GOOGLE MEETS

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

1.לפי הגרף של כתובות הip נוכל לראות לראות שנעשה שימוש נרחב בכתובת 18::2001:4860:4864:6:4000 נשים לב שכותבת 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 וידיאו(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 הip נותן לנו אינדיקציה פחות חזקה משאר הגרפים שהוזכרו למעלה, אבל עדיין יכול לספק לנו רמזים לגבי השימוש בתעבורת הרשת, לדוגמה: משחקים מקוונים יעדיפו שימוש בip4, לעומת שירותים מודרניים שיעדיפו שימוש בipv6 (לדוגמה; AWS,Google).
הבחירה בipv6 לא מפתיעה אותנו מכיוון שgoogle "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 שמשמש לVoip וWebRTC, עוד אינדיקציה שמדובר בשיחת וידיאו
פורט 61319 - פורט דינאמי שהרבה פעמים משמש אותו בתקשורת בשיחות וידיאו ולמרות שישנם עוד אפשרויות עם נתחשב במכלול הנתונים נוכל לסמן את google meets כשוד העיקרי
6.גרף upstream/downstream: יחס דומה בין הupstream ל downstream יכול לרמוז לנו על שיחה קולית/ שיחת וידיאו (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 הip 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 וידיאו כמו YouTube או Google Meets, שם החבילות גדולות יותר).

התפלגות כתובות IP (IP Distribution) – אם נראה שהתעבורה מופנית לכתובות שמקושרות לשרתי 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.

יחס Upstream/Downstream – 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 לדוגמא, ההבדלים העיקריים יהיו בעיקר בגודל החבילות, הפורטים בהם נעשה שימוש, והיחס בין הזרימה הנכנסת והיוצאת.

edge

נתבונן 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 שרתיי 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 בדפוסי התעבורה של גלישה רגילה ולא שירות תקשורת בזמן אמת.
6. **יחס Upstream/Downstream** 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.

יחס Upstream/Downstream

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 UDP, המאפשר שיפור ביצועים בהזרמת תוכן והפחתת השהיות, במיוחד בפלטפורמות כגון YouTube ו-Google Drive.

יחס Upstream/Downstream

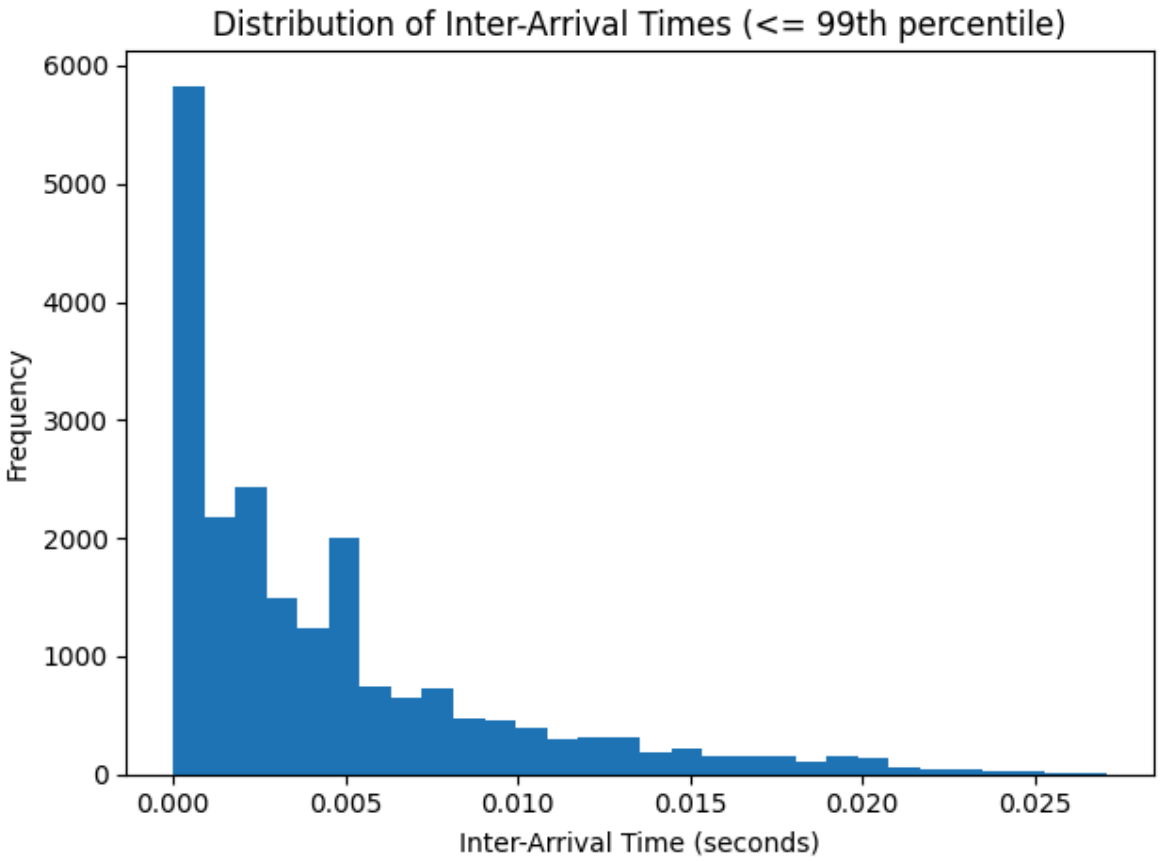
יחס ההורדה להעלאה (Downstream/Upstream) מצביע על כך שרוב תעבורת הדפדפן מורכבת מהורדת תוכן מהשרתים למשתמשים, כגון דפי אינטרנט, קבצים, וסרטוני וידאו. תעבורת ההעלאה כוללת בעיקר בקשות לטעינת דפים, שליחת טפסים, ואינטראקציות עם שירותי ענן. ניתן לראות כי במקרים בהם משתמשים בשירותים אינטראקטיביים כמו שיחות וידאו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

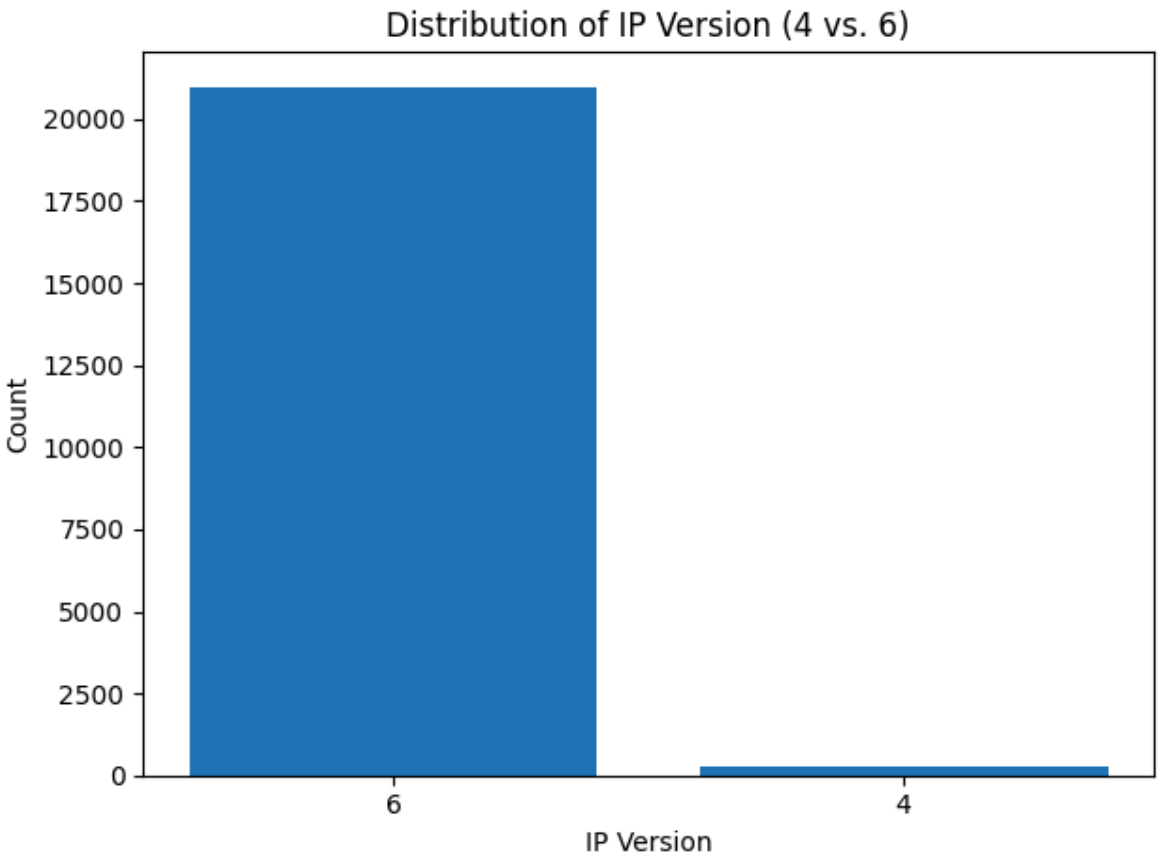
סיכום

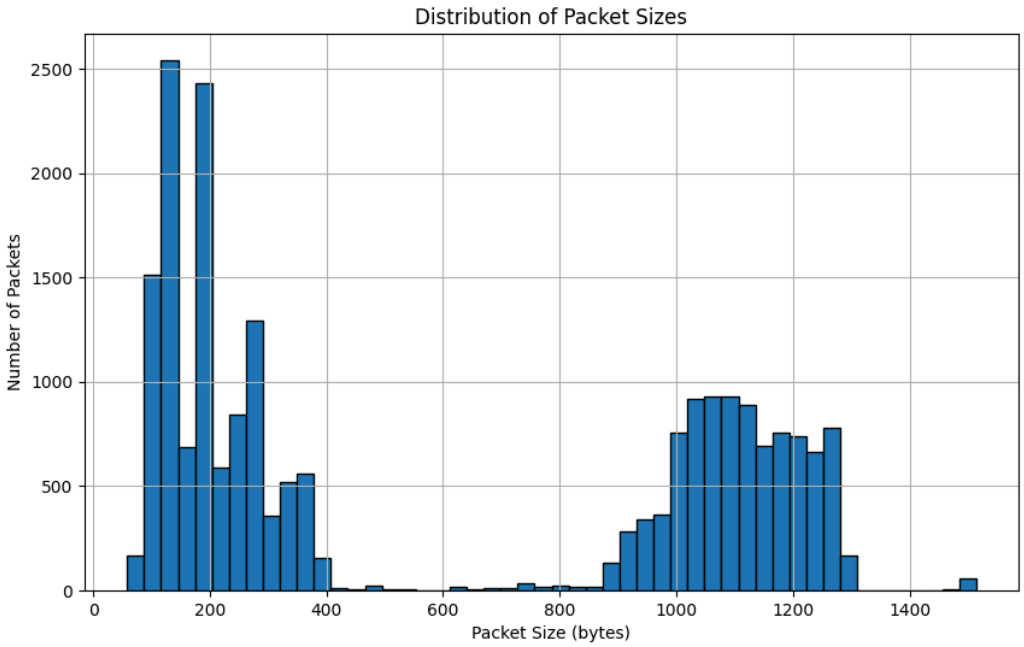
הנתונים מעידים כי התעבורה של Chrome מאופיינת בגישה נרחבת לשירותי Google ולתכנים המתארחים ברשתות CDN. רוב התקשורת נעשית בפרוטוקולי HTTP מאובטחים, תוך שימוש בפרוטוקולים מתקדמים כמו QUIC לשיפור הביצועים. כמו כן, תבנית התעבורה מצביעה על כך שרוב הנתונים נמשכים מהשרתים למשתמשים, דבר המתאים לאופי הדפדפן ככלי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

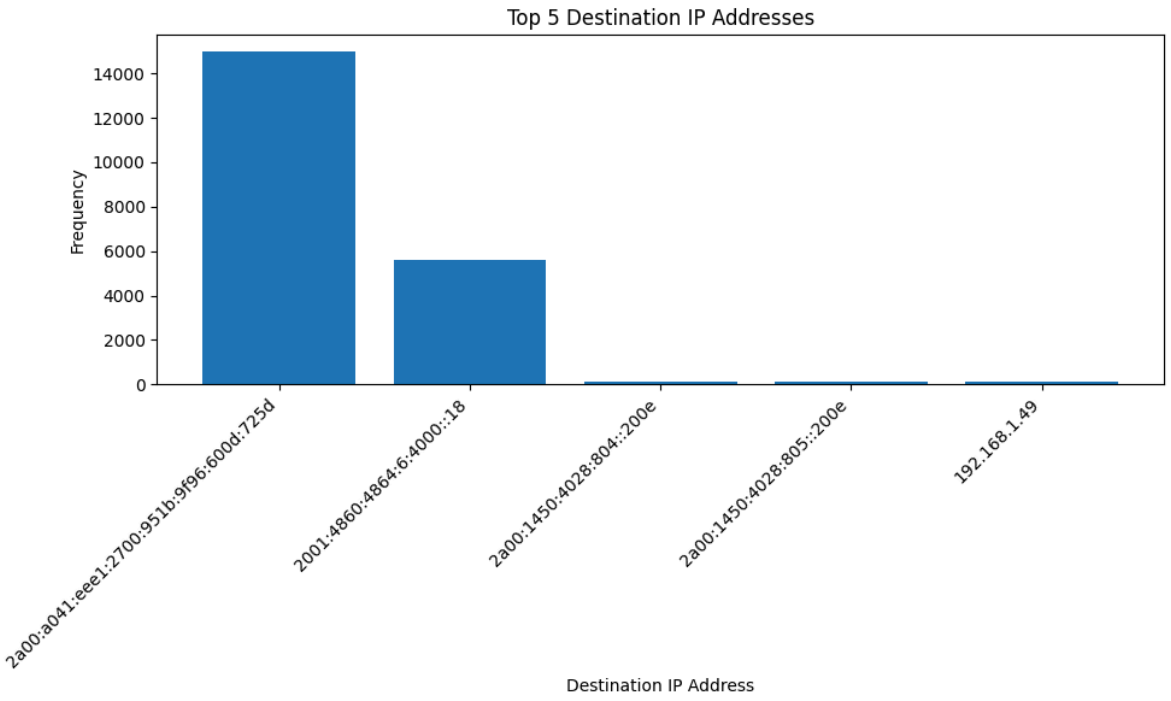
גרפים לכל אפליקציה

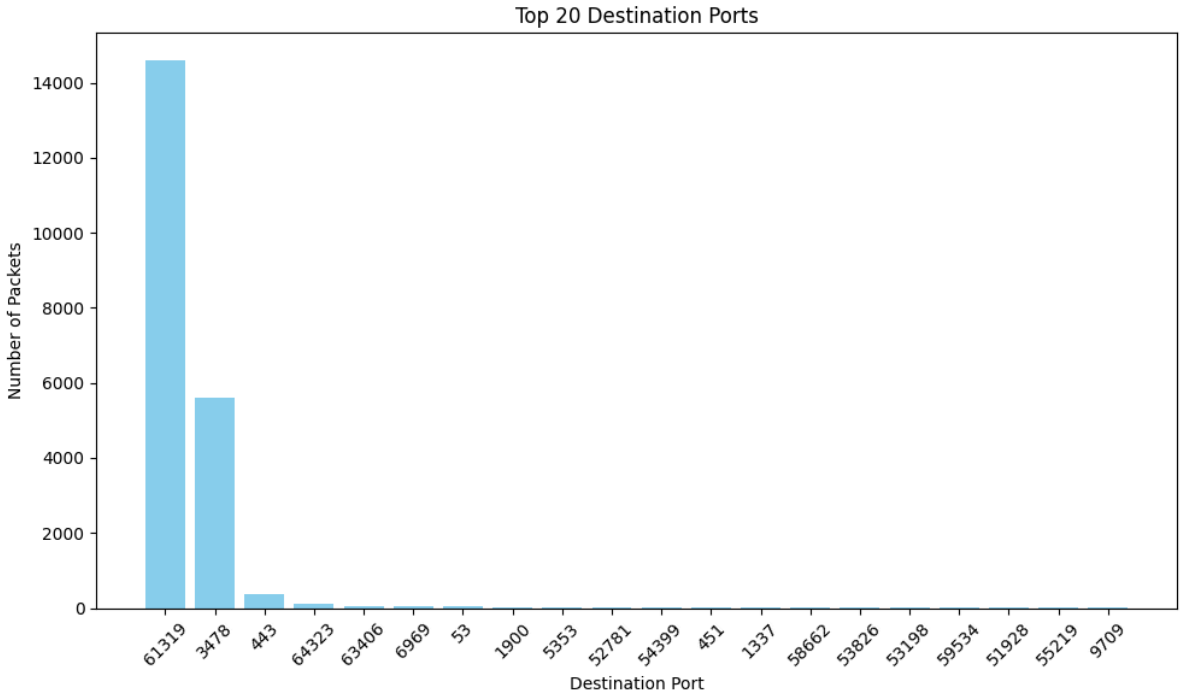
GOOGLE MEETS

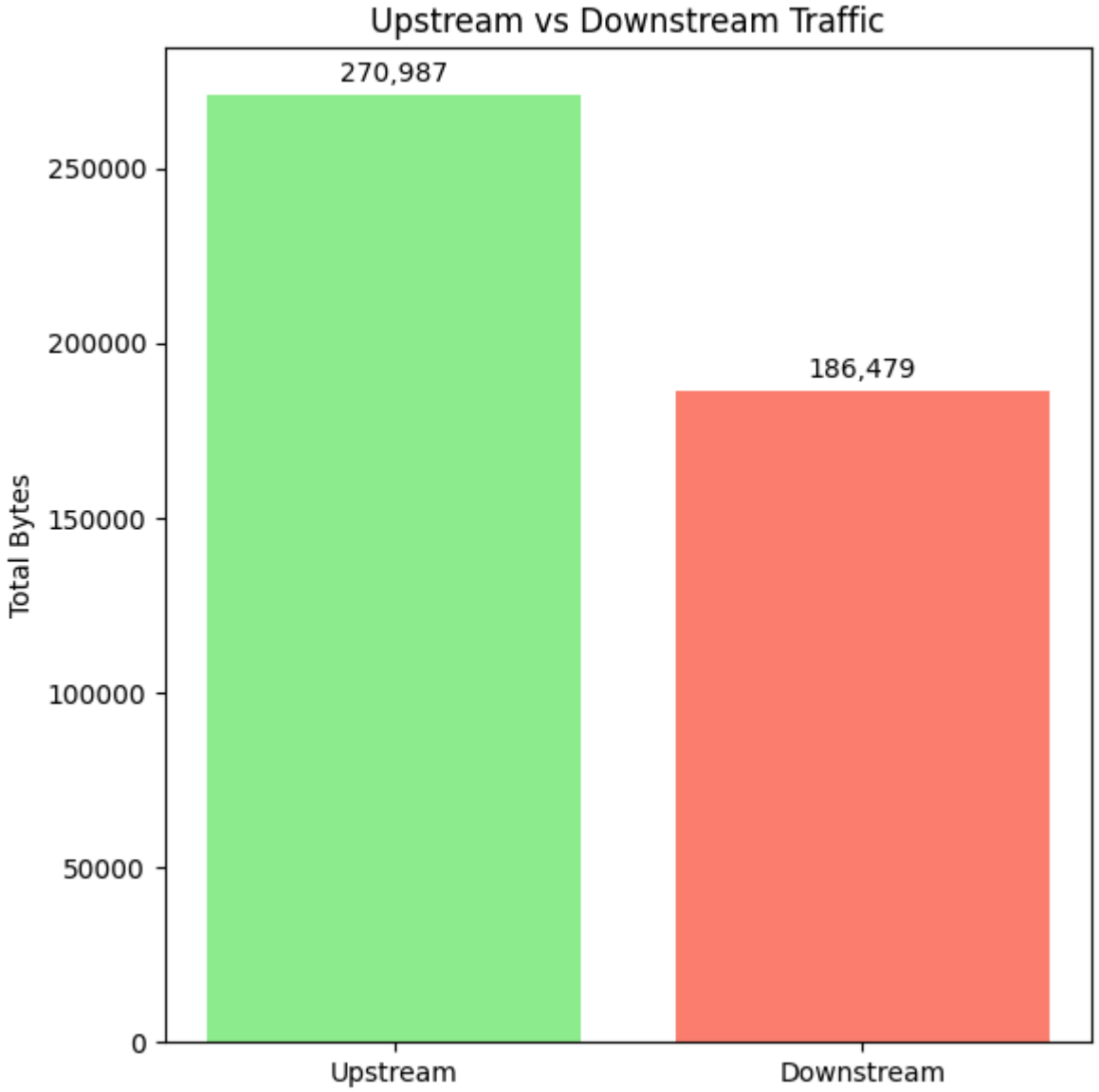

Distribution of Inter-Arrival Times (<= 99th percentile)
Frequency
6000
5000
4000
3000
2000
1000
0
0.000
0.005
0.010
0.015
0.020
0.025
Inter-Arrival Time (seconds)


Distribution of IP Version (4 vs. 6)
Count
20000
17500
15000
12500
10000
7500
5000
2500
0
6
4
IP Version

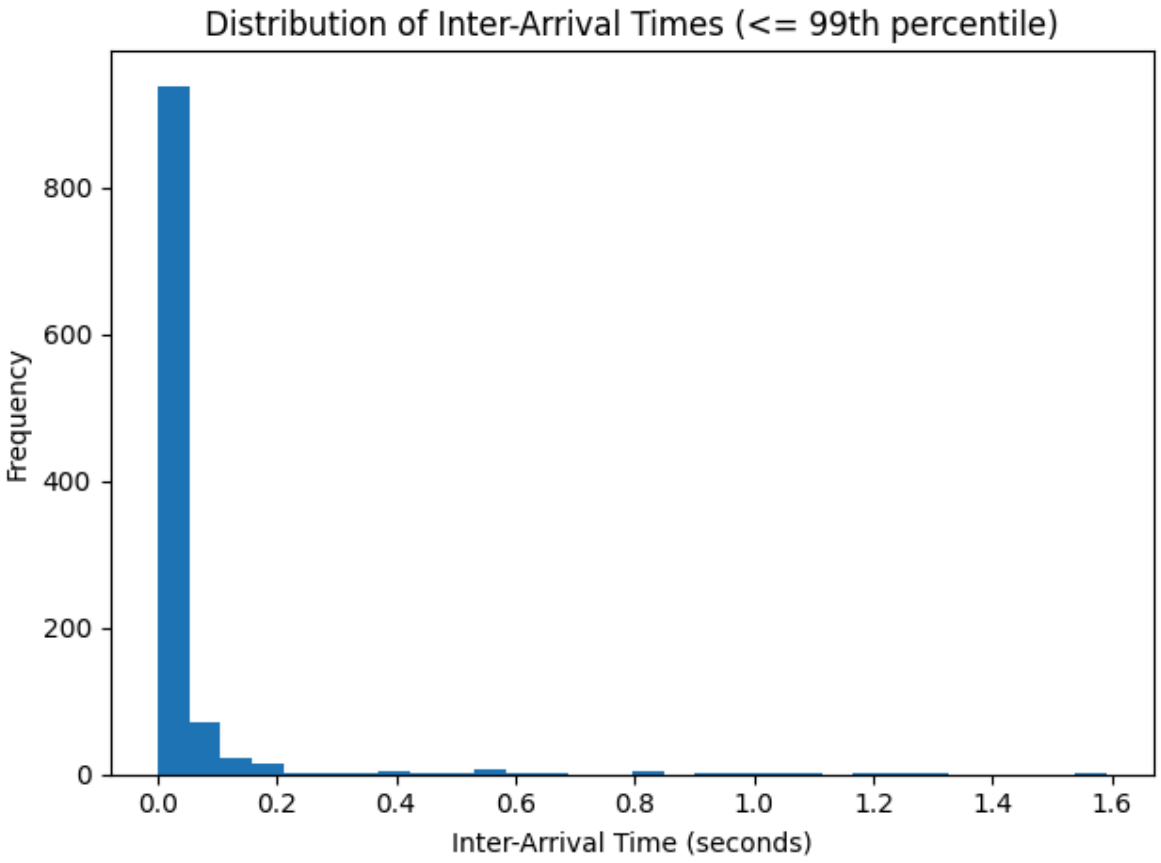

Distribution of Packet Sizes
Number of Packets
Packet Size (bytes)
0
500
1000
1500
2000
2500
0
200
400
600
800
1000
1200
1400

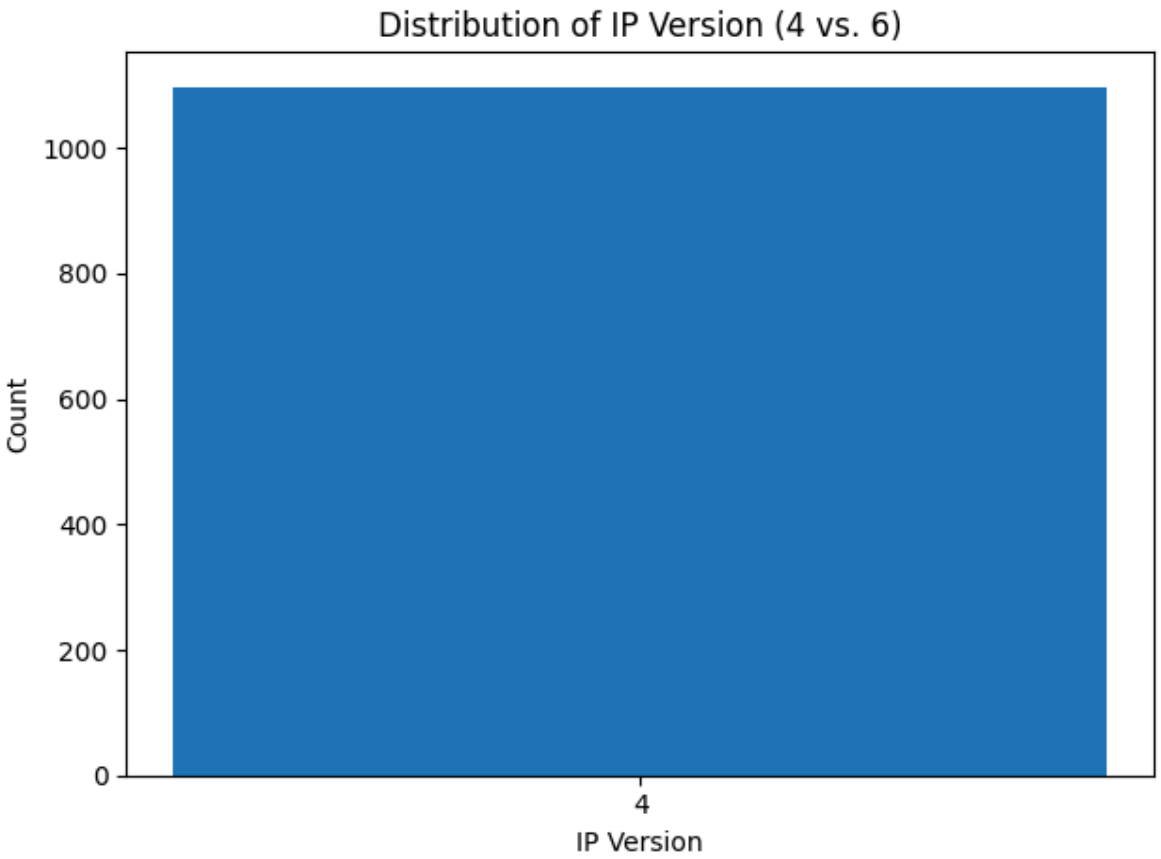

Top 5 Destination IP Addresses
Frequency
Destination IP Address
0
2000
4000
6000
8000
10000
12000
14000
2a00:a041:eee1:2700:951b:9f96:600d:725d
2001:4860:4864:6:4000::18
2a00:1450:4028:804::200e
2a00:1450:4028:805::200e
192.168.1.49

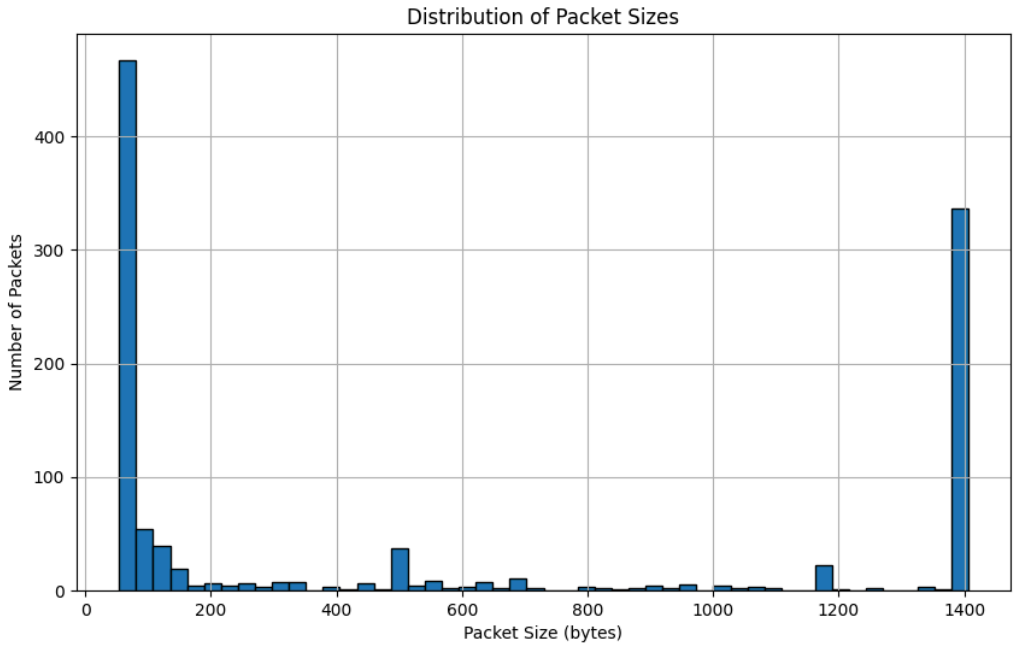

Top 20 Destination Ports
Number of Packets
0
2000
4000
6000
8000
10000
12000
14000
61319
3478
443
64323
63406
6969
53
1900
5353
52781
54399
451
1337
58662
53826
53198
59534
51928
55219
9709
Destination Port

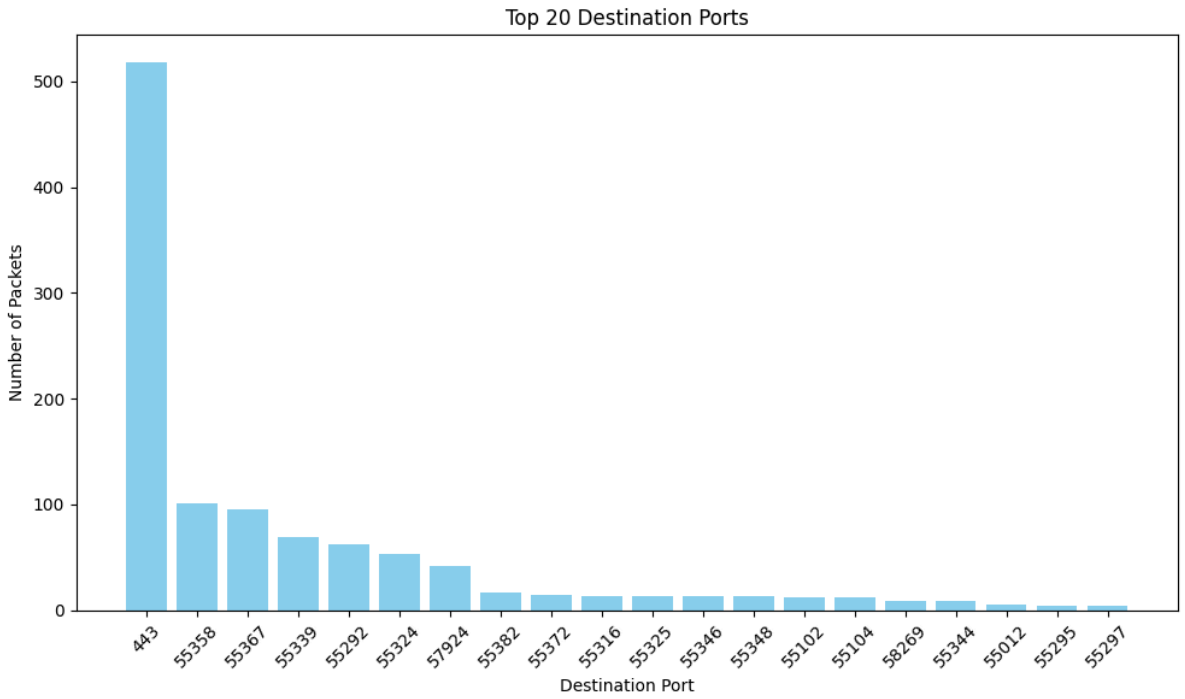

Upstream vs Downstream Traffic
270,987
186,479
Total Bytes
250000
200000
150000
100000
50000
0
Upstream
Downstream

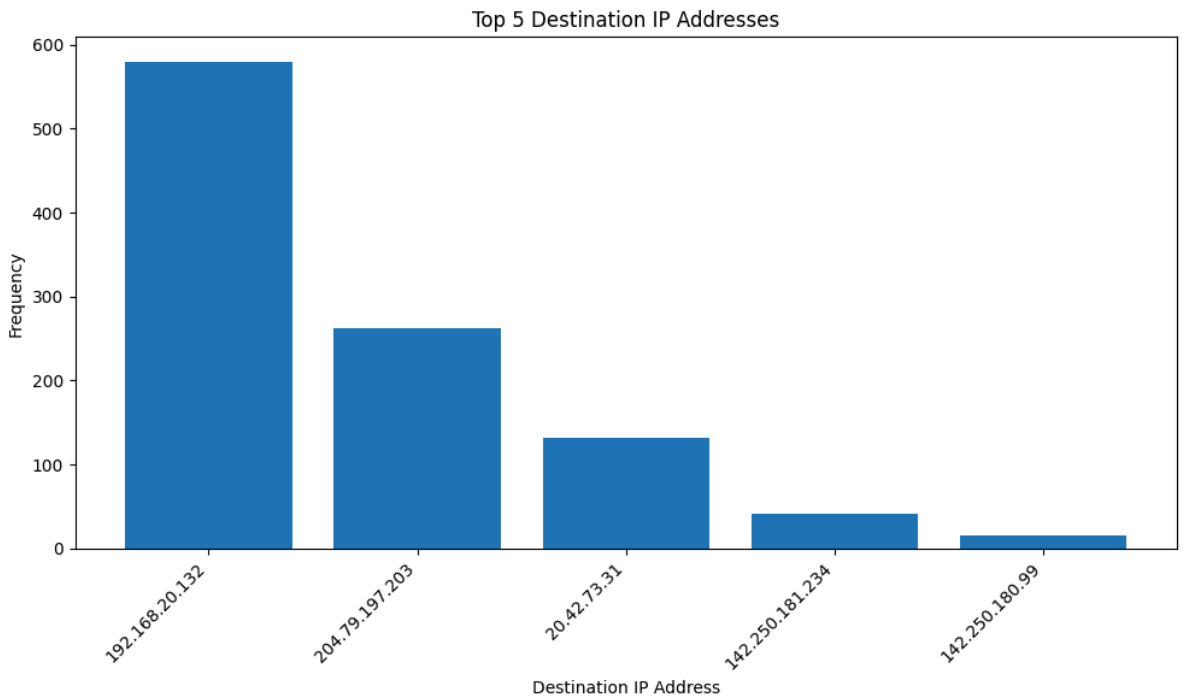
EDGE

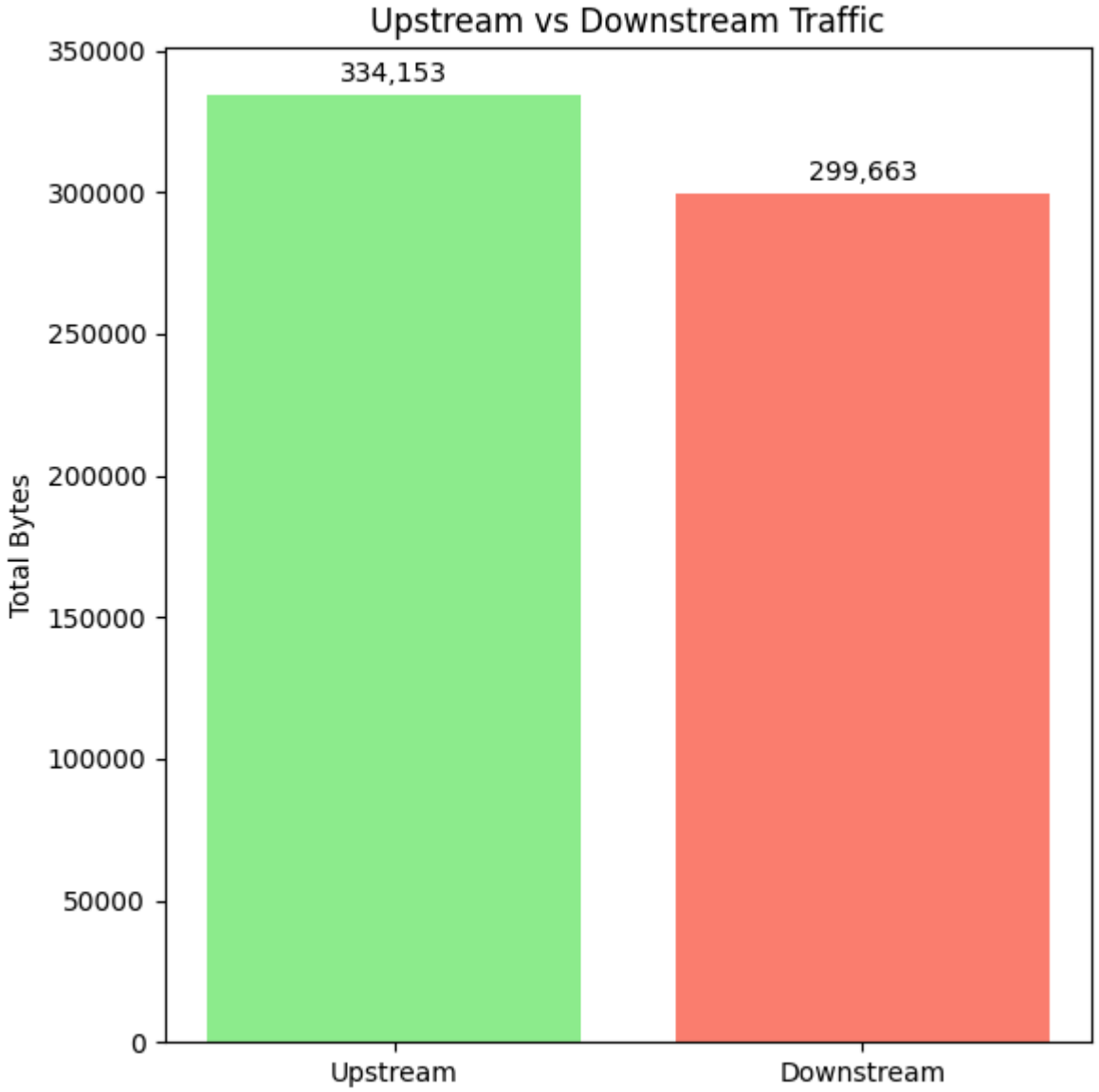

Distribution of Inter-Arrival Times (<= 99th percentile)
Frequency
0
200
400
600
800
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
1.6
Inter-Arrival Time (seconds)


Distribution of IP Version (4 vs. 6)
Count
0
200
400
600
800
1000
4
IP Version

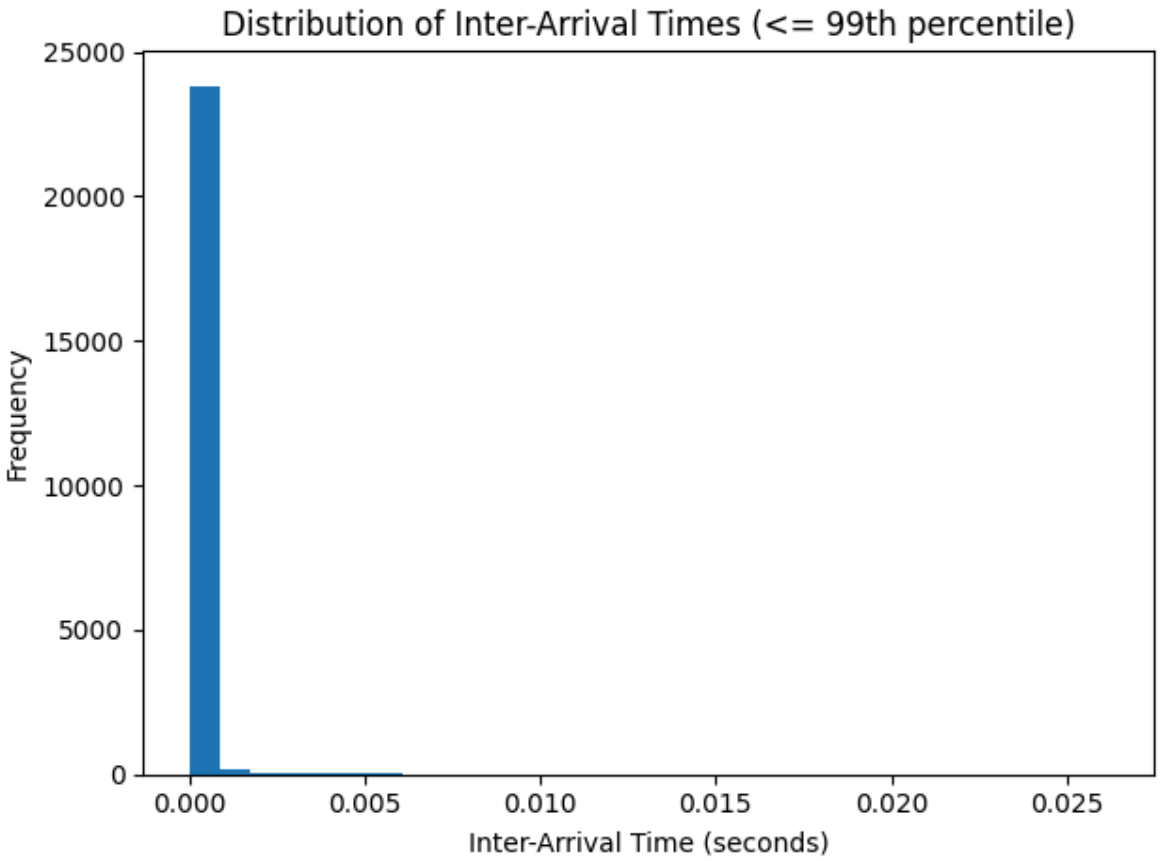

Distribution of Packet Sizes
Number of Packets
Packet Size (bytes)
0
100
200
300
400
0
200
400
600
800
1000
1200
1400

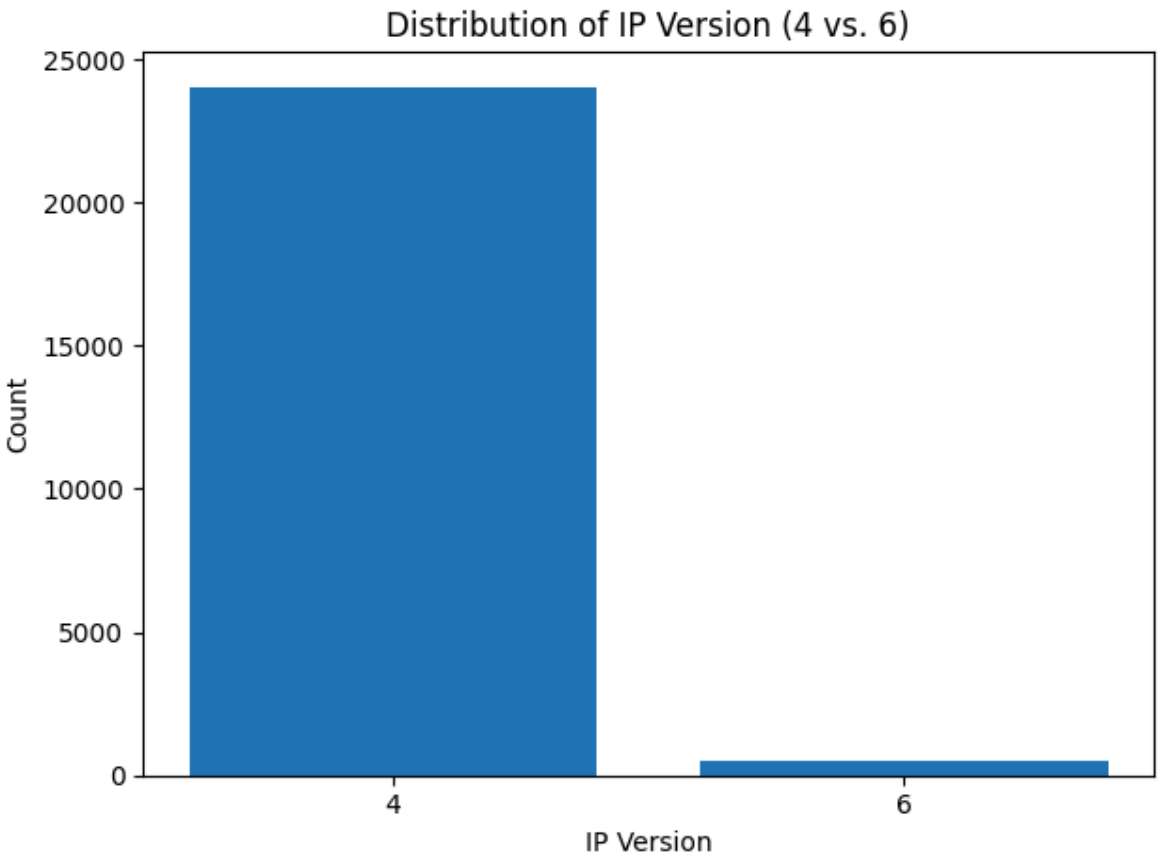

Top 20 Destination Ports
Number of Packets
Destination Port
0
100
200
300
400
500
443
55358
55367
55339
55292
55324
57924
55382
55372
55316
55325
55346
55348
55102
55104
58269
55344
55012
55295
55297

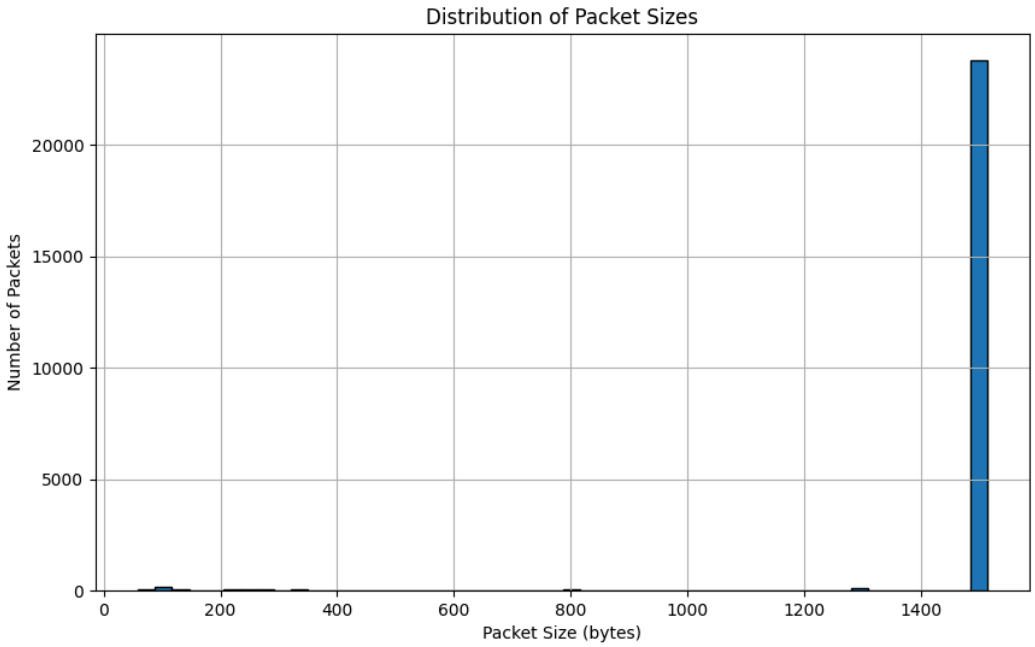

Top 5 Destination IP Addresses
Frequency
600
500
400
300
200
100
0
192.168.20.132
204.79.197.203
20.42.73.31
142.250.181.234
142.250.180.99
Destination IP Address

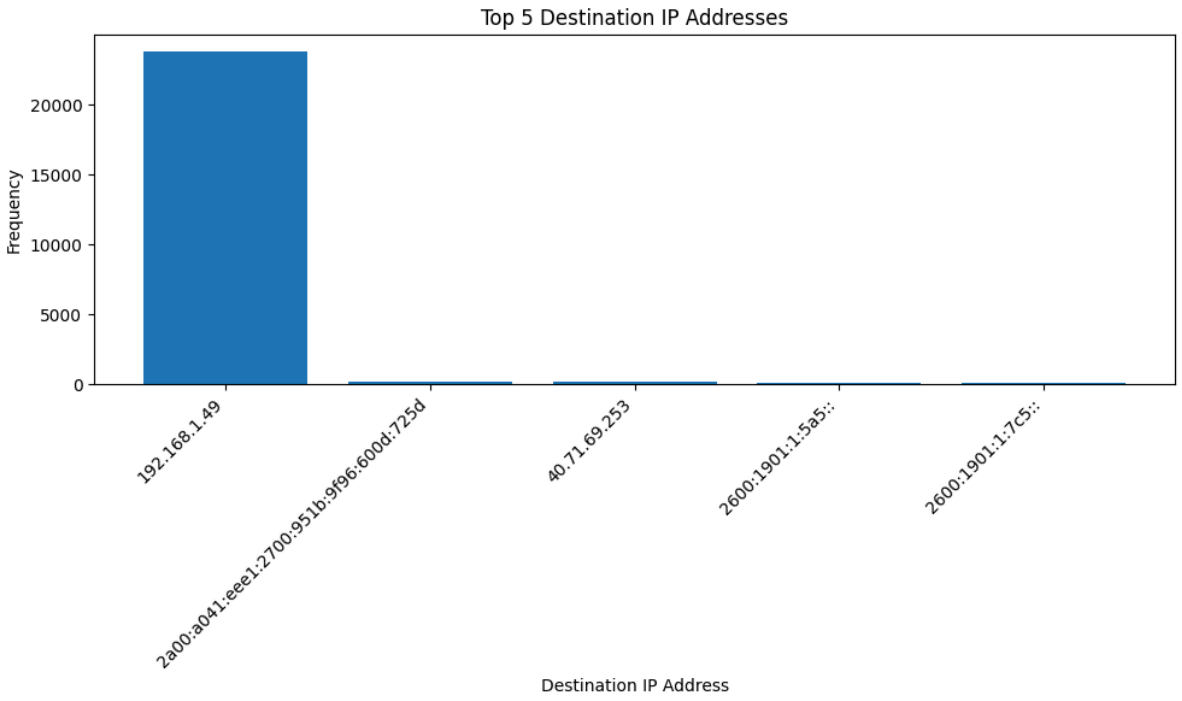

Upstream vs Downstream Traffic
Total Bytes
350000
300000
250000
200000
150000
100000
50000
0
334,153
299,663
Upstream
Downstream

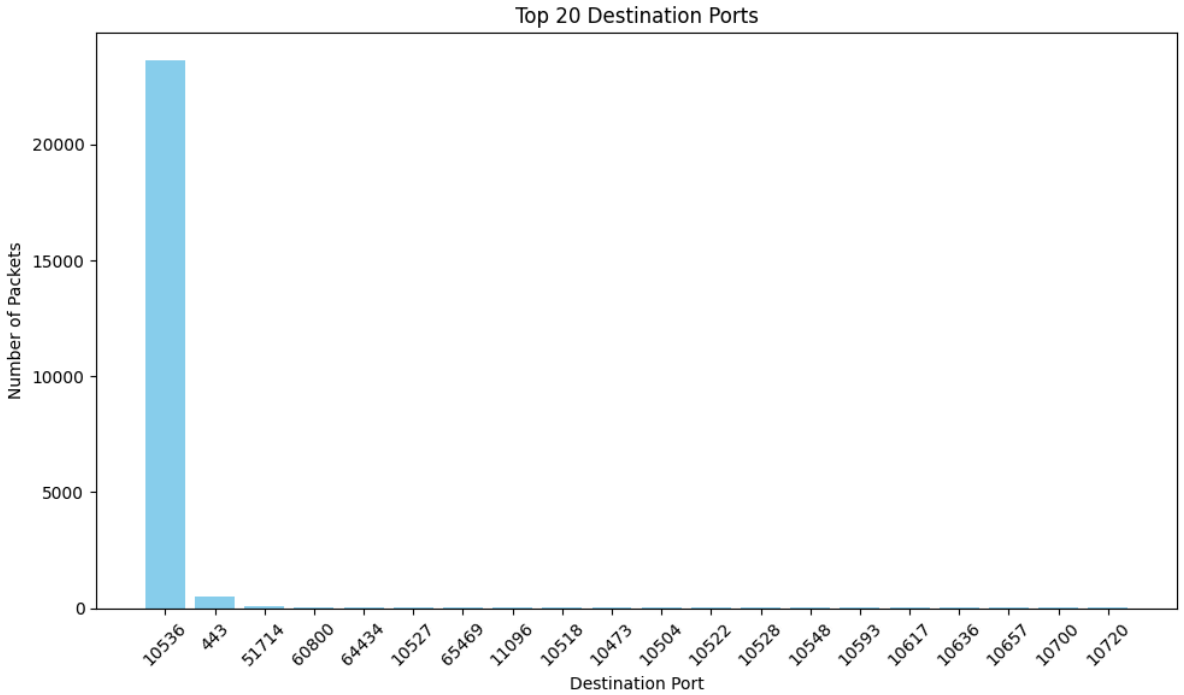
spotify

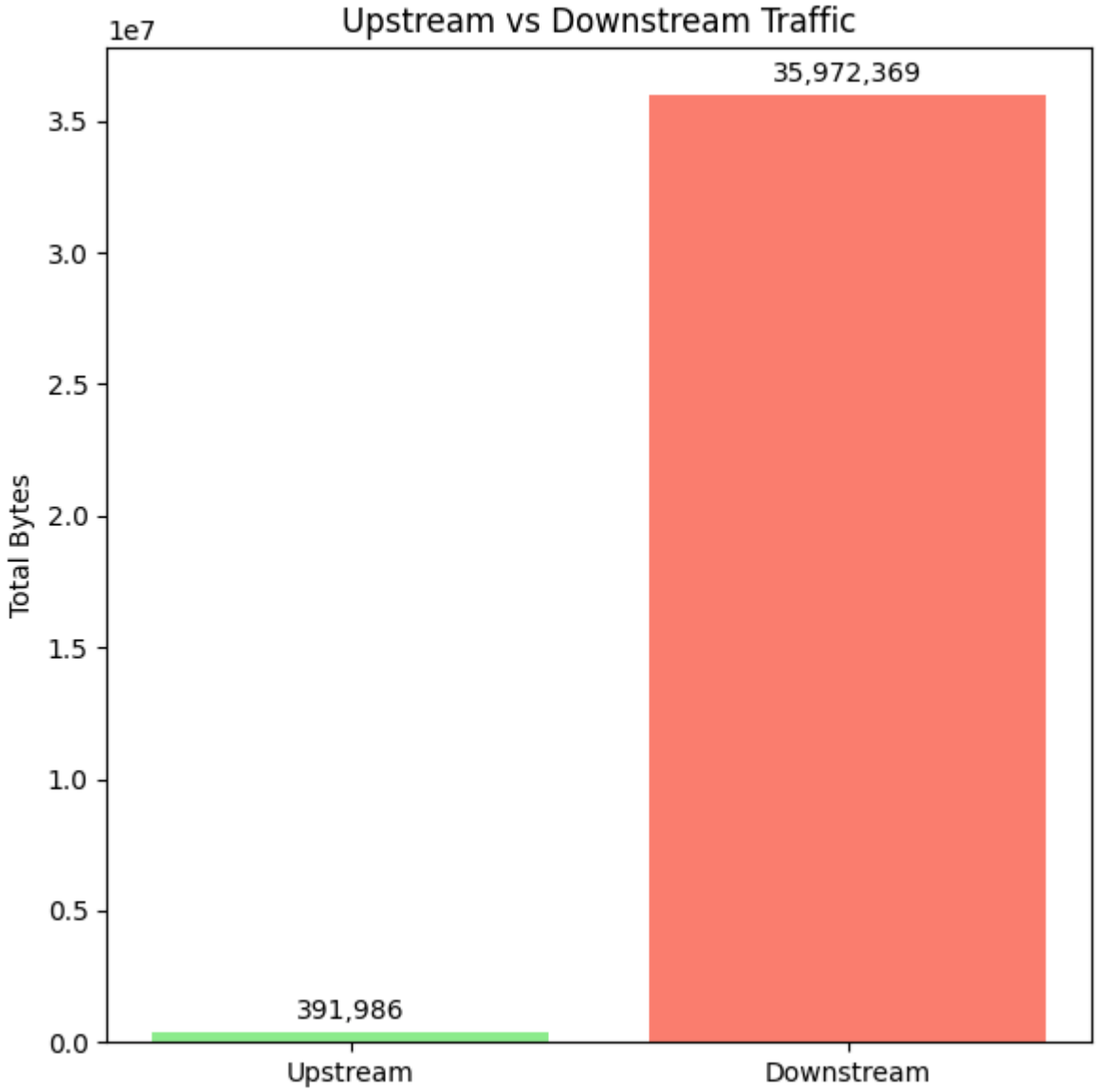

Distribution of Inter-Arrival Times (<= 99th percentile)
Frequency
25000
20000
15000
10000
5000
0
0.000
0.005
0.010
0.015
0.020
0.025
Inter-Arrival Time (seconds)


Distribution of IP Version (4 vs. 6)
Count
25000
20000
15000
10000
5000
0
4
6
IP Version

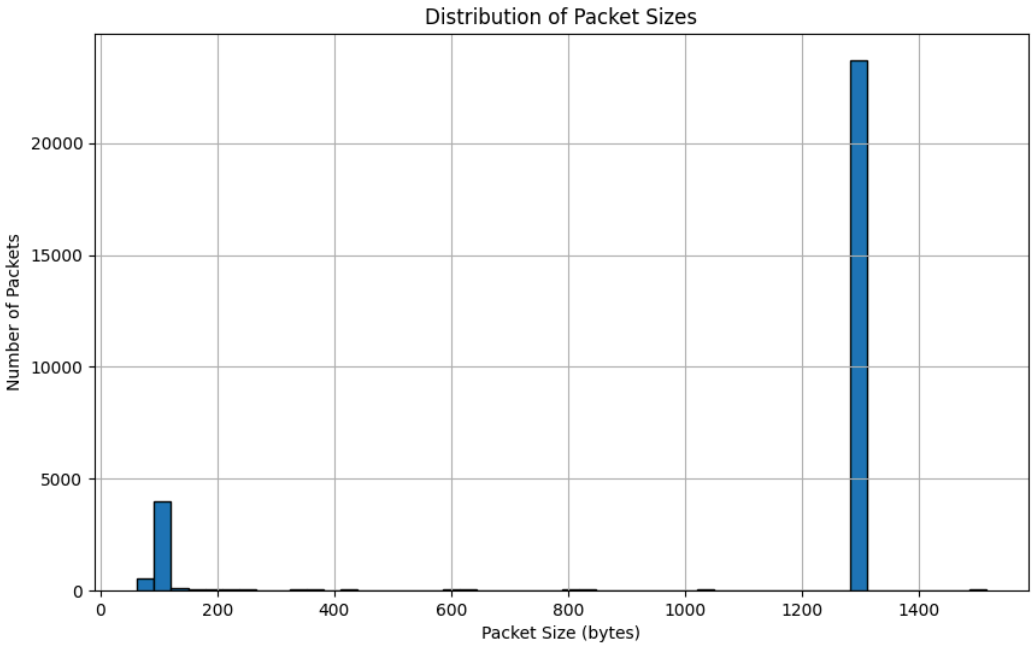

Distribution of Packet Sizes
Number of Packets
0
5000
10000
15000
20000
0
200
400
600
800
1000
1200
1400
Packet Size (bytes)

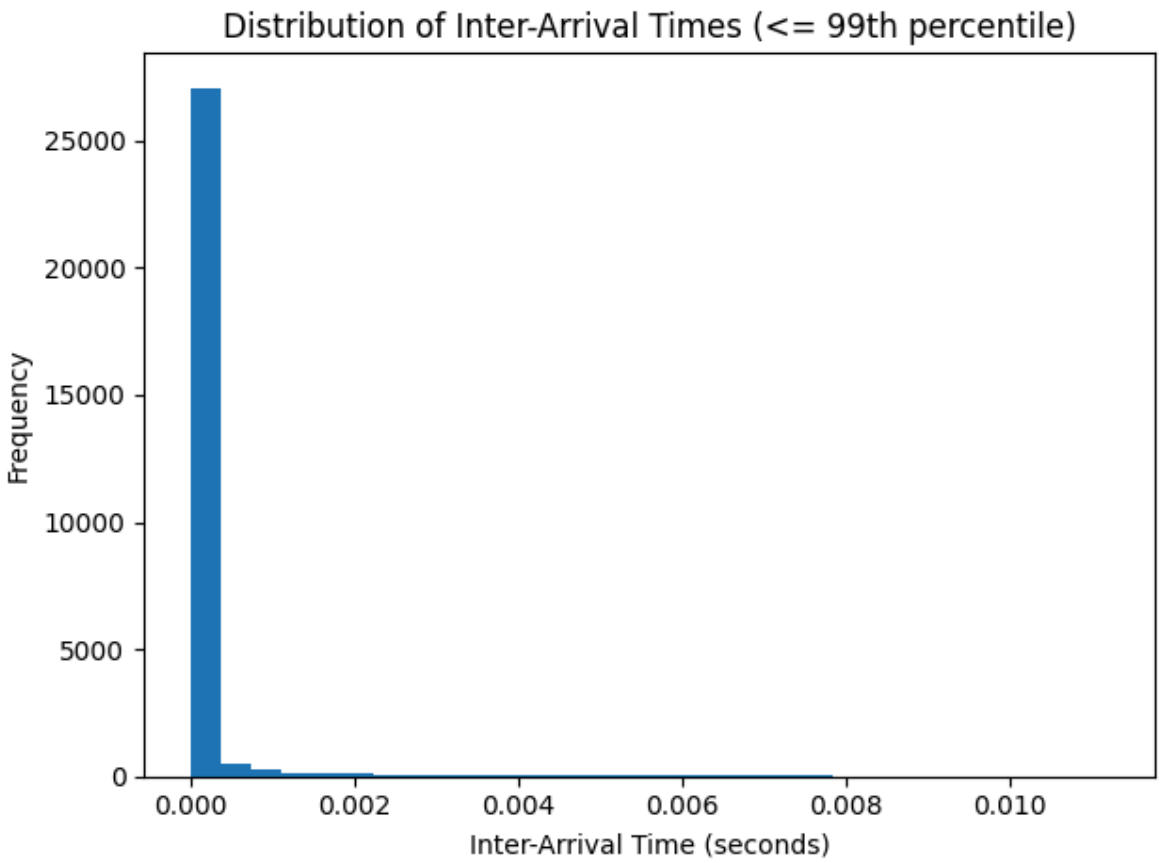

Top 5 Destination IP Addresses
Frequency
0
5000
10000
15000
20000
192.168.1.49
2a00:a041:eee1:2700:951b:9f96:600d:725d
40.71.69.253
2600:1901:1:5a5::
2600:1901:1:7c5::
Destination IP Address

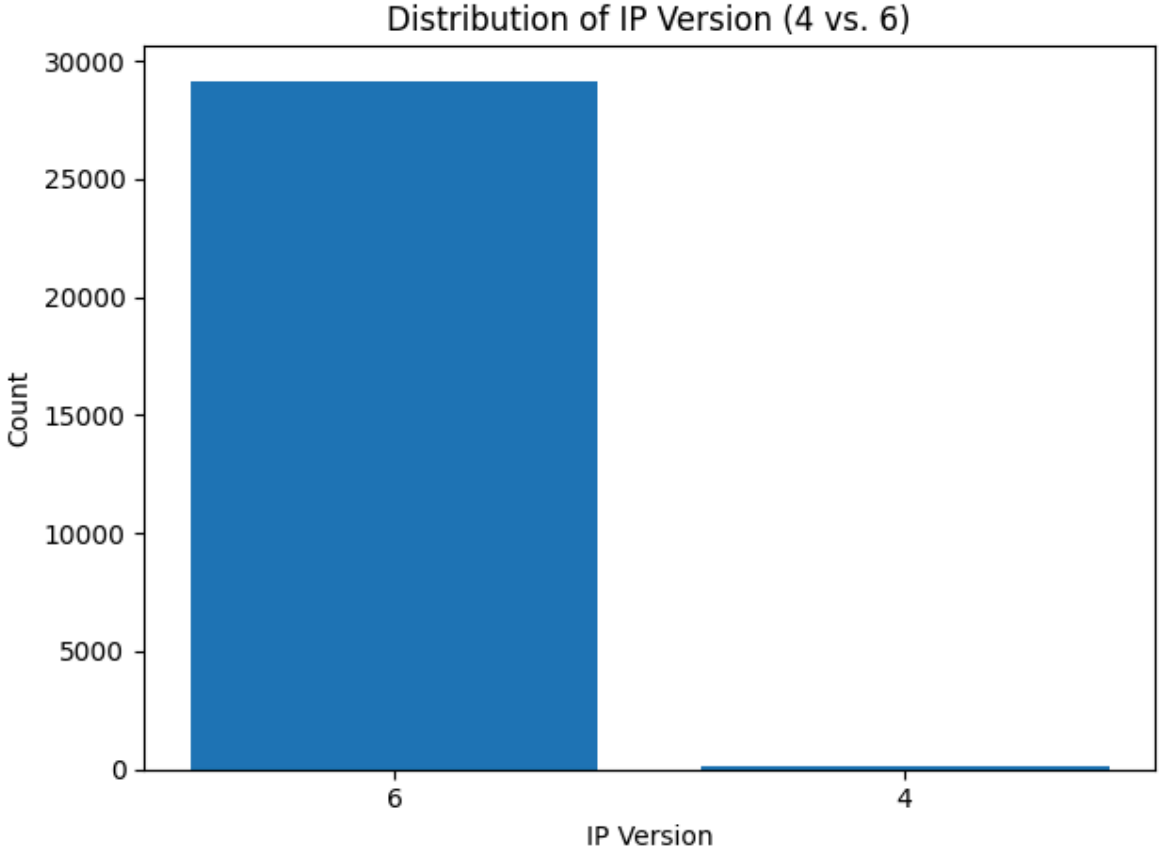

Top 20 Destination Ports
Number of Packets
0
5000
10000
15000
20000
10536
443
51714
60800
64434
10527
65469
11096
10518
10473
10504
10522
10528
10548
10593
10617
10636
10657
10700
10720
Destination Port

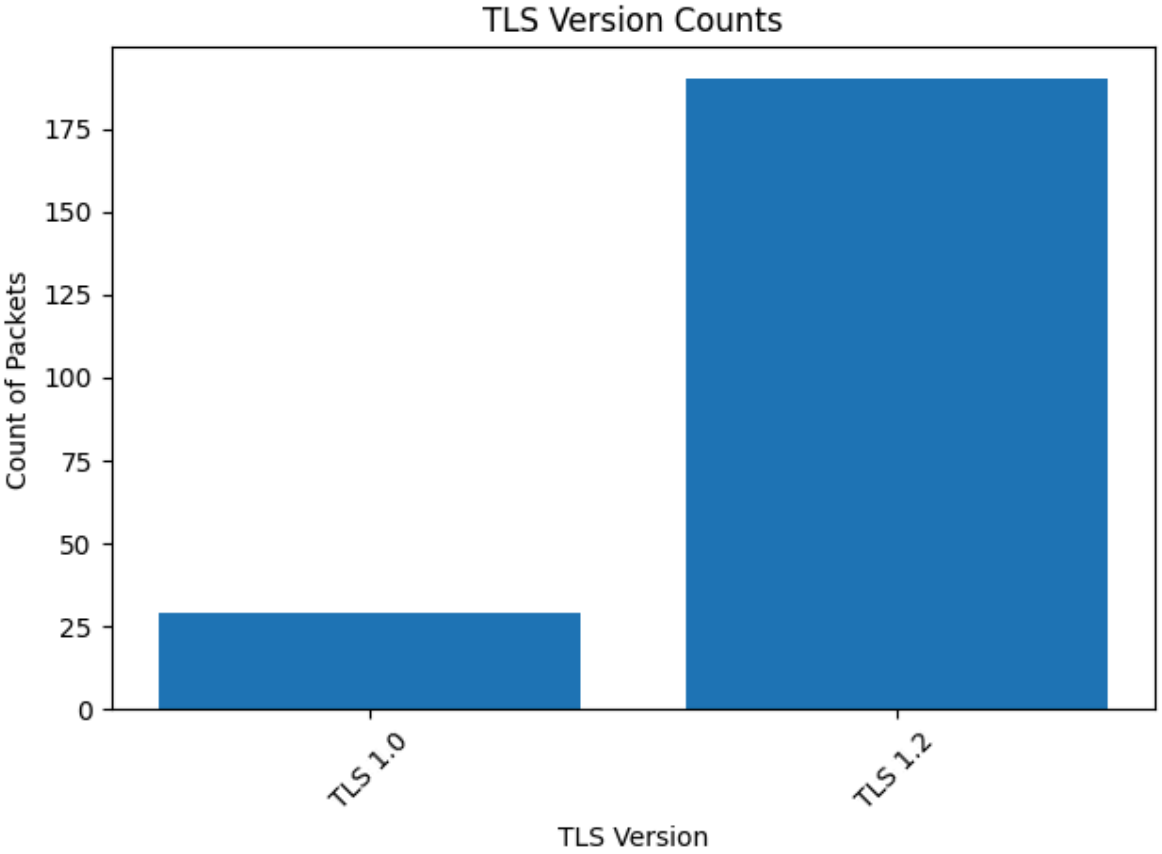

Upstream vs Downstream Traffic
1e7
35,972,369
391,986
Total Bytes
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Upstream
Downstream

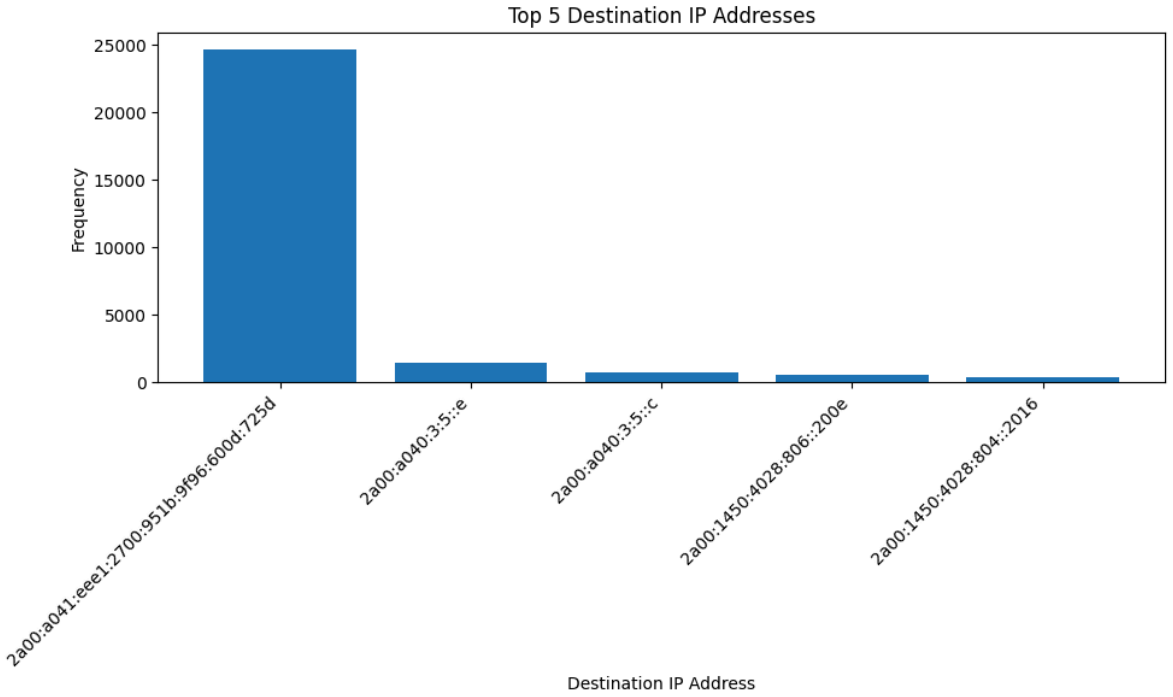
YOUTUBE


Distribution of Packet Sizes
Number of Packets
0
5000
10000
15000
20000
0
200
400
600
800
1000
1200
1400
Packet Size (bytes)

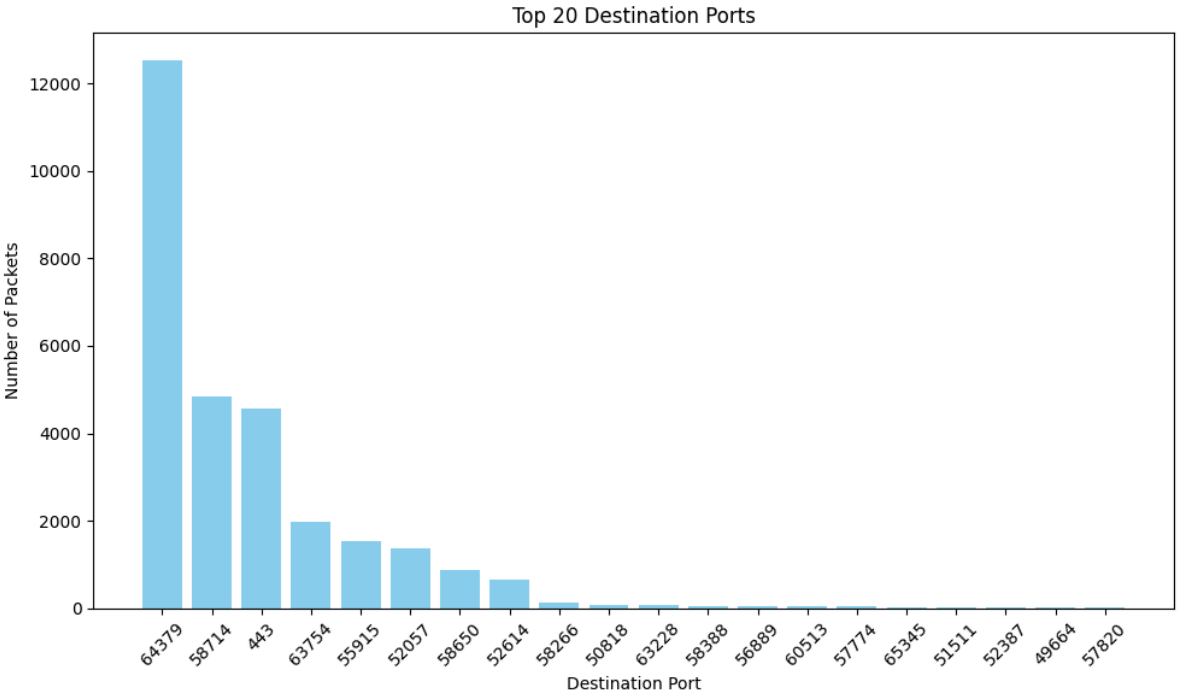

Distribution of Inter-Arrival Times (<= 99th percentile)
Frequency
0
5000
10000
15000
20000
25000
0.000
0.002
0.004
0.006
0.008
0.010
Inter-Arrival Time (seconds)

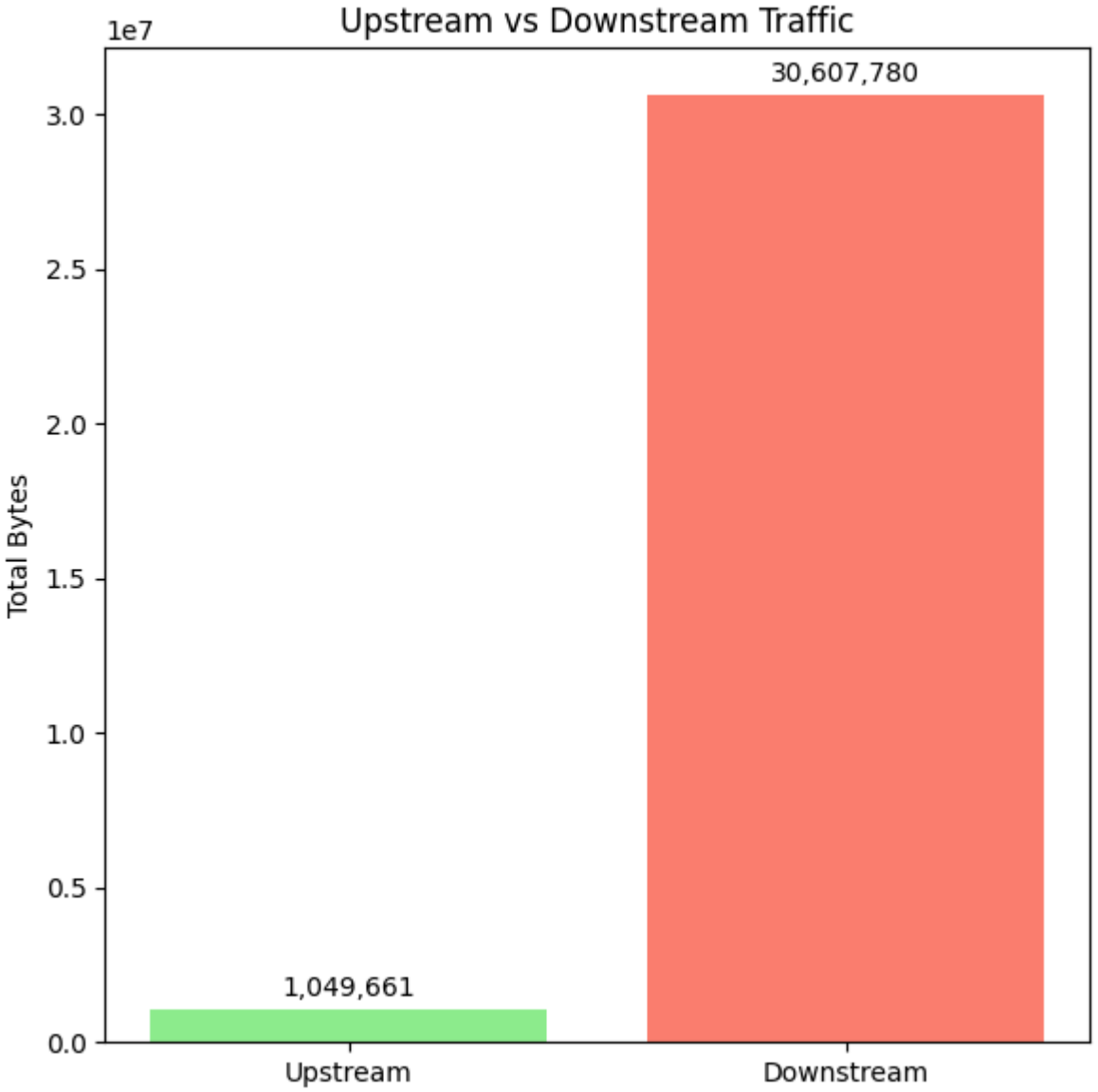

Distribution of IP Version (4 vs. 6)
30000
25000
20000
15000
10000
5000
0
Count
6
4
IP Version


TLS Version Counts
175
150
125
100
75
50
25
0
Count of Packets
TLS 1.0
TLS 1.2
TLS Version

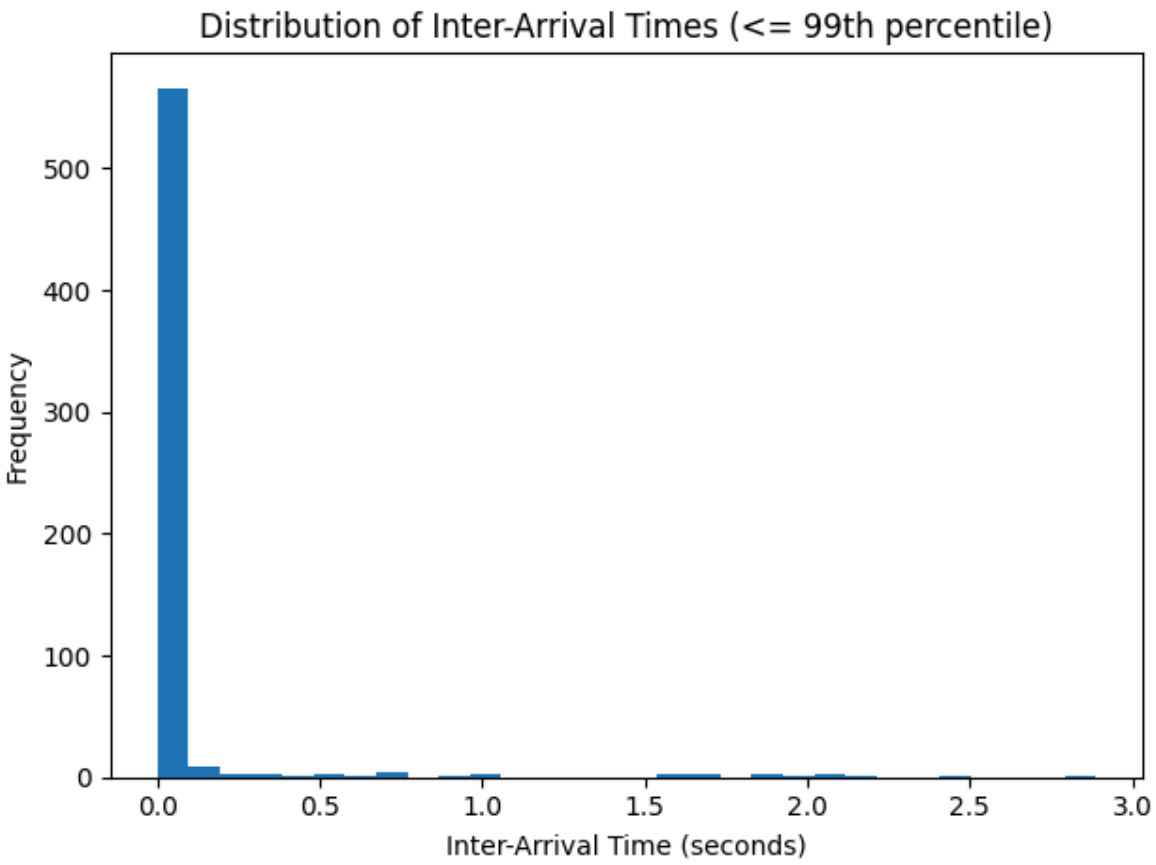

Top 5 Destination IP Addresses
Frequency
25000
20000
15000
10000
5000
0
2a00:a041:eee1:2700:951b:9f96:600d:725d
2a00:a040:3:5::e
2a00:a040:3:5::c
2a00:1450:4028:806::200e
2a00:1450:4028:804::2016
Destination IP Address

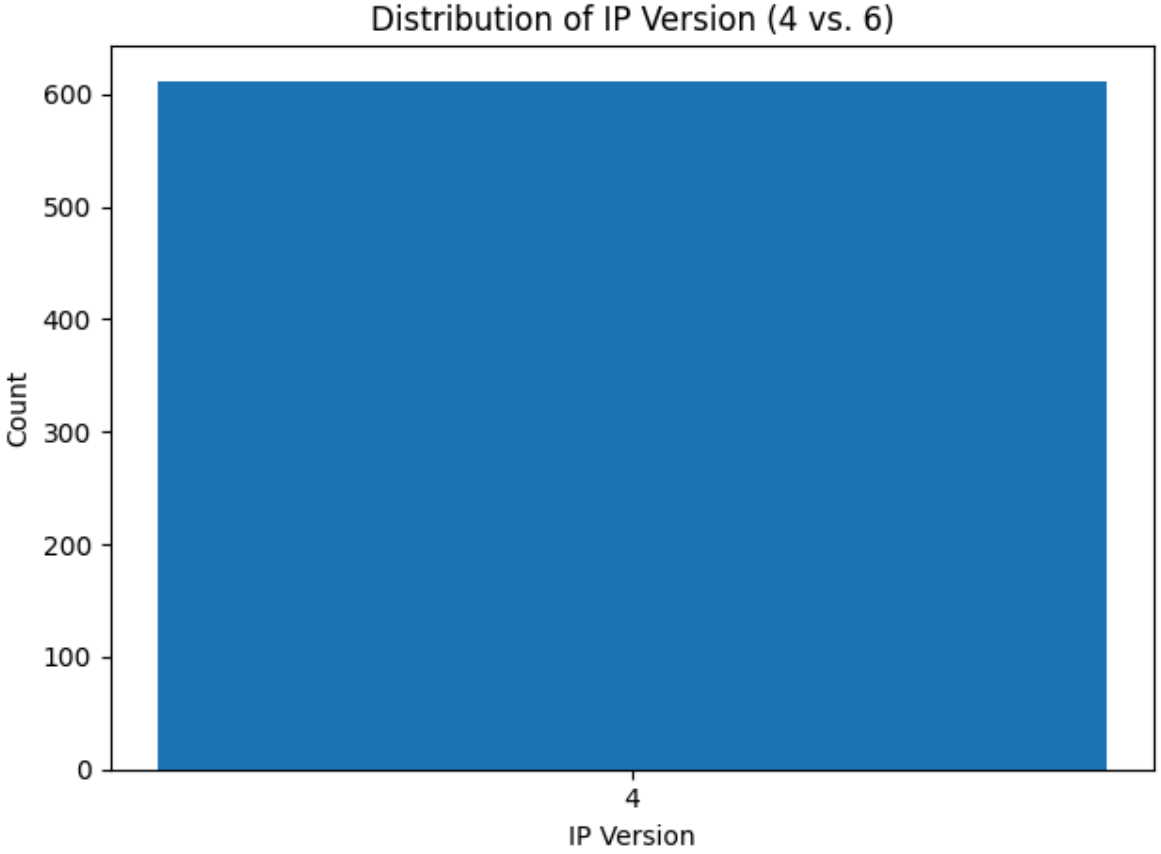
D

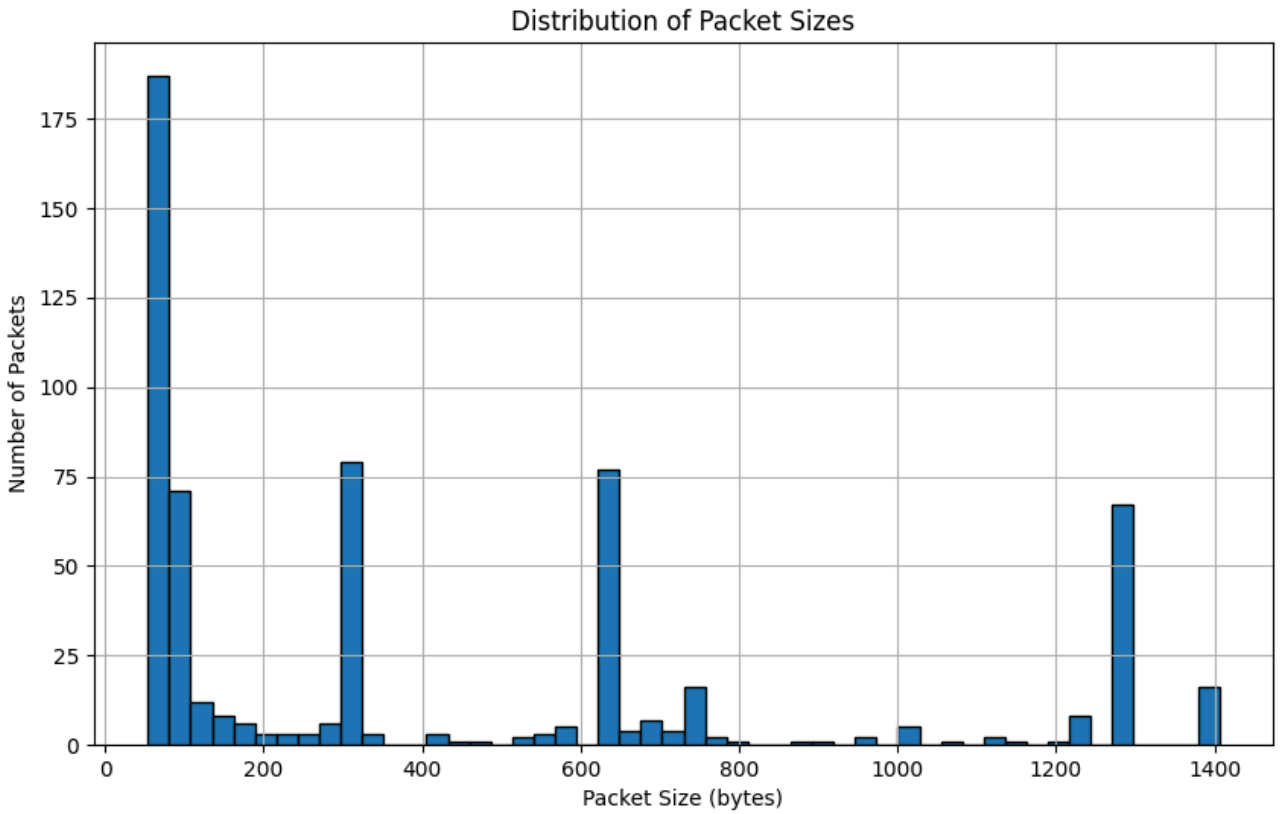

Top 20 Destination Ports
Number of Packets
0
2000
4000
6000
8000
10000
12000
64379
58714
443
63754
55915
52057
58650
52614
58266
50818
63228
58388
56889
60513
57774
65345
51511
52387
49664
57820
Destination Port

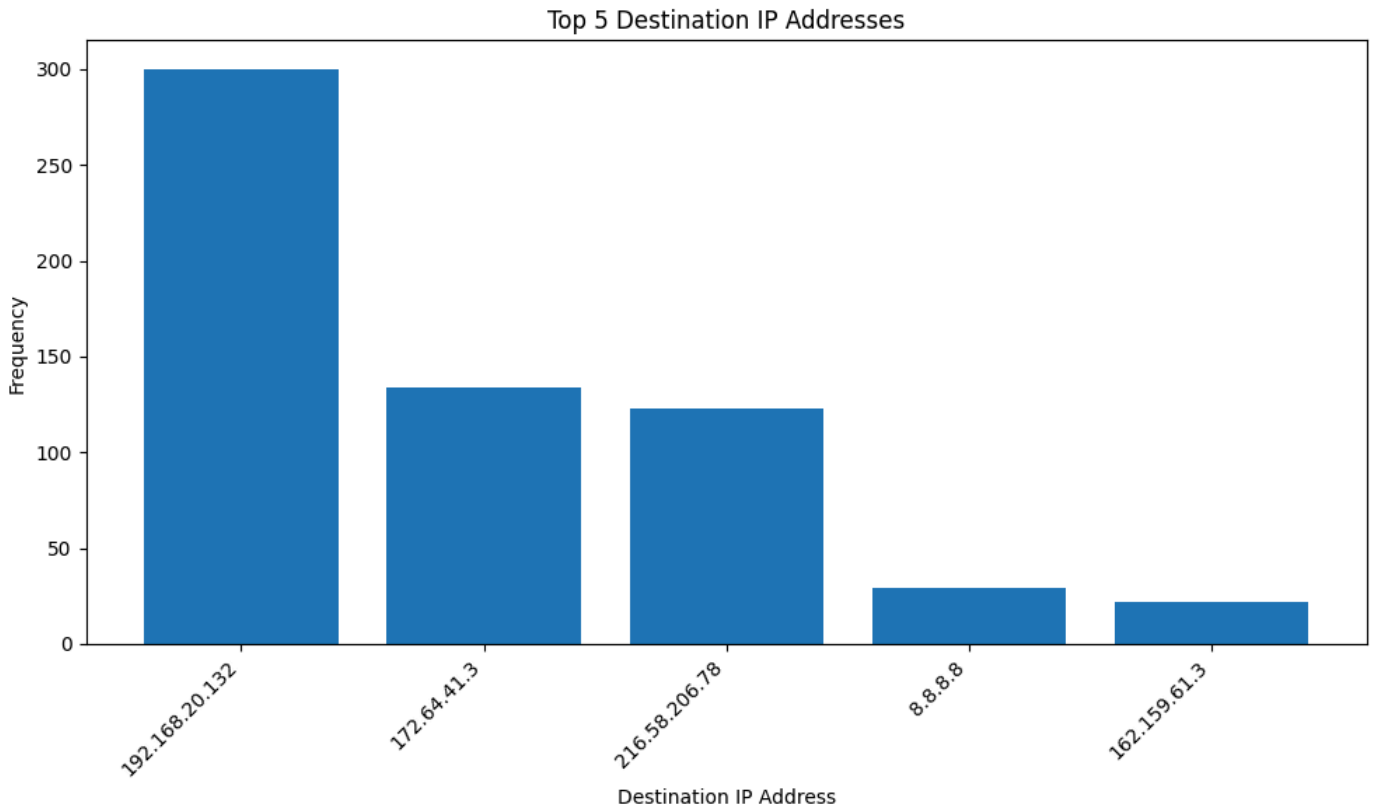

Upstream vs Downstream Traffic
1e7
30,607,780
1,049,661
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Total Bytes
Upstream
Downstream

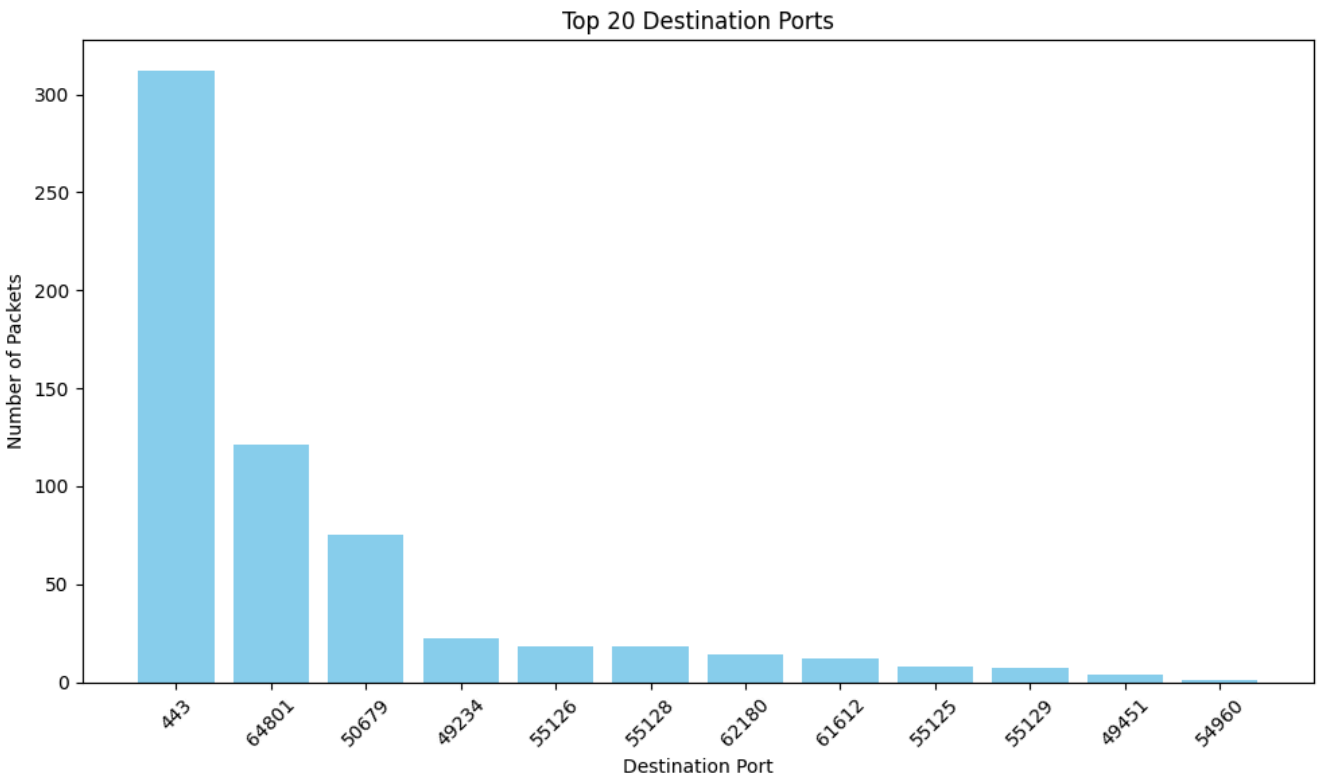
chrome

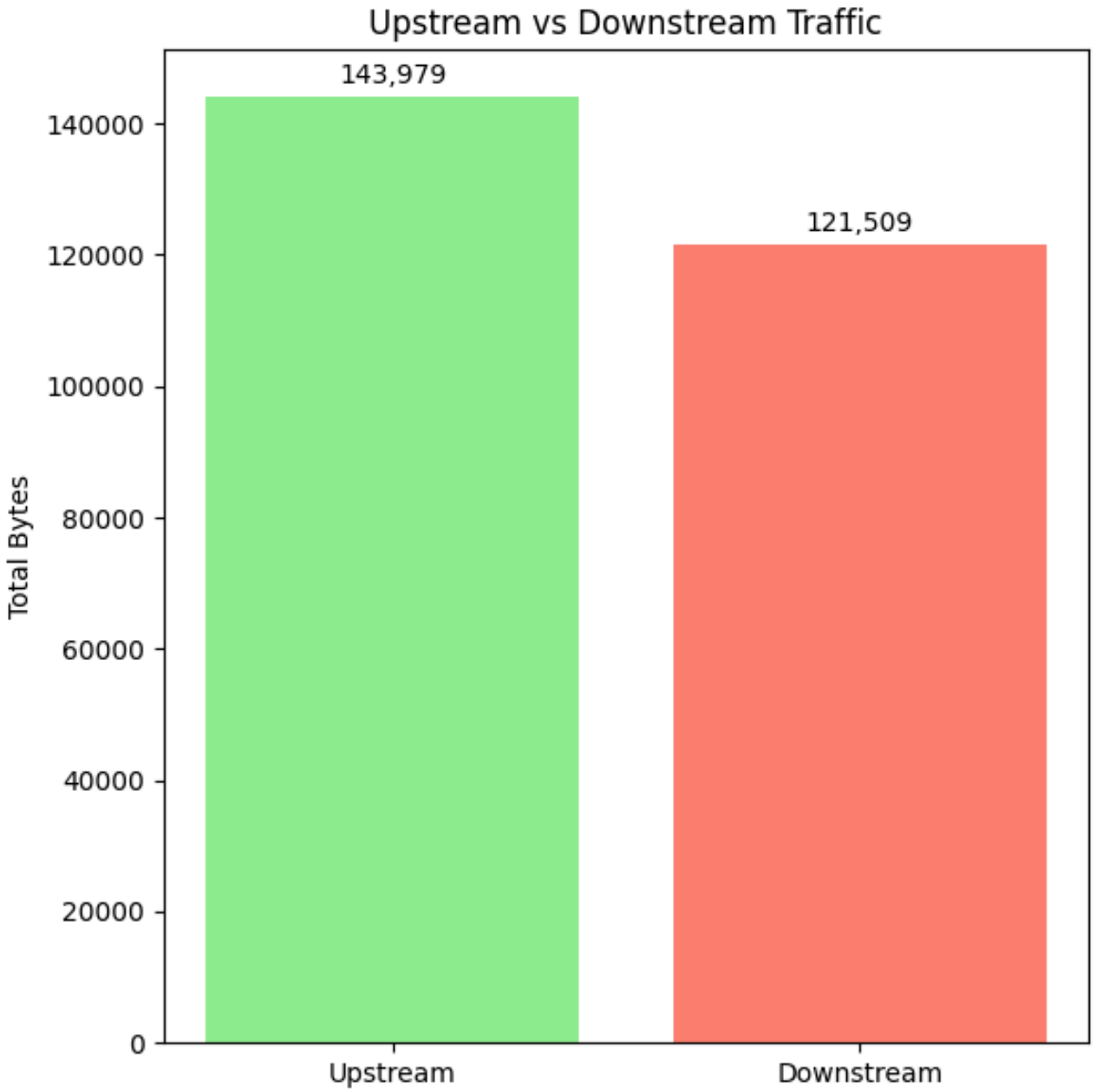

Distribution of Inter-Arrival Times (<= 99th percentile)
Frequency
500
400
300
200
100
0
0.0
0.5
1.0
1.5
2.0
2.5
3.0
Inter-Arrival Time (seconds)


Distribution of IP Version (4 vs. 6)
Count
600
500
400
300
200
100
0
4
IP Version


Distribution of Packet Sizes
Number of Packets
175
150
125
100
75
50
25
0
0
200
400
600
800
1000
1200
1400
Packet Size (bytes)


Top 5 Destination IP Addresses
Frequency
300
250
200
150
100
50
0
192.168.20.132
172.64.41.3
216.58.206.78
8.8.8.8
162.159.61.3
Destination IP Address


Top 20 Destination Ports
Number of Packets
300
250
200
150
100
50
0
443
64801
50679
49234
55126
55128
62180
61612
55125
55129
49451
54960
Destination Port


Upstream vs Downstream Traffic
143,979
121,509
Total Bytes
0
20000
40000
60000
80000
100000
120000
140000
Upstream
Downstream