|  |
| --- |
|  |
| Network Computers Manager |
| פרויקט גמר בסייבר |
|  |
| **שם התלמיד: אריאל וסטפריד**  **ת"ז: 209368570**  **מנחים: ציכאל צ'רנובילסקי וגד רוזנטל**  **בית ספר: אורט גוטמן נתניה**  **כיתה: י"ב 8** |
|  |

**‏מאי 16**

|  |
| --- |
|  |

# תוכן עניינים

[תוכן עניינים 1](#_Toc451269529)

[רקע 2](#_Toc451269530)

[תיאור המוצר המוגמר 5](#_Toc451269531)

[מבט אישי על העבודה ותהליך הפיתוח 7](#_Toc451269532)

[תיאור הממשק למשתמש 9](#_Toc451269533)

[סביבת העבודה 13](#_Toc451269534)

[תיאור המודולים 14](#_Toc451269535)

[האלגוריתמים המרכזיים בפרוייקט 16](#_Toc451269536)

[תדפיס של הקוד 17](#_Toc451269537)

# רקע

**תקציר ורציונל הפרויקט**

תארו שאתם אחראיים על התפקוד של כל המחשבים ברשת אחת. בדרך כלל רשת כזו מונה מאות מחשבים, ואם יש בעיה תפקידכם הוא להגיע אל המחשב הספציפי ולטפל בו. בעיה יכולה להיות דבר פשוט בקבצים או מחשב שלא נדלק. האם באמת צריך לעבור ממחשב למחשב כל הזמן כדי לפתור בעיות ולפקח על פעילות המחשבים?

פריוקט זה מנסה לתת פתרון נוח עבור ניהול מחשבים ברשת על ידי מתן כלים לניהול מרחוק. בזמן שבו יש מחשבים בכל מקום ועיקר העבודה מתבצעת מהם יש צורך לפקח עליהם. כך, המנהל יכול לראות אילו מחשבים פועלים, אילו תוכנות רצות וגם לעבור על עץ הקבצים. כך מנהלים יכולים לראות מה קורה במשרד או הטכנאי יכול לעבור על המחשבים.

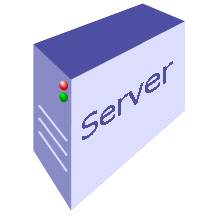
לדוגמה: אחד העובדים לא כיבה את המחשב בסוף יום העבודה. התוכנה מספקת אפשרות לכיבוי אוטומטי של מחשב או כמה בזמן רצוי.

דוגמה נוספת: ישנה פגיעה במערכת הקלט של אחד המחשבים. המערכת מאפשרת גישה אליו מרחוק כדי לבצע פעולות אחרונות (לדוגמה להוריד ממנו קובץ) לפני כיבוי לשם תיקון.

**מבוא ורקע כללי**

הרעיון העיקרי של הפרוייקט הוא מתן גישה נוחה מרחוק לשאר המחשבים ברשת. לכן, הפרויקט צריך גישה למחשבים דרך הרשת ולהצליח להשפיע על פעולותיו. כדי לעשות זו יש לפרויקט כמה מרכיבים עיקיים:

* מרכיב עיקרי בפרויקט שלי הוא פרוטוקול Wake on LAN. Wake on LAN, אחד מהתכונות העתיקות ביותר במערכות ההפעלה, המכונה לעיתים כ"השכמה מרחוק", היא טכנולוגיה המאפשרת להפעיל מחשב ברשת מרחוק על-ידי שליחת מנת נתונים מיוחדת (בנקראת מנת Magic). בעזרת התאמה בהגדרות, גם אם המחשב כבוי, מתאם הרשת עדיין "יאזין" לרשת, כך שכאשר המנה המיוחדת מגיעה, מתאם הרשת יכול להפעיל את המחשב.
* מרכיב נוסף חשוב בפרויקט שלי הוא תקשורת. תקשורת בעולם המחשבים מבוססת על Socket, שהם נקודות קצה עבור זרם נתונים בתקשורת בין תהליכים על גבי רשת מחשבים. רוב הסוקטים כיום מבוססים על ה – Internet Protocol (IP). בפרויקט שלי התקשורת בין השרת ללקוחות מתבצעת באמצעות Internet Socket, כאשר בשכבת התעבורה יש שימוש בפרוטוקול ה-TCP, שייחודו בכך שהוא מוודא שכל הנתונים שנשלחו התקבלו ובסדר הנכון, ואחרת שולח אותם שוב. בפרויקט שלי יש חשיבות לכך שלא יהיה איבוד מידע ופרוטוקול ה-TCP/IP מתאים בדיוק למטרה זו.
* מרכיב שלישי בעל חשיבות לפרוייקט הוא היכולת להתעסק עם מערכת ההפעלה. כך ניתנת לתוכנה גישה לקבצים, לתהליכים וכדומה. לשם כך אני משתמש ב – Windows API. ה-Windows API הוא סט כלים תכנותיים אשר נותנים למתכנתים גישה למערכת ההפעלה. כך, הפרויקט יכול לגשת דרך מערכת ההפעלה לקבצים ולתוכניות.
* מרכיב נוסף בפרויקט הוא שימוש ב-GUI שאפשר להתחבר אליו דרך הדפדפן. כך, אפשר לגשת לשרת מכל מחשב ברשת על ידי הדפדן. דבר זה ניתן על ידי מודול Flask אשר פותח שרת HTTP במחשב ומטפל בתקשורת בין השרת ללקוח (הדפדפן). השרת פונה לקוד שנכתב על ידי המשתמש בעת בקשת דף ומחזיר את מה שמחזיר הקוד.
* בנוסף, הפרויקט משלב עבודה עם מסד נתונים. הנתונים שהתוכנה אוספת לגבי כל אחד ממחשבי הרשת נשמרים במסד הנתונים, שהעבודה איתו היא בטכנולוגיית ה – SQLite, שמממשת את רוב הסטנדרט של SQL (שהיא השפה המקובלת לטיפול ועיבוד מידע בבסיסי נתונים). להבדיל מרוב המערכות לניהול בסיסי נתונים, SQLite אינה תהליך עצמאי נפרד, אלא ספריה בתוך התהליך באופן אינטגרלי. זוהי בחירה פופולרית כאשר מפתחים בסיס נתונים מוטמע עבור צד לקוח כשירות ניהול מידע מקומי. מסד הנתונים שאותו מנהלת התוכנה שלי שומר מידע לשימוש מקומי בלבד, ולכן בחרתי להשתמש ב-SQLite שלא דורש הרצה של SQL Server.



דפדפן

שרת HTTP

שרת ראשי

עם מסד נתונים

לקוחות

לקוחות

לקוחות

תאור הרשת בפרויקט ותקשורת בין חלקיה

# תיאור המוצר המוגמר

שם המוצר הוא Network Computers Manager.

ביכולתו להדליק ולכבות מחשבים מרחוק (בתוך הרשת) לפי זמן שנקבע מראש. על מחשבים בהם פועלת תוכנת הלקוח אפשר לבצע פעולות נוספות: גישה לקבצים, מחיקתם או יצירת חדשים, גישה לתהליכים עצירתם או הפעלת תהליכים אחרים. כל זאת כאשר ממשק המשתמש של התוכנה נפתח בדפדפן וכך, יכול להפתח מכל מחשב ברשת בעזרת הדפדפן, כל עוד השרת עובד באחד המחשבים ברשת.

המטרות המרכזיות של ה-Network Manager Tool הן הקלת העבודה על מנהל הרשת. הוא יכול לפקח על המחשבים ופעולותיהם מרחוק ואין לא צורך לגשת אליהם פיזית. בנוסף, הממשק מאפשר גישה לשרת מכל מחשב ברשת דרך הדפדפן כך שגם אם מנהל הרשת לא ליד העמדה שמחוברת למחשב השרת, כל עוד עמדתו מחוברת לרשת הוא יכול לגשת אליה. כל זה קורה תוך תקשורת מאובטחת בין השרת והלקוחות.

שאלות שהמערכת עונה עליהן:

**כיצד ימצאו תוכנות הלקוח את השרת?** כל כמה שניות, השרת שולח הודעת Broadcast שכוללת את המפתח הפומבי שלו ו-Hash של הודעה שנקבע מראש. תוכנת הלקוח שהופעלה זה עתה תאזין לקשורת ותאתר את ההודע הזו, לאחר אימות של המסר שנקבע מראש, יתחיל הלקוח בתהליך החיבור לשרת.

**כיצד להפעיל מרחוק מחשב?** קיימת אפשרות להפעיל מחשב מרחוק דרך כרטיס הרשת. יש לסדר בהגדרות המחשב שגם כאשר הוא כבוי, כרטיס הרשת ישתמש במעט חשמל כדי להאזין לתקשורת . כאשר כרטיס הרשת מוצא Magic Packet שמיועדת לו, הוא יפעיל את המחשב.

**כיצד לגשת לקבצים ולתהליכים של מחשב מרוחק?** דבר זה נעשה בעזרת תקשורת שרת – לקוח. השרת שולח ללקוח שלו את הבקשה שלו (לדוגמה: מחיקת קובץ ספציפי) והלקוח בעזרת הגישה ש-Windows API מאפשר לו, מבצע אצ הפעולה ומחזיר תשובה לשרת.

השוואת העבודה עם פתרונות ויישומים קיימים:

ישנן תוכנות המבצעות Wake on LAN וגם תוכנות דרכן אפשר לפקח מרחוק על המחשבים ברשת. לא נמצאה תוכנה שלממשקה אפשר לגשת דרך הדפדפן, כאמור דבר המאפשר נוחות וגישה לשרת גם מהמחשבים שלא מריצים אותו עליהם. בנוסף, התקשורת בין השרת והלקוח מאובטחת ולכן אין חשש שגורם זר ישפיע על מחשבים ברשת. לעומת זאת בתוכנה הנוכחית, אין פיקוח על דברים הקשורים בחומרה כמו פיקוח על טמפרטורת מעבד וצריכת משאבי מערכת. בנוסף אין תמיכה באותיות עבריות במערכת הקבצים והתהליכים.

# מבט אישי על העבודה ותהליך הפיתוח

במהלך העבודה עמדתי לפני כמה אתגרים והיו לי כמה מחקרים לעשות:

* תחילה, להבין כיצד להפעיל מחשב מרחוק. למדתי שקיים פרוטוקול Wake on LAN שאני יכול להיעזר בו. למדתי שיש צורך לאפשר הגדרות מסוימות ב-BIOS של המחשב ובהגדרות מערכת ההפעלה כדי לאפשר לפרוטוקול לעבוד ואכן להפעיל את המחשב.
* שנית היה עלי להבין כיצד אני יכול לדעת שמחשב היעד אכן קיים וכיצד למצוא אותו. לאחר חיפוש באינטרנט וקריאה של חומר, הבנתי שכל עוד המחשב כבוי, אי אפשר לדעת על קיומו. כדי לפתור את הבעיה היה עליי למצוא את המחשב כאשר הוא פועל ולשמור במאגר נתונים את קיומו. כך אדע שהמחשב קיים ואוכל ליידע את המשתמש על כך גם כאשר הוא לא פועל ולא נמצא ברשת.
* לאחר מכן היה עליי להבין כיצד למצוא מחשבים ברשת. על כך היה עליי להשתמש בפרוטוקול ARP – Address Resolution Protocol. התוכנה עוברת על כל הכתובות ה-IP האפשריות ברשת ושלחת ב-broadcast שאלה למי יש את הכתובת. מחשב בעל הכתובת מחזיר פקטת תשובה עם כתובת ה-MAC שלו. כך המחשב מקבל כתובות IP ו-MAC של כל ישויות הקיימות ברשת.

ארוע מעניין במהלך העבודה שהוסיף לאתגר היה ההצעה של גד, עוזר ההוראה, לפתח GUI בממשק web שיפתח בדפדפן. כך שמעתי על הספריה Flask ולמדתי להשתמש בה לצורך פיתוח ממשק משתמש. בנוסף גם למדתי מעט HTML ו-CSS לשם שיפור עיצוב הדף.

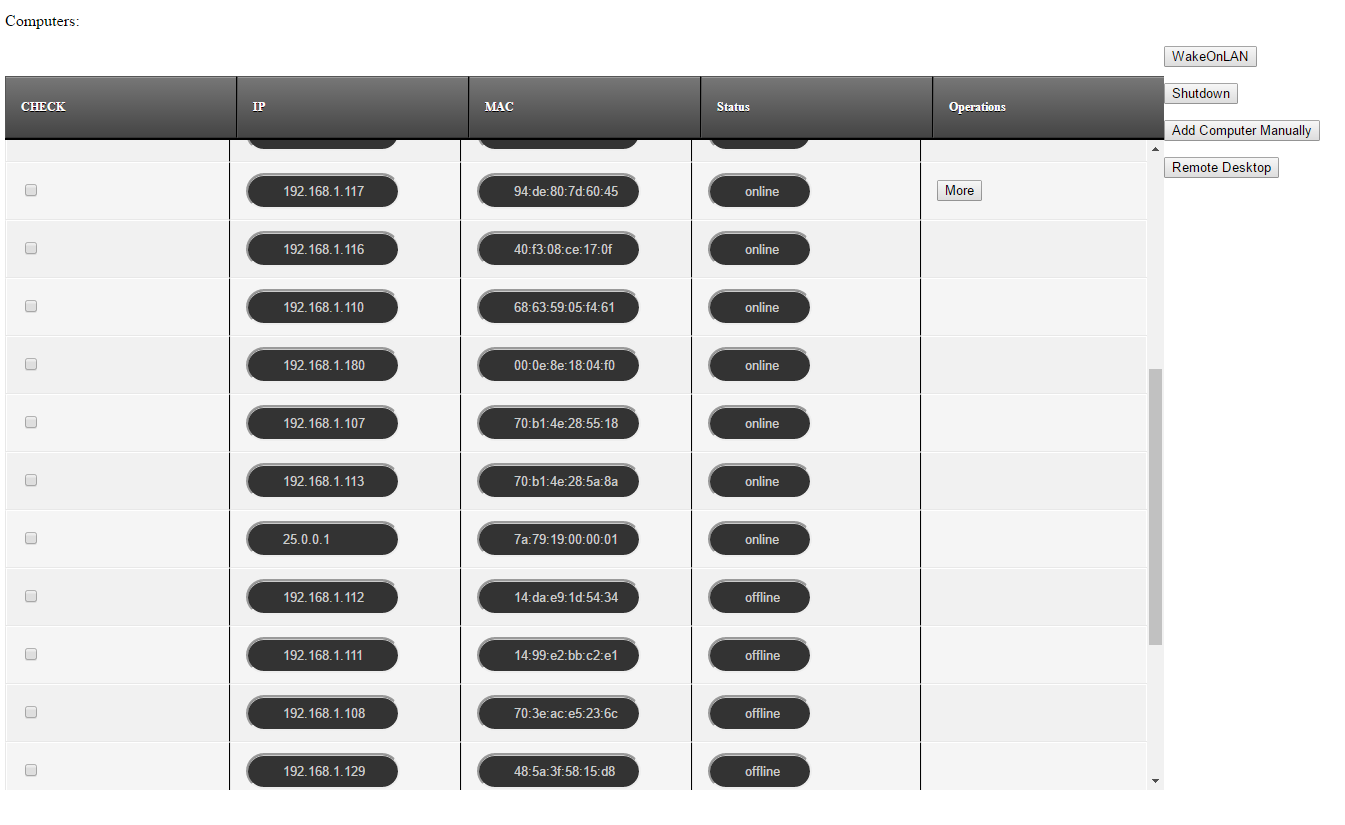
דבר החסר בפרוייקט והייתי רוצה להוסיף לו היה לי עוד זמן הוא התקנה יותר קלה של הפרויקט. התחלתי לחקור בנושא אך לא נותר לי די זמן. רציתי להקל לרמה שכל הצורך יהיה בהתקנת תוכנת השרת בלבד והוא ידאג לשאר – התקנת הלקוחות, הלקוחות יכניסו עצמם ל-Registry כדי שיופעלו עם הפעלת המחשב ואף בעצמם יטפלו ב-BIOS כדי לסדר את ההגדרות לתמיכה ב-Wake on LAN.

אני רוצה להודות למיכאל צ'רנובילסקי ולגד רוזנטל על העזרה במהלך הפרויקט, והזמן שהשיקעו בי ומתן עזרה.

# תיאור הממשק למשתמש

תחילה, יש להתקין את תוכנת השרת על מחשב אחד ברשת (לפחות) ואת תוכנת הלקוח על כל המחשבים.

כדי לאפשר הדלקת מחשבים מרחוק, בכל מחשב יש לאפשר ב-BIOS את האפשרות ל-Wake on LAN או Wake on magic packet תחת הקטגוריה Power management.

לאחר שכל אלו נעשו, יש להפעיל את השרת. מייד יפתח חלון חדש או לשונית חדשה בדפדפן שתציג את ההודעה: Server is starting. It might take a while…. יש לחקות עד לעליית השרת.

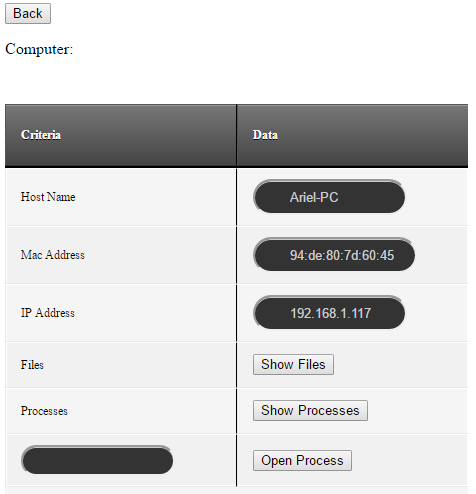
החלון הראשי:

מציג טבלה של כל המחשבים ברשת שהשרת יודע על קיומם. אפשר לבחור מהם מחשבים ולהפעיל אותם על ידי לחיצה על כפתוח Wake on LAN שיביא למסך הזה:



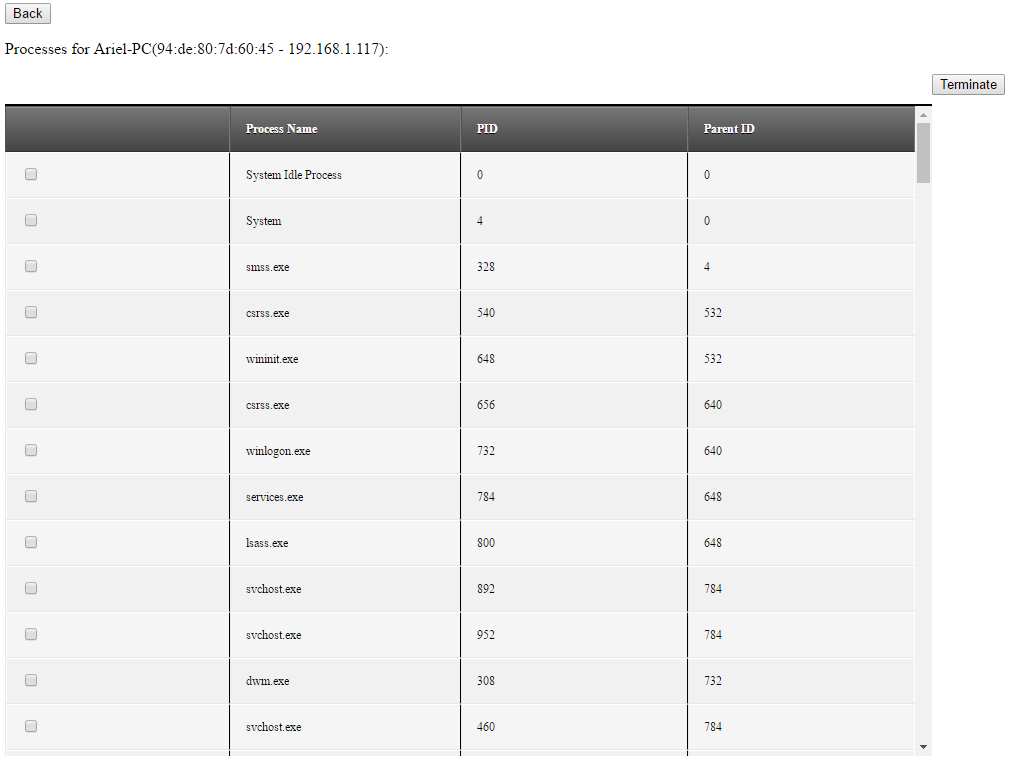
כאן אפשר לבחור אם להפעיל את המחשב בזמן ספציפי או מייד ולבחור את הזמן. אפשר גם לעשות שפעולה זו תחזור על עצמה על יום. לחיצה על Shutdown במסך הראשי תביא לחלון זהה.

ליד מחשבים שעליהם מופעלת תוכנת הלקוח יופיע כפתוח More, לחיצה עליו תביא למסך:



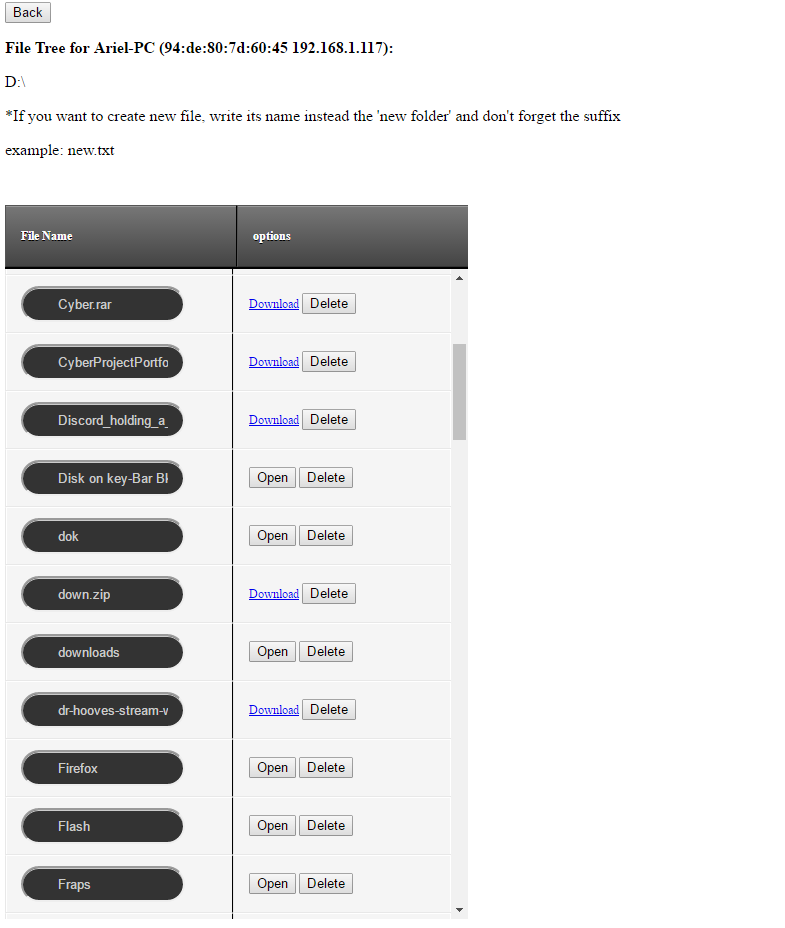
מסך זה מציג מידע על המחשב הספציפי הזה. כאן אפשר לכתוב פקודה שתרוץ בshell של המחשב ולשלוח אותה עם לחיצה על Open Process, אפשר לגשת לחלון התהליכים וחלון הקבצים על ידי לחיצה על Show Processes ו-Show Files בהתאם.

חלון תהליכים:



מציג את כל התהליכים הרצים על המחשב. אפשר לבחור מתוכם ואז ללחוץ על Terminate לסגירתם המיידית.

חלון הקבצים:

מציג את התוכלה של תיקיות. לחיצה על הכפתוח Open תציג את תכולת התיקייה. לחיצה על Delete תמחק את הקובץ או התיקייה לאלתר.

כדי לגשת לממשק המשתמש דרך הדפדפן יש לכתוב את כתובת ה-IP של המחשב עליו רץ השרת, נקודותיים ואז-5000. לדוגמה:



# סביבת העבודה

הפרויקט נכתב ב-Python, ב- HTML וב-CSS. ליבת הפרויקט, ועיקרו נכתבו בשפה Python בשל הנוחות של השפה. ה-GUI נכתב ב-Python, ב-HTML וב-CSS. HTML ו-CSS שימשו לעיצוב ה-GUI עצמו כדי שיהיה אפשר להציג אותו בקלות ונוחות בדפדפן. הקוד שמחבר בין ה-GUI לתוכנה נכתב ב-Python. כדי לחבר בין הקוד שנכתב ב-Python לדפדפן שמשתמש בפרוטוקול HTTP, השתמשתי בספריה שהוכנה עבור Python בשם Flask. זו יוצרת שרת HTTP, מכסה את התקשורת איתו ומעניקה למתכנת כלים כדי להציג בקלות דפי HTML שהוא עיצב.

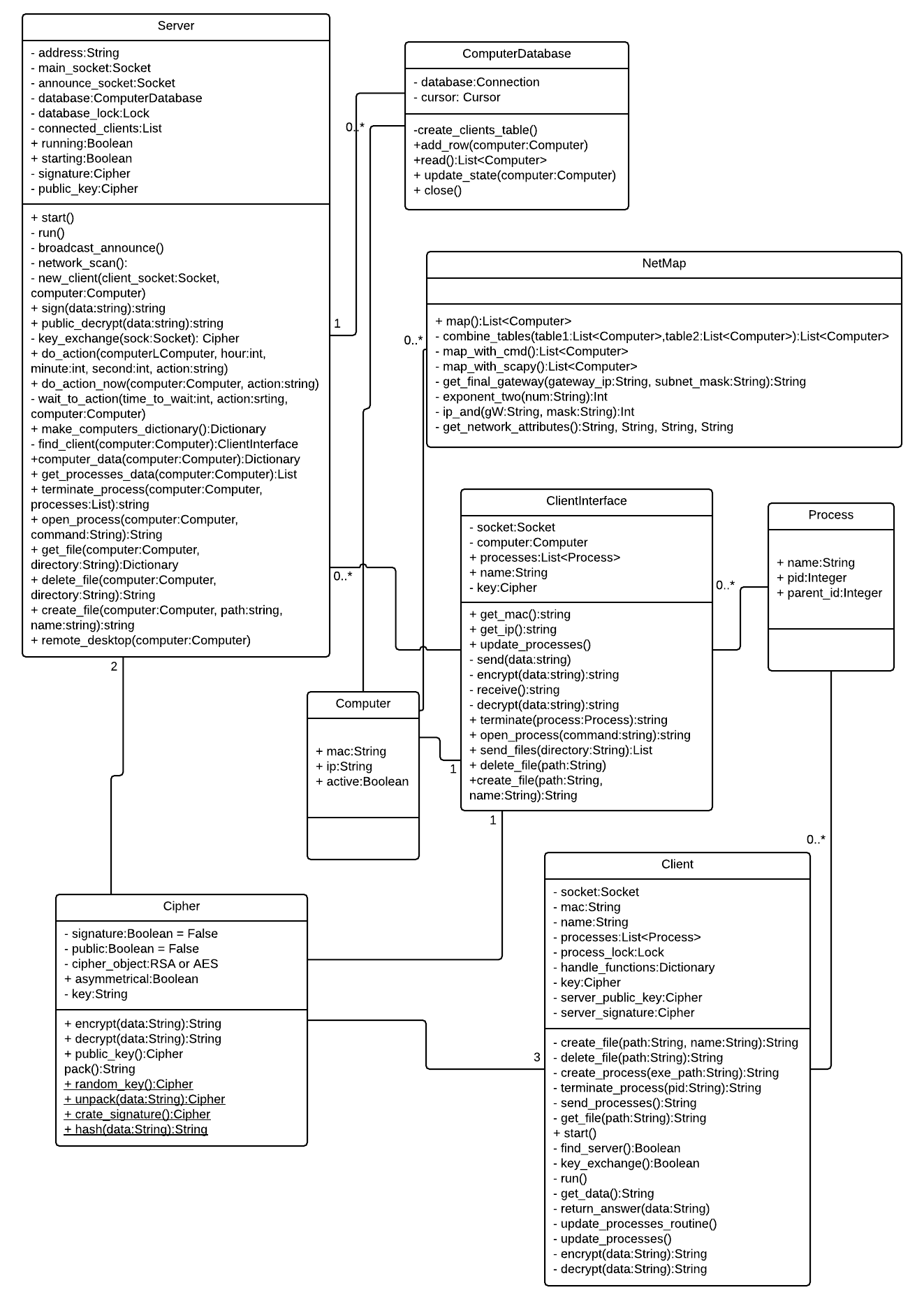
סביבת העבודה בה השתמשתי עבור שלוש השפות היא PyCharm. היא תוכנה מקצועית ונוחה לעבודה על פרויקטים מרובי קבצים ומאפשרת גם הרצה ו-debugging של הסקריפטים.



# תיאור המודולים

המודולים המרכיבים את הפרוייקט והקשרים ביניהם:

* מודול GuiEngine. מודול זה מפעיל את ממשק המשתמש ואת מנוע השרת ומהווה את החוליה המקשרת ביניהם.
* מודול Server מהווה את תוכנת השרת העיקרית. הוא מופעל על ידי מודול GuiEngine ומתופעל חלקית על ידיו. מודול זה משתמש במודולים הבאים:
  + מודול ComputerDatabase שמהווה את הקישור של השרת למאגר הנתונים שלו.
  + מודול NetMap שתפקידו מיפוי הרשת ומציאת כל היישויות המחוברות בה.
  + מודול ClientInterface שמכסה את הממשק של השרת לקשר עם הלקוחות.
  + מודל Cipher שאחראי על ההצפנה ואבטחת המידע.
* מודול ClientInterface משתמש במודולים: WakeOnLan שמכסה את הפעלת המחשבים וכיבויים מרחוק, ובמודול Process שמכיל אובייקט לייצוג תהליך.
* מודול ComputerDatabase משתמש באובייקט Computer לייצוג מחשב ממודול ClientInterface.
* מודול Client מהוות את תוכנת הלקוח. הוא משתמש במודולים:
  + Process שמכיל את האובייקט Process.
  + Cipher
* כל המודולים משתמשים במודול Constants שמכיל את הקבועים של התוכנה.



תרשים UML של המחלקות המרכיבות את הפרויקט

# האלגוריתמים המרכזיים בפרוייקט

בין הבעיות בהן התקלתי במהלך הפרויקט:

* מימוש שרת מולטי-קליינט:

הבעיה הראשון שעמדה לפניי בפיתוח המוצר היא יצירת שרת מולטי קליינט. כלומר, הייתי צריך לממש שרת שמתחברים אליו מספר לקוחות בו זמנית והוא מסוגל לדבר עם כולם. יש צורך ביצירת פרוטוקול תקשורת שיגדיר את אופי ההתנהלות של התקשורת. עליי גם לוודא שהמידע יהיה מאובטח ולהצפין אותו וכך לוודא שהמידע יעבור במלואו בבירור למרות ההצפנה.

פתרון: פיתחתי פרוטוקול פשוט משלי בו קיימות כמה הודעות אשר השרת והלקוח מכירים ואיתן הם מתקשרים ומעבירים ביניהם את המידע. כדי להצפין באופן יעיל את המידע, תחילה יש העברה של מפתחות אסימטריים של RSA ובעזרתם מועבר מפתח סימטרי של AES. שאר התקשורת מתבצעת בהצפנת AES כיוון שהצפנה סימטרית דורשת פחות משאבי מערכת מאשר הצפנה אסימטרית. כדי שלקוחות ימצאו את השרת, כל פרק זמן של 10 שניות, השרת מודיע ב-broadcast לכל הרשת על קיומו. כך לקוח שמופעל מאזין לרשת ויודע היכן נמצא השרת ומחבר אליו. דוגמת שלבי התקשורת בין השרת והלקוח:

I am Server

Connection Request

Public RSA Key

RSA( AES Key ) + Hash( AES Key )

Terminate Process

OK

שלב Broadcast

שלב Key Exchange

תקשורת בין שרת ולקוח



לקוח

שרת

* כיבוי והדלקה מרחוק של מחשבים

עליי לדעת כיצד להפעיל ולכבות מרחוק מחשבים ללא מגע. עליי גם לדעת כיצד ללמש זו ב-Python ללא בעיות.

* קבלת גישה לתהליכים ולקבצים של המחשב

האם התוכנה שלי, שנכתבה ב-Python ומופעלת על ידי מערכת ההפעלה יכולה לקחת תפקידים של מערכת ההפעלה? כלומר, על התוכנה לסייר בין הקבצים, ליצור חדשים ולמחוק קיימים. התוכנה צריכה גם להיות מסוגלת להפעיל ולסגור תהליכים הרצים על המחשב.

* שמירת מאגר מחשבים של הרשת

כיצד התוכנה תוכל לזכור את קיומם של מחשבים שלא מחוברים לרשת. אם לדוגמה, יפול החמשל והשרת יאלץ לרוץ מחדש, כיצד הוא יוכל לזכור את כל המחשבים שהכיר בריצה הקודמת ללא סריקה מחודשת? וכיצד ידע על קיומם של מחשבים שכבר לא מחוברים לרשת?

# תדפיס של הקוד