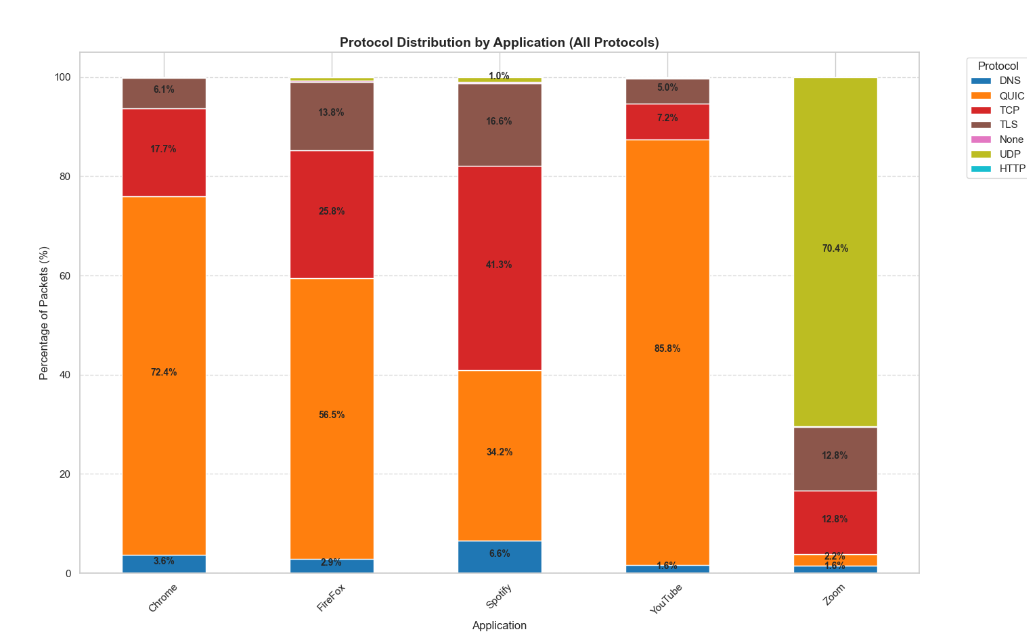
יום שלישי 04 מרץ 2025

19:24

חלק 3 ניתוח הגרפים:

**PROTOCOLS GRAPH**



הגרף מציג את התפלגות הפרוטוקולים בכל אפליקציה. ניתן לראות כי TCP ו-QUIC הם הדומיננטיים ברוב האפליקציות, למעט Zoom, שבו UDP הוא הפרוטוקול המרכזי (70.4%) בשל הצורך בהעברת מידע במהירות וללא עיכובים.

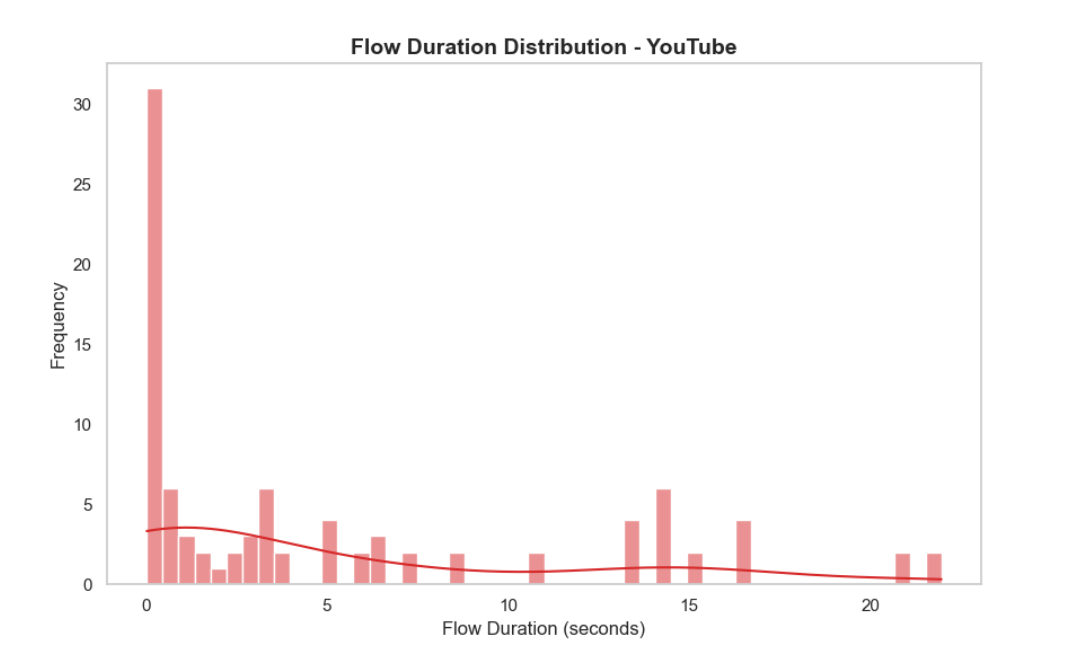
Chrome, Firefox, Spotify, ו-YouTube מסתמכות בעיקר על TCP ו-QUIC, כיוון שהן פועלות בעיקר בדפדפן, שם נדרשת תקשורת אמינה ומסודרת.

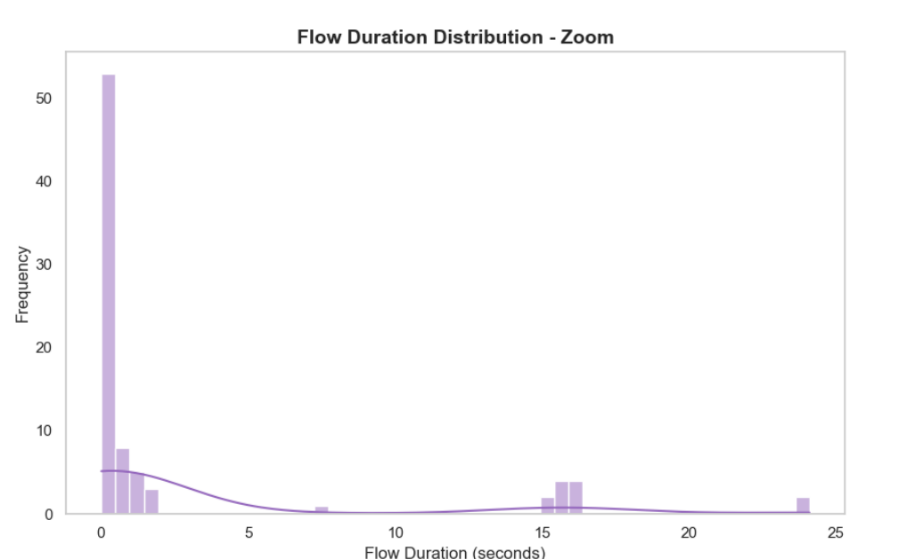
QUIC בולט במיוחד ב-Chrome וב-YouTube, שכן מדובר בפרוטוקול מודרני של גוגל המשפר ביצועים, במיוחד בהזרמת וידאו.

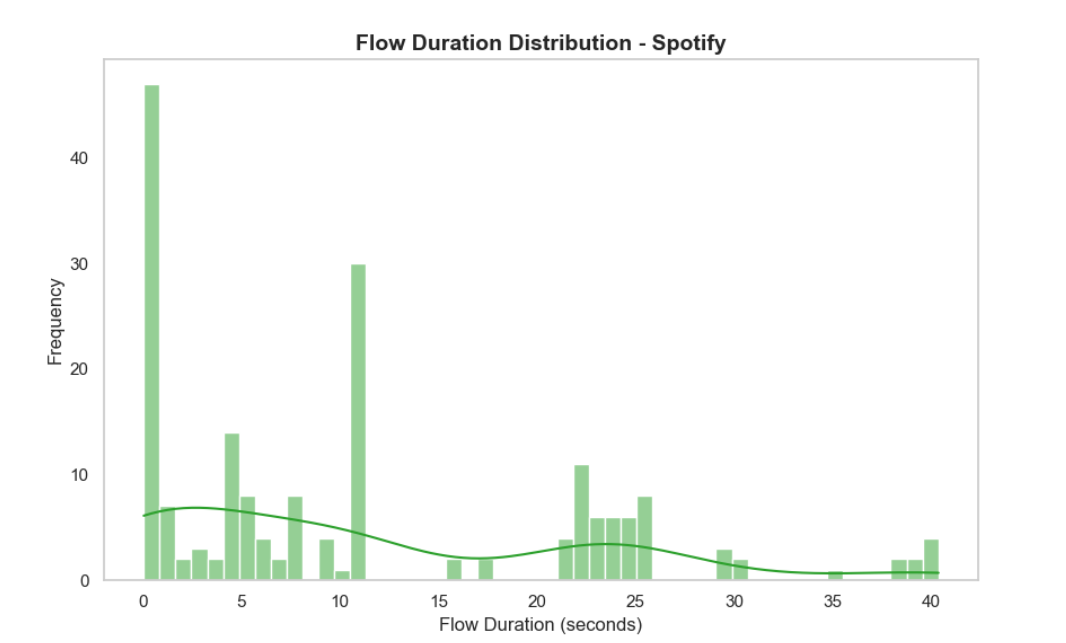
Zoom משתמש בעיקר ב-UDP (ולא ב-TCP), מכיוון שפרוטוקול זה מקטין השהיות ומאפשר שיחות וידאו ושמע בזמן אמת.

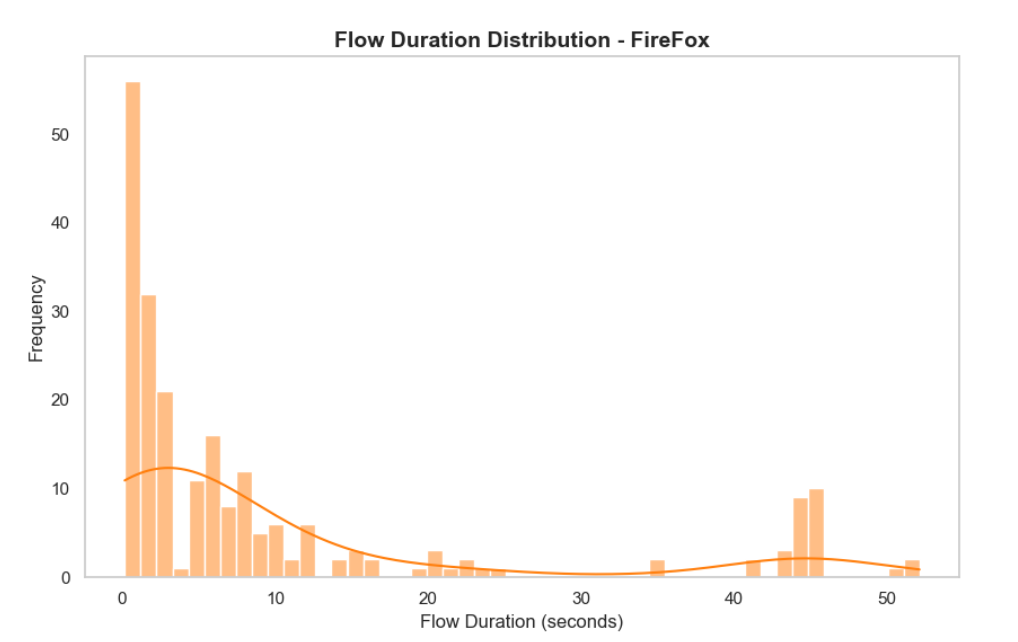
ההבדלים בפרוטוקולים משקפים את הצרכים הייחודיים של כל אפליקציה – אמינות מול מהירות תגובה.

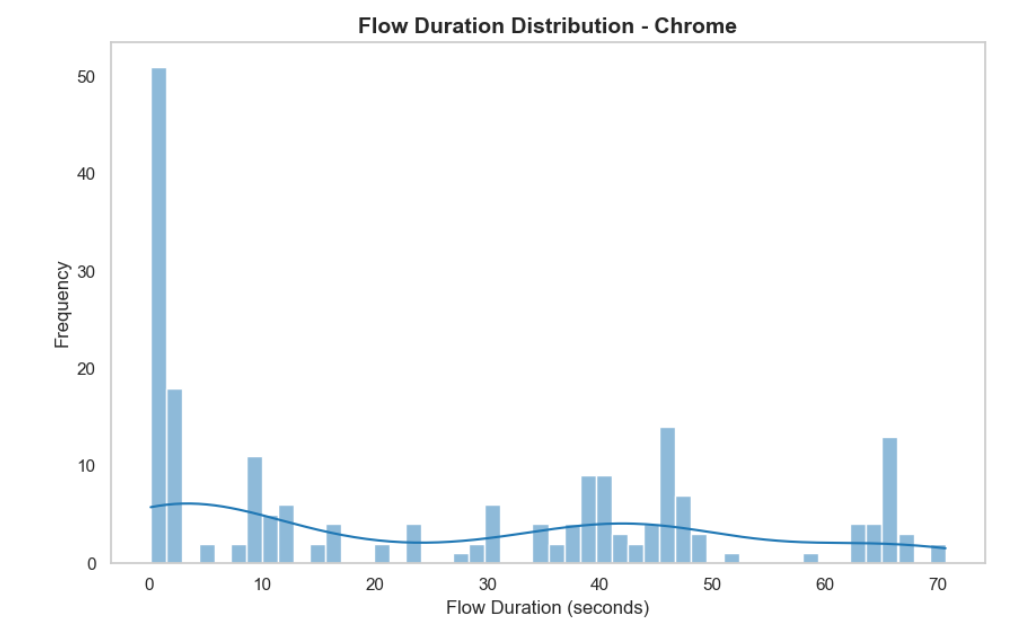
**Flow Lengths Graphs**











זרימה (Flow) מוגדרת כרצף של חבילות ברשת החולקות 5 מאפיינים ייחודיים (5-Tuple):  
  
1 כתובת Source IP – כתובת השולח

2כתובת Destination IP – כתובת המקבל

3 פורט מקור – מספר הפורט של השולח

4 פורט יעד – מספר הפורט של המקבל

5 פרוטוקול – למשל TCP, UDP

זמני ניתוק (Timeouts)

* Active Timeout: אם חיבור נמשך זמן רב, הוא מחולק למקטעים (למשל, כל 5 דקות).
* Inactive Timeout: אם אין חבילות חדשות למשך זמן מסוים (למשל, 30 שניות), הזרימה נסגרת.

כיצד מזהים סיום זרימה?

* ב-TCP: החיבור נסגר באופן יזום ע"י FIN/ACK או RST
* ב-UDP: הזרימה נסגרת כאשר אין תעבורה לזמן מסוים (Timeout)

**השוואת אופן הזרימה ב-YouTube וב-Spotify**

* YouTube מבצע buffering, שבו קטעי וידאו נטענים מראש כדי למנוע השהיות.
* Spotify משתמש בהזרמה רציפה במקום טעינה מוקדמת, כיוון שהעברת אודיו דורשת רוחב פס קטן יותר מווידאו.  
   כתוצאה מכך:

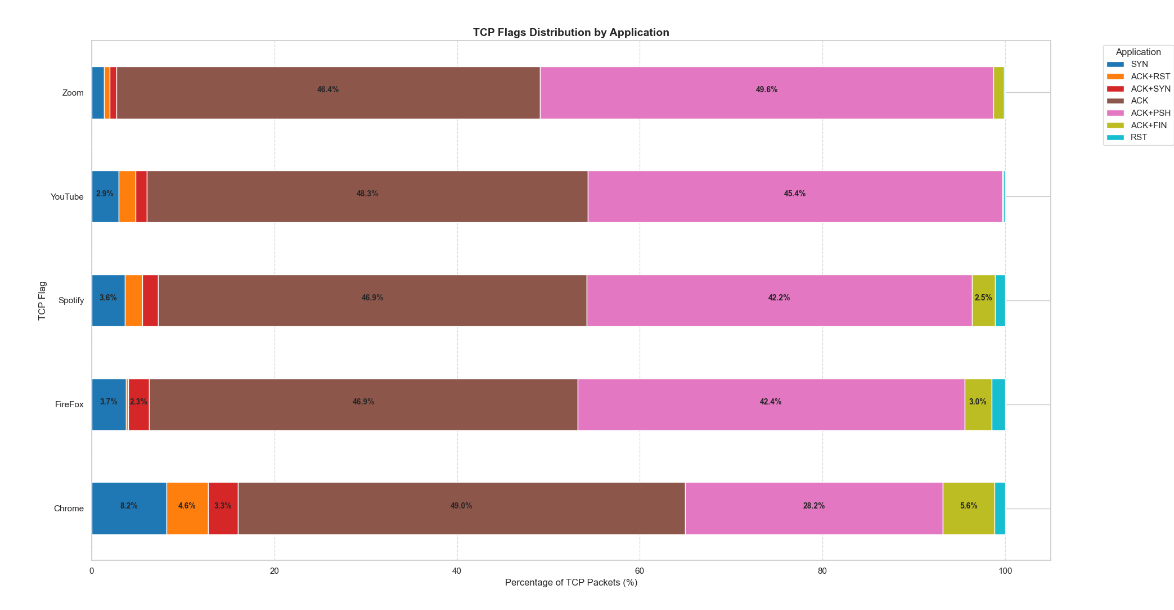
ביוטיוב – רוב החיבורים קצרים ולא רציפים.

בספוטיפיי – החיבורים ארוכים ומתרחשים בקפיצות חדות.

**השוואה מול שאר האפליקציות**

רוב היישומים דומים ליוטיוב מבחינת מבנה החיבורים: חיבורים קצרים ולא רציפים.  
 Zoom וגלישה בדפדפנים כמו CHROME ו FIREFOX נשענים על חבילות מידע קטנות (bite-size data), ולא על הזרמת מדיה כבדה. לכן, משך הזרימה קצר יותר משמעותית בהשוואה ל-YouTube ו-Spotify.

**TCP FLAGS**



הגרף מציג את ההתפלגות של דגלי TCP.   
. כל צבע מייצג דגל שונה, כולל SYN, ACK, PSH, FIN, RST ודגלים משולבים כמו ACK+PSH.  
  
 ניתן לראות כי Zoom, YouTube ו-Spotify מציגים דפוסים דומים, עם רוב החבילות הנושאות את הדגלים ACK ו-ACK+PSH, דבר שמצביע על תקשורת זורמת של נתונים  
  
 ב-Zoom יש מעט חבילות SYN ורובן המכריע מסווגות כ-ACK+PSH, מה שמעיד על זרימה מתמשכת של נתונים ללא יצירת חיבורים חדשים רבים. ב-YouTube ההתפלגות דומה אך עם מעט יותר חבילות SYN, מה שמעיד על הקמת חיבורים חדשה לעיתים.  
  
 Spotify דומה מאוד במבנה, אך מכיל פחות ACK+PSH בהשוואה לYouTube.

FireFox ו-Chrome, לעומת זאת, מציגים יותר חבילות SYN ו-RST, מה שמעיד על פתיחה וסגירה תכופה של חיבורים, דבר שמאפיין גלישה באינטרנט שבה נטענים דפים רבים בזמן קצר. ב-Chrome ניתן לראות אחוז גבוה יחסית של חבילות FIN ו-RST, דבר המעיד על ניתוקי חיבורים תכופים וסיום חיבורים יזום על ידי הדפדפן. Firefox דומה בהתנהגותו אך מציג מעט פחות חבילות RST בהשוואה ל-Chrome.  
  
 הגרף מדגים כיצד ניתן לזהות שימוש ביישומים שונים לפי דפוסי דגלי ה-TCP שלהם, כאשר סטרימינג ושיחות וידאו מאופיינים בזרימה קבועה של חבילות ACK+PSH, ואילו דפדפנים מציגים יותר חבילות SYN, FIN ו-RST.