



Electronic Evidence Guide

Octopus Conference
Strasbourg
6th to 8th June 2012

Guide Background

- **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 development of a guiding paper on electronic evidence
- It will provide an important tool for law enforcement and judges in their efforts to investigate, prosecute and adjudicate cybercrimes.

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 is the Guide 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 presented to you all in the past few days for your review
- Review meeting held at the Octopus Conference on 7th June 2012

Guide Structure and Content

- 1. Introduction**
- 2. Evidence sources**
- 3. Data held by third parties**
- 4. Search and seizure + on site / suspect**
 1. Dead Box
 2. Live Data Forensics
- 5. Capturing evidence from the Internet**
 1. Online Sources
 2. Covert Online Investigations
- 6. Analysing evidence**

Guide Structure and Content

7. Preparation and Presentation of the Evidence

8. Jurisdiction

9. Role Specific Considerations

1. Law Enforcement
2. Prosecutors
3. Judges
4. Private Sector

10. Case Studies

11. Glossary

12. Further Considerations

13. Appendices

To Be Done

- Excellent feedback from the review to be incorporated in the guide.
- IPA regional Review on 4th and 5th September 2012.
- Finalisation and publication



Cybercrime Training for Judges and Prosecutors

“Basic and Advanced Courses”

Octopus Conference

Strasbourg

6th to 8th June 2012

Course Background

- An underlying basic course entitled “Introductory Cybercrime and Electronic Evidence Training for Judges and Prosecutors” has been developed as an output of the European Union/Council of Europe Joint Project on Regional Cooperation on Cybercrime in the IPA region.
- The proposed “advanced” course is to provide further knowledge and skills based upon the outputs from the basic course and additional requirements identified by delegates and trainers.


Why is This Training Necessary

- Judges and prosecutors play an important role in the investigation and adjudication of individuals or groups that have committed crimes.
- With the increased number of incidents where these crimes have an element of cybercrime there is an increased need for judges and prosecutors to be properly trained to understand the nature of these crimes and to also be aware of the legislation and the instruments for international cooperation available to handle cases of cybercrimes.

Basic Course Aim

The course is designed to provide judges and knowledge with an introductory level of knowledge on cybercrime and electronic evidence. The course provides legal as well as practical information about the subject matters and concentrated on how these issues impact on the day-to-day work of the delegates.

Cybercrime Course Timetable

 Council of Europe Cybercrime for Judges and Prosecutors Training Course								
Timetable - Module 1								
	09:00 - 10:00	10:00 - 11:00	11:00 - 12:00	12:00 - 13:00	13:00 - 14:00	14:00 - 15:00	15:00 - 16:00	16:00 - 17:00
Day 1	1.1.1 Course Opening and Introductions		1.1.2 Introduction to Cybercrime Threats, trends and challenges		BREAK	1.1.3 Introduction to Technology Part 1		
Day 2	1.2.1 Daily Review	1.2.2 Introduction to Technology Part 2		1.2.3 Cybercrime as a Criminal Offence in Domestic Legislation	BREAK	1.2.4 Procedural Law and Investigative Measures in Domestic Legislation		1.2.5 Introduction to Technology Part 3
Day 3	1.3.1 Daily Review	1.3.2 Electronic Evidence Practice and Procedure		1.3.3 Electronic Evidence Procedural and Investigative Law	BREAK	1.3.4 International Cooperation		1.3.5 Delegate Feedback and Course Closure

Courses Delivered

- February 2012 – Training Skills course – Zagreb
- April and May 2012 – 8 courses in IPA region
- Delivered by new trainers
- To be incorporated in national training programmes in the region
- Final workshop on 11th and 12th July in Zagreb



Course Aim

- This course is designed to build upon the learning outcomes of the basic cybercrime training course for judges and prosecutors and should be attended only by those that have successfully completed that course.
- The aim of the course is to provide the knowledge and skills to allow judges and prosecutors to fulfill their roles relating to cybercrime investigations. They will be able to consider the issues relevant to such investigations.

Course Objectives

- At the end of this course the delegates will be able to:
- Identify types of crime committed
- Conduct the investigation
- Establish the location of evidence, witnesses and suspects
- Secure evidence in an acceptable way, irrespective of where it is held
- Prepare for search and seizure activities involving electronic evidence,
- Deal with digital devices that are part of the investigation
- Brief forensic specialists and others needed to support the investigation phase,
- Prepare for interviews with suspects,
- Prepare and present cybercrime evidence
- Consider the relevant aspects that will be met during the judicial process.

The Course Activities

- 4 courses covering 8 countries – 2 days each
- 12 hours teaching time per course
- Courses in Tirana, Ankara, Skopje & Zagreb
- Existing trainers and past trainees (circa 24 per course)
- Interactive moderated practical exercises
- Probably 4 groups of 6?
- Paper Feed Exercises
- Presentations on specific subjects (e.g. what can the forensic examiner do for the investigator)
- Video record the entire courses for future use in country

Stages of the Investigation

- Complaint received – Identify crimes
- Develop investigation strategy
- Identify where evidence is and how to get it
- Identify the offender(s)
- Plan for arrest, search and seizure
- Plan for interview
- Gather all evidence
- Prepare case for prosecution
- Decide how evidence will be presented
- Deal with court and trial issues



Questions