Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics

Souradip Nath
Arizona State University
Tempe, Arizona, USA
snath8@asu.edu

Keb Summers
Arizona State University
Tempe, Arizona, USA
kesummer@asu.edu

Jaejong Baek
Arizona State University
Tempe, Arizona, USA
jaejong@asu.edu

Gail-Joon Ahn
Arizona State University
Tempe, Arizona, USA
gahn@asu.edu

***Abstract*—In the era of ubiquitous digital platforms and pervasive mobile device usage, digital evidence has become increasingly integral to civil and criminal justice systems. However, the unique characteristics of digital evidence present significant challenges to maintaining its integrity and ensuring its admissibility in legal proceedings. This paper explores the critical role of Chain of Custody (CoC) in digital forensics, a simple yet powerful process vital for ensuring the trustworthiness and security of digital evidence throughout its lifecycle. We investigate the theoretical foundations and practical implementations of CoC, categorizing contemporary practices into three main categories: Traditional Paper Trail, System-oriented, and Infrastructure-driven approaches. Through a comprehensive analysis, we evaluate these practices against key criteria, highlighting their strengths and limitations in preserving evidence integrity. This study offers an extensive review of existing CoC methodologies and underscores opportunities for future research aimed at enhancing the reliability and security of the digital investigation process.**

***Index Terms*—Digital Forensics, Digital Evidence, Chain of Custody, Evidence Admissibility, Blockchain**

I. Introduction

In today's interconnected world, digital devices such as smartphones, wearables, and connected vehicles have become integral to daily life, continuously generating vast amounts of data. These mobile devices not only store extensive personal information but also remain portable and easily operable, creating a rich digital footprint that follows individuals wherever they go. The field of digital forensic sciences has emerged to leverage this data, enabling forensic investigators to uncover hidden truths in complex scenarios by analyzing information from suspects, victims, and others involved in a case. This capability has led to a significant increase in the use of digital evidence in civil and criminal proceedings in recent years [1].

The importance of digital evidence and the legitimacy of digital forensics are well-established in legal contexts. For example, the U.S. court formally recognized digital information as acceptable evidence and implemented the mandatory electronic discovery (eDiscovery) system in 2006, laying the foundation for this field [2]. Over the past decade, digital evidence has played a critical role in solving major cases, such as the *Boston Marathon Bombing* in 2013, where digital forensic analysis of security footage and suspects' digital devices provided crucial insights [3]. Similarly, in the *College Admissions Bribery Scandal* in 2019, digital evidence, including emails and text messages, was instrumental in exposing fraudulent activities [4].

Despite its growing importance, the use of digital evidence presents unique challenges compared to traditional physical evidence, particularly concerning its admissibility in court. The vast amount of data and its rapid creation and transmission make digital evidence susceptible to manipulation, alteration, or degradation. Several cases have highlighted the difficulties in maintaining the integrity and authenticity of digital evidence, leading to its exclusion from court proceedings [5]. For instance, in the case, *Jones v. Riot Hospitality Group (2024)*, the District Court dismissed the lawsuit after determining that the plaintiff had intentionally deleted pertinent text messages with co-workers, which were critical evidence in the case [6]. Ensuring the integrity of digital evidence and the investigative process, as well as establishing the evidence's admissibility, are fundamental challenges in digital forensics. The admissibility of evidence is governed by specific regulations, such as the Federal Rules of Evidence in the United States. Rule 901, which addresses the authentication of evidence, requires that evidence be proven to be original and free from tampering [7]. In digital forensics, this entails not only demonstrating the integrity of the digital evidence but also verifying the legitimacy of its source. This underlines the importance of originality and unbroken continuity of forensic investigations. Chain of Custody (CoC) is a straightforward yet critical procedure that documents the complete and chronological journey of evidence, ensuring transparency in how it has been handled and maintaining its integrity and authenticity throughout the investigative process [8].

The inherent complexity in digital evidence has intensified the challenge of maintaining authenticity and establishing the admissibility of both the evidence and its corresponding CoC. This challenge has encouraged academic efforts to develop solutions that are both theoretically robust and practically applicable in everyday digital forensics practices. With the emergence of advanced intelligent systems and cutting-edge technologies such as Cloud Computing and Blockchain, there is a growing focus on leveraging these technologies to improve the reliability and security of CoC practices. This paper explores various CoC practices proposed in academic literature and observed in real-world forensic scenarios. It also addresses the unique challenges faced in this field, emphasizing the need

979-8-3503-8674-5/24/$31.00 ©2024 IEEE
DOI 10.1109/TPS-ISA62245.2024.00012

for further research into applying such advanced technologies and secure infrastructures to advance digital forensics.

The remainder of the paper is structured as follows: Section II outlines the foundational concepts of digital forensics and CoC. Section III explores the essential requirements for a robust digital forensics CoC considering both legal and practical aspects. Section IV provides a comprehensive description of the different CoC approaches, with a qualitative analysis of the merits and demerits of each. Section V critically examines these practices against the identified requirements and criteria. The paper concludes with a synthesis of key insights and future research directions that enrich the digital forensics landscape.

II. Background

Digital Forensics. Amidst the rapid evolution of the digital landscape, the scope of digital forensics has expanded significantly, evolving from a focus on digital data stored within computers for use as evidence in legal cases to a broader array of activities and processes [9]. Ken Zatyko, former director of the Defense Computer Forensics Laboratory, defined digital forensics as *"the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence."* This involves analyzing legally relevant digital information stored or transmitted in binary format, adhering to protocols such as search authorization, maintaining a secure CoC, using validated tools, ensuring reproducibility, and providing comprehensive reports and potential expert testimony [10].

Digital forensics encompasses the entire lifecycle of digital evidence, from identification to presentation in court. It draws data from diverse sources, including online repositories, digital devices, and external storage systems. These data sources are essential for uncovering user activities and understanding events. Various models have been proposed to standardize the digital forensics process, typically following a six-phase progression: Identification, Collection, Preservation, Examination, Analysis, and Presentation, as depicted in Figure 1. This process involves identifying potential data sources, protecting evidence from alteration, collecting data, analyzing it, and presenting findings in a coherent report in a court of law [2].

Forensics Ecosystem. The digital forensics ecosystem comprises a complex network of stakeholders and technologies that underpin systematic and scientifically driven investigations involving digital evidence. Understanding this ecosystem is crucial for comprehending how digital evidence is handled throughout a case's lifecycle, from initial identification to court presentation. Figure 2, adapted from Almazrouei et al. (2019) [11], illustrates the digital forensics ecosystem's dynamics. It includes interactions between various stakeholders categorized into four main domains: Forensic Services, Investigative, Legal, and External Stakeholders. These interactions involve the exchange and examination of digital evidence. For instance, forensic investigators may share evidence with other experts for independent analysis.

Grasping the roles and interactions of these stakeholders is essential for understanding the handling and progression

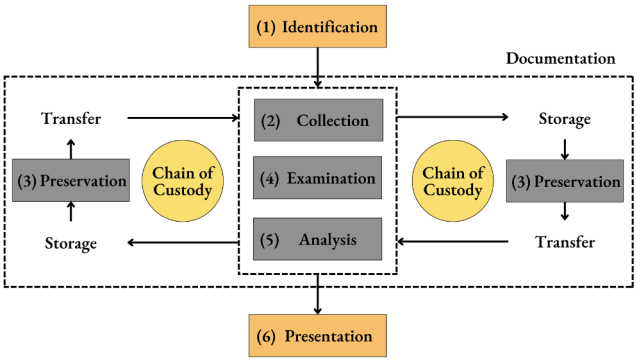

Fig. 1: The Six-Phase Lifecycle of the Digital Forensics Investigation Process.

of digital evidence. This understanding also highlights the challenges of preserving the integrity and admissibility of evidence, as discussed in Section I. For example, Ćosić et al. (2012) used Petri nets to model the lifecycle of digital evidence and the influence of human factors across all investigative stages [12]. The collection, examination, and analysis phases are particularly vulnerable to tampering or manipulation, given the involvement of multiple stakeholders. Addressing these challenges is crucial for ensuring trustworthy and secure forensic investigations, especially as the ecosystem evolves with emerging intelligent systems and technologies.

Digital Evidence vs. Physical Evidence. Digital evidence, like physical evidence (e.g., documents, weapons, fingerprints), provides critical information linking individuals and events to criminal activities. However, key differences distinguish digital evidence from traditional forms of physical evidence [13]:

- **Broader Information Range:** Digital evidence can encompass a vast array of data;
- **Sensitivity:** It involves handling data that may be both personally and physically sensitive;
- **Complex Interactions:** Digital evidence often intersects with broader criminal justice issues beyond traditional evidence collection roles;

Despite its advantages in providing extensive information for convictions, digital evidence poses unique challenges. Its large volume, rapid creation, and potential for manipulation make authentication complex. Digital evidence is also vulnerable to various external influences and human factors that can threaten its integrity. Unlike physical evidence, which is straightforward to document, digital evidence requires more complex procedures. The ease of remote access, file copying, and user mobility complicates the documentation and preservation of digital evidence [14]. The volatile nature of digital evidence necessitates meticulous documentation throughout the investigation. Only the evidence that remains unaltered and reliable meets the admissibility standards in court [15]. Therefore, a robust CoC is crucial to ensure the integrity and authenticity of digital evidence throughout the legal process.

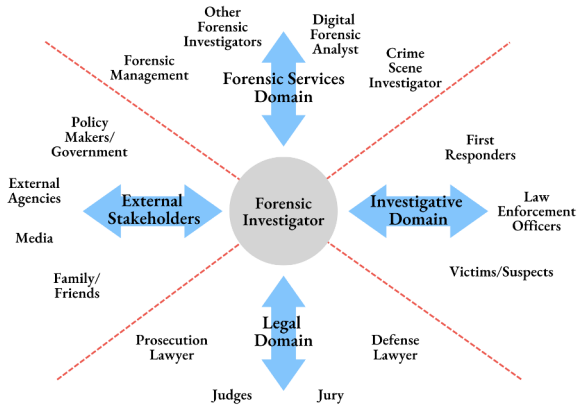

Fig. 2: Different Stakeholders Involved in the Digital Forensics Ecosystem.

Chain of Custody. In digital forensics, the principle *"if you didn't write it down, it didn't happen"* reflects the vital need for thorough documentation, given the volatile nature of digital evidence. Proper documentation is essential to verify that the evidence presented in court is genuine and untampered. The CoC process ensures this by meticulously recording each step of the evidence's journey throughout the case lifecycle. According to guidelines [16], CoC documentation should address the following:

- WHAT? What is the evidence?
- HOW? How was it collected and stored?
- WHO? Who took possession of it?
- WHEN? When was it collected, transferred, or handled?
- WHERE? Where did the evidence travel?
- WHY? Why was the evidence transferred?

The CoC must provide a detailed account of evidence handling, including the identities, locations, and actions of individuals involved in its examination and analysis. This comprehensive documentation maintains evidence integrity and enhances transparency and accountability throughout the forensic process. In legal proceedings, the CoC is crucial for supporting the investigator's testimony. When presented in court, the CoC affirms the authenticity and integrity of the evidence, corroborating the investigator's claims. Moreover, it also complies with standards such as the Daubert Standard [17], which determines the admissibility of expert testimony by requiring that any scientific methods and principles used are both relevant and reliable. The CoC documentation ensures that all documented processes and methodologies can withstand legal scrutiny, safeguarding against claims of mishandling or tampering and supporting the court's ability to make informed decisions about the case [9].

III. Chain of Custody Requirements for Digital Forensics

Recent research and guidelines have outlined a multitude of essential requirements for maintaining the digital evidence CoC in digital forensics investigations. Despite varying approaches, they all share common goals. Here is a summary of these crucial requirements:

(R_1) *The digital CoC must be **comprehensive**, enabling the documentation of diverse forensic activities throughout various phases of the investigative process.*

As elaborated in Section II, the digital investigative process encompasses a spectrum of diverse forensic activities, spanning from evidence collection to its ultimate disposition [8].

(R_2) *The digital CoC must be **complete**, ensuring that every forensic activity during the investigative process is documented with unbroken continuity.*

A break in the CoC signifies a period during which control of the evidence becomes uncertain, and actions conducted on the evidence remain unaccounted for. These breaks create potential vulnerabilities for malicious activities that could jeopardize the integrity of the evidence, as highlighted in [18].

(R_3) *The storage and preservation of digital evidence must maintain a **high level of security**, upholding all three aspects of security – confidentiality, integrity, and availability.*

As emphasized earlier, the central objective of the CoC is to preserve the integrity of digital evidence, making it compliant with the requisite standards for admissibility in legal proceedings [19]. Equally significant is safeguarding this evidence from unauthorized access as it might expose sensitive information about the involved stakeholders. Moreover, for the investigative process to proceed seamlessly, it is imperative to ensure that authorized individuals can promptly access and examine the evidence whenever necessary.

(R_4) *Once entries to the CoC are made and authorized, they must remain **unaltered and immutable.***

Once documented, CoC entries should remain unaltered to preserve credibility and avoid misinterpretation during legal proceedings [2], [19], [20].

(R_5) *All stakeholders interacting with evidence and CoC must be **irrefutably authenticated** to ensure **non-repudiation**, providing undeniable proof of their identity.*

Every individual who handles the evidence should be accountable and identifiable through their interaction with the CoC [21]. This ensures the ability to trace back and verify the individuals responsible for the evidence at any given point in the CoC.

(R_6) *The digital CoC process must be **verifiable** by all stakeholders involved in the forensic ecosystem.*

Especially, in the legal domain, the digital CoC should enable the court and the jury to corroborate the integrity of the evidence by scrutinizing each documented event linked to the evidence, as authorized by the respective overseeing investigator, thereby deeming it admissible.

(R_7) *The digital CoC must enforce **access control** measures, considering various factors, including the stakeholder's role in the investigation and the nature of the evidence.*

Effective access control within the digital CoC is imperative due to the diverse roles played by stakeholders throughout the investigation process. Given that various individuals and entities are involved in the forensic ecosystem, each with distinct responsibilities at different stages of the investigation, it becomes essential to tailor access rights within the CoC accordingly [19].

Establishing an unbroken CoC requires meeting these essential requirements, but from a practical standpoint, some additional factors must be considered.

(R_8) *CoC models must be **usable** for real-world implementation and provide tangible benefits.*

(R_9) *The framework should have an **intuitive and user-friendly design** with acceptable complexity and learnability to accommodate the diverse backgrounds of forensic stakeholders.*

(R_{10}) *The CoC should balance computational (bandwidth, storage, power, etc.) and non-computational (physical space, human resources, etc.) **resource needs**, considering budget constraints and resource availability.*

(R_{11}) *The framework must consider both **direct costs and potential liabilities**, especially when using third-party services for the storage of the evidence and/or deployment of the CoC framework.*

IV. Chain of Custody Practices

In this section, we explore and evaluate various CoC practices both from academic literature and real-world digital forensics applications. We break down these practices into their fundamental principles and discuss the implications of each, including the integration of modern digital infrastructures and systems. In Figure 3, we encapsulate the distinctive features of the different CoC practices, illustrating the taxonomy of the digital CoC landscape.

A. Traditional Paper Trail of Chain of Custody

One of the most straightforward methods for maintaining the CoC involves the use of traditional paper forms. This approach relies on detailed documentation to capture crucial information during the evidence collection, examination, and analysis phases. These forms chronologically record every individual who handles the evidence and track its movement throughout the investigative process. The primary goal of CoC is to ensure thorough and transparent record-keeping, which is facilitated by these paper forms. For instance, NIST introduced a CoC template in 2012 [22], originally designed for physical evidence but also applicable to digital evidence management.

The CoC paper form includes several key sections. The metadata section links the evidence to the specific case and includes relevant case details. A comprehensive description of the seized evidence is provided, followed by a section that tracks the evidence's trajectory throughout its lifecycle. During the examination and analysis phases, when custody transitions between forensic investigators occur, the form is updated to record these transfers, including the reasons for the transfers and the signatures of authorized personnel.

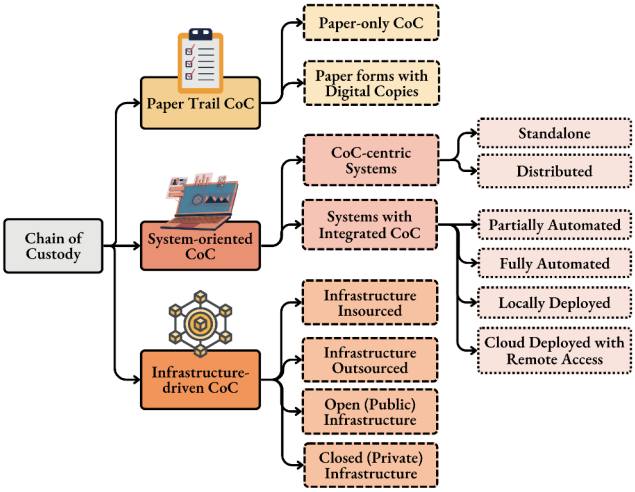

Fig. 3: Taxonomy of CoC Practices in Digital Forensics.

Despite its simplicity, the paper-based CoC approach offers several benefits. It provides transparency by offering a clear and traceable record of evidence interactions, which is crucial for legal proceedings. The method ensures accountability by restricting access and requiring signatures from authorized personnel, thereby reinforcing security and responsibility. Furthermore, physical forms are subject to strict physical access controls and can be signed by multiple involved parties to validate each stage of the process.

With technological advancements, traditional paper forms are increasingly replaced by digital formats, often managed via spreadsheet software [23]. However, original physical copies with signatures are usually retained for legal proceedings to meet due process requirements. Paper systems, being less reliant on technical resources, remain viable in resource-constrained scenarios. Although evolving, the traditional paper-based method remains a critical component of evidence documentation, ensuring that all necessary information is captured and maintained throughout the investigative process [24]–[26].

B. System-oriented Chain of Custody

Digital evidence poses unique challenges not encountered with traditional physical evidence, as highlighted in Section II. These challenges underscore the need for advanced systems to manage the CoC effectively. The complexity of documenting every interaction with digital evidence has prompted the development of specialized systems designed to automate and streamline the CoC process, ensuring the evidence's integrity and admissibility in legal proceedings [27].

One of the pioneering frameworks in this domain is the Digital Evidence Management Framework (DEMF) proposed by Ćosić et al. (2010) [28]. The DEMF framework was among the first to systematically enhance CoC documentation across all stages of the investigative process. It captures four critical factors associated with each interaction involving digital evidence:

```
DEMF = f{
    fingerprint_of_the_file,   // what
    biometric_characteristics, // who
    timestamp,                 // when
    gps_location               // where
}
```

This work can be regarded as a foundation of the system-oriented CoC approaches, exerting a significant influence on various system-based CoC practices, which are discussed next.

CoC-centric Systems (Metadata-driven Approaches). As digital evidence acquisition technology has advanced and forensic imaging formats have become more sophisticated, researchers have sought to leverage the arbitrary metadata associated with forensic images to capture several important details pertaining to the digital evidence to improve its integrity. This approach aims to capture comprehensive details related to the evidence within the forensic image, ultimately contributing to the creation of a more detailed CoC record.

Metadata-driven approaches aim to incorporate detailed information about the evidence into forensic images, enhancing the integrity of the CoC. Forensic file formats like Advanced Forensic Format 4 (AFF4) support flexible metadata capture, which helps in documenting evidence more comprehensively [15]. Researchers have explored using metadata schemas such as Resource Description Framework (RDF) in conjunction with AFF4 to manage and exchange metadata across distributed forensic environments [29] [30].

Furthermore, metadata-driven methods have also been applied to comprehensively capture the forensic workflow and effectively preserve the digital CoC. This method involves specifying a byte-level structure for the CoC, meticulously documenting critical information related to the case, the evidence, and the examiner responsible for its handling. This detailed CoC data is then appended to the forensic image, alongside its system metadata. To ensure the CoC's integrity, the CoC-appended image is subjected to digital signing using the examiner's private RSA key. This digital signing process occurs both during the evidence collection and examination phases. Furthermore, this iterative process expands the CoC whenever there is a change of custody and a new examiner takes charge of the evidence. Thus, the entire record of the forensic analysis performed on the evidence is preserved in the CoC. It's worth noting the noble contributions of Shah et al. (2017) [31] in this context.

Systems with Integrated CoC. With the growing prominence of digital forensics and increasing volumes of evidential data, law enforcement agencies have adopted various evidence management systems, such as ERIN7 [32], EvidenceOnQ [33], ChainLinx [34], and Evidence Manager [35]. These systems are designed to enhance the efficiency and integrity of evidence handling by establishing immutable CoC through automated evidence logs [23]. They document every interaction with the evidence in an unalterable audit trail, which is crucial for maintaining the evidence's integrity.

Many of these systems assign unique barcode values to individual evidence items, facilitating accurate tracking and reference. They automate the CoC process by generating and recording date-time stamps for all transactions, which are stored in a permanent audit trail. While some systems still require manual scanning of barcodes, they significantly streamline the documentation process. This audit trail records details such as user logins, transaction timestamps, data changes, and device IP addresses. The comprehensive log can be reproduced as a CoC report for legal proceedings.

These evidence management systems may be deployed locally or support distributed connectivity through the cloud, allowing remote access. They enhance CoC reliability by automating the documentation process and integrating with other forensic tools, which helps in maintaining accountability, transparency, and security [29].

System-driven approaches are experiencing a surge in popularity for upholding the integrity of digital evidence. Their appeal lies in their capacity to automate the documentation of the chronological history of evidence handling in the form of a CoC. This diminishes reliance on manual oversight to ensure the integrity of the investigative process, as system-imposed restrictions ensure adherence to CoC requirements. This enhancement significantly bolsters the reliability of the CoC, especially since these systems frequently rely on real-world transducers like GPS, time-stamp generators, biometric identification, and digital signatures [29]. Moreover, they can be integrated with other forensic tools, becoming an integral component of the investigative process.

C. Infrastructure-driven Chain of Custody

In recent years, the landscape of digital forensics has evolved significantly due to the complexities introduced by digital evidence and the stringent legal requirements for evidence admissibility. This evolution has led to a shift towards infrastructure-driven approaches, leveraging advanced technologies like Cloud Computing, Blockchain, and IoT. These technologies play a pivotal role in maintaining the integrity and accountability of digital evidence throughout its lifecycle. Over a decade ago, researchers began to observe a shift towards distributed forensic investigations, with multiple analysts collaborating across different geographic locations [15]. This shift was accompanied by the advent of IoT technologies, which introduced the concept of Digital Witnesses [2]. IoT devices, including smart cameras and sensors, are capable of collecting and storing digital data relevant to their surroundings, potentially serving as crucial evidence in legal and investigative contexts. These IoT devices can act as

preservers and sharers of data, constituting Digital Evidence that can be communicated with other interconnected devices or the cloud. Collaboration among IoT devices forms the foundation of this approach, with the underlying infrastructure serving as a pivotal enabler in establishing a trusted CoC. To embrace this digital transformation, recent researchers have diligently directed their endeavors toward forging a widely distributed and decentralized digital forensics infrastructure, with the overarching goal of enhancing the management of investigative processes and upholding the integrity of digital evidence originating from diverse sources.

To address these changes in the digital forensics landscape, there has recently been a notable shift away from the traditional practice of centralized evidence storage, often located on local on-premise servers, to decentralized solutions employing distributed databases managed by trusted entities [19], [21], [36]. This trend arises from a critical need to address the easily manipulable nature of digital data and to safeguard the integrity of evidence in an increasingly interconnected digital landscape. By introducing redundancy through distributed storage, the goal is to ensure the consistent state of all evidence instances within the distributed environment, thus minimizing the risk of tampering or unauthorized alterations. This distributed storage is often realized through commercial cloud solutions implemented on top of a public infrastructure. However, it's essential to note that commercial distributed storage solutions are not always recommended for digital forensics, particularly in police investigations where the utmost security and control are required [37]. Therefore, a collaborative effort involving law enforcement agencies, the court system, and other authorized entities becomes imperative to establish dedicated distributed storage systems implemented on top of a private infrastructure tailored to the unique needs of storing and preserving digital evidence.

Similarly, the concept of decentralization has also found its way into the implementation of the CoC. The CoC serves a vital role in enhancing transparency throughout the investigative process, documenting every interaction with digital evidence to ensure its integrity and admissibility. By decentralizing and distributing the storage and preservation of the CoC among trusted stakeholders, transparency and accountability are significantly bolstered. The redundancy introduced in the storage architecture further reinforces the immutability of the CoC, safeguarding against any attempts at tampering or unauthorized alterations. Moreover, with the integration of cryptographic technologies like digital signatures, and grey hashing [38], the CoC can harness the full potential of this decentralized infrastructure to not only meet the stringent requirements of digital forensics but also satisfy legal standards, ensuring a robust and trustworthy process from start to finish.

For instance, in recent years, various attempts have been undertaken to harness the potential of Blockchain technology to realize this decentralized approach to maintain and preserve digital CoC. Noteworthy among these efforts is the Ethereum-based CoC framework proposed by Bonomi et al. (2018) [21], which stands as a prominent example in this context. However, full decentralization is challenging to achieve within the digital forensics ecosystem due to its inherent requirements of security, accountability, and governance. As a result, many researchers [2], [19], [21], [36], [38]–[40] have shifted their focus towards implementing the CoC via private, permissioned blockchains such as Hyperledger (closed infrastructure), where the participation to the network is authorized by a central certified authority, unlike public blockchain networks (open infrastructure) such as Bitcoin.

Shifting towards such infrastructure-driven methods has notably increased the complexity of the CoC process when compared to the traditional, more straightforward approaches. However, it has concurrently introduced a range of advantages, including immutability, transparency, security, and decentralization, in ensuring the chronological record of evidence handling within the CoC framework for forensic applications by harnessing the power of the underlying complex infrastructure. Based on our extensive literature review and analysis, we summarize the merits and demerits inherent to each of the practices in Table I.

V. Chain of Custody Quality Assessment

In this section, we conduct a qualitative comparison of the various CoC practices discussed in Section IV based on a set of parameters derived from the requirements outlined in Section III and the unique characteristics observed in each CoC practice. Our evaluation framework consists of four primary criteria: **(1) Documentation**, **(2) Legal Credibility**, **(3) Applicability**, and **(4) Resource Requirements**. Each criterion is further subdivided into specific subcriteria to perform a comparative analysis of the strengths and limitations of each CoC practice and identify opportunities for further exploration.

A. Criteria for Comparing Chain of Custody Practices

We first introduce the criteria and subcriteria used to qualitatively assess the three categories of CoC practices for digital evidence. These criteria are:

(C_1) **Documentation.** As previously emphasized, the CoC essentially functions as a chronological record of all activities related to digital evidence throughout the case's lifecycle. In Section III, through (R_1) and (R_2), we address two critical aspects of the CoC documentation process: Comprehensiveness and Completeness. It is important to note that different CoC practices adopt varying approaches to ensure comprehensive and complete documentation. The primary distinctions between these approaches lie in the following aspects:

- **Manual Inputs:** There are two dimensions to consider here. First, the extent to which the documentation process relies on manual obligations to record data. Second, the volume of data that necessitates manual recording.
- **Data Redundancy:** Redundant documentation involves maintaining one or more backups of the primary CoC document. This redundancy increases the resource costs associated with maintaining consistency among all document instances but also enhances the process's resilience against intentional or unintentional tampering.

CoC Practice	Merits	Demerits
Paper Trail CoC [22]	• Feasible in resource-constrained environments due to the lack of need for computational resources • Minimal maintenance cost • Highly usable due to low complexity, requires no specialized training • Easy integration with the existing legal and investigation process	• Huge reliance on manual obligation for comprehensive and complete documentation of the investigative process • Each record's verification is tied to a physical signature, a vulnerable point that could be exploited through malicious forgery • Often reliant on witness testimonies to resolve gaps for legal credibility • Requires non-computational resources: human labor, storage space with physical access control, etc.
System-oriented CoC [28] [29] [32]	• A balance between automated processes and manual involvement to ensure compliance with legal requirements • Digital signatures are more secure than physical signatures, therefore improving verifiability and accountability • With the support of the system, manual labor is significantly reduced from recording and maintaining trails of paper forms	• Transparency of the investigative process is still reliant on the manual obligation to record everything during the investigation process • Different systems utilized during different stages of the investigation can cause issues in compatibility and interoperability therefore increasing chances for compromising immutability • Usage and maintenance cost is higher than paper trail CoC
Infrastructure-driven CoC [19] [21] [36]	• Automated comprehensive and complete documentation of all interactions with the evidence without reliance on a manual obligation • High transparency and immutability depending on the nature of the infrastructure chosen (e.g., Blockchain) • High verifiability and accountability with integrating cryptographic technologies such as hashing, digital signatures, etc. • Decentralized and redundant design of the infrastructure can distribute the attack surface area, potentially reducing the possibility of tampering and unauthorized access	• Introduces substantial complexity, particularly affecting usability and learnability • Understandability of the underlying infrastructure is low, requires very specialized training to use • Highly resource-intensive. Requires substantial computational power, bandwidth, storage, etc. • Suffers from challenges such as cost of security, scalability, resource utilization, efficiency, etc. • Challenging to integrate with the existing forensic tools and the legal ecosystem

TABLE I: Qualitative Analysis of the merits and demerits of different Chain of Custody Practices based on our literature review and analysis. Only a few examples of each practice are cited in the table.

(C_2) **Legal Credibility.** As discussed in Section I, the admissibility of digital evidence presents a dual challenge: preserving the integrity of digital evidence and the investigative process, along with establishing the admissibility of evidence in legal proceedings. As the CoC plays a pivotal role in tackling both of these challenges its legal credibility hinges on ensuring several such aspects:

- **Immutability**: It pertains to the ability of the CoC to ensure that once entries are documented and authorized, they cannot be altered or tampered with in any way.
- **Transparency**: It ensures that there is a comprehensive record of every step taken, making the entire investigative process open and comprehensible to all relevant parties.
- **Accountability**: It entails the clear and irrefutable identification of every individual involved in handling the digital evidence throughout the investigative process.
- **Verifiability**: This involves providing a means for all parties to confirm the accuracy and reliability of the information recorded in the CoC.

(C_3) **Applicability.** This criterion aims at assessing the practicality of implementing the conceptual CoC framework in real-world digital forensic scenarios encompassing a spectrum of vital considerations, as follows:

- **Complexity**: This metric delves into the intricacy of the CoC framework's implementation, seeking to understand how involved and multifaceted the process might be.
- **Learnability**: The concept of learnability assesses how quickly individuals, particularly forensic professionals, can grasp how to efficiently use and interact with the CoC framework. A framework that is intuitive and readily understandable expedites the incorporation of best practices. Conversely, a steep learning curve may necessitate substantial training and thus potentially hinder widespread adoption.
- **Usability**: It evaluates the user-friendliness of the CoC framework. It considers aspects such as the intuitiveness of the interface and the overall ease of interaction.
- **Cost**: This aspect takes into account the financial implications of implementing and maintaining the CoC framework.

It encompasses both the initial costs required for setup and integration and the long-term expenses for maintenance.

(C_4) **Resource Requirements.** This criterion delves into the crucial aspect of comprehending what resources are necessary for the practical deployment and maintenance of a CoC framework. A thorough examination of resource needs is essential in assessing the scalability, sustainability, and adaptability of the CoC framework in real-world digital forensic applications.

- **Non-Computational**: This category encompasses the designated but limited resources such as human elements and physical space essential for the CoC framework's operationality. It involves factors like the allocation of human labor and physical space for several activities like documentation, storage, and preservation.
- **Computational**: This dimension focuses on more dynamic and expandable resources, including computational resources vital for the CoC framework's function. It encompasses elements such as logical storage, computational power for processing and analysis, and the necessary bandwidth for efficient data transfer and communication.

B. Qualitative Comparison of Chain of Custody Practices

Table II conducts a qualitative evaluation of the three broad categories of CoC practices, as elaborated in Section IV, against the criteria outlined earlier. The table primarily employs relative terminology (e.g., Low, Medium, High) to subjectively characterize and assess each practice while simultaneously emphasizing the distinctions among them. It is crucial to acknowledge that this analysis involves an inherent element of subjectivity, and our evaluations of each technique and criterion are based on our best judgment. While alternative viewpoints may exist regarding the precise assessment of each technique, we assert that the criteria delineated in the assessment framework serve as valuable guidelines for steering future research in the domain of digital CoC.

The documentation process for the paper trail CoC is primarily manual due to its reliance on the manual obligation to record every event associated with the evidence accurately. However, some processes can be automated with the assistance of the system, although a significant portion still relies on individual interactions. In contrast, the infrastructure-driven CoC benefits from an underlying infrastructure that automatically records and securely stores a comprehensive log of every interaction, along with a wealth of related information benefitting from inherent data redundancy due to its distributed nature. For CoC systems, which often have central data storage, there's the potential for multiple backups to safeguard against data loss or tampering. However, paper-based practices typically have a straightforward documentation process that doesn't inherently require data redundancy. While some may choose to create digital backups of paper forms to protect against data loss, it's not a fundamental component of the process.

The evaluation of sub-criteria under the umbrella of legal credibility reveals the extent to which each CoC process relies on other processes to fulfill these criteria and their susceptibility to potential malicious exploitation. For instance, the low transparency observed in the paper trail CoC results from its heavy reliance on manual obligations for recording transactions. Additionally, each record's verification is tied to a physical signature, a vulnerable point that could be exploited through malicious forgery. Often, gaps in this CoC need resolution through witness testimonies. In contrast, infrastructure-driven CoCs minimize their reliance on manual obligations by leveraging the underlying digital infrastructure to ensure the fulfillment of legal criteria.

Criteria	Sub-criteria	Paper	System	Infra.
(C_1)	Manual Inputs	High	Medium	Low
	Data Redundancy	Low	Medium	High
(C_2)	Immutability	Medium	Medium	High
	Transparency	Low	Medium	High
	Accountability	Low	High	High
	Verifiability	Low	Low	High
(C_3)	Complexity	Low	High	High
	Learnability	High	Medium	Low
	Usability	High	Medium	Medium
	Cost	Low	Medium	High
(C_4)	Non-Computational	High	Low	Low
	Computational	Low	Medium	High

(C_1) Documentation, (C_2) Legal Credibility, (C_3) Applicability, (C_4) Resource Requirements

TABLE II: Qualitative Comparison of the Chain of Custody Practices. This assessment framework is derived from the requirements outlined in Section III, and the unique characteristics observed in each CoC practice described in Section IV.

The applicability of each CoC practice carries distinct characteristics. Paper-based forms, with their manual entries and physical signatures, require no specialized training, possess minimal maintenance costs, and exhibit high usability. Conversely, system-driven approaches introduce a degree of complexity, necessitating training for individuals interacting with the system. Usability here depends significantly on the design of the system interface. Infrastructure-driven CoCs, while potent, present substantial complexity, particularly regarding learnability. The diverse range of individuals involved in the investigative process can find understanding the underlying infrastructure challenging. Nevertheless, usability can be enhanced through an intuitive design.

Finally, the resource requirements for each of the practices align with their inherent characteristics. In the case of the paper-based CoC process, its predominantly manual nature necessitates a substantial amount of human labor compared to the other approaches. Notably, the paper forms' typical central storage within a physically secured location adds to the demand for non-computational resources, especially physical access control measures. On the other hand, both the systems and infrastructure-driven CoC frameworks significantly rely on computational resources such as processing power, ample storage, sufficient bandwidth, and more. Since the physical infrastructure underlying these processes is often outsourced,

they are not very dependent on non-computational resources.

VI. Discussion and Research Direction

In this section, we briefly summarize the qualitative comparison of various CoC practices conducted in the previous section, using criteria that address key aspects of credibility and practicality. Also, we discuss the implications of our findings and explore potential research directions to advance the field of digital forensics.

Despite its limitations in offering fully transparent and verifiable documentation for legal proceedings, the paper trail CoC excels due to its simplicity, familiarity, and cost-effectiveness. Its straightforward approach integrates well with existing legal systems, where gaps in documentation can often be addressed through expert witness testimonies during court hearings. This adaptability makes it a widely used method in practical forensic and legal contexts.

Conversely, infrastructure-driven CoCs, while complex and resource-intensive, provide essential assurances of immutability, transparency, accountability, and verifiability by leveraging the capabilities of the underlying infrastructure, making them crucial for consideration by digital forensics and legal authorities. However, the lack of standardized practical implementations in industry or government remains evident, as these technologies are primarily confined to academic research and exploration. For example, blockchain-based CoC frameworks have been extensively studied in recent years, but their adoption in real-world applications is still limited due to several unresolved challenges in optimizing these resource-intensive infrastructures for digital forensics. Despite blockchain's inherent advantages of immutability, transparency, and security — qualities that are ideal for maintaining a chronological history of evidence handling, issues such as scalability, resource utilization, and cost-effectiveness continue to impede its broader adoption in forensic and legal contexts [41].

System-oriented CoCs, as highlighted throughout this assessment, find a middle ground. They strive to automate processes while maintaining manual involvement to ensure compliance with the defined requirements. Although practical and applicable to some extent, their limited real-world application warrants further investigation by the community.

Building on this understanding of the inherent strengths, weaknesses, and potential areas for improvement, we identify the following future research directions in the evolving field of digital forensics and CoC:

- **Exploration of Tailored and Optimized Systems:** While infrastructure-driven CoCs offer significant security and assurance, their generic capabilities often lead to resource-intensive implementations with high computational power and bandwidth needs. Future research should focus on designing bespoke, optimized systems and infrastructures specifically tailored to meet the security and practicality requirements of digital forensics. This entails carefully selecting capabilities to remove unnecessary features and functionalities that add overhead without contributing to the core objectives of CoC. For example, similar to efforts in optimizing blockchain architectures for IoT ecosystems [42], in-depth investigations are needed to develop customized CoC solutions that ensure better adaptability and performance in forensic applications.
- **Actor-Centric Design and Evaluation:** To develop more applicable and usable CoC frameworks, it is essential to apply actor-centric analysis during both the design and evaluation phases. Building on principles such as *security by design* [43], future research should focus on directly eliciting requirements from a diverse range of stakeholders, including forensic experts, investigators, and legal practitioners. Engaging these stakeholders across all relevant domains ensures that CoC frameworks are not only based on robust security principles but also tailored to meet the varied needs and preferences of their end users. This approach can help identify and overcome adaptability challenges in theoretical frameworks, resulting in solutions that are both secure and practical for real-world applications.
- **Context-aware Chain of Custody:** Enhancing the integrity of digital evidence can be achieved by incorporating contextual data, such as time, location, and device status. This approach improves the traceability of evidence and supports legal reliability by meeting standards like the Daubert Standard, providing detailed insights into the evidence's origin and handling. When combined with AI and automation, context-aware CoC can streamline anomaly detection and prevent tampering in real-time, ensuring the authenticity of digital evidence. However, future research should explore how to effectively address the computational demands and privacy and legal concerns associated with implementing context-aware CoC systems, ensuring efficient storage and processing of contextual data.

VII. Conclusion

In this paper, we offer a comprehensive survey of the recent CoC practices in both academic research and real-world forensic applications. We begin by outlining the fundamental requirements for CoC in digital forensics, based on insights from industry standards and scholarly discussions. Our study categorizes these practices into three primary groups: Traditional Paper Trail, System-oriented, and Infrastructure-driven approaches. Using an assessment framework that covers legal, security, and practical considerations, we highlight the strengths and limitations of each CoC practice. Our analysis identifies areas where existing methods excel and where they fall short and proposes future research directions to address these gaps. We recommend exploring tailored and optimized systems that are specifically designed to meet the security and practicality needs of digital forensics while minimizing resource intensity. Additionally, we advocate for an actor-centric design and evaluation approach to develop more usable and effective CoC frameworks. By synthesizing current best practices and offering these recommendations for future exploration, our study illuminates new directions for advancing the field of digital forensics.

VIII. Acknowledgments

This work was partially supported by grants from the National Science Foundation (NSF-SFS-1663651, NSF-CICI-2232911).

References

[1] K. Ericksen, "Cracking cases with digital forensics," https://www.rasmussen.edu/degrees/justice-studies/blog/cracking-cases-with-digital-forensics/, 2018, accessed: 2023-08-21.

[2] H. Al-Khateeb, G. Epiphaniou, and H. Daly, "Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger," *Blockchain and Clinical Trial: Securing Patient Data*, pp. 149–168, 2019.

[3] "In boston bombing, flood of digital evidence is a blessing and a curse," https://www.cnn.com/2013/04/17/tech/mobile/boston-bombing-evidence-search-verge/index.html, 2013, accessed: 2023-10-04.

[4] "The college admissions scandal that shook higher education," https://www.bestcolleges.com/blog/operation-varsity-blues-college-admissions-scandal/, 2023, accessed: 2023-10-04.

[5] "Legal lessons learned: 5 times digital evidence was denied in court," https://blog.pagefreezer.com/legal-lessons-learned-5-times-digital-evidence-was-denied-in-court, 2017, accessed: 2023-08-21.

[6] A. Zaller, "Plaintiff's intentional deletion of text messages results in dismissal of case," https://tinyurl.com/yfnfxekr, 2024, accessed: 2024-09-12.

[7] "Rule 901 – authenticating or identifying evidence," https://www.rulesofevidence.org/article-ix/rule-901/, accessed: 2023-08-22.

[8] J. Ćosić, Z. Ćosić, and M. Bača, "Chain of digital evidence based model of digital forensic investigation process," *IJCSIS-Int. J. Comput. Sci. Inf. Secur*, vol. 9, no. 7, 2011.

[9] B. Nelson, A. Phillips, and C. Steuart, *Guide to computer forensics and investigations*. Cengage Learning, 2014.

[10] K. Zatyko, "Commentary: Defining digital forensics," *Forensic Magazine*, vol. 20, 2007.

[11] M. A. Almazrouei, I. E. Dror, and R. M. Morgan, "The forensic disclosure model: What should be disclosed to, and by, forensic experts?" *International Journal of Law, Crime and Justice*, vol. 59, p. 100330, 2019.

[12] J. Ćosić and Z. Ćosić, "Chain of custody and life cycle of digital evidence," *Computer technology and application*, vol. 3, no. 2, 2012.

[13] S. E. Goodison, R. C. Davis, and B. A. Jackson, "Digital evidence and the us criminal justice system. identifying technology and other needs to more effectively acquire and utilize digital evidence." 2015.

[14] Y. Prayudi and A. Sn, "Digital chain of custody: State of the art," *International Journal of Computer Applications*, vol. 114, no. 5, 2015.

[15] M. Cohen, S. Garfinkel, and B. Schatz, "Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow," *digital investigation*, vol. 6, pp. S57–S68, 2009.

[16] W. Jansen and R. Ayers, "Guidelines on pda forensics," *NIST special publication*, vol. 800, p. 72, 2004.

[17] D. D. Blinka, "The daubert standard in wisconsin: A primer," *Wisconsin Lawyer, March 2011, at 14*, 2011.

[18] "Cisa insights: Chain of custody and critical infrastructure systems," accessed: 2023-09-21.

[19] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with poc in hyperledger composer," *Digital investigation*, vol. 28, pp. 44–55, 2019.

[20] A. A. Khan, A. A. Shaikh, and A. A. Laghari, "Iot with multimedia investigation: A secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth," *Arabian Journal for Science and Engineering*, pp. 1–16, 2022.

[21] S. Bonomi, M. Casini, and C. Ciccotelli, "B-coc: A blockchain-based chain of custody for evidences management in digital forensics," *arXiv preprint arXiv:1807.10359*, 2018.

[22] "Nist's sample chain of custody form," https://www.nist.gov/document/sample-chain-custody-formdocx, accessed: 2023-08-15.

[23] S. R. Ropero-Miller, Jeri D., "Landscape study of software-based evidence management systems for law enforcement," https://www.ojp.gov/pdffiles1/nij/grants/300703.pdf, 2021, accessed: 2023-09-09.

[24] T. D'Anna, M. Puntarello, G. Cannella, G. Scalzo, R. Buscemi, S. Zerbo, and A. Argo, "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," in *Healthcare*, vol. 11, no. 5. MDPI, 2023, p. 634.

[25] "What is the chain of custody in digital forensics?" https://online.champlain.edu/blog/chain-custody-digital-forensics, 2024, accessed: 2024-09-12.

[26] U. S. E. A. Commission, "Best practices: Chain of custody," https://www.eac.gov/sites/default/files/bestpractices/Chain_of_Custody_Best_Practices.pdf, accessed: 2024-09-12.

[27] J. Alex, "Paper-based vs. electronic evidence tracking," https://pmievidencetracker.com/2020/02/17/paper-based-vs-electronic-evidence-tracking/, accessed: 2024-09-12.

[28] J. Ćosić and M. Bača, "Do we have full control over integrity in digital evidence life cycle?" in *Proceedings of the ITI 2010, 32nd International Conference on Information Technology Interfaces*. IEEE, 2010, pp. 429–434.

[29] G. Giova *et al.*, "Improving chain of custody in forensic investigation of electronic digital systems," *International Journal of Computer Science and Network Security*, vol. 11, no. 1, pp. 1–9, 2011.

[30] K. N. Nithesh, U. Agarwal, and H. Faizal, "Use of aff4 "chain of custody"-methodology for foolproof computer forensics operation," *International Journal of Communication and Networking System*, vol. 1, no. 1, pp. 49–57, 2012.

[31] M. S. M. B. Shah, S. Saleem, and R. Zulqarnain, "Protecting digital evidence integrity and preserving chain of custody," *Journal of Digital Forensics, Security and Law*, vol. 12, no. 2, p. 12, 2017.

[32] "Evidence tracker (erin7) — erin technology llc," https://erintechnology.com/evidence-tracker/, accessed: 2023-10-19.

[33] "Evidence management — fileonq," https://fileonq.com/evidence-management/, accessed: 2023-10-19.

[34] "Chainlinx flyer," https://justicetrax.com/wp-content/uploads/2015/10/ChainLinx_24ARP2014.pdf, accessed: 2023-10-19.

[35] "Evidence manager - percs.com," https://percs.com/evidence-manager.html, accessed: 2023-10-19.

[36] M. Lusetti, L. Salsi, and A. Dallatana, "A blockchain based solution for the custody of digital files in forensic medicine," *Forensic Science International: Digital Investigation*, vol. 35, p. 301017, 2020.

[37] M. Li, C. Lal, M. Conti, and D. Hu, "Lechain: A blockchain-based lawful evidence management scheme for digital forensics," *Future Generation Computer Systems*, vol. 115, pp. 406–420, 2021.

[38] M. Ali, A. Ismail, H. Elgohary, S. Darwish, and S. Mesbah, "A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and blockchain," *Symmetry*, vol. 14, no. 2, p. 334, 2022.

[39] S. Mercan, M. Cebe, R. S. Aygun, K. Akkaya, E. Toussaint, and D. Danko, "Blockchain-based video forensics and integrity verification framework for wireless internet-of-things devices," *Security and Privacy*, vol. 4, no. 2, p. e143, 2021.

[40] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, "Mf-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture," *IEEE Access*, vol. 9, pp. 103 637–103 650, 2021.

[41] A. H. Lone and R. N. Mir, "Forensic-chain: Ethereum blockchain based digital forensics chain of custody," *Sci. Pract. Cyber Secur. J*, vol. 1, pp. 21–27, 2018.

[42] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *Proceedings of the second international conference on Internet-of-Things design and implementation*, 2017, pp. 173–178.

[43] P. J. Brooke and R. F. Paige, "Fault trees for security system design and analysis," *Computers & Security*, vol. 22, no. 3, pp. 256–264, 2003.