Digital Investigation 28 (2019) 146–151

Contents lists available at ScienceDirect

Digital Investigation

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

Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework

Graeme Horsman

School of Science, Engineering & Design, Teesside University, Middlesbrough, United Kingdom

ARTICLE INFO

Article history:
Received 21 June 2018
Received in revised form
18 January 2019
Accepted 18 January 2019
Available online 25 January 2019

Keywords:
Digital forensics
Investigation
Digital evidence
Decision making
Reporting

ABSTRACT

In the field of digital forensics it is crucial for any practitioner to possess the ability to make reliable investigative decisions which result in the reporting of credible evidence. This competency should be considered a core attribute of a practitioner's skill set and it is often taken for granted that all practitioners possess this ability; in reality this is not the case. A lack of dedicated research and formalisation of investigative decision making models to support digital forensics practitioner's is an issue given the complexity of many digital investigations. Often, the ability to make forensically sound decisions regarding the reliability of any findings is arguably an assumed trait of the practitioner, rather than a formally taught competency. As a result, the digital forensic discipline is facing increasing recent scrutiny with regards to the quality and validity of evidence it's practitioners are producing. This work offers the Digital Evidence Reporting and Decision Support (DERDS) framework, designed to help the practitioner assess the reliability of their '*inferences, assumptions of conclusions*' in relation to any potentially evidential findings. The structure and application of the DERDS framework is discussed, demonstrating the stages of decision making a practitioner must undergo when evaluating the accuracy of their findings, whilst also recognising when content may be deemed unsafe to report.

Introduction

Without retracing well documented concerns, in summary, a lack of field governance, entry requirements and standards (see, Meyers and Rogers, 2004; Lillis et al., 2016) has led to diverse practices in many areas of the digital forensics discipline. Practitioners in digital forensics are often diverse in terms of possessed knowledge, experience and capability, yet often, many are entrusted with the same task of investigating and reporting upon complex digital crime. Such disparity in experience means that the reliability of investigative decision making (DM) by digital forensic practitioners is both paramount and concurrently has to be questioned. Collie (2018, p.154) has recently alluded to this issue.

> 'Information everywhere means potential evidence everywhere. Knowing where to start can be difficult, even for professionals in the field. Knowing how to retrieve digital evidence, particularly in a forensically sound way, can complicate things further. But it is upon knowing how to interpret the data, once collected, that justice will hinge. And this, frequently, is where the system falls apart.' (Collie, 2018 p154).

Digital investigations are multifaceted, complex processes where practitioners are required to 'make sense' of large quantities of digital data stored in varying formats, where many variables can impact an overall reliable explanation of the relevance of any potential evidence. This process involves placing meaning and context behind particular pieces of digital data in line with any suspected offence for purposes of reliability establishing whether a breach of law has occurred. Of particular concern lies the interpretative analysis of potential evidentially relevant data which is often undertaken solely by an investigating practitioner who maintains responsibility for all stages of the examination process, including the reporting of findings and any subsequent presentation of evidence to a court of law. A digital forensic practitioner must be competent to make investigative decisions and shoulders the burden of accountability for erroneous DM, a scenario that is neither risk-averse or satisfactory. Where an inability to make

E-mail address: g.horsman@tees.ac.uk.

https://doi.org/10.1016/j.diin.2019.01.007
1742-2876/© 2019 Elsevier Ltd. All rights reserved.

forensically sound judgements exists, evidence standards are jeopardized, increasing the risk of miscarriages of justice or simply cases being dropped by criminal justice processes.

A concern that digital forensic practitioners may lack the ability to consistently interpret digital evidence accurately, raises issues of evidential reliability. Any subsequent investigation can 'impact a person's livelihood or liberty … it is crucial to avoid mistakes, missed opportunities, misinterpretations, and miscarriages of justice' (Casey et al., 2018), where the importance of digital evidence in many criminal investigations cannot be understated where in some cases it is the primary evidence source. Arguably no room for investigative error exists, yet such mistakes are beginning to be noted. During the presentation of oral evidence to the UK Justice Committee on May 15th 2018, Professor Peter Sommer and Dr Jan Collie raised a number of concerns surrounding digital forensics, of which notable comments are provided below:

> 'There is not enough funding for real, trained analysis. At police stations, for instance, a police officer who has probably only been trained for about a day to use the equipment—he can click it in and press the buttons—quite commonly mishandles the evidence'.
>
> 'It is that anomalous nature that is of concern. Somebody might be charged in one area but not in another, with the same evidence, because of the expertise of the people dealing with the evidence'.
>
> 'Digital forensics units are quite good at keeping up to date with technology for extracting data and making copies, but they then pass the copies, largely uninterpreted, to police officers, who are not experts and who are not digital forensics people. General policing investigators do not necessarily have the tools to search that information effectively and understand it'.
>
> 'Lack of resources is often used as an argument for not implementing quality standards. We have to move away from thinking of quality standards as an optional add-on, and think of it as integral to the way to deliver quality forensic science'. (Justice Committee, 2018)

Whilst these points should arguably be treat with caution due to limited detailed empirical evidence outlining such concerns, they are suggestive of an underlying issue in the field of DF.

Investigative decision making

As with all disciplines, digital forensic practitioners remain vulnerable to human error, limitations of knowledge and general mistake (Christensen et al., 2014). In DF, it must also be acknowledged that errors may not always be technical or procedural in origin, where non-technical sources of error (highlighted by Sunde (2017, p.17) to include things like 'misinterpretations of the meaning, value or reliability of a piece of evidence, a biased decision, or essential evidential information being overlooked') are also a concern. Whilst all provide quality management challenges which must be addressed by organisations seeking to maintain high standards of practice, the fostering of robust investigative DM can be a preventative measure against poor examination results. Unfortunately, this skill is not always championed. In 2009, Beebe alluded to the fact that digital forensic organisations fail to develop and support appropriate investigative DM. Although, DM issues have been acknowledged (James and Gladyshev, 2013a), as of yet, there are few formalised methods to support the practitioner with their investigative judgements, despite Casey (2018) recently indicating that 'the scientific validity and reliability of forensic results' was becoming a worry. Whilst academic work typically focuses on the capturing of processes involved with specific evidence types (see for example frameworks aimed at cloud computing (Taylor et al., 2011), email and network forensics (Sibiya et al., 2012)) or alternatively, formalising the overall investigation stages (see Valjarevic and Venter, 2012; Kohn et al., 2013), work to support the practitioner make reporting decisions is sparse. To provide context, throughout the course of an investigation, practitioners identify information which may be deemed of relevance (if interpreted correctly) to their investigation. In this context, practitioners could be considered '*gatekeepers*' in terms of disclosure of this information. Before opting to include potentially evidential data within a written statement or report, the practitioner must decide as to whether they fully understand it. Whilst at a high-level, this decision appears binary; either they do, or they don't, this remains an oversimplified view.

In reality, the decision to report upon a piece of digital evidence is one which is multifaceted and complex, and should take into account the practitioner's understanding of the surrounding facts of the case, their competence to report on any findings, their confidence in the interpretation of such data and the robustness of any associated testing which has led to any subsequent findings. Establishing confidence is a crucial element of investigative decision making, as emphasized by the term 'sufficient confidence' in Pollitt et al. (2018), which is a minimum level of confidence which must be reached as part of a decision making process. In the context of defining sufficient confidence within investigative DM in digital forensics, a practitioner must establish a threshold which must be achieved in order to establish sufficient confidence which should take into consideration the facts of a case, claims made by parties involved and the impact of any competing hypotheses on a practitioners assumed understanding of any data in question should be considered and evaluated accordingly (Casey, 2018). A digital forensic practitioner as part of their DM must possess sufficient confidence in their interpretation of any digital evidence before it can be reported.

Every piece of evidence reported by a practitioner during an investigation is done so following a practitioner's '*inferences, assumptions or conclusions*' which have influenced their decision to report upon an identified artefact or piece of data. As a result, it is vital that practitioners underpin this process with robust investigative DM allowing them to test the reliability of such judgements and ensure admissibility of their reported evidence.

This work provides the Digital Evidence Reporting and Decision Support (DERDS) framework to support digital forensic practitioners during the process of determining when to reliably disclose digital data within their statement and reports. The DERDS framework provides a formalisation of sound investigative DM to enable practitioners to establish when and how to test the accuracy and reliability of their interpretative inferences made regarding digital data. In essence, the DERDS framework captures and formalises investigative acumen, for reference by practitioners and those operating in this area.

Context for applying the DERDS framework

In most digital forensic investigations a practitioner will highlight multiple pieces of digital data which they may consider potentially evidential. Before opting to report this information to their client, their interpretation of such data must be accurate, and its impact on the investigation understood. The prevention of errors at this stage is key to ensuring any negative impact on those involved in the criminal justice process is minimised. The decision to report on a piece of potential digital evidence should be one which has been subject to scrutiny and evaluation prior to submission, given the potential serious consequences of misjudgements. When content is reported by a practitioner as evidence, the decision to do so must be based on robust forensic knowledge and testing which has been subject to peer review. There should be an absence of misinterpretation and in many cases, the processes and procedures undertaken as part of an investigation should be reproducible with an outcome with sufficient confidence to meet a decision-maker's threshold. Ultimately, 'digital forensics is meant to be based on science, not supposition' (Collie, 2018 p155). To support this process Fig. 1 outlines the DERDS framework, designed to guide a practitioner through the necessary steps for determining when it is safe to report the specific findings of their examination in an effort to minimise unsafe disclosures of evidence which may not be accurately or fully understood. The DERDS framework formalises a practitioner's investigative DM process assisting them to determine when to report upon a piece of digital evidence found within their investigation.

It is important to clarify that the DERDS framework is for application at what is coined, the 'micro-level' of a digital forensic investigation, in relation to each singular 'evidence type' of a practitioner's findings (for example, Internet search terms, deleted pictures etc). For example, if the practitioner identifies two pieces of potential evidence (for example a set of search terms and a set of deleted pictures) the DERDS framework should be applied to each evidence type in order to ensure that any *conclusions, inferences or assumptions* regarding their relevance to a case in question has been correctly established. The DERDS framework targets this level of a digital forensic investigation due to the intrinsic application of what is commonly referred to as 'push-button' forensics; the use of automated recovery and data parsing tools to gather potential digital evidence, absent of the application of robust evaluation of its meaning (Sammons, 2012; James and Gladyshev, 2013b; Collie, 2018). Whilst automation offers many investigative advantage in terms of the speed of data processing, any subsequent results should not be reported without the robust appraisal of their meaning having been carried out. It is proposed that this assessment should be undertaken in line with the stages documented in the DERDS framework.

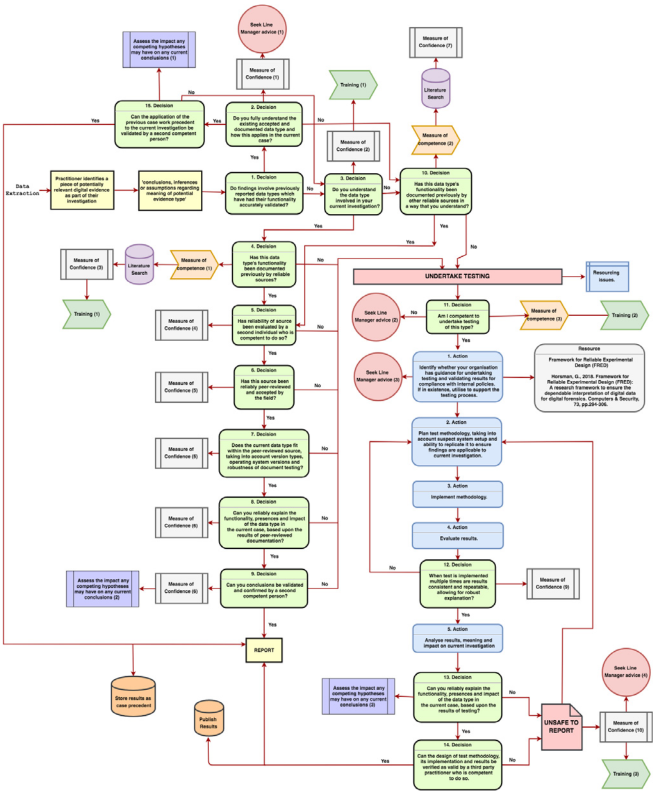
Data Extraction
Practitioner identifies a piece of potentially relevant digital evidence as part of their investigation
'conclusions, inferences or assumptions regarding meaning of potential evidence type'
1. Decision
Do findings involve previously reported data types which have had their functionality accurately validated?
2. Decision
Do you fully understand the existing accepted and documented data type and how this applies in the current case?
3. Decision
Do you understand the data type involved in your current investigation?
4. Decision
Has this data type's functionality been documented previously by reliable sources?
5. Decision
Has reliability of source been evaluated by a second individual who is competent to do so?
6. Decision
Has this source been reliably peer-reviewed and accepted by the field?
7. Decision
Does the current data type fit within the peer-reviewed source, taking into account version types, operating system versions and robustness of document testing?
8. Decision
Can you reliably explain the functionality, presences and impact of the data type in the current case, based upon the results of peer-reviewed documentation?
9. Decision
Can you conclusions be validated and confirmed by a second competent person?
10. Decision
Has this data type's functionality been documented previously by other reliable sources in a way that you understand?
15. Decision
Can the application of the previous case work precedent to the current investigation be validated by a second competent person?
Assess the impact any competing hypotheses may have on any current conclusions (1)
Seek Line Manager advice (1)
Measure of Confidence (1)
Measure of Confidence (2)
Training (1)
Measure of Confidence (7)
Literature Search
Measure of competence (2)
Measure of Confidence (3)
Literature Search
Measure of competence (1)
Training (1)
Measure of Confidence (4)
Measure of Confidence (5)
Measure of Confidence (5)
Measure of Confidence (6)
Measure of Confidence (6)
Assess the impact any competing hypotheses may have on any current conclusions (2)
REPORT
Store results as case precedent
Publish Results
UNDERTAKE TESTING
Resourcing issues.
11. Decision
Am I competent to undertake testing of this type?
Seek Line Manager advice (2)
Measure of competence (3)
Training (2)
1. Action
Identify whether your organisation has guidance for undertaking testing and validating results for compliance with internal policies. If in existence, utilise to support the testing process.
Seek Line Manager advice (3)
Resource
Framework for Reliable Experimental Design (FRED)
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.
2. Action
Plan test methodology, taking into account suspect system setup and ability to replicate it to ensure findings are applicable to current investigation.
3. Action
Implement methodology.
4. Action
Evaluate results.
12. Decision
When test is implemented multiple times are results consistent and repeatable, allowing for robust explanation?
Measure of Confidence (9)
5. Action
Analyse results, meaning and impact on current investigation
13. Decision
Can you reliably explain the functionality, presences and impact of the data type in the current case, based upon the results of testing?
Assess the impact any competing hypotheses may have on any current conclusions (3)
14. Decision
Can the design of test methodology, its implementation and results be verified as valid by a third party practitioner who is competent to do so.
UNSAFE TO REPORT
Seek Line Manager advice (4)
Measure of Confidence (10)
Training (3)
Yes
No

Fig. 1. The DERDS framework.

Users of the DERDS framework

The DERDS framework is designed to support those who are actively involved in digital forensic case work and require additional formalized investigative DM support. Whilst some experienced and reliable practitioners who have honed their skills across multiple years in service may deem such DM a natural part of their case processing, benefit from the DERD framework in regards to mitigating the risk of mistakes and misinterpretations can still be acquired. The formalization of DM in digital forensics offered in this work serves as a reminder of logical decision and the processes involved with attaining this. For those experienced, but lacking such confidence in their DM it may serve as supportive guidance, and as a codified process flow for making sound judgements in relation to their interpretation of any digital evidence.

In comparison, inexperienced practitioners arguably require formailised guidance to support reliable DM as part of the investigative process. The DERDS framework is also aimed at those studying the discipline of digital forensics, establishing a formalised process flow for reporting reliable evidence, whilst also highlighting the key competencies required of an examiner; for example the ability to research and test effectively. Finally, the DERDS framework should be considered a quality management resource for laboratories and senior staff tasked with maintaining the standard of work where quality assurance procedures can be developed at key requisite stages of the DM process.

Application of the framework

The application of the DERDS framework commences when a practitioner has identified a piece of potentially relevant digital evidence as part of their investigation, which may occur multiple times throughout the course of an examination of a case's exhibits. When digital content is identified for potential reporting, a practitioner will maintain '*inferences, assumptions or conclusions*' regarding this information's context and meaning within the confines of their investigation. It is the accuracy of these inferences which must be evaluated and tested before determining whether this content can be reliably reported, ultimately contributing to the understanding of a suspect offence and supporting the criminal justice process. The DERDS framework provides three pathways for a practitioner to determine and test the reliability of their investigative '*inferences, assumptions or conclusions*'.

Pathway 1:- following previous case work precedents

The first stage in the DERDS framework is to determine whether the piece of potential evidence under scrutiny is comparable to that which has previously been validated and accepted in a previous case work precedent (Decision 1), in which case, Pathway 1 can be potentially followed. To provide an example, where Internet artefacts relating to browser 'X' (version 'Y') have been located in a current case, can any '*inferences, assumptions or conclusions*' be validated against the results of a previously validated and accepted investigation of browser 'X' (version 'Y'). Where an evidence type can be confirmed (reliably) as previously being reported upon in past casework and its interpretation and impact has been accurately described and validated, then a practitioner may opt to pursue the use of this previous interpretation and rely upon it when producing a current report, subject to their ability to understand it. This is the shortest path in the DERDS framework for a practitioner to be in a position to reliably report their findings. There are caveats to be placed upon this pathway, notably that a previous case work precedent must have been set following robust the implementation of rigorous testing by a competent individual who has had such work reviewed and accepted. This prevents the continued dissemination of unreliable knowledge. In addition, the current piece of evidence under scrutiny must falls within the boundaries of the previous case work precedent (considering factors such as application version and operating system version types) before it can be relied upon to interpretive support. A practitioner must also fully understand the previous interpretation of this artefact (noted within the previous case work precedent) and how it can be applied in their current case to support their interpretation of identified data (Decision 2). Here, a practitioner must decide upon the relevance of a previous case work precedent and while they are assumed competent to do so, this decision will involve a measure of how confident (1) they are in terms of its application in the current case. Arguably a practitioner who maintains any doubt as to the application of a previous case work precedent, or their understanding of it in relation to their current interpretation of evidence must not report upon their interpretation of any findings in their current work with without carrying out testing or a review for existing published material which may support their interpretation (discussed in Sections 2.4-2.5 - Pathways 2 & 3). Correspondence with a senior practitioner or line manager may support any decision to follow previous case work precedents, and this should be carried out. Finally, a practitioner should have the application of a previous case work precedent to their interpretation of evidence validated by a second competent individual. In doing so, the practitioner should also at this stage consider any competing hypotheses which may exist in regards to the digital data under investigation and identify any impact they may have upon their understanding of the data and the reliability of their interpretation. Where competing hypotheses are not available, digital forensic practitioners have a duty to imagine potential the competing hypotheses in order to follow the scientific practice of falsification. At which point a practitioner can proceed to report their findings in the knowledge that their interpretation of evidence in their current case is comparable to what has previously and reliably been documented.

Pathway 2:- following existing published works

Where no existing case work precedent exists, practitioners are faced with two possible routes through the DERDS framework; to identify and follow the interpretation of any evidence provided in existing published works or test and validate their own findings. It is key to note that in Pathway 2, published works is a generic concept used to cover a range of material which is accessible and available including material formally published in academic journals to content acquired from formal training courses and institutes. Whilst some sources may be more reliable than others, validity checks are embedded within the DERDS framework to prevent the use of poor quality information (Decisions 4–6).

Following Pathway 2, practitioners must first decide whether they fully understand the information they have highlighted as potentially evidential (Decision 3). This decision also involves a measure of confidence (2) where less than full confidence prevents a practitioner from simply cross checking their findings against existing published work; additional thorough testing of the functionality of any potential evidence is required. To provide an example, a level of understanding must be both technical and contextual. Assuming that a practitioner has exercised keyword searching functionality across their case, leading to key term hits for relevant terms, the appearance of such hits alone are not always a marker of any wrongdoing. To achieve a full understanding of this evidence type, both the reason for the keyword hit occurring and why it is present on a suspect's device must be understood; the cause of such hits should be fully investigated and determined. If a practitioner confidently understands the evidence type which they have highlighted, they should then opt to validate this information through reference to dependable, peer-reviewed published material, increasing the reliability of their interpretation. In order to pursue this option, existing reliable published work regarding the evidence type must be in existence (Decision 4). This stage involves both competence and confidence validation. First a practitioner must be competent (1) carry out a thorough search for reliable published literature. This is a skill set not typically associated with digital forensic practitioners, hence the requirement for a competency check and potential upskilling (Training 4). If a practitioner can locate a relevant source, a measure of confidence is required regarding its reliability (Measure of Confidence 4) where a decision must be made based on a number of factors including author details, location of published work, any citation information and peer-reviewed status. The source must also be reviewed and validated by a second competent individual, should the resource be relied upon as part of the interpretation of evidence in the current case (Decision 5). Any identified source should have been subject to robust peer-review and be accepted by the digital forensic field as '*known-good*' knowledge (Decision 6) drawing analogy to evidence admissibility rules such as those introduced through Daubert in the United States. This task is not straightforward, requiring a measure of confidence (5) to be established.

Crucially, for any resource to be relied upon by the practitioner to support their interpretation of findings, it must be applicable in terms of comparable platforms and version types (Decision 7). Research which documents different test conditions may limit the reliability of its use in a current case context (as noted in Section 2.3). Sommer (2018, p.118) indicates that 'most digital devices are akin to a whole scene of crime. There will be a large number of potential artefacts and different requirements of how they are to be handled'. As a result, it is imperative that any published resource relied upon for validating a practitioner's interpretation of evidence is comparable in context and settings in order to be reliably applied to current work. Given the diversity of evidence types and pace of change, in many cases practitioners may struggle to identify directly applicable material to rely upon. The practitioner must also be able to apply the findings of the peer reviewed work in a way which allows them to confirm their understanding of current case evidence (Decision 8). Finally, all working conclusions must be validated by a second competent person (practitioner peer review - Decision 9), before any findings in question can be reliably reported. Peer review is a crucial stage in the process of validating results and one which is difficult to apply. Sommer (2018 p.119) notes that peer require requires the review and evaluation of work by a competent individual who can undertake this task. Yet questions may be raised as to whether enough practitioners with the required experience and expertise exist, raising concerns over the reliability and sustainability of peer-review as a quality management process. Yet the burden of operating with appropriately trained and experienced staff lies with the digital forensic organisation and it remains best practice to ensure such reviews take place. Finally, as part of Decision 9, and as with Pathway 1, the impact of competing hypotheses should be considered. Any negative responses to Decisions 4–9 prohibit a practitioner from reporting their results, where additional requirements of undertaking testing to validate their '*inferences, assumptions or conclusions*' regarding their findings is required.

Pathway 3:- validation via testing

Where a practitioner is unsure of the interpretation of their findings and is unable to pursue Pathways 1 or 2 of the DERDS framework, the practitioner must undertake their own testing to validate their '*inferences, assumptions or conclusions*'. The act of testing maintains resource considerations and whilst the accuracy of any investigation should not be compromised by resource restrictions, in reality, constraints are in operation both in terms of time and equipment and this should be considered. Decision 12 provides a gateway to testing in the form of a competency test. Whilst many practitioners possess the technical skills to investigate complex forms of digital data, it is also assumed that testing forms a key competency of the practitioners skill set. Whilst it is arguable that a competent digital forensic practitioner should be capable of robust testing, it is likely not always the case. Testing provides the foundation from which the reliable interpretation of result is built. Flawed testing is detrimental both in terms of potentially producing incomplete or inaccurate results, but also due to the potential of creating a false sense of confidence that such results have been acquired due to testing should weaknesses in test methodologies remain undetected. As a result, flawed testing can actually increase the dissemination of erroneous knowledge under the guise that it is more reliable and should be treated as 'known good'. As a result, it is crucial that Decision 12 is answered honestly by the practitioner, taking into account a measure of their own competence. A non-competent examination should seek advice from those in senior positions where additional training may be required to upskill the practitioner with regards to sound testing methods and practices (Training 2). Decision 12 is not designed to undermine an examiner, but protect them from the dangers of producing and relying on unreliable findings.

Those examiners who are deemed competent to test are faced with first identifying a valid testing methodology to implement as part of their work (Action1). Discussions with appropriate senior staff within their laboratory is necessary to identify existing compliant procedures in use within their workplace which may adhere to existing standards. Academic sources documenting digital forensic test strategies are sparse, however this article recommends the use of the Framework for Reliable Experimental Design (FRED), a six stage process designed to facilitate robust testing in digital forensics (Horsman, 2018). The FRED framework is designed to support the robust planning and implementation of testing in digital forensics, supporting the evaluation and analysis of subsequent results. Whilst in-depth guidance from Horsman (2018) is provided, Actions 2–5 and Decision 14 provide for the key testing stages.

On completion of testing, the practitioner is required to address whether they are now in a position to reliably confirm their '*inferences, assumptions or conclusions*' made regarding their findings (Decision 13). As with Pathways 1 and 2, this process should also take into account the impact of competing hypotheses. Those who are, should have the findings of their testing procedures and results validated by a second, competent person (Decision 14). If this can be achieved, then a practitioner will be in a position to reliably report the results of their work. Given that this information should be classified as '*known good*' knowledge, the results of this work should both be published and disseminated to support the delivery of good practice within the digital forensic field and stored as a Previous Case Work Precedent. If, following testing either the evidence type's functionality cannot be reliably explained or the work cannot be validated by another competent individual, then findings are unsafe to report. In such cases, a practitioner is faced with two options. First, the testing phase can be readdressed, developing and expanding test methodologies in an effort to exhaust any discrepancies in the data set and establish an understanding of the functionality of any identified evidence. Second, a practitioner can seek support from their line manager in order to acquire additional expertise to support the practitioner as they seek to validate their '*inferences, assumptions and conclusions*' regarding an evidence type. This may also act as a competency indicator, triggering the need for additional training (Training 3).

Example application of the DERDS framework

To provide an example of the application of the DERDS framework, consider the situation where a practitioner encounters application 'X', a mobile device chat application for the first time during an investigation. Basic keyword searching reveals potentially relevant string matches contained within what appears to be log files associated with 'X', indicative of content associated with an offence of grooming being carried out on the suspect device. At this point, the practitioner cannot be sure of the reasoning behind the presence of this content having neither encountered 'X' before (and therefore could potentially rely on past experiences, if they were correct) or tested. Therefore it is argued that the practitioner can move forward in two ways. First they could report on the string matches albeit untested, relying on assumptions and risking misinterpretation of the data and mistake. Or second, a practitioner could enter into the DERDS process. In doing so, the practitioner has the 3 pathway options as discussed in sections 2.3-2.5. The practitioner could opt to follow previous case precedents involving an examination of 'X' if any exist, providing they understand the implications of past work and it can be directly and reliably applied to the current investigation of 'X'. A practitioner may seek support from senior colleagues regarding the level of confidence attributed to a past precedent in order to determine whether it is applicable in the current instance. If a precedent can be relied upon they may be in a position to report upon the results of 'X' in the current instance, relying on a past accepted interpretation of 'X's' function.

If no past precedents exist but a practitioner understands the basic concepts of the relevant data identified in an examination of 'X' (for example, records in an SQL database where SQL is understood) and it remains a case as to how evidential records came to be retained on the device, a practitioner may seek to identify published works depicting the function of 'X'. This option seeks to rely on published works which have already carried out rigorous and reliable testing which a practitioner can rely upon in their current case. Where published work has documented the function of 'X', and it is both reliable (to be determined by the practitioner, considering things like peer-review) and applicable to the current investigation, such information can be used to support a practitioner in their current interpretation of data relating to 'X'. This path is reliant on a practitioner being able to identify an applicable, reliable source of published work (should one exist). The danger which exists here is that erroneous or non-applicable (wrong of historic version of 'X' has been examined where structures and functionality have now changed) published work are relied upon, and support in terms of training may be required to identify reliable material. This may also be supplemented by senior experienced staff if necessary. If not applicable published works are available, a practitioner must implement testing as a final option.

Testing allows the practitioner to personally determine the function of 'X' providing they are competent to carry out testing and complete testing correctly. Again, this may require training and support from senior staff members who are versed in completing testing. An organisation should develop and maintain and accepted testing framework which can be trusted. Is on completion, testing has allowed the practitioner to reliably understand the function of 'X' (having completed the various stages of pathway 3 in DERDS), only then can the findings related to the current investigation of 'X' be reported.

Whilst the DERDS framework may not 100% prevent errors from occurring, it seeks to increase the rigour of processes involved with the interpretation and testing of digital evidence before the reporting process takes places. DERDS offers pathways for a practitioner to seek to increase the reliability of their results rather than relying on under-tested inferences which may lead to incorrect and unreliable evidence being reported.

Cost

Although the DERDS framework does not explicitly make reference to cost as a factor, in reality costing issues are likely to arise and influence decision making in some instances and at various points (Overill and Silomon, 2010; Hitchcock et al., 2016). Arguably, cost should not influence the use of the DERDS framework nor should it be a barrier to the reliable interpretation of digital evidence, however in reality it will be influential as digital forensic investigations are costly. DERDS advocates process which are designed to help increase the reliability of evidence before it is reported. Processes such as reviewing existing bodies of literature and carrying out in-depth testing take time and utilise resources, which in turn costs money. It is argued that despite costs, such processes are important to ensure evidence reliability, but costs associated with for example, the purchase of test equipment to carry out in-depth testing, may in some cases be too much of a burden for an organisation to invest in. Cost implications must be considered on a case by case basis by organisations and the risks of not engaging in processes such as those noted in DERDS should be evaluated.

Concluding thoughts

The DERDS framework formalises the stages of investigative decision making to support the practitioner when attempting to establish and test the reliability of their '*inferences, assumptions or conclusions*' about specific evidence types identified during their investigation. Practitioners will follow one of three pathways to determine whether they are safe to report their findings, based on markers of reliability. The framework aims to intercept practitioners who have not fully validated their findings, preventing the reporting of potential misinterpreted data, found as part of an investigations. It is also hoped that this work provides a resource from which sound decision making processes can be both developed and checked. It is hoped that as a result of the correct engagement with the DERDS framework, those who may have previously reported upon unsafe digital findings would be alerted to weaknesses in their work due to the three pathways included and their checkpoints. Whilst in theory, the framework offers an additional level of vetting, in practice, costs are involved in its implementation in terms of practitioner time and resources. As a result, organisational policies will likely determine the true extent to which DERDS can be engagement with. In addition, it also makes assumptions that suitable knowledge is present with senior management staff who take responsibility and act as gatekeepers for key decision making. A degree of up-skilling may also be required with regards to pathways 2 and 3 and this requires training investment and the correct implementation by an organisation.

One of the key requirements of DERDS is honest and committed engagement by practitioners using it. A potential issue lies with the 'confident examiner', someone who may assume they are correct without proper validation of their reasoning. Whilst in some regards this will always be an issue due to the way practitioners work, often individually responsible for our case loads where weaknesses in peer-review systems exist. In some instances the 'confident examiner' cannot be stopped from making mistakes, but this is due to their own lack of 'honest' engagement with frameworks such as DERDS. Such circumstances directly influence the inclusion of frequent confidence measures in DERDS which require a practitioner to truthfully evaluate their understanding at various stages where any forms of doubt should raise concerns. Whilst practitioners may still proceed wrongly past such checks, it is argued that this would be due to passive surface engagement with DERDS. As a result, secondary checks by 'senior staff' are also offered as failsafes, but again require committed engagement. The DERDS framework is offered as a tool to improve current procedures for ensuring evidence reliability, a hopeful step in the right direct, but it alone is by no means the answer to preventing all misinterpretation of digital evidence and further work in this area must continue.

Acknowledgements

I would like to formally acknowledge the support of members of the practitioner forum www.forenicsfocus.com who engaged with discussions surrounding the development of the DERDS framework, providing valuable input and feedback.

References

Beebe, N., 2009, January. Digital forensic research: the good, the bad and the unaddressed. In: IFIP International Conference on Digital Forensics. Springer, Berlin, Heidelberg, pp. 17–36.

Casey, E., 2018. Clearly conveying digital forensic results. Digit. Invest. 24, 1–3.

Casey, E., Geradts, Z., Nikkel, B., 2018. Transdisciplinary strategies for digital investigation challenges. Digit. Invest. 25, 1–4.

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.

Collie, J., 2018. Digital forensic evidence-Flaws in the criminal justice system. Forensic Sci. Int. 289, 154.

Hitchcock, B., Le-Khac, N.A., Scanlon, M., 2016. Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. Digit. Invest. 16, S75–S85.

Horsman, G., 2018. Framework for Reliable Experimental Design (FRED): a research framework to ensure the dependable interpretation of digital data for digital forensics. Comput. Secur. 73, 294–306.

James, J.I., Gladyshev, P., 2013a. A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. Digit. Invest. 10 (2), 148–157.

James, J.I., Gladyshev, P., 2013b. Challenges with Automation in Digital Forensic Investigations arXiv preprint: arXiv:1303.4498.

Justice Committee, 2018. Oral Evidence: Disclosure of Evidence in Criminal Cases. HC 859.

Kohn, M.D., Eloff, M.M., Eloff, J.H., 2013. Integrated digital forensic process model. Comput. Secur. 38, 103–115.

Lillis, D., Becker, B., O'Sullivan, T., Scanlon, M., 2016. Current Challenges and Future Research Areas for Digital Forensic Investigation arXiv preprint. arXiv:1604.03850.

Meyers, M., Rogers, M., 2004. Computer forensics: the need for standardization and certification. Int. J. Digital Evid. 3 (2), 1–11.

Overill, R.E., Silomon, J.A., 2010, September. Digital meta-forensics: quantifying the investigation. In: Proc. 4th International Conference on Cybercrime Forensics Education & Training (CFET 2010), Canterbury, UK (September 2010).

Pollitt, M., Casey, E., Jaquet-Chiffelle, D.O., Gladyshev, P., 2018. A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence (No. 0002). OSAC/NIST.

Sammons, J., 2012. The Basics of Digital Forensics: the Primer for Getting Started in Digital Forensics. Elsevier.

Sibiya, G., Venter, H.S., Ngobeni, S., Fogwill, T., 2012, August. Guidelines for procedures of a harmonised digital forensic process in network forensics. In: Information Security for South Africa (ISSA), vol. 2012. IEEE, pp. 1–7.

Sommer, Peter, 2018. Accrediting digital forensics: what are the choices? Digit. Invest. 25, 116–120.

Sunde, N., 2017. Non-technical Sources of Errors when Handling Digital Evidence within a Criminal Investigation (Master's thesis).

Taylor, M., Haggerty, J., Gresty, D., Lamb, D., 2011. Forensic investigation of cloud computing systems. Netw. Secur. 2011 (3), 4–10.

Valjarevic, A., Venter, H.S., 2012, August. Harmonised digital forensic investigation process model. In: Information Security for South Africa (ISSA), vol. 2012. IEEE, pp. 1–10.