

BOOK SYLLABUS

10 Modules with 6 Sections Each

Chapter 1: Foundations of Cybercrime	1-30
1. Introduction to Cybercrime	
2. Classification of Cyber Offences	
3. Cybercrime Trends and Statistics	
4. Cybercriminal Ecosystems	
5. Impact on Society and Economy	
6. Emerging Challenges in Cybercrime	
Chapter 2: Legal Frameworks for Cybercrime	31-63
1. International Cyber Laws	
2. National Cybercrime Legislation	
3. Jurisdiction in Cyberspace	
4. Data Protection and Privacy Laws	
5. Electronic Transactions Regulations	
6. Legal Compliance Requirements	
Chapter 3: Digital Evidence Fundamentals	64-96
1. Nature of Digital Evidence	
2. Types of Digital Evidence	
3. Sources of Digital Evidence	
4. Evidence Preservation Principles	
5. Integrity and Authenticity	
6. Chain of Custody Procedures	
Chapter 4: Cybercrime Investigation Techniques	97-151
1. Investigation Planning	
2. Evidence Collection Methods	
3. Digital Crime Scene Management	
4. Interview and Interrogation Techniques	
5. Case Documentation	
6. Investigation Reporting	
Chapter 5: Digital Forensics	152-173
1. Computer Forensics	
2. Mobile Device Forensics	
3. Network Forensics	

4. Cloud Forensics
5. Malware Analysis
6. Forensic Tools and Platforms

Chapter 6: Cyber Offences and Evidence Analysis **174-176**

1. Hacking and Unauthorized Access
2. Identity Theft Investigations
3. Financial Cybercrime Analysis
4. Cyberstalking and Harassment Cases
5. Ransomware Investigations
6. Evidence Correlation Techniques

Chapter 7: Admissibility of Digital Evidence **177-180**

1. Rules of Evidence
2. Electronic Records in Courts
3. Expert Witness Testimony
4. Evidence Authentication
5. Challenges to Admissibility
6. Judicial Interpretation

Chapter 8: Privacy, Ethics, and Human Rights **181-184**

1. Privacy Rights in Digital Investigations
2. Ethical Issues in Cybercrime Investigations
3. Surveillance and Monitoring
4. Human Rights Considerations
5. Data Retention Policies
6. Balancing Security and Privacy

Chapter 9: Advanced Topics in Cybercrime **185-189**

1. Artificial Intelligence and Cybercrime
2. Cryptocurrency Crimes
3. Dark Web Investigations
4. IoT Security Incidents
5. Cyber Terrorism
6. Cross-Border Cybercrime Cooperation

Chapter 10: Future Directions and Case Studies

190-194

1. Landmark Cybercrime Cases
2. Digital Evidence Case Analysis
3. Emerging Technologies and Law
4. Cybersecurity Policy Development
5. Future Investigation Techniques
6. Research Directions and Innovations