Page 1244 - 1257 **DOI:** *https://doij.org/10.10000/IJLMH.114505*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 2

2023

Cyber Forensics in India

K. SNIGDHA[1]

ABSTRACT

As the world becomes more digitally connected, computer forensics becomes more important every day. For the purpose of identifying cybercriminals and recovering crucial, stolen data, digital evidence management is essential. Computer forensics aids in the identification, gathering, and archiving of evidence from an electronic device by utilizing technology and investigation procedures to make the information usable in the court of law as evidence. Computer forensics conducts a structured investigation and upholds a chain of evidence to pinpoint precisely what happened on computing equipment and who was responsible for it. There is no single codified statute or law in India that addresses computer forensics. The reason might be that technology law in India is still in its infancy. In order to combat cybercrime using the most up-to-date forensic technology, it is necessary to alter current regulations and create a new techno-legal framework. The present paper explores types of cyber forensics and the investigation procedure for obtaining such information. Further, the paper also ponders on the question of whether cyber forensics breaches an individual's right to privacy and if there is any way to keep the person's private information safe.

Keywords: *Cyber forensics, right to privacy, admissibility of cyber forensics.*

I. INTRODUCTION

Digital or cyber forensics are alternate terms for computer forensics. It belongs to the field of digital forensic science. Computer forensics aids in the identification, gathering, and archiving of evidence from an electronic device by utilizing technology and investigation procedures to make the information usable in the court of law as evidence. Computer forensics conducts a structured investigation and upholds a chain of evidence to pinpoint precisely what happened on a computing equipment and who was responsible for it. For digital forensics, the data must first be obtained in a method that protects its integrity. The information or system is then examined by investigators to determine whether it was altered, if so, how, and by whom. Applications of computer forensics are frequently unrelated to criminal activities. The forensic method is also used as part of data recovery procedures to gather data from a crashed server, failed drive, reformatted operating system (OS), or any other situation where a machine has

[1] Author is a student at Symbiosis Law School, India.

 [ISSN 2581-5369]

abruptly stopped to function.

As the world becomes more digitally connected, computer forensics becomes more important every day. For the purpose of identifying cybercriminals and recovering crucial, stolen data, digital evidence management is essential. It is the responsibility of a computer forensics investigator to gather, review, and preserve this evidence. The integrity of digital evidence used in court cases in both the civil and criminal justice systems is helped by computer forensics. As computers and other data-gathering tools are used increasingly often in every aspect of life, the relevance of digital evidence, as well as the forensic processes used to collect, preserve, and investigate it, has expanded in terms of aiding in the resolution of crimes and other legal concerns. Most of the data that modern devices collect are never visible to the average person. For instance, automobile computers secretly collect information on a driver's gear selection, braking, and speed changes. Due to the potential importance of this information in resolving a legal issue or a crime, computer forensics frequently assists in discovering and securing it

In the 1840s, Hans Gross (1847-1915), who applied scientific research in criminal inquiry, laid the foundation for modern digital forensics. In order to offer forensic services to all local authorities, the Federal Bureau of Investigation (FBI) in the USA created a forensic laboratory later in 1942. After the first computer crime ever occurred in 1978, the Florida Computer Crime Act went into effect. The phrase "computer forensics" was first used in literature in 1992. The International Organization on Computer Evidence (IOCE) was founded as a result of this in 1995. With the establishment of the first regional computer forensic laboratory by the FBI in 2000, computer forensics rose to prominence[2].

Cyber forensics is employed to find concrete proof of a computer-assisted crime or to assist in the investigation of cybercrime. Everyone with a stake in the legal system, law enforcement, corporate leaders, educators, and the government is interested in Cyber Forensics. Both the practice of criminal law and private law frequently use cyber forensics, though it has typically been connected to criminal law. Many professions, including the military, commercial enterprise, academia, and law, can benefit from understanding cyber forensics. For something to withstand cross-examination in court, it needs to meet strict standards. Cyber Forensics is turning into a source of research since courts do not accept software tools like Encase, Pasco, and Ethereal as expert witnesses, making human expert witnesses crucial.

There is no single codified statute or law in India that addresses computer forensics. The reason

[2] Sharon Kerketta, *A STUDY ON THE CHALLENGES OF DIGITAL FORENSIC INVESTIGATION IN INDIA: A LEGAL PERSPECIVE*, 1 DE JURE NEXUS 2, 2-3 (2021).

 [ISSN 2581-5369]

might be that technology law in India is still in its infancy. Not a single body oversees the field of digital forensics. Delivering justice and resolving complex situations including digital complications are the main uses of digital forensics in India. In order to combat cybercrime using the most up-to-date forensic technology, it is necessary to alter current regulations and create a new techno-legal framework. In India, crimes like email spoofing and Facebook account hacking are fairly widespread, but because the laws are lax and the police are ineffective, the offenders are free to conduct additional crimes. While cybercrimes have steadily increased in India, there is an extremely low conviction rate for these offenses. Several nations including the USA, UAE, Pakistan, Nigeria, Saudi Arabia, etc. conduct cyberattacks against India. In India, crimes like identity theft, phishing, credit/debit card fraud, and email fraud are all fairly common. Hence, strong cyber law enforcement and strict cyber security are required in this country[3].

(A) Research Objectives:

The following objectives are to be fulfilled through the research:

1. To understand cyber forensics as a concept and its standing in India
2. To understand the admissibility of cyber forensics as evidence
3. To revisit some important cases where cyber forensics played a major role
4. To explore the legal and ethical issues surrounding the use of digital evidence in criminal trials, such as issues related to privacy and data protection.

(B) Research Questions:

The above mentioned objectives are to be fulfilled by answering the following questions:

1. What is cyber forensics? What is the standing of cyber forensics in India?
2. How can cyber forensics be used as evidence?
3. What moral and legal concerns surround the gathering, examination, and presentation of digital evidence in court?
4. How successful are the present cyber forensic methods and technologies for finding and recovering digital evidence?

(C) Research Methodology:

The research is conducted using doctrinal methods and the results have been presented in a

[3]Shruti Verma and Saurabh Mehta, *A Study to Examine Cyber Forensic: Trends and Patterns in India*, Int J Technol Manag. 21, 22-24 (2019).

 [ISSN 2581-5369]

descriptive manner. The materials for the study are secondary in nature and have been collected from trustable sources of JSTOR, Manupatra, and others. The author also employed an applied style of legal research in the conclusion of this article. In the preponderance of its project, the author will also use the analytical mode of legal research. The paper will discuss types of cyber forensics, the investigation procedure and its admissibility in Indian courts and if cyber forensics breach individual's right to privacy.

(D) Literature Review:

1. "Cyber Forensic: A New Approach to Combat Cyber Crime[4]"

The paper starts with explaining what cyber forensics is and further describing the admissibility of cyber forensics in Indian courts. The paper also explains tools used in cyber forensics and the investigations process in brief, later shifting to challenges faced by cyber forensics in India and how they can be tackled.

2. "Cyber Forensic Tools: A Review[5]"

This paper starts with a history and evolution of cyber forensics and cybercrime in India and as the name of the paper suggests, it moves on to explain different tools used in cyber forensics in great detail.

3. "A STUDY ON THE CHALLENGES OF DIGITAL FORENSIC INVESTIGATION IN INDIA: A LEGAL PERSPECIVE[6]"

The present research focuses on investigation procedures and challenges faced by cyber forensics in India in great detail and suggests some recommendations to tackle the said challenges.

4. "A Study to Examine Cyber Forensic: Trends and Patterns in India[7]"

The study focuses on cybercrime trends in India and how "well" the forensics department was able to solve the crimes. It them moves on to elaborate on the stand of cyber forensics with respect to the legislative and judiciary system.

[4]Shubham Maheshwari & Navnidhi Sharma, *Cyber Forensic: A New Approach to Combat Cyber Crime*, 15 ACCLAIMS (2021).
[5]B. V Prasanthi, *Cyber Forensic Tools: A Review*, 41 IJETT (2016).
[6]Sharon Kerketta, *A Study on the Challenges of Digital Forensic Investigation in India: A Legal Perspecive*, 1 DE JURE NEXUS LAW JOURNAL 2-9 (2021).
[7]Shruti Verma & Saurabh Mehta, *A Study to Examine Cyber Forensic: Trends and Patterns in India*, 6 Int J Technol Manag 21-25 (2015).

 [ISSN 2581-5369]

5. "Role of Cyber Forensics in Investigation of Cyber Crimes[8]

The paper discuses the legislations regarding cyber forensics and cyber security in India and if cyber forensics breaches the right to privacy of an individual and goes on the suggest some procedures to make the cyber forensics department more ethical and safer.

II. CYBER FORENSICS IN INDIA

The legal and judicial systems in India should be taken into consideration because they appear to be working in an outdated manner. With the rise of cybercrimes, it is necessary to alter current policies and create a new techno-legal framework to combat cybercrime with the aid of cutting-edge forensic technologies. Identity theft, phishing, email fraud, credit card fraud, debit card fraud, and other crimes are all quite prevalent in India. There has been a sharp increase in cybercrime, and the trends in this area are not good. Only 13301 cyber crimes were reported in 2011, compared to 62189 reported in 2014 through May, which may have reached the approximate number of 149254. The use of cyber forensics in the investigation process and the demand for forensics labs will undoubtedly expand as cyber crime increases. The best possible evidence will be extracted from digital data through forensics, and this will produce accurate results, enabling the court to make the best possible decisions[9].

Parliament on cyber forensics:

Cyber forensics is still a young field in India and is being given less attention by our government. Cyber forensics currently lacks established standards and regulations, which makes it challenging to gather evidence. The techno-legal concerns that cyber security, cyber forensics, and cyber law face are not ones that the parliament is particularly interested in addressing at the moment.

Judicial system on cyber forensics:

Due to the lack of structure in cyber law, the judicial system has difficulty reaching decisions. It is challenging for the judicial system to make a conclusion because the Indian cyber legislation has several flaws due to lack of attention.

Police on cyber forensics:

Since there are no established standard practises for gathering evidence and conducting forensic analysis, problems and crises that the police must deal with are exacerbated by infrastructure

[8]Prashant Saurabh & Amrit Jay Kumar Roy, *Role of Cyber Forensics in Investigation of Cyber Crimes*, 4 IJLMH 786 - 798 (2021).
[9]Shruti Verma and Saurabh Mehta, *A Study to Examine Cyber Forensic: Trends and Patterns in India*, Int J Technol Manag. 21, 22-24 (2019).

 [ISSN 2581-5369]

limitations. Inadequate infrastructure for research and development is a problem in India. There were only 25 forensic labs to investigate the offences out of 5693 cyber crime reports that were lodged in 2013.

India must establish fully functional cyber forensics labs in all major police headquarters. It takes time and effort to build up the cyber forensic laboratory step by step; it cannot be done all at once. In India, there is a definite need for cyber forensic training institutions. Making policies and educating the general public as well as the police, attorneys, and judges are necessary. In order to prevent cybercrimes, India must focus on creating the legal framework and organized processes to resolve criminal cases and finish the forensics.

(A) Types of cyber forensics:

In order to identify the perpetrator by presenting the evidence to the court, cyber forensics gathers data as evidence for a crime (using electronic equipment) while following to suitable investigation protocols. The main objective of cyber forensics is to maintain the chain of evidence and documentation to pinpoint the digital criminal. Cyber forensics can:

1. Retrieve deleted data, chat histories, emails, and more.
2. Erase calls and SMS
3. Record calls and play them back later.
4. Track who utilized which system when and for how long.
5. Find which user executed which program.

Depending on the area that requires digital inquiry, there are various forms of computer forensics. Here are the fields:

1. *Network forensics:* it entails keeping track of and evaluating network traffic to and from the criminal's network. Network intrusion detection systems and other automated techniques are some of the tools used for this purpose.
2. *Email forensics*: In this kind of forensics, specialists examine the criminal's email and retrieve deleted email threads to extract important case-relevant data.
3. *Malware forensics*: This area of forensics deals with crimes relating to hacking. This includes analyzing malware or malicious software to determine its source, function, and likely consequences.
4. *Memory forensics*: This area of forensics obtains raw data from the memory (such as cache, RAM, etc.) in order to extract information. A similar forensic related to this is

 [ISSN 2581-5369]

disk forensics which examines and analyses data from modified and deleted sources.

5. *Mobile forensics*: They look over and evaluate the cell phone's data. It requires retrieving information from mobile devices, such as contacts, incoming and outgoing text messages, images, and video files.
6. *Database forensics*: This area of forensics looks at and evaluates data from databases and the metadata that goes with it.
7. *Incident response forensics*: Identifying the underlying cause of a cyber incident or attack in order to stop such problems in the future is the goal of incident response forensics.

(B) Stages of investigation in cyber forensics:

According to Richard H. Ward[10], an investigator's job is to defend the innocent by obtaining information, evaluating the reliability of the information, identifying and tracking down the perpetrators of crimes, and providing evidence of their guilt to a court of law. In other words, identification, preparation, collection, examination, analysis, and reporting are the six steps an investigator must take when conducting an investigation.

1. *Identification*: Identification is the first step in the investigative process, during which the investigator looks for the answers to questions like "who," "what," "when," "where," and "how," and from there determines how to move the case forward. It clarifies the accessibility of possible evidence retained on electronic storage devices including laptops, cell phones, and PDAs.
2. *Preparation*: Preparing entails setting up tools, procedures, and search warrants. The preservation of evidence stage of the investigation involves freezing or securing the crime scene to stop any action that could change or erase data saved on a digital device. Data authenticity must be preserved because preservation fosters credibility and reduces the possibility of misdirection.
3. *Collection*: This process entails obtaining pertinent data either directly from the device or by documenting it. Personal computers are seized from the scene of the incident, files are copied or printed from the server, and network activity is recorded according to a set, accepted protocol. In this stage of the investigation, every piece of information that may be gleaned from electronic devices, equipment, and media is covered. Mobile

[10]Dr. Richard Ward, Lecturer in Cyber Security, Faculty of Computing, Engineering and Science at University of South Wales.

 [ISSN 2581-5369]

phones are a valuable source of information for cases because they are not only a mode of communication between two individuals but also help uncover facts.

4. *Examining:* After the material is gathered from potential sources, it is systematically examined. A thorough investigation is conducted to look at data files. Examining and documenting prospective evidence's source, genesis, creation, alteration, or destruction is the process of examination. This documentation method ensures that both the exculpatory and incriminating information is preserved.
5. *Analysis*: To analyze is to make judgments based on information obtained. To ensure that the information may serve as credible proof, it must be evaluated. At this step, a simulation of the crime scene is displayed to show the connections between events and to interpret the result using digital evidence. The most difficult and time-consuming step is evidence analysis because a scad data must be analyzed.
6. *Reporting*: At the last stage, a report is written to provide a summary of the investigation's findings, the data that was recovered, and the investigator's actions. Every detail is kept from all earlier forensic stages and is recorded in the report. An excellent report will have thorough notes, documentation, visuals, and tool-generated information. Physical evidence, records of interrogations, and other pertinent information obtained throughout the case are included in the final report. With the use of this report, the prosecution in a court of law attempts to convict a suspect.

(C) Admissibility of cyber forensics:

The relevance of electronic records for establishing offences has been realised in the digital age where the majority of conversations and transactions take place online. As a result, through revisions, s.65 of the Indian Evidence Act has been enlarged to grant sanction to electronic records as digital evidence.

Section 65 of the Indian Evidence Act:

"Cases in which secondary evidence relating to documents may be given.—Secondary evidence may be given of the existence, condition, or contents of a document in the following cases:—

a. When the original is shown or appears to be in the possession or power— of the person against whom the document is sought to be proved, or of any person out of reach of, or not subject to, the process of the Court, or of any person legally bound to produce it, and when, after the notice mentioned in section 66, such person does not produce it;

b. when the existence, condition or contents of the original have been proved to be admitted in

 [ISSN 2581-5369]

writing by the person against whom it is proved or by his representative in interest"[11]

S.65-A and S.65-B establish the following criteria for electronic records' admissibility as digital evidence:

1. Evidence is acquired through a computer that was regularly used for any authorised activity produced the evidence.

2. Information of the kind used as evidence was routinely entered into the computer as part of a routine.

3. The computer's operation does not jeopardise the correctness of the electronic record that was created.

Only when a certificate supporting the electronic record being used as evidence is it possible to rely on secondary electronic evidence. There is no need to produce such a certificate for primary evidence in an electronic record. Due to the sensitivity of these evidences, the court must closely monitor them to assure uniqueness. The courts have reaffirmed time and time again that evidence obtained using modern methods and tools cannot be rejected as evidence, given that their veracity can be established.

In *R.M. Malkani v. State of Maharashtra*[12], the Supreme Court noted that, in light of technological advancements, taped conversations are admissible as evidence so long as they are pertinent to the issues at hand, the voice can be recognised, and the accuracy of the conversation is established by removing the possibility that the taped version could have been altered. Under section 7 of the IEA[13], a contemporaneous Sellotape recording of a pertinent conversation qualifies as a relevant fact and is admissible in court.

According to the court's ruling in *State vs. Mohd. Afzal and Others*[14], computer-generated electronic documents are evidence and can be used as proof in court provided, they are established in accordance with Section 65B of the Evidence Act.

The offence of seeking a bribe was attempted to be proven in *Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke*[15] by producing a tape-recorded discussion, which the Supreme Court said was inadmissible. In fact, the conversation is not audible and was not taken into consideration for spectrographic analysis, according to the Directorate of Forensic Science

[11]Indian evidence act I.E.A. § 65 (Gazette of I 1872).
[12]*R. M. Malkani vs State Of Maharashtra*, 1973 AIR 157.
[13]Section 7 of the Indian Evidence Act- Facts which are the occasion, cause, or effect, immediate or otherwise, of relevant facts, or facts in issue, or which constitute the state of things under which they happened, or which afforded an opportunity for their occurrence or transaction, are relevant.
[14]*State vs. Mohd. Afzal and Others*, 2003 VIIAD Delhi 1
[15]*Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke*, (2015) 3 SCC 123.

 [ISSN 2581-5369]

Laboratories, State of Maharashtra, in its report.

The Supreme Court's ruling in *Arjun v. Kailash*[16] will ensure that the compliance burden under Section 65B(4) is partially reduced until a thorough review of the laws governing electronic evidence is conducted. The recent breach of electronic evidence (in the form of WhatsApp talks) underlines the necessity for measures to be put in place to preserve and keep electronic records in addition to the practical challenges. In a recent ruling, the Punjab & Haryana High Court cited Arjun v. Kailash and came to the conclusion that Whatsapp discussions are inadmissible as evidence unless a certificate required by Section 65B is supplied (4). It may be necessary to produce a certificate in accordance with Section 65B(4) to verify authenticity, but other measures must also be taken to protect the privacy and confidentiality of the data contained in electronic records. A five-judge committee's report from November 2018 that contained draught rules for the preservation, retrieval, and authentication of electronic records was cited by Justice Nariman in his ruling. While the application of Section 65B is now more clear, there are still numerous procedures that must be taken to guarantee the security, preservation, and confidentiality of data gathered in the form of electronic evidence.

III. IMPORTANT CASES WHERE CYBER FORENSICS PLAYED A MAJOR ROLE

1. *Apple trade secret theft case*[17]

At Apple's autonomous automobile division, an engineer by the name of Xiaolang Zhang announced his resignation and stated he would be returning to China to care for his ailing mother. He caused concern when he revealed to his management that he intended to work at a Chinese producer of electronic vehicles. A Federal Bureau of Investigation (FBI) affidavit states that after reviewing Zhang's online activities on the business network, Apple's security team discovered that he had taken trade secrets from secure company databases in the days before his resignation. The FBI charged him with a violation in 2018.

2. *ENRON scandal*[18]

Enron, a U.S. firm that went bankrupt in 2001, erroneously reported billions of dollars in sales in one of the most widely documented accounting fraud scandals. This caused financial loss to

[16] ARJUN PANDITRAO KHOTKAR v. KAILASH KUSHANRAO GORANTYAL AND ORS, (E SUPREME Ct. INDIA 2020).

[17]Jacob J Pritt, *Apple Sues Former High-Level Employee for Trade Secret Use, Disclosure,* NATIONAL LAW REVIEW (March 24, 2021), https://www.natlawreview.com/article/apple-sues-former-high-level-employee-trade-secret-use-disclosure

[18]Enron Task Force, *Transcript of Statement by Deputy Attorney General Paul J.Mcnulty on the Convictions of Former Enron Chief Executive officers Ken Lay and Jeff Skilling*, (May 25, 2006), https://www.justice.gov/archive/enron/pdf/layskillingverdictstatementvydagmcnulty.pdf.

numerous employees and others who had invested in the company. Terabytes of data were analysed by computer forensic specialists to comprehend the intricate fraud scheme. The Sarbanes-Oxley Act of 2002, which established new accounting compliance rules for public firms, was passed in part as a result of the scandal. In 2001, the business declared bankruptcy.

3. *Google trade secrets theft case*[19]

A former executive of both Uber and Google, Anthony Scott Levandowski, was accused of 33 counts of stealing trade secrets in 2019. Levandowski worked on Google's self-driving car project from 2009 to 2016, during which time he downloaded thousands of program-related files from a password-protected corporate server. According to The New York Times, he left Google and founded the self-driving truck firm Otto, which Uber acquired in 2016. Levandowski was given a sentence of 18 months in jail, $851,499 in fines and reparations, and a guilty plea to one count of theft of trade secrets. In January 2021, Levandowski was granted a presidential pardon.

4. *Larry Thomas*[20]

Larry killed a person and was later convicted based on one of his social media posts in which he was wearing the same bracelet as was found on the crime scene.

5. *Michael Jackson*[21]

Detectives used information and medical papers from Michael Jackson's doctor's iPhone that proved the doctor had prescribed fatal dosages of drugs to Jackson which led to his death in 2009.

IV. DIGITAL FORENSICS VS. RIGHT TO PRIVACY

People's concerns about how their personal information is handled in the course of an investigation are growing because any revelation could seriously violate their right to privacy. Private data might only be accessed under common data protection standards if it meets specific precursor requirements. Yet, police enforcement personnel frequently exempted in order to stop and identify criminality. In other words, information pertaining to illegal activity is not protected. When electronic data is provided to forensic science analysts, there is a chance that privacy will be violated. It makes sense to assume that forensic investigators should have access

[19]Former Uber Executive Sentenced To 18 Months In Jail For Trade Secret Theft From Google, United States Department of Justice (Aug. 4, 2020), https://www.justice.gov/usao-ndca/pr/former-uber-executive-sentenced-18-months-jail-trade-secret-theft-google.
[20]*United States v. Larry Thomas,* (U.S. Ct. App. for the 8th Cir. 2022).
[21]Peter Wehrwein, Propofol: the drug that killed Michael Jackson, Harvard Health Blog (Nov. 7, 2011), https://www.health.harvard.edu/blog/propofol-the-drug-that-killed-michael-jackson-201111073772.

 [ISSN 2581-5369]

to anything that might be useful in finding the accused so that the victim can receive justice. Yet, sometimes, the investigator takes not only the necessary information but also all of the confidential information that is irrelevant to the case or is not valuable for it. They apply it to different ends. So, there is always a chance that privacy will be violated during a cyber forensics inquiry. With the development of computer forensic tools, it is now easier to search for and discover particular data sets in the context of an inquiry, such as emails, credit card numbers, passport numbers, phone numbers, identification card numbers, images, videos, etc.

This may be comparable to the contentious Aadhar Card case, when the UDIAI used to gather all the data from Indian individuals on behalf of the government. As a result, in such circumstances, it would be simple for any unauthorised person to manipulate the account and use it for illicit reasons if they had access to the PIN, password, Username, or other necessary information due to the forensic science analyst. Thus, in a manner we may say that if forensic investigators acquire access to that personal information which is not essential for the case in hand, then it should fall under the ambit of breach of right to privacy. In India, there is a need for some sort of regulatory body that can create a code of conduct and accredit forensic investigators. This code of conduct may also include rules for the violation of a person's right to privacy if a disclosure of personal information puts that person's life in danger.

Cyber forensics are governed by well-established international organisations. The forensic science department of the Indian government may adopt those organisations' codes of conduct. The International Society of Forensic Computer Examiners is one such group that the Indian forensic department ought to join. In the subject of cyber forensics, it is one of the most well-known organisations. One must pass the test and receive a certificate from the organisation in order to be a competent forensic investigator. The majority of the world accepts their accreditation.

Frank Law[22] and others in their research have proposed certain procedures to make sure digital forensics do not infringe on anyone’s right to privacy. According to their theory, encryption is one way to safeguard private data in digital form and helps prevent illegal information exposure. The challenge is in how to encrypt the data such that the investigator can only access the pertinent information and is unable to access any extraneous information. And as for the procedure, they think the following steps need to be taken to ensure data privacy:

1. Investigators should not view the content of digital storage media where digital data

[22]Frank Y.W Law et al., *Protecting Digital. Data Privacy in Computer Forensic Examination*, University of Hong Kong 3 (2011).

 [ISSN 2581-5369]

privacy is a problem; instead, they should analyse a bit-stream image that was obtained using standard computer forensic procedures.

2. An encryption key is to be created by the data owner
3. The image will next be scanned in order to create index files that link the data content to the image's sector positions. The index files will then be encrypted in order to guard against information leakage.
4. The investigator will create a list of keywords that are pertinent to the investigation prior to looking through the index files' contents. These terms will be used to look for digital proof in the image that was obtained.
5. The data owner provides the investigator with the key for searching, and they can then use the list of approved terms to conduct their search. It would be possible to retrieve the image sector where pertinent keyword hits are noted. The image might then be used to extract relevant digital data for further analysis.

V. ANALYSIS AND CONCLUSION

Using cyber forensics is a novel strategy for stopping cybercrime. Therefore, it is important for professionals to have ongoing education and training that will enable them to handle the complexity of crime. In order for cyber forensic analysts and investigators to be able to handle crimes from which the cybercriminal would not be able to escape, it is necessary to perform sufficient and comprehensive training. Training comes in many forms, including three-day workshops, corporate courses, and specialist courses. This will enable students to gain more hands-on experience, which will lead to the most effective and efficient use of tools and procedures. The tools and strategies that were mentioned above are some of the top ones that are utilised by numerous nations and are continuously updated.

After a comprehensive investigation, the key issue is how to present the evidence in court. After the research and analysis, the most challenging element is ensuring that the evidence is relevant to the cybercriminal. As already discussed, the training offers in-depth research on this subject to aid the investigators in gathering information that will be acceptable as evidence in court. To ensure that the provision of the specific and authentic evidence is not compromised, the specialist works precisely and in strict confidence[23]. The specialist created a report to be presented in court after assembling all the case's information and supporting documentation. In

[23]B.V. Prasanthi, Prathyusha Kanakam & S Mahaboob Hussain, *Cyber Forensic Science to Diagnose Digital Crimes- A study*, 5 INT'L J. COMPUT. 110, 107-113 (2017)

 [ISSN 2581-5369]

order for the court to fully comprehend all the details and processes used by the professional, they must also testify in accordance with the nature and circumstances of the case.

Also, it has been observed that everyone who uses the internet should be properly informed on its benefits and drawbacks. It is important to use the internet responsibly, and awareness is the key. The legislation governing the right to privacy in relation to cyberspace is still in its infancy, thus it is up to the individual to guarantee that their privacy rights are not violated out of ignorance.

Cyber forensics and cybercrimes have developed as a result of the technology's lightning-quick development. The use of diverse tools and techniques in the cyber forensic is emerging as a new strategy to combat cybercrime. Using general criteria, professionals can acquire the evidence and compile it, then present their findings as verifiable evidence in a court of law. The expansion of this industry is a double-edged sword that benefits both criminals and cyber forensic analysts. As the tool has its own limitations and only the specialist can make the most of it by using his knowledge, the specialist cannot rely completely on it. In order to obtain vast data that can be used as evidence without violating the subject's right to privacy, specialists must be trained appropriately and act ethically.

*****

 [ISSN 2581-5369]