Science & Justice, Volume 64, Issue 1, January 2024, pp. 38-42
DOI:10.1016/j.scijus.2023.11.007

Interpreting digital traces:- 8 foundational pillars to support the formation of opinion in digital forensics

Graeme Horsman

Abstract

The field of digital forensics (DF) is facing increasing scrutiny of the quality of the work it produces. Fundamental to it is the need for its practitioners to be able to accurately determine the meaning of potentially relevant digital traces found during an examination of a device. As the reliance on digital evidence continues to grow, so does the importance of digital trace-interpretation. It is therefore imperative that this task is conducted robustly, where this work describes 'eight pillars' that should underpin how a practitioner has gone about interpreting any given digital trace.

Keywords: Digital Forensics; Digital Trace; Investigation; Interpretation.

1 Introduction

As part of any digital forensic (DF) investigation, practitioners will identify digital traces that must have their meaning interpreted [1; 2]. This often involves determining what a trace is, as well as identifying any actions which may have led to it being present on a device or system [2]. The complexity involved in conducting this work can vary, where in some cases this task may be straightforward if a digital trace is of a type that the DF community considers itself to reliably understand, and any given assessment of its meaning is thought to be accepted. However, there are instances where a trace is encountered and its meaning may remain the subject of debate or, it has not yet been established. In these cases, practitioners will be required to conduct additional exploratory and interpretive work [5]. In both instances, whenever the meaning of any given trace is offered by an investigating DF practitioner (their 'opinion' of what it is, and the circumstances surrounding its presence), it must be accurate. This requires it to have been achieved through robust and effective investigative and interpretive practices if it is to be relied upon by all those parties involved in the wider investigative process [3]. These practices should also be transparent to, and understood by all those seeking to rely on any trace-interpretation provided, and to facilitate the appraisal of any interpretive work conducted. Whilst it could be argued that the field of DF is behind the curve in terms of formalising the processes that underpin digital trace interpretation, existing interpretive principles from broader forensic science disciplines can be looked to for support. In particular, guidance from the Forensic Science Regulator [8] in England and Wales, National Institute of Forensic Science Australia New Zealand [9], The European Network of Forensic Science Institutes [10] and the Association of Forensic Science Providers [11] is of value.

Determining the meaning of any digital trace is a complex and multifaceted task, where to support those conducting this work, a 'pillared' framework for practitioners to utilise, support and demonstrate the quality of their interpretive work is offered. It is suggested that any opinion formed by a practitioner with regard to the significance of a digital trace can and should be underpinned with evidence that their practice addresses and conforms to eight interpretative 'pillars', notably - *'mode of interpretation', 'trace generation', 'trace creation assessment', 'repeatability', 'validation', 'transparency', 'acceptance' and 'competence'*. It is argued that any robust and accurate interpretive process must show alignment to these foundational pillars in

order to illustrate that reliable digital trace-interpretation processes have taken place. Conducting trace-interpretation in line with the proposed eight pillars gives structure, transparency and clarity to a practitioner's interpretive process, and each of the eight pillars and this approach are discussed below.

2 Meaning

Establishing the meaning of digital traces is a fundamental role of any DF practitioner and their interpretations of traces often form the core of their work. When providing what they believe to be the meaning of any potentially relevant digital traces, practitioners are in many cases doing this via event reconstruction techniques [6] and are seeking to address the following two questions.

1. *What is this digital trace?*: This can be a question of 'type', for instance what type of file is '*X*'? Or, what data structure is data '*D*' stored in.

2. *What actions could (or could not) have caused the digital trace to be present on a device/system in its current form?:* Practitioners must try to determine those actions (for example, physical interactions with the device by a user, or autonomous system functionalities etc.) that could, or could not have created or modified any trace in question and why it is there.

Any responses to these two questions will often contribute to addressing wider investigatory queries which may include identifying, understanding and linking suspects to specific actions or behaviours on a device or system. When conducting this work, practitioners must utilise methods that are valid and reliable, and it should be clear as to what work has been done which has allowed them to arrive at their opinion of a trace's meaning. It is suggested that those conducting this task should look to structure their interpretive process around eight 'pillars for trace interpretation' in order to demonstrate its quality.

2.1 Underpinning meaning: '*eight pillars of evidence*'

A digital trace's meaning should be formed via a set of methodical and robust investigative and interpretative processes. These must not be deployed inconsistently or be *ad hoc* in structure, instead it is suggested that they should be built around the following eight core pillars of trace-interpretation - 'mode of interpretation', '*trace generation', 'trace creation assessment', 'repeatability', 'validation', 'transparency*', '*acceptance*' and *'competence*' (see Figure 1). For every interpretation of a trace provided by a practitioner, their underpinning interpretive processes must show compliance with each of the aforementioned eight pillars and provide confirmation as to how this has been done.

Together, these pillars form foundational components that are required of a practitioner when they are determining and subsequently proposing an opinion with regard to the meaning of a digital trace. This structured approach helps to facilitate procedural transparency, and facilitates scrutiny of their work for the purposes of quality control and assurance. Each of these pillars are discussed in turn, starting with '*Mode of Interpretation*'.

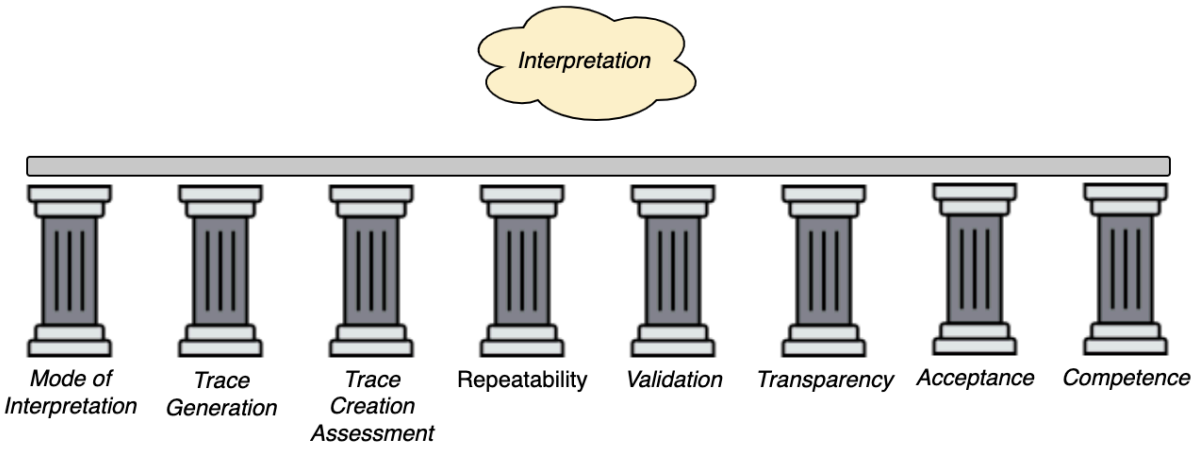

Figure 1: The eight pillars underpinning the interpretation of a digital trace.

2.2 Pillar 1: - Mode of Interpretation

When practitioners convey their opinion concerning the meaning of any trace, they must be clear as to how they have managed and expressed any level of uncertainty in regard to it. This is to prevent any recipient of it (or even the practitioner themselves) from being misled, and to reduce the chance of, or ideally stop it from being misinterpreted. When determining a trace's meaning, any interpretation offered may be expressed as an evaluative or investigative opinion depending on the 'mode' that a practitioner is tasked with operating in. An evaluative opinion is defined as 'an opinion of evidential weight (evaluation of a likelihood ratio), based upon case specific propositions and clear conditioning information' [8]. Any 'interpretation of evidence takes place within a framework of circumstances', at least ' two competing, mutually exclusive propositions' and it is 'the probability of the evidence given each of the stated propositions' that is considered [8; 15]. This opinion must then be formed upon the four principles of balance, logic, robustness and transparency [11], considered cornerstones of sound opinion, and each requires further elaboration (see work by the Association of Forensic Science Providers [11] and the Forensic Science Regulator [8] for a more detailed discussion).

When forming an opinion, it is crucial for it to be impartial and equitable. This means it is one that acknowledges the position of both the prosecution and defence [8, 11], and considers at least one appropriate pair of propositions [8] - this is a *balanced* approach. A *logical* approach ensures that an opinion, and any uncertainty surrounding it has been formed using a robust and valid framework of reasoning, and one that prevents 'illegitimately transposing the conditional' [8, 21]. The Association of Forensic Science Providers [11] provides an accessible example of this, stating that an 'expert will address the probability of the evidence given the proposition and relevant background information and not the probability of the proposition given the evidence and background information'. A *robust* opinion is one that can withstand scrutiny, having been based upon sound knowledge, derived from the use of valid methods and where necessary and appropriate, supported by accurate and representative datasets [8, 11]. Finally, there must be *transparency* in regard to how any practitioner has formed their opinions, the processes utilised, any key impactful metrics observed, and any data or knowledge they have sought to rely upon [8, 11].

It is suggested that in many cases, practitioners will more often express their interpretation of a digital trace as an investigative opinion; an 'explanation generated to account for observations' [11]. These observations may be derived from any testing they have conducted. In some cases, these explanations can be ranked 'using estimates of probabilities based upon the knowledge and experience of the expert and taking into account all uncertainties relating to the observations and the framework of circumstances' [8]. This work will consider primarily the formation of investigative opinions in relation to digital trace interpretation given their perceived prominence, however, where practitioners are conducting trace interpretation in evaluative mode, references to fundamental evaluative reporting guidance should be sought.

Practitioners must also be aware of the risks posed by the varying forms of bias during the interpretation process [19; 20]. Whilst combating bias is beyond the remit of this paper, practitioners must be aware of its risks and take steps to engage in accepted methods to reduce the risk and impact of it on the forensic interpretative process.

Prior to starting any technical processes involved with interpreting digital traces, a practitioner must understand the interpretative mode that they are required to work within as this will influence the shape, form and requirements of their work, and the structure of any supplied opinion. Trace interpretation approaches such as the Case Assessment and Interpretation model may offer support to practitioners in the DF field when forming their opinions [16], and guidance has also been offered from a number of governing bodies [8, 9, 10, 11].

2.3 Pillar 2:- Trace generation

Under Pillar 2, for any trace identified as requiring interpretation, a practitioner will typically consider and explore any potential origins of it, and those actions/functions that could have led to its creation. Here, it is necessary to draw reference to Cook et al's., [22] 'hierarchy of propositions' which defines three main categories of proposition, and a practitioner may consider addressing any or all in relation to a given trace. A practitioner could be required to form an opinion concerning the origin of a digital trace, effectively where it has come from - this is defined as a 'source-level' proposition. In addition, a practitioner may need to consider those actions and functions that they believe could have possibly led to the creation or modification of a given digital trace - an 'activity-level' proposition. Finally, offence-level propositions concern evidence of the offence. Practitioners are unlikely to operate at an offence-level and therefore limited consideration of this level will be given from here on.

When a digital trace is discovered that a practitioner intends to interpret, it is suggested that they will typically be concerned with addressing source and activity level issues that may be relevant to any current inquiries. Depending on the level of proposition being considered, and should a practitioner be required to operate in evaluative mode, an appropriate pair (or multiple pairs) of propositions considering both defence and prosecution stances should be defined in regard to a trace. If a practitioner is working in investigative mode (or is unable to work evaluatively), they should formulate a list of sources, actions or functions (depending on the proposition level they are interested in) that they have suppose could (and if required, could not) have led to a trace's presence on a device/system in its current form. These may be derived from statements made by alleged suspects, case information or intelligence, or the practitioner's knowledge and past experiences. It is important to acknowledge that any set of explanations for a trace identified by a practitioner may not be exhaustive. Additional possible

sources/actions regarding a trace may exist beyond those that a practitioner has considered, and additional explanations may have been missed. Further it should be stressed that a practitioner must consider both possible sources/actions etc., and sources/actions that may not have generated a trace.

All speculative explanations that a practitioner may have considered for a trace when in investigative mode should be formally documented (to facilitate procedural transparency) and any expectations for subsequent testing be stated [16]. Documenting this information will help to support any future assessment of the reliability of any opinion offered and underpinning interpretive processes [16]. In addition, it may reveal limitations in any work that has been conducted and serve to assist in the development of a risk assessment in regard to any methods used or intended for use, and the need to validate them (see pillar 5).

It is important to maintain transparency in regard to any sources and causal actions/functions considered given that in many scenarios multiple may exist. It is unlikely all those that are identified can be assessed as part of the process of determining the meaning of a trace. Some potential causal actions/functions may not be known to a practitioner, or be of a type where it is considered impractical or infeasible to explore them due to limited time and resources, or that spending such resources in this capacity may be considered unjustified. In most instances any practitioner's opinion of a trace's meaning will not be absolute, instead likely derived from the deliberation of a subset of causal actions/functions that they determine to be the most relevant to consider in the case's circumstances. This subset should be derived from their knowledge, experience, and strategic and sensible decision making which takes into account the availability of any wider investigative intelligence or statements. A practitioner may subjectively order these hypotheses in a way that means they go on to test them in an order they consider to be most likely to have occurred. The extent and boundaries of the subset of causal actions/functions should be defined so that the remit from which a trace's meaning has been derived by a practitioner is clear, and any limitations can be established. In addition, if later in the investigative process subsequent possible causes for the trace are put forward by another, this transparency permits a review of whether the practitioner considered these, and if so, why they may have been disregarded.

2.3 Pillar 3:- Trace Creation Assessment

Any set of potential sources or causal activities/functions identified under Pillar 2 must be assessed in order to determine whether they could generate traces that are comparative to those that are the focus of a practitioner's interpretative work. This requires experimentation, where the impact of each potentially causal action, when observed in an environment that is comparable to the conditions (system/device) that any trace requiring interpretation exists within [23], must be observed and recorded. Here, a practitioner is attempting to identify and define any methods that they can show to be capable of generating a trace that is comparable to the one they are observing in their case work, and any relevant methods which cannot do this [4]. If a method can be shown to create a relevant trace, then they must identify and describe the conditions (acceptance criteria) required for it to be used accordingly.

A practitioner must exercise caution and recognise that multiple activities/functions may be capable of creating trace-types that are comparable. To offer a simplistic example of this,, a

folder on a device may contain files placed there by a user, and also be the location that a piece of software stores output files by default. These two distinct causal actions/functions may create the same trace type (as in a stored file), but the trace is as a result of two distinctly different activities on a given system.

A practitioner may determine/develop their own trace interpretation method, or identify an existing method that has been documented in literature deriving from apparent credible sources. In the case of the latter, a practitioner must be confident that any information details a method sufficiently to allow for it to be understood.

2.4 Pillar 4:- Repeatability

It is argued that any methods identified in Pillar 3 to support trace-interpretation must perform consistently for them to be used as part of reliably determining the meaning of a trace. Under Pillar 4, practitioners must demonstrate that their methods produce repeatable results, and that the results are reproducible [27]. In essence, when their method is deployed multiple times in an unchanged environment using the same conditions/variables and data, any traces generated must be comparable in nature [27]. In addition, if their method was to be used by someone else, providing that the acceptance criteria for the method are met, the same results should be obtained [27].

If any trace interpretation method proposed by a practitioner cannot be shown to perform consistently, then its use for supporting a practitioner to form an opinion of a trace should be met with caution. If a practitioner cannot establish the conditions that govern the source or creation of a trace, then they may struggle to offer a reliable interpretation of it. Any trace interpretation method that generates inconsistent results may lead to the explanation of a trace that may only partially represent it, or at worst be incorrect.

2.6 Pillar 5:- Validation

Under Pillar 2, practitioners will have identified a series of potential provenances and causal actions for any trace. Each of these will then be assessed under Pillar 3, where a practitioner will identify and define any methods and their acceptance criteria that are capable of generating a trace that is comparable to the one they are observing in their case work. The repeatability of any method is determined under Pillar 4.

In Pillar 5, all of a practitioner's methods for trace-interpretation require validation, which ‘involves demonstrating that a method used for any form of analysis is fit for the specific purpose intended, i.e. the results can be relied on’ and objective evidence provided to support this position [17]. Here, a practitioner must show that their chosen method(s) can produce a trace that is relevant to their work. Detailed support for this task can be acquired from the Forensic Science Regulator guidance on method validation [17]. Any method (and its results) that a practitioner intends to rely upon to support their task of interpreting a trace must be fully described, showing what they reliably do, under what conditions they can be trusted to perform, and who the intended end users of both the method and the results are [17]. Often, any methods used to support trace-interpretation will be used within DF organisations as well as by courts and legal personnel who seek to rely and act upon the results generated by them. Therefore the requirements of both will need satisfying, where expert evidence admissibility criteria is defined under Part 7 of the Criminal Practice Directions 2023. Here, a number of benchmarks are set out which any method utilised during trace interpretation must address. A

technical specification for the method should be documented setting out what it does, how it does it and its limitations and scope [17]. Any method should also be risk assessed in order to address any potential concerns around its use including any issues that may exist around incompleteness, inaccuracy or the potential for the misinterpretation of any results it may generate.

All of the interpretative work that has been undertaken by a practitioner must be evaluated to determine whether it is effective at allowing a dependable opinion regarding the meaning of a trace to be formed. In essence, this task involves determining whether the impact of causal action/function (or in some cases multiple) can be shown to be linked with the creation of a comparable trace, therefore allowing them to form an opinion of the trace's meaning. If this is possible, a practitioner must determine whether any opinion of a trace that they have reached is defensible when subject to scrutiny. This means a quality review of their technical and interpretative work should be conducted and evidenced [7].

It is necessary at this point to stress that practitioners will be validating their trace-interpretation method, rather than any single tool. A method is defined as 'a logical sequence of procedures or operations intended to accomplish a defined task' and this could include the use of tools [17]. It is a practitioner's method in totality that supports their formation of an opinion of a trace, and while part of this may include the use of tools to find, process and present relevant data, there are also components of the method that do not involve tools, for example, when practitioners are interpreting any observations. Method validation processes must be designed to test all components of the interpretative process, including both the technical and interpretative parts, and facilitate the testing of any final opinion generated.

2.7 Pillar 6: Transparency

Any proposed trace's meaning should be supported with a portfolio of evidence that outlines and details all of the investigative and interpretative practices that a practitioner has undertaken which has led them to form an opinion. All datasets used during testing should be archived and remain available for scrutiny if required, including details of processes run and results obtained. Any methods developed and/or deployed, including any configurations used, should be documented. This should not be an unfamiliar task as practitioners should be versed in the need to maintain contemporaneous records of work conducted [24]. In addition, where theory and literature derived from apparent credible sources is sought and forms the basis of any formed meaning, copies of this work should be retained where possible.

2.8 Pillar 7:- Acceptance

Under Pillar 7, a practitioner should subject their interpretation of a trace to peer review, likely from those within the DF community who are suitably qualified to do so, and via the use of appropriate peer review methodologies [7]. Peer review is an integral part of quality control and assurance processes, helping to identify and rectify errors through the imposition of rigorous assessment practices [18]. It is also a practice that is recognised in evidence admissibility tests such as Daubert v. Merrell Dow Pharms., 516 U S. 869 (U S. 1995) [7]. By exposing any proposed trace-interpretation to peer review in order to seek an acceptance of it, practitioners are allowing others to review their investigative and interpretative work. If conducted properly, this should result in those conducting any review to provide a robust evaluation of the reliability and accuracy of the proposed interpretation, resulting in the general sense, in either concerns with it being raised, or an endorsement of it.

Peer review can exist in multiple forms, ranging from 'in-house' reviews conducted by trained colleagues, to the production and submission of any written work that depicts practices and methodologies, to a recognised and respected scientific journal for scrutiny. Further methods such as practitioner forums, blogs and social communities may also offer peer review, likely of a more informal nature. Practitioners should recognise that not all forms of peer review are of equal and appropriate quality, and they must determine and expose their interpretive work to a form of review that is suitably equipped for evaluating such an important practice as trace-interpretation. It is perhaps necessary here to stress the importance of peer review as a practice in the field of DF. Efforts should be made to ensure that peer review can be sought readily and delivered robustly and systematically allowing any verdicts derived from it to be relied upon when assessing the value of any information, and to inform future courses of conduct.

Finally, in some cases a trace's meaning may already appear to have been accepted by the general DF community - often seen with common operating system artefacts. Whilst this likely provides a practitioner with some confidence regarding the accuracy of any interpretation, it does not always guarantee that it is correct. In some instances due the advancement of knowledge over periods of time, new or adjusted interpretations for a trace may be offered, rendering previous versions obsolete. If a practitioner seeks to rely on an accepted interpretation, they should take steps to ensure that it remains currently acknowledged as good practice.

2.8 Pillar 8:- Competence

Competence is defined by The European Network of Forensic Science Institutes [13] as follows:

> 'The ability to perform the task of a certain role. A competent person has the knowledge and the ability to apply this knowledge, has the skills, the right behaviour and the attitudes for the role. Qualification, experience and training, although important, do not guarantee competence.'

Practitioners engaging in the process of interpreting a digital trace must be competent to undertake this task and be able to demonstrate their competency through assessment [8; 12]. It should be noted that not all roles within a DF organisation may encompass the task of trace-interpretation, therefore a practitioner must be sure that they are currently operating in a capacity that permits them to do so. Each organisation should define the remit of their staff roles, and alongside this a competency framework for each to ensure staff meet these requirements in order to be operational [14].

Competency can be a troublesome concept to address for any practitioner, and the Forensic Science Regulator in England and Wales states that it 'cannot be simply measured in years, number of cases examined, educational achievements, post-nominals or seniority, nor is it equivalent to credibility or eloquence although all these elements may contribute' [8]. In specific regard to digital trace interpretation, as a minimum it is suggested that practitioners must be able to evidence their competency in regards to the effective use of any methods used during the trace-interpretation process, any data sources and types, knowledge and understanding of the process by which the data may have been generated, testing, validation

and interpretative methods for digital trace interpretation and, accepted approaches for presenting any findings.

In regard to competency, there is often focus placed upon '*technical competency*'. This is generalised as the ability to utilise tools and methods effectively, conduct investigative tasks, and understand digital devices and the fundamental nature of digital data as an evidence source - a technically proficient practitioner. When considering the task of trace-interpretation, all opinion evidence provided is expert evidence, and practitioners must also be competent to express their opinions as experts. This requires practitioners to be capable of forming and expressing opinion through the use of established, logical and accepted methods, understanding the remit of their role and all of the legal obligations placed upon them. In England and Wales, practitioners should refer to the Forensic Science Regulator's Code of Practice [25] for details of role and competency requirements, where a need for competence in regard to the giving of expert evidence is stressed. In addition, the Association of Chief Police Officers' [26] express the need for expert witness training to be provided to practitioners to ensure they understand evidential processes linked with giving evidence, their responsibilities when doing so, and crucially, the ' distinction between expert evidence and evidence of fact'. Practitioners must receive training in order to operate as competent experts or they risk performing the role of an expert ineffectively. There cannot be an assumption that 'technically sound' practitioners automatically make effective experts; the additional skill set required of an expert must be taught, learned and honed.

Competency must also be maintained meaning engagement with appropriate forms of continuous professional development is crucial [13].

3 Summary

The formation of a digital trace's meaning is not something that should be done through guess work, hunches or ad hoc processes. Instead, this interpretative process contains multiple structured tasks that together should lead to accurate and reliable interpretations that are underpinned with the robust forensic practices that have led a practitioner to their conclusions. Here, the trace-interpretation process is visualised using the eight aforementioned pillars of evidence in order to show what is involved in conducting this work effectively. In most cases, practitioners should be capable of providing details of these pillars of evidence in order to underpin any trace-interpretive work they have undertaken.

References

1. Horsman, G., 2022. Forming an investigative opinion in digital forensics. Wiley Interdisciplinary Reviews: Forensic Science, 4(6), p.e1460.
2. van Baar, R.B., van Beek, H.M. and Van Eijk, E.J., 2014. Digital forensics as a service: A game changer. Digital Investigation, 11, pp.S54-S62.
3. Horsman, G., 2019. Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. Digital Investigation, 28, pp.146-151.
4. Sunde, N. and Dror, I.E., 2021. A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making. Forensic Science International: Digital Investigation, 37, p.301175.

5. Casey, E., 2011. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.
6. Carrier, B.D. and Spafford, E.H., 2004. Defining event reconstruction of digital crime scenes. Journal of forensic sciences, 49(6), pp.1291-1298.
7. Sunde, N. and Horsman, G., 2021. Part 2: The Phase-oriented Advice and Review Structure (PARS) for digital forensic investigations. Forensic Science International: Digital Investigation, 36, p.301074.
8. Forensic Science Regulator., 2021. Forensic Science Regulator Codes of Practice and Conduct Development of Evaluative Opinions FSR-C-118 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/960051/FSR-C-118_Interpretation_Appendix_Issue_1__002_.pdf
9. National Institute of Forensic Science Australia New Zealand., 2017. An introductory guide to Evaluative Reporting. https://www.anzpaa.org.au/ArticleDocuments/2314/An%20Introductory%20Guide%20to%20Evaluative%20Reporting%20(1).PDF.aspx
10. The European Network of Forensic Science Institutes., 2016. ENFSI guideline for evaluative reporting in forensic science. https://enfsi.eu/wp-content/uploads/2016/09/m1_guideline.pdf
11. Association of Forensic Science Providers., 2009. Standards for the formulation of evaluative forensic science expert opinion. Sci. Justice, 49, pp.161-164.
12. Forensic Science Regulator, 2020. Codes of Practice and Conduct Appendix: Digital Forensic Services FSR-C-107. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912389/107_FSR-C-107_Digital_forensics_2.0.pdf
13. The European Network of Forensic Science Institutes., 2011. Guidance on the assessment of competence for forensic practitioners. Available at: https://enfsi.eu/wp-content/uploads/2017/11/QCC-CAP-006-001.pdf
14. Forensic Science Regulator, 2023. Forensic Science Regulator Draft Code of Practice. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1131659/E02852302_Forensic_Science_Draft_CoP_Web_Accessible.pdf
15. Evett, I.W., 1998. Towards a uniform framework for reporting opinions in forensic science casework. Science & Justice, 3(38), pp.198-202.
16. Cook, R., Evett, I.W., Jackson, G., Jones, P.J. and Lambert, J.A., 1998. A model for case assessment and interpretation. Science and Justice, 38(3), pp.151-156.
17. Forensic Science Regulator., 2017. Forensic Science Regulator Guidance Method Validation in Digital Forensics FSR-G-218 Issue 2. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/921392/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf
18. Horsman, G. and Sunde, N., 2020. Part 1: The need for peer review in digital forensics. Forensic Science International: Digital Investigation, 35, p.301062.
19. Zapf, P.A. and Dror, I.E., 2017. Understanding and mitigating bias in forensic evaluation: Lessons from forensic science. International Journal of Forensic Mental Health, 16(3), pp.227-238.
20. Forensic Science Regulator., 2020. Forensic Science Regulator Guidance Cognitive Bias Effects Relevant to Forensic Science Examinations FSR-G-217. Available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/914259/217_FSR-G-217_Cognitive_bias_appendix_Issue_2.pdf
21. Aitken, C., Roberts, P. and Jackson, G., 2010. Fundamentals of probability and statistical evidence in criminal proceedings: guidance for judges, lawyers, forensic scientists and expert witnesses.
22. Cook, R., Evett, I.W., Jackson, G., Jones, P.J. and Lambert, J.A., 1998. A hierarchy of propositions: deciding which level to address in casework. Science & Justice, 38(4), pp.231-239.
23. Horsman, G., 2018. Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. Computers & Security, 73, pp.294-306.
24. Horsman, G., 2021. Contemporaneous notes for digital forensic examinations. Forensic Science International: Digital Investigation, 37, p.301173.
25. Forensic Sciecne Regulator, 2023. Forensic Science Regulator: Code of Practice. Available at: https://www.gov.uk/government/publications/statutory-code-of-practice-for-forensic-science-activities/forensic-science-regulator-code-of-practice-accessible
26. The Association of Chief Police Officers, 2012. ACPO Good Practice Guide for Digital Evidence. Available at: https://npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf
27. Brunty, J., 2023. Validation of forensic tools and methods: A primer for the digital forensics examiner. Wiley Interdisciplinary Reviews: Forensic Science, 5(2), p.e1474.

Interpreting digital traces:- 8 foundational pillars to support the formation of opinion in digital forensics

Horsman, Graeme

2023-12-03

Horsman G. (2024) Interpreting digital traces:- 8 foundational pillars to support the formation of opinion in digital forensics. Science & Justice, Volume 64, Issue 1, January 2024, pp. 38-42
https://doi.org/10.1016/j.scijus.2023.11.007