

# **מטלה 1-רטשות תקשורת**

**מגישיים :**

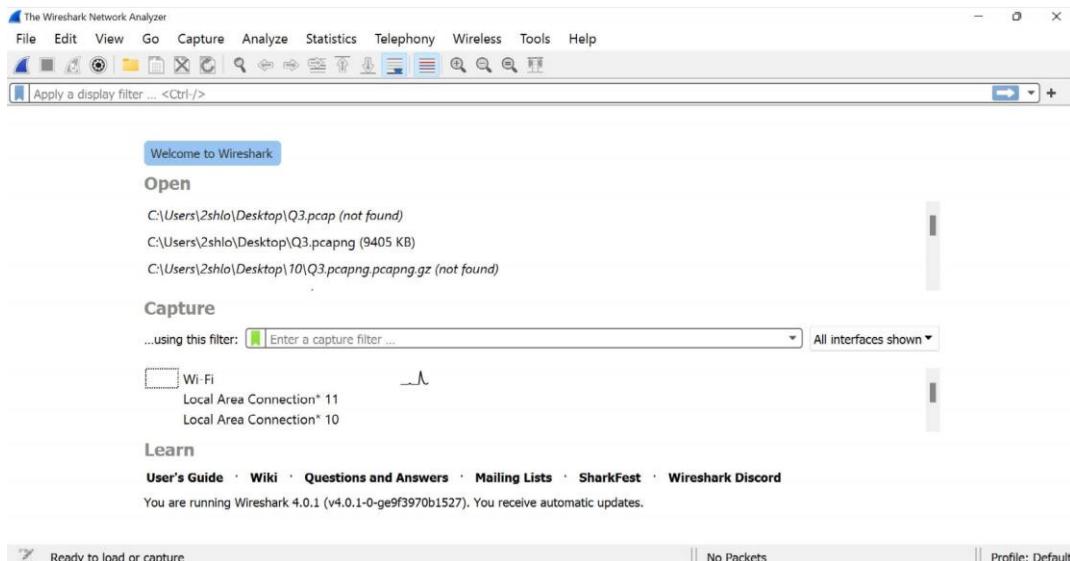
**שלומי זכריה - 315141242**

**יסמין כהן - 212733836**

## תרגיל 1:

נפתח את Wireshark ונסתכל על המסר הראשי, נראה שיש לנו כמה ממשקים שביהם ניתן להסניף מידע.

נבחר את הממשק שמקשור לאינטרנט החיצוני(לכן נבחר "WIFI")

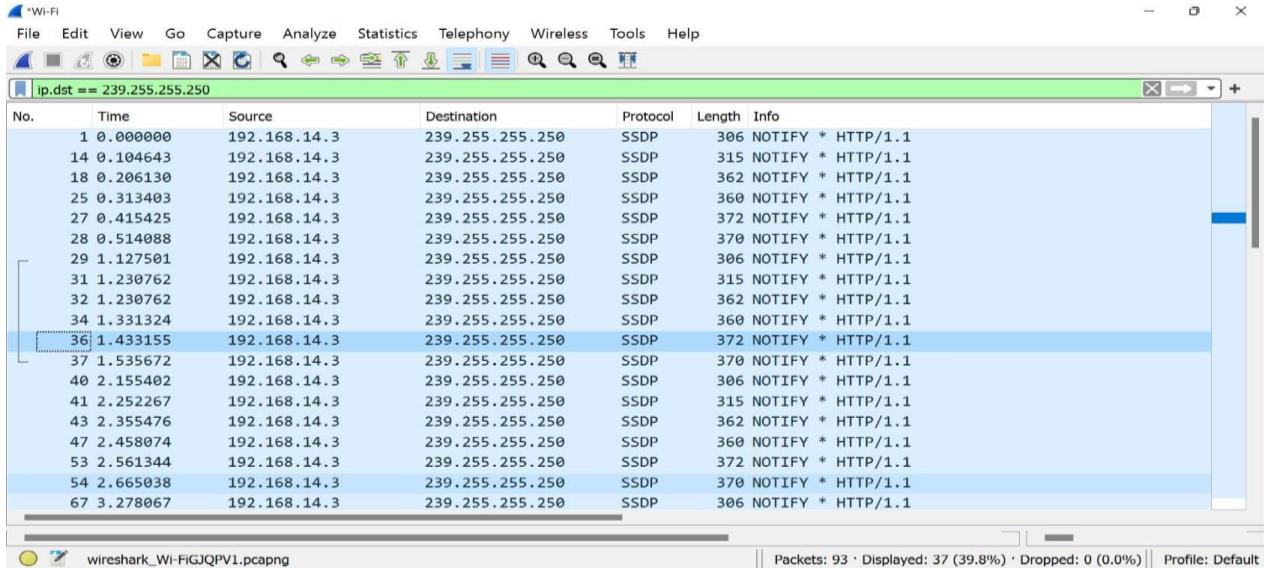


## תרגיל 2:

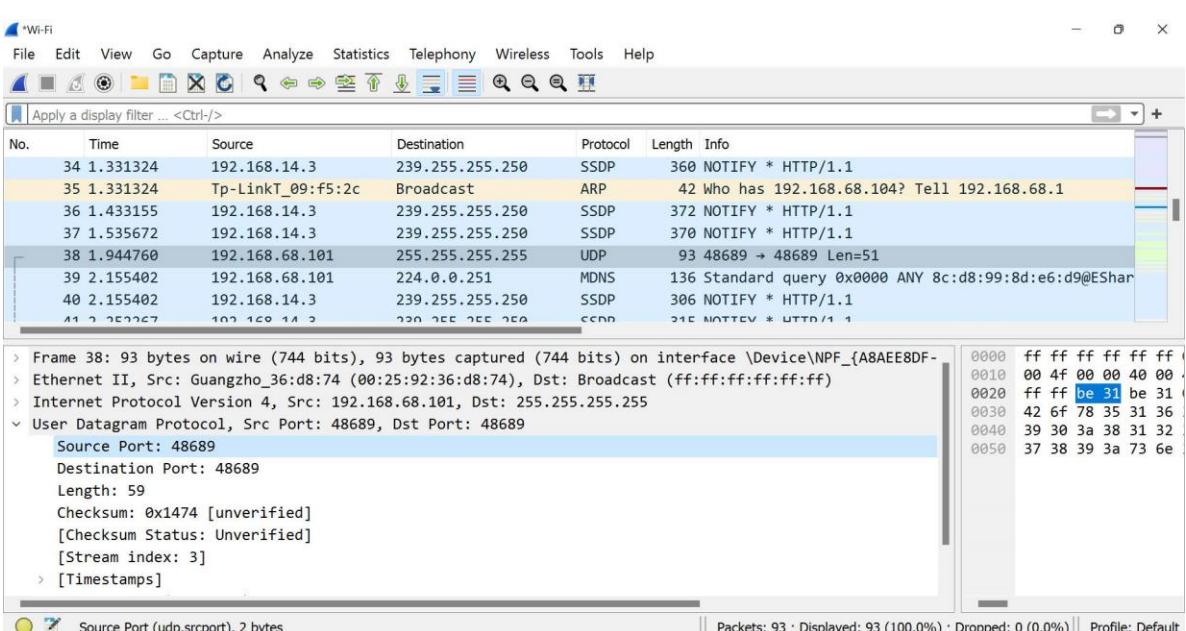
נפעיל את קלייט החבילות(פקטות), החבילות מצטברות מהר, עם הרבה סוגים ולכן  
נצרוך להכיר את מנגנון הסינון !

No.	Time	Source	Destination	Protocol	Length	Info
65	3.181352	192.168.68.101	224.0.0.251	MDNS	136	Standard query 0x0000 ANY 8c:d8:99:8d:e6:d9@EShare-12
66	3.181352	13.107.4.52	192.168.68.106	TCP	54	80 → 55644 [ACK] Seq=539 Ack=156 Win=4194048 Len=0
67	3.278067	192.168.14.3	239.255.255.250	SSDP	306	NOTIFY * HTTP/1.1
68	3.380915	Tp-LinkT_09:f5:2c	Broadcast	ARP	42	Who has 192.168.68.102? Tell 192.168.68.1
69	3.380915	192.168.14.3	239.255.255.250	SSDP	315	NOTIFY * HTTP/1.1
70	3.380915	Tp-LinkT_09:f5:2c	Broadcast	ARP	42	Who has 192.168.68.104? Tell 192.168.68.1
71	3.380915	192.168.68.101	224.0.0.251	MDNS	136	Standard query 0x0000 ANY 8c:d8:99:8d:e6:d9@EShare-12
72	3.380915	192.168.14.3	239.255.255.250	SSDP	362	NOTIFY * HTTP/1.1
73	3.481802	192.168.14.3	239.255.255.250	SSDP	366	NOTIFY * HTTP/1.1
74	3.583562	192.168.14.3	239.255.255.250	SSDP	372	NOTIFY * HTTP/1.1
75	3.686383	192.168.68.101	224.0.0.251	MDNS	136	Standard query 0x0000 ANY 8c:d8:99:8d:e6:d9@EShare-12
76	3.686383	192.168.14.3	239.255.255.250	SSDP	370	NOTIFY * HTTP/1.1
77	3.891470	192.168.68.101	224.0.0.251	MDNS	184	Standard query response 0x0000 SRV, cache flush 0 0 5
78	4.198275	192.168.68.101	224.0.0.251	MDNS	402	Standard query response 0x0000 TXT, cache flush PTR _
79	4.300896	192.168.14.3	239.255.255.250	SSDP	306	NOTIFY * HTTP/1.1
80	4.403877	192.168.14.3	239.255.255.250	SSDP	315	NOTIFY * HTTP/1.1
81	4.505297	192.168.14.3	239.255.255.250	SSDP	362	NOTIFY * HTTP/1.1
82	4.617819	192.168.14.3	239.255.255.250	SSDP	360	NOTIFY * HTTP/1.1

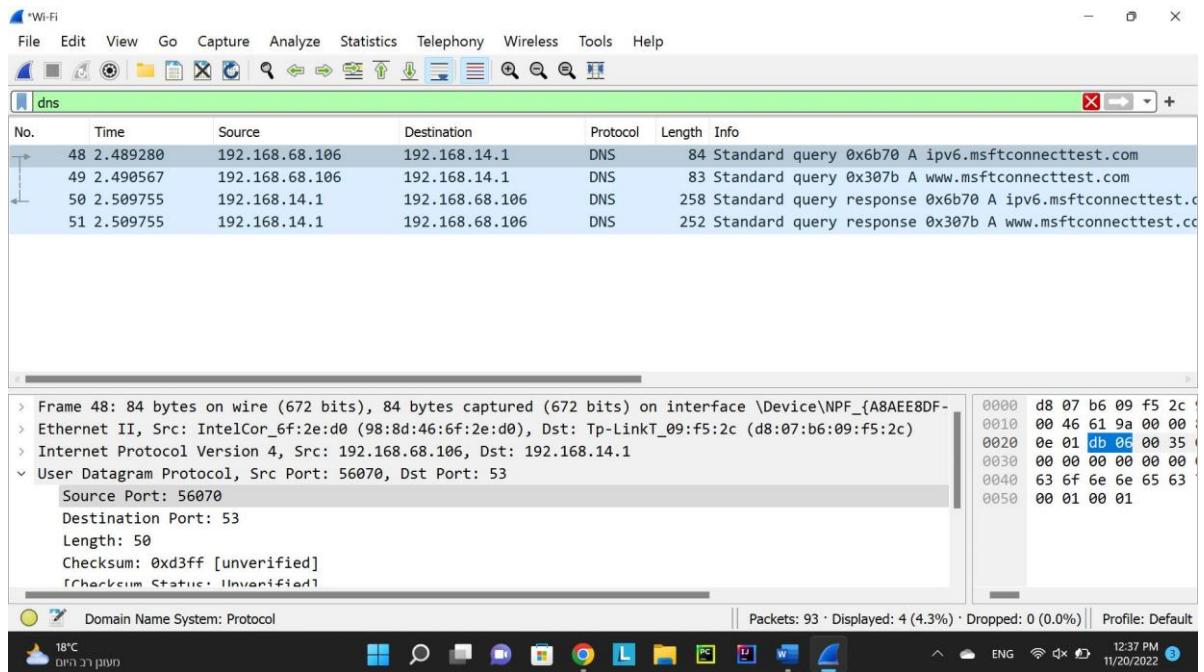
## 1.2. גSON את כל החבילות לפ' IP מסויים לבחירתנו(בדוגמא שלנו בחרנו (239.255.255.250=destination IP



## 2.2. גSON את כל החבילות לפ' port מסויים לבחירתנו(בדוגמא שלנו בחרנו UDP port= 48689) ונראה שהפרוטוקול שמשתמש בפורט הנ"ל הוא

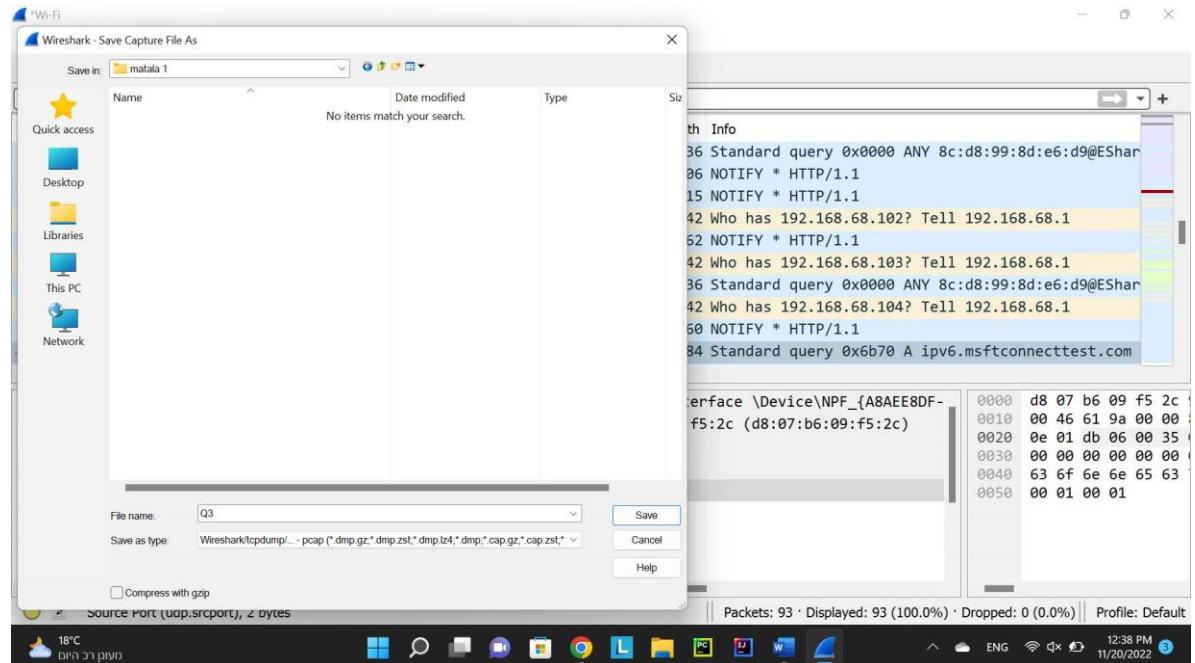


## 3.2 גSONן את החבילות לפי פרוטוקול מסוים לבחירתנו (בדוגמא שלנו בחרנו בפרוטוקול DNS)



### תרגיל 3:

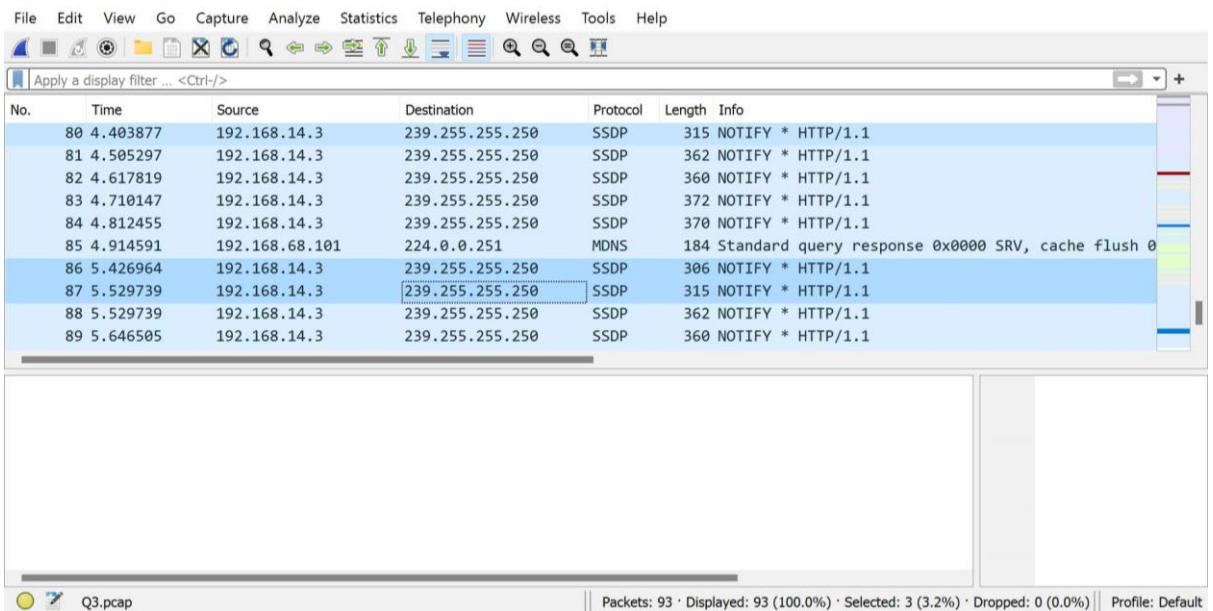
נשמור את הקלטת של pcap , ונראה שפורמט ההקלטה הוא: " pcap "



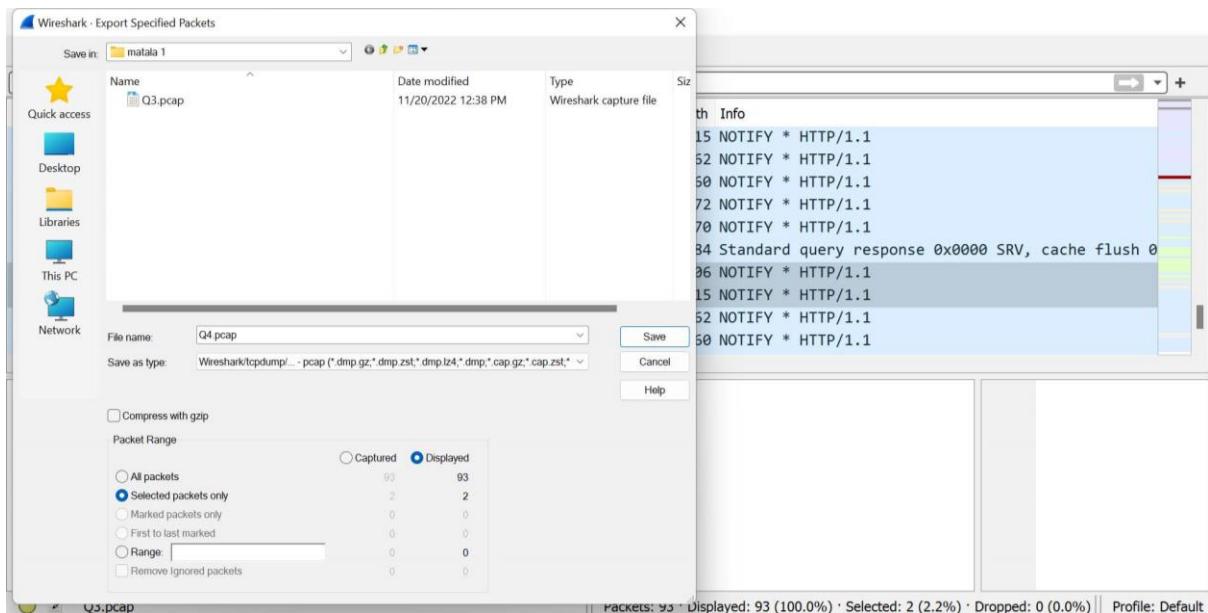
\* ניתן לראות את סוג הפורמט איפה שרשום "Export as"

## תרגיל 4:

נבחר שתי חבילות לבחירתנו



איפה שרשום "selected packets only" נבחר באפשרות "packet range" ונשמור



## תרגיל 5:

בהגדרות קיימת אפשרות להפעיל “Promiscuous mode” .

סביר על אפשרות זו:

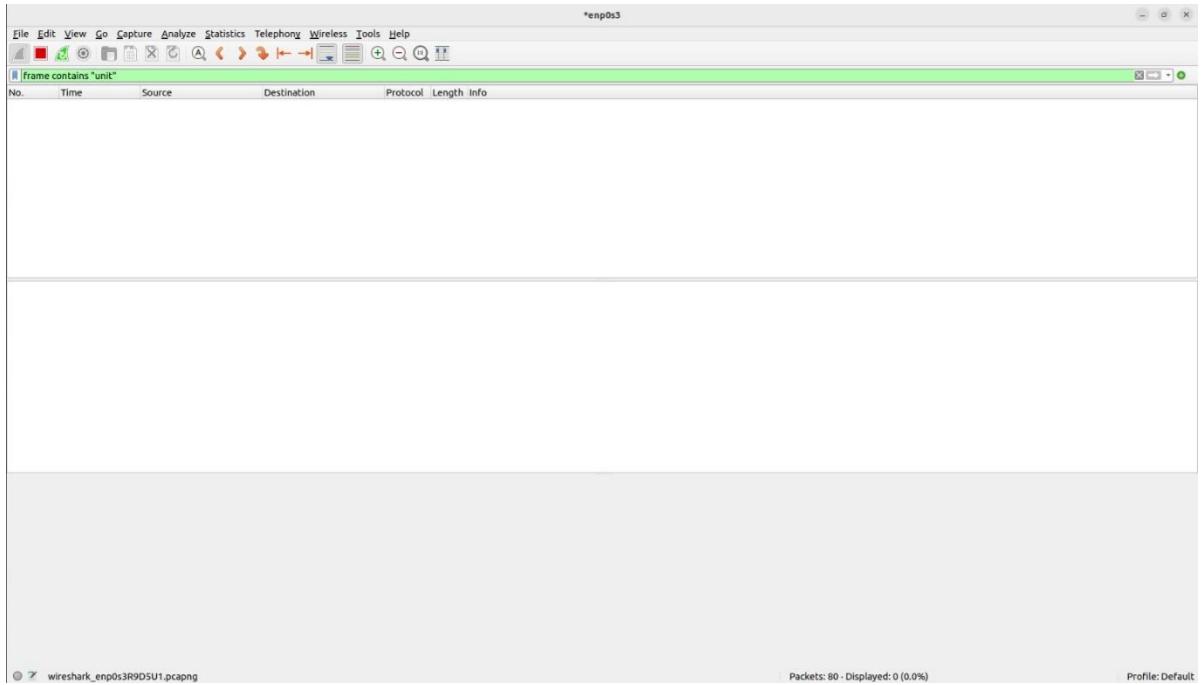
הכרטיס רשות לפltr את ה-frames שמיועדות אליו (ה-e-frame) או לאו (ה-frame) היא השכבה האחורונה לפני שמייעד מועבר לשכבה הפיזית ומשמשת כיחידה ל传递 מידע בפרוטוקלים).

אם נפעיל את האפשרות “Promiscuous mode” הCards רשות לפltr רק את ה-frames המיועדים אליו, וזה אומר שכל frame שmagua לCards הרשות גם frame שישיכת למחשב אחר, עדין תשתכל ותשמר.

לכן משתמשים בו “Promiscuous mode” כדי לנתח ולתעד את כל התעבורה מאותו רשות, ולא רק את חבילות המידע המיועדות עבור אותו Cards רשות.

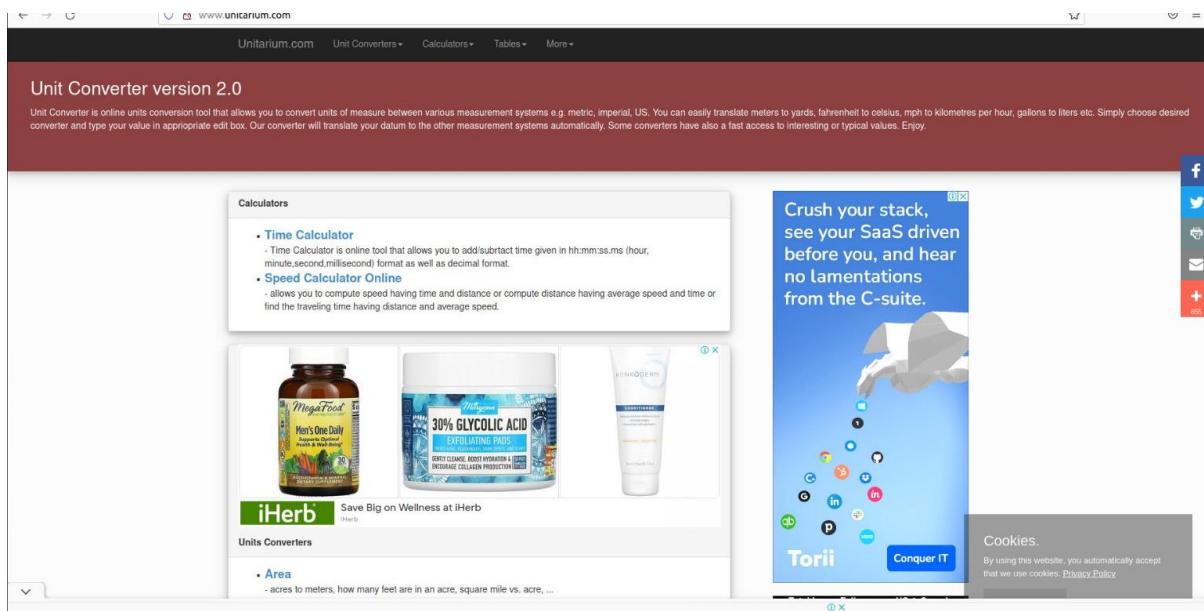
## תרגיל 6:

נפעיל את ה-Wireshark ונרשום בחיפוש “unit”



## תרגיל 9 המשך :

מכאן נכנסו לכתובת : <http://www.unitarium.com>



לאחר מכן נחזור אל ה-Wireshark

A screenshot of the Wireshark application window. The title bar shows "File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help". A search bar at the top has the filter "frame contains 'unit'". The main pane displays a list of network frames. Frame 180 is highlighted in green and expanded to show its details. The details pane shows the frame number, source, destination, protocol (DNS), length (77 bytes), and info (144 Standard query response 0x4803 AAAA unitarium.com SOA ns51.domaincontrol.com). The bytes pane shows the raw hex and ASCII data for this frame. The status pane at the bottom provides frame statistics: 180 frames total, 77 bytes captured, 610 bytes on wire, and 77 bytes displayed.

לאחר שנכנסו לאתר : <http://www.unitarium.com> , נוכל לראות שלאחר שרשמו בchipos "unit" ביצע סינון עבור smcils את המחרוזת "unit".

## תרגיל 7 :

נפעיל את Wireshark ולאחר מכן נכנס אל הכתובת: <http://www.sha1-online.com>

The screenshot shows a Firefox browser window with the URL [www.sha1-online.com](http://www.sha1-online.com) in the address bar. The page title is "SHA1 and other hash functions online generator". There is a search bar with the placeholder "hash" and a dropdown menu set to "sha-1". Below the search bar, there is a link to "SHA-1 MD5 on Wikipedia". At the bottom of the page, there is a banner with the text "We love SPAIN and oldpics.org".

נעזר את ה – Wireshark ונסנן את התעבורה על פי ה프וטוקול HTTP

The screenshot shows the Wireshark application capturing traffic on the interface "enp0s3". The "http" protocol tab is selected. The packet list shows numerous HTTP requests and responses between various IP addresses, primarily 10.0.2.15 and 93.184.220.29. The details and bytes panes show the structure of the captured packets.

## תרגיל 7 המשך :

נזהה את חבילות הבקשה ואת חבילות התגובה לבקשת

No.	Time	Source	Destination	Protocol	Length	Info	מזהה לבקשת
13	8.166840114	10.0.2.15	34.107.221.82	HTTP	35	351 REST /canonical.html HTTP/1.1	מזהה לבקשת
19	8.246740020	34.197.221.82	10.0.2.15	HTTP	352	357 GET /success.txt?ipv4 HTTP/1.1	מזהה לבקשת
40	8.359204915	10.0.2.15	34.107.221.82	HTTP	279	279 HTTP/1.1 200 OK (text/plain)	בשורה
47	8.418751335	34.107.221.82	10.0.2.15	HTTP	47	471 Request	בשורה
51	8.429833923	10.0.2.15	72.246.151.16	OCSP	942	942 Response	מזהה לבקשת
55	8.437363624	72.246.151.16	10.0.2.15	OCSP	171	171 Response	מזהה לבקשת
111	8.471030743	34.107.221.82	10.0.2.15	OCSP	853	853 Response	
116	8.829336105	93.184.229.29	10.0.2.15	OCSP	478	478 Request	
170	1.298309572	10.0.2.15	93.184.229.29	OCSP	852	852 Response	
174	1.365521589	93.184.229.29	10.0.2.15	OCSP	405	405 GET / HTTP/1.1	
256	3.744812460	10.0.2.15	94.23.157.180	HTTP	185	185 GET /index.html HTTP/1.1	
270	3.744812460	94.23.157.180	10.0.2.15	HTTP	303	303 GET /index.html HTTP/1.1	
272	3.744812460	10.0.2.15	84.121.17.100	HTTP	728	728 HTTP/1.1 200 OK (text/css)	
279	4.012189963	94.23.157.180	10.0.2.15	HTTP	371	371 GET /cc.silk tide.com/cookieconsent.latest.min.js HTTP/1.1	
283	4.095622863	10.0.2.15	52.216.1.251	HTTP	603	603 HTTP/1.1 403 Forbidden	
290	4.253450943	52.216.1.251	10.0.2.15	HTTP/XML	364	364 GET /favicon.ico HTTP/1.1	
292	4.482063865	10.0.2.15	94.23.157.180	HTTP	1728	1728 HTTP/1.1 200 OK (image/vnd.microsoft.icon)	
307	4.474273218	94.23.157.180	10.0.2.15	HTTP			

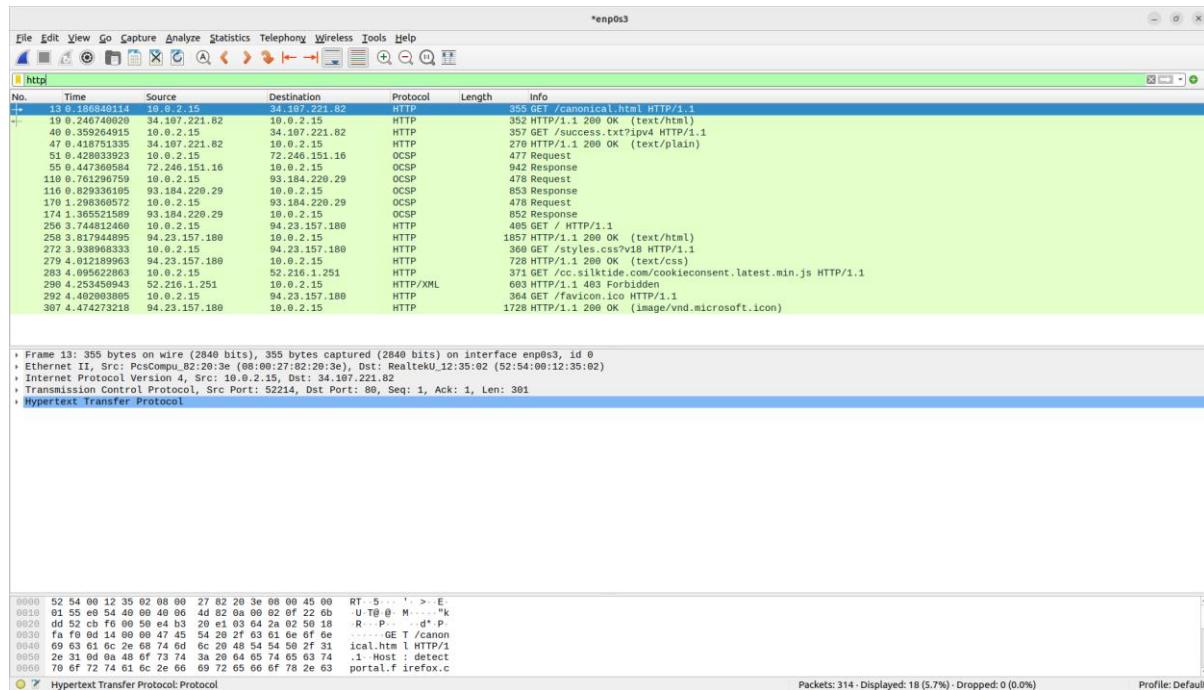
\* חבילות הבקשה מודגשות בצבע כחול

\* חבילות התגובה לבקשת מודגשות בצבע צהוב

\* בתמונה מוסבר איך זיהנו את חבילות הבקשה וחבילות התגובה לבקשת

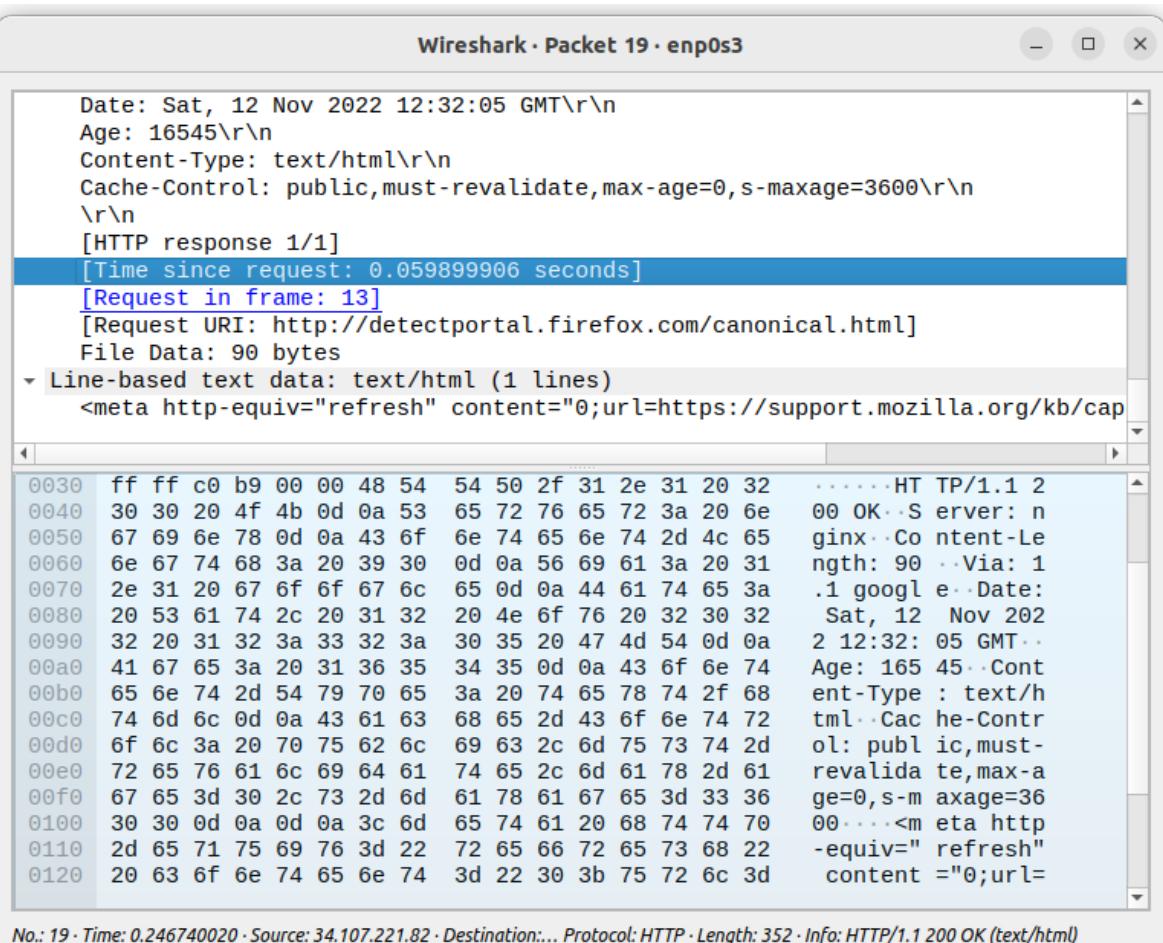
## תרגיל 8 :

נזהה חבילת בקשה ונבחר אותה



0.05989990 Sec: 1.8 הזמן שנקח לחבילת התגובה להגעה לאחר חבילת הבקשה הוא:

\* נכנסו לחבילת התגובה של חבילת הבקשה, שנסוביר על זה בסעיף 4.



No.: 19 · Time: 0.246740020 · Source: 34.107.221.82 · Destination:... · Protocol: HTTP · Length: 352 · Info: HTTP/1.1 200 OK (text/html)

Close

Help

## HTTP/1.1 : HTTP – גרסה ה-2.8

Wireshark · Packet 13 · enp0s3

```

> Ethernet II, Src: PcsCompu_82:20:3e (08:00:27:82:20:3e), Dst: RealtekU_12:35:01 (08:00:27:82:20:3e)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82
> Transmission Control Protocol, Src Port: 52214, Dst Port: 80, Seq: 1, Ack: 1, Len: 301
  Hypertext Transfer Protocol
    GET /canonical.html HTTP/1.1
      Host: detectportal.firefox.com\r\n
      User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:106.0) Gecko/20100101
      Accept: */*\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Cache-Control: no-cache\r\n
      Pragma: no-cache\r\n
      Connection: keep-alive\r\n

```

Time	Source	Destination	Protocol	Length	Info
00:00.000000	fa f0 0d 14 00 00 47 45	54 20 2f 63 61 6e 6f 6e	.....GE T /canon		
00:04.000000	69 63 61 6c 2e 68 74 6d	6c 20 48 54 54 50 2f 31	ical.htm l HTTP/1		
00:05.000000	2e 31 0d 0a 48 6f 73 74	3a 20 64 65 74 65 63 74	.1..Host : detect		
00:06.000000	70 6f 72 74 61 6c 2e 66	69 72 65 66 6f 78 2e 63	portal.f irefox.c		
00:07.000000	6f 6d 0d 0a 55 73 65 72	2d 41 67 65 6e 74 3a 20	om..User -Agent:		
00:08.000000	4d 6f 7a 69 6c 6c 61 2f	35 2e 30 20 28 58 31 31	Mozilla/ 5.0 (X11		
00:09.000000	3b 20 55 62 75 6e 74 75	3b 20 4c 69 6e 75 78 20	; Ubuntu ; Linux		
00:0a.000000	78 38 36 5f 36 34 3b 20	72 76 3a 31 30 36 2e 30	x86_64; rv:106.0		
00:0b.000000	29 20 47 65 63 6b 6f 2f	32 30 31 30 30 31 30 31	) Gecko/ 20100101		
00:0c.000000	20 46 69 72 65 66 6f 78	2f 31 30 36 2e 30 0d 0a	Firefox /106.0..		
00:0d.000000	41 63 63 65 70 74 3a 20	2a 2f 2a 0d 0a 41 63 63	Accept: */...Acc		
00:0e.000000	65 70 74 2d 4c 61 6e 67	75 61 67 65 3a 20 65 6e	ept-Lang uage: en		
00:0f.000000	2d 55 53 2c 65 6e 3b 71	3d 30 2e 35 0d 0a 41 63	-US,en;q =0.5..Ac		
01:00.000000	63 65 70 74 2d 45 6e 63	6f 64 69 6e 67 3a 20 67	cept-Enc oding: g		
01:10.000000	7a 69 70 2c 20 64 65 66	6c 61 74 65 0d 0a 43 61	zip, def late..Ca		
01:20.000000	63 68 65 2d 43 6f 6e 74	72 6f 6c 3a 20 6e 6f 2d	che-Cont rol: no-		

Help Close

## PcsCompu\_82:20:3e : המכשיר ממנה הבצעה הבקשה : 3.8

File Edit View Go Capture Analysis Statistics Telephony Wireless Tools Help

enp0s3

http

No.	Time	Source	Destination	Protocol	Length	Info
1	13:0.186840114	10.0.2.15	34.107.221.82	HTTP	355	GET /canonical.html HTTP/1.1
2	13:0.246740620	34.107.221.82	10.0.2.15	HTTP	352	HTTP/1.1 200 OK (text/html)
3	40:0.359264915	10.0.2.15	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
4	40:0.360000000	34.107.221.82	10.0.2.15	HTTP	242	HTTP/1.1 200 OK (text/plain)
5	0:0.428633923	10.0.2.15	72.246.151.16	OCSP	477	Request
5	0:0.428633923	10.0.2.15	72.246.151.16	OCSP	942	Response
55	0:0.447360584	72.246.151.16	10.0.2.15	OCSP	478	Request
55	0:0.447360584	72.246.151.16	10.0.2.15	OCSP	942	Response
110	0:0.712967579	10.0.2.15	93.184.228.29	OCSP	478	Request
110	0:0.712967579	10.0.2.15	93.184.228.29	OCSP	853	Response
116	0:0.829336189	93.184.228.29	10.0.2.15	OCSP	478	Request
170	1:0.285366070	10.0.2.15	93.184.228.29	OCSP	853	Response
170	1:0.285366070	10.0.2.15	93.184.228.29	OCSP	478	Request
256	3:0.744812469	10.0.2.15	94.23.157.180	HTTP	405	GET / HTTP/1.1
256	3:0.744812469	10.0.2.15	94.23.157.180	HTTP	1857	HTTP/1.1 200 OK (text/html)
258	3:0.817944889	94.23.157.180	10.0.2.15	HTTP	728	HTTP/1.1 200 OK (text/css)
277	3:0.938968333	10.0.2.15	94.23.157.180	HTTP	360	GET /styles.css?v18 HTTP/1.1
279	4:0.012189963	94.23.157.180	10.0.2.15	HTTP	728	HTTP/1.1 200 OK (text/css)
283	4:0.095622883	10.0.2.15	52.216.1.251	HTTP	371	GET /cc.silktide.com/cookieconsent.latest.min.js HTTP/1.1
290	4:0.253458943	52.216.1.251	10.0.2.15	HTTP/XML	603	HTTP/1.1 403 Forbidden
292	4:0.402983880	10.0.2.15	94.23.157.180	HTTP	364	GET /favicon.ico HTTP/1.1
307	4:0.4742723218	94.23.157.180	10.0.2.15	HTTP	1728	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

device name

Frame 13: 355 bytes captured (2840 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu\_82:20:3e (08:00:27:82:20:3e), Dst: RealtekU\_12:35:02 (08:00:27:82:20:3e)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82
 Transmission Control Protocol, Src Port: 52214, Dst Port: 80, Seq: 1, Ack: 1, Len: 301
 Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
0000	52.54.00.12.35.02.08.00	27.82.20.08.00.05.00	RT-5 .. ' > E			
0010	01.55.e9.54.40.00.40.00	4d.82.0a.00.02.0f.22.6b	U T@ M ... "k			
0020	dd.52.cb.f4.00.50.e4.b3	26.e1.03.64.2b.02.59.18	R .. P .. d" P			
0030	fa.f8.0d.14.99.99.47.43	54.29.10.61.64.66.2f.31	.....GE T /canon			
0040	00.00.00.00.00.00.00.00	3a.20.48.54.65.66.2f.31	ical.htm l HTTP/1.1			
0050	2e.31.0d.0a.48.6f.73.74	3a.29.64.65.74.65.63.74	.1..Host : detect			
0060	70.7f.72.74.61.6c.66.78	69.72.65.66.78.2e.63	portal.f irefox.c			

Hypertext Transfer Protocol: Protocol

Packets: 314 - Displayed: 18 (5.7%) - Dropped: 0 (0.0%) Profile: Default

## 4.8 נראה היכן נמצא חבילה התגובה של חבילת הבקשה

Frame 19: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface enp0s3, id 0

Ethernet II, Src: Realetek\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_82:26:3e (08:00:27:82:26:3e)

Internet Protocol Version 4, Src: 34.107.221.82, Dst: 10.0.2.15

TCP, Src Port: 52214, Dst Port: 80

HTTP/1.1 200 OK (text/html)

Content-Type: text/html; charset=UTF-8

Content-Length: 1728

Connection: keep-alive

Cache-Control: private

Server: Apache/2.4.18 (Ubuntu)

Set-Cookie: PHPSESSID=...; expires=Thu, 21 Oct 2021 07:53:49 GMT; path=/; domain=.silktide.com; HttpOnly; Secure

...

Frame (frame), 352 bytes

שנמצא מצד שמאל



\* נזהה זאת בעזרת הסימן :

## 5.8 פורט היעד של החבילה (Destination Port)

Time to Live: 64

Protocol: TCP (6)

Header Checksum: 0x4d82 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.0.2.15

Destination Address: 34.107.221.82

Transmission Control Protocol, Src Port: 52214, Dst Port: 80, Seq: 1, Ack: 1, Len: 301

Source Port: 52214

Destination Port: 80

[Stream index: 0]

[Conversation completeness: Incomplete, DATA (15)]

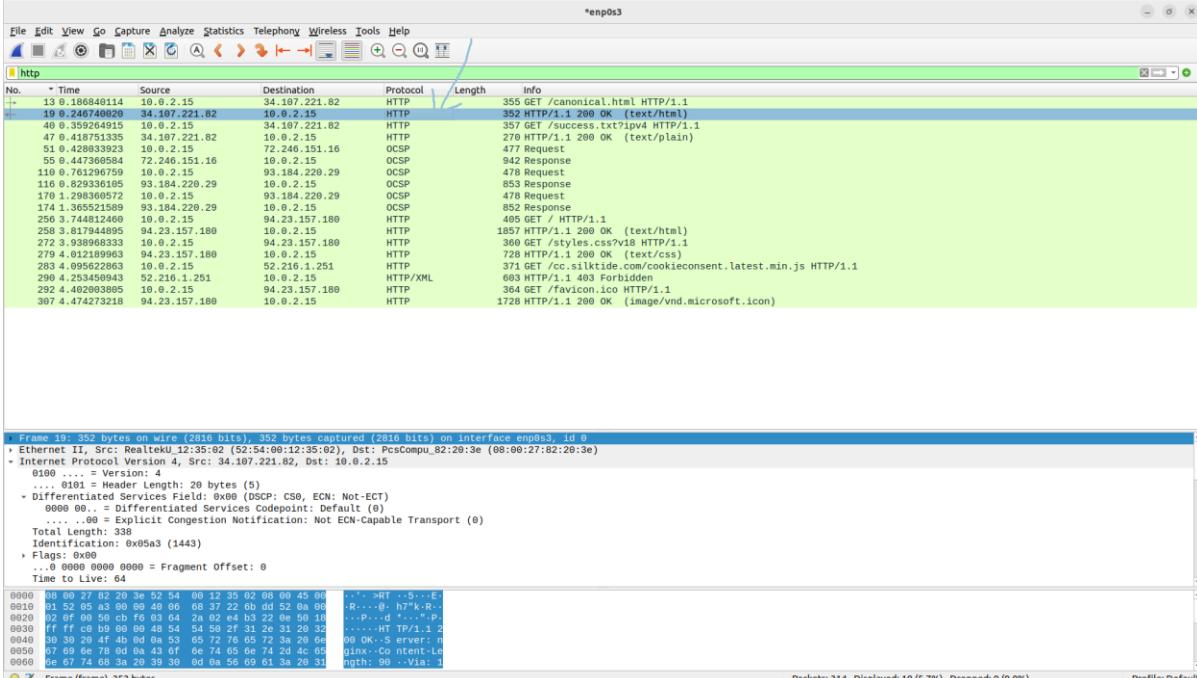
[TCP Segment Len: 301]

Sequence Number: 1 (relative sequence number)

0020	dd 52 cb f6 00 50	e4 b3 20 e1 03 64 2a 02 50 18	.R...P... .d*.P.
0030	fa f0 0d 14 00 00	47 45 54 20 2f 63 61 6e 6f 6e	.....GE T /canon
0040	69 63 61 6c 2e 68	74 6d 6c 20 48 54 54 50 2f 31	ical.htm l HTTP/1
0050	2e 31 0d 0a 48 6f	73 74 3a 20 64 65 74 65 63 74	.1..Host : detect
0060	70 6f 72 74 61 6c	2e 66 69 72 65 66 6f 78 2e 63	portal.f irefox.c
0070	6f 6d 0d 0a 55 73	65 72 2d 41 67 65 6e 74 3a 20	om..User -Agent:
0080	4d 6f 7a 69 6c 6c	61 2f 35 2e 30 20 28 58 31 31	Mozilla/ 5.0 (X11
0090	3b 20 55 62 75 6e	74 75 3b 20 4c 69 6e 75 78 20	; Ubuntu ; Linux
00a0	78 38 36 5f 36 34	3b 20 31 30 36 2e 30	x86_64; rv:106.0
00b0	29 20 47 65 63 6b	6f 2f 32 30 31 30 30 31 30 31	) Gecko/ 20100101
00c0	20 46 69 72 65 66	6f 78 2f 31 30 36 2e 30 0d 0a	Firefox /106.0..
00d0	41 63 63 65 70 74	3a 20 2a 0d 0a 41 63 63	Accept: */*..Acc
00e0	65 70 74 2d 4c 61	6e 67 75 61 67 65 3a 20 65 6e	ept-Lang uage: en
00f0	2d 55 53 2c 65 6e	3b 71 3d 30 2e 35 0d 0a 41 63	-US,en;q =0.5..Ac
0100	63 65 70 74 2d 45	6e 63 6f 64 69 6e 67 3a 20 67	cept-Enc oding: g
0110	7a 69 70 2c 20 64	65 66 6c 61 74 65 0d 0a 43 61	zip, def late..Ca

## תרגיל 9:

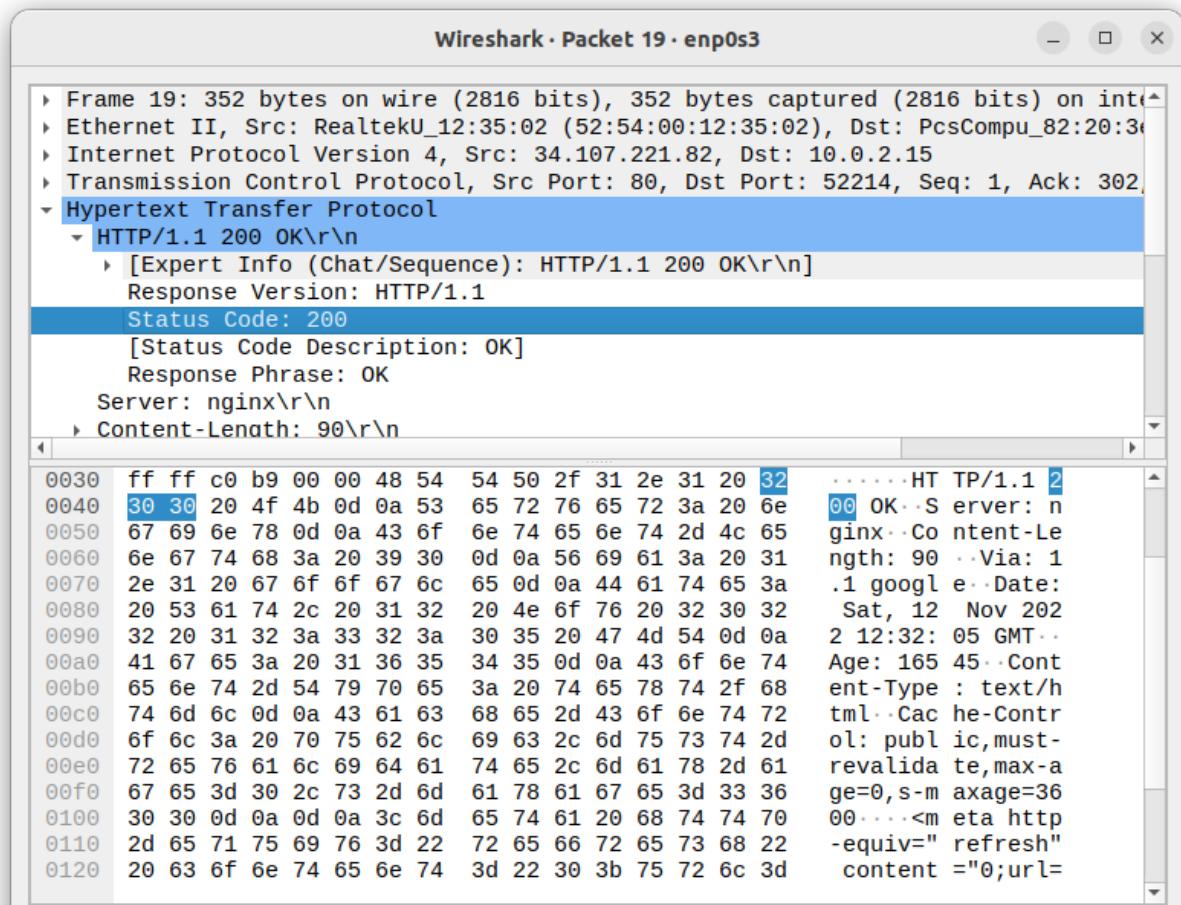
### נזהה את חבילת התגובה



The screenshot shows the Wireshark interface with the following details:

- Packets:** 314 - Displayed: 18 (5.7%) - Dropped: 0 (0.0%)
- Profile:** Default
- Selected Packet:** Frame 19: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface enp0s3, id 0
- Frame Details:**
  - Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_82:20:3e (08:00:27:82:20:3e)
  - Internet Protocol Version 4, Src: 34.107.221.82, Dst: 10.0.2.15
  - Transmission Control Protocol, Src Port: 80, Dst Port: 52214, Seq: 1, Ack: 302
  - Hypertext Transfer Protocol
    - HTTP/1.1 200 OK\r\n
    - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    - Response Version: HTTP/1.1
    - Status Code: 200
    - [Status Code Description: OK]
    - Response Phrase: OK
    - Server: nginx\r\n
    - Content-Length: 90\r\n
- Selected Hex Data:** 00 00 27 02 20 3e 52 54 00 12 35 02 00 00 45 00 .R..>T ..5..E.  
0010 01 52 05 a3 00 00 49 06 68 37 22 6b dd 52 0a 00 ..R...@ h7'k-R.  
0020 02 0f 00 59 cb f6 03 04 28 02 e4 b3 22 0e 50 18 ..P...d \*...P.  
0030 ff ff c0 b9 00 00 48 54 54 50 2f 31 2e 31 20 32 187 HTTP/1.1 200 OK (text/html)  
0040 6e 67 74 68 3a 20 39 30 65 72 76 65 72 3a 20 6e 360 GET /success.txt?ipv4 HTTP/1.1  
0050 67 69 6e 78 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 728 HTTP/1.1 200 OK (text/css)  
0060 6e 67 74 68 3a 20 39 30 52 210.1.251 371 GET /cc.silk tide.com/cookieconsent.latest.min.js HTTP/1.1  
0070 2e 31 20 67 6f 6f 67 6c 65 0d 0a 44 61 74 65 3a 603 HTTP/1.1 403 Forbidden  
0080 20 53 61 74 2c 20 31 32 20 4e 6f 76 20 32 30 32 364 GET /favicon.ico HTTP/1.1  
0090 32 20 31 32 3a 33 32 3a 30 35 20 47 4d 54 0d 0a 1728 HTTP/1.1 200 OK (image/vnd.microsoft.icon)  
00a0 41 67 65 3a 20 31 36 35 34 35 0d 0a 43 6f 6e 74 1857 HTTP/1.1 200 OK (text/html)  
00b0 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 360 GET /styles.css?v18 HTTP/1.1  
00c0 74 6d 6c 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 270 HTTP/1.1 200 OK (text/css)  
00d0 6f 6c 3a 20 70 75 62 6c 69 63 2c 6d 75 73 74 2d 371 GET /cc.silk tide.com/cookieconsent.latest.min.js HTTP/1.1  
00e0 72 65 76 61 6c 69 64 61 74 65 2c 6d 61 78 2d 61 603 HTTP/1.1 403 Forbidden  
00f0 67 65 3d 30 2c 73 2d 6d 61 78 61 67 65 3d 33 36 364 GET /favicon.ico HTTP/1.1  
0100 30 30 0d 0a 0d 0a 3c 6d 65 74 61 20 68 74 74 70 00...<m eta http-equiv="refresh" content ="0;url=1  
0110 2d 65 71 75 69 76 3d 22 72 65 66 72 65 73 68 22  
0120 20 63 6f 6e 74 65 6e 74 3d 22 30 3b 75 72 6c 3d  
0130 6e 67 74 68 3a 20 39 30 6d 0a 56 69 61 3a 20 31 1728 HTTP/1.1 200 OK (image/vnd.microsoft.icon)

### 1.9. מטטוו הקוד של חבילת התגובה (Status Code 200)

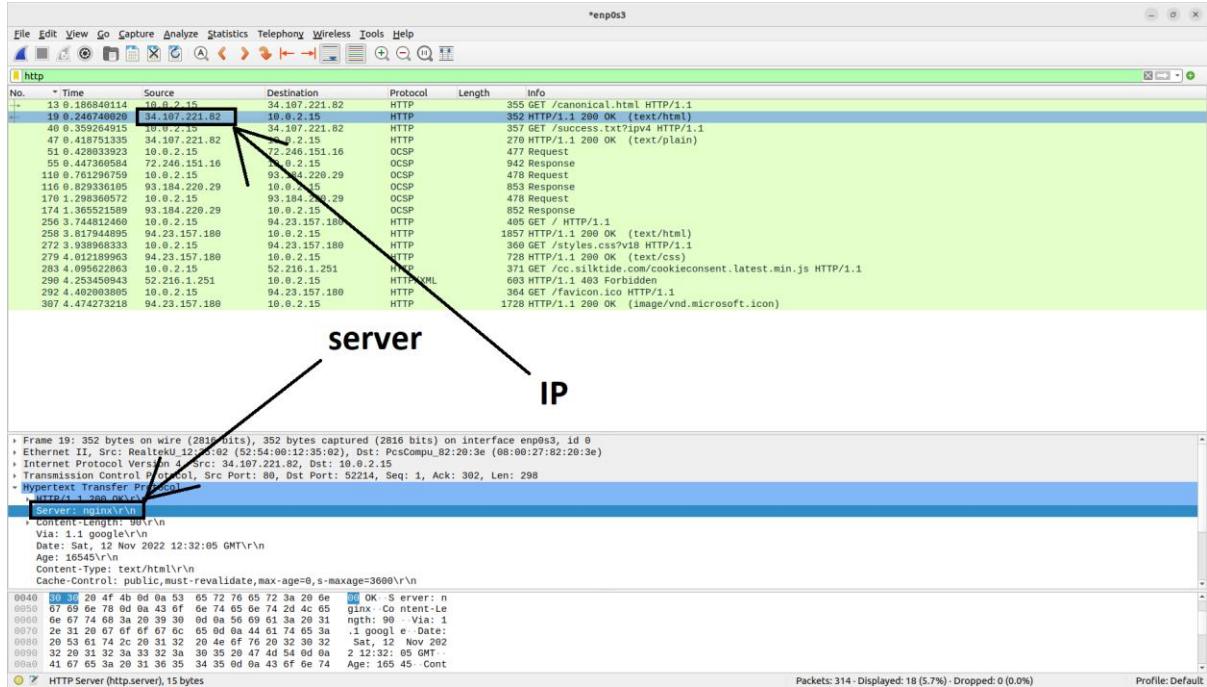


The screenshot shows the Wireshark interface with the following details:

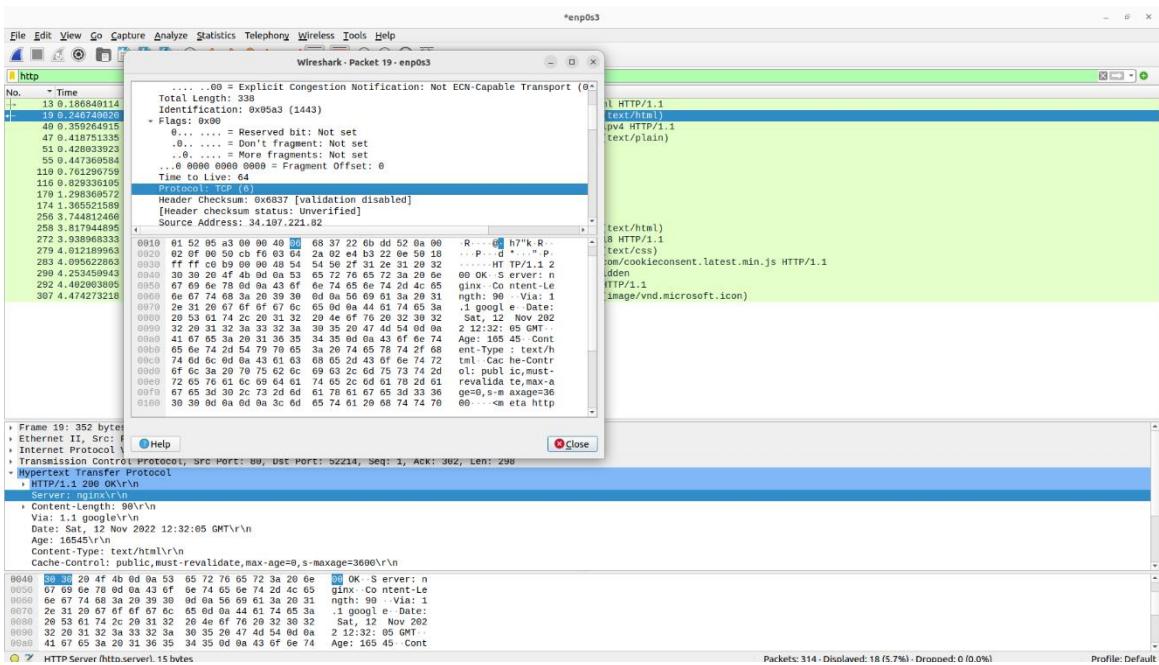
- Packets:** 314 - Displayed: 18 (5.7%) - Dropped: 0 (0.0%)
- Selected Hex Data:** 00 00 27 02 20 3e 52 54 00 12 35 02 00 00 45 00 .R..>T ..5..E.  
0010 01 52 05 a3 00 00 49 06 68 37 22 6b dd 52 0a 00 ..R...@ h7'k-R.  
0020 02 0f 00 59 cb f6 03 04 28 02 e4 b3 22 0e 50 18 ..P...d \*...P.  
0030 ff ff c0 b9 00 00 48 54 54 50 2f 31 2e 31 20 32 187 HTTP/1.1 200 OK (text/html)  
0040 6e 67 74 68 3a 20 39 30 65 72 76 65 72 3a 20 6e 360 GET /success.txt?ipv4 HTTP/1.1  
0050 67 69 6e 78 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 728 HTTP/1.1 200 OK (text/css)  
0060 6e 67 74 68 3a 20 39 30 52 210.1.251 371 GET /cc.silk tide.com/cookieconsent.latest.min.js HTTP/1.1  
0070 2e 31 20 67 6f 6f 67 6c 65 0d 0a 44 61 74 65 3a 603 HTTP/1.1 403 Forbidden  
0080 20 53 61 74 2c 20 31 32 20 4e 6f 76 20 32 30 32 364 GET /favicon.ico HTTP/1.1  
0090 32 20 31 32 3a 33 32 3a 30 35 20 47 4d 54 0d 0a 1728 HTTP/1.1 200 OK (image/vnd.microsoft.icon)  
00a0 41 67 65 3a 20 31 36 35 34 35 0d 0a 43 6f 6e 74 1857 HTTP/1.1 200 OK (text/html)  
00b0 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 360 GET /styles.css?v18 HTTP/1.1  
00c0 74 6d 6c 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 270 HTTP/1.1 200 OK (text/css)  
00d0 6f 6c 3a 20 70 75 62 6c 69 63 2c 6d 75 73 74 2d 371 GET /cc.silk tide.com/cookieconsent.latest.min.js HTTP/1.1  
00e0 72 65 76 61 6c 69 64 61 74 65 2c 6d 61 78 2d 61 603 HTTP/1.1 403 Forbidden  
00f0 67 65 3d 30 2c 73 2d 6d 61 78 61 67 65 3d 33 36 364 GET /favicon.ico HTTP/1.1  
0100 30 30 0d 0a 0d 0a 3c 6d 65 74 61 20 68 74 74 70 00...<m eta http-equiv="refresh" content ="0;url=1  
0110 2d 65 71 75 69 76 3d 22 72 65 66 72 65 73 68 22  
0120 20 63 6f 6e 74 65 6e 74 3d 22 30 3b 75 72 6c 3d  
0130 6e 67 74 68 3a 20 39 30 6d 0a 56 69 61 3a 20 31 1728 HTTP/1.1 200 OK (image/vnd.microsoft.icon)

## 2.9. השרת שמננו התקבלה : nginx .

ה – IP של השרת : 34.107.221.82



## 3.9. כמות החבילות TCP שהו נחצאות כדי להרכיב את החבילה : 6



#### 4.9 סוג ה – connection בין השרת ללקוח : keep-alive

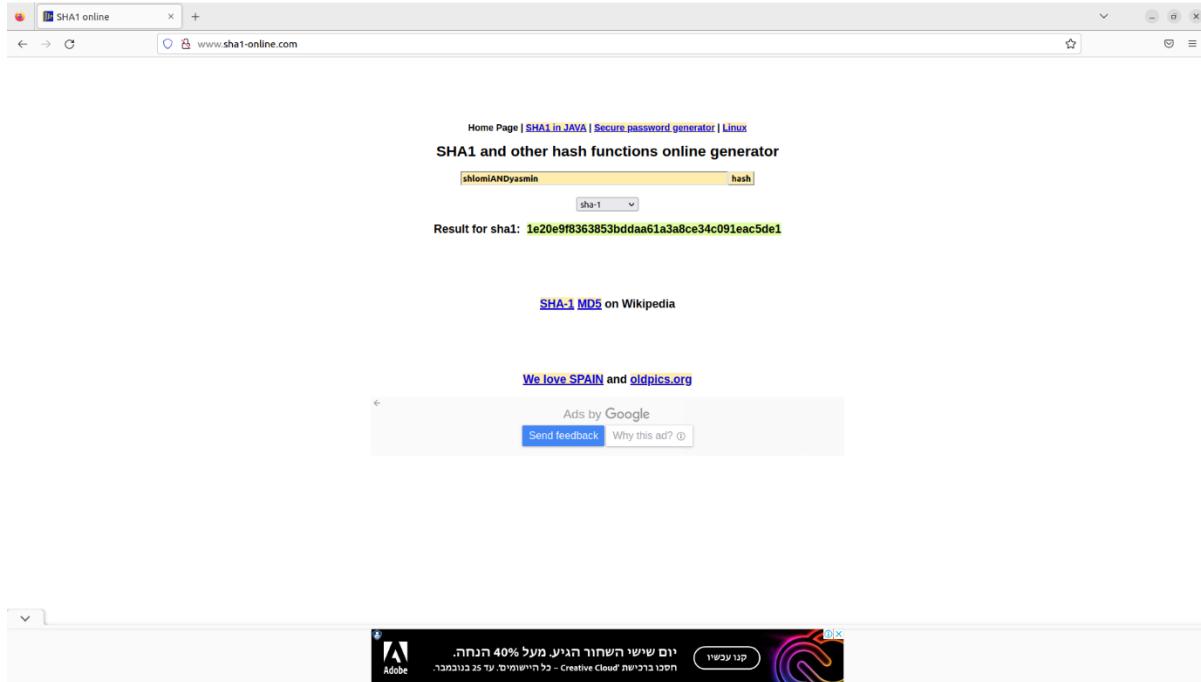
סביר זאת בקצרה , היא מתודת המאפשרת לחבר יחיד של TCP להשאר פתוח עבור מספר של בקשות/תגובה( HTTP persistent connection).

The screenshot shows a Wireshark capture window titled "Wireshark · Packet 13 · Q7-Q8-Q9.pcapng". The packet details pane displays an HTTP request for "/canonical.html" over HTTP/1.1. The "HTTP Headers" section includes the "Connection: keep-alive\r\n" header. The "TCP payload" section shows the raw hex and ASCII data of the request. The status bar at the bottom indicates the packet number (No.: 13), time (Time: 0.186840114), source (Source: 10.0.2.15), destination (Destination: 34...), protocol (Protocol: HTTP), length (Length: 355), and info (Info: GET /canonical.html HTTP/1.1). A "Close" button is visible in the bottom right corner.

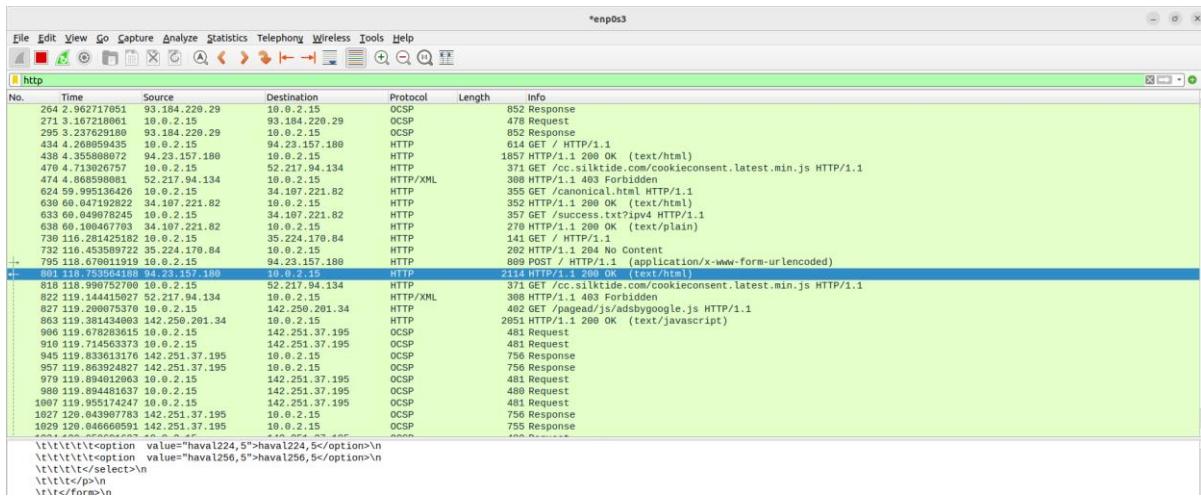
## תרגיל 10 :

בעודנו מפעילים את ה – Wireshark נכנס לאתר : <http://www.sha1-online.com> נרשם את השם שלנו ("shlomiANDyasmin") ולחץ hash (אתר הצפנה לפי "hash") נרשם את השם שלנו ("shlomiANDyasmin") ולחץ hash

נראה את התוצאה של ההצפנה מוגשת בצדוק



## ונחזר אל WireShark



## 1.10. ניתן לראות שהחישוב נעשה על ידי שרת מרוחק ולא על ידי דף

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

- post:** A red arrow points from the word "post" in the text area to the "Method" field of the selected packet (No. 891), which shows "POST".
- חבילת התגובה (Result):** A red arrow points from the word "Result" in the text area to the "Text item (text, 108 bytes)" section, which displays the response body.
- Text item (text, 108 bytes):** The response body contains HTML code, including a select dropdown with options for "haval224" and "haval256", and a link to "http://www.top-places-in-spain.com".
- Frame (2114 bytes): Uncompressed entity body (5027 bytes):** The raw response frame is shown below the text item.
- Packets: 3141 - Displayed: 76 (2.4%):** Statistics at the bottom of the window.
- Profile: Default:** Profile selection at the bottom right.

\* מזהה את חבילת הבקשה לפי הבקשה "post"

\* נמצא את חבילת התגובה שלה ונראה שכן היא ביצעה את החישוב(Result)

## 2.10. הפרמטרים שנשלחו בבקשת ה – HTTP (מסומן במסגרת אדומה)

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

- Host:** A red box highlights the "Host" field of the selected packet (No. 891), which shows "www.shai-online.com".
- User-Agent:** Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:106.0) Gecko/20100101 Firefox/106.0\r\n
- Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8\r\n
- Accept-Language:** en-US;q=0.5\r\n
- Accept-Encoding:** gzip, deflate\r\n
- Content-Type:** application/x-www-form-urlencoded\r\n
- Content-Length:** 110\r\n
- Origin:** http://www.shai-online.com\r\n
- Connection:** keep-alive\r\n
- Referer:** http://www.shai-online.com/\r\n
- Cookie:** \_gads=ID:050be056ea40c28-22335a5528d70063:T=1668535215:RT=1668535215:S=ALNI\_Mb\_S0FyJHUTE8kgaKok15FvcSxbw; \_\_gpi=UID=00000b20bf23a702:T=1668535215:RT=1668535215:S=ALNI\_MYU-ADg6RCwTr1h6kGKh5; Upgrade-Insecure-Requests: 1\r\n
- pA4A-Up grade-In:** A red box highlights the "pA4A-Up grade-In" field in the status bar at the bottom.
- Packets: 3173 - Displayed: 78 (2.5%):** Statistics at the bottom of the window.
- Profile: Default:** Profile selection at the bottom right.

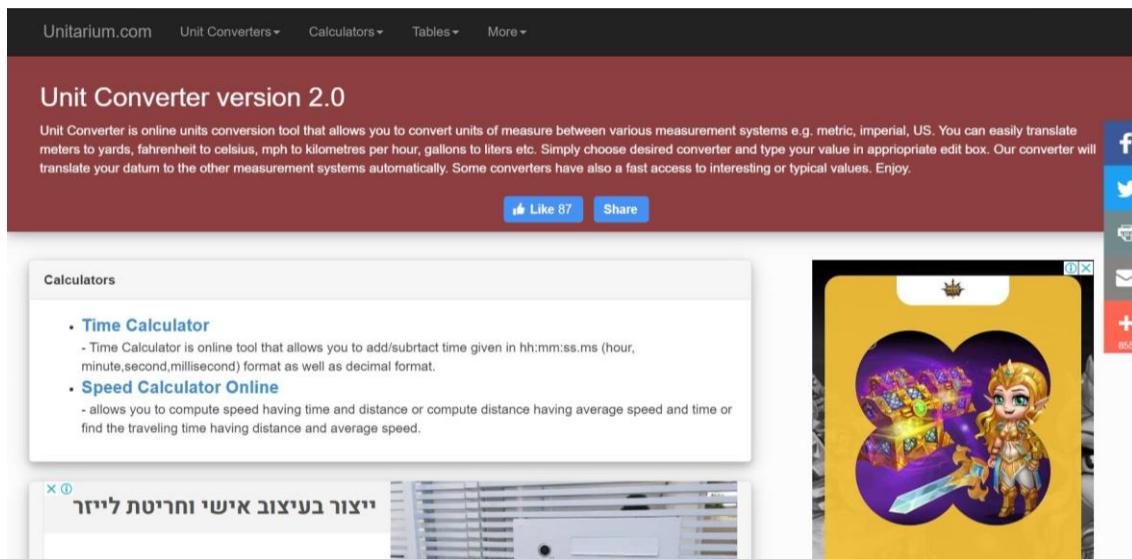
**3.10.** היה צריך לבצע את התקשרות HTTP מכיוון, שבבקשת HTTP מוגדר משאבי שהדף מכיר ותומך בהן (למשל הדף דן תומך בשפה האנגלית וכו'..) , אם לא היינו יוצרים תקשורת HTTPS והיינו נתונים לצד הלוקוח לבצע את החישוב, היה יכול לקרוטה שהדף של הלוקוח לא היה תומך בסוג התוכן (שפה, סוג קובץ וכו'..) ווותם ביצענו את העברת המשאבי מהשרת שזה לוקח לנו זמן מיותר, בנוסף החישוב מצד הלוקוח מגדיל עלויות (bandwidth).

**4.10.** נסביר את הסיכון האפשרי בלבצע את החישוב בשרת מרוחק ולא דרך הדף דן המקומי:

כל מי שמחובר לרשות שלנו יכול לעקוב אחרי התעבורה. לאחר שהשרת המרוחק מסיים את החישוב של ההצעה, הוא שולח לנו את חבילת התגובה שבה ניתן לראות את התוכן שהוא שלח לנו, אך כל מי שמחובר לרשות שלנו יכול לעקוב אחרי התעבורה ולהכנס למידע התוכן של חבילת התגובה.

## תרגיל 11 :

נכנו לאתר : <http://www.unitarium.com>



לאחר מכן נחזיר אל Wireshark ונבצע follow http stream

\*לפניהם נשלחו מהלך : חבילת בקשה אחת (באדום)

\*לפי התמונה נשלחו מהשרת : חבילת תגובה אחת (בכחול)

\*לפי התמונה נראה שככל חבילת התגובה מהשרת, נקבל file text/HTML

Wireshark - Follow HTTP Stream (tcp.stream eq 5) - enp0s3

GET / HTTP/1.1  
Host: www.unitarium.com  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:106.0) Gecko/20100101 Firefox/106.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Cookie: \_\_atuvc=2%7C45%2C2%7C46; \_\_ga=GA1.2.1877245389.1668176669; \_\_gads=ID=595b4bb0353d961a-224c8b7022d704d:RT=1668176669:S=ALNI\_MbMNAUMB8agVrrfKuQypkHNgxSa7A; \_\_gpi=UID=00000b1e5320fa4b:RT=1668176669:ST=1668610310:S=ALNI\_Mb925K-C806X\_bGL5I\_opSb83BC2g; \_\_atuvs=6374f905fa9ba214001; \_\_gid=GA1.2.944908805.1668610310  
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK  
Date: Wed, 16 Nov 2022 14:55:51 GMT  
Server: Apache  
Upgrade: h2, h2c  
Connection: Upgrade, Keep-Alive  
Vary: Accept-Encoding  
Content-Encoding: gzip  
Content-Length: 4902  
Keep-Alive: timeout=5  
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">  
<html>  
<head>  
<title>Unit Converter</title>  
<meta name="description" content="Units of Measurement Converter/Calculator translates value given in one unit system to other systems of measurement. Our converters do their job automatically when you type." />  
<meta name="keywords" content="unit,measure,measurement,converter,calculator,length,temperature,volume,speed" />  
<link rel="canonical" href="http://www.unitarium.com">  
<meta property="og:url" content="http://www.unitarium.com" />  
<meta property="og:type" content="website" />  
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />  
<meta http-equiv="Content-Language" content="en" />  
<meta name="robots" content="noopd">  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<meta name="viewport" content="width=device-width, initial-scale=1">  
<link href="/netdna.bootstrapcdn.com/bootstrap/3.1.1/css/bootstrap.min.css" rel="stylesheet">  
<script src="https://ajax.googleapis.com/ajax/libs/jquery/2.1.3/jquery.min.js"></script>  
<link rel="stylesheet" href="css/2018.css" />  
<script async src="pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script>  
<script>  
 (adsbygoogle = window.adsbygoogle || []).push({  
 google\_ad\_client: "ca-pub-3566458821250586",  
 enable\_page\_level\_ads: true  
 })  
</script>

client packet : 1  
server packet : 1

Entire conversation (20 KB)

Show data as ASCII

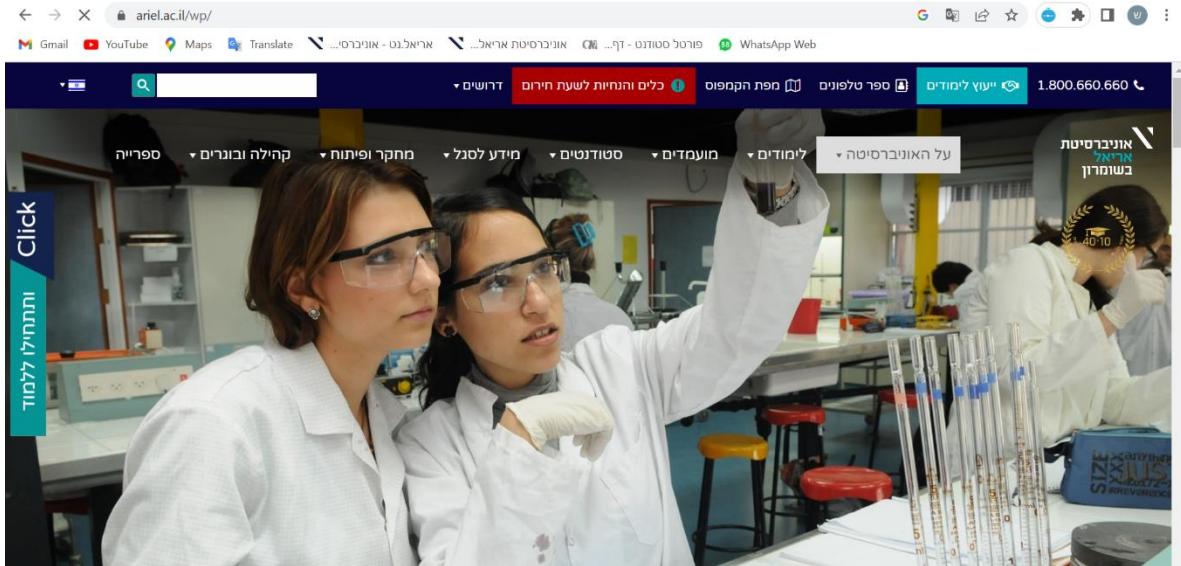
Find Next

Filter Out This Stream Print Save as... Back Close

Help

## תרגיל 12 :

נכנו לאתר [http מסויים](https://www.ariel.ac.il/wp) לבחירתנו : [/https://www.ariel.ac.il/wp](https://www.ariel.ac.il/wp)



נחזיר אל ה-IP Wireshark, וنعשה filter עבור ה-IP של האתר (IP=34.96.118.58)

A screenshot of the Wireshark application. The title bar says 'ip.src == 34.96.118.58'. The main window displays a list of network packets. The first few packets are TCP SYN and ACK segments. Then, at frame 6733, a TLSv1.3 'Server Hello, Change Cipher Spec' packet is shown. This packet contains the server's chosen cipher suite. Below the packet list is a hex dump of the selected cipher's parameters. The bottom status bar shows the file name 'wireshark\_Wi-Fi4KNQV1.pcapng', the number of packets (20836), the displayed range (3379), and the profile (Default). The system tray shows the date and time as 11/17/2022 21:31 PM.

\* ניתן לראות בתמונה את חבילת הבקשה ב프וטוקול TLSv1.3

\* הלקוח שלח בקשה אל השירות (server hello, change cipher spec)

\* בעצם בקשה עברו "לחיצת ידיהם" בין הלקוח לשרת

## תרגיל 12 המשך :

נבחר חבילת שרשום אצלם ב/info "Application Data" (מוסמן במסגרת שחורה)

The screenshot shows a Wireshark interface with a list of network packets. A specific packet is highlighted with a black rectangle. The details pane shows the protocol as TLSv1.3 and the content as '483 Application Data'. The bytes pane shows the raw hex and ASCII data for this packet.

The screenshot shows a detailed view of a selected packet (Frame 6759) in Wireshark. The Transport Layer Security section is expanded, showing TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol. The bytes pane shows the raw data for this application layer segment.

\***פרוטוקול TLS**, בפועל עד שכבה שתפקידה הוא אבטחה

\***ניתן לראות שהפרוטוקול של המידע באפליקציה הוא HTTP (מוסמן בתמונה)**

\***קיבלנו את המידע של האפליקציה אבל ניתן לראות שהמידע מוצפן**

מכאן נוכל להסיק שבactually היה פה תקשורת בקשה ותגובה והפרוטוקול של האפליקציה הוא HTTP, נשים לב שהימ"ט עוד שכבה (TLS) שבactually מabitח את המידע והוא שומרת על המידע (מפני ציטותים, גורם זדוני וכו') בעזרת הצפנה .

## תרגיל 13 :

ניתן להשתמש במילת החיפוש nslookup (ב-CMD) לביצוע שאלות  
מ长时间内，我们可以在CMD中使用nslookup命令来执行查询。例如，要在CMD中使用nslookup命令来执行查询。

```
C:\Users\2shlo>nslookup icecream.com
Server: Box.Home
Address: 192.168.14.1

Non-authoritative answer:
Name: icecream.com
Address: 151.101.195.10

C:\Users\2shlo>
```

\*שם השרת שנutan תשובה לשאלתה הוא : icecream.com

\*שרת זה אינו שרת מהימן (non-authoritative answer)

\*כתובת ה- IP עבור הדומיין : 151.101.195.10

## תרגיל 14 :

**1.14.** נבצע שוב את השאלה רק שהפעם ה- Wireshark מופעל

No.	Time	Source	Destination	Protocol	Length	Info
45	1.524029	192.168.68.106	192.168.14.1	DNS	90	Standard query 0xeacc A smartscreen-p
46	1.542119	192.168.14.1	192.168.68.106	DNS	218	Standard query response 0xeacc A smar
333	29.474902	192.168.68.106	192.168.14.1	DNS	85	Standard query 0x0001 PTR 1.14.168.19
334	29.482825	192.168.14.1	192.168.68.106	DNS	107	Standard query response 0x0001 PTR 1.
335	29.484401	192.168.68.106	192.168.14.1	DNS	72	Standard query 0x0002 A icecream.com
336	29.489984	192.168.14.1	192.168.68.106	DNS	88	Standard query response 0x0002 A iced
337	29.492423	192.168.68.106	192.168.14.1	DNS	72	Standard query 0x0003 AAAA icecream.c
338	29.634588	192.168.14.1	192.168.68.106	DNS	152	Standard query response 0x0003 AAAA i
831	53.314249	192.168.68.106	192.168.14.1	DNS	82	Standard query 0xc90d A client.wns.wi
832	53.331796	192.168.14.1	192.168.68.106	DNS	141	Standard query response 0xc90d A clie
974	54.878607	192.168.68.106	192.168.14.1	DNS	75	Standard query 0x06ef A windows.msn.c
976	54.897122	192.168.14.1	192.168.68.106	DNS	150	Standard query response 0x06ef A wind
1089	55.946547	192.168.68.106	192.168.14.1	DNS	74	Standard query 0x9fd7 A assets.msn.co
1091	55.965840	192.168.14.1	192.168.68.106	DNS	199	Standard query response 0x9fd7 A asse
1125	56.364449	192.168.68.106	192.168.14.1	DNS	71	Standard query 0x3f8d A www.msn.com

ניתן לראות שקיים 3 שאלות עבורי הדומיין icecream.com (מודגשים בתמונה)

**2.14.** נסביר את ההבדל בין שלושת הדומיינים:

הראשון הוא מסוג **ptr** קלומר pointer : היכולת של רשומה זו היא למפות כתובות IP לשם.

השני מסוג **A** קלומר address : היכולת של רשומה זו היא למפות שם לכתובת IP.

השלישי מסוג **AAAA** : היכולת למפות שם לכתובת IPv6

**3.14.** נבחר את השאלה הבאה (מסומן בתמונה)

No.	Time	Source	Destination	Protocol	Length	Info
45	1.524029	192.168.68.106	192.168.14.1	DNS	90	Standard query 0xeacc A smartscreen-p
46	1.542119	192.168.14.1	192.168.68.106	DNS	218	Standard query response 0xeacc A smar
333	29.474902	192.168.68.106	192.168.14.1	DNS	85	Standard query 0x0001 PTR 1.14.168.19
334	29.482825	192.168.14.1	192.168.68.106	DNS	107	Standard query response 0x0001 PTR 1.
335	29.484401	192.168.68.106	192.168.14.1	DNS	72	Standard query 0x0002 A icecream.com
336	29.489984	192.168.14.1	192.168.68.106	DNS	88	Standard query response 0x0002 A iced
337	29.492423	192.168.68.106	192.168.14.1	DNS	72	Standard query 0x0003 AAAA icecream.c
338	29.634588	192.168.14.1	192.168.68.106	DNS	152	Standard query response 0x0003 AAAA i
831	53.314249	192.168.68.106	192.168.14.1	DNS	82	Standard query 0xc90d A client.wns.wi
832	53.331796	192.168.14.1	192.168.68.106	DNS	141	Standard query response 0xc90d A clie
974	54.878607	192.168.68.106	192.168.14.1	DNS	75	Standard query 0x06ef A windows.msn.c
976	54.897122	192.168.14.1	192.168.68.106	DNS	150	Standard query response 0x06ef A wind
1089	55.946547	192.168.68.106	192.168.14.1	DNS	74	Standard query 0x9fd7 A assets.msn.co
1091	55.965840	192.168.14.1	192.168.68.106	DNS	199	Standard query response 0x9fd7 A asse
1125	56.364449	192.168.68.106	192.168.14.1	DNS	71	Standard query 0x3f8d A www.msn.com

פורט יעד השאלתה שנשלחה הוא : 53 (מוסמן בתמונה במסגרת אדומה)

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

**dns**

No.	Time	Source	Destination	Protocol	Length	Info
45	1.524029	192.168.68.106	192.168.14.1	DNS	90	Standard query 0xeacc A smartscreen-p
46	1.542119	192.168.14.1	192.168.68.106	DNS	218	Standard query response 0xeacc A smar
333	29.474902	192.168.68.106	192.168.14.1	DNS	85	Standard query 0x0001 PTR 1.14.168.19
334	29.482825	192.168.14.1	192.168.68.106	DNS	107	Standard query response 0x0001 PTR 1.
335	29.484401	192.168.68.106	192.168.14.1	DNS	72	Standard query 0x0002 A icecream.com
336	29.489984	192.168.14.1	192.168.68.106	DNS	88	Standard query response 0x0002 A iced
337	29.492423	192.168.68.106	192.168.14.1	DNS	72	Standard query 0x0003 AAAA icecream.c
338	29.634588	192.168.14.1	192.168.68.106	DNS	152	Standard query response 0x0003 AAAA i
831	53.314249	192.168.68.106	192.168.14.1	DNS	82	Standard query 0xc90d A client.wns.wi
832	53.331796	192.168.14.1	192.168.68.106	DNS	141	Standard query response 0xc90d A clie
974	54.878607	192.168.68.106	192.168.14.1	DNS	75	Standard query 0x06ef A windows.msn.c
976	54.897122	192.168.14.1	192.168.68.106	DNS	150	Standard query response 0x06ef A wind
1089	55.946547	192.168.68.106	192.168.14.1	DNS	74	Standard query 0x9fd7 A assets.msn.co
1091	55.965840	192.168.14.1	192.168.68.106	DNS	199	Standard query response 0x9fd7 A asse
1125	56.364449	192.168.68.106	192.168.14.1	DNS	71	Standard query 0x3f8d A www.msn.com

```

> Frame 335: 72 bytes on wire (576 bits), 72
| 0000  d8 07 b6 09 f5 2c 98 8d 46 6f 2e d0 08 00 45 00  ....,.. Fo.
| 0010  00 3a 5e 1f 00 00 80 11 00 00 c0 a8 44 6a c0 a8  :^.... ...
| 0020  0e 01 dd 02 00 35 00 26 d3 f3 00 02 01 00 00 01  ....5.& ...
| 0030  00 00 00 00 00 00 08 69 63 65 63 72 65 61 6d 03  .....i cec
| 0040  63 6f 6d 00 00 01 00 01 com.....
Source Port: 56578
Destination Port: 53

```

4.14. ניתן לראות שהחטילה נשלחה דרך פרוטוקול UDP (מוסמן במסגרת שחורה)

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

**dns**

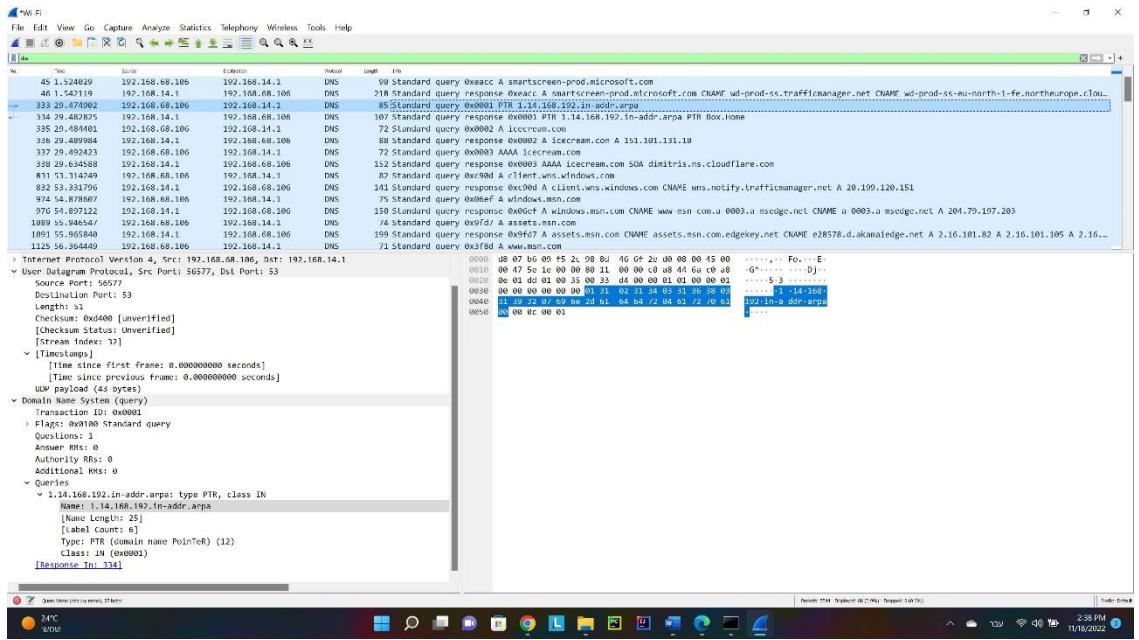
No.	Time	Source	Destination	Protocol	Length	Info
45	1.524029	192.168.68.106	192.168.14.1	DNS	90	Standard query 0xeacc A smartscreen-p
46	1.542119	192.168.14.1	192.168.68.106	DNS	218	Standard query response 0xeacc A smar
333	29.474902	192.168.68.106	192.168.14.1	DNS	85	Standard query 0x0001 PTR 1.14.168.19
334	29.482825	192.168.14.1	192.168.68.106	DNS	107	Standard query response 0x0001 PTR 1.
335	29.484401	192.168.68.106	192.168.14.1	DNS	72	Standard query 0x0002 A icecream.com
336	29.489984	192.168.14.1	192.168.68.106	DNS	88	Standard query response 0x0002 A iced
337	29.492423	192.168.68.106	192.168.14.1	DNS	72	Standard query 0x0003 AAAA icecream.c
338	29.634588	192.168.14.1	192.168.68.106	DNS	152	Standard query response 0x0003 AAAA i
831	53.314249	192.168.68.106	192.168.14.1	DNS	82	Standard query 0xc90d A client.wns.wi
832	53.331796	192.168.14.1	192.168.68.106	DNS	141	Standard query response 0xc90d A clie
974	54.878607	192.168.68.106	192.168.14.1	DNS	75	Standard query 0x06ef A windows.msn.c
976	54.897122	192.168.14.1	192.168.68.106	DNS	150	Standard query response 0x06ef A wind
1089	55.946547	192.168.68.106	192.168.14.1	DNS	74	Standard query 0x9fd7 A assets.msn.co
1091	55.965840	192.168.14.1	192.168.68.106	DNS	199	Standard query response 0x9fd7 A asse
1125	56.364449	192.168.68.106	192.168.14.1	DNS	71	Standard query 0x3f8d A www.msn.com

```

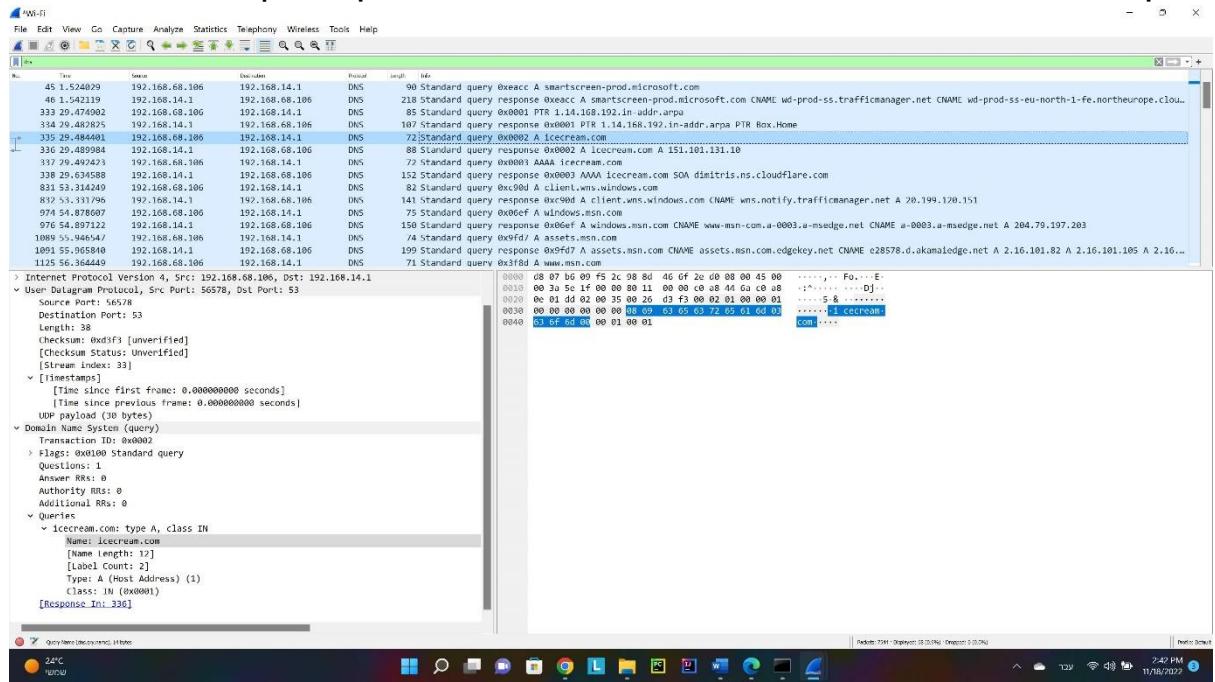
> Frame 335: 72 bytes on wire (576 bits), 72
| 0000  d8 07 b6 09 f5 2c 98 8d 46 6f 2e d0 08 00 45 00  ....,.. Fo.
| 0010  00 3a 5e 1f 00 00 80 11 00 00 c0 a8 44 6a c0 a8  :^.... ...
| 0020  0e 01 dd 02 00 35 00 26 d3 f3 00 02 01 00 00 01  ....5.& ...
| 0030  00 00 00 00 00 00 08 69 63 65 63 72 65 61 6d 03  .....i cec
| 0040  63 6f 6d 00 00 01 00 01 com.....
Source Port: 56578
Destination Port: 53

```

## 5.14 ניתן לראות שהשאילתת נעשתה באופן רקורסיבי, השאלתה הראשונה נשלה אל השרת.in-addr.arpa



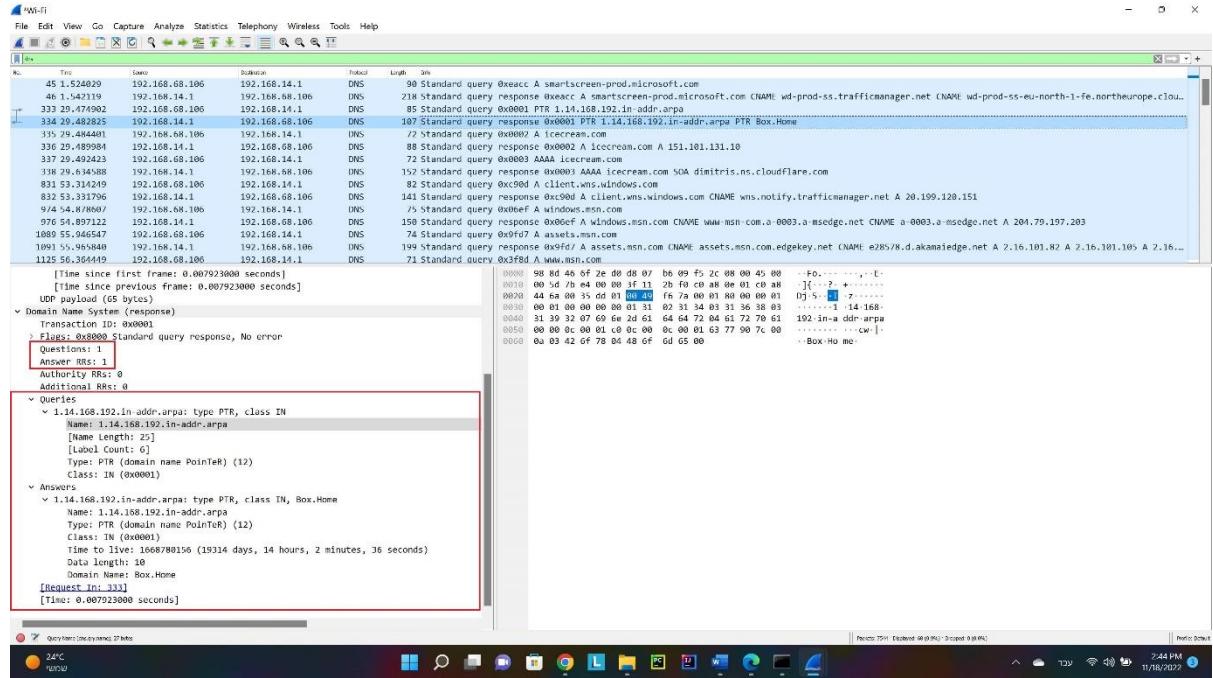
מכאן אנחנו פונים אל השרת "icecream.com" שנמצא בתוך "in-addr.arpa".



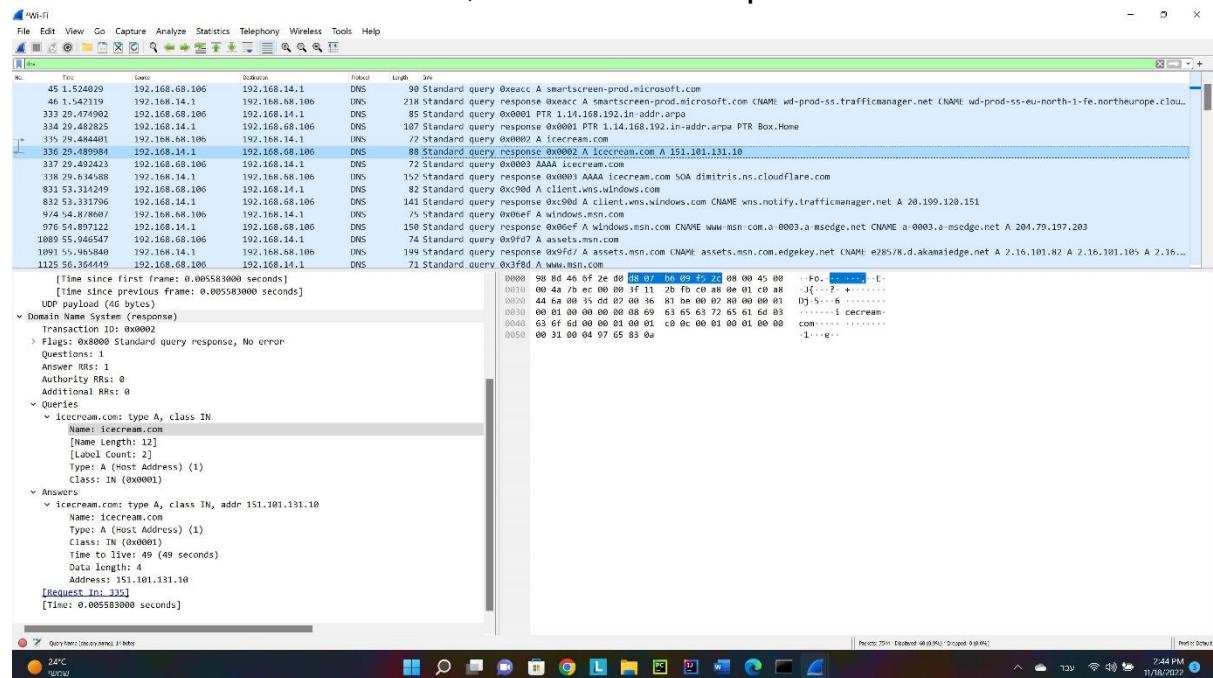
לכן נסיק מכך שזה בוצע באופן רקורסיבי

## 6.14. נסכל על הabilities תגובה לשאילתת response query

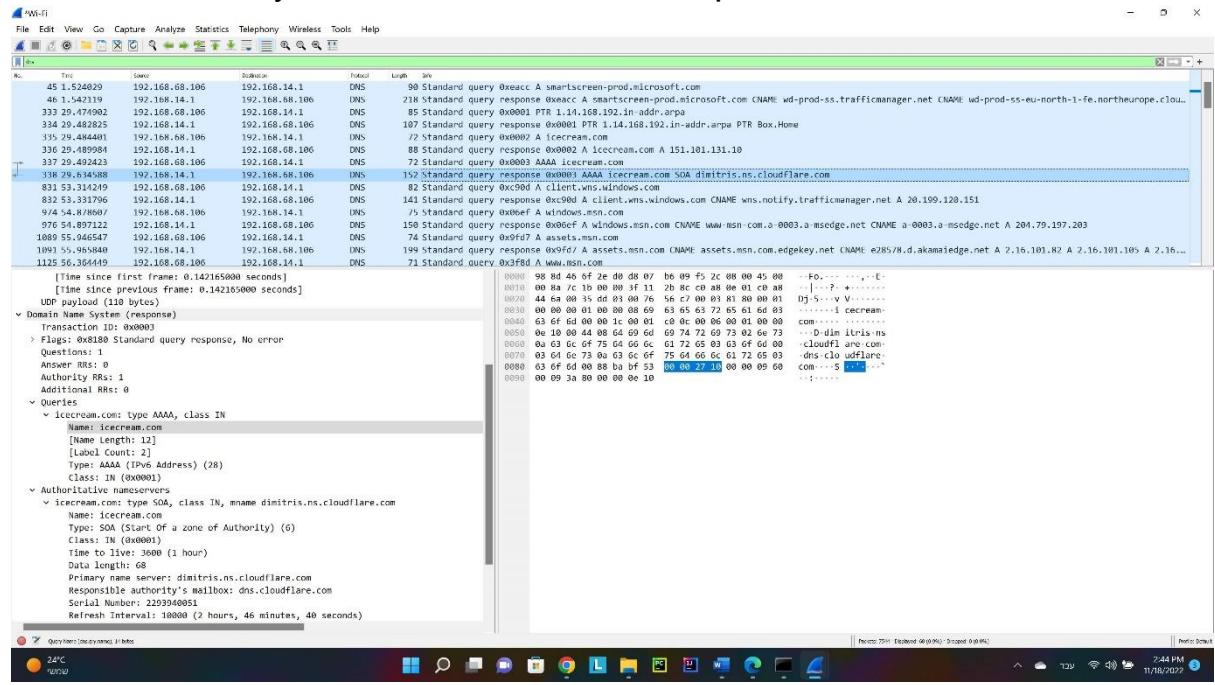
עבור חבילת השאלתה הראשונה קיבלנו תשובה אחת, answer RRS=1



עבור חבילת השאלתה השנייה קיבלנו תשובה אחת, answer RRS=1



## עבור חבילת השאלתה השלישייה קיבלונו תשובה אחת , Authority RRS=1



עכשו נסביר את ההבדלים המהותיים, חבילות התגובה לשאלתה הראשונה והשנייה הם אינם שרתים סמכותיים לעומת התגובה לשאלתה השלישייה שכן היא משרת סמכותי

### 7.14. הבדל בין שאלתה מסוג A לשאלתה מסוג AAAA הוא :

שאילתה מסוג A בעצם מבקשת את הIPv4 משם הדומיין לעומת שאלתה מסוג AAAA שהיא מבקשת את הIPv6 , בנוסף A מחרירה תשובה מהשרת שאינו סמכותי לעומת AAAA שהיא מחרירה תשובה משרת סמכותי.

## תרגיל 15:

נרשום בחילון הפקודות all/ipconfig וניתן שהשתת DNS שיש לנו על המחשב הוא:

DNS servers : 192.168.14.1

```
Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . :
  Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
  Physical Address. . . . . : 98-8D-46-6F-2E-D0
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . : fe80::da87:a32d:9948:bdd6%18(PREFERRED)
  IPv4 Address. . . . . : 192.168.68.106(PREFERRED)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : Friday, November 18, 2022 1:50:40 PM
  Lease Expires . . . . . : Friday, November 18, 2022 4:50:39 PM
  Default Gateway . . . . . :
    192.168.68.1
  DHCP Server . . . . . : 192.168.68.1
  DHCPv6 IAID . . . . . : 160992582
  DHCPv6 Client DUID. . . . . : 00-01-00-01-29-53-D2-A3-98-8D-46-6F-2E-D0
  DNS Servers . . . . . :
    192.168.14.1
    192.168.68.1
  NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
  Description . . . . . : Bluetooth Device (Personal Area Network)
  Physical Address. . . . . : 98-8D-46-6F-2E-D4
  DHCP Enabled . . . . . : Yes
```

## תרגיל 16:

ה-IPv6 של השרת הוא : fe80::da87:a32d:9948:bdd6%18

```
Windows IP Configuration

  Host Name . . . . . : DESKTOP-HJCP53R
  Primary Dns Suffix . . . . . :
  Node Type . . . . . : Hybrid
  IP Routing Enabled. . . . . : No
  WINS Proxy Enabled. . . . . : No

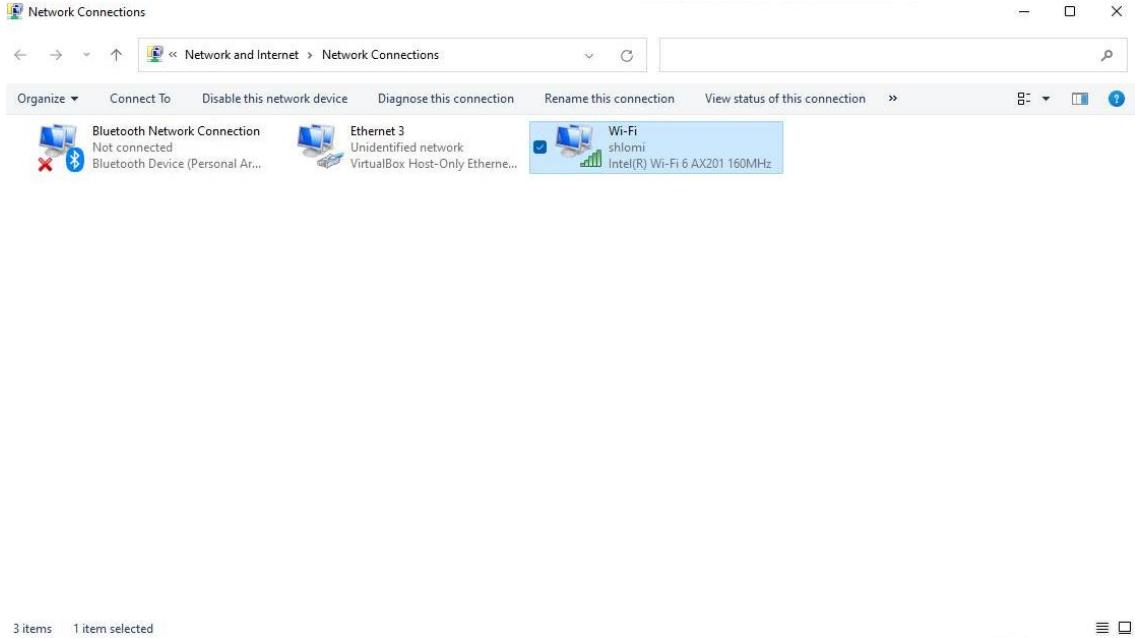
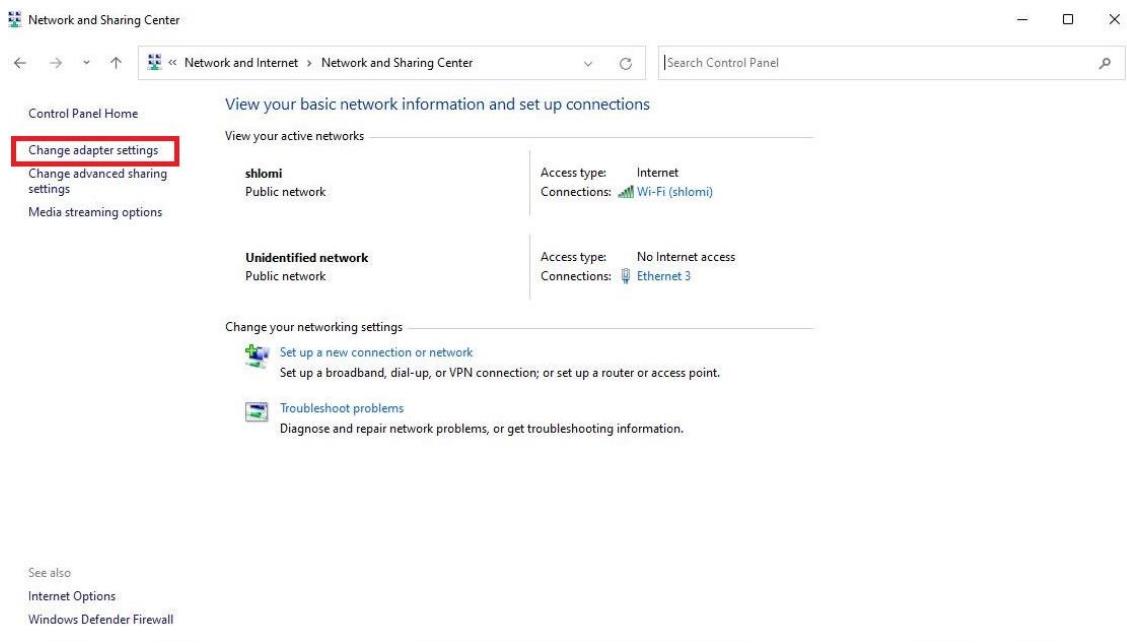
  Ethernet adapter Ethernet 3:
    Connection-specific DNS Suffix . :
    Description . . . . . : VirtualBox Host-Only Ethernet Adapter
    Physical Address. . . . . : 0A-00-27-00-00-05
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . : fe80::5f43:9fac:f470:4f2b%5(PREFERRED)
    Autoconfiguration IPv4 Address. . . : 169.254.45.23(PREFERRED)
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :
    DHCPv6 IAID . . . . . : 688521255
    DHCPv6 Client DUID. . . . . : 00-01-00-01-29-53-D2-A3-98-8D-46-6F-2E-D0
    NetBIOS over Tcpip. . . . . : Enabled

  Wireless LAN adapter Local Area Connection* 3:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
    Physical Address. . . . . : 98-8D-46-6F-2E-D1
    DHCP Enabled. . . . . : Yes
```

## תרגיל 17 :

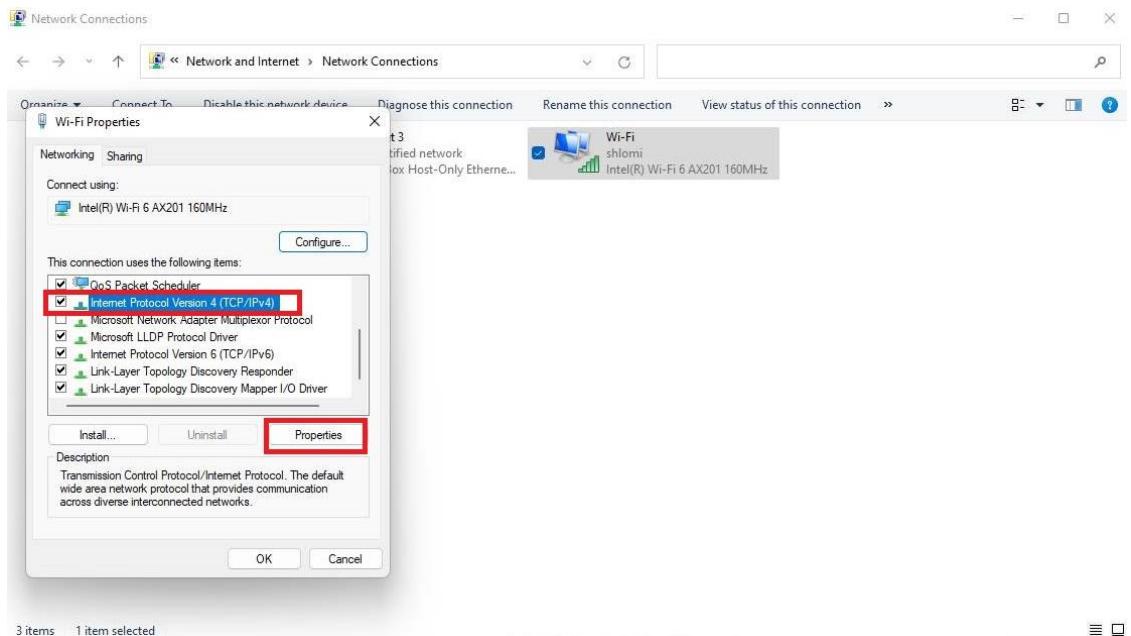
חשוב להכיר את האפשרות לשינוי ההגדרות של שרת ה – DNS, בעצם לבדוק אם הוא מוגדר באופן ידני או אוטומטי.

לשם כך נכנס ללוח הבקרה “Wi-Fi” ← “change adapter setting” ←

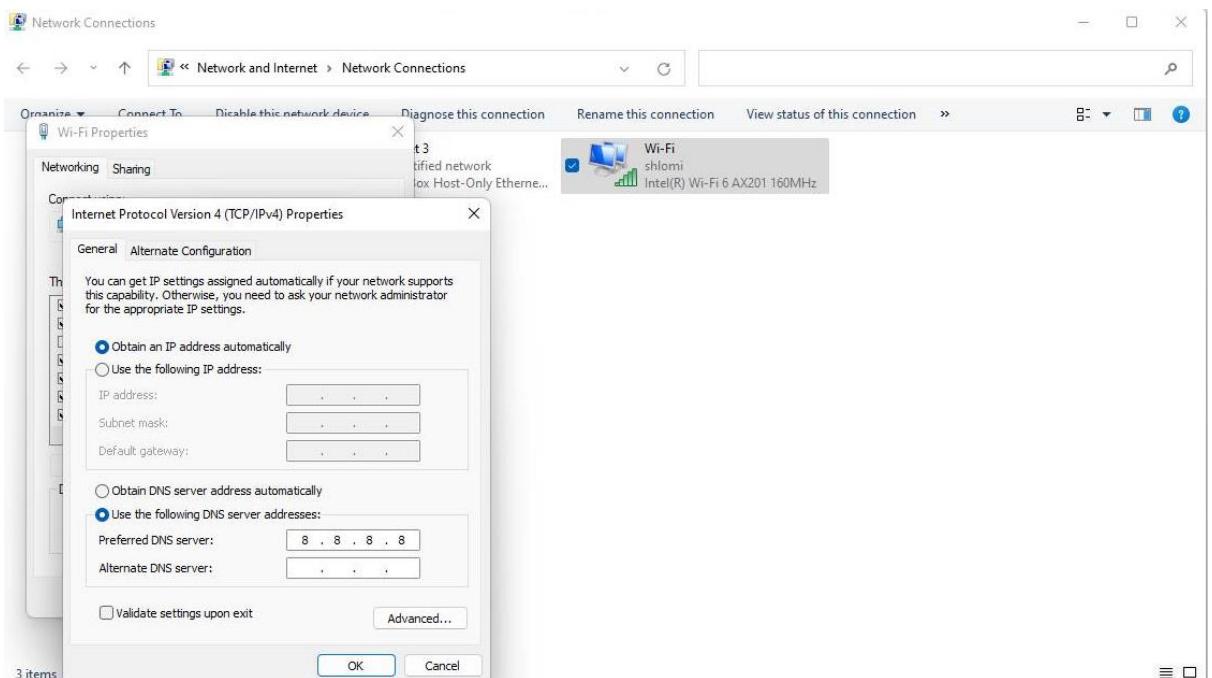


## תרגיל 17 המשך :

נכנו ל “properties” ← “Internet Protocol Version 4 (TCP/IPv4) ← “properties”

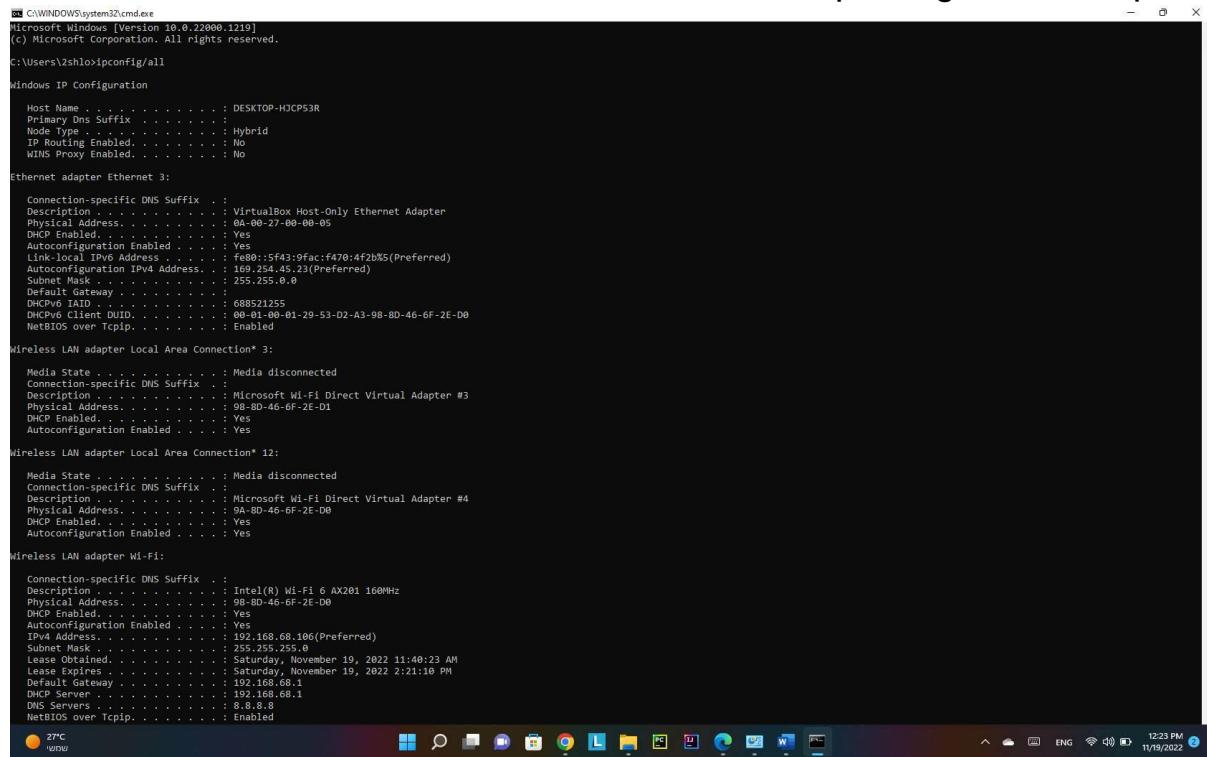


נשנה את כתובות השרת ה – ל – 8.8.8.8 (שרת ה-DNS של גוגל)



## תרגיל 17 המשך :

נבדוק שוב עם ipconfig/all את כתובות שרת ה-DNS שלנו



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.1719]
(c) Microsoft Corporation. All rights reserved.

C:\Users\zhih\>ipconfig/all

Windows IP Configuration

Host Name . . . . . : DESKTOP-HJCP53R
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
Dhcp Enabled . . . . . : No
Dns Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No

Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . . . . . : VirtualBox Host-Only Ethernet Adapter
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address . . . . . : 0A-00-27-00-00-05
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::5f43:9fac:f478:4f2b%5(Preferred)
Autoconfiguration IPv4 Address . . . . . : 169.254.45.23(PREFERRED)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 688521255
DHCPv6 Client OUID . . . . . : 00-01-00-01-29-53-D2-A3-98-8D-46-6F-2E-D0
NetBIOS over Tcpip . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 3:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Physical Address . . . . . : 98-8D-46-6F-2E-D1
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 12:

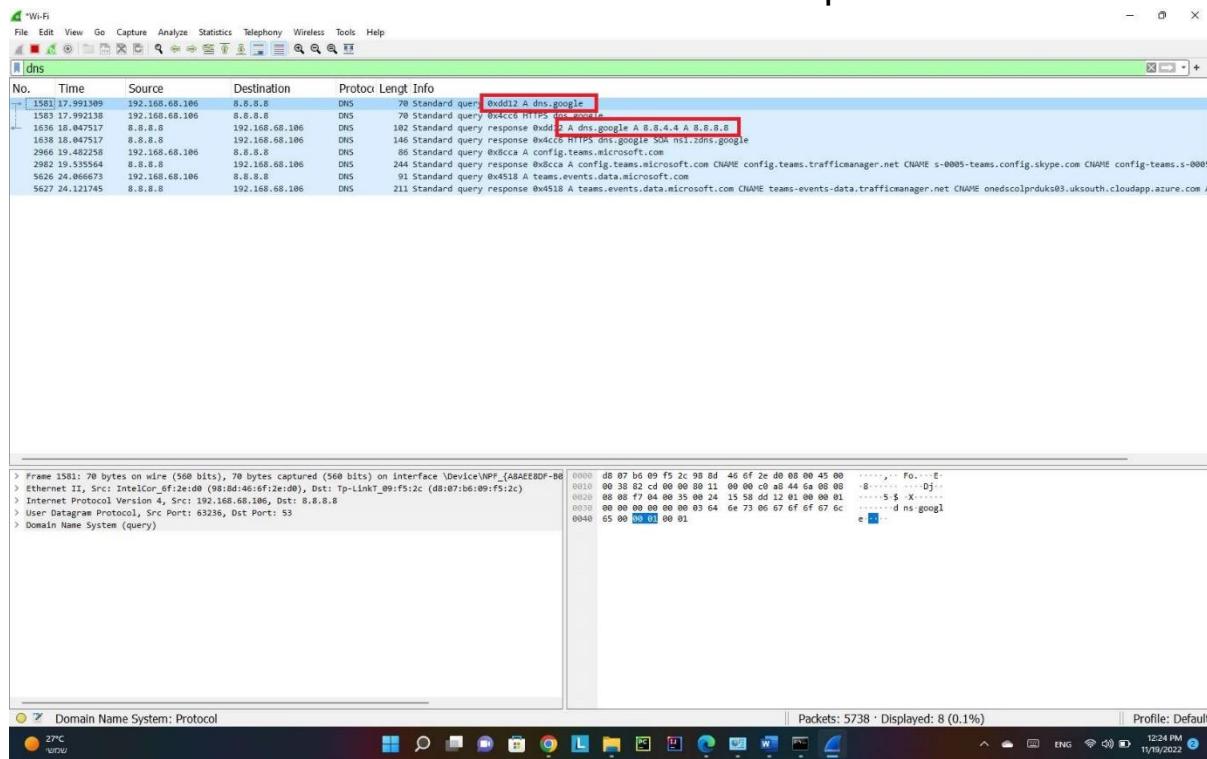
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address . . . . . : 9A-8D-46-6F-2E-D0
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address . . . . . : 98-8D-46-6F-2E-D0
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address . . . . . : 192.168.68.106(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Saturday, November 19, 2022 11:49:23 AM
Lease Expires . . . . . : Saturday, November 19, 2022 2:21:10 PM
Default Gateway . . . . . : 192.168.68.1
DHCP Server . . . . . : 192.168.68.1
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip . . . . . : Enabled

C:\Users\zhih\>
```

נראה עם Wireshark שאקן יש שימוש בשרת ה-DNS של גוגל



## תרגיל 18:

סביר למה חבילת תגובה לשאלתה יותר "כבה" מחייבת השאלתה:  
חבילת השאלתה מכילה את השאלות, לעומת זאת חבילת התגובה גם מכילה את  
השאלות של החבילת השאלתה (היא מעתיקה אותו) וגם מכילה את התשובה  
לשאלתה, אך היא תהיה יותר כבה.

## תרגיל 19:

### 1.19. נכנס לחילון הפקודות ונרשם "ipconfig/displaydns"

```
C:\WINDOWS\system32\cmd.exe
> ipconfig /all
> ipconfig /displaydns

Windows IP Configuration

icecream.com
Record Name . . . . . : icecream.com
Record Type . . . . . : A
Time To Live . . . . . : 230
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 151.101.105.10

Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 230
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 151.101.3.10

Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 230
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 151.101.67.10

Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 230
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 151.101.131.10

array16.prod.do.dsp.mp.microsoft.com
Record Name . . . . . : array16.prod.do.dsp.mp.microsoft.com
Record Type . . . . . : A
Time To Live . . . . . : 1815
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 20.54.79.4

C:\Users\zshlo>
```

### 2.19. ננקה את הרשומה בעזרת dns/ipconfig/flushdns

```
C:\WINDOWS\system32\cmd.exe
Time To Live . . . . . : 8
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . . : 40.126.32.75

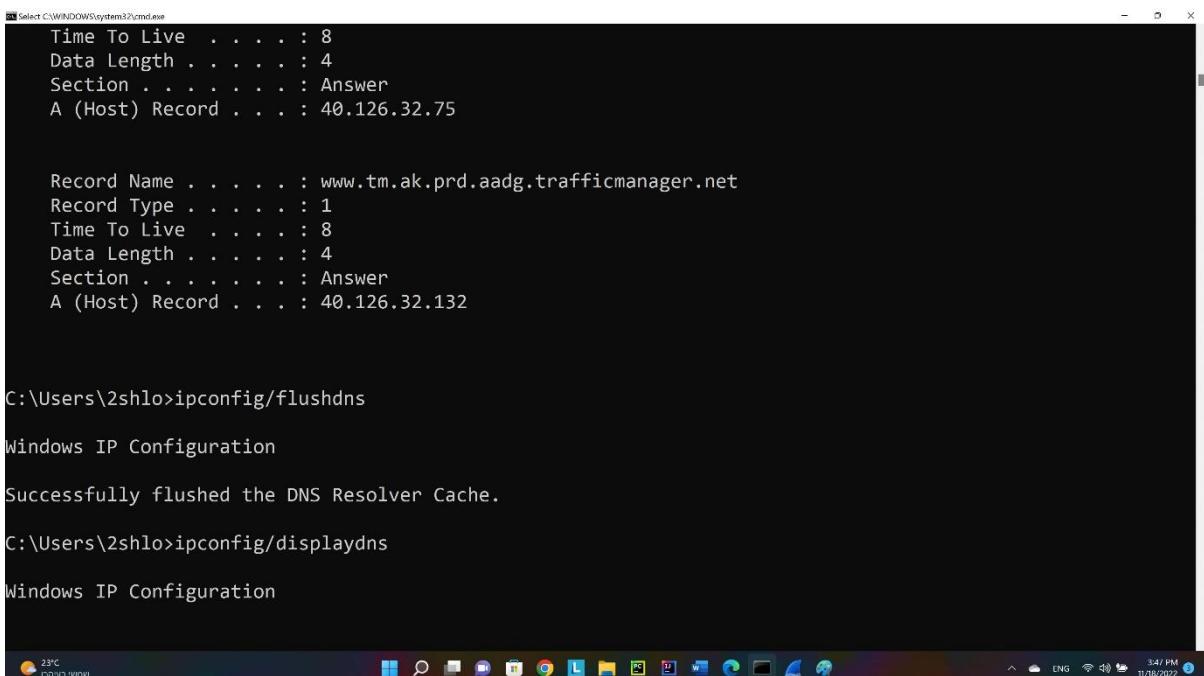
Record Name . . . . . : www.tm.ak.prd.aadg.trafficmanager.net
Record Type . . . . . : 1
Time To Live . . . . . : 8
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . . : 40.126.32.132

C:\Users\zshlo>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

לאחר מכן נרשם שוב את הפקודה ipconfig/displaydns



```
Time To Live . . . . : 8
Data Length . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.75

Record Name . . . . : www.tm.ak.prd.aadg.trafficmanager.net
Record Type . . . . : 1
Time To Live . . . . : 8
Data Length . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 40.126.32.132

C:\Users\2shlo>ipconfig/flushdns

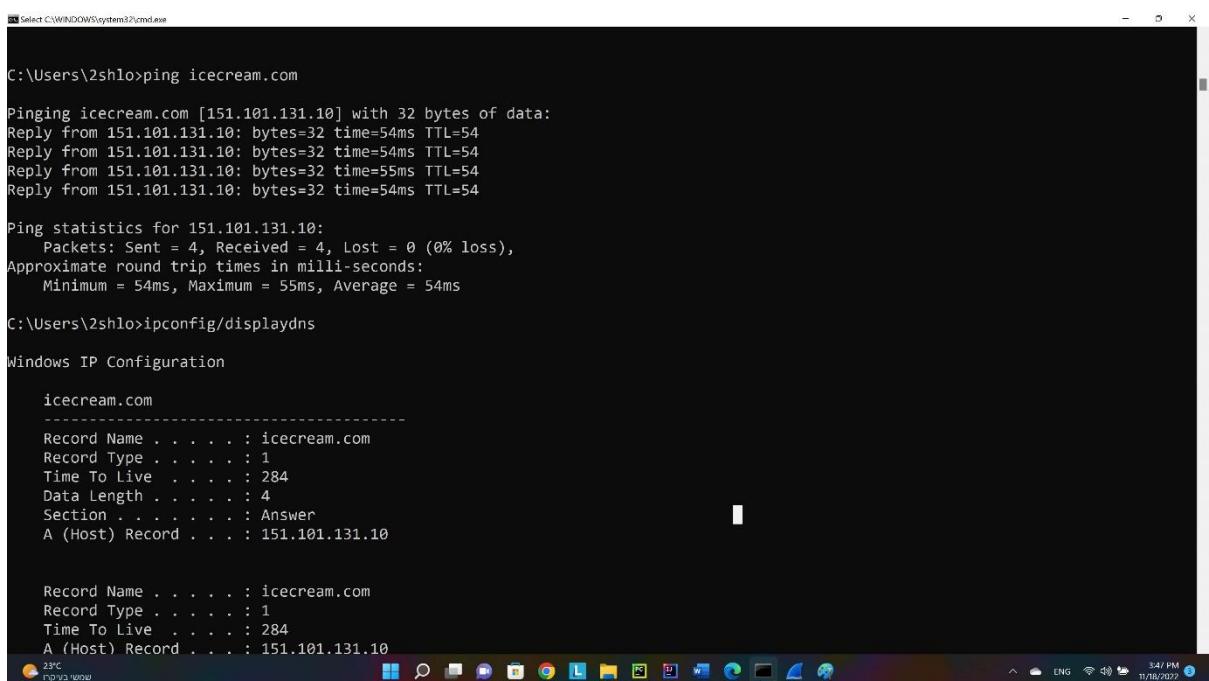
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\2shlo>ipconfig/displaydns

Windows IP Configuration
```

3.19 נרשם את הפקודה ping icecream.com ולאחר מכן שוב נרשם את הפקודה ipconfig/displaydns



```
C:\Users\2shlo>ping icecream.com

Pinging icecream.com [151.101.131.10] with 32 bytes of data:
Reply from 151.101.131.10: bytes=32 time=54ms TTL=54
Reply from 151.101.131.10: bytes=32 time=54ms TTL=54
Reply from 151.101.131.10: bytes=32 time=55ms TTL=54
Reply from 151.101.131.10: bytes=32 time=54ms TTL=54

Ping statistics for 151.101.131.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 55ms, Average = 54ms

C:\Users\2shlo>ipconfig/displaydns

Windows IP Configuration

icecream.com
-----
Record Name . . . . : icecream.com
Record Type . . . . : 1
Time To Live . . . . : 284
Data Length . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 151.101.131.10

Record Name . . . . : icecream.com
Record Type . . . . : 1
Time To Live . . . . : 284
A (Host) Record . . . : 151.101.131.10
```

כתובת ה-IP של האתר icecream.com הוא : 151.101.131.10  
זמן שהדומיין יהיה ברשימה הוא : (time to live) 284

## תרגיל 20 :

נסביר את התהיליך שבו אנחנו נכנסים לאתר אינטרנט, ואתר מוצג לנו בדף:

תחליה הלקוח שולח בקשה אל השרת, הבקשה היא פרוטוקול DNS כדי שבעצם נוכל להפוך את השם של האתר(הדומיין) לכתובת IP כדי שנוכל לייצר תקשורת בין הלקוח לשרת (בעצם כמו סוף טלפונים של דומיינים זה-IP הוא מספר הטלפון).

לאחר שיש לנו את IP של השרת ואת שם הדומיין, נשלח בקשה מהלקוח מסווג פרוטוקול HTTP שבה הלקוח מבקש מהשרת להכנס לאתר(לחיצת ידיהם)

השרת מקבל את הפרטים ושולח האם הוא מאשר לו לקבל את המשאבים כדי שהדף יציג את האתר המבוקש(נקרא גם "לחיצת ידים", מוחזר text/HTML/text)

לאחר שהדף מקבל את האישור מהשרת הוא שולח לו בקשה מסווג פרוטוקול HTTP שבה הלקוח שולח אם הוא תומך במאשבים(GET), בעצם נשלח לשרת מהצד השני את הפרטים עבור אותו לקוח(אם הוא תומך בשפה שלו, האם הדף של הלקוח יכול להציג את הנתונים וכו...)

השרת מקבל את הפרטים מהלקוח ושולח לו בחזרה תגובה, ואם נניח שהשרת מאשר את העברת המאשבים אז השרת גם שולח חבילה שבה הוא מאשר את העברת המשאבים וגם שולח את המשאבים עצמם.

הדף מקבל את המשאבים, מציג אותם עבור הלקוח והתקשרות נסגרת.