

## **“Investigation & Nabbing of Accused in Cyber Crime/Offences”**

*Abhinit Verma  
New Law College  
Pune*

The investigation machineries in India still follow the tools of traditional usage. Due to the very use of traditional methods of investigation, the rate of conviction is comparably low in India to the other nations. Investigation is something that cannot be a uniform process. The method of investigation changes as per the demand & circumstances of the cases. In every cyber related issues the first step is to investigate the matter. Therefore, the process of investigation must be established & the usage of special skills & scientific tools must be taken into consideration.

### **Investigation in Cyber Crime-**

Investigation is the process to bring the truth with the availability of evidences. When a cybercrime related offence is committed and the matter comes to the police, the police have the sole authority of investigating the matter along with the power to arrest the accuse under section 78 & section 80 of the IT Act.

Although the Indian legal system introduced the IT act, but the said act is more business law in nature and therefore the conventional criminal laws are followed while investigating the matter of cyber-crime. The IT Act 2000 provides special procedure to be followed while investigating the matter related to cyber-crime but at the same time the conventional procedural laws cannot be waved off. After the amendment of 2008, the act empowers an officer of the rank of inspector to investigate the matter under this act.

### **Processing steps of conduction of investigation-**

Digital forensic department/agency is concerned with the conduction of investigation of crime related to the cyber issues and the team after the investigation process catch hold the accused to put him/her behind the bars.

The word ‘forensic’ simply means- to investigate the matter with the application of scientific methods and techniques.

The development of science gave birth to the digital forensic, which is aiding a lot for the investigation of cybercrime issues & traditional crime investigation.

### **Investigating process:-**

#### **1. Acquisition**

When a digital forensic expert goes to the crime scene for investigation, then the first thing he shall do is- acquire all those systems, digital devices, computer devices, machines for the process of investigation as these things might provide evidences related to the crime. So,

basically here the forensic expert has to identify all those things which might provide essential information under the process of investigation.

Some of the major steps to be followed during the process of acquisition are-

- i) Labelling the setup.
- ii) Classify/Assign/tag all parts
- iii) Shutting down devices
- iv) Disassemble the setup
- v) Assimilate the documents.

## **2. Data Acquisition**

After the acquisition of devices found at the crime scene, the next step of the investigation is data acquisition.

As the devices have been acquired, therefore, now the team of forensic experts will collect the data from the storage devices such as- hard disks, CD-ROM, pen drives, etc.

After the collection of data they need to distinguish between relevant data & irrelevant data & as so as they collect the relevant data, they need to put it in the form of evidences.

## **3. Data Recovery**

Data recovery is one of the most important parts of cyber investigation. It may happen that the cyber-criminal would have deleted the original data stored in the computer, which would have been a major evidence to track the cyber-criminal. Therefore, it is the responsibility as a digital forensic expert to recover the hidden, deleted, and lost data.

By using the tools and techniques of digital forensic it is possible to recover deleted data of a month or even a year.

## **4. Forensic Analysis**

After the availability of all the data found at the crime scene and the recovered data, the digital forensic team sits together and analyse the data thoroughly. It is necessary to bring out meaningful information from the data collected from all the devices acquired. Therefore, with due process the data are analysed and put forward in the court of law in the form of evidences.

## **5. Presentation**

The last step to be performed in the investigation process is the presentation. After due process of investigation the task of presentation plays an important role in the court of law. Therefore, with all the evidences collected and information gathered, the final duty is to

present all the curricular in a form which would provide justice to the victim and punish the criminal for the said crime committed.

- ❖ As we know that we still follow the traditional method of investigation but as an exception the state of Maharashtra has used the information technology more efficiently & created two important computerized systems known as CIPA and CCIS. These computerized systems consist of database of criminals & their records which helps the investigating officer to access the information without performing field work.

### **\*Challenges in the process of Investigation**

There are certain challenges that an investigating officer faces during the process of investigation. Such as –

#### **a.) Jurisdiction & Problem**

In cybercrime related issues it is very difficult to frame the jurisdictional power. While the investigation is performed the investigating agency has to carry out the process of search & seizure, etc. Therefore, to accomplish the investigation procedure the aspect to determine jurisdiction is the most important thing which is one of the most difficult tasks to perform in the cases related to cybercrime.

#### **b.) IP address & Investigation**

Whenever a cybercrime offence is committed by using a system or a computer, the best way to trace the culprit is through the IP address i.e. the Internet Protocol address. But many a time's proxy servers are used by the criminals which creates a lot of problem to trace the cyber-criminal through the particular IP address.

Although the amendment of 2008 has modified the nature of law related to cybercrime, but still there are numerous problems before the investigating machineries. Therefore, the basic principle of investigation has to change and new tools and techniques have to be effectively implemented.