

# רשתות מחשבים

פרק 3ב' - Wireshark

ברק גונן

מבוסס על ספר הלימוד "רשתות מחשבים" מאת

עומר רוזנבוים

# מה נלמד?

- ▶ למדנו אודות מודל 5 השכבות
  - Encapsulation - כל שכבה עוטפת את המידע של השכבה שמעליה
- ▶ בשיעור זה נצפה במידע שעובר ב- 5 השכבות
  - נלמד לעבוד עם כלי חדש



# רקע- Wireshark

- ▶ Wireshark הוא כלי לניתוח רשתות
- ▶ לתוכנה שני מרכיבים:
  - Packet sniffer- קולט פקטות שנשלחות או מתקבלות במחשב
  - Packet analyzer- מנתח את הפקטות
- ▶ שימושים:
  - איתור בעיות ברשת תקשורת- שימוש לגיטימי
  - האזנה לתקשורת, קליטת סיסמאות - שימוש זדוני
- ▶ למרבית הטכנולוגיה שנעסוק בה יש שימושים לגיטימיים וזדוניים. הבחירה היא בידי המשתמש.



# איך עובד packet sniffer?



- ▶ אפליקציות שרצות על המחשב שולחות ומקבלות פקטות
- ▶ הפקטות עוברות דרך כרטיס הרשת
  - למעט שתי אפליקציות שמתקשרות על אותו מחשב
- ▶ כל פקטה שמגיעה לכרטיס הרשת משוכפלת
  - עותק אחד ממשיך ברשת
  - עותק שני נשמר במחשב

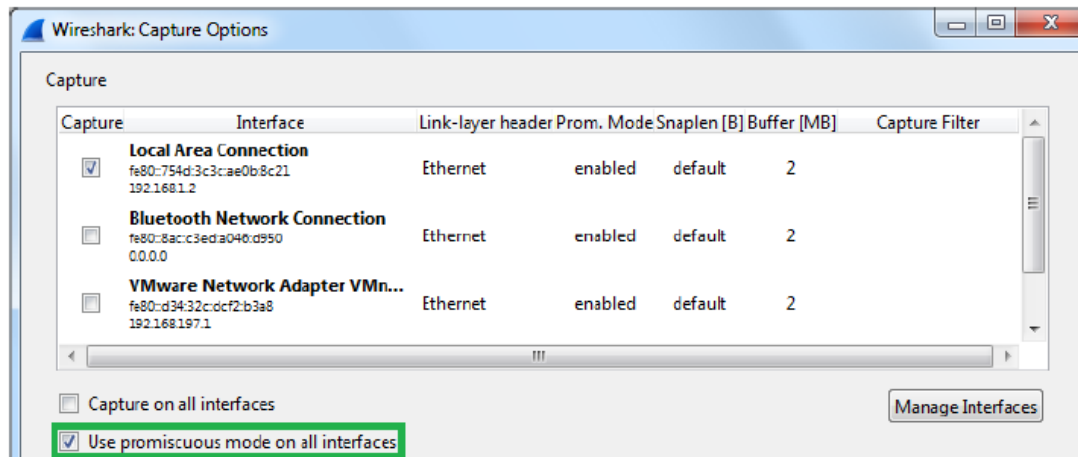
# אילו פקטות מגיעות לכרטיס הרשת?

- ▶ לעיתים ברשת LAN מחשב מקבל frames שאינן מיועדות אליו:
  - ברשת WiFi
  - כאשר ברשת יש Hub - מקבל frame ומפיץ לכל מי שמחובר אליו
- ▶ כל frame נשלח עם כתובת ייחודית, וכרטיס הרשת מעביר למחשב רק מה ששייך לו
- ▶ למה הדבר דומה? לדוור שמשאיר את הדואר של כל הבנין בכניסה לבנין, כל משפחה עוברת על הדואר ולוקחת רק מה שמיועד לה



# Promiscuous mode

- ▶ במצב promiscuous, כרטיס הרשת מפסיק לפלטר רק את ה-frames שמיועדות אליו
- ▶ כל frame שמגיעה לכרטיס, גם כזו ששייכת למחשב אחר ב-LAN, משוכפלת ונשמרת
- ▶ למה הדבר דומה? אחד מדיירי הבנין משכפל את המכתבים של כל הדיירים, שומר לעצמו עותק ומחזיר את המכתב המקורי לערמת המכתבים שהשאיר הדורך
- ▶ ניתן לקבוע מצב זה בתפריט ה-options של wireshark:



# צפיה בשכבות התקשורת - תרגיל מודרך

▶ הפעילו הסנפה חדשה ב-wireshark



▶ גילשו בדפדפן לאתר כלשהו  
▶ לאחר שהאתר עלה, עיצרו את ההסנפה



# צפיה בשכבות התקשורת - המשך

- ▶ נפלטר לפי http
- ▶ מדוע? משום ש-http הוא פרוטוקול הגלישה באינטרנט

The screenshot shows the Wireshark interface with the filter 'http' applied. The packet list contains 23 entries, including DNS queries and responses, and QUIC traffic. The packet details pane for packet 23 shows the following structure:

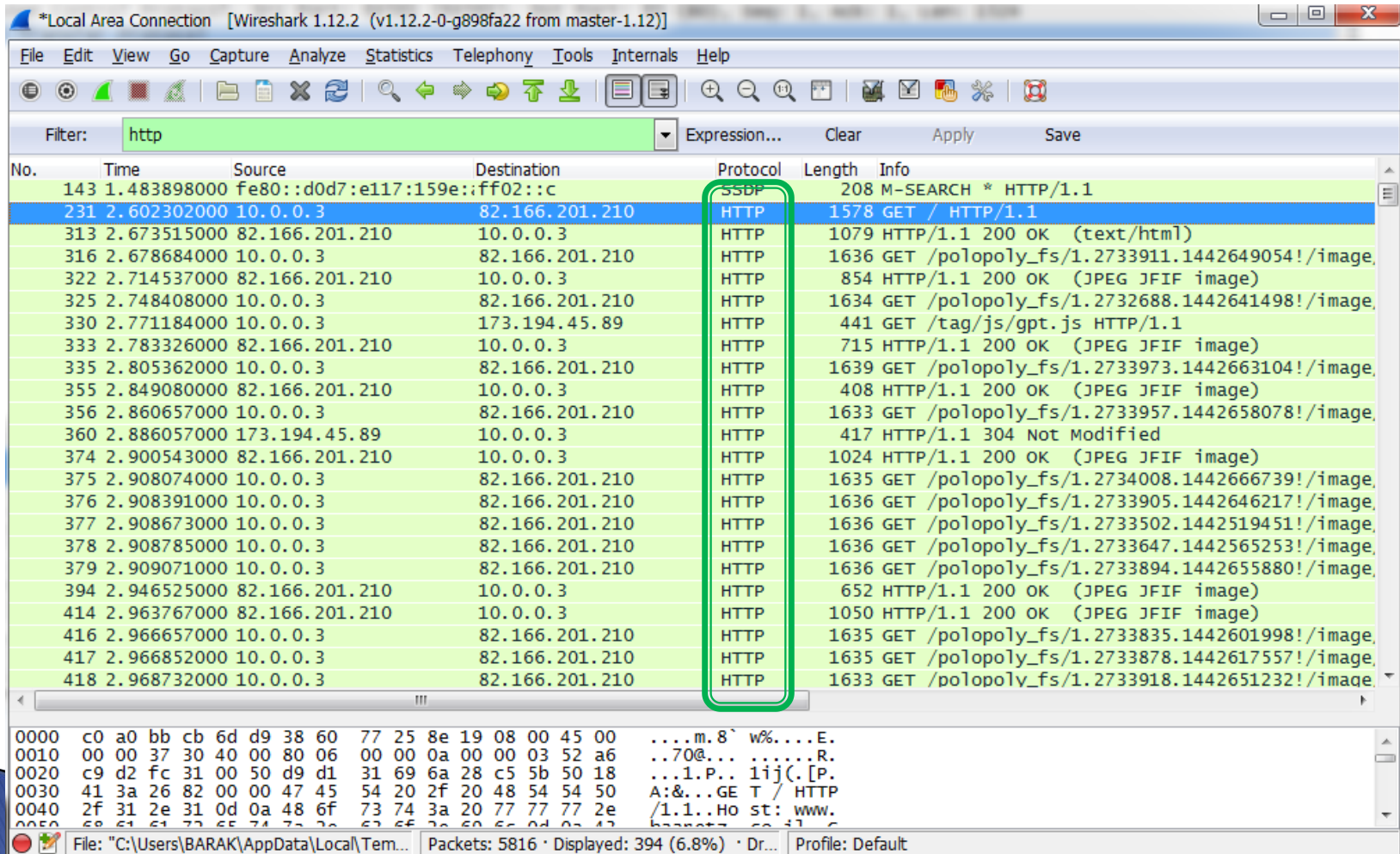
```

0000  c0 a0 bb cb 6d d9 38 60 77 25 8e 19 08 00 45 00  ....m.8`w%....E.
0010  00 00 37 30 40 00 80 06 00 00 0a 00 00 03 52 a6  ..70@... ..R.
0020  c9 d2 fc 31 00 50 d9 d1 31 69 6a 28 c5 5b 50 18  ...1.P.. ij]([.P.
0030  41 3a 26 82 00 00 47 45 54 20 2f 20 48 54 54 50  A:&...GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e  /1.1..Ho st: www.
0050  68 61 61 73 65 74 73 2a 62 65 7a 60 65 04 02 43  h...t...
  
```



# צפיה בשכבות התקשורת- המשך

כעת אנו צופים רק בפקטות ששייכות לפרוטוקול http ▶



Wireshark 1.12.2 (v1.12.2-0-g898fa22 from master-1.12)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
143	1.483898000	fe80::d0d7:e117:159e::ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
231	2.602302000	10.0.0.3	82.166.201.210	HTTP	1578	GET / HTTP/1.1
313	2.673515000	82.166.201.210	10.0.0.3	HTTP	1079	HTTP/1.1 200 OK (text/html)
316	2.678684000	10.0.0.3	82.166.201.210	HTTP	1636	GET /polopoly_fs/1.2733911.1442649054!/image
322	2.714537000	82.166.201.210	10.0.0.3	HTTP	854	HTTP/1.1 200 OK (JPEG JFIF image)
325	2.748408000	10.0.0.3	82.166.201.210	HTTP	1634	GET /polopoly_fs/1.2732688.1442641498!/image
330	2.771184000	10.0.0.3	173.194.45.89	HTTP	441	GET /tag/js/gpt.js HTTP/1.1
333	2.783326000	82.166.201.210	10.0.0.3	HTTP	715	HTTP/1.1 200 OK (JPEG JFIF image)
335	2.805362000	10.0.0.3	82.166.201.210	HTTP	1639	GET /polopoly_fs/1.2733973.1442663104!/image
355	2.849080000	82.166.201.210	10.0.0.3	HTTP	408	HTTP/1.1 200 OK (JPEG JFIF image)
356	2.860657000	10.0.0.3	82.166.201.210	HTTP	1633	GET /polopoly_fs/1.2733957.1442658078!/image
360	2.886057000	173.194.45.89	10.0.0.3	HTTP	417	HTTP/1.1 304 Not Modified
374	2.900543000	82.166.201.210	10.0.0.3	HTTP	1024	HTTP/1.1 200 OK (JPEG JFIF image)
375	2.908074000	10.0.0.3	82.166.201.210	HTTP	1635	GET /polopoly_fs/1.2734008.1442666739!/image
376	2.908391000	10.0.0.3	82.166.201.210	HTTP	1636	GET /polopoly_fs/1.2733905.1442646217!/image
377	2.908673000	10.0.0.3	82.166.201.210	HTTP	1636	GET /polopoly_fs/1.2733502.1442519451!/image
378	2.908785000	10.0.0.3	82.166.201.210	HTTP	1636	GET /polopoly_fs/1.2733647.1442565253!/image
379	2.909071000	10.0.0.3	82.166.201.210	HTTP	1636	GET /polopoly_fs/1.2733894.1442655880!/image
394	2.946525000	82.166.201.210	10.0.0.3	HTTP	652	HTTP/1.1 200 OK (JPEG JFIF image)
414	2.963767000	82.166.201.210	10.0.0.3	HTTP	1050	HTTP/1.1 200 OK (JPEG JFIF image)
416	2.966657000	10.0.0.3	82.166.201.210	HTTP	1635	GET /polopoly_fs/1.2733835.1442601998!/image
417	2.966852000	10.0.0.3	82.166.201.210	HTTP	1635	GET /polopoly_fs/1.2733878.1442617557!/image
418	2.968732000	10.0.0.3	82.166.201.210	HTTP	1633	GET /polopoly_fs/1.2733918.1442651232!/image

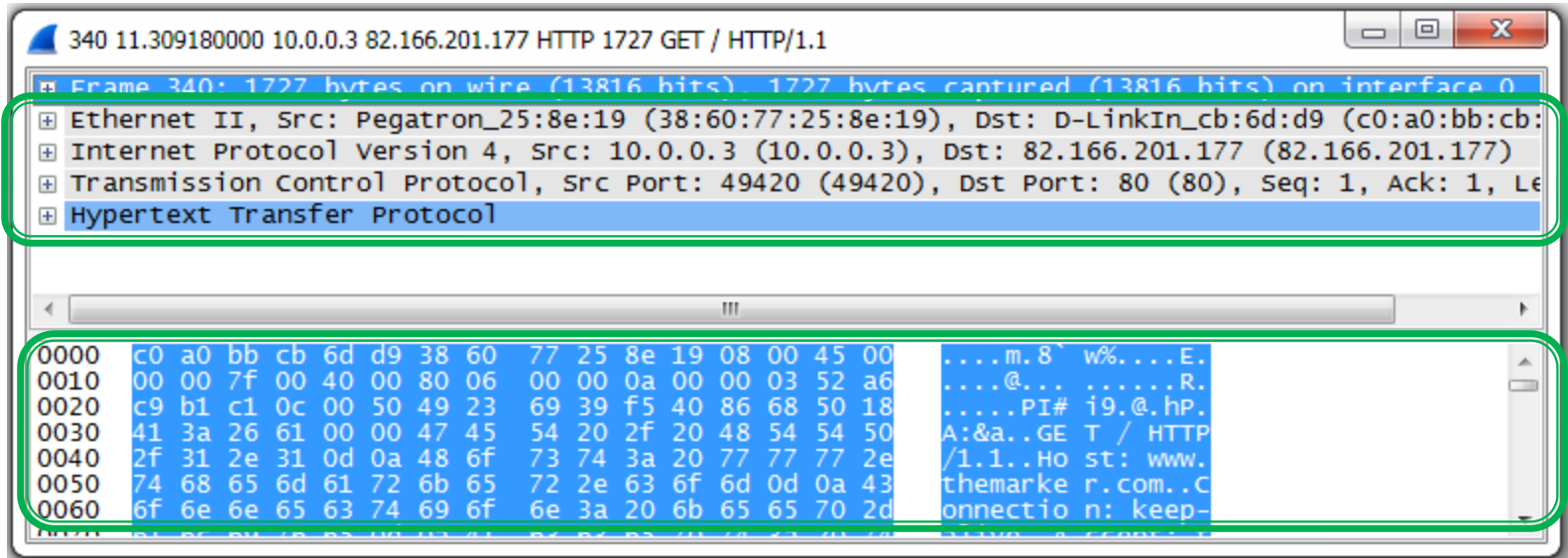
0000 c0 a0 bb cb 6d d9 38 60 77 25 8e 19 08 00 45 00 .....m.8` w%....E.  
 0010 00 00 37 30 40 00 80 06 00 00 0a 00 00 03 52 a6 ...70@... ..R.  
 0020 c9 d2 fc 31 00 50 d9 d1 31 69 6a 28 c5 5b 50 18 ...1.P.. lij(. [P.  
 0030 4f 3a 2e 82 00 00 47 45 54 20 2f 20 48 54 54 50 A:&...GE T / HTTP  
 0040 21 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..HO st: www.  
 0050 68 61 61 73 65 74 73 2a 63 6f 2a 60 66 0d 0a 43 hanna... .il C

File: "C:\Users\BARAK\AppData\Local\Tem... Packets: 5816 · Displayed: 394 (6.8%) · Dr... Profile: Default

# צפיה בשכבות התקשורת- המשך

לחיצה כפולה על אחת הפקטות תפתח אותה בחלון חדש ▶

שכבות  
התקשורת



המידע שעבר, בפורמט הקס  
ובפורמט ASCII

# סיכום כלל המידע שעבר ב-Frame

```

340 11.309180000 10.0.0.3 82.166.201.177 HTTP 1727 GET / HTTP/1.1
Frame 340: 1727 bytes on wire (13816 bits), 1727 bytes captured (13816 bits) on interface 0
Interface id: 0 (\Device\NPF_{0D08FA9B-C0E0-44AD-AF82-219BFAF7E515})
Encapsulation type: Ethernet (1)
Arrival Time: Sep 19, 2015 20:10:06.192903000
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1442682606.192903000 seconds
[Time delta from previous captured frame: 0.084466000 seconds]
[Time delta from previous displayed frame: 1.304752000 seconds]
[Time since reference or first frame: 11.309180000 seconds]
Frame Number: 340
Frame Length: 1727 bytes (13816 bits)
Capture Length: 1727 bytes (13816 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Number of per-protocol-data: 1]
[Hypertext Transfer Protocol, key 0]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Pegatron_25:8e:19 (38:60:77:25:8e:19), Dst: D-LinkIn_cb:6d:d9 (c0:a0:bb:cb:6d:d9)
Internet Protocol Version 4, Src: 10.0.0.3 (10.0.0.3), Dst: 82.166.201.177 (82.166.201.177)
Transmission Control Protocol, Src Port: 49420 (49420), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1727
Hypertext Transfer Protocol

0000  c0 a0 bb cb 6d d9 38 60 77 25 8e 19 08 00 45 00  ....m.8`w%....E.
0010  00 00 7f 00 40 00 80 06 00 00 0a 00 00 03 52 a6  ....@... ..R.
0020  c9 b1 c1 0c 00 50 49 23 69 39 f5 40 86 68 50 18  ....PI# i9.@.hp.
0030  41 3a 26 61 00 00 47 45 54 20 2f 20 48 54 54 50  A:&a..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e  /1.1..Host: www.
0050  74 68 65 6d 61 72 6b 65 72 2e 63 6f 6d 0d 0a 43  themarker.com..C
0060  6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d  onnection: keep-
0070  61 6c 69 76 65 0d 03 41 62 62 65 70 74 2a 20 74  alive Accept: t

```

- ▶ מיצאו את:
  - כמות הביטים שנשלחו
  - מספר ה-frame
  - זמן השליחה

# שכבת ה-data link

- ▶ לכל כרטיס רשת קיימת כתובת ייחודית בת 6 בתים. מיצאו אותה.

```

340 11.309180000 10.0.0.3 82.166.201.177 HTTP 1727 GET / HTTP/1.1
+ Frame 340: 1727 bytes on wire (13816 bits), 1727 bytes captured (13816 bits) on interface 0
- Ethernet II, Src: Pegatron_25:8e:19 (38:60:77:25:8e:19), Dst: D-LinkIn_cb:6d:d9 (c0:a0:bb:cb:6d:d9)
  + Destination: D-LinkIn_cb:6d:d9 (c0:a0:bb:cb:6d:d9)
  + Source: Pegatron_25:8e:19 (38:60:77:25:8e:19)
    Type: IP (0x0800)
  + Internet Protocol Version 4, Src: 10.0.0.3 (10.0.0.3), Dst: 82.166.201.177 (82.166.201.177)
  + Transmission Control Protocol, Src Port: 49420 (49420), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1727
  + Hypertext Transfer Protocol
  
```

0000	c0	a0	bb	cb	6d	d9	38	60	77	25	8e	19	08	00	45	00	....m.8`w%....E.
0010	00	00	7f	00	40	00	80	06	00	00	0a	00	00	03	52	a6	....@... ..R.
0020	c9	b1	c1	0c	00	50	49	23	69	39	f5	40	86	68	50	18	.....PI# i9.@.hP.
0030	41	3a	26	61	00	00	47	45	54	20	2f	20	48	54	50		A:&a..GE T / HTTP
0040	2f	31	2e	31	0d	0a	48	6f	73	74	3a	20	77	77	77	2e	/1.1..Host: www.
0050	74	68	65	6d	61	72	6b	65	72	2e	63	6f	6d	0d	0a	43	themark r.com..C
0060	6f	6e	6e	65	63	74	69	6f	6e	3a	20	6b	65	65	70	2d	onnectio n: keep-

# שכבת הרשת - network

מיצאו את:

- שם הפרוטוקול של שכבת הרשת
- כתובת מחשב היעד

```

340 11.309180000 10.0.0.3 82.166.201.177 HTTP 1727 GET / HTTP/1.1
+ Frame 340: 1727 bytes on wire (13816 bits), 1727 bytes captured (13816 bits) on interface 0
+ Ethernet II, Src: Pegatron_25:8e:19 (38:60:77:25:8e:19), Dst: D-LinkIn_cb:6d:d9 (c0:a0:bb:cb:6d:d9)
+ Internet Protocol Version 4, Src: 10.0.0.3 (10.0.0.3), Dst: 82.166.201.177 (82.166.201.177)
  Version: 4
  Header Length: 20 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    [Total Length: 1713 bytes (reported as 0, presumed to be because of "TCP segmentation offload")]
  Identification: 0x7f00 (32512)
  + Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  + Header checksum: 0x0000 [validation disabled]
  Source: 10.0.0.3 (10.0.0.3)
  Destination: 82.166.201.177 (82.166.201.177)
    [Source GeoIP: unknown]
    [Destination GeoIP: Unknown]
+ Transmission Control Protocol, Src Port: 49420 (49420), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1727
+ Hypertext Transfer Protocol
0000  c0 a0 bb cb 6d d9 38 60 77 25 8e 19 08 00 45 00  ....m.8`w%...E.
0010  00 00 7f 00 40 00 80 06 00 00 0a 00 00 03 52 a6  ...@.....R.
0020  c9 b1 c1 0c 00 50 49 23 69 39 f5 40 86 68 50 18  ...PI# i9.@.hp.
0030  41 3a 26 61 00 00 47 45 54 20 2f 20 48 54 54 50  A:&a..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e  /1.1..Host: www.
0050  74 68 65 6d 61 72 6b 65 72 2e 63 6f 6d 0d 0a 43  themarke r.com..C
0060  6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d  onnectio n: keep-
  
```

# שכבת התעבורה - transport

מיצאו את:

- שם הפרוטוקול של שכבת התעבורה
- פורט המקור ופורט היעד

340 11.309180000 10.0.0.3 82.166.201.177 HTTP 1727 GET / HTTP/1.1

- Frame 340: 1727 bytes on wire (13816 bits), 1727 bytes captured (13816 bits) on interface
- Ethernet II, Src: Pegatron\_25:8e:19 (38:60:77:25:8e:19), Dst: D-LinkIn\_cb:6d:d9 (c0:14:00:00:00:00)
- Internet Protocol Version 4, Src: 10.0.0.3 (10.0.0.3), Dst: 82.166.201.177 (82.166.201.177)
- Transmission Control Protocol, Src Port: 49420 (49420), Dst Port: 80 (80), Seq: 1, A**
  - Source Port: 49420 (49420)
  - Destination Port: 80 (80)
  - [Stream index: 7]
  - [TCP Segment Len: 1673]
  - Sequence number: 1 (relative sequence number)
  - [Next sequence number: 1674 (relative sequence number)]
  - Acknowledgment number: 1 (relative ack number)
  - Header Length: 20 bytes
  - ... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
  - window size value: 16698
  - [Calculated window size: 66792]
  - [window size scaling factor: 4]
  - Checksum: 0x2661 [validation disabled]
  - urgent pointer: 0
  - [SEQ/ACK analysis]
- Hypertext Transfer Protocol**

```

0020  c9 b1 c1 0c 00 50 49 23 69 39 f5 40 86 68 50 18  ...PI# 19.@.hp.
0030  41 3a 26 61 00 00 47 45 54 20 2f 20 48 54 54 50  A:&a..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e  /1.1..Host: www.
0050  74 68 65 6d 61 72 6b 65 72 2e 63 6f 6d 0d 0a 43  themarker.com..C
0060  6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d  onnection: keep-
0070  61 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 74  alive..Accept: t
0080  65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61  ext/html.applica
    
```

# שכבת האפליקציה - application

מיצאו את:

- שם הפרוטוקול של שכבת האפליקציה
- כתובת האתר אליו התבצעה הגלישה

```

340 11.309180000 10.0.0.3 82.166.201.177 HTTP 1727 GET / HTTP/1.1
+ Frame 340: 1727 bytes on wire (13816 bits), 1727 bytes captured (13816 bits) on interface 0
+ Ethernet II, Src: Pegatron_25:8e:19 (38:60:77:25:8e:19), Dst: D-Link_08:00:27:00:00:00
+ Internet Protocol Version 4, Src: 10.0.0.3 (10.0.0.3), Dst: 82.166.201.177 (82.166.201.177)
+ Transmission Control Protocol, Src Port: 49420 (49420), Dst Port: 80 (80)
- Hypertext Transfer Protocol
+ GET / HTTP/1.1\r\n
  Host: www.themarker.com\r\n
  Connection: keep-alive\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (windows NT 6.1; wow64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36\r\n
  Accept-Encoding: gzip, deflate, sdch\r\n
  Accept-Language: he-IL,he;q=0.8,en-US;q=0.6,en;q=0.4\r\n
+ [truncated]Cookie: __gads=ID=7598cff2e8ceef41:T=1415607279:S=ALNI...
  
```

0030	41 3a 26 61 00 00 47 45 54 20 2f 20 48 54 54 50	A:&a..GE T /
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e	/1.1..Ho st:
0050	74 68 65 6d 61 72 6b 65 72 2e 63 6f 6d 0d 0a 43	themark r.co
0060	6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d	onnectio n: k
0070	61 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 74	alive..A ccep
0080	65 78 74 2f 68 74 6d 6c 7c 61 70 70 6c 60 62 61	ext/html app

# Encapsulation

בזמן שאתם עוברים בין השכבות, שימו לב לכך שכל שכבה מוסיפה את ה-header שלה למידע שמועבר:

```
.....m.8`w%....E.
.....@.....R.
.....PI# i9.@.hP.
A:&a..GE T / HTTP
/1.1..Ho st: www.
themarket r.com..C
onnectio n: keep-
```

ה-header של  
שכבת ה-data link

```
.....m.8`w%....E.
.....@.....R.
.....PI# i9.@.hP.
A:&a..GE T / HTTP
/1.1..Ho st: www.
themarket r.com..C
onnectio n: keep-
```

ה-header של  
שכבת ה-network

```
.....m.8`w%....E.
.....@.....R.
.....PI# i9.@.hP.
A:&a..GE T / HTTP
/1.1..Ho st: www.
themarket r.com..C
onnectio n: keep-
```

ה-header של  
שכבת ה-transport

```
.....m.8`w%....E.
.....@.....R.
.....PI# i9.@.hP.
A:&a..GE T / HTTP
/1.1..Ho st: www.
themarket r.com..C
onnectio n: keep-
```

המידע שעובר  
בשכבת ה-  
application

ה-headerים אמורים להיות קריאים על ידי מחשב, לא אדם, לכן אינם מורכבים מתווי ASCII בעלי משמעות שימו לב, שמידע של שכבת האפליקציה עובר בכל השכבות



## סיכום- מה ראינו?

- ▶ באיזה פרוטוקול עבר המידע של האפליקציה?
  - Hypertext Transfer, או בקיצור HTTP
- ▶ באיזה פרוטוקול ופורט עשתה שימוש שכבת ה-transport?
  - בפרוטוקול Transmission Control Protocol, או בקיצור TCP
  - פורט היעד הוא פורט 80- פורט קבוע ל- HTTP
- ▶ באיזה פרוטוקול עשתה שימוש שכבת ה-network?
  - Internet Protocol, או בקיצור IP
- ▶ באיזה פרוטוקול עשתה שימוש שכבת ה-data link?
  - בפרוטוקול Ethernet
  - בהמשך נכיר את משמעות הכתובת בעלת 6 הבתים

## תרגיל – הסנפת סיסמה גלויה

▶ היכנסו לאתר הבא:

<http://cyber.org.il/networks/links/plain-password.html>

▶ הזינו סיסמה כלשהי והקישו register

▶ הכניסו ל-wireshark את הפילטר הבא:

▶ frame contains "txtPa"

▶ מוצאים את הסיסמה...?

▶ רוב הסיסמאות באינטרנט עוברות בצורה מוצפנת

▶ ניתן להעזר בתרגיל המודרך "הסנפת סיסמה גלויה" שבספר הלימוד, לאחר

תרגיל 3.1



# תרגיל – Follow TCP Stream

- ▶ הריצו על מחשבכם את הלקוח מתרגיל 2.6 (שרת פקודות בסיסי)
- ▶ ב-wireshark, בצעו פילטור לפי tcp
- ▶ בחרו את אחת מהפקטות שפולטרו, לחצו על קליק ימני- Follow TCP Stream

```
Follow TCP Stream
Stream Content
TIME
24Thu Jan 01 13:37:00 1970
NAME
14Tomer's Server
RAND
011
TIME
24Tue Sep 11 09:59:00 2001
EXIT
```