INTERPOL

Cybercrime and Digital Evidence capacity building & tools

Simon Hirrle
Specialized Officer Cybercrime

INTERPOL

1. **Capacity building**
   a) **Cybercrime**
   b) Digital Evidence
2. Tools

- INTERPOL Cyber Capabilities Development Unit
- INTERPOL Projects, e.g. ACCDP, GLACY+, LEADER

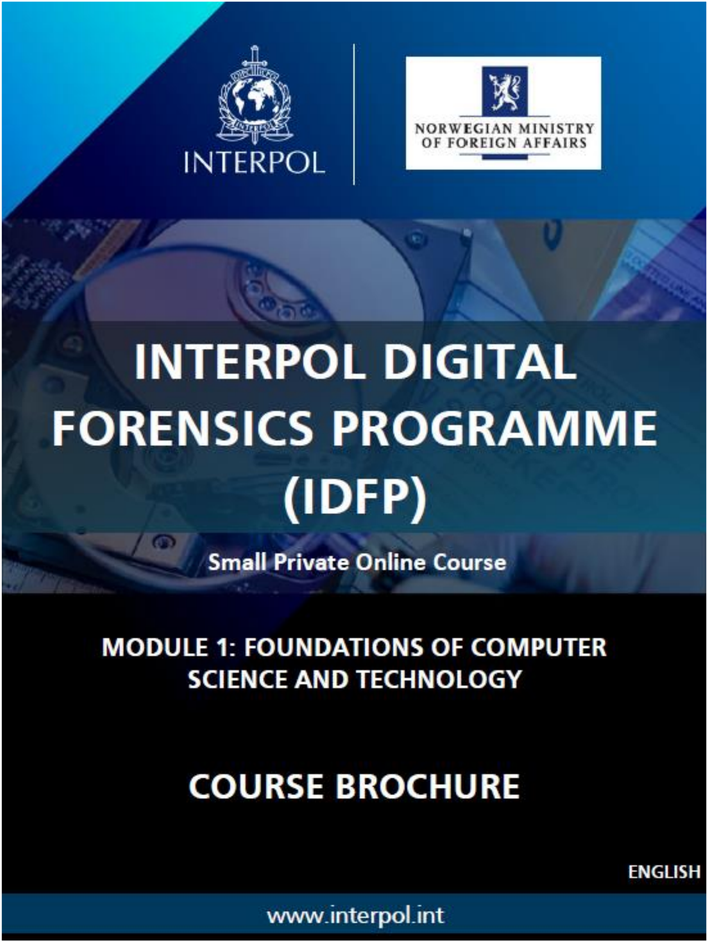
- Cryptocurrency Investigation Training
- Digital Evidence Workshop
- Open Source Intelligence Training (OSINT)
- Social Media Intelligence Training (SOCMINT)
- Domain Investigation Training
- Digital Currency Investigation Training
- Chinese OSINT Training
- Router Investigation Training
- Ransomware Investigation Training
- (and more)

INTERPOL
KICKOFF AND DRAFTING WORKSHOP ON STRATEGY DEVELOPMENT GUIDEBOOK
ASEAN CYBER CAPACITY DEVELOPMENT PROJECT PHASE 2
SINGAPORE
16-20 DECEMBER 2019
INTERPOL
Cybercrime or Cy

INTERPOL

1. **Capacity building**
   a) Cybercrime
   b) **Digital Evidence**
2. Tools

Project LEADER



INTERPOL | NORWEGIAN MINISTRY OF FOREIGN AFFAIRS

INTERPOL DIGITAL FORENSICS PROGRAMME (IDFP)

Small Private Online Course

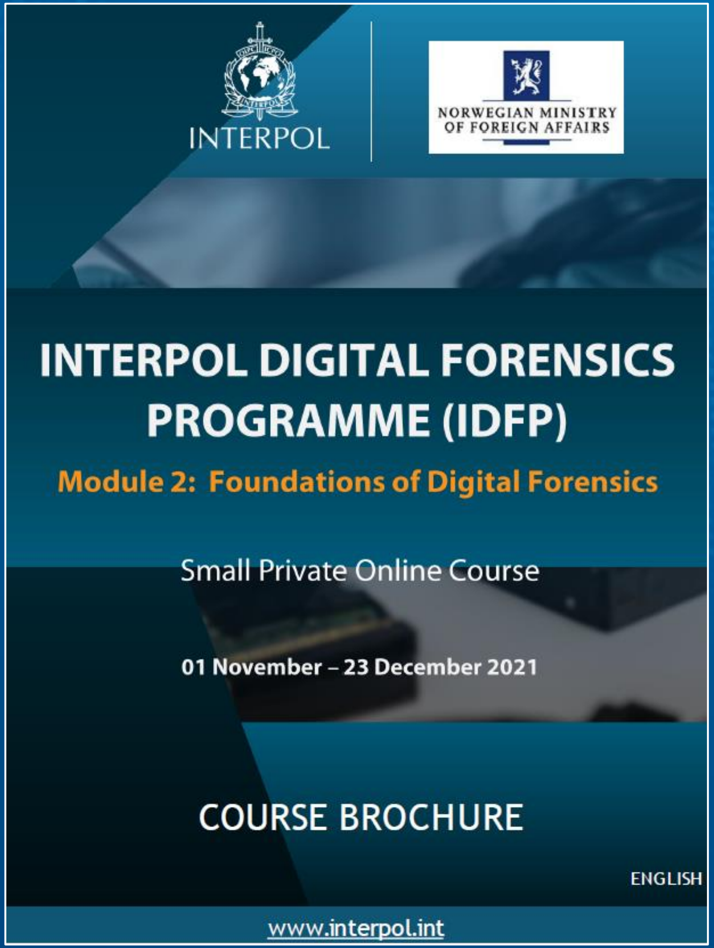
MODULE 1: FOUNDATIONS OF COMPUTER SCIENCE AND TECHNOLOGY

COURSE BROCHURE

ENGLISH

www.interpol.int

(completed)



INTERPOL | NORWEGIAN MINISTRY OF FOREIGN AFFAIRS

INTERPOL DIGITAL FORENSICS PROGRAMME (IDFP)

Module 2: Foundations of Digital Forensics

Small Private Online Course

01 November – 23 December 2021

COURSE BROCHURE

ENGLISH

www.interpol.int

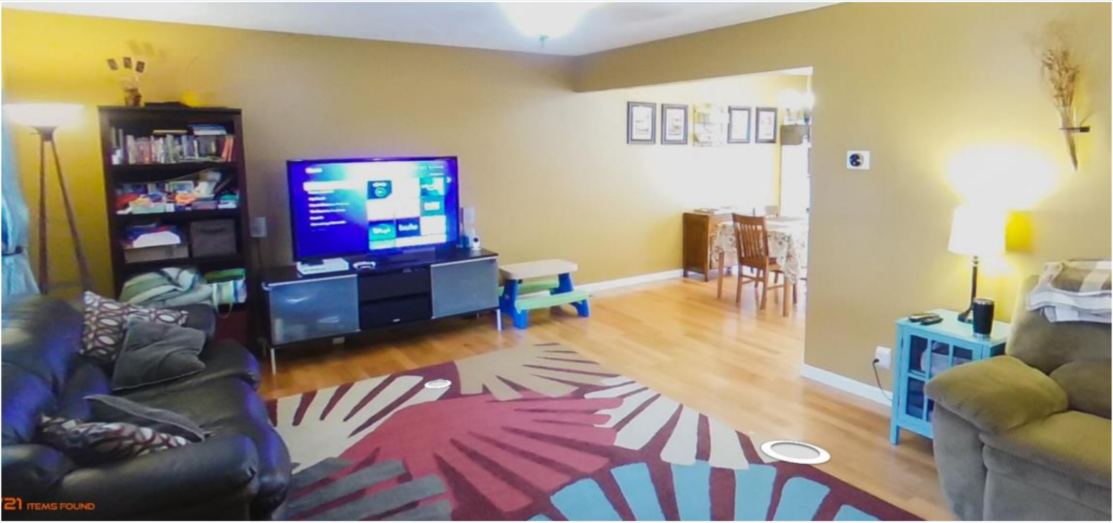
(ongoing)

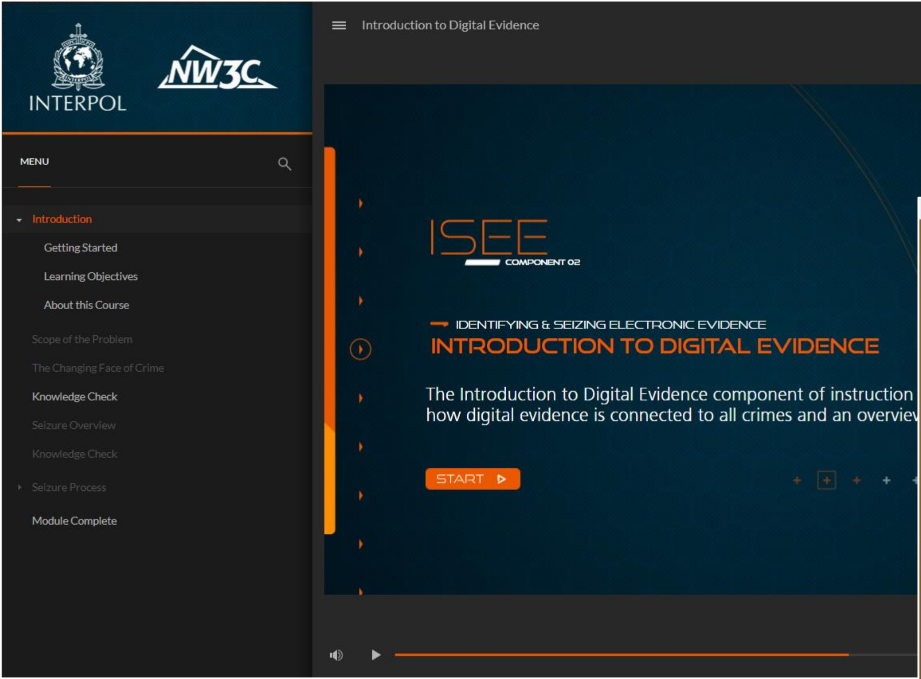
INTERPOL

1. **Capacity building**
   a) Cybercrime
   b) **Digital Evidence**
2. Tools

ACCDP (ASEAN Cyber Capacity Development Project)

- E-learning module on digital evidence identification and seizure (available for LEA's)
- E-learning module on obtaining electronic evidence (2022)

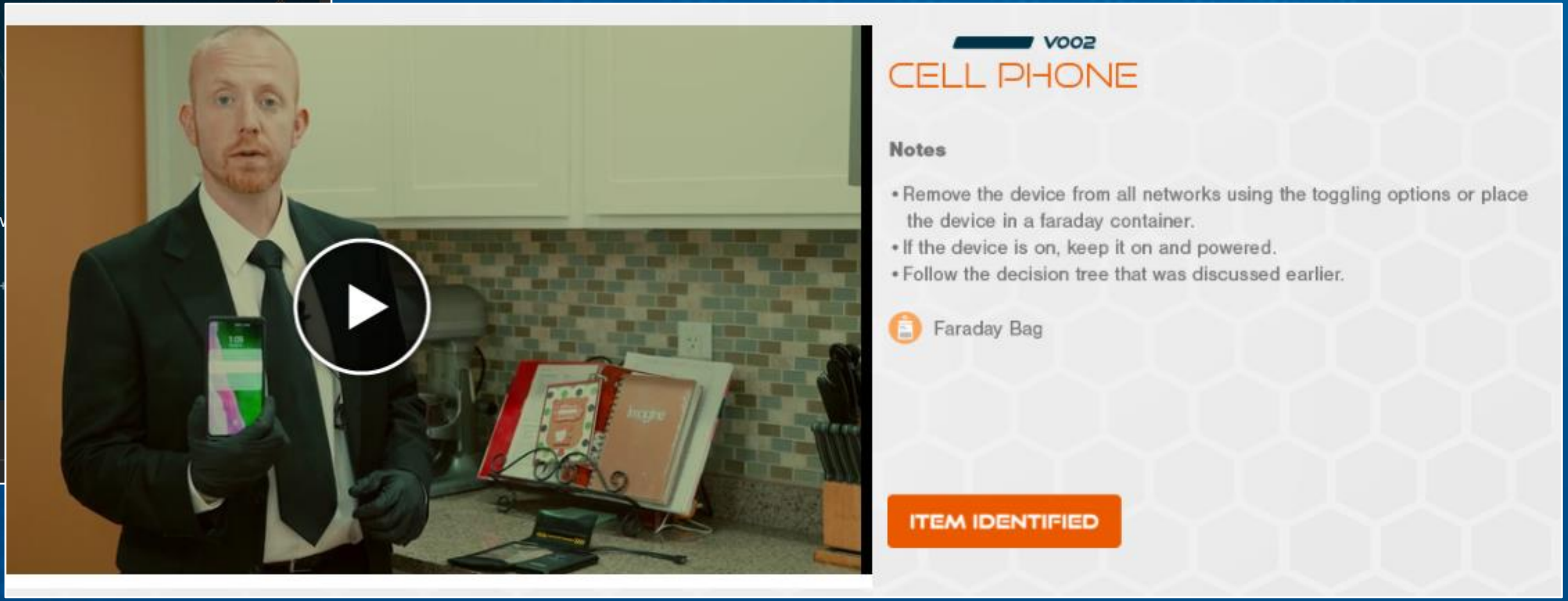




IDENTIFYING & SEIZING ELECTRONIC EVIDENCE

INTRODUCTION TO DIGITAL EVIDENCE

The Introduction to Digital Evidence component of instruction
how digital evidence is connected to all crimes and an overvie



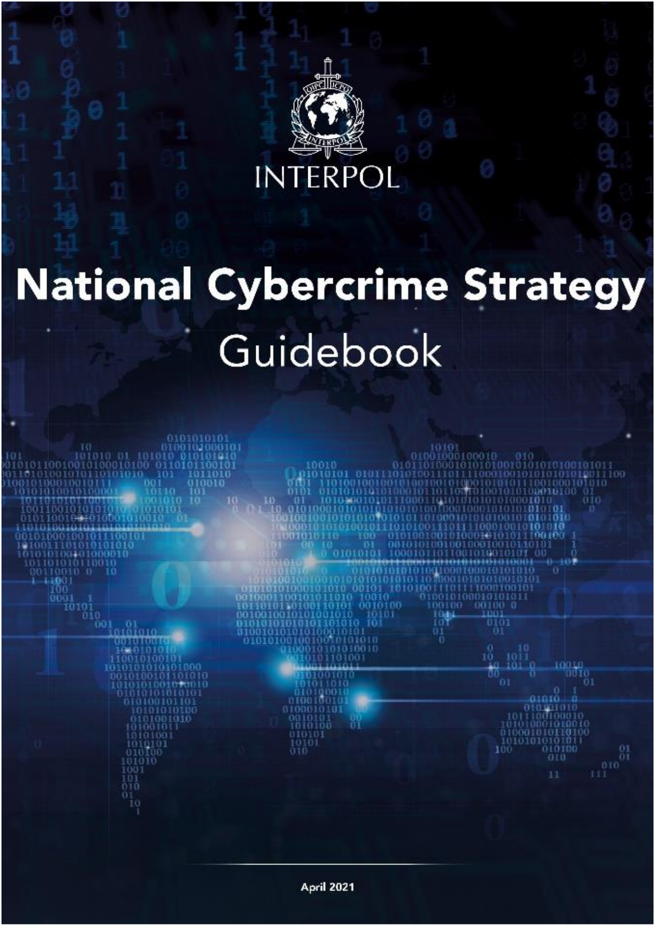
Notes

- Remove the device from all networks using the toggling options or place the device in a faraday container.
- If the device is on, keep it on and powered.
- Follow the decision tree that was discussed earlier.

INTERPOL

1. Capacity building
   a) Cybercrime
   b) Digital Evidence
2. **Tools**

ACCDP (ASEAN Cyber Capacity Development Project)



INTERPOL

National Cybercrime Strategy

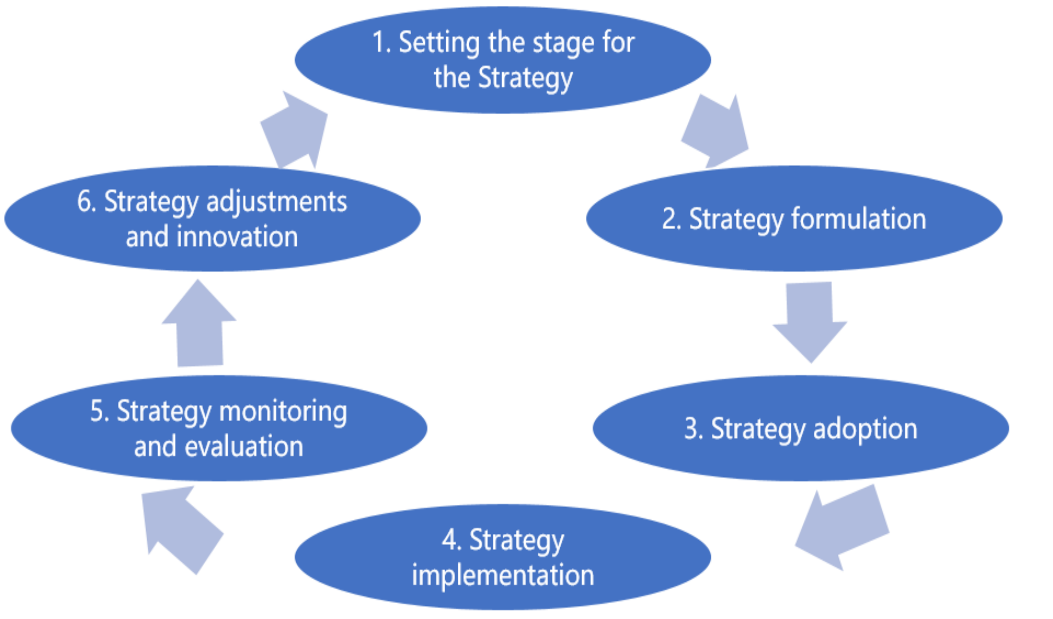
Guidebook

April 2021

= step-by-step guide to draft or revise a national cybercrime strategy

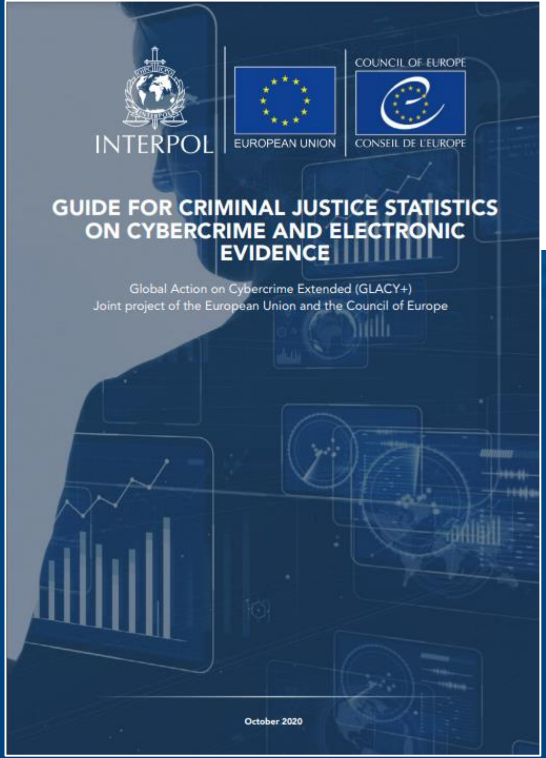
https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project

Strategy Life Cycle:


1. Setting the stage for the Strategy
2. Strategy formulation
3. Strategy adoption
4. Strategy implementation
5. Strategy monitoring and evaluation
6. Strategy adjustments and innovation

INTERPOL

1. Capacity building
   a) Cybercrime
   b) Digital Evidence
2. **Tools**



COUNCIL OF EUROPE

INTERPOL | EUROPEAN UNION | CONSEIL DE L'EUROPE

GUIDE FOR CRIMINAL JUSTICE STATISTICS ON CYBERCRIME AND ELECTRONIC EVIDENCE

Global Action on Cybercrime Extended (GLACY+)
Joint project of the European Union and the Council of Europe

October 2020

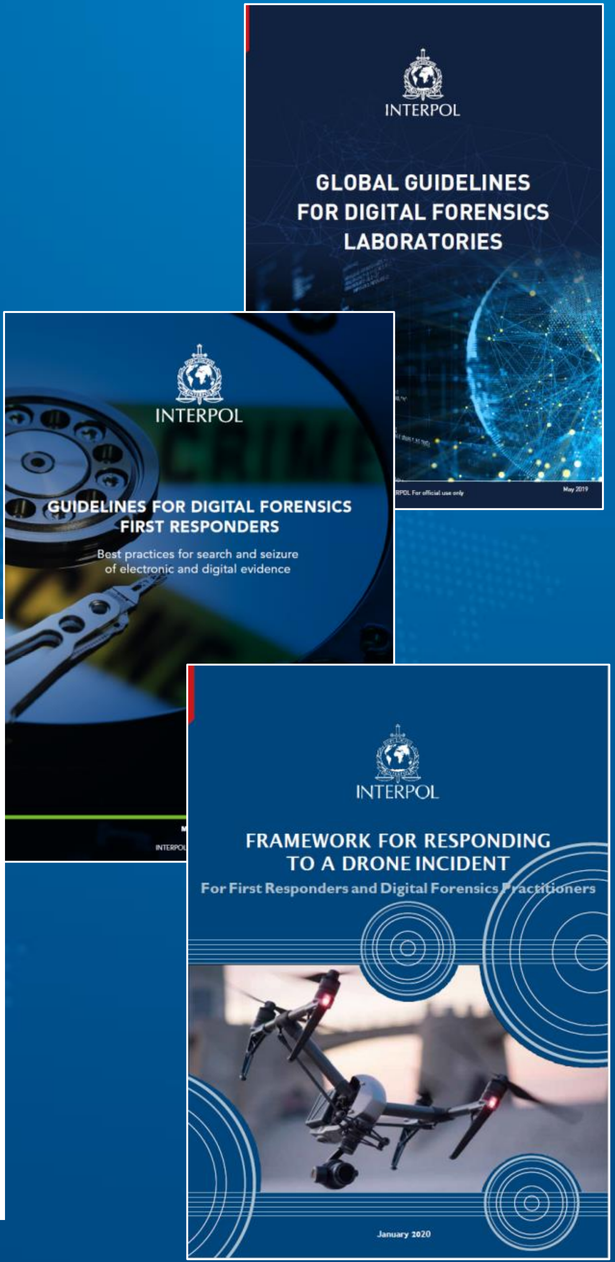
https://www.**interpol**.int/en/Crimes/Cybercrime/Cyber-capabilities-development/**Glacy**

GLACY+ Project

- Guide for criminal justice statistics on cybercrime and electronic evidence (published)
- Law enforcement training strategy (not yet published)

Digital Forensics Laboratory (DFL)

- Global guidelines for Digital Forensics First Responders by INTERPOL Innovation Centre – Digital Forensics Laboratory (IC-DFL)
- Global guidelines for Digital Forensics Laboratories (IC-DFL)
- Framework for responding to a Drone Incident (IC-DFL)



INTERPOL

GLOBAL GUIDELINES FOR DIGITAL FORENSICS LABORATORIES

RPOL For official use only

May 2019

INTERPOL

GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS

Best practices for search and seizure of electronic and digital evidence

INTERPOL

FRAMEWORK FOR RESPONDING TO A DRONE INCIDENT

For First Responders and Digital Forensics Practitioners

January 2020

INTERPOL

Thank You! Questions?

s.hirrle@interpol.int

d.kim@interpol.int

dfl@interpol.int

leader@interpol.int