שהדף לא השתנה
אז אין צורך לשלוח את כל התוכן
מחדש.

---

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?



בקשה אחת Get

Q: 13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

A: התגובה שחוזרת מהשרת

Info	Length	Protocol	Destination	Source	Time	No.
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1	535	HTTP	128.119.245.12	192.168.1.213	23:55:13.604195 2022-03-16	1045
HTTP/1.1 200 OK (text/html)	655	HTTP	192.168.1.213	128.119.245.12	23:55:13.744727 2022-03-16	1070

Q: 14. What is the status code and phrase in the response?

A: 200 OK

Q: 15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

```
[Reassembled TCP Segments (4861 bytes): #1066(1420), #1067(1420), #1069(1420), #1070(601) 4]
[Frame: 1066, payload: 0-1419 (1420 bytes)]
[Frame: 1067, payload: 1420-2839 (1420 bytes)]
[Frame: 1069, payload: 2840-4259 (1420 bytes)]
[Frame: 1070, payload: 4260-4860 (601 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4861]
```

A: 4 סגמנטים

Q: Answer the following questions:

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

A: 3 בקשות Get לכתובות כפולות

Info	Length	Protocol	Destination	Source	Time	No.
GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	535	HTTP	128.119.245.12	192.168.1.213	00:13:48.143856 2022-03-17	1021
HTTP/1.1 200 OK (text/html)	1355	HTTP	192.168.1.213	128.119.245.12	00:13:48.281756 2022-03-17	1080
GET /pearson.png HTTP/1.1	481	HTTP	128.119.245.12	192.168.1.213	00:13:48.289993 2022-03-17	1081
HTTP/1.1 200 OK (PNG)	825	HTTP	192.168.1.213	128.119.245.12	00:13:48.428254 2022-03-17	1110
GET /8E_cover_small.jpg HTTP/1.1	448	HTTP	178.79.137.164	192.168.1.213	00:13:48.565602 2022-03-17	1136
HTTP/1.1 301 Moved Permanently	225	HTTP	192.168.1.213	178.79.137.164	00:13:48.633049 2022-03-17	1152

Q: 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.

Info	Length	Protocol	Destination	Source	Time	No.
GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	535	HTTP	128.119.245.12	192.168.1.213	00:13:48.143856 2022-03-17	1021
HTTP/1.1 200 OK (text/html)	1355	HTTP	192.168.1.213	128.119.245.12	00:13:48.281756 2022-03-17	1080
GET /pearson.png HTTP/1.1	481	HTTP	128.119.245.12	192.168.1.213	00:13:48.289993 2022-03-17	1081
HTTP/1.1 200 OK (PNG)	825	HTTP	192.168.1.213	128.119.245.12	00:13:48.428254 2022-03-17	1110
GET /8E_cover_small.jpg HTTP/1.1	448	HTTP	178.79.137.164	192.168.1.213	00:13:48.565602 2022-03-17	1136
HTTP/1.1 301 Moved Permanently	225	HTTP	192.168.1.213	178.79.137.164	00:13:48.633049 2022-03-17	1152

סדרתי, כי אם נסתכל על הזמנים נוכל
לראות שרק לאחר התמונה הראשונה נשלחה
בקשה לתמונה השנייה.

Answer the following questions:

Q

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

A:

Info	Length	Protocol	Destination	Source	Time
GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1	458	HTTP	128.119.245.12	192.168.1.213	00:54:25.432792 2022-03-17 135
HTTP/1.1 401 Unauthorized (text/html)	771	HTTP	192.168.1.213	128.119.245.12	00:54:25.568169 2022-03-17 151

```
Line-based text data: text/html (12 lines)
DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n!>
html><head>\n>
title>401 Unauthorized</title>\n>
head><body>\n/>
h1>Unauthorized</h1>\n>
p>This server could not verify that you\n>
are authorized to access the document\n
requested.  Either you supplied the wrong\n
credentials (e.g., bad password), or your\n
browser doesn't understand how to supply\n
the credentials required.</p>\n
body></html>\n/>
```

401 Unauthorized

Q:

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

```
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
Credentials: wireshark-students:network
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Cache-Control: max-age=0\r\n
r\n\
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
```

Credentials: