Electronic Evidence From Seizure to Trial

Nigel Jones
Director of the Centre for Cyberforensics
Canterbury Christ Church University
United Kingdom

Project supported by a grant from Norway

Agenda

- Considerations for electronic evidence
  - How do I know if the evidence is genuine
  - What processes have been applied,
  - What do I need to show
  - What checks can I make
- Good Practice
  - How can guidelines help

Electronic Evidence – A Definition

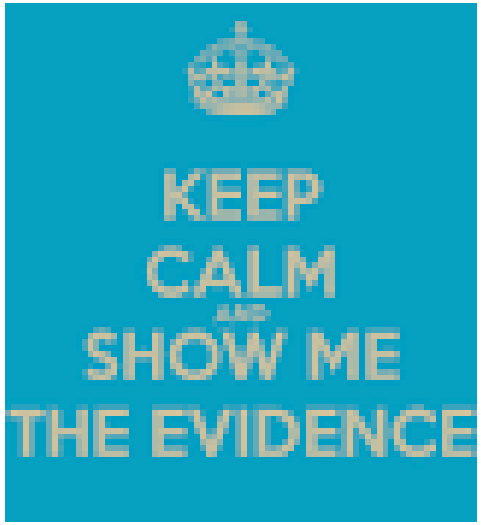
Digital or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence as court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.

Casey, Eoghan (2004) Digital Evidence and Computer Crime, Second Edition

What is Electronic Evidence?

- Electronic evidence is no different from traditional evidence in that is necessary for the party introducing it into legal proceedings, to be able to demonstrate that it is no more and no less than it was, when it came into their possession. In other words, no changes, deletions, additions or other alterations have taken place.

Is the Following Message Genuine?



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


Unique
Characteristics

Unique characteristics

Electronic evidence shares most properties with traditional forms of evidence, but possesses some unique characteristics that distinguish it:

- **It's invisible to the untrained eye**: Electronic evidence is often found in places where only specialists would search or locations reachable only by means of very specific tools. Just as a scanning electron microscope allows an entomologist to identify key morphologic features of fly eggs, specific tools exist in digital forensics to examine and analyse data found in computers.

Unique characteristics

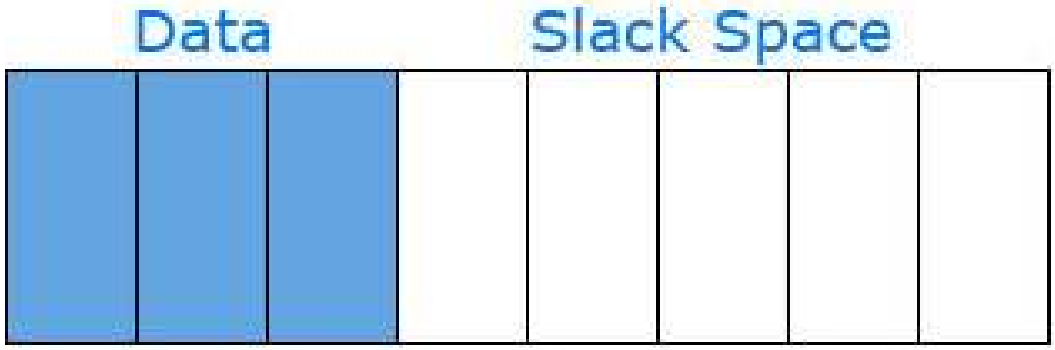
- **It may need to be interpreted by an specialist**: Information found on computers is of little use to a non-specialist as he will not be able to extract the properties or the related evidence that assures that the relevant information is truthful and has not been manipulated or tampered with. In some cases, just as in blood spatter pattern analysis, highly specialised knowledge must be applied.

Unique characteristics

- **It is highly volatile**: Sometimes, electronic evidence is found on devices in which the state (0 or 1 per bit) of their memory gets overwritten every time a specific event happens. In some cases it might be the loss of power, in other cases it could be that an automated system overwrites old information in order to leave spaces to store new information. Devices on which electronic evidence might reside must be preserved as soon as possible.

Unique characteristics

- **It may be altered or destroyed through normal use**: Devices constantly change the state of their memories, be it on user request (“save this document”, “copy this file”) or automatically by the computer operating system (“allocate space for this program”, “temporarily store information to swap it between devices”). This characteristic highlights the importance of handling the electronic device in an appropriate way from the moment it is identified as relevant for an investigation.



Unique characteristics

- **It can be copied without limits**: digital information can be copied indefinitely and each copy will be exactly like the original. This unique attribute allows multiple, exact copies of the original to be distributed and analysed by different specialists at the same time. It also allows electronic evidence to be presented as-is in a court along with the specialist witness report.


Considerations

Considerations for Electronic Evidence

- **Handling by specialists**: Each electronic device has specific characteristics, so specific procedures must be strictly followed to access its memory where electronic evidence could be stored. In the case of electronic evidence, one of the most prominent risks is the unintentional modification of part of the evidence. This could raise doubts about the specific changes, and whether the incriminating or exonerating evidence has been tampered with, which could in turn raise admissibility problems in Court.

Considerations for Electronic Evidence

- **Rapid evolution of electronic evidence sources:** New technologies develop very quickly and there is a need for constant update not only of the new technologies themselves but also of the procedures and techniques that have to be applied in order to seize their content and analyse it.

Considerations for Electronic Evidence

- **Use of proper procedures, techniques and tools**: As in more traditional forensic disciplines, digital forensic specialists require, besides the specialist knowledge, specific tools to undertake their job properly, such as to capture all original information from advice. It is imperative that adequate techniques and tools are used, and that procedures are traceable and repeatable by other specialists, so that the captured information is of evidentiary value.

Considerations for Electronic Evidence

- **Admissibility**: Since the ultimate goal is the use of acquired and analysed evidence to support a case in court, electronic evidence must be obtained in compliance with existing legislation and best practice procedure to be admissible in a trial. Although the details differ depending on national legislation, the following basic criteria must generally be taken into account.

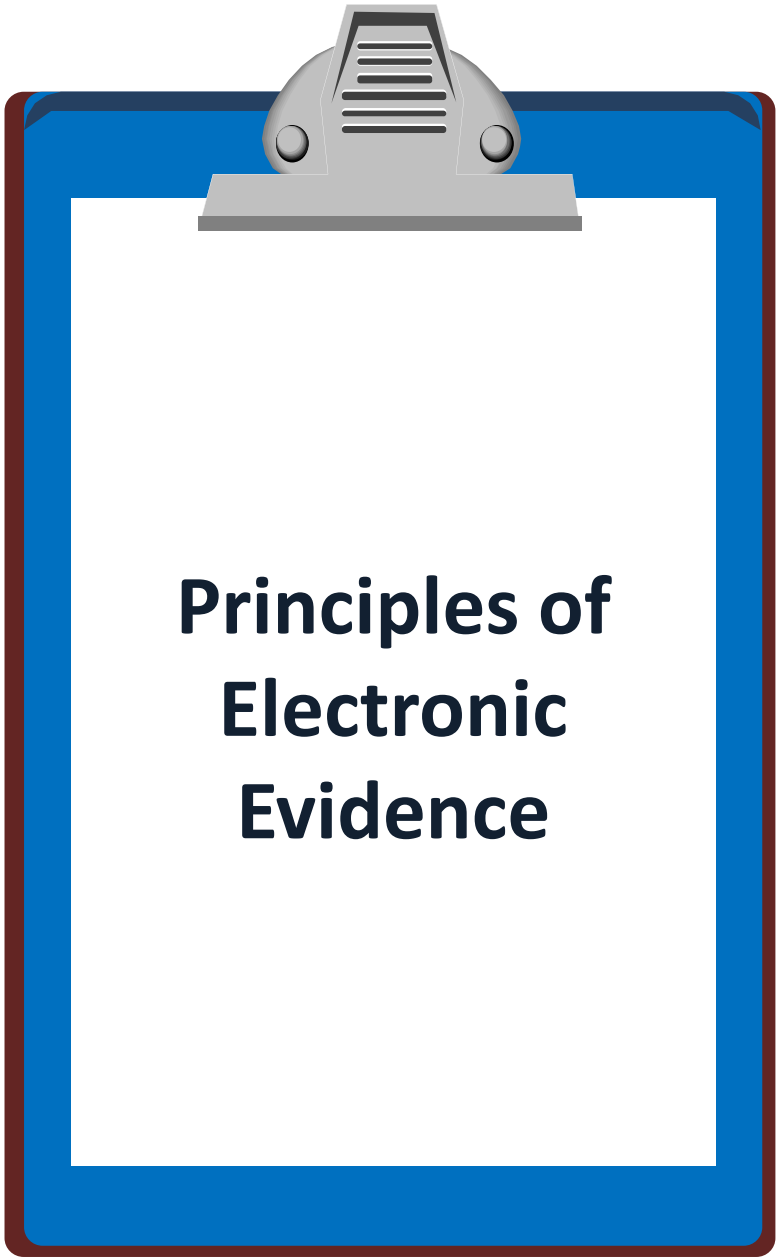
Considerations for Electronic Evidence

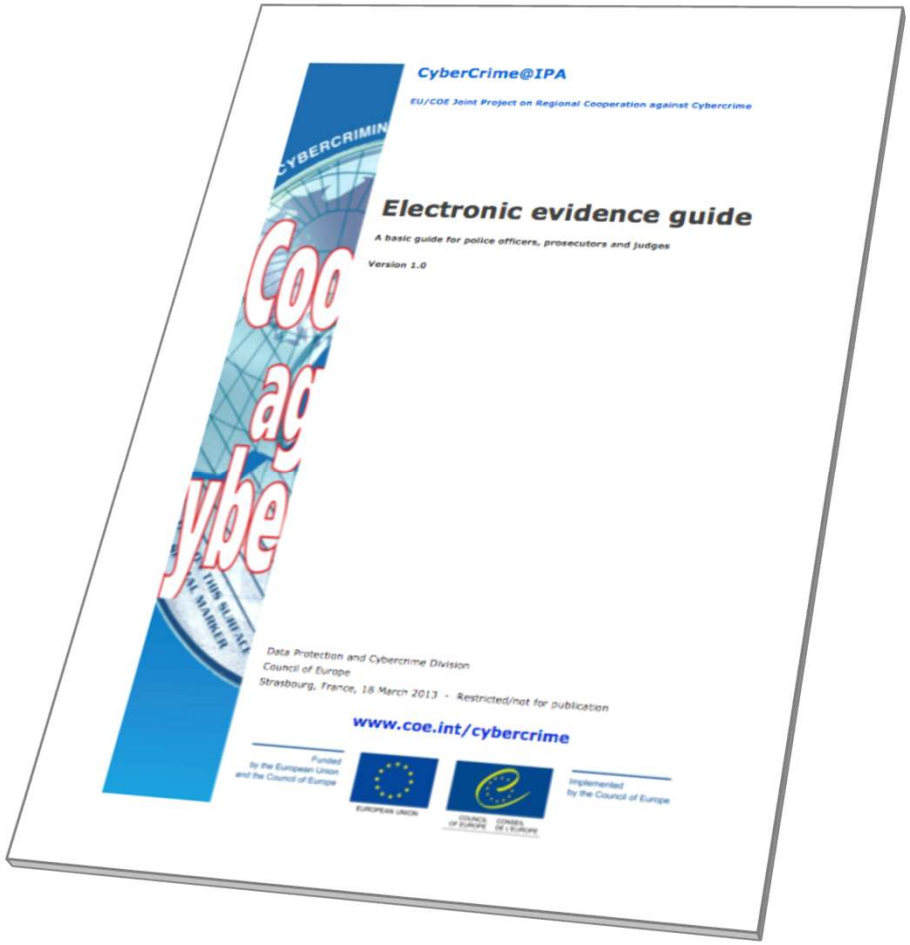
- **Authenticity**: It must be possible to positively tie evidentiary material to the investigated incident.
- **Completeness**: It must tell the whole story and not just a particular perspective.
- **Reliability**: There must be nothing about how the evidence was collected and subsequently handled which causes doubt about its authenticity and veracity.

Considerations for Electronic Evidence

- **Believability**: It must be readily believable and understandable to a judge and/or the members of a jury.
- **Proportionality**: its application to Digital Forensics establishes that the whole investigative process must be adequate and appropriate: the benefits that are to be gained by using a specific measure must outweigh the harms for the party or parties affected by the measure.

BELIEVABILITY MATTERS


Principles of
Electronic
Evidence

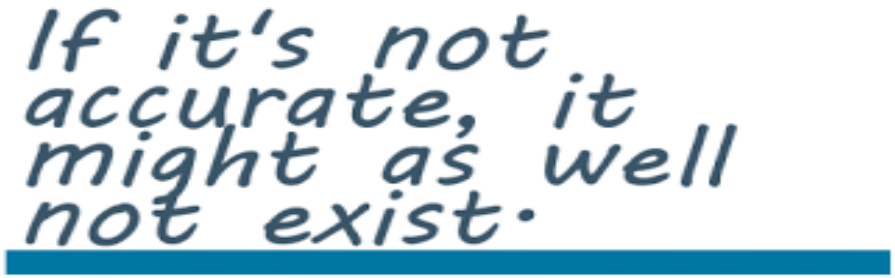


The COE Electronic Evidence Guide

Principle 1 – Data Integrity

No action taken should change electronic devices or media, which may subsequently be relied upon in court.

- When handling electronic devices and data, they must not be changed, either in relation to hardware or software. The person in charge is responsible for the integrity of the material recovered from the scene and thus for commencing a forensic chain of custody.
- There are circumstances where a decision will be made to access the data on a “live” computer system to avoid the loss of potential evidence. This must be undertaken in a manner, which causes the least impact on the data and by a person qualified to do so. Principles 2 to 5 should be taken into account if this course of action is found necessary.



Principle 2 – Audit Trail

- An audit trail or other record of all actions taken when handling electronic evidence should be created and preserved. An independent third party should be able to examine those actions and achieve the same result.
- It is imperative to accurately record all activities to enable a third party to reconstruct the first responder's actions at the scene in order to ensure probative value in court. All activity relating to the seizure, access, storage or transfer of electronic evidence must be fully documented, preserved and available for review.

Principle 3 – Specialist Support

- If it is assumed that electronic evidence may be found in the course of an operation, the person in charge should notify specialists/external advisers in time.
- For investigations involving search and seizure of electronic evidence it may be necessary to consult external specialists. All external specialists should be familiar with the principles laid down in this or similar relevant documents. A specialist should have necessary and appropriate:
  - Specialist expertise and experience in the field,
  - Investigative knowledge,
  - Knowledge of the matter at hand,
  - Legal knowledge,
  - Communication skills (for both oral and written explanations)
  - Language skills.

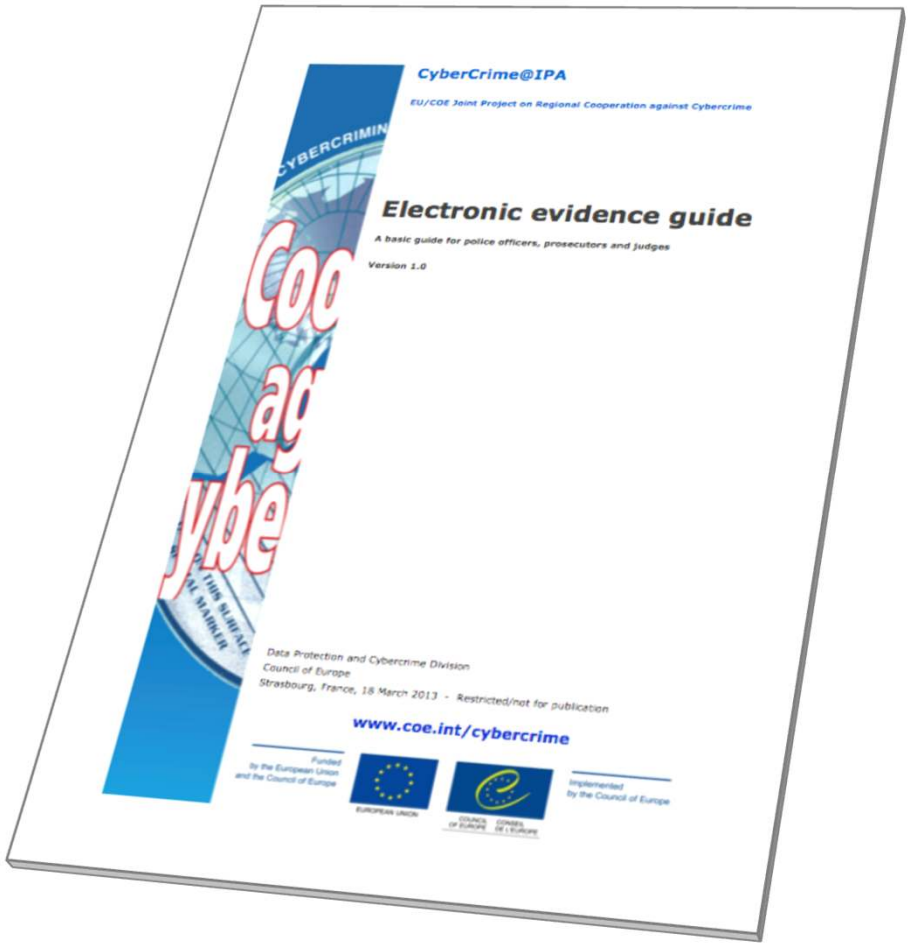
Principle 4 – Appropriate Training

- First responders must be appropriately trained to be able to search for and seize electronic evidence if no experts are available at the scene.
- In exceptional circumstances where it is necessary that a first responder collects electronic evidence and/or access original data held on an electronic device or digital storage media, the first responder must be trained to do it properly and to explain the relevance and implications of his/her actions.

Principle 5 - Legality

- The person and agency in charge of the case are responsible for ensuring that the law, the general forensic and procedural principles, and the above listed principles are adhered to. This applies to the possession of and access to electronic evidence.
- Each Member State should take its own legal documents and regulations into consideration when interpreting the measures proposed in this document.


Good Practice
Guidelines



The COE Electronic Evidence Guide

Background of the guide

Authors:

Nigel Jones (United Kingdom)

Esther George (United Kingdom)

Fredesvinda Insa Mérida (Spain)

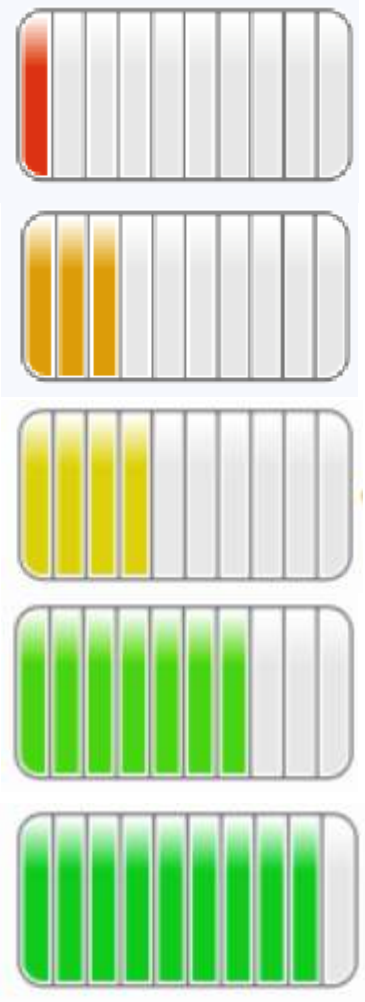
Uwe Rasmussen (Denmark)

Victor Völzow (Germany)

Background of the guide

- **The need:** Requests made by participants in many activities organised under the different cybercrime projects of the Council of Europe, including joint projects with European Union pointing out on the need for more guidance in dealing with electronic evidence.
- The Cybercrime@IPA project in cooperation with the global Project on Cybercrime supports the ongoing development of a guiding paper on electronic evidence
- It provides an important tool for law enforcement and judges in their efforts to investigate, prosecute and adjudicate cybercrimes.

Progress to date



- 1st Meeting in February 2012 set out the structure of the guide and allocated tasks
- Chapters developed between February and May 2012 and commented on by the development team
- 2nd Meeting in May 2012 finalised the draft that was reviewed by subject matter experts
- Review meeting held at the Octopus Conference on 7th June 2012
- Changes to the Guide based on feedback of experts
- February 2013: Release of the guide by Council of Europe
- Review meeting held at the Octopus Conference on 3rd to 6th December 2013
- 2014: Revision and additions to the sections „Capturing evidence from the Internet“ and „Analysing evidence“

The purpose of the guide

- **The purpose:** provide support and guidance in the identification, handling, and examination of electronic evidence.
- It is not intended to be a manual of instruction with step-by-step directions as to how to deal with electronic evidence through all the phases of an investigation.
- It is primarily a basic level document however; some are more detailed sections that provide very practical advice for specialists.

How the guide should be used

- The guide is broken down into chronological sections that aim to provide support for any person dealing with electronic evidence.
- These cover all stages from the initial identification of sources of potential evidence, to search and seizure of data including capture from the Internet, and on to analysis, preparation and reporting of evidence.
- There then follows specialist sections for law enforcement, prosecutors, judges, and the private sector investigator, lawyers, notaries and clerks.

Document Symbols

Information

Important Information

Highly Technical Information

Basic Knowledge

Advanced Knowledge

Specialised Knowledge

Guide structure and content

1. **Introduction**
2. **Evidence sources**
3. **Search and seizure & on site / suspect**
   incl. Dead Box and Live Data Forensics
4. **Capturing evidence from the Internet**
   incl. online sources, covert online investigations, DarkNet
5. **Data held by third parties**
6. **Analysing evidence**
7. **Preparation and presentation of the e**

Guide structure and content

8. Jurisdiction

9. Role Specific Considerations

- 9.1. Law Enforcement
- 9.2. Prosecutors
- 9.3. Judges
- 9.4. Private Sector

10. Case Studies

11. Glossary

12. Further Considerations

13. Appendices

Appendices

Appendix A – Search and seizure law enforcement flowchart

Appendix B – Live forensics flowchart

Appendix C – Private sector preparation flowchart

Appendix D – Private sector search and seizure flowchart

Appendix E – Acquisition of digital evidence flowchart

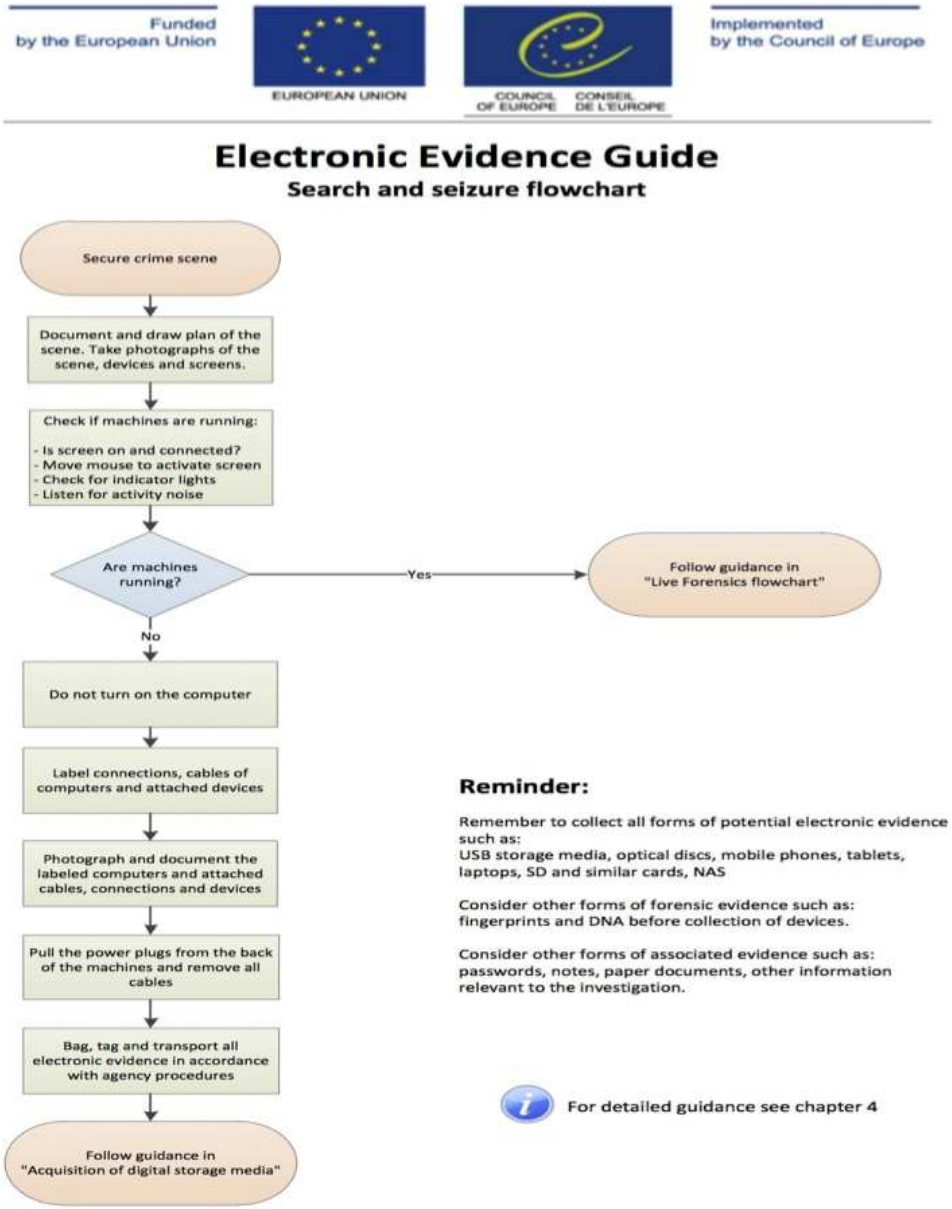
Appendix F – Chain of custody record

Appendix G – Custodian Questionnaire

Appendix H – Template exhibit labels

Appendix I – Acquisition sheet

Appendices


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

Appendices

Funded by the European Union

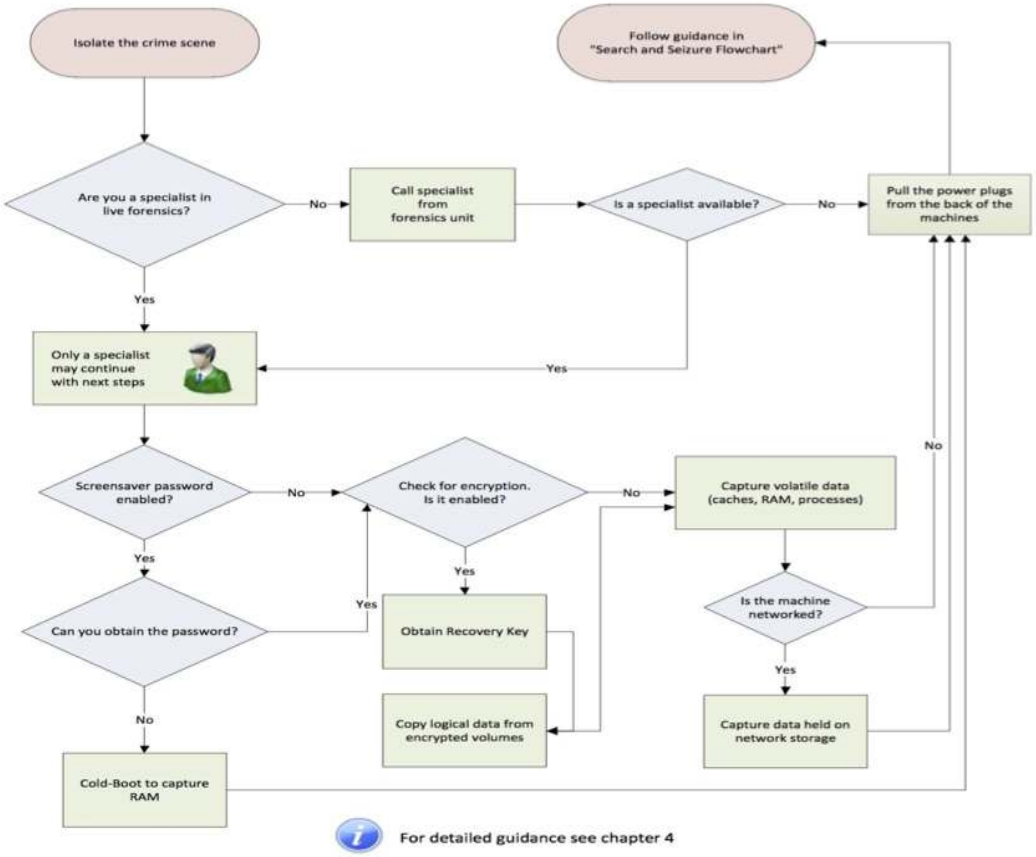
EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Electronic Evidence Guide

Live Data Forensics Flowchart



Appendices

Funded by the European Union

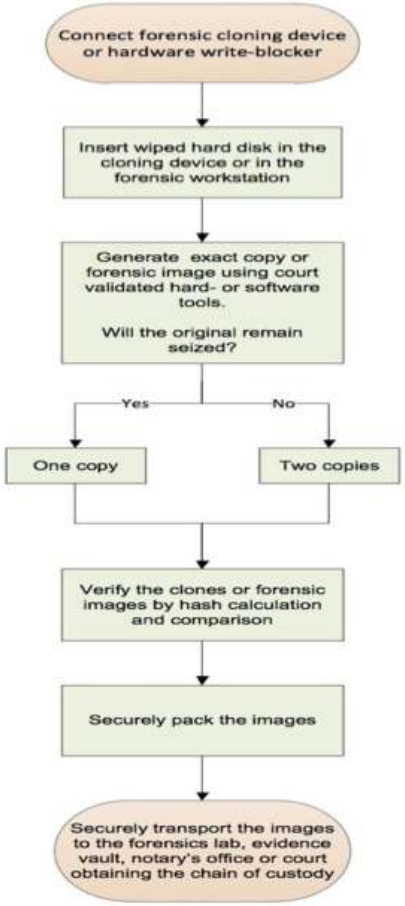
EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Electronic Evidence Guide

Acquisition of digital evidence flowchart



Appendices

Electronic Evidence Guide

CHAIN OF CUSTODY RECORD

Case Reference .....

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

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

Who the guide is for?

- This guide has been prepared for use by countries that are developing their response to cybercrime and establishing rules and protocols to deal with electronic evidence.
- Most of the existing guides have been created for the law enforcement community. This guide is for a wider audience and includes judges, prosecutors and others in the justice system such as private sector investigators, lawyers, notaries and clerks.

Availability of the Electronic Evidence Guide

Availability

www.coe.int/cybercrime

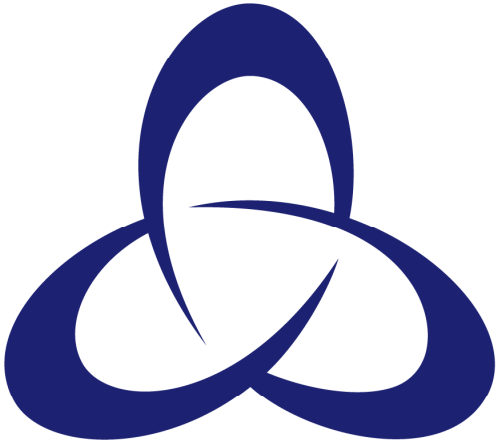
Validity of the Guide

- This guide and the information contained within are considered valid until 31st December 2015.
- It is intended that the guide will be updated before that date to take into account any relevant changes in technology, procedures and practices that are relevant to the content of this guide.
- Any person or organisation wishing to use the guide after the above date should contact the Council of Europe to obtain the latest version.

The Budapest Convention

The Budapest Convention offers many provisions to enhance investigations where electronic evidence is involved. Some of these are mentioned in this guide; however this is not a guide to the Convention and the reader should always refer to the authoritative documents available from the Council of Europe when seeking to use these provisions.

Questions?



Canterbury Christ Church University

Nigel Jones
Director of the Centre for Cyberforensics
Canterbury Christ Church University
United Kingdom
nigel.jones@canterbury.ac.uk