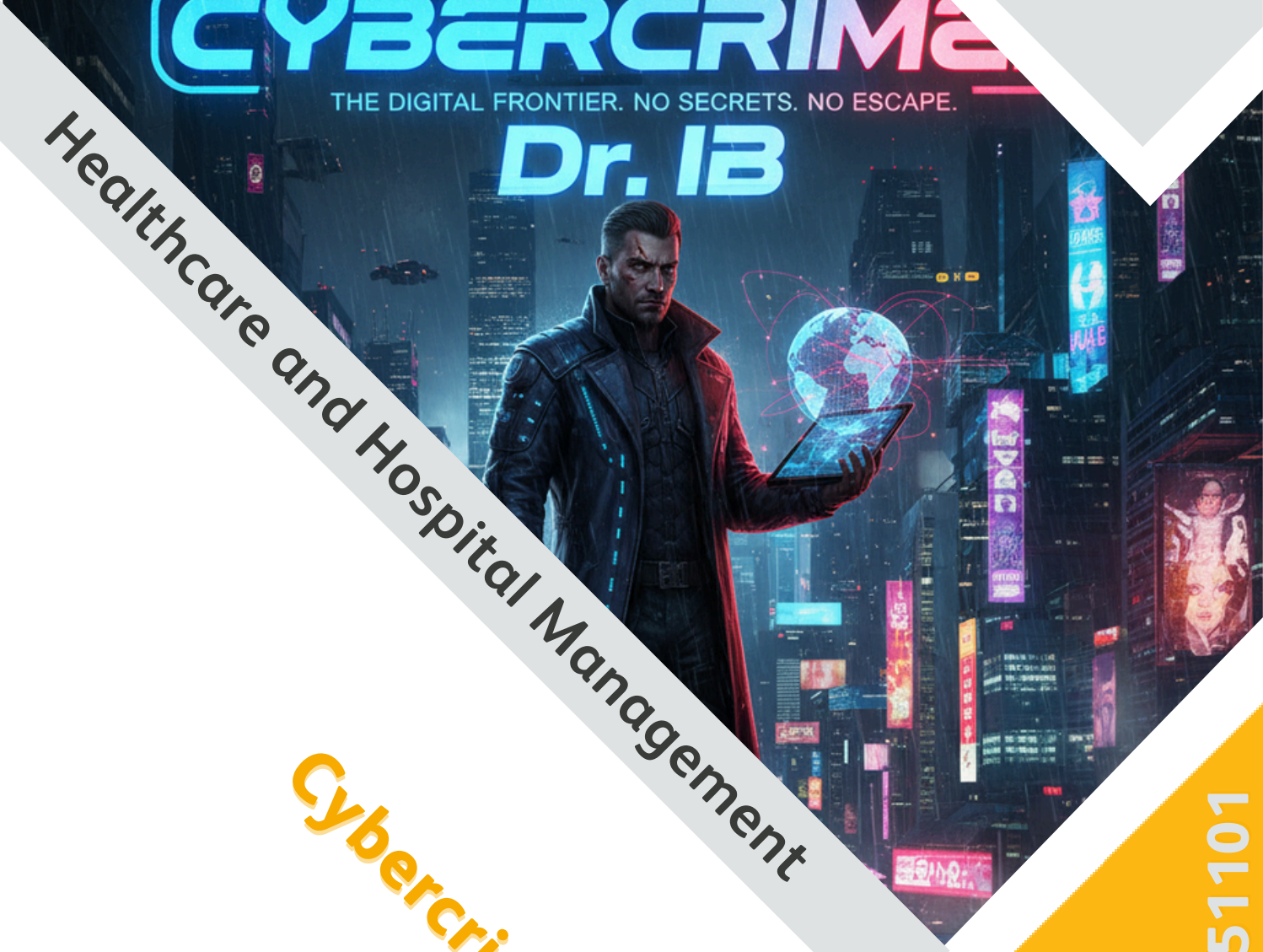

Healthcare and Hospital Management

Cybercrimes Dr IB

Code: 251101

FUTURE CENTRE
مركز المستقبل

futurecentre.net

Course Introduction

The digital landscape is the new frontier for criminal activity, with cybercrimes posing a significant and evolving threat to individuals, organizations, and national security. These crimes are not just technologically complex but also span multiple jurisdictions, requiring a sophisticated understanding of law, technology, and investigative techniques. This course, led by an expert perspective (Dr. IB), provides a comprehensive framework for understanding, investigating, and preventing cybercrime.

This intensive program delves into the anatomy of various cyber offenses, from hacking and phishing to ransomware attacks and digital fraud. Participants will learn the fundamental principles of digital forensics, evidence collection, and the legal protocols required to build a prosecutable case. Through a combination of theoretical knowledge, real-world case studies, and practical labs, this course equips professionals with the skills to effectively combat cybercriminal activity in a structured and methodical manner.

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

- **Categorize** different types of cybercrimes and understand the motivations and methodologies behind them.
- **Apply** a structured investigative framework (e.g., the “Dr. IB” methodology) to a cybercrime incident.
- **Identify** and **preserve** digital evidence from various sources (computers, mobile devices, cloud environments) in a forensically sound manner.
- **Understand** the legal and ethical considerations for cybercrime investigations, including search warrants, privacy laws, and chain of custody.
- **Analyze** attack vectors and indicators of compromise (IOCs) to trace threat actors and understand the scope of a breach.
- **Develop** strategies for incident response, evidence documentation, and presenting findings in a legal context.

Who Should Attend?

This course is designed for professionals involved in security, law enforcement, legal, and IT fields:

- **Law Enforcement Officers** and **Digital Forensic Investigators**
- **Cybersecurity Analysts** and **Incident Responders**
- **IT Auditors** and **Risk & Compliance Professionals**
- **Corporate Security Directors** and **Legal Counsel**
- **Network and Systems Administrators** responsible for security
- **Students** of cybersecurity, criminal justice, or law

Course Outline

Day 1: Foundations of Cybercrime

Morning Session: The Cybercrime Landscape

- Introduction: Defining Cybercrime and its Economic/Social Impact.
- Typology of Cybercrimes: Hacking, Fraud, Identity Theft, Cyberstalking, Ransomware.
- The “Dr. IB” Investigative Framework: A Methodical Approach.

Afternoon Session: The Legal Framework

- Key Cybercrime Laws and Regulations (e.g., Computer Fraud and Abuse Act, GDPR).
- Jurisdictional Challenges in International Cybercrime.
- Obtaining Search Warrants and Legal Authority for Digital Searches.

Day 2: Digital Forensics Fundamentals

Morning Session: Crime Scene & Evidence Handling

- The Principles of Digital Forensics: ACPA (Acquisition, Preservation, Analysis, Presentation).
- Chain of Custody: Documentation and Evidence Integrity.
- Live vs. Static Evidence Acquisition: Best Practices.

Afternoon Session: Hands-On Acquisition

- Imaging Hard Drives and Mobile Devices using forensic tools (e.g., FTK Imager, Autopsy).
- **Practical Lab:** Create a forensic image of a provided storage device and verify its hash.

Day 3: Forensic Analysis and Triage

Morning Session: Data Analysis

- Analyzing File Systems (NTFS, FAT, APFS) for evidence.
- Finding Artifacts: Browser History, Email, USB Device Connections, and Metadata.

Afternoon Session: Network Forensics

- Introduction to Packet Analysis with Wireshark.
- Identifying Malicious Network Traffic and IOCs.
- **Practical Lab:** Analyze a packet capture file to identify a command-and-control (C2) server address.

Course Outline

Day 4: Investigating Specific Cybercrimes

Morning Session: Financial and Fraud Investigations

- Tracing Cryptocurrency Transactions (Bitcoin, Ethereum).
- Investigating Phishing Campaigns and Business Email Compromise (BEC).

Afternoon Session: Malware and Intrusion Analysis

- Basics of Malware Analysis: Static and Dynamic Techniques.
- Investigating a Ransomware Attack: From Initial Access to Data Encryption.
- **Case Study:** Dissect a real-world data breach case from start to finish.

Day 5: Incident Response and Courtroom Presentation

Morning Session: The Incident Response Lifecycle

- Preparation, Identification, Containment, Eradication, and Recovery.
- Writing a Technical and Legal Investigative Report.

Afternoon Session: Capstone and Testimony

- **Capstone Exercise:** Conduct a full investigation on a simulated cybercrime scenario, from evidence collection to report writing.
- How to Testify as an Expert Witness: Presenting Digital Evidence in Court.
- **Course Recap:** “Dr. IB” Methodology Review and Best Practices.
- **Final Q&A and Certification.**

المقدمة

يُمثل المجال الرقمي آفاقًا جديدة للنشاط الإجرامي، حيث تُشكل الجرائم الإلكترونية تهديدًا كبيرًا ومتطورًا للأفراد والمؤسسات والأمن القومي. ولا تقتصر هذه الجرائم على تعقيدها التكنولوجي فحسب، بل تمتد أيضًا إلى ولايات قضائية متعددة، مما يتطلب فهمًا متعمقًا للقانون والتكنولوجيا وأساليب التحقيق. تُقدم هذه الدورة، التي يُقدمها خبير (الدكتور آي بي)، إطارًا شاملًا لفهم الجرائم الإلكترونية والتحقيق فيها ومنعها.
يتعمق هذا البرنامج المكثف في تشريح مختلف الجرائم الإلكترونية، من القرصنة والتصيد الاحتيالي إلى هجمات برامج الفدية والاحتيال الرقمي. سيتعلم المشاركون المبادئ الأساسية للتحليل الجنائي الرقمي، وجمع الأدلة، والبروتوكولات القانونية اللازمة لبناء قضية قابلة للمقاضاة. من خلال مزيج من المعرفة النظرية ودراسات الحالة الواقعية والمختبرات العملية، تُزود هذه الدورة المهنيين بالمهارات اللازمة لمكافحة أنشطة الجرائم الإلكترونية بفعالية وبطريقة منظمة ومنهجية.

طريقة التدريب

- التقييم المسبق
- تدريب جماعي مباشر
- استخدام أمثلة واقعية ودراسات حالة وتمارين
- مشاركة ونقاش تفاعلي
- عرض تقديمي باستخدام باور بوينت، وشاشة LCD، ولوح ورقي
- أنشطة واختبارات جماعية
- يحصل كل مشارك على ملف يحتوي على نسخة من العرض التقديمي
- شرائح ومطبوعات
- التقييم اللاحق

أهداف الدورة

عند إكمال هذه الدورة بنجاح، سيكون المشاركون قادرين على:

- **تصنيف** أنواع مختلفة من الجرائم الإلكترونية وفهم الدوافع والمنهجيات وراءها.
- **تطبيق** إطار تحقيق منظم (على سبيل المثال، منهجية "الدكتور آي بي") على حادثة جريمة إلكترونية.
- **تحديد** الأدلة الرقمية من مصادر مختلفة (أجهزة الكمبيوتر، الأجهزة المحمولة، بيئات السحابة) والحفاظ **عليها** بطريقة سليمة من الناحية الجنائية.
- **فهم** الاعتبارات القانونية والأخلاقية للتحقيقات في الجرائم الإلكترونية، بما في ذلك أوامر التفتيش، وقوانين الخصوصية، وسلسلة الحراسة.
- **تحليل** متجهات الهجوم ومؤشرات الاختراق (IOCs) لتتبع الجهات الفاعلة في التهديد وفهم نطاق الاختراق.
- **تطوير** استراتيجيات للاستجابة للحوادث، وتوثيق الأدلة، وتقديم النتائج في سياق قانوني

من ينبغي أن يهتم؟

تم تصميم هذه الدورة للمحترفين العاملين في مجالات الأمن وإنفاذ القانون والقانون وتكنولوجيا المعلومات:

- **ضباط إنفاذ القانون** والمحققون **الجنائيون الرقميون**
- **محللو الأمن السيبراني** والمستجيبون **للحوادث**
- **مدققو تكنولوجيا المعلومات** ومحترفو **المخاطر والامتثال**
- **مديري الأمن المؤسسي** والمستشارين **القانونيين**
- **مسؤولو الشبكات والأنظمة** المسؤولون عن الأمن
- **طلاب** الأمن السيبراني أو العدالة الجنائية أو القانون

محتويات الكورس

اليوم الأول أساسيات الجريمة الإلكترونية

الجلسة الصباحية: مشهد الجرائم الإلكترونية

- المقدمة: تعريف الجريمة الإلكترونية وأثرها الاقتصادي والاجتماعي.
- تصنيف الجرائم الإلكترونية: القرصنة، الاحتيال، سرقة الهوية، المطاردة الإلكترونية، برامج الفدية.
- الإطار التحقيقي "دكتور آي بي": نهج منهجي.

جلسة بعد الظهر: الإطار القانوني

- القوانين واللوائح الرئيسية المتعلقة بالجرائم الإلكترونية (على سبيل المثال، قانون الاحتيال وإساءة استخدام الكمبيوتر، واللائحة العامة لحماية البيانات).
- التحديات القضائية في الجرائم الإلكترونية الدولية.
- الحصول على أوامر التفتيش والسلطة القانونية للبحث الرقمي

اليوم الثاني أساسيات الطب الشرعي الرقمي

الجلسة الصباحية: مسرح الجريمة والتعامل مع الأدلة

- مبادئ الطب الشرعي الرقمي: ACPA (الاستحواذ، الحفظ، التحليل، العرض).
- سلسلة الحراسة: سلامة الوثائق والأدلة.
- الاستحواذ على الأدلة المباشرة مقابل الاستحواذ على الأدلة الثابتة: أفضل الممارسات.

جلسة بعد الظهر: اكتساب عملي

- تصوير محركات الأقراص الصلبة والأجهزة المحمولة باستخدام أدوات الطب الشرعي (على سبيل المثال، FTK Imager، Autopsy).
- **المختبر العملي:** إنشاء صورة جنائية لجهاز تخزين مقدم والتحقق من التجزئة الخاصة به

اليوم الثالث التحليل الجنائي والفرز

الجلسة الصباحية: تحليل البيانات

- تحليل أنظمة الملفات (NTFS، FAT، APFS) للحصول على الأدلة.
- العثور على القطع الأثرية: سجل المتصفح، والبريد الإلكتروني، واتصالات أجهزة USB، والبيانات الوصفية.

جلسة بعد الظهر: تحليلات الشبكات

- مقدمة إلى تحليل الحزم باستخدام Wireshark.
- تحديد حركة المرور الضارة على الشبكة ومؤشرات IOC.
- **المختبر العملي:** تحليل ملف التقاط الحزمة لتحديد عنوان خادم الأوامر والتحكم (C2).

محتويات الكورس

اليوم الرابع التحقيق في جرائم إلكترونية محددة

الجلسة الصباحية: التحقيقات المالية والاحتيالية

- تتبع معاملات العملات المشفرة (بيتكوين، إيثريوم).
- التحقيق في حملات التصيد الاحتيالي واختراق البريد الإلكتروني للشركات (BEC).

جلسة بعد الظهر: تحليل البرامج الضارة والاختراقات

- أساسيات تحليل البرامج الضارة: التقنيات الثابتة والديناميكية.
- التحقيق في هجوم برامج الفدية: من الوصول الأولي إلى تشفير البيانات.
- **دراسة الحالة:** تحليل حالة خرق البيانات في العالم الحقيقي من البداية إلى النهاية

اليوم الخامس الاستجابة للحوادث والعرض في قاعة المحكمة

الجلسة الصباحية: دورة حياة الاستجابة للحوادث

- التحضير، والتحديد، والاحتواء، والاستئصال، والاسترداد.
- كتابة تقرير تحقيقي فني وقانوني.

جلسة بعد الظهر: المشروع الختامي والشهادة

- **تمرين التخرج:** إجراء تحقيق كامل في سيناريو محاكاة الجريمة الإلكترونية، من جمع الأدلة إلى كتابة التقارير.
- كيفية الإدلاء بشهادتك كشاهد خبير: تقديم الأدلة الرقمية في المحكمة.
- **ملخص الدورة:** مراجعة منهجية "دكتور آي بي" وأفضل الممارسات.
- **الأسئلة والأجوبة النهائية والشهادة**

Terms & Conditions

Complete & Mail to future centre or email

Info@futurecentre.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
https://futurecentre.net/

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 future centre, 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.

Registration & Payment

Complete & Mail to future centre or email

Info@futurecentre.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

Course Calander:

- 05/01/2026 - 09/01/2026 Click Now
- 06/04/2026 - 10/04/2026 Click Now
- 06/07/2026 - 10/07/2026 Click Now
- 05/10/2026 - 09/10/2026 Click Now

VENUES

- LONDON
- BARCELONA
- KUALA LUMPER
- AMSTERDAM
- DAMASCUS
- ISTANBUL
- SINGAPORE
- PARIS
- DUBAI

OUR PARTNERS

THANK YOU

CONTACT US

+963 112226969

+963 953865520

Info@futurecentre.com

Damascus - Victoria - behind Royal Semiramis hotel

FUTURE CENTRE
مركز المستقبل

futurecentre.net