CYBER FORENSICS: REVOLUTIONIZING THE ADMINISTRATION OF CRIMINAL JUSTICE

Mangal Kumar Raj, Ph.D. (Research Scholar), Department of Law and Governance.
Central University of South Bihar, Gaya, India

ABSTRACT

The advancement of science and technology the modern society depend upon electronic device such as computer, mobile phone, camera, smartwatch etc, to complete their daily business of life. These advancement leads to serious related crimes. Cyber forensics, is the branch of technology that uses investigation techniques to help identify, collect, and store evidence from an electronic device. It is also known as computer forensics or digital forensics. The paper will analyse the brief overview of various stakeholders of cyber forensics that revolutionise the administration of criminal justice system with the relevant case laws in India. Hence, it is the need of the hour to protect cyber integrity against the cyber-crimes and criminals.

Keywords: Cyber Forensics, Cyber Crimes, Criminal Justice, Investigation Technique, etc**.**

Introduction

The science and technologies proliferate into everyday life, we come close to realizing new and existing online opportunities.[1] One such opportunity is in Cyber forensics, unique process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally accepted. The American Heritage Dictionary defines forensics as "relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law"[2]

Cyber forensics involves the identification, documentation, and interpretation of computer media for using them as evidence and/or to rebuild the crime scenario.[3] The process of locating, gathering, safeguarding, evaluating, and presenting computer-related evidence in a way that is accepted by the law is known as computer forensics. Digital forensics, data forensics, system forensics, network forensics, email forensics, cyber forensics, forensics analysis, enterprise forensics, proactive forensics, and other words have emerged from the more recent branching into other overlapping fields of computer forensics.

Cyber forensics is the study of how and what went wrong. System forensics is done on separate computers. In order to identify the origins of security breaches, network forensics collects and analyses network events. Another name for the same procedure used on the Web is "web forensics." The major in data forensics focuses on both volatile and non-volatile data analysis. Ongoing forensics is known as proactive forensics, and it offers the chance to proactively and consistently gather prospective evidence. One or more emails are dealt with as evidence in forensic investigations by email forensics specialists.

According to National Crime Record Bureau Cybercrime reporting surged by 24.4%, totalling 65,893 cases, a significant surge from 52,974 cases in 2021. Cyber fraud constituted the majority of cases (64.8%) of registered cases, followed by extortion (5.5%), and sexual exploitation (5.2%). The crime rate under this category rose from 3.9 in 2021 to 4.8 in 2022.[4]

Cyber Forensics

[1]Prashant Saurabh & Amrit Jay Kumar Roy, "Role of Cyber Forensics in Investigation of Cyber Crimes," International Journal of Law Management & Humanities 4 (2021): 786-798.
[2]W.G. Kruse & J.G. Heiser, Computer Forensics Incident Response Essentials (Addison Wesley Pearson Education, Boston, 2002)
[3]M. Baggily, R. Mislan, & M. Rogers, Mobile Phone Forensics Tool Testing: A Database Driven Approach, International Journal of Digital Evidence, Fall, vol. 6, no. 2 (2007)
[4] https://ncrb.gov.in/en/cyber-crimes

Evidence is gathered using forensic technologies following the information-gathering and questioning phase. The gathered evidence needs to be properly preserved without being tempered with. Methods for investigating cybercrime:

- Searching who is
- Tracking IP address
- Analysis of webserver logs
- Tracking of email account
- Trying to recover deleted evidences
- Trying to crack the password
- Trying to find out hidden data a computer forensic investigator should follow some of
- the investigation methodologies in order to find out the truth.

To discover the truth, they must adhere to certain processes. It is important to collect evidence without interfering with the evidence's chain of custody. After the evidence has been acquired, the original data should be kept secure, and the duplicate data should be worked on. The forensic investigator should protect the integrity of the data. Both the organization's and the investigator's reputations shouldn't be ruined by the inquiry procedure.

Cyber Forensics in Cyber-Crime Investigation

As cybercrime is increasing there is a robust need for cyber forensic experts in all industry models and more importantly among law enforcement agencies who rely on cyber forensics to find cyber criminals.[5] Cyber forensic investigators are the experts in investigating of the encrypted data using various types of software and tools. There are many upcoming techniques that investigators use depending on the type of cybercrime they are dealing with.[6] The tasks for cyber investigators include recovering of the deleted files, cracking passwords, finding the source of the security breach etc. Once collected, the evidence is then stored and translated to make it presentable before the court of law or for police to further examine.[7] The aim of cyber forensics is to preserve evidence in its most original form so that a structured investigation can be performed to reconstruct past events.

[5] Britz, Computer Forensics and Cyber-Crime: An Introduction, 2d ed. (Pearson Education India, 2009).
[6] K.K. Sindhu & B.B. Meshram, Digital Forensics and Cyber-Crime Datamining (2012).
[7]Heum Park, SunHo Cho, & Hyuk-Chul Kwon, Cyber Forensics Ontology for Cyber-Criminal Investigation, in Forensics in Telecommunications, Information and Multimedia, 160-165 (Springer Berlin Heidelberg, 2009).

Crime Analysis

The International Association of Crime Analysts (I.A.C.A.) offers this statement about crime analysis: Crime analysis is a scientific process in the sense that it involves the collection of valid and reliable data, employs systematic techniques of analysis, and seeks to determine, for predictive purposes, the frequency with which events occur and the extent to which they are associated with other events.

In more concrete terms, Reuland identifies four specific functions for crime analysis:[8]

1. **To support resource deployment**- Crime analysis for this purpose involves detecting patterns in crime or the potential for crime in order to enhance the effectiveness of daily patrol operations, surveillance, stakeouts, and other tactics. These analyses influence personnel deployment and resource allocation.
2. **To assist in investigating and apprehending offenders-** By comparing files that contain modus operandi characteristics with files of new suspect attributes, departments hope to make more and better arrests.
3. **To prevent crime-** Crime analysts focus on identifying locations, times of day, or situations where crimes appear to cluster so that departments can take steps to "harden" these potential targets to make them less likely targets of crime.
4. **To meet administrative needs-** Law enforcement administrators need to provide other individuals and agencies with crime-related information, including city agencies, courts, government offices, community groups, and the media. Administrators may need to use crime analysis in this context for legislative, political, and financial purposes.

Crime analysis may also serve strategic purposes for planning agencies, crime prevention units, patrol and investigative commanders, and community relations units in terms of their programmatic, planning, development, and evaluation functions.

It is clear that crime analysis is a process for which computerized data processing is tailor made. However, it is true that law enforcement agencies have been doing some form of crime analysis from time immemorial. Policing hasn't been random and it hasn't been reactive to the exclusion of all other considerations. Crime analysis has always guided decision-making. However, the crime analysis that we think of now is orders of magnitude different from what was performed

[8] M.M. Reuland, Information Management and Crime Analysis: Practitioners' Recipes for Success, Washington, D.C.: Police Executive Research Forum (1997).

prior to the advent of desktop computers. These have increased the power and speed of crime analysis tremendously. The advent of community policing has provided another recent impetus to enhanced crime analysis. For these and other reasons, the number of departments with crime analysis units has been growing over the past several years.

Right to Privacy and Cyber Forensics

Cyber forensics balanced against the right to privacy, which is also a fundamental human right.[9] There isn't even one defined law in India that addresses the development of cyber-forensics. This might be because technology law in India is still in its infancy. As there are no laws controlling cyber forensics, all one needs to do to become a cyber-forensic expert is to finish an approved course in the field after receiving their degree. There is no organization who governs the profession of cyber forensics in India.[10] Since delivering justice and resolving complex cases are the main uses of cyber forensics in India, it is imperative to establish a regulatory organisation that can verify that those working in this field are truly qualified to carry out their duties. The majority of the time, the information and proof acquired from the examination of digital media must be used in court. This is because more and more people have access to the internet, which is contributing to the rise in crimes involving digital media.[11] For example, if a girl is getting blackmailed on a messenger app, then the sole and most effective way of proving it in the court will be to give evidence,[12] which in such cases, most of the time are in digital forms.

Right to privacy is a fundamental right which is guaranteed under the Article 19 of constitution of India. There is a possibility of privacy infringement when the data in electronic forms are given to forensic science analyst. It is rational enough to consider that forensic investigators should have right to access everything which can be helpful in tracking down the accused so that victim can get justice.[13] However, the majority of the time, the investigator gathers all the private information that is not relevant to the case or helpful in solving it, in addition to the information that is needed. They put it to other uses. Therefore, there is always a chance that privacy will be violated during a cyber forensics' inquiry. This may have similarities to the

[9]Naeem Allahrakha, Balancing Cyber-Security and Privacy: Legal and Ethical Considerations in the Digital Age, Legal Issues in the Digital Age 4, no. 2 (2023): 78-121.
[10]Ramesh C. Joshi & Brij B. Gupta (eds.), Security, Privacy, and Forensics Issues in Big Data (IGI Global, 2019).
[11]Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, Journal of the Indian Law Institute (2011): 663-677.
[12]Ishaani Priyadarshini, Introduction on Cybersecurity, in Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, 1-37 (2019).
[13]Ana Nieto et al., Privacy-Aware Digital Forensics, (2019): 157-195.

contentious Aadhar Card case, in which the government employed UDIAI to gather all information from Indian individuals. Therefore, in such circumstances, it won't be difficult for any unauthorised person to get the PIN, password, username, or other necessary information thanks to the forensic scientific analyst, then it will not be difficult for them to manipulate the account and use it for illegal purposes. Therefore, it appears that forensic investigators should be in violation of their right to privacy if they obtain access to private information that is not needed for the current case. In India, there is a need for a regulatory body that will create a code of conduct and grant forensic investigator certification. This code of conduct may also include provisions for violating the privacy rights of those whose lives may be impacted by the disclosure of private information.

International organisations that regulate cyber forensics are already well-established. The forensic science department and Indian government may accept those groups' codes of conduct. It will facilitate a speedy investigation. "The International Society of Forensic Computer Examiners" (ISFCE) is one such group that the Indian forensic department ought to embrace. It is among the most well-known companies in the cyber-forensics industry. One must pass the test and receive a certificate from the organisation in order to be certified as a forensic investigator. The majority of the globe accepts their accreditation. The National Treaty of the Council of Europe's Convention on Crime likewise systematically addresses cybercrime.

It's a multinational treaty which has addressed the issue of cybercrime along with breach of the Right to Privacy.[14] Moreover, it has also tried to harmonize and balance the step to gather cyber forensic evidences in Cybercrime as well as giving strong code and regulations for protecting the rights of privacy of individuals. The signatory nations provide for the common ground of laws, principles and procedures along with aiding international cooperation in the investigation of International cyber-crimes.[15] The treaty's main aim is protection of Information technology and to provide for criminal penalties in the following scenario

- Accessing a computer without authorization or using in excess of authorization.
- Blocking data without authorization
- Interfering with the data without permission
- Interfering with a system without any authority or permission

[14] Ramendra Nath Verma, Cyber Laws and Privacy Issues in India, in Global Perspectives on Media, Politics, Immigration, Advertising, and Social Networking, 164 (2019).
[15] Neelam Rai, Right to Privacy and Data Protection in the Digital Age-Preservation, Control and Implementation of Laws in India, 11 Indian JL & Just. 115 (2020).

- Misusing devices.

Apart from the mentioned treaty, there exist additional bilateral accords that safeguard persons' rights in the context of cyber forensics. Additionally, the framework for the cyber relationships between the United States and India provides specific guidelines for cooperation, investigation, and security that are in line with a number of other national and international obligations.

Challenges of Cyber Forensics

The court benefits from the preservation of data or information for the purpose of serving as evidence, but there may be certain technical and human barriers to such gathering of the information. This is similar to how, no matter how effective any technology or system may be, there always has been a drawback to the same. Some of the limitations are as follows:[16]

- Some facilities which are there within the browsers for the purpose of saving the WWW pages to disk are not perfect because it may save the texts but not the related images.
- There might be difference between what is there on the screen which can be seen and what is saved on the disk.[17]
- The method which has been used to save a particular file might not carry individual labelling regarding when and where it was obtained.[18] Such files can be easily forged or modified.
- Most times it becomes difficult for the system to locate the page which was acquired at last. If the entire series is examined,[19] it becomes even difficult to point which one was later and which was earlier.
- Many ISPs use proxy servers in order to speed up their delivery of pages which are popular on web.[20] Hence, the user might not be sure of what he has received from that particular website by his ISP.

[16] Vihara Fernando, Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges, in 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1-7 (IEEE, 2021).
[17]Abdullah Ayub Khan et al., Digital Forensics and Cyber Forensics Investigation: Security Challenges, Limitations, Open Issues, and Future Direction, 14 Int'l J. Electronic Security & Digital Forensics, no. 2, 124-150 (2022).
[18] Abhishek Kumar Pandey et al., Current Challenges of Digital Forensics in Cyber Security, in Critical Concepts, Standards, and Techniques in Cyber Forensics, 31-46 (2020).
[19]Zubair A. Baig et al., Future Challenges for Smart Cities: Cyber-Security and Digital Forensics, 22 Digital Investigation 3-13 (2017).
[20]Kenneth Okereafor & Rania Djehaiche, A Review of Application Challenges of Digital Forensics, 21 Intl J. Simulation Systems Science & Tech. 35-1 (2020).

Case Laws

1. State of Maharashtra v. Dr. Praful B. Desai,[21] in this case, the Supreme Court observed that the evidence can be both oral and documentary and electronic records can be produced as evidence. This means that evidence, even in criminal matters, can also be by way of electronic records. This would include video-conferencing. Video-conferencing is an advancement in science and technology which permits one to see, hear and talk with someone far away, with the same facility and ease as if he is present before you i.e. in your presence. Thus, it is clear that so long as the accused and / or his pleader are present when evidence is recorded by video-conferencing, that evidence is recorded in the "presence" of the accused and would thus fully meet the requirements of Section 273 Criminal Procedure Code. Recording of such evidence would be as per "procedure established by law". The advancement of science and technology is such that now it is possible to set up video- conferencing equipment in the court itself. In that case evidence would be recorded by the Magistrate or under his direction in the open court"
2. Anvar P.V. v. P.K. Basheer & Others (2014)[22] The Supreme Court of India, in this case, addressed the admissibility of electronic evidence under Section 65B of the Indian Evidence Act. It laid down guidelines for the proper certification and production of electronic evidence in court.
3. Rajesh Rajput v. State of Chhattisgarh (2017), This case involved the authentication of electronic evidence. The Chhattisgarh High Court emphasized the need for proper certification and authentication of electronic records for their admissibility.
4. Shafhi Mohammad v. State of Himachal Pradesh (2018), The Supreme Court clarified the admissibility of electronic evidence, stating that the procedural requirements under Section 65B of the Indian Evidence Act are procedural safeguards rather than technical requirements.
5. Karnataka High Court Guidelines on Electronic Evidence (2017): While not a case law, the Karnataka High Court issued comprehensive guidelines on the collection, preservation, and presentation of electronic evidence. These guidelines serve as a reference for legal practitioners and investigators involved in cyber forensics cases.

[21] State of Maharashtra v. Prafulla B. Desai (Dr.) (2003) 4 SCC 601.
[22] Sandra Jini Saju & Anvar P.V v. P.K. Basheer & Ors, (2014) 10 SCC 473, Section 65A and 65B- Admissibility of Electronic Records, Indian Journal of Legal Review (IJLR) 3(1) (2023), 579-782, ISSN – 2583-2344.

Conclusion and Suggestion

In order to bring charges against computer-based crimes on a war footing, it is necessary to safeguard processes related to manpower. In order to serve as a deterrent to crime for others, it is imperative that the system ensures that computer crime and its perpetrators face severe penalties. The majority of offences under the Information Technology Act are now punishable by up to three years in jail and are subject to bail. This sentence should be extended to a term that would alter the mindset of a cybercriminal and deter them from performing nearly identical acts in the future. It is necessary to set up a separate bench in order to efficiently track and record computer cases. The police department can demonstrate its skill in cybercrime cases thanks to the establishment of cyber judges.

Suggestion

The following are suggestions recommended:

- Internet security to be tightened
- Encryption technology to be used
- Intrusion detection systems to be used
- Cyber forensic lab should be get established in all the police stations
- Establishment of cyber courts for handling cyber-crime cases.
- Educating the public on cyber-crimes cases
- Motivating cyber-crime victims for registering complaint against the criminals.