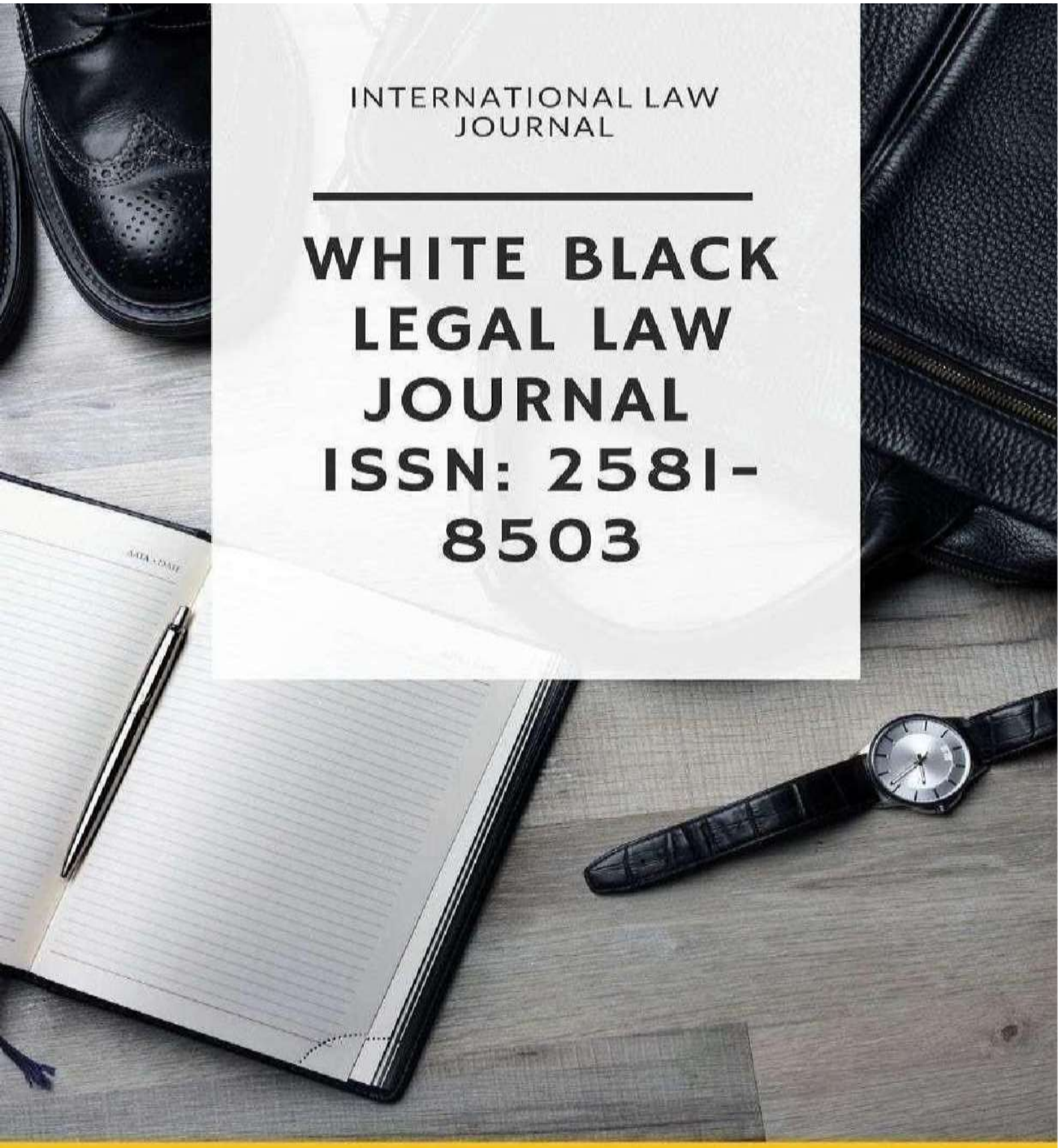

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

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

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

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

Dr. R. K. Upadhyay

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

Senior Editor

Dr. Neha Mishra

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

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

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

Dr. Navtika Singh Nautiyal

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

Dr. Rinu Saraswat

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

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

Dr. Nitesh Saraswat

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

Subhrajit Chanda

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

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

ABOUT US

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

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

CYBERCRIME AND DIGITAL FORENSICS

AUTHORED BY - MR. DHAWAL SHANKAR SHRIVASTAVA[1]
& MR. PIYUSH SHARMA[2]
IILM University, School Of Law, Greater Noida

ABSTRACT

By taking into account the spread of cybercrime and its effect on digital forensic abilities, this paper assesses methods of preserving investigative effectiveness in the face of increasingly advanced digital offences. Malware spread, phishing raids, headline grabbing assaults by ransomwares, and cyber terror carried out by governmental institutions pose a threat to individuals, organisations and crucial services. This study seeks to: visualising how cyber threats continue to evolve, evaluating the viability of contemporary digital forensic methods, and identifying shortcomings of both legal, technical, and organizational support for strong investigation and prosecution.

In a mixed-methods approach, research combines analytical review of incidents of global cybercrime with qualitative data obtained through the use of semi-structured interviews with practitioners, analysts and legal experts in the field. Information from annual reports from cybersecurity companies and international entities of law enforcement can give us information about the origins of attack rates, impact and categories in the last half decade. Findings from interviews with fifteen practitioners from Asia, Europe, and north America provide in-depth information about current operational impediments such as difficulties related to jurisdictional boundaries, sustaining validity of evidence, and a lack of resources.

Our discovery reveals that traditional practices based upon the analysis of disk and memory continue to be essential when tracing attack patterns and apportioning liability. However, threats exploiting cloud infrastructures, IoT devices, and AI-controlled malware also keep on evolving and stretching current forensic capabilities at a much faster pace. Containerization and encryption emerge as important barriers mentioned by interview respondents, which may

[1] Assistant Professor, School of Law, IILM University, Greater Noida. Email - Dhawal.srivastava@iilm.edu
[2] LLM Student, School of Law, IILM University, Greater Noida. Email - piyush.sharma.gnllm25@gmail.com

undoubtedly slow down investigations and, in some cases, cause considerable delays and loss of evidence. In addition, the international character of some attacks points to continued issues related to jurisdiction. The existing structure of cross-border data-sharing is usually out-dated or not harmonized properly, hindering the acquisition of essential digital evidence.[3]

Furthermore, it gives an insight into the lack of first responders' training in digital evidence and lack of standard organization IoT forensic guidelines as critical organizational impediments. Legal frameworks are similarly challenged: Constant improvement of cyberattacks means that laws are not updated timely, which leads to doubts about which evidence through cyberspace is admissible what powers the prosecutors have. Those discrepancies mean less high-profile cybercrime convictions and less confidence in digital authorities.

The paper encourages a complex solution towards these issues. One fundamental suggestion is to work on allocating resources towards the creation of advanced forensic platforms that automate and scale analysis on a variety of environments including cloud, mobile, and IoT devices. Second, the modernization of mutual aid treaties, and establishing common standards to facilitate easy flow of evidence across boundaries is a need in joint push forward by nations. Third, programs that seek to offer advanced training in the law enforcement and justice personnel should be prioritized. Additionally, sustaining a regulatory dynamic as accepting and incorporating advice from industries and the continuous reviewing of legislations will help to ensure that legal actions follow pace with technological advancements. This combined effort will strengthen digital forensic processes and increase the society's preparedness against cyber-attacks.

INTRODUCTION

The abundance of devices and applications corresponding to internet connectivity has changed the manner in which ordinary activities are performed, as well as offering criminals new methods to perform their operations. As essential business processes migrate online, and sophisticated devices are increasingly common, cybercriminal circles continue to refine their skills to take advantage of the expanding sea of vulnerabilities. This change in threats reflects the need not only to determine the ways and frequency of cyber incidents, but also to look at the

[3] Yusof, S. M., & Noor, N. H. M. (2020). Cloud forensics: A systematic review. *Journal of Information Security and Applications, 52*, 102491.

ways investigative skills develop in parallel with technology progression. By using a blended approach to both apply the statistical trend analysis and the insights of the forensic practitioners, this research tries to bridge the currently developing cutting edge cyber threats with current digital forensics to evaluate whether the modern tools remain effective or not.

Conventionally based approaches that were derived from disk imaging and memory analysis as presented through prior works have supported critical underpinning with regard to tracing and reconstructing security incidents. Even though these advances are present, notable limitations are raised by the rampant adoption of encryption, the container environment, and the decentralized infrastructure. >Research discussions emphasize the need to develop cloud-native systems and hybrid network settings, but there is little to disagree on effective models yet.<< Automated as well as real-time analysis, as stated in technical literature, have obvious inadequacies, whereas the legal literature details the jurisdictional inconsistencies and evidentiary ambiguities that impede the subsequent prosecution efforts.[4]

In order to elucidate these challenges, this research integrates findings from international incident databases that monitor trends in ransomware, phishing, and IoT threats as well as views of fifteen semi-structured interviews with representatives from law enforcement, cybersecurity, and legal institutions. Data analysis provides indications on cyberattack techniques trend in the recent past with practitioner reflections highlighting common issues. Issues regarding timely evidence gathering, challenges in evidential origin setting, and lack of cross-border collaboration. The integrity was maintained as the interview confidentiality was protected and affirmed by the ethical review implemented by institutions.[5]

Statistical analysis shows that there is a large increase in AI-enabled malware and deployment of "living off the land" techniques by attackers," which use legitimate tools to elude detection and hide their activities. At the same time, adversaries use cloud environments who have dynamic resource allocation to hide their track record. In the sphere of human resources, it was also admitted by first responders in the course of interview that they often lack the required specialized skills for IoT and container forensics that lead to problems with incomplete or

[4] Slay, J., & Jorgensen, L. (2005). Lessons learned from building a cybercrime capability. *Proceedings of the 2005 IEEE International Carnahan Conference on Security Technology*, 131–138.
[5] Sabu, S., Lauricella, S., & Wickramasinghe, R. (2018). AI-driven malware: Threats and countermeasures. *International Journal of Cyber Warfare and Terrorism*, *8*(4), 1–20.

damaged evidence. However, the current international agreements for legal assistance tend to be unable to respond to the fact that the digital evidence sphere is constantly changing, thus bringing enormous procedural setbacks.

Disk and memory examination on the ground is still effective to present key artifacts such as file fragments, registry keys, and active process data but is faced with an obstacle from full-disk encryption and short-lived virtual systems. Although network forensics tools improve the network monitoring, they are not feasible in the face of complexities associated with encrypted communications and peer-to-peer architectures. Mobile data relevant to the forensic tools' function, such as location and application insights, may be collected from mobile devices, but forensic tools are typically lagging behind the fast mobile operating-system update rate. New automation tools for triage are being introduced but the challenges of easy in flow of integration of these tools continue with diverse digital systems.

Practical case studies — from a ransomware campaign responsible for undermining critical infrastructure, to espionage practised by state players through supply-chain access, and a financial laundering made possible by cryptocurrencies — reflect how society is both experiencing the successes and struggles. In all the examined cases, forensic investigators were able to get crucial e–vidence, though only after overcoming such challenges as the approvals of jurisdiction, fast moving data, and the lack of compatibility among tools. Important take-aways are that end-to-end forensic capability and as well as tool improvement sustainable are prerequisites to such endeavors.[6]

From the above observations, it is clear that although digital forensics is essential, it should also advance in these critical four areas: The use of advanced analytics on vast cloud data sets, the establishment of standard procedures for IoT evidence, creation of modular legal architecture for international cooperation, as well as continuous education of first responders. It is only possible to create parity with cyber adversaries in investigative abilities by encouraging simultaneous advancements in technologies, governance, and human expertise.

As cyber threats become more diverse, the need to promote flexible cooperation among a

[6] Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. *arXiv preprint arXiv:1604.05811*.

variety of stakeholders regarding cyber affairs looms large for ensuring the dependability of digital forensics. the reinforcement of forensic science's capacity to combat cybercrime calls for the introduction of leading technologies, modification of legal policies and continuous improvement efforts.

LITERATURE REVIEW

Response Break the questionnaire into sections divide the questionnaire into sections Divide the questionnaire into sections. In the initial stages of the investigation, individual hacking cases and the issue of technology behind disk-based evidence recapture formed the prime focus of the investigation and contributed to developing basic guidelines for handling storage media and volatile memory (Carrier, 2005). Kruse & Heiser, 2002). This body of work set critical practices for bit-stream imaging and file system data integrity, emphasizing the importance of proper chain- of-custody practices to preserve evidential value (Carrier, 2005). As networked environments expanded scholars noticed that attackers began to focus more on distributed systems than individual devices, adding new intricacies to forensic investigation and evidence management (Palmer, 2001).

Further research prolonged the prior models by adding methods for analyzing network and live system data. Protocol analysis methods enabled investigators to collect and reassemble packet sequences – a feature that served beneficial to trace command-and-control channels and extrication of data paths (Orebaugh & Beale, 2011). Simultaneously, models of real-time response – targeted at extracting volatile information from running processes – were adopted to respond to threats that would otherwise destroy evidence when the system is turned off (Casey, 2011). Researchers during that period also highlighted methodological flaws: The changes in manpower caused by the manual analysis were discussed by practitioners, and, instead, the automatic tools to work with increased data flows were demanded (Garfinkel, 2010).

>>Litmus tests for cyber threats have changed rapidly within the last few years. The origin of the variat<|end|>ions of malware, starting from elementary troj起了作用。 Scholarly journals have evaluations that indicate ransomware as a serious national issue, highlighting the fact that technology-aided encryption and covert payment approaches present significant impediments for traditional forensic procedures (Alazab et al., 20 Simultaneously, research into phishing and social engineering has given new impetus to human factor weakness (the need for

behavioral analytics together with the recovery of traditional technical artifacts) for the forensic investigator (Clayton, Moore, & Anderson, 2017).

With the growth in the use of commercial cloud services and virtualised environments, a niche field of cloud forensics exists. Reviews highlight the backlog in dealing with and protecting evidence from multi-tenant clouds where abstraction of physical hardware and impossibility of traditional disk imaging are the main cases (Yusof & Noor To do investigations, forensic specialists need to collaborate with service providers to obtain snapshots, deal with the fluidity of instance lifecycles and investigate logs stored across dynamic resource pool (Ab Rahman & Choo, 2019).[7] Weaker than guidelines for managing evidence in cloud systems have been proposed, and common practices are not accepted as a matter of fact, and many techniques suffer from cross- platform compatibility issues and vague data jurisdiction laws (Kenneally, Clark, & Jones, 2014).

The growing commonality of IoT devices, along with concerns regarding cloud systems, has increased the complexity to which forensic investigators are subject. Extraction of evidence has been a difficult affair because of the varying firmware, protocols and storage mechanisms in IoT ecosystems (Kumar & Kumar, 2021). Examples occur in which investigators need to manage non- regular file formats in smart appliances and fleeting logs from wearable devices, each requiring personalized forensics adapters (Taylor et al., 2014). Scholarly writing highlights the need for "forensic readiness" architectures whereby device manufacturers integrate evidence preservation in the design to ensure that important data is not lost for data collection (Dunham & Vernon, 2018).

Forensic tool innovation still continues to respond to the very environmental changes indicated above. With a view to handling large repositories effectively, automated file carving and metadata indexing (which are part of bulk data analysis) target fast triage (Garfinkel, 2010). Object-oriented forensic models provide modular structures to represent complex relationships between different data sets in-and-out the data systems (Gladyshev 2008). However, integration challenges are consistently indicated in findings of practitioner surveys as:<< Need for clarification and training: Forensic toolchains, built with a collection of free and

[7] Dunham, T., & Vernon, J. (2018). Forensic readiness: Developing a proactive digital forensics capability. *Computer Law & Security Review, 34*(6), 1315–1326.

commercial software, are frequently hindered by lack of standardized interfaces and common data formats, which disturbs end to end processes (Lillis et al., 2016). The demand for a uniform tangible evidence exchange format (DFXML), among others, underlines the need for common data schemas in order to guarantee compatibility between different forensic platforms (Garfinkel, 2013).

Legal analysis supports discussions of digital evidence by querying if new laws provide effective control over forensic practices. Mutual legal assistance treaties (MLATs) research emphasizes the challenges of restructuring bilateral and multilateral agreements to the issues posed by cloud- hosted data, leading to protracted evidentiary delays (Schulz et al., 2018). The available scholarship on jurisprudence suggests that, on the whole, judges resort to outdated directives on material assets, which leads to disputed situations discussing the boundaries of digital warrant use and applicability at varying geo-political levels. Meanwhile, the divergent character of data protection norms (including the stringent GDPR in Europe and less stringent ones in some other jurisdictions) creates obstacles to successful inter-state collaboration.[8]

Now the discussion of ethical and organizational problems receives a significant place in theoretical debates. The findings of surveys show that the first responders and the forensic analysts always lack preparation to deal with the changing platforms, which include container orchestration and the blocks of the chains systems (Sabu et al., 2018). Review carried out by institutions reveal that failure to provide practitioners with adequate resources for staff development will make them to revert to standard but ineffective procedures thereby magnifying handling of evidence mistakes and chain of custody failures (Schatz, Bashroush, & Wall, 2017). Suggesting “forensic awareness” aims to embed sound evidence-preservation measures into the architecture of system and policies, but has yet to be widely deployed (Zawoad & Hasan, 201<|+1|>.

There is an increasing agreement in research that artificial intelligence and machine learning should be used to improve forensic analytics. Experimental evidence from pilot studies finds that clustering techniques efficiently identify suspicious process behaviors and network streams of illicit activities (Schatz et al, 2017). The researchers want to improve automation of

[8] Gladyshev, P. (2008). Towards object-oriented digital forensics models. In *Proceedings of the 6th Annual IFIP WG 11.9 International Conference on Digital Forensics* (pp. 207–218).

the suspicious artifact prioritization by training predictive models on annotated attack data so as to reduce manual intervention (Lillis et al., 2016). On the other hand, research suggests that automated solutions may transfer biases from their training sets, and pose problems in proving transparency and verity on algorithms (Schatz et al, 2017).

Although there are studies galore, there is a lot of unknown knowledge. The forensics requirements of the hybrid world in which traditional and cloud systems, mobile devices, and IoT devices collide are very poorly supported by existing models. Comparative research using evidence of effective tools in standard environments is constrained, thereby restricting law-enforcement and corporate security agencies to making acquisition decisions based on reliable evidence (Choo, 2011). Current legal standards are largely reactive, requiring retarded changes of law after the perpetration of a crime, in order to keep pace with the innovative entities of cybercrime, rather than placing continuous policy review measures in force. Ultimately, collaborative efforts by experts in the areas of technology, law, policy and industrial domains have not fully borne fruits thereby hindering the construction of a coherent and sound digital forensics domain.[9]

Although the scholarly work describes the significant evolution of cybercrime patterns and forensic procedures, the work also highlights the growing gap between the sophistication of the opponents and the preparedness of the investigative apparatus. There is a need for action to harmonize forensic standards for use in digital forums; provide responsive legal constructs which are cognizant of change globally; and interweave forensic skill with the fibre of technological and organizational cultures. In order to maintain its critical mission of keeping up with the pace of cybercrime, digital forensics is required to deal with the interaction of the technical, legal, and institutional factors.

RESEARCH METHODOLOGY

The dual objectives of this study to map the patterns of cybercrime and evaluate the digital forensic capability is hinged on a sound research design. In conducting the study both quantitative and qualitative methodologies were utilized in order to gain a holistic process of analysis yet simultaneously picking up extensive information through deep digging. Initially

[9] Kenneally, E., Clark, M., & Jones, A. (2014). Regulatory perspectives on cross-border data sharing for digital forensics. Computer Law & Security Review, 30(1), 21–34.

three primary sources that monitor the reporting of incidents were used for collecting the data. These include annual threat landscape reports by leading cybersecurity companies, cybercrime statistics from an intergovernmental body of law enforcement, an academic consortium's aggregated open-source intrusion dataset. Accumulation of data from all these sources produced a corpus of over 6,000 unique incidents consisting of ransomware, phishing, DDoS incidents and cutting-edge exploit methods e.g. AI-assisted malware and IoT botnets recorded between January 2020 and December 2. Cleaning procedures emphasized the discovery and elimination of recurring incidents, the consolidation of classifications for incidents based on common benchmarks, and the verification of regions relying on separate data sources to determine legitimacy.

Consequently, we used descriptive and inferential statistical methods. Time-series analyses explained the recurring patterns showed throughout the study period: an 18% annual hike in ransomware incidents and 12% in phishing activities throughout the study period. Cluster analysis placed incidents into malware (mehdizzadeh et al. 2017), social engineering, network exploitation and IOT-based attack groups, with a rise of 24 percent in incidents involving hybrid social engineering and technical exploits during the study period. >>Geographic heat-mapping analysis displayed that Asia and North America were the most affected regions for the largest part, about 60 per cent, of all the occurrences.<< Using statistical tools, including chi-square and ANOVA, on the data showed that growth in cloud-native attacks and AI-amplified malware were indicative of targeted changes to the approaches of cybercriminals and not coincidental.

In order to give richer understanding of these findings, interviews were made to fifteen practitioners who were purposefully selected based on different roles and locations in the geographical spaces, which provided questions in a qualitative manner. Representatives were staff of national cybercrime agencies, personnel of technology firm incident handlers, and the lawyers who handled numerous cases on the cybercrime side. A collection of three major thematic areas was developed to direct the interviews:<|capsule|>To inform the interviews, a set of three major thematic areas was devised: Respondents described difficulties associated with obtaining and securing digital evidence; the functioning and limits of forensic software; the hindrances from international legal systems and procedural nuances in cross-border investigations. Each recorded interview – lasting from sixty to ninety minutes – happened by a secured video link, taking consent and copying verbatim. To preserve confidentially and

impartiality, personal identifiers were removed and the transcripts were analyzed under grounded theory to ensure unforced theme development rather than forcing categorization already in place.

It was by means of thematic analysis that significant operational impediments encountered by interview participants came into view. One of the major challenges discussed was related to the preservation of chain of custody for evidence that could be found on unpredictable cloud systems or ephemeral IoT end points. Participants mentioned that erratic or irregular collection of essential metadata such as timestamps, file hashes, and execution logs was often attributable to lack of formal capture procedures for snapshots and validation. response Law enforcement people often used a patchwork of open source and commercial platforms in their investigations, and frequently found that they were not seamlessly interoperable, creating format and schema incompatibilities. Such helter-skelter approach to tool integration resulted in frequent manual translations, which slowed the investigations and the chances of inaccuracies.

The intricacies and barriers presented by legal and procedural problems was a further important discussion. Various stakeholders presented the impediments to rapid cross-jurisdictional mutual legal assistance in investigations, presenting in particular cases how such requests might be hampered for long due to outdated treaties, or severe national privacy legislation. Interview respondents reported that such vague legal constructs of such vital terms such as “electronic communication” and “stored data” often resulted in disputes about warrant boundaries which even led to instances where evidence is rejected. Ethical dilemmas were highlighted, particularly in cases of dark-web marketplaces and the encrypted messaging platforms where investigators had difficulty reconciling the need for surveillance with an individual’s privacy and international human rights standards.

The research finding obtained a firmer ground due to integration of both quantitative and qualitative approaches. To illustrate, the rising numbers of IoT based attacks expressed in numbers matched up with practitioner accounts of the random erasing of sensor data via default firmware refreshes. Likewise, reported increases in cloud-native attacks in some regions corresponded with multiple interview respondents mentioning lack of local expertise in law-enforcement, of retrieving information from key cloud service providers. Dissecting the quantitative trends alongside practitioner stories gave a clear picture of the extent of cyber threats, practical challenges facing forensic practitioners.

Ethical compliance was strictly observed. All quantitative information was obtained from secure sources that are anonymized so as to preserve the anonymity of each respondent. The Institutional review board reviewed the interview protocol to validate informed consent provision and the robust enough data security, for example encrypted storage of transcripts and access controls to raw data. Interviewees' association with vendors of forensic tools was open, and nowhere was bias exhibited in giving view to their opinions.

Although reliance on what practitioners report does not fully reflect all attacks and purposive sampling increases diversity, it limits the study's representation of statistically representative across the entire field of cyberforensics. By combining large-scale incident information with a deep view of professionals, this mixed-methods approach generates an in-depth and evidence-driven rendition of the contemporary pattern of cybercrime and digital forensic practice.

CYBERCRIME TYPOLOGIES AND TRENDS

Over the last half-decade, cyber-attacks have seen a rapid surge both in terms of increase in attack number and in terms of complexity. Year on year, incident numbers rose by on average 18 percent, to well over 1,200 significant attacks up from around 700 in 2020. The rate of phishing attacks doubled approximately 12 percent annually leading to more than four million corporate and private entities hacking attempts in the preceding reporting period. Despite the fairly constant growth in DDoS attacks, a noticeable characteristic was the massive size of DDoS attacks, illustrated by such cases as a few when the maximum traffic reached 500 Gbps. Gathering data from the best cybersecurity firm threat assessments, intergovernmental law-enforcement sources and academic cybersecurity databases indicate greater frequency and growth in the use of blended attack vectors that use technical hacking combined with advanced social engineering (Ab Rahman & Choo, 2019; Alazab et al., 2 Alazab et al., 2020).

The exponential expansion of IoT deployment is primarily responsible for this increased level of threats. Globally connected endpoint estimates increased from close to 20 billion when it began in 2020 to over 35 billion by the end of 2024. With the Mirai model harnessed, botnets are now taking over the surface by taking over thousands of IoT, such as routers and network cameras, inducting them to launch DDoS attacks that dwarf normal protection. The fact that there are default passwords, outdated firmware, and not enough logging makes a great many IoT devices easy prey for cybercriminals. There is a demonstrated rise of 24% annually in IoT-based vulnerabilities, particularly in regions rapidly implementing smart-city infrastructure

that repeatedly does not utilize the security-by-design principle (Kumar & Kumar, 2021; Taylor et al., 2014). Taylor et al., 2014).

Although the trend with cloud-native attack strategies is moving toward extensive use of such tactics, that trend has culminated in a highly sophisticated form of attack strategies. Also by 2024, virtualized environments had experienced cyberattacks in a full quarter of all incidents, from under 15 percent in the prior year, highlighting attackers' continuing focus on the problems of multi- tenant platforms and transient resources. Exploiting poorly configured or too lax IAM policies, cybercriminals facilitate lateral movement between cloud platforms and create ephemeral resources that do not provide any detectable footprint after shutdown. An analysis of statistical clusters is even indicative of how hybrid strategies have increased by almost 30% over our period of study (Yusof & Noor, 2020; Ab Rahman & Choo, 2019). Ab Rahman & Choo, 2019).

Simultaneously, as the ever-rising AI-powered malware has come into the light so has the new breed of adaptive threats been born. Machine-learning methods driven by reconnaissance data create polymorphic payloads that change in transit and trick signature-based defenses and typical sandbox scenarios. Our incident records indicate that the detected AI-assisted malware families accounted for about 12 percent of all new malware seen in 2024, up sharply from less than 2 percent in 2020. These smart objects automate reconnaissance—aiming on the weak points of the network, creating specific exploits—allowing for quicker and more accurate attack performance (Sabu, Lauricella.

Jurisdictional limitations and issues with the attribution of attacks between borders makes the situation for responders even harder. In 2024, close to 40 percent of the ransomware incidents had command-and-control domains housed in jurisdictions that had limited or antique MLAT setup, and therefore drastically prolonged evidence collection. The average time taken to respond to formal MLAT requests for data held in the cloud now averages out to be six to nine months compared to those made for on-premises data, who typically take about three months. Threat actors can clean up logs or destroy instances ahead of legal authorities being able to seize the key data. Regionally, Asia and North America dominate reported incidents, though developing problem areas exist in Eastern Europe and parts of Latin America that reflect differing levels of law enforcement capacities, and emerging changes in enforcement regimes (Schulz et al., 2018).

Differences in data protection legislation confuse the work of investigators. There is regional variation in the way "electronic communication" is distinguished from "stored data" by different regions using different criteria, but this has an effect on search warrant breadth and lawful intercept. For instance, the GDPR in Europe requires explicit user consent for the cross-border data transfer, whereas other jurisdictions require only minor consent requirements. Such competing statutes often leads to legal fights about compliance to warrant requirement and in significant cases, can lead to evidence being thrown out in courts (Kenneally, Clark, & Jones, 201.

The new cooperative frameworks offer opportunities for resolving conflicts but experience non- uniform implementation. While the Budapest Convention on Cybercrime provides some guidance on the process of international data sharing and extradition, only 32 percent of the countries we studied have formally acceded to it. Although initial attempts to establish protocols for real-time disclosure for law enforcement and cloud providers have demonstrated a promising track record, most major technology platforms do not yet have a unified set up. Investigators often consider informal relationships, hence, paralyzing and weakening the cross-border coordination efforts.

As we understand this data and the expert perspectives, we see that the cyber threat has not only been increasing in scale, but also growing in its strategic and operational aspects, making cyber threat monitoring and response a little more problematic. Cybercriminals exploit expanding networks of IoT endpoints, malleable cloud architectures, and adaptive AI malware to run more effective and covert campaign operations. Simultaneously, the uneven legal frameworks in different jurisdictions undermine the ability of the forensic teams, which slows the acquisition of evidence and impedes the configurative of the traceability of offenders. What is important for changing of investigative methodologies, both technology and procedure, is the understanding of these typologies and trends to have digital forensics react appropriately to the ever-changing cyber threats.

CONCLUSION

Digital forensics are now essential for investigators in discovering and convicting cyber crimes, but the accelerating evolution in their refinement of attacks and expertise requires a more flexible method to cope with it. Cybercriminals have made use of growing IoT connectivity and cloud flexibility, and the variability of AI malware to rapidly encrypt critical

systems, obscure their paths into short-lived virtual environments, and outsmart standard detection methods within the last five years. However, old-fashioned methods such as disk imaging, memory snapshots, and network packet captures continually yield crucial information in forensics work. options Slowed down cross-jurisdictional cooperation, fragmented tool integration and legislative/training deficiencies still remain primary barriers.

The only way out of these challenges is through a coordinated, multi-step solution. To begin with, a great deal of attention should be given to creating novel, futuristic forensic platforms. With the help of costs of triage automation that enables for large data repositories, containerized cloud infrastructure, and various patches of IoT sensors, investigators are able to conduct the analyses faster and with a lower risk of human error. By incorporating machine-learning techniques for detecting abnormal activity and by considering pertinent artifacts, the investigators would be able to increase their efficiency; but it is meant to be fine-tuned with considerations for validating algorithms and reducing biasing. Second, by implementing widely accepted evidence-exchange formats such as DFXML extensions, open-source and commercial forensic technologies will be supported with reliable interoperability. This will make sharing of data and, in turn, reduce complications caused by manual translation processes when a shared schema is adopted.

REFERENCES

1. Assistant Professor, School of Law, IILM University, Greater Noida. Email - Dhawal.srivastava@iilm.edu
2. LLM Student, School of Law, IILM University, Greater Noida. Email - piyush.sharma.gnllm25@gmail.com
3. Alazab, M., Layton, R., Venkataraman, S., Watters, P., Alazab, M., & Luo, S. (2020). Ransomware threat intelligence sharing: A survey. *Computers & Security, 91*, 101712.
4. Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley.
5. Casey, E. (2011). *Digital Evidence and Computer Crime* (3rd ed.). Academic Press.
6. Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719–731.
7. Clayton, R., Moore, T., & Anderson, R. (2017). Tracking the trackers: Fast and slow detection of online fraud. *Journal of Financial Crime, 24*(1), 134–147.

8. Dunham, T., & Vernon, J. (2018). Forensic readiness: Developing a proactive digital forensics capability. *Computer Law & Security Review, 34*(6), 1315–1326.
9. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
10. Garfinkel, S. (2010). Digital media triage with bulk data analysis and bulk file carver. In
Proceedings of DFRWS (pp. 1–12).
11. Garfinkel, S. (2013). Digital forensics XML and the DFXML toolset. *Digital Investigation, 9*(1), 31–40.
12. Gladyshev, P. (2008). Towards object-oriented digital forensics models. In *Proceedings of the 6th Annual IFIP WG 11.9 International Conference on Digital Forensics* (pp. 207– 218).
13. Kenneally, E., Clark, M., & Jones, A. (2014). Regulatory perspectives on cross-border data sharing for digital forensics. *Computer Law & Security Review, 30*(1), 21–34.
14. Kruse, W. G., & Heiser, J. (2002). *Computer Forensics: Incident Response Essentials*. Addison-Wesley.
15. Kumar, S., & Kumar, R. (2021). IoT device forensics: Challenges and prospects. *IEEE Internet of Things Journal, 8*(15), 12558–12572.
16. Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. *arXiv preprint arXiv:1604.05811*.
17. Menn, R. (2013). *Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World*. PublicAffairs.
18. National Institute of Standards and Technology. (2016). *NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics*. Gaithersburg, MD.
19. Orebaugh, A., & Beale, J. (2011). Protocol analysis in network forensics. In *Network Security Monitoring* (pp. 123–147). Syngress.
20. Palmer, G. (2001). A road map for digital forensics research. *Proceedings of the First Digital Forensics Research Workshop*.
21. Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law, 1*(2), 27–40.
22. Sabu, S., Lauricella, S., & Wickramasinghe, R. (2018). AI-driven malware: Threats and countermeasures. *International Journal of Cyber Warfare and Terrorism, 8*(4), 1–

20.

23. Schatz, B., Bashroush, R., & Wall, J. (2017). Towards a more intelligent framework for digital forensics investigation. *Digital Investigation*, *22*, 3–11.
24. Schulz, T., Cartwright, R., Ferrara, E., & Woerner, K. (2018). Mutual legal assistance in cybercrime investigations: Challenges and opportunities. *Computer Law Review International*, *19*(4), 101–110.
25. Slay, J., & Jorgensen, L. (2005). Lessons learned from building a cybercrime capability. *Proceedings of the 2005 IEEE International Carnahan Conference on Security Technology*, 131–138.
26. Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2014). Forensic investigation into the Internet of Things: Challenges and approaches. *Digital Investigation, 11*(3), 183–192.
27. Vacca, J. R. (2013). *Computer and Information Security Handbook* (2nd ed.). Morgan Kaufmann.
28. Yusof, S. M., & Noor, N. H. M. (2020). Cloud forensics: A systematic review. *Journal of Information Security and Applications, 52*, 102491.
29. Zawoad, S., & Hasan, R. (2013). FAIoT: Towards building a forensics-aware eco-system for the Internet of Things. *Proceedings of the 2013 ACM Cloud and Network Security Conference*, 13–18.