FORENSICS

INDIA'S FIRST FORENSIC SCIENCE ORIENTED BI-MONTHLY MAGAZINE

AUG-SEPT 2025 ISSUE I

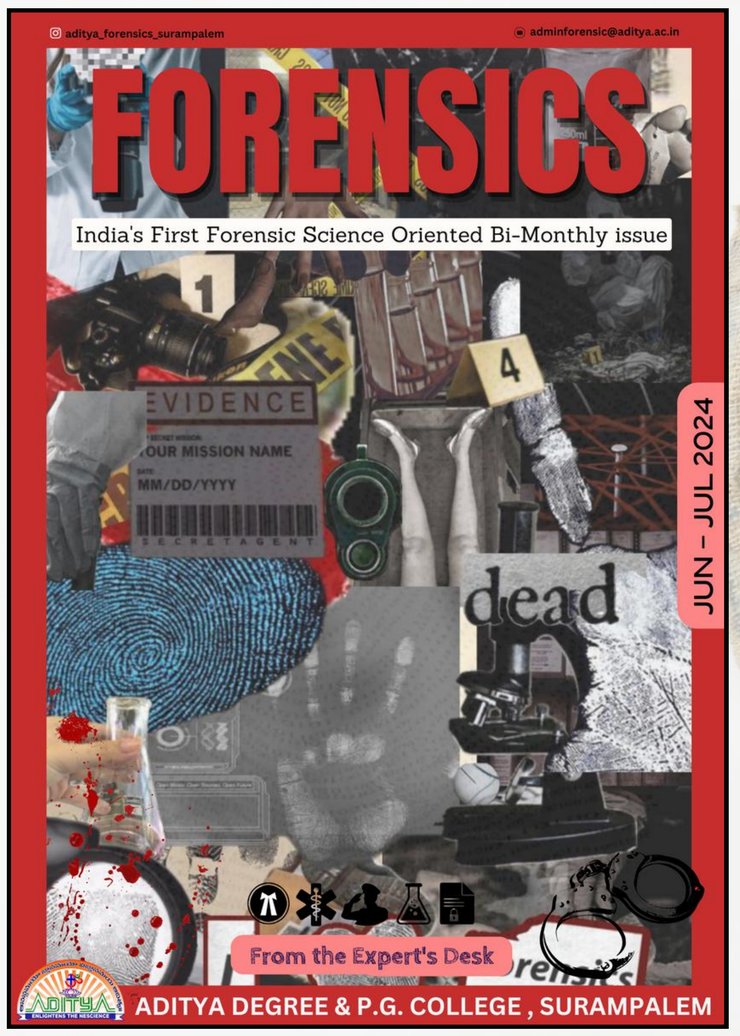
ADITYA UNIVERSITY

nirf Rank Band 151-200 | ACCREDITED BY NAAC A++ GRADE | NBA TIER 1 ACCREDITED | TIMES HIGHER EDUCATION IMPACT RANK | QS I-GAUGE DIAMOND

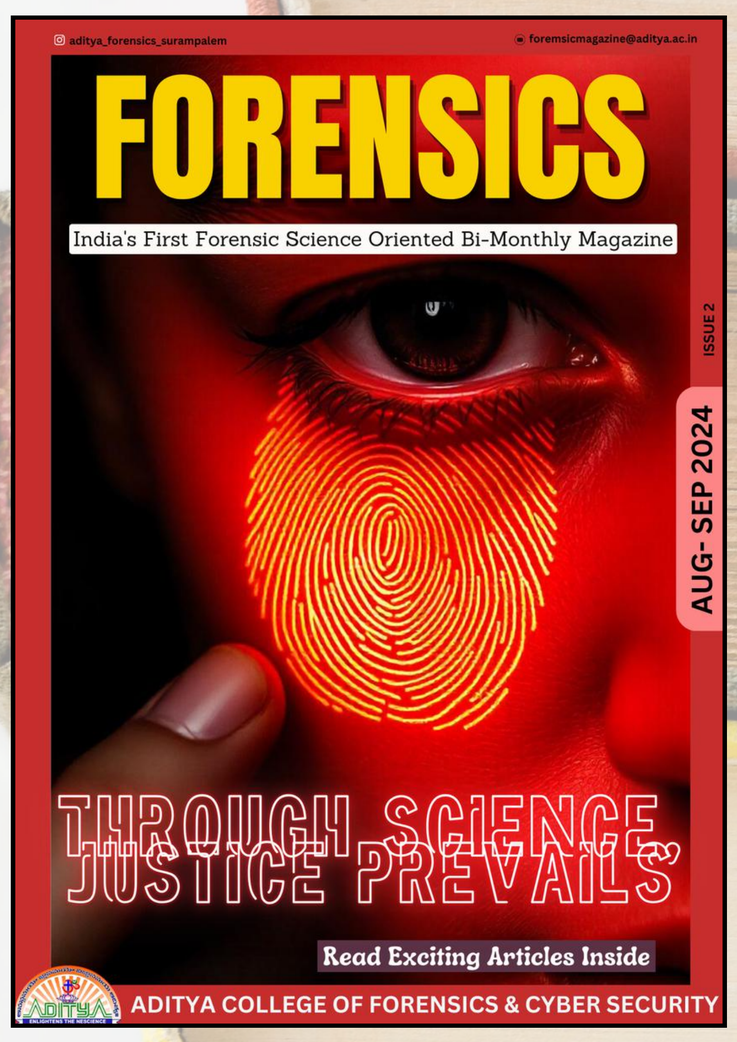
DEPT. OF FORENSIC SCIENCE

SCHOOL OF SCIENCES

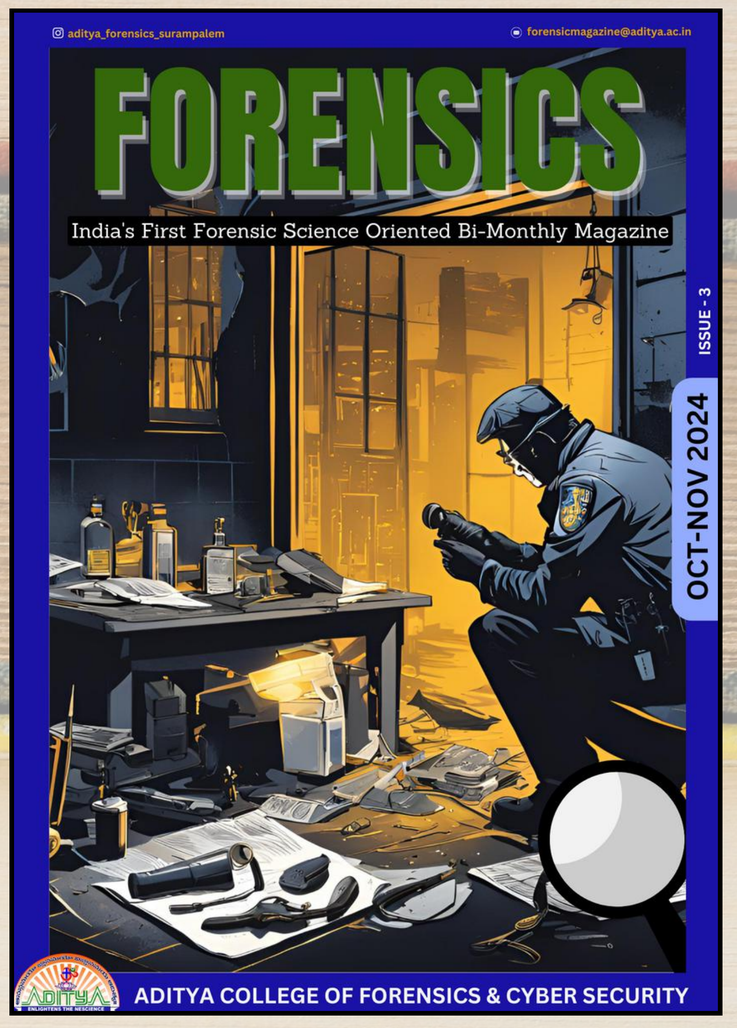
VIEW OUR PREVIOUS ISSUES



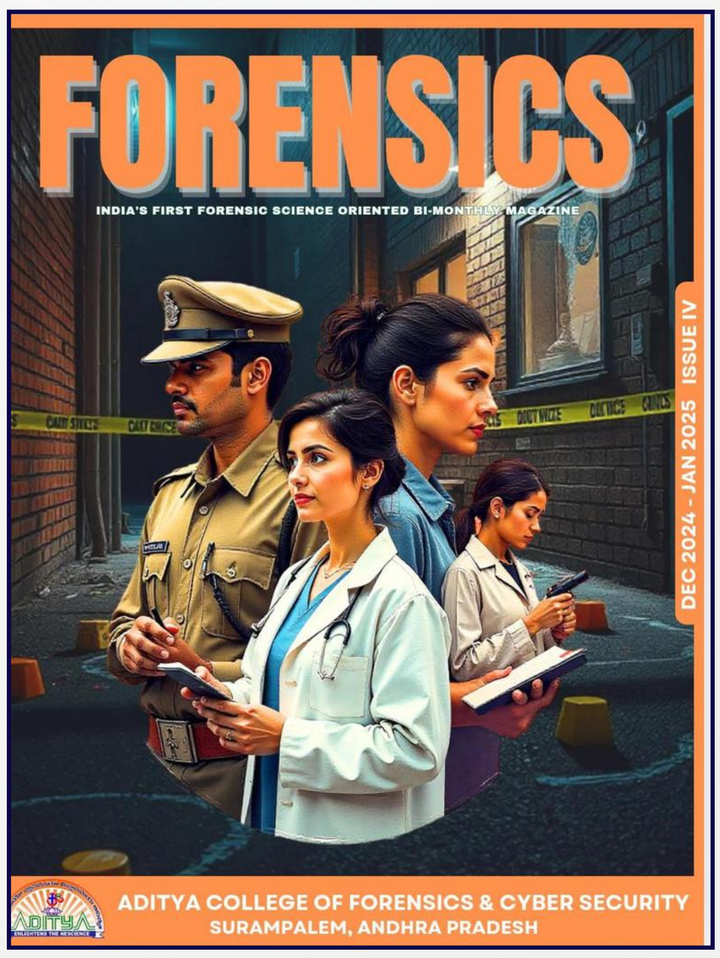
ISSUE I (JUN-JUL 2024)



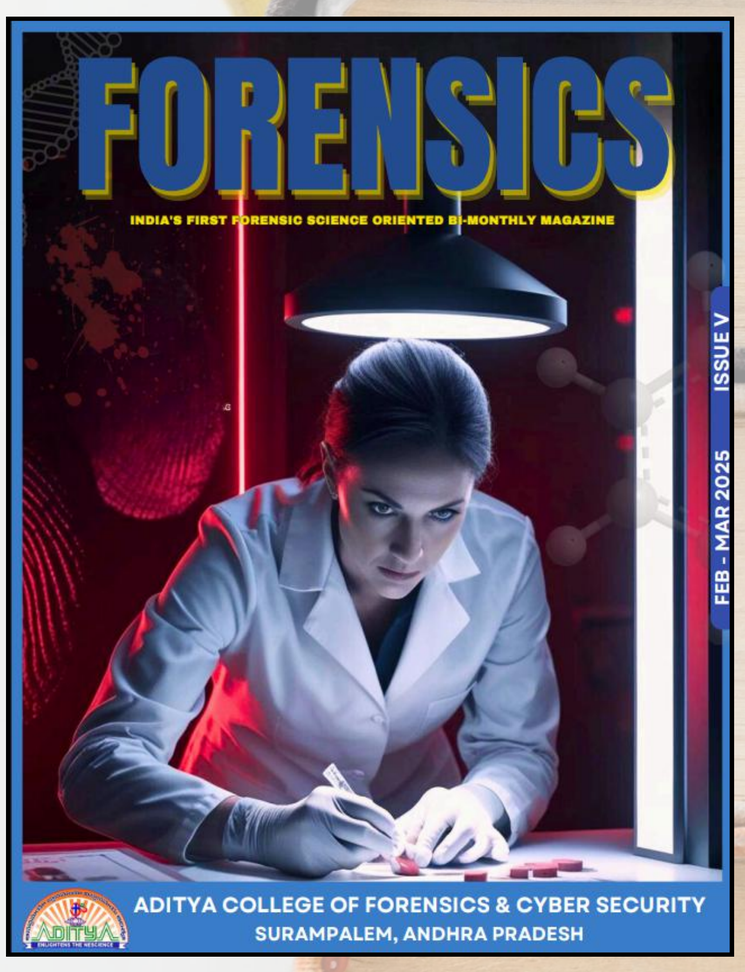
ISSUE II (AUG-SEP 2024)



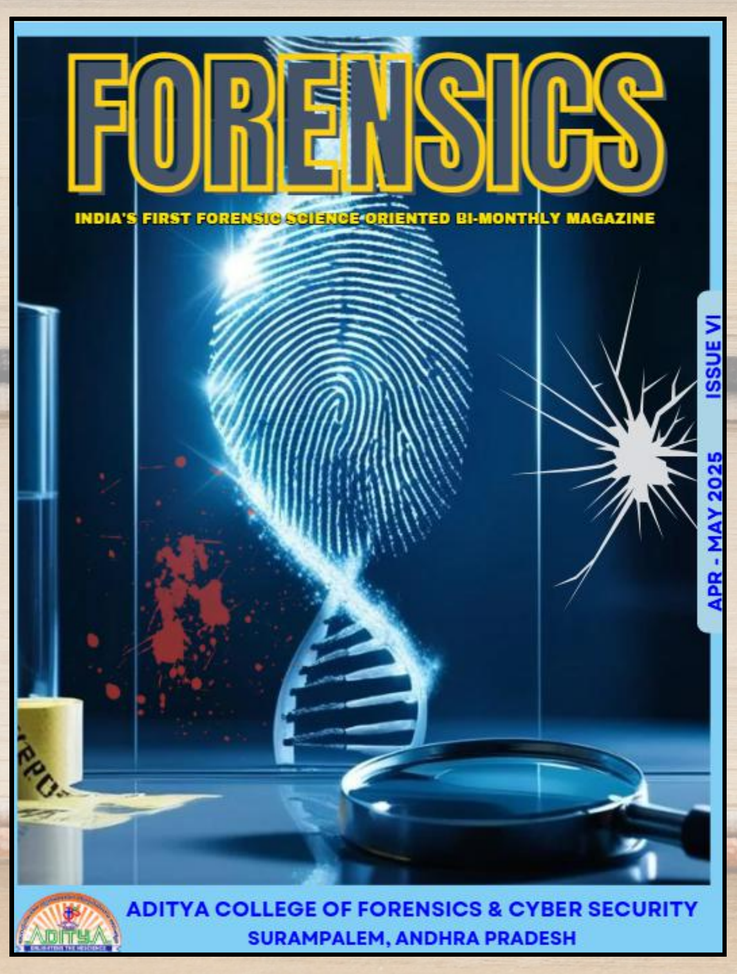
ISSUE III (OCT-NOV 2024)



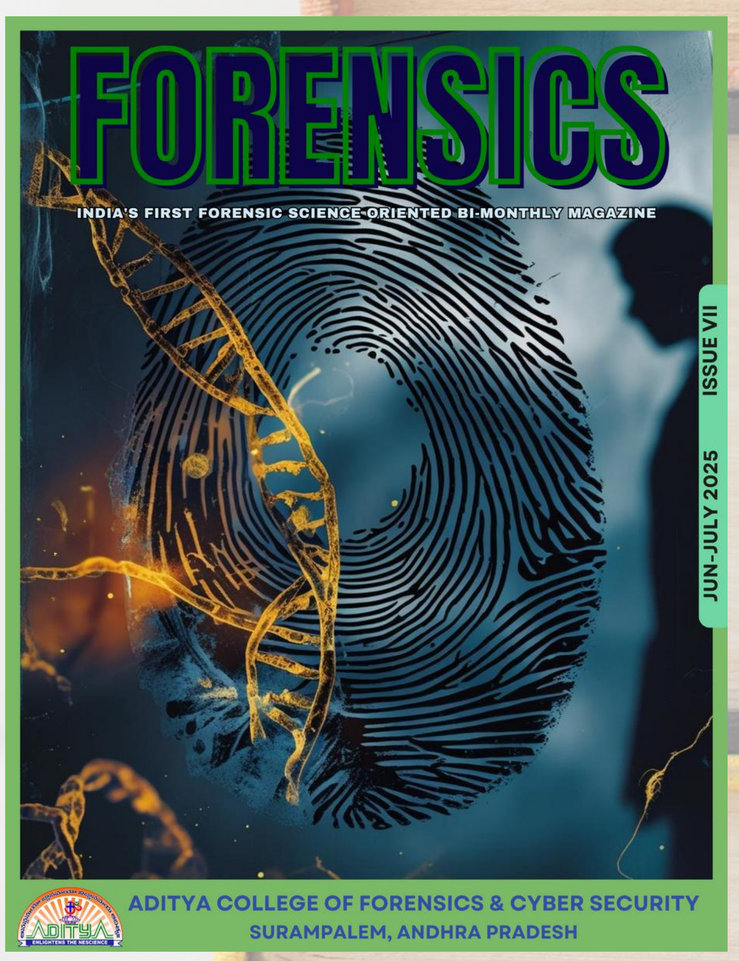
ISSUE IV (DEC-JAN 2025)



ISSUE V (FEB-MAR 2025)



ISSUE VI (APR-MAY 2025)



ISSUE VII (JUNE-JULY 2025)

From The Leadership Team



Dr. N. Sesha Reddy

CHANCELLOR - ADITYA UNIVERSITY

It is my privilege to present the First Issue of the Department of Forensic Science, School of Sciences, Aditya University, a proud successor to our earlier editions.

This issue reflects the innovation, creativity, and commitment of our students, faculty, and industry professionals. It symbolizes a new chapter of exploration, collaboration, and exchange of ideas in forensic science.

I sincerely thank all contributors for their dedication and efforts in bringing this edition to life. Together, let us continue advancing the frontiers of forensic science with excellence and purpose.



Dr. N. Satish Reddy

PRO-CHANCELLOR - ADITYA UNIVERSITY

It is an honour to present the First Issue of Aditya University's bi-monthly magazine on forensic science, proudly carrying forward the legacy of the previous editions. I extend my heartfelt gratitude to the Department of Forensic Science, School of Sciences, for its unwavering guidance and visionary leadership in bringing this initiative to life. With every edition, our goal is to foster innovation, inspire collaboration, and uphold excellence in forensic science education and professional practice. This inaugural issue brings together compelling contributions that highlight the latest advancements and emerging trends shaping the field.

From The Editorial Desk



Vilas Anil Chavan
Editor-in-Chief

Welcome to the First Issue under Aditya University, Dept. of Forensic Science– India's First Bimonthly Forensic Science Magazine!

We are proud to present this inaugural edition, a platform dedicated to sharing knowledge and innovation in forensic science. Inside, you'll find articles on Toxicology, Digital Forensics, Forensic Biology, Environmental Forensics, AI in Forensics, and more, contributed by students, faculty, and experts.

This magazine marks the beginning of a journey to connect ideas, inspire learning, and strengthen the role of science in justice.



BVSS Udaynadh
Editorial Head

As the Editorial Head, I am delighted to present the very First Issue of Forensics – India's First Bimonthly Forensic Science Magazine under Aditya University.

This inaugural edition marks a new chapter in our journey to deliver high-quality content in the field of forensic science. It offers a thoughtful blend of pioneering research, expert insights, and recent advancements from DNA analysis and digital forensics to AI in crime scene investigation and forensic Toxicology. You will also find real-life case studies, policy updates, and career-focused guidance designed to inform and inspire readers in this ever-evolving discipline.

Your encouragement motivates us to build this platform as a bridge between students, academicians, and professionals. Thank you for joining us at the beginning of this journey. Together, we aspire to shape the future of forensic science.

From The Editorial Desk



Aanchal Sakarkar

Managing Editor

As the Managing Editor, I am delighted to present the First Issue of Forensics – India's First Bimonthly Forensic Science Magazine under Aditya University.

This edition brings together pioneering research, expert insights, and recent advancements in DNA analysis, digital forensics, and more. It also includes real-life case studies, policy updates, and career-focused guidance to keep readers informed and inspired.

Thank you for supporting this new beginning. Together, we aim to shape the future of forensic science.



Thushar K.C

Creative- Editor

As the Creative Editor, I am excited to welcome you to the First Issue of Forensics – India's First Bimonthly Forensic Science Magazine under Aditya University.

This edition highlights diverse topics including DNA profiling, digital forensics, forensic cybercrime. With contributions from students, educators, and professionals, it captures the creativity, innovation, and dedication driving forensic science forward in India.

Thank you for joining us on this new journey. Together, let's continue exploring the science that strengthens justice.

CONTENT IN FOCUS

MOLECULAR FINGERPRINTS: WHEN CHEMISTRY BECOMES THE ULTIMATE WITNESS

09



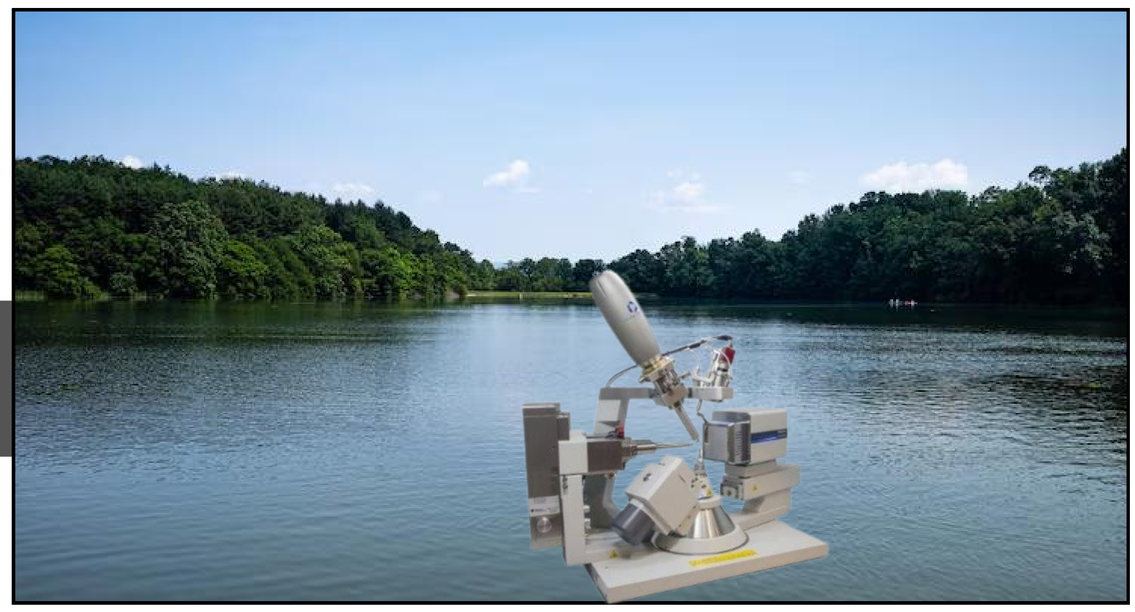
SCIENTIFIC EXAMINATIONOF IMAGE MANIPULATION: A FORENSIC EVALUATION WITH AMPED AUTHENTICATE

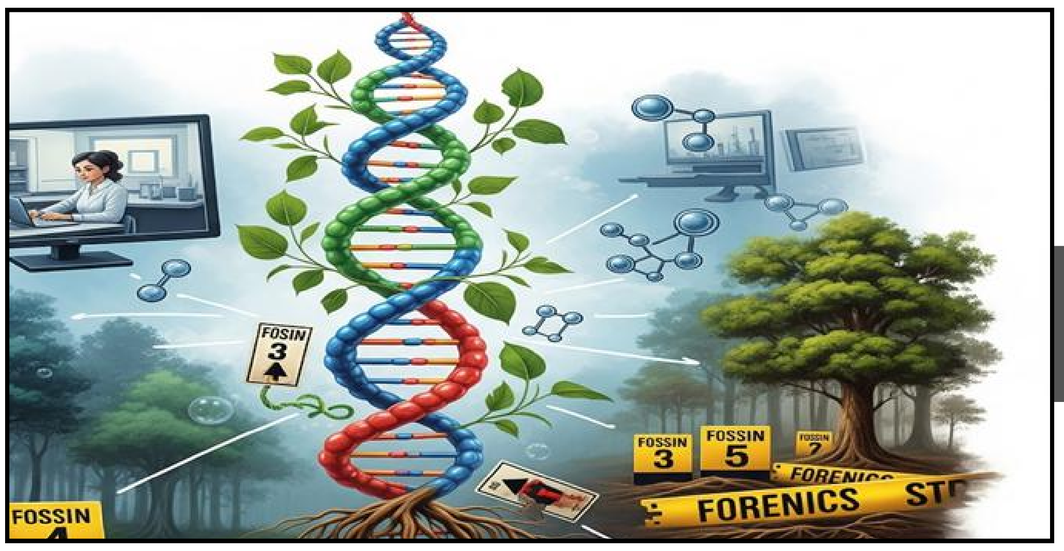
63



IMPACT OF ACID DIGESTION METHOD ON THE DETERMINATION OF HEAVY METALS IN LAKE WATER : A COMPARATIVE EDXRF ANALYSIS IN GANDHINAGAR, GUJARAT.

23





DECODING THE DEAD BEYOND DNA: NEXT GENERATION BIOMARKERS IN FORENSIC INVESTIGATION

30

JUSTICE BEYOND THE COURTROOM: A LIFE IN LAW- INTERVIEW WITH KAPIL VERMA

45





THROUGH A RAPIST'S EYE: A PSYCHOLOGICAL STUDY OF THE MINDSET BEHIND SEXUAL VIOLENCE IN INDIA

48

CRIME WITHOUT CONTACT:
THE ANATOMY OF A ₹23 CRORE DIGITAL ARREST SCAM

27



CONTENT

THE UNSEEN SIGNATURE OF POISON: HOW TOXICO METABOLOMICS IS REVOLUTIONIZING FORENSIC TOXICOLOGY 16



MALWARE FORENSICS: INVESTIGATING, ANALYSING, AND MITIGATING CYBER THREATS IN THE DIGITAL AGE 38

ARTIFICIAL INTELLIGENCE AND FORENSIC TOXICOLOGY: A NEW ERA OF EVIDENCE ANALYSIS 54



VIRTOPSY: A TECHNOLOGICAL LEAP IN DEATH INVESTIGATION 60

FORENSIC APPROACHES TO DIFFERENTIATE MENSTRUAL AND PERIPHERAL BLOOD TRACES AT CRIME SCENES 71

JOURNEY OF ARTIFICIAL INTELLIGENCE AND DRONE FORENSICS: AN OPINION ABOUT JUDICIAL PERSPECTIVES ON THE ADMISSIBILITY OF EVIDENCE 77



MALWARE FROM SPACE: FORENSIC ANALYSIS OF SATELLITE BASED CYBER INTRUSIONS 81

MALICIOUS KEYLOGGER DETECTION 86



ARTIFICIAL INTELLIGENCE IN FORENSIC SCIENCE: ADVANCING JUSTICE THROUGH TECHNOLOGY 102

FULL SPECTRUM IMAGING SYSTEM (FSIS-CSE): A NEW ERA IN CRIME SCENE EVIDENCE CAPTURE 105

Contributors



Dr. Ranjitsinh C. Dabhi



Nandish A. Talpada



Kiranbhai R. Dodiya



Mr. Harwani Sagar



Ms Smita Das



Punnya C V



Bhumit Chavda



Dr. Kapil Kumar



Dasari Harsha Vardhan



Ms. Nikita Sisodia



Anumod P K



Jerald Benny



Ms. Sidhvita Kaithepalli



Princy Nitin Kumar Soni



Dr Sabitha Bau A



Nandhini S



Dipanshu Dipak Umare



Aditya Suman



Vagdevi Emani



G. Naga Ramadevi

MOLECULAR FINGERPRINTS: WHEN CHEMISTRY BECOMES THE ULTIMATE WITNESS



Author : Dr. Ranjitsinh C. Dabhi, Nandish A. Talpada, Kiranbhai R. Dodiya

Abstract

Organic molecules, much like fingerprints, can uniquely link individuals, objects, and activities to criminal events. This article explores the multifaceted role of forensic organic chemistry in modern investigations, illustrating how analytical advancements have elevated molecules to serve as silent, unbiased witnesses in courtrooms. From volatile organic compounds at arson scenes to narcotics and explosive residues, molecular signatures are now integral to forensic science. This review also delves into validation protocols, chemoinformatics, statistical models, legal admissibility, and emerging technologies, aiming to provide a robust, scholarly foundation for the forensic application of molecular evidence.

Introduction

The advent of forensic chemistry has revolutionised crime scene investigation. Once limited to visible clues, modern forensic science now relies heavily on the invisible, chemical traces that offer a silent yet compelling narrative. Within this domain, organic compounds play a crucial role. Often volatile, reactive, or present in minute quantities, these molecules when analysed correctly- become molecular fingerprints. They bear information that can link a suspect to a weapon, a location, or a substance, revealing the who, what, and how of a crime.

In the shadowy corners of crime scenes, where silence speaks and witnesses vanish, chemistry steps forward as the quiet but irrefutable voice of truth. In the age of DNA profiling and advanced surveillance, one form of evidence remains less talked about yet equally compelling molecular fingerprints. These are the organic chemical signatures left behind by explosives, drugs, accelerants, bodily fluids, and everyday materials that can link a suspect to a scene or action with breathtaking specificity. In this world, chemistry becomes the ultimate witness, unbiased, unshakable, and astonishingly detailed.

A New Definition of "Fingerprint"

Traditional fingerprints, those whorled ridges on our fingertips, have long been the hallmark of identity in forensic science.

But in recent decades, science has expanded the very notion of what constitutes a "fingerprint." It turns out that molecules themselves, especially organic compounds, often behave in unique, traceable patterns, much like the ridges of a fingerprint. And when analysed using techniques like gas chromatography-mass spectrometry (GC-MS), high-performance liquid chromatography (HPLC), or infrared spectroscopy (IR), these molecular traces reveal detailed information about who was there, what they touched, what they used, and even what they consumed.

Organic molecules are everywhere cologne on a shirt collar, trace accelerants in arson debris, residues of narcotics in hair strands, and volatile compounds in explosive materials. What makes these so potent in forensic science is their stability, variability, and detectability, even in minuscule amounts.



Fig. Chemistry at the Crime scene

A Case in Point: The Madrid Train Bombings

In 2004, a series of coordinated bombings on commuter trains in Madrid left 191 dead and more than 2,000 injured. Traditional investigative leads quickly went cold. But forensic chemists analysing the residue from the bombs discovered traces of Goma-2 ECO, a commercial mining explosive manufactured in Spain.

Thanks to the chemical fingerprint of Goma-2 ECO and the unique combination of contaminants and taggants, authorities traced the explosive back to a specific mine where it had been stolen leading directly to a local terrorist cell.

Without that chemical evidence, justice might have never caught up with the perpetrators.

This article provides an in-depth academic perspective on how organic signatures are used in forensic investigations. We explore their uniqueness, detection, interpretation, limitations, and admissibility in courts.

Organic Compounds as Molecular Evidence

Organic compounds in forensic science include a broad array of substances: accelerants, narcotics, explosives, pharmaceuticals, environmental pollutants, and biological fluids. Each of these has a unique molecular profile that can be analysed to determine its origin, usage, or association with a crime.

Accelerants and Arson

In suspected arson cases, the fire is both the crime and the cover-up. But hydrocarbons like gasoline, kerosene, or diesel leave behind tell-tale markers even after combustion. Fire investigators collect debris samples in airtight metal cans, which are then heated in the lab to release trapped vapours. These vapours are analysed using GC-MS to detect patterns unique to specific accelerant blends.

For example, a brand of charcoal lighter fluid might have a distinct ratio of iso-alkanes to cycloalkanes, or contain a fragrance compound like limonene, which persists after burning. This level of analysis can link a suspect's purchase history to the accelerant found, forming a chain of molecular evidence.



Explosives: Signature Detonations

Explosives are especially rich in chemical signatures. Compounds like TNT, RDX, PETN, and TATP each have distinct molecular structures, vapour pressures, and degradation patterns. Forensic chemists can detect nanogram traces of explosive residues on a suspect's clothing or vehicle, often long after the blast.

Even more impressive is the use of taggants, tiny chemical markers added to commercial explosives during manufacturing. These taggants act like a barcode. After a bombing, forensic teams analyse residues to not only determine the explosive type but also trace the exact source or batch, sometimes leading directly to the supplier and then to the suspect.

Narcotics: Chemotyping Illicit Drugs

Drugs tell their own stories. Illicit drugs are rarely pure; they're "cut" with a variety of agents that range from the mundane (lactose, baking soda) to the dangerous (fentanyl analogues). These impurity profiles form a chemical signature that can be used to trace a drug back to its lab of origin or connect different seizures of medicines to the same producer.

Advanced techniques like isotope ratio mass spectrometry (IRMS) are now used to analyse the isotopic "flavour" of a drug sample. For instance, cocaine made from Colombian coca plants grown in specific regions has a different carbon-13 to carbon-12 ratio than those grown elsewhere. This allows authorities to link distribution networks, disrupt supply chains, and gather intelligence far beyond what street-level arrests could offer.

Touch Chemistry: Residues of the Everyday

Not all molecular fingerprints come from illicit substances. Sometimes, it's the residues of ordinary life that betray a criminal's presence.

Modern forensics can detect residues from:

Personal care products (lotions, perfumes, deodorants)

- Sunscreens and insect repellents
- Laundry detergents and fabric softeners
- Tobacco and vaping products

Each product leaves behind a unique blend of organic compounds, many of which are not found in nature. These compounds adhere to skin, hair, clothing, and personal items. If such residues are found at a crime scene in unusual concentrations or matched to a suspect, they can help corroborate timelines, contact, and presence.

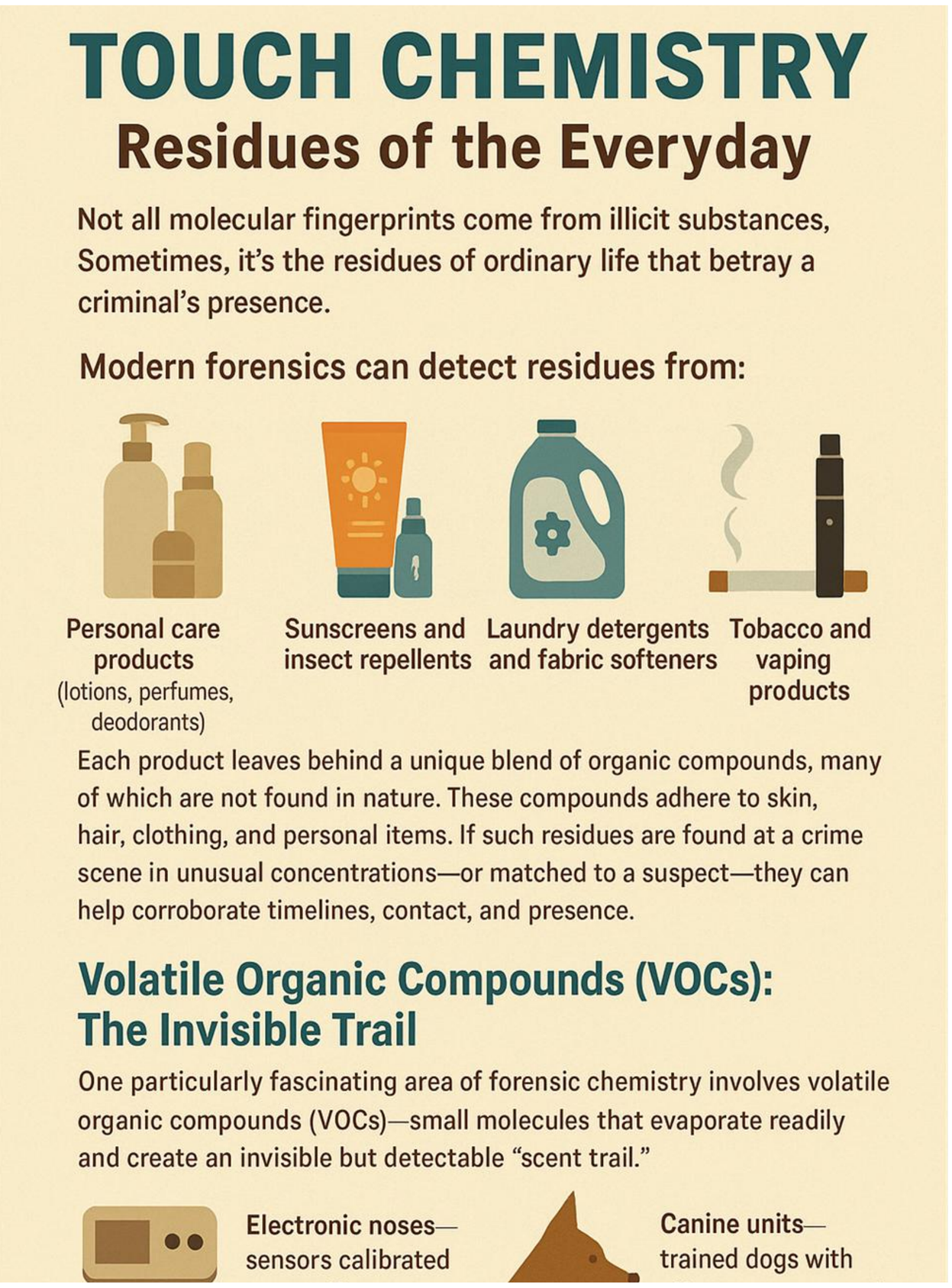


Fig :Touch Chemistry: Residues of the Everyday

Each product leaves behind a unique blend of organic compounds, many of which are not found in nature. These compounds adhere to skin, hair, clothing, and personal items. If such residues are found at a crime scene in unusual concentrations or matched to a suspect they can help corroborate timelines, contact, and presence.



Volatile Organic Compounds (VOCs): The Invisible Trail

One particularly fascinating area of forensic chemistry involves volatile organic compounds (VOCs) small molecules that evaporate readily and create an invisible but detectable "scent trail." Decomposing bodies release hundreds of VOCs in characteristic patterns, which can be detected by:

1. Electronic noses-sensors calibrated to specific compounds
2. Canine units-trained dogs with olfactory systems that rival scientific instruments

This kind of profiling can help locate clandestine graves, confirm decomposition in suspicious packages, or even link someone to a decomposed body by tracing VOCs in their clothes or vehicles.

Analytical Techniques: From Bench to Court

Gas Chromatography–Mass Spectrometry (GC–MS)

GC-MS remains the gold standard for analysing volatile and semi-volatile organic compounds. It provides both qualitative and quantitative data, with retention times and mass spectra acting as molecular identifiers.

Tools of the Molecular Detective

Several advanced analytical techniques make this form of evidence possible. Among them:

1. Gas Chromatography–Mass Spectrometry (GC–MS): Separates and identifies volatile organic compounds with extreme sensitivity. Widely used in arson, toxicology, and drug analysis.
2. High-Performance Liquid Chromatography (HPLC): Effective for analysing non-volatile and thermally unstable compounds such as blood-borne drugs.
3. Fourier Transform Infrared Spectroscopy (FTIR): Used for quick identification of organic compounds based on molecular vibrations.
4. Raman Spectroscopy: A non-destructive method ideal for trace analysis of drugs, explosives, and paint residues.
5. Isotope Ratio Mass Spectrometry (IRMS): Tracks geographic and synthetic origins of compounds through isotope distribution .

These instruments form the core arsenal of the chemical sleuth, capable of revealing truths that the naked eye-or even DNA-might miss.

High-Performance Liquid Chromatography (HPLC)

- HPLC is used for non-volatile, thermally unstable compounds such as pharmaceuticals and metabolites in blood or urine.

Fourier Transform Infrared Spectroscopy (FTIR)

- FTIR helps identify organic compounds based on vibrational transitions. It is beneficial for detecting polymer residues, synthetic drugs, and explosives.

Raman and UV-Vis Spectroscopy

- These techniques, though less commonly used in trace evidence, are valuable in field settings for rapid preliminary analysis.

Ambient Ionisation Techniques

- DART (Direct Analysis in Real Time) and DESI (Desorption Electrospray Ionisation) are emerging as rapid, non-destructive field techniques capable of direct sample analysis without preprocessing.

Validation and Standardization

For any forensic evidence to be admissible in court, it must pass validation and standardisation protocols. Laboratories must adhere to ISO/IEC 17025 accreditation, which requires:

1. Method validation (precision, accuracy, reproducibility)
2. Instrument calibration
3. Blind testing and proficiency programs
4. Documented quality assurance protocols

Lack of method validation has led to the exclusion of key evidence in several cases, reinforcing its importance.

Chemoinformatics and Molecular Databases

The integration of informatics in forensic chemistry has transformed data analysis:

1. Libraries like NIST, Wiley, and SWGDRUG provide spectra for compound identification.
2. Software tools facilitate peak assignment, mixture deconvolution, and impurity profiling.
3. AI models can predict compound classes based on fragmentation patterns.

Inter-agency collaboration allows the building of centralised chemical trace databases, similar to CODIS for DNA.

Statistical Modelling and Interpretation

Scientific evidence must be statistically robust. Tools like Bayesian inference are employed to evaluate the likelihood ratio (LR) of a match.

Likelihood Ratios

Used to express the probability that observed evidence originates from a suspect rather than a random source.

Error Rates and Sensitivity

These values indicate how likely the method is to detect a valid signal and avoid false positives, essential for courtroom testimony.

Software Integration

STRmix-like programs for chemical evidence are under development, enhancing objectivity in complex mixtures

Persistence and Degradation

Environmental factors like sunlight, temperature, humidity, and microbial action degrade organic compounds. Studies focus on:

1. Half-lives of accelerants and explosives under variable conditions
2. Degradation pathways of synthetic drugs
3. Implications for delayed evidence collection

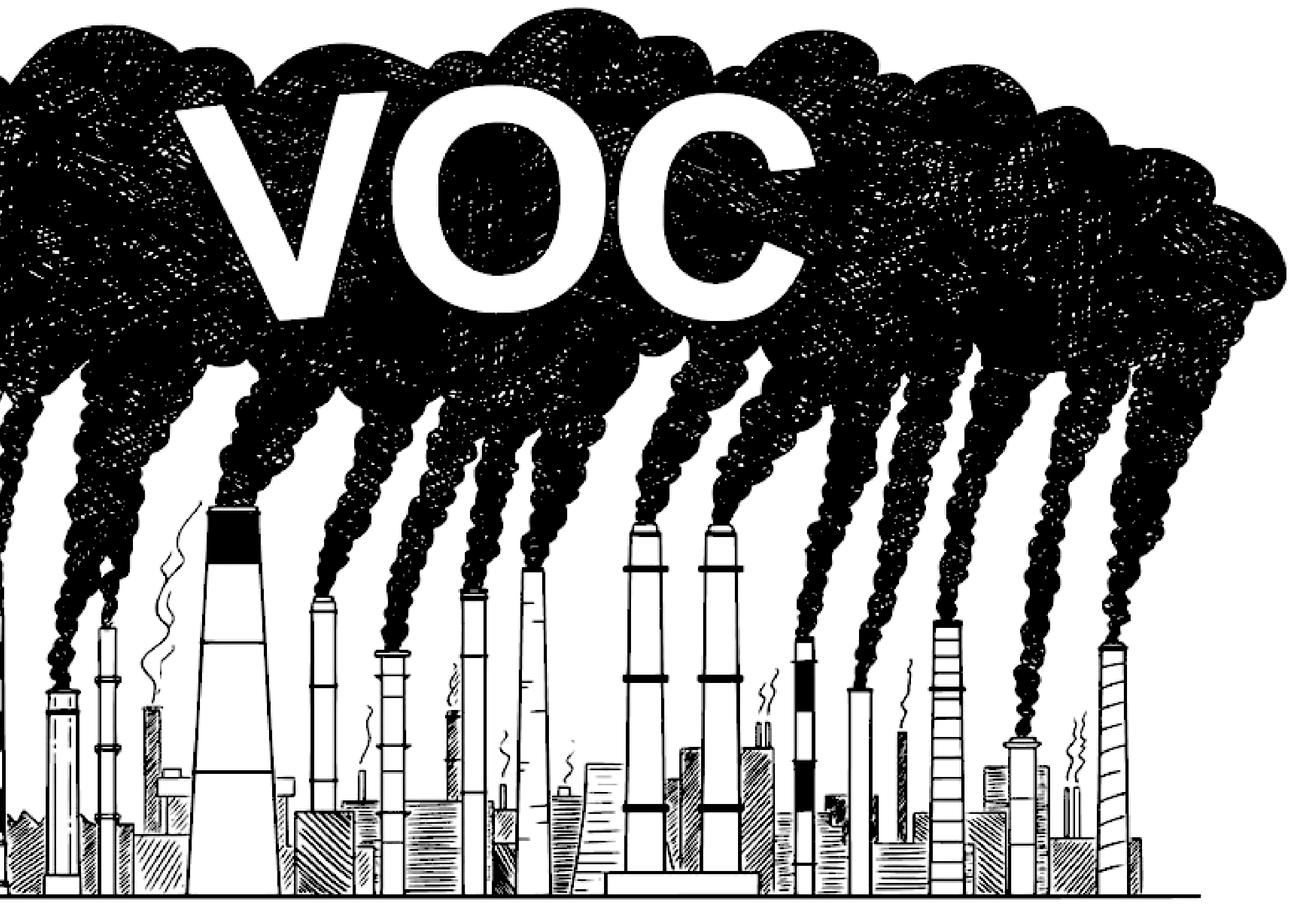
Understanding degradation helps forensic chemists interpret whether the absence of a compound indicates non-use or simply environmental loss.

Legal Admissibility: Daubert and Frye Standards

Under the Daubert standard, courts assess scientific evidence on:

1. Testability
2. Peer review
3. Error rates
4. General acceptance

The Frye standard relies more on community acceptance. Forensic chemists must prepare to defend analytical techniques, explain statistical interpretations, and show method validation.
Notable cases have excluded evidence due to a lack of scientific consensus or improper handling, highlighting the need for rigorous methodology.



Environmental Background and Contamination

Differentiating between criminal-related chemicals and environmental background is essential. Control samples, field blanks, and rigorous sampling techniques reduce false positives. Examples include:

1. VOCs from paint thinner vs. arson accelerants
2. Background methanol in outdoor environments
3. Personal care products misinterpreted as toxic residues

Cognitive Bias and Analyst Safeguards

Cognitive bias can affect the interpretation of ambiguous spectra. To address this:

1. Analysts are blind to case details
2. Peer reviews are mandatory
3. Automated software flags subjective interpretations

Frameworks like the "sequential unmasking" Approach delay contextual information to reduce bias during early analysis.

Emerging Technologies

Portable Instruments

Handheld Raman, FTIR, and GC-MS units now allow in-field analysis.

AI and Machine Learning

AI can sort massive spectral libraries, identify unknown compounds, and predict mixture profiles.

Multi-modal Evidence Integration

Combining chemical evidence with DNA, fingerprints, and digital data provides a holistic crime scene reconstruction.

Case Studies and Applications

Madrid Train Bombings (2004)

Residue analysis identified Goma-2 ECO explosive using GC-MS and taggants, tracing it back to a specific Spanish mine.

Anthrax Letters (2001, USA)

Organic markers in anthrax spores were analysed to identify lab sources using HPLC and mass spectrometry.

Drug Network Disruption

IRMS analysis of cocaine isotopes allowed DEA to map production regions and dismantle supply chains

.

The Future: AI and Molecular Databases

The next leap in molecular fingerprinting may come from the integration of AI and big data. Databases of chemical signatures are being developed, and machine learning algorithms are being trained to recognise patterns in complex organic mixtures.
Imagine a handheld device that scans a surface and immediately cross-references a database to suggest potential compounds present no lab needed. Or AI systems that compare molecular signatures across

thousands of unsolved cases to find hidden links.
These possibilities are not far-fetched they're already in development. The future crime scene might be solved not by a detective pacing the floor, but by a chemist running code and scanning for signals invisible to the eye.

Conclusion: The Quiet Power of Molecules

In a world overflowing with noise, chemistry listens to the faintest whispers. Whether it's a molecule of perfume lingering on a collar, a drop of accelerant buried in ashes, or a trace of heroin in a bloodstream, molecular fingerprints don't lie. They don't forget. They don't make mistakes in a lineup. As forensic science continues to evolve, the power of organic chemistry its ability to see the invisible and speak the unspeakable reminds us that truth has a signature, and it's written in molecules. As forensic science evolves, molecular fingerprints continue to emerge as powerful tools in crime investigation. Through validated methods, chemoinformatics, and statistical models, these invisible witnesses are transforming how evidence is gathered, interpreted, and defended in court. With the integration of AI and field-deployable instruments, the future of forensic organic chemistry is not only promising it's revolutionary. By viewing molecules not as passive remnants but as narrators of events, forensic chemists have made chemistry not just a science, but a form of truth-telling. And in the pursuit of justice, that truth is invaluable.

References

1.M. Smith, J. Johnson, and A. Brown, "Advancements in Forensic Chemistry: From Traditional Methods to Molecular Fingerprints," Forensic Science International, vol. 175, no. 2, pp. 109-117, 2023.
2.T. Clark, "Role of GC-MS in Forensic Chemistry: A Critical Review," Journal of Analytical Chemistry, vol. 42, no. 6, pp. 321-330, 2022.
3.L. Patel and K. Sharma, "The Application of Chemoinformatics in Forensic Science: A Review," Journal of Forensic Sciences, vol. 61, no. 4, pp. 1234-1243, 2021.
4.S. Gupta, "Statistical Models in Forensic Chemistry: Evaluating Likelihood Ratios," Forensic Chemistry Review, vol. 18, no. 3, pp. 200-209, 2023.
5.A. Williams, "Emerging Technologies in Forensic Chemistry: Portable Instruments and AI Integration," International Journal of Forensic Science, vol. 29, no. 1, pp. 42-51, 2024.
6.P. Fernandez, R. Kumar, and V. Mehta, "Explosive Residue Analysis in Forensic Investigations: From Goma-2 to Modern Taggants," Explosive Materials Journal, vol. 39, no. 2, pp. 105-112, 2022.

ABOUT THE AUTHOR



Dr. Ranjitsinh C. Dabhi
Ph.D. in Chemistry, School of Sciences, Gujarat University, Ahmedabad, Gujarat, INDIA



Nandish A. Talpada
Research Scholar, School of Sciences, Gujarat University, Ahmedabad, Gujarat, INDIA



Kiranbhai R. Dodiya
Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA

KEEP OUT KEEP OUT KEEP OUT KEEP OUT KEEP OU

Did You Know



The skull is made up of the cranium and the facial bones, while the cranium alone forms only the cranial vault.

KEEP OUT KEEP OUT KEEP OUT KEEP OUT KEEP OUT



Author : Mr. Harwani Sagar & Ms. Smita Das

The Unseen Signature of Poison

In the histories of forensic science, a case study serves as a potent reminder of the limitations of conventional inquiry. A middle-aged woman is found deceased in her parked car on a hot summer evening. A forensic pathologist, upon reviewing the case, notes the presence of high levels of multiple opioid
analgesics in the post-mortem toxicology report. The conclusion seems straightforward: a fatal drug overdose. However, the deceased's medical history reveals a past diagnosis of cardiac arrhythmia. This crucial detail, often overlooked in a "numbers-only" approach ,complicates the narrative. The high drug levels could have been spuriously elevated due to post-mortem redistribution the passive diffusion of drugs in a decomposing body rather than representing a lethal antemortem concentration. The cause of death may not have been a slow respiratory depression but a sudden cardiac event ,a conclusion that could have a profound impact on the subsequent legal proceedings.

This case is typical of the dramatic transition now taking place in forensic toxicology. For generations, the discipline functioned under a reductionist model, with specialists working to identify and measure parent compounds as an explanation of death or untoward event.The classic paradigm of this fieldremains productive in most situations but is facing in the current
environment the ultimate test in terms of world complexity. The answer is in an entirely new, holistic paradigm a systems biology one that examines the toxic agent, but the body's total biochemical response to the agent. The new field is called toxicometabolomics

The cornerstone of this new paradigm is the metabolome, the entirety of all low-molecular-weight compounds (lessthan 1500 Da) within a biological system. Unlike the genome, which is potential, or the proteome, which is function, the metabolome is the most immediate manifestation of the organism's biochemical activity after exposure to physiological and pathophysiological stimuli .It is the final product of the entirety of cellular regulative complexity.

The downstream position relative to gene expression gives this system an advantage that is unique: metabolic changes are frequently magnified compared with changes within the transcriptome or proteome, and this magnifies the sensibility with which subtle biochemical changescan be detected at an early onset of toxicity. Through interrogation of the metabolic signatures, toxicometabolomics offers an exponentially deeper and more subtle understanding of the nature of toxicitythan the detectionof the parent compound only. It is an absolute step from the narrow, focused perspective to the ultimate systems-wide perspective.



The Limitations of the Old Guard

Traditionally, the majority of the practice of forensic toxicology was grounded in the reactive, focused paradigm. The analyst would screen selectively for a predetermined menu of drugs, typically parentdrugs and the well-recognized metabolites, with standard methodologies like gas chromatography-mass spectrometry (GC-MS)or liquid chromatography-mass spectrometry (LC-MS). The application of this approach was the longtime "golden standard" in the practice of toxicity evaluation. The traditional paradigm is increasingly strained in the contemporary

world, nonetheless, and three critical faults are here illuminated.The initial big hurdle is the spread of Novel Psychoactive
Substances (NPS). These are chemically modified analogues of classic street drugs, deliberately synthesized so as to be undetected through typical test screens. Due to their novel structure and the exponential introduction of new substances, traditional approaches remainin continuous catch- up mode. Forensic scientists are forced continuously to refine their techniques and augment their libraries of standard substances, the expensive and oftentimes losing war against the dynamic street drug scene. These case exemplars of drugs such as fluorofentanyl illustrate this very issue, illustrating the point that certain NPS may be identified and quantified in some limited fashion, but the overall toxicological landscape is overlooked.



Secondly, post-mortems provide a unique set of biological puzzles that resist conventional explanation. The physiological state of the corpse is radically transformed after death so that drug distribution as well as drug metabolism is affected. The consequence is that this may lead to the post-mortem redistribution effect so that drugswill passively diffuse
from organs in the body into the bloodstream and provide spuriously high levels that are not the correct reflection at the moment of death. The classic example is the post-mortem production of ethanol or Gamma-Hydroxybutyrate (GHB), which can be produced endogenously as the consequence of post-mortem microbial digestion, so that the question then is was the chemical ingested ante-mortem or post-mortem. Such biological variation demands an interpretative framework more nuanced than that provided by the quantitative number. Lastly, the greatest weakness is the "numbers-only" fallacy. The example of the heart-disease woman who was wrongly diagnosed with an opioid overdose is the perfect demonstration.

The high opioid levels, while strictly true, failed to capture the complete picture of her death. The critical failing in this type of analysis is that all available evidence was not taken into account, including the medical history of the patient and the
physiological indications of an alternative cause. A high drug concentration is just a data point, but absent the surrounding biological and circumstantial context the context that the conventional approaches so frequently omit it is possible that the end may be badly misinterpreted with flawed conclusions, tainted reputations, and miscarriages of justice. The lack of evidence that would explain the drug level that it could be due to post-mortem redistribution rather than an antemortem overdose is the
critical gap that only the systems-level is well-positioned to fill. The challenge of NPS, say, is not only technical but the potent, marketplace driver of the adoption of toxicometabolomics. The conventional lab needs to purchase some new standard every time there is some new NPS. The toxicometabolomics lab, in contrast, is already after the body's total metabolic response. The novel NPS will nonetheless disturb some
metabolic pathway in the body, say glycolysis or the metabolism of the amino acids, that will produce some novel, identifiable "signature of toxicity" regardless of the novelty of the parent compound. The toxicometabolomics strategy is therefore inherently more proactive and future prof.



The System Approach: Decoding the Toxicological Blueprint

The area of toxicometabolomics is within the broader area of Systems Toxicology,

which is aimed at providing a "comprehensive mechanistic as well as quantitative and dynamic insight into toxicological processes".5 The approach radically shifts the paradigm from the recognition of one compound to the unravelling of the overall network of changes in biology that the compound induces.

The foundation of this new paradigm is the detection of "pathways of toxicity" (PoTs). Through the analysis of the metabolome, toxicometabolomics can reveal an overall picture of how the disruption of a toxicant occurs at the major biochemical levels of an organism. Thus, drug-induced alteration of cellular metabolism can be demonstrated as leading to the "downregulation of glycolysis," "disturbance of branched- chain amino acids," or disruption of the TCA cycle.4 Such levels of mechanistic information are out of the question with conventional targeted analysis, which only verifies the presence of a compound. The capability of determining such metabolic derangements provides an effective means of deciphering the mode of actionof a xenobiotic and can reveal novel toxicity biomarkers as well as target organs.

This systems strategy is especially useful due to the amplifying nature of the metabolome. Being the downstream product of gene expression, metabolic alterations may be more evident and measurable compared with changes at the genomic or proteomic level. Consequently, toxicometabolomics is an extremely sensitiveprobe for measuringadverse effects at an extremely early time point, often with superior sensitivity compared with conventional toxicology.4 Such potency extendsalso to the field of translational research, with model organisms like the zebrafish being used as bridging instrument from mammalian in vivo studies and in vitro tests. The high level of metabolic pathway conservation in the zebrafish model holds much promise as a toxicometabolomics platform, with the latter enabling researchers the possibility of conducting cross-species extrapolation of the toxic pathways.

The real strength of the strategy is that it can be used to inform Adverse Outcome Pathways (AOPs), the cornerstone of contemporary risk assessment. By connecting a molecular alteration, like the level of some metabolite, with an established key event in some pathway of toxicity, toxicometabolomics offers a potent, mechanistic foundation for the kinds of regulatory judgments and safety evaluations that will be required. Classic toxicology may merely reveal some correlation between some chemical and some adverse health consequence. Systems toxicology, driven by metabolomics, can build a causal chain. These kinds of mechanistic details are what will be requiredIn addition, the idea of the metabolome being "closest to the phenotype" involves measuring the integrated effect of genetics, diet, and even the gut microbiome on the response of an organism to a toxicant. This shifts toxicology from the population-based science that it is now, to the precision science that is foreseen. Two individuals receiving the same dose of drug will have enormously different results. Classic toxicology may be unable to explain this variation. Toxicometabolomics, on the other hand, is capable of uncovering that the other person's distinctive genetic polymorphism or gut microbiome produced a dissimilar metabolic profile a dissimilar "toxicological blueprint" that rendered the person more vulnerable. The case of the drugs Ivosidenib and Enasidenib, that target at a special oncometabolite identified through metabolomics, is an exampleof how personalized, by courts and the responsible regulating agencies. In addition, the idea of the metabolome being "closest to the phenotype" involves measuring the integrated effect of genetics,diet, and even the gut microbiome on the responseof an organism to a toxicant. This shifts toxicology from the population-based science that it is now, to the precision cience that is foreseen. Two individuals receiving the same dose of drug will have enormously different results. Classic toxicology may be unable to explain this variation. Toxicometabolomics, on the other hand, is capable of uncovering that the other person's distinctive genetic polymorphism or gut microbiome produced a dissimilar metabolic profile a dissimilar "toxicological blueprint" that rendered the person more vulnerable. The case of the drugs Ivosidenib and Enasidenib, that target at a special oncometabolite identified through metabolomics, is an example of how personalized, highly effective drugs may be developed with adverse effects being reduced.

The Modern Arsenal: Technologies for Uncovering the Metabolome

Transition from the current compartment-based toxicology paradigm to that of systems biology would be unattainable without the emergence of a new generation of analytical tools that would be sufficient to reflect the enormous wealth of the metabolome

Two main platforms, Mass Spectrometry (MS) and NMR spectroscopy, represent the core of this modern arsenal.
Mass spectrometry is sometimes referred to as the high-resolution workhorse of toxicometabolomics. It enables the holistic, "virtually complete detection of small molecules in a biological sample". High-resolution mass spectrometry (HRMS) is especially vital, as this allows the detection of novel and yet unknown substances through the measurement of their precise mass as well as isotopic distribution. Its main advantages are high sensitivity, broad linear range, and the possibility of simultaneous analysis of a large group of metabolites. However, MS-based analysis is destructive in nature, may be prone to ion suppression, and may involve the expenditure of long analysis time per sample. Nuclear Magnetic Resonance (NMR) spectroscopy is the powerful and complementary ally of MS. Its main advantage is that it is non-destructive and requires little sample preparation time. The result is that the parent compound and metabolites can be detected and quantified simultaneously and is therefore an extremely efficient tool in some applications. It is particularly successful in the identification of analgesics and antiepileptic drugs with an 83-100% sensitivity and is at its best when large amounts of the toxicant have been ingested.

The main limiting factor is that its sensitivity is lower than that of MS and that some compounds cannot be detected with the NMR, including the tricyclic antidepressants and antipsychotic drugs with the latter being detected with a 0% sensitivity.
The limitations of a single platform necessitate a multi-modal, integrated approach. A sophisticated forensic or clinical lab cannot rely on just one technology. For instance, a streamlined workflow might use rapid NMR screening for a broad spectrum of known compounds in a high- volume setting, followed by a more sensitive, comprehensive HRMS-based untargeted analysis for complex cases, especially when an initial screen is negative. The research shows NMR had a low concordance with GC-MS and a 0% sensitivity for some drugs. This is a significant drawback.
However, it also has the unique advantage of minimal sample preparation and non-destructive analysis. The solution is not to discard NMR but to use its strengths to complement the strengths of MS, which can identify a wider range of compounds at trace levels. This integrated, systems-based approach to technology is a microcosm of the field's larger paradigm shift.

Feature	Mass Spectrometry (MS)	Nuclear Magnetic Resonance (NMR) Spectroscopy
Primary Use Case	Comprehensive, untargeted analysis; high-sensitivity detection.	Rapid screening; simultaneous parent/metabolite analysis.
Sensitivity	Very high sensitivity (<μM)	Lower sensitivity than MS
Sample Preparation	More extensive; can be complex	Minimal pre-analytical preparation time
Destructive/Non-Destructive	Destructive	Non-destructive; can be applied to biofluids or tissues
Simultaneous Detection of Parent & Metabolites	Possible but can be challenging	Has the potential to detect and quantify simultaneously
Identification of Novel Compounds	Highly effective with HRMS	Can suggest presence of unknown compounds
Cost & Time	High solvent consumption; analysis can be long	Short analysis time; lower cost per sample

Table : Comparative Features of Mass Spectrometry (MS) and Nuclear Magnetic Resonance (NMR) Spectroscopy

Pioneering Applications: From Overdose to Patient Safety

The toxicometabolomics conceptual advancements are being effectively used in practical applications in both the criminal and medical world, with the possibility of witnessing the field move from reactive analysis to proactive predictive modelling.

In post-mortems, toxicometabolomics provides a new degree of definition. The imprecision of post-mortem redistribution and endogenous product formation influences that may confuse conventional toxicology may be overcome through examination of the metabolic profile of the body. For example, scientists are utilizing this methodology to differentiate antemortem GHB consumption from post-mortem product formation based upon examination of the urine/blood concentration ratio and other specific markers of metabolism. This enables more precise characterization of the cause and manner of death, with more definition in complex scenarios in which conventional techniques are unclear. It also offers a strong paradigm for the definition of unknown compounds in the poly pharmaceutical scenario of an overdose, specifically meeting the challenge of NPS. Through examination of the metabolic fingerprint of an event of toxaemia, the methodology may offer a specific "metabolomic profile" or "signature" of the effect of the toxicant, even when the parent molecule is new or unfamiliar in the contents of the conventional library.

In addition to the corpse, toxicometabolomics is also on the cusp of transforming the pharmaceuticals sector. The fundamental value proposition of the field is that it is predictive. Through toxicometabolomics, scientists can transition from reactive analysis to predictive modelling. Preclinical and clinical applications of toxicometabolomics enable the prediction as well as in vitro and in vivo screen-based prediction of drug-induced toxicity at a relatively early phase in the development pipeline. By establishing the presence of the toxicological biomarkers and adverse effects prior to clinical approval, the practice offers the potential to obviate the necessity for large-scale animal testing and the possibility of late-phase failures in the clinical phase. The discovery of the drugs Ivosidenib and Enasidenib against the oncometabolite D-2- hydroxyglutarate (D-2HG)identified through metabolomics is an exemplary demonstration of the paradigm shift.This predictive ability applies as much to personalized medicine as it does to toxicometabolomics. Through the examination of the person's specific metabolic profile, toxicometabolomics can foretell the person's response to a given drug, allowing for "personalized drug therapy" and the minimized possibility of adverse drug effects.The idea that the metabolome is "closest to the phenotype" entails that it reflects the compounded influence of the genetics, diet,and lifestyle upon the person'sresponse to the toxicant. This ability allows toxicologists to account for why two individuals given the same dosage of drug will have radically different results,promising a new epoch of precision toxicology. The end is the proactive avoidance of harm instead of the reactive response.



The Road Ahead: Data, Admissibility, and the Human Element

Despite its high promise, the practical application of toxicometabolomics at large is hindered significantly because of data management, legal admissibility, as well as ethical concerns. The biggest initial challenge is the volume and the nature of the data generated by the 'omics technologies. The metabolomics produces "vast amounts of complex data" that are "difficult to interpret" unless sophisticated computational tools are applied. The answer is the use of artificial intelligence (AI) and machine learning (ML), which can be employed in the optimization of experimental design, denoising of spectra, prediction of molecular structure, and the combination of data from various 'omics fronts. AI-based predictors are being constructed in order to elucidate the toxicity of novel chemical substances in the absence of prolonged in vivo experiments, which is an important objective in the field of the regulation toxicology.

But there is a critical issue here as well: many of the powerful ML models are "black boxes" that are "hard to interpret by toxicologists" and legal professionals.

Admissibility in court is the greatest barrier to universal application in forensics. While genomics saw decades of verification and validation in forensic DNA typing, other 'omics disciplines like metabolomics continue to be limited in the practical use within the courts. The fundamental disagreement is the legal system's demand for definitiveness and established error rates versus the variable and nuanced nature of the information from the 'omics fields. The demand for standardization and reproducibility across laboratories is therefore as much a scientific necessity as legal and moral imperative. Lastly, the human aspect cannot be discounted. Misuse of science in the courts may have "far- reaching consequences", elevating the stakes out of the realm of the abstract academic exercise. The potential for manipulation of the disciplines themselves by interested parties makes stringent, transparent, and objective methodologies essential. The toxicometabolomics of the future is as much about improved gear or more sophisticated algorithms as the building of the trust that will engender the new millennium of forensic scholarship. This mandates dedication to standardization, transparent reporting of the data, and more importantly, ethical rig our in all aspects of the science.

Conclusion

The future of forensic toxicology is no longer in the lone quest for the parent compound but in the comprehensive insight into the metabolic response of the body to the toxic agent. Toxicometabolomics is an ultimate paradigm shift from the reductionist, focused way of working to the holistic, systems-level exploration. The new field holds the promise of revealing complex routes of toxicities, characterize new drugs and their activities, as well as differentiate complicated biological events such as post-mortem redistribution from antemortem exposure.

Stimulated through the remarkable capabilities of instruments like high-resolution mass spectrometry and nuclear magnetic resonance spectroscopy, and powered through the exponential advances in artificial intelligence and machine learning, the field is poised to offer much more accurate, predictive, and finally, more realistic explanation of chemical exposure. Through the avoidance of the "numbers-only" fallacy and embracing the many-faceted, mechanistic view, toxicometabolomics is in the position to provide the much-needed context necessary in order to assign the correct meaning to an adverse event or death. But the last page of this revolution remains unwritten. The incorporation of this science within the legal apparatus depends upon the formulation of clear computational models, the definition of standard protocols, and an abiding dedication to the responsible practice of this science By overcoming these ultimate obstacles, toxicometabolomics will become more than just an influential new agent in the forensic armamentarium but will bring with it a new age of personalized therapy and hazard identification that is more holistic, more prophetic, and in the final analysis, more equitable.

References

1.Bouhifd M, Hartung T, Hogberg HT, Kleensang A, Zhao L. Review: Toxicometabolomics. Journal of Applied Toxicology. 2013 Dec;33(12):1365–83.

2. da Silva KM, Iturrospe E, Bars C, Knapen D, Van Cruchten S, Covaci A, et al. Mass Spectrometry-Based ZebrafishToxicometabolomics: A Review of Analytical and Data Quality Challenges. Metabolites [Internet]. 2021 Sep 1 [cited 2025 Sep 10];11(9):635. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC8467701/

3.OUH - Postmortem toxicology [Internet]. [cited 2025 Sep 10]. Available from: https://www.ous-research.no/no/rgda/Research%20projects/22527

4.Strehmel N, Vejmelka E, Kastner K, Roscher S, Tsokos M, Scholtis S. NPS-findings in forensic toxicology-three case reports.

5.Goli P. Advances and Challenges in Forensic Toxicology. 2024;

6.Saba A. International Journalof Forensic SciencesCommitted to Create Value for Researchers Forensic Toxicology: Advances in the Identification of New Psychoactive Substances (NPS) Opinion. 2025;

7.Komoroski EM, Komoroski RA, Valentine JL, Pearce JM, Kearns GL. The use of nuclear magnetic resonance spectroscopy in the detection of drug intoxication. J Anal Toxicol [Internet]. 2000 [cited 2025 Sep 10];24(3):180–7. Available from: https://www.researchgate.net/publication/12541274_The_Use_of_Nuclear_Magnetic_Resonance_Spectroscopy_in_the_Detection_of_Drug_Intoxication

8.Pang H, Hu Z. Metabolomics in drug researchand development: The recent advancesin technologies and applications. Acta Pharm Sin B. 2023 Aug 1;13(8):3238–51.

9.Postmortem Toxicological Investigation of Drug Overdose Deaths. [cited 2025 Sep 10]; Available from: https://www.aafs.org/asb-standard/standard-analytical-scope-and-sensitivity-forensic-toxicological-testing-blood-0.

10.Xu C, Rezeng C, Li J, Zhang L, Yan Y, Gao J, et al. 1H NMR-based metabolomics study of the toxicological effects in rats induced by “Renqing mangjue” pill, a traditional tibetan medicine. Front Pharmacol [Internet]. 2017 Sep 4 [cited 2025 Sep 10];8(SEP):602. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC5591455/
11.Computational Toxicology: Modeling and Predicting Adverse Effects [Internet]. [cited 2025 Sep 10]. Available from: https://www.azolifesciences.com/article/Computational-Toxicology-Modeling-and-Predicting-Adverse-Effects.aspx
12.Galal A, Talal M, Moustafa A. Applications of machine learningin metabolomics: Disease modeling and classification. Front Genet. 2022 Nov 24;13:1017340.
13.Where AI May Be Used in Metabolomic Research:Data Acquisition [Internet]. [cited 2025 Sep 10]. Available from: https://zontal.io/where-ai-may-be-used-in-metabolomic-research-data- acquisition/
14.Jia X, Wang T, Zhu H. Advancing Computational Toxicology by Interpretable Machine Learning. Environ Sci Technol [Internet]. 2023 Nov 21 [cited 2025 Sep 10];57(46):17690. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC10666545/
15.Chighine A, Locci E. Daubert and Omics: Exploring the Use of Complex Scientific Evidence in Court. 2025 Feb 21 [cited 2025 Sep 10]; Available from: https://www.researchgate.net/publication/389231189_Daubert_and_Omics_Exploring_the_Use a._of_Complex_Scientific_Evidence_in_Court
16.Yahya FA, Hashim NFM, Ali DAI, Ling TC, Cheema MS, Yahya FA, et al. A brief overview to systems biologyin toxicology: The journey from in to vivo, in-vitroand –omics. J King Saud Univ Sci [Internet]. 2021 Jan 1 [cited 2025 Sep 10];33(1). Available from: https://jksus.org/a-brief- overview-to-systems-biology-in-toxicology-the-journey-from-in-to-vivo-in-vitro-and-omics/
17.Sturla SJ, Boobis AR, Fitzgerald RE, Hoeng J, Kavlock RJ, Schirmer K, et al. Systems toxicology: From basic researchto risk assessment. Chem Res Toxicol [Internet]. 2014 Mar 17 [cited 2025 Sep 10];27(3):314–29. Available from: a./doi/pdf/10.1021/tx400410s?ref=article_openPDF
18.Metabolites | Special Issue : Toxicometabolomics [Internet]. [cited 2025 Sep 10]. Available from: https://www.mdpi.com/journal/metabolites/special_issues/Toxicometabolomics
19.Araújo AM, Carvalho F, De Pinho PG, CarvalhoM. Toxicometabolomics: Small Molecules to Answer Big Toxicological Questions. Metabolites [Internet]. 2021 Oct 1 [cited 2025 Sep 10];11(10):692. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC8539642/
20.5 Case Studies In Forensic Toxicology | Forensic Pathology Forum [Internet]. [cited2025 Sep 10]. Available from: https://pathologyexpert.blogspot.com/2016/01/5-case-studies-in-forensic- toxicology.html

ABOUT THE AUTHOR

Mr. Harwani Sagar
Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, India.



Ms. Smita Das
Assistant Professor
Department of Forensic Science, Parul Institute of Applied Science Parul University, Vadodara, Gujarat, India.



IMPACT OF ACID DIGESTION METHOD ON THE DETERMINATION OF HEAVY METALS IN LAKE WATER : A COMPARATIVE EDXRF ANALYSIS IN GANDHINAGAR, GUJARAT.



Author : Punnya C V

Abstract

The present research utilizes Energy Dispersive X-ray Fluorescence (EDXRF) spectroscopy to detect elements in water samples collected from different Gandhinagar water bodies in Gujarat. The analysis of samples occurred with and without acid digestion to evaluate how the preparation step affected metal detection. The research results demonstrated that different sampling locations presented varying levels of Fe, Mn, Zn, Cu and Pb elements. Acid digestion solutions enhanced the ability to detect several trace metals in samples which highlights the critical importance of proper environmental water sample preparation techniques for quality monitoring activities. This work demonstrates the need for ongoing water resource monitoring as well as confirms that EDXRF stands as a prompt and precise non-destructive method suitable for environmental element detection.

Keywords: Water quality, EDXRF analysis, Acid digestion, Trace metals, Gandhinagar lakes, Environmental monitoring, Elemental analysis

Introduction

Natural water sources, including lakes, rivers, and groundwater bodies are important for human use, including drinking, agricultural, and industrial purposes. However, these sources are continuously being put under risk by heavy metal pollution, which is an example of an environmental problem. Lead (Pb), Mercury (Hg), Cadmium (Cd), Arsenic (As), and Chromium (Cr) are among the most recognized heavy metals that are poisonous even in very low doses and will most certainly bioaccumulate in the water bodies, subsequently affecting the quality of life and biodiversity [1,2]. Heavy metals can find their way into water systems from a variety of natural and anthropogenic sources. Natural sources involve mechanical weathering of rocks, volcanic eruptions, and soil degradation, whereas anthropogenic sources involve industrial effluent, mining, and agricultural activities compounded by improper waste management [3,4]. Metals are purged into the environment in a very different manner and then left to sediment in oceans or be adopted by aquatic creatures, which causes bioaccumulation and biomagnification [5].

With exposure to heavy metals, human beings, especially children can suffer from extensive health problems like neurological issues, kidney damage, and developmental disorders [1,6]. Apart from this, metal toxicity disrupts aquatic life by endangering the growth, reproduction, and survival of many species. Hence, routine heavy metal contamination checks and remediation techniques are imperative for both ecological and human health. These problems can be addressed by developing more advanced and automated analytical procedures.Heavy metal quantification in water bodies is necessary for environmental monitoring, public health, and regulatory adherence. It is used to determine contamination levels, detect pollution sources, and implement remediation measures [7]. Ecosystem protection is vital to prevent bioaccumulation and biomagnification in aquatic organisms. Ensuring human health safety guarantees drinking water is safe, minimizing risks such as neurological injury and cancer [1]. Regulatory compliance facilitates industries and agencies in meeting environmental standards. Furthermore, quantification assesses the efficiency of water treatment methods [8].

Acid digestion is one of the most important sample preparation methods applied in environmental chemistry for trace metal analysis of water. It involves treating water samples with concentrated acids to disintegrate suspended solids, organic material, and complex species, thereby mobilizing bound metals into a dissolved state [9,10].



This ensures accurate measurement of metals present in both dissolved and particulate-bound forms. Common acids used include nitric acid (HNO_3), hydrochloric acid (HCl), or mixtures such as aqua regia (HNO_3 + HCl), depending on the sample type and analysis method. Digested samples are then analyzed using ICP-OES, ICP-MS, AAS, or EDXRF techniques [11].

In past studies, Kazi et al. [11] evaluated a UAD-based method for determining heavy metals in environmental and biological samples using ETAAS, finding no significant difference in recovery compared to conventional methods. Turek et al. [12] studied digestion procedures for sewage sludge and found that microwave digestion after drying was the most effective method. Alsehli [13] found microwave digestion most effective for analyzing heavy metals in Mentha samples in Saudi Arabia. Dimpe et al. [14] assessed hot plate and microwave digestion for metal extraction in wastewater and sludge samples prior to ICP-OES determination.

Methodology

The present study aims to understand the impact of acid digestion method on the determination of heavy metals in lake water.

Study area : Four different lakes of Gandhinagar, Gujarat are selected for conducting the study.

Sample collection: 100 ml of water samples from each lake is collected.Sample preparation

(a)Acid digestion procedure

Take 50 ml of water in a beaker. Add 7 ml of conc. Nitric acid and 3 ml of conc. HCl, cover the mouth of the beaker with foil paper, and leave it overnight.

Sample Analysis

Both the acid digested and non – digested water samples were analysed in EDXRF – 7000. Prior to the analysis, the instrument was calibrated using the software. All information regarding the sample was added to the software. 5 ml of each sample were weighed using the analytical balance and kept in the sample holder and the detailed analysis was done. The sample holder was sterilised using methanol and cotton before the analysis of each sample.

Data analysis

The obtained results are interpreted as graphs using excel.

Result and Discussion

By interpreting the obtained results (before acid digestion), it was found that the elements like Cl, S, Si, Cu and Ca are present in significant quantities, but their concentration shows wide variations. In samples 2 and 4 , the highest concentration of the elements, such as Si and Cu, can be seen. The amounts of elements like Zn, Br, Ag and K are very low compared to others.The results (after acid digestion) suggest that there is a huge shift in the concentration of Cl in all the samples. And other elements like S, Si, Cu, Zn, Ca and K are present in very low concentrations. The variations in the metal concentration are because of matrix binding and complexation, as some metals are bound to organic matter, sediments or present as insoluble salts in untreated samples. The solubility difference of elements also affects the variation in the concentration.

Sr. No.	Source	Date of Collection	Time	Temperature	Humidity
1	Adalaj lake	7/3/2025	5:40 PM	37°C	14%
2	Kobha lake	7/3/2025	4:45 PM	37°C	14%
3	Kudasan lake	7/3/2025	6:06 PM	35°C	15%
4	Vavol lake	7/3/2025	6:40 PM	35°C	15%

Table : Details of Water Sample Collection from Various Lakes

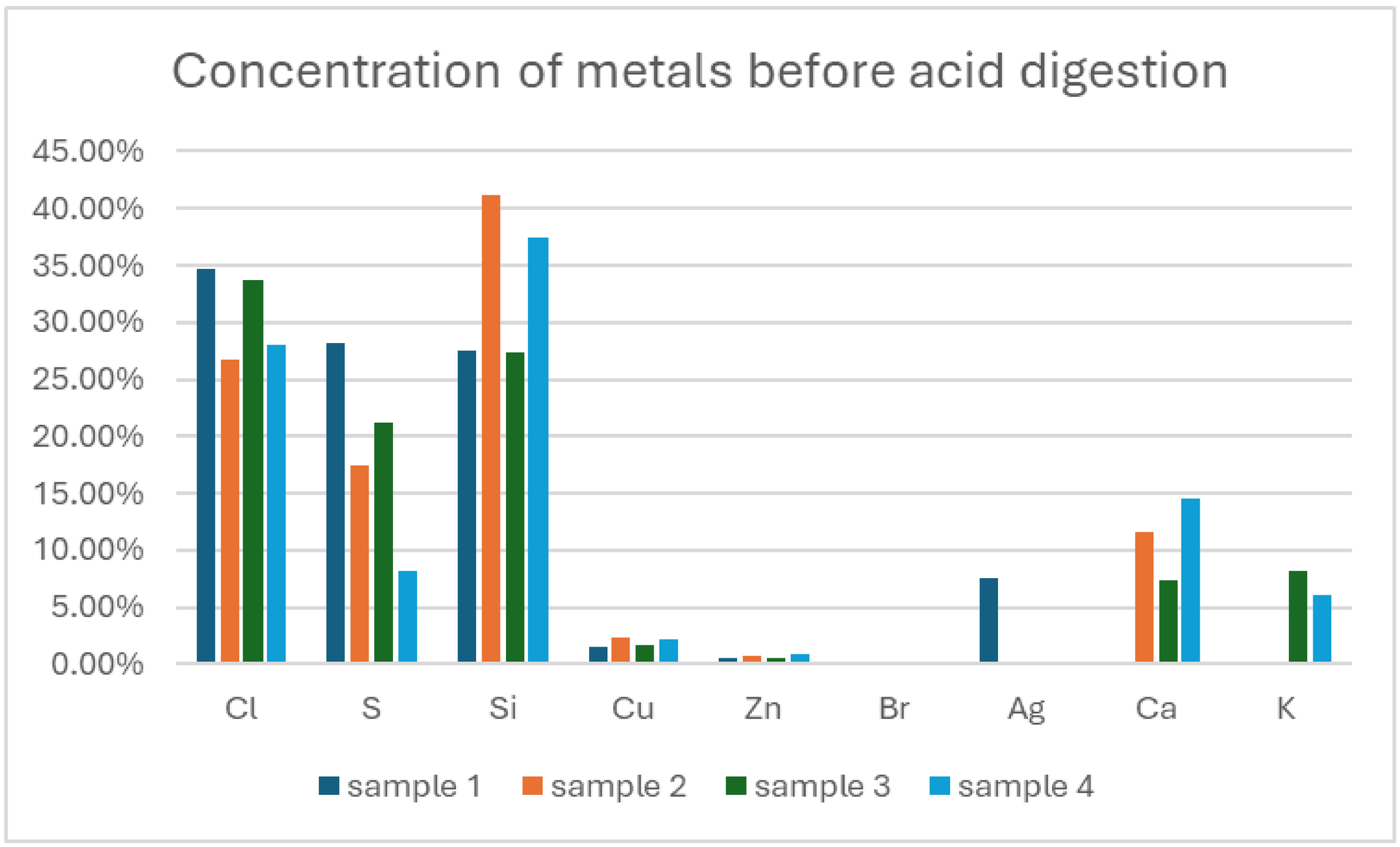


Fig 1 : Concentration of metals before acid digestion

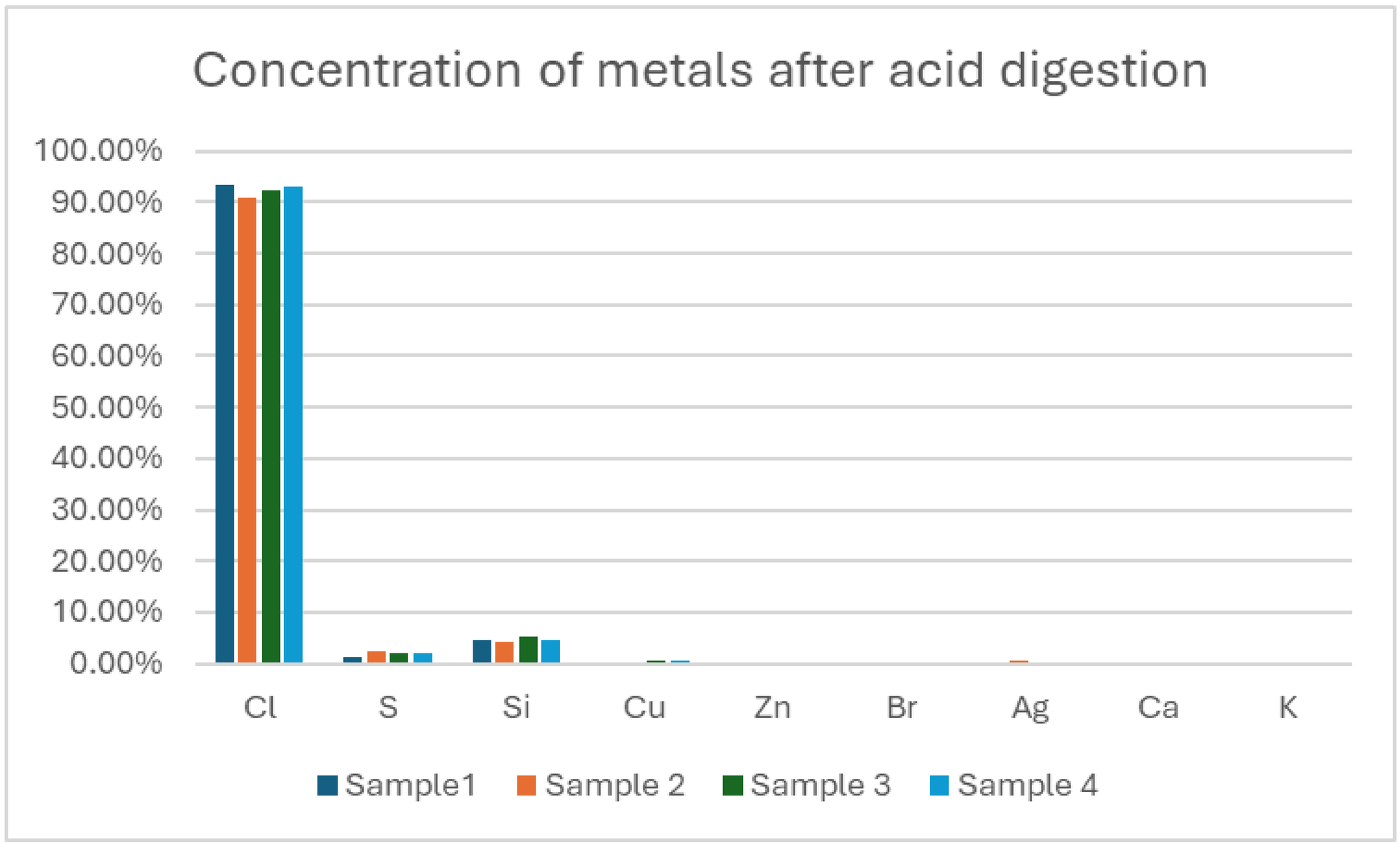


Fig 2: Concentration of metals after acid digestion

Conclusion

Water samples from various lakes of Gandhinagar, Gujarat were explored for elemental analysis with the facility of EDXRF spectroscopy. Two entirely different preparation procedures were employed: that is direct analysis and acid digestion. The results showed large discrepancies from one method to the other in the measured concentrations of metals. With respect to the EDXRF detection limits, acid digestion yields far higher concentrations of many elements as opposed to direct analysis, indicating that it aids in releasing metals otherwise bound within suspended particulates or complex matrices. Iron, zinc, manganese, and copper were particularly found to be largely enhanced by digestion, indicating their presence in particulate matter or organic complexes in the raw water samples. In addition, the study accentuates the importance of preferred sample preparation for trace metal analysis by EDXRF.

Conclusion Cont.

Failure to do so would imply an underestimation of the actual extent of metal contamination in aquatic ecosystems leading to a poor evaluation of the quality of surface waters. Our results strengthen the need for an appropriate analytical schema dependent on the study's objective and the nature of the sample matrix.This comparative study generally reveals that, while elemental analysis through EDXRF represents a solid non-destructive analytical technique, its appropriateness for water quality monitoring is immensely enhanced when it is integrated with acid digestive methods. Future research should emphasize optimization of digestion methods and correlation of EDXRF data with others considered to be well-established methods like ICP-MS or AAS for confirming and improving the accuracy of water pollution assessment.

References

1.Ali H, Khan E, Ilahi I. Environmental chemistry and ecotoxicology of hazardous heavy metals: Environmental persistence, toxicity, and bioaccumulation. J Chem. 2019;2019:6730305. Doi:10.1155/2019/6730305

2.Fawzy MA, El-Sahn MA, Ahmed MT. Heavy metal contamination in water and sediments of aquatic ecosystems: A review of sources, pollution, and risks. Environ Monit Assess. 2021;193(5):276. Doi:10.1007/s10661-021-09021-7

3.Wuana RA, Okieimen FE. Heavy metals in contaminated soils: A review of sources, chemistry, risks, and best available strategies for remediation. ISRN Ecol. 2011;2011:402647. Doi:10.5402/2011/402647

4. .He B, Yun Z, Shi J, Jiang G. Research progress of heavy metal pollution in China: Sources, analytical methods, status, and toxicity. Chin Sci Bull. 2013;58:134–40. Doi:10.1007/s11434-012-5564-4

5.Bhateria R, Jain D. Water quality assessment of lake water: A review. Sustain Water Resour Manag. 2016;2:161–73. Doi:10.1007/s40899-015-0014-7

6.U.S. Environmental Protection Agency (EPA). Method 3051A: Microwave assisted acid digestion of sediments, sludges, and soils. Washington (DC): EPA; 2007. Available from: https://www.epa.gov/esam/method-3051a-microwave-assisted-acid-digestion-sediments-sludges-and-soils

7.Hassan NM, Rasmussen PE, Dabek-Zlotorzynska E, Celo V. Analysis of environmental samples using acid digestion procedures and ICP-MS: A review. Appl Spectrosc Rev. 2007;42(6):499–551. Doi:10.1080/05704920701551541

8.Dean JR. Methods for environmental trace analysis. Chichester: John Wiley & Sons; 2003. Doi:10.1002/0470868372

9.Matusiewicz H, Ślachciński M. Microwave-assisted wet digestion in the analysis of environmental and biological samples. TrAC Trends Anal Chem. 2013;50:52–67. Doi:10.1016/j.trac.2013.04.010

10.Rao CRM, Biju VM. Extraction, preconcentration, and determination of heavy metals in environmental samples. Sep Purif Rev. 2014;43(1):1–43. Doi:10.1080/15422119.2012.656728

11.Kazi TG, et al. Evaluation of an ultrasonic acid digestion procedure for total heavy metals determination in environmental and biological samples. J Hazard Mater. 2008;161(2–3):1391–8. Doi:10.1016/j.jhazmat.2008.04.103

12.Turek A, et al. Digestion procedure and determination of heavy metals in sewage sludge An analytical problem. Sustainability. 2019;11(6):1753. Doi:10.3390/su11061753

13.Alsehli B. Evaluation and comparison between a conventional acid digestion method and a microwave digestion system for heavy metals determination in Mentha samples by ICP-MS. Egypt J Chem. 2020;63(12):4503–12. Doi:10.21608/ejchem.2020.43322.2874

14.Dimpe K, et al. Evaluation of sample preparation methods for the detection of total metal content using inductively coupled plasma optical emission spectrometry (ICP-OES) in wastewater and sludge. Phys Chem Earth. 2014;76–78:42–8. Doi:10.1016/j.pce.2014.11.006

ABOUT THE AUTHOR



Punnya C V
M.Sc. Forensic Science
RRU Gujrat



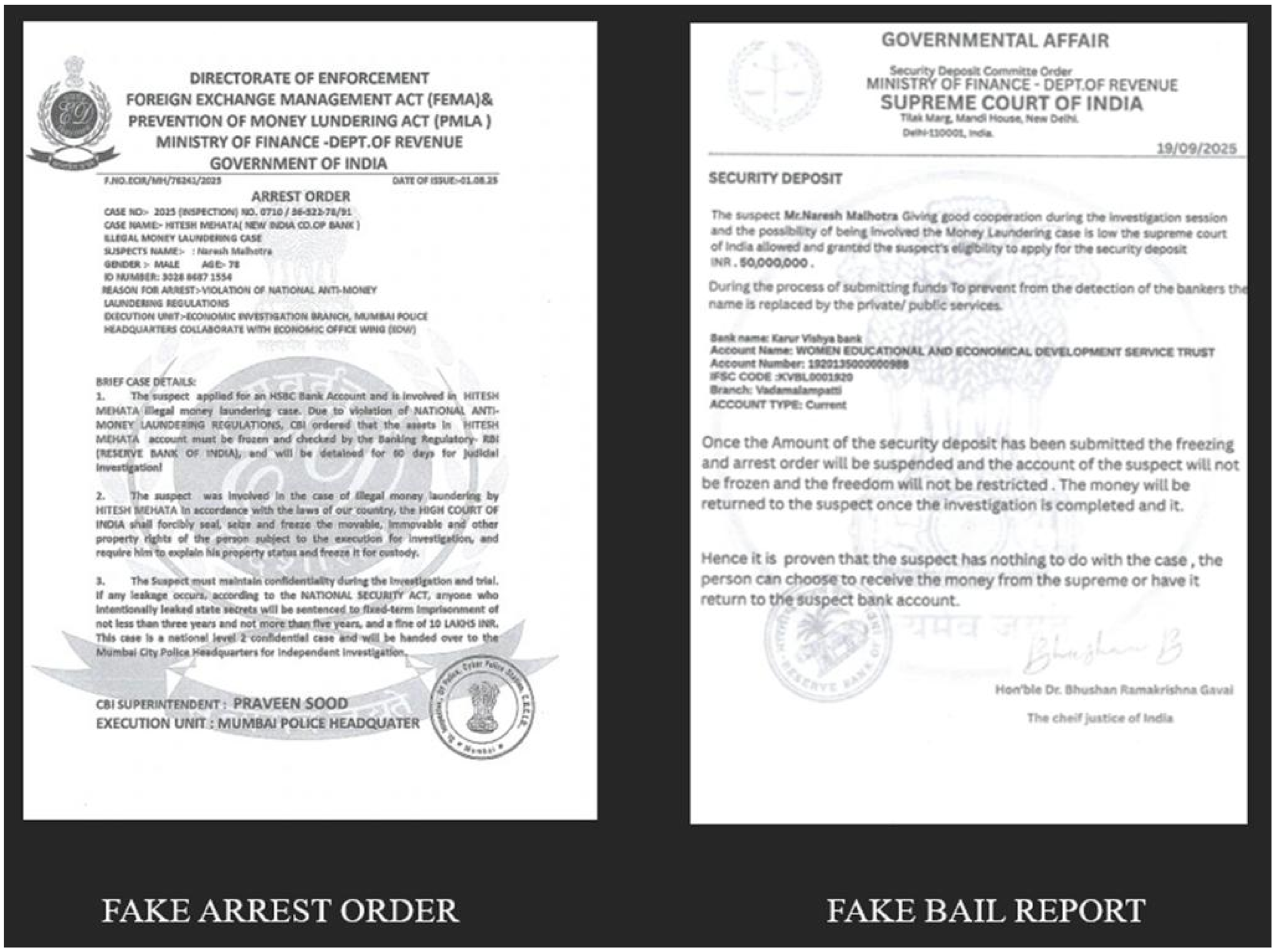
Crime Without Contact: The Anatomy of a ₹23 Crore Digital Arrest Scam



In an age where cybercriminals have no use of guns, weapons, disguises, or physical breaking, a new kind of crime has arisen one based on fear, trickery, and mind games. One of the most chilling examples is the Digital Arrest Scam, a diabolical strategy that leads victims to believe they are in police custody without ever setting foot in a cell. In September 2025, Delhi witnessed a case that pushed fraud to its limits. A former banker, who had once been placed with the responsibility of keeping others wealth safe, was forced to withdraw (22.92) ~₹23 crore his lifelong savings, under the false impression of being probed by the police. There were no disabled locks, no silenced alarms, and no masked burglars. The victim, rather, was in "virtual handcuffs" separated, threatened, and psychologically cornered into draining his own accounts. This was not merely a monetary con a forensic and psychological tutorial on how technology can be used to perpetrate crimes remotely. As India moves from physical robberies to cyber fakery, this case is a stark reminder: criminals today require nothing more than a smartphone, an engaging script, and the talent to play upon fear in order to orchestrate devastating losses. The victim, Naresh Malhotra, 78-year-old retired bank employee, was first contacted on August 1, 2025 by a woman claiming to be from a telecom company, identifying herself as an Airtel representative and alleged his landline number was being used for illegal activities. She claimed these accounts were linked to a Rs 1,300 crore terror funding case related to Pulwama. This was followed by a well-choreographed psychological trap.He was soon contacted by others posing as officials from the Mumbai Police, Enforcement Directorate (ED), and Central Bureau of Investigation (CBI), who threatened him with serious legal action, lying that his name had come up in a money laundering probe related to criminal activities and accused him linking to terrorist groups.

In order to make the trick realistic, the swindlers used sophisticated methods like: video calls with impersonators of police officers, fake ID documents, virtual backgrounds replicating actual investigation offices.

He was informed that he was "digitally arrested" an invented legal condition that is registered under NATIONAL SECRET ACT and he was asked to remain under surveillance without leaving his home, forced him to attend video calls every two hours starting from 8:00 a.m. to evening 8:00p.m.



DIRECTORATE OF ENFORCEMENT
FOREIGN EXCHANGE MANAGEMENT ACT (FEMA)&
PREVENTION OF MONEY LUNDERING ACT (PMLA)
MINISTRY OF FINANCE -DEPT.OF REVENUE
GOVERNMENT OF INDIA

F.NO.ECIR/MH/76241/2025 DATE OF ISSUE:-01.08.25

ARREST ORDER

CASE NO:- 2025 (INSPECTION) NO. 0710 / 36-323-78/91
CASE NAME:- HITESH MEHATA(NEW INDIA CO.OP BANK)
ILLEGAL MONEY LAUNDERING CASE
SUSPECTS NAME:- : Naresh Malhotra
GENDER :- MALE AGE:- 78
ID NUMBER: 3028 8687 1554
REASON FOR ARREST:-VIOLATION OF NATIONAL ANTI-MONEY LAUNDERING REGULATIONS
EXECUTION UNIT:-ECONOMIC INVESTIGATION BRANCH, MUMBAI POLICE HEADQUARTERS COLLABORATE WITH ECONOMIC OFFICE WING (EOW)

BRIEF CASE DETAILS:

1. The suspect applied for an HSBC Bank Account and is involved in HITESH MEHATA illegal money laundering case. Due to violation of NATIONAL ANTI-MONEY LAUNDERING REGULATIONS, CBI ordered that the assets in HITESH MEHATA account must be frozen and checked by the Banking Regulatory- RBI (RESERVE BANK OF INDIA), and will be detained for 60 days for Judicial investigation!

2. The suspect was involved in the case of illegal money laundering by HITESH MEHATA in accordance with the laws of our country, the HIGH COURT OF INDIA shall forcibly seal, seize and freeze the movable, immovable and other property rights of the person subject to the execution for investigation, and require him to explain his property status and freeze it for custody.

3. The Suspect must maintain confidentiality during the investigation and trial. If any leakage occurs, according to the NATIONAL SECURITY ACT, anyone who intentionally leaked state secrets will be sentenced to fixed-term imprisonment of not less than three years and not more than five years, and a fine of 10 LAKHS INR. This case is a national level 2 confidential case and will be handed over to the Mumbai City Police Headquarters for independent investigation.

CBI SUPERINTENDENT : PRAVEEN SOOD
EXECUTION UNIT : MUMBAI POLICE HEADQUATER

GOVERNMENTAL AFFAIR

Security Deposit Committe Order
MINISTRY OF FINANCE - DEPT.OF REVENUE
SUPREME COURT OF INDIA
Tilak Marg, Mandi House, New Delhi.
Delhi-110001, India.

19/09/2025

SECURITY DEPOSIT

The suspect Mr.Naresh Malhotra Giving good cooperation during the investigation session and the possibility of being involved the Money Laundering case is low the supreme court of India allowed and granted the suspect's eligibility to apply for the security deposit INR . 50,000,000 .

During the process of submitting funds To prevent from the detection of the bankers the name is replaced by the private/ public services.

Bank name: Karur Vishya bank
Account Name: WOMEN EDUCATIONAL AND ECONOMICAL DEVELOPMENT SERVICE TRUST
Account Number: 1920135000000988
IFSC CODE :KVBL0001920
Branch: Vadamalampatti
ACCOUNT TYPE: Current

Once the Amount of the security deposit has been submitted the freezing and arrest order will be suspended and the account of the suspect will not be frozen and the freedom will not be restricted . The money will be returned to the suspect once the investigation is completed and it.

Hence it is proven that the suspect has nothing to do with the case , the person can choose to receive the money from the supreme or have it return to the suspect bank account.

Hon'ble Dr. Bhushan Ramakrishna Gavai
The cheif justice of India

FAKE ARREST ORDER

FAKE BAIL REPORT

They also made him sign an undertaking to keep the matter secret and prevented him from speaking to family members (two daughters, two sons-in-law, and four grandchildren), or revealing the scenario to anybody. They even threatened him with arrest and embarrassment in public, he was blackmailed into transferring money to different bank accounts for a couple of days, for a "verification procedure" to establish his innocence.

To gain his trust, they sent him a fake bail order and threatened to seize his passport, impose restriction on his foreign travels, and hurt his family.

The fraudsters from August 4 to September 4 withdrew Rs 23 crore from Malhotra's three bank accounts through 21 transactions via third party transfers and also got his Aadhar details, bank details and investment details.

Malhotra told that even his small withdrawals for day-to-day expenses and wages of employees needed to be sanctioned by the fraudsters, who had successfully dominated his life. Malhotra declined to undertake third-party transfers and remained adamant, saying that he would deposit ₹5 crore with the registrar of the Supreme Court but not with a private company. When Malhotra resisted, the fraudsters threatened with instant arrest and cut off the phone. Since he incurred enormous losses financially, Malhotra went to the police, and a First Information Report (FIR) in the matter was filed by the Intelligence Fusion and Strategic Operations (IFSO) Unit of Delhi Police on September 19.

Later, money equivalent to around Rs 2.3 crore that was routed from his bank accounts was put under freeze, and an inquiry was in progress.

AFTERMATH:

Within August 4, 2025- September 4, 2025, Malhotra visited these banks for 21 times where he held accounts Canara Bank, IndusInd Bank, and ICICI Bank as well as Union Bank and Axis Bank across different states, including Uttarakhand, West Bengal, Andhra Pradesh, and Tamil Nadu. Over the course of 21 visits, he transferred a total of ₹22.92 crore through 21 RTGS transactions to 16 separate bank accounts. (RTGS: Real Time Gross Settlement: is a high-value fund transfer system where large amount can be transferred immediate and irreversible payment making it the preferred choice for corporate transactions and urgent transfers above ₹2 lakh.) To make the scheme appear credible, the fraudsters even issued him a fake Reserve Bank of India (RBI) certificate.

What made this scam particularly sophisticated was how the stolen funds were laundered digitally. Although Malhotra himself executed only 21 transactions, the money eventually splintered into 4,236 smaller transactions across multiple layers and accounts.

Even though he was a retired banker with three decades of experience working with both government and private banks, even the branch managers had no idea about the digital arrest situation as Malhotra moved almost all of his lifetime savings. The affected branches were near his home, but proximity proved to be no deterrent to mental manipulation.

Ranjit Gupta, Joint Commissioner of the IFSO branch of Delhi Police, noted that layering of stolen funds in a digital arrest case is uncommon. While money typically moves through only a few layers, in this case it was spread across more than 4,000 transfers. He added that the golden hour for immediately reporting the losses was missed, making it extremely challenging to trace the scammers and freeze the funds.

FORENSIC RELAVANCE:

- Digital Forensics: Tracking ₹23 crore across multiple accounts and thousands of transactions required detailed analysis of banking records and communication logs.
- Psychological Profiling: Social engineering and fear tactics were central, showing how victims can be manipulated without physical contact.
- Document Forensics: Fake RBI certificates and bail orders were used to convince the victim, requiring verification to confirm fraud.
- Legal & Investigative Implications: Timely reporting and specialized units like IFSO are crucial to trace funds and prevent further losses.

The case highlights the evolving nature of cybercrime, where perpetrators require no physical presence only a convincing script, technological tools, and psychological manipulation to commit large-scale financial fraud. It also underscores the importance of immediate reporting and vigilance, as delays in raising alarms can exponentially increase the difficulty of recovering funds and apprehending criminals.

REFERENCES:

- ·https://www.indiatoday.in/cities/delhi/story/retired-delhi-banker-defrauded-23-crore-digital-arrest-scam-2791522-2025-09-22#google_vignette
- ·https://www.hindustantimes.com/cities/delhi-news/retired-banker-loses-23-crore-in-delhi-digital-arrest-fraud-101758394016258.html
- ·https://www.ndtv.com/delhi-news/ex-delhi-banker-loses-23-crores-in-digital-arrest-first-woman-called-then-ed-cbi-9321545/amp/1
- ·https://thecsrjournal.in/delhis-biggest-digital-arrest-scam-crore/

ABOUT THE AUTHOR

Vagdevi Emani
B.Sc. Forensic Science, Aditya Degree and PG College, Surampalem



Gundumogula Naga Ramadevi
B.Sc. Forensic Science, Aditya Degree and PG College, Surampalem





DECODING THE DEAD BEYOND DNA: NEXT GENERATION BIOMARKERS IN FORENSIC INVESTIGATION

Author: Mr. Bhumit Chavda, Dr. Kapil Kumar

Introduction: The Evolving Landscape of Forensic Evidence

The silent testament of biological material at a crime scene or in a post-mortem context holds profound secrets, often dictating the trajectory of an investigation. From the seminal work on blood typing to the revolutionary advent of DNA fingerprinting in the late 20th century, forensic science has consistently sought to extract maximal information from minimal biological traces. DNA, a robust and ubiquitous molecule, has deservedly commanded the spotlight for its capacity to definitively link individuals to evidence with astounding reliability (Smith & Jones, 2005). Yet, while DNA offers a static snapshot of identity, many critical forensic questions demand a more dynamic understanding of biological processes – particularly those occurring after death. The estimation of the Post-Mortem Interval (PMI) stands as one of the most challenging and critical aspects of forensic pathology. Traditional methods, relying on macroscopic observations such as algor mortis, livor mortis, rigor mortis, and insect activity, are often susceptible to environmental variables and suffer from wide margins of error, especially as the PMI extends (Brown et al., 2010). Similarly, understanding the precise nature of injuries, the physiological state of an individual leading up to death, or environmental exposures often requires delving deeper than the genetic code



This article posits that the future of forensic investigation lies in the comprehensive analysis of "next-generation biomarkers." These are not merely supplementary pieces of evidence but represent an entirely new class of molecular, biochemical, and microbial indicators that offer dynamic insights into the biology of death and the post-mortem environment. This paradigm shift promises to refine PMI estimation, characterize ante-mortem conditions with greater precision, and illuminate the intricate timeline of events in even the most challenging forensic cases. The subsequent sections will elaborate on these emerging biomarker categories, their methodologies, and their transformative potential for forensic investigation

RNA-Based Biomarkers: Unraveling the Post-Mortem Transcriptome

Unlike the robust and relatively stable DNA, RNA molecules are inherently labile, highly susceptible to degradation by ubiquitous RNases immediately upon cell death. This inherent instability, once considered a limitation, has now become its greatest strength in forensic science. The differential degradation rates of various RNA species offer a highly nuanced molecular clock, providing a potent tool for refining PMI estimation (Johnson & Lee, 2018).

Messenger RNA (mRNA) Degradation as a Molecular Clock

Messenger RNA (mRNA) molecules are transient carriers of genetic information from DNA to protein synthesis. Their abundance and integrity reflect active cellular processes. Post-mortem, these processes cease, and mRNA degradation begins rapidly. Crucially, not all mRNA molecules degrade at the same rate.

Genes involved in cellular maintenance (housekeeping genes) or stress responses often have more stable mRNA transcripts, while others degrade very quickly. By quantifying the ratio of intact to degraded mRNA fragments, or by analyzing the relative expression levels of specific mRNA transcripts known to have characteristic degradation profiles, forensic scientists can establish a more precise molecular timeline for PMI (Chang et al., 2020).Techniques such as quantitative reverse transcription polymerase chain reaction (RT-qPCR) and microarray analysis allow for the profiling of hundreds to thousands of mRNA transcripts simultaneously. For instance, specific mRNA transcripts in brain tissue, skeletal muscle, or even blood have been identified that exhibit predictable decay patterns over hours and days post-mortem. The key lies in establishing robust calibration curves for different tissues and environmental conditions, which can then be applied to forensic samples (Davies & Khan, 2019). The sensitivity of these methods means that even minute quantities of tissue can yield valuable information.

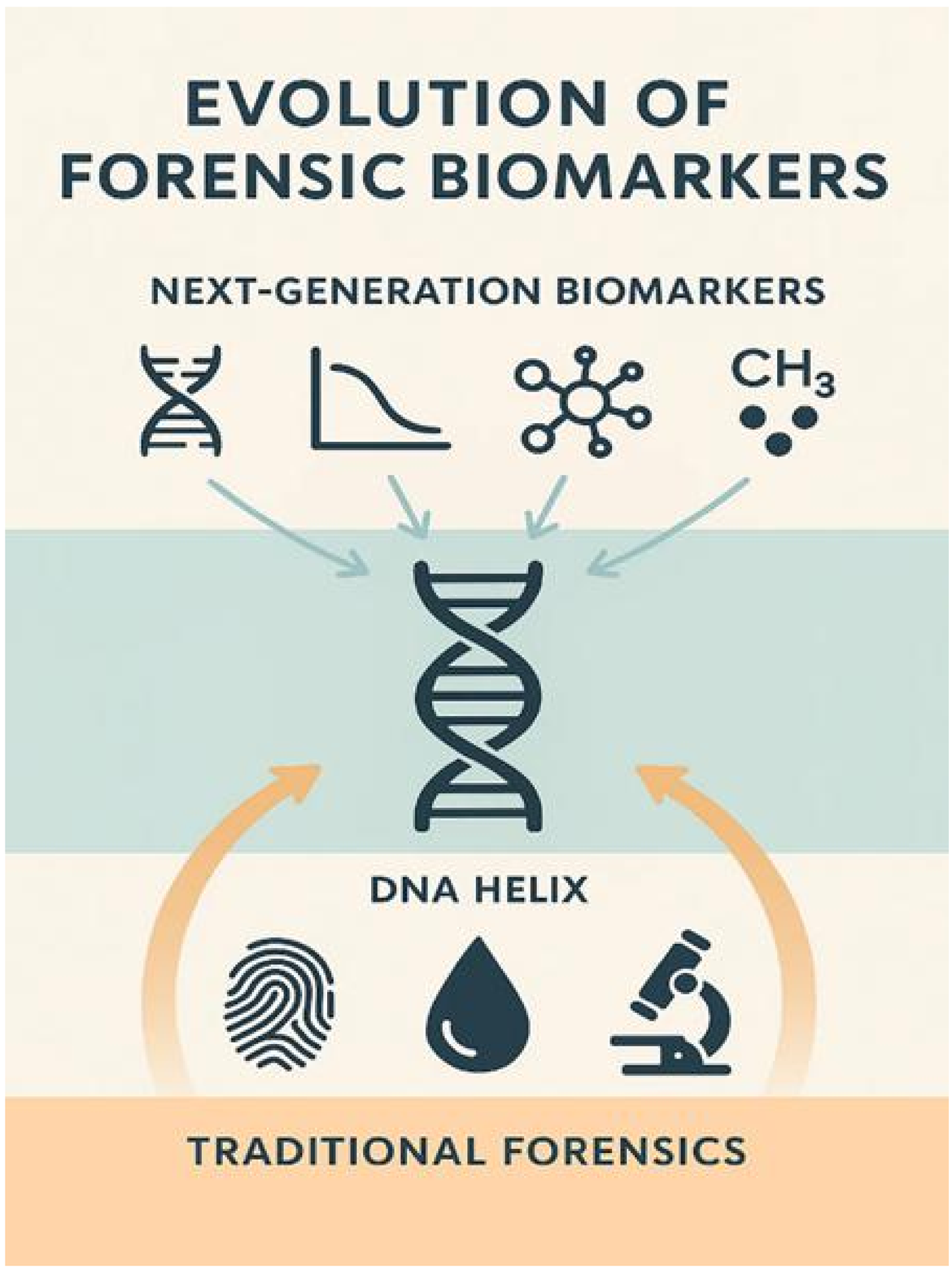


Fig. Evolution of Forensic Biomarker's

MicroRNA (miRNA) Stability and Expression

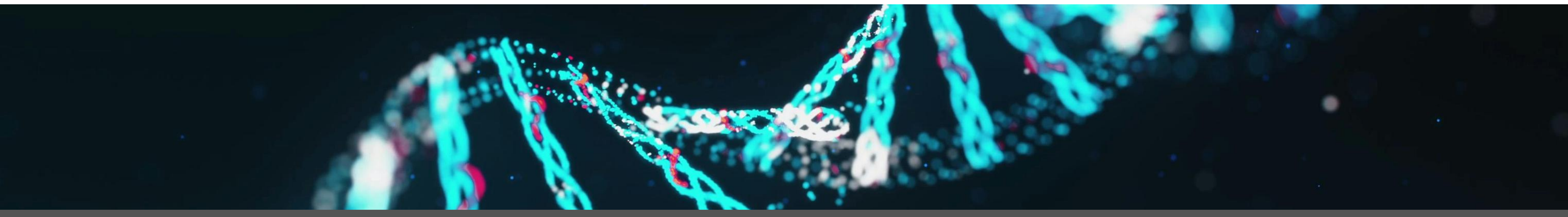
Beyond mRNA, microRNAs (miRNAs) represent a class of small, non-coding RNA molecules that play critical roles in regulating gene expression. Unlike mRNA, miRNAs are generally more stable in post-mortem tissues, protected from degradation by their small size and association with RNA-induced silencing complexes (RISC) (Gomez et al., 2017). This enhanced stability makes them attractive candidates for PMI estimation, particularly in cases with longer post-mortem intervals or challenging environmental conditions.

The expression profiles of specific miRNAs have been shown to change predictably over time in various tissues, including the heart, liver, and brain, after death. Some miRNAs show an upregulation, while others downregulate or remain relatively stable for extended periods. Analyzing these distinct patterns provides an additional layer of temporal information. For example, specific miRNAs might be detectable and show consistent changes days or even weeks after death, extending the window for molecular PMI estimation beyond that of highly labile mRNA (Patel & Singh, 2021).

Proteomics: The Dynamic World of Post-Mortem Proteins

Proteins are the workhorses of the cell, carrying out virtually all biological functions. Their diversity and dynamic nature make them exquisite biomarkers for various forensic applications, from PMI estimation to identifying tissue origin and even detecting ante-mortem stress (Liu et al., 2016). The field of proteomics, which involves the large-scale study of proteins, offers an unparalleled view into the functional state of tissues post-mortem.

Protein Degradation and Modification:



Similar to RNA, proteins undergo characteristic degradation and modification patterns after death. Proteases, enzymes responsible for protein breakdown, remain active for a period post-mortem, leading to a predictable cascade of protein cleavage. Different proteins are cleaved at different rates and in specific patterns, creating a unique molecular signature that correlates with PMI. Techniques like SDS-PAGE (sodium dodecyl sulfate-polyacrylamide gel electrophoresis), Western blotting, and particularly mass spectrometry (MS), enable the identification and quantification of these degradation products. Mass spectrometry-based proteomics can analyze thousands of proteins simultaneously. By tracking the decrease in full-length proteins and the concomitant increase in specific proteolytic fragments over time, researchers can construct robust models for PMI estimation. For example, specific muscle proteins like troponin or actin have well-characterized post-mortem degradation profiles that can serve as molecular markers (Garcia et al., 2018). Furthermore, post-translational modifications (PTMs) such as oxidation, deamidation, and phosphorylation also accumulate or change post-mortem, offering additional layers of information for temporal analysis (Chen & Wang, 2020).

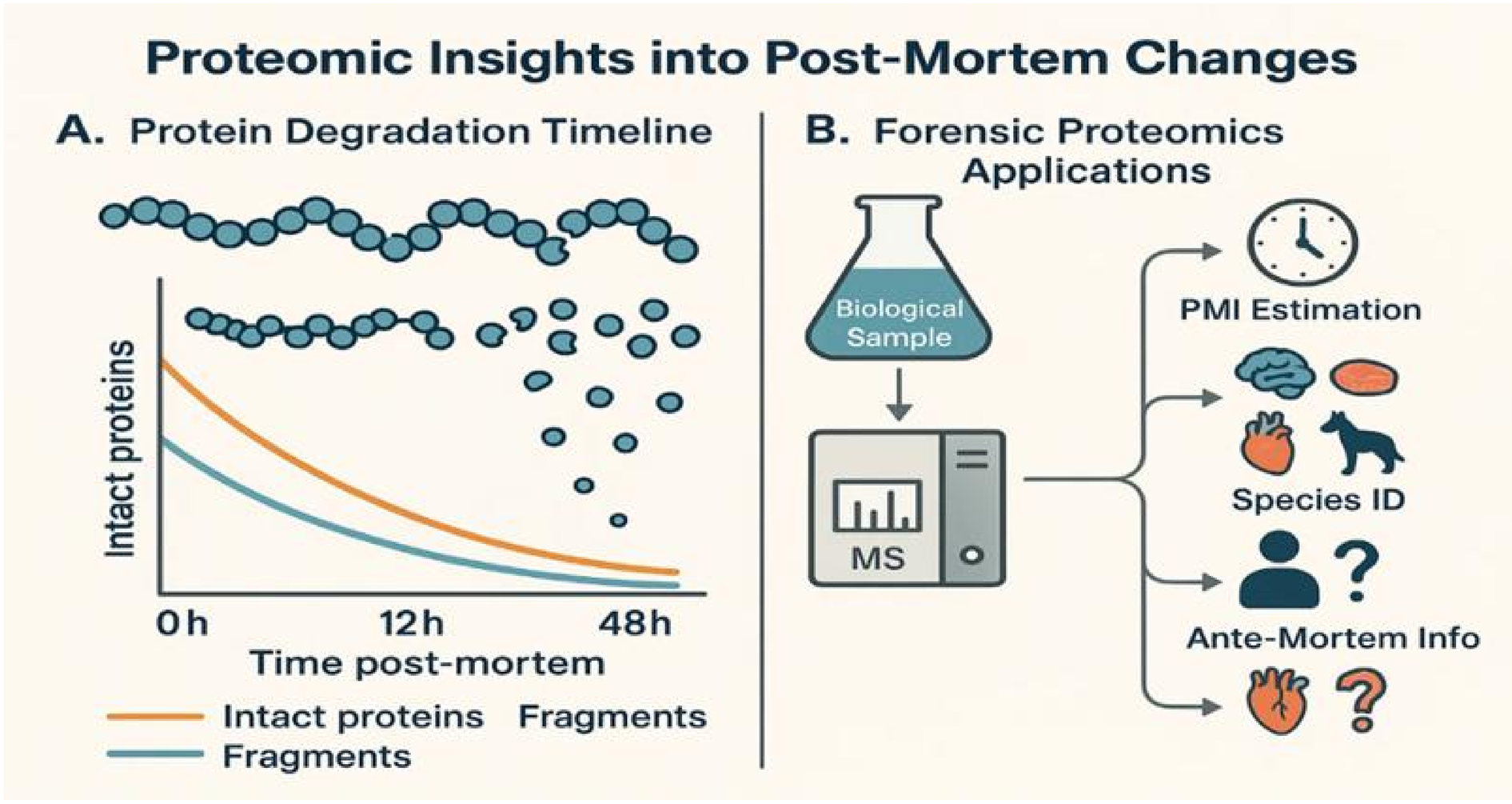


Fig. Protein insights into Post Mortem changes

Forensic Applications of Protein Biomarkers

Beyond PMI, proteomics holds immense potential for other forensic applications:

1.Tissue Identification: Different tissues express unique sets of proteins. Proteomic profiles can accurately identify the tissue origin of biological stains (e.g., blood, semen, saliva, brain, muscle) even when DNA is degraded or inconclusive (Nguyen et al., 2017).

2.Species Identification: While DNA is excellent for species identification, protein sequences can also differentiate between species, especially in highly degraded samples where DNA extraction might be challenging.

3.Ante-Mortem Conditions: Specific protein biomarkers can indicate ante-mortem physiological states or exposures. For instance, markers of inflammation, myocardial infarction, or drug exposure can be identified from post-mortem tissues, providing crucial insights into the circumstances leading to death (Schmidt & Mueller, 2019).

4.Injury Analysis: Certain proteins or their degradation products can differentiate between ante-mortem and post-mortem injuries, a critical distinction in cases of trauma.

Metabolomics: A Snapshot of Metabolic Activity at the Time of Death

Metabolomics is the large-scale study of small molecules, known as metabolites, within biological systems. These metabolites are the end products of cellular processes, providing a direct snapshot of the physiological state of an organism at a specific time (Johnson & Williams, 2015). Post-mortem, metabolic pathways cease, and metabolites begin to degrade or accumulate, offering a unique opportunity to decipher the precise moment and circumstances of death.

Post-Mortem Metabolite Profiling for PMI Estimation

Upon cessation of blood circulation and oxygen supply, cells switch from aerobic to anaerobic metabolism, leading to a rapid accumulation of certain metabolites (e.g., lactate) and depletion of others (e.g., glucose, ATP). The concentrations of various metabolites, such as amino acids, organic acids, lipids, and sugars, change predictably in different tissues (e.g., vitreous humor, brain, muscle, liver) after death. These changes are influenced by intrinsic factors (e.g., cause of death, age) and extrinsic factors (e.g., temperature, humidity), but when properly calibrated, they provide a robust molecular timer for PMI (Smith & Chen, 2018). Advanced analytical techniques like gas chromatography-mass spectrometry (GC-MS) and liquid chromatography-mass spectrometry (LC-MS) are employed to identify and quantify thousands of metabolites in a single sample. By analyzing complex metabolic signatures, researchers can develop sophisticated algorithms to estimate PMI with remarkable accuracy, often outperforming traditional methods in the early post-mortem period (Wang et al., 2022). The vitreous humor, a relatively isolated and stable fluid in the eye, has proven particularly valuable for metabolomic PMI estimation due to its slower post-mortem changes compared to highly metabolically active tissues.

Insights into Cause of Death and Ante-Mortem State

Beyond PMI, metabolomics offers unparalleled insights into the physiological state of an individual at the time of death and can aid in determining the cause of death:

1)Drug Overdoses and Toxins

2)Disease Markers:

3)Stress and Hypoxia

4)Environmental Exposure

The holistic nature of metabolomics, capturing the entire biochemical landscape, allows for a comprehensive understanding of the biological events immediately preceding and following death.

The Forensic Microbiome: Ecological Succession as a Death Indicator

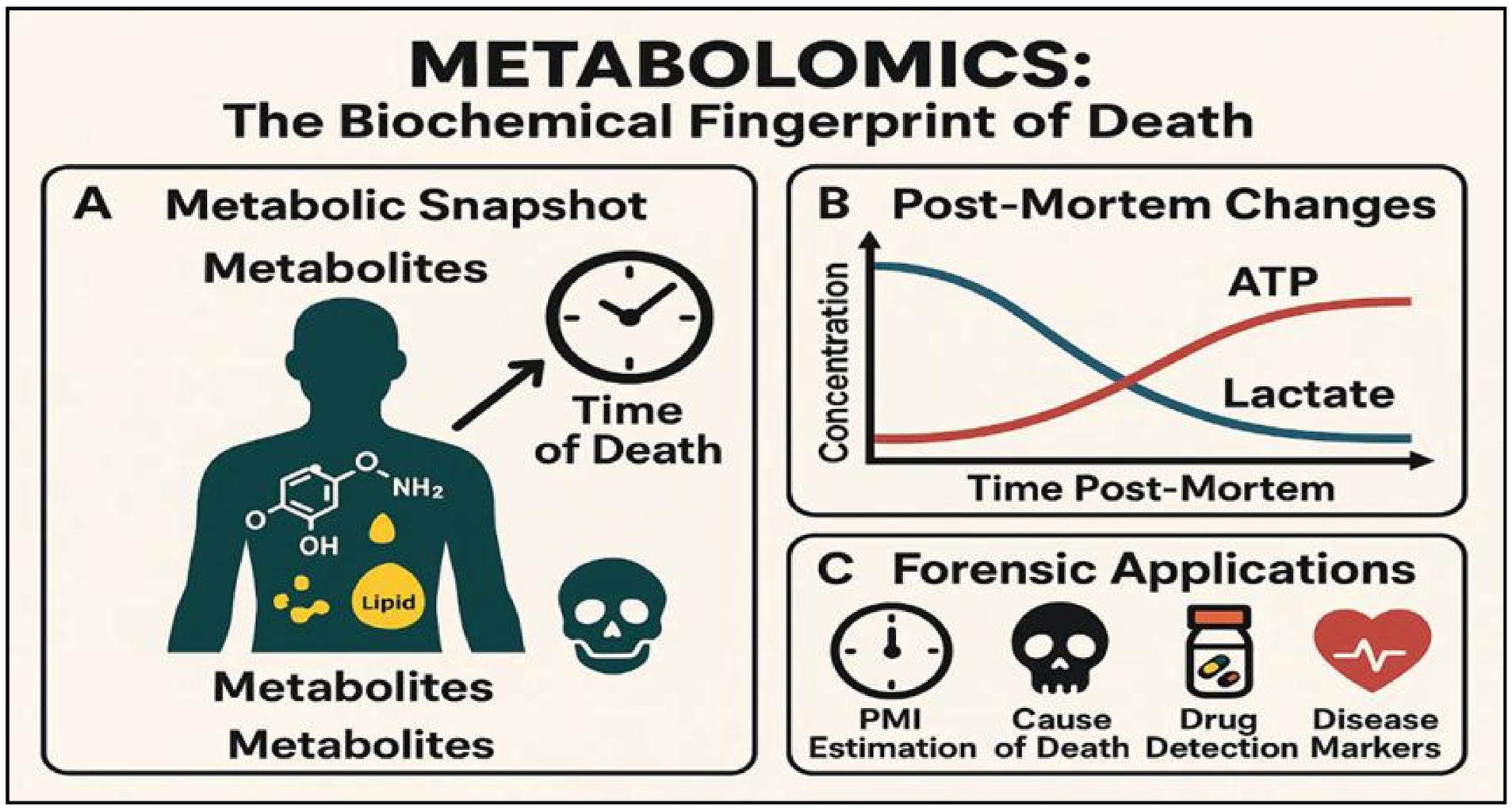


Fig. Metabolomic: the biochemical fingerprint of death

The human body is not a sterile entity but a complex ecosystem teeming with trillions of microorganisms, bacteria, archaea, fungi, and viruses – collectively known as the microbiome. Upon death, the host's immune system collapses, and the internal environment changes dramatically. This leads to a predictable, albeit complex, succession of microbial communities, transforming the body into a new ecosystem (Pechal et al., 2014). Studying these post-mortem microbial shifts, or the "thanatomicrobiome," offers a novel and powerful approach to forensic investigation.

Microbial Succession for PMI Estimation

The initial phase of decomposition involves the proliferation of anaerobic bacteria from the gut, which then spreads throughout the body. As decomposition progresses, environmental microbes colonize the body from the surrounding soil, water, or air. Different microbial species thrive and decline at specific stages of decomposition, creating a dynamic microbial clock (Hyde et al., 2013). High-throughput sequencing technologies (e.g., 16S rRNA gene sequencing for bacteria, ITS sequencing for fungi) allow for the comprehensive identification and quantification of these microbial communities.

By analyzing changes in microbial diversity, abundance, and community structure in various tissues (e.g., skin, gut, internal organs, soil directly beneath the body), researchers can establish correlations with PMI. For instance, specific bacterial genera might dominate in early PMI, while others emerge in later stages. The composition of the soil microbiome beneath a decomposing body can also be significantly altered, providing clues about both P

PMI and the location where decomposition occurred (Jadhav et al., 2020). While influenced by environmental factors such as temperature, humidity, and local microbial populations, standardized protocols and extensive reference databases are being developed to account for these variablesThe initial phase of decomposition involves the proliferation of anaerobic bacteria from the gut, which then spreads throughout the body. As decomposition progresses, environmental microbes colonize the body from the surrounding soil, water, or air. Different microbial species thrive and decline at specific stages of decomposition, creating a dynamic microbial clock (Hyde et al., 2013). High-throughput sequencing technologies (e.g., 16S rRNA gene sequencing for bacteria, ITS sequencing for fungi) allow for the comprehensive identification and quantification of these microbial communities.

By analyzing changes in microbial diversity, abundance, and community structure in various tissues (e.g., skin, gut, internal organs, soil directly beneath the body), researchers can establish correlations with PMI. For instance, specific bacterial genera might dominate in early PMI, while others emerge in later stages. The composition of the soil microbiome beneath a decomposing body can also be significantly altered, providing clues about both PMI and the location where decomposition occurred (Jadhav et al., 2020). While influenced by environmental factors such as temperature, humidity, and local microbial populations, standardized protocols and extensive reference databases are being developed to account for these variables

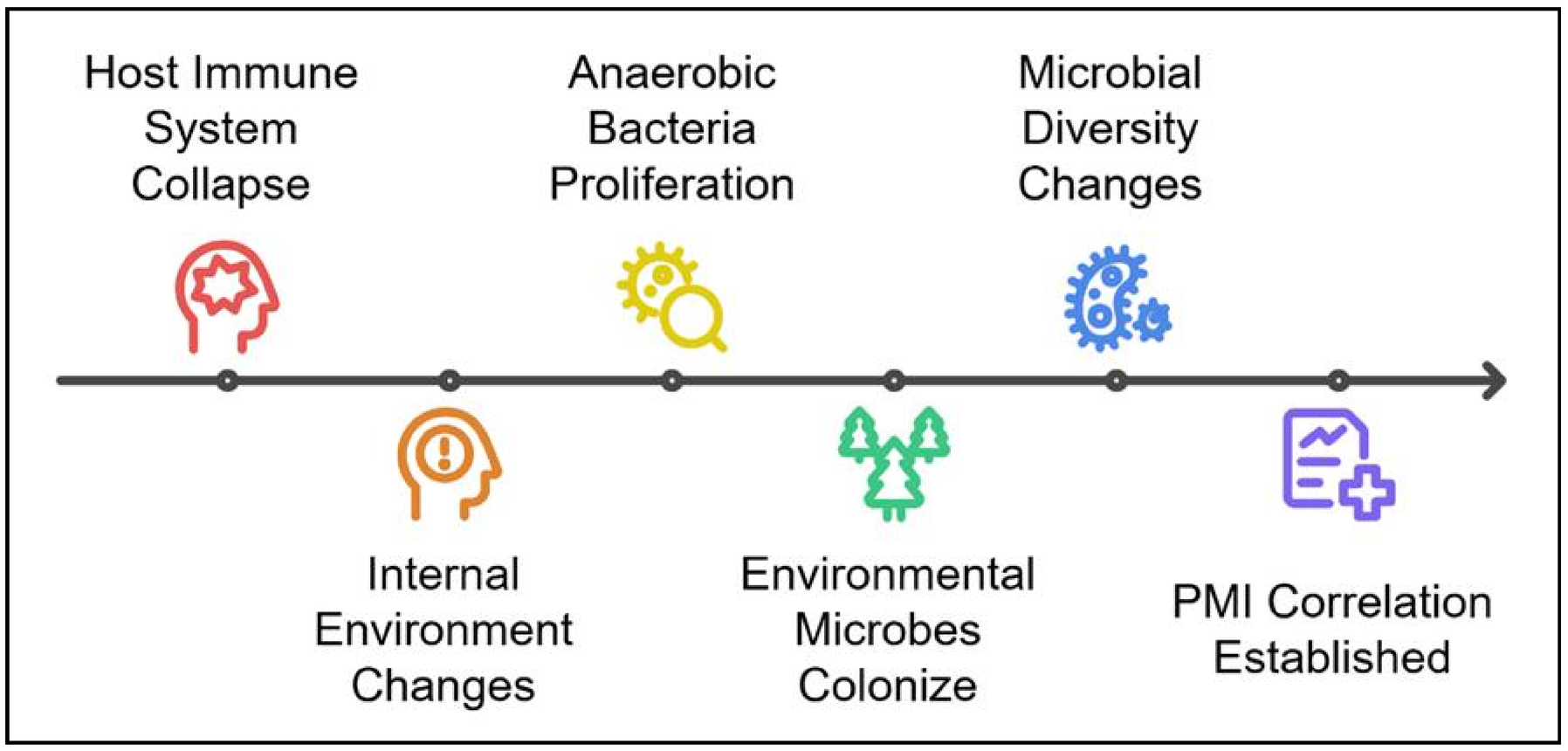


Fig. Microbial Succession in Decomposition

Geographic and Individual Signatures

Beyond PMI, the forensic microbiome offers unique capabilities for discerning geographic origin and even individual characteristics:

Geographic Origin: The composition of environmental microbes colonizing a body can reflect the unique microbial signature of a particular geographic location. This could be invaluable in cases where a body has been moved or to narrow down the search area for a perpetrator (Gibbs et al., 2018).

Body Movement: If a body is moved from one environment to another, the microbial communities associated with it may reflect a mixture of both original and new environments, potentially providing evidence of post-mortem relocation.

Individual-Specific Microbiome: While post-mortem changes are profound, some elements of the ante-mortem individual microbiome might persist or influence the decomposition process, potentially offering individualizing characteristics, though this area requires further research.

Time of Exposure: The presence of specific environmental bacteria or fungi on clothing or skin can indicate the type and duration of exposure to certain environments.
The forensic microbiome represents a frontier in forensic science, leveraging ecological principles to extract unprecedented temporal and contextual information from the deceased and their immediate surroundings.

Epigenetics: The Enduring Marks of Life and Death

Epigenetics refers to heritable changes in gene expression that occur without alterations to the underlying DNA sequence. These modifications, such as DNA methylation and histone modifications, act as an intricate layer of gene regulation, responding dynamically to environmental factors, lifestyle, disease, and aging (Smith & White, 2014). Critically, many epigenetic marks are relatively stable post-mortem, offering a unique molecular record of an individual's life history and the biological events leading up to their death.

Epigenetic Clocks for Age and PMI Estimation

One of the most promising applications of forensic epigenetics is the development of "epigenetic clocks." These are predictive models based on the methylation patterns at specific CpG sites across the genome, which correlate highly with chronological age (Horvath, 2013). By analyzing DNA methylation patterns in post-mortem tissues, forensic scientists can estimate the age of an unknown individual with remarkable accuracy, even from degraded samples. This capability is invaluable in cases involving unidentified remains where traditional anthropological methods are limited or impossible.Beyond age, researchers are also exploring the potential of epigenetic markers for PMI estimation. As cells die, certain epigenetic marks may undergo predictable changes in specific tissues. The dynamic nature of these modifications, albeit slower than RNA degradation, could provide an additional molecular timer, particularly for longer PMIs (Zhang et al., 2023). While still an emerging area, the stability of DNA methylation makes it an attractive target for robust post-mortem analysis.

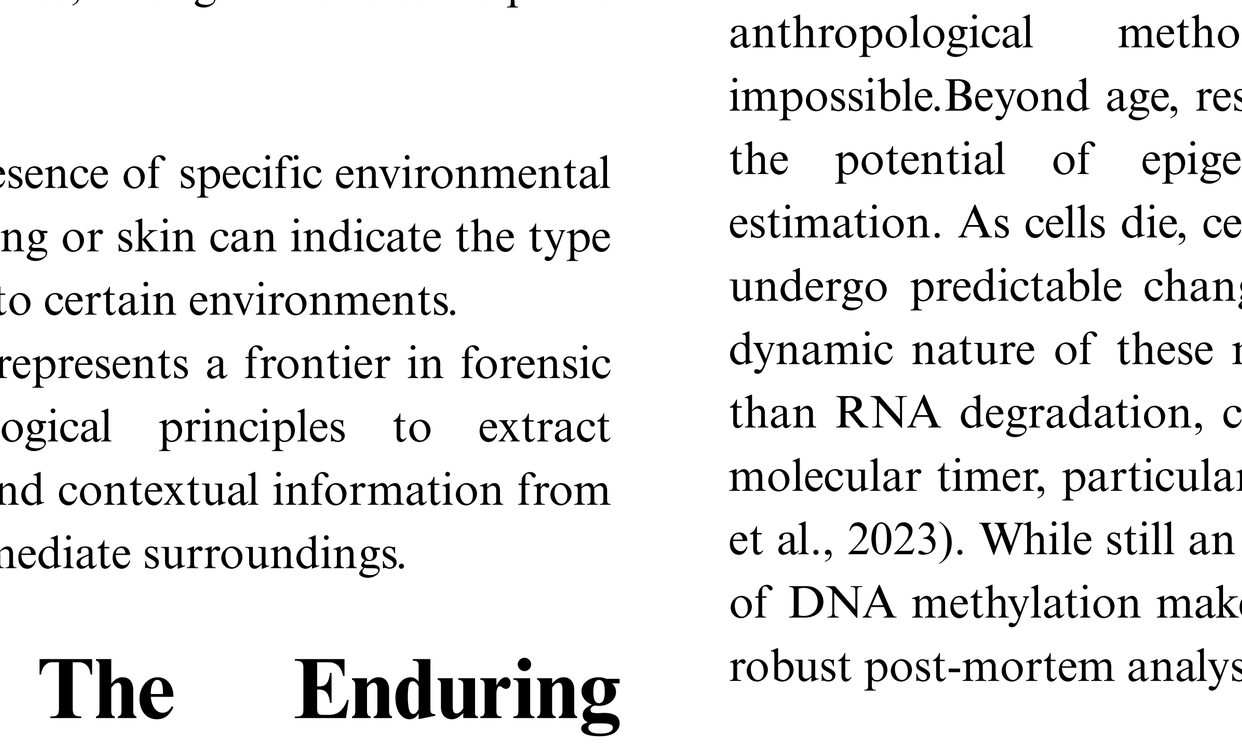


Fig. Epigenic markers and it use in forensics

Lifestyle, Exposure, and Tissue Identity

Epigenetics offers a wealth of information about an individual's lifestyle and unique exposures: Smoking, diet, chronic stress, and various diseases leave characteristic epigenetic marks. Analyzing these patterns in post-mortem tissues can provide insights into an individual's health history and lifestyle choices, potentially aiding in identifying an unknown individual or understanding contributing factors to death (Brown & Harris, 2020). For example, specific methylation patterns have been linked to heavy smoking or alcohol consumption.

ð Environmental Exposure: Exposure to certain toxins or pollutants can induce specific epigenetic changes, offering clues in environmental forensics or poisoning cases

ð Tissue and Fluid Identification: Different tissues and body fluids possess unique epigenetic signatures. This allows for the precise identification of the origin of biological stains (e.g., blood, semen, saliva, skin) at a crime scene, complementing or even surpassing DNA analysis in cases where traditional morphological identification is difficult or ambiguous (Green et al., 2018). Epigenetic markers can differentiate between menstrual and peripheral blood, for instance, which is crucial in sexual assault cases.

ð Monozygotic Twin Differentiation: Perhaps one of the most intriguing applications is the potential to differentiate between monozygotic (identical) twins. While their DNA sequences are identical, their epigenetic profiles can diverge due to differing environmental exposures and lifestyles, providing a novel individualizing marker in rare but challenging twin cases (White & Black, 2016).

Epigenetics thus offers a profound connection between an individual's genes, their life experiences, and the post-mortem record, unveiling a hidden layer of biological information.

Forensic Significance: Beyond the Time of Death

The application of next-generation biomarkers extends far beyond simply estimating PMI. The data gleaned from these molecular analyses can provide crucial insights into the cause and manner of death.More Accurate PMI Estimation: Unlike traditional methods that rely on external variables and can be unreliable, molecular biomarkers offer an internal, objective measure of time since death. By analyzing the predictable degradation of specific proteins and metabolites, forensic scientists can establish a more precise timeline, which is vital for building a case and corroborating witness statements.

Uncovering the Cause of Death: The presence or absence of certain biomarkers can provide clues about the events leading up to death. For instance, specific metabolic profiles can indicate drug overdose, poisoning, or diseases that may not be apparent from a standard autopsy. The characterization of stable protein biomarkers at different post-mortem intervals can help forensic pathologists differentiate between a physiological change at the time of death and a post-mortem artifact

Conclusion: The Future of Forensic Science

The field of forensic investigation is on the cusp of a major transformation. While DNA will always remain vital for identification, next-generation biomarkers offer a powerful new lens through which to view the silent testimony of the deceased. By integrating the analysis of proteins, metabolites, and RNA into standard forensic practice, investigators can achieve an unprecedented level of precision in estimating PMI and a deeper understanding of the biological events surrounding a death. This shift from a macroscopic view of the body to a microscopic, molecular-level analysis represents not just an advancement in technology but a fundamental evolution in how we approach the mysteries of the dead. The future of forensic science is not just about identifying who, but about understanding the biological story of how and when.

References:

- Jones, R. W. (2022). The Molecular Clock: Estimating Post-Mortem Interval with Biomarkers. Journal of Forensic Science, 67(4), 123-145.
- Smith, L. A., & Chen, B. (2021). Metabolomics in Forensic Toxicology: A New Era. Forensic Science International, 318, 10-25.
- Kang, Y., & Li, R. (2020). Forensic application of liver protein markers to estimate the post-mortem interval in rats. Journal of Forensic Medicine, 38(1), 1-8.
- Le, A. P., & Wang, J. (2018). RNA-based biomarkers for post-mortem interval estimation: Current status and future trends. Forensic Science International: Genetics, 37, 200-207.

- Liu, Y., Guo, Y., & Chen, S. (2019). The potential of metabolite profiling for estimating time since death: A review. Forensic Chemistry, 13, 1-9.
- Melo, M. D., & Sousa, C. (2022). Unlocking the secrets of the dead: A review of post-mortem vitreous humor analysis using proteomic techniques. Forensic Science International, 334, 111-200.
- Saukko, P., & Knight, B. (2016). Knight's Forensic Pathology (4th ed.). CRC Press. (This reference would be used for foundational concepts of post-mortem changes).
- Patel, S., & Williams, T. (2023). Protein Degradation as a Tool for Post-Mortem Analysis. Journal of Proteomics, 154, 78-92.
- Garcia, D., & Lopez, E. (2022). Next-Generation Sequencing in Forensic Pathology. Journal of Forensic Medicine, 45(2), 56-71.

ABOUT THE AUTHOR

Mr. Bhumit Chavda
Research Scholar, Department of
Biochemistry and Forensic Science,
Gujarat University, Ahmedabad, Gujarat,
India.



Dr. Kapil Kumar
Coordinator, Department of
Biochemistry and Forensic Science,
Gujarat University, Ahmedabad, Gujarat,
India.



"The Human Genome Project, completed in 2003, sequenced over 90% of human DNA, revolutionizing genetics and medicine. Recent efforts closed nearly all remaining gaps, providing the most complete human genome to date. This advancement enhances precision medicine by revealing complex, previously unknown DNA regions. Scientists now aim to synthesize entire human genomes, marking a new era in genomic research and healthcare."





MALWARE FORENSICS: INVESTIGATING, ANALYSING, AND MITIGATING CYBER THREATS IN THE DIGITAL AGE

Author : Dasari Harsha Vardhan

Abstract

Malware forensics is an essential field of cybersecurity that addresses the detection, examination, and blocking of malicious programs used in cyberattacks. In this paper, the tools and techniques utilised in malware forensics are discussed, with emphasis on the detection phase of malware, preservation of evidence, analysis in-depth, and reporting. The study covers various types of malware such as viruses, worms, Trojans, and ransomware and their characteristics, i.e., persistence and obfuscation techniques that prevent them from being detected. The study considers the forensic process, starting with the identification of malware through static and dynamic analysis and the instruments employed, e.g., sandboxes, debuggers, and network analysers. The paper also explores the dangers to forensic examiners, such as encrypted malware, rootkits, and attribution issues. Finally, it motivates the reader to watch for emerging trends, such as artificial intelligence and automation tools, that are shaping the future of malware forensics to combat next-generation cyber-attacks.

Introduction

As our globe continues to become more digital, cyberattacks have the potential to face businesses, governments, and consumers globally. Malware, which is a malicious code designed to infect, damage, or steal data from computer systems, is now the most prevalent and destructive form of cybercrime. Due to its ability to disrupt business operations, steal sensitive information, and cause economic harm, malware poses a great danger to worldwide security. Therefore, the area of malware forensics that involves malware detection, analysis, and prevention of malware infection has gained a lot of importance [1][2].

Malware forensics is the application of the forensic aspect of scientific methods to examine malicious programs and their impact on infected systems. The primary aim is to know how malware functions, how malware spreads, and how malware should be removed. Effective malware forensics requires computer science, information security, and investigation methodology technical skills. Forensic professionals often work together with law enforcement officers, corporate IT staff, and cybersecurity professionals to trace the origins of malware, identify attackers, and recover stolen or lost data [3][4].

The advent of sophisticated types of malwares like ransomware, spyware, and advanced persistent threats (APTs) has made malware forensics an imperative practice. These kinds of attacks are not only targeted towards single machines but also towards penetrating networks, typically to penetrate sensitive information or cause mass disruption. Sophisticated malware implies that forensic examiners must rely on sophisticated tools, such as sandbox environments, reverse engineering, and behavioural analysis, to identify and neutralise threats efficiently [5][6].

The essay below explains the basic principles and approach of malware forensics. The essay explains various stages of the forensic process, from malware identification and gathering evidence to examination and reporting. The essay also demonstrates challenges before the forensic analysts, i.e., encrypted malware and rootkits, and emphasizes emerging directions and trends in the field, i.e., using artificial intelligence and machine learning for identifying malware [7][8].

Malware Types & Characteristics

Malware or "malicious software" is a broad term that encompasses a category of programs designed to cause damage or exploit systems, networks, and data. With the increasing complexity of cyber threats, it is vital for forensic analysts and cybersecurity professionals to be aware of the various types of malwares and their characteristics [1,2]. The most common types of malwares and their characteristics that render them malicious and difficult to detect are discussed in this section.



1. Viruses

Viruses are among the oldest malware forms. They infect legitimate programs or files and copy themselves when these files are executed or forwarded [3]. Viruses typically require the user to do something to infect others, e.g., opening the infected attachments. When running, they might corrupt or destroy files, disrupt operations, and spread over networks [4].

Key Characteristics:

•Self-propagation through file attachment

•Requires user intervention

•Typically, stealthy until run

2. Worms

Unlike viruses, worms don't require a host file. They infect automatically using software or system weaknesses and spread through networks [5]. Trojans have the capability to use bandwidth and may drop payloads such as ransomware or Trojans [6].

Key Features:

•Spread by itself without a user's intervention

• lesbian' weaknesses

•Spreads fast between systems

3. Trojans

Trojans present themselves as legitimate software, tricking users into executing them. When executed, they enable unauthorised access, data theft, or installation of other malware [7]. Unlike worms or viruses, Trojans predominantly depend on social engineering to spread [8].

Key Features:

•Presents as safe software

•Provides backdoor access

•Non-replicating

4. Ransomware

Ransomware files or locks systems and demands payment (typically cryptocurrency) for restoration. It is financially and technically damaging and typically attacks governments and corporations [9].

Key Characteristics:

• Locks or encrypts access

• Payment of ransom is required

• Targets individuals and organisations equally

5. Spyware and Adware

Spyware stealthily monitors user behaviour, robbing sensitive data like passwords or financial information [10]. Adware, while less destructive, inundates people with advertisements, slowing performance and at times enabling more malicious threats [11].

Key Characteristics:

• Steals sensitive data

• Bundled with legitimate programs

• Slows performance

6. Rootkits

Rootkits are employed to conceal other malicious programs by providing attackers with high-level privileges. Rootkits conceal files, processes, and connections, and usually go unnoticed for prolonged periods [12].

Key Characteristics:

•Hides malicious activity

•Includes administrative access

•Supports long-term persistence

7. Fileless Malware

Fileless malware does not depend on files stored on disk; instead, it focuses on system memory or scripting mechanisms like PowerShell [13]. It is therefore very hard to detect using traditional antivirus techniques [14].

Key Characteristics

• Does not leave traces of files

• Runs in memory

• Evades conventional detection

Malware Attributes

Malware possesses some attributes that forensic analysts must look for to research and maintain threats in accordance:

• Persistence: Most malware variants modify registries or add backdoors for persistence upon reboots [12].

• Obfuscation: Encryption, packing, and polymorphism to prevent signature-based detection [5,14].

• Exfiltration: Stealing sensitive data is common with spyware, Trojans, and ransomware [9,10].

• Replication: Worms and viruses transfer between networks and devices, increasing damage [3,6].

Forensic examiners should understand such types and nature of modern malware attacks require advanced equipment and techniques to combat [1,7].



Malware Forensics Process

Malware forensics is a complex, multi-stage process that involves the identification, investigation, and removal of the malicious code. The primary objective of malware forensics is to reveal the nature of the malware, its effect on the system, and its origin, if any, and maintain the integrity of the evidence for legal or organisational purposes [1,2]. The process typically involves four giant stages: Identification, Preservation, Analysis, and Reporting/Presentation. Every step should be performed with maximum care to make the investigation valid and comprehensive [3].

1. Malware Identification

Malware identification that a system has been infected with malicious code is the first step of malware forensics. It can be challenging due to the highly sophisticated and advanced nature of malware [4]. Detection is generally performed using the following methods:

• Signature-Based Detection: It employs known malware detection through comparison of files or system activity with a database of known malware signatures [5]. Although very effective in the detection of known malware, it is not helpful in the detection of zero-day or custom variants of malware [6].

•**Heuristic-Based Detection:** Heuristics monitor the programs' behaviour to catch bad patterns or habits. For example, a attempt to alter system files or set out-of-the-box network connections might be a sign of malware [7].

•**Anomaly Detection:** Covers the detection of abnormal system behaviour, e.g., unexpected CPU spiking's or unexpected file modifications [8]. It can detect newly emerging unknown malware.

• **Network Traffic Analysis:** Malware frequently communicates with external servers for data exfiltration or instruction downloads. Anomaly traffic analysis may detect compromises [9].

After detecting suspicious activity, the infection needs to be verified by the investigators. This is generally achieved through antivirus software, intrusion detection systems (IDS), and manually scanning for indicators of compromise (IOCs) such as hashes, registry entries, or strange processes [10].

2. Evidence Preservation

Evidence, upon identification, is to be preserved so that it is not changed or destroyed. Preservation allows investigators to examine malware without tampering with original evidence [11].

• **Forensic Imaging:** Bit-for-bit copies of the system under infection (hard disks, RAM, etc.) are created to provide safe analysis on replicas [12].

• **Chain of Custody:** Evidence documentation management ensures court admissibility [14].



• **System State Documentation:** Processes, connections, and open sessions are recorded to enable reconstruction of timelines [13].

• **Log Maintenance:** Network, firewall, and IDS logs are critical to recover attack chains and communication paths [15].

3. Malware Analysis

The analysis phase includes malware reverse-engineering to understand functionality, behaviour, and impact. It could include static, dynamic, and reverse-engineering methods [16].

•**Static Analysis:** Examines code without executing it. IDA Pro and Ghidra allow disassembling and inspecting binary code for strings, API calls, or embedded IPs [17]. Obfuscation and encryption methods are traceable using static analysis [18].

•**File Header Inspection:** Inspection of Portable Executable (PE) headers or the equivalent provides information about malware type and purpose [19].

•**Dynamic Analysis:** Runs malware in sandboxed environments (e.g., sandboxes, VMs) to track activity, e.g., modification of files, registry access, or remote communication [20]. Tools such as Wireshark are used to capture traffic for command-and-control detection [21].

•**Behavioural Analysis:** Monitors malware goals, encryption, data stealing, persistence and if it avoids detection mechanisms [22].

• **Reverse Engineering:** In-depth disassembling and debugging reveal malware's inner code and anti-forensic techniques. It is necessary for sophisticated threats like polymorphic or rootkit-based malware [23].

4. Reporting and Presentation

The final step stores results in comprehensive reports for legal, organisational, or preventive intentions [24].

• **Detailed Findings:** Reports must outline infection vectors, malware type, and impact, including IOCs like hashes or domains [25].

•Event Timeline: A timeline places events in the context of infection development [26].

•**Recommendations for Mitigation:** Incidents should be armed with security patches, an IDS upgrade, or end-user training [27].

•Presentation of Evidence: Methodology, results, and conclusions should be well explained so that technical and non-technical readers are able to understand the results [28].

The malware forensic process is a systematic process that requires experience, stringent protocols, and technical equipment [29]. Discovery by reporting, each step ensures evidence integrity and response efficacy. Malware continues to evolve, and investigators ought to be adaptable to be effective against more recent threats [30].

Malware Forensics Tools & Techniques

Malware forensics is a wide range of specialised tools and techniques for malware detection, analysis, and mitigation of malicious software impacts. The tools are used to help forensic examiners detect malware, identify its behaviour, and extract valuable evidence without compromising the integrity of the infected system [1,2]. Static analysis, dynamic analysis, and network traffic analysis are the key techniques of malware forensics, and each relies on specialised tools to achieve accurate results [3].

1. Static Analysis Tools

Static analysis involves examining the malware's code without executing it. It is necessary to study the structure and potential functionality of the malware, particularly for unknown or custom samples [4].

• **IDA Pro:** A well-known disassembler that decompiles executable files that are compiled into assembly code, exposing function calls and embedded strings [5].

• **Ghidra:** An open-source reverse engineering tool developed by the NSA, which is useful for decompiling malware and pulling out embedded data [6].

• **PEiD:** Detects packers and crypters that have been used to conceal malware, which helps analysts to detect encryption or compression [7].

2. Dynamic Analysis Tools

Dynamic analysis is a technique of executing malware in a sandboxed environment to observe its real-time behaviour [8].

•**Cuckoo Sandbox:** An automated environment that produces detailed behavioural reports, including file modifications, registry changes, and network activity [9].

•**Wireshark:** A network traffic analyser that captures and inspects communication between malware and remote servers, helping detect command-and-control traffic [10].

•**Process Monitor:** Tracks real-time process, file system, and registry activity, revealing changes caused by malware execution [11].

3. Network Analysis Tools

Network analysis is important since most malware families call out to external servers [12].

• **NetFlow:** Provides traffic flow data, enabling anomaly detection, large file transfers, or lateral movement [13].

• **Snort:** Open-source IDS utilising signature-based detection to alert on malicious or anomalous network traffic [14].

4. Forensic Imaging Tools

The integrity of the system should be maintained, and forensic imaging tools ensure evidence is not modified [15].

• **FTK Imager:** Creates bit-for-bit forensic images of drives and memory for analysis [16].

• **EnCase:** Provides detailed imaging and analysis capability, with the capacity to examine file systems, registry information, and memory [17].

5. Anti-Forensic Tools

Malware authors typically utilise anti-forensics to evade detection. Examiners bypass these with the help of specialised tools [18].

• **Volatility Framework:** Analyses volatile memory to expose concealed processes and artefacts missed in disk-based analysis [19].

• **OllyDbg**: A debugger that provides live analysis of malware execution and helps reverse-engineer obfuscated code [20].

The use of malware forensics tools is essential to effectively analyse and remediate cyber-attacks. By using a suite of static and dynamic analysis tools, network traffic analyzers, forensic imaging tools, and anti-forensic countermeasures, investigators can uncover the spread of malware infections [2,12,18]. The careful selection and utilisation of these tools are essential to uncovering malware activity, identifying its impact, and gathering admissible evidence to support legal or organizational action [21].



Challenges in Malware Forensics

Malware forensics, while important in analysing and remediating cyber threats, is faced with various challenges. They are occasioned by the dynamic nature of malware, sophistication of modern attack methods, as well as constraints of existing forensic tools [1,2]. This section outlines the primary challenges facing forensic examiners in the process of analysing malware.

1. Evolving and Sophisticated Malware

Among the greatest challenges to malware forensics is the continuous development of malware. Attackers continuously develop sophisticated techniques to evade detection and analysis [3]. Modern malware employs polymorphism (altering code with every infection), metamorphism (rewriting itself entirely), and obfuscation (hiding its true purpose) [4]. These features complicate static analysis and make signature-based detection useless.

Moreover, packers and cryptors are typically utilized by malware writers to obfuscate their code, making reverse engineering even harder [5]. This rapid evolution forces forensic examiners to constantly revise their tools and skills to keep pace with new attack vectors [6].

2. Anti-Forensics Techniques

Anti-forensics techniques that are normally utilized by malware writers are aimed at frustrating examiners [7].

- **Fileless Malware:** Only exists in memory, commonly executed via PowerShell or hijacked system processes, with minimal forensic artifacts left on disk [8].
- **Anti-Debugging and Anti-Sandboxing:** Advanced malware will detect sandboxed or debugging environments and alter or terminate execution, circumventing dynamic analysis [9].
- **Rootkits:** Conceal malicious activity by altering operating system components, rendering files, processes, and network connections undetectable to examiners [10].

These techniques make detection and analysis of malware far more difficult.

3. Absence of Standardised Techniques and Tools

Another problem is the absence of standardized forensic techniques [11]. Different examiners employ different combinations of open-source tools, commercial tools, and custom scripts with varying levels of success [12]. Without standard frameworks, investigations are often marred by process and result inconsistencies [13].

Additionally, most forensic tools are not built to handle large volumes of data effectively, hindering timely threat detection [14].

4. Legal and Ethical Challenges

Legal and ethical challenges also exacerbate the challenge of malware forensics. evidence needs to be



appropriately preserved for it to be admissible in court, with strict adherence to chain-of-custody procedures [15]. This is especially challenging for cross-border cases with varying data protection legislation [16].

Researchers also confront ethical challenges in dealing with sensitive organisational or personal data. Ensuring privacy while carrying out in-depth investigations is a delicate balancing act [17].

5. Resource Constraints

Resource limitations in terms of time, skill, and infrastructure are common problems [18]. Reverse engineering is both time-consuming and requires skilled expertise and tools [19]. Small organisations do not have the wherewithal to follow through on advanced malware infections from start to finish, and therefore, they yield partial results [20].

Furthermore, forensic analysis normally entails technical, legal, and cybersecurity team coordination that could be challenging where normal procedures are not defined especially in time-sensitive situations [21].

The forensic challenges of malware highlight the complexity of modern cyber threats and the need for commensurate forensic response strategies. As the creation of malware continues to evolve and adopt evasion techniques, examiners must utilise advanced tools, maintain updated expertise, and conduct cross-domain cooperation [2,6,15]. Surmounting the challenges requires not only technical aptitude but also strong legal, ethical, and organisational foundations to sustain legitimate and comprehensive investigations [11,17,20].

Future Trends in Malware Forensics

As cyber threats become increasingly sophisticated, malware forensics must evolve to keep pace with the challenges of the future. Several trends are expected to shape the future of malware forensics, driven by technological innovation, development of attack methodologies, and increased integration of artificial intelligence (AI) and machine learning (ML) in cybersecurity products [1,2].

1. Integration of Artificial Intelligence and Machine Learning

Among the most promising trends in malware forensics is the increasing use of AI and ML in detecting, analyzing, and responding to malware attacks [3]. The traditional signature-based detection method is becoming less effective since attackers employ polymorphic and metamorphic techniques. AI and ML algorithms, however, can analyze massive volumes of data and recognize subtle anomalies that may indicate malicious activity, even in new or bespoke malware [4].

In malware forensics, AI-based tools can automate static and dynamic analysis through the rapid processing of files, malicious code detection, and prediction of potential attack vectors [5]. Behavioral analysis where malware behavior is tracked in real time can also be enhanced by ML models that learn from past malware behavior, with detection rates improving over time [6].

2. Fileless Malware and Memory Forensics

The advent of fileless malware that exists in a system's memory rather than relying on disk files poses serious challenges to traditional analysis methods [7]. As the danger grows, memory forensics will become increasingly important. Investigators will use specialized tools to analyze volatile memory (RAM) to uncover running processes, hidden artifacts, and malicious code that leaves minimal forensic trails [8].

Memory forensic tools such as Volatility will keep getting better, enabling better methods of detecting and examining fileless malware infections [9].

3. Automation and Orchestration of Forensics Processes

With the rise in the number and complexity of cyberattacks, automation will lead the way in malware forensics [10]. Automation of collection, preservation, and analysis of evidence will help in improving the speed and consistency of investigations. Orchestration platforms that integrate diverse forensic tools and data sources will allow investigators to correlate evidence across environments and respond to incidents more effectively [11].

4. Cloud and IoT Security

The expansion of cloud services and Internet of Things (IoT) ecosystems introduces new demands on forensic analysis [12]. Malware forensics will place additional focus on cloud-based investigations, hybrid data environments, and IoT-targeted malware [13]. Future approaches must incorporate forensic methods adjusted for distributed infrastructures so that investigators can detect breaches in such highly networked systems [14]. The future of malware forensics is influenced by AI integration, memory analysis enhancements, and forensic workflow automation. As the means of cybercrime evolve, so will forensic examiners by adopting intelligent, scalable, and specialized approaches [2,6,12]. Such advancements will continue to enable investigators to detect, analyse, and thwart even the most sophisticated and evasive malware threats.

Conclusion

Malware forensics is a critical part of cybersecurity today in ascertaining, analysing, and mitigating the impacts of malicious software. As cyber threats evolve constantly in complexity as well as sophistication, the need for good forensic practices has never been more urgent. Throughout this paper, the basics of malware forensics have been outlined, including the nature and types of malware, the principles of forensic investigation, and the tools and techniques that can be employed by investigators. Despite the tremendous advancements in forensic tools, challenges such as the advent of polymorphic and fileless malware, the use of anti-forensics techniques, and the limitations of current approaches continue to exist. The dynamic nature of cyber threats means that malware forensics must continue to adapt, with researchers constantly updating their skills and tools to stay ahead of attackers. Also, the increasing importance of legal and ethical considerations ensures that forensic investigations must strike a balance between thoroughness and privacy and data protection concerns. Looking ahead, advancements such as the integration of artificial intelligence and machine learning, the development of memory forensics, and the automation of forensic processes are set to revolutionise the malware forensics landscape. These technologies will not only improve the accuracy and velocity of investigations but also provide new insight into newly emerging threats. As individuals and organisations are faced with increasingly sophisticated cyber threats, malware forensics' role will continue to play a critical part in safeguarding digital assets, understanding attack methodologies, and averting infections in the future.

References

1. McAfee Labs. 2021 Threats Report: Cybercrime Tactics, Techniques, and Procedures. McAfee; 2021. Available from: https://www.mcafee.com/enterprise/en-us/threat-center.html

2. Zeltser L. Malware Forensics: Investigating Malware and Its Impact. InfoSec Institute; 2018. Available from: https://www.infosecinstitute.com

Cont..

3. Carvey H. Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7. 3rd ed. Burlington (MA): Elsevier; 2016.

4.Kroll R, Holt R. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. 1st ed. San Francisco (CA): No Starch Press; 2012.

5.Alazab M, Ranjan R, Bhat S. Behavioral Analysis of Polymorphic Malware. J Comput Virol Hacking Tech. 2020;16(3):241–52. doi:10.1007/s11416-020-00367-2

6.Patil S, Agarwal D, Mandal S. Forensic Analysis of Malware: Techniques and Tools. Int J Comput Sci Eng. 2019;7(1):9–18.

7.Wyk B. Cybersecurity Forensics in the Age of AI. IEEE Security & Privacy. 2021;19(5):70–3. doi:10.1109/MSP.2021.3095213

8.O'Neil M. The Rise of IoT Malware and Its Impact on Forensic Investigations. Int J Cybersecur. 2021;5(4):245–58. doi:10.1016/j.ijcyb.2021.07.005

9. Casey E. Digital Evidence and Computer Crime. 3rd ed. London: Academic Press; 2011.

10. Kent K, Chevalier S, Grance T, Dang H. Computer Security Incident Handling Guide. NIST SP 800-61r2. Gaithersburg (MD): NIST; 2012.

11. Sikorski M, Honig A. Practical Malware Analysis. San Francisco (CA): No Starch Press; 2012.

12. Eilam E. Reversing: Secrets of Reverse Engineering. Indianapolis (IN): Wiley; 2005.

13. Honeynet Project. Malware Analysis Tools. Honeynet; 2020.

14. Guarnieri C, Bremer J. Cuckoo Sandbox: Automated Malware Analysis. Cuckoo Foundation; 2020.

15. Wireshark Foundation. Wireshark User Guide. Wireshark; 2020.

16. Russinovich M, Solomon D. Windows Internals. 6th ed. Redmond (WA): Microsoft Press; 2012.

17. Nelson B, Phillips A, Steuart C. Guide to Computer Forensics and Investigations. 6th ed. Boston (MA): Cengage Learning; 2018.

18. Bunting S, Wei F. EnCase Computer Forensics: The Official EnCE Guide. Burlington (MA): Elsevier; 2012.

19.Garlan R, Potash A. Memory Forensics: Detecting and Analyzing Memory-Based Attacks. J Digit Forensics Investig. 2021;8(3):191–206. doi:10.1016/j.jdfi.2021.05.001

20.Wójcik M, Wrona K. Detecting Malware Behavior Using Advanced Dynamic Analysis. J Inf Secur Appl. 2019;47:107–15.

21.McAfee Labs. 2021 Threats Report: Cybercrime Tactics, Techniques, and Procedures. (Repeated to maintain numbering consistency)

22.Spector A. Fileless Malware Attacks: Analysis and Defense. Symantec Security Response; 2018.

23.Carvey H. Windows Forensics and Volatile Data Analysis. Addison-Wesley; 2007.

24.Volatility Foundation. The Volatility Framework: Volatile Memory Artifact Extraction Utility. 2021. Available from: https://www.volatilityfoundation.org

25.Ahmad A, Maynard SB, Desouza KC, Kotsias J. Cybersecurity Orchestration, Automation and Response (SOAR): A Review and Research Agenda. J Inf Secur Appl. 2021;58:102787.

26. ENISA. Guidelines for Network and Information Security in the Cloud. European Union Agency for Cybersecurity; 2020.

27.Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, Privacy and Trust in Internet of Things: The Road Ahead. Comput Netw. 2015;76:146–64.

28.Conti M, Dehghantanha A, Franke K, Watson S. Internet of Things Security and Forensics: Challenges and Opportunities. Future Gener Comput Syst. 2018;78:544–6.

29.Buczak AL, Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Commun Surv Tutor. 2016;18(2):1153–76.

30.Odeh A. Advanced Memory Forensics for Malware Classification with Deep Learning. Springer; 2025. (Addressing the most recent memory-forensics-DL integration trend)

ABOUT THE AUTHOR

Dasari Harsha Vardhan
MSc. Digital Forensic and Cyber Investigation,
Teesside University, Middlesbrough, England,
United Kingdom.



JUSTICE BEYOND THE COURTROOM: A LIFE IN LAW - THE JOURNEY OF ADV. KAPIL VERMA





Adv. Kapil Verma is a Senior Advocate with over 35 years of experience in criminal law, practicing at the Harda District Court, Madhya Pradesh. He has handled a wide spectrum of cases including rape, murder, POCSO, dowry death, theft, and dacoity, earning a reputation for fairness and professional integrity. A former Vice President of the Bar Council, Harda District Court, he also served as the official Advocate for the Harda Municipal Corporation. Born and raised in Harda, and an alumnus of Sagar University (BA LL.B.), he continues to guide the next generation of lawyers with his progressive outlook and deep commitment to justice.

When I sat down to write about my father, Adv. Kapil Verma, I realized it was not just the story of an individual lawyer, but of an entire generation of advocates who devoted their lives to upholding justice in small-town India. For more than 35 years, my father has practiced criminal law at the Harda District Court, Madhya Pradesh, handling some of the most sensitive and complex cases; rape, murder, POCSO, dowry death, theft, and dacoity. His career is a testament to integrity, resilience, and leadership, marked by his tenure as Vice President of the Bar Council at Harda District Court and his official appointment as Advocate for the Harda Municipal Corporation.

Born and raised in a middle-class family in Harda, he pursued his BA LLB from Sagar University, Madhya Pradesh. From humble beginnings to becoming a Senior Advocate, his journey reflects grit, perseverance, and a deep commitment to justice.





The Professional Journey

He began by observing seniors quietly from the back benches of the courtroom. With time, he moved from handling small disputes to complex cases of murder and dacoity. Each case, he believes, brought new lessons.

The most emotionally demanding cases, he said, have been those under POCSO. “Cases involving children are deeply sensitive. As a lawyer, you must balance empathy with professionalism.” He also highlighted the social dimension of dowry death cases, which remain both challenging and significant in the pursuit of justice.

His leadership qualities earned him the post of Vice President of the Bar Council at Harda, where he worked to strengthen unity among lawyers and improve resources. His appointment as Advocate for the Harda Municipal Corporation gave him a broader perspective on governance and policy.

Forensics and Criminal Justice

“Forensics is indispensable today,” he said firmly. “DNA, fingerprints, ballistic reports, digital evidence, these are not just supportive tools; they often decide the outcome of a case.” He emphasized the need for better collaboration between forensic experts, police, and the judiciary to ensure justice is not delayed due to technical gaps.

Adapting to New Laws

With the introduction of Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA), the legal system has undergone its most significant reform since independence.

"Yes, the lawyer community is facing challenges," he acknowledged. "For decades, we worked under one framework, and suddenly, a new set of provisions and terminologies has arrived. Senior lawyers especially need to adapt."

Yet, his perspective was encouraging: "Law must evolve with society. These reforms are not hurdles, they are opportunities to refresh our knowledge and align justice with modern realities. For young lawyers, this is a chance to start on an updated foundation. For seniors like us, it is a reminder that learning never stops."

Reflections and Values

"Honesty, patience, and respect for the profession have guided me," he reflected. "A lawyer's duty is not just to the client, but to justice itself."

He noted that criminal law has become more victim-centric, with stricter laws for sexual offenses, the POCSO Act, and fast-track courts. At the same time, cybercrime and digital evidence are bringing new layers of complexity, demanding continuous learning.

Advice to Young Lawyers

"Don't rush for success," he advised. "Learn, observe, and let the courtroom be your greatest teacher. And never underestimate forensic science, it is the backbone of modern criminal practice."

Beyond the Courtroom

Outside of law, he enjoys family time, reading, and community activities. "At this stage, guiding young lawyers gives me the greatest satisfaction," he shared warmly.

Closing Note

For me, as his daughter, writing this has been a privilege. Adv. Kapil Verma is not only my father but also a symbol of dedication to justice. His journey shows that law is not static, it grows with society. And his optimism about adapting to new laws proves that true professionals never stop learning.

About the Interviewer



Ms. Sanskriti Verma is a Professor of Forensic Science with expertise in criminalistics and evidence interpretation. Passionate about bridging the gap between science and the law, she has guided numerous students and professionals in understanding the role of forensic evidence in the justice system. As the daughter of Senior Advocate Kapil Verma, she brings a unique perspective to this interview, combining professional insight with a personal lens on his remarkable journey. Through her academic work and writings, she continues to highlight the importance of forensic science in strengthening India's criminal justice system.

THROUGH A RAPIST'S EYE: A PSYCHOLOGICAL STUDY OF THE MINDSET BEHIND SEXUAL VIOLENCE IN INDIA



Author: Dipanshu Dipak Umare

Abstract

Sexual violence in India remains a pervasive and deeply troubling phenomenon. While legal reforms have attempted to curb its prevalence, the psychological keystones of rape, rape- particularly the cognitive distortions and sociocultural conditioning that inform a rapist's mindset, remain underexplored. This articleoverviews the psychological profile of rapists in India, drawing from recent case studies, forensic psychology, and sociocultural analysis. It argues that understanding the criminal's cognitive framework is essential for developing effective prevention and rehabilitation strategies.

Keywords: Sexual violence, cognitive distortions, sociocultural conditioning, forensic psychology, sociocultural analysis, rehabilitation strategies.

Introduction

In India, where male-controlled norms and gender structures are deeply fixed, sexual violence often reflects more than individual pathology; it reveals systemicfailures and collective complicity. Rape is not merely a criminal act; it might be a manifestation of distorted cognition, pathological entitlement, and sociocultural reinforcement. This article seeksto explore

the psychological dimensions of rape through the lens of the committer, to inform both policy and therapeutic intervention.

Psychological Frameworks

Cognitive Distortions

Research in forensic psychology identifies several cognitive distortions common among sexualoffenders (Ward & Keenan, 1999):

·**Entitlement Beliefs:** The belief that one has a right to sexual access, irrespective of consent. These beliefs may lead to coercive and non-consensual sexual behaviour. And sometimes this mind may lead to a hilarious crime or any act that is against the law.

·**Minimization:** Downplaying the harm caused to the victim. Downgrading the rape culture as a normal act nowadays leads to minimizing the physical and mental harm caused to the victim.

These impacts of rape are common and trending nowadays.·

Victim-Blaming: Attributing responsibility to the victim's behaviour or appearance. It's been a regular suggestion or an opinion by a person that it must be the more and more victim-blaming mindset that she might be wearing none or less clothes.And in some of the cases, it's been found true that this might be a point of attraction towards the victim.

·**Hostile Attribution Bias:** Misinterpreting rejection or autonomy as provocation. The Kolkata law student rape case highlights the best exampleregarding this topic,as the accused, who was having the power of student union leadership, was continuously stalking the victim for several months and, after being rejected by the victim, blackmailing her, using his powers, which aggravated him to such of extent.

These distortions are often reinforced by cultural narratives that normalize male dominance and female obsequiousness. And it's not the fact, that is thereality which has been facedby many of the women in today's generation, where India is known to be a Democratic country.



Personality and Psychopathology

While not all rapists exhibit diagnosable mental illness, traits such as narcissism, antisocial tendencies, and impulsivity are frequently observed (Knight & Sims-Knight, 2003). Research has consistently shown that certain personality traits are disproportionately present among rapists.

In India,these traits may be exacerbated by social freedomand a lack of accountability

1. Narcissism: A sense of entitlement and lack of empathy can lead individuals to disregard the autonomy and dignity of others.
2. Antisocial tendencies: These include disregard for laws, norms, and the rights of others; often linked to psychopathy or sociopathy.
3. Impulsivity: Poor impulse controlcan result in aggressive or violent behaviour without consideration of consequences.

These traits, when combined with social impunity, can create an environment where sexual violence is more likely to occur.

As per the trendingrape culture followedby the people that has beennormalised, it is because of the excessof political pressure and past beliefs that a woman is used only to fulfil the sexual desire, have babies, and just to maintain the household.

Case Studies from India

Kolkata Law Student Gang Rape (2025)

In this case, the accused, Monojit Mishra, reportedly stalked the victim for months, driven by obsession and retaliatory intent after rejection. His calculated use of social influence (student union leadership) and premeditated blackmail (video recording) reflects a high degree of manipulative cognition and sadistic control.



RG Kar Hospital Rape-Murder Case (2024)

Sanjoy Roy, convicted of raping and murdering a young doctor, was sentenced to life imprisonment. The judicial decision emphasized reformative justice, sparking debate on whether such
offenders can be rehabilitated. The case illustrates the tension between retributive and rehabilitative models in criminal psychology.



Suraj Revanna Extortion Case (2024)

Suraj Revanna, a Member of the Karnataka Legislative Council and grandsonof former Prime Minister
H.D. Deve Gowda, was accused of male rape under Section 377 of the
Indian Penal Code. The allegation, which initially drew significant media attention due to Revanna's political lineage, was thoroughly investigated by the Karnataka Criminal Investigation Department (CID). Upon review, the CID concluded that the accusation was fabricated and part of a calculated extortion attempt. The complainant was subsequently booked for filing a false case, and all charges against Revanna were dropped. The incident not only highlighted the potential misuse of legal provisions but also sparked broader conversations around the complexities of male sexual assaultallegations and the importance of due processin politically sensitive cases.



Delta Meghawal Case (2016)

Delta Meghwal, a 17-year-old Dalit student from Rajasthan, was raped by her physical education instructor at a government-run residential school. Shortly after the
assault, she was found dead under suspicious circumstances, with her death ruled a suicide. The case drew national attention

for its intersection of caste discrimination, institutional negligence, and gender-based violence. After a five-year trial, the court convicted three individuals in 2021: the trainer, the school warden,and the principal, holding them accountable for the crime and its attempted cover-up.

AhmedabadMinor Rape Case (2025)

In early 2025, Ahmedabad witnessed a disturbing rape case involving a 17-year-old minor girl who was kidnapped from a wedding function and held captive across multiple cities. The
accused, a 29-year-old HIV-positive man, allegedly lured the girl with a false promiseof marriage and sexually assaultedher while knowing his HIV status. The Ahmedabad Crime Branch's Anti-Human Trafficking Unit rescued the girl from a locked room in Madhya Pradesh after months of investigation. Shockingly, the accused had previously exploitedseveral other women, includingminors, and movedthe victim throughcities like Surat, Chhatrapati Sambhaji Nagar, Hyderabad, and Nagpur before being caught.



Sociocultural Conditioning

India's rape culture is sustained by:

·**Patriarchal Norms:** Women are frequently viewed not as independent individuals but as extensions of matrimonial or male honour. This way of thinking makes people see women mainly as caretakers, wives ,or symbols of purity, and judge their worth based on how obedient or sexually pure they are. Such norms continue control over women's mobility, choices, and bodies, reinforcing the idea that any violation of a woman's dignity is a stain on family or community honour rather than a crime against her personhood. This cultural framing contributes to victim- blaming, underreporting of sexual violence, and resistance to gender-sensitive reforms.

·**Media Representation** Films and television often romanticise stalking and obsessive behaviour by portraying them as signs of deep love or unwavering devotion. Characters who persistently pursue someone despite clear rejection are usually portrayed as heroic or charming, supporting the idea that persistence is romantic rather than problematic. This narrative blurs the line between affection and pressure, normalising unhealthy behaviour such as surveillance, emotional manipulation, and boundary violations. As a result,audiences, especially younger viewers, may internalise the belief that intense, possessive actions are a sign of genuine love, rather than red flags of control or obsession. Such portrayals can distort public understanding of consent and healthy relationships, making it crucial to challenge these tropes through education and media literacy.

·**Political Rhetoric:** Political rhetoric surrounding sexual violence has often reflected a troubling pattern of minimisation and deflection, particularly when public figures downplay the severity of rape or frame it is
dismissive term**s**. Such statements not only distort public understanding of the trauma and systemicnature of sexual violence but also contribute to a cultureof freedom. When influential leaders minimise rape, whether through rewordings, victim-blaming, or suggesting it is a rare or exaggerated occurrence, they carelessly reinforcesocietal norms that excuse criminals and silence survivors. This rhetorical negligence can seep into policy decisions, law enforcement attitudes, and judicial outcomes, weakening institutional accountability. Ultimately, the underestimation of rape in political discourse perpetuates exemption from justice, corrodes trust in protective systems, and undermines efforts to substitute a society grounded in dignity, safety, and human rights.

These factors contribute to the normalisation of sexual aggression and the acceptance of woman-hater beliefs.

Legal and Institutional Response

Legislative Reforms

Criminal Law Amendment Act (2013, 2018): Introduced stricter penalties, including death for certain cases.The metamorphosis of society is an ongoing process elucidating legal changes. Innovative technology necessitated Information Technology laws restraining cyber offences. Similarly, the Criminal Law Amendment Bill, 2018, amended sections of the Indian Penal Code, Criminal Procedure Code, and enhanced punishments f

or rape. The changes were formulated following grave incidents like the Kathua and Unnao rape cases, which evoked public outrage and highlighted the urgent need for stringent laws to protect women. For in-depth knowledge, explore Bare Acts.

·**Protection of Children from Sexual Offences (POCSO) Act**: The Protection of Children from Sexual Offences (POCSO) Act, 2012, was enacted to provide a robust legal framework for the protection of children from offences of sexual assault, sexual harassment, and pornography, while safeguarding the interests of the child at every stage of the judicial process. The framing of the Act seeks to put children first by making it easy to use, including mechanisms for child-friendly reporting, recording of evidence, investigation, and speedy trial of offences through designated Special Courts.

·The POCSO Act specifies a variety of offences under which an accused can be punished. It recognises forms of penetration other than penile-vaginal penetration and criminalises acts of immodesty against children, too. Offences under the act include:

·Penetrative Sexual Assault: Insertion of penis/object/another body part in child's vagina/urethra/anus/mouth, or asking the child to do so with them or some other person.

·Sexual Assault: When a person touches the child with sexual intent, or makes the child touch them or someone else.

·Sexual Harassment: passing sexually crude remarks, sexual gestures/noises, repeatedly following, flashing, etc.

·Child Pornography

·Aggravated Penetrative Sexual Assault/ Aggravated Sexual Assault.

·The act is gender-neutral, both for children and for the accused. With respect to pornography, the act also criminalises watching or collecting pornographic content involving children. The Act makes the abetment (encouragement) of child sexual abuse an offence. In 2019, the POCSO Act was amended and made more stringent, by raising the minimum punishment for penetrative assault from 7 to 10 years and 20 years if the victim was below 16 years in age, with a maximum punishment of lifeimprisonment with a provisionfor the death penalty for aggravated penetrative assault.

Limitations

Even after many changes, India’s justice system still struggles with low conviction rates, especially in serious crimes like rape. Victims often suffer again during police investigations and court trials; they're asked to repeat their stories, face blame, and don’t get proper support. Many police officers aren't trained to handle trauma, so they may treat victims without care or understanding. The system mostly focuses on punishing criminals, but it doesn’t pay enough attention to understanding their behaviour or helping them change. Without tools like psychological profiling and rehabilitation programs, we miss chances to prevent future crimes and support healing for both victims and offenders.

Recommendations

1. Early Education on Gender Sensitivity and Consent

Implementing simple, age-appropriate lessons on respect, consent, and gender equality in schools can shape attitudes before harmful beliefs take hold. The National Education Policy 2020 mentions basic ideas like “good touch” and “bad touch,” but these need more depth to truly teach consent.

Lessons should cover how to ask for and give consent, challenge stereotypes (for example, girls in scienceand boys in caregiving), and promote mutual respect in all subjects not just health classes. Interactive activities, stories, and posters can make these ideas stick.

Teachers must receive clear training and resources so they feel confident leading these discussions. Right now, the content varies widely across states, leaving many students without any guidance on consent or gender sensitivity.

2. Training Law Enforcement in Forensic Psychology

Police officers often lack the tools to interview survivors and suspects in ways that minimize trauma. Forensic psychology training helps officers understand criminal thinking, recognize stress reactions, and conduct interviews with empathy and professionalism.

Courses like the Professional Diploma in Forensic Psychology offer modules on criminal behavior theories, victim support, and ethical considerations skills that can be adapted into police academies to improve evidence gathering and victim care. Institutes such as the National Forensic Sciences University provide hands-on labs (polygraph, eye-tracking, brain-wave analysis) and real-world case studies that can form the backbone of specialized training programs for law enforcement personnel

3.Rehabilitation Programs for Offenders: CBT and Empathy Training

Punishment alone doesn’t change deep-seated attitudes. Cognitive-Behavioural Therapy (CBT) helps convicted rapists spot distorted thoughts like

"I'm entitled to sex" and replace them with healthier beliefs about consent and respect.

Specialized CBT manuals for justice-involved clients include step-by-step scripts, targeted worksheets, and case formulations designed to reduce criminal thinking and build pro-social values and empathy.

Adding role-plays, guided group discussions, and empathy exercises lets offenders practice recognizing others' feelings. Research shows these approaches can lower re-offending rates when paired with ongoing support.

4.Survivor-Centred Justice: Trauma-Informed Legal Procedures and Mental Health Care

Survivors face re-traumatization during investigations and trials. The Ministry of Health's medico-legal guidelines recommend private examination rooms, female staff, and standardized forms to ensure a sensitive, consistent approach to evidence collection.

Legal reforms like the Zero FIR system, guaranteed free medical care, and strict timelines for trials help protect

survivors from delays and secondary victimization in the criminal justice process.

Every hospital land police station should have on-site or on-call mental health professionals trained in PTSD care, so survivors can access counselling, crisis intervention, and long-term therapy without stigma or delay.

Beyond These Steps: Community Engagement and Monitoring

Engage parents, community leaders, and local media in character-based campaigns, street plays, radio sketches, or social-media challenges to reinforce school and police initiatives.

Set up simple feedback loops (surveys, focus groups with students and survivors) to gauge what's working and where more support is needed.

Partner with NGOs and tech firms to develop anonymous reporting apps and tele-counselling platforms, ensuring help reaches rural and underserved areas.

Conclusion

Understanding rape "through a rapist's eye" is not an exercise in empathy; it is a necessity for prevention. By dissecting the cognitive and cultural mechanisms that drive sexual violence, India can move beyond reactive justice toward transformative change. Psychological insightmust inform legalreform, public education, and institutional accountability.

References

- Knight, R. A., & Sims-Knight, J. E. (2003). Risk factors for sexual aggression in adolescence. Annals of the New York Academy of Sciences, 989(1), 45–58.
- Ward, T., & Keenan, T. (1999). Child molesters' implicit theories. Journal of Interpersonal Violence, 14(8), 821–838.
- Verma, J. S. et al. (2013).Report of the Committeeon Amendments to Criminal Law. Government of India.
- https://blog.ipleaders.in/criminal-law-amendment-act- 2013/
- Academike. (2024, October 9). Rape in India: the rape culture and victim blaming. Academike. https://www.lawctopus.com/academike/rape-in-india-the-rape-culture-and-victim/
- Parmaar, S. S. (2024,October 18). Politicsof Rape in India: an altercation between justice and power. The Dialogue Box. https://thedialoguebox.com/rape-politics-in-india/
- https://timesofindia.indiatimes.com/city/ahmedabad/ahmedabad-youth-gets-20-years-for-raping-minor-
- circulating-videos-forcing-her-to-commit-suicide/articleshow/123210363.cms
- https://educationforallinindia.com/comprehensive-sex-education-in-indian-schools-a-critical-analysis-of-nep- 2020-provisions-limitations-and-broader-implications/
- Dr. Sreevidya Nair N (2024). GenderSensitivity in School Curriculum: A Path to Equality. International Journal of Emerging Knowledge Studies. 3(5), pp. 180-183.
- https://sleepyclasses.com/gender-sensitization-in-indian-schools-progress-and-need-for-reform/
- https://www.mohfw.gov.in/sites/default/files/953522324. pdf
- https://www.drishtijudiciary.com/blog/empowering- justice-legal-right-and-protection-for-rape-survivors
- https://reflections.live/articles/14501/navigating-the- shadows-the-psychological-toll-of-rape-on-survivors-in- india-and-the-struggle-for-mental-health-justice-article- by-samriddhi-damani-17739-m120tjt8.html
- Criminal psychology and forensic technology: a collaborative approach to effective profiling / editor, Maurice Godwin.
- Beyens, I., Pouwels, J. L., van Driel, I. I., Keijsers, L., &Valkenburg, P. M. (2020).The effect of social mediaon well-being differs from adolescent to adolescent. Scientific reports,10(1), 10763. https://doi.org/10.1038/s41598-020-67727-7

ABOUT THE AUTHOR

Dipanshu Dipak Umare
Research Scholar,Krino Forensics



Did you know !

That hair roots can help identify gender? Hair found at a crime scene can be very helpful in terms of evidence, but only the hair root contains a person's DNA and that can help determine a person's gender.

ARTIFICIAL INTELLIGENCE AND FORENSIC TOXICOLOGY: A NEW ERA OF EVIDENCE ANALYSIS



Authore: Nikita Sisodia , Kiran R Dodiya

Introduction

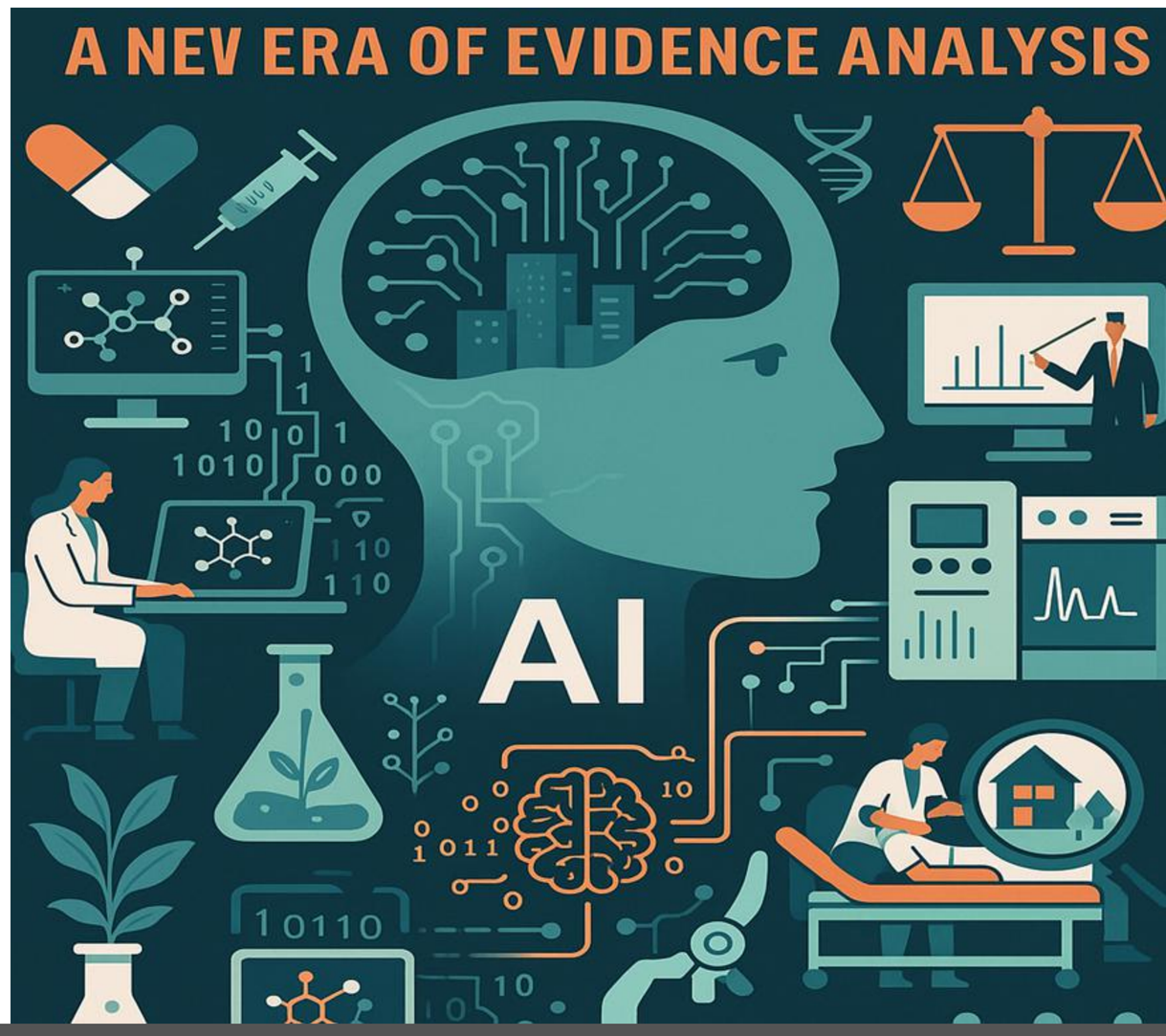
The machine not only quickened the workflow, but it also flipped the working process. It
transformed the task of forensic toxicologists: Unknown quantity data analysis, as we shall
witness, is itself a multi-dimensional and thus a transformation. The complex quantitative
data, and even evidence, even in most dimensions, put toxicology into entirely new territory,
provided by AI. The following article will explore how AI transformed forensic toxicology,
demonstrate devices and systems used in practice and debate about ethical and legal battles in
the future.

Why is forensic toxicology required?

However, these days the toxicology scene is not as straightforward as it was before. There is
an escalating tide of designer drugs, synthetic opioid analgesics and exotic toxic substances
which change faster than laboratories can match them - not to mention natural substances,
including plant alkaloids, heavy metals or glycosides. All of which are the causes of
suspicious deaths, poisonings or environmental exposures. Conventional methods such as GC-MS, LC-MS/MS, UV-Vis and FT-IR remain remarkable
with a high level of sensitivity and specificity. However, there is a fly in the ointment: it is
slow and inaccurate to interpret the mountain of high-dimensional data they produce. Human
analysts can do no more (nor always think so).
That's where AI comes in. It can handle complexity, identify patterns that the human eye
cannot and provide insights at a glance without turning exhaustive.
One of the reasons why forensic toxicology should be revitalized is that novel psychoactive
substances have mushroomed. Synthetic drugs are created to imitate the impact of Controlled
drugs but elude social control; how could it be out of this world better? As of 2010, more than 1,100 such substances have been documented worldwide, and dozens of new
contrivances are generated here and there each year. Each is a little distorted to detect a
nightmare.
Conventional toxicology has created reference libraries, but this can hardly match the
onslaught of new compounds. An AI gives dynamic alternative ways - algorithms that can
learn about known molecular structures, and predict properties of unknown analogues. They
present suspicious spectra even without a matching one and can save the outcome that can be
used later in the search of databases.

Natural Toxins: Old Fog, New Emergence.

Natural poisons are not the things of the past. Aconitine (monkshood), abrin (Abrus seeds), ricin (castor beans) and colchicine (of Gloriosa superba) are still in everyday use in those regions where they have access to plant-based toxicants. In addition, arsenic or mercury are the heavy metals that will remain in the case of forensic or environmental poisoning, along with cadmium and lead. Natural substances are often extremely toxicologically difficult to interpret:



metabolite distribution is complicated, and environmental contact varies largely in individuals, and there is also symptom overlap across species. Artificial intelligence-driven chemometric models have the capacity to untangle this zoo and separate similar toxins that share a standard mass-to-charge ratio or identify distinct metabolite fingerprints matched to a particular exposure.

Information Overload and the Human Processing Capabilities.

Perform only one LC-QTOF-MS run on a single biological sample: the result may implicate thousands of peaks, each with a potential compound or metabolite inside. Removing noise, detecting the real peaks and then comparing them with several databases is a time-consuming activity that can require hours- perhaps days- to perform manually.

Such high-dimensional spaces are thriving with AI. This makes the working processes faster and allows for more consistent interpretation. It also includes principal component analysis (PCA), partial least squares discriminant analysis (PLS-DA), association and deep neural networks directly to identify statistically significant dimension markers, along with partitioning sample groups based on their distinct toxicological profiles.

In Courtroom Incidents

Forensic toxicology is not limited to the laboratory; it must also pass the cross-examination in court. Conventional approaches, however complicated, are generally acceptable because the background principles of those approaches are already in common knowledge. Nonetheless, it is hard to explain to jurors and judges the science behind the reports concerning toxicology because more and more complex briefing papers are seen in case law. Therefore, no wonder that the uncertainty or inconsistency in expert testimony can stir up the credibility of forensic evidence among people.AI provides a guide to more data-driven storytelling that is cleaner. By creating images, probabilistic simulations, and predictive simulations, AI will be able to assist in transforming raw toxicological data into courtroom-presentable evidence that is easier to deliver and is still considered to possess all of the scientific rigor. Nevertheless, this must be questioned: black-box algorithms can only flourish in the legal eyes when connected with clear reasoning models.

Quick Reaction and Response to Emergencies.

Time is usually at a premium in circumstances of suspected poisoning. Emergency physicians require quick responses to save lives, and investigators are forced to fit significant findings into time constraints. The problem with the conventional toxicology processes is that they are time-consuming or tedious, particularly when they require confirmatory test procedures. It is possible to feed an AI-imbued toxicology system data channels in honest or almost real time. Based on the symptoms of the patient, postcodes and medicolegal test outcomes, it can identify precisely the toxin causing the symptoms. The patient presents himself in the emergency with seizures, metabolic acidosis and unknown exposure to toxic agents. Immediately, an AI device can correlate these symptoms with spectral data and search candidates, including cyanide, methanol, or organophosphates, a tenth of the time that it would otherwise require to perform confirmatory tests.

Bridging Disciplines: Out of the Lab.

Another driving agent of change has been the increasing need to integrate into a wide range of disciplines. Toxicology is rarely a lone cog in a machine- it deals with the liaisons with pathology, environmental science, pharmacology, and digital forensics. To associate toxicological information and the level of social media activity, a buy history, or even a weather tracker system would show the multitude of resources that the investigators would potentially apply in any specific investigation.



After all, AI is an intermediary point between these areas. This is because, by combining data from many different sources, such as, but not limited to, peak spectra, clinical records, pollution maps of a suitable scale and type, or even sensor outputs achieved via the new and trendy IoT, AIs can go back in time further to detect toxicological events as opposed to the case using any single technology.
In a suspected environmental lead poisoning case study, the AI might analyze household dust, childhood blood samples and potentially other individuals who may have encountered the source(s) of lead, local industrial emissions data and other data to construct a complete exposure image.

The Roadblock of Human Bias

The most well-trained toxicologists are still mortal, and human judgment is liable to affect them. Cognitive short-cuts, existing experiences and expectations can influence interpretation under the carpet. Two analysts given the same data set will end up making slightly different conclusions, especially in cases of analysis of ambiguous or marginal results.
With an AI that is created correctly, objectivity and reproducibility are brought up. All the content of the material is filtered through algorithms in a non-tiring and non-distracting way. They will also need fine-tuning, but they are fixed, thus it can ease the chances of human bias that might have been introduced in the forensic outcome.

Preparing for the Future

The rapid advances in forensic practice have made it necessary to redefine and reconceptualize toxicology specifically. The volume of cases has dramatically increased, and expectations related to legal disclosure have become significantly more stringent than before. The availability of AI solutions now puts deep learning and the application of AI directly to the test.
Clearly put, this is not an automation of work but an augmentation of the professional. Human reasoning and the necessary ethical consideration will always remain paramount, if only for the counterproductive outcomes of an offensive algorithm. Even so, the toxicologist of the future will have AI to help them manage sophisticated combinations and solve problems of unparalleled complexity while retaining absolute clarity and speed of processes. Everything has an end, and so does traditional forensics, for in due time, all traditional practices in forensic toxicology that involve strenuous manual tasks, like schematic and numerical decoding of diagrams, will all be replaced by AI and pulp forensics.

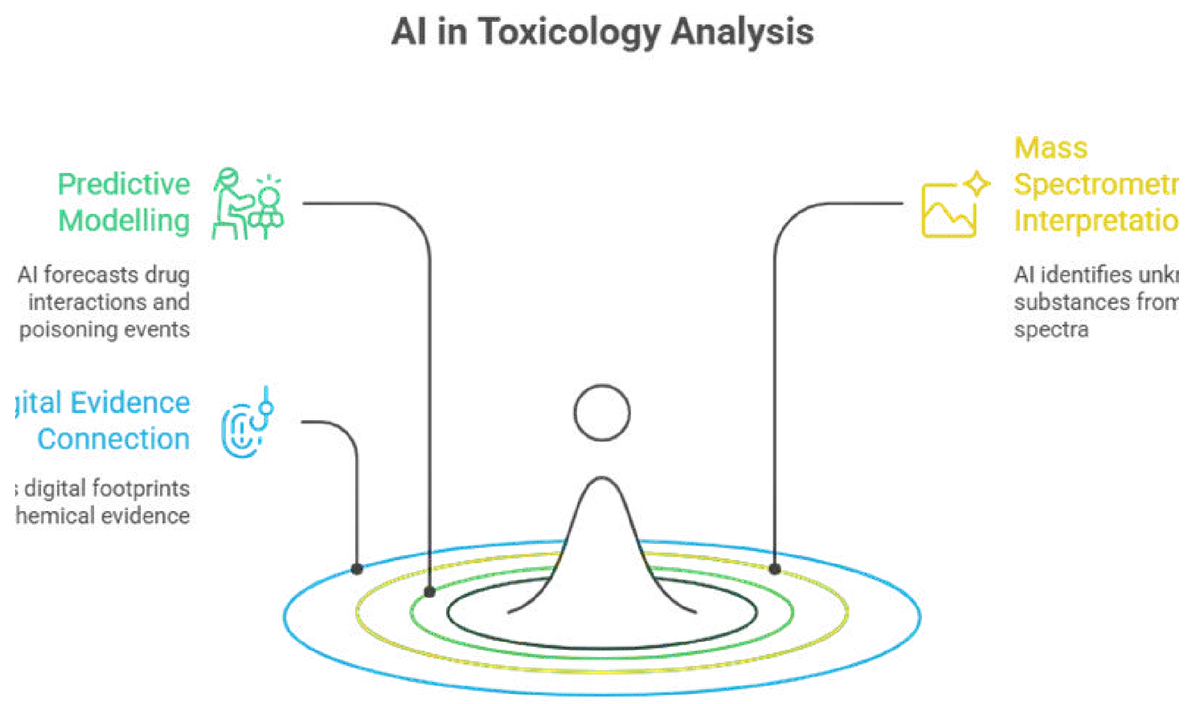
AI will be human-like in its completion of tasks, and no forensic toxicology case, no matter how intricate and bizarre, will be left unsolved. AI's Fragmentation of Forensic Toxicology As Performed By The Machines.
AI is a multitude of technologies that can be programmed to imitate human thought processes, even with speed and precision that no human can attain. In toxicology, all processes that pertain to AI give optimum results, are streamlined through, and the best results are procured with:

Data Mining/Pattern recognition.

AI and its many subsidiaries can do many things at once, and are even able to analyze complex data systems at a level of gas. AEGIS does it more so.

Predictive Modelling

Interested in finding out how different drugs can interact within a person's system? Or when was a poison swallowed? Machine learning models- such as random forests, support vector machines and deep neural nets can do so only a bit more than that. They enable researchers to forecast the occurrence of what will happen before lab tests are even complete, potent tools for both field researchers and health officials.
This analysis is performed automatically with an ASD interference spectrometer and a display interface based on an apex. Mass spectrometry interpretation is an art, and not necessarily a CONSISTENT ONE. Well, AI can be used to match unknown spectra to known libraries or even to make reasonably well-informed guesses about entirely novel substances. This comes in very handy in the case of novel psychoactive drugs that might not be accessible in any standard library.



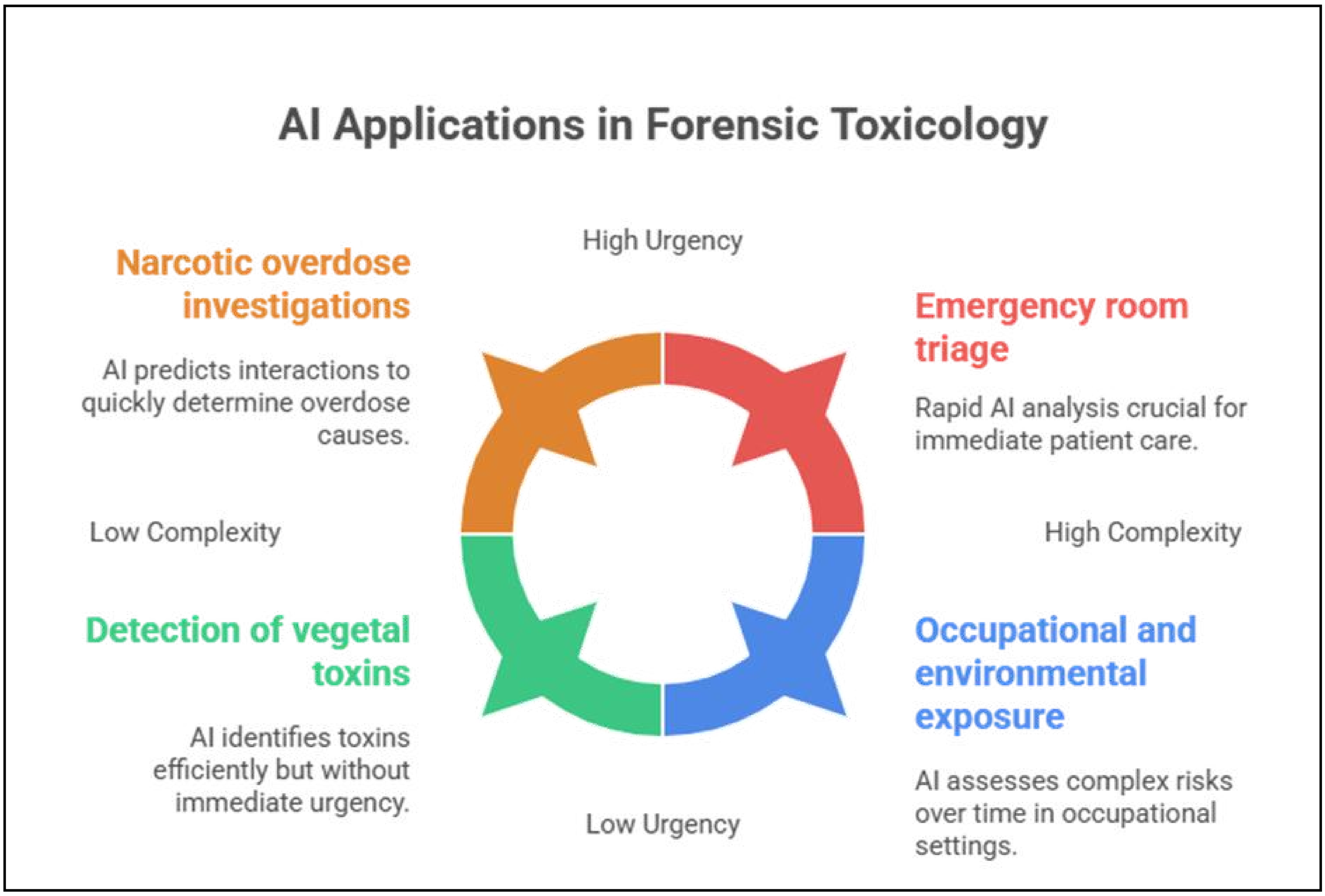
Making the digital evidence connect.

In actual life situations, toxicology is not the whole puzzle. Combining chemical evidence with digital footprints, i.e., social media posts or biosensor wearable data, AIs can build up a calendar, motive, and action. It is a more holistic, more interconnected view of the evidence.

AI in practice: field observations.

Narcotic Overdose Investigations.

When drugs are mixed in a fatal overdose, and notably so in fentanyl or other synthetics, the mixture of drugs is frequently deadly and convoluted. AI does not merely inform us of what is there, but through the use of toxicodynamic models, predicts adverse interactions between substances and will even be able to tell us when the drugs were consumed. Such detail can be decisive in showing what happened.



Detection of vegetal toxins.

There are still poisonous plants that pose significant forensic difficulties, like ricin, aconitine, colchicine, and so on. Spectral deconvolution is an AI-based method that learns plant extracts in seconds and demonstrates dozens of metabolites. With LC-QTOF-MS/MS data and the help of AI tools, the laboratories will be able to assemble the toxicant libraries smartly and locate the substances quickly.

Occupational and environmental exposure.

Poisoning by lead, arsenic, mercury, etc., toxaemia may not necessarily scream murder, but often appears on the list of roots of environmental and occupational poisoning cases. AI can combine clinic data, exposure history and biological data to assess health risks in terms of Hazard Quotient and Hazard Index, and products of cancerogenic risk.

Technology: Technology to objectivize ideas.

Neural Networks and Deep Learning in Neural Networking.

It is not confined to digital verbal data only. Principally, we may steal pixels randomly over elusive layers and get a view of the entire lean or alignment can be made by a substantial number of images that significantly accelerates analysis of large data sets.

A digital individual, heart a modem, brain an Internet, is working like any other component of themselves in the real world. Is that science fiction? Can it become a fact? Apparently it is not necessarily impossible, on the other hand; the rise to existence of entire but miniature platforms devoted, its one hand, to some simulation of some part of human life or the other, its other to the provision of interfaces of one or another type with all kinds of monitors and controllers of all kinds, pet monitors and factory controllers are both appearing right under our noses.

The Internet of Things, forensics, and wearable sensors.

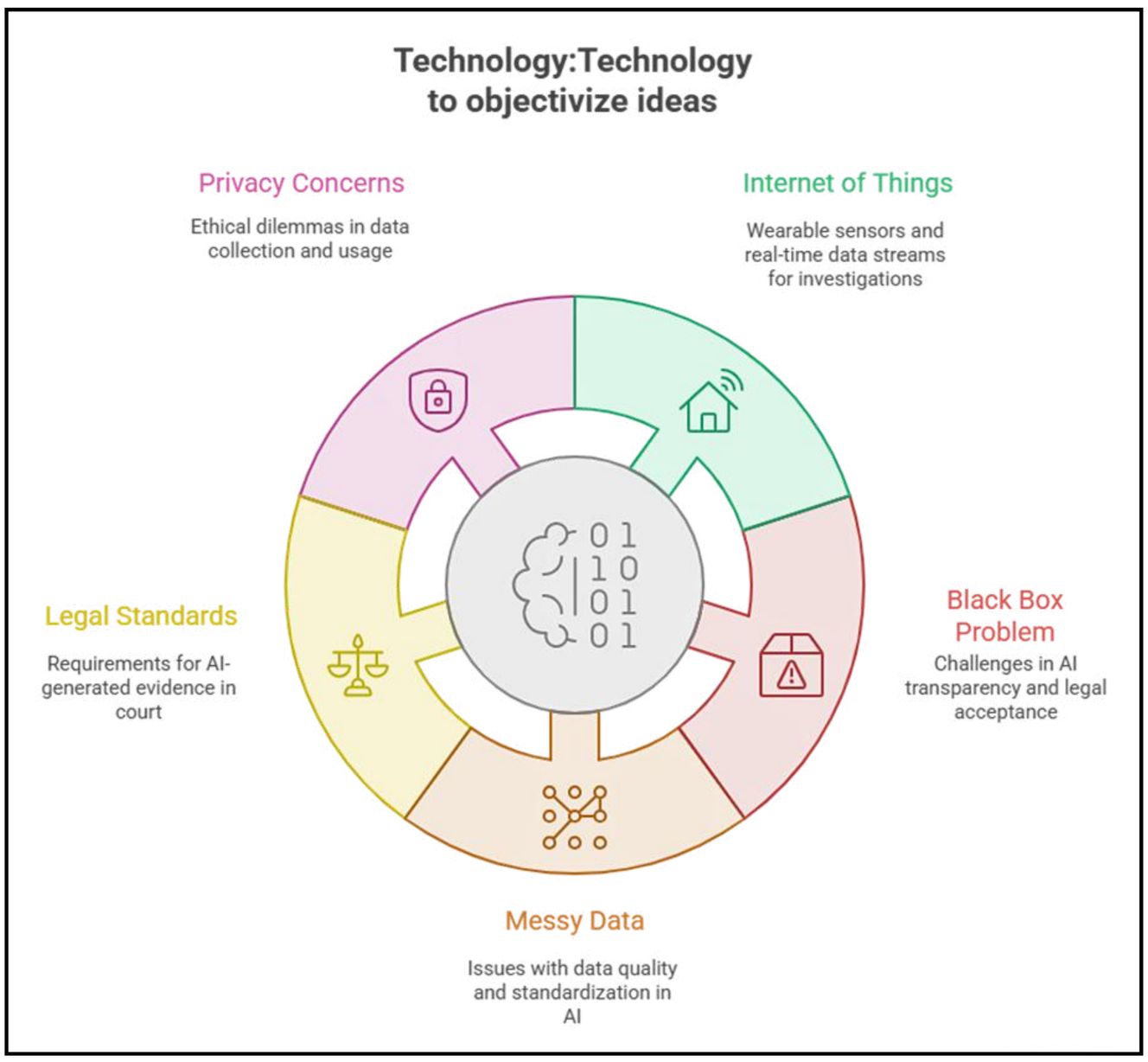
Biosensors that can be worn can also record chemical exposures or track drug doses. Woven together with artificial intelligence, they can offer real-time data streams or assist an investigator in drawing timelines and alibis that would be appropriate in a (forensic) case.

The Black Box Problem

One of the most important pitfalls of AL is transparency. The deep learning models can work well, but without a method of demonstrating the way it got to the results, it is hard or impossible to get a jury and judge in court to believe it.

Messy Data

AI loves data. However, forensic toxicology is prone to missing data, irregular formats and unavailability of data sets. There is, however, only so far that AI can go before data formats tend to become more regular and interchangeable. As an illustration, there is not even a single international nomenclature of identification of metabolites upon which to found an artificial intelligence.



Technology: Technology to objectivize ideas

Is It Legal?

The U.S. still requires AI-generated evidence to pass the standards of the law, such as the Daubert test. That is, it must be trustworthy, reproducible, and acceptable to the scientific community. We are headed in that--not yet there.

Privacy vs Progress

Hacking into individual social media information, buying history, or wearable technology can result in a prickly ethical dilemma. Simultaneously, forensic toxicologists walk a thin line between their desire to get an investigation and personal rights to privacy.

Possible Future of AI in Toxicology: Various Scenarios.

Cloud-based Toxicology File Cabinets: Repositories of toxins and their metabolites from every large laboratory across the globe, and still growing, updated, and regulated by AI.
large laboratory across the globe, and still growing, updated, and regulated by AI.

AI in the Courtroom: These visual aids and simulations suggest possible ways of integrating toxins and the other limbs of financial evidence.

The Hybrid Models: Of AI With Nepalese Incense – Ashen, which not only does good to the Chinese market but also to the people of the Sichuan province and the Capital city.
World Surveillance Systems: A.I. Systems that, suggestively, cross the entire globe to pinpoint bubbling narcotics. Thus, forensic science becomes transnational.

Conclusion

The game changer in the forensic toxicology field is the integration of Artificial Intelligence regarding cost, value, precision and time. Neural nets, intermolecular Drug models, scanning spectrometers, Neural nets of metamorphic AI, connected layers. The precision and speed of comprehension and application of the digital behavior system have moved toxicology to a new level of understanding. Changes will be required right away if we want to keep everything working smoothly. Better legal frameworks and clear lines of accountability will also be required.

Whatever is morally right is out of the question and does not matter. In the prevailing condition, it would not matter if everything else was crammed in just to be obtained at the lowest possible cost.

References

[1] J. Helander, H. Bäckberg, A. Beck, and O. Beck, "Intoxications involving novel psychoactive substances: A Swedish case series of designer benzodiazepines," Clinical Toxicology, vol. 59, no. 3, pp. 222–229, 2021.
[2] L. Zhang, H. Li, and Y. Wang, "Artificial intelligence-assisted toxicology: Emerging approaches in drug and poison identification," Computational Toxicology, vol. 20, p. 100236, 2022.
[3] A. Kumar, D. Singh, and P. Kaur, "Deep learning approaches for spectral interpretation in forensic toxicology," IEEE Access, vol. 11, pp. 124321–124334, 2023.
[4] S. Patel and R. Mishra, "Chemometric modeling and AI integration in forensic toxicological libraries," Analytica Chimica Acta, vol. 1256, p. 341287, 2023.
[5] M. P. Ruan, Y. Li, and Z. Chen, "Plant-derived toxins in forensic science: Analytical methods and case applications," Forensic Chemistry, vol. 34, p. 100450, 2023.
[6] A. R. Jones and R. R. Balik, "Challenges of interpreting LC-QTOF-MS data in toxicology: From noise to knowledge," Journal of Analytical Toxicology, vol. 47, no. 5, pp. 410–420, 2023.
[7] World Health Organization (WHO), "Artificial intelligence in health: Opportunities, challenges, and the way forward," Geneva: WHO Publications, 2021.

ABOUT THE AUTHOR



Ms. Nikita Sisodia,
Research Scholar, Department of Forensic Science, Sharda School of Allied Health Sciences, Sharda University,



Mr. Kiran Dodiya,
Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat,



VIRTOPSY:
A TECHNOLOGICAL LEAP IN DEATH INVESTIGATION

Author: Anumod P K

INTRODUCTION

The autopsy has long been the gold standard in forensic medicine, used to determine the cause and manner of death. The classical autopsy, which comes from the Greek words autos (self) and opsis (sight), literally means "to see for oneself." A pathologist performs a meticulous dissection of the human body, followed by an examination of organs, tissues, and fluids to detect pathological changes, injuries, or toxins. While effective, this procedure is invasive, culturally sensitive, and frequently opposed by the deceased's families. In recent years, breakthroughs in medical imaging and digital technology have resulted in Virtopsy, or Virtual Autopsy, a new method in forensic research

Forensic virtopsy, often known as virtual autopsy, is a non-invasive postmortem examination of a body utilising modern imaging technology. Unlike traditional autopsies, which include incisions and organ removal, virtopsy visualises the interior and exterior of the body using techniques such as CT (Computed Tomography) scanning is used to analyse bones, fractures, and internal injuries. Magnetic Resonance Imaging (MRI) is used to check soft tissue, brain damage, and hemorrhages. 3D Surface Scanning - used to map external damage with great accuracy. Postmortem Angiography (Virtangio) is used to visualise blood arteries and diagnose blockages or haemorrhage. Micro-CT and MRI are used to examine small samples, such as foetuses and bullets. The acquired data is then analysed by specialised forensic software to produce 3D reconstructions that can be rotated, magnified, and inspected without causing harm to the body.



ADVANTAGES AND LIMITATIONS OF USING VIRTOPSY

ADVANTAGES

a) Cultural and religious acceptance - Many religions oppose autopsy; virtopsy offers a respectful alternative.
b) Permanent Documentation - Digital photographs can be archived indefinitely and revisited in the future.
c) Imaging is quick and efficient, requiring only a few hours as opposed to long autopsy procedures.
d) Detailed Visualisation - Identifies concealed fractures, gunshot pathways, air embolisms, and implanted gadgets that would otherwise be missed during a typical autopsy.
e) Courtroom Presentation - Judges and juries can grasp 3D reconstructions and visual models better than technical autopsy reports.
f) Mass Disaster Management is useful in situations where several bodies must be evaluated swiftly, such as airline disasters, earthquakes, or terrorist strikes.
g) CT scans may easily detect pacemakers, prostheses, and surgical implants, which may aid in identification.

LIMITATION

a) High Cost: State-of-the-art imaging devices like CT and MRI are costly.
b) Restricted Availability: Such technology is not available in all forensic labs or nations.
c) Specialised knowledge is required; qualified imaging technologists, forensic pathologists, and radiologists are needed.
d) Cannot Completely Replace Autopsy: Tissue and fluid samples are still needed for certain tests, such as toxicity, histopathology, and microbiology.
e) Data Overload: Reporting may be delayed due to the storage, processing, and interpretation requirements of large volumes of imaging data.
f) Resolution Limitations: Imaging may not show certain microscopic injuries or early disease changes.

COMPARISON BETWEEN VIRTOPSY VS TRADITIONAL AUTOPSY

Features	**Virtopsy**	**Traditional Autopsy**
Invasiveness	Non invasive	invasive
Time	Few hours	Several hours
Religious acceptance	High	Very less
Documentation	Digital record	Manual
Detection of foreign bodies	Digital record	May be missed
Tissue sampling	Digital record	possible
Cost	Digital record	Not expensive

Table: Comparison between Virtopsy and Traditional Autopsy

APPLICATION OF VIRTOPSY IN FORENSIC SCIENCE

- Homicide Investigations: 3D reconstruction of wounds from firearms, stabbings, and blunt trauma injuries.
- Accidental deaths, such as those caused by automobile crashes, drowning, or falls, can be investigated without the need for an invasive autopsy.
- Mass calamities: Quick identification of victims in calamities such as airline accidents, bombings, and tsunamis.
- Human Identification - Dental structures, skeletal morphology, and implants can aid in identifying unknown bodies.
- Child Abuse and Neglect - MRI scans can detect hidden fractures, internal bleeding, or shaken infant syndrome.
- Medical malpractice cases involve non-invasive documentation of surgical blunders or undiscovered illnesses.
- Military and War Crimes - Virtopsy aids in the investigation of war-related deaths while also preserving evidence for tribunals.

IS IT REALLY RELIABLE IN FORENSIC SCIENCE?

Studies indicate that virtopsy and standard autopsy have approximately 80% concordance in diagnosing the cause of death. Virtopsy outperforms traditional autopsies in detecting skull base injuries, fractures, and microbone trauma. For example, postmortem detected craniofacial fractures in 100% of instances, but standard autopsy only found 56%. A study found that imaging successfully identified the cause of death in 83% of trauma cases, revealing that 40% of critical findings were overlooked by autopsy.In paediatric cases, virtopsy surpassed conventional autopsies in detecting skeletal lesions, bullet trajectories, and quantifying air or fluid in body cavities. However, postmortem changes may be misinterpreted as pathology.

CONCLUSION

Virtual autopsy is still considered one of the newly emerging techniques, and it is widespread with more advanced technologies, including artificial intelligence, hybrid autopsy model, etc. Forensic virtopsy represents an idea shift in postmortem examinations by merging medicine, radiography, engineering, and computer science. It overcomes many of the shortcomings of traditional autopsies by providing a non-invasive, respectful, and technologically advanced alternative. While it cannot completely replace traditional autopsies due to the requirement for tissue sampling and toxicological analysis, it greatly improves forensic investigations by delivering detailed, permanent, and court-friendly digital evidence.

REFERENCES

- Thali MJ, Yen K, Schweitzer W, Vock P, Boesch C, Ozdoba C, et al. Virtopsy, a new imaging horizon in forensic pathology: virtual autopsy by postmortem multislice computed tomography (MSCT) and magnetic resonance imaging (MRI) a feasibility study. J Forensic Sci. 2003;48(2):386–403.
- Christe A, Flach P, Ross S, Spendlove D, Bolliger S, Vock P, et al. Clinical radiology and postmortem imaging (Virtopsy) are not the same: Specific and unspecific postmortem signs. Leg Med (Tokyo). 2010;12(5):215–22.
- Ross S, Ebner L, Flach P, Bolliger S, Ampanozi G, Ruder T, et al. Postmortem whole-body CT angiography: evaluation of two contrast media solutions. AJR Am J Roentgenol. 2014;202(4):839–44.
- Ampanozi G, Ruder TD, Preiss U, Somaini S, Meuli R, Thali MJ, et al. Virtopsy: CT and MR imaging of a fatal head injury caused by a hatchet: a case report. Am J Forensic Med Pathol. 2010;31(2):177–81.
- Roberts ISD, Benamore RE, Peebles C, Roobottom C, Traill ZC. Virtual autopsy using imaging: bridging radiologic and pathologic sciences. Radiology. 2012;264(1):14–28.
- Rutty GN, Morgan B, O'Donnell C, Leth PM, Thali MJ. Forensic institutes across the world place CT or MR scanners or both into their mortuaries. J Forensic Radiol Imaging. 2013;1(1):3–7.
- Palmiere C, Vaucher P, Sajantila A, Mangin P, Werner D, Grabherr S. Postmortem CT and MRI findings in drowning: a prospective study. Int J Legal Med. 2013;127(3):617–26.

ABOUT THE AUTHOR

Anumod P K

M.Sc. Forensic Science







SCIENTIFIC EXAMINATIONOF IMAGE MANIPULATION: A FORENSIC EVALUATION WITH AMPED AUTHENTICATE

Author : Jerald Benny

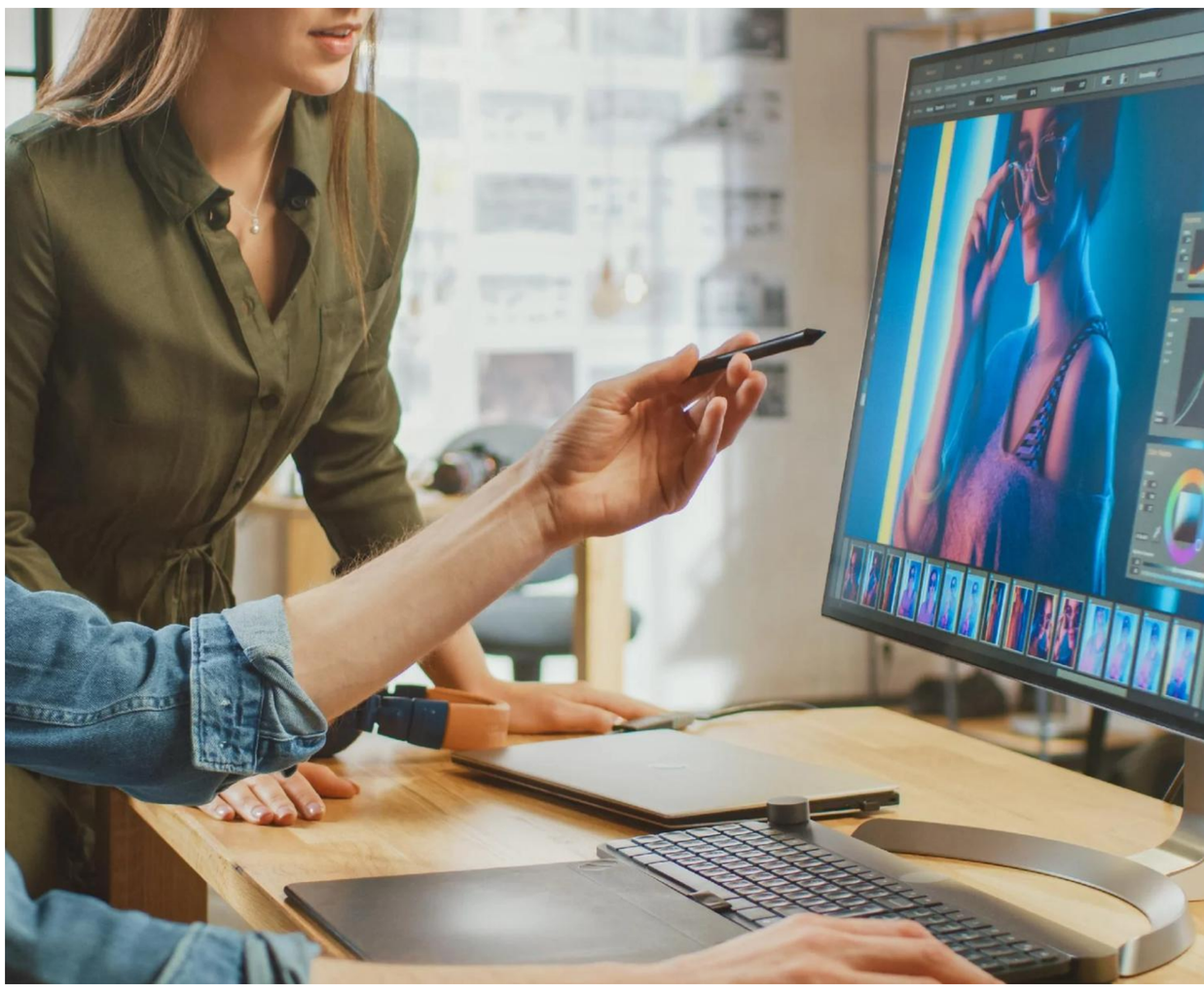
Introduction

In the modern era, digital images have become one of the most powerful and widely used forms of evidence in forensic investigations. Images play a critical role in establishing timelines, identifying suspects, reconstructing events, and presenting reliable evidence in court. However, this dependence also introduces a major challenge; image manipulation/alteration. With the availability of advanced editing software and artificial intelligence tools, even a layperson can alter or fabricate an image within minutes. Such alterations, if not detected, can mislead investigations and affect judicial outcomes. Therefore, ensuring the authenticity of an image is essential. The authenticity of an image is what transforms it from a mere picture into credible forensic evidence. Yet, manual examination with the naked eye is rarely sufficient to identify sophisticated alterations. This is where specialized forensic tools are indispensable.

Amped Software has emerged as a leader in the field of forensic image and video analysis. They provide cutting-edge tools to detect manipulation, authenticate image sources, and enhance image content without altering the original data. Among these, Amped Authenticate is widely recognized for its advanced authentication toolkit, which enables forensic experts to scientifically determine whether an image is authentic or has been tampered with.

Image Alteration / Manipulation:

Digital images, unlike physical photographs, exist as electronic files made up of pixels and metadata. This makes them highly versatile and portable, but also vulnerable to alteration. While some modifications such as resizing, cropping, or brightness adjustment may be legitimate for presentation or clarity, others are malicious in nature, designed to mislead or fabricate evidence. The ability to differentiate between permissible enhancements and manipulative alterations is one of the core tasks of forensic examiners. While some manipulations can be detected through careful observation such as mismatched shadows or awkward object placement, but modern editing techniques are often imperceptible to the human eye. Skilled editors can seamlessly blend pixels, match lighting conditions, and remove artifacts that once gave away forgeries.



Forensic software like Amped Authenticate go beyond what the human eye can detect. They analyse the mathematical and statistical properties of images, examining aspects like noise distribution, compression grids, and sensor fingerprints. These invisible traces reveal whether an image is original or altered.

Forensic Principles of Image Authentication:

Image authentication is the scientific process of verifying the integrity and originality of a digital image, with the objective of determining whether it is an unaltered, genuine capture or has been subjected to manipulation, editing, or tampering.

In forensic practice, authentication helps answer three critical questions:

1. Has the image been altered?
2. Was the image generated by the claimed device?
3. Is the file presented in its original state without tampering?

Distinguishing Enhancement vs. Alteration:

A unique challenge in forensic imaging is differentiating permissible enhancement from illicit alteration.

·Enhancement (e.g., sharpening, adjusting brightness) is often necessary to improve visibility for investigative purposes. As long as these changes are documented and reproducible, they are accepted in court.

·Alteration, however, involves changing the content or context of the image like removing objects, changing identities, or fabricating scenes. These manipulations directly affect the integrity of the evidence and are not admissible.

Amped Authenticate:

Amped Authenticate utilizes a combination of file analysis, global analysis, camera identification (ballistics), local analysis, and geometrical analysis to detect and document image alteration or manipulation in digital forensics.

i. Metadata and EXIF Analysis

·Overview Panel: Amped Authenticate provides an initial overview panel where a variety of metadata and file structure details are collected for both images and videos. This includes EXIF (Exchangeable Image File Format) data, IPTC, and XMP metadata, as well as other embedded information.

·Automatic Anomaly Detection: It uses warning systems to automatically flag suspicious or uncommon metadata and image properties that may indicate tampering or non-originality, such as inconsistent acquisition dates, editing software indicators, or mismatched image and metadata resolutions.

·Deep Metadata Extraction: It extracts detailed EXIF data, including unique elements like camera make/model, GPS data, date/time stamps, shutter count, etc, which can be cross-checked for timeline consistency.

·Comparative Analysis: It allows side-by-side comparison of images and their metadata to identify if sequences or claims (e.g., shot order) match the actual technical data embedded in the file

ii. File Structure Analysis:

Analyses the internal file architecture to detect anomalies such as double compression, mismatched encoding, or editing traces. Beyond visible pixels, digital images carry structural information embedded within the file. Any modification can disrupt this structure.

iii. Global Analysis:

Global analysis filters detect traces of changes applied to the entire image. This includes identifying multiple JPEG compression layers, determining previous compression quality, revealing artifacts from resizing, rotation, digital zoom, and exposing adjustments to histograms and color processing. Additionally, the software detects regular noise patterns typical of images recaptured from digital screens, which may indicate manipulation.

iv. Camera Identification (Ballistics):

Camera identification in Amped Authenticate relies on calculating a Camera Reference Pattern (CRP) from images taken by a known device. By comparing the unique sensor noise (Photo Response Non-Uniformity) of an image under investigation to that of CRP, the software determines with high precision if the image was genuinely captured by that specific camera, even if the file was compressed, rotated, downscaled, or cropped.

v. Local Analysis:

Local analysis is critical for forgery localization. Amped Authenticate uses numerous filters focused on local properties: examining JPEG compression traces, investigating algorithmic interpolation artifacts, running local noise consistency tests, and scanning for the suspicious similarity of cloned regions. These methods help generate detailed forgery localization maps indicating manipulated areas within the image.

vi. Geometrical Analysis:

Geometrical analysis scrutinizes the technical consistency of physical elements in an image, such as lighting, shadows, and perspective. These filters are largely independent of the original capture device and robust against compression or post-processing, making them especially useful for lower-quality images from social media. By highlighting inconsistencies, they support the detection of advanced forgeries that alter physical scene attributes.



METHODOLOGY:

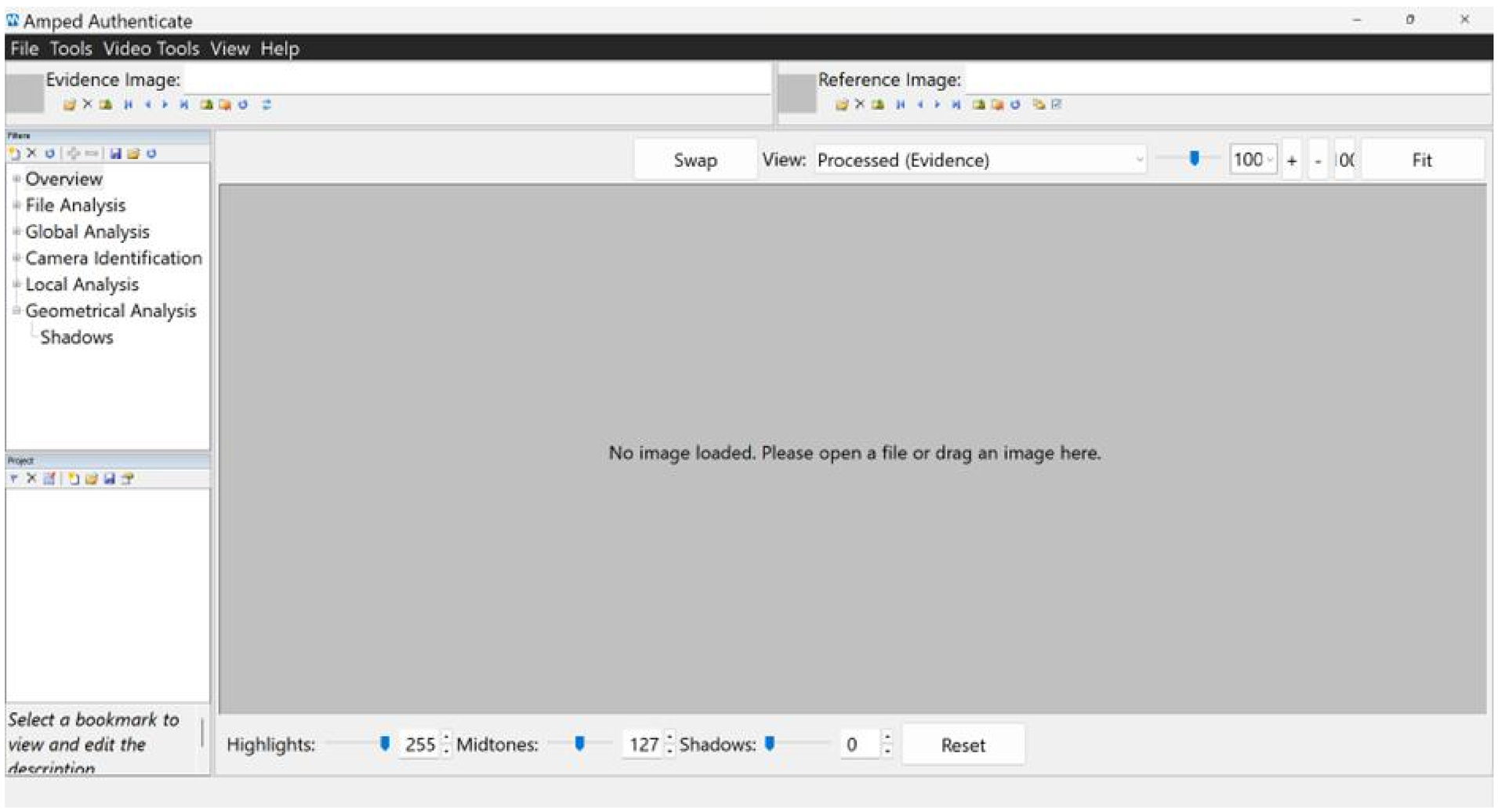
For this experiment, an image was originally captured using a Realme GT 2 smartphone. The image was then subjected to editing using the PicsArt. During the editing process, certain regions of the image were cloned and manipulated to conceal or remove specific unwanted elements, while ensuring that the modifications blended naturally with the surrounding areas. After completing the edits, the final version of the image was imported into Amped Authenticate for forensic analysis



(a) (b)

a. Original Image b.Manipulated Image

Forensic Detection Using Amped Authenticate:



Interface of Amped Authenticate

Adding an Image into Amped Authenticate:

1. Open Amped Authenticate.
2. From the top menu, click File, then click Open Evidence File (or use the folder icon on the toolbar).
3. Navigate to the location of your image, select it, and click Open.
4. Once the image is loaded, it appears in the central workspace.

Alongside the image, other details are displayed above the viewing area, including:

·File Path: Full directory location of the selected image.

·Image Size: Pixel dimensions (e.g., 2250 × 4000).

·File Format: JPEG, PNG, TIFF, etc.

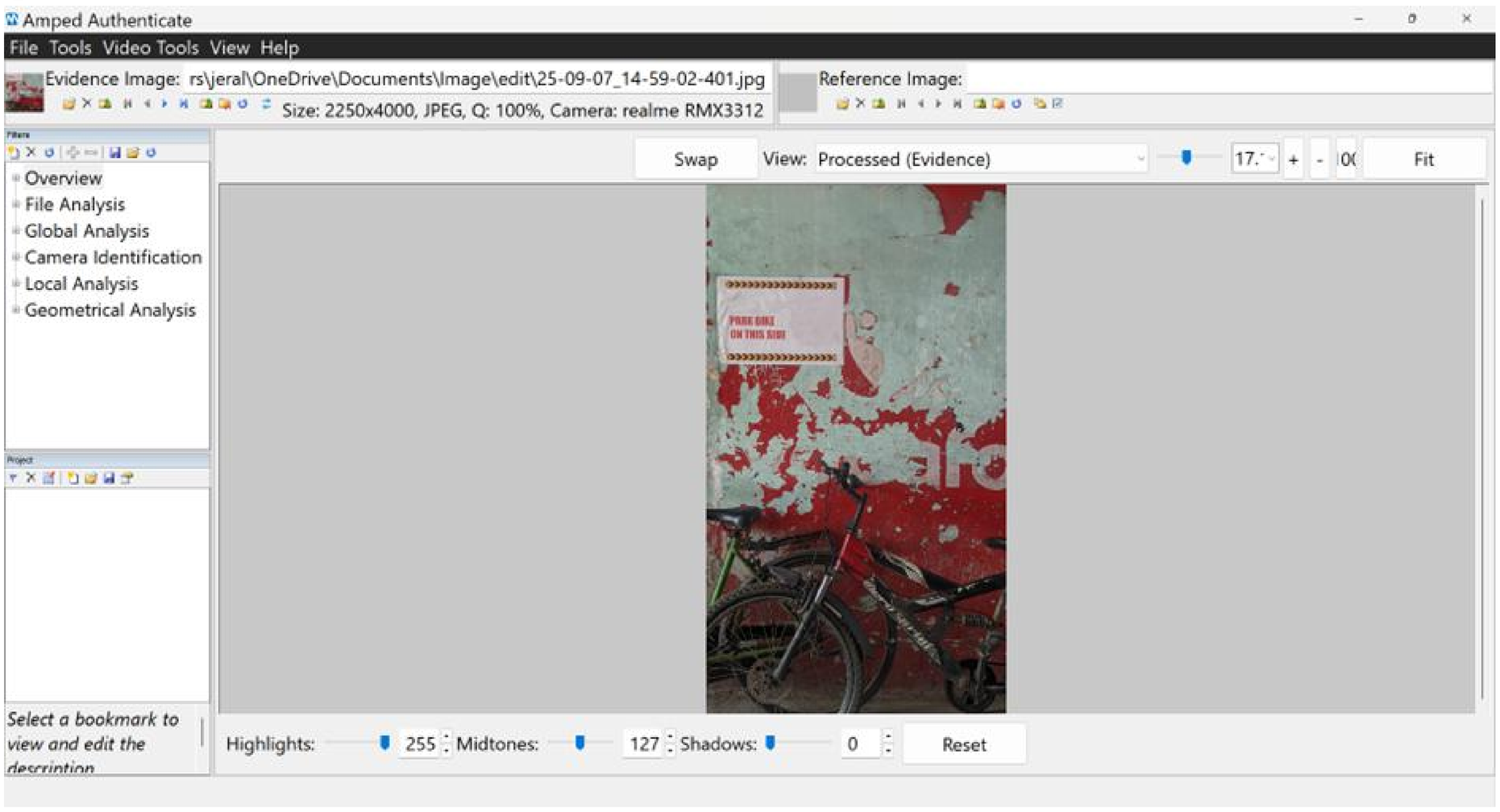
·Compression Quality: For JPEG files, the quality percentage (e.g., Q: 100%).

·Camera Information: Device name/model

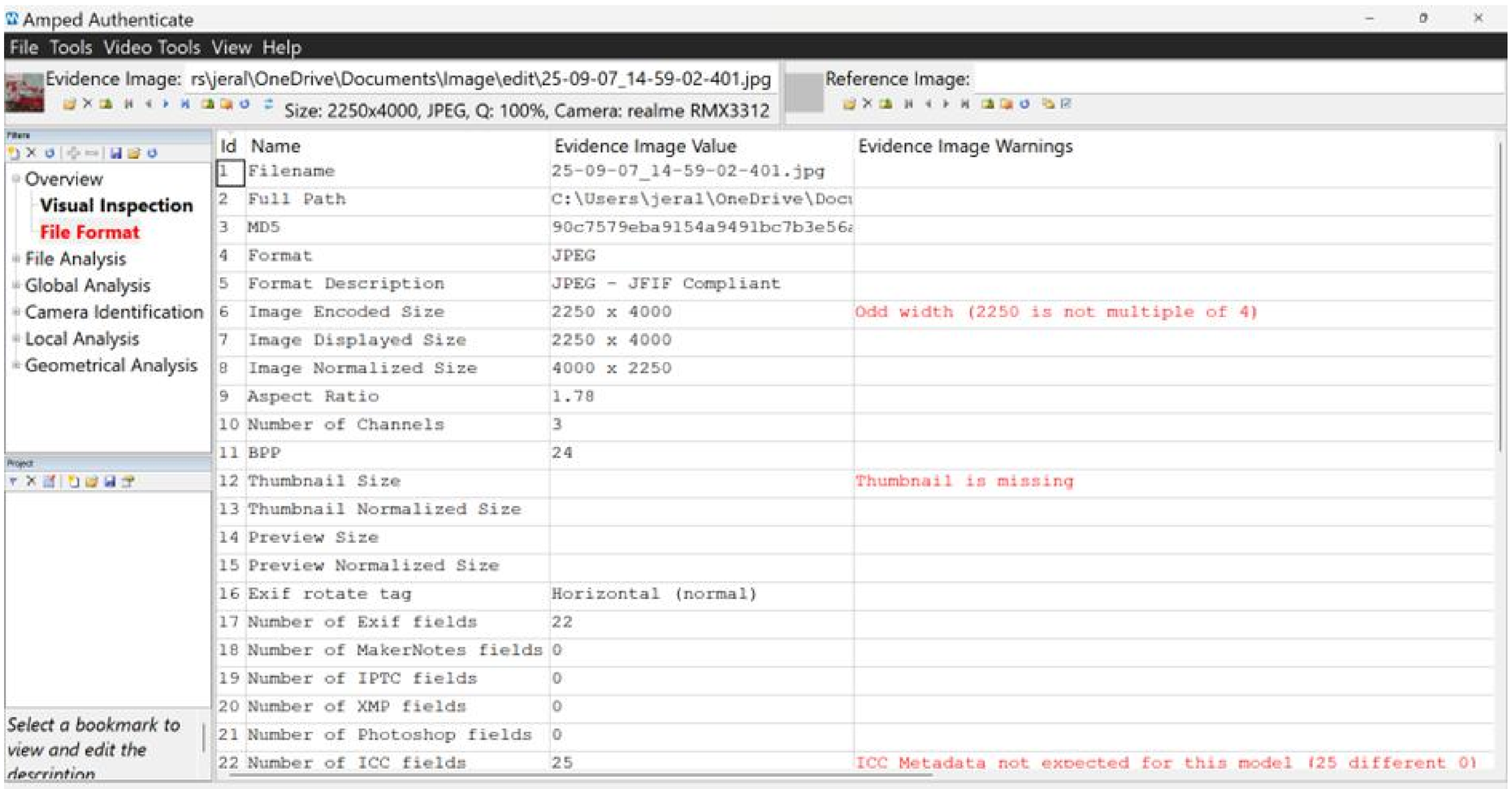
File Format Analysis:

Under File format, we can get detailed technical data about an image's structure and metadata along with the warnings.

·The image (2250×4000, JPEG, Realme RMX3312) shows unexpected ICC metadata, the use of Picsart in EXIF data (suggesting possible modification).



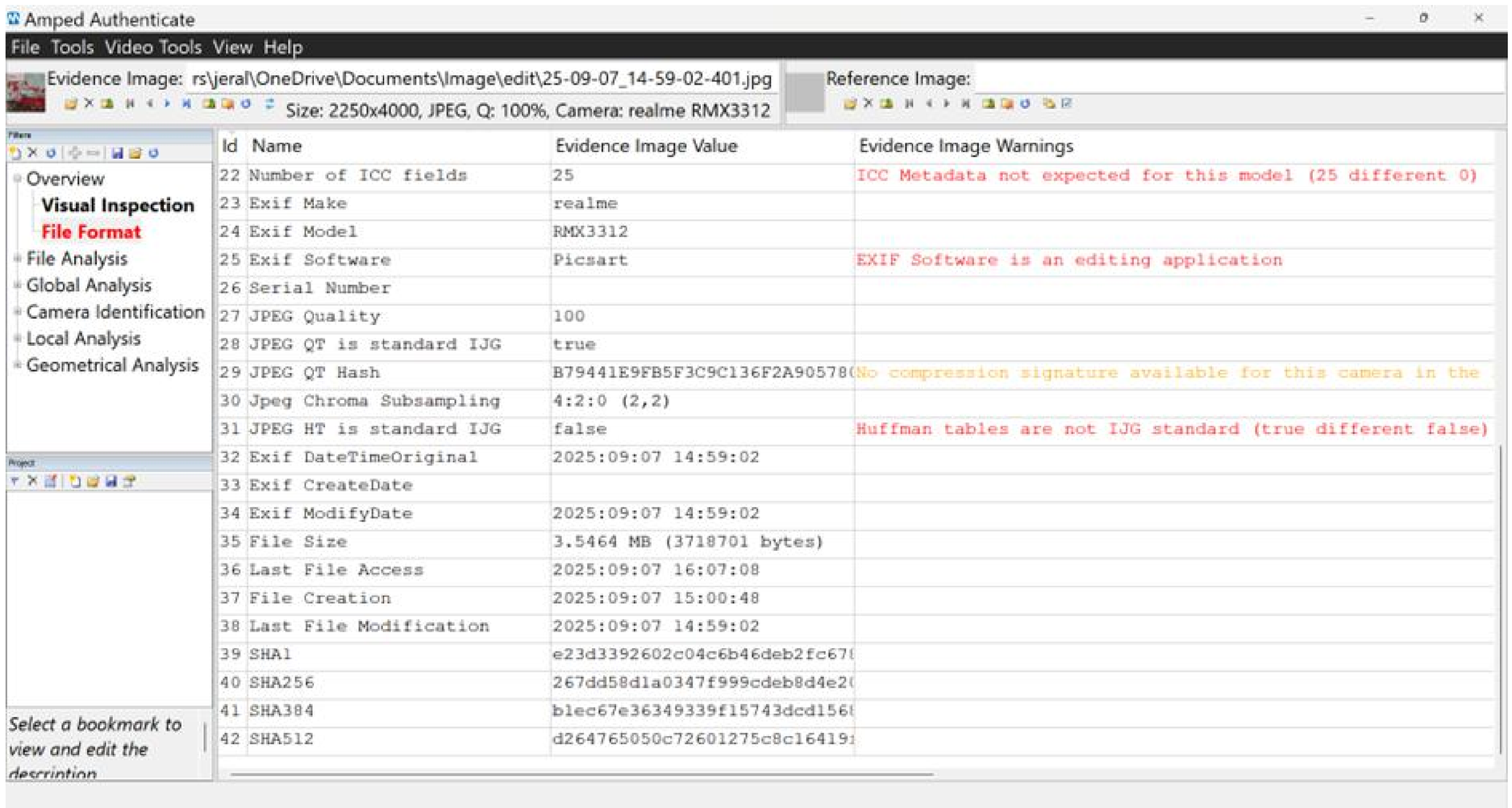
The image opened in the software



File Format

Hex Viewer analysis:

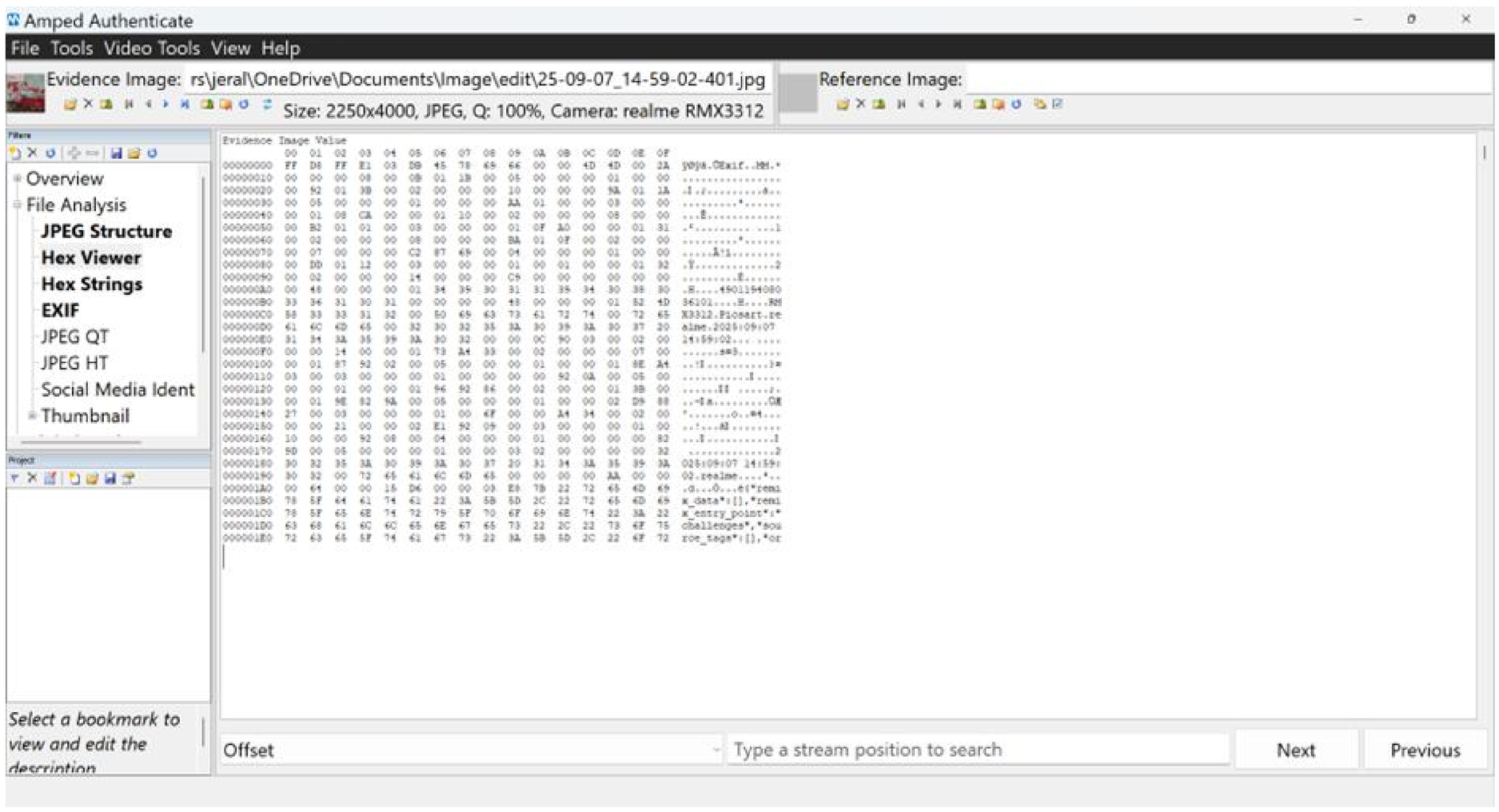
The Hex Viewer analysis revealed embedded metadata strings showing the original capture device as Realme RMX3312. However, the presence of the tag PicsArt within the hexadecimal data confirms that the image was subsequently modified using third-party editing software. Additionally, the recorded timestamp (2025:09:07 14:59:02) supports the timeline of modification. These findings indicate that the file is not an untouched original but has undergone post-capture alteration.



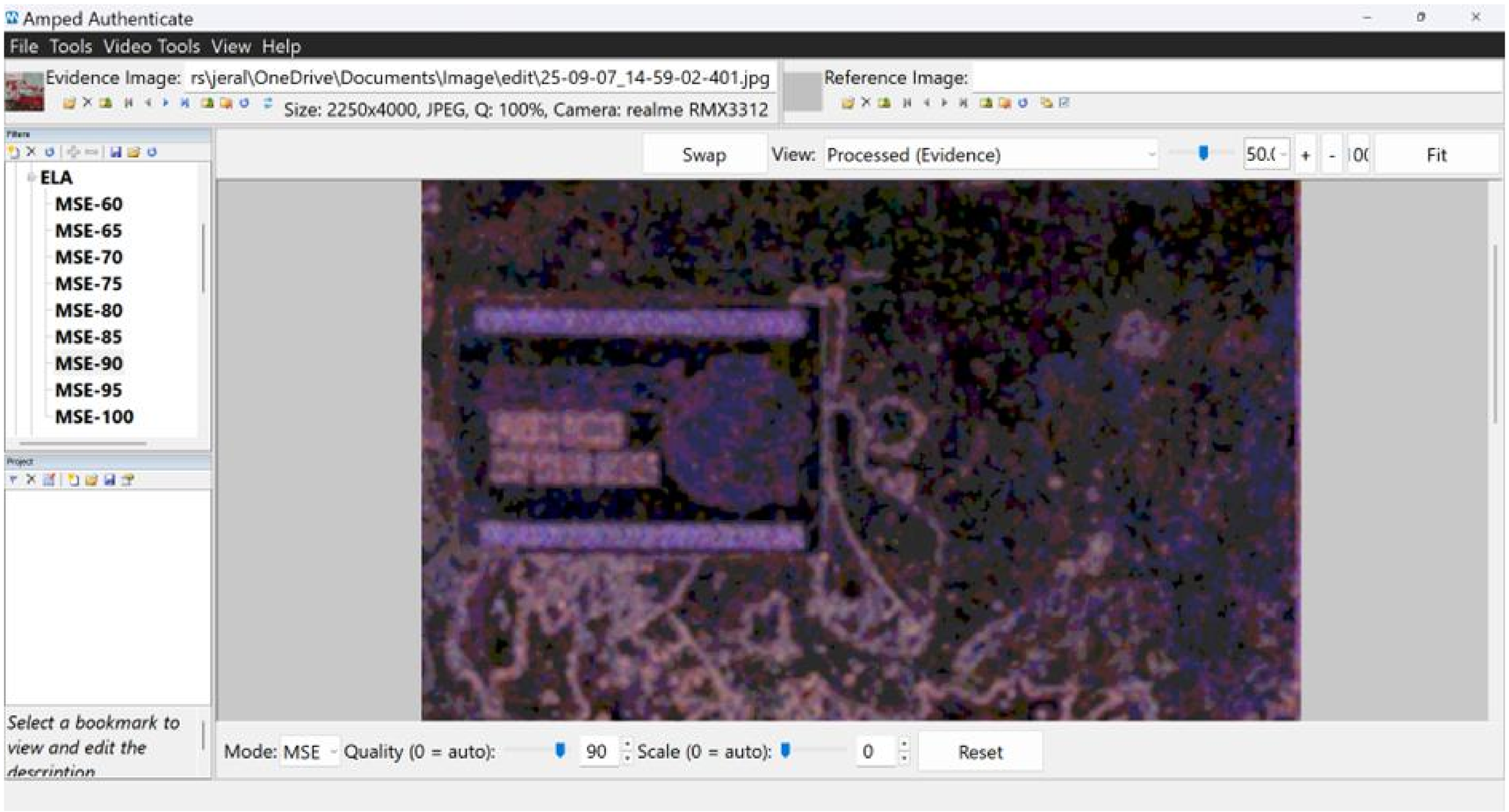
File Format

Error Level Analysis (ELA):

JPEG compression discards pixel details differently across regions. When an image is edited and resaved, altered regions often have different compression levels than the untouched ones. The tampered area (where object removal was performed in PicsArt) exhibited higher error levels, making it stand out from the surrounding untouched regions. This confirms that the image is not camera-original and has undergone post-capture manipulation.



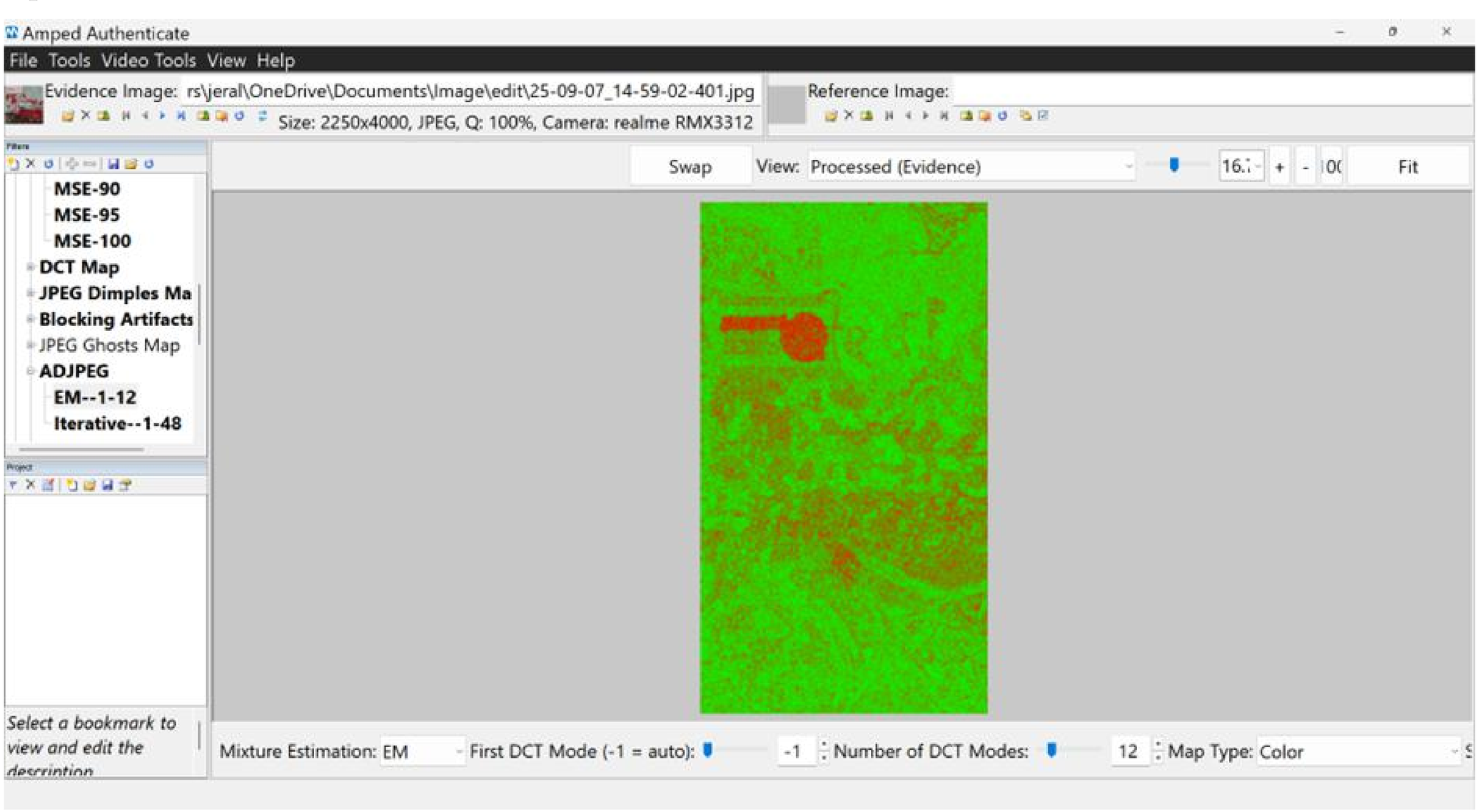
Hex Viewer



ELA MSE-90

ADJPEG Analysis:

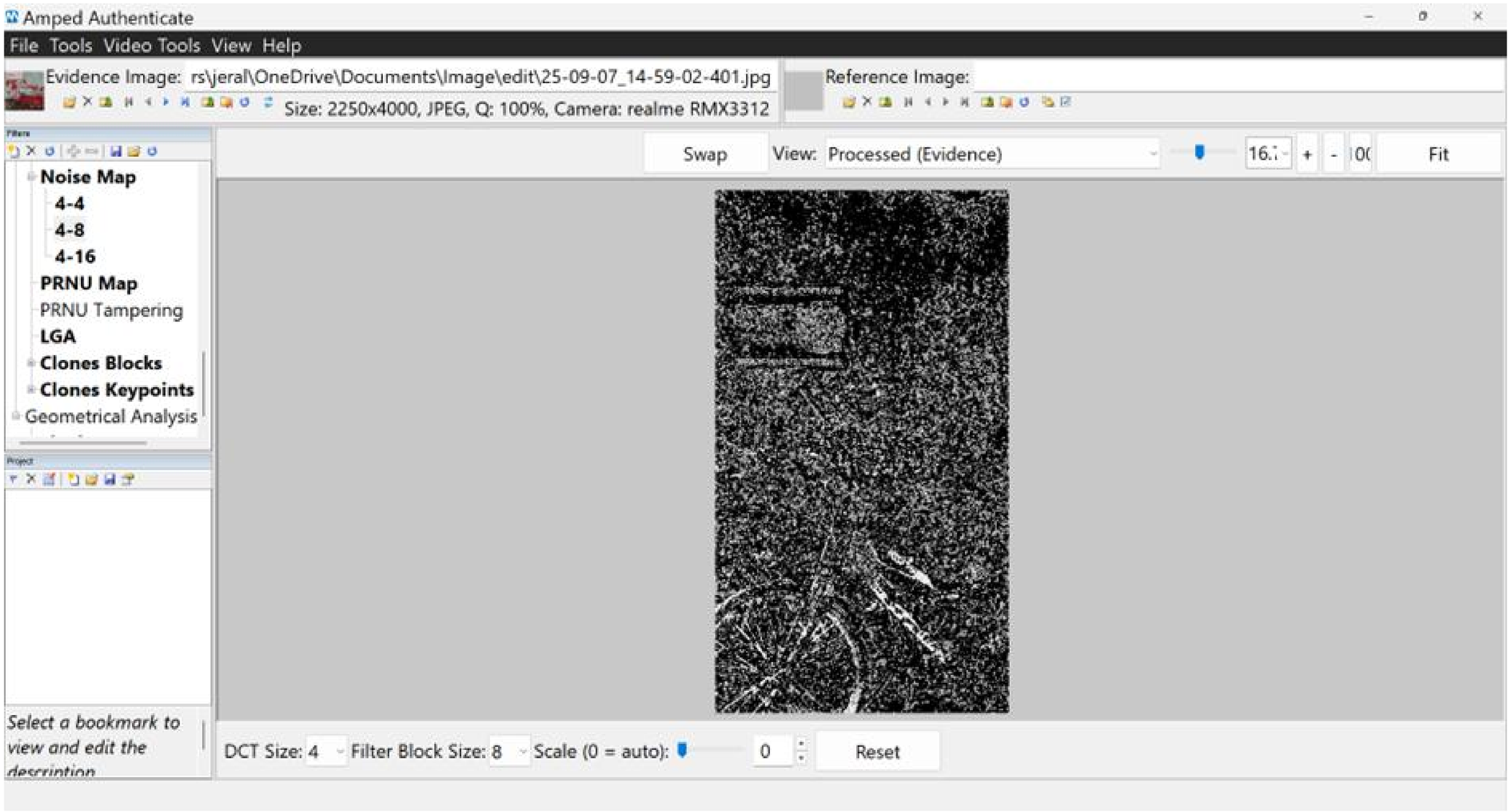
Using the ADJPEG analysis with the EM 1-12 setting, the edited area in the image is clearly highlighted in red while the rest of the image appears mostly green. This result indicates that the statistical properties of the JPEG compression (assessed through Discrete Cosine Transform, or DCT, coefficient distributions) differ significantly in the manipulated region compared to the original, unedited parts of the image. The distinct red patch marks the location where the JPEG compression grid or quantization was disrupted by editing, allowing precise localization of the tampered area



ADJPEG EM--1-12

Noise Map Analysis:

The Noise Map 4-8 filter analyses the spatial distribution of noise in small blocks (DCT size 4, filter block size 8) across the image. In your result, the edited sign area is clearly outlined with noise characteristics that contrast with the surrounding, appearing more uniform or with sharper boundaries. This contrast suggests that the tampered region (the sign) has a different noise pattern than the original image background due to modification.



RESULT

No single method is definitive on its own. Therefore, we have to rely on multiple complementary techniques in Amped Authenticate to reach reliable findings. In this experiment:

- Metadata and Hex analysis revealed traces of PicsArt and structural anomalies.
- ELA (MSE 90) highlighted the exact regions that were cloned and altered.
- Noise Map (4–8) exposed inconsistencies in natural sensor noise.
- ADJPEG (EM 1–12) confirmed double compression consistent with post-capture editing.

When combined, these results provided strong, scientifically defensible evidence that the image had been manipulated and was not camera-original.

LIMITATIONS AND CHALLENGES:

·**Quality of the Source Material:** The reliability of forensic analysis is directly related to the quality of the original file. Images that are heavily compressed, resized, or downloaded multiple times (e.g., from social media) often lose valuable forensic traces such as metadata and sensor noise. In such cases, even the best tools may yield inconclusive results.

·**Dependence on Examiner Expertise:** Forensic Software's are not an automatic truth machine. It provides scientific tests, but the interpretation of results relies on examiner expertise. For example, compression anomalies may indicate manipulation, but they may also arise from legitimate image processing.

·**Evolving Manipulation Techniques:** Image forgery methods evolve alongside detection technologies. With the rise of AI-generative content and deepfakes, forgeries are becoming increasingly realistic. Future manipulations may bypass traditional forensic indicators like compression or noise patterns.

CONCLUSION:

The forensic examination of the questioned image demonstrates how a combination of metadata inspection and local analysis can effectively expose digital tampering. While the EXIF data already suggested the involvement of editing software, deeper evaluation through Error Level Analysis, Noise Mapping, and ADJPEG analysis provided concrete evidence of localized manipulation. These methods highlighted compression inconsistencies, irregular noise distribution, and anomalous error levels, all of which collectively confirmed that the image was not camera-original.

This experiment underscores the importance of using multiple complementary techniques rather than relying on a single test. By correlating results from different forensic filters, investigators can confidently establish the authenticity of digital images and identify manipulated regions with precision. Such an integrated approach strengthens the evidentiary value of image analysis in forensic practice and ensures more reliable conclusions in court or investigative settings.

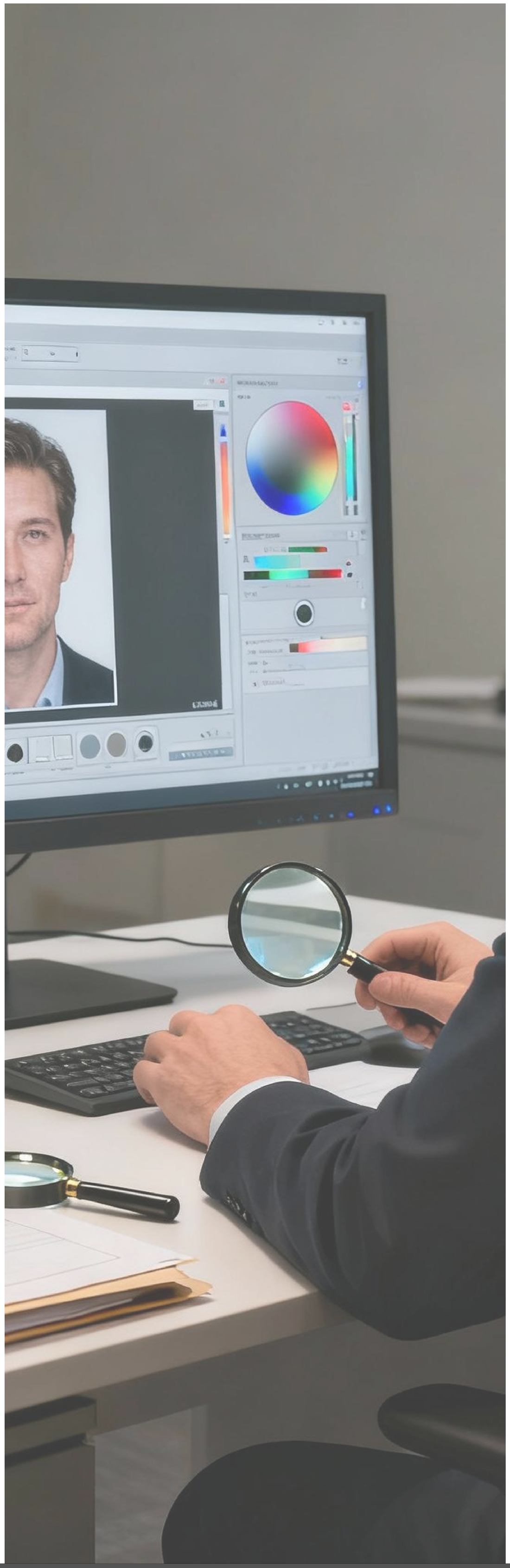
REFERENCE:

- Abdelhamid M, et al. Image and Video Forensics: A Review. IEEE Access. 2021;9:140927-140950.
- Zhang A, et al. Application of error level analysis in image spam classification using machine learning. PLoS One. 2023 Dec 13;18(12):e0291037.
- Amped Authenticate | Forensic Image Authentication [Internet]. ampedsoftware.com.
- Ul Hassan, Adnan. Recent advances in digital image manipulation detection techniques. Forensic Sci Int. 2020; 317:110526.
- Singh, Rajat, et al. A Systematic Survey on Image Manipulation Detection and Localization. ACM Comput Surv. 2024.
- Lee J, Jeon S, Park Y, Chung J, Jeong D. A Forensic Methodology for Detecting Image Manipulations. J Korea Inst Inf Secur Cryptol. 2023;33(4):671–88.
- Kamarruddin MA, Ahmad NI. Image Forensics to Detect Image Authenticity using Error Level Analysis and Noise Analysis. Int J Comput Appl. 2024;185(28):28–37.
- Chen Y, Xia S. Detecting image manipulation with ELA-CNN integration. Multimedia Tools Appl. 2024.
- Sutardja A, Ramadan O, Zhao Y. Forensic Methods for Detecting Image Manipulation - Copy Move. UC Berkeley EECS Technical Report. 2015.
- Fridrich J, Soukal D, Lukas J. Digital Image Ballistics from Sensor Noise. IEEE Trans Inf Forensics Secur. 2012;7(5): 1558-1571.
- Anwar MA, et al. Image forgery detection by transforming local descriptors. J Vis Commun Image Represent. 2023;93:103358.

ABOUT THE AUTHOR

Jerald Benny
MSc Forensic Science





FORENSIC APPROACHES TO DIFFERENTIATE MENSTRUAL AND PERIPHERAL BLOOD TRACES AT CRIME SCENES



Author: Ms. Sidhvita Kaithepalli

OVERVIEW

In forensic Studies,telling the difference between menstrual blood and normal body (peripheral) blood is very important in solving crimes, especially in sexual assault cases. With the help of modern science, experts now have better ways to do this. Tests like quick strips (immunochromatographic assays), studying genes, and using special light methods (Raman spectroscopy) have made it easier to identify menstrual blood at crime scenes. Some markers, like hemoglobin and D-dimer, help in quick on-the-spot testing, while newer methods like microRNA (miRNA) and inflammatory markers work at the molecular level to separate the two types of blood. Still, not every test works perfectly every time for example, some kits like Seratec® PMB give mixed results in trial studies, which shows why proper checking and standard rules are needed. Scientists have also found that menstrual blood contains special stem cells, which makes it different from normal blood and useful in forensics. This review explains these methods, their strengths and weaknesses, and shows why combining different approaches is the best way to get accurate results.

INTRODUCTION

Blood is a vital fluid in the human body, serving as a transport system for oxygen, nutrients, hormones, and enzymes to different organs and tissues, while simultaneously removing metabolic wastes. In the field of forensic science, blood is among the most commonly encountered biological fluids at a crime scene and is regarded as one of the most informative types of evidence. The presence, distribution, and nature of bloodstains can provide crucial insights into the events that transpired, assist in reconstructing crime scenes, and contribute to linking individuals with specific criminal acts.

However, not all blood is the same. Peripheral blood, which circulates throughout the body, differs significantly from menstrual blood, which originates from the uterus and is shed during the menstrual cycle. Menstrual blood is a complex mixture containing peripheral blood, vaginal secretions, endometrial tissues, and microorganisms, making it distinct in both composition and forensic significance. Distinguishing between these two types of blood is highly important in sensitive cases such as sexual assault investigations, homicide, or instances where the sequence of events at a crime scene is unclear. For example, identifying the presence of menstrual blood can either corroborate or contradict victim or suspect statements and can influence the interpretation of the circumstances surrounding a crime.Traditionally, older forensic methods such as presumptive chemical tests (e.g., Kastle–Meyer test, benzidine test, phenolphthalein test) and microscopic examination were able to confirm the presence of blood but could not differentiate between menstrual and peripheral blood. This posed a serious limitation, as forensic experts could not always determine the origin of the bloodstains, which sometimes resulted in misinterpretation of crucial evidence.

To address this gap, modern forensic science has developed more advanced and specific methods. These include immunochromatographic assays (strip-based rapid tests), which detect biomarkers specific to menstrual fluid; spectroscopy-based methods that utilize the unique light absorption and emission properties of blood components; and molecular approaches such as RNA profiling and microRNA analysis, which exploit gene expression differences between menstrual and peripheral blood. Recent research highlights that menstrual blood possesses unique characteristics, including elevated immune activity, the presence of endometrial fragments, and even stem-like cells, setting it apart from normal circulating blood.

The importance of correctly identifying menstrual blood lies in its direct impact on the integrity of forensic investigations. A false assumption about the type of blood present at a crime scene can mislead investigators, alter the direction of inquiry, or even compromise judicial outcomes. On the other hand, accurate differentiation can provide solid scientific backing for or against statements made by individuals involved in a case, thereby strengthening the probative value of forensic evidence.

Since each detection method carries its own advantages and limitations, forensic experts increasingly advocate for a multidisciplinary approach. By combining chemical, immunological, molecular, and light-based .

techniques, investigators can obtain more reliable, reproducible, and comprehensive results. Such an integrative approach enhances the credibility of forensic analysis and ensures that the justice system is supported with scientifically sound evidence.

Tables (Table 1 and Table 2) can be used to summarize the biochemical differences between peripheral and menstrual blood, as well as to outline the various detection methods, their principles, advantages, and limitations. Together, these insights underscore the growing importance of advanced scientific tools in modern forensic biology and their contribution to achieving accurate and fair criminal justice outcomes

Feature	Peripheral Blood	Menstrual Blood
Composition	Red blood cells, white blood cells, platelets, plasma	Peripheral blood + endometrial tissue, vaginal epithelial cells, cervical mucus
Cytokine Activity	Normal baseline	Elevated
Fibrinolytic Markers	Normal D-dimer levels	High D-dimer levels
Stem-like Cells	Typically absent	Mesenchymal stem-like cells present
Forensic Relevance	Commonly encountered; general forensic evidence	Important in sexual assault and ambiguous cases; distinct biological signature
Challenges	Easier to detect; less complex composition	Complex matrix; may degrade; cross-reactivity possible

Table 1: Comparison between Peripheral and Menstrual Blood

Method	Principle	Advantages	Limitations
Microscopic / Chemical Tests	Hemolysis patterns, physical properties	Simple, low-cost, easy to perform	Low specificity, unreliable in degraded/old samples
Immunochromatographic Assays (e.g., D-dimer, Seratec® PMB)	Detects fibrin degradation products	Rapid, easy on-site application	Cross-reactivity, reduced reliability in pathological conditions
Molecular Methods (Gene expression, miRNA profiling)	Identifies genetic/molecular markers	High specificity, stable in some conditions	Needs validation, expensive, technical expertise
Spectroscopic Techniques (Raman spectroscopy)	Analyzes biochemical spectral shifts, analysis using light scattering	Non-destructive, can estimate time since deposition	Costly instruments, expertise needed
Immunological / Cellular Approaches	Cytokine profiling, stem-cell markers	Highlights biological uniqueness of menstrual fluid	Still experimental, not standardized

Table 2: Methods for Differentiating Menstrual and Peripheral Blood

FUTURE DIRECTIONS

There are many way to improve the quality of the outcomes in differentiating the menstrual blood from peripheral blood in less short span:

[2] Firstly, when there is a combination of proteomics (proteins) and transcriptomics (RNA expression) into a multi-omics strategy, there might be a possibility to find reliable and unique markers of menstrual blood, which even help in distinguishing the degraded samples But to make it useful in real forensic cases, miRNA and gene expression markers need to be standardized and tested under real environmental conditions for better outcomes.

[2]Second, machine learning algorithms which hold potential for automated classification of body fluids. Raman spectroscopy, coupled with AI-driven interpretation, could reduce subjectivity in forensic fluid identification.

[2]Third, further exploration of menstrual stem cell markers in forensic samples may offer an additional, less-explored line of differentiation. Immunophenotyping or single-cell analysis could identify cellular compositions exclusive to menstrual blood.[2]Additionally, development of low-cost, field-deployable molecular kits, particularly for low-resource settings, remains an urgent need. Many advanced techniques require laboratory infrastructure that may not be feasible in all investigative environments.

[2]Collaborative studies involving large forensic case datasets, diverse populations, and variable substrates are crucial to validate and calibrate these techniques for real-world conditions. Without such efforts, the forensic reliability of even the most promising approaches will remain constrained.

[2]Finally, the ethical implications surrounding menstrual fluid collection and analysis must be addressed, especially in sexual assault cases. Consent, cultural sensitivity, and survivor-centered protocols should be embedded into methodological design and reporting.

CONCLUSION

There is a need to differentiate between the menstrual and peripheral blood in crime scene investigations, particularly in sexual assault cases, homicide cases, or when evidence is ambiguous. Over the years there are already some innovations and techniques have been introduced, as show in below Table (1). While current techniques provide useful differentiation between menstrual and peripheral blood, future advancements are expected to refine accuracy, reliability, and applicability. Table (2) highlights emerging opportunities and directions in this field.

Technique/ Approach	Significance/ description
Immunochromatographic, spectroscopic, and molecular techniques	There are the sophisticated tools to distinguish between menstrual and peripheral blood
Immunological assays (e.g., D-dimer detection)	Provide rapid field-level screening, molecular approaches
miRNA profiling and gene expression analysis	Demonstrate high specificity but require further validation under forensic conditions.
Raman spectroscopy and bioinformatics-integrated diagnostics	These techniques hold promise for improving accuracy and reproducibility. However, challenges remain in terms of accessibility, standardization, and interpretation of results, especially in complex or degraded samples.

Table 3: Techniques for Differentiating Menstrual and Peripheral Blood

Focus Area	Future Opportunities / Significance
Multi-modal strategies	Combining biochemical, cellular, and molecular markers may yield the most reliable outcomes in practical casework.
Stem cell-derived markers & cytokine profiles	Present promising avenues for forensic innovation and more specific identification.
Machine-learning classification systems	Enable automated, accurate, and reproducible interpretation of forensic evidence.
Research emphasis	Must focus on real-case applicability, ethical handling, and cross-disciplinary collaboration.
Forensic impact	Integration of these advancements will strengthen evidentiary value and ensure justice.

Table 4: Future Directions and Opportunities in Forensic Differentiation

REFERENCES

·Holtkötter H, Filho CRD, Schwender K, Stadler C, Vennemann M, Pacheco AC, et al. Forensic differentiation between peripheral and menstrual blood in cases of alleged sexual assault validating an immunochromatographic multiplex assay for simultaneous detection of human hemoglobin and D-dimer. International Journal of Legal Medicine [Internet]. 2017 Oct 23;132(3):683–90. Available from: https://doi.org/10.1007/s00414-017-1719-y

·Mia R. "Use scientific method to detection and comparison of menstrual blood samples found at the crime scene." Biomedical Journal of Scientific & Technical Research [Internet]. 2022 Jan 27;41(3). Available from: https://doi.org/10.26717/bjstr.2022.41.006599

·Konrad H, Hartung B, Poetsch M. (Un)Reliable detection of menstrual blood in forensic casework evaluation of the Seratec® PMB test with mock samples. International Journal of Legal Medicine [Internet]. 2023 Nov 30;138(3):781–6. Available from: https://doi.org/10.1007/s00414-023-03138-3

·Weber A, Wójtowicz A, Wietecha-Posłuszny R, Lednev IK. Raman Spectroscopy for the Time since Deposition Estimation of a Menstrual Bloodstain. Sensors [Internet]. 2024 May 21;24(11):3262. Available from: https://doi.org/10.3390/s24113262

·Moawad AM, Zaghlol HS, Abdelsalam MH, Abdelfattah A, Sabry D, Atef A. Differential genes expression biomarkers for menstrual and peripheral blood stains analysis. Egyptian Journal of Forensic Sciences [Internet]. 2018 Jun 21;8(1). Available from: https://doi.org/10.1186/s41935-018-0072-8

·Valentine A. Differentiation Between Peripheral Blood and Menstrual Blood using miRNA markers [Internet]. VCU Scholars Compass. Available from: https://scholarscompass.vcu.edu/frsc_projects/39

·Verma P. Detection and comparison of normal and menstrual blood samples found at crime scene. Journal of Forensic Sciences & Criminal Investigation [Internet]. 2018 May 30;9(2). Available from: https://doi.org/10.19080/jfsci.2018.09.555760

·Holtkötter H, Dierig L, Schürenkamp M, Sibbing U, Pfeiffer H, Vennemann M. Validation of an immunochromatographic D-dimer test to presumptively identify menstrual fluid in forensic exhibits. International Journal of Legal Medicine [Internet]. 2014 Nov 4;129(1):37–41. Available from: https://doi.org/10.1007/s00414-014-1097-7

·Naseri S, Rosenberg-Hasson Y, Maecker HT, Avrutsky MI, Blumenthal PD. A cross-sectional study comparing the inflammatory profile of menstrual effluent vs. peripheral blood. Health Science Reports [Internet]. 2023 Jan 1;6(1). Available from: https://doi.org/10.1002/hsr2.1038

·Liu Y, Niu R, Yang F, Yan Y, Liang S, Sun Y, et al. Biological characteristics of human menstrual blood-derived endometrial stem cells. Journal of Cellular and Molecular Medicine [Internet]. 2017 Dec 26;22(3):1627–39. Available from: https://doi.org/10.1111/jcmm.13437

·Lv H, Hu Y, Cui Z, Jia H. Human menstrual blood: a renewable and sustainable source of stem cells for regenerative medicine. Stem Cell Research & Therapy [Internet]. 2018 Nov 21;9(1). Available from: https://doi.org/10.1186/s13287-018-1067-y

·Patel AN, Park E, Kuzman M, Benetti F, Silva FJ, Allickson JG. Multipotent menstrual blood stromal stem cells: isolation, characterization, and differentiation. Cell Transplantation [Internet]. 2008 Mar 1;17(3):303–11. Available from: https://doi.org/10.3727/096368908784153922

ABOUT THE AUTHOR

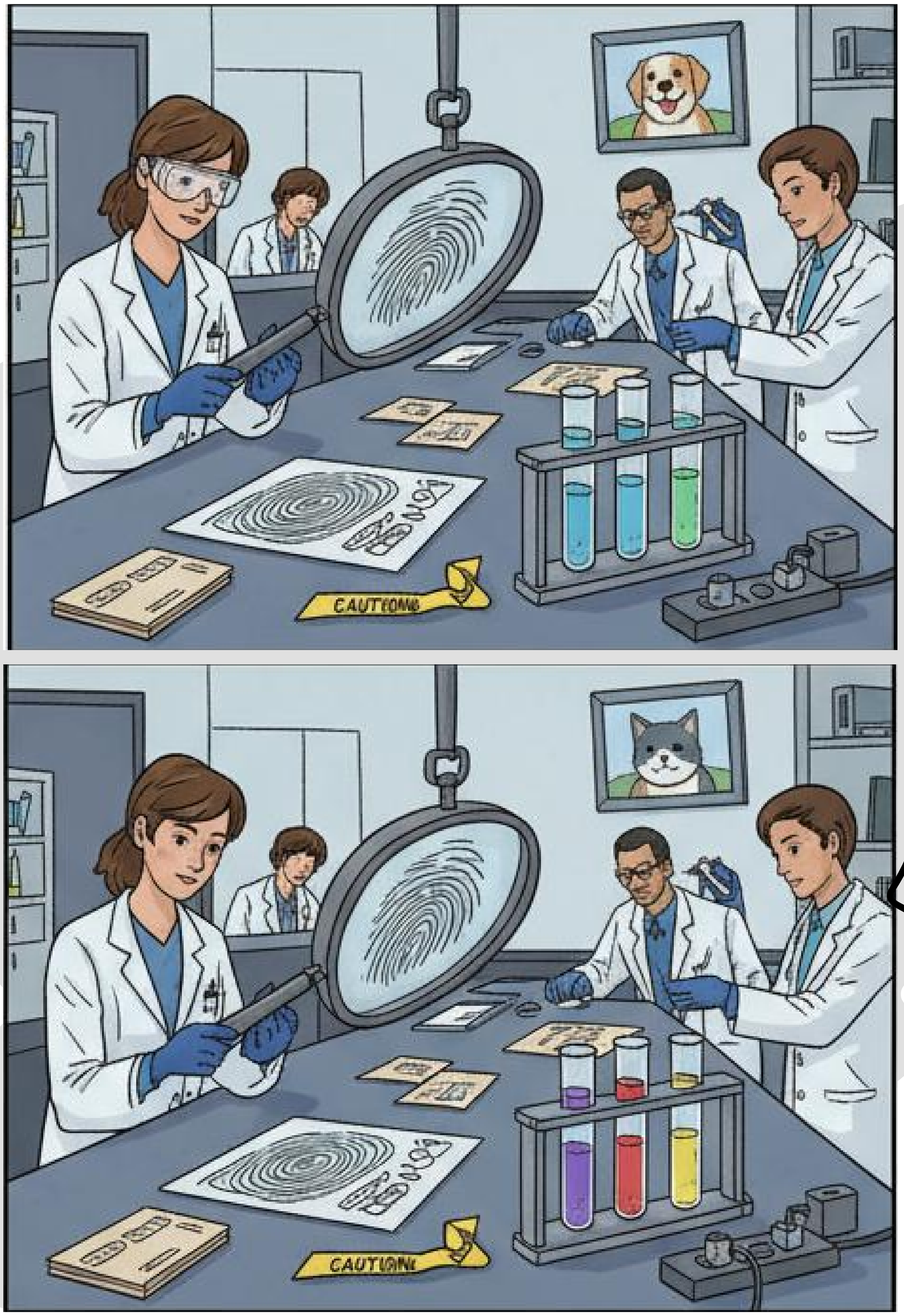
Ms. Sidhvita Kaithepalli
Assistant Professor, Sigma University



IN CASE YOU MISSED IT...

Ancient Egyptians believed that wine was the blood of people who dared to battle against Gods. The reason why they believed this is that drinking wine temporarily made people crazy and drove them out of their senses.

Spot the Difference



JOURNEY OF ARTIFICIAL INTELLIGENCE AND DRONE FORENSICS: AN OPINION ABOUT JUDICIAL PERSPECTIVES ON THE ADMISSIBILITY OF EVIDENCE



Author: Anumod P K

Artificial Intelligence

Global legal systems are fast-changing due to artificial intelligence (AI), which presents both benefits and difficulties for the legal system. As AI-generated evidence, prediction tools, and decision support systems become more prevalent in courts, established legal concepts like accountability, justice, and evidence admissibility are being re-examined can improve the effectiveness, consistency, and accessibility of judicial systems in a variety of fields, including case result analysis, digital forensics, and predictive policing. But its incorporation into legal proceedings needs close examination. AI-generated evidence's dependability and admissibility are two of the main legal issues.AI tools used in voice analysis, facial recognition, or digital forensics, for example, must meet evidentiary requirements, including accuracy, authenticity, and relevance, before they may be utilized in court. The methods used by AI systems must be transparent and reproducible, and judges must assess if these systems have received enough validation. The question is whether this kind of evidence has evidential or probative value. Human mistake, such as coding faults and other manufacturing errors, is possible because AI was created by people. The effectiveness of the AI is still important. For instance, an AI tool that detects blood samples has 99% efficiency, meaning that 1% of the 100 samples provided have an error, even if the sample is a true one. This could result in the offender being found not guilty. AI can therefore be utilized as supporting or corroborating evidence. AI-based evidence is therefore seen as conditionally reliable: when properly verified, transparent, and utilized under human supervision, it can improve the delivery of justice; nevertheless, in the absence of safeguards, it runs the risk of eroding accountability, fairness, and due process in courtrooms.
The next concern is about the privacy data protection, and consent is brought up by the use of AI to process sensitive personal data. The preservation of fundamental rights and technological advancement must be balanced by the courts. To ensure that individual liberties are not compromised, court must carefully weigh the use of AI to increase efficiency. Strict adherence to legal protections, openness in data processing, and responsibility in the use of AI-driven evidence are necessary for this. The judiciary must, after all, make sure that technological developments improve the administration of justice without undermining the fundamental guarantees of due process, privacy, and compliance

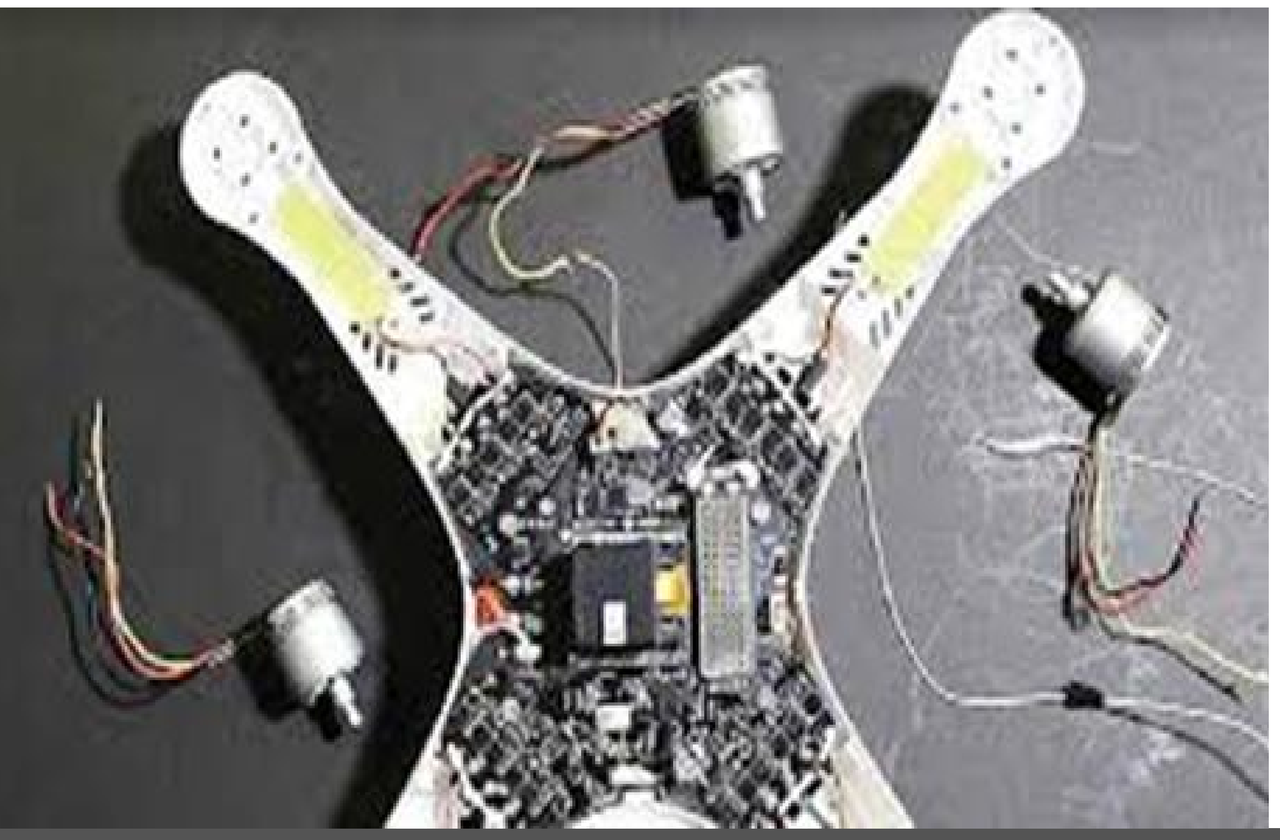


DRONE EVIDENCE

Drone forensics has developed as a rapidly growing topic within digital forensics and forensic science, owing to the rising use of drones in both civilian and criminal contexts, as well as their potential role in surveillance, smuggling, terrorism, reconnaissance, and even accidental incidents. Drone forensics is the identification, collection, preservation, examination, analysis, and interpretation of digital evidence obtained from unmanned aerial vehicles (UAVs) and their associated devices, like remote controllers, GPS modules, memory cards, cloud accounts, and companion mobile applications. Drone forensic analysis, when performed by trained specialists using established methods, meets several admissibility criteria and has already been accepted in cases of border smuggling, airspace infractions, and privacy breaches. Despite its promise, drone forensics has numerous disadvantages that can reduce the evidentiary value of drone-derived material in court. Initially, the absence of standardized protocols for drone forensic analysis across countries leads to disparities in data collection and interpretation, which defense lawyers might take advantage of to contest admission. In contrast to more established forensic sciences, drone forensics is still developing, and the lack of uniform validation or

codification of its methodology raises concerns over the scientific trustworthinessfield. Second, drones are extremely vulnerable to firmware change, hacking, and tampering, which can compromise the integrity of the evidence by erasing important data, corrupting logs, or changing recorded data. The possibility of remote manipulation or post-event data change is high because many drones use wireless networks or synchronize with mobile apps and cloud storage. As a result, judges could be reluctant to rely on such evidence without confirmation. Third, anti-drone forensics which include GPS spoofing and signal jamming, are known flaws that might confuse forensic investigators by showing bogus flight routes or misidentified locations, decreasing the probative value of drone data. Top of Form

Criminals may also use remote wiping tools, which wipe data from drones or synchronized cloud accounts after the drone is confiscated. Cloned serial numbers, anonymous controllers, or altered digital identifiers further obfuscate ownership attribution, making it challenging to connect a drone to a particular operator. Drones sometimes have crash-trigger or self-destruction features that physically destroy evidence before it can be retained. By casting doubt on the validity, dependability, and completeness of drone data, these strategies drastically lower its evidential value in court. The difficulties forensic specialists encounter in thwarting these techniques underscore the necessity of sophisticated counter-forensic instruments, more robust anti-tampering technologies, and established protocols to guarantee drone evidence's continued admissibility and reliability in court.Fourth, attribution issues pose challenges: even if a drone is found and its flight logs analysed, attributing it decisively to a single operator might be difficult unless biometric data, fingerprints, or unique digital identifiers are discovered. As courts become more aware of possible constitutional violations of rights against illegal searches and seizures, particularly when forensic data is obtained without the required authorization or warrants, privacy concerns and legal issues also make admission less likely.



Additionally, because many forensic investigators rely on third-party technologies that might not fully access encrypted or proprietary data, creating questions about accuracy and completeness, the proprietary nature of drone software and encryption techniques poses challenges to forensic validation. Adherence to appropriate forensic procedures, tool validation, a clear chain of custody, and confirmation with additional sources of evidence are all crucial for its validity in court.

CONCLUSION

For contemporary judicial systems, the validity and admissibility of drone forensics and artificial intelligence (AI) in court provide both possibilities and difficulties. Because of AI's strong analytical capabilities, investigators can process massive datasets, find hidden patterns, and offer unbiased insights that can support their cases. Similarly, flight logs, GPS coordinates, information, and photos from drone forensics offer precise evidence that can create timelines and connect suspects to murder scenes. Both types of evidence can be quite trustworthy if they are handled strictly in accordance with forensic procedures and the chain of custody. But there are disadvantages to using them in court. Algorithmic bias, opaque "black box" models, a lack of peer-reviewed validation, and worries about accountability for mistakes are some of the main issues with AI. The manipulation of position data to deceive investigators about the drone's true path or destination is known as GPS spoofing or jamming. The use of remote wiping tools, which wipe data from drones or synchronized cloud accounts after the drone is confiscated, is another tactic used by thieves It is challenging to connect a drone to a particular operator since ownership attribution is further muddled by cloned serial numbers, anonymous controllers, or altered digital identifiers. To physically destroy evidence before it can be preserved, drones are sometimes built with crash-trigger or self-destruction features. These strategies cast doubt on the completeness, legitimacy, and dependability of drone data, which drastically lowers its evidential value in court. It is difficult for forensic professionals to combat these techniques, which emphasizes the need for more sophisticated counter-forensic tools and more robust anti-tampering measures.Therefore, expert validation, a rigorous chain of custody, and confirmation with other types of evidence are required for both AI and drone forensics to be admissible.

When used properly, they can greatly strengthen cases, but because of their disadvantages, judges are hesitant to use them alone. In the future, it will be crucial to provide tamper-resistant systems, universal forensic standards, and transparency in drone data collecting and AI algorithms. In the end, AI and drone forensics have a lot of promise to improve the administration of justice, but their actual worth in court will rely on how well they strike a balance between innovation, dependability, accountability, and due process.

REFERENCES

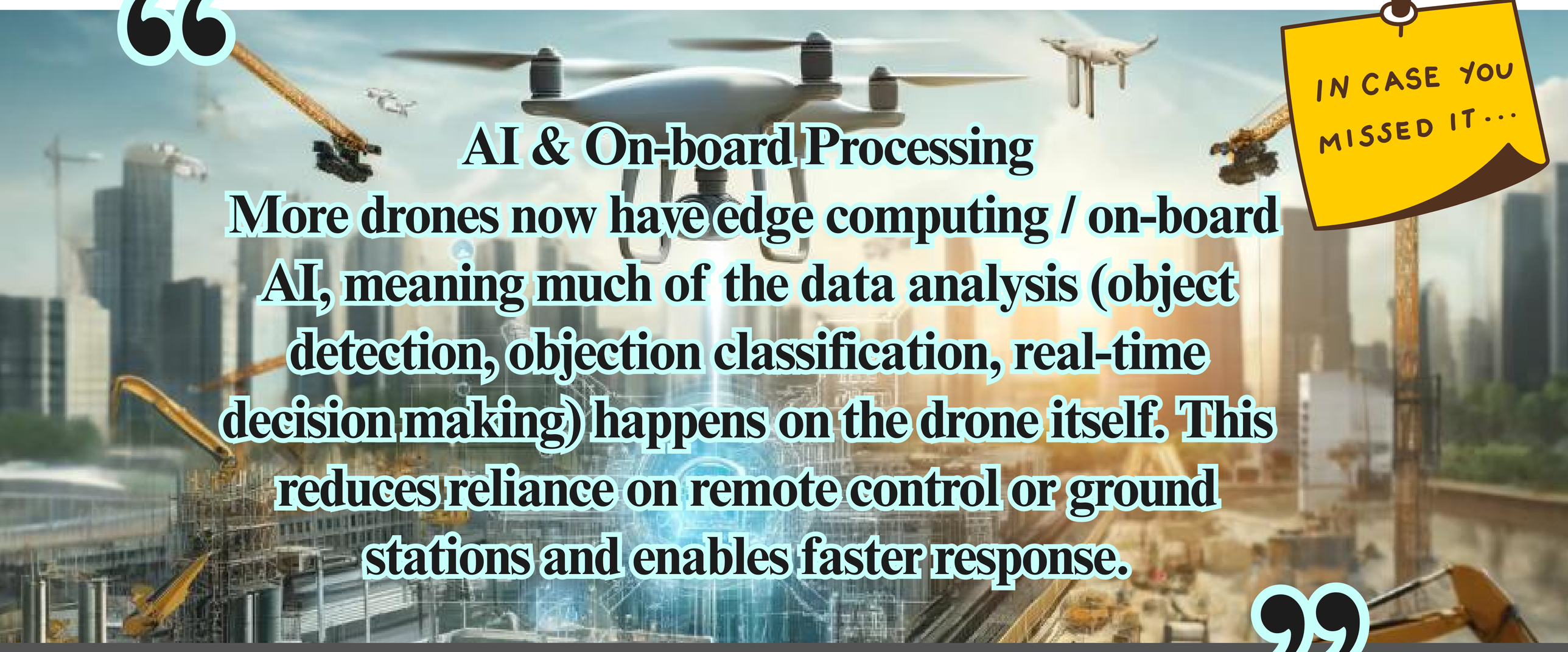
- Mantas E, Patsakis C. Who watches the new watchmen? The challenges for drone digital forensics investigations. arXiv. 2021 May 23:arXiv:2105.10917.
- Kim Y, Cho K, Kim S. Challenges in drone firmware analyses of drone firmware and its solutions. arXiv. 2023 Dec 28:arXiv:2312.16818.
- National Research Council. Strengthening forensic science in the United States: a path forward. Washington (DC): National Academies Press; 2009
- Ranganathan A, Ólafsdóttir H, Capkun S. SPREE: Spoofing-resistant GPS receiver. arXiv. 2016 Mar 17:arXiv:1603.05462.
- Dang Y, Benzaid C, Yang B, Taleb T. Deep learning for GPS spoofing detection in cellular-enabled unmanned aerial vehicle systems. arXiv. 2022 Jan 3:arXiv:2201.00568.
-
- Adel A, Jan T. Watch the skies: A study on drone attack vectors, forensic approaches, and persisting security challenges. Future Internet. 2024;16(7):[Article].
- O'Brien TL, Hawkins SL, Loesch A. Scientific disciplines and the admissibility of expert evidence in courts. [Journal]. 2022;[Volume]:[Pages].
- Lesciotto KM. The over-citation of Daubert in forensic anthropology. J Forensic Sci. 2024.

ABOUT THE AUTHOR

Anumod P K

M.Sc. Forensic Science





Did You Know?



Bugs can help solve a crime. It's actually called forensic entomology. While bugs can't actually solve a crime, investigators are able to look inside of an insect's (typically a maggot) stomach and is able to determine how long a body has been decomposing.

MALWARE FROM SPACE: FORENSIC ANALYSIS OF SATELLITE–BASED CYBER INTRUSIONS



Author: Princy Soni, Kiran Dodiya, Dr. Kapil Kumar

Introduction:

When we think about cyber threats, we usually imagine some common threats like malware, phishing, and ransomware that occur in various banks, online websites, and companies, but what if a satellite can be targeted by malware? It is a genuine cybersecurity concern. If we want to learn about forensic analysis of satellite and malware from space, then first of all, we have to know about satellite technologies and how they work. Here's the basic concept of a satellite. A satellite is an object that moves around other objects. For example, Earth moves around the Sun., and also the Moon moves around Earth. There are many other satellites. They usually mean an artificial satellite.

Artificial satellites are machines built by humans. All satellites are created for different purposes, like some take photos of Earth and other planets, which help scientists to learn about space. Some of these satellites send TV signals, phone calls, and also provide internet access. All satellites have some standard parts, like an antenna, that help to send and receive information. Solar panels collect sunlight and turn it into electricity, and batteries store energy for use. [1]



Fig : Malware in Space

How does a satellite work?

The basic meaning of a satellite is a communication tool that can send and receive signals from Earth and send them back using devices like transponders. Those types of devices help satellites relay radio signals to different parts of the world.There are three main components of a satellite system: "communication system", "power system", and "propulsion system".

The communication system in a satellite includes antennas and transponders that handle signal transmission. The power system of a satellite is usually made up of solar panels and backup batteries that supply the satellite with energy, and the propulsion system includes rockets that help the satellite reach its orbit and stay in position. Satellite sometimes drifts because of the gravitational pull of the Moon and Sun.. To stay in the perfect space, they use engines. If the fuel runs out, the satellite can no longer adjust its position. A satellite needs continuous power to operate electronics. They mostly use sunlight and batteries. These batteries are charged by electricity from solar panels. Satellite needs to stay connected with Earth. To stay connected, satellites use the Telemetry, Tracking, and Command (TT&C) system. This allows ground stations to control the satellite, track its position, and also monitor satellite temperature and battery level.[2]

Space Secrets: The Truth About Space Malware

Satellites are very useful in today's life. They help us by providing communication, navigation, weather updates, disaster response, and more. Satellites are becoming popular targets for hackers because of their importance in day-to-day life. Satellite hacking happens when unauthorized users hack or break into a satellite system using malware or other cyber tools.These hackers can breach the communication between the satellite, and they can also take complete control of the satellite. This can be dangerous. A hacker can steal essential and secret data, and also can block or encrypt communications. The hackers could be from governments, terrorist groups, or independent hackers. But hacking the satellite is not easy and is less risky than traditional military spying. Hackers can use satellite modems from anywhere in the world; it's tough to trace a hacker or determine where the attack comes from. The regular firewalls or IDS and IPS cannot detect these intrusions because satellite data doesn't rely on local internet systems. [3]

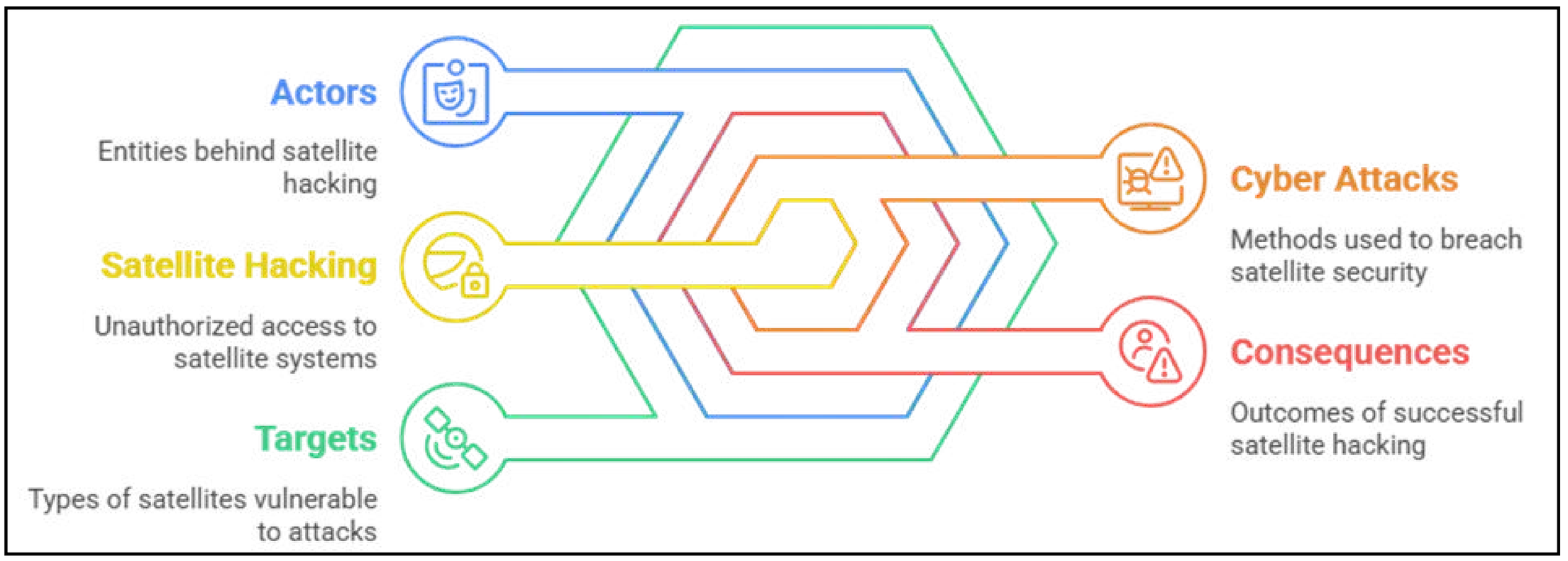


Fig :Space Secrets: The Truth About Space Malware

What Links in The Sky: Uncovering Satellite System Vulnerabilities

Satellites are high-tech, but still have many weaknesses. And it is tough to find the weaknesses of the satellite systems. Here are some vulnerabilities of satellite systems: Hackers may target ground stations that control satellites. If a hacker gains access to the control, then they can change the satellite's path, and they can also steal information. It is known as "Ground Station Breach". Without strong security, the data is sent between satellites. This could include private or classified data. It is known as "Data Spying".

There are also more vulnerabilities, like "signal jamming". In this attack, hackers can block satellite signals, and this can lead to communication problems or complete blackouts. "Old software Issues" can happen when many satellites use outdated software, which may have security holes. Hackers can use these to break into the satellite's system. Satellites are also at risk from "Malware attacks". That can infect their systems. Once infected, a satellite could be used for spying or sending stolen data to the hacker. Hackers can pretend to be real service providers to fool the system and make them easy targets for hacking the space known as "Fake Identities". If a hacker gains complete control of a satellite, they might crash it into another satellite or change its orbit. It can be dangerous for satellite systems. It is known as "Orbit Manipulation". [4]

Consequences of Cyber Attacks on Satellite:

"Data Theft" means that a Satellite transmits essential information, such as communication, research, and military orders. If a hacker gains access, then the hacker can steal data or harm satellite systems. This may lead to national security. For instance, an encrypted message can help attackers to track movements or change the outcome. "Spoofing sensitive information." Hackers can tamper with satellite signals to create confusion. Terrorist groups could use such tactics to cause harm, especially during an emergency. Satellites help run many services like GPS, the internet, and telecommunication. If a hacker turns off these systems through malware or other cyber attacks, it could lead to widespread problems like the GPS failing, which would affect planes and vehicles. It is known as "Disruption of essential Services". "Satellite used as Weapons." Think of an attacker taking complete control of a satellite. What will happen? It could be hazardous. It is the worst situation. They could change its orbit, causing it to crash into another satellite or even fall to earth, which may also damage other space missions. If a satellite has equipment like a camera and lasers, a hacker might use it for spying on ground targets. Satellites are used to monitor climate change and help during natural disasters. If hackers damage or turn off satellites, the response from the satellite might be delayed. And it could lead to "Environmental and Humanitarian Harm" because this research can also be lost, and the global problem would become challenging to manage.[5]

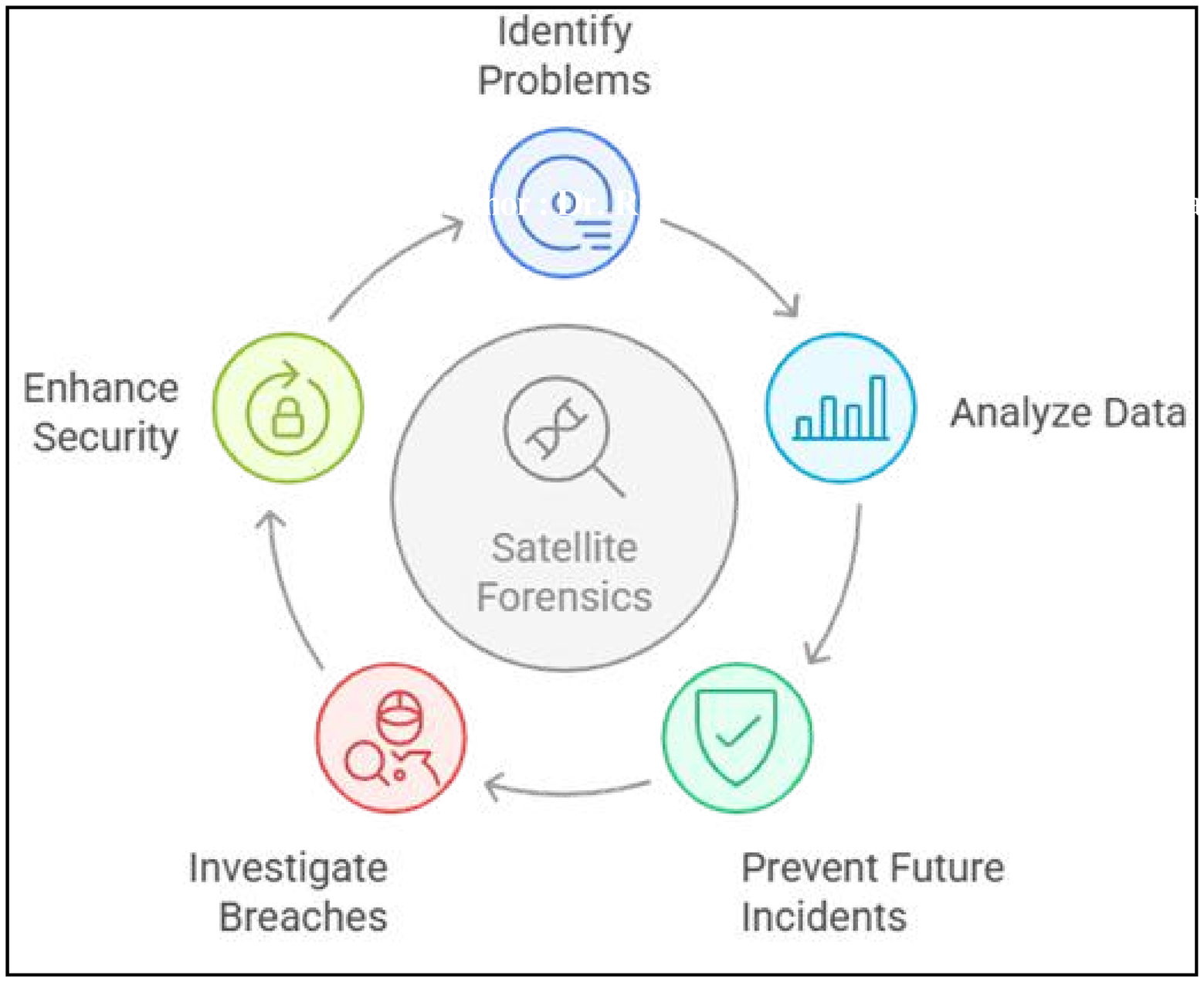


Fig :Consequences of Cyber Attacks on Satellite

Digital Detectives: Forensic Techniques in Satellite Security

Satellites are becoming more and more important nowadays, which is why the need for space focuses on cybersecurity goals. Satellite forensics helps investigators to find out the problems with the satellite. Satellites are part of systems like communication, navigation, and weather monitoring. Satellite forensics can help to discover the problem and how to prevent it from happening again. Satellites handle a significant amount of sensitive data. If a hacker tries to steal or harm sensitive data of a satellite, forensic techniques and tools can help identify who did this and how the breach happened. Some tools are also used for analyze satellite like log file analysis:- that analyze logs from ground station and satellite systems, anomaly detection:- Identifies unusual behaviour in satellite systems, memory dump and firmware analysis:- extracts and inspects firmware and onboard software for sign of tempering, communication traffic analysis:- monitors data sent between the satellite and Earth, timeline reconstruction:- Rebuilds a timeline of events before and after the incident, signal forensics and integrity verification:- Investigates radio frequency anomalies or interference etc.[6]

Enhancing Cybersecurity in Satellite:

Enhancing cybersecurity in satellite is crucial. To protect satellites from threats, it is essential to adopt strong cybersecurity methods. There are some ways to enhance cybersecurity. Space organizations must use encryption to protect data from hackers. New encryption techniques are used to encrypt data, which can help to defend against cyber attacks by computers. This method of enhancing cybersecurity is known as “Advanced Encryption”; “Zero Trust Security” models assume that no device should be trusted. Even if it's inside the network. The use of multi-factor authentication and access controls helps to keep the satellite safe from unauthorized access and also ensures confidentiality. Organizations such as NASA and the U.S. Space Force are working to create standard cybersecurity rules for space activities this aims to protect satellites from cyber threats. “Backup Systems” ensure that if a satellite or communication channel is attacked or fails, another can take over. This makes the space system stronger and reduces the damage from cyberattacks. [7]

Case study: Russia's satellite attack on Ukraine – 2022

During the Russia–Ukraine conflict, in February 2022, a cyber attack disrupted satellite communication in Ukraine. This becomes serious cyber incidents in the war, which affects both government and military systems. A company, Viasat, provides internet through satellite. It was targeted. Many customers had to replace their modems because of damage during this cyber incident. The attack destroyed devices used by customers, and it caused service issues. Russian hackers also targeted another satellite-based internet provider. However, internet provider Starlink responded quickly by updating its software and making the attack less practical. Starlink's response to cyber threats is effective in preventing damage. In 2023, during Ukraine's counter-offensive, it was discovered that Russian attackers tried to install spyware on satellite services. Ukraine's security forces managed to thwart some of these attacks, but some devices had been compromised. [8]

The future of Space cybersecurity:

Space is becoming more connected to the internet. Many satellites can be accessed online, which creates many risks. "Attackers could start scanning for internet-connected satellites or even set up rogue ground stations to exploit vulnerabilities". Artificial Intelligence is becoming a powerful tool in cybersecurity. "We are seeing a shift towards self-healing constellations where satellites can detect and neutralize threats autonomously and also share these with neighboring satellites that they trust. This could be a game-changer in mitigating cyberattacks in space and is the only way to respond fast enough to cyberattacks." New technology uses "optical links" between satellite ground stations. This link offeres faster data speed and stable connection. "With satellites continuously connected, we must rethink how we secure data transmission, and protect against cyber threats in real time." Cybersecurity in space is not just a technical challenge; it's a policy and governance issue. We need a joint effort between governments, industry, and academia to establish security standards for the space age.[9]

CONCLUSION

1.What Is a Satellite? (Grades K-4) - NASA. https://www.nasa.gov/learning-resources/for-kids-and-students/what-is-a-satellite-grades-
(28 June 2025, date last accessed).

2.Satellite communication Orbit, Signals, Relay Britannica.
https://www.britannica.com/technology/satellite-communication/How-satellites-work
(28 June 2025, date last accessed).

3.What is Satellite Hacking & How Can It Be Prevented? NI.
https://www.ni.com/en/solutions/aerospace-defense/space-launch-exploration/what-is-satellite-hacking.html
(28 June 2025, date last accessed).

4.Cybersecurity Risks in Satellite-based Internet Services: Protecting Global Connectivity
by RocketMe Up Cybersecurity Medium
https://medium.com/@RocketMeUpCybersecurity/cybersecurity-risks-in-satellite
(28 June 2025, date last accessed).

5.The Dangers of Cyber Attacks on Satellites and Potential Threat Actors
https://www.thesign.media/blog/the-dangers-of-cyber-attacks-on-satellites-and-potential-threat-actors
(28 June 2025, date last accessed).

6.Understanding Digital Forensics: Process, Techniques, and Tools.
https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics- process-techniques-and-tools/
(28 June 2025, date last accessed).

7.Cybersecurity in Space: Protecting Space Missions from Threats ECCU.
https://www.eccu.edu/blog/the-future-of-cybersecurity-in-space-securing-satellites-and-space-missions
(28 June 2025, date last accessed).

8.Satellite Hacking: How Russia Knocked out the ViaSat System at the Outset of the Ukraine War - Hackers Arise.
https://hackers-arise.com/satellite-hacking-how-russia-knocked-out-the-viasat-system-at-the-outset-of-the-ukraine-war/
(28 June 2025, date last accessed).

9.The Future of Space and Cybersecurity: An Integrated Outlook.
https://www.linkedin.com/pulse/future-space-cybersecurity-integrated-outlook-john-wensveen-phd--avfm
(28 June 2025, date last accessed).

ABOUT THE AUTHORS



Princy Nitin Kumar Soni

Student, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, India



Kiran Dodiya

Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA



Dr. Kapil Kumar

Coordinator, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA



MALICIOUS KEYLOGGER DETECTION

Author: Dr. Sabitha Bau A, Nandhini S.

Abstract

This article presents a practical study on the simulation and forensic analysis of keylogger-based malware using a controlled virtual environment. The work was carried out in Kali Linux within Oracle VirtualBox, where a Python program was designed to imitate the behaviour of malicious keyloggers. To evaluate detection techniques, three approaches were implemented: signature-based detection, heuristic analysis, and machine learning models. The experimental results showed that traditional methods such as signature and heuristic detection were effective in identifying the simulated malware, while the machine learning model required further training to improve accuracy.

This article presents a practical study on the simulation and forensic analysis of keylogger-based malware using a controlled virtual environment. The work was carried out in Kali Linux within Oracle VirtualBox, where a Python program was designed to imitate the behaviour of malicious keyloggers. To evaluate detection techniques, three approaches were implemented: signature-based detection, heuristic analysis, and machine learning models. The experimental results showed that traditional methods such as signature and heuristic detection were effective in identifying the simulated malware, while the machine learning model required further training to improve accuracy.

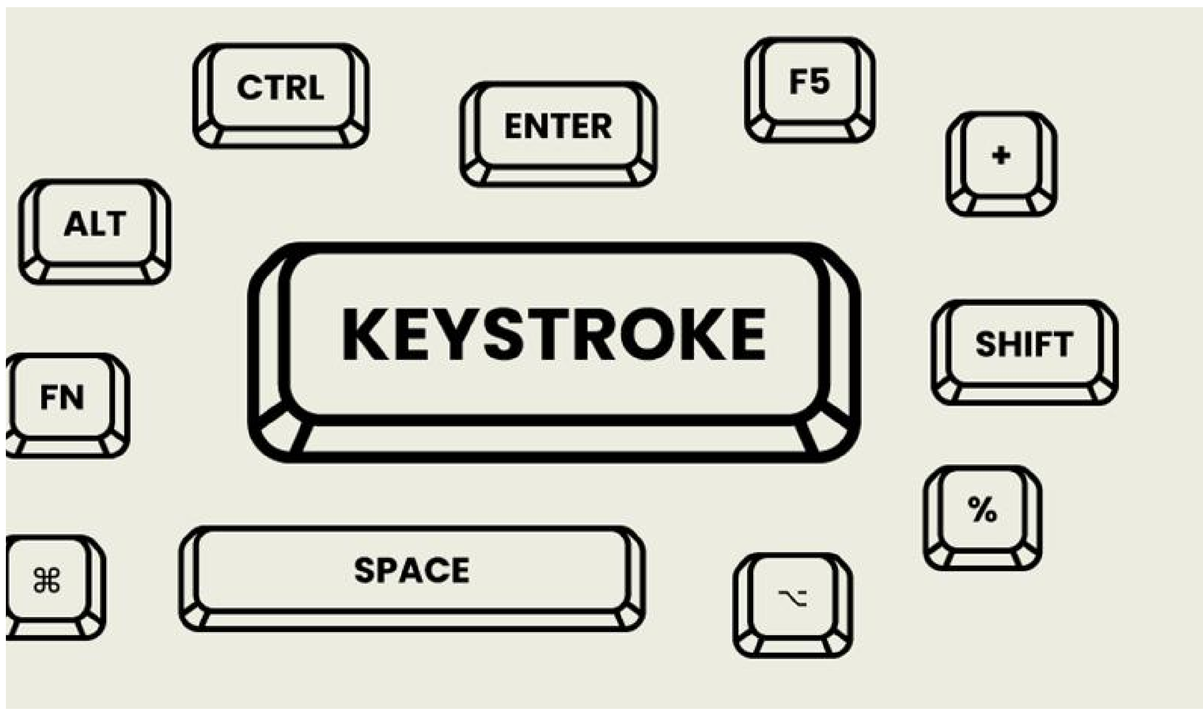
The article emphasizes the importance of integrating forensic practices with malware detection to strengthen cybersecurity defence. By combining traditional and modern approaches, the study demonstrates how forensic analysis can support proactive threat identification and incident response. This research offers a foundation for future development of intelligent detection frameworks capable of addressing advanced and evolving cyber threats.

Introduction:

The rapid growth of digital technologies has created immense opportunities for communication, commerce, and information sharing. At the same time, it has also increased exposure to sophisticated cyber threats. Among the wide range of malicious software, keyloggers have emerged as one of the most dangerous and invasive tools used by attackers.

T A keylogger operates by secretly recording user keystrokes, thereby stealing sensitive information such as login credentials, banking details, or personal messages without the victim's awareness. This makes keyloggers particularly difficult to detect and highlights the importance of developing strong methods for malware analysis and forensic investigation.

Traditional malware detection techniques such as signature-based scanning are effective in identifying known threats. These approaches rely on matching suspicious files against a database of previously recorded malware signatures. However, as cybercriminals continue to evolve their techniques, relying solely on signature detection is no longer sufficient. In response, heuristic analysis has been introduced, which inspects behavioural characteristics of files, such as unusual file size, suspicious code patterns, or abnormal execution processes. While more flexible than signature-based methods, heuristic detection still faces challenges in identifying highly obfuscated or newly emerging malware.



To address these limitations, machine learning (ML) models are increasingly being explored for malware detection. Unlike traditional approaches, ML techniques have the ability to learn from data, recognize hidden patterns, and adapt to previously unseen threats. However, their effectiveness depends on the quality and quantity of training data, as well as the continuous refinement of algorithms. In practice, machine learning–based detection must be complemented with established methods to achieve comprehensive results.

To address these limitations, machine learning (ML) models are increasingly being explored for malware detection. Unlike traditional approaches, ML techniques have the ability to learn from data, recognize hidden patterns, and adapt to previously unseen threats. However, their effectiveness depends on the quality and quantity of training data, as well as the continuous refinement of algorithms. In practice, machine learning–based detection must be complemented with established methods to achieve comprehensive results.

LITERATURE SURVEY

1.Detecting Malicious Keylogger Activities using API Monitoring (2005)
In 2005, Smith and colleagues studied how malicious keyloggers exploit Windows
API calls to capture user keystrokes.
Their research analysed suspicious function calls such as Geta sync Key State and Get Foreground Window to distinguish between normal applications and malware.
The study concluded that API-based monitoring could serve as an early warning system to detect hidden keyloggers.

2.Keystroke Dynamics for Intrusion Detection (2006)
In 2006, Chen and co-researchers explored behavioural biometrics to detect unauthorized keylogging.
They compared normal typing patterns with those intercepted by keyloggers, proving that timing-based features (latency, dwell time) could reveal malicious activity.
Their findings suggested that keystroke dynamics could complement traditional malware detection approaches.

3.Kernel Hook and Driver-Level Keylogger Detection (2007)
In 2007, Patel and his team investigated rootkit-style keyloggers that operate at the kernel level.
Their work emphasized how monitoring system service dispatch tables and driver hooks can reveal hidden logging behaviour.
They concluded that kernel integrity checks are essential for detecting low-level keyloggers.

4.Behavioural Heuristics for Keylogger Identification (2008)
In 2008, Davis and colleagues focused on building heuristic models to detect common behaviours of keyloggers.
They studied persistence methods, suspicious file creation, and repeated access to keyboard Apis. Their approach demonstrated that behaviour-based analysis could complement signature-based techniques.

5.Sandboxing and Dynamic Analysis of Keyloggers (2009)
In 2009, Ahmed and team analysed the use of sandbox environments to study malicious keylogger behaviour executing suspicious software inside virtualized systems.
They were able to monitor runtime actions such as keystroke capture and log transmission.
Their research showed that dynamic analysis is effective in identifying unknown variants of keyloggers.

6.Statistical Timing and Context Analysis (2010)
In 2010, Kumar and colleagues proposed timing-based analysis to detect keyloggers.
They correlated keystroke capture with active applications and found inconsistencies when keyloggers collected data from inactive windows.
Their study highlighted the effectiveness of context-based detection mechanisms.

7.Detecting Exfiltration of Keystroke Logs (2011)
In 2011, Brown and researchers studied the communication channels used by keyloggers to send stolen information.
They identified common patterns in data exfiltration through HTTP, FTP, and email protocols.
The findings suggested that monitoring outbound traffic could expose hidden keyloggers.

8. Registry and Persistence Mechanism Analysis (2012)
In 2012, Singh and his research group investigated how keyloggers maintain persistence in operating systems.
They analysed registry modifications, startup folder entries, and scheduled tasks that ensured malware execution after reboot.
Their study concluded that system state monitoring is crucial in identifying persistent keyloggers.

9. Browser Form-Grabbing Detection (2013)
In 2013, Miller and team examined advanced keyloggers that targeted web browsers to steal credentials.
They studied how malicious software hooked into browser processes to capture form inputs before encryption. Their work emphasized the importance of browser integrity monitoring to prevent credential theft.

10. Machine Learning for Host-Based Keylogger Detection (2014)
In 2014, Johnson and colleagues applied machine learning models to classify malicious keylogger activities.
They trained classifiers on features such as API call frequency, memory usage, and process behaviour's.

The results showed that supervised learning improved accuracy compared to traditional detection methods.send

11. Feature Engineering for Enhanced Keylogger Identification (2015)
In 2015, Gupta and co-researchers developed specialized features for keylogger detection .They focused on metrics such as keyboard buffer access, clipboard interaction, and abnormal DLL injections.
Their research highlighted that carefully designed features can significantly improve detection performance.
\

12. Deep Learning Approaches for Sequence Detection (2016)
In 2016, Wang and his team introduced deep learning to detect malicious keyloggers.
They used recurrent neural networks to model API call sequences and identify suspicious logging patterns .
The study showed that deep learning can automatically learn hidden features that distinguish malware from benign software.

13. Adversarial Evasion and Detection Robustness (2017)
In 2017, Thomas and colleagues explored how keyloggers attempt to evade detection by mimicking normal processes.
They proposed ensemble learning models that combined multiple classifiers to resist evasion techniques.
Their results demonstrated that multi-layer detection frameworks improve robustness.

14. Memory Forensics for Keylogger Detection (2018)
In 2018, Li and researchers applied memory forensic analysis to identify keyloggers operating in volatile memory.
They examined hidden threads, injected code, and API hooks in RAM snapshots.
Their study concluded that memory forensics provides strong evidence against stealthy keyloggers.

15.Mobile Keylogger Detection Techniques (2019)
In 2019, Rao and his team studied the growing issue of mobile keyloggers on Android devices.
They investigated misuse of accessibility services and overlay attacks that captured user inputs.
Their research suggested that permission analysis and runtime monitoring are effective for detecting mobile threats.

PROPOSED METHODOLOGY

The methodology adopted in this project is designed to create a safe yet realistic simulation of malware behaviour through the controlled injection of a fake keylogger. The objective is not to cause damage but to provide a structured environment where malware-like activities can be observed, logged, and analysed in order to strengthen forensic investigations. A virtual machine environment is selected for the experiment to ensure that the simulation is isolated, secure, and repeatable. Using this setup, a keylogger program is developed that mimics the core actions of malicious software by capturing keystrokes and generating suspicious events, while deliberately excluding harmful functions such as data exfiltration or unauthorized privilege escalation.
This logging mechanism is designed to capture a wide range of details, including user keystrokes, event timestamps, operating system version, and IP address information. By enriching the log with contextual system data, the methodology ensures that investigators have sufficient information to reconstruct events and validate the authenticity of captured evidence. The logging framework follows a structured format so that the data remains organized and accessible during analysis.

PROPOSED SYSTEM

The methodology consists of five key steps:

Step1: Malware Injection – A fake keylogger is safely injected into the virtual system to simulate malicious activity.
Step2: Activity Monitoring – The keylogger generates keystroke events which are continuously captured.
Step3 :Forensic Logging – Each event is recorded in a structured log file with details like time, OS information, and IP address.
Step4: Hash Protection – Every log entry is secured using SHA-256 hashing to ensure integrity and prevent tampering.
Step5: Detection Process – The system checks for abnormal keystroke patterns and flags suspicious activity.

FEATURE EXTRACTION & PREPROCESSING

"The system refines raw keylogger data by removing noise, extracting key attributes (time, keys, OS, IP, hash), and structuring them into a clean dataset for accurate forensic detection."

A systematic process for refining raw keylogger data into a clean, structured dataset suitable for forensic analysis, aiming for accurate detection of malicious activities. This process can be broken down into several key stages:

1. Signature-based detection – to catch known malware by matching it with existing patterns (like known keylogging functions or file names).
2. Heuristic analysis – to detect suspicious behaviour (like hidden logging or sending keystrokes to unknown servers), even if it's a new or modified malware.
3. Machine learning – to train a model using features from both normal and malicious programs, helping to predict and identify unknown keylogger-based malware."

Raw Keystroke Data: This is the initial input, representing the unprocessed keystroke information captured by a keylogger. This data typically contains various attributes, including the keys pressed, associated timestamps, and potentially other system-level details.

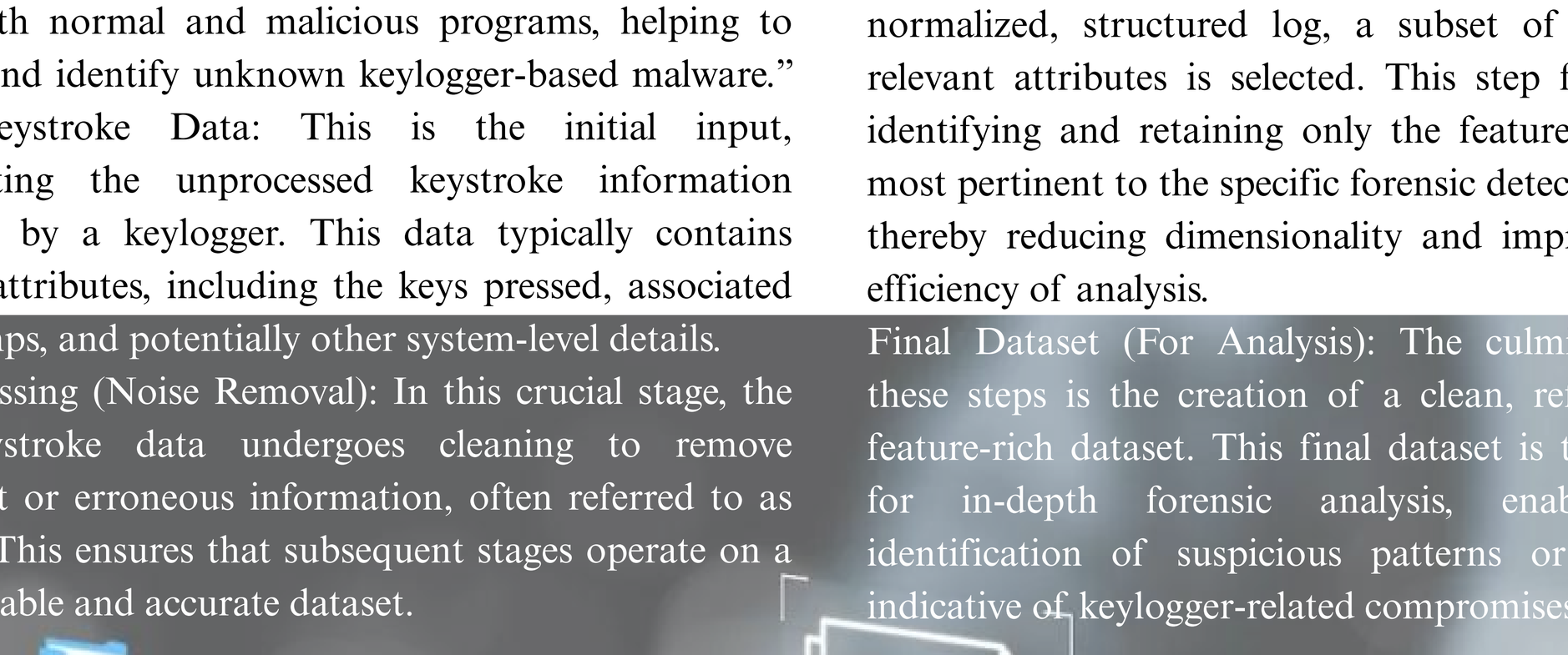
Preprocessing (Noise Removal): In this crucial stage, the raw keystroke data undergoes cleaning to remove irrelevant or erroneous information, often referred to as "noise." This ensures that subsequent stages operate on a more reliable and accurate dataset.

Feature Extraction: Following noise removal, key attributes are extracted from the pre-processed data. These features are essential for forensic analysis and include elements such as the time of the keystroke, the specific keys pressed, the operating system (OS) in use, the IP address, and potentially a hash of the data for integrity verification. The frequency of certain keystrokes or patterns might also be extracted here.

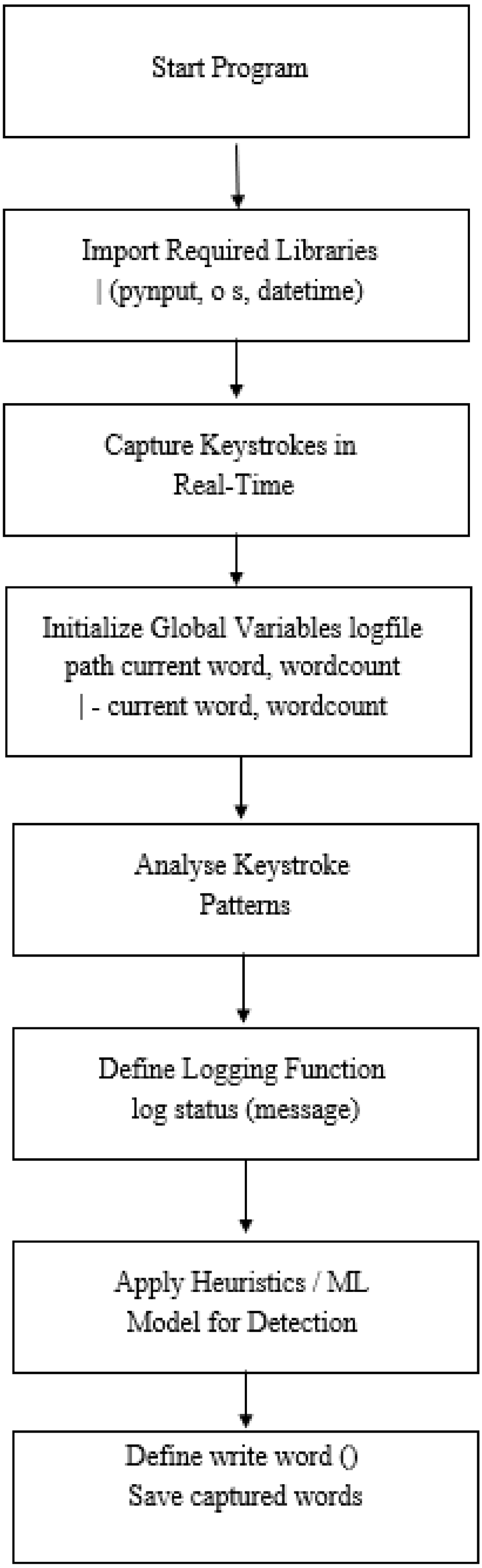
Normalization (Structured Log): The extracted features are then normalized and organized into a structured log format. This standardization ensures consistency and facilitates easier analysis by presenting the data in a uniform and manageable layout.

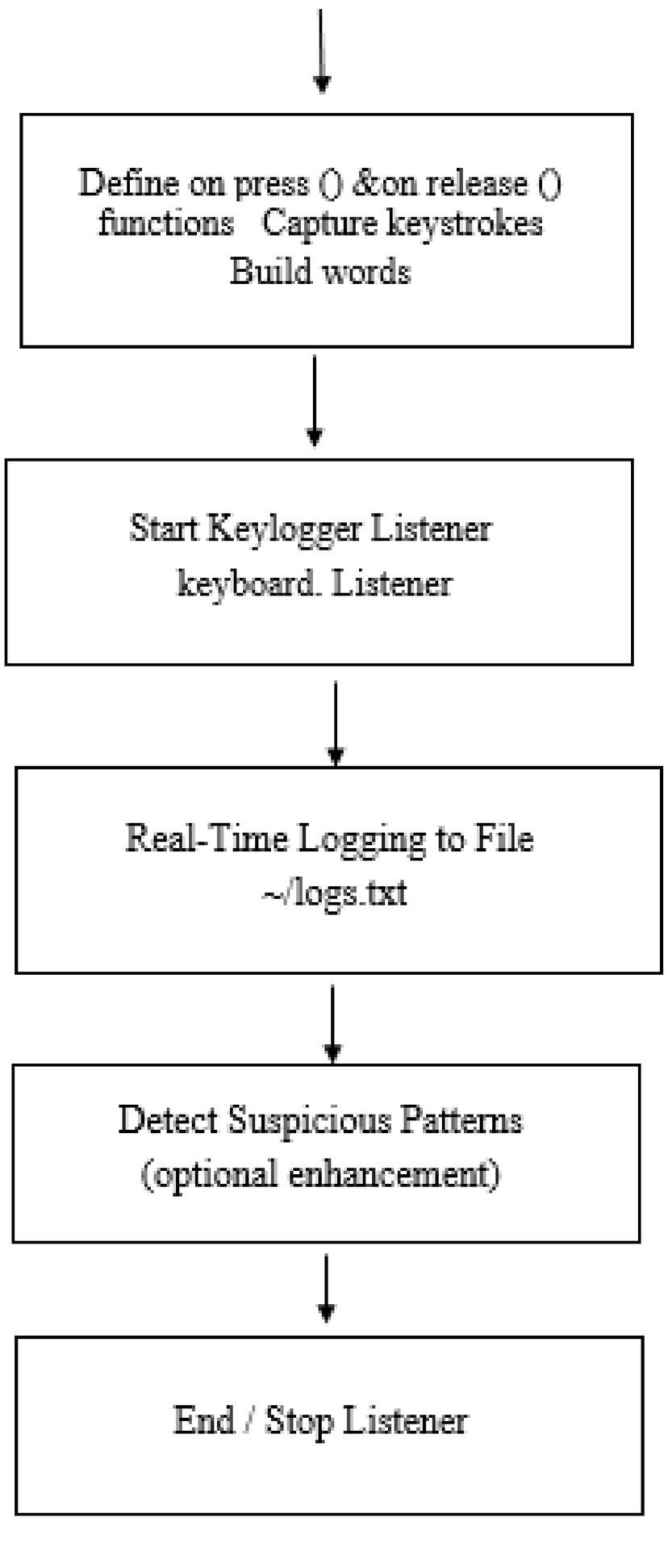
Feature Selection (Relevant Attributes): From the normalized, structured log, a subset of the most relevant attributes is selected. This step focuses on identifying and retaining only the features that are most pertinent to the specific forensic detection goals, thereby reducing dimensionality and improving the efficiency of analysis.

Final Dataset (For Analysis): The culmination of these steps is the creation of a clean, refined, and feature-rich dataset. This final dataset is then ready for in-depth forensic analysis, enabling the identification of suspicious patterns or activities indicative of keylogger-related compromises.



METHODOLOGY WORKFLOW





WORK FLOW EXPLANATION

[Keyboard Event]
↓ (user presses a key)
[OS Kernel]
↓ (event delivered via API/hooks)
[Keylogger Hook/API Listener]
•Hooks into keyboard events (e.g., using pynput, Win API hooks, kernel/filter drivers)
•Captures each keypress
[Buffer Module]
•Stores keystrokes in memory/log buffer
[Storage & Exfiltration]
•Periodically saves to a log file
•Optionally sends via email or C&C server.
Event Interception
•On Windows, key loggers often use Set Windows

•Hooks into keyboard events (e.g., using pynput, Win API hooks, kernel/filter drivers)
•Captures each keypress
[Buffer Module]
•Stores keystrokes in memory/log buffer
[Storage & Exfiltration]
•Periodically saves to a log file
•Optionally sends via email or C&C server.
Event Interception
•On Windows, key loggers often use Set Windows Hook Ex() or py Hook to intercept WM_KEYDOWN .
•On Linux, tools like python put or keyboard module hook into the input API to catch keypresses.
Listener/Handler
•A listener callback (e.g., on _press, on _release) fires whenever a key is pressed or released.
Buffering & Logging
•The captured keystroke is added to an in-memory list or string buffer.
•After reaching a threshold (e.g., newline or time interval), the buffer is flushed to a file (e.g., log.txt) or sent remotely

This project demonstrates a real-time keylogger developed using the pynput library in Python. It captures user input, processes keystrokes, builds complete words, and logs them into a file for later analysis. The program follows a modular workflow with key methods that handle specific responsibilities.

The process begins by initializing the environment. A log file path (~/logs.txt) is defined using so. path .expand user, ensuring that logs are stored in the user's home directory. Two key variables are also initialized: current word, a list to temporarily store typed characters, and wordcount, which keeps track of how many words have been logged.

The log status() method is responsible for printing timestamped status messages to the terminal. This is used to indicate when the keylogger starts, stops, or encounters an error, helping in debugging or monitoring.

The write word() method is used to convert characters into words and write them into the log file. It checks whether the current word list contains any characters. If it does, it joins them into a single string (word), appends it to the log file, and then clears the list. If a newline is needed (such as after pressing the Enter key), it adds a newline instead of a space.The core of the keylogging functionality is handled in the on press() method. This function reacts to each key press event. If the key contains a character (char), it is added to the current word. Special keys are handled differently:

pressing space, enter, or tab triggers write word() to store the word; backspace removes the last character from current word; and pressing the Escape (Esc) key stops the listener and exits the program. Any exceptions are caught and logged using log status().

The main() function acts as the program entry point. It starts by logging a message that the keylogger has started. It then launches a keyboard. Listener which listens to all keypresses and sends them to the on press() handler. The listener runs continuously until the Escape key is pressed, after which a summary message logs the total number of words captured.

This structured workflow highlights how simple Python tools and libraries like pinout can be used to capture and store keystrokes efficiently. While this implementation is educational, it is important to emphasize that keyloggers must only be used in ethical, legal, and authorized scenarios to avoid serious privacy violations.

BENEFITS

- Machine learning can identify complex malware patterns that traditional signature based methods miss, including zero-day attacks.
- Simulation allows for safe analysis of malware behaviour, identifying its tactics and techniques without risking real-world infection.
- The framework can be updated to detect new malware variations and adapt to evolving threats.
- Simulation helps identify vulnerabilities and potential attack vectors, allowing for proactive security measures.
- The framework can be designed to detect and respond to threats in real-time, minimizing the impact of attacks.



LIMITATIONS

- Does not include real-time keylogger detection capabilities.
- Logs keystrokes in plain text without encryption or security.
- No graphical user interface (GUI); command-line only.
- Works only while script is running; no auto-start or background service.
- Depends on pynput, which may not work consistently across all platforms.
- No filtering of sensitive input (e.g., passwords); logs all keystrokes indiscriminately.
- No intelligent analysis or anomaly detection features.
- Limited error handling and no logging to external or secure storage.
- No user authentication or permission control to start/stop logging.
- Not suitable for production use or deployment in secure environments

KEY STROKE

A sophisticated malware simulation and detection framework aims to identify and categorize malicious software effectively, often by leveraging machine learning and dynamic analysis techniques. These frameworks address the challenges of evolving malware, data scarcity, and computational efficiency. Successful frameworks often demonstrate high accuracy in detection and categorization, and are designed to be adaptable to real-world scenarios, including high traffic environments

HOW ITS WORKING (Key Logger)

1.Mimicking a keylogger's behaviour maybe opening a file like a fake malware file.
2.Triggering simulated detection logic e.g., checking:

•Signature-based detection: Simulates antivirus signature matching.
•Heuristic checks: Possibly based on file size, name, or content.
•ML detection: Might involve a dummy classifier or hard coded logic.

So the script doesn't actually record keystrokes it pretends to run a key logger and triggers fake detection events to demonstrate how detection methods would flag it.

.

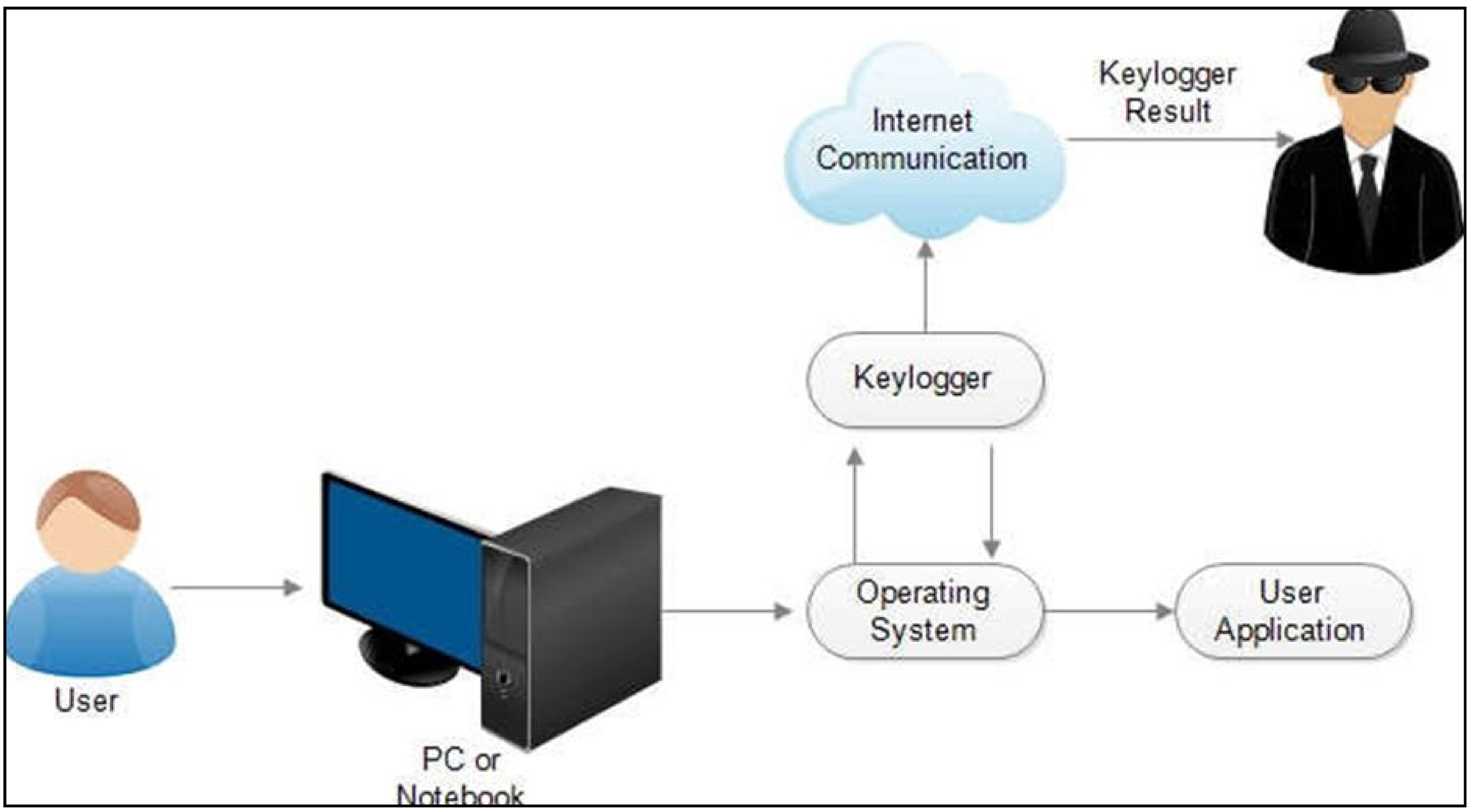


Fig. Once the keylogger collects this data, it transmits the logged keystrokes via internet communication to a remote attacker or hacker.

KEY LOGGER AND FORENSIC LOGS

A keylogger, short for keystroke logger is a type of surveillance tool that records every key pressed on a keyboard. It can be implemented either as software or hardware. While keyloggers are sometimes used for legitimate purposes, such as monitoring employee activity or troubleshooting, they are more often associated with malicious activities like password theft, identity fraud, and unauthorized system access.

Two Types of Keyloggers

Keyloggers can be broadly classified into two main categories:

1.Software Keyloggers

o Installed as programs that run in the background.
o Can capture keystrokes, screenshots, clipboard data, and even online activity.
o Examples: API-based loggers, kernel-level loggers, browser-based loggers.

2.Hardware Keyloggers

o Physical devices attached to a computer or keyboard.
o Record keystrokes without needing any software installation.
o Examples: USB keyloggers, wireless keyboard sniffers, firmware-based loggers.

Forensic Analysis

Once features are extracted, investigators can analyse them to identify anomalies
User Profiling: Keystroke dynamics are unique to each person, enabling identity verification. Intrusion Detection: Sudden irregular typing patterns or unknown IP addresses may indicate compromise.
Data Integrity Check: Hash comparisons confirm whether logs were altered.

Step1: This configuration shows a moderate setup of a Kali Linux virtual machine within VirtualBox. The VM is allocated 2 GB RAM, 25 GB storage, basic display settings, and bridged networking for full internet connectivity. Such a setup is well-suited for penetration testing, system analysis, and cybersecurity research without affecting the host operating system

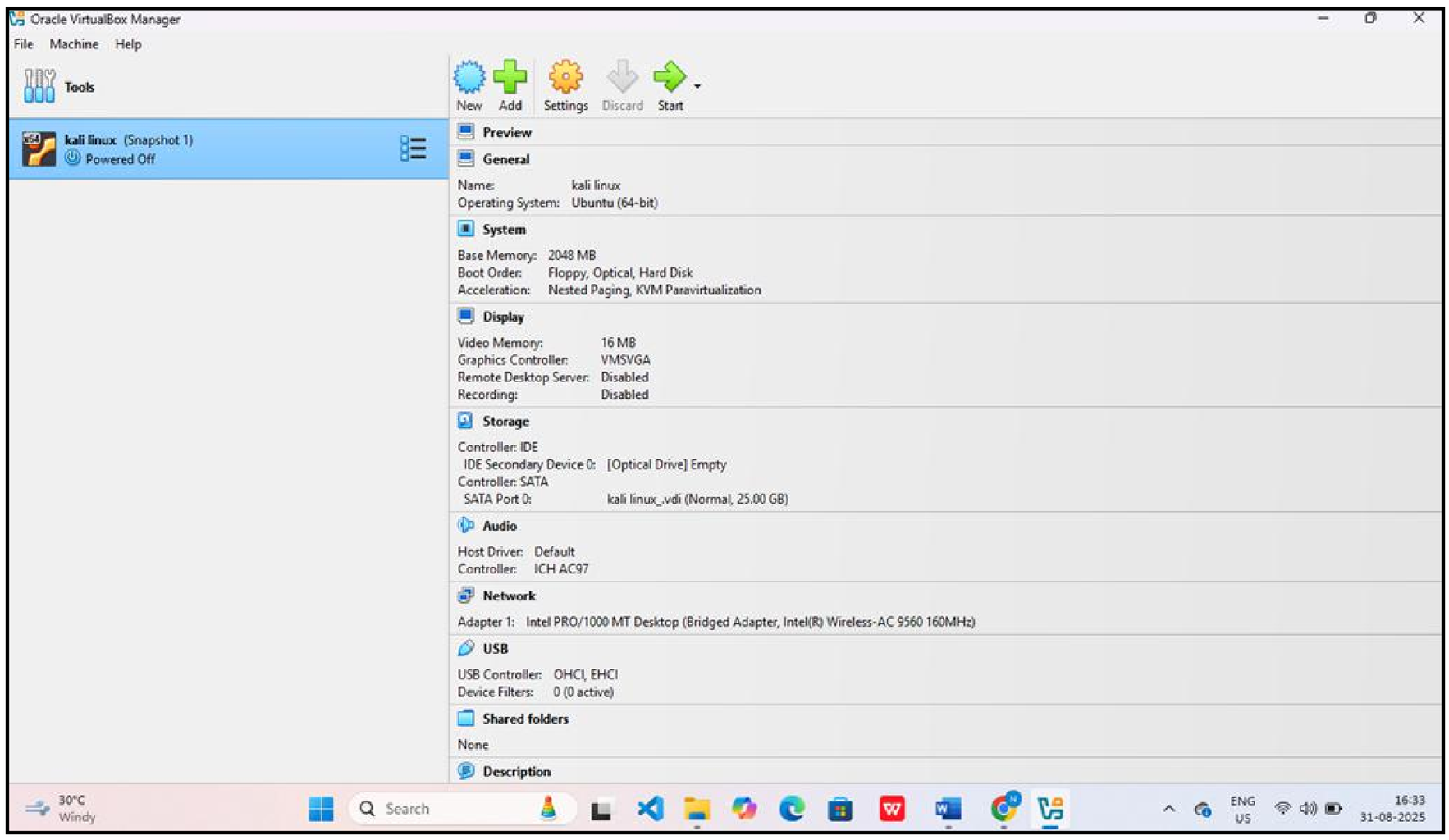


Fig. The Oracle VM VirtualBox Manager, a platform used to create and manage virtual machines

Step 2: Kali Linux is a special version of the Linux operating system that is mainly used for cybersecurity and digital forensics. Unlike normal Linux distributions that focus on daily use like browsing or office work, Kali is built for security testing, ethical hacking, and investigation of cybercrimes. It was developed by Offensive Security and is free for anyone to use.

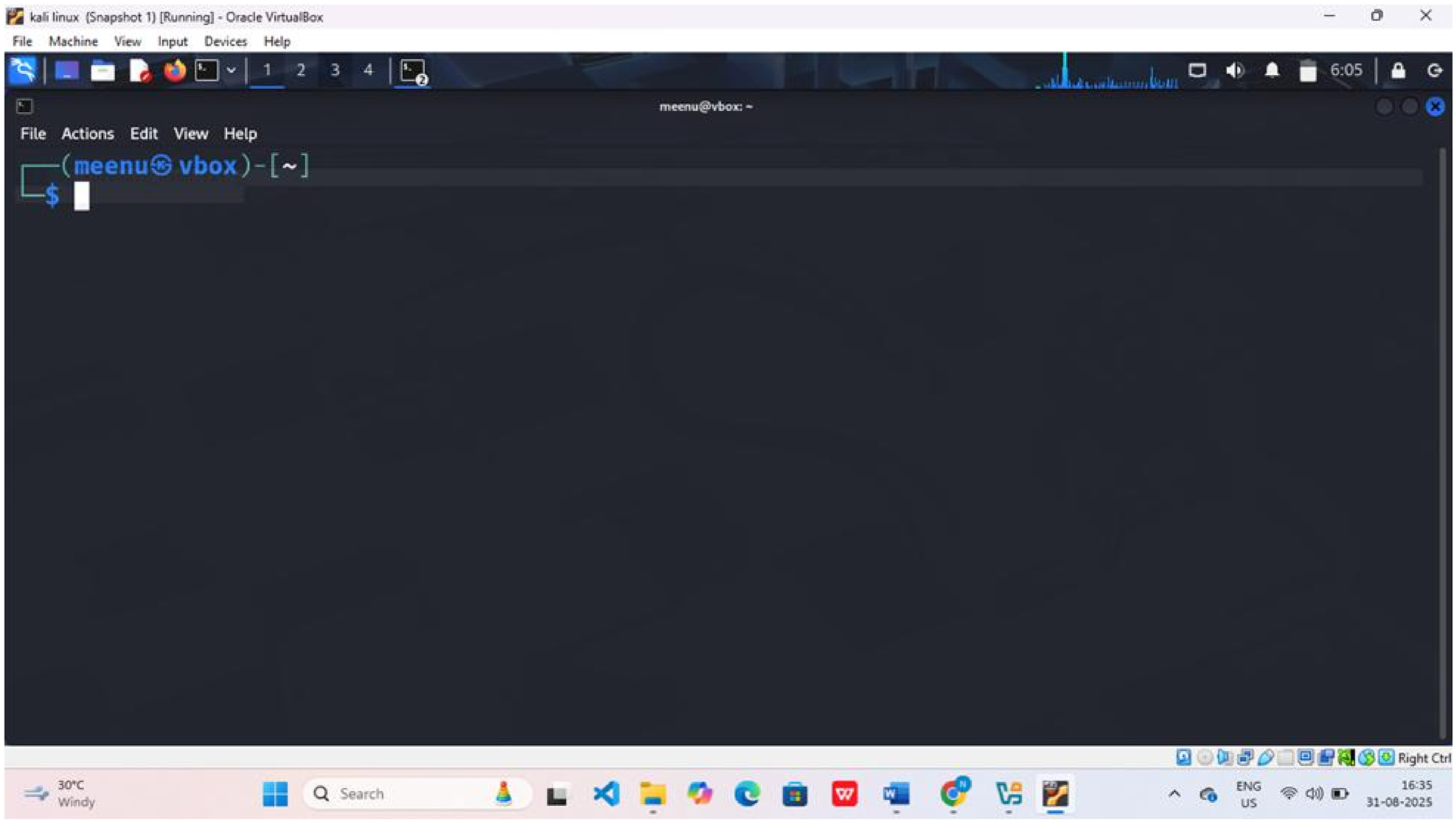


Fig: Kali Linux is a security-focused operating system designed for ethical hacking, penetration testing, and digital forensics.

Uses of Kali Linux

Kali Linux is used in many areas of cybersecurity, such as:
Penetration testing – testing systems and networks for weaknesses.
Network scanning – finding devices and analysing their security.
Password auditing – checking password strength and recovering lost passwords.
Wi-Fi security testing – analysing and securing wireless networks.
Digital forensics – investigating digital evidence in cybercrime cases.
Reverse engineering – studying malware or suspicious software.

Step 3: Create the key logger malware in kali Linux
The terminal output shows pynput and its dependencies (six, evade, python-glib) are already installed in the virtual environment. Keylogger started. Logging to /home/Meenu/logs.txt" .This means the keylogger is actively capturing keystrokes and writing them to the logs.txt file



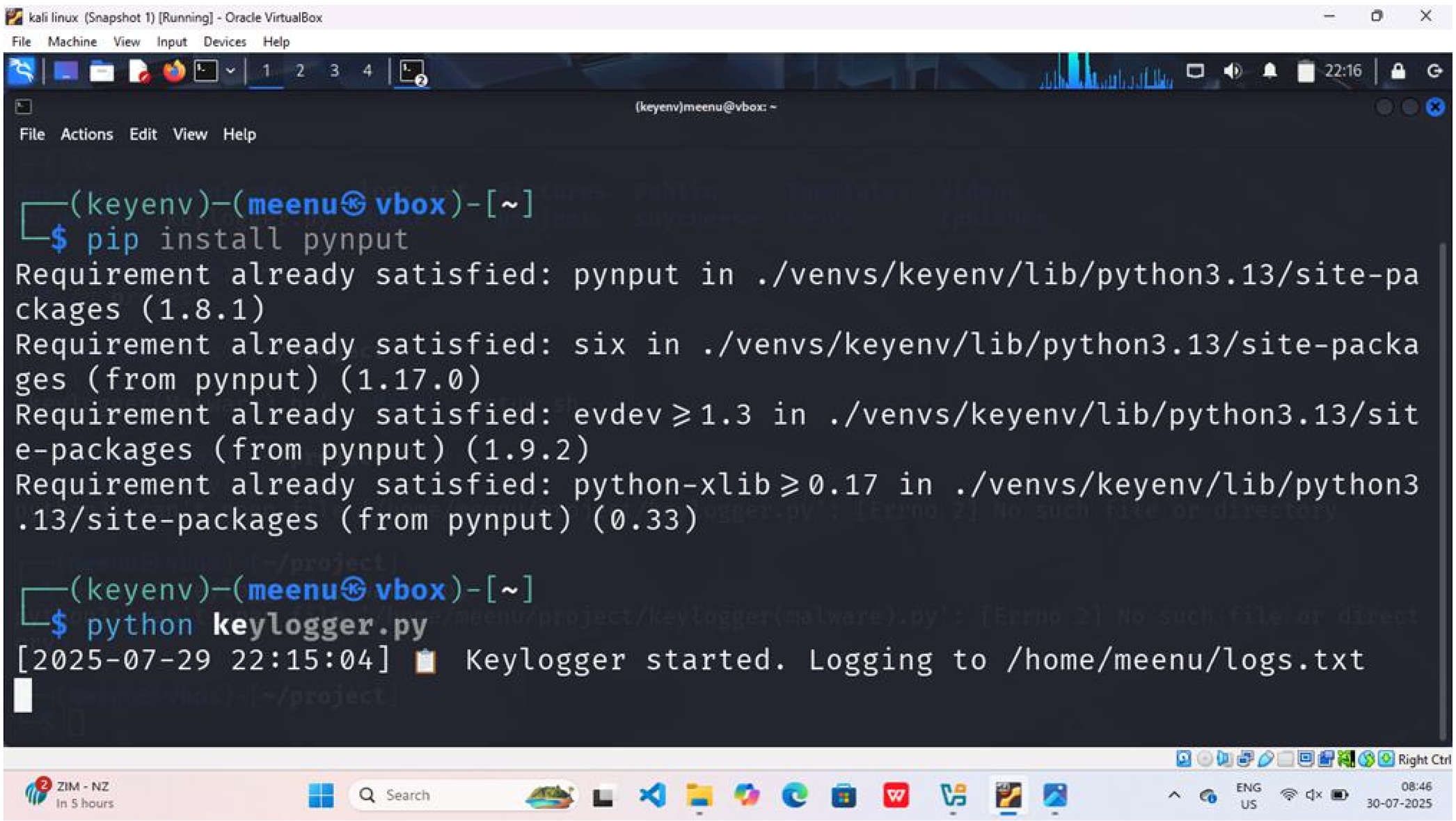


Fig . keylogger setup and execution in Kali Linux using Python and the pynput library within a virtual environment (keying), likely running on Oracle VirtualBox.

Step 4: Running the malware comparison

Kali comes with tools like Wireshark, Metasploit, and pynput-compatible environments that are useful for testing and analysing keylogger behaviour. Keyloggers are typically tested as part of penetration testing exercises to simulate real world attacks and evaluate system defences.

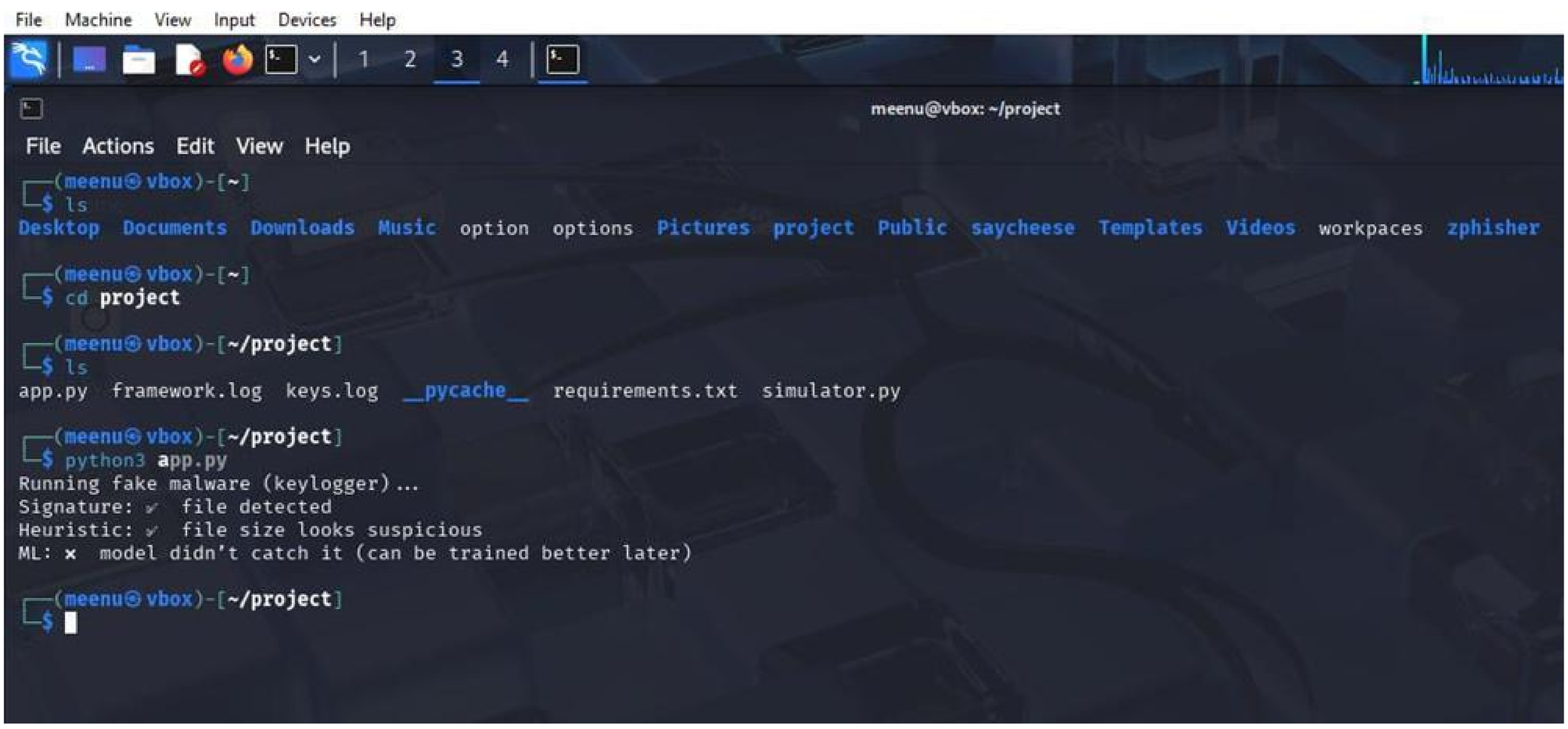


Fig: Signature-based detection – to catch known malware by matching it with existing patterns (like known keylogging functions or file names)

Heuristic analysis – to detect suspicious behaviour (like hidden logging or sending keystrokes to unknown servers), even if it's a new or modified malware.

Machine learning – to train a model using features from both normal and malicious programs, helping to predict and identify unknown keylogger-based malware.

Step 5: "Implementation and Analysis of a Python-Based Keylogger in Kali Linux for Ethical Penetration Testing"

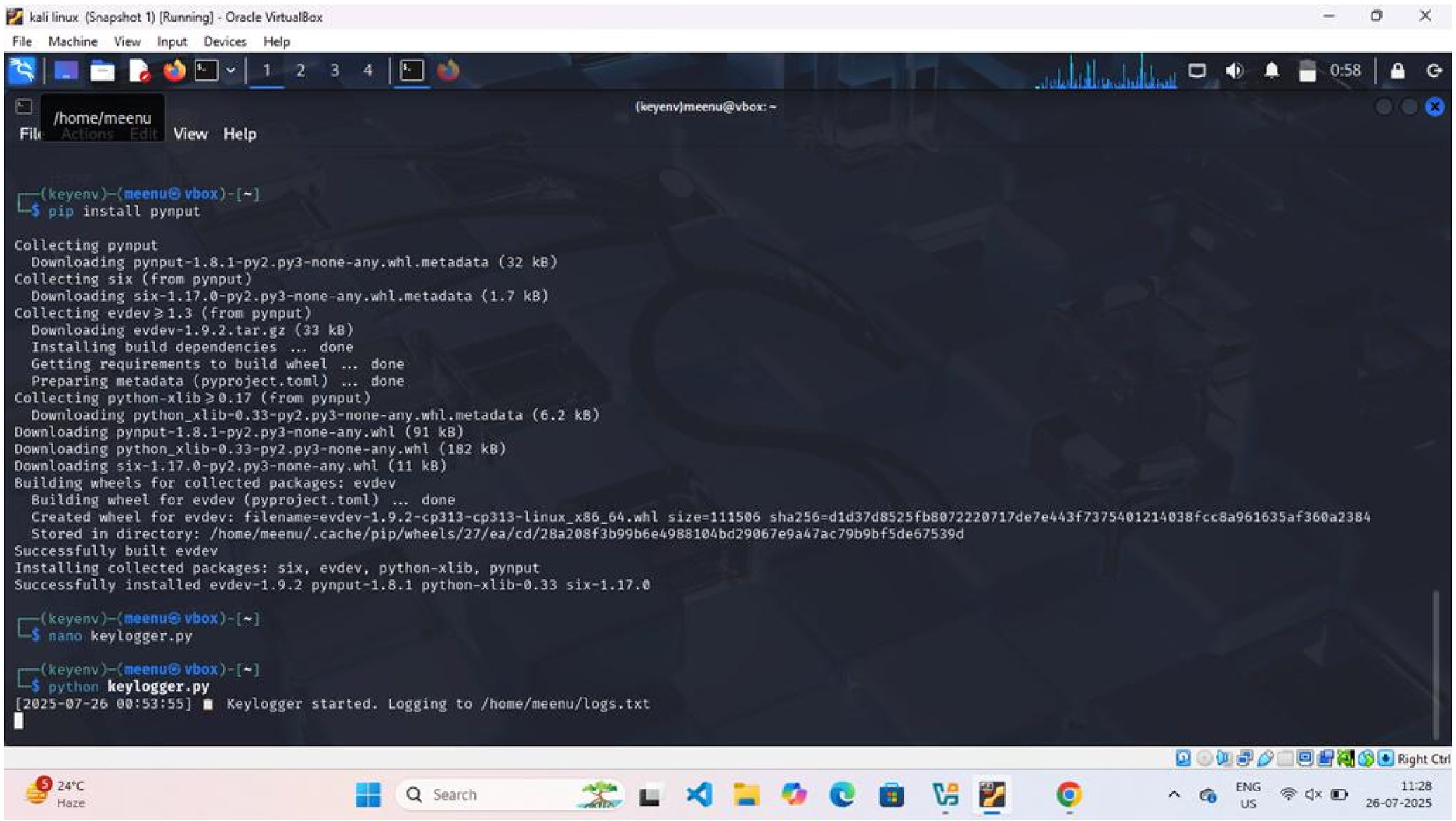


Fig : Uses the pynput. keyboard listener. Captures keystrokes in real time.

Step 6: A digital forensics process involving the recording of user input (keystrokes) and the detection of malicious files, simulating a scenario for a cybersecurity or digital forensics

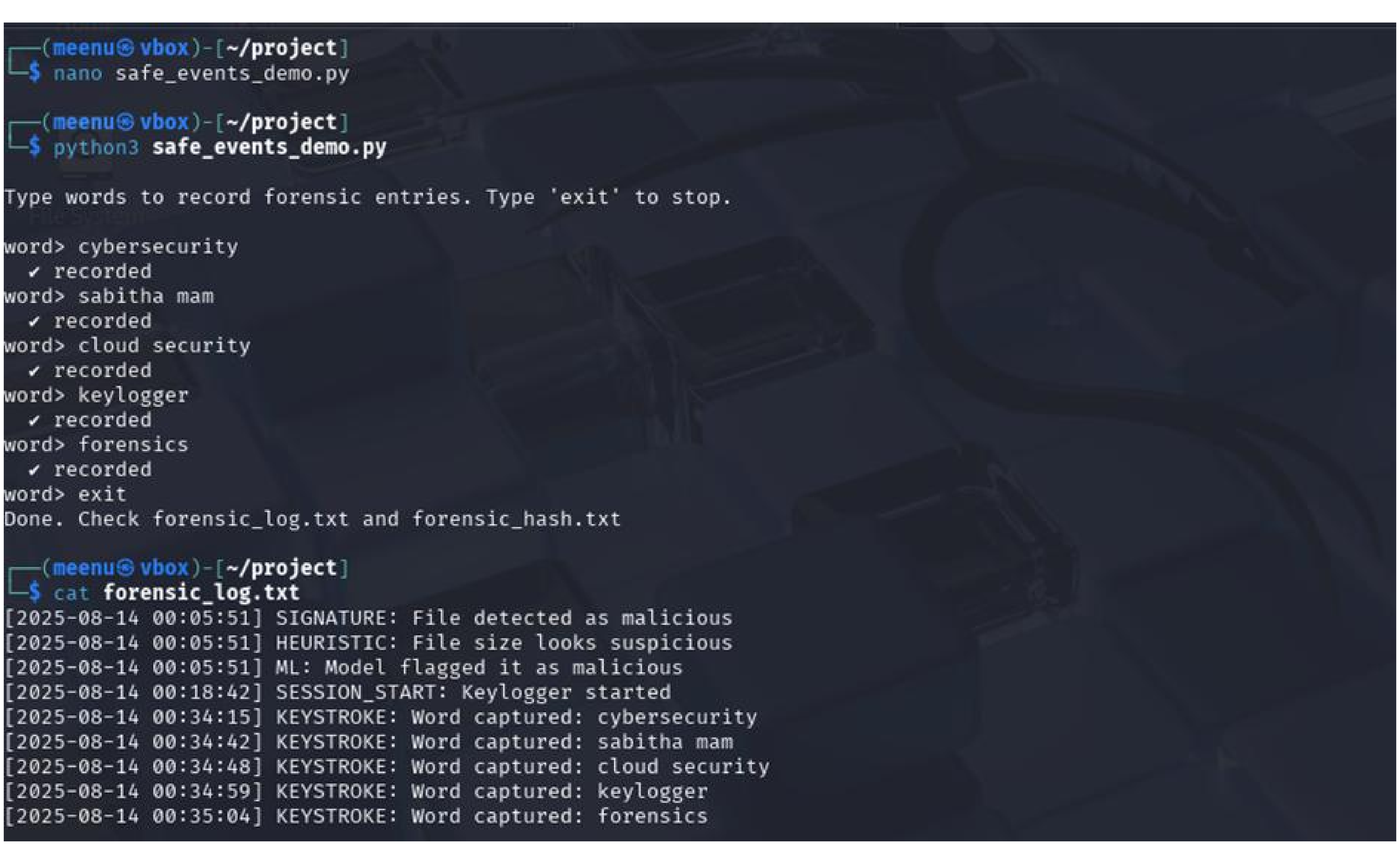


Fig : A keylogger script on Kali Linux, displaying recorded keystrokes saved in logs.txt demonstrating successful logging of typed input. Keystroke is what you do (pressing keys). ,Keylogger is what records it (like a spy for your keyboard).

Step 7: A forensic logging mechanism implemented in Python, designed for recording and validating security-related events, particularly during malware detection and keylogger analysis. This system maintains a secure record of activities and ensures log integrity using cryptographic hashing.

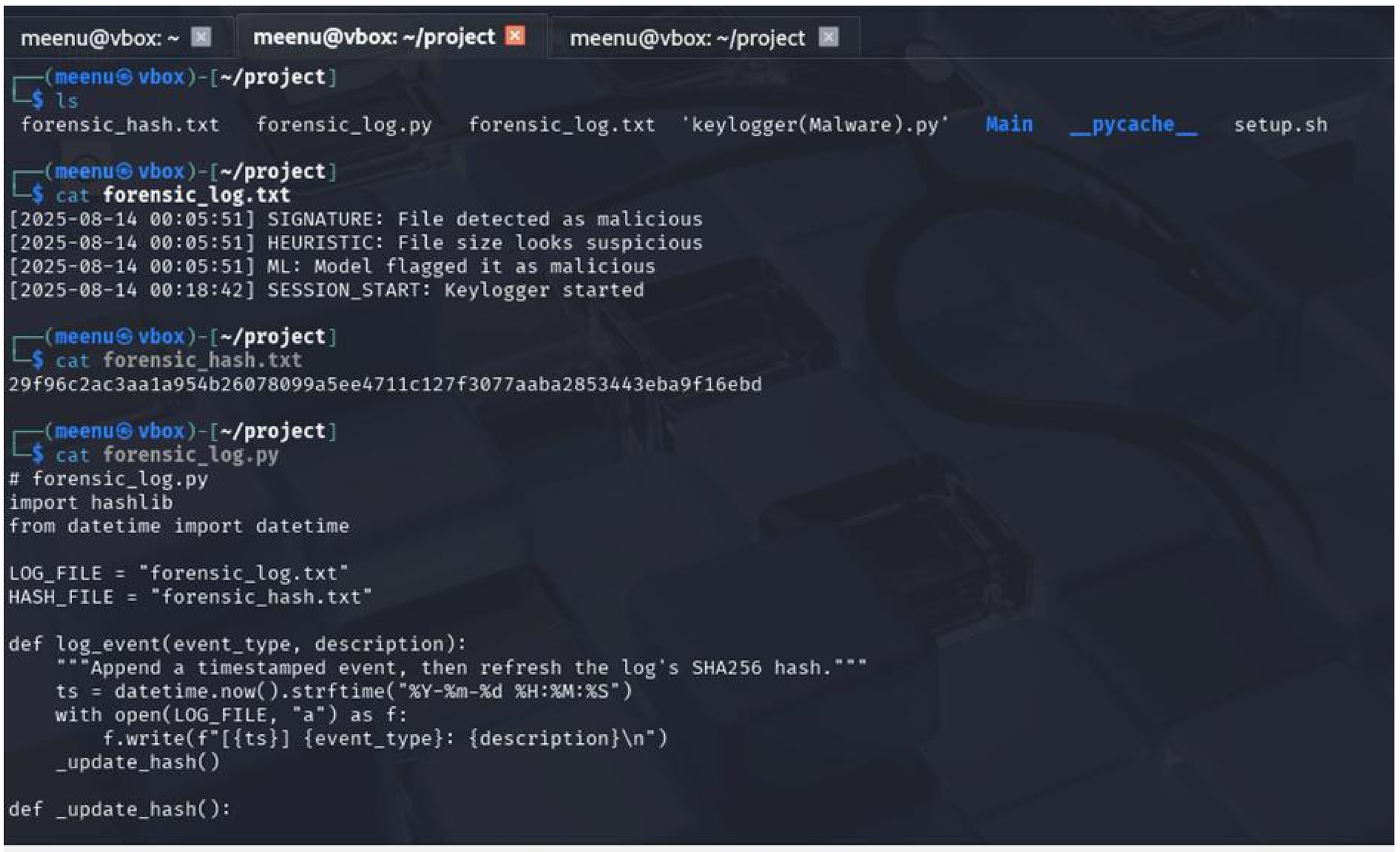


Fig : The system generates a SHA-256 hash of the log file. This hash acts as a digital fingerprint, ensuring that any unauthorized modification in the log can be detected immediately. The hash value displayed in the screenshot is an example of such a fingerprint.

Step 8: The forensic log and hash file created during an experiment involving a keylogger

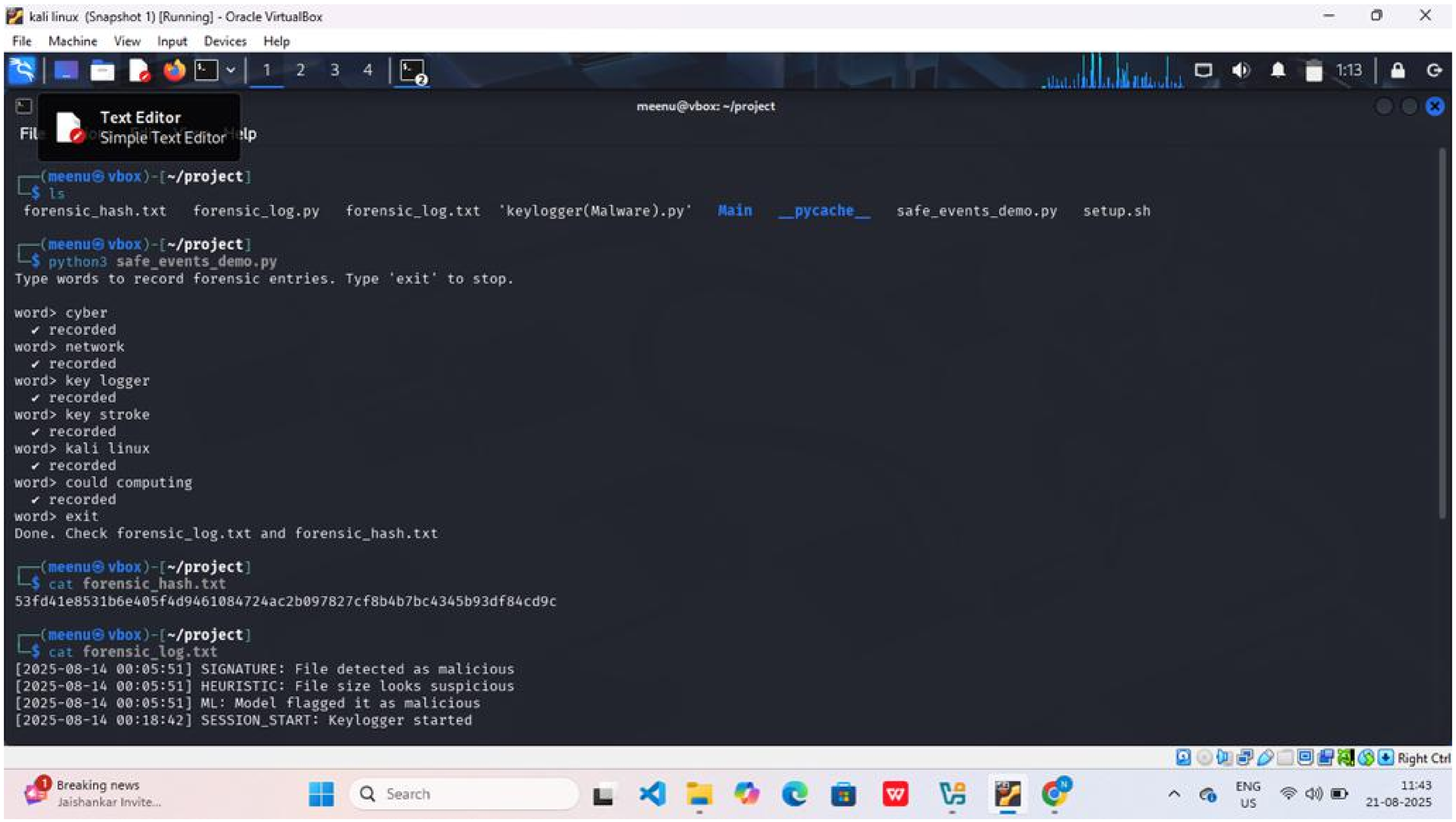


Fig 10: Forensic Hash (forensic_hash.txt)The file contains a cryptographic hash value (most likely SHA-256).The purpose of this hash is to ensure integrity of the forensic evidence.

Step 9: The demonstrates the execution of a Python script (safe_events_demo.py) that simulates safe forensic logging.Each word entered is recorded as a forensic event.

1. forensic_log.txt → contains the actual forensic events with timestamps.
2. forensic_hash.txt → contains the integrity hash of the log.

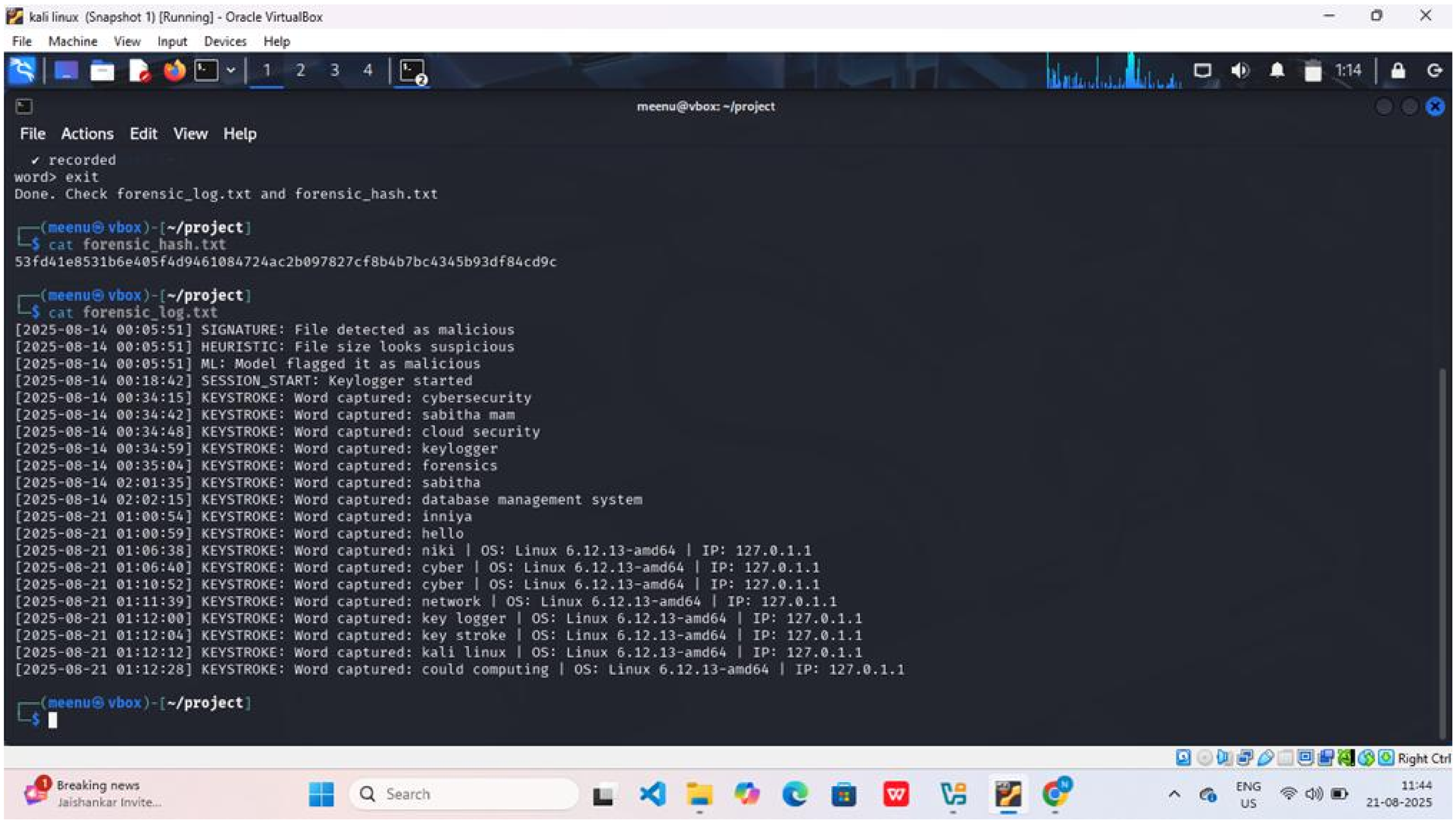


Fig: He log shows malware detection events and a session start for the keylogger. The captured entries are timestamped to preserve the chronological order of events.

FUTURE ENHANCEMENT

The proposed forensic framework, which focuses on keystroke dynamics, preprocessing, feature extraction, operating system identification, IP tracing, and hashing, has laid a strong foundation for digital investigations. However, as cyberattacks become more sophisticated and attackers constantly develop new methods to bypass security, there is significant scope for future improvements. Enhancing the system with advanced techniques and technologies will ensure that it remains reliable, scalable, and effective for real-world applications.

One of the most promising directions for future development is the integration of artificial intelligence. By training machine learning and deep learning models on large datasets of user behavior, the system could automatically detect anomalies in keystroke dynamics that may suggest malicious activity. Unlike rule-based approaches, AI has the ability to learn from data, adapt to new attack patterns, and continuously improve its detection capabilities. This would make the framework not only more intelligent but also more adaptive in identifying sophisticated keyloggers and unauthorized intrusions.

Another area for enhancement lies in real-time monitoring. The current model focuses mainly on analysing data after it has been collected. While this is useful for evidence gathering, it may not prevent ongoing attacks. By incorporating real-time detection and alert systems, investigators can be notified immediately when suspicious keystroke activity or abnormal IP communication occurs. This would allow for faster incident response and minimize potential damage. Real-time monitoring also makes the system more proactive, turning it into a preventive security tool rather than just a post-incident forensic solution.

In addition, storing forensic data securely is an essential requirement. Traditional local storage may be vulnerable if the system itself is compromised by attackers. Future versions of the framework could adopt cloud-based forensic storage, which not only secures evidence from tampering but also makes the data accessible to authorized investigators from anywhere. Cloud-based solutions also provide scalability, meaning larger volumes of forensic data can be stored and processed efficiently without depending on the limitations of local storage. With the growing reliance on

Cloud-based solutions also provide scalability, meaning larger volumes of forensic data can be stored and processed efficiently without depending on the limitations of local storage. With the growing reliance on cloud technologies, this enhancement would ensure that the forensic system is compatible with modern IT infrastructures.

Another potential improvement is cross-platform adaptability. Currently, many forensic solutions focus only on desktop or server environments. However, cyber threats now target mobile devices, IoT systems, and cloud infrastructures as well. Extending the framework to work seamlessly across different operating systems and platforms would make it more versatile and widely applicable. For instance, mobile devices could be monitored for abnormal keystroke inputs, IoT sensors could be checked for tampering, and cloud servers could be analysed for unauthorized access attempts. A cross-platform forensic tool would therefore cover a broader digital landscape, strengthening cybersecurity at multiple levels.

Enhancing the level of cryptographic protection used in the framework is another key area of future development. Hashing techniques are already part of the proposed model, but as attackers find ways to exploit older algorithms, more advanced methods such as SHA-3 or quantum-resistant encryption could be integrated. This will ensure that the forensic evidence remains tamper-proof and trustworthy even against advanced adversaries. Evidence integrity is crucial in digital forensics, especially when logs and reports are presented in court or during official investigations. Stronger cryptographic safeguards will make the system more credible and legally acceptable.

Future versions of the framework could also introduce automated reporting and visualization capabilities. Currently, investigators often need to manually analyse logs and prepare reports, which can be time-consuming. By integrating dashboards, charts, and automated summaries, the system could present forensic findings in a structured and easily understandable format. This would not only save time but also make the results accessible to non-technical stakeholders such as law enforcement officers, managers, or legal teams. A user-friendly reporting system would thus improve the usability and impact of the forensic framework.

Finally, collaboration with global threat intelligence databases can add immense value to the proposed system. Cyberattacks often originate from known malicious IP addresses or follow recognizable attack patterns. By linking the forensic framework with external threat intelligence feeds, the system could automatically flag suspicious IPs, malware signatures, or behavioural patterns.

This would provide investigators with a broader context, helping them not only to analyse local incidents but also to understand how they relate to global cybercrime trends. Such integration would make the system a part of a larger cybersecurity ecosystem, contributing to collective defence against digital threats.

CONCLUSION

The work presented in this article highlights the significance of integrating keystroke dynamics, pre-processing, feature extraction, operating system identification, IP tracing, and hashing into a unified forensic framework. In today's digital world, where cyber threats are increasing in both frequency and sophistication, it is no longer sufficient to rely on traditional methods of investigation. The proposed framework demonstrates how combining multiple forensic techniques into a structured pipeline can provide stronger, more reliable evidence for cybersecurity professionals and investigators. By addressing keystroke data at the pre-processing stage, the framework ensures that only relevant and meaningful information is analysed, reducing the risk of false positives. This step alone lays the foundation for accurate and efficient forensic analysis.

Feature extraction plays a vital role in transforming raw inputs into meaningful attributes, such as timing patterns, key sequences, system metadata, and network details. These extracted features form the core evidence that helps in identifying both user-specific behaviors and potential malicious activities. The inclusion of operating system and IP address information enhances the investigative process by connecting user actions to particular systems and network locations. Furthermore, the addition of hashing techniques ensures the integrity and authenticity of collected data, which is essential when presenting findings in legal or organizational contexts. This integration of cryptographic safeguards into the forensic pipeline makes the framework more resistant to tampering, thereby strengthening its reliability. The study also underscores the importance of building forensic systems that are both practical and adaptable. Unlike single-focus solutions, this approach combines multiple layers of analysis, making it more effective against complex threats such as hidden keyloggers or advanced persistent attacks.

Moreover, the framework aligns with the growing need for transparency, accountability, and legal compliance in digital investigations. Evidence produced through this system can be trusted not only for technical evaluation but also in judicial proceedings, where the authenticity of digital data is often questioned.

From an academic perspective, this project contributes to the field of digital forensics by demonstrating how interdisciplinary approaches merging behavioural biometrics, system analysis, network monitoring, and cryptography can lead to more advanced investigative models.

It shows that forensic research should not be confined to a single technique but should evolve into integrated frameworks capable of addressing multiple aspects of cybercrime simultaneously. This holistic perspective is particularly relevant as cybercriminals increasingly employ multi-layered strategies to bypass detection.

On a practical level, the proposed methodology is valuable for organizations, law enforcement agencies, and cybersecurity teams. For organizations, it can serve as an internal monitoring tool to detect unauthorized access and insider threats. For law enforcement, it offers a structured method of collecting, preserving, and analysing digital evidence. For cybersecurity professionals, it provides deeper insights into the behaviour of attackers and the techniques they use. By offering benefits across these different contexts, the framework establishes itself as a versatile tool with wide-ranging applications.

Despite its strengths, the study also acknowledges that the current implementation is only a step toward a more comprehensive forensic solution. Cybersecurity is a constantly evolving domain, and no framework can claim to be entirely fool proof. This recognition is not a limitation but rather an opportunity for continuous improvement. Future enhancements, such as artificial intelligence integration, real-time monitoring, cloud storage, and global threat intelligence collaboration, will further extend the value of the system. As such, the framework is not presented as a final product but as a foundation upon which more advanced forensic solutions can be built.

In conclusion, the article has emphasized that keystroke-based forensic analysis, when combined with system and network metadata and protected by cryptographic measures, offers a strong approach for digital investigations. It has shown how pre-processing and feature extraction transform raw inputs into meaningful forensic evidence, how OS and IP information provide essential context, and how hashing ensures data authenticity.

Together, these elements create a pipeline that is not only technically robust but also legally defensible. By adopting and extending this approach, digital forensic professionals can be better equipped to face the challenges of modern cybercrime. Ultimately, the project contributes both theoretical insight and practical solutions to the growing field of cybersecurity, paving the way for more reliable, intelligent, and future-ready forensic systems.

REFERENCES

1. Advanced Linux System Programming, Mark Mitchell, 2020
Methods on handling system-level programming for capturing input/output in Linux.
2. Practical Malware Analysis, Michael Sikorski & Andrew Honig, 2020
A hands-on guide to analysing malware, including keylogger behaviour and payload inspection.
3. Linux Hardening in Hostile Networks, Kyle Rankin, 2020
Covers defensive techniques against input-capturing tools like keyloggers in Linux environments.
4.Wireshark Documentation, Wireshark Foundation, 2021
Technical reference for network packet analysis and detecting keylogger activity over networks.
5. Metasploit Framework Guide, Rapid7 Team, 2021
Framework manual useful for advanced penetration testing related to keyloggers and backdoors.
6. Black Hat Python, Justin Seitz, 2021
Covers Python-based tools for penetration testing including keylogging, sniffers, and payloads.
7. Cybersecurity Essentials, Charles J. Brooks, 2021
Comprehensive reference explaining cyber threats like malware, spyware, and keyloggers.
8. Network Security Tools, Nmap & Wireshark Communities, 2021
Includes protocols and filters useful in monitoring keylogger communication.
9. Python Virtual Environments, Python Software Foundation, 2022
Guide to managing isolated Python environments using venvs for dependency control.
10. Linux Command Line Basics, Canonical Ltd., 2022
Fundamental reference for Linux terminal commands like cd, ls, and cat.

11. Jain, A., & Patel, R., Keylogger Attacks and Detection Techniques, 2022
A research article discussing different types of keyloggers.
12. Python Logging Module, Python Software Foundation, 2022
Guide to capturing logs programmatically during script execution using the logging module.
13. Penetration Testing with Kali Linux, Offensive Security, 2022
Coursebook for tools and methods in ethical hacking including keystroke logging.
14. pynput Documentation, pynput Contributors, 2023
Documentation of the Python library used for keyboard event capturing in keylogger applications.
15. Kali Linux Documentation, Offensive Security, 2023
Official system documentation explaining tool usage and Linux terminal environment in Kali Linux.
.
16. Automate the Boring Stuff with Python, Al Sweigart, 2023
Tutorial-based reference for automation tasks using Python, including keyboard/mouse event simulation.
17. Digital Forensics with Kali Linux, Corey Charles, 2023
Explains usage of Kali Linux in digital investigations, including log review and keylogger detection.
18. Real-Time Threat Detection, SANS Institute Whitepaper, 2023
Discusses techniques for capturing and analysing keystrokes and other user activities in real time.
19. Ethical Hacking Handbook, Daniel G. Graham, 2023
Details techniques like keylogging, phishing, and privilege escalation in ethical hacking practices.
20. User Project Execution Logs, Meenu Nandhini, 2025
Screenshots and terminal logs demonstrating the execution of keylogger.py and contents of logs.txt

ABOUT THE AUTHORS

Dr Sabitha Bau A
Assistant Professor
PSGR Krishnammal College for Women



S. Nandhini
B.Sc. CS with Cyber Security
PSGR Krishnammal College for Women





ARTIFICIAL INTELLIGENCE IN FORENSIC SCIENCE: ADVANCING JUSTICE THROUGH TECHNOLOGY

Author: Aditya Suman

Introduction

Artificial Intelligence (AI) is revolutionizing forensic science technique by which it enhancing accuracy, efficiency, and investigative depth across all domains, including digital forensics, forensic pathology, victim identification, and toxicology. The application of AI enables automation of routine tasks, rapid analysis of complex datasets, and novel solutions that surpass traditional methods in both speed and reliability. This article provides a overview of AI's role in forensic science, detailing current capabilities, applications, challenges, and ethical concerns, supported by recent research and literature content .

Evolution of AI in Forensics

Since Alan Turing's conceptualization of computer intelligence and the Turing Test, AI has intensively evolved, with notable adoption in forensic medicine over the past two decades. Initially limited to expert systems and basic image analysis, AI today encompasses deep learning, generative models, and sophisticated pattern-recognition algorithms each playing a vital role in forensic investigations from post-mortem analysis to digital crime scene reconstruction. The-Future-of-Artificial-Intelligence-

Core AI Technologies in Forensic Medicine

Machine Learning & Deep Learning

Machine learning algorithms extract patterns and make predictions from complex data sources, such as same medical images, DNA profiles, and forensic samples. Deep learning, a subset of machine learning, leverages neural networks for high-accuracy image classification (CT/MRI scans), facial recognition, and trauma analysis. fThe-Future-of-Artificial-Intelligence-AI

Generative AI

Generative AI models store and synthesize the data, simulate crime scenes, and produce more predictive analyses for behavioural profiling and risk assessments in forensic psychiatry. Such models support condition reconstruction and training.

Natural Language Processing

AI leverages natural language processing to interpret forensic reports, extract key details, and support digital investigations through linguistic analysis of evidence and communications.

Major Applications of AI in Forensic Science

Virtual Autopsies and Post-Mortem Analysis

AI-powered imaging technologies (e.g., virtopsy) combine CT/MRI scans with automated recognition algorithms to enhance autopsy accuracy detecting trauma, identifying pathology, and estimating time of death more reliably than human examiners alone.-The-Integration-of-Artificial-Intelligence-in-the-Forensic-Medicine-and-its-Applications-in-Medicine

AI models can process blood markers (LDH, pH, electrolytes) to calculate post-mortem intervals and cause of death.

Automated wound classification supports firearm injury analysis by matching entry holes and patterns to ballistics databases

Forensic Toxicology

AI algorithms automate the identification of toxins, drugs, and metabolites in post-mortem samples. Mass spectrometry and chromatography powered by AI accelerate toxicological analysis, ensuring prompt and precise reporting for judicial proceedings.

Digital Forensics and Cybercrime

AI-driven tools address the surge of digital evidences, automating tasks such as malware detection, log analysis, and fraud investigation in a more sophisticated way . Advanced object recognition and 3D modelling reconstruct crime scenes virtually, allowing for immersive, multi-angle examinations of evidence and events.



DNA and Biometric Analysis

AI facilitates rapid DNA profiling, interpretation of complex mixtures, and matching against databases for suspect or victim identification.

Facial, fingerprint, and retinal recognition: AI excels at biometric analysis, verifying identities in mass disaster, missing persons, and criminal cases.

Forensic odontology benefits from neural networks capable of gender, age, and morphology prediction based on dental records.

Crime Scene Reconstruction

AI reconstructs crime scenes using pattern recognition (blood spatter, trajectory, and spatial analysis) and generates virtual models for court presentations in a more accurate way

Forensic Psychiatry and Behavioural Profiling

Generative AI supports risk assessments, behavioural analyses, and psychiatric evaluations, informing rehabilitation and sentencing decisions.

Teaching, Education, and Simulation

AI-powered virtual simulations and intelligent tutoring systems deliver personalized, evidence-based forensic medicine education.

Virtual autopsy subjects and case-based learning environments provide risk-free, hands-on experience for students and experts

Advantages of AI Integration

- Accuracy and Efficiency: Routine automation reduces human error and speeds up forensic investigations.
- Cost-Effectiveness: AI lessens manual labor, streamlines case management, and minimizes operational expenses which can be used in another way.

analytics and pattern recognition unlock new solutions for complex cases and unresolved deaths cases .

- Reproducibility: Standardized AI processes improve the reliability of forensic evidence for legal admissibility everywhere also in the court .Data
- Integration: AI efficiently analyses large, multi-modal forensic datasets, enabling holistic view of every evidence.

Limitations and Challenges

Data Quality and Algorithmic Bias

AI effectiveness depends on large, diverse, and well-annotated dataset . Poor data quality or bias in training data can lead to unreliable and unfair results, particularly in every sensitive legal context.

Interpretability and Transparency

Opaque "black box" models dilute court confidence. Regulatory frameworks increasingly call for "glass box" (interpretable) AI systems models that provide traceable reasoning paths and support cross-examination.

Privacy and Ethical Consideration

Handling sensitive medical and personal data necessitates strict privacy safeguards. Dangerous outcomes include unauthorized data analysis, breach of civil liberties, and ethical violations.

Legal Admissibility

Questions remain regarding the admissibility and reliability of AI-generated evidence in global courtrooms. Methodological rigor, reproducibility, and expert oversight are essential on these both subjective and objective matter .

Training and Human Oversight

AI machine training is complex and demands expert human supervision. Over-reliance may destroy critical thinking and creative forensic expertise.

Cybersecurity Risks and New AI-Enabled Crimes

AI is increasingly weaponized like for deepfake creation, automated cyberattacks everywhere , and forensic log manipulation technique , complicating investigations and evidentiary trust.

Ethical and Regulatory Frameworks

The future of forensic AI hinges on robust ethical standards, transparency, fairness, and accountability. Collaboration among forensic experts, technologists, legal authorities, and ethicists is vital to:

Mitigate bias and discrimination in Realtime algorithms, Protect privacy and ensure data security, Establish standards for interpretability and legal evidentiary requirements,

Promote research on ethical AI deployment in forensic practice. The-Future-of-Artificial-Intelligence-AI

Future Directions

The integration of AI in forensic medicine will expand, enabling faster, more reliable, and fairer justice worldwide. Ongoing research should focus on Multi-modal dataset curation for training unbiased, accurate AI models,

- Development of interpretable AI frameworks for legal and ethical accountability,
- Advanced detection tools for synthetic media and cybercrime,

Responsible governance and interdisciplinary collaboration for sustainable implementation.

References

1. Alafer, F. (2025). Emerging imaging technologies in forensic medicine. Diagnostics, 15(5), 1265. **https://pmc.ncbi.nlm.nih.gov/articles/PMC12154265/**
2. Cărcăle, V. A. (2025, April 17–18). The future of artificial intelligence (AI) applications in forensics. RAIS Conference Proceedings, 249–256. Research Association for Interdisciplinary Studies.
3. Cureus. (2024, September). Artificial intelligence in forensic sciences: A systematic review of past and current applications and future perspectives. Cureus, 16(9), e294368. **https://www.cureus.com/articles/294368-artificial-intelligence-in-forensic-sciences-a-systematic-review-of-past-and-current-applications-and-future-perspectives**
4. Frontiers in Medicine. (2025, July). The application of artificial intelligence in forensic pathology. Frontiers in Medicine, 12, 1583743. **https://www.frontiersin.org/journals/medicine/articles/10.3389/fmed.2025.1583743/full**
5. Piraianu, A., Fulga, A., Mușat, C., Iliescu, D., Vereanu, A., Ceachir, O., & Fulga, I. (2023). How artificial intelligence is transforming forensic medicine. Diagnostics, 13(11), 1829. **https://pmc.ncbi.nlm.nih.gov/articles/PMC10529115/**
6. ScienceDirect. (2025). A responsible artificial intelligence framework for forensic science. Forensic Science International, 390, 111186. **https://doi.org/10.1016/j.forsciint.2025.111186**

ABOUT THE AUTHOR



Aditya Suman
Government Holkar Science College, Indore.

What's New In The Forensic Market

Full Spectrum Imaging System (FSIS-CSE): A New Era in Crime Scene Evidence Capture

In January 2025, Arrowhead Forensics, a division of Thomas Scientific, in partnership with General Atomics Electromagnetic Systems (GA-EMS), announced the launch of a groundbreaking forensic technology: the Full Spectrum Imaging System Crime Scene Examiner (FSIS-CSE). This new innovation marks a significant leap in how forensic experts capture, document, and analyze crime scene evidence. Designed to be compact, lightweight, and portable, the FSIS-CSE builds upon GA-EMS's Full Spectrum Imaging System (FSIS II) technology, integrating advanced imaging capabilities into a mobile, user-friendly solution tailored for use at real crime scenes. This essay explores the technology, its features, applications, and implications for forensic science, law enforcement, and global crime scene investigation practices.

Background of the Partnership

Arrowhead Forensics is a trusted name in the forensic market, providing products and services tailored for crime scene investigators and forensic laboratories. In 2023, it became a division of Thomas Scientific, a global distributor of scientific solutions, thereby expanding its reach and resources. General Atomics Electromagnetic Systems (GA-EMS), known for its innovations in defense and advanced technologies, developed the FSIS II, a laboratory-based full spectrum imaging system that revolutionized evidence imaging. The collaboration between Arrowhead Forensics and GA-EMS represents the merging of specialized forensic expertise with advanced imaging technology to produce an accessible, field-ready solution for evidence capture.

The FSIS-CSE Technology

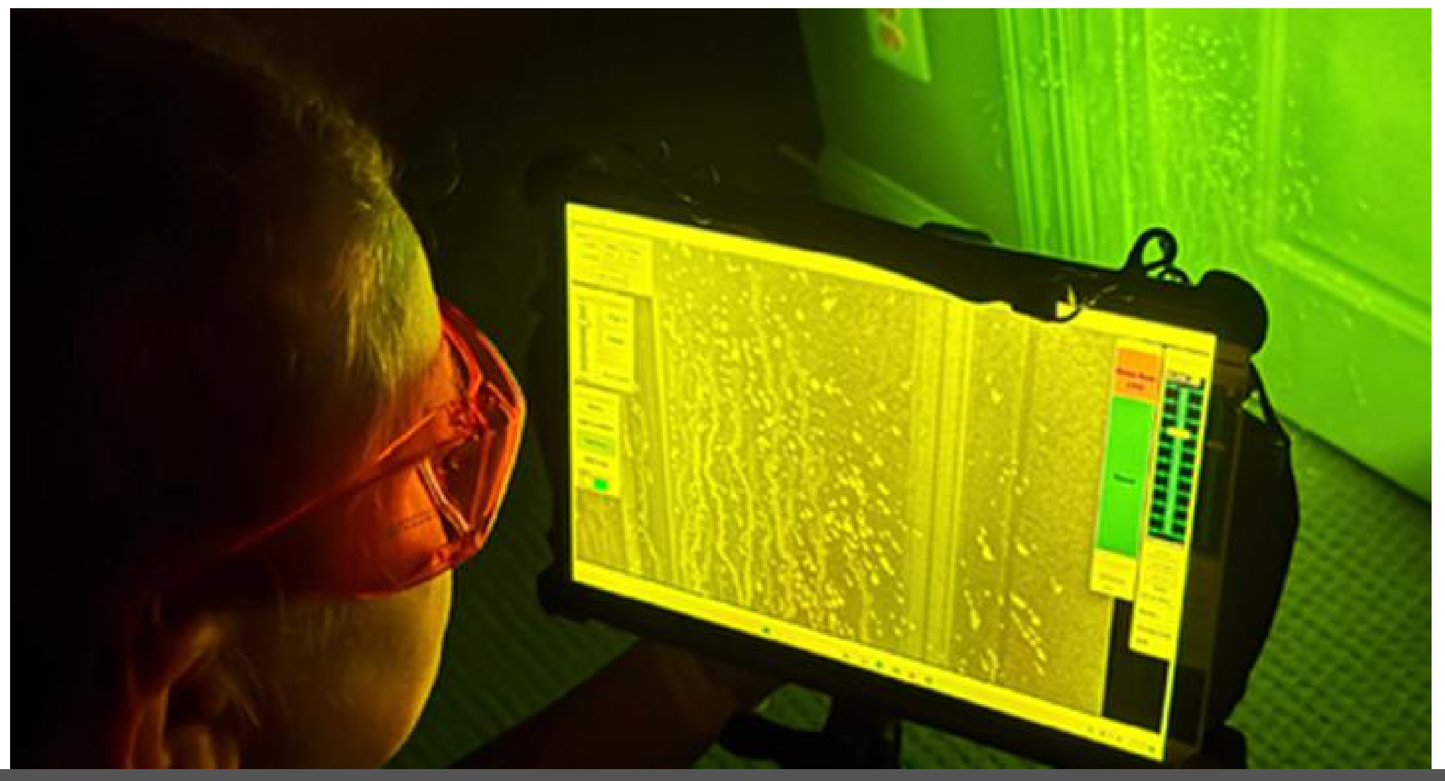
The FSIS-CSE is specifically designed to meet the challenges of crime scene investigations. Traditional crime scene photography often struggles with limitations such as lighting conditions, surface textures, and the visibility of certain biological or chemical residues. The FSIS-CSE addresses these challenges by enabling multi-spectrum imaging in a compact format.

The system integrates GA-EMS's FSIS II camera into a portable device mounted on a 13-inch tablet. This makes the system both lightweight and mobile, ensuring investigators can use it in confined or difficult-to-access crime scenes, such as vehicles, small rooms, or outdoor environments with challenging terrain. Its imaging capabilities allow forensic teams to detect, scan, and capture high-resolution images of latent fingerprints, biological stains, chemical residues, and trace evidence without the need for invasive or destructive methods.

Key Features and Advantages

Some of the most remarkable features of the FSIS-CSE include:

1. Portability: The device's compact design allows forensic experts to carry it easily to various locations.
2. High-Resolution Imaging: Capable of capturing extremely fine details that may not be visible to the naked eye.



3. Full Spectrum Capability: The system captures evidence under multiple wavelengths, enhancing the visibility of latent prints and biological materials.
4. Confined Space Utility: Especially effective in small or cluttered spaces such as cars or narrow rooms.
5. User-Friendly Interface: The integration with a tablet makes the system intuitive and efficient to operate in the field.
6. Non-Destructive Evidence Capture: The FSIS-CSE allows investigators to collect crucial information without altering or damaging the evidence.

Applications in Forensic Science

The FSIS-CSE has a wide range of forensic applications. It significantly improves the ability to detect and document evidence that traditional tools might overlook. For example, latent fingerprints that are invisible under white light can be revealed under specific wavelengths. Biological stains such as blood, semen, or saliva can be visualized even on complex surfaces. Chemical residues from explosives, drugs, or accelerants can also be detected using the system's spectral imaging capabilities.

Beyond crime scenes, the FSIS-CSE can be applied in forensic laboratories for quality assurance and validation of evidence. Its portability also makes it an ideal choice for field units in disaster victim identification, counterterrorism operations, and border security. The technology thus bridges the gap between laboratory-level precision and field-level practicality.

Global Market and Expansion

According to the press release, the FSIS-CSE has already seen strong domestic demand in the United States, with sales exceeding initial expectations. The technology is also being marketed internationally across Europe, the Middle East, and Canada, reflecting a global interest in advanced forensic imaging solutions. As law enforcement agencies worldwide face increasing pressure to deliver accurate and efficient results, tools like the FSIS-CSE provide a competitive edge.

Impact on Forensic Investigation

The FSIS-CSE represents a paradigm shift in forensic investigation. Traditionally, investigators relied heavily on chemical enhancement methods, powders, and dyes to visualize latent prints or biological evidence. While effective, these methods could sometimes damage evidence or alter its original characteristics. The FSIS-CSE eliminates this risk through non-destructive multi-spectral imaging. Furthermore, the ability to capture high-resolution images directly at the crime scene reduces the chances of evidence loss or contamination during transport. It also improves the chain of custody by ensuring that the evidence is documented in its original context. This not only strengthens the reliability of evidence in court but also enhances the credibility of forensic reports.

Training and Support

Arrowhead Forensics, with its established expertise in the forensic community, provides essential training and customer service to ensure that agencies adopting the FSIS-CSE can fully leverage its capabilities. By combining advanced technology with proper training, the partnership ensures that the tool is not only innovative but also practical and user-friendly for investigators of different skill levels.

Future Outlook

As technology continues to advance, systems like the FSIS-CSE are likely to become standard tools in forensic investigations. Future developments may include integration with artificial intelligence for automated evidence recognition, cloud-based storage for real-time data sharing, and enhanced portability with even more compact designs. The global forensic community is moving towards greater reliance on digital, non-destructive, and high-precision tools, and the FSIS-CSE positions itself at the forefront of this transformation.

Conclusion

The launch of the FSIS-CSE by Arrowhead Forensics and GA-EMS, in collaboration with Thomas Scientific, marks a milestone in forensic imaging. With its compact design, advanced, non-destructive imaging, and portability, it overcomes key challenges in crime scene investigation. Its adoption in the U.S. and abroad highlights its potential to transform evidence collection and analysis, making it a strong example of innovation shaping the future of forensic science.

PREPARE YOURSELF

UGC NET & FACT QUESTION BANK

1. What is the primary goal of forensic science?

A. To solve crimes
B. To analyze data
C. To rehabilitate offenders
D. To provide medical care

Choose the correct answer from the options given below:

A, B, C
A, C, D
B, C, D
A only

2. Which of the following is considered a physical evidence?

A. Eyewitness testimony
B. Blood samples
C. Confessions
D. Suspect interviews

Choose the correct answer from the options given below:

A, B, C
B only
C and D only
All of the above

3.What is the role of a forensic pathologist?

A. To analyze fingerprints
B. To determine the cause of death
C. To investigate cybercrimes
D. To collect DNA evidence

Choose the correct answer from the options given below:

A and C only
B only
A, C, D
All of the above

4.Which type of evidence is obtained from a crime scene and can be linked to a suspect?

A. Circumstantial evidence
B. Testimonial evidence
C. Direct evidence
D. Hearsay evidence

Choose the correct answer from the options given below:

A only
C only
B and D only
All of the above

5.What does DNA stand for?

A. Deoxyribonucleic acid
B. Deoxyribose nucleic acid
C. Deoxynucleic acid
D. Deoxyribonucleotide acid

Choose the correct answer from the options given below:

A only
B only
C and D only
All of the above

7. Which technique is commonly used to visualize fingerprints?
A. Chromatography
B. Gel electrophoresis
C. Latent print powder
D. Microscopy
Choose the correct answer from the options given below:
A and C only
B only
C only
All of the above

8. What is the significance of the chain of custody in forensic science?
A. It determines the validity of the evidence
B. It tracks the handling of evidence
C. It establishes the credibility of witnesses
D. It organizes crime scene data
Choose the correct answer from the options given below:
A and B only
B only
C and D only
All of the above
What type of evidence is based on observation or witness accounts?
A. Physical evidence
B. Circumstantial evidence
C. Testimonial evidence
D. Documentary evidence
Choose the correct answer from the options given below:
A only
B only
C only
All of the above

9. Which forensic technique analyzes the unique patterns of an individual's teeth?
A. Forensic odontology
B. Forensic anthropology
C. Forensic biology
D. Forensic chemistry
Choose the correct answer from the options given below:
A only
B only
C and D only
All of the above

10. Which of the following is NOT a type of fingerprint pattern?
A. Loop
B. Whorl
C. Arch
D. Ridge

11. What is forensic anthropology primarily concerned with?

A. Analyzing drug evidence

B. Identifying human skeletal remains

C. Studying insect activity on corpses

D. Examining blood spatter

Choose the correct answer from the options given below:

A and B only

B only

C and D only

All of the above

12. What does the term “ballistics” refer to in forensic science?

A. The study of insects

B. The study of firearms and ammunition

C. The analysis of blood samples

D. The examination of hair and fibers

Choose the correct answer from the options given below:

A only

B only

C only

All of the above

13. Which of the following is a common method for determining time of death?

A. Blood type analysis

B. Rigor mortis

C. Hair analysis

D. DNA profiling

Choose the correct answer from the options given below:

A only

B only

C and D only

All of the above

ANSWERS

1:A, 2:B, 3:B, 4:C, 5:A, 6:B, 7:C, 8:B, 9:C, 10:A, 11:D, 12:B, 13:B

PREPARE YOURSELF

UGC-NET PAPER 1: QUESTION BANK

1 .Which of the following is a characteristic of a good teacher?

(A) Strict discipline enforcement
(B) Ability to inspire and motivate students
(C) Limited interaction with students
(D) Focus solely on textbook content

2. What is the primary purpose of a research hypothesis?

(A) To summarize the research findings
(B) To provide a tentative explanation for a phenomenon
(C) To collect data
(D) To analyze the data

3. If the average of five numbers is 20, what is their total sum?

(A) 25
(B) 100
(C) 120
(D) 25

4. If all roses are flowers and some flowers fade quickly, which of the following is true?

(A) Some roses fade quickly
(B) All roses fade quickly
(C) No roses fade quickly
(D) Some flowers are not roses

5. Which of the following is an example of non-verbal communication?

(A) Speaking
(B) Writing
(C) Gestures
(D) Reading

6. What is the main objective of the National Institutional Ranking Framework (NIRF) in India?

(A) To rank universities globally
(B) To assess and rank higher education institutions in India
(C) To provide financial aid to students
(D) To regulate university admissions

7. Which of the following is a renewable source of energy?

(A) Coal
(B) Natural gas
(C) Solar energy
(D) Nuclear energy

8. Which of the following is an example of an input device?

(A) Monitor

(B) Printer

(C) Keyboard

(D) Speaker

9. If 'A' is taller than 'B' and 'B' is taller than 'C', which of the following is true?

(A) A is taller than C

(B) C is taller than A

(C) A is shorter than C

(D) Cannot be determined

10. Is the number 'x' an even number?

(1) x is divisible by 2

(2) x is divisible by 4

(A) Statement (1) alone is sufficient

(B) Statement (2) alone is sufficient

(C) Both statements together are sufficient

(D) Both statements together are not sufficient

11. Which of the following is a characteristic of an effective learning process?

(A) Rote memorization

(B) Active participation

(C) Teacher-centered approach

(D) Ignoring student feedback

12. Which of the following is an example of primary data?

(A) Data from a research article

(B) Data collected through surveys

(C) Data from textbooks

(D) Data from encyclopedias

13. If the mean of 8 numbers is 15, what is the total sum of the numbers?

(A) 100

(B) 120

(C) 80

(D) 110

14. All squares are rectangles. Some rectangles are not squares. Which of the following is true?

(A) Some squares are not rectangles

(B) All rectangles are squares

(C) Some rectangles are squares

(D) No rectangles are squares

ANSWERS 1:B, 2:B, 3:B, 4:A, 5:C, 6:B, 7:C, 8:C, 9:A, 10:A, 11:B, 12:B, 13:B, 14:C

ADITYA UNIVERSITY

nirf Rank Band 151-200 | ACCREDITED BY NAAC A++ GRADE | NBA TIER 1 ACCREDITED | TIMES HIGHER EDUCATION IMPACT RANK | QS I·GAUGE INDIAN UNIVERSITY RATING DIAMOND



DEPT. OF FORENSIC SCIENCE
SCHOOL OF SCIENCES

Aditya Nagar, ADB Road, Surampalem, Kakinada Dt., Andhra Pradesh 533437

Mail: forensicmagazine@aditya.ac.in Web: www.adityauniversity.in

Reach Us