

GLACY
Global Action on Cybercrime
Action globale sur la cybercriminalité


Workshop on electronic evidence


Organised by the Ministry of Information and Communication Technology of Mauritius
and the Council of Europe
Balaclava, Mauritius, 12 August 2014


**About electronic evidence:
concept, relevance and principles
(Introduction to the Electronic Evidence Guide)**

Victor Völzow
 Council of Europe consultant, Hesse State Police Academy, Germany

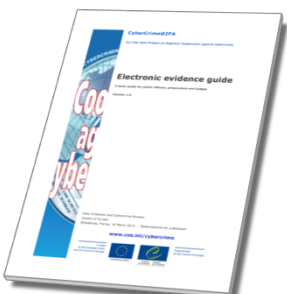
www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
Implemented
by the Council of Europe

CONSEIL DE L'EUROPE



The Electronic Evidence Guide



The Electronic Evidence Guide

2

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.

Background of the guide



Authors:

Nigel Jones (United Kingdom)
Esther George (United Kingdom)
Fredesvinda Insa Mérida (Spain)
Uwe Rasmussen (Denmark)
Victor Völzow (Germany)

The purpose of the guide



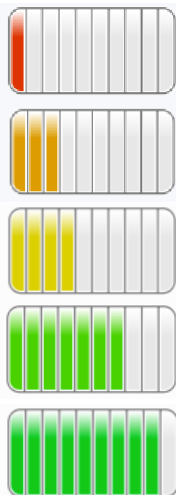
- **The purpose:** provide support and guidance in the identification, handling, and examination of electronic evidence.
- It is not intended to be a manual of instruction with step-by-step directions as to how to deal with electronic evidence through all the phases of an investigation.
- It is primarily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

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.

Progress to date



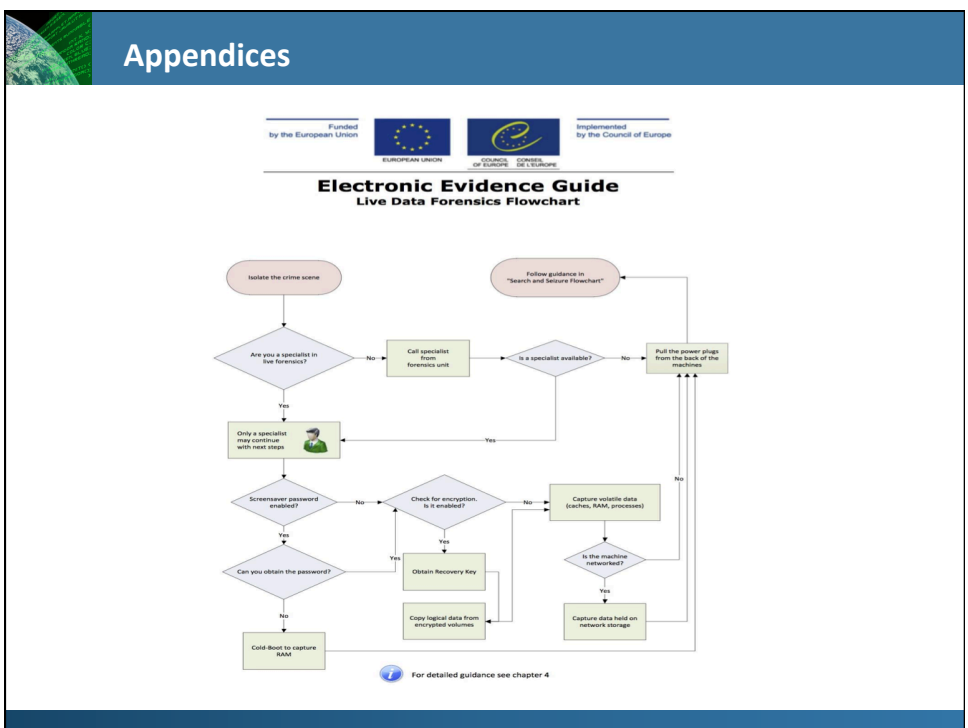
- 1st Meeting in February 2012 set out the structure of the guide and allocated tasks
- Chapters developed between February and May 2012 and commented on by the development team
- 2nd Meeting in May 2012 finalised the draft that was reviewed by subject matter experts
- Review meeting held at the Octopus 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“

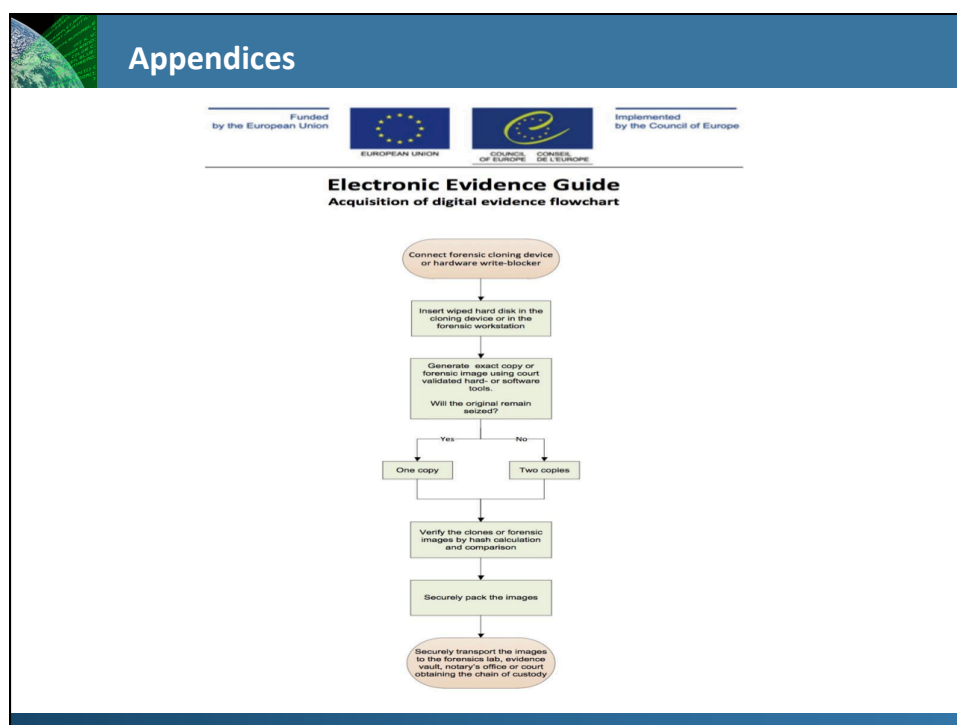
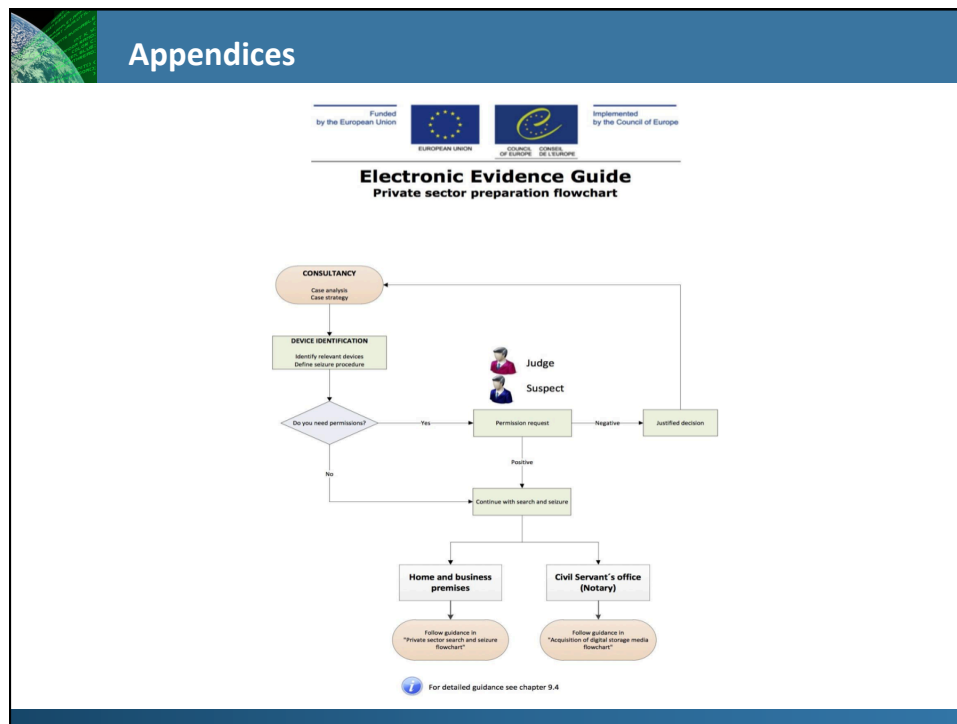
Guide structure and content

- 1. Introduction**
- 2. Evidence sources**
- 3. Data held by third parties**
- 4. Search and seizure & on site / suspect**
 - 4.1. Dead Box
 - 4.2. Live Data Forensics
- 5. Capturing evidence from the Internet**
 - 5.1. Online Sources
 - 5.2. Covert Online Investigations
- 6. Analysing evidence**
- 7. Preparation and Presentation of the Evidence**

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
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



COE

Implemented by the Council of Europe

Electronic Evidence Guide

CHAIN OF CUSTODY RECORD


Case Reference

Book **of**

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

Availability of the Electronic Evidence Guide


Availability



www.coe.int/cybercrime

Questions

Any questions?



Please ask!