בס"ד

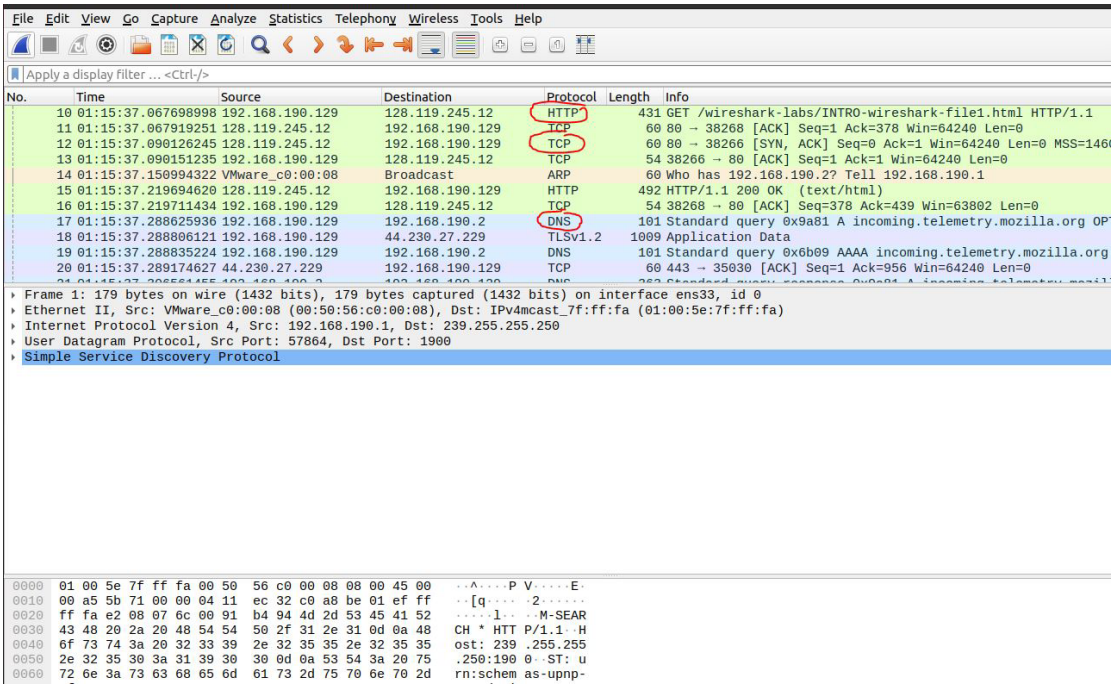
מגיש: [אלמוג יעקב]

מטלה 1 בתקשורת - פתרון

Wireshark Lab: Intro

.1

נבחר את הפרוטוקולים: HTTP, TCP, DNS.

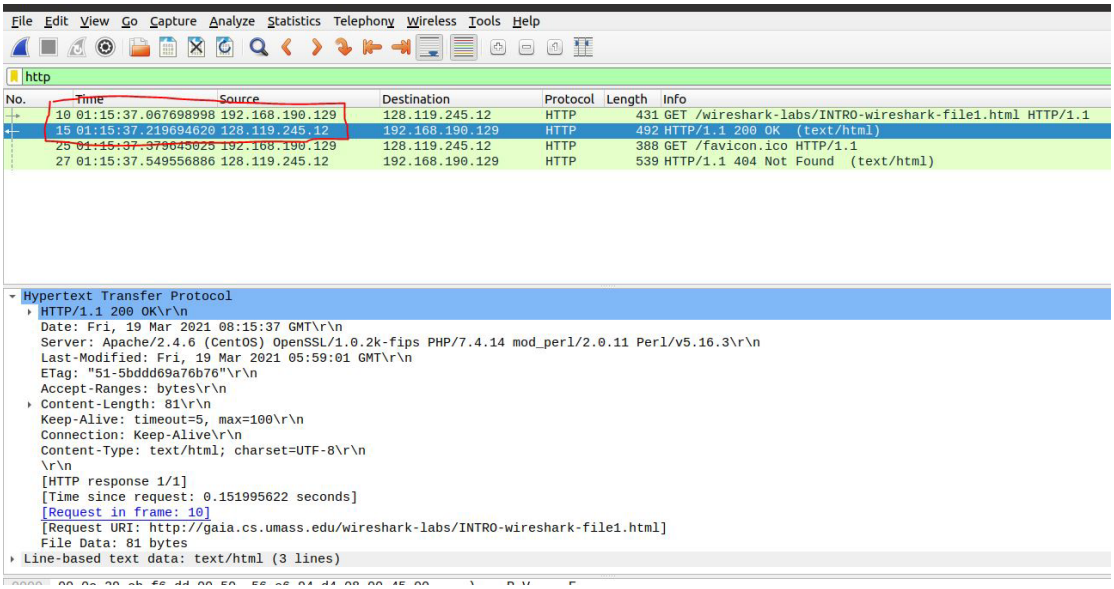


.2

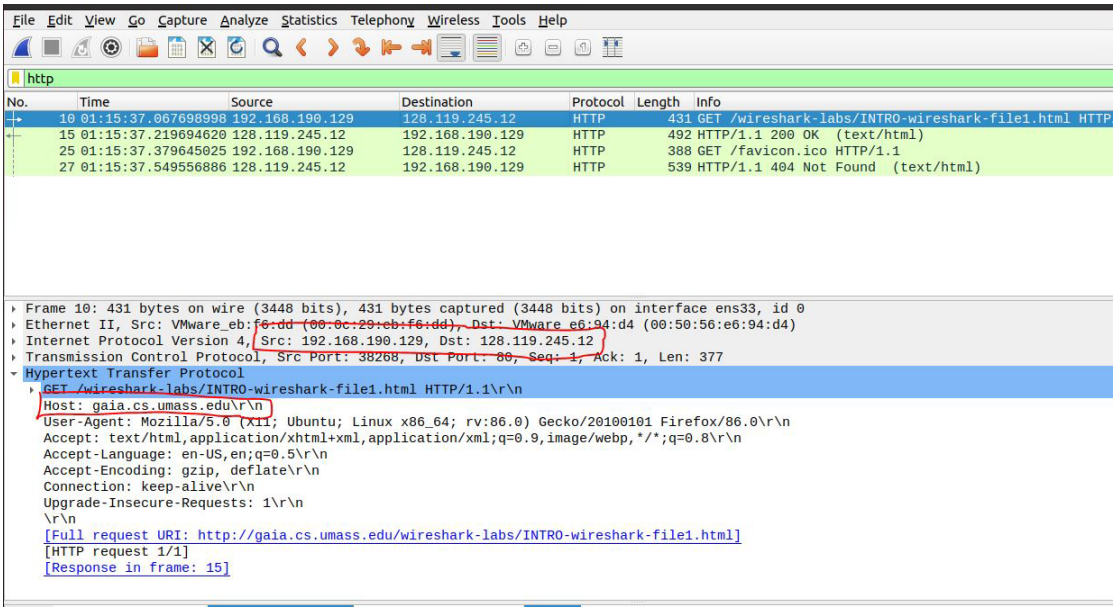
נחסר את הפרש הזמן מזמן הודעת ה-HTTP GET לזמן ההודעה שקיבלנו מהשרת.

כפי שניתן לראות שני ההודעות התבצעו באותה שניה ולכן נותר לחשב את ההפרש בms.

נקבל: 0.219694620-0.067698998 = **0.151995622**.



.3
כתובת המחשב שלנו: 192.168.190.129.
כתובת השרת: 128.119.245.12.
תחת הודעת ה-HTTP GET ניתן לראות בשדה "Internet Protocol" את הכתובת של המחשב שלנו (Source) שנשלחת ע"י הדפדפן ואת הכתובת של השרת (Destination) התואם לשם הכתובת הנתונה כפי שניתן לראות תחת שדה ה-"Host".



.4
פלט הודעות ה-HTTP כפי שהתבקשנו להדפיס בשאלה:

```
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)
```

בס"ד

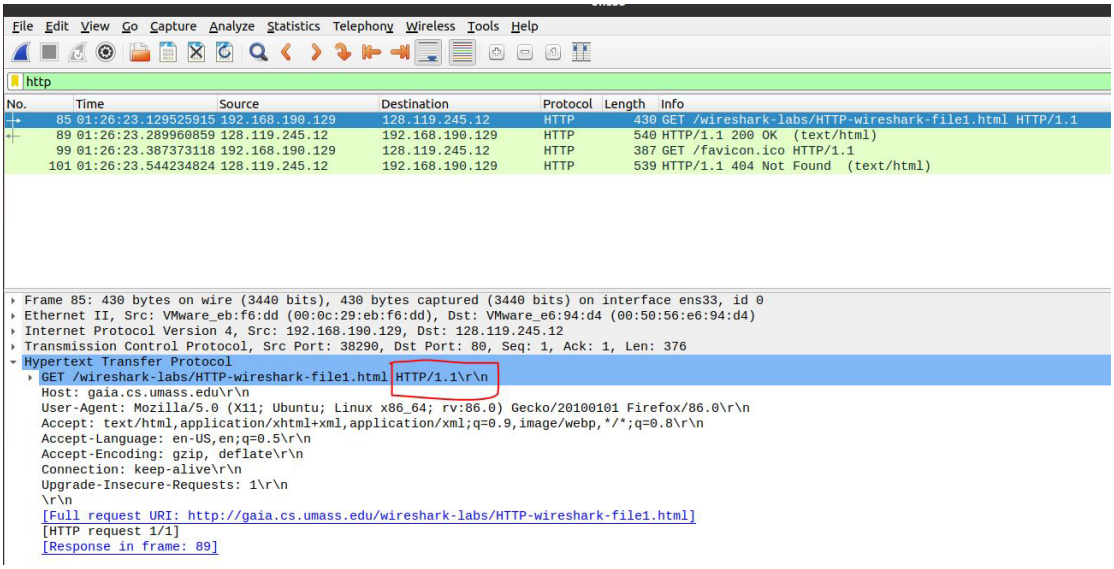
מגיש: [אלמוג יעקב]

Wireshark Lab: HTTP

1.

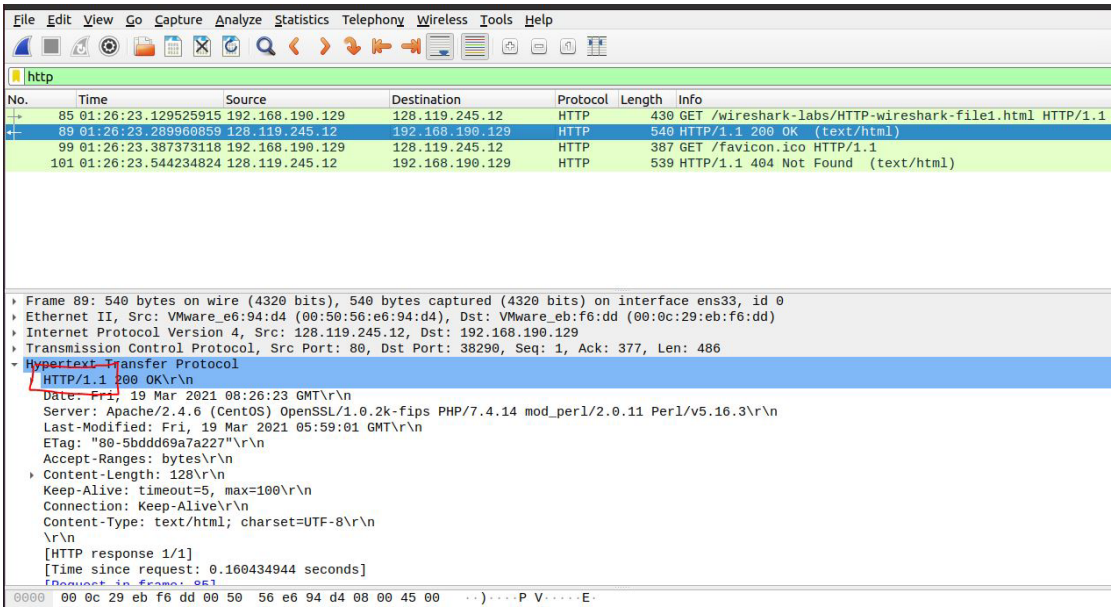
א. HTTP 1.1.

ניתן לראות את גרסת ה-HTTP של הדפדפן שלנו תחת הודעת ה-HTTP GET שהדפדפן שולח:

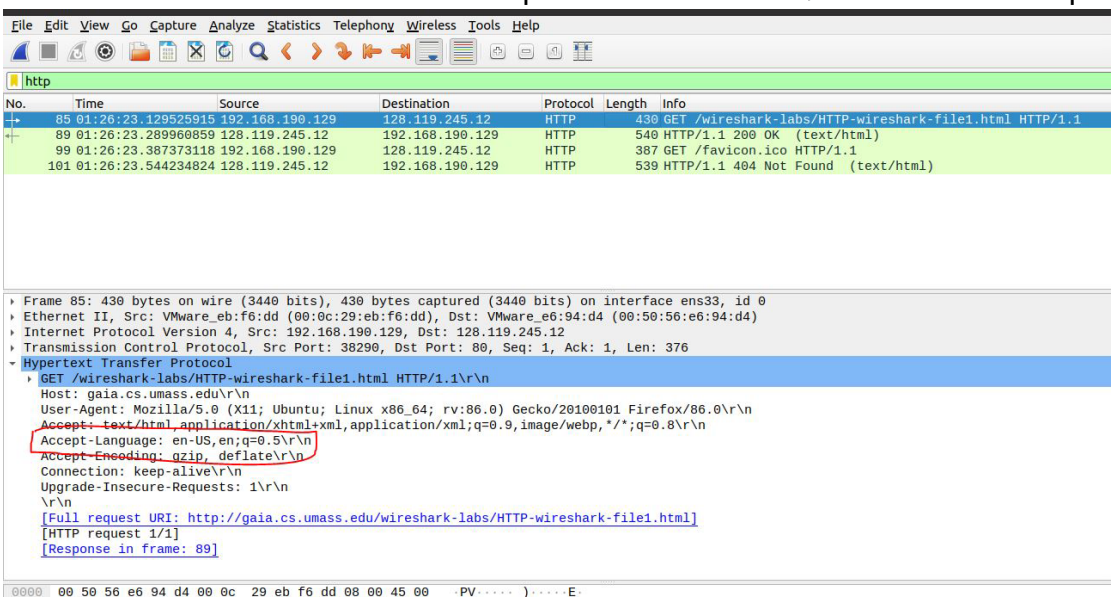


ב. HTTP 1.1.

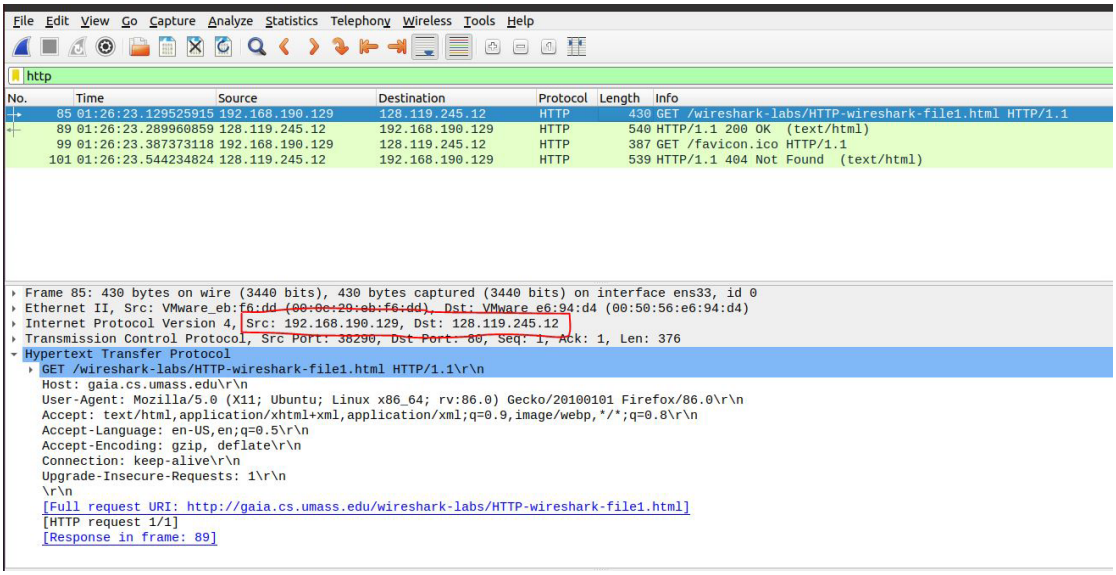
ניתן לראות את גרסת ה-HTTP של הסרבר תחת תגובת השרת להודעת ה-HTTP GET שהדפדפן שלח:



.2
הדפדפן שלנו מציין שהוא מקבל את השפה האנגלית en-US.
ניתן לראות זאת תחת הודעת ה-HTTP GET שהדפדפן שלח.

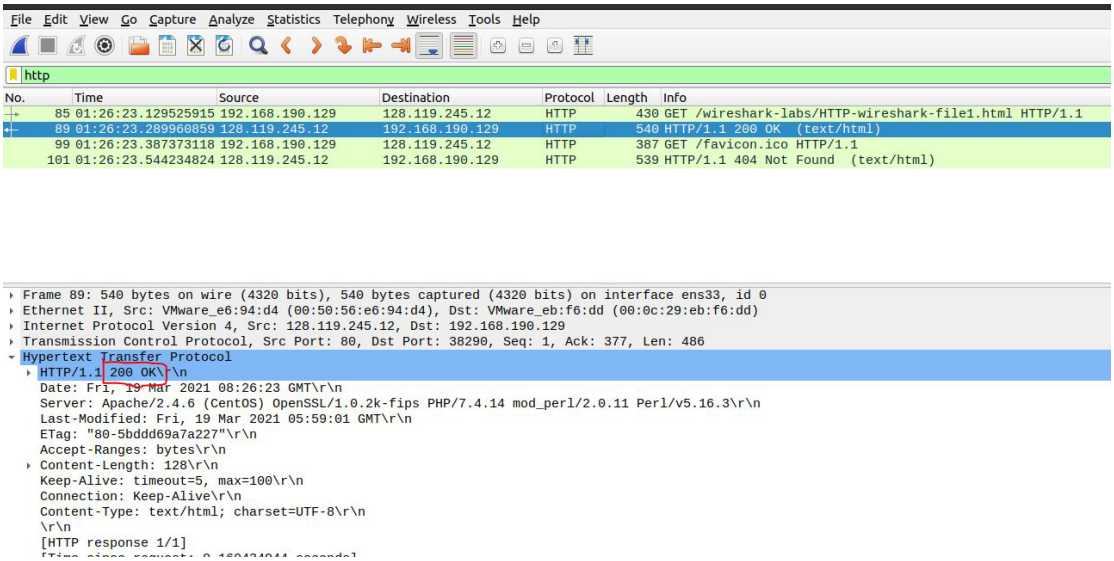


.3
כתובת המחשב שלנו: 192.168.190.129.
כתובת השרת: 128.119.245.12.
תחת הודעת ה-HTTP GET ניתן לראות בשדה "Internet Protocol" את הכתובת של המחשב שלנו (Source) שנשלחת ע"י הדפדפן ואת הכתובת של השרת (Destination) התואם לשם הכתובת הנתונה כפי שניתן לראות תחת שדה ה-"Host".



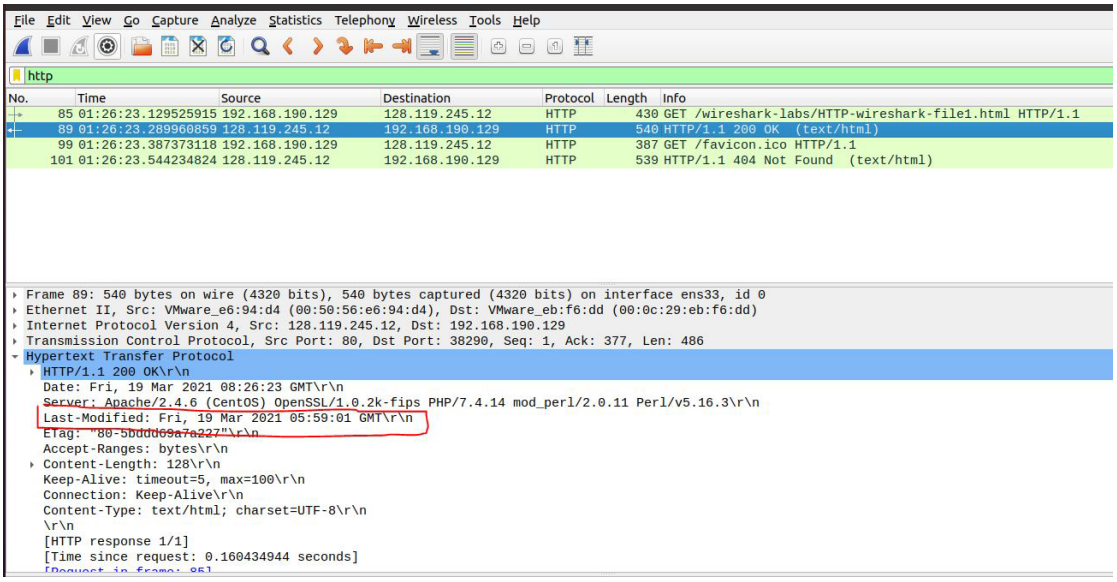
.4

סטטוס הקוד והביטוי אותם שלח השרת הינם 200: OK כפי שניתן לראות בהודעה שקיבלנו מהשרת:



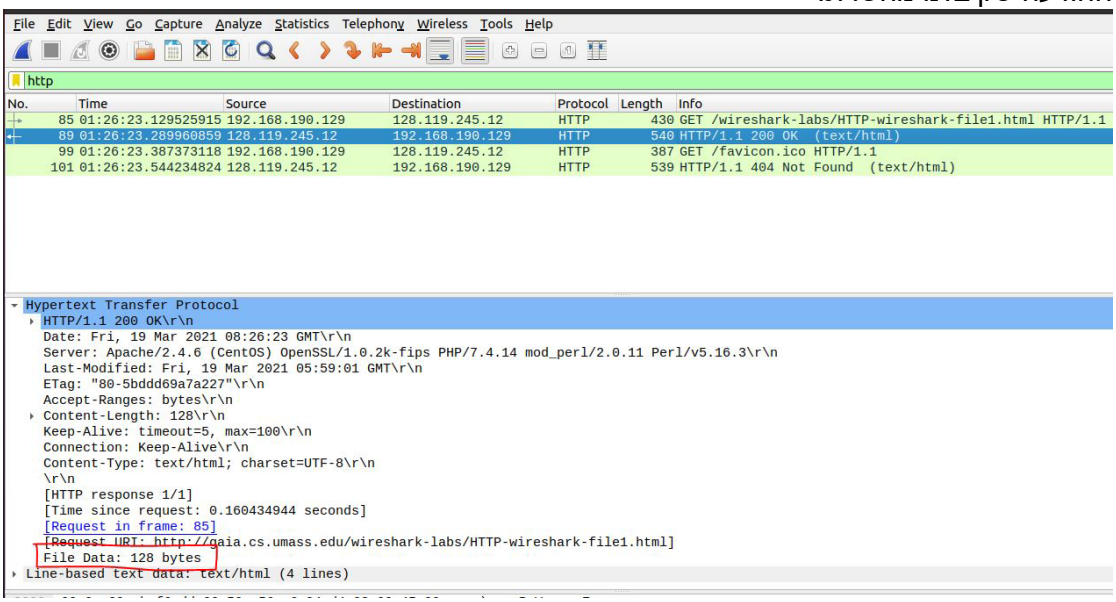
.5

קובץ ה-HTML שקיבלנו מהשרת שונה לאחרונה בתאריך 19.03.2021 05:59:01 כפי שניתן לראות בשדה "Last-Modified" תחת ההודעה שקיבלנו מהשרת.



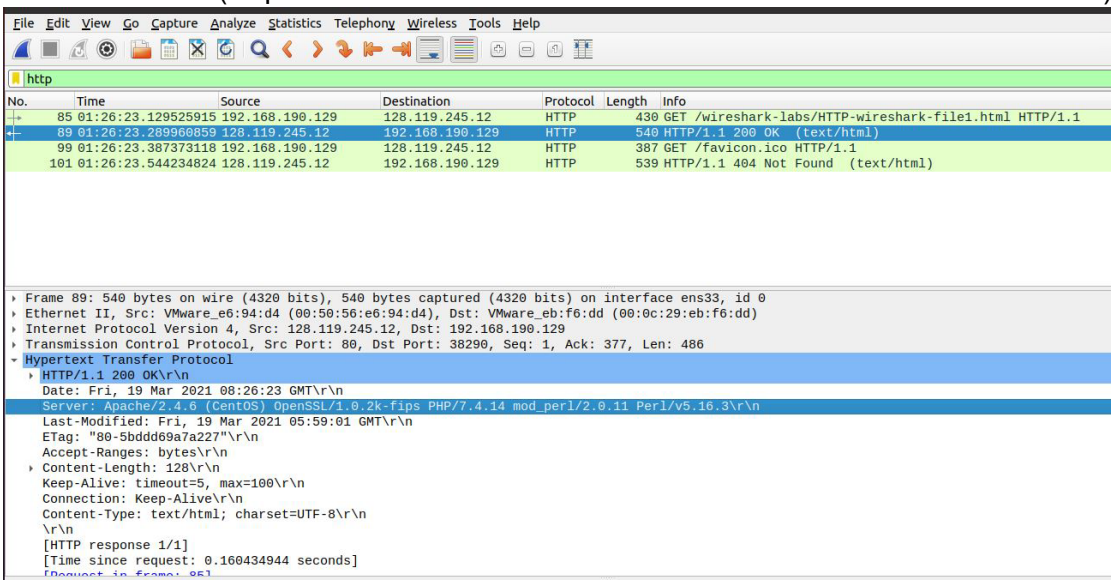
.6

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



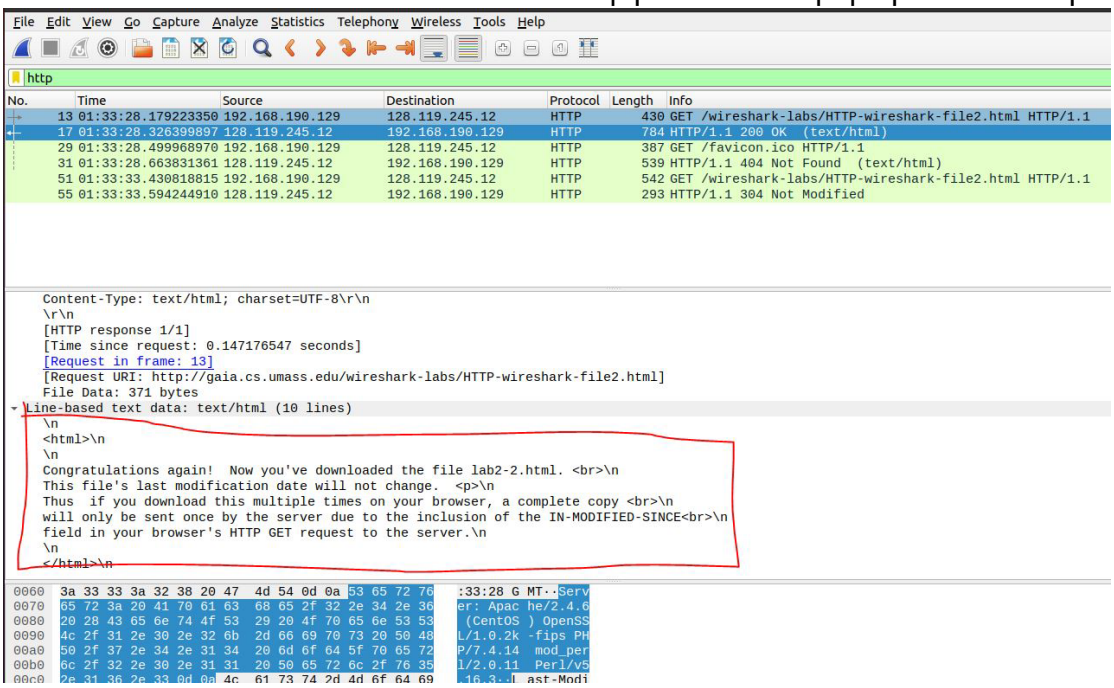
.7

לא. הנתונים הגולמיים תואמים בדיוק למה שמוצג בחלון רישום החבילות
(הנתונים ברישום החבילות הם "תצוגה מסודרת" של הנתונים גולמיים שהתקבלו)

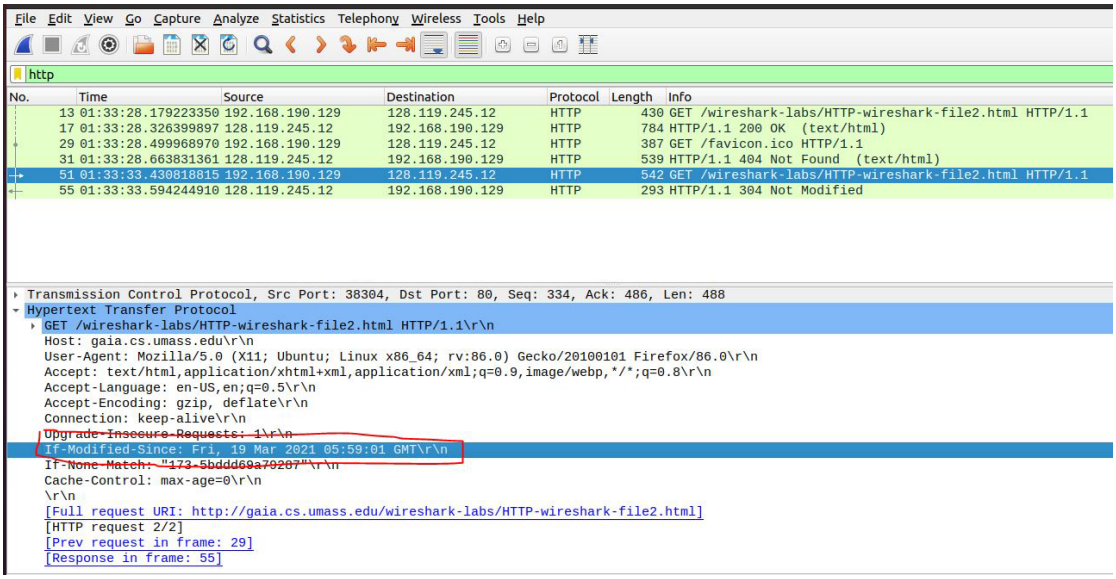


.8
בהודעת ה-HTTP GET לא מופיע השדה "IF-MODIFIED-SINCE".

.9
ניתן לראות את תוכן הקובץ במפורש ובאופן קריא בתגובת השרת:



.10
כן, השדה "IF-MODIFIED-SINCE" מופיע.
הזמן הנמצא תחת הכותרת "IF-MODIFIED-SINCE" מייצג את תאריך השינוי האחרון של הקובץ אותו הורדנו כשניגשנו לאחרונה לאתר.

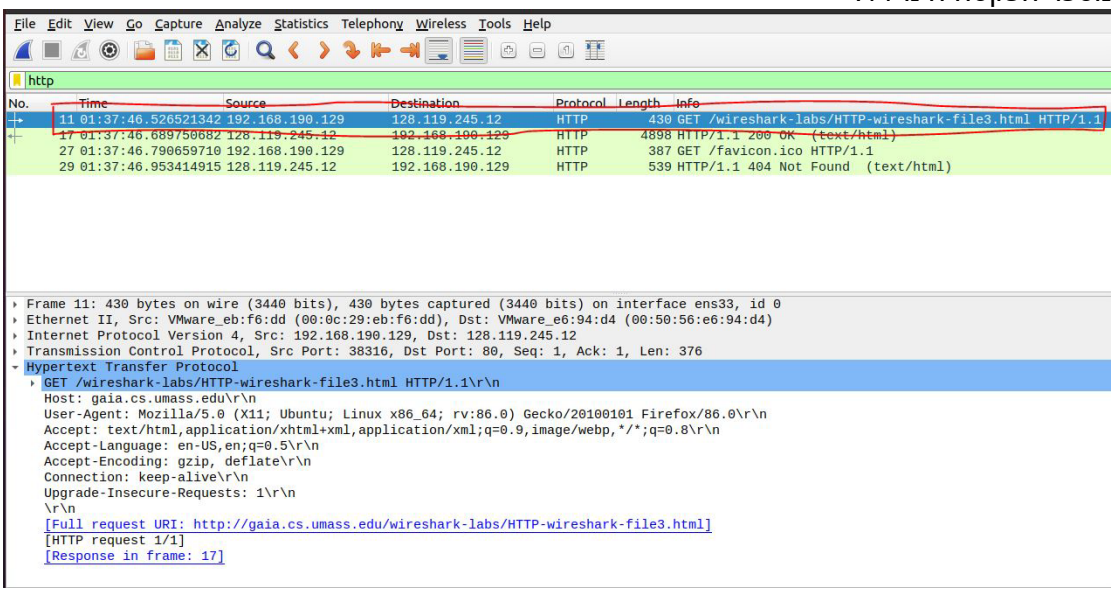


.11
סטטוס קוד ה-HTTP והביטוי שהתקבל בהודעת השרת הוא 304: Not Modified
מאחר והקובץ לא שונה מזמן השינוי של הקובץ הקיים במטמון אז השרת לא יחזיר את תוכן האתר כי הדפדפן יטען את האתר מהמטמון (אין הבדל בין הקבצים ולכן נטען את הקובץ מהמטמון).
(אם הקובץ שונה, השרת יחזיר את הקובץ העדכני כך שהדפדפן יטען מחדש את הקובץ העדכני.).

.12

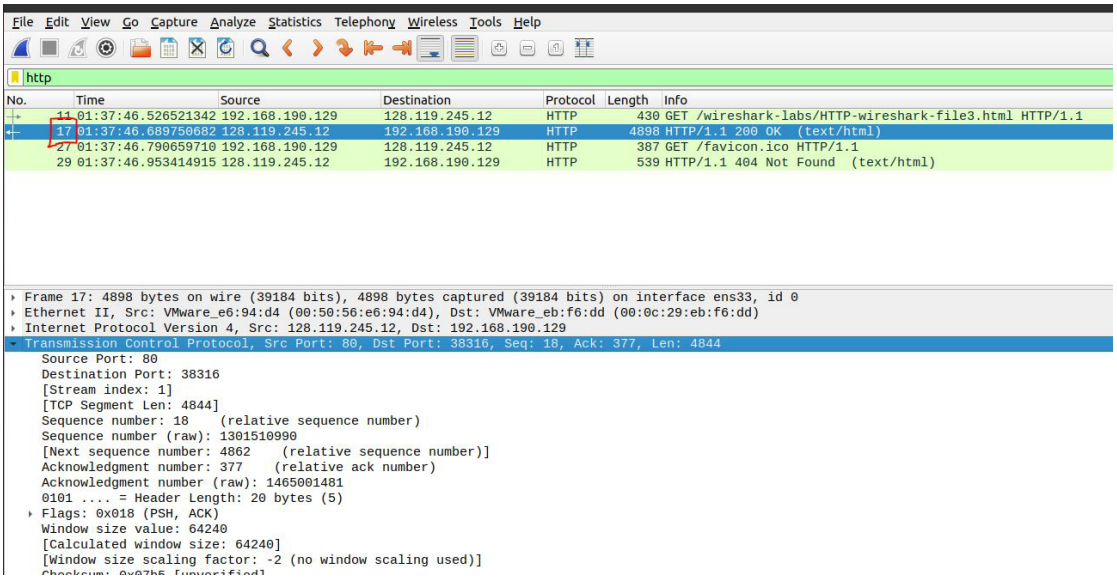
עבור התוכן של Bill or Rights הדפדפן שלח הודעת HTTP GET אחת.

מספר הפקטה הינו 11.



.13

מספר הפקטה של הודעת השרת הינו 17 וסטטוס הקוד והביטוי שקיבלו מהשרת הינם 200: OK.

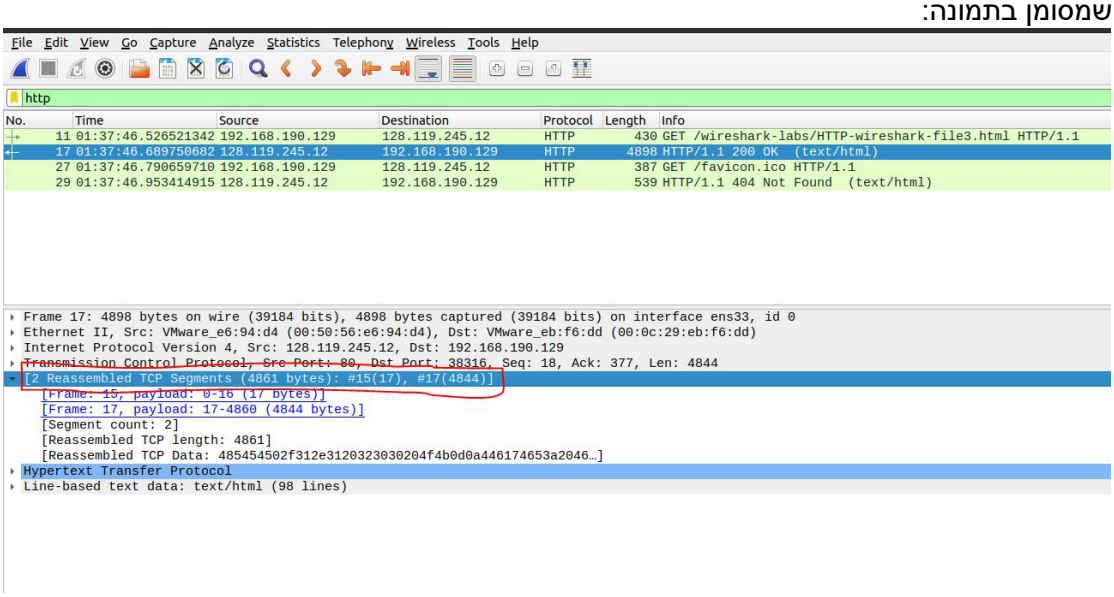


.14

הסטטוס קוד והביטוי הינם 200: OK כפי שמצויין בתמונה לעיל תחת הטאב של "Info" בפקטה מספר 17.

.15

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



.16

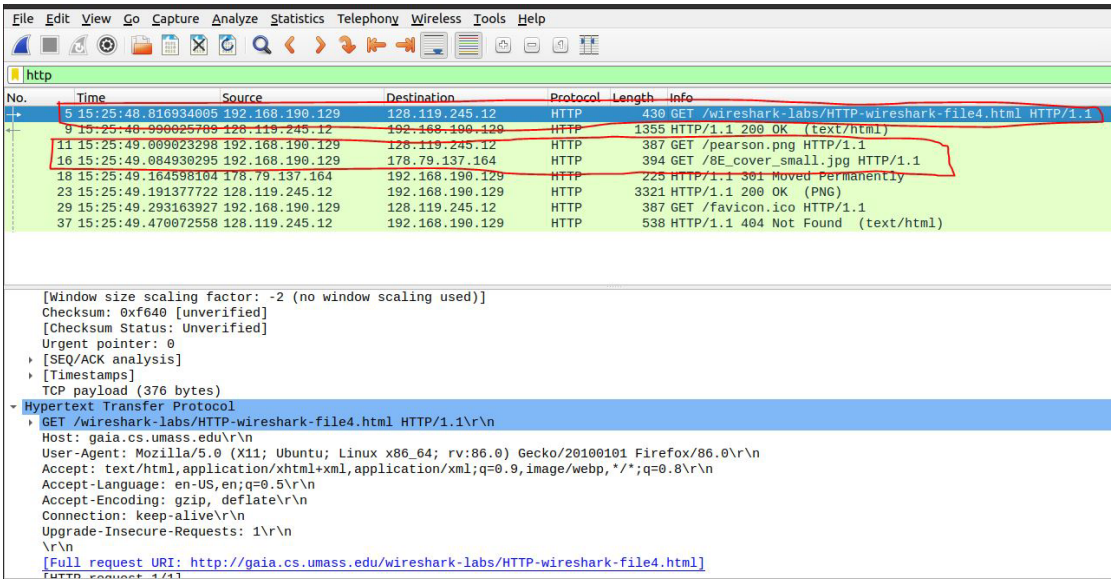
הדפדפן שלח 3 הודעות HTTP GET.

ניתן לראות לאיזה כתובות אתרים נשלחו הודעות אלו תחת הטאב "Destination" בחלון הפקטות:

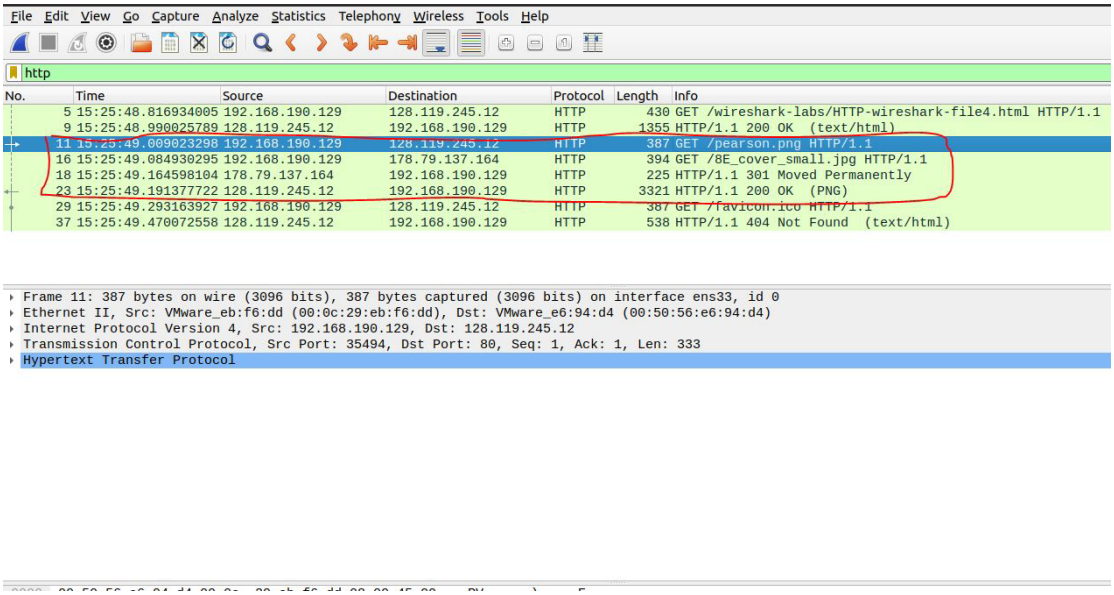
ההודעה הראשונה נשלחה לכתובת 128.119.245.12.

ההודעה השנייה נשלחה לכתובת 128.119.245.12.

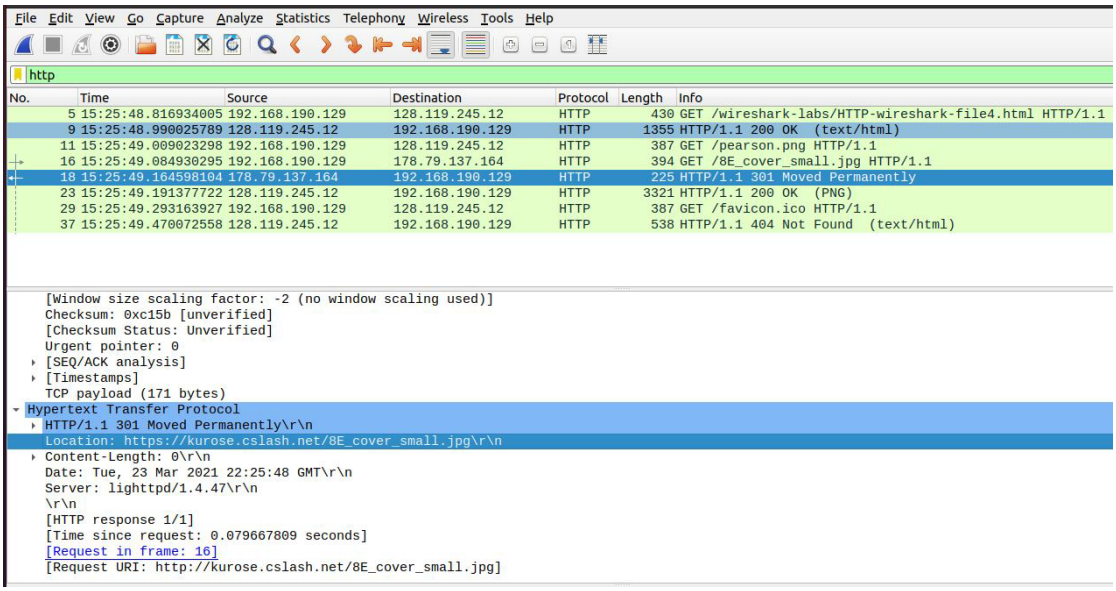
ההודעה השלישית נשלחה לכתובת 178.79.137.164.



.17
נשים לב כי בקשת תמונת ה-PNG מהשרת הינה בפקטה מספר 11 ובקשת תמונת ה-JPG הינה בפקטה מספר 16.
השרת החזיר הודעה עבור תמונת ה-JPG בפקטה מספר 18 לפני שהשרת החזיר הודעה עבור תמונת ה-PNG. והרי הודעת ה-HTTP GET עבור תמונת ה-PNG נשלחה ראשונה.
כלומר, הדפדפן הוריד את התמונות במקביל ולא באופן סדרתי כיוון שאם היה מוריד באופן סדרתי אז הדפדפן היה אמור להוריד את תמונת ה-JPG רק לאחר שתמונת ה-PNG תתקבל.

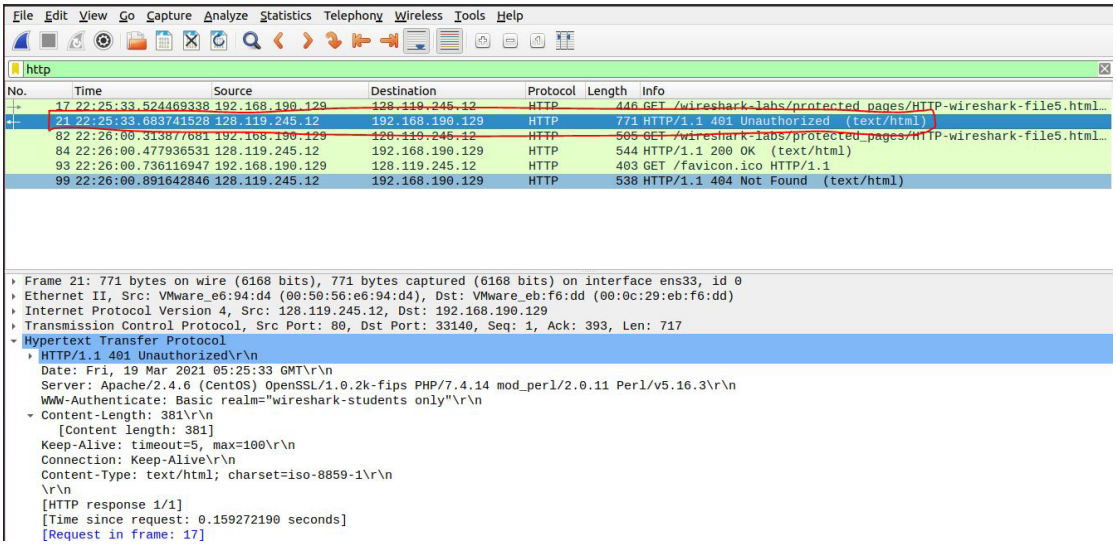


- נשים לב כי עבור הקריאה לתמונת ה-JPG הסרבר החזיר סטטוס קוד 301 בפקטה מספר 18 עם כתובת חדשה בפרוטוקול HTTPS.



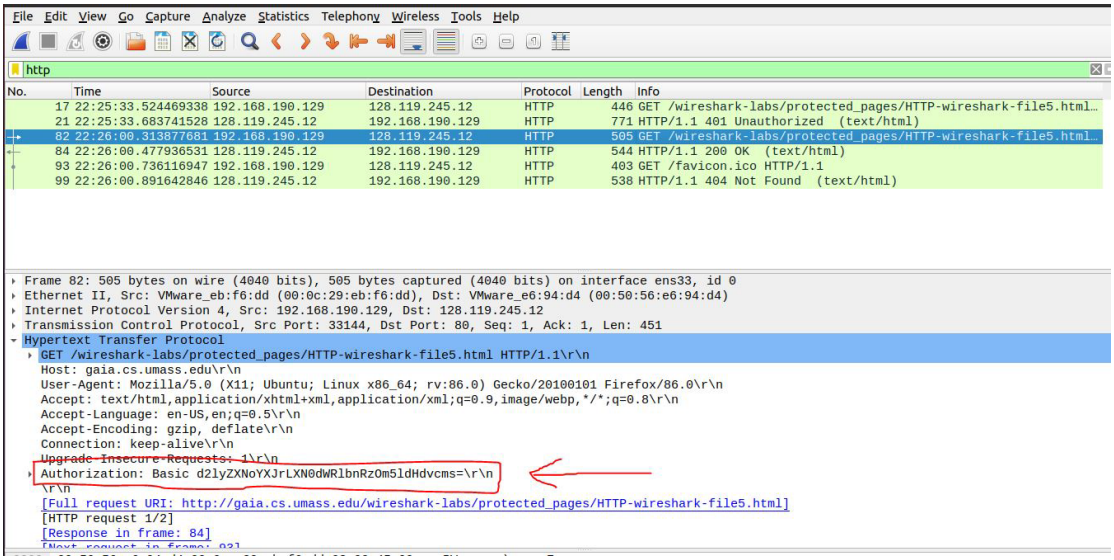
.18

נשים לב כי הודעת ה-HTTP GET הראשונה לשרת הינה בפקטה 17 ותגובת השרת הינה בפקטה 21.
כעת ניתן לומר כי הסטטוס קוד והביטוי אותם החזיר השרת בתגובה להודעת ה-HTTP GET הראשונה הינם 401: Unauthorized כמו שניתן לראות בתמונה תחת הטאב "Info".



.19

נשים לב כי הודעת הHTTP GET הראשונה הינה הפקטה מספר 17 והודעת הHTTP GET השנייה הינה בפקטה מספר 82.
הודעת הHTTP GET השניה של הדפדפן כוללת את השדה Authorization: Basic.



בס"ד

מגיש: [אלמוג יעקב]

נשים לב שבהודעה הראשונה שדה זה אינו מופיע: