|  |  |
| --- | --- |
| Part-I Introduction to Cybercrimes | Crimes  Cybercrimes/Cyber terrorism/Cyberspace, Digital forensics education, training and awareness |
| Part-II Policies and Laws | Computer crimes |
| Part-III Prevention |  |
| Part-IV Tools and Techniques for combating cybercrimes |  |
|  |  |

Laws/act/policies/Developing countries where lack of resources/

Security threats, new and emerging threats, types, etc.

Mobile crimes

Networking crimes, virtual machines forensics

Internet crimes, Terrorist use of the internet, Social media and Big Data, cloud forensics,

Prevention/counter measures

Investigation

Preparing for Prosecution and Testifying

Cyber Investigative Roles, High-tech investigations of cybercrime, report writing

Digital forensics, Forensics Labs , tools and techniques

Seizure of Digital Information

Conducting Cyber Investigations

Digital Forensics and Analyzing Data, Lab considerations

Investigating Insider Threat Using Enterprise Security Management

the rise of cyber liability insurance

Operating System, File systems, legacy file system, registries, etc