MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere

Șef departament: conf. univ., dr. Ion FIODOROV

_____

"___" _____ 2022

METODE ȘI TEHNICI DE EXTRAGERE A DATELOR DE PE SUPORTURILE DIGITALE ÎN CADRUL INVESTIGĂRII INFRACȚIUNILOR INFORMATICE

Teză de master

Student: **Zmeu Cristin, SI-211M**

Coordonator: **Zgureanu Aureliu, conf. univ., dr.**

Chișinău, 2023

ADNOTARE

La proiectul de master: „METODE ȘI TEHNICI DE EXTRAGERE A DATELOR DE PE SUPORTURILE DIGITALE ÎN CADRUL INVESTIGĂRII INFRACȚIUNILOR INFORMATICE”, elaborat de Zmeu Cristin, Chișinău, 2023.

Cuvinte cheie: forensics, software, hardware, OS, copia digitală, căutarea informațiilor textuale, căutarea informațiilor grafice.

Structura tezei: Teza de master este constituită din introducere, trei capitole și concluzii, 60 pagini de text de bază, inclusiv 26 de figuri.

În teza de master s-a efectuat analiza situației în domeniul criminalisticii dispozitivelor mobile, precum și a dispozitivelor de stocare a informației, analiza posibilităților programelor criminalistice, s-a descris procesul de ridicare, extragere, examinare și analiză a datelor informatice. Au fost descrise regulile de elaborare a planșei fotografice, a unui raport de expertiză, iar în final au fost descrise recomandări pentru situațiile tipice întâlnite în cadrul analizei.

Semnificația și valoarea aplicativă, modalitățile de examinare și analiză a datelor extrase, vor permite ridicarea calității expertizei judiciare a sistemelor informatice dar și va contribui la procesul de instruire a organelor de drept.

Criminalistica dispozitivelor de stocare a informației și a dispozitivelor mobile, ca ramură a criminalisticii digitale, reprezintă entitatea ce vizează extragerea, recuperarea și analiza datelor conținute în memoria digitală, utilizând echipamente și metode prin care se respectă cadrul legal.

În conținut sunt: Introducere, 4 capitole, concluzii și bibliografie (17 titluri). Conținutul este expus pe 60 de pagini și conține 26 de figuri.

În capitolul 1 al tezei de master a fost descris conceptul de infracțiune informatică și înțelesul acestei noțiuni.

În capitolul 2 sunt descrise tacticile efectuării acțiunilor de urmărire penală în cadrul cercetării infracțiunilor informatice.

În capitolul 3 au fost analizate metodele de examinare, de fixare a stării dispozitivelor, dispozitivele de extragere a informației digitale, achiziția informației prin intermediul copiei live, precum și procesarea acestora prin intermediul produselor soft-ware disponibile.

În capitolul 4 au fost analizate modalitățile și tipurile de date informatice posibile de extras din memoria internă a dispozitivului mobil, produsele soft-ware predestinate extragerii datelor din dispozitivele mobile, procesarea și examinarea datelor extrase, cu ulterioara întocmire a raportului de expertiză sau de constatare tehnico-științifică.

Lista de bibliografie include principalele surse de informare utilizate în procesul de proiectare.

ANNOTATION

At the master project: „Methods and techniques of data extraction from digital media in the framework of the investigation digital crimes", developed by Zmeu Cristin, Chișinău 2023.

Keywords: forensics, software, hardware, OS, digital copy, textual information search, graphical information search.

Thesis structure: The master's thesis consists of an introduction, three chapters and conclusions, 60 pages of basic text, including 26 figures.

The master's thesis analyzed the situation in the field of mobile device forensics, as well as information storage devices, analyzed the possibilities of forensic programs, described the process of collecting, extracting, examining and analyzing computer data. The rules for drawing up the photographic plate, an expert report were described, and finally, recommendations were described for the typical situations encountered during the analysis.

The meaning and applicative value, the methods of examination and analysis of the extracted data, will allow raising the quality of the judicial expertise of the computer systems, but will also contribute to the training process of the legal bodies.

The forensics of information storage devices and mobile devices, as a branch of digital forensics, represents the entity that aims to extract, recover and analyze data contained in digital memory, using equipment and methods that comply with the legal framework.

In the content are: Introduction, 4 chapters conclusions, and bibliography (17 titles).The content is laid out on 60 pages and contains 26 figures.

In chapter 1 of the master's thesis, the concept of computer crime and the meaning of these notions were described.

In chapter 2, the tactics of carrying out criminal prosecution actions in the framework of computer crime investigations are described.

In chapter 3, the methods of examination, fixing the status of devices, devices for extracting digital information, searching for information through live copy, as well as their processing through available software products were analyzed.

In chapter 4, the methods and types of computer data that can be extracted from the internal memory of the mobile device, the software products predestined for the extraction of data from mobile devices, the processing and examination of the extracted data, with the subsequent drawing up of the expert or technical assessment report were analyzed.

The bibliography list includes the main sources of information used in the design process.

CUPRINS

INTRODUCERE

Actualitatea și importanța temei. Dezvoltarea sistemelor informatice, globalizarea rețelelor informatice și apariția unor mijloace noi de legătură și comunicarea între persoane au avut o influență benefică pentru viața economică, socială şi politică a lumii, însă totodată au dus și la dezvoltarea fenomenului infracțional, care a înregistrat noi forme de manifestare a criminalității. Este vorba de criminalitatea informatică ce reprezintă o amenințare gravă, în condițiile în care aproape toate domeniile vieții sociale se bazează pe sisteme informatice.

Treptat, lumea virtuală a evoluat și din perspectiva oportunităților pe care le oferă oamenilor, fiind, fără îndoială, o sursă de resurse informaționale valoroase, dar și un spațiu imens pentru victime și infractori. Astfel, răspândirea sistemelor informatice și a internetului a facilitat migrarea infracțiunilor tradiționale în spațiul virtual, ceea ce a condus la apariția infracțiunilor informatice. Criminalitatea informatică constituie un pericol sporit atât pentru fiecare subiect în parte, cât și pentru statele lumii, precum și pentru comunitatea internațională, având un caracter transfrontalier. Lupta cu aceste infracțiuni trebuie să devină una dintre prioritățile comunității internaționale, impunându-se elaborarea reglementărilor pentru combaterea acestor tipuri de infracțiuni.

Actualmente, organele de urmărire penală se confruntă cu o adevărată provocare în asigurarea unui spațiu sigur într-o eră digitală, pentru că de cele mai dese ori, metodele și tehnicile de operare, sunt descoperite de infractori înainte ca organele de drept să înțeleagă că acest lucru e posibil. Performanțele calculatoarelor, ale telefoanelor mobile și internetului, ale tabletelor și altor gadget-uri sunt însușite foarte rapid de către infractori, reieșind din faptul că scopul urmărit de aceștia este de a încălca norma de drept, iar aceste sistemele informaționale oferă posibilitatea de a fi folosite drept instrumente în realizarea unor scopuri infracționale.

Actualitatea și importanța prezentei teze rezidă și în identificarea soluțiilor pentru o serie de probleme privind cercetarea infracțiunilor informatice, având în vedere absența instruirilor organelor de drept în domeniul dat, precum și faptul că, până în prezent, fiecare angajat, în momentul când se pune în fața problemei de cercetare a unor ilegalități informatice, o face în limitele competenței sale, nefiind informat de corectitudinea activităților și căror indici de la fața locului să le acorde prioritate. Totodată, o atenție aparte, în această lucrare, se acordă aplicării metodelor și tehnicilor de extragere și examinare a datelor informatice în cazul acestor infracțiuni, întrucât, aceste acțiuni sunt de o deosebită importanță în vederea depistării și stabilirii probelor digitale.

O altă particularitate abordată în prezenta lucrare, sunt metodele și tehnicile utilizate pentru examinarea sistemelor informaționale, extragerea datelor de pe aceste astfel, încât dispozitivul de stocare a informației să rămână intact, aceasta fiind principiul de bază al activității experților criminaliști în cadrul efectuării expertizelor mijloacelor și tehnologiilor informaționale, de asemenea sunt studiate și metodele

de extragere și examinare a datelor de pe dispozitivele mobile, securitatea cărora este în continuă dezvoltare, iar noi tehnici și metode de a extrage datele de pe acestea sunt din ce în ce mai greu de depistat.

Toate acestea au determinat actualitatea temei prezentului studiu, o asemenea cercetare în domeniul vizat reprezentând una din sarcinile prioritare ale organelor de drept.

Scopul și obiectivele tezei. Scopul prezentei lucrări rezidă în identificarea metodologiei și a tehnicilor adecvate de investigare a infracțiunilor informatice, atât prim prisma actelor juridice cât și la nivel practic, în special în procesul de extragere a datelor de pe suporturile digitale în cadrul cercetării infracțiunilor informatice cu păstrarea intactă a suporturilor respective. Atingerea scopului propus este condiționată de realizarea următoarelor obiective:

- prezentarea fenomenului de criminalitate informatică, reglementarea acesteia de actele juridice interne cât și internaționale;
- prezentarea fenomenului de monitorizare și identificare a ilegalităților informatice;
- descrierea efectuării acțiunilor de urmărire penală, ridicarea purtătorilor sau a dispozitivelor informatice ce au contribuit la săvârșirea infracțiunii;
- descrierea și prezentarea metodelor de extragere a informației de pe dispozitivele de stocare a informației;
- descrierea și prezentarea metodelor de extragere a informației de pe dispozitivele mobile;
- examinarea datelor extrase, selectarea probelor relevante pentru cauza penală, întocmirea raportului de expertiză și remiterea materialelor pentru ulterioara analiză și transmiterea dosarului în judecată.

Bibliografie

Cărți și monografii

1. Крылов В.В. ”*Информационные компьютерные преступления: Учебное и практическое пособие*”. Москва: Инфра-М – Норма, 1997.
2. Моцкобили И. ”*Хакеры рвутся к мировому господству*”. În: Комерсант – Daily, 1998.
3. Алексей Гултяев ”*Востановление даных*” ediția a 2-a, 2006.
4. Iurie O., Lilian L., Constantin R. ”*Cercetarea la fața locului”*, Chișinău 2003.

Standarde, norme, ghiduri de utilizare

5. Codul penal al Republicii Moldova https://www.legis.md/cautare/getResults?doc_id=133053&lang=ro#
6. Codul de procedură penală al Republicii Moldova https://www.legis.md/cautare/getResults?doc_id=133060&lang=ro#
7. Legea Nr. 68 ”Cu privire la expertiza judiciară și statulul expertului judiciar” https://www.legis.md/cautare/getResults?doc_id=132473&lang=ro
8. *Ghidul ordonatorului expertizei judiciare*, Chișinău 2022.
9. Instrucțiunea CI 6.4-3.01(1)2020 *Utilizarea echipamentului ”Tableau TD3 Touch Screen Forensic Imager”.*
10. Instrucțiunea CI 6.4-3.07(1)2020 *Utilizarea echipamentului ”Ditto Forensic FieldStation”.*
11. Instrucțiunea CI 6.4-3.08(1)2020 *Virtualizarea sistemelor informatice.*
12. Procedura CPT 3.1-01(2)2020 *Pregătirea spre examinare și efectuarea copiei criminalistice a informației digitale din dispozitivele de stocare*
13. Procedura CPT 3.1-02(2)2020 *Examinarea informațiilor stocate pe purtători de informații*
14. Procedura CPT 3.1-03(2)2020 *Examinarea dispozitivelor mobile*

Pagini WEB

15. Specialist hardware for all weathers, [citat 25.11.2022]. Disponibil: https://ondatashop. com/msab-field/ .
16. UFED Touch 2, [citat 29.11.2022] http://aimtech.ru/catalog/155
17. Oxygen Forensic Detective [citat 15.12.2022]. Disponibil: https://ondatashop.com/oxygen-forensic-suite-2014/