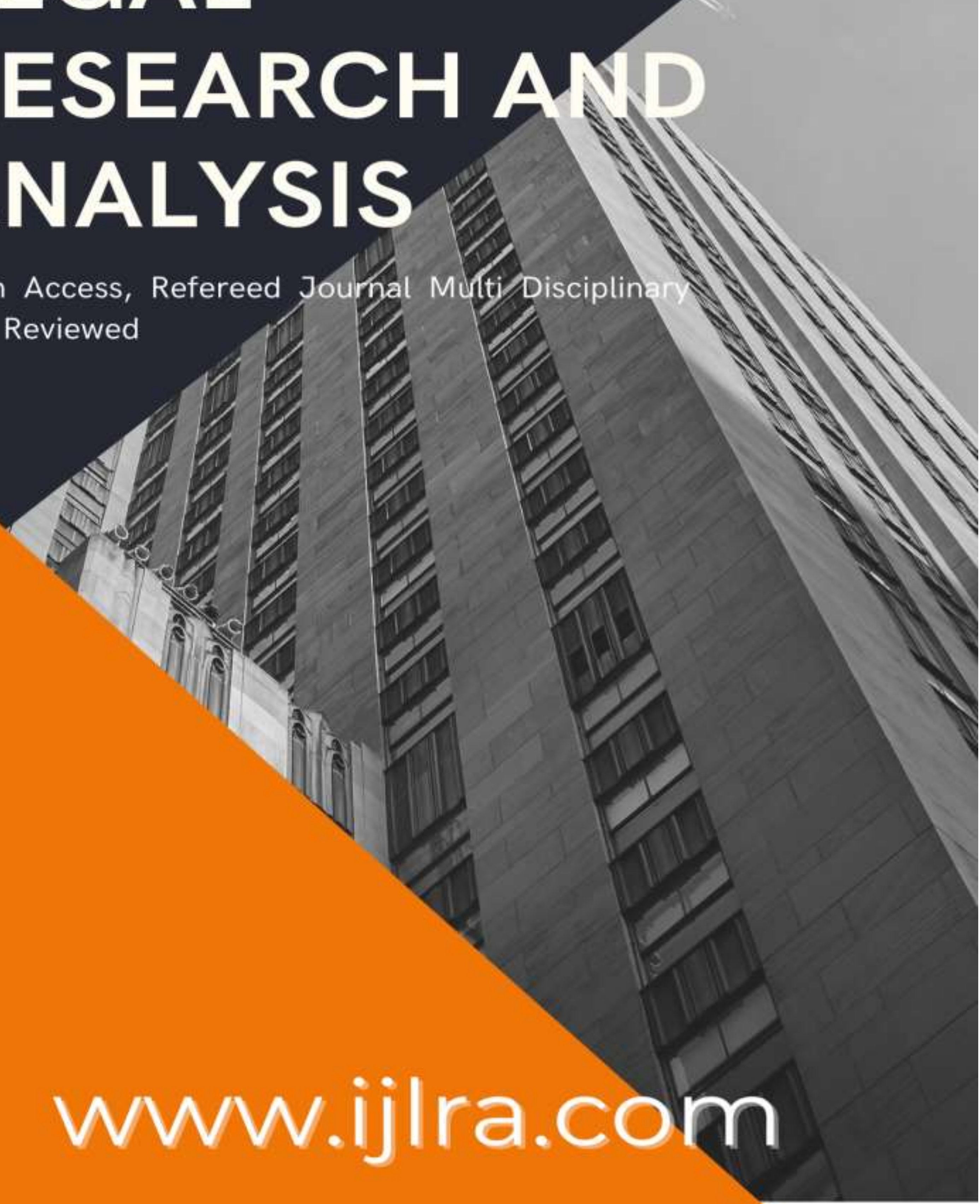
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN
2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

DIGITAL FORENSICS IN LAW ENFORCEMENT: IMPORTANCE AND CHALLENGES

AUTHORED BY - KAVYASHREE R & APOORVA SRI A R

ABSTRACT

India is currently in a digital era where individuals rely on the internet for nearly every aspect of their daily lives, from waking up to going to bed. As technology evolves rapidly, so do cybercrime and cyberthreats. In this context, digital forensics, plays a crucial role. Computer science and legal forensics combine to gather digital evidence, store it on the computer for case investigation, and then present it in a court of law. In an earlier period where there was no development, there were a lot of people working on an investigation, and because there was no access to the internet, it was time-consuming. However, with the help of digital advancements, we have improved a lot in solving crimes. A key development in this regard is the latest legislation, Bharatiya Sakshya Adhiniyam, 2023, an amendment to the Indian Evidence Act, 1872, which places considerable focus on electronic evidence and its admissibility and procedural aspects of presenting in court. While digital forensics offers a powerful tool for investigation, its complexity in understanding and lack of widespread knowledge in this field pose significant challenges to its adoption. This paper will discuss its advantages and disadvantages, its current standing in the Indian courts, and potential solutions if problems arise. Finally, the paper also discusses the need for technological adaptation to effectively combat cybercrime.

KEYWORDS: Digital Forensics, Cybercrime, Internet, Technology, Investigation.

I. INTRODUCTION

Digital Forensics is like peering into digital universe where every bit and byte holds secrets waiting to be discovered. It holds the key to unlock the hidden secrets. With the help of this technique detectives can probe the cyberspace to find crucial information, resolve cases that are extremely complex in nature and prevent digital crimes. Digital forensics is not just for investigations into malicious software, child pornography, and white-collar crime, it is an

 ISSN: 2582-6433

essential part of homeland security and the fight against terrorism[1]. There are millions of people using the Internet worldwide, and the number is rising daily. Computer networks, automated data systems, and the Internet offer an endless amount of opportunities for illicit activity. Through the use of computers, crimes are being committed against individuals, groups, governments, and property[2]. The evidence backlog has not been significantly reduced in practice, despite the fact that the digital forensic procedure has advanced significantly in recent years[3]. With increase in the rate of cyber-attacks and cyber-crimes there is a necessity to safeguard a digital data. The use of electronic devices, such as computers, smartphones, the internet, etc., has led to the growth of this field.

II. DIGITAL FORENSICS

Digital forensic science focuses on the investigation and analysis of digital devices like computers, laptops, smartphones, and storage media to gather evidence for legal purposes. It involves techniques to recover, preserve, and analyze data from these devices to uncover digital evidence that can be used in criminal investigations or legal proceedings[4]. Digital forensics plays a crucial role in identifying cybercrimes, data breaches, and other digital incidents by examining digital artifacts and electronic records[5]. It's a fascinating field that combines technology, law, and investigative skills to solve complex digital mysteries.

Digital forensics is primarily used for two purposes:

- **Investigation**

  An investigation will be started once the crime is committed. So, the common place to look for getting clues is the smartphone and laptop of a suspect. A Digital forensics specialist looks for information that is crucial to the investigation after identifying a suspect and taking their laptop or smartphone into evidence. Evidence must be handled within legally acceptable standards so that the results they obtain can be used as proof. Prosecution may then use the material they found during the investigation whether it be

[1] Rogers, M.K. and Seigfried, K. (2004) 'The future of computer forensics: a needs analysis survey,' Computers & Security, 23(1), pp. 12–16. https://doi.org/10.1016/j.cose.2004.01.003.

[2] Newman, R.C. (2007). Computer Forensics: Evidence Collection and Management (1st ed.). Auerbach Publications. https://doi.org/10.1201/9780849305627.

[3] Lillis, D. et al. (2016) Current challenges and future research areas for digital forensic investigation. https://arxiv.org/abs/1604.03850.

[4] M. Harbawi and A. Varol, "The role of digital forensics in combating cybercrimes," 2016 4th International Symposium on Digital Forensic and Security (ISDFS), Little Rock, AR, USA, 2016, pp. 138-142, doi: 10.1109/ISDFS.2016.7473532.

[5] Fenu, G. and Solinas, F. (2013) 'COMPUTER FORENSICS INVESTIGATION AN APPROACH TO EVIDENCE IN CYBERSPACE,' Research Gate, pp. 77–88. https://iris.unica.it/handle/11584/109723.

 ISSN: 2582-6433

documents, browsing history, or even metadata can be used to build a strong case against the suspect.

- **Data Recovery**

  The professionals also help in the recovery of the data. They retrieve the data that was previously lost, which is beneficial for those who have lost some necessary data, such as a business that has had a system crash and that may also be important for ongoing case[6]. Investigators can monitor digital footprints, access records, and recreate information with the aid of data recovery techniques.

III. IMPORTANCE OF DIGITAL FORENSICS

- **Digital Evidence Collection**

  To collect digital evidence effectively, it is crucial to rely on the expertise of a digital forensics specialist. These professionals are trained to preserve digital evidence while ensuring its integrity, making it admissible in court. They use various data recovery methods to retrieve information from digital devices, even when it has been deleted or corrupted.

  A key process in this field is forensic imaging, which creates an exact, bit-by-bit copy of the original device to prevent data alteration or loss. This allows for detailed analysis through methods such as keyword searches, metadata reviews, and timeline reconstructions.

  Forensic specialists also use a variety of specialized tools and software designed to make digital evidence collection more precise and efficient. Their skills and access to advanced technology allow for the effective gathering and analysis of digital evidence, which plays a crucial role in investigations and legal proceedings as it can be used in the Court.

- **Data Recovery**

  The speedy recovery of data from digital devices is one of the main benefits of computer forensics. When handling digital evidence, quick data recovery is essential, and computer forensics makes it possible to retrieve lost or erased data quickly. Forensic

[6] DeVry University (2023) What is Computer Forensics? https://www.devry.edu/blog/what-is-computer-forensics.html.

techniques can be used to retrieve encrypted or destroyed data, which may provide important details regarding illicit activities.

This involves restoring data from a variety of devices, including laptops, smartphones, and hard drives, utilizing sophisticated recovery tools and methodologies. Quick data recovery is essential for investigations because it enables forensic professionals to examine the evidence and find important information quickly, which increases the overall efficacy of digital investigations.

- **Enhanced Investigation Efficiency**

  Through the use of specialized techniques and tools for obtaining and evaluating digital evidence, computer forensics greatly increases the effectiveness of investigations. The preservation of evidence is a major advantage because, in the wrong hands, digital data can be quickly changed or destroyed. Maintaining the integrity of the evidence strengthens the investigation and raises the likelihood of a successful resolution through the use of appropriate forensic techniques.

  Computer forensics which is a branch of Digital forensics also improves data security by locating weaknesses in systems and suggesting countermeasures to avoid similar occurrences in the future.

- **Legal Support**

  When using digital forensics in investigations, strong legal support can be expected. The digital evidence recovered and analyzed by forensic experts, such as deleted files, browsing histories, and emails, can withstand scrutiny in court. This evidence can be instrumental in proving innocence or guilt, establishing timelines, and uncovering motives in criminal cases.

  Additionally, Digital forensics plays a crucial role in identifying cybercriminals and supporting prosecutions, bolstering the credibility of the evidence presented in legal proceedings and contributing to a just legal process.

- **Accurate Data Analysis**

  Digital forensics allows for precise analysis of digital data, providing valuable insights for investigations. Advanced forensic techniques enable investigators to gather and thoroughly examine digital evidence from sources like hard drives, mobile devices, and network logs.

 ISSN: 2582-6433

Standardized procedures ensure that data is validated for integrity and reliability. This accurate analysis helps investigators uncover patterns, establish connections, and generate leads, ultimately supporting legal proceedings and enabling sound conclusions based on solid evidence[7].

- **Prevention of Cybercrime and future crimes**

  Digital forensics is an essential tool for preventing cybercrime by identifying and analyzing digital evidence. As cyber threats increase in the digital age, cybersecurity has become more critical than ever.

  Digital forensics helps detect cyber threats through the analysis of digital footprints like log files and network traffic. It also enables experts to find system vulnerabilities and strengthen cybersecurity measures. By tracking down cybercriminals and deterring future attacks, computer forensics is a key weapon in the fight against cybercrime.

  Digital footprints, user accounts, and IP addresses are among the pieces of evidence that forensic investigation might find that connect suspects to crimes[8]. Future crimes can be prevented by leveraging insights from forensic investigations.

- **Effective Fraud Detection**

  Digital forensics excels at detecting fraud efficiently. By promoting the use of higher modern frameworks for digitization techniques, which allows powerful benches to help investigate seismic cases in many layers of peer oceans. When forensic investigators examine the digital footprints of financial transactions, emails and other digital evidence, they hope to find common threads or irregular activity across them.

  Digital forensics also assists in risk assessment by identifying system vulnerabilities and suggesting ways to mitigate fraud risks. The use of cutting-edge technologies like machine learning and artificial intelligence further enhances fraud detection, making computer forensics a vital tool in combating financial crimes.

- **Ensuring system integrity**

  Digital forensics ensures integrity of computer systems by preserving the data and

[7] Ali, A. (2024) Advantages and Disadvantages of Computers Forensics » Hubvela. https://hubvela.com/hub/technology/advantages-disadvantages-computers/forensics/#4-strong-legal-support.
[8] Welch, T. (1997) 'Computer Crime Investigation and Computer Forensics,' Information Systems Security, 6(2), pp. 56–80. https://doi.org/10.1080/10658989709342536.

 ISSN: 2582-6433

information at original state during investigations.

- **In-depth Analysis**
  To reconstruct events and create timelines of illegal behaviour, forensic specialists can examine digital artifacts including emails, log files, and file metadata.

- **Expert Testimony**
  In court, forensic specialists can give reliable testimony that helps juries and judges understand intricate technical aspects.

IV. CASES STUDIES AND LEGAL PRECEDENTS

a) BTK Killer case

Digital Forensics played a key role in this case. Analysts examined the computer device of Rader's and uncovering the vital information. They recovered the deleted files, photos of victims, and detailed logs of his activities all of which helped establish his identity. Investigators also decoded encrypted messages and uncovered hidden files through advanced forensic techniques leading to arrest and conviction[9].

b) Larry J. Thomas Vs State of Indiana[10]

Rito Llamas-Juarez was killed during an attempted robbery that Thomas was convicted guilty of. Although there were eyewitnesses in the case that attested to Thomas's presence at the crime scene, digital forensics added even more weight to the evidence.

The authorities considered the posts made on the offender's Facebook account while conducting their investigation. They discovered that he had been posting pictures of himself with an assault rifle on social media under the username "Slaughtaboi Larro." The gun in Thomas's internet photos and the ammunition used in the murder case were identical. Additionally, a bracelet discovered at the crime scene was matched to the images. It was a bracelet similar to the one Thomas had been sporting in the internet photos. Thomas was consequently taken into custody and locked up.

[9] Espinosa, C. and Espinosa, C. (2024) 'Digital forensics and the BTK killer - Blue Goat Cyber,' Blue Goat Cyber, 26 April. https://bluegoatcyber.com/blog/digital-forensics-and-the-btk-killer-a-case-study-in-solving-crimes/.
[10] Larry J. Thomas Vs State of Indiana, 18A-CR-1714.

 ISSN: 2582-6433

c) **Krenar Lusha case**

The authorities were able to track down Lusha because he got information from the internet on building bombs, detonators, search belts, etc. He also expressed his hatred for Jews and Americans in correspondence with other users on the internet. Lusha was apprehended by the police downloading videos on how to make mobile detonators after they obtained a search order for his flat. Incriminating tangible evidence was also discovered, such as parts for gasoline bombs, ammunition for guns, and cell phones used to set off explosives. The police were able to apprehend him before he could commit any violent or destructive crimes because of digital forensics.

d) **State of Tamil Nadu v. Suhas Katti[11]**

In this case, a fake email address was made in order to damage the victim's reputation by disseminating obscene and disparaging information about her. The accused was charged under Section 67 of the IT Act and Sections 469 and 509 of the Indian Penal Code, 1860. The Court's severe penalties made it abundantly evident that cyber harassment and defamation are serious offenses.

e) **Nasscom vs. Ajay Sood & Others[12]**

In this case, Court held that phishing on internet is an illegal activity though it is not defined under any statute. It categorized phishing as passing off which caused damage to Nasscom trademark rights. The court granted injunction to defendants from using the Nasscom's trademark. The local commissioner was appointed to gather the evidence and two hard disc containing false e-mail were found. The digital evidence played a crucial role in the case.

f) **United States v. Wurie, 2013[13]**

In 2007, a drug dealer was arrested and two cell phones were collected and inspected. Based on information from the cell phone, the police were able to locate the drug dealer's residence using digital forensics. They then requested a search warrant and discovered additional drugs and firearms in the dealer's apartment.

---

[11] State of Tamil Nadu v. Suhas Katti, (2008) 150 DLT 769.
[12] Nasscom vs. Ajay Sood & Others, 119(2005)DLT596.
[13] (United States v. Wurie, 724 F.3d 255 (1st Cir. 2013).

 ISSN: 2582-6433

g) **U.S. v. Hilton**[14]

In this instance, the appellant's hard drive contained child pornography that was found using computer forensics. The appellant contended that the Child Pornography Prevention Act (CPPA), which dealt with the possession of child pornography, was unconstitutional due to its definition that encompassed images that "appear to be" children. This might potentially include legal adult pornography that bore similarities to child exploitation. A district judge concurred, dismissing the accusations for being too ambiguous. A higher court reversed this ruling, reiterating the indictment and permitting the prosecution to move further on the grounds that the appellant's challenge to the CPPA was inadmissible.

h) **The Enron scandal, 2001-2002**

Due to the extent of the financial manipulation and the manner digital forensics was used to reveal the truth, the Enron incident is still a key case in corporate fraud investigations. In order to retrieve erased evidence, piece together intricate financial transactions, and ultimately apprehend corporate offenders, digital forensic techniques were crucial. The case demonstrated the significance of digital evidence in contemporary financial crimes and paved the way for stricter rules and corporate governance compliance requirements.

i) **The Boston Marathon bombing, 2013**

The Boston Marathon bombing was terrorist attack which killed 3three people and injured hundreds. The investigation brought to light how important digital forensics is to contemporary criminal investigations. Digital forensic techniques were critical to identifying the suspects, reconstructing the crime, and apprehending the criminals. These techniques ranged from the collecting and processing of copious quantities of video and photographic evidence to tracking internet activities and communications. This case showed how digital forensics may use technology to help solve complicated, well-known crimes and support public safety.

j) **Pegasus Spyware Scandal, 2010**

India became embroiled in the debate about the deployment of Pegasus spyware in

[14] *U.S. v. Hilton*, Crim. No. 97-78-P-C, Civil No. 02-235-P-C (D. Me. Mar. 20, 2003).

 ISSN: 2582-6433

2021. Experts in digital forensics were crucial in examining claims of unauthorized monitoring by tracing the spyware through mobile device analysis. This particular instance illustrated the significance of digital forensics in revealing intricate cyber spying operations.

V. CHALLENGES IN DIGITAL FORENSICS

The digital forensics is a process of investigation did in the field of computers and other electronic devices. They have a prominent place in this digital era as discussed above, still as every coin has its other side these computer forensics also have their challenges. The challenges which will be faced by the computer forensics are briefly explained below

I. TECHNICAL ISSUES:

1. **Technology Advancement:**

   Every day, new gadgets emerge on the scene bringing with them intriguing benefits as well as drawbacks. Technological advancement may also result in insoluble problems since humans are constantly seeking out new information and tend to overlook how it will impact us down the road[15]. This is also what is bound to occur to computer forensics; when they attempt to look into a crime, more technologically sophisticated criminals will have ways around them. The task of solving a case will then become indefinite[16].

   University of Washington, "Synthesize" software tool issue, 2017:

   The University developed a program called "Synthesize" that was used to generate lifelike recordings of celebrities performing, conversing, or simply being in the room. This was another illustration of the deep fake technology that was popular around the time when artificial intelligence began to develop quickly. The digital forensic investigators are left wondering whether transparency and accountability will be provided in light of this software capability[17].

---

[15] Maria Karyda & Lilian Mitrou, *Internet forensics: Legal and Technical Issues*, 2 SECOND INTERNATIONAL WORKSHOP ON DIGITAL FORENSICS AND INCIDENT ANALYSIS (WDFIA 2007) 3–12 (2007).

[16] Cisomag, CHALLENGES AND APPLICATIONS OF DIGITAL FORENSICS CISO MAG | CYBER SECURITY MAGAZINE (2021), https://cisomag.com/challenges-and-applications-of-digital-forensics/ (last visited Sep 23, 2024).

[17] Suwajanakorn, S. *et al.* (2017) *Synthesizing obama: Learning Lip Sync from audio: ACM Transactions on Graphics: Vol 36, no 4, ACM Transactions on Graphics*. Available at: https://dl.acm.org/doi/10.1145/3072959.3073640 (Accessed: 23 September 2024).

 ISSN: 2582-6433

2. **Police not getting warrant and mishandling:**

   The admissibility of digital forensics evidence in court is beset with difficulties since the police must follow certain procedures in order for it to be accepted, one of which being obtaining a warrant in advance. In several instances, despite the effectiveness of the law enforcement's digital forensics investigation, the admittance of the suspects was denied on the grounds that no warrant had been granted[18].Police digital forensics gather, store, and present evidence in court. However, there are a few instances during this process where evidence is handled improperly, harming the victim. These occur most frequently in rape cases when texts discovered on a mobile phone are handled improperly for personal gain[19].

   The United States v. Suarez and Vincent Tabbachino (2010) [20]:

   This case highlighted the need for evidence preservation in law enforcement. The prosecution used Solomon Dwek, a cooperating witness, to communicate with the defendants under a pseudonym. The court found that agents Russ and McCarthy were unable to produce the SMS text communications, leading to the defendants not being found guilty of conspiracy to commit extortion, attempted extortion, and bribery.

   Krumwiede v. Brighton Associates, 2006[21]:

   Brighton Associates fired Director of Business Development, Krumwiede, who later worked for a competing company. Brighton counterclaimed for breach of contract and misappropriation of a business opportunity. Krumwiede agreed to have his laptop forensically analyzed by a neutral expert, who found that he had altered thousands of files and metadata, leading to willful and bad faith spoliation of evidence. The court found Krumwiede's conduct contemptuous and warranted a default judgment. The digital forensic experts were unable to preserve important digital evidence, leading to the dismissal of the case.

3. **Cross contamination:**

   Digital evidence that has been contaminated by other sources loses some of its

---

[18] SEARCH WARRANTS FOR DIGITAL DEVICES - UNC SCHOOL OF ..., https://www.sog.unc.edu/sites/www.sog.unc.edu/files/additional_files/2.0 Handout re Search Warrants for Digital Devices -- version for Court of Appeals Judges.pdf (last visited Sep 23, 2024).

[19] Police mishandling digital evidence, forensic experts warn, THE GUARDIAN (2018), https://www.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn (last visited Sep 23, 2024).

[20] *U.S. v. Suarez*, Criminal Action No. 09-932 (JLL) (D.N.J. Aug. 26, 2010)

[21] *Krumwiede v. Brighton Associates, L.L.C.*, Case No. 05 C 3003 (N.D. Ill. Aug. 9, 2006)

admissibility, which might lead to serious issues throughout the legal proceedings as it calls into doubt the authenticity of the evidence. Data corruption during storage, carelessness when transferring digital evidence, contaminated computer forensics workstations, improper handling of digital evidence, and data transfers without proper protections are some of the ways that investigators can cause contamination[22].

II. LEGAL ISSUES:

1. Privacy concerns:

The primary stage in the usage of digital forensics is accessing an individual's personal information. For example, the first step an investigator takes to obtain information regarding a crime is to learn about the criminal and any relevant facts. In typical forensic cases, this involves entering someone's property and obtaining a warrant in order to gather information. However, in computer forensics, there may be situations in which it is necessary to interfere with a person's personal information in order to gather information[23]. In these situations, the privacy of the individual may be violated, which may also compromise the validity of the evidence[24].

The American Society of Crime Laboratory Directors has created a set of guidelines for digital and multimedia evidence, which addresses privacy concerns. Another strategy is to allow forensic specialists, attorneys, and other professionals to work together and communicate with one another[25].

Apple vs. FBI, 2016[26]

Apple was ordered to build a covert backdoor by the FBI in order to obtain data from an iPhone that belonged to one of the San Bernardino attackers. This request was

[22] Let's start a new journey today, DIGITAL FORENSICS AND EVIDENCE HANDLING FOR LEGAL PROCEEDINGS | CHARTERED INSTITUTE OF PROFESSIONAL CERTIFICATIONS, https://charteredcertifications.com/learning/courses/digital-forensics-evidence-handling (last visited Sep 23, 2024).

[23] Neil C. Rowe, *Privacy concerns with Digital Forensics*, CYBER LAW, PRIVACY, AND SECURITY 1464–1481 (2019).

[24] Frank Y.W. Law et al., *Protecting Digital Data Privacy in computer forensic examination*, 3089 2011 SIXTH IEEE INTERNATIONAL WORKSHOP ON SYSTEMATIC APPROACHES TO DIGITAL FORENSIC ENGINEERING 1–6 (2011).

[25] Amit Jaju, ETHICAL DIGITAL FORENSICS – BALANCING INVESTIGATION PROCEDURES WITH PRIVACY CONCERNS PRIVACY PROTECTION - PRIVACY - UNITED STATES (2023), https://www.mondaq.com/unitedstates/privacy-protection/1306880/ethical-digital-forensics-balancing-investigation-procedures-with-privacy-concerns (last visited Sep 23, 2024).

[26] Apple v. FBI, EPIC, https://epic.org/documents/apple-v-fbi-2/#:~:text=The%20case%20is%20captioned%20%E2%80%9CIn,%2C%20on%20February%2016%2C%202016. (last visited Sep 23, 2024).

submitted in order to look into a possible criminal. Here, Apple was asked to provide digital forensics for an inquiry aimed at opening a backdoor and gathering data, but they declined due to potential privacy issues it could create.

2. **Admissibility and Reliability concerns:**

Although forensic evidence is growing in India, there are still problems with its admissibility. The new amendment act, Bharatiya Sakshya Adhiniyam, 2023, explains in detail the provisions pertaining to forensic evidence and their procedure which is under section 61, 62, 63, but case jurisdiction, search and seizure, spoliation of evidence, and issues with "good faith," evidence preservation, investigation, and analysis make it difficult for the courts to admit such evidence[27]. The solution which can be opted for this issue is a proper protocol need to be followed for this digital evidence and that includes identification, collection, acquisition and preservation. If these steps are followed we can mitigate the admissibility issues[28]. There is no clear explanation in sec 63 of Bharatiya Sakshya Adhiniyam, 2023 on who can give certificate or if he refuses to give such certificate what could be done. This is a major backdrop for this section because the certificate given holds all the authenticity and the person giving it should also be authenticated.

There are six primary criteria that they fall under if reliability is an issue: process, tool, documentation, technique, examiner, and data set. Their absence of standard and scientific proof makes them all part of the responsibility as well as openness problem. Their lack of dependability makes it extremely difficult for suspects and defendants to exercise their legal rights. Numerous nations have responded to this issue by creating expert commissions and criteria to be improved[29].

Shafhi Mohammad v. State of Himachal Pradesh[30]:

referred to the Ministry of Home Affairs' (MHA) action plan on the use of videography in police investigations, which outlines capacity building in terms of forensic facilities, training, equipment, a plan for necessary funding, and the creation of Standard

[27] James Tetteh Ami-Narh & Patricia A.H. Williams, DIGITAL FORENSICS AND THE LEGAL SYSTEM: A DILEMMA OF OUR TIMES RESEARCH ONLINE, https://ro.ecu.edu.au/adf/41/ (last visited Sep 23, 2024).
[28] Ofori AY, *Digital Forensics Investigation Jurisprudence: Issues of admissibility of digital evidence*, 6 JOURNAL OF FORENSIC, LEGAL & INVESTIGATIVE SCIENCES 1–8 (2020).
[29] Radina Stoykova, *Digital evidence: Unaddressed threats to fairness and the presumption of Innocence*, 42 COMPUTER LAW & SECURITY REVIEW 105575 (2021).
[30] Shafhi Mohammad v. State of Himachal Pradesh, 2022 SCC OnLine SC 2115

Operating Procedures (SOP). "The time is ripe that steps are taken to introduce videography in investigation, particularly for crime scene as desirable and acceptable best practice as suggested by the Committee of the MHA to strengthen the Rule of Law," the Court said, issuing the required directives. Aside from the production of a certificate, which was reaffirmed in Anvar, it is quite desirable in such cases that the procedures for authenticating electronic evidence be further enhanced. With this method, the forensic elements of electronic or digital record become more crucial.

Tomaso Bruno & Anr vs State Of U.P[31]:

The prosecution's electronic evidence, which included hotel CCTV footage, was deemed untrustworthy by Tomaso Bruno and Elisabetta Boncompagni due to its lack of certification under Section 65B of the Indian Evidence Act, 1872. The conditions for using electronic records as evidence in Indian courts are described in this section. The Court recognized that although Section 65B certification improves the validity and dependability of electronic evidence, it does not completely exclude the admission of electronic evidence in the absence of the certificate. The Court ruled that if the evidence is trustworthy and its authenticity is shown by other methods, such witness testimony, it may still be included.

3. **Judicial flexibility:**

The most difficult expertise for judges and attorneys to possess is digital knowledge since it will significantly affect how justice is administered. There are still instances where cases are misdirected because to insufficient understanding of cybercrime and digital forensics. This could only be decreased if aspiring attorneys and seasoned attorneys in their area are taught the necessary information about cyber concerns[32]. The other problem in the legal system is that the judicial system have the authority to decide whether digital evidence is admissible, which might have a biased impact on one party or the other. The people's loss of trust in the legal system will result from the courts' abuse of authority[33].

[31] Tomaso Bruno & Anr vs State Of U.P (2015) 7 SCC 178

[32] LEGAL ISSUES FOR COMPUTER FORENSICS, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1361&context=acis2003 (last visited Sep 23, 2024).

[33] Cyber forensics, LEGAL SERVICE INDIA - LAW, LAWYERS AND LEGAL RESOURCES, https://www.legalserviceindia.com/legal/article-10974-cyber-forensics.html (last visited Sep 23, 2024).

The State of Arizona v. Jodi Ann Arias 2013 [34]**:**

This case involved Arias being accused of murdering her boyfriend Travis Alexander. The defense argued that law enforcement's handling of digital evidence, including child pornography, contributed to Arias' mental state. The court found one claim of procedural misconduct, including unqualified officer handled digital evidence in search and seizure, failing department procedure. Arias was convicted and sentenced to natural life in prison. The case highlights the importance of legal procedures in digital forensic investigations.

4. **Section 532 of BNSS:**

This provision permits all appeal procedures to be conducted electronically or by electronic communication, as well as the issuing of summonses and warrants, the questioning of the complainant and witnesses, the trial before Sessions Court and High Court, and the recording of evidence. Although this clause permits the court to conduct all proceedings digitally, which will be mitigate the burden of courts but artificial intelligence and deep fake technologies will eventually surpass the electronic processes now employed in courts since they are more susceptible to manipulation[35].

Digital forensic labs:

Although the law permits the use of electronics in court hearings, the relatively poor infrastructure and inefficient labs make it difficult to trust the evidence that digital forensic investigators find[36].

III. SOCIAL ISSUES:

1. **Bias and discrimination:**

Law enforcement now uses facial recognition technologies to identify offenders based on factors such as gender, color, and structure of the face. These may be accurate in many circumstances, but in a few, they may lead to the erroneous conviction of common people. Because individuals are being assumed to be

[34] *State v. Arias*, 248 Ariz. 546, (Ariz. Ct. App. 2020)
[35] *Navigating challenges: Technology in criminal trials under BNSS (Bharatiya Nagarik Suraksha Sanhita)* (2024) *NICKELED AND DIMED*. Available at: https://nickledanddimed.com/2024/06/09/navigating-challenges-technology-in-criminal-trials-under-bnss-bharatiya-nagarik-suraksha-sanhita/ (Accessed: 24 September 2024).
[36] Sharma, R. (no date) *Revolutionising Digital Forensics: India's New Legal Frontiers, Bar and Bench - Indian Legal news*. Available at: https://www.barandbench.com/columns/revolutionizing-digital-forensics-indias-new-legal-frontiers (Accessed: 24 September 2024).

offenders based on racism and sexism, this might lead to a major crisis between the people and the government[37].

2. **Ethics in digital Forensics:**

   The philosophical study of moral good and bad as well as moral right and wrong can be referred to as ethics. This is important to understand in the field of digital forensics because, as all digital technology is created by humans, there is a high potential for manipulation[38]. While adhering to professional ethics can help bring about justice, working in any other field may have negative social effects. Since they provide the foundation for its operation, technical, legal, and social concerns will all be covered by digital forensics ethics. They should establish appropriate codes to operate in such a manner and remain impartial throughout[39].

3. **Global issues:**

   Because the internet is a global technology, cybercrime primarily occurs between two nations. As a result, determining the place of jurisdiction of the crime presents several challenges, to the point where digital forensics are useless. For the case to go with greater efficiency, both nations' collaboration must be strengthened. In that scenario, it will be very difficult to accept those evidence because digital forensics standards vary between nations[40].

VI. CONCLUSION:

Cybercrimes are on the rise because to the rising influence of digital technology in today's environment. Digital forensics is one technique that law enforcement uses to combat crimes that are committed. Cybercrime experts in the area are in charge of this forensics. The field of digital forensics is significant and fraught with difficulties that fall into three categories: technological, legal, and societal. This study has emphasized the potential answers to all of the

[37] Amit Jaju, ETHICAL DIGITAL FORENSICS – BALANCING INVESTIGATION PROCEDURES WITH PRIVACY CONCERNS PRIVACY PROTECTION - PRIVACY - UNITED STATES (2023), https://www.mondaq.com/unitedstates/privacy-protection/1306880/ethical-digital-forensics-balancing-investigation-procedures-with-privacy-concerns (last visited Sep 23, 2024).

[38] Rowe, N.C. (no date) 'Privacy concerns with Digital Forensics', *Advances in Public Policy and Administration*, pp. 145–162. doi:10.4018/978-1-4666-9905-2.ch008.

[39] LEGAL AND ETHICAL CONSIDERATION IN DIGITAL FORENSICS, https://merryinsider.hashnode.dev/legal-and-ethical-consideration-in-digital-forensics (last visited Sep 23, 2024).

[40] Benefits and challenges of digital forensics, GLOBAL CYBER SECURITY NETWORK (2024), https://globalcybersecuritynetwork.com/blog/benefits-and-challenges-of-digital-forensics/#What_are_the_Challenges_of_Digital_Forensics (last visited Sep 23, 2024).

 ISSN: 2582-6433

problems and previous examples that addressed the problems in digital forensics. It is clear from the solutions and precedent cases that more has to be done to enforce the laws in this area. This may be done by standardizing procedures, establishing clear rules, and raising the level of understanding of judges and attorneys in this area. As these changes are implemented, the admissibility and reliability of the digital evidence gathered by the digital forensic investigators will rise, ultimately leading to the administration of justice.

VII. RECOMMENDATION AND FUTURE DIRECTIONS

The study will encourage policymakers and legal institutions to invest in digital forensic education and training to bridge the knowledge gap. Recommendations from this research could lead to more streamlined procedures for presenting digital evidence in court, making legal processes more efficient. With better integration of technology, the Indian judiciary can more effectively combat cybercrime, ensuring justice is served in a timely and accurate manner.