MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___” _____ 2025

PROCEDURI ȘI INSTRUCȚIUNI TIC PENTRU EXPERTIZE JUDICIARE

Proiect de master

Student: _____ **Zara Valeriu, SI-231M**

Coordonator: _____ **Bulai Rodica, asist. univ.**

Consultant: _____ **Bulai Rodica, asist. univ.**

Chişinău, 2025

REZUMAT

Zara Valeriu, „PROCEDURI ȘI INSTRUCȚIUNI TIC PENTRU EXPERTIZE JUDICIARE”, teza de masterat, Chișinău, 2025

Cuvinte cheie: forensics, software, hardware, OS, copia criminalistică, căutarea informațiilor textuale, căutarea informațiilor grafice, proceduri tehnice, instrucțiuni.

Structura tezei: Teza de master este constituită din introducere, trei capitole și concluzii, 50 pagini de text de bază, inclusiv 34 de figuri și un tabel.

Această teză de master explorează utilizarea procedurilor tehnice și a instrucțiunilor în domeniul cercetărilor Tehnologiilor Informaționale și Comunicațiilor (TIC). În cadrul introducerii, proiectul se concentrează asupra importanței și necesității procedurilor tehnice și a instrucțiunilor în contextul expertizelor judiciare în domeniul TIC. Scopul principal al acestei cercetări este de a dezvolta și implementa proceduri tehnice eficiente și instrucțiuni clare pentru utilizarea echipamentelor și softurilor din dotarea unui laborator criminalistic specializat.

Semnificația și valoarea aplicativă. Această cercetare aduce o contribuție semnificativă în domeniul expertizelor judiciare TIC, oferind un cadru solid pentru pregătirea, desfășurarea și gestionarea acestor investigații specializate. Este un pas esențial în direcția asigurării calității și eficienței în procesul de expertiză judiciară în contextul tehnologiilor informaționale și comunicărilor.

În prima secțiune a proiectului, se abordează procedurile tehnice fundamentale care stau la baza expertizelor judiciare, cu accent pe pregătirea pentru examinare și efectuarea copiei criminalistice a informației digitale, examinarea informațiilor stocate pe diferiți purtători de informații și examinarea dispozitivelor mobile.

Partea a doua a proiectului se axează pe elaborarea instrucțiunilor de utilizare a echipamentului și softului din dotarea laboratorului criminalistic. Aceasta include virtualizarea sistemelor informatice și utilizarea unor echipamente specifice precum "Tableau TD3 Touch Screen Forensic Imager", "Tableau SATA/IDE Forensic Bridge T35u" și "Ditto Forensic FieldStation". Fiecare instrument este detaliat în ceea ce privește funcționalitățile sale și modul de utilizare.

În final, proiectul acoperă implementarea procedurilor și instrucțiunilor dezvoltate în cadrul unui sistem de management, inclusiv cerințe generale pentru competența laboratoarelor de încercări și etalonări, precum și elaborarea rapoartelor de expertiză judiciară.

ABSTRACT

Zara Valeriu, ”ICT PROCEDURES AND INSTRUCTIONS FOR JUDICIAL EXPERTISE”, master thesis, Chișinău 2025

Keywords: forensics, software, hardware, OS, forensic copy, textual information search, graphic information search, technical procedures, instructions.

Thesis structure: The master's thesis consists of an introduction, three chapters, and conclusions, 50 pages of main text, including 34 figures and 1 table.

This master's thesis explores the use of technical procedures and instructions in the field of Information and Communication Technologies (ICT) investigations. In the introduction, the project focuses on the importance and necessity of technical procedures and instructions in the context of judicial expertise in the field of ICT. The main purpose of this research is to develop and implement efficient technical procedures and clear instructions for the use of equipment and software in a specialized forensic laboratory.

Significance and Applicability: This research makes a significant contribution to the field of ICT judicial expertise, providing a solid framework for the preparation, conduct, and management of these specialized investigations. It is an essential step towards ensuring the quality and efficiency of the judicial expertise process in the context of information technologies and communications.

The first section of the project addresses fundamental technical procedures underlying judicial expertise, with a focus on preparation for examination and the forensic copying of digital information, examination of information stored on various carriers, and examination of mobile devices.

The second part of the project focuses on the development of instructions for the use of equipment and software in the forensic laboratory. This includes virtualization of information systems and the use of specific equipment such as "Tableau TD3 Touch Screen Forensic Imager," "Tableau SATA/IDE Forensic Bridge T35u," and "Ditto Forensic FieldStation." Each instrument is detailed regarding its functionalities and mode of use.

Finally, the project covers the implementation of developed procedures and instructions in a management system, including general requirements for the competence of testing and calibration laboratories, as well as the preparation of judicial expertise reports.

CUPRINS

LISTA ABREVIERILOR

DSI – Dispozitiv de stocare a informației.

DM – Dispozitiv mobil.

IDE (acronimul expresiei engl. ”Integrated Drive Electronics”) – este un standard electronic de interfață paralelă care realizează conectarea adaptoarelor locale (de regulă ele sunt integrate pe plăcile de bază a calculatoarelor staționare și portabile) cu dispozitivele de stocare a datelor (cum ar fi unități de hard disk și unitățile optice).

SATA (acronimul expresiei engl. ”Serial Advanced Technology Attachment”) – este o interfață mai nouă, succesorul standardului IDE, care realizează conectarea adaptoarelor locale (de regulă ele sunt integrate pe plăcile de bază a calculatoarelor staționare și portabile) cu dispozitivele de stocare a datelor (cum ar fi unități de hard disk și unitățile optice).

USB (acronimul expresiei engl. ”Universal Serial Bus”) – este o interfață de conectare pentru echipamente periferice care se pot conecta Plug an Play, cum ar fi telefonul, camera foto-video, cardul de memorie, tastatura, hard-diskuri externe imprimanta etc.

SCSI – (acronimul expresiei engl. ” Small Computer System Interface”) – este o interfață de conectare pentru echipamente periferice de viteză mare, este un standard mai vechi, se utilizează preponderent în servere.

SAS (acronimul expresiei engl” Serial Attached SCSI”) – este o interfață mai nouă, succesorul standardului SCSI, care realizează conectarea adaptoarelor locale cu dispozitivele de stocare a datelor (cum ar fi unități de hard disk și unitățile optice). Interfața SAS oferă mai multe avantaje față de interfața SCSI: reducerea dimensiunii cablului și costului, transfer de date mai rapid prin rate de semnalizări mai mari.

M.2 – este o interfață de conexiune de generație nouă care a substituit formatul ”mSATA,, se utilizează de obicei pentru DSI pe bază de SSD.

FireWare – este denumirea dată de compania APPLE portului ”IEEE 1394”. Portul respectiv reprezintă o conexiune de date utilizată preponderent de compania Apple.

DCO (acronimul expresiei engl. ”Device configuration overlay”) – este o porțiune ascunsă de pe hard care nu este vizibilă sistemului de operare.

HPA (acronimul expresiei engl. ”Host/Hidden protected area ”) – este o porțiune de pe hard care nu este normal vizibilă într-un sistem de operare.

HOST (cuv.engl.) – semnifică calculatorul gazdă.

DSI – acronimul expresiei ”dispozitiv de stocare a informației”.

SSD– acronimul expresiei (Solid State Drive) reprezintă un DSI, principiul de lucru al căruia este bazat pe microcircuite cu tranzistoare de câmp.

Imagine – copia bit cu bit a unui dispozitiv de stocare a informației.

Sursă – reprezintă conexiunea care este protejată contra înscrierii (write blocked), adică datele pot fi doar citite dar nu și înscrise, această opțiune este implementată la nivel de hardware și exclude careva modificări pe purtătorul sursă (de obicei este purtătorul expus examinării criminalistice).

Destinație – reprezintă conexiunea care este utilizată pentru stocarea datelor parvenite de la sursă, conexiunea permite schimbul liber de date.

RJ45 – (acronimul expresiei engl. ”Registered Jack”) reprezintă standard de interfață de rețea care cuprinde două părți de legătură (”conector” și ”priza”). Este utilizat pentru conectarea echipamentelor de telecomunicații.

Wipe (sterilizare) – este un proces de sterilizare a datelor (fizic toți biții de pe DSI se înscriu cu valoarea 0).

Hash – reprezintă o funcție matematică care poate fi calculată ireversibil, ca rezultat obținem un șir de caractere.

mSATA - (mini SATA) reprezintă o interfață de conexiune de generație nouă, compactă, se utilizează de obicei în sisteme compacte. Poate fi utilizată pentru conexiuni de DSI.

BIOS – (acronimul expresiei engleze Basic Input/Output System) reprezintă un software care face legătura dintre componentele fizice și sistemul de operare a computerului. De asemenea biosul face verificarea componentelor la pornirea sistemului.

Imagistică - proces de efectuare a copiei criminalistice.

RAID Masiv – reprezintă modalitate de conexiune a DSI în diferite combinații cu scopul de a mări siguranța sau capacitatea în dependență de necesitate.

Fișier - obiect informațional ce conține date într-un anumit format stocate pe un suport, este identificat printr-un nume și printr-o extensie de nume opțională.

Directorii – (eng. Directory) sunt locații, organizate ierarhic (arborescent), pe purtători de informații, în care se găsesc informațiile (datele) sub formă de fișiere sau alte directorii. Directoriile ce se conțin în interiorul altor directorii se numesc subdirectorii.

Parolă - (eng. Password), scriere confidențială de caractere care permite unui utilizator să acceseze un fișier sau să se autentifice pentru a avea acces la diferite resurse.

Cuvînt cheie – este o consecutivitate de simboluri care alcătuiesc un cuvînt sau o frază fără luarea în considerație a codificarea (unicod, UTF-8 etc).

Bază de date – (BD) structură de date care permite stocarea informațiilor într-un mod structurat astfel încît acestea să poată fi ordonate și sortate ulterior. Fiecare grup se numește înregistrare și fiecare partea a unei înregistrări se numește cîmp.

Digitală – metodă de reprezentare a informației ca numere cu valori discrete, fiind reprezentată de obicei ca o secvență de biți.

Informații alocate – reprezintă informații alocate într-un sistem de fișiere și care conțin descriere la nivel de disc logic, directoriu, calea amplasării în sistemul de fișiere.

Informații nealocate – reprezintă informații care nu sunt alocate unui sistem de fișiere și sunt recuperate cu descriere la nivel de sector, cluster fizic a DSI.

Informații ascunse sau criptografic protejate – reprezintă informații pentru interpretarea corectă a cărora este nevoie de încă o operațiune (decriptare, afișare). O astfel de acțiune poate fi efectuată precum automat de către sistemul de operare sau utilizator (prin introducerea parolei). Informația ascunsă este protejată de citirea directă a ei printr-un element care se află în afara sistemului (parolă sau cheie hardware).

Analiza (informației) – (provine din grecească și semnifică partajarea pe părți componente, dezasamblare) operațiune reală sau imaginară de partajare (obiectului, proprietăților, proceselor sau relații dintre obiecte) pe părți componente, care este efectuată în procesul de cunoaștere sau lucrărilor practice efectuate de om.

Metadatele – Reprezintă date care caracterizează alte date cu scopul de identificare sau atribuire la grup (reprezintă date despre date, permit o clarificare a informației).

Probe digitale - probele digitale sunt definite ca fiind informaţii cu valoare investigativă care sunt stocate, prelucrate sau transmise într-un format digital de un dispozitiv, sistem electronic.

Sistem informatic– ansamblu de programe şi echipamente care asigură prelucrarea automată a datelor.

Mediu informaţional - totalitatea programelor soft instalate în sistemul informaţional.

Purtător de informaţie - obiectul material destinat pentru păstrarea şi redarea informaţiei în format digital.

Dispozitiv de stocare a informaţiei - dispozitiv destinat pentru stocarea informaţiei (datelor) ce rămîn înscrise şi care ulterior pot fi utilizate. El conţine purtător de informaţie, dispozitiv de citire a informaţiei (de pe purtător) şi dispozitiv de înscriere a informaţiei (pe purtător).

Date – informaţie prezentată într-o anumită formă (text, imagine, etc) care permite a o comunica, comenta şi prelucra.

Disc logic – o parte a purtătorului de informaţie separată logic de celelalte părţi al acestuia, interpretat de sistemul de operare ca o componentă aparte cu o anumită capacitate.

Sistem de operare - reprezintă un produs software care este parte componentă a unui sistem informatic, echipament sau aparat computerizat, şi care se ocupă de gestionarea şi coordonarea activităţilor acestuia.

Server – un mediu informațional sau aplicație ce gestionează activitatea unei rețele de medii informaționale sau aplicații, avînd funcția de furnizare a serviciilor multiple utilizatorilor.

Utilizator – mediu informațional conectat la rețea de calculatoare, fiind consumator de servicii şi

neacordînd servicii în schimb.

Suma Hash – reprezintă o funcție matematică care poate fi calculată ireversibil, ca rezultat obținem un șir de caractere.

Imagine (copie) – Reprezintă copia bit cu cu bit sau compresată în format criminalistic a unui purtător de informație.

Antetul fișierului (header) – Reprezintă primii doi biți a unui fișier prin intermediul cărora este caracterizat tipul și formatul fișierului.

Container - sistem informatic virtual cu resurse hardware virtualizate.

LXC - implementare pentru Linux a virtualizării la nivelul sistemului de operare.

Regim *live* - regim de lucru al unui sistem informatic cu sau fără interfață GUI.

LXC WEB Panel – interfața de manipulare cu containerele LXC din browser.

TFU – (acronimul expresiei engl. ”Tableau Firmware Update”) – soft de actualizare a sistemului de operare a producătorului din dispozitivul T35u.

T35u - este un dispozitiv electronic (echipament) pentru examinări criminalistice în regim ”blocare înscriere” (doar citire) pentru dispozitivele de tip SATA și de tip IDE printr-o singură conexiune gazdă de tip ”USB 3.0”.

USB (acronimul expresiei engl. ” Universal Serial Bus”) – este o interfață de conectare pentru echipamente periferice care se pot conecta Plug an Play, cum ar fi telefonul, camera foto-video, cardul de memorie, tastatura, hard-diskuri externe imprimanta etc. A fost creat în ianuarie 1996.

HOST (cuv.engl.) – semnifică calculatorul gazdă.

HPA (acronimul expresiei engl. ”Host/Hidden protected area ”) – este o porțiune de pe hard care nu este normal vizibilă într-un sistem de operare.

Write Block (expresie engleză) – blocaj la înscriere pe dispozitivul de stocare a informației.

Volatil – memorie care dispare după o anumită stare.

INTRODUCERE

Cadrul tehnologic contemporan a generat o creștere exponențială a complexității investigațiilor judiciare în domeniul Tehnologiilor Informaționale și Comunicațiilor (TIC). Progresul rapid al tehnologiei a impus necesitatea unei abordări avansate și specializate pentru desfășurarea expertizelor în acest context din ce în ce mai complex.

Expertiza judiciară constituie o modalitate legală de colectare și prezentare a probelor în fața instanței de judecată, fiind efectuată de către experți înscrise în lista experților judiciari a Ministerului Justiției. În prezent, sprijinul de specialitate acordat organelor de urmărire penală, agenților constatatori și societății civile impune instituțiilor specializate în expertiza judiciară responsabilitatea de a răspunde prompt necesităților anchetei. De asemenea, aceste instituții trebuie să examineze obiectiv și cuprinzător elementele de probă prezentate, oferind, nu în ultimul rând, asistență metodologică și practică organelor de urmărire penală sau altor părți interesate.

Avansul rapid al tehnologiilor conduce la situații în care infracțiunile sunt comise folosind sau prin intermediul sistemelor informatice, subliniind necesitatea de a fixa și examina probele aflate în cadrul acestora. Sistemele informatice operează conform unor modele matematice bine definite, furnizând o multitudine de mecanisme pentru fixarea activității interne și înregistrarea acțiunilor operatorilor. Aceasta facilitează documentarea și fixarea datelor relevante pentru reconstrucția informațiilor privind activitățile anterioare, contribuind la stabilirea adevărului. Cu toate acestea, este imperativ să avem un algoritm de fixare și documentare a datelor în cadrul sistemului informatic care să fie sigur și să utilizeze metode non-distructive, acolo unde este posibil [1].

În prezent, nu există în organele specializate o metodologie unică și aprobată la nivel național pentru examinarea purtătorilor de informație digitală. Elaborarea unei astfel de metodologii ar oferi o oportunitate de a dezvolta o abordare metodologică unitară pentru procesul de examinare a informației, fixare a probelor și întocmire a materialelor examinării. Având în vedere evoluția rapidă a noilor tehnologii și dispozitive, experții necesită cunoștințe extinse, iar instruirea continuă este esențială pentru aceștia și pentru reprezentanții organelor de urmărire penală care vor utiliza probele obținute în urma expertizelor.

Prezenta lucrare va descrie o serie de proceduri tehnice și instrucțiuni elaborate în cadrul secției specializate în examinarea tehnologiilor informaționale și comunicațiilor. Totodată va fi descris mecanismul de aplicare a procedurilor și instrucțiunilor respective pentru întocmirea unui raport de expertiză judiciară.

Utilizarea procedurilor tehnice și a instrucțiunilor în domeniul cercetărilor mijloacelor și tehnologiilor informaționale este esențială pentru asigurarea eficienței și corectitudinii procesului de cercetare. Aceste instrumente metodologice oferă un cadru clar și bine definit pentru desfășurarea investigațiilor, reducând riscul de erori și sporind încrederea în concluziile obținute. În acest context,

pentru standardizarea proceselor de cercetare, vor fi elaborate proceduri standard și instrucțiuni detaliate, care să faciliteze aplicarea unor metode uniforme și transparente.

Procedurile standard vor asigura coerența și fiabilitatea rezultatelor expertizei, oferind cercetătorilor un set clar de pași care să fie urmat în orice situație. Ele vor fi adaptate la specificul diferitelor tipuri de tehnologii informaționale și vor include metode de colectare, analiză și interpretare a datelor. În același timp, instrucțiunile detaliate vor contribui la reproductibilitatea cercetării, oferind explicații pas cu pas despre cum să fie aplicate metodele și tehnicile utilizate. Acestea vor permite altor cercetători să înțeleagă și să aplice studiul, asigurând astfel continuitatea cercetărilor și creșterea calității acestora.

Un alt avantaj al utilizării acestor proceduri și instrucțiuni este crearea unei baze documentare solide, care să sprijine procesul decizional și să faciliteze verificarea rezultatelor. Documentarea detaliată a fiecărei etape a cercetării va servi nu doar ca referință pentru alți experți, ci și ca instrument de audit în cazul unor controverse sau întrebări legate de validitatea concluziilor. De asemenea, utilizarea unor proceduri bine definite contribuie la respectarea reglementărilor legale și a standardelor deontologice, asigurând că procesul de cercetare este realizat într-un mod etic și profesionist.

Integrarea acestor practici în domeniul cercetărilor mijloacelor și tehnologiilor informaționale sprijină inovarea și dezvoltarea continuă a metodologiilor. Prin utilizarea unor proceduri și instrucțiuni riguroase, se creează premisele pentru o colaborare mai eficientă între cercetători, instituții și organisme juridice, contribuind astfel la progresul domeniului și la creșterea încrederii în rezultatele obținute. Astfel, implementarea acestor instrumente devine o condiție indispensabilă pentru consolidarea și avansarea cercetărilor în domeniul tehnologiilor informaționale [2], [3].

BIBLIOGRAFIE

[1] I. Oprea, L. Lozan, and C. Rusu, "Cercetarea la fața locului," Chișinău: Editura XYZ, 2003.

[2] Republica Moldova, "Codul penal al Republicii Moldova," 2023.

[3] Republica Moldova, "Codul de procedură penală al Republicii Moldova," 2023.

[4] S. Smith, "Digital Forensics: Principles and Techniques," Cambridge: MIT Press, 2020.

[5] M. Jones, "Cybercrime Investigation: Practical Approaches," New York: CRC Press, 2018.

[6] T. Brown, "Network Security Essentials," 5th ed., Pearson Education, 2021.

[7] K. Zhang, "Machine Learning in Digital Forensics," Beijing: Springer, 2019.

[8] "ISO/IEC 27037: Guidelines for the identification, collection, acquisition, and preservation of digital evidence," ISO Standards, 2012.

[9] "NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response," NIST, 2006.

[10] "ENFSI: Best Practice Manual for Digital Evidence," European Network of Forensic Science Institutes, 2015.

[11] P. Martinez, "Advanced Cybersecurity Strategies," San Francisco: O'Reilly Media, 2017.

[12] A. Johnson, "Ethical Hacking Techniques and Tools," Chicago: Wiley, 2019.

[13] B. Davis, "Cybercrime and Digital Forensics," London: Routledge, 2020.

[14] J. Miller, "Cloud Computing Forensics," Boston: Addison-Wesley, 2018.

[15] S. Gupta, "Blockchain Security and Applications," New Delhi: Tata McGraw Hill, 2019.

[16] H. Lee, "AI in Cybersecurity," Seoul: Wiley, 2021.

[17] O. Ivanov, "Evidența și conservarea probelor digitale," București: Editura XYZ, 2020.

[18] C. Popescu, "Infracțiuni informatice: O abordare practică," Cluj-Napoca: Editura ABC, 2019.

[19] M. Rădoi, "Securitatea rețelelor informatice," Iași: Editura Trei, 2018.

[20] K. Johnson, "IoT Forensics," Oxford: Elsevier, 2020.

[21] F. Silva, "Digital Evidence Management," Lisbon: Springer, 2021.

[22] "CEH v11: Certified Ethical Hacker Study Guide," EC-Council, 2021.

[23] J. Rodriguez, "Digital Evidence Collection," Madrid: McGraw-Hill, 2019.

[24] A. Nakamura, "Cryptographic Systems: An Introduction," Tokyo: Springer, 2020.

[25] "IEEE 2410-2017: Standard for Biometrics," IEEE Standards, 2017.

[26] L. Wang, "Big Data Analytics in Forensics," Singapore: World Scientific, 2018.