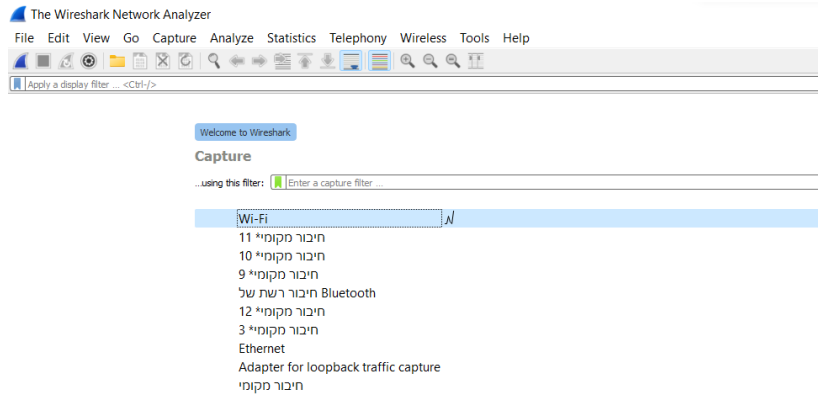


## רשתות תקשורת – מטלה 1

מגישים: זאב קהת, ת"ז 203283908; **להשלים**

1. בחרתי בממשק ה-wifi כיוון שאני עובד על מחשב נייד שמחובר לרשת הביתית בחיבור wifi. ניתן לראות במסך הראשי של ה-wireshark שזהו ממשק החיבור האינטרנטי היחיד שקולט תעבורת רשת:



2. תשובות לפי סעיפים:

א. סיננתי את החבילות לפי `ip.dst == 10.0.0.13` (ה-default gateway שלי).

No.	Time	Source	Destination	Protocol	Length	Info
30	2.774751	10.0.0.18	10.0.0.13	TCP	164	60690 → 8009 [PSH, ACK] Seq=111 Ack=1 Wi
32	2.824493	10.0.0.18	10.0.0.13	TCP	54	60690 → 8009 [ACK] Seq=111 Ack=111 Wi
39	3.155629	10.0.0.18	10.0.0.13	TCP	164	60629 → 8009 [PSH, ACK] Seq=111 Ack=1 Wi
41	3.205094	10.0.0.18	10.0.0.13	TCP	54	60629 → 8009 [ACK] Seq=111 Ack=111 Wi
194	7.790789	10.0.0.18	10.0.0.13	TCP	164	60690 → 8009 [PSH, ACK] Seq=111 Ack=1 Wi
196	7.855486	10.0.0.18	10.0.0.13	TCP	54	60690 → 8009 [ACK] Seq=221 Ack=221 Wi
197	8.167774	10.0.0.18	10.0.0.13	TCP	164	60629 → 8009 [PSH, ACK] Seq=111 Ack=1 Wi
201	8.216214	10.0.0.18	10.0.0.13	TCP	54	60629 → 8009 [ACK] Seq=221 Ack=221 Wi
239	12.821791	10.0.0.18	10.0.0.13	TCP	164	60690 → 8009 [PSH, ACK] Seq=221 Ack=2 Wi
241	12.872635	10.0.0.18	10.0.0.13	TCP	54	60690 → 8009 [ACK] Seq=331 Ack=331 Wi
243	13.182477	10.0.0.18	10.0.0.13	TCP	164	60629 → 8009 [PSH, ACK] Seq=221 Ack=2 Wi
247	13.230076	10.0.0.18	10.0.0.13	TCP	54	60629 → 8009 [ACK] Seq=331 Ack=331 Wi
297	17.838530	10.0.0.18	10.0.0.13	TCP	164	60690 → 8009 [PSH, ACK] Seq=331 Ack=3 Wi
299	17.886819	10.0.0.18	10.0.0.13	TCP	54	60690 → 8009 [ACK] Seq=441 Ack=441 Wi
302	18.198543	10.0.0.18	10.0.0.13	TCP	164	60629 → 8009 [PSH, ACK] Seq=331 Ack=3 Wi
304	18.246774	10.0.0.18	10.0.0.13	TCP	54	60629 → 8009 [ACK] Seq=441 Ack=441 Wi

- ב. סיננתי את החבילות לפי `source port 443` הוא של `https`, כלומר גלישה אינטרנטית מאובטחת:

No.	Time	Source	Destination	Protocol	Length	Info
3	0.298113	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	443 → 60721 [ACK] S
5	0.351390	2a04:4e42:54::272	2a10:8009:cdd3:0:60...	TCP	86	443 → 60964 [ACK] S
10	0.518873	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	443 → 60710 [ACK] S
24	2.358662	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	443 → 60852 [ACK] S
35	3.073419	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	443 → 60851 [ACK] S
37	3.144240	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	443 → 60733 [ACK] S
86	5.378068	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	[TCP Dup ACK 3#1] 4
89	5.634187	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	[TCP Dup ACK 10#1]
185	6.720235	2600:1901:1:c36::	2a10:8009:cdd3:0:60...	TCP	74	443 → 61440 [FIN, A
189	7.419400	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	[TCP Dup ACK 24#1]
198	8.170326	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	[TCP Dup ACK 35#1]
202	8.269274	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	[TCP Dup ACK 37#1]
214	10.241029	170.114.15.94	10.0.0.18	TCP	54	443 → 60717 [ACK] S
215	10.551862	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	[TCP Dup ACK 3#1] 4
222	10.752703	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	[TCP Dup ACK 10#1]
237	12.483461	2407:30c0:182::aa72...	2a10:8009:cdd3:0:60...	TCP	74	[TCP Dup ACK 24#1]

> Frame 24: 74 bytes on wire (592 bits) captured on interface (eth0) 0000 fc b3 bc ef a7 6d 00 b8 c2 b3 75 da 86 dd 62 89 ...m-

ג. סיננתי לפי פרוטוקול http :

No.	Time	Source	Destination	Protocol	Length	Info
15223	301.333868	10.0.0.18	4.246.174.31	HTTP/X...	322	POST /metadata.svc HTTP/1.1
15235	301.527494	4.246.174.31	10.0.0.18	HTTP/X...	752	HTTP/1.1 200 OK
64062	2025.677387	10.0.0.18	10.0.0.26	HTTP	300	GET /dd.xml HTTP/1.1
64067	2025.681664	10.0.0.18	10.0.0.13	HTTP	313	GET /ssdp/device-desc.xml HTTP/1.1
64068	2025.681799	10.0.0.18	10.0.0.11	HTTP	313	GET /ssdp/device-desc.xml HTTP/1.1
64071	2025.684437	10.0.0.26	10.0.0.18	HTTP/X...	489	HTTP/1.1 200 OK
64079	2025.689611	10.0.0.11	10.0.0.18	HTTP/X...	1227	HTTP/1.1 200 OK
64080	2025.692957	10.0.0.13	10.0.0.18	HTTP/X...	1227	HTTP/1.1 200 OK
64819	2026.701232	10.0.0.18	10.0.0.16	HTTP	364	GET /upnphost/udhisapi.d HTTP/1.1
64825	2026.729164	10.0.0.16	10.0.0.18	HTTP/X...	1114	HTTP/1.1 200 OK
71515	2039.341741	2a10:8009:cdd3:0:60...	2a02:3d0:8:a000::	HTTP	356	GET /msdownload/update/v HTTP/1.1
71520	2039.351959	2a02:3d0:8:a000::	2a10:8009:cdd3:0:60...	HTTP	326	HTTP/1.1 304 Not Modified
73470	2084.447200	2a10:8009:cdd3:0:60...	2606:2800:133:672:1...	HTTP	320	GET /msdownload/update/v HTTP/1.1
73472	2084.508823	2606:2800:133:672:1...	2a10:8009:cdd3:0:60...	HTTP	364	HTTP/1.1 304 Not Modified

3. שמרתי את ההקלטה בתור Wireshark Capture File (ההקלטה לא מצורפת להגשה בגלל הגבלת גודל ההגשה ל-10 MB):

שם	תאריך שינוי	סוג	גודל	מצב
Ex1	19/11/2022 20:59	Microsoft Word מסמך של	934 KB	
Ex1	19/11/2022 21:00	Wireshark capture file	40,455 KB	
Q1	19/11/2022 20:10	קובץ PNG	146 KB	

4. שמירת 2 פקטות בפורמט wcf (הקלטה המכילה את 2 הפטקות מצורפת להגשה):

No.	Time	Source	Destination	Protocol	Length	Info
64825	2026.729164	10.0.0.16	10.0.0.18	HTTP/X...	1114	HTTP/1.1 200 OK
64080	2025.692957	10.0.0.13	10.0.0.18	HTTP/X...	1227	HTTP/1.1 200 OK
64079	2025.689611	10.0.0.11	10.0.0.18	HTTP/X...	1227	HTTP/1.1 200 OK
64071	2025.684437	10.0.0.26	10.0.0.18	HTTP/X...	489	HTTP/1.1 200 OK
15235	301.527494	4.246.174.31	10.0.0.18	HTTP/X...	752	HTTP/1.1 200 OK
15223	301.333868	10.0.0.18	4.246.174.31	HTTP/X...	322	POST /metadata.svc HTTP/1.1
15186	301.093213	2a10:8009:cdd3:0:60...	2a02:26f0:fe00:4ad:...	HTTP/X...	310	POST /fwlink/?LinkId=252669&clid=0x409 HTTP/1.1
84737	2689.272902	2a02:26f0:129:395:...	2a10:8009:cdd3:0:60...	HTTP	337	HTTP/1.1 304 Not Modified
84735	2689.222782	2a10:8009:cdd3:0:60...	2a02:26f0:129:395:...	HTTP	301	GET / HTTP/1.1
84726	2689.132447	2a02:26f0:129:3ac:...	2a10:8009:cdd3:0:60...	HTTP	337	HTTP/1.1 304 Not Modified
84724	2689.082914	2a10:8009:cdd3:0:60...	2a02:26f0:129:3ac:...	HTTP	301	GET / HTTP/1.1
73737	2087.792778	2606:2800:133:672:1...	2a10:8009:cdd3:0:60...	HTTP	364	HTTP/1.1 304 Not Modified
73735	2087.724109	2a10:8009:cdd3:0:60...	2606:2800:133:672:1...	HTTP	361	GET /msdownload/update/v3/static/trustedr/en/c HTTP/1.1
73734	2087.713412	2606:2800:133:672:1...	2a10:8009:cdd3:0:60...	HTTP	364	HTTP/1.1 304 Not Modified
73732	2087.644246	2a10:8009:cdd3:0:60...	2606:2800:133:672:1...	HTTP	320	GET /msdownload/update/v3/static/trustedr/en/s HTTP/1.1

5. הפעלת הקלטה של Wireshark ב-promiscuous mode גורמת להקלטה לאסוף את כלל הפקטות העוברות ברשת שאליה אני מחובר, לעומת מצב רגיל שיקלוט רק פקטות שאמורות להגיע לכתובת שלי (פקטות אלי וממני, או פקטה שנותבה דרכי). השימוש ב-promiscuous נפוץ בעיקר כאשר נרצה לנטר תעבורה כלל-רשתית – לצרכי ניהול רשת, אבטחת רשת, איסוף מידע מתוך הרשת ועוד.

6. הסינון "`<string>`" frame contains מפלטר על הפקטות הנקלטות ומשאיר בתצוגה רק את אלו שכוללות בתוך הפקטה את המחרוזת שחיפשנו, ללא קשר לפרוטוקול. לכן אם אגלוש לאתר נוסף שמכיל בתוכו את המילה unit, גם הפקטות הקשורות לתעבורה הזאת יעלו בסינון :

No.	Time	Source	Destination	Protocol	Length	Info
717	18.867029	10.0.0.18	10.0.0.138	DNS	82	Standard query 0x2feb AAAA covid-19.unitarium.com
718	18.867028	10.0.0.18	10.0.0.138	DNS	79	Standard query 0x8bd3 A games.unitarium.com
719	18.867029	10.0.0.18	10.0.0.138	DNS	78	Standard query 0x2c84 AAAA time.unitarium.com
720	18.867029	10.0.0.18	10.0.0.138	DNS	82	Standard query 0xc5f9 A covid-19.unitarium.com
721	18.867033	10.0.0.18	10.0.0.138	DNS	79	Standard query 0x8005 AAAA games.unitarium.com
740	18.880568	2a10:8009:cdd3:0:2b::	2a00:1450:4006:80d::	HTTP	461	GET /pagead/js/adsbygoogle.js HTTP/1.1
862	18.921773	2a10:8009:cdd3:0:2b::	2a10:8009:cdd3:0:60::	DNS	118	Standard query response 0xc5f9 A covid-19.unitarium.com A 23.229.240.161
863	18.921773	2a10:8009:cdd3:0:2b::	2a10:8009:cdd3:0:60::	DNS	173	Standard query response 0x2feb AAAA covid-19.unitarium.com SOA ns51.domaincontrol.com
1000	18.961092	2a10:8009:cdd3:0:2b::	2a10:8009:cdd3:0:60::	DNS	115	Standard query response 0x8bd3 A games.unitarium.com A 23.229.240.161
1001	18.961092	2a10:8009:cdd3:0:2b::	2a10:8009:cdd3:0:60::	DNS	170	Standard query response 0x8005 AAAA games.unitarium.com SOA ns51.domaincontrol.com
1008	18.961092	2a10:8009:cdd3:0:2b::	2a10:8009:cdd3:0:60::	DNS	114	Standard query response 0x24af A time.unitarium.com A 23.229.240.161
1009	18.961092	2a10:8009:cdd3:0:2b::	2a10:8009:cdd3:0:60::	DNS	169	Standard query response 0x2c84 AAAA time.unitarium.com SOA ns51.domaincontrol.com
1117	19.000261	10.0.0.18	23.229.240.161	HTTP	422	GET /js/cookies.min.js HTTP/1.1
2608	21.046226	10.0.0.18	23.229.240.161	HTTP	824	GET /favicon.ico HTTP/1.1
2685	21.242655	23.229.240.161	10.0.0.18	TCP	1454	80 → 62398 [ACK] Seq=23222 Ack=2435 Win=20480 Len=1400 [TCP segment of a reassembled PDU]
2686	21.242655	23.229.240.161	10.0.0.18	HTTP	1160	HTTP/1.1 404 Not Found (text/html)

7. זיהיתי את שתי החבילות (בקשה ותגובה) לפי המילה GET, והקישור ביניהן שנעשה ע"י wireshark (גם בתוך חבילת הבקשה ניתן לראות הפנייה – response in frame: 371). בחבילת התגובה אכן ניתן לראות שמתקבל קובץ html מהשרת. Get היא מתודה של פרוטוקול HTTP לבקשת מידע (במקרה הזה עמוד אינטרנט) משרת. בגישה הראשונה לאתר נראה בכותרת GET /, כלומר קבלת "הדף הראשי" של השרת, כשאחריה נראה עוד בקשות GET למידע משלים מהשרת.

No.	Time	Source	Destination	Protocol	Length	Info
364	6.294953	10.0.0.18	94.23.157.180	HTTP	533	GET / HTTP/1.1
371	6.354763	94.23.157.180	10.0.0.18	HTTP	457	HTTP/1.1 200 OK (text/html)
374	6.393476	10.0.0.18	94.23.157.180	HTTP	438	GET /styles.css?v18 HTTP/1.1
389	6.454907	94.23.157.180	10.0.0.18	HTTP	728	HTTP/1.1 200 OK (text/css)
434	6.581482	10.0.0.18	52.217.0.109	HTTP	449	GET /cc.silktide.com/cookieconsent.latest.min.js HTTP/1.1
437	6.757684	52.217.0.109	10.0.0.18	HTTP/X..	308	HTTP/1.1 403 Forbidden
443	6.791508	10.0.0.18	94.23.157.180	HTTP	481	GET /favicon.ico HTTP/1.1
462	6.855228	94.23.157.180	10.0.0.18	HTTP	328	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

8. נסתכל על חבילת הבקשה :

א. כשאני בוחר בפורמט זמן של milliseconds, ניתן לראות שפקטת התגובה (מס' 371 בהקלטה) הגיעה 60 מאיות השנייה לאחר שליחת הבקשה :

No.	Time	Source	Destination	Protocol	Length	Info
364	6.294	10.0.0.18	94.23.157.180	HTTP	533	GET / HTTP/1.1
371	6.354	94.23.157.180	10.0.0.18	HTTP	457	HTTP/1.1 200 OK (text/html)
374	6.393	10.0.0.18	94.23.157.180	HTTP	438	GET /styles.css?v18 HTTP/1.1
389	6.454	94.23.157.180	10.0.0.18	HTTP	728	HTTP/1.1 200 OK (text/css)
434	6.581	10.0.0.18	52.217.0.109	HTTP	449	GET /cc.silktide.com/cookieconsent.latest.min.js HTTP/1.1
437	6.757	52.217.0.109	10.0.0.18	HTTP/X..	308	HTTP/1.1 403 Forbidden
443	6.791	10.0.0.18	94.23.157.180	HTTP	481	GET /favicon.ico HTTP/1.1
462	6.855	94.23.157.180	10.0.0.18	HTTP	328	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

ב. גרסת ה-http מופיעה בשורת ה-info והיא 1.1.

ג. הבקשה נשלחה מהמחשב שלי, בכתובת 10.0.0.18 (מפורט 62585).

ד. חבילת התגובה נמצאת בשורה מס' 371 (מופיעה בתמונה לעיל).

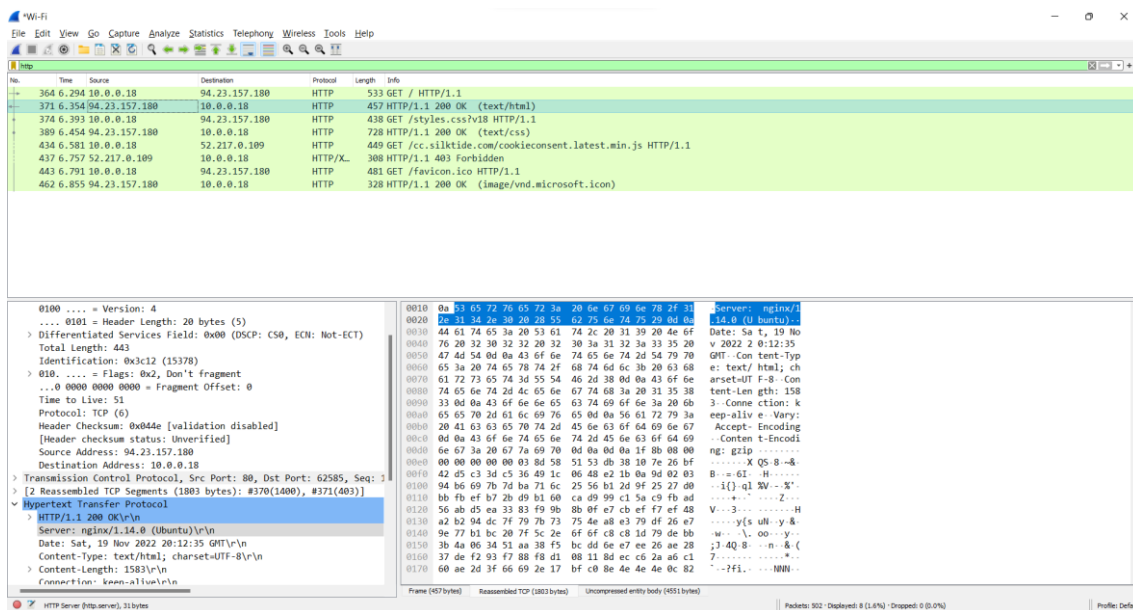
ה. חבילת הבקשה הגיעה לפורט היעד 80, שהוא פורט הסטנדרטי לתעבורת HTTP בשרתים:

```
Source Address: 10.0.0.18
Destination Address: 94.23.157.180
Transmission Control Protocol, Src Port: 62585, Dst Port: 80, Seq: 1
Source Port: 62585
Destination Port: 80
```

9. נסתכל על חבילת התגובה:

א. קוד התגובה הוא OK, כלומר הבקשה התקבלה והקובץ המבוקש צורף לחבילת התגובה.

ב. התגובה התקבלה משרת מסוג ubuntu, שנמצא ב-IP 94.23.157.180:



ג. החבילה הורכבה משתי חבילות TCP:

```
[2 Reassembled TCP Segments (1803 bytes): #370(1400), #371(403)]
[Frame: 370, payload: 0-1399 (1400 bytes)]
[Frame: 371, payload: 1400-1802 (403 bytes)]
[Segment count: 2]
[Reassembled TCP length: 1803]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a53657276
```

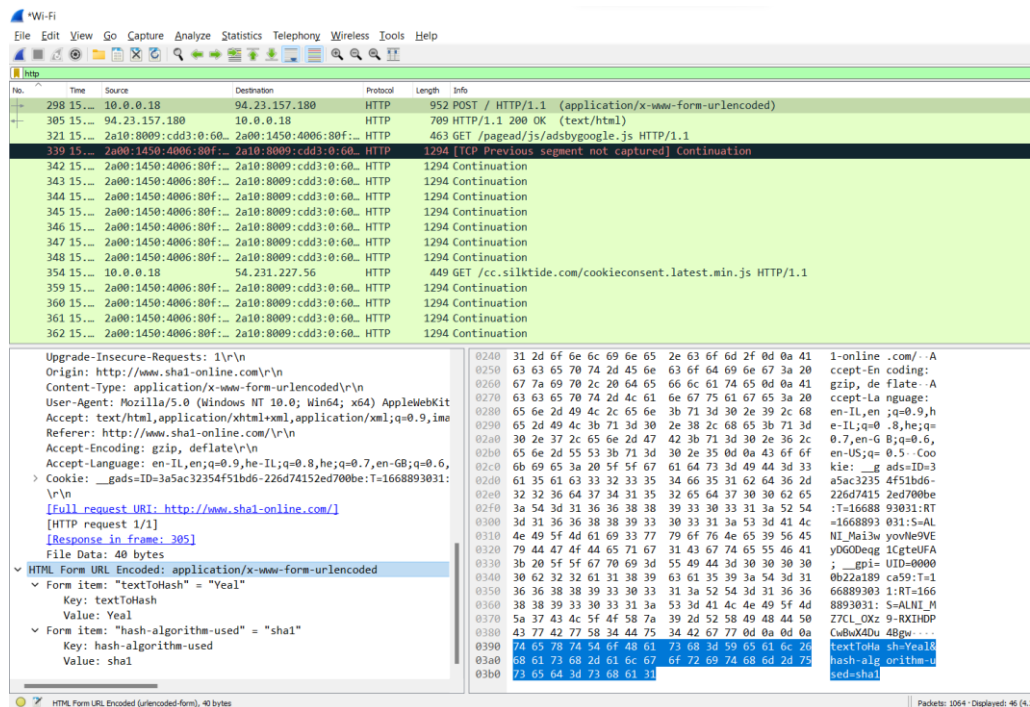
ד. סוג הקשר בין השרת ללקוח הוא keep-alive, כלומר קשר פרסיסטנטי. המשמעות היא שהקשר לא ייסגר לאחר בקשת ה-get הראשונה, אלא יישאר פתוח ורציף לכל בקשות ה-get של הלקוח מהשרת. כך, הלקוח לא יצטרך לחדש קשר עם השרת לכל בקשה שיש, והחיבור רציף ומהיר יותר.

```
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Server: nginx/1.14.0 (Ubuntu)\r\n
Date: Sat, 19 Nov 2022 20:12:35 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Content-Length: 1583\r\n
Connection: keep-alive\r\n
```

10. הכנסתי שם ולחצתי על hash:

א. החישוב נעשה בדפדפן. ניתן לראות בפקטה שהוחרזה שהחישוב נעשה בפורמט html (פורמט web) ע"י שימוש בפרמטרים שהוזנו בפקטת ה-post.

ב. בבקשה שנשלחה נוספו 2 פרמטרים למילוי בטופס ה-html: השם שהוזן עבור ה-hashing (ערך textToHash) ואלגוריתם ה-hashing שבחרתי (ערך hash-algorithm-used):



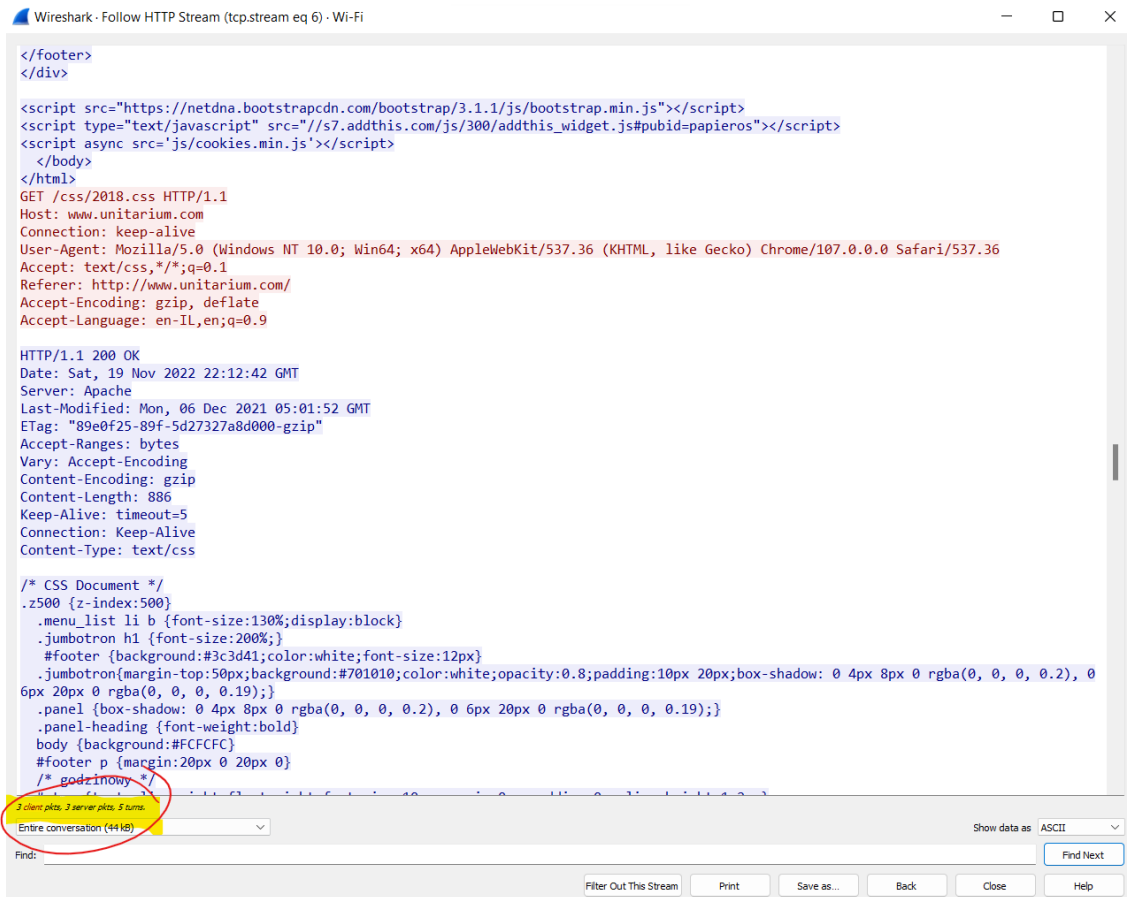
ג. חישוב בצד הלקוח היה מיותר את פעולת ה-hashing, כיוון שפריצה ל-DB של האתר הייתה נותנת לתוקף את כל מה שהוא צריך עבור גישה לכלל החשבונות – ה-hashים שנוצרו בצד הלקוח היו נשלחים לשרת, ולכן היו משרתים בעצמם כסיסמאות. ברגע שהחישוב נעשה בצד השרת, הלקוח שולח סיסמא והסיסמא מותאמת ע"י האתר ל-hash שמספק גישה לאתר. במצב זה, פריצה ל-DB לא נותנת לפורץ את היכולת להשתמש בסיסמאות ללא פיצוח של הסיסמאות העמדות מאחוריהן.

ד. החזרת תשובה מרחוק במקום חישוב בדפדפן עלולה לייצר הזדמנות ל-man in the middle: אם התוקף יושב על התעבורה שבין הדפדפן לשרת (פריצה של קו תעבורה יחיד), הוא יוכל לקלוט את כל התעבורה מהדפדפן לשרת. כך, התוקף יוכל לקלוט כל שם שמוזן בדפדפן, להתחזות לשרת ולהחזיר hash מזויף כרצונו, וכך בעצם להשתלט באופן מלא על ה-hashים של הדפדפן. כשהחישוב מבוצע בדפדפן עצמו, ע"מ שהתוקף יוכל להשתלט על כלל ה-hashים הוא יצטרך לשבת על התעבורה שבין הלקוחות השונים לבין הדפדפן בשביל לבצע תקיפת man in the middle, מה שידרוש הרבה יותר מאמץ.

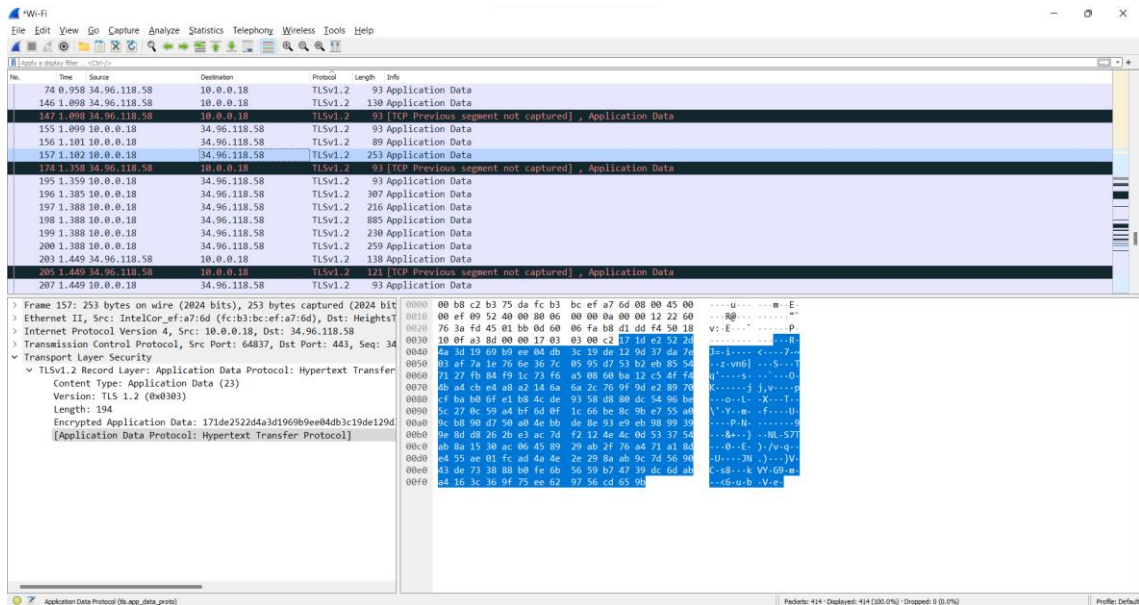
11. נשלחו 3 חבילות מהלקוח לשרת, ו-3 חבילות נשלחו בתגובה מהשרת ללקוח:

- החבילה הראשונה החזירה קובץ html של הדף הראשי של האתר.
- החבילה השנייה החזירה קובץ css, שנועד לספק את העיצוב של דף ה-html.
- החבילה השלישית החזירה את התמונות שדף ה-html אמור להציג.





12. התקבלו פקטות מוצפנות, בפרוטוקול TLSv1.2. הגישה לאתר https מאובטחת ומוצפנת בין שני הקצוות (שרת-לקוח במקרה הזה), ולכן לא ניתן לראות את פרטי הבקשה, אלא רק את נתוני המעטפת שאינם מוצפנים.



13. שם השרת לא ידוע (התקבל UnKnown), השרת אינו מהימן (Non-authoritative answer) וכתובות ה-IP של הדומיין הינן:

א. 151.101.131.10

ב. 151.101.67.10

ג. 151.101.3.10

ד. 151.101.195.10

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.1219]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bkeha>nslookup icecream.com
Server: UnKnown
Address: 2a10:8009:cdd3:0:2b8:c2ff:feb3:75da

Non-authoritative answer:
Name: icecream.com
Addresses: 151.101.131.10
           151.101.67.10
           151.101.3.10
           151.101.195.10
```

14. ביצעתי את השאילתה עם Wireshark מופעל (תיעוד לתשובות בסוף הסעיף):

- א. בוצעו 5 שאילתות לגבי הדומיין – 4 שאילתות לחיפוש שם הדומיין, ועוד שאילתת PTR.
- ב. להלן ההבדלים בין השאילתות:

1) שאילתת ה-PTR היא "שאילתת DNS הפוכה" שבדקת אם כתובת ה-IP הרשומה של האתר אכן מובילה וזהה לכתובת המילולית של האתר.

2) לאחר מכן קיימות שתי שאילתות DNS סטנדרטיות (אחת עבור כל סוג IP – v4 ו-v6), שבה המחשב בודק אם מידע אודות כתובת ה-IP של הכתובת icecream.com רשומה בשרת ה-root שלי (שרת ה-root שלי הוא של verisign, בכתובת a.root-servers.net). בקשות אלו נענו בשלילה.

3) לאחר קבלת תשובה שלילית על הימצאות כתובות ה-IP בשרת ה-root, נשלחו שתי שאילתות DNS סטנדרטיות לאיתור כתובות ה-IP (גם פה, v4 ו-v6) לפי פרוטוקול חיפוש של כתובות (TLD והלאה), אליהן התקבלו תגובות.

4) כלל הבקשות נשלחו על פרוטוקול תעבורה של UDP.

5) השאילתה נעשתה באופן רקורסיבי. מסקנה זו נובעת משתי עובדות:

א) לאחר שה-root לא מצא את הכתובות אצלו, נשלחה שאילתה נוספת מהמחשב לשירות אחר לחיפוש כתובת ה-IP המבוקשת. אם השאילתה הייתה נעשית איטרטיבית, פעולה זו הייתה נענית בהפנייה לשרת שתחתיו יושב הדומיין או לחלופין שרת אחר שיודע להמשיך להפנות אותי עד לקבלת הדומיין. מכיוון שנשלחה שאילתה אחת, וכל הפעולה נעשתה "מאחורי הקלעים" עד לקבלת תשובה (תהליך החיפוש היה "שקוף" למחשב שלי), ניתן להבין שהפעולה נעשתה באופן רקורסיבי.

ב) בבדיקת חבילת הבקשה ניתן לראות בסעיף Flags של ה-DNS שרשום "Recursion desired: Do query recursively", ובחבילת התגובה ניתן לראות שהבקשה נענית בחיוב "Recursion available: Server can do recursively".

6) התקבלו סה"כ 5 תגובות, אחת לכל שאילתה:

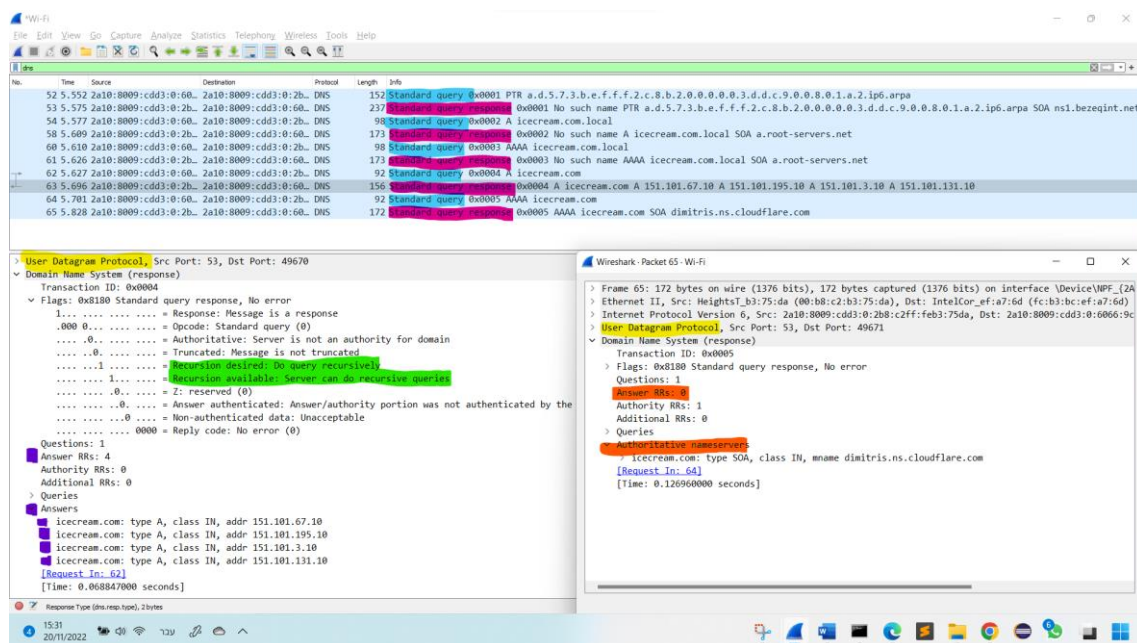
א) לשאילתה הראשונה (PTR) התקבלה תשובה שלילית (שהשם לא נמצא בכתובת ה-IP שנבדקה).

ב) לשאילות 2,3 (מול ה-root עצמו, לבדיקת הימצאות כתובת ה-IPv4 ו-IPv6 עליו) – התקבלו תשובות שליליות, שמלבד פרטים טכניים מזעריים (הגעה לפורט אחר) אין הבדלים ביניהן.

ג) לשאילתה 4 (חיפוש כתובת IPv4) התקבלה תגובה עם 4 תשובות – כתובות ה-IP השונות של הדומיין אותו חיפשנו.

ד) לשאילתה 5 (חיפוש כתובת IPv6) התקבלה תגובה ללא תשובה (אך ללא שגיאות), כשבתוכה הפנייה ל-zone חיפוש. המשמעות של תשובה זו היא שקיימת כתובת IPv4 אך לא קיימת כתובת IPv6.

7) ההבדל המהותי הוא שלכל אתר קיימת כתובת IPv4, לעומת IPv6 שטרם הוטמע באופן מלא. לכן, המשמעות של אי-קיום של כתובת IPv4 היא שהאתר לא קיים / אינו מחובר לאינטרנט (מצב בינארי), אך אי-קיום של כתובת IPv6 אינו מעיד באופן חד משמעי על מצב האתר בכתובת המילולית שחיפשנו.



15. שרת ה-DNS שלי:

א. כתובת mac - 2a10:8009:cdd3:0:2b8:c2ff:feb3:75da

ב. כתובת IP – 10.0.0.138



```
C:\WINDOWS\system32\cmd.exe

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : local
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : FC-B3-BC-EF-A7-6D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2a10:8009:cdd3:0:7bf3:4451:6743:8344(Preferred)
Temporary IPv6 Address. . . . . : 2a10:8009:cdd3:0:6066:9ca7:2d70:a768(Preferred)
Link-local IPv6 Address . . . . . : fe80::2a82:8289:2a5f:628a%3(Preferred)
IPv4 Address. . . . . : 10.0.0.18(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 19 תמוז 2022 19:46:10
Lease Expires . . . . . : 20 תמוז 2022 01:17:41
Default Gateway . . . . . : fe80::2b8:c2ff:feb3:75da%3
                             10.0.0.138
DHCP Server . . . . . : 10.0.0.138
DHCPv6 IAID . . . . . : 66892732
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-5E-D3-F0-FC-B3-BC-EF-A7-6D
DNS Servers . . . . . : 2a10:8009:cdd3:0:2b8:c2ff:feb3:75da
                             10.0.0.138
NetBIOS over Tcpip. . . . . : Enabled
```

16. אין ל-DNS של IPv6.

17. בוצע:

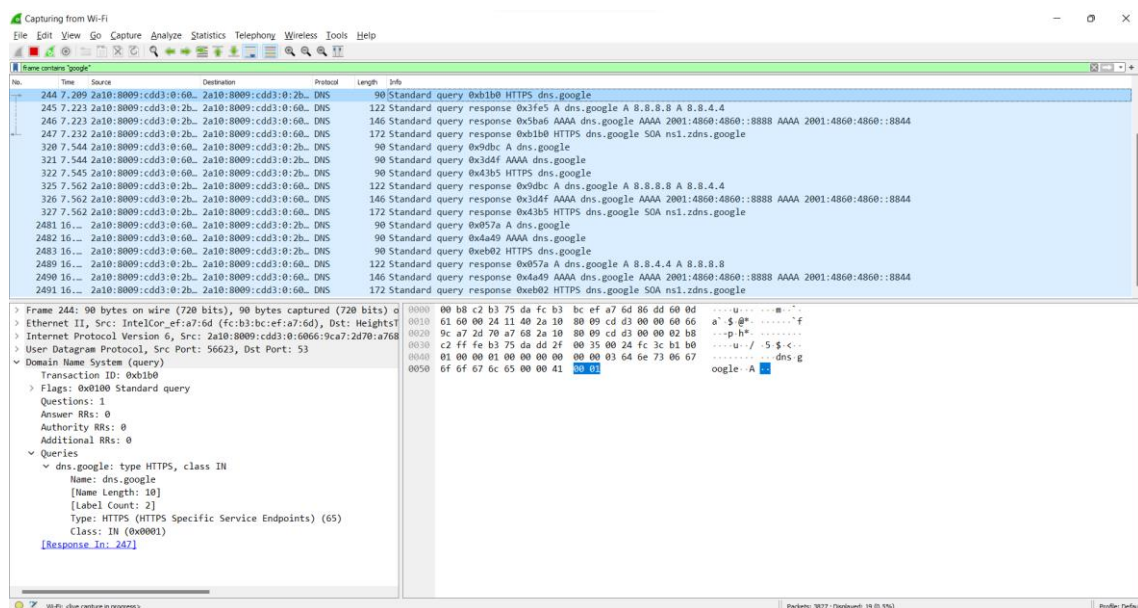
```
C:\WINDOWS\system32\cmd.exe

IPv4 Address. . . . . : 10.0.0.18(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 19 תמוז 2022 19:46:10
Lease Expires . . . . . : 20 תמוז 2022 01:47:52
Default Gateway . . . . . : fe80::2b8:c2ff:feb3:75da%3
                             10.0.0.138
DHCP Server . . . . . : 10.0.0.138
DHCPv6 IAID . . . . . : 66892732
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-5E-D3-F0-FC-B3-BC-EF-A7-6D
DNS Servers . . . . . : 2a10:8009:cdd3:0:2b8:c2ff:feb3:75da
                             8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : FC-B3-BC-EF-A7-71
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

C:\Users\bkeha>
```



18. חבילת ה-response ל-query תמיד תהיה כבדה יותר מאשר חבילת ה-query עצמה, מכיוון ששתיהן בנויות באותו פורמט, אך חבילת ה-response תמיד תכיל את כל חבילת ה-query ובנוסף תכיל גם את התשובות לשאילתות, כלומר, השאילתה מוכלת בתוך התשובה, אך התשובה אינה מוכלת בשאילתה, ולכן התשובה גדולה ממש מהשאילתה.

19. להלן התיעוד :

א. הרשומה טרם המחיקה – בנספחים.

ב. לאחר המחיקה :

```
C:\WINDOWS\system32\cmd.exe
C:\Users\bkeha>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\bkeha>ipconfig /displaydns
Windows IP Configuration

mssplus.mcafee.com
-----
No records of type AAAA

mssplus.mcafee.com
-----
Record Name . . . . . : mssplus.mcafee.com
Record Type . . . . . : 1
Time To Live . . . . . : 0
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 0.0.0.1

scinstallcheck.mcafee.com
-----
No records of type AAAA

scinstallcheck.mcafee.com
-----
Record Name . . . . . : scinstallcheck.mcafee.com
Record Type . . . . . : 1
Time To Live . . . . . : 0
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 0.0.0.1

1.0.0.0.in-addr.arpa
-----
Record Name . . . . . : 1.0.0.0.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 0
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : scinstallcheck.mcafee.com
```

ג. להלן ה-displaydns לאחר הפינג ל-icecream.com. הדומיין יהיה רשום ברשומה למשך 290 שניות, כפי שרשום בסעיף ה-TTL :

```
C:\WINDOWS\system32\cmd.exe
C:\Users\bkeha>ping icecream.com

Pinging icecream.com [151.101.131.10] with 32 bytes of data:
Reply from 151.101.131.10: bytes=32 time=50ms TTL=54
Reply from 151.101.131.10: bytes=32 time=54ms TTL=54
Reply from 151.101.131.10: bytes=32 time=50ms TTL=54
Reply from 151.101.131.10: bytes=32 time=72ms 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 = 50ms, Maximum = 72ms, Average = 56ms

C:\Users\bkeha>ipconfig /displaydns

Windows IP Configuration

icecream.com
-----
Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 290
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 151.101.131.10

Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 290
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 151.101.3.10

Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 290
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 151.101.67.10

Record Name . . . . . : icecream.com
Record Type . . . . . : 1
Time To Live . . . . . : 290
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 151.101.195.10
```

20. גלישה לאתר מתבצעת באופן הבא :

- א. ראשית, המכשיר ממנו אני מנסה לגלוש לאתר יבדוק אם כתובת האתר שהזנתי נמצא בזיכרון ה-cache של המכשיר, כלומר האם המכשיר יודע בעצמו לתרגם את הכתובת המילולית שהזנתי בשורת החיפוש לכתובת ה-IP של השרת המאחסן של האתר אותו אני מחפש. ההנחה בשאלה היא שכתובת ה-IP של האתר אינה שמורה ב-cache שלי, ולכן המכשיר יפעל לפי פרוטוקול DNS לאיתור כתובת ה-IP.
- ב. ע"מ למצוא את ה-IP, יתחיל המכשיר בסדרת שאילתות ל-DBים המאחסנים מעין "מילון" של תרגום כתובות מילוליות לכתובות ה-IP. השאילתה הראשונה תלך לשרת root, בד"כ בהכוונה של ה-ISP. שרת ה-root יכווין את השאילתה לשרת TLD בהתאם לסוג הסיימת של כתובת האתר. שרת ה-TLD יכווין לשרת נמוך יותר בהיררכיה שמאחסן את הדומיין (שם כללי של האתר – ariel, google, amazon) המבוקש.
- ג. השרת המאחסן של הדומיין המבוקש יחזיר את השאילתה חזרה לשואל המקורי (אני) בתצורה של query response (חבילת תגובה לשאילתה). בתוך החבילה, יהיו תשובות לשאילתה בתצורת פרטים על הדומיין אותו חיפשתי וכיצד למצוא אותו – כתובת ה-IP של האתר אותו חיפשתי (המוען של חבילת התגובה), השם האמיתי של הדומיין וכו'.
- ד. מרגע זה המחשב שלי יודע למצוא את האתר אותו אני מחפש (כתובת ה-IP של האתר), ולכן הפעולה הבאה של המחשב תהיה פנייה לכתובת ה-IP שקיבלתי עם בקשה לקבלת קובץ התצוגה של האתר אותו חיפשתי. בהתאם להנחות במטלה, נניח שהאתר אינו מאובטח ולכן

התקשורת מתנהלת בפרוטוקול http. לכן הבקשה לקבלת קובץ התצוגה תהיה כבקשת get של הדפדפן.

ה. אם הפעולה תקינה והאתר תקין, תישלח חזרה מהאתר חבילת תגובה עם אישור של הבקשה (ok) וקובץ html (או כל ייצוג אחר) של הנתביב אותו רשמתי בשורת החיפוש. במידה וקיימים קבצים משלימים לתצוגה של הדפדפן (כגון קבצי css, ad-ons וכולי), בקשות ותשובות לקבלת קבצים אלו יעברו אוטומטית למחשב שלי.

ו. כעת, כתלות בהגדרות השרת, הקשר יוכל להיסגר עם סיום כל בקשת get (non-persistent), או להישאר פתוח להמשך תקשורת בין הלקוח לשרת כחלק מאותו "סשן" (persistent).

## נספח – רשומת ה-DNS השמורים לפני המחיקה

```
C:\WINDOWS\system32\cmd.exe

Windows IP Configuration

realprotect1.mcafee.com
-----
Record Name . . . . . : realprotect1.mcafee.com
Record Type . . . . . : 5
Time To Live . . . . . : 3
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : realprotect1.realprotectcloud.com

Record Name . . . . . : realprotect1.realprotectcloud.com
Record Type . . . . . : 1
Time To Live . . . . . : 3
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 18.158.137.188

Record Name . . . . . : realprotect1.realprotectcloud.com
Record Type . . . . . : 1
Time To Live . . . . . : 3
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 3.70.83.66

www.qacafe.com
-----
Record Name . . . . . : www.qacafe.com
Record Type . . . . . : 1
Time To Live . . . . . : 74133
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 69.16.221.138

array509.prod.do.dsp.mp.microsoft.com
-----
Record Name . . . . . : array509.prod.do.dsp.mp.microsoft.com
Record Type . . . . . : 1
Time To Live . . . . . : 661
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 52.184.217.56
```



```
C:\WINDOWS\system32\cmd.exe

array513.prod.do.dsp.mp.microsoft.com
-----
Record Name . . . . . : array513.prod.do.dsp.mp.microsoft.com
Record Type . . . . . : 1
Time To Live . . . . . : 1485
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 52.184.214.53

insight.adsrvr.org
-----
Record Name . . . . . : insight.adsrvr.org
Record Type . . . . . : 1
Time To Live . . . . . : 9213
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 3.33.220.150

Record Name . . . . . : insight.adsrvr.org
Record Type . . . . . : 1
Time To Live . . . . . : 9213
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 52.223.40.198

Record Name . . . . . : insight.adsrvr.org
Record Type . . . . . : 1
Time To Live . . . . . : 9213
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 35.71.131.137

Record Name . . . . . : insight.adsrvr.org
Record Type . . . . . : 1
Time To Live . . . . . : 9213
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 15.197.193.217

mssplus.mcafee.com
-----
No records of type AAAA
```

```
C:\WINDOWS\system32\cmd.exe

mssplus.mcafee.com
-----
Record Name . . . . . : mssplus.mcafee.com
Record Type . . . . . : 1
Time To Live . . . . . : 0
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 0.0.0.1

sync.technoratimedia.com
-----
Record Name . . . . . : sync.technoratimedia.com
Record Type . . . . . : 1
Time To Live . . . . . : 13743
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 129.159.70.95

pixel.wp.com
-----
Record Name . . . . . : pixel.wp.com
Record Type . . . . . : 1
Time To Live . . . . . : 1764
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 192.0.76.3

play.google.com
-----
Record Name . . . . . : play.google.com
Record Type . . . . . : 1
Time To Live . . . . . : 31
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 172.217.19.142

scinstallcheck.mcafee.com
-----
No records of type AAAA

scinstallcheck.mcafee.com
-----
Record Name . . . . . : scinstallcheck.mcafee.com
```

```
C:\WINDOWS\system32\cmd.exe
scinstallcheck.mcafee.com
-----
Record Name . . . . . : scinstallcheck.mcafee.com
Record Type . . . . . : 1
Time To Live . . . . . : 0
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 0.0.0.1

moodlearn.ariel.ac.il
-----
Record Name . . . . . : moodlearn.ariel.ac.il
Record Type . . . . . : 1
Time To Live . . . . . : 791
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 34.96.118.58

moodlearn.ariel.ac.il
-----
Record Name . . . . . : moodlearn.ariel.ac.il
Record Type . . . . . : 1
Time To Live . . . . . : 791
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 34.96.118.58

ctldl.windowsupdate.com
-----
Record Name . . . . . : ctldl.windowsupdate.com
Record Type . . . . . : 5
Time To Live . . . . . : 2
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : wu-bg-shim.trafficmanager.net

Record Name . . . . . : wu-bg-shim.trafficmanager.net
Record Type . . . . . : 5
Time To Live . . . . . : 2
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : wu.azureedge.net
```