Universitatea Tehnică a Moldovei

Laborator criminalistic securizat pentru expertize în domeniul TI

Masterand: Gaina Ion

Conducător: Putere Alexandru
lect. univ.

Chișinău, 2020

Ministerul Educației Culturii și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susținere

Şef departament: conf. univ., dr. Ion Fiodorov

„__”_____ 2020

Laborator criminalistic securizat pentru expertize în domeniul TI

Teză de master în Securitate Informațională

Masterand: **Gaina Ion**

Conducător: **Putere Alexandru**
lect. univ.

Chișinău, 2020

ADNOTARE

la teza de master cu tema

LABORATOR CRIMINALISTIC SECURIZAT PENTRU EXPERTIZE ÎN DOMENIUL TI,

Chișinău, 2020

Structura tezei. Teza de master este constituită din introducere, cinci capitole, concluzii și recomandări, bibliografie cu 20 de titluri, 70 pagini de text de bază, inclusiv 45 de figuri.

Cuvinte cheie: Copia digitală, examinarea setărilor de bios, căutarea informațiilor textuale, căutarea informațiilor grafice, analiza metadatelor, infrastructura de stocare, infrastructura de rețea, infrastructura de procesare.

Domeniul de studiu și obiectivele tezei propuse spre susținere se încadrează în domeniul creării unui laborator securizat pentru executarea expertizei mijloacelor și tehnologiilor informaționale în cadrul căreia s-au evidențiat așa obiective ca, efectuarea copiei digitale a unui sistem informatic și conservarea acesteia, noțiunea de copie digitală și diferența ei de cea analogică , procesarea datelor obținute în urma copiei digitale a sistemului informatic, examinarea siguranței procedurii de copie digitală, proiectarea infrastructurii de rețea, procesare și stocare a laboratorului cu capacitatea de 10 posturi de lucru.

Noutatea și originalitatea științifică a lucrării constă în posibilitatea de implementare a unui laborator criminalistic securizat pentru expertize în domeniul TI semiautomat, aplicarea metodei de copie digitală la conservarea probelor în cadrul procesului penal, și demonstrarea veridicității acestora la examinarea ulterioară.

Semnificația și valoarea aplicativă, modalitățile de examinare și infrastructura laboratorului expuse în lucrare vor permite ridicarea calității expertizei judiciare a sistemelor informatice dar și va contribui la procesul de menținere a acreditarii laboratoarelor naționale.

ANNOTATION

at master thesis with theme

SECURE FORENSIC LABORATORY FOR IT EXPERTISE, Chisinau, 2020

The structure of thesis. The master's thesis consists of an introduction, five chapters, conclusions, recommendations, a bibliography with 20 titles, and 70 pages of basic text, including 45 figures.

Keywords: Digital copy, examination of BIOS settings, the searching for textual information, the searching for graphical information, metadata analysis.

The field of study and the objectives of the thesis proposed for defense fall within the field of creating a secure laboratory for the execution of expertise in information devices and technologies in which such objectives have been highlighted as the digital copying of a computer system and its preservation, the notion of digital copying and its difference from the analog one, processing the data obtained from the digital copy of the computer system, examining the security of the digital copy procedure, designing of the infrastructures of the network, infrastructure of processing and storing, for the laboratory with the capacity of 10 workstations.

The novelty and scientific originality of the paper consists in the possibility of implementing a secure semi-automated IT forensic laboratory for expertise, applying the digital copy method to the preservation of evidence in criminal proceedings, and demonstrating their veracity in the subsequent examination.

The meaning and applicative value: the examination modalities and the laboratory infrastructure exposed in the paper will raise the quality of the judicial expertise of the information systems. And they will also contribute to the process of maintaining the accreditation of the national laboratories.

CUPRINS

LISTA ABREVIERILOR ȘI DIFINIȚIILOR

DSI – Dispozitiv de stocare a informației.

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 cuvânt 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 încât acestea să poată fi ordonate și sortate ulterior. Fiecare grup se numește înregistrare și fiecare partea a unei înregistrări se numește câmp.

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 greacească 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 informații 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 informațional - totalitatea programelor soft instalate în sistemul informațional.

Purtător de informație - obiectul material destinat pentru păstrarea și redarea informației în format digital.

Dispozitiv de stocare a informației - dispozitiv destinat pentru stocarea informației (datelor) ce rămân înscrise şi care ulterior pot fi utilizate. El conține purtător de informație, dispozitiv de citire a informației (de pe purtător) şi dispozitiv de înscriere a informației (pe purtător).

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

Disc logic – o parte a purtătorului de informație separată logic de celelalte părți 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, și care se ocupă de gestionarea și coordonarea activităților acestuia.

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

Utilizator – mediu informațional conectat la rețea de calculatoare, fiind consumator de servicii și neacordând 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 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.

INTRODUCERE

Tehnologiile informaționale au devenit un instrument pentru modernizarea stilului de viață a omului. La moment ele își au influența în toate domeniile vieții. Indiferent în ce activitate omul este implicat (economică, politică, socială), oricum într-o oarecare măsură sunt implicate și tehnologiile informaționale. În unele cazuri tehnologiile informaționale devin un instrument pentru a atinge scopuri infracționale. Aceasta cauzează o necesitate stringentă de a examina tehnologiile informaționale cu scopul de a obține probe care pot demonstra vinovăția sau nevinovăția persoanei care a utilizat o anumită tehnologie informațională. Complexitatea tehnologiilor în acest caz ne poate cauza dificultăți semnificative. Pentru a depăși aceste dificultăți sunt necesare metodici si echipamente specializate în domeniul examinării mijloacelor și tehnologiilor informaționale. Combinarea acestor metode și tehnologii este posibilă în cadrul unor condiții specifice a unui laborator. Activitățile de căutare și trasare a probelor sunt caracteristice științei denumită criminalistică, care este de obicei aplicabilă pentru obiectele materiale și nemateriale cu scopul de a obține probe prin metode științifice. De aici apare necesitatea de a aplica metode științifice sau efectuarea unor cercetări asupra tehnologiilor informatice cu scopul documentării acestora în rapoarte de expertiză judiciară.

Expertiza Judiciară reprezintă o modalitate legală de acumulare și prezentare a probelor în instanța de judecată, este efectuată de către experți care sunt prezenți în lista experților judiciari a Ministerului Justiției. Situația actuală în sprijinul de specialitate a organelor de urmărire penală, agenților constatatori, și societate civilă solicită de la instituțiile specializate în expertiza judiciară în primul rând, de a răspunde rapid la necesitățile anchetei și în al doilea rând de a examina obiectiv și multilateral corpurile delicte prezentate, la fel nu în ultimul rând de a acorda un ajutor metodic și practic organului de urmărire penală sau persoanelor cointeresate.

Dezvoltarea rapidă a tehnologiilor ne cauzează situații în care infracțiunile sunt efectuate cu utilizarea sistemelor informatice sau prin intermediul acestora, respectiv apare necesitatea de a fixa și examina probele care vor fi în interiorul acestora. Sistemele informatice activează după modele matematice care sunt bine determinate cu o mulțime de mecanisme de fixare a activității sale interne și logării acțiunilor efectuate de operator. Acest fapt permite documentarea și fixarea datelor importante pentru restabilirea informațiilor cu privire la activitățile anterioare. Aceste informații pot confirma sau infirma unele activități efectuate într-un sistem informatic care până la final vor duce la stabilirea adevărului. Cu toate acestea noi avem nevoie de un algoritm de fixare și documentare a datelor ce se conțin în sistemul informatic care să fie sigur, cu utilizarea metodelor non distructive (în cazul în care este posibil).

La ziua de azi în organele de specialitate nu există o metodologie unică de examinare a purtătorilor de informație digitală aprobată și întărită la nivel național. Elaborarea unei metodologii pentru examinarea purtătorilor de informație digitală va oferi o oportunitate de a dezvolta o abordare metodologică unică a

procesului de examinare a informației, fixare a probelor, întocmire a materialelor examinării. Situația actuală de dezvoltare a noilor tehnologii și dispozitive solicită de la experți un spectru larg de cunoștințe nivelul cărora este necesar permanent de perfecționat. Tot odată putem preciza că o instruire continuă necesită nu doar experții care efectuează astfel de expertize dar și reprezentanții organului de urmărire penală care nemijlocit vor recepționa probele obținute în urma expertizei.

Metodologia examinărilor poate fi dependentă de o infrastructură care este construită în baza acesteia, ea poate fi simplistă sau mai complicată însă la final rezultatele trebuie să fie aceleași. Prezenta lucrare va descrie unele din posibile arhitecturi a unui laborator în domeniul IT cu aplicarea unor mecanisme și tehnologii de securitate a informației bazate pe metodologia existentă. Prin elaborarea acestei infrastructuri se tinde spre crearea unui mecanism semiautomat de prelucrare și analiză a datelor extrase din sistemele informatice. La moment există mai multe modalități de examinare a unui sistem informatic însă acestea necesită o implicare semnificativă a factorului uman care în fine poate cauza unele erori. Prin elaborarea unor mecanisme semiautomate se propune a minimiza acest factor și respectiv de a majora calitatea examinărilor efectuate. De asemeni putem constata că complexitatea tehnologiilor informaționale cauzează o varietate enormă de sarcini care trebuie soluționate în cadrul examinărilor tehnologiilor informatice. Toate aceste varietăți necesită resurse și metodologii. Un alt punct care se dorește să fie atins în această lucrare este elaborarea unei infrastructuri modulare a unui laborator de examinări tehnologii IT. Se presupune că fiecare modul va fi independent la etapa sa și va permite utilizatorului să schimbe succesiunea modulelor în dependență de necesitățile sale fără a afecta rezultatele examinării. Pentru a obține aceste rezultate este necesar de cunoscut elemente constructive a dispozitivelor care stochează informația precum și metodologia de examinare a sistemelor informatice. În baza acestor cunoștințe crearea infrastructurii necesare. Deci la final infrastructura propusă trebuie să conțină module flexibile semiautomate, un nivel de securitate a informației minim solicitat de legislația in vigoare și o eficiență maximă raportată la numărul de utilizatori ai sistemului.

În cadrul lucrării date se va crea o infrastructură a unui laborator de examinări tehnologii IT în care vor activa 10 persoane. Infrastructura fa fi elaborată și optimizată în așa fel ca influența activității fiecăruia să nu fie afectată reciproc. Maximă productivitate la utilizarea resurselor comune.

CONCLUZII ȘI RECOMANDĂRI

Sistemele informatice au o complexitate suficient de mare pentru ca o examinare rapidă și de o singură persoană să nu ne dea suficiente rezultate în investigații de securitate sau în cadrul procesului penal, acest fapt se datorează imperfecțiunii ființei umane. În cadrul acestei lucrări au fost abordate unele metodologii care ar permite conservarea datelor pentru un proces de examinare mai de durată sau repetat. Acest fapt ne permite să efectuăm de asemenea niște examinări simultane astfel soluționarea cauzei va fi mai rapidă. Unele lucrări cu diferit profil de activitate pot fi efectuate în același timp apoi completate unele cu altele. Toate acestea sunt posibile în cadrul unui laborator de examinări IT modular, care poate aplica diferite proceduri de analiză simultan. Aceste proceduri de analiză pot fi efectuate de o persoană prin profil predefinit sau de câteva în dependență de necesitățile examinării.

De asemenea în lucrarea dată sunt discutate unele algoritme de examinare a unui sistem informatic după efectuarea copiei digitale a dispozitivului de stocare a informației. Au fost abordate posibilitățile de căutare a informației textuale, problematica căutării acesteia în diferite codificări și în cazul prezenței acesteia în fotografii și fișiere scanate. A fost abordată tematica recuperării datelor din sistemele informatice, structura acestora și modalitățile de recuperare a acestora. Una din tematici actuale este căutarea informației grafice, posibilitățile de camuflare a acesteia în fișiere video și posibilitățile de camuflare a acesteia după miniaturile create de sistem. De asemenea a fost abordată o tematică care deseori ne acordă multe probe ferme în cazuri când ne disperăm să căutăm. Este vorba de metadatele fișierelor. Metodele descrise în lucrare sunt ușor aplicabile în cazul în care persoana care le aplică are suficiente cunoștințe în domeniu. Însă în cazul în care nu e, aceasta poate efectua doar etapele cunoscute de către el, iar celelalte etape vor fi efectuate de către o altă persoană care posedă suficiente competențe. În cadrul laboratorului proiectat cu totalitatea produselor soft și componentelor hard o astfel de abordare este acceptabilă și poate fi utilizată în producție.

Una dintre recomandări ar fi instruirea tuturor persoanelor care au tangență cu efectuarea copiei digitale cu scopul de a eficientiza rolul probelor digitale în procesul judiciar. Probele digitale pot fi conservate nu numai prin intermediul copiei digitale a întregului sistem dar și a unei părți componente a acesteia. Acest lucru este suficient de simplificat în cadrul modulului unu al laboratorului și permite setarea unor operațiuni în câteva clicuri.

În cadrul acestei lucrări de asemenea a fost abordată și veridicitatea metodei căreia ia fost dedicat un capitol întreg. Acest proces este foarte important și din acest considerent laboratorul trebuie să posede așa o posibilitate în regim automatizat. În urma verificării veridicității metodei sa constatat că aceasta posedă unii parametri importanți în aprecierea veridicității cum ar fi ”repetabilitatea „ și ”reproductibilitatea„. În continuare recomandam tuturor utilizarea metodelor și echipamentelor abordate în lucrarea respectivă inclusiv si a algoritmului de examinare urmând pașii descriși în lucrare. De asemeni

recomandam aplicarea infrastructurii laboratorului abordate în lucrarea respectivă cu scopul eficientizării activităților de laborator. Echipamentele descrie în lucrare sunt suficient de moderne pentru ziua de astăzi, însă cu timpul pot fi înlocuite cu alte elemente cu aceiași funcționalitate dar parametri mai avansați.

BIBLIOGRAFIE

1. ”Analiza și Validarea”, [online] COMP 2555: Principles of Computer Forensics, Autumn 2014 - [citat 18 Septembrie 2020]. Disponibil: www.cs.du.edu
2. ”Copia criminalistică”, [online] autor Sally Vandeven, septembrie 2014 [citat 23 Septembrie 2020]. Disponibil: – https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447
3. Dispozitive de stocare prin metode acustice [online] [citat 19 Septembrie 2020]. Disponibil: https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BC%D1%8F%D1%82%D1%8C_%D0%BD%D0%B0_%D0%BB%D0%B8%D0%BD%D0%B8%D1%8F%D1%85_%D0%B7%D0%B0%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B8
4. Dispozitive de stocare prin metode holografice [online] [citat 25 Septembrie 2020]. Disponibil: https://www.pctechguide.com/removable-storage/holographic-data-storage
5. Dispozitive de stocare laser [online] [citat 22 Septembrie 2020]. Disponibil: https://megamikejr.com/wp-content/uploads/2011/04/
6. Dispozitive de stocare pe principiu magnetic [online] [citat 23 Septembrie 2020]. Disponibil: http://ffden-2.phys.uaf.edu/211.fall2000.web.projects/J%20Kugler/magnetic.html
7. Dispozitive de stocare pe principiu magneto optic [online] [citat 26 Septembrie 2020]. Disponibil: http://ingrit.com/ingolf/career/index.htm
8. Dispozitiv de stocare pe bază moleculară [online] [citat 28 Septembrie 2020]. Disponibil: http://www.chem.gla.ac.uk/wp/magazine/improving-flash-memory-using-molecular-storage/
9. Energia stocată în condensatoare [online] [citat 29 Septembrie 2020]. Disponibil: http://hyperphysics.phy-astr.gsu.edu/hbase/electric/capeng.html
10. Ghidul de utilizare a echipamentului [online] ”Tableau TD3 Touch Screen Forensic Imager” – [citat 5 octombrie 2020]. Disponibil: https://www.guidancesoftware.com/docs/default-source/document-library/user-guide/td3-forensic-imager-user-guide.pdf?sfvrsn=19
11. Ghidul de utilizare a echipamentului ”Tableau T8-R2 USB Forensic Bridge” [online] [citat 7 octombrie 2020]. Disponibil:– https://tableau.guidancesoftware.com/pdf/en/Tableau_T8_R2_Product_Brief.pdf
12. Ghidul de utilizare a echipamentului ”Tableau SATA/IDE Forensic Bridge T35u” [online]– [citat 12 octombrie 2020]. Disponibil:https://www.guidancesoftware.com/docs/default-source/document-library/quick-start-guide/t35u-quick-reference-guide.pdf?sfvrsn=12

13. Ghidul de utilizare a echipamentului ”Tableau eSATA Forensic Bridge T35es R2” [online] [citat 18 Septembrie 2020]. Disponibil:– https://www.digitalintelligence.com/files/T35es-R2_Quickstart.pdf
14. Ghidul de utilizare a echipamentului ”Tableau T6es Forensic SAS Bridge” [online]– [citat 18 Septembrie 2020]. Disponibil: https://tableau.guidancesoftware.com/pdf/en/Tableau_T6es_Quickstart.pdf
15. Publicație web din 03.02.2011 – ”Validarea instrumentelor criminalistice și a software-ului” –[citat 18 Septembrie 2020]. Disponibil: [online] http://www.forensicmag.com/article/2011/03/validation-forensic-tools-and-software-quick-guide-digital-forensic-examiner
16. Publicație web din ianuarie 2015 – ”Validarea copiilor criminalistice pentru asigurarea integrității dovezilor digitale” [online]– [citat 12 octombrie 2020]. Disponibil: http://forensicphotoshop.blogspot.md/2015/01/validation-of-forensic-images-for.html
17. ”Metoda validării în criminalistica digitală”, iunie 2016 [online] –[citat 23 Septembrie 2020]. Disponibil: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/528123/FSR_Method_Validation_in_Digital_Forensics_FSR-G-218_Issue_1.pdf
18. Memorie bazată pe semiconductori [online] https://en.wikipedia.org/wiki/Semiconductor_memory
19. ”Standarde de calitate pentru criminalistica digitală”, Council of the Inspectors General on Integrity and Efficiency, Noiembrie 2012 [online] [citat 20 Septembrie 2020]. Disponibil: https://www.ignet.gov/
20. Stocare prin electrostatică [online] [citat 15 Septembrie 2020]. Disponibil: https://www.learncax.com/knowledge-base/blog/by-category/cfd/electrostatic-precipitators-esp-analysis-using-cfd