מגישים :

ערן לוי - 311382360

דביר ביטון - 318765856

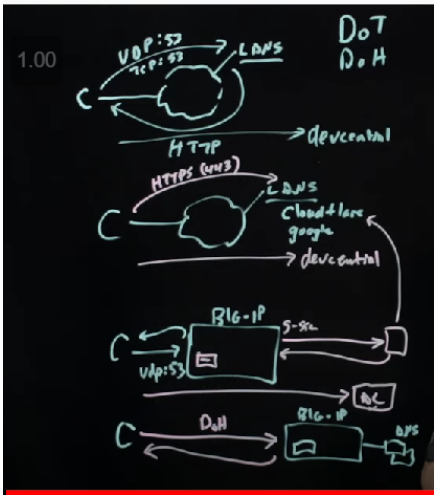
קישור לגיט המכיל את כל הקבצים המלאים -
https://github.com/dvirBiton1/netWork-Ex4

לשים לב שיש בגיט תיקיות עבור הקובץ 10mb ועבור 1mb התמונות והזמנים נכונים אך בהדפסות כתוב 1mb במקום 10mb. כאן בתשובות התייחסו רק לקובץ 1mb. מכיוון שהקובץ של 10mb לא נתמך כבר מ 25% איבוד.

חלק א' - DoH

DNS over HTTPS

הינה שיטה חדשה יותר המוצעת לשימוש. כמו שמרמז השם, זוהי שיטת תשאול DNS בחיבור HTTPS מאובטח.



התמונה הזאת עוזרת להבין את ההבדל העיקרי בין DoH לבין dns רגיל.
בחלק הראשון של התמונה אנו רואים את dns הרגיל שבעצם אדם מבקש משרתי ה dns היכן נמצא הכתובת אותה הוא מבקש.
אחרי זה אנחנו רואים את DoH שרעיונה העיקרי הוא בעצם להפעיל את dns באמצעות https וכך החיבור הרבה יותר מאובטח, על תמונה זאת אנחנו נסתמך בתשובות הבאות.

1. הציגו יתרון אחד לשימוש ב-DoH והסבירו אותו (כמובן, מעבר לעובדה שהוא מאובטח ומוצפן)

תשובה:

- היתרון הגדול של doh, זה שהוא עובד על פני http ולכן הוא מקבל את כל יתרונותיו למשל: אם הוא בhttp2 אז הוא "ידחוף" לנו. וכו כן את כל שאר הייתרונות של http. (העברה paraleel…)

2. הציגו והסבירו על שני חסרונות לשימוש בשיטת DoH לעומת DNS הרגיל

תשובה:

החסרונות הם:

- DOH מחליש את אבטחת הסייבר(מכיוון שיש הרבה דעות חלקות באינטרנט יכול להיות שמנקודת מבט ראשונית זה יראה הזוי שdoh מחליש אבטחה כי כל רעיונו זה הגביר אבטחה).
  מומחים רבים אומרים שהפרוטוקול משפר מאות פתרונות אבטחת סייבר, שיהפכו חסרי תועלת ברגע שמשתמשים יתחילו להשתמש ב-DoH בתוך הדפדפנים שלהם, מה שמסמא את כלי האבטחה מלראות מה המשתמשים עושים.
  והיו מומחים רבים שהזהירו על הנושא הזה, שקולם לא נשמע מכיוון בגלל אלו שטוענים ש-DoH הוא הדבר הגדול ביותר.
  כאשר פרוטוקול ה-DNS מוצפן, ארגון לא יכול עוד להשתמש בנתונים של שאילתת DNS (סוג שאילתה, תגובה, IP מקורי וכו') כדי לדעת אם משתמש מנסה לגשת לדומיין ידוע שגוי, שלא לדבר על הפעלת חסימה או הפנייה מחדש פעולה בנושא.
- DOH לא מונע למעשה מעקב אחר משתמשי ISPS
  אחת הנקודות העיקריות שתומכי DoH התברברו עליהן בשנה האחרונה היא ש-DoH מונעת מספקיות האינטרנט לעקוב אחר בקשות ה-DNS של המשתמשים, ומכאן מונעת מהם לעקוב אחר הרגלי התנועה באינטרנט של המשתמשים.
  זה נכון DoH מונע מ-ISP לצפות בבקשות ה-DNS של משתמש.
  עם זאת, DNS אינו הפרוטוקול היחיד המעורב בגלישה באינטרנט. יש עדיין אינספור נקודות נתונים אחרות שספקי שירותי אינטרנט יכולים לעקוב אחריהם כדי לדעת לאן משתמש הולך.
  כל מי שאומר ש-DoH מונע מ-ISP לעקוב אחר משתמשים או משקר או לא מבין איך פועלת תעבורת אינטרנט.
  אם משתמש ניגש לאתר שנטען באמצעות HTTP, השימוש ב-DoH הוא חסר טעם, מכיוון ש-ISP עדיין יידע לאיזו כתובת URL המשתמש ניגש פשוט על ידי הסתכלות על בקשות ה-HTTP הפשוטות.
  יתר על כן, ספקי האינטרנט ממילא יודעים הכל על התעבורה של כולם. לפי התכנון, הם יכולים לראות לאיזו כתובת IP המשתמש מתחבר בעת גישה לאתר.
- עוד חסרון שיש לנו הוא למשל כאשר אני כן רוצה לעקוב אני לא יוכל, למשל אחרי עובדים בחברה שלי. בקרת הורים וכו'.

3. בחרו אחד מהחסרונות משאלה (2), הציעו דרך למתן\לעקוף\לפתור חיסרון זה והסבירו אותה.

תשובה:

העצה היא שחברות צריכות לבחון שיטות חלופיות לחסימת תעבורה יוצאת, פתרונות שאינם מסתמכים רק על נתוני DNS, אך הדבר יגרור מאמץ כספי וזמן לעדכון מערכות, דבר שארגונים רבים לא יהיו מוכנים לעשות. אבל זה קצת בעיה שלהם כי אם אתה רוצה לעקוב אחרי עובדים בחברה שלך, תמצא אתה פתרון לזה, אנו מנסים לייעל בכלליות את כל האינטרנט ולא עבוד חברה ספציפית שרוצה לעקוב אחרי העובדים שלה . או אחרי הורה שרוצה לעשות חסימות לילד שלו.(עבור אותו הורה ישנם עוד הרבה אפשרויות לחסימה).

ישנן 4 דרכים בהן ניתן לשלב את שיטת ה-DoH באינטרנט שלנו:

1. מימוש DoH ברמת האפליקציות (לדוגמא: לעדכן את קוד הדפדפן כך שישלחו שאילתות דרך HTTPS)
2. מימוש DoH ברמת שרת proxy* ברשת (מהמחשב לשרת נשלח לפורט 53 והלאה, כבר 443)
3. מימוש DoH ברמת שרת proxy מקומי (על המכונה רץ שרת proxy)
4. התקנת plugin המממש DoH ברמת הגדרות המחשב ("מעכשיו, אתה שולח רק DoH")

כתבו השוואה בין כל ארבעת השיטות, בהשוואתכם הראו יתרונות וחסרונות לכל שיטה והציגו מהי, לדעתכם, השיטה המועדפת מבין הארבעה. כלומר, הציגו את השיטה בה, לדעתכם, היתרונות הגדולים ביותר לעומת החסרונות הקטנים ביותר.

<u>ההבדל בין 1 ל-2</u> הוא שב-1 המימוש עובד תחת הגדרות הדפדפן בלבד והשאילתות שלך בטוחות בזכות ספק האינטרנט שלך דרך הדפדפן.

עבור 2 , הוא די מזכיר את 1 (בעת גישה לדפי אינטרנט בדפדפן שלך)

אמנם לרוב שרתים פרטיים אלה מוצעים על ידי הספקים המציעים לך שרתים ללא עלות אשר אין אמון מלא בהם. אם אינך משלם עבור שירותים בכסף, ייתכן שתשלם בדרך אחרת - כמו נתונים פרטיים משלך גם אם פועל DoH - כתוצאה מכך נפגעת הפרטיות שלך.

לכן 1 עדיף על 2 במקרה הזה.

<u>ההבדל בין 1 ל-3</u> הוא זה שב-1 המימוש עובד תחת הגדרות דפדפן בלבד, עם זאת, בעוד שהשאילתות שלך בטוחות מספק מהאינטרנט שלך, עדיין ספקי DoH יכולים לעקוב לא משנה עד כמה הם נוקשים לגבי פרטיות.

לעומת זאת ב-3 שרת proxy מקומי שולח בקשות לרשימת ספקים ומסווה ביעילות את התעבורה שלך מכל ספק זר ולכן 3 מבטיח יותר הגנה.

<u>ההבדל בין 1 ל-4</u> הוא זה ש-1 עובד תחת הדפדפן בלבד.

בעוד שב-4 מדבר רק על כל התוכנות שנמצאות אצלנו במחשב כמו ZOOM, Skype או כל תוכנה תקשורתית אחרת שנמצאת במחשב שלנו.

במקרה הזה כל מקרה לגופו, a על הדפדפן ו-d הוא על התוכנות במחשב אז כל אחד לא מכסה את השני במקרה הזה אז אין העדפה.

ההבדל בין 2 ל-3 עבור 2, שרתים פרטיים אלה מוצעים על ידי הספקים המציעים לך שרתים ללא עלות אשר אין אמון בהם ובנוסף 2 פועל על הדפדפן בלבד.

אם כבר לממש DoH אז עם 3, הוא אמין ומספק FireWall לא רק עבור הדפדפן אלא כל שאילתת DNS שיוצאת מהמחשב ל-HTTPS.

ההבדל בין 2 ל-4 עבור 4, הוא ממש DoH עבור אפליקציות במחשב כמו skype בעוד ש-2 מספק DoH רק עבור הדפדפן, כלומר כל אחד מכסה איזור אחר ולכן אין מה להשוות.

ההבדל בין 3 ל-4 עבור 4 מימוש DoH עבור תוכנות במחשב בעוד ש-3 הוא שרת פרוקסי מקומי שמתרגם כל שאילתת DNS שיוצאת מהמחשב לHTTPS.

היינו בוחרים ב-3 להיות השיטה המועדפת עלינו כי היא יכולה לכסות את 1 ואת 2 איתה.

5. נניח שאנו ברשת שקיים בה איבוד פקטות (packet loss) באחוז לא ידוע ואנו רוצים לטעון דף שצריך 25 שאילתות כדי לבקש את כל המשאבים שבו. הציגו יתרון ברור שיש ל-DoH לעומת Do53. (רמז: מנגנון הקיים ב-TCP)

תשובה:

Do35 משתמש בפרוטוקול UDP

היתרון ששאילתות DoH שאבדו מסתמכות עליהן הן מדיניות השידור מחדש של פרוטוקול TCP הבסיסי ולא טיימר קבוע.

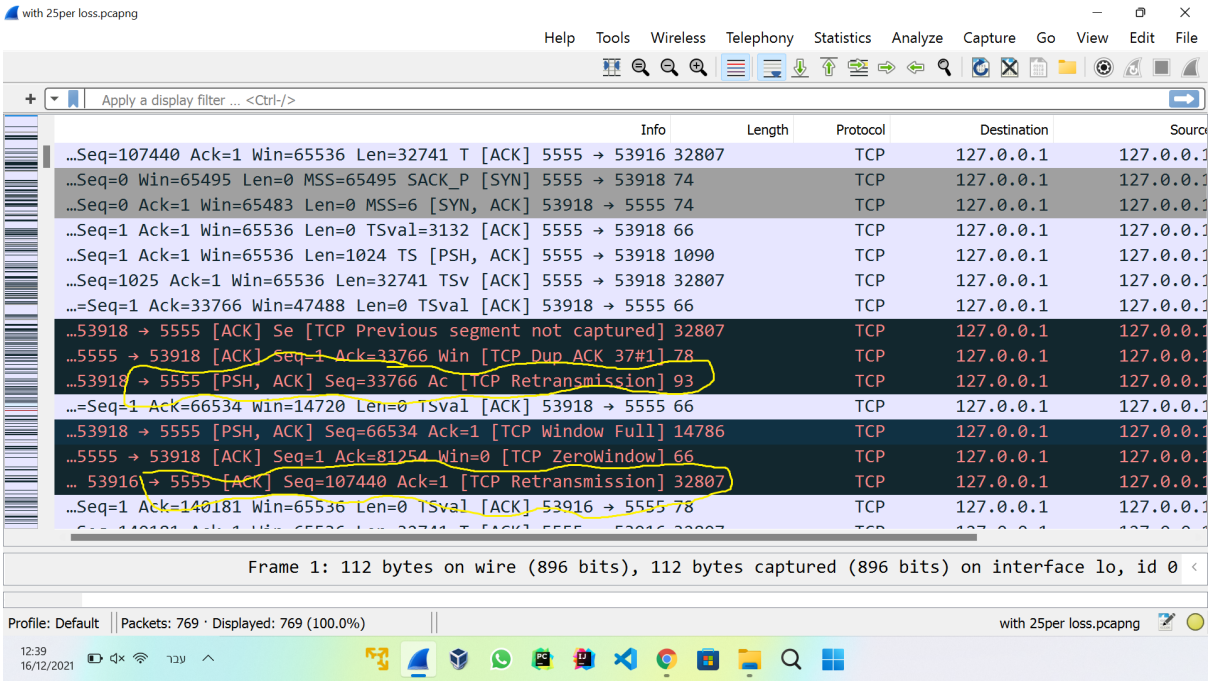
DoH בהשוואה לDo35 מאחר וDoH עובד עם TCP אז מופעל בו מנגנון TCP Fast Retransmit לפיכך DoH יוכל לשחזר במהירות רבה יותר שאילות DNS שאבדו בטעינת הדף מאשר Do35 שאין בו את האפשרות הזו.

חלק ב'

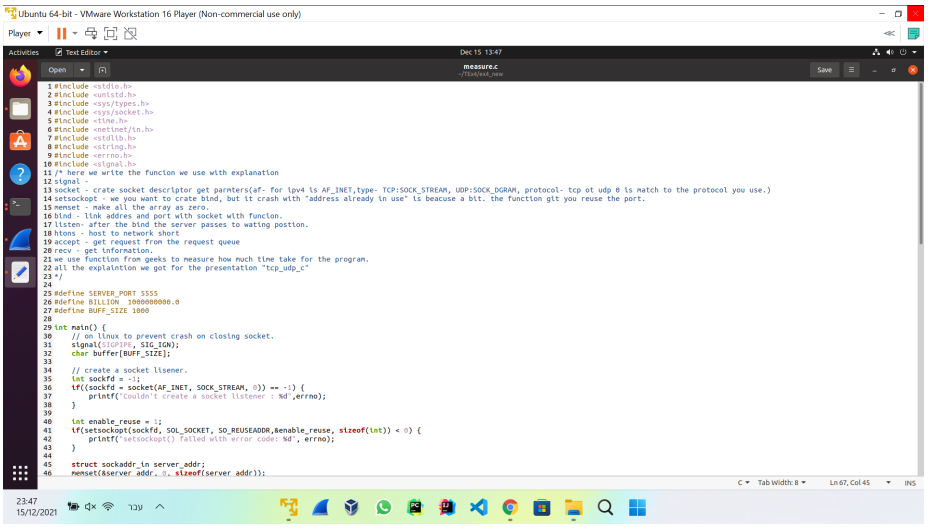
רשמנו הסברים כלליים על הפונקציות שעבדנו איתם בקוד. (ההסברים לקוחים המצגות של התרגול, והפונקציה של הזמן זה מאתר geeks).

נראה רק בכלליות תמונה שמראה שוורשארק את האיבוד של החבילות בכדי לראות את התיעודים של הווארשארק יש להיכנס לגיט שרשום למעלה.

צילום שאפשר לראות בוואשארק את הפעולה שגורמת לאיבוד חבילות בעצם קוראת שליחה חוזרת מכיוון שאנחנו בפרוטוקול tcp ולכן ככל שאנו עולים באחוזי האיבוד יקח לתוכנית יותר זמן לרוץ:



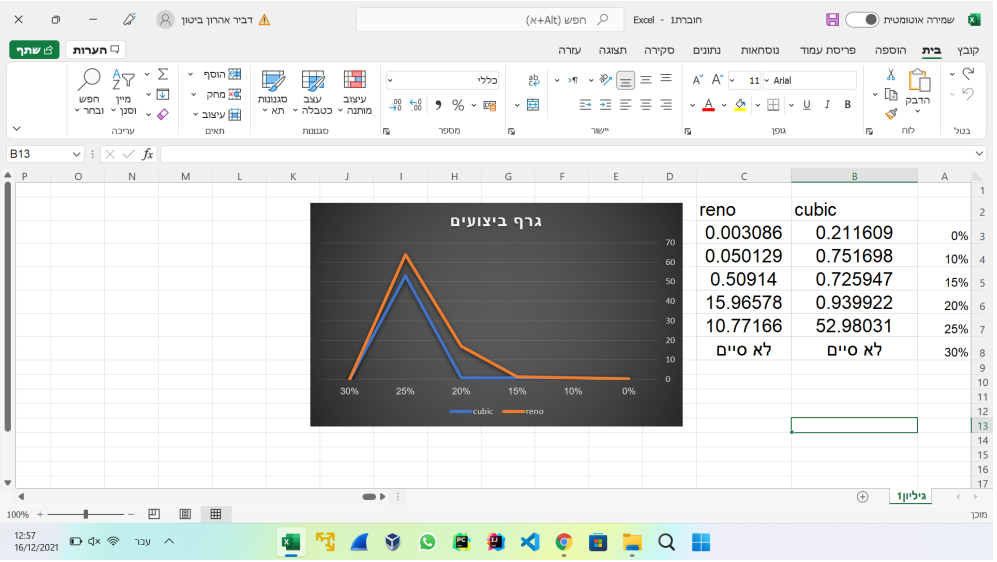
צילום של הסבר על הפונקציות:



טבלה שמסכמת את כל המקרים:

reno CC AVG Time	cubic CC AVG Time	packet Loss
0.003086	0.211609	0%
0.050129	0.751698	10%
0.509140	0.725947	15%
15.965781	0.939922	20%
10.771660	52.980310	25%
לא סיים	לא סיים	30%

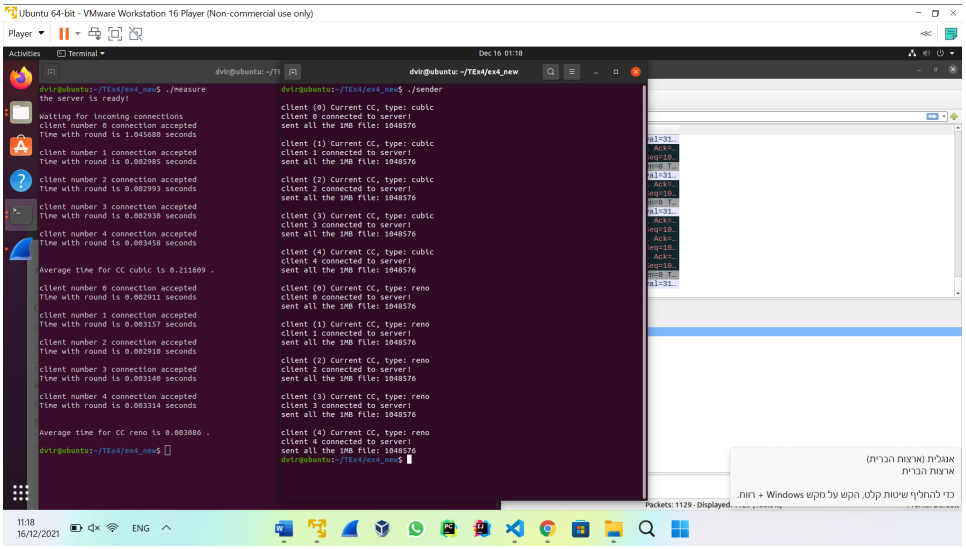
גרף:



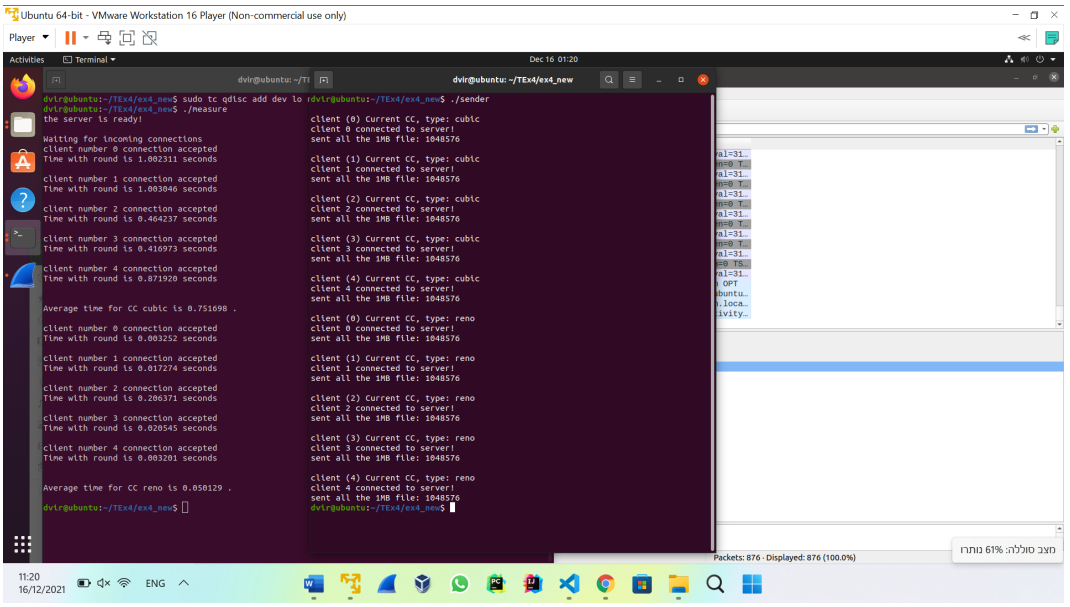
reno	cubic	
0.003086	0.211609	0%
0.050129	0.751698	10%
0.50914	0.725947	15%
15.96578	0.939922	20%
10.77166	52.98031	25%
לא סיים	לא סיים	30%

צילומי מסך::

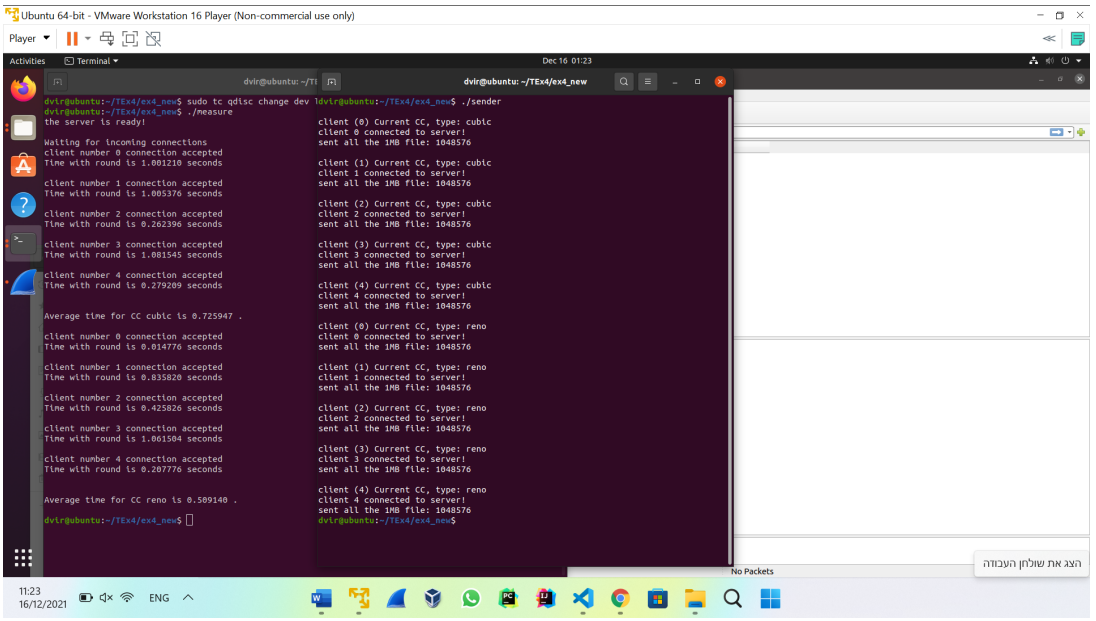
0% :



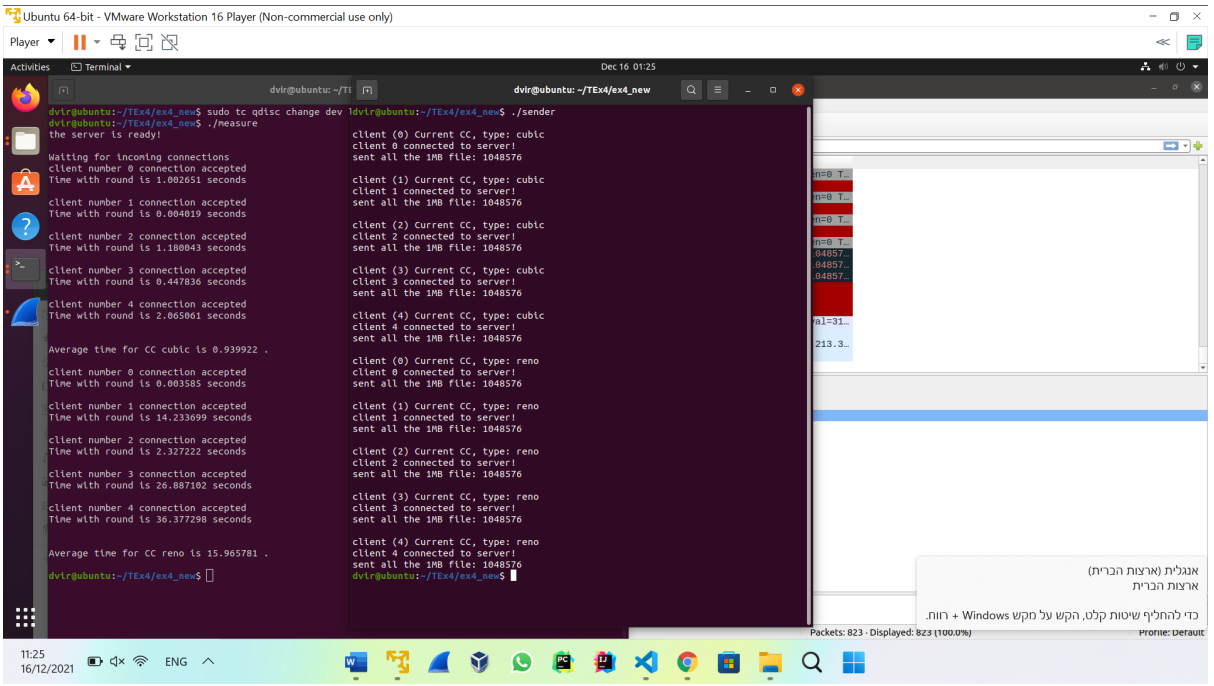
: 10%


Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Activities
Terminal
Dec 16 01:20
dvir@ubuntu: ~/TEx4/ex4_new
dvir@ubuntu:~/TEx4/ex4_new$ sudo tc qdisc add dev lo r
dvir@ubuntu:~/TEx4/ex4_new$ ./sender
dvir@ubuntu:~/TEx4/ex4_new$ ./measure
the server is ready!
Waiting for incoming connections
client number 0 connection accepted
Time with round is 1.002311 seconds
client number 1 connection accepted
Time with round is 1.003046 seconds
client number 2 connection accepted
Time with round is 0.464237 seconds
client number 3 connection accepted
Time with round is 0.416973 seconds
client number 4 connection accepted
Time with round is 0.871920 seconds
Average time for CC cubic is 0.751698 .
client number 0 connection accepted
Time with round is 0.003252 seconds
client number 1 connection accepted
Time with round is 0.017274 seconds
client number 2 connection accepted
Time with round is 0.206371 seconds
client number 3 connection accepted
Time with round is 0.020545 seconds
client number 4 connection accepted
Time with round is 0.003201 seconds
Average time for CC reno is 0.050129 .
client (0) Current CC, type: cubic
client 0 connected to server!
sent all the 1MB file: 1048576
client (1) Current CC, type: cubic
client 1 connected to server!
sent all the 1MB file: 1048576
client (2) Current CC, type: cubic
client 2 connected to server!
sent all the 1MB file: 1048576
client (3) Current CC, type: cubic
client 3 connected to server!
sent all the 1MB file: 1048576
client (4) Current CC, type: cubic
client 4 connected to server!
sent all the 1MB file: 1048576
client (0) Current CC, type: reno
client 0 connected to server!
sent all the 1MB file: 1048576
client (1) Current CC, type: reno
client 1 connected to server!
sent all the 1MB file: 1048576
client (2) Current CC, type: reno
client 2 connected to server!
sent all the 1MB file: 1048576
client (3) Current CC, type: reno
client 3 connected to server!
sent all the 1MB file: 1048576
client (4) Current CC, type: reno
client 4 connected to server!
sent all the 1MB file: 1048576
Packets: 876 · Displayed: 876 (100.0%)
מצב סוללה: 61% נותרו
11:20
16/12/2021
ENG

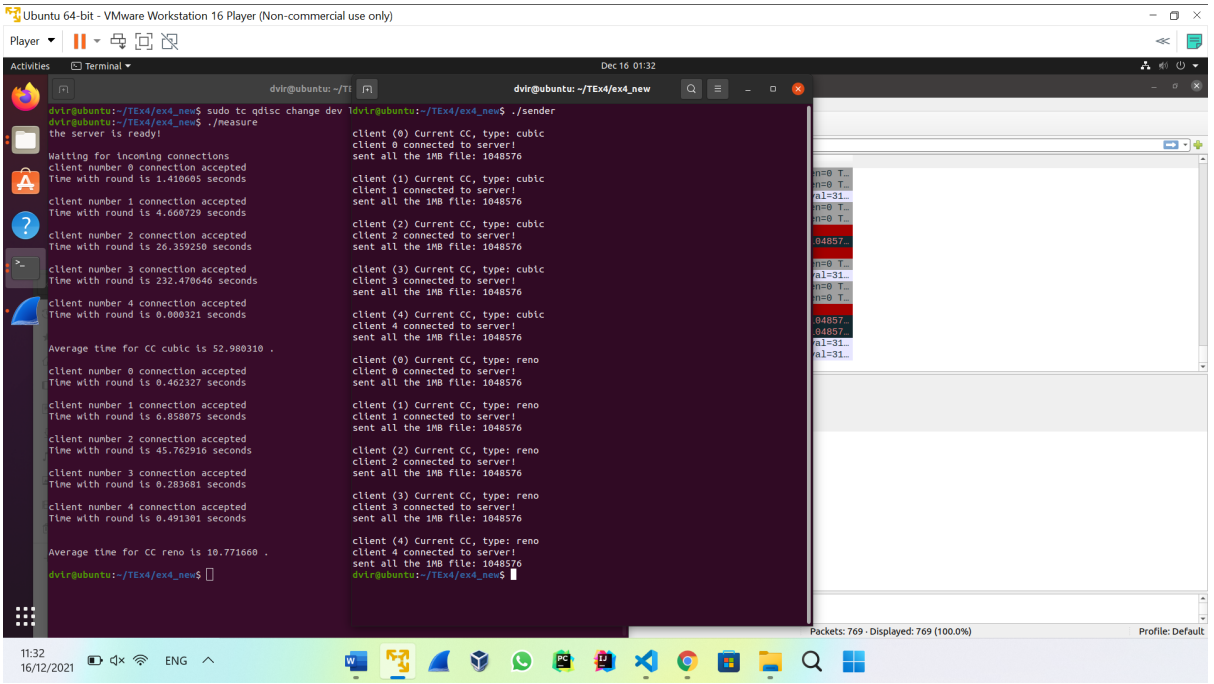
:15%


Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Activities
Terminal
Dec 16 01:23
dvir@ubuntu: ~/TEx4/ex4_new
dvir@ubuntu:~/TEx4/ex4_new$ sudo tc qdisc change dev l
dvir@ubuntu:~/TEx4/ex4_new$ ./sender
dvir@ubuntu:~/TEx4/ex4_new$ ./measure
the server is ready!
Waiting for incoming connections
client number 0 connection accepted
Time with round is 1.001210 seconds
client number 1 connection accepted
Time with round is 1.005376 seconds
client number 2 connection accepted
Time with round is 0.262396 seconds
client number 3 connection accepted
Time with round is 1.001545 seconds
client number 4 connection accepted
Time with round is 0.279209 seconds
Average time for CC cubic is 0.725947 .
client number 0 connection accepted
Time with round is 0.014776 seconds
client number 1 connection accepted
Time with round is 0.835820 seconds
client number 2 connection accepted
Time with round is 0.425826 seconds
client number 3 connection accepted
Time with round is 1.001504 seconds
client number 4 connection accepted
Time with round is 0.207776 seconds
Average time for CC reno is 0.509140 .
client (0) Current CC, type: cubic
client 0 connected to server!
sent all the 1MB file: 1048576
client (1) Current CC, type: cubic
client 1 connected to server!
sent all the 1MB file: 1048576
client (2) Current CC, type: cubic
client 2 connected to server!
sent all the 1MB file: 1048576
client (3) Current CC, type: cubic
client 3 connected to server!
sent all the 1MB file: 1048576
client (4) Current CC, type: cubic
client 4 connected to server!
sent all the 1MB file: 1048576
client (0) Current CC, type: reno
client 0 connected to server!
sent all the 1MB file: 1048576
client (1) Current CC, type: reno
client 1 connected to server!
sent all the 1MB file: 1048576
client (2) Current CC, type: reno
client 2 connected to server!
sent all the 1MB file: 1048576
client (3) Current CC, type: reno
client 3 connected to server!
sent all the 1MB file: 1048576
client (4) Current CC, type: reno
client 4 connected to server!
sent all the 1MB file: 1048576
No Packets
הצג את שולחן העבודה
11:23
16/12/2021
ENG

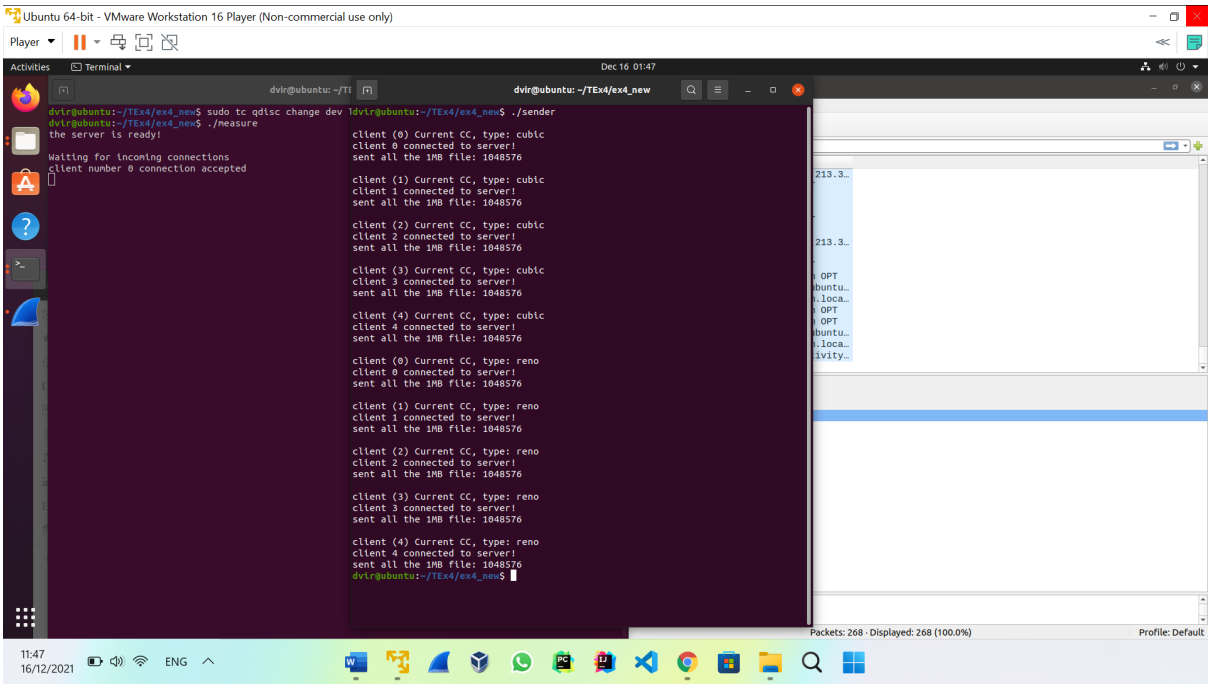
:20%


Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
Dec 16 01:25
dvir@ubuntu: ~/TEx4/ex4_new
dvir@ubuntu:~/TEx4/ex4_new$ sudo tc qdisc change dev l
dvir@ubuntu:~/TEx4/ex4_new$ ./measure
the server is ready!
Waiting for incoming connections
client number 0 connection accepted
Time with round is 1.002651 seconds
client number 1 connection accepted
Time with round is 0.004019 seconds
client number 2 connection accepted
Time with round is 1.180043 seconds
client number 3 connection accepted
Time with round is 0.447836 seconds
client number 4 connection accepted
Time with round is 2.065061 seconds
Average time for CC cubic is 0.939922 .
client number 0 connection accepted
Time with round is 0.003585 seconds
client number 1 connection accepted
Time with round is 14.233699 seconds
client number 2 connection accepted
Time with round is 2.327222 seconds
client number 3 connection accepted
Time with round is 26.887102 seconds
client number 4 connection accepted
Time with round is 36.377298 seconds
Average time for CC reno is 15.965781 .
dvir@ubuntu:~/TEx4/ex4_new$
dvir@ubuntu:~/TEx4/ex4_new$ ./sender
client (0) Current CC, type: cubic
client 0 connected to server!
sent all the 1MB file: 1048576
client (1) Current CC, type: cubic
client 1 connected to server!
sent all the 1MB file: 1048576
client (2) Current CC, type: cubic
client 2 connected to server!
sent all the 1MB file: 1048576
client (3) Current CC, type: cubic
client 3 connected to server!
sent all the 1MB file: 1048576
client (4) Current CC, type: cubic
client 4 connected to server!
sent all the 1MB file: 1048576
client (0) Current CC, type: reno
client 0 connected to server!
sent all the 1MB file: 1048576
client (1) Current CC, type: reno
client 1 connected to server!
sent all the 1MB file: 1048576
client (2) Current CC, type: reno
client 2 connected to server!
sent all the 1MB file: 1048576
client (3) Current CC, type: reno
client 3 connected to server!
sent all the 1MB file: 1048576
client (4) Current CC, type: reno
client 4 connected to server!
sent all the 1MB file: 1048576
dvir@ubuntu:~/TEx4/ex4_new$
אנגלית (ארצות הברית)
ארצות הברית
כדי להחליף שיטות קלט, הקש על מקש Windows + רווח.
Packets: 823 · Displayed: 823 (100.0%)
Profile: Default
11:25
16/12/2021
ENG

:25%



: 30%



אפשר לראות שהתוכנית רצה אבל זה לוקח ממש הרבה זמן.