CYBER LEGAL HANDBOOK

for Station House Officers

Compliments to

Krishnaja Olappamanna
Final Year LLB Student, School of Law
&
Dr. P. Vinod Bhattathiripad
M. Sc., M. Phil. (Comp. Sc.) .Ph. D. (Cyber Forensics)
Chief Technology officer

Telangana State Police

Cyber-Legal Handbook

For Station House Officers

Version 21.0

Prepared by

Krishnaja Olappamanna
Final Year LLB Student, School of Law
SASTRA Deemed to be University, Tamil Nadu

Under the guidance of

Dr. P. Vinod Bhattathiripad
M. Sc., M. Phil. (Comp. Sc.) .Ph. D. (Cyber Forensics)
Chief Technology officer (Honorary Advisor) to the DGP, Kerala Police
Author of the book "Judiciary-friendly Forensics of Software Copyright Infringement"

Upon special request from

Mr. Loknath Behera IPS
Director General of Police and the State Police Chief, Kerala

Acknowledgement

The basic idea of this handbook was conceived by Dr. P. Vinod Bhattathiripad. The table formats and the ingredients for Table 4 were also obtained from him. The ingredients for Table 2 and 3 were obtained after extensive research in the field and also with the help of the various available law books and other related materials. As part of the quality control process of this handbook, feedbacks from a few practicing law experts and police officers were sought. The inputs from the following experts / potential users are acknowledged here. (Note that they are listed below in the sequence in which they were met for feedback).

1. Mr.C.Sivaprasad, Inspector of Police, Cyber Crime P S, Kozhikode.
2. Adv. Suresh Menon, Advocate& Web development expert, Kozhikode.
3. Mr. P.T. Sabunath, ASI, Nadakkavu Police Station, Kozhikode.
4. Mr. P.M. Rajeev, ASI, Nadakkavu PS, Kozhikode.
5. Mrs. M. Reetha, SHO, Vanitha Police Station, Kozhikode.
6. Mrs. C. K. Jisha, Writer, Vanitha Police Station, Kozhikode.
7. Mr. K. S. Sudarshan, SP, Crime branch, Thrissur.
8. Mr. B. Vineeth Kumar, SCPO, Cyber Cell, Palakkad.
9. Mr. K. V. GovindanUnni, CPO, Cyber Cell, Palakkad.
10. Mr. K. S. Haridasan, SCPO, Cyber Cell, Palakkad.
11. Mr. S. Kaliraj Mahesh Kumar IPS, DPC Kozhikode.
12. Adv. Ashokan, Advocate, Kozhikode.

Cyber-Legal Handbook
for Station House Officers

Instructions to the users

This handbook is primarily meant for those Station House Officers (SHOs) who often come across petitions and complaints involving cyber evidence. The handbook is expected to serve them as a quick reference guide while dealing with petitions involving cyber evidence. Also, it can assist the SHO in attributing the various offences in the petition to the relevant sections in the concerned Acts while the cases are 'charged'. In the same way, the handbook can assist in following the procedural aspects of cyber evidence collection from the various formal cyber sources in a manner that is admissible to the judiciary. As a word of caution, this handbook is not meant for cyber forensic staff in the Police.

This handbook consists of a series of four tables. Each table carries specialized contents related to cyber offences and cyber evidence. All these tables are serially connected and are self-explanatory. However, here is a brief account about each of the four tables.

Table 1 is the main table. It carries almost all possible offences in the cyber space and also the related provisions in the Information Technology Act 2000 (including the amendments introduced in 2008). Further, it can properly lead the user on to the concerned sections of Table 2, Table 3 and Table 4. In other words, the stand-alone Tables 2, 3 and 4 are as well connected to Table 1and this connection is briefly explained below.

Corresponding to each entry in Table 1, one can find one or more entries in Table 2 where almost all the related offences and the relevant sections in the Indian Penal Code are cohesively arranged.

In addition, against each entry in Table 1, one can find one or more entries in Table 3 where almost all related offences and the relevant sections in other related Acts are properly classified and presented.

Finally, against each entry in Table 1, one can find one or more entries in Table 4 where the pieces of evidence to be collected are structurally detailed along with their sources.

The simplest way to quickly make this handbook functionally useful is by subjecting the received petition through Table 1. For this, the SHO is advised to follow the following step-by-step procedure:

Step 1: First scribble down all the cyber-related offences found in the petition.

Step 2: Go to the 2nd column ("Nature of offence") in Table 1, which carries a list of almost all possible offences. From this list, identify those offences which are relevant to the petition.

Step 3: Go to the 3rd column (IT Act Provisions). This column lists out almost all the provisions in the Information Technology Act which are relevant in the context of the identified offences in the petition. From this list, identify those sections which are relevant to charge case against this petition.

Step 4: Go to the 4th column (Other related Acts). This column properly leads to concerned part of Table 2(which lists out the related IPC provisions) and also

to the relevant part of Table 3 (where almost all the related provisions in the POCSO Act, Kerala Police Act and Kerala Gaming Act are listed). From these parts of the two tables, the SHO is expected to identify those sections which are relevant to charge the case.

Step 5: Go to the 5th column (Cyber Evidence Collection). This column leads to Table 4 where the different types of sources and platforms (from where the relevant pieces of cyber evidence are expected to be collected) are structurally presented.

Thank you for using this handbook. All valuable user feedbacks are welcome and will be given proper treatment while preparing the subsequent version. Please send the user feedback to cyberhandbooksho@gmail.com.

Table 1: Cyber offences and provisions in the IT Act

Sl. No	Nature of cyber offence	IT Act Provisions (B stands for Bailable offence and NB stands for Non Bailable offence) (C stands for Cognizable offence and NC for Non-Cognizable offence)	Provision in other Acts	Cyber evidence collection
1.1	**Threat**	Sec 43(C): Contamination and Virus. Sec 65: Tampering with computer source document. (B) (C) Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B) (C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C) Sec 66E: Violation of privacy. (B)(C) Sec 66F: Cyber Terrorism. (NB)(C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB)(C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	Refer to 2.1,2.2,2.4, 2.5 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.

1.2	**Obscenity**	Sec 66E: Violation of privacy. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C)	Refer to 2.2 and 2.4 in Table 2.	Refer to the appropriate item in Table 4.
1.3	**Intimidation**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer source document. (B)(C) Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) C) Sec 66E: Violation of privacy. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually	Refer to 2.2,2.3 and 2.4 in Table 2.	Refer to the appropriate item in Table 4.

		explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C)		
1.4	**Vulgarity**	Sec 66E: Violation of privacy. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C)	Refer to 2.2 and 2.4 in Table 2.	Refer to the appropriate item in Table 4.
1.5	**Defamation**	Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in	Refer to2.2 and 2.4 in Table 2.	Refer to the appropriate item in Table 4.

		electronic form. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)		
1.6	**Cyber stalking**	Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	Refer to 2.4 in Table 2.	Refer to the appropriate item in Table 4.
1.7	**Mental torture**	Sec 66E: Violation of privacy. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C)	Refer to 2.4 in Table 2.	Refer to the appropriate item in Table 4.
1.8	**Terrorism**	Sec 66F: Cyber Terrorism. (NB) (C) Sec 69: Power to issue directions for interception or monitoring or	Refer to 2.5 in Table 2.	Refer to the appropriate item in

		decryption of any information through any computer resource. (NB) (C) Sec 69A: Sec 69A: Power to issue directions for blocking for public access of any information through any computer resource. (NB) (C) Sec 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. (B) (NC) Sec 70: Protected System Sec 70B: Indian computer emergency response team to serve as National agency for incident response.		Table 4.
1.9	**Cheating**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in	Refer to 2.2 and 2.7 in Table 2 and Refer to 3.3 in Table 3.	Refer to the appropriate item in Table 4.

		sexually explicit act etc. in electronic form. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)		
1.10	**Fraud**	Sec 43: Damage to computer, computer system etc. Sec 43A: Failure to protect data. Sec65: Tampering with computer source document. (B)(C) Sec 66: Computer related offences. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)	Refer to 2.2, 2.3 and 2.7 in Table 2 and Refer to 3.3 in Table 3.	Refer to the appropriate item in Table 4.
1.11	**Fabrication**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer source document. (B)(C) Sec 66: Computer related offences. (B)(C) Sec 67: Publishing or transmitting of obscene material in electronic	Refer to 2.3 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.

		form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)		
1.12	**Forgery**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer source document. (B)(C) Sec 66: Computer related offences. (B)(C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)	Refer to 2.3 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.

1.13	**Software infringement**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer source document. (B)(C) Sec 66: Computer related offence. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) C)	Refer to 2.2 in Table 2.	Refer to the appropriate item in Table 4.
1.14	**Piracy**	Sec 65: Tampering with computer source document. (B)(C) Sec 66: Computer related offences. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) C)	Refer to 2.2 and 2.3 in Table 2.	Refer to the appropriate item in Table 4.
1.15	**Theft**	Sec 43: Damage to computer, computer system etc. Sec 43A: Failure to protect data. Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure	Refer to 2.1 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.

		of information in breach of lawful contract. (B) (C)		
1.16	**Online bank theft**	Sec 43: Damage to computer, computer system etc. Sec 43A: Failure to protect data. Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C)	Refer to 2.1 in Table 2.	Refer to the appropriate item in Table 4.
1.17	**Hacking (attack on password)**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer source document. (B)(C) Sec 66: Computer related offences. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C) Sec 66F: Cyber Terrorism. (NB)(C)	Refer to 2.1, 2.2 and 2.5 in Table 2.	Refer to the appropriate item in Table 4.
1.18	**Spoofing**	Sec 66D: Cheating by Personation by using Computer Resource. (B)(C)	Refer to 2.2 in Table 2.	Refer to the appropriate item in Table 4.
1.19	**Misappropriation**	Sec 65: Tampering with computer source document. (B)(C) Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the	Refer to 2.2 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.

		electronic signature, password or any other unique identification feature of any other persons. (B) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 72: Breach of confidentiality and privacy. (B) (NB) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)		
1.20	**Counterfeiting**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C)	Refer to 2.6 in Table 2.	Refer to the appropriate item in Table 4.
1.21	**Breach of trust**	Sec 43A: Failure to protect data. Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B)(C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 66E: Violation of privacy. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)	Refer to 2.4 and 2.7 in Table 2 and Refer to 3.3 in Table 3.	Refer to the appropriate item in Table 4.
1.22	**Online blackmailing**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C)	Refer to 2.2 and 2.4in Table 2 and	Refer to the appropriate item in Table 4.

		Sec 66E: Violation of privacy. (NB) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C)	Refer to 3.3. in Table 3.	
1.23	**Tampering**	Sec 65: Tampering with computer source document. (B)(C)	Refer to 2.3 in Table 2.	Refer to the appropriate item in Table 4.
1.24	**Phishing, data diddling etc.**	Sec 66: Computer related offences. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C)	Refer to 2.2 in Table 2.	Refer to the appropriate item in Table 4.
1.25	**Child abuse**	Sec 66E: Violation of privacy. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C) Sec 69A: Power to issue directions	Refer to 2.2 and 2.4 in Table 2 and 3.1 in Table 3.	Refer to the appropriate item in Table 4.

		for blocking for public access of any information through any computer resource. (NB) (C)		
1.26	**Fake profile**	Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C)	Refer to 2.2, 2.3 and 2.4 in Table 2.	Refer to the appropriate item in Table 4.
1.27	**Web defacement**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer document. (B) (C) Sec 66: Computer related offences. (B) (C)	Refer to 2.3 and 2.4 in Table 2.	Refer to the appropriate item in Table 4.
1.28	**ATM Online fraud**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C)	Refer to 2.1 and 2.2 in Table 2.	Refer to the appropriate item in Table 4.
1.29	**ATM Physical burglary**	- NIL -	Refer to 2.1 and 2.2 in Table 2.	Refer to the appropriate item in Table 4.
1.30	**Failure to preserve and retain data by intermediaries.**	Sec 67C: Preservation and retention of information by intermediary. (B) (C)	Refer to 2.1, 2.2, 2.3 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.

1.31	**Failure from the certifying authorities or any employee of such authority.**	Sec 68: Power of controller to give directions. (B) (NC)	Refer to 2.1, 2.2, 2.3 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.
1.32	**Failure by the intermediary to assist the agency.**	Sec 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource. (NB) (C) Sec 69A: Power to issue directions for blocking for public access of any information through any computer resource. (NB) (C) Sec 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. (B) (NC)	Refer to 2.7 in Table 2.	Refer to the appropriate item in Table 4.
1.33	**Secure access to computer system**	Sec 70: Protected System	Refer to 2.1, 2.2, 2.3, 2.5 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.
1.34	**Failure to comply with directions of CERT.**	Sec 70B: Indian computer emergency response team to serve as National agency for incident response.	Refer 2.7 in Table 2.	Refer to the appropriate item in Table 4.
1.35	**Offences relating to Digital signature certificate.**	Sec 71: Penalty for Misrepresentation. (B) (NC) Sec 73: Penalty for publishing Electronic Signature Certificate false in certain particulars. (B)(NC)	Refer 2.1, 2.2, 2.3 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.

		Sec 74: Publication for fraudulent purpose. (B) (NC)		
1.36	**Offences committed outside India.**	Sec 75: Offence or contraventions committed outside India.	Refer 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.
1.37	**Offences relating to religion.**	Sec 66D: Cheating by Personation by using Computer Resource. (B)(C) Sec 66F: Cyber Terrorism. (NB)(C) Sec 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. (B) (NC)	Refer to 2.2 and 2.5 in Table 2.	Refer to the appropriate item in Table 4.
1.38	**Offences related to OTP, UPI etc.** (other than petition received within half an hour) (petition received within half an hour of transaction shall be transferred to the online group of Nodal officers)	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	Refer to 2.2 and 2.3 in Table 2.	Refer to the appropriate item in Table 4.

1.39	**Email / Logic bombing**	Sec 43: Damage to computer, computer system etc. Sec 66: Computer related offences. (B) (C) Sec 66F: Cyber Terrorism. (NB) (C)	Refer to 2.1 and 2.2 in Table 2.	Refer to the appropriate item in Table 4.
1.40	**Web jacking**	Sec 66E: Violation of privacy. (NB) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 66F: Cyber Terrorism. (NB) (C) Sec 43A: Failure to protect data.	Refer to Table 2.1 in Table 2.	Refer to the appropriate item in Table 4.
1.41	**Salami attacks**	Sec 43: Damage to computer, computer system etc. Sec 43A: Failure to protect data. Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 67C: Preservation and retention of information by intermediary. (B) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	Refer to 2.1, 2.2 and 2.7 in Table 2.	Refer to the appropriate item in Table 4.
1.42	**Netrespass**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) C)	Refer to table 2.1, 2.2 and 2.7 in Table 2	Refer to the appropriate item in Table 4.

		Sec 66E: Violation of privacy. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC)		
1.43	**Misrepresentation**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 66E: Violation of privacy. (NB) (C) Sec 71: Penalty for Misrepresentation. (B) (NC) Sec 72: Breach of confidentiality and privacy. (B) (NC)	Refer to Table 2.1, 2.2, 2.3 and 2.7 in Table 2 and Refer to 3.3 in Table 3.	Refer to the appropriate item in Table 4.
1.44	**Sale of illegal articles and Trafficking**	Sec 66E: Violation of privacy. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	Refer to table 2.2, 2.3 and 2.4 in Table 2.	Refer to the appropriate item in Table 4.

1.45	**Internet homicide**	-NIL-	Refer to 2.8 in Table 2.	Refer to the appropriate item in Table 4.
1.46	**Internet time theft**	Sec 43(h): charge the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network. Sec 65: Tampering with computer source document. (B)(C)	Refer to 2.1 in Table 2.	Refer to the appropriate item in Table 4.

TABLE 2: Related Provisions in IPC:

Sl. No	Offences (B stands for Bailable offence and NB stands for Non Bailable offence) (C stands for Cognizable offence and NC for Non-Cognizable offence)	Section
2.1	Punishment for theft. (NB) (C)	Sec 379
	Theft by clerk or servant of property in possession of master. (NB) (C)	Sec 381
	Dishonestly receiving stolen property. (NB)(C)	Sec 411
	Punishment for extortion. (NB)(C)	Sec 384
	Punishment for robbery. (NB)(C)	Sec 392
	Punishment belonging to gang of thieves. (NB)(C)	Sec 401
	Punishment for dacoity. (NB)(C)	Sec 395
	Making preparation to commit dacoity. (NB)(C)	Sec 399
	Punishment for belonging to gang of dacoits. (NB)(C)	Sec 400
	Assembling for purpose of committing dacoity. (NB)(C)	Sec 402
	Dishonest misappropriation of property. (B) (NC)	Sec 403
	Dishonestly receiving property stolen in the commission of dacoity. (NB) (C)	Sec 412
	Assisting in concealment of stolen property. (NB)(C)	Sec 414
	Punishment for criminal trespass. (B) (C)	Sec 447
2.2	Punishment for Cheating. (B) (NC)	Sec 417

	Cheating and dishonestly inducing delivery of property. (NB)(C)	Sec 420
	Punishment for criminal Breach of Trust. (NB) (C)	Sec 406
	Criminal breach of trust by clerk or servant. (NB)(C)	Sec 408
	Criminal breach of trust by public servant or by banker, merchant or agent. (NB)(C)	Sec 409
	Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect. (B) (NC)	Sec 418
	Punishment for cheating by Personation. (B) (C)	Sec 419
	Punishment for criminal intimidation. (B) (NC)	Sec 506
2.3	Punishment for forgery. (B) (NC)	Sec 465
	Forgery for the purpose of cheating. (NB)(C)	Sec 468
	Destruction of document or electronic record to prevent its production as evidence. (B) (NC)	Sec 204
	Falsification of accounts. (B) (NC)	Sec 477A
	Punishment for false evidence. (B) (NC)	Sec 193
	Threatening any person to give false evidence. (NB)(C)	Sec 195A
	False Personation for purpose of act or proceeding in suit or prosecution. (B) (NC)	Sec 205
	Issuing or signing false certificate. (B) (C)	Sec 197
2.4	Sale etc. of Obscene books etc. (B)(NB) (C)	Sec 292

	Sale etc. of Obscene objects to young person. (B) (C)	Sec 293
	Obscene acts and songs. (B) (C)	Sec 294
	Sexual harassment and punishment for sexual harassment. (NB)(C)	Sec 354A
	Voyeurism. (Bailable in 1st Conviction and Non Bailable in 2nd Conviction) (C)	Sec 354C
	Stalking. (Bailable in 1st Conviction and Non Bailable in 2nd Conviction) (C)	Sec 354D
	Punishment for Defamation. (B) (NC)	Sec 500
	Printing or engraving matter known to be defamatory. (B) (NC)	Sec 501
	Sale of printed or engraved substance containing defamatory matter. (B) (NC)	Sec 502
	Intentional insult with intent to provoke Breach of peace. (B) (NC)	Sec 504
	Criminal intimidation by an anonymous communication. (B) (NC)	Sec 507
	Words, gesture or act intended to insult the modesty of women. (B) (C)	Sec 509
	Kidnapping, abducting or inducing woman to compel her marriage etc. (NB) (C)	Sec 366
	Punishment for criminal intimidation. (B) (NC)	Sec 506
2.5	Punishment for criminal conspiracy. (Bailable or Non Bailable) (Cognizable or Non-Cognizable)	Sec 120B
	Waging or attempting to wage war or abetting waging of war against the	Sec 121

	government of India. (NB)(C)	
	Conspiracy to commit offence punishable by Sec 121. (NB)(C)	Sec 121A
	Sedition. (NB)(C)	Sec 124A
	Promoting enmity between different groups on ground of religion, race, place of birth, residence, language etc. and doing acts prejudicial to maintenance of harmony. (NB)(C)	Sec 153A
	Imputations, assertions prejudicial to national- integrity. (NB)(C)	Sec 153B
	Intentional insult with intent to provoke breach of peace. (B) (NC)	Sec 504
	Collecting arms etc, with intention of waging war against the Government of India. (NB) (C)	Sec 122
	Punishment for unlawful assembly. (B) (C)	Sec 143
2.6	Making or selling instrument for counterfeiting coin. (NB)(C)	Sec 233
	Making or selling instrument for counterfeiting Indian coin. (NB)(C)	Sec 234
	Possession of instrument or material for the purpose of using the same for counterfeiting coin. (NB)(C)	Sec 235
	Counterfeiting currency notes or bank notes. (NB) (C)	Sec 489A
2.7	Nonattendance in obedience to an order from public servant. (B) (NC)	Sec 174
	Omission to produce document to public servant by person legally bound to give it. (B) (NC)	Sec 175
	Omission to give notice or information to public servant by person legally bound to give it. (B) (NC)	Sec 176
	Refusing oath or affirmation when duly required by public servant to make it. (B) (NC)	Sec178
	Refusing to answer public servant authorized to question. (B) (NC)	Sec 179

	False statement on oath or affirmation to public servant or person authorized to administer an oath or affirmation. (B) (NC)	Sec 181
	False information, with intent to cause public servant to use his lawful power to the injury of another person. (B) (NC)	Sec 182
	Omission to assist public servant when bound by law to give assistance. (B) (NC)	Sec 187
	Disobedience to order duly promulgated by public servant. (B) (C)	Sec188
2.8	Abetment of a thing	Sec 107
	Punishment of abetment if act abetted is committed in consequence, and where no express provision is made for its punishment. (B/NB) (C/NC)	Sec 109

TABLE 3 : Related Provisions in the POCSO Act, The Kerala Police Act and Kerala Gaming Act.

Sl. No	Offence (B stands for Bailable offence and NB stands for Non-Bailable offence) (C stands for Cognizable offence and NC for Non-Cognizable offence)	Section
3.1	Punishment for Sexual harassment. (NB) (C)	Sec 12 of POCSO Act
	Use of child for Pornographic purpose. (NB) (C)	Sec 13 of POCSO Act
	Punishment for using child for Pornographic purpose. (NB) (C)	Sec 14 of POCSO Act
	Punishment for storage of pornographic material involving Child. (NB) (C)	Sec 15 of POCSO Act
3.2	Penalty for causing grave violation of public order or danger.(B) (C)	Sec 118 of Kerala Police Act
	Punishment for atrocities against women. (B) (C)	Sec 119 of Kerala Police Act
	Penalty for causing nuisance and violation of public order. (B) (NC)	Sec 120 of Kerala Police Act
3.3	Penalty for opening, etc., any enclosure, etc., for certain forms of gaming	Sec 3 of Kerala Gaming Act
	Penalty for being found in a gaming house	Sec 4 of Kerala Gaming Act
	Penalty for opening, etc., a common gaming house	Sec 7 of Kerala Gaming Act
	Penalty for being found gaming in a common gaming house	Sec 8 of Kerala Gaming Act
	Penalty for refusing to give name and address and for giving false name and address	Sec 9 of Kerala Gaming Act

Note-1: Certain sections from the following Acts can also be found relevant to the petition received by the SHO.

1. The Copyright Act, 1957
2. Trade Marks Act., 1999
3. The Patents Act, 1970
4. The Immoral Traffic (Prevention) Act, 1956
5. Indecent representation of women (prohibition) Act,1985
6. Prevention of terrorism Act, 2002
7. Terrorist and Disruptive Act,1987
8. Negotiable instruments Act, 1881
9. Foreign Exchange Management Act, 1999
10. Arms Act, 1959
11. Narcotic drug and psychotropic substance Act, 1985
12. Theft Act, 1968
13. Currency notes forgery Act, 1899.
14. Indian explosives Act,1884
15. Protection of civil rights Act, 1955
16. The Banker's Books Evidence Act, 1891
17. Reserve Bank of India Act, 1934

TABLE 4: Evidence to be extracted through Cyber Forensics

Note 1: SHOs are expected to seek expert opinion from qualified cyber forensic experts and make such expert(s) as prosecution witness because cyber forensic technology is often outside the area of expertise of SHO.

Note 2: Seizure procedure shall be carried out only under the guidance of qualified cyber forensic experts.

Sl. No	Platform	Evidence to be collected	Sources of evidence	Procedure and Admissibility
4.1	Peer-to- Peer-technology-based Social Media Apps like Whatsapp, Instagram, Snap chat ,Telegram, IMO etc.	1. Handles, User ID, password, IP address, date and time stamps, phone number, IMEI Code. 2. Owner details (CAF) of the phone number.	1.Social media service provider 2. Source device 3. Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc. 4.Telecom Service Provider	See Sec 91,166A, 166B of CrPc and Sec 65B of IEA.
4.2	Client-Server-technology-Based Social Media apps like facebook,Tiktoc etc.	1. Handles, User ID, password, IP address, date and time stamps.	1. Social media service provider. 2. Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	See Sec 91,166A,166B of CrPc and Sec 65B of IEA.

		2.Owner details (CAF) of the phone number.	3.Telecom Service Provider	
4.3	Operating system	Transaction logs	Operating systems like android, IOS etc. in the source device, event logs.	See Sec 65B of IEA.
4.4	Data base	Evidence of addition of a record or deletion of a record or modification of a record in the tables of database.	Data base, transaction log of the data base, operating system event logs etc.	See Sec 65B of IEA.
4.5	Call / SMS details	Call details record (CDR)	Telecom Service Provider	See Sec 91,166A,166B of CrPc and Sec 65B of IEA.
4.6	Net telephone and other communication	IP Dump/IPDR Dump	Telecom service provider	See Sec 91,166A,166B of CrPc and Sec 65B of IEA.
4.7	Software Copyright Infringement	Evidence of copyright infringement after comparing the 2 sets of software by subjecting them	Plaintiff and defendant software packages in the Storage devices like hard disk,	See Sec 64 of Copyright Act and Sec 65B of IEA.

		through AFC OR POSAR Test.	DVD, CD, Pendrive, SD Card, flash memory etc.	
4.8	Software Theft	Evidence of plaintiff's original possession of the software and evidence of defendant's illegal possession of the software (Sec 328 of IPC).	Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc of both plaintiff and defendant.	See Sec 91,94,95 of CrPc and Sec 65B of IEA.
4.9	Data Piracy	Evidence of plaintiff's original possession of the data and evidence of defendant's illegal possession of the data (Sec 328).	Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc of plaintiff and defendant.	See Sec 91,94of CrPc and Sec 65B of IEA.
4.10	Deleted Data recovery	Deleted file	Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	See Sec 91,94,166A ,166B of CrPc and Sec 65B of IEA.
4.11	Fund misappropriation	Evidence of addition of a record or deletion of a record or modification of a record in the tables of fund databases.	Fund data base, operating system event logs etc.	See Sec 91,94,166A ,166B of CrPc and Sec 65B of IEA.

4.12	Counterfeiting	Name and version of the software tool used for fabrication, date and time stamps and other details from the hex dump of image.	Hex dump of the non-compressed image obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc. Note: These evidence are unlikely to exist in the hex dump of the compressed images received through social media apps like WhatsApp, facebook etc. Try only from the originally fabricated / forged images.	See Sec 91,94,95,166A, 166B of CrPc and Sec 65B of IEA.
4.13	Image / Video fabrication / forgery	Name and version of the software tool used for fabrication, date and time stamps and other details from the hex dump of image/video.	Hex dump of the Image/Video obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc. Note: These evidence are	See Sec 91,166A,166B of CrPc and Sec 65B of IEA.

			unlikely to exist in the hex dump of the compressed images / videos received through social media apps like whatsapp, facebook etc. Try only from the originally fabricated / forged images / videos.	
4.14	Audio fabrication	1.Name and version of the software tool used for fabrication, date and time stamps and other details. 2. Evidence to establish the ownership of the voice as required by forensics linguistic methods.	1.Hex dump of the Audio file obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc. Note: These evidence are unlikely to exist in the hex dump of the compressed audios received through social media apps like whatsapp, facebook etc. Try only from the originally fabricated /	See Sec 91,166A,166B of CrPc and Sec 65B of IEA.

			forged audios. 2.Voice samples from the Audio File.	
4.15	Cyber warfare and Cyber Terrorism	Handles, User ID, password, IP Address, date and time stamps of the source of communication, content of communication (encrypted or not), related activity logs etc.	1. Related devices and networks, CDR, IP dump, IPDR dump. 2.Operating system event logs etc obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	See Sec 91,94,166A, 166B of CrPc and Sec 65B of IEA.
4.16	Cyber attacks	Handles, User ID, password, IP Address, date and time stamps of source, related activity logs etc.	1. Related devices and networks, CDR, IP dump, IPDR dump. 2.Operating system event logs etc obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	See Sec 91,166A,166B of CrPc and Sec 65B of IEA.
4.17	E-mail communication	Handles, User ID, password, E-Mail	Source code of the received	See Sec 91,166A,16

		address, IP addresses, date and time stamps of the sender and other dispatch details.	Email. Additional information: Sender's details are to be collected from Email service provider.	6B of CrPc and Sec 65B of IEA.
4.18	Theft of documents using the Outbox of the E-mail system.	Handles, User ID, password, Date and time stamps of uploading to and the subsequent downloading from the Outbox.	Outbox of the E-mail system.	Sec 65B of IEA.
4.19	Cyber spoofing	Handles, User ID, password, Original IP address, details of the software tool used for spoofing, date and time stamps of spoofing.	1. The App and the Device used for spoofing, related networks etc. 2. Operating system event logs etc obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	See Sec 91,166A,16 6B of CrPc and Sec 65B of IEA.
4.20	Hacking	Handles, User ID, password, IP	1. Related devices and networks,	See Sec 91,166A,16

		Address, date and time stamps of the source, related activity logs etc.	CDR, IP dump, IPDR dump. 2.Operating system event logs etc. obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	6B of CrPc and Sec 65B of IEA.
4.21	Ransomware attacks	Handles, User ID, password , IP address, date and time stamps of the source, decryptions keys, related activity logs etc.	1.Source device, related network devices etc. 2.Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	See Sec 91,166A,166B of CrPc and Sec 65B of IEA.
4.22	RAM Analysis	Necessary Artifacts from RAM	RAM of Mobile, Computer, Electronic weighing machines, Electronic meters etc.	See Sec 91,166A,166B of CrPc and Sec 65B of IEA.
4.23	CCTV Video Clippings	1.Required scenes 2. Date and time stamps of the required scenes. 3. Original video	Hardisk of the CCTV system	See Sec 91,166A,166B of CrPc and Sec 65B of

		creation details from the hex dump of the video clipping obtained from the hard disk of the CCTV system.		IEA.
4.24	Steganographic images / videos/ audio.	1. Name and version of the software tool used for fabrication, date and time stamps and other details from the hex dump of image/video. 2. The software codes inserted through Steganographic technique have to be separated from the image / video and then to be analyzed with the objective of finding the fraudulent motives of the codes.	Hex dump of the image. Note: These evidence are unlikely to exist in the hex dump of the compressed images / videos / audio received through social media apps like whatsapp, facebook etc. Try only from the originally fabricated / forged images / videos/ audio.	See Sec 91,166A, 166B of CrPc and Sec 65B of IEA.
4.25	ATM withdrawal through victim's A/C.	Handles, user ID, password, IP address, date and time stamps and bank details.	From the respective bank manager.	See Sec 91,166A, 166B of CrPc and Sec 65B of IEA.

4.26	Card details theft using skimmer and PIN theft using camera.	Skimmer details and camera details.	ATM, skimmer, camera.	See Sec 91,166A, 166B of CrPc and Sec 65B of IEA.
4.27	Card details theft using a Wi-Fi Modem spliced on the broadband cable.	1. Wi-Fi modem details. 2. Date and time stamps of spicing to be obtained from the event logs of the bank network server. 3. Stolen data to be recovered from the criminal's computer.	ATM fraudulently spliced, Wi-Fi modem, camera, bank network server etc.	See Sec 91,166A, 166B of CrPc and Sec 65B of IEA.
4.28	Online Banking	1. Debit card number. 2. Name of the account holder. 3. Bank with branch. 4. SMS received regarding the transfer. 5. Cash transfer details from bank. 6. Recipient's bank A/C details / E-wallet details.	Items 1 to 4 to be collected from the account holder. Item 5 to be collected from the account holder's bank. Item 6 to be collected from the recipient's bank.	See Sec 91, 166A, 166B of CrPc and Sec 65B of IEA.

CYBER LEGAL HANDBOOK
for
Station House Officers

Telangana State Police

www.tspolice.gov.in