INVESTIGATION OF CYBER OFFENCES AND CYBER POLICE IN INDIA: AN ANALYTICAL STUDY

Written by ***Dr. Shiv Raman* & Ms. Nidhi Sharma*****

** Assistant Professor, Amity Law School, Amity University Gurugram, Haryana, India*

*** Assistant Professor, Amity Law School, Amity University Gurugram, Haryana, India*

INTRODUCTION

Another way for the protection and detection of Cyber-crimes in India is- Crime and Criminal tracking system, which is approved by the Central Govt. in 2009 under national E- Governance project to detect Cyber-crimes in India by using IT, enabled tracking and Crime detection system. But unfortunately, till today it is not completed by all the States in India.

DETECTION OF CYBER-CRIMES

There are different ways to deal with detection of different Cyber-crimes. These Cyber-crimes can broadly be divided in to two parts:

1	Cyber-crimes, where Computer is target for Cyber Offence.
2	Cyber-crimes, where Computer used as a mean(s) for the commission of crime.

The Investigation process of such crimes is often not exactly similar as other crimes.

The process of cyber investigation:

Cyber-crimes usually transgress geographical hurdles. Cyber-crime is a fast-growing meadow of crimes. The Cyber criminals are exploiting the speed barriers and anonymity of the internet for the commission of different types of criminal activities. No border, virtual or physical, can cause serious harm and rise real threat to worldwide victims other than Cyber-crimes.[i]In order to deal with the issue of Cyber-crimes, the Criminal Investigation Department (CID's) of various cities established, Cyber Crime Cells (CCC) in various parts of the country. The IT Act, 2000 made it clears that- *'whenever a Cyber-crime has been committed, it has a global jurisdiction and hence a complaint can be filed at any Cyber cell'.*[ii] Therefore to combat Cyber-crimes, the CBI (Central Bureau of Investigation) has created specialized units:

1. • Cyber Crimes Investigation Cell (CCIC)
2. • Cyber Crimes Research & Development Unit (CCRDU)
3. • Cyber Forensics Laboratory (CFL)
4. • Network Monitoring Centre

iii

1. **Cyber-crimes Investigation Cell (CCIC):**

The CCIC was established in Sep. 1999. The CCIC has jurisdiction in all over the India. It acts as a part of division of economic offence. CCIC is empowered to investigate all the Cyber-crimes under IT Act, 2000. CCIC also acts round the clock as Nodal point of contact Interpol to report Cyber-crimes in India. The CCIC of India is also a member of 'Cyber-crimes Technology Information Network System, Japan'.

2. **Cyber-crimes Research and Development Unit (CCRDU):**

It's the responsibility of CCRDU to track the development and changes, which take place in ever changing area. It has the following functions:

1	To ensure cooperation and coordination with State Police forces.
2	To collect and compile the data of reported Cyber-crime cases to Police for investigation.
3	To coordinate with software experts in identification of areas, which require attention of State Police?
4	To obtain the information of Cyber-crimes cases reported in other countries and prepare a monthly Cyber-crime digest.

3. **Cyber Forensics Laboratories (CFL):**

The Cyber Forensic Laboratories are one of the primary wings of Cyber Investigation to provide investigative services in computer forensics (digital forensics), forensic data revival, and digital evidence detection. CFL could analyze the forensic data and recover digital evidence while maintaining the veracity of the electronic evidence for detection and trial. The basic functions of the Cyber Forensics Laboratory (CFL) are-

1	To find out and Scientific analysis of Digital Foot- Print.
2	To provide scientific analysis in support of the Crimes Investigation by Law enforcement Agencies and CBI.
3	To assist on site for Computer seizure and search on request.
4	To provide consultation services for activities or investigations, where media analysis is probable as occurring.
5	To provide expert testimony.
6	To provide adequate research and development in Cyber forensics.

The information and analysis so collected can be used as evidence in court of law. That aspect is discussed in details in later part of the chapter.

4. Cyber crime Investigations:

The Cyber-crimes can be defined as- ***'a crime in which a Computer is the object of the crime or is used as a tool for the commission of cyber offence'.*** The Cyber-crime can also be defined as – ***'a crime where Computer is the target or a crime committed through the use of a Computer'***. There is a long list of identified Cyber-crimes. All the crimes have different legal punishment provided in Information Technology laws.

The Cyber-crime Investigation is almost similar to the investigation of regular crimes, except the Cyber investigators use Computer as tool of Investigation and data as sources of evidences. The investigation of Cyber-crime has consequently become a highly specialized professional field.[iv]

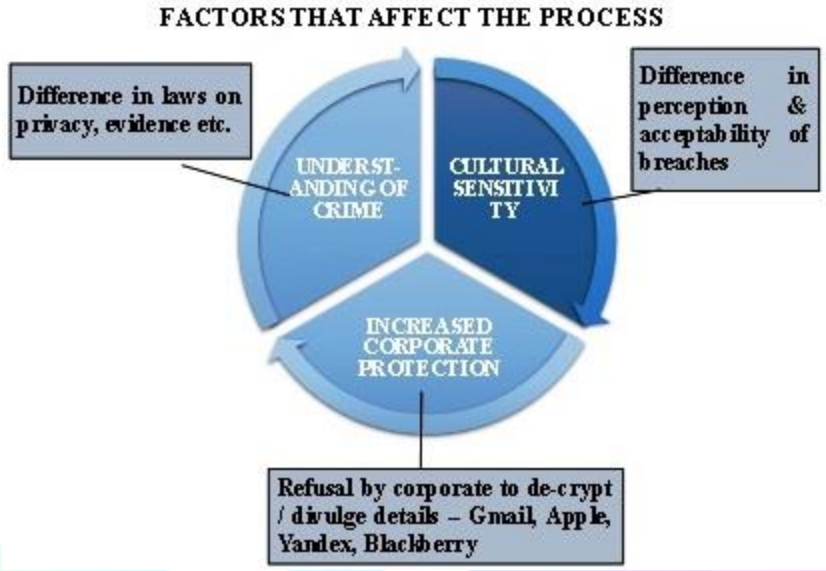
5. Hurdles/ Barriers in Investigation of Cyber-crimes:

Generally, a Cyber Crime investigator has to face so many complexities while doing investigation. Here below is list of some complexities in:

1	Obtaining the cooperation of witnesses
2	Selection of appropriate Cyber jurisdiction
3	Practical and Logical barriers
4	Identification of suspects
5	Search and seizure of E- documents and devices
6	Encryption of problems
7	Securing and locating of relevant material
8	Lacking of mutual assistance

9	Securing extradition of cyber criminal

These hurdles can be removed by harmonizing laws and technical expertise of investigation and sharing information between Police and private sector investigations and enhancing International cooperation.[v]Furthermore Cyber Investigator has to face some practical and technical issues for a fair and honest Cyber investigation due to following reasons:



[vi]

6. Relevant Legal Provision in Cr.Pc, 1973 for Cyber Investigation:

The Code of Criminal Procedure, 1973 contained various legal provision regarding the investigation of Criminal offence which is also applicable to Investigation of Cyber offences also. Here below is list of those legal provisions:

1	Power of Police when arrest without warrant-Sec. 41
2	Power to search of place entered by person sought to be arrested- Sec. 47
3	Issuing summons to produce document or other thing- Sec. 91
4	Grounds when search warrant may be issued- Sec. 93
5	Power to search of place suspected to contain stolen property, forged documents, etc.- Sec. 94
6	Power of Police officer to seize certain property- Sec. 102
7	Power of Police arrest to prevent the commission of cognizable offences- Sec. 151
8	Procedure to be adopted for investigation- Sec. 157

9	Investigation report submitted to magistrate- Sec. 158
10	Police officer's power to require attendance of witnesses- Sec. 160
11	Power of Police of examination of witnesses- Sec. 161
12	Power of search by Police officer- Sec. 165
13	When officer in-charge of Police station may require another to issue search warrant- Sec. 166
14	Letter of request to competent authority for investigation in a country or place outside India- Sec. 166A
15	Procedure when investigation cannot be completed in twenty-four hours- Sec. 167
16	Police diary of proceedings in investigation- Sec. 172
17	Report of Police officer on completion of investigation- Sec. 173
18	Power to summon persons Sec. 175[vii]

The followings charts are showing the Seizure process to be adopted by a Cyber Investigator with precautions **(Chart No. 1 & 2)** and the submission report after investigation **(Chart No. 3)**:

Chart No. 1: The Seizure of Digital Evidence Process

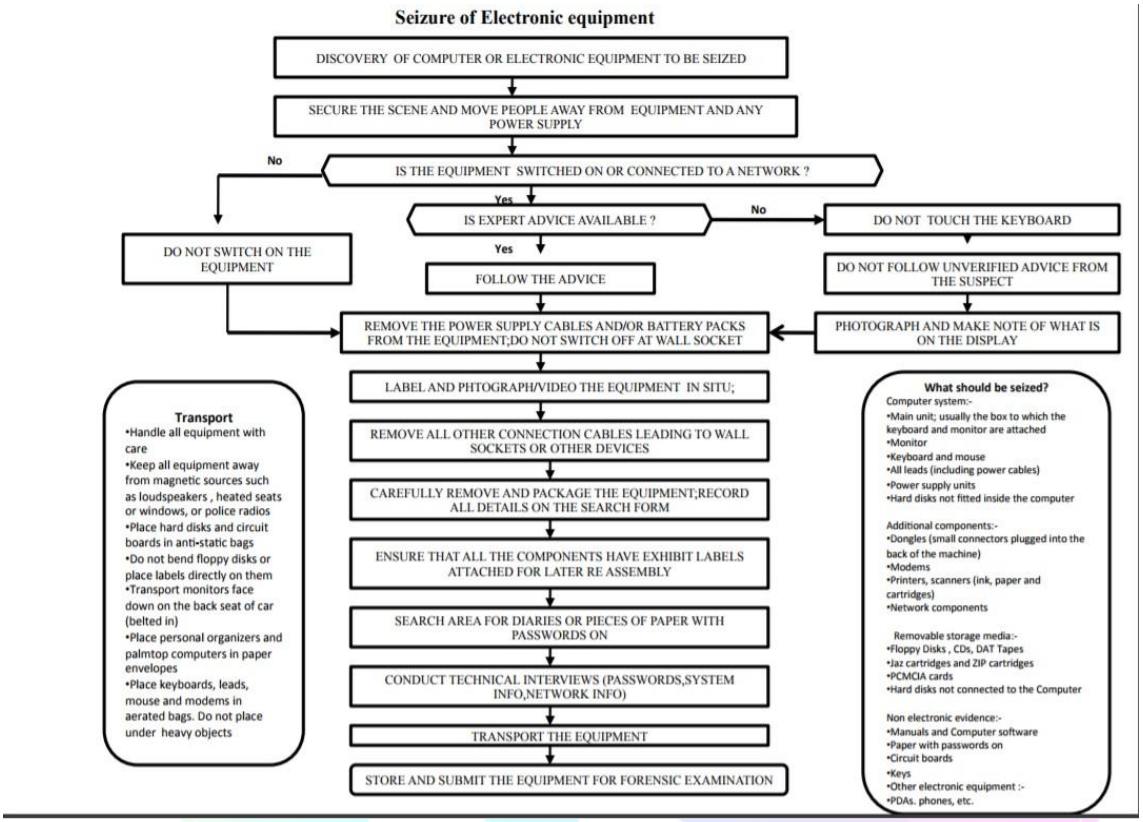
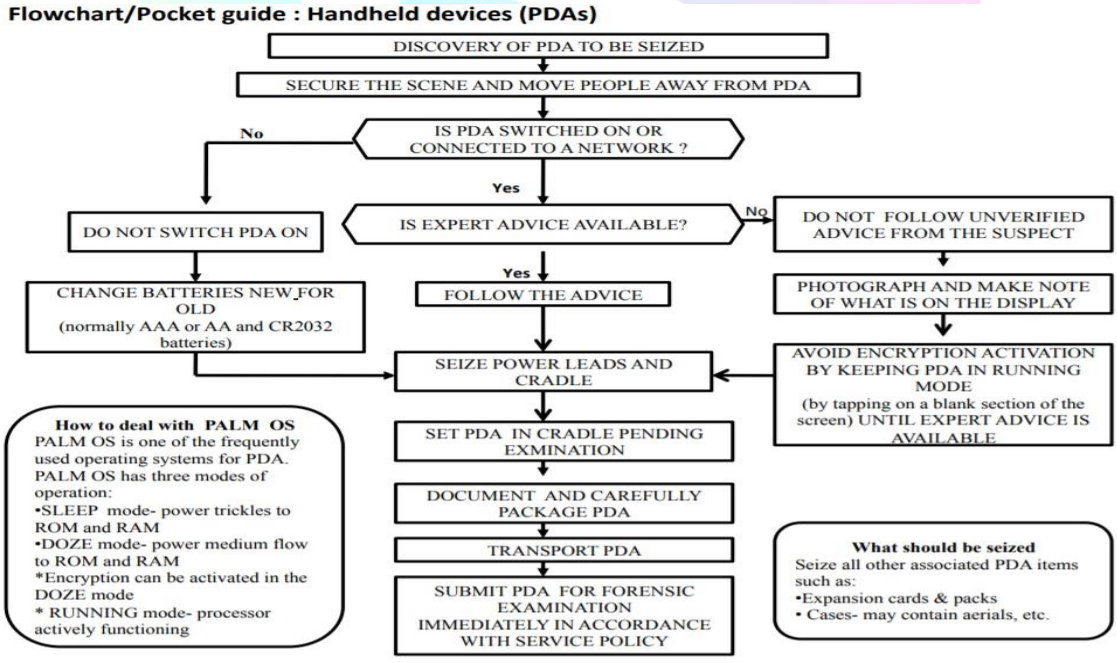
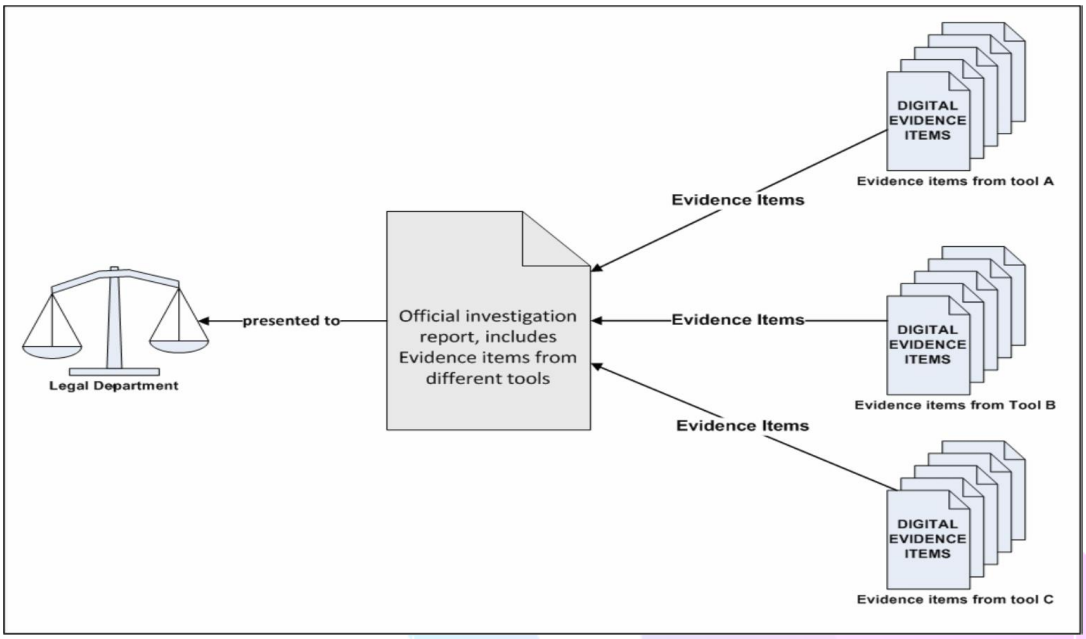


Chart NO. 2:



viii

Chart No. 3: Submission of Report after Investigation:



7. Determination of Cyber Criminal Jurisdiction, Provisions in Cr. Pc, 1973 and It Act, 2000:

The origin of word jurisdiction has origin from the Latin word '*jus, juris* and *diare'* meaning thereby *'Law' and 'Speak'.* Jurisdiction and competency of the court is the most important aspects of every Criminal Justice System. Every jurisdictional error and incompetency of court is always an error of law of court. Every court has inherent right to decide these things. A decision without jurisdiction and incompetency is a ***coram non judice*** and *denial of justice.* Jurisdiction is the legal and statutory right of the court to hear and decide a case.

Today cyber-world has no geological precincts. It can establish instant remote communications with anyone who can have access the computer or Internet. Generally, web-user is unaware of source and the network and servers/routes exactly from where the information on a site is being accessed. Jurisdictional issues are of primary importance in Cyber-world. World Wide Web (www) does not make the clear geographical and jurisdiction border. The web user though physically in one place but may be in jurisdiction of other country virtually or technologically. Even a single Cyber /web- transaction may engross the laws of at least three jurisdictions. Those are:

1	The laws of the Country/ State where- the user victim or accused reside.
2	The laws of the Country/ State of the location of transaction-server host.

3	The laws of the Country/ State of the person or business with whom the transaction takes place.

*Technically even the intermediary server hosting Country/ State also have jurisdiction for being the Intermediary both accessory and victim of Cyber-crime. Here below is the list of legal provisions enumerated in Code of Criminal Procedure Code, 1973 and Information Technology Act, 2000 which deal with the determination of jurisdiction for Investigation of Cyber Offences:

1	Place of Trail/ Inquiry where the offence was committed- Sec. 177
2	If the offence committed in more than one jurisdiction- any of the relevant jurisdiction- Sec. 178
3	Where the accused found to possess the property obtained in theft, extortion or stolen property- Sec. 181
4	Offences Committed by letters, massages- where send or received- Sec. 182
5	Offences committed outside India by a Indian citizen, on aircraft registered in India, tried as if offence committed in India with prior sanction of Central Govt.- Sec. 188
6	Period of limitation to take cognizance- Sec. 468
7	Confiscation of any Computer or accessory liable to be confiscated if used for commission of offence- Sec. 77 r/w Sec. 81 of IT Act, 2000.
8	Compensation, penalty, confiscation not to interfere with other remedies under statutes
9	Compounding of offences, where the sentence is below 3 years Sec. 77A of IT Act, 2000
10	Offence with 3-year punishment are bailable- Sec. 77B
11	Power to investigation is given to Inspector and above the rank of Inspector-Sec. 78 of IT Act, 2000
12	Inspection provision- to be consistent with Sec. 80, which gives the power of Police Inspector/ officer to search and arrest, without warrant any person who has committed, is committing or about to commit any offence under IT act, 2000- Sec. 80

8. Rules in CBI Manual, 2005 for Investigation of Cyber-crimes, Ch- 18:

In order to deal with Cyber-crimes effectively, the Central Bureau of Investigation (CBI) is empowered with its other Units (which we have discussed in Chapter), under Chapter-18 of the CBI Manual, 2005 made the followings arrangements for cyber investigations as:

1	Cartridges or disk- can be used for storage of copies of files from Computer, useful for investigation
2	Labeling of Evidence- Label cables, where they are plug in, disks, the various other parts of computer and to write /protect disks
3	Dismantle the hardware with screwdrivers 7 other tools for the purpose of seizure
4	Use of Gloves- Often latest prints can be taken from disks or other storage hardware or media
5	Material needs for packing- Tapes, boxes, rubber bands, bubble wrap and if he does not have access to anti-static wrap then papers, bags can be used.
6	Recording Equipment- to video graph and taking photographs of the crime scene
7	Custody of report sheets and other paper for inventories and seize evidences[ix]

9. Steps to be taken by Cyber Investigators for Investigation of Cyber offences:

A Cyber Investigator is required to take certain steps and to follow a specified procedure for the Investigation. In investigation process of every crime, the Investigator must first determine the explicit basics of the crime and whether the laws in their jurisdiction could strong enough to sustain prosecution. For example, can the charges be sustained even if guilt is proven? It is often advantageous to seek advice from with the prosecutor to gain additional insight into specific crimes.

10. Accomplishment of Preliminary Investigation:

While conducting a cybercrime investigation, regular investigative methods are still important. Asking who, what, where, when, why and how, these questions is still important. The investigator should ask the following questions:

Qus.	Who are the possible suspects?
Qus.	What crimes were committed?
Qus.	Were these crimes limited to India's jurisdiction?
Qus.	What evidence is there to collect?

Qus.	What types of physical and digital evidence were involved with the crime?
Qus.	Does any of the evidence need to be photographed/ preserved immediately?
Qus.	When were the crimes committed?
Qus.	Where the physical and digital evidence might be placed?
Qus.	How can the evidence be preserved and maintained for court proceedings?[x]

11. Steps to be taken by Investigators:

The Cyber-crime Investigator to take the followings steps for the investigation of Cyber offence:

1	To take the digital evidence from hard-disk, biometric devices, smartcards, digital cameras and answering machines, prints, PDAs, CDs, modems, scanners, servers, pen-drives, GPS, keyboard, Fax machines, and mouse's in secure storage devices.
2	Take pictures of Crime-scene, if Computer screen is ON, and then take the pictures, videos or note in Memo of seizure.
3	Drawing of Network architecture, sketch/ video/ photograph.
4	To prepare a set of questions for FSL lab examination & write the name of individual present there,
5	Position of equipment, password slips, details of the modem used, details of the Network connections, papers.
6	A list of suspected person and mitigation actions.
7	After incident used logs, system alarms, service provider details, user names, back-up plan, user management software, CCTV footages- if any.
8	Wi-Fi connection and its details, to protect media from magnetic field, right of accession.[xi]

12. Latest Reported matters on Cyber-crime Investigation:

1) Sting Operation Campaigning of '*Aam Aadmi Party*':

The Digital evidence all over the world, have own complexities and utilities, which need certain additional safeguards before that made admissible in the court of law.

The use of Mobile forensics in India is very less. The mobile phones are rarely sent to central cyber forensics laboratories for examination. It increased a long-backlog of pending

examinations and lingers on the cases for an unlimited time. One more thing about digital evidence is improper acquisition of digital evidence can make it inadmissible.

The Anti-Corruption Bureau of India has recently removed this lacuna and incrimination aspect while analyzing the digital data obtained during ***the sting operation campaigning*** of Aam Aadmi Party. The Aam Aadmi Party's sting operations seem to have slight impact upon dishonest officials. Merely about 30 people have acted on the Chief Minister's advice to secretly doing of these sting operations. The Anti-Corruption Bureau affirmed that- most of these recordings are of very poor quality that it could not be the basis of action. Those recordings were not clear and also the complainants are not to ask incriminating questions. After the launch of anti-corruption helpline, the Anti Corruption Department has received about 40,000 calls in first week. Now the officials are guiding the callers on properly conducting sting operations.

2) Mobile Forensics Would Solve Northern Railways Recruitment Paper Leak Case:

Now the mobile phones are commonly used for commissions of crimes. It includes conventional crimes and modern technology linked crimes. Mobile phones have valuable digital evidence which is relevant for trial. Our law enforcement agencies are away from complicated mobile forensics investigations. However, that would be necessary for them to do so in future. The Indian telecom companies are still unaware of least concern of Indian laws pertaining to preservation of digital evidence pertaining to various cases. They are violating the provisions of Information Technology Act, 2000 and the Information Technology (Intermediaries Guidelines) Rules 2011. The investigators in Northern Railways recruitment Exam have summoned 50 persons for interrogation.

The police arrested six persons for possessing coded slips of solved answers. Total four mobile phones were also confiscated, used by the master minds. Two of the accused had deleted SMSs of particular questions prior to their entry in examination centre and investigators have not found any text message connected to the questions on their mobiles. All the mobiles were sent to Central Forensic Science Laboratory for retrieving the deleted messages and the reports were pending.

CONCLUSION

After the above discussion we can conclude that- *'Cyberspace presents a challenging new frontier for criminology, police science, law enforcement and policing. Since the 1990s, academics and practitioners have observed how cyberspace has emerged as a new field of criminal activity.'*- **Gottschalk, Petter (2010).**

This aspect has changed the modes, nature and scope of criminalization and victimization. The legislative will and initiative is very significant, which is required to amended from time to time. Further then the legislative framework, even the NCCS (National Cyber Security Strategy) is very essential. Our Country must aim to develop a very secure and pliant cyberspace for cyber citizens, Netizens, businesses and government organizations. A Cyber security law develop and articulates the vision, objectives, guiding principles and approach to meet cyber security targets. The advancement of Cyber Crime Investigation Modules, hands on training to cyber-crime investigators on Cyber Crime Investigation and Forensics, accessibility of required devices and equipments with the State Forensic Science Laboratories and infrastructure are other important determinants in effective cyber-crime policing and investigation. Finally, we can say - more professionalism, more expertise, updated technologies, experts and analysts required for cyber-crime investigation and cyber policing ever before.

ENDNOTES

[i] IJSTM.com, Vol. No. 6, Issue No. 04, April 2017.
[ii] How to Register Cyber Crime Complaint with Cyber Cell of Police- online Complaint procedure- by Ramanuj, May 25, 2014.
[iii]Available at https://www.yumpu.com
[iv] https://www.yumpu.com
[v] Available at www.slideshare.net
[vi]Available at http://www.nja.nic.in
[vii] Bare Act, The Code of Criminal Procedure, 1973.
[viii] Secure of Digital Space by Dr. S. Murugan IPS- https://www.slideshare.net/prpoint/secure-digital-space-by-dr-s-murugan-ips

[ix] Available at https://www.yumpu.com/en/document/view/28923514/crime-manual-2005-full-in-pdf-central-bureau-of-investigation
[x] Available at http://www.iacpcybercenter.org/officers/cyber-crime-investigations/
[xi] Available at http:slideshare.net/karnikaseth/cybercrime-investigations-and-it-act2000.