בס"ד

תקשורת ומחשוב – מטלה 1

מגישים: חיים גולדפישר 315599563, אור יצחק 208936039

חלק ראשון: Intro

שאלה 1:

3 סוגים שונים של פרוטוקולים שהופיעו: TCP HTTP SSL.

שאלה 2:

לפי הווירשארק , לקח בשנייה:

Time
2022-04-10 16:59:35.612023
2022-04-10 16:59:36.645813

שאלה 3:

נסתכל שוב בווירשארק:

Source	Destination
10.0.0.19	128.119.245.12

הכתובת שלנו: 10.0.0.19

הכתובת של האתר: 128.119.245.12

שאלה 4:

נציג את 2 הפרוטוקולים שהתקבלו לאחר פעולת ההדפסה:

Get:

```
C:\Users\goldi\AppData\Local\Temp\wireshark_Wi-FI00LJK1.pcapng 18196 total packets, 4 shown

No.     Time                           Source                Destination           Protocol Length Info
  12966 2022-04-10 16:59:35.612023     10.0.0.19             128.119.245.12        HTTP     672    GET /wireshark-labs/INTRO-
wireshark-file1.html HTTP/1.1
Frame 12966: 672 bytes on wire (5376 bits), 672 bytes captured (5376 bits) on interface
\Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 0
Ethernet II, Src: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f), Dst: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6)
Internet Protocol Version 4, Src: 10.0.0.19, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 51299, Dst Port: 80, Seq: 1, Ack: 1, Len: 618
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    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/100.0.4896.75 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: en-US,en;q=0.9,he;q=0.8,he-IL;q=0.7,hi;q=0.6\r\n
    If-None-Match: "51-5dc46863dc1ce"\r\n
    If-Modified-Since: Sun, 10 Apr 2022 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 13612]
    [Next request in frame: 14545]
```

Ok:

בס"ד

```
C:\Users\goldi\AppData\Local\Temp\wireshark_Wi-Fi00LJK1.pcapng 18196 total packets, 4 shown

No.     Time                           Source                Destination           Protocol Length Info
  13612 2022-04-10 16:59:36.645813     128.119.245.12        10.0.0.19             HTTP     293    HTTP/1.1 304 Not Modified
Frame 13612: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface
\Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 0
Ethernet II, Src: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6), Dst: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.19
Transmission Control Protocol, Src Port: 80, Dst Port: 51299, Seq: 1, Ack: 619, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Sun, 10 Apr 2022 13:59:37 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-5dc46863dc1ce"\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 1.033790000 seconds]
    [Request in frame: 12966]
    [Next request in frame: 14545]
    [Next response in frame: 14642]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

HTTP חלק שני:

שאלה 1:

נסתכל על פרוטוקול ה"גט":

```
C:\Users\goldi\AppData\Local\Temp\wireshark_Wi-FICC9CK1.pcapng 64940 total packets, 2 shown

No.     Time                           Source                Destination           Protocol Length Info
  41720 2022-04-10 17:44:02.098527     10.0.0.19             128.119.245.12        HTTP     560    GET /wireshark-labs/HTTP-
wireshark-file1.html HTTP/1.1
Frame 41720: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface
\Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 0
Ethernet II, Src: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f), Dst: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6)
Internet Protocol Version 4, Src: 10.0.0.19, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 51489, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
Hypertext Transfer Protocol
```

ניתן לראות שהגרסה היא 1.1

שאלה 2:

שוב נסתכל על הפרוטוקול:

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\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/100.0.4896.75 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: en-US,en;q=0.9,he;q=0.8,he-IL;q=0.7,hi;q=0.6\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: 42250]
```

ניתן לראות שהשפות שהשרת יכול לקבל הן אנגלית-ארה"ב ועברית.

שאלה 3:

כמו במה שעשינו בחלק הקודם:

Source	Destination
10.0.0.19	128.119.245.12

ומכאן שהכתובת שלי היא 10.0.0.19 ושל האתר היא 128.119.245.12.

בס"ד

שאלה 4:

נסתכל בפרוטוקול ה"אוקיי":

```
C:\Users\goldi\AppData\Local\Temp\wireshark_Wi-FiCC9CK1.pcapng 64940 total packets, 2 shown

No.     Time                           Source                Destination           Protocol Length Info
  42250 2022-04-10 17:44:02.787088     128.119.245.12        10.0.0.19             HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 42250: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
\Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 0
Ethernet II, Src: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6), Dst: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.19
Transmission Control Protocol, Src Port: 80, Dst Port: 51489, Seq: 1, Ack: 507, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
```

הקוד שהתקבל הוא 200.

שאלה 5:

נסתכל שוב בפרוטוקול:

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 51489, Seq: 1, Ack: 507, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 10 Apr 2022 14:44:03 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 10 Apr 2022 05:59:01 GMT\r\n
    ETag: "80-5dc46863de10e"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

העדכון האחרון בוצע ביום ראשון ה10.4.2022 בשעה 5:59:01.

שאלה 6:

נסתכל בפרוטוקול:

```
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 10 Apr 2022 14:44:03 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 10 Apr 2022 05:59:01 GMT\r\n
    ETag: "80-5dc46863de10e"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 128\r\n
      [Content length: 128]
```

ניתן לראות שעברו 128 בתים.

שאלה 7:

לא ראיתי כאלו.

שאלה 8:

לא מצאתי הודעה כזאת.

שאלה 9:

כן. נסתכל במה שהופיע על גבי הדפדפן:

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE field in your browser's HTTP GET request to the server.

כעת, נסתכל על מה שהופיע בפרוטוקול ה"אוקיי":

No.	Time	Source	Destination	Protocol	Length	Info
4737	2022-04-10 18:22:39.494709	10.0.0.19	128.119.245.12	HTTP	560	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4917	2022-04-10 18:22:39.740035	128.119.245.12	10.0.0.19	HTTP	784	HTTP/1.1 200 OK (text/html)
6470	2022-04-10 18:22:41.988780	10.0.0.19	128.119.245.12	HTTP	672	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
6578	2022-04-10 18:22:42.159916	128.119.245.12	10.0.0.19	HTTP	293	HTTP/1.1 304 Not Modified

```
> Frame 4917: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{D74F2CB2-932B-4194-89FA-1670BCCC3423}, id 3
> Ethernet II, Src: HeightsT_2d:03:f6 (00:b8:c2:2d:03:f6), Dst: CyberTAN_09:a2:8f (00:45:e2:09:a2:8f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.19
> Transmission Control Protocol, Src Port: 80, Dst Port: 51785, Seq: 1, Ack: 507, Len: 730
> Hypertext Transfer Protocol
v Line-based text data: text/html (10 lines)
    \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
```

כלומר התוכן מופיע בצורה מדויקת בפרוטוקול עצמו.

שאלה 10:

נסתכל בפרוטוקול ה"גט" של הפעם השנייה שפתחנו את הלינק:

```
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    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/100.0.4896.75 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: en-US,en;q=0.9,he;q=0.8,he-IL;q=0.7,hi;q=0.6\r\n
    If-None-Match: "173-5dc46863ddd26"\r\n
    If-Modified-Since: Sun, 10 Apr 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 2/2]
    [Prev request in frame: 4737]
    [Response in frame: 6578]
```

הכותרת הזאת אכן מופיעה כפי שניתן לראות. המידע שמתקבל הינו הפעם האחרונה בה התבצע עדכון (נשים לב שהוא זהה לתאריך שקיבלנו בשאלה 5).

שאלה 11:

נסתכל בפרוטוקול "לא השתנה":

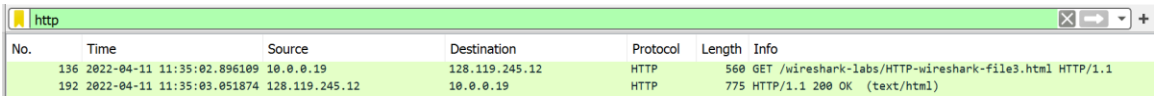
```
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
```

בס"ד

הקוד שהוחזר הוא 304. השרת לא החזיר את התוכן של הקובץ משום שלא בוצע בו שינוי מהפעם הקודמת שהוא התקבל. כלומר במצב זה, אין שום צורך להחזיר שוב את אותו התוכן.

שאלה 12:

נסתכל על רשימת החבילות עם הסינון:

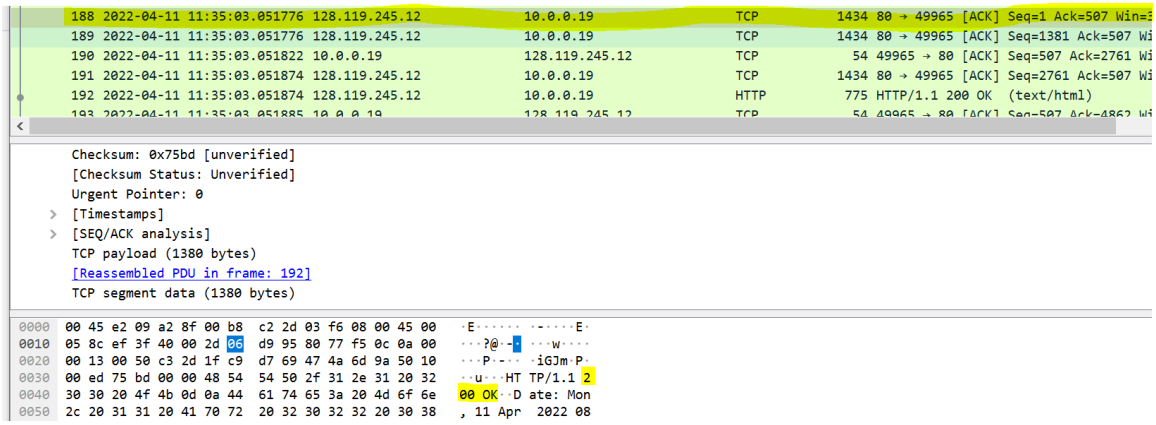


No.	Time	Source	Destination	Protocol	Length	Info
136	2022-04-11 11:35:02.896109	10.0.0.19	128.119.245.12	HTTP	560	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
192	2022-04-11 11:35:03.051874	128.119.245.12	10.0.0.19	HTTP	775	HTTP/1.1 200 OK (text/html)

יש כאן בקשת אחת מסוג "גט". המספר הסידורי של חבילת ה"גט" הוא 136.

שאלה 13:

נסתכל על רשימת החבילות עם הסינון:



188	2022-04-11 11:35:03.051776	128.119.245.12	10.0.0.19	TCP	1434	80 → 49965 [ACK] Seq=1 Ack=507 Win=
189	2022-04-11 11:35:03.051776	128.119.245.12	10.0.0.19	TCP	1434	80 → 49965 [ACK] Seq=1381 Ack=507 Wi
190	2022-04-11 11:35:03.051822	10.0.0.19	128.119.245.12	TCP	54	49965 → 80 [ACK] Seq=507 Ack=2761 Wi
191	2022-04-11 11:35:03.051874	128.119.245.12	10.0.0.19	TCP	1434	80 → 49965 [ACK] Seq=2761 Ack=507 Wi
192	2022-04-11 11:35:03.051874	128.119.245.12	10.0.0.19	HTTP	775	HTTP/1.1 200 OK (text/html)
193	2022-04-11 11:35:03.051885	10.0.0.19	128.119.245.12	TCP	54	49965 → 80 [ACK] Seq=507 Ack=4862 Wi

```
Checksum: 0x75bd [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (1380 bytes)
[Reassembled PDU in frame: 192]
TCP segment data (1380 bytes)
```

```
0000  00 45 e2 09 a2 8f 00 b8  c2 2d 03 f6 08 00 45 00   ·E····· ·-····E·
0010  05 8c ef 3f 40 00 2d 06  d9 95 80 77 f5 0c 0a 00   ···?@·-· ···w····
0020  00 13 00 50 c3 2d 1f c9  d7 69 47 4a 6d 9a 50 10   ···P·-·· ·iGJm·P·
0030  00 ed 75 bd 00 00 48 54  54 50 2f 31 2e 31 20 32   ··u···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
0050  2c 20 31 31 20 41 70 72  20 32 30 32 32 20 30 38   , 11 Apr  2022 08
```

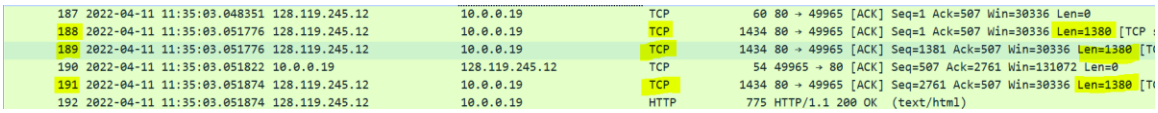
כפי שמצוין למטה בהדגשה, מדובר בחבילה 188.

שאלה 14:

ניתן לראות בצילום של שאלה 13: אוקיי, קוד 200. (מודגש למטה בצהוב)

שאלה 15:

נסתכל על חבילות מסוג טי פי סי שיש להן תוכן משלב ה"גט" עד ה"אוקיי":

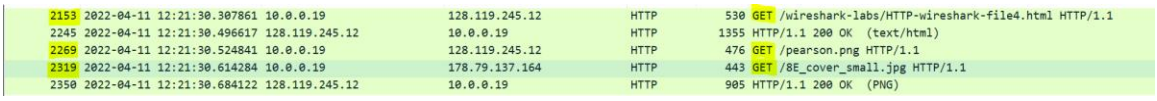


187	2022-04-11 11:35:03.048351	128.119.245.12	10.0.0.19	TCP	60	80 → 49965 [ACK] Seq=1 Ack=507 Win=30336 Len=0
188	2022-04-11 11:35:03.051776	128.119.245.12	10.0.0.19	TCP	1434	80 → 49965 [ACK] Seq=1 Ack=507 Win=30336 Len=1380 [TCP
189	2022-04-11 11:35:03.051776	128.119.245.12	10.0.0.19	TCP	1434	80 → 49965 [ACK] Seq=1381 Ack=507 Win=30336 Len=1380 [T
190	2022-04-11 11:35:03.051822	10.0.0.19	128.119.245.12	TCP	54	49965 → 80 [ACK] Seq=507 Ack=2761 Win=131072 Len=0
191	2022-04-11 11:35:03.051874	128.119.245.12	10.0.0.19	TCP	1434	80 → 49965 [ACK] Seq=2761 Ack=507 Win=30336 Len=1380 [T
192	2022-04-11 11:35:03.051874	128.119.245.12	10.0.0.19	HTTP	775	HTTP/1.1 200 OK (text/html)

מכאן שנשלחו 3 חבילות עם תוכן: חבילות מספר 188,189 ו191.

שאלה 16:

נסתכל על החבילות (חשוב לי לציין שרק אחת התמונות הוצגה, השנייה נכשלה).



2153	2022-04-11 12:21:30.307861	10.0.0.19	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
2245	2022-04-11 12:21:30.496617	128.119.245.12	10.0.0.19	HTTP	1355	HTTP/1.1 200 OK (text/html)
2269	2022-04-11 12:21:30.524841	10.0.0.19	128.119.245.12	HTTP	476	GET /pearson.png HTTP/1.1
2319	2022-04-11 12:21:30.614284	10.0.0.19	178.79.137.164	HTTP	443	GET /8E_cover_small.jpg HTTP/1.1
2350	2022-04-11 12:21:30.684122	128.119.245.12	10.0.0.19	HTTP	905	HTTP/1.1 200 OK (PNG)

בס"ד

קיימות 3 חבילות מסוג "גט". המספר הסידורי שלהן הוא: 2153, 2269 ו2319. 2 חבילות נשלחו אל כתובת 128.119.245.12. חבילה נוספת נשלחה אל כתובת שונה: 178.79.137.164.

שאלה 17:

אמנם רק תמונה אחת ירדה בסופו של דבר, אך ניתן להבחין בכך ששני החבילות של ה"גט" נשלחו אחת אחרי השנייה, רק לאחר מכן אחת התמונות הורדה. כך שניתן לומר ששתי ההורדות של התמונות נעשות באופן מקביל ולא באופן סדרתי.

שאלה 18:

נסתכל ברשימות החבילות המסוננת:

No.	Time	Source	Destination	Protocol	Length	Info
1446	2022-04-11 12:32:45.530690	10.0.0.19	128.119.245.12	HTTP	576	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html H
1622	2022-04-11 12:32:45.686466	128.119.245.12	10.0.0.19	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

המספר של חבילת ה"גט" היא 1446 ושל התגובה היא 1662. כפי שניתן לראות, התגובה היא קוד 401 – לא מורשה.

שאלה 19:

נסתכל בתוכן של חבילת ה"גט":

16944	2022-04-11 12:33:10.485974	10.0.0.19	128.119.245.12	HTTP	661	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5
17035	2022-04-11 12:33:10.645391	128.119.245.12	10.0.0.19	HTTP	544	HTTP/1.1 200 OK (text/html)

```
> Transmission Control Protocol, Src Port: 57403, Dst Port: 80, Seq: 1, Ack: 1, Len: 607
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
```

ניתן לראות שיש כאן שדה חדש בשם "הרשאה". מצוין בו שיש הרשאה "בסיסית" וכן בפנים ניתן לראות את שם המשתמש והסיסמא שהזנו.