ROMÂNIA

MINISTERUL APĂRĂRII NAȚIONALE

ACADEMIA TEHNICĂ MILITARĂ "FERDINAND I"

FACULTATEA DE SISTEME INFORMATICE ŞI SECURITATE CIBERNETICĂ

Specializarea: Calculatoare și sisteme informatice pentru apărare și securitate națională

Aplicație digital forensics pentru sistemul de operare Microsoft Windows

CONDUCĂTOR ȘTIINȚIFIC

Lect. Dr. Ing. Alin Puncioiu

STUDENT:

Stud. Sg. Maj. Cristian Băluți

BUCUREȘTI

2024

Cuprins

1. Introducere

Într-o eră digitală unde volumele de date cresc exponențial și amenințările cibernetice devin din ce în ce mai sofisticate, nevoia de instrumente avansate de digital forensics este mai mare ca niciodată.

Lucrarea de diplomă intitulată "Aplicație digital forensics pentru sistemul de operare Microsoft Windows" are ca obiectiv dezvoltarea unei soluții software care să răspundă acestei cerințe esențiale.

Proiectul se concentrează pe crearea unei aplicații server-client care permite colectarea, analiza și raportarea datelor digitale într-un mod eficient și sistematic, oferind astfel o resursă valoroasă pentru investigații în domeniul IT.

1.1. Descrierea sumară a proiectului

Această aplicație este proiectată să execute o serie de pași critici în domeniul digital forensics.

În primul pas, se va implementa un sistem de monitorizare EDR (Endpoint Detection and Response), pentru a detecta activitățile suspecte pe un dispozitiv Windows.

Ulterior, un script personalizat va fi folosit pentru a colecta artefacte digitale relevante, care vor fi esențiale în construirea unei imagini comprehensive a activității sistemului.

Pasul trei implică utilizarea unui instrument precum Autopsy pentru achiziția și analiza memoriei RAM și a discului sistemului, esențiale pentru identificarea posibilelor metode de persistență și alte dovezi digitale, precum fișierele Prefetch și User Assist.

Finalizarea acestui proces va consta în generarea unui raport detaliat care va fi transmis înapoi clientului, oferind o imagine clară a situației de securitate și a oricăror compromiteri ale sistemului.

2. Cerințe Software

2.1. Cerințe funcționale

- **Monitorizarea EDR:** Aplicația trebuie să poată monitoriza activitatea sistemului în timp real pentru a detecta și a înregistra comportamente suspecte sau anomalii.
- **Colectarea Artefactelor:** Trebuie să existe un mecanism prin care aplicația să colecteze artefacte digitale din diverse locații ale sistemului de operare, cum ar fi fișiere de sistem, registri de Windows, fișiere temporare, și jurnale de evenimente.
- **Achiziția de Date:** Aplicația va avea capacitatea de a efectua achiziții de date volatile, cum ar fi conținutul memoriei RAM, și non-volatile, cum ar fi date de pe disc, într-un mod care nu alterează sau compromite integritatea datelor.
- **Analiza Datelor:** După colectarea datelor, aplicația trebuie să le analizeze pentru a identifica modele, și a descoperi dovezi de utilizare a sistemului sau de compromitere.
- **Generarea de Rapoarte:** Aplicația trebuie să genereze rapoarte detaliate, ușor de înțeles, care să includă toate descoperirile relevante ale analizei, împreună cu orice recomandări pentru acțiuni ulterioare.
- **Interfața Utilizator:** Trebuie să fie disponibilă o interfață grafică pentru utilizatori, care să permită accesul ușor la toate funcționalitățile aplicației, inclusiv configurarea, monitorizarea și revizuirea rapoartelor.
- **Securitatea Datelor:** Aplicația trebuie să asigure securitatea datelor pe întreg parcursul procesului de forensics, de la colectare la raportare, utilizând protocoale de criptare și autentificare.

2.2. Cerințe nefuncționale

- **Performanță**: Aplicația trebuie să fie capabilă să proceseze și să analizeze date într-un mod eficient, cu timp minim de așteptare.
- **Fiabilitate**: Trebuie să fie extrem de fiabilă, cu o rată minimă de eroare, pentru a asigura acuratețea și integritatea analizei forensice.
- **Usabilitate**: Interfața cu utilizatorul trebuie să fie intuitivă și ușor de navigat, chiar și pentru utilizatorii care nu sunt experți în forensics.
- **Scalabilitate**: Arhitectura software-ului trebuie să fie scalabilă, permițând adăugarea de noi funcționalități sau module fără a afecta performanța sistemului existent.
- **Securitate**: Aplicația trebuie să implementeze măsuri de securitate puternice pentru a preveni accesul neautorizat la date și pentru a proteja împotriva atacurilor cibernetice.
- **Compatibilitate**: Trebuie să fie compatibilă cu diferite versiuni ale sistemului de operare Windows, fără a necesita modificări majore.
- **Documentația**: Documentația trebuie să fie completă, clară și actualizată, pentru a ajuta la implementarea, utilizarea și întreținerea aplicației.

3. Arhitectura sistemului

3.1. Client

- Interfața Utilizatorului
    - **Design UI/UX:** Designul interfeței cu utilizatorul trebuie să fie clar, intuitiv și ușor de utilizat pentru a simplifica procesul de digital forensics, chiar și pentru utilizatori care nu sunt experți tehnici.
    - **Dashboard**: Un panou de control centralizat care afișează starea curentă a procesului de analiza și acces rapid la activare/dezactivare de funcții.

- Funcționalități de Colectare a Datelor
    - **Instrumente de Colectare**: Capabilitatea de a rula scripturi și instrumente automate pentru extragerea datelor de pe sistemul clientului, inclusiv memorie, fișiere și setări de sistem.
    - **Planificator de sarcini**: Posibilitatea de a programa colectări de date la intervale regulate sau la declanșarea anumitor evenimente.
- Comunicarea cu Serverul
    - **Protocol de Comunicare**: Implementarea unui protocol de comunicare sigur, cum ar fi TLS/SSL, pentru transferul datelor între client și server.
    - **Autentificare și Autorizare**: Mecanisme de securitate pentru a verifica identitatea clientului și a asigura că numai clienții autorizați pot iniția colectarea și transmisia datelor.

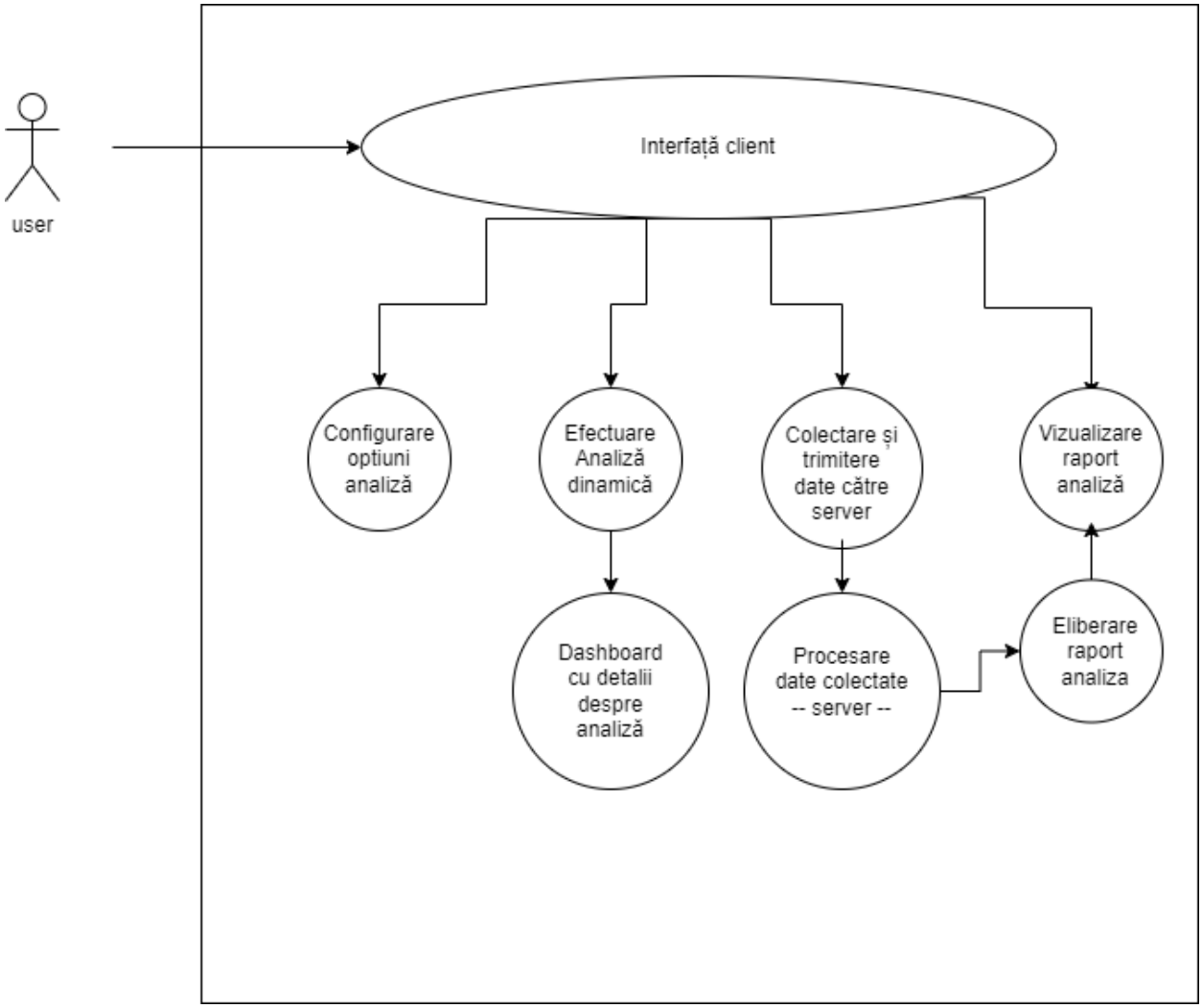
- Procesare și Prelucrare Locală
    - **Analiză Preliminară**: Capacitatea de a efectua analize preliminare ale datelor înainte de a le trimite serverului pentru a reduce volumul de date transmise și a oferi rezultate rapide atunci când este necesar.
    - **Caching Local**: Stocarea temporară a datelor pentru a optimiza performanța și pentru a asigura că datele nu sunt pierdute în cazul unei întreruperi a conexiunii cu serverul.
- Securitate
    - **Criptarea Datelor**: Toate datele sensibile stocate local sau transmise trebuie să fie criptate pentru a proteja integritatea și confidențialitatea informațiilor.
    - **Prevenirea Manipulării**: Măsuri de protecție împotriva alterării datelor și a artefactelor colectate, inclusiv utilizarea hash-urilor criptografice pentru a verifica integritatea datelor.

3.2. Server

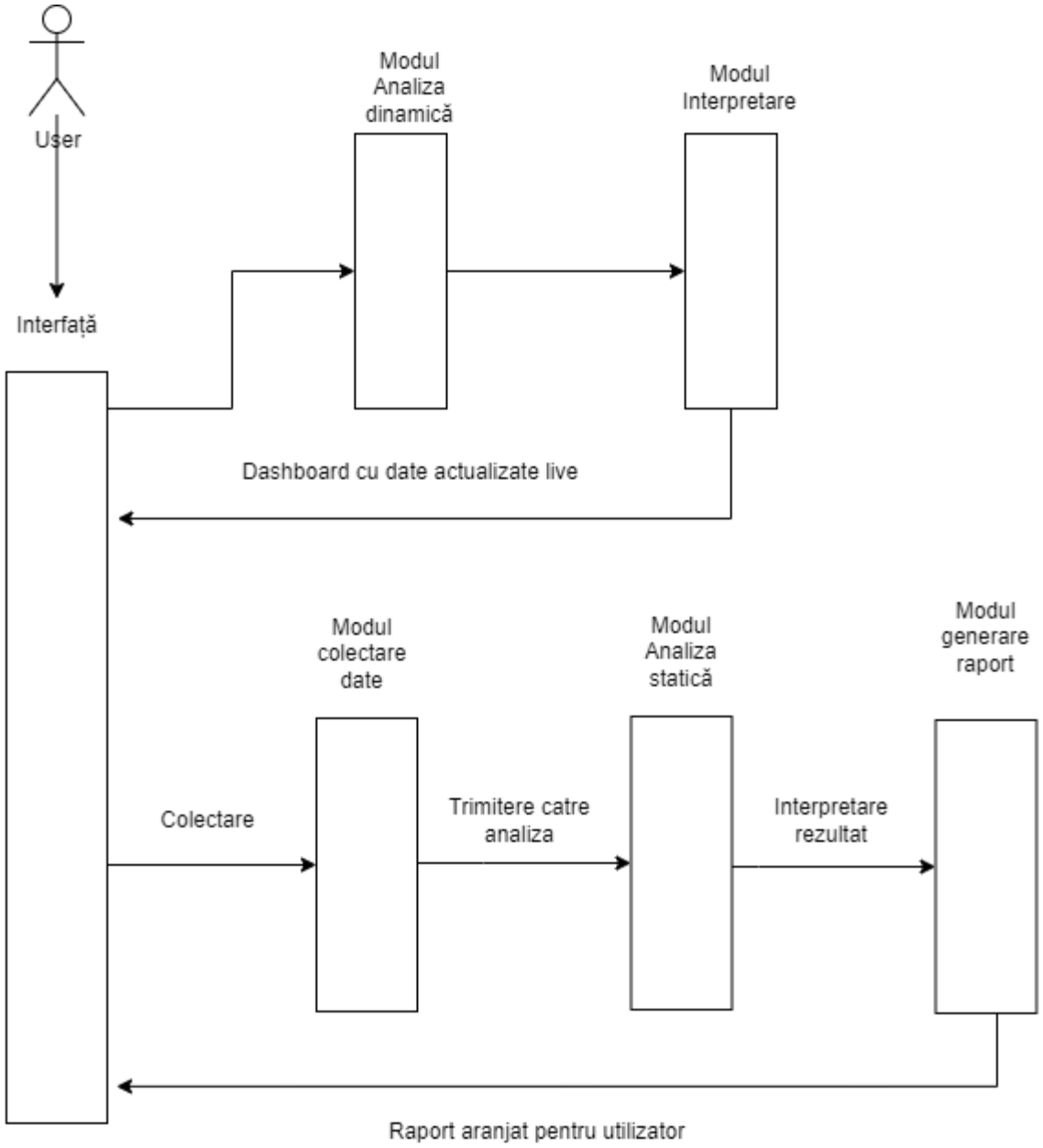
- Managementul Datelor
    - **Baza de Date**: Utilizarea unei baze de date robuste pentru stocarea eficientă și organizarea datelor colectate de la clienți.
    - **Securitatea Datelor**: Implementarea protocoalelor de securitate pentru a proteja baza de date împotriva accesului neautorizat și a vulnerabilităților.
- Procesarea și Analiza Datelor
    - **Motor de Procesare**: Un sistem puternic de procesare a datelor care poate rula algoritmi complexi și poate efectua operațiuni de analiză de tip forensics pe volume mari de date.
    - **Instrumente de Analiză**: Integrarea cu instrumente avansate de digital forensics pentru a efectua analize automatizate și manuale.
- Comunicarea cu Clientul
    - **API-uri și Servicii Web**: Implementarea API-urilor sau a serviciilor web pentru a facilita schimbul de date între client și server și pentru a permite integrarea cu alte sisteme.
    - **Gestionarea Conexiunilor**: Menținerea și gestionarea conexiunilor securizate cu multiple instanțe de client.
- Scalabilitate și Performanță
    - **Scalabilitate Orizontală și Verticală**: Capacitatea de a adăuga mai mult hardware sau de a aloca mai multe resurse pentru a gestiona creșterea volumului de date și a solicitărilor de procesare.
    - **Load Balancing**: Distribuirea încărcăturii pe mai multe servere sau nuclee de procesare pentru a asigura performanță și disponibilitate.

4. Diagrame UML

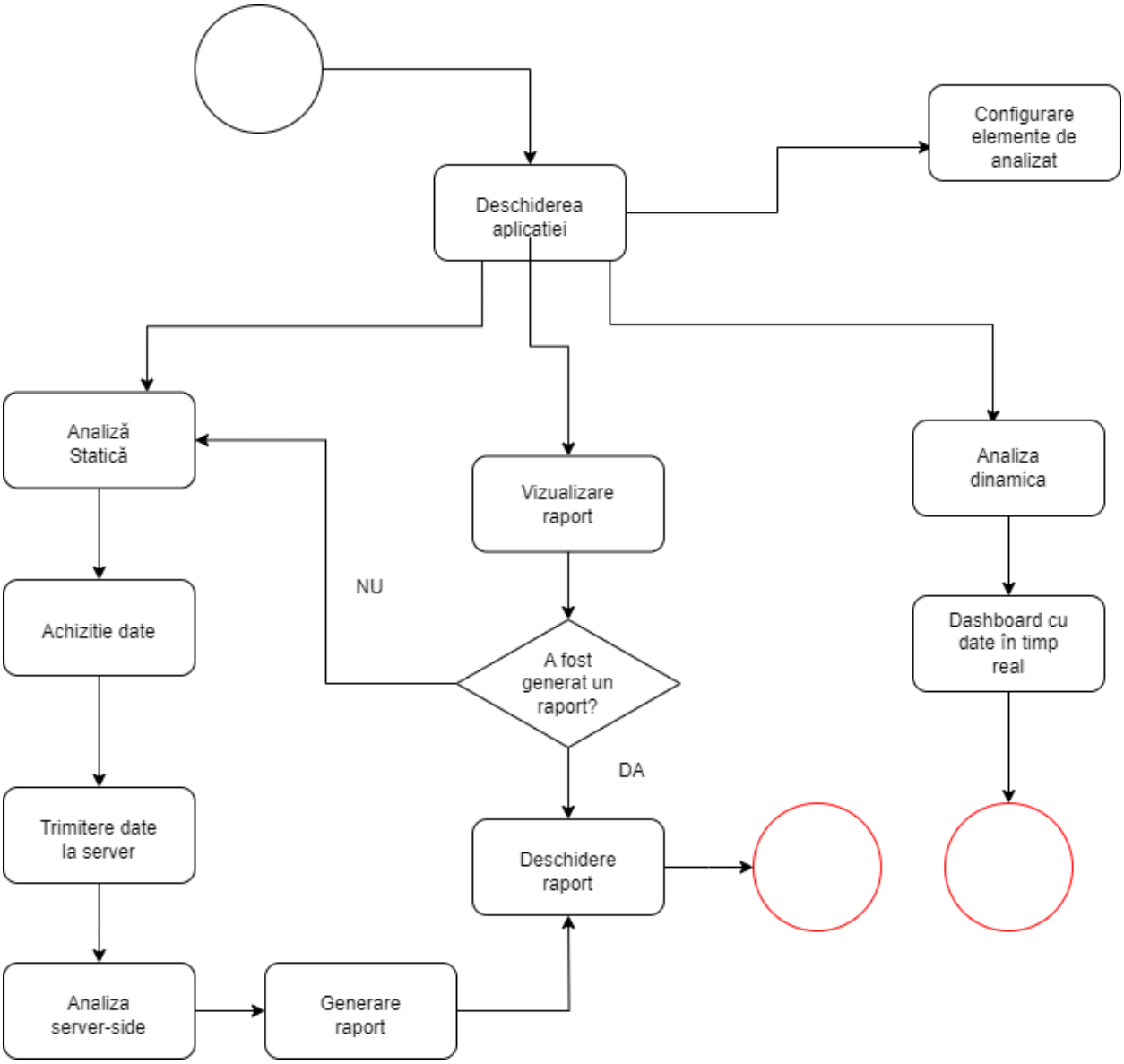
4.1. Diagrama cazurilor de utilizare



4.2. Diagrama de secvență



4.3. Diagrama de activități



5. Testare

5.1. Strategia de testare

Strategia de testare constă în următoarele etape:

- Planificarea Testelor
  - **Definirea Obiectivelor de Testare**: Stabilirea a ceea ce trebuie să fie testat, inclusiv funcționalități, performanță, securitate, și compatibilitate.
- Scrierea Cazurilor de Test
  - **Cazuri de Test Funcționale**: Verificarea funcționalităților sistemului în diferite scenarii, inclusiv condiții de margine și cazuri neobișnuite.
  - **Cazuri de Test de Performanță**: Testarea timpului de răspuns al sistemului, a utilizării resurselor și a comportamentului sub încărcătură.
  - **Cazuri de Test de Securitate**: Identificarea vulnerabilităților de securitate, inclusiv testele de penetrare și cele pentru prevenirea atacurilor cibernetice.
  - **Cazuri de Test de Compatibilitate**: Asigurarea că sistemul funcționează pe diferite platforme și în diverse medii de rețea.
- Execuția Testelor
  - **Testare Manuală**: Realizarea testării manuale pentru a verifica aspectele UI/UX și pentru a efectua teste exploratorii.
  - **Testare Automată**: Implementarea scripturilor de testare automată pentru a eficientiza procesul de testare și a asigura consistența.
  - **Testare Regresie**: Verificarea că modificările recente nu au afectat funcționalități existente.

5.2. Plan de testare

- Verificare mediu de testare. Un sanbox de windows.
- Deployerea unor amenințări în mediul de testare.
- Deschiderea aplicației.
- Rularea analizei statice, cât și cea dinamică.â

Testare manuală

- Verificarea rezultatelor analizei dinamice cu cele așteptate conform malware-ului.
- Verificarea rezultatelor din raport conform malware-ului.

Testare automată

- Executarea testelor ce verifică rezultatele raportului.
- Rularea testelor unitare pentru verificarea algoritmică

6. Bibliografie

- Digital forensics - André Årnes
- Handbook of Digital Forensics and Investigation - Eoghan Casey
- https://resources.infosecinstitute.com/topics/digital-forensics/free-open-source-computer-forensics-tools/
- https://recfaces.com/articles/digital-forensics