

מטרה 1 בתקשות - פתרון

Wireshark Lab: Intro

.1

נבחר את ה프וטוקולים: HTTP, TCP, DNS

Wireshark Screenshot showing captured traffic. Key frames highlighted:

- Frame 10: 431 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
- Frame 11: 60 80 → 38268 [ACK] Seq=1 Ack=378 Win=64240 Len=0
- Frame 15: 54 38266 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 MSS=1460
- Frame 17: 101 Standard query 0x9a81 A incoming.telemetry.mozilla.org OP
- Frame 18: 492 HTTP/1.1 200 OK (text/html)

.2

נחסר את הפרש הזמן בין הودעת ה-HTTP GET לבין ההודעה שקיבלו מהשרת. כפי שניתן לראות שני ההודעות התבכו באותה שניה ולכן ניתן לחשב את הפרש בזאת.

$$\text{נקבל: } 0.219694620 - 0.067698998 = 0.151995622$$

Wireshark Screenshot showing a zoomed-in view of the first two frames. Both are selected (indicated by a double red border).

Frame 10 (Selected):

```

HTTP/1.1 200 OK\r\n
Date: Fri, 19 Mar 2021 08:15:37 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Fri, 19 Mar 2021 05:59:01 GMT\r\n
ETag: "51-5bdd69a76b76"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\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 1/1]
[Time since request: 0.151995622 seconds]
[Request in frame: 10]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Data: 81 bytes

```

Frame 15 (Selected):

```

HTTP/1.1 200 OK (text/html)

```

.3

כתובת המחשב שלנו: 192.168.190.129
 כתובת השירות: 128.119.245.12

תחת הודעתה HTTP GET ניתן לראות בשדה "Internet Protocol" את הכתובת של המחשב שלנו (Source) שנשלחת ע"י הדפסן ואת הכתובת של השירות (Destination) התואם לשם הכתובת הנתונה כפי שניתן לראות תחת שדה ה-"Host".

```

No. Time Source Destination Protocol Length Info
10 01:15:37.067698998 192.168.190.129 128.119.245.12 HTTP 431 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
15 01:15:37.219694620 128.119.245.12 192.168.190.129 HTTP 492 HTTP/1.1 200 OK (text/html)
25 01:15:37.379645025 192.168.190.129 128.119.245.12 HTTP 388 GET /favicon.ico HTTP/1.1
27 01:15:37.549556886 128.119.245.12 192.168.190.129 HTTP 539 HTTP/1.1 404 Not Found (text/html)

Frame 10: 431 bytes on wire (3448 bits), 431 bytes captured (3448 bits) on interface ens33, id 0
Ethernet II, Src: VMware_eb:f6:dd (00:0c:29:eb:f6:dd), Dst: VMware_e6:94:d4 (00:50:56:e6:94:d4)
Internet Protocol Version 4, Src: 192.168.190.129, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 38268, Dst Port: 80, Seq: 1, Ack: 1, Len: 377
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 15]

```

.4

פלט הודעתה HTTP כפי שהtabקשו להציג בשאלת:

No.	Time	Source	Destination	Protocol	Length	Info
10	01:15:37.067698998	192.168.190.129	128.119.245.12	HTTP	431	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 10:	431 bytes on wire (3448 bits), 431 bytes captured (3448 bits) on interface ens33, id 0					
Ethernet II,	Src: VMware_eb:f6:dd (00:0c:29:eb:f6:dd), Dst: VMware_e6:94:d4 (00:50:56:e6:94:d4)					
Internet Protocol Version 4,	Src: 192.168.190.129, Dst: 128.119.245.12					
Transmission Control Protocol,	Src Port: 38268, Dst Port: 80, Seq: 1, Ack: 1, Len: 377					
Hypertext Transfer Protocol						
	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n					
	Host: gaia.cs.umass.edu\r\n					
	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n					
	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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					
	\r\n					
	[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]					
	[HTTP request 1/1]					
	[Response in frame: 15]					
No.	Time	Source	Destination	Protocol	Length	Info
15	01:15:37.219694620	128.119.245.12	192.168.190.129	HTTP	492	HTTP/1.1 200 OK (text/html)
Frame 15:	492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface ens33, id 0					
Ethernet II,	Src: VMware_e6:94:d4 (00:50:56:e6:94:d4), Dst: VMware_eb:f6:dd (00:0c:29:eb:f6:dd)					
Internet Protocol Version 4,	Src: 128.119.245.12, Dst: 192.168.190.129					
Transmission Control Protocol,	Src Port: 80, Dst Port: 38268, Seq: 1, Ack: 378, Len: 438					
Hypertext Transfer Protocol						
	HTTP/1.1 200 OK\r\n					
	Date: Fri, 19 Mar 2021 08:15:37 GMT\r\n					
	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n					
	Last-Modified: Fri, 19 Mar 2021 05:59:01 GMT\r\n					
	ETag: "51-5bddd69a76b76"\r\n					
	Accept-Ranges: bytes\r\n					
	Content-Length: 81\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 1/1]					
	[Time since request: 0.151995622 seconds]					
	[Request in frame: 10]					
	[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]					
	File Data: 81 bytes					
	Line-based text data: text/html (3 lines)					

Wireshark Lab: HTTP

.1

א. HTTP 1.1

ניתן לראות את גרסת ה-HTTP של הדף שולחן תחת הודעת ה-GET שהדפסן שולח:

The screenshot shows a Wireshark capture window with the following details:

- Protocol:** http
- Frame 85:** 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits) on interface ens33, id 0
 - Ethernet II, Src: VMware_eb:f6:dd (00:0c:29:eb:f6:dd), Dst: VMware_e6:94:d4 (00:50:56:e6:94:d4)
 - Internet Protocol Version 4, Src: 192.168.190.129, Dst: 128.119.245.12
 - Transmission Control Protocol, Src Port: 38290, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
- HyperText Transfer Protocol:**
 - GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 - Host: gaia.cs.umass.edu\r\n
 - User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
- [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]**
- [HTTP request 1/1]**
- [Response in frame: 89]**

ב. HTTP 1.1

ניתן לראות את גרסת ה-HTTP של הסרבר תחת תגובת הרשות להודעת ה-GET שהדפסן שולח:

The screenshot shows a Wireshark capture window with the following details:

- Protocol:** http
- Frame 85:** 430 bytes on wire (3420 bits), 430 bytes captured (3420 bits) on interface ens33, id 0
 - Ethernet II, Src: VMware_e6:94:d4 (00:50:56:e6:94:d4), Dst: VMware_eb:f6:dd (00:0c:29:eb:f6:dd)
 - Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.190.129
 - Transmission Control Protocol, Src Port: 80, Dst Port: 38290, Seq: 1, Ack: 377, Len: 486
- HyperText Transfer Protocol:**
 - HTTP/1.1 200 OK\r\n
 - Date: Fri, 19 Mar 2021 08:26:23 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
 - Last-Modified: Fri, 19 Mar 2021 05:59:01 GMT\r\n
 - ETag: "80-5bddde9a7a27"\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
- [HTTP response 1/1]**
- [Time since request: 0.160434944 seconds]**
- [Request in frame 85]**

.2

הדף שלנו מצין שהוא מקבל את השפה האנגלית.en-US.
ניתן לראות זאת תחת הودעת HTTP GET שהדף שלח.

No.	Time	Source	Destination	Protocol	Length	Info
+ 85	01:26:23.129525915	192.168.190.129	128.119.245.12	HTTP	430	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
+ 89	01:26:23.289960859	128.119.245.12	192.168.190.129	HTTP	540	HTTP/1.1 200 OK (text/html)
+ 99	01:26:23.387373118	192.168.190.129	128.119.245.12	HTTP	387	GET /favicon.ico HTTP/1.1
101	01:26:23.544234824	128.119.245.12	192.168.190.129	HTTP	539	HTTP/1.1 404 Not Found (text/html)

```

> Frame 85: 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits) on interface ens33, id 0
> Ethernet II, Src: VMware_eb:f6:dd (00:0c:29:eb:f6:dd), Dst: VMware_e6:94:d4 (00:50:56:e6:94:d4)
> Internet Protocol Version 4, Src: 192.168.190.129, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 38290, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
> Hypertext Transfer Protocol
>   GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 89]
```

.3

כתובת המחשב שלנו: 192.168.190.129
כתובת השרת: 128.119.245.12

תחת הודעת HTTP GET ניתן לראות בשדה "Internet Protocol" את הכתובת של המחשב שלנו (Source) שנשלחת ע"י הדף והכתובת של השרת (Destination) התואם לשם הכתובת הנתונה כפי שניתן לראות תחת שדה ה-"Host".

No.	Time	Source	Destination	Protocol	Length	Info
+ 85	01:26:23.129525915	192.168.190.129	128.119.245.12	HTTP	430	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
+ 89	01:26:23.289960859	128.119.245.12	192.168.190.129	HTTP	540	HTTP/1.1 200 OK (text/html)
+ 99	01:26:23.387373118	192.168.190.129	128.119.245.12	HTTP	387	GET /favicon.ico HTTP/1.1
101	01:26:23.544234824	128.119.245.12	192.168.190.129	HTTP	539	HTTP/1.1 404 Not Found (text/html)

```

> Frame 85: 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits) on interface ens33, id 0
> Ethernet II, Src: VMware_eb:f6:dd (00:0c:29:eb:f6:dd), Dst: VMware_e6:94:d4 (00:50:56:e6:94:d4)
> Internet Protocol Version 4, Src: 192.168.190.129, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 38290, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
> Hypertext Transfer Protocol
>   GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 89]
```

.4

סיטוטו הקוד והביטוי אוטם שלח השרת הינט OK: 200 כפי שניתן לראות בהודעה שקיבלו מהשרת:

No.	Time	Source	Destination	Protocol	Length	Info
85	01:26:23.129525915	192.168.190.129	128.119.245.12	HTTP	430	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
89	01:26:23.289960859	128.119.245.12	192.168.190.129	HTTP	540	HTTP/1.1 200 OK (text/html)
99	01:26:23.387373118	192.168.190.129	128.119.245.12	HTTP	387	GET /favicon.ico HTTP/1.1
101	01:26:23.544234824	128.119.245.12	192.168.190.129	HTTP	539	HTTP/1.1 404 Not Found (text/html)

```

> Frame 89: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface ens33, id 0
> Ethernet II, Src: VMware_e6:94:d4 (00:50:56:e6:94:d4), Dst: VMware_eb:f6:dd (00:0c:29:eb:f6:dd)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.190.129
> Transmission Control Protocol, Src Port: 80, Dst Port: 38290, Seq: 1, Ack: 377, Len: 486
> Hypertext Transfer Protocol
  > HTTP/1.1 200 OK
    Date: Fri, 19 Mar 2021 08:26:23 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 19 Mar 2021 05:59:01 GMT\r\n
    ETag: "80-5bddd69a7a227"\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 1/1]
  [Time since request: 0.160434944 seconds]
  [Document in frame: 0]

```

.5

קובץ HTML שקיבלו מהשרת שונה בתאריך 05:59:01 19.03.2021 כפי שניתן לראות בדף "Last-Modified" תחת ההודעה שקיבלו מהשרת.

No.	Time	Source	Destination	Protocol	Length	Info
85	01:26:23.129525915	192.168.190.129	128.119.245.12	HTTP	430	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
89	01:26:23.289960859	128.119.245.12	192.168.190.129	HTTP	540	HTTP/1.1 200 OK (text/html)
99	01:26:23.387373118	192.168.190.129	128.119.245.12	HTTP	387	GET /favicon.ico HTTP/1.1
101	01:26:23.544234824	128.119.245.12	192.168.190.129	HTTP	539	HTTP/1.1 404 Not Found (text/html)

```

> Frame 89: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface ens33, id 0
> Ethernet II, Src: VMware_e6:94:d4 (00:50:56:e6:94:d4), Dst: VMware_eb:f6:dd (00:0c:29:eb:f6:dd)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.190.129
> Transmission Control Protocol, Src Port: 80, Dst Port: 38290, Seq: 1, Ack: 377, Len: 486
> Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 19 Mar 2021 08:26:23 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 19 Mar 2021 05:59:01 GMT\r\n
    ETag: "80-5bddd69a7a227"\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 1/1]
  [Time since request: 0.160434944 seconds]
  [Document in frame: 0]

```

.6

גודל התוכן שקיבלנו מהשרת הוא 128 ביטים כפי שניתן לראות תחת שדה ה"File Data" תחת ההודעה שקיבלנו מהשרת.

.7

לא. הנתונים הגלמים תואמים לבדוק למה שמוצג בחלון רישום החבילות
(הנתונים ברישום החבילות הם "תצוגה מסווגת" של הנתונים גלמים שהתקבלו)

.8

בהודעת ה-HTTP לא מופיע השדה "IF-MODIFIED-SINCE"

.9

ניתן לראות את תוכן הקובץ במפורש ובאופן קרייא בתגובה השירות:

Content-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1]\n[Time since request: 0.147176547 seconds]\n[Request in frame: 13]\n[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]\nFile Data: 371 bytes

- Line-based text data: text/html (10 lines)

```

<html>
<head>
<title>Congratulations!</title>
</head>
<body>
<p>Congratulations again! Now you've downloaded the file lab2-2.html. <br>
This file's last modification date will not change. <br>
Thus if you download this multiple times on your browser, a complete copy <br>
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>
field in your browser's HTTP GET request to the server.<br>
</p>
</body>
</html>
```

0060 3a 33 33 3a 32 38 20 47 4d 54 0d 0a 53 65 72 76 :13:28 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36
0080 29 28 43 65 66 74 4f 53 29 20 4f 70 65 6e 53 53
0090 4c 2f 31 26 30 2e 32 6b 2d 66 69 70 73 20 50 48
00a0 50 2f 37 2e 34 2e 31 34 20 6d 6f 64 5f 70 65 72
00b0 6c 2f 32 2e 30 2e 31 31 20 56 65 72 6c 2f 76 35
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69

:13:28 G MT..Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3 ast-Modi

.10

כ, השדה "IF-MODIFIED-SINCE" מופיע.

הזמן הנמצא תחת הכותרת "IF-MODIFIED-SINCE" מיצג את תאריך השני האחרון של הקובץ אותו הורדנו כ שניגשנו לאחרונה לאתר.

> Transmission Control Protocol, Src Port: 38304, Dst Port: 80, Seq: 334, Ack: 486, Len: 488

- 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 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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: Fri, 19 Mar 2021 05:59:01 GMT\r\n

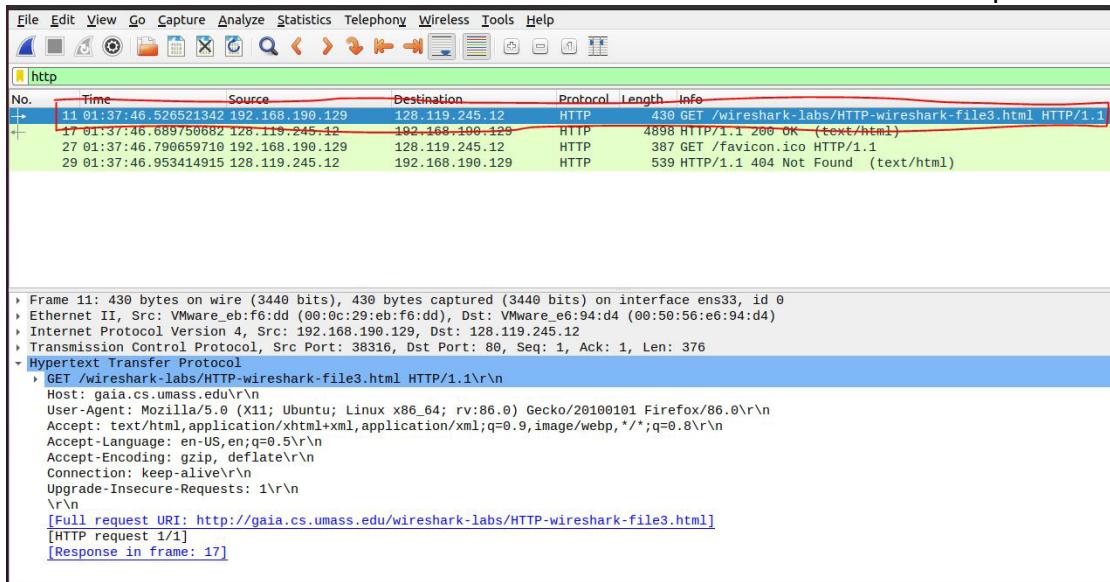
If-None-Match: "173-5bdd69a70207"\r\n
 Cache-Control: max-age=0\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
 [HTTP request 2/2]
 [Prev request in frame: 29]
 [Response in frame: 55]

.11

טיטויס קוד ה-HTTP והבטויו שהתקבל בהודעת השירות הוא 304: Not Modified. מאחר והקובץ לא שונה זמן השינוי של הקובץ המקורי במתਮן אז השירות לא יציג את תוכן האתר כי הדף נטען את האתר מהמתמן (אין הבדל בין הקבצים ולכן נטען את הקובץ מהמתמן). אם הקובץ שונה, השירות יציג את הקובץ העדכני כך שהדף נטען מחדש את הקובץ העדכני.)

.12

עבור התוכן של Bill or Rights הדפדן שלח הודעה HTTP GET אחת.
מספר הפקטה הינו 11.



```

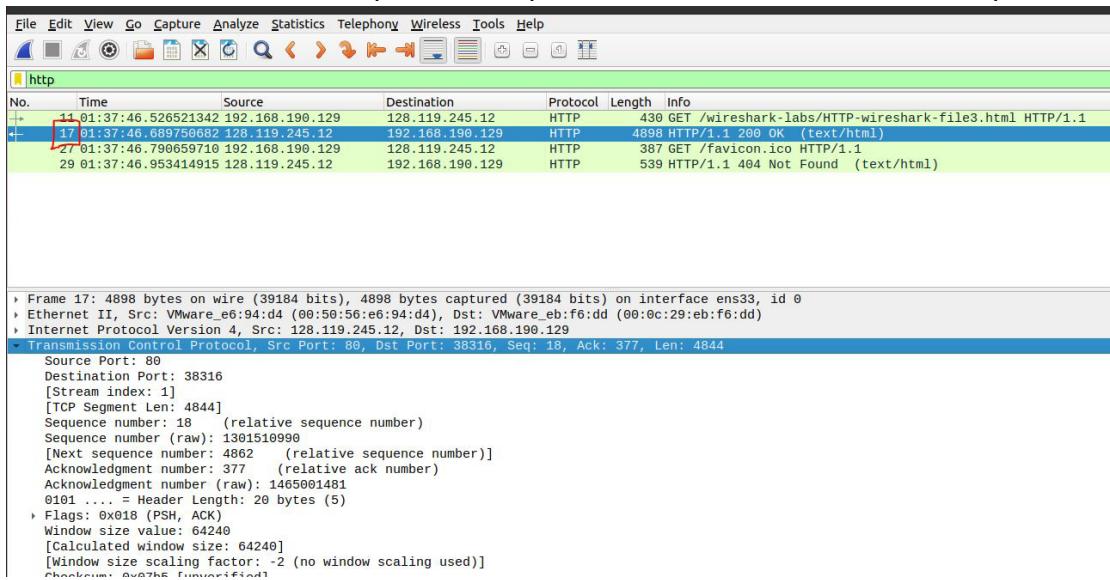
No. Time Source Destination Protocol Length Info
11 01:37:46.526521342 192.168.190.129 128.19.245.12 HTTP 430 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+- 17 01:37:46.689759682 128.19.245.12 192.168.190.129 HTTP 4898 HTTP/1.1 200 OK (text/html)
27 01:37:46.790659710 192.168.190.129 128.19.245.12 HTTP 387 GET /favicon.ico HTTP/1.1
29 01:37:46.953414915 128.19.245.12 192.168.190.129 HTTP 539 HTTP/1.1 404 Not Found (text/html)

> Frame 11: 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits) on interface ens33, id 0
> Ethernet II, Src: VMWare_eb:f6:dd (00:0c:29:eb:f6:dd), Dst: VMWare_e6:94:d4 (00:50:56:e6:94:d4)
> Internet Protocol Version 4, Src: 192.168.190.129, Dst: 128.19.245.12
> Transmission Control Protocol, Src Port: 38316, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
- Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
  [HTTP request 1/1]
  [Response in frame: 17]

```

.13

מספר הפקטה של הודעה השרת הינו 17 וסטטוס הקוד והbattleio שקיבלו מהשרת הינם OK.



```

No. Time Source Destination Protocol Length Info
11 01:37:46.526521342 192.168.190.129 128.19.245.12 HTTP 430 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
+- 17 01:37:46.689759682 128.19.245.12 192.168.190.129 HTTP 4898 HTTP/1.1 200 OK (text/html)
27 01:37:46.790659710 192.168.190.129 128.19.245.12 HTTP 387 GET /favicon.ico HTTP/1.1
29 01:37:46.953414915 128.19.245.12 192.168.190.129 HTTP 539 HTTP/1.1 404 Not Found (text/html)

> Frame 17: 4898 bytes on wire (39184 bits), 4898 bytes captured (39184 bits) on interface ens33, id 0
> Ethernet II, Src: VMWare_e6:94:d4 (00:50:56:e6:94:d4), Dst: VMWare_eb:f6:dd (00:0c:29:eb:f6:dd)
> Internet Protocol Version 4, Src: 128.19.245.12, Dst: 192.168.190.129
> Transmission Control Protocol, Src Port: 80, Dst Port: 38316, Seq: 18, Ack: 377, Len: 4844
  Source Port: 80
  Destination Port: 38316
  [Stream index: 1]
  [TCP Segment Len: 4844]
  Sequence number: 18 (relative sequence number)
  Sequence number (raw): 1301510990
  [Next sequence number: 4862 (relative sequence number)]
  Acknowledgment number: 377 (relative ack number)
  Acknowledgment number (raw): 1465001481
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window size value: 64240
  [Calculated window size: 64240]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x07E5 [Unverified]

```

.14

הסטטוס קוד והbattleio הינם OK כי שמצוין בתמונה לעיל תחת הטאב של "Info" בפקטה 17.

.15

מספר קטעי ה-TCP המכילים את הנתונים הנדרשים בצד לשאת את ה-HTTP היחיד הוא 2 כפי שמוסמן בתמונה:

Frame 17: 4898 bytes on wire (39184 bits), 4898 bytes captured (39184 bits) on interface ens33, id 0
 Ethernet II, Src: VMware_e6:94:d4 (00:50:56:e6:94:d4), Dst: VMware_eb:f6:dd (00:0c:29:eb:f6:dd)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.190.129
 Transmission Control Protocol, Src Port: 80, Dst Port: 38316, Seq: 18, Ack: 377, Len: 4844
 [2 Reassembled TCP Segments (4861 bytes): #15(17), #17(4844)]
 [Frame: 15, payload: 0-16 (17 bytes)]
 [Frame: 17, payload: 17-4860 (4844 bytes)]
 [Segment count: 2]
 [Reassembled TCP length: 4861]
 [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2046...]
 Hypertext Transfer Protocol
 Line-based text data: text/html (98 lines)

.16

הדף שלח 3 הודעות GET HTTP.

ניתן לראות לאיזה כתובות אטרים נשלחו הודעות אלו תחת הטאב "Destination" בחולון הפקחות:

.128.119.245.12 .המודעה הראשונה נשלחה לכתובת 128.119.245.12

.128.119.245.12 .המודעה השנייה נשלחה לכתובת 128.119.245.12

.178.79.137.164 .המודעה השלישית נשלחה לכתובת 178.79.137.164

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Length Info

5 15:25:48.816934000 192.168.190.129 128.119.245.12 HTTP 43 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 9 15:25:49.090025700 128.119.245.12 192.168.190.129 HTTP 1355 HTTP/1.1 200 OK (text/html)
 11 15:25:49.090923290 192.168.190.129 128.119.245.12 HTTP 387 GET /pearson.png HTTP/1.1
 16 15:25:49.084930295 192.168.190.129 178.79.137.164 HTTP 391 GET /BE_cover_small.jpg HTTP/1.1
 18 15:25:49.164598164 178.79.137.164 192.168.190.129 HTTP 225 HTTP/1.1 301 Moved Permanently
 23 15:25:49.191377722 128.119.245.12 192.168.190.129 HTTP 3321 HTTP/1.1 200 OK (PNG)
 29 15:25:49.293163927 192.168.190.129 128.119.245.12 HTTP 387 GET /favicon.ico HTTP/1.1
 37 15:25:49.470072558 128.119.245.12 192.168.190.129 HTTP 538 HTTP/1.1 404 Not Found (text/html)

[Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0xf640 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 > [SEQ/ACK analysis]
 > [Timestamps]
 TCP payload (376 bytes)
 Hypertext Transfer Protocol
 > GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]

.17

נשים לב כי בקשת תמונה ה-PNG מהשרת הינה בפקטה מס' 11 ובקשת תמונה ה-JPG הינה בפקטה מס' 16.
 הרשות החזיר הودעה עבור תמונה ה-JPG בפקטה מס' 18 לפני שהשרות החזיר הודעה עבור תמונה ה-PNG. והרי הודעתה ה-HTTP GET עברו תמונה ה-PNG נשלחה ראשונה.
 לעומת זאת, הדף הורד את התמונות במקביל ולא באופן סדרתי כיוון שאם היה מוריד באופן סדרתי אז הדף היה אמר להוריד את תמונה ה-JPG רק לאחר שתמונה ה-PNG תתקבל.

No.	Time	Source	Destination	Protocol	Length	Info
5	15:25:48.816934005	192.168.190.129	128.119.245.12	HTTP	430	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
9	15:25:48.990025789	128.119.245.12	192.168.190.129	HTTP	1355	HTTP/1.1 200 OK (text/html)
11	15:25:49.009023295	192.168.190.129	128.119.245.12	HTTP	387	GET /pearson.png HTTP/1.1
16	15:25:49.084930295	192.168.190.129	178.79.137.164	HTTP	394	GET /8E_cover_small.jpg HTTP/1.1
18	15:25:49.164598104	178.79.137.164	192.168.190.129	HTTP	225	HTTP/1.1 301 Moved Permanently
23	15:25:49.191377722	128.119.245.12	192.168.190.129	HTTP	3321	HTTP/1.1 200 OK (PNG)
29	15:25:49.293163927	192.168.190.129	128.119.245.12	HTTP	387	GET /favicon.ico HTTP/1.1
37	15:25:49.470072558	128.119.245.12	192.168.190.129	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```

Frame 11: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits) on interface ens33, id 0
Ethernet II, Src: VMware_eb:f6:dd (00:0c:29:eb:f6:dd), Dst: VMware_e6:94:d4 (00:50:56:e6:94:d4)
Internet Protocol Version 4, Src: 192.168.190.129, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 35494, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
Hypertext Transfer Protocol

```

- נשים לב כי עברו הקראיה לתמונה ה-JPG השרת החזיר סטטוס קוד 301 בפקטה מס' 18 עם כתובת חדשה בפרוטוקול HTTPS.

No.	Time	Source	Destination	Protocol	Length	Info
5	15:25:48.816934005	192.168.190.129	128.119.245.12	HTTP	430	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
9	15:25:48.990025789	128.119.245.12	192.168.190.129	HTTP	1355	HTTP/1.1 200 OK (text/html)
11	15:25:49.009023295	192.168.190.129	128.119.245.12	HTTP	387	GET /pearson.png HTTP/1.1
16	15:25:49.084930295	192.168.190.129	178.79.137.164	HTTP	394	GET /8E_cover_small.jpg HTTP/1.1
18	15:25:49.164598104	178.79.137.164	192.168.190.129	HTTP	225	HTTP/1.1 301 Moved Permanently
23	15:25:49.191377722	128.119.245.12	192.168.190.129	HTTP	3321	HTTP/1.1 200 OK (PNG)
29	15:25:49.293163927	192.168.190.129	128.119.245.12	HTTP	387	GET /favicon.ico HTTP/1.1
37	15:25:49.470072558	128.119.245.12	192.168.190.129	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```

[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xc15b [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (171 bytes)
Hypertext Transfer Protocol
HTTP/1.1 301 Moved Permanently\r\n
Location: https://kurose.cslash.net/8E_cover_small.jpg\r\n\r\n
Content-Length: 0\r\n\r\n
Date: Tue, 23 Mar 2021 22:25:48 GMT\r\n
Server: lighttpd/1.4.47\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.079667809 seconds]
[Request in frame: 16]
[Request URI: http://kurose.cslash.net/8E_cover_small.jpg]

```

.18

נשים לב כי הודעת HTTP הראשונה לשרת הינה בפקטה 17 ותגובה השרת הינה בפקטה 21.-cut ניתן לומר כי הסטטוס קוד והיבטי אותו החזיר השרת בתגובה להודעת HTTP GET הראשונה הינט 401: Unauthorized כמו שניתן לראות בתמונה תחת הטאב "Info".

```

Frame 21: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface ens33, id 0
Ethernet II, Src: VMware_e6:94:d4 (00:0c:29:eb:f6:dd), Dst: VMware_e6:94:d4 (00:0c:29:eb:f6:dd)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.190.129
Transmission Control Protocol, Src Port: 80, Dst Port: 33140, Seq: 1, Ack: 393, Len: 717
Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Date: Fri, 19 Mar 2021 05:25:33 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  Content-Length: 381\r\n
  [Content length: 381]
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=iso-8859-1\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.159272190 seconds]
  [Request in frame: 17]

```

.19

נשים לב כי הודעת HTTP הראשונה הינה הפקטה מס' 17 והודעת HTTP השנייה הינה בפקטה מס' 82.

הודעת HTTP השנייה של הדף כוללת את השדה Authorization: Basic

```

Frame 82: 505 bytes on wire (4040 bits), 505 bytes captured (4040 bits) on interface ens33, id 0
Ethernet II, Src: VMware_eb:f6:dd (00:0c:29:eb:f6:dd), Dst: VMware_e6:94:d4 (00:0c:29:eb:f6:dd)
Internet Protocol Version 4, Src: 192.168.190.129, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 33144, Dst Port: 80, Seq: 1, Ack: 1, Len: 451
Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
  Authorization: Basic d2lyZXNoYXJrLXN0dWlbnRz0m5ldHdvcmcs=\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
  [HTTP request 1/2]
  [Response in frame: 84]
  [Time since request: 0.021 seconds]

```

נשים לב שבהודעה הראונונה שדה זה אינו מופיע:

No.	Time	Source	Destination	Protocol	Length	Info
17	22:25:33.524469338	192.168.190.129	128.119.245.12	HTTP	446	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
21	22:25:33.683741528	128.119.245.12	192.168.190.129	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
82	22:26:00.313877681	192.168.190.129	128.119.245.12	HTTP	505	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html...
84	22:26:00.477936531	128.119.245.12	192.168.190.129	HTTP	544	HTTP/1.1 200 OK (text/html)
93	22:26:00.736116947	192.168.190.129	128.119.245.12	HTTP	403	GET /favicon.ico HTTP/1.1
99	22:26:00.891642846	128.119.245.12	192.168.190.129	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```

> Frame 17: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface ens33, id 0
> Ethernet II, Src: VMware_eb:f6:dd (00:0c:29:eb:f6:dd), Dst: VMware_e6:94:d4 (00:58:56:e6:94:d4)
> Internet Protocol Version 4, Src: 192.168.190.129, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 33140, Dst Port: 80, Seq: 1, Ack: 1, Len: 392
- Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
  [HTTP request 1/1]
  [Response in frame: 21]

```