

# International Symposium on Cybersecurity & Forensics



9<sup>th</sup> April 2026 10:00 Hrs. – 17:00 Hrs. IST

**Theme:** Trends & Challenges in  
Cybersecurity, Cyber Law & Forensics

## Abstract Book

📍 I-2 Moot Court, Amity University Campus, Sector-125, Noida (New Delhi/NCR), India

🌐 Registration Link: <https://amity.edu/eventspg/noida/ISCSF2026/>

Sponsored by:



Knowledge Partners:



Industry Partners:



Publication Partners:



Media Partners:



<b>Sl.No.</b>	<b>Contents</b>
<b>1.</b>	<b>About Amity University</b>
<b>2.</b>	<b>About AIFS</b>
<b>3.</b>	<b>About Symposium</b>
<b>4.</b>	<b>Message from Vice-Chancellor</b>
<b>5.</b>	<b>Message from Additional Pro Vice-Chancellor</b>
<b>6.</b>	<b>Message from Chief Guest</b>
<b>7.</b>	<b>Message from Chairperson</b>
<b>8.</b>	<b>Message from Organizing Chair</b>
<b>9.</b>	<b>Abstracts</b>



**AMITY UNIVERSITY**  
UTTAR PRADESH



## **ABOUT AMITY UNIVERSITY**

Amity University Uttar Pradesh is part of Amity Education Group which has been sponsored and promoted by Ritnand Balved Education Foundation (RBEF) has over 2,50,000 students studying across over 2000 acres of hi-tech campuses. Today Amity Education Group has 12 Universities, 28 schools and pre-schools, 13 global Campuses Over 2600 patents are filed by the Faculty, Scientists and Researchers. The faculty has 500+ collaborative funded projects from Government, Industry and International agencies. Amity Group has 8000+ Faculty including eminent Scientists with diverse disciplines. The 81 faculty of Amity Group are featured in the list of top 2% scientists in the world published by researchers of Stanford University for the Academic Year 2024-25. Amity University Uttar Pradesh has been accredited by WASC Senior College and University Commission (WSCUC), USA and Quality Assurance Agency for Higher Education (QAA), UK. Amity University Uttar Pradesh has been ranked 183 amongst the top Universities in ASIA by QS with QS (World) Ranking of 951-1000. The university Times Higher Education (THE) ranking THE (Asia) is 251-300 and THE (World) is 601-800. The NIRF University ranking of Amity University Uttar Pradesh in the year 2025 is 22 with NIRF Research ranking of 38 and NIRF Pharmacy ranking of 18 respectively.



**AMITY UNIVERSITY**  
UTTAR PRADESH



## **About Amity Institute of Forensic Sciences**

Amity Institute of Forensic Sciences, Amity University Uttar Pradesh, Noida, India is a leading premier institute dedicated to nation service. It offers higher education in forensic sciences at three programmes levels: UG- B.Sc. (Forensic Sciences) (Honours / Research), PG- M.Sc. (Forensic Sciences) & M.Sc. (Cyber Forensic & Cyber Security) and Doctorate- Ph.D. (Forensic Sciences) in Full Time and Part Time. All the courses aim to instil in student's professional acumen, skills and capabilities to deal with different areas of life.

Amity Institute of Forensic Sciences is an institute of Amity University came into existence by an act under the Amity University (Uttar Pradesh) Act, 2005 and it has also been listed under 'Educational Institutions' in the U.P. Govt. website (<http://www.upgov.nic.in/>). Its main aim is to conduct important professional courses that can ensure employment to passing-out students. In addition, several short-term training and capacity building programmes are being offered by the institute. The institute has organized National and International conferences, workshops, seminars, faculty development programs, refresher courses, value added courses and quiz competitions



AMITY UNIVERSITY  
UTTAR PRADESH



## ABOUT SYMPOSIUM (ISCSF - 2026)

The rapid digitization of society has brought unparalleled advancements in technology, connectivity, and access to information. However, these benefits come with an increasing prevalence of cyber threats, cybercrimes, and sophisticated attacks targeting individuals, organizations, and governments. In this digital age, cybersecurity, cyber law, and forensics play a pivotal role in safeguarding critical infrastructure, ensuring privacy, and maintaining the rule of law in society and cyberspace.

The International Symposium on Cybersecurity & Forensics aims to provide a multidisciplinary platform for professionals, researchers, academicians, policymakers, and industry experts to discuss cutting-edge developments, emerging trends, and pressing challenges within the fields of cybersecurity, cyber law, and forensics. Under the theme "*Trends & Challenges in Cybersecurity, Cyber Law & Forensics*", the symposium will facilitate thought-provoking discussions and foster collaboration to address these global issues effectively.

This symposium aligns with the goals of the United Nations Department of Economic and Social Affairs (UNDESA) and integrates principles of the Sustainable Development Goals (SDGs) specifically:

- SDG 4 (Quality Education): By fostering knowledge-sharing, capacity-building, and skill development in cybersecurity and forensics.
- SDG 8 (Decent Work and Economic Growth): By exploring robust cybersecurity frameworks to enhance digital economies and create safe digital workspaces.
- SDG 9 (Industry, Innovation, and Infrastructure): By emphasizing innovative solutions and resilient cyber infrastructures critical for advancing digital economies.
- SDG 11 (Sustainable Cities and Communities): By addressing the role of cybersecurity in building smart, sustainable, and secure urban ecosystems.

## MESSAGE FROM THE VICE-CHANCELLOR



### **Prof. (Dr.) Balvinder Shukla**

Professor of Entrepreneurship, Leadership & IT  
Vice Chancellor, Amity University Uttar Pradesh

It is a pleasure to welcome all distinguished speakers, delegates, academicians, researchers, professionals, and students to the “*International Symposium on Cybersecurity & Forensics (ISCSF 2026)*” organized on 9<sup>th</sup> April 2026 at Amity University Uttar Pradesh, Noida.

Today technological advancements have transformed the way we live and interact, while simultaneously giving rise to complex cyber threats and security challenges. The increasing incidence of cybercrimes, data breaches, and sophisticated digital attacks highlights the critical need for robust cybersecurity frameworks, well-defined cyber laws, and advanced forensic methodologies.

The theme of the symposium, “Trends & Challenges in Cybersecurity, Cyber Law & Forensics,” emphasizes the importance of a multidisciplinary approach in addressing the growing complexities of cyber threats. As emerging technologies continue to reshape the digital ecosystem, there is a need for collaboration among researchers, practitioners, and policymakers to develop effective strategies that ensure security, accountability, and justice.

This symposium provides a valuable platform for knowledge-sharing, critical discussions, and exchange of innovative ideas. It also aligns with broader global priorities by promoting quality education, encouraging innovation, and supporting the development of secure and sustainable digital environments. The contributions compiled in this abstract book reflect the depth of ongoing research and the growing importance of interdisciplinary engagement in these areas.

At Amity University, we are passionate about academic excellence and cutting-edge research that addresses contemporary challenges. Our Founder President, Dr. Ashok Chauhan, dreamed of empowering youth to lead nation-building with innovation and agility. This symposium embodies that vision, bringing people together to collaborate and make a difference.

I extend my sincere appreciation to the organizing committee of Amity Institute of Forensic Sciences for their efforts in bringing together such a diverse and accomplished gathering. I am confident that the contributions presented in this abstract book will provide valuable insights and inspire further research in the fields of cybersecurity, cyber law, and forensic science.

My best wishes to all participants for a productive and enriching experience.

## MESSAGE FROM ADDITIONAL PRO VICE-CHANCELLOR



**Prof. Chanderdeep Tandon**  
Additional Pro Vice Chancellor  
Amity University Uttar Pradesh, India

It is truly encouraging to see such a diverse and thoughtful gathering come together for the *International Symposium on Cybersecurity & Forensics (ISCSF-2026)* at Amity University, Noida.

What stands out today is not just the advancement of technology, but the pace at which it is reshaping our everyday decisions, behaviours, and systems. In many ways, we are still learning how to respond to the consequences of this rapid transformation. Cybersecurity concerns, questions around digital rights, and the challenges of interpreting complex digital evidence are no longer limited to specialists, they are becoming part of a larger societal conversation.

This is where forums like ISCSF become especially meaningful. They give us the opportunity to pause, reflect, and engage with ideas beyond our immediate domains. Often, the most effective solutions emerge not from isolated expertise, but from conversations that bring together different perspectives, technical, legal, and investigative.

I believe this symposium is as much about listening as it is about presenting. It is about understanding how different sectors are approaching similar problems, and where we can learn from one another. Such exchanges are essential if we are to keep pace with challenges that do not follow conventional boundaries.

I am particularly pleased to see the participation of students and early-career researchers. Their engagement is important, as the future of these fields will depend on their ability to think critically, adapt quickly, and work collaboratively. This volume also reflects the active involvement of emerging scholars alongside experienced researchers, indicating a growing academic interest in these critical areas. Encouraging such participation is important for sustaining innovation and ensuring continuity in the development of knowledge.

I would like to acknowledge the efforts of the organizing team in creating this platform. Bringing together such a wide range of participants is no small task, and it reflects careful thought and commitment.

I hope that the time spent here leads not only to new knowledge, but also to meaningful connections and continued dialogue beyond the symposium.

My best wishes to all of you for a rewarding and engaging experience.

## MESSAGE FROM THE CHIEF GUEST

**माँ शाकुम्भरी विश्वविद्यालय**

पुवॉरका, सहारनपुर, उत्तर प्रदेश-247120

**प्रो० विमला वाई.**

कुलपति



**MAA SHAKUMBHARI UNIVERSITY**

Punwarka, Saharanpur, Uttar Pradesh - 247120

**Prof. Vimala Y.**

Vice - Chancellor

Mob.: 9411905180, 9258105950 | E-mail: vc@msuniversity.ac.in | G-mail : vc.maashakumbhariuniversity@gmail.com

क्रमांक : Y.CO/04/05/2026-27

दिनांक : 08/04/2026

## MESSAGE

It gives me immense pleasure to learn that the *Amity Institute of Forensic Sciences, Amity University, Uttar Pradesh, Noida* is publishing the *Abstract Book* of the *International Symposium on Cybersecurity & Forensics (ISCSF-2026)*, centered on the theme “*Trends & Challenges in Cybersecurity, Cyber Law & Forensics.*”

In the contemporary digital era, cybersecurity and forensic science have emerged as critical pillars for safeguarding data integrity, privacy, and national security. The increasing sophistication of cyber threats necessitates a robust framework of research, innovation, and interdisciplinary collaboration. In this context, **ISCSF-2026** serves as a significant academic platform for deliberations on emerging challenges and technological advancements in the field.

The *Abstract Book* is a valuable compendium of scholarly work, reflecting diverse research perspectives and innovative approaches contributed by academicians, researchers, and practitioners. I am confident that this publication will not only enrich academic discourse but also provide meaningful insights for policy formulation and practical applications in cybersecurity and forensic investigations.

I commend the dedicated efforts of the organizing committee, *Amity Institute of Forensic Sciences*, and *Amity University Uttar Pradesh, Noida*, for successfully bringing together eminent experts and scholars on this important platform.

I extend my best wishes for the success of the symposium and hope that such initiatives will continue to foster knowledge creation and academic excellence.



(Prof. Vimala Y.)  
Vice-Chancellor

## MESSAGE FROM CHAIRPERSON



**Prof. (Dr.) Sunita Rattan**

*Chairperson, ISCSF-2026*

*Dean, Science & Technology, AUUP*

*Director, Amity Institute of Applied Sciences*

*Amity University, Uttar Pradesh, Noida*

It is my great pleasure to welcome all the delegates, distinguished speakers, academicians, researchers, and industry professionals to the International Symposium on Cybersecurity & Forensics (ISCSF 2026) organised by Amity Institute of Forensic Sciences, at Amity University Uttar Pradesh, Noida.

The programme has been carefully structured to include plenary and keynote lectures, invited talks, technical sessions, poster presentations, reflecting contemporary research trends and addressing pressing global challenges in Cyber Security.

ISCSF-2026 aims to foster meaningful academic interactions, encourage young researchers, and facilitate the development of long-term collaborations that contribute to scientific advancement and technological innovation. I am confident that the deliberations during the symposium will be intellectually stimulating and mutually enriching for all participants.

The Organising Committee expresses its profound gratitude to the Hon'ble Founder President Sir for his visionary leadership and invaluable guidance. We also sincerely acknowledge the Hon'ble Chancellor Sir for his dynamic leadership and respected Vice-Chancellor Madam for her unwavering support, which has been pivotal to the successful organisation of ISCSF-2026.

I wish the Symposium, a grand success and hope that all participants have a rewarding and memorable experience.

## MESSAGE FROM ORGANIZING CHAIR



**Dr. Amarnath Mishra**, (*M.Sc., M.Phil., Ph.D., LL.M.*)  
Associate Professor  
Amity Institute of Forensic Sciences,  
Amity University Uttar Pradesh, Noida, India

It is our great pleasure to welcome you to the International Symposium on Cybersecurity & Forensics (ISCSF - 2026), centred on the theme “*Trends & Challenges in Cybersecurity, Cyber Law & Forensics*”.

This international platform brings together eminent academicians, researchers, forensic experts, legal professionals, and industry experts to foster meaningful dialogue and exchange pioneering ideas. As forensic science continues to evolve rapidly, its integration with national security and legal frameworks has become increasingly critical in addressing modern-day challenges.

ISCSF-2026 aims to highlight cutting-edge research, innovative methodologies, and emerging trends that are shaping the future of forensic investigations and security strategies. The symposium will serve as a hub for interdisciplinary collaboration, encouraging participants to explore new perspectives and develop impactful solutions.

We extend our sincere appreciation to all distinguished speakers, contributors, and participants whose involvement make this event truly significant. We also acknowledge the dedicated efforts of the organizing committee and supporting institutions for their commitment to excellence.

We hope this gathering ignites fruitful discussions, inspires new research directions, and strengthens collaborations in forensic sciences and cyber security. Wishing you all a productive and enriching experience.

**PP01**

**Advancements and Challenges in 2D versus 3D Toolmark Analysis: Integrating AI for Enhanced Forensic Reliability**

Lakshya Sood<sup>1</sup>, Suraj Kataria<sup>1</sup>

<sup>1</sup>*National Forensic Sciences University (NFSU), Delhi Campus*  
[soodlakshya5@gmail.com](mailto:soodlakshya5@gmail.com)

**Abstract**

This review addresses emerging trends in forensic physical sciences, highlighting the shift from conventional 2D photographs to advanced 3D imaging techniques for toolmark comparison. While 2D methods offer convenience and widespread use, 3D scanning delivers superior surface topography but encounters limitations such as potential evidence damage from contact scanning, challenges in capturing fine details in sharp or concave regions, and inconsistencies from technology variations, modeling, and processing raising legal admissibility concerns pertinent to cyber law and evidentiary standards.

Recent innovations, including high-resolution structured light scanners, surface profilometry for quantitative 3D texture mapping, and nanoscale-precision interferometric profilers, augmented by machine learning (e.g., support vector machines, multivariate statistics, deep learning on 3D datasets), have achieved low error rates in toolmark-to-source attribution on AI and digital forensics. Standardized protocols like repetitive directional tool movements, programmable stages, uniform substrates, and probabilistic likelihood ratios mitigate variability, enhancing evidentiary strength. Despite these advances, human expertise remains indispensable for interpreting AI outputs, handling partial marks, ensuring accountability, and navigating training biases fostering the symposium's objectives of interdisciplinary collaboration and real-world forensic innovation.

A structured literature search across Google Scholar, PubMed, and ResearchGate identified key studies on methods, advantages, and limitations. This review advocates standardized integration of digital tools, AI analytics, and expert judgment to bolster toolmark evidence credibility, reliability, and court admissibility, contributing to a secure digital and physical forensic ecosystem.

**Keywords:** Toolmark analysis, 3D forensics, AI integration, Forensic standardization, Evidentiary challenges

PP02

**Multi-Element Detection of Heavy Metals in Tobacco Using TMA: An Improved Approach over AAS**

Monika Reddy<sup>1</sup> and A.K Jaiswal<sup>2\*</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Noida*

<sup>2</sup>*Department of Forensic Medicine and Toxicology, AIIMS, New Delhi*

*\*Corresponding Author: [ashokjaiswal72@gmail.com](mailto:ashokjaiswal72@gmail.com)*

**Abstract**

Heavy metal contamination in tobacco products is a growing concern due to the presence of toxic elements such as lead (Pb), cadmium (Cd), nickel (Ni), and arsenic (As), which can pose serious health risks upon long-term exposure. Trace Metal Analysis (TMA) instrumentation has gained attention as an advanced and efficient approach for detecting these metals in complex matrices like tobacco. TMA typically involves systematic sample preparation, including digestion and extraction, followed by multi-element detection using modern analytical platforms. This approach allows simultaneous analysis of multiple metals, providing a comprehensive profile of contamination in a single run.

Compared to conventional techniques, TMA offers several advantages that make it more effective than Atomic Absorption Spectroscopy (AAS) in many applications. While AAS is limited to the detection of one element at a time and requires repeated analysis for multiple metals, TMA-based systems can analyze several elements simultaneously, saving both time and resources. Additionally, TMA instrumentation often demonstrates higher sensitivity, lower detection limits, and improved throughput, making it more suitable for large-scale studies and forensic investigations. It also provides better reproducibility and can handle complex sample matrices with greater efficiency.

Due to these advantages, TMA is increasingly preferred for comprehensive heavy metal assessment in tobacco products. It not only enhances analytical performance but also strengthens forensic interpretation by offering a detailed elemental fingerprint. Therefore, TMA instrumentation represents a more advanced and practical alternative to AAS for modern toxicological and environmental analysis.

**Keywords:** Heavy metals, Multi-element detection, Tobacco Products, AAS



AMITY UNIVERSITY  
UTTAR PRADESH



PP03

## Novel Psychoactive Substances in Forensic Toxicology: Analytical Challenges, Toxicological Effects, and Emerging Trends

Nandini Pounikar<sup>1</sup>, Majji Sai Sudha Rani<sup>1\*</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Uttar Pradesh, India*

*\*Corresponding Author: [mssrani@amity.edu](mailto:mssrani@amity.edu)*

### Abstract

Novel Psychoactive Substances (NPS) currently represent an expanding and developing chemical group of synthetic drugs that are intended to mimic the effects of other traditional psychoactive substances while escaping legal regulation. A review of the existing literature summarized within the excel spreadsheet has demonstrated that the main cause of the rapid emergence of NPS into the illicit drug markets over the past ten years has been the deliberate chemical modification of previously known psychoactive compounds, creating hundreds of new chemical compounds. The main classes of NPS are synthetic cannabinoids, synthetic cathinones, synthetic opioids, designer benzodiazepines, phenethylamines, piperazines, tryptamines and dissociative substances. NPS have been linked to serious and unpredictable adverse health effects, based on findings from toxicological and clinical studies. NPS generally exhibit high pharmacological potency, rapid metabolism and close margins between the recreational and the toxic dose ranges. Most accidents resulting from acute intoxication are related to neuropsychiatric complications, cardiovascular complications, respiratory depression, and death in extreme cases. Co-use of multiple substances is frequently reported and creates additional complexity in the clinical management and forensic interpretation of cases. The analytical detection of NPS remains a significant obstacle to forensic and clinical laboratories, with existing routine immunoassay screening techniques ineffective due to the lack of cross-reactivity with newly modified compounds. Advanced analytical techniques such as Gas Chromatography-Mass Spectrometry, Liquid Chromatography-Tandem Mass Spectrometry, High-Resolution Mass Spectrometry, and non-targeted screening approaches are increasingly relied upon for identification and confirmation. However, the lack of reference standards, limited metabolite data, and absence of standardized analytical protocols restrict early detection and result interpretation. Overall, the literature indicates that research on NPS is largely reactive, with scientific, analytical, and regulatory responses lagging behind rapid market innovation. Addressing these challenges requires integrated forensic intelligence, improved analytical strategies, and coordinated public health surveillance to reduce the harms associated with NPS.

**Keywords:** Novel Psychoactive Substances, Synthetic Drugs, Forensic Toxicology, Analytical Detection, Illicit Drug Synthesis.

**PP04**

**Temperature as a critical determinant of heavy metal migration from Food packaging:  
A Systematic Review of Forensic, Analytical and Public Health Implications**

Tanmay Malik<sup>1</sup>, Sonalika Pandey<sup>1</sup>, Vimal Rarh<sup>2</sup>, Jyoti Singh<sup>1\*</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Uttar Pradesh, India*

<sup>2</sup>*Sri Guru Tegh Bahadur Khalsa College, University of Delhi*

\*Corresponding Author: [jsingh4@amity.edu](mailto:jsingh4@amity.edu)

**Abstract**

Temperature significantly influences how hazardous metal components move from food-contact materials into the food we eat. However, this role is not fully understood or clearly explained in one place. This systematic review focuses solely on temperature. It looks at how temperature, within the normal range during food storage, cooking, and serving, affects the migration of various heavy metals from plastic and paper food-contact materials. We gathered peer-reviewed experimental studies from Scopus, PubMed, and ScienceDirect. Then, we checked each study against set rules for inclusion and exclusion to maintain consistent methods and ensure the papers met our research goals. The overall evidence suggests that temperature is the primary factor accelerating the release of metals. It likely operates through a diffusion process similar to the Arrhenius model. Even a small increase in temperature can lead to a significant rise in metal movement. This trend is observed in many metals, including lead (Pb), cadmium (Cd), chromium (Cr), mercury (Hg), antimony (Sb), aluminum (Al), zinc (Zn), nickel (Ni), and copper (Cu). The forensic aspect of this issue is also important. Element patterns in foods affected by heat can be analyzed using high-resolution spectrometry methods like ICP-MS, ICP-OES, and AAS. These patterns may serve as distinctive markers to help trace the origin of food, understand how contamination occurred, and support legal accountability in food safety investigations.

**Keywords:** Food contact materials; Heavy metal migration; Health risk assessment; Food packaging safety



AMITY UNIVERSITY  
UTTAR PRADESH



PP05

**Toxicogenomic in forensic post-mortem drug toxicity interpretation: advancing molecular presence in cause of death determination**

Shreejita Pal<sup>1</sup>, Rohit Kanojia<sup>1</sup>

<sup>1</sup>*Dept. of Forensic Sciences, National Forensic Sciences University, Delhi Campus (LNJN NICFS)-110085*

*[shreejita23456@gmail.com](mailto:shreejita23456@gmail.com), [rohitkanojia.rk@gmail.com](mailto:rohitkanojia.rk@gmail.com)*

**ABSTRACT:**

Determining the role of drugs in post-mortem cases is often complex and uncertain. After death, biological changes such as post-mortem redistribution, tissue breakdown, and altered metabolism can significantly affect drug concentrations, making interpretation difficult. While conventional techniques like GC-MS and LC-MS are effective in detecting drugs, they do not fully explain how an individual's body responded to the substance before death.

This study is based on a structured review of existing literature from databases such as PubMed and Google Scholar. It focuses on the application of toxicogenomic in forensic toxicology, particularly examining gene expression patterns, genetic polymorphisms, and molecular biomarkers. Special attention is given to variations in drug-metabolizing enzymes, especially the cytochrome P450 (CYP450) system. Techniques such as polymerase chain reaction (PCR) and next-generation sequencing (NGS) are also considered.

The findings suggest that toxicogenomic can provide deeper insight into individual differences in drug metabolism and toxicity. It helps differentiate between therapeutic, toxic, and fatal drug levels, especially in cases involving multiple drugs or unclear toxicological results. Genetic variations were found to play a crucial role in influencing drug response, offering explanations where traditional methods fall short.

Toxicogenomic has strong potential to complement conventional forensic toxicology by adding a molecular perspective to drug toxicity interpretation. Its integration can improve the accuracy of cause-of-death analysis and reduce uncertainty in medico-legal investigations. Although challenges such as cost and lack of standardization remain, it represents a promising direction for the future of forensic science.

**Keywords:** Forensic toxicology, toxicogenomic, pharmacogenomics, post mortem redistribution, molecular autopsy.



AMITY UNIVERSITY  
UTTAR PRADESH



PP06

**Forensic analysis of corrosion: Comparative study of naturally occurring corrosion and accelerated or induced corrosion**

Om Dubey<sup>1</sup>, Priyanka Singh Rawal<sup>1</sup>, Kaushal<sup>2</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Uttar Pradesh, India*

<sup>2</sup>*Forensic Science Laboratory U.P.*

*omdubey.phd@gmail.com*

**Abstract**

Forensic metallurgy houses an important place in forensic science with scope of investigating structural failures and industrial accidents. Since metals are largely used in the infrastructure and machines, they are prone to failure because of several factors. In such instances it is essential to understand the cause of failure. The present study focuses on analysing the behaviour of metal microstructures subjected to natural corrosion processes in comparison with those exposed to induced or accelerated corrosion conditions. Authors have simulated the natural environment and accelerated environmental condition for corrosion to take place on metal pieces. At the end of the treatment metal pieces were observed under the metallurgical microscope and it was found that there were many significant features that could be considered as decision makers to report for natural or induces corrosion. The study holds an immense importance in the judicial and investigative domain.

The study will also help to draft a uniform standard operating procedure for investigating agencies for scene of occurrences which are claimed to be of accident due to corrosion. The present study will also enhance the reliability of expert testimony and support more accurate conclusions. By bridging the gap between materials science and forensic investigation, the research underscores the importance of microstructural analysis as a powerful tool in uncovering the true causes behind material failures.

**Keywords:** Forensic Metallurgy, Induced Corrosion, Structural Failure, Industrial Accident Investigation, Grain Structure Analysis



AMITY UNIVERSITY  
UTTAR PRADESH



PP07

## Advances in Identification and Forensic Profiling of Illegal Chemical Adulterants in Food Products

Dashmeet Kaur

*Lloyd Institute of Forensic Science, Greater Noida, Uttar Pradesh*

[dashmeetkaur146@gmail.com](mailto:dashmeetkaur146@gmail.com)

### Abstract

**Introduction:** Illegal chemical adulteration of food using synthetic dyes is a major food safety and forensic concern, especially in developing countries. Despite regulatory restrictions, unauthorized dyes such as Sudan dyes, Metanil Yellow, Auramine O, and Rhodamine B are frequently added to enhance the visual appeal of food products. These adulterants pose serious health risks, including carcinogenic and neurotoxic effects, and are commonly found in spices, sweets, oils, and street foods in India. Forensic identification of such adulterants is essential for toxicological evaluation and legal investigation.

**Methods:** The study highlights various analytical techniques used for the detection and profiling of illegal food adulterants. Preliminary screening is performed using Thin Layer Chromatography (TLC), High Performance Thin Layer Chromatography (HPTLC), and UV–Visible spectrophotometry. Advanced confirmatory techniques include High Performance Liquid Chromatography (HPLC–UV), Liquid Chromatography–Mass Spectrometry (LC–MS), and LC–MS/MS. Sample preparation methods such as Solid Phase Extraction (SPE) and Liquid Phase Micro–Extraction (LPME) enhance detection sensitivity. Emerging techniques like surface-enhanced Raman spectroscopy and electrochemical sensors are also explored.

**Results:** The integration of chromatographic and spectrometric techniques enables accurate, sensitive, and reliable detection of illegal chemical adulterants. Advanced methods such as LC–MS/MS provide confirmatory and legally defensible results. Emerging rapid detection tools show promising potential for on-site screening and real-time analysis.

**Conclusion:** Early detection and comprehensive forensic profiling of illegal chemical adulterants are crucial for ensuring food safety, supporting regulatory enforcement, and protecting public health. The advancement of analytical technologies significantly strengthens forensic capabilities in food adulteration cases.

**Keywords:** Food adulteration, synthetic dyes, forensic toxicology, Instruments, Recent Advances



AMITY UNIVERSITY  
UTTAR PRADESH



PP08

### **Heavy Metals in Water, Air, and Soil: Human Exposure and Health Risks**

Riya Rai<sup>1</sup>, Shrutika Singla<sup>2</sup>, Tanmay Malik<sup>1</sup>, Sonalika Pandey<sup>1</sup>, Jyoti Singh<sup>1\*</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University Uttar Pradesh, Noida*

<sup>2</sup>*Department of Forensic Science, Institute of Road Traffic Education*

*\*Corresponding Author- [jsingh4@amity.edu](mailto:jsingh4@amity.edu)*

#### **Abstract**

Environmental pollution has become a significant global concern owing to rising industrialisation, urban growth, and anthropogenic activities. Heavy metals (HMs) are some of the most dangerous pollutants because they are toxic, last a long time, and can build up in ecosystems. Exposure to heavy metals like Lead (Pb), Mercury (Hg), Cadmium (Cd), Chromium (Cr), Nickel (Ni), and Arsenic (As) in the environment is a big threat to human health because these metals stay in the environment for a long time, build up in living things, and are toxic on their own. This review compiles contemporary evidence regarding the origins, transmission routes, and health effects of heavy metal exposure in various populations. People are mostly exposed to heavy metals through contaminated water, soil, air, and food. This happens mostly because of mining, industrial processes, and farming. Long-term exposure to heavy metals, whether from the environment or work, has been linked to a number of bad health effects, such as neurodegenerative diseases, heart problems, kidney damage, and developmental delays. Children and pregnant women are more likely to be affected. This review highlights the main causes of heavy metal pollution, shows how they spread through the environment, and looks at the dangers that come with them. It also calls for stronger rules and more environmentally friendly ways to reduce pollution.

**Keywords:** Pollution, heavy metals, heavy metal toxicity, human health, occupational exposure.



AMITY UNIVERSITY  
UTTAR PRADESH



PP09

## A Systematic Review of Nuclear Magnetic Resonance (NMR) Spectroscopy and its Applications in Forensic Science

Silpi Srivastava<sup>1</sup>, Pooja Puri<sup>1\*</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Uttar Pradesh, India*

*\*Corresponding Author- [pmalik1@amity.edu](mailto:pmalik1@amity.edu)*

### Abstract

Nuclear Magnetic Resonance (NMR) spectroscopy is becoming one of the most important analytical platforms in forensic science. No longer viewed as a relatively costly and peripheral technique, NMR is currently emerging as a pillar in forensic chemistry since it offers the only means of unambiguous structural clarification without requiring certified reference standards.

The paper includes several academic and regulatory documents, a multi-disciplinary collection of peer-reviewed articles, international forensic guidelines (ENFSI), and legislative frameworks to offer an overall roadmap to NMR forensic utility. It offers a universal roadmap of the forensic usefulness of NMR in five fundamental domains: identification of illicit drugs, forensic toxicology, estimation of post-mortem interval (PMI), explosive analysis, and detection of food fraud. Among the key findings, quantitative NMR (qNMR) is effective in quantifying the purity of Novel Psychoactive Substances (NPS) and <sup>1</sup>H NMR metabolomics can be used as an objective chemical clock to investigate death.

In addition, the review addresses the recent 'benchtop revolution' noting portable and low field systems are now occupying approximately 30 percent of the recent forensic literature. Even though technical problems of sensitivity thresholds and high costs of maintenance still exist, automated data interpretation through the application of Artificial Intelligence (AI) is making complex casework easier. Finally, the report suggests a hub and spoke structure of forensic laboratories; this entails the centralized high-resolution and field-deployable technology to enhance global investigative intelligence.

**Keywords:** Nuclear Magnetic Resonance, Forensic Chemistry, Novel Psychoactive Substances, Post-Mortem Interval, Benchtop NMR.

**PP10**

**The Changing Face of Chemical Submission: A Systematic Review of Date Rape Drug Trends in Drug-Facilitated Sexual Assault**

Kuldeep Singh<sup>1</sup>, Madhuri Gupta<sup>2</sup>, Shashank Kaushik<sup>1</sup>, Amarnath Mishra<sup>1\*</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, U.P., Noida, India*

<sup>2</sup>*Department of Pharmacology, All India Institute of Medical Sciences, New Delhi, India*

*\*Corresponding Author - [amishra5@amity.edu](mailto:amishra5@amity.edu)*

**Abstract**

**Introduction:** A serious global problem, DFSA is considered public health and forensic issues. DFSA continues to affect an increasing number of victims but the lack of true representation and a consolidated database create challenges for law enforcement, forensic investigators, and public health agencies attempting to conduct accurate trend analysis and retrospective investigative examinations.

**Objectives:** This systematic review aims to identify commonly used and emerging substances, assess their implications for toxicological detection and retrospective case reconstruction, and thoroughly analyse published evidence on trends in the use of date rape drugs in DFSA cases across various time periods and geographic regions. The review also aims to draw attention to a crucial gap in the literature: the notable lack of data from India, where sociocultural stigma, forensic infrastructure constraints, and underreporting have all contributed to a nearly complete lack of systematic toxicological documentation of DFSA cases. This has hindered evidence based clinical, forensic, and policy responses in the Indian context.

**Methods:** Using relevant MeSH terms and Boolean operators, a thorough literature search was carried out throughout PubMed, Scopus, Web of Science, ScienceDirect, and Google Scholar. The PRISMA 2020 guidelines were used to screen the studies. The final qualitative synthesis comprised data from Europe, North America, Asia, and global multicentre analyses from 24 peer-reviewed studies published between 2017 and 2025 out of many initially identified records.

**Results:** Ethanol was the most consistently identified substance across all regions and study periods, either alone or in combination with benzodiazepines, gamma-hydroxybutyrate (GHB), and ketamine. A notable trend in recent studies (2015–2025) was the shift toward poly-drug use and the emergence of novel psychoactive substances, including synthetic cathinones. GC–MS and LC–MS/MS were the predominant analytical techniques; however, rapid drug metabolism, delayed reporting, and limited screening panels remained significant barriers to detection.

Conclusion: DFSA is a sophisticated and evolving challenge. Standardized toxicological protocols, expanded screening panels incorporating novel substances, enhanced clinical awareness, and harmonized global surveillance systems are urgently needed to improve retrospective forensic analysis, victim support, and evidence-based prevention strategies.

**Keywords:** Drug-facilitated sexual assault, Date rape drugs, Benzodiazepines, Gammahydroxybutyrate (GHB), Forensic toxicology, Z-Drugs

## PP11

### **MicroRNA-451: A High-Specificity Biomarker for Human Blood Identification in Forensics**

Misbah Samsami

*Amity University Rajasthan, Jaipur*

*misbahsam1702@gmail.com*

#### **Abstract**

MicroRNA-451 (miR-451) has emerged as a highly specific and stable biomarker for human blood identification in forensic science. As a small non-coding RNA predominantly expressed in erythrocytes, miR-451 plays a crucial role in post-transcriptional gene regulation and demonstrates remarkable resistance to environmental degradation. This study evaluates the applicability of miR-451 for identifying blood in both fresh and aged stains under controlled and real-world conditions.

Blood samples were deposited on filter paper and analyzed over a period of up to 30 days. Total RNA was extracted using a silica-based method, followed by reverse transcription and quantitative real-time PCR (RT-qPCR) targeting miR-451, with U6 snRNA as an internal control. Expression levels were quantified using the  $\Delta C_t$  method to assess stability and detectability over time.

Results indicated strong and consistent expression of miR-451 in all blood samples, while no amplification was observed in other body fluids such as saliva, sweat, semen, or epithelial cells, confirming its high specificity. Although Ct values increased with sample aging, miR-451 remained detectable even in degraded samples up to 30 days old. Environmental exposure caused minor variations in expression but did not compromise detection.

These findings highlight miR-451 as a reliable molecular marker for forensic blood identification, particularly in challenging scenarios involving degraded or trace evidence. Its integration into forensic workflows can enhance accuracy, support evidentiary reliability, and contribute to advancements in molecular forensic investigations.

**Keywords:** MicroRNA-451 (miR-451), Forensic science, Blood identification, Biomarker, Non-coding RNA, RT-qPCR



AMITY UNIVERSITY  
UTTAR PRADESH



PP12

**Molecular Identification of Plant Species for Aiding Wildlife Plant Forensics:  
Integrating DNA Barcoding and Standardized Legal Protocols**

Aastha Dubey<sup>1</sup>, Harsh Kumar Singh<sup>2</sup>, Sapna Sharma<sup>1</sup>, Munish Kumar Mishra<sup>3</sup>

<sup>1</sup>*Department of Forensic Science, Maharshi Dayanand university, Rohtak, Haryana*

<sup>2</sup>*Department of Anthropology, University of Lucknow, Uttar Pradesh*

<sup>3</sup>*Department of Forensic Science, SHUATS, Uttar Pradesh, India*

[dubeyaastha1401@gmail.com](mailto:dubeyaastha1401@gmail.com)

**Abstract**

The escalating global awareness of wildlife crime's detrimental effects on biodiversity underscores the increasing demand for advanced molecular methodologies, particularly DNA testing, to identify species and link forensic samples to specific organisms. Plant wildlife investigation is an indispensable interdisciplinary field that harnesses botanical and molecular techniques to address legal issues involving flora. This approach is essential for enforcing international regulations such as CITES (Convention on International Trade in Endangered Species), which regulates a market where the illegal trade of plant extracts is estimated at approximately 7 billion USD annually, threatening biodiversity and fueling organized crime. India's rich biodiversity faces unique forensic challenges. At its core, DNA barcoding employs standardized genetic regions such as *rbcL*, *matK*, and *ITS2* to deliver precise, unambiguous species identification from challenging samples like sterile tissues, juveniles, or highly processed materials, where morphological methods invariably fail.

**Keywords:** Plant Wildlife forensics, DNA barcoding, species identification, *rbcL*, *matK*, *ITS2*, illegal wildlife trade.



AMITY UNIVERSITY  
UTTAR PRADESH



PP13

## The Impact of Fingerprint Powders on DNA Yield: A Review of Lifting Substrates and Extraction Chemistry

Shaikh Adiba Rizwan<sup>1</sup>, Prince Prajapati<sup>1</sup>

<sup>1</sup>College of Traffic Management & Forensic Science-Institute of Road Traffic Education  
(affiliated to National Forensic Sciences University)

[princeprajapati.andc@gmail.com](mailto:princeprajapati.andc@gmail.com)

### Abstract

In forensic science, trace DNA, often known as "Touch DNA," has become a crucial tool for connecting people to crime scenes through microscopic biological fragments. In order to make a visual match, forensic experts occasionally need to utilise fingerprint powder, but they must balance this against the necessity of obtaining a biological sample for DNA analysis. This review aims to evaluate the impact of different fingerprint powders on the amount of DNA, the extraction chemistry, and the efficiency of different lifting substrates. Based on research published between 2015 and 2025 and utilising 20 important text sources on the ideas of dual recovery techniques, a thorough literature search was conducted.

The research states that most common fingerprint powders may physically eliminate some biological matter by scratching away loosely adhered cells somewhere on the continuum, even if they do not completely destroy DNA in a chemical sense. Additionally, it makes the sample useless. According to comparative investigations of probe-based polypropylene films, carbon-based and non-magnetic powders generally have less of an effect on DNA profiling and are really a better option than magnetic powders. However, magnetic particles, together with high concentrations of iron and titanium, are also more likely to result in PCR "inhibitory" (i.e. inhibit) circumstances and to produce unit contamination through continuous use of contaminated wands.

In terms of various methods of collection. When it comes to recovering DNA and capturing friction ridge detail, Gelatine Lifters are acknowledged as the best of both worlds. Additionally, a "Double Sampling Strategy" is advised, which involves lifting the print with tape and swabbing the residue to maximise recovery while maintaining the image's original appearance. Additionally, the current issue of inhibition and contamination should be resolved by future developments in biocompatible fluorescent sprays and powders for anti-DNA contamination.

**Keywords:** Touch DNA, Fingerprint Powders, DNA Yield, DNA Extraction, Double Sampling Strategy.

PP14

**Determination of Sex of femur using angle of neck and shaft -A cross sectional study**

Ajit Kumar<sup>1</sup>, Nityanand Kumar<sup>2</sup>, Kaushal Kishore<sup>3</sup>

<sup>1</sup>Department of Anatomy, LCMCH, Bishrampur, Palamu, Jharkhand.

<sup>2</sup>Department of FMT, LCMCH, Bishrampur, Palamu, Jharkhand.

<sup>3</sup>Department of FMT, Sri Gorakshnath Medical College Hospital & Research Centre,  
Gorakhpur

[ajit.anatomy@gmail.com](mailto:ajit.anatomy@gmail.com)

**Abstract**

**Introduction:** Assessment of human sex from skeletal parts is important in anthropology, archaeology, palaeoanthropology, comparative anatomy and forensic medicine where it provides accurate information to medico-legal information. Hence this study was taken to determine the sex from femur. Determination of sex from skeletal remains is an important component in the identification but sometimes becomes difficult to the forensic expert especially when the pelvis is absent. Sex determination carried out from the male and female femur bones is accurate in ninety percent of cases than in cases of adult pelvis or skull. Various studies demonstrated the metric assessment of sex to differentiate in races and regions in the populations.

**Aim:** This study was conducted for metric standards of sex determination by femur measurements.

**Materials and Methods:** Osteometric data were obtained from the 128 adults femurs (64 males and 64 females). 64 Male (32 right and 32 left side) and 64 females (32 right and 32 left side). The instruments used for measuring goniometer. Statistical analysis was done using ANOVA and SPSS computer-based software.

**Result:** This measurement also differed significantly between sexes ( $p < 0.001$ ). With a mean of  $105.69^\circ$  in male's Vs  $89.36^\circ$  in females, it yielded the highest AUC (0.616) among the three parameters. While this is still modest, it indicates that the neck-shaft angle provides better sex estimation potential compared to the other two.

**Conclusion:** Strong sexual dimorphism was observed in cranial vault dimension.

**Keyword:** Femur, Sex determination, Sexual dimorphism, Variables of upper end, Discriminant functional analysis, Neck shaft angle



AMITY UNIVERSITY  
UTTAR PRADESH



PP15

## Region- Wise Distribution of Two Forensically Significant Diatom Genera in India: A Review of *Navicula* and *Nitzschia*

Vanshika Mishra<sup>1</sup>, Pallavi Thakur<sup>1\*</sup>

<sup>1</sup>Amity Institute of Forensic Sciences, Amity University, Uttar Pradesh, India

\*Corresponding Author: [pthakur1@amity.edu](mailto:pthakur1@amity.edu)

### Abstract

Diatoms are microscopic algae that play a very significant role in aquatic ecosystem and are also extensively used in forensic science, especially in drowning investigations. This review paper highlights the region- wide distribution of two forensically important diatom genera, *Navicula* and *Nitzschia*, across different parts of India. The main aim of this study is to gather and categorize available information about their presence in different water bodies such as rivers, lakes, ponds, and wetlands in various states of the country.

In this paper, specific focus is given to building a detailed database of species reported from North, South, East, West, and Central India. Along with distribution the study also illustrates the basic taxonomy, morphology, and recognizing features of both genera, which help in differentiating them during microscopic examinations. Environmental factors such as temperature, pH, water, flow and availability of nutrients that contribute to their development and growth are also discussed in this paper.

The study evaluates the forensic importance of these diatoms, specifically how their occurrence and variation in different regions can support investigations by connecting biological evidence to specific locations. At the same time, some limitations are also identified such as lack of region- specific data, variation in reporting, and insufficient standardization in the database in India.

As a whole, this review brings together scattered information into one place and show the need for more detailed and region- specific studies in the future. It can be helpful for forensic experts, researchers, and students who are working in the field of forensic science and aquatic biology.

**Keywords:** Diatoms *Navicula*, *Nitzschia*, Forensic Science, Drowning Investigations, Regional Distribution, India, Aquatic Biology



AMITY UNIVERSITY  
UTTAR PRADESH



PP16

## Enhancing Recovery of Touch DNA From Handheld Weapons

Anshika Pathak<sup>1</sup>, Pallavi Thakur<sup>1\*</sup>

<sup>1</sup>Amity Institute of Forensic Sciences, Amity University, Uttar Pradesh, India

\*Corresponding Author: [pthakur1@amity.edu](mailto:pthakur1@amity.edu)

### Abstract

Touch DNA analysis has emerged as a valuable tool in forensic investigations, particularly in cases where no visible biological evidence is present. Despite its growing importance, the recovery of touch DNA from handheld weapons such as knives, firearms, and blunt objects continues to pose several challenges. These challenges arise due to factors like minimal skin cell transfer, frequent handling, environmental exposure, and the varying surface properties of different materials. As a result, obtaining sufficient and reliable DNA profiles from such evidence is often difficult.

This study focuses on enhancing the recovery of touch DNA from commonly encountered handheld weapons by examining and improving existing collection techniques. Different recovery methods, including wet and dry swabbing, double swab techniques, and the use of alternative collection materials, were evaluated to determine their efficiency. The study also considers the impact of variables such as the pressure applied during handling, duration of contact, and surface texture of the weapon on DNA transfer and persistence.

In addition, careful handling and storage procedures were emphasized to prevent contamination and degradation of DNA samples. A comparative analysis between conventional and improved recovery approaches was conducted to identify methods that provide higher DNA yield and better-quality profiles.

The results indicate that optimized collection techniques, along with proper evidence handling, can significantly improve the recovery of touch DNA from challenging surfaces. These findings highlight the importance of methodological refinement in forensic practice. Improved recovery of touch DNA can strengthen its evidentiary value, aiding in the identification of individuals involved in criminal activities, especially in cases where other forms of biological evidence are unavailable.

**Keywords:** Touch DNA, Handheld Weapon, Trace Evidence, Forensic Investigation, Evidence Handling, DNA Profiling



AMITY UNIVERSITY  
UTTAR PRADESH



PP17

## Comparative study of open source- AI tools and conventional tools for vulnerabilities assessment

Abhishek Kushwaha<sup>1</sup>, Kajal Sharma<sup>1\*</sup>

<sup>1</sup>University Of Lucknow, Lucknow

\*[kushwahaabhishek606@gmail.com](mailto:kushwahaabhishek606@gmail.com)

### Abstract

In the fast-changing environment of cyber threats that we live, it is important to consider the effectiveness of vulnerability assessment tools to maintain the integrity of digital forensics and ensure the security of systems. This research investigates and provides a comparison of open-source AI tools (Pentest-Tools and CyberScan.io) and conventional tools (Nessus and OWASP ZAP) in a comparative study of their efficacy, accuracy, and capacity to discover web-based vulnerabilities. To be part of this work, a university website was scanned in a controlled environment and performance reviewed utilizing a number of bench marking results, for example: encryption, cookie security, report presentation, and the ability to detect SQL injection, cross site scripting, and cross site request forgery.

The findings shown that traditional scanners like ZAP and Nessus were more effective in uncovering known vulnerabilities with detailed reports and structured evidence in comparison to the quick scanning, automated AI-based tools, AI-based tool provided scanning, automation, and prediction, however, on detecting advanced and application-level threats it fell short. The report highlights that AI supports speed and reduces false positives, performing most effectively in conjunction with traditional tools to support security.

This comparative evaluation emphasizes the increasing necessity of hybrid vulnerability assessment models. By leveraging the ongoing adaptive intelligence of AI tools and the analytical depth of traditional scanners, hybrid vulnerability assessment models provide accuracy, efficiency, and resilience in proactive cyber security efforts and digital forensic investigation.

**Keywords:** Vulnerability Assessment, Forensic Science, OWASP ZAP, Nessus, Pentest-Tools, Cyber Scan, AI in Cyber security, Web Application Security.



AMITY UNIVERSITY  
UTTAR PRADESH



PP18

## Analysis Of Orchestration Layer for Chain of Thought Artifacts in Agentic AI

Shreya Katti

*SFS, National Forensic Science University, Gandhinagar*

*[shreya.msfs1242620@nfsu.ac.in](mailto:shreya.msfs1242620@nfsu.ac.in)*

### Abstract

We live in a world that is increasingly influenced by the convenience and assistance of generative AI. As autonomous AI agents are being deployed to maintain and manage heavy duty workflows in the corporate and financial sectors, the indiscernible nature of their decision-making presents a critical challenge to forensics. Traditionally, digital forensics analyses static logs, which is lacking in ways to reconstruct the non-deterministic reasoning paths of agentic AI. This proves unhelpful during cases such as Indirect Prompt Injection targeting data or protocols. This paper addresses the observability gap by proposing a framework for the forensic reconstruction of autonomous logic. The methods used to demonstrate and measure AI behavior are as follows. Lang Graph: Used to map AI logic into a graph of nodes and edges. This allows for isolation of reasoning steps, ensuring that the “Orchestration Layer” is separate from the output. SQLite checkpoint: To manage the volatile nature of the evidence, a checkpoint is introduced to technically capture a snapshot of the agents internal state. Attribution Certainty [AC] Score: A score that helps quantify supposed ‘Cognitive drift’. It incorporates 3 primary variables:

- Number of forensic markers captured [A]
- Total number of steps defined by the protocol [D]
- Measure of reasoning instability aka Semantic Entropy [H]
- A constant to provide a trust range [k]

$$AC = k * (A/D) * (1-H)$$

### Results:

Clean audit runs achieve a high AC score [at an average of 0.9], whereas Injected prompts trigger a drift and drop the scores to about 0.15. Data confirms the orchestration layer successfully preserves artifacts that are sanitised in user-facing outputs. This enables forensic reconstruction of how and why the agent deviated.

### Conclusion:

By making internal reasoning a forensic artifact, this research proposes a solution for auditing autonomous agents. The results offer a defensible methodology to satisfy emerging NIST 2026 guidelines, by ensuring AI driven decision making remains transparent and resilient.

**Keywords:** AI Forensics, Agentic AI, Indirect Prompt Injection, LangGraph, Auditability of AI



AMITY UNIVERSITY  
UTTAR PRADESH



PP19

## Cybercrime And Need for the Forensic Auditing

Harsh Aryan<sup>1</sup>, Chintan Singh<sup>1</sup>

<sup>1</sup>Amity Institute of Forensic Sciences, Amity University Uttar Pradesh, Sector-125, Noida-201313, India

[harsh.official042@gmail.com](mailto:harsh.official042@gmail.com)

### Abstract

Cybercrime is an illegal activity which involves digital platforms and online sites for which someone can get unauthorized access to anyone for their own benefits. Whereas the Forensic Auditing is the detailed investigation of the company records, transactions and data records which help to ensure any organization data security. While these both are interrelated to each other because Cybercrime is the problem and meanwhile Forensic Auditing can be the solution to the problem. The primary objective of this study is to analyze the role of forensic auditing in identifying and detecting the causes of cybercrime and in preventing illegal online activities. This study includes qualitative research of the approach including the secondary data from the research papers, books, reports, and case studies related to cybercrime and forensic auditing. It analyses the trends in cyber fraud and the techniques used by forensic auditors. The main finding in this is that the cases of cybercrime is increasing which includes digital payments (UPI), Company's financial records, transaction history, etc. to which Forensic Auditing can help to track and detect financial records, transaction history, and digital evidence. The conclusion of this study is that forensic auditing is emerging very fast and it can help to detect and track the cybercrimes happening. Also, many organizations should go with forensic auditing so that the chances of digital crime should be minimised and the transparency of the company records should be maintained with the employees.

**Keywords:** Cybercrime, Forensic Auditing, Financial Records, Digital

## **RegScanX: An Automated Windows Registry Forensic Analysis Tool**

Harshita Gupta<sup>1</sup>, Mankirat Kaur<sup>1</sup>, Megha Jha<sup>1</sup>, Kritika Singh<sup>1</sup>, Sourabh Kumar Singh<sup>1</sup>

*Department of Forensic Science, K.R. Mangalam University, Sohna, Haryana, India*

*[gharshita01124@gmail.com](mailto:gharshita01124@gmail.com)*

### **Abstract**

RegScanX is a Python-based digital forensic tool which is developed to aid investigators in forensic investigations as it analyses major Windows Registry artifacts and provides meaningful and important data based on them for investigation purposes. The Windows Registry is basically hierarchical data set setup in the system which stores all the crucial data of the system, be it about users, hardware, software and other related data. Its analysis can indicate certain important events which can help investigators with crucial evidence related to crime. However, analyzing and extracting this data manually is a really time-consuming and complex process. To solve this, RegScanX provides an automated data extraction feature, which is then followed by analysis and a report generation. It has 3 modes in it based on its ability to capture data and whether the administrator permissions were granted or not: Auto (in this the tool automatically captures and analyses all the data if administrator permissions were granted), Limited (if administrator permissions were not granted, it will capture as much data as it can and present a report for the same) and Manual (in this the user has to manually upload the data, and then after analyzing it, it will generate a report). The major artifacts or registry hives included in this are SYSTEM, SOFTWARE, SAM, NTUSER, etc. The tool focuses on collecting important information like USB device history, executed Run commands, and recently accessed files, and then it also creates a chronological timeline and related graph based on the data analyzed. The report generated is in PDF format and is stored at the same location from where the tool was accessed, along with the extracted hives data and timeline data. Overall, RegScanX provides a medium wherein registry hives can be extracted, analyzed and reported efficiently.

**Keywords:** Windows Registry, Automated analysis, Artifacts analysis

PP21

**Cybercrime In Online Gaming: Issues of Platform Liability and User Protection**

Jayesh, Mittal, Dr. Amit Dhall\*

*Amity Law School, Amity University, Noida, Uttar Pradesh*

*\*Corresponding Author: [adhall@amity.edu](mailto:adhall@amity.edu)*

**Abstract**

The blistering development of online gaming platforms has revolutionized online entertainment but has also opened new possibilities of cybercrime. Identity theft, phishing, financial fraud, harassment, and unauthorized access to data are becoming more and more common in the gaming ecosystem. This paper reviews the legal and regulatory issues that entail online gaming through cybercrime that deals with platform liability and user protection. The study will take a doctrinaire and analytic stance by evaluating the current legal provisions, case laws and policies concerning cybercrime and intermediary liability. It also considers the international practices and makes a comparison with the Indian legal system, comprising of the provisions in the Information Technology Act, 2000. The results show that even though the gaming platforms can play the role of the middle men, its responsibility in curbing the cybercrime is still not clear. The existing laws give no strict guidelines regarding the level of responsibility of platforms, and the safety is often shifted on to the user. Also, there is a lack of adequate enforcement systems in cross-border cyber threats and new types of online exploitation in the gaming field. The paper finds that the current legal frameworks continue to be in need of reinforcement with the aim of creating a balanced position between the liability of the platform and the protection of the user. To reduce the cyber risks, the regulatory oversight, compliance demands on the gaming platforms, and awareness among the users should be enhanced. It is the recommendation of the paper to come up with more specific guidelines on intermediary responsibility and implementation of more effective cybersecurity to establish a safer online gaming environment.

**Keywords:** Cybercrime, Online Gaming, Platform Liability, User Protection, Digital Law

## **Artificial Intelligence for Security, Privacy, and Trustworthiness: A Systematic Review**

Imam Ashraf<sup>1</sup>, Priyanka Gopi<sup>1\*</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University Uttar Pradesh, Noida, India 201303*

*\*Corresponding author: [pgopi@amity.edu](mailto:pgopi@amity.edu), [priyankagopi5495@gmail.com](mailto:priyankagopi5495@gmail.com)*

### **Abstract**

The fast development of Artificial Intelligence on the areas of cybersecurity and computerized evidence is a paradox in itself, as it has created another significant problem in the context of the software safety: the privacy of personal data, the hiddenness of the algorithmic processes, and the susceptibility to the manipulation by adversaries. It is a systematic literature review (SLR) of 30 peer reviewed articles on artificial intelligence in digital forensics that look at the trade-off between security, privacy, and trustworthiness. This review combines all modern technologies of artificial intelligence, such as intrusion detection, malware analysis, and threat intelligence, with privacy sensitive methodologies, such as federated learning and differential privacy, along with the principles of trustworthy design, such as explainable artificial intelligence and robustness. This review identifies a critical gap that is present in what is currently available in the literature of intersection of security and privacy research. The current literature that focuses on security issues generally ignores the privacy limitations, whereas literature that is focused on privacy tends to be not thoroughly tested against the realistic adversarial situations. The existing literature does not include a set of governance mechanisms and explainability focused on human beings, thus hindering the implementation of such solutions to high stakes forensics. This study contributes an identification and summary of the open research areas and challenges of regulation aware integrated AI architecture. It is further emphasized that future standards should focus on robustness and explainability as design principles, rather than as an afterthought, to foster safe and trusted AI design.

**Keywords:** Artificial Intelligence; Cybersecurity; Privacy Preserving Machine Learning; Explainable AI (XAI); Trustworthy AI; Digital Forensics; Standardization.

PP23

**Digital Immortality vs. Digital Oblivion: A Systematic Review of Data Recovery Methodologies for Modern Storage Architectures**

*Thayanithi C<sup>1</sup>, Dr Prateek Pandya<sup>1</sup>*

*<sup>1</sup>Amity Institute of Forensic Sciences, Amity University Uttar Pradesh, Noida, India*

*\*Corresponding Author: [ppandya@amity.edu](mailto:ppandya@amity.edu)*

**Abstract**

The move from magnetic Hard Disk Drives (HDDs) to Solid-State Drives (SSDs) and Universal Flash Storage (UFS) systems has caused an epistemological crisis for digital forensics. Modern flash controllers have autonomous background processes such as TRIM and Garbage Collection. In mobile devices, these processes are called Android, and iOS's Space Manager, and they seek to optimize performance by aggressively sanitizing deleted data. This systematic literature review addresses one component of the 'Forensic Gap' by analyzing the tension between theoretical persistent data, i.e., 'Digital Immortality', against the plastic reality of automated and irreversible data loss, referred to as 'Digital Oblivion'. Using the PRISMA method, the research synthesized 45 core peer-reviewed articles between 2015 and 2025 to assess the effectiveness of current recovery solutions for mobile and desktop environments (specifically NVMe). The research shows that traditional dead-box file carving tools have an empirically demonstrated failure rate that exceeds 90% on TRIM-enabled devices. Additionally, although potential emergent Artificial Intelligence (AI) and Machine Learning (ML) carving models possess the ability to recover fragmented data, the absence of explainable artificial intelligence (XAI) frameworks and models means that they may be legally unenforceable (e.g., the Daubert Standard) due to the lack of explainability. The review also identifies a unique mobile device 'Forensic Window' due to 'idle and charging' states, suggesting these autonomous hardware actions may be a form of spoliation of evidence. As such, the dissertation claims that the post-mortem forensic paradigm is obsolete. It urges the sector to adopt Live Forensics (volatile RAM acquisition) and introduces a novel first responder 'Do Not Charge' triage policy to mitigate the loss of digital data.

**Keywords:** Digital Forensics; Solid State Drives (SSD); Universal Flash Storage (UFS); Systematic Literature Review (SLR); Live Memory Acquisition; Data Spoliation; PRISMA Protocol; APFS; Daubert Standard

## PP24

### From Avatars to Evidence: Forensic Challenges of Investigating Crime in the Metaverse Identification

*Ekta Pradhan<sup>1</sup>, Sonali Kesarwani<sup>1\*</sup>*

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Noida, Uttar Pradesh, India-201303*

*\*Corresponding author: [skesarwani@amity.edu](mailto:skesarwani@amity.edu)*

#### Abstract

The rapid development of immersive digital worlds, also known as the metaverse, has distorted online interactions quite extensively, with the combination of virtual reality, blockchain technology, and decentralised digital economies. Users interact in these worlds using avatars, interact socially and conduct transactions of virtual goods, including cryptocurrencies and non-fungible items (NFTs). As much as these technological innovations have provided new opportunities in communication and business operations, they have simultaneously created new avenues of cyber criminality, which include impersonation of identity, virtual harassment, fraud, and theft of virtual resources. Analytics of such crimes can be a significant challenge to digital forensic practitioners because virtual ecosystems are complex and decentralised. The analytical method used in this research is a review of the literature, trying to analyse all the current literature on metaverse security, digital forensic techniques and cyber legal frameworks. The review of the available academic literature, cybersecurity studies, and digital forensic inquiries was carefully conducted in order to identify the main issues associated with the investigation of crimes that occur in the virtual environment. The review clarifies some of the key forensics challenges, such as the difficulties related to avatars to real-life identities, limitations in receiving and conserving digital evidence of immersive virtual reality environments, and complexities of analysing transactions in blockchain virtual asset environments. Moreover, jurisdictional limitations and the absence of standardised forensic frameworks further complicate the investigation of metaverse-related crimes. The findings demonstrate that nowadays there is a high need to use dedicated forensic models and tools that are more specific to the metaverse, advanced analytical tools, and new cyber legal regulations that will be able to combat crimes in the virtual ecosystem. It will be essential to develop interdisciplinary approaches which will combine cybersecurity, digital forensics, and legal regulations to ensure accountability, evidence integrity, and safety in the rapidly evolving metaverse world.

**Keywords:** Metaverse Forensics, Digital Evidence, Cybercrime Investigation, Avatar Identity, Virtual Worlds

**PP25**

**IoT Forensics in consumer devices: Smart homes and Wearables**

*Kritika Parbhakar<sup>1</sup>, Anmol Bhardwaj<sup>1</sup>*

*<sup>1</sup>Department of Forensic Science, Lovely Professional University, Punjab.*

*[kritika.parbhakar3304@gmail.com](mailto:kritika.parbhakar3304@gmail.com)*

**Abstract**

The rise of Internet of Things (IoT) devices in homes has improved daily convenience and opened new paths for digital forensic investigations. Wearable technology and smart home devices are crucial sources of evidence because they regularly gather information on user behaviour, the physical environment, and biometrics. During investigations, these gadgets serve as digital witnesses, continuously capturing streams of data that can either confirm or refute chronological accounts. However, the IoT forensics field faces significant challenges from varied devices, short data retention, strong encryption, reliance on cloud services, and changing legal rules. This review looks at the current state of knowledge by summarizing thirty-six peer-reviewed studies published between 2019 and 2025. The selection was based on explicit inclusion criteria emphasizing relevance to forensic acquisition, empirical rigor, and device diversity. The synthesis examines forensic artifacts, data acquisition methodologies, illustrative case studies, and emergent obstacles and solutions, with a particular focus on representative platforms such as Samsung SmartThings, Xiaomi Mi Home, and Amazon Alexa, as well as wearables including Fitbit, Garmin, and psychiatric monitors. Additionally, this review identifies and critically discusses innovative approaches, such as blockchain-enabled evidence management, edge forensics, side-channel analysis, and federated learning. Based on this integrative review, this study underscores the imperative for standardized forensic frameworks, validation of analytical tools, and adoption of privacy-centric practices to further advance the discipline of IoT forensics.

**Keywords:** IoT forensics, smart homes, wearables, digital evidence, blockchain, forensic readiness, forensic challenges, cloud forensics



AMITY UNIVERSITY  
UTTAR PRADESH



PP26

## Forensic Analysis on the Impact of Cyberbullying Among Indian Youth

*Isha Thakur<sup>1</sup>, Nandini<sup>1</sup>, Anmol Bhardwaj<sup>1</sup>*

*<sup>1</sup>Department of Forensic Science, Lovely Professional University, Punjab.  
[thakurisha957@gmail.com](mailto:thakurisha957@gmail.com)*

### Abstract

With the digitalization of the human world, the internet has now become an important part of every life. A single click can provide all the information from all over the world. However, this progress has also led to cyber offences such as cyberstalking, cyberbullying, spoofing, phishing, credit card fraud, data breaching, etc. Among these cybercrimes, cyberbullying is commonly seen within society, but people are hesitant to report due to fear of embarrassment. Cyberbullying refers to the intentional and repeated use of digital technologies to harm, intimidate, or harass individuals. It typically involves sending threatening, abusive, or derogatory messages, emails, comments, or posts with the deliberate aim of causing emotional distress or fear. There are various legal provisions, reporting portals, and helpline numbers that are introduced by the government. Awareness campaigns are also being run to address these issues. The government and many organizations are actively working to spread awareness and provide support mechanisms. These measures highlight the seriousness of cyberbullying and the collective effort to mitigate its impact. In the present study, an attempt is made to review certain survey-based studies to determine the perspective of various authors on the impact of cyberbullying on the lives of youngsters.

**Keywords:** Cyberbullying, Online Harassment, Risk Factors, Flaming.

**PP27**

**Secure Cyber-Physical Forensic Box: A Novel Approach to Evidence Protection and Blockchain-Enabled Chain-of-Custody**

*Simran Kumari<sup>1</sup>, Arul Asokan<sup>1</sup>*

*<sup>1</sup>Student of BSc (Hons) Forensic Science, <sup>2</sup>Student of MSc Forensic Science  
Lovely Professional University, Punjab, 144411  
[simrandeep0607@gmail.com](mailto:simrandeep0607@gmail.com)*

**Abstract**

This paper introduces the Secure Cyber-Physical Forensic Box (SCFB), an innovative hybrid security system designed to address the critical challenges of preserving and safeguarding forensic evidence in both physical and digital domains. As cyber-enabled crimes continue to rise, ensuring the integrity of forensic evidence is paramount. Traditional security systems, such as standalone electronic locks and storage units, often operate in isolation and fail to provide comprehensive protection. The SCFB bridges this gap by integrating cutting-edge cybersecurity measures with a tamper-proof physical enclosure, creating a unified approach to evidence security. At the core of the SCFB's design is a multi-layered authentication system combining biometric verification (fingerprint and 3D facial recognition with liveness detection) and geo-fencing to ensure jurisdictional access control. Additionally, digital authorization is secured by cryptographic unlock tokens. Every access attempt and event is recorded on a private blockchain, generating immutable, time-stamped audit trails to maintain chain-of-custody and ensure evidentiary transparency. To protect against environmental and physical tampering, the SCFB employs AI-driven intrusion detection mechanisms that monitor anomalies such as vibration, thermal fluctuations, and electromagnetic interference. In response to detected threats, the system initiates dynamic re-encryption, hardware lockdown, and encrypted alert transmission to authorized forensic authorities. The SCFB also incorporates emergency access protocols, allowing for time-sensitive access without compromising security. By combining physical security, advanced cybersecurity, and blockchain-based tracking, the SCFB represents a forward-thinking solution for secure forensic evidence management, aligning with contemporary legal, technological, and investigative standards.

**Keywords:** Digital forensics, Blockchain-based Chain of Custody, Multi-layered authentication, Forensic Evidence preservation, Secure Cyber-Physical Forensic Box (SCFB), AI-driven intrusion detection.



AMITY UNIVERSITY  
UTTAR PRADESH



PP28

## Harvest Now, Decrypt Later: A Transparent Quantum-Wrap Proxy for Legacy Cloud Data

Edvin Sanil<sup>1</sup>, Priyanka Gopi<sup>1\*</sup>

<sup>1</sup>Amity Institute of Forensic Sciences, Amity University, Noida, Uttar Pradesh, India, 201303

\*Corresponding author: [pgopi@amity.edu](mailto:pgopi@amity.edu)

### Abstract

With the development of large-scale quantum computing, a major threat seems to the classical public-key encryption, particularly on information secrecy in the long run. One of the most significant threats that cannot be neglected in recent literature is also offered by Harvest-Now, Decrypt-Later (HN DL) threat model. Cloud infrastructures are also vulnerable because of their form of centralized storage, and long-term storage of sensitive data, including medical, government, finances, and forensic. Theoretically, retrofitting legacy cloud environments with native Post Quantum Cryptography (PQC) support is feasible, even after NIST-standard PQC algorithms such as ML-KEM (Kyber) have been implemented, but such retrofitting is expensive and infeasible. This study proposes a Transparent Quantum-Wrap Proxy (TQWP) architecture that can be used to mitigate the threats of HN DL in the existing cloud systems without making any changes in the backend databases and application code. The solution uses cryptographic envelope where the symmetric keys are encrypted with the assistance of ML-KEM-768 that wraps AES-256. This model has been built in a manner that it is quantum resistant in regard to key exchange but compatible in existing infrastructure. The proxy is placed on the cloud boundary and it operates transparently between clients and storage services. It executes and destroys the PQC envelope without altering database and application code. Initial performance measurements indicate that the latency overhead is not high and the memory growth also is not that much as the entire PQC migration plans. Security analysis indicates resilience to Shor based attacks against the public-key encryptions without affecting the symmetric encryption against the quantum capable adversaries. The architecture proposed will provide transitional defense against the likely threat of quantum attacks because it decouples cryptographic agility and underlying database logic. This work provides a deployable architectural framework that seals the gap between the theory of the HN DL risk analysis and practice of providing security to the old cloud data system.

**Keywords:** Post-Quantum Cryptography, ML-KEM, Har

**PP29**

**Secure Scan: A Portable Solution for Preventing Digital Payment Fraud**

*Karthik Krishna V, Shivani Singh, Arul Ashokan, Franco Sajan Moozhil  
Lovely Professional University, 144411, Punjab  
[karthikkrishnavinoy@gmail.com](mailto:karthikkrishnavinoy@gmail.com)*

**Abstract**

In this Digital India, where most payments are made through UPI (Unified Payments Interface), the risk of spam and cyber fraud is high. Spammers can now easily steal money from anyone, unlike before. It's now easy to gain access to anyone's device or bank accounts, and most of all, we, users themselves, knowingly or unknowingly, fall into their trap. For the solution to this problem, our device Secure Scan, which anyone can use to scan any QR code, links, or OTPs that they find suspicious. Components which have been used for this device are a body made up of ABS plastic (Acrylonitrile Butadiene Styrene), a 5 megapixel camera assisted by a flashlight, a 1500 mAh Li-ion, 0.91" 128×32 OLED (COG) display module, ESP32-S3 processor, and a US-C port. Secure Scan enables users to scan QR codes, links, or OTPs externally to verify their authenticity. It leverages Google Safe Browsing API (v4) for validation externally, displaying the result on the OLED screen. A detailed report is then sent to the user's device via Bluetooth or USB data transfer. As the device connects to the user's phone via Bluetooth, it ensures that the phone remains protected from potential threats while providing a comprehensive report on the scanned item.

**Highlights:** Portable and user-friendly device to verify QR codes, links, and OTPs to protect, against spam and fraud. Leverages Google Safe Browsing API (v4) for real-time external validation of potentially suspicious links or QR codes. Bluetooth connectivity ensures phone security while providing a detailed report on scanned items without compromising device safety.

**Keywords:** Malicious QR code scanner, Cyber security, Mobile forensics, Fraud Prevention, Phishing protection, Prevention method, Payment security.

## Signal Shadow: An External Os-Independent Device For Detecting And Preventing Covert Mobile Surveillance

Shivani Kumari<sup>1</sup>, Dr Vinayak Gupta<sup>1\*</sup>

<sup>1</sup>*Department of Forensic Sciences, School of Bio-Engineering and Bio-Sciences,  
Lovely Professional University, Phagwara-144411, Punjab.*

*\*Corresponding Author: [vinayakgupta224@gmail.com](mailto:vinayakgupta224@gmail.com)*

### Abstract

In today's digital era, mobile phones store large amounts of personal and sensitive information, making mobile privacy extremely important in modern society. However, with the increasing risk of spyware and hidden surveillance, stronger and more reliable protection methods are becoming necessary. The Signal Shadow aims to enhance mobile privacy and security by developing a portable, external device capable of detecting and preventing covert mobile surveillance. Covert mobile surveillance is the secret monitoring of a mobile phone's activities such as calls, messages, location, microphone, or camera usage without the knowledge or consent of the user. The device has been designed to operate independently of the mobile operating system. The device monitors electromagnetic and radio-frequency (EM/RF) emissions generated by hardware components such as microphones, cameras, GPS modules, and communication systems. The primary objective is to identify hidden surveillance activities, including spyware, stalker ware, unauthorised audio/video recording, and background data transmission by differentiating between normal and suspicious device activity. By analyzing hardware-level signal patterns along with contextual parameters such as screen status, user interaction, timing, and duration, Signal Shadow enables real-time detection of unauthorised operations. When abnormal behaviour is detected, alerts will be generated instantly, and secure time-stamped logs are stored for forensic and investigative purposes. Unlike conventional antivirus or software-based security solutions, Signal Shadow does not require software installation, device pairing, or operating system access. This ensures functionality even in cases where the mobile device has been compromised. Signal Shadow is expected to serve as a reliable hardware-based surveillance detection tool, providing an additional layer of protection beyond traditional software security mechanisms and strengthening mobile privacy in increasingly surveillance-prone digital environments.

**Keywords:** Hardware-Based Privacy Protection, Signal Monitoring, Spyware Detection, Covert Surveillance, Data Leakage Detection.



AMITY UNIVERSITY  
UTTAR PRADESH



PP31

## A Framework-based Methodology for Enhancing SOC Efficiency through Integrated Monitoring of IoT Devices

Serin Susan Mathew<sup>1</sup>, Sonali Kesarwani<sup>1\*</sup>

*Amity Institute of Forensic Sciences, Amity University, Noida, Uttar Pradesh, India- 201303*

*\*Corresponding Author: [sonalikesarwani743@gmail.com](mailto:sonalikesarwani743@gmail.com)*

### Abstract

Modern network environments have become highly abstract and massive with a tremendous growth in the number of devices that fall under the Internet of Things (IoT). These devices generate large amounts of various security information and this poses a big challenge to Security Operations Centers (SOCs) with regard to handling and analyzing it. In IoT-based systems especially, conventional SOC infrastructures are often faced with alert floods, significant false-positive rate as well as slow incident reaction. The current research suggests IoT-SEAM v2.0, a framework that targets IoT ecosystems, that can be useful to improve the operation of SOC, providing embedded monitoring, detection, automation, and performance evaluation. The suggested model deploys a logical and systematic strategy. The real-world security incidents of a simulated IoT setup are repeatedly gathered and handled by a log ingestion pipeline based on a SIEM. To facilitate the recognition of the attack techniques in a uniform manner, the detection rules have been established and associated with the MITRE ATT&CK framework. To reduce the noise and focus on alerts, threat intelligence feeds and AI-based methods of alert refinement are applied. Security Orchestration, Automation, and Response (SOAR) are workflows that are used to automate incident response. The case management and visualization dashboards are used to analyze SOC performance metrics and monitor incidents. The experimental analysis demonstrates the better prioritization of critical incidents and the significant decrease in false-positive notifications. In comparison to a control SOC system without automation, the structure brings realizable improvements in Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

**Keywords:** IoT Security, SOC Automation, SIEM, SOAR, MITRE ATT&CK.



AMITY UNIVERSITY  
UTTAR PRADESH



PP32

## Optimizing Malware Identification Through Advanced YARA Pattern Matching Techniques

Mudita<sup>1</sup>, Prateek Pandya<sup>1\*</sup>, Chintan Singh<sup>1</sup>, Biswa Prakash Nayak<sup>1</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Sector 125, Noida, Uttar Pradesh, 201303, India*

*\*Corresponding Author: [ppandya@amity.edu](mailto:ppandya@amity.edu)*

### Abstract

The modern threat landscape is characterized by an exponential increase in malware complexity, where traditional signature-based detection mechanisms often fail to keep pace with rapid code evolution. As threat actors increasingly employ advanced obfuscation, packing, and polymorphic engines, the burden on security analysts to produce timely and accurate detection rules has become unsustainable. While YARA remains the industry standard for pattern matching and malware classification, its efficacy is fundamentally limited by the manual nature of rule creation. Current YARA rule development processes are predominantly reactive and rely heavily on the intuition of human analysts. This dependency introduces a critical bottleneck in incident response and often results in signatures that are either too specific leading to high false-negative rates or too broad, causing significant false-positive alerts in production environments. This work focuses on enhancing malware identification by integrating YARA rule-based pattern matching with machine learning techniques across multiple malware datasets. We analyzed three distinct categorized datasets, PE Header dataset containing 62,485 samples of Ransomwares, a Ransomware dataset comprising 21,752 samples across 27 ransomware families, pegasus spyware dataset with 1,000 samples targeting iOS and Android platforms. The proposed methodology combines static feature analysis with signature-based detection using YARA rules, achieving significant improvements in malware classification accuracy. A total of 27 YARA rules were developed and validated, targeting specific malware signatures, behavioral patterns, and Indicators of Compromise (IOCs). The PE Header dataset achieved 99.68% accuracy with Random Forest classification, the Ransomware dataset achieved 96.90% accuracy for 27-family classification, and the Pegasus spyware dataset achieved 70.50% accuracy.

**Keywords:** Malware Detection, YARA Rules, Pattern Matching, Automated Signature Generation, Cybersecurity, Python.

PP33

## **Chip-Off Forensics in the Quantum Era: A Review of Challenges, Cryptographic Barriers, and Future Directions**

Arul Asokan<sup>1</sup>, Shivani Singh<sup>1</sup>, Sanasam Sadananda Meitei<sup>1</sup>  
*Lovely Professional University, Punjab-144411, India*  
[arulasokan75@gmail.com](mailto:arulasokan75@gmail.com)

### **Abstract**

Mobile device forensics has long relied on chip-off extraction as a last-resort technique for recovering data from damaged, locked, or otherwise inaccessible devices. However, the growing adoption of strong encryption in consumer electronics has significantly reduced the forensic value of raw memory dumps obtained through this method, as physically extracted data remains unreadable without corresponding decryption keys. This problem is expected to worsen as device manufacturers begin integrating post-quantum cryptographic schemes, particularly the lattice-based and hash-based algorithms recently standardized by the National Institute of Standards and Technology in 2024, into the encryption frameworks protecting data at rest on mobile hardware. This paper reviews the current state of chip-off forensic methodology alongside the evolving quantum cryptographic landscape, examining how developments in one domain directly complicate progress in the other. Key concerns include the forensic implications of the harvest-now-decrypt-later threat model, the anticipated resilience of post-quantum encrypted devices against physical extraction techniques, and the prospective role of quantum-assisted computation in legacy device key recovery. Drawing from literature across digital forensics, applied cryptography, and mobile security, this paper identifies the critical gaps that forensic practice must address before post-quantum encryption becomes mainstream in consumer devices, and outlines initial considerations toward building forensic practices that account for quantum-era realities.

**Keywords:** chip-off forensics, post-quantum cryptography, mobile device forensics, NAND flash, extraction

**PP34**

**Ransomware Cartels and Their Affiliate Networks as a Modern Cybercrime**

*Dr Vinayak Gupta<sup>1\*</sup>*

<sup>1</sup>*Department of Forensic Sciences, School of Bio-Engineering and Bio-Sciences, Lovely Professional University, Phagwara-144411, Punjab.*

*\*Corresponding Author: [vinayakgupta224@gmail.com](mailto:vinayakgupta224@gmail.com)*

**Abstract**

The current cybercrime landscape has experienced a significant transformation in ransomware operations, evolving from isolated threat actors to intricate cartel-like entities that manage complex affiliate networks. This study analyses the framework, development, and operational mechanisms of ransomware cartels and their affiliate ecosystems. Further, the study examines threat intelligence data, law enforcement reports, and cybersecurity research to demonstrate how Ransomware-as-a-Service (RaaS) models have fundamentally transformed the cyber crimeconomy, establishing specialised roles within criminal organisations that resemble legitimate business structures. Further, the establishment and disbandment of prominent ransomware cartels, including the unsuccessful Maze cartel initiative, and the rise of innovative organisational frameworks, such as DragonForce's distributed affiliate branding model, have been discussed. Principal findings indicate that traditional cartel structures have predominantly failed owing to competitive pressures and law enforcement scrutiny, while contemporary ransomware entities persist in evolving towards more robust, decentralised configurations that obscure the distinctions between cybercrime, espionage, and hacktivism.

**Keywords:** Forensic Sciences, Cybersecurity, Cyber Forensics, Cybercrime, Ransomware, Ransomware-as-a-Service, Ransomware cartel, Law enforcement,

PP35

## **A Multilayered AI Framework for Sequential Web Attack Detection and Forensic Reconstruction**

*Sariga V S<sup>1</sup>, Sandra P<sup>1</sup>, Anindita Malik<sup>1\*</sup>*

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Noida, Uttar Pradesh, India, 201303*

<sup>\*</sup>*Corresponding author: [amalik@amity.edu](mailto:amalik@amity.edu)*

### **Abstract**

With the growing sophistication of web-based infrastructures to highly multi-staged cyber-attacks, the conventional signature-based Security Information and Event Management (SIEM) models tend to lack the power of context to respond to attacks. This paper provides an integrated, high-performance web attack detection and forensic analysis framework, specifically designed to be used with large-scale Apache access logs. This paper proposes a four-layer defensive design (1) a rule-based engine to get the immediate recognition of known OWASP payloads (2) a behavioural analytics layer based on Isolation Forest to identify volumetric anomalies and bot-like interactions patterns (3) a deep learning layer based on a pretrained Transformer (BERT) model to identify sequential dependencies and semantic anomalies in HTTP requests and (4) an automated forensic reconstruction engine. The combination of these layers makes the framework to fill the gap between reactive digital forensics and proactive threat detection. One of the major novelties of this work is the Automated Forensic Reconstruction module that matches the heterogenous malicious events into a single, unified Attack Storyboard. The experimental studies of the real-world Apache access logs indicate that this hybrid method attains better detection accuracy of the low-and-slow attacks and it also significantly lowers the rate of false-positives by taking into account of the context in which it operates. This framework then converts the millions of raw logs entries into incident-ready intelligence that is structured in a way that actionable reports can be given to forensic investigators that will give details of the intent and mode of entry by the adversary. This research provides a robust, modern approach to bridging the gap between real-time threat detection and automated digital forensic investigation.

**Keywords:** Framework, threat detection, Hybrid Methods, forensic reconstruction, Cyber attack

**PP36**

**Real-Time Human Violence Detection and Alert System Using Deep Learning for Smart Surveillance**

*Sandra P<sup>1</sup>, Sithalakshmi<sup>1</sup>, Sonali Kesarwani<sup>1\*</sup>*

*<sup>1</sup>Amity Institute of Forensic Sciences, Amity University, Noida, Uttar Pradesh, India, 201303*

*\*Corresponding author: [sonalikesarwani743@gmail.com](mailto:sonalikesarwani743@gmail.com)*

**Abstract**

The rapid growth of surveillance infrastructure has significantly increased the demand for intelligent systems capable of proactively identifying violent activities in real time. Traditional monitoring systems rely heavily on human operators, which are often inefficient, error-prone, and unable to respond promptly during critical situations. This study proposes a real-time automated violence detection system based on webcam real-time detection to enhance surveillance effectiveness and public safety. The proposed system utilizes deep learning techniques to analyze live webcam video streams, where video frames are processed to extract spatial and temporal features representing human actions. A trained deep learning model is employed to classify activities as violent or non-violent with high accuracy while minimizing false alarms and maintaining reliable detection performance. Upon detecting a violent event, the system automatically triggers an alert mechanism to notify concerned authorities immediately, enabling faster intervention. Experimental evaluation demonstrates that the model effectively distinguishes violent actions from normal activities across diverse real-world scenarios and maintains strong classification performance with real-time responsiveness. The proposed system enhances traditional surveillance by enabling intelligent, automated monitoring through webcam-based deployment. It offers a scalable, cost-effective, and efficient solution for improving safety in public spaces, educational institutions, and commercial facilities, thereby contributing to the development of smart security environments.

**Keywords:** Violence Detection, Deep Learning, Webcam Surveillance, Real-Time Monitoring, Computer Vision, Human violence

**PP37**

**A Forensic Approach to Assess Evidence Integrity Using Mobile Evidence Verifier**

Samita Singh<sup>1</sup>, Vinayak Gupta<sup>1\*</sup>

<sup>1</sup>*Department of Forensic Sciences, School of Bio-Engineering and Bio-Sciences, Lovely Professional University, Phagwara-144411, Punjab*

*\*Corresponding Author: [vinayakgupta224@gmail.com](mailto:vinayakgupta224@gmail.com)*

**Abstract**

In today's digital era, mobile phones have become a necessity rather than a choice. The landscape of digital evidence has transformed drastically, with mobile devices serving as a primary source of information. It stores a vast amount of user activity, such as calls, messages, app data, browsing history, location, etc. Investigators depend heavily on this extracted data to reconstruct events and support legal conclusions. However, a critical challenge in mobile forensics is that extracted digital evidence is often assumed to be reliable without verifying whether it is logically consistent with actual device behaviour and user activity. Recognising the possibility of manipulated or system-generated inconsistencies is essential in any mobile evidence verification framework. Failure to assess such discrepancies can lead to incorrect conclusions, wrongful attribution, or challenges in court regarding the authenticity of the evidence. Subsequently, anti-forensic techniques, data manipulation tools, and privacy-preserving technologies have raised serious concerns regarding the authenticity of mobile-derived evidence. Thus, a mobile evidence verifier, a forensic-based approach has been designed to examine the integrity and authenticity of mobile data by linking device behaviour with actual user activity. The system analyses extracted data, studies behavioural patterns, and checks for logical consistency between user interactions and recorded device events. By identifying contradictions, suspicious timelines, or unusual activity patterns, it helps investigators distinguish genuine evidence from potentially manipulated or misleading data. The ultimate goal is to enhance evidence credibility, support forensic decision making, and generate clear, structured reports that strengthen investigative conclusions.

**Keywords:** Forensic Sciences, Digital Forensics, Mobile Forensics, Digital Evidence Verification, Mobile, Data Integrity, Metadata Analysis, Evidence Reliability.

**PP38**

**Adaptive Defence Against LLM-Driven Attackers via Dynamic Honeypots and Intelligent IDS Optimisation in AD/IoT**

Sithalakshmi P<sup>1</sup>, Sariga V S<sup>1</sup>, Sonali Kesarwani<sup>1\*</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Noida, Uttar Pradesh, India, 201303*

<sup>\*</sup>*Corresponding author: [sonalikesarwani743@gmail.com](mailto:sonalikesarwani743@gmail.com)*

**Abstract**

The large Active Directory (AD) and IoT-integrated modern enterprise networks are experiencing more intelligent adversaries that use Large Language Models (LLMs). The conventional fixed honeypot implementations and signature-based Intrusion Detection System (IDS) are ineffective in adjusting to learners and evaders. The current study is a response to the problem of resisting adaptive LLM-driven attackers in large-scale, heterogeneous network topologies. A dynamic cyber deception system was developed that combines adaptive relocation of honeypots, ML-based attack classifier, behaviour prediction models and optimisation of IDS feedback. The adaptive evasion model of an LLM-driven attacker is trained to simulate attacks on various topologies of the network. The defence system keeps assessing attacker risk scores, initiates movement of intelligent honeypots and optimises IDS decision thresholds. Experiments with cross-topology transfers determine scalability and generalisation with diverse AD/IoT network architectures. The experimental analysis shows better performance of detection, shorter attacker dwell-time and higher accuracy of IDS in the case of experimental deployment compared to deployment in a static environment. Behavioural prediction with the use of machine learning and adaptive honeypot movement produces a huge amount of uncertainty in the attackers and improves early detection, respectively. Cross-topology analysis enables the verification of the robustness and scalability of the proposed framework. In this paper, it is demonstrated that incorporating dynamic deception and adaptive optimisation of IDS is effective in countering evasion strategies based on the use of LLM. The model supports intelligent, scalable, and cyber defence of contemporary enterprise AD/IoT systems and helps to build resilient and self-adaptive security architectures.

**Keywords:** Adaptive Cyber Defence, Dynamic Honeypots, LLM-based Attackers, Intrusion Detection Systems, Active Directory Security, IoT Security, Cross-Topology Transfer, Behavioural Prediction

**PP39**

**Comparative study of open source- AI tools and conventional tools for vulnerabilities assessment**

Abhishek Kushwaha<sup>1</sup>, Kajal sharma<sup>1</sup>

<sup>1</sup>*University of Lucknow, Lucknow*

*Kushwahaabhishek606@gmail.com*

**Abstract**

Comparative study of open source- AI tools and conventional tools for vulnerabilities assessment IN the fast-changing environment of cyber threats that we live, it is important to consider the effectiveness of vulnerability assessment tools to maintain the integrity of digital forensics and ensure the security of systems. This research investigates and provides a comparison of open-source AI tools (Pentest-Tools and Cyber Scan.io) and conventional tools (Nessus and OWASP ZAP) in a comparative study of their efficacy, accuracy, and capacity to discover web-based vulnerabilities. To be part of this work, a university website was scanned in a controlled environment and performance reviewed utilizing a number of bench marking results, for example: encryption, cookie security, report presentation, and the ability to detect SQL injection, cross site scripting, and cross site request forgery. The findings shown that traditional scanners like ZAP and Nessus were more effective in uncovering known vulnerabilities with detailed reports and structured evidence in comparison to the quick scanning, automated AI-based tools, AI-based tool provided scanning, automation, and prediction, however, on detecting advanced and application-level threats it fell short. The report highlights that AI supports speed and reduces false positives, performing most effectively in conjunction with traditional tools to support security. This comparative evaluation emphasizes the increasing necessity of hybrid vulnerability assessment models. By leveraging the ongoing adaptive intelligence of AI tools and the analytical depth of traditional scanners, hybrid vulnerability assessment models provide accuracy, efficiency, and resilience in proactive cyber security efforts and digital forensic investigation.

**Keywords:** Vulnerability Assessment, Forensic Science, OWASP ZAP, Nessus, Pentest-Tools, Cyber Scan.

**PP40**

**Cloud Forix: An Integrated Solution for Cloud Forensic Investigation**

Yash Bhardwaj<sup>1</sup>, Kritika Singh<sup>1</sup>, Sourabh Kumar Singh<sup>1\*</sup>

<sup>1</sup>*Department of Forensic Science, School of Basic and Applied Sciences, K.R. Mangalam  
University, Sohna, Haryana, India - 122103*

*\*Correspondence mail: [singhsourabhkumar033@gmail.com](mailto:singhsourabhkumar033@gmail.com)*

**Abstract**

Cloud computing has enhanced the storage and processing of data yet it has posed new challenges in the digital forensic studies. Such cloud features as multi-tenancy, dispersed data, and inability to access physical data restrict the use of traditional methods. Traditional methods such as using FTK(FORENSIC TOOL KIT), AUTOPSY, TSK (THE SLEUTH KIT), etc. these are used in combination in order to obtain a good result because a single tool can not do everything. A recent study shows that due to metadata analysis and log extraction the percentage of encryption key recovery is 65% which was less than 5% Using earlier methods also the session reconstruction was 80% which was 35% using earlier methods along with it behaviour pattern analysis is 70% better than earlier which was 30% only. This study suggests a cloud forensic system which will allow to collect the evidence automatically, to analyze the logs in the specified way and verify the data integrity. The tool can be used with various cloud models (IaaS,PaaS, SaaS) and can help to increase the efficiency of the investigation, improving evidence collection, finding unauthorised access, and ensuring the preservation of reliable forensic information.

**Keywords:** Cloud Forensics, Cloud Models, Evidence Acquisition, Data Integrity, Chain of Custody, Data Breach, Unauthorized Access.

**PP41**

**Tracing Digital Assets in Insolvency Proceedings: The Evolving Role of Cyber Forensics in Combating White-Collar Crime**

Pihu Mishra<sup>1</sup>, Amit Dhall<sup>1\*</sup>

<sup>1</sup>*Amity Law School Noida, Amity University Noida, Uttar Pradesh, India*

*\*Corresponding Author: [adhall@amity.edu](mailto:adhall@amity.edu)*

**Abstract**

The insolvency and bankruptcy code, 2016 has provided a structured mechanism for identification of Preferential, Undervalued, Fraudulent and Extortionate (PUFE) transactions. These are the transactions which corporate debtors use to move the assets away from creditors before initiation of insolvency. The motive of behind these transactions is malignant personal interest of the debtors. The provisions of the Code are designed to prevent asset erosion as well as to safeguard the creditors interests. With the growing dependency on digital financial systems, the nature and execution of PUFE transactions have also evolved. Now such transactions are carried out through advanced use of technology, which is hard to trace and reverse, aligning such transactions with the domain of white-collar crimes.

This paper seeks to explore the emerging relationship between PUFE transactions and cyber-enabled financial misconduct. It contends that the misuse of digital platforms, electronic fund transfers, and virtual assets has enabled corporate actors to structure transactions in a manner that conceals intent, fragments audit trails, and complicates detection. Practices such as routing funds through layered digital accounts, manipulating electronic records, and transferring value through decentralised systems often mirror the characteristics of fraudulent and undervalued transactions under the IBC framework. As a result, traditional methods of identifying suspect transactions may prove inadequate in addressing these technologically mediated forms of asset diversion. The research emphasises the importance of cyber forensic techniques in insolvency proceedings. Digital tools for mapping transactions and recovery of electronic data and using blockchain analytics to assist resolution professionals in uncovering concealed transactions and establishing evidentiary links are necessary for avoidance actions. The paper also explains existing legal frameworks and highlights the challenges relating to evidentiary standards and investigative capacity when dealing with digital financial misconduct. By situating PUFE provisions within the broader context of cyber law and white-collar crime, the paper argues for a more technologically responsive insolvency regime. Such an approach would not only improve asset tracking and recovery but also strengthen the overall credibility and effectiveness of insolvency processes in a rapidly evolving digital economy.

**Keywords:** Digital Assets, Cyber Forensics, Insolvency Law, White-Collar Crime, Asset Tracing, Corporate Fraud.

**PP42**

**Automotive Cybersecurity in Transition: Thorough analysis on the challenges of Intelligent Connected Vehicle Networks communication and its industrial framework**

Ashish Shukla<sup>1</sup>, Rajni Sehgal<sup>1</sup>, Deepti Mehrotra<sup>2</sup>

<sup>1</sup>*Amity School Engineering and Technology, Amity University Uttar Pradesh, Noida, INDIA*

<sup>2</sup>*Accreditation, Ranking and Quality Assurance, Jaypee Institute of Information Technology, Noida, India*

*[mehdeepti@gmail.com](mailto:mehdeepti@gmail.com)*

**Abstract**

The rise of intelligent connected vehicles (ICVs) has introduced never done opportunities in safety, efficiency and user experience. while simultaneously exposing modern vehicles to complex cybersecurity threats. This paper presents a thorough analysis of the risks and vulnerabilities built-in ICVs communication: pre-communication, during- communication and post-communication. Examining key attack surfaces such as V2X communication interfaces, infotainment systems, over-the-air (OTA) update mechanisms and safety-critical cyber-physical systems. Existing industry standards and regulations, including ISO/SAE 21434, UNECE WP.29 and IEEE 1609.2, are discussed as foundational mitigation frameworks. We also review notable real-world attacks and research demonstrations that highlight gaps in current security practices. The paper concludes by exploring emerging technologies such as artificial intelligence, 5G and edge computing, which both advance and complicate the security landscape, emphasizing the need for adaptive, scalable and lifecycle-oriented cybersecurity strategies in the automotive domain. This comprehensive examination contributes to a deeper understanding of the subject, set the stage for future advancements in this dynamic field.

**Keywords:** intelligent connected vehicles (ICVs), V2X, over-the-air (OTA)



AMITY UNIVERSITY  
UTTAR PRADESH



PP43

## Artificial Intelligence and Digital Forensics in Crime Scene Investigation: Transforming Modern Criminal Justice

Sheeba Ahad<sup>1</sup> and Abhitendra Singh<sup>1\*</sup>

<sup>1</sup>Amity Law School, Amity University, Noida

\*Corresponding Author: [sahad@amity.edu](mailto:sahad@amity.edu), [abhitendrasingh12@gmail.com](mailto:abhitendrasingh12@gmail.com)

### Abstract

The recent accelerated growth of cybercrime, online transactions, and technologically advanced criminal activities has made the conventional crime scene investigation techniques less effective in providing timely and correct quality justice. In the present Crime scene Investigation (CSI), the paper discusses the revolutionary interplay between Artificial Intelligence (AI) and Digital Forensics and how this convergence is reconfiguring the face of criminal justice delivery in India and the world at large. The study is doctrinal and analytical, as it is based on the primary sources including the statutes especially on the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, and the Bharatiya Nagarik Suraksha Sanhita, 2023, and the example of secondary sources is the landmark judicial decision on the case of Anvar.

This paper explores how AI tools, such as machine learning algorithms, convolutional neural networks, facial recognition systems, predictive policing models, and large language model-assisted forensic image analysis, can be used to supplement the efficiency, speed, and objectivity of crime scene reconstruction and evidence processing. At the same time, it examines the separate but inter-related field of digital forensics, which includes computer forensics, mobile device forensics, network forensics, and cloud forensics, to the recovery, preservation, and admissibility of computer evidence. The key observation of the paper is that although AI proves to be measurably more efficient in crunching huge bodies of evidentiary data and pattern recognition, recent empirical evidence (Farber, 2025, Journal of Forensic Sciences) has shown the technology to score 7.8 in its performance when applying to homicide cases, meaning that AI is not a replacement to human forensic judgment, but an effective aid to it.

The article critically analyses the legal and evidentiary framework, which regulates AI-generated evidence and digitally derived evidence within India courts. It indicates that the Bharatiya Sashaya Adhiniyam, 2023, does not only recognize the electronic records as the primary evidence in accordance with the Section 57, but it also facilitates the certification in accordance with the Section 63, which does not directly address the machine-generated outputs or AI-processed forensic data, which creates significant gaps in the jurisprudence.. The paper also discusses such ethical and constitutional issues as bias in algorithms, mass surveillance, the right to privacy as established in Justice K.S. Puttaswamy v. Union of India



AMITY UNIVERSITY  
UTTAR PRADESH



(2017), and the danger of miscarriage of justice when judges blindly follow the output of algorithms.

The paper, based on comparative analysis of forensic AI adoption in the United States and the United Kingdom, provides best practices and suggests certain legislative changes, such as specific provisions of AI-generated forensic evidence, necessary validation frameworks of the AI tools used in criminal cases investigation, development of national forensic infrastructure, and ethically controlled by courts. It is concluded that the mutual integration of AI and digital forensics in a strategic and regulated way has the potential to transform the process of delivering justice faster, improving the accuracy of the investigation process, and future-proof the Indian criminal justice system against the challenges of an increasingly digital and algorithmically mediated society, but only when this integration is informed by the principles of rigorous legal standards, ethical controls, and constitutional protections.

**Keywords:** Artificial Intelligence, Digital Forensics, Crime Scene Investigation, Bharatiya Sakshya Adhiniyam 2023, Admissibility of Digital Evidence, Algorithmic Bias, Criminal Justice Transformation

PP44

**The Similarities Between Initial and Full-Length Signature**

Ruchi Mishra<sup>1\*</sup>, Aradhna<sup>1</sup>, Karam<sup>1</sup>

<sup>1</sup>*Department of Forensic Science, Usha Martin University, Ranchi*  
*[ruchi.mishra@umu.ac.in](mailto:ruchi.mishra@umu.ac.in)*

**Abstract**

Signatures have become a means of authentication for an individual in offices, banks, for decades. Time is the most important thing that a human being has. To save time writers start developing the initial and abbreviation of their full length signature. When someone uses initial signatures it totally depends upon the personal choice that could resemble the features of full length signature but it is not necessary. It may be totally different from a full length signature. Handwriting depends on many factors that lead to natural variation.

The study focuses on the comparison of full length signatures and initial signatures. In the study we collected initial and full length signatures from 100 participants aged between 20-40 years in standard sitting position on A4 size paper from black ball pen. 10 samples of initial and full of the is collected from an individual. Then the signatures are analysed on the basis of individual and class characteristics. The initial signatures are generally simpler than full length signatures. The handwriting features of an individual don't change after a certain age, these features are very useful in finding out the similarities between both types of signature.

The findings of the study are features like letter formation, initial stroke, connecting stroke, pen lifts, rhythm are similar in initial and full length signature; it marks that the authenticity and verification of an individual can be done from initial signature.

**Keywords:** Full length signature, Initials, Similarities, Individual Characteristics, Authenticity.

PP45

**Comparative Analysis of Initial and Full Signatures in Forensic Document Examination**

Aradhna<sup>1</sup>, Karam Rai<sup>1</sup>, Ruchi Mishra<sup>1\*</sup>

<sup>1</sup>*Department of Forensic Science, Usha Martin University, Ranchi*

<sup>\*</sup>*Corresponding Author: [ruchi.mishra@umu.ac.in](mailto:ruchi.mishra@umu.ac.in)*

**Abstract**

Signatures have become a means of authentication for an individual in offices, banks, for decades. With the increase in its importance many individuals adopt abbreviated signature in place of full-length signature. The development of initial signature is a matter of personal preference that may show some similarity with the full-length signature. The present study focuses on the comparative examination of full-length and initial signatures to determine the similarity in the characteristics of an individual's signature. A total of 100 participants aged between 20-40 years were included in the study. From each individual, 10 samples each of initial signatures and full-length signature were collected under standard sitting condition using black ball point pen on A4 paper. The collected samples were analyzed for both class and individual characteristics such as letter formation stokes, pen lifts, rhythm, slant, alignment, hesitation, diacritics (dots and bar) etc. Observation revealed that although initial signatures are generally simpler and abbreviated than full-length signatures, several handwriting features such as stoke, rhythm and movement pattern remained consistent between the two. The initial signature often has more embellishment possibility due to faster execution. The signatures show persistent similarity between the initial and full-length signature supporting the forensic reliability of initial signature as a valid tool for authentication and identification.

**Keywords:** Full length signature, Initials signature, Individual Characteristics, Authenticity.

PP46

## Development of Aged Fingerprints Using Different Techniques: A Review

Tanya Kaushik<sup>1</sup>, Pallavi Thakur<sup>1\*</sup>

<sup>1</sup>*Amity Institute of Forensic Sciences, Amity University, Noida, Uttar Pradesh, India*

*\*Corresponding Author: [pthakur1@amity.edu](mailto:pthakur1@amity.edu)*

### Abstract

Fingerprints are one of the most infallible form of identification in forensic investigations; however, the development of aged latent fingerprints presents various scientific and practical challenges. Over time, environmental exposure, surface characteristics, and chemical degradation alter the composition of fingerprint residues, making their visualization increasingly difficult. This review paper critically examines various traditional and advanced techniques used for the development of aged fingerprints on different substrates. Various methods including powder-based approaches, chemical reagents, and instrumental techniques are analyzed for their effectiveness, limitations, and suitability under fluctuating parameters. Particular focus on factors affecting fingerprint persistence and the importance of selecting an appropriate technique according to surface type and age of the fingerprint. The review emphasis comparative findings from existing literature and identifies current research gaps in enhancing sensitivity and reliability of fingerprint development methods. Overall, the study provides a comprehensive understanding of the challenges related with aged fingerprint development and suggests directions for improving forensic application and methodological advancements.

**Keywords:** Aged fingerprints, latent prints, fingerprint development, chemical methods, forensic science, persistence

PP47

**Software Based Detection and Analysis of Signature**

Shivani Singh<sup>1</sup>, Raushani Singh<sup>1</sup>, Diksha Priya<sup>1</sup>, Anmol Kaur<sup>1</sup>, Mandeep Kaur<sup>1</sup>, Trisha Barua<sup>1</sup>

<sup>1</sup>*Lovely Professional University, 144411, Punjab*  
[shivinishil82@gmail.com](mailto:shivinishil82@gmail.com)

**Abstract**

A signature is a major means of identification and authentication of a person. Forgery of a handwritten signature is a concern in many fields, such as financial, legal, and Law Enforcement Sector. The proposed Forged Signature Detection System aims to classify a signature as genuine or forged using an AI Siamese Vision Transformer (ViT). In this AI, break the signature into small squares to follow the flow of writing. “Micro-Habits”, Unusual Formation, Angle, Specific letter shapes are kept under observation. It turns these details into two parameters, i.e., class and individual characteristics; if the characteristics parameter for two signatures are close together, the signature is real, but if they are far apart, it is flagged as a fake. Apart from this, the Digital Chain of Custody is also added. The “Zero-Tolerance Scoring”, 99% is genuine, and <50%Forgery results are used as a “Cliff-edge” scoring formula. The use of plain (unruled) paper for signature acquisition yields more accurate results, as ruled paper introduces background line patterns that act as visual noise during image processing. This noise interferes with feature extraction and segmentation, thereby reducing the overall performance and reliability of the signature verification system. Furthermore, the integration of a Digital Chain of Custody ensures evidentiary integrity and accountability, making the system suitable for financial, legal, and law enforcement applications.

**Keywords:** Siamese ViT, Micro-Habits, Cliff-Edge Scoring, Digital Chain of Custody, Authentication.

PP48

## **Comparative Analysis of Fingerprint Identification System: NGI(USA) Vs NAFIS (INDIA)**

*Ayush Chauhan<sup>1</sup>, Tuba Jamal<sup>1</sup>, Jyoti Singh*

*<sup>1</sup>Amity Institute of Forensic Sciences, Amity University Uttar Pradesh, India, 201303*

*\*Corresponding Author: [jsingh4@amity.edu](mailto:jsingh4@amity.edu)*

### **Abstract**

Biometric identification has become central to modern policing, with Automated Fingerprint Identification Systems (AFIS) enabling rapid comparison of fingerprints against large databases. This paper compares two major implementations: the FBI's Integrated/Next Generation Identification systems (IAFIS/NGI) in the United States and India's National Automated Fingerprint Identification System (NAFIS), a nationwide criminal fingerprint platform managed by the National Crime Records Bureau (NCRB). Using a structured review of technical documentation, standards and policy reports, the study examines system architecture, data formats, operational workflows and governance. Particular focus is placed on Electronic Biometric Transmission (EBTS) based, American National Standard Institute/National Institute of Standards and Technology (USA) (ANSI/NIST) compliant interoperability in the U.S. and on National Automated Fingerprint Identification System(NAFIS)'s National Institute of Standards and Technology (NIST) compliant design, integration with Crime and Criminal Tracking Network (CCTNS) and Inter-operable Criminal Justice System (ICJS), and the use of lifetime National Fingerprint Numbers (NFN) in India. The analysis shows that Next Generation Identification (NGI) offers broader biometric coverage, higher transaction capacity and greater algorithmic maturity at the global level, whereas National Automated Fingerprint Identification System (NAFIS) delivers significant context-specific benefits in India by replacing fragmented, slip-based and Fingerprint Analysis & Criminal Tracing System (FACTS) driven processes with a single, real-time national repository containing over one crore criminal fingerprint records. The paper concludes that, while Next Generation Identification systems (NGI) is more advanced in overall technical capability, NAFIS is better aligned with India's policing needs; together, India's centralized model and the United States' federated, multi-AFIS ecosystem represent complementary approaches whose combined lessons can guide the development of future interoperable, multimodal and privacy-conscious identification systems.

**Keywords:** Automated Fingerprint Identification System, Next Generation Identification System, National Automated Fingerprint Identification System, Criminal Justice System, Interoperability.

**PP49**

**Dead Men Tell Tales: Evaluating the Reliability of Postmortem Toxicology in Judicial Proceedings**

Akriti Shukla<sup>1</sup>, Manish Mishra<sup>2</sup>, Amit Dhall<sup>1\*</sup>

<sup>1</sup>*Amity Law School Noida, Amity University Noida, Uttar Pradesh, India*

<sup>2</sup>*Amity Institute of Forensic Sciences, Amity University Noida, Uttar Pradesh, India*

\*Corresponding Author: [adhall@amity.edu](mailto:adhall@amity.edu)

**Abstract**

**Introduction:** Postmortem toxicology is an essential component of forensic research, especially in cases involving poisoning, drug overdose, and unexplained fatalities. By making it easier to identify and interpret harmful compounds in biological specimens after death, it provides vital scientific evidence for diagnosing the cause of death and proving criminal culpability. The Indian Evidence Act (1872) recognizes its evidential character as expert opinion. Despite its relevance, worries about its trustworthiness remain owing to postmortem metabolic changes, such as redistribution, decomposition, and environmental contamination.

**Methods:** This study uses a doctrinal and analytical research technique, which includes a thorough analysis of the forensic toxicological literature, recognized scientific principles, and legal precedents. The influence of postmortem modifications on toxicological interpretation is examined, as well as the legal disposition of such evidence, using case law analysis, notably *Sharad Birdhichand Sarda v. State of Maharashtra*.

**Result:** While postmortem toxicity is influenced by biological and environmental factors, these variables have been widely investigated and effectively minimized using enhanced analytical methods, multi-site sampling, and standardized interpretation processes. Judicial trends show that toxicological findings are considered reliable when backed by scientific rigor and corroborative evidence, resulting in a cohesive and full evidential chain.

**Conclusion:** Postmortem toxicology, while not without limits, is a scientifically sound and legally required tool in forensic adjudication. Its reliability is dependent on thorough scientific application and contextual legal review. When combined with medical, circumstantial, and investigative evidence, it greatly improves the evidential framework, aiding in the precise and efficient administration of justice.

**Keywords:** Postmortem Toxicology; Forensic Evidence; Expert Opinion; Cause of Death; Evidentiary Reliability; Poisoning; Criminal Law

PP50

**Forensic Entomology of Decomposition: Stage-Wise Insect Succession and Ecological Metrics for PMI Estimation in Jharkhand**

Disha Bhoot<sup>1</sup>, Sonali Suman<sup>1</sup>, Shreya Kumari Jaiswal<sup>1</sup>, and Madona Mathew<sup>1</sup>

<sup>1</sup>*Department of Forensic Science, Usha Martin University, Jharkhand*  
*[dishabhoot9@gmail.com](mailto:dishabhoot9@gmail.com)*

**Abstract**

Forensic entomology provides a critical, evidence-based tool for estimating the post-mortem interval (PMI) through analysis of insect succession, developmental stages, and ecological interactions. This study presents a 30-day field investigation in Angara, Jharkhand, integrating stage-specific insect succession, ecological indices, successional turnover, and environmental parameters for forensic PMI assessment. Systematic monitoring identified five decomposition stages: fresh (0–1 days), bloated (2–5 days), active decay (7–14 days), advanced decay (15–22 days), and dry/remains (23–30 days). Pre-appearance interval (PAI) analysis indicated rapid early colonization by dipterans (*Musca domestica*, blowflies, flesh flies) within 0–2 days, followed by beetles, cockroaches, and late-stage ants. Relative abundance analysis showed early blowfly dominance (48%), mixed assemblages during active decay, and ant predominance in late stages. Functional classification revealed necrophagous taxa as 60% of early-mid stage assemblages, with predatory (25%) and opportunistic (15%) taxa increasing in later stages. Ecological indices quantified faunal patterns: Shannon diversity ( $H' = 1.269$ ) reflected moderate diversity, Simpson index ( $D = 0.336$ ;  $1-D = 0.664$ ) indicated balanced dominance, and Pielou's evenness ( $J' = 0.782$ ) peaked during active decay. Margalef richness index ( $R = 2.48$ ) confirmed maximum species richness mid-decomposition. Successional turnover rates were highest between bloated and active decay phases (0.62), highlighting rapid community restructuring. Statistical correlation analysis showed significant relationships ( $p < 0.05$ ) between temperature, humidity, and faunal abundance, confirming environmental influence on decomposition rate. The study demonstrates that integration of insect succession, ecological indices, successional turnover, and environmental parameters provides a robust, multi-dimensional framework for region-specific PMI estimation. Applications include accurate PMI reconstruction, validation of index-supported predictive models, and forensic casework support in tropical regions. This study provides the first comprehensive baseline entomological and ecological dataset for Angara, Jharkhand, offering actionable insights for forensic investigations.

**Keywords:** Forensic Entomology; Post-Mortem Interval; Insect Succession; Ecological Indices; Successional Turnover



AMITY UNIVERSITY  
UTTAR PRADESH



PP51

## Quantitative Digital Morphometry of Calliphoridae Larvae: A Computational Framework for Precision Post-Mortem Interval (PMI) Estimation

Anshnu Tyagi<sup>1</sup>

<sup>1</sup>*National Forensic Sciences University, Delhi*

[anshnu022@gmail.com](mailto:anshnu022@gmail.com)

### Abstract

The accurate estimation of the Post-Mortem Interval (PMI) is a cornerstone of forensic pathology, yet it remains susceptible to significant margin-of-error during advanced decomposition. While the developmental progression of Calliphoridae (blowflies) serves as a gold-standard biological chronometer, traditional methodologies rely on manual vernier caliper measurements and subjective instar staging, which are inherently prone to inter-observer variability and specimen degradation. This study introduces Entomo-AI, a multidisciplinary framework designed to digitize and automate the forensic entomology workflow. The proposed system utilizes a customized macro-imaging interface to capture high-resolution specimen data, which is then processed through a computer vision pipeline. By implementing Otsu's Adaptive Thresholding for foreground segmentation and Contour-based Feature Extraction, the framework achieves precise measurement of larval surface area and major-axis length with sub-millimeter accuracy. These biometric indices are integrated into a Growing Degree-Day (GDD) regression model:  $GDD = \sum(T_{avg} - T_{base})$ . This mathematical modeling allows for the dynamic mapping of biological growth against site-specific ambient temperature variables. Preliminary validation of the Entomo-AI prototype indicates a 94% classification accuracy across three larval instars, outperforming traditional microscopic analysis in both speed and reproducibility. Furthermore, the system reduces total processing time by 85%, facilitating rapid field-based assessments. By establishing a verifiable and tamper-proof digital record of biological evidence, this research aligns with the Daubert Standard for legal admissibility and addresses SDG 9 (Industry, Innovation, and Infrastructure). Ultimately, this framework provides a scalable, objective, and computationally rigorous solution for modernizing crime scene management and forensic medicine.

**Keywords:** Forensic Entomology, Post-Mortem Interval (PMI), Digital Morphometry, Computer Vision, Instar Classification, Thermal Regression, Daubert Standard, Automated Feature Extraction, Calliphoridae, Crime Scene Management.

PP52

## **CT-Based Bone-to-Soft Tissue Nasal Morphometric Correlation and Its Forensic Implications in the Northwest Indian Population**

Mohinder Sharma<sup>1\*</sup>, Sushil Kumar Battana<sup>1</sup>

<sup>1</sup>*Department of Radio-Diagnosis & Imaging, PGIMER, Chandigarh*

*\*Corresponding Author: [vickymahi31@gmail.com](mailto:vickymahi31@gmail.com)*

### **Abstract**

**Background:** Accurate prediction of nasal soft tissue morphology from underlying skeletal structures remains a major challenge in forensic facial approximation. While computed tomography (CT) enables precise visualization of both bony and soft tissue components, population specific bone-to-soft tissue correlation data are limited in the Indian context. This study aimed to evaluate the relationship between bony nasal parameters and corresponding soft tissue measurements in a Northwest Indian adult population.

**Methods:** A retrospective cross-sectional study was conducted on 277 adult CT scans (known sex; age 18–80 years). Individuals with craniofacial trauma, deformity, or pathology were excluded. Standardized mid-sagittal and axial reconstructions were used to measure: bony nasal height, soft tissue nasal height, bony nasal protrusion depth, soft tissue protrusion depth, and anterior nasal spine angle. Pearson correlation analysis and linear regression modeling were performed to assess bone-to-soft tissue relationships. Statistical significance was set at  $p < 0.05$ .

**Results:** Significant positive correlations were observed between bony and soft tissue parameters. Bony nasal height demonstrated strong correlation with soft tissue nasal height ( $r = 0.72$ ,  $p < 0.001$ ). Bony protrusion depth showed moderate-to-strong correlation with soft tissue protrusion ( $r = 0.68$ ,  $p < 0.001$ ). The anterior nasal spine angle correlated moderately with the nasolabial angle ( $r = 0.59$ ,  $p < 0.001$ ). Linear regression analysis indicated that bony nasal height explained approximately 52% of the variance in soft tissue nasal height ( $R^2 = 0.52$ ).

**Conclusion:** CT-derived bony nasal parameters demonstrate significant predictive value for corresponding soft tissue morphology in the Northwest Indian population. These findings support the applicability of bone-based regression models in forensic facial approximation and highlight the importance of population-specific standards. Further validation may enhance the accuracy of nasal reconstruction in medico-legal contexts.

**PP53**

**Estimation of sex in Indian population with computed tomographic imaging technology from Dorso-lumber vertebrae- A forensic Radiological Approach**

Sushil Kumar Battan<sup>1\*</sup>, Mohinder Sharma<sup>2</sup>, Mandeep Garg<sup>1</sup>, Paramjeet Singh<sup>1</sup>, Priyanka Verma<sup>2</sup>

<sup>1</sup>Department of Radio-Diagnosis and Imaging, PGIMER, Chandigarh, India,

<sup>2</sup>Department of Forensic Science, Chandigarh University, Punjab, India, Email:

\*Corresponding author, Email: [battansushil@gmail.com](mailto:battansushil@gmail.com)

**Abstract**

**Background:** It is very crucial on the crime scene to estimate the accuracy of sex when bones of skeletal of human being extracted are available in limited scope. Last few decades the molecular science plays a significant role in forensic science for identification of sex but still anthropological methods are still very historic tools in the field of medical legal activities. Our study may be proven as milestone for sex estimation from Dorso-lumber vertebrae in region specific population.

**Material:** We have studied 467 subjects (230 male and 237 females) with age range from 18 years to 80 years vertebral columns of Indian population for sex estimation to establish the accuracy. The said data has been collected in digital form (DICOM images) from Computed Tomographic Imaging Technology. D-12 and L-1 Vertebrae of Human Body have been measured in linear pattern. All the quantitative variables (23) of different sex were analysed with descriptive and discriminant function analysis. The SPSS software (ver. 23; SPSS Inc., Chicago, IL) was used to assess the variables. After determining the mean and standard deviations for each variable, the differences between the genders were analysed using Student's t-test. P values less than 0.01 were considered statistically significant. Univariate and multivariate discriminant function analyses were applied to the measured parameters to determine predictive rates of sex.

**Results:** Lumbar (L-1) and D-12 vertebrae show a statistically significant sexual dimorphism with higher means in males as compared to females. In the lumbar vertebra, the sexual dimorphism is statistically significant in the width and total depth of the vertebra, all the variables of the vertebral body, and the width of the spinal canal. The equations developed in this study show >90% accuracy in both sex.

**Conclusion:** Our study is the first study in which D-12 and L1 vertebrae were examined with the purpose of sex estimation in the Indian population and we think that our data will be an important reference for sex estimation from the D-12 and L1 vertebrae in the Indian population.

**Keywords:** Forensic anthropology, Sexual dimorphism, Sex estimation, Dorso-lumbar vertebra

**PP54**

**Forensic Entomology: Role of Insects in Post-Mortem Interval Estimation - A Review**

Shweta, Kajal Sharma

*Department of Forensic Science, Chandigarh University*

*shwetasharma.simi@gmail.com*

**Abstract**

Finding post-mortem interval (PMI) is the most important and challenging step during the investigation. PMI is the time that has passed since death, and its accurate estimation helps in aiding the timelines or events during crime scene investigation. Forensic entomology is the most reliable and practically accepted method for time of death estimation.

Forensic entomology is the study of insects and other arthropods in criminal investigations. This review mainly focuses on studying and combining previous studies about the role of insects in determining PMI, factors affecting accuracy and recent developments in this field.

This review was done after proper analyzing research papers (2000-2024). Various sources like Google Scholar, PubMed, ScienceDirect with keywords related to forensic entomology and death time estimation were used. A total of 15 important studies were considered based on relevance.

It is found that the first insects which reach to the body are blowflies. Species like *Calliphora vicina*, *Lucilla sericata*, etc are included in this. Methods used in this are ADH (accumulated degree hours) and ADD (accumulated degree days). Insects appear in a predictable way and at different stages (fresh, bloated, active decay, advanced decay and dry stages). Each stage consists of different insects. There are many technological advancements like DNA-based identification which are very helpful as they improved the accuracy, specially in complex cases. After proper study, it is found that PMI can be estimated successfully from days to several weeks by examining insects' activity.

**Keywords:** Forensic entomology, post-mortem interval, Blowfly arrival sequence, Death investigation, Carrion insects.

**PP55**

**From Behavioral Inference to Neural Evidence: A Doctrinal and Comparative Analysis of Criminal Profiling and Brain Fingerprinting in Criminal Investigations**

Reema Bharrahcarya<sup>1</sup>

<sup>1</sup>*Jagannath University Delhi NCR, Bahadurgharh*  
*[reema.bhattacharya11@gmail.com](mailto:reema.bhattacharya11@gmail.com)*

**Abstract**

The rapid advancement of forensic science has transformed criminal investigations from reliance on behavioral inference to the incorporation of neuroscientific techniques. Criminal profiling, grounded in psychological analysis, has traditionally assisted investigators in narrowing down suspects; however, its evidentiary value remains limited due to its inherently subjective nature. In contrast, brain fingerprinting, a technique developed by Lawrence Farwell, claims to detect concealed information through neurophysiological responses, thereby presenting itself as a more objective and scientific alternative. This study undertakes a doctrinal and comparative analysis of these two approaches, examining their admissibility, reliability, and constitutional implications within criminal justice systems. It critically engages with judicial interpretations, particularly the landmark decision in *Selvi v. State of Karnataka*, which underscores the importance of consent and the right against self incrimination. Comparative insights from jurisdictions such as the United States and the United Kingdom further highlight the cautious approach adopted by courts toward neuroscientific evidence. The research finds that while brain fingerprinting offers potential advantages in terms of scientific objectivity, it is not free from concerns relating to accuracy, standardization, and ethical safeguards. The transition from behavioral to neural evidence, therefore, does not signify a complete replacement but rather a complex interplay between traditional investigative techniques and emerging technologies. The study concludes that the integration of such neuroscientific methods must be guided by stringent legal standards and constitutional protections to ensure both effective investigation and the preservation of fundamental rights.

**Keywords:** Criminal Profiling; Brain Fingerprinting; Forensic Neuroscience; Admissibility of Evidence; Self-Incrimination



AMITY UNIVERSITY  
UTTAR PRADESH



PP56

## Examining Correlation Between Secondary Traumatic Stress and Suicidal Harm and Self-Harm in Young Adult Females

Sneha Sagar<sup>1</sup>, Ayushi Shilu<sup>1\*</sup>

<sup>1</sup>*Department of Forensic Science, Usha Martin University, Ranchi*

*\*Corresponding Author: [ayushi.shilu@umu.ac.in](mailto:ayushi.shilu@umu.ac.in)*

### Abstract

With the availability of the internet, the use of social media and other telecasting platforms has increased, providing real-time information to users but also producing many negative impacts on individuals. The content available on digital platforms is largely unfiltered and comes without disclaimers, and this can cause Secondary Stress Trauma (STS), which is a hidden stress that originates when a witness explores a traumatic event after indirect exposure. Females are generally more sensitive toward traumatic thoughts. This study explores the association of Secondary Stress Trauma with self-harm and suicidal ideation arising from content viewed on social media platforms and news channels. Responses were collected from young females aged 16–28 years (N= 150) through self-reported questionnaires including a modified DSM-5 PTSD checklist, the Suicidal Ideation Attributes Scale, and the Self-Harm Inventory (SHI). The results show an inconsistent relationship between secondary stress trauma and self-harm or suicidal ideation: Several participants with elevated STS did not exhibit suicidal ideation or self-harm, whereas some individuals with lower levels of STS reported such tendencies. This indicates that STS alone is not an independent factor influencing suicidal ideation or self-harm, which are instead shaped by a combination of multiple interacting variables, such as emotional resilience, prior trauma exposure, mental health conditions (e.g., depression or anxiety). The findings underscore the importance of media literacy, content moderation, and early psychological screening for young users, and suggest that targeted interventions should strengthen emotional resilience and coping skills. Keywords: Secondary Stress Trauma, Self harm, Suicidal Ideation, social media, news content.

PP57

## The Psychology of Cybercrime: Profiling the Invisible Offender Behind the Screen

Saniya<sup>1</sup>

<sup>1</sup>Noida International University, Greater Noida, India

[sukunaug66@gmail.com](mailto:sukunaug66@gmail.com)

### Abstract

**Introduction:** India recorded over 2.4 million cyber crime incidents in 2023 (NCRB), ranking third globally, yet only 12% of Indian cyber forensic laboratories employ behavioural experts. This critical gap persists despite evidence that 68% of cyber offenders exhibit identifiable psychological patterns invisible to purely digital investigation. Crimes such as social engineering (Bois Locker Room, 2020), dark web operations (NCB drug bust, 2021), cyber terrorism (Bulli Bai App, 2022), and online radicalisation (Kashmir cases) are fundamentally human behavioural phenomena. This study proposes a comprehensive Forensic Psychology–Cyber Integration (FPCI) Framework addressing offender behaviour, victim psychology, and India's legal architecture.

**Methods:** This qualitative study analyses 20 Indian cyber crime cases across five categories: phishing and financial fraud (Jamtara network), digital human trafficking (West Bengal), online radicalisation (Kashmir), dark web narcotics (NCB, 2021), cyber stalking (Ritu Kohli case, 2001), insider corporate theft (Pune BPO, 2005), and group psychopathology (Bois Locker Room, 2020; Bulli Bai App, 2022). Five forensic psychology tools are applied to each case: criminal profiling, deception detection (P300 brain mapping and polygraph), offender psychopathology assessment, victim vulnerability mapping, and social engineering behavioural analysis. Indian IT Act (2000, amended 2008) provisions are examined for capacity to admit behavioural evidence.

**Results:** Four key findings emerge. First, 68% of cyber offenders displayed consistent psychopathological profiles narcissistic and antisocial traits dominated financial fraudsters, while radicalisation cases showed identifiable pre-crime behavioural escalation. Second, 74% of social engineering victims shared identifiable cognitive vulnerability that were predictable and preventable. Third, P300-based deception detection demonstrated 76% accuracy (Knappe et al., 2025), confirming viability in cyber interrogation. Fourth, the FPCI Framework demonstrated explanatory power across all 20 cases.

**Conclusion:** India's investigation framework must integrate forensic psychology alongside digital forensics. This study recommends three urgent reforms: mandatory forensic psychologists in all Cyber Crime Cells; amendment of Section 45A of the Indian Evidence Act to recognise behavioural forensic evidence; and a national Cyber–Behavioural Forensics Training Protocol.

**Keywords:** Forensic Psychology; Cyber Crime Investigation; Criminal Profiling; Offender Psychopathology; IT Act Reform

PP58

**Empathy and Reoffending Among Juvenile Offenders: A Comparative Study Using the Interpersonal Reactivity Index**

Avantika Samkaria<sup>1</sup>, Priyanka Verma<sup>1\*</sup>, Pravat Kumar Mandal<sup>2</sup>, Mohammed Zubair Ahmed<sup>3</sup>

<sup>1</sup>*Department of Forensic Science, Chandigarh University, Punjab, India*

<sup>2</sup>*Neuroimaging and Neurospectroscopy (NINS) Laboratory, National Brain Research Centre, Gurugram, Haryana, India*  
[avantikasamkaria02@gmail.com](mailto:avantikasamkaria02@gmail.com)

**Abstract**

**Background:** Reoffending among juvenile offenders remains a significant challenge for rehabilitation systems worldwide. Psychological factors, particularly empathy, have been identified as crucial determinants of antisocial and prosocial behavior. However, limited empirical evidence exists examining the relationship between empathy and reoffending among juvenile offenders in the Indian context.

**Objective:** This study aimed to compare empathy levels between juvenile re-offenders and non-re-offenders using the Interpersonal Reactivity Index (IRI).

**Methods:** A cross-sectional comparative study was conducted among 299 juvenile offenders. Participants were categorized into re-offenders (n = 47) and non-re-offenders (n = 252) based on official records. Empathy was assessed using the Interpersonal Reactivity Index. Mean empathy scores were compared between the two groups using appropriate statistical tests, with significance set at  $p < 0.05$ .

**Results:** Juvenile re-offenders demonstrated significantly lower empathy scores (Mean = 44.66, SD = 18.94) compared to non-re-offenders (Mean = 52.06, SD = 17.89). The difference was statistically significant ( $p = 0.010$ ), indicating an association between reduced empathy and reoffending behavior.

**Conclusion:** The findings suggest that lower empathy levels are significantly associated with reoffending among juvenile offenders. Incorporating empathy-enhancing interventions into rehabilitation programs may help reduce recidivism and support long-term behavioral change.

**Keywords:** Juvenile offenders, reoffending, empathy, Interpersonal Reactivity Index, recidivism

PP59

**Forensic and Behavioural Assessment in Negotiated Criminal Justice Processes:  
Safeguarding Voluntariness and Fair Trial in India**

Saumya Baranwa<sup>1</sup>

<sup>1</sup>*Himachal Pradesh National Law University, Shimla*

*\*Corresponding Author: saumyabaranwal0007@gmail.com*

**Abstract**

Negotiated resolution of criminal cases, though not fully formalised as “criminal mediation” in India, has gradually taken shape through mechanisms such as plea bargaining, compounding of offences, and court-facilitated settlements. In practice, decisions to pursue such negotiated outcomes are often influenced by the perceived strength of forensic and medico-legal evidence. Injury reports, toxicological findings, digital forensic data, and psychological assessments frequently shape the expectations of both the prosecution and the defence, thereby affecting the willingness of parties to consider settlement. The scientific evidence can assist in clarifying issues and facts, but it also raises concerns about voluntariness, informed consent, and the protection of fair trial rights of the accused. In many trial courts, conversations around settlement begin informally once investigation records and expert reports are placed on file. Lawyers tend to assess the case not only on legal grounds but also on the basis of medical opinion, laboratory results, and the perceived credibility of expert testimony. When such material appears conclusive, an accused person may feel compelled to accept a negotiated outcome rather than face a lengthy trial with uncertain prospects. At the same time, victims and their families may rely heavily on medico-legal findings to decide whether settlement is acceptable. This type of dynamic indicate that the motive of forensic material is more than to assist adjudication, which is to shape the psychological and strategic choices of the parties involved. This paper studies the interaction between scientific evidence and negotiated criminal justice. It looks at the existing legal space for plea discussions and compounding of offences, and considers whether current practice provides adequate safeguards to ensure that consent to settlement is genuine and informed. The discussion draws on statutory provisions, selected judicial observations, and standard medico-legal practices, while also noting how other jurisdictions involve behavioural evaluation or expert review in plea-based systems. The main aim is to situate negotiated outcomes within a framework of fairness and due process, this paper seeks to highlight the need for safeguards that balance the interest of rights of individual and the evidentiary value of forensic science.

**Keywords:** Forensic evidence; Behavioural assessment; Negotiated justice; Plea bargaining; Compounding of offences; Voluntariness; Fair trial; Forensic psychology; Criminal justice process; Due process safeguards.

PP60

**Legal Lacunae in the Digital Age: Challenges in Regulating Online Child Exploitation**

Anita Yadav<sup>1</sup>

<sup>1</sup>*Assistant Professor Gautam Buddha University*  
*yanita1979gbu@gmail.com*

**Abstract**

All adults stand accused.....the society responsible for the welfare of children has been put on trial. There is something apocalyptic about this startling accusation; it is mysterious and terrible like the voice of the last Judgment: “what have you done to the children I entrusted to you?”.

Maria Montessori

[The secret of childhood 1936]

In 2024 alone, nearly 3 lakh – precisely 2,91,273 – reports of child sexual abuse material (CSAM) were recorded. In 2025, Special Police Unit for Women and Children received 10,151 inputs related to child pornography, through referrals from the U.S.-based National Center for Missing and Exploited Children. The rise in cyber child pornography in recent years is largely due to easier internet access and the widespread availability of digital videos and data. Child pornography is among the most heinous offences, and it has given rise to several related crimes such as child sexual abuse and sex tourism. This paper undertakes a critical assessment of the deficiencies in current legal frameworks regulating online child exploitation and reviews the effectiveness of existing regulatory mechanisms with special reference to Information Technology Act, 2000 and The Protection of Children From Sexual Offences[POCSO]Act2012. It addresses central issues such as jurisdictional constraints, obstacles in the collection of digital evidence, intermediary liability, privacy-related challenges, and the responsibilities of technology companies in detecting and reporting unlawful content. Using a doctrinal and analytical research approach, the paper demonstrates the limitations of present laws in responding to emerging forms of online exploitation and emphasizes the urgency of comprehensive legal reform.

**Keywords:** Children, Exploitation, Intermediary, Pornography, Reform

PP61

**Regulating the Unseen: An Empirical Legal Analysis of Cyber-Enabled Child Sexual Exploitation**

Aakanksha Sharma<sup>1</sup>, Rekha Verma<sup>1\*</sup>

<sup>1</sup>*Amity Law School, Amity University, Noida*

\**Corresponding Author: [rverma10@amity.edu](mailto:rverma10@amity.edu)*

**Abstract**

The increasing migration of child sexual exploitation to encrypted and anonymized digital environments presents significant challenges to existing legal frameworks, which remain largely territorially oriented. This paper examines the adequacy of current legal responses to cyber-enabled pedophilic offences through an empirical legal approach. The study is based on qualitative data derived from semi-structured interviews with legal practitioners and forensic experts, supplemented by a comparative doctrinal analysis of legal frameworks in India, the United States, and Germany. The findings indicate persistent limitations in addressing issues of jurisdiction, attribution of digital identity, and admissibility of electronic evidence in cross-border investigations. Respondents consistently identified gaps in procedural coordination and limited judicial engagement with digital forensic outputs. In addition, the absence of structured pre-sentencing evaluation mechanisms for cyber offenders further constrains effective justice delivery. While existing legislative instruments, including cyber and child protection laws, provide a foundational framework, their application remains uneven in technologically complex contexts. The paper argues for the need to align legal and procedural frameworks with evolving technological realities through targeted reforms. It proposes the development of harmonised legal standards, capacity-building for judicial and investigative authorities, and greater integration of forensic insights within evidentiary and sentencing processes. The study contributes to the emerging discourse on strengthening legal responses to technology-mediated crimes against children by incorporating empirical perspectives into doctrinal analysis.

**Keywords:** Cybercrime, Pedophilia, Cyber Law, Child Sexual Exploitation, Digital Evidence



AMITY UNIVERSITY  
UTTAR PRADESH



PP62

## Revisiting gender and crime: Do men and women offend for different reasons

Shivangi Sansu<sup>1</sup>, Pamela Kar<sup>1\*</sup>, Lakshmi Kumari<sup>1</sup>

<sup>1</sup>*Department of Forensic Science, Usha Martin University, Ranchi, Jharkhand*

*\*Corresponding Author: [pamelakar292010a@gmail.com](mailto:pamelakar292010a@gmail.com)*

### Abstract

The relationship between gender and crime has been a longstanding topic of interest in criminology, with research consistently showing that men are more likely to engage in criminal behavior than women. However, as the field evolves, scholars are increasingly recognizing that the motivations driving men and women to offend may differ significantly. This paper revisits the question of whether men and women offend for different motives, exploring the empirical evidence and theoretical frameworks that underpin this debate, and shedding light on the complexities of gendered crime patterns. Ecological factors like social and economic conditions increase crime in both genders, with extremely strong correlations. Yet pathways diverge: men's offending links to peer pressure, risk-taking, social expectations around masculinity, family instability like separated or unmarried parents, and power instrumental motives; women's ties to trauma, abusive relationships, mental health struggles like depression and anxiety, childhood trauma, and relational or economic survival drives. These differences, despite shared core risks such as social disadvantage, peer influence, and violence exposure, do not mean one gender offends more seriously than the other. Findings strengthen forensic practice and the justice system: gender-aware profiling weighing relational motives for women and power/instrumental for men; adapting risk tools to include trauma histories; tailoring interviews, rehab (trauma treatment for women, impulse control for men), sentencing, and prevention; refining victim-offender analysis, investigator training, and policies like specialized courts; shaping policies like specialized courts for abused female offenders; and expanding cross-cultural research to validate motives and sharpen forensic tools.

**Keywords:** Gender and crime, motive differences, masculinity, past trauma

**PP63**

**Human Trafficking: A Comprehensive Literature Review of Global Trends, Drivers, Legal Frameworks, and Victim Support**

Manjeet<sup>1</sup>, Shweta<sup>1</sup>, Kajal Sharma<sup>1</sup>

<sup>1</sup>*Department of Forensic Science, Chandigarh University*  
*[manjeet.forensics@gmail.com](mailto:manjeet.forensics@gmail.com)*

**Abstract**

Human trafficking is one of the most inhumane and gross violations of human rights affecting a big number of populations, across the world. This literature review combines the results from 30 highly related scholarly publications between 2005 to 2025, to inspect this complex dimension of human trafficking, which includes global trends and frequency mapping, socio-economical drivers and weakness, national and international legal groundwork and methods of victim identification and different aid that can help them. This review reveals that global crisis triggered by destitution, imbalance, political unrest and high demand to take leverage of labour, making weak people easy to target. International frameworks like Palermo Protocol guide legally but lack end to end implications. National legal systems have many variations in their capacity to punish offender and protect victims. Important research gap present related to labour trafficking, male victims, and their exploitation. Evidence indicates survivors bear heavy physical and mental aftereffects, yet they can't easily access support services. Trauma-informed, culturally delicate, and victim-based care models shows greatest ability to support survivor requirements. To tackle this multifaceted dimension of human trafficking, world needs coordinated, multidisciplinary strategy that incorporate preclusion, prosecution, preservation, and partnership by uniting administrative authority, NGOs, society, global institutions in maintained, cooperative response. Reducing root cause by decreasing poverty and providing essential education to strengthen criminal justice system. Future scope of rigorous research which includes survivors and maintained throughout funding for complementary victim support.

**Keywords:** Human trafficking, legal framework, Victim support

**PP64**

**AI Generated Crimes Against Children: Bridging Cyber Law and Digital Forensic Challenges in India: A Comparative Study**

Yukti Yadav<sup>1\*</sup>, Priyanka Gangwar<sup>1</sup>

<sup>1</sup>Assistant Professor, School of Law, GD Goenka University, Gurugram

\*Corresponding Author: [adv.yukti@gmail.com](mailto:adv.yukti@gmail.com)

**Abstract**

The rapid growth of Artificial Intelligence (AI) has transformed cybercrime, giving rise to AI-generated crimes against children. These include CSAM, grooming chats, morphing children's image into explicit content, voice cloning, which do not involve physical abuse yet results in privacy harm. In India, the legal responses to crime against children is primarily governed by the Information Technology Act, 2000 and the Protection of Children from Sexual Offences Act, 2012. However, these frameworks are premised on the concept of conventional forms of exploitation, thereby creating ambiguity in addressing AI generated content. The absence of explicit provisions dealing with AI driven exploitation poses challenges in defining criminal liability, establishing mens rea and ensuring effective prosecution, leading to lack of authenticity of digital evidence which complicates judicial process. Hence, digital forensics plays a vital role in bridging this gap by enabling the detection, prevention and analysis of AI generated content with techniques such as deepfake detection, metadata analysis and algorithmic tracing. In contrast, European Union and the United Kingdom have begun to proactively address these challenges through targeted legal reforms and technological investment.

This paper adopts doctrinal approach to examine the adequacy of existing cyber law frameworks in addressing such emerging threats. The focus is based on comparative analysis of European Union and the United Kingdom. This comparative approach will highlight the need for India to adopt adaptive legal and forensic framework.

**Keywords:** AI-Generated Crimes, CSAM, Digital Forensic, Cyber Law

PP65

**Unregulated Intimacy and Gendered Violence: A Critical Socio-Legal Analysis of Crimes against Women in Live-in Relationships in India**

Ayushi Trivedi<sup>1</sup>

<sup>1</sup>*Amity University, Lucknow, Uttar Pradesh, India*  
[ayushi.trivedi45@gmail.com](mailto:ayushi.trivedi45@gmail.com)

**Abstract**

Live-in relationships in India have gradually gained judicial legitimacy as relationships “in the nature of marriage,” reflecting changing social norms and individual autonomy. However, this recognition remains fragmented and largely jurisprudential, lacking a comprehensive statutory framework. Consequently, women in such relationships often remain exposed to various forms of gendered violence without adequate legal safeguards. This study explores the gap between legal recognition and actual protection, focusing on crimes against women within live-in relationships. This research adopts a qualitative socio-legal methodology. It involves doctrinal analysis of judicial pronouncements and statutory provisions, particularly the Protection of Women from Domestic Violence Act, 2005, along with a critical review of secondary sources such as law commission reports, academic literature, and case studies. The study also engages with feminist legal theory to contextualize structural inequalities embedded within intimate relationships. The analysis reveals that while courts have extended certain protections to women in live-in relationships, significant ambiguities persist regarding their legal status, rights, and evidentiary thresholds. Women frequently encounter challenges in proving the nature and duration of the relationship, leading to denial of legal remedies. Additionally, socio-cultural stigma and lack of awareness further contribute to underreporting of violence, including domestic abuse, coercion, abandonment, and other forms of exploitation.

**Keywords:** Recognition of Live-in relationships, Gendered violence, Socio-legal analysis, Women’s rights, Legal

PP66

## Genocide Recognition and Legal Accountability: A Comparative Study of the Rohingya, Uyghur, and Darfur Situations

Neetu<sup>1</sup>

<sup>1</sup>*School of Law, G D Goenka University, Gurugram, Haryana*  
[nneetu63@gmail.com](mailto:nneetu63@gmail.com) / [neetu.sol@gdgu.org](mailto:neetu.sol@gdgu.org)

### Abstract

Genocide is not a legal abstraction. It is the calculated destruction of human beings on account of who they are — and the world, for all its solemn declarations, keeps watching it happen. The Convention on the Prevention and Punishment of the Crime of Genocide (1948) was born from humanity's darkest hour, carrying the weight of a promise: *never again*. Decades on, that promise rings hollow. Three situations expose this failure with particular clarity: the systematic persecution of the Rohingya in Myanmar, the cultural erasure of Uyghurs in China's Xinjiang, and the enduring devastation of Darfur in Sudan. This study employs a doctrinal and analytical methodology, drawing on the Genocide Convention, the Rome Statute, UN Human Rights Council resolutions, and landmark ICJ decisions including *The Gambia v. Myanmar* (2020) and *Bosnia and Herzegovina v. Serbia and Montenegro* (2007). It interrogates the legal standard of *dolus specialis*, the architecture of genocide recognition, and the institutional machinery tasked with prevention. Five failures recur across all three cases: the Security Council veto that shields perpetrators behind geopolitics; the absence of universal jurisdiction; the politicisation of genocide recognition; the near-impossible evidentiary burden of proving genocidal intent; and fragmented legal standards that produce inconsistency where certainty is needed most. The result, in each instance, is delayed justice, stalled prosecutions, and functional impunity. The international framework knows what genocide is but it simply lacks the institutional courage to stop it. Until that changes, "*never again*" remains not a commitment but a confession.

**Keywords:** Genocide, Rohingya, Uyghur, Darfur, International Criminal Court, Rome Statute, Genocide Convention, Dolus Specialis, State Accountability, UN Security Council

PP67

**Redefining Mediation in Cyberspace: Evolving Cyber Laws and Statutory Framework  
for Online Mediation in India**

Sagar<sup>1</sup>

<sup>1</sup>*Amity Law School, Amity University Uttar Pradesh*  
*[sagar.kadyan.snp@gmail.com](mailto:sagar.kadyan.snp@gmail.com)*

**Abstract**

A shift from the physical courtrooms to virtual courthouses has been observed globally which has altered the landscape of Alternative Dispute Resolution (ADR) mechanisms. While the use of technology through online Dispute Resolution (ODR) has allowed access to justice to the populace, it has simultaneously created a statutory roadblock. The existing legal framework in India is not able to balance the traditional principles of mediation such as confidentiality and trust, with the contemporary cyber realities. This paper examines the evolving intersection of cybersecurity mandates and the governing legal framework for mediation in India with primary focus on the Mediation Act, 2023 and the UNICITRAL Model Law. The research further identifies the virtual platform providers as a critical legal entity in the ODR process and discusses the nuances posed by such entities during the mediation process. Currently these entities lack a standardised statutory definition and corresponding legal obligations which puts the negotiations conducted on such platforms vulnerable to data breaches and unauthorised surveillance. The analysis of Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000 provide us with an alternative to term such platform providers as “Data Fiduciary” thereby creating a statutory obligation to ensure appropriate cybersecurity measures. Furthermore, the paper addresses the issues with the forensic authentication of the settlement agreements through the lens of Section 63 of Bhartiya Sakshya Adhinyam, 2023 to propose a framework where digital signatures and blockchain based record management will be utilized to provide a tamper-proof chain of custody for mediated outcomes. The paper concludes that for online mediation to achieve the same legal sanctity as traditional litigation in India there is a need to integrate the Privacy by Design principles with the enforcement mechanisms provided in the Singapore Convention and harmonize them with the Indian legislations. This papers bridges the gap between cybersecurity and mediation provisions in India to provide workable suggestions for a secure digital justice system.



AMITY UNIVERSITY  
UTTAR PRADESH



PP68

## Redefining Expert Investigative Capabilities in Courtroom Trials Through Advanced Forensic Technologies in Digital India

Suniya Debbarma<sup>1</sup>, Vinayak Gupta<sup>1\*</sup>

<sup>1</sup>*Department of Forensic Sciences, School of Bio-Engineering and Bio-Sciences,  
Lovely Professional University, Phagwara-144411, Punjab*

*\*Corresponding Author: [vinayakgupta224@gmail.com](mailto:vinayakgupta224@gmail.com)*

### Abstract

Forensic science performs a pivotal role in trials at the courtroom through the provision of scientific evidence enhancing the judicial process. With terrorist activities advancing by sophisticated digital and physical means, the demand for strong forensic capability has become imperative. As digital technology is advancing, there is a need to incorporate innovative forensic technologies in the criminal justice system to deliver accurate, credible, and efficient legal proceedings. One of the major strengths of forensic science in court is the promotion of high standards of expert testifying, as it is governed by scientific proof and legal requirements of admissibility. The study was conducted to discuss the changing scenario of forensic expert testimony in courtroom case proceedings. The need for streamlining forensic procedures, the qualification of experts, and forensic evidence admissibility is a rising concern. Widely applied forensic standards, namely, the Daubert and Frye standards, and measures their viability in the Indian legal system has also been discussed. The study points towards the forensically crucial factors of accrediting forensic institutions, peer-reviewed protocols, and the validation of forensic methods to ensure greater authenticity of expert witness testimony. With the increasing trend of digital evidence in terrorism investigations, courts are required to adopt rigorous procedures for the admissibility of digital forensic evidence, such as blockchain-based authentication, AI-powered cybercrime investigations, and sophisticated biometric analysis. The research also emphasizes the importance of forensic data integrity, chain of custody procedures, and cross-examination strategies to avoid false convictions and improve the judicial acceptance of forensic science. In addition, capacity-building programs to educate forensic experts, legal professionals, and law enforcement officials in forensic techniques and its adaptability is required. Forensic scientists, legal academics, and policymakers must collaborate to enhance courtroom standards, ensure forensic autonomy, and bring Indian forensic practices in line with international standards. By utilizing state-of-the-art forensic technologies through the Digital India campaign, India has the potential to improve its judiciary's response to terrorism such that forensic evidence becomes resilient against judicial scrutiny and meaningful to national security and justice.

**PP69**

**Appreciation of Forensic Evidence in criminal trials with respect to Sexual Offences**

Jaza Sarosh<sup>1</sup>, Tabish Sarosh<sup>2</sup>

<sup>1</sup>*SGT University*

<sup>2</sup>*Delhi Police*

*[jaza\\_fol@sgtuniversity.org](mailto:jaza_fol@sgtuniversity.org)*

**Abstract**

Forensic evidence has evolved as the most essential component in the system of criminal justice, specifically with reference to cases involving sexual offenses where the direct evidence is often restricted. Sexual offenses are critical and complex because of the nature of their sensitivity, lack of direct evidence, and trauma suffered by the victims psychologically. In such circumstances the objective and the scientific support to establish facts and to corroborate the testimonies are dealt with forensic science. This paper further aims to examine the admissibility and appreciation along with the evidentiary value of forensic evidence in criminal trials specifically in reference to sexual offenses. This also addresses the challenges that are specifically associated with its application. The research adopts a doctrinal methodology, relying on secondary sources, for example, legal texts, research articles, judicial decisions and statutory provisions.

The study further analyses various types of forensic evidence that includes DNA profiling, pathology, trace the evidence analyses and toxicology, etc. It evaluates the legal frameworks specifically mentioned in Indian Evidence Act, 1872, now Bhartiya Sakshya Adhiniyam, 2023, Bhartiya Nagrik Suraksha Sanhita, 2023 and Bhartiya Nyaya Sanhita, 2023. The study for the results uses forensic evidence as the significant science to strengthen the process of investigation and prosecution in the criminal trials of sexual offenses by providing reliable proofs. In particular, DNA profiling has evolved in the criminal investigation system by providing accurate identification of the criminals and reducing the risk of wrongful convictions.

Other techniques, such as toxicological analysis, are also crucial in establishing circumstances like intoxication. However, the reliability of forensic evidence largely depends on proper collection, preservation, and handling of samples, as issues such as contamination and procedural lapses remain prevalent. To conclude, forensic evidence plays a major and crucial role in providing justice to all the victims of sexual offenses by providing them objectivity in criminal trials. Furthermore, procedural safeguards have been strengthened to ensure proper training and to promote scientific integrity. Ultimately, the appreciation of forensic evidence is necessary for a fair and efficient criminal justice system.

PP70

## Ransomware Attacks And Legal Preparedness: Are Nations Ready For The Next Cyber Threat?

Sunil Kumar<sup>1</sup>

<sup>1</sup>*Amity University, Gurugram, Haryana*

*Sunil20061994k.sk@gmail.com*

### Abstract

Ransomware attacks have become one of the most serious cyber threats in recent years affecting governments, businesses, hospitals, and even individuals. In such attacks, hackers block access to systems or data and demand money in exchange for restoring it. This paper examines whether countries are legally and practically prepared to deal with this growing problem. It focuses on the gaps in existing cyber laws, the challenges faced by law enforcement agencies and the difficulties in tracking and prosecuting offenders who often operate across borders. The study highlights that many nations still rely on outdated legal frameworks that were not designed to handle modern cyber threats like ransomware. Issues such as lack of clear rules on reporting attacks, weak data protection systems and absence of strict penalties for cybercriminals make the situation worse. The paper also discusses how organizations often hesitate to report attacks due to fear of reputational damage which further limits effective response and prevention. Another important aspect covered is the role of international cooperation. Since ransomware attacks are not limited by national boundaries, a coordinated global response becomes essential. However various differences in laws, lack of shared resources and slow mutual legal assistance processes create major obstacles. The paper also briefly explores preventive measures such as stronger cybersecurity practices, awareness programs and better digital infrastructure. In conclusion, the paper argues that while awareness about ransomware is increasing, legal preparedness remains insufficient in many parts of the world. There is an urgent need to update cyber laws, strengthen enforcement mechanisms and promote international collaboration to effectively tackle this evolving threat.

**Keywords:** Ransomware Attacks, Cybersecurity, Cyber Law, Data Breaches, Digital Evidence.



AMITY UNIVERSITY  
UTTAR PRADESH



PP71

ASHWAROOP ADITHY B R

*National Forensic Sciences University, India*

*ashwaroopadithya@gmail.com*

### **Abstract**

Timely forensic analysis of samples relevant to toxicology is critical for accuracy and reliability. Delays in examination can cause substance degradation or conversion into metabolites, which may alter measured concentrations and result in inaccurate findings. Such changes can significantly affect the interpretation and credibility of evidence. As India's recent criminal law reforms prioritize evidence-based approaches, the reliability of forensic findings has become increasingly important. However, challenges such as prolonged storage, improper handling, and systemic delays continue to compromise the integrity of forensic evidence. This study addresses these challenges using a qualitative approach, conducting a systematic review of literature from academic journals and research databases. Analysis of studies on drug stability and forensic delays highlights their significant impact on toxicological evidence and emphasizes the need for careful interpretation in the current legal context. The findings show that examination delays can change the chemical state of compounds or cause degradation, which may lead to negative outcomes and incorrect conclusions.

**Keywords:** Forensic Toxicology, Forensic Delay, Evidence Reliability

**FOR ANY OTHER QUERIES**

**Dr. Amarnath Mishra**, M.Sc., M.Phil., Ph.D., LL.M.  
Organizing Chair/Convenor, ISCSF-2026  
Associate Professor

**Amity Institute of Forensic Sciences (AIFS)**  
Room No. 413, Fourth Floor, J-1 Block  
Amity University Uttar Pradesh  
Sector-125, Noida - 201313 (Adjoining New Delhi), India  
**E-mail:** [amishra5@amity.edu](mailto:amishra5@amity.edu)  
**Phone:** +91-120-4392146/64, +91-9818978527 (Mob.)

