

## GOOGLE MEETS

נתבונן בגרפים בעמודים הבאים ונסביר איך נוכל לדעת שנעשה שימוש בשיחת וידאו ובפרט google meets.

1. לפי הגרף של כתובות ה־ip נוכל לראות לראות שנעשה שימוש נרחב בכתובת 18::2001:4860:4864:6:4000 נשים לב שכתובת זו נמצאת בטווח שמוקצה על ידי גוגל. בעזרת מאגר נתונים גדול מספיק (או לחלופין פקודת "whois" בטרמינל) נוכל לתת כיוון לשימוש בתעבורת הרשת על בסיס כתובות ip ששומשו באופן תדיר.
2. לפי התפלגות זמני ההגעה נוכל לראות שכמעט כל המידע עבר בהפרש של פחות מ 20ms מה שמכניס אותנו לקטגוריה של "voip".  
לכן מספר האפשרויות לשימוש שנעשה מצטמצם משמעותית.
3. לפי התפלגות גדלי החבילות נוכל לראות משהו מעניין, חלק מגדלי החבילות הם יחסית גדולות מה שמסמל על שירותי וידאו (1000-1300) וחלק אחר הרבה יותר קטן מה מה שמסמל על שירות של שיחה קולית.  
הסיבה שאנחנו רואים את ההתפלגות הזאת היא כי צד אחד השתמש וידאו וגם קול וצד שני רק בקול.
4. הגרף שמסמל את התפלגות ה־ip נותן לנו אינדיקציה פחות חזקה משאר הגרפים שהוזכרו למעלה, אבל עדיין יכול לספק לנו רמזים לגבי השימוש בתעבורת הרשת, לדוגמה: משחקים מקוונים יעדיפו שימוש ב־ip4, לעומת שירותים מודרניים שיעדיפו שימוש ב־ip6 (לדוגמה; AWS, Google).  
הבחירה ב־ip6 לא מפתיעה אותנו מכיוון ש־google "מעודדת" שימוש בפרוטוקול זה במידה והוא זמין, לכן נוכל לקבל עוד אינדיקציה שאנחנו משתמשים בשירות מודרני כמו google meets
5. בגרף התפלגות הפורטים נוכל לראות שימוש מאוד נפוץ ב: פורט 3478 - פורט שממשש ל־WebRTC Voip, עוד אינדיקציה שמדובר בשיחת וידאו פורט 61319 - פורט דינאמי שהרבה פעמים משמש אותנו בתקשורת בשיחות וידאו ולמרות שישנם עוד אפשרויות עם נתחשב במכלול הנתונים נוכל לסמן את google meets כשוד העיקרי
6. גרף upstream/downstream: יחס דומה בין ה־upstream ל־downstream יכול לרמוז לנו על שיחה קולית/ שיחת וידאו (צד אחד יהיה גדול מהשני אם צד אחד השתמש בוידאו והצד השני רק בקול).

לסיכום: כלל הנתונים מצביעים שנעשה שימוש בתעבורת רשת לצורך שיחת וידאו.  
דרך הגרף של ה־ip נוכל לדעת שהשירות נעשה על ידי גוגל ולכן נעשה שימוש ב־google meets.

## Spotify

ניתן לזהות שמדובר בפקטות של **Spotify** על סמך הנתונים המוצגים בגרפים השונים באופן הבא:

כתובות IP – ניתן לבדוק האם כתובות ה-IP שבגרף משויכות לטווח הכתובות של Spotify על ידי שימוש בפקודת whois או במאגרי נתונים חיצוניים.

זמני הגעה (Latency Distribution) – אם רוב זמני ההגעה קצרים (פחות מ-20ms), זה יכול להעיד על שירות סטרימינג מבוסס CDN, כמו Spotify.

התפלגות גדלי החבילות (Packet Size Distribution) – בשירותי סטרימינג אודיו כמו Spotify, רוב החבילות נוטות להיות קטנות (בניגוד לשירותי וידאו כמו YouTube או Google Meets, שם החבילות גדולות יותר).

התפלגות כתובות IP (IP Distribution) – אם נראה שהתעבורה מופנית לכתובות שמקושרות לשירותי Spotify (לדוגמה, שרתים של AWS או Google Cloud שבהם Spotify מאחסנים את השירותים שלהם), זה מהווה אינדיקציה נוספת.

התפלגות הפורטים (Port Distribution) – Spotify משתמשת בפורטים ספציפיים לסטרימינג אודיו (למשל, TCP 4070 או שימוש בפרוטוקולים כמו QUIC). אם נתוני הגרף מציגים שימוש באותם פורטים, זה יכול להעיד על כך שהתעבורה שייכת ל-Spotify.

Upstream/Downstream on – בשירותי סטרימינג כמו Spotify, היחס בין downstream ל-upstream יהיה גבוה, כי רוב הנתונים מורדים מהשרתים למשתמשים (הזרמת שירים) ורק מעט מידע נשלח חזרה (שליחת פקודות שליטה כמו ניגון, דילוג וכו').

בהשוואה לנתונים שמוצגים עבור Google Meets, ההבדלים העיקריים יהיו בעיקר בגודל החבילות, הפורטים בהם נעשה שימוש, והיחס בין הזרימה הנכנסת והיוצאת.

## edge

נתבון בגרפים הבאים וננתח את תעבורת הדפדפן Edge:

1. **כתובות IP** מגרף כתובות ה-IP ניכר שעיקר התעבורה מופנה לכתובות השייכות לבלוקים שהוקצו ל-Microsoft. כתובות אלו מעידות על גישה למערך שרתי מיקרוסופט, אשר אחראים על הפצת עדכונים, תכנים ושירותים נוספים הקשורים ל-Edge. שימוש עקבי בכתובות מסוג זה מעיד על שילוב הדוק בין הדפדפן לבין מיקרוסופט, ומאפשר בידול לעומת דפדפנים אחרים.
2. **זמני הגעה (Latency Distribution)** מניתוח זמני ההגעה ניתן לראות שכבר חלק ניכר מהבקשות נקלטות בטווח של 30–100 מיליסקנד. טווח זה מצביע על פעילות של גלישה רגילה, בה זמני התגובה אינם קריטיים כמו בתקשורת בזמן אמת, אלא מספיק מהירים לביצוע הורדות, טעינת דפים ועיבוד בקשות דינמיות. הערכים הללו משקפים פעילות גלישה אינטרנטית שגרתית.
3. **התפלגות גודל חבילות (Packet Size Distribution)** בנוגע לגודל החבילות, ניכר ששווי המשקל מוטה לעבר חבילות קטנות שמאפיינות את העברת בקשות HTTP, ACKs, עיבוד נתונים שונים ותמונות. יחד עם זאת, מופיעות גם חבילות גדולות יותר, בגודל של עד 1500 בתים, המייצגות העברת מידע כבד יותר בעת הורדת דפי אינטרנט ותוכן מולטימדיה. תבנית זו מייצגת את דפוסי הגלישה הרגילים של דפדפן מודרני, שם ההבדלים בגודל החבילות תלויים בסוג הנתונים המועברים.
4. **התפלגות כתובות (IP Distribution)** התפלגות ה-IP בדפדפן Edge הגרף שמסמל את התפלגות ה-IP נותן לנו אינדיקציה פחות חזקה משאר הגרפים שהוזכרו למעלה, אך עדיין יכול לספק לנו רמזים לגבי השימוש בתעבורת הרשת. לדוגמה, משחקים מקוונים יעדיפו שימוש ב-IPv4, לעומת שירותים מודרניים שיעדיפו שימוש ב-IPv6 (כגון AWS ו-Google). במקרה של דפדפן Edge, ראינו נטייה ברורה יותר לשימוש ב-IPv4. ייתכן שהדבר נובע מהגדרות הרשת המקומיות, מהתמיכה של שרתי היעד בפרוטוקולים השונים או מהאופן שבו מיקרוסופט מנהלת חיבורים בדפדפן שלה. בניגוד לשירותים כמו Google, אשר "מעודדים" שימוש ב-IPv6 כאשר הוא זמין, ייתכן כי Edge מעדיף חיבור יציב יותר דרך IPv4 במקרים מסוימים.
5. **שימוש בפרוטוקולים ופורטים (Port & Protocol Distribution)** ניתוח גרף הפורטים מציג פעילות שמאופיינת בשימוש בפרוטוקולי HTTP ו-HTTPS (פורטים 80 ו-443) – התקשורת הסטנדרטית הנדרשת לביצוע גלישה. עדיין קיימת עדות לשימוש אפשרי בפרוטוקולים מבוססי UDP (כגון QUIC) אשר מעידים על אופטימיזציה נוספת להעברת נתונים, אולם למאורע העיקרי יש את התמיכה הבסיסית בדפדפן Edge של גלישה רגילה ולא שירות תקשורת בזמן אמת.
6. **Upstream/Downstream on** ניתוח התצוגה של יחס העלייה להורדה מצביע על העדפה מובהקת להורדת נתונים – מאפיין אופייני לתעבורת גלישה. המשתמשים בביצוע גלישה בדפדפן Edge נוטים לקבל את רוב הנתונים מהשרתים (כגון תוכן דפי אינטרנט, תמונות וסקריפטים) ונשלחים רק בקשות ותעודות סטטוס, מה שמוביל לאסימטריה ברורה בין כמות הנתונים היורדת לזו העולה.

**לסיכום:** כלל הנתונים הללו מצביעים על תעבורה המיועדת לשימוש בדפדפן Edge – פעולה המתאפיינת בגלישה אינטרנטית שגרתית, העברת תוכן מאובטח ועדכונים באופן מהיר, ושימוש עקבי בשירותי Microsoft. תבניות הזמן, גודל החבילות, התפלגות כתובות ה-IP והשימוש בפרוטוקולים ופורטים, כולם מצביעים על פעילות של הורדת תכנים לצד בקשות מתוזמנות, אשר יחד מספקות חווית גלישה חלקה ויעילה.

# YOUTUBE

נתבונן בגרפים הבאים וננתח את תעבורת YouTube

## כתובות IP

מגרף כתובות ה-IP ניתן לראות שהתעבורה של YouTube מופנית בעיקר לכתובות IP השייכות לבלוקים של Google, שכן YouTube הוא בבעלות Google. גישה מרובה לכתובות אלו מעידה על חיבורים ישירים לשרתי YouTube המספקים וידאו, פרסומות ושירותים נוספים כגון אחסון מטמון (CDN) להאצת טעינת התוכן.

## זמני הגעה (Latency Distribution)

מהגרף ניתן להסיק שרוב הבקשות נענות בטווח זמן ממוצע של עשרות עד מאות מילי-שניות. זמני הגעה אלו אופייניים לשירותי הזרמת וידאו, בהם נדרש איזון בין חוויית משתמש חלקה לבין אופטימיזציה של טעינת נתונים. עיכובים גבוהים יותר יכולים להעיד על עומס רשת או מרחק גיאוגרפי משרת ה-CDN הקרוב ביותר.

## התפלגות גודל חבילות (Packet Size Distribution)

הגרף מציג שילוב של חבילות קטנות וגדולות. החבילות הקטנות משמשות לבקרת חיבורי TCP ו-UDP, לשליחת בקשות HTTP ולתיאום זרימת הנתונים. החבילות הגדולות (קרובות ל-1500 בתים) משמשות להעברת קטעי וידאו מקודדים, במיוחד בעת הפעלה ברזולוציות גבוהות. צפייה בתוכן יוצרת נוכחות מוגברת של חבילות גדולות, בעוד פעולות כמו חיפוש סרטונים והעלאת תגובות יובילו לחבילות קטנות יותר.

## התפלגות כתובות (IP Distribution)

התפלגות כתובות ה-IP מצביעה על שימוש משמעותי במערך שרתי YouTube, כאשר ייתכן שימוש גם ב-IPv6, בהתאם למדיניות ניתוב הרשת של Google. ריבוי הכתובות מצביע על עבודה עם רשתות CDNs, שמטרתן לאפשר הפצת וידאו בצורה יעילה תוך מזעור עומסי רשת והשהיות.

## שימוש בפרוטוקולים ופורטים (Port & Protocol Distribution)

הגרף מעיד על שימוש רחב בפרוטוקולים TCP ו-UDP. פרוטוקול QUIC, שמבוסס על UDP, משחק תפקיד מרכזי בזרימה החלקה של וידאו ב-YouTube, במיוחד על גבי HTTPS (פורט 443). שימוש זה משפר את זמני טעינת הווידאו על ידי הפחתת ההשהיות הנגרמות על ידי TCP.

## Upstream/Downstream on

יחס ההורדה (Downstream) גבוה באופן משמעותי מהעלאה (Upstream), דבר אופייני לפלטפורמות הזרמת וידאו. רוב התעבורה מופנית להורדת קטעי וידאו, בעוד שהעלאה מצומצמת יותר ומשמשת בעיקר למשלוח פקודות שליטה (כגון הפעלה, דילוג קדימה, שינוי רזולוציה) או העלאת תוכן חדש.

## סיכום

התבנית של תעבורת הרשת מעידה בבירור על פעילות צפייה ב-YouTube: העברת וידאו בקצבים גבוהים, שימוש בפרוטוקולים אופטימליים להזרמה, וגישה לרשתות CDN מבוזרות של Google. יחס הנתונים, זמני ההגעה והגודל המשתנה של החבילות משקפים אופטימיזציה של רשת להפעלת וידאו חלקה תוך הפחתת השהיות.

## chrome

### כתובות IP

הגרף מציג את כתובות ה-IP אליהן התעבורה של הדפדפן מופנית. ניתן לראות שמרבית הכתובות שייכות לטווחים המוקצים לשרתי Google, דבר המעיד על השימוש הנרחב בשירותי החברה לצורך טעינת דפי אינטרנט, אחסון נתונים, ועדכון רכיבי הדפדפן. בנוסף, ניתן לזהות גישה אל שרתי צד שלישי, כגון ספקי תוכן ואחסון CDN, אשר מספקים רכיבים נוספים כמו תמונות, סקריפטים, ופרסומות.

### זמני הגעה (Latency Distribution)

מהגרף ניתן להבחין כי זמני ההגעה של מרבית הבקשות נופלים בטווח של 30–100 מילי-שניות, מה שמעיד על ביצועי תקשורת יציבים ותגובה מהירה בטעינת אתרים. זמני הגעה קצרים במיוחד נצפו בבקשות לשרתי Google ו-CDN קרובים, בעוד שבקשות לשירותים מרוחקים מציגות עיכובים גדולים יותר, בהתאם לעומס הרשת ולמרחק הגיאוגרפי.

### התפלגות גודל חבילות (Packet Size Distribution)

בגרף ניתן לראות שתי מגמות בולטות: חבילות קטנות המשמשות לשליחת בקשות HTTP ולתיאום התקשורת, לצד חבילות גדולות המיועדות להורדת נתונים משמעותיים כמו קובצי HTML, תמונות, וסרטונים. גודל החבילות משתנה בהתאם לתוכן הדף ולמנגנוני הדחיסה בהם נעשה שימוש לצורך אופטימיזציה של התעבורה.

### התפלגות כתובות (IP Distribution)

התפלגות ה-IP משקפת את הדומיננטיות של Google בתעבורת הדפדפן, לצד גישה לשירותים חיצוניים. ניתן לראות העדפה ברורה לשימוש בפרוטוקול IPv6 בחלק מהבקשות, בעיקר לשירותים מודרניים המאפשרים תאימות לשיטה זו, בעוד שבקשות אחרות נשענות על IPv4 בהתאם להגדרות הרשת ולתמיכת השרתים.

### שימוש בפרוטוקולים ופורטים (Port & Protocol Distribution)

הגרף מציג שימוש אינטנסיבי בפרוטוקולי HTTP (פורט 80) ו-HTTPS (פורט 443), כאשר HTTPS הוא הדומיננטי ביותר, דבר התואם את מגמות האבטחה המודרניות. ניתן לראות גם עדויות לשימוש בפרוטוקול QUIC המבוסס על UDP, המאפשר שיפור ביצועים בהזרמת תוכן והפחתת השהיות, במיוחד בפרסומות כגון Google Drive ו-YouTube.

### Upstream/Downstream on

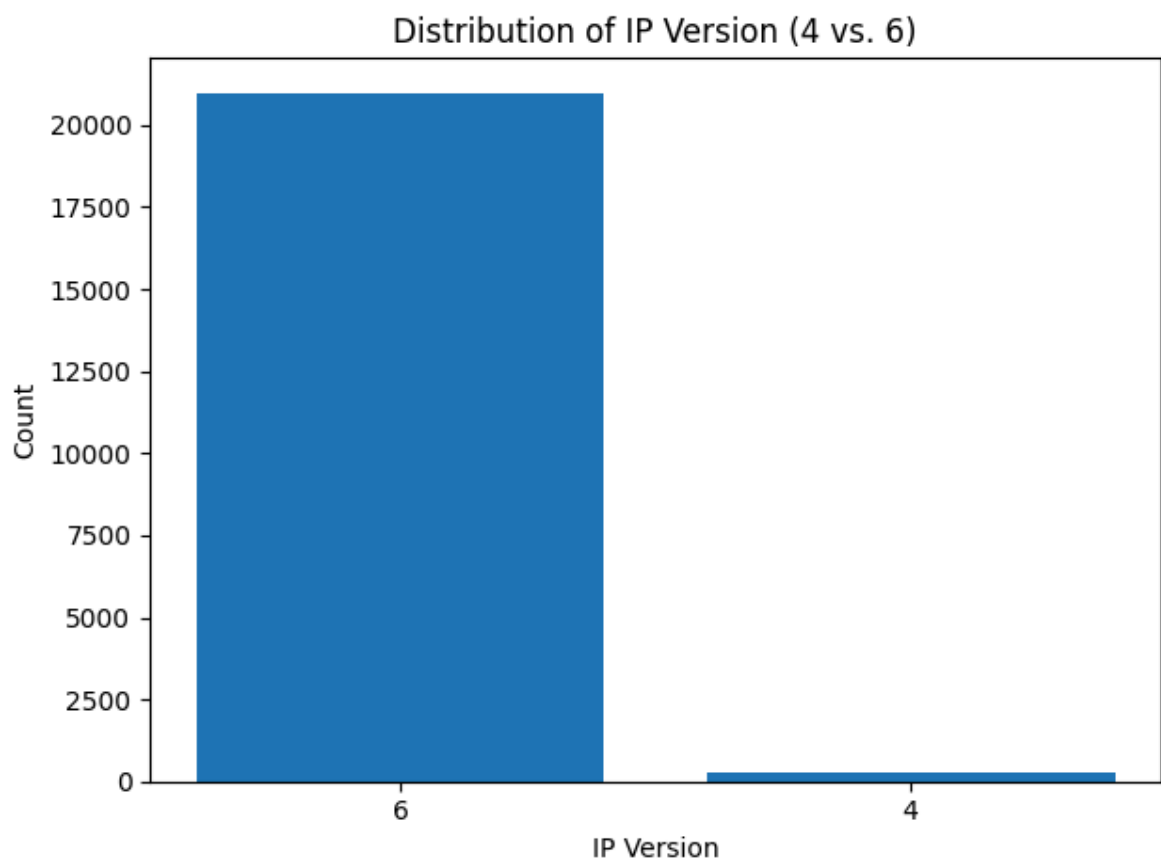
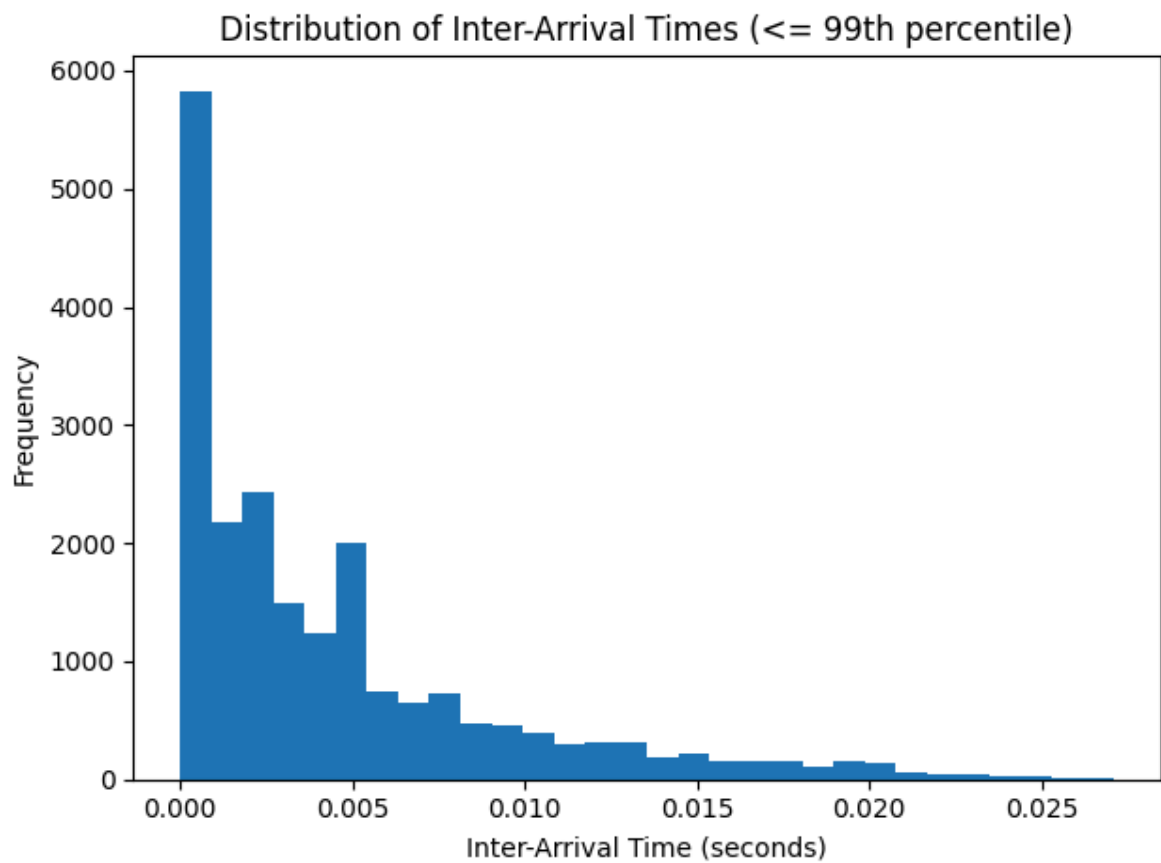
יחס ההורדה להעלאה (Downstream/Upstream) מצביע על כך שרוב תעבורת הדפדפן מורכבת מהורדת תוכן מהשרתים למשתמשים, כגון דפי אינטרנט, קבצים, וסרטוני וידאו. תעבורת ההעלאה כוללת בעיקר בקשות לטעינת דפים, שליחת טפסים, ואינטראקציות עם שירותי ענן. ניתן לראות כי במקרים בהם משתמשים בשירותים אינטראקטיביים כמו שיחות וידאו או העלאת קבצים, יחס זה הופך מאוזן יותר.

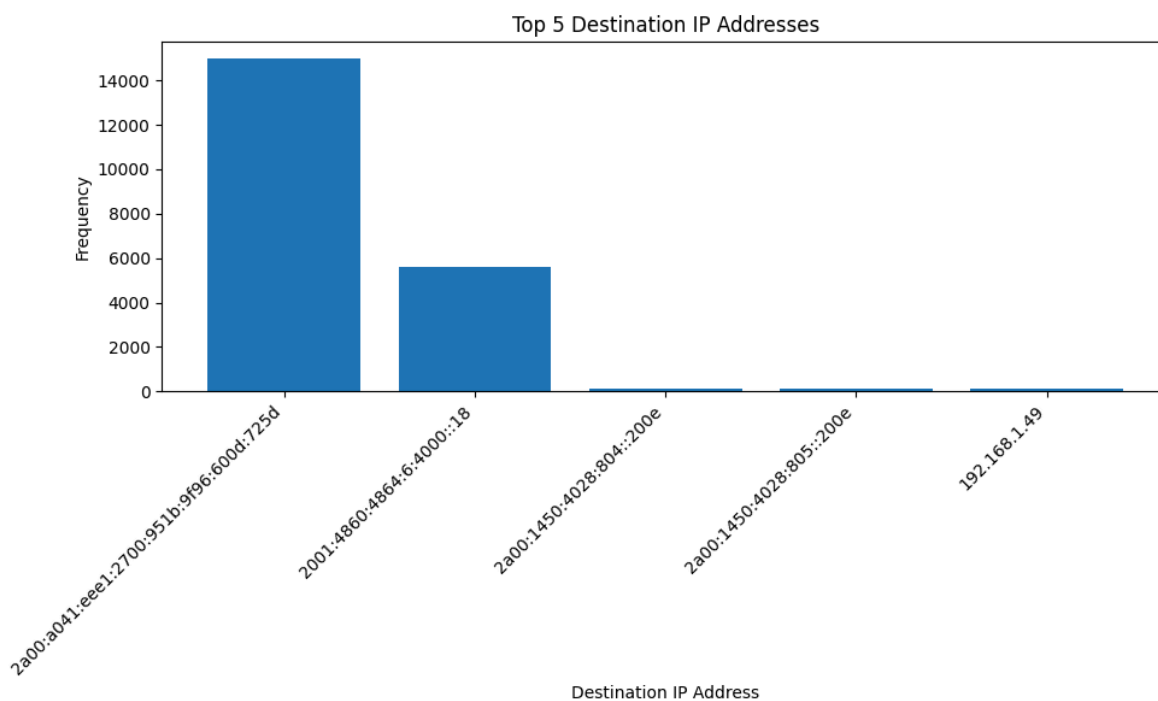
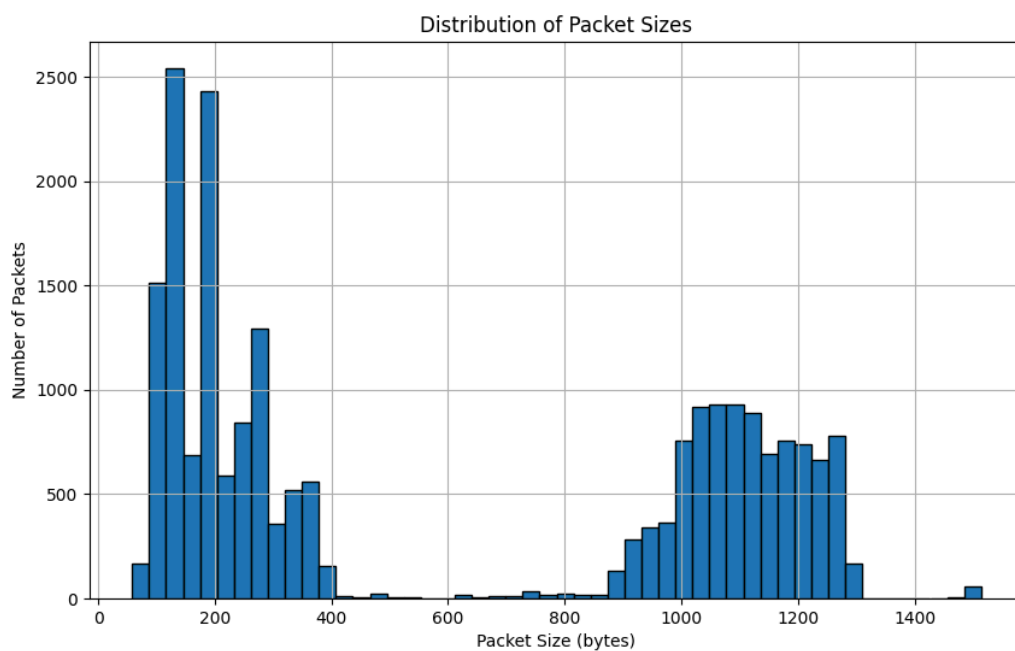
### סיכום

הנתונים מעידים כי התעבורה של Chrome מאופיינת בגישה נרחבת לשירותי Google ולתכנים המתארחים ברשתות CDN. רוב התקשורת נעשית בפרוטוקולי HTTP מאובטחים, תוך שימוש בפרוטוקולים מתקדמים כמו QUIC לשיפור הביצועים. כמו כן, תבנית התעבורה מצביעה על כך שרוב הנתונים נמשכים מהשרתים למשתמשים, דבר המתאים לאופי הדפדפן ככלי לצריכת תוכן. ביצועי הרשת נותרו יציבים, כאשר זמני ההגעה מאפשרים חוויית גלישה מהירה ויעילה.

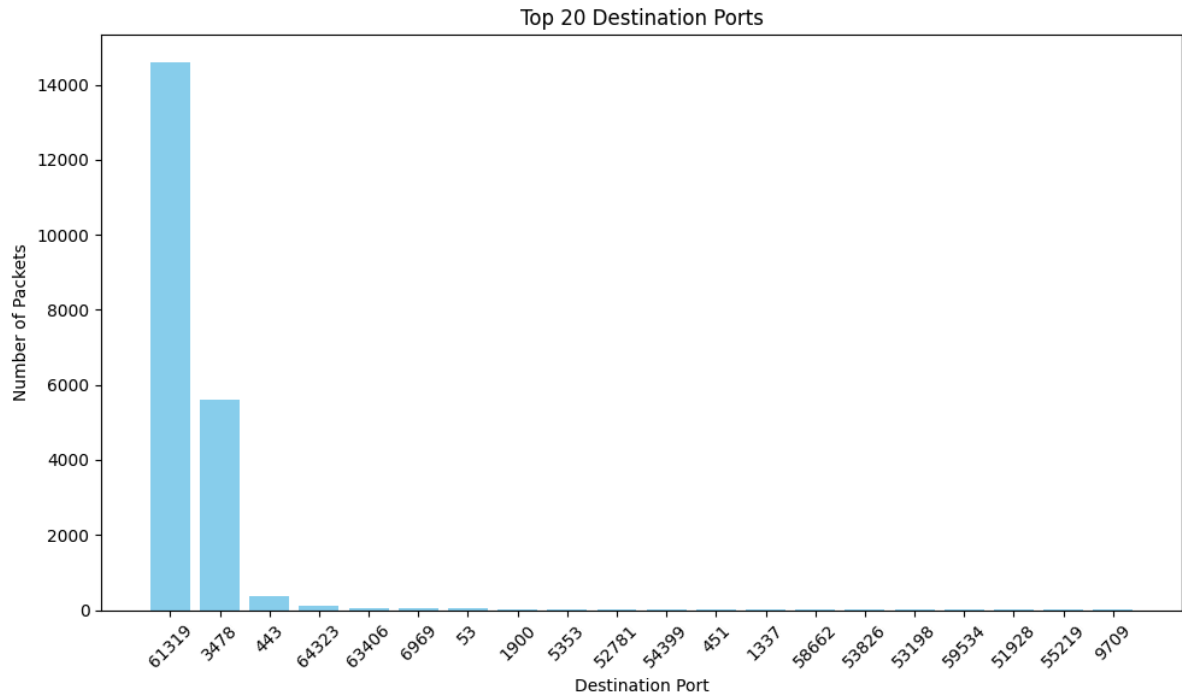
**גרפים לכל אפליקציה**

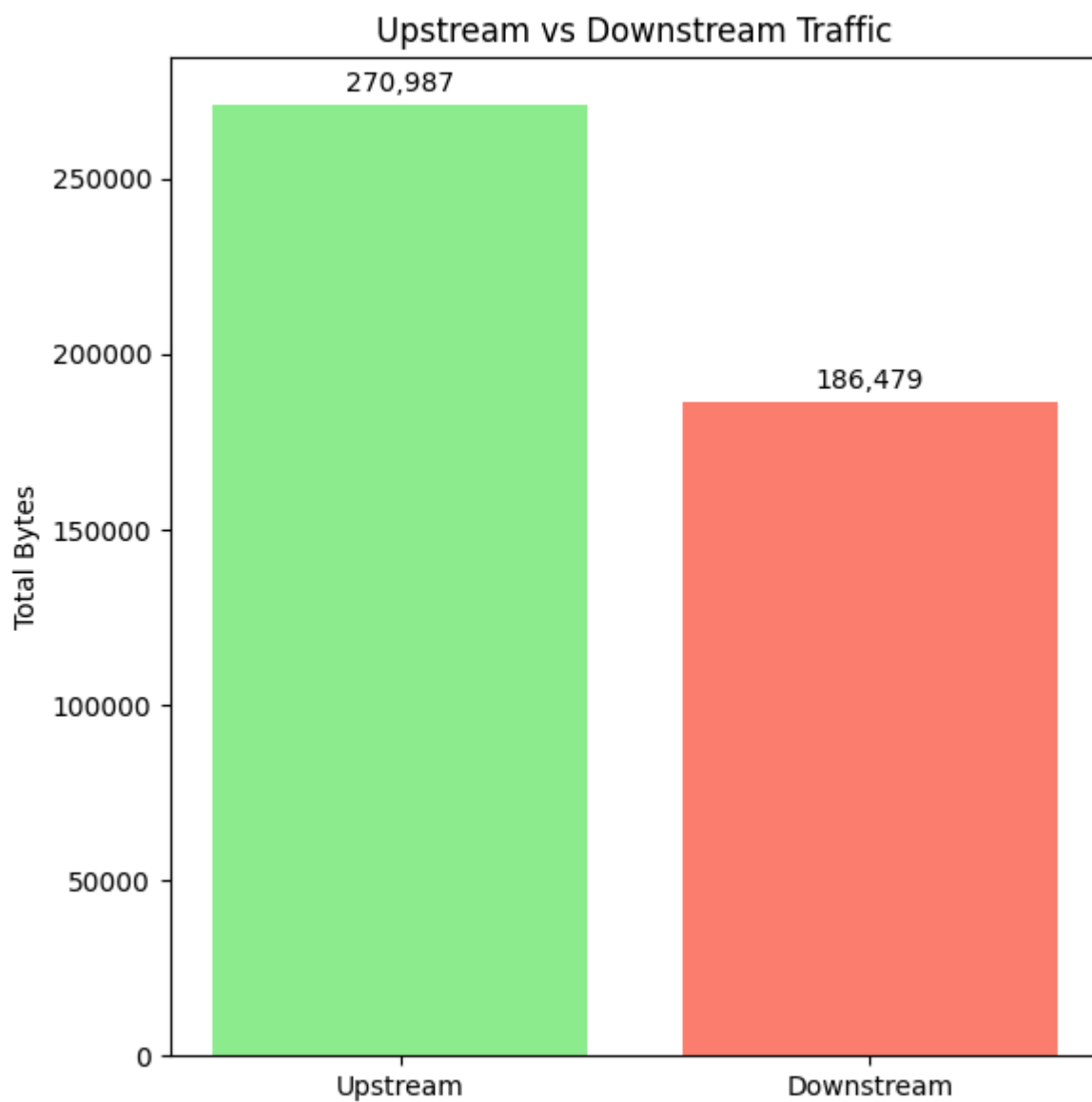
**GOOGLE MEETS**





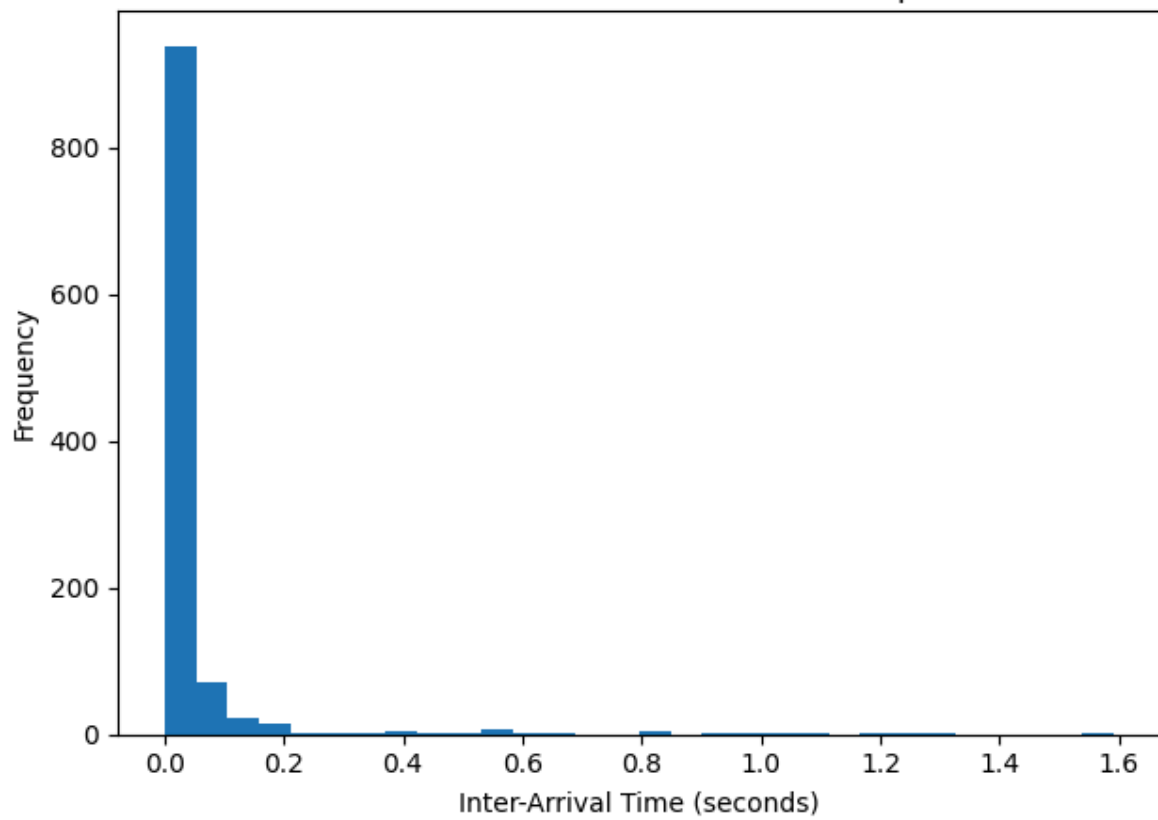




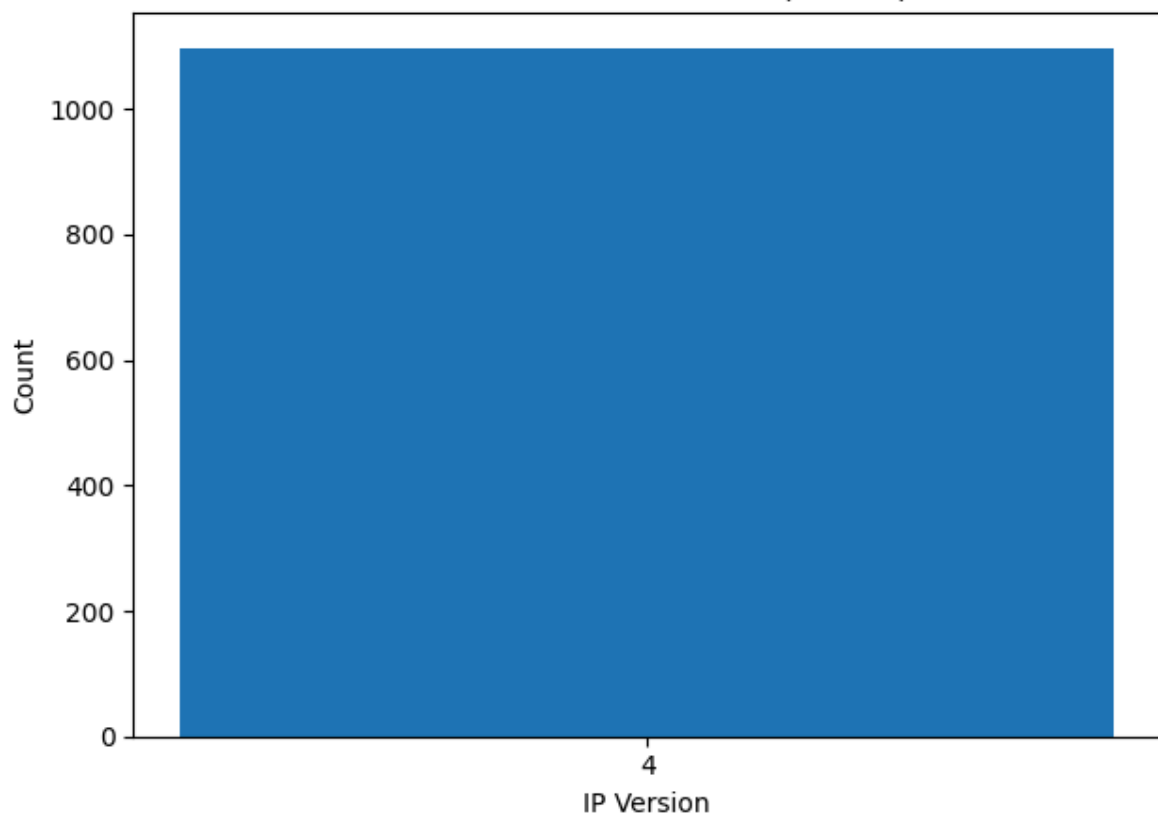


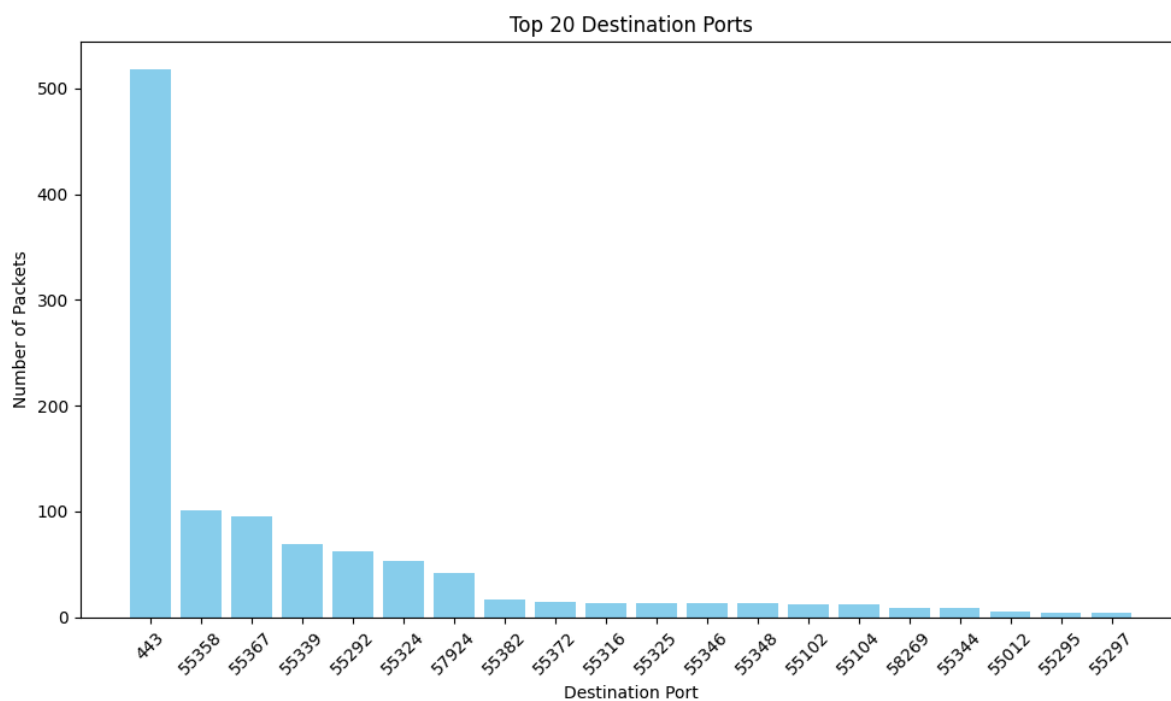
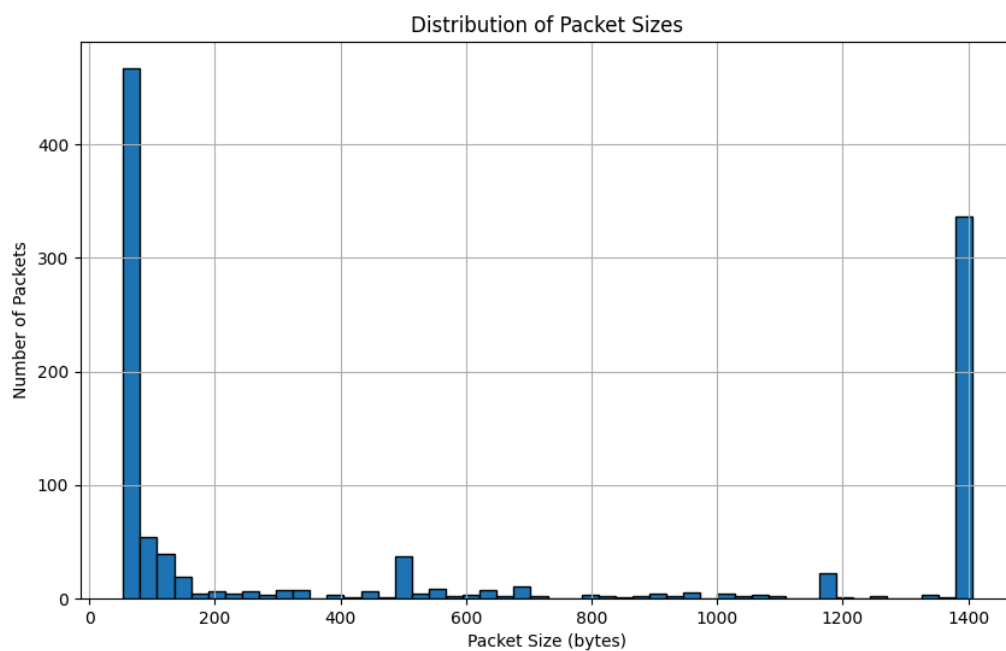
**EDGE**

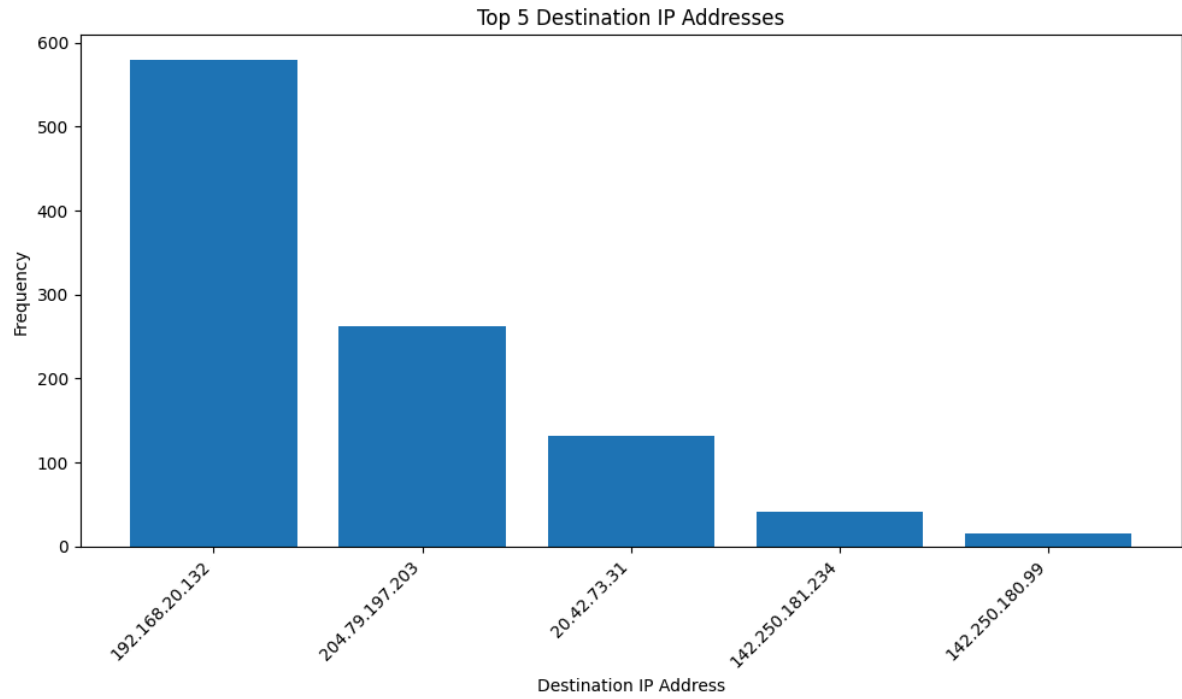
Distribution of Inter-Arrival Times ( $\leq$  99th percentile)

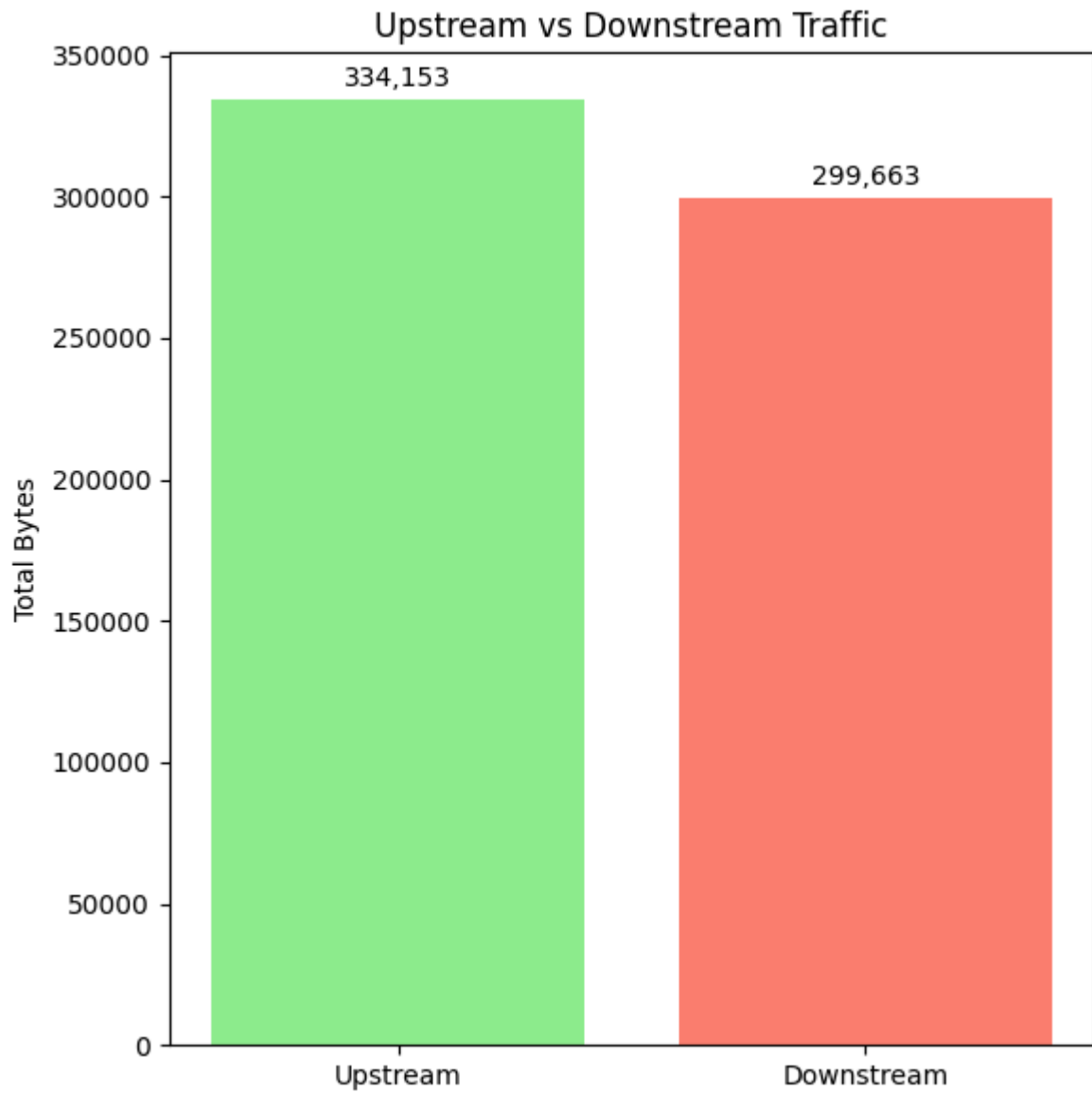


Distribution of IP Version (4 vs. 6)

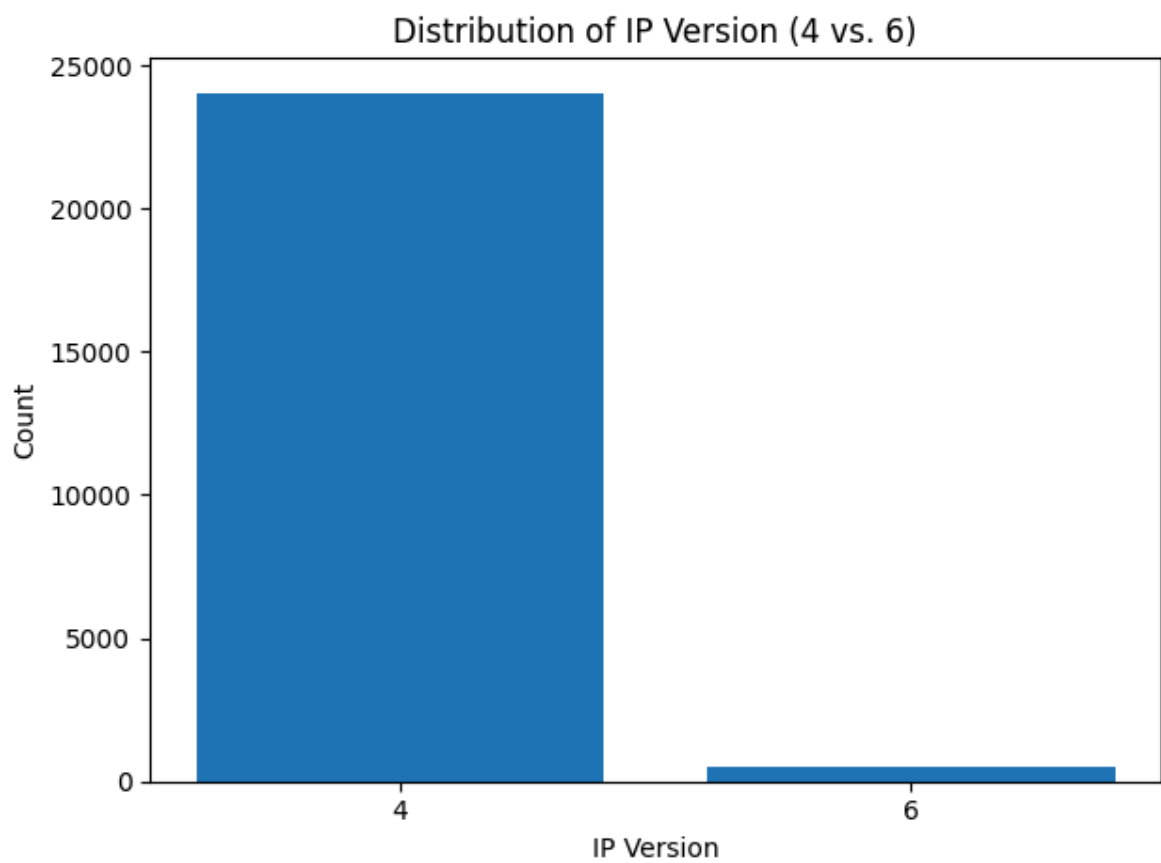
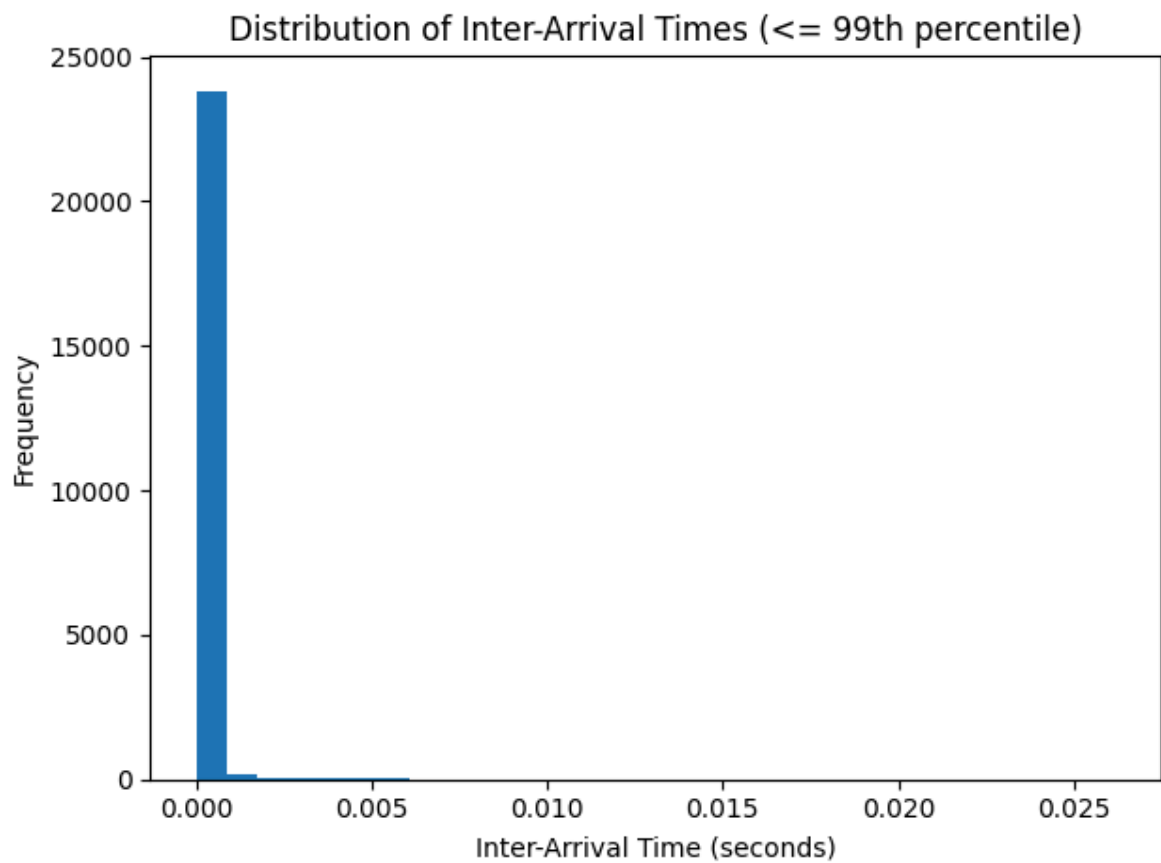


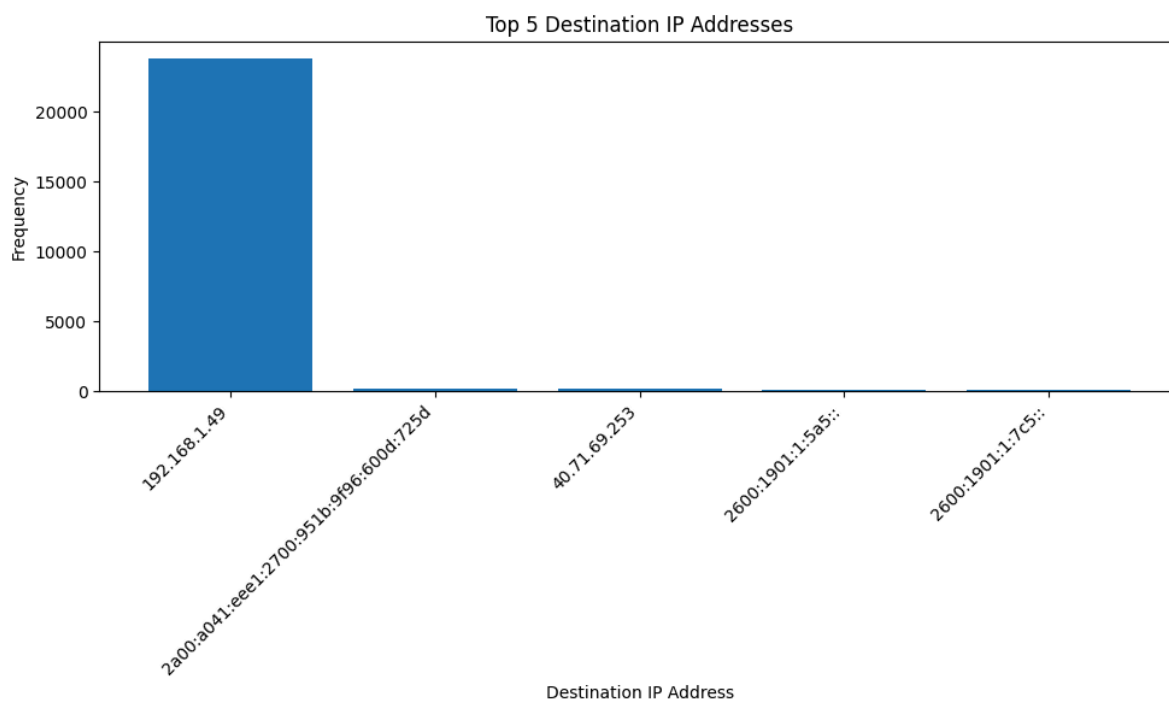
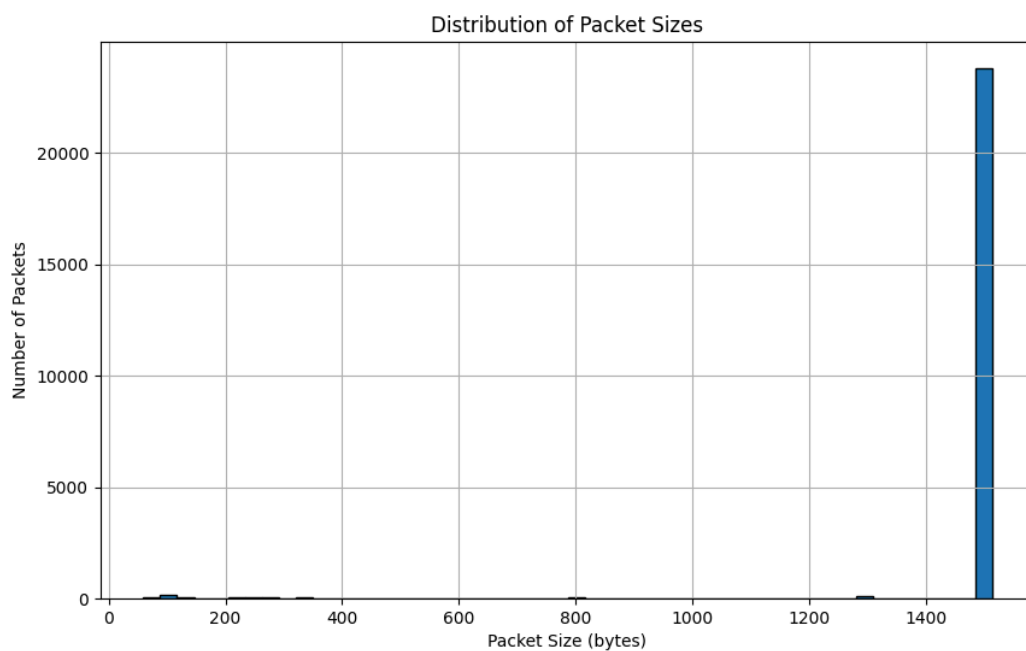




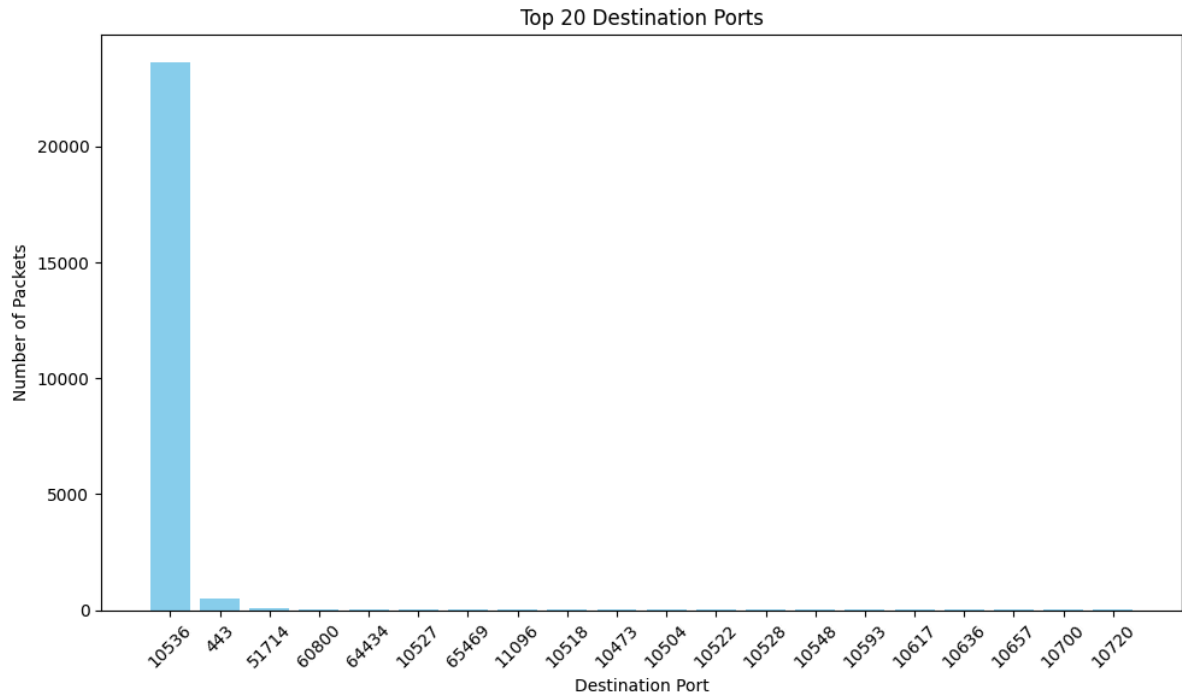


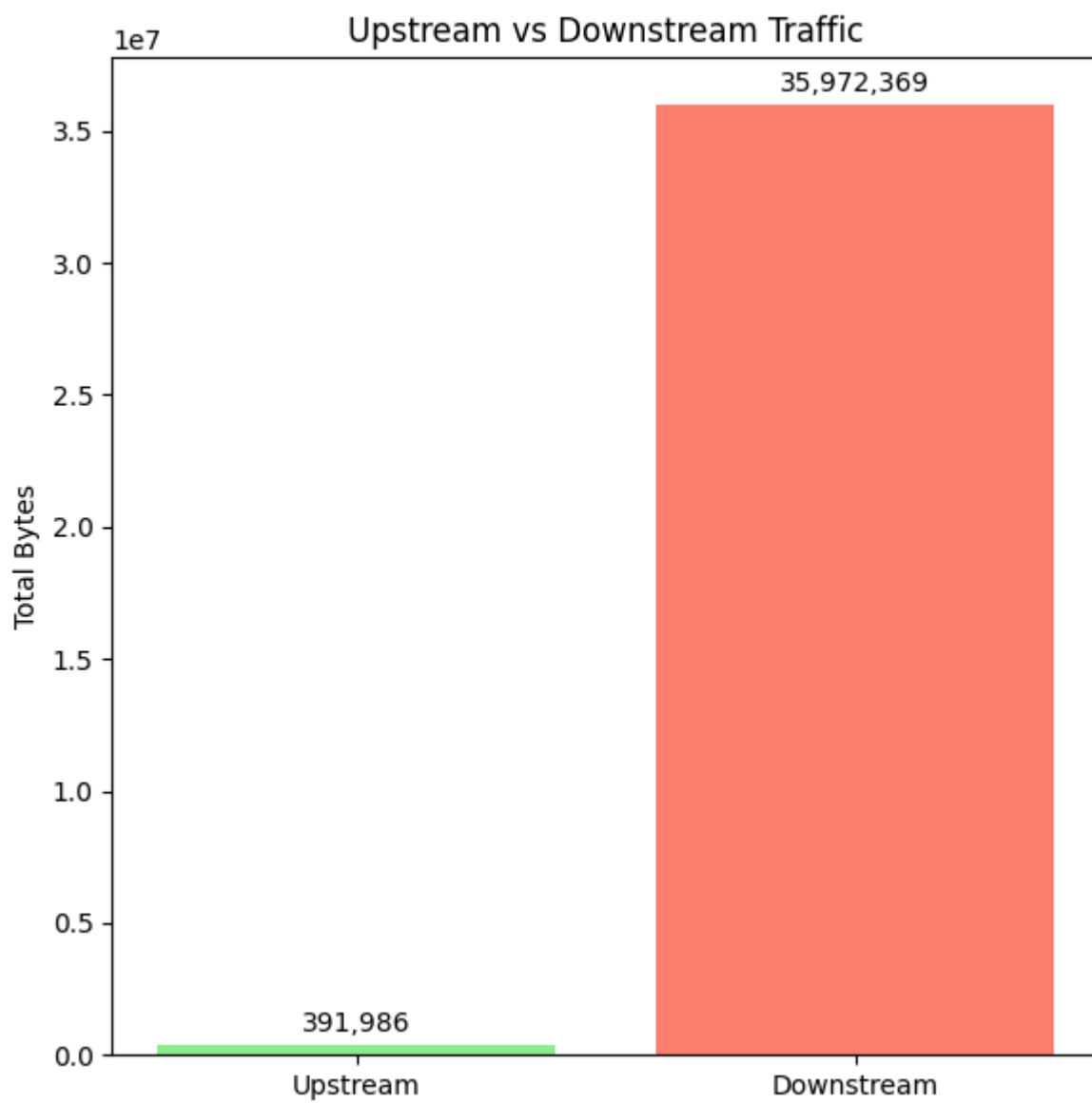
**spotify**



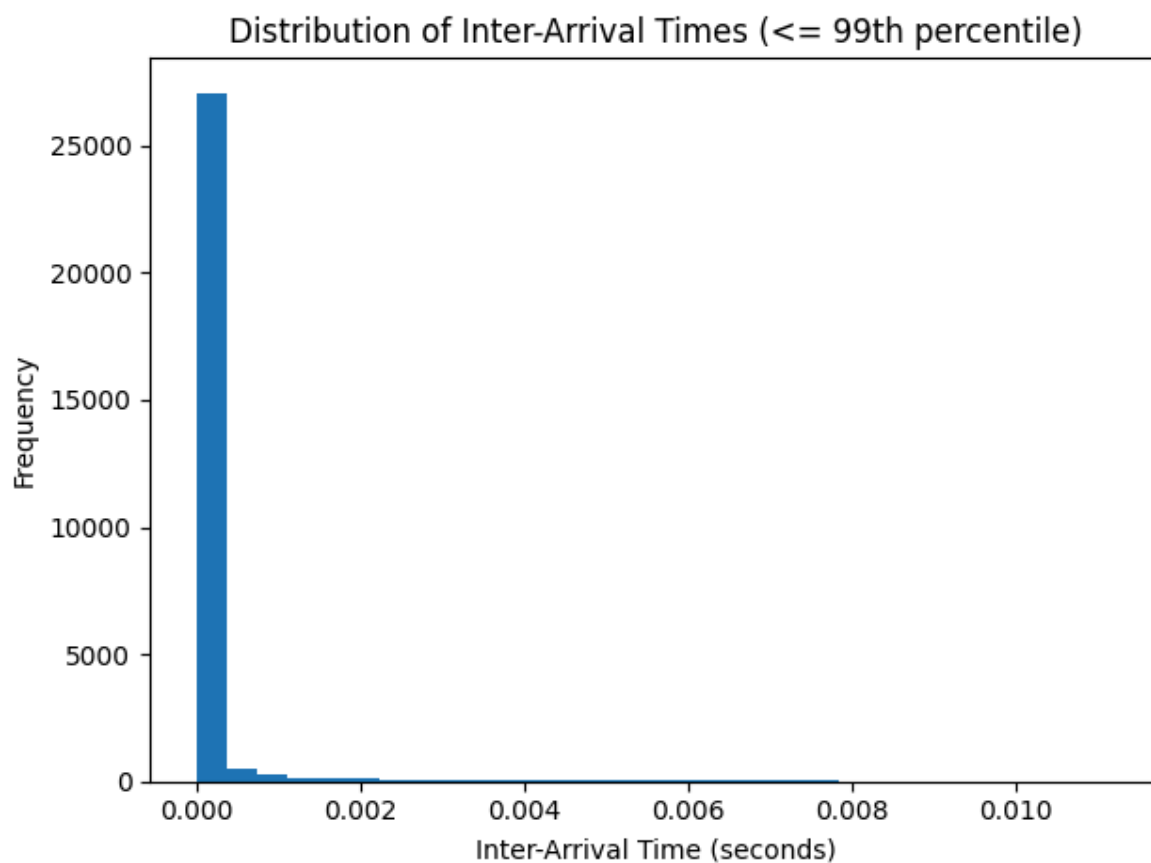
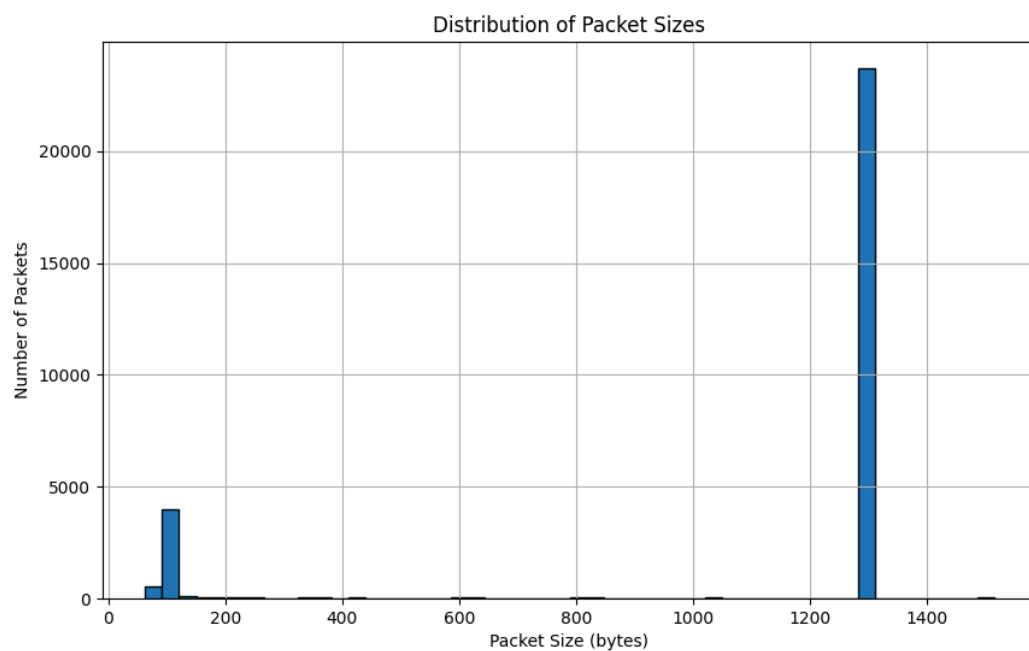


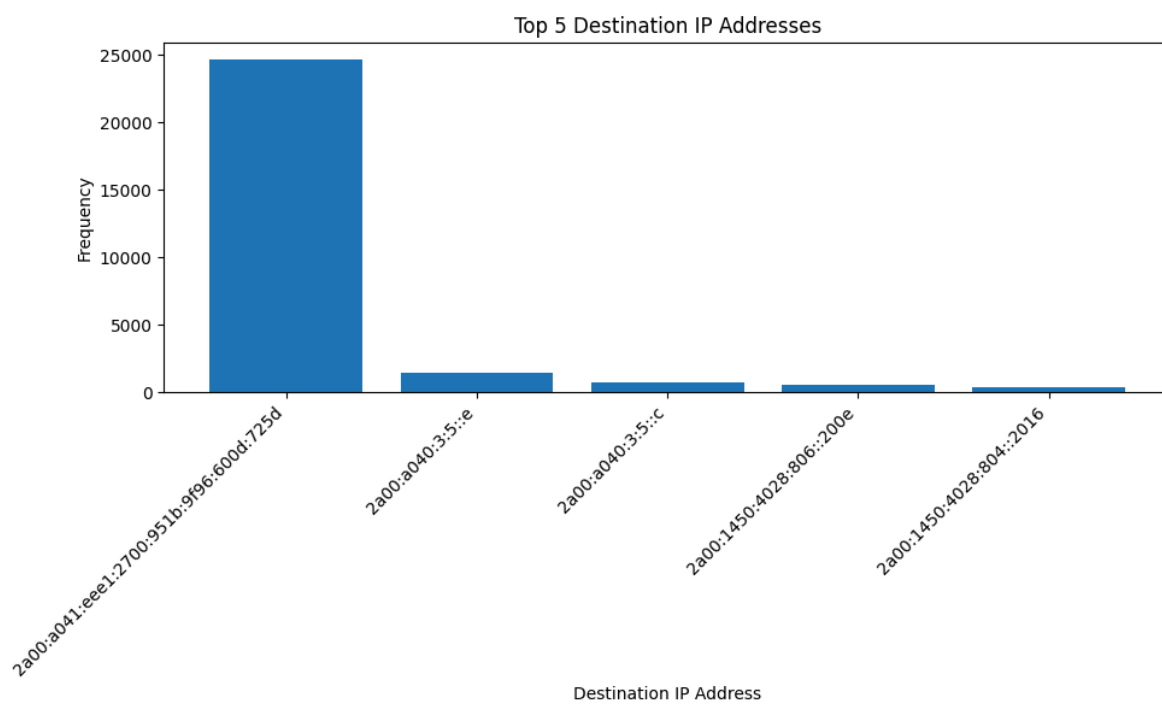
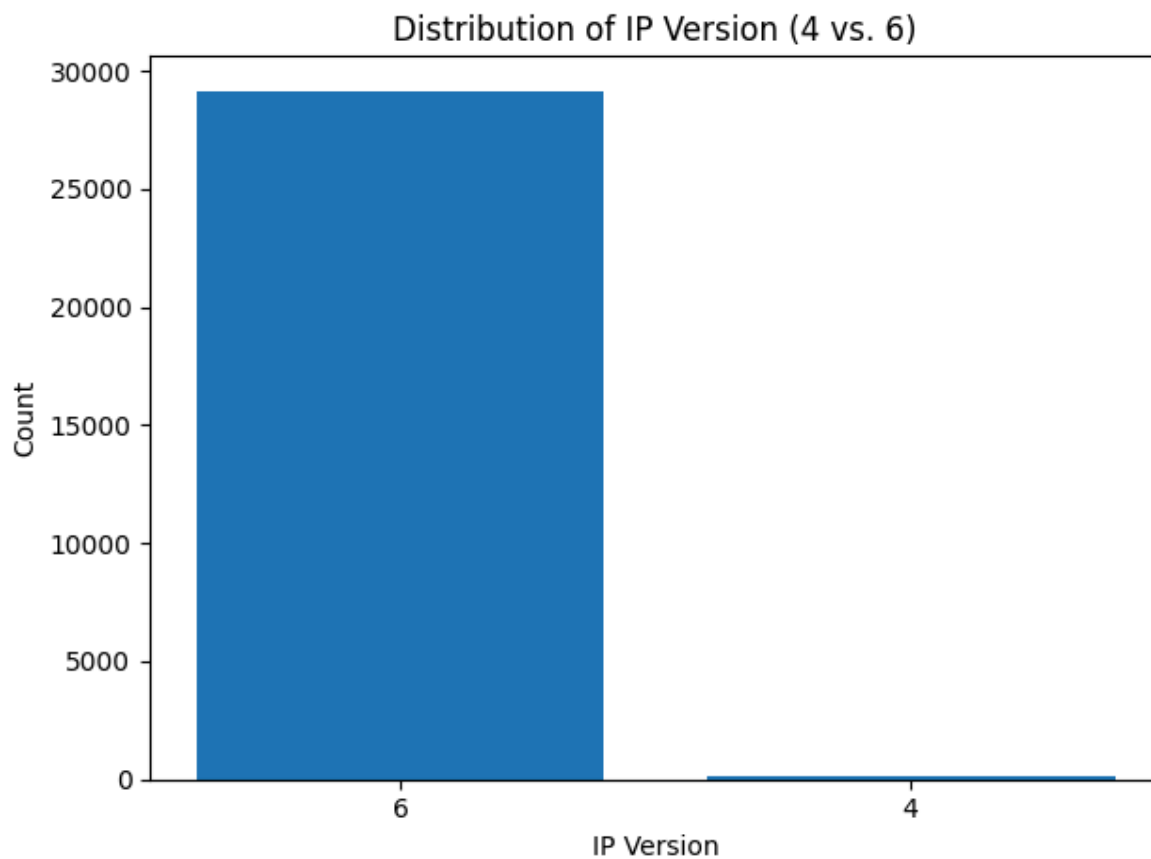


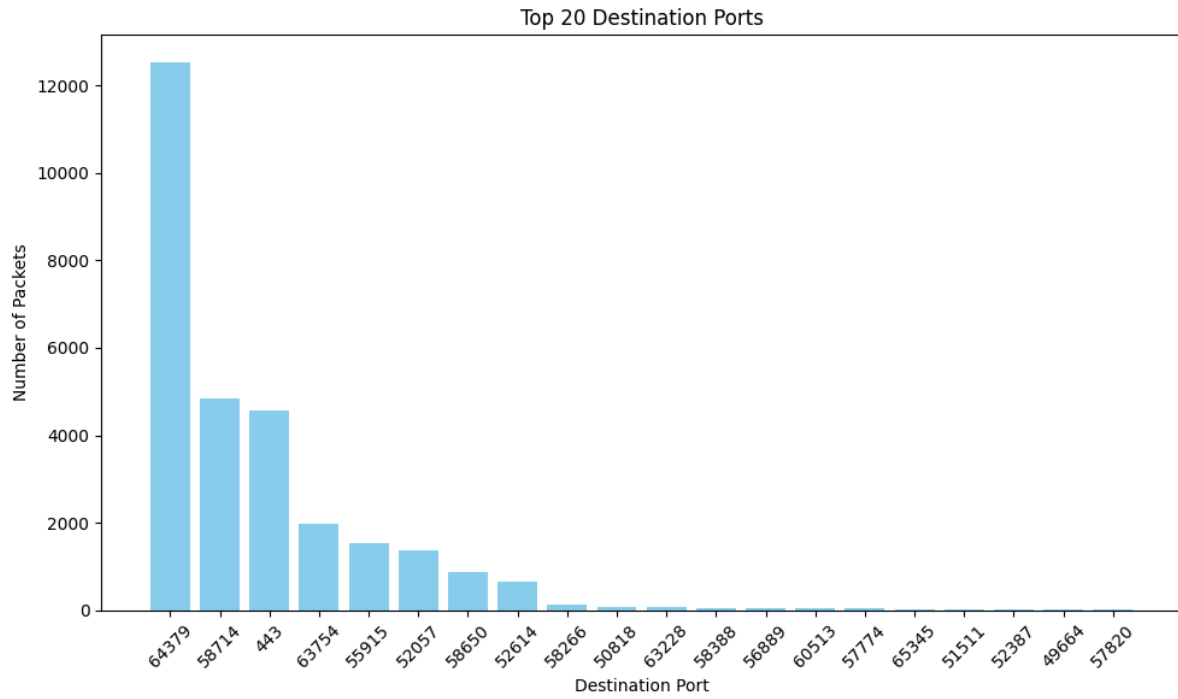


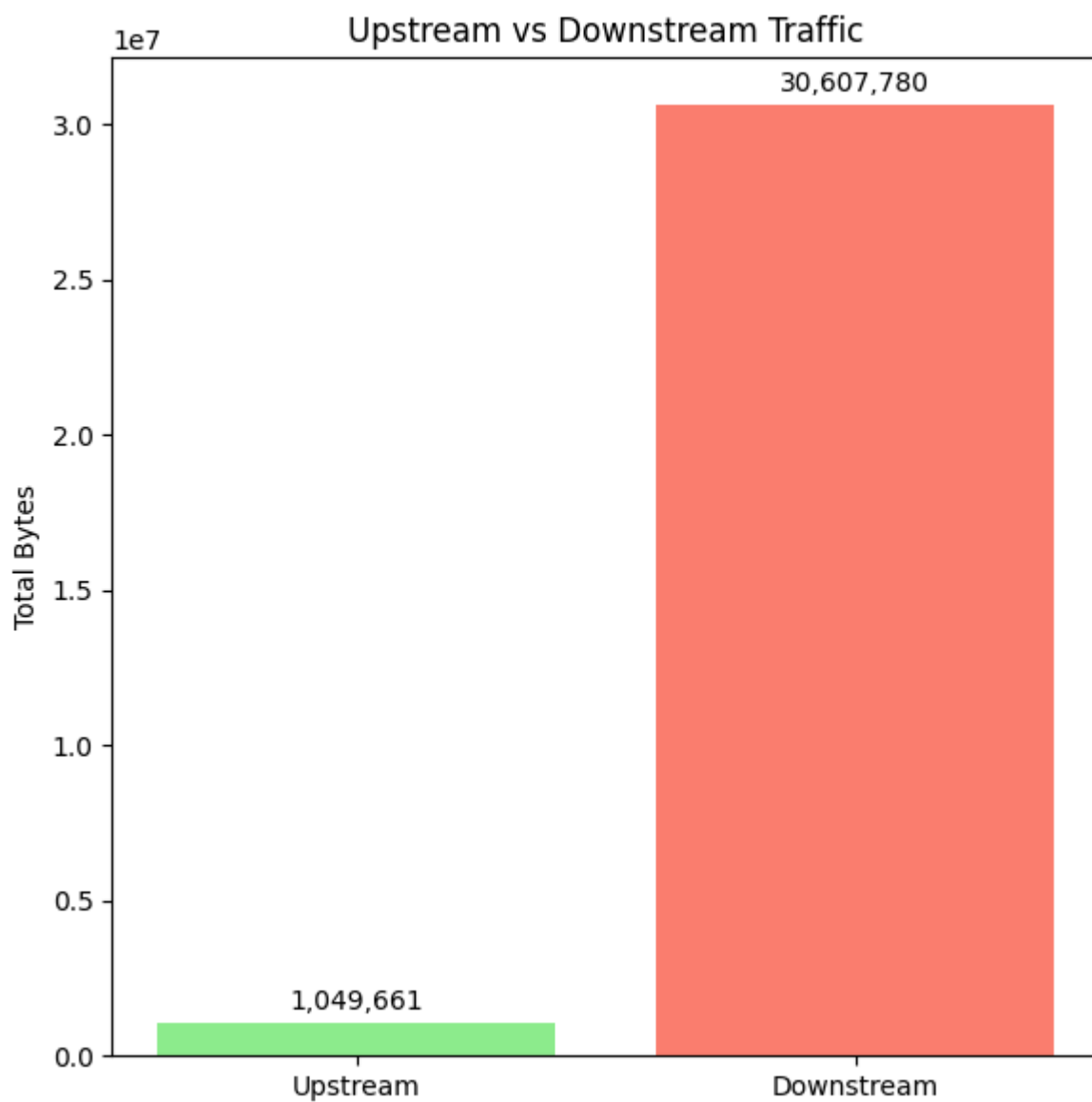


**YOUTUBE**

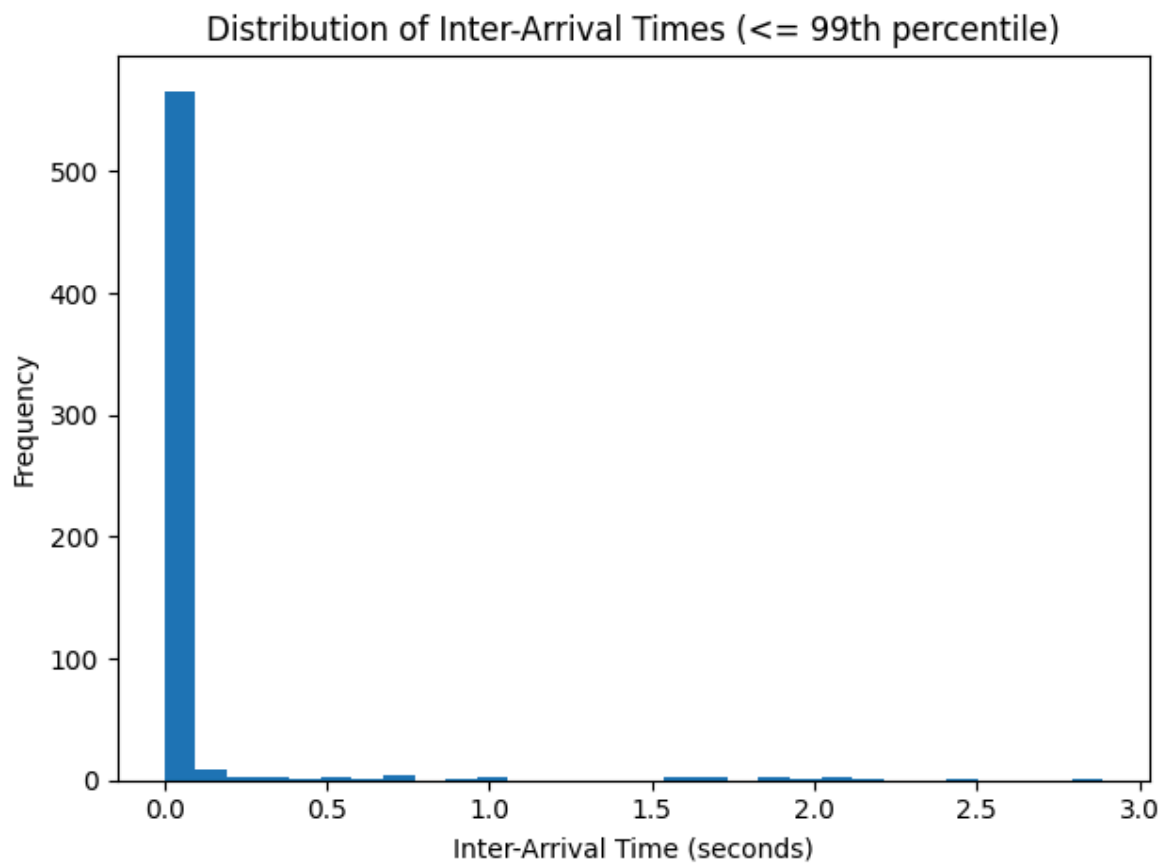




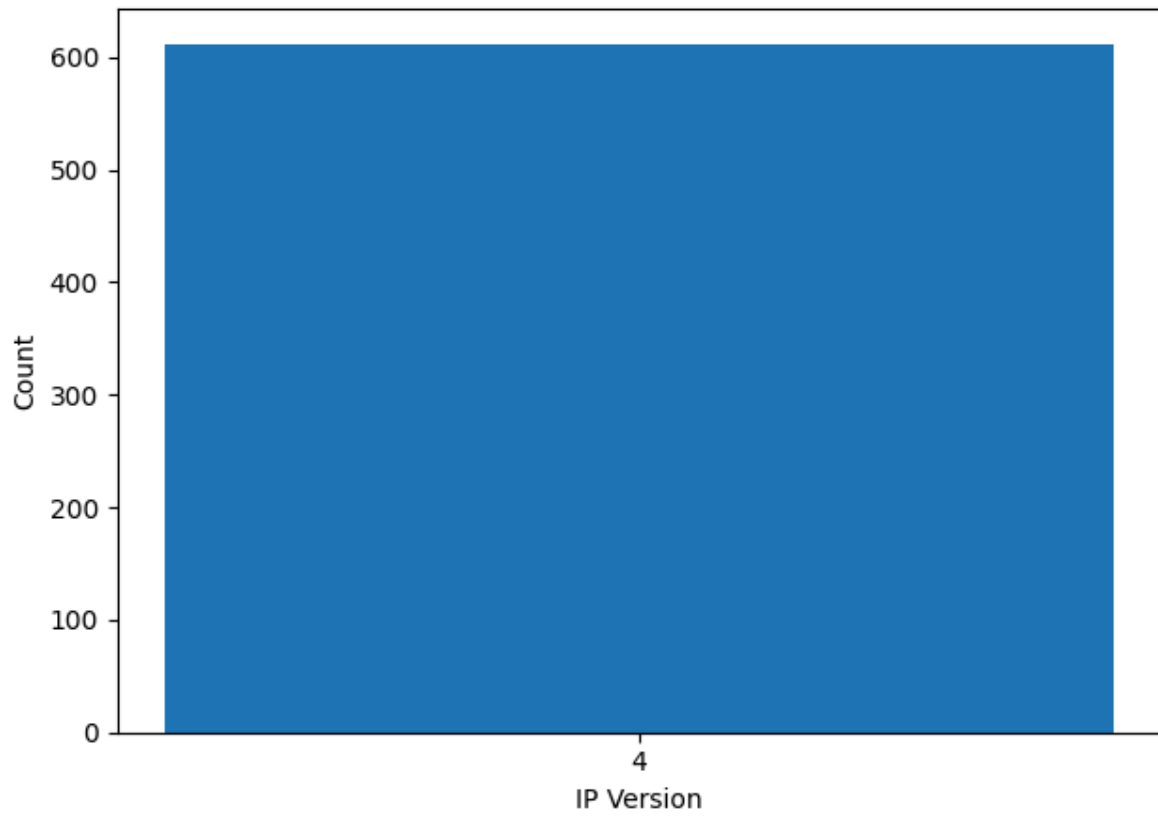




## chrome



Distribution of IP Version (4 vs. 6)



Distribution of Packet Sizes

