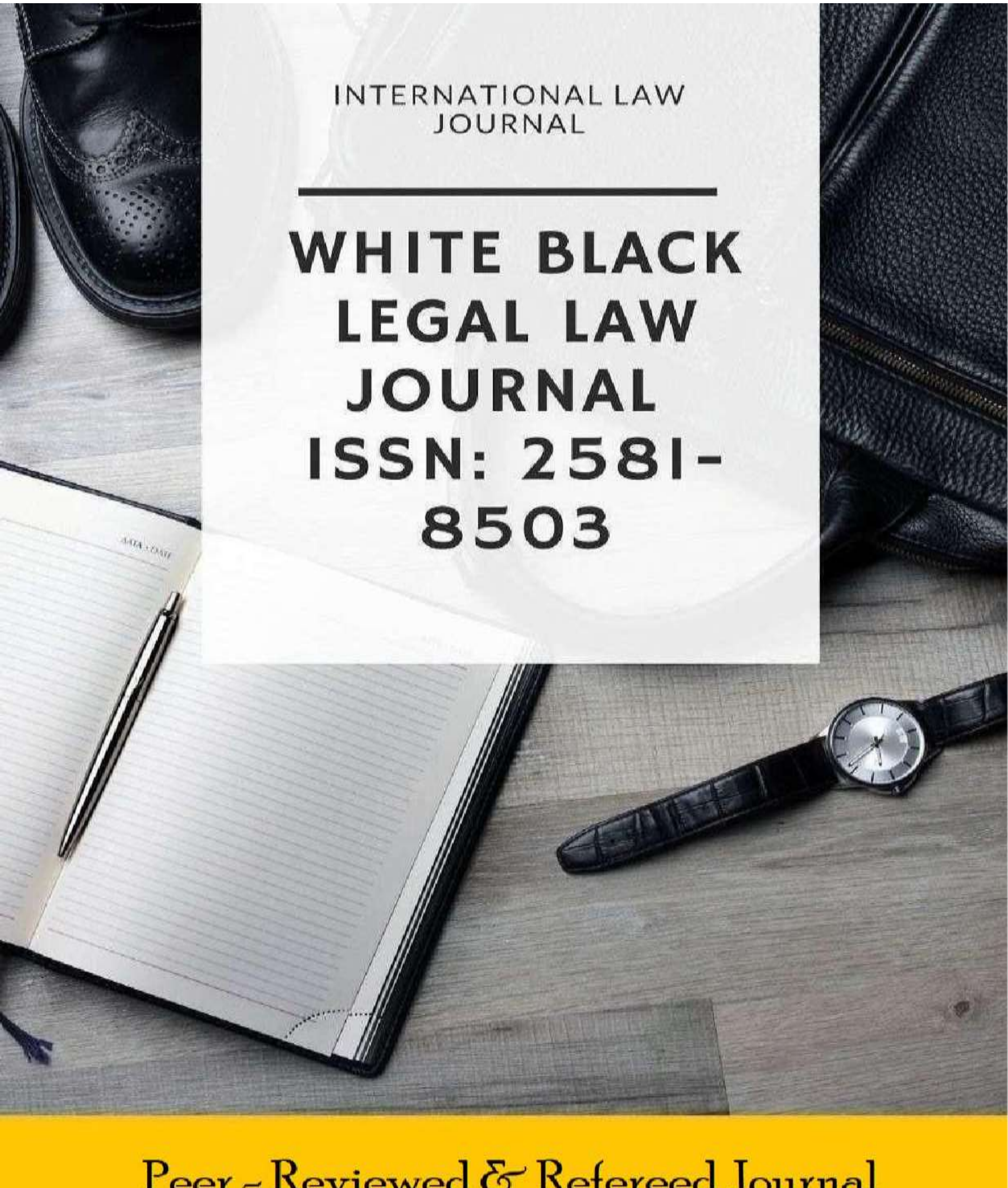

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

OPEN SOURCE TOOL IN CYBER FORENSIC AND ITS EVIDENTIARY VALUE

AUTHORED BY - AAKANKSHA CHANDRA

Abstract

Digital realm is a breeding ground for both the technologies and the crimes. With increase in technologies, Cyber forensic develop as an indispensable asset contributing unparalleled advantage to the digital investigation based significantly on different open source tools; it emerged as a powerful technique that revolutionised the cyber forensic world. In particular, Open source tool is a software that are easily accessible by everyone and become glorious in past few years because of its affordability, flexibility, compatibility.

The present paper focuses on functionalities, vulnerabilities of different open source tool providing multifaceted approach in collection, preservation and presentation of digital evidence. Additionally, the paper focuses on the evidentiary value of open source tool in court of law with reference to authenticity, hearsay evidence, best evidence and chain of custody. Also explores the legal framework and the legal cases that examine the evidentiary value of collected evidence through the tool which undermines the integrity and reliability in the court of law. The paper try to provide some basic suggestion to alleviate the challenges associated with the serviceability of tools in the cyber world.

Key Words: Cyber forensic, Chain of Custody, Expert Opinion, Hearsay Evidence

1. INTRODUCTION

In an age defined by the relentless expansion of digital technologies, the digital realm has become both a breeding ground for criminal activity and a treasure trove of evidence. The field of cyber forensics has emerged as a vital discipline to investigate cybercrimes, recover digital evidence, and bring perpetrators to justice. Central to the success of cyber forensics are open source tools, a category of software applications and utilities developed collaboratively and made freely available to the public.[1]

An open source tool refers to a software program or application that is developed, distributed, and made available to the public with its source code. It is open for everyone to view, modify, and distribute. Such as Linux operating system, Mozilla Firefox, Apache Open Office etc. These tools are often licensed under open source licenses, such as the GNU General Public License (GPL) or the MIT License, which provide legal frameworks for how the software can be used, modified, and distributed. Open source tools have revolutionized the landscape of cyber forensics by providing investigators, cyber security professionals, and law enforcement agencies with a diverse arsenal of powerful, cost-effective, and customizable solutions. These tools play an indispensable role in the identification, preservation, analysis, and presentation of digital evidence, ensuring the integrity and admissibility of such evidence in legal proceedings.[2]

This realm of open source tools encompasses a wide spectrum of applications tailored to specific aspects of cyber forensics. From disk imaging and data recovery to network traffic analysis, memory forensics, and malware analysis, these tools empower forensic experts to navigate the complex and ever-evolving digital landscape.

One of the hallmark features of open source tools is their transparency, as their source code is open for scrutiny and verification. This transparency not only fosters trust in the tools but also encourages collaboration and contributions from a global community of developers, enhancing the tools' capabilities over time.[3]

Moreover, open source tools democratize access to cyber forensics resources, making them available to organizations with varying budgets and needs, from large law enforcement agencies to small businesses seeking to protect their digital assets. The affordability and adaptability of open source solutions have democratized cyber forensics, enabling a broader range of stakeholders to actively

[1] John Perry Barlow, A Declaration of the Independence of Cyberspace, 18 *DLTR* 5-7 (2019)

[2] V Nagaraju, L Fiondella, T Wandji, An Open-Source Tool to Support the Quantitative Assessment of Cyber Security for Software Intensive System Acquisition, 16 *JIW* 31-50 (2017)

[3] Altay Aksulu, A Comprehensive Review and Synthesis of Open Source Research, 11 *JAIS 576-656* (2010)

engage in digital investigations.[4]

In this exploration of open source tools in cyber forensics, we will delve deeper into the diverse categories of tools available, their evident value in solving cybercrimes, and their role in preserving the integrity of digital evidence. We will also examine the ethical and legal considerations surrounding their use, ensuring that the benefits they offer are harnessed responsibly and within the confines of legal jurisdictions. Ultimately, open source tools stand as indispensable assets in the quest to uncover the truth hidden within the vast digital landscape of the 21st century.[5]

2. UNDERSTANDING OPEN SOURCE TOOLS IN CYBER FORENSICS

In the field of cyber forensics, a diverse range of open source tools plays a pivotal role in uncovering digital evidence and solving cybercrimes. These tools can be categorized into several essential categories, each serving a specific function in the investigative process. From data recovery tools that retrieve deleted files to disk imaging tools that create forensic copies of storage devices, memory analysis tools that examine volatile memory for insights, and network traffic analysis tools that dissect communication patterns within computer networks, these categories provide investigators with the necessary resources to navigate the complex digital landscape and ensure the integrity of digital evidence.[6] Each category plays a vital role in the collection, preservation, and analysis of digital artifacts, contributing to the successful resolution of cybercrimes and the pursuit of justice in the digital age. Some of the categories of Open source tools are:

- **Data Recovery Tools:** Data recovery tools are indispensable in the realm of cyber forensics as they facilitate the retrieval of digital data that has been deleted or lost. Whether intentionally or accidentally, when data is deleted, it often remains recoverable from storage devices such as hard drives, solid-state drives, or removable media. These tools employ various algorithms and scanning methods to identify and restore deleted files, directories, and even fragmented data. In a forensic context, data recovery tools are used to salvage crucial evidence, including

[4] Stephen Mason, Andrew Sheldon, Hein Dries, Proof: the technical collection and examination of electronic evidence 9 *ULP* (2017)
[5] *Id.*
[6] *Supra note 2 at 4*

documents, images, emails, and other digital artefacts. By doing so, investigators can piece together a comprehensive picture of events, actions, or communications relevant to an investigation.[7]

- **Disk Imaging Tools:** Disk imaging tools play a pivotal role in preserving the integrity of digital evidence during cyber forensic investigations. These tools create exact, bit-by-bit copies or forensic images of storage devices like hard drives and digital media. What sets them apart is their ability to capture not only active data but also unallocated and hidden data, ensuring nothing is altered in the original evidence. These images serve as an unchanging source of data for analysis, reducing the risk of contamination and ensuring the admissibility of evidence in a court of law. Disk imaging tools are fundamental in maintaining the chain of custody and accurately reproducing the state of a storage device at the time of seizure.[8]
- **Memory Analysis Tools:** Memory analysis tools specialize in scrutinizing the volatile memory (RAM) of a computer or device. In this ephemeral realm, critical data such as running processes, open network connections, encryption keys, and traces of recent activities can be found. Cyber forensics professionals use memory analysis to uncover evidence of malicious activities, volatile artifacts related to cyberattacks, and insights into system behavior at a given point in time. These tools are invaluable for identifying and mitigating cyber threats, as they allow investigators to access real-time system snapshots, even if the system was powered off or rebooted during an incident.[9]
- **Network Traffic Analysis Tools:** Network traffic analysis tools are instrumental in dissecting the communication flow within computer networks. They capture and scrutinize network packets, protocols, and traffic patterns to reveal crucial information about network activity. Cyber forensics experts employ these tools to understand the scope and impact of network-related cybercrimes, such as data breaches, Distributed Denial of Service (DDoS) attacks, and network intrusions. By analyzing network traffic, investigators can trace the origin and progression of an attack, identify compromised systems, and piece together the events leading

[7] An Open and Secure Internet: We Must Have Both, US Department of State *available at*: https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm (last visited on Seo 07, 2023)

[8] The Ethics of Privacy Protection (June 2, 2020) *available at:* https://www.researchgate.net/publication/3296 (last visited on Seo 07, 2023)

[9] Debashree Debnath, Cyber crime in Social media Issue and challenges, 3 *IJLMH* 2153-217- (2020)

up to a cyber-incident. This category of tools aids in both incident response and proactive network security.[10]

3. BENEFITS OF OPEN SOURCE TOOLS IN CYBER FORENSIC INVESTIGATIONS

In the ever-evolving landscape of cybercrime and digital investigations, the utilization of open source tools has emerged as a fundamental strategy for cyber forensic professionals. Open source tools, developed collaboratively and made freely available to the public, offer a plethora of advantages that significantly enhance the effectiveness and efficiency of cyber forensic investigations. In this discussion, we will delve into the benefits of employing open source tools in these critical investigations, highlighting their impact on data collection, cost-effectiveness, transparency, and adaptability to the evolving challenges of the digital realm.[11]

1. Cost-Effectiveness:

Open source tools are renowned for their affordability. They are typically available for free, eliminating the need for significant financial investments in proprietary software. This cost-effectiveness ensures that even organizations with limited budgets can access powerful cyber forensic tools, democratizing the field and enabling a broader range of stakeholders to engage actively in digital investigations.[12]

2. Wide Accessibility and Transparency:

The open source nature of these tools promotes transparency and trustworthiness. Their source code is open for scrutiny, allowing experts to validate the functionality and security of the tools. This transparency not only fosters trust but also encourages collaboration and contributions from a global community of developers, leading to constant improvements and innovation.[13]

[10] Id.
[11] Josh Lerner, Jean Tirole, The Economics of Technology Sharing: Open Source and Beyond 19 *JEP* 90-120 (2005).
[12] Id.
[13] Id.

3. Customization and Flexibility:

Open source tools are highly customizable, enabling investigators to tailor them to meet specific requirements and challenges posed by diverse cybercrime scenarios. This flexibility ensures that digital forensic professionals can adapt the tools to suit the unique characteristics of each case, from data recovery to malware analysis.[14]

4. Global Community Support:

Many open source forensics tools have active user communities that provide support, updates, and additional plugins or extensions. This collective knowledge and assistance are invaluable when encountering complex forensic challenges, allowing investigators to tap into a wealth of expertise from around the world.

5. Preservation of Digital Evidence:

Open source tools are designed with a focus on preserving the integrity of digital evidence. They employ validated and documented methods to ensure that evidence collected using these tools is admissible in court, adhering to chain of custody and forensic best practices.[15]

6. Cross-Platform Compatibility:

Open source tools are often developed to work on multiple operating systems, ensuring compatibility with a wide range of devices and platforms encountered during investigations. This cross-platform support enables investigators to tackle cases involving diverse technology ecosystems.[16]

7. Educational Resource:

Open source tools are widely used in educational programs and training for digital forensics professionals. They provide hands-on experience and help train the next generation of cyber investigators, further strengthening the field.[17]

[14] Id.

[15] Ratan Lal & Dhiraj Lal, The Law of Evidence (Lexis Nexis, Delhi, 2017)

[16] Abhinav Prakash, Law of Evidence (Universal Law Publishing Co. Pvt. Ltd., Delhi, 2019)

[17] *Supra note 11 at 8*

4. CHALLENGES AND POTENTIAL VULNERABILITIES ASSOCIATED WITH OPEN SOURCE TOOLS

While open source tools offer numerous advantages in cyber forensic investigations, it's crucial to recognize that they are not without challenges and potential vulnerabilities. As with any technology, there are considerations and risks that digital forensic professionals should be aware of when utilizing open source tools in their investigations.[18] In this discussion, we will explore some of the key challenges and vulnerabilities associated with open source tools in the context of cyber forensics, including issues related to quality control, support, security, and legal considerations.

1. Quality Control and Reliability:

One of the challenges with open source tools is the variable quality control and reliability. Since these tools are often developed by a diverse community of volunteers, the level of rigor in testing and development may vary. As a result, some open source tools may not be as stable or reliable as their commercial counterparts, potentially leading to inaccuracies in forensic analysis.[19]

2. Limited Support:

While open source tools often have active user communities, the level of support may not always be as robust as what is available for commercial software. This can pose challenges when investigators encounter complex or unique forensic scenarios and require timely assistance or bug fixes.[20]

3. Security Risks:

Open source tools, like any software, can be susceptible to security vulnerabilities. If these vulnerabilities are not promptly identified and patched, they can be exploited by malicious actors. This poses a risk both to the integrity of the forensic analysis and to the security of the investigator's own systems.[21]

[18] Bianna E. Ine, Hidden in Plain Sight: The Ever-Increasing Use of Open Source Intelligence 29 *AIJ* 141-144 (2011).

[19] Theodora Vardouli, Leah Buechley Leonardo, Open Source Architecture: An Exploration of Source Code and Access in Architectural Design *Leonardo*, 47 *MIT* 51-55 (2014)

[20] P. Cortes "A European Legal Perspective on Consumer Online Dispute Resolution'' 15 *CTLR* 90-100 (2009)

[21] Id.

4. Lack of Documentation:

Some open source tools may lack comprehensive documentation, making it challenging for users, especially those new to the tool, to understand its features and functionalities.

Insufficient documentation can hinder the effective use of the tool and result in suboptimal forensic processes.[22]

5. Legal and Licensing Issues:

Open source tools may be subject to various licensing agreements, some of which could have legal implications if not properly understood and followed. Failure to comply with licensing requirements may lead to legal issues that affect the admissibility of evidence in court.[23]

6. Limited Features and Integration:

In certain cases, open source tools may lack advanced features or seamless integration with other forensic software or platforms. This can necessitate additional effort and workaround solutions to achieve desired results, potentially impacting efficiency.[24]

7. Versioning and Compatibility:

Compatibility issues can arise when open source tools are updated or when they interact with different operating systems or hardware configurations. Ensuring that the tools remain up-to-date and compatible with the latest technologies can be a time-consuming challenge.[25]

5. EVIDENTIARY VALUE OF DIGITAL EVIDENCE

In today's increasingly digitized world, the evidentiary value of digital evidence has become a cornerstone of modern investigations and legal proceedings. From cybercrimes and data breaches to financial fraud and intellectual property disputes, digital evidence plays a pivotal role in uncovering the truth, establishing culpability, and delivering justice. This chapter delves into the multifaceted nature of digital evidence, examining its legal framework, admissibility in court, the role of expert

[22] Id.

[23] *Supra at 21*

[24] *Supra note 15 at 9*

[25] Id at 21

testimony, and the critical importance of maintaining a secure chain of custody.[26]

- **Legal Framework Dealing with Digital Evidence**

To ensure the proper handling and utilization of digital evidence, a comprehensive legal framework has been established in many jurisdictions. These legal regulations address issues such as the collection, preservation, and presentation of digital evidence. Understanding the nuances of these laws and regulations is crucial for investigators and legal professionals to navigate the complexities of digital evidence in accordance with legal standards.

In India, the legal framework dealing with digital evidence primarily revolves around the Information Technology Act, 2000, and the Indian Evidence Act, 1872. These laws provide guidelines and regulations regarding the admissibility and treatment of digital evidence in legal proceedings. Here are the key provisions related to digital evidence under these acts:

1. Information Technology Act, 2000

The Act talks about Admissibility of Electronic Records. The Act deals specifically with the admissibility of electronic records as evidence in court. It outlines the conditions that electronic records must meet to be considered admissible.[27] According to Section 65B, electronic records, including computer-generated documents, emails, and digital images, are admissible in court if the following conditions are met:

- The electronic record must be produced by the computer during the regular course of operations.
- The information contained in the electronic record must be stored on a computer or any other device capable of storing such information.
- The electronic record must be produced using the appropriate technology that ensures its accuracy.

In addition the Act also provides 'Protection of action taken in good faith'.[28] The Act provides

[26] Id at 27
[27] The Information Technology Act, 2000 (Act 21 of 2000), s. 65B
[28] The Information Technology Act, 2000 (Act 21 of 2000), s. 85

protection to government officials and law enforcement agencies who seize, retain, or handle digital evidence in good faith during investigations. It shields them from legal actions related to any damage or loss of data that may occur during the process.

2. Indian Evidence Act, 1872:

Interpretation Clause defines various terms used in the Indian Evidence Act,[29] including "document." In modern legal practice, digital records, emails, and other forms of electronic evidence are considered "documents" under this act.[30]

The Act deals with Opinion of Examiner of Electronic Evidence under Section 45A. This section allows for the opinion of an examiner of electronic evidence to be admitted as evidence. If a court deems it necessary to have the opinion of an expert to prove the authenticity or integrity of digital evidence, the opinion of such an expert can be considered by the court.[31]

It's important to note that the admissibility of digital evidence in India is subject to strict compliance with the provisions of Section 65B of the Information Technology Act, which sets specific requirements for electronic records to be considered admissible. Failure to meet these requirements can lead to the exclusion of digital evidence from legal proceedings.[32]

Additionally, other relevant laws and regulations may apply depending on the nature of the case and the specific type of digital evidence involved, such as the Indian Penal Code (IPC) for cybercrimes and the Code of Criminal Procedure (CrPC) for procedural matters related to investigations and trials. Legal practitioners and digital forensic experts must carefully navigate these legal provisions to ensure the admissibility and reliability of digital evidence in Indian courts.

- **Admissibility of digital evidence in court** - It is subject to several rules and principles, including rules of authenticity, hearsay, and best evidence. In India, these principles are primarily governed by the Information Technology Act, 2000, and the Indian Evidence Act,

[29] Indian Evidence Act, 1872 (Act no 1 of 1872) s.3
[30] Indian Evidence Act, 1872 (Act no 1 of 1872) s. 65B
[31] Indian Evidence Act, 1872 (Act no 1 of 1872) s. 45A
[32] Id at 30

1872. Here's an elaboration of each of these principles along with relevant provisions in Indian law:

1. Rules of Authenticity:

Principle of Authenticity ensures that digital evidence accurately represents the events or information it purports to depict. To be admissible, digital evidence must be proven to be genuine and unaltered.[33]

- **Relevant Provisions in India:**

Section 65B of the Information Technology Act, 2000 outlines the conditions that electronic records must meet to be considered authentic and admissible. It requires that electronic records be produced by a computer during the regular course of operations, stored on a computer or another device, and produced using appropriate technology to ensure accuracy.[34]

2. Hearsay:

Principle of Hearsay is a rule of evidence that generally prohibits the introduction of statements made by individuals not testifying in court. This rule is relevant when dealing with digital evidence such as emails, text messages, or social media posts that contain statements made by third parties.[35]

Relevant Provisions in India:

Section 65B(4) of the Information Technology Act, 2000 addresses the issue of hearsay in digital evidence by allowing for the admissibility of statements contained in electronic records if they are produced as evidence in a court proceeding. It essentially creates an exception to the hearsay rule for electronic records.[36]

3. Best Evidence:

Principle of Best Evidence Rule requires that the most reliable and original form of evidence be presented in court whenever possible. This principle aims to prevent the introduction of secondary or inferior evidence, such as copies, when the original is available.

[33] Supra note 20 at 10

[34] *Supra at 30*

[35] *Supra at 31*

[36] Id at 30

Relevant Provisions in India:

Section 65B (1) of the Information Technology Act, 2000 emphasizes the importance of the best evidence in the context of electronic records. It specifies that an electronic record should be presented in its original form to establish its authenticity and admissibility. Copies may be admissible if they satisfy the conditions outlined in Section 65B.[37]

- **Role of expert testimony in establishing the reliability of digital evidence**

The role of expert testimony in establishing the reliability of digital evidence is crucial in legal proceedings. Digital forensic experts play a pivotal role in explaining and validating digital evidence, ensuring that it is correctly interpreted, and providing assurance of its authenticity and integrity.

Indian Evidence Act, 1872 mentioned that the opinion of an examiner of electronic evidence to be admitted as evidence.[38] If a court deems it necessary to have the opinion of an expert to prove the authenticity or integrity of digital evidence, the opinion of such an expert can be considered by the court.[39] In addition, the court may accept the expert's opinion without examining the expert personally if the expert's testimony is in the form of an affidavit.[40]

Section 65B of the Information Technology Act, 2000: While not directly related to expert testimony, this section outlines the conditions that electronic records must meet to be considered admissible. Digital forensic experts often play a role in ensuring that electronic records meet these conditions and can provide testimony to support their admissibility.[41]

Section 65B(4): This subsection specifically mentions that any information contained in an electronic record that is printed on a paper, stored, recorded, or copied in optical or magnetic media must be accompanied by an affidavit of a person who is in charge of maintaining the record. This affidavit can be provided by a digital forensic expert.[42]

[37] Id at 30

[38] Indian Evidence Act, 1872 (Act 1 of 1872), s. 45A

[39] *Supra at 30*

[40] *Supra at 30*

[41] Id. at 31

[42] *Supra at 30*

- **Chain of custody issues: maintaining the reliability and credibility of digital evidence.** Chain of custody issues are of paramount importance in maintaining the reliability and credibility of digital evidence in legal proceedings.[43] The term "chain of custody" refers to the recorded and time-stamped history of how physical and digital evidence was handled, controlled, and transferred from the time it was first gathered until it was presented in court. To prove that the evidence hasn't been tampered with, changed, or compromised in any way during the investigation, the chain of custody must be properly maintained. Here's an explanation of the significance of chain of custody issues in digital forensics:
- **Preservation of Integrity:** The chain of custody is a critical safeguard for ensuring the integrity of digital evidence. It establishes a clear and documented trail that can be followed from the moment evidence is collected to its introduction in court. This trail helps prove that the evidence presented in court is the same as what was originally collected and that it has not been tampered with.[44]

  Admissibility in Court: Without a properly maintained chain of custody, digital evidence may be challenged for its authenticity and credibility in court. To ensure admissibility, courts require that evidence be handled and stored in a secure and controlled manner throughout its lifecycle. A break in the chain of custody can result in the evidence being excluded from legal proceedings.
- **Establishing Trustworthiness**: Maintaining the chain of custody builds trust in the reliability of digital evidence. It provides a record of who had custody of the evidence, when and how it was handled, and under what conditions. This transparency is essential for demonstrating that the evidence was not subject to unauthorized access, alterations, or contamination.[45]
- **Accountability and Accountability**: The chain of custody holds individuals and organizations accountable for the handling of digital evidence. Those involved in the collection, storage, and analysis of digital evidence must document their actions and adhere to established protocols. Any deviations or breaches of custody can be identified and addressed through the chain of custody documentation.[46]

[43] J. Hoinle, Online Dispute Resolution: The Emperor's New Clothes, 17 *IRLCT* 27 (2003)

[44] Orin S. Kerr, Digital Evidence and the New Criminal Procedure 105 *CLR* 279-318 (2005)

[45] A Davison, *The Law of Electronic Commerce* (Cambridge University Press, England, 2009)

[46] Shrier D, Canale, G Pentland A, *Mobile Money & Payments: Technology Trends* (Massachusetts Institutes of Technology Connection Science & Engineering; Cambridge, USA, 2016)

- **Legal and Ethical Standards**: Properly maintained chain of custody practices are consistent with legal and ethical standards in digital forensics. They align with the principles of due process and the right to a fair trial. Courts rely on the integrity of the chain of custody to ensure that evidence is not manipulated or fabricated.[47]
- **Chain of Custody Documentation:** Chain of custody documentation typically includes details such as the date and time of evidence collection, the names and signatures of individuals involved, a description of the evidence, and any transfers or changes in custody. Digital evidence may also include information about forensic analysis, storage conditions, and any security measures implemented.[48]

6. CASE STUDIES

1**. United States - *United States* v. *Jones*,**[49]

Facts: The case involved the use of a GPS tracking device by law enforcement to monitor a suspect's movements without a warrant. The device was attached to the suspect's vehicle.

Issue: The primary issue was whether the warrantless use of a GPS tracking device violated the Fourth Amendment's protection against unreasonable searches and seizures.

Decision: The Supreme Court of the United States ruled that attaching a GPS tracking device to a vehicle and monitoring its movements without a warrant constituted an unlawful search under the Fourth Amendment. This decision established that digital evidence obtained through warrantless GPS tracking could be excluded from court proceedings.

2. **United Kingdom - *R* v. *T*,**[50]

Facts: In this case, the defendant was accused of possessing indecent images of children on his computer. The prosecution relied on digital evidence recovered from the defendant's computer.

Issue: The main issue was whether the digital evidence obtained from the defendant's computer was admissible in court and whether it could be proven to be authentic and unaltered.

[47] Frank Sylvio Gahapa Talom & Robertson Khan Tengeh, *The Impact of Mobile Money on the Financial Performance of the SMEs in Douala, Cameroon* (Journal of Bank Management, Finance and Sustainability, India 2019)

[48] Digital Business in Belgium, *available at*: https://ca.practicallaw.thomsonreuters.com/1-620-2591?transitionType=Default&contextData=(sc.Default) (last visited on Sept 08, 2023)

[49] 2012 US 457 SC

[50] 2009 UK 732 OB

Decision: The court accepted the digital evidence after expert testimony established the authenticity and integrity of the images. This case highlighted the importance of expert testimony in establishing the reliability of digital evidence.

3. **Canada - *R* v. *Vu*,**[51]

Facts: The case involved the search of a suspect's residence, where police seized computer hard drives containing digital evidence. The suspect argued that the search violated his Charter rights.

Issue: The primary issue was whether the search and seizure of digital evidence violated the suspect's right to be protected against unreasonable search and seizure under the Canadian Charter of Rights and Freedoms.

Decision: The Supreme Court of Canada held that the search and seizure of digital evidence were unreasonable because the police failed to properly catalog and secure the seized items. This case emphasized the importance of maintaining the chain of custody for digital evidence.

4. **Australia - *R* v. *Lawrence*.**[52]

Facts: In this case, the defendant was charged with hacking into computer systems and stealing sensitive information. The prosecution relied on digital evidence recovered from the defendant's computer.

Issue: The main issue was whether the digital evidence obtained from the defendant's computer was admissible and whether it was sufficient to establish the defendant's guilt.

Decision: The court admitted the digital evidence, and the defendant was convicted based on the digital evidence and other circumstantial evidence. This case underscored the significance of digital evidence in prosecuting cybercrimes.

5. India

- ***Anvar P.V.* v. *P.K. Basheer & Others*,**[53]

Facts: In this case, the petitioner sought to admit electronic evidence, particularly electronic records, in a civil case. The electronic evidence in question included printouts of certain email communications

[51] CA 2013 SC 247
[52] 2014 AU (357) SC
[53] 2014 SCC Online 254

and computer-generated records. The petitioner argued that these electronic records should be admissible as evidence.

Issue: The primary issue in this case was whether electronic records, specifically email communications and computer-generated records, could be admitted as evidence in a civil case in India.

Decision: The landmark judgment provided significant guidance on the admissibility of electronic evidence in India. The court held that electronic records could be admitted according to the rules of Section 65B of the Indian Evidence Act, 1872, which addresses the admission of electronic records, the court determined that electronic records might be admitted as evidence.

Key points from the decision:

- The court emphasised the need of adhering to Section 65B's obligations, which include having some body in a position of responsibility for the operation of the relevant equipment or computer certify electronic documents.
- The court ruled that the certification required under Section 65B (4) should be done at the time of producing the electronic evidence in court.
- The judgement made it clear that electronic evidence would not be accepted if Section 65B standards were not met, and the party seeking to rely on such evidence would face its exclusion.

- ***Shafhi Mohammad* v. *State of Himachal Pradesh,***[54]

Facts: The case involved the seizure of a mobile phone from the accused during a narcotics investigation. The prosecution relied on call records and text messages extracted from the mobile phone as digital evidence.

Issue: The key issue was whether the call records and text messages obtained from the mobile phone were admissible in court.

Decision: The Court held that call records and text messages extracted from a mobile phone were admissible as secondary evidence under Section 63 and Section 65 of the Indian Evidence Act. The court emphasized the importance of following proper procedure and ensuring the integrity of digital evidence.

[54] 2018 SCC Online 355

7. SUGGESTION AND CONCLUSION

There are few suggestions regarding the topic

1. Proper training and education as open source tool is an evolving field. So that professionals, experts become more potential in using this tool in cyber forensic.
2. Standardization and certification is required to ensure proper and high- quality investigation.
3. Continued research and development is required for proper development and use of open source tool in cyber forensic investigation.
4. Collaboration with legal experts
5. Formulate the guidelines for using open source tool to maintain data privacy.

- ## Conclusion

Open source tools have emerged as invaluable assets in the realm of cyber forensic investigations, significantly enhancing the evidentiary value of digital findings in legal proceedings. As we move forward, embracing these tools, fostering collaboration, and continually improving their capabilities will be essential in the ongoing battle against cybercrime and the pursuit of digital justice

The benefits are undeniable. Open-source tools offer cost-effectiveness, accessibility, and a rich ecosystem of constantly evolving resources that empower investigators to stay at the forefront of digital crime detection and mitigation. They provide the necessary transparency and trustworthiness required in forensic work, fostering greater confidence in the integrity of digital evidence.

Additionally, open-source solutions offer versatility, customization, and interoperability across a range of operating platforms, allowing them to easily adapt to the ever changing digital scene. Hey enable investigators to scale their resources and expertise in accordance with the complexity of the case at hand, resulting in more efficient and accurate investigations.

In the courtroom, the evidentiary value of open-source tools cannot be overstated. Their transparent and openly accessible nature enhances their credibility, making it easier for forensic experts to explain their methodologies and findings to judges and juries. This transparency also serves as a safeguard against challenges to the admissibility of digital evidence.

8. REFERENCES

- **Books**

- Ratan Lal & Dhiraj Lal, The Law of Evidence (Lexis Nexis, Delhi, 2017)
- Abhinav Prakash, Law of Evidence (Universal Law Publishing Co. Pvt. Ltd., Delhi, 2019)

- **Journal/ Articles**

- John Perry Barlow, A Declaration of the Independence of Cyberspace, 18 DLTR 5-7 (2019)
- V Nagaraju, L Fiondella, T Wandji, An Open-Source Tool to Support the Quantitative Assessment of Cyber Security for Software Intensive System Acquisition, 16 JIW 31-50 (2017)
- Altay Aksulu, A Comprehensive Review and Synthesis of Open Source Research, 11 JAIS 576-656 (2010)
- Stephen Mason, Andrew Sheldon, Hein Dries, Proof: the technical collection and examination of electronic evidence 9 ULP (2017)
- Bianna E. Ine, Hidden in Plain Sight: The Ever-Increasing Use of Open Source Intelligence 29 AIJ 141-144 (2011).
- Theodora Vardouli, Leah Buechley Leonardo, Open Source Architecture: An Exploration of Source Code and Access in Architectural Design Leonardo, 47 MIT 51-55 (2014)
- P. Cortes "A European Legal Perspective on Consumer Online Dispute Resolution'' 15 CTLR 90-100 (2009)
- J. Hoinle, Online Dispute Resolution: The Emperor's New Clothes, 17 IRLCT 27 (2003)
- Orin S. Kerr, Digital Evidence and the New Criminal Procedure 105 CLR 279-318 (2005)

- **Websites**

- https://ca.practicallaw.thomsonreuters.com/1-620-
- https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm