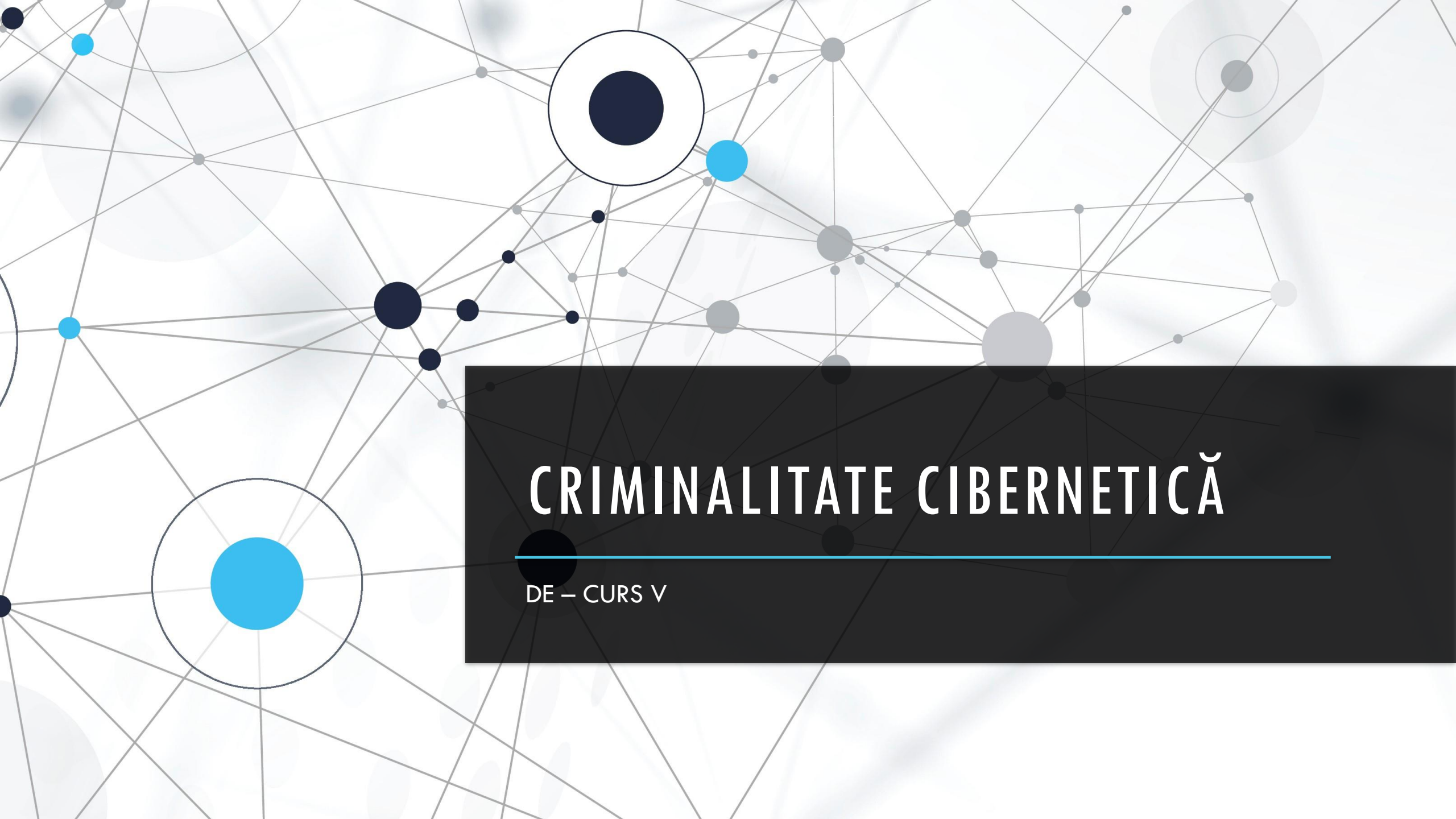




CRIMINALITATE CIBERNETICĂ

DE – CURS V

CRIMINALITATE CIBERNETICĂ PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

Conținut

- Bune practici internaționale cu privire la investigațiile informatice

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

GENERALITĂȚI

Investigarea criminalistică a sistemelor informatice prezintă o serie de particularități care o diferențiază în mod fundamental de alte tipuri de investigații.

Investigarea criminalistică a sistemelor informatice poate fi definită ca:

Utilizarea de metode științifice și certe de asigurare, strângere, validare, identificare, analiză, interpretare, documentare și prezentare a probelor de natură digitală obținute din surse de natură informatică

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

MODEL DE BUNE PRACTICI

1. • **Identificarea incidentului**
2. • **Pregătirea investigației**
3. • **Formularea strategiei de abordare**
4. • **Asigurarea probelor**
5. • **Strângerea probelor**
6. • **Examinarea probelor**
7. • **Analiza probelor**
8. • **Prezentarea probelor**
9. • **Restituirea probelor**

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

MODEL DE BUNE PRACTICI .

Un posibil model de bune practici în domeniul investigațiilor criminalistice de natură informatică cuprinde următorii pași:

1. **Identificarea incidentului** - recunoașterea unui incident informatic și determinarea tipului acestuia. Nu reprezintă efectiv o etapă a investigației criminalistice dar are un impact semnificativ asupra următoarelor etape.
2. **Pregătirea investigației** - pregătirea instrumentelor, verificarea procedurilor, obținerea documenter ce permit investigarea, etc.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

MODEL DE BUNE PRACTICI ..

3. **Formularea strategiei de abordare** - formularea unei strategii în funcție de tehnologia implicată și de posibilele consecințe asupra persoanelor și instituțiilor implicate. Scopul formulării acestei strategii este să maximizeze potențialul obținerii de probe relevante minimizând în același timp impactul negativ asupra victimei.

4. **Asigurarea probelor** - izolarea, asigurarea și păstrarea probelor de natură fizică și digitală. Aceasta include îndepărtarea celor care ar putea denatura probele în orice fel.

5. **Strângerea probelor** - înregistrarea ambianței fizice și copierea probelor digitale folosind practici și proceduri comune și acceptate.

6. **Examinarea probelor** - examinarea în profunzime a probelor, în căutarea elementelor care sunt în legătură cu fapta penală investigată. Acest lucru presupune localizarea și identificarea probelor precum și documentarea fiecărui pas, în scopul facilitării analizei.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

MODEL DE BUNE PRACTICI ...

7. **Analiza probelor** - determinarea semnificației probelor și relevarea concluziilor cu privire la fapta investigată.

8. **Prezentarea probelor** - sintetizarea concluziilor și prezentarea lor într-un mod inteligibil pentru nespecialiști. Această sinteză trebuie susținută de o documentație tehnică detaliată.

9. **Restituirea probelor** - dacă este cazul, returnarea către proprietarii de drept a obiectelor reținute în timpul investigației. Dacă este cazul, determinarea, în funcție de prevederile legilor procedurale penale, confiscării obiectelor.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

CARACTERISTICI SPECIFICE

Investigarea criminalistică a sistemelor informatice trebuie să prezinte o serie de caracteristici specifice, necesare asigurării unui grad înalt de corectitudine a concluziilor rezultate.

1. autenticitate (dovada sursei de proveniență a probelor);
2. credibilitate (lipsa oricăror dubii asupra credibilității și solidității probelor);
3. completitudine (prelevarea tuturor probelor existente și integritatea acestora);
4. lipsa interferențelor și contaminării probelor ca rezultat al investigației sau al manipulării probelor după ridicarea acestora

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

CONDIȚII SPECIFICE

Investigația criminalistică presupune asigurarea elementelor necesare:

1. existența unor proceduri pre-definite pentru situațiile întâlnite în practică;
2. anticiparea posibilelor critici ale metodelor folosite, pe temeiul autenticității, credibilității, completitudinii și afectării probelor oferite;
3. posibilitatea repetării testelor realizate, cu obținerea unor rezultate identice;
4. anticiparea problemelor legate de admisibilitatea probelor;
5. acceptarea faptului că metodele de cercetare utilizate la un moment dat pot face subiectul unor modificării în viitor.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

PROBELE DIGITALE

Probele digitale sunt acele informații cu valoare doveditoare pentru organele de urmărire penală și pentru instanțele judecătorești, care sunt stocate, prelucrate sau transmise prin intermediul unui sistem informatic.

Ele sunt definite ca:

orice informație cu valoare probantă care este fie stocată, prelucrată sau transmisă într-un format digital.

Probele digitale cuprind probele informatice, probele audio digitale, video digitale, cele produse sau transmise prin telefoane mobile, faxuri digitale, etc.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

PROBE DIGITALE – PARTICULARITĂȚI

Probele digitale aparent nu sunt evidente, fiind conținute în echipamentele informatice ce le stochează. Sunt necesare echipamente de investigație și de aplicații specifice pentru a face ca aceste probe să fie disponibile, tangibile și utilizabile.

Probele digitale sunt foarte „fragile”, în sensul că pot fi modificate sau pot dispărea foarte ușor, prin metode care de multe ori sunt la îndemâna făptuitorilor. Din această cauză investigatorii trebuie să ia măsuri speciale de protecție pentru a strânge, păstra și examina aceste probe.

Păstrarea acestor tipuri de probe a devenit o preocupare crescândă a investigatorilor din întreaga lume.

Necesitatea uniformizării practicii în domeniu a dus la elaborarea de standarde cu privire la probele digitale.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

BUNE PRACTICI ÎN INVESTIGARE

Bunele practici internaționale în materia investigării infracțiunilor informatice.

Datorită avansului permanent al tehnicii de calcul, modul efectiv de realizare a investigațiilor informatice nu poate fi consemnat în actele normative.

Organizațiile răspunzătoare de aplicarea legii dezvoltă în mod continuu practici și proceduri de natură să ghideze modul în care se realizează investigațiile, la un anumit nivel al tehnicii.

Aspectele pot fi preluate din practica INTERPOL, sau ale autorităților din SUA, Marea Britanie etc., urmărind principiile investigațiilor și mai puțin tehnologii sau instrumente folosite la un moment dat.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

PRELEVAREA PROBELOR

La locul în care se află sistemele informatice investigate,

- investigatorii se vor asigura de accesul la acestea.
- atât accesul fizic,
- dar cât și informațional

Recomandarea Consiliului Europei (95) 13 menționează ca necesară includerea în legislațiile naționale penale a obligației de permite accesul la sistemele informatice, atât din partea celor care răspund de sistemele informatice, cât și a oricăror persoane ce au cunoștință de modul de funcționare a acestora. Pe lângă accesul fizic, aceste persoane au datoria de a furniza și informații referitoare la securitatea sistemului, informații care să permită investigatorilor accesul la datele stocate în sistemele informatice respective.

Înainte de a trece la examinarea sistemelor informatice, nu trebuie neglijate procedurile criminalistice tradiționale de analiză a spațiului percheziționat, cum ar fi prelevarea probelor fizice (amprente, alte urme materiale). De asemenea poate avea relevanță imaginea aflată pe ecranul monitorului în momentul pătrunderii organelor de cercetare penală. Aceasta poate fi păstrată prin fotografiere, filmare, etc.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ LOCUL INVESTIGĂRII

O primă decizie ce trebuie luată privește

- analiza sistemului informatic la fața locului,
- sau ridicarea acestuia și analiza în laborator.

În luarea acestei decizii, trebuie avute în vedere următoarele aspecte:

- calitatea superioară a analizei efectuate în condiții de laborator;
- măsura în care ridicarea sistemului informatic afectează activitatea suspectului.

În acest sens, trebuie reținute recomandările Camerei Internaționale de Comerț ce menționează regula evitării ridicării sistemelor informatice ale întreprinderilor, dacă aceasta ar duce la afectarea desfășurării activităților lor normale.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

CRITERII DE APRECIERE

Următoarele criterii sunt utile în aprecierea oportunității ridicării sistemelor informatice:

a. Criteriul volumului probelor.

Particularitatea sistemelor informatice de a permite stocarea unui volum foarte mare de informație într-un spațiu de dimensiuni fizice reduse face ca investigația să necesite un volum mare de timp pentru obținerea probelor relevante. Astfel, cercetări pe o perioadă de timp mare pot fi conduse mult mai eficient în laborator.

b. Criteriul dificultăților de natură tehnică.

1. problema evitării distrugerii datelor în decursul investigației. Analiza sistemelor informatice de către investigatori ce nu au cunoștințe suficiente asupra echipamentului sau programelor utilizate poate duce la distrugerea din greșeală a datelor.

2. problema reconstituirii sistemului în laborator. Datorită varietății foarte mari a componentelor tehnice ale calculatoarelor, pentru ca sistemul să poată funcționa corect în laborator, este necesară ridicarea tuturor echipamentelor prezente la locul percheziției. În cazul ridicării parțiale a componentelor sistemului, este posibilă prezența unor incompatibilități fie între echipamentele sistemului informatic ridicat și cele din laborator (de exemplu incompatibilitatea calculatorului cu echipamentele periferice - imprimante, etc.), fie între programele de pe sistemul ridicat și echipamentele din laborator.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

RIDICAREA SISTEMULUI INFORMATIC

O dată decisă ridicarea sistemului informatic aflat la locul percheziției, trebuie luate unele măsuri care să permită reconstituirea exactă a acestuia în laborator.

În primul rând, trebuie consemnat modul de aranjare în spațiu a echipamentelor sistemului informatic ridicat. Aceasta se poate face fie prin fotografierea sistemului din toate unghiurile, fie prin filmare video. În procesul de fotografiere sau filmare, este necesar să se insiste asupra cablajelor ce conectează diferitele componente ale echipamentului. Consemnarea, în variantă foto sau video, are relevanță și pentru a arăta starea în care se găsea echipamentul în momentul ridicării, prevenind astfel plângerile legate de o eventuală deteriorare a acestuia în decursul anchetei.

În procesul de ridicare a componentelor sistemului trebuie să fie avută în vedere necesitatea păstrării integrității și identității datelor. Orice avariere a suportului pe care se află datele duce în mod inevitabil la distrugerea acestora. Organele de cercetare penală trebuie instruite în mod special pentru a proteja probele de natură electronică.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

PROCEDURA RIDICĂRII .

Procedura ridicării sistemelor informatice este următoarea:

etapa 1 : închiderea sistemului (dacă a fost găsit închis, nu trebuie repornit)

- deconectarea de la alimentarea cu energie electrică (nu va produce, în cele mai multe cazuri, pierderea de date, dar poate evita ștergerea unor informații relevante, cum ar fi fișierele temporare);
- închiderea conform procedurii normale (de preferat atunci când calculatorul este conectat în rețea, sau atunci când investigatorul este asistat de o persoană ce are cunoștințe asupra modului de funcționare a sistemului respectiv, precum și asupra procedurilor ce sunt folosite pentru închiderea lui).

etapa a 2-a: etichetarea componentelor

- În cazul în care se impune dezasamblarea fiecare componentă a sistemului trebuie etichetată înainte de modificarea configurației în vederea ridicării probelor. În cazul cablurilor, se etichetează atât cablul, cât și suporturile de unde a fost debransat. În cazul existenței unor suporturi care nu au conectate cabluri, este recomandabil ca să fie etichetate "neocupat". Se poate realiza și o schiță a componentelor, cu precizarea simbolurilor folosite pentru etichetare.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

PROCEDURA RIDICĂRII ..

etapa a 3-a: protejarea la modificare

- Toate suporturile magnetice de stocare a datelor trebuie protejate împotriva modificării conținutului lor. Unele tipuri de hard-discuri sau stick-uri de memorie au contacte speciale care realizează protejarea la scriere.

etapa a 4-a: ridicarea propriu-zisă

- Ridicarea probelor trebuie făcută cu multă grijă, evitându-se orice avariere a componentelor. Este recomandabilă împachetarea componentelor în ambalajul original, dacă acesta poate fi găsit, sau în ambalaj special ce asigură protecția electrostatică a acestora. De asemenea, toate suporturile magnetice de stocare a datelor, vor fi ambalate și sigilate în așa fel încât accesul la ele nu este permis, până la desfacerea în laborator.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ SUSPECTUL

În timpul investigației, dacă suspectul este prezent, organul de urmărire penală trebuie să împiedice orice apropiere a acestuia de sistemul informatic. Mai ales dacă suspectul are pregătire superioară în domeniul informatic, acesta poate altera voit datele aflate pe calculatorul său, fără ca investigatorii să poată sesiza acest lucru. Calculatorul suspectului poate conține unele comenzi ce pot produce pierderea datelor, comenzi ce pot fi mascate sub numele unor comenzi uzuale ale sistemului de operare folosit.

Dacă suspectul insistă să ajute investigatorii în procesul de închidere a calculatorului sau a procesului de ridicare a componentelor sistemului, aceștia pot cere suspectului să le descrie operațiunile pe care acesta dorește să le execute, și chiar să le scrie pe hârtie. Investigatorii nu vor urma indicațiile suspectului, ci le vor remite experților ce efectuează analiza probelor. Aceștia vor putea fi avertizați în acest mod de eventualele capcane introduse de suspect

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

ROLUL ALTOR PERSOANE

De la persoanele prezente la percheziție, sau de la alte persoane care au cunoștință de modul de operare a sistemului informatic respectiv pot fi obținute informații importante. Fiecare martor trebuie interviuat asupra modului în care sunt folosite sistemele informatice ridicate. Sunt relevante modalitățile de introducere, sortare și stocare a datelor pe computer, precum și practicile referitoare la diverse aspecte legate de utilizarea lui curentă.

În cazurile în care se anchetează incidente legate de pătrunderea neautorizată în sisteme informatice ale unor firme/organizații, de cele mai multe ori specialiștii instituției-victimă sunt cele mai importante ajutoare ale investigatorilor.

Astfel investigatorii nu trebuie să folosească tehnici de pătrundere activă în sistem pentru prelevarea probelor, bucurându-se de sprijinul celor care administrează sistemul.

În unele situații speciale, calculatoarele altor persoane, situate la aceeași locație pot deține probe relevante. De exemplu, documente relevante pot fi găsite în calculatorul secretarelor persoanelor investigate.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

TRANSPORTAREA ÎN LABORATOR

Transportarea probelor reținute trebuie făcută cu multă grijă, având în vedere „fragilitatea” lor.

Este necesar să fie luate precauțiuni legate de protejarea față de șocuri fizice, umiditate, căldură și mai ales de influența undelor electromagnetice.

În legătură cu acest din urmă aspect trebuie evitată plasarea echipamentelor în apropierea surselor de radiații electromagnetice, cum ar fi aparate de fax, copiatoare, stații radio, telefoane celulare.

Este recomandabilă măsurarea cu instrumente speciale a câmpului electromagnetic în spațiile unde sunt depozitate echipamentele ridicate.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

ANALIZA PROBELOR

Odată aduse în laborator, componentele trebuie asamblate pentru a reconstitui sistemul original.

Pentru aceasta se vor folosi fotografiile sau casetele video filmate înainte de ridicarea probelor, respectându-se conexiunile originale, precum și informațiile obținute de la martori în legătură cu practicile de utilizare a sistemului informatic respectiv.

Primul pas în analiza probelor de natură electronică este legat de necesitatea asigurării veridicității lor. Pentru a putea dovedi veridicitatea probelor, este necesară ambalarea și sigilarea acestora în modul amintit mai sus .

Primul pas în asigurarea protecției împotriva modificării datelor din sistemele informatice trebuie făcut chiar în timpul percheziției, prin luarea măsurilor de protejare fizică la scriere a mediilor de stocare.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

ANALIZA CONȚINUTULUI

Se recomandă ca analiza criminalistică a conținutului discului să se realizeze pe o copie fidelă a discului original. Procedul nu presupune doar copierea tuturor fișierelor aflate pe disc, ci a întregului conținut al discului, sector cu sector, inclusiv fișierele temporare, fișierele de schimb, fișierele șterse, chiar informația aflată pe porțiunile avariate ale discului, etc.

O asemenea copie de această natură se realizează cu ajutorul unor programe speciale. Se recomandă realizarea a două copii, pe una dintre ele realizându-se analiza propriu-zisă, cealaltă fiind o copie de rezervă.

Copierea trebuie realizată după un procedeu demn de încredere. Pentru a putea avea această caracteristică, copierea trebuie:

- să asigure posibilitatea verificării de către terți; instanța de judecată sau partea adversă trebuie să poată să verifice acuratețea copiei realizate.
- să aibă ca rezultat copii sigure, ce nu pot fi falsificate.

Este recomandată consemnarea detaliată a întregului proces de copiere, indicând echipamentele, programele și mediile de stocare utilizate.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

PĂSTRAREA PROBELOR

Păstrarea în siguranță a probelor se realizează în primul rând prin copierea conținutului sistemelor informatice originale, și desfășurarea investigației criminalistice asupra unei copii de lucru, având aceleași caracteristici cu originalul.

Ca o metodă de siguranță în plus, se poate realiza autentificarea matematică a conținutului unui mediu de stocare, fie el hard-disc sau stick, mediu optic, etc.

Acest procedeu constă în realizarea prin procedee matematice a unei imagini a mediului de stocare respectiv, imagine ce poate servi ca referință în cazul în care este contestată integritatea acestuia. Autentificarea se realizează cu ajutorul unor programe speciale ce oferă un grad de siguranță ridicat.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

PREGĂTIREA ECHIPEI DE INVESTIGATORI

Natura infracțiunilor cere ca cercetarea penală să se realizeze în cadrul unei echipe de investigatori. Necesitatea investigației în echipă reiese din nevoia garantării unei obiectivități sporite și eficiente, derivată din conjugarea competențelor și specializărilor membrilor echipei.

Se apreciază că un bun investigator trebuie să posede:

1. cunoștințe suficiente asupra tehnicilor informatice, care să îi permită să înțeleagă filozofia funcționării unui sistem informatic, să analizeze documentația tehnică și să apeleze, dacă este nevoie, la tehnici informatice evolute care să-l ajute în atingerea scopului urmărit;
2. cunoștințe suficiente asupra tehnicilor utilizate de firme, în special asupra sistemelor contabile, pentru a putea înțelege caracteristicile sistemelor care ar putea face obiectul unor fraude, astfel încât să poată stabili atât modul de operare cât și să dirijeze investigația până acolo unde ar putea găsi probele delictului;
3. cunoștințe suficiente asupra tehnicilor de securitate internă, astfel încât investigația să poată fi efectuată cu rapiditate și să fie îndreptată în direcția justă.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

APTITUDINI

Pe lângă nivelul de cunoștințe al anchetatorilor sunt necesare și alte aptitudini ce trebuie să existe sau să fie dezvoltate în, pentru ca aceștia să poată conduce ancheta.

Astfel, putem aminti:

- personalitate extrovertită (datorită faptului că, în general, specialiștii în domeniile tehnice, și în special informatice, posedă mai puține abilități de comunicare inter-umană),
- înclinare spre detaliu (foarte importantă, mai ales având în vedere specificul probelor electronice: abundența informațiilor aflate pe un spațiu de stocare de dimensiuni fizice reduse; cu toate acestea, este importantă păstrarea unei viziuni de ansamblu asupra anchetei),
- gândire logică, comunicare bună (importantă mai ales pentru a asigura prezentarea rezultatelor investigației într-un mod relevant, atât în scris, cât și în fața instanței),
- obiectivitate.

PRACTICI ÎN INVESTIGAȚIA INFORMATICĂ

INSTRUMENTE

Instrumente necesare investigației (echipamente și programe pentru calculator)

Investigarea criminalistică a sistemelor informatice necesită utilizarea unor instrumente specifice. Ca echipamente, echipa de investigatori trebuie să dispună de medii de stocare a datelor, în cantitate suficientă, și de calitate superioară, pentru a permite copierea acestora de pe sistemul informatic analizat.

În analiza sistemelor informatice este folosit un număr semnificativ de programe de calculator. Cu titlu de exemplu se pot menționa programe pentru copierea exactă a conținutului memoriei fizice, pentru analiza și compararea fișierelor, pentru catalogarea conținutului discului, pentru validarea și autentificarea matematică a datelor, pentru recuperarea fișierelor șterse, programe de decriptare sau programe antivirus.

Este necesar ca programele de calculator folosite de organele de urmărire penală să fie înregistrate din punct de vedere al protecției drepturilor de autor aparținând producătorilor acestor programe.