# Dovezile în format electronic de la punerea sub sechestru până la etapa procesuală

Nigel Jones

Director al Centrului pentru Criminalistică Cibernetică

Universitarea Canterbury Christ Church

Regatul Unit

*Proiect sprijinit prin intermediul unei finanțări norvegiene*

# Agenda

- Considerații legate de dovezile în format electronic
  - Cum verific dacă dovezile sunt autentice
  - Ce procese se aplică
  - Ce trebuie să demonstrez
  - Ce verificări pot face
- Bune practici
  - Cum pot fi de ajutor ghidurile

# Probele în format electronic - o definiție

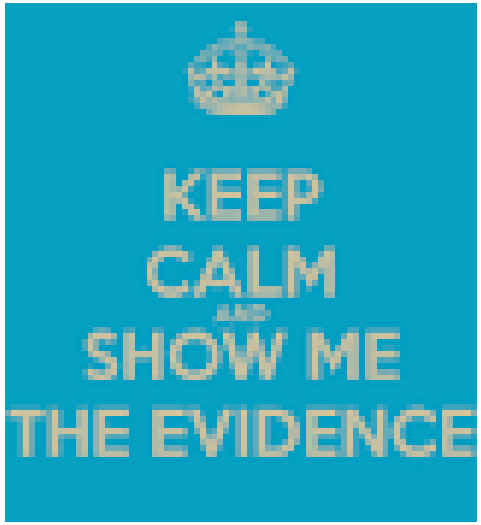
Probele în format digital sau electronic reprezintă materialul probatoriu stocat sau transmis într-o formă digitală pe care o parte într-un proces o poate folosi în instanță. Înainte de a accepta probele în format digital, instanța va stabili dacă acestea sunt relevante, dacă sunt autentice, dacă reprezintă dovezi indirecte și dacă sunt acceptabile copiile sau dacă este necesară solicitarea unui original.

Casey, Eoghan (2004) Digital Evidence and Computer Crime (Probele în format digital și infracțiunile informatice), ediția a doua

# Ce sunt dovezile în format electronic?

- Dovezile în format electronic nu sunt diferite față de probele tradiționale în sensul că partea care le introduce pe rolul instanței trebuie să fie capabilă să demonstreze că ele nu sunt cu nimic modificate față de momentul la care au intrat în posesia sa. Cu alte cuvinte, nu au avut loc niciun fel de modificări, ștergeri, adăugiri sau orice alte alterări ale acestora.

# Este mesajul de mai jos autentic?



Sent on 11th September 2015
From: 00007@hushmail.com
To: hitechproducts@gmail.com

**Subject:** This is an offer your should not refuse

**Text:** Good day Hitech Products. I am a security specialist who would like to make you an offer that you really should not refuse. You have a very good business that relies on the Internet for selling your products. I would like to offer you the opportunity to accept my services in preventing any attacks on your system that may affect your business. The cost for this service is a one off payment of €100,000.

Please do not ignore this offer, as I would not like to see any damage caused to your business. This is a once only offer that explores at midnight on Sunday 20th September.

To accept this offer, please reply to this email address by the deadline and I will send instructions regarding the payment.

Thank you for allowing me to offer this service

007 Security Services


Caracteristici
unice

# Caracteristici unice

Dovezile în format electronic au trăsături în mare parte comune cu formele tradiționale de probe, însă posedă câteva caracteristici unice care le fac speciale:

- **Sunt invizibile pentru ochii nespecialiștilor:** Probele electronice se regăsesc adesea în locuri în care numai specialiștii s-ar gândi să caute sau în locații care sunt accesibile numai prin intermediul unor instrumente foarte specifice. Așa cum scanarea cu ajutorul unui microscop electronic permite unui entomolog să identifice trăsăturile morfologice esenț muscă, există în criminalistica ciber specifice care permit examinarea și care se găsesc în computere.

# Caracteristici unice

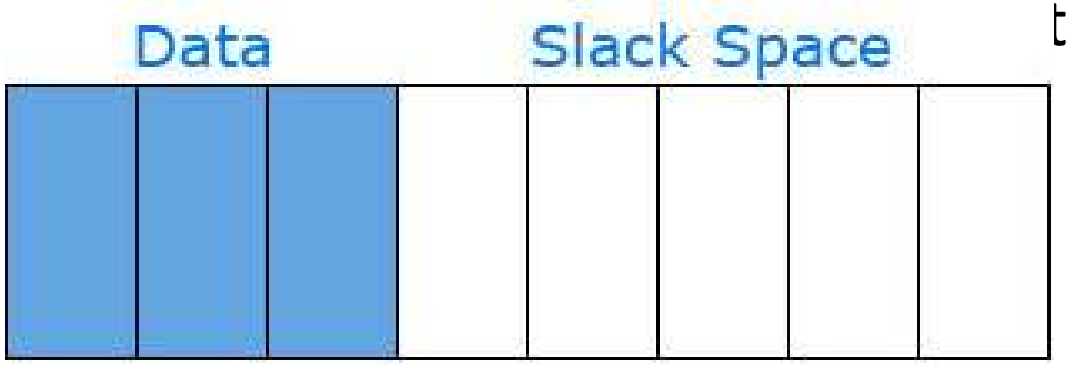
- Uneori trebuie interpretate de către un specialist: Informațiile culese din computere sunt de puțin ajutor unui nespecialist atât timp cât acesta nu are capacitatea de a extrage proprietățile sau dovezile asociate care dea asigurarea autenticității informațiilor relevante și a faptului ca acestea nu au fost manipulate sau alterate. În unele cazuri, exact ca și exemplul analizei tiparului de împroșcare cu sânge din criminalistică, trebuie aplicate cunoștințe de lizare.

# Caracteristici unice

- **Sunt caracterizate de o volatilitate ridicată:** Câteodată, dovezile în format electronic se regăsesc pe dispozitive la care starea curentă (0 sau 1 per bit) a memoriei lor poate fi suprascrisă de fiecare dată când are loc un eveniment specific. În unele cazuri, acest lucru poate fi constituit de o cădere de tensiune, în alte cazuri, se poate întâmpla ca un sistem automatizat să suprascrie informațiile mai vechi pentru a lăsa loc informațiilor noi. Dispozitivele
  regăsi probe digitale trebuie s
  cât de repede posibil.

# Caracteristici unice

- **Pot fi alterate sau distruse printr-o utilizare normală:** Dispozitivele își modifică în permanență starea memoriei, fie la cererea utilizatorului („salvează documentul”, „copiază fișierul”) sau în mod automat la solicitarea sistemului de operare a computerului respectiv („alocă spațiu pentru acest program”, „stochează temporar informații pentru a fi transmise ulterior între dispozitive”). Această caracertistică subliniază importanța tratării dovezilor în format electronic de o manieră corespunzătoare de la tificate ca fiind relevante



# Caracteristici unice

- **Poate fi copiată fără limitări:** informația în format digital poate fi copiată la infinit și fiecare copie va reprezenta o reproducere perfectă a originalului. Acest atribut unic permite ca mai multe copii perfecte ale originalului să fie distribuite și analizate de către mai mulți specialiști în același timp. De asemenea, acest lucru permite ca dovezile în format electronic să fie prezentate ca atare în instanță, însoțite de un ra
partea unui specialist.


Considerații

# Considerații legate de dovezile în format electronic

- **Manipularea de către specialiști:** Fiecare dispozitiv electronic are caracteristici specifice, așa încât trebuie urmate proceduri stricte pentru a le accesa memoria în care s-ar putea regăsi aceste probe în format electronic. În cazul probelor în format electronic, unul dintre riscurile majore este reprezentat de modificarea neintenționată a unei părți a probelor. Această eventualitate ar putea genera dubii cu privire la schimbările specifice intervenite, precum și în legătură cu posibilitatea ca dovezi de natură a incrimina sau exonera autorul s ceea ce ridică subsecvent admisibilitate în instanță.

# Considerații legate de dovezile în format electronic

- **Evoluția rapidă a surselor de dovezi în format electronic:** Noile tehnologii se dezvoltă foarte rapid și este necesară punerea la punct nu numai cu noile tehnologii în sine, dar și actualizarea procedurilor și tehnicilor care trebuie aplicate pentru a le putea sechestra conținutul și analiza.

# Considerații legate de dovezile în format electronic

- **Utilizarea de proceduri, tehnici și instrumente adecvate:** Ca și în cazul disciplinelor criminalistice mai tradiționale, specialiștii în criminalistică cibernetică au nevoie, pe lângă cunoștințele specializate, de instrumente specializate pentru a-și duce în mod adecvat la îndeplinire misiunea, precum cea de capturare a tuturor informațiilor originale de pe un dispozitiv. Este imperativă folosirea de tehnici și instrumente adecvate și este obligatoriu ca procedurile să fie trasabilitate și repetabilitate de către a încît informația astfel capturată probatorie.

# Considerații legate de dovezile în format electronic

- **Admisibilitatea:** Din moment ce scopul ultim îl reprezintă utilizarea dovezilor acumulate și analizate pentru a veni în sprijinul unei cauze înfățișate în instanță, dovezile în format electronic trebuie să fie obținute în conformitate cu legislația în vigoare și cu procedurile de bună practică astfel încît să fie admisibile în instanță. Cu toate că diferă condițiile concrete de la o legisl
  la alta, următoarele criterii de
  luate în considerare.

# Considerații legate de dovezile în format electronic

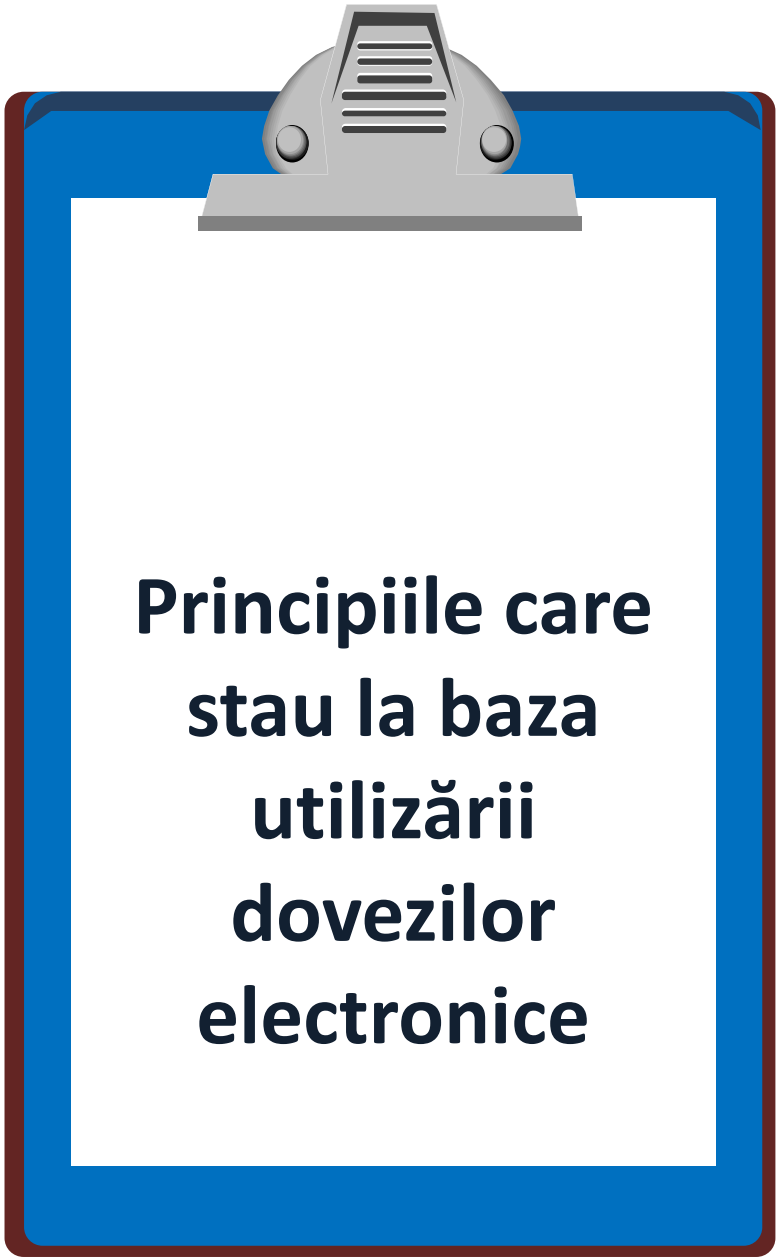
- **Autenticitate:** Trebuie să existe posibilitatea de a face o legătură pozitivă între materialul probatoriu și incidentul investigat.
- **Caracter complet:** Trebuie să constituie o imagine completă, nu doar o perspectivă specifică
- **Demne de încredere:** Trebuie să nu persiste nimic în legătură cu modul de strângere și manipulare ulterioară a probelor care să unce vre îndoială autenticității cestora.

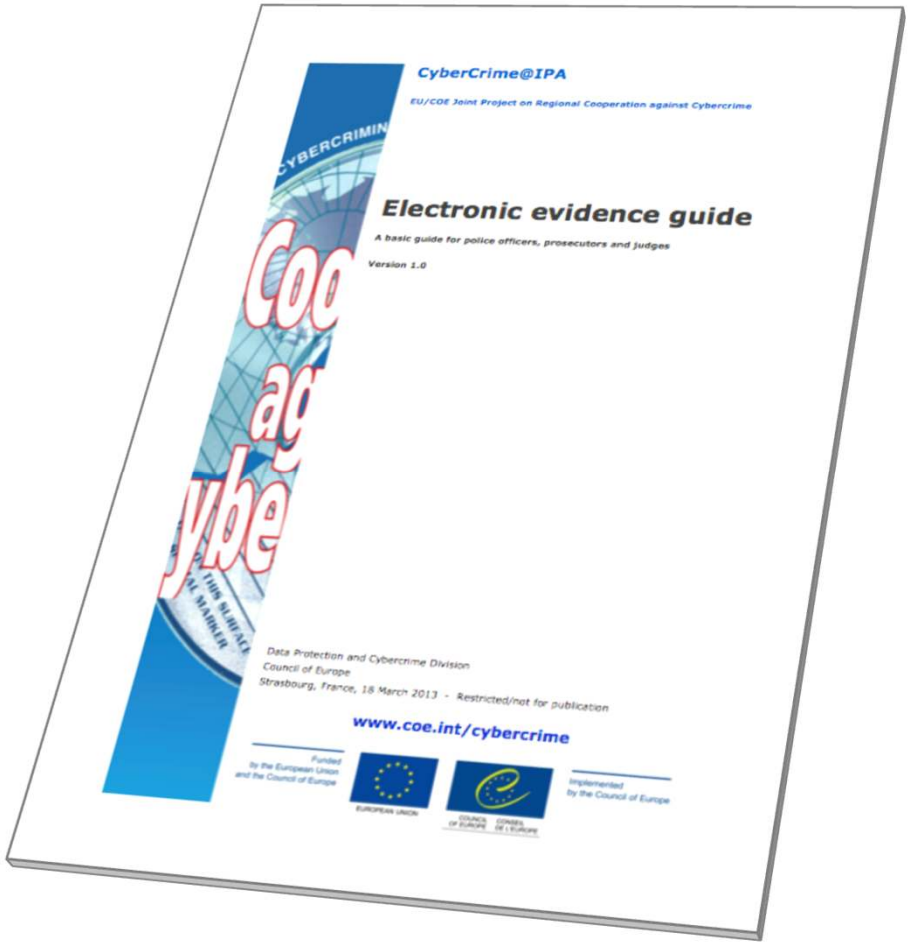


# Considerații legate de dovezile în format electronic

- **Credibilitate:** Trebuie să fie ușor de crezut și înțeles pentru un judecător și/sau jurați.
- **Proporționalitate:** aplicarea acestui principiu în criminalistica cibernetică necesită ca întreg proces de investigație să fi fost adecvat și corespunzător: beneficiile acumulate de pe urma utilizării unei măsuri specifice trebuie să depășească pagubele provocate părții sau părților afectate de măsura respectivă.

BELIEVABILITY MATTERS


Principiile care stau la baza utilizării dovezilor electronice

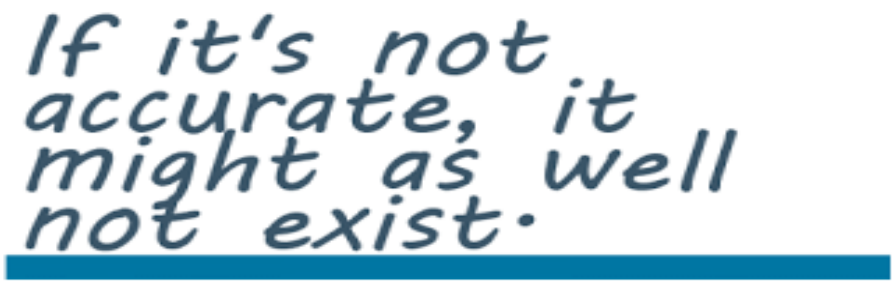



# Ghidul Consiliului Europei privind folosirea dovezilor în for electronic

# Principiul 1 - integritatea datelor

Nu poate fi întreprinsă nicio acțiune care să aducă modificări dispozitivelor sau mediilor de stocare electronice, care urmează să fie prezentate ulterior în instanță.

- Atunci cînd sunt manipulate dispozitivele și datele electronice, acestea trebuie să nu sufere modificări, nici din punctul de vedere al hardware-ului, nici al software-ului. Persoana care a primit această sarcină este responsabilă de integritatea materialelor recuperate de la fața locului și, este prin urmare, responsabilă pentru demararea procedurii de luare în custodie în scop criminalistic.
- Pot apărea circumstanțe care să impună luarea deciziei de a accesa datele de pe un sistem informatic „în direct” pentru a evita pierderea unor potențiale probe. Această acțiune trebuie întreprinsă de o manierp care să producă un impact minim asup
persoană calificată în acest sens. Pri
luate în considerare dacă se consider



# Principiul 2 - Pista de audit

- trebuie creată și păstrată corespunzător o pistă de audit sau orice altă formă de înregistrare a tuturor acțiunilor întreprinse la momentul manipulării dovezilor în format electronice. O terță parte trebuie să poată examina toate aceste acțiuni întreprinse și să poată ajunge la același rezultat.
- Este imperativă înregistrarea cu acuratețe a tuturor activităților pentru a permite unei terțe părți să refacă acțiunile întreprinse „la prima mână” pentru a putea asigura valoarea probatorie în instanță. Toate activitățile referitoare la punerea sub sechestru, transferul dovezilor în format electr deplin documentate, păstrate și moment pentru verificare.

# Principiul 3 - Sprijinul oferit de specialiști

- Dacă, pe parcursul unei operațiuni, se preconizează că vor fi găsite dovezi în format electronic, responsabilul de operațiune trebuie să informeze în timp util specialiștii/consultanții externi.
- Pentru investigațiile care presupun percheziția informatică și punerea sub sechestru de probe în format electronic, poate fi necesară consultarea unor specialiști externi. Toți specialiștii externi trebuie să fie familiarizați cu principiile prezentate în acest document sau în documente similare relevante. Un specialist trebuie să dețină la un nivel corespunzător:
  - expertiză și experiență specializată în domeniu,
  - cunoștințe în domeniul realizării de investigații
  - cunoștințe legate direct de problema investigată
  - cunoștințe juridice,
  - abilități de comunicare (atât pentru explicațiile verbale, cât și pentru cele oferite în scris).
  - Abilități de folosire a limbilor străine.

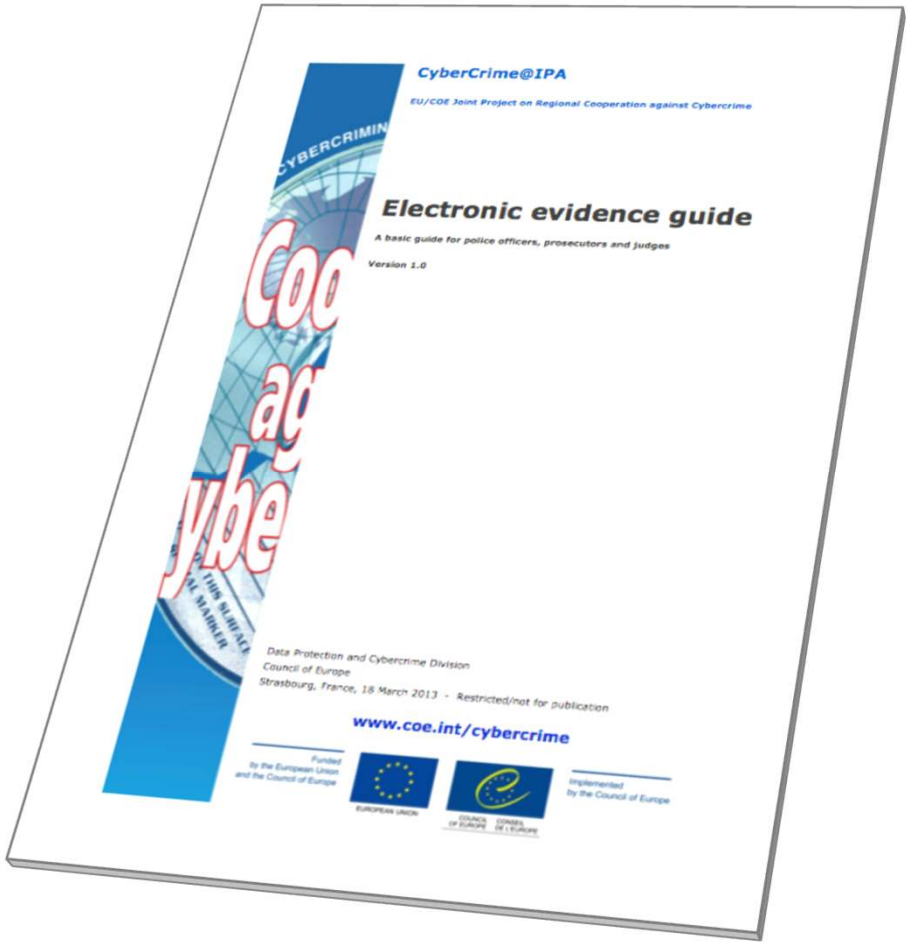
# Principiul 4 - Pregătirea corespunzătoare

- Primele persoane care intră în contact cu datele respective trebuie să fie pregătite în mod corespunzător din punct de vedere profesional pentru a efectua percheziția informatică și pentru a pune sub sechestru probele electronice dacă nu sunt disponibili experți la fața locului.
- În circumstanțe excepționale în care este necesar ca prima persoană aflată la fața locului să colecteze ea însăți probele electronice și/sau să acceseze date originale stocate pentru un dispozitiv electronic sau un m
digitală, această persoană trebu
să realizeze în mod adecvat acea
trebuie să i se explice relevanț
acțiunilor sale

# Principiul 5 - Legalitatea

- Persoana și organismul responsabil de cauza penală respectivă sunt direct răspunzători de respectarea dispozițiilor legale, a principiilor criminalistice generale și a celor procedurale, precum și a principiilor prezentate mai sus. Aceste reguli se aplică posesiei de și accesului la probe electronice.
- Fiecare Stat Membru trebuie să ia în considerare propriile prevederi și norme juridice atunci când interpretează măsurile propuse în document.


Ghidul privind
bunele practici




# Ghidul Consiliului Europei privind probele electronice

# Contextul elaborării ghidului

## Autori:

Nigel Jones (Marea Britanie)

Esther George (Marea Britanie)

Fredesvinda Insa Mérida (Spania)

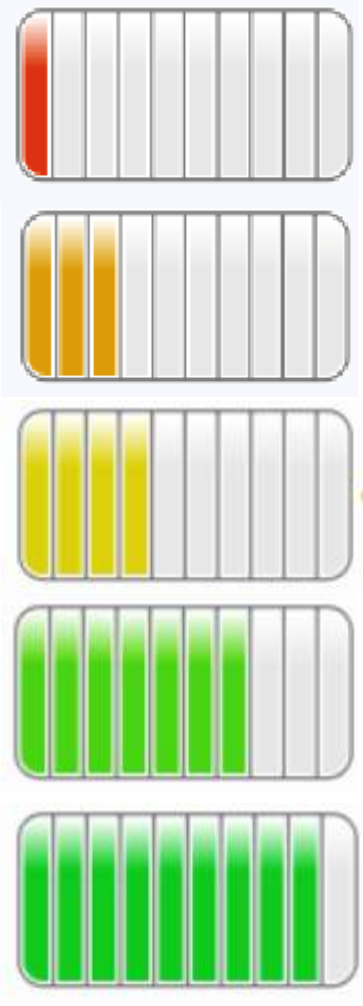
Uwe Rasmussen (Danemarca)

Victor Völzow (Germania)

# Contextul elaborării ghidului

- **Nevoia:** Cererile formulate de participanții la numeroasele activități organizate în cadrul diferitelor proiecte de combatere a criminalității cibernetice ale Consiliului Europei, incluzând proiecte comune cu Uniunea Europeană au subliniat nevoia unui nivel superior de îndrumare pentru tratarea probelor electronice.
- Proiectul Cybercrime@IPA organizat în cooperare cu proiectul global privind criminalitatea informatică vine în sprijinul actualizării în permanență a unui document de îndrumare pe tema dovezilor în format electronic.
- Acesta oferă un instrument important pentru organismele de aplicare a legii și pentru sistemul judecătoresc în eforturile acestira
  urmări penal și judeca criminalitat

# Progresul înregistrat până în prezent



- Prima reuniune din februarie 2012 a stabilit structura ghidului și modul de repartizare a sarcinilor de lucru.
- Capitolele au fost elaborate între lunile februarie și mai 2012 și au fost însoțite de comentarii din partea echipei de redactare
- Cea de-a doua reuniune din mai 2012 a finalizat versiunea preliminară care a fost supusă revizuirii de către experți specializați pe domenii
- Întâlnirea de revizuire s-a desfășurat în cadrul Conferinței Octopus din data de 7 iunie 2012
- Modificările aduse ghidului s-au bazat pe reacțiile din partea experților
- Februarie 2013: Publicarea ghidului de către Consiliul Europei
- Întâlnire de revizuire desfășurată în cadrul Conferinței Octopus între 3-6 decembrie 2013
- 2014: Revizuiri și adăugiri la capitolele „Capturarea probelor din Internet” și „Analizarea dovezilor”

# Scopul ghidului:

- **Scopul:** de a oferi sprijin și îndrumare în identificarea, manipularea și examinarea dovezilor în format electronic.
- Nu se intenționează ca acest ghid să constituie un manual care să ofere instrucțiuni pas cu pas legate de modul în care pot fi tratate probele electronice pe durata tuturor etapelor unei urmăriri penale.
- Este, în primul rând, un document de nivel primar; există și că
  mai detaliate care oferă
  practice pentru specialiști.

# Cum ar trebui utilizat acest ghid

- Acest ghid este defaclact în secțiuni cronologice care au menirea de a oferi sprijin oricărei persoane care are de a face cu dovezi în format electronic.
- Aceste secțiui acoperă toate etapele de la identificarea inițială a surselor de potențiale probe, până la efectuarea percheziției informatice și la punerea sub sechestru a datelor incluzând capturile de date provenite din Internet, continuînd până la analiza, pregătirea și efectuarea raportului de expertiză asupra probelor.
- Aceste secțiuni sunt urmate de capitole specializate pentru organele politienesti, procuratură, judecători, pre
  investigatorii din sectorul p
  notari și grefieri.

# Simboluri utilizate în document

Informație

Informație
importantă

Informație specializată
de natură tehnică

Cunoștințe
de bază

Cunoștințe
de nivel avansat

Cunoștințe
specializate

# Structura și conținutul ghidului

1. **Introducere**
2. **Izvoarele probelor**
3. **Efectuarea percheziției și punerea sub sechestru într-o locație/asupra suspectului** incluzând Dead Box și Live Data Forensics
4. Capturarea datelor folosind Internetul incluzând sursele online, investigația online desfășurată sub acoperire, DarkNet
5. **Datele deținute de terți**
6. **Analizarea probelor**
7. **Pregătirea și prezentarea dovezilor**

# Structura și conținutul ghidului

**8. Competența de jurisdicție**

**9. Considerații specifice rolului jucat de fiecare instituție**

- 9.1. Organele polițienești
- 9.2. Procurorii
- 9.3. Judecătorii
- 9.4. Sectorul privat

**10. Studii de caz**

**11. Glosar**

**12. Considerații suplimentare**

**13. Anexe**

# Anexe

Anexa A - Diagrama privind efectuarea de percheziții și punerea sub sechestru de către organele polițienești

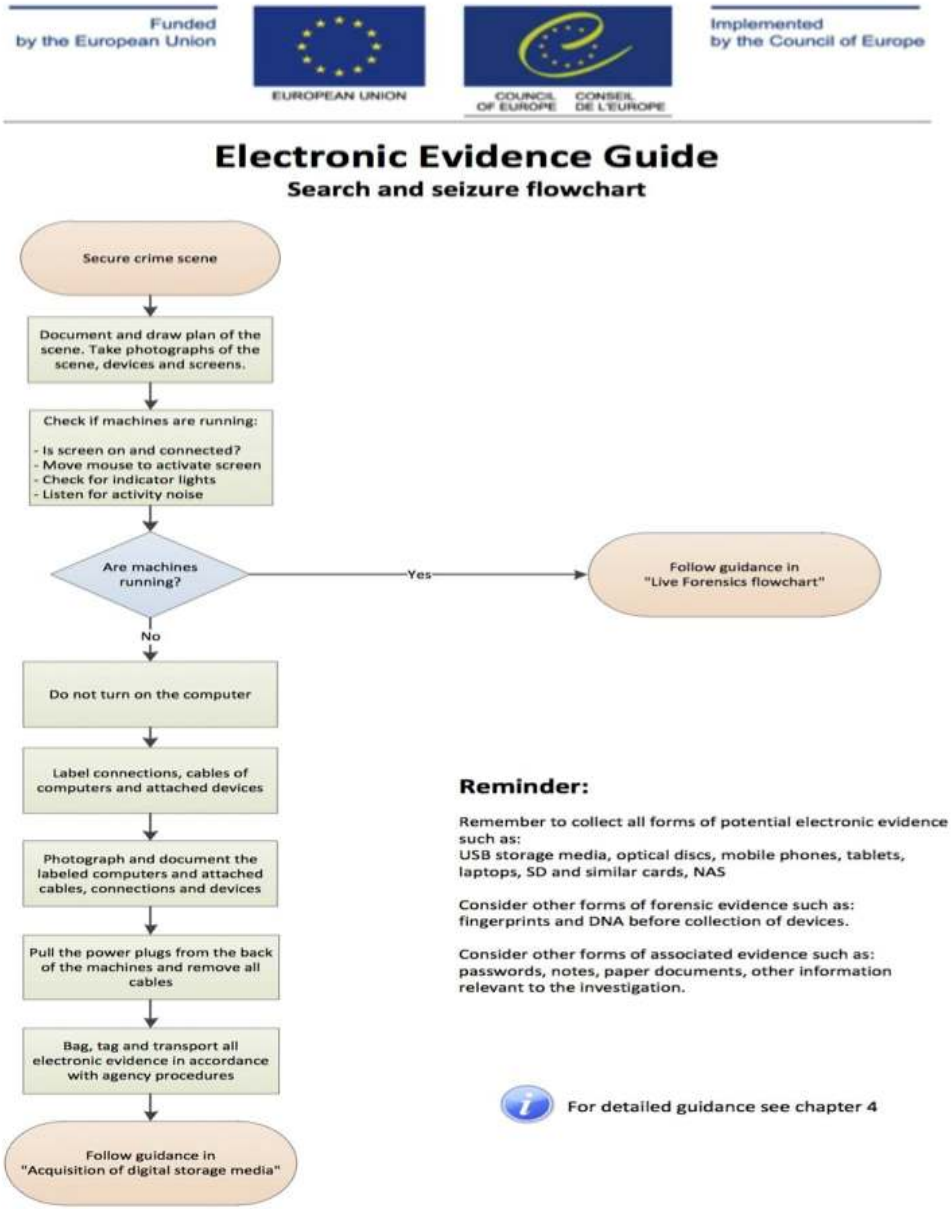
Anexa B - Diagrama criminalistică

Anexa C - Diagrama privind pregătirile în sectorul privat

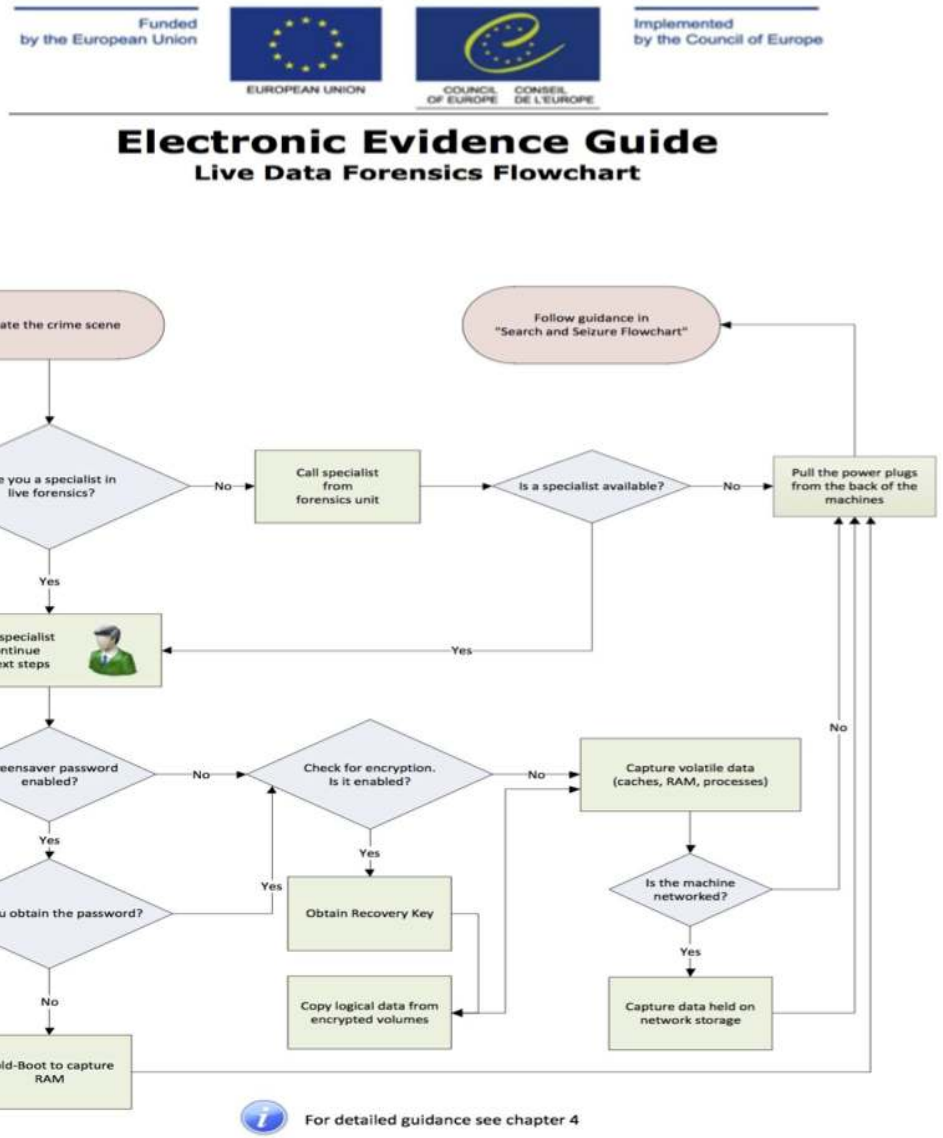
Anexa D - Diagrama privind percheziționile și punerea sub sechestru în sectorul privat

Anexa E - Diagrama privind achiziția d
format digital

# Anexe


Funded by the European Union
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe
Electronic Evidence Guide
Search and seizure flowchart
Secure crime scene
Document and draw plan of the scene. Take photographs of the scene, devices and screens.
Check if machines are running:
- Is screen on and connected?
- Move mouse to activate screen
- Check for indicator lights
- Listen for activity noise
Are machines running?
Yes
Follow guidance in "Live Forensics flowchart"
No
Do not turn on the computer
Label connections, cables of computers and attached devices
Photograph and document the labeled computers and attached cables, connections and devices
Pull the power plugs from the back of the machines and remove all cables
Bag, tag and transport all electronic evidence in accordance with agency procedures
Follow guidance in "Acquisition of digital storage media"
Reminder:
Remember to collect all forms of potential electronic evidence such as:
USB storage media, optical discs, mobile phones, tablets, laptops, SD and similar cards, NAS
Consider other forms of forensic evidence such as: fingerprints and DNA before collection of devices.
Consider other forms of associated evidence such as: passwords, notes, paper documents, other information relevant to the investigation.
For detailed guidance see chapter 4

# Anexe


Funded by the European Union
EUROPEAN UNION
COUNCIL OF EUROPE CONSEIL DE L'EUROPE
Implemented by the Council of Europe
Electronic Evidence Guide
Live Data Forensics Flowchart
Isolate the crime scene
Follow guidance in "Search and Seizure Flowchart"
Are you a specialist in live forensics?
No
Call specialist from forensics unit
Is a specialist available?
No
Pull the power plugs from the back of the machines
Yes
Only a specialist may continue with next steps
Yes
Screensaver password enabled?
No
Check for encryption. Is it enabled?
No
Capture volatile data (caches, RAM, processes)
No
Yes
Yes
Yes
Can you obtain the password?
Obtain Recovery Key
Is the machine networked?
Yes
No
Copy logical data from encrypted volumes
Capture data held on network storage
Cold-Boot to capture RAM
For detailed guidance see chapter 4

# Anexe

Funded by the European Union

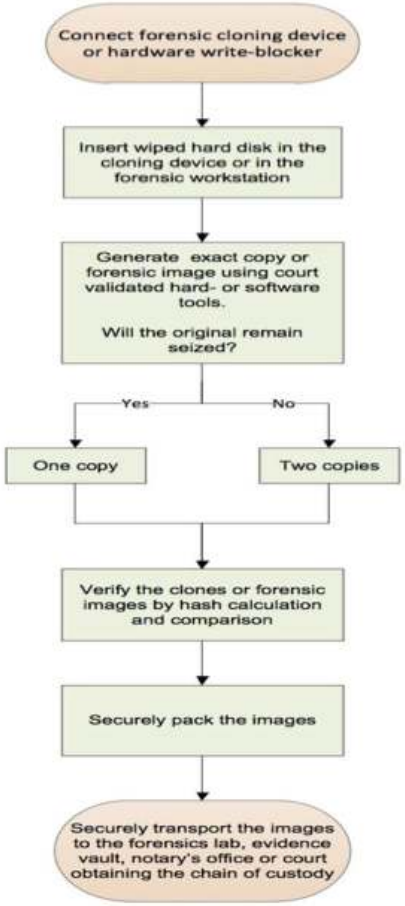
EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

## Electronic Evidence Guide

### Acquisition of digital evidence flowchart



# Anexe


**Electronic Evidence Guide**

**CHAIN OF CUSTODY RECORD**

**Case Reference** .....

**Book** ..... **of** .....

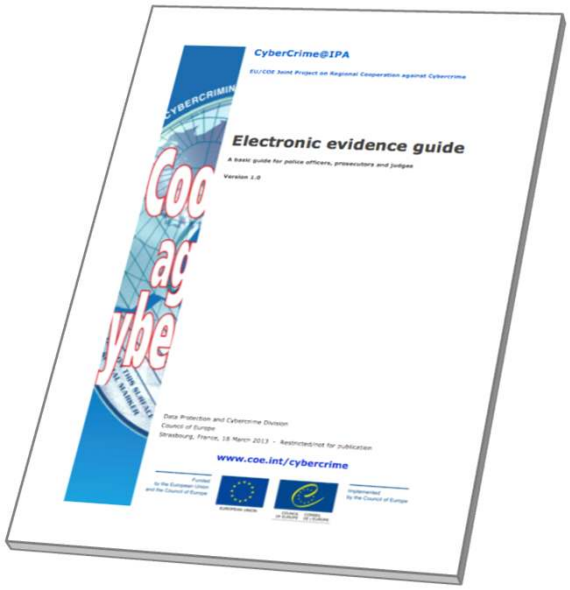
*Council of Europe Chain of Custody Record – V 1.0 28/5/12*

# Cui i se adresează ghidul?

- Ghidul a fost redactat pentru a fi utilizat de către acele țări care sunt în procesul de pregătire a modului de reacție în fața criminalității informatice și de stabilire a regulilor și protocoalelor de tratare a probelor electronice.
- Majoritatea ghidurilor existente în materie au fost create pentru comunitatea organismelor de aplicare a legii. Acest ghid se adresează unui public mai larg, care include judecători, procurori și alte părți ale sistemului de justiție, precum investigatorii din sectorul privat, avocații, notarii și grefierii

# Disponibilitatea Ghidului privind probele

## Este disponibil la adresa




## www.coe.int/cybercrime

# Valabilitatea ghidului

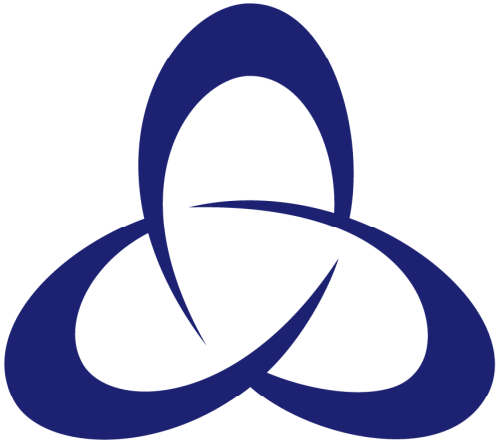
- Acest ghid și informațiile conținute sunt considerate a fi valabile până la data de 31 decembrie 2015.
- Se intenționează actualizarea ghidului înainte de această dată pentru a ține cont de orice schimbări relevante intervenite în tehnologie, proceduri și practici care sunt relevante pentru conținutul acestui ghid.
- Orice persoană sau instituție care dorește să utilizeze ghidul după data precizată mai sus contacteze Consiliul Europei pentru a i dispoziție ultime versiune.

CONTENT VALIDITY

# Convenția de la Budapesta

Convenția de la Budapesta oferă multe prevederi care au menirea de a îmbunătăți calitatea investigațiilor care presupun dovezi în format electronic. Unele dintre acestea sunt menționate în ghid; cu toate acestea, acest document nu reprezintă un ghid al Convenției iar utilizatorul trebuie să consulte documentele oficiale care sunt puse la dispoziție de Consiliul Europei în cazul în care dorește să facă uz de aceste pre

# Întrebări?



Canterbury Christ Church University

Nigel Jones

Director al Centrului pentru Criminalistică Cibernetică

Universitarea Canterbury Christ Church

Regatul Unit

nigel.jones@canterbury.ac.u