



Law & Property Rights

Cybercrimes Dr IB

-
- Location: London
 - Date: From 6/1/2025 To 10/1/2025
 - Investment: \$5950 (Excluding VAT)



LONDON ROYAL
ACADEMY

WWW.LONDONRA.COM



Course Introduction

Cybercrimes: Dr. IB is a 5-day intensive course designed to provide a deep dive into the evolving landscape of cybercrime, focusing on the latest threats, attack vectors, and investigative techniques. This course will equip participants with the knowledge and skills to understand, investigate, and combat cybercriminal activities effectively.

Training Method

- Pre-assessment
- Live group instruction
- Use of real-world examples, case studies and exercises
- Interactive participation and discussion
- Power point presentation, LCD and flip chart
- Group activities and tests
- Each participant receives a binder containing a copy of the presentation
- slides and handouts
- Post-assessment






Course Objectives

Upon completion of this course, participants will be able to:

- Understand the various types of cybercrimes: Including hacking, phishing, malware, ransomware, and data breaches.
- Analyze cybercrime trends and threat intelligence: To identify emerging threats and predict future attacks.
- Investigate cybercrimes: Using forensic techniques to gather evidence and reconstruct cyberattacks.
- Understand legal and ethical considerations: Related to cybercrime investigations and prosecutions.
- Develop strategies to prevent and mitigate cybercrime risks: For individuals, organizations, and society.

Who Should Attend?

This course is suitable for:

- Law enforcement officers: Cybercrime investigators, digital forensics specialists, and intelligence analysts.
 - Cybersecurity professionals: Security analysts, threat intelligence analysts, and incident responders.
 - Legal professionals: Prosecutors, defense attorneys, and legal professionals specializing in cybercrime.
 - Government officials: Working in cybersecurity and law enforcement agencies.
 - Academia: Researchers, faculty, and students in cybersecurity, computer science, and criminal justice.
- 

Course Outline

Day 1: Foundations of Cybercrime

- Introduction to Cybercrime:
 - o Defining cybercrime
 - o Types of cybercrimes (hacking, phishing, malware, ransomware, etc.)
 - o The impact of cybercrime on individuals, organizations, and society
- Legal and Ethical Considerations:
 - o Computer crime laws and regulations
 - o Digital evidence collection and admissibility
 - o Ethical considerations in cybercrime investigations

Day 2: Cybercrime Investigation Techniques

- Digital Forensics Fundamentals:
 - o Data acquisition and preservation
 - o Network forensics and traffic analysis
 - o Malware analysis and reverse engineering
- Incident Response and Handling:
 - o Incident response planning and procedures
 - o Investigating cyberattacks and data breaches
 - o Collecting and analyzing digital evidence

Day 3: Advanced Cyber Threats and Emerging Technologies

- Advanced Persistent Threats (APTs):
 - o Tactics, techniques, and procedures (TTPs) of APTs
 - o Detecting and responding to APTs
- The Internet of Things (IoT) Security:
 - o IoT vulnerabilities and attacks
 - o Securing IoT devices and networks

Course Outline

- Cryptocurrency and Blockchain:
 - o Cybercrime related to cryptocurrency
 - o Investigating cryptocurrency transactions

Day 4: Cybercrime and the Dark Web

- The Dark Web and Deep Web:
 - o Understanding the dark web and its role in cybercrime
 - o Investigating activities on the dark web
 - o Dark web intelligence gathering
- Cybercrime Markets and Underground Forums:
 - o Analyzing cybercrime markets and underground forums
 - o Identifying and tracking cybercriminals

Day 5: Future Trends and Challenges in Cybercrime

- Emerging Cyber Threats:
 - o Artificial intelligence and cybercrime
 - o Biometric security and privacy
 - o The impact of 5G and other emerging technologies
- Combating Cybercrime:
 - o International cooperation and collaboration
 - o Building a global response to cybercrime
 - o The role of technology and innovation in combating cybercrime

Registration & Payment

Complete & Mail to London Royal Academy or email
registration@londonra.com



Registration Form

- Full Name (Mr / Ms / Dr / Eng)
- Position
- Telephone / Mobile
- Personal E-Mail
- Official E-Mail
- Company Name
- Address
- City / Country

Payment Options

- Please invoice me
- Please invoice my company





Terms & Conditions

Complete & Mail to London Royal Academy or email
registration@londonra.com



Cancellation and Refund Policy

Delegates have 14 days from the date of booking to cancel and receive a full refund or transfer to another date free of charge. If less than 14 days' notice is given, then we will be unable to refund or cancel the booking unless on medical grounds. For more details about the Cancellation and Refund policy, please visit www.londonra.com/terms-and-conditions/

Registration & Payment

Please complete the registration form on the course page & return it to us indicating your preferred mode of payment. For further information, please get in touch with us

Course Materials

The course material, prepared by the LRA, will be digital and delivered to candidates by email

Certificates

Accredited Certificate of Completion will be issued to those who attend & successfully complete the programme.

Travel and Transport

We are committed to picking up and dropping off the participants from the airport to the hotel and back.



VENUES

 LONDON

 BARCELONA

 KUALA LUMPER

 AMSTERDAM

 ISTANBUL

 SINGAPORE

 PARIS

 DUBAI

OUR PARTNERS



THANK YOU

CONTACT US

 +44 2080898183

 info@londonra.com

 **Mayfair Office:** 1 Mayfair Pl, 1st Floor,
W1J 8AJ London, UK

 **City Office** :124 City Road,
EC1V 2NX London, UK

 **Dubai Office** :Park Towers,
DIFC Office 7

CH No: 15668865



LONDON ROYAL
ACADEMY
WWW.LONDONRA.COM