# ROMÂNIA NECLASIFICAT

# MINISTERUL APĂRĂRII NAŢIONALE Exemplar nr.

ACADEMIA TEHNICĂ MILITARĂ „FERDINAND I”

##### APROB

DECANUL FACULTĂŢII DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ

**Col. prof. univ. dr. ing.**

**Ion BICA**

## TEMA Nr. \_\_

a proiectului de licenţă aparţinândstudentului ***BĂLUȚI Cristian***

din facultatea SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ,

specializareaCALCULATOARE ŞI SISTEME INFORMATICE PENTRU APĂRARE ŞI SECURITATE NAŢIONALĂ

cu tema:

***„Aplicații de tip digital forensics pentru Microsoft Windows”***

## DETALII

1. PRECIZĂRI ŞI DATE INIŢIALE:

Tendința de creștere a amenințărilor cibernetice din mediul online este direct proporțională cu avansul tehnologic în ceea ce privește mecanismele de asigurare a unui minim de protecție a cetățenilor, spațiul cibernetic fiind mereu animat de cursa continuă dintre atacatori și cei care sunt afectați de aceste atacuri. Datorită gradului mare de accesibilitate la tehnologii moderne, precum și evoluției ascendentă în ceea ce privește nivelul de sofisticare al atacurilor, criminalitatea cibernetică a ajuns la un nivel foarte ridicat, acest lucru având ca punct de plecare utilizatori (grupuri de utilizatori) rău intenționați care încearcă să obțină acces la informații confidențiale/ clasificate, atât ale unor persoane fizice cât și juridice, dar și ale unor entități publice civile sau militare, prin intermediul aplicațiilor de tip malware.

Pentru a investiga în mod eficient activitatea efectuată pe un sistem informatic și existența de fișiere malițioase, soluțiile actuale pot utiliza combinații de tehnici avansate de evaluare a amenințărilor, care includ verificarea în timp real a indicatorilor de compromitere, analiza forensics sumară la apariția anomaliilor de sistem, analiza artefactelor specifice sistemului de operare, analiza activității utilizatorului conectat la sistemul investigat, extragerea și identificarea de fișiere posibil malițioase.

Proiectul își propune să studieze stadiul actual al realizărilor din domeniul analizei de tip digital forensics pentru sisteme Windows, prin documentarea modalităților de efectuare de astfel de analize în vederea identificării instrumentelor tehnice adecvate pentru desfășurarea investigației și automatizării execuției acestora pentru simplificarea proceselor de analiză avansată și creșterea timpului de răspuns la identificarea unor anomalii ca urmare a analizei forensics a sistemului țintă. Proiectul va avea două componente, o componentă automatizată care va permite execuția de programe scripturi pentru analiza superficială a probei digitale țintă și o componentă de analiză statică ce va detalia modalitatea de efectuare a unei investigații forensics pe un sistem de operare Windows, pe baza unei metodologii avansată descrisă în lucrare.

2. MEMORIUL TEHNIC VA CONŢINE:

**A) Introducere**

- motivația lucrării;

- obiectivele lucrării;

- structura pe capitole, etc.

**B) Tehnici și tehnologii de analiză**

- documentarea amenințărilor cibernetice actuale, a vulnerabilităților sistemelor și serviciilor informatice și a riscurilor asociate potențialei exploatări a acestora;

- documentarea instrumentelor de analiză compatibile cu sistemele de operare Windows ce ar putea fi utilizate pentru efectuarea unor analize forensics;

- prezentarea conceptelor de analiză forensics specifice sistemelor de operare Windows:

* descrierea tipurilor de sisteme de fișiere;
* detalierea artefactelor generate de sistemul de operare;
* detalierea artefactelor generate de acțiunile utilizatorilor și ale aplicațiilor.
* detalierea metodelor si tehnologiilor necesare pentru efectuarea de analize de disc și/ sau de RAM.

**C) Crearea soluției tehnice**

- descrierea proceselor și procedurilor de analiză selectate;

**-** prezentareacerințelor funcționale și specificații de proiectare;

**-** descrierea arhitecturii soluției și module componente;

- detalierea modurilor de funcționare și a elementelor de automatizare incluse în cadrul procedeului de analiză;

- detalierea tehnologiilor utilizate;

- testarea ansamblului și prezentarea rezultatelor experimentale.

- detalierea metodelor de analiză forensics manuală pentru efectuarea de analize avansate amănunțite.

**D) Concluzii şi perspective**

- prezentarea concluziilor și sinteza ideilor principale;

- evidențierea contribuțiilor aduse de lucrare;

- descrierea unor direcții viitoare de cercetare/

**E) Bibliografie**

**F) Anexe (dacă e cazul)**

1. LUCRĂRI GRAFICE DE ÎNTOCMIT:

- Scheme bloc şi diagrame;

- Codul sursă al modulelor dezvoltate.

4. BIBLIOGRAFIE:

- Resurse disponibile pe Internet.

5. PRACTICA DE DOCUMENTARE:

- Academia Tehnică Militară „Ferdinand I”, Bucureşti

6. CONDUCĂTOR ŞTIINTIFIC:

**alin puncioiu**

7. DATA PRIMIRII PROIECTULUI:

8. DATA PREDĂRII PROIECTULUI:

## DIRECTORUL DEPARTAMENTULUI DE

## CALCULATOARE ȘI SECURITATE CIBERNETICĂ

**Col. prof. univ. dr. ing.**

**Mihai TOGAN**