



Sources of error in digital forensics

Graeme Horsman

Cranfield Forensic Institute, Cranfield University, College Rd, Cranfield, Wharley End, Bedford, MK43 0AL, UK

ARTICLE INFO

Keywords:

Digital forensics
Error
Digital evidence
Quality assurance
Investigative process

ABSTRACT

The occurrence of errors in forensic practice is inevitable, and whilst we may not feel comfortable with the idea, the truth of it must be acknowledged. At a time where forensic science is under intense scrutiny regarding the quality of its work, there has never been a greater need for it. In relation to the field of digital forensics (DF), the support it offers law enforcement is fundamental to many of its inquiries, and ensuring the reliability and accuracy of its services is vital. Errors in forensic practice can have far-reaching consequences for all those involved in an investigation, and practitioners and their organisations must take steps to identify, mitigate and manage them. This work focuses on the concept of error in relation to the field of DF. It first explores what an error is and the language used to describe one before mapping potential sources of error against the stages of the DF investigative process. This is done to assist those in the DF field to identify error sources, what they are and where they come from, and to facilitate the attribution of errors to a source, helping them to address them effectively.

1. Introduction

Digital evidence now plays an essential role in helping law enforcement to conduct their inquiries effectively (Sunde, 2017), and it is widely reported to be present in over 90 % of criminal cases (National Police Chiefs Council, 2020; Miller, 2023). It often assists investigators to understand any alleged law-breaching conduct, meaning that it is essential that any tasks conducted by those in the field of digital forensics (DF) can be relied upon by all parties that are subject to, and involved in the course of a lawful investigation (Neale et al., 2022). For all forensic examination work undertaken, practitioners and their organisations should strive to produce results that are accurate and dependable, as the consequences of unsound forensic evidence and any subsequently based testimony can cause harm to all parties involved (Erbacher, 2010; Casey, 2002, 2019). Yet, it should be noted that the occurrence of error in forensic practices is inevitable, despite historically some experts having denied their existence within their respective forensic fields (Murrie et al., 2019).

Stoykova et al (2022, p.1) states that 'law enforcement authorities are dependent on DF methods to ensure evidence reliability and compliance with fair trial requirements of evidence authenticity, reliability, and contestability in criminal proceedings'. The idea of error can cause discomfort and invoke concern, particularly in the many subfields of forensic science where a number of miscarriages of justice have been reported following flawed forensic processes and the misinterpretation of information (Dioso-Villa, 2015; Gill, 2018; Sunde and Dror, 2019).

Casey (2002, p.1) goes further, noting that in some cases, 'having incorrect information is potentially more damaging than having no information' and it is recognised that errors can lead to unsafe legal decision making. Errors can also be expensive, wasting both time and resources (Dimpe and Kogeda, 2017), and whilst we may not like them, the potential for them to exist in our forensic processes and practices needs to be acknowledged.

It is tempting for those in the DF field to form narratives around a requirement to eliminate errors from the investigative process in their entirety, and whilst this would obviously be an ideal situation, it is realistically unachievable. The field of DF must accept that the occurrence of errors is unpreventable (Horsman and Sunde, 2020) and understand that just because we may not recognise or notice them, does not mean they aren't there. The field has a responsibility to actively seek to identify errors in their work, rectify them, manage their impact, and to try and improve future practice (McKemmish, 2008). By acknowledging the potential for errors to exist in the digital investigation process, it is suggested that a dedicated portion of the efforts of practitioners and their organisations when it comes to quality control and assurance measures should be directed towards developing robust methods for identifying them, understanding their effect, and the reasons for their occurrence. This position is supported by Christensen et al (2014 p.123) who 'urge forensic practitioners to ensure that potential sources of error and method limitations are understood and clearly communicated and advocate that the legal community be informed regarding the differences between interobserver errors, uncertainty, variation, and

E-mail address: graeme.horsman@cranfield.ac.uk.

<https://doi.org/10.1016/j.fsidi.2024.301693>

Received 14 November 2023; Accepted 14 January 2024

Available online 9 February 2024

2666-2817/© 2024 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

mistakes'. By accepting that forensic processes/procedures may not operate perfectly all of the time, we must observe the need to understand any metrics and variables that may compromise their performance.

Reedy (2021) suggests that a decline in the standard of DF examinations is being witnessed. In jurisdictions such as England and Wales there is a push for DF organisations to seek alignment with overarching accreditation schemes (Tully et al., 2020), put in place to try and reduce error (Hughes, et al., 2022). On a larger scale, it is likely that jurisdictions worldwide are equally seeking to bolster forensic practices. Whilst it is both natural and understandable to fear error, points of learning can be gleaned from them in order to enhance practice (Mayo, 1996; Schickore, 2005). Arguably, when trying to develop robust and reliable practices, the determination of error is as equally important as the identification of a correct response for any given task; this allows us to ascertain an acceptable remit of operation. Through the making and detection of errors, those in DF can establish, develop and enhance investigative techniques and begin to recognise and evaluate their working conduct. Yet concerningly, at present 'there is no empirical understanding of how frequently error occurs in the discipline' (Hughes, et al., 2022 p.1). Detecting and understanding error in the field of DF is a necessary part of any quality assurance and control protocols and this begins with determining what sources of error exist within the investigative process and where such errors may occur.

This work focuses on the concept of error in relation to the field of DF. It first explores what an error is and the language used to describe one before mapping potential sources of error against the stages of the DF investigative process. This is done to assist those in the DF field to identify error sources, what they are and where they come from, and to facilitate the attribution of errors to a source, helping them to address them effectively.

2. What is an error?

The Oxford English Dictionary (2023) defines an error as "a mistake", where Du (2017, p.140) goes further stating 'errors refer to the degree that measurement results deviate from the true value'. Christensen et al. (2014) note that defining 'error' can be problematic, and it can be expressed in a number of ways (Earwaker et al., 2020) and therefore the concept of 'error' is perhaps best described as deceptively simple. Fundamentally, it is a descriptor that acknowledges something as being incorrect, but it is perhaps the informal use of the term that can create difficulty.

'Error' may be used casually (*'a throwaway comment'*) or inconsistently to describe the results of any observed task that were unexpected. As a result, caution should be exercised when the use of the term error is witnessed as it may be deployed as a label for outcomes that an individual subjectively believes to be incorrect; but this may not be the case. In such instances, a judgement on the 'correctness' of any outcome may be made due to a 'hunch' or following 'personal biases', and in absence of a logical and scientifically rigorous evaluation of any available data that provides justification for their judgement. As a result, someone may believe something is erroneous because they think it looks wrong, but it may not be. Those in DF should be vigilant of the informal use of the term error, and where it is witnessed seek to ascertain the remit of any logic and reasoning deployed in the process of reaching such a decision.

Errors are 'deviations from accuracy or correctness' (Dictionary.com, 2022). Being able to consistently and accurately identify errors requires knowing what the correct behaviour or 'accepted performance' is for any given process/procedure and being able to distinguish it from what is being seen. It also requires recognition that any task's 'accepted performance' may not be restricted to a single outcome, and instead include a range of conclusions. This task calls for the use of scientific testing and a sound evidence base from which to make any judgements.

2.1. Recognising the importance of errors

Errors are part of everyday life (Kryeziu, 2015), and their resulting consequences can range in severity. In some situations, errors can be navigated with little to moderate inconvenience, however, for those in forensic science disciplines, errors can have catastrophic consequences (Kloosterman et al., 2014; Robertson, 2013; Du, 2017), fuelling public mistrust in these disciplines (Kaplan et al., 2020). As Metcalfe (2017 p.466) states, 'nobody wants to make errors in a situation that counts', and errors are typically considered negative 'things' (Eldridge et al., 2022). Whilst it is recognised that they can carry ramifications for those that make them and may even make them feel bad, errors can be valuable learning experiences (Overbye et al., 2020). We must be careful so as to not throw away all of the points of learning that can be gained from the occurrence of error, as in most cases understanding the cause and impact of it offers the potential to improve current and future practices (Tulis et al., 2016). Perhaps best summarised by Einhorn (1986) - by accepting the occurrence of errors we better prepare ourselves to make less future errors.

Those in forensic science use specialised methods and techniques to identify, access and interpret information, allowing them to try and understand any relevant events that are alleged to have taken place. These actions may exonerate or implicate potential suspects (Etter, 2013). Due to the importance of this work it is understandable that errors in this context are perceived as bad, as we are immediately drawn to the worst case scenarios (Eldridge et al., 2022). These concerns may drive a belief that we can never make errors and Jeanguenat and Dror (2018) note that there is sometimes a 'zero tolerance' attitude for error, but this is a difficult stance to uphold. A fear of making errors may prevent growth in forensic fields and stunt the development of both new knowledge and investigative techniques. It is understandable that when entering uncharted territory in any discipline, the manifestation of error in our work is likely until we gain a robust understanding of any environment. Errors in these situations should have limited real-life impact as the process of new knowledge discovery should be ring-fenced, and any learning gleaned should be fully validated before (or if) it encroaches on operational practice.

Providing we are willing to, errors can facilitate learning (Tulis et al., 2016) if we understand any causes, and corrective feedback is identified and offered as opposed to simply chastising those responsible. If it is perceived that any errors will result solely in punishment, there is a risk of paralysing any discipline's development, leading to its value over time degrading. Errors should be used to shape and improve future performance (Overbye et al., 2020), and it is perhaps necessary at this point to stress that this work is not providing a justification for reckless or negligent practices that could or are likely to result in error; genuine efforts to perform properly and diligently must be made at all times by all those in forensic science. However, forensic fields should push beyond their comfort zones in order to advance their practices, but this should be done in a controlled manner. There is no silver bullet solution to preventing error in forensics (Budowle et al., 2009) and it is important that practitioners in DF prepare for errors to be made. Methods should be put in place that both check for the occurrence of error, and to manage their impact and extract points of relevant information from an event for the purposes of practice-improvement when one is detected (Mera et al., 2022).

2.1.1. Attribution of error

Whilst the concept of attributing error to a source may again cause unease, it is an important part of ensuring we can learn from any error discovered, and for evaluating and improving practices. Whilst identifying the presence of an error may prevent or limit any consequences relating to it, in order to try and stop or restrict any repeat occurrences of it we need to understand where the error has come from and why it has occurred. In essence, errors need to be attributable to their source, so that appropriate measures can be taken to address and improve that

source. If the source of an error can be determined, steps can also be taken to determine what causal factors may have contributed to the occurrence of the error, which if it were not for them, an error may have been prevented or its severity lessened (Center for Chemical Process Safety, n.d.) (See Fig. 1).

Again, error attribution should not be seen as a 'blame game', rather a fundamental quality assurance process for long term practice improvement. Once a source of error is established it may be possible to stop it, and improvements can be made via training, education or procedural development.

2.2. Forms of error

To start, it is important to distinguish error from mistake. Nassaji (2018, p1.) provides the following clarification - 'errors are defined as deviations that are competence-based and occur as a result of a lack of knowledge. Mistakes, however, are performance-related and occur even though the learner has the knowledge'. Both can be problematic to the forensic process and steps to detect and prevent both should be taken. Sunde (2022) notes that there are typically two groupings for errors in DF, technical (tool/instrument-based etc.) and non-technical (decision making etc.) and these can occur across multiple stages of an investigation. Practitioners in DF are concerned with the scientific measurement of digital data found within their casework and often conduct experiments as part of their investigative processes when attempting to examine data and interpret the meaning of any potentially relevant digital traces. In the context of DF work, measurement errors may occur (the 'difference between any target's true value and the measured value' (Keyence, n.d.)) and can be generalised into the following three types.

1. **Systematic error:** Barlow (2002) describes systematic error as a 'reproducible inaccuracy' which could be as a result of equipment or process issues. The important element of systematic errors are that they are 'biased due to a specific cause' (Keyence, n.d.) and the size of the error is consistent when the conditions are deployed (Huang et al., 2021). In DF, systematic errors can occur due to a tool's implementation of an algorithm (Horsman and Sunde, 2020) or the misconfiguration/misimplementation of a process/procedure. Horsman and Sunde (2020) highlight that systematic tool errors in DF generally lead to results that are incomplete, inaccurate or misinterpreted (SWGDE, 2018). As DF is founded upon computer science, systematic errors are likely one of the most commonly encountered error types (SWGDE, 2018).
2. **Random error:** A random error is 'an error in measurement caused by factors which vary from one measurement to another' (Oxford Languages, 2023) when conditions are fixed (Vosk and Imwinkelried, 2017). Random errors may be difficult to measure as they are often based on natural processes (SWGDE, 2018).
3. **Negligent errors:** Keyence (n.d.) note that 'this type of error is caused by the inexperience of or the incorrect operations performed by the measuring individual'. Negligent errors may be as a result of a practitioner not being appropriately trained in the use of or the interpretation of results provided by certain tools/methods.

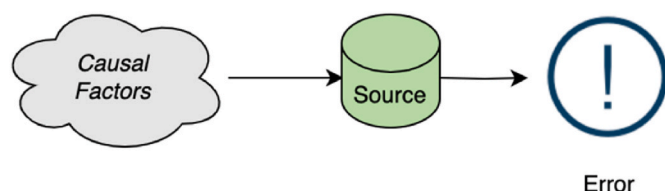


Fig. 1. Errors, sources and causal factors.

3. Mapping sources of error to the investigative process

The field of DF is transitioning from its ad hoc beginnings to a more formalised forensic science (Casey, 2009). As part of this development, arguably and understandably, focus has been on the expansion of its capability, possibly to the detriment of the formalisation of its quality assurance processes. We see this now with some of the challenges expressed (financials aside) in regard to attempts of DF organisations to adhere to overarching accreditation standards (Tully et al., 2020). All forensic disciplines must constantly strive to develop and improve their practices (Budowle et al., 2009), the result of which is the inevitable discovery of new errors and the identification of old ones. Errors can originate from a number of sources in forensic science and it is important that efforts are made to try and recognise and deduce these (Christensen et al., 2014). Christensen et al (2014 p.124) state that 'the importance of implementing measures to minimise and account for error and limitations in forensic sciences methods should now be apparent. Understanding and appropriately communicating these issues can resolve confusion over the significance of results and can prevent intentional or unintentional misuse of error'. Gearing up to detect and address errors is often a task considered with forthcoming practice in mind, however, the discovery of errors can also affect the validity of past work. Any errors identified may undermine decisions and findings presented in previous cases, resulting in unsafe legal decisions having been made.

At present, there is limited work that discusses the origin of error in DF and this can impact upon both past and future work. HSchiffer (2009, p.114) notes that 'a lack of data regarding sources of error has been observed across all forensic fields'. As a result, this work proposes a need to identify potential sources of error and for these to be mapped to the main stages of the DF investigative process. The following three justifications for doing this are offered.

1. **Identify error:** Service demands and staffing levels can make it difficult for forensic labs to avoid errors (Committee on Identifying the Needs of the Forensic Sciences Community National Research Council, 2009). If we accept that error is inevitable, then steps should be taken to understand where errors are occurring in the investigative process, why they are happening, and the types of error occurring. Budowle et al. (2009, p.801) acknowledges this point, stating that 'it is important to identify potential error and focus on those areas where error is most likely to occur'. This allows practitioners and organisations to develop quality assurance measures that specifically support somewhat 'error-prone' parts of the investigative process.
2. **Manage and mitigate error:** Once the locations and types of error can be comprehended, DF practitioners and their organisations can begin to understand and evaluate their impact and any associated risks to the quality of any work being produced by them. It is not enough to just state the presence of error, protocols to manage the effect of errors must be designed and efforts for error mitigation that targeted specifically known error-types should be made.
3. **Prepare for error:** Error detection and management cannot be deployed as a one time only process, it must be continuous. To effectively map potential sources of error to the DF process requires constant re-evaluation of the field. Whilst some sources of error are fundamental to the investigative process, the field is dynamically changing and developing its examination methods and techniques, meaning new sources of error could continuously originate. In addition, reviews for error must take place in current practice, future potential practices, and a review of past practices for error should be undertaken (Budowle et al., 2009). Once errors are discovered, understanding their immediate impact is important, but it is also necessary to evaluate past instances where any erroneous practices of a similar nature may have also occurred. We should not just consider outcomes that are likely to end up in court as being worthy

of error detection processes, all work should be reviewed for error, regardless of its severity or importance (Christensen et al. (2014)).

*To note:- This work intends to provide a starting point for error-source mapping for the field of DF, and it should be recognised that this task cannot be considered static; continuous evaluations must take place in order to determine new sources and types.

3.1. Errors and the investigative process

Informally, we may consider the forensic process as being from 'crime scene to court' (White, 2010) and issues can occur at any stage. When mapping errors, it is necessary to consider two factors, (1) the key stages of an investigation, and (2) sources of errors that can occur at each stage.

Considering first, the generally accepted main stages of the digital investigation process, as documented by Horsman and Sunde (2022) are as following.

1. *Incident Response: Identification, Handling, Preservation & Collection.* This is a stage that occurs when first responders are called to an incident and subsequently determine the need to identify, handle, preserve and collect digital devices/data. In some cases, pre-planning may be limited as they may not understand the extent of any circumstances surrounding an incident until they arrive. Those in attendance at this stage are unlikely to be trained DF professionals. In cases of pre-planned operations, this stage will not take place and the investigative process will start from stage 2 noted below.
2. *Review of Client Requirements (Pre Device/Data Seizure) & Planning.* This stage occurs pre-scene attendance and device collection and allows any client to determine the initial remit of any digital inquiries. This may be done in advance of the deployment of any planned operation.
3. *Identification, Handling, Preservation & Collection (Planned).* In contrast to stage 1 above, this stage involves the planned for identification, handling, preservation and collection of digital devices or data in accordance with any instructions noted in stage 2.
4. *Review of Client Requirements (Post Device/Data Seizure) & Planning.* This stage involves determining any instructions for the examination of any devices or data once seized.
5. *Exhibit Handling (In-Lab).* This stage involves the processing of exhibits within a lab environment.
6. *Data Acquisition.* This stage involves the acquisition of data from any seized data-source noted in stage 5.
7. *Data Processing/Examination.* This stage involves the examination of any data acquired from stage 6.
8. *Analysis, Interpretation and Evaluation.* This stage involves the analysis, interpretation and evaluation of any data processed in stage 7.
9. *Presentation of Findings for Peer Review.* This stage involves the peer review of any findings noted from stage 8.
10. *Presentation/Communication of Results.* This stage involves the production of any findings derived from the completed investigative process which address any client requirements.

To avoid repetition of content, each of these stages will not be re-described in detail here, instead the reader is directed to the narratives provided by Horsman and Sunde (2022). However, each stage is contextualised in the following sections when referring to sources of error.

Throughout the 10 stages of the investigative process outlined above, the following six main sources of error are identified.

1. Client errors.

2. Wider investigative/forensic team errors.
3. Practitioner errors.
4. Tools/instruments errors.
5. Method errors.
6. Trace errors.

Fig. 2 maps the six error sources across the 10 stages of the DF investigative process, highlighting at which stages each error source could be primarily present. Each of the six error sources are discussed in Sections 4-9 and their impact on the stages of an investigation highlighted and described.

4. Client error

Within the context of this work, the term client is defined widely. A client is considered to be any entity that is the subject of a DF investigation or invoking the need for one, and therefore is providing instructions or information that may be relied upon or used to guide forensic decision making and procedures later in the investigative process. Practitioners must ascertain the requirements of any client and evaluate the best course of action for addressing them. Practitioners rely on clients to provide them with all of the necessary case-related information needed for them to undertake an investigation, and that they provide this information accurately. In addition, support must be provided to clients to help them understand the DF process and how it applies to any of their exhibits being subjected to it. The following are defined as clients within the scope of this work:-

1. Any victims of an incident, where the need for a digital forensic examination is subsequently identified. Their devices or data may be subject to analysis, or they may provide testimony to law enforcement or a forensic team that may try to highlight potential relevant information (for example, providing relevant 'screen names' in alleged grooming cases, or highlighting messages of interest).
2. Any defendant subject to an investigation where a digital forensic examination is being carried out which concerns information alleged to pertain to their course of conduct. They may provide testimony to law enforcement or a forensic team outlining their version of events or data that they believe is pertinent to any alibi.
3. Both prosecution & defence counsels who are acting for any victim/defendant and who may instruct a forensic team.
4. Any officer in charge (OIC) of an investigation who maintains responsibility for a case where digital exhibits are contained and require forensic investigation following their instruction.

Often before any technical work can begin, the requirements of any client need to be established with accuracy (Cook et al., 1998) so that a practitioner can determine how best to address them. It is suggested that clients (as they are defined above) will feature at the following preparatory stages of the investigative process, where errors may occur.

1. *Review of Client Requirements (Pre Device/Data Seizure) & Planning:* A client may feature prior to any scene-attendance and device seizure; during the planning stage relating to any incident or operation. Here, a client may be any instructing counsel or a victim/defendant who has disclosed information around any alleged events that may be relied upon later in the forensic process when making decisions about device seizure and beyond. In turn, a client may be any OIC leading an investigation or operation concerning an incident, and is seeking to provide what they consider critical information for guiding any forensic work in line with their requirements. The information disclosed at this stage may impact how any scene attendance is conducted and the amount and type of devices being seized and subjected to a forensic examination (Horsman, 2021b). Clients errors occurring here may include:

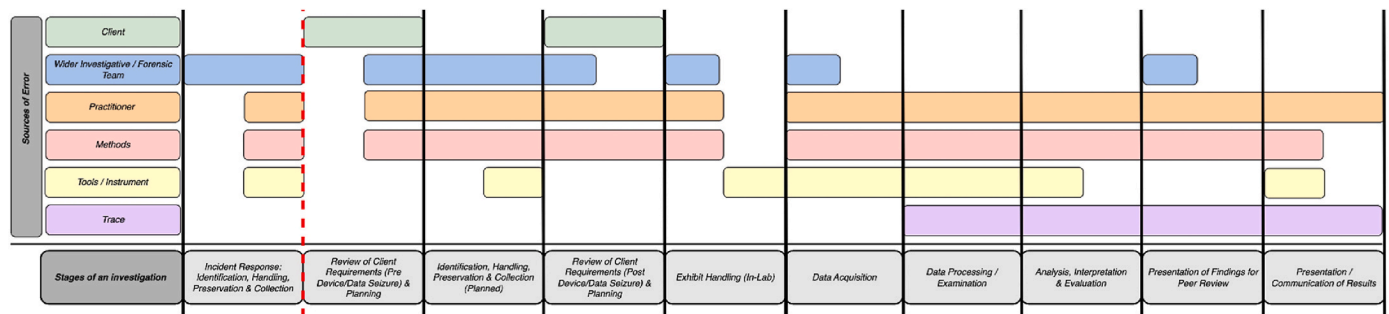


Fig. 2. Mapping sources of error to stages of a digital investigation.

- Any instructing clients may provide or state information regarding the circumstances of a case incorrectly. Alternatively, clients may provide information that is incorrect, but not realise this to be the case. This may be due to flaws in any witness versions of events, the misinterpretation of any alleged events, or via false testimony made by a victim/defendant.
 - Any instructing client may fail to understand the investigative value and opportunities provided by digital devices (Horsman, 2021) and omit to factor them into their requirements as part of search and seizure. This may lead to the failure to identify and collect devices/data that may have been pertinent to an inquiry. Or alternatively, the wrong type of device/data could be collected.
 - Any instructing counsel may misunderstand the requirements of their alleged offence and how any forms of digital evidence can support their case. This may result in relevant devices/data being missed or the wrong devices/data being seized.
 - A client may not understand the capability of any forensic services at their disposal and therefore fail to identify devices that are relevant due to a belief that they cannot be examined.
 - A client may not have established the relevant legal permissions to seize any devices.
2. *Review of Client Requirements (Post Device/Data Seizure) & Planning:* Whilst similar to (1), here clients (likely instructing counsels and OICs) may define their requirements in terms of what if they believe they need from a DF examination of any devices, in relation to supporting their case. Clients errors occurring here may include:
 - Failing to identify and understand information that is both relevant to their case, and that may exist on any device/data being examined. As a consequence, omitting to state a requirement to search for it as part of any DF examination.
 - Offence-pertinent information may be communicated to any forensic team incorrectly meaning that any subsequent forensic procedures may be misaligned with what is required, potentially increasing the chance of case-relevant data being missed, or examination delays.
 - Failing to understand the capability of an DF team, impacting the scope and remit of any investigative actions that they ask for.
- ### 5. Wider investigative/forensic team error
- A wider investigative/forensic team includes all of those individuals involved in the conducting of an investigation, beyond that of the DF practitioner. Examples may include front line police officers who attend an incident and subsequently seizure of a digital device (but are not in charge of the case), other law enforcement officers and associated roles involved in an incident, or staff supporting the DF practitioner internal to their laboratory (technicians, other practitioners etc.).
- It is suggested that any wider investigative/forensic team will feature at the following stages of the investigative process, where errors may occur.
1. *Incident Response: Identification, Handling, Preservation & Collection:* This stage does not typically feature in the traditional DF investigative process, often because it is conducted on an ad hoc basis, often beyond the scope and oversight of a DF practitioner and typically by front line police. When responding to an incident, police officers may subsequently deem it necessary to identify, handle and seize digital devices for further investigation. Given that in these cases, any devices may end up entering the DF investigative process, errors occurring here are pertinent to discussions and could include:
 - An officer may breach their authorised powers of search and seizure and unlawfully collect devices for investigation.
 - An officer may fail to understand the value of any digital devices to their inquiry and omit to seize them, or seize unnecessary items. This may be due to a lack of knowledge or training, or their decision making could be impacted by the stress of a situation (Jean-guenat and Dror, 2018).
 - An officer may incorrectly utilise an approved method for the identification, handling and seizure of any devices, impacting upon evidence continuity and integrity protocols and potentially compromising the value of any subsequent digital evidence.
 - It is considered unlikely that an officer will utilise tools/instruments as part of an incident response event. However, where this is the case, an officer may mis-deploy a tool, incorrectly use a tool, or utilise an inappropriate tool for the given case circumstances. This may lead to a misinterpretation of any results, or results that misrepresent the importance of a device to the current inquiry.
 2. *Review of Client Requirements (Pre Device/Data Seizure) & Planning:* Members of a wider investigative team may also be involved in reviewing any client requirements during a planning and pre-seizure meeting. Their role here is often to support clients to determine and understand the most appropriate course of action for a given investigative scenario. Errors occurring here may include:
 - Failing to accurately and effectively communicate any available and case-relevant forensic capability.
 - Failing to understand any case and client requirements.
 - Failing to understand or acknowledge any client-requirements.
 - Misadvising parties in regard to the forensic process and appropriate courses of action.
 - Relaying or providing case information incorrectly.
 3. *Identification, Handling, Preservation & Collection (Planned):* Many of the same issues noted above in (1) when operating in an incident response capacity also apply at this stage. In addition to these potential errors, the following are noted:
 - Failure to deploy any agreed course of action correctly.
 4. *Review of Client Requirements (Post Device/Data Seizure) & Planning:* Once any devices are in lawful possession, an examination strategy can be discussed in line with any client requirements (Horsman, 2022, 2023). Any wider investigative/forensic teams may support this process where those error-types noted at the 'Review of Client Requirements (Pre Device/Data Seizure) & Planning' stage above in (2) also apply here.

5. **Exhibit Handling (In-Lab):** Any device handling inside of a DF lab is likely to be conducted by the wider forensic team support staff which could include exhibit management personnel. Their role involves ensuring that relevant devices are received appropriately within their organisation, stored and handled properly during the course of their forensic examination, and subsequent return to a client. Errors occurring here may include:-
 - Administrative errors regarding property receipt, management and storage.
 - Failure to identify errors in chains of exhibit continuity.
 - Physical exhibit handling errors (breakages etc.).
6. **Data Acquisition:** The acquisition of a device may be conducted by an in-lab technician (unless specialist acquisition methods require practitioner input). Errors in the acquisition process may include:
 - Utilising an acquisition method that was not agreed upon.
 - Wrongly deploying an acquisition method.
 - Physical breakage of equipment/devices.
7. **Presentation of Findings for Peer Review:** Any practitioner conducting forensic work should subject their work to peer-review (Horsman and Sunde, 2020).

6. Tool error

Practitioners will utilise tools at multiple stages of the investigative process, ranging from device identification through to the presentation and communication of results. DF practitioners rely upon the results provided by their tools (Marshall and Paige, 2018) in order to inform future investigative processes and to interpret the meaning of any relevant traces (Garfinkel, 2010), but it must be recognised that tools are unlikely to always perform in a way that is completely error-free all of the time (Flandrin et al., 2014; Horsman, 2018; Horsman and Lyle, 2021). Arshad et al. (2018) note that there are previous instances where DF tools have been blamed for failing to correctly interpret data (Cole et al., 2015), most notably in the Casey Anthony trial (Horsman, 2018). Whilst we may initially expect any software product we purchase to perform perfectly, this is an unrealistic stance to adopt given the complexity of the tasks that in many cases they are trying to perform. With that said, tool-purchasers should still expect a level of quality from the product, but with specific reference to the field of DF, be prepared to evaluate them as part of their own quality control and assurance processes (Pan and Batten, 2009; Horsman, 2019; Horsman and Lyle, 2021). While tool testing is unlikely to detect all errors that may be present, it should provide an idea of reliability (Beckett and Slay, 2007). Legally, ruling such as *Daubert* means that the 'known or potential rate of error' of a DF tool should be noted (Lyle, 2010; Meixner and Diamond, 2014), however Jones and Vidalis (2019) suggest many tools fail to satisfy this criteria, and their error rates are unknown. Even if a tool is tested for error, due to updates, tool testing must be continuous (Baggili et al., 2007).

Christensen et al. (2014, p.124) define tool (instrument or technological) error 'as the difference between an indicated instrument value and the actual (true) value', a concept that in the field of DF is deceptively simple. Sources of tool error may include flaws in their source code or from abstraction errors (Carrier, 2002, 2003), where Lyle (2010) expands, stipulating that error may come from any algorithm intended for any given process and how any tool has opted to deploy the algorithm. In some cases the identification of a tool error may be more straightforward, for example in cases where a tool maintains explicit instructions for conducting a task to find string 'X' within a dataset, and when used in this way, instances of 'X' were not *flagged* by the tool, but inline with the tool's stated capability, they should have been. Tool-error detection may be easier when any results generated by a tool can be readily and reliably evaluated or where the correct answer is obvious or indisputable.

Yet in DF, it is not always possible to operate a tool in conditions that make it apparent when the right or wrong result is being observed. Error

detection may be more evident in cases where the 'type' of data is the focus of task (for example, recover of file type 'A' is required, yet file type 'B' is presented by a tool), however, errors involving quantity of data are far more difficult to detect (for example, a search for files of type 'F' where none are found, but 100 exist and have been missed). For this reason we must first consider some of the fundamental aspects that are required in relation to determining a DF tool error.

The task of distinguishing tool error from an accepted accurate performance requires three fundamental components.

1. Before using a tool for any given task, it is necessary to determine whether it is capable of conducting the task. This is often a complicated task, and one that starts with determining what a tool states that it can and can't do. DF tools cannot be responsible for the production of errors when performing tasks they were not meant to perform. This may seem obvious when more straightforward examples are provided; you cannot blame a key for failing to open a door, if that key was never intended for use with that door's lock.
2. As Cohen (2010, p.25) states, 'regardless of how "good" a tool is, it must be properly used'. Any tool used to conduct a task must be deployed in a way that is approved by the producer/vendor.
3. Only when points (1) and (2) are established, can a tool's performance in relation to a task be evaluated in order to determine the accuracy of its performance. The correct ('accepted/truth') outcome for any given task must first be established. In simple terms, it is impossible to determine when a tool's performance has resulted in error, if we cannot first establish what a correct result should look like. Then any discrepancy between the tool's performance and the known correct performance be established.

It is necessary to discuss the aforementioned 3 components in more detail, starting with determining the capability of a tool.

6.1. Establishing a 'scope of performance'

Carrier (2002, p.5) states 'digital forensic tools typically process data through a series of rules. The developers of the original application being analysed designed these rules'. To support any user of their tools, tool producers/vendors should be clear as to what their tool does and how it does it. All DF tools have a 'scope of performance' which denotes what a tool can do, and the boundaries in which a tool can be used safely (Cohen, 2010) (see Fig. 3). The challenge for DF practitioners often lies with reliably determining the remit of this scope, as it may not always be stated in detail (Marshall, 2010; Vincze, 2016). When a tool is used within the scope of performance, tool-users should be able to rely upon the results it generates (emphasis should be placed on 'should', where independent tool evaluation is still encouraged). In DF, a tool-error occurs when a tool is performing a task which is within its scope of performance, the tool is used to perform the task in a way that is approved by the producer/vendor and the results it produces are established as being 'incorrect'. Any tool that is used to conduct tasks that are outside of its stated scope of performance cannot be held responsible for any results that it generates that are found to be subsequently incorrect.

The vendor/producer of any tool is responsible for defining a scope of performance for their products. This should outline what their tool can do and the conditions and variables that they have validated as needing to be met in order for the tool to perform as they intended. Whilst it would also be helpful for vendors/producers to outline what their tool can't do (within reason, or to prevent foreseeable confusion/misinterpretation of any of the tools functionality), this is often not explicitly addressed.

Those using DF tools must remember that it is a tool's vendor/producer that determines what their tool's scope of performance is, and tool-users should refer directly to any instructional information that is provided. Whilst a tool-user may make assumptions in regard to what they think a tool should do (particularly if any instructions describing

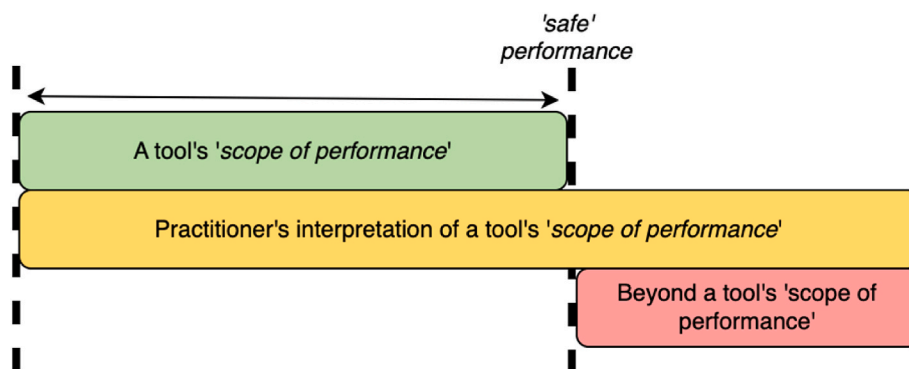


Fig. 3. A tool's 'scope of performance'.

the extent of a tool's functionalities lacks detail), caution should be exercised. If a user believes a tool is capable of something it cannot do - they interpret the tool's scope of performance as being wider than it actually is, then its performance cannot be guaranteed.

To provide an example, consider a tool which claims to recover deleted picture files from storage media. In order to determine whether the tool is performing accurately, users need to know how the file recovery algorithm operates (its safe operational parameters), how to deploy it, and the conditions required for its performance to be as the producer/vendor intended it to be. Only once this information is known are those using the tool able to begin to understand if the tool performs accurately, or erroneously. To expand on this illustration, let's assume that the aforementioned tool is used to recover files from a device that is known to contain 100 deleted picture files, however the tool only recovers 10 of these files having been deployed in a way that is approved by the vendor/producer. Immediate thoughts may be that the tool has performed erroneously, however, determining this will depend on how the tool's scope of performance has been defined. In an extreme example, let's assume that a tool's scope of performance is silent in regards to the type of picture files it can recover, where the remaining 90 unrecovered files are a different type of picture file to the 10 that the tool has recovered. In this simplified scenario, it may be possible to make a case both for, and against, the occurrence of a tool error, depending on how the tool's scope of performance is interpreted.

6.1.1. Interpreting a tool's scope of performance

If the tool's scope of performance is defined vaguely, then the tool's functionality may be interpreted widely by a tool user. In the case noted above in Section 6.1, the failure of the tool to recover the remaining 90 pictures could be considered to be a tool error. This is considered here as an approach of 'strict interpretation' meaning tools are held liable for any failures in performance that can be interpreted as reasonably falling within the boundaries of any vague description of their tool's scope of performance that they provide. Here, where a scope of performance suggests a tool can recover 'picture files', this could be interpreted to mean all types of picture file formats, placing this functionality burden onto the tool. There are clear issues with the strict interpretative approach as it places a significant responsibility onto the tool producer/vendor, which in reality is likely unjust and unreasonable.

Conversely, where a vague scope of performance is provided, a user can opt to interpret it tentatively, meaning that only explicitly stated and described functionality can be relied upon, and the inner-workings of any tool's functionality cannot be assumed. A tool user may subsequently take on the task of determining the tool's scope of remit themselves by conducting a series of functionality tests. Taking a tentative interpretative approach, in our example, without more details of the picture recovery function and was intended to operate it cannot be assumed that the tool should have recovered the remaining 90 files. In this position, it would not be possible to determine with certainty that a tool error has occurred, where instead the 90 files may be of a type where

their recovery is beyond what the tool was intended to be capable of.

6.2. Using the tool correctly

DF tools are complex, often with a large number of configurable options. Such tools often require a user to be trained in their use as misconfiguration can impact the shape and size of any results a tool provides. The responsibility for using a DF tool correctly is joint; a practitioner must deploy a tool properly (Lyle, 2010), in the conditions that it was intended to operate and whilst configuring it appropriately. However, this can only be done if a tool's producer/vendor has provided detailed instructions which define how their tool should be configured to perform within its defined scope of performance.

An absence of operational instructions may lead to a tool being misconfigured or used in a way that generates results that either.

- Appear incorrect as they did not match what the tool user expected to see. Yet the results are in fact correct for the configuration used, however this did not match what the user intended the tool to do.
- Appear correct, but the configuration used has had an impact on the overall results provided (for example, the scope of a search function has been restricted, resulting in missed instances of strings which would have been flagged if the tool was configured correctly).

It is worth restating at this point that tool errors can only occur when a tool is operating in a way that is approved by the vendor/provider for any given task. Misconfigured tools are often the result of user error, unless mistakes in any tool's instructions are present. Similar to the issues noted above, where a tool's usage instructions (or training packages) are ambiguous, users may be forced to decide how any tool should be deployed themselves. This arguably makes it harder to distinguish the difference between a tool-error and user error, should any tool's results be called into question.

6.3. Establishing failed performance

If a user has correctly utilised a tool to conduct a task that is within its stated remit and it has subsequently produced questionable results, then the accuracy of these results must be evaluated. Determining whether any results are erroneous requires first knowing what the accepted truth for a given task is, however, in many DF cases, establishing this truth value may not be obvious or easy to do. In some cases, erroneous responses may be obvious to a practitioner or error messages may be generated by the tool itself (Kumari and Mohapatra, 2016). Yet in some cases, a tool may provide a response for a given task that looks right, but is in fact not correct, making error detection difficult. Often, in these instances the error will concern the quantity of results being provided by a tool (e.g. presenting the user with the right number of recovered files or parsed records) where only a subset of information may be offered and relevant data has been missed. Practitioners rely on their tools to sift

and search large amounts of data as it is impractical to conduct this task manually. Results that are erroneous in terms of quantity are difficult to detect, and emphasis is placed upon the need to evaluate tools prior to them being used in live circumstances in order to instill confidence in their operation. To add complexity to this situation, any source-data being examined may itself contain errors that when processed by a tool, questionable-looking results are generated. These situations may create the look of a tool error, but providing the data has been processed in line with the tool's specification, not a tool error. To provide some context, consider the example provided by Lyle (2010, p.137) who states that 'the presence of a faulty sector is not an error made by the tool, but it might or might not be considered an error as far as the imaging process is concerned.'

When developing any DF tool, its producers/vendors will have tested and evaluated its performance against a finite set of test data, likely synthetically generated in nature. It is hoped and assumed that this process is robust, however, once the tool is actively used in industry, it will likely be exposed to scenarios not seen during its development process. In these cases a discrepancy may occur between the performance expected of a tool by its producer/vendor and that seen by the user, and the reliability of a tool may begin to be questioned.

This is perhaps where producers/vendors must try to support their tool's users by being explicit in terms of what their tool can and cannot do and the remit of their testing in order to define the limits of their tool's capability. Whilst it is recognised that defining this information can be a burden for producers/vendors, the benefits of a full and transparent statement regarding a tool's capability is important to both them and the DF field. This information would support tool evaluation by users having a greater understanding of the tool's operating conditions and therefore arguably increasing the robustness of the evaluation process. Currently, tool evaluation requires tool users and their organisations to construct complex test scenarios and ground truth dataset in order to try and determine any performance issue. By knowing what the tool's vendor/producer has contracted as acceptable performance, testing can be more targeted and confirmatory in nature. Should any tool-performance issues be raised, such transparency in a tool's capability makes it easier to attribute where fault lies (for example, with the tool, or with the user due to misuse of the tool).

It is also recognised that requesting this level of detail from a tool vendor/provider may stunt tool development due to the need for resources to be invested in fully testing and documenting their tools capability. Put bluntly, tool vendors/providers may simply be put off by this burden and leave the DF market, which can only be seen to have a negative impact on this field. Yet from a quality assurance and error-attribution standpoint, clarity in a tool's capability helps practitioners to identify and distinguish error from merely limitation.

Tool errors can result in data being missed during an investigation or misinterpreted leading to incomplete and inaccurate examinations being undertaken. Errors that occur at a tool level can move up through the investigative chain and directly impact the quality of future investigative steps (Dimpe and Kogeda, 2017). When errors are detected, there is arguably an obligation on the tool vendor/provider to fix them, as performance is not what was contracted for. Given the context of the DF field, errors are of utmost concern and therefore many if not all vendors/producers would endeavour to fix their tools where an error is identified. In contrast, limitations may not carry such an obligation, where producers/vendors may not intend to, or are unable to expand the function of their tool to cover any limitation identified.

7. Methods

At all stages of the DF investigative processes, appropriate methods should be used as part of any work conducted. The Forensic Science Regulator (2020) defines a method as 'a logical sequence of procedures or operations intended to accomplish a defined task. A method includes the interaction of the operator and may include multiple tools or none'.

Methods can have both technical and non-technical components, and may encompass the use of a tool (Marshall and Paige, 2018) or a tool may incorporate a number of methods (Brunty, 2023). In some cases, a method may be a series of steps undertaken by an individual, in absence of a DF tool. All experts using methods in DF are under an obligation to ensure they are valid, where for example in England and Wales, this is enforced within the Criminal Practice Directions 2023 and by the Forensic Science Regulator (2020).

Technical methods are utilised across the investigative process for identifying, collecting, acquiring and investigating, and presenting digital data. However, in addition we may see formalised non-technical methods which are deployed for tasks such as the identification of client requirements (for example, Cook et al.'s., 1998 case assessment and interpretation approach) or for the peer review of any work conducted. Effective methods when followed properly should provide a systematic and consistent way of achieving a task or goal satisfactorily. Such methods could support the making of strategic decisions or to ensure a robust evaluation of available case information is undertaken. Alternatively, a method may outline a series of steps required for such technical tasks as acquiring data from a digital device in a way that preserves its integrity (Forensic Science Regulator, 2020). Any results obtained during the course of an investigation must be repeatable and reproducible (Hughes and Karabiyik, 2020; Brunty, 2023), meaning any methods used must be robust. Under accreditation schemes such as ISO17025, methods must be shown to be 'fit for the specific purpose intended', where method validation is a core quality assurance task that practitioners and their organisations must engage with (Forensic Science Regulator, 2020).

In relation to errors involving methods, the following scenarios are presented.

1. *The wrong method is used:* At any point in the DF investigative process, the wrong method could be chosen for a given task and subsequently used. This work does not consider this to be a method error - rather an error attributable to the method-deployer. In these cases, responsibility for deploying any method which leads to an error lies with those who made the decision to deploy it. This may be the practitioner, or such decisions may sit at an organisational level where a method has been designated for use in circumstances that are ultimately not suitable. Methods have a defined purpose and scope of use, and similar to those issues detailed in 'Section 6 Tool Error', use of methods in circumstances beyond their scope are not method errors, rather user error.
2. *The method is wrong:* All methods are designed to meet a defined set of requirements that allows them to complete a task. Methods should be meticulously designed, subject to peer review and carry evidence of their validation. If a method when used as it was intended to be used results in an error, the method is wrong. Technically the method is at fault and the source of an error, however, methods are often designed by practitioners and organisations, therefore when attributing such an error, in reality a flaw in the methods development and validation processes must have been present. These are a fault of the method developer. It should be recognised that methods can become incorrect over time as any target of them changes. In addition, any method may be accepted as valid, only for future work to determine method flaws.
3. *The method is deployed incorrectly:* Where a method is used in the wrong conditions or not deployed in the way that it was intended, these are method-implementation errors and a fault of those deploying the method. Similar to tools, methods must be used as they were intended to be used, following any instructions defined by the method creator.

Methods are not living, breathing things, and therefore they cannot realistically be responsible for an error, although they may cause one. Methods are a collection of instructions, created by a human, and

therefore method errors are ultimately errors that originate from their creator.

8. Practitioner error

Practitioners may be involved at all stages of an investigation, either technically, as part of decision support or during the development of an investigative strategy, and therefore errors made by practitioners have the potential to impact the entirety of the investigative process. Whilst they are relied upon to make good investigative decisions, errors will happen (Horsman, 2019b), and these could be at any point during their work. DF practitioners are human, and just as human error occurs in normal life events, it can also occur in the forensic process (Budowle et al., 2009; Erbacher, 2010; Sunde and Dror, 2021). Such errors ‘may be random or systematic, may be related to negligence or incompetence, and is, for the most part, unintentional and unquantifiable’ (Christensen et al., 2014 p.124). Whilst deliberate error on the part of the practitioner is possible, it is hoped that such instances are rare, but certainly not unheard of and must be considered (Morgan, 2023) (see National Registry of Exonerations, 2020).

When discussing the practitioner as a source of error, it is suggested that the following types exist.

1. *Tool use*: In section 2, the specifics of ‘tool error’ have been defined, where a ‘tool use’ error must be distinguished. A practitioner may commit a tool use error when:-
 - a. Selecting/deploying a tool in circumstances where it should not be used. This may be when any case circumstances dictate that it is not appropriate for the tool to be used, or that the tool is deployed in a scenario that requires it to operate beyond its scope of performance (Horsman, 2018).
 - b. Misconfiguring a tool which results in any functionality performed not being appropriate for the task being undertaken (Horsman, 2018).

Depending on the stage of an investigation where a tool use error occurs, they may result in data failing to be acquired from a device, data being missed during any data processing stages, or, the misrepresentation and subsequent presentation of data which may compromise any interpretation of a trace by a practitioner.

2. *Method choice*: A practitioner may choose a method that is not suitable for a given task (‘using the wrong method’), leading to the occurrence of error.
3. *Method deployment*: A practitioner may deploy a correctly chosen method, incorrectly (in whole or part), leading to error.
4. *Method development*: A practitioner may be responsible for the production of a method that is not fit for purpose, and when used it leads to error.
5. *Misinterpretation*: A fundamental part of a practitioner’s workload involves interpretation, and interpretative errors can occur in the following ways -
 - a. *Misinterpretation of case requirements*: A practitioner may misinterpret the investigative requirements of their client and therefore pursue a course of conduct which results in error.
 - b. *Misinterpretation of capability*: A practitioner may misinterpret the capability of any investigative methods and tools that they have available, which may result in a limited or flawed examination of data.
 - c. *Misinterpretation of results*: A practitioner may use methods and tools to access, sort and sift data, at which point potentially relevant subsets of information may be observed. The meaning and importance of these traces may be misinterpreted (Budowle et al., 2009; Cohen, 2010), in essence, they may reach the wrong conclusion (Triplett and Schade, 2012).

6. *Missing relevant content*: A practitioner may fail to address traces that are present within and relevant to their case.
7. *Communication errors*: Whilst a practitioner may possess results that are not erroneous, they may fail to communicate those results to any client accurately.

In regard to the above categories of error, and whilst this paper focuses on sources rather than causes factors (see Fig. 1), it feels appropriate to acknowledge that there may be any number of causal factors including:-

1. *Biases*: Practitioners may make errors due to bias (Edmond et al., 2017; Sunde and Dror, 2019).
2. *Incompetence*: A practitioner may have an inability to conduct a given task successfully. This may occur due to a lack of knowledge or understanding in regard to a given task.
3. *Negligence*: Errors may occur through a failure to take due care during any investigative tasks.
4. *Malice*: Practitioners may cause errors through deliberate bad practice.
5. *Stress* (Jeanguenat and Dror, 2018).
6. *Lack of knowledge*: Practitioners may not have the knowledge required to complete a task which ultimately leads to the cause of an error. This may be due to a lack of training or experience.
7. *Workload*: Case backlogs are often reported in the field of DF (Kao et al., 2020) and when coupled with the increasing need and demand for DF examinations, overworked practitioners are more prone to error.

Practitioner errors can be reduced through appropriate ‘quality assurance systems, training, proficiency testing, peer review, and adhering to validated protocols and discipline best practices’ (Christensen et al., 2014 p.124). In addition, practitioners must continuously strive to improve and validate their own practices, and hold themselves to account with regard to their ability to conduct their forensic work.

9. Trace error

All DF examinations set out to determine the presence and meaning of any relevant digital traces. Practitioners will deploy methods that allow them to try and understand what any trace means in the context of their inquiry and whether it is of evidential relevance. Whilst sections 4-8 have highlighted potential sources of error concerned with the investigative process, trace-errors should also be considered. A trace error occurs when a digital trace incorrectly represents the event it intended to describe. To provide context to this, consider an example where a digital trace is created on a system and its accompanying creation timestamp does not reflect the actual time and date of its creation event. Alternatively, location information may not correlate accurately with the physical position that any location information intended to describe. Practitioners cannot assume that all traces have resulted from correctly performing services and systems and accurately reflect the state of an event. van Zandwijk and Boztas’s (2019) study of traces from the iPhone Health App contextualise the need to determine the reliability of any trace itself.

A practitioner may identify appropriate methods and tools that are functioning correctly as part of their investigation. However, the target of their methods and tools - ‘the trace’, may be fundamentally erroneous and in some cases, trace-errors may be difficult for practitioners to detect. In some cases, when an erroneous trace is analysed, the outcome may be of such an unexpected nature that a practitioner may raise concerns and subsequently go on to conduct further tests and detect such a trace-error. In other cases, a trace error may be more subtle in nature, for example if a timestamp was incorrect by 1 h. Detecting trace errors often requires the production and study of ground truth data which describes the behaviour of any service responsible for the creation of the

trace.

Trace errors may occur at the stages of an investigation which focus on identifying and understanding traces - Data Processing/Examination, Analysis, Interpretation and Evaluation, Presentation of Findings for Peer Review and Presentation/Communication of Results. Erroneous traces may lead to the following errors.

- *Missed data*: Erroneous traces may have a structure that ultimately means any tools and methods may fail to identify them (resulting in them being missed during an examination).
- *Misrepresentation*: Erroneous traces may be parsed and displayed incorrectly impacting any subsequent review of them by a practitioner.
- *Misinterpretation*: Erroneous traces may cause a practitioner to misinterpret case related events.

Trace errors have the potential to compromise the value of any digital investigation as any results provided may not be trustworthy.

10. Conclusions

This work has discussed six sources of error and mapped them to the 10 stages of the DF investigative process. The need to understand, identify and attribute errors for the purposes of quality control and assurance has been stressed given that errors are inevitable in practice and their impact can be severe. Errors may not just impact a single stage of the investigative process, and instead, a single error may go on to undermine the reliability and accuracy of the entirety of an investigation. DF organisations and their practitioners should prepare for error in their practice, and design processes that actively look to detect them. By aligning error sources to investigative stages, it is hoped this work begins to map 'error' within the DF process and help make their detection easier, and identify areas that require bolstering.

Understanding error in DF is a continuing process and whilst it is hoped this work provides a foundation to build from, it is recognised that continuous review and evaluation must take place. As the field develops, new sources of error may materialise and their impact will require appraisal. This will be a resource intensive practice, but given the potential implications of error it is argued as one that is worth doing.

Declaration of competing interest

The author has no conflicts to declare.

Data availability

No data was used for the research described in the article.

References

- Arshad, H., Jantan, A.B., Abiodun, O.I., 2018. Digital forensics: review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems* 14 (2).
- Baggili, I.M., Mislan, R., Rogers, M., 2007. Mobile phone forensics tool testing: a database driven approach. *International Journal of Digital Evidence* 6 (2), 168–178.
- Barlow, R., 2002. Systematic Errors: Facts and Fictions arXiv preprint hep-ex/0207026.
- Beckett, J., Slay, J., 2007. Digital forensics: validation and verification in a dynamic work environment. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE, 266a–266a.
- Bruntz, J., 2023. Validation of forensic tools and methods: a primer for the digital forensics examiner. *Wiley Interdisciplinary Reviews: Forensic Sci.* 5 (2), e1474.
- Budowle, B., Bottrell, M.C., Bunch, S.G., Fram, R., Harrison, D., Meagher, S., Oien, C.T., Peterson, P.E., Seiger, D.P., Smith, M.B., Smrz, M.A., 2009. A perspective on errors, bias, and interpretation in the forensic sciences and direction for continuing advancement. *J. Forensic Sci.* 54 (4), 798–809.
- Carrier, B., 2002. Open Source Digital Forensics Tools: the Legal Argument.
- Carrier, B., 2003. Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of digital evidence* 1 (4), 1–12.
- Casey, E., 2002. Error, uncertainty and loss in digital evidence. *International Journal of Digital Evidence* 1 (2).
- Casey, E., 2009. *Handbook of Digital Forensics and Investigation*. Academic Press.
- Casey, E., 2019. The chequered past and risky future of digital forensics. *Aust. J. Forensic Sci.* 51 (6), 649–664.
- Center for Chemical Process Safety, n.d. Causal Factor (CF). Available at: <https://www.aiche.org/ccps/resources/glossary/process-safety-glossary/causal-factor-cf>.
- 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.
- Cohen, F., 2010. Toward a science of digital forensic evidence examination. In: *Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics*, Hong Kong, China, vol. 6. Springer Berlin Heidelberg, pp. 17–35. January 4–6, 2010, Revised Selected Papers.
- Cole, Kelly A., Gupta, Shruti, Gurugubelli, Dheeraj, Rogers, Marcus K., 2015. A review of recent case law related to digital forensics: the current issues. In: *Annual ADFSL Conference on Digital Forensics, Security and Law*. 2.
- Committee on Identifying the Needs of the Forensic Sciences Community National Research Council, 2009. 'Strengthening Forensic Science in the United States: A Path Forward'. <https://www.ojp.gov/pdffiles1/nij/grants/228091.pdf>.
- Cook, R., Evett, I.W., Jackson, G., Jones, P.J., Lambert, J.A., 1998. A model for case assessment and interpretation. *Sci. Justice* 38 (3), 151–156.
- Dictionary.com, 2022. 'Error' Available at: <https://www.dictionary.com/browse/error?s=t>. (Accessed 14 August 2022).
- Dimpe, P.M., Kogeda, O.P., 2017. Impact of using unreliable digital forensic tools. *Proceedings of the World Congress on Engineering and Computer Science* 1, 118–225.
- Dioso-Villa, R., 2015. A repository of wrongful convictions in Australia: first steps toward estimating prevalence and causal contributing factors. *Flinders Law Journal* 17 (2), 163–202.
- Du, M., 2017. Analysis of errors in forensic science. *Journal of Forensic Science and Medicine* 3 (3), 139–143.
- Earwaker, H., Nakhaeizadeh, S., Smit, N.M., Morgan, R.M., 2020. A cultural change to enable improved decision-making in forensic science: a six phased approach. *Sci. Justice* 60 (1), 9–19.
- Edmond, G., Towler, A., Grown, B., Ribeiro, G., Found, B., White, D., Ballantyne, K., Searston, R.A., Thompson, M.B., Tangen, J.M., Kemp, R.I., 2017. Thinking forensics: cognitive science for forensic practitioners. *Sci. Justice* 57 (2), 144–154.
- Einhorn, H.J., 1986. Accepting error to make less error. *J. Pers. Assess.* 50 (3), 387–395.
- Eldridge, H., Stimac, J., Vanderkolk, J., 2022. The benefits of errors during training. *Forensic Sci. Int.: Synergy* 4, 100207.
- Erbacher, R.F., 2010. Validation for digital forensics. In: *2010 Seventh International Conference on Information Technology: New Generations*. IEEE, pp. 756–761.
- Etter, B., 2013. The contribution of forensic science to miscarriage of justice cases. *Aust. J. Forensic Sci.* 45 (4), 368–380.
- Flandrin, F., Buchanan, W.J., Macfarlane, R., Ramsay, B., Smales, A., 2014. Evaluating Digital Forensic Tools (DFTs).
- Forensic Science Regulator, 2020. Method validation in digital forensics FSR-G-218. https://assets.publishing.service.gov.uk/media/5f6ca608d3bf7f7231ac65e0/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf.
- Garfinkel, S.L., 2010. Digital forensics research: the next 10 years. *Digit. Invest.* 7, S64–S73.
- Gill, P., 2018. DNA evidence and miscarriages of justice. *Forensic Sci. Int.* 294, e1–e3.
- Horsman, G., 2018. "I couldn't find it your honour, it mustn't be there!"—Tool errors, tool limitations and user error in digital forensics. *Sci. Justice* 58 (6), 433–440.
- Horsman, G., 2019. Tool testing and reliability issues in the field of digital forensics. *Digit. Invest.* 28, 163–175.
- Horsman, G., 2019b. Formalising investigative decision making in digital forensics: proposing the digital evidence reporting and decision support (DERDS) framework. *Digit. Invest.* 28, 146–151.
- Horsman, G., 2021. Digital evidence and the crime scene. *Sci. Justice* 61 (6), 761–770.
- Horsman, G., 2021b. The COLLECTORS ranking scale for 'at-scene' digital device triage. *J. Forensic Sci.* 66 (1), 179–189.
- Horsman, G., 2022. Digital Evidence Strategies for Digital Forensic Science Examinations. *Science & Justice*.
- Horsman, G., 2023. The Importance of Digital Evidence Strategies. *Wiley Interdisciplinary Reviews: Forensic Science*, p. e1507.
- Horsman, G., Lyle, J.R., 2021. Dataset construction challenges for digital forensics. *Forensic Sci. Int.: Digit. Invest.* 38, 301264.
- Horsman, G., Sunde, N., 2020. Part 1: the need for peer review in digital forensics. *Forensic Sci. Int.: Digit. Invest.* 35, 301062.
- Horsman, G., Sunde, N., 2022. Unboxing the digital forensic investigation process. *Sci. Justice* 62 (2), 171–180.
- Huang, Y., Pei, J., Nielsen, P.V., Bonhoux, F., Lechene, S., Keller, F.X., Wu, S., Xu, C., Cao, Z., 2021. Experimental techniques. In: *Industrial Ventilation Design Guidebook*. Academic Press, pp. 185–277.
- Hughes, N., Karabiyik, U., 2020. Towards reliable digital forensics investigations through measurement science. *Wiley Interdisciplinary Reviews: Forensic Sci.* 2 (4), e1367.
- Hughes, N., Ziemak, E., Martinez, C., Stout, P., 2022. Toward a cost-benefit analysis of quality programs in digital forensic laboratories in the United States. *Wiley Interdisciplinary Reviews: Forensic Sci.* 4 (1), e1422.
- Jeanguenat, A.M., Dror, I.E., 2018. Human factors affecting forensic decision making: workplace stress and well-being. *J. Forensic Sci.* 63 (1), 258–261.
- Jones, A., Vidalis, S., 2019. Rethinking digital forensics. In: *Annals of Emerging Technologies in Computing (AETiC)*. Print ISSN, 2516-0281.
- Kao, D.Y., Wu, N.C., Tsai, F., 2020. A triage triangle strategy for law enforcement to reduce digital forensic backlogs. In: *2020 22nd International Conference on Advanced Communication Technology (ICACT)*. IEEE, pp. 1173–1179.
- Kaplan, J., Ling, S., Cuellar, M., 2020. Public beliefs about the accuracy and importance of forensic evidence in the United States. *Sci. Justice* 60 (3), 263–272.

- Keyence, n.d. Types of Error. Available at: <https://www.keyence.com/ss/products/measurement-selection/basic/error.jsp>.
- Kloosterman, A., Sjerps, M., Quak, A., 2014. Error rates in forensic DNA analysis: definition, numbers, impact and communication. *Forensic Sci. Int.: Genetics* 12, 77–85.
- Kryeziu, L., 2015. Learning from errors. *ILIRIA International Review* 5 (1), 391–408.
- Kumari, N., Mohapatra, A.K., 2016. An insight into digital forensics branches and tools. In: 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). IEEE, pp. 243–250.
- Lyle, J.R., 2010. If error rate is such a simple concept, why don't I have one for my forensic tool yet? *Digit. Invest.* 7, S135–S139.
- Marshall, A.M., 2010. Quality standards and regulation: challenges for digital forensics. *Measurement and Control* 43 (8), 243–247.
- Marshall, A.M., Paige, R., 2018. Requirements in digital forensics method definition: observations from a UK study. *Digit. Invest.* 27, 23–29.
- Mayo, D.G., 1996. *Error and the Growth of Experimental Knowledge*. University of Chicago Press.
- McKemmish, R., 2008. *When Is Digital Evidence Forensically Sound?* Springer US, pp. 3–15.
- Meixner, J.B., Diamond, S.S., 2014. The hidden Daubert factor: how judges use error rates in assessing scientific evidence. *Wis. Law Rev.* 1063.
- Mera, Y., Rodríguez, G., Marin-Garcia, E., 2022. Unraveling the benefits of experiencing errors during learning: definition, modulating factors, and explanatory theories. *Psychonomic Bull. Rev.* 1–13.
- Metcalfe, J., 2017. Learning from errors. *Annu. Rev. Psychol.* 68, 465–489.
- Miller, C.M., 2023. A survey of prosecutors and investigators using digital evidence: a starting point. *Forensic Sci. Int.: Synergy* 6, 100296.
- Morgan, J., 2023. Wrongful convictions and claims of false or misleading forensic evidence. *J. Forensic Sci.* 68 (3), 908–961.
- 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.
- Nassaji, H., 2018. Errors versus Mistakes. *The TESOL Encyclopedia of English Language Teaching*, pp. 1–5.
- National Police Chiefs Council, 2020. *Digital forensic science strategy*. <https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf>.
- National Registry of Exonerations 2019 annual report. https://www.law.umich.edu/special/exoneration/Documents/Exonerations_in_2019.pdf, 2020–. (Accessed 3 February 2023).
- Neale, C., Kennedy, I., Price, B., Yu, Y., Nuseibeh, B., 2022. The case for zero trust digital forensics. *Forensic Sci. Int.: Digit. Invest.* 40, 301352.
- Overbye, K., Bøen, R., Huster, R.J., Tamnes, C.K., 2020. Learning from mistakes: how does the brain handle errors?. In: *Everything You and Your Teachers Need to Know about the Learning Brain*, p. 20.
- Oxford English Dictionary, 2023. 'error' Available at: <https://www.oed.com/search/dictionary/?scope=Entries&q=error>. (Accessed 4 August 2023).
- Oxford Languages, 2023. *Random error*. <https://languages.oup.com/google-dictionary-en/>.
- Pan, L., Batten, L.M., 2009. Robust performance testing for digital forensic tools. *Digit. Invest.* 6 (1–2), 71–81.
- Reedy, P., 2021. The risks for digital evidence. In: *Strategic Leadership in Digital Evidence*, p. 71.
- Robertson, J., 2013. Understanding how forensic science may contribute to miscarriages of justice. *Aust. J. Forensic Sci.* 45 (2), 109–112.
- Schickore, J., 2005. 'Through thousands of errors we reach the truth'—but how? On the epistemic roles of error in scientific practice. *Stud. Hist. Philos. Sci.* 36 (3), 539–556.
- Schiffer, B., 2009. *The Relationship between Forensic Science and Judicial Error: a Study Covering Error Sources, Bias, and Remedies*. Université de Lausanne, Faculté de droit et des sciences criminelles.
- Sunde, N., 2017. *Non-technical Sources of Errors when Handling Digital Evidence within a Criminal Investigation* (Master's Thesis, Politihøgskolen and NTNU. Faculty of Technology and Electrical Engineering, Department of Information Security and Communication Technology).
- Sunde, N., 2022. Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations. *Forensic Sci. Int.: Digit. Invest.* 40, 301317.
- Sunde, N., Dror, I.E., 2019. Cognitive and human factors in digital forensics: problems, challenges, and the way forward. *Digit. Invest.* 29, 101–108.
- Sunde, N., Dror, I.E., 2021. A hierarchy of expert performance (HEP) applied to digital forensics: reliability and biasability in digital forensics decision making. *Forensic Sci. Int.: Digit. Invest.* 37, 301175.
- SWGDE, 2018. *Establishing confidence in digital and multimedia evidence forensic results by error mitigation analysis*. Available at: https://drive.google.com/file/d/1jBAJohuntNCLUzgV_x7aINf_JycfVddu/view.
- Triplett, Michele, Schade, William, 2012. *Practitioner error vs. Deficient procedures*. Available at: <https://prints.nwlean.net/PractitionerError.pdf>.
- Tulis, M., Steuer, G., Dresel, M., 2016. Learning from errors: a model of individual processes. *Frontline Learning Research* 4 (2), 12–26.
- Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R., Watson, T., 2020. Quality standards for digital forensics: learning from experience in England & Wales. *Forensic Sci. Int.: Digit. Invest.* 32, 200905.
- 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. Invest.* 28, S126–S133.
- Vincze, E.A., 2016. Challenges in digital forensics. *Police Pract. Res.* 17 (2), 183–194.
- Vosk, T., Imwinkelried, E.J., 2017. *Forensic Science: Measurements in Forensic Science—Of Errors and Uncertainty*.
- White, P. (Ed.), 2010. *Crime Scene to Court: the Essentials of Forensic Science*. Royal society of chemistry.



DSPACE

<https://dspace.org/>

Sources of error in digital forensics

Horsman, Graeme

2024-02-09

Elsevier

<https://doi.org/10.1016/j.fsidi.2024.301693>

Horsman G. (2024) Sources of error in digital forensics. Forensic Science International: Digital Investigation, Volume 48, March 2024, Article number 301693