This training catalogue on combating and preventing cybercrime represents the culmination of more than a decade of dedicated effort by the UNODC Global Programme on Cybercrime to enhance the capabilities of law enforcement agencies (LEAs) and criminal justice practitioners in addressing cyber threats.

In its work, the Global Programme on Cybercrime recognizes that all Member States face similar cybercrime issues but encounter different challenges in countering them. Furthermore, within each country, the level of knowledge and expertise varies among institutions. This is the approach that the Programme has been following since its establishment. In other words, the Global Programme on Cybercrime has been committed to providing Member States with comprehensive, sustainable solutions tailored to their specific contexts and requirements in prevention and combating cybercrime. This approach ensures that the impact and benefits of our initiatives are maximized for individuals and communities worldwide.

Following the establishment of the UNODC Regional Centre for Combatting Cybercrime in Doha discussions about developing a course catalogue gained momentum. In December 2023 experts of the UNODC Global Programme on Cybercrime gathered at the UNODC HQ in Vienna, not only to celebrate the Programme’s 10th anniversary but also to draft the most frequently delivered training programs across the globe over the past decade. This initiative aimed at supporting the operations of the newly established Centre by providing a catalogue of training programs that would be provided by the Centre. Between February 25th and 29th, 2024, fifteen Programme staff members from ten countries across four continents convened at the UN House in Qatar to further this initiative by exchanging their experience and insights regarding the design, delivery, and evaluation of capacity development solutions within the Programme. These insights were derived from the implementation of numerous initiatives over the past decade. By the conclusion of this mission, the team successfully produced the first draft of the course catalogue.

The implementation of a comprehensive course catalogue can significantly boost the capacity of Member staff, empower them with the knowledge, skills, and resources they need to effectively address cyber threats, safeguard national security, and protect citizens, businesses, and critical infrastructure from the impacts of cybercrime.

We are deeply grateful for the invaluable collaboration and support of the State of Qatar and other donor countries of the UNODC Global Programme on Cybercrime. Their trust in the technical expertise and global reach of the Programme has been instrumental in advancing our shared goals across all regions of the world.

This catalogue benefited from the valuable input of UNODC Global Programme on Cybercrime staff: A.M. Chandra Bahadur, Marie-Line Billaudaz, Renata Delgado-Schenk, Nariman Elgendy, Joshua James, Gabriel Juarez, Mariana Kiefer, Jordi Martin, Julian Millan, Himal Ojha, Amr Rahwan, Kamal Sawal Toure and Mustafa Ünal Erten.

Nayelly Loya Marin
Head of the Global Programme on Cybercrime
The UNODC Regional Centre for Combatting Cybercrime in Doha

The UNODC Regional Centre for Combatting Cybercrime in Doha was established in June 2023, and is fully funded by the state of Qatar. It operates as part of the UNODC Global Programme on Cybercrime with the mandate to support Member States in combating cyber-related crimes through provision of capacity building and training activities.

The Centre’s mission is to support the mission of UNODC’s Global Programme on Cybercrime that is to work on strengthening global responses to counter and prevent cyber-related crime through innovative, integrated, and customized solutions. The Centre’s vision is to become the most referred-to cybercrime training centre in the MENA Region and beyond.

The UNODC Regional Centre for Combatting Cybercrime in Doha is aiming at providing training programs and capacity development activities to:

• strengthen capacities of criminal justice practitioners and law enforcement officers on how to investigate, prosecute and adjudicate cybercrime.
• enhance capacities of policy makers and government officials in preventing and countering cybercrime.
• strengthen cooperation mechanisms and synergies between government agencies at the national and international level to prevent and fight against cybercrime.
• increase capacity of the governmental institutions, private sector and CSOs to protect the public especially vulnerable groups as children and women against cybercrime.

The UNODC Regional Centre for Combatting Cybercrime in Doha works closely with official entities such as law enforcement officers, public prosecutors, police officers, museums, schools or universities across Qatar, MENA region and beyond.
The Centre envisages realizing its mission by providing activities under the below five key pillars; each of which is designed to address different aspects of cybercrime prevention and mitigation:

- **Pillar 1: Short-Term Courses:** Centre’s short-term courses offer intensive, focused training on: cyber investigations, digital evidence, digital forensics, prevention of online child sexual abuse, virtual assets, and prevention of cybercrime. These courses are designed predominantly for professionals of the criminal justice sector seeking to strengthen their knowledge, skills and abilities in countering and preventing cybercrime in a condensed timeframe.

- **Pillar 2: Diploma Program with a University:** Collaborating with a renowned university based in Qatar, the Centre plans to offer a comprehensive diploma program in cybercrime prevention and investigation.

- **Pillar 3: Prevention Activities:** Prevention is key to a resilient cyber ecosystem. Centre’s prevention activities aim to educate and raise awareness among individuals, organizations, and society to protect against cybercrime and fostering a safer use of Internet.

- **Pillar 4: Research:** The Centre plans to serve as a hub for cutting-edge research in cybercrime prevention mostly focusing on building a regulatory framework to counter and prevent cybercrime. Research will also support evolution and expansion of evidence-based prevention activities.

- **Pillar 5: Mentoring:** Mentoring plays a crucial role in nurturing future cyber security professionals. With mentoring, UNODC experts/mentors support trained national officials in their work against cybercrime. UNODC mentors will gradually scale back their support as trained criminal justice practitioners become trainers and are able to replicate their training at home and in other countries.

Transversal areas: The Centre acknowledges that collaboration amongst countries, private sector and fostering public-partnership relationships is to increase efficiency and effectiveness of criminal justice response. For this reason, the Centre can offer regional, bilateral, or national training. It also envisages the provision of collaborative training with the private sector.

**Mustafa Ünal Erten**  
Chief of the UNODC Regional Centre for Combatting Cybercrime in Doha
Contents

Foreword 1
The UNODC Regional Centre for Combatting Cybercrime in Doha 2
Global Programme on Cybercrime Training Catalogue 6
    Areas of intervention 7
Area: Cybercrime Investigations 8
    1. Overview Cyber Investigations 8
    2. Investigative Environment 9
    3. Digital Agent: Cyber Patrolling and Undercover Operations 10
    4. Open Source Intelligence Techniques (OSINT) 11
    5. Deep and Darknet Investigations 12
    6. Ransomware Investigation 13
    7. Online Scams Investigation 14
    8. Cyber Attacks Investigation 15
Area: Child Sexual Abuse and Exploitation Material 16
    9. CSAM/CSEM Investigation 16
    10. Peer-to-Peer (P2P) Networks Investigation 17
    11. Victim Identification 18
Area: Digital Forensics 19
    12. Basic Digital Forensics 19
    13. Intermediate Digital Forensics 21
    14. Advance Digital Forensics 22
    15. Digital evidence legal Aspects 23
    16. Litigation Techniques (Advanced) 24
    17. Introduction Technical Digital Evidence Story Telling Training Course 25
Area: Virtual Assets 26
    18. Basic Cryptocurrency Investigation 26
    19. Intermediate Cryptocurrency Investigation 27
    20. Advanced Cryptocurrency Investigation 28
Area: Prevention 29
    21. Cybercrime Prevention 29
Area: General Concepts 30
    22. Understanding Technology and Cybercrime Modality 30
    23. Instructor Development Program (Training of Trainers Course) 31
Global Programme on Cybercrime Training Catalogue

Considering the dimension of the cybercrime risk, the specialized areas that involve and traverse this type of crime, and the diverse capacities that the Member States have to counter it, the Global Programme on Cybercrime promotes long-term, sustainable capacity building to prevent and counter cybercrime through supporting national structures. Our mission is to strengthen global responses to counter and prevent cyber-related crime through innovative, integrated, and customized solutions.

The programme integrates into its package of services technical assistance that goes from preventing to adjudication of crime; detecting to presenting digital evidence to the court; gathering and analyzing evidence; support to the investigation, prosecution and sentencing; in cyber-dependent and cyber-enabled crimes, including online child sexual abuse and exploitation and criminal/illicit use of virtual assets.

Specifically, UNODC draws upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity building, normative assistance, prevention and awareness raising, cooperation, and research and analysis on cybercrime trends. These areas of intervention are delivered through a holistic programmatic approach: capacity building/technical assistance, cooperation, and normative assistance/legal framework.
Areas of intervention

1. **Cyber Investigations.**
   Work to build and strengthen the skills and capacities of criminal justice practitioners and law enforcement officers on how to prevent, disrupt, investigate, prosecute and judge cyber-dependent and cyber-enabled offences.

2. **Online Child Sexual Abuse and Exploitation.**
   Coordinate detection and response between all actors to cases of online child sexual abuse and exploitation and child sexual abuse material, ensuring a victim-centered approach.

3. **Digital Forensics.**
   Work to build and strengthen the skills and capacities of criminal justice practitioners in identifying, seizing, processing, preserving, and reporting digital evidence.

4. **Digital Evidence.**
   Work to build and strengthen the skills and capacities of criminal justice practitioners in identifying, understanding, requesting, analyzing, preserving, and presenting digital evidence.

5. **Virtual Assets.**
   Recognizing the unique features of virtual assets, work to build and strengthen the skills and capacities of criminal justice practitioners and law enforcement officers to investigate, trace and analyze virtual assets.

6. **Prevention.**
   Work to educate people on the safe use of technology to mitigate/ameliorate risks of being victims of crime.
Area: Cybercrime Investigations

1. Overview Cyber Investigations

**Introduction:** This course will provide an overview of the main investigation techniques and legal aspects present in cyber-enabled and cyber-facilitated crimes.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target audience:** Law enforcement, investigators, prosecutors.

**Delivery:** Online/in person.

<table>
<thead>
<tr>
<th>OSINT Basic</th>
<th>OSINT Intermediate</th>
<th>OSINT Advanced*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirements:</strong></td>
<td><strong>Requirements:</strong></td>
<td><strong>Requirements:</strong></td>
</tr>
<tr>
<td>• Basic knowledge of Information and Communication Technology concepts</td>
<td>• Understanding technology foundational course</td>
<td>• Understanding technology foundational course</td>
</tr>
<tr>
<td>• Basic knowledge on cyber-enabled and cyber-facilitated modalities</td>
<td>• Introduction to cybercrime</td>
<td>• Introduction to cybercrime</td>
</tr>
<tr>
<td>• National legislation and frameworks on cyber-enabled and cyber-facilitated crimes</td>
<td>• Basic cyber investigation course</td>
<td>• Basic cyber investigation course</td>
</tr>
<tr>
<td><strong>Syllabus</strong></td>
<td><strong>Syllabus</strong></td>
<td><strong>Syllabus</strong></td>
</tr>
<tr>
<td>• Investigation environment</td>
<td>• Investigation techniques</td>
<td>• AI generative technology</td>
</tr>
<tr>
<td>• OSINT</td>
<td>• AI tools</td>
<td>• Expert testimony</td>
</tr>
<tr>
<td>• P2P</td>
<td>• Virtual reality &amp; Metaverse</td>
<td>• Cross-examination of evidence</td>
</tr>
<tr>
<td>• Deep and darknet</td>
<td>• Cyber patrolling</td>
<td>• Mock trial</td>
</tr>
<tr>
<td>• Reporting</td>
<td>• Practical exercise</td>
<td><strong>Delivery:</strong> In person.</td>
</tr>
<tr>
<td>• Legal aspects</td>
<td><strong>Length:</strong> 5 days</td>
<td><strong>Length:</strong> 5 days</td>
</tr>
<tr>
<td><strong>Length:</strong> 5 days</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The UNODC Global Programme on Cybercrime develops advanced courses based on the urgent needs of the beneficiaries.
Area: Cybercrime Investigations

2. Investigative Environment

**Introduction:** This course will provide the knowledge and skills necessary to develop and establish a secure environment to carry out investigation of cyber-enabled and cyber-facilitated crimes.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target:** Law enforcement and investigators.

**Delivery:** In person.

---

### Overview

**Requirements:**
- Understanding technology foundational course
- Introduction to cybercrime

**Syllabus**
- Compartmentalization
- Cross-contamination
- Isolation
- Data hygiene
- Credentials
- Anonymization
- Infrastructure

**Length:** 2 days
Area: Cybercrime Investigations

3. Digital Agent: Cyber Patrolling and Undercover Operations

Introduction: This course will provide the knowledge and skills necessary to implement undercover operations and cyber patrolling of cyber-enabled and cyber-facilitated crimes.

Course structure: The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

Target audience: Law enforcement, investigators.

Delivery: Online/in person.

Overview

Requirements:
• Understanding technology foundational course
• Introduction to cybercrime

Syllabus
• Investigators profile
• Cyber patrolling
• Channels of communication
• Documentation and collection of evidence
• Under cover techniques
• Legal mandate

Length: 2 day
**Area: Cybercrime Investigations**

4. **Open Source Intelligence Techniques (OSINT)**

**Introduction:** This course will provide OSINT investigation knowledge and skills necessary for law enforcement, investigators and prosecutors to effectively detect, investigate and prosecute cyber-enabled and cyber-facilitated crimes.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target audience:** Law enforcement, investigators.

**Delivery:** Online/in person.

<table>
<thead>
<tr>
<th>OSINT Basic</th>
<th>OSINT Intermediate</th>
<th>OSINT Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirements:</strong></td>
<td><strong>Requirements:</strong></td>
<td><strong>Requirements:</strong></td>
</tr>
<tr>
<td>• Basic knowledge of Information and Communication Technology concepts</td>
<td>• Basic knowledge of Information and Communication Technology concepts</td>
<td>• Basic knowledge of Information and Communication Technology concepts</td>
</tr>
<tr>
<td>• Basic knowledge on cyber-enabled and cyber-facilitated modalities</td>
<td>• Basic knowledge on cyber-enabled and cyber-facilitated modalities</td>
<td>• Basic knowledge on cyber-enabled and cyber-facilitated modalities</td>
</tr>
<tr>
<td>• National legislation and frameworks on cyber-enabled and cyber-facilitated crimes</td>
<td>• National legislation and frameworks on cyber-enabled and cyber-facilitated crimes</td>
<td>• National legislation and frameworks on cyber-enabled and cyber-facilitated crimes</td>
</tr>
<tr>
<td><strong>Syllabus</strong></td>
<td><strong>Syllabus</strong></td>
<td><strong>Syllabus</strong></td>
</tr>
<tr>
<td>• Environment</td>
<td>• Practical exercise</td>
<td>• Case theory</td>
</tr>
<tr>
<td>• Analysis techniques</td>
<td>• Documentation</td>
<td>• Cross-examination</td>
</tr>
<tr>
<td>• Tools</td>
<td>• Reporting</td>
<td>• Litigation techniques</td>
</tr>
<tr>
<td>• Databases</td>
<td>• Case law</td>
<td>• Mock exercise</td>
</tr>
<tr>
<td>• Reporting</td>
<td>• Privacy and human rights</td>
<td><strong>Length:</strong> 5 days</td>
</tr>
<tr>
<td>• Legal aspects</td>
<td><strong>Length:</strong> 3 days</td>
<td><strong>Length:</strong> 5 days</td>
</tr>
</tbody>
</table>

**Length:** 3 days
Area: Cybercrime Investigations

5. Deep and Darknet Investigations

Introduction: This course will provide deep and darknet investigation knowledge and skills necessary for law enforcement, investigators and prosecutors to effectively detect, investigate and prosecute cyber-enabled and cyber-facilitated crimes.

Course structure: The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

Target audience: Law enforcement, investigators, prosecutors.

Delivery: Online/in person.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Syllabus</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deep and Darknet investigations Basic</strong></td>
<td></td>
<td>5 days</td>
</tr>
<tr>
<td>Basic knowledge of Information and Communication Technology concepts</td>
<td>Environment</td>
<td></td>
</tr>
<tr>
<td>Basic knowledge on cyber-enabled and cyber-facilitated modalities</td>
<td>Darknet ecosystem &amp; tools</td>
<td></td>
</tr>
<tr>
<td>National legislation and frameworks on cyber-enabled and cyber-facilitated crimes</td>
<td>Anonymity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forums</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Undercover operations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CoC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reporting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal considerations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal aspects and human rights considerations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Syllabus</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deep and Darknet investigations Intermediate</strong></td>
<td></td>
<td>5 days</td>
</tr>
<tr>
<td>Basic knowledge of Information and Communication Technology concepts</td>
<td>Profiling</td>
<td></td>
</tr>
<tr>
<td>Basic knowledge on cyber-enabled and cyber-facilitated modalities</td>
<td>Advanced search techniques</td>
<td></td>
</tr>
<tr>
<td>National legislation and frameworks on cyber-enabled and cyber-facilitated crimes</td>
<td>Seizing markets</td>
<td></td>
</tr>
<tr>
<td>Deep and Darknet investigations basic</td>
<td>Legal aspects</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Syllabus</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deep and Darknet investigations Advanced</strong></td>
<td></td>
<td>5 days</td>
</tr>
<tr>
<td>Basic knowledge of Information and Communication Technology concepts</td>
<td>The UNODC Global Programme on Cybercrime develops advanced courses based on the urgent needs of the beneficiaries.</td>
<td></td>
</tr>
<tr>
<td>Basic knowledge on cyber-enabled and cyber-facilitated modalities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>National legislation and frameworks on cyber-enabled and cyber-facilitated crimes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Syllabus

*CoC*

Length: 5 days
Area: Cybercrime Investigations

6. Ransomware Investigation

**Introduction:** This course will provide knowledge and skills necessary for law enforcement, investigators and prosecutors to effectively investigate and prosecute ransomware cases.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target audience:** first responders, law enforcement, investigators, prosecutors.

**Delivery:** In person.

---

### Overview

**Requirements:**
- Basic knowledge of Information and Communication Technology concepts
- Basic knowledge on cyber-enabled and cyber-facilitated modalities
- National legislation and frameworks on cyber-enabled and cyber-facilitated crimes
- Any UNODC cyber investigation course basic

**Syllabus**
- Concepts & typologies
- Life cycle
- Encryption
- Payments
- RaaS
- Legal challenges

**Length:** 5 days
7. Online Scams Investigation

Introduction: This course will provide knowledge and skills necessary for law enforcement, investigators and prosecutors to effectively investigate and prosecute online scam cases.

Course structure: The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

Target audience: First responders, law enforcement, investigators, prosecutors.

Delivery: In person.

Overview

Requirements:
- Basic knowledge of Information and Communication Technology concepts
- Basic knowledge on cyber-enabled and cyber-facilitated modalities
- National legislation and frameworks on cyber-enabled and cyber-facilitated crimes
- Any UNODC cyber investigation course basic

Syllabus
- Typologies
- Life cycle
- Mules
- Luring tactics
- Pig butchering
- BEC
- Payments
- Private sector
- Legal considerations

Length: 5 days
Area: Cybercrime Investigations

8. Cyber Attacks Investigation

Introduction: This course will provide knowledge and skills necessary for law enforcement, investigators and prosecutors to effectively investigate and prosecute Cyber-attack cases, with a special attention to Distributed Denial of Service (DDOS).

Course structure: The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

Target audience: First responders, law enforcement, investigators, prosecutors.

Delivery: In person.

Overview

Requirements:
• Basic knowledge of Information and Communication Technology concepts
• Basic knowledge on cyber-enabled and cyber-facilitated modalities
• National legislation and frameworks on cyber-enabled and cyber-facilitated crimes
• Any UNODC cyber investigation course basic

Syllabus
• Concept & typologies
• Life cycle
• Counter measures
• Payments
• Private sector
• DDOS
• Legal aspects

Length: 5 days
Area: Child Sexual Abuse and Exploitation Material

9. CSAM/CSEM Investigation

**Introduction:** This course will provide cybercrime investigation knowledge and skills necessary for law enforcement, investigators and prosecutors to effectively carry out CSAM/CSEM investigations.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target audience:** Investigators, law enforcement, prosecutors, judges.

**Delivery:** In person.

### CSAM/CSEM Investigation (basic)

**Requirements:**
- Basic knowledge of Information and Communication Technology concepts
- National legislation and frameworks on CSAM
- OSINT Investigation (basic)
- Deep and Darknet investigation
- Investigative environment (basic)

**Syllabus**
- Terminology & typologies
- Reactive & proactive investigation
- Platforms
- Phases
- Cooperation
- Virtual CSAM

**Length:** 4 days

### CSAM/CSEM Investigation (intermediate)

**Requirements:**
- Basic knowledge of Information and Communication Technology concepts
- National legislation and frameworks on CSAM
- OSINT Investigation (basic)
- Deep and Darknet investigation
- Investigative environment (basic)
- CSAM/CSEM investigation basic

**Syllabus**
- Grooming
- Abuse
- Exploitation
- Enabling environments

**Length:** 3 days

### CSAM/CSEM Investigation (advanced techniques)

**Requirements:**
- Basic knowledge of Information and Communication Technology concepts
- National legislation and frameworks on CSAM
- OSINT Investigation (basic)
- Deep and Darknet investigation
- Investigative environment (basic)
- CSAM/CSEM investigation basic

**Syllabus**
- Counter-detection strategies
- Livestreaming
- Darknet & deepweb
- Payments
- Luring techniques
- Case law
- Lab exercise

**Length:** 5 days
Area: Child Sexual Abuse and Exploitation Material

10. Peer-to-Peer (P2P) Networks Investigation

Introduction: This course will provide cybercrime investigation knowledge and skills necessary for law enforcement and investigators to effectively detect and investigate CSAM present in P2P networks.

Course structure: The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

Target audience: first responders, law enforcement, investigators, prosecutors.

Delivery: In person.

Overview

Requirements:
• Basic knowledge of Information and Communication Technology concepts
• National legislation and frameworks on CSAM
• Any UNODC Cyber Investigation course

Syllabus
• Concept & typologies
• Architecture & protocols
• Detection software
• Categorization
• Reporting
• Legal aspects
• Case law
• Lab exercise

Length: 5 days
11. Victim Identification

**Introduction:** This course will provide cybercrime investigation knowledge and skills necessary for law enforcement and investigators to effectively carry out CSAM victim identification tasks.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target audience:** Investigators, law enforcement, prosecutors, judges.

**Delivery:** In person.

**CSAM/CSEM Investigation (basic)**

**Requirements:**
- Basic knowledge of Information and Communication Technology concepts
- National legislation and frameworks on CSAM
- Any UNODC Cyber Investigation course
- OSINT Investigation (basic)

**Syllabus**
- Software
- OSINT techniques
- Categorization
- Databases
- Hashing
- Data analysis
- Reporting
- Cooperation
- Legal aspects
- Case law
- Lab exercise

**Length:** 5 days
Area: Digital Forensics

12. Basic Digital Forensics

**Introduction:** Courses are built with free and open-source tools by default. Swap for commercial tools where audience uses specific tools in their labs already.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Delivery:** This course can be conducted in a training facility or online. This course will be structured around classroom-based sessions and computer-based trainings using real-life scenarios.

<table>
<thead>
<tr>
<th>Foundational Digital Forensics Training Course (Basic)</th>
<th>Digital Crime Scene Triage Course (Basic)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> This training course will enable a new investigator or first responder to perform digital forensics using best practices.</td>
<td><strong>Description:</strong> This training course will enable a new investigator or first responder to perform digital crime scene preservation, acquisition and triage using best practices.</td>
</tr>
<tr>
<td><strong>Target:</strong> This training course will give a high-level overview of digital forensic investigation concepts and terminology for non-technical practitioners.</td>
<td><strong>Target:</strong> New Investigators, First Responder</td>
</tr>
<tr>
<td><strong>Requirements:</strong> None / Audience – Anyone</td>
<td><strong>Requirements:</strong> None</td>
</tr>
<tr>
<td><strong>Syllabus</strong></td>
<td><strong>Syllabus:</strong></td>
</tr>
<tr>
<td>• Digital Forensic Concepts</td>
<td>• Standard Operating Procedure (SoP)</td>
</tr>
<tr>
<td>• Theory</td>
<td>• Live Data Forensics basics</td>
</tr>
<tr>
<td>• Terms</td>
<td>• Data source Identification</td>
</tr>
<tr>
<td>• Best Practices</td>
<td>• Chain of Custody (CoC)</td>
</tr>
<tr>
<td><strong>Length:</strong> 2 days</td>
<td>• Data Acquisition</td>
</tr>
<tr>
<td></td>
<td>• Triage</td>
</tr>
<tr>
<td></td>
<td>• Reporting</td>
</tr>
<tr>
<td></td>
<td><strong>Length:</strong> 5 days</td>
</tr>
</tbody>
</table>
Area: Digital Forensics

12. Basic Digital Forensics

Introduction: Course are built with free and open-source tools by default. Swap for commercial tools where audience uses specific tools in their labs already.

Course structure: The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

Delivery: This course can be conducted in a training facility or online. This course will be structured around classroom-based sessions and computer-based trainings using real-life scenarios.

Introduction to Digital Forensic Investigation Procedure (Basic)

Description: This training course will provide theoretical and practical knowledge on standard operating procedures applied in digital forensic investigations for new digital forensic investigators, with a focus on data extraction, analysis, presentation and reporting.

Target: New Digital Forensic Investigators

Requirements: None

Syllabus:
- SoP / Write Blockers
- Data source Identification
- CoC
- Acquisition
- Extraction
- Analysis
- Presentation
- Reporting

Length: 5 days

Introduction to Server Log Analysis (Basic)

Description: This training course allows new digital forensic investigators to request, parse, and analyze internet-related log information to form investigative leads through link analysis.

Target: New Digital Forensic Investigators

Requirements: None

Syllabus:
- Digital Forensic Concepts
- Theory
- Terms
- Best Practices

Syllabus:
- What can you request from ISPs
- Integrity Checking
- How to investigate ISP logs
- Lead generation
- Link analysis
- Server Log Analysis

Length: 2 days
Area: Digital Forensics

13. Intermediate Digital Forensics

Delivery: This course can be conducted in a training facility or online. This course will be structured around classroom-based sessions and computer-based trainings using real-life scenarios.

Target: Digital Forensic Professional or First Responder with experience with digital devices.

- **Introduction to Computer Forensics (Intermediate)**
  - **Description:** This intermediate training course will provide in-depth knowledge and skills to understand file systems and artifacts, preparing an investigator to preserve and analyze digital evidence from computers.
  - **Requirements:**
    - Introduction to Digital Forensic Investigation Procedure
    - Practical experience in computer investigations.
  - **Syllabus:**
    - File Systems
    - Common artifacts
    - Hands on investigation of case study (multiple images)
    - Investigation reporting
  - **Length:** 3 days

- **Live Data Forensics: Extraction and analysis of Random Access Memory (Intermediate)**
  - **Description:** This intermediate training course enables digital forensic professionals and first responders to extract, parse, and analyze volatile data for use in forensic investigation reports.
  - **Requirements:**
    - Introduction to Digital Forensic Investigation Procedure
    - Practical experience in computer investigations.
  - **Syllabus:**
    - SoP
    - Data Source ID
    - CoC
    - Acquisition
    - RAM
    - Extraction
    - Analysis
    - Presentation
    - Reporting
  - **Length:** 5 days

- **Mobile Device Forensic Investigation (Intermediate)**
  - **Description:** This intermediate training course will provide in-depth knowledge and skills to understand file systems and artifacts, preparing an investigator to preserve and analyze digital evidence from mobile devices.
  - **Requirements:**
    - Introduction to Digital Forensic Investigation Procedure
    - Practical experience in mobile investigations.
  - **Syllabus:**
    - File Systems
    - Common artifacts
    - Hands on investigation of case study (multiple images)
    - SoP
    - Data Source ID
    - CoC
    - Acquisition
    - Extraction
    - Analysis
    - Presentation
    - Reporting
  - **Length:** 5 days
Area: Digital Forensics

14. Advance Digital Forensics

**Delivery:** This course can be conducted in a training facility or online. This course will be structured around classroom-based sessions and computer-based trainings using real-life scenarios.

**Target:** Digital Forensic Professional

### Advanced Data Structures and Data Recovery Training Course (Advance)

**Description:** This advanced training course will provide digital forensic investigators with in-depth knowledge on common data structures in computer and mobile devices, and show how to manually parse, analyze and recover data from such data structures.

**Requirements:**
- Any advanced intermediate training on digital forensics
- Practical experience in computer investigations.

**Syllabus:**
- Hex editor
- Data Storage
- Data Structures
- Data Structure Reversing
- Malware Data Structures
- Reversing

**Length:** 5 days

### Network Forensic Investigation and Analysis (Advance)

**Description:** This advanced training course will provide in-depth knowledge and skills to understand network traffic structures and artifacts, preparing an investigator to preserve and analyze digital evidence from a computer network.

**Requirements:**
- Any advanced intermediate training on digital forensics
- Practical experience in computer investigations.

**Syllabus:**
- IPv4/6
- TCP/IP Tracing
- Protocol analysis
- Tracing
- Sniffing
- Network dump analysis

**Length:** 5 days

### Cloud Forensic Investigation and Analysis (Advance)

**Description:** This advanced training course will prepare an investigator to use various tools to collect, preserve, parse, and analyze data from cloud services.

**Requirements:**
- Any advanced intermediate training on digital forensics
- Practical experience in computer investigations.

**Syllabus:**
- Scrapers
- Credentials
- APIs
- CoC from cloud services
- Connected devices

**Length:** 5 days

The Global Programme on Cybercrime customizes advanced courses based on the urgent needs of the beneficiaries.
15. Digital Evidence Legal Aspects

**Introduction:** This course will provide knowledge and skills necessary for law enforcement, investigators, prosecutors and judges to effectively manage digital evidence in case work.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target:** Prosecutors, judges.

**Delivery:** Online/In person.

---

### Digital evidence legal aspects (basic)

**Requirements:**
- Basic knowledge of Information and Communication Technology concepts

**Syllabus**
- Concept and typologies
- Data
- Environments
- Hashing
- Evidence management
- Investigative techniques
- CoC
- Cross-border cooperation
- Private sector request
- Procedural rules
- Good practices

**Length:** 4 days

---

### Digital evidence (intermediate)

**Requirements:**
- Basic knowledge of Information and Communication Technology concepts
- Digital evidence basic

**Delivery:** This course can be conducted in a training facility or online. This course will be structured around classroom-based sessions and computer-based trainings using real-life scenarios.

**Syllabus:**
- Crime scene practice
- Protocols
- SoPs
- Procedural law
- Reporting

**Length:** 4 days
16. Litigation Techniques (Advanced)

**Introduction:** This course will provide knowledge and skills necessary for law enforcement, investigators and prosecutors to effectively litigate and participate in litigation actions before court of cyber-enabled and cyber-facilitated crimes.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target:** Prosecutors, judges.

**Delivery:** Online/in person.

---

### Digital evidence (intermediate)

**Requirements:**
- Basic knowledge of Information and Communication Technology concepts
- Basic knowledge on cyber-enabled and cyber-facilitated modalities
- National legislation and frameworks on cyber-enabled and cyber-facilitated crimes
- Any UNODC cyber investigation course

**Syllabus:**
- Case theory
- Argumentation
- Testimonies
- Litigation techniques
- Mock case practice

**Length:** 5 days
Area: Digital Forensics

17. Introduction Technical Digital Evidence Story Telling Training Course

**Introduction:** This introductory course will cover aspects of physical and digital artifacts and the conversation process from artifact observation to digital evidence that supports investigation hypotheses.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target:** Forensic experts.

**Delivery:** This course will be conducted in a training facility or online. This course will be structured around classroom-based sessions and computer-based training using real-life scenarios.

---

**Digital evidence (intermediate)**

**Requirements:**
None

**Syllabus:**
- Hardware
- Data
- Information
- digital forensic SoP review
- digital artifacts
- investigation hypothesis process
- building an investigation story
- supporting a story with digital evidence
- impartiality – alt hypt.
- reporting as a story

**Length:** 2 days
18. Basic Cryptocurrency Investigation

**Delivery:** This course will be conducted in a training facility. This course will be structured around classroom-based sessions and computer-based trainings using real-life scenarios.

**Target:** Investigators, prosecutors.

### Introduction to blockchain technology and Bitcoin investigation course

**Description:** This introduction training course will help investigators develop an understanding of the underlying technologies around the blockchain, Bitcoin, and perform a basic Bitcoin transaction tracing.

**Requirements:** None

**Syllabus:**
- Cryptocurrency ecosystem
- Blockchain technologies
- Cryptocurrency Addresses
- Cryptocurrency Wallets
- Bitcoin technology
- Basic tracing
- Case studies + hands on

**Length:** 5 days

### Introduction to alternative cryptocurrencies and smart contract investigation

**Description:** This introductory training course will help investigators develop an understanding of the underlying technologies around alternative cryptocurrencies and smart contracts.

**Requirements:**
- A basic understanding of blockchain technologies.

**Syllabus:**
- Types of alternate cryptocurrencies
- Underlying technology of most popular coins
- Definition of smart contracts (Decentralized Finance (DeFi))
- Underlying technology of smart contracts
- Reading smart contracts
- Case studies + hands on

**Length:** 5 days

### Fraud related to virtual assets

**Description:** This introductory training course will help raise awareness of types of fraud related to virtual assets through case studies and trend analysis.

**Requirements:** None

**Syllabus:**
- Fake crypto investments
- Fraudulent cryptocurrency transfer
- Modus operandi
- Identifying fraud
- Case studies + hands on

**Length:** 3 days
Area: Virtual Assets

19. Intermediate Cryptocurrency Investigation

**Delivery:** This course will be conducted in a training facility. This course will be structured around classroom-based sessions and computer-based trainings using real-life scenarios.

**Target:** Investigators.

<table>
<thead>
<tr>
<th>Virtual asset tracing, seizing and forfeiture training course</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> This hands-on, intermediate training course will cover all aspects of advanced virtual asset investigation, seizing virtual assets and introduce virtual asset forfeiture.</td>
</tr>
<tr>
<td><strong>Requirements:</strong></td>
</tr>
<tr>
<td>• Understanding of blockchain and the most popular cryptocurrencies.</td>
</tr>
<tr>
<td><strong>Syllabus:</strong></td>
</tr>
<tr>
<td>• Creation of wallets</td>
</tr>
<tr>
<td>• Transfer of virtual assets</td>
</tr>
<tr>
<td>• Investigation standard operating procedure</td>
</tr>
<tr>
<td>• Search and seizure</td>
</tr>
<tr>
<td>• Chain of custody</td>
</tr>
<tr>
<td>• Seizure</td>
</tr>
<tr>
<td>• Forfeiture best practices</td>
</tr>
<tr>
<td>• Case studies + hands on</td>
</tr>
<tr>
<td><strong>Length:</strong> 5 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intermediate smart contract investigation course</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> This hands-on, intermediate training course will help investigators understand and investigate various types of smart contract technologies.</td>
</tr>
<tr>
<td><strong>Requirements:</strong></td>
</tr>
<tr>
<td>• A basic understanding of blockchain technologies and smart contracts.</td>
</tr>
<tr>
<td><strong>Syllabus:</strong></td>
</tr>
<tr>
<td>• Identifying smart contracts in the wild</td>
</tr>
<tr>
<td>• Creating smart contracts</td>
</tr>
<tr>
<td>• Reading smart contracts</td>
</tr>
<tr>
<td>• Analyzing smart contracts</td>
</tr>
<tr>
<td>• Transaction analysis</td>
</tr>
<tr>
<td>• Chain hopping</td>
</tr>
<tr>
<td>• Case studies + hands on</td>
</tr>
<tr>
<td><strong>Length:</strong> 5 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Digital Forensic Investigation on Cryptocurrency Wallets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> This hands-on, intermediate training course will help investigators understand and investigate various types of smart contract technologies.</td>
</tr>
<tr>
<td><strong>Requirements:</strong></td>
</tr>
<tr>
<td>• A Basic digital forensic skills.</td>
</tr>
<tr>
<td><strong>Syllabus:</strong></td>
</tr>
<tr>
<td>• Computer and mobile search for cryptocurrency addresses,</td>
</tr>
<tr>
<td>• Search for cryptocurrency wallets</td>
</tr>
<tr>
<td>• Analysis of cryptocurrency wallets</td>
</tr>
<tr>
<td>• Hardware wallets</td>
</tr>
<tr>
<td>• Cracking wallet encryption</td>
</tr>
<tr>
<td>• Wallets on computers</td>
</tr>
<tr>
<td>• Wallets on mobile devices</td>
</tr>
<tr>
<td>• Case studies + hands on</td>
</tr>
<tr>
<td><strong>Length:</strong> 4 days</td>
</tr>
</tbody>
</table>
Area: Virtual Assets

20. Advanced Cryptocurrency Investigation

**Delivery:** This course will be conducted in a training facility. This course will be structured around classroom-based sessions and computer-based trainings using real-life scenarios.

**Target:** Investigators.

---

**Virtual asset tracing, seizing and forfeiture training course**

**Description:** This hands-on, intermediate training course will help investigators understand and investigate various types of smart contract technologies.

**Requirements:**
- Understanding of blockchain and the most popular cryptocurrencies.

**Syllabus:**
- Creation of wallets
- Transfer of virtual assets
- Investigation standard operating procedure
- Search and seizure
- Chain of custody
- Seizure
- Forfeiture best practices
- Privacy coins and transactions
- Monero
- Zcash
- Dash
- Coin mixers
- Search for addresses
- Operation strategy
- Case studies + hands on

**Length:** 5 days

---

**Cryptocurrency mining investigations**

**Description:** This hands-on, advanced training course will cover the investigation of cryptocurrency mining farms, how to respond to illicit mining operations, collection analysis of mining machines, digital forensic investigation of mining machine.

**Requirements:**
- Understanding of digital forensic investigation principles, computer networking, blockchain.

**Syllabus:**
- Cryptocurrency mining procedure and technology
- Cryptocurrency mining machines, data extraction from miners
- First response to mining farms
- Confidence building to respond to mining farms
- Tracking remote access in mining machines
- Cryptocurrency tracing from mining machines
- Case studies + hands on

**Length:** 5 days
Area: Prevention

21. Cybercrime Prevention

Introduction: This course aims to equip participants with the knowledge, skills, tools, and abilities needed to raise awareness of safer internet and technology usage, thereby reducing the risks of cybercrime, especially for children and at-risk groups. Upon completion, participants will have the foundational knowledge to disseminate prevention strategies.

Course structure: The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

Target: Educators, caregivers, or individuals who engage daily with children and youth in formal and informal learning settings.

Requirements:
- Basic knowledge of Information and Communication Technology concepts.
- Basic communication skills.

Delivery: Online / in person

Syllabus
- Introduction to Cybercrime
- Cyber security tips
- Cyber Hygiene
- Cyber Interpersonal Violence
- Cyberbullying
- Online Grooming
- Sextortion
- Morphing
- Reporting Mechanism
- Digital citizenship
- Cyber Ethics
- Digital footprint
- Disinformation/Misinformation
- Parental control tools.

Length: 4 days
Area: General Concepts

22. Understanding Technology and Cybercrime Modality

Description: Comprehensive list of technical and legal terms related to cybercrime and digital forensic investigation plus examples of usage. Day two will discuss technical cybercrime issues and threat actors.

Course structure: The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

Target: Investigators, prosecutors, judges

Requirements: None

Delivery: This course will be conducted in a training facility or online. This course will be structured around classroom-based sessions and computer-based trainings using real-life scenarios.

Syllabus
- Technical and legal terms
- why and how does cybercrime work
- threat actors
- cybercrime as a service
- DDoS
- Ransomware

Length: 2 days
Area: General Concepts

23. Instructor Development Program (Training of Trainers Course)

**Description:** This is a specialized training on planning, designing, organizing training programs to provide teaching and coaching to new or less experienced instructors on how to train others. This course will provide a continuous professional development opportunity to improve the skills of instructors, to assist those involved in managing training programmes, to provide standards for the development of training, and to help achieve consistency in the planning, implementation and evaluation of training.

**Course structure:** The course will be structured around a combination of theoretical and practical exercises tailored to national needs.

**Target:** Investigators, prosecutors, judges who are intending to be trainers of certain thematic topic.

**Requirements:** None

**Delivery:** This course will be conducted in a training facility. This course will be structured around student centered learning concept with classroom-based sessions, demonstrations and practical individual and group exercises and assignments conducted in the classroom.

**Syllabus**
- Introduction of the course and participants
- Importance of certification—training policy, consistency, quality...
- The role of an effective instructor.
- Meaning of training, education, learning and development.
- Batori’s Box.
- Training standards and checklists.
- Nine instructional events/steps of Robert Gagne
- Instructional System Design. Training Cycle.
- Adult Learning Principles.
- Andragogy
- Needs Assessment and Task Analysis.
- Instructional Goals and Objectives.
- Blooms Taxonomy.
- Lesson Plans
- Methods of Instruction.
- Instructional strategies for generations.
- Rules of presentation design.
- Effective presentation Skills.
- Test and Evaluation.

**Length:** 5 days