Cyber Forensics Vs Traditional Forensics: A Critical Analysis

Dr. K. Prasanna Rani[1], Dr. T. Raghu Ram[2]
[1]*Assistant Professor of Law, Telangana University, Nizamabad*
[2]*Prl. District Judge*

Abstract- ***The high rate of digitalisation in the modern society has shifted the face of criminal activities thus making the modern society rely more on forensic science in aiding legal investigations. Conventional forensic methods, including fingerprint sample examination, ballistics, DNA profiling, and examination of trace evidence, remain important in solving such physical crime cases. Nonetheless, these approaches are no longer effective due to the exponential growth in the number of cyber-enabled offences. Cyber forensics has become an important discipline that concerns itself with identifying, preserving, analyzing and reporting digital evidence supplementing the normal investigational paradigms. The article is critical of changes in the development of both of the branches of forensics and critical on the aspect by which a dual approach has been required by changing patterns of crime. This paper examines the underlying distinction between conventional and cyber forensic processes and how each area gathers, processes, and authenticates evidence. Classical forensics is very dependent on physical evidences, laboratory, and proven scientific theories, but cyber forensics needs specialisation to recover information, examine networks, malware, and trace digital footprints. Comparing the proficiencies and weaknesses of the two systems, the article highlights the direct impact of the nature of evidence tangible or digital one on the strategy and results of investigations. Also, to provide the evidence of the practical implementation, challenges, and increasing the necessity of the integrated forensic capabilities, the article also includes real-world case studies in India and other countries. The problems concerning the evidentiary standards, admissibility of digital evidence, legal gaps, and infrastructural limitations are examined to highlight the intricacies of the investigators and courts. The article concludes that a hybrid forensic system, which is a combination of conventional and cyber approach is necessary to combat crime in the modern society, enhance judicial procedures and to guarantee the accuracy of evidence in the fast growing digitalized society.***

Keywords: Cyber Forensics, Traditional Forensics, Digital Evidence, Crime Investigation, Legal Challenges, Case Studies, Forensic Science Integration.

I. INTRODUCTION: EVOLUTION OF FORENSICS IN THE DIGITAL AGE

Although its groundbreaking was largely based on the study of physical evidence, forensic science has considerably changed along with the technological advancement of the new world. In the past, investigators were dependent on fingerprint matching, serology and ballistics and subsequently DNA profiling as a means of reconstructing events and determining perpetrators. As a scientific analysis of crimes laid down in laboratories, these practices established a stable framework of criminal investigation and formed the image of the trust in forensic evidence in society. But with the advent of the mass digitalisation, the established patterns of investigation have been shaken and new crime patterns have emerged, requiring more technologically advanced responses.

The online revolution of the society, characterized by the growth of the internet, smartphone, cloud computing and artificial intelligence has significantly escalated the level of activities that occur online. As this has changed so has criminal behaviour. Hacking, phishing, financial cyberfraud, digital piracy, cyberstalking, and data theft are all crimes that have become more prevalent, and are often done remotely and anonymously. The crimes do not often leave any tangible evidence; they leave digital footprint in their devices, networks and, online platforms. The change has resulted in the creation of cyber forensics as a specialised area that is competent enough to detect, gather, examine, and scrutinize electronic evidence in a scientifically justifiable way.

The overlapping of the traditional and cybercrime has resulted in a dual investigative environment where the two types of forensic science exist concurrently. Most contemporary cases have become physical and digital in nature, including crimes organized on the mobile platform, fraud related to the use of electronic transactions or

physical crimes captured on electronic devices. Such a convergence highlights the importance of the investigators to keep pace, modernize the technical skills and incorporate multi-disciplinary forensic techniques. The history and development of digital forensics, thus, is not only a history of the technological usage but a wider 21st-century shift in the conceptualisation of evidence, its storage and presentation in court. This paper discusses this development by critically comparing cyber and traditional forensic practices and offers an insight on the challenges and opportunities that characterize the modern forensic practice.

II. FOUNDATIONS AND METHODOLOGIES OF TRADITIONAL FORENSICS

The classical forensic science is the historical backbone of criminal investigations and is based on thoroughly known scientific principles of law enforcement that have served the police department more than 100 years. Its development is based on the Exchange Principle of Locard that states that no contact is left without a trace- a principle on which the philosophy of crime scene investigation is based. Traditional forensics needed several decades to grow with the development of biology, chemistry, physics, and medicine, and it led to the creation of specialised branches with the ability to examine fingerprints, DNA, marks on the tools, toxic substances, and ballistic patterns. This scientific foundation has seen to it that the traditional forensic evidence remains highly credible in the world in the context of the courts.

2.1 Crime Scene Science and Locard's Principle

The initial phase of conventional investigation starts at the crime scene, whereby a systematic observation and a controlled evidence recovery occurs. The Exchange Principle suggests that according to Locard, criminals invariably leave traces that include fibres, hair, soil, blood drop, fingerprints, or footwear impressions that act as critical pointers to the reconstruction. Such evidences enable investigators to determine presence, movement or behavioural patterns of the involved persons. The concept of crime scene management focuses on handling without contamination, restricted access areas and scientifically directed search pattern of grid, spiral or quadrant.

2.2 Laboratory-Based Analytical Techniques

When evidence is taken to a forensic laboratory, a broad range of analysis methodologies are implemented by specialists. Serology and DNA profiling are applied to biological evidence, trace evidence is microscopically examined, and chemical evidence is revealed with the help of chromatography, spectroscopy or mass analysis. The matching of firearms is done using ballistics and cartridge casing that are found under comparison microscopes. Document examiners test the handwriting, composition of ink and paper properties and the toxicologists identify the poison, drugs and metabolites found in the bodily fluids. Such laboratory tests continue to be a key in the production of reproducible and scientifically validated results.

2.3 Chain of Custody and Evidentiary Standards

One major characteristic of conventional forensics is its strict chain-of-custody measures. All the evidence should be recorded, covered, labelled and traced back to the crime scene up to the court room. This process is very important in terms of transparency which has a great impact on the admissibility of evidence in the courts. Conventional forensic methodology has earned the judicial confidence due to its scientific reliability provable in terms of repeatability, peer review and expert testimony. This organized evidential system has helped to achieve convictions in most of the criminal cases.

The traditional forensics is therefore an unavoidable aspect of the investigation mechanism, which is found in the era of technology. It has an advantage in that it can be used to derive meaning out of physical evidence and recreate real world events- which even now remains in the vocational repertoire as digital forensics is becoming more and more a hybrid practice in its own right.

III. RISE OF CYBER FORENSICS: SCOPE, TOOLS, AND PROCESSES

The most ancient and stable form of the investigative practice is traditional forensic science, which has been the foundation of the criminal justice long before the digital age. It is based on the scientific principles in uncovering the perpetrators of the crime, re-creating the criminal incidents, and supplying the courts with objective evidence. The most significant point of its development is the Exchange Principle of Locard, according to which,

when two objects collide, material is always exchanged. This is a very simple but deep concept that redefined the policing as it used to be by focusing on the physical traces that a suspect is unlikely to tamper with due to the ease of fabrication or manipulation by confessions and eyewitness records. With the development of scientific knowledge, especially in biology, chemistry, physics, medical sciences, the traditional forensics evolved into highly specialised branches of knowledge that were able to analyse the fingerprints, DNA, tool marks, blood patterns, toxic substances, and ballistic trajectories. Traditional forensic evidence has gained a steady level of credibility in courts worldwide because of their basis on universally recognized scientific practices which in many cases have become the ultimate evidence used in a criminal case.

2.1 Crime Scene Science and Locard's Principle

The crime scene is where physical clues are initially revealed and the process of investigation starts. The foundational principle of crime scene science is that offenders always leave something, fibres, soil particles, fingerprints, biological stains, footprints, or impressions of damage are the things that they leave, and they may also take something away without knowing it is the principle of Locard. Such traces remain invaluable as they enable the investigators to know what, who, and how the course of actions happened. In order to conserve these clues, the crime scene officers employ organized search patterns like grid, spiral or quadrant search depending on the size and the complexity of the scene. The attention to control contamination should be taken as an essential element of the given stage: investigators should reduce access, use protective devices and manipulate the possible evidence with sterilized means to avoid accidental transfer or destruction of it. They would establish the basis of the proper laboratory analysis and believable presentation in court by being careful to gather and record all the possible traces and document them.

2.2 Laboratory-Based Analytical Techniques

Upon gathering, physical evidence is relocated to forensic labs where experts make use of scientific tools and methods in order to reveal the concealed information. Serological examination and DNA profiling of biological material-like blood, saliva or hair is done to prove identity or family connection. Trace evidence such as fibres, glass, paint chips, etc., is examined under the microscope to identify source, as well as match material sources. Drugs, poisons, accelerants and explosive residues are detected with the help of such sophisticated analytical methods as chromatography, spectroscopy and mass spectrometry. Crime investigators compare bullets and cartridge casings under comparison microscopes to determine the gun that was used to perpetrate an offense. The handwriting analysts examine strokes, ink, and document changes, whereas forensic toxicologists examine the materials of the body fluids to determine intoxication, poisoning, or overdose. These laboratory tests are based on approved scientific guidelines and results obtained are accurate, reproducible and can be used to provide expert testimony.

2.3 Chain of Custody and Evidentiary Standards

One of the strong points of conventional forensics is the strict adherence to the chain of custody which is a written procedure that ensures the evidence that was at the crime scene is carried to the courtroom. All products should be closed, marked, registered and kept in a controlled environment to avoid those products being tampered or contaminated. When a break in the chain occurs, courts attach a lot of weight to the physical evidence since it can easily be questioned and found to be untrustworthy, as any failure to meet these standards may result in a court battle. The admissibility of the traditional forensic methods which has been scientifically proven as seen by peer review, repeatability and interpretation by experts has also enhanced their admissibility. This rigorous evidentiary system has decisively led to solving of heavy crimes, convictions and elimination of erroneous results.

Although it is the digital age, traditional forensics still cannot be replaced. Crimes of an increasingly physical and cyber-related character have necessitated that the physical traces of a crime such as blood, DNA, weapons, fingerprints, or chemical residues be read alongside computer-based methods of investigation. The traditional value of forensics has remained that it fulfils the ability to recreate the reality of occurrences with the use of physical evidence that will close the gap between science and legal truth amidst the swiftly changing world of crime.

IV. COMPARATIVE ANALYSIS: TRADITIONAL VS. CYBER FORENSIC APPROACHES

With the advent of cyber forensics, the investigative world has been transformed in terms of the tools, types of evidence and procedural complexities. Whereas conventional forensics studies physical evidence in the form of fingerprints, blood, weapons, and biological evidence, cyber forensics studies intangible digital evidentiary traces that are created on devices, networks and in clouds. This section compares the two approaches in a systematic manner, underlining the differences in their operations, the complexity of the evidence as well as their practical implications on modern investigation.

4.1 Key Differences in Nature of Evidence

The difference between the two lies in the nature of evidence that they deal with. This difference is summarised in the table below:

Table 1: Nature of Evidence in Traditional vs. Cyber Forensics

Parameter	Traditional Forensics	Cyber Forensics
Type of Evidence	Physical, biological, chemical	Digital, electronic, metadata
Examples	DNA, fingerprints, fibres, weapons	Log files, emails, IP addresses, browser history
Visibility	Often visible or chemically detectable	Mostly invisible, requires tools to extract
Degradation	Subject to physical decay	Subject to deletion, encryption, alteration
Storage	Physical storage conditions required	Forensic imaging, bit-by-bit clones

The nature of traditional forensic evidence is usually hardy and physical whereas the digital evidence is volatile and can vanish at the press of a button. This weakness renders cyber forensics time-based and tool-apt.

4.2 Methodological Comparison

Traditional and cyber forensics have a serious divergence in the manner of investigation- collection to analysis.

Table 2: Methodological Differences

Stage	Traditional Forensics	Cyber Forensics
Collection	Securing scene, physical recovery, contamination control	Imaging devices, capturing volatile memory, hashing
Preservation	Sealing, packaging, refrigeration (for biological samples)	Write blockers, digital hashing (MD5/SHA-1)
Analysis	Microscopy, DNA profiling, ballistics comparison	Log analysis, malware reverse engineering, network forensics
Tools Used	Microscopes, chemical reagents, comparison microscopes	EnCase, FTK, Autopsy, Wireshark, Volatility
Time Sensitivity	Moderate; evidence decays over time	High; evidence may disappear instantly

The field of cyber forensics demands a lot of technical expertise as digital systems keep on evolving and attackers will usually strive to leave no trails by encrypting or anonymising.

4.3 Investigative Scope and Limitations

Each of the two systems used in forensics has its own strengths and weaknesses. These are as outlined in the following table:

Table 3: Strengths and Limitations

Aspect	Traditional Forensics	Cyber Forensics
Strengths	Highly reliable scientific methods; strong judicial acceptance	Ability to track online activity; essential for cybercrime; scalable across networks
Limitations	Limited for technology-driven crimes; dependent on physical availability	Highly technical; requires specialised labs; susceptible to encryption and data wiping
Suitable For	Murder, rape, assault, theft, physical damage investigations	Cyber fraud, hacking, identity theft, ransomware, digital financial crimes

The current crimes frequently demand an integrative type of investigation, including cyber-facilitated human trafficking, financial frauds with the use of online payments, or real-life crimes organized online.

4.4 Comparative Interpretation

The comparative study shows that both traditional and cyber forensics cannot be used alone to address the sophisticated nature of criminal behaviour in the modern world. Conventional forensics provides scientific accuracy when it comes to physical contact aspects whereas cyber forensics identifies behaviour patterns and communication logs in the online world. Combined knowledge is needed in the area where physical and cybercrime merge such as the recruitment of terrorists using social media that leads to violence in real life. The two types of evidences

need to be drawn closer and closer so that the investigators could create an elaborate map that traverses both the physical space and the virtual universe of the Internet.

Although classical forensics can enjoy the benefits of well-established procedures and high esteem in courts, cyber forensics is still confronted with such issues as encryption, cross-border jurisdiction when retrieving data, and the swift technological obsolescence. The given comparison reveals that the training, investment, and interdisciplinary cooperation is necessary to guarantee that both areas of forensics can efficiently work within the contemporary investigation system.

V. EVIDENTIARY AND LEGAL CHALLENGES IN BOTH FORENSIC SYSTEMS

Both conventional and digital forensic systems are important to the contemporary investigations but both have huge evidentiary and legal hurdles that affect their efficacy in the court of law. Classical forensic investigates actual, physical evidence, and cyber forensics is carried out in a place where evidence is ephemeral, intangible, and widely geographically distributed. Crime is becoming more and more hybrid, with physical activity being accompanied by digital footprint, and legal system has to contend with new issues of admissibility and authenticity, compliance with the process, and access across jurisdictions. This part examines these difficulties in more detail to identify the loopholes that remain between the practice of science and the expectations of the law.

5.1 Evidentiary Challenges in Traditional Forensics

Courts generally hold traditional forensic evidence to be true, although, its accuracy relies on the way it was handled on the crime scene, the accuracy of the laboratory, and the expert testimony. The initial difficulty is seen in the contamination risk, where biological samples (blood, DNA or trace materials) are vulnerable to mishandling or improper packaging. Interpretive subjectivity is another problem of this kind - for example, bloodstain pattern analysis or bite-mark examination has in certain instances been accused of relying on expert interpretation as opposed to deterministic science. Moreover, when forensic labs have backlogs, it means that the process of analysis can be slowed, which interferes with the chain of custody. Courts also question the use of validated scientific protocols, use of calibrated instruments, and the competency of the experts. Therefore, although physical evidence is deemed to be powerful, the admissibility of such evidence is frequently based on procedural accuracy and expert reliability as opposed to evidence.

5.2 Evidentiary Challenges in Cyber Forensics

The situation with cyber forensics is much more complicated as the digital evidence is volatile and can be easily modified. One of the main issues is volatility - the information in RAM, processes or network traffic may disappear in some seconds. Also, encryption, anonymisation networks (VPNs/Tor), remote wiping, or cloud storage are frequently used by criminals, and it can be hard or impossible to recover such data in a timely manner. It is also essential to establish the authenticity of evidence, which is legally required and necessitates forensic hashing (MD5, SHA-1) to indicate that there has been no manipulation of evidence. The cyber evidence, unlike the traditional forensics, may be at numerous geographic locations, which creates problems in jurisdiction in cases where the servers are in a foreign country. Chain of custody is more complex as digital imaging, duplication, and transfer are accompanied by several stakeholders and software programs. Due to such reasons, courts tend to be suspicious or doubtful when admitting digital evidence unless all the procedures of the recovery work are properly documented.

5.3 Legal and Procedural Challenges Across Both Systems

The two areas of forensics have common law complications albeit presented in diverse ways. Among them is the requirement of admissibility, including the Daubert or the Frye test in most jurisdictions that any scientific evidence must be both reliable and peer-reviewed and generally accepted in the field of practice. Although conventional forensics has decades of validation history, cyber forensics changes at an extremely high rate to the point in which legal standards tend to be behind technological reality. Privacy and constitutional rights is another significant difficulty especially in the course of cyber investigations. Gaining access to a device, decryption and access to information stored in the cloud can be in conflict with personal privacy rights, and it is essential to strictly follow the search warrants and authorisation of laws. Also, cyber investigations often require intercountry cooperation, which

requires mutual legal assistance treaties (MLATs) that may postpone evidence retrieval. Legal scrutiny of traditional forensics extends to expert reliability, method disclosure, presentation in court, but since the sciences involved with this field of activities are established, legal acceptance is mostly easier.

5.4 Interpretive and Judicial Challenges

Scientific findings have to be interpreted by courts that lack scientific knowledge which exposes them to misinterpreting them or relying too heavily on them based on expert statements. Under traditional forensics, judges have to consider probabilistic matches in DNA, trace comparisons or ballistics interpretations with no misconception of accuracy levels. In the field of cyber forensics, the judges have to judge the logs, packet captures, metadata trails or malware analyses which are highly technical and need specialised interpretation. In a case where the legal system is not digital literate, there exists a risk of under-valuing or over-valuing cyber evidence, resulting in unequal dispensing of justice. This demonstrates the necessity of judicial education, revision of legal codes and better cooperation of the forensic community and the legal community.

Both cyber and traditional forensic systems in spite of their scientific underpinnings face serious evidentiary and legal limitations in their transition out of the investigation phase and into the court of law. These problems should be known because they want to strengthen the forensic reliability and bring justice up with the technological development.

VI. REAL-WORLD APPLICATIONS AND CASE STUDIES ACROSS BOTH DOMAINS

Perhaps, the practical aspect of the sphere of forensic science can be considered to be best seen within the context of a practical situation where science directly applies into the identification of a crime, the identification of a suspect, and the ultimate conviction of a crime suspect. Traditional and cyber forensics have led to landmark cases resolutions and this proves that these two disciplines are indispensable in contemporary criminal justice. Although traditional forensic science has been successful in understanding physical, biological, and chemical evidence, cyber forensics has proven to be essential in a more computerized world, whereby evidence is usually stored, relayed or manipulated using computer-like equipment. The combination of these areas explains a symbiotic ecosystem of investigative tactics that reacts to the criminal behaviour changes. The section that follows discusses major case studies in the two areas, their methodological strengths, and operational difficulties, and the modes of interpretation employed by researchers.

6.1 Traditional Forensic Case Studies

Case Study 1: The Nirbhaya Case (2012) – DNA, Serology, and Trace Evidence

The classic forensic science featured prominently in one of the most well-publicised crime cases in India, as the reconstruction of the assault was carried out using the method of traditional forensic science, as well as associating the perpetrators to the crime. DNA profiling of the biological samples at the victim and the bus identified the individuals with a high level of statistical certainty to the accused. The forensic story received support through serological testing, fibre examination and trace materials like hair, blood droplets and clothing damage. The case also proved that physical evidence can be used to get people to convict, despite inconsistent or incomplete witness accounts. It also pushed to the fore the fact that India is becoming more dependent on scientific means of rapid processing of evidence when it comes to high-stakes crimes.

Case Study 2: The Aarushi–Hemraj Double Murder Case (2008) – Limitations in Crime Scene Management

This opportunity showed the merits and demerits of the conventional forensics in India. Fingerprinting, bloodstain pattern analysis, and weapon reconstruction were tried but as the crime scene was early mishandled, the crime scene was contaminated and the evidence was lost. The presence of unsealed rooms, disturbed rooms by more than one visitor and slow evidence gathering, despite the techniques used, destroyed the results despite the advanced techniques. As it is presented in this case, the highly advanced forensic tools turn out to be ineffective unless crime scene measures are followed strictly.

Case Study 3: O.J. Simpson Trial (1995) – Chain-of-Custody as a Decisive Factor

The case of the O.J. Simpson murder trial in the United States is a classical example in the impact in which the integrity of evidence has on the outcomes of the judicial process. Even though forensic evidence, including DNA analysis and fibre comparisons, radically incriminated the suspect, the defence counsel could debate the standards of chain

of custody and laboratory handling, and possible contamination. The case was a reminder to the world forensic practitioners that even scientific evidence irrespective of its possible accuracy must be backed up with a perfect procedural rigour.

6.2 Cyber Forensic Case Studies

Case Study 4: The Indian ATM Malware Heist (2018) – Log Analysis and Malware Tracking

In 2018, there was a massive ATM based cyberattack on Cosmos Bank ATMs, where attackers stole almost 94 crore by co-ordinating malware attacks and committing international fraud. The cyber forensic teams were investigating the logs of the server, network packet and hacked SWIFT systems to track the route of intrusion. The reverse engineering of the malware was useful in the identification of script-based malicious commands that had by-passed authentication mechanisms. The case demonstrated that cybercrime syndicates are highly complex and specialised digital investigation skills are needed.

Case Study 5: Bengaluru Bitcoin Scam (2020)- Blockchain Forensics on Practice.

Among the high-profile frauds was money laundering through the crypto currency provider of large sums of money. The police would use blockchain college technology to track wallet addresses, transaction routes, and exchange locations. Although cryptocurrencies provide pseudonymity, identities of the persons involved might be traced by tracing the KYC logs of IPs and timestamps and dereferencing the logs. The case unveiled the current approaches of research in relation to criminal activities founded on blockchain.

Case Study 6: Sony pictures Hack (2014) - Attribution by Digital footprints.

The cross-border attack cyber forensics was exhibited by hacking of Sony pictures entertainment by a group of people connected to North Korea. Malware signature, command-and-control infrastructure, linguistic patterns, and IP address routing were analyzed by them. The attribution was based on the matching of similarities in code of malware with past attacks, and this shows that cyber forensics can create behavioural profiles similar to how traditional profiling was made but using digital artefacts.

6.3 Integrated Forensic Case Studies: When Both Domains Converge

Case Study 7: The 26/11 Mumbai Attacks (2008) – Synergy of Physical and Digital Evidence

The Mumbai terror attacks involved using both the traditional and cyber forensic tools at the same time. Traditional forensics examined explosives, guns, DNA of dead attackers and ballistic precipitations. The cyber forensics monitored GPS, VoIP communication, mobile phones, and the internet-based logistics the attackers were utilizing. This multi-layered study indicated that hybrid forensic models were needed in recent terrorist incidents.

Case Study 8: Child Trafficking & Online Exploitation Rings – Digital Trails Supporting Physical Rescues

Cyber forensics (IP tracking, social media profiling, analysis of encrypted chats) can be used to initiate investigations into organised child exploiting networks, but conventional forensic measures (victim identification, fingerprint analysis, medical examination, etc.) are still used in their resolution. This synergy operation makes sure that the digital trace is converted into action of ground level enforcement.

Case Study 9: Corporate Espionage Incidents – Dual Evidence Streams

Intellectual property theft cases often combine internal surveillance videos, physical access logs and traces of document manipulation with electronic evidence in the form of email history, USB usage, and the logs of data egression. These types of hybrid cases bring out the fact that the contemporary workplace crime scene is both physical and digital.

6.4 Cross-domain Case Study Analytical Insights.

In all these case studies, it was proved that:

1. Traditional forensics remains essential in a crime that involves a physical injury, environmental evidence, and/or biological evidence.
2. Cyber forensic is now essential in the crime that is perpetrated using the digital system, remote networks or anonymity via the internet.
3. Combination of investigations is a new way of doing things especially in matter touching on terrorism, financial crimes, and organised transnational offences.
4. The interdisciplinary cooperation among laboratory scientists, cyber experts, crime scene investigators, and other legal professionals is gaining more importance in investigative success.

5. The procedural integrity plays a significant role in case outcomes and is not limited by technical complexity of the situation- the mistake in the chain-of-custody or information on the paper assumptions may suppress even the best scientific evidence.

VII. CONCLUSION: TOWARDS AN INTEGRATED FORENSIC FRAMEWORK FOR THE DIGITAL ERA

The crime in a twenty-first century has prompted the development of forensic science to shift back and forth towards a more sophisticated and hybrid model, which embraces both the material and digital realms. The old or classical forensic science based on biology, chemistry, physics, and forever history of the Exchange Principle of Locard, has given the courts a way to trust the physical evidence and reenact the crime as well as how and why the human being is involved in the criminal activity. At the same time, cyber forensics has become an indispensable science in the world in which criminal behaviour is becoming more and more expressed through digital networks, remote communication, and technologically mediated interaction. Co-existence of these two systems is no longer a choice but a structural requirement of the modern investigative agencies, law institutions and security systems.

A forensic integrated approach recognizes that the distinction between physical and digital crime scenes is becoming increasingly unclear. Digital tools, online communication, or the electronic storage of information are now common in terrorism, financial fraud, organised crime and even conventional violent offences. On the other hand, most cybercrimes also cause physical outcomes, and therefore, a traditional forensic validation is carried out by examination of documents, fingerprinting, or biological samples. The cases that have been taken into consideration in the two spheres indicate that none of the systems is sufficient; however, together, these two systems enable the investigators to construct coherent stories, attribute blame in a more refined manner and present a multidimensional image of evidence that cannot be disputed in court. The nature of such synergy is that piece of evidence, whether founded on a fingerprint, a server log, etc, contributes to a bigger picture of the crime.

However, the transition to an integrated structure also shows the critical problems that should be considered to ensure forensic dependability. The legal systems must react to the novel form of digital evidence, not by simply setting and maintaining the high admissibility guidelines, but by training the judges, prosecutors, and defence counsel to understand technology. The investigative organizations should invest in post-modern laboratory, interdisciplinary training, integrated chain-of-custody systems to link the traditional and digital processes. The fact that the crimes of the modern times are hybrid in nature is also important as it demands modernized laws that will enable the forensic processes to be grounded in science and morally reasonable. Without these reforms, the shortcomings of the procedural norms or the interpretation of the evidence might be bound to compromise the outcomes of the judicial procedure.

In the end, the future of forensic science is in creating a single and interoperable and scientifically sound framework that harmoniously combines both physical and digital techniques. These types of frameworks should focus on the accuracy, transparency and inter-disciplinary partnership but should be flexible enough to follow the fast-changing technologies and criminal behaviour patterns. Due to the growing interdependence of societies and the increased dependence on technology, the criminal justice system needs to be as dynamic, holistic, and futuristic in their forensics. An actually integrated forensic model will not only increase the efficiency of the investigative process and the credibility of the evidence presented but will also make the people more confident in the judicial system once again, and science will be invaluable in the process of pursuing justice in the digital age.

REFERENCES

[1]. “Mukesh & Anr vs State for NCT of Delhi & Ors” (2017 May 5). AIR 2017 SCC 2161. Supreme Court of India. Retrieved from https://indiankanoon.org/doc/68696327/ Indian Kanoon

[2]. Acharya, A. B. (2013). The ‘Nirbhaya’ Delhi gang rape case: A forensic odontology overview. *Journal of Forensic Dental Sciences*, 5(2), 169–173.

[3]. Acharya, A. B. (n.d.). The ‘Nirbhaya’ case (New Delhi) – forensic odontology case summary. Retrieved from https://ashithacharya.com/cases ashithacharya.com

[4]. Anonymised. (2023). Forensic science and its limitations in rape and murder cases: A study

of Indian context. *Journal of Forensic Sciences & Medicine*, 9(1). https://journals.lww.com/jfsm/fulltext/2023/09010/forensic_science_and_its_limitations_in_rape_and.17.aspx LWW Journals

[5]. Bose, D. (2013). Forensic DNA profiling in the Nirbhaya rape case. *Economic & Political Weekly*, 48(40), 15–18.

[6]. Broadhurst, R., & Chang, L. Y. (2013). Cybercrime and industrial espionage. *Handbook of Cybercrime*, Routledge.

[7]. Central Bureau of Investigation v. Dr. Rajesh Talwar & Nupur Talwar, Sessions Trial No. 477/2012 (Ghaziabad CBI Court, 2013).

[8]. CrowdStrike. (2020). *Global Threat Report: State-Sponsored Espionage and Insider Threats*.https://www.crowdstrike.com/resources/reports/

[9]. Federal Bureau of Investigation. (2014). *Update on Sony investigation*. FBI Press Release.https://www.fbi.gov/news/press-releases/update-on-sony-investigation

[10]. Govindarajan, V., & Bhaskar, A. (2025). Forensic odontology in sexual offences – a review based on decided cases. *Multidisciplinary Review*, 8, e2025207. https://doi.org/10.31893/mr.2025207 ResearchGate

[11]. Haggard, S., & Lindsay, J. R. (2015). North Korea and the Sony hack: Exporting instability through cyberspace. *Asia-Pacific Issues*, No. 117, East-West Center. https://www.files.ethz.ch/isn/191548/api117.pdf ETH Zurich Files

[12]. INTERPOL. (2020). *Global Assessment: Online Child Sexual Exploitation*.https://www.interpol.int/en/Crimes/Crimes-against-children/Child-sexual-exploitation

[13]. Ismail, M. (2017). *A case study analysis of the Sony Pictures Entertainment hack* (Master's thesis). University of Southern Mississippi. https://aquila.usm.edu/masters_theses/360/

[14]. Ismail, M. (2017). A case study analysis of the Sony Pictures Entertainment hack. (Master's thesis). University of Southern Mississippi. Retrieved from https://aquila.usm.edu/cgi/viewcontent.cgi?article=1360&context=masters_theses Aquila Digital Community

[15]. Jadhav, R. (2018, August 14). Cosmos Bank loses $13.5 million in cyber attack. *Reuters*. https://www.reuters.com/world/india/cosmos-bank-loses-135-million-cyber-attack-2018-08-14/

[16]. Jadhav, R. (2018, August 14). Cosmos Bank loses $13.5 million in cyber attack. *Reuters*. https://www.reuters.com/article/world/cosmos-bank-loses-135-million-in-cyber-attack-idUSKBN1KZ1J8/ Reuters

[17]. Kiwia, D., Dehghantanha, A., Choo, K.-K. R., & Slaughter, J. (2018, July 27). A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. arXiv. https://arxiv.org/abs/1807.10446 arXiv

[18]. Kolesnikov, O. (2018). Cosmos Bank SWIFT/ATM U.S. $13.5 million cyber attack: Detection using security analytics. *Securonix Threat Research*. https://www.securonix.com/blog/cosmos-bank-attack/

[19]. Kolesnikov, O. (2018). Cosmos Bank SWIFT/ATM US$13.5 million cyber attack — detection using security analytics. *Securonix Threat Research*. Retrieved from https://www. securonix. com/blog/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/ Securonix

[20]. Lynch, M., & Jasanoff, S. (1998). Contested identities: Science, law, and forensics in the O.J. Simpson case. *Social Studies of Science*, 28(5–6), 675–697.

[21]. Mohd. Ajmal Amir Kasab v. State of Maharashtra, Criminal Appeal No. 373–374 of 2012 (Supreme Court of India).

[22]. Mukesh & Anr. v. State for NCT of Delhi, Criminal Appeal Nos. 607-608 of 2017 (Supreme Court of India, May 5, 2017). https://indiankanoon.org/doc/68696327/

[23]. Nuna, A., & Gupta, T. (2024, December 23). *The role of forensic evidence, DNA tests, and narco-analysis in the Indian legal system*. SSRN. https://doi.org/10.2139/ssrn.5069346 SSRN

[24]. Pathak, A., Sharma, R. D., & Dey, D. (2018, April 11). How vulnerable are the Indian banks: A cryptographers' view. arXiv. https://arxiv.org/abs/1804.03910 arXiv

[25]. People of the State of California v. Orenthal James Simpson, Case No. BA097211 (Superior Court of California, 1995).

[26]. Quayle, E., & Jones, T. (2011). Sexual exploitation of children online: Forensic and

investigative responses. *Child Abuse & Neglect*, 35(8), 627–635.

[27]. Raghavan, V. (2009). 26/11 Mumbai attacks: Lessons for forensic investigation. *Journal of Defence Studies*, 3(2), 75–92.

[28]. Ram Pradhan Committee. (2009). *Report on the 26/11 Mumbai Terror Attacks*. Government of Maharashtra.

[29]. Rao, T. S., Raveesh, B. N., & Srinivasan, K. (2015). Aarushi case: A forensic and legal analysis. *Indian Journal of Psychiatry*, 57(4), 433–437.

[30]. Sharma, D. (2018). An insight into the awareness and utilization of "dental forensics" in India. *Journal of Forensic Dental Sciences*, 10(2), 83-88. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6080160/ PMC

[31]. Sharma, P. (2014). Aarushi: The anatomy of a murder. *HarperCollins India* — includes documentation of forensic lapses.

[32]. Singh, A. (2022). Cryptocurrency crime and blockchain forensics in India. *International Journal of Cyber Research*, 4(1), 21–29.

[33]. The Hindu Bureau. (2021, January 30). Bitcoin scam: CCB submits 11,000-page chargesheet. *The Hindu*. https://www.thehindu.com/news/national/karnataka/bitcoin-scam-ccb-submits-chargesheet/article33696557.ece

[34]. Weinstein, I. (1996). DNA evidence in the O.J. Simpson trial. *Journal of Law and Policy*, 4(2), 439–455.