Forensic Science International: Digital Investigation 51 (2024) 301841

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

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

Uncertainty and error in location traces

Cléo Berger *, Benoît Meylan, Thomas R. Souvignet

University of Lausanne, School of Criminal Justice, Batochime, 1015 Lausanne, Switzerland

ARTICLE INFO

Keywords:
Location traces
Positioning
Error
Uncertainty
Forensic science
Digital investigation
Digital traces

ABSTRACT

Location traces are highly informative because of their potential to infer physical activity or presence. Their prevalence has increased largely due to the rise of digital devices, their encompassed location-based services and other positioning technologies (Raubal et al., 2004). However, there is little research that explores and supports their exploitation, which hampers the confidence that can be placed in it. Location traces are indeed subject to uncertainty and errors, notably in their production and exploitation processes. This article aims to shed some light on the uncertainty and errors associated with smartphone location traces and calls for research to be developed on that topic. Several empirical examples are developed throughout the article to better illustrate these issues.

1. Introduction

The Sydney Declaration recently established seven fundamental principles to strengthen the core of the forensic field and better articulate its object of study, its method, and its objectives (Roux et al., 2022). Such contributions arose after strong criticism of forensic science emerged throughout the 21st century, notably in the UK with the Forensic Science Regulator Act in 2021 (Samuels, 2022). Guidelines for sounder forensic science, including digital forensic science, require assessment of scientific validity.

In light of the growing digitisation and enhanced traceability of human activities, investigations recurrently have to deal with digital devices and media (Casey et al., 2018; Ribaux, 2023). Consequently, digital traces are more often than not part of forensic operations conducted to assist the administration of justice. The considerable volume and diversity of digital traces create significant backlogs and require substantial resources, while their exploitation often yields considerable amounts of information that can be used to reconstruct events. In addition, the fact that there is a large number of digital traces in relation to a particular activity or event does not mean that they are representative of it. Therefore, quality assessment of digital traces becomes necessary (ENFSI, 2015; Forensic Science Regulator, 2023; Pollitt et al., 2018; SWGDE, 2021), which is a challenge in an ever changing environment (Ribaux, 2023).

Among digital traces, spatial location traces offer the potential to reflect on actions or presences in the physical world. They offer the opportunity to address spatial inquiries faced in investigations, and are a typical example of this extended traceability and the problems that it poses for forensic scientists.

This work aims at unravelling uncertainty and errors that arise when using location traces, to guide further work and considerations on their exploitation. Firstly, it reviews the definitions and sources of uncertainty and errors in forensic science in Section 2 before presenting location traces in Section 3. Section 4 presents an investigation methodology derived from Ribaux (2023). Section 5 develops the errors found in location traces, following the presented investigation methodology, with illustrative examples and suggestions for mitigation. Section 6 discusses challenges, further work, and limitations pertaining to location errors. The conclusions of this work are presented in Section 7.

2. Uncertainty and error in forensic science

The concepts of uncertainty and error are frequently used in the discussion of evidence reliability. However, neither term appears to have a consensual definition and they are often confused. The relationship between uncertainty and error is ambiguously brought up, as uncertainty in traces or techniques leaves room for errors to occur, but the risk of errors (e.g., in interpretation) is never zero, which generates uncertainty regarding reliability. Both are ubiquitous and must be managed with adequate resources. (Georgiou et al., 2023)

Uncertainty refers to 'a state of partial lack of information' (Ryser, 2024, p. 63) that an observer has of any situation, which implies its subjectivity (Georgiou et al., 2023). Forensic scientists are not exempt from uncertainty and must therefore account for its ever-present exis-

* Corresponding author.
E-mail addresses: cleo.berger@unil.ch (C. Berger), benoit.meylan@unil.ch (B. Meylan), thomas.souvignet@unil.ch (T.R. Souvignet).

https://doi.org/10.1016/j.fsidi.2024.301841
Received 1 July 2024; Accepted 5 October 2024
Available online 16 October 2024

tence, as well as communicate it throughout investigative and evaluative processes (Casey, 2020). Subjective probabilities, specifically Bayesian approaches, provide strong frameworks to estimate uncertainty (Vuille and Taroni, 2021). This can often prove difficult to carry out, as quantification may not be adequate for all sources of uncertainty (Georgiou et al., 2023). The process of dealing with uncertainty entails the assessment of the confidence placed in a given observation, which must encompass the limitations of our knowledge with regard to all phenomena that impact the trace (Ryser, 2024). Indeed, uncertainty impacts 'the type, quantity, and quality of knowledge available' (Ryser, 2024, p. 63).

As for errors, there is a great variability of its definitions in forensic science (Georgiou et al., 2023; Horsman, 2024; Murrie et al., 2019). Definitions alternatively relate to the causes that provoke such errors, to the consequences that they have, or to their systematic nature (Martire et al., 2024; Ryser, 2024). Among the various definitions, Horsman (2024) asserts that an error is made when an incorrect result or behaviour is reached or obtained unintentionally, due to a 'lack of knowledge' or skill (Nassaji, 2018, p. 1). To characterise an error implies knowing the correct or expected output and being able to differentiate it from the incorrect one (Horsman, 2024).

2.1. Nature and causes of errors

Errors in forensic science may arise due to various causes (Christensen et al., 2014). Common sources of error include human error, tool error and methodological error (Dror and Charlton, 2006; Rudin and Inman, 2005). These can sometimes overlap, leading to fundamental questions about our practices (Dror and Charlton, 2006; Rudin and Inman, 2005). The nature of an error is often a valuable piece of information too, as it allows to understand the materialisation of errors and to introduce adequate countermeasures. In this regard, systematic and random errors are generally opposed, as the former results from recurrent issues, while the latter proves unpredictable and varies in nature. Systematic errors skew results' interpretation because they produce incorrect outputs consistently, and therefore give a systematically misconstrued view of a situation.

In digital forensic science, tool errors are particularly important. Indeed, the processing and analysis of digital traces rely heavily on the use of tools. These tools process raw digital data in a succession of steps, referred to as 'abstraction layers', which help to make them understandable to humans (Carrier, 2003). Typically, these abstraction layers transfer an input into an output through a fixed set of rules (Carrier, 2003). These operations are associated with a margin of error, as any of these layers contains the risk of producing an incorrect output (Carrier, 2003; Lyle, 2010). Tool errors seem to be, for the most part, systematic rather than random (Arshad et al., 2018; Lyle, 2010; SWGDE, 2018).

On top of that, these errors can then propagate and accumulate through other layers or may fail to produce a comprehensible result (Hargreaves et al., 2024). To list a few possible errors, a tool may fail to find relevant information, to extract it properly, or to display it appropriately (Hargreaves et al., 2024). Essentially, tools introduce some complexity that is hard to manage in a quality control setting, on top of the proprietary content that some tools may rely on, that complicates the validation of results. This highlights the wide array of plausible errors and the difficulty to assess a tool's reliability. Tools should be designed to meet reliability criteria, including the provision for usable, comprehensive, accurate, deterministic and verifiable results (Carrier, 2003). In practice, these requirements are seldom met.

Digital investigations are not, however, exempt of human and methodological errors. On one hand, practitioners may make errors due to a lack of skills or knowledge, to their negligence, or to their failure to comply with established guidelines. For instance, practitioners can misuse tools, which can result in the production of an incorrect output (Horsman, 2019; Lyle, 2010). On the other hand, methodological errors are due to structural limitations that impede the practitioner's ability to fulfil their duties correctly, by following methods or principles that fail to yield the anticipated outcome. Methodological errors are nonetheless due to procedures put in place by humans. Both types of errors can overlap or be difficult to discriminate (Dror and Charlton, 2006; Rudin and Inman, 2005). One could argue that tool errors also result, at least in part, from human errors if their implementation is flawed. These errors may stem from difficulties in dealing with the changes in scale that come with digital traces (Ribaux, 2023). In particular, their diversity and volume pose new challenges and significantly increase the number of considerations to adopt in this complex environment.

2.2. Role and estimation of errors

Errors cannot be completely avoided, even with the implementation of safeguards (Eldridge et al., 2022; Horsman, 2024; Martire et al., 2024; Murrie et al., 2019). Refusal to acknowledge their existence can further the damage they create, by perpetuating harmful practices and limiting the scope of new field developments, for fear of introducing new errors (Horsman, 2024; Martire et al., 2024). Indeed, error examination offers the potential to improve (Budowle et al., 2009; Martire et al., 2024) and to strengthen the reliability of practices, especially in a favourable learning environment (Eldridge et al., 2022). However, this potential has long been ignored, as the occurrence of errors was strongly refuted.

In current times, error rates are often required in procedural guidelines in addition to the results obtained through measurements, operations of tools or methods. However, they are difficult to compute for digital traces. Indeed, depending on the type of error considered, error rates might vary. Consequently, without a clear definition or consensus on the types of error in question, they cannot be purposefully discussed (Martire et al., 2024). Moreover, calculating error rates is easier said than done, as it can be challenging to estimate an error rate that accurately reflects the actual risk of error, in a specific situation; it may not contribute significantly to assessing the reliability of the evidence (Budowle et al., 2009). It is also difficult to keep up with the latest technological developments in order to adapt quality control processes (Casey, 2019, No. 6). A combination of error rates to provide an overall estimation of errors does not necessarily make sense either (Lyle, 2010). Ultimately, even if error rates could be calculated, the question remains as to what constitutes an acceptable error rate, which is far from being an easy task (Dror, 2020b). Some authors suggest that the error in itself is not the only thing important, but rather, the way it is dealt with (Budowle et al., 2009). Budowle et al. (2009) therefore argue that the concept of error should be conveyed qualitatively: its causes, its consequences and how to mitigate it.

3. Location traces

Spatial location traces (hereafter: location traces) are reflective of a position in the real world (Casey et al., 2020). They are found predominantly in digital devices, in particular smartphones. This abundance of location traces results from the increased traceability these devices allow (Casey, 2019, No. 6). Indeed, such traces often result from the use of location-based services. They act as a link between the spatial location of a smartphone and its surrounding environment, encompassing the activities and services available in the area (Raubal et al., 2004). The expansion of location-based services can be attributed to the progress of wireless communications on the one hand, and of geolocation technologies on the other (Raubal et al., 2004). Smartphones materialise the ability to assist users in their everyday tasks, including navigation, finding relevant places or accessing area-based content (online meeting platforms, streaming services, etc.). The location of a device becomes yet another component that can be exploited in the digital world (Spichiger, 2022b). The ability to obtain a relatively accurate position simplifies the user experience, who does not have to report it themselves for these services to operate.

Hence, location traces can be categorised into two distinct groups: those resulting from positioning technologies (i.e., geolocation technologies), the aim of which is to provide a location, and those that inform on a location, despite not being designed with this purpose in mind (e.g., the content of a picture, text messages suggesting a meeting point, etc.). Spichiger (2022b, pp. 24-26) defines the former as a 'localisation' (p. 24) and the latter as a 'location-based feature' (p. 26). Locations can be obtained using a variety of positioning technologies, primarily Global Navigation Satellite System (GNSS), cellular network infrastructures and WiFi access points, but additional means also include Bluetooth Low-Energy or other embedded sensors (Casey et al., 2020; Maghdid et al., 2016; Ralf et al., 2004). While smartphones often rely on a combination of these to determine their location (Maghdid et al., 2016), the information available can vary depending on, among other things, the environment, the smartphone's settings or the parameters of the application requesting the location.

Location traces (in the broad sense) have the potential to provide information about the whereabouts of the person who was in possession of the digital device at a given time, which may be an essential piece of information to solve a case. More broadly, they allow to identify places of interest, reconstruct journeys, detect meeting points and identify relevant relationships and entities (Rossy, 2024). The informative value of these traces is enormous and might provide leads in an investigation or be evaluated as evidence in a court of law. Other typical contributions include linking cases between them (Rossy, 2011), inferring upon recurrent crime structures and patterns, or the litigation of security and civil issues (Ribaux, 2023; Roux et al., 2022). For example, spatio-temporal analysis is an essential component in the detection of recurrent crime.

Although location traces are routinely used in criminal investigations, little research has been conducted to establish their reliability. The following sections explore the errors that occur when considering them.

4. Investigation methodology

To further develop location traces in smartphones, a general 'investigation methodology' will be proposed below. This guideline will then allow us to present errors and general issues occurring at the different stages in which location traces exist.

During their life cycle, digital traces progress through various stages, from their creation and storage to their potential analysis or exploitation. A model presented by Ribaux (2023, p. 204) outlines these stages and describes a general investigation methodology, divided into three distinct phases, representing the transitions between them:

- Trace production
- Trace investigation
- Reconstruction

To ensure optimal results, each phase should be grounded in a comprehensive understanding of the mechanisms and methods employed in the preceding stages. This section aims to explore this model through the lens of location traces to visualise how errors at each step could affect the conclusion.

4.1. Trace production

The model starts with the generation of a trace, which Jaquet-Chiffelle and Casey (2021) defines as 'the perceptible results of an event of interest'. In the scope of this article, the event of interest would reference a presence. In this context, the mere presence of a device can lead to the generation of several traces that are stored either on the device itself or elsewhere. It is essential to understand the process of trace generation (1) to grasp what it reveals about specific activities. This step corresponds to more than just a technical event, as it involves how the device acquires its current location, how this data is processed, and finally, how and where it is stored. Finally, during the time elapsed between the trace creation and its detection or extraction, extrinsic or intrinsic events could also alter the details it contains (Jaquet-Chiffelle and Casey, 2021). This temporal interval can be characterised by the persistence of the trace (2).

Numerous questions can arise at each step of the process, such as whether the information is up-to-date, how accurate it is, and whether its accuracy is stored alongside the trace or ignored. Understanding these mechanisms, in particular, how position information and associated metadata are handled, is crucial to the whole methodology. Indeed, as it will be shown in later sections of this article, interpretation errors can result from a lack of knowledge of these elements.

4.2. Trace investigation

During the second phase of the general methodology, which is called the investigation phase, the (digital) trace, will undergo various steps, mostly based on tools and human observations. The aim is to extract information from the traces.

These steps share common characteristics, which are to limit the degradation of the trace and to ensure the integrity of the data along the way. This part describes how to go from a trace, stored on a device or elsewhere, to information that is deemed relevant and can be used to construct hypotheses.

The first step in this phase involves identifying and collecting devices of interest. Although this step will not be discussed in detail in this paper, which focuses on potential errors in location traces, it remains a critical aspect of the investigation phase, which can obviously lead to numerous problems. In the same vein, the way in which a trace is judged to be relevant or not will not be discussed here. The errors that can arise from these choices are mostly random errors, but there could also be cases where the errors are systematic. This is particularly the case when the decision on relevance is made by a tool or is determined by methodological guidelines, or when there is a lack of knowledge about the device's functionality to guide the choice of seizure, for example with IoT (Servida et al., 2023). Some types of devices may be systematically ignored, even though they may contain location traces.

Once the equipment is seized, the location traces it contains are stored in its storage media (e.g. eMMc chip, MicroSD card), and need to be extracted (3) in order to be exploited. It should be noted that traces could also be stored remotely, but the issues raised are identical. Once the device is acquired, the trace must be detected. This could be done by applying some processing or examination steps, like parsing the data, structuring the information in a data model and presenting it in a way that is readable by analysts or investigators. This phase can be iterative and performed in many different ways, which may produce different results. In most cases, the acquisition, parsing, structuring and presentation rely heavily on tools, some of which are open source, but most of which operate as black boxes (Hargreaves et al., 2024). The main risk of this approach is a lack of understanding of the mechanisms at work, such as whether the acquisition is an exact copy of the device memory, what data model the tools are using, what abstraction layers or choices the tool is making, whether it is appropriate for the type of data at hand and whether it suits the investigator's needs.

4.3. Reconstruction

The final part of this general investigation methodology is the reconstruction of the initial event, again in this context, the presence of the device at a given location. This step focuses on hypothesis and reasoning. It can be seen as the analysis or examination of one or more traces (4). The aim is to explain the existence of the trace(s) by elaborating and testing hypotheses in order to answer given questions (5). This process, described by Ribaux (2023, p. 224) as the hypothetico-deductive process, is highly recursive. In the end, one or more hypotheses could be more likely to explain the traces collected.

The traces available at this stage can and should be used in combination. It strengthens the evaluation that could be made of the hypotheses and enables the investigator or analyst to keep an overview. The traces could come from different devices or be processed by different tools, which could help detect inconsistencies.

5. Errors related to location traces in smartphones

This section outlines the unintentional errors that can be encountered when working with location traces from smartphones (or similarly, from other digital devices). Indeed, errors could be made at any stage of the trace generation, investigation and event reconstruction processes. These stages have been identified in the previous section:

1. Trace generation
2. Trace persistence
3. Trace detection and extraction
4. Trace examination and display
5. Trace interpretation and event reconstruction

Errors will be discussed for each of these successive stages, in order to identify their specific issues. Most of these errors have technical, human or methodological causes. Casey (2019, No. 6) stresses that such errors are recurrent in digital forensic science.

The typology presented is not exhaustive and does not purport to describe all possible errors. Its purpose is to identify categories of potential errors and to demonstrate that there is still much to be acknowledged in order to integrate location traces into the forensic analysis of digital devices. This provides insight into issues surrounding location traces and raises awareness of the need to take precautions in this regard.

5.1. Trace generation

Trace generation is an essential aspect to consider. Understanding the mechanisms by which the trace is produced allows hypotheses to be developed in subsequent steps about the activity that generated it. However, several issues may hinder the outcome of a subsequent analysis.

First of all, uncertainty about the trace generation may amount to errors later in the process. In the case of location traces, several positioning methods may be involved in their production. In general, an accuracy value should be associated (explicitly or implicitly) with such a trace, which - in theory - represents the uncertainty associated with the position obtained. On average, the accuracy of each positioning method is different (therefore resulting in different reliability), and also depends on the context. This is a consequence of their differentiated resolution power and the measures used to obtain a position.

The positioning method(s) that produced a location trace are not systematically stored in the device. Consequently, the interpretation of a trace would be hindered or erroneous at a later stage, given that the positioning method conditions the accuracy of a trace and what it reflects about an activity. This introduces uncertainty into what can be inferred from a location trace. A GNSS-derived location would, on average, position a smartphone within a few meters of its actual location. In contrast, a cell connection may only allow the identification of an area in which the smartphone is located (Merry and Bettinger, 2019; Ralf et al., 2004; Zandbergen, 2009). Hence, uncertainty about the positioning method that produced a location trace is problematic.

In addition, some positioning methods operate as black boxes. WiFi and cellular network location traces originate from information contained in crowd-sourced databases (Spichiger, 2022b), maintained by location services such as Apple or Google. Not only can they contain significant errors, but the location information is directionally biased (Merry and Bettinger, 2019), potentially by the locations from which the majority of users access these services (Spichiger, 2022b).
In the case of cellular network-derived locations, the smartphone connection also follows complex rules that are highly dependent on the situation and environment. A common misconception is that it relies on the closest cell tower, or the one with the strongest signal nearby (Ogulenko et al., 2022).
As a result, the reliability of traces derived from such methods is difficult to establish without knowledge of the underlying management. This may affect the information that can be reconstructed from a trace. Alternatively, the accuracy itself may not be registered in the device, even if assessed (e.g., for cellular network-related traces), which is the case in most situations.
Finally, the context in which the location was obtained may be lost, which is a significant aspect to consider in order to establish meaning. A location trace can represent different information: a position, a search linked to a place in a navigation application, etc. If this is not specified, the scope of the analysis could be reduced. Losing information about the conditions under which the trace was created, assessing the uncertainty inherent to the trace and proposing meaningful reconstructions is challenging.

On top of these uncertainties, actual errors can occur at this point. Firstly, the location trace could result from an incorrect positioning. They sometimes produce aberrant values, outside of the expected accuracy. They mainly rely on radio signal propagation, which is subject to interference, obstructions, reflections in the environment, and so on. These propagation methods are not secure against loss and do not guarantee the efficiency of signal transmission (Hoy, 2015, p. 20). Systematic errors therefore occur due to these effects on signal propagation (Spichiger, 2022b). The possibility of this type of error is tedious to characterise because it requires complex modelling of an environment, with very specific settings.
Secondly, although less common, the location information may also be incorrectly stored on the device, i.e. the trace may not correspond to the position obtained. This has more to do with information management and storage than with positioning methods. These errors do occur, but it is very difficult to assess their frequency without dedicated research.

Uncertainties and errors in the generation of location traces are systematic and primarily due to the technologies used to produce such traces (positioning methods and smartphone specifications). It is recommended that trace generation issues should be addressed through systematic testing in order to develop a sound understanding of smartphone positioning and trace creation. While GNSS-based methods are very well understood, grey areas remain for other or combined methods. Why smartphones rely on either of these methods is also rarely explored in research, and is likely more complex than the mere availability of the best (or most accurate) positioning option. This kind of research is essential if meaningful conclusions are to be drawn from location traces.

On top of that, case-specific testing may be required to evaluate or reconstruct the specific significance of a trace. Research on cell site analysis (Tart et al., 2021, 2012), or other sensors (Van Zandwijk and Boztas, 2021, 2019) has been conducted, but more research remains necessary. Relying on a combination of traces to strengthen conclusions later is also a good way to counter their shortcomings.

An empirical example is as follows. An image with an incorrect associated location is considered. By analysing the Exif data of Fig. 1, the coordinates indicate the port of Ouchy in Lausanne (Switzerland). However, the content of the image clearly corresponds to the port of Evian (France), located on the opposite side of Lake Geneva (about 15 km away).

This discrepancy is due to the fact that the smartphone was in ‘airplane mode’ during the crossing of the lake; at the moment the photo was taken, it associated the last available location information, which was the point just before the network connection was lost. This relatively simple and well-known example illustrates that a positioning error at the time of creation persists through the exploitation process and is still present during the trace interpretation phase.

The issue of buffering the position can also be propagated to the locations of third-party items. Fig. 2 plots an Apple AirTag at Geneva

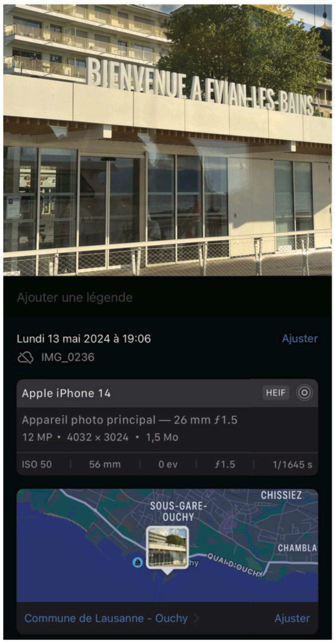

Fig. 1. Picture of Evian (FR) pier internally located at Ouchy (CH) pier - 12 km away

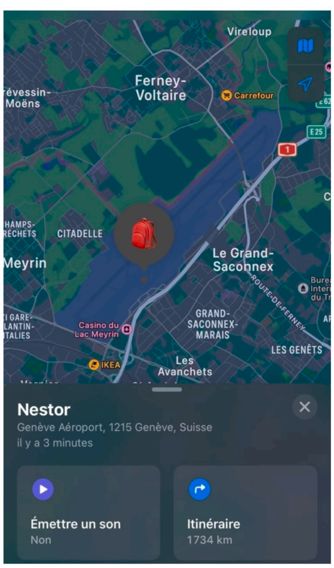

Fig. 2. Apple AirTag located - 3 minutes ago - in Geneva airport (CH) while actually in Athens airport (GR) - 1734 km away

airport (CH) three minutes ago when it was actually at Athens airport (GR) at this time. The discrepancy in distance of 1734 km could be due to the iPhones on the plane accessing cellular networks upon landing and reporting the proximity of the tags (in the aircraft's baggage hold) while still internally positioned in Geneva.

Another typical example of error during the generation of location traces is the relocation of a mobile communication device, such as a WiFi access point. This error arises because mobile devices use several methods for positioning, including cell towers and WiFi. When a smartphone wants to locate itself based on a WiFi network signal, it sends a request to a location service, which then returns a corresponding location. These databases are populated by various devices in the field. However, accounting for changes in the network can take time. For example, when a WiFi access point is moved during a relocation, the API response will still provide the old position until the database entry is updated. Consequently, the location trace stored on the phone will be incorrect. The same problem can occur with cell towers, although it is less common.

5.2. Trace persistence

On top of that, a period of time will likely elapse between the creation of the trace and the consideration of the device in an investigation. The temporal persistence of the trace in digital devices may have an impact on the subsequent reconstruction.

The volatility of digital traces is well-documented. Traces can be lost over time, giving a false impression of completeness if other traces are still abundant, or misrepresenting a situation. For instance, attempts to establish patterns of important places, or travel between points may be affected by the representativeness of remaining location traces, which is not necessarily correlated with their persistence.

These are not errors, so to speak, but rather limitations that must be accounted for in later stages. Traces always offer partial and incomplete perspectives on events and activities (Margot, 2017). While digital traces often result from extended traceability, it would be hazardous to conclude that an important amount of traces implies their representativeness of a situation. The interpretation of the trace, in particular, must take this into account.

Digital practitioners and analysts must remain cautious later on, as the loss of traces is inevitable. The absence of a trace is not the same as a trace of absence; a fundamental tenet to remember when trying to assess a physical presence in a given location.

5.3. Trace detection and extraction

Once an investigation has begun and a device has been seized, the next step is to detect and extract location traces. These are combined here, as they often go hand in hand with the data acquisition and examination processes.

This step will determine whether or not exploitable location traces are obtained. First, location traces need to be detected. Current knowledge of where these traces are found and in what format is essential. Smartphones rely heavily on databases and log files to store relevant information, but this varies between manufacturers, (versions of) operating systems, or over time. Keeping up with the latest developments proves difficult, but necessary to detect relevant traces. In practice, detection and extraction rely heavily on tools that access and retrieve traces from devices. The tools must therefore operate accurately and retrieve all traces without distorting them. However, these tools process the data acquired from the devices. In theory, the acquisition process must be sound and ensure data integrity, to prevent alteration of the forensic image. In reality, when it comes to smartphone acquisition, the completeness and quality of the acquired data are dependent on the device model, the acquisition suite and the user experience. If the tool is poorly implemented or out of date, it may also discard or ignore traces. Depending on the type of data acquisition, it may be possible to recover more or less traces. Consequently, a forensic image may be incomplete (Hargreaves et al., 2024) or contain altered traces. This is an error as it results from an incorrect output and is systematic in nature.

A concrete example is the Apple Unified Logs, which was introduced in all Apple devices in 2016.[1] Unified Logs (officially OSLog[2]) have been known to advanced specialists for almost a decade and it is one of the most valuable traces on Apple devices, yet it still suffers from acquisition and interpretation issues in the tools. In the present era, the

[1] Apple 2016 WWDC https://devstreaming-cdn.apple.com/videos/wwdc/2016/721wh2etddp4ghxhpcg/721/721_unified_logging_and_activity_tracing.pdf (visited on 29.06.2024).

[2] Apple developer's documentation https://developer.apple.com/documentation/oslog (accessed on 29.06.2024).

majority of mainstream forensic tools lack the ability to facilitate the acquisition of the Unified Logs. This is evidenced by the lack of both a logical acquisition mechanism, analogous to the log collect command, and the processing of the related files, such as tracesv3 files, that could be obtained by advanced acquisition techniques. As a result, the general public is unable to access and process these valuable traces.

The literature suggests several mitigations that should be enforced in the use of tools. First, tool capabilities and processes should be transparently disclosed by developers and companies, as should user manuals. This should, at the very least, prevent human errors in the use of tools, if they are properly trained and in adequate environments. While this seems obvious, when working with specific traces, it can be difficult to understand exactly how a trace has been processed by a tool. Moreover, tools should be tested to ensure they produce sound results. Horsman (2019) points out that black-box testing is often the only realistic way to test a software, since the source code is not available. However, there is a lack of standardisation in tool testing procedures (or at least guidelines) and what constitutes adequate test data sets, so testing is often a personal initiative that is poorly specified. However, a tool is only a means to an end and should not be the cornerstone of digital investigations, as this would take the focus away from the real objective: the exploitation of traces. Finally, cross-verification may be an option. Dual-tool verification can be set up (Interpol, 2019), with the disadvantage that it can give a false impression of validity, especially as distinct tools may rely on common libraries or algorithms (Sunde, 2022). Manual analysis and blind validation or peer review offer more robust solutions, although this may once again depend on how knowledgeable the practitioner is. Generally speaking, systematic means should be sought to deal with systematic errors (Arshad et al., 2018), such as those arising from the use of tools. Focusing on methodological aspects to ensure the validity of the approach is more important than simply ensuring that a particular tool behaves as expected.

5.4. Trace examination and display

Again, digital traces, particularly location traces rely heavily on tools to produce information that is comprehensible for humans ((Casey, 2019, No. 6); Hargreaves et al. (2024)). Notably, traces susceptible to be found in large quantities or that are well-suited can be transformed into tables, visualisations or graphs (e.g., displaying coordinates or other spatial information on a map). Digital forensic tools, supporting raw forensic images, may provide built-in visualisation of locations. Yet, these displays encapsulate some transformations or operations on the traces that are not apparent to the user. The tool interprets the trace to convey meaning to the practitioner; a role generally reserved for humans. In order to display a location on a map, a tool must assume that the trace is indeed a location trace and that it corresponds to a particular type of coordinate system. These tools thus offer a false sense of simplicity, by demonstrating ridiculously easy solutions for displaying such traces and concealing the considerations that should be made by practitioners to ensure correct processing and analysis. Their examination is then accessible to non-forensic scientists (such as detectives). In reality, these traces involve a complexity that is difficult to manage, even for trained professionals, due to uncertainties and possibilities for errors mentioned in previous sections. This may therefore lure the user into a false ease of interpretation. This abstraction of data can lead to errors (Casey, 2002; Hargreaves et al., 2024).

These tools often rely on proprietary content as well and their processes may not be disclosed, which also makes it difficult to verify the information displayed.

Hargreaves et al. (2024) mention several examples of errors that could be produced by tools when considering location traces in smartphones. First of all, a tool might not include the accuracy when displaying a physical location on a map, therefore giving a misleading impression of a precise location. It could also incorrectly display a location on a map, or display a location that was not actually visited by the

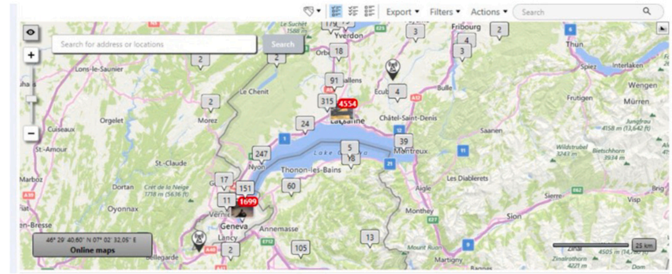

Fig. 3. Default tool visualisation that may lead to misinterpretation

device (but stored for other reasons, as presented in the example below) (Hargreaves et al., 2024).

Specifically, this last example occurs with Snapchat locations. Indeed, the current extraction of Snapchat locations by certain tools produces errors. During the extraction from a smartphone, some location traces appear clearly inconsistent. In fact, one of several examples shows two tracks 72 km apart within an interval of one second. The significant spatio-temporal distance between these two traces makes it impossible for the phone to be in both locations at the given timestamps. The possible low accuracy could be one explanation, but other hypotheses can be put forward, as in some examples, the distance between traces could be hundreds of kilometres. In order to determine whether the error occurs in the observation or in the display of the traces, it is necessary to retrace the processing steps. A direct analysis of the database suggests that the spatial information of both sent and received Snapchat elements is stored in the same place. Thus, the tool in question does not differentiate between a location trace of sent or received content. The smartphone could be in either a reported location or in neither. In this case, it is possible to conclude that the error occurs in the observation and display of traces, where the position of the smartphone is incorrectly inferred. Fortunately, the fact that two positions are relatively far apart in a very short time allows these anomalies to be detected, but in the case of an isolated trace, the error may go unnoticed.

Another example is shown in Fig. 3. The map displays all locations, retrieved from cellular network-related location traces, extracted from a phone during one of our academic exercises. The data corresponds to a few days of activity (e.g. train and car journeys), but there are scattered data points over a distance of about a hundred kilometres. Knowing the actual destinations of the phone (ground truth activity), it became apparent that there was clearly inaccurate or even false data being presented by the tool. Spichiger (2022a) used this example to illustrate the shortcomings of the tool's results and to challenge the EAFS 2022 audience with a number of his hypotheses regarding the potential sources of these anomalous results (including tool decoding errors, weak signal reception, and so forth). None of the experts present were able to provide an explanation for this behaviour, and none of the hypotheses put forward were actually correct.

Going back to the trace, in particular the cache_encryptedB.db database, we noticed that all the out-ranged traces had one thing in common: a Cell-ID (CI field) value of "-1" (Fig. 4). By excluding all elements with the same value, the map became relatively clearer, and the journeys began to delineate more precisely (see Fig. 5). Some of our current research (not yet published) suggests that these large area entries are part of the responses received from Apple's location database. However, assuming the veracity of the displayed traces without further investigation could have serious consequences.

The aforementioned example also demonstrates another source of error that has not been previously identified. These errors are caused by tool approximations. Currently, some tools round trace values, presumably for internal consistency. The Figs. 6 and 7 show how a major digital forensic tool approximates all latitude and longitude values for locations (at least from cache_encryptedB.db) without informing the user.

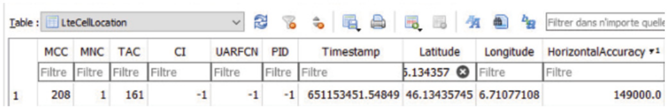

Fig. 4. Entry from LteCellLocation table -cache_encryptedB.db - with a Cell-ID (CI) value of -1

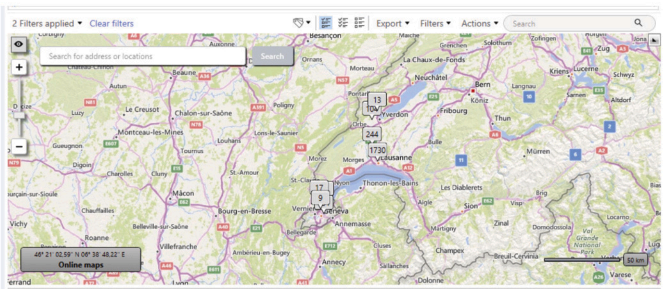

Fig. 5. Display excluding cache_encryptedB.db entries with Cell-ID (CI field) equals to -1

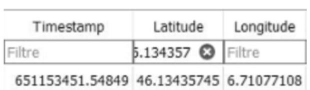

Fig. 6. Latitude and longitude values in cache_encryptedB.db given to 8 decimal places

Fig. 7. Latitude and longitude values displayed on Cellebrite given to 6 decimal places

Other relevant information might also be discarded, to easily communicate a position (i.e., the source of a trace, the context in which it was created, etc.) or to ignore uncertainty about other aspects of the trace. Temporal uncertainty is particularly important when considering digital traces (Casey, 2019, No. 6, p. 6).

Indeed, location traces are almost always associated with temporal information. Thus, errors can also stem from this component (Casey, 2019, No. 6). The temporal trace associated with a location trace is very often a simple timestamp indicating when the device was at that location. In some cases, however, different types of temporal information are associated with a location trace. If the details of these different types of timestamps are present in the device alongside the location trace, it is important that they are preserved during the investigation process. For instance, in the case of travel itineraries, the temporal information may indicate the beginning or end of the itinerary, and thus be associated respectively with the starting position or the destination. This scenario is generally well handled by tools. However, other less trivial examples pose more problems. Indeed, some tools tend to standardise the data as much as possible, often by relying on overly generic data models. An illustrative example is the following situation: location traces place a smartphone at a location 20 kilometres from an incident, twice in the morning and then a third time at 8 PM on the same day (Table 1[3]). As the incident occurred around 8 PM that day, this last trace could be a defence argument saying that the smartphone was too far away from the events for the owner to be involved.

However, by examining the data source, it is possible to see that there are in fact three timestamps associated with the same location information: the first corresponding to the entry into the area, the second to the exit, and the last to the creation or update of the record in the respective database (see Table 2). Therefore, the location trace itself seems legitimate, but the 8 PM timestamp associated with it does not correspond to any time when the smartphone was actually at that location. This whole confusion arises because the specificity of the timestamp is lost during the exploitation process aimed at standardising data models.

Table 1
Location traces as shown *Significant Locations Visits.*

Timestamp	Latitude	Longitude
08:48:16	46.519972	6.572333
09:05:38	46.519972	6.572333
20:12:25	46.519972	6.572333

All of these errors or issues are once again systematic and at least partially caused by tools. Mitigation options for tools are generally the same as those suggested in the previous subsection (trace detection and extraction). However, general methodologies should also be implemented so that practitioners systematically analyse and interpret the trace themselves. Sunde (2022, p. 6) emphasises that reliability should be verified by practitioners. On top of that, methods and procedures could incorporate discrepancy detection in location traces. This could help to assess the overall coherence and combination of traces before considering them individually. This solution still does not cover all possible cases, for example when only one or few location traces are recovered. Case-specific testing may once again be required to assert reliability. A case-based approach is fundamental, and there may not be a single solution that will allow to solve all potential issues. Overall, simply displaying traces without analysing them is problematic.

5.5. *Trace interpretation and event reconstruction*

In order to 'correctly' interpret a trace, one needs general knowledge of all the preceding stages that have played a role in its generation and processing: its production mechanisms and accuracy, its storage in the smartphone, followed by its retrieval and potential processing or transformation. Uncertainties and risks of potential errors associated with such processes and operations should be included in the interpretation. If some of these are ignored, conclusions or hypotheses may be drawn beyond what the nature of the trace would allow, or may simply be incorrect. Questions addressed to the forensic scientist must also match with their capacity to address them. Of course, errors related to reading or understanding the trace cannot be excluded either. Location traces must not only be treated on their own, but it is also important that they are contextually interpreted (Pietro et al., 2019). Experts must then formally conduct source or activity level evaluation, by considering competing hypotheses and assigning probabilities to the observed trace within each of them. The overall evaluation of digital traces is gaining momentum and strength in digital forensic communities. Bayesian approaches have been developed in the last few years to interpret location traces from smartphones, which prove promising (Casey et al., 2020; Spichiger, 2022b, 2023; Vink et al., 2022).

In addition to the importance of understanding previous stages, it is also essential to note that all previous errors or uncertainties could also lead to errors during the interpretation. The information about corresponding uncertainties or their awareness may have been lost; the risk of an error may therefore not be perceived. Errors can also pile up subsequently and produce even more significant discrepancies at this stage. This could have repercussions beyond the work carried out by the forensic scientist. Even if the exploitation of the location trace does not present any error, any subsequent decision could also misinterpret the practitioner's conclusions or be taken out of context (Budowle et al., 2009). The interface between the forensic scientist and the recipient of his or her conclusions can be problematic, as their expectations

[3] Path to the database containing *Significant Location Visits*: /private/var/mobile/Library/Caches/com.apple.routined/Local.sqlite (Table: ZRTLEARNEDLOCATIONOFINTERESTVISITMO).

Table 2
Original record in the database.

Entry Timestamp	Exit Timestamp	Created on Timestamp	Latitude	Longitude	Source
08:48:16	09:05:38	20:12:25	46.519972	6.572333	Significant Location

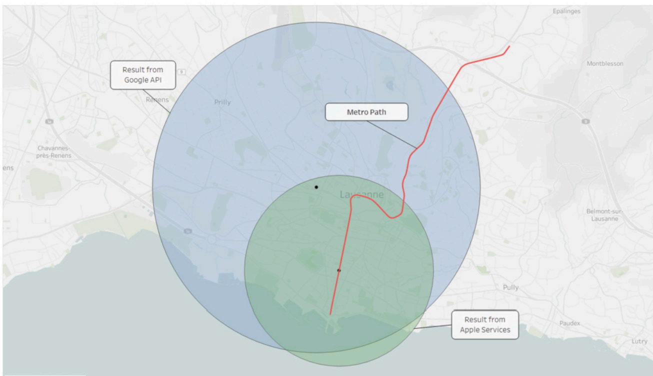

Fig. 8. Metro path (red line) and the locations returned by Google Location API (blue circle) and Apple services (green circle).

or comprehension may differ. Therefore, existing uncertainties should be communicated throughout the forensic scientist's work, so that the recipient or decision maker takes it into account accordingly (Casey, 2020). Experts also need to clearly communicate how their findings should be interpreted by recipients; expectations on both sides need to be discussed and managed; the scope of expertise and capabilities need to be expressed.

Errors in the transition from traces to hypotheses are highly dependent on the person (or tool) performing the task, the parameters they consider, and their knowledge of the context related to the location trace. For example, if the accuracy of the positions is not taken into account in the elaboration and evaluation of hypotheses, the results will certainly be erroneous. To illustrate this problem, consider a connection to a cell tower in a tunnel, where cell towers are regularly deployed along the entire length of the tunnel, and the identifier remains the same throughout. Using the example from one of the metro lines in Lausanne, the location derived from the Cell-ID was obtained using both Google Location API[4] and Apple services. The first thing to notice is that both services return quite different locations, one being relatively near the centre of the metro line, the other near the southern part of the line (see Fig. 8). The accuracy associated with those locations is also different, around 3 kilometres for Google API and 1.5 kilometres for Apple services.

Here, the importance of taking accuracy into account is clear. The hypotheses resulting from the analysis would otherwise contain some errors. Furthermore, it would be even better to take into account the context surrounding the location trace, which implies having a good knowledge of the local area. This could allow more precise hypotheses to be made. In this case, the associated context allows us to hypothesise that the phone is in the metro tunnel, which significantly narrows the zone of uncertainty compared to the previous consideration, which was a circle with a radius of 3 km. This is even more important in the case of CDR,[5] where no accuracy is given, and 3 km is not the typical range of an antenna in an urban area (Cherian and Rudrapatna, 2013), so the hypothesis could be even more erroneous as it would not cover the entire length of the metro.

[4] Google Geolocation API: https://developers.google.com/maps/documentation/geolocation/overview (request made on 28.06.2024).

[5] Call Detail Record.

This example also emphasises the importance of understanding how location services work, as smartphones use them (or very similar systems) to locate themselves. Here, both return different information, despite being given the same input. In this particular case, it is possible that two different cells cover the northern and southern parts respectively. The difference between the two results could also be the source of errors and underlines the value of crossing data sources.

In a study, Sunde (2021, p. 8) found that digital forensic reports overall lacked quality and did not conform to recommended good practices in forensic science, which could lead to 'a high risk of erroneous or misleading results' (p. 8). An alarming rate of reports expressed conclusions at high levels on the hierarchy of issues, ignoring the requirements necessary to formulate them, while the conclusions steered clear of comprehensive certainty descriptors, making it difficult for the recipient to assess the actual value of the results and conclusions given by the practitioners.

In addition, digital forensic scientists are also subject to cognitive bias (Dror, 2020a), which has been shown to have subsequent negative effects on the administration of justice, as it can lead to errors. Digital forensic science is particularly prone to bias, as current practices do not endorse its rigorous mitigation or do not propose reliable overseeing of its processes (Page et al., 2018; Sunde and Dror, 2019). This is particularly true when the process 'involves subjectivity, interpretation or opinion' (Sunde and Dror, 2019, p. 3). The question of what contextual information should be provided to forensic scientists often arises, as it is both necessary for the trace to acquire meaning (Roux et al., 2022) and can introduce bias (Sunde, 2022).

Given the impact of human errors, it is important to identify the effects and sources of bias. Bias can be present throughout the entire process, due to human, organisational or case-related factors (Sunde and Dror, 2019).

Both systematic errors (lack of knowledge and inappropriate methodology, presence of bias) and random errors (punctual errors inherent to human beings) can therefore occur at these stages. Emphasis must be placed on methodology. Strong frameworks and methodologies for digital investigation and trace evaluation must be adopted. To name a few examples, methodologies that encourage empirical testing, that implement and create environments that help mitigate bias, that encourage cross-verification and validation of results (i.e. blind verification) are sought. Another aspect is the development of competing hypotheses and, ideally, the consideration of more than one trace to strengthen conclusions (Casey, 2002).

6. Discussion

6.1. Call for research

Errors in location traces appear to be mainly systematic, which is consistent with the literature on errors in digital forensic science. This is especially true because of the significant reliance on tools to conduct investigations, but also because of the lack of knowledge about location traces and therefore the lack of appropriate methodologies to consider them. Errors can accumulate and propagate at different stages, which also might create even more important issues. This situation is alarming and raises concern for the proper administration of justice.

Indeed, location traces are sometimes ruled inadmissible in US courts, because of the lack of knowledge on which their exploitation relies, or at least their lack of 'general acceptance'. An example is given in Casey (2019, No. 6, p. 652).

We strongly believe that the existence of uncertainties and errors should not paralyse the field, but rather help to guide improvements and the selection of mitigation strategies (Sunde, 2022). Collaboration is particularly important to overcome errors in forensic science and to move towards their effective identification, mitigation and management (Martire et al., 2024). This could potentially be done through monitoring processes that constantly re-evaluate the field and its practices (Budowle et al., 2009; Horsman, 2024). In addition, although errors will occur, they can have a positive outcome during training, if they are detected and corrected (Eldridge et al., 2022). Uncertainty must also be clearly communicated at every stage of the forensic scientist's work (Casey, 2020).

Digital forensic scientists therefore must strengthen their practices in order to conduct sound investigations. Standardisation, sometimes seen as a magical remedy, is often difficult to set up and can distract forensic scientists from their actual goal: reliable exploitation of the trace and the inferences they allow. Instead, going back to the core of the discipline should help to guide meaningful and reliable approaches (Pollitt et al., 2018; Roux et al., 2022). A global approach that combines traces will counter the inherent limitations of a compartmentalised approach.

More specifically, the lack of understanding of location traces and their production mechanisms results in several fundamental limitations that hinder their exploitation. Although they are often combined with other traces or data sources and do not always lead to convictions on their own, the potential they offer to reflect on activities in the physical world suggests their importance in investigations and, possibly, subsequent trials.

There is a clear need for research on location traces, which are perceived as valuable, but have little traction in the academic community. We call for a stronger framework to guide the exploitation of location traces, both in terms of methodology and expectations. In particular:

1. Their production mechanisms and accuracy should be further studied to assess reliability and limit errors,
2. The role that tools should play to support their exploitation,
3. Reasonable conclusions to be drawn from location traces should then be defined to help structure their exploitation,
4. The integration of location traces into larger considerations and investigations.

It is essential that digital practitioners benefit from this research and that they are trained accordingly. This will root future practice in empirically tested results.

Testing will be necessary to better understand the occurrence of errors in trace evidence (Casey, 2019, No. 6), but error rates should not be derived from inappropriate forms of quality assessment, such as proficiency testing (Budowle et al., 2009; Christensen et al., 2014). The complexity of the events that forensic science has to deal with does not always make it possible to empirically reproduce their exact conditions and to assess the uncertainties associated with them. However, on the one hand, empirical tests should help to understand the way in which location traces are generated and their meaning, in addition to the errors that occur during their creation and through their persistence on digital devices. These tests assess the general conditions in which location traces are found. On the other hand, depending on the context of the case, the other traces and data available, and the questions of interest, the approach has to be adapted in order to assess the reliability and relevance of the location traces in the given situation. A case-by-case consideration must be made to understand their potential. Forensic scientists must maintain a practical, critical and open-minded approach in order to effectively challenge the traces under consideration.

6.2. Future work

To contribute to this call for research and in order to reduce the potential for errors among practitioners, the authors are currently conducting a series of experiments to gain deeper insight into location traces, from their creation to their interpretation.

Smartphones are developing in an environment with a wide range of connectivity options, generating a large number of parameter options that could influence the trace. By splitting the investigation methodology, we can focus on fewer parameters at a time to understand how their variation is reflected in the trace.

First, there is a clear focus on understanding the smartphone positioning process and its reliability, as this is the starting point for most location traces, but as shown in this paper, other stages are also prone to generating errors and are the subject of more in-depth research.

In addition, the diversity of location traces is being explored, as a number of relevant traces (such as smartphone logs and tag traces) have not yet been fully considered. This requires a formalisation of spatial location (and more broadly spatio-temporal) traces to provide a clearer view of what is included in the scope of the research.

There is also a need to conceptualise the characteristics of such traces and how they should be handled in investigations.

6.3. Limitations

This article focuses on unintentional errors, leaving out intentional ones. In fact, there are other situations that can hinder the use of location traces. In particular, the location of a device can be spoofed through various means and at various levels (e.g. GNSS spoofing), which would produce inaccurate location traces. On top of that, a user could try to delete or modify location traces after they have been created, for example before the device is seized. These possibilities also have implications for the exploitation of location traces. Unintentional contamination or data transfer has also not been fully considered, although in some cases this possibility cannot be excluded. For example, some navigation applications (e.g. Google Maps) allow synchronisation or sharing of locations between devices. Finally, this article suggests errors that are known to occur in location traces, but for which it is difficult to provide frequency estimates due to the lack of research.

7. Conclusion

Location traces are valuable in digital investigations. They provide information about presence in the physical world and therefore allow to address spatial queries.

However, location traces suffer from reliability issues. They are created in complex environments, with a significant amount and variety of traces. Using several examples, we demonstrated that there are many uncertainties and errors in their creation and exploitation processes. In particular, their production mechanisms are not sufficiently understood for their fundamental reliability to be established. Some documented and reproducible device positioning errors (such as a buffer effect) are shifted to location traces, which may not be known or detected by the analyst. Furthermore, the exploitation of location traces relies on tools, that are often black boxes with multiple layers of abstraction. This further complicates their understanding. Some of the examples given highlighted how mainstream tools can introduce inaccuracies or fallacy suggestions that can lead to misinterpretation. Finally, there is a lack of conceptualisation of location traces, and the conclusions and hypotheses that can be drawn from them are not defined. Due to the variety of location traces and contexts in which they are produced, the meaning to be reconstructed is not always clear. Going back to the trace should help to solve this problem.

In conclusion, there is a gap between the perceived value and the knowledge that underpins the exploitation of location traces. This should be addressed through further research. In order to contribute to this call for research, the authors are currently undertaking conceptual work and a series of experiments to gain a deeper insight into location traces, from their creation to their interpretation and use for forensic purposes.

CRediT authorship contribution statement

Cléo Berger: Conceptualization, Writing – original draft. **Benoît Meylan:** Conceptualization, Visualization, Writing – original draft. **Thomas R. Souvignet:** Conceptualization, Supervision, Visualization, Writing – original draft.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We would like to thank our esteemed colleagues for proofreading this article: Prof. Eoghan Casey, Céline Vanini and Prof. Timothy Bolle.

Data availability

Data will be made available on request.

References

Arshad, H., Jantan, A.B., Abiodun, O.I., 2018. Digital forensics: review of issues in scientific validation of digital evidence. J. Inf. Process. Syst. 14 (2), 346–376. https://doi.org/10.3745/JIPS.03.0095.
Budowle, B., Bottrell, M.C., Bunch, S.G., Fram, R., Harrison, D., Meagher, S., et al., 2009. A perspective on errors, bias, and interpretation in the forensic sciences and direction for continuing advancement. J. Forensic Sci. 54 (4), 798–809. https://doi.org/10.1111/j.1556-4029.2009.01081.x.
Carrier, B., 2003. Defining digital forensic examination and analysis tools using abstraction layers 1 (4).
Casey, E., 2002. Error, uncertainty, and loss in digital evidence 1 (2).
Casey, E., 2019. The chequered past and risky future of digital forensics. Vol. 51. https://doi.org/10.1080/00450618.2018.1554090.
Casey, E., 2020. Standardization of forming and expressing preliminary evaluative opinions on digital evidence. Forensic Sci. Int.: Digit. Investig. 32, 200888. https://doi.org/10.1016/j.fsidi.2019.200888.
Casey, E., Jaquet-Chiffelle, D.-O., Spichiger, H., Ryser, E., Souvignet, T., 2020. Structuring the evaluation of location-related mobile device evidence. Forensic Sci. Int.: Digit. Investig. 32, 300928. https://doi.org/10.1016/j.fsidi.2020.300928.
Casey, E., Ribaux, O., Roux, C., 2018. Digital transformations and the viability of forensic science laboratories: crisis-opportunity through decentralisation. Forensic Sci. Int. 289, e24–e25. https://doi.org/10.1016/j.forsciint.2018.04.055.
Cherian, S.S., Rudrapatna, A.N., 2013. Lte location technologies and delivery solutions. Bell Labs Tech. J. 18 (2), 175–194.
Christensen, A.M., Crowder, C.M., Ousley, S.D., Houck, M.M., 2014. Error and its meaning in forensic science. J. Forensic Sci. 59 (1), 123–126. https://doi.org/10.1111/1556-4029.12275.
Dror, I.E., 2020a. Cognitive and human factors in expert decision making: six fallacies and the eight sources of bias. Anal. Chem. 92 (2), 7998–8004.
Dror, I.E., 2020b. The error in "Error Rate": why error rates are so needed, yet so elusive. J. Forensic Sci. 65 (4), 1034–1039.
Dror, I.E., Charlton, D., 2006. Why experts make errors. J. Forensic Identif. 56 (4), 600–616.
Eldridge, H., Stimac, J., Vanderkolk, J., 2022. The benefits of errors during training. Forensic Sci. Int.: Synergy 4, 100207. https://doi.org/10.1016/j.fsisyn.2021.100207.
ENFSI, 2015, November. Best practice manual for the forensic examination of digital technology.
Forensic Science Regulator, 2023, March. Code of practice. Version 1.
Georgiou, N., Morgan, R., French, J., 2023. The shifting narrative of uncertainty: a case for the coherent and consistent consideration of uncertainty in forensic science. Aust. J. Forensic Sci. 55 (6), 781–797. https://doi.org/10.1080/00450618.2022.2104370.
Hargreaves, C., Nelson, A., Casey, E., 2024. An abstract model for digital forensic analysis tools - a foundation for systematic error mitigation analysis. Forensic Sci. Int.
Horsman, G., 2019. Tool testing and reliability issues in the field of digital forensics. Digit. Investig. 28, 163–175. https://doi.org/10.1016/j.diin.2019.01.009.
Horsman, G., 2024. Sources of error in digital forensics. Forensic Sci. Int.: Digit. Investig. 48, 301693. https://doi.org/10.1016/j.fsidi.2024.301693.
Hoy, J., 2015. Forensic Radio Survey Techniques for Cell Site Analysis. Wiley, Chichester, West Sussex, UK.
Interpol, 2019, May. INTERPOL global guidelines for digital forensics laboratories.
Jaquet-Chiffelle, D.-O., Casey, E., 2021. A formalized model of the trace. Forensic Sci. Int. 327, 110941. https://doi.org/10.1016/j.forsciint.2021.110941.
Lyle, J.R., 2010. If error rate is such a simple concept, why don't I have one for my forensic tool yet?. Digit. Investig. 7, 135–139.
Maghdid, H.S., Lami, I.A., Ghafoor, K.Z., Lloret, J., 2016. Seamless outdoors-indoors localization solutions on smartphones: implementation and challenges. ACM Comput. Surv. 48 (4), 1–34. https://doi.org/10.1145/2871166.
Margot, P., 2017. Traceology: the bedrock of forensic science and its associated semantics. In: Rossy, Q., Decary-Hétu, D., Delémont, O., Mulone, M. (Eds.), The Routledge International Handbook of Forensic Intelligence and Criminology, Routledge. Taylor & Francis Group, Routledge, pp. 30–39.
Martire, K.A., Chin, J.M., Davis, C., Edmond, G., Growns, B., Gorski, S., et al., 2024. Understanding 'error' in the forensic sciences: a primer. Forensic Sci. Int.: Synergy 8, 100470. https://doi.org/10.1016/j.fsisyn.2024.100470.
Merry, K., Bettinger, P., 2019. Smartphone GPS accuracy study in an urban environment. PLoS ONE 14 (7), e0219890. https://doi.org/10.1371/journal.pone.0219890.
Murrie, D.C., Gardner, B.O., Kelley, S., Dror, I.E., 2019. Perceptions and estimates of error rates in forensic science: a survey of forensic analysts. Forensic Sci. Int. 302, 109887. https://doi.org/10.1016/j.forsciint.2019.109887.
Nassaji, H., 2018. Errors versus mistakes. In: Liontas, J.I. (Ed.), The TESOL Encyclopedia of English Language Teaching, 1st ed., pp. 1–5.
Ogulenko, A., Benenson, I., Toger, M., Östh, J., Siretskiy, A., 2022. The fallacy of the closest antenna: towards an adequate view of device location in the mobile network. Comput. Environ. Urban Syst. 95 (101826). https://doi.org/10.1016/j.compenvurbsys.2022.101826.
Page, H., Horsman, G., Sarna, A., Foster, J., 2018. A review of quality procedures in the UK forensic sciences: what can the field of digital forensics learn? Sci. Justice 59 (1), 83–92. https://doi.org/10.1016/j.scijus.2018.09.006.
Pietro, D.S., Kammrath, B.W., De Forest, P.R., 2019. Is forensic science in danger of extinction? Sci. Justice 59 (2), 199–202. https://doi.org/10.1016/j.scijus.2018.11.003.
Pollitt, M., Casey, E., Jaquet-Chiffelle, D.-O., Gladyshev, P., 2018. A framework for harmonizing forensic science practices and digital/multimedia evidence. In: Organization of Scientific Area Committees for Forensic Science.
Ralf, B., C, C., M, K., T, M., 2004. Indoor and outdoor positioning in mobile environments—a review and some investigations on WLAN-positioning. Ann. GIS 10 (2), 91–98. https://doi.org/10.1080/10824000409480660.
Raubal, M., Miller, H.J., Bridwell, S., 2004. User-centred time geography for location-based services. Geogr. Ann., Ser. B., Hum. Geogr. 86 (4), 245–265. https://doi.org/10.1111/j.0435-3684.2004.00166.x.
Ribaux, O., 2023. De la police scientifique à la traçologie: Le renseignement par la trace. Sciences forensiques. Presses Polytechniques et Universitaires Romandes, Lausanne.
Rossy, Q., 2011. Méthodes de visualisation en analyse criminelle: Approche générale de conception des schémas relationnels et développement d'un catalogue de patterns. Doctoral dissertation.
Rossy, Q., 2024. L'analyse spatiotemporelle. Lecture. Lausanne, Suisse.
Roux, C., Bucht, R., Crispino, F., De Forest, P., Lennard, C., Margot, P., et al., 2022. The Sydney declaration – revisiting the essence of forensic science through its fundamental principles. Forensic Sci. Int. 332, 111182. https://doi.org/10.1016/j.forsciint.2022.111182.
Rudin, N., Inman, K., 2005. Fingerprints in print, the sequel. CAC Newsl., 6–10.
Ryser, E., 2024. Facteurs d'incertitude en science forensique numérique. Doctoral dissertation, Université de Lausanne. Ecole des Sciences Criminelles, Lausanne, Suisse.
Samuels, A., 2022. Forensic science regulator: the forensic science regulator act 2021. Med.-Leg. J. 90 (2), 86–89. https://doi.org/10.1177/00258172211068227.
Servida, F., Fischer, M., Delémont, O., Souvignet, T.R., 2023. Ok Google, start a fire. IoT devices as witnesses and actors in fire investigations. Forensic Sci. Int. 348, 111674. https://doi.org/10.1016/j.forsciint.2023.111674.
Spichiger, H., 2022a. Where your iphone is not: issues with error and data visualisation in location-related evidence from ios devices. In: 9th European Academy of Forensic Science Conference. Stockholm.
Spichiger, H., 2022b. The evaluation of mobile device evidence under person-level, location-focused propositions. Thèse de doctorat, Ecole des Sciences Criminelles. Université de Lausanne, Lausanne, Suisse.
Spichiger, H., 2023. A likelihood ratio approach for the evaluation of single point device locations. Forensic Sci. Int.: Digit. Investig. 44, 301512. https://doi.org/10.1016/j.fsidi.2023.301512.
Sunde, N., 2021. What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices. Sci. Justice 61 (5), 586–596. https://doi.org/10.1016/j.scijus.2021.06.010.
Sunde, N., 2022. Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations. Forensic Sci. Int.: Digit. Investig. 40, 301317. https://doi.org/10.1016/j.fsidi.2021.301317.
Sunde, N., Dror, I.E., 2019. Cognitive and human factors in digital forensics: problems, challenges, and the way forward. Digit. Investig. 29, 101–108. https://doi.org/10.1016/j.diin.2019.03.011.
SWGDE, 2018. SWGDE establishing confidence in digital and multimedia evidence forensic results by error mitigation analysis.
SWGDE, 2021. SWGDE establishing a quality management system for a digital and multimedia organization under ISO-IEC 17025 or 17020.
Tart, M., Brodie, I., Patrick-Gleed, N., Edwards, B., Weeks, K., Moore, R., Haseler, R., 2021. Cell site analysis; use and reliability of survey methods. Forensic Sci. Int.: Digit. Investig. 38, 301222. https://doi.org/10.1016/j.fsidi.2021.301222.

Tart, M., Brodie, I., Gleed, N., Matthews, J., 2012. Historic cell site analysis – overview of principles and survey methodologies. Digit. Investig. 8 (3), 185–193. https://doi.org/10.1016/j.diin.2011.10.002.

Van Zandwijk, J.P., Boztas, A., 2021. The phone reveals your motion: digital traces of walking, driving and other movements on iPhones. Forensic Sci. Int.: Digit. Investig. 37, 301170. https://doi.org/10.1016/j.fsidi.2021.301170.

Van Zandwijk, J.P., Boztas, A., 2019. The iPhone health app from a forensic perspective: can steps and distances registered during walking and running be used as digital evidence? Digit. Investig. 28, S126–S133. https://doi.org/10.1016/j.diin.2019.01.021.

Vink, M., Sjerps, M., Boztas, A., van Zandwijk, J.P., 2022. Likelihood ratio method for the interpretation of iPhone health app data in digital forensics. Forensic Sci. Int.: Digit. Investig. 41, 301389. https://doi.org/10.1016/j.fsidi.2022.301389.

Vuille, J., Taroni, F., 2021. Measuring uncertainty in forensic science. IEEE Instrum. Meas. Mag. 24 (1), 5–9. https://doi.org/10.1109/MIM.2021.9345602.

Zandbergen, P.A., 2009. Accuracy of iPhone locations: a comparison of assisted GPS, WiFi and cellular positioning. Trans. GIS 13, 5–25. https://doi.org/10.1111/j.1467-9671.2009.01152.x.