The Function of Digital Evidence and Forensic Computers in Cybercrimes Investigation: A Case Study of India

AKHILESH KUMAR PANDEY[1], AMIT SHARMA[2]
[1, 2] *Assistant Professor, School of Law, Monad University, Hapur*

Abstract— In the current era of information security, cyberattacks become more and more significant, which makes the use of computer forensics for data gathering, analysis, and documentation necessary. Digital forensics investigators can preserve and analyze digital evidence using a range of commercial and open-source technologies at their disposal. But it's still difficult to identify and prove digital crimes in court. To help comprehend attacker intent, a skilled forensic analyst gathers and analyzes relevant data. This study emphasizes the significance to efficient digital resources and techniques for searching, identifying, and maintaining electronic evidence. It concentrates on the investigation process for storage media and developing cybercrimes. The utilization of digital forensic methods and instruments in investigations involving digital forensics is also covered. Cybercrime cases in India indicate that the country doesn't have enough technical professionals to handle the cases. There are remarkably few police officers with technical training. The judicial department is similarly missing something. The second significant concern is the jurisdiction of the judiciary to handle cybercrime crimes. Police and judicial personnel must get frequent training. The Information Technology Act should be changed, and offenders should face harsh penalties. Several of the IT Act's clauses that solely stipulate minimum penalties need to be amended.

Index Terms- Cyber Crime, Forensic Computers, Digital Evidence, IT Act 2008

I. INTRODUCTION

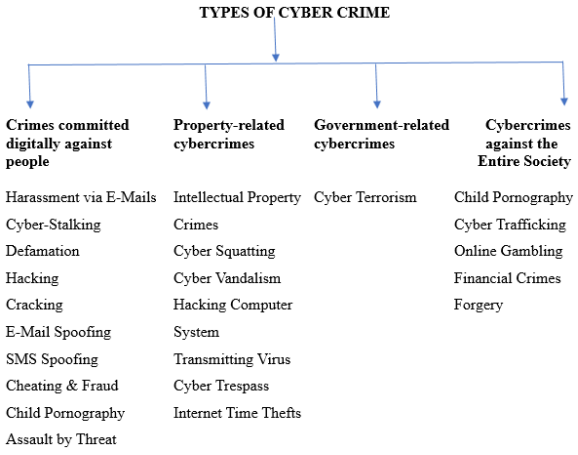
In today's interconnected digital landscape, cyberattacks pose a significant threat to networks, computers, software, businesses, industries, and the Internet. The ease with which digital data can be manipulated, duplicated, restored, or destroyed necessitates the reliance on computer forensics and legal services to uncover, analyze, and present digital evidence. However, the fragility of digital evidence demands meticulous attention from investigators to ensure its integrity remains intact throughout the investigative process. This article delves into the application of digital technologies and methodologies in forensic investigations, particularly focusing on the crucial role they play in criminal investigations. It covers the introduction, protocols, types of cybercrimes, and methodologies for investigating them, including examination of storage media. The study seeks to streamline and expedite investigations by emphasizing the core storage system investigation process, thereby facilitating the prompt identification and resolution of cybercrimes.

II. CYBER CRIME

The proliferation of cybercrime represents a significant challenge in the contemporary digital realm, as technology is increasingly exploited both as a tool and a target for illicit activities. The ubiquity of the World Wide Web has amplified the prevalence of cybercrimes globally, exerting adverse effects on the social and economic development of emerging nations. While advancements in computer technology have enhanced quality of life and efficiency in many societies, malevolent actors have capitalized on these innovations for nefarious purposes. In response to this burgeoning threat, countries like India have enacted legislation such as the Information Technology Act of 2000, subsequently revised in 2008 to bolster its efficacy and stringency.

Cybercrimes encompass a range of illicit activities wherein contemporary telecommunication networks, including the Internet and mobile phones, are leveraged to harm individuals' reputation, infringe upon their privacy, or cause physical and psychological harm. These crimes, spanning from child pornography to hacking and copyright infringements, pose significant challenges to national

security and financial stability. Moreover, cyberwarfare, involving actions transcending national borders and implicating multiple countries, further complicates the landscape of digital forensics. Traditionally associated with criminal investigations, digital forensics focuses on computer-based or computer-facilitated crimes, necessitating specialized expertise and methodologies to combat this evolving threat landscape. Types of cybercrime is given below:



Cyberstalking, involving harassment and defamation through digital communication and computer networks, represents a serious threat to individuals' safety and privacy. Intellectual property crimes encompass theft of literary and creative works, including copyright infringement, patent violations, and trade secret theft. Botnets, combinations of networks and robots, are utilized to orchestrate Distributed Denial-of-Service (DDoS) attacks, disrupting online services. Hackers exploit vulnerabilities to gain unauthorized access to computer networks and disseminate viruses, malicious attachments capable of replicating data. Internet time theft involves hackers accessing accounts without authorization to exploit services and passwords.

Cracking refers to unauthorized access to computers for data theft or viewing private information. Phishing and vishing schemes entail stealing credit card information via deceptive emails or phone calls, respectively. Carding, or credit card trafficking, involves using stolen credit cards for illicit purposes. Email spoofing deceives recipients by falsifying sender addresses, while cross-site scripting enables attackers to run malicious scripts on websites or browsers. Child sexually abusive material (CSAM) depicts children being exploited in sexually explicit contexts, while sexting involves exchanging explicit content via cell phones. Cyber grooming entails establishing online friendships to coerce individuals into sexual acts.

Cyber trespassing involves unauthorized access to computer infrastructures for data gathering, while cyber vandalism entails damaging computer systems. Electronic devices like laptops and cell phones can be used for harassment or bullying. Malicious crypto mining involves illicit coin mining activities. Cyber trafficking encompasses recruiting victims online and facilitating victim exploitation. Identity theft involves assuming false identities for information theft. Furthermore, uploading objectionable content, altering website layouts, and defaming others are unlawful activities. Unauthorized data access or modification is a crucial step in internet drug sales, violating laws and jeopardizing online security.

III. FORENSIC COMPUTERS

Computer forensics, also known as the methodical search for digital media for evidence, facilitates the reconstruction of a user's actions in various contexts. This process, often termed computer forensic analysis, ensures the preservation and presentation of computer-related data. It finds utility in criminal cases, legal disputes, and human resources/employment actions, providing crucial insights into digital activities and facilitating informed decision-making processes. Through meticulous examination and analysis of digital evidence, computer forensics enables investigators to uncover relevant information, establish timelines of events, and reconstruct digital interactions with a high degree of accuracy and reliability. This forensic discipline plays a vital role in upholding the integrity of digital evidence and promoting justice across diverse domains.

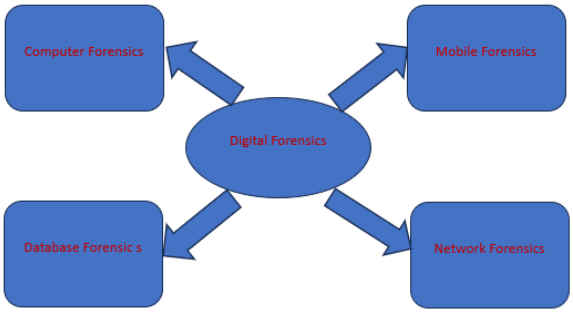


Fig 1. Diagram of many types of forensics research from digital forensics

Cyber Forensics and Digital Forensics are indeed closely related fields, both focusing on the examination of digital data-storage devices to uncover evidence relevant to criminal activities. As illustrated in Figure 1, digital forensics falls under the umbrella of forensic sciences, presenting unique challenges in obtaining direct evidence of criminal activity.

For instance, nominal suspects may be implicated through confirmation in document authentication processes. While various forms of forensics are employed for analysis, digital forensics primarily investigates processes. Unlike traditional specialized forensics, which may suffice in providing answers to isolated issues based on basic research, the distinguishing feature of digital forensics lies in its requirement to demonstrate the entire causal chain as true or false before proceeding to court.

In the realm of crimes involving computers and the Internet, computer forensics emerges as a critical subfield of forensic science. While computers were initially limited to data production, they now encompass all digital data-related equipment. The mission of computer forensics is to conduct crime investigations by leveraging digital data evidence to ascertain the root cause of a particular crime, employing a variety of techniques. This encompasses tools for mobile device examination, MAC-OS investigation, and forensic analysis of digital data. The table of contents includes a compendium of general forensic and data analysis techniques applicable across all branches of forensic research.

MAC-OS: One operating system that can be used as an analysis repository is MAC. This information is susceptible to fraudulent activity.

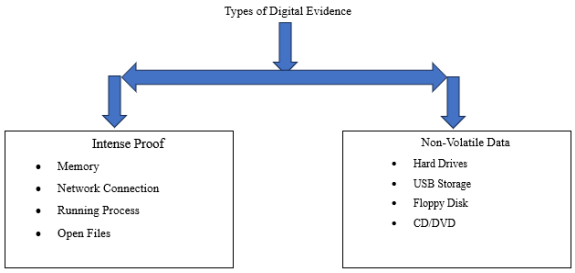
Mobile devices: These include PDAs, GPS services, tablet PCs, and any other device that can communicate, store digital data, and have internal memory. Numerous forms of personal data, including contacts, images, calendars, notes, SMS, and MMS messages, are stored on each mobile device. Smartphones may also have contacts and messages from social networks, video, email, site browsing data, and GPS data.

Digital Evidence: -
Under the Indian Evidence Act, any document, including electronic records, produced for scrutiny in court is considered evidence. Digital evidence refers to probative data that has been digitally saved or communicated and may be presented by a party in a lawsuit. Judges must determine the reliability, relevance, and authenticity of digital material before admitting it as evidence. According to the Information Technology Act of 2000, electronic records encompass data generated, recorded, saved, transferred, or microfilmed.

The prosecution of cybercrimes relies heavily on the collection and analysis of digital evidence by qualified law enforcement personnel. While digital evidence may not always directly identify the perpetrator, it can provide crucial information such as geolocation, timing of the crime, and targeted victims. Identifying the offender can be a complex task, and victims may be asked by the police to gather evidence, although they may not always know how to proceed. Additionally, challenges related to jurisdictional concerns may arise, hindering the apprehension of accused individuals due to device location issues.

To address digital crimes effectively, the Information Technology Act of 2000 has amended relevant legislation, including the Indian Evidence Act, which was drafted over a century ago. Section 65B of the Indian Evidence Act, 1872 was emphasized by the Calcutta High Court in the case of Amitabh Bagchi v. Ena Bagchi[1]. The court ruled that evidence presentation may not always require a witness to be physically present; instead, testimony can be provided

through alternative means such as video conferencing. Video conferences are considered "electronic records" as per the Act. Sections 65A and 65B outline requirements for electronic records evidence and their admissibility. These legal provisions are essential fori. ensuring justice in cases involving cybercrimes and reflect the evolving nature of digital evidence in the legal landscape. Types of digital evidence is given below:



The key characteristics of digital evidence are essential considerations in the admissibility and reliability of such evidence in legal proceedings. These characteristics include:

Admissibility: Digital evidence must conform to both legislation and common law regulations. It should be relevant to the proposition being demonstrated, and courts may deem evidence collected without proper authority as inadmissible. Obtaining warrants for the search and examination of digital devices is often required, which can complicate investigations, especially if evidence of one crime is discovered while investigating another.

Reliability: Digital evidence should originate from a credible and uncontested source to ensure its reliability.

Completeness: The evidence should provide a comprehensive overview of the offender's activities, aiding in drawing conclusions about the case.

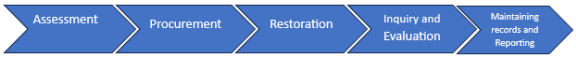
Persuasiveness to Judges: Digital evidence should be presented in a manner that is persuasive and understandable to judges, facilitating informed decision-making.

Authenticity: The evidence must be authentic and directly linked to the event or incident under investigation. Courts often assess the reliability of digital evidence, requiring investigators to demonstrate its legitimacy by elaborating on various factors such as:

i. The reliability of the computer equipment used.
ii. The process of initial data entry.
iii. Measures taken to ensure the accuracy of entered data.
iv. Data storage methods and security measures implemented to prevent data loss.
v. Verification of program correctness and the reliability of computer programs involved in data processing.

Ensuring these key characteristics are met enhances the credibility and effectiveness of digital evidence in legal proceedings, providing valuable insights into the case at hand.

The phases of the investigation process for digital evidence are given below chart: -



Computer forensics professionals encounter various challenges, categorized into three main types: technological, legal, and administrative.

Technical Issues:
Encryption: Encryption techniques can hinder access to crucial digital evidence, requiring forensic experts to employ advanced decryption methods to uncover relevant information.

Expanding storage: The ever-increasing volume of digital data poses challenges in terms of storage capacity and management during forensic investigations.

New technologies: Rapid advancements in technology introduce new devices, operating systems, and applications, necessitating continuous education and adaptation by forensic professionals to effectively analyze and extract digital evidence.

Anti-forensics: Perpetrators may employ anti-forensic techniques to conceal or manipulate digital evidence,

making it more challenging for investigators to retrieve accurate information.

Legal Issues:
Trojan Defence: Legal challenges may arise, such as the "Trojan Defence," where defense attorneys argue that actions were automated by a Trojan without the user's knowledge, even if no malicious code is found on the suspect's computer. This can create doubt regarding the integrity and reliability of digital evidence.

Administrative Issues:

- Legislative ties: Computer forensics professionals may face challenges due to legislative constraints that limit their investigative capabilities or impose procedural hurdles.
- Standards adoption: Limited adoption of standardized procedures and protocols in computer forensics can lead to inconsistencies in practices and methodologies across different jurisdictions or organizations.
- Author unpopularity: The lack of recognition or popularity of certain forensic tools or methodologies may hinder their acceptance and utilization by forensic professionals.
- Expensive professional fees: High fees associated with professional certification or membership in forensic organizations may act as a barrier to entry for aspiring forensic professionals, limiting the pool of qualified practitioners.

Addressing these challenges requires ongoing training, collaboration with legal experts, advocacy for standardized practices, and adaptation to emerging technologies and techniques in the field of computer forensics.

IT Act 2008: -
It seems like you've provided a detailed comparison between various sections of the Information Technology Act (IT Act) and the Indian Penal Code (IPC) pertaining to cybercrimes and related offenses. Here's a breakdown of the comparison you've presented:

Definition of "Writing" or "Typewritten or Printed Form": Section 4 of the Information Technology Act expands the definition of writing to include electronic form, making electronic records legally admissible. This provision facilitates the transition from traditional paper-based documentation to electronic formats.

Penalties for Cybercrimes: The IT Act and IPC penalize similar cybercrimes, such as hacking, data theft, virus introduction, computer damage, and illegal access to computer systems. While the penalties may vary slightly between the two sets of laws, both aim to address these offenses in the digital realm.

Data Theft: Section 378 of the IPC covers physical property theft, but the interpretation of "corporeal" might exclude digital properties. However, the intent of the drafters could be to encompass properties of all kinds, including digital assets.

Penalties for Various Offenses: Sections of the IPC such as 424, 411, 419, 463, 465, and 468 cover offenses related to dishonesty, fraud, cheating by personation, identity theft, and forgery. The penalties may include imprisonment, fines, or both, with variations in the maximum duration of imprisonment and fines.

Penalties for Publishing or Distributing Pornographic Content: Sections 67, 67A, and 67B of the IT Act deal with the publication or distribution of pornographic content through electronic means. These offenses are comparable to section 292 of the IPC, which addresses the sale, distribution, or possession of pornographic material in physical form.

Overall, while there may be differences in the penalties and specific provisions between the IT Act and the IPC, both legal frameworks aim to address cybercrimes and related offenses effectively in the digital age.

Section 67C of the Information Technology Act mandates intermediaries to preserve and retain specific information as prescribed by the Central Government. Non-compliance can result in imprisonment for up to three years and a fine. Intermediaries include telecom, internet, webhosting, search engines, online payment sites, auction sites, marketplaces, and cyber cafes. However, the IT Act

does not have an equivalent provision in the Indian Penal Code, highlighting the specialized nature of regulations governing intermediaries' role in the digital ecosystem.

A clear comparison between the treatment of cyber-crimes under the Information Technology (IT) Act and the Indian Penal Code (IPC) in terms of compounding, billability, and other legal procedures. Here's a breakdown of the key points you've highlighted:

Compounding and Billability:
Under the IT Act, offenses punishable by imprisonment of three years or less are compoundable, except for certain exceptions. Such offenses are generally non-bailable.

Offenses under the IPC related to cyber-crimes are generally bailable, except for specific non-bailable offenses like publishing or transmitting obscene material and cyber terrorism.

Types of Offenses:
The IT Act includes provisions for offenses such as publishing or transmitting obscene material, containing sexually explicit acts, depicting children in sexually explicit acts, and cyber terrorism, which are non-bailable.

The IPC covers cyber-crimes such as forgery, mischief, and criminal breach of trust, with varying degrees of billability and compound ability.

Compounding and Court Permission:
Compoundable offenses under both the IT Act and the IPC require court permission for compounding, indicating a legal procedure for resolving such offenses outside of court.

Intermediaries' Responsibilities:
The IT Act imposes specific responsibilities on intermediaries regarding data preservation, which is absent in the IPC. This underscores the specialized nature of regulations governing intermediaries in the digital domain under the IT Act.

The legal procedures and distinctions between cyber-crime offenses under the IT Act and the IPC, providing clarity on the treatment of such offenses within the Indian legal framework. the potential discrepancies and conflicts that can arise between the Indian Penal Code (IPC) and the Information Technology (IT) Act regarding the bailability and compound ability of certain offenses. Here's a breakdown of the key points:

Anomalies Between IPC and IT Act:
Certain offenses, such as hacking, data theft, theft, identity theft, cheating by personation, and obscenity, may have different bailability and compound ability provisions under the IPC compared to the IT Act.

This discrepancy can lead to situations where offenses classified under similar categories are treated differently in terms of bail and compounding based on whether they fall under the IPC or the IT Act.

Legal Conflicts and Judicial Intervention:
The Bombay High Court addressed one such conflict in the case of Gagan Harsh Sharma v. The State of Maharashtra[2]. The case likely involved a situation where non-bailable IPC sections conflicted with bailable and compoundable sections of the IT Act, leading to legal ambiguity and the need for judicial intervention to resolve the issue.

The legal difficulties and possible conflicts resulting from the differential handling of offenses under the IT Act and the IPC are adequately captured. It also emphasizes the judiciary's responsibility to resolve these disparities to provide uniformity and clarity in the enforcement of laws pertaining to offenses other than cybercrimes.

B.N. Firos vs. State of Kerala and others[3] The case of B.N. Firos, proprietor of Comtech IT Solutions, involves a challenge to a Notification that designates computers, systems, and networks as "protected systems" under Section 70(1) of the Information Technology Act, 2000 (IT Act). The petitioner filed a Writ Petition contesting this Notification. However, the Writ Petition was dismissed, and the dismissal was upheld in a writ appeal by a Division Bench of the High Court.

The court's decision was based on an analysis of the relevant legal provisions, particularly the amendment to Section 70(1) of the IT Act introduced by Act No. 10 of 2009. This amendment tightened the criteria for

declaring a system as a "protected system," restricting it to computer resources that directly or indirectly impact Critical Information Infrastructure facilities. The court noted that this amendment narrowed down the scope of "government work" related to Critical Information Infrastructure facilities.

In essence, the court affirmed the validity of the Notification designating computers, systems, and networks as protected systems under Section 70(1) of the IT Act, considering the stricter criteria introduced by the 2009 amendment. This decision underscores the importance of safeguarding Critical Information Infrastructure and reflects the evolving legal framework governing cybersecurity in India.

Future Directions

Digital forensics has seen significant advancements in recent years, including the use of Artificial Intelligence and Machine Learning for efficient data analysis, blockchain analysis for illegal activities, cloud forensics for data storage on cloud platforms, memory forensics for extracting evidence from RAM, IoT forensics for extracting evidence from interconnected devices, and live forensics for real-time analysis of a running system. These technologies have enabled efficient tasks like image recognition, text analysis, and anomaly detection, reducing investigation time and resources. Blockchain analysis has also emerged, allowing for the analysis of transactions on blockchain networks, aiding law enforcement agencies in investigations. Cloud forensics has been developed to address challenges such as data privacy, jurisdictional issues, and multi-tenant architectures. Memory forensics has been able to recover valuable information from memory dumps, while IoT forensics has been able to analyze interconnected devices like smart home appliances and industrial sensors. Live forensics has also enabled real-time analysis of systems, allowing for remote investigations and monitoring of system activity. The discovery and conviction of cybercriminals and other perpetrators of digital crimes are made possible by investigators' increased ability to stay up to date with new threats and efficiently acquire evidence from a variety of digital sources.

To give cybercrime investigators, the skills and information they need to properly investigate and combat digital crimes, training and education are crucial. An outline of the common educational and training programs for cybercrime detectives is provided below:

Professional Schooling:

Bachelor’s degree: A bachelor's degree in computer science, cybersecurity, digital forensics, or a similar discipline is often the first step for aspiring cybercrime investigators. A strong foundation in computer systems, networks, programming, and cybersecurity principles is provided by these programs.

Master's Degree: To further their expertise in cyber investigations, information assurance, digital forensics, or cybersecurity, some investigators seek master's degrees in these fields. Advanced knowledge and abilities in fields like cyber law, incident response, and forensic analysis can be obtained with a master's degree.

Certificates: In addition to a formal education, the profession of cybercrime investigation highly values certificates like the Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Certified Cyber Forensics Professional (CCFP). These credentials show proficiency in particular digital forensics and cybersecurity domains.

Cybercrime investigators often come from law enforcement backgrounds and receive specialized training in cyber investigations, including digital evidence collection, forensic analysis techniques, and cybercrime laws. These training programs are often partnered with organizations like the FBI, Secret Service, and NW3C. Digital forensics training is crucial for investigators to understand how to collect, preserve, and analyze digital evidence in accordance with legal standards. Training programs from organizations like IACIS, SANS Institute, and universities provide hands-on training in digital forensics tools and techniques. Continuing education opportunities, such as workshops, conferences, webinars, and online courses, help investigators stay updated on the latest trends and techniques in cybersecurity and digital forensics. Specialized training programs, offered by government agencies, private companies, academic institutions, or industry

associations, offer in-depth training on advanced topics relevant to investigators' areas of specialization. Law enforcement agencies and technology companies are working together to combat cybercrime and ensure the safety and security of digital environments. They often share information about emerging cyber threats, vulnerabilities, and attack techniques, enabling proactive measures to mitigate risks and protect users. They also collaborate on joint investigations into cybercrimes like data breaches, online fraud, and hacking attacks, providing expertise, resources, and technical assistance to law enforcement. Technology companies often partner with law enforcement to provide cybersecurity training and workshops, helping officers develop the skills needed to investigate and respond to cybercrimes effectively. They also work on developing tools and technologies to detect, prevent, and mitigate cyber threats. They also collaborate on policy development and advocacy initiatives to address cybercrime challenges at national and international levels. Technology companies may also voluntarily cooperate with law enforcement by providing access to user data, logs, and other relevant information for criminal investigations. The collaborative effort of technology businesses and law enforcement agencies is crucial in the fight against cybercrime, improving cybersecurity, and protecting digital ecosystems. Together, they can successfully handle the intricate and ever-evolving issues posed by cyber threats by utilizing their own knowledge, resources, and skills.

Postscript: -

The fight against cybercrime relies heavily on the partnership between law enforcement and technology companies. This collaboration entails the sharing of information regarding emerging threats, conducting joint investigations, and providing cybersecurity training. Technology companies offer their expertise, resources, and technical support to identify and gather evidence against cyber criminals. Likewise, law enforcement agencies join forces in cybercrime investigations, equipping their officers with the necessary skills. Together, they develop tools and technologies to detect, prevent, and mitigate cyber threats. Their combined efforts also contribute to the development of policies and advocacy initiatives, advocating for legislative reforms and cybersecurity standards. Furthermore, technology companies may assist law enforcement agencies by granting access to user data and aiding in criminal investigations. Ultimately, the collaboration between law enforcement and technology companies is essential in the battle against cybercrime, as it enhances cybersecurity capabilities and safeguards digital ecosystems. To effectively address cyber threats and protect digital ecosystems, law enforcement and technology businesses collaborate to advance the field of cybercrime investigation by providing access to resources, knowledge, and technologies. Through this collaboration, law enforcement agencies and technology companies can enhance their capabilities, achieve better investigative outcomes, and ultimately reduce the detrimental impact of cybercrime on individuals, businesses, and society.

REFERENCES

[1] Barkha, Mohan UR. Cyber law and crimes. IT Act 2000 and Computer Crime Analysis. 3rd ed. 2011. p. 1-8

[2] Information Technology Act 2000. 2017. Available from: http://www.dot.gov.in/act-rules/information-technologyact-2000

[3] Available from: https://en.wikipedia.org/wiki/Article_ (grammar). 2008.

[4] Cyber crimes and the law. 2011. Available from: http:// www.legalindia.com/cyber-crimes-and-the-law

[5] Cybercrime.Retri eved from https:/en. wikipedia.org/wiki/(10 June 2016)

[6] Hassan, Nihad A. "Introduction: Understanding digital forensics." Digital Forensics Basics. Apress, Berkeley, CA, 2019. 1-33

[7] Meghanathan, Natarajan, Sumanth Reddy Allam, and Loretta A. Moore. "Tools and techniques for network forensics." arXiv preprint arXiv:1004.0570 (2010)

[8] https://www.educba.com/what-is-digital-forensics

[9] Brown, Chrostopher L.T. Computer Evidence Collection &Presentation, Firewall Media.