GLACY

Global Action on Cybercrime
Action globale sur la cybercriminalité

Digital Forensics Laboratory Management and Procedures Guide

Global Action on Cybercrime
From GLACY to GLACY+
GLACY Closing and GLACY+ Launching Conference
Bucharest 26th to 28th October 2016

Agenda

DIGITAL FORENSICS LABORATORY
MANAGEMENT AND PROCEDURES GUIDE

RESTRICTED – Not for Publication

Version

www.coe.int/cybercrime

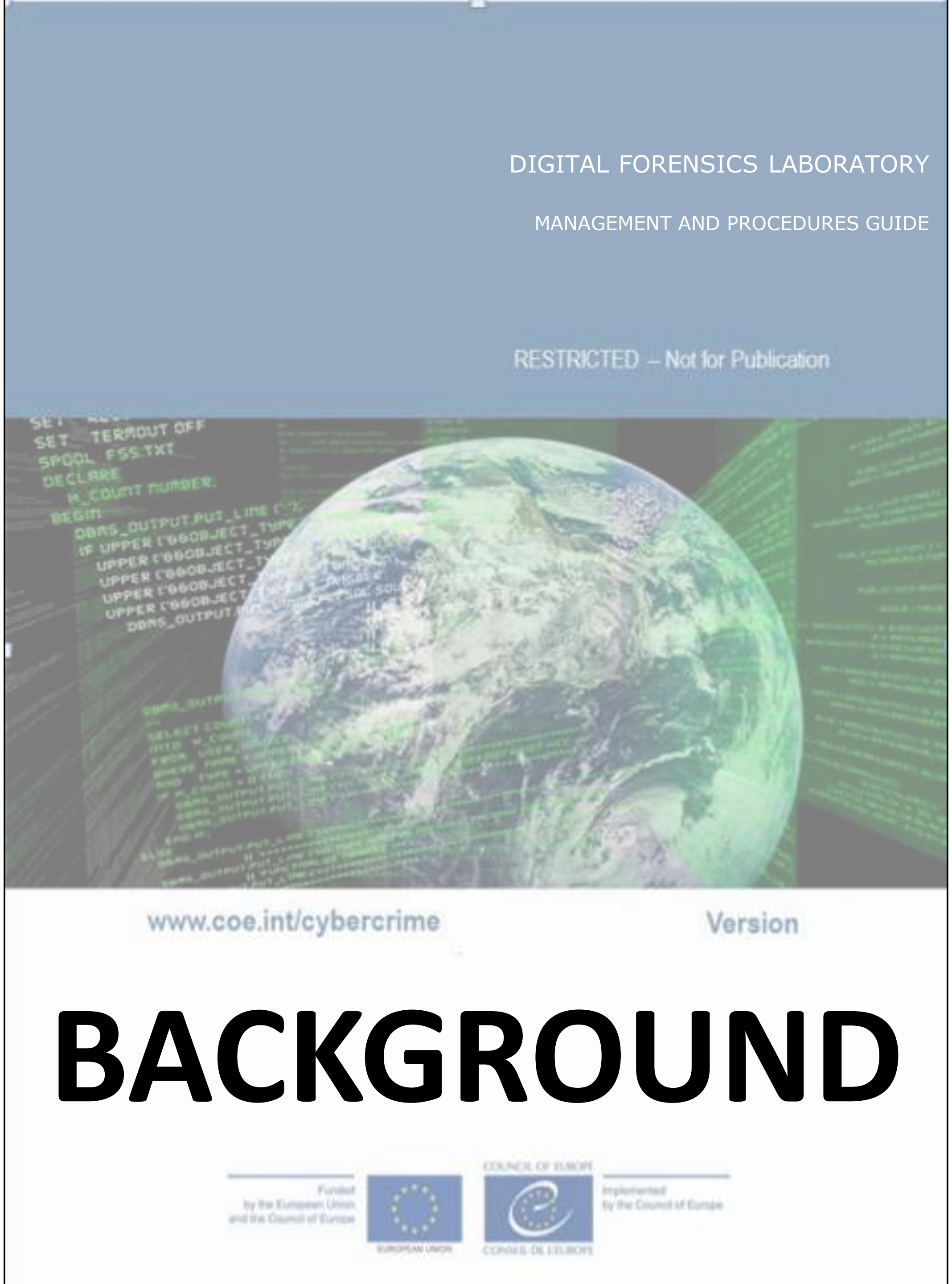
Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

- Background
- Who is the Guide for
- Purpose of the Guide
  - What is in the Guide
  - What is not in the Guide
  - Symbols and Explanations
- Guide Structure and Content



DIGITAL FORENSICS LABORATORY

MANAGEMENT AND PROCEDURES GUIDE

RESTRICTED – Not for Publication

www.coe.int/cybercrime

Version

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

BACKGROUND

Background of the guide

- **The Need:** Following on from the production of the electronic evidence guide, countries requested a similar guide for digital forensic activities.
- The **Electronic Evidence** guide covered stages from the crime scene to the door of the laboratory.
- The **Digital Forensics Laboratory Management and Procedures Guide** picks up the procedures from when the lab door is opened until the evidence is produced for court

Background of the guide

Authors:

Nigel Jones (United Kingdom)

Victor Völzow (Germany)

Andrea Bradley (United Kingdom)

Branko Stamenkovic (Serbia)

Background of the guide

ELECTRONIC EVIDENCE GUIDE

A BASIC GUIDE FOR POLICE OFFICERS, PROSECUTORS AND JUDGES

RESTRICTED – Not for Publication

www.coe.int/cybercrime

Version 2.0

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

DIGITAL FORENSICS LABORATORY

MANAGEMENT AND PROCEDURES GUIDE

RESTRICTED – Not for Publication

www.coe.int/cybercrime

Version

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

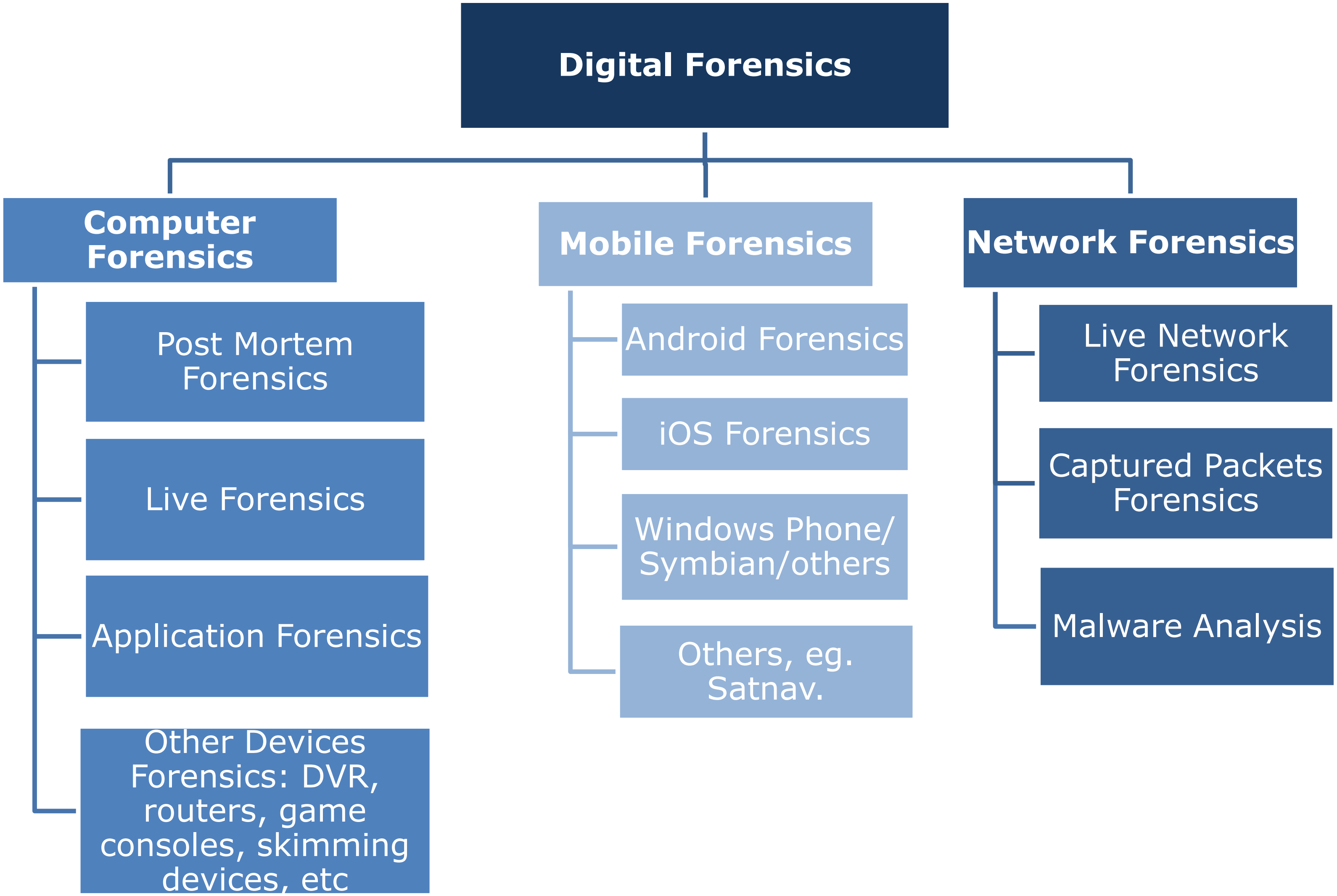
Background of the guide

What is Digital Forensics

- Digital forensics is the branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on data stored on a computer system, digital device or other storage media.

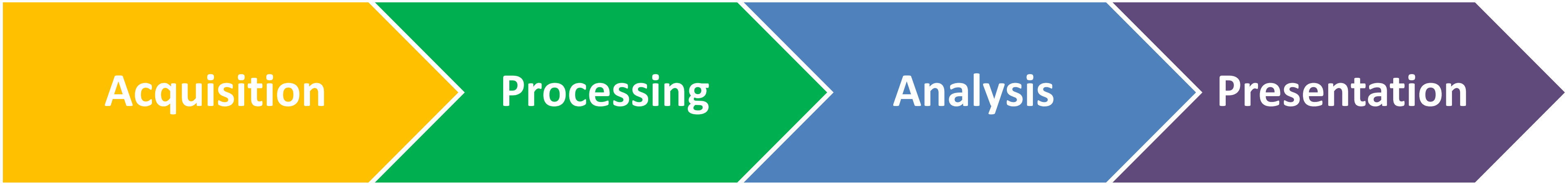
- Each and every branch of Digital Forensics requires extensive training and experience making it impossible for one forensic examiner to be expert in all areas. The following chart shows the main subcategories and subject areas of Digital Forensics.

Background of the guide



- Digital Forensics
  - Computer Forensics
    - Post Mortem Forensics
    - Live Forensics
    - Application Forensics
    - Other Devices Forensics: DVR, routers, game consoles, skimming devices, etc
  - Mobile Forensics
    - Android Forensics
    - iOS Forensics
    - Windows Phone/ Symbian/others
    - Others, eg. Satnav.
  - Network Forensics
    - Live Network Forensics
    - Captured Packets Forensics
    - Malware Analysis

Steps in Digital Forensics Examination

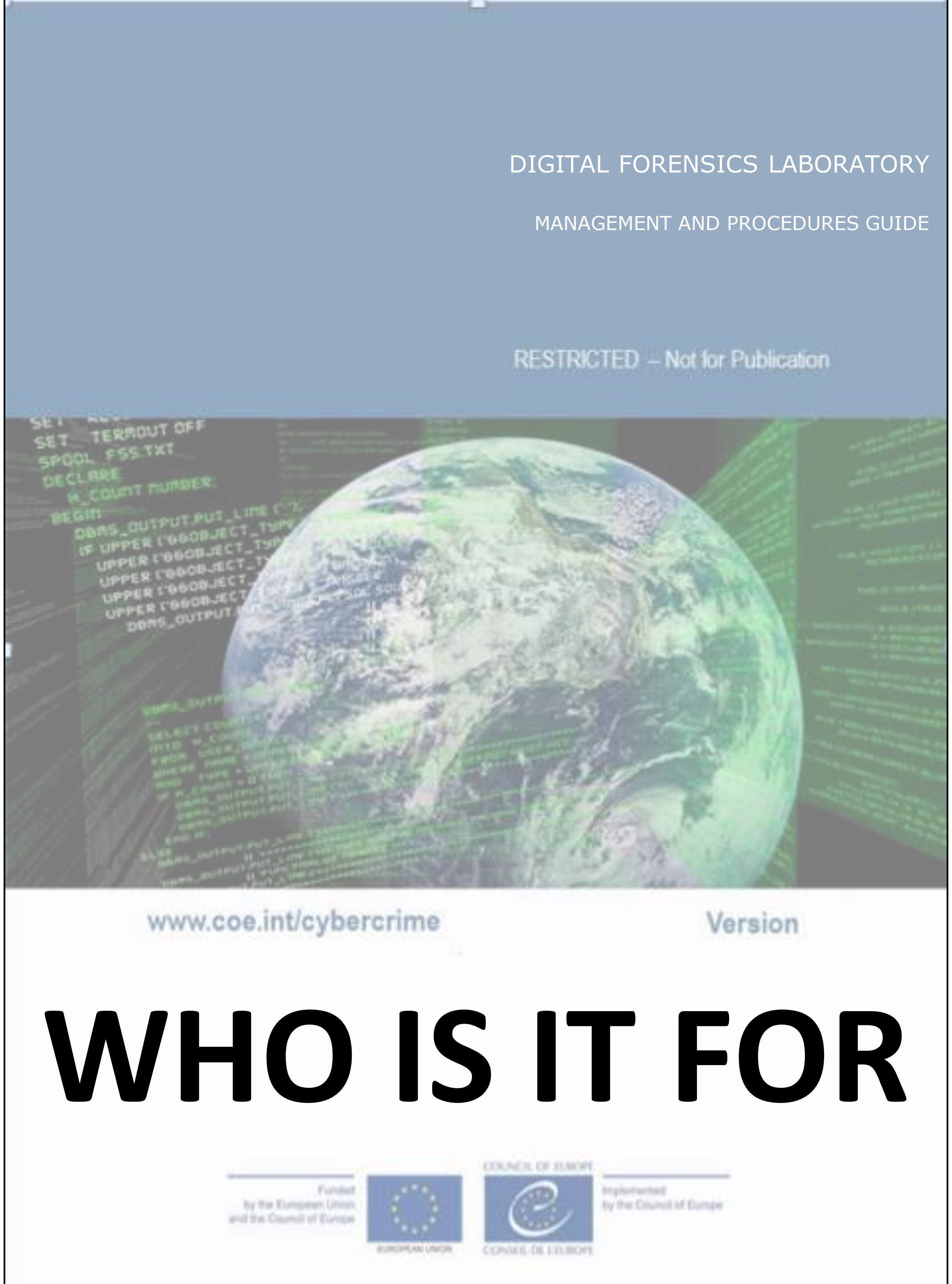


Acquisition

Processing

Analysis

Presentation



DIGITAL FORENSICS LABORATORY

MANAGEMENT AND PROCEDURES GUIDE

RESTRICTED – Not for Publication

www.coe.int/cybercrime

Version

Funded
by the European Union
and the Council of Europe

Implemented
by the Council of Europe

WHO IS IT FOR

Who is the Guide for?

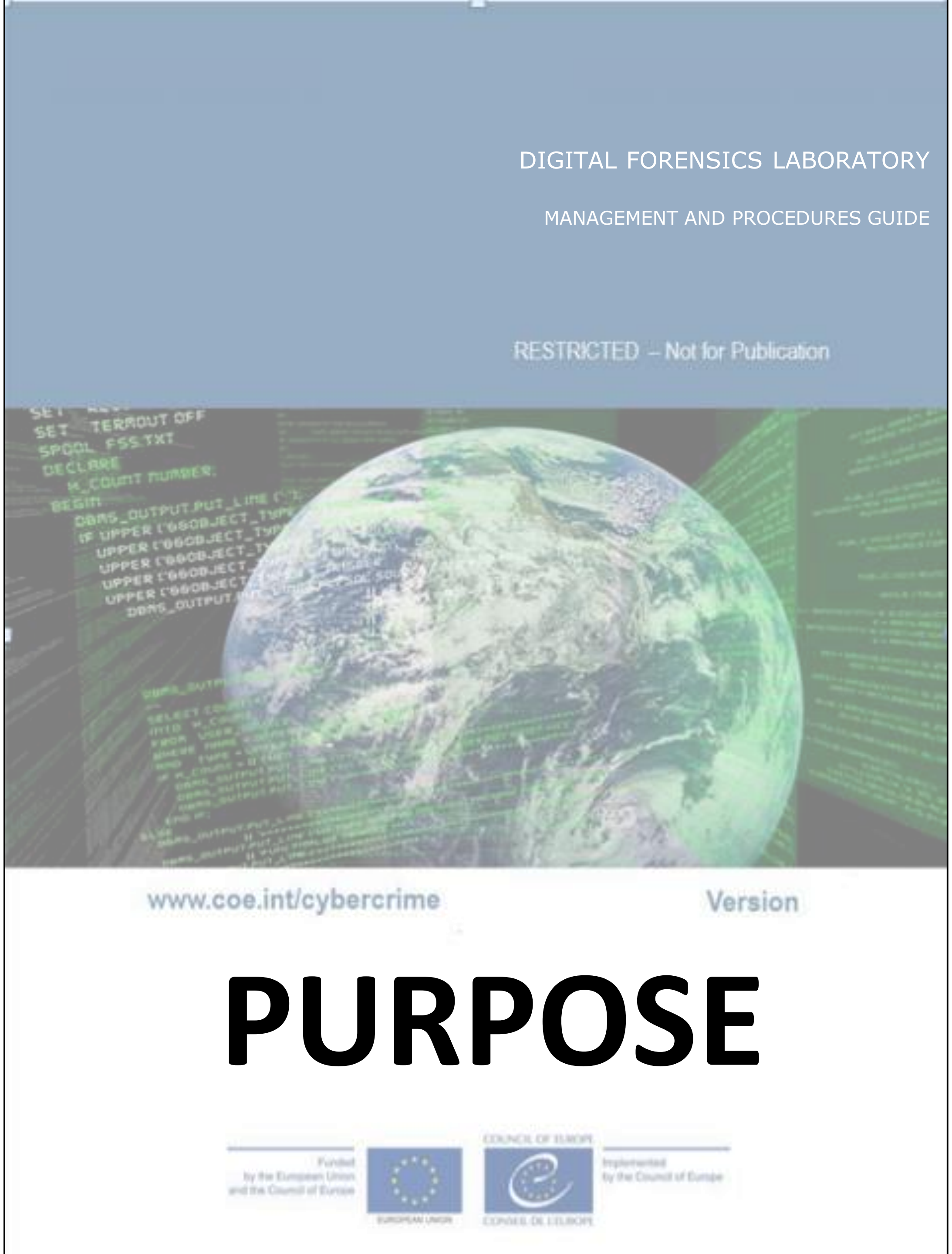
- The Guide provides support and guidance to:
- **Managers** and **Practitioners** of **Digital Forensics Laboratories**
- The guide should also be at the disposal of **Prosecutors and Judges.** Although members of Judiciary are not, by rule of the thumb, obliged to be well acquainted, or specialised, in sciences other than legal; contemporary criminal acts and their perpetrators are putting additional pressure on professionals both in Prosecution and Courts to better understand and enhance their knowledge about cybercrime and raise their capabilities to render legal and rightful decisions in cybercrime criminal cases.

How the Guide should be used

- This Guide should be seen as a template document that can be used by countries to consider when developing their digital forensics capability. The advice given is intended to be used at both strategic and tactical levels, according to their national legislation, practice and procedure.
- The overarching principles described in the **Electronic Evidence Guide** are just as relevant to the procedures conducted in the laboratory environment and are in accordance with generally accepted good practice for dealing with electronic evidence. The principles are set out below to reinforce their importance:

Electronic Evidence Principles

- The Guide follows the principles adopted in the **Electronic Evidence Guide**, covering:
- Principle 1 – Data Integrity
- Principle 2 – Audit Trail
- Principle 3 – Specialist Support
- Principle 4 – Appropriate Training
- Principle 5 – Legality



DIGITAL FORENSICS LABORATORY

MANAGEMENT AND PROCEDURES GUIDE

RESTRICTED – Not for Publication

www.coe.int/cybercrime

Version

PURPOSE

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

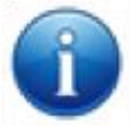
What is in the Guide

- The purpose of the Guide is to provide support and guidance to managers and practitioners of digital forensics laboratories in the setting up and running of such laboratories in such a way that any evidence produced by them is dealt with in such a manner that will ensure its authenticity for later admissibility in court.
- Although the Guide is not intended to be an instruction manual with step-by-step directions, it does provide an overview of the kinds of issues that often arise when developing and running a digital forensics laboratory and offers advice on how to deal with them. Readers of this document should check if such advice already exists at the national level.

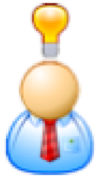
What is not in the Guide

- The guide does not make any recommendations regarding the hardware and software choices that may be available. Each country and organisation will decide what is appropriate given their needs and available funds. It should be remembered that digital forensics equipment and commercial software can be a very expensive long term commitment and is not easy to change once the initial decision is made.
- Details of the types of costs associated with forensic software purchases and information about some options to use open source software, are dealt with elsewhere in this document.

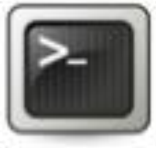
Symbols and Explanations



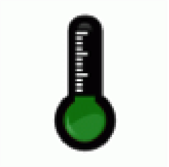
This symbol indicates the section contains information.



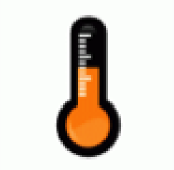
This symbol indicates important information.



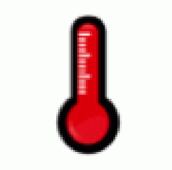
This symbol indicates highly technical information



This symbol indicates the section contains basic knowledge



This symbol indicates advanced knowledge



This symbol specialised knowledge

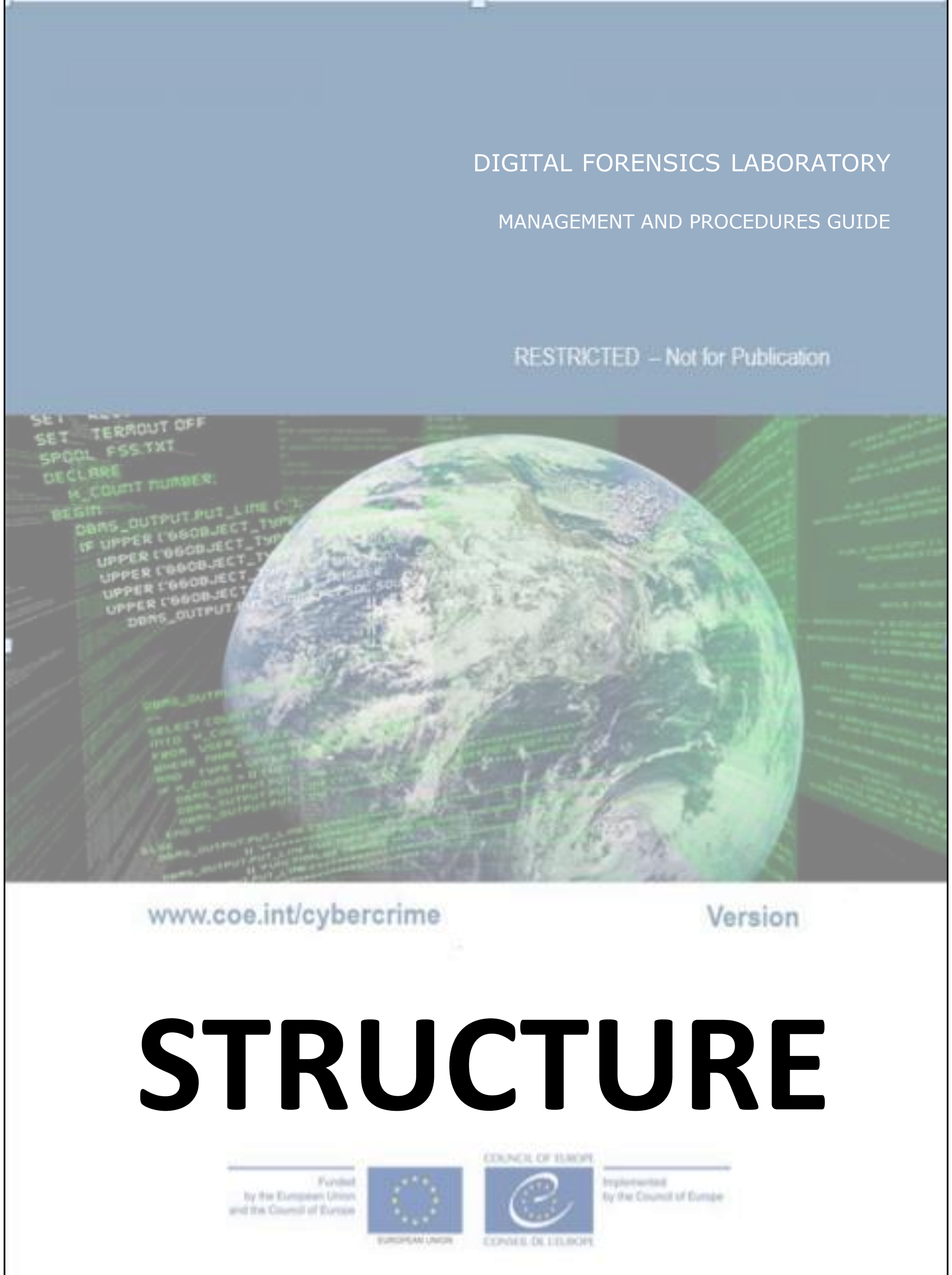
Symbols and Explanations

Prosecutors considerations

Prosecutors considerations are very important to the criminal justice officials who are involved in development and management of digital forensics laboratory and to the staff employed within a digital forensics laboratory in technical roles relating to the digital forensics processes and procedures, since the outcome of the process should be evidence or evidentiary material, which should represent a corner stone for Prosecutorial decision in the criminal case.

Depending on the country's Criminal Legal framework, involvement of the Prosecutors will be at different stages, in the criminal justice process. In some jurisdictions, Prosecution will only request digital forensics expert opinion. In others, Prosecution will be more involved in the expertise processes, including involvement into particular phases of the process itself. In some jurisdictions, Prosecutors have an advisory role or legal responsibility for the investigation process.

Whichever legal framework exists, it is very likely that Prosecutors will be first judiciary officials who are going to be presented with evidence adduced from the digital forensic process. This guide, together with the Council of Europe Electronic Evidence Guide, and the information contained therein should be accessible to Prosecutors and other parties involved in the criminal justice process, irrespective of legal framework.



DIGITAL FORENSICS LABORATORY

MANAGEMENT AND PROCEDURES GUIDE

RESTRICTED – Not for Publication

www.coe.int/cybercrime

Version

STRUCTURE

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Guide structure and content

- **Introduction**
- **Management of a Digital Forensics Laboratory**
  - **Research**
  - **Budgeting/Capacity**
  - **Premises**
    - Security, Location, Size, Air conditioning
  - **Staff**
    - Recruiting, Police Officers or Police Support Staff?, Vetting, Staff Development and Human Resources, Welfare, Health and Safety
  - **Physical Laboratory Requirements**
    - Office Equipment, Software and hardware, Quality Assurance/ Review procedure, Streamlined Examination and Reporting, Retention of Data, Education and Training of All Stakeholders

Guide structure and content

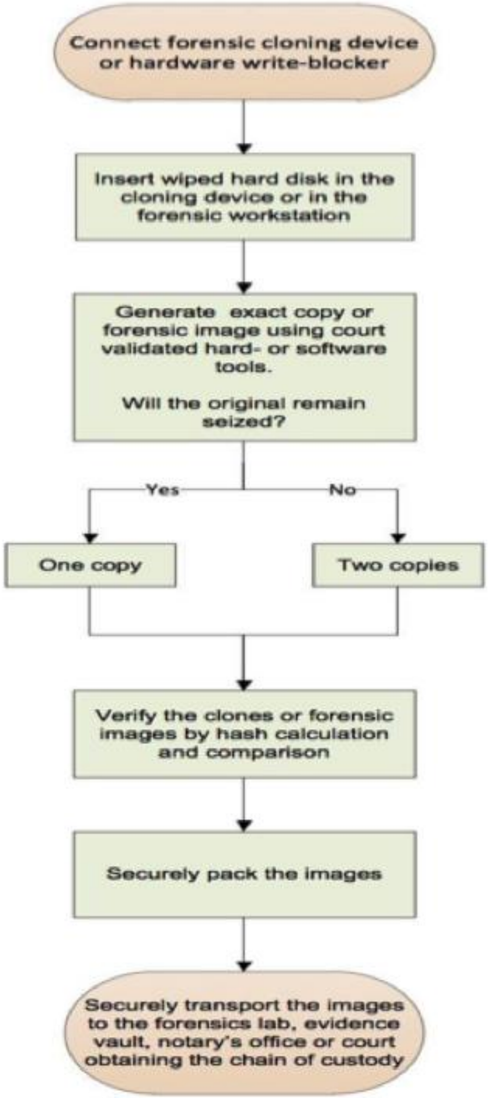
- **Digital Forensics Lab Processes and Procedures**
  - **Overall Process Model**
  - **Acquisition Stage**
    - Processing of computer systems, Processing of mobile devices
  - **Processing Stage**
    - Processing of computer systems, Processing of mobile devices
  - **Analysis Stage**
    - Analysing computer systems, Analysing mobile devices
  - **Presentation Stage**
    - Admissibility of electronic evidence, Report writing, Expert witness status, Alternative presentation methods
- **Appendices**

Appendices

- EU Competency Framework
- Acquisition Process Flow Chart
- Processing Flow Chart
- Analysis Flow Chart
- Presentation Flow Chart
- Chain of custody record
- Exhibit Form
- Imaging Form
- Digital Forensics Analysis Form / Spreadsheet
- Digital Forensics Report Template

Appendix Example

Acquisition of digital evidence flowchart



Connect forensic cloning device or hardware write-blocker

Insert wiped hard disk in the cloning device or in the forensic workstation

Generate exact copy or forensic image using court validated hard- or software tools.

Will the original remain seized?

Yes

No

One copy

Two copies

Verify the clones or forensic images by hash calculation and comparison

Securely pack the images

Securely transport the images to the forensics lab, evidence vault, notary's office or court obtaining the chain of custody

Validity of the Guide

- This guide and the information contained within are considered valid until 31st December 2017.
- 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.

Questions

Digital Forensics Laboratory Management and Procedures Guide

Global Action on Cybercrime
From GLACY to GLACY+
GLACY Closing and GLACY+ Launching Conference
Bucharest 26th to 28th October 2016

THANK YOU
for your attention!