

מטלה 1

ת"ז מגישים: 209326776, 322998287

קישור להקלטות נמצא בקישור:

<https://drive.google.com/drive/folders/1qigfleDlw5z5LXQFBMRp6XE7H3MZti?usp=sharing>

שאלה 1:

בחרנו בממשק wifi שמחובר לאינטרנט חיצוני.

שאלה 2:

1. סינונו לפי destination ip ע"י כך שרשמנו בשורת הפילטר ip.dst==208.67.222.222

Wireshark capture showing DNS queries to 208.67.222.222. The filter is ip.dst==208.67.222.222. The table shows several DNS Standard query packets from 10.0.2.15 to 208.67.222.222.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	208.67.222.222	DNS	108	Standard query 0x7720 A firefox.settings.servi
2	0.000096863	10.0.2.15	208.67.222.222	DNS	108	Standard query 0x0d7c AAAA firefox.settings.servi
7	0.077167149	10.0.2.15	208.67.222.222	DNS	95	Standard query 0x7bf7 A detectportal.firefox.com
8	0.077455293	10.0.2.15	208.67.222.222	DNS	95	Standard query 0x0cf8 AAAA detectportal.firefox.c
34	0.357609605	10.0.2.15	208.67.222.222	DNS	88	Standard query 0x7632 A ocsph.digicert.com OPT
35	0.357609645	10.0.2.15	208.67.222.222	DNS	88	Standard query 0xea1f AAAA ocsph.digicert.com OPT
42	0.385055580	10.0.2.15	208.67.222.222	DNS	99	Standard query 0x25c8 A contile.services.mozilla
43	0.385159940	10.0.2.15	208.67.222.222	DNS	99	Standard query 0xa48d AAAA contile.services.mozil
50	0.429251867	10.0.2.15	208.67.222.222	DNS	89	Standard query 0x4cf2 AAAA cs9.wac.phicdn.net OPT
54	0.498700035	10.0.2.15	208.67.222.222	DNS	82	Standard query 0x1d7b A example.org OPT
55	0.498700070	10.0.2.15	208.67.222.222	DNS	82	Standard query 0xc5a6 AAAA example.org OPT

2.

Wireshark capture showing TCP connections to 443. The filter is tcp.srcport==443. The table shows several TCP packets from 10.0.2.15 to 208.67.222.222.

No.	Time	Source	Destination	Protocol	Length	Info
6	8.946835150	10.0.2.15	208.67.222.222	TCP	60	[TCP ACKed unseq segment] 443 → 59492 [ACK] Seq=
10	13.325286971	34.117.237.239	10.0.2.15	TCP	60	443 → 57320 [ACK] Seq=1 Ack=40 Win=65535 Len=0
11	13.367932868	34.117.237.239	10.0.2.15	TLSv1.2	93	Application Data
19	13.906381949	34.120.208.123	10.0.2.15	TCP	60	443 → 43588 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
22	13.907848106	34.120.208.123	10.0.2.15	TCP	60	443 → 43588 [ACK] Seq=1 Ack=518 Win=65535 Len=0
24	13.966076594	34.120.208.123	10.0.2.15	TLSv1.2	210	Server Hello, Change Cipher Spec, Encrypted Hands
29	13.967680985	34.120.208.123	10.0.2.15	TCP	60	443 → 43588 [ACK] Seq=157 Ack=569 Win=65535 Len=0
31	13.968083215	34.120.208.123	10.0.2.15	TCP	60	443 → 43588 [ACK] Seq=157 Ack=746 Win=65535 Len=0
32	13.968083585	34.120.208.123	10.0.2.15	TCP	60	443 → 43588 [ACK] Seq=157 Ack=1098 Win=65535 Len=0
33	13.968083746	34.120.208.123	10.0.2.15	TCP	60	443 → 43588 [ACK] Seq=157 Ack=1519 Win=65535 Len=0
34	14.012620352	34.120.208.123	10.0.2.15	TLSv1.2	161	Application Data

פרוטוקול שמשתמש ב port הנל הוא TCP.

סינונו לפי source port ע"י כך שרשמנו בשורת הפילטר tcp.srcport==443

נשים לב כי TLSv הוא סוג של TCP.

3. סינונו לפי פרוטוקול DNS ע"י כך שרשמנו בשורת הפילטר dns

Wireshark capture showing DNS queries. The filter is dns. The table shows several DNS Standard query packets from 10.0.2.15 to 208.67.222.222.

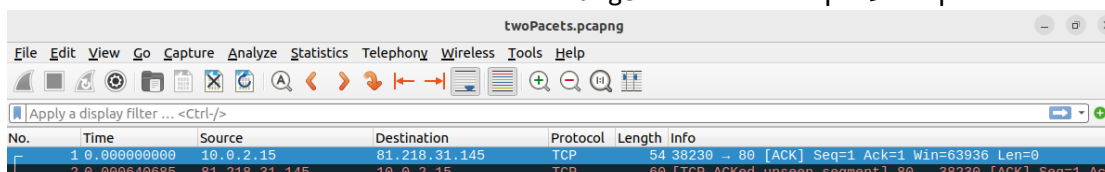
No.	Time	Source	Destination	Protocol	Length	Info
3	8.788759637	10.0.2.15	208.67.222.222	DNS	101	Standard query 0xe7fe A incoming.telemetry.mozill
4	8.788922652	10.0.2.15	208.67.222.222	DNS	101	Standard query 0xd528 AAAA incoming.telemetry.moz
13	13.797371529	10.0.2.15	208.67.220.220	DNS	101	Standard query 0xd528 AAAA incoming.telemetry.moz
14	13.797497276	10.0.2.15	208.67.220.220	DNS	101	Standard query 0xe7fe A incoming.telemetry.mozill
15	13.854461313	208.67.220.220	10.0.2.15	DNS	307	Standard query response 0xd528 AAAA incoming.tele
16	13.855467739	10.0.2.15	208.67.220.220	DNS	114	Standard query 0x6901 AAAA prod.ingestion-edge.pr
17	13.858791500	208.67.220.220	10.0.2.15	DNS	233	Standard query response 0xe7fe A incoming.teleme
23	13.913690544	208.67.220.220	10.0.2.15	DNS	207	Standard query response 0x6901 AAAA prod.ingestic
40	17.406473835	10.0.2.15	208.67.220.220	DNS	92	Standard query 0x7b4a A completion.amazon.com OPT
41	17.406684856	10.0.2.15	208.67.220.220	DNS	92	Standard query 0x703b AAAA completion.amazon.com
42	17.620638295	208.67.220.220	10.0.2.15	DNS	163	Standard query response 0x703b AAAA completion.am

שאלה 3:**2-3.pcapng**

פורמט ההקלטה הוא pcapng הלוכד pacets של נתונים ברשת.

שאלה 4:

שמרנו שתי פאקטות ע"י כך ששממנו ב range 1-2



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	81.218.31.145	TCP	54	38230 → 80 [ACK] Seq=1 Ack=1 Win=63936 Len=0
2	0.000640685	81.218.31.145	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 → 38230 [ACK] Seq=1 Ack=

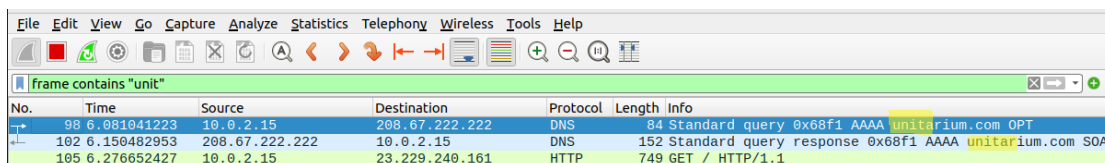
שאלה 5:

במצב promiscuous הסניפר מאזין לכל התעבורה שעוברת דרך כרטיס הרשת, כך שיכול לקבל מידע של כל מה שעבר בכרטיס הרשת גם מה שלא היה מיועד אליו.

השימושים יהיה אפשר להסניף מהכרטיס רשת גם פאקטות שלא נשלחו אליו

שאלה 6:

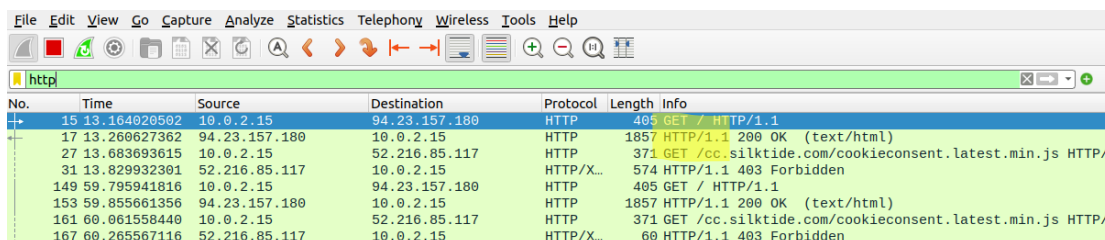
הסינון מכיל את כל הפאקטות שמכילים את המילה "unit"



No.	Time	Source	Destination	Protocol	Length	Info
98	6.081041223	10.0.2.15	208.67.222.222	DNS	84	Standard query 0x68f1 AAAA unitarium.com OPT
102	6.150482953	208.67.222.222	10.0.2.15	DNS	152	Standard query response 0x68f1 AAAA unitarium.com SOA
105	6.276652427	10.0.2.15	23.229.249.161	HTTP	749	GET / HTTP/1.1

שאלה 7:

שמנו בפילטר http בשביל לסנן לפי פרוטוקול HTTP
לפי הinfo אנחנו יודעים מהי חבילת בקשה ומהי חבילת תגובה לבקשה, המילה get מסמנת בקשה (והשורה)



No.	Time	Source	Destination	Protocol	Length	Info
15	13.164020502	10.0.2.15	94.23.157.180	HTTP	405	GET / HTTP/1.1
17	13.260627362	94.23.157.180	10.0.2.15	HTTP	1857	HTTP/1.1 200 OK (text/html)
27	13.683693615	10.0.2.15	52.216.85.117	HTTP	371	GET /cc.silktide.com/cookieconsent.latest.min.js HTTP/
31	13.829932301	52.216.85.117	10.0.2.15	HTTP/X...	574	HTTP/1.1 403 Forbidden
149	59.795941816	10.0.2.15	94.23.157.180	HTTP	405	GET / HTTP/1.1
153	59.855661356	94.23.157.180	10.0.2.15	HTTP	1857	HTTP/1.1 200 OK (text/html)
161	60.061558440	10.0.2.15	52.216.85.117	HTTP	371	GET /cc.silktide.com/cookieconsent.latest.min.js HTTP/
167	60.265567116	52.216.85.117	10.0.2.15	HTTP/X...	60	HTTP/1.1 403 Forbidden

שאלה 8: חבילת הבקשה:

1. ניתן לראות בתמונה למעלה כי הזמן בין חבילת הבקשה הראשונה לתגובה הוא:

$$13.260627362 - 13.164020502 = 0.09660686$$

2. גרסת http היא 1.1 – מסומן איפה רואים בתמונה למעלה במרקר צהוב.

3. הקו של המכשיר ממנו התבצעה הבקשה הוא 10.0.2.15, ניתן לראות כי הבקשה התבצעה מהמחשב שלי.

```
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: www.sha1-online.com\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:106.0) Gecko/20100101 Firefox/106.0\r\n
```

4. החבילה נמצאת ב 94.23.157.180 (רואים עם החיצים בצד שמאל חץ ימינה זה הבקשה וחץ שמאלה זה התגובה שלו)

5. dst portn הוא 80 ממורקק בתמונה למטה היכן רואים.

The image shows a Wireshark packet capture. The top pane displays a list of packets. Packet 15 is a GET request from 10.0.2.15 to 94.23.157.180 on port 80. The bottom pane shows the details of the selected packet, highlighting the 'Destination Port: 80' in the Transmission Control Protocol section.

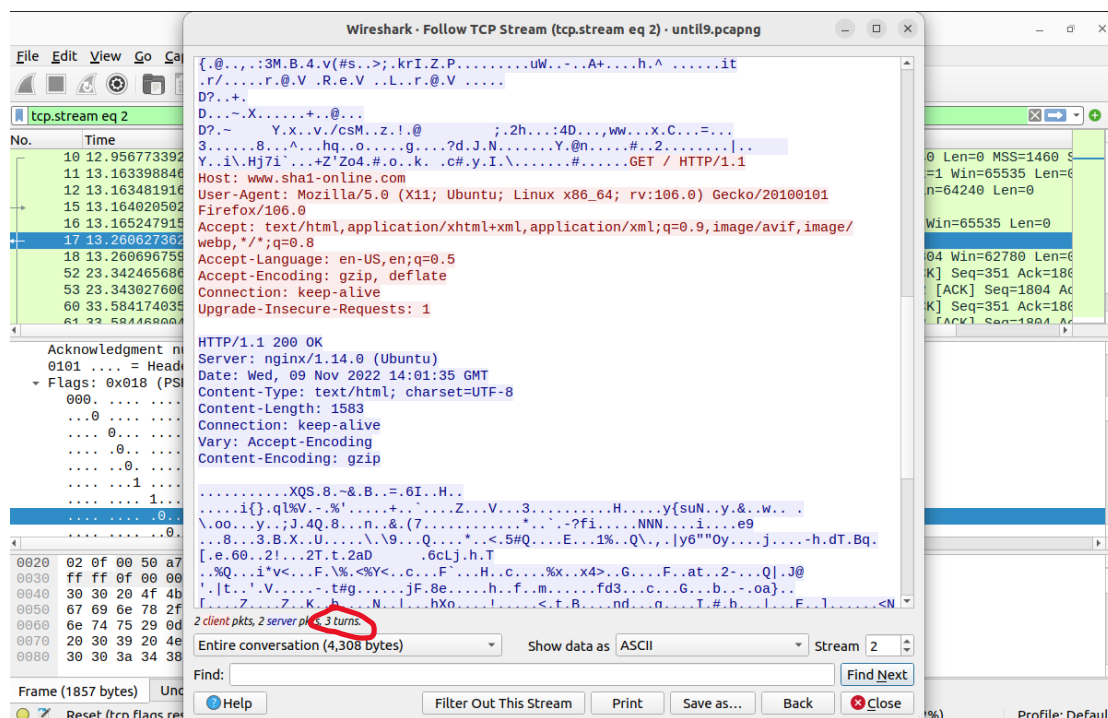
שאלה 9: חבילת התגובה:

1. הסטטוס קוד הוא 200 OK – מסומן באדום בתמונה למעלה. האובייקט נמצא והוא מצורף להודעה זו.

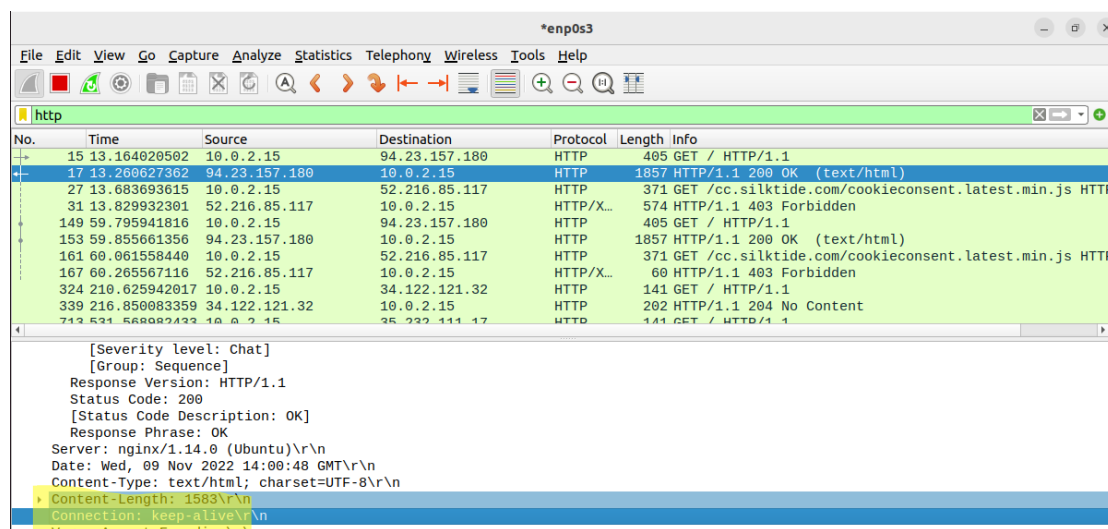
2. ה:ip source 94.23.157.180

```
Server: nginx/1.14.0 (Ubuntu)\r
```

3. הוחזרו 3 חבילות



4. סוג הconnection בין השרת והלקוח הוא Keep-alive/r/n (מסומן בתמונה למטה). התקשורת הנ"ל נותנת הוראה לחיבור להישאר פתוח עבור מספר בקשות ותגובות. במקום שהחיבורים יסגרו לאחר כל בקשה.



שאלה 10:-

1. החישוב נעשה בשרת מרוחק. ניתן לראות בצילום מסך שבשדה של info כתוב POST- כלומר בקשה לחפש בשרת.
2. הפרמטרים שנשלחו הם key:textToHash value:renanan
3. היה עדיף להשתמש ב http כיוון שהקוד שנמצא בצד השרת לא חשוף ללקוח כלל.
4. הסיכון הוא שיראו את התגובה שמתקבלת כיוון שאין הצפנה.

No.	Time	Source	Destination	Protocol	Length	Info
113	12.548626894	10.0.2.15	94.23.157.100	HTTP	614	GET / HTTP/1.1
129	12.813093081	94.23.157.100	10.0.2.15	HTTP	636	HTTP/1.1 200 OK (text/html)
141	12.936917489	10.0.2.15	52.217.139.184	HTTP	371	GET /cc.silktide.com/cookieconsent.latest.min.js HTTP
173	13.336513940	52.217.139.184	10.0.2.15	HTTP/X...	574	HTTP/1.1 403 Forbidden
247	23.309814483	10.0.2.15	94.23.157.100	HTTP	800	POST / HTTP/1.1 (application/x-www-form-urlencoded)
253	23.462856410	94.23.157.100	10.0.2.15	HTTP	887	HTTP/1.1 200 OK (text/html)
255	23.515873946	10.0.2.15	52.217.139.184	HTTP	371	GET /cc.silktide.com/cookieconsent.latest.min.js HTTP
257	23.770732003	52.217.139.184	10.0.2.15	HTTP/X...	574	HTTP/1.1 403 Forbidden
32843	10.0.2.15	172.217.22.98	10.0.2.15	HTTP	401	GET /pagead/js/adsbygoogle.js HTTP/1.1
398566	172.217.22.98	10.0.2.15	10.0.2.15	HTTP	9163	HTTP/1.1 200 OK (text/javascript)
528.25.340011805	10.0.2.15	172.217.22.67	10.0.2.15	OCSP	480	Request

Frame 247: 800 bytes on wire (6400 bits), 800 bytes captured (6400 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu_7b:91:d6 (08:00:27:7b:91:d6), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 94.23.157.100

Transmission Control Protocol, Src Port: 45534, Dst Port: 80, Seq: 561, Ack: 1883, Len: 746

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "textToHash" = "renana"
 - Key: textToHash
 - Value: renana
- Form item: "hash-algorithm-used" = "sha1"
 - Key: hash-algorithm-used
 - Value: sha1

שאלה 11:

מהלוקח נשלחו 2 חבילות, וגם מהשרת נשלחו 2 חבילות.

Wireshark - Follow HTTP Stream (tcp.stream eq 1) - 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: atuvcc=4%7C45; _ga=GA1.2.1508106666.1668001339; gads-ID=2591dF9c7a4e997e-224be28d1ed700e0:T=1668001339:RT=1668001339:S=ALNI_MaOfsm uWFjDaidW266nIGHW6ydwEQ; gpi=UID=00000b1de1f34627:T=1668001339:RT=1668157468:S=ALNI_MY-0A7taa0IepfHJBNj_Q7U 0Wf72w; _atuvs=636e101bac9a404e001; _gid=GA1.2.1622828837.1668157527

Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK

Connection: Upgrade, Keep-Alive

Content-Encoding: gzip

Content-Length: 5039

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

Date: Fri, 11 Nov 2022 09:09:04 GMT

Keep-Alive: timeout=5

Server: Apache

Upgrade: h2,h2c

Vary: Accept-Encoding

<!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." />

2 client pkts, 2 server pkts, 3 turns.

Entire conversation (23 kB)

Show data as ASCII

Find:

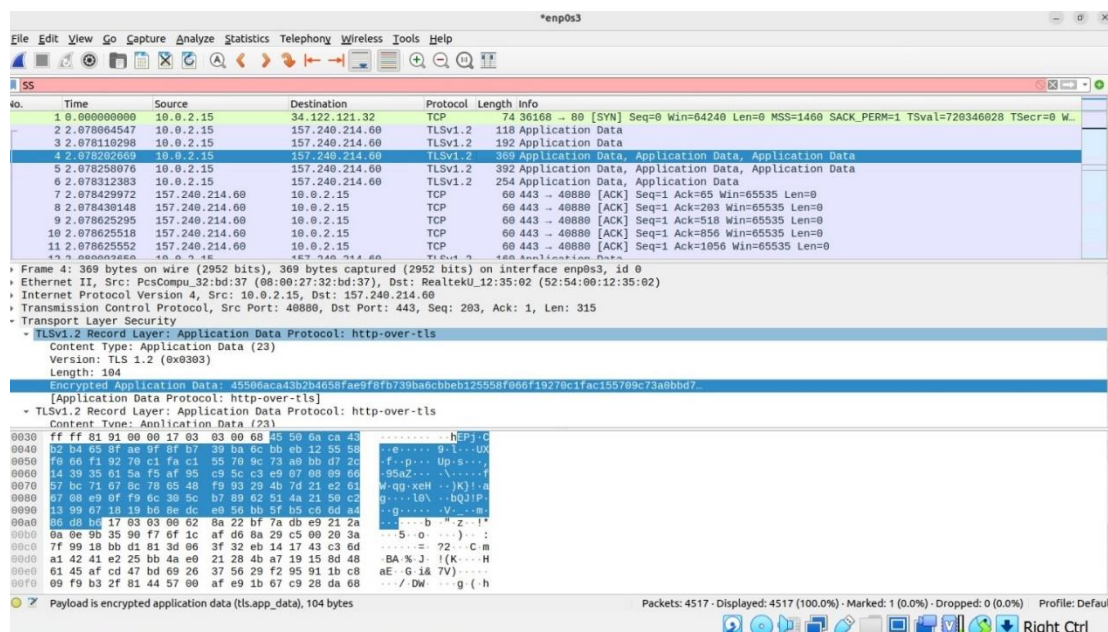
Find Next

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

Profile: Default

שאלה 12:

התוכן מוצפן ולכן אנו אומנם רואים את הפאקטות אבל לא את מה שהועבר. בפס הכחול כתוב encrypted – כלומר המידע מוצפן.



שאלה 13:

שם השרת שנותן את התשובה לשאילתה לא ידוע והוא לא מהימן.

כתובת הִקו של הדומיין:

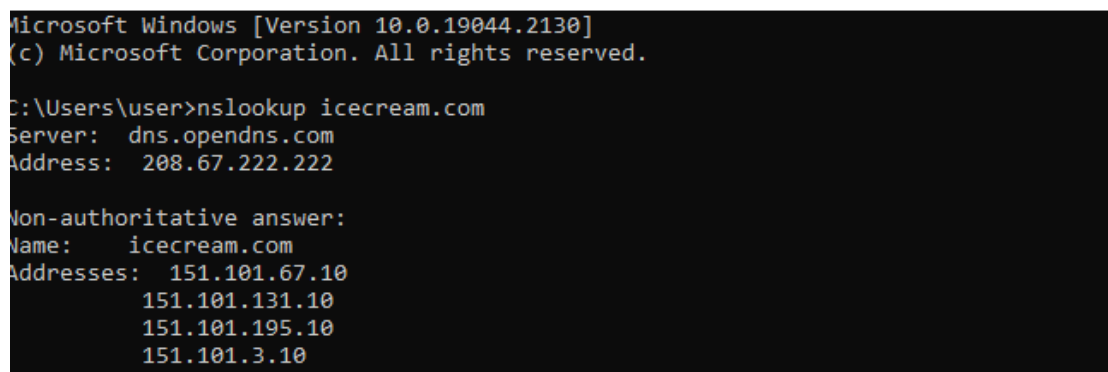
151.101.67.10

151.101.131.10

151.101.195.10

151.101.3.10

Select שורת הפקודה



שאלה 14:

1. יש 4 שאילות

2. ההבדל הוא סוג ה־type -השאילתה הראשונה השנייה והרביעית היא מסוג AAAA השלישית

היא מסוג A

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.0.138	DNS	83	Standard query 0x4260 AAAA icecream.com OPT
2	0.119994033	10.0.0.138	10.0.2.15	DNS	146	Standard query response 0x4260 AAAA icecream.com SOA d
5	37.096490123	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xda78 AAAA connectivity-check.ubuntu.c
6	37.112317835	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0xda78 AAAA connectivity-check
7	37.113785378	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xbaba A connectivity-check.ubuntu.com
8	37.113985916	10.0.2.15	10.0.0.138	DNS	100	Standard query 0x8af6 AAAA connectivity-check.ubuntu.c
9	37.129830941	10.0.0.138	10.0.2.15	DNS	148	Standard query response 0xbaba A connectivity-check.ub
10	37.131659011	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0x8af6 AAAA connectivity-check

3. לפורט יעד 53 (בתמונה מטה שאילתה מסומנת)

4. UDP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.0.138	DNS	83	Standard query 0x4260 AAAA icecream.com OPT
2	0.119994033	10.0.0.138	10.0.2.15	DNS	146	Standard query response 0x4260 AAAA icecream.com SOA d
5	37.096490123	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xda78 AAAA connectivity-check.ubuntu.c
6	37.112317835	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0xda78 AAAA connectivity-check
7	37.113785378	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xbaba A connectivity-check.ubuntu.com
8	37.113985916	10.0.2.15	10.0.0.138	DNS	100	Standard query 0x8af6 AAAA connectivity-check.ubuntu.c
9	37.129830941	10.0.0.138	10.0.2.15	DNS	148	Standard query response 0xbaba A connectivity-check.ub
10	37.131659011	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0x8af6 AAAA connectivity-check

...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0xbb87 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 10.0.0.138
↳ User Datagram Protocol, Src Port: 55600, Dst Port: 53
Source Port: 55600
Destination Port: 53
Length: 49
Checksum: 0x16db [unverified]
[Checksum Status: Unverified]

5. באופן רקורסיבי

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.0.138	DNS	83	Standard query 0x4260 AAAA icecream.com OPT
2	0.119994033	10.0.0.138	10.0.2.15	DNS	146	Standard query response 0x4260 AAAA icecream.com SOA
5	37.096490123	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xda78 AAAA connectivity-check.ubuntu.
6	37.112317835	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0xda78 AAAA connectivity-che
7	37.113785378	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xbaba A connectivity-check.ubuntu.com
8	37.113985916	10.0.2.15	10.0.0.138	DNS	100	Standard query 0x8af6 AAAA connectivity-check.ubuntu.
9	37.129830941	10.0.0.138	10.0.2.15	DNS	148	Standard query response 0xbaba A connectivity-check.u
10	37.131659011	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0x8af6 AAAA connectivity-che

↳ User Datagram Protocol, Src Port: 55600, Dst Port: 53
↳ Domain Name System (query)
Transaction ID: 0x4260
↳ Flags: 0x0100 Standard query
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
... .. = Truncated: Message is not truncated
... ..1... .. = Recursion desired: Do query recursively
... ..0... .. = Z: reserved (0)
... ..0... .. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0

6. לכל השאילתות מסוג AAAA יש 0 תשובות, לשאילתה מסוג A יש 3 תשובות, ההבדל

7. המהותי בסעיף

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.0.138	DNS	83	Standard query 0x4260 AAAA icecream.com OPT
2	0.119994033	10.0.0.138	10.0.2.15	DNS	146	Standard query response 0x4260 AAAA icecream.com SOA
5	37.096490123	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xda78 AAAA connectivity-check.ubuntu.c
6	37.112317835	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0xda78 AAAA connectivity-check
7	37.113785378	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xbaba A connectivity-check.ubuntu.com
8	37.113985916	10.0.2.15	10.0.0.138	DNS	100	Standard query 0x8af6 AAAA connectivity-check.ubuntu.c
9	37.129830941	10.0.0.138	10.0.2.15	DNS	148	Standard query response 0xbaba A connectivity-check.ub
10	37.131659011	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0x8af6 AAAA connectivity-check

.... 1... .. = Recursion available: Server can do recursive queries
.... .0.. .. = Z: reserved (0)
.... ..0. = Answer authenticated: Answer/authority portion was not authenticated by the server
.... ..0. = Non-authenticated data: Unacceptable
.... ..0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 1

Queries

- icecream.com: type AAAA, class IN
- Authoritative nameservers
- Additional records

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.0.138	DNS	83	Standard query 0x4260 AAAA icecream.com OPT
2	0.119994033	10.0.0.138	10.0.2.15	DNS	146	Standard query response 0x4260 AAAA icecream.com SOA
5	37.096490123	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xda78 AAAA connectivity-check.ubuntu.c
6	37.112317835	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0xda78 AAAA connectivity-check
7	37.113785378	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xbaba A connectivity-check.ubuntu.com
8	37.113985916	10.0.2.15	10.0.0.138	DNS	100	Standard query 0x8af6 AAAA connectivity-check.ubuntu.c
9	37.129830941	10.0.0.138	10.0.2.15	DNS	148	Standard query response 0xbaba A connectivity-check.ub
10	37.131659011	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0x8af6 AAAA connectivity-check

.... 1... .. = Recursion available: Server can do recursive queries
.... .0.. .. = Z: reserved (0)
.... ..0. = Answer authenticated: Answer/authority portion was not authenticated by the server
.... ..0. = Non-authenticated data: Unacceptable
.... ..0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 1

Queries

- connectivity-check.ubuntu.com: type A, class IN

Answers

7. הגרסה ממנה הם מבקשים את הכתובת. שאלתה מסוג A היא מגרסה IPv4 שאלתה מסוג

AAAA היא מגרסה IPv6

Type: AAAA (IPv6 Address)

שאלה 15:

213.57.22.5

213.57.2.5

```
DNS Servers . . . . . : 2001:4860:4860::8888
                        2001:4860:4860::8844
                        213.57.22.5
                        213.57.2.5
                        2001:4860:4860::8888
                        2001:4860:4860::8844
NetBIOS over Tcpip . . . . . : Enabled
```

שאלה 16:

2001:4860:4860:8888

2001:4860:4860:8844

שאלה 17:

אכן כתובת ה DNS השתנתה

DNS Servers : 8.8.8.8

בתמונה למטה אפשר לראות שנעשה שימוש בשרת 8.8.8.8 של google

	Info	Length	Protocol	Destination	Source	Time
Standard query response 0x9448 A www.googlea	174	DNS	10.0.0.14	8.8.8.8	1.453135	80
Standard query response 0xd1dc HTTPS www.goo	135	DNS	10.0.0.14	8.8.8.8	1.453135	81
Standard query response 0x92ee HTTPS account	129	DNS	10.0.0.14	8.8.8.8	1.469228	86
Standard query 0xa90a A ssl.gstatic.com	75	DNS	8.8.8.8	10.0.0.14	1.470384	87
Standard query 0x2d94 HTTPS ssl.gstatic.com	75	DNS	8.8.8.8	10.0.0.14	1.470725	88
Standard query 0xa7f8 A www.google.com	74	DNS	8.8.8.8	10.0.0.14	1.471313	89
Standard query 0x1ed5 HTTPS www.google.com	74	DNS	8.8.8.8	10.0.0.14	1.471601	90
Standard query response 0xa90a A ssl.gstatic	91	DNS	10.0.0.14	8.8.8.8	1.483419	105
Standard query response 0x1ed5 HTTPS www.goo	99	DNS	10.0.0.14	8.8.8.8	1.483419	106
Standard query response 0xa7f8 A www.google	90	DNS	10.0.0.14	8.8.8.8	1.483419	107

שאלה 18:

נסתכל על עמודת ה length רואים כי חבילות התגובה כבדות יותר, כיוון שבתגובה חוזר לנו המידע אותו ביקשנו.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.0.138	DNS	83	Standard query 0x4260 AAAA icecream.com OPT
2	0.119994033	10.0.0.138	10.0.2.15	DNS	146	Standard query response 0x4260 AAAA icecream.com SOA d
5	37.096490123	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xda78 AAAA connectivity-check.ubuntu.c
6	37.112317835	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0xda78 AAAA connectivity-check
7	37.113785378	10.0.2.15	10.0.0.138	DNS	100	Standard query 0xbaba A connectivity-check.ubuntu.com
8	37.113985916	10.0.2.15	10.0.0.138	DNS	100	Standard query 0x8af6 AAAA connectivity-check.ubuntu.c
9	37.129830941	10.0.0.138	10.0.2.15	DNS	148	Standard query response 0xbaba A connectivity-check.ub
10	37.131659011	10.0.0.138	10.0.2.15	DNS	161	Standard query response 0x8af6 AAAA connectivity-check

שאלה 19:

```
C:\Users\user>ipconfig/displaydns
```

```
Windows IP Configuration
```

```
35ed156481a96fa27a41c9a0d100537a.clo.footprintdns.com
```

```
-----
Record Name . . . . . : 35ed156481a96fa27a41c9a0d100537a.clo.footprintdns.com
Record Type . . . . . : 5
Time To Live . . . . . : 2
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : 1.perf.msedge.net
```

```
Record Name . . . . . : 1.perf.msedge.net
Record Type . . . . . : 5
Time To Live . . . . . : 2
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : a-0019.a-msedge.net
```

```
Record Name . . . . . : a-0019.a-msedge.net
Record Type . . . . . : 5
Time To Live . . . . . : 2
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : a-0019.a.dns.azurefd.net
```

```
Record Name . . . . . : a-0019.a.dns.azurefd.net
Record Type . . . . . : 5
Time To Live . . . . . : 2
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : a-0019.standard.a-msedge.net
```

.1
.2

```
C:\Users\user>ipconfig/flushdns
```

```
Windows IP Configuration
```

```
Successfully flushed the DNS Resolver Cache.
```

```
C:\Users\user>ipconfig/displaydns
```

```
Windows IP Configuration
```

.3 כותבת IP 151.101.67.10
time to live:289

```
C:\Users\user>ipconfig/displaydns

Windows IP Configuration

icecream.com
-----
Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 289
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 151.101.67.10

Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 289
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 151.101.131.10

Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 289
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 151.101.195.10

Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 289
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 151.101.3.10
```

שאלה 20:

כאשר אנו מבקשים לגלוש לאתר http מסוים, דבר ראשון נרצה את כתובת ה־ip שלו, ה־DNS אחראי על הכתובות והוא מקשר אותנו עם כתובת ה־ip של האתר. אנו שולחים בקשת http ומחכים לקבל תגובה מהשרת, לאחר שהתגובה מתקבלת מתחילה השיחה, אנו שולחים את הבקשה שרצינו ומקבלים תשובה ואז נוכל לשלוח עוד בקשה.