

משתתפי הפרויקט:

אילת ג'יבלי 208691675 ayelet47654@gmail.com

עדי מלאכי 207740846 adida901@gmail.com

אליעזר רווח 313368102 ezezer2@hotmail.com

MEASUREMENT OF VPN PERFORMANCE

מטרת הפרויקט:

מהו המחיר שנשלם על הצפנה מורכבת ביותר - הצפנה בשכבת הרשת?
הכנה למדידות - להבין איך פרוטוקול בסיסי של VPN עובד, וכן הפרוטוקולים הספציפיים שאותם נבחן.
המדידות - נבחן את השפעת השימוש במנהרה מאובטחת על שליחת המסרים ברשת- מהירות שליחתם, אורך המסרים, מסלול הנתבים.
לשם כך בחנו את שליחת המסרים בלי חקצ לעומת שליחת מסרים עם חקצ, וכמו כן בחנו את ההבדלים בין ספק חקצ בתשלום לספק חנימי.
בפרויקט זה לא נחקר אלגוריתמי הצפנה השונים או אלגוריתמי המיתוג.
התוצאות הצפויות - כאשר נשלח מסרים על ידי חקצ נצפה לראות שאורך המסר אכן יגדל, מהירות שליחת המסר וקבלת תשובה תואט משמעותית, שהמסר יעבור מסלול נתבים הרבה יותר ארוך.

הכנה למדידות:

מהו Virtual Private Network?

רשת וירטואלית פרטית מתייחס לטכנולוגיה המאפשרת הקמת רשת פרטית על גבי רשת ציבורית, המוסיפה אבטחה ופרטיות לכל מסר. כאשר שולחים מסר, כל שכבה במודל השכבות מוסיפה רישא משלה
מטרתו של חקצ היא הסתרת הרישא של שכבת הרשת בכל מסר שנשלח, על ידי הוספת רישא חדשה עם קו וירטואלי - שימוש בטכנולוגיית "tunneling".
בנוסף, ישנם מנגנוני הצפנת ההודעה ופענוח, ניהול מפתחות, זיהוי משתמשים ומכשירים.

על מה אנחנו מגנים בעת שימוש ב Vpn?

רישא של שכבת התעבורה כולל בתוכו מידע פרטי כמו: כתובת קו של השולח והמקבל.
כאשר מידע זה עובר ברשת, כל אחד שינסה להאזין לתקשורת יכול לקשר את האתרים אליהם נכנסת עם כתובת הקו שלך.
כמובן שגם כל המידע שעבר מהשכבות מעל - ייתכן שהוא מוצפן וייתכן שלא.
ולכן במקרה שבו הפרוטוקולים שהיו בשימוש בשכבות מעל לא היו מוצפנים, חקצ יצפין את כל המידע שעובר אליו משכבות אלו.

איך VPN מצפין את המידע?

תהליך תקשורת בעזרת vpn מורכב מ:

1. זיהוי הלקוח - כאשר מתחברים לשרת מתבצע תהליך של רישום, והענקת "מפתח" ללקוח. כל פעם שמסר נשלח לשרת הוא נשלח עם המפתח המזהה שהלקוח קיבל בהתחברות הראשונה.
2. הצפנת המידע בעת שליחת המסר - שימוש באלגוריתמי הצפנה ידועים להצפנת כל הרישא המקורי.
3. "tunneling" - הוספת רישא IP נוסף לפני הרישא המקורי של הIP. [ראה נספח 1.1](#)

כלים:

1. תוכנת nordVPN בתשלום, שעובדת עם פרוטוקול wireGuard.
2. תוכנת tunnelBear חינמית, שעובדת עם פרוטוקול openVpn. <https://nordvpn.com/he/fastest-vpn-site/>
3. תוכנת jperf משמשת למדידת bandwidth, delay jitter, datagram loss. התוכנה מאפשר לשנות פרמטרים ומאפיינים של tcp, udp. <https://www.tunnelbear.com/>
4. תוכנת wireshark כדי לנתח את החבילות והתעבורה. <https://github.com/andygrove/jperf>
5. תוכנת open visual trace כדי לצפות בזמן אמת במסלול הפיזי של החבילה. <https://www.wireshark.org/>
<https://visualtraceroute.net/>

המידדות:

- תנאי הניסויים: כל אחד מאיתנו יושב בביתו, המרחק הפיזי ביננו רחוק.
- התשתיות שונות:
- לקוח 1(אילת): תשתית הוט, חיבור קווי.
- לקוח 2(עדי): תשתית בזק ומעליו שירות סינון של אינטרנט רימון, עבודה על גבי WIFI.
- שרת(אלי): תשתית בזק, חיבור קווי.

1. ניתוח תקשורת מעל vpn בעזרת wireshark:

- מהלך הניסוי: הפעלנו את אפליקצית wireshark שתאזין לתקשורת על גבי NordVpn, (שרת - ישראל). הבחנו בנקודות הבאות:
1. כל התקשורת מופיעה תחת פרוטוקול wireguard ששולח עם פרוטוקול udp.
 2. כל המידע מוצפן ולא קריא.
 3. הקו היחיד שמופיע כיעד הינו הקו הוירטואלי שניתן לנו משרת החק! בשל כך, לא ניתן לסנן ולהאזין לתקשורת לפי ip של אתר או שרת ספציפי, וכן לא לפי פרוטוקול ספציפי משכבת התעבורה (tcp, http, ..), מאחר והכל מוסתר. [ראה נספח 2.1](#)
- כל אחד שינסה להקשיב לתעבורה מבחוץ לא יוכל להבין לאיזה אתרים התחברנו ואיזה מידע עבר. תוצאות הניסוי: לא ניתן לראות דרך wireshark האם אורך/נפח המסרים גדל מאחר שלא ניתן לזהות בין המסרים השונים.
- רמת האבטחה עם wireguard גבוהה מאוד.

2. בדיקה ראשונית של השפעת חקפ על איכות התקשורת בעזרת jperf:

נשתמש בתוכנת jperf על מנת להקים קשרי שרת - לקוח ביננו, השליחה מבוצעת עם פרוטוקול tcp.

[ראה נספח 3.1](#)

ניסוי ראשוני:

לקוח 1(אילת) ישלח מספר חבילות זהה בגדלי window size ו- max segment size משתנים לשרת(אלי).

פעם אחת ללא חקפ, ופעם אחת עם.

מטרת הניסוי - לבדוק האם רואים את יתרון בולט ללא חקפ ולשחק עם ההגדרות של השליחה.

במאמר של Guo Chao נעשה ניסוי דומה. [ראה נספח 3.2](#)

תוצאות הניסוי:

3. השוואה נוספת של השפעת חקפ על איכות התקשורת בעזרת jperf:

בעזרת הגדרות דיפולטיביות [ראה נספח 3.1](#), הלקוחות ישלחו לשרת את החבילות. השליחה בוצעה סה"כ 4 פעמים:

1. בלי חקפ.

2. עם nordVpn על גבי שרת מחוץ לישראל.

3. עם nordVpn על גבי שרת בישראל.

4. עם tunnelBear על גבי השרת הדיפולטיבי - romania.

לאחר מכן, ננסה מהצד השני - ליצור שרת מחובר ל חקפ.

נשווה בין התוצאות.

הניסוי בוצע מספר פעמים בימים שונים על מנת לוודא גרפים עקביים.

תוצאות הניסוי:

[ראה נספח 3.3](#) אצל לקוח 1(אילת)

כמו שציפינו בעת חיבור לשרתים הנמצאים במדינות מחוץ לישראל, ניתן לראות כי השליחה יותר איטית, פחות יציבה ויותר חבילות נאבדות בדרך.

רואים כי בעת שימוש בשרת חקפ מאיטליה החיבור איטי במיוחד.

אמנם, באופן לא צפוי, נראה שעם שרת חקפ בישראל, השליחה יותר מהירה ויציבה.

[ראה נספח 3.4](#) אצל לקוח 2(עדי)

ניתן לראות, שהגרפים של ללא חקפ ו- חקפ עם שרת מארה"ב מאוד דומים למעט בהתחלתם. להפתעתנו- שוב, רואים באופן מובהק כי עם שרת חקפ בישראל השליחה יותר מהירה ויציבה.

[ראה נספח 3.5](#) אצל השרת(אלי)

כמו שראינו קודם, בעת חיבור עם שרת מאיטליה, נאבדות המון חבילות בדרך והחיבור הואט משמעותית.

דרך ארצות הברית הגרף נשאר גם כן יחסית יציב, אך כן רואים האטה מצד השרת.

דרך שרת מישראל, נאבדות מעט חבילות אך לא נראה שינוי במהירות.

לא היה ניתן לפתוח שרת שמחובר ל חקפ.

4. השוואת ביצועים בין פרוטוקול wireguard לbין פרוטוקול openVPN:

לאחר הניסוי הקודם, העלנו את ההשערות הבאות לגבי שימוש ב חק:

1. המרחק הפיזי של השרת אותו בוחרים משפיע על הביצועים.

2. הפרוטוקול שבו הספק משתמש גם כן משפיע מאוד על הביצועים.

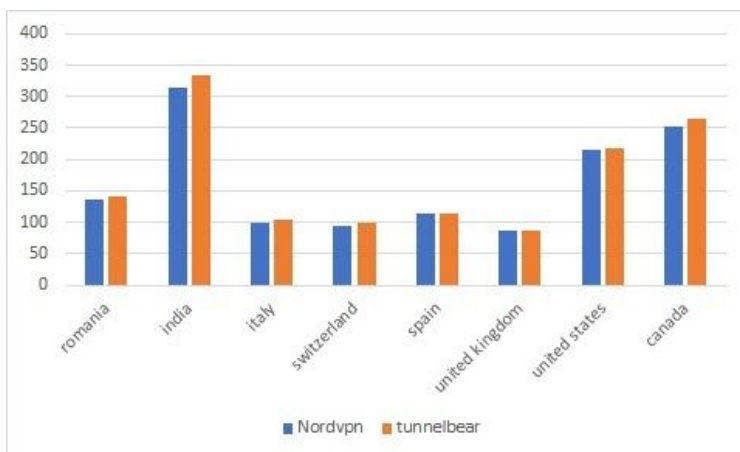
ולכן, החלטנו לבצע את הניסוי הבא:

שלחנו פינג לאתר של המכללה שוב ושוב, מ ספקי חק שונים - חינמי (tunnelBear) העובד על

פרוטוקול openVPN ובתשלום (nordVPN) העובד על פרוטוקול wireguard .

כל פעם בחרנו שרת במדינה אחרת (אקראית) והשוונו את המהירות הממוצעת שהתקבלה.

ראה נספח 4.1



מיקום שרת חק:	מהירות ממוצעת - wireguard:	מהירות ממוצעת - openVPN:	מרחק מישראל:
רומניה	137ms	140ms	2,811.4 km
הודו	314ms	334ms	4,532 km
איטליה	98ms	105ms	4,170.5 km
שווייץ	94ms	99ms	4,146.1 km
ספרד	115ms	115ms	5,478.7 km
בריטניה	88ms	86ms	5,529.4 km
ארה"ב	216ms	218ms	10,853 km
דנמרק	104ms	100ms	9,644 km

ניתן לראות כי nordVPN מספק תוצאות יותר טובות.

כמו כן, המרחק הפיזי של השרת מישראל השפיע במידה מסוימת, אבל לא תמיד.

אנחנו משערים שפקטור משפיע נוסף הוא כנראה איכות האינטרנט באותם המדינות. ראה נספח 4.2

5. מעקב אחרי נתיב החבילה:

לסיום, עקבנו אחרי מסלול החבילה עד לשרת של אתר המכללה בעזרת open visual trace, בעת שימוש ב nordVPN.

מדדנו את מס' הראוטים בדרך של החבילה, ביחס למרחק הפיזי מישראל שבו נמצא שרת חק. ההשערה שלנו היא: ככל שהמרחק של שרת חק יותר גדול, החבילה תצטרך לעשות סיבוב יותר גדול ולכן יקח לה יותר זמן להגיע ליעדה, ונרגיש עיכוב במהירות האינטרנט.

תוצאות הניסוי:

תוצאות סופיות:

לא התאפשרה שליחה עם udp על גבי nordVPN:

בעת שהלקוח מחובר ל nordvpn, ניסינו שוב ושוב אך כל ניסיון שליחה של החבילות לשרת נכשל, והחבילות לא הגיעו.

ללא חיבור ל חק השרת קיבל את החבילות שנשלחו בעזרת udp.

באופן מפתיע, כשעבדנו עם tunnelbear החבילות כן נשלחו.

על כן הוצאנו את הניסוי על udp מהפרויקט.

פתיחת שרת על מחשב המשתמש ב חק:

לאחר ניסיונות רבים, הסקנו שאנחנו לא יכולים לפתוח שרת ממחשב של אחד מאיתנו המחובר ל חק.

השאלה הנשאלת היא למה? האם הגיוני שלא ניתן לאבטח את תקשורת השרת?

לאחר דיון ומחשבה, הבנו שלא מדובר בעניין האבטחה.

מאחר וכתובת ה־ip של השרת מוסווית על ידי כתובת של שרת אחר, לא ניתן לשלוח פשוט לכתובת ה־ip של מחשב השרת מסרים.

לאחר בדיקה מעמיקה, מצאנו שקיימת דרך מיוחדת להקמת שרת במחשב המשתמש ב חק.

רשת תקשורת כזו נקראת P2P, והיא עובדת כך:

כל אחד מהקצוות מתפקד הן כלקוח והן כשרת, וכל אחד מהקצוות מסוגל ליזום או לסיים התקשרות וכן לספק או לדרוש שירותים.

NordVPN מספקת שרתי P2P מיוחדים – מאות שרתים הנמצאים במיקומים שונים ברחבי העולם ומותאמים לשיתוף קבצים.

לא ניתן להשוות את אורך המסרים:

עקב ההצפנה לא רואים מהי החבילה המקורית.

חיבור לרשת בעזרת חק עם שרת הנמצא בישראל:

באופן מפתיע מאוד, מצאנו כי חיבור בעזרת חק העובד עם שרת בישראל, הינו יותר מהיר מאשר חיבור ללא חק!

על מנת להגיע לתוצאה סופית, ניסינו לחשב סטטיסטיקה:

שלחנו 10 פעמים ping לאתר של עזריאלי, עם חק בישראל ובלי חק.

קיבלנו: ממוצע במהירות בבדיקות בלי חק הוא 88, עם פיזור של 12-13~.

ממוצע המהירות בבדיקות עם חק הוא 75.1, עם פיזור של 6~.

וכך ניתן לראות חד משמעית, כי בניגוד להגיון, חיבור עם חק שעובד עם שרת בישראל אכן יותר מהיר מאשר ללא חק!

השאלה הנשאלת היא: איך?

מסקנות:

אכן, ישנו מחיר לאבטחה כל כך מורכבת. אבטחה בשכבת הרשת מגדילה את נפח המסר,

משתמשת באלגוריתמי הצפנה וגם מנתבת את המסרים דרך שרת נוסף. ועל כן, מורגשת

האטה בתעבורה בעת שימוש במנהרה מאובטחת.

בעבר ההשפעה על האיטיות הייתה משמעותית, ולכן היה צריך לבחור בין מהירות לאבטחה.

אך כיום, ראינו שמתפתחים פרוטוקולים חדשים ומהירים עם טכנולוגיות חדשות (למשל -

wireguard) המאיצים את תהליך ההצפנה ובכך גורמים להבדלים להיות מינורים.

ספרות:

Virtual Private Network, Charlie Scott, Paul Wolfe, Mike Erwin-

https://books.google.co.il/books?hl=en&lr=&id=OuFQ3t7eF4IC&oi=fnd&pg=PP11&dq=virtual+private+network&ots=hqjPyzGM5y&sig=FAcAFLKfRVDoyx20RO9RKBzuhg&redir_esc=y#v=onepage&q=virtual%20private%20network&f=false

Formal Verification of the WireGuard Protocol, Kevin Milner, Jason A. Donenfeld -

<https://www.wireguard.com/papers/wireguard-formal-verification.pdf>

MEASUREMENT OF VPN PERFORMANCE BETWEEN DIFFERENT DEVICES, Guo Chao-

<https://www.theseus.fi/bitstream/handle/10024/59833/thesis.pdf;jsessionid=20DA9FE53C88E98A5506D52FEED87756?sequence=1>

נספחים:

נספח 1.1 - המחשת אופן הסתרת הרישא המקורית של פרוטוקול ה קו מאחורי רישא נוספת.

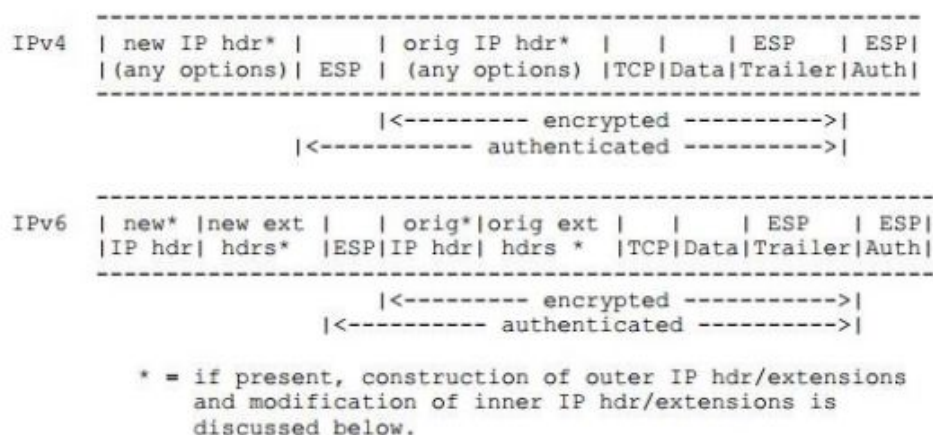
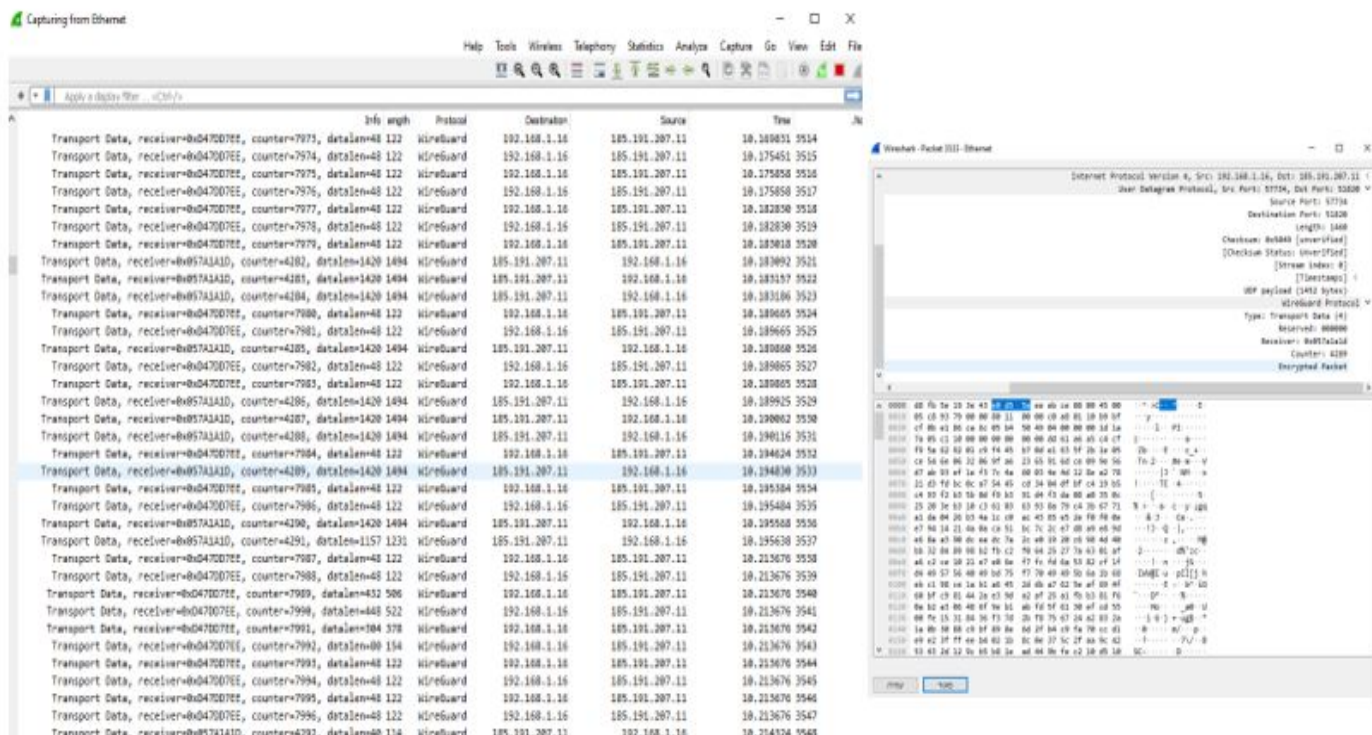
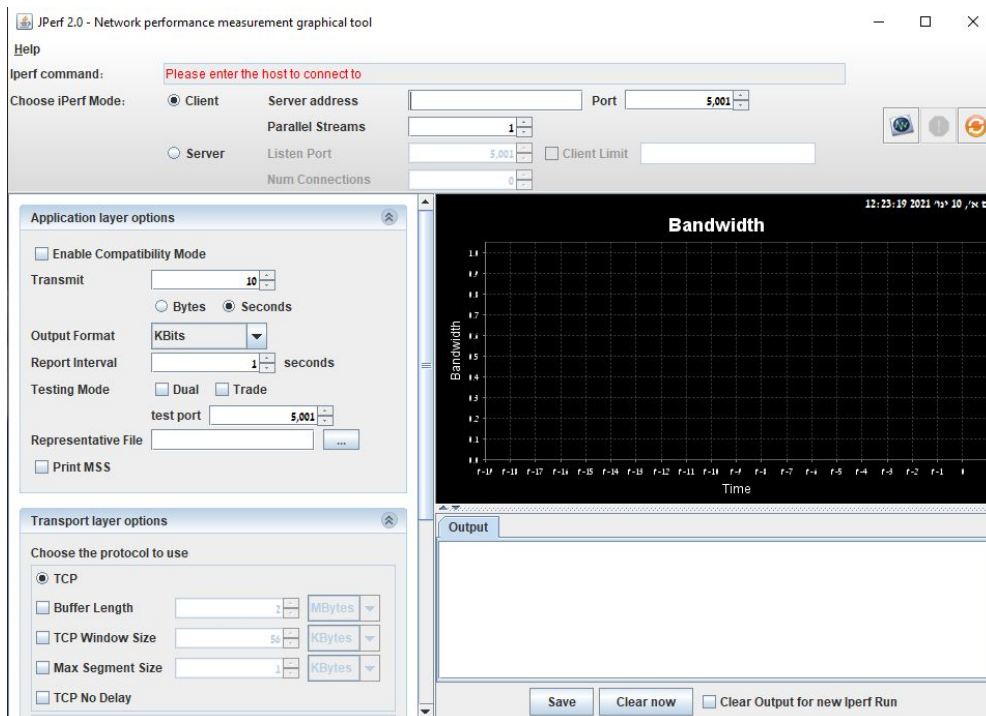


FIGURE 3.8 Tunnel mode (ESP) (RFC 2406)

נספח 2.1 - תוצאות wireshark



נספח 3.1 - הגדרות iPerf דיפולטיות



נספח 3.2 - תוצאות ניסוי דומה המוצג במאמר:

מדובר בניסוי מ-2013 שבדק את התקשורת עם חק + tcp ב-jperf.
 רואים בבירור שבעבר החק האט בצורה הרבה יותר משמעותית את קצב התעבורה.

ללא חק:

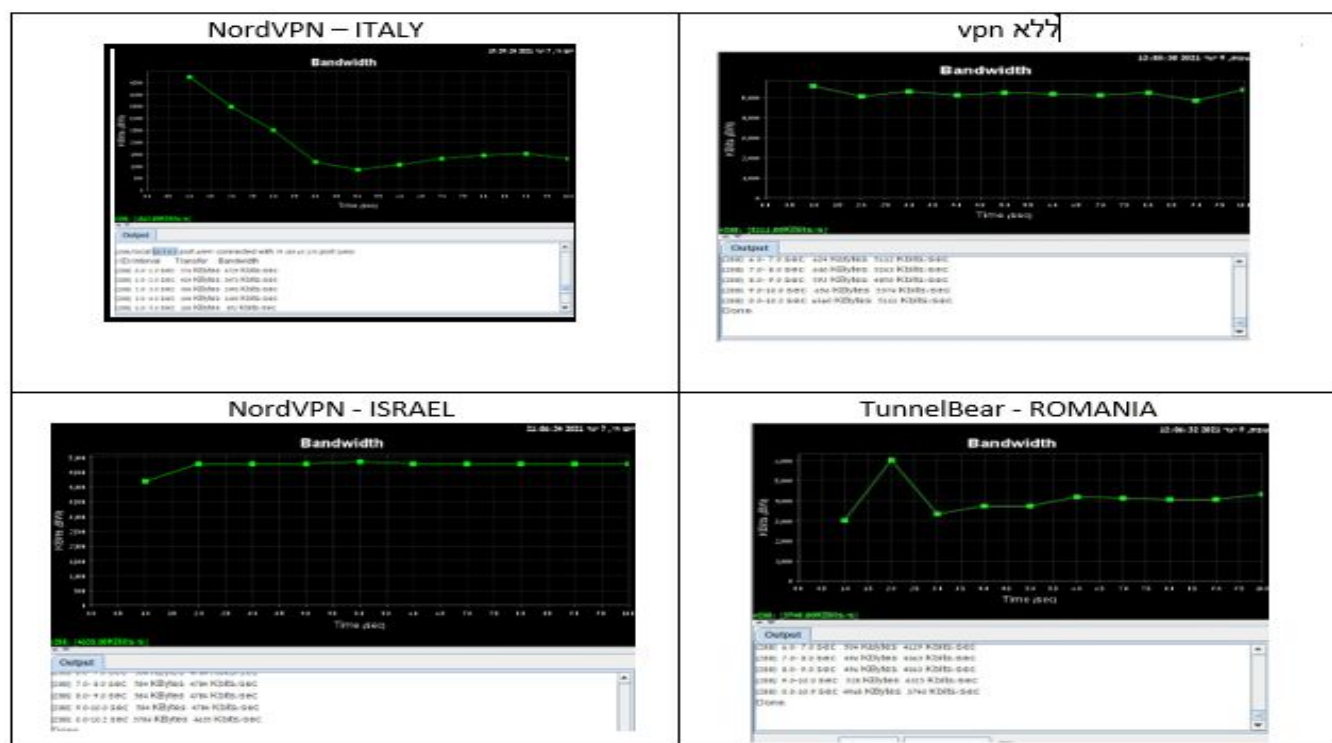
TCP window size Max segment size	1 Kbyte	2 Kbytes	4 Kbytes	8 Kbytes	16 Kbytes	32 Kbytes	64 Kbytes
1 Kbyte	83887 Kbits/sec	83895 Kbits/sec	83893 Kbits/sec	83895 Kbits/sec	68791 Kbits/sec	83887 Kbits/sec	83894 Kbits/sec
2 Kbytes	83890 Kbits/sec	83889 Kbits/sec	83894 Kbits/sec	83889 Kbits/sec	68791 Kbits/sec	83889 Kbits/sec	83889 Kbits/sec
4 Kbytes	83890 Kbits/sec	83887 Kbits/sec	83893 Kbits/sec	83887 Kbits/sec	68791 Kbits/sec	83890 Kbits/sec	83887 Kbits/sec
8 Kbytes	83893 Kbits/sec	83894 Kbits/sec	83890 Kbits/sec	83894 Kbits/sec	68789 Kbits/sec	83895 Kbits/sec	83893 Kbits/sec
16 Kbytes	83896 Kbits/sec	83895 Kbits/sec	83887 Kbits/sec	83895 Kbits/sec	67111 Kbits/sec	83892 Kbits/sec	83887 Kbits/sec
32 Kbytes	83890 Kbits/sec	83890 Kbits/sec	83890 Kbits/sec	83889 Kbits/sec	67112 Kbits/sec	83890 Kbits/sec	83889 Kbits/sec
64 Kbytes	83892 Kbits/sec	83895 Kbits/sec	83888 Kbits/sec	83892 Kbits/sec	67113 Kbits/sec	83893 Kbits/sec	83893 Kbits/sec

עם חק:

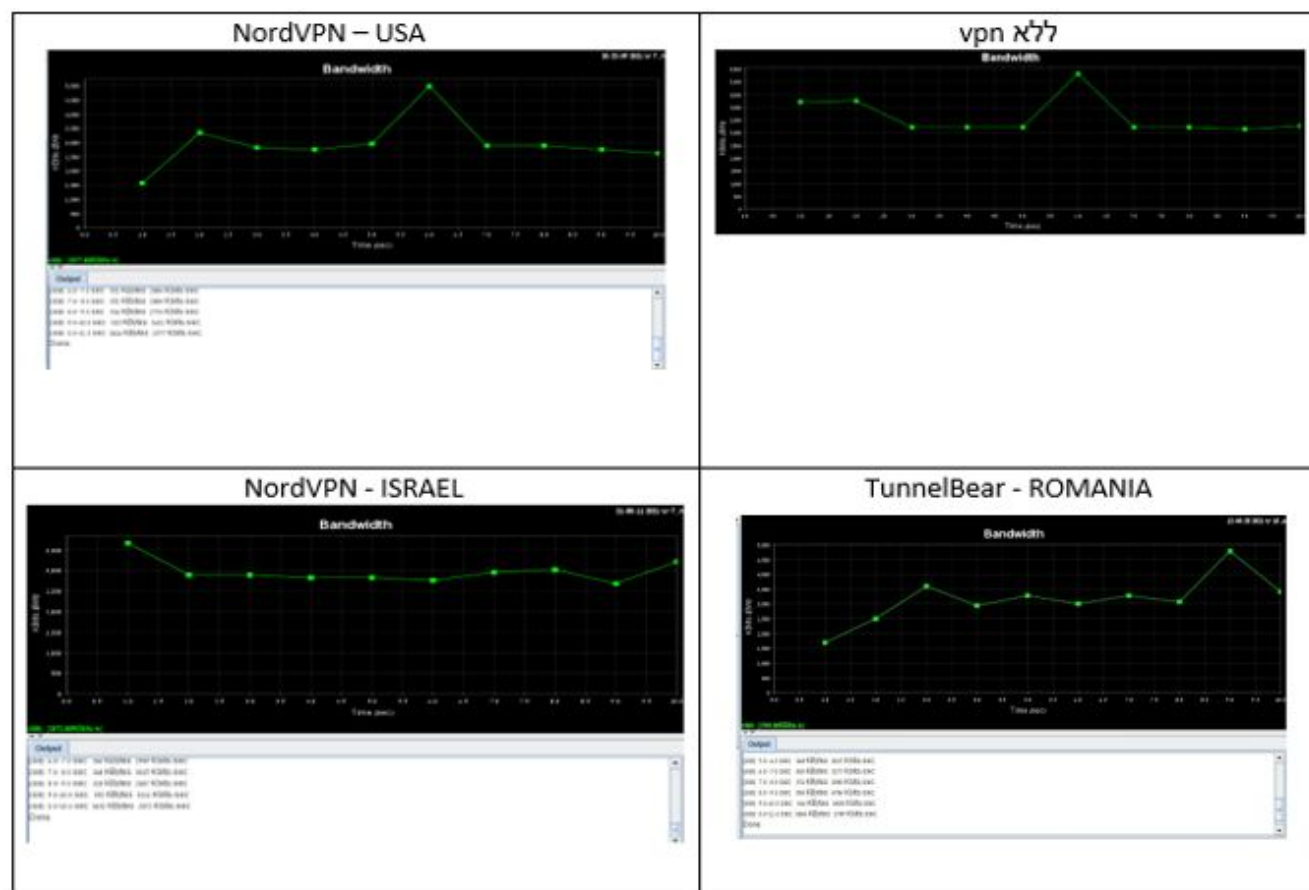
TABLE 5.3 TCP outcome

TCP window size Max segment size	1 Kbyte	2 Kbytes	4 Kbytes	8 Kbytes	16 Kbytes	32 Kbytes	64 Kbytes
1 Kbyte	38592 Kbits/sec	35237 Kbits/sec	31881 Kbits/sec	28528 Kbits/sec	53688 Kbits/sec	33556 Kbits/sec	30204 Kbits/sec
2 Kbytes	28802 Kbits/sec	31598 Kbits/sec	31598 Kbits/sec	30199 Kbits/sec	53408 Kbits/sec	28523 Kbits/sec	32163 Kbits/sec
4 Kbytes	33835 Kbits/sec	34393 Kbits/sec	28801 Kbits/sec	31580 Kbits/sec	53967 Kbits/sec	30759 Kbits/sec	30759 Kbits/sec
8 Kbytes	31319 Kbits/sec	30200 Kbits/sec	31039 Kbits/sec	29082 Kbits/sec	53408 Kbits/sec	28802 Kbits/sec	32436 Kbits/sec
16 Kbytes	31319 Kbits/sec	31039 Kbits/sec	31597 Kbits/sec	31878 Kbits/sec	53688 Kbits/sec	31598 Kbits/sec	33275 Kbits/sec
32 Kbytes	28803 Kbits/sec	31318 Kbits/sec	30759 Kbits/sec	30201 Kbits/sec	53967 Kbits/sec	32157 Kbits/sec	34954 Kbits/sec
64 Kbytes	33556 Kbits/sec	29081 Kbits/sec	31597 Kbits/sec	29640 Kbits/sec	53687 Kbits/sec	31877 Kbits/sec	32716 Kbits/sec

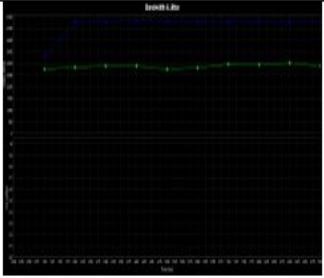
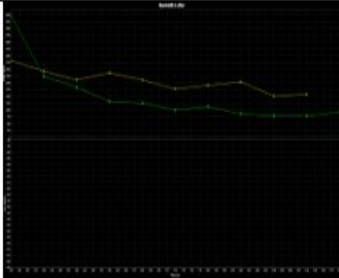

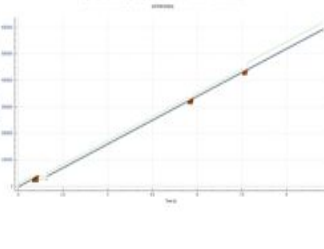
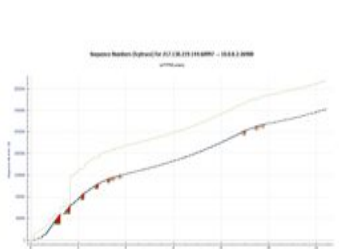
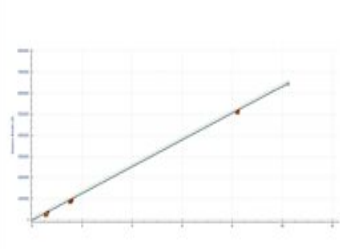
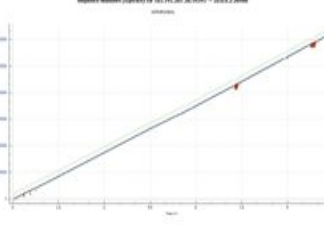
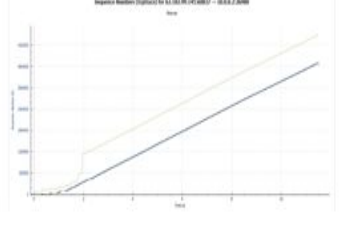
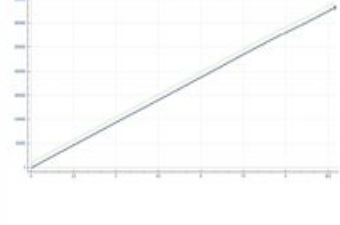
נספח 3.3 - תוצאות ניסוי 3 - אילת



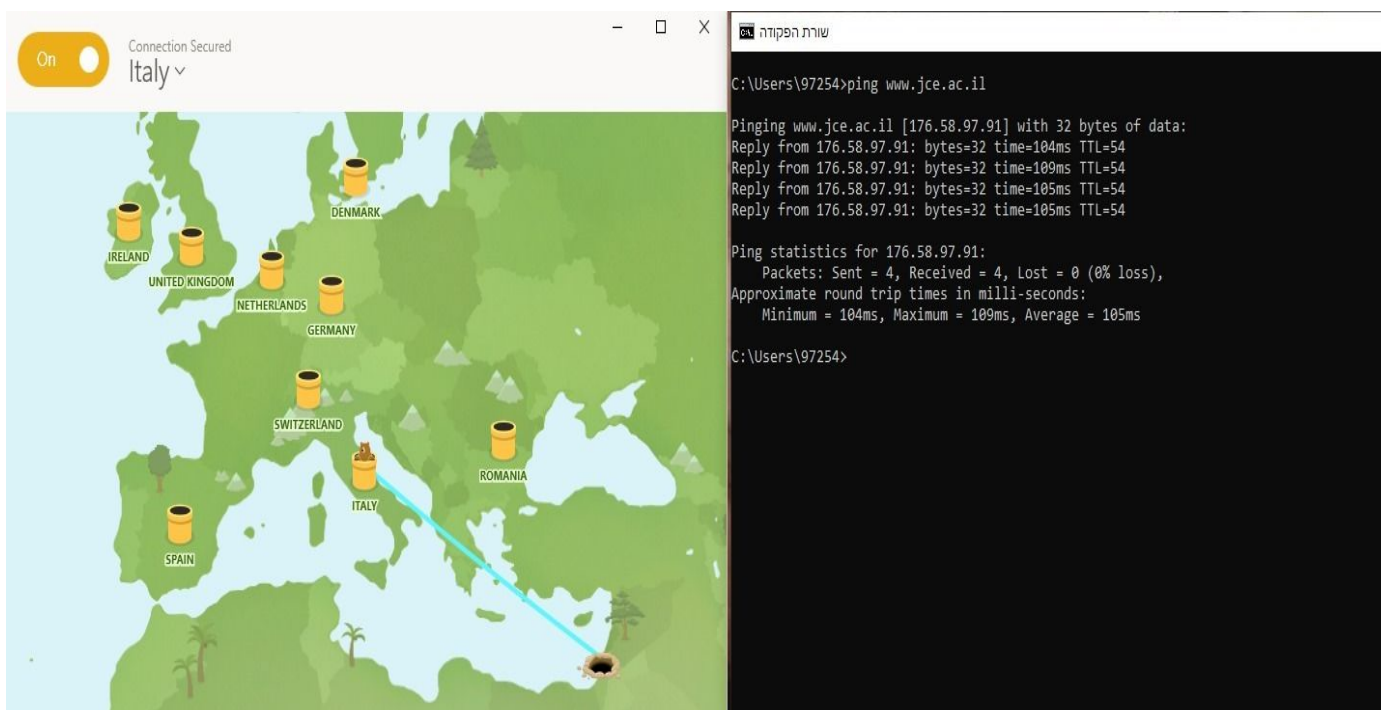
נספח 3.4 - תוצאות ניסוי 3 - עדי



נספח 3.5 - תוצאות ניסוי 3 - אלי

VPN - Israel	VPN- outside Israel	No VPN	
			הגרף שהוצג בצד השרת:
	ירוק = איטליה, צהוב = ארצות הברית		לקוח 1 (אילת)
			לקוח 2 (עדי)
			

נספח 4.1 - דוגמה לתוצאה מניסוי 4 בעזרת tunnelbear



נספח 4.2 - הבדלי מהירות האינטרנט במדינות השונות (חלקי)

את הרשימה המלאה ניתן למצוא כאן -

https://en.wikipedia.org/wiki/List_of_countries_by_Internet_connection_speeds

Rank ♦	Country/Territory ♦	Average connection speed (Mbit/s) ♦
1	Taiwan	85.02
2	Singapore	70.86
3	Jersey	67.46
4	Sweden	55.18
5	Denmark	49.19
6	Japan	42.77
7	Luxembourg	41.69
8	Netherlands	40.21
9	Switzerland	38.85
10	San Marino	38.73
11	Norway	38.46
12	Andorra	38.31
13	Spain	36.06
14	Belgium	35.69
15	United States	32.89
16	Latvia	32.74
17	New Zealand	32.72
18	Estonia	31.55
19	Hong Kong	31.37
20	Hungary	31.10
21	Lithuania	30.66
22	France	30.44
23	Slovakia	29.45
24	Finland	29.34
25	Canada	28.76
26	Slovenia	27.83
27	Germany	24.64
28	Poland	24.38
29	Ireland	23.87
30	Malaysia	23.86
31	Czech Republic	23.27
32	Portugal	22.75
33	Madagascar	22.57
34	United Kingdom	22.37
35	Iceland	22.13