SHAMOON COLLEGE OF ENGINEERING

מערכת ניתוח תעבורת רשת

פרויקט גמר בהנדסת תוכנה

הוכן לשם השלמת הדרישות לקבלת תואר ראשון .B.Sc בהנדסה

מאת: קגנר ולדיסלב

מנחה: ד"ר מיכאל אורלוב

הוגש למחלקה להנדסת תוכנה

המכללה האקדמית להנדסה ע"ש סמי שמעון

אשדוד

מאי 2014

אייר ה'תשע"ד

מערכת ויזואליזציה של נתונים חד-ממדי

תוכן עניינים

1. מבוא 2

2. סקר ספרות 3-7

3. מסמך דרישות-SRS 8-19

4. תרשימי Class Diagram 20-25

5. פירוט מימוש המערכת-תצורה סופית 26-39

6. כלים וטכנולוגיות שונות..... 40-42

7. STD+STR 43-54

מבוא

בתגובה לפופולריות הגוברת של טור ומערכות עקיפת צנזורה אחרות, צנזורים במדינות לא דמוקרטיות הגדילו את היכולות טכניות שלהם ועכשיו יכולים לזהות ולחסום תעבורת רשת שנוצרה על ידי המערכות הללו בקנה מידה ארצי. מערכות תקשורת צנזורה עמידות חדשות כגון SkypeMorph, StegoTorus, CensorSpoofer מטרתם להתחמק מתשומת לב צנזורים על ידי חיקוי פרוטוקולים נפוצים כמו סקייפ ו-HTTP.

אפילו צנזור חלש מאוד, מקומית יכול להבחין בקלות התנועה של מערכות אלה מפרוטוקולי החיקוי. אנחנו מראים עשרות שיטות פסיביות ואקטיביות שיכולים לזהות אפילו הפעלת רשת אחת, ללא כל צורך לבצע ניתוח תנועה מתוחכם. אנו זיהינו את הדרישות שמערכת צנזורה עמידה חייבת לספק לחיקוי פרוטוקול אחר בהצלחה והגנו למסקנה כי " unobservability by imitation" היא גישה פגומה מיסודו. אז אנחנו רוצים להציג את העיצוב החדש של מערכות תקשורת לא נצפות.

מודלים לניתוח רשת:

- התקפות פסיביים כרוכות בצפייה וניתוח תעבורת רשתות התנהגותם. טכניקות אופייניות הן ניתוח סטטיסטי תנועה, בדיקה מעמיקה במנות, וניתוח התנהגות.
- התקפות פעילות כרוכות במניפולציה של תעבורת רשת. טכניקות אופייניות מעכבות , שחרור , או הזרקת מנות לחיבורים , שינוי תוכן מנה והפסקת קשרים .
- התקפות יזומות במטרה לזהות גורמי רשת מעורבים בעקיפה על ידי שליחת בדיקות שהם בעלות מבנה לעורר תגובה לזיהוי. לדוגמא, צנזור יכול לנסות לגלות גשרי טור על ידי ייזום חיבורי לכתובות ה -IP האקראי או חשודות.

פקדים מקומיים (LO) לכל היותר כמה מכשירים ברשת ויכולים רק לבחון במספר קטן של חיבורים. דוגמאות הם נתבים ביתיים או נקודות גישה לאינטרנט אלחוטי , מעקב אחר עובדים בחברות, וכו '

לצנזור "מתעלם" ברמת מדינה (OB) יש משאבים מוגבלים חישובית ו/או אחסון. הוא לא יכול לשמור את ההיסטורית מעקב על רשת במשך זמן רב, ולא לבצע ניתוח תנועה מעמיקה.

לצנזור "יודע הכל" ברמת מדינה (OM) יש משאבי עיבוד ואחסון בשפע. הוא יכול לצבור נתונים שנאספו במקומות שונים ברשת ולאחסן את כל התנועה יורטה למצב לא מקוון, ניתוח המחשוב יקר.

סקר ספרות

Tor היא רשת תוכנה חופשית המאפשרת גלישה אנונימית באינטרנט. המערכת מתבססת על תוכנה שיכולה לרוץ באחד משני אופנים. באופן אחד, התוכנה מותקנת במחשבים שמהם גולשים, ומנתבת את הגלישה דרך מחשבים אחרים באינטרנט. במחשבים אלו פועלת התוכנה באופן השני, שבו היא מאפשרת ניתוב חבילות מידע עבור התקשרויות בהן אינה לוקחת חלק. חבילות המידע המועברות בין המחשבים בתוך רשת TOR אינן מזהות את מקור המידע או את יעדו - אלה חשופים רק בנקודת הכניסה לרשת ובנקודת היציאה ממנה. מכיוון שלמחשבים המעבירים את המידע אין מידע על מקורו או יעדו, אין דרך להתחקות אחרי מקור המידע היוצא מן הרשת. תכונה זו מקנה אנונימיות לגלישה דרך הרשת, שכן אין דרך לזהות את הגולשים לפי כתובת ה-IP שלהם - זו מוסתרת במהלך ההעברה ברשת, והמחשבים ברשת אינם שומרים יומנים של המידע המועבר.

על אנונימיות בעולם הוירטואלי

בואו נחזור לעולם האינטרנט. בתאריך ה-1.1.11 בשעה 11:11 אליס רוצה להשאיר באתר החדשות של בוב תגובה לכתבה שפורסמה שם. כשאליס מתחברת לאינטרנט, ספק האינטרנט שלה (סניף הדואר המקומי) מקצה לה כתובת IP (לדוגמא, 1.1.1.1). כתובת ה-IP מקבילה למספר תיבת הדואר מהדוגמא שראינו בעולם האמיתי, זוהי הכתובת של אליס בעולם הוירטואלי. לבוב (במקרה זה, לאתר האינטרנט של בוב) גם יש כתובת IP משלו (נניח, 2.2.2.2). כעת, כל פעילות אינטרנטית שאליס תבצע תהיה מזוהה עם כתובת ה-IP שלה. כשאליס משאירה תגובה באתר של בוב, המחשב של אליס מכין הודעה, ממלא בפרטי ההודעה את פרטי השולח (כתובת ה-IP של אליס) ואת פרטי המקבל (כתובת ה-IP של בוב) ובגוף ההודעה הוא מכניס את התגובה אותה אליס רוצה לשלוח.

כמו בעולם האמיתי, ניתן לאתר את פרטיה האמיתיים של אליס (שם, כתובת פיסית וכו') בהתבסס על כתובת ה-IP הוירטואלית שלה. כתובת זו (1.1.1.1) שהוקצתה לה ע"י ספק

האינטרנט שלה שייכת לספק ורשומה על שמו. מידע זה הוא פומבי באינטרנט וכל אחד יכול לבדוק על שם מי רשומה כל כתובת IP. לדוגמא, בדיקה פשוטה באינטרנט (באתר כמו ipaddresslocation.org) מעלה כי כתובת ה-IP ממנה אני גולש כעת (79.181.205.194), רשומה על שם בזק בינלאומי, רחוב השחם 40, פ"ת, טלפון 1800014014.

אם בוב רוצה לאתר את פרטיו של משאיר התגובה, הוא יכול לאתר בקלות את פרטיו של ספק האינטרנט של משאיר התגובה ואז לפנות לספק ולבקש את הפרטים המלאים של המשתמש שגלש בתאריך 1.1.11 בשעה 11:11 מכתובת IP זו (1.1.1.1). כל ספק אינטרנט מחוייב לשמור את היסטוריית ההקצאות אותן ביצע לכתובות ה-IP הרשומות על שמו ולכן ספק האינטרנט של אליס יכול למצוא בקלות שאליס גלשה בתאריך זה בשעה זו עם כתובת IP זו. מכיוון שאליס היא לקוחה שלו, ספק האינטרנט מחזיק גם את פרטיה האמיתיים (שם, כתובת פיסית, פרטי חיוב וכו'). מכיוון שספק האינטרנט מחוייב לפרטיות משתמשיו סביר להניח כי הוא לא ימסור פרטים אלה לבוב אבל אם גופי החוק יבקשו זאת ממנו הוא מחוייב לספקם.

כמו שראינו, הן בעולם האמיתי והן בעולם הוירטואלי, האנונימיות של השולח הינה מאוד מוגבלת.

על מנת לשפר בצורה דרמטית את האנונימיות שלה בעולם האמיתי, אליס תשלח את חבילתה לבוב דרך מספר מתווכים שיעזרו לה להסתיר את זהותה האמיתית מבוב. אליס בוחרת באופן אקראי 3 אנשים, כל אחד מיבשת אחרת. הראשון, פרנק מפריס, צרפת (תיבת דואר 333). השניה, דבי ממלבורן, אוסטרליה (ת"ד 444). השלישי, עלי מרבט, מרוקו (ת"ד 555). כעת, אליס שולחת את החבילה לפרנק שישלח אותה לדבי שתשלח אותה לעלי שישלח אותה ליעדה הסופי, בוב. כל תחנה במסלול זה מכירה את כתובת התחנה שלפניה במסלול ואת כתובת התחנה שאחריה במסלול, ולא יותר. מאחר והחבילה מטיילת בין מספר תחנות ברחבי כדור הארץ, לבוב יהיה מאוד קשה לפרום את השרשרת ולהבין שמקור החבילה הוא אליס.

עיקרון זה צריך להיות מוכר לצופי סדרת הטלוויזיה "הבורר". באחת מהסצינות הטובות ביותר בסידרה, פארוקי מסביר לאחים קובלובה איך שומרים על אנונימיות בבחירת הבלדר לחבילת הסמים אותה הם רוצים להעביר: "תמצא לי מישהו שימצא לך מישהו שיארגן לך מישהו. אל תפספס, שלושה מישהו. אני אכלתי אותה 12 שנים כי הורדתי מישהו אחד בדרך". אז גם אנחנו שומרים על עיקרון זה ובוחרים 3 מישהו שיעזרו לנו לשמור על זהותה של אליס מפני בוב.

איך זה יתבצע בפועל? כמו בובת מטריושקה...

אליס מכינה את החבילה למשלוח. תחת פרטי השולח היא כותבת את פרטיו של עלי (ת"ד 555, רבט, מרוקו) ותחת פרטי המקבל היא כותבת את פרטיו של בוב (ת"ד 222, ירושלים, ישראל). אז היא לוקחת את החבילה ושמה אותה בתוך קופסא גדולה יותר. על קופסא זו היא כותבת את פרטיה של דבי (ת"ד 444, מלבורן, אוסטרליה) תחת פרטי השולח ואת פרטיו של עלי תחת פרטי המקבל. בנוסף היא נועלת את החבילה עם מנעול שרק עלי מכיר את הקוד שלו. כעת אליס לוקחת את החבילה הכפולה ושמה אותה בתוך קופסא גדולה יותר. היא כותבת את פרטיו של פרנק (ת"ד 333, פריס, צרפת) תחת פרטי השולח ואת פרטיה של דבי תחת פרטי המקבל. אליס גם נועלת חבילה זאת במנעול שקוד פתיחתו ידוע רק לדבי. לבסוף אליס לוקחת את החבילה המשולשת ושמה אותה בתוך חבילה גדולה יותר. הפעם היא משתמשת בפרטיה (ת"ד 111, זיכרון יעקב, ישראל) תחת פרטי השולח ואת פרטיו של פרנק תחת פרטי המקבל. כמו מקודם, חבילה זו ננעלת במנעול שקוד פתיחתו ידוע אך ורק לפרנק.

החבילה של אליס יוצאת לדרך כאשר היעד הראשון הוא פרנק. בעת קבלתה, פרנק פותח את החבילה (רק לו יש את הקוד המתאים) ורואה בפנים חבילה נוספת. הוא לא יכול לפתוח אותה (רק דבי מכירה את הקוד) אבל הוא רואה שהיעד הבא הוא דבי. אז פרנק שולח את החבילה הפנימית לדבי שמקבלת, פותחת ורואה בפנים חבילה נוספת (נעולה) שמיועדת לעלי. דבי שולחת את החבילה הפנימית לעלי שפותח ומוצא בפנים חבילה נוספת. הפעם עלי רואה שהיעד הסופי הוא בוב והוא מעביר לו את החבילה הפנימית ביותר. השימוש במנעולים מבטיח, כי כל מתווך בדרך יוכל לדעת מה היעד הבא אחריו ולא יותר מזה. באופן זה, לכל תחנה במסלול (מלבד אליס) יש ידע חלקי לגבי המסלול אותו עוברת החבילה.

אם בוב רוצה לפרום את המסלול ולהגיע לשולח המקורי, עליו להתחיל במתווך האחרון במסלול ממנו הגיעה החבילה (עלי). בוב צריך לפנות לסניף הדואר של עלי במרוקו, לתת להם את פרטיו של עלי, כפי שהופיעו על החבילה ולבקש מהם את פרטיו האמיתיים. רק אז הוא יכול לגשת לעלי ולשאול אותו מהיכן הגיעה החבילה. עלי לא יודע מי היה המקור של החבילה אבל הוא יודע שהתחנה לפניו במסלול היתה דבי. כעת בוב צריך לחזור על תהליך זה מול דבי והרשויות באוסטרליה וגם אם הוא יזכה לשיתוף פעולה הוא יוכל לקבל רק את פרטיו של מי שקדם לדבי במסלול (פרנק). ושוב בוב צריך לחזור על התרגיל מול פרנק והרשויות בצרפת, ורק אם מהלך זה יהיה מוצלח הוא יוכל להגיע לתחנה שלפני פרנק, אליס היקרה. כעת בוב צריך לפנות לרשויות במדינתה של אליס על מנת לקבל את פרטיה המלאים.

איך לשמור על אנונימיות בעולם הוירטואלי

העיקרון שהצגנו לגבי העולם האמיתי (3 מתווכים אקראיים) מיושם בעולם הוירטואלי ע"י מערכת שנקראת TOR, the onion routing, או ניתוב בצל בעברית. מערכת TOR יכולה לעזור לכל משתמש באינטרנט לשמור על האנונימיות שלו.

כיצד זה פועל?

ראשית, על אליס להתקין במחשב שלה מערכת TOR. כעת, כאשר אליס רוצה לגלוש באינטרנט בצורה אנונימית, מערכת ה-TOR המותקנת אצלה תבחר באופן אקראי 3 מתווכים ברשת ה-TOR (כמו פרנק, דבי ועלי מדוגמת העולם האמיתי). המתווכים ברשת ה-TOR הם משתמשים רגילים שלמען חופש הביטוי וזכויות האדם התנדבו להתקין תוכנה שתעביר תעבורת אינטרנט אנונימית עבור משתמשי TOR. כשאליס רוצה להשאיר תגובה באתר של בוב, תוכנת ה-TOR של אליס תיקח את התגובה ותעטוף אותה בשכבות, כפי שראינו בדוגמא מהעולם האמיתי. השכבה הפנימית ביותר תכיל את התגובה אותה אליס רוצה לשלוח ואת כתובת ה-IP של עלי (5.5.5.5) בתור השולח ואת כתובת ה-IP של בוב (2.2.2.2) בתור המקבל. בשכבה החיצונית הבאה התהליך חוזר על עצמו עם ה-IP של דבי (4.4.4.4) בתור השולחת וה-IP של עלי בתור המקבל. בשכבה החיצונית הבאה ה-IP של פרנק (3.3.3.3) הוא השולח וה-IP של דבי

הוא המקבל. ובשכבה החיצונית ביותר ה-IP של אליס הוא השולח (1.1.1.1) ושל פרנק הוא המקבל. בנוסף, כמו בדוגמת העולם האמיתי, כל שכבה מוצפנת, ורק היעד של השכבה יכול לפענחה ולדעת למי להעביר הלאה. מאחר וכל תחנה במסלול מקלפת את השכבה שלה ומעבירה לתחנה הבאה, עיקרון זה נקרא ניתוב בצל.

סיכום

רשת Tor נועדה לספק למשתמשים תקשורת אנונימית. לקוחות טור עם ממסרים ברשימה בפומבי כדי להגיע אנונימי ליעדים שלהם. עם זאת, מאחר ורשימת ממסרים מופיע בפומבי, היא יכולה להיחסם בקלות על ידי צנזורה.

פרויקט Tor חזה את האפשרות של נקודות כניסה לרשת Tor ברשומות מוסתרות, הידוע בכינויו גשרים. אנו מתייחסים לנושא של גילוי רשת Tor על ידי ניתוח תעבורת תקשורת ביניהם וצומת ברשת שלהם.

ביבליוגרפיה

[1] Does Skype use encryption? https://support.skype.com/en/faq/FA31/Does-Skype-use-encryption. [Online; accessed April 2012].
[2] Number of Skype users in 2010. http://about.skype.com/press/2011/05/microsoft_to_acquire_skype.html [Online; accessed April 2012].
[3] Skype Software. http://skype.com. [Online; accessed April 2012].
[5] SkypeKit. http://developer.skype.com/public/skypekit. [Online; accessed April 2012].
[6] Tor BridgeDB. https://gitweb.torproject.org/bridgedb.git/tree. [Online; accessed April 2012].
[7] Ethiopian Government Bans Skype, Google Talk And All Other VoIP Services. http://techcrunch.com/2012/06/14/ethiopian-government-bans-skype-google-talk-and-all-other-voip-services/, 2012. [Online, accessed May 2012].
[8] Skype ban in the UAE could be lifted, as it is ”purely a licensing matter”. http://thenextweb.com/me/2012/04/21/skype-ban-in-the-uae-could-be-lifted-as-it-is-purely-a-licensing-matter/, 2012. [Online, accessed May 2012].
[9] J. Appelbaum and N. Mathewson. Pluggable transports for circumvention. https://gitweb.torproject.org/torspec.git/blob/HEAD: /proposals/180-pluggable-transport.txt. [Online; accessed April 2012].
[10] S. A. Baset and H. G. Schulzrinne. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. In INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings, pages 1–11, 2006.

מסמך דרישות – SRS

הקדמה

1.1. מטרת המסמך

מטרת המסמך היא לרכז את כל הנתונים הדרושים לקבלת כל ההחלטות הדרושות בפרויקט. המטרה היא לענות על כל סימן שאלה שיכול להופיע במהלך הפיתוח וכל זאת על-מנת להגדיל את הסיכויים לתהליך פורה. מסמך זה מיועד למפתחים וללקוחות כאחד. כמו-כן, מסמך זה מספק מידע על ההתנהגות החיצונית של המערכת, דרישותיה, אילוציה והגדרת הממשק מנקודת מבט המשתמש וקהל היעד.

1.2. הגדרות וראשי תיבות

מונח	משמעות
SENDER	השולח – לקוח קצה המשתמש ברשת (כגון TOR)
RECEIVER	המקבל (לדוגמא BRIDGH)
DB	בסיס נתונים של הצנזור
פונקציונלי	תהליך שגורר פעולה בפועל
גיבוי	שמירה של מצב ביניים כלשהו שלאחר מכן ניתן לשחזרו.

1.3. קהל היעד: אנשי סיסתם / חוקרים – משתמשי התוכנה יהיו אותם אנשים אשר מריצים POC או בונים האפליקציה לניתוח רשתות וייצוג המידע בצורה גרפית.

1.4. הנחות, אילוצי מערכת

- למשתמש להיות בעל ידע בסיסי במחשבים, על מנת להפעיל את התוכנה.
- המערכת תהיה ידידותית וקלה לתפעול ככל האפשר.
- המערכת תהיה בשפה האנגלית.

תיאור התוכנה

1.5. מטרת הפרויקט

הגדרת הבעיה:

מערכות תקשורת צנזורה עמידה כגון Tor משמשות יותר ויותר על ידי אנשים במדינות לא דמוקרטיות כדי לעקוף את ההגבלות על גישה לאינטרנט, חולקים את המידע , לגלוש לאתרים חסומים על ידי המשטר , וכו'. בתגובה, צנזורים ממשלתיים השתפרו מאוד ביכולות טכניות שלהם וכעת הם מסוגלים לבצע בזמן אמת בדיקות עמוקות ניתוח תעבורה באמצעי אחסון ברמת ספק שירותי אינטרנט של תעבורת רשת. עלייה בכוח צנזורה זו מאיימת להפוך את מערכות תקשורת ללא זמינות למשתמשים הזקוקים להם ביותר. לטור, בפרט, יש בעיה שתנועת טור נשארה לזיהוי על ידי התבניות האופייניות שלה וחתימות תוכן.

פתרון הבעיה:

באופן אינטואיטיבי, unobservability אומר שצנזור אינו יכול לזהות את התנועה שנוצרה על ידי מערכת עקיפה, ולא לזהות את נקודות הקצה העוסקים בעקיפה. מערכת עקיפה שלנו שואפת להשיג unobservability ידי חיקוי פרוטוקול המשמש באופן נרחב ללא צנזורה. מטרות חיקוי \ כוללות HTTP, סקייפ, וIETFbased ה-VoIP.

מטרת המערכת:

התוכנה שלנו מגדירה את פורמט מנות שבו אין תבניות הניתנת לזיהוי תכולת המנה. לכן, אנו מקווים, ציוד (Deep Packet Inspection (DPI צריך להיות מסוגל לחסום מנות, או לזהות מארחים. בנוסף לפורמט המנות, אנו מגדירים את הפרוטוקול אשר עמיד בפני יריב פסיבי או אקטיבי.

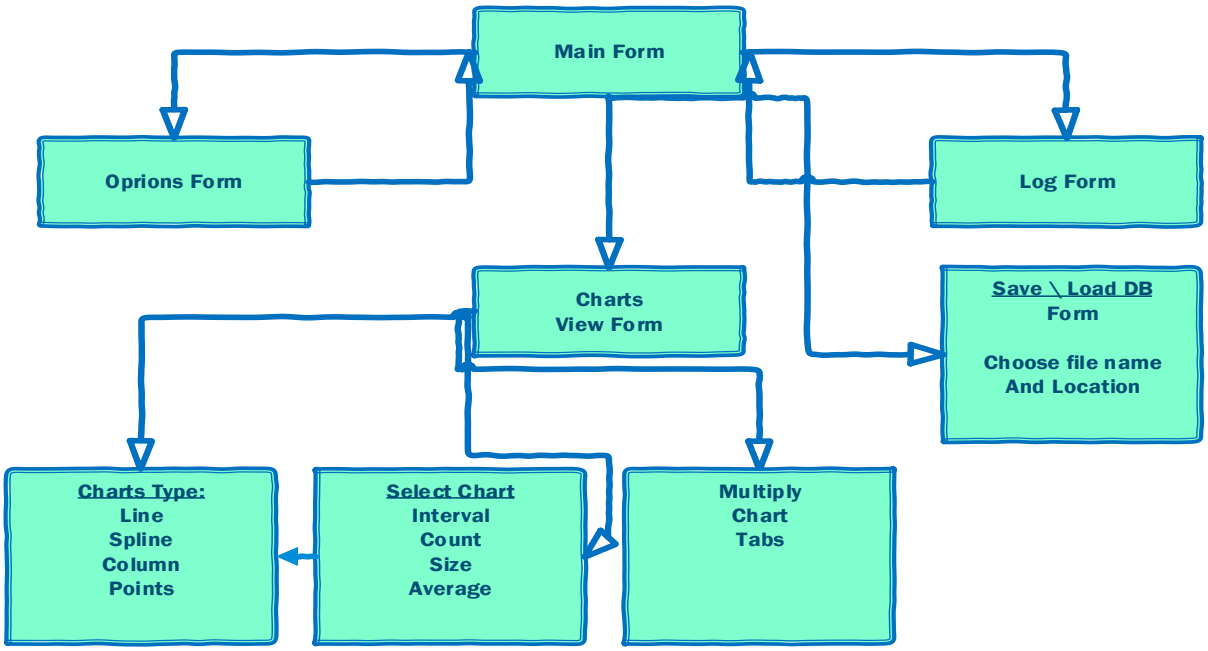
מידע ויזואלי הוא למעשה ייצוג של מידע מופשט על ידי סמלים גרפיים כגון: צבעים, תמונות, תרשימים, גרפים וציורים. המטרות של וויזואליזציה הן שיש אפשרות לסכם כמויות גדולות של נתונים ויש אפשרות לנתח נתונים ולמצוא קשרים חדשים.

1.6. סקירת ה-Actors

רכיבי רשת - מקור הנתונים נותן את הנתונים לניתוח והניסויים.

User - משתמש הבודק את המידע ומנתח גרפים והשינויים בהם.

1.7. מבנה המערכת



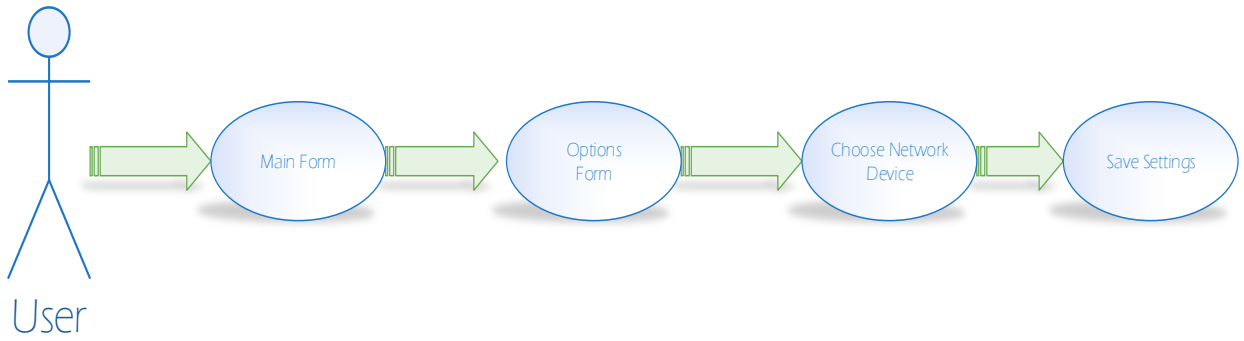
1.8. פעולות עיקריות

- הפעלה \ כיבוי ניתוח תעבורת רשת.
- טעינת נתונים סטטיסטים מקובץ.
- בחירת נתוני מקור והוספת גרף חדש.
- פעולות שונות על הגרפים(צביעת הגרף, שינוי מראה הגרף).
- הגדלת המערכת למסך מלא.
- אתחול המסכים \ איפוס DB.
- בחירת מקור תעבורת רשת.
- פתיחת חלון לוג.

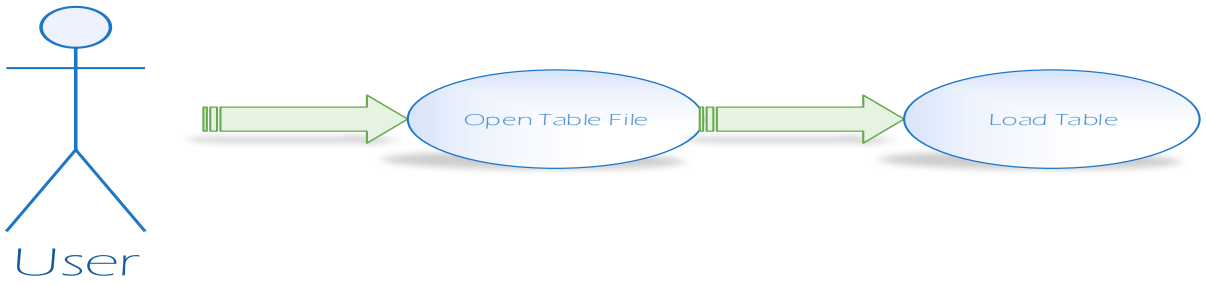
2. סקירת ה-Use Case

המטרה: ללכוד את ההיבט הדינמי של המערכת, כלומר משמשים כדי לאסוף את הדרישות של המערכת, כולל השפעות פנימיות וחיצוניות. דרישות אלה הן בעיקר דרישות. לכן, תרשים זה בא על מנת לתאר את הפונקציונאליות והמשתמשים במערכת.

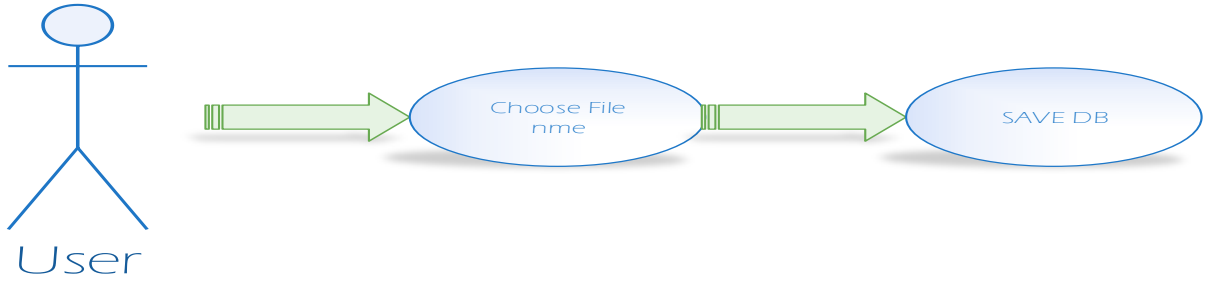
2.1. בחירת רכיב רשת לניתוח תעבורה



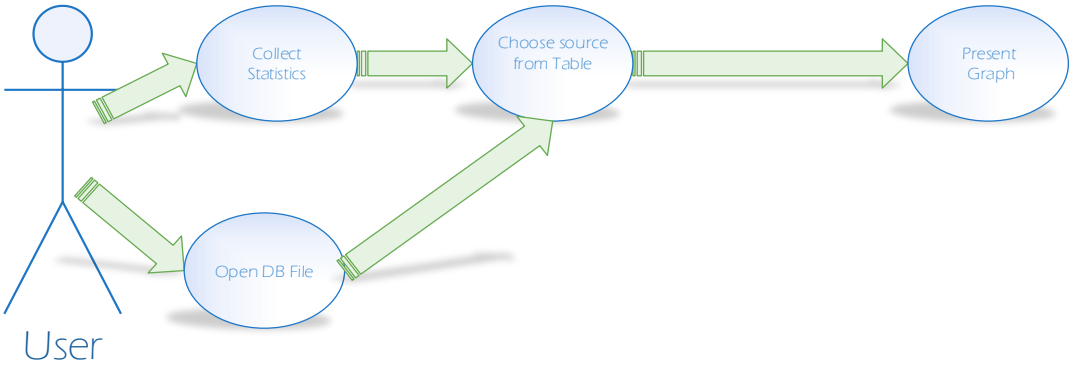
2.2. טעינת DB מקובץ קיים במחשב.



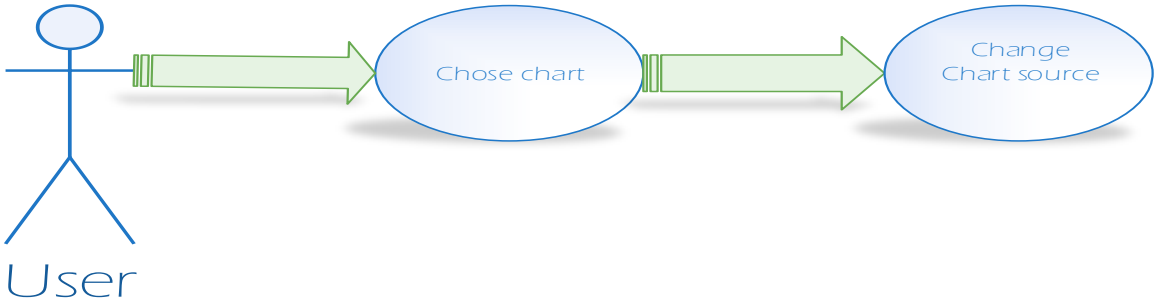
2.3. שמירת DB לקובץ במחשב.



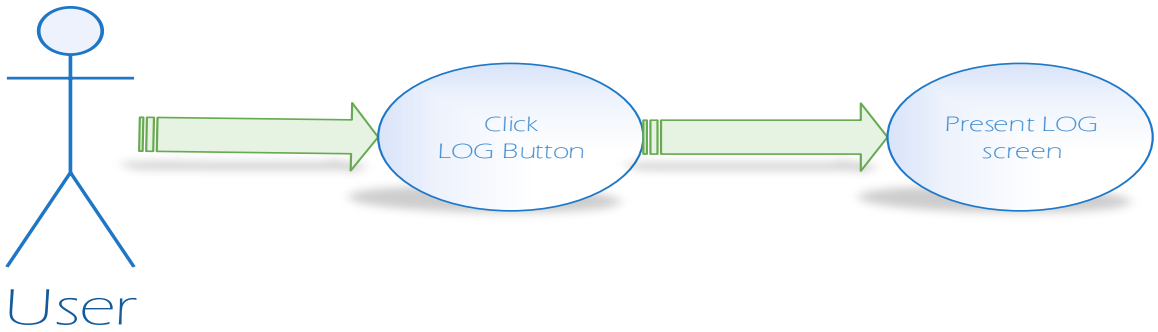
2.4. הצגת גרף.



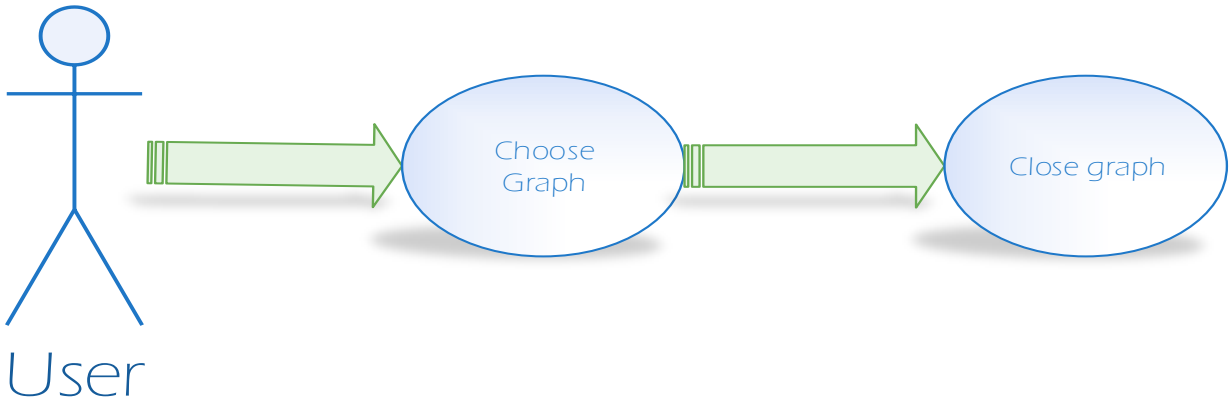
2.5. שינוי סוג הגרף.



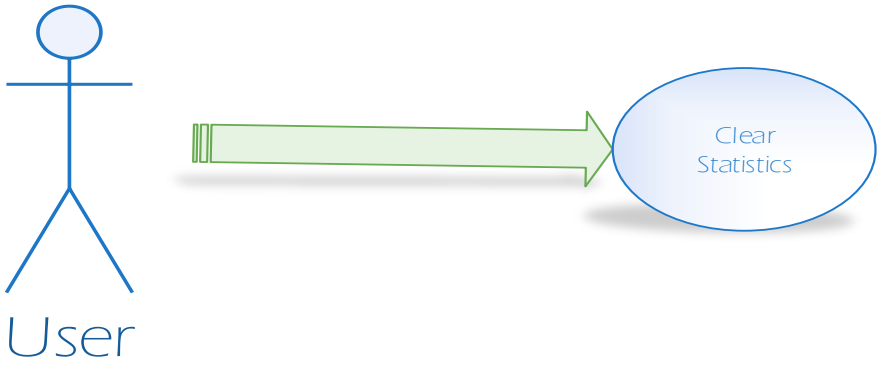
2.6. פיתחת מסך LOG.



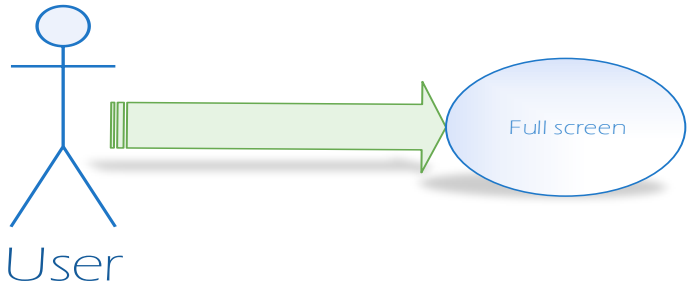
2.7. סגירת גרף.



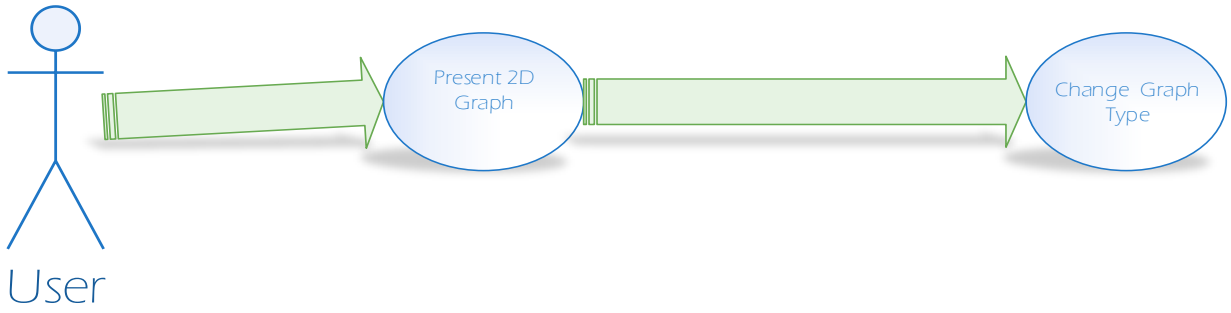
2.8. מחיקת סטטיסטיקה.



2.9. הגדלת התוכנה למסך מלא.



3.12 שינוי סוג הגרף(גרף עמודות ,גרף נקודות וכד').



מפרט דרישות

3. דרישות פונקציונאליות

3.1. קלט

- התוכנה צריכה להיות מחוברת לרכיב רשת.
- התוכנה צריכה לפתוח קבצי dbm.

3.2. נתונים

3.2.1. עיבוד נתונים

- הצגת המידע בצורה גרפית.
- הצגת הנתונים בטבלה.
- בחירת גרף.
- הצגת סוגי גרפים:

1. Line- הצגת גרף רציף רגיל.
2. Spline- הצגת גרף רציף מעוגל.
3. Column- הצגת גרף עמודות.
4. Points- הצגת גרף נקודות.

- שינוי מראה הגרף:

1. Marker- הדגשת הנקודות.
2. Chart Color- צביעת הגרף.
3. BgColor- החלפת צבע הרקע לגרף.
4. 3D Chart- שינוי הגרף מדו-מימד לתלת-מימד.
5. Reset- לאחר הגדלת הגרף מחזיר את התצוגה לגודל המקורי.

4.3 כלים נוספים

- הגדלת התוכנה למסך מלא.
- מחיקת סטטיסטיקה.

4. דרישות לא פונקציונאליות

- יצירת חשבון משתשמש בגוגל.
- קבלת developer Key.

5. דרישות טכניות

- בסיס נתונים מסוג יעיל.
- שפת התכנות היא C# .

6. דרישות עיצוב

ויזואליות: לצורך יצירת סביבה נעימה למשתמשי המערכת ותתופעל ע"י עכבר ומקלדת.

7. דרישות אבטחה

הגישה למאגר הנתונים של המערכת תהיה אפשרית דרך הממשק.

8. דרישות בטיחות

המערכת תרוץ על מחשב בתנאי חדר סבירים.

9. דרישות סביבה

התוכנה תעבוד רק במערכת windows.

10. דרישות משאבים

10.1. דרישות חומרה

- ניצול יעיל וחכם של הזיכרון.

10.2. דרישות תוכנה

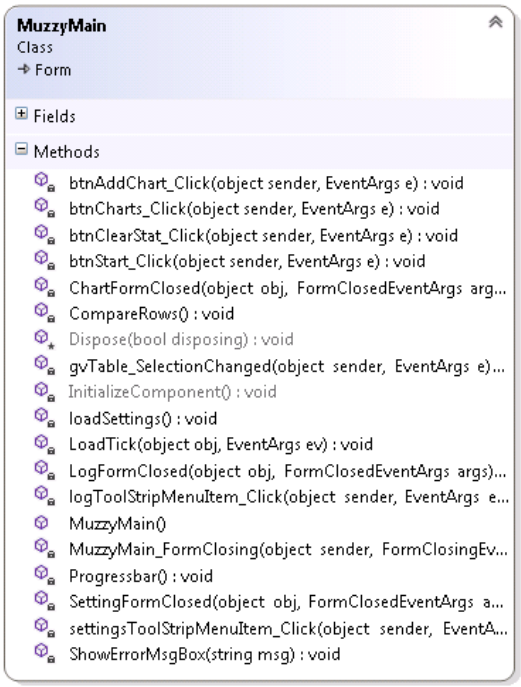
- המערכת צריכה להיות בלתי תלויה בתוכנות נלוות, תעבוד באופן עצמאי, ללא השפעה על תוכנות המשתמש האחרות המותקנות במחשב.
- על המערכת להיות ידידותית וקלה לתפעול.

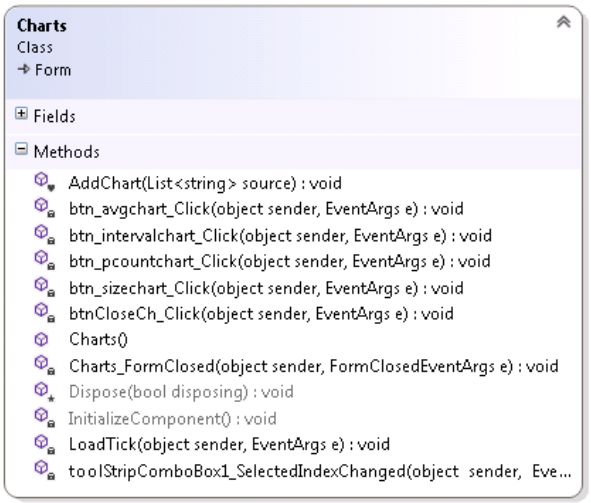
10.3. דרישות תקשורת

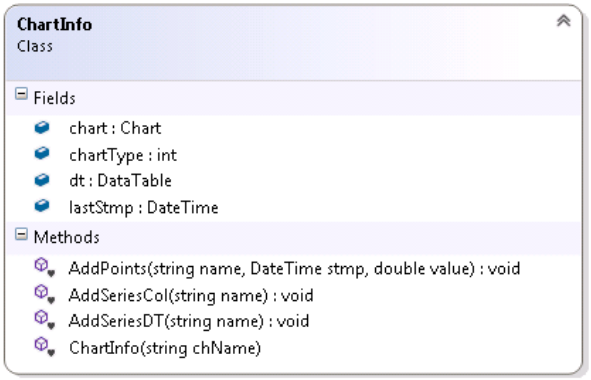
- התוכנה תעבוד על רכיבי רשת מקומיים.

CLASS DIAGRAM

1. FORMS:

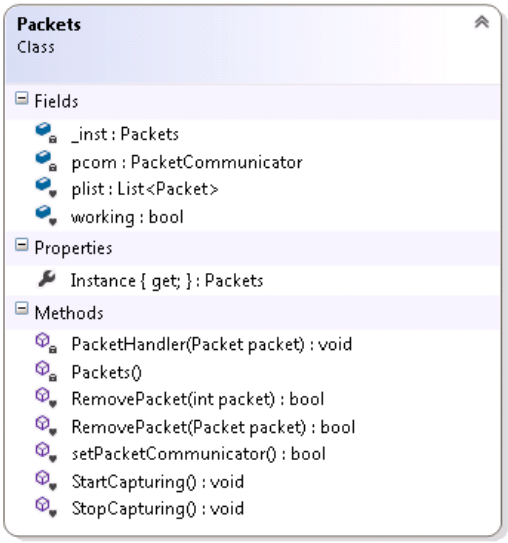


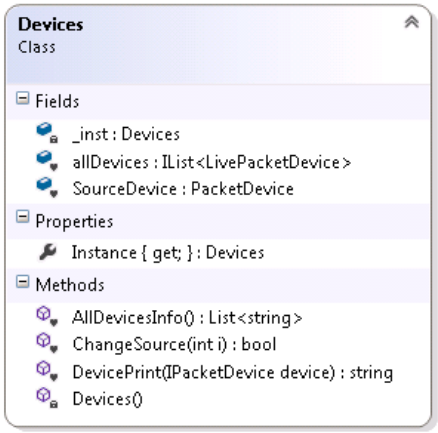


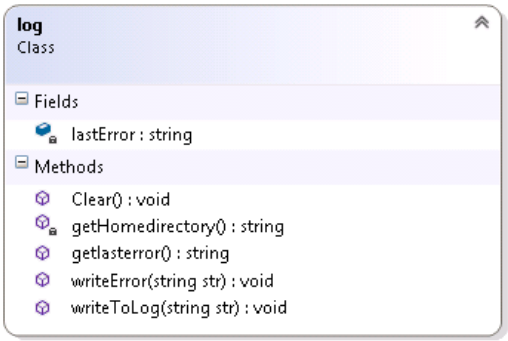


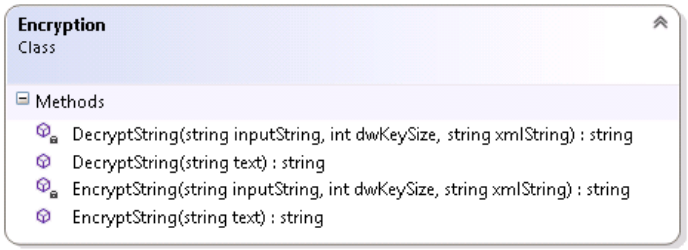
MUZZIMAIN CLASS – מחלקה למסך ראשי של המערכת
CHARTS CLASS – מחלקה למסך גרפים
CHARTINFO CLASS – מחלקה לשמירת נתון גרף

2. HELPER CLESSES:



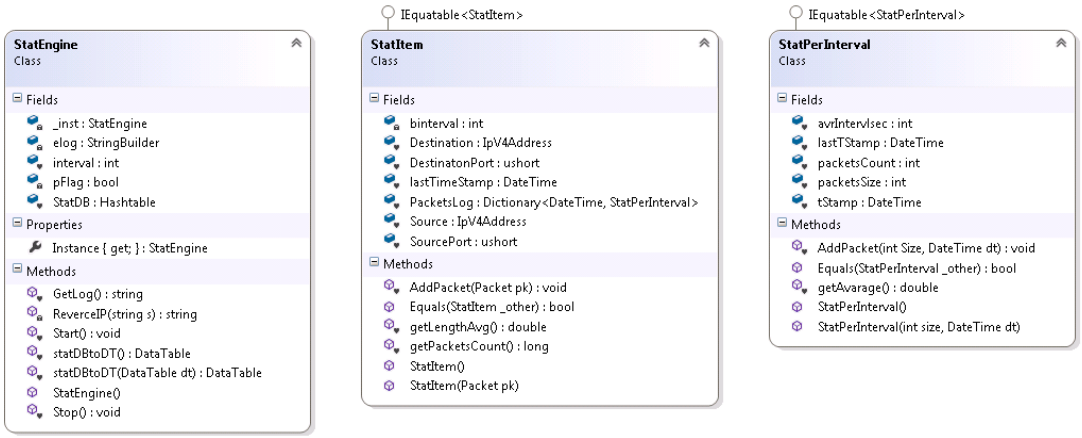






LOG CLASS – מחלקה לכתיבת לוג לקובץ.
ENCRYPTION CLASS – מחלקה להצפנת מידע.
DEVICES CLASS – מחלקה לטיפול ברכיבי הרשת.
PACKETS CLASS – מחלקה חיבור לרכיב הרשת וטיפול בפקתות.

3. STATISTICS DATA BASE:

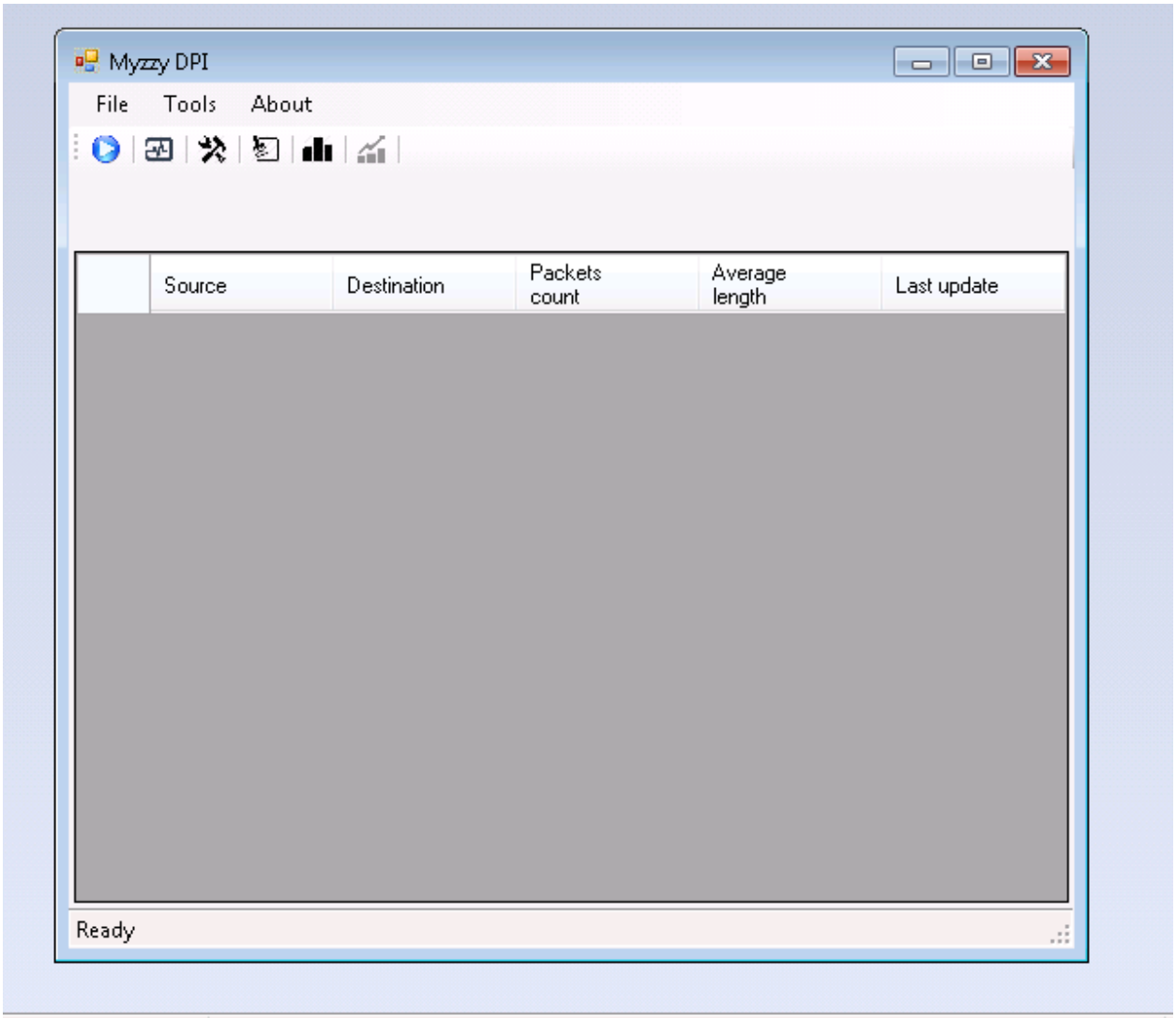


STATENGINE CLASS – מחלקה לשמירה וטיפול בבסיס נתונים לסטטיסטיקה.
STATITEM CLASS – מחלקה לשמירת יחידה סטטיסטית.
STATINTERVAL CLASS – מחלקה לשמירת מידע על פקתות של יחידה סטטיסטית.

הצגת התוכנה

מסך ראשי

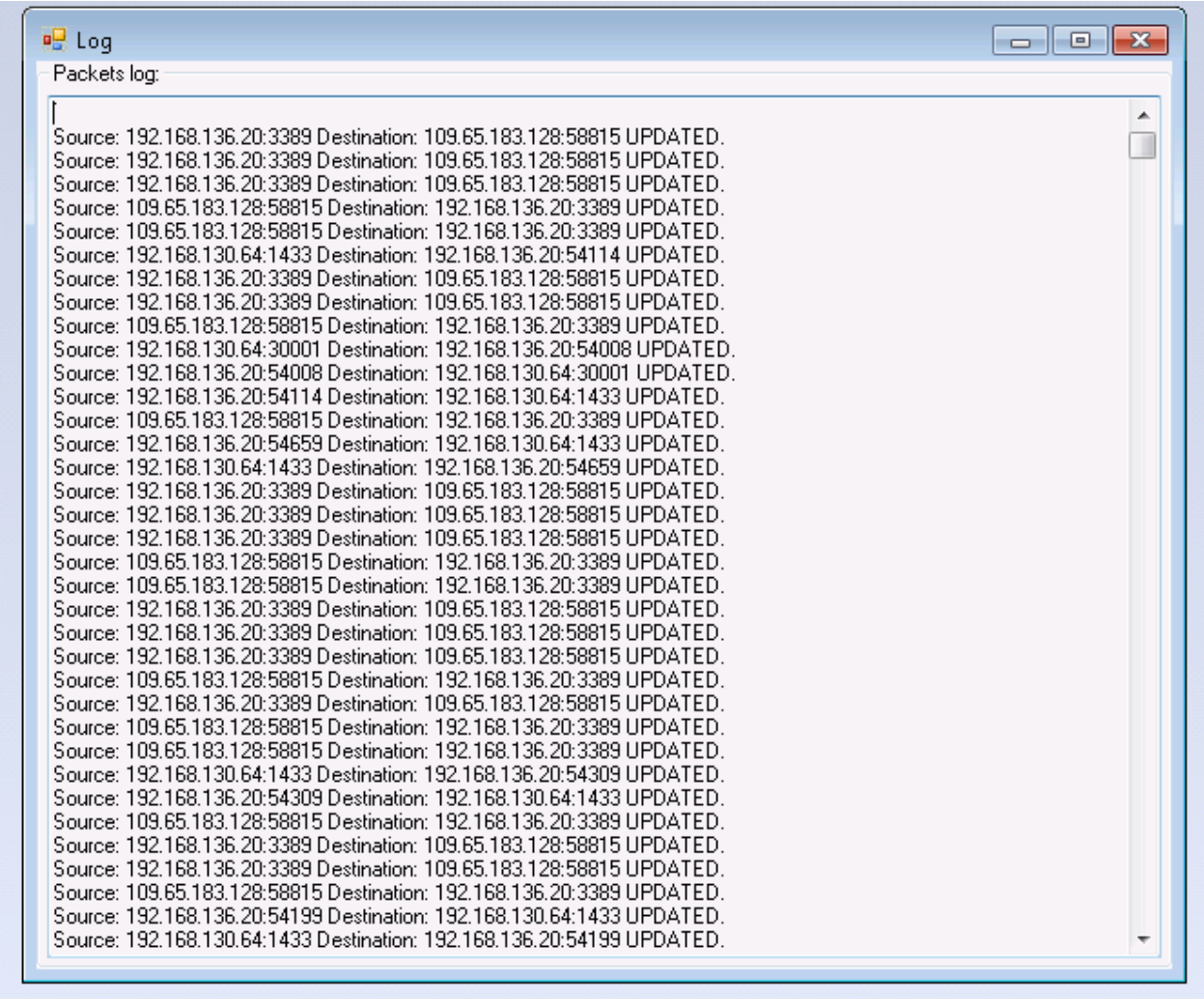
תיאור: החלון הראש המוצג כאשר המערכת מופעלת.



החלון מאפשר שימוש בתפריט הראשי, פתיחת הגדרות תוכנה, מחיקת סטטיסטיקה, גישה לחלון LOG, הוספת גרף והפעלה \ עצירת ניתוח תעבורה.

חלון LOG

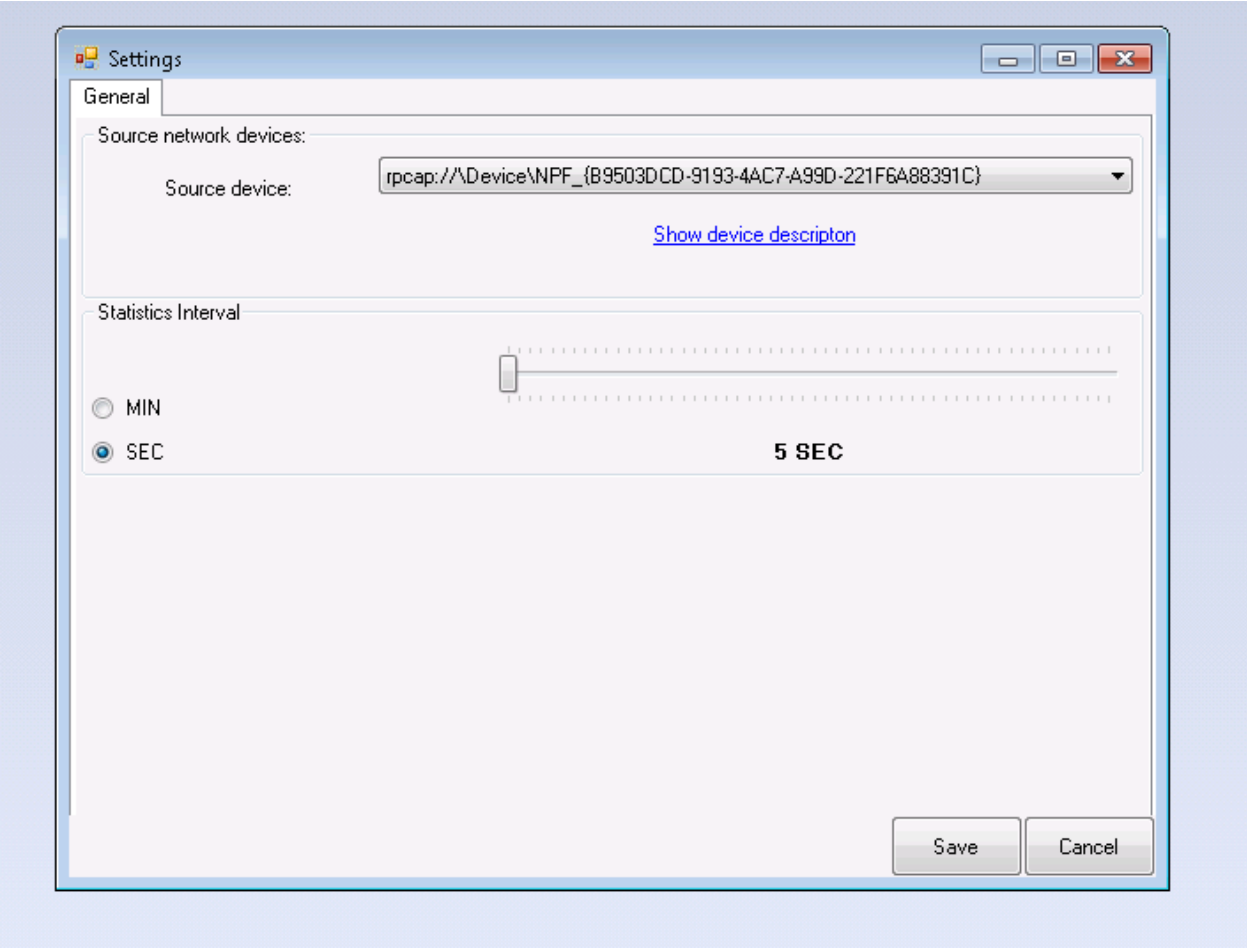
תיאור: החלון המוצג כאשר מפותחים LOG.



החלון מאפשר גישה לLOG.

חלון הגדרות התוכנה.

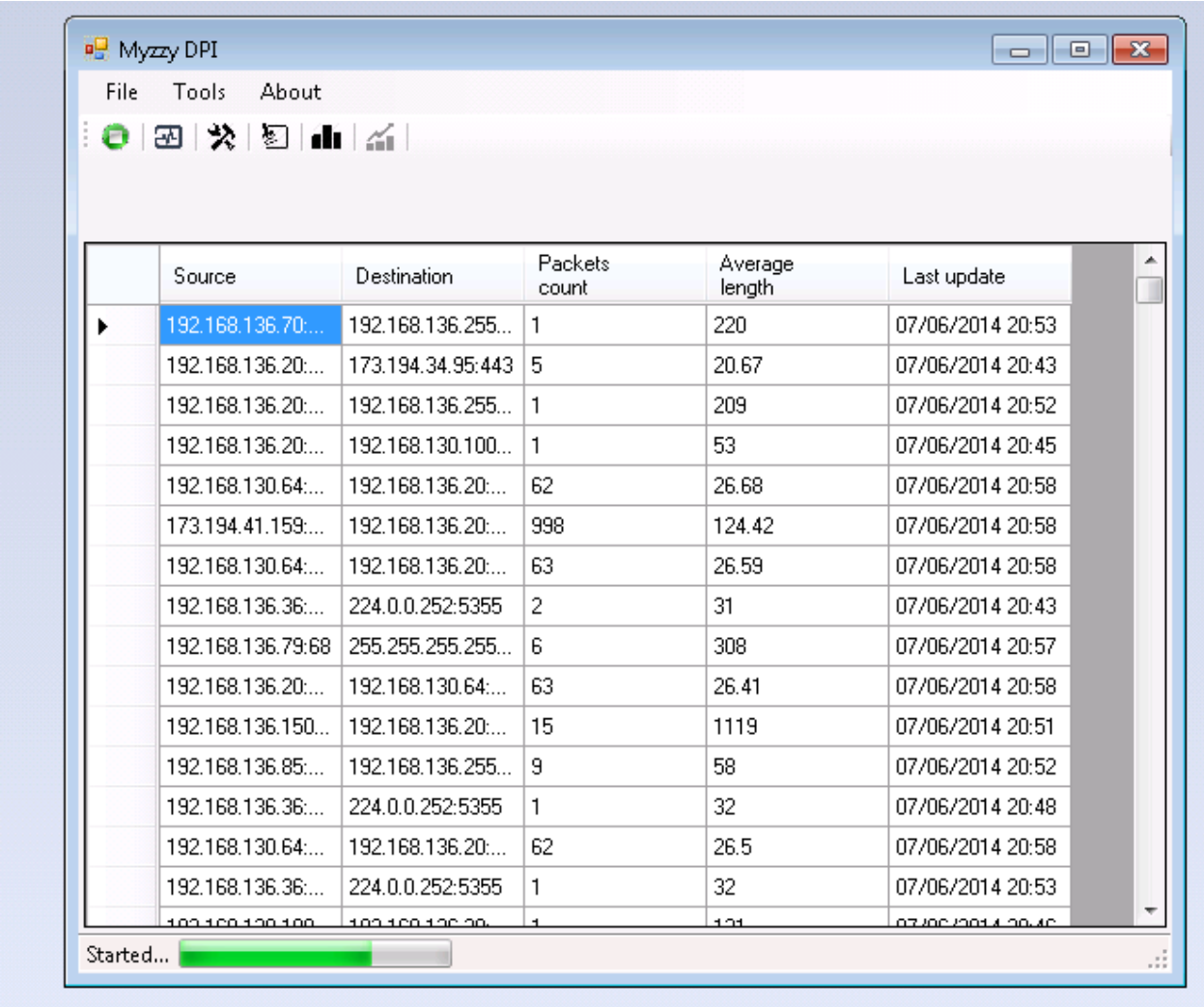
תיאור : חלון לקביעת הגדרות התוכנה.



החלון מאפשר קביעת הגדרות התוכנה: בחירת רכיב רשת והצגת מידע על רכיב ספציפי.

חלון הצגת טבלת סטטיסטיקה אחרי התחברות לרכיב רשת

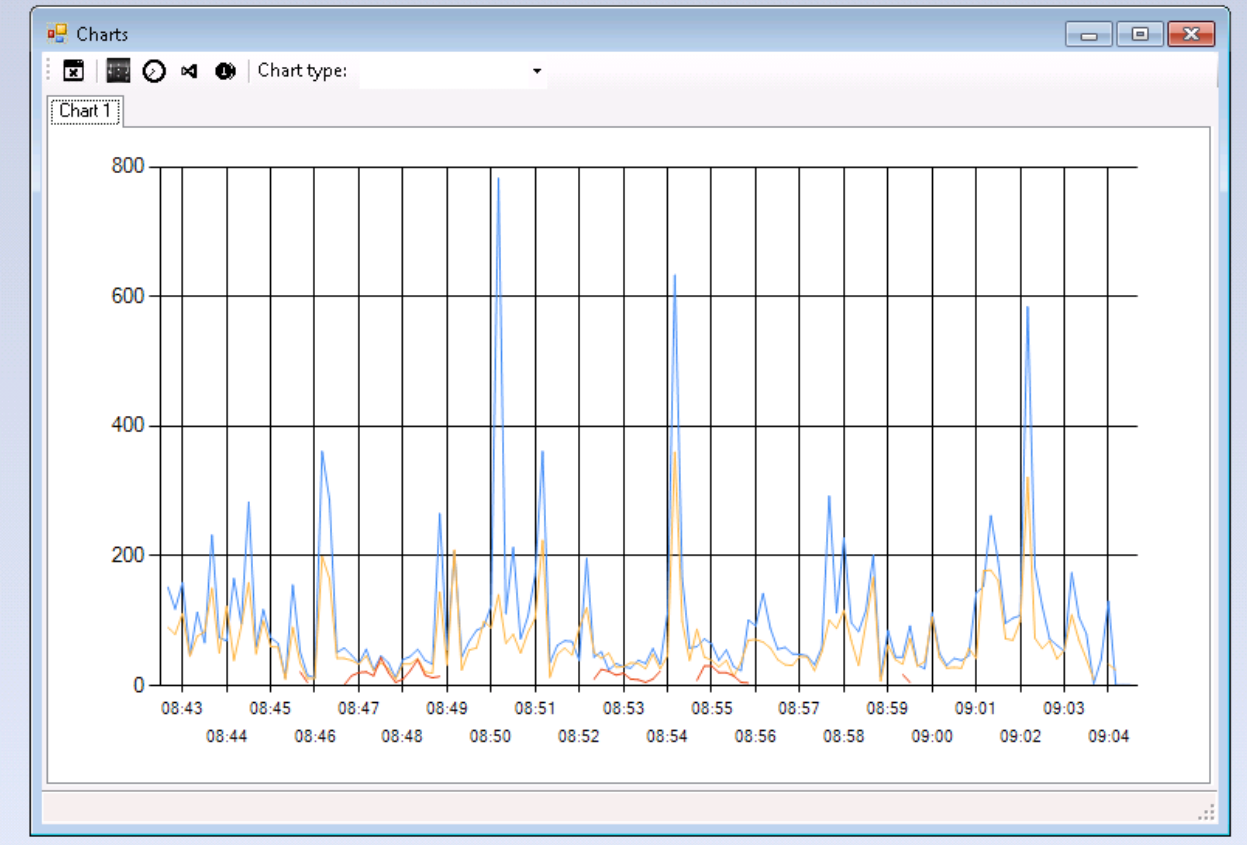
תיאור: הצגת טבלת סטטיסטיקה ב GridView אחרי התחברות לרכיב רשת.



Source	Destination	Packets count	Average length	Last update
192.168.136.70:...	192.168.136.255...	1	220	07/06/2014 20:53
192.168.136.20:...	173.194.34.95:443	5	20.67	07/06/2014 20:43
192.168.136.20:...	192.168.136.255...	1	209	07/06/2014 20:52
192.168.136.20:...	192.168.130.100...	1	53	07/06/2014 20:45
192.168.130.64:...	192.168.136.20:...	62	26.68	07/06/2014 20:58
173.194.41.159:...	192.168.136.20:...	998	124.42	07/06/2014 20:58
192.168.130.64:...	192.168.136.20:...	63	26.59	07/06/2014 20:58
192.168.136.36:...	224.0.0.252:5355	2	31	07/06/2014 20:43
192.168.136.79:68	255.255.255.255...	6	308	07/06/2014 20:57
192.168.136.20:...	192.168.130.64:...	63	26.41	07/06/2014 20:58
192.168.136.150...	192.168.136.20:...	15	1119	07/06/2014 20:51
192.168.136.85:...	192.168.136.255...	9	58	07/06/2014 20:52
192.168.136.36:...	224.0.0.252:5355	1	32	07/06/2014 20:48
192.168.130.64:...	192.168.136.20:...	62	26.5	07/06/2014 20:58
192.168.136.36:...	224.0.0.252:5355	1	32	07/06/2014 20:53

חלון הצגת גרף

תיאור: הצגת גרף על פי בחירה ב GraphView .



החלון מציג נתונים בצורה גרפית ומאפשר השוואה ויזואלית כולל אפשרות לשינוי סוג הגרף, צורה של גרף וסגירה.

כלים וטכנולוגיות חדשות

פקדים

הפקדים הם הכלים בהם משתמשים לבניית ממשק המשתמש - החלונות שרואה המשתמש ודרכם הוא מתקשר עם התוכנה. במערכת שבנינו השתמשנו בפרויקט ב-2 סוגים עיקריים של פקדים: DatagridView, Chart.

הפקד DataGridView מאפשר הצגת נתונים בצורה טבלאית ממקור נתונים. בשלבי ניתוח תעבורה ניתן לצפות בנתונים בצורה טבלאית, והפקד ממלא פעולה זו בצורה הטובה והיעילה ביותר ב-#C.

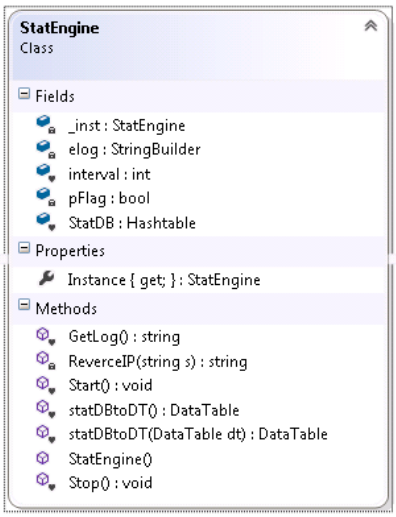
הפקד Chart, מאפשר הצגת נתונים בצורה גרפית ממקור נתונים. בשלבי ניתוח תעבורה ניתן להציג את הנתונים בצורה גרפית, והפקד ממלא פעולה זו בצורה הטובה והיעילה ביותר ב-#C. בעזרת פקד זה הצלחנו להציג את הנתונים בצורה גרפית ולתת לגרפים אלו יכולות ויזואליות ,ופונקציונליות רבה כגון: שינוי צורת הגרף, שינוי סוג הגרף ועוד.

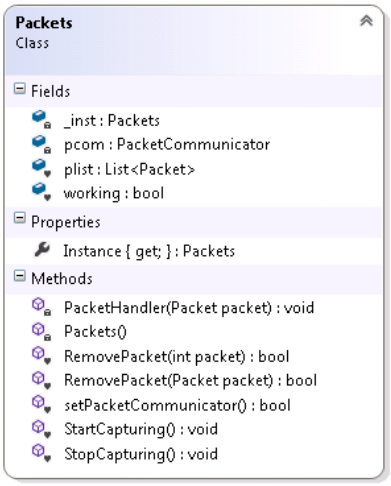
Design Patterns (תבנית עיצוב)

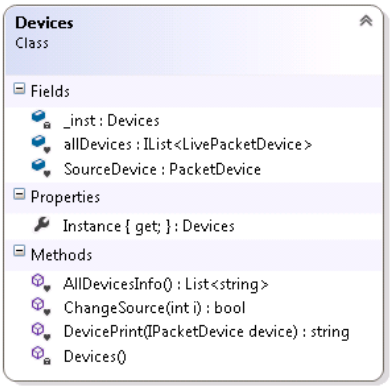
Design Patterns זהו פתרון כללי לבעיה שכיחה בעיצוב תוכנה. תבנית עיצוב אינה עיצוב סופי שניתן להעבירו הישר לקוד, אלא תיאור או תבנית לדרך לפתרון בעיה, שעשויה להיות שימושית במצבים רבים. תבניות עיצוב מונחות עצמים מציגות לרוב יחסים וקשרי גומלין בין מחלקות או אובייקטים, בלי לפרט את המחלקות או אובייקטים היישום הסופיים המעורבים. אלגוריתמים אינם נחשבים כתבנית עיצוב כיוון שהם פותרים בעיות חישוביות ולא בעיות עיצוב.

אנו השתמשנו בתבנית עיצוב עיקרית במערכת: תבנית Singelton.
תבנית Singelton היא תבנית עיצוב, אשר נועדה למקרים בהם מעוניינים להגביל את יצירת המופעים של מחלקה מסוימת למופע יחיד. תבנית זו מקושרת לעתים גם למקרים בהם רוצים להגביל את מספר המופעים לכמות קבועה כל שהי ולא למופע דווקא יחיד. תבנית זו שימושים כאשר נדרש רק מופע אחד על מנת לתאם פעולות במערכת. אנו השתמשנו בתבנית זו כדי ליצור מופע חד פעמי של מסד נתונים.

הפרדנו בין הרכיה של מסד הנתונים למבט שזהו ה-FORM שלנו שבו אנו מציגים גם את הטבלה וגם את הגרפים, לכל הרכיבים יש מחלקות נפרדות שחלק מהן שולטת בגרף , חלק במסד נתונים וחלק באיסוף נתונים.







1. **בדיקות עיצוב – GUI**

זיהוי הבדיקה	E1-001			
מטרת הבדיקה	חלונות פעילים.			
תנאים מקדימים				
צעד	**תיאור בדיקה**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	מעבר בין חלונות המערכת.	מעבר תקין בין חלונות המערכת.	✓	מעבר בין החלונות תקין.

זיהוי הבדיקה	E1-002			
מטרת הבדיקה	עיצוב הממשק (Forms).			
תנאים מקדימים				
צעד	**תיאור בדיקה**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	כל החלונות עוצבו כפי שהוגדרו במסמכים הקודמים.	חלונות מעוצבים כנדרש.	✓	חלונות מעוצבים כנדרש.

זיהוי הבדיקה	E1-003			
מטרת הבדיקה	אחידות הממשק (Forms).			
תנאים מקדימים				
צעד	**תיאור בדיקה**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	מעבר על כל חלונות הממשק ובדיקה שכל הפקדים בחלונות אחידים.	חלונות ופקדים אחידים.	✓	חלונות ופקדים אחידים.

זיהוי הבדיקה	E1-004			
מטרת הבדיקה	תצוגה ונוחיות.			
תנאים מקדימים				
צעד	**תיאור בדיקה**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	חלונות לא עמוסים מדי, מסודרים ומכילים את המידע הנדרש.	תצוגה נוחה ונעימה של הנתונים.	✓	חלונות מסודרים, מציגים מידע רלוונטי.

2.בדיקות פונקציונאליות \ תהליכיות

זיהוי הבדיקה	05-02E			
מטרת הבדיקה	בדיקת התחברות לרכיב רשת.			
תנאים מקדימים	כניסה למערכת.			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	לחץ על כפתור TOOLS.	תיפתח לשונית.	✓	נפתחה לשונית.
2	לחץ על כפתור OPTIONS.	יפתח חלון בחירת רכיב רשת.	✓	נפתח חלון בחירת רכיב רשת.
3	שינוי רכיב רשת ולחץ לשמירה.	נתונים נשמרו בהצלחה.	✓	נתונים נשמרו בהצלחה.

זיהוי הבדיקה	10-02E			
מטרת הבדיקה	תחילת ניתוח נתוני תעבורת רשת.			
תנאים מקדימים	בחירת רכיב רשת.			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	לחץ על כפתור TOOLS.	תיפתח לשונית.	✓	נפתחה לשונית.
2	לחץ על כפתור OPTIONS.	יפתח חלון בחירת רכיב רשת.	✓	נפתח חלון בחירת רכיב רשת.
3	בחירת רכיב רשת ולחץ לשמירה.	נתונים נשמרו בהצלחה.	✓	נתונים נשמרו בהצלחה.
4	לחיצה על כפתור START.	תחילת ניתוח נתוני תעבורת רשת וטעינה לטבלה.	✓	תחילת ניתוח נתוני תעבורת רשת וטעינה לטבלה.

זיהוי הבדיקה	15-02E			
מטרת הבדיקה	מחיקת סטטיסטיקה.			
תנאים מקדימים	יש נצוני סטטיסטיקה.			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	לחץ על כפתור CLEAR STATISTIC.	טבלת סטטיסטיקה התרוקן.	✓	טבלת סטטיסטיקה התרוקנה.

זיהוי הבדיקה	20-02E			
מטרת הבדיקה	לטעון סטטיסטיקה מהמחשב .			
תנאים מקדימים	כניסה למערכת.			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	לחץ על כפתור FILE.	תיפתח לשונית.	✓	נפתחה לשונית.
2	לחץ על כפתור Open.	יפתח חלון בחירת קובץ קיים.	✓	נפתח חלון בחירת קובץ.
3	בחירת קובץ רצוי בחלון הבחירה ולחיצה על אישור.	טעינת הטבלה עם נתונים.	✓	הטבלה עם נתונים נטענה.

זיהוי הבדיקה	25-02E			
מטרת הבדיקה	בחירת תצוגה גרפית.			
תנאים מקדימים	יש נתונים סטטיסטים.			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	לחיצה על כפתור הוספת גרף.	פתיחת חלון תצוגת גרף.	✓	מצב תצוגה גרף.
2	לחיצה על טאב של הגרף.	העברה לגרף.	✓	העברה לגרף.

זיהוי הבדיקה	30-02E			
מטרת הבדיקה	שינוי צורת גרף.			
תנאים מקדימים	גרף טעון ומוצג.			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	בחירת צורת גרף.	בחירת צורת גרף.	✓	שינוי צורת גרף.

זיהוי הבדיקה	35-02E			
מטרת הבדיקה	מסך מלא.			
תנאים מקדימים	כניסה למערכת.			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	לחיצה על כפתור מסך מלא.	התוכנה נפתחת במסך מלא.	✓	התוכנה נתחה במסך מלא.

זיהוי הבדיקה	40-02E			
מטרת הבדיקה	שינוי סוג גרף.			
תנאים מקדימים	גרף טעון ומוצג.			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	לחיצה על כפתור סוג הגרף שינוי סוג גרף.	שינוי סוג הגרף.	✓	גרף שינה את הסוג.

זיהוי הבדיקה	45-02E			
מטרת הבדיקה	שמירת נתוני סטטיסטיקה לקובץ.			
תנאים מקדימים	יש נתוני סטטיסטיקה.			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	לחץ על כפתור FILE.	תיפתח לשונית.	✓	נפתחה לשונית.
2	לחץ על כפתור SAVE.	יפתח חלון בחירת קובץ.	✓	נפתח חלון בחירת קובץ.
3	בחירת קובץ רצוי בחלון הבחירה או שם חדש ולחיצה על אישור.	שמירת נתונים לקובץ.	✓	שמירת נתונים לקובץ.

זיהוי הבדיקה	50-02E			
מטרת הבדיקה	פתיחת חלון LOG.			
תנאים מקדימים	אין			
צעדים לביצוע:	**תיאור הצעד**	**תוצאה צפויה**	**עבר / נכשל**	**מה התקבל בפועל**
1	לחיצה על כפתור LOG	פתיחת חלון LOG.	✓	נפתח חלון LOG.