1. לאיזו שכבה שייך HTTP במודל השכבות?

2. לפניך שני ETHERNET FRAME ב-HEX. עליך לתרגם אותם כדי פענח התוכן ששייך לHTTP ולהסביר כל שדה של HTTP (**<u>הבהרה:</u>** לא מבקשים ששתרגמו השדות של IP וכו' אתם רק צריכים לזהות כל דבר איפוה הוא נמצא כך שתוכלו להשיג המידע ששייך לHTTP. את המידע הזה דווקא תתצטרכו לתרגם לצורה קריאה והלהסביר מה יש בו):

א. <u>חבילה 1</u>

00 03 ff 02 99 d4 00 01 29 00 99 d4 08 00 45 00 01 81 41 9e 40 00 80 06 31 bc c0
a8 02 65 c0 a8 02 67 dc fe 00 50 67 be 74 24 75 26 15 f6 50 18 40 29 bd 23 00 00
47 45 54 20 2f 66 6f 72 6d 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63
63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a
20 65 6e 2d 75 73 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61
2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 38 2e 30 3b
20 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20 54 72 69
64 65 6e 74 2f 34 2e 30 3b 20 53 4c 43 43 32 3b 20 2e 4e 45 54 20 43 4c 52 20 32
2e 30 2e 35 30 37 32 37 3b 20 2e 4e 45 54 20 43 4c 52 20 33 2e 35 2e 33 30 37 32
39 3b 20 2e 4e 45 54 20 43 4c 52 20 33 2e 30 2e 33 30 37 32 39 3b 20 4d 65 64
69 61 20 43 65 6e 74 65 72 20 50 43 20 36 2e 30 3b 20 49 6e 66 6f 50 61 74 68 2e
33 3b 20 2e 4e 45 54 34 2e 30 43 3b 20 2e 4e 45 54 34 2e 30 45 29 0d 0a 41 63
63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74
65 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e 32 2e 31 30 33 0d 0a 43 6f 6e
6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a

ב. <u>חבילה 2</u>

00 01 29 00 99 d4 00 03 ff 02 99 d4 08 00 45 00 03 42 b5 48 40 00 80 06 bc 50 c0
a8 02 67 c0 a8 02 65 00 50 dc fe 75 26 15 f6 67 be 75 7d 50 18 fe a6 ae 9e 00 00
48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 4d 69
63 72 6f 73 6f 66 74 2d 49 49 53 2f 35 2e 31 0d 0a 44 61 74 65 3a 20 53 75 6e 2c
20 31 33 20 46 65 62 20 32 30 31 31 20 31 39 3a 34 39 3a 32 34 20 47 4d 54 0d 0a
43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d 0a 41 63
63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d 0a 4c 61 73 74 2d 4d 6f
64 69 66 69 65 64 3a 20 53 75 6e 2c 20 31 33 20 46 65 62 20 32 30 31 31 20 31 38

3a 33 32 3a 31 38 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 36 34 62 31 37 65 35 38
61 63 63 62 63 62 31 3a 39 37 61 22 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74
68 3a 20 35 36 38 0d 0a 0d 0a ef bb bf 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c
20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20
31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 20 22 68 74 74 70
3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f
78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0d 0a
3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e
6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a
0d 0a 3c 66 6f 72 6d 20 6e 61 6d 65 3d 22 69 6e 70 75 74 22 20 61 63 74 69 6f 6e
3d 22 66 6f 72 6d 5f 61 63 74 69 6f 6e 2e 61 73 70 22 20 6d 65 74 68 6f 64 3d 22
67 65 74 22 3e 0d 0a 46 69 72 73 74 20 6e 61 6d 65 3a 20 3c 69 6e 70 75 74 20 74
79 70 65 3d 22 74 65 78 74 22 20 6e 61 6d 65 3d 22 46 69 72 73 74 4e 61 6d 65 22
20 76 61 6c 75 65 3d 22 4d 69 63 6b 65 79 22 20 2f 3e 3c 62 72 20 2f 3e 0d 0a 4c
61 73 74 20 6e 61 6d 65 3a 20 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 74 65 78 74
22 20 6e 61 6d 65 3d 22 4c 61 73 74 4e 61 6d 65 22 20 76 61 6c 75 65 3d 22 4d 6f
75 73 65 22 20 2f 3e 3c 62 72 20 2f 3e 0d 0a 3c 69 6e 70 75 74 20 74 79 70 65 3d
22 73 75 62 6d 69 74 22 20 76 61 6c 75 65 3d 22 53 75 62 6d 69 74 22 20 2f 3e 0d
0a 3c 2f 66 6f 72 6d 3e 20 0d 0a 0d 0a 3c 70 3e 49 66 20 79 6f 75 20 63 6c 69 63
6b 20 74 68 65 20 22 53 75 62 6d 69 74 22 20 62 75 74 74 6f 6e 2c 20 74 68 65 20
66 6f 72 6d 2d 64 61 74 61 20 77 69 6c 6c 20 62 65 20 73 65 6e 74 20 74 6f 20 61
20 70 61 67 65 20 63 61 6c 6c 65 64 20 22 68 74 6d 6c 5f 66 6f 72 6d 5f 61 63 74
69 6f 6e 2e 61 73 70 22 2e 3c 2f 70 3e 0d 0a 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f
68 74 6d 6c 3e 0d 0a 0d 0a

עזרה:

גודלו של Ethernet header הוא 14 בתים. מבנה HEADER של ETHERNET:

6 Bytes	
Destination Address	
Source Address	
DATA TYPE	**Data**
Data	

לפני ה-Header מופיעים 8 בתים של Preamble לזיהוי התחלת המסגרת, אך הם לא מופיעים ב-WireShark.

גודלו של IP header ללא options הינו 20 בתים. מבנה HEADER של IP:

4 Bytes				
Version	**Ihl**	**Type Of Service**	**Total Legth**	
Identification			**Flags**	**Fragment Offset**
Time To Live		**Protocol**	**Header Checksum**	
Source Address				
Destination Address				
Options				**Padding**
Data				

גודלו של TCP header הינו 20 בתים. מבנה HEADER של TCP:

<table>
<tr><th colspan="5">4 Bytes</th></tr>
<tr><td colspan="2">Source Port</td><td colspan="3">Destination Port</td></tr>
<tr><td colspan="5">Sequence Number</td></tr>
<tr><td colspan="5">Acknowledgment Number</td></tr>
<tr><td>Data Offset</td><td>Reserved</td><td>Control Bits</td><td colspan="2">Window</td></tr>
<tr><td colspan="2">Checksum</td><td colspan="3">Urgent Pointer</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

3. צייר sequence diagram (עליך לצייר את הדיאגרמה או להשתמש בתכונה של ה-wireshark) של שיחות HTTP המופיעות ב-trace (HTTP-Full-Client.pcap).
4. אילו סוגי **בקשות** אתה מזהה ב-TRACE (HTTP-Full-Client.pcap)? ציין מספר PACKET עבור כל בקשה. אילו סוגי בקשות נוספים מוגדרים בפרוטוקול?
5. מה ההבדל בין סוגי בקשות אלו?
6. מתי כדאי להשתמש בכל סוג בקשה?
7. אילו סוגי **תשובות** אתה מזהה ב-TRACE (HTTP-Full-Client.pcap)? ציין מספר PACKET עבור כל תשובה וכן את הבקשה עבורה התקבלה התשובה. כיצד זיהית את הבקשה? כמה סוגי תשובות מוגדרים בפרוטוקול?
8. מה המשמעות של כל תשובה?
9. בתוך איזה פרוטוקול ארוז פרוטוקול HTTP? מדוע? מה מוסיף פרוטוקול זה ל-HTTP?
10. ב-PACKET כלשהו התחילה שיחה עם השרת. מה תוכנה של השיחה? על פני כמה PACKETS מתפרסת השיחה?
11. מדוע כאשר ביקשנו את דף with_css_img.htm יש יותר מבקשה אחת לשרת? מי אחראי לטפל בזה?
12. בקובץ HTTP-NOTRECOGNIZE.pcap ישנה שיחת HTTP אבל wireshark לא מזהה זאת. מדוע?

מעבדה HTTP - תשובות

1. שכבת האפליקציה.
2. א. מעניין אותנו רק ה-HTTP

```
GET /form.html HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)
Accept-Encoding: gzip, deflate
Host: 192.168.2.103
Connection: Keep-Alive
```

ב.

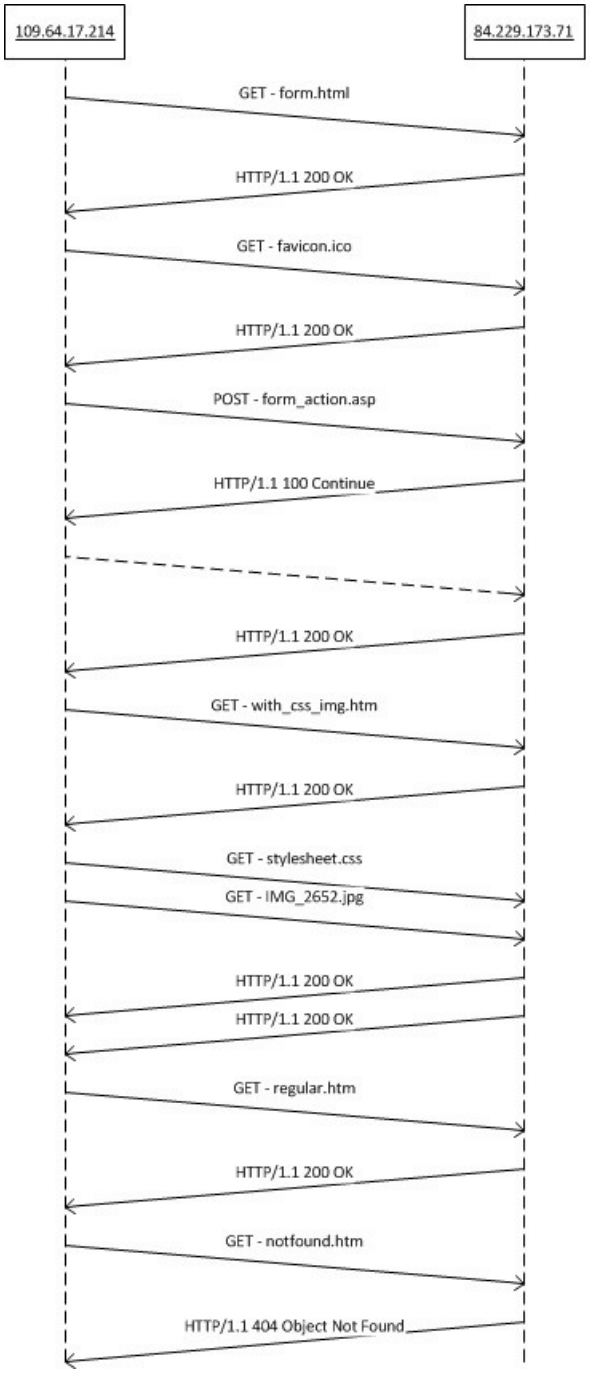
```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Sun, 13 Feb 2011 19:49:24 GMT
Content-Type: text/html
Accept-Ranges: bytes..Last-Modified: Sun, 13 Feb 2011 18:32:18 GMT
ETag: "64b17e58accbcb1:97a"
Content-Length: 568

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" >
<body>
<form name="input" action="form_action.asp" method="get">
First name: <input type="text" name="FirstName" value="Mickey" /><br />
Last name: <input type="text" name="LastName" value="Mouse" /><br />
<input type="submit" value="Submit" />
</form>

<p>If you click the "Submit" button, the form-data will be sent to a page called "html_form_action.asp".</p>
```

</body>
</html>

.3



4. סוגי **הבקשות** ב-TRACE:

   א. GET - 6

   ב. POST - 66

סוגי הבקשות הנוספים המוגדרים בפרוטוקול הם[1]:

א. "OPTIONS" ; Section 9.2

ב. "HEAD" ; Section 9.4

ג. "PUT" ; Section 9.6

ד. "DELETE" ; Section 9.7

ה. "TRACE" ; Section 9.8

ו. "CONNECT" ; Section 9.9

5. ההבדלים והשימושים מוסברים ב RFC בפרק 9.

6. כנ"ל.

7. סוגי **התשובות** ב-TRACE:

א. 200 ok. - 7 עבור בקשה של form.html ניתן לזהות זאת על ידי פרוטוקול ה TCP.

ב. 100 continue. - 67 עבור בקשה של form_action.asp כנ"ל.

ג. 404 object not found. - 284 עבור בקשה של notfound.htm כנ"ל.

מוגדרים סה"כ 41 סוגים שונים[2].

8. א. המשאב נמצא ואני שולח לך אותו.

ב. על הלקוח להמשיך עם הבקשה, השרת ממתין להמשך הבקשה.

ג. המשאב המבוקש לא נמצא על השרת.

9. הוא ארוז בתוך TCP. פרוטוקול זה מוסיף את היכולת לזהות את הקשר בין הבקשה לתשובה וכן דואג לכך שהנתונים יעברו ברשת באופן תקין והחבילות תגענה בסדר הנכון אל הדפדפן.

10. תוכן השיחה:

```
GET /form.html HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*
Accept-Language: he-IL
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; GTB6.6; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Accept-Encoding: gzip, deflate
Host: 84.229.173.71
Connection: Keep-Alive
```

[1] http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html

[2] http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html#sec10.1.1

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Tue, 15 Feb 2011 19:17:39 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Tue, 15 Feb 2011 17:24:57 GMT
ETag: "8608c4435cdcb1:9b7"
Content-Length: 569

...<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" >

<body>
<form name="input" action="form_action.asp" method="POST">
First name: <input type="text" name="FirstName" value="Mickey" />
Last name: <input type="text" name="LastName" value="Mouse" />
<input type="submit" value="Submit" />
</form>
If you click the "Submit" button, the form-data will be sent to a page called "html_form_action.asp".
</body>
</html>

POST /form_action.asp HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*
Referer: http://84.229.173.71/form.html
Accept-Language: he-IL
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; GTB6.6; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: 84.229.173.71
Content-Length: 31
Connection: Keep-Alive
Cache-Control: no-cache
FirstName=Mickey&LastName=Mouse

HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Tue, 15 Feb 2011 19:17:41 GMT

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Tue, 15 Feb 2011 19:17:41 GMT

```
Content-Length: 103
Content-Type: text/html
Set-Cookie:
ASPSESSIONIDSARDBTAS=BLBNDCGBOIDKCKMFHMBGJNIJ; path=/
Cache-control: private

The Server Get Your Request. It will be consider.<br />
<hr />
First Name is:  Last Name is:
<hr />
```

11. מכיוון שניתן לראות כי דף זה מכיל הפניות אל תמונה וכן אל דף סגנונות אנו רוצים לקבל את שניהם ולכן עבור כל אחד מהם יש בקשה נפרדת. הדפדפן שלנו אחראי לטפל בבקשות אלו.

12. מכיוון שהבקשות לא נשלחות אל הפורט של HTTP (80) התוכנה לא יודעת לזהות את הבקשות כ-HTTP.