The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 4 | Issue 6 | June 2026
ISSN: 2583-973X (Online), SJIF IF(2026): 5.6
Website: www.theacademic.in

Cyber Forensics: - A Tool to Detect Cyber Crime in India

Akshita

LL.M. Graduate (Independent Researcher), E.mail Id.:- akshitabaliyan123@gmail.com

DOI : https://doi.org/ 10.5281/zenodo.21391750

ARTICLE DETAILS

Research Paper

Received: 21-05-2026

Accepted: 28-06-2026

Published: 15-07-2026

Keywords:

Cybercrime, cyber Forensics, digital forensics, digital criminology, computerised proof, computer forensics.

ABSTRACT

Cybercrime is a global issue, and India is no special case. Cybercrime has arisen as quite difficult for all law regulation offices, government, organizations, and people in India. The rising development of technology and the web has set out new open doors for hoodlums to take advantages through advanced digital means. Digital forensics or cyber forensics is an instrument that can be utilized to research and distinguish cybercrime in India and in the entire world. Cyber forensics play important role in detecting cyber-crime and helps in finding the real culprit behind that crime through the use of cyber forensics tools. This paper tells about the concept of cyber- crime, cyber forensics, its significance, and the way that it very well may be utilized to recognize cybercrime in India, tools and procedure utilized by cyber forensics experts in digital forensics investigation. The paper additionally tells about the challenges looked by law enforcing organizations and the suggestions that should be taken to conquer them.

Introduction

Cybercrime has arisen as a significant danger in the computerized time. Cybercrime is a type of crime that is committed using computers, networks, or through internet. Cybercrime can take place in many forms, including hacking, cyber fraud, cyberbullying, cyberstalking, and online misrepresentation. With the rising utilization of computers, cell phones, and the web, cybercrime has become more common than any other crime. Cybercrime can affect the busisness of people, organizations, and state run administrations like

government. India, in the same way as other different nations, has seen a huge expansion in cybercrime as of late. To handle this developing danger, digital criminology has arisen as a significant apparatus to recognize and explore cyber-crime; this digital criminology is known as cyber forensics or digital forensics. Digital crime scene investigation also known as cyber forensics is the method involved with gathering, analysing, and saving computerized or digital proof for legal purposes. "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" (Kruse & Heiser, 2002).

"Cyber forensics involves the identification, documentation, and interpretation of computer media for using them as evidence and to rebuild the crime scenario" (Baggili, Mislan, & Rogers, 2007). Cyber forensics is the practice of collecting, analysing and preserving digital evidence in a way that is admissible in a court of law. "According to computer forensics defined as the process of identifying, collecting, preserving, analysing and presenting the computer-related evidence in a manner that is legally acceptable by court" (Caloyannides, 2004) . Cyber forensics technology is a digital field that involves the use of various digital and cyber tools and tech regulations connected with cybercrime. Also, global associations or international organisations, like Interpol and Europol, have laid out cybercrime units that work with public policing to examine and recognize cybercrime. These associations likewise give the unmistakable approach to dividing of data and their digital legal sciences advances between different nations to further develop cybercrime examinations.

India has seen a huge expansion in cybercrime lately. As per the NCRB report, cybercrime cases in India expanded by 63.5% from 2017 to 2018. The most widely recognized kind of cybercrime in India is online fraud, which represents 35.7% of all cybercrime cases, so to manage these sorts of cybercrimes digital legal sciences or digital forensics play a significant part. When the proof has been gathered, cyber forensics experts utilize various methods and advancements to identify that cybercrime. One of the critical difficulties of cyber forensics is that it's a dynamic and continuously changing nature of innovation. The aim of this research paper is to look at the job of digital criminology or cyber forensics in distinguishing cybercrime in India. The paper will start by giving an outline of cybercrime and cyber forensics, trailed by a top to bottom conversation on cyber forensics or digital forensics, its strategies, and its applications in identifying and researching cybercrime. At long last, the paper will conclude with a conversation on the difficulties or challenges faced in executing digital criminology or cyber forensics in India and the ideas or suggestions given on the best way to manage these difficulties.

Cybercrime and Cyber forensics

Cybercrime alludes to crimes that include the utilization of computers or computer organizations also known as computer network, for example, hacking, fraud, phishing, malware circulation, and refusal of administration assaults. Cybercrime can result in monetary loss, robbery of delicate data, interruption of basic frameworks and disorganisation of critical system. "The first known cybercrime was the "The Morris Worm" in 1988, which infected thousands of computers through the internet" (Gandhi, 2012).

"The mid-2000s saw the rise of another kind of cybercrime i.e. phishing. Lawbreakers or criminals conveyed messages and emails that appeared be from genuine sources, requesting that beneficiaries to give individuals personal data. This procedure permitted crooks to take data from countless individuals without a moment's delay. Cybercrime likewise turned out to be more coordinated, with criminal gatherings utilizing the web to convey and arrange their exercises. The ascent of cell phones and virtual entertainment like social media set out new opportunities for cybercriminals. Cybercrime is now a global problem, with criminals using increasingly sophisticated techniques to steal data and money" (Bhangla & Tuli, 2021). The utilization of machine learning and AI is additionally making it simpler for crooks and hoodlums to carry out attacks and complete assaults. As technology keeps on growing and developing, it necessitates the amendment of existing policies and to adopt new norms to regulate it. India has been doing whatever it may take to address cybercrime and safeguard against cyber assaults and attacks through the execution of digital regulations. These digital regulations are also known as cyber laws. The Information Technology (IT) Act, 2000, is the essential regulation administering cybercrime in India. The act has been amended a few times to stay aware of the changing idea of cybercrime. Moreover, the Indian Penal Code, 1860, additionally contains arrangements that can be utilized to prosecute cyber-crime .This law characterizes different kinds of cybercrime, for example, hacking, virus assaults, and cyber terrorism, data theft and layouts punishments and penalties for guilty parties. The Act also covers electronic transactions, digital signatures, and data protection.

Cybercrime alludes to crimes that are done utilizing computers or the web. Here is an outline of most common and absolute types of cyber-crime:

1. *Hacking*: Hacking is an unauthorized access to a computer or network system. The aim of a hacker is to steal data, damage the system, or simply to gain access of the system.

2. *Phishing*: It involves using email, text messages, or other forms of communication to trick individuals into sharing their personal information, such as passwords or credit card details. This information is then used for identity theft or other fraudulent activities.

3. *Malware*: Malware refers to malicious software that is designed to harm a computer system or steal data. Malware can take many forms, including viruses, worms, and Trojan horses.

4. *Ransomware*: Ransomware is a type of malware that encrypts a victim's data and demands payment in exchange for the decryption key. Ransomware attacks are typically carried out for financial gain.

5. *Identity theft*: Identity theft involves stealing someone's personal information, such as their name, social security number, or credit card details, and using that information to carry out fraudulent activities.

6. *Cyber stalking*: Cyber stalking involves using the internet or other digital technologies to harass or threaten someone. This can include sending threatening messages, posting personal information online, or monitoring someone's online activity without their consent.

7. *Cyberbullying*: Cyberbullying involves the use of internet to harass or intimidate someone. It includes sending hurtful messages, spreading rumours online, or posting embarrassing photos or videos.

8. *Child pornography*: Child pornography involves creating, distributing, or possessing images or videos of children engaged in sexual activity. This is a serious crime that can have severe legal consequences.

As technology continues to evolve, almost certainly, new sorts of cybercrime will arise, making it significant for people and associations to stay careful and do whatever it may take to safeguard themselves from digital dangers and cyber threats.

TABLE I CYBER-CRIME REPORTED IN INDIA EVERY YEAR

Year in which cyber-crime reported	**Number of crime reported in each year**
2014	9,622
2015	11,592
2016	12,317
2017	21,593
2018	27,248
2019	44,735

2020	50,035

Source- Google Images (News 18)

Cyber forensics- Cyber forensics is the most common way of gathering, examining, and protecting computerized proof to explore and prosecute cybercrimes. It includes utilizing specific techniques and apparatuses to analyse the information from computers, networks and other digital gadgets to distinguish and find digital hoodlums. Digital forensics assumes a basic part in fighting cybercrime, as it permits specialists to recreate occasions covering the way to an occurrence, distinguish culprits, and accumulate proof that can be utilized in legal procedure.

Cyber forensics has its underlying foundations in customary scientific science. “During the period of1970s, cyber forensics was utilized to explore computer violations. The main utilization of digital forensics in a criminal case was in 1984, when examiners utilized information from a computer to convict a suspect in a homicide” (Saurabh & Roy, 2021). Digital forensics depends on various tools and techniques to examine digital wrongdoings. One of the main instruments is forensics software, which is utilized to examine information from computerized gadgets. These product apparatuses can recuperate erased records; break down network traffic, and quest for proof of malware. One more significant tool in digital forensics is the utilization of steganography, which is the act of concealing data inside other data. This method is utilized by cybercriminals to conceal their exercises. Digital legal specialists use steganography recognition devices to reveal secret data.

Cyber forensics and Artificial Intelligence- Cyber forensics examinations include gathering and investigating digital proof from different computerized sources, like computers, cell phones, and other advanced gadgets. As the amount of advanced digital information keeps on developing, customary techniques for examination have become less powerful. This has prompted a rising interest in the utilization of computerized reasoning (computer based intelligence) in digital legal examinations. Artificial intelligence can possibly change the field of digital cyber sciences in more w than one way. One of the greatest advantages of artificial intelligence is its ability to process and break down a lot of information rapidly and precisely. This can help investigators identify patterns and abnormality that may be indicative of cybercrime. Artificial intelligence algorithms can likewise be prepared to perceive explicit kinds of computerized proof, for example, malware or steganography, making it more straightforward to distinguish these sorts of dangers. One more benefit of Artificial Intelligence in cyber forensics is its capacity to robotize certain errands. “Artificial Intelligence can also be utilized to distinguish and follow suspects, as well as to foresee future digital dangers in view of historical data. Artificial Intelligence additionally has a

few impediments in the field of digital legal sciences. Due to Covid pandemic in the year 2020, the growth of AI has been increasing day by day. This is due to the need of digitalizing the human elements and to provide the solution of the problems through artificial intelligence" (Singh & Loura, 2021). "One of the greatest difficulties is the absence of standardisation in the field. Various examiners and organisations might utilize various instruments and techniques, which can make it hard to foster the AI algorithms that can be applied all around" (Rughani, 2017).

Artificial intelligence algorithms are just however great as the information they seem to be prepared on, and assuming that that information is one-sided, the calculation might create one-sided results. This can be especially dangerous in cases including delicate issues, like race, religion, or orientation. At long last, artificial intelligence can likewise be restricted by its failure to perceive setting. "Digital forensics examinations frequently require a profound comprehension of the setting where digital evidence was gathered, for example, the particular programming and equipment setups utilized by a suspect. An AI algorithm is unable to completely comprehend these variations which can prompt mistaken or incomplete results" (Mukkamala & Sung, 2003).

Cyber forensics and Cyber security- Cyber security allude to the assurance of computer systems and networks from unauthorised access, theft, or harm. Cyber security is fundamental to stop cybercrime and safeguard delicate data, like monetary records, individual data, and licensed innovation i.e. intellectual property. Cyber forensics and cyber security are firmly related, and they cooperate to forestall and examine cybercrime. Cyber forensics is utilized to examine and tackle digital assaults, while cyber security means to prevent and safeguard computer system and network from digital assaults. Cyber forensics is utilized in cyber security to break down and distinguish digital - attacks, recognize the reason and degree of the attack, and follow the beginning of the attack. Cyber security is utilized in cyber forensics to prevent and distinguish digital attacks, safeguard advanced proof, and save information for scientific examination.

Relationship between Cyber Forensics and Indian Law.

Cyber forensics is the most common way of gathering, examining, and protecting computerized proof to explore and prosecute cybercrimes. The essential law for governing digital forensics and cybercrime examination procedure in India is Information Technology Act, 2000 (IT Act) and its resulting amendments. The IT Act gives a legal regime for managing different cyber offenses, including unauthorised access, hacking, data robbery, cyber fraud, online misrepresentation, and different cybercrimes. It characterizes offenses and punishments connected with cybercrimes and furthermore frames the procedure for examination, assemble, and conservation of electronic proof for evidence. Under the IT Act, the Indian

government has laid out the Indian Computer Emergency Response Team (CERT-In) as the public organization for network safety episode reaction. CERT-In is liable for gathering, dissecting, and scattering data about digital occurrences, as well as organizing reactions to digital dangers. "The Indian Penal Code also contains the sections which deal with offences like defamation, bullying, fraud, pornography, theft these are some of the offences which also takes place in the dark world of cyber space. The punishment for cyber offences are given under chapter XI of Information Technology Act, 2000. The Indian Evidence Act also contains the provisions regarding the acceptance of electronic proofs/evidences in courtroom" (Maheshwari & Sharma, 2021). The Information Technology (Guidelines for Cyber Cafe) Rules, 2011, these guidelines force specific commitments on cyber cafe holders to keep up with records of clients and report dubious exercises to the specialists. The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009: These guidelines frame the methods and shields for capture, checking, and unscrambling of data by government offices for the reasons for public safety or examination of cybercrimes. Article 21 of Indian constitution states that "No person shall be deprived of his life and personal liberty except according to the procedure established by law." With regards to digital forensics, Article 21 assumes a big role in guaranteeing the freedoms and protection of people during the examination and collection of electronic proof. While digital forensics is vital for exploring and forestalling cybercrimes, it should be led in a way that regards the principles of fair treatment, decency, and security of individual freedoms. With regards to digital forensics or cyber forensics, the principles got from Article 21 can be applied in the accompanying ways:

1. *Protection of Privacy*- Article 21 recognizes the right to privacy as a vital part of the right to life and individual freedom (personal liberty). During cyber forensics examinations, the protection of people privacy and the data of their personal source should be defended. Legal agents should follow legal methods, for example, getting suitable search warrants or court orders, and stick to the guideline of proportionality in gathering and examining electronic evidence.
2. *Admissibility of Evidence*- Article 21 likewise guarantees that any hardship of personal liberty should be as indicated by the procedure laid out by legislation. This implies that any proof acquired through digital criminology should be gathered and saved adhering to lawful systems and rules. Adherence to the endorsed legal system, including the Information Technology Act, 2000, and other important regulations, is fundamental to guarantee the acceptability of electronic proof in court.
3. *Fair Trial*- Article 21 ensures the right to a fair trial, which incorporates the right to introduce a defense and challenge the proof against a charged individual. In digital criminology, the examination ought to be

led in a fair and unbiased way, guaranteeing that the privileges of the accused, for example, the right to be informed regarding the charges and the right to legal representation, are maintained.

4. *Protection against Arbitrary Actions*- Article 21 shields people from arbitrary or unlawful activities by the state. It guarantees that digital criminology examinations are led inside the limits of the law and that the powers of policing are not abused to encroach upon the privileges of people.

In general, while digital criminology or cyber forensics is critical for exploring cybercrimes and keeping up with cyber safety or cyber security, it should be done in a way that maintains the standards of Article 21, guaranteeing the right to life and personal liberty protection of privacy, and fair trial of people in this procedure. It is foremost to take note of that the legal parts of digital criminology or cyber forensics can differ from one jurisdiction to other jurisdiction. Regulations and guidelines connected with cybercrime and digital proof can contrast, and legal experts and digital scientific examiners should keep awake up-to-date with the applicable rules and regulations in their particular jurisdiction.

Steps involved in Cyber forensics in detecting cyber- crime

The steps involved in a typical cyber forensics investigation may vary depending on the nature of the case and the tools and techniques used by the investigators. However, here is a general overview of the steps involved:

1. *Recognition of Evidence*: The first step in a cyber forensics investigation is identifying the evidence that needs to be collected. This may involve identifying the types of digital devices, systems, and networks that are relevant to the case.

2. *Assemble of Evidence*: Once the evidence has been identified, the next step is to collect it in a manner that preserves its integrity and maintains a chain of custody. This may involve using specialized tools and techniques to acquire data from digital devices, such as computers, servers, and mobile devices.

3. *Conservation of Evidence*: The collected evidence needs to be preserved in a secure and controlled environment to prevent tampering or contamination. This may involve creating a forensic image of the device, which is an exact replica of the data on the device.

4. *Examination of Evidence*: Once the evidence has been collected, the next step is to analyse it to examine relevant information. This may involve using specialized software tools to search for keywords, file types, and other indicators that could help in the investigation.

5. *Demonstration of Findings*: After the analysis is complete, the investigator must present their findings in a clear and concise manner. This may involve creating reports, visual aids, or other forms of communication to convey complex technical information to a non-technical audience.

6. *Legal and moral Considerations*: Throughout the investigation, the investigator must also consider legal and ethical considerations, such as maintaining the privacy of individuals involved in the investigation and following relevant laws and regulations.

7. *Testimony*: If the investigation leads to a legal proceeding, the investigator may be called upon to provide testimony in court or other legal settings.

Generally speaking, an effective cyber forensics investigation requires an intensive comprehension of digital system, particular instruments and techniques and a sharp eye on every detail.

Tools and techniques used in cyber forensics in detecting cybercrime

Cyber forensics involves various tools and techniques that are used to collect and examine digital evidence. Some of the commonly used instruments and strategy in cyber forensics are as follows:

1. *Disk Imaging*: Disk imaging is the process of creating a complete copy of a hard drive, including all data, files, and system information. This technique is used to preserve digital evidence and to analyse the data for forensic investigation.

2. *Network Forensics*: Network forensics involves analyzing network traffic to detect and investigate cybercrime. This technique involves the use of various tools, such as packet sniffers, network analysers, and intrusion detection systems, to capture and analyse network traffic.

3. *Memory Forensics*: Memory forensics involves analyzing the contents of a computer's memory to detect and investigate cybercrime. This technique is used to recover data that has been lost or deleted and to analyse data to determine the cause of a cyber- attack.

4. *Malware Analysis*: Malware analysis involves analyzing malicious software, such as viruses, Trojans, and worms, to detect and investigate cybercrime. This technique involves the use of various tools, such as sandboxing and debugging tools, to analyse the behaviour of malware and to identify its origin and purpose.
5. *Log Analysis/log examination*: Log analysis includes breaking down system logs, for example, occasion logs and security logs, to recognize and explore cybercrime. This method includes the utilization of

different devices, like log analysis software, to distinguish uncertain exercises and to follow the beginning of a digital assault.

6. *Steganography examination*: Steganography analysis includes the utilization of different instruments, for example, steganalysis programming, to recognize and break down secret information.
7. *Data Recovery*: Data recovery includes retrieve lost or deleted information from computerized gadgets, for example, hard drives, USB drives, and cell phones. This procedure is utilized to regain information that is basic to a forensic examination.

> "Cyber forensics is an essential apparatus in the battle against cybercrime. The utilization of different devices and methods in empowers examine cyber forensics to gather, break down, and protect digital proof to research and address cybercrime" (Karie, Kebande, & Venter, 2019).

Challenges faced by cyber forensics in detecting cyber-crime.

Cyber forensics also called digital forensics, is the most common way of gathering, examining, and safeguarding electronic information as a proof in a criminal examination. Coming up next are a portion of the challenges that cyber forensics specialists face in recognizing cybercrime:

1. *Encryption*- Encryption is the method involved with changing over plaintext information into figure text, making it incomprehensible to unapproved clients. Encoded information represents a huge test to cyber forensics experts since they should have the option to decode the information to get to the data put away inside it.

2. *Anti-forensic techniques*- Cybercriminals utilize different anti-forensics techniques to disguise their exercises, for example, record cleaning, steganography, and information stowing away. These strategies make it hard for cyber forensics experts to recover and examine electronic proof.

3. *Jurisdictional issues*- Cybercrime is many times transnational, implying that the culprit and casualty might be situated in various nations. This can make jurisdictional issues, as various nations might have various regulations with respect to cybercrime.

4. *Privacy concerns*- Cyber forensics experts should adjust the need to gather proof with the protection privileges of people. This can be a fragile equilibrium, as the assortment and investigation of electronic evidence might possibly attack an individual's privacy.

5. *Lack of standardization*- There is a lack of standardisation in the field of cyber forensics, which makes it hard to look at and assess changed techniques and devices. This can prompt irregularities in the manner that proof is gathered and examine.

6. *Rapidly evolving technology*- Technology is continually developing, and cybercriminals are continuously tracking down better approaches to take advantage of technology for criminal activities. This implies that cyber forensics specialists should continually refresh their abilities and information to stay aware of the latest patterns and techniques. It will help in detecting cyber threats and preventing the commission of cyber-crime and other related offences.

Generally, the challenges looked by cyber forensic specialists in identifying cybercrime are complicated and continually developing. To be compelling, they should keep up-to-date with the most recent innovation and techniques, be versatile and adaptable, and work cooperatively with other policing and network protection.

3. Awareness campaigns- Public awareness campaigns on cybercrime and digital forensics ought to be directed to teach residents on the risks of cybercrime and the significance of revealing cybercrime events.

4. Standardization- There is a need to create and carry out standardised systems and conventions for cyber forensics examinations. This will guarantee that proof is gathered and examined in a steady and solid way, making it permissible in court.

Suggestion

Cyber forensics plays a vital role in detecting and investigating cybercrime in India. Here are some suggestions for improving cyber forensics capabilities in India:

1. *Education and awareness*- There is a need to increase awareness and schooling about cyber forensics among law agencies, prosecutors, judges. Specific preparation projects and seminars on cyber forensics ought to be given to enforcing agencies to upgrade their abilities and knowledge.

2. *Legal structure*- There is a need to reinforce the legal structure connected with cybercrime and digital forensics in India. The regulations and guidelines connected with cybercrime ought to be refreshed and made more rigid to block cyber criminals.

3. *Awareness campaigns*- Public awareness campaigns on cybercrime and digital forensics ought to be directed to teach residents on the risks of cybercrime and the significance of revealing cybercrime events.

4. *Standardization*- There is a need to create and carry out standardised systems and conventions for cyber forensics examinations. This will guarantee that proof is gathered and examined in a steady and solid way, making it permissible in court.

Conclusion

Cyber forensics is a significant instrument for recognizing cybercrime in India, there is a requirement for additional interest in preparing and limit working for experts and for the improvement of refreshed regulation and guidelines. Cyber forensics is the method involved with gathering, breaking down, and safeguarding electronic information and data to help examinations connected with cybercrime. With the rising predominance of cybercrime, digital forensics has turned into a fundamental device for law enforcing agencies and associations to investigate and summon cybercriminals. In summary cyber forensics is a fundamental apparatus in tackling cybercrime, and its significance is probably going to increment as the pervasiveness of cybercrime keeps on rising. Cyber forensics assumes a crucial part in fighting cybercrime in the rea of digitalisation. Through the assortment and examination of advanced proof, digital forensics specialists can distinguish and indict cybercriminals, guaranteeing that they are considered responsible for their activities. While cybercrime stays a critical test, preceded with headways in cyber forensics procedures and tools give desire to a more secure and safer web-based climate.

References

1. Kruse, W. G., & Heiser, J. G. (2002*). Computer forensics: Incident response essentials.* Addison-Wesley Pearson Education.

2. Baggili, I. M., Mislan, R., & Rogers, M. (2007). *Mobile phone forensics tool testing: A database driven approach. International Journal of Digital Evidence*, 6(2), 168–178.

3. Caloyannides, M. A. (2004). *Privacy protection and computer forensics* (2nd ed.). Boston, MA: Artech House.

4. Gandhi, V. K. (2012). *An overview study on cyber crimes in Internet. Journal of Information Engineering and Applications*, 2(1), 37–42.

5. Bhangla, A., & Tuli, J. (2021). *A study on cyber crime and its legal framework in India. International Journal of Law Management & Humanities*, 4(2), 493–504.

6. Saurabh, P., & Roy, A. J. K. (2021). *Role of cyber forensics in investigation of cyber crimes. International Journal of Law Management & Humanities*, 4(3), 786–798.

7. Singh, K. D. P., & Loura, J. (2021). *Cyber security in civil aviation: Current trends. Dehradun Law Review*, 13(2), 125–143.

8. Rughani, P. H. (2017). *Artificial intelligence based digital forensics framework. International Journal of Advanced Research in Computer Science*, 8(8), 139–144.

9. Mukkamala, S., & Sung, A. H. (2003). *Identifying significant features for network forensic analysis using artificial intelligent techniques. International Journal of Digital Evidence*, 1(4), 1–17.

10. Maheshwari, S., & Sharma, N. (2021). *Cyber forensic: A new approach to combat cyber crime. Pen Acclaims: A Multi-Disciplinary National Journal*, 15, 1–13.

11. Karie, N. M., Kebande, V. R., & Venter, H. S. (2019). *Diverging deep learning cognitive computing techniques into cyber forensics. Forensic Science International: Synergy*, 1, 61–67.