United Nations
Office on Drugs and Crime

GLOBAL PROGRAMME ON CYBERCRIME

Ransomware Investigation

(25 - 26 March 2025)

Objective	To equip investigators with comprehensive knowledge and practical skills necessary for investigating ransomware incidents, from basic concepts to advanced methodologies.
Introduction	Ransomware has emerged as the most significant threat in the cybersecurity landscape. The training program aims to equip participants with the essential knowledge and practical skills required to effectively investigate ransomware incidents.
Course structure	**Theoretical Basics**: Introduction to ransomware, its types, working, and Payment analysis. **Advanced Investigation Techniques**: In-depth analysis of ransomware behaviour, detection methods, and response strategies. **Practical Hands-On Activities**: Real-world scenarios and lab exercises to reinforce learning
Requirements	Familiarisation with operating systems and networking is recommended as a prerequisite for this training. **Hardware**: Computer Workstation for hands-on exercise. **Software (free)**: Virtualization Software (Virtualbox), Digital Forensics Tool (Autopsy), Incident Response Tool (Magnet Response), Data Visualization and OSINT Tool (Maltego Community), Memory Forensics Tool (Volatility), Endpoint Forensics Tool (Redline)
Delivery	In-person
Syllabus	•Understanding of Ransomware attacks. •Forensics analysis and live simulation of malware •Handling and Recovery of data •Case studies + Hands-On Activities
Length	2 days (09:30 – 16:00)

United Nations
Office on Drugs and Crime

GLOBAL PROGRAMME ON CYBERCRIME

Day 1	Understanding Ransomware and Its Key-points
09:00 - 09:30	Registration, Photo Session & Welcome
09:30 - 10:30	Introduction to Ransomware
10:30 - 10:45	Coffee Break
10:45 - 11:45	Ransomware attack Lifecycle
11:45 - 12:45	Encryptions and Payment analysis
12:45 - 13:45	Lunch Break
13:45 - 14:45	Ransomware-as-a-Service (RaaS)
14:45 - 15:00	Break
15:00 - 16:00	Identify and Handle Ransomware Attack
Day 2	**Advance Investigations and Case study**
09:30 - 10:30	Case study of notable Ransomware attacks
10:30 - 10:45	Coffee Break
10:45 - 11:45	Lab setup and Ransomware Investigation Scenario
11:45 – 12:45	Cryptocurrency analysis and Ransomware data Decryption
12:45 - 13:45	Lunch Break
13:45 - 14:45	Role-Playing Incident Response - Exercises.
14:45 - 15:00	Break
15:00 - 16:00	Ransomware Security Measures and Q&A