Universe International Journal of Interdisciplinary Research
(International Peer Reviewed Refereed Journal)
DOI No. –05.2023-86314248

© UIJIR | ISSN (O) – 2582-6417
MAY 2023 | Vol. 3 Issue 12
www.uijir.com

NABBING OF A CYBER CRIMINAL – THE INVESTIGATION PROCESS

Author's Name: Ms. Ananya Kumar[1], Dr. Poonam Verma[2]

Affiliation:

1. Ph.D Research Scholar Gautam Buddha University, Greater Noida, UP, India
2. Assistant Professor, Gautam Buddha University, Greater Noida, UP, India

Corresponding Author Name & E-Mail: Dr. Poonam Verma ,pverma279@gmail.com

Abstract

In India, the apparatuses for conducting investigations still adhere to the tools that have traditionally been used. In India, where conventional methods of investigation are still widely used, the percentage of people found guilty of crimes is far lower than it is in other countries. An investigation is not something that can be done in a standardised manner. The strategy for the investigation shifts according to the demands placed on it and the specifics of each case. The first thing to do in any situation involving cyberspace is to conduct an investigation into the topic. As a result, the procedure of the inquiry needs to be developed, and it is necessary to take into consideration the utilisation of specialised talents and scientific equipment.

Keywords: Investigation in cyber-crime, IT Act 2000, cyber-criminals

DOI: https://doi-ds.org/doilink/05.2023-86314248/UIJIR

INTRODUCTION

The investigative mechanisms in India continue to rely on traditional methods and techniques. The employment of conventional investigative techniques in India has resulted in a relatively lower rate of conviction in comparison to other countries. The process of investigation is inherently non-uniform. The approach to inquiry varies depending on the exigencies and conditions of the cases. The initial course of action in any cyber-related matter is to conduct an investigation. Hence, it is imperative to establish a systematic process of inquiry and take into account the utilisation of specialised skills and scientific instruments.

INVESTIGATION IN CYBER CRIMES

The process of investigation involves the gathering and analysis of evidence in order to uncover the truth. In instances where cybercrime has been committed and reported to the authorities, the police are granted exclusive jurisdiction to conduct an investigation and detain the alleged perpetrator in accordance with the provisions outlined in sections 781 and 802 of the Information Technology Act. Despite the fact that the Indian legal system has adopted the IT act, this act is more business law in nature3; therefore, the conventional criminal laws are applied when investigating cybercrime. The Information Technology Act of 2000 specifies a special procedure to be followed when investigating cybercrime, but standard procedural laws cannot be disregarded4. After the 2008 amendment, an officer with the rank of inspector is authorised to conduct an investigation under this act5

STEPS OF CONDUCTING AN INVESTIGATION: THE PROCESS

A digital forensic department or agency is concerned with the conduct of investigations into crimes related to cyber concerns, and the team, after the investigation process has been completed, catches hold of the accused in order to place him or her behind bars.
To conduct an investigation of a problem using scientific procedures and techniques is what is meant by the term "forensic," which has a very straightforward meaning.

---

1 Power to investigate offences - Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer of not less than the rank of [Inspector] shall investigate any offence under this Act.
2 Power of police officer and other officers to enter, search, etc.- (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer not below the rank of Inspector or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without a warrant any person found there who is reasonably suspected of having committed, of committing, or of being about to commit an offence under this Act.
Explanation-
For purposes of this subsection, "Public Place" refers to any public conveyance, hotel, store, or other location intended for or accessible to the general public.
If a person is arrested under subsection (1) by an officer other than a police officer, that officer

DOI: https://doi-ds.org/doilink/05.2023-86314248/UIJIR

shall, without undue delay, bring or send the person arrested before a magistrate with jurisdiction in the case or the officer in command of a police station.
Subject to the provisions of this section, the provisions of the Code of Criminal Procedure of 1973 shall apply to any entry, search, or arrest made pursuant to this section.
3 IT Act, 2000 is based on the UNICTRAL MODEL LAW
4 The standard laws being used by the Criminal Procedure Code
5 Substituted in 2009, earlier the minimum rank was of DSP.

The advancement of science led to the development of digital forensic, which is proving to be of great assistance in the investigation of cybercrime issues as well as more traditional forms of criminal activity.

INVESTIGATING PROCESS:

ACQUISITION THE DEVICE

When a digital forensics expert visits a crime scene to conduct an investigation, the first thing he must do is acquire all systems, digital devices, computer devices, and machinery for the investigation process, as these objects may contain evidence relating to the crime.
In this particular stage of the investigation, the forensic expert is tasked with locating all of the items that have the potential to provide crucial pieces of information to the team.
During the process of acquisition, some of the most important steps that need to be taken are as follows:

[1] Labelling the setup.
[2] Categorise, assign, and label all of the components.
[3] Powering down all electronic apparatus
[4] Deconstruct the configuration (dissembling the device or evidence)
[5] Assimilating the papers.

ACQUISITION THE DATA

The gathering of data is the next stage of the investigation, following the retrieval of any electronic devices that were discovered at the crime scene.
Since the devices have been obtained, the group of forensic experts will now collect the data from the various storage devices, which may include hard discs, CD-ROMs, flash drives, and other similar items.

After they have gathered the data, they must differentiate between relevant data and irrelevant data, and as soon as they have gathered the relevant data, they must put it in the form of evidences.

RECOVERY OF THE DATA

The process of data recovery is among the most essential aspects of an online inquiry. It is possible that the cybercriminal would have deleted the original data that was stored in the computer, which would have been a significant piece of evidence that might have been used to trace down the

DOI: https://doi-ds.org/doilink/05.2023-86314248/UIJIR

cybercriminal. For this reason, it is the obligation of a digital forensics professional to recover the data that has been buried, erased, or lost.

It is feasible to recover deleted data from a month or even a year ago by making use of the tools and techniques that are associated with digital forensics.

presented in the form of evidence inside the legal system by due process.

PRESENTING THE INVESTIGATION

The presentation of the findings is the very last thing that needs to be done in the inquiry process. Following the completion of all necessary steps of the investigation, the task of presentation plays a significant role in the legal system. The final job, then, is to present all of the curricular material in a form that would offer justice to the victim and punish the criminal for the crime that was committed, using all of the evidence that was collected and all of the information that was obtained.

- CIPA and CCIS are two significant computerised systems that have been developed by the state of Maharashtra. Despite the fact that we continue to employ the conventional approach to conducting investigations, this is an area in which the state of Maharashtra has made innovative use of information technology. Because these computerised systems contain a database of criminals and the records associated with them, investigating officers are able to access the information they need without having to go out into the field.

CHALLENGES IN THE INVESTIGATION PROCESS

During the investigation procedure, an investigating officer faces a number of obstacles. In addition to –

Jurisdictional Issues in the Cyberspace

When dealing with matters relating to cybercrime, it can be particularly challenging to articulate jurisdictional authority. While the investigation is being conducted, the agency that is conducting it is required to carry out the process of search and seizure, among other things. As a result, in order to finish the investigation process, determining jurisdiction is the most crucial thing to do, despite the fact that it is one of the most difficult things to complete in situations involving cybercrime.

Investigation and the game of Dark Web

When a cybercrime is done by using a system or a computer, the IP address, also known as the Internet Protocol address, is the most effective technique to track down the perpetrator of the crime because it identifies the device being used. However, criminals frequently make use of proxy servers, which makes it very difficult to track down the offender by means of a specific IP address. This presents a significant challenge to law enforcement.
Despite the fact that the nature of the law pertaining to cybercrime was altered by an amendment in 2008, there are still a great many issues that need to be resolved before the investigative

DOI: https://doi-ds.org/doilink/05.2023-86314248/UIJIR

© UIJIR | ISSN (O) – 2582-6417
MAY 2023 | Vol. 3 Issue 12
www.uijir.com

machinery. As a result, the fundamental premise of investigation needs to be modified, and the application of new instruments and procedures needs to be made in an efficient manner.

CONCLUSION AND SUGGESTION

In conclusion, the current investigative mechanisms in India rely on traditional methods, resulting in a relatively lower rate of conviction in comparison to other countries. Therefore, it is essential to establish a systematic process of inquiry and take into account the utilization of specialized skills and scientific instruments. The process of investigation in cybercrime involves the

acquisition of devices, data, recovery of data, forensic analysis, and presenting the investigation. The digital forensic department or agency is concerned with the conduct of investigations into crimes related to cyber concerns. Challenges in the investigation process include jurisdictional issues in cyberspace, lack of proper training and education, and a lack of coordination among different agencies. To address these challenges, it is recommended that the government invest in modern technology and specialized training programs for law enforcement personnel. Additionally, the establishment of a centralized agency for cybercrime investigation and collaboration with international agencies can help improve the conviction rate and combat cybercrime effectively.

DOI: https://doi-ds.org/doilink/05.2023-86314248/UIJIR