Pakistan Journal of Criminology
Vol. 16, No. 02, April—June 2024 (119-132)

Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations

Naeem AllahRakha[1]

Abstract

As cybercrimes grow more sophisticated, network and cloud forensics have become vital investigative tools. However, complex legal, ethical, and practical challenges around extraterritorial evidence, privacy rights, volatile data, and specialized skills constrain these processes. This study critically reviews academic literature and industry reports to examine these multifaceted considerations holistically. It aims to aggregate the latest insights around regulations, technical protocols, certification regimes, and international cooperation frameworks shaping network and cloud forensics. The study follows qualitative research methodology, a doctrinal approach used for the analysis of regulation, and grounded theory used for the analysis of related literature. The results reveal gaps around the liability limitations of internet service and cloud providers, ethical bounds for ancillary data collection, and anti-forensic obfuscation techniques. Proposed solutions include accountability in technology design through transparency and oversight. Simplify procedures for cross-border legal assistance requests. Develop lightweight encryption methods that still enable lawful access as well as promote collaboration between industry and academia to advance cybersecurity tools.

Keywords: Network Forensic, Cloud Forensic, Digital Investigation, Legal Framework, Digital Evidence

Introduction

With the continued advancement of digital technologies, network and cloud forensics have become indispensable tools for investigating cybercrimes. However, the complexity of these environments also raises critical legal, ethical, and practical challenges that must be addressed for the accountability of the culprits (Pollitt, Caloyannides, Novotny, & Shenoi, 2004). Fundamentally, network and cloud forensics involve extracting and analyzing digital evidence from networks, hosts, applications, and cloud platforms to uncover traces of malicious or criminal activity. However, entities like internet service providers, cloud providers, and software vendors have no consistent legal obligation to

[1] The author is a professional lawyer and a member of the Punjab Bar Council and Lahore High Court Bar Association. He can be reached at chaudharynaeem133@gmail.com ORCID: 0000-0003-3001-1571

support investigations, leading to issues accessing relevant data (Opara-Martins, Sahandi, & Tian, 2016). The collecting network or cloud evidence can impose on bystander privacy, and tracing attacks across national borders runs into jurisdictional constraints (Fereday & Muir-Cochrane, 2006). On the practical front, the volatile and encrypted nature of digital evidence, chain of custody complexities, and the need for specialized skills make network and cloud forensics inherently complicated (Malik et al., 2024).

Network forensics is a specialized field within digital forensics that focuses on monitoring and analyzing computer network traffic for various purposes, including information gathering, legal evidence, and intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. It's crucial for organizations to exercise caution when dealing with potential attacking IP addresses, as responding to them can't conclusively confirm the identity of the attacker and may inadvertently alert them, leading to potential destruction of evidence or further attacks. Analysts in this field should utilize a range of tools suited to different situations and be mindful of their limitations. Network forensic analysis tools offer features such as reconstructing events, visualizing traffic flows, profiling activity, and searching for specific keywords within application content, all of which contribute to effective network forensics investigation and analysis (Guan, 2014).

A network source is a set of defined IP addresses. The IP addresses can be public IP addresses or IP addresses from VCNs within your tenancy. A common sources of network-based evidence have a variety of elements, including traffic logs documenting communication activities, packet captures providing detailed snapshots of data transmission, firewall rules delineating network access permissions, router configurations outlining network infrastructure setups, and user account records tracing individual interactions. Additionally, application and operating system logs offer insights into system activities, while alerts from Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) flag potential security breaches. Furthermore, network forensic investigators rely on hardware and software components like servers and printers, along with wireless network data from LANs, MANs, PANs, and WANs, each offering distinct connectivity parameters. Network forensic investigators examine two primary sources: full-packet data capture and log files from devices such as routers, proxy servers, and web servers. These files identify traffic patterns by capturing and storing source and destination IP addresses, TCP ports, Domain Name Service (DNS) site names, etc. (Rodrigues et al., 2017).

Cloud forensics involves the application of digital forensic methods in cloud computing environments to investigate criminal activities, such as data

breaches or identity thefts that occur using cloud services. This field requires experts to employ specialized techniques to detect and analyze evidence within cloud systems, ensuring its integrity and admissibility in legal proceedings. Investigators collaborate with various cloud actors, including providers, consumers, brokers, carriers, and auditors, to facilitate internal and external investigations effectively. Ensuring the integrity of evidence requires adherence to stringent legal and regulatory standards to uphold the validity of findings in legal proceedings. Ultimately, cloud forensics safeguards digital assets and holds perpetrators accountable for their actions in the evolving landscape of cybercrime (Simou, Kalloniatis, Kavakli, & Gritzalis, 2014).

Cloud computing revolutionizes how data is stored, managed, and processed by utilizing remote servers over the internet rather than local infrastructure. It offers three primary service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides virtualized computing resources over the internet, such as servers and storage, as exemplified by Amazon Web Services (AWS) and Microsoft Azure. PaaS offers a platform allowing developers to build, deploy, and manage applications without dealing with the underlying infrastructure, as demonstrated by Google App Engine and AWS Elastic Beanstalk. SaaS delivers software applications over the internet on a subscription basis, like Gmail, Slack, and Microsoft Office 365, eliminating the need for installation and maintenance. Each model caters to specific needs, providing flexibility, efficiency, and cost-effectiveness in managing IT resources (Bello et al., 2021).

The widespread adoption of cloud services has significant ramifications for digital forensic investigations. The distributed architecture of cloud environments adds layers of complexity regarding evidence acquisition (Awuson-David et al., 2021). Investigators must identify and coordinate with relevant cloud providers, submission managers, and infrastructure owners to collect artifacts. However, legal ambiguity around jurisdictional boundaries and multi-tenancy arrangements often constrains this process (Bacon et al., 2017). Moreover, the virtualized nature of cloud platforms obscures the location of relevant logs and records needed to recreate attack timelines (Liyanage, Braeken, Shahabuddin, & Ranaweera, 2023). Tracing attacks also become complicated by the geo-distribution and federation of cloud assets across vendors. Consequently, some scholars argue for establishing international forensic standards tailored to the cloud ecosystem, spanning legal agreements, technology requirements, and methodology guidelines to enable credible investigations (NIST, 2020).

The Internet of Things (IoT) represents a vast network of interconnected devices, enabling communication between them and the cloud, as well as among

the devices themselves. Examples include connected cars, smart appliances, security systems, agricultural equipment, retail, healthcare monitors, manufacturing machinery, and urban infrastructure. In the realm of digital forensics, it stands out for its broader scope of potential evidence sources, extracting data directly from smart environments like kitchen appliances and wearable devices. This branch of forensics relies on sensors embedded in various IoT devices to collect and transfer data to the cloud for storage and analysis. Cybersecurity measures are essential for safeguarding these interconnected devices and their networks from cyber threats and attacks, ensuring the integrity and security of IoT ecosystems (Atlam et al., 2020).

Literature Review

Network forensics refers to the capture, recording, and analysis of network events to discover the source of security attacks or other problem incidents (He et al., 2016). Meanwhile, cloud forensics is the application of scientific methods toward identifying, collecting, validating, analyzing, interpreting, documenting, and presenting digital evidence derived from cloud computing resources (Sammons, 2015). As cyberattacks grow increasingly sophisticated, network and cloud forensics have become indispensable tools for investigating cybersecurity breaches and crimes (Abiodun et al., 2022). However, several complex legal, ethical, and practical challenges confront digital forensic practitioners and law enforcement agencies (Wilson-Kovacs et al., 2023). There's no consistent legal obligation across jurisdictions to compel internet service providers (ISPs), cloud providers, and vendors to preserve or share digital evidence with authorities (Hörnle, 2021). Developing standardized regulations globally is complicated by issues like data sovereignty, liability assignments, privacy rights, etc. (Cuno et al., 2019).

The collecting of extraterritorial evidence also faces uncertain international cooperation, authorization delays, or outright rejection (Stephan, 2023). Scholars identify notable regional differences in legal approaches. The US leans toward imposing strict mandates on service providers to support government investigations. In contrast, the EU prioritizes data protection and privacy rights (Taylor, 2023). Network and cloud forensics also raise ethical challenges regarding individual privacy and civil liberties. Tracing the source of cyberattacks often requires collecting ancillary data from uninvolved third parties, which could reveal sensitive personal information unrelated to the attack (Skopik & Pahi, 2020). Furthermore, the backdoors developed for forensic collection purposes could also be exploited illegally by rogue elements, violating user privacy

(Aacoub et al., 2022). Hence, technical implementations must be cautiously designed to avoid overstepping ethical bounds.

On the applied front, practitioners face complications like criminal obfuscation techniques, anti-forensics, jurisdictional constraints, certification requirements for tools, budget constraints, and steep learning curves in unpacking encoded evidence (Reedy, 2023). Practical issues like volatility and encryption of collected artifacts, broken chains of custody, and the need for specialized skills under strict regulations. Developing pragmatic strategies to address these multifaceted technical challenges remains an open research problem (Stoykova, 2021). The full potential of network and cloud forensics requires resolving legal ambiguities, upholding ethical norms, and tackling practical complexities through collaborative efforts between legislators, technologists, and forensic experts globally (Dhirani et al., 2023).

Methodology

This study employs a qualitative literature review methodology to critically examine the legal, ethical, and practical considerations in network and cloud forensics. Relevant academic articles and industry reports published over the past 5 years are systematically identified from scientific databases like IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar using a defined search strategy. The search terms include "network forensics," "cloud forensics," "digital investigations," combined with "regulation," "privacy," "evidence," "tools," etc. in multiple permutations. Around 400 highly cited articles meeting the quality and topical relevance criteria are selected for in-depth review. Thematic analysis is applied to categorize the key issues, challenges, and recommendations along a legal, ethical and practical dimensions discussed across these sources.

Specific aspects like jurisdictional constraints, privacy implications, volatility of evidence, certification needs, etc. are coded accordingly. Additional governmental reports and technology standards from organizations like ISO, NIST, etc. supplement the analysis to incorporate applied perspectives. The coded themes help to develop a holistic, evidence-based understanding of the multifaceted considerations shaping the current state and future direction of network and cloud forensics. The distribution of the challenges across categories is quantified to prioritize the key issues statistically. Finally, new recommendations are synthesized to advance legal frameworks, ethical guidelines, and technical capabilities supporting network and cloud investigations. This methodology enables the derivation of actionable, pragmatically grounded recommendations through a rigorous qualitative literature analysis process.

Results

Standards ensure the integrity and reliability of network and cloud forensics processes. In digital forensics, where evidence collection and preservation are paramount, adherence to established standards is essential for maintaining the admissibility of evidence in court. For network forensics, the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) have developed guidelines to ensure the validity and reliability of investigative methods. ISO/IEC 27041:2015 provides guidance on ensuring the suitability and adequacy of incident investigative methods. This standard helps investigators conduct thorough examinations of network infrastructures, ensuring that evidence is collected in a manner that preserves its integrity and authenticity.

Similarly, for the analysis and interpretation phases of network forensics, ISO/IEC 27042:2015 offers guidelines to ensure consistency and accuracy in examining digital evidence. These standards help forensic analysts utilize appropriate tools and methods to uncover relevant information from network data, ensuring that findings are reliable and defensible in legal proceedings. Cloud forensics, which involves investigating digital evidence stored on cloud computing platforms, presents unique challenges due to the distributed and dynamic nature of cloud environments. To address these challenges, standards such as ISO/IEC 27037 provide guidelines for the identification, collection, acquisition, and preservation of digital evidence in cloud settings. These standards assist forensic practitioners in navigating the complexities of cloud infrastructures while adhering to best practices for evidence handling.

Discussion

Evidence gathering must adhere to legal protocols to ensure admissibility in court. Photographs and other evidence can be challenged on grounds of authenticity, relevance, fairness, accuracy, and prejudice. A photograph should be a fair and accurate representation of the scene as it appeared to the person taking the photograph and others who were present at the time (Madison, 1984). Demonstrative evidence, like photos, explains testimony. Substantive evidence comprises collected exhibits. Both require establishing relevance and probative value without undue prejudice (Brain & Broderick, 1991). The evidence must represent the original crime scenes fairly and accurately. Investigators usually need warrants or valid consent before processing scenes. Moreover, the exclusionary rule bars evidence obtained illegally. Likewise, evidence must have a fully documented chain of custody, which is maintained by a series of signatures

as the evidence passes from hand to hand until it reaches a designated custodian (Badiye, Kapoor, & Menezes, 2024).

Investigators serve as factual witnesses, restricting opinions to their domain expertise. While an individual qualified as an expert witness can offer opinion testimony, the defense can hire their own experts. If the defendant's pockets are deep enough and the stakes are high enough, the defense can always find someone with impressive credentials to offer a contrary opinion. However, experts may face rigorous cross-examination and rebuttals from counter-experts. Photographs persist as visual evidence, reminding jurors of key facts. Investigators should also photo-document the absence of expected artifacts. Accidental associations that ingress scenes before isolation require extensive scene photography as relevance determination occurs later (Sanders, 2009).

Courts apply exclusionary rules to render certain types of logically relevant evidence inadmissible to advance procedural fairness, incentivize diligence, allocate error risks, or serve other policy goals (Turner & Weigend, 2019). The admissibility of digital evidence also faces restrictions beyond bare relevance. A key requirement is authenticating the integrity of digital artifacts entering the judicial record. Investigators must fully document scene isolation, collection, storage, and analysis protocols to demonstrate no tampering or contamination. Chain of custody logs indicating handling by various custodians provide additional validation. These authenticity safeguards uphold fairness while engendering public trust in verdicts relying on digital evidence.

Exclusionary rules may also apply specifically to certain digital evidence types. For instance, logs of chat conversations could constitute hearsay if submitted to establish asserted facts. However, they may still be admissible to show a contextual user mindset. Similarly, rules constraining the admission of character evidence could bar presenting an accused’s browsing history to demonstrate a propensity for criminality. Nevertheless, judges enjoy discretion in evaluating digital evidence within case specifics. On the applied side, practitioners require extensive training to forensically acquire and parse various digital artifacts while avoiding spoliation. Certification regimes are emerging to validate baseline expertise. Moreover, wide adoption of encryption and anti-forensics techniques poses escalating practical hurdles for evidence harvesting (Roberts, 2022).

Failing to maintain forensic data can have severe legal implications for companies, especially considering the stringent regulations surrounding data protection and privacy. These regulations, such as HIPAA, GDPR, and CCPA, mandate that organizations implement reasonable measures to safeguard personal information. Failure to comply can result in hefty fines and legal action. One significant legal implication is the requirement to notify affected individuals and

regulatory authorities promptly in the event of a data breach. For instance, under the GDPR, companies must notify the Information Commissioner's Office (ICO) within 72 hours of discovering a breach. In the United States, state attorneys general and various regulatory bodies like the Federal Trade Commission (FTC) must also be informed. Failure to report breaches promptly can lead to substantial penalties, as demonstrated by Marriott's $124 million fine for a delayed breach notification (Khaled, Pattel, & Siddiqui, 2020).

The companies failing to maintain forensic data may face challenges in demonstrating their commitment to resolving breaches lawfully. Legal experts advise promptly seeking counsel upon discovering a breach to determine the appropriate timing and recipients for breach notifications. This proactive approach is crucial in mitigating further damage and maintaining a positive standing with regulators and the public. Furthermore, without comprehensive forensic data, it becomes challenging for companies to investigate and address breaches effectively. This lack of evidence can hinder legal proceedings and regulatory compliance efforts, potentially exacerbating the consequences of a breach (Johnstone & Sarre, 2004).

Public cloud environments pose significant challenges for digital forensics investigations due to the inherent jurisdictional complexities and difficulties in data retrieval from large-scale distributed infrastructure. A key issue is that data in the cloud can be stored redundantly across multiple physical servers located in different legal jurisdictions across the world. This makes the determination of ownership, privacy protections, and applicability of local laws ambiguous (Dove et al., 2015). Investigators require proper legal authority like warrants and subpoenas to retrieve relevant evidence, which is hard to enforce given the rapid data replication and migration capabilities of public clouds. Moreover, public cloud vendors may not readily capture or release customer data to investigators due to privacy protection laws and confidentiality agreements. Negotiating access to protected data causes delays. Even if obtained, decrypting and analyzing extremely large volumes of customer data from public cloud servers is technically challenging (Abiodun et al., 2022).

Principles of ethical behavior in digital forensics are essential to ensuring fairness, integrity, and respect for individuals' rights. Beneficence and nonmaleficence underscore the importance of acting in the best interests of all involved while avoiding harm. Fidelity and responsibility demanded an unwavering commitment to truthfulness and accountability in handling evidence. Integrity ensures that investigators maintain honesty and transparency throughout the process. Justice mandates equal treatment and adherence to legal standards, safeguarding against bias or discrimination. Respect for people's rights and dignity

requires protecting privacy and upholding confidentiality. Accurate representation of qualifications, maintaining evidence integrity, and truthful data representation are paramount. Clear documentation, impartial examination, and testimony contribute to impartiality and credibility. Confidentiality must be upheld, and violations must be reported to uphold professional standards (Jahn, 2011).

Ethics in digital forensics ensure investigations are conducted with integrity and respect for individuals' rights. Professionals in this field establish trust and authenticity in their work by adhering to principles such as protecting privacy, maintaining evidence integrity, and complying with legal standards. Ethical considerations guide forensic analysts to approach their tasks without bias, ensuring the credibility of the investigation process. In cybersecurity, ethical practices are essential for preserving the integrity of investigations and ensuring that digital evidence is used responsibly and lawfully. Expert handling of forensic evidence is imperative to produce accurate results, as ethical lapses can significantly impact the outcome of criminal cases (Irons & Konstadopoulou, 2001).

Conclusion

Digital forensics is used to catch lawbreakers via the data they use. And this involves collecting, analyzing, and organizing electronically stored information (ESI) so that attorneys can present it in court. Digital devices like computers, mobiles, and IoT gadgets are increasingly being used in crimes ranging from financial fraud, homicides, and child pornography to cyber stalking, theft of trade secrets, and terror plots. They also contain vital evidence to reconstruct the sequence of events and prove or refute allegations, even in traditional crimes not directly involving technology abuse. Hence, digital forensics has become indispensable for modern investigations. While crime labs handle securing digital evidence and analysis, lawyers play a crucial role in determining what is relevant, advising on retrieval procedures, evaluating implications, and contextualizing evidence presented in court.

For effective discharge of these responsibilities, a basic grasp of common digital forensic tools and techniques is vital for any practicing lawyer today. Digital forensics is a rapidly evolving field, and it is important for lawyers to stay up-to-date on the latest techniques and technologies. One needs awareness of the capabilities and limitations of data extraction and analysis methodologies to guide investigators on sources of potential evidence on devices, clouds, and networks, examining timelines of file manipulations, internet usage traces, etc. Knowledge of common artifacts like registry keys, metadata tags, access logs, etc. allows assessment of the authenticity and integrity of evidence by recovering, analyzing,

and presenting digital evidence. It helps uncover the truth and hold individuals accountable.

The technical implications of recovering and handling digital evidence that may be altered, encrypted, or remotely wiped need consideration for maintaining the evidentiary chain of custody. Factors affecting the reliability of forensic tools in extracting usable data from damaged devices, overwritten files, and complex media like RAM and cryptographic volumes have legal relevance to admissibility. Capabilities to retrieve information from locked devices and various file formats facilitate evidence discovery. Electronic data has a significant role in legal matters, especially given that's how most sensitive information is stored today. With advances in technology, the way trial lawyers obtain evidence for their clients is constantly changing. Digital forensics is how evidence is obtained from digital media in a defensible manner. With proprietary data formats and privacy-enhancing technologies commonplace, lawyers should cultivate working knowledge of standard forensic protocols, data recovery techniques, cryptography, steganography, and networking essentials. Keeping up with the state of the art would enable sound legal counsel and the interpretation of digital evidence, better assisting the judiciary, clients, and the public interest.

Recommendations

In digital investigations, network and cloud forensics uncover evidence essential for solving cybercrimes and ensuring digital security. However, with explosive growth in cloud adoption and networked devices, traditional digital forensic approaches need rethinking to address emerging complexities in investigations involving such environments. To ensure the integrity and admissibility of evidence, organizations should establish clear protocols and procedures for conducting network and cloud forensic investigations. This includes documenting the chain of custody, defining the roles and responsibilities of investigators, and adhering to industry best practices such as those outlined by organizations like ISO (International Organization for Standardization) and NIST (National Institute of Standards and Technology).

As cyber threats continue to evolve, investing in advanced forensic tools and technologies is paramount. This includes utilizing machine learning algorithms for anomaly detection, employing block-chain technology for ensuring data integrity, and leveraging artificial intelligence for automating certain aspects of the investigation process. Establish international coordination frameworks clearly defining the jurisdictions, liabilities, and duties of public cloud providers to support forensic data access and analysis under legal authorization. Organizations should invest in regular training programs to ensure that investigators are

equipped with the latest knowledge and techniques in network and cloud forensics. Drive further R&D into lightweight, distributed forensic analytics models leveraging edge computing capable of on-site evidence analysis.

Collaboration between forensic investigators and legal experts is important for directing the legal complexities associated with network and cloud forensics. Legal experts can provide guidance on obtaining and preserving evidence in a manner that is admissible in court. As concerns around data privacy continue to escalate, it is imperative for organizations to implement comprehensive data privacy measures throughout the forensic investigation process. This includes obtaining consent from relevant parties before accessing data, anonymizing personally identifiable information (PII) wherever possible, and adhering to privacy regulations. Network and cloud forensics often require a multidisciplinary approach that combines expertise from various fields, such as computer science, law enforcement, cybersecurity, and digital forensics. Collaboration to continually advance forensic tools' capabilities against new intrusion vectors, encryption methods, anti-forensics tactics, and infrastructure complexity.

References

Abiodun, O. I., Alawida, M., Omolara, A. E., & Alabdulatif, A. (2022). Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 10217-10245. https://doi.org/10.1016/j.jksuci.2022.10.018

AllahRakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, 16(2), 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Atlam, H. F., Hemdan, E. E.-D., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2020). Internet of Things Forensics: A Review. *Internet of Things*, *11*, 100220. https://doi.org/10.1016/j.iot.2020.100220

Awuson-David, K., Al-Hadhrami, T., Alazab, M., Shah, N., & Shalaginov, A. (2021). BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. *Future Generation Computer Systems*, *122*, 1-13. https://doi.org/10.1016/j.future.2021.03.001

Badiye, A., Kapoor, N., & Menezes, R. G. (2024). *Chain of Custody*. StatPearls Publishing. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK551677/

Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., Ajayi, A. O., & Owolabi, H. A. (2021). Cloud computing in the

construction industry: Use cases, benefits, and challenges. *Automation in Construction*, 122, 103441. https://doi.org/10.1016/j.autcon.2020.103441

Brain, R. D., & Broderick, D. J. (1991). Demonstrative evidence: The next generation. *Litigation, 17*(4), 21–55. http://www.jstor.org/stable/29759484

Cuno, S., Bruns, L., Tcholtchev, N., Lämmel, P., & Schieferdecker, I. (2019). Data Governance and Sovereignty in Urban Data Spaces Based on Standardized ICT Reference Architectures. *Data*, 4(1), 16. https://doi.org/10.3390/data4010016

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors (Basel), 23*(3), 1151. https://doi.org/10.3390/s23031151

Dove, E. S., Joly, Y., Tassé, A.-M., Public Population Project in Genomics and Society (P3G) International Steering Committee, International Cancer Genome Consortium (ICGC) Ethics and Policy Committee, & Knoppers, B. M. (2015). Genomic cloud computing: legal and ethical points to consider. *European Journal of Human Genetics*, 23(10), 1271–1278. https://doi.org/10.1038/ejhg.2014.196

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods, 5*(1), 80–92. https://doi.org/10.1177/160940690600500107

Guan, Y. (2014). Network Forensics. In *Managing Information Security* (2nd ed., pp. 313-334). https://doi.org/10.1016/B978-0-12-416688-2.00011-8

He, J., Chang, C., He, P., & Pathan, M. S. (2016). Network forensics method based on evidence graph and vulnerability reasoning. *Future Internet*, 8(4), 54. https://doi.org/10.3390/fi8040054

Hörnle, J. (2021). Digital Investigations in the Cloud—Criminal Enforcement Cooperation. In *Internet Jurisdiction Law and Practice*. Oxford. https://doi.org/10.1093/oso/9780198806929.003.0006

International Organization for Standardization. (2015). ISO/IEC 27041:2015 — Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method (1st ed.). https://www.iso27001security.com/html/27041.html

International Organization for Standardization. (2015). ISO/IEC 27042:2015 — Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence (1st ed.). https://www.iso27001security.com/html/27042.html

Irons, A. D., & Konstadopoulou, A. (2001). Professionalism in digital forensics. *Digital Evidence and Electronic Signature Law Review, 15*(1), 45-50. Retrieved from https://sas-space.sas.ac.uk/5584/1/1798-2461-1-SM.pdf

ISO/IEC. (2012). ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/standard/44381.html

Jahn, W. T. (2011). The 4 basic ethical principles that apply to forensic activities are respect for autonomy, beneficence, nonmaleficence, and justice. *Journal of Chiropractic Medicine*, *10*(3), 225–226. https://doi.org/10.1016/j.jcm.2011.08.004

Johnstone, R., & Sarre, R. (2004). *Regulation: Enforcement and Compliance*. Research and Public Policy Series No. 57. Australian Institute of Criminology. Retrieved from https://www.aic.gov.au/sites/default/files/2020-05/rpp057.pdf

Khaled, N., Pattel, B., & Siddiqui, A. (2020). *Digital Twin Development and Deployment on the Cloud: Developing Cloud-Friendly Dynamic Models Using Simulink®/Simscape® and Amazon AWS*. In Digital Twin Development and Deployment on the Cloud (pp. 11-20). https://doi.org/10.1016/B978-0-12-821631-6.00002-5

Liyanage, M., Braeken, A., Shahabuddin, S., & Ranaweera, P. (2023). Open RAN security: Challenges and opportunities. *Journal of Network and Computer Applications, 214*, 103621. https://doi.org/10.1016/j.jnca.2023.103621

Madison, B. V. III. (1984). Seeing can be deceiving: Photographic evidence in a visual age - How much weight does it deserve? *William & Mary Law Review*, *25*(4), 705. Retrieved from https://scholarship.law.wm.edu/wmlr/vol25/iss4/9

Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. *Sensors*, 24(2), 433. https://doi.org/10.3390/s24020433

National Institute of Standards and Technology. (2020, August). NIST Cloud Computing Forensic Science Challenges (NISTIR 8006). U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8006

Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. *Journal of Cloud Computing*, 5(4). https://doi.org/10.1186/s13677-016-0054-z

Pollitt, M., Caloyannides, M., Novotny, J., & Shenoi, S. (2004). *Digital forensics: Operational, legal and research issues*. In S. De Capitani di Vimercati, I. Ray, & I. Ray (Eds.), Data and Applications Security XVII (pp. 297-312). Springer. https://doi.org/10.1007/1-4020-8070-0_28

Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*, *6*, 100313. https://doi.org/10.1016/j.fsisyn.2022.100313

Roberts, P. (2022). *The Accused's Extraneous 'Bad Character'*. In Roberts, P., & Zuckerman, A. (Eds.), Criminal Evidence (3rd ed., pp. 257-279). Oxford. https://doi.org/10.1093/oso/9780198824480.003.0014

Rodrigues, G. A. P., Albuquerque, R. D. O., Deus, F. E. G., Jr., R. T. D. S., Júnior, G. A. D. O., Villalba, L. J. G., & Kim, T.-H. (2017). Cybersecurity and network forensics: Analysis of malicious traffic towards a Honeynet with

deep packet inspection. *Applied Sciences*, 7(10), 1082. https://doi.org/10.3390/app7101082

Sammons, J. (2015). The Basics of Digital Forensics. In *The Primer for Getting Started in Digital Forensics* (2nd ed., pp. 1-14). https://doi.org/10.1016/B978-0-12-801635-0.00001-2

Sanders, J. (2009). Science, Law, and the Expert Witness. *Law and Contemporary Problems*, 72(1), 63–90. http://www.jstor.org/stable/40647166

Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics: Identifying the major issues and challenges. In M. Jarke et al. (Eds.), *Advanced Information Systems Engineering: CAiSE 2014. Lecture Notes in Computer Science* (Vol. 8484). Springer. https://doi.org/10.1007/978-3-319-07881-6_19

Skopik, F., & Pahi, T. (2020). Under false flag: Using technical artifacts for cyber-attack attribution. *Cybersecurity*, 3, 8. https://doi.org/10.1186/s42400-020-00048-4

Stephan, P. B. (2023). International Law Futures. In *The World Crisis and International Law: The Knowledge Economy and the Battle for the Future* (pp. 251-282). Cambridge University Press.

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review, 42*, 105575. https://doi.org/10.1016/j.clsr.2021.105575

Taylor, M. (2023). Conceptual Approaches to Data Protection in the European Union and the United States. In *Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality* (pp. 18-32). Cambridge University Press.

Turner, J. I., & Weigend, T. (2019). The Purposes and Functions of Exclusionary Rules: A Comparative Overview. In S. Gless & T. Richter (Eds.), *Do Exclusionary Rules Ensure a Fair Trial?* (pp. xx-xx). Ius Gentium: Comparative Perspectives on Law and Justice, vol 74. Springer. https://doi.org/10.1007/978-3-030-12520-2_8

Wilson-Kovacs, D., Helm, R., Growns, B., & Redfern, L. (2023). Digital evidence in defence practice: Prevalence, challenges and expertise. *The International Journal of Evidence & Proof, 27*(3), 235-253. https://doi.org/10.1177/13657127231171620

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 21, 115–158. https://doi.org/10.1007/s10207-021-00545-8