DIPLOMA IN CYBERCRIME INVESTGATION

SYLLABUS:

BOOK NO.1- CYBERCRIME BASICS.

(1) Cybercrime, tools and techniques.

1.0 Objectives.
1.1 Definition of cybercrime.
1.2 Tools and techniques used to commit cybercrime.
1.3 Types of cybercrime.
1.4 Characteristics of cybercrime.
1.5 Questions for self-study.
1.6 Answers for self-study.

(2) Identification of Computer Peripherals.

2.0 Objectives.
2.1 Characteristics of computer.
2.2 Composition of computer.
2.3 Other components of computer.
2.4 Questions for self-study.
2.5 Answers for self-study.

(3) Computer Network.

3.0 Objectives:
3.1 Types of Networking Technologies.
3.2 Difference between internet and intranet.
3.3 Wireless Fidelity WI-FI.
3.4 Network Topologies.
3.5 Network Devices.
3.6 Network commands.
3.7 Questions for self-study.
3.8 Answers for self-study

(4) Internet Protocol (IP) , ISP , IP and ISP Infrasturcture.

4.0 Introduction.
4.1 Concept of Internet Service Provider (ISP).
4.2 Internet Protocol (IP) Address.
4.3 Internet and ISP.
4.4 Internet Infrastructure.
4.5 ISP Infrastructure.
4.6 Domain Name System (DNS).
4.7 DNS Servers.

(4) E-mail.

5.0 Objectives.
5.1 History of Email.
5.2 What is Email.
5.3 Email service providers.
5.4 Uses of Email.
5.5 Mail server.
5.6 How Email works.
5.7 Email Address.
5.8 Anatomy of Email message.
5.9 How to send Email
5.10 Advantage of Email.
5.11 Disadvantage of Email.
5.12 Email tracing.
5.13 Email tracking.
5.14 Questions for self-study.
5.15 Answers for self-study.

(5) Social Networking sites.

6.0 Objectives.
6.1 Social networking site.
6.2 Types of social networking site.
6.3 Important social networking sites in India.
6.4 Advantages and disadvantages of social networking site.
6.5 Threats of social networking sites.
6.6 Mobile social networking.
6.7 Using social networking sites for Investigation.
6.8 Questions for self-study.
6.9 Answers for self-study.

(7) Basics of cell phone investigation.

7.0. Objectives.
7.1 Introduction.
7.2 How does mobile phone works.
7.3 Mobile Technologies.
7.4 Cell phone crimes.
7.5 Mobile crime Investigation.
7.6 Information available with mobile service providers.
7.7 Mobile number portability.
7.9 Seizure panchnama content of Mobile handset.
7.9 Understanding 1G to 5G.
7.10 Questions for self-study.
7.10 Answers for self-study.

(8) IP Address and GPRS, GSM AND GPRS Architecture.

8.0 Objectives.

8.1 IP Address and GPRS.
8.2 GSM Network Architecture.
8.3 GPRS Network Architecture.
8.4 Questions for self-study.
8.5Answers for self-study.

(9) Information Technology Amendment Act 2008.

9.0 Objectives.
9.1 Introduction.
9.2 Information Technology Act 2000.
9.3 Offences under IT Act.
9.4 Mapping of IT Act 2000 with Bhartiya Naya Sanhita 2023.
9.5 Questions for self-study.
9.6 Answers for self-study.

(10) Digital evidence Basics.

10.0. Objectives.
10.1. Introduction.
10.3. Digital evidence, characteristics and its source.
10.4. Digital Evidence vs. physical evidence.
10.5. Relevance of Digital evidence.
10.6.Types of Digital evidence.
10.7. Collection of Digital evidence.
10.8. Tools for Digital Evidence.
10.9. Computer forensics.
10.10. Classification of cyber forensics.
10.11. Five key elements of cyber forensics process.
10.12. Data created unanimously.
10.13. Steps for crime scene investigation.
10.14. Request for preservation of Digital Evidence.
10.15. Questions for self-study.
10.16. Answers for self-study.

(11) Mobile and Cyber forensics.

11.0 Objectives.
11.1 Introduction.
11.2 Types of Mobile device operating system.
11.3 Hardware characteristics of mobile phone.
11.4 Types of mobile crime.
11.5 Evidence in mobile Devices.
11.6 Memory organization in mobile devices.

11.7 File system optimized for flash memory.
11.8 Extraction and analysis techniques of phone memory.
11.9 Tools for extraction and analysis of mobile device.
11.10 Challenges associated with mobile phone forensics.
11.11 Mobile device forensics Guidelines.
11.12 Flow chart of mobile seizure.
11.13 Computer Forensics.
11.14 Evidence gathering Doctrine.
11.15 Classification of Cyber Forensics.
11.16 Five key elements of Cyber Forensics.
11.17 Expectations from Cyber Forensics Analyst.
11.18 Questions for self-study.
11.19 Answers for self-study.

(12) Search and seizure of Digital evidence and Legal provisions for Digital evidence.

12.0 Objectives.
12.1 Principals of Digital forensics.
12.2 Precautions to be taken while collecting Digital evidence.
12.3 Data created unintentionally.
12.4 Steps for Digital crime scene investigation.
12.5 Preliminary review scene of offence.
12.6 Investigative tools and equipment.
12.7 Evaluating scene of offence.
12.8 Preliminary interview at scene of offence.
12.9 Scene of offence.
12.10 Collection of Digital evidence.
12.11 Procedure for gathering evidence from live system.
12.12 Forensics Duplication.
12.13 Sealing and transportation.
12.14 Pancha Nama and seizure proceedings.
12.15 Chain of custody form.
12.16 Digital evidence collection form.
12.17 Hashing.
12.18 Questions to be asked to FSL.
12.19 Case Law regarding search and seizure of Digital Evidence.
12.20 Legal provisions for search and seizure.
12.21 Questions for self-study.
12.22 Answers for self-study.

(13) Tools for Cyber forensics.

13.0 Objectives.
13.1 Introduction.
13.2 Definition of Cyber forensics.
13.3 Methodology of Computer forensics.
13.4 Authentication tools.

13.5 Analysis tools.
13.6 Memory analysis tools.
13.7 Forensics Workstations.
13.8 Widely used tools and software’s for cyber forensics.
13.9 Questions for self-study.
13.10 Answers for self-study.

BOOK NO.2- CYBERCRIME INVESTIGATION PART-1

(1) Content in First Information Report (FIR) of cybercrime.

1.0 Objectives.
1.1FIR of credit/Debit card.
1.2FIR of Insurance/Job/Loan/Lottery/All online frauds.
1.3FIR of Matrimony/Gift fraud.
1.4FIR of social media cybercrimes.
1.5FIR of Email related cybercrimes.
1.6FIR of Data/source code theft crime.
1.7FIR of Mobile/Laptop theft.
1.8FIR of DOS/DDOS attack.
1.9Questions for self-study.
1.10Answers for self-study.

(2) How to report Cybercrime.

2.0 Objectives.
2.1 Help Line 1930
2.2 How to Utilize National cybercrime Reporting portal.
2.3 Steps for National cybercrime reporting portal.
2.4 Questions for self-study.
2.5 Answers for self-study.

(3) How to stop and refund fraud money of Victim.

3.0. Objectives.
3.1. Introduction.
3.2. Different methods to stop fraud money and refund to victim.
3.4. Questions for self-study.
3.5. Answers for self-study.

(4) Pre-investigation Assessment.

4.0 Objectives.
4.1 Pre-investigation Assessment.
4.2Preliminary review of scene of offence.
4.3 Evaluating the scene of offence.
4.4 Preliminary interview at the scene of offence.
4.5 Pre-investigation Technical Assessment.
4.6 Issuance of preservation notice.

4.7 Flow chart of Standard operating procedure for Investigation.
4.8 Questions for Self-study.
4.9 Answers for self-study.

(5) Format of Letter to Intermediatory and their Email ids.

5.0. Objectives.
5.1. Letter formats to intermediary.
5.2 Mail ids of Intermediaries.
5.3 Questions for self-study.
5.4 Answers for self-study.

(6) Call Detail Record (CDR) Analysis.

6.0 Objectives.
6.1 Introduction.
6.2 Guidelines of DOT.
6.3 Apps to know, MSP of mobile number.
6.4 Types of CDR.
6.5 CDR Analysis.
6.6 Questions for self-study.
6.7 Answers for self-study.

(7)Email Investigation and Header Analysis.

7.0 Objectives.
7.1 Email, Mailer, Mail server, Mailbox.
7.2 Email Related Cyber Crimes.
7.3 Working of Email
7.4 Mail Server?
7.5 Components of Email.
7.6 Components of E-Mail Header
7.7 Most known mail service providers.
7.8 Email Header Analysis.
7.9 Steps in Email Header Analysis.
7.10 Requesting details from intermediaries.
7.11 Collection of Email as evidence.
7.12 Google Takeout.
7.13 Presentation of Email as evidence in court.
7.14 Case study.
7.15 Investigation of Case Study.
7.16 Questions for self-study.
7.17 Answers for self-study.

(8) Fake Website Investigation.

8.0 Objectives.

8.1 What is Website?
8.2 Components of Website.
8.3 What is fake website.
8.4 Types of fake website.
8.5 How to identify fake website.
8.6 Types of cybercrime by using fake website.
8.7 Steps in fake website investigation.
8.8 Identification of IP Address of fake website.
8.9 What is web defacement and its investigation.
8.10 Case study.
8.11 Investigation of case study.
8.12 Questions for self-study.
8.13 Answers for self-study.

(9) Investigation from Bank Account.

9.0 Objectives.
9.1 Bank account and its different types.
9.2 Legal provisions to ask for Bank Details.
9.3 How bank account statement is useful in investigation.
9.4 Different modes of Money transfer.
9.5 Abbreviations in Bank account statement.
9.6 Banking Terminology.
9.7 UPI.
9.8 Duties of Investigating officer after receiving Bank statement.
9.9 Questions for self-study.
9.10 Answers for self-study.

(10) Hotspot Dongle Tracking.

10.0 Objectives:
10.1 Portable Hotspot Tracking.
10.2 Internet Dongle.
10.3 How criminals exploit Hotspot Dongle.
10.4 Steps to investigate Hotspot Dongle.
10.5 Questions for self-study.
10.6 Answers for self-study.

(11) Virtual Identity Tracking.

11.0 Objectives:
11.1 Virtual Identity Tracking.
11.2 How criminals exploit WhatsApp virtual Identity.
11.3 How to trace virtual number.
11.4 For what, Questions to be asked to WhatsApp.
11.5 Types of response from WhatsApp and Investigation steps.

11.6 Questions for self-study.
11.7 Answers for self-study.

(12) VPN and Proxy Tracking.

12.0 Objectives.
12.1 VPN and Security.
12.2 The pros and cons of using VPN.
12.3 VPN services for computer.
12.4 VPN services for Android phone.
12.5 Can I trust VPN.
12.6 Proxy Tracking.
12.7 Types of proxies for Anonymity.
12.7 How to track criminal who is using Proxy.
12.9 Questions for self-study.
12.10. Answers for self-study.

(13) Spoof call/VIOP call Tracking.

13.0. Objectives.
13.1. Spoof call/VoIP call.
13.2. What is a spoof call/
13.3. What is a VOIP call?
13.4. Challenges in tracking spoof/VOIP Call.
13.5. Methods to track spoof and VOIP Call.
13.6. Spoof SMS.
13.7. Crimes done with Spoof/VOIP Call.
13.8. Questions for self-study.
13.9. Answers for self-study.

(14) Investigation of Facebook related crime.

14.0. Objectives.
14.1. Report of Facebook crime and sections applied.
14.2. Seizure of Evidence from Complainant.
14.3. How to take screen shot of Facebook page and post.
14.4. Request Letter to Facebook.
14.5. Facebook Reply.
14.6. How to access Facebook report.
14.7. correspondence to email service providers.
14.8. Email Reply.
14.9. Correspondence to Internet service providers.
14.10. Reply from ISP’s.
14.11. Letter to Mobile service provider.
14.12. Seizure from accused.
14.13. Questions for self-study.

14.14. Answers for self-study.

(15) Investigation of Wallet Frauds.

15.0 Objectives.
15.1 Introduction.
15.2 Steps to investigate Wallet Frauds.
15.3 BHIM UPI Fraud.
15.4 Investigation of BHIM UPI Fraud.
15.5. Questions for self-study.
15.6 Answers for self-study.

(16) IP Logger

16.0 Objectives.
16.1 Introduction.
16.2 What is Grabify/ Blasze.
16.3 Crimes in which Grabify/ Blasze. Link is used by Criminals.
16.4 Uses of Grabify / Blasze.Link.
16.5 How to creat and use Grabify / Blasze.Link.
16.6 Details we get by using Grabify/ Link.
16.7 Questions for self- study.
16.8 Answers for self-study.

(17) Sim box fraud and Investigation.

17.0 Objectives.
17.1 Introduction
17.2 Case study.
17.3 Steps to investigate SIM box call.
17.4 Questions for self-study.
17.5 Answers for self-study.

(18) Googalization of Target.

18.0 Objectives.
18.1 Introduction.
18.2 Steps of Googalization
18.3 Letter to Google.
18.4 Reply from Google.
18.5 Google My Activity.
18.6 Questions for self-study.
18.7 Answers for self-study.

(19) Malware Analysis.

19.0 Objectives.
19.1 Malware.
19.2 Worms.
19.3 Virus and its types.
19.4 Trojan and its type.
19.5 Malware Analysis tools.
19.6 Questions for self-study.
19.7 Answers for self-study.

(20) Information Gathering from suspect’s mobile number.

20.0 Objectives.
20.1 How to find Telecommunication service provider (TSP)?
20.2 How to get bank information from mobile number?
20.3 How to get criminal’s address from mobile number?
20.4 How to get social media information from mobile number?
20.5 How to get travel history of suspect mobile number?
20.6 How to get vehicle information from mobile number?
20.7 How to get Google timeline activity of suspect mobile number?
20.8 Questions for self-study.
20.9 Answers for self-study.

(21) Drone Investigation.

21.0 Objective.
21.1 Drone.
21.2 Different types of Drones.
21.3 Software’s used in Drones.
21.4 Drone Forensics.
21.5 Advantages and Disadvantages of Drone.
21.6 Uses of Drones.
21.7 Storage devices in Drones.
21.8 Tools used in Drone Forensics.
21.9 Crimes involving Drones.
21.10 Investigation of Drone related crimes.
21.11 Tracing Drone related crimes suspect.
21.12 Questions for self-study.
21.13 Answers for self-study.

(22) Artificial Intelligence (AI) powered cybercrime.

22.0 Objectives.
22.1 What is AI, how does it work, and its importance.
22.2 Advantages and Disadvantages of AI.
22.3 Types of AI.
22.4 Where AI is Used?

22.5 AI’s ethical challenges.
22.6 Types of AI operated crime.
22.7 Investigation steps in AI operated crime.
22.8 What information to be sought from service provider, in detection of AI crime/
22.9 How to trace accused of AI operated crime.
22.10 Questions for self-study.
22.11 Answers for self-study.

(24) Chat GPT.

23.0 Objectives.
23.1 What is Chat GPT?
23.2 Who created Chat GPT?
23.3 How does Chat GPT works?
23.4 Uses of Chat GPT.
23.5 Advantages and Limitations of Chat GPT.
23.6 How to open account of Chat GPT?
23.7 How to write prompt for Chat GPT?
23.8 How criminals can Leverage LLM’s for cybercrime.
23.9 Questions for self-study.
23.10 Answers for self-study.

(24) CCTV Footage Analysis.

24.0 Objectives.
24.1 Introduction.
24.2 Types of Digital Video Recorder (DVR)
24.3 Types of CCTV Cameras.
24.4 Types of NVR’s.
24.5 Types of CCTV video footage video files.
24.6 Equipment’s required for CCTV Footage retrieval.
24.7 Collection of CCTV footage in storage Device.
24.8 CCTV footage seizure panchnama.
24.9 Questions for self-study.
24.10 Answers for self-study.

(25) Hash Value.

25.0 Objectives.
25.1What is Hash Values?
25.2Importance of Has Value.
25.3 Different Algorithms used in computing Hash Value.
25.4 How to calculate Hash Value.
25.5 Case laws regarding Hash Values.

(26) Audio-Video recording of scene of crime.

26.0 Objectives.
26.1 Introduction.
26.2 Videography provisions in BNSS 2023.
26.3 Methods of searching crime scene.
26.4 Procedure to conduct search and seizure.
26.5 Procedure of processing scene of crime.
26.6 Audio-videography during search and seizure.
26.7 Procedure for storage and transportation.
26.8 DO’s and DON’T’s by IO during video recording.
26.9 Procedure of Audio-Video recording of scene of crime.
26.10 Drawing of seizure Memo.
26.11 Documentation and fallow-up at police station.
26.12 App based solution e-Sakashya.
26.13 Aid-Memoir of Audio-video recording.
26.14 Questions for self-study.
26.15 Answers for self-study.

(27) Audio/Video Sampling.

27.0 Objectives.
27.1 Introduction.
27.2 Crimes in which, voice samples are taken.
27.3 Legal provisions regarding voice sampling in India.
27.4 Precautions in taking voice samples.
27.5 Procedure of voice sampling.
27.6 post-voice sampling procedure.
27.7 Storage and handling of voice samples.
27.8 Sending samples to FSL.
27.9 Post analysis procedure.
27.10 Questions for self-study.
27.11 Answers for self-study.

(28) Forensics GAIT Analysis/Comparison.

28.0 Objectives.
28.1 Forensic GAIT Analysis.
28.2 Classification of GAIT Pattern.
28.3 Forensics GAIT Analysis approaches.
28.4 Forensics GAIT Analysis features/ Parameters.
28.5 Factors affecting GAIT pattern and analysis.
28.6 Steps in recreation of crime scene for forensics Gait Analysis.
28.7 Steps in GAIT Analysis at FSL.
28.8 Example of recreation of crime scene.
28.9 Questions for self-study.
28.10 Answers for self-study.

(29) Requisition Letter to FSL.

29.0 Objectives.
29.1 Format of requisition Letter to FSL.
29.2 Information to be furnished by IO to FSL.
29.3 Questions to be asked in case of Computer as a target to FSL in cybercrime.
29.4 Questions to be asked in case of threatening Emails.
29.5 Questions to be asked in case of creation of Obscene profile.
29.6 Questions to be asked to FSL, in case of Computer as an instrument.
29.7 Questions to be asked to FSL, when we provide Mobile Handset for Analysis.
29.8 Sample of requisition letter to FSL.
29.9 Questions for self-study.
29.10 Answers for self-study.

(30) Submission and proving of Digital/Electronic Evidence in court of Law.

30.0 Objective.
30.1 Introduction.
30.2 Production of Secondary Digital Evidence.
30.3 Admissibility of Secondary Digital Evidence.
30.4 Proving secondary Digital Evidence.
30.5 Bhartiya Sakshya Adhiniyam 2023 sec 63(2)(4).
30.6 Format of Certificate u/s 63(4) of BSA. 2023 Part A, B.
30.7 Format of Bankers Book Evidence Act 2,8 (a)(b)(c) 1891.
30.8 Case Law of Supreme Court on Submission of Digital Evidence.
30.9 Questions for self-study.
30.10 Answers for self-study.

(31) Website Blocking.

31.0 Objectives.
31.1 What is Website Blocking?
31.2 Crimes in which website blocking is done?
31.3 Steps to be taken in Blocking Website.
31.4 Procedure for submitting complaint to Director CERT-In.
31.5 Letter format for Blocking Website.
31.6 Questions for self-study.
31.7 Answers for self-study.

(32) Mutual Legal Assistance (MLA) And Letters Rogatory (LR).

32.0 Objectives.
32.1 Mutal Legal Assistance in criminal matter.
32.2 Procedure for making Letters Rogatory request.
32.3 Procedure for making Mutual Legal Assistance request.
32.4 Service of Summons, Notices and judicial processes.
32.5 Miscellaneous provisions relating to Reciprocal arrangements.
32.6 Informal Request.

32.7 Extradition Request.
32.8 Questions for self-study.
32.9 Answers for self-study.

(33) Open-source Intelligence Tools.

33.0 Objectives.
33.1 Introduction.
33.2 Role of OSINT in cyber security.
33.3 Open-source software’s, Advantages and Disadvantages.
33.4 Closed source software’s, Advantages and Disadvantages.
33.5 Types of OSINT and their uses.
33.6 Questions for self-study.
33.7 Answers for self-study.

BOOK NO.3- CYBERCRIME INVESTIGATION PART 2

Different types of cyber frauds, Modus, Investigation, case studies-

(1) Task fraud.

1.0 Objectives
1.1 Introduction.
1.2 Modus operandi of Task fraud.
1.3 Flow chart of Task Fraud.
1.4 Expected area of evidence in Task fraud.
1.5 Standard operating procedure of investigation of Task fraud.
1.6 Case study of Task fraud.
1.7 Investigation of case study of Task fraud.
1.8 Questions for self-study.
1.9 Answer for self-study.

Digital arrest/Courier fraud.

2.0 Objectives.
2.1 Introduction.
2.2 Modus operandi of Digital arrest / Courier fraud.
2.3 Flow chart of modus of Digital arrest fraud.
2.4 Expected area of evidence in Digital arrest / FedEx fraud.
2.5Standard operating procedure of investigation of Digital arrest/ FedEx fraud.
2.6 Flow chart of Investigation of Digital arrest fraud.
2.7 Case study of Digital arrest and FedEx fraud.
2.8 Investigation of case study.
2.9 Questions for self-study.
2.10 Answer for self-study.

(3) Stock market fraud.

3.0 Objectives.
3.1 Introduction.
3.2 Modus operandi of MSEB or MNGL fraud.
3.3 Expected area of evidence in MSEB or MNGL fraud.
3.4 Flow chart of modus of MSEB or MNGL fraud.
3.5 Standard operating procedure of investigation of MSEB or MNGL fraud.
3.6 Flow chart of investigation of MSEB/MNGL Fraud.
3.7 Case study of MSEB or MNGL fraud.
3.8 Investigation of MSEB or MNGL fraud case study.
3.9 Questions for self-study.

3.10 Answer for self-study.

(4) MSEB/MNGL bill fraud.

4.0 Objectives.
4.1 Introduction.
4.2 Modus operandi of Stock market fraud.
4.3 Flow chart of modus of Stock market fraud.
4.4 Expected area of evidence in Stock market fraud.
4.5 Standard operating procedure of investigation of Stock market fraud.
4.6 Flow chart of investigation of stock market fraud.
4.7 Flow chart of investigation of stock market fraud.
4.8 Case study of Stock market fraud
4.9 Investigation of case study of Stock market fraud.
4.10 Questions for self-study.
4.11 Answer for self-study.

(5) Customer care/Helpline number fraud.

5.0 Objectives.
5.1 Introduction.
5.2 Modus operandi of Costumer care or Helpline number Fraud.
5.3 Flow chart of Costumer care or Helpline number Fraud.
5.4 Expected area of evidence in Costumer care or Helpline number Fraud.
5.5 Standard operating procedure of investigation of Costumer care or Helpline number Fraud.
5.6 Flow chart of Investigation of Customer care fraud.
5.7 Case study of Costumer care or Helpline number Fraud.
5.8 Investigation of case study of Costumer care or Helpline number Fraud.
5.9 Questions for self-study.
5.10 Answer for self-study.

(6) UPI/ OTP Fraud.

6.0 Objectives.
6.1 Introduction.
6.2 Modus operandi of UPI or OTP Fraud.
6.2 Flow chart of modus operandi of UPI or OTP Fraud.
6.3 Expected area of evidence in UPI or OTP Fraud.
6.4 Standard operating procedure of investigation of UPI or OTP Fraud.
6.5 Flow chart of investigation of UPI fraud.
6.6 Standard operating procedure of investigation of UPI fraud.
6.7 Case study of UPI or OTP Fraud.
6.8 Investigation of case study of UPI or OTP Fraud.
6.9 Questions for self-study.
6.10 Answer for self-study.

(7) Job Fraud.

7.0 Objectives
7.1 Introduction.
7.2 Types of Job frauds.
7.3 Modus operandi of Job fraud.
7.4 Flow chart of Modus operandi of Job fraud.
7.5 Expected area of evidence in Job fraud.
7.6 Standard operating procedure of investigation of Job fraud.
7.7 Case study of Job fraud.
7.8 Investigation of case study of Job fraud.
7.9 Questions for self-study.
7.10 Answer for self-study

(8) KYC Updation fraud.

8.0 Objectives
8.1 Introduction.
8.2 Modus operandi of KYC updating fraud.
8.3 Flow chart of modus operandi of KYC updating fraud.
8.4 Expected area of evidence in KYC updating fraud.
8.5 Standard operating procedure of investigation of KYC updating fraud.
8.6 Case study of KYC updation fraud.
8.7 Investigation of case study of KYC updation fraud.
8.8 Questions for self-study.
8.9 Answer for self-study.

(9) OLX Fraud.

9.0 Objectives
9.1 Introduction.
9.2 Modus operandi of OLX fraud.
9.3 Expected area of evidence in OLX fraud.
9.4 Flow chart of modus operandi of OLX fraud.
9.5 Standard operating procedure of investigation of OLX fraud.
9.6 Case study of OLX fraud.
9.7 Investigation of case study of OLX fraud.
9.8 Questions for self-study.
9.9 Answer for self-study.

(10) Matrimony / Gift fraud.

10.0 Objectives
10.1 Introduction.
10.2 Modus operandi of Matrimony or Gift fraud.
10.3 Flow chart of Matrimony or Gift fraud.

10.4 Expected area of evidence in Matrimony or Gift fraud.
10.5 Standard operating procedure of investigation of Matrimony or Gift fraud.
10.6 Flow chart of investigation of Matrimony/Gift Fraud.
10.7 Case study of Matrimony or Gift fraud.
10.8 Investigation of case study of Matrimony or Gift fraud.
10.9 Questions for self-study.
10.10 Answer for self-study.

(11) Lottery fraud.

11.0 Objectives
11.1 Introduction.
11.2 Modus operandi of Lottery fraud.
11.3 Flow chart of modus operandi of Lottery fraud.
11.4 Expected area of evidence in Lottery fraud.
11.5 Standard operating procedure of investigation of Lottery fraud.
11.6 Flow chart of investigation of Lottery Fraud.
11.7 Case study of Lottery fraud.
11.8 Investigation of case study of Lottery fraud.
11.9 Questions for self-study.
11.10 Answer for self-study.

E-commerce Fraud.

12.0 Objectives
12.1Introduction.
12.2 Modus operandi of E Commerce fraud.
12.3 Flow chart of modus operandi of E Commerce fraud.
12.4 Expected area of evidence in E Commerce fraud.
12.5 Standard operating procedure of investigation of E Commerce fraud.
12.6 Flow chart of investigation of E-Commerce fraud.
12.7 Case study of E Commerce fraud.
12.8 Investigation of case study of E Commerce fraud.
12.9 Questions for self-study.
12.10 Answer for self-study.

(13) QR Code Fraud.

13.0 Objectives.
13.1 What do you mean by QR Code?
13.2 QR Code Scam
13.3 Modus operandi of QR Code Scam.
13.4 Steps in investigation of QR code scam
13.5 How to trace accused of QR Code fraud.
13.6 Flow chart of modus operandi of QR Code fraud.
13.7 Expected areas of Evidence.

13.8 Case study.
13.9 Investigation of Case study.
13.10 Precautions in QR Code scam.
13.11 Questions for self-study.
13.12 Answers for self-study.

(14) Online Loan Fraud.

14.0 Objectives
14.1 Introduction.
14.2 Modus operandi of Online loan fraud.
14.3 Flow chart of modus operandi of Online loan Fraud.
14.4 Expected area of evidence in Online loan fraud.
14.5 Standard operating procedure of investigation of Online loan fraud.
14.6 Flow chart of investigation of Loan Fraud.
14.7 Case study of Online loan fraud.
14.8 Investigation of case study of Online loan fraud.
14.9 Questions for self-study.
14.10 Answer for self-study.

(15) SIM Swapping Fraud.

15.0 Objectives
15.1 Introduction.
15.2 Modus operandi of Sim swapping fraud.
15.3 Flow chart of modus operandi of Sim swapping Fraud.
15.4 Expected areas of Evidence in sim swapping fraud.
15.5 Standard operating procedure of investigation of Sim swapping fraud.
15.6 Flow chart of investigation of SIM Swapping fraud.
15.7 Case study of sim swapping fraud.
15.8 Investigation of case study of Sim swapping fraud.
15.9 Questions for self-study.
15.10 Answer for self-study.

(16) Social media- Based Fraud.

16.0 Objectives
16.1 Introduction.
16.2 Modus operandi of social media-based fraud.
16.3 Flow chart of Modus operandi of social media-based Fraud.
16.4 Expected area of evidence in social media-based fraud.
16.5 Standard operating procedure of investigation of social media-based fraud.
16.6 Case study of social media-based fraud.
16.7 Investigation of case study of social media-based fraud.
16.8 Questions for self-study.
16.9 Answer for self-study.

(17) ATM Fraud.

17.0 Objectives
17.1 Introduction.
17.2 Modus operandi of ATM fraud.
17.3 Flow chart of modus operandi of ATM Fraud.
17.4 Flow chart of investigation of ATM Fraud.
17.5 Expected area of evidence in ATM fraud.
17.6 Standard operating procedure of investigation of ATM fraud.
17.7 Case study of ATM fraud.
17.8 Investigation of case study of ATM fraud.
17.9 Questions for self-study.
17.10 Answer for self-study.

(18) Stalking/ Sextortion.

18.0 Objectives
18.1 Introduction.
18.2 Modus operandi of Cyber stalking/sextortion fraud.
18.3 Flow chart of modus operandi of Cyber stalking/sextortion Fraud.
18.4 Expected area of evidence in Cyber stalking/sextortion fraud.
18.5 Standard operating procedure of investigation of Cyber stalking/sextortion fraud.
18.6 Flow chart of investigation of Sextortion.
18.7 Case study of Cyber stalking/sextortion fraud.
18.8 Investigation of case study of Cyber stalking/sextortion fraud.
18.9 Questions for self-study.
18.10 Answer for self-study.

(19) Cyber Social Media Impersonation Fraud.

19.0 Objectives
19.1 Introduction.
19.2 Modus operandi of Social media impersonation fraud.
19.3 Flow chart of Modus operandi of social media impersonation Fraud.
19.4 Expected area of evidence in social media impersonation fraud.
19.5 Standard operating procedure of investigation of social media impersonation fraud.
19.6 Case study of social media impersonation fraud.
19.7 Investigation of case study of social media impersonation fraud.
19.8 Questions for self-study.
19.9 Answer for self-study.

(20) Insurance Fraud.

20.0 Objectives
20.1 Introduction.
20.2 Modus operandi of Insurance fraud.
20.3 Flow chart of Modus operandi of Insurance Fraud.

20.4 Expected area of evidence in Insurance fraud.
20.5 Standard operating procedure of Insurance fraud.
20.6 Case study of Insurance fraud.
20.7 Investigation of case study of Insurance fraud.
20.8 Questions for self-study.
20.9 Answer for self-study.

(21) Advertisement Fraud.

21.0 Objectives
21.1 Introduction.
21.2 Modus operandi of Advertisement fraud.
21.3 Flow chart of Modus operandi of Advertisement Fraud.
21.4 Expected area of evidence in Advertisement fraud.
21.5 Standard operating procedure of investigation of Advertisement fraud.
21.6 Case study of Advertisement fraud.
21.7 Investigation of case study of Advertisement fraud.
21.8 Questions for self-study.
21.9 Answer for self-study.

(22) Aadhar Enabled Payment System (AEPS) Fraud.

22.0 Objectives.
22.1 Introduction.
22.2 Uses of AEPS.
22.3 Benefits of AEPS.
22.4 Requirements for AEPS transections.
22.5 How to use AEPS.
22.6 Modus operandi of AEPS fraud.
22.7 Standard operating procedure in investigating AEPS fraud.
22.8 Questions for self-study.
22.9 Answers for self-study.

(23) Man In Middle Attack.

23.0 Objectives.
23.1 What is man in middle attack?
23.2 How MITM Attack occurs?
23.3 Types of MITM Attack.
23.4 Modus operandi of MITM Attack.
23.5 Damage caused by MITM Attack
23.6 How to restore MITM infected system?
23.7 Precautions to prevent MITM Attack.
23.8 Reporting incidence of MITM Attack
23.9 Reported attacks of MITM in India.
23.10 Standard operating procedure of investigation of MITM Attack.

23.11 Flow chart of investigation of email spoofing/MITM Attack.
23.12 Questions for self-study.
23.13 Answers for self-study.

(24) Ransomware Attack.

24.0 Objectives.
24.1 What is Ransomware?
24.2 How Ransomware attack happens?
24.2 Modus operandi of Ransomware attack.
24.3 Damaged caused by Ransomware attack.
24.4 How to recover damaged caused by Ransomware attack.
24.5 How to restore Ransomware infected system?
24.6 Precautions to be taken to avoid Ransomware attack.
24.7 Reporting incidence of Ransomware attack.
24.8 Reported incidences of Ransomware attacks in India.
24.9 Standard operating procedure for investigation of Ransomware attack.
24.10 Questions for Sel-study.
24.11 Answers for self-study.

(25) Cryptocurrency Frauds.

25.0 Objectives.
25.1 Introduction.
25.2 Characteristics of cryptocurrency.
25.3 Cryptocurrency Wallet.
25.4 Types of cryptocurrency crime and cybercrime.
25.5 Modus operandi of cryptocurrency fraud.
25.6 Tracking fraudulent cryptocurrency wallet.
25.7 Standard operating procedure in investigation crypto fraud.
25.8 Tracing accused and cryptocurrency funds.
25.9 Steps in tracking, tracing and analysis of cryptocurrency.
25.10 Case study no 1
25.11 Steps in investigation of Case study no 1.
25.12 Case study no 2.
25.13 Steps in investigation of case study no.2.
25.14 Questions for self-study.
25.15 Answers for self-study.

(26) DOS and DDOS Attack.

26.0 Objectives.
26.1 What is DOS and DDOS attack?
26.2 Types of DDOS attacks.
26.3 Modus operandi of DDOS Attack.
26.4 Examples of DDOS attacks in India.
26.5 Steps in investigation of DDOS attack.

26.6 How to prevent DDOS Attacks.
26.7 Case Study.
26.8 How the attack happened.
26.9 How to trace accused in DDOS Attack.
26.10 Questions for self-study.
26.11 Answers for self-study.

(27) ATM Device in Middle Attack.

27.0 Objectives.
27.1 Introduction.
27.2 ATM Components.
27.3 Modus operandi of Denial-of-Service Attack.
27.4 Denial of Service Attack, recent cases.
27.5 Nature of Attack.
27.6 Attack Techniques,
27.7 How to trace accused in Device in middle attack cases.
27.8 Case study.
27.9 Preventives in Device in middle attack.
27.10 Questions for self-study.
27.11 Answers for case study.

(28) APK Fraud.

28.0 Objectives
28.1 Introduction.
28.2 What is an APK?
28.3 Modus Operandi of   APK files.
28.4 How to Detect Malicious APKs?
28.5 Case study of APK
28.6 How to Protect Against APK Attacks.
28.7 Investigation of APK fraud case.
28.8 Case study Jocker Malware.
28.9 Investigation of case study.
28.10 Conclusion
28.11 Questions for self- study.
28.12 Answers for self -study.