



ספר פרויקט- AntiVirus AV Project

שם התלמיד: מייקל חושהנג

ת.ז התלמיד: 325179091

שם העבודה: AntiVirus AV Project

שם בית הספר: מקיף עירוני ח'

שם המנחה: שלום ואנונו

תאריך ההגשה: 13/5/2021



תוכן העניינים

1. מבוא.....	3
2. הגדרות.....	5
3. מבנה/ארכיטקטורה של המערכת.....	7
4. מדריך למשתמש.....	18
5. בסיס הנתונים.....	34
6. מדריך למפתח.....	37
7. סיכום אישי.....	39
8. ביביליוגרפיה.....	41

1. מבוא

ספר הפרויקט שלי יכלול את המבנה של הפרויקט שלי והסברים בנוגע לארכיטקטורה שלו, מדריך למשתמש, הסבר בנוגע לבסיס הנתונים שהשתמשתי בו ומדריך למפתח, עם הסברים בנוגע לקוד ומדוע נכתב בצורה שנכתב (בנוסף להערות הקוד).

אני מאמין כי לכל אדם קיימת הזכות לפרטיות והזכות להגן על עצמו מפני תקיפות שונות במחשבו האישי, ועל כן יצרתי תוכנה המעניקה למשתמשיה את היכולות הללו.

הפרויקט שיצרתי עוסק באבטחת המחשב של המשתמש וכן בשמירה על פרטיותו.

התוכנה שיצרתי מספקת שירותים שונים, אך המרכזי שביניהם הינו סריקת וירוסים והתוכנות הזדוניות והסרתן. בנוסף לכך, התוכנה מספקת שירותים נוספים לאבטחת המשתמש כגון מציאת פער לעדכונים למחשב וסריקת חיבורים חשודים ברשת האינטרנט.

התוכנה מספקת גם שירותי אבטחת פרטיות המשתמש הכוללים גריסת קבצים בסל המחזור או קבצים זמניים של מערכת הפעלה, ניהול חומת האש, שמירת סיסמאות במנהל הסיסמאות ותקייה מאובטחת לשמירה על קבצים פרטיים.

לפני תחילת פיתוח הפרויקט, ביצעתי חקר של המצב הקיים בשוק- השווייתי בין ארבעה אנטי וירוסים שונים בהקשר השירותים שהם מציעים, הממשק הגרפי למשתמש, וזמן ביצוע סריקת הוירוסים והתוכנות הזדוניות (עבור סריקה מלאה). התוכנות שביניהן השווייתי הינן: Norton, McAfee, AVG ו-Microsoft Windows Defender

עבורי, אחד האתגרים המשמעותיים ביותר היה לחקור לעומק כיצד לבצע את סריקת הוירוסים שכן תוכנות האנטי וירוס בשוק אינן מגלות כיצד הן עושות זאת.

פתרון אחד עבור בעיה זו היה לסרוק כל קובץ במחשב (בהתאם למצב הסריקה) ולאכסן את פונקציית הגיבוב (hash) שלו. לאחר מכן, הייתי משווה את חתימות ה-hash הללו באתר [VirusShare](https://VirusShare.com) (אתר בעל מאגרי hash של קבצים זדוניים) אחד אחד במטרה לבדוק אם הם קיימים בכל אחד ממאגרי ה-hash הזדוניים שלו. כמובן שדרך זו אינה יעילה, אורכת זמן רב, וגוזלת משאבים רבים מן המחשב.

על כן, מצאתי שיטה יעילה הרבה יותר. לאחר מחקר מעמיק, גיליתי כי קיים שירות של סריקת וירוסים על ידי אתר [Virus Total](https://VirusTotal.com), זהו אתר המשתמש ב-API (Application Programming Interface) ובעזרתו מקבל את

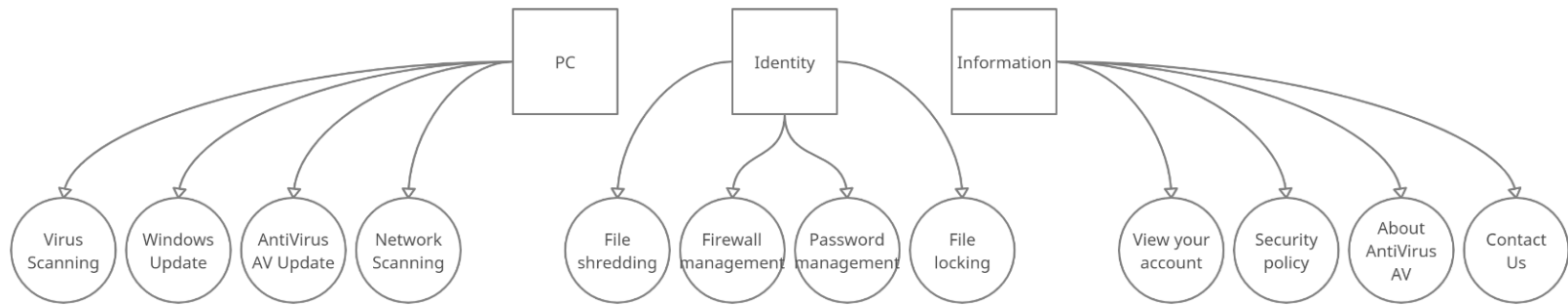
פונקציית הגיבוב (hash) של קובץ, סורק אותו באמצעות 60-80 תוכנות אנטי וירוס שונות, ומחזיר תשובה האם הקובץ הוא בעל פוטנציאל להוות איום על המחשב או לא. התהליך עבור חתימת hash אחת של קובץ מתרחש בין מאית לעשירית השניה, כך שהדרך מהירה ויעילה ביותר.

לאחר שמצאתי את האתר [Virus Total](https://www.virustotal.com) הייתה מוטלת עליי המשימה לקבל גישה לאתר במטרה להעלות יותר מ-10 קבצים לדקה, שכן זהו הקצב הרגיל עבור משתמש שאינו רשום באתר. לאחר חודשים של תקשורת ביני ובין חברת Virus Total, ובעזרתה של המחנכת שלי, הצלחתי לקבל גישה לאתר. היה עליי לספק לאתר כתובת מייל אקדמאית המעידה כי אני מבצע מחקר/עבודה אקדמאית בעזרת השירותים שלהם (במטרה לקבל קצב העלאה גבוה יותר), ואכן יש לי כתובת מייל אקדמאית (המייל הארגוני של משרד החינוך), אך כאשר הייתי צריך לקבל קוד אישור במייל, לא קיבלתי כלום (כך עובד המייל הארגוני של משרד החינוך עבור תלמידים), לכן הייתי צריך לבקש את עזרת המחנכת שלי (עבור מייל ארגוני של מורים אכן ניתן לקבל מיילים מכתובות אחרות). כלל התקשורת התרחשה שלושה וחצי חודשים, ולבסוף קיבלתי קצב העלה של 200 אלף קבצים בדקה, כך שתוכנת האנטי וירוס שלי אכן מסוגלת לסרוק וירוסים במהירות וביעילות.

2. הגדרות

תוכנת האנטי וירוס שבניתי מספקת שירותים רבים למשתמש המתחלקים לשני סוגי שירותים- שירותי אבטחת המחשב, ושירותי אבטחת פרטיות המשתמש.

להלן תרשים סכמתי של השירותים השונים שהמערכת מספקת למשתמש:



שירותי אבטחת המחשב כוללים שירות סריקת וירוסים, שירות מציאת עדכונים למחשב ושירות סריקת חיבורים חשודים ברשת האינטרנט.

סריקת וירוסים- זהו שירות המאפשר למשתמש לסרוק קבצים במחשב שלו ולקבוע האם הם מהווים איום על המחשב או לא, במידה ונמצאו קבצים זדוניים ניתן למחוקם.

בכדי לבצע את סריקת הוירוסים בפרויקט השתמשתי בשירות אינו מוכר- שירות סריקת הוירוסים של Virus Total.

שירות [Virus Total](#) הוא שירות סריקת וירוסים אינטרנטי חנימי המשתמש בשירות API המכיל מתודות שונות שהמרכזית שביניהן מקבלת פונקציית גיבוב (hash) של קובץ מסוים, בודקת האם הוא בעל פוטנציאל להוות איום על המחשב באמצעות בדיקתו בעזרת 60-80 תוכנות אנטי וירוס שונות, ובהתאם לכך מחזירה תשובה בהקשר להיותו של הקובץ זדוני או לא.

* Application Programming Interface -API (ממשק תכנות יישומים) היא ערכה של ספריות קוד ופונקציות שניתן לבצע בה שימוש. בפרויקט שלי, קיים שימוש מרכזי ביותר בשירות ה-API שחברת VirusTotal מספקת לי במטרה לסרוק וירוסים.

מציאת עדכונים למחשב- שירות זה הוא שירות המספק מענה למציאת פער לעדכונים של המחשב. השירות בודק מול שרת של חברת Microsoft האם קיימים עדכונים למחשב/לאפליקציות המחשב או לדרייברים של המחשב, ואם כן- מתקינם.



סריקת חיבורים חשודים - שירות זה מזהה חיבורים חשודים ומנתקם מהמחשב במידה ונמצאו. השירות סורק פורטים (Port) שהם בעלי פוטנציאל להוות חיבור חשוד, ובצורה זו קובע אם יש לנתק את החיבור או לא.

שירותי אבטחת פרטיות המשתמש כוללים שירות גריסת קבצים, שירות ניהול חומת האש של Windows, שירות ניהול סיסמאות ושירות נעילת קבצים אישיים.

גריסת קבצים - זהו שירות המאפשר למשתמש לגרוס קבצים מסל המחזור של המחשב וכן מהקבצים הזמניים של מערכת ההפעלה Windows במטרה לשמור הן על פרטיות המשתמש והן בכדי להקל את זיכרון המחשב. הגריסה כותבת בקבצים מידע אקראי ולאחר מכן מוחקת אותם כמספר הפעמים שהמשתמש בוחר - במטרה להקשות על שחזור הקבצים.

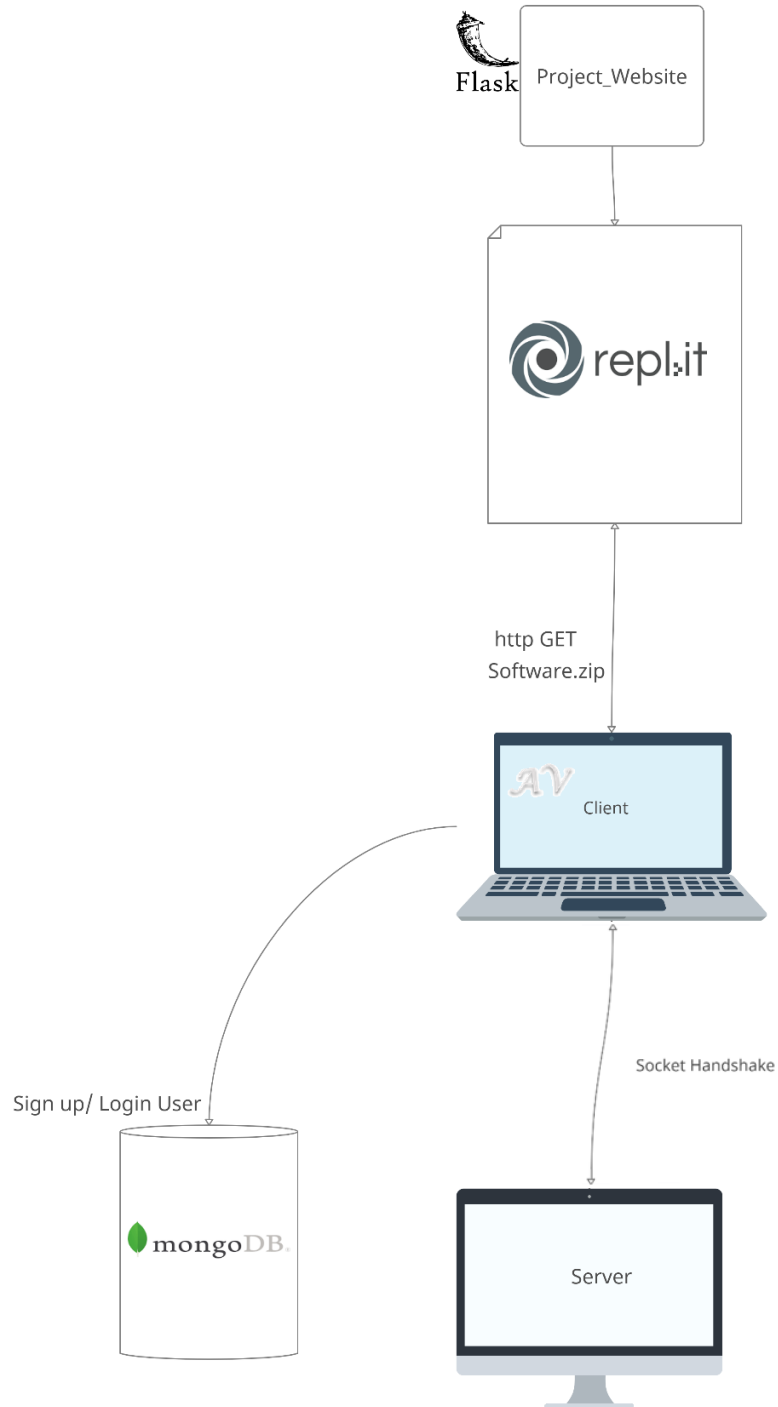
ניהול חומת האש - שירות זה מאפשר למשתמש להוסיף ולהסיר חוקים (מעבר של אפליקציות) עבור חומת האש של מערכת ההפעלה Windows וכן שירות זה מאפשר למשתמש לאפשר ולחסום מעבר של פורטים (Ports) דרך חומת האש.

ניהול סיסמאות - שירות זה מאפשר למשתמש לרשום סיסמאות שהוא מעוניין לזכור עם פרטים עבור כל סיסמה.

נעילת קבצים אישיים - זהו שירות המאפשר למשתמש לנעול קבצים פרטיים לשם שמירה על פרטיותו.

3. מבנה ארכיטקטורה של המערכת

להלן דיאגרמת הבלוקים הראשית של הפרויקט-

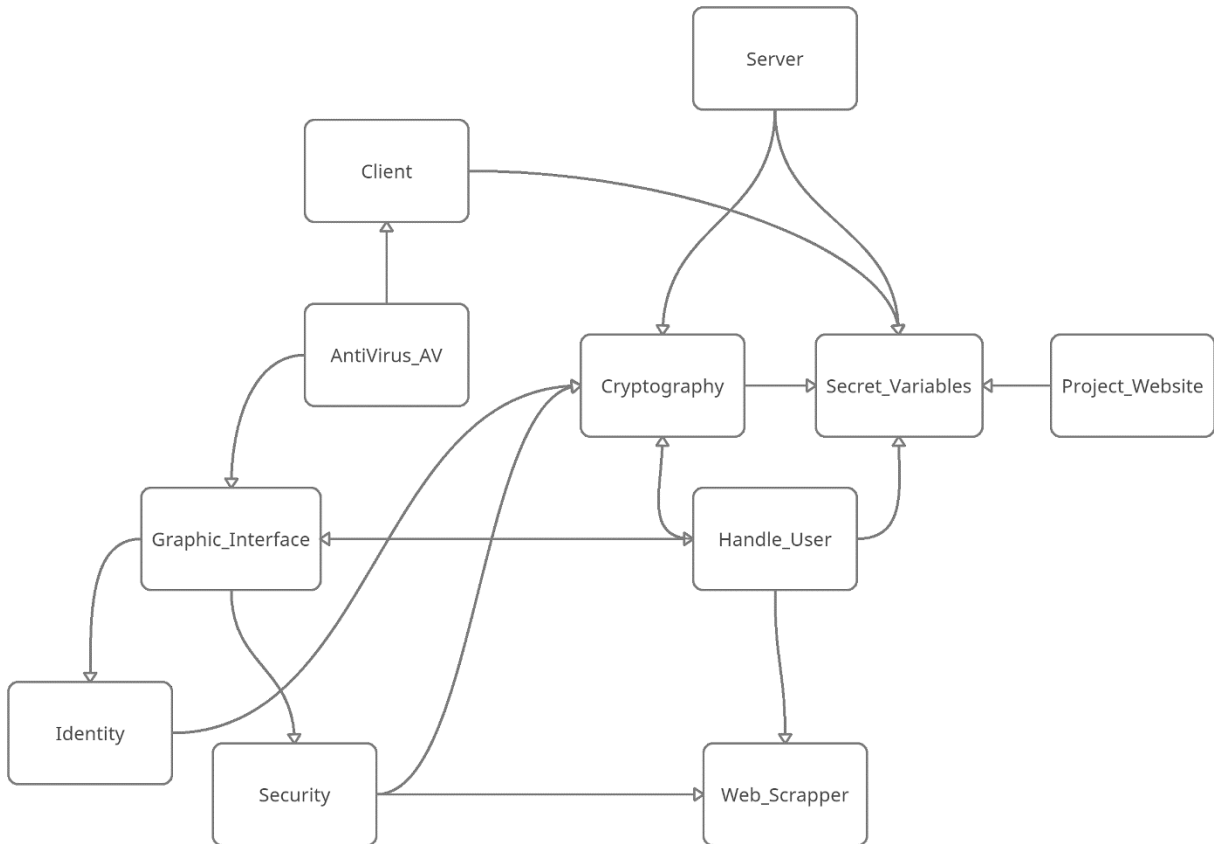


הסבר על דיאגרת הבלוקים הראשית של הפרויקט-

שם הבלוק	הסבר על הבלוק
Project_Website	האתר הראשי של הפרויקט- בנוי באמצעות ספריית Flask ב Python ומורץ על הענן בעזרת שירותי Repl.it . בעזרת האתר המשתמש מוריד את תיקיית ה- zip של הפרויקט.
Client	הלקוח של מערכת האנטי-וירוס. הלקוח מתחבר לשרת הראשי על ידי ביצוע לחיצת יד הכוללת העברת קוד מהשרת ללקוח אשר פותח את תוכנת האנטי וירוס אשר מוצגת למשתמש ע"י ממשק המשתמש אשר נבנה בעזרת ספריית Tkinter ב Python.
Server	השרת הראשי של מערכת האנטי-וירוס, השרת והלקוח מבצעים "לחיצת יד" ע"י העברת קוד אשר פותח את מסכי המערכת.
MongoDB	יחידת בסיס הנתונים של הפרויקט. נמצאת על הענן ומנוהלת על ידי שירותי MongoDB .

זרימת המידע בין המודולים (dataflow)

התרשים הבא מציג את זרימת המידע (data flow) ואת הקשר בין המודולים השונים של פרויקט האנטי וירוס שיצרת:



המודולים של המערכת

שם המודול	פירוט והסבר על המודול
Server (מודול השרת הראשי)	מודול זה אחראי על הרצת שרת ה- Socket עבור הפרויקט שאליו יתחברו לקוחות לצורך הפעלת הפרויקט.
Client (מודול הלקוח)	היחידה אחראית על ההתחברות לשרת הראשי של הפרויקט.
AntiVirus_AV (התוכנית הראשית)	תוכנית זו אחראית על הרצת מודול הלקוח אשר יתחבר אל השרת המרכזי. כמו כן, התוכנית אחראית על ניהול קבצים שונים שהמערכת משתמשת בהם לצורך ניהול השירותים השונים שהיא מספקת.
Cryptography (מודול ההצפנה)	מודול האחראי על ביצוע ההצפנות בכל הפרויקט. המודול מבצע הצפנה מסוג Vigenère Cipher וכן הצפנה לפונקציית גיבוב (hash). כמו כן, המודול מצפין ומפענח צפנים לפי קודים שונים להצפנה הנלקחים מתוכנית הנתונים הסודיים
Secret_Variables (מודול הנתונים הסודיים)	תוכנית המכילה סיסמאות, קודים ומפתחות הצפנה סודיים.
Handle_User	מודול העוסק בהרשמת משתמשים חדשים לבסיס הנתונים של המערכת ובניהול התחברויות משתמשים למערכת.
Graphic_Interface (מודול ממשק המשתמש)	המודול מציג למשתמש את מסכי המערכת השונים כלומר, זהו מודול ממשק משתמש גרפי.
Security (תוכנית האבטחה)	תוכנית המכילה את שירותי אבטחת המחשב שהמערכת מספקת: סריקת וירוסים, מציאת פער

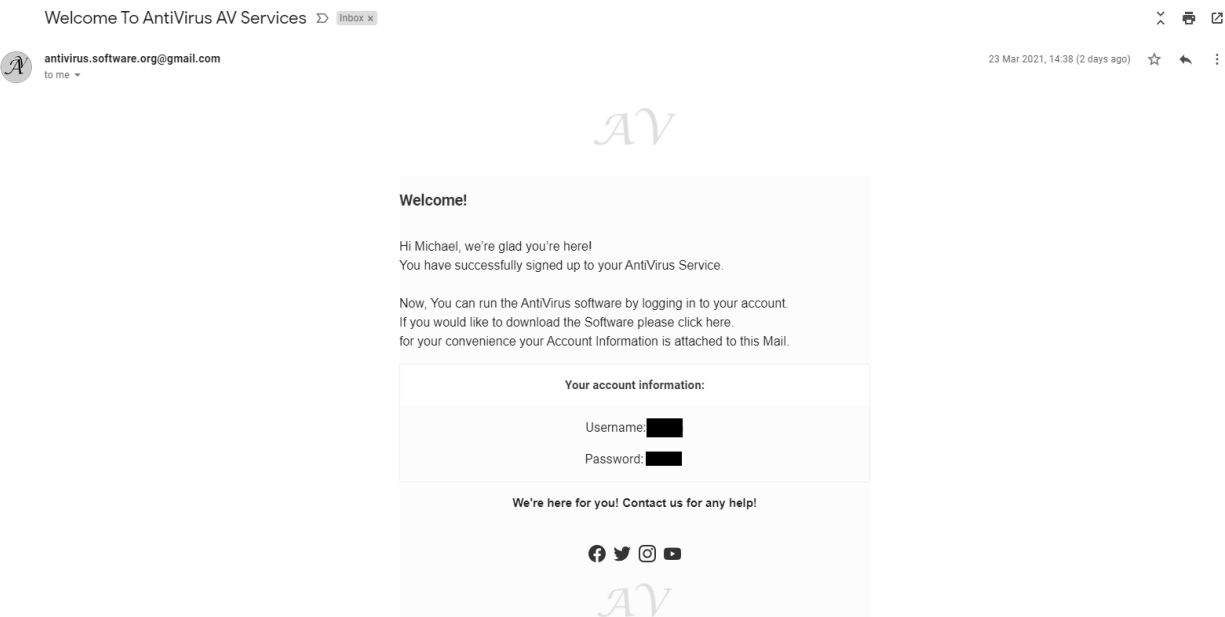
לעדכוני המחשב, עדכון תוכנת האנטי וירוס וסריקת חיבורים חשודים.	
תוכנית המכילה את שירותי אבטחת פרטיות המשתמש שהמערכת מספקת: גריסת קבצים, ניהול חומת האש של Windows, ניהול סיסמאות ונעילת קבצים פרטיים.	Identity (תוכנית הפרטיות)
מודול האחראי על הרצת אתר ה- Flask של מערכת האנטי וירוס- לפרויקט קיים אתר אינטרנטי אשר מורץ על ידי שרתי Repl.it בכתובת: AntiVirus-AV-Website	Project_Website (אתר הפרויקט)
תוכנית שמטרתה לשלוח מייל למשתמשים חדשים המצטרפים למערכת האנטי וירוס. המייל מכיל את פרטי ההרשמה וברכת הצטרפות למערכת. כמו כן, למודול זה תפקיד חשוב נוסף והוא לקחת מידע מן האינטרנט: המודול מספק לתוכנית האבטחה את הגרסה האחרונה של מערכת ההפעלה Windows הנלקחת מאתר Microsoft בכדי למצוא פער לעדכוני המחשב.	Web_Scrapper

כדי להפעיל את המערכת, ראשית יש להפעיל את תוכנית השרת הראשי ואת התוכנית הראשית של מערכת האנטי וירוס. התוכנית הראשית של מערכת האנטי וירוס מריצה גם את מודול הלקוח.

לאחר הרצת תוכניות אלו, השרת הראשי שולח ללקוח את קוד אישור להפעלת המערכת אשר נלקח ממודול הנתונים הסודיים. כאשר הקוד מתקבל, המערכת משווה את הקוד שהתקבל עם קוד הקיים בה, ובמידה והוא זהה לקוד שיש בה, נשלח אישור להפעלת המערכת וכתוצאה מכך מופעלת התוכנית האחראית על הצגת מסכי ממשק המשתמש, אשר מציגה את מסכי ההתחברות וההרשמה למערכת בהתחלה, ולאחר מכן את שאר מסכי המערכת. המטרה של פעולה זו היא ליצור את הקשר הראשוני בין המערכת והשרת ולוודא כי לא שונו נתונים סודיים על ידי המשתמש - תהליך זה הוא HandShake בין השרת ללקוח.

Use Case הרשמה והתחברות למערכת-

כאשר המשתמש נרשם אל מערכת האנטי וירוס, מודול ממשק המשתמש מקבל בתור קלט את פרטי המשתמש. פרטי המשתמש כוללים שם פרטי, מייל, שם משתמש וסיסמה. פרטי המשתמש מועברים אל תוכנית ניהול המשתמש שבה הם עוברים הצפנה בעזרת מודול ההצפנה של הפרויקט (לשם שמירה על פרטיות המשתמש). תוכנית ניהול המשתמש פונה אל בסיס הנתונים של הפרויקט אשר נמצא בשירות הענן [MongoDB](#), ורושמת את פרטי ההתחברות של המשתמש בבסיס הנתונים. נוסף על כך, תוכנית ניהול המשתמש מעבירה לתוכנית Web_Scrapper את נתוני המשתמש (מוצפנים) במטרה לשלוח למשתמש מייל עם ברכת הצטרפות ופרטי המשתמש שלו במערכת האנטי וירוס.



כאשר משתמש מתחבר אל מערכת האנטי וירוס, מודול ממשק המשתמש מקבל בתור קלט את שם המשתמש והסיסמה של המשתמש ומעבירים אל תוכנית ניהול המשתמש. תוכנית זו בודקת האם קיים משתמש בעל שם משתמש וסיסמה התואמים לאלו שסופקו בבסיס הנתונים ואם כן, נשלח אישור להצגת מסכי מערכת האנטי וירוס.

בסיס הנתונים של הפרויקט כולל אוסף מילונים בשם UsersDataBase אשר מקבל קבצי json, אלו הם עצמים המהווים מילונים שכן הם בעלי מפתחות וערכים עבור על מפתח. כל קובץ מילוני מכיל את פרטי המשתמש השונים.

Use Case סריקת וירוסים-

כאשר המשתמש מפעיל את שירות סריקת הוירוסים, נפתח חלון סריקת הוירוסים בו המשתמש יכול לבחור את סוג הסריקה. סוגי הסריקה הקיימים הם סריקה מלאה (סריקה אשר בודקת קבצים בעלי פוטנציאל להוות איום על המחשב), סריקה מלאה (אשר סורקת את כל סוגי הקבצים במחשב) וסריקה מותאמת אישית שהיא סריקה מלאה עבור נתיב סריקה משתנה. עבור סוג סריקה מותאמת אישית (בלבד) מקבל מודול ממשק המשתמש את נתיב הסריקה שהמשתמש הכניס אל תיבת הקלט. מודול ממשק המשתמש מעביר (במידה וקיים) את נתיב הסריקה לתוכנית האבטחה, נתיב הסריקה ברירת המחדל הוא כונן C: (במידה ולא שונה). בתחילה, תוכנית האבטחה מכניסה אל רשימה את כל נתיבי הקבצים אשר מיועדים לסריקה, עבור סוג סריקה מהירה אלו קבצי jar, bat, DLL, dll, exe. עבור סוג סריקה מלאה אלו כל סוגי הקבצים. במידה ולא זהו קבצים כבעלי פוטנציאל להוות וירוסים סריקת הוירוסים אינה מתבצעת שכן אין צורך בה. אך, כאשר התוכנית אכן מזהה קבצים בעלי פוטנציאל להוות איום על המחשב, התוכנית מתחילה לשלוח (בעזרת ריבוי פעולות - threading) את נתיבי הקבצים אל מתודת סריקה עמוקה. פונקציית הסריקה העמוקה יוצרת עבור כל קובץ את פונקציית הגיבוב (hash) שלו, ושולחת אותה אל מתודת הסריקה של שירותי Virus Total. מתודה זו שולחת את פונקציית הגיבוב של כל קובץ אל שירותי Virus Total בכדי לבדוק כמה תוכנות אנטי וירוס אימתו שהקובץ זדוני, במידה וקיימות מעל 20 (יותר משליש) תוכנות אנטי וירוס שאימתו כי הקובץ הוא בעל פוטנציאל להוות איום, הוא נכנס אל רשימת הקבצים הזדוניים. במידה ושירותי Virus Total לא הצליחו לסרוק את הקובץ, הוא נכנס אל רשימת הקבצים שלא נסרקו. לבסוף, התוכנית מציגה את תוצאות הסריקה, ובמידה ונמצא קובץ זדוני, המערכת מעבירה את נתיבו למודול ממשק המשתמש בכדי שיציגו למשתמש במטרה שיבחר אם ברצונו למחוק אותו או לא, ובמידה וכן הקובץ נמחק.

Use Case גריסת קבצים-

כאשר המשתמש מפעיל את שירות גריסת הקבצים, נפתח חלון גורס הקבצים, בו המשתמש בוחר את סוג הגריסה ואת נתיבה. סוגי הגריסה הקיימים הם Basic, Safe, Complete. סוג גריסה Basic גורס פעמיים את הקבצים, סוג גריסה Safe גורס 5 פעמים את הקבצים וסוג גריסה Complete גורס את הקבצים 10 פעמים. נתיבי הגריסה האפשריים הם סל המחזור, ותיקיית הקבצים הזמניים של מערכת ההפעלה. כאשר המשתמש

בוחר את נתיב הגריסה ואת סוגה, מודול ממשק המשתמש מעביר נתונים אלו אל תוכנית הפרטיות, שבהתאם לכל בחירה מבצעת את הפעולה המתאימה לה. עבור בחירת גריסת קבצים מסל המחזור או מתיקיית הקבצים הזמניים של מערכת ההפעלה- עבור כל קובץ, תוכנית הפרטיות פותחת אותו, מוחקת את הרשום בו, ממלאת את הקובץ בתווים אקראיים בבסיס 64 בהצפנת ascii (במטרה להעלים את הכתוב בו ולהקשות על שחזור הכתוב) ולאחר מכן מוחקת את הקובץ. פעולה זו חוזרת כמספר הפעמים של סוג הגריסה.

Use Case מציאת פער לעדכוני מערכת ההפעלה Windows-

כאשר המשתמש מפעיל את שירות מציאת העדכונים למערכת ההפעלה, נשלחת קריאה ממודול ממשק המשתמש אל תוכנית האבטחה להפעלת השירות. התוכנית בודקת לראשונה האם קיימת גרסת מערכת הפעלה (Windows) חדשה או גרסת Build חדשה (לדוגמא עדכון מ Windows 8 אל Windows 10 מגרסת build 19041.928 אל גרסת build 19042.928) ע"י פנייה אל מודול לקיחת המידע. מודול זה לוקח את גרסת מערכת ההפעלה האחרונה מאתר [Microsoft](https://www.microsoft.com) ומחזיר אותה לתוכנית האבטחה ובהתאם לכך התוכנית יודעת אם לבצע עדכון למערכת ההפעלה או לא. העדכון מתבצע בעזרת הפעלת כלי יצירת מדיית התקנה עבור Windows (MediaCreationTool20H2.exe). במידה ולא נמצא עדכון למערכת ההפעלה- תוכנית האבטחה בודקת האם קיים עדכון לאפליקציות ולדרייברים של Microsoft המותקנים במחשב. התוכנית משתמשת במודול הבנוי ב- Windows Powershell במטרה להתחבר אל שרת של Microsoft. השרת מספק לתוכנית רשימה של אפליקציות ודרייברים שהיא יכולה לעדכן ומעדכן אותם במחשב.

הסבר על תהליך סריקת הוירוסים במודול ה- Security

שם הפונקציה	מטרת הפונקציה	קלט	פלט
1. get_suspicious_files	לבדוק האם קיימים קבצים חשודים שיש לסרוק בנתיב סריקה מסוים ובסוג סריקה מסוים.	הפונקציה מקבלת את סוג הסריקה ואת נתיב הסריקה.	הפונקציה מחזירה רשימה של קבצים חשודים לסריקה.
1. virus_scan	הפונקציה היא הפונקציה הראשית של סריקה הוירוסים, היא מקבלת את רשימת הקבצים החשודים לסריקה, מבצעת את ההדפסות של הסריקה (למשתמש) ושולחת כל קובץ חשוד לסריקה ע"י קריאה לפונקציה <code>deep_scan</code> . לאחר סיום הסריקה, במידה ונמצאו קבצים זדוניים, הפונקציה מציגה את מסך מחיקת הקבצים הזדוניים.	הפונקציה מקבלת את סוג הסריקה ואת נתיב הסריקה.	X
2. deep_scan	הפונקציה יוצרת עבור כל קובץ שהיא מקבלת את פונקציית הגיבוב של הקובץ (hash) ושולחת אותו לפונקציית הסריקה ובהתאם לתוצאת הסריקה מכניסה (במידה והקובץ הוא וירוס) את נתיב הקובץ לרשימה של קבצים נגועים (זדוניים).	הפונקציה מקבלת את נתיב הקובץ.	X
3. virus_total_scanner	הפונקציה שולחת את פונקציית הגיבוב של הקובץ אל סורק של שירותי VirusTotal, ובודקת את תוצאת	הפונקציה מקבלת את נתיב הקובץ ואת פונקציית הגיבוב של הקובץ.	הפונקציה מחזירה אמת/שקר בהתאם לזיהוי הקובץ כקובץ נגוע (זדוני) או לא.

הסריקה. במידה ויותר
מ-20 (שליש) מתוכנות
האנטי-וירוס קבעו כי
הקובץ זדוני, הפונקצייה
מחזירה ערך חיובי
(אמת) לפונקציית ה
deep_scan ובמידה
לא, היא מחזירה ערך
שלילי (שקר).

מימוש קוד סריקת הוירוסים במודול Security -

```
def get_suspicious_files(scan_type, path=ROOT):  
    """  
    the function checks if there are suspicious files that need to be checked  
    and returns the suspicious file list.  
    :param scan_type: the type of the scan.quick or full  
    :param path: the requested path to be scanned; default path ---> ROOT  
    :return: a list of suspicious files that need to be deep scanned.  
    :rtype: list  
    """  
    files_list = list()  
    if scan_type == 'quick': # quick scanning- getting specific types of files  
        extensions_list = ['.exe', '.dll', '.DLL', '.bat', '.jar']  
        for root, dirs, files in os.walk(path):  
            for file in files:  
                file_path = root + os.sep + file  
                if Path(file_path).suffix in extensions_list:  
                    files_list.append(file_path)  
  
    elif scan_type == 'full': # full scanning- getting all types of files  
        for root, dirs, files in os.walk(path):  
            for file in files:  
                file_path = root + os.sep + file  
                files_list.append(file_path)  
    return files_list
```



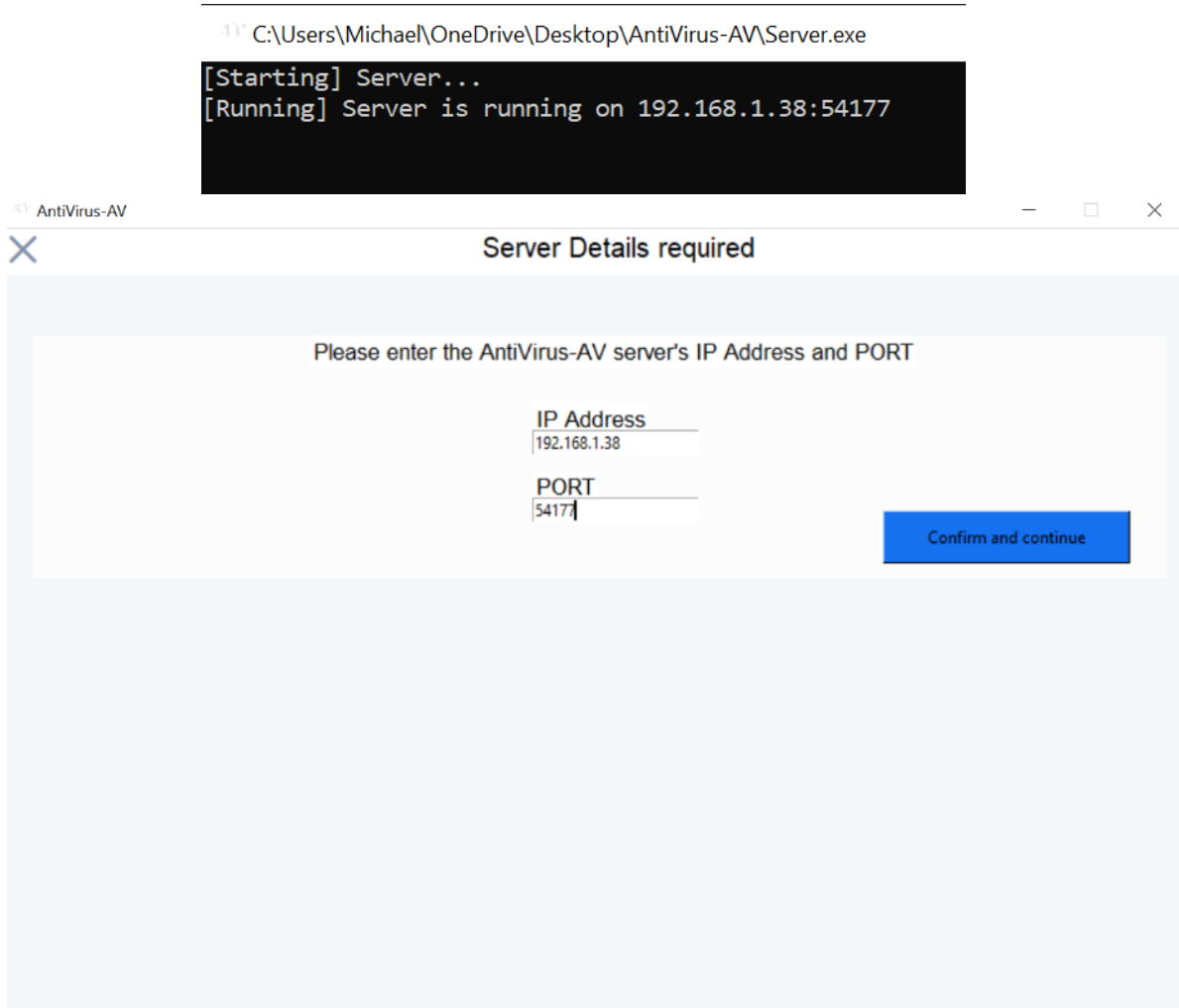
```
def deep_scan(file_path):  
    """  
    The function is used in order to read the file's Hash and send it to  
    Virus Total Scanner in order to determine if the file is infected.  
    :param file_path: the path of the file to be scanned  
    :return: None  
    """  
    global infected_files  
    try:  
        with open(file_path, "rb") as file:  
            file_content = file.read()  
            hashed_content = hashlib.md5(file_content).hexdigest()  
            is_infected = virus_total_scanner(file_path, hashed_content)  
            if is_infected: # if more than 20 AntiViruses determined that the file is infected  
                infected_files.append(file_path)  
    except:  
        pass  
  
def virus_total_scanner(file_path, hashed_content):  
    """  
    The function scans the file's hash content with  
    Virus Total scanning services and returns if the given hashed content is infected.  
    :param file_path: the file's path  
    :param hashed_content: the file's hash  
    :return: True/False according to whether the file is infected or not.  
    :rtype: bool  
    """  
    global failed_scanning  
    response = virus_scanner.get_virus_total_service().get_file_report(hashed_content) # getting the file report from virus total services  
    response = (json.dumps(response, sort_keys=False, indent=4))  
    if "response_code": 1 in response:  
        positive = response[response.find('"positives":'):response.find('"positives":') + 20]  
        found = True # Boolean auxiliary variable  
        for i in range(20):  
            if i in positive:  
                found = False  
        return found  
    elif "response_code": 0 in response: # failed to scan  
        failed_scanning.append(file_path)  
    return False
```

4. מדריך למשתמש

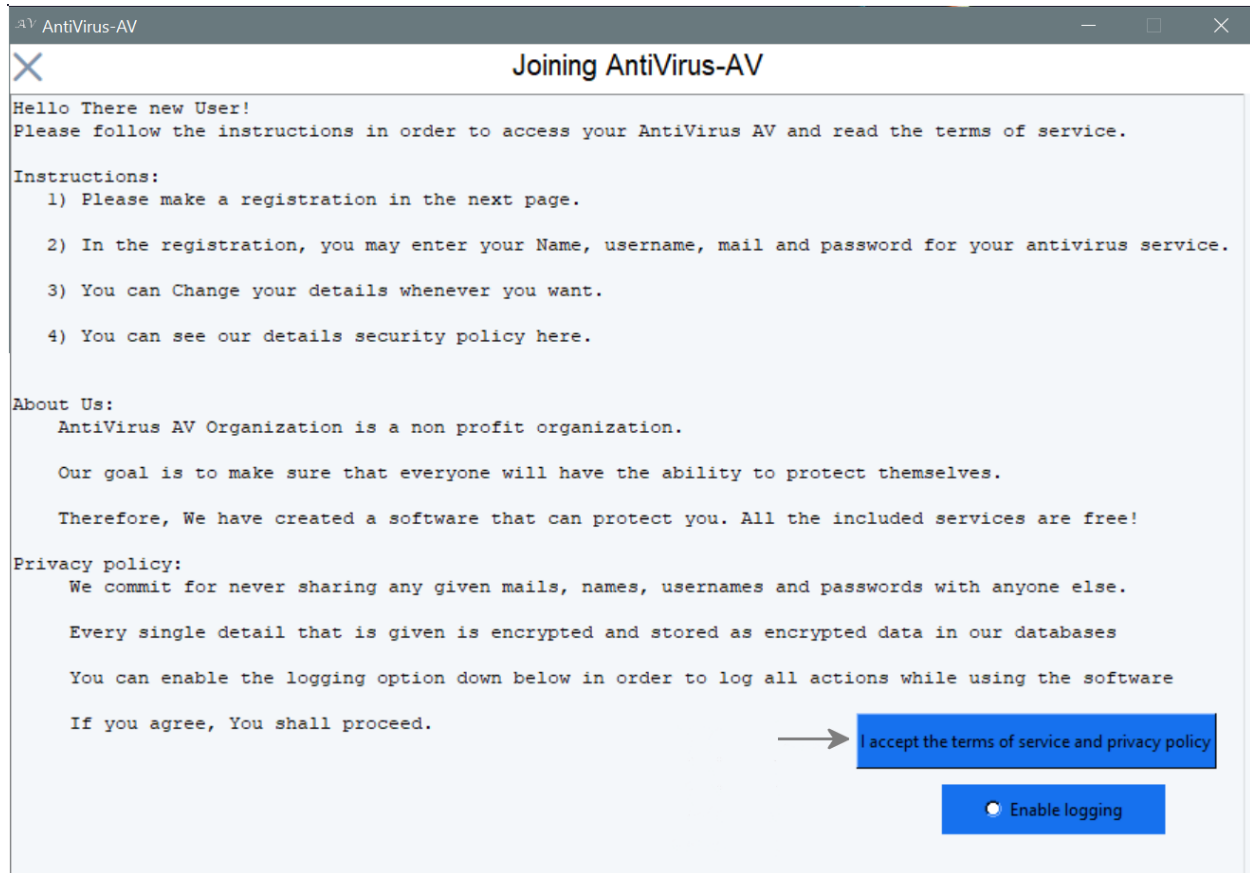
*הערה: מדריך זה נכתב בלשון זכר אך מתייחס אל שני המינים.

שלום לך משתמש יקר! אני שמחים לראות כי בחרת להשתמש במערכת האנטי וירוס שלנו. במטרה להפעיל את מערכת האנטי וירוס, יש לבצע מספר שלבים:

1. בשלב הראשון, יש להריץ את קובץ ה- Server.py (קובץ השרת הראשי) של מערכת האנטי-וירוס בבדי להתחבר למערכת. לאחר הרצת הקובץ יש להריץ את האפליקציה AntiVirus_AV.py בתוך תיקיית ה- Application תוך מתן הרשאות מנהל מערכת לקובץ. לאחר הרצת האפליקציה, ייפתח מסך אשר ידרוש את פרטי ההתחברות לשרת הראשי של מערכת האנטי-וירוס, יש להזין אותם כפי שהם מוצגים בשורת הפקודה (Command prompt) לאחר הרצת קובץ השרת הראשי (Server.py).



2. בשלב הבא, ייפתח מסך הכניסה, אנא קרא את הוראות ההרשמה, ולחץ על כפתור ההרשמה Sign Up במטרה להירשם לאפליקציית האנטי וירוס. אל דאגה! אנו לא משתפים שמות משתמשים, סיסמאות או כל נתון אחר שאנו מקבלים מכם. עדיין מודאגים? בדקו את הצהרת הפרטיות שלנו [About AntiVirus](#).
[AV](#).



The screenshot shows a window titled "Joining AntiVirus-AV". It contains the following text:

Hello There new User!
Please follow the instructions in order to access your AntiVirus AV and read the terms of service.

Instructions:

- 1) Please make a registration in the next page.
- 2) In the registration, you may enter your Name, username, mail and password for your antivirus service.
- 3) You can Change your details whenever you want.
- 4) You can see our details security policy here.

About Us:

AntiVirus AV Organization is a non profit organization.

Our goal is to make sure that everyone will have the ability to protect themselves.

Therefore, We have created a software that can protect you. All the included services are free!

Privacy policy:

We commit for never sharing any given mails, names, usernames and passwords with anyone else.

Every single detail that is given is encrypted and stored as encrypted data in our databases

You can enable the logging option down below in order to log all actions while using the software

If you agree, You shall proceed.

At the bottom right, there are two buttons: "I accept the terms of service and privacy policy" and "Enable logging".

כפתור ה- Enable logging מאפשר למערכת לכתוב תיעוד לכל הפעולות שמהשתמש מבצע במערכת. מתן הרשאה לאפשרות זו עשוי לתפוס שטח אחסון מהמחשב.



AntiVirus-AV

Back Please enter your details below

First Name
Michael

Mail
aelkhosh@gmail.com

Username
admin

Password

Sign Up

AntiVirus-AV

Access Required

Access is required- Please Make a Login or Sign up

Login

→ Sign Up

3. כעת, לחץ על כפתור ההיכנסות למערכת Login, סמן את תיבת הזכור אותי (Remember me) במטרה לאפשר גישה ישירה ומהירה יותר בעתיד לאפליקציית האנטי וירוס (לא חובה).

AntiVirus-AV

Back Please enter your details below

Username
admin

Password

Login

☒ Remember Me

AntiVirus-AV

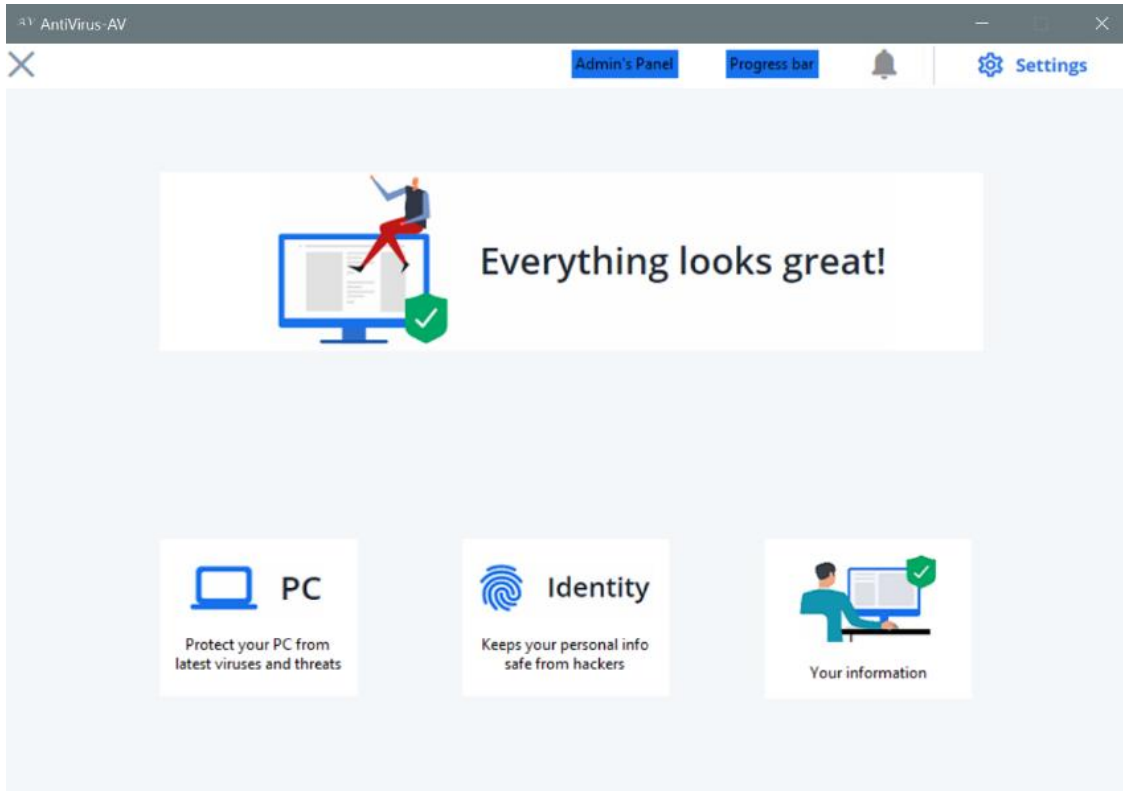
Access Required

Access is required- Please Make a Login or Sign up

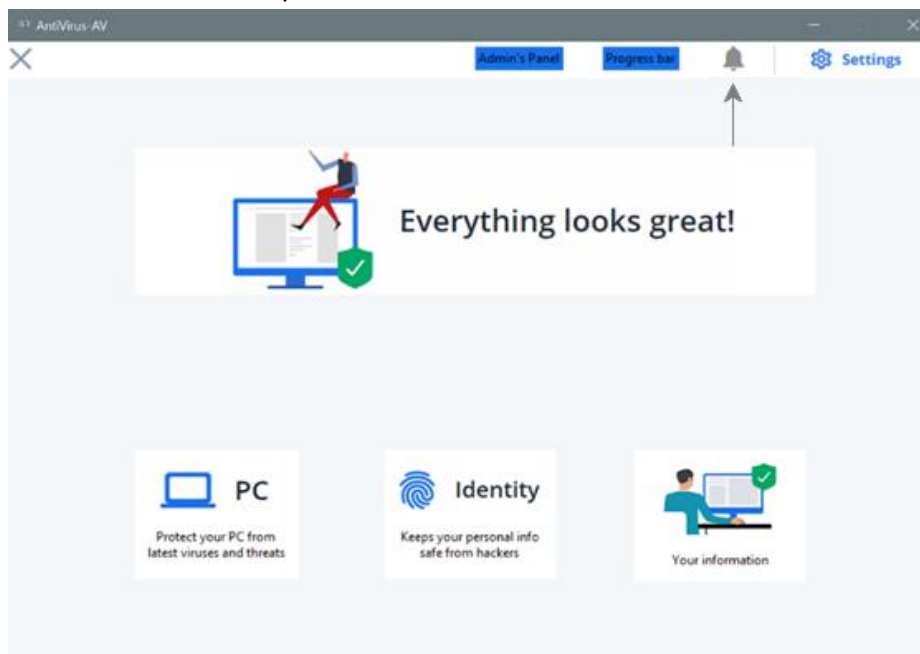
→ Login

Sign Up

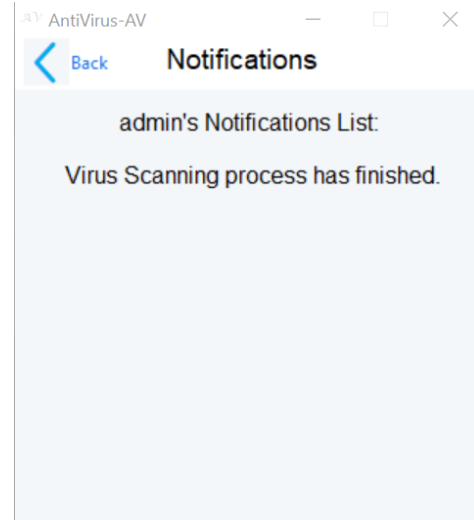
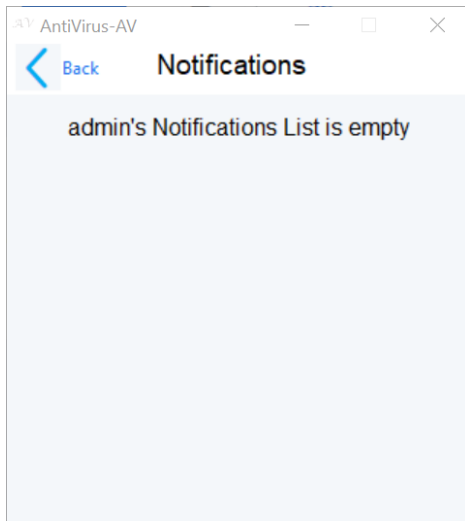
לאחר ההתחברות, תופנה אל המסך הראשי של תוכנת האנטי וירוס. בעת, תוכל להתחיל להשתמש בתוכנת האנטי וירוס.



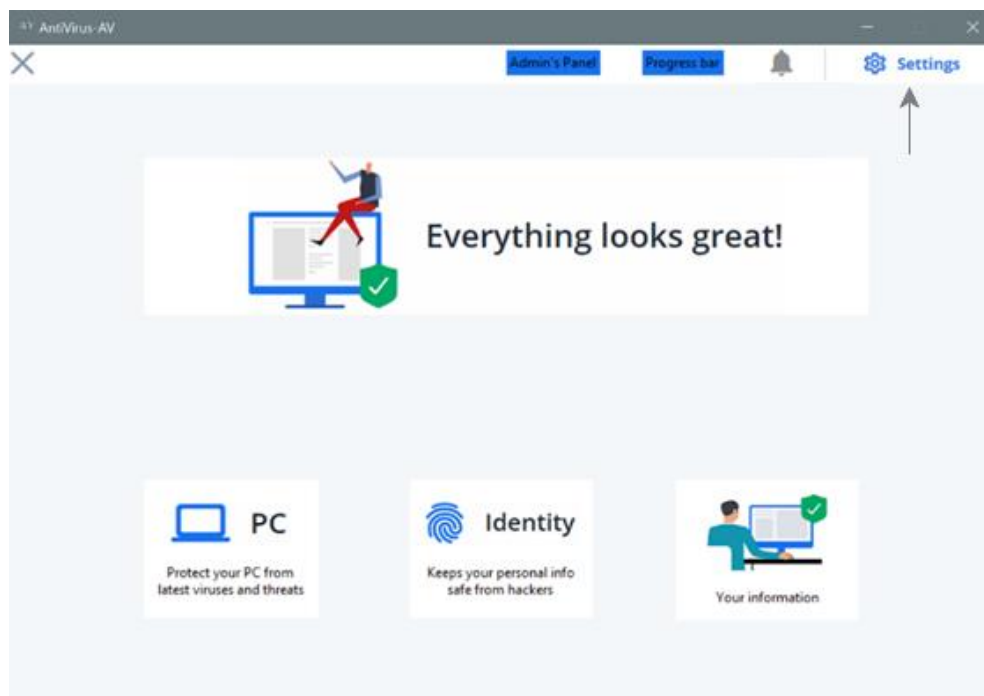
במסך הראשי, תוכל למצוא את מרכז ההתראות ע"י לחיצה על כפתור ההתראות. מרכז ההתראות הוא חלונית בה ניתן לראות את כל הודעות המערכת למשתמש. הודעת מערכת מתקבלת לאחר שהמערכת מסיימת לבצע פעולה.



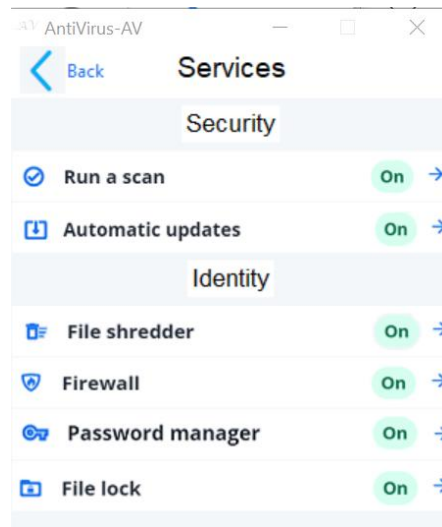
חלונות ההתראות-



כמו כן, במסך הראשי תוכל לעסוק בהגדרות המערכת ע"י לחיצה על כפתור ההגדרות (Settings)



מסך ההגדרות-



במסך זה, קיימת אפשרות לכבות שירות מסוים שהמערכת מספקת ע"י לחיצה על אותו השירות. פעולה זו אינה מומלצת אך עדיין ניתנת לביצוע. כאשר שירות כבוי, לא ניתן להשתמש בו.

המסך הראשי מתחלק ל-3 חלקים מרכזיים, חלק אבטחת המחשב תחת הכותרת PC, חלק אבטחת פרטיות המשתמש תחת הכותרת Identity והחלק המידעי תחת הכותרת Your information.

בחלון אבטחת המחשב, תוכל למצוא שירותים שונים שהמערכת מספקת לאבטחת המחשב.

השירותים כוללים את:

1. שירות סריקת הוירוסים המרכזי של המערכת.
2. שירות מציאת עדכונים למערכת ההפעלה (Windows).
3. שירות עדכון תוכנת האנטי וירוס AntiVirus AV.
4. שירות סריקת חיבורים חשודים במחשב.



בחלון אבטחת פרטיות המשתמש, תוכל למצוא שירותים שונים שהמערכת מספקת לאבטחת פרטיות המשתמש.

השירותים כוללים את:

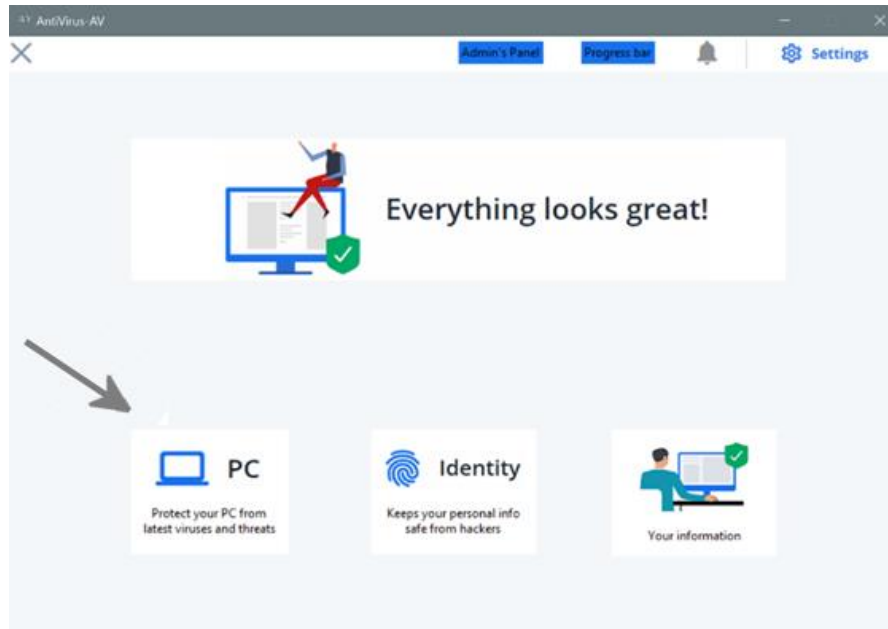
1. שירות גריסת הקבצים.
2. שירות ניהול חומת האש של Windows.
3. שירות ניהול סיסמאות.
4. שירות נעילת הקבצים של המערכת.

בחלון המידע, תוכל למצוא מידע נוסף על החברה, על מדיניות האבטחה והפרטיות שלה וכן ניתן ליצור קשר עם החברה.

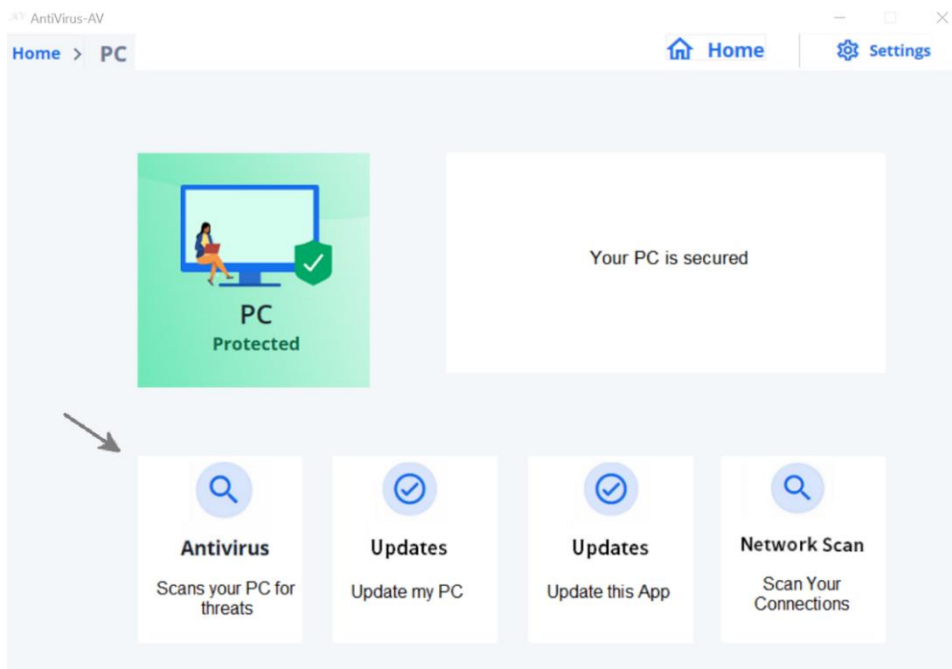
כעת נדגים כיצד להפעיל שלושה שירותים מרכזיים שמערכת מספקת.

שירות מספר 1- שירות סריקת הוירוסים (Virus Scanning)

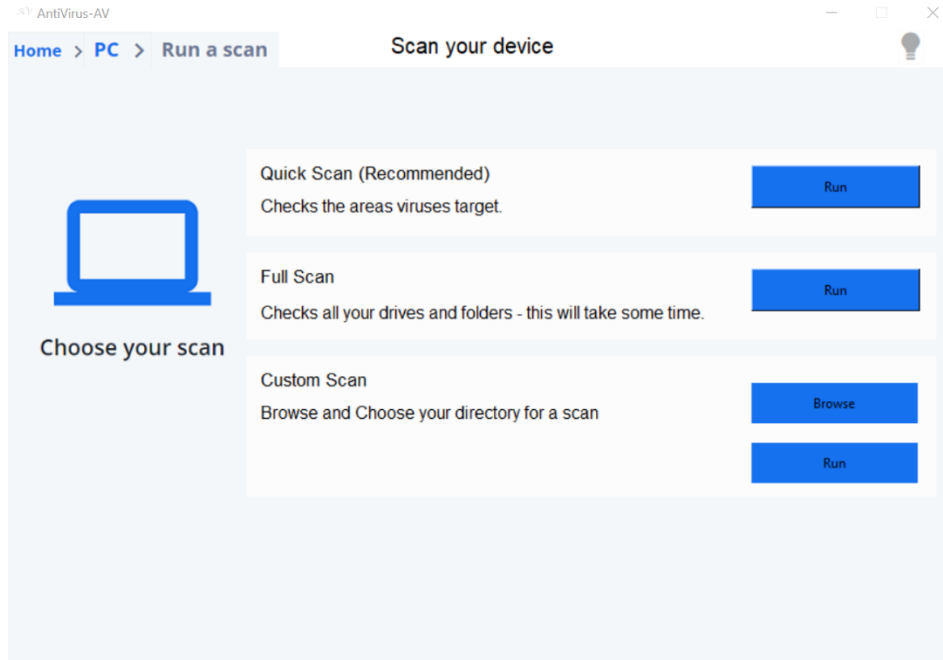
בבדי לגשת לשירות סריקת הוירוסים, יש לגשת לדף המרכזי העוסק באבטחת המחשב תחת הכותרת PC.



לאחר מכן, יש להכנס אל שירות סריקת הוירוסים אשר נמצא תחת הכותרת AntiVirus.



מסך סריקת הוירוסים-



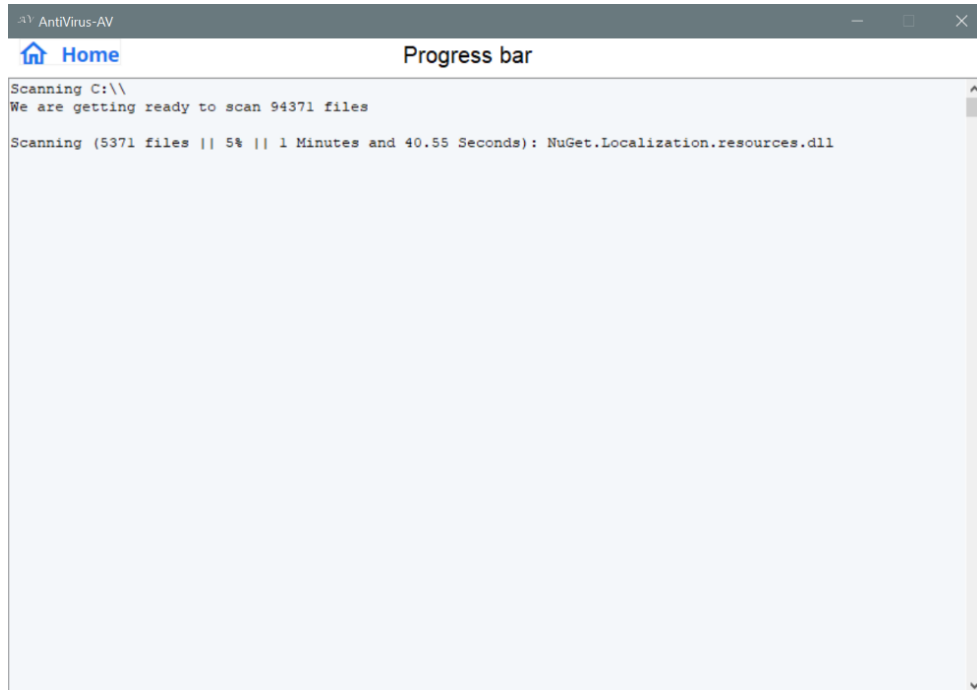
בדף שירות סריקת הוירוסים ניתן לבחור את סוג הסריקה המבוקש:

סריקה מהירה (Quick Scan)- היא סריקה הבודקת סוגים מסוימים של קבצים במחשב אשר עושיים להיות בעלי פוטנציאל להוות איום על המחשב.

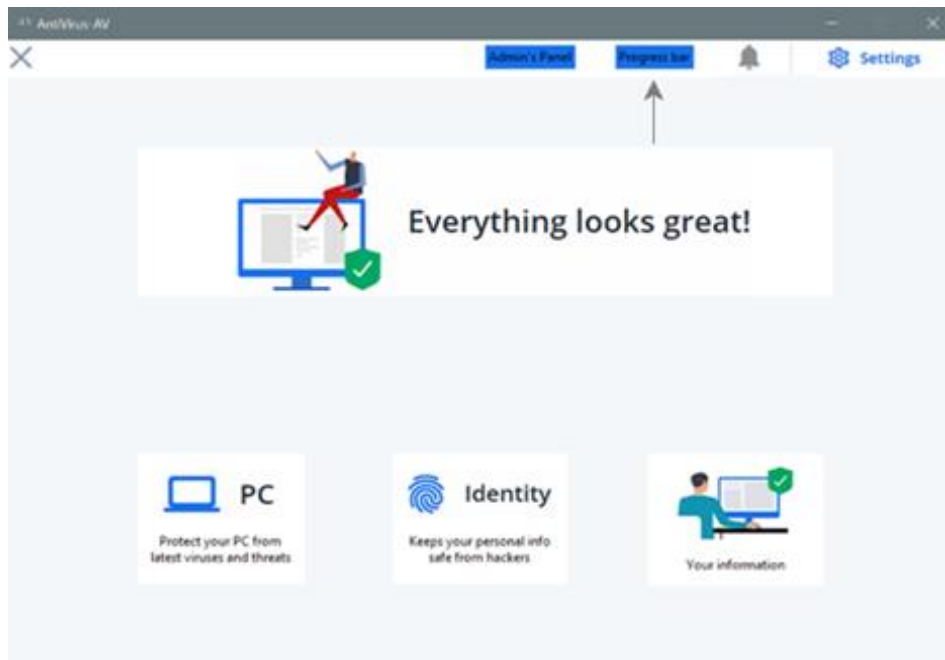
סריקה מלאה (Full Scan)- היא סריקה הבודקת את כל הקבצים במחשב, סריקה זו עשויה לארוך זמן רב יותר מהסריקה המהירה.

סריקה מותאמת אישית (Custom Scan)- זוהי סריקה מלאה אשר מתבצעת עבור מיקום ספציפי הנבחר ע"י המשתמש, יש ללחוץ על כפתור בחירת מיקום הסריקה (Browse) ורק לאחר מכן להריץ את הסריקה.

מהלך הסריקה-

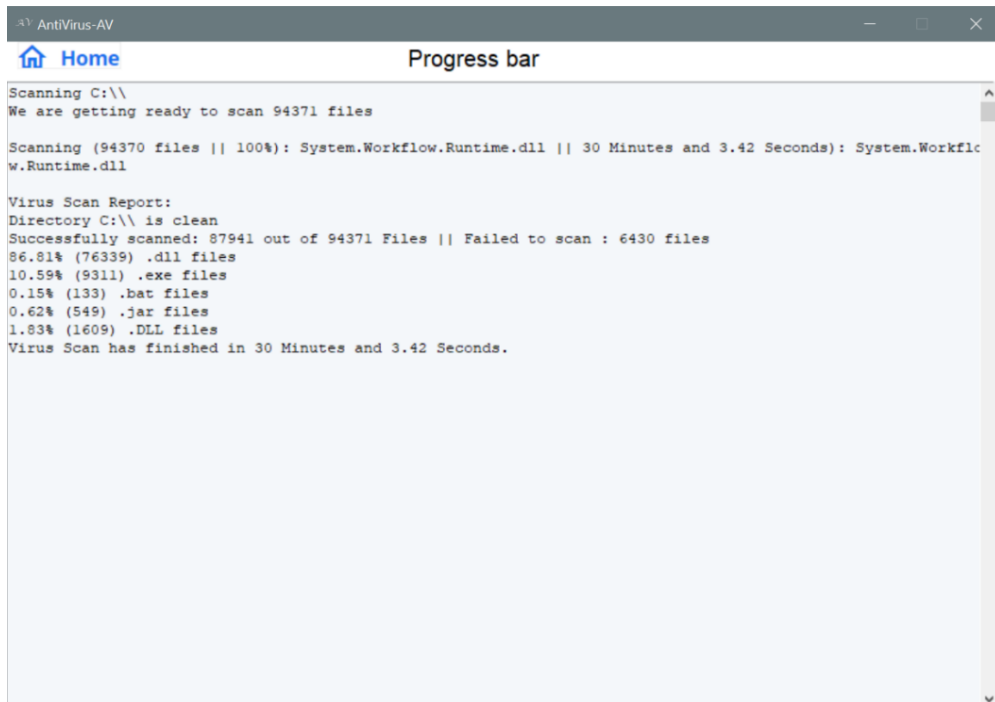


במהלך הסריקה, ניתן לצאת ממסך הפלט ע"י לחיצה על כפתור הבית (Home) בצד שמאל מעלה, תוכל תמיד לחזור למסך זה ע"י לחיצה במסך הבית על כפתור ה- Progress Bar.

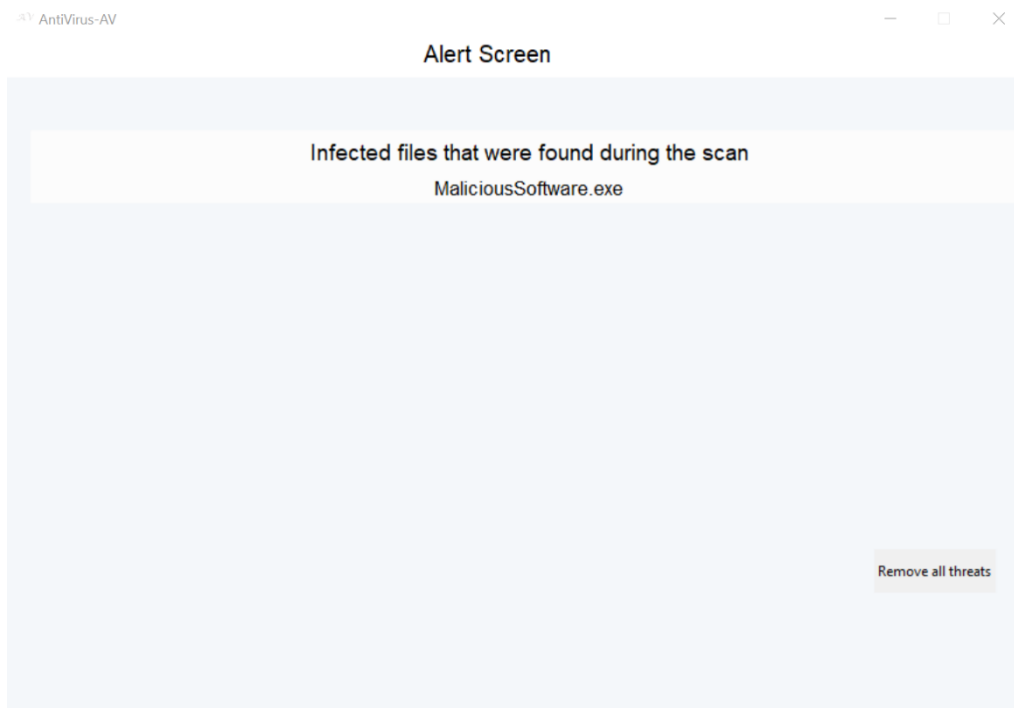




לאחר הרצת סריקת הוירוסים, המשתמש מקבל דוח סריקה שבו הוא יוכל לראות אם נמצאו קבצים זדוניים המהווים איום על המחשב ובמידה ונמצאו הוא יוכל למחוקם.

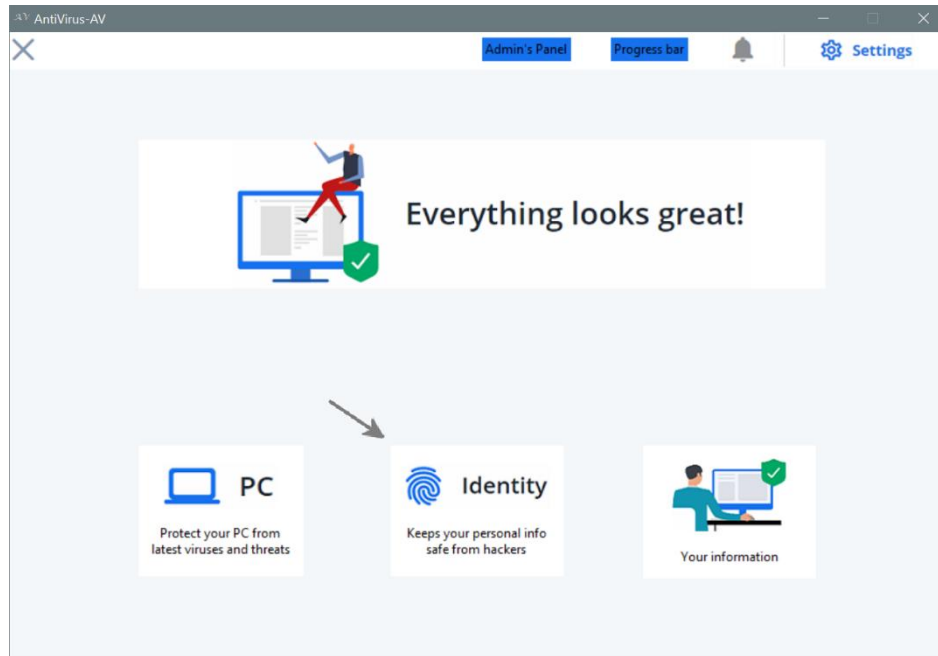


במידה ונמצא קובץ חשוד, ייפתח מסך האזהרה, שבו המשתמש יוכל להחליט אם למחוק את הקובץ או לא.

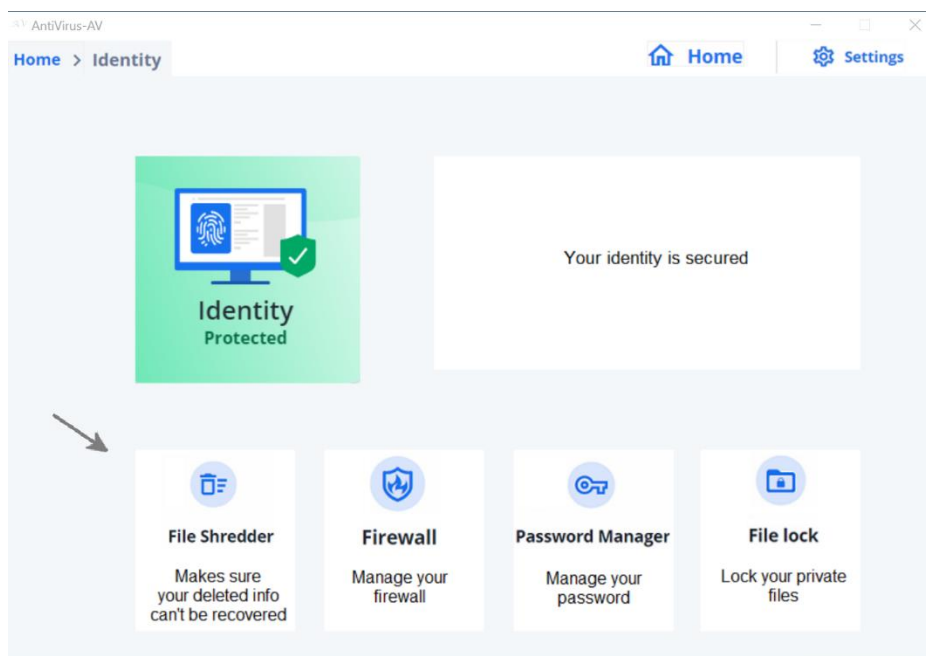


שירות מספר 2- שירות גריסה הקבצים (File Shredding)

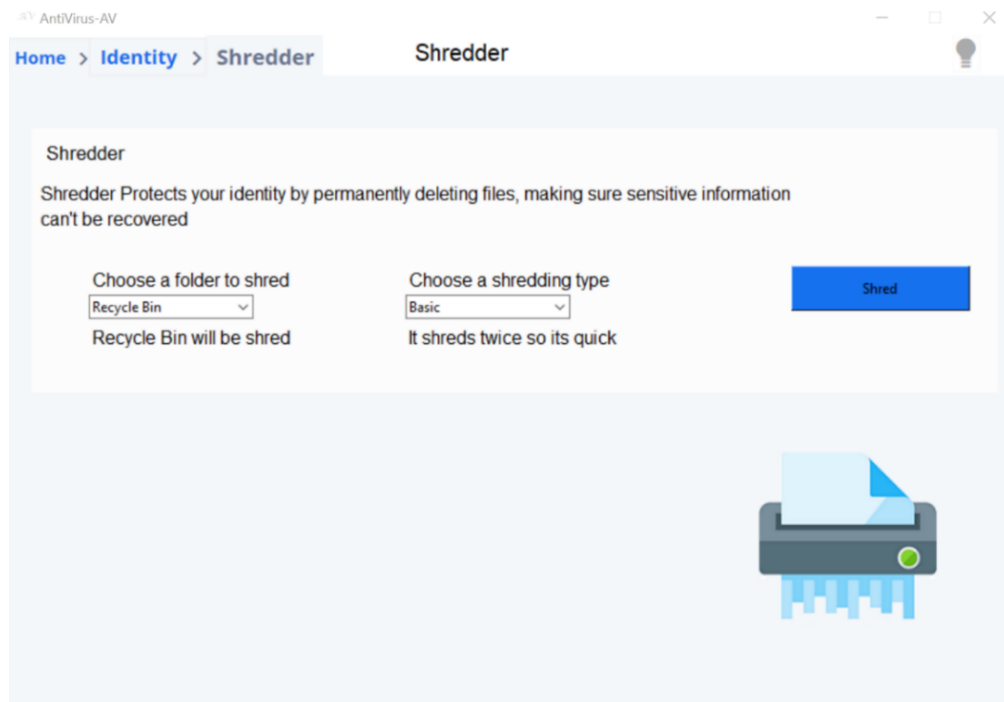
בכדי לגשת לשירות גריסת הקבצים, יש לגשת לדף המרכזי העוסק בפרטיות המשתמש תחת הכותרת Identity.



לאחר מכן יש להכנס לשירות גריסת הקבצים תחת הכותרת File Shredder.



מסך גריסת הקבצים-



במסך זה, ניתן לבחור את מיקום גריסת הקבצים- גריסת קבצים מסל המחזור או גריסת קבצים זמניים של מערכת ההפעלה.

כמו כן ניתן לבחור את סוג הגריסה- גריסה בסיסית, גריסה בטוחה וגריסה מוחלטת. ההבדלים בין סוגי הגריסות הוא במספר חזרות הגריסה לכל סוג גריסה.

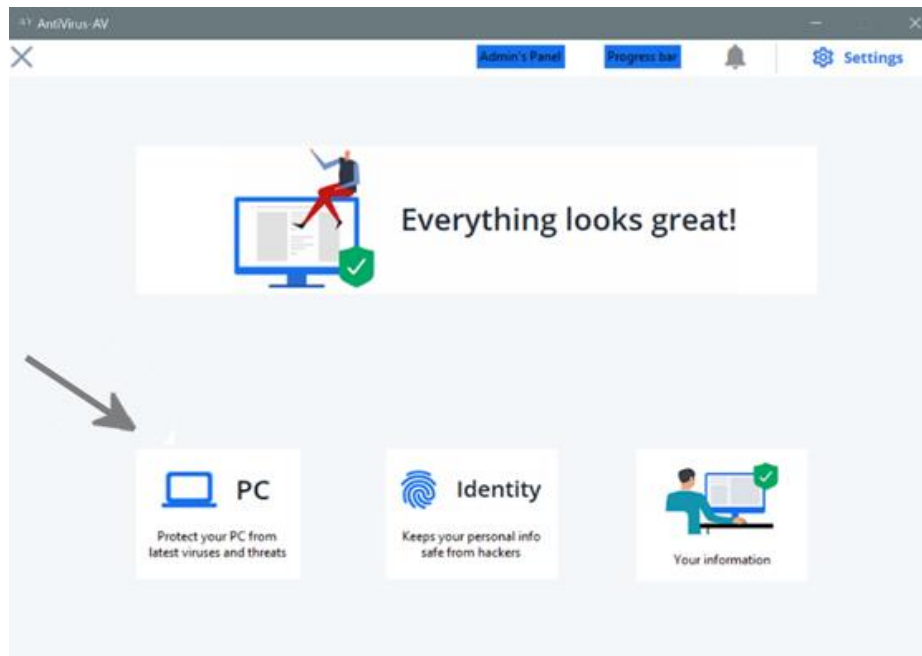
לאחר הרצת גורס הקבצים המשתמש יקבל את דוח הגריסה שבו הוא יוכל לראות את תוצאות הגריסה.



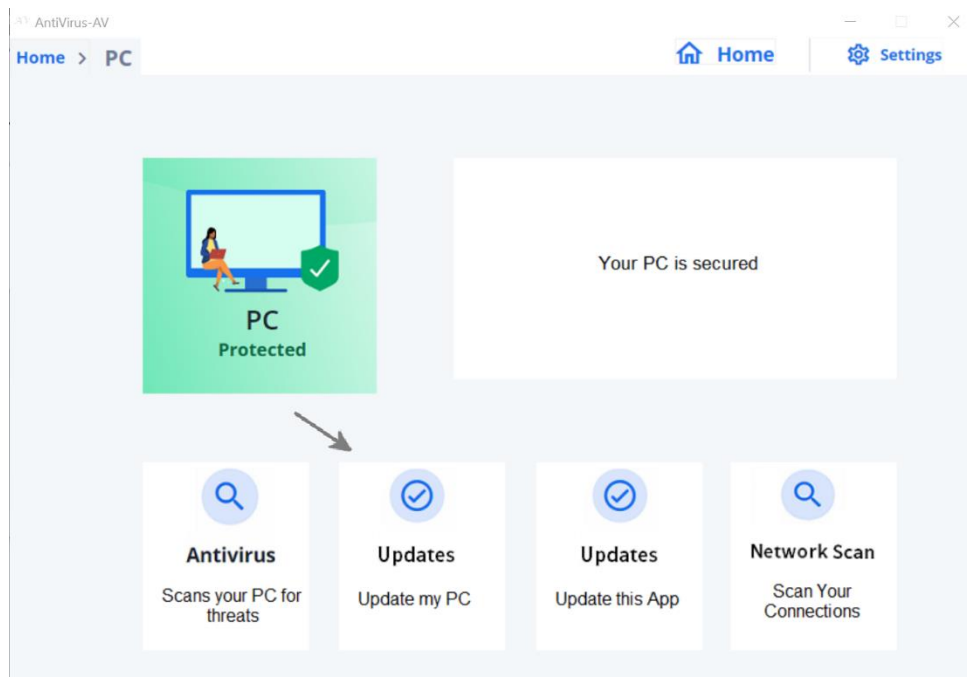
שירות מספר 3- שירות מציאת עדכונים למחשב (Updates)

בכדי לגשת לשירות מציאת עדכונים למחשב, יש לגשת לדף המרכזי העוסק באבטחת המחשב תחת הכותרת

.PC

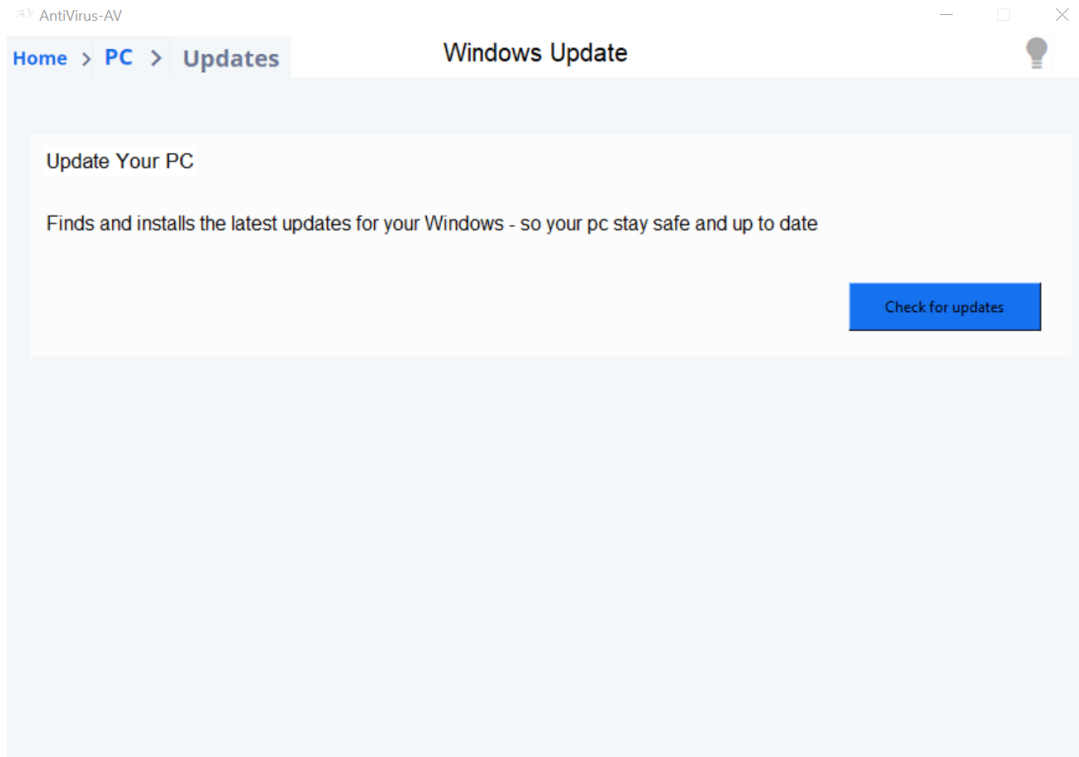


לאחר מכן, יש להכנס לשירות מציאת העדכונים למחשב הנמצא תחת הכותרת Updates.

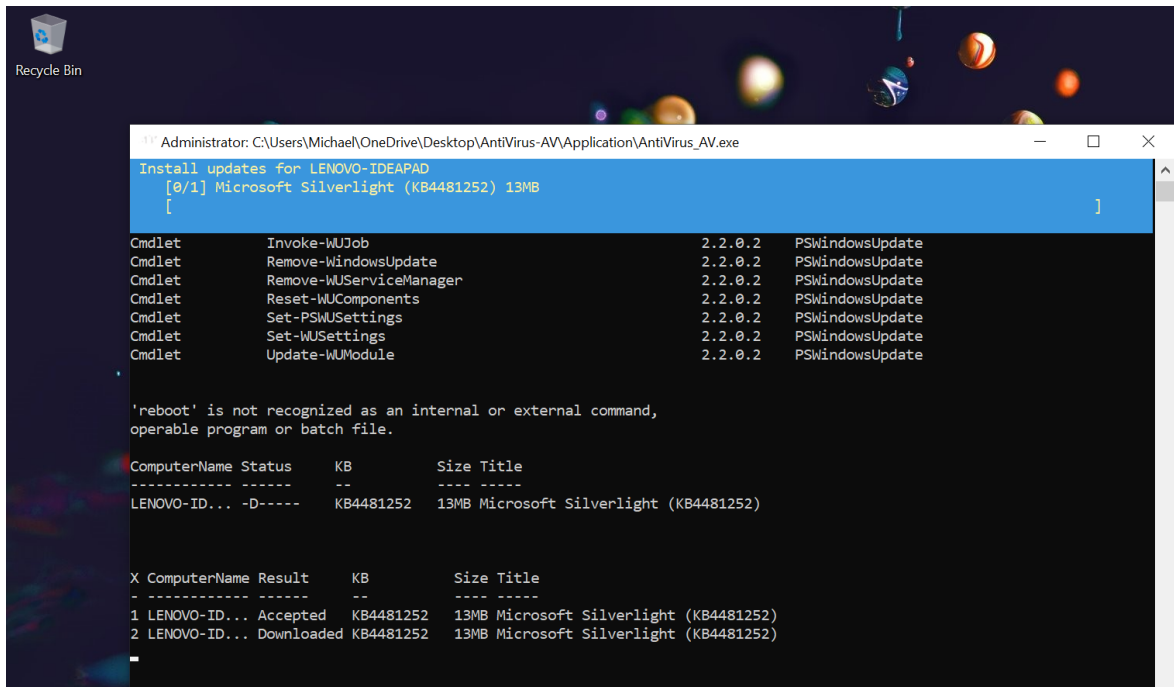




מסך העדכונים-



התקנת עדכון לדרייבר המחשב-



5. בסיס הנתונים

בסיס הנתונים בו השתמשתי במהלך פיתוח הפרויקט שלי הוא MongoDB. זהו שירות חינוכי המהווה מסד נתונים הנמצא בענן אשר פתוח וזמין לכל משתמש.

שירות [MongoDB](#) הוא שירות אשר דוגל בתפיסת NoSQL שהיא קטגוריה חדשה של בסיס נתונים אשר מעניקים פתרון אחסון וגישה למידע במבנה שאינו טבלאי, כפי שנפוץ בדרך כלל בבסיסי נתונים. השם NoSQL הוא קיצור של **Not Only SQL**, שמטרתו להדגיש שאכן קיימת תמיכה בשפת השאילתות SQL.

בפרויקט שלי, הקמתי בסיס נתונים הנקרא Users שבתוכו נמצאת טבלה הנקראת UsersDataBase. רשימת העמודות בטבלה כוללת מספר זהות (אוטומטי ומובנה ב-MongoDB), שם, מייל, שם משתמש, סיסמא ותאריך הצטרפות. כל העמודות הכרחיות לשם ביצוע ההרשמה, כולן מהוות משתנה מסוג מחרוזת (String) וכולן עוברות תהליך הצפנת hash/הצפנת ויז'נר (Vigenère cipher) מרגע קליטתם למערכת לשם שמירה על פרטיותו של המשתמש. דוגמא לרשומה במסד הנתונים עבור הרשמת משתמש

```
_id: ObjectId("606594907cb73a074441aa82")
Name: "&{{377g"
Mail: "F{{377g#$Y<qk#5NE@{:C"
Username: "21232f297a57a5a743894a0e4a801fc3"
Password: "21232f297a57a5a743894a0e4a801fc3"
```

דוגמה חזותית לרשומה
בבסיס הנתונים (במבנה
טבלאי)

ID	Name	Mail	Username	Password
ObjectId("603e63e992138e4dff47ba3a")	"3e06fa3927cbdf4e9d93ba4541acce86"	"F{{377g#\$Y<qk#5NE@{:C"	"21232f297a57a5a743894a0e4a801fc3"	"21232f297a57a5a743894a0e4a801fc3"

הסבר על התנהלות הפונקציות המרכזיות במודול ניהול המשתמש (Handle User) אל מול
בסיס הנתונים:

שם הפונקציה	מטרת הפונקציה	קלט	פלט
connect_to_db	פונקצייה שמתחברת לשירות בסיס הנתונים DataBase MongoDB בעזרת פרטי התחברות	X	X
insert_user_to_database	פונקצייה שמקבלת את פרטי המשתמש מוצפנים בתור מילון (json) ומכניסה אותם אל בסיס הנתונים.	הפונקציה מקבלת את פרטי המשתמש	הפונקציה מחזירה True/False בהתאם להצלחתה להכניס את פרטי המשתמש לבסיס הנתונים
authenticate_user	הפונקציה מאמתת את המשתמש על ידי קבלת סיסמה והחזרת אמת/שקר בהקשר להיות הסיסמה נכונה	הפונקציה מקבלת את סיסמת המשתמש	הפונקציה מחזירה True/False בהתאם לתנאי שבו הסיסמה שהתקבלה שווה לסיסמה השמורה במערכת
login_user	הפונקצייה אחראית על התחברות המשתמש למערכת האנטי-וירוס ועל הצגת כל התגובות עבור קלט פרטי המשתמש (סיסמה קצרה מדי, סיסמה או שם משתמש שגויים וכיוצא בזאת)	הפונקצייה מקבלת שם המשתמש וסיסמת המשתמש	X
register_user	הפונקצייה אחראית על הרשמת המשתמש לבסיס הנתונים על ידי קליטת פרטי המשתמש, הצפנתם ורק לאחר מכן הכנסתם לבסיס הנתונים	הפונקציה מקבלת את השם הפרטי, שם המשתמש, המייל והסיסמה מהמשתמש	X



מימוש הקוד במודול Handle User

```
def connect_to_db():
    """
    The function creates a connection to the DataBase.
    :return: the connection
    :rtype: Object
    """

    print('Connecting to MongoDB DataBase...')
    return MongoClient(DataBaseAccess)


def authenticate_user(password):
    """
    The function authenticates the user by comparing the given password to the stored password
    :param password: the given password to be compared to the stored password
    :return: True/False according to the authentication of the user
    """
    global user_instance

    return user_instance.get_password() == password


def insert_user_to_database(user_details):
    """
    The function gets a list of the user's details and inserts it to the database
    and returns True/False according to the success or failure of the action.
    :param user_details: dictionary of the user's details
    :return: True/False according to the success or failure of the action
    :rtype: boolean
    """
    database = connect_to_db().Users.UsersDataBase # connecting to the database

    try:
        database.insert_one(user_details) # inserting user's details to the database
        return True
    except:
        return False
```

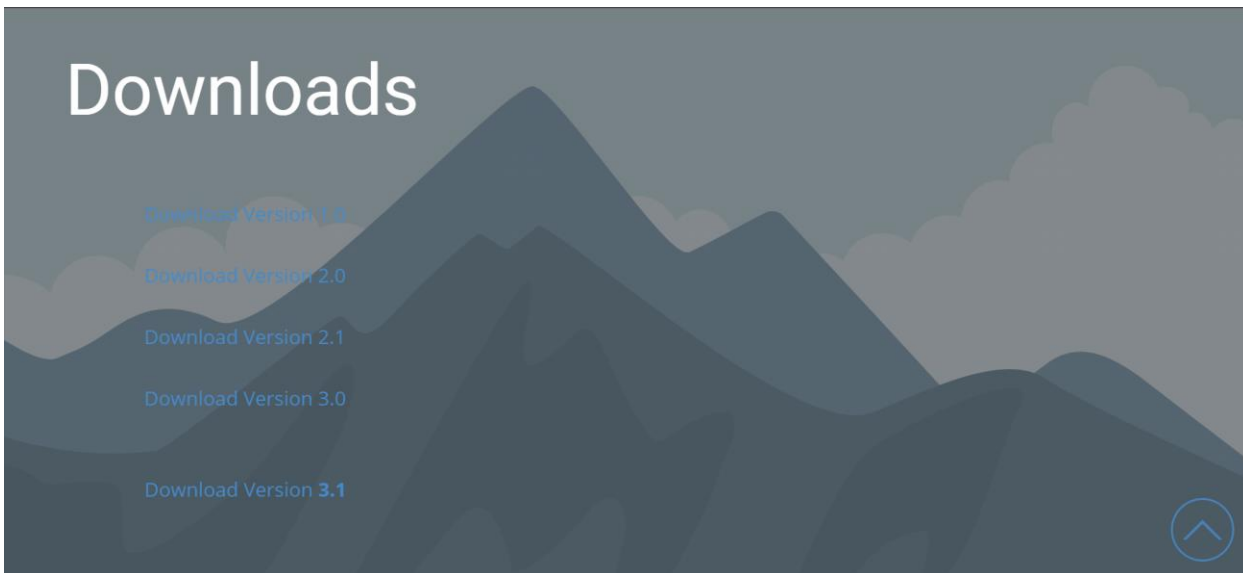
6. מדריך למפתח

*הערה: מדריך זה נכתב בלשון זכר אך מתייחס אל שני המינים.

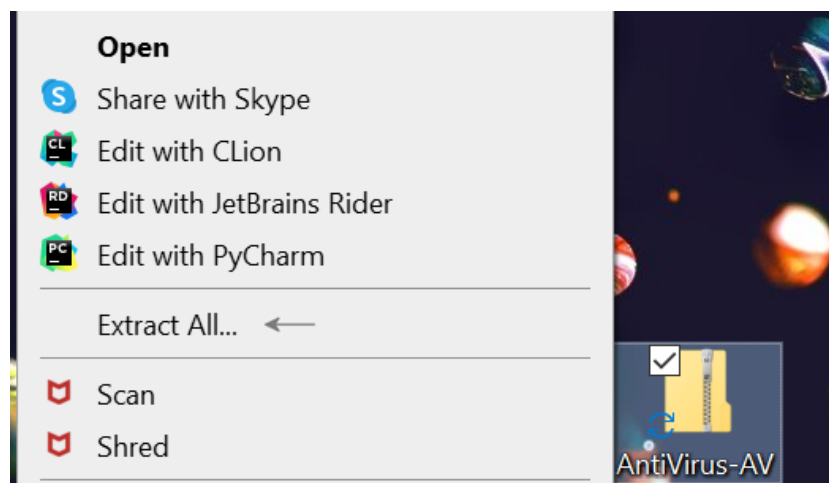
שלום לך מפתח יקר! אני שמחים לראות כי בחרת להשתמש במערכת האנטי וירוס שלנו.

במטרה להפעיל את מערכת האנטי וירוס, יש לבצע מספר שלבים:

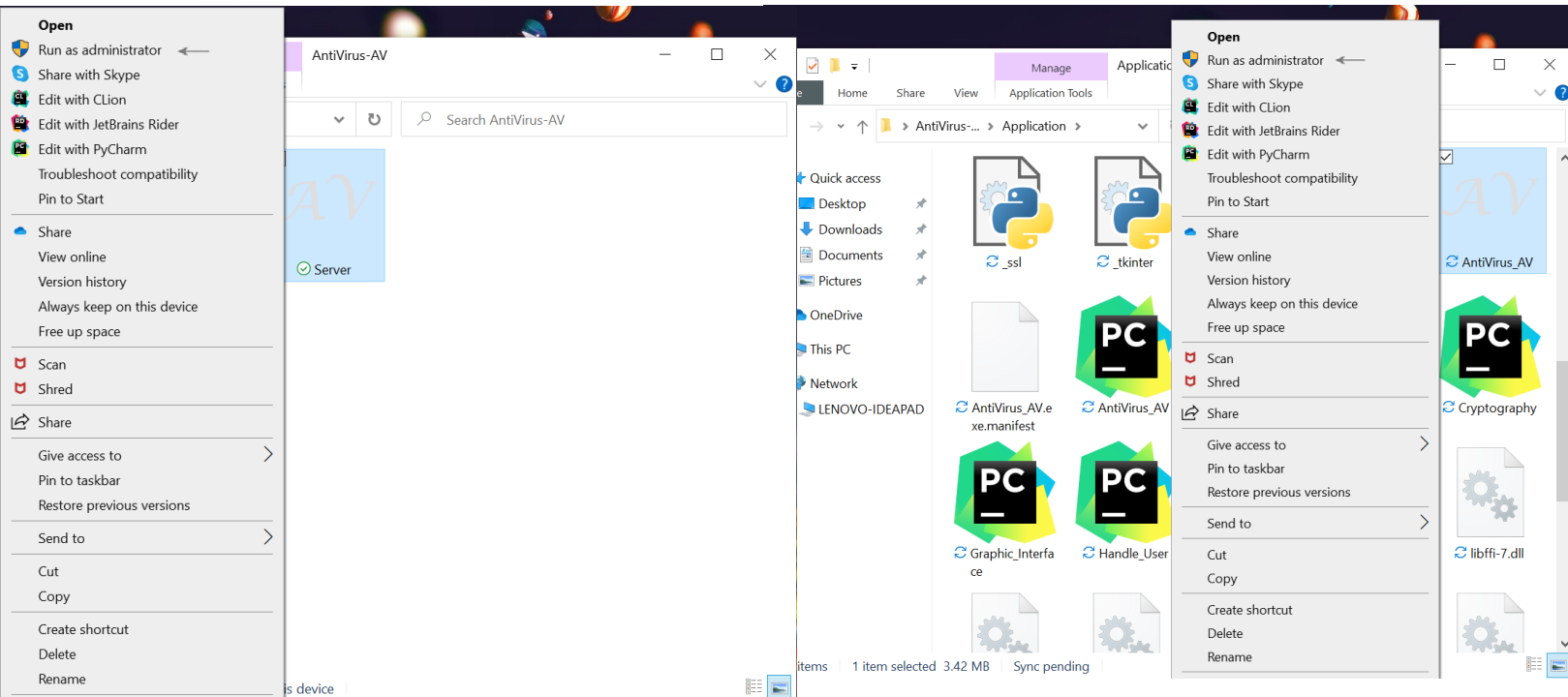
1. ראשית, עליך להכנס לאתר [Download AntiVirus AV](#), לחץ על הגרסה האחרונה (3.1) והורד את קובץ ה-zip (תיקייה דחוסה) של האפליקציה.



2. כעת חלץ את התיקייה, באמצעות לחיצה עם מקש ימני של העכבר, ובחירת חלץ קבצים.



3. כעת, לחץ ראשית על הרצה במצב מנהל מערכת (run as administrator) על קובץ ה- Server.exe במטרה לתת למערכת את ההרשאות המתאימות לה. לאחר מכן, בצע את אותה הפעולה עבור הקובץ AntiVirus_AV.exe אשר נמצא בתיקיית ה- Application.



7. סיכום אישי

באופן אישי, העבודה על הפרויקט היוותה עבורי אתגר משמעותי ביותר שכיום, אני שמח שקיבלתי על עצמי. בתחילת הדרך, שאפתי לייצר תוכנה חינוכית שתוכל לספק שירותים חינוכיים לצורכי אבטחת המחשב ופרטיות המשתמש של משתמשים בכל רחבי העולם שכן לא קיימות תוכנות רבות העושות זאת בחינם ובצורה איכותית. כיום, אני יכול להעיד כי אכן עמדתי במשימה זו- לאחר השקעה ממושכת הצלחתי לייצר תוכנה מקצועית אשר מסוגלת לשמור הן על אבטחת המחשב והן על פרטיותו של המשתמש.

אני יכול להעיד על עצמי, שלכל אורך פיתוח הפרויקט, הייתי חדור מטרה ונחוש ביותר להצליח ליצור את הפרויקט בצורה הטובה והיעילה ביותר שיכולתי, ראייה לכך היא שיצרתי שלושה גרסאות שונות של ממשק המשתמש בכדי שהשימוש בתוכנה יהיה קל ונוח עבור המשתמש, וכן בכדי להעצים את חווית השימוש בתוכנה.

העבודה על הפרויקט הקנתה לי כלים רבים וידע במגוון תחומים שאותם אקח להמשך דרכי בתחום מדעי המחשב והגנת הסייבר. אחד מהכלים המרכזיים והחשובים שקיבלתי ושאקח להמשך דרכי הינו ההתנהלות והעבודה שביצעתי אל מול חברה גדולה (Virus Total) בעזרת שירות סריקת הוירוסים (API) שהם סיפקו לפרויקט שלי.

כלי נוסף שקיבלתי במהלך העבודה על הפרויקט שלי הוא מיומנות בסריקת וירוסים וקבצים זדוניים וכן זיהוי קבצים חשודים בעלי פוטנציאל גבוה להיות וירוסים.

נוסף על כך, במהלך פיתוח הפרויקט קיבלתי ידע ומיומנויות בניהול בסיס נתונים בעזרת שירות MongoDB שבעזרתו ניהלתי את רשומות המשתמשים הרשומים למערכת האנטי וירוס.

יתר על כן, כלים נוספים חשובים לא פחות שקיבלתי במהלך העבודה על פרויקט הסייבר שלי הם ידע נרחב ע"י חקירה עצמית בתחומים Tkinter, Sockets, Cryptography, Flask - Web Scrapping, שכן בתחומים אלו נעזר הפרויקט שלי.

בפניי עמדו קשיים ואתגרים רבים במהלך פיתוח הפרויקט. האתגר הקשה ביותר שעמד בפניי היה למצוא את הדרך היעילה והמהירה ביותר לסרוק, למצוא וירוסים ותוכנות זדוניות במחשב. אני יכול להעיד על עצמי שאכן עמדתי במשימה זו לאחר השקעה רבה- הצלחתי לייצר תוכנה המספקת שירות מהיר, נוח ואף יעיל ביותר לסריקת קבצים במחשב.



קושי נוסף שעמד בפניי הינו הקושי לקבל גישה לאתר Virus Total על מנת שאוכל לייצר סריקת וירוסים מהירה, יעילה ואיכותית. בסופו של דבר התגברתי על קושי זה בעזרתה של המחנכת שלי כפי שמפורט בפרק המבוא לספר זה.

מסקנה חשובה אליה הגעתי לאחר סיום פיתוח הפרויקט היא שאין דבר שלא אוכל להצליח בו אם לא ארצה אותו, אשקיע בו ואעבוד עליו בנחישות ובחריצות כפי שעבדתי על פיתוח הפרויקט.

לו הייתי מתחיל לעבוד על הפרויקט היום, לא הייתי משנה שום דבר. אני חושב שדרך העבודה שלי ושילבי העבודה שלי אשר כללו תכנון מקדים לפרויקט, השקעה יום יומית והתמודדות עצמית עם בעיות ופתרון בעזרת חיפוש ולמידה עצמית היו נהדרים ועל כן לא הייתי משנה את אופן העבודה שלי על הפרויקט.



8. ביבליוגרפיה

1. [StackOverFlow](#)
2. [geeksforgeeks](#)
3. [PyPI](#)
4. [VirusTotal](#)
5. [MongoDB](#)
6. [Repl.it](#)