

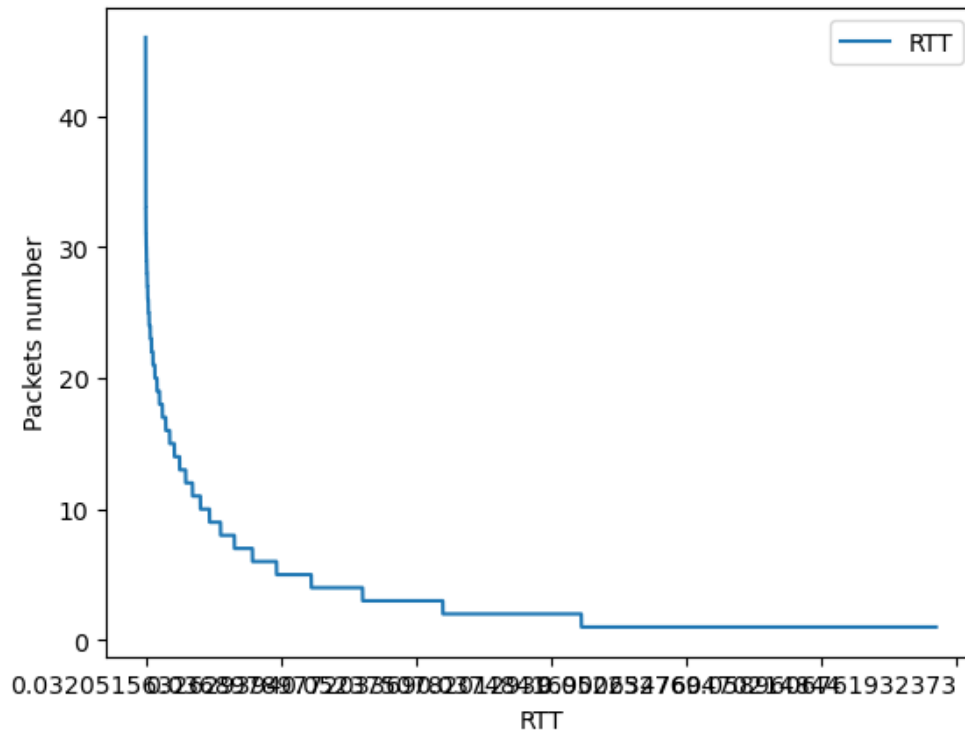
## מטלה 2 – מעבדת התקפה:

במטלה הנ"ל בנינו מתקפת DDOS בשתי שפות תכנות שונות C וpython, על מנת להשוות את המהירות של התוכניות מדדנו גם את מהירות שליחת הפאקטות בכל אחת מהתוכניות, וגם שלחנו ממחשב נפרד בקשות ping אל המחשב המותקף ומדדנו את מהירות הבקשה על ידי השרת המותקף.

\*\*\* עשינו את הגרפים על פי הבקשה שהייתה בעבודה וכאשר יצרנו אותם על פי ציר ה Y וה X המבוקשים הגרפים לעיתים נראו מוזר. כאשר הפכנו את הצירים הגרפים נראו לנו יותר הגיוניים. ולכן הוספנו גם אותם קובץ ה PDF.

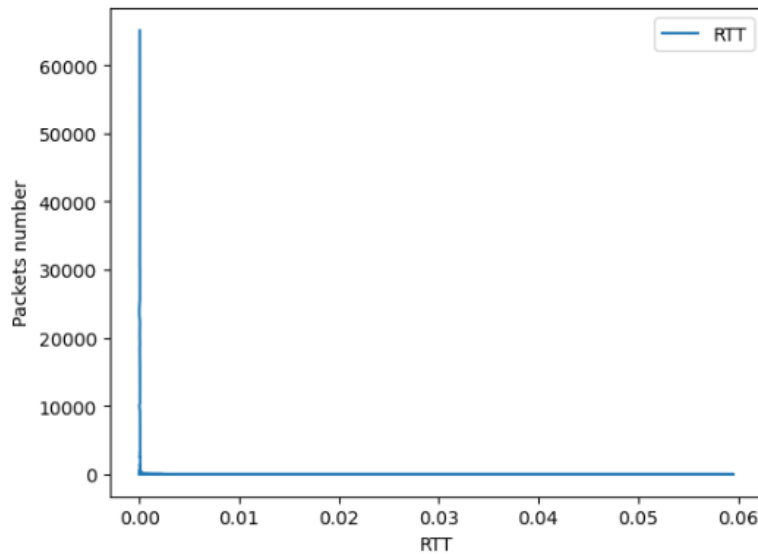
ממצאי המעבדה:

### Syn packet p



RTT ממוצע לפאקטה – 0.046585630378723146 שניות.  
זמן שליחה כולל – 46619.4866502285 שניות. (בערך 12 שעות)  
STD - 0.026509590870472034 שניות  
התמונה לעיל מציגה את מתקפת ה SYN, ניתן לראות שנשלחו יותר מ 40 פאקטות ב RTT של 0.320515,

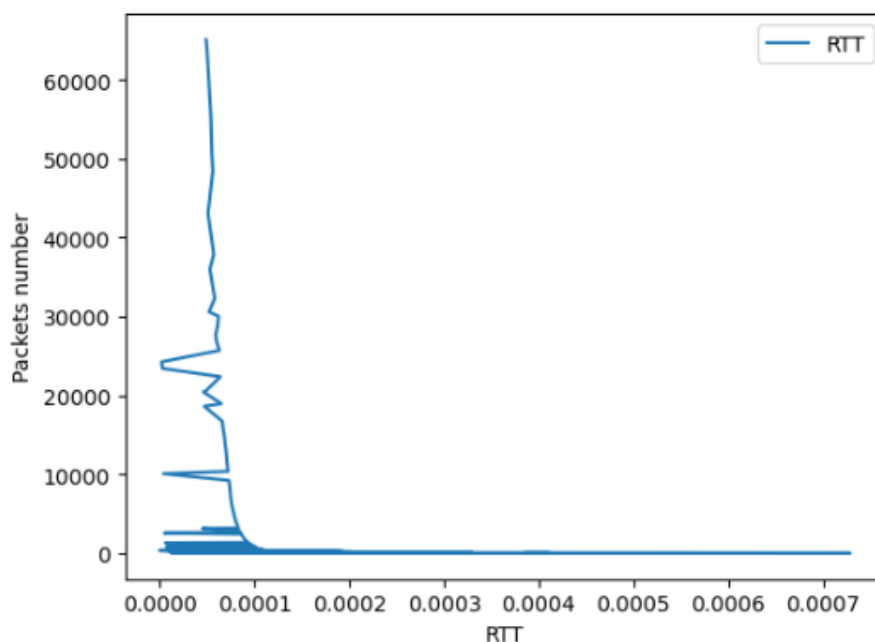
### Syn\_packet\_c



RTT ממוצע לפאקטה – 0.00006264535477385 שניות  
זמן שליחה כולל - 67.566686 שניות  
STD - 0.000105 שניות

בתמונה לעיל, ניתן לראות כי הרוב המוחלט של הפאקטות שנשלחה בטווח הזמן שקטן מ-0.01 שניות, על מנת להפוך את הגרף לקריא יותר, הוספנו גרף נוסף אשר כולל בתוכו את 500 נקודות ה-RTT הראשונות מתוך כלל הנקודות (1570), כך שהורדנו את הנקודות הזניחות, שבהם יש רק פאקטה אחת שנשלחה ב-RTT מסוים.

### *RTT 500/1570*

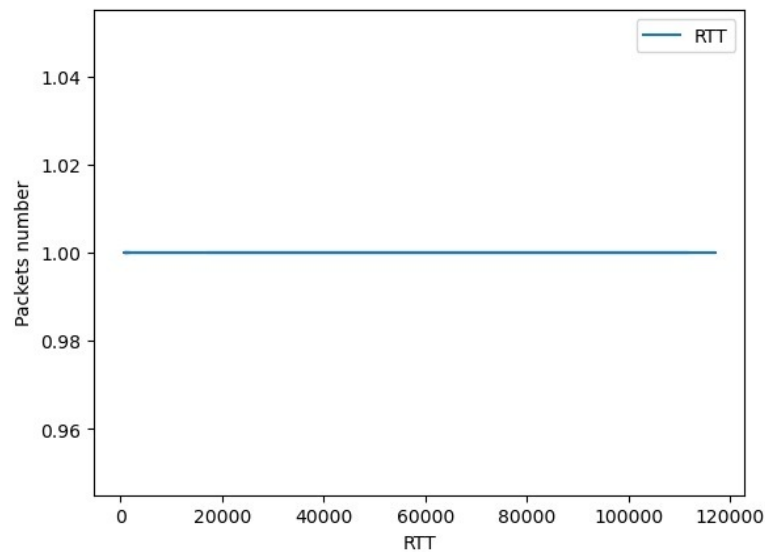


ניתן לראות שכאשר לקחנו רק 500 נקודות מתוך סך הנקודות והורדנו את הנקודות הזניחות, שרמת הדיק של ה-RTT הגיע לעשרת אלפית השנייה.

### סיכום syn:

ניתן לראות שכאשר המתקפה ממומשת בשפת C, ממוצע ה-RTT של הפאקטות קטן פי 743 מממוצע ה-RTT של התוכנית בpython. כלומר כל פאקטה שנשלחה בשפת C נשלחה פי 743 יותר מהר מאשר פאקטות שנשלחו בpython, המהירות של השליחה משפיעה על מתקפת ה-DDoS והופכת אותה לעוצמתית יותר. מכך אנו מסיקים שגם הפינגים של תוכנית ה-C יהיו איטיים יותר, כלומר המתקפה עובדת ויש עומס על השרת המותקף.

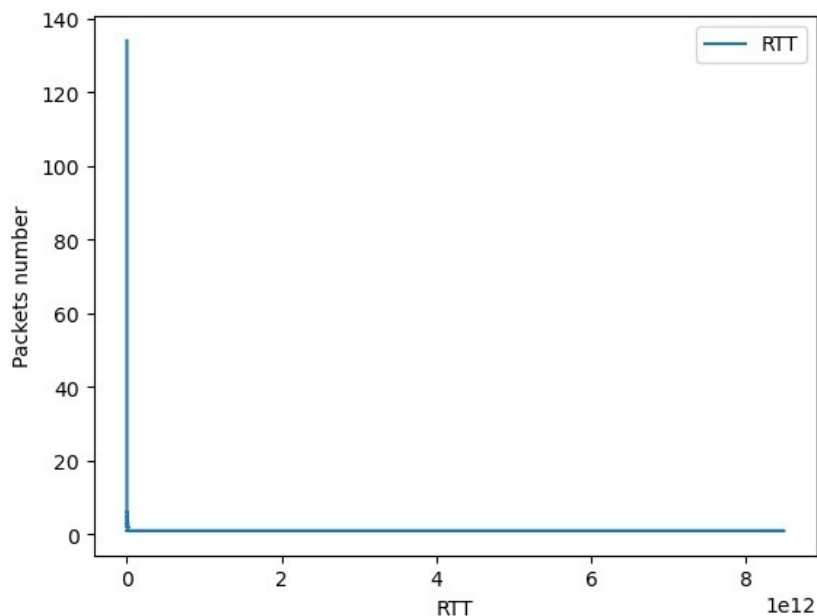
### Pings results c



RTT ממוצע לפינג – 17.338142857142856 מילי-שניות  
SDT - 39.6787196975499 מילי-שניות

כיוון שתוכנית ה-C עבדה מהר יחסית היא סיימה לרוץ בתוך קצת יותר מדקה, אנחנו שלחנו פינג ממחשב המונטור בכל 5 שניות, כך שבסופו של דבר נשלחו רק 14 פינגים שונים, שלכל אחד מהם היה RTT אחר, וזו הסיבה שהגרף שלנו הוא קו ישר.

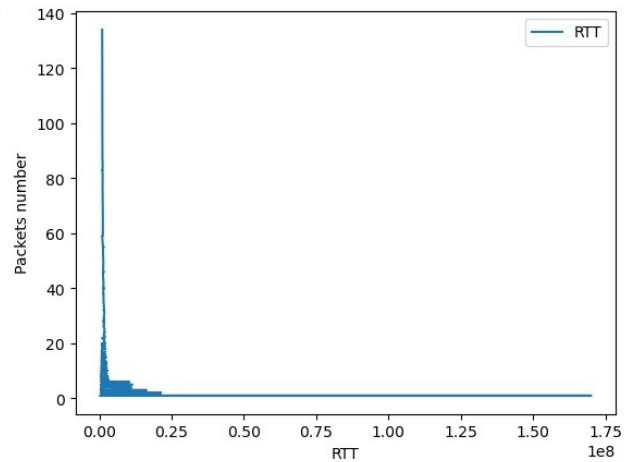
### Pings results p



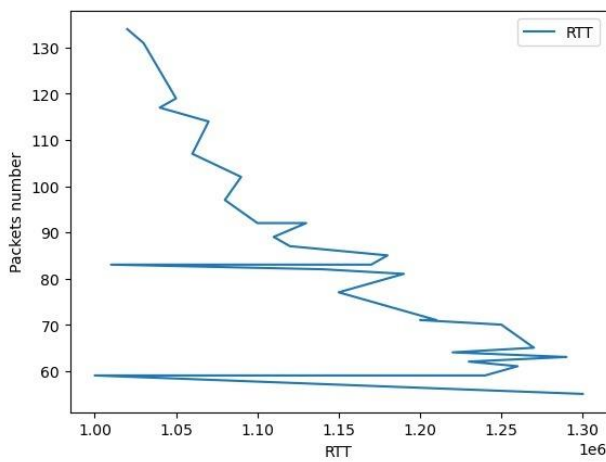
RTT ממוצע לפינג – 3.6950768733850055 מילי-שניות  
STD – 119.5658982426305 מילי-שניות

מהגרף הנ"ל ניתן לראות שרוב הפינגים ששלחנו מהמחשב המונטור חזרו בפרק זמן קצר מאוד, כלומר מתקפת ה-DDOS שהפעלנו לא פעלה באופן עוצמתי מספיק. על מנת לראות את הגרף בצורה מיטבית, העלנו עוד שני גרפים אשר מורידים תוצאות זניחות (תוצאות של RTT שבהם היו לא הרבה פאקטות).

גרף א' – 900/1020 פינגים



גרף ב' – 30/1020 פינגים



משני הגרפים הנ"ל ניתן לראות שרוב הפינגים חזרו בפרק זמן שקצר מ  $0.000025$  מילי-שניות כלומר בערך זמן נורמטיבי של פינג, המתקפה בקושי מורגשת.

#### סיכום ping –

בנוסף, ניתן לראות שכאשר המתקפה בוצעה ב  $C$  זמן ה  $RTT$  של שליחת פינג הגיעה  $ms117$  בשיא, בניגוד לפייתון שלא נראה חריגות כמעט בכלל למרות אורך המתקפה. ה  $RTT$  הממוצע לפינג בתוכנית  $C$  היה גדול פי  $5.5$  מה  $RTT$  הממוצע לתוכנית `python`.

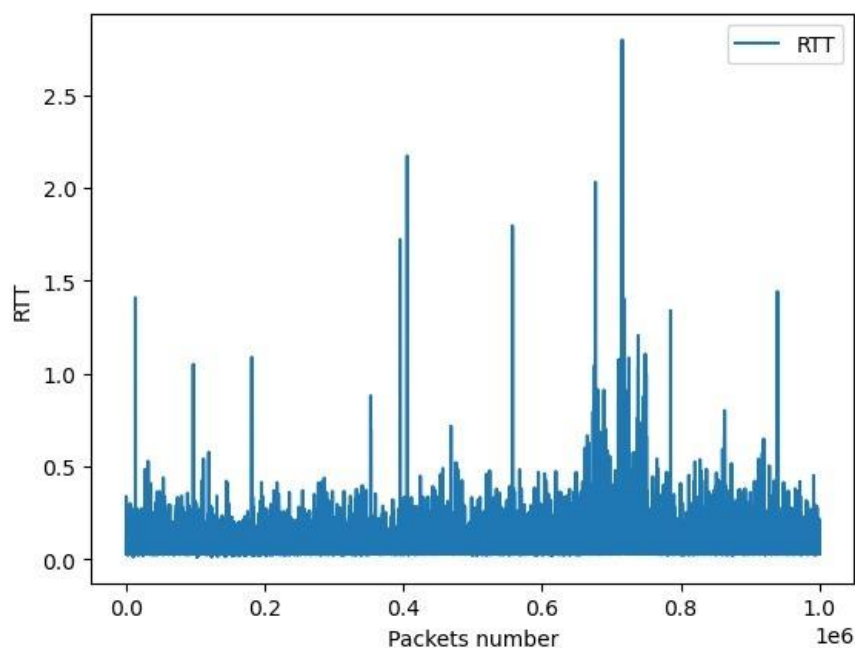
#### סיכום כללי –

מהגרפים מעלה ומהמסקנות שהסקנו ולמדנו מהם קיבלנו עוד חיזוק להנחה המקורית שהייתה לנו שאמרה שתוכנית ה  $DDOS$  בשפת  $C$  אפקטיבית יותר, הן מבחינת מהירות ההרצה שלה והן מבחינת ההשפעה שלה על המחשב המותקף.

כבר בזמן ההרצה שמנו לב להתרחשות, כאשר ההרצה של תוכנית הפייתון לקחה סביבות  $12$  שעות, בעוד שההרצה של תוכנית ה  $C$  לקחה בערך  $3$  דקות. כלומר השליחה הייתה של הפאקטות ב  $C$  הייתה מהירה יותר, ולכן הגיוני גם שהיא יוצרת עומס על השרת. ניתן לשער מהנתונים שאם היינו מריצים את התוכנה של  $C$  ליותר איטרציות (יותר ממיליון) המתקפה הייתה ארוכה יותר והייתה משפיעה ומעמיסה על השרת הרבה יותר.

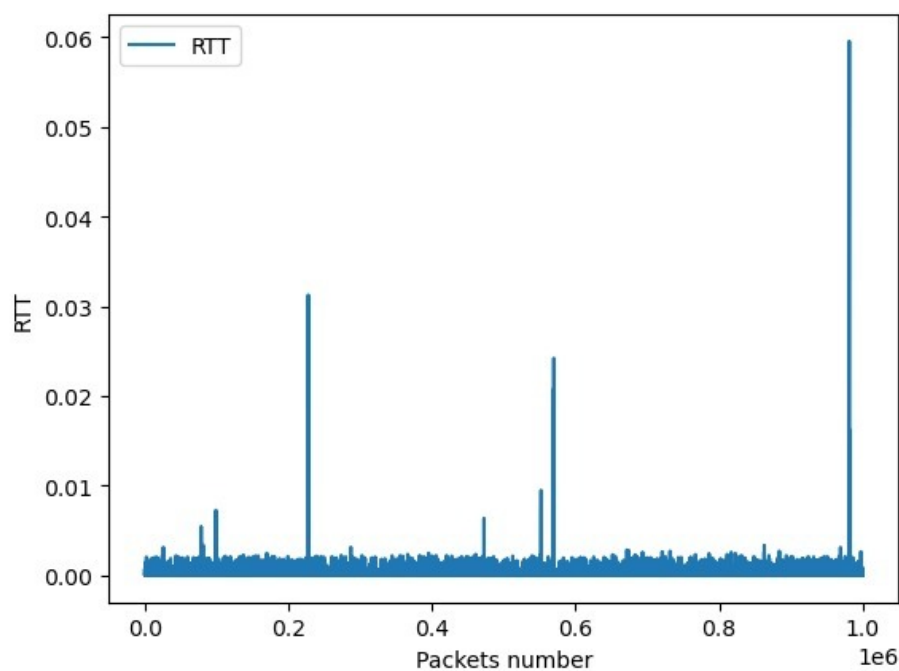
\*\*\* גרפים בהם ציר הX והY הפוכים –

Syns\_packet\_p



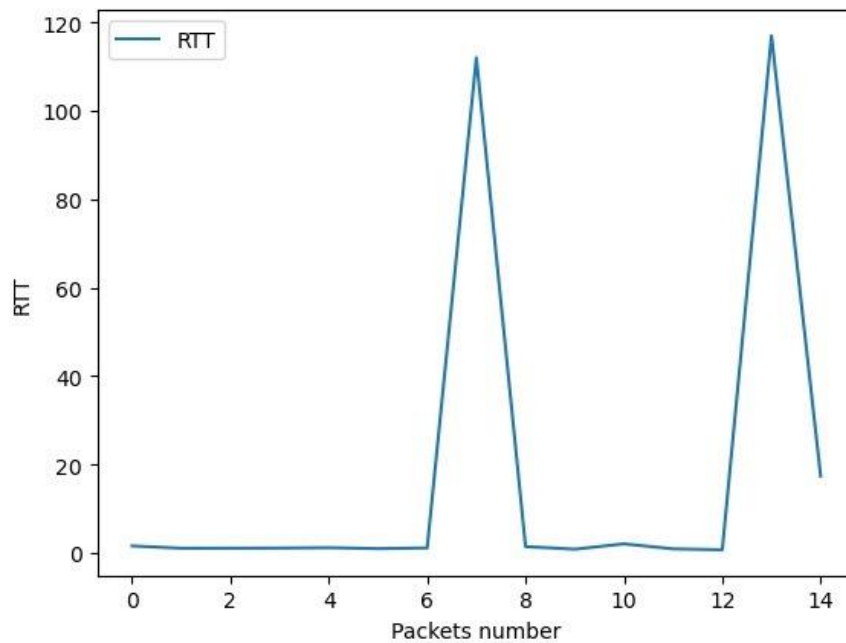
בגרף הנ"ל ניתן לראות את הRTT של כל פאקטת SYN שנשלחה לשרת המותקף.

Sync\_packet\_c



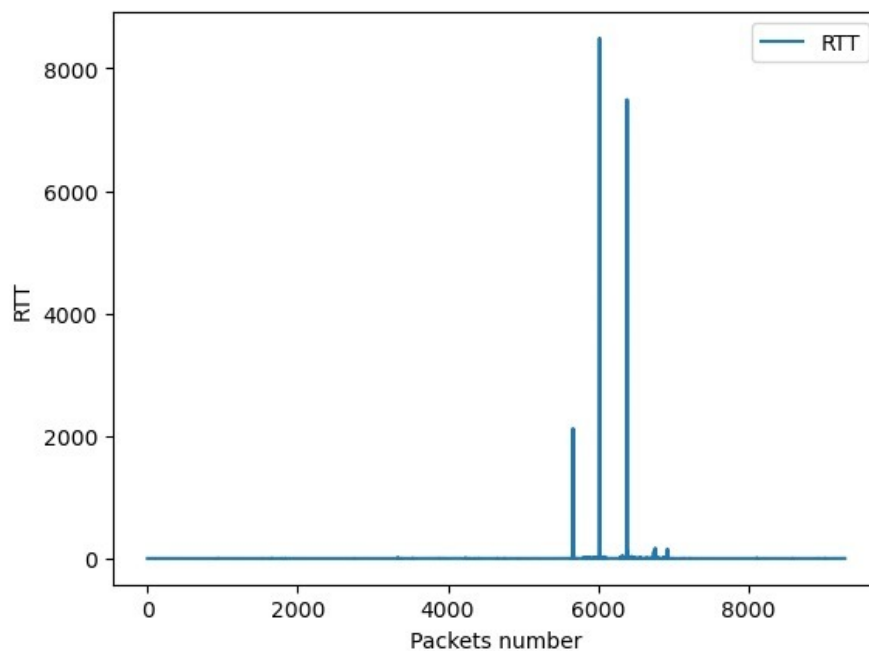
בגרף הנ"ל ניתן לראות את הRTT של כל פאקטת SYN שנשלחה לשרת המותקף. ביחס לגרף של הפייתון ניתן לראות שהחסם העליון של גרף הC הוא RTT 0.6 וכאשר משווים אותו לגרף של הפייתון רואים שהיו הרבה חבילות SYN שנשלחו בפייתון בזמן קרוב ל0.6, ובתוכנת הפייתון זה נחשב זמן סביר. כלומר שליחת הפאקטות בפייתון ארכה זמן רב יותר.

Pings\_results\_c



בגרף הנ"ל ניתן לראות את הRTT של כל פינג שנשלח לשרת המותקף. ביחס לכמות הפינגים שנשלחו (14) היו 2 פינגים שלהם RTT גבוה מאוד, דבר שהשפיע גם כל הממוצע וניתן לראות זאת בבירור מהגרף.

Pings\_result\_p



בגרף הנ"ל ניתן לראות את הRTT של כל פינג שנשלח לשרת המותקף. ביחס לגרף של תוכנת C ניתן לראות שלא היו הרבה פינגים באופן יחסי (מתוך 9288) שהחזירו תוצאה גבוהה, גם שגם הממוצע היה 3.69 ms שזה RTT נורמטיבי ל-ping. כלומר המתקפה בקושי השפיעה.