

# GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS

Best practices for search and seizure of electronic and digital evidence

# SITUATION

Digital devices form a critical source of information in investigations into all types of crime. Evidence in an electronic format ('electronic evidence' or 'digital evidence') can be difficult to obtain and understand.

Without effective digital forensics capability, law enforcement bodies may fail to obtain crucial evidence, misinterpret its meaning or importance, or even unintentionally destroy it.



## INTERPOL RESPONSE

In pursuit of providing guidance and support to law enforcement agencies across the globe, INTERPOL Project LEADER in collaboration with the INTERPOL Innovation Centre (IC) developed the INTERPOL Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence.

These Guidelines aim to establish best practices for handling and using digital evidence during search and seizure preparatory and execution stages. Key technical considerations are also identified on the effective preservation of data to ensure that it can support law enforcement in criminal investigations, and it can be admissible in court.

# TARGET AUDIENCE

The Guidelines are intended to assist law enforcement officers from different crime areas who may attend to a crime scene, being responsible for collecting, securing, and transporting electronic and digital evidence.

## CONTENT



#### Search and Seizure Preparation Phase Planning, destination of evidence and equipment preparation

**Technical considerations** 

Creation of a forensic copy and/or its alternatives; HASH

function



#### Search and Seizure Execution Phase

Securing, assessing, documenting the scene; collection, handling, seizure and transport of the evidence



### Specific procedures

For smartphones, SIM cards and media devices, servers, PCs and laptops, IoT devices, gaming consoles, drones, CCTV, Automobiles, Virtual assets devices and shipborne equipment.



The Guidelines are based on:

- The Electronic Evidence Guide of the Council of Europe,
- The Digital Evidence Collection Certificate Manual of the National Centre of Excellence in Cybersecurity in Spain (INCIBE), and
- Other best practice guides of law enforcement agencies concerning the seizure and treatment of electronic evidence.

If you wish a copy of the Guidelines, please send a message to dfl@interpol.int



INTERPOL Global Complex for Innovation 18 Napier Road 285510 Singapore

www.interpol.int

With the support of:

