

F.No 22006/2/2017-CIS-II.
Government of India/Bharat Sarkar
Ministry of Home Affairs/GrihMantralaya

North Block, New Delhi-110001
Dated the 2nd February, 2018

To

1. The Chief Secretaries of all State Governments/UT Administrations

Subject: CCPWC scheme-capacity building courses for Police Officers, Prosecutors & Judicial Officers


Over a period of time there has been phenomenal increase in use of computers, smartphones and internet. With this increase, cybercrimes have emerged as a major challenge for law enforcement agencies. Capacity building of police, prosecutors and Judicial officers in the field of cyber domains essential for strengthening criminal justice response to victims of cyber crime as well as taking steps for preventing such crimes.

2. Government of India is implementing a scheme under Nirbhaya fund titled "Cyber Crime prevention against women and Children (CCPWC)" during the period 2017-2020. This scheme envisages to train 27500 police officers, prosecutors & judicial officers in cybercrime awareness program of 3 days duration and 13500 officials in 5 days cybercrime investigation program in next two years through National/State/UT police academies/institutes. Ministry of Home Affairs will extend financial assistance of Rs 3000/- per trainee for 3 day course and Rs 5000/- for 5 day program for organizing such programs. Training targets for central and State/UT Administrations are given at Annexure-I.
3. A 2 days workshop on 11-12 January 2018 at New Delhi with officers from central training institutes, stakeholder Ministries, States, academia and professional bodies was organized to recommend course structure for these programs. Accordingly, the suggested course structure for 3 days program for police officers, 3 days programs for prosecutors & judicial officers and 5 days cybercrime investigation module for police officers are at annexure-II, III and IV respectively.
4. It has been decided that BPR&D, NPA and Govt. of MP will be organizing the ToT program to train the trainers as per details given below:

Train the Trainer program	Organizing agency	Duration	Target
3 days cybercrime awareness for police officers	BPR&D	2 days	3 rd week of Feb 18
3 days cybercrime & cyber law program for PPs& Judicial officers	NPA	2 days	-do-
5 days cybercrime investigation course for police officers	MP Govt.	3 days	-do-

5. Institutes conducting the ToT program will make available standardized course content/handbook for these courses to the trainers for use in the programs to be conducted in their States/UTs.
6. All States/UTs, Central training institutes are requested to schedule & start conducting 3 days & 5 days training programs at the earliest with following guidelines:
 - i. Targets indicated for training of women officers are minimum targets and all efforts need to be made for training as many women officers as possible.
 - ii. Since large number of officers have to be trained in a time bound manner, all States/UTs are requested to depute their trainers in adequate number to the ToT programs conducted by NPA, BPR&D and Govt. of MP.
 - iii. Certain targets for smaller UTs and NE states as indicated in Ann-I have been included in the targets of Delhi and NEPA respectively and financial assistance for such targets will be given to Delhi and NEPA. These UTs and NE states have to depute their officers in the programs conducted by Delhi & NEPA respectively.
 - iv. All States/UT administrations are requested to depute officers in the 3 days and 5 days training programs organized by NPA, BPR&D and NEPA also, in addition to those deputed for training in their own training institutes.
 - v. The cyber forensic training labs being setup under CCPWC scheme, funds for which have already been released to the States/UTs, must be used to the best possible extent for organizing these programs.
 - vi. States/UTs requiring trainer support for conducting such programs may request National Police Academy for assistance, which will make all possible efforts to provide trainers as per mutual convenience.
 - vii. All States/UTs/Central institutes are required to furnish progress report every quarter as per Annexure V.
7. All the States/UT administrations are requested to take immediate steps to start organizing these training programs.

The receipt of this letter may please be acknowledged.


21/7/2018
(Kumar Alok)
Join Secretary (CIS)

Copy to:

1. Home Secretaries of all State Governments/UTs.
2. The DGPs of all State Governments/UTs
3. DG BPR&D
4. Director NPA
5. Director NEPA

Indicative targets for Cybercrime training programs under CCPWC scheme							Annexure-I	
SL	State/UT	3 day course for LEAs			3 day course for PP & Judicial officers		5 day course for LEAs	
		Police stations	Any gender	Women	Prosecutors	Judges	Any SHO	SHO women
1	Andhra Pradesh	1017	1000	100	125	125	630	20
2	Arunachal Pradesh	101	100	10	2#	2#	24	1
3	Assam	347	300	30	50	50	241	9
4	Bihar	1064	1000	100	200	200	650	50
5	Chhattisgarh	428	400	40	100	100	280	20
6	Goa	26	23	2	10	10	24	1
7	Gujarat	650	600	60	250	250	470	30
8	Haryana	295	250	25	75	75	195	5
9	Himachal Pradesh	116	100	10	25	25	70	5
10	Jammu & Kashmir	222	200	20	50	50	195	5
11	Jharkhand	506	450	45	150	150	390	10
12	Karnataka	951	900	90	300	300	630	20
13	Kerala	520	500	50	150	150	630	20
14	Madhya Pradesh	1095	1000	100	350	350	630	20
15	Maharashtra	1162	1100	110	600	600	630	20
16	Manipur	100	45	5	5#	5#	24	1
17	Meghalaya#	39	22	3	5#	5#	24	1
18	Mizoram#	38	22	3	5#	5#	24	1
19	Nagaland	78	45	5	5#	5#	24	1
20	Odisha	614	550	55	150	150	230	20
21	Punjab	399	350	35	100	100	135	15
22	Rajasthan	861	800	80	250	250	545	30
23	Sikkim#	29	23	2	3#	3#	24	1
24	Tamil Nadu	1541	1500	150	300	300	910	40
25	Telangana	721	700	70	130	130	480	20
26	Tripura	81	50	5	10	10	24	1
27	Uttar Pradesh	1528	1400	140	600	600	910	40
28	Uttarakhand	156	120	12	50	50	99	1
29	West Bengal	585	500	50	250	250	380	20
	TOTAL STATE(S)	15270	14050	1407	4275	4275	9522	428
30	A & N Islands*	24	23	2	2*	2*	19	1
31	Chandigarh	17	20	5	5*	5*	5*	5*
32	D&N Haveli*	2	1*	1*	1*	1*	1*	1*
33	Daman & Diu*	5	1*	1*	1*	1*	1*	1*
34	Delhi UT	192	180	20	100	100	115	10
35	Lakshadweep*	16	2*	1*	1*	1*	5*	5*
36	Puducherry	53	45	5	5*	5*	24	1
	TOTAL UT(S)	309	268	32	100	100	158	12
	TOTAL (ALL INDIA)	15579	14318	1439	4375	4375	9680	440
	BPR&D (CDTS)		682	561	500	500	230	50
	NPA		0	0	100	100	0	0
	NEPA		0	0	25	25	90	10
	Total		15000	2000	5000	5000	10000	500

*Target included in Delhi. Each UT to depute officers in programs conducted by Delhi

Target included in NEPA. Each state to depute officers in programs conducted by NEPA

Cyber Crime Awareness Program for Police Officers (3 days)**Course description**

Considering the rapid increase of ICT in all walks of life, most of the crimes now have an element of misuse of computers, smartphones, communication networks etc. These technologies are increasingly being used by criminals in committing conventional crimes. Increasing use of internet and social media has resulted in a plethora of varied crimes being committed in the cyber domain. Therefore, it has become imperative for the Law Enforcement Agencies to have an in-depth understanding of the working of the cyber domain and the modus operandi of crimes being committed therein. This understanding cannot be limited to a few specialist investigative officers, but is a must for all police officers, especially those who act as first responders to victims of crime and recording them.

Participant profile

The participants are the first responders to victims and complainants at the police stations i.e. SHO, SI, HCM and the Duty Officers. These officers are the first to interact with the victims and record their complaints. They are expected to understand the crime victimization as described by the complainants and record it faithfully and apply the relevant sections of the IPC and other applicable Acts such as the IT Act.

Participants should possess a working knowledge of mobile phones and computers.

Learning Outcomes

After the course, the participants will have learnt to –

1. Understand the various types of cybercrimes and the current trends
2. Record the cybercrime as reported by the victim and relate the legal provisions to the reported cyber crime
3. Provide immediate counseling of the victims and restore their confidence; give immediate advice for damage control to the victims and at the same time safeguard the immediately available evidence in the cybercrime
4. Identify the agencies to be approached for initiating investigation
5. Explain the precautions for preventing cyber frauds/ crimes to public

Pedagogy

Lecture/ Case discussions/ demonstrations/ Hands-on exercises within a classroom setting with computers provided to individual participants. The optimal class size is 25 participants. Course content focuses on all types of cybercrimes – criminal intimidation, ransom, financial frauds etc. and the legal aspects associated with such crimes, fundamentals of electronic evidence and basic steps of cyber investigation. Participants will be given brief assignments to be completed through use of laptop or smartphones.

Sessions: 24, each of 45 minutes duration

Cyber Crime Awareness Program for Police Officers (3 days)

Sessions Breakup

1. Inauguration and Assessment (1 session)

The participants will undergo a brief 20 question test to assess their present knowledge/ awareness of cybercrimes and related issues

2. Introduction to Computer Hardware and other electronic devices and their terminologies (1 session)

At the end of the session the participants will have adequate understanding and familiarization with the terminologies of –

- 2.1 Computers, laptops, I-Pads and their peripherals
- 2.2 Computer networks – Servers and Client machines
- 2.3 Storage media like hard discs, pen drives, CD, DVD, SD cards, Cloud etc.
- 2.4 Digital cameras, mobile phones etc.

3. Introduction to Internet and mobile technologies (2 sessions)

At the end of the session the participants will have adequate understanding and familiarization with the terminologies of –

- 3.1 Internet – Concept
- 3.2 Use of Internet in homes, Educational institutions, Business, Government and other organizations etc.
- 3.3 Telecom Service Providers (TSP) and Internet Service Providers (ISP)
- 3.4 Wired and wireless Internet; concept of WiFi
- 3.5 Use of e-mail

4. An introduction to Cyber Crimes (4 sessions)

At the end of the session the participants will have adequate understanding and familiarization with the terminologies of –

- 4.1 Meaning of Cybercrime
- 4.2 Types of cybercrime – e-mail threats, cyber stalking, Identity theft, creation of fake facebook profiles, e-mail hacking, Online Frauds like Nigerian Frauds, job frauds etc.
- 4.3 Cybercrimes of advanced types – Hacking of websites and emails, Ransom ware, Phishing, Malware, BOTNET, DDOS, Steganography, Cyber warfare, Dark Web, Crypto-currencies etc.
- 4.4 Safety tips against cybercrimes
- 4.5 Special focus of on understanding of cybercrimes against women & Children such as matrimonial websites, cyber bullying etc.

5. Introduction to social media like Facebook, Whatsapp etc. (2 sessions)

At the end of the session the participants will have adequate understanding and familiarization with the terminologies of –

- 5.1 Meaning of Social Media
- 5.2 Use of Social Media on computers and smartphones
- 5.3 Types of Social Media such as Facebook, Twitter, Pinterest, Whatsapp, YouTube, Tinder, Instagram, Telagram, Skype etc.
- 5.4 Chatrooms

6. Demonstration/ Hands on Practice on use of Social Media (2 sessions)

At the end of the session the participants will have adequate understanding and familiarization of Social Media through **demonstration** on –

- 6.1 Opening of Social Media accounts; information provided by the user at this stage
- 6.2 Settings, functioning and use of Social Media accounts
- 6.3 How criminals misuse the violate the Social Media accounts
- 7. **Introduction to online and cash less transactions like ATM, credit and debit cards, BHIM app, e-wallet, PayTM etc. (2 sessions)**
At the end of the session the participants will have adequate understanding and familiarization with the terminologies of –
 - 7.1 Concept of Debit and Credit cards; their security features, CVV number, PIN
 - 7.2 Use of cards in physical shops and online shopping (Amazon, Flipkart etc.)
 - 7.3 ATM machines and their functioning
 - 7.4 Concept of Point of Sale (POS), use of cards at POS
 - 7.5 Concept of Mobile Applications – BHIM, PayTM, etc.
 - 7.6 Safety precautions, Second level authentication, One Time Password (OTP)
- 8. **Demonstration/ Hands on Practice on online and cash less transactions like ATM, credit and debit cards, BHIM app, e-wallet, PayTM etc. (2 sessions)**
At the end of the session the participants will have adequate understanding and familiarization of above e-commerce transactions through **demonstration** on –
 - 8.1 Various types of cards and their safety features
 - 8.2 Demonstrations and videos of Point of Sale machines; how cards are likely to be copied/ skimmed
 - 8.3 Modus Operandi of criminals to obtain card information and passwords etc.
 - 8.4 Display of various Mobile Applications – BHIM, PayTM, etc.
 - 8.5 Video demonstration of an online transaction through Amazon, Flipkart etc.
 - 8.6 Demonstrations on Safety precautions, Second level authentication, One Time Password (OTP)
- 9. **Recap of sessions and activities of Day 1 and Day 2 (2 sessions)**
At the end of the session the participants will have revised the knowledge acquired in two days and have greater clarity on all theoretical and practical aspects –
- 10. **Relevant sections of IT Act and IPC (1 session)**
At the end of the session the participants will have adequate understanding and familiarization with the sections of IPC and IT Act attracted in the cybercrime.
- 11. **Basics of a Good cyber crime FIR / Report (1 session)**
At the end of the session the participants will acquire the following capabilities:
 - 11.1 Draft a good report/ complaint listing out the details of the crime (Where, When, How, Whom etc.) as provided by the victim
 - 11.2 Incorporate all relevant details such as mobile numbers, bank account numbers, email IDs, URL etc.
 - 11.3 Relate the relevant sections of the IPC and IT Act as applicable and incorporate in the FIR

12. Institutional set up for cybercrime investigation (1 session)

At the end of the session the participants will acquire the knowledge of the following:

- 12.1 Overall steps to be taken and the role of other investigators in the cybercrime
- 12.2 Institute and organizations – cybercrime police stations, cybercells etc. functioning in the respective states; along with their Contact details.

13. Counseling and advice to victims of cybercrime (1 session)

At the end of the session the participants will acquire the knowledge skills to –

- 13.1 Provide immediate counseling of the victims and restore their confidence
- 13.2 Give immediate advice for damage control to the victims
- 13.3 Safeguard the immediately available evidence in the cybercrime

14. Case studies and Advisories for public (1 session)

In this session, a compilation of good case studies and advisories issued from time to time by the Government, NGOs and other organizations will be made available to the participants. At the end of the session the participants will acquire the knowledge and skills to –

- 14.1 Disseminate knowledge on safety aspects and precautions in use of social media, online financial transactions, use of internet to school and college students, women's groups and other vulnerable users

15. Simulation Exercise (1 session)

In this session, the participants will undergo a group simulation exercise through role play to apply the relevant law, write a report on the cybercrime, counsel the victim and transfer the case to the concerned investigator. Several scenarios on various kinds of cybercrimes will be developed for this exercise.

16. Assessment and Valedictory (1 session)

The participants will undergo a 20 questions test to assess the level of their acquisition and understanding of the knowledge, concepts and skills imparted during the course.

Recommended timetable for 3 days Cybercrime Awareness course for Police officers

10:00 – 10:45	10:45 – 11:30	11:30 -11:45	11:45 – 12:30	12:30 13:15	13:15 14:15	14:15 15:00	15:00 15:45	15:45 16:00	16:00 16:45	16:45 17:30
1	2	Tea Break	3	4	Lunch Break	5	6	Tea Break	7	8
Inauguration and Assessment Test	Introduction to Computer Hardware and other electronic devices and their terminologies		Introduction to Internet and mobile technologies			An introduction to Cyber Crimes-general and specific to women & children			An introduction to Cyber Crimes - general and specific to women & children	
Introduction to social media like Facebook, Whatsapp etc.			Demonstration/ Hands on Practice on use of social media			Introduction to online and cash less transactions like ATM, credit and debit cards, BHIM app, e- wallet, PayTM etc.			Demonstration/ Hands on Practice on online and cash less transactions like BHIM app, e-wallet, PayTM, ATM, credit and debit cards etc.	
Recap of activities of Day 1 and Day 2	Relevant sections of IT Act and IPC		Basics of a Good cyber crimeFIR / Report	Institutional set up for cybercrime investigation		Counseling and advice to victims of cyber crime	Case studies and Advisories for public		Simulation exercise	Assessment and Valedictory Session

**Cyber Crime & Cyber law Awareness Program (3 days)
for Prosecutors & Judicial Officers**

Course description

Considering the rapid increase of ICT in all walks of life, most of the crimes now have an element of misuse of computers, smartphones, communication networks etc. These technologies are increasingly being used by criminals in committing conventional crimes. Increasing use of internet and social media has resulted in a plethora of varied crimes being committed in the cyber domain. Therefore, it has become imperative for the public prosecutors and judicial officers to understand the working of the cyber domain and the modus operandi of crimes being committed therein so as to evaluate the electronic evidences for nailing the culprits. This 3 days program aims to equip the participants with basic understanding of cybercrimes, evidences associated with various types of cybercrimes and the legal provisions thereof.

Participant profile

The participants of the course will be public prosecutors as well as officers from judiciary. Participants should possess a working knowledge of mobile phones and computers.

Learning Outcomes

After the course, the participants will have learnt to –

1. Understand the various types of cybercrimes
2. Have a fair idea of technology elements & their functioning in cybercrimes
3. Be able to examine the correctness of chain of custody of evidence
4. Be able to identify relevance of intermediaries and their legal obligations
5. Evaluate the relevance of presented evidences
6. Apply the legal provisions to the electronic evidences to confirm its tenability

Pedagogy

Lecture/ Case discussions/ demonstrations/ Hands-on exercises within a classroom setting with computers provided to individual participants. The class size must not exceed 25 participants.

Sessions: 24, each of 45 minutes duration

Cyber Crime & Cyber law Awareness Program (3 days) for Prosecutors & Judicial Officers

Sessions Breakup

1. Inauguration and Assessment (1 session)

The participants will undergo a brief 20 question test to assess their present knowledge/ awareness of cybercrimes and related issues

2. Basics of communication devices & media: .):Cybercrime perspective(3 sessions)

At the end of the session the participants will have adequate understanding and familiarization with–

- 2.1 Computers, laptops, I-Pads and their peripherals
- 2.2 Computer networks – Servers and Client machines
- 2.3 Storage media like hard discs, pen drives, CD, DVD, SD cards, Cloud etc.
- 2.4 Internet – Concept
- 2.5 IP addresses
- 2.6 Use of Internet in homes, Educational institutions, Business, Government and other organizations etc.
- 2.7 Telecom Service Providers (TSP) and Internet Service Providers (ISP)
- 2.8 Mobile phone basics
- 2.9 Wired and wireless Internet; concept of WiFi
- 2.10 Use of e-mail

3. An introduction to Cyber Crimes (2 sessions)

At the end of the session the participants will have adequate understanding and familiarization with –

- 3.1 Meaning of Cybercrime
- 3.2 Types of cybercrime – e-mail threats, Identity theft, e-mail hacking, Online Frauds like Nigerian Frauds, job frauds etc.
- 3.3 Cybercrimes of advanced types – Hacking of websites and emails, Ransom ware, Phishing, Malware, BOTNET, DDOS, Steganography, Cyber warfare, Dark Web, Crypto-currencies etc.
- 3.4 Safety tips against cybercrimes
- 3.5 Special focus on understanding of cybercrimes against women & Children such as matrimonial websites, cyber bullying etc.

4. Introduction to Cybercrime-social media like Facebook, Whatsapp etc. (2 sessions)

At the end of the session the participants will have adequate understanding and familiarization of:

- 4.1 Meaning of Social Media
- 4.2 Use of Social Media on computers and smartphones
- 4.3 Types of Social Media such as Facebook, Twitter, Pinterest, Whatsapp, YouTube, Tinder, Instagram, Telegram, Skype etc.
- 4.4 Chatrooms

5. Handling Digital Evidence: SOPs and hands on(4 sessions)

- 5.1 Search
- 5.2 Seizure of evidence

- 5.3 Preservation of evidence
 - 5.4 Chain of custody
 - 5.5 SOP for handling Digital evidence
 - 5.6 RAM dump & data analysis demo
- 6. Relevant sections of IT Act and IPC (4 sessions)**
At the end of the session the participants will have adequate understanding and familiarization with the sections of IPC and IT Act attracted in the cybercrime.
- 7. Appreciation of Electronic Evidence: (2 sessions)**
At the end of the session the participants will acquire the following capabilities:
- 7.1 Understand types of Electronic Evidence
 - 7.2 Documentary Evidence Vs Electronic Evidence
 - 7.3 Computer printouts Vs Banking records
 - 7.4 Sec 65B procedure
 - 7.5 Latest judgments& case studies
- 8. E-Mail Investigation: (1 session)**
At the end of the session the participants will acquire the knowledge of the following:
- 8.1 E-Mail Tracing & Analysis of E-Mail Header
 - 8.2 Admissibility of Email as Evidence
 - 8.3 IP Spoofing v/s Proxy Server & legal Issues
- 9. Intermediaries & Due Diligence Rule (1 session)**
- 9.1 Provisions in IT Act and Related Rules
 - 9.2 Who are intermediaries
 - 9.3 Case Laws
 - 9.4 Civil & Criminal liabilities of Intermediaries
 - 9.5 Bazee.com Case Study
 - 9.6 Due Diligence concepts
- 10. Challenges in conducting trial in Cyber Crimes (3 sessions)**
In this session, the participants will undergo a group simulation exercise through role play to apply the relevant law, write a report on the cybercrime, counsel the victim and transfer the case to the concerned investigator. Several scenarios on various kinds of cybercrimes will be developed for this exercise.
- 11. Assessment and Valedictory (1 session)**
The participants will undergo a 20 questions test to assess the level of their acquisition and understanding of the knowledge, concepts and skills imparted during the course.

**Recommended timetable for 3 days Cybercrime & Cyber Law Awareness course
for Prosecutors & Judicial Officers**

10:00 – 10:45	10:45 – 11:30	11:30 - 11:45	11:45 – 12:30	12:30 13:15	13:15 14:15	14:15 15:00	15:00 15:45	15:45 16:00	16:00 16:45	16:45 17:30
1	2	Tea Break	3	4	Lunch Break	5	6	Tea Break	7	8
Inauguration and Assessment Test	Basics of communication devices & media (Computer, Internet & Mobile etc.):Cybercrime perspective	Tea Break	Basics of communication devices & media (Computer, Internet & Mobile etc.):Cybercrime perspective		Lunch Break	An introduction to Cyber Crimes-general and specific to women & children		Tea Break	An introduction to Cyber Crimes – social media and demonstration/hands on	
Handling Digital Evidence: SOPs and hands on exposure		Tea Break	Handling Digital Evidence: SOPs and hands on exposure		Lunch Break	Understanding legal framework-IT Act , IPC, Indian evidence Act etc.		Tea Break	Understanding legal framework-IT Act , IPC, Indian evidence Act etc.	
Appreciation of Electronic Evidence	Appreciation of Electronic Evidence	Tea Break	E-Mail Investigation	Intermediaries & Due Diligence Rule	Lunch Break	Challenges in conducting trial in Cyber Crimes – A Case Study	Challenges in conducting trial in Cyber Crimes – A Case Study	Tea Break	Challenges in conducting trial in Cyber Crimes – A Case Study	Assessment and Valedictory Session

Cyber Crime Investigation Program (5 days) for Police officers**Course description**

Considering the rapid increase of ICT in all walks of life, most of the crimes now have an element of misuse of computers, smartphones, communication networks etc. These technologies are increasingly being used by criminals in committing conventional crimes. Increasing use of internet and social media has resulted in a plethora of varied crimes being committed in the cyber domain. Investigation of such crimes requires knowledge and skills to use technical tools for extracting legally tenable evidences for securing conviction in the court of law. Therefore, it has become imperative for the officers entrusted with investigation of cybercrimes to become proficient in this domain. This course aims to achieve so by training on cybercrime identification, crime scene management, investigation procedures, case studies, hands on exposure to use of tools and documentation related exposure to carry out proper cybercrime investigations.

Participant profile

- a. Police officers of the rank of SI and above rank
- b. Pre training examination must be cleared or should have attended three day cybercrime awareness training program

Learning Outcomes

Upon completion of the course, the participants will have learnt to –

1. Identify and apply the SOP for crime scene management
2. Carry out search, seizure and proper storage of potential digital evidences
3. Use various forensic tools for mobile data analysis, disks, CDRs, network etc.
4. Use social media analysis tools
5. Document requisitions for seeking evidence from other agencies such as TSPs, ISPs, banks, wallet companies, financial institutions, content hosting platforms, OTT players etc.
6. Initiate LR under MLAT for cases having international dimensions

Pedagogy

Lecture/ Case discussions/ demonstrations/ Hands-on exercises within a lab with computers provided to individual participants. The class size must not exceed 25 participants. The lab should have forensic facilities such as write blockers, imagers, pen drives, HDDs, disk analyzers, mobile forensic kit, E-mail analyzer, OSINT tools, CDR/IPDR analysis tool, skimmers, network traffic/packet analyzer, CCTV/DVR etc.

Sessions:40, each of 45 minutes duration

Cyber Crime Investigation Program (5 days) for Police officers

Session breakup

1. Overview of Cybercrimes-2 sessions

At the end of the session the participants will have adequate understanding and familiarization with the terminologies of:

- 1.1 Definition.
- 1.2 Classification of Cybercrime.
 - 1.2.1 Cybercrime against individuals.
 - 1.2.2 Cybercrime against property.
 - 1.2.3 Cybercrime against Originations
 - 1.2.4 Cybercrime against Society.
 - 1.2.5 Cybercrime against Nation.
- 1.3 Important Cybercrime.
 - 1.3.1 Social Media Websites/Platform related crimes
 - 1.3.1.1 Fake Profile
 - 1.3.1.2 Cyber Defamation
 - 1.3.1.3 Cyber Stalking/Bullying
 - 1.3.1.4 Cyber Pornography
 - 1.3.2 Email related crime.
 - 1.3.2.1 Email spoofing.
 - 1.3.2.2 Phishing/Vishing
 - 1.3.2.3 Email bombing.
 - 1.3.2.4 Spamming
 - 1.3.2.5 Email Frauds.
 - 1.3.3 Financial Cybercrimes.
 - 1.3.3.1 Debit/Credit card frauds.
 - 1.3.3.2 Illegal Online transaction.
 - 1.3.3.3 Job Frauds.
 - 1.3.3.4 Lottery Frauds.
 - 1.3.3.5 Insurance Frauds.
 - 1.3.3.6 Ponji Scheme Frauds.
 - 1.3.4 Others Cyber Crimes.
 - 1.3.4.1 Hacking
 - 1.3.4.2 Intellectual Property Right Violations.
 - 1.3.4.3 DOS/D-DOS Attacks.
 - 1.3.4.4 Virus/Warm Attacks
 - 1.3.4.5 Malware Attacks.
 - 1.3.4.6 Spywares.
 - 1.3.4.7 Cyber Pornography
 - 1.3.4.8 Web Defacement
 - 1.3.4.9 Salami Attack
 - 1.3.4.10 Online Sale of Illegal Articles
 - 1.3.4.11 Internet Time Theft.
 - 1.3.4.12 Trojan
 - 1.3.4.13 Key logger
 - 1.3.4.14 Web jacking
 - 1.3.4.15 Cross Site Scripting (XSS)
 - 1.3.4.16 Cyber Terrorism
- 1.4 Glossary of Cybercrime Terms

2. Information Gathering-4 sessions

At the end of the session the participants will have adequate understanding and familiarization of:

- 2.1 Open Source Intelligence.
- 2.2 Information From Internet/Mobile Service Providers (ISP/MSP)
 - 2.2.1 Subscriber Data Records (SDR)
 - 2.2.2 Customer Application Form (CAF)
 - 2.2.3 Call Detail Records (CDR)
 - 2.2.4 Internet Packet Data Records (IPDR)
 - 2.2.5 Tower Dump Data Records
- 2.3 Information From Email Client
- 2.4 Information From Social Media Networking Sites.
- 2.5 Information From Financial Institutions/Banks/wallets
- 2.6 Information From Websites/Domains from Domain Host Provider
- 2.7 Information From National Voters Service Portals
- 2.8 Information From Unique Identification Authority of India (UIDAI)
- 2.9 Information From Ministry of Road Transport & Highways (For Driving License)

3. Scene of Crime Management (10 sessions)

At the end of the session the participants will have adequate understanding, familiarization and hands on experience with:

- 3.1 Pre-search considerations
- 3.2 Search & seizure
- 3.3 Server systems
- 3.4 Documentation or Panchnama
- 3.5 Labeling, Packing & Transportation
- 3.6 Mobile Devices
- 3.7 DVR Systems**

4. IP, website and Email Investigation (3 sessions)

At the end of the session the participants will have adequate understanding and familiarization with the terminologies of –

- 4.1 Concept of IP Address, DHCP server, MAC address, Domain name System, Web Server, who.is, Url, Surveillance, Proxy server, Anonymous Surfing, firewall, email architecture
- 4.2 Email Investigation and Tracking with Hands on.
- 4.3 Website defacement investigation with hands on
- 4.4 How to seek information's from Email service providers (ESP)/ Internet Service Provider (ISP)
- 4.5 Secure email services , dark web email services

5. Communication Device (Mobile Phone, Satellite Phone, GPS Device Etc.) Based Investigation (5 sessions)

At the end of the sessions the participants will have adequate understanding and familiarization with legal provisions, types of evidences, evidentiary sources, agencies involved in:

- 5.1 Mobile Interception & authorization.

- 5.2 Legal provision of interception in Indian Telegraph Act with Recent Guidelines.
- 5.3 Collection of information/evidences from smart phone, mobile phones and SIM cards.
- 5.4 Search and seizure of mobile phones and precautions to be taken
- 5.5 How to seek information's from mobile service providers
- 5.6 CDR /IPDR Analysis and its uses in Investigation with hands on.
- 5.7 Concept of GPRS Logs & its use in investigation (use of chat programmes like we-chat, Viber, whats-app, Skype) & VOIP, etc
- 5.8 VOIP investigation

6. Social Media Related Crime Investigation (3 sessions)

At the end of the sessions the participants will have adequate understanding and familiarization with investigation aspects of social media crimes:

- 6.1 Social media & Different types of Crimes Reported on Social Media
- 6.2 Modus Operandi of Social Media Crimes
- 6.3 Investigation Procedures on Social Media Crimes
- 6.4 Process of Contacting Intermediaries for Inputs
- 6.5 Usage/privacy/security on Social Networking Sites Blocking/Takedown
- 6.6 Process of Digital Evidence Seizures and Reporting
- 6.7 Investigation of cases with reference to uploading and circulation of pornographic defamatory photos, suicide videos with case studies and hands on.
- 6.8 Social media monitoring & Intelligence collection

7. Crime Against Women & Child (1 session)

At the end of the session the participants will have adequate understanding for carrying out investigations of:

- 7.1 Child pornography
- 7.2 Rape/Gang rape imagery
- 7.3 Use of online media for Human trafficking

8. Investigation Of Financial Frauds (3 sessions)

At the end of the sessions, the participants will have adequate knowledge & understanding to handle investigation of financial frauds by learning on:

- 8.1 Types of Financial Frauds
 - 8.1.1 OTP frauds , ATM skimming , Job fraud , Credit card fraud , hacking of bank accounts , loan frauds , gift frauds , cheating by impersonation , unsecured transaction ,identity theft etc
- 8.2 Investigation procedure of financial frauds and role of Ecommerce website & mobile app, Payment Gateways, Banks, ISP/MSP
- 8.3 Freezing Of Bank Account during Investigation
- 8.4 Investigation of bank fraud cases including the collection of evidences (type of documents required and whom to approach) with case studies.

9. Investigations abroad (1 session)

At the end of the session, the participants will have adequate knowledge & understanding to exercise MLAT framework:

- 9.1 MLAT framework
- 9.2 Concept of LR, SOP& documentation
- 9.3 Role of MHA and CBI

10. Cyber Laws (2 sessions)

- 10.1 Provisions of IT Act 2000 and rules
- 10.2 Linkage with IPC and Indian Evidence Act
- 10.3 Relevant provisions of other Acts

11. Investigation Challenges (2 sessions)

At the end of the session, the participants will have adequate understanding of various challenges faced in cybercrime investigations through various examples and group discussion.

12. Simulation & Evaluation Exercises (3 sessions)

These sessions provide an opportunity to test their learning by carrying out investigation in a simulated environment.

13. Assessment and Valedictory (1 session)

The participants will undergo a 20 questions test to assess the level of their acquisition and understanding of the knowledge, concepts and skills imparted during the course.

Recommended Time Table for Cybercrime Investigation Course (Five Days) for Police Officers												
Day	9:30 to 1000	10:00 To 10:45	10:45 To 11:30	Tea Break	11:45 To 12:30	12:30 To 13:15	13:15 To 14:00	Lunch	15:00 To 15:45	15:45 To 16:30	Tea Break	16:45 To 17:30
		1	2		3	4	5		6	7		8
1	Registration & Inauguration	Overview of Cybercrimes		Tea Break	Information Gathering Case Study/Scenario Analysis			Lunch	Information Gathering (Case Study Exercise)	Scene of Crime Management: Inspection, Documentation, Securing SOC	Tea Break	Scene of Crime Management: Inspection, Documentation, Securing SOC
2		Scene of Crime Management: Pre-search Preparation & Required Forensic Tool Kits		Tea Break	Scene of Crime Management: Search, Seizure & Documentation			Lunch	Scene of Crime Management: Simulation Exercises		Tea Break	Scene of Crime Management: Group Exercise
3		IP, Website & E-mail Investigation		Tea Break	IP, Website & E-mail Investigation Case Study	Communication Device (Mobile Phone, Satellite Phone, GPS Device Etc.) Based Investigation		Lunch	Communication Device (Mobile Phone, Satellite Phone, GPS Device Etc.) Based Investigation		Tea Break	Communication Device (Mobile Phone, Satellite Phone, GPS Device Etc.) Case Study
4		Social Media Investigation		Tea Break	Social Media Investigation Case Study	Crime Against Women & Child	Financial Frauds	Lunch	Financial Frauds Case Study		Tea Break	Investigation Abroad
5		Cyber Laws		Tea Break	Investigation Challenges		Simulation & Evaluation Exercises	Lunch	Simulation & Evaluation Exercises		Tea Break	Valediction

Progress Report

Name of State/UT:

Period of Report: 17-18 18-19 19-20 Quarter:: I II III IV

Note: Please '✓' in appropriate box

(I) 3 days awareness programs for Police Officers.

No	Program date from/to	Venue	Participants (Number of Police officers)		Total trainees
	1	2	3	4	5
1			Men	Women	
2					
...					

(II) 3 days Awareness programs for PPs & Judicial officers

No	Program date from/to	Venue	Judicial Officers (Number)	Public Prosecutors (Number)	Total trainees
	1	2	3	4	5
1					
2					
.....					

(III) 5 days Cybercrime investigation program for Police Officers.

No	Program date from/to	Venue	Participants (Number of Police officers)		Total trainees
	1	2	3	4	5
1			Men	Women	
2					
.....					

Note: Utilization Certificate of the Grant-in Aid provided to the States/UTs has to be furnished as per GFR format

(Authorized signatory)
Name/Designation