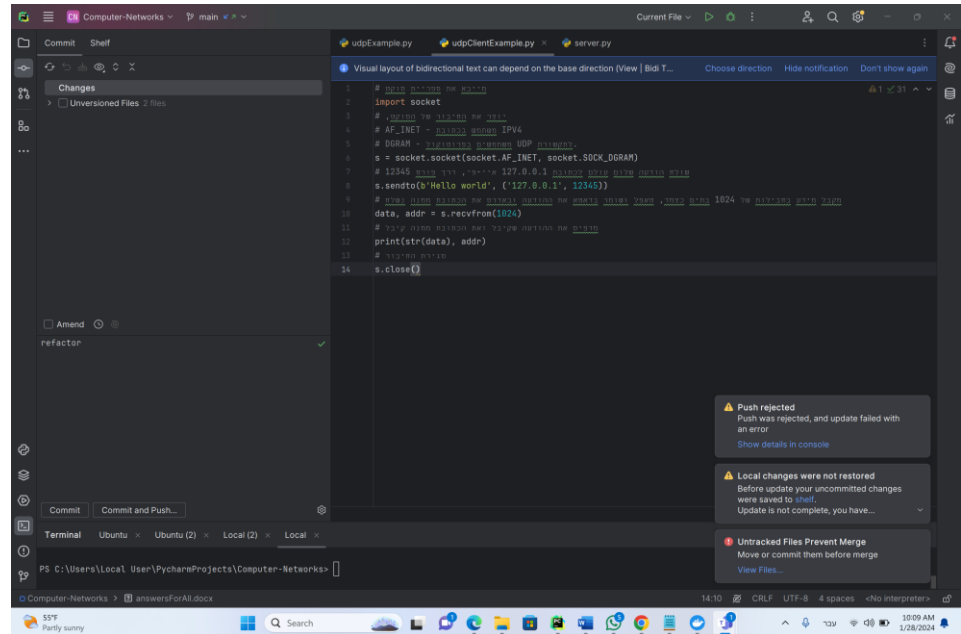


חלק 1

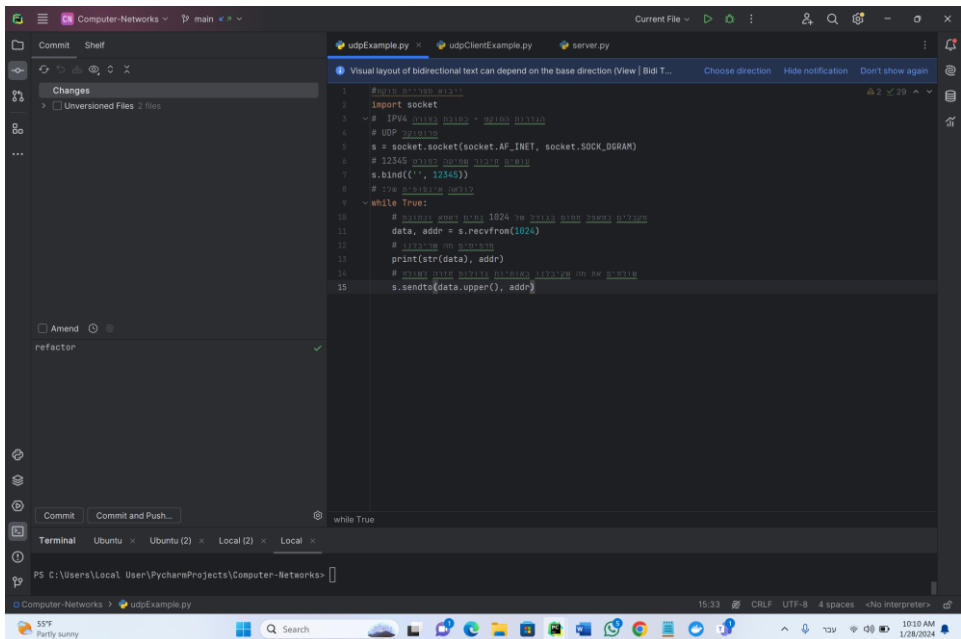
בחלק זה התבקשנו להעתיק מההרצאה שקופיות קוד.

לקוח:



```
1 # Import the socket module
2 import socket
3
4 # Create a socket object
5 s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
6
7 # Send data to the server
8 s.sendto('Hello world', ('127.0.0.1', 12345))
9
10 # Receive data from the server
11 data, addr = s.recvfrom(1024)
12
13 # Print the received data
14 print(str(data), addr)
15
16 # Close the socket
17 s.close()
```

שרת:



```
1 # Import the socket module
2 import socket
3
4 # Create a socket object
5 s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
6
7 # Bind the socket to the address
8 s.bind(('', 12345))
9
10 # Listen for incoming messages
11 while True:
12     # Receive data from the client
13     data, addr = s.recvfrom(1024)
14
15     # Print the received data and address
16     print(str(data), addr)
17
18     # Send the received data back to the client
19     s.sendto(data.upper(), addr)
```

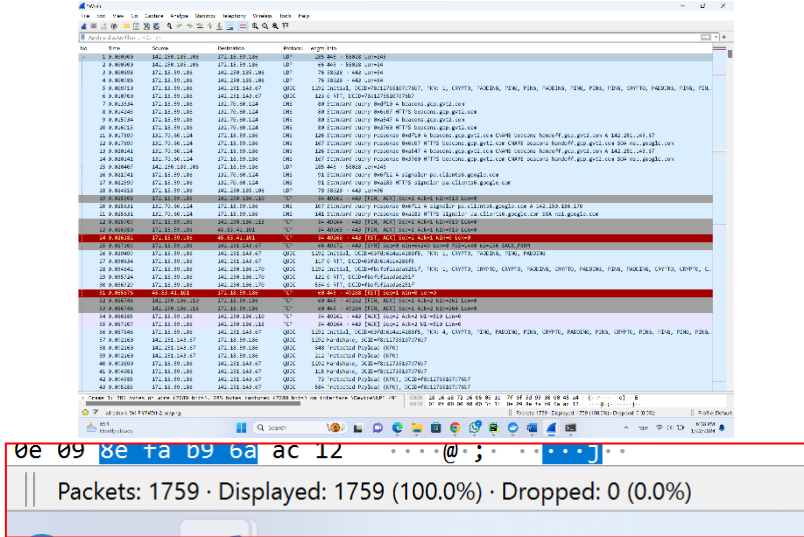
חלק 2

פתחו את wireshark (במידת הצורך - הורידו והתקינו את wireshark).
ביחרו את כרטיס הרשת שאתם גולשים דרכו והתחילו להסניף את המידע.
פתחו דפדפן וגלשו באינטרנט למספר אתרים.

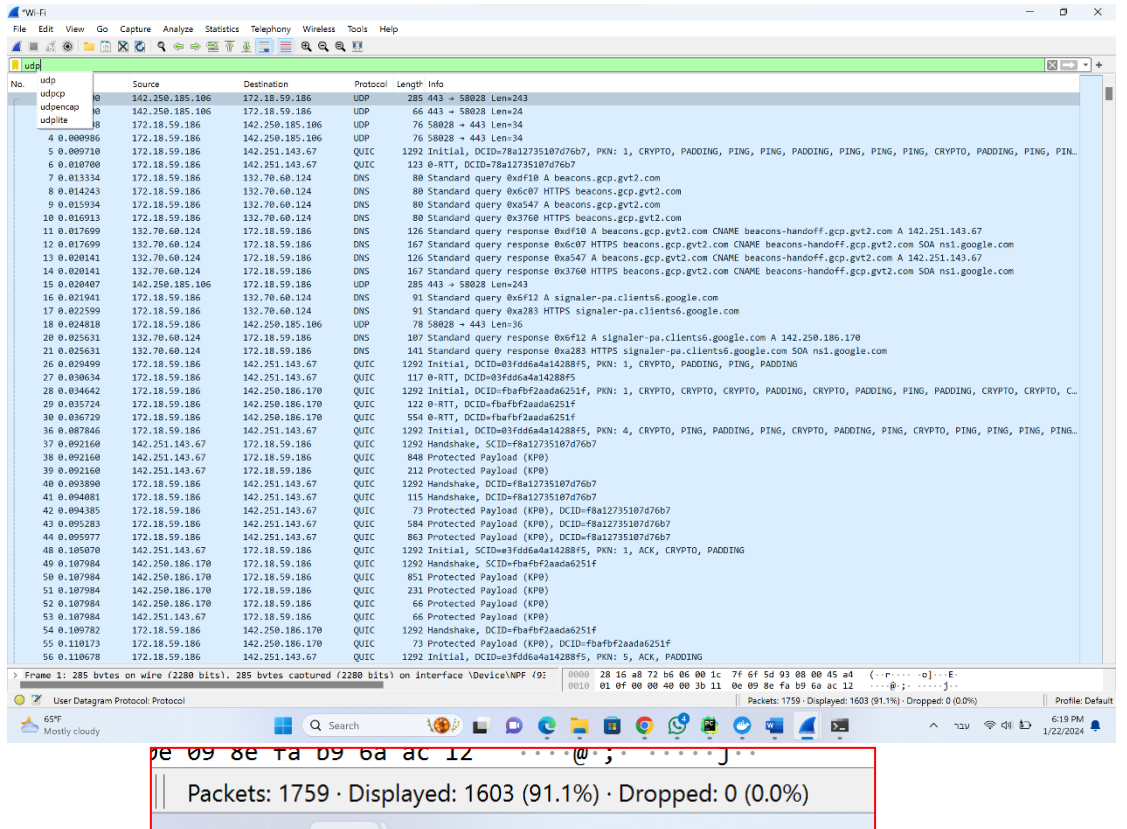
עיצרו את הסנפת התעבורה.

א.

כמה חבילות הוסנפו? (הסתכלו בחלק התחתון של התוכנה הוסנפו 1759 חבילות



ב בעזרת שורת הסינון, סננו רק חבילות שנשלחו על גבי פרוטוקול udp.
יש 1603 חבילות בפרוטוקול UDP



ג. בידקו מהי כתובת ה IP במחשב שלכם שאתם משתמשים בה כרגע (למשל בעזרת
ipconfig/ifconfig).
הכתובת של המחשב שלנו: 172.18.59.186

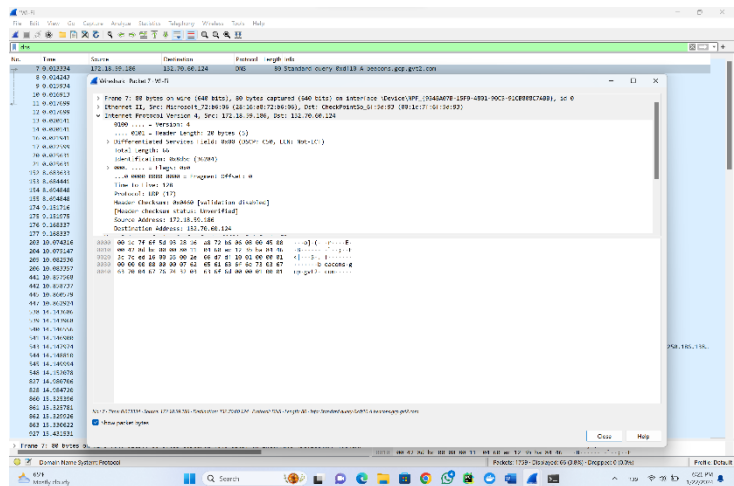
```
Command Prompt
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 10:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::b2e0:7c7c:c03a:af34%15
IPv4 Address. . . . . : 192.168.230.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::1ed1:7ba1:83d9:50a3%23
IPv4 Address. . . . . : 192.168.190.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : biu.ac.il
Link-local IPv6 Address . . . . . : fe80::7c2f:4002:790e:c6dc%14
IPv4 Address. . . . . : 172.18.59.186
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 172.18.59.254
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter vEthernet (WSL (Hyper-V firewall)):
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::abf1:ea3d:feb4:7b0b%53
IPv4 Address. . . . . : 172.22.208.1
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
C:\Users\Local User>
```

Wireless LAN adapter Wi-Fi:

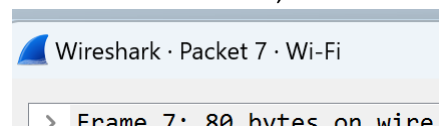
```
Connection-specific DNS Suffix . : biu.ac.il
Link-local IPv6 Address . . . . . : fe80::7c2f:4002:790e:c6dc%14
IPv4 Address. . . . . : 172.18.59.186
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 172.18.59.254
```

ד. מבין שלל החבילות שהסנפתם ביחור חבילת DNS (תוכלו לזהות אותה לפי העמודה Protocol). שימו לב, DNS הינו פרוטוקול שכבת אפליקציה, שרץ על גבי פרוטוקול udp בשכבת התעבורה.
- האם החבילה נשלחה אל המחשב שלכם או שאתם שלחתם אותה מהמחשב שלכם? הסבירו כיצד הגעתם למסקנה.

זה צילום מסך כללי לסעיף ובשביל הדגשות,
צילומים חלקי מסך



חבילה מספר 7, החבילה נשלחה מהמחשב שלנו, אנחנו שלחנו אותה.



ניתן להסיק זאת SRC IP ששווה ל 172.18.59.186 שזו בדיוק הכתובת IP שמצאנו בסעיף קודם למחשב שלנו.



- הסתכלו על פירוק החבילה לשכבות. מאיזה פורט נשלחה החבילה? לאיזה פורט נשלחה

החבילה? כלומר, לאיזה פורט האזין הלקוח ולאיזה פורט האזין השרת?

החבילה נשלחה אל פורט 53, השרת האזין לפורט 53

ונשלחה מפורט 60694, הלקוח האזין לפורט 60694

✓ User Datagram Protocol, Src Port: 60694, Dst Port: 53

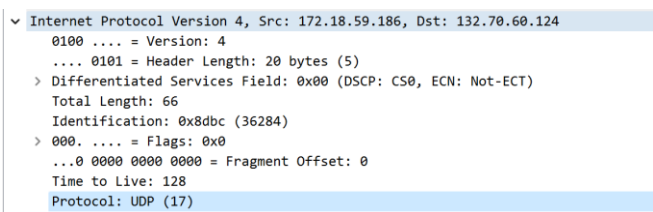
Source Port: 60694

Destination Port: 53

- הדגימו בתוך שכבת הרשת את כתובת ה IP של השולח ואת כתובת ה IP של המקבל.

שימו לב, במידה והחבילה שבחרתם אינה השתמשה ב IPv4, ביחרו חבילה אחרת (אם

אתם לא רואים כתובת IP כמו שראינו בכיתה - אזי ביחרו חבילה אחרת).

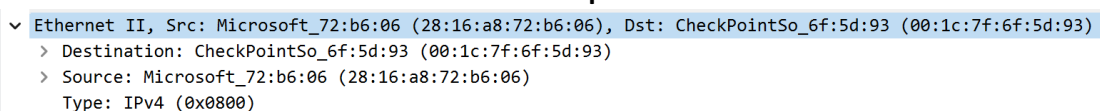


גרסא 4, IPv4

IP שולח: 172.18.59.186

IP מקבל: 132.70.60.124

- מהי כתובת ה MAC של השולח? ומהי של המקבל?



כתובת ה MAC של השולח:

28:16:a8:72:b6:06

כתובת ה MAC של המקבל:

00:1c:7f:6f:5d:93

ה. חיזרו על סעיף ד' - אך כעת עם החבילה ההפוכה. כלומר, אם בסעיף ד בחרתם בחבילה שהמחשב שלכם שלח - כעת ביחרו את החבילה שהמחשב שלכם קיבל. שימו לב, עליכם לבחור את החבילה הספציפית שמתאימה.

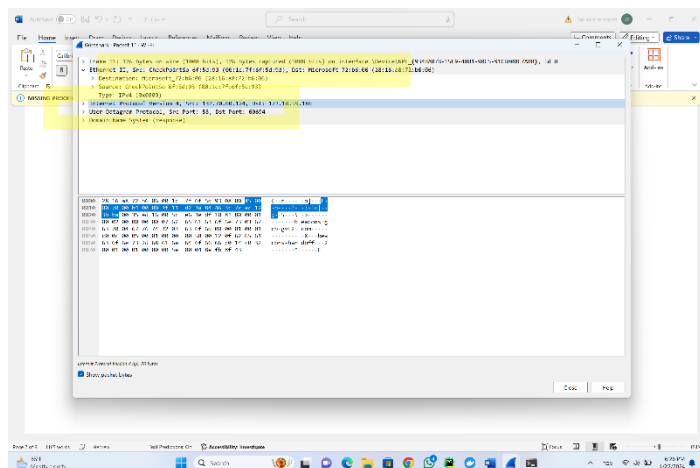
החבילה הספציפית המתאימה היא לא אחרת מאשר: 11

Time	Source	Destination	Protocol	Length	Info
7	0.013334	172.18.59.186	DNS	88	Standard query 0xdf10 A beacons.gvt2.com
8	0.014243	172.18.59.186	DNS	88	Standard query 0xc607 HTTPS beacons.gvt2.com
9	0.015934	172.18.59.186	DNS	88	Standard query 0xa547 A beacons.gvt2.com
10	0.016913	172.18.59.186	DNS	88	Standard query 0x3760 HTTPS beacons.gvt2.com
11	0.017699	132.70.60.124	DNS	126	Standard query response 0xdf10 A beacons.gvt2.com CNAME beacons-handoff.gvt2.com A 142.251.143.67

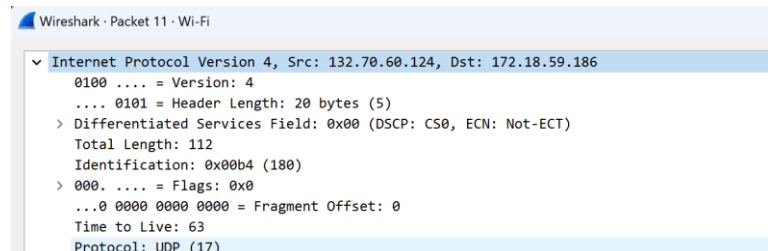
החבילה נשלחה אל המחשב שלנו

ניתן להסיק זאת מקו src שניתן לראות שהוא 132.70.60.124 שזוהי כתובת IP לא שלנו, וכן ה-DST IP היא בדיוק הכתובת של המחשב שענינו בג.

החבילה נשלחה מפורט אליו מאזין השרת – 53, ונשלחה אל הפורט אליו מאזין הלקוח -60694



הדגמת כתובות הIP.

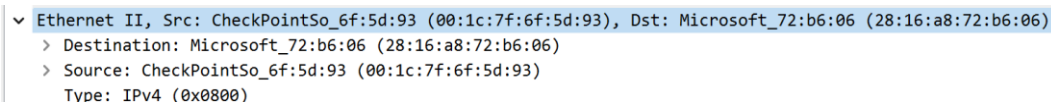


כתובת MAC של המקבל:

28:16:a8:72:b6:06

כתובת MAC של השולח:

00:1c:7f:6f:5d:93



ו. בעזרת שורת הסינון, סננו את כל החבילות כך שיופיעו רק חבילות שהמחשב שלכם שלח ורק חבילות בפרוטוקול DNS. הסתכלו על שכבת התעבורה של כמה מהחבילות - ובפרט על ה port source שלהם וה port destination שלהם. האם אתם שמים לב למשהו? מה המשמעות של זה?

שהשרת מאזין אליו)

[illegible]

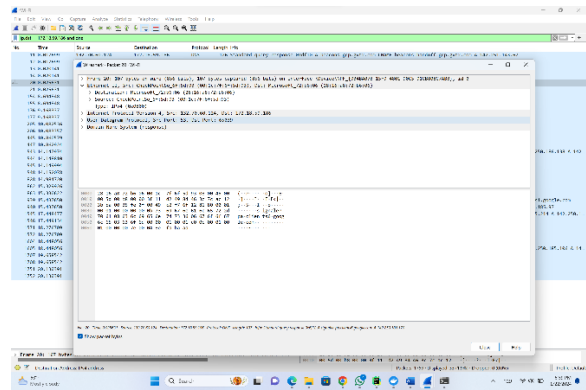
חבילות שהסתכלנו בהן...

התשובה כאן אמורה להשלים/לחזק את תשובתכם לסעיף הקודם.

[illegible]

חבילה שבדקנו כדי לראות את התכונה החוזרת, 53=SRC PORT

בשלחות מאותו מקור (השרת)

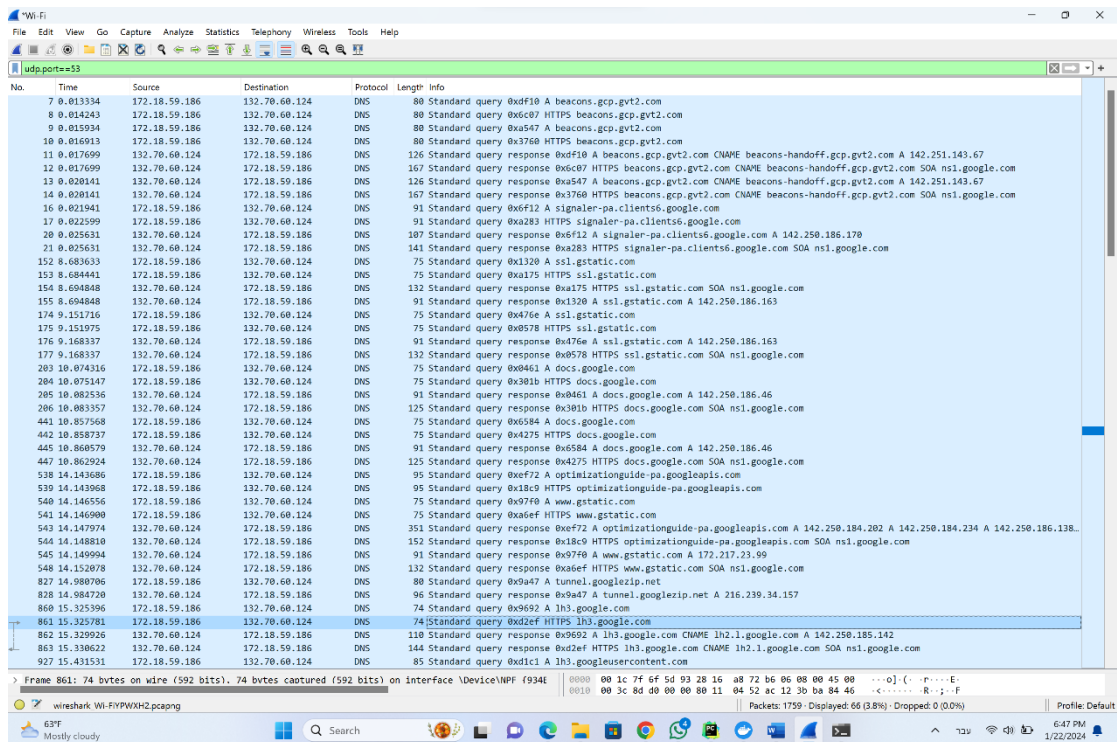


ז.

על בסיס תשובתיכם לשני הסעיפים האחרונים - כיצד תוכלו לבצע סינון בשורת הסינון לכל החבילות שנשלחו בפרוטוקול DNS, בלי לסנן מפורשות לפי DNS? (כלומר, אסור לכתוב בשורת הסינון)

נוכל לסנן ע"י מספר פורט (53)

יוציג לנו את כל החבילות שנשלחו בפרוטוקול DNS (החבילות שהפורט יעד שלהן הוא 53, אלו החבילות שהמחשב שלנו שלח לשרת, ואלה שהפורט מקור הוא 53 אלו הן החבילות שאנחנו קיבלנו מהשרת)



חלק 3

*בהוראות התרגיל היה רשום שרתים במחשב 1 ולקוח באחר, אבל מתגובת המרצה בפורום והנחיות נוספות הבנו שרק ע"י פיצול השרתים למחשבים נפרדים יהיה ניתן להסניף את כלל החבילות הקשורות לתוכנית.

IP address Father Server, Client : 10.100.102.186

IP address Son Server: 10.100.102.143

הרצנו את השרת בן ממחשב אחד, והלקוח ושרת אב ממחשב נוסף. נראה קודם כל תמונות להמחשת הריצה, ואז את ההסנפה.

שרת בן הרצנו עם פורט 12345, IP של אבא : 10.100.102.186, פורט אבא : 44444, וקובץ יעד: ips.txt שרת אב הרצנו עם פורט 44444, IP אבא : 1-, כנל על פורט אב כי אין אב, קובץ יעד: parent.txt

לקוח:

מבחינת ריצת לקוח:

ביקש כתובת biu.ac.il שיש לשרת בן, קיבל חזרה

1.2.3.4

אח"כ ביקש גוגל, לא היה בשרת בן, העביר לאבא

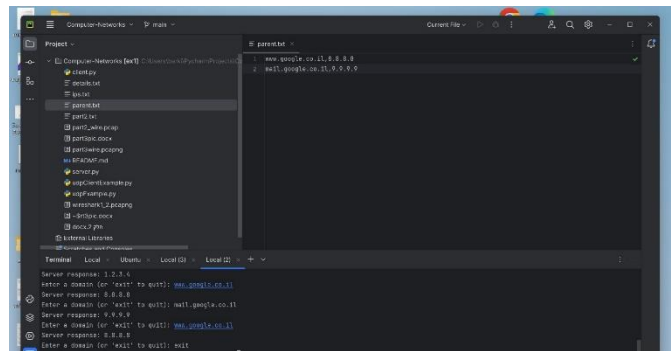
ואז חזר בסופו של דבר 8.8.8.8

ביקש מייל שגם לא היה בשרת בן, אך בסוף חזר

9.9.9.9

ואז ביקש שוב גוגל שעבשיו השרת בן מכיר וחזר

8.8.8.8



שרת בן:

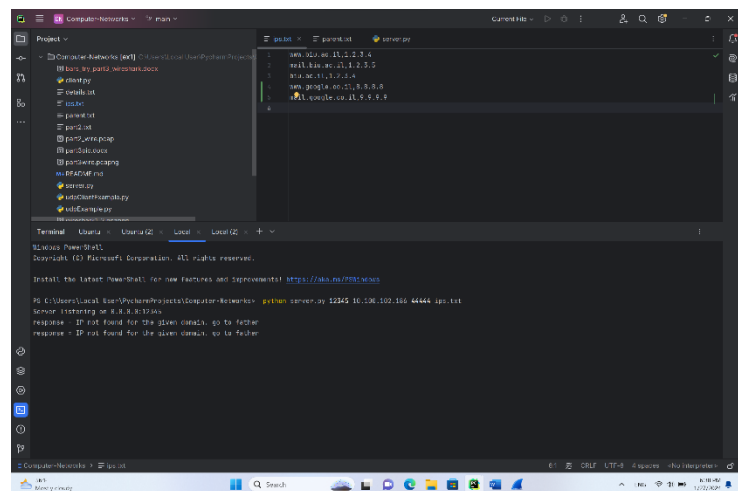
פה ניתן לראות את הטרימינל של ההרצה של

השרת בן + קובץ הידע שלו ips.txt מהפלט

רואים כי פעמיים הוא שלח בקשות למידה

לשרת אב ושאלו הקובץ שלו עודכן ב2 שורות

חדשות.

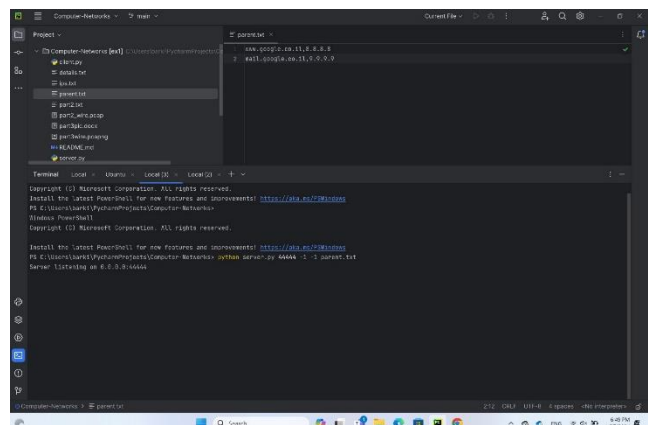


שרת אב:

מבחינת הרצה בשרת אב, לא הוספנו הדפסות אבל

אנחנו יודעים שהוא מסר מידע לגבי שתי כתובות

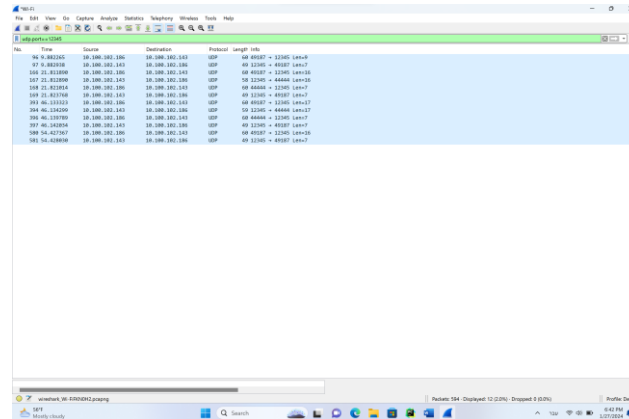
שהבן לא ידע והיה צריך "ללמוד"



נעבור כעת להסנפה, הסנפנו מהמחשב בו הרצנו את השרת בן, כי כך יכולנו לתפוס את התקשורת גם בין השרתים וגם בין השרת ללקוח.

מבחינת הסברים על החבילות, למען הסדר:

סיננו את ההסנפה לחבילות שעברו דרך 12345 משום שזה הפורט של השרת בן שנמצא במחשב אחד (בו ביצענו את ההסנפה) השרת בן שמתקשר גם עם הלקוח וגם עם השרת אב מאזין לפורט 12345 ולכן נתייחס לחבילות שעברו בפורט זה.



No.	Time	Source	Destination	Protocol	Length	Info
96	9.882265	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345 Len=9
97	9.882938	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187 Len=7
166	21.811890	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345 Len=16
167	21.812890	10.100.102.143	10.100.102.186	UDP	58	12345 → 44444 Len=16
168	21.821014	10.100.102.186	10.100.102.143	UDP	60	44444 → 12345 Len=7
169	21.823768	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187 Len=7
393	46.133323	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345 Len=17
394	46.134299	10.100.102.143	10.100.102.186	UDP	59	12345 → 44444 Len=17
396	46.139789	10.100.102.186	10.100.102.143	UDP	60	44444 → 12345 Len=7
397	46.142034	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187 Len=7
580	54.427367	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345 Len=16
581	54.428030	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187 Len=7

נסתכל מקרוב על החבילות של ריצת התוכנית שתפסנו:

No.	Time	Source	Destination	Protocol	Length	Info
96	9.882265	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345 Len=9
97	9.882938	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187 Len=7
166	21.811890	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345 Len=16
167	21.812890	10.100.102.143	10.100.102.186	UDP	58	12345 → 44444 Len=16
168	21.821014	10.100.102.186	10.100.102.143	UDP	60	44444 → 12345 Len=7
169	21.823768	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187 Len=7
393	46.133323	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345 Len=17
394	46.134299	10.100.102.143	10.100.102.186	UDP	59	12345 → 44444 Len=17
396	46.139789	10.100.102.186	10.100.102.143	UDP	60	44444 → 12345 Len=7
397	46.142034	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187 Len=7
580	54.427367	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345 Len=16
581	54.428030	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187 Len=7

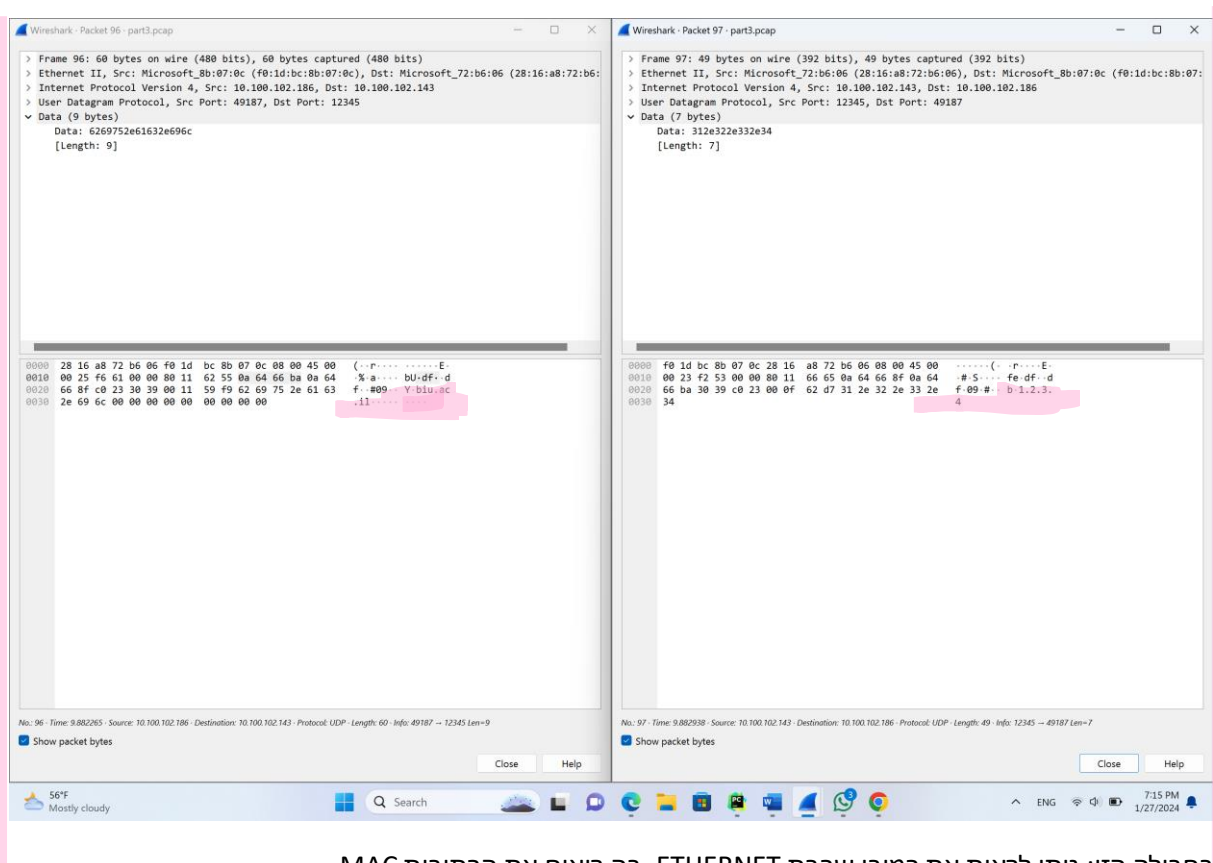
נסביר את הסימונים, מסדר התהליך שהסברנו בריצת התוכנית, אנחנו יודעים שהייתה בקשה לשרת בן לדבר שהוא יודע, אח"כ שתי בקשות שלא הכיר ולכן צריכה להיות תקשורת בין השרתים ואז בקשה שהשרת בן למד ולכן שוב רק בין השרת בן ללקוח.

בסימון כאן, ההדגשה בצהוב -> חבילות שעברו בין פורט שרת הבן לפורט לא ידוע שזהו ככל הנראה פורט הלקוח כי לא קיבענו אותו.

ריבוע אדום – בקשה ראשונה לכתובת ששרת הבן לא הכיר, ניתן לראות מעבר מהפורט של הלקוח ככל הנראה לבן, ואז מעבר לפורט 44444 שזה שרת אב וחזרה את התהליך.

ריבוע כתום – בקשה שני לכתובת שהשרת לא הכיר. ניתן לראות מעבר מהפורט של הלקוח ככל הנראה לבן, ואז מעבר לפורט 44444 שזה שרת אב וחזרה את התהליך.

ונעבור לחבילות הספציפיות לפי הסדר. נתחיל בסט הצהוב הראשון



בחבילה הזו: ניתן לראות את כמובן שכבת ETHERNET, בה רואים את הכתובות MAC

אח"כ שכבת ה-INTERNET, אנחנו רואים את כתובות ה-IP, הלקוח ב(186) שרת בן ב(143)

אחכ" DATAGRAM, את הפורטים – מעבר בין 49187 שזה כנראה הפורט שהלקוח שלנו קיבל לבין פורט 12345 שזה הפורט שהשרת בן מאזין לו.

צד שמאל זו החבילה שנשלחה מהלקוח אל השרת בן, נסתכל בשכבת ה-DATA, נראה שכתוב גיבריש אך אם נסתכל על ההדגשה למטה בפירוט ההודעה, ניתן לראות את התרגום של הגיבריש – זה בדיוק biu.ac.il שאנחנו יודעים מההרצה שזו בדיוק ההודעה ששלחנו מהלקוח.

ובצד ימין, מופיעה החבילת תגובה של השרת בן ללקוח וכמו שהיינו מצפים, ניתן לראות בשכבת ה-DATA, למטה בפירוט ההודעה את התרגום של ה-DATA = 1.2.3.4 שזו התגובה שהשרת החזיר ללקוח על השאלה הזו.

נסביר על הסט חבילות בריבוע האדום עכשיו.

ניתן לראות (משמאל לימין)

נשלחה הודעה מהלקוח (פורט 49187) ממחשב עם סיומת IP 186 כידוע.

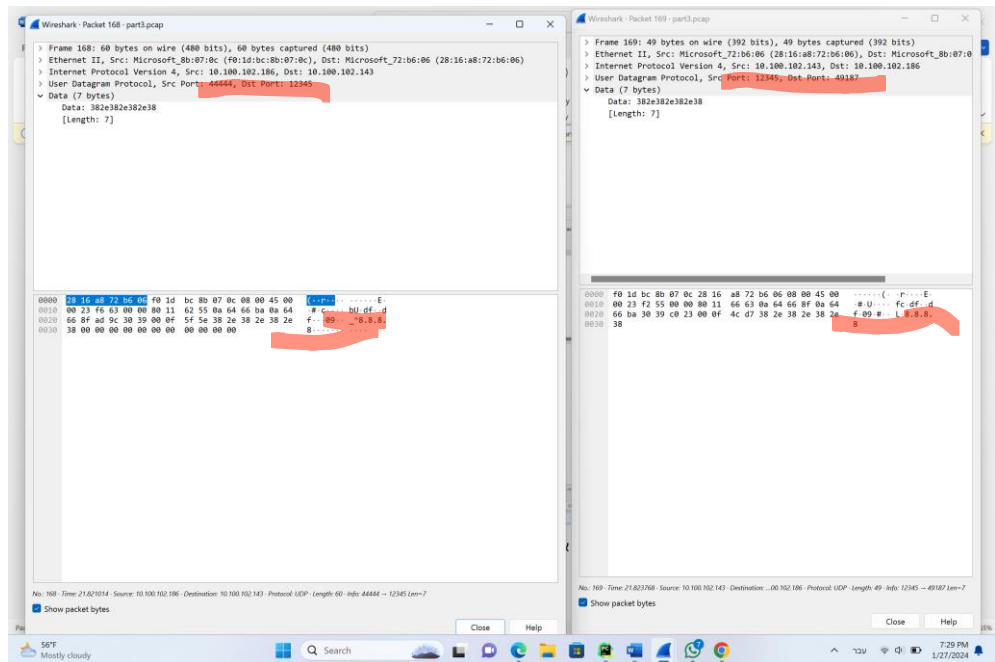
בהודעה כמו שנצפה מהרצה הלקוח מבקש את הכתובת של GOOGLE, וזה נשלח לשרת בן, שמאזין 12345 במחשב עם סיומת IP 143

ואז בצד ימין רואים שהשרת בן שולח דרך פורט 12345 לפורט

44444 את הבקשה של GOOGLE אל השרת אב בעצם, כי הוא לא מכיר עוד את הכתובת וצריך ללמוד אות.

לכן, ניתן לראות שבחבילה הבאה במספר – 168, (צד שמאל) אחרי שהשרת בן העביר את בקשת הלקוח שלא ידע לענות אליה אל שרת האב, השרת אב החזיר לשרת בן הודעה מ44444 ל12345 עם התשובה – 8.8.8.8

ואז בחבילה הבאה: 169, צד ימין, השרת בן מחזיר מ12345 ל49187 את התשובה אחרי שככל הנראה עדכן אצלו את המידע החדש, מחזיר ללקוח הודעה 8.8.8.8



עבור: הסט הבא לא אפרט כי זה בדיוק כמו הפירוט על הריבוע האדום שעשיתי עכשיו רק עבור כתובת אחרת.

393	46.133323	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345	Len=17
394	46.134299	10.100.102.143	10.100.102.186	UDP	59	12345 → 44444	Len=17
396	46.139789	10.100.102.186	10.100.102.143	UDP	60	44444 → 12345	Len=7
397	46.142034	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187	Len=7

(הריבוע הכתום)

ונעבור להסבר זריז על הסט הצהוב האחרון:

580	54.427367	10.100.102.186	10.100.102.143	UDP	60	49187 → 12345	Len=16
581	54.428030	10.100.102.143	10.100.102.186	UDP	49	12345 → 49187	Len=7

פה ניתן לראות את 2 החבילות
האחרונות בריצה – שמאל,
בקשה מהלקוח לשרת הבן,
GOOGLE, שהבן למד קודם.

ובגלל שהבן למד הוא יכול
להחזיר במסלול ההפוך את
8.8.8.8, התשובה ולא צריך
שוב עירוב של שרת האב.

