Forensic Science International: Digital Investigation 44 (2023) 301501

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS 2023 EU - Selected papers of the Tenth Annual DFRWS Europe Conference

Contamination of digital evidence: Understanding an underexposed risk

Jan Gruber [a], Christopher J. Hargreaves [b], Felix C. Freiling [a, *]

[a] Department of Computer Science, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Martensstr. 3, 91058, Erlangen, Germany
[b] Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford, OX1 3QD, United Kingdom

ARTICLE INFO

Article history:

Keywords:
Contamination
Digital evidence
Digital investigations

ABSTRACT

The dangers of contamination have received considerable attention in the literature regarding the investigation of physical crime scenes and physical evidence. The understanding of contamination in the context of digital evidence appears to be much less understood. Based on experiences from the field of physical evidence, we develop a generalized definition of contamination that also covers digital evidence, namely the "inadvertent transfer of traits to an object of relevance at any point in the forensic process". We illustrate the definition by presenting several examples and counterexamples for contamination of digital evidence. By addressing the specifics of digital evidence in this context, we argue that our definition can be useful to understand the risks arising through contamination in this domain.

1. Introduction

Between 1993 and 2009, German law enforcement chased an unknown female serial killer known as the "Phantom of Heilbronn". The hypothesis on the perpetrator was formed based on DNA evidence that had been found on all crime scenes. The chase came to a dramatic end when it turned out that the DNA belonged to a woman who had been working at the factory producing the cotton swabs used to gather the DNA traces: the phantom was the result of evidence contamination.

This story is just one of several notable examples in which physical evidence had been inadvertently altered by adding DNA from other sources. All these examples illustrate the risks of handling evidence that is invisible to the human eye. For decades now, forensic technicians have been well aware of (cross-) contamination when conducting classical crime scene work (Lee et al., 2001, pp. 56 & 259), and so for physical evidence, where "[c]ontamination is a fact of life for investigators" (Gehl and Plecas, 2017, p. 143), there appears to be an increasing awareness for the adverse effect in that contamination "can have a significant negative impact on the investigation if the existence of the contamination is not known" (Schwendener et al., 2016, p. 517). Therefore, forensic science developed strict regulations and processes on how to act and proceed at a crime scene, an example being so-called "Police Elimination Databases" like those employed in Austria (Pickrahn et al., 2015), which have been set up to help identifying crime scene contaminations by investigators. Still, while it is not known with certainty in how many cases a DNA sample is contaminated by investigators or examiners (Fonneløp et al., 2016, p. 122), studies from Austria suggest that approximately 1–2% of biological traces are contaminated (Pickrahn et al., 2015).

Since physical evidence is often considered to be fundamentally different from digital evidence, the question arises whether contamination is also possible when handling digital evidence. This question is becoming increasingly relevant as investigative methods get closer to running or "live" systems. The challenges of encryption and ever-increasing volumes of data have led incident responders and forensic investigators to develop and explore methods like triage (Casey, 2013), live analysis (Adelstein, 2006), and selective imaging (Faust et al., 2021). However, interacting with a live system will inevitably result in changes that provide an increased potential for inadvertent modifications; in addition, it can be shown that this holds true both for work at the crime scene but also for post-acquisition lab environments.

Given this chance of modifications to the examination object or derived evidence, there is an urgent need to discuss the phenomenon of contamination at digital crime scenes more clearly. Previous works (Lyle, 2006; Lim and Khoo, 2009; Delport and Olivier, 2012) already identified contamination as a problem by name, but did not go into the details of this specific topic. So overall, contamination of digital evidence remains an elusive concept.

In this paper, we revisit works on traditional contamination published in other subdisciplines of forensic science and identify

* Corresponding author.
E-mail address: felix.freiling@fau.de (F.C. Freiling).

https://doi.org/10.1016/j.fsidi.2023.301501

crucial properties of contamination (Section 2). Based on these, we develop a generalized definition of contamination—valid both for physical and digital evidence—in Section 3, namely the "inadvertent transfer of traits to an object of relevance at any point in the forensic process". We illustrate the definition by presenting several examples and counterexamples for contamination of digital evidence (Section 4). By addressing the specifics of digital evidence in this context, we argue that our definition can be useful to understand the risks arising through contamination in this domain (Section 5).

Overall, our exposition is intended to serve as a proposal to the community to develop a common understanding of an important yet underexposed phenomenon. Highlighting its intricacies, we point to several remaining challenges and outline a research gap (Section 6).

2. A brief history of contamination research

Based on decades of experience with physical evidence, researchers in forensic science appear to be well aware of contamination effects and have already proposed guidelines and best practices to avoid them. We now briefly revisit some milestones on this path and then characterize common elements of definitions of contamination. As contamination seems to be most relevant (and probably most dangerous) when dealing with microscopic particles, it is not suprising that most of the literature concerns handling of DNA evidence.

2.1. An overview of physical contamination

Already back in 2005, van Oorschot et al. (2005) described that fingerprint brushes, gloves, and other tools routinely used during examinations could contaminate evidential items. This can happen either via direct DNA transfer initiated by the forensic technician or via an indirect DNA transfer by items being previously examined (Poy and van Oorschot, 2006). In the past, such shortcomings in contamination avoidance during lab work also led to severe consequences and false accusations in actual proceedings (see Morris, 2012, as an example).

Those observations were then taken up by Meakin and Jamieson (2013) who presented a review of the risk of transfer of so-called "trace DNA"—a term that describes a small number of DNA particles "that cannot be attributed to a particular biological source", but contain enough information to recover a full DNA profile and identify an individual person (Meakin and Jamieson, 2013, p. 434). They described scenarios of direct and indirect transfer of trace DNA and presented several factors affecting deposition, persistence, and analytical recovery.

Given the increased sensitivity of DNA analytics, Margiotta et al. (2015) conducted experiments regarding the contamination risk by gloves in forensic casework and quantified a high risk of DNA transfer, which underlined the need of awareness, the necessity of DNA-free gloves and instruments, appropriate cleaning systems and multiple layers of gloves. Additionally, Fonneløp et al. (2016) experimentally analyzed the risk of contamination caused by police investigators and secondary DNA transfer from evidence bags and underlined that there is a need to evaluate existing practices, identify weaknesses in evidence handling, then suggest and implement improvements in the lab to finally demonstrate the effectiveness of contamination monitoring (Fonneløp et al., 2016, p. 122). As the main result of their work, Fonneløp et al. (2016) presented 12 practical guidelines that reduce the risk of contaminating a DNA sample. Those included guidelines, like the frequent change of gloves and the wearing of double gloves, the separation of suspect and victim exhibits, establishing national elimination databases and other recommendations (Fonneløp et al., 2016, p. 128). Pickrahn et al. (2017) quantified the chance of DNA contamination in Austrian cases and underlined the importance of reference profiles stored in such databases since they identified that police contamination is a real issue (Pickrahn et al., 2017).

2.2. Efforts to grasp traditional contamination

Besides laboratory studies that have been motivated by practical needs, Inman and Rudin (2000) discuss the issue from a conceptual point of view and provide the following working definition of contamination (Inman and Rudin, 2000, p. 211):

> "Any substance inadvertently introduced into or onto an item of evidence after its recognition by a responsible party."

Their definition focuses on the physical matter ("substances") added to an evidence item *after* the crime scene has been identified and secured.

A comparable but differing definition is put up by Grübler (2021 translated by the authors)[1]:

> "Unintentional contamination of traces and reference material with a similar material that is irrelevant for the creation of the evidence […]. If the contamination is not recognized, the trace causation leads to false-positive results […]."

Grübler (2021) also refers to the physical matter (calling it "material") but further specifies that contamination cannot occur with any material but only with the same kind of material. Moreover, both emphasize the unintentionality of the act. Conversely, Grübler (2021) does not consider temporal aspects and omits to limit the time frame in which contamination could occur. Another difference is that he includes—in contrast to Inman and Rudin (2000)—the actual effects of undetected contamination ("false-positive results") in his definition.

Gehl and Plecas (2017, p. 113) are even more explicit in their criminalistics textbook:

> "Contamination is the unwanted alteration of evidence that could affect the integrity of the original exhibit or the crime scene. This unwanted alteration of evidence can wipe away original evidence transfer, dilute a sample, or deposit misleading new materials onto an exhibit."

In their definition, they focus not only on the ultimate outcome, as Grübler (2021) did, but the more subtle effects on the evidence. In a broader understanding, they include evidence destruction ("wipe away") as well. In agreement with the previous definitions, they also focus on the physical matter ("materials"; "sample"). Since they use the adjective "unwanted", they make clear that the effects are undesired. In this definition, the temporal aspect, which is emphasized by Inman and Rudin (2000), is also missing.

[1] Original wording: "unbeabsichtigte Verunreinigung von Spuren und Vergleichsmaterial mit gleichartigem, aber für die Spurenentstehung irrelevantem Material […]. Wird die Verunreinigung nicht erkannt, führt die Spurenverursachung zu falsch-positiven Ergebnissen (Trugspuren)." (Grübler, 2021, pp. 362 f.).

Although Gehl and Plecas use the terms “exhibit” and “crime scene”, what necessitates that the items and locations have to be recognized as such beforehand, their comments clarify, however, that they do not draw temporal distinctions, which makes it difficult to distinguish these effects from other concepts, like evidence dynamics (Chisum and Turvey, 2000) in general.

Lastly, we have a look at an official definition of a standards body: The standard ISO 21043−1:2018(en) 'Forensic Sciences Part 1 Terms and Definitions' by ISO/TC 272 (2018) is more brief. According to this document, contamination is the

> “undesirable introduction of a substance to an item at any point in the forensic process ”.

While the other definitions refer to evidence, the ISO's definition refers to “item[s]”, which are in turn defined as any “object, substance or material that is collected, derived or sampled as part of the forensic process” (ISO/TC 272, 2018, 3.19). Using this definition, they limit the scope of contamination on relevant items. Again, the standardization body focuses here on physical matter. They regarded a temporal confinement since the forensic process must have been started, and the result is characterized by undesirability—only implicitely stating missing intent.

2.3. Aspects of a common definition of physical contamination

There exist several other definitions focusing on biological evidence. While Schwendener et al. (2016, p. 518) distinguish between contamination and pollution, other publications describe similar aspects as those used in the definitions above (see, for example, Pickrahn et al., 2015; UK Forensic Science Regulator Guidance, 2016). So while the above definitions differ from each other in detail, we can observe four intersecting aspects:

1. an alteration through introduction (or transfer) of substance,
2. an item of evidence in the forensic process,
3. temporal confinement to the forensic process, and
4. unintentionality.

While the focus of all definitions was physical evidence, interestingly, all but the first aspect are directly applicable also to digital evidence. We revisit these four aspects in the following section, in which we develop a generalized definition of contamination that covers both physical and digital evidence.

3. A generalized definition of contamination

We now revisit the four aspects of contamination definitions identified in the previous section and investigate their applicability to digital evidence in order to arrive at a more general definition of contamination. We begin with the arguably most important aspect.

3.1. Alteration through transfer

The first aspect concerns the alteration of evidence through the introduction of physical matter. While it appears unreasonable to apply this to digital evidence, it has been observed that the transfer of physical matter is not the core concept underlying evidence modification (Inman and Rudin, 2002). For example, toolmarks leave traces at the crime scene without exchanging physical substance. The underlying principle rather is the more general notion of *transfer of traits* (Inman and Rudin, 2002, p. 15), meaning the transfer of patterns that change the interpretation of what is found at the crime scene. It is straightforward to observe that such transfers can also happen in the domain of digital evidence. In general, such transfers exist in various manifestations which can be classified as additive or subtractive, actively or passively induced, and direct or indirect, as illustrated in Fig. 1.

The addition or removal of evidence is considered on a semantic level. By using these terms, we differentiate between introducing new information or removing existing one. For some readers, it may appear somewhat surprising that this concept includes the destruction of traces. Still, one can understand the removal of traces as another transfer with a new pattern that contains less information of relevance. As an example in the physical domain, one might think of a footwear mark on a dusty surface, where investigators fail to protect it from heavy rain by setting up an appropriate cover. In the digital domain, we can imagine similar effects, like overwriting ring buffers or chunks of data that have been marked free before, hence introducing new patterns.

Moreover, trait transfers can be passive or active, as indicated in the above examples. We consider it to be active if it is linked to an investigator's action and, thus, its immediate effect. Conversely, we believe a transfer to be passive if it is a consequence of the refrainment to take a necessary measure to avoid or stop it. In both cases, the investigators are responsible for the contamination that occurs.

Finally, the transfer may not necessarily be induced directly. New traits could be brought in via an intermediary tool, system, or person as well. For example, at a physical crime scene, an intermediary contaminating tool might be a fingerprint brush, an evidence bag, or another item used during the examination, as described by Poy and van Oorschot (2006). In the digital domain, failure to sanitize media prior to a disk clone, could be analogous.

It is worth noting that, at least in theory, such modifications—including relocation, obscuration, obliteration, and removal of evidence—are entirely avoidable.

3.2. Object of relevance

All previously mentioned definitions of physical contamination refer to items and further restrict those by speaking of evidence, traces, or—in the broadest sense—anything collected during the forensic process. By narrowing down this second aspect, we stress that it is not about the alteration of any object but an object that is considered ex ante of relevance for the investigation. To be contaminated, such an object must be subject to a transfer of traits, which results in a violation of evidence integrity,[2] thus altering the semantics of the evidence comprised of the physical or digital object at hand.

It is worth noting that contamination is defined regarding an object and not a specific location, such as the scene of the deed or a body location since there are several occasions for contamination to happen—not just at a crime scene but also in lab environments.

3.3. Temporal confinement

Besides the spatial aspect, the concept of contamination should be restricted to a confined period of time. It is paramount to underline that it can only occur after investigators of law enforcement or another empowered and responsible party have identified the object mentioned above as potentially relevant for the investigation, and initiated the forensic process by doing so. This commonly

[2] Rare and rather theoretical edge cases, like an in situ replacement of an identical byte string, are intentionally not captured by our definition because it does not have any adverse effect.

involves establishing necessary crime scene protocols and other precautions during seizure and lab work.

Drawing on the definitions of ISO/TC 272 (2018) and Inman and Rudin (2000), changes before the initiation of the forensic process are not considered contamination. The term *evidence dynamics*, a concept described initially by Chisum and Turvey (2000, p. 7) that refers "to any influence that changes, relocates, obscures, or obliterates physical evidence, regardless of intent", captures such temporally preceeding changes (See also Chisum and Turvey, 2011, p. 144).

Thus, contamination is directly related to the protective function of the police officers or any competent investigator, analyst, or examiner tasked with conducting the forensic process, which includes securing evidence from any alteration after locking the scene, and the subsequent analysis and examination activities.

3.4. Missing intent

Lastly, the salient feature is missing intent regarding the transfer of traits. In crime scene and laboratory work, the central paradigm is to limit changes to evidence as much as possible; however, sometimes they are inevitable and, therefore, they are allowed as long as necessary, when the person is competent to decide and able to explain the relevance and implications (Williams, 2012, p. 6). This stems from the trade-off between completeness of the evidence collection and intrusiveness, i.e., the number of induced changes, of the employed method (Hargreaves, 2009, p. 118 ff). With physical evidence, some analyses require the destruction of (parts of) the evidence item. Such trade-offs also exist in the digital domain: think of the acquisition of the main memory of a running system, which necessitates an intrusive interaction and specific changes to it (Huebner et al., 2007, pp. 2 f.) because the alternative is missing potentially crucial volatile memory.

Thus, the feature of unintentionality is characterized by the fact that the investigator does not consider that conducting a measure or its omission will result in unintended and unforeseen modifications. This feature distinguishes contamination sharply from deliberate changes. On the one hand, a conflict of investigative objectives might necessitate intentional changes that require accepting the unavoidable alteration. On the other hand, a badly intended change by the investigator with the goal to compromise the availability or usefulness of evidence to the forensics process (Harris, 2006) has to be considered as evidence tampering.

3.5. Definition

We now combine the four aspects presented above into a generalized definition of contamination:

> Contamination is any inadvertent transfer of traits to an object of relevance at any point in the forensic process.

In solid distinction to the concept of evidence dynamics, we emphasize temporal demarcation and unintentionality. Therefore, we consider contamination and its effects to be a subset of evidence dynamics, as illustrated in Fig. 2. A distinction between the more general evidence dynamics and contamination is helpful because the latter is directly affected by the investigators' actions. However, the exact point in time of its start might be subject to the forensic process model used.

Overall, all changes to relevant pieces of evidence after the initiation of the forensic process violating its integrity without intent must be called contamination. We believe that the generalized definition provides a common ground by taking a new and more precise perspective on contamination because it abstracts from the specifics of physical evidence and holds for both physical and digital evidence. While remaining applicable to physical evidence, our new definition helps to characterize the existence of contamination in digital investigations more accurately, as illustrated by examples in the following section.

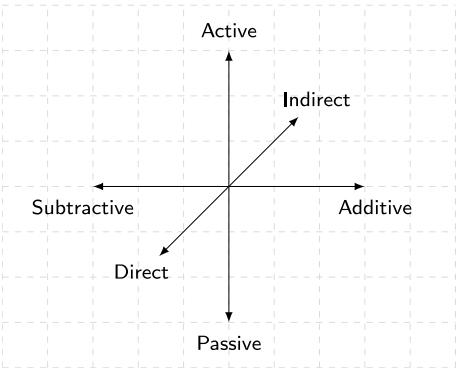

Fig. 1. Three dimensions of transfer of traits for contamination; contamination can stem from a measure taken by a responsible party (active) or the refrainment from taking some action (passive). By doing so, either new information is brought to the object of relevance (additive), or it could be removed from it (subtractive). Such a transfer could happen via another system involved (indirect) as well as without any intermediary (direct).

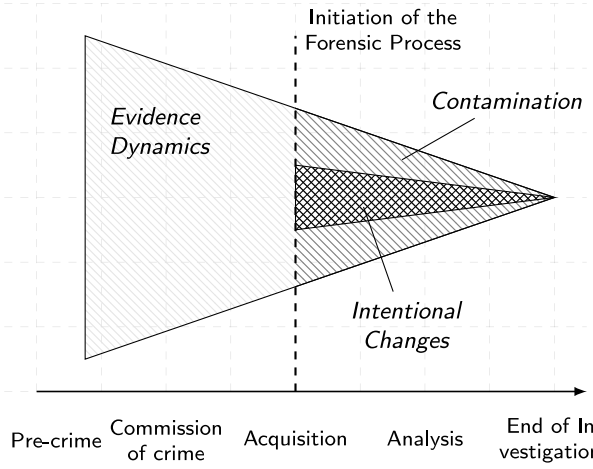

Fig. 2. Relation of contamination to the broader concept of evidence dynamics described by Chisum and Turvey (2000); Most notable is that contamination can be considered a subset of evidence dynamics connected to the investigator's actions after identifying an object of relevance. It is important to strictly distinguish those from intentional changes necessitated by the analysis process itself or stemming from a conflict of investigative goals. The conical shape should indicate that there tends to be less opportunity for evidence dynamics and contamination as the process progresses toward the end of the investigation.

4. An example-guided contemplation of digital evidence contamination

With the goal to further improve the understanding of contamination in the digital domain and explore the applicability of the previously presented definition, we give several examples of Digital Forensics (DF) fieldwork that result in contamination, and then we present non-contamination examples to delineate the phenomenon. Lastly, we examine two edge cases that illustrate that it is not always as easy to grasp and categorize the phenomenon.

Table 1
Classification of the contamination examples discussed in Section 4 regarding the characteristics of the respectively observed transfer of traits and the phase of occurrence.

Scenario	Characteristics of the trait transfer			Phase
	Additive/Subtractive	***Direct/Indirect***	***Active/Passive***	
File deletion by systemd-tmpfiles-service	Subtractive	Direct	Passive	Live response
Media data copying by thumbnailing service	Additive	Direct	Active	Live response
Malware artifact deletion by EDR action	Subtractive	Direct	Passive	Live response
Cloud storage synchronization	Additive/Subtractive	Indirect	Passive	Live response
Cache overwrite of smart home sensor	Additive/Subtractive	Direct	Active	Live response
Modifications by SQLite write-ahead log	Additive/Subtractive	Direct	Active	Lab work
Failing to employ software write blocking	Additive/Subtractive	Direct	Active	Lab work
Remote wipe of mobile device	Subtractive	Indirect	Passive	Lab work
Signal's RCE in Cellebrite UFED	Additive/Subtractive	Indirect	Passive	Lab work

4.1. Examples of contamination

First, we discuss several occasions of contamination during live analyses; afterward, we refer to contamination in lab work. In both phases, we aim to capture the phenomenon's essence by highlighting and discussing the previously identified properties of possible and not even unlikely scenarios summarized in Table 1. This excursion should illustrate by example that adapting the definitions from the physical domain captures what we also intuitively understand as contamination.

4.1.1. Contamination during live responses

Media Data Copying by Thumbnailing Service: To provide convenient file previews to the user, modern desktop environments, such as GNOME (as well as XFCE), run a thumbnailing service. GNOME, for example, relies on a D-Bus service called `Tumbler`, which provides thumbnails for various URIs and MIME types upon an application's request. To do so, it can resort to plugins, such as the `FFmpegThumbnailer`, `PopplerThumbnailer` and others.[3] Following the "Thumbnail Managing Standard" by Finke and Sessink (2001), thumbnails are stored in the user's home directory. Conducting a live response using a storage medium containing some files of types that are considered by the thumbnailing service and its plugins can, therefore, lead to copying the file previews to the system under investigation if the investigator opens a directory containing those files via the file browser. The investigator who does not intentionally want to copy those data to the system under investigation actively initiates a direct and additive transfer of traits of the thumbnail information to the object of relevance after the forensic process has been started. The use of an unclean storage media in this example can be seen remotely analogous to a polluted cotton swab for collecting DNA trace material.

File Deletion by systemd-tmpfiles: Modern servers run many daemon processes to keep the system in good condition. One essential and on many Linux distributions already pre-installed service is `systemd-tmpfiles`, which automatically creates, deletes, and cleans up certain volatile and temporary files (Debian, 2022). For long-running server systems, this service offers a convenient timer-based solution to clean up space routinely. During a live response, such a timer-based clean-up could be initiated by `systemd-tmpfiles`, which might delete crucial evidence from the system under investigation. The investigator's passive omission to disable this autonomous service of the operating system may lead to a direct and subtractive transfer of traits, although the forensic process has already been initiated. One might argue that digital deletion is not subtractive since it is just overwriting several data fields with zeros (or another value indicating its invalidity), which comprises an additive transfer. While this is plausible on a low level, it seems preferable to define this on the semantic level of evidence regarding the case-relevant available information. Furthermore, there is an increased risk of unwanted and irreversible removal of traces when working with devices that are capable of wear-leveling/trimming.

Malware Artifact Deletion by Endpoint Detection & Response (EDR): When a serious incident occurs, and the stress level rises, many processes run in parallel, and mitigation, as well as containment measures, might intervene more than required. An obvious example is an endpoint detection and response agent doing its job after updating signatures. While this is desirable from the viewpoint of cyber defense, it may destroy crucial evidence, e.g., an implant stored as an obfuscated "one-liner PowerShell script" in an autostart-registry key, which must be considered an object of relevance for the investigation and should have been analyzed further. Such a deletion of malware artifacts by the EDR comprises a direct and subtractive trait transfer. When it happens before the forensic process has been kicked off, then it is certainly part of evidence dynamics; however, if it happens passively after initiating the forensic process due to omitting to synchronize between analysis and containment activities, we consider it to be contamination, which might make the job unnecessarily hard and jeopardize the investigation.

Cross-Device Synchronization of Cloud Storage: Cloud storage services, like Dropbox, Google Drive, OneDrive, and iCloud, offer the ability to conveniently store and share files to colloborate. They synchronize seamlessly between different devices and provide the option to share specific data with certain users (Farina et al., 2014). Unsurprisingly, such services have also been misused to share Child Sexual Abuse Material (CSAM) between offenders. In practice, investigators might conduct a live response when executing a search warrant in such a case to circumvent encryption. If the system under investigation is then still connected to the internet for some time, which might be necessary in some cases to lawfully acquire remote data accessible by the machine, background synchronization of one of the above-mentioned cloud storage services might result in a passive transfer of traits. Given that some remote storage infrastructure is involved, this transfer is indirect in its nature. Imagine a case when an accomplice has been tipped off and tries to cover his tracks by deleting files from a shared folder providing an excuse to the offender who might claim that he did not even want to possess the material and has already tried to delete it. Here, it is a decision that needs to be made while considering the benefits and risks of maintaining or removing network connectivity. The choice

[3] https://gitlab.xfce.org/xfce/tumbler/-/tree/master/plugins, commit `1d304f4`.

should be intentional, and informed; the discussion of contamination issues can feed into that decision.

Cache Modifications in Smart Home Devices: Another variant of a cache overwrite with a cyber-physical dimension can be found in the field of smart home devices. Certain lightbulbs are equipped with a motion sensor to trigger switching on the light. In the case of death investigations, for instance, timestamps related to motion sensor activations could be important evidence. However, some products, for example specific motion sensors, cache such timestamps only for the last activation, thus having the potential to be easily overwritten (DSTL, 2020, Fig. 10). Now imagine a missing person case; when the responding detectives enter the apartment to find a body, their movement inevitably leads to overwriting the motion sensor's last activation timestamp. This timestamp update comprises a direct and additive trait transfer, ultimately resulting in a loss of information. In such a scenario, detectives must consider this piece of data an object of relevance because it may be a crucial piece of evidence to narrow down the time of death.

4.1.2. Contamination during lab work

Looking at the following examples, we show that contamination cannot only occur when dealing with "live" systems but also in lab analyses.

Failing to Boot into Forensic Live OS: Nowadays, DF laboratories may resort to software write blockers in the form of bootable live Operating Systems (OSes), e.g., *Grml-Forensic*[4] or *TSURUGI Acquire*,[5] because physical withdrawal of storage media is often not possible anymore when examining modern notebooks. Those forensic live OSes used for acquisition employ kernel-level write protection; however, if—for one reason or another—the examiner fails to hit the required key sequence to boot directly into the forensic live OS, various modifications, like updates, changed access timestamps, cache clean-ups, and other autonomous actions, happen. This inevitably results in contamination in the form of an actively induced direct transfer of traits—possibly a wild interplay of simultaneously adding and removing relevant information.

Remote Wiping of Mobile Devices: Not only the provider of tailored “crypto phones” like the infamous *EncroChat devices* but also the major manufacturers of mobile operating systems, i.e., Apple and Android, provide their customers the ability to remotely conduct a factory reset of a smartphone linked to their account in case of loss or theft.[6] Criminals could misuse this feature to cover their traces after being targeted by investigating authorities who seized their devices. Therefore, a Standard Operating Procedure (SOP) is to cut off the network connectivity of mobile devices. Nevertheless, there are various imaginable ways where remote wiping could occur, though: obviously, one option is that the seizing officer might fail to activate the so-called “airplane mode”. Another option could be that the seized device runs out of battery when lying on the backlog waiting to be processed. If the device is then powered with some network connectivity enabled (e.g., a SIM still included, an eSIM, or Wi-Fi enabled), and a failure to use Faraday solutions, the device might connect to the internet and receive the command to perform a factory reset. In both cases, we observe a passive, indirect, and subtractive transfer of traits, thus, leading to an inevitable loss of evidence because every potential digital object of relevance stored on the mobile device has been wiped.

Modifications by SQLite Write-ahead Log: SQLite databases are important datastores, especially common on mobile devices today. A journal, the so-called write-ahead log (WAL), is frequently used to provide atomicity and durability. Its task is to buffer changes made to the database; after a certain number of operations, they are executed at once (Liu et al., 2016, p. 561). To conduct in-depth analyses, examiners often need to extract those file-based databases from previously acquired images. However, when regular SQLite database viewers are employed to view such databases, those tacitly apply changes recorded in a potentially provided write-ahead log, which may result in loosing important evidence by viewing only the “full up-to-date version” of the datastore (Caithness, 2012). While the original disk image's integrity remains untouched, the integrity of the derived piece of evidence is inadvertently violated since committing changes in the WAL constitutes an actively induced direct transfer of traits onto the object of relevance—the SQLite database. This can lead to an addition or subtraction of traces which is relevant if that derived copy is relied on as evidence. Think of a deleted entry that is committed just by opening the SQLite database.

Signal's RCE on Cellebrite UFED: In 2021, Signal's technical report, in which they documented how they have achieved Remote Code Execution (RCE) on the forensic tools called Cellebrite UFED and Physical Analyzer, alerted many forensic practitioners. There, Marlinspike described how a vulnerability in FFmpeg, which had been used for file parsing by these Cellebrite products, could lead to RCE during the processing of the acquired evidence and, hence, allows compromising the examination (Marlinspike, 2021). Though remaining a mind game, Marlinspike (2021) pointed out what we consider an interplay of anti-forensics and contamination. Hypothetically, an actual exploit payload could “seek to undetectably alter previous reports” or “compromise the integrity of future reports” (Marlinspike, 2021).[7] Such an anti-forensic measure (undoubtedly constituting a criminal act, of course) would initiate a trait transfer after starting the forensic process during the DF examination and severely hamper the integrity of the data acquisition, which constitutes the object of relevance here. The DF examiners have no intent for such a modification but are obliged to avoid it by using up-to-date and secure tools, much like they would be obliged to keep unauthorized persons out of the crime scene perimeter. This points out the risk of contamination stemming from anti-forensics.

4.2. Examples of non-contamination

To further delineate the phenomenon, we now present some counterexamples of contamination, i.e., where certain aspects of the definition are missing. This is critical to ensure that the definition does not go too far since the defined term has a clearly negative connotation.

Well-meaning IT-Support: Consider a compliance case, e.g., related to the disclosure of trade secrets, where high-level management commissions IT-support staff to inspect the respective employee's Windows system to substantiate a gut feeling. Basically, they are instructed to do some triage for e-discovery—a task for which they have never been trained. Unfortunately but unsurprisingly, they do it badly and browse the network share containing

[4] https://grml-forensic.org/, accessed on 06.12.2022.
[5] https://tsurugi-linux.org/, accessed on 06.12.2022.
[6] E.g., Google's “Find My Device App” for Android mobile devices.
[7] The term “report” is used to described the containers created by Cellebrite UFED's acquisition containing the device data.

the trade secrets from the suspect's computer, hence, unwantedly initiating an additive trait transfer regarding all sorts of objects of relevance, like the “shellbags” and “recent files”-registry keys, Microsoft Edge's WebCache, “jump lists”, and so on. While this scenario fulfills three out of four aspects of the definition presented in Section 3, the critical point is that the forensic process has not been initiated yet because the inspection aimed to verify a gut feeling and to establish initial suspicion potentially kicking off an investigation; therefore, we consider this an example of evidence dynamics with obviously very adverse effects. However, we want to stress here that the initiation of the forensic process does only necessitate a responsible party but not necessarily law enforcement authorities of some kind.

Accessing Hidden Disk Areas: The Host Protected Area (HPA) and Device Configuration Overlay (DCO) constitute disk areas whose access is prohibited by the disk controller (Gupta et al., 2006). When inspecting the storage devices in a case related to CSAM, an examiner might consider making those particular disk sectors accessible to ensure they are not missing any relevant sectors. Using `hdparm`, he sends ATA commands to modify the drive's configuration, which constitutes a transfer of traits. This example does not constitute contamination according to the definition above, since two definitional aspects are not fulfilled: The most obvious one is the absence of inadvertence; on the contrary, the action was purposeful and well-balanced since the examiner was aware of only changing the configuration related to the HPA and DCO to acquire more disk sectors. The second aspect ruling out contamination effects is to argue that the disk configuration parameters do not constitute an object of relevance here.

4.3. Examples of edge cases

Scrutinizing various scenarios, we present two examples of evidence acquisition whose categorization regarding contamination effects is debatable.

Jailbreak-enabled Mobile Data Acquisitions: Due to improved device security features, data acquisition of mobile devices is increasingly difficult. One common way to get access to the device data is the use of custom boot loaders. Since digital signatures secure boot chains on modern devices, boot ROM vulnerabilities have been exploited to gain more complete data acquisitions (Fukami et al., 2021, p. 5). An instance of this approach is the so-called `checkra1n`-jailbreak tool for the mobile operating system iOS. Given that iOS runs in a restricted mode to impede access to internal functions or file system data, “jailbreaking” may be employed to gain root privileges and collect certain otherwise unaccessible pieces of data, such as system databases on the device (Katalov, 2019). Obviously, this is an invasive procedure entailing several changes to the device. By introducing a high amount of modifications that might not even be specifiable more closely since it is a closed-source binary, one could argue for the presence of an inadvertent trait transfer. However, in the absence of valid alternatives, examiners might decide to accept a relatively high amount of intrusiveness to improve the completeness of the evidence collection. Therefore, we refrain from calling this contamination since the trait transfers induced by exploiting the boot ROM vulnerability and the OS modifications are on purpose, and the modified objects are considered irrelevant, or at least less relevant than the ones gained; but this is certainly a decision that should be based on a full understanding of the effects of the modifications.

Page Smearing in RAM Acquisitions: In many investigations, examiners can find crucial evidence in main memory. Especially in intrusion analyses, Random Access Memory (RAM) acquisition and its subsequent analysis are needed to identify (fileless) malware artifacts. Still, in classical investigations where encryption is employed, it can be helpful to extract secrets for later use (Hargreaves and Chivers, 2008; Halderman et al., 2009).

However, on modern systems with more than 8 GB of RAM and heavy load, RAM acquisitions might suffer from so-called “page smearing”. This term describes an inconsistency between the acquired page tables and the contents of the physical pages in the dump because they changed during the time needed to perform the complete acquisition. Besides losing eventually crucial data because of overwritten injected code or corrupted kernel data structures, this might also lead to a wrong assignment of memory pages to housing processes (Case and Richard, 2017, p. 24) or corruptions of content data (Pagani et al., 2019, p. 9:5) due to the temporal dimension of the acquisition. The investigators intend to acquire an atomic, consistent, and correct snapshot (Vömel and Freiling, 2012) at the moment of running the main memory acquisition tool of their choice. Yet, there is actually a passive trait transfer stemming from the operating system's ongoing write operations after the forensic process has been started by deciding to acquire the RAM. The trait transfer here can be both additive or subtractive since evidence could be lost by inconsistent kernel data structures or added by some new information placed in memory pages. Though, it is uncertain if an object of relevance is concerned—a question that is hard to answer. When dealing with a virtualized system, it is sensible to resort to the hypervisor and grab the RAM by snapshotting the VM to avoid any smearing in the majority of cases. Nevertheless, if an investigator is confronted with a bare metal system, live smears are practically unavoidable; while not being optimal, collecting RAM with some smearing is definitely more efficacious than losing all the evidence. Hence, we refrain from speaking in black-and-white terms and argue to apply the proposed definition with a sense of proportion.

5. Discussion

In view of the many practical examples and counterexamples provided in the previous Section 4, we now broaden the scope to the overarching aspects and discuss the specifics and the intricacies of digital contamination.

5.1. Specifics of digital contamination

We identified three significant specialties impacting digital contamination, making it substantially different from the phenomenon in the physical sphere. Those are a direct cause of the features of the “abstract” cyber domain.

5.1.1. The wealth of autonomous processes

Most notable is the existence of far more latent processes that might not be noticed by the investigators securing the crime scene. On a (strictly) physical scene, there are similar issues, e.g., insect activities on bodies, the volatilization of gaseous substances, or—most dramatically—the indirect transfer of particles containing DNA. Those, however, are limited in number and not nearly as numerous as arbitrarily running processes on digital systems. Given the real possibility of virtually arbitrary programs running on the system under investigation, another difference is that on a digital system, the evidence and its meaning could be changed entirely by such processes during the examination; in the physical domain, the evidence could not just be dispersed or added arbitrarily. When working with digital evidence, it seems substantially harder to quantify the subtractive variant of

contamination. In contrast, the additive variant might be detected and mitigated in some cases, e.g., think of a log entry caused by the investigator's action. However, it remains opaque, which data was potentially and unknowingly overwritten during the examination. Such opaqueness is a feature that is also reflected in the spatial dimension.

5.1.2. Spatial detachment of cause and effect

Much like the commission of cybercrime, there is a spatial detachment of cause and effect, which is very specific to the cyber domain. We have illustrated several indirect trait transfers involving remote systems in the examples (Section 4). Unlike with analogous evidence, the perpetrator or third parties might retain the ability to remotely intervene on a scene or impact seized evidence, although it has already been "secured" by competent responders. We can imagine several examples in that regard ranging from a still established command-and-control channel during a live analysis, a perpetrator who has not been taken into custody initiating remote wiping of a seized mobile device, to an anti-forensics measure such as the RCE exploiting a bug in forensic tools, as Marlinspike (2021) described. That spatial decoupling indeed is a unique and delicate feature of the digital domain.

5.1.3. Complexity and quantity problems

A major difference is that (strictly) physical and digital crime scenes differ regarding volume, variety, and number of items that have to be considered by the investigators. Carrier (2003) aptly named these specifics the *complexity* and *quantity problem*. With digital traces, it is thus often impossible to discriminate and evaluate their relevance at first. Furthermore, traces in digital systems can have various expressions and characteristics resembling their respective trace abstraction, basically the facet of the trace that is used for establishing an association. Since a tool-based translation of data is always needed to view data at a useful level of abstraction and actually make sense of the facets at hand, it is far more challenging here to identify the "evidence items" than it is in the physical world.

5.2. Intricacies of the common definition

Since our common definition (Section 3) mirrors physical contamination, we now want to critically review it in light of the specifics of digital evidence mentioned above. The *transfer of traits* and its connected qualities, the requirement of *missing intent*, and the temporal placement after the *forensic process initiation* are solid building blocks. However, discussing the *object of relevance* is very intricate because it is tremendously difficult to grasp in digital scenes.

One might argue to exclude this building block from the definition altogether; however, this would lead to an expansion, even a delimitation of covered situations, because it would capture alterations of objects which are clearly irrelevant to a case since they do not even remotely contribute to answering questions of factuality, guilt, and unlawfulness. We want to underline that if an irrelevant object is modified, it should not be called contamination because dropping such a restriction would mean that every real-world crime scene would be contaminated, even with perfect handling of the site.

When working with digital evidence, the problem of determining relevance becomes even more precarious: in many cases, there is only a vague idea of what might be relevant at first. During the analysis, examiners deal with different levels of abstraction, but on which level should we operate to determine contamination effects? To date, there is no method to adjudge the perfect level of abstraction to work on, and so there is none to determine the abstraction level to pin down contamination.

Linked to these thoughts, we assume a temporal aspect of relevance and put up for discussion, whether it is contamination or not, if an object is accidently, but incorrectly, deemed to be of relevance, and is inadvertently altered. We would argue to consider this to be contamination at that point, though it will be practically irrelevant. The other way round, an inadvertent alteration of an object initially identified as irrelevant but later considered as relevant is a comparably complex edge case. Here, the discussion revolves around whether the forensic process regarding this object has been initiated or not. This is easier to answer in the physical domain: if it has not been seized and packaged in an evidence bag, it will likely fall under the concept of evidence dynamics. In digital, however, we see the need for future discussions.

5.3. Implications of the improved understanding

Intending to tackle this problem, standardization organizations created tailored regularities in the analogous world: the ISO-standard 18385:2016 (ISO/TC 272, 2016) regulates the requirements for products to collect, store, and analyze DNA evidence; FSR-G-206 (UK Forensic Science Regulator Guidance, 2016) published by the British government provides guidance on how to control and avoid contamination in scene examination involving DNA evidence recovery. Still, regarding digital evidence, there exist only general guidelines (e.g., ISO/IEC JTC 1/SC 27, 2012). However, given its increasing importance, it seems imperative to improve awareness and procedures in this subdiscipline.

We can infer several learnings from the examples presented in Section 4. Though, we refrain from trying to derive any specific guidelines since those would be either too specific (e.g., "check when the `systemd-tmpfiles` timer triggers next") or would be far too broad and general (e.g., "improve the education of the examiners and limit direct interaction with the system under investigation"). A general consequence is that any inadvertent changes to objects of relevance have to be avoided, and, if this is—for whatever reason—not possible, the alterations have to be detected and labeled as such to enable a correct interpretation given that knowledge. Overall, this boils down to having intent for any alteration—including its side effects. Purposeful alterations, however, inevitably require a solid understanding of the system, the action, and its implications.

Easing this task requires SOPs that are peer-reviewed. There is not only a requirement for evaluating the correctness of the results but for reviewing the potential contamination effects. SOPs derived from there will profit in soundness, while the provided definition is also helpful to evaluate non-SOPs.

Regarding traditional crime scene work, a lack of research in quality assurance and a unified understanding of quality as such has yet to be sought (Chowdhury, 2021). In the digital domain, this observation can be considered equally delicate. In digital forensics, we can already resort to cryptographic hash functions to ensure data integrity and similarity hashing, e.g., by employing a piecewise approach (Breitinger and Baier, 2012), for determining the resemblance of data. Nevertheless, there is a strong need to develop methods and metrics for measuring acquisition quality and the intrusiveness of analysis tools and techniques (Hargreaves, 2009). Here, we need both simple metrics and a contextualized focus on the semantics of evidence.

In that regard, we want to highlight two points: First, it is essential to conduct rigorous experiments to collect leftover artifacts and quantify the impact of certain system interactions and forensic tools, which is a necessary prerequisite even to be able to have intent. Second, we would like to initiate the strive for precise documentation of contamination in live scenarios and lab environments, as some of our examples already did. An according

knowledge base can help to rule out misinterpretations and identify fields to improve evidence acquisition, handling, and analysis. Based on such findings, the digital forensics research community should strive to develop methods for identifying digital contamination and propose targeted countermeasures to minimize it, much like it has already happened concerning DNA evidence in classical forensic science.

6. Summary

Acquisition and analysis of digital traces constitute a vital part of almost every investigation nowadays. Availability, completeness, and reliability of digital evidence are often crucial to solve cases. In the present paper, we propose a definition of evidence contamination that not only covers physical evidence but also extends to digital evidence. To recapitulate, the proposed notion of contamination is characterized by

1. a transfer of traits to
2. an object of relevance
3. at any point in the forensic process
4. without intent.

We present several examples of partly severe contamination effects in digital forensics to shed further light on it. Those illustrate how easily digital evidence might be contaminated, resulting from a more or less convoluted trait transfer. Even if contamination does not imply wrong conclusions regarding the guilt or innocence of an individual, contamination in the sense of our harmonized definition might cause serious misinterpretation errors and, therefore, severely hamper the reconstruction of the deed (or incident).

In contrast to traditional contamination definitions, we identify that the wealth of autonomous processes, the spatial detachment of cause and effect, as well as the complexity and quantity problems related to digital crime scenes seem to favor this phenomenon in the cyber domain. Moreover, those features lead to several intricacies revolving around the many abstraction layers when dealing with digital evidence, making digital contamination, in some respects, much more complex and partly ambiguous compared to its physical counterpart.

To conclude, there is a real possibility that examiners contaminate digital evidence during their analyses. Hence, it is necessary to raise awareness of that phenomenon in the community of practitioners. Furthermore, researchers should strive to measure and document contamination, evaluate procedures to minimize the risk, work on detection capabilities, and, therefore, aid in preserving evidence of the best possible quality.

CRediT authorship contribution statement

Jan Gruber: Conceptualization, Methodology, Investigation, Writing - Original draft, Writing - Review & Editing, Visualization. **Christopher J. Hargreaves:** Conceptualization, Methodology, Supervision, Writing - Review & Editing. **Felix C. Freiling:** Conceptualization, Funding Acquisition, Methodology, Supervision, Writing - Review & Editing.

Acknowledgements

The authors thank Elisa Schwarz for the fruitful discussions in the course of her master's thesis. Work has been supported by DFG (German Research Foundation) as part of the Research and Training Group 2475 “Cybercrime and Forensic Computing” (grant number 393541319/GRK2475/1-2019).

References

Adelstein, F., 2006. Live forensics: diagnosing your system without killing it first. Commun. ACM 49, 63–66. https://doi.org/10.1145/1113034.1113070.
Breitinger, F., Baier, H., 2012. A fuzzy hashing approach based on random sequences and hamming distance. In: 7th Annual Conference on Digital Forensics, Security and Law (ADFSL), pp. 89–101. http://tubiblio.ulb.tu-darmstadt.de/102073/.
Caithness, A., 2012. The forensic implications of SQLite's write ahead log. Technical Report. CCL Solutions Group. https://web.archive.org/web/20220922074815/https://digitalinvestigation.wordpress.com/2012/05/04/the-forensic-implications-of-sqlites-write-ahead-log/.
Carrier, B.D., 2003. Defining digital forensic examination and analysis tool using abstraction layers. Int. J. Digit. Evid. 1.
Case, A., Richard III, G.G., 2017. Memory forensics: the path forward. Digit. Invest. 20, 23–33. https://doi.org/10.1016/j.diin.2016.12.004.
Casey, E., 2013. Triage in digital forensics. Digit. Invest. 10, 85–86. https://doi.org/10.1016/j.diin.2013.08.001.
Chisum, W.J., Turvey, B.E., 2000. Evidence dynamics: locard's exchange principle & crime reconstruction. J. Behav. Prof. 1, 1–15.
Chisum, W.J., Turvey, B.E., 2011. In: Crime Reconstruction, 2nd ed. Academic Press, San Diego, CA.
Chowdhury, M., 2021. A broken system? Examining the perilous state of quality assurance in crime scene practice. Sci. Justice 61, 564–572. https://doi.org/10.1016/j.scijus.2021.07.001.
Debian, 2022. Manual systemd-tmpfiles. Debian. https://dyn.manpages.debian.org/testing/systemd/systemd-tmpfiles.8.en.html.
Delport, W., Olivier, M.S., 2012. Isolating instances in cloud forensics. In: Peterson, G.L., Shenoi, S. (Eds.), Advances in Digital Forensics VIII - 8th IFIP WG 11.9 International Conference on Digital Forensics, Pretoria, South Africa, January 3-5, 2012, Revised Selected Papers. Springer, pp. 187–200. https://doi.org/10.1007/978-3-642-33962-2_13.
DSTL, 2020. Hue, Smartwatches and Nintendo Switch. Technical Report Digital Forensics Bulletin. 13th ed. DIIS: DSTL/PUB125049. Defence Science and Technology Laboratory. https://web.archive.org/web/20230119073315/https://us5.campaign-archive.com/?u=a5a2a1131e612711f02b96e2c&id=34cb5884cb.
Farina, J., Scanlon, M., Kechadi, M.T., 2014. Bittorrent sync: first impressions and digital forensic implications. Digit. Invest. 11, S77–S86. https://doi.org/10.1016/j.diin.2014.03.010.
Faust, F., Thierry, A., Müller, T., Freiling, F.C., 2021. Selective imaging of file system data on live systems. Digit. Invest. 36 (Supplement), 301115. https://doi.org/10.1016/j.fsidi.2021.301115.
Finke, J., Sessink, O., 2001. Thumbnail managing standard. Technical Report. freedesktop.org. https://specifications.freedesktop.org/thumbnail-spec/thumbnail-spec-latest.html.
Fonneløp, A.E., Johannessen, H., Egeland, T., Gill, P., 2016. Contamination during criminal investigation: detecting police contamination and secondary DNA transfer from evidence bags. Forensic Sci. Int.: Genetics 23, 121–129. https://doi.org/10.1016/j.fsigen.2016.04.003.
Fukami, A., Stoykova, R., Geradts, Z.J.M.H., 2021. A new model for forensic data extraction from encrypted mobile devices. Digit. Invest. 38, 301169. https://doi.org/10.1016/j.fsidi.2021.301169.
Gehl, R., Plecas, D., 2017. Introduction to Criminal Investigation: Processes, Practices and Thinking. Justice Institute of British Columbia.
Grübler, J., 2021. 'Kontamination'. In: Wirth, I. (Ed.), Kriminalistik-Lexikon, 5th ed. C.F. Müller GmbH, Heidelberg, pp. 362–363.
Gupta, M.R., Hoeschele, M.D., Rogers, M.K., 2006. Hidden disk areas: HPA and DCO. Int. J. Digit. Evid. 5.
Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W., 2009. Lest we remember: cold-boot attacks on encryption keys. Commun. ACM 52, 91–98. https://doi.org/10.1145/1506409.1506429.
Hargreaves, C.J., 2009. Assessing the Reliability of Digital Evidence from Live Investigations Involving Encryption. Ph.D. thesis. Cranfield University, UK.
Hargreaves, C.J., Chivers, H., 2008. Recovery of encryption keys from memory using a linear scan. In: Proceedings of the Third International Conference on Availability, Reliability and Security, ARES 2008, March 4-7, 2008, Technical University of Catalonia. IEEE Computer Society, Barcelona , Spain, pp. 1369–1376. https://doi.org/10.1109/ARES.2008.109.
Harris, R., 2006. Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem. Digit. Invest. 3, 44–49. https://doi.org/10.1016/j.diin.2006.06.005.
Huebner, E., Bem, D., Henskens, F.A., Wallis, M., 2007. Persistent systems techniques in forensic acquisition of memory. Digit. Invest. 4, 129–137. https://doi.org/10.1016/j.diin.2008.02.001.
Inman, K., Rudin, N., 2000. Principles and Practice of Criminalistics: The Profession of Forensic Science. CRC Press.
Inman, K., Rudin, N., 2002. The origin of evidence. Forensic Sci. Int. 126, 11–16. https://doi.org/10.1016/S0379-0738(02)00031-2.
ISO/IEC JTC 1/SC 27, 2012. Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Standard. International Organization for Standardization, Geneva, CH.
ISO/TC 272, 2016. Minimizing the Risk of Human DNA Contamination in Products Used to Collect, Store and Analyze Biological Material for Forensic Purposes – Requirements. Standard. International Organization for Standardization,

Geneva, CH.
ISO/TC 272, 2018. Forensic Sciences – Part 1: Terms and Definitions. Standard. International Organization for Standardization, Geneva, CH.
Katalov, V., 2019. iOS Device Acquisition with Checkra1n Jailbreak. https://web.archive.org/web/20220914142952/https://blog.elcomsoft.com/2019/11/ios-device-acquisition-with-checkra1n-jailbreak/.
Lee, H.C., Palmbach, T., Miller, M.T., 2001. Henry Lee's Crime Scene Handbook. Academic Press.
Lim, N., Khoo, A., 2009. Forensics of computers and handheld devices: identical or fraternal twins? Commun. ACM 52, 132–135. https://doi.org/10.1145/1516046.1516080.
Liu, Y., Xu, M., Xu, J., Zheng, N., Lin, X., 2016. Sqlite forensic analysis based on WAL. In: Deng, R.H., Weng, J., Ren, K., Yegneswaran, V. (Eds.), Security and Privacy in Communication Networks - 12th International Conference, SecureComm 2016, Guangzhou, China, October 10-12, 2016, Proceedings. Springer, pp. 557–574. https://doi.org/10.1007/978-3-319-59608-2_31.
Lyle, J.R., 2006. A strategy for testing hardware write block devices. Digit. Invest. 3, 3–9. https://doi.org/10.1016/j.diin.2006.06.001.
Margiotta, G., Tasselli, G., Tommolini, F., Lancia, M., Massetti, S., Carnevali, E., 2015. Risk of DNA transfer by gloves in forensic casework. Forensic Sci. Int.: Genet. Suppl. Series 5, e527–e529. https://doi.org/10.1016/j.fsigss.2015.09.208.
Marlinspike, M., 2021. Exploiting Vulnerabilities in Cellebrite UFED and Physical Analyzer from an App's Perspective. https://web.archive.org/web/20220909054459/https://signal.org/blog/cellebrite-vulnerabilities/.
Meakin, G., Jamieson, A., 2013. DNA transfer: review and implications for casework. Forensic Sci. Int.: Genetics 7, 434–443. https://doi.org/10.1016/j.fsigen.2013.03.013.
Morris, S., 2012. Rape accused was victim of forensics error, regulator finds. The Guardian. https://www.theguardian.com/world/2017/mar/12/netherlands-will-pay-the-price-for-blocking-turkish-visit-erdogan.
van Oorschot, R.A.H., Treadwell, S., Beaurepaire, J., Holding, N.L., Mitchell, R.J., 2005. Beware of the possibility of fingerprinting techniques transferring DNA. J. Forensic Sci. 50, 1417–1422.
Pagani, F., Fedorov, O., Balzarotti, D., 2019. Introducing the temporal dimension to memory forensics. ACM Trans. Priv. Secur. 22, 9:1–9:21. https://doi.org/10.1145/3310355.
Pickrahn, I., Kreindl, G., Müller, E., Dunkelmann, B., Zahrer, W., Cemper-Kiesslich, J., Neuhuber, F., 2015. Contamination when collecting trace evidence—an issue more relevant than ever? Forensic Sci. Int.: Genet. Suppl. Series 5, e603–e604. https://doi.org/10.1016/j.fsigss.2015.09.238.
Pickrahn, I., Kreindl, G., Müller, E., Dunkelmann, B., Zahrer, W., Cemper-Kiesslich, J., Neuhuber, F., 2017. Contamination incidents in the pre-analytical phase of forensic DNA analysis in Austria—statistics of 17 years. Forensic Sci. Int.: Genetics 31, 12–18. https://doi.org/10.1016/j.fsigen.2017.07.012.
Poy, A., van Oorschot, R., 2006. Beware; gloves and equipment used during the examination of exhibits are potential vectors for transfer of DNA-containing material. Int. Congr. 1288, 556–558. https://doi.org/10.1016/j.ics.2005.09.126.
Schwendener, G., Moret, S., Cavanagh-Steer, K., Roux, C., 2016. Can "contamination" occur in body bags? The example of background fibres in body bags used in Australia. Forensic Sci. Int. 266, 517–526. https://doi.org/10.1016/j.forsciint.2016.07.012.
UK Forensic Science Regulator Guidance, 2016. The control and avoidance of contamination in scene examination involving DNA evidence recovery. Standard. The Forensic Science Regulator. Birmingham, UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/915221/FSR_G-206_Issue_2_Final.pdf.
Vömel, S., Freiling, F.C., 2012. Correctness, atomicity, and integrity: defining criteria for forensically-sound memory acquisition. Digit. Invest. 9, 125–137. https://doi.org/10.1016/j.diin.2012.04.005.
Williams, J., 2012. ACPO Good Practice Guide for Digital Evidence.