BOCA
BOLETIM DE CONJUNTURA

CONTROLLED CONTAMINATION OF DIGITAL EVIDENCE: CONCEPTUAL PROPOSAL AND EXPERIMENTAL VALIDATION IN AN ACQUISITION SCENARIO

CONTAMINAÇÃO CONTROLADA DE EVIDÊNCIAS DIGITAIS: PROPOSTA CONCEITUAL E VALIDAÇÃO EXPERIMENTAL EM UM CENÁRIO DE AQUISIÇÃO

CONTAMINACIÓN CONTROLADA DE EVIDENCIAS DIGITALES: PROPUESTA CONCEPTUAL Y VALIDACIÓN EXPERIMENTAL EN UN ESCENARIO DE ADQUISICIÓN

10.56238/bocav25n74-014

Fabio Vivan Grigollo[1], Roberto Fabiano Fernandes[2]

ABSTRACT

This study investigates the feasibility and applicability of the concept of Controlled Contamination in computer forensics, analyzing whether documenting and isolating contamination in specific scenarios enables the use of digital traces without compromising their validity. Based on international guidelines and current national legislation, the study addresses concepts related to the preservation of evidence, the chain of custody, and evidentiary integrity. The methodology combines a literature review with practical experimentation to analyze studies on the contamination of digital traces and their effects on the reliability of the evidence. The experimental study was conducted in a controlled environment that simulated a scenario in which data were transferred from a cloud to a hard drive, which was subsequently imaged, enabling detailed forensic analysis of the traceability of the contamination. The results provide evidence on the possibility of maintaining the validity of the evidence in specific scenarios, provided that contamination is appropriately documented and traced, thereby enabling a comparative analysis with existing studies on the chain of custody and evidentiary admissibility. This research proposes an innovative approach that could redefine how digital evidence contamination is handled, directly impacting forensic practices, expert training, and how courts evaluate digital evidence. Furthermore, the research may inform the development of new guidelines, within legal limits, that permit the analysis and use of certain types of partially contaminated evidence in criminal investigations and legal proceedings. The originality of this study lies in the introduction of the concept of Controlled Contamination and the practical demonstration of its viability in specific scenarios, highlighting the importance of rigorous documentation to maintain the reliability of digital evidence. The study seeks to expand chain-of-custody guidelines and to advance methodological approaches in computer forensics, thereby improving

[1] Dr. in Research Specialty Projects. Universidad Internacional Iberoamericana Arecibo. Porto Rico. E-mail: fabio.vivan@doctorado.unib.org
[2] Dr. in Engineering and Knowledge Management. Universidade Federal de Santa Catarina (UFSC). Santa Catarina, Brasil. E-mail: fernandes.roberto@posgrad.ufsc.br

understanding of the effects of contamination and enabling the development of new criteria for evaluating the admissibility of digital evidence in legal contexts.

Keywords: Computer Forensics. Chain of Custody. Evidence Preservation. Controlled Contamination. Validity of Digital Evidence.

RESUMO

Este estudo investiga a viabilidade e aplicabilidade do conceito de Contaminação Controlada na computação forense, analisando se a documentação e o isolamento de contaminações em cenários específicos permitem o uso de vestígios digitais sem comprometer sua validade. Fundamentado nas diretrizes internacionais e na legislação nacional vigente, o estudo aborda conceitos relacionados à preservação de vestígios, à cadeia de custódia e à integridade probatória. A metodologia utilizada combina revisão bibliográfica e experimentação prática, analisando estudos sobre a contaminação de vestígios digitais e seus impactos na confiabilidade da prova. O estudo experimental foi realizado em ambiente controlado, simulando um cenário em que dados são transferidos de uma nuvem para um disco rígido, que posteriormente é clonado, permitindo a análise detalhada da rastreabilidade da contaminação por meio de softwares forenses. Os resultados fornecem evidências sobre a possibilidade de manter a validade da prova em cenários específicos, desde que a contaminação seja devidamente documentada e rastreada, permitindo, ainda, uma análise comparativa com os estudos já existentes sobre a cadeia de custódia e a admissibilidade probatória. A pesquisa propõe uma abordagem inovadora que pode redefinir a forma como a contaminação de vestígios digitais é tratada, impactando diretamente as práticas forenses, os treinamentos de peritos e a forma como os tribunais avaliam provas digitais. Além disso, a investigação pode contribuir para a criação de novas diretrizes, dentro dos limites legais, permitindo que certos tipos de vestígios parcialmente contaminados sejam analisados e utilizados em investigações criminais e em processos judiciais. A originalidade deste estudo reside na introdução do conceito de Contaminação Controlada e na demonstração prática de sua viabilidade em cenários específicos, destacando a importância da documentação rigorosa para a confiabilidade das provas digitais. O estudo busca ampliar as diretrizes da cadeia de custódia e avançar metodologicamente na computação forense, permitindo um melhor entendimento dos impactos da contaminação e possibilitando a proposta de novos critérios para avaliar a admissibilidade de vestígios digitais em contextos jurídicos.

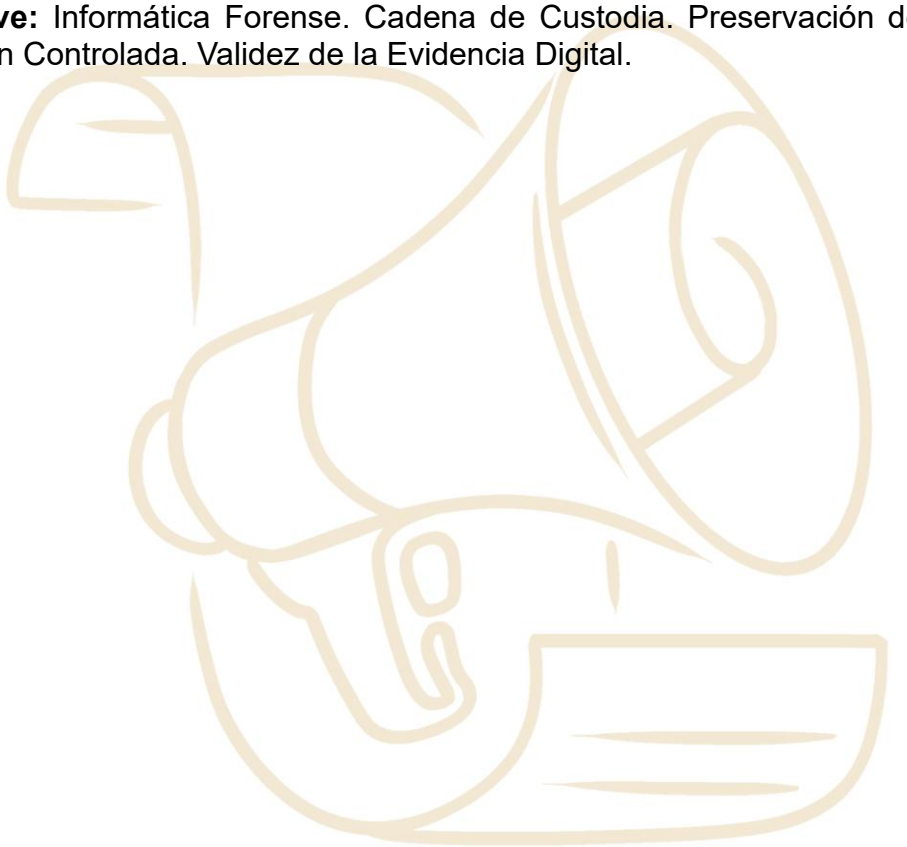
Palavras-chave: Computação Forense. Cadeia de Custódia. Preservação de Vestígios. Contaminação Controlada. Validade da Prova Digital.

RESUMEN

Este estudio investiga la viabilidad y aplicabilidad del concepto de Contaminación Controlada en la informática forense, analizando si la documentación y el aislamiento de la contaminación en escenarios específicos permiten el uso de rastros digitales sin comprometer su validez. Basado en directrices internacionales y en la legislación nacional vigente, el estudio aborda conceptos relacionados con la preservación de la evidencia, la cadena de custodia y la integridad probatoria. La metodología combina una revisión de la literatura con experimentación práctica para analizar estudios sobre la contaminación de rastros digitales y sus efectos en la fiabilidad de la evidencia. El estudio experimental se llevó a cabo en un entorno controlado, simulando un escenario en el que los datos fueron transferidos desde un entorno en la nube a un disco duro, que posteriormente fue sometido a la creación de una imagen forense, lo que permitió un análisis detallado de la trazabilidad de la contaminación. Los resultados aportan evidencia sobre la posibilidad de mantener la validez de la prueba en escenarios específicos, siempre que la contaminación sea debidamente documentada y rastreada, lo que permite un análisis comparativo con estudios existentes sobre la cadena de custodia y la admisibilidad probatoria. Esta investigación

propone un enfoque innovador que puede redefinir la forma en que se gestiona la contaminación de la evidencia digital, impactando directamente en las prácticas forenses, la formación de peritos y la manera en que los tribunales evalúan las pruebas digitales. Además, los hallazgos pueden contribuir al desarrollo de nuevas directrices que, dentro de los límites legales, permitan el análisis y uso de ciertos tipos de evidencias parcialmente contaminadas en investigaciones penales y procesos judiciales. La originalidad de este estudio radica en la introducción del concepto de Contaminación Controlada y en la demostración práctica de su viabilidad en escenarios específicos, destacando la importancia de una documentación rigurosa para mantener la fiabilidad de la evidencia digital. El estudio busca ampliar las directrices de la cadena de custodia y avanzar en los enfoques metodológicos de la informática forense, contribuyendo a una mejor comprensión de los efectos de la contaminación y al desarrollo de nuevos criterios para evaluar la admisibilidad de la evidencia digital en contextos jurídicos.

Palabras clave: Informática Forense. Cadena de Custodia. Preservación de Evidencias. Contaminación Controlada. Validez de la Evidencia Digital.



1 INTRODUCTION

The integrity of digital evidence is a fundamental pillar of digital forensics, essential to ensuring the validity and admissibility of evidence in judicial proceedings.

The chain of custody, as defined by international standards and guidelines, aims to preserve the authenticity and reliability of collected data by minimizing the risk of contamination or improper manipulation. However, in practice, there are scenarios in which evidence contamination, even partial, may occur due to technical limitations, time constraints, accidental contamination, or the need for immediate data acquisition in specific contexts.

In this context, this article proposes and introduces the concept of Controlled Contamination, a new paradigm in digital forensic analysis that seeks to allow the use of evidence even when specific contaminations related to its original structure occur.

The central hypothesis of this study is that, under certain circumstances, it is possible to document, isolate, and mitigate evidence contamination while preserving its reliability and ensuring its continued viability within investigative processes.

To explore this issue, this study conducts a literature review on evidence, contamination, and chain of custody, identifying possibilities for the use of digital evidence that has undergone specific contamination in defined scenarios. The review also outlines current legal limits. Additionally, an experimental laboratory study was conducted to demonstrate the practical applicability of the controlled contamination concept, using, as an example, the forensic acquisition of cloud data before device imaging in a specific scenario.

The experiment analyzed the impact of such contamination on evidentiary value, considering the possibility of tracing and documenting contamination events during the process.

The results provide preliminary guidelines for applying controlled contamination in digital forensic investigations, particularly in emergency contexts, and open avenues for further research to establish objective technical and methodological criteria to distinguish contaminations that fully compromise evidence from those that can be recorded and isolated without investigative bias.

This study experimentally validated the concept of controlled contamination by analyzing a practical case involving the forensic acquisition of cloud data before device imaging. The impact of contamination was assessed with respect to traceability and evidentiary reliability, examining whether identification, isolation, and proper documentation enable continued use of the evidence.

2 THEORETICAL FRAMEWORK

Digital forensics is a discipline that seeks to acquire, analyze, and present electronically stored information, with applications in the investigation of digital incidents and crimes (Ramírez, Gonzales, and Castro, 2019).

According to Castellanos (2017), this is a multidisciplinary field that integrates computational analysis techniques with forensic sciences, ensuring that information is collected and preserved accurately to be legally admissible in judicial proceedings.

The stage of collecting digital traces is essential for the investigation and must follow standardized procedures to guarantee data integrity. According to Arellano and Castañeda (2012), the collection should include a detailed inventory of the analyzed devices, with photographic records and documentation of serial numbers, labels, and other essential details.

Grigollo and Fernandes (2024) provide a recent study that analyzed the chain-of-custody practices adopted by judicial experts in Brazil, from the collection to the disposal of traces, based on a questionnaire administered to 152 experts, of whom 121 responded.

The results revealed significant variation in the adoption of standardized protocols, with 34.7% of experts occasionally omitting records during trace collection and acquisition, and 9.1% never documenting these stages. Furthermore, 45.5% of respondents do not regularly record the examinations and analyses performed, and 71.9% never received specific training on the chain of custody.

The research highlights the need for greater standardization, training, and implementation of technological tools to ensure the reliability of forensic procedures, with 90.9% of experts expressing interest in adopting structures, such as conceptual frameworks, to improve chain-of-custody management.

Brasil (2023) notes that, according to ISO 27037:2013, forensic acquisition must be conducted in a manner that preserves the authenticity of digital evidence, including techniques such as generating forensic images and performing hash verification to ensure the integrity of extracted data.

Poersch and Kuntze (2010) emphasize that forensic analysis must assess the relevance, materiality, and credibility of collected traces, ensuring that the scientific methods used are valid and reliable for judicial purposes. The chain of custody is one of the pillars of digital evidence admissibility.

According to Carvalho (2020), this process documents all stages of trace handling, from collection to presentation in court, ensuring that the data are not altered or contaminated.

Nandhakumar et al. (2012) highlight the importance of using advanced acquisition formats, such as AFF4, to ensure the preservation of trace authenticity and traceability throughout its lifecycle. A break in the chain of custody can render evidence inadmissible in the judicial process.

According to Cantore (2014), failures in documentation or unauthorized access to traces can compromise the credibility of evidence and result in its exclusion from the process.

Machado et al. (2021) emphasize the need to adopt best practices to prevent trace contamination, thereby ensuring the reliability and validity of expert findings.

The MJSP (2023, pages 132-136) presents various perspectives on the chain of custody and the validity of evidence in criminal proceedings, as summarized in Table 1.

Table 1

Extraction of contributions on the topic

Author (apud MJSP, 2023, pages 132-136)	Contribution Summary
Prado (2014)	Highlights the importance of the chain of custody in guaranteeing probative integrity and preventing illicit evidence.
Prado (2021)	States that Law No. 13,964/2019 introduced articles 158-A to 158-F in the CPP, but without significant innovations, generating debates about its effectiveness and legal consequences.
Menezes, Borri and Soares (2018)	Discuss the illegality of evidence derived from a broken chain of custody.
Ávila and Borri (2019)	Criticize the insufficiency of norms in protecting penal evidence.
Matida (2020)	Emphasizes the need for a fair process and proper evidence preservation.
Souza and Vasconcellos (2020)	Analyze precedents from the STJ and STF on the validity of the chain of custody.
Duarte (2020)	Questions the applicability of chain of custody norms to digital evidence.
Ramos (2021)	Advocates for the uselessness of evidence whose chain of custody has been compromised.
Kant de Lima, Nuñez and Carvalho (2021)	Point out structural difficulties in Brazil for the effective implementation of the chain of custody.

Author (apud MJSP, 2023, pages 132-136)	Contribution Summary
Lopes Jr. (2021)	Stresses that the digitization of evidence imposes new challenges, requiring empirical and comparative studies to improve the application of the chain of custody in Brazil.

Source: Adapted from MJSP (2023, pages 132-136).

MJSP (2023, pages 132-136, apud Prado, 2014) argues that the violation of the chain of custody should invalidate the evidence and its derivatives, while MJSP (2023, pages 132-136, apud Badaró, 2017) advocates for a case-by-case analysis by the judge. Decisions by the STJ, such as in HC No. 160,662-RJ and REsp 1,795,341/RS, reinforce the importance of the topic.

According to Brasil (2019), articles 158-A to 158-F of the Code of Criminal Procedure establish the guidelines for the chain of custody of traces in criminal investigations. Article 158-A defines the chain of custody as the set of procedures intended to guarantee the integrity and traceability of evidence from its collection to its disposal. Article 158-B details the stages of this process, including recognition, isolation, collection, packaging, transportation, processing, storage, and disposal of traces. Article 158-C provides that the collection must be conducted by official experts and forwarded to the custody center, and that the responsible expert may not interfere before release. Article 158-D establishes rules for packaging and sealing traces, guaranteeing their inviolability and traceability. Article 158-E requires Criminalistics Institutes to have custody centers for the storage and control of traces, with detailed records of access and movement. Finally, Article 158-F provides that the analyzed traces are returned to the custody center and stored or deposited in an appropriate location as determined by the competent authority.

Therefore, the chain of custody is one of the pillars of the validity and admissibility of evidence in judicial proceedings, ensuring the integrity and authenticity of probative elements. However, there are divergences regarding the consequences of breaking this preservation flow.

While some maintain that a violation of the chain of custody should automatically lead to the exclusion of the evidence and all derived elements, others argue that admissibility should be assessed on a case-by-case basis, considering the actual impact of the violation on the evidence's reliability.

This controversy reveals the need for more refined approaches, such as controlled contamination, in which the chain-of-custody assessment is not limited to a rigid exclusion

criterion but weighs the degree of trace compromise and its influence on the credibility of the process.

Recent studies indicate that the standardization and training of professionals are essential to mitigate failures in handling digital traces (Grigollo & Fernandes, 2024, 2025), underscoring the importance of conceptual frameworks to enhance the reliability of the chain of custody.

Thus, ongoing research is justified by the need to deepen this debate and to propose a more balanced concept of trace contamination that combines probative security and investigative pragmatism, thereby clarifying the boundaries between acceptable contamination and irreversible trace compromise.

3 METHODOLOGY

This chapter presents the procedures adopted for conducting the study and details the methods used to substantiate and validate the concept of Controlled Contamination.

The methodology combines the collection of secondary data with laboratory experimentation, enabling theoretical and practical analysis of the impacts of digital trace contamination.

3.1 RESEARCH APPROACH

The research adopts a qualitative, experimental approach to assess the feasibility of using digital traces even after contamination in specific scenarios, provided they are appropriately documented and traceable.

The study is divided into two main stages: the Literature Review, where an assessment of norms, guidelines, national legislation, and scientific studies on trace preservation and chain of custody is conducted, with a focus on identifying elements related to trace contamination; and a second stage of practical Experiment in the Laboratory, where a real case of digital trace contamination is simulated to assess whether the documentation and isolation of the contamination allow its use.

3.2 EXPERIMENT STRUCTURE

The laboratory experiment was conducted in a controlled environment to simulate a real-world scenario of digital trace contamination and to assess its impact on evidence validity.

3.2.1 Test Environment

The experiment was performed in a digital forensics laboratory equipped with specialized tools for the acquisition, examination, and analysis of digital traces. The equipment and software used include the Windows 10 operating system, installed on a 120GB disk (source). The computer used for testing was a Dell laptop, described in Table 2.

To obtain the test files, a OneDrive account accessed via Windows 10 was used to download a test package containing six .pdf files and four .doc files.

Subsequently, a new 240GB disk (destination) was used to perform a physical forensic copy of the previously mentioned disk. To perform this copy, a Tableau TD1 forensic duplicator device was employed, which was sufficient for this test scenario.

The forensic copy was analyzed using EnCase Forensics v22.4, currently provided by OpenText. This tool was used to analyze the extracted data and perform the necessary forensic checks. The computer used for analysis was a desktop described in Table 3.

3.2.2 Experimental Procedures - trace definition, simulation, and analysis

The experiment followed a set of pre-defined steps to ensure the reproducibility and validity of the results.

Initially, the trace to be used was defined: in this experiment, a 120GB disk with Windows 10 installed on a Dell computer, as specified in Table 2.

Table 2

Collection Object

Model:	Dell Inc. Inspiron 3442
System type:	x64-based PC
Processor(s):	1 processor(s) installed.
[01]:	Intel64 Family 6 Model 69 Stepping 1 GenuineIntel ~1700 Mhz

Source: Author.

While the device described in Table 2 was used to simulate a realistic collection environment, ensuring controlled and representative conditions of a practical digital trace acquisition scenario, the device described in Table 3 was subsequently used to process, examine, and analyze the trace.

Table 3

Device for Processing the Trace

Model:	Gigabyte Z790 AORUS ELITE AX
Processor(s):	1 processor(s) installed.
Configuration:	Four 4TB NVMe units, i9 processor, RTX 4090 video card and 128GB of DDR5 memory

Source: Author.

In the first stage, contamination simulation was performed. To facilitate subsequent assessment of the controlled contamination in this case, the initial intervention involved downloading files before imaging the device. The objective of this action was to determine how the alterations could be detected and isolated in subsequent analysis, ensuring that the contamination could be traced without compromising the integrity of the trace.

After this step, a forensic disk image was performed, ensuring that the data could be examined later and that the state of the digital trace with the simulated contamination was preserved.

In the second stage, post-contamination analysis employed forensic tools to track changes in the system timeline, enabling the identification and isolation of the contamination.

This process enabled verification of the intervention's specific impacts and ensured that all modifications resulting from downloading cloud files were properly documented and distinguished from other events in the system.

Furthermore, detailed documentation of the detected alterations was performed, demonstrating that the contamination was identified and controlled, without compromising the integrity of the original trace. This procedure ensures the traceability of the actions performed and reinforces the validity of the preserved data for forensic investigation.

4 ANALYSIS CRITERIA

The experimental results were evaluated with respect to the impact of contamination on the chain of custody, assessing whether the contamination compromised the traceability of the trace and whether it could harm the integrity of the examined material.

The preservation of the chain of custody is essential in digital forensics, as it ensures that evidence can be examined without risk of tampering or compromise of its authenticity.

Another criterion analyzed was the documentation of contamination, assessing whether the contaminated part could be clearly and objectively recorded and isolated. Proper documentation is fundamental to ensure that the intervention performed in the environment

can be identified and distinguished from other events, thereby ensuring transparency in the process and enabling future analyses to determine which data were affected.

The validity of the digital evidence was also assessed, including whether it could still be reliably used as evidence even after controlled contamination.

This analysis sought to determine whether the original data remained intact and whether it was possible to demonstrate that the contamination did not affect their credibility or probative value.

From these analyses, the study sought to define preliminary guidelines for the practical application of controlled contamination in digital forensics, ensuring that its use occurs in a technical, documented manner and without compromising the integrity of the digital evidence in specific scenarios.

5 DEFINITIONS OF THE CONTROLLED CONTAMINATION CONCEPT

Controlled contamination is applied in this study to a scenario in which specific alterations to the digital evidence are made during its collection or handling. Still, these alterations can be documented, isolated, and tracked in a way that preserves the reliability of the essential information.

Unlike the conventional concept of contamination, which compromises the integrity of the trace and can invalidate it judicially, the controlled contamination concept proposes that the affected part be delimited and recorded, where technically feasible, thereby allowing the digital evidence to remain usable.

This concept is based on the premise that the chain of custody should include standardized procedures for documenting contamination incidents and that, as long as there is a reliable audit trail, the digital evidence remains valid in an investigative process.

6 EXPERIMENTAL CASE STUDY

To validate the applicability of controlled contamination, a laboratory experiment was conducted based on a realistic field forensic acquisition case.

The study simulates a scenario in which an expert must access and download data stored in the cloud and on the device itself before imaging the device, thereby generating specific, isolatable, and trackable contaminations in the original trace.

6.1 EXPERIMENT: IMMEDIATE *DOWNLOAD* OF CLOUD DATA BEFORE FORENSIC IMAGING

Regarding the Scenario, during a search and seizure, the expert encounters an environment where time is minimal, the cloud with potentially highly relevant content is

accessible on the equipment to be imaged, and the device's USB ports are blocked, with a high risk that the cloud data will be deleted remotely before being copied.

Regarding the Decision, considering that the expert encountered some technical problems that would take time to overcome, they chose to download the files directly onto the computer to be imaged, knowing that this would modify the system *timeline* and generate new activity records that could be attributed to the moment when the specialist was performing the collection or acquisition.

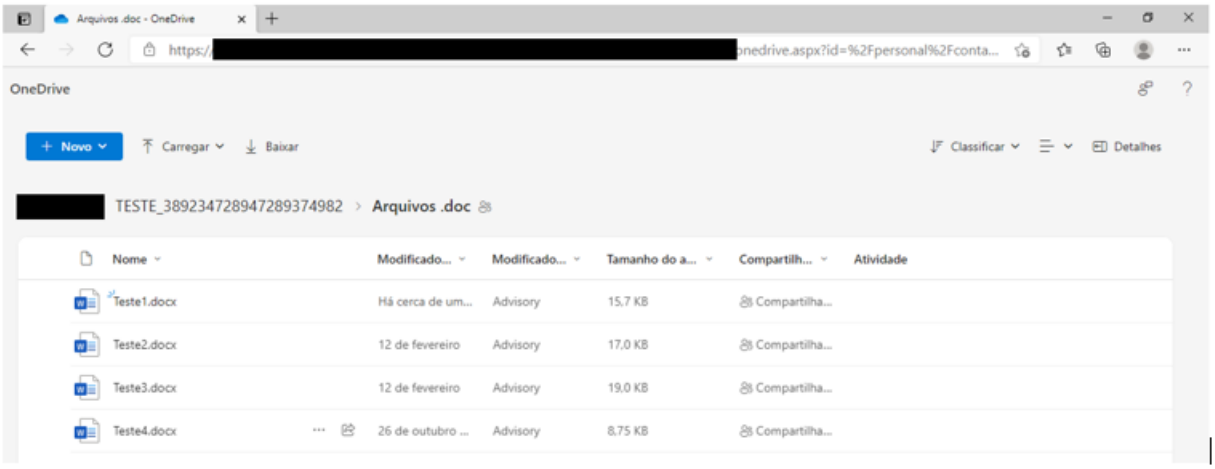
The experiment's objective was to assess the impact of this modification on the chain of custody and to verify whether it was possible to isolate and document the contamination without invalidating the digital evidence.

6.2 Practical Test Execution and Results Obtained

In the controlled-contamination simulation, before forensic imaging, files were downloaded directly from the cloud to the computer for imaging. This action aimed to avoid the loss of data relevant to the investigation, considering the risk of remote deletion of the content.

Figure 1

OneDrive .doc Files

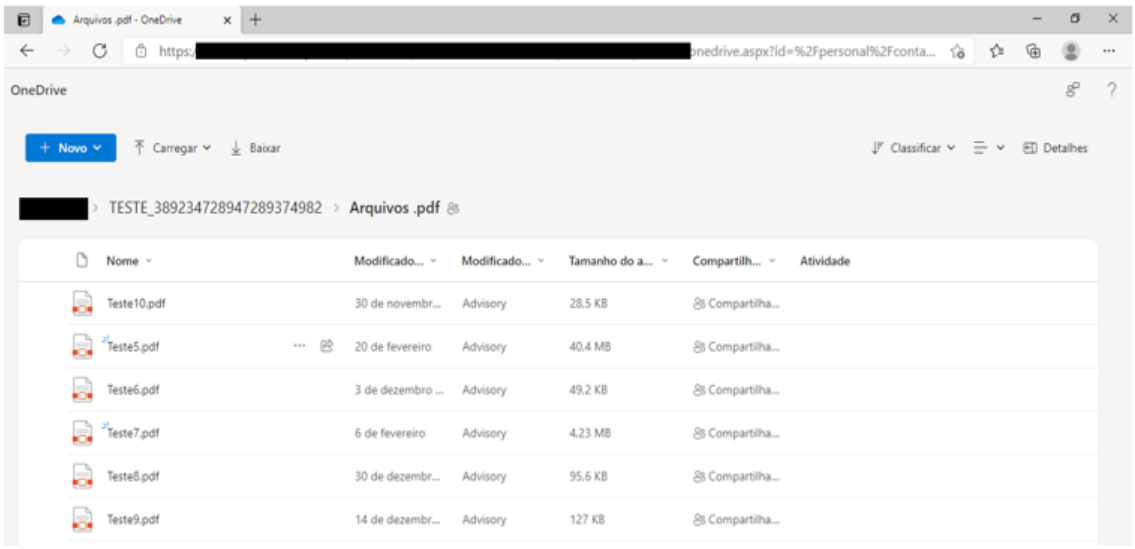


Source: Author.

Figure 1 presents the four documents in .doc format downloaded from the cloud, while Figure 2 shows the six files in .pdf format transferred to the machine.

Figure 2

OneDrive .pdf Files

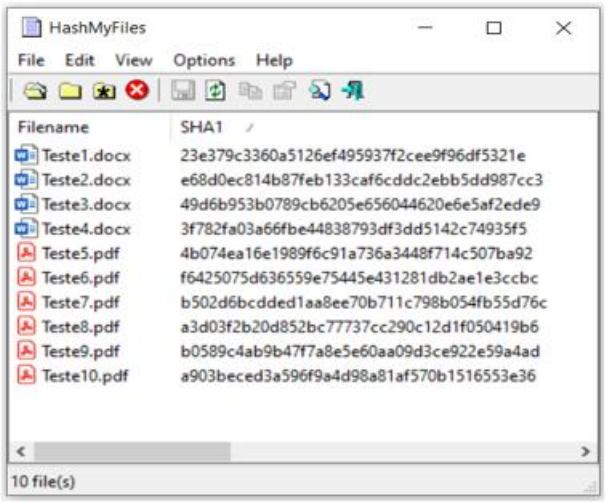


Source: Author.

The integrity of these files was immediately ensured by generating SHA-1 hashes, as illustrated in Figure 3, using the HashMyFiles tool. This procedure ensured that, at the time of download, each file was assigned a unique identifier, enabling subsequent verification.

Figure 3

SHA1



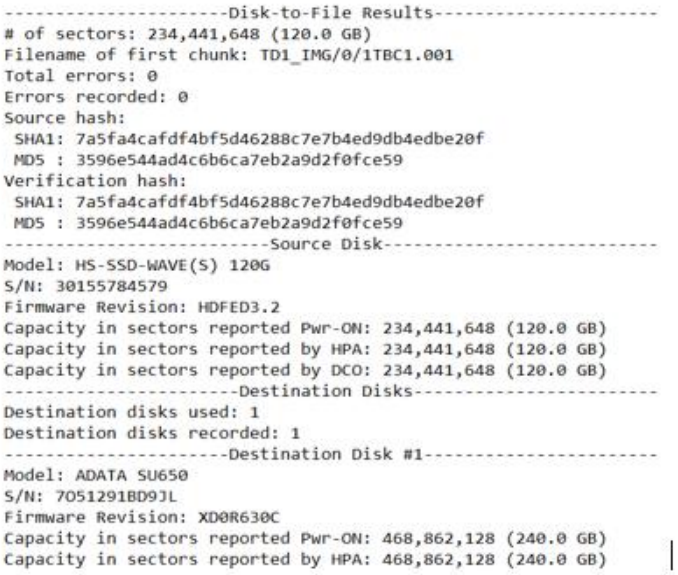
Source: Author.

After the download, the trace was forensically acquired using the *Tableau* TD1 device. The integrity of the image was verified by comparing the *hash* of the original disk with that of

the copy, as shown in Figure 4. This step confirmed that the trace data structure remained intact at the time of forensic acquisition.

Figure 4

Disk-to-File Results



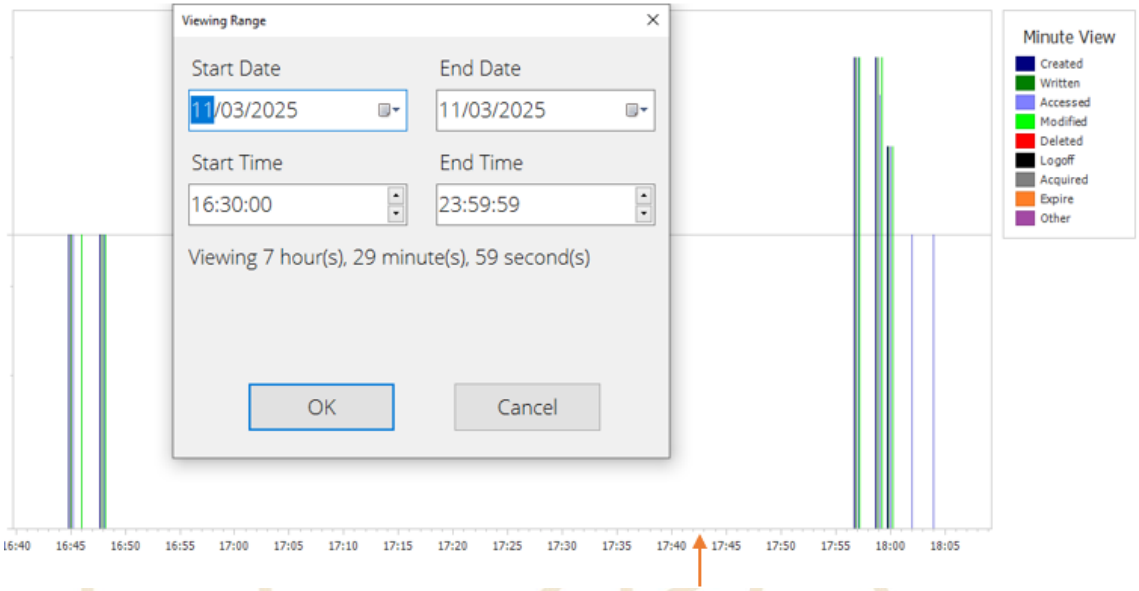
Source: Author.

The post-contamination analysis was conducted with *EnCase Forensics* v22.4, exploring the *timeline* functionality to segment events before and after the download.

The *timeline* visualization, as shown in Figure 5, revealed that activity records outlined prior to the download reflected only regular system operations. In contrast, the time window corresponding to the file download showed the expected modifications.

Figure 5

Timeline



Source: Author.

After this activity, the *timeline* of the imaged image showed no more events, as the machine was imaged immediately after the acquisition of the cloud files.

This behavior confirms that all expert activity was isolated and documented, without subsequent interference.

Figure 6

Table

	Item Path	File Created	Last Written	Last Accessed	SHA1
4	Disk Image\D\Users\EstudoArtigo\Downloads\Teste1.docx	11/03/25 17:57:17 ...	11/03/25 17:57:20...	11/03/25 17:57:29 ...	23e379c3360a5126ef495937f2cee9f96df5321e
5	Disk Image\D\Users\EstudoArtigo\Downloads\Teste1.docx:Zone.Identifier				6c65ae358c6a8e96ae2840ae8774d7c7dbe576a6
6	Disk Image\D\Users\EstudoArtigo\Downloads\Teste10.pdf	11/03/25 17:59:32 ...	11/03/25 17:59:33...	11/03/25 17:59:34 ...	a903beced3a596f9a4d98a81af570b1516553e36
7	Disk Image\D\Users\EstudoArtigo\Downloads\Teste10.pdf:Zone.Identifier				f138a16eba51ce5f19984b905e1783def0e5adb5
8	Disk Image\D\Users\EstudoArtigo\Downloads\Teste2.docx	11/03/25 17:57:26 ...	11/03/25 17:57:27...	11/03/25 17:57:29 ...	e68d0ec814b87feb133caf6cddc2ebb5dd987cc3
9	Disk Image\D\Users\EstudoArtigo\Downloads\Teste2.docx:Zone.Identifier				8d2795a92583094f9363b28b861bbfc5bfef69be
10	Disk Image\D\Users\EstudoArtigo\Downloads\Teste3.docx	11/03/25 17:57:34 ...	11/03/25 17:57:35...	11/03/25 17:57:35 ...	49d6b953b0789cb6205e656044620e6e5af2ede9
11	Disk Image\D\Users\EstudoArtigo\Downloads\Teste3.docx:Zone.Identifier				9a97ed1d7315ce9ffb161de796acfb0923dcf5f4
12	Disk Image\D\Users\EstudoArtigo\Downloads\Teste4.docx	11/03/25 17:57:40 ...	11/03/25 17:57:41...	11/03/25 17:57:41 ...	3f782fa03a66fbe44838793df3dd5142c74935f5
13	Disk Image\D\Users\EstudoArtigo\Downloads\Teste4.docx:Zone.Identifier				2cdf9ceaaaff3c9faea49e7252aaca46c85c6f08
14	Disk Image\D\Users\EstudoArtigo\Downloads\Teste5.pdf	11/03/25 18:00:13 ...	11/03/25 18:00:20...	11/03/25 18:02:48 ...	4b074ea16e1989f6c91a736a3448f714c507ba92
15	Disk Image\D\Users\EstudoArtigo\Downloads\Teste5.pdf:Zone.Identifier				4dc00b03c09a80c6b1a0f49585afdfd459d8f03c
16	Disk Image\D\Users\EstudoArtigo\Downloads\Teste6.pdf	11/03/25 18:00:05 ...	11/03/25 18:00:06...	11/03/25 18:00:15 ...	f6425075d636559e75445e431281db2ae1e3ccbc
17	Disk Image\D\Users\EstudoArtigo\Downloads\Teste6.pdf:Zone.Identifier				dccc9c21062b8dddf8b4d276c71c5f8289518a06
18	Disk Image\D\Users\EstudoArtigo\Downloads\Teste7.pdf	11/03/25 17:59:52 ...	11/03/25 17:59:58...	11/03/25 18:00:32 ...	b502d6bcdded1aa8ee70b711c798b054fb55d76c
19	Disk Image\D\Users\EstudoArtigo\Downloads\Teste7.pdf:Zone.Identifier				ea5a84357ba57f534e276806420ff16da8fd37cb0
20	Disk Image\D\Users\EstudoArtigo\Downloads\Teste8.pdf	11/03/25 17:59:46 ...	11/03/25 17:59:47...	11/03/25 17:59:48 ...	a3d03f2b20d852bc77737cc290c12d1f050419b6
21	Disk Image\D\Users\EstudoArtigo\Downloads\Teste8.pdf:Zone.Identifier				b725835fc7c753e2d2fd0fe5b4b019c45f5aa72a
22	Disk Image\D\Users\EstudoArtigo\Downloads\Teste9.pdf	11/03/25 17:59:42 ...	11/03/25 17:59:42...	11/03/25 17:59:43 ...	b0589c4ab9b47f7a8e5e60aa09d3ce922e59a4ad

Source: Author.

Verification of the downloaded files' metadata showed that the creation, modification, and access dates remained consistent, as shown in Figure 6, indicating no tampering with the records. Furthermore, the *hashes* of the downloaded files, calculated before and after imaging, remained identical, demonstrating that the files remained integral throughout the process.

Therefore, the experiment validated the possibility of identifying, isolating, and documenting contamination in a controlled manner and without compromising the digital evidence.

In specific scenarios, the results indicate that, provided the procedure is conducted in a documented and traceable manner, the modifications can be clearly and accurately attributed, thereby ensuring the admissibility of the evidence in a forensic investigation.

7 RESULTS AND ANALYSIS

The download of files from the cloud prior to forensic imaging generated system records, but the impacts are completely traceable and isolatable, guaranteeing the integrity of the digital evidence. No alterations were observed that indicated the removal of previously existing data in allocated areas. The identified changes corresponded to the creation of new artifacts and records associated with the download, which are discernible in the forensic *timeline* in this specific scenario.

Browsing history, cookies, and cache may record these events when the download occurs via a browser. At the operating system level, the *Windows Event Log* may contain records of network access and download execution. At the same time, other logs may indicate communication with cloud servers and other relevant information for tracking.

In the file system, the *Master File Table* (MFT) and other means record the creation and movement of downloaded files, allowing verification of exactly which data was added to the system during the period. If there were an active *shadow copy (Volume Shadow Service)*, it could capture changes before imaging. Furthermore, references to the use of download applications may have been stored in artifacts such as *Prefetch* and *SuperFetch*.

Created files have *timestamps* for creation, modification, and last access, enabling complete traceability of their addition to the system.

All records generated by the download were identifiable and isolable, were auditable, and ensured that the only operation performed by the expert before imaging was the addition of the downloaded files, without compromising the validity of the digital evidence in this tested scenario.

The forensic timeline analysis in EnCase objectively demonstrated that no interference occurred beyond that necessary to preserve data essential to the investigation.

The experimental results demonstrated that controlled contamination did not compromise the digital evidence's chain of custody in this scenario, because all alterations caused by the download were documented adequately during the procedure and can be traced.

The analysis of the system timeline confirmed that the modifications can be audited, segmented, and isolated, preserving the validity of the digital evidence. Furthermore, forensic records demonstrate that the alterations occurred within a specific period and could be identified and distinguished from other events in the system, thereby ensuring the traceability of the intervention.

The analysis also confirmed that the contamination did not compromise the trace's reliability. The timeline before the event was not modified; it remained intact, and the logs, together with the forensic timeline, demonstrated that the changes were traceable and delimited. These factors ensure that the trace can be considered valid and admissible, since any impact from the download can be clearly identified, isolated, and documented within the forensic investigation, and is therefore auditable.

8 MATHEMATICAL FORMALIZATIONS

8.1 MATHEMATICAL MODEL

The chain of custody can be represented as an ordered sequence of events, each with a corresponding timestamp and hash.

Let:

$E = \{e_1, e_2, ..., e_n\}$: set of events recorded in the chain of custody

$T = \{t_1, t_2, ..., t_n\}$: times associated with each event

$H(e_i)$: *hash* function of the trace state after event e_i

The relationship between events can be expressed by:

$\forall\ i \in \{2, ..., n\}, H(e_i) = f(H(e_{i-1}), \Delta e_i)$

Where Δe_i represents the transformation or contamination between events.

The function f represents a conceptual abstraction of the transformation of the trace state, not a cryptographic hash function in the strict sense.

8.2 CONTAMINATION IMPACT METRIC

The contamination impact **I** is defined as: I = |A_c| / |A_t|

Where:

A_c = set of contaminated artifacts

A_t = total artifacts in the trace

If I ≤ ε (for example, **ε =** 0.05**),** the trace can be considered admissible in certain scenarios.

The value ε is a technical parameter proposed in this study, based on reasonableness criteria, and not a mathematically absolute limit.

It is emphasized that metric I constitutes a simplified proportional measure, aimed at quantifying the relative impact of contamination on the set of trace artifacts. It is a normative and technical model, not a statistical one, that does not account for differentiated weights across artifact types nor for the individual probative relevance of each element. Thus, the value of I should be interpreted as an auxiliary indicator of impact, to be analyzed alongside documentation of the chain of custody, traceability of alterations, and the technical-legal context of the concrete case.

8.3 DIGITAL EVIDENCE CONFIDENCE FUNCTION

The confidence function **C** is defined as:

C = D / (D + U)

Where:

D = number of correctly documented events

U **=** number of events with documentation failures

It is suggested that the trace be considered valid when C ≥ 0.95, in specific scenarios.

It is further noted that the proposed limit of C ≥ 0.95 is normative and not mathematical.

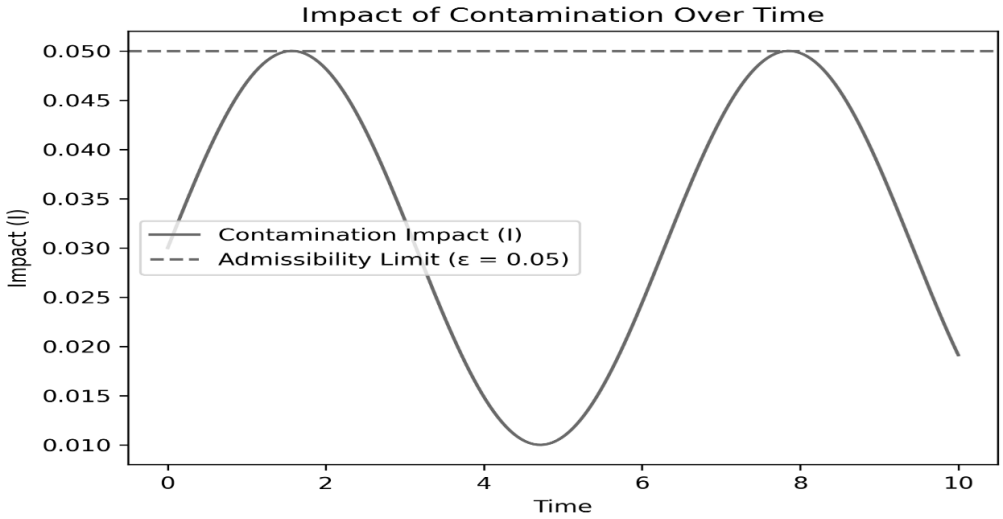
8.4 GRAPH OF CONTAMINATION IMPACT METRIC OVER TIME

During the analysis of the controlled contamination concept, a simulation of the contamination impact metric over time was developed to represent realistic scenarios in which minor alterations occur in the digital trace due to justified technical interventions, such as downloading relevant data before forensic imaging

(Figure 7). For this, a simulated impact function I(t**)** was adopted, defined as a smooth, continuous oscillation between 1% and 5% over the trace acquisition time, to represent discrete fluctuations arising from the expert's technical activity.

Figure 7

Impact



Source: Author.

The horizontal axis of the simulation represents time, considering the entire forensic process, from collection to analysis of the digital trace. The vertical axis corresponds to the value of the impact metric **I**, defined as the ratio between the number of contaminated artifacts and the total number of artifacts present in the trace, i.e., $I=|Ac|/|At|$. This index allows quantifying the degree of contamination that occurred during the procedure.

To assess evidence admissibility, a technical tolerance limit for contamination was established, $\varepsilon = 0.05$ (5%), which serves as the maximum acceptable parameter for the trace to remain valid under the controlled contamination model in specific scenarios. The simulation demonstrated that all variants of the impact metric remained below this threshold over time, indicating that even if there are punctual interventions in the digital trace, provided they are adequately documented and traceable, there is no prejudice to its probative validity in specific scenarios.

This behavior supports the thesis that contamination, when controlled and auditable, does not necessarily compromise the trace's integrity or admissibility.

Thus, the incorporation of objective metrics, such as the function I(t), into forensic protocols is proposed to enable a technical and quantitative assessment of the extent of contamination, thereby promoting greater transparency and legal certainty in the handling of digital traces in forensic contexts.

8.5 NUMERICAL EXAMPLE OF THE CONFIDENCE FUNCTION

Consider a total of 100 events, of which 96 were documented correctly.

Then we have:

D = 96

U = 4

Applying the formula: C = 96 / (96 + 4) = 0.96

Therefore, the trace shows high reliability under the defined criterion, in this specific scenario.

9 PROCEDURAL AND ALGORITHMIC FORMALIZATION

To reinforce the reproducibility of the experiment and the practical applicability of the controlled contamination concept, this section presents the formalization of the study's main procedures in pseudocode. The algorithmic representation sought to standardize and structure the critical stages of the chain of custody and the execution of the forensic experiment, thereby promoting greater methodological clarity and enabling its integration into technical frameworks and automated systems. The described algorithms align with internationally recognized forensic practices and were developed to facilitate the adoption of the proposed structure by experts and forensic tool developers.

9.1 PSEUDOCODE FOR CHAIN OF CUSTODY WITH CONTROLLED CONTAMINATION

The following algorithm represents the logical flow of a chain-of-custody process that incorporates the concept of controlled contamination, enabling the registration, tracking, and differentiation of routine forensic events and justified technical interventions.

Figure 8

Simplified representation

```
Algorithm ChainOfCustodyWithControlledContamination

Input: digital evidence E
Output: chain of custody log with traceability

Initialize chainOfCustody ← []

For each event in forensicProcess:
    event ← CaptureEvent()
    timestamp ← GetTimestamp()
    hash ← CalculateHash(E)

    If event == "download":
        MarkAsContamination(event)
        ContaminationRecord ← {
            type: "controlled contamination",
            timestamp: timestamp,
            artifacts: DownloadedFiles(),
            hash: hash
        }
        Add(ContaminationRecord, chainOfCustody)
    Otherwise:
        NormalRecord ← {
            type: "normal event",
            timestamp: timestamp,
            event: event,
            hash: hash
        }
        Add(NormalRecord, chainOfCustody)

Return chainOfCustody
```

Source: Author.

This structure enables the technical documentation of controlled contamination throughout the chain of custody, ensuring auditability and reinforcing the validity of the digital trace in specific forensic contexts.

9.2 PSEUDOCODE OF THE EXPERIMENTAL PROCEDURE

Next, Figure 9 presents pseudocode for the laboratory experiment described in this study, detailing the critical stages of the simulation, from collection to trace analysis, with contamination tracking.

Figure 9

Controlled Contamination

```
Algorithm ControlledContamination

Initialize system with originalDisk (120GB)
Connect to the OneDrive account
Download files (.doc and .pdf)
For each downloaded file:
   Generate SHA-1 hash
   Store metadata (creation, modification, access)
   Record event as "controlled contamination"
Clone originalDisk bit by bit to forensicDisk (240GB)
Validate cloning integrity using comparative hash
Analyze timeline using EnCase
Isolate contamination interval (download events)
Document contamination
Validate evidence reliability

End
```

Source: Author.

The algorithmic representation facilitates standardization and reproducibility of experiments in forensic environments, providing a logical basis for the practical implementation of the controlled contamination concept.

10 DISCUSSIONS

The discussion of the experimental results underscores the need for a clear criterion to distinguish a usable trace from a completely compromised trace.

The findings demonstrate that, as long as the alteration is appropriately documented and traceable, the trace remains valid for the investigation in specific scenarios.

The differentiation between a controlled modification and an irreversible contamination depends on the ability to isolate the alterations and guarantee that the original part of the trace remains intact and reliable.

Detailed documentation of the alterations is essential to ensure the admissibility of evidence, preventing controlled interventions from being mistaken for irreversible compromises.

Finally, the practical application of this concept in digital forensics requires standardizing records of contamination within the chain of custody. The implementation of specific guidelines for controlled contamination can increase the security and reliability of digital evidence in real investigations, ensuring that modifications necessary for data preservation do not invalidate their probative utility

11 CONCLUSIONS AND LIMITATIONS

The results of this study demonstrated that the Controlled Contamination concept is feasible in certain scenarios, provided that there is a rigorous process for identifying, documenting, and isolating contamination. This approach allows the digital trace to continue to be used in investigations, ensuring traceability of alterations and data integrity.

Controlled contamination may represent an evolution in how the chain of custody addresses accidental modifications or necessary interventions during trace collection, thereby improving the criteria for accepting digital evidence.

This study opens the door to revisions to the admissibility criteria for digital traces, suggesting a new technical artifact that can be incorporated into forensic examination guidelines.

Even though the ideal scenario is one where no type of contamination occurs, the study reinforces that, when properly controlled and documented, contamination does not necessarily or automatically compromise the validity of the evidence.

In the specific case of the cloud-based download performed before imaging the equipment, it was demonstrated that the integrity of the original trace was preserved because the procedure was conducted in a controlled manner and without interference with the set of pre-existing data in the allocated area.

Furthermore, the files were stored in a designated area of the media under the supervision of a specialized expert. They maintained their probative value because they were extracted as relevant elements before any intentional deletion intended to conceal evidence.

However, it is necessary to consider that, in specific scenarios, contamination may cause overwriting in memory sectors and impacts on non-allocated areas, which could hinder techniques for recovering previously deleted files, such as forensic carving. Although this may affect the investigation by reducing the likelihood of recovering deleted data, it does not automatically invalidate the trace; instead, it imposes additional challenges on the analysis.

Given the findings, it is recommended that specific forensic protocols be developed to document controlled contamination, establish a traceability structure that enables validation of which parts of the trace remain reliable, and adapt forensic norms to account for this type of scenario in the analysis of digital evidence.

Regarding the study's limitations, it is essential to note that the experiment simulated a single practical case. In contrast, numerous other controlled contamination scenarios can occur, such as extractions from mobile devices.

Future studies may explore these variations to validate the applicability of the concept on a larger scale and in different forensic contexts. Furthermore, the impact of contamination may vary with the operational environment and the type of digital trace analyzed, underscoring the need for additional experiments to extend the applicability of the proposed methodology.

It is recommended as good practice to immediately record the *hashes* of downloaded files, documenting them in the collection terms still at the seizure location, always in the presence of the court officer or the parties present. This procedure strengthens the chain of custody, ensuring the trace's reliability and mitigating the risk of future judicial challenges to the evidence's validity. The adoption of standardized forensic structures and frameworks can contribute to consolidating this process, ensuring that controlled contamination is applied in a technically and legally secure manner.

Finally, in this research, by crossing the laboratory testing procedures performed with the elements of the literature review, which indicate the need to assess evidence admissibility case by case, considering the real impact of controlled contamination on its reliability, it was evidenced that, in the analyzed scenario, the trace can be admitted, even if contaminated. This result reinforces the Controlled Contamination concept, demonstrating that, when properly documented and traceable, contamination does not necessarily or automatically invalidate the evidence, contributing to a more flexible and pragmatic understanding of the chain of custody in forensic investigations.

REFERENCES

Arellano, L. E., & Castañeda, C. M. (2012). La cadena de custodia informático-forense. Revista ACTIVA, (3), 67–81. ISSN 2027-8101

Brasil, E. C. A. (2023). Identificação e análise das ferramentas de computação forense aplicadas em investigações no Brasil [Trabalho de Conclusão de Curso, Bacharelado em Sistemas de Informação, Universidade Federal do Ceará, Campus Quixadá]. Quixadá, Brasil.

Brasil. (2019). Lei n. 13.964, de 24 de dezembro de 2019. Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), e a Lei n. 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), e outras normas. Diário Oficial da União. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm

Cantore, J. A. G. (2014). Cadena de custodia de evidencias. Anales de la Facultad de Ciencias Médicas, 47(1).

Carvalho, R. W. R. (2020). A importância da cadeia de custódia na computação forense. Revista Brasileira de Criminologia, 9(2), 134–138. https://doi.org/10.15260/rbc.v9i2.463

Castellanos, B. J. P. (2017). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales. Cuadernos de Contabilidad, 18.

Grigollo, F. V., & Fernandes, R. F. (2024). Study on the adoption of historical record and chain of custody by Brazilian judicial experts from the collection to the disposal of evidence: A survey questionnaire. Revista de Gestão Social e Ambiental, 18(8), Article e08431. https://doi.org/10.24857/rgsa.v18n8-168

Grigollo, F. V., & Fernandes, R. F. (2025). Proposal of a conceptual framework to represent the historical record of events in the chain of custody: A doctoral thesis review. Derecho y Cambio Social, 22(80), Article e2660. https://doi.org/10.54899/dcs.v22i80.2660

Machado, N. T., & cols. (2021). Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta. Revista Científica General José María Córdova, 19(33), 181–203. https://doi.org/10.21830/19006586.726

Ministério da Justiça e Segurança Pública (Brasil). (2023). Diagnóstico e proposição de um modelo sobre a cadeia de custódia no Brasil: Estudo preliminar em cinco capitais representantes das cinco regiões brasileiras. MJSP.

Nandhakumar, N. K., Agarwal, U., & Faizal, H. (2012). Use of AFF4 chain of custody - Methodology for foolproof computer forensics operation. International Journal of Communication and Networking System, 1(1), 49–54. ISSN 2278-2427

Poersch, C. G., & Kuntze, G. M. (2010). Modelo de coleta e análise de vestígios em sistemas computacionais. Universidade do Sul de Santa Catarina.

Martínez-Ramírez, D. A., & cols. (2019). Evidência digital focada em unidades de estado sólido (SSD): Uma revisão. Visão Eletrônica, 1, 183–198.