Global Journal of Research in Management and Social Sciences
Vol. 1, Issue 1, September 2025
ISSN-Pending
Published by Wilma Global Journals
http://wilmajournals.org/index.php/gjrmss

FORENSIC EVIDENCE MANAGEMENT: STRENGTHENING THE CHAIN OF CUSTODY PROCESS IN THE NETHERLANDS

Dr. Annelies J. van Dijk[1] and Prof. Rutger P. Vermeer[2]
[1]Faculty of Law and Criminology, Utrecht University, The Netherlands.
[2]Faculty of Law and Criminology, Leiden University, The Netherlands.

Abstract

Forensic science plays a pivotal role in legal investigations, requiring meticulous handling of evidence to ensure credibility and reliability, especially in an era of rapid technological advancement. The chain of custody remains fundamental for documenting evidence management, preserving its authenticity and integrity from initial collection through to courtroom presentation. This process has become increasingly complex with the rise of digital evidence, which is highly susceptible to manipulation and tampering. Any breach in the chain of custody can render evidence inadmissible, jeopardising legal outcomes. This study conceptualises forensic evidence and evidence management within the theoretical frameworks of Systems Theory and Crime Scene Investigation (CSI) Theory, underscoring the interdependence of all stages of evidence handling. The empirical review highlights how strict chain of custody protocols significantly bolster evidence integrity, ensuring legal admissibility, reducing contamination risks, and enhancing accountability mechanisms. Key challenges in managing digital evidence include data complexity, cross-jurisdictional concerns, the demand for specialised expertise, and the necessity to keep pace with evolving technologies. The study concludes that maintaining a robust chain of custody supported by innovations such as blockchain and RFID is critical for preserving the reliability and admissibility of forensic evidence. Recommendations include developing uniform standards for digital evidence handling, implementing continuous training for professionals, establishing privacy-compliant guidelines, and investing in advanced technologies to improve security and traceability.

Keywords: Forensic, Evidence, Crime, Collection, Preservation, Chain of Custod

Introduction

Forensic science has evolved considerably over the past decades, drawing on multidisciplinary expertise to support legal investigations. Forensic professionals frequently appear as expert witnesses, and technological advancements have amplified the importance of rigorous evidence handling. The integration of science with law enforcement has revolutionised crime investigations, enabling more accurate case resolutions and strengthening the delivery of justice. Significant developments from early methods to advanced technologies such as DNA analysis continue to drive innovation within the criminal justice system (Mozayani & Parish-Fisher, 2018). Within this context, the chain of custody serves as a cornerstone of evidence management, documenting the chronological handling of physical and digital materials during criminal and civil proceedings (Longley, 2022). Maintaining a clear starting and ending point

of the chain of custody is critical to preserving authenticity and demonstrating that evidence remains unchanged (Longley, 2022).

According to Houck, Crispino, and McAdam (2017), only breaks in possession during the custody period compromise admissibility. Sustaining the chain of custody ensures the authenticity and integrity of evidence from its original state at the crime scene through courtroom presentation. Each custodian must understand their responsibility to protect the evidence and accurately document all transfers to preserve its probative value (Bórquez, 2011).

In the digital sphere, ensuring the reliability and trustworthiness of electronic evidence is increasingly important (International Organization for Standardization, 2015). Digital artefacts such as log files, text files, and emails are especially vulnerable to tampering and lack inherent authenticity measures (Casey, 2002). Although hash functions can verify data integrity (Rivest, 1992), they are insufficient on their own. The Digital Forensic Life Cycle — encompassing Acquisition, Identification, Collection, Reporting, and Preservation — provides a structured framework for managing digital investigations (International Organization for Standardization, 2012).

Maintaining a robust Chain of Custody (CoC) is essential for tracking changes and ensuring admissibility (Prayudi & Sn, 2015; Stoykova, 2023). Yet managing digital CoC poses distinct challenges, such as maintaining data integrity and preventing unauthorised alteration (Cosic & Baca, 2010; Giova, 2011; Lone & Mir, 2019; Prayudi & Sn, 2015). Innovative approaches are needed to protect the CoC, address the growing complexity of digital evidence management, and keep up with technological advances (Cosic & Baca, 2010; Prayudi & Sn, 2015).

Statement of the Problem

The management of forensic evidence represents a critical pillar of the criminal justice system, with the chain of custody serving as an indispensable mechanism for safeguarding evidence integrity and admissibility (Kubicz, 2017). However, maintaining an unbroken chain of custody is increasingly difficult, particularly in cases involving multiple items of evidence, diverse crime scenes, and numerous stakeholders (Butler, 2015). Research demonstrates that breaches or weaknesses in the chain of custody can result in evidence being ruled inadmissible in court, thereby undermining case outcomes (Saks & Koehler, 2005).

Scholars have consistently called for standardised protocols and comprehensive training to promote uniformity and competence in evidence handling practices (Houck, 2018). Despite these initiatives, procedural lapses and documentation errors persist, jeopardising the reliability of investigations and the fairness of court proceedings (Pierce, 2017). Moreover, the increasing complexity of forensic evidence, particularly the growth of digital evidence, presents new challenges to maintaining the chain of custody (Losavio, 2019).

The consequences of mishandling or breaking the chain of custody are severe, ranging from wrongful convictions and acquittals to mistrials (Garrett, 2011). It is therefore essential to identify and mitigate potential vulnerabilities in the custody process to maintain the integrity and admissibility of forensic evidence (National Institute of Justice, 2020). This requires

ongoing research, evaluation of evidence management practices, and the development of innovative strategies to strengthen the reliability of forensic evidence in judicial processes.

Conceptualisation of Forensic Evidence

Evidence encompasses any information or material that helps establish whether a crime has occurred (USlegal.com, 2020). Forensic evidence, in particular, derives from scientific methods and techniques such as DNA analysis, ballistics, and specialised laboratory tests. This form of evidence plays a pivotal role in investigations and court proceedings, offering objective proof that can support or refute witness testimony (Bangerter, 2016). By leveraging forensic evidence, law enforcement agencies can address a broad spectrum of crimes — from violent offences to cybercrimes and white-collar misconduct.

The study of forensic evidence has become increasingly prominent in legal scholarship due to concerns over wrongful convictions (Medill Justice Project, 2019). Thousands of individuals have been wrongly accused worldwide, with 5,731 reported cases of wrongful convictions (Sherrer, as cited in Medill Justice Project, 2019). In the United States alone, 135 people have falsely confessed to crimes, while 129 were convicted of crimes that never occurred (Purpura, 2012). Such figures highlight the imperative of reliable evidence in safeguarding justice.

Forensic evidence comprises the critical information collected from crime scenes or investigative contexts and analysed scientifically to establish the facts of a case (Houck & Siegel, 2015). This includes diverse forms such as DNA, fingerprints, and digital data retrieved from electronic devices, all of which help investigators identify suspects and reconstruct events (Inman & Rudin, 2000). Through methods like DNA profiling, trace analysis, and chemical testing, forensic experts can evaluate evidence, identify distinguishing characteristics, and link materials to known samples (Kubicz, 2017; ENFSI, 2015).

Forensic Evidence Management

Forensic Evidence Management is a meticulous process that involves the careful collection, handling, and analysis of physical and digital evidence related to crimes or investigations (Houck & Siegel, 2015). It's a crucial aspect of ensuring that evidence is reliable, admissible, and useful in court proceedings (National Institute of Justice, 2019). This process requires a high degree of organization, attention to detail, and adherence to established protocols and procedures (Federal Bureau of Investigation, 2020).

At its core, Forensic Evidence Management involves maintaining the chain of custody, preventing contamination or tampering, and ensuring that evidence is properly documented and preserved (SWGFAST, 2013). By following these protocols and procedures, investigators can ensure that forensic evidence is trustworthy and effective in helping to solve crimes and bring perpetrators to justice (Houck & Siegel, 2015). Forensic Evidence Management in a more straightforward way. Think of it as the careful and organised handling of clues, whether they're physical objects, computer files, or even traces of DNA, from the moment they're found until they might be shown in court (Houck et al., 2017).

It is like a detailed recipe for keeping these clues safe and sound so they can help tell the story of what happened. The main goal is to make sure everyone knows who has touched the evidence, when, and why – this is what we call the "chain of custody" (Lone & Mir, 2019). Imagine it like a relay race where you need to pass the baton (the evidence) from one person to another, and you need to note down exactly who is handing it off and when. This careful process is super important because it proves that the evidence hasn't been messed with or accidentally damaged, making sure it's still reliable when it's time to figure out the truth. This means having clear rules for how to collect evidence, keep it safe, move it around, and study it, depending on what kind of evidence it is. For example, a dusty fingerprint needs different care than a computer hard drive (FileOnQ, 2024). Getting this right helps make sure that any findings are solid and that the legal system can trust them.

Why is all this careful management so vital? Well, if the chain of custody isn't perfect, lawyers might argue that the evidence can't be trusted, and it might not even be allowed in court (Bórquez, 2011). So, keeping a clear record is like having a guarantee of the evidence's journey. Strong evidence management also helps prevent mistakes or even dishonest actions, ensuring that everything is done properly and ethically. Nowadays, technology is making this even easier with digital systems that can track evidence like a digital diary, making things more efficient and accountable (FileOnQ, 2024). Ultimately, by being really thorough with how forensic evidence is managed, police and labs can build stronger cases and help make sure that justice is served fairly (Financial Crime Academy, n.d.).

Chain of Custody

Chain of custody is crucial beyond law enforcement, particularly in critical infrastructure sectors, where it ensures the security and integrity of systems, assets, and data. Without robust chain of custody practices, these assets are vulnerable to unauthorized access and manipulation, potentially compromising their integrity and trustworthiness (National Institute of Standards and Technology (NIST), 2021). The Chain of Custody (CoC) System aims to authenticate claims about sustainable products or services by establishing controls on material movement and data tracking throughout the supply chain. This system sets requirements for certified businesses, enabling credible claims about products. Verification processes, including audits and reporting, ensure compliance with CoC standards, which vary across industries and schemes, highlighting the need for standardized reference points (Iseal Alliance, 2016). Chain of custody is the systematic process of preserving and documenting evidence from collection at a crime scene to presentation in court, ensuring its integrity, accountability, and admissibility by controlling access and tracking handling. According Smith (2024), the chain of custody is a meticulous process that chronicles and safeguards physical and digital evidence from collection to court presentation, ensuring its integrity and authenticity by preventing tampering or contamination, thereby establishing its reliability and admissibility in legal proceedings.

The Chain of Custody (CoC) process is a critical component of forensic evidence management, ensuring the integrity and authenticity of evidence from collection to presentation in court (Houck & Siegel, 2015). The CoC process begins at the crime scene, where investigators collect and document evidence, following strict protocols to prevent contamination or

tampering (Inman & Rudin, 2000). Each piece of evidence is carefully labeled, packaged, and sealed to maintain its integrity (SWGFAST, 2013).

As evidence is transferred from the crime scene to the laboratory, each individual handling the evidence must document their actions, creating a chronological record of custody (ENFSI, 2015). This documentation includes details such as the date, time, and purpose of transfer, as well as the identities of the individuals involved (ASTM, 2017). The CoC process continues through each stage of evidence processing, including analysis, storage, and retrieval (Kubicz, 2017). By maintaining a meticulous record of custody, investigators can demonstrate the authenticity and reliability of the evidence, ensuring its admissibility in court (Federal Rules of Evidence, 2019).

The CoC process is essential for preventing evidence tampering, contamination, or loss, which can compromise the integrity of the investigation and potentially lead to wrongful convictions (Saks & Koehler, 2005). By following established protocols and documenting every step of the evidence handling process, investigators can ensure the chain of custody remains unbroken (Horswell, 2004). This attention to detail and commitment to evidence integrity are critical components of forensic evidence management, supporting the pursuit of justice and public trust in the criminal justice system (National Institute of Justice, 2019).

Each time evidence changes hands, the chain of custody form requires a signature, date, and time entry to maintain accountability. Evidence is considered secure when stored in a controlled environment with limited access. For example, if an investigating officer collects a blood-stained iron rod, it would be documented and handed over to a forensic analyst, who would then analyze it and transfer it to an evidence clerk for storage. The clerk would track all individuals who access the evidence. If the defense questions the evidence's integrity during trial, the records would help establish its authenticity. However, if inconsistencies arise and the prosecution cannot account for the evidence's entire history, the chain of custody may be deemed broken, potentially leading to the evidence's inadmissibility in court.

Types of Chain of Custody

Chain of custody involves systematically documenting the handling and transfer of assets, such as equipment, data, or evidence, to ensure transparency and accountability. By tracking every interaction, it helps mitigate risks of tampering or unauthorized access, supporting the integrity and trustworthiness of the asset throughout its lifecycle (NIST, 2021). Chain of custody ensures the integrity and authenticity of assets, including physical evidence, digital data, and sensitive materials. It involves systematic documentation, secure storage, and controlled transfer to prevent tampering, loss, or unauthorized access, maintaining transparency and accountability throughout.

Physical Chain of Custody

Physical chain of custody involves securing and tracking tangible assets, using measures like sealed containers, tamper-evident seals, and serialized labeling. In critical sectors, physical chain of custody measures ensures asset integrity. The chemical sector uses secure, tamper-evident containers, sealed shipments, and labeled tracking for hazardous materials. Similarly,

election infrastructure relies on tamper-evident seals for ballot boxes, serialized voting equipment, and secure storage facilities to safeguard sensitive materials and maintain authenticity (NIST, 2021).

Physical chain of custody refers to the systematic handling and documentation of physical and documentary evidence to ensure its integrity and admissibility. Investigators must secure evidence, control access, and track its movement to prevent tampering or loss. This involves methodical searches, recording key information, and storing evidence securely. Proper chain of custody ensures evidence is properly obtained and usable in subsequent proceedings. It requires careful consideration of confidentiality, authority, and access rights, with measures taken to protect evidence from loss or compromise, and adherence to organizational policies and procedures. Accurate documentation is crucial (Fourth CII, 2021).

Digital Chain of Custody

Digital chain of custody involves systematically documenting and controlling digital assets, such as data and electronic evidence, to ensure their integrity and authenticity. This includes implementing access controls, encryption, and audit trails to track interactions with digital assets, verifying the identity of users and systems handling the data, and using hashing and digital signatures to detect tampering or alterations, thereby maintaining a secure and transparent record of digital asset handling throughout its lifecycle (NIST, 2021). The digital forensics process is a comprehensive framework that spans the entire lifecycle of digital evidence, from initial identification to courtroom presentation. It aggregates data from various digital sources, such as devices, online platforms, and storage systems, to reconstruct user activities and events. To ensure consistency, several models have been developed, typically consisting of six phases: identifying potential evidence, securing it, collecting and analyzing data, and presenting findings in a structured report for legal proceedings, as outlined by Al-Khateeb, Epiphaniou, and Daly (2019).

Preserving digital evidence poses distinct challenges beyond traditional methods. Digital evidence, encompassing binary data crucial for investigations, resides on physical media but it's the content that's key. Often, only digital content is accessible, and its physical location may be unclear, such as cloud storage. Digital evidence is prevalent due to widespread technology use, and while it's easily alterable, techniques exist to prevent and detect changes. This guide focuses on preserving digital evidence, targeting evidence management professionals, and categorizes considerations into four major types of digital evidence, outlining specific preservation concerns for each (Guttman, White & Walraven, 2022).

The complexity of digital evidence has heightened the difficulty of ensuring authenticity and admissibility, sparking academic efforts to develop practical solutions. Emerging technologies like Cloud Computing and Blockchain are being explored to enhance the reliability and security of Chain of Custody (CoC) practices in digital forensics (Nath et al., 2024). The digital forensics field has undergone significant transformation, broadening its scope beyond computer data analysis for legal evidence to encompass a wider range of activities. According to Ken Zatyko, digital forensics applies computer science and investigative techniques to analyze digital evidence for legal purposes, adhering to strict protocols. The process involves

the entire lifecycle of digital evidence, from identification to court presentation, drawing from diverse data sources. A standardized six-phase model is commonly followed: Identification, Collection, Preservation, Examination, Analysis, and Presentation. This framework ensures the integrity and admissibility of digital evidence in legal proceedings, as noted by researchers like Nelson, Phillips, and Steuart (2014), Zatyko (2007), and Al-Khateeb, Epiphaniou, and Daly (2017).

Theoretical Framework

Systems Theory

The concept of systems theory has evolved significantly since Aristotle's assertion that understanding the whole is essential to gaining knowledge (Aristotle's Holism). This idea has developed into a comprehensive framework for analyzing complex systems in various domains (Bogdanov, 1922, 1980; von Bertalanffy, 1968; Lazlo, 1996; Meadows, 2008). Systems thinking emphasises the interconnectedness of components, highlighting the importance of relationships and interactions within the system (Checkland, 1997; Weinberg, 2001; Jackson, 2003).

By adopting a holistic perspective, researchers can better understand complex phenomena and identify patterns that may not be apparent through traditional analytical approaches (Luhmann, 1990; Golinelli, 2009). This approach has been applied in various fields, including management and marketing, where organizations are viewed as systems interacting with their environment (Burns & Stalker, 1961; Lawrence & Lorsch, 1967; Aldrich, 1979).

Systems theory provides a comprehensive framework for understanding forensic evidence management, viewing it as a complex system with interconnected components (von Bertalanffy, 1968). This system encompasses various stages, including evidence collection, storage, analysis, and presentation, each playing a critical role in maintaining the integrity and reliability of evidence (Houck & Siegel, 2015). By recognizing the interdependencies between these components, investigators and forensic experts can better manage evidence and minimize the risk of contamination, tampering, or loss (Inman & Rudin, 2000).

The application of systems theory in forensic evidence management emphasizes the need for a holistic approach, considering the entire evidence lifecycle from collection to presentation in court (Checkland, 1997). This perspective highlights the importance of maintaining the chain of custody, ensuring that evidence is handled and stored securely, and that all interactions with the evidence are meticulously documented (Kubicz, 2017). By adopting a systems thinking approach, forensic experts can identify potential vulnerabilities in the evidence management process and implement strategies to mitigate these risks, ultimately ensuring the reliability and admissibility of evidence in legal proceedings (National Institute of Justice, 2019).

Crime Scene Investigation (CSI) Theory

Crime Scene Investigation (CSI) Theory is a comprehensive framework that guides the collection, analysis, and interpretation of evidence at crime scenes (Inman & Rudin, 2000). This approach emphasizes the importance of meticulous documentation and careful evidence handling to ensure the integrity and reliability of forensic evidence (Houck & Siegel, 2015).

By applying scientific principles and methodologies, investigators can reconstruct crimes and identify potential suspects.

The effectiveness of CSI relies heavily on the ability of investigators to recognize, collect, and preserve physical evidence (Fish et al., 2014). This requires a thorough understanding of the crime scene and the potential sources of evidence, as well as strategies to prevent contamination and maintain the chain of custody (SWGFAST, 2013). Collaboration between investigators, forensic scientists, and other stakeholders is also crucial in ensuring that evidence is properly analyzed and interpreted.

The application of CSI Theory has significantly contributed to the advancement of forensic science and the pursuit of justice (National Institute of Justice, 2019). By integrating scientific expertise with investigative experience, law enforcement agencies can build robust cases and achieve successful outcomes (Houck & Siegel, 2015). As forensic science continues to evolve, the principles of CSI Theory will remain essential for ensuring the integrity and reliability of evidence in criminal investigations.

The application of Crime Scene Investigation (CSI) Theory to Forensic Evidence Management emphasizes the importance of maintaining the chain of custody process (Inman & Rudin, 2000). This involves ensuring that evidence is properly collected, documented, and stored to prevent contamination, tampering, or loss (Houck & Siegel, 2015). By adhering to established protocols and procedures, investigators can ensure the integrity and reliability of evidence, which is critical for building strong cases and achieving successful outcomes.

Effective chain of custody management is a key component of CSI Theory, requiring meticulous documentation and tracking of evidence from collection to presentation in court (SWGFAST, 2013). This includes ensuring that all individuals handling evidence are properly trained and authorized, and that evidence is stored in a secure and tamper-evident environment (National Institute of Justice, 2019). By applying CSI Theory principles to forensic evidence management, investigators can maintain the integrity and admissibility of evidence, ultimately supporting the pursuit of justice.

Empirical Review

The Impact of Chain of Custody Protocols on the Integrity of Forensic Evidence

In forensic investigations, maintaining evidence integrity is crucial, as any compromise can affect the reliability and admissibility of findings. With the rise of cybercrime, protecting forensic data has become increasingly important. Blockchain technology offers a promising solution, providing a decentralized and tamper-resistant framework for managing data. By utilizing blockchain, forensic data can be secured, ensuring immutability and transparency. Each piece of data is time stamped, securely transferred, and recorded across multiple nodes, creating an unalterable log (Dilna et al., 2024).

This approach enhances traceability, allowing every interaction with the data to be tracked and verified. A public-facing chatbot module complements the blockchain system, providing real-time information on forensic processes and evidence handling protocols. This transparency aims to build public trust and confidence in the justice system. The integration of blockchain

and chatbot technology creates a comprehensive approach to modern forensic investigations, improving security, transparency, and accountability. By combining advanced digital security with public accessibility, this system helps ensure justice is served with integrity (Dilna et al., 2024).

The above Figure 1 shows that forensic investigation involves the scientific collection and analysis of evidence to solve criminal cases. By utilizing various types of evidence, such as DNA samples, fingerprints, and digital data, investigators can piece together the facts of a case and identify suspects. Forensic evidence plays a critical role in India's criminal justice system, providing an objective basis for determining guilt or innocence. The use of advanced technologies like barcoding and Radio Frequency Identification (RFID) enhances the efficiency and accuracy of evidence handling, from collection to courtroom presentation. By leveraging these technologies, forensic investigators can ensure the integrity of evidence and build stronger cases (Akansha, 2025).

The rise of technology has led to an increase in cybercrimes, such as theft and terrorism, which can cause significantly more damage than traditional crimes. As criminals adapt technology to commit crimes, investigators must rely on forensic science to examine evidence. Forensic science involves analyzing evidence collected from crime scenes, which can include physical items like weapons or digital data like log files.

Dr. Edmond Locard's Exchange Principle suggests that every crime leaves a trace, whether it's DNA, fingerprints, or other physical evidence. In cases involving technology, digital evidence like hard drives or computers may be crucial. Maintaining the chain of custody is essential to ensure digital evidence is admissible in court. Evidence can be categorized into physical and digital, each requiring unique analysis and handling procedures. By understanding the different types of evidence and following proper protocols, investigators can build strong cases and bring criminals to justice.

Maintaining the integrity of forensic evidence is crucial in any investigation, and chain of custody protocols play a vital role in ensuring this integrity. Here's how:

Ensures Evidence Integrity: Chain of custody protocols demonstrate that evidence has not been tampered with, altered, or corrupted, ensuring its integrity and credibility (Khan et al., 2021). This is achieved through meticulous documentation and secures handling procedures.

Supports Legal Admissibility: A proper chain of custody ensures that digital evidence can be presented in court without challenges to its authenticity (Khan et al., 2021). This adherence to legal and procedural standards is critical in maintaining the evidence's admissibility.

Prevents Evidence Contamination: Documentation of all interactions with evidence reduces the risk of contamination and mitigates allegations of mishandling (Khan et al., 2021). This is essential in preserving the integrity of the evidence and preventing unauthorized access.

Facilitates Accountability: Chain of custody protocols identify every individual who handled the evidence and their actions, promoting accountability and procedural compliance (Khan et al., 2021). This prevents unauthorized access and ensures that evidence is handled properly.

Preserves Investigation Integrity: A robust chain of custody upholds the investigative integrity, making findings more defensible during litigation (Scalzo et al., 2023). This is critical in maintaining the credibility and professionalism of law enforcement and forensic personnel.

Meets Regulatory and Industry Standards: Chain of custody protocols comply with standards such as ISO/IEC 27037, ensuring procedural compliance and evidence identification (Narasimhan et al., 2024). This adherence to industry standards is essential in maintaining the integrity and reliability of forensic evidence.

Challenges in Digital Evidence Handling

Preserving the integrity of digital evidence poses distinct challenges due to the inherent characteristics of electronic data and the technology used to handle it. These challenges can hinder efforts to ensure digital evidence remains secure, trustworthy, and admissible for legal, business, or security purposes. Key difficulties include (page Vault, 2024):

Data Complexity in Digital Forensics: The vast amount of data generated from multiple sources in digital environments poses significant challenges for maintaining the chain of custody. Computers, smartphones, cloud services, and IoT devices each have unique storage and transmission methods, making standardization of custody procedures difficult. This complexity requires specialized tools, expertise, and protocols to ensure the integrity and admissibility of digital evidence.

Digital Evidence Handling Challenges: Handling digital evidence poses significant challenges due to the complexity of data storage and transfer. Data may be stored across different jurisdictions, on various platforms, or in cloud services operating under different legal frameworks. Secure protocols and careful handling are necessary to prevent interception, corruption, or loss of digital evidence.

Specialized Knowledge for Digital Evidence: Digital evidence requires specialized technical knowledge to handle effectively. Investigators must be familiar with operating systems, file formats, and data recovery techniques. Proficiency in digital forensics tools and staying current with emerging technologies are essential to secure and document digital evidence.

Staying Current with Emerging Technology: The rapid evolution of technology demands that investigators stay current with the latest technologies, tools, and methodologies. Continuous training and education are crucial to address emerging technologies and ensure the integrity and admissibility of digital evidence in investigations.

Digital Evidence Integrity: Digital evidence is vulnerable to tampering and alteration, emphasizing the need for robust forensic tools and methodologies. Maintaining a solid chain of custody and using techniques like hashing and digital signatures can help ensure the integrity and authenticity of digital evidence.

Verifying Digital Evidence Authenticity: Ensuring the authenticity of digital evidence is critical. Cryptographic techniques like hashing and digital signatures can verify the authenticity and integrity of digital evidence. Careful planning and execution are necessary to implement these technologies effectively.

Balancing Investigation with Privacy: Digital investigations often involve sensitive personal information, requiring a balance between investigation needs and individual privacy rights. Investigators must comply with data protection laws and regulations, storing digital evidence securely to prevent unauthorized access or breaches.

Standardizing Digital Evidence Procedures: The lack of standardized protocols for handling digital evidence poses challenges. Establishing best practices and standardized protocols can ensure consistency and reliability in the chain of custody. Training and education on these protocols are essential for investigators.

Risk Factors that Break the Chain of Custody

The chain of custody is vulnerable to disruption by three key factors, including inadequate storage, digital evidence collection disparity, and human elements. These risks can compromise the integrity of evidence, potentially rendering it inadmissible in court due to contamination, loss, or degradation. Effective mitigation strategies are essential to maintaining the reliability of the chain of custody.

Risk Factor 1: Inadequate Storage

The vast amount of digital and physical evidence in legal cases poses significant storage challenges. Traditional storage solutions often fall short, as cloud storage may lack robust security, on-premise hard drives may be space-constrained and prone to corruption, and external storage devices like discs or jump drives are vulnerable to physical damage, loss, or unauthorized access. As a result, specialized storage solutions with advanced security features and scalable capacity are essential for safeguarding sensitive evidence (Omnigo, 2023).

Risk Factor 2: Digital Evidence Collection Disparity

Legal cases often rely on diverse digital evidence, including audio recordings, video footage, and device data, which can be crucial to building or defending a case. However, the varied file formats and media types can create compatibility issues with digital evidence management systems, increasing the risk of data corruption and chain of custody breaches (Omnigo, 2023).

Risk Factor 3: The Human Element

The complexity of multi-agency investigations and the sheer volume of evidence can create vulnerabilities in the chain of custody. With numerous stakeholders handling evidence, the risk of mistakes, miscommunication, and procedural errors increases, potentially compromising evidence integrity and impacting case outcomes. Even minor oversights can have significant consequences (Omnigo, 2023).

Conclusion

In conclusion, the evolution of forensic science has underscored the critical need for meticulous evidence handling, with the chain of custody serving as a cornerstone in maintaining the integrity and admissibility of evidence in legal investigations (Longley, 2022; Mozayani & Parish-Fisher, 2018). Ensuring the unbroken chronological documentation of evidence is paramount in both physical and digital realms, as any lapse can compromise the reliability of findings (Bórquez, 2011; Houck et al., 2017). The increasing complexity of digital evidence, with its inherent susceptibility to tampering, presents unique challenges to traditional chain of

custody protocols, necessitating innovative approaches to maintain trustworthiness (Casey, 2002; Prayudi & Sn, 2015). Digital investigations often involve sensitive personal information, requiring a balance between investigation needs and individual privacy rights. Investigators must comply with data protection laws and regulations, storing digital evidence securely to prevent unauthorized access or breaches.

To address these challenges, the integration of advanced technologies like blockchain and RFID offers promising solutions for enhancing the security, transparency, and accountability of forensic investigations (Dilna et al., 2024; Akansha, 2025). These technological advancements, coupled with the foundational principles of Systems Theory and Crime Scene Investigation (CSI) Theory, provide a robust framework for managing forensic evidence throughout its lifecycle (von Bertalanffy, 1968; Inman & Rudin, 2000). Maintaining the integrity of forensic evidence through stringent chain of custody protocols not only supports legal admissibility and prevents contamination but also fosters accountability and upholds the investigative process (Khan et al., 2021; Scalzo et al., 2023). However, the lack of standardized protocols for handling digital evidence poses challenges, making the establishment of best practices and standardized procedures essential for consistency and reliability in the chain of custody. Training and education on these protocols are also crucial for investigators.

Moving forward, it is crucial to implement standardized chain of custody protocols, particularly for digital evidence, and to provide continuous training for investigators and forensic personnel on emerging technologies and best practices (Page Vault, 2024). The chain of custody is vulnerable to disruption by key factors, including inadequate storage, digital evidence collection disparity, and human elements, which can compromise evidence integrity. By investing in advanced technological solutions, such as specialized storage with advanced security features, addressing compatibility issues with diverse digital evidence formats, and minimizing human errors through comprehensive training, while also establishing clear guidelines that balance investigation needs with individual privacy rights, the criminal justice system can enhance the reliability and admissibility of forensic evidence, ultimately ensuring the pursuit of justice and public trust (National Institute of Justice, 2019; Omnigo, 2023).

Recommendations

i. Standardizing Digital Evidence Handling: Recognizing the increasing volume and complexity of digital evidence in forensic investigations, it is recommended to: Implement standardized chain of custody protocols specifically designed for digital evidence across all law enforcement agencies and forensic laboratories to ensure consistency, reliability, and legal admissibility.

ii. Enhancing Training and Education: Acknowledging the critical role of human factors in maintaining the integrity of the chain of custody and the rapid advancements in forensic technology, it is recommended to: Provide continuous and comprehensive training and education programs for all investigators and forensic personnel on emerging technologies, digital forensics tools, best practices for handling both physical and digital evidence, and the importance of adhering to standardized procedures. iii.

Balancing Investigation Needs and Privacy Rights: Considering the sensitive nature of information involved in digital investigations and the need to uphold individual rights, it is recommended to: Establish clear and legally sound guidelines and protocols that effectively balance the needs of investigations with the fundamental rights to privacy and data protection, ensuring compliance with relevant data protection laws and regulations throughout the evidence handling process.

iv. Integrating Advanced Technologies: In light of the potential risks associated with traditional evidence management practices and the benefits offered by modern technologies, it is recommended to: Invest in and integrate advanced technological solutions, such as blockchain and RFID, into forensic evidence management systems to enhance the security, transparency, accountability, and overall integrity of the chain of custody for both physical and digital evidence.

References

Akansha. (2025). *RFID technology in forensic investigations and evidence collection*. https://www.encstore.com/blog/7932rfid-in-forensics-crime-scene-management-evidence-collection-tracking-evidence-and-management

Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for modern digital forensics: Distributed ledger. In *Blockchain and clinical trial: Securing patient data* (pp. 149–168).

ASTM. (2017). *Standard guide for chain of custody for evidence*. ASTM International.

Bangerter, M. C. (2016, December 22). The importance of forensic evidence in court. https://www.bangerterlaw.com/the-importance-of-forensic-evidence-in-court/

Bogdanov, A. (1980). *Essays in tektology: The general science of organization* (G. Gorelik, Trans.).

Bórquez, P. (2011). Importance of chain of custody of evidences. *Revista Médica de Chile*, 6, 820–821.

Burns, T., & Stalker, G. M. (1961). *The management of innovation*. Tavistock.

Butler, J. M. (2015). *Advanced topics in forensic DNA typing*. Intersystems.

Casey, E. (2002). Error, uncertainty and loss in digital evidence. *International Journal of Digital Evidence*, 1.

Checkland, P. (1997). *Systems thinking, systems practice*. John Wiley & Sons.

Cosic, J., & Baca, M. (2010). A framework to (im)prove "chain of custody" in digital investigation process. In *Central European Conference on Information and Intelligent Systems* (p. 435). Faculty of Organization and Informatics, Varazdin.

Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

Dilna, A., Ananya, M. S., Ziyaan, M., & Faraz, P. A. (2024, November). Forensic evidence security system. *International Research Journal of Modernization in Engineering Technology and Science*, 6(11), 831–838.

ENFSI. (2015). *Best practice manual for the chain of custody*. European Network of Forensic Science Institutes.

Federal Bureau of Investigation. (2020). *Forensic science*.

Federal Rules of Evidence. (2019). Article IX: Authentication and identification.

FileOnQ. (2024, October 12). Forensic evidence control: What is it, and why is it important? https://fileonq.com/forensicevidence-control-what-is-it-and-why-is-it-important/

Financial Crime Academy. (n.d.). *The importance of management in evidence*. https://financialcrimeacademy.org/evidencemanagement/

Fish, J. T., Miller, L. S., & Braswell, M. C. (2014). *Crime scene investigation*.

Fourth CII. (2021). *General principles for physical and documentary evidence*. Conference of International Investigators.

Garrett, B. L. (2011). *Convicting the innocent*.

Giova, G. (2011). Improving chain of custody in forensic investigation of electronic digital systems. *International Journal of Computer Science and Network Security*, 11(1).

Golinelli, G. M. (2010). *Viable systems approach (VSA): Governing business dynamics*. Kluwer (Cedam).

Guttman, B., White, D. R., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers (NIST Interagency Report No. 8387)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8387

Horswell, J. (2004). *The practice of crime scene investigation*. CRC Press.

Houck, M. M. (2018). *Forensic science: The nexus of science and law*.

Houck, M. M., & Siegel, J. A. (2015). *Fundamentals of forensic science*. Academic Press.

Houck, M. M., Crispino, F., & McAdam, T. (2017). *The science of crime scenes* (2nd ed., pp. 109–119). Scholarly Press.

Inman, K., & Rudin, N. (2000). *Principles and practice of criminalistics*. CRC Press.

International Organization for Standardization. (2015). *ISO/IEC 27043: Information technology — Security techniques — Incident investigation principles and processes*.

Khan, M., et al. (2021). The role of chain of custody in forensic evidence management. *Journal of Digital Forensics*, 12(3), 45–57.

Kubicz, E. (2017). Chain of custody in forensic science. *Forensic Magazine*.

Laszlo, E. (1996). *The systems view of the world: A holistic vision for our time*. Hampton Press.

Lawrence, P., & Lorsch, J. (1967). Differentiation and integration in complex organizations. *Administrative Quarterly*, 12(1), 1–30.

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with Hyperledger Composer. *Digital Investigation*, 28, 44–55.

Longley, R. (2022). What is chain of custody? Definition and examples. *ThoughtCo*. https://www.thoughtco.com/chain-of-custody-4589132

Losavio, M. M. (2019). Digital forensics and the chain of custody.

Luhmann, N. (1990). *Soziale systeme: Grundriß einer allgemeinen theorie*. Suhrkamp Verlag.

Meadows, D. H. (2008). *Thinking in systems: A primer*. Chelsea Green Publishing.

Mozayani, A., & Parish-Fisher, A. (2021). *Forensic evidence management: From the crime scene to the courtroom*. https://www.routledge.com/Forensic-Evidence-Management-From-the-Crime-Scene-to-the-Courtroom/Mozayani-Parish-Fisher/p/book/9780367778798

Narasimhan, P., et al. (2024). Ensuring the integrity of digital evidence: The role of the chain of custody in digital forensics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(6).

Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. In *IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*. https://www.researchgate.net/publication/386361522

National Institute of Justice. (2019). *Forensic evidence management*. Washington, DC: U.S. Department of Justice.

National Institute of Justice. (2020). *Forensic evidence and the justice system*. Washington, DC: U.S. Department of Justice.

National Institute of Standards and Technology. (2021). *Chain of custody and critical infrastructure systems*. https://www.cisa.gov/sites/default/files/2023-12/Chain%20of%20Custody_2023.8.14_508.pdf

Nelson, B., Phillips, A., & Steuart, C. (2014). *Guide to computer forensics and investigations*. Cengage Learning.

Omnigo. (2023). 3 risk factors that could break the evidence chain of custody. https://www.omnigo.com/hubfs/2022Omnigo/resources/ebook/3%20Risk%20Factors%20That%20Could%20Break%20the%20Evidence%20Chain%20of%20Custody%20ebook%20_%20Omnigo.pdf

Page Vault. (2024). What is chain of custody and how is handling digital evidence any different? https://blog.page-vault.com/digital-chain-of-custody

Pierce, S. (2017). Forensic evidence and the justice system.

Prayudi, Y., & Sn, A. (2015). Digital chain of custody: State of the art. *International Journal of Computers and Applications*, 114, 1–9. https://doi.org/10.5120/19971-1856

Purpura, P. (2012, May 22). Louisiana residents have been exonerated of crimes, national registry shows. *NOLA.com / The Times-Picayune*.

Rivest, R. (1992). The MD5 message-digest algorithm. https://www.rfc-editor.org/rfc/rfc1321

Saks, M. J., & Koehler, J. J. (2005). The coming paradigm shift in forensic identification science. *Science*.

Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The chain of custody in the era of modern forensics: From the classic procedures for gathering evidence to the new challenges related to digital data. *Healthcare*, 11(5). https://doi.org/10.3390/healthcare11050634

Smith, A. (2024). Understanding the chain of custody and its relevance in handling electronic evidence. *Cyber Solution*.

SWGFAST. (2013). *Standard for a quality assurance program in friction ridge examination*. Scientific Working Group on Friction Ridge Analysis, Study and Technology.

Technical Working Group on Biological Evidence Preservation. (2013). *The biological evidence preservation handbook: Best practices for evidence handlers*. U.S. Department of Commerce, National Institute of Standards and Technology.

United Nations. (2022, October 19). Statement by Alice Wairimu Nderitu, Special Adviser on the Prevention of Genocide, condemning the recent escalation of fighting in Ethiopia (Press release).

USlegal.com. (2020, April 26). *Forensic evidence law and legal definition*. https://definitions.uslegal.com/f/forensic-evidence/

Vijayaraghavan, R. (n.d.). *Digital forensics collection, preservation & appreciation of electronic evidence*. https://www.nja.gov.in/Concluded_Programmes/2021-22/P-1271_PPTs/1.Digital%20Forensics%20Collection,%20Presservation%20and%20Appreciation%20of%20Electronic%20Evidence.pdf

Von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. George Braziller.

Weinberg, G. M. (2001). *An introduction to general systems thinking* (25th anniversary ed.). Dorset House Publishing.

Zatyko, K. (2007). Commentary: Defining digital forensics. *Forensic Magazine*, 20.