מטלת המוניטור – מעבדת סייבר הגנה – אוניברסיטת אריאל בשומרון תשפ"ב

המטרה

פיתוח תכנה המנטרת את השירותים הרצים על גבי המחשב המריץ אותה.

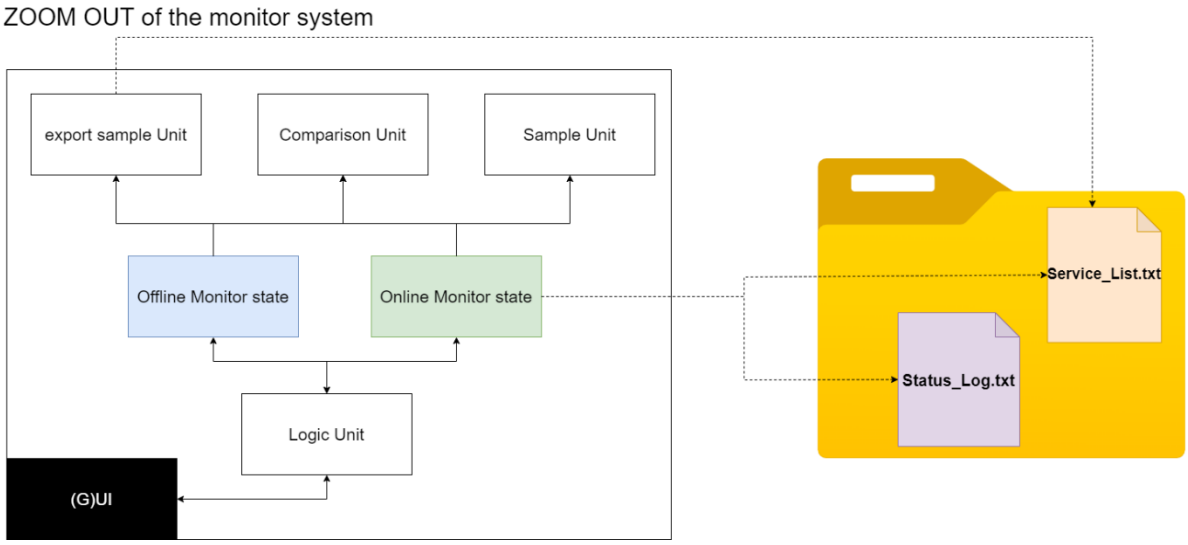
התכנה יכולה לעבוד באחד משני המצבים הבאים:

- **ONLINE**
  - מצב בו המשתמש מתבקש להזין מספר X של שניות.
  - כל X שניות התכנה תדגום את השירותים הרצים במערכת, ותכניס אותם לקובץ.
  - לאחר כל דגימה תתבצע השוואה בינה לבין הדגימה הקודמת לה.
  - התכנה תציג שינויים שהתרחשו בין שתי הדגימות ותכניס אותם לקובץ לוג.
- **OFFLINE**
  - מצב בו המשתמש מזין שני תאריכים בהם התרחשה דגימה.
  - התכנה שולפת את שתי הדגימות מקובץ הדגימות.
  - מתבצעת השוואה בין שתי הדגימות המוצגת למשתמש.

בנוסף המערכת היא מרובת פלטפורמות. כלומר ניתן להפעיל אותה גם על windows, וגם על linux.

תהליך הפיתוח

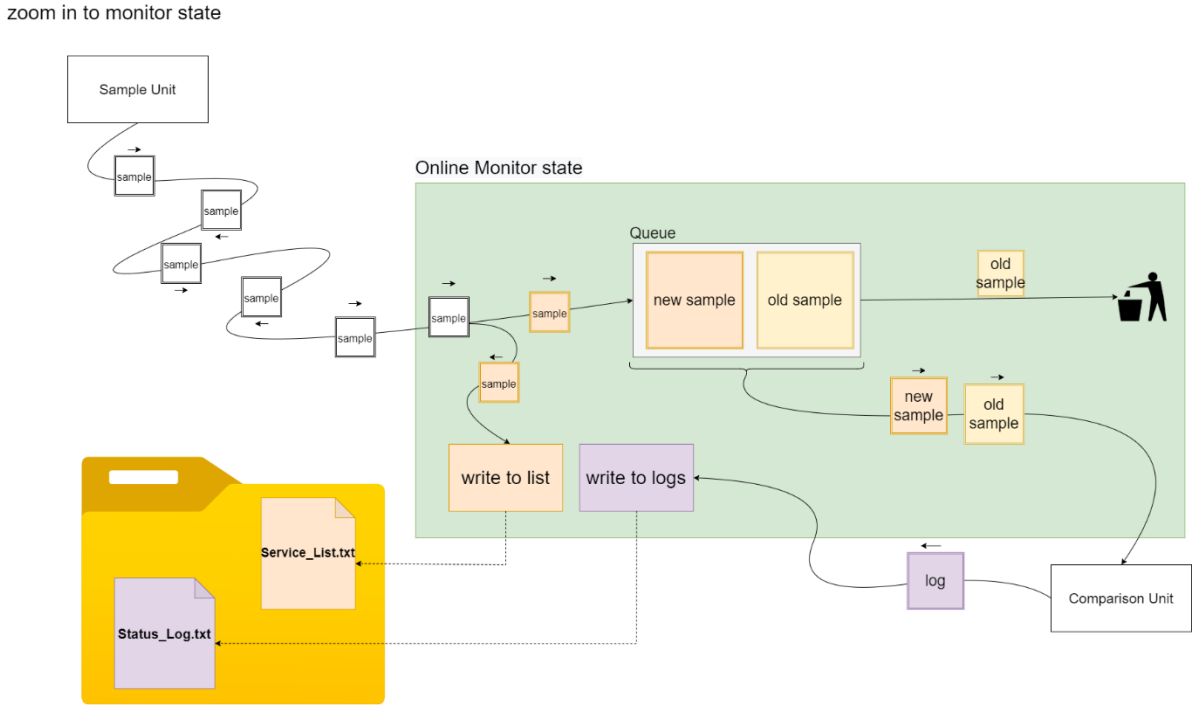
התמונה הבאה מראה את המערכת בצורה תיאורטית, במבט מלמעלה:



- **הסבר:**
  - המשתמש מתקשר עם התכנה דרך ה **UI**, ובוחר באיזה מצב לעבוד.
  - מצב אונליין פונה כל X שניות שהוגדר לו ליחידת הדגימה וההשוואה
  - מצב אופליין מחלץ עם יחידת החילוץ שני דגימות, ופונה איתם ליחידת ההשוואה.

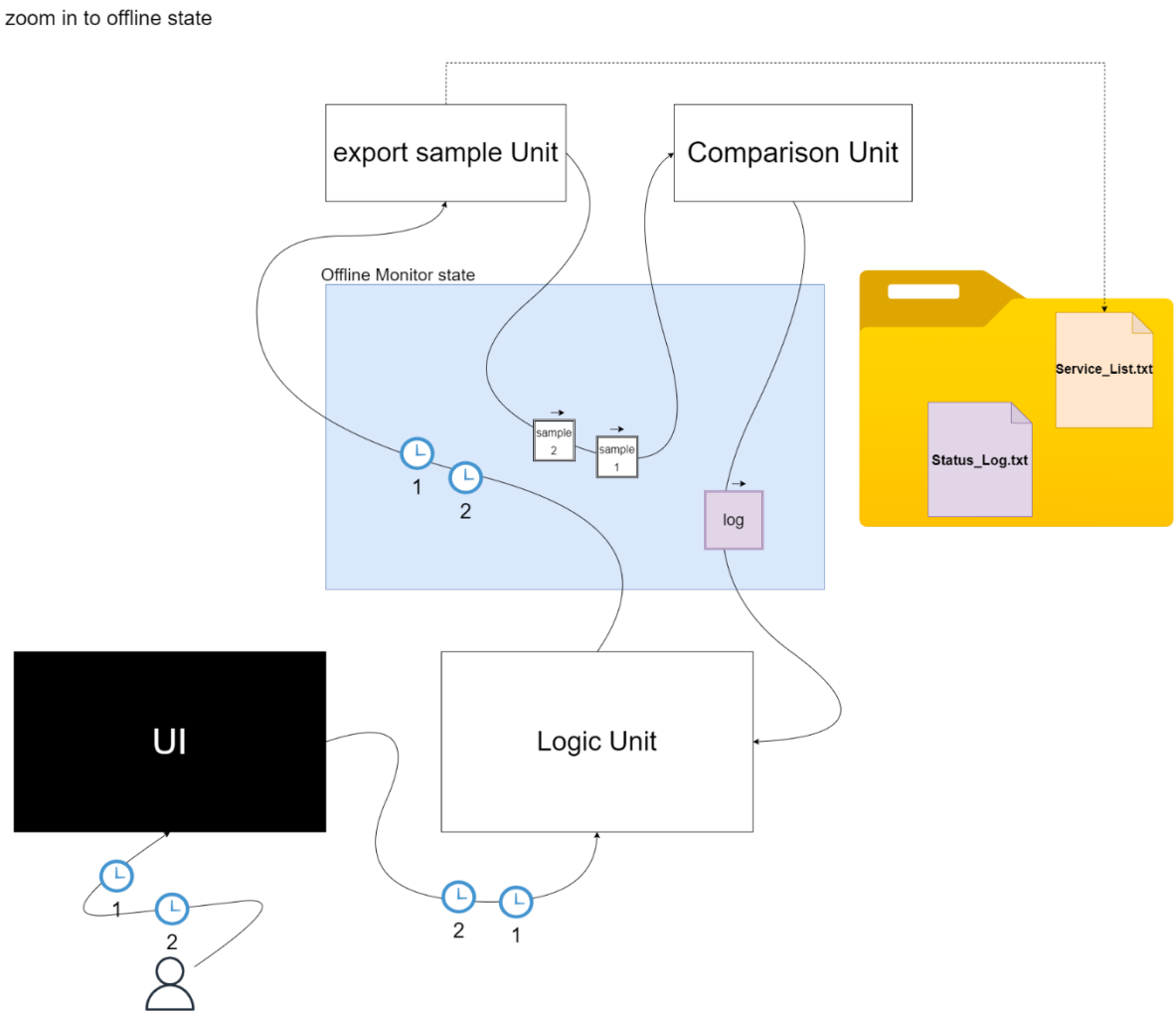
  - הסבר מפורט על רעיון הביצוע של כל אחד משני המצבים, בשני עמודים הבאים.

התמונה הבאה היא מבט רעיוני על אופן פעולת מצב האונליין:



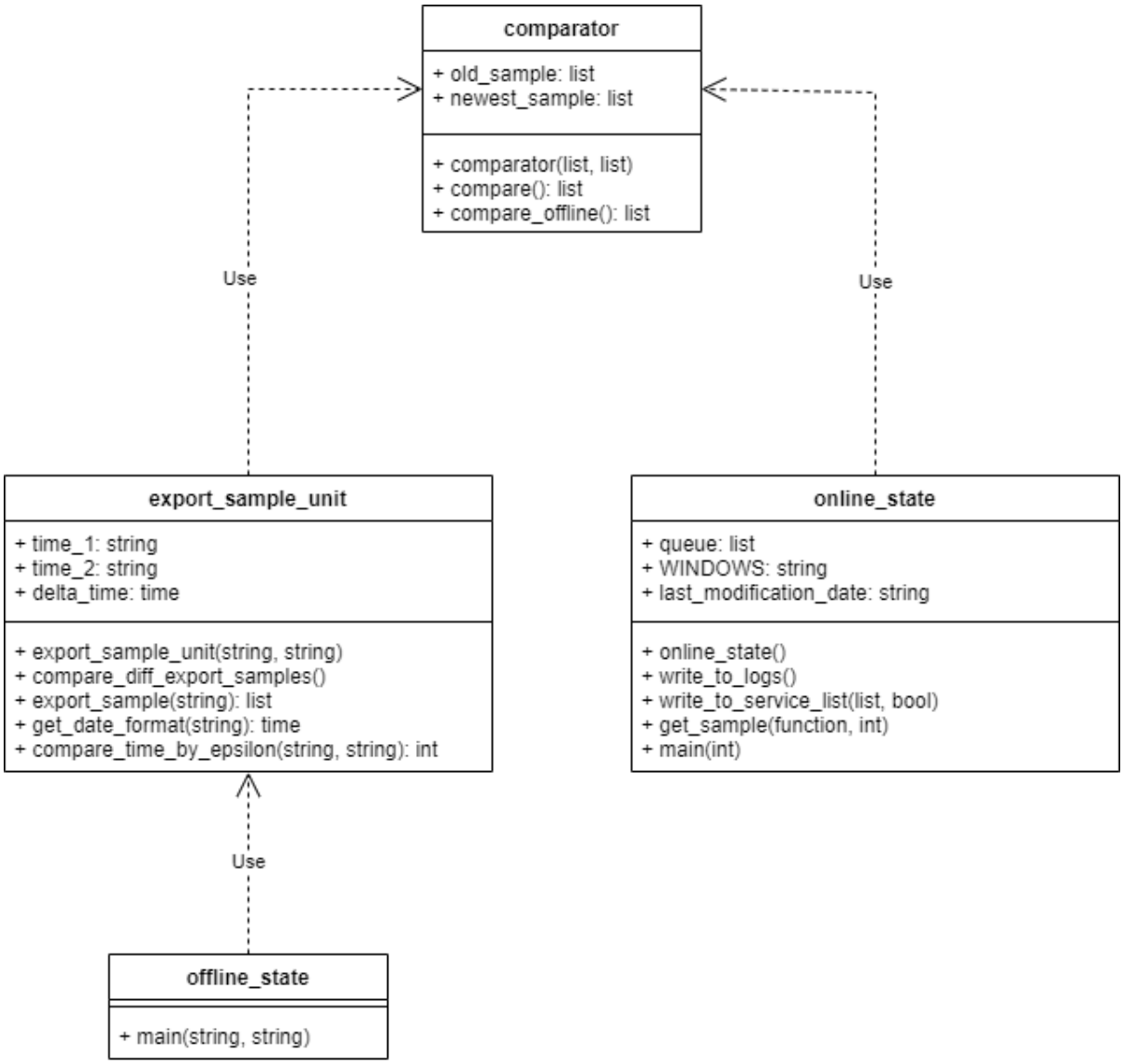
- **הסבר:**
  - כל X שניות מתקבלת דגימה חדשה
  - כל דגימה נכתבת בקובץ הדגימות
  - ולאחר מכן נכנסת לתור. גודלו המקסימלי של התור הוא 2.
  - כשהתור מגיע לגודל 2 אחרי שנכנסה דגימה חדשה, שתיהן נשלחות להשוואה.
  - הלוג שחוזר מההשוואה מוצג למשתמש (אם הלוג לא ריק, כלומר כשיש שינוי) ונכתב לקובץ לוג.
  - כשנכנסת דגימה חדשה לתור, הדגימה הראשונה שבו מושלכת, הקודמת הופכת לישנה, ואז נכנסת החדשה – וככה התהליך הזה חוזר על עצמו.

התמונה הבאה היא מבט רעיוני על אופן פעולת מצב האופליין:



- **הסבר (מעקב מהמשתמש בעקבות החיצים):**
  - המשתמש מזין דרך ה **UI** 2 זמנים בהם התרחשו שתי דגימות.
  - הזמנים מועברים לניהול של מצב האונליין
  - משם הזמנים עוברים ליחידת חילוץ הדגימות, שמחלצת את שתי הדגימות הקרובות ביותר לשעות שקיבלה, מהקובץ בו שמורות הדגימות.
  - מיחידת החילוץ חוזרות שתי דגימות.
  - שתי הדגימות מועברות ליחידת ההשוואה, שמוציאה לוג עליהם.
  - לוג זה מוצג למשתמש.

להלן UML שנוצר על פי התכנון הרעיוני שהוצג קודם:



הוראות התקנה והפעלה

- עשו clone לפרויקט בקישור הבא: https://github.com/amirg00/Service-Monitor.git
- בתוך תקית service-monitor הכנסו לתקית monitor
- הריצו את main.py
- גרסת הפייטון בפרויקט היא 3.9
- משם מלאו אחר ההוראות של התכנה.

אבטחה

- נקטנו כמה פעולות שמטרתם אבטוח הפרויקט מפני חבלות זדוניות.
  - במצב האונליין אנחנו רק כותבים לקובץ, ואת כל ההשוואות אנחנו עושים על ידי שמירה זמנית של כל דגימה, כפי שהוסבר למעלה.
  - במידה ולא התכנה היא שנגעה/מחקה את הקובץ, תופיע התראה על כך.

- חשבנו על כל מיני דרכים אותם לא הספקנו לבצע, וביניהם:
  - שמירת hash של הקבצים, כך שאם המשתמש ישנה משהו כשהתכנה לא פועלת, במידה ולא נמצא את ה hash או שנגעו בקבצים – נעלה התראה.
  - הפיכת קבצי הקוד לקובץ הרצה, ולא לתת את קוד המקור...