פרויקט גמר רשתות תקשורת

מגישות:

אביה אורן 322273301

נטע כהן 325195774

קישורים ללינקדאין :

אביה : www.linkedin.com/in/aviya-oren-80471926b

נטע :

https://www.linkedin.com/in/%D7%A0%D7%98%D7%A2-%D7/%9B%D7%94%D7%9F-27696327a

קישור לgithub של הפרויקט:

https://github.com/OrenAviya/Networks_FinalProject

חלק יבש:

סיכום המאמר "Practical Traffic Analysis Attacks on Secure Messaging Applications":

הרעיון המרכזי המובא במאמר הוא:
המאמר מתאר דרך למעקב והשגת מידע רגיש מתוך התכתבויות באפליקציות הודעות, במאמר מתואר חקר על יכולת הבקרה והמעקב על אנשים דרך ההודעות באפליקציות הודעות IM = instant messaging , למשל whatsapp או telegram . למרות ההצפנה שבד"כ משתמשים בה באפליקציות כגון אלו ניתן לבצע מעקב וניתוח התעבורה כך שמתאפשר זיהוי מנהל / משתתף בקבוצה מסויימת יריבה וזיהוי פעילים ומשתתפים בה.
לרוב שירותי הודעות מיידיות ראשיים אינם מטשטשים דפוסי תעבורה כי זה יקר לביצוע. ודרך דפוסים אלו אפשר לגלות על השולח כל מיני דברים.
כותבי המאמר מקווים שהתוצאות שהשיגו במחקר שלהם ובפיתוח שרת הפרוקסי שיכול להגן על מעבירי ההודעות יזהירו את ספקי הודעות מיידיות ויגרמו להם לקחת אמצעים יעילים יותר להגן על לקוחותיהם.

ראשית נתייחס לשאלה - כיצד התוקף משיג נתונים בסיסיים "ground truth" על התעבורה של הערוץ? וכיצד הוא מדייק את הנתונים שלו מול המציאות?

1. מקרה ראשון - אם התוקף יכול להצטרף לערוץ אליו הוא רוצה להאזין (איפה שנשלחות ההודעות האטרקטיביות לבדיקה מבחינתו) **ולצפות** במה שמעבירים באותו ערוץ הוא יכול להשוות את הנתונים שהוא רואה לנתונים שהוא משיג ולגלות מה הדיוק של הנתונים שהוא לוכד.
2. מקרה שני - התוקף יכול להצטרף כמנהל ואף ל**שלוח הודעות** בעצמו בקבוצה בנוסף על היותו **צופה.**
3. במקרה הגרוע- התוקף לא יכול ממש להצטרף לערוץ אבל יכול לזהות משתתפים ומנהלים דרך תקשורת אחד על אחד . כלומר אם יצליח לזהות כתובת פרטית של אחד ממשתתפי הקבוצה ולנתח את התעבורה שלו , יוכל בהנחה שהוא יודע שזהו אחד מהחברים בקבוצה, להשליך מתוך ניתוח התעבורה הפרטית שלו על המסרים שנשלחים בערוץ- בקבוצה.

כאמור לעיל הניתוח כולו מתבצע באמצעות הגודל והתזמון/תדירות של החבילות שעוברות ברשת , היות והמסרים עצמם מוצפנים.

כיצד מתבצע הניתוח בפועל?

באופן כללי - הגודל והתזמון של חבילות יכולות להדליף מידע על זהות השולח או המקבל בגלל הדמיון בין החבילות שנשלחו מהמשתמש שנבדק והתקבלו בערוץ (אם זו אותה סוג

של הודעה יש לה גודל כמעט שווה והזמנים יהיו דומים אזי ניתן להניח שזו השתתפות פעילה של האדם השולח בקבוצה הנבדקת.)

באופן יותר ספציפי- אפשר לבצע מעקב זה תוך שימוש בשני אלגוריתמים אפשריים-

1.Event-Based Algorithm

כלומר, אם שני "אירועים" / הודעות אחד בתעבורת הערוץ ואחד בתעבורה שנשלחה מאדם מסויים נשלחות מספיק "קרוב" בזמן הוא יוצר התאמה ואם יש התאמות מרובות ביחס לכמות ההודעות שנשלחו בכלל (בהשוואה לtrashhold שנקבע מראש) אזי התוקף יודע ל"סמן" את האדם כפעיל באותו ערוץ תקשורת.

2.shape-Based Algorithm

אלגוריתם זה מבוסס על "צורת" התעבורה וה"צורה" היא בעצם וקטור של אורכי מנות לאורך זמן. כלומר לפי הצורה שיוצרות החבילות - מתאפשר לו להשוות ולזהות חבילות מאותו סוג שנשלחו והגיעו לכל המשתתפים בערוץ.

איך מחושבת הצורה - הווקטור הנ"ל?

זיהוי " אירוע" - הודעה מסויימת ואז נרמול התעבורה לפי חבילות בגובה שווה. הצורה הסופית מתקבלת מהווקטור שנוצר ממעבר על גבהי האירועים לאורך זמן ההקלטה.
גם כאן - ההשוואה היא בין התעבורה של משתמש פרטי למול התעבורה הכללית בקבוצה.

נתייחס לשאלה נוספת - כיצד התוקף מאזין בסתר לתעבורת הרשת? כיצד הוא מגלה את כתובת הIP של המשתמש הפרטי שאותו הוא מעוניין לבדוק?

ישנן כמה דרכים לבצע זאת:

1. האזנת סתר לתעבורת הרשת של ספקי האינטרנט או ה-IXP שבהם התוקף שולט, למשל, אם זהו ארגון ממשלתי ששולט בחלק מהרשת. דוגמא לכך יכולה להיות חומת האש הגדולה של סין.
2. לחלופין, היריב יכול להאזין לרשת תעבורה של אנשים ספציפיים (למשל, פעילים חשודים), לאחר קבלת צו האזנת סתר.

כותבי המאמר רצו לדמות "התקפה" של יריב (למשל ממשלה) על תקשורת רגישה כלשהי (למשל פוליטית) . ולכן מידלו את התעבורה בערוצי רשת ומיינו אותה לפי חמשת סוגי ההודעות הנמצאים בשכיחות הגבוהה ביותר בתעבורה ברשת : קבצים, תמונות , סרטים, אודיו (שמע) , והודעות טקסט.

הנתונים סוכמו לטבלה 2 במאמר:

TABLE II: Distribution of various message types

Type	Count	Volume (MB)	Size range	Avg. size
Text	12539 (29.4%)	3.85 (0.016%)	1B-4095B	306.61B
Photo	20471 (48%)	1869.57 (0.765%)	2.40Kb-378.68Kb	91.33KB
Video	6564 (15.4%)	232955.19 (95.3%)	10.16Kb-1.56Gb	35.49MB
File	903 (2.1%)	47.46 (0.019%)	2.54Kb-1.88Mg	52.56KB
Audio	2161 (5.1%)	9587.36 (3.92%)	2.83Kb-98.07Mg	4.44MB

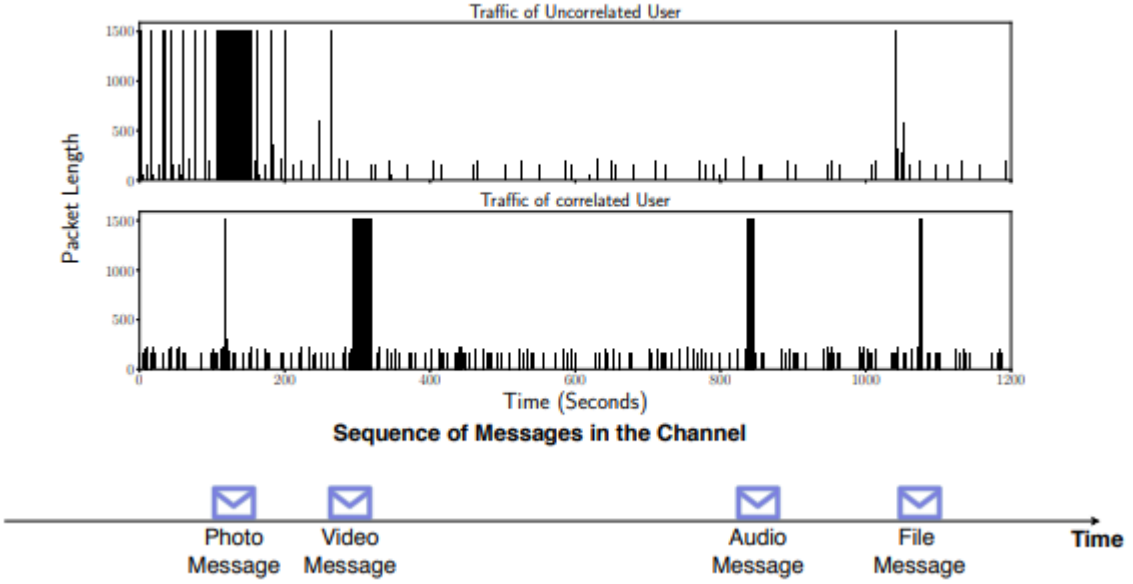
בטבלה נבחנו ההודעות לפי 4 פרמטרים :

1. כמות ההודעות מהסוג הזה.
2. שטח האחסון שסוג זה תפס בזיכרון
3. טווח הגדלים שהודעות מסוג זה יכולות לקבל
4. גודל ממוצע

סיכום הטבלה :

- הודעות טקסט ותמונות תופסים אחוז נכבד מסך כל התעבורה. (תמונות עם 48% והודעות טקסט עם 29.4%) ואחריהם מגיעים וידאו (15.4%), שמע (5.1%) וקבצים(2.1%)
- נפח האחסון נתפס רובו (95%) ע"י סרטונים וסרטים (וידאו) .
- טווח הגדלים של תמונות והודעות טקסט קטן יחסית לטווח הגדלים של שמע וקבצים וכל אלו קטנים מאוד לעומת טווח הגדלים שוידאו יכול לקבל הנע בין 10KB ו1.56GB!
- גודלם הממוצע מהקטן לגדול של מסרים מכל סוג הוא : הודעת טקסט: 306.61B , קובץ : 52.56KB , תמונה:91.33KB , שמע : 4.44MB , וידאו: 35.49MB

לאחר מידול זה של התעבורה הכללית ברשת, כותבי המאמר חקרו את היכולת לחלץ מידע על משתתפים בערוץ תקשורת מסוים.



איור 8 במאמר , מדגים איך ניתן לזהות קורלציה בין תעבורה של משתמש שלא שייך לקבוצה מסויימת (הגרף העליון) לבין תעבורה של משתמש ששייך לקבוצה מסויימת (הגרף התחתון) ע"י השוואה של התעבורה שלהם לתעבורת הערוץ.

איך זה מתבצע?

עבור תעבורה בערוץ מסוים ניתן לראות את המרחקים בין החבילות שנשלחו וכן את גודל החבילות וכך לזהות אילו חבילות שייכות לאותה ההודעה/ "אירוע". זהו שלב זיהוי "אירוע מסויים" - רצף פאקטות שמייצגות מסר אחד שנשלח בקבוצה.

התוקף יכול לחלץ מהתקשורת המוצפנת צרורות של פאקטות אלו , לבדוק האם הן נשלחו באותו "פרק זמן" (טראשהולד שנקבע מראש) ולקבוע שזהו "אירוע" אחד, כלומר שהתעבורה הזו שייכת להודעה אחת.
לאחר מכן יוכל להשוות אירועים אלו לאירועים מקבילים שהתרחשו באותו זמן בתעבורה שנלכדה אצל משתמש ספציפי ולקבוע האם הוא ממשתתף בערוץ או לא.

הדרך בה מנסים כותבי המאמר להתמודד עם מעקב שכזה היא יצירת שרת פרוקסי דרכו מועברות חבילות התעבורה שנשלחות מהמנהל ומתקבלות אצל המשתתפים. מה שהפרוקסי עושה זה "מחיקת" הדפוס שיצר השרת המקומי של השולח ושינוי ה"זמנים" או הוספת פקטות מדומות כך שלא יוכלו העוקבים לקשר בין החבילות שנשלחו לכדי "אירוע אחד".

הם גם מוכיחים שבאמצעות אלגוריתם זה הם מצליחים להפחית את יכוולת המעקב של "תוקף" ביותר מ20%

חלק רטוב- ניתוח תעבורה בקבוצות :

<u>נדרש לבצע :</u>

1. להראות הבדלים בקבוצות שונות שנשלחים בהם בד"כ סוגי הודעות שונים (גדולים יותר ופחות למשל)
(אפשר להניח שיש לנו מרגל בקבוצה שיודע אילו קבצים הועברו ומתי)

הקדמה למחקר:

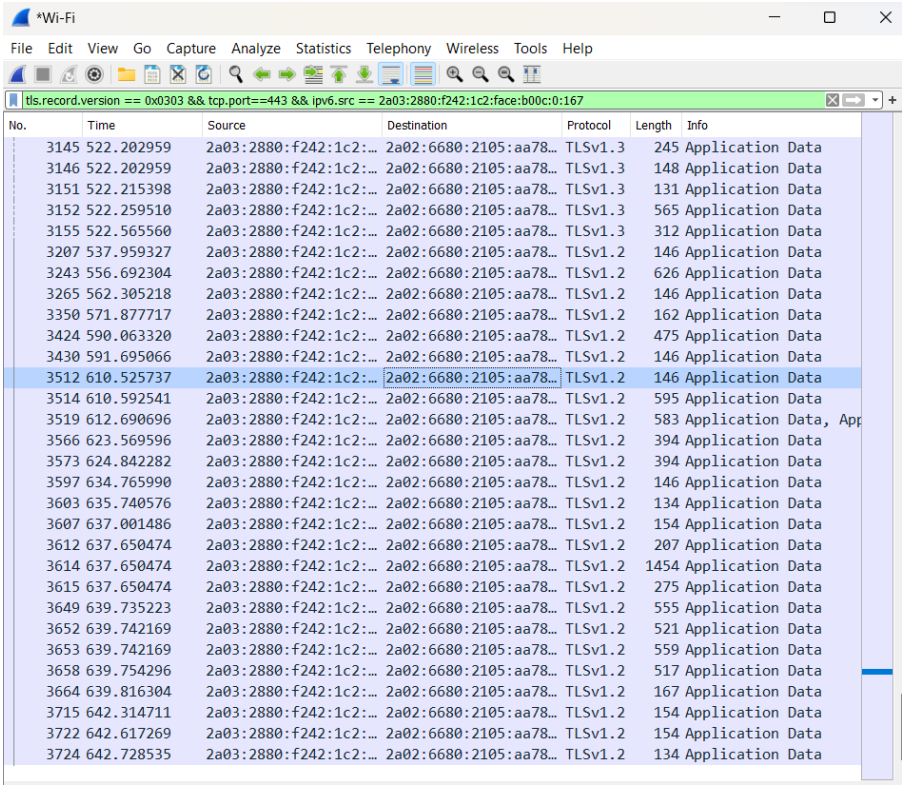
בחרנו להאזין לקבוצות בווצאפ. (מתוך הנחה שאנחנו נמצאות בקבוצות).

ע"מ לדעת איזה סינון ידרש ממנו כדי לזהות את הפאקטות הנכונות חיפשנו מה כתובת הipv6 של שרת whatsappweb:

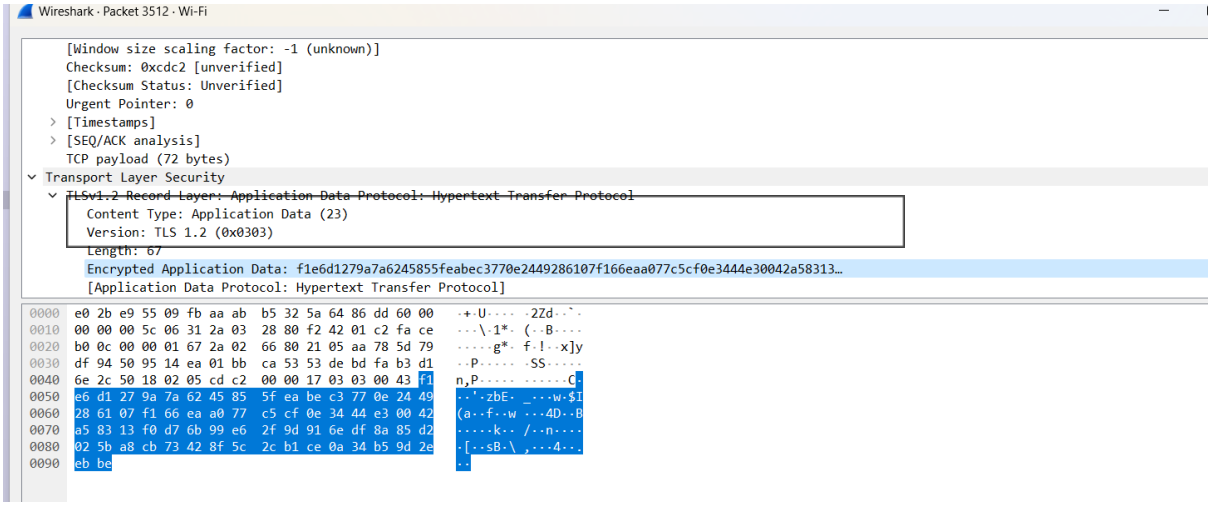
```
C:\Users\97258>nslookup web.whatsapp.com
Server:  UnKnown
Address:  fe80::a8ab:b5ff:fe32:5a64

Non-authoritative answer:
Name:    mmx-ds.cdn.whatsapp.net
Addresses:  2a03:2880:f242:c8:face:b00c:0:167
          157.240.195.56
Aliases:  web.whatsapp.com
```

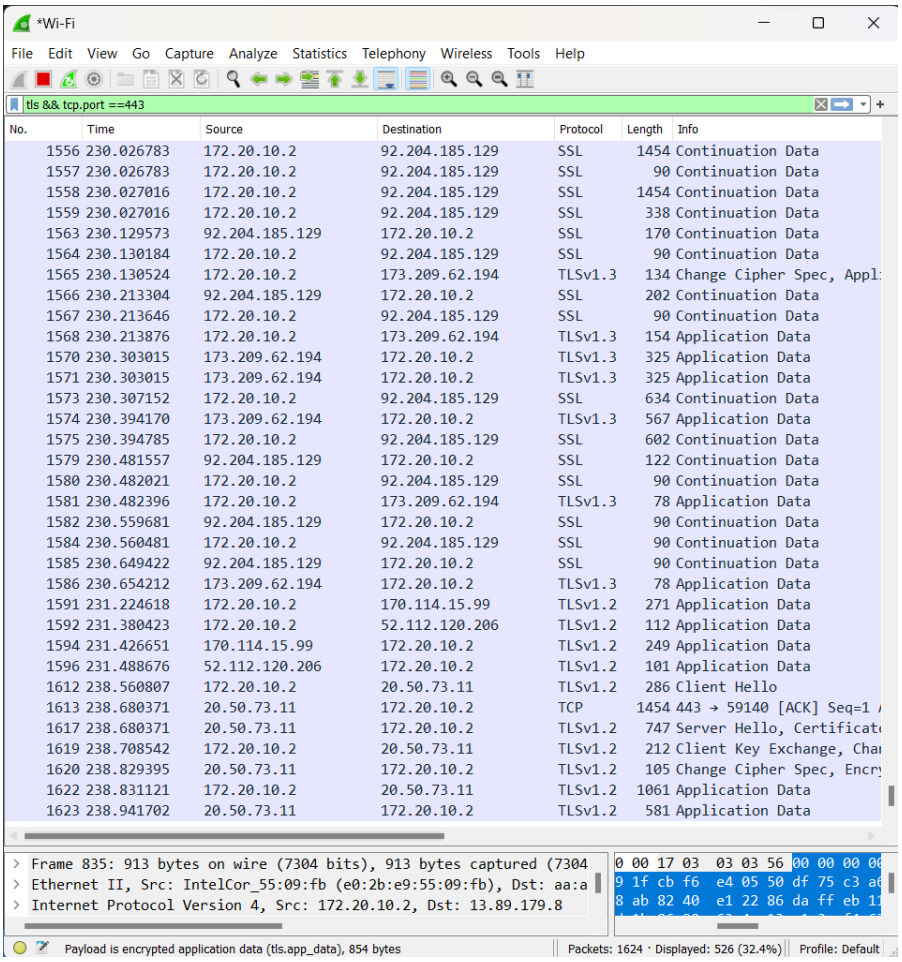
את הכתובת הזו אנחנו רואות בכל פעם שמופיעה הודעה מווצאפ: בתמונה ניתן לראות את הסינון שבחרנו כדי לתמצת כמה שיותר את התעבורה לכדי הודעות בלבד (ועדיין ישנם רעשים , בהמשך נתמודד איתם).
אנחנו בוחנות רק הודעות המתקבלות בווצאפ.
ניתן לראות שהשרת זהה עבור כל ההודעות על אף שהן מתקבלות **מקבוצות שונות.**



דבר נוסף וחשוב להבין - הודעות ווצאפ מוצפנות כמו בדוגמא:



ע"מ להגיע לסינון הזה , הקלטנו הקלטה של פעילות המחשב כאשר האפליקציה ווצאפ **סגורה,** וסיננו את התעבורה לפי מסנן tls והפורט הנכון וכך הגענו למסקנה שהתעבורה משרתים בצורת ipv4 שאנו רואות אינה קשורה לווצאפ וכן שרתים נוספים שאינן השרת של ווצאפ ניתן לראות בדוגמא את צילום המסך ווירשארק במקרה כזה:



נסיון ראשוני:

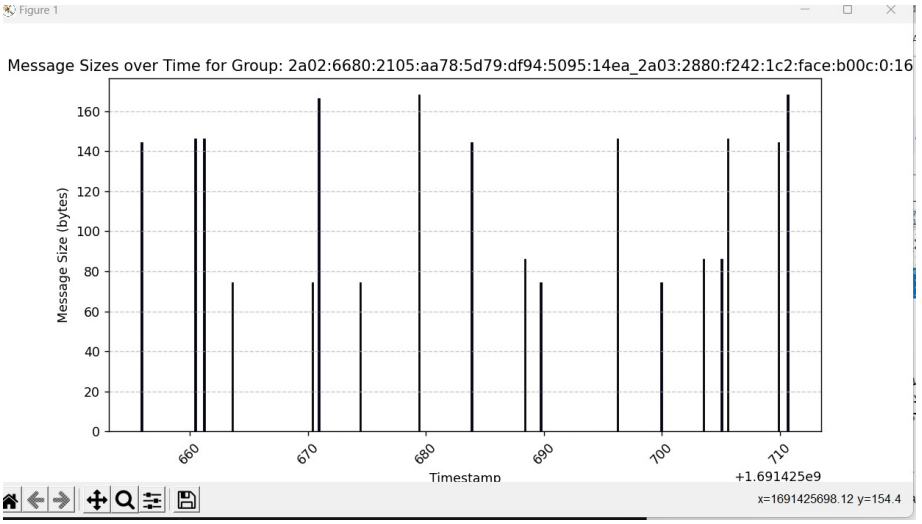
נשאלת השאלה- איך נדע להבחין ולהסיק מסקנות מהמידע המצומצם שיש לנו בווירשארק (גודל הפאקטה וזמן השליחה)?

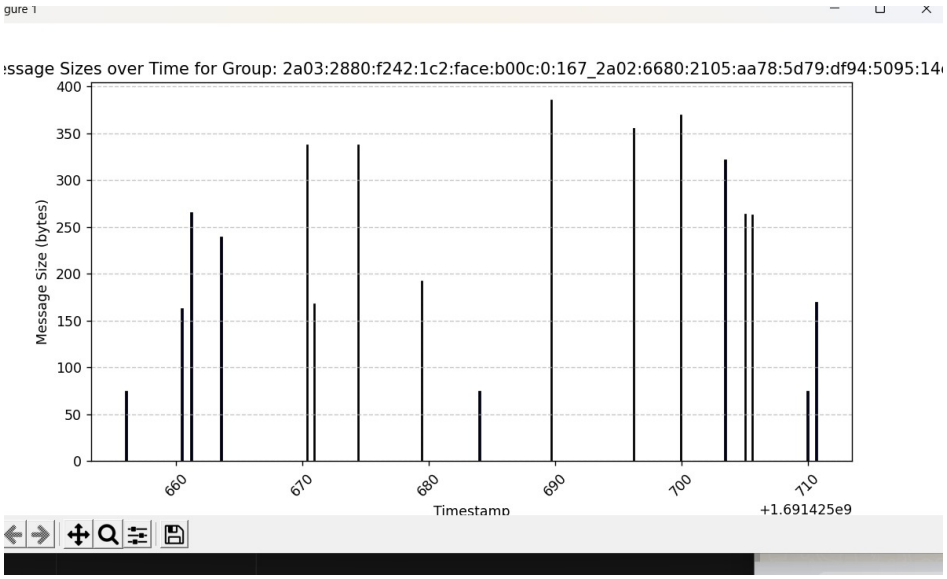
ניסינו לתפוס את ההבדלים בתעבורה בין סרטונים תמונות והודעות טקסט קצרות.
פתחנו קבוצה והקלטנו בווירשארק את התעבורה מהשרת של ווצאפ (שגילינו לפי סינון פרוטוקול tcp , הפורט המתאים והשרת שמצאנו) וזיהוי הודעות שנשלחו מאפליקציה כאשר זו הייתה האפליקציה היחידה הפתוחה במחשב שלנו.

בנוסף כתבנו קוד שיקלוט את התעבורה בפרוטוקול TCP במשך דקה, יחלק אותה לקבוצות לפי המקור והיעד וגם ויציג לנו אך ורק את קבוצות ההודעות שמקורן במחשב שלנו ויעדן בשרת של וואטסאפ או להפך.

כך יצרנו גרפים המראים את הפאקטות שעוברות והפרטים המוצגים לגביהן הם הזמן שעבר בין פאקטה לפאקטה והגודל שלה (בדומה לגרפים שהוצגו במאמר.)

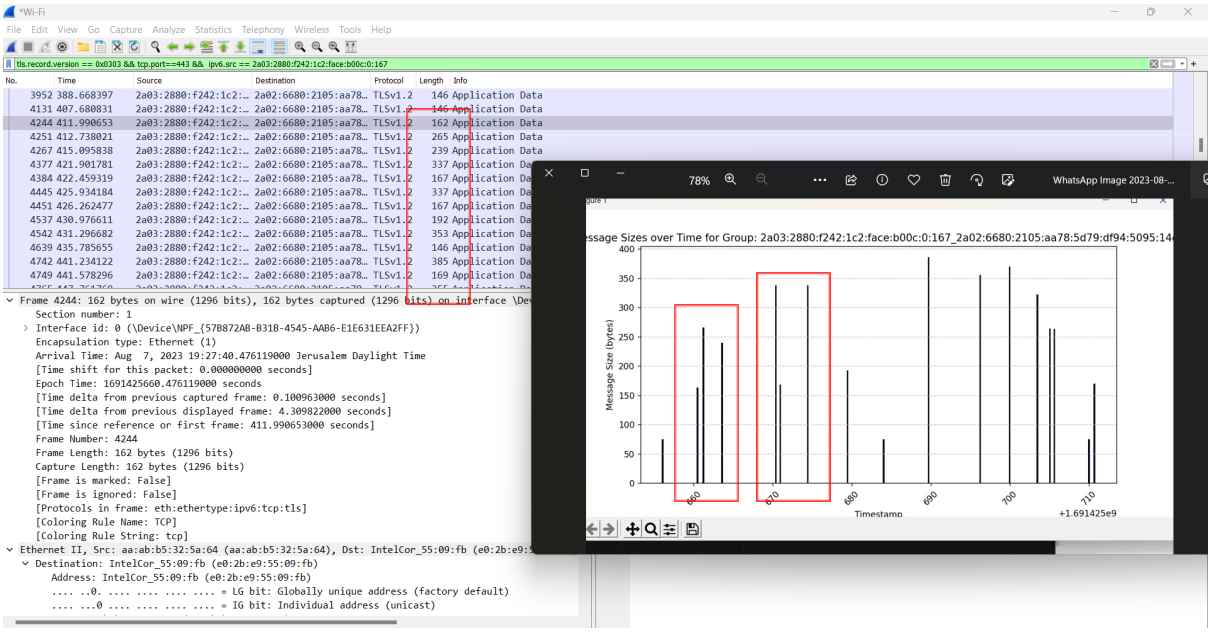
למשל הגרפים לאחר דקת תקשורת קצרה בהודעות טקסט בקבוצה שלנו :





ניסינו להתאים בין מה שראינו בווירשארק לבין הגרף שהציג הקוד.

בצילום המסך שלמטה (איור 6) רואים קשר בין גודל הפאקטות בווירשארק וכמובן המקור והיעד לבין הגרף (ישנן גם פאקטות שלא חופפות)

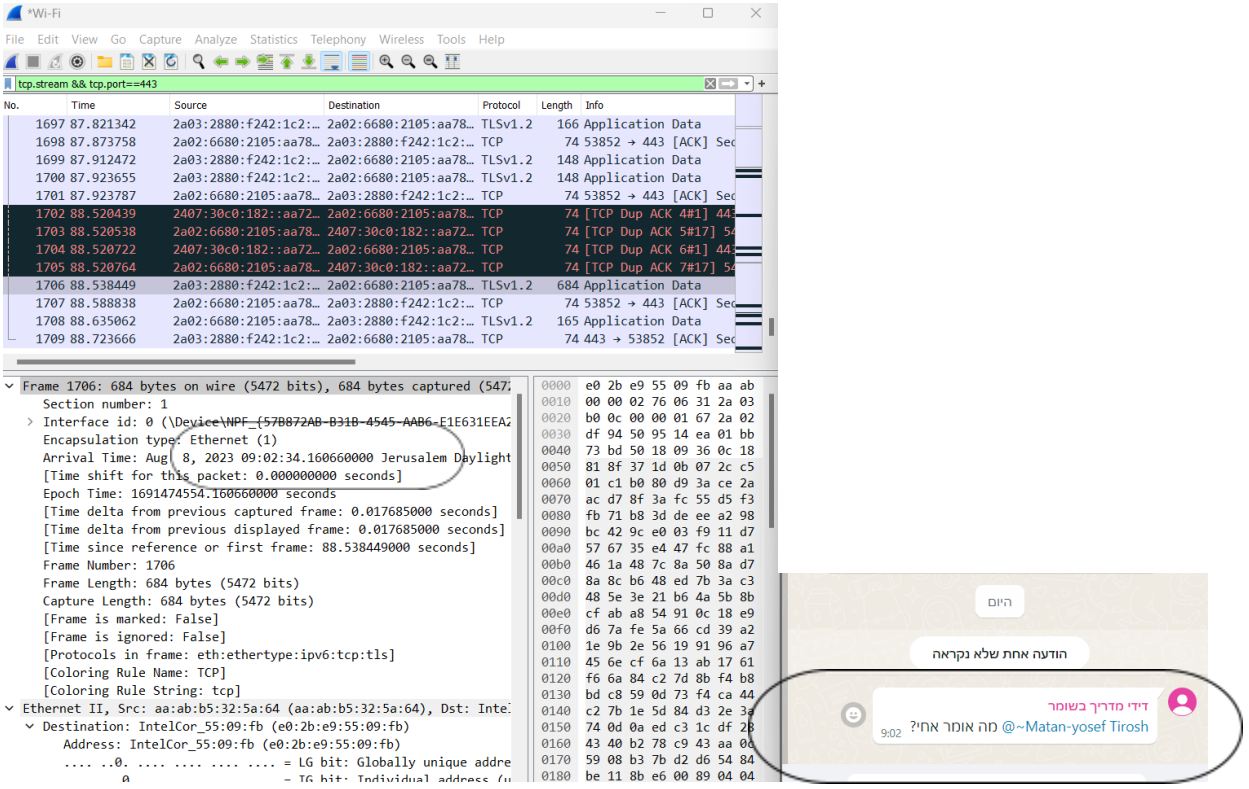


(איור 6): נביט מפאקטה בגודל 162 שהיא העמודה השניה בגרף שלנו לאחריה 265 239 וגם 337 מתאימות וכן אפשר לבדוק הלאה. ישנן פאקטות שמופיעות בווירשארק אך לא נכנסו לגרף . ההשערה שלנו היא שהסינון של הקוד לא מדוייק ונכנסות בו גם פאקטות שהן "רעשי רקע" מבחינתנו ולכן ההתאמה לא מדוייקת.

מצאנו התאמה בין גודל הפאקטות אך עדיין חסר לנו מידע לגבי איך הן מתחלקות ותוך כמה זמן נשלחת הודעה שלמה

בהמשך למחקר שלנו - ניסינו לעקוב אחד "stream" אחד כדי לדעת אילו הודעות שייכות לאותה שיחה

קור אותה ע"מ לדעת לסנן אך ורק הודעות שאינן לחיצות

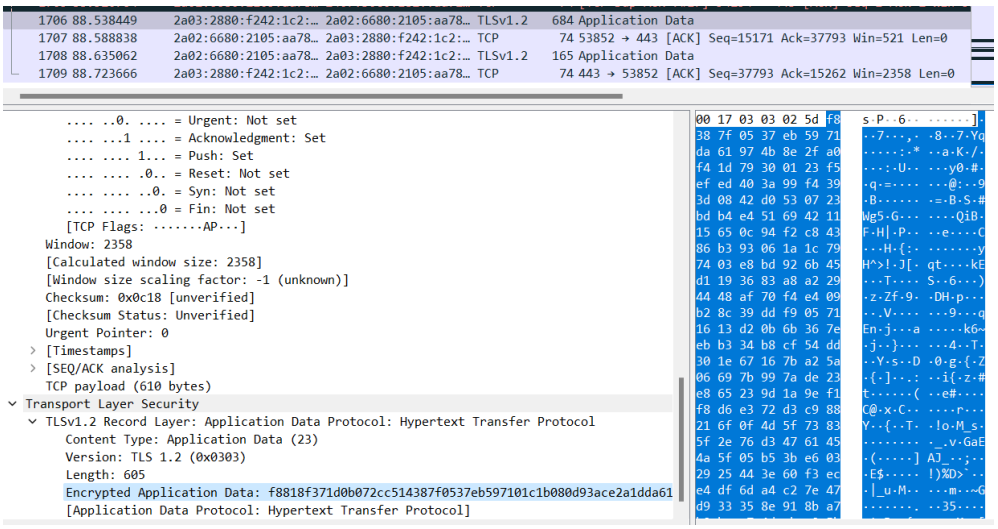


רואים שהזמנים חופפים בין ההודעה והפאקטה שנתפסה ורואים שלפניה ואחריה זוהי כבר לא אותה הודעה כי הפאקטות לפניה ואחריה מקורן לא בשרת וצאפ שממנו מגיעות ההודעות אלא בשרת של המחשב שלנו מול וצאפ.

נשים לב למאפיינים - הפרוטוקול הוא TLS גרסה 1.2 בהוא אחראי להצפנת הData.

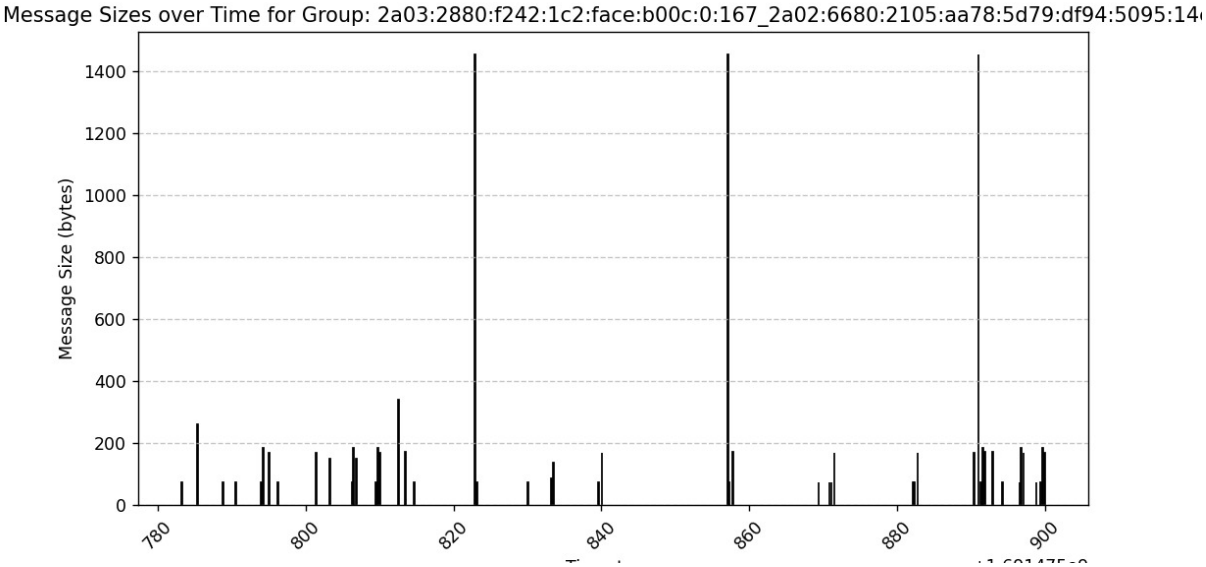
בנוסף הפורט והשרת תואמים לגילויים הקודמים שלנו לגבי שרת וצאפ- המשתמש בפורט 443 ובכתובת יעד ומקור ipv6: Src: 2a03:2880:f242:1c2:face:b00c:0:167 , Dst: 2a02:6680:2105:aa78:5d79:df94:5095:14ea

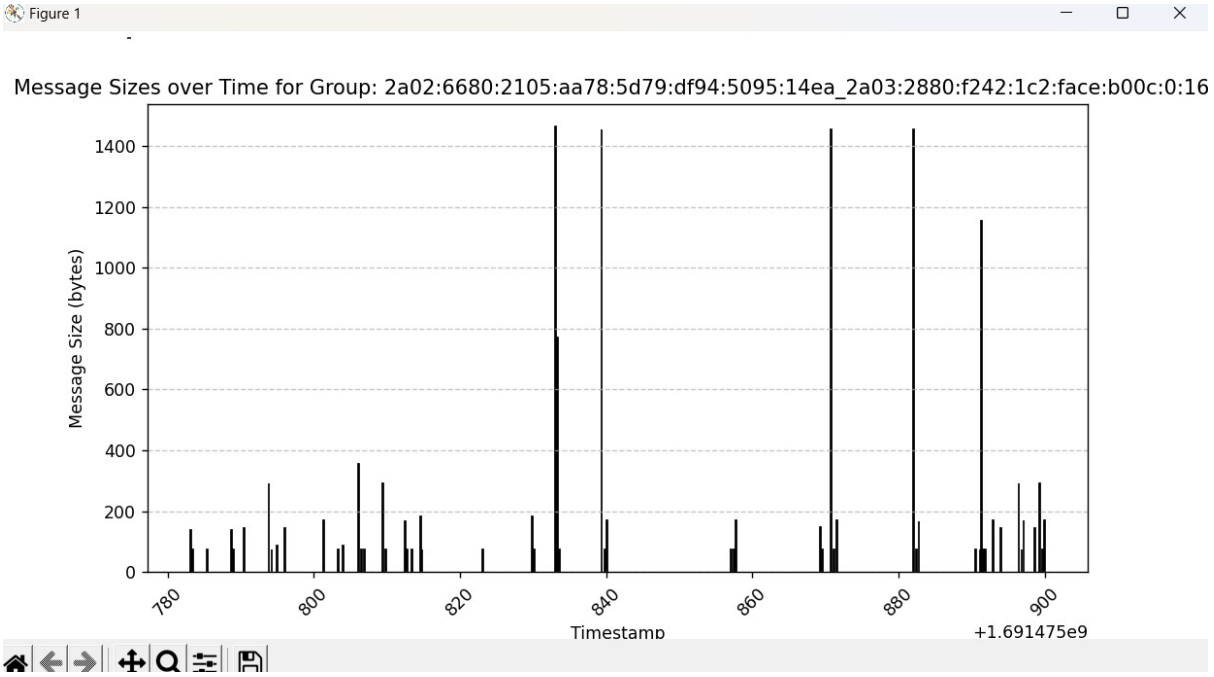
בתיאור כתוב לנו "application data" ובנוסף אפשר לראות בתוכן הפאקטה את הדאטה המוצפן:



אז בדוגמא זו ההודעה הייתה כנראה מספיק קצרה כך שהיא נשלחה בחתיכה אחת. באורך 605 בייטים.

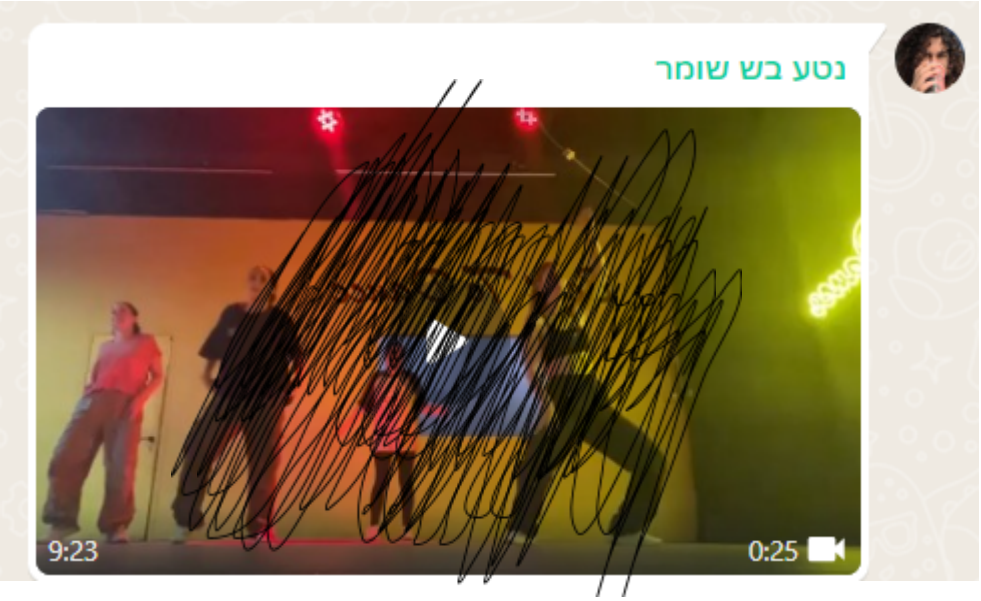
על מנת לבדוק כמה פאקטות שייכות לאותה הודעה ואיך נראה ההבדל בין סרטונים ותמונות להודעות רגילות פתחנו שיחה בקבוצה שלנו (בזמן שלא היו הודעות אחרות באפליקציה) ואלו התוצאות אחרי 2 דקות שנתנו לקוד לרוץ ובתוכן שלחנו תמונות וסרטונים בקבוצה:





בהקלטת הווירשארק המתאימה ראינו כמה חפיפות:

למשל בשעה 9:23 לקראת סופה נצפו 3 פאקטות גדולות המקבילות בערך לגודל 1450 ובדיוק בזמן זה נשלח סרטון בקבוצה שבחנו:



סיכום ביניים- ממצאים שראינו עד עכשיו:

- שרת ווצאפ במחשב שלנו - שממנו ואליו מגיעה התעבורה אותה אנחנו בוחנות הוא:
  2a03:2880:f242:1c2:face:b00c:0:167
  הפורט המתאים : 443
- ניתן לראות שהשרת זהה עבור כל ההודעות על אף שהן מתקבלות מקבוצות שונות.
- ההודעות המתקבלות משרת זה ואליו מוצפנות ע"י פרוטוקול TLS כלומר אי אפשר לדעת מה תוכן ההודעה רק את גודלה ואת הזמן שנשלחה.
- הודעות טקסט לעיתים נשלחות בפאקטות גדולות וסרטונים ותמונות ככל הנראה מחולקים לכמה פאקטות גדולות.

לאחר נסיונות אלו שיפרנו את הקוד :

הקוד גם ישמור קובץ טקסט ובו כל הפאקטות שתפס.

המחקר עצמו - הקלטת 4 קבוצות:

לצורך המחקר, לפי מה שהתבקשנו, פתחנו 4 קבוצות שונות , בכל קבוצה נשלח תוכן אחר שיהיה העיקרי .

נקליט 10 דקות כל קבוצה ונבדוק את ההבדלים בין הגרפים שיוצגו.

בנוסף נבדוק ונשווה את הקלטות הווירשארק ואת המידע שתפס הקוד שלנו. ונבדוק סטטיסטיקות של הפרשי זמן בין הודעות. בעזרת קובץ EXCEL אליו נייצא את תוצאות הווירשארק

קבוצה 1 - הודעות טקסט

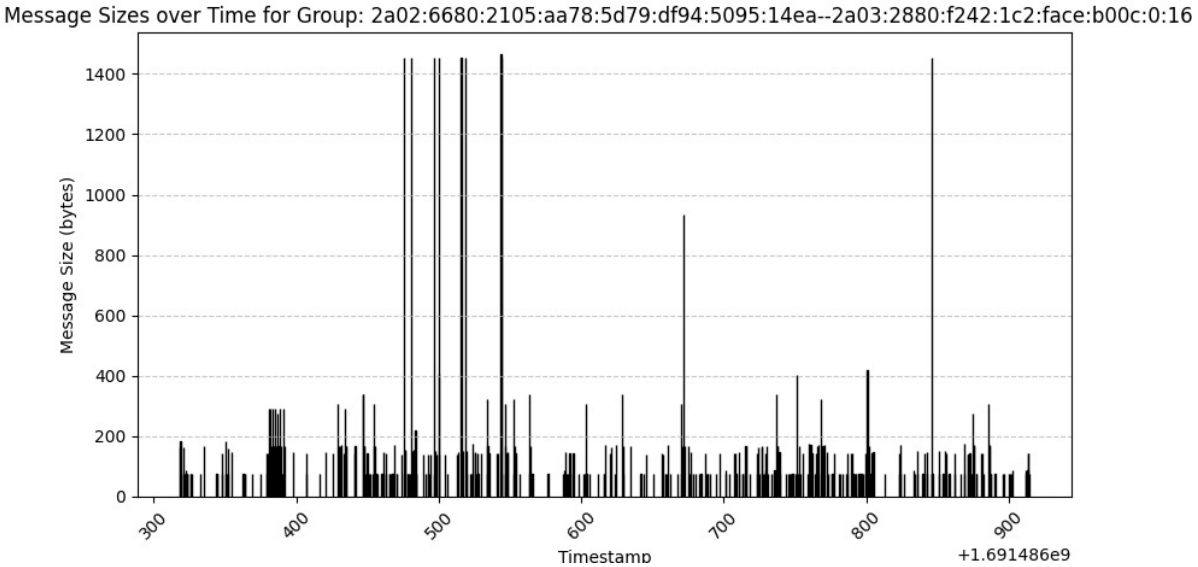
קבוצה 2- תמונות

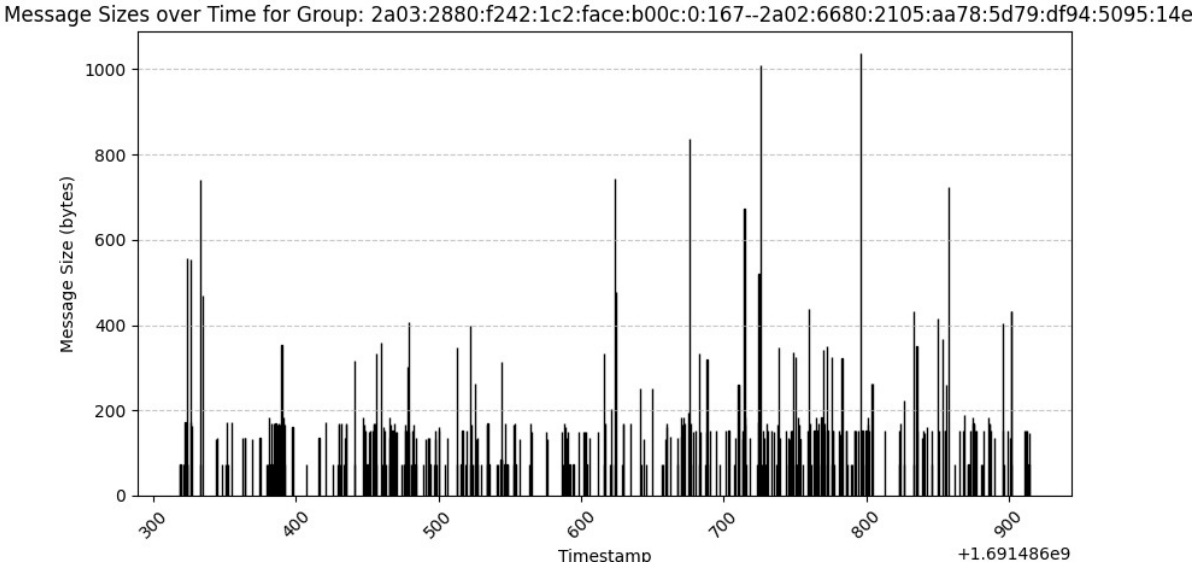
קבוצה 3 - סרטונים

קבוצה 4 - שמע , הקלטות קוליות.

האזנה מספר 1 - הודעות טקסט:

10 דקות של הודעות טקסט בקבוצה
תוצאות :





חלק מקובץ הטקסט שמכיל את סיכום הפאקטות שנתפסו:

```
קובץ  עריכה  הצג
Message ID: 1, Size: 144 bytes, Timestamp: 1691486381.0722673, protocol:IPv6
 Message ID: 3, Size: 86 bytes, Timestamp: 1691486381.3102603, protocol:IPv6
Message ID: 1, Size: 290 bytes, Timestamp: 1691486382.0475986, protocol:IPv6
Message ID: 1, Size: 144 bytes, Timestamp: 1691486382.3660066, protocol:IPv6
Message ID: 1, Size: 167 bytes, Timestamp: 1691486382.6645062, protocol:IPv6
Message ID: 1, Size: 167 bytes, Timestamp: 1691486383.0758529, protocol:IPv6
Message ID: 1, Size: 290 bytes, Timestamp: 1691486383.5634902, protocol:IPv6
 Message ID: 2, Size: 74 bytes, Timestamp: 1691486383.8816204, protocol:IPv6
Message ID: 1, Size: 167 bytes, Timestamp: 1691486384.1091974, protocol:IPv6
Message ID: 1, Size: 167 bytes, Timestamp: 1691486384.3893328, protocol:IPv6
Message ID: 1, Size: 290 bytes, Timestamp: 1691486384.8802652, protocol:IPv6
 Message ID: 3, Size: 74 bytes, Timestamp: 1691486385.4458358, protocol:IPv6
Message ID: 1, Size: 167 bytes, Timestamp: 1691486385.7117865, protocol:IPv6
Message ID: 1, Size: 274 bytes, Timestamp: 1691486386.5602794, protocol:IPv6
Message ID: 2, Size: 144 bytes, Timestamp: 1691486386.9212866, protocol:IPv6
 Message ID: 1, Size: 167 bytes, Timestamp: 1691486387.273663, protocol:IPv6
Message ID: 1, Size: 167 bytes, Timestamp: 1691486387.5273738, protocol:IPv6
Message ID: 1, Size: 290 bytes, Timestamp: 1691486388.2417438, protocol:IPv6
 Message ID: 1, Size: 74 bytes, Timestamp: 1691486388.6006684, protocol:IPv6
 Message ID: 1, Size: 167 bytes, Timestamp: 1691486388.881173, protocol:IPv6
Message ID: 2, Size: 167 bytes, Timestamp: 1691486389.3522506, protocol:IPv6
  Message ID: 3, Size: 74 bytes, Timestamp: 1691486389.955151, protocol:IPv6
 Message ID: 9, Size: 74 bytes, Timestamp: 1691486390.8704865, protocol:IPv6
Message ID: 1, Size: 290 bytes, Timestamp: 1691486391.0725043, protocol:IPv6
 Message ID: 1, Size: 74 bytes, Timestamp: 1691486391.3986616, protocol:IPv6
Message ID: 2, Size: 167 bytes, Timestamp: 1691486391.7557876, protocol:IPv6
Message ID: 1, Size: 146 bytes, Timestamp: 1691486397.4638715, protocol:IPv6
```

```
Group Identifier: 2a03:2880:f242:1c2:face:b00c:0:167--2a02:6680:2105:aa78:5d79:df94:5095:14ea
Message ID: 16, Size: 74 bytes, Timestamp: 1691486318.7190757, protocol:IPv6
Message ID: 29, Size: 74 bytes, Timestamp: 1691486318.9255006, protocol:IPv6
Message ID: 21, Size: 74 bytes, Timestamp: 1691486321.1241717, protocol:IPv6
  Message ID: 8, Size: 74 bytes, Timestamp: 1691486321.351541, protocol:IPv6
Message ID: 2, Size: 173 bytes, Timestamp: 1691486322.3140736, protocol:IPv6
 Message ID: 12, Size: 74 bytes, Timestamp: 1691486322.539243, protocol:IPv6
Message ID: 7, Size: 557 bytes, Timestamp: 1691486323.2481687, protocol:IPv6
Message ID: 17, Size: 74 bytes, Timestamp: 1691486323.4712477, protocol:IPv6
  Message ID: 8, Size: 74 bytes, Timestamp: 1691486323.672129, protocol:IPv6
 Message ID: 5, Size: 173 bytes, Timestamp: 1691486325.999489, protocol:IPv6
 Message ID: 4, Size: 555 bytes, Timestamp: 1691486326.220316, protocol:IPv6
Message ID: 1, Size: 163 bytes, Timestamp: 1691486326.6325421, protocol:IPv6
Message ID: 1, Size: 741 bytes, Timestamp: 1691486332.4837043, protocol:IPv6
 Message ID: 1, Size: 74 bytes, Timestamp: 1691486332.7104511, protocol:IPv6
 Message ID: 2, Size: 469 bytes, Timestamp: 1691486334.910576, protocol:IPv6
 Message ID: 1, Size: 134 bytes, Timestamp: 1691486344.112352, protocol:IPv6
Message ID: 1, Size: 136 bytes, Timestamp: 1691486344.3510554, protocol:IPv6
 Message ID: 2, Size: 74 bytes, Timestamp: 1691486347.9070206, protocol:IPv6
 Message ID: 6, Size: 74 bytes, Timestamp: 1691486350.2991254, protocol:IPv6
Message ID: 5, Size: 173 bytes, Timestamp: 1691486351.0795243, protocol:IPv6
 Message ID: 2, Size: 74 bytes, Timestamp: 1691486352.3966522, protocol:IPv6
Message ID: 2, Size: 172 bytes, Timestamp: 1691486354.5929966, protocol:IPv6
Windows (CRLF)   100%   שורה 47, עמודה 77
```

שמנו לב שחוזרות על עצמן פאקטות בגודל 74 בייט והן רעש מבחינתנו.
לכן כרגע אנו לא מחשיבות אותן כחבילות שמעבירות הודעות ממש אלא כרעש קבוע של האפליקציה. כלומר לחיצות הידיים , ואכן רואים בהקלטת הווירשארק המתאימה(למטה) שכל הפאקטות שגודלן 74 הן מסוג ACK- התחלת קשר.

```
*Wi-Fi
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
tcp.port==443 && (ipv6.src==2a03:2880:f242:1c2:face:b00c:0:167 || ipv6.dst==2a03:2880:f242:1c2:face:b00c:0:167)
No.  Time        Source                  Destination             Protocol  Length  Info
145  30.084955   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TLSv1.2   167  Application Data
147  30.162685   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TLSv1.2   167  Application Data
153  30.285412   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TLSv1.2   169  Application Data
157  30.932037   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TCP        74  53852 → 443 [ACK] Seq=2030 Ack=2407 Win=515 Len=0
158  32.328460   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TLSv1.2   144  Application Data
161  32.547416   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TCP        74  53852 → 443 [ACK] Seq=2100 Ack=2484 Win=521 Len=0
171  33.723375   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TCP        74  53852 → 443 [ACK] Seq=2100 Ack=2561 Win=520 Len=0
173  34.562647   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TCP        74  53852 → 443 [ACK] Seq=2100 Ack=2641 Win=520 Len=0
175  36.209684   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TCP        74  53852 → 443 [ACK] Seq=2100 Ack=2721 Win=520 Len=0
176  36.673581   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TLSv1.2   306  Application Data
179  36.978681   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TCP        74  53852 → 443 [ACK] Seq=2332 Ack=2832 Win=519 Len=0
184  37.241366   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TLSv1.2   167  Application Data
186  37.282006   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TLSv1.2   167  Application Data
189  37.372055   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TCP        74  53852 → 443 [ACK] Seq=2518 Ack=3509 Win=517 Len=0
190  37.384391   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TLSv1.2   173  Application Data
193  37.446935   2a02:6680:2105:aa78:… 2a03:2880:f242:1c2:… TLSv1.2   169  Application Data
> Frame 157: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{57B872AB-B31B-4545-AAB6-E1E631EEA2FF}, id 0
> Ethernet II, Src: IntelCor_55:09:fb (e0:2b:e9:55:09:fb), Dst: aa:ab:b5:32:5a:64 (aa:ab:b5:32:5a:64)
> Internet Protocol Version 6, Src: 2a02:6680:2105:aa78:5d79:df94:5095:14ea, Dst: 2a03:2880:f242:1c2:face:b00c:0:167
> Transmission Control Protocol, Src Port: 53852, Dst Port: 443, Seq: 2030, Ack: 2407, Len: 0
```

ייצאנו לקובץ CSV את הפאקטות המתאימות (ללא הרעש) בעזרת סינון נוסף בווירשארק.

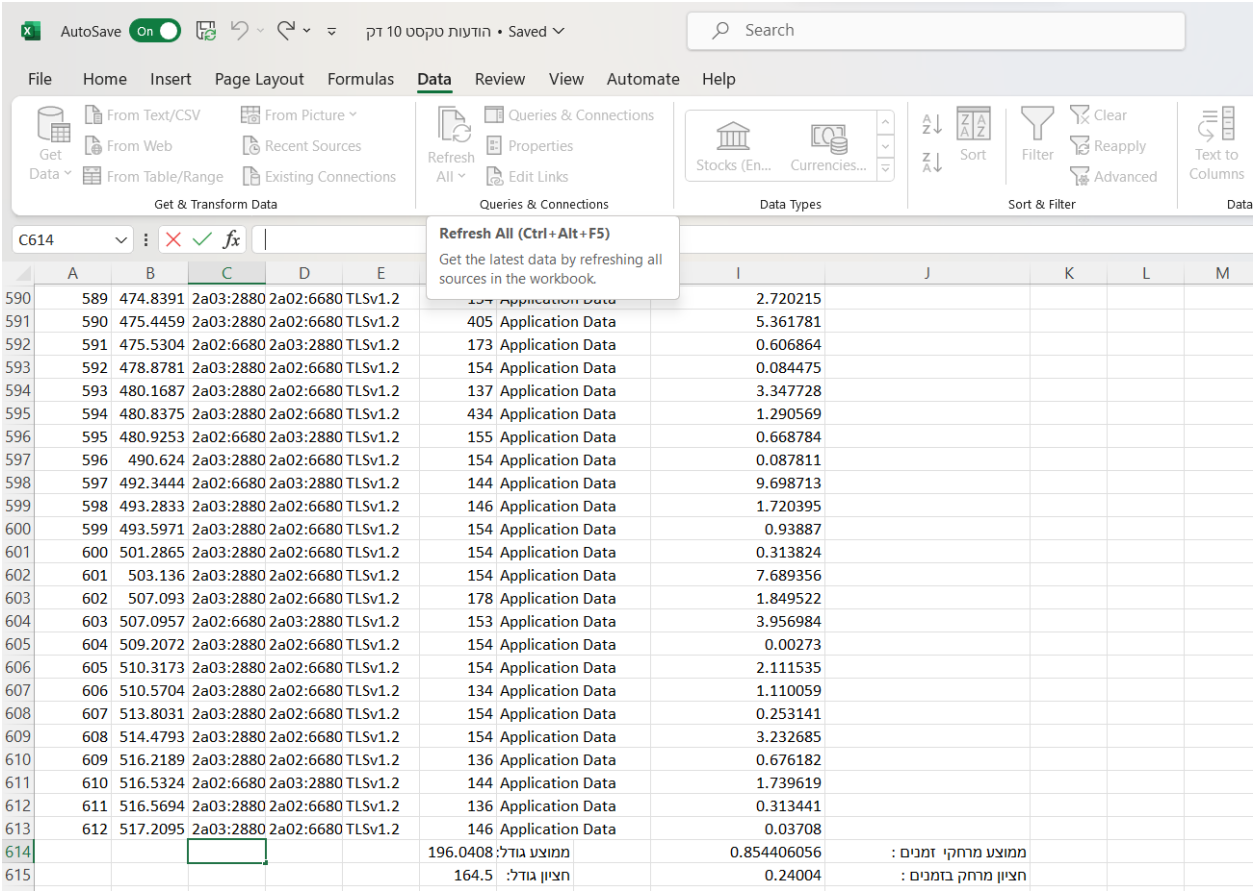
ביצענו ממוצע על עמודת הגודל.
גילינו שהגודל הממוצע הוא 196 עבור כל פאקטה.

החציון עבור גודל הפאקטות הוא 164.5

ממוצע המרחק בין חבילה לחבילה הוא: 0.8544

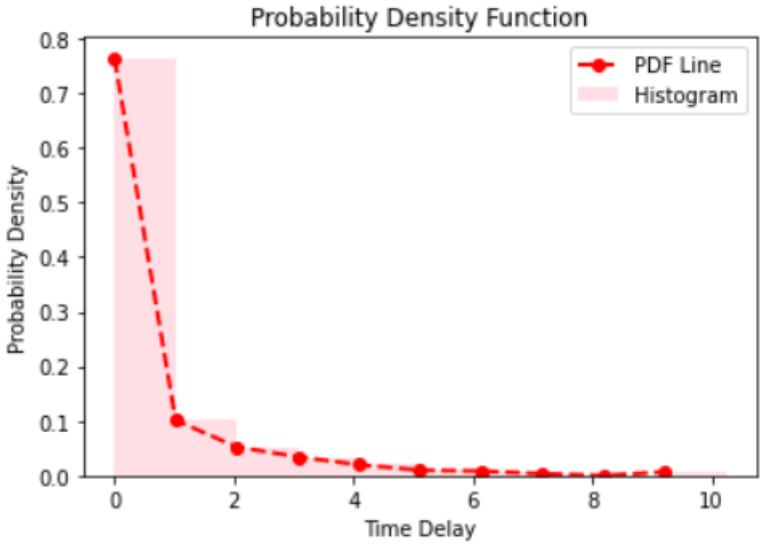
והחציון הוא: 0.24

כפי שניתן לראות בצילום המסך של האקסל:



	A	B	C	D	E			I	J	K	L	M
590	589	474.8391	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	2.720215				
591	590	475.4459	2a03:2880	2a02:6680	TLSv1.2	405	Application Data	5.361781				
592	591	475.5304	2a02:6680	2a03:2880	TLSv1.2	173	Application Data	0.606864				
593	592	478.8781	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	0.084475				
594	593	480.1687	2a03:2880	2a02:6680	TLSv1.2	137	Application Data	3.347728				
595	594	480.8375	2a03:2880	2a02:6680	TLSv1.2	434	Application Data	1.290569				
596	595	480.9253	2a02:6680	2a03:2880	TLSv1.2	155	Application Data	0.668784				
597	596	490.624	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	0.087811				
598	597	492.3444	2a02:6680	2a03:2880	TLSv1.2	144	Application Data	9.698713				
599	598	493.2833	2a03:2880	2a02:6680	TLSv1.2	146	Application Data	1.720395				
600	599	493.5971	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	0.93887				
601	600	501.2865	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	0.313824				
602	601	503.136	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	7.689356				
603	602	507.093	2a03:2880	2a02:6680	TLSv1.2	178	Application Data	1.849522				
604	603	507.0957	2a02:6680	2a03:2880	TLSv1.2	153	Application Data	3.956984				
605	604	509.2072	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	0.00273				
606	605	510.3173	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	2.111535				
607	606	510.5704	2a03:2880	2a02:6680	TLSv1.2	134	Application Data	1.110059				
608	607	513.8031	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	0.253141				
609	608	514.4793	2a03:2880	2a02:6680	TLSv1.2	154	Application Data	3.232685				
610	609	516.2189	2a03:2880	2a02:6680	TLSv1.2	136	Application Data	0.676182				
611	610	516.5324	2a02:6680	2a03:2880	TLSv1.2	144	Application Data	1.739619				
612	611	516.5694	2a03:2880	2a02:6680	TLSv1.2	136	Application Data	0.313441				
613	612	517.2095	2a03:2880	2a02:6680	TLSv1.2	146	Application Data	0.03708				
614						196.0408	:ממוצע גודל	0.854406056	: ממוצע מרחקי זמנים			
615						164.5	:חציון גודל	0.24004	: חציון מרחק בזמנים			

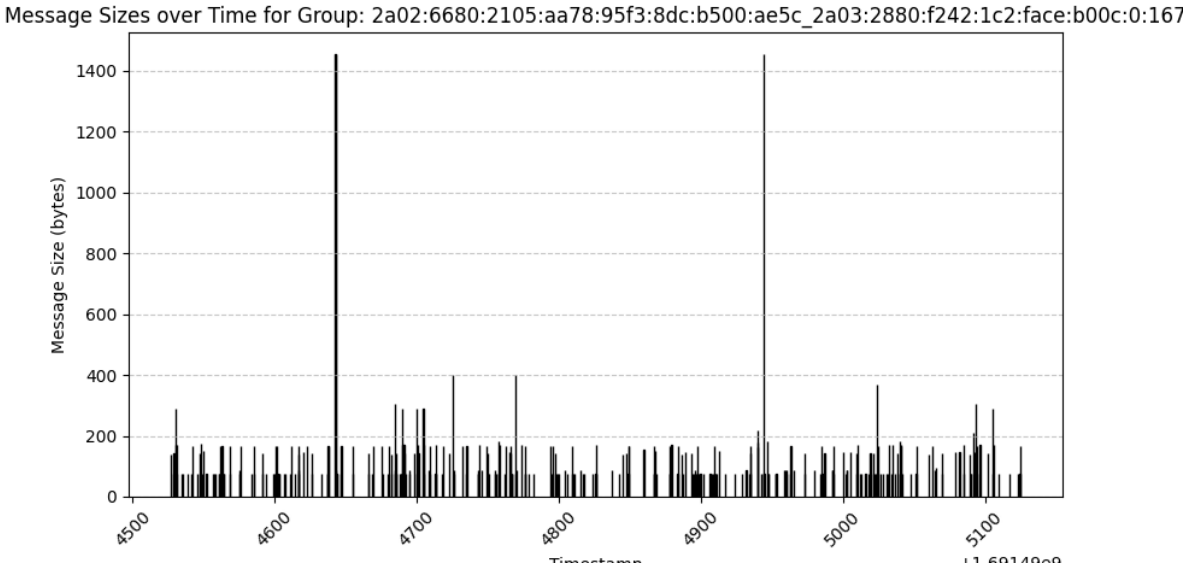
העלינו את קובץ האקסל שיצרנו לJupyter notebook כדי ליצור את גרף הPDF:



האזנה מספר 2- תמונות:

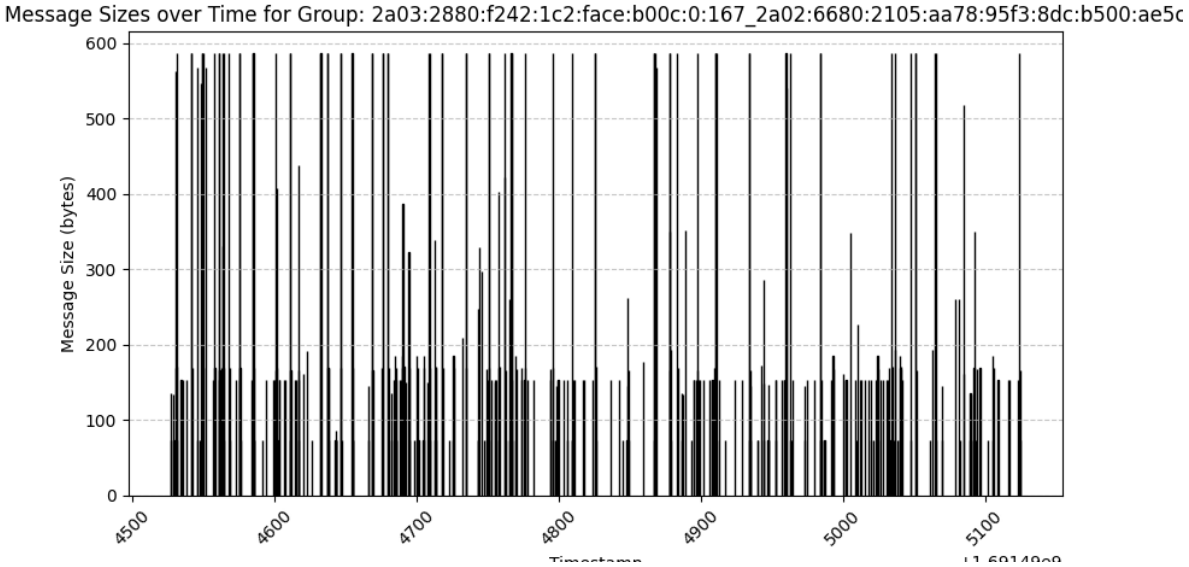
הקלטנו 10 דקות של שליחת תמונות .

ואלו היו גרפי התוצאות :



<u>הגרף העליון:</u> מייצג את מה שיצא מהמחשב שלנו אל שרתי ווצאפ. אולם אנחנו שלחנו את התמונות ממכשירים אחרים אל הקבוצה. לכן הוא לא משמעותי כרגע למעקב אחר שליחת תמונות

<u>הגרף התחתון:</u> מייצג מבחינתנו את התעבורה המרובה בתמונות שנשלחה ועברה משרתי ווצאפ אל המחשב שלנו.



בהקלטת הווירשארק שמנו לב כי הרבה מהפאקטות באורך 590 בערך הן מסוג ACK ולכן רעש מבחינתנו

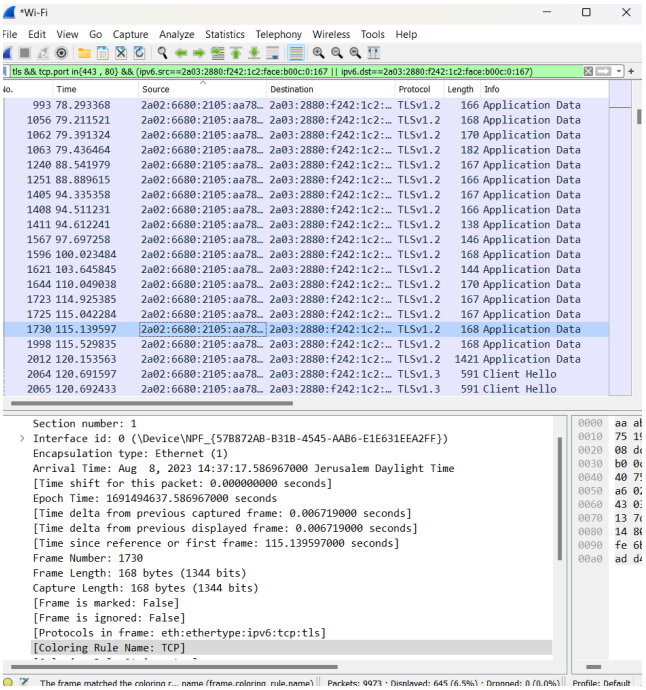
No.	Time	Source	Destination	Protocol	Length	Info
6375	388.549041	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	586	Application Data
6640	411.603813	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
6641	411.603813	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
7174	437.393545	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
7175	437.393545	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
7223	440.515694	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
7224	440.515694	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
7225	440.515694	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	586	Application Data
7569	461.677361	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
7570	461.677361	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
7820	511.531045	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
7821	511.531045	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
8094	514.341625	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
8184	524.977599	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
8193	528.838626	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
8194	528.838626	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
8229	541.930634	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	586	[TCP Previous segment
8230	541.930634	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	586	Ignored Unknown Recor
8236	543.026957	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	[TCP Retransmission]
8830	601.819189	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
8833	601.881895	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
8834	601.881895	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
9001	616.811873	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
9002	616.811873	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
9004	616.811873	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
9005	616.811873	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
9006	616.811873	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	586	Application Data
9337	626.900860	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
9558	634.224204	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
9817	650.203205	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
2064	120.691597	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.3	591	Client Hello
2065	120.692433	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.3	591	Client Hello
6940	421.814303	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.3	591	Client Hello
2077	120.796560	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.3	903	Application Data
2079	120.796832	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.3	903	Application Data

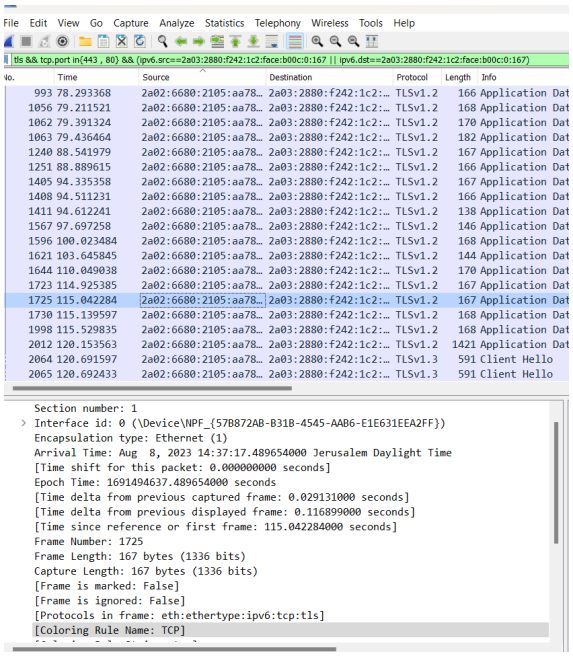
בשני הגרפים נתמקד לרגע במשותף -
קבוצות של עמודות צפופות בגובה באזור 150-180 .

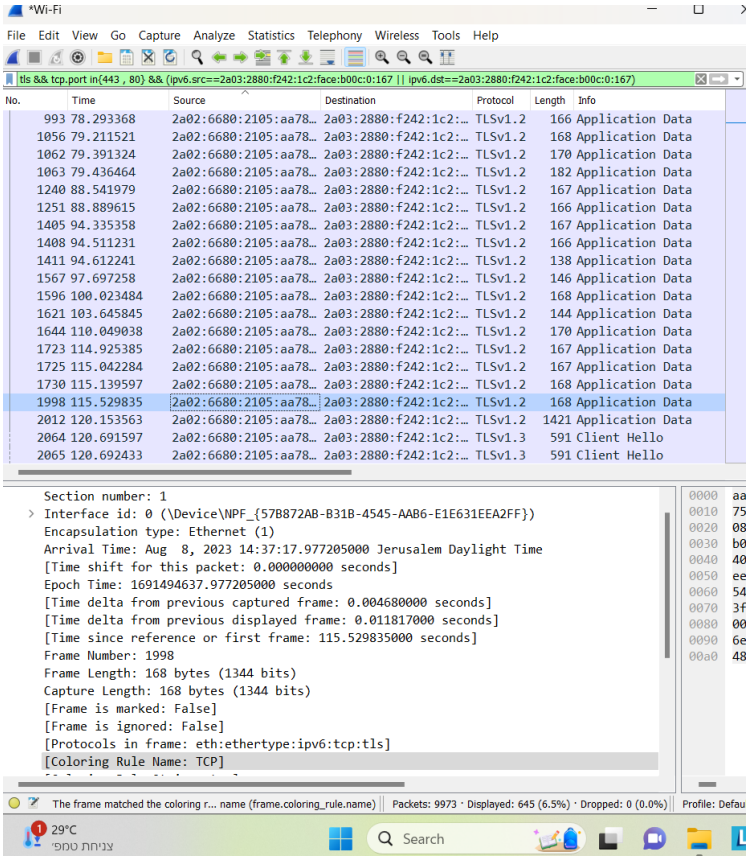
נביט בהקלטת הווירשארק במיון לפי מקור השולח :

נבחין בצמדים או שלישיות של חבילות שהגיעו בזמן ממש דומה ברמת הבדל של 0.01 שניות. ההנחה שלנו היא שכל צמד כזה הוא תמונה שהמידע בה חולק כמה חבילות. למשל :

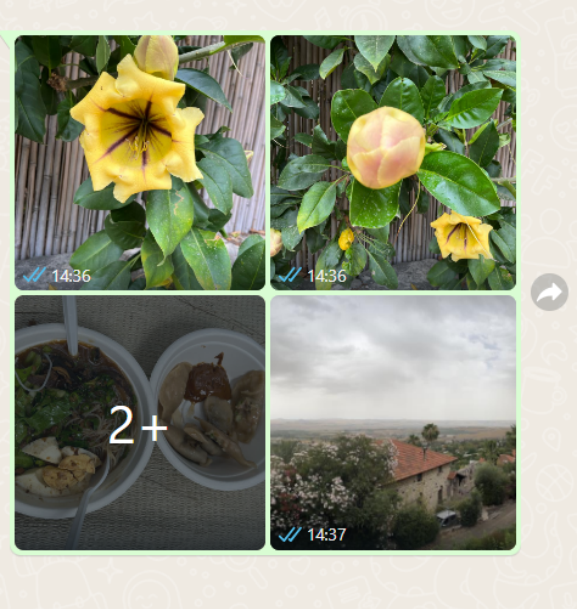
אפשר לראות בזמן 115…(הפאקטות המסומנות בכחול) :הבדלים מזעריים בזמן השליחה בשעה 14:37 ותכף נסתכל בקבוצה מה נשלח בשעה זו.



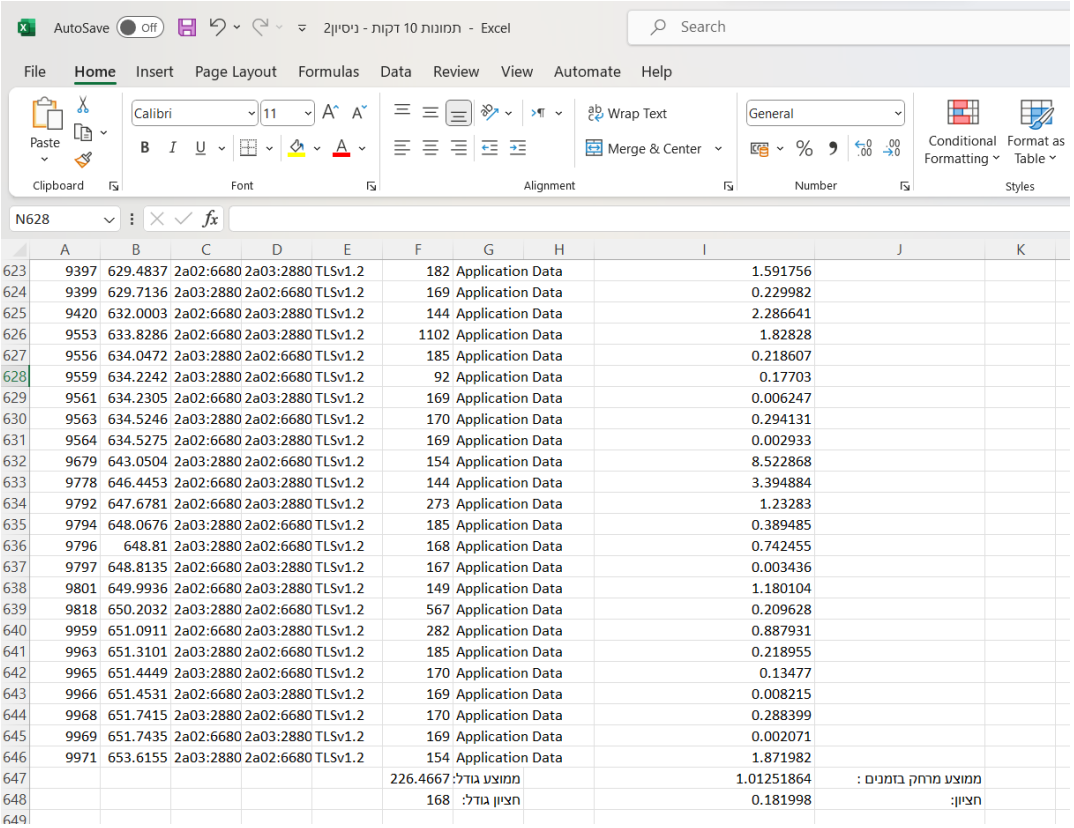




ואכן בשעה 14:37 נשלחה תמונה והיא כנראה חולקה ל3 חבילות כל אחת 167/8 בגודלה.



בקובץ האקסל שייצאנו מהווישארק לאחר מכן ביצענו median וגם average על גודל הפאקטות והמרחק בזמנים בין פאקטה לפאקטה. כמו שמובא בצילום:



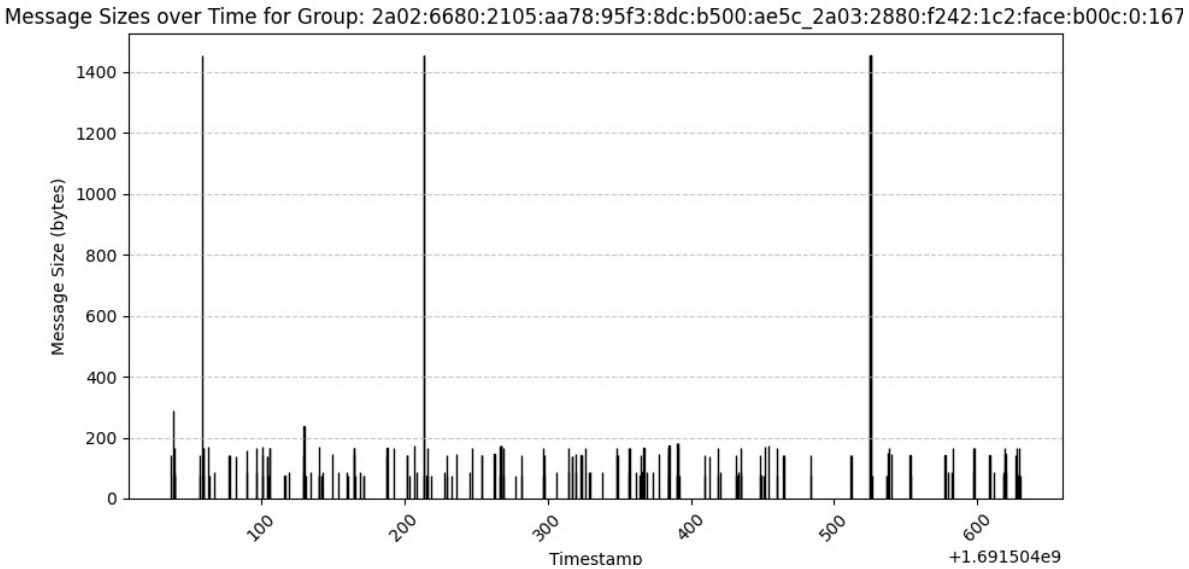
	A	B	C	D	E	F	G	H	I	J	K
623	9397	629.4837	2a02:6680	2a03:2880	TLSv1.2	182	Application Data		1.591756		
624	9399	629.7136	2a03:2880	2a02:6680	TLSv1.2	169	Application Data		0.229982		
625	9420	632.0003	2a02:6680	2a03:2880	TLSv1.2	144	Application Data		2.286641		
626	9553	633.8286	2a02:6680	2a03:2880	TLSv1.2	1102	Application Data		1.82828		
627	9556	634.0472	2a03:2880	2a02:6680	TLSv1.2	185	Application Data		0.218607		
628	9559	634.2242	2a03:2880	2a02:6680	TLSv1.2	92	Application Data		0.17703		
629	9561	634.2305	2a02:6680	2a03:2880	TLSv1.2	169	Application Data		0.006247		
630	9563	634.5246	2a03:2880	2a02:6680	TLSv1.2	170	Application Data		0.294131		
631	9564	634.5275	2a02:6680	2a03:2880	TLSv1.2	169	Application Data		0.002933		
632	9679	643.0504	2a03:2880	2a02:6680	TLSv1.2	154	Application Data		8.522868		
633	9778	646.4453	2a02:6680	2a03:2880	TLSv1.2	144	Application Data		3.394884		
634	9792	647.6781	2a02:6680	2a03:2880	TLSv1.2	273	Application Data		1.23283		
635	9794	648.0676	2a03:2880	2a02:6680	TLSv1.2	185	Application Data		0.389485		
636	9796	648.81	2a03:2880	2a02:6680	TLSv1.2	168	Application Data		0.742455		
637	9797	648.8135	2a02:6680	2a03:2880	TLSv1.2	167	Application Data		0.003436		
638	9801	649.9936	2a02:6680	2a03:2880	TLSv1.2	149	Application Data		1.180104		
639	9818	650.2032	2a03:2880	2a02:6680	TLSv1.2	567	Application Data		0.209628		
640	9959	651.0911	2a02:6680	2a03:2880	TLSv1.2	282	Application Data		0.887931		
641	9963	651.3101	2a03:2880	2a02:6680	TLSv1.2	185	Application Data		0.218955		
642	9965	651.4449	2a03:2880	2a02:6680	TLSv1.2	170	Application Data		0.13477		
643	9966	651.4531	2a02:6680	2a03:2880	TLSv1.2	169	Application Data		0.008215		
644	9968	651.7415	2a03:2880	2a02:6680	TLSv1.2	170	Application Data		0.288399		
645	9969	651.7435	2a02:6680	2a03:2880	TLSv1.2	169	Application Data		0.002071		
646	9971	653.6155	2a03:2880	2a02:6680	TLSv1.2	154	Application Data		1.871982		
647						226.4667	:ממוצע גודל		1.01251864	ממוצע מרחק בזמנים :	
648						168	:חציון גודל		0.181998	:חציון	
649											

אכן הגודל המדיאני היה 167 . מה שתומך בהשערתנו שהחלוקה היא לפאקטות בגודל 167 בערך.

ממוצע מרחק בזמנים : 1.01251864
חציון מרחק בזמנים: 0.181998

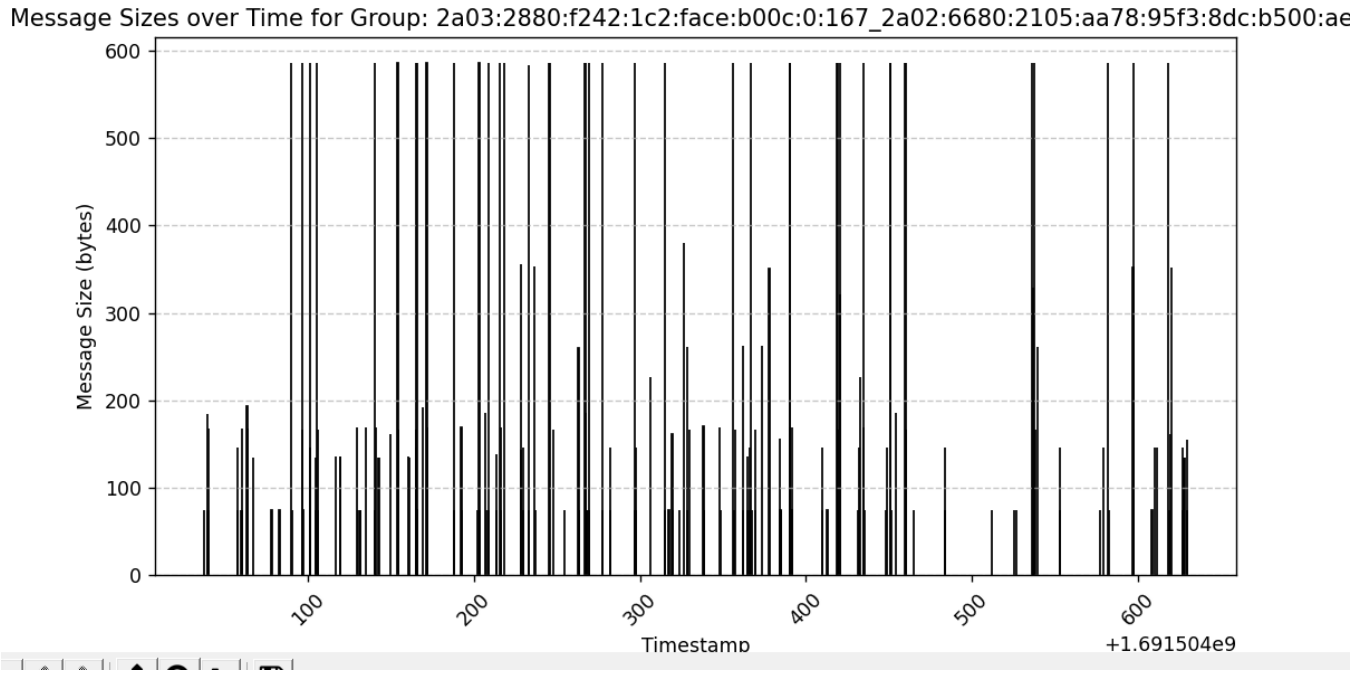
כלומר חציון המרחק בזמנים קטן יותר מהודעות טקסט. ואילו הגודל של חבילה ממוצעת דומה.
כלומר הגדלים הם דומים אבל נשלחים בצמדים צפופים יותר, כי הקבצים גדולים יותר ומחולקים ליותר חתיכות.

האזנה מספר 3 - סרטונים:

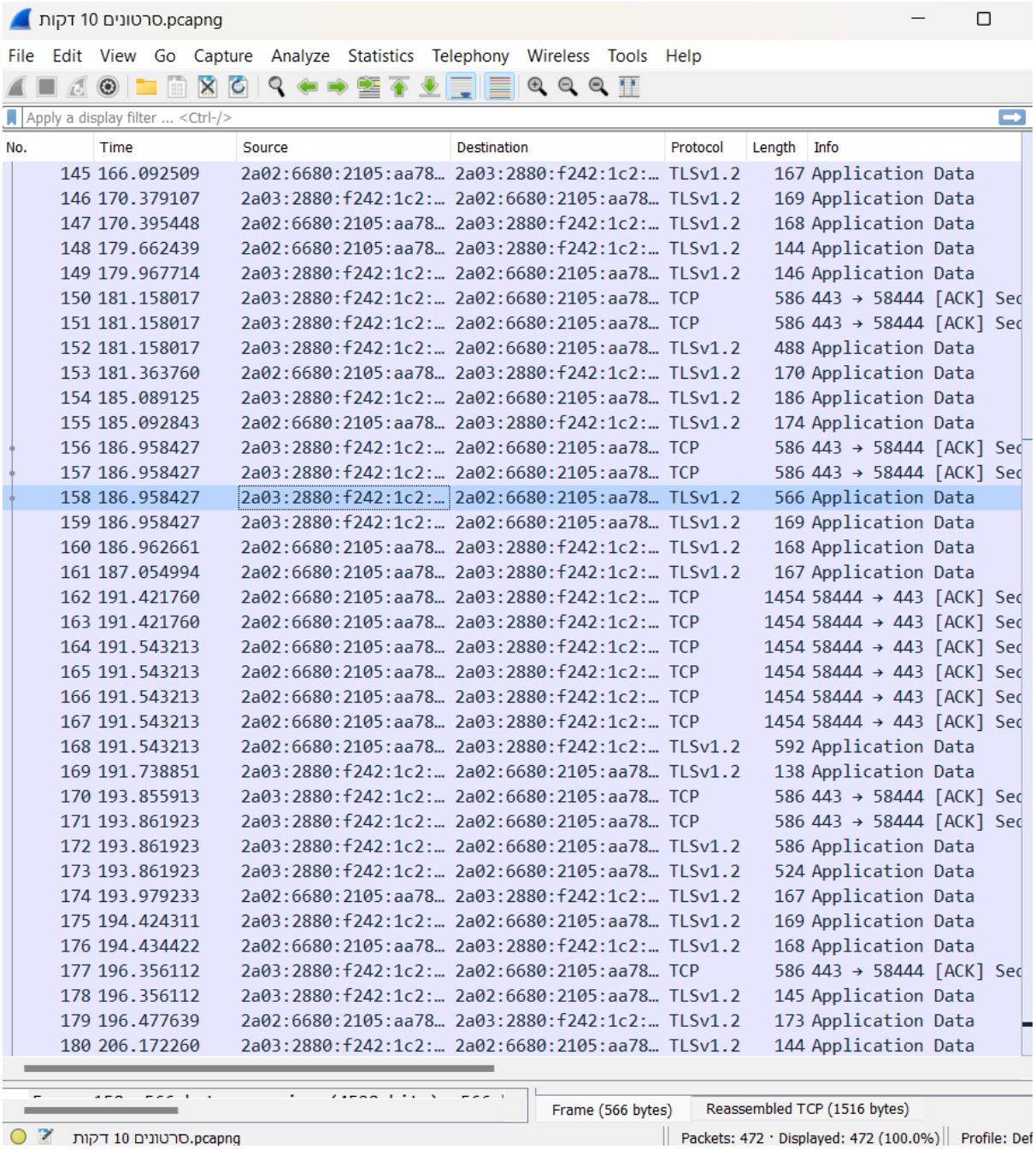


הגרף העליון: מייצג את מה שיצא מהמחשב שלנו אל שרתי ווצאפ. אולם אנחנו שלחנו את התמונות ממכשירים אחרים אל הקבוצה. לכן הוא לא משמעותי כרגע למעקב אחר שליחת תמונות

הגרף התחתון: מייצג מבחינתנו את התעבורה המרובה בסרטונים שנשלחה ועברה משרתי ווצאפ אל המחשב שלנו.



נבחן את הקלטת הווירשארק המתאימה :

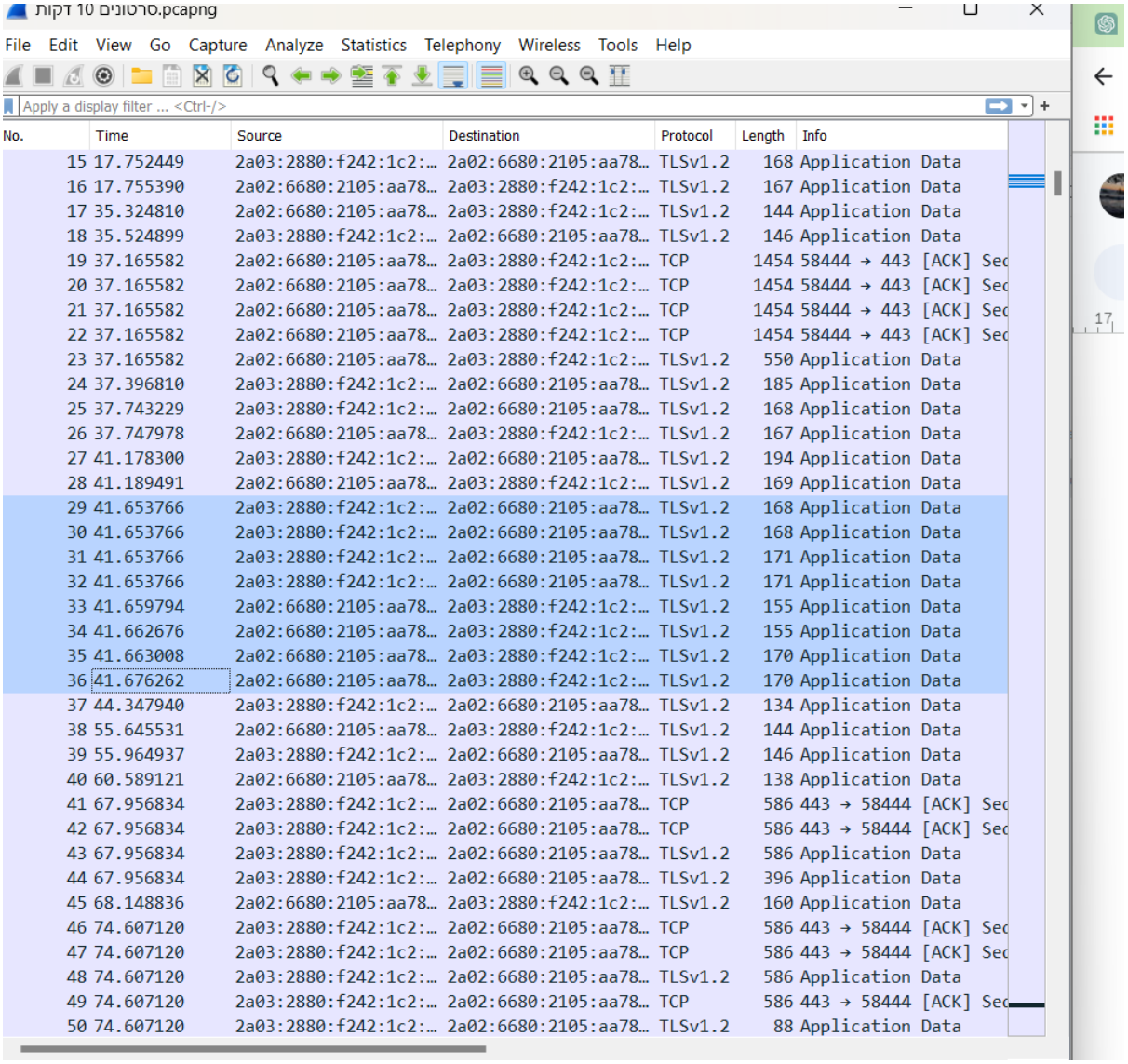


No.	Time	Source	Destination	Protocol	Length	Info
145	166.092509	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	167	Application Data
146	170.379107	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	169	Application Data
147	170.395448	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	168	Application Data
148	179.662439	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	144	Application Data
149	179.967714	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	146	Application Data
150	181.158017	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
151	181.158017	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
152	181.158017	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	488	Application Data
153	181.363760	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	170	Application Data
154	185.089125	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	186	Application Data
155	185.092843	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	174	Application Data
156	186.958427	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
157	186.958427	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
158	186.958427	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	566	Application Data
159	186.958427	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	169	Application Data
160	186.962661	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	168	Application Data
161	187.054994	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	167	Application Data
162	191.421760	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
163	191.421760	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
164	191.543213	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
165	191.543213	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
166	191.543213	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
167	191.543213	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
168	191.543213	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	592	Application Data
169	191.738851	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	138	Application Data
170	193.855913	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
171	193.861923	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
172	193.861923	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	586	Application Data
173	193.861923	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	524	Application Data
174	193.979233	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	167	Application Data
175	194.424311	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	169	Application Data
176	194.434422	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	168	Application Data
177	196.356112	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
178	196.356112	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	145	Application Data
179	196.477639	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	173	Application Data
180	206.172260	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	144	Application Data

ניתן לראות שהעמודות הגבוהות מציינות בכל פעם קבוצת פאקטות גדולות (הקוד מצוות פאקטות שנשלחות בהפרש זמן קטן מ0.1 שניות.)
למשל פאקטות 162-167 נמצאות בעמודה אחת בגרף העליון.
בנוסף ניתן להבחין שהפאקטות בסוג של רצף לאחר יצירת קשר ACK ובכל פעם הגודל של החבילות המחולקות משתנה...כנראה לפי גודל הסרטון.

למשל פאקטות 170-172 ככל הנראה מייצגות תחילת קשר ואחריו שליחת סרטון בחתיכות בגדלים 586 +524 אחכ נראה שינוי קל בזמנים ומעבר להודעה אחרת גם פאקטות 175 ו176 נראות משוייכות להודעה אחת , ייתכן וזהו לא סרטון אלא הודעה בגודל קטן יותר שהתפצלה לגדלים 168+169

רצף נוסף מעניין שמצאנו :

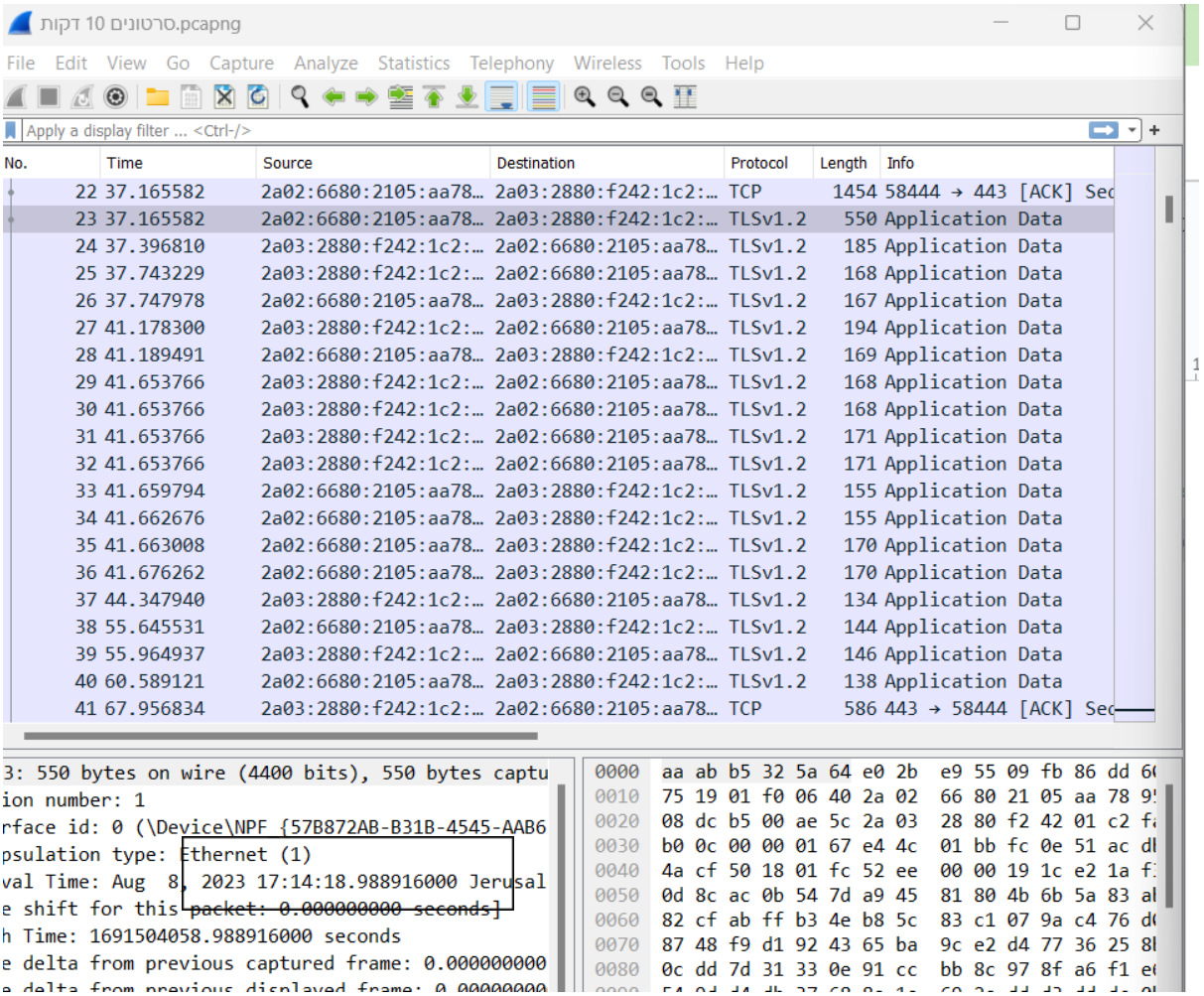


No.	Time	Source	Destination	Protocol	Length	Info
15	17.752449	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	168	Application Data
16	17.755390	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	167	Application Data
17	35.324810	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	144	Application Data
18	35.524899	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	146	Application Data
19	37.165582	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
20	37.165582	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
21	37.165582	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
22	37.165582	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TCP	1454	58444 → 443 [ACK] Sec
23	37.165582	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	550	Application Data
24	37.396810	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	185	Application Data
25	37.743229	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	168	Application Data
26	37.747978	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	167	Application Data
27	41.178300	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	194	Application Data
28	41.189491	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	169	Application Data
29	41.653766	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	168	Application Data
30	41.653766	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	168	Application Data
31	41.653766	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	171	Application Data
32	41.653766	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	171	Application Data
33	41.659794	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	155	Application Data
34	41.662676	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	155	Application Data
35	41.663008	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	170	Application Data
36	41.676262	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	170	Application Data
37	44.347940	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	134	Application Data
38	55.645531	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	144	Application Data
39	55.964937	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	146	Application Data
40	60.589121	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	138	Application Data
41	67.956834	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
42	67.956834	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
43	67.956834	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	586	Application Data
44	67.956834	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	396	Application Data
45	68.148836	2a02:6680:2105:aa78…	2a03:2880:f242:1c2:…	TLSv1.2	160	Application Data
46	74.607120	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
47	74.607120	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
48	74.607120	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	586	Application Data
49	74.607120	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TCP	586	443 → 58444 [ACK] Sec
50	74.607120	2a03:2880:f242:1c2:…	2a02:6680:2105:aa78…	TLSv1.2	88	Application Data

הרצף המסומן בכחול פאקטות 29-36 נראות כולן בהפרשי זמן ממש קטנים כאשר לפי המידע שבתוך הפאקטות הן שייכות לזמן : 17:14:23:

לפי המידע גם ראינו שהפאקטות שלפניהן ואחריהן שייכות כולם לדקה הזו , יתר על כן כל הפאקטות בין ACK בפאקטה 22 ועד הACK הבא בפאקטה 41 מהדקה הזו.

לכן נצרף צילום מסך חדש :

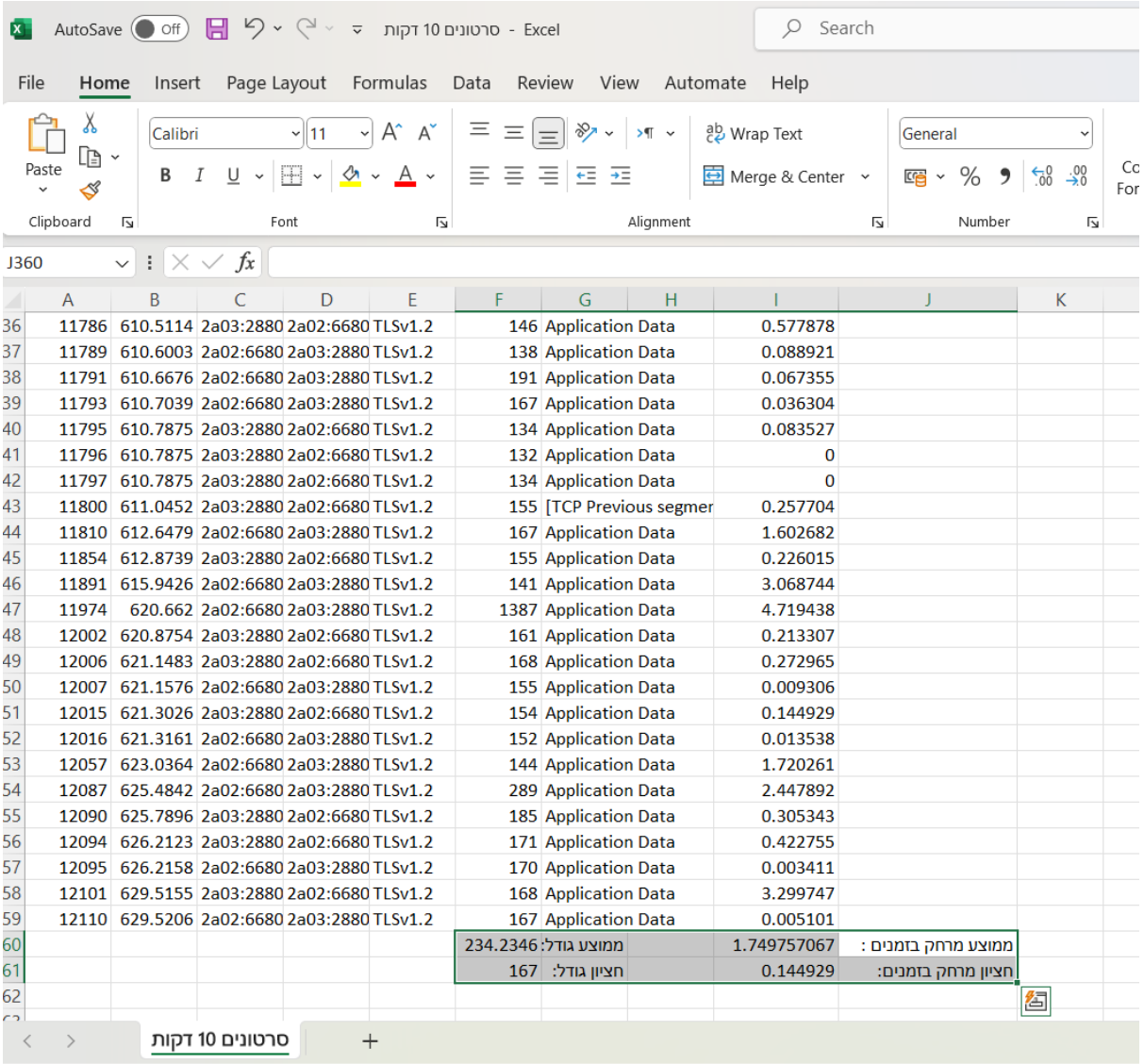


ואכן בקבוצת הווצאפ נשלחו שלושה סרטונים בדקה הזו שניים ממקור שלנו לשרת ווצאפ ואחד שהתקבל משרת ווצאפ אלינו.

היות ואנו לא מבחינות בוודאות בהבדל בין הסרטונים כי הפאקטות מעורבבות נסתפק בכך שרואים שהפאקטות מחולקות לחתיכות קטנות בגדלים 146-185 והראשונה שאחרי יצירת הקשר גדולה יותר (586)

אף על פי כן גם כאן כשביצענו ממוצע וחציון על גודל הפאקטות לא קיבלנו הבדל משמעותי בין ההאזנות כלומר הממוצע היה 234 והחציון - 167

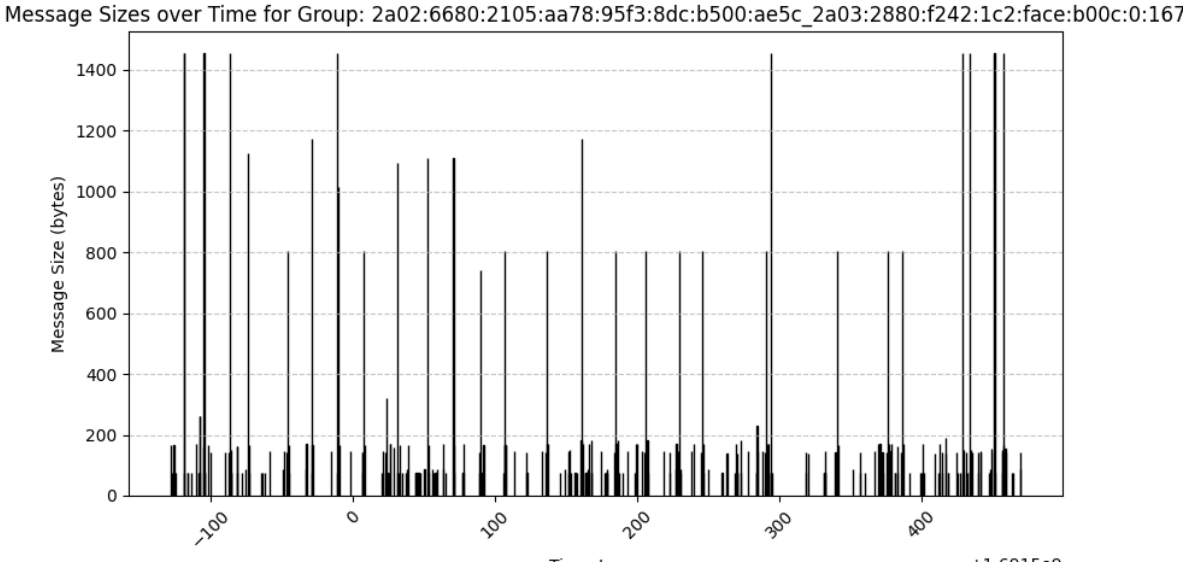
כאן הממוצע מרחק בזמנים גדל ל 1.749
ואילו החציון מרחק בזמנים הוא 0.144 - קטן יותר מהתמונות



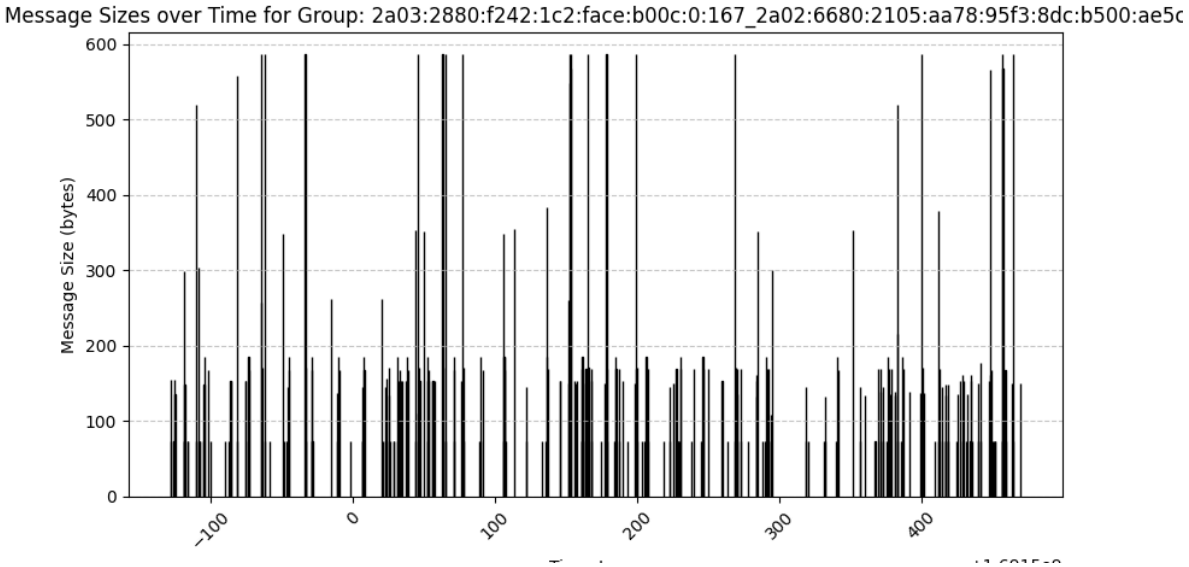
	A	B	C	D	E	F	G	H	I	J	K
36	11786	610.5114	2a03:2880	2a02:6680	TLSv1.2	146	Application Data		0.577878		
37	11789	610.6003	2a02:6680	2a03:2880	TLSv1.2	138	Application Data		0.088921		
38	11791	610.6676	2a02:6680	2a03:2880	TLSv1.2	191	Application Data		0.067355		
39	11793	610.7039	2a02:6680	2a03:2880	TLSv1.2	167	Application Data		0.036304		
40	11795	610.7875	2a03:2880	2a02:6680	TLSv1.2	134	Application Data		0.083527		
41	11796	610.7875	2a03:2880	2a02:6680	TLSv1.2	132	Application Data		0		
42	11797	610.7875	2a03:2880	2a02:6680	TLSv1.2	134	Application Data		0		
43	11800	611.0452	2a03:2880	2a02:6680	TLSv1.2	155	[TCP Previous segmer		0.257704		
44	11810	612.6479	2a02:6680	2a03:2880	TLSv1.2	167	Application Data		1.602682		
45	11854	612.8739	2a03:2880	2a02:6680	TLSv1.2	155	Application Data		0.226015		
46	11891	615.9426	2a02:6680	2a03:2880	TLSv1.2	141	Application Data		3.068744		
47	11974	620.662	2a02:6680	2a03:2880	TLSv1.2	1387	Application Data		4.719438		
48	12002	620.8754	2a03:2880	2a02:6680	TLSv1.2	161	Application Data		0.213307		
49	12006	621.1483	2a03:2880	2a02:6680	TLSv1.2	168	Application Data		0.272965		
50	12007	621.1576	2a02:6680	2a03:2880	TLSv1.2	155	Application Data		0.009306		
51	12015	621.3026	2a03:2880	2a02:6680	TLSv1.2	154	Application Data		0.144929		
52	12016	621.3161	2a02:6680	2a03:2880	TLSv1.2	152	Application Data		0.013538		
53	12057	623.0364	2a02:6680	2a03:2880	TLSv1.2	144	Application Data		1.720261		
54	12087	625.4842	2a02:6680	2a03:2880	TLSv1.2	289	Application Data		2.447892		
55	12090	625.7896	2a03:2880	2a02:6680	TLSv1.2	185	Application Data		0.305343		
56	12094	626.2123	2a03:2880	2a02:6680	TLSv1.2	171	Application Data		0.422755		
57	12095	626.2158	2a02:6680	2a03:2880	TLSv1.2	170	Application Data		0.003411		
58	12101	629.5155	2a03:2880	2a02:6680	TLSv1.2	168	Application Data		3.299747		
59	12110	629.5206	2a02:6680	2a03:2880	TLSv1.2	167	Application Data		0.005101		
60						234.2346	:ממוצע גודל		1.749757067	: ממוצע מרחק בזמנים	
61						167	:חציון גודל		0.144929	:חציון מרחק בזמנים	
62											

האזנה מספר 4 - הודעות קוליות:

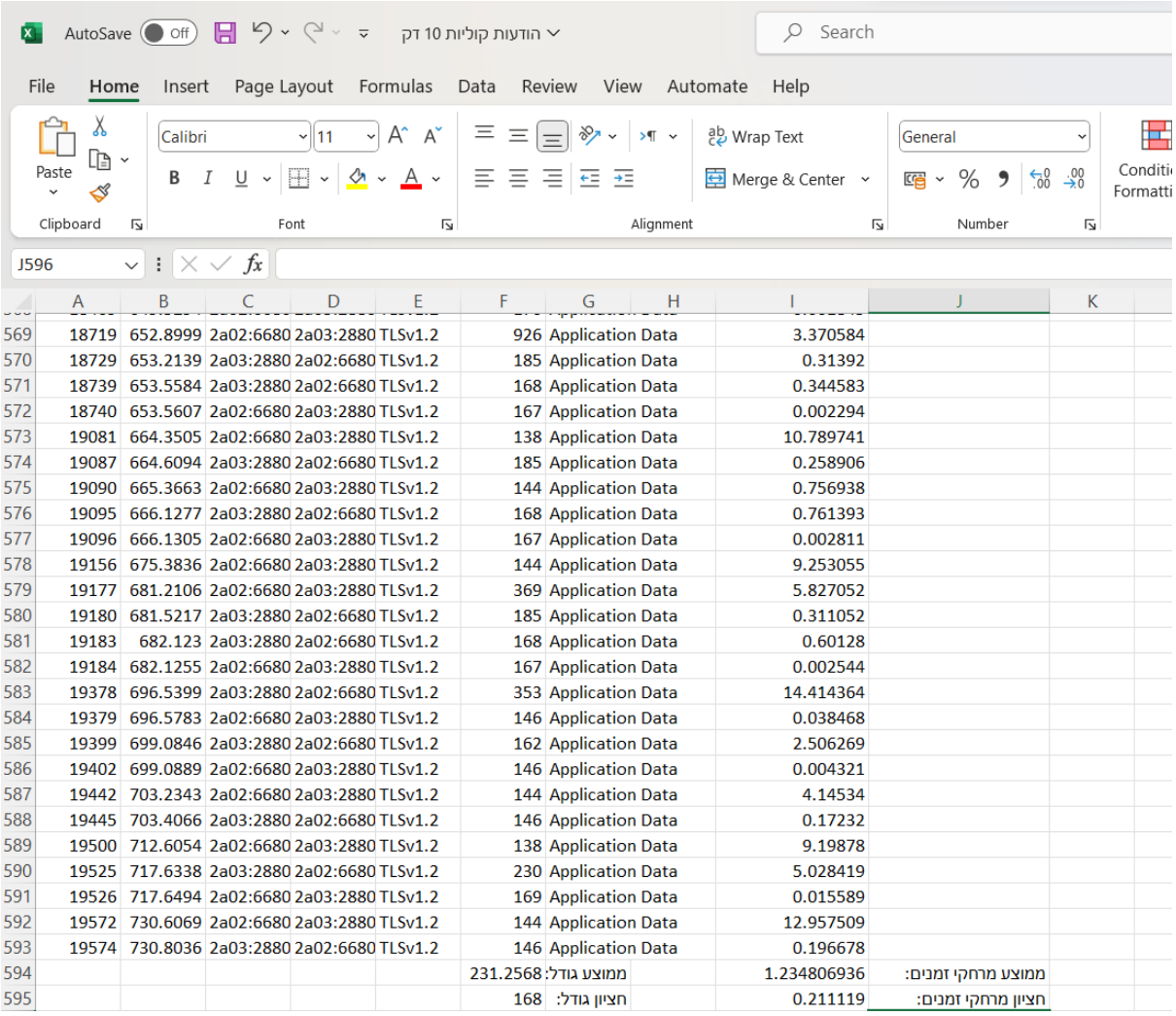
האזנו במשך 10 דקות להקלטות והודעות קוליות ואלו הגרפים :



הגרף העליון: מיצג את ההקלטות שנשלחו מהמכשיר שלנו אל שרתי ווצאפ.
הגרף התחתון : מייצג את התעבורה מרובת ההקלטות שנשלחה משרתי ווצאפ אלינו.



גם כאן לפי האקסל החציון הוא הודעה בגודל 168 בדומה לסרטונים ולתמונות
ההשערה שלנו כרגע היא שהשרת של ווצאפ מחלק את ההודעות לחתיכות בגודל הזה
כי ניתן להבחין ברצפים של הודעות בזמנים צפופים
נבחין בקובץ האקסל שבו אספנו את הפאקטות :



	A	B	C	D	E	F	G	H	I	J	K
569	18719	652.8999	2a02:6680	2a03:2880	TLSv1.2	926	Application Data		3.370584		
570	18729	653.2139	2a03:2880	2a02:6680	TLSv1.2	185	Application Data		0.31392		
571	18739	653.5584	2a03:2880	2a02:6680	TLSv1.2	168	Application Data		0.344583		
572	18740	653.5607	2a02:6680	2a03:2880	TLSv1.2	167	Application Data		0.002294		
573	19081	664.3505	2a02:6680	2a03:2880	TLSv1.2	138	Application Data		10.789741		
574	19087	664.6094	2a03:2880	2a02:6680	TLSv1.2	185	Application Data		0.258906		
575	19090	665.3663	2a02:6680	2a03:2880	TLSv1.2	144	Application Data		0.756938		
576	19095	666.1277	2a03:2880	2a02:6680	TLSv1.2	168	Application Data		0.761393		
577	19096	666.1305	2a02:6680	2a03:2880	TLSv1.2	167	Application Data		0.002811		
578	19156	675.3836	2a02:6680	2a03:2880	TLSv1.2	144	Application Data		9.253055		
579	19177	681.2106	2a02:6680	2a03:2880	TLSv1.2	369	Application Data		5.827052		
580	19180	681.5217	2a03:2880	2a02:6680	TLSv1.2	185	Application Data		0.311052		
581	19183	682.123	2a03:2880	2a02:6680	TLSv1.2	168	Application Data		0.60128		
582	19184	682.1255	2a02:6680	2a03:2880	TLSv1.2	167	Application Data		0.002544		
583	19378	696.5399	2a03:2880	2a02:6680	TLSv1.2	353	Application Data		14.414364		
584	19379	696.5783	2a02:6680	2a03:2880	TLSv1.2	146	Application Data		0.038468		
585	19399	699.0846	2a03:2880	2a02:6680	TLSv1.2	162	Application Data		2.506269		
586	19402	699.0889	2a02:6680	2a03:2880	TLSv1.2	146	Application Data		0.004321		
587	19442	703.2343	2a02:6680	2a03:2880	TLSv1.2	144	Application Data		4.14534		
588	19445	703.4066	2a03:2880	2a02:6680	TLSv1.2	146	Application Data		0.17232		
589	19500	712.6054	2a02:6680	2a03:2880	TLSv1.2	138	Application Data		9.19878		
590	19525	717.6338	2a03:2880	2a02:6680	TLSv1.2	230	Application Data		5.028419		
591	19526	717.6494	2a02:6680	2a03:2880	TLSv1.2	169	Application Data		0.015589		
592	19572	730.6069	2a02:6680	2a03:2880	TLSv1.2	144	Application Data		12.957509		
593	19574	730.8036	2a03:2880	2a02:6680	TLSv1.2	146	Application Data		0.196678		
594						231.2568	:ממוצע גודל		1.234806936	:ממוצע מרחקי זמנים	
595						168	:חציון גודל		0.211119	:חציון מרחקי זמנים	

כאן ממוצע מרחקי הזמנים בין הפאקטות היה 1.234

והחציון היה 0.2111- יותר גדול מהסרטונים והתמונות אבל יותר קטן מהודעות טקסט.

מסקנות המחקר :

מהאזנה לתעבורת הרשת עבור קבוצות ווטסאפ שונות ניתן להסיק מאפיינים ייחודיים לכל קבוצה. היקף פעילות בקבוצה, סוגי ההודעות הנשלחות בה ושינויי רמות פעילות לפי שעות.

האם ניתן להסיק את הקבוצות בהן אדם משתתף בעזרת הטכניקות המפורטות במאמר? כן. מהאזנה כזו אפשר לאמת גם השתתפות חשוד בקבוצה מסויימת ובדיקת היקף פעילות שלו בה, בהינתן גישה לתעבורת הרשת של החשוד ובהינתן מרגל מטעמנו בקבוצות הווטסאפ בהן אנחנו חושדים שהוא משתתף.

מטרתן של הטכניקות המפורטות במאמר :

- להצליח לזהות "אירועים" ע"י בחינה של צפיפות זמן שליחת הפאקטות ויכולת לצרף מספר פאקטות לכדי מסר אחד - אירוע אחד.
- להתחקות אחר מנהלים ומשתתפים בקבוצות, דרך מעקב והשוואת צורת התעבורה או צפיפות אירועים בין משתמש ספציפי לתעבורת הקבוצה.
- להתחקות אחר התעבורה המרכזית שמועברת בקבוצה.

אנחנו השתדלנו לבצע גרפים שיתארו לנו את תעבורת הקבוצה כמו שמתואר במאמר. וזו הכנה טובה לשימוש בשיטותיהם. כלומר הקוד שיצרנו קולט את הפאקטות שעוברות ברשת, ומחלק לפי תקשורת בין שרתים את הודעות. הוא מייצר גרף עבור כל ערוץ תקשורת ובתוכו מסווג פאקטות "קרובות מספיק" לכדי הבנה שזוהי "הודעה" אחת.

ע"מ להגיע למסקנות על מנהלים ומשתתפים פעילים בקבוצה נצטרך השוואה בין תעבורת החשודים בפעילות בקבוצה לגרפי התעבורה שיש לנו מהאזנה לקבוצה דרך המרגל שלנו. כדי להשיג תעבורה של משתמש ספציפי נצטרך אישור להאזנה כמו שציינו בסיכום המאמר למעלה, ורק אז נוכל להאזין לתקשורת פרטית של משתמש.

על מנת לאמת השתתפות (לא פעילה) בקבוצה נשווה בין תעבורת הרשת משרת הווטסאפ של החשוד אליו לבין התעבורה של הקבוצה שאנחנו בודקים. יכול להיות שהתעבורה שמגיעה אל החשוד תהיה רבה יותר, אם הוא מקבל הודעות גם מקבוצות נוספות, אך נתייחס לזה כאל רעש ונבדוק התאמה עם תעבורת הקבוצה המסוימת בגודל וזמני ההודעות.

על מנת לאמת השתתפות פעילה של החשוד בקבוצה נשווה בין תעבורת הרשת ממנו אל שרת הווטסאפ שלו (ההודעות הנשלחות ממנו) לבין התעבורה המתקבלת אצלנו מהקבוצה. נבצע הבחנה בין 2 מקרים:

1. המותקף פעיל לכל היותר בקבוצה אחת בפרק זמן של בדיקה -

אזי אפשר להיות בטוחים שהוא שולח הודעות לקבוצה אחת, ולכן אם נזהה התאמה של כל ההודעות לחלק מהתעבורה של הקבוצה אותה אנחנו בודקים אז נדע שאכן הוא פעיל בקבוצה הזאת ואף נוכל לסווג באחוזים את רמת הפעילות שלו ביחס לכל ההודעות שנשלחות בקבוצה.

2. המותקף פעיל בכמה קבוצות בפרק הזמן של הבדיקה -
אזי אי אפשר להיות בטוחים לאיזה קבוצה הוא שלח את ההודעה בכל פעם (בגלל ההצפנה של ווטסאפ), לכן לא נצפה שכל ההודעות שהוא שלח יתאימו להודעות שקיבלנו בתעבורת הקבוצה. נבדוק אילו הודעות כן מתאימות ואם נמצא שכן יש אחוז מסוים של הודעות שנשלחו על ידו ומתאימות בזמן ובגודל להודעות שהתקבלו בקבוצה אז הסיכוי גבוה שהוא כן פעיל בה.
דוגמה לבעייתיות של המצב - אם החשוד שלח הודעה בקבוצה אחרת, ובאותו זמן התקבלה הודעה בקבוצה הנבדקת אז זה עלול להיחשב כהתאמה, מה שאומר שהרעש מההודעות הנשלחות הלא רלוונטיות יעלה לנו את אחוז הטעות.
לכן צריך קודם כל לבצע את הבדיקה של ההשתתפות בקבוצה, ז"א לבדוק שתעבורת הקבוצה מוכלת בתעבורה הכללית בין שרת הווטסאפ לחשוד, ואז לבדוק את אחוז פעילות החשוד בקבוצה בידיעה שזהו אחוז הפעילות המירבי.

ניתן גם להתחקות אחר התעבורה המרכזית המועברת בקבוצה:
ע"מ להתחקות אחר סוג התעבורה בקבוצה , נצטרך להתבונן עמוקות בהקלטות התעבורה ולנסות לפענח האם צפיפות ההודעות מראה על קבצים גדולים מחולקים או על הודעות טקסט במרווחים שונים. (מה שהקוד שלנו מבצע.) ואפשר להשתמש בנתונים מהמאמר על מנת להסיק בהסתברות גבוהה אילו סוגי הודעות נשלחים בקבוצה.

אם כך, ראינו שטענת כותבי המאמר נכונה - הצפנת ההודעות של אפליקציות ההודעות המידיות לא מספיקה לחשאיות המשתמשים שלה, וגוף בעל יכולות יוכל בקלות לעקוב אחרי משתמשים וקבוצות ולקבל הרבה מידע מהאזנה לתעבורת הרשת המוצפנת. לכן על מנת לאפשר למשתמשים שלהן פרטיות מירבית הן בהחלט צריכות להשתמש בכלים שיפחיתו את שקיפות התעבורה, כפי שמוצע במאמר.