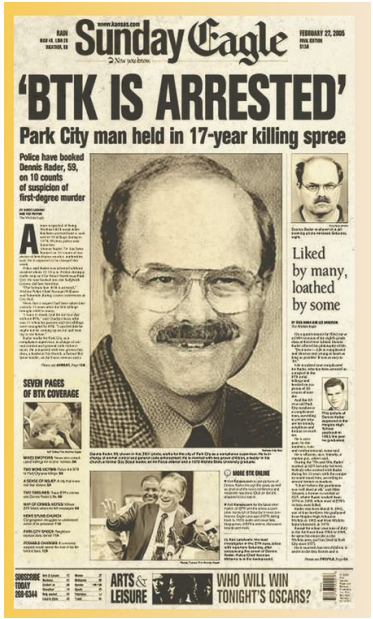
The Sixth IEEE International Conference on Trust, Privacy and Security
in Intelligent Systems, and Applications (TPS-ISA), 2024

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

Souradip Nath, Keb Summers, Jaejong Baek, and Gail-Joon Ahn

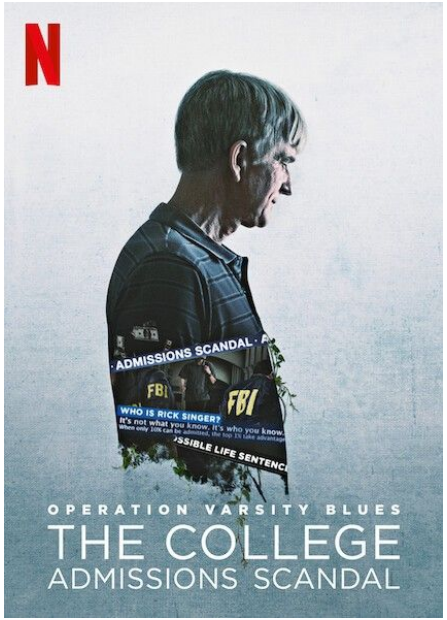
October 28, 2024

Motivation



Arrest of the
BTK killer, 2005

Boston Marathon
Bombing, 2013



College Admission
Scandal, 2019

Motivation

Arrest of the
BTK killer, 2005

Boston Marathon
Bombing, 2013

College Admission
Scandal, 2019

Digital Evidence Admissibility

- **Authenticity**
  - The digital evidence must be proven to originate from a credible source and not fabricated
  - E.g., *An email presented in court must be shown to have come from the defendant's verified account, confirming it as genuine evidence, and not maliciously fabricated.*

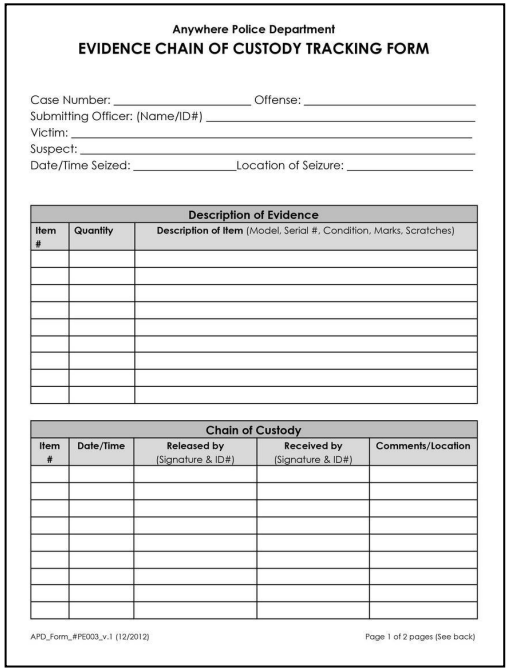
- **Integrity**
  - The digital evidence must remain unaltered from the time it was collected until it is presented in court
  - E.g., *A screenshot of a social media post must be preserved in its original form, with metadata intact, to ensure it has not been edited before being used as evidence in court.*

What is a Chain of Custody (CoC)?

A chronological history of the evidence throughout the life cycle of the case from its collection to presentation in the court.

The documentation must address the following queries:

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



Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

NIST Template for CoC (2012)

Research Questions

- **RQ1:** What are the essential **security** and **operational** requirements for a digital evidence Chain of Custody?

- **RQ2:** What are the **existing frameworks** for Chain of Custody, as proposed in the academic literature and implemented in practice?

- **RQ3:** What **evaluative criteria** should be employed to assess the quality of a digital evidence Chain of Custody framework?

Methodology

(1) Literature Review

Scientific Literature Review

Grey Literature Review

- Blog Posts
- News Articles
- Product Documentation
- Guidelines and Reports

(2) Analysis and Modeling

Requirement Extraction

- Security Requirements
- Operational Requirements

Taxonomy Generation

- Commonalities Analysis
- Categorization of Frameworks

(3) Assessment

Comparative Analysis

- Assessment Framework Derivation
- Qualitative Comparison

Identifying Research Gaps

- Assessing Pros and Cons
- Proposing Research Directions

Research Outcomes

RQ1: Requirements → **RQ2:** Practices → **RQ3:** Quality Assessment

Chain of Custody Requirements

Security Requirements

- Comprehensiveness
- Completeness
- Security and Access Control
- Immutability
- Authentication and Non-repudiation
- Verifiability

Operational Requirements

- Usability and Applicability
- Complexity and Learnability
- Resource Needs (Computational and Non-Computational)
- Direct and Indirect Costs and Liability

Chain of Custody Requirements

Security Requirements

- **Comprehensiveness**
- **Completeness**
- Security and Access Control
- Immutability
- Authentication and Non-repudiation
- Verifiability

Operational Requirements

- Usability and Applicability
- Complexity and Learnability
- Resource Needs (Computational and Non-Computational)
- Direct and Indirect Costs and Liability

Chain of Custody Requirements

Security Requirements

- Comprehensiveness
- Completeness
- **Security and Access Control**
- Immutability
- Authentication and Non-repudiation
- Verifiability

Operational Requirements

- Usability and Applicability
- Complexity and Learnability
- Resource Needs (Computational and Non-Computational)
- Direct and Indirect Costs and Liability

Chain of Custody Requirements

Security Requirements

- Comprehensiveness
- Completeness
- Security and Access Control
- **Immutability**
- Authentication and Non-repudiation
- Verifiability

Operational Requirements

- Usability and Applicability
- Complexity and Learnability
- Resource Needs (Computational and Non-Computational)
- Direct and Indirect Costs and Liability

Chain of Custody Requirements

Security Requirements

- Comprehensiveness
- Completeness
- Security and Access Control
- Immutability
- **Authentication and Non-repudiation**
- Verifiability

Operational Requirements

- Usability and Applicability
- Complexity and Learnability
- Resource Needs (Computational and Non-Computational)
- Direct and Indirect Costs and Liability

Chain of Custody Requirements

Security Requirements

- Comprehensiveness
- Completeness
- Security and Access Control
- Immutability
- Authentication and Non-repudiation
- **Verifiability**

Operational Requirements

- Usability and Applicability
- Complexity and Learnability
- Resource Needs (Computational and Non-Computational)
- Direct and Indirect Costs and Liability

Chain of Custody Requirements

Security Requirements

- Comprehensiveness
- Completeness
- Security and Access Control
- Immutability
- Authentication and Non-repudiation
- Verifiability

Operational Requirements

- **Usability and Applicability**
- Complexity and Learnability
- Resource Needs (Computational and Non-Computational)
- Direct and Indirect Costs and Liability

Chain of Custody Requirements

Security Requirements

- Comprehensiveness
- Completeness
- Security and Access Control
- Immutability
- Authentication and Non-repudiation
- Verifiability

Operational Requirements

- Usability and Applicability
- **Complexity and Learnability**
- Resource Needs (Computational and Non-Computational)
- Direct and Indirect Costs and Liability

Chain of Custody Requirements

Security Requirements

- Comprehensiveness
- Completeness
- Security and Access Control
- Immutability
- Authentication and Non-repudiation
- Verifiability

Operational Requirements

- Usability and Applicability
- Complexity and Learnability
- **Resource Needs (Computational and Non-Computational)**
- Direct and Indirect Costs and Liability

Chain of Custody Requirements

Security Requirements

- Comprehensiveness
- Completeness
- Security and Access Control
- Immutability
- Authentication and Non-repudiation
- Verifiability

Operational Requirements

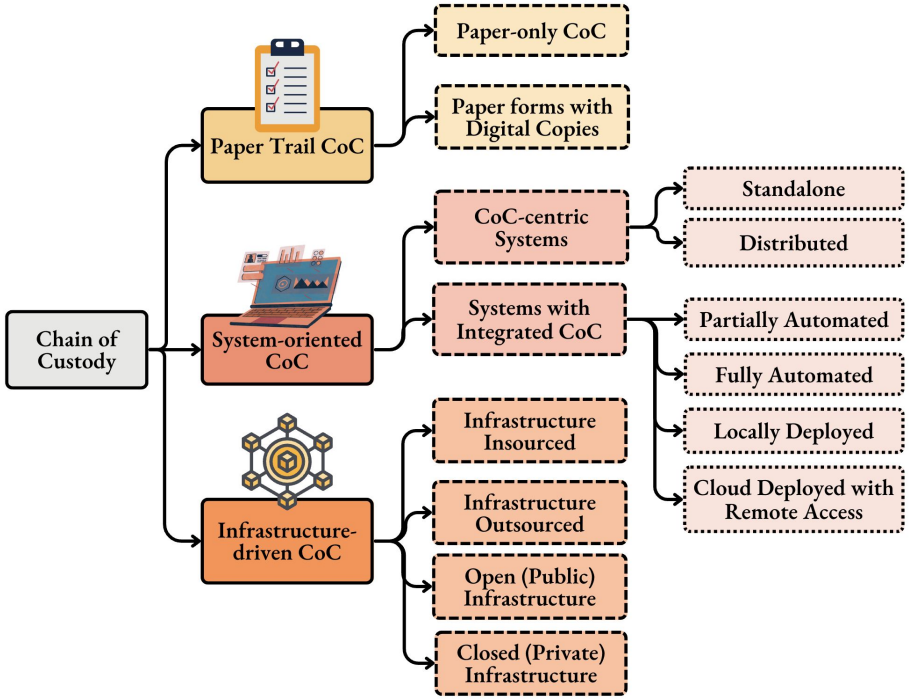
- Usability and Applicability
- Complexity and Learnability
- Resource Needs (Computational and Non-Computational)
- **Direct and Indirect Costs and Liability**

Chain of Custody Practices

We explore various CoC practices both from academic literature and real-world digital forensics applications

We categorize them into three distinct categories:

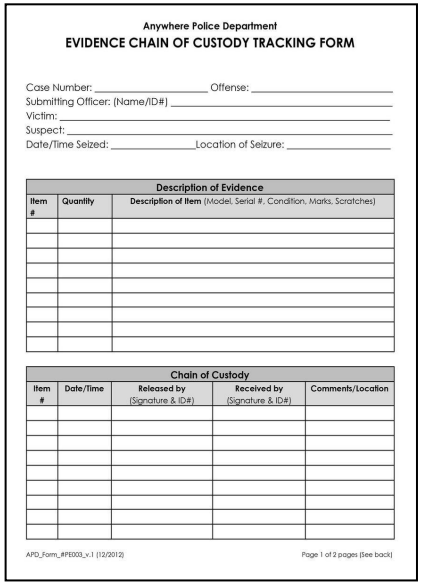
- Traditional Paper Trail CoC
- System-oriented CoC
- Infrastructure-driven CoC



Taxonomy of CoC Practices in Digital Forensics

Traditional Paper Trail Chain of Custody

- Paper forms to chronologically record every individual who handles the evidence and track its movement
- Offers a clear and traceable record of evidence interaction with accountability by requiring signatures from authorized personnels
- Simple, straightforward, transparent, and usable in resource-constrained environments



Anywhere Police Department

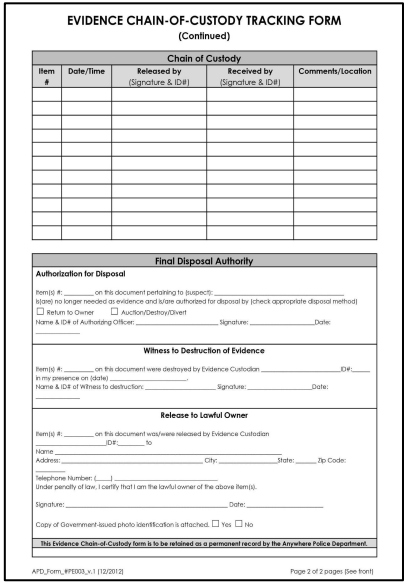
EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)



EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM
(Continued)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)
☐ Return to Owner ☐ Auction/Destroy/Divert
Name & ID# of Authorizing Officer: _____ Signature: _____Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:____
in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian _____ID#:_____ to
Name _____
Address: _____ City: _____State: _____ Zip Code: _____
Telephone Number: (_____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).
Signature: _____ Date: _____
Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

APD_Form_#PE003_v.1 (12/2012) Page 2 of 2 pages (See front)

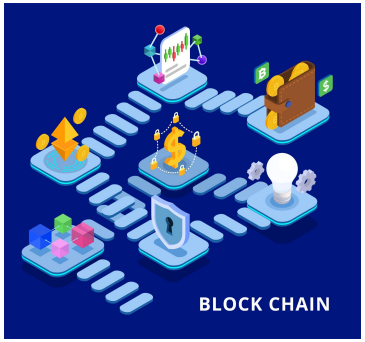
NIST Template for CoC (2012)

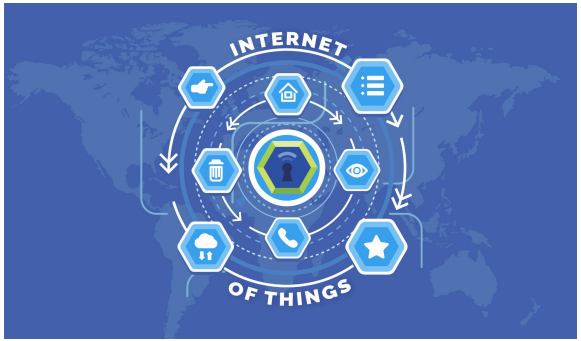
System-oriented Chain of Custody

- Systems that automate evidence tracking with metadata and digital signatures
- CoC-centric Systems vs. Systems with integrated CoCs
- Manual labour significantly reduced with the aid of automated evidence tracking and logging

Infrastructure-driven Chain of Custody

- Leveraging advanced technologies like Cloud Computing, Blockchain, and IoT for CoC and Digital Forensics ecosystem
- Distributed and Decentralized infrastructures to support more real-world forensic workflows
- Infrastructure outsourced vs. insourced
- Underlying infrastructure ensures immutability, transparency, and cryptographic security





Chain of Custody Quality Assessment

- **Documentation**
  - Manual Inputs
  - Data Redundancy
- **Legal Credibility**
  - Immutability
  - Transparency
  - Accountability
  - Verifiability
- **Applicability**
  - Complexity
  - Learnability
  - Usability
  - Cost
- **Resource Requirements**
  - Non-Computational
  - Computational

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

Qualitative Comparison of the CoC Practices

Key Findings

- **Paper Trail is easy-to-use but might not be the most secure option**
  - Straightforward approach integrates well with existing ecosystem
  - Highly practical due to simplicity, familiarity, and cost-effectiveness
  - Provides limited security, but highly adaptable

- **Infrastructure-driven CoCs are secure, but confined to academic research**
  - Underlying infrastructure meets the security requirements
  - Highly resource-intensive and lacks standardized practical implementation

- **System-oriented CoCs find a middle ground, but still limited in application**
  - Somewhat practical and adaptable, but still relies on manual obligation for compliance
  - Limited real-world application needs further investigation

Research Direction

- **Exploration of Tailored and Optimized Systems**
  - Need for Bespoke, optimized systems and infrastructures for practical and secure CoC
  - Careful selection of capabilities to remove unnecessary features and functionalities that add overhead without contributing to the core objectives of CoC

- **Actor-centric Design and Evaluation**
  - Actor-centric analysis during both the design and evaluation phases
  - Directly eliciting requirements from a diverse range of stakeholders to meet the varied needs and preferences of their end users

- **Context-aware Chain of Custody**
  - Incorporating contextual data to improve the traceability of evidence
  - Integration of AI to streamline anomaly detection and prevent tampering in real-time
  - Explore computational demands and privacy and legal concerns

The Sixth IEEE International Conference on Trust, Privacy and Security
in Intelligent Systems, and Applications (TPS-ISA), 2024

Thank you

Souradip Nath | souradipnath.com | snath8@asu.edu | @souradipnath04

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

October 28, 2024