WIREs Forensic Science, Volume 4, Issue 6, November/December 2022, Article number e1460
DOI:10.1002/wfs2.1460

Article Title: Forming an Investigative Opinion in Digital Forensics

Article Category:- PERSPECTIVE

Authors:

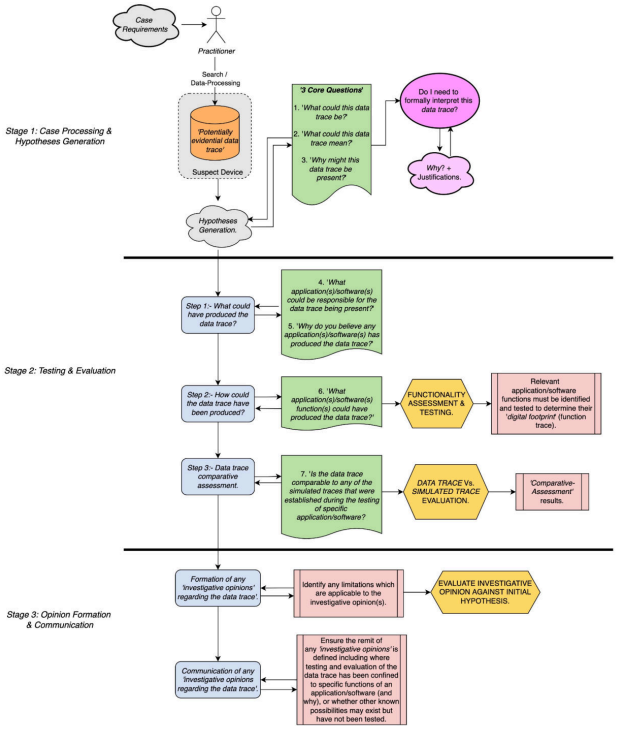
Dr Graeme Horsman
School of Computing, Engineering & Digital Technologies
Teesside University
graeme.horsman@googlemail.com
ORCID:- 0000-0002-0685-0650

No conflicts of interest to declare

ABSTRACT

As we now see digital evidence play a role in many investigative scenarios, it is imperative that those seeking to rely upon it as part of criminal justice processes can do so, absent any concern regarding its validity. Interpreting the meaning of digital data and its potential value to a criminal inquiry as part of a digital forensic examination is a complex and multifaceted process requiring the practitioner to possess the relevant knowledge, experience and insight needed to determine the case-significance of a given data trace accurately. Erroneously interpreted data that is communicated to a client and subsequently relied upon can have far-reaching consequences for all those involved in the investigative process. This work discusses the process of forming investigative opinions in digital forensic science examinations, what this means in practice and the ways in which it can be achieved. Focus will be given to the process of forming an investigative opinion when underpinned through the reconstruction and testing of a suspect system/setup, with a formal three-stage methodology for doing this outlined.

Graphical Abstract



Forming an Investigative Opinion in Digital Forensics

Abstract

As we now see digital evidence play a role in many investigative scenarios, it is imperative that those seeking to rely upon it as part of criminal justice processes can do so, absent any concern regarding its validity. Interpreting the meaning of digital data and its potential value to a criminal inquiry as part of a digital forensic examination is a complex and multifaceted process requiring the practitioner to possess the relevant knowledge, experience and insight needed to determine the case significance of a given data trace accurately. Erroneously interpreted data that is communicated to a client and subsequently relied upon can have far-reaching consequences for all those involved in the investigative process. This work discusses the process of forming investigative opinions in digital forensic science examinations, what this means in practice and the ways in which it can be achieved. Focus will be given to the process of forming an investigative opinion when underpinned through the reconstruction and testing of a suspect system/setup, with a formal three-stage methodology for doing this outlined.

Keywords: Digital Forensics; Investigative Opinion; Testing; Interpretation; Evidence.

Introduction

Given the reliance placed upon forensic science evidence as part of many criminal investigations (Reedy, 2020), it is imperative that any communicated findings are reliable (Reid and Howes, 2020). Achieving this often requires the deployment of techniques and procedures which facilitate the analysis and interpretation of whichever data-type is, or may be the assumed target of an inquiry, where these processes must be subject to robust evaluation (Casey, 2011). As part of any digital forensic science (DFS) investigation, a practitioner

will first spend time developing a DFS strategy which best suits the needs of the case in question (Reith et al., 2002), providing the most effective path for an investigation. 'Investigation-effectiveness' should not be considered a case of 'showing the suspect has done it' but instead, one where all available evidence that may prove or disprove any suspected event(s) is identified and interpreted correctly. This then leads to the '*correct*' case outcome - that a suspected offence subject to an inquiry is rightly proved, disproved, or that it is determined that insufficient information exists and this limitation is conveyed. This process is complex, where there are arguably two main general areas for potential concern when considering procedural quality assurance; the practitioner, and their tools. While the need for tool evaluation, testing and validation is an area with much emerging commentary (Marshall and Paige, 2018; Horsman, 2019; Tully et al., 2020), including guidance from the Forensic Science Regulator (FSR) (Forensic Science Regulator, 2020) in England and Wales, and the National Institute of Standards and Technology (NIST) (National Institute of Standards and Technology, 2019) in the U.S. this is a space which this work will not explore. Instead, to support the discussions raised here and for simplicity of argument, we will assume that the hypothetical practitioner is utilising tools that are performing and configured effectively. This leaves the practitioner, the second avenue of scrutiny and a focus of this work. As DFS practitioners are the ones who interpret and communicate the meaning of any potential digital evidence found as part of their examination, it is important they consistently do this right.

A practitioner will often commence any DFS examination of a suspect device by attempting to identify any potentially relevant data traces (example may include operating system artefacts which describe certain user behaviour, or logs showing how software applications have been configured) which may reside upon it. These data traces must then have their meaning and value in relation to a given inquiry interpreted (van Zandwijk and Boztas, 2021). This task is far from straightforward, requiring the practitioner to possess the relevant knowledge, experience and insight needed to determine the case-significance of a given data trace accurately. The failure to undertake this process correctly can have far-reaching consequences as a practitioner's interpretations are then often communicated to those who have commissioned a device's

examination, who in turn may make subsequent investigative decisions based upon this information. Decisions that are made following reliance upon a practitioner's potential evidence that is later found to be unreliable may have both financial and reputational consequences for all involved in the investigative process, as well as a potential impact on the liberty of the persons subject to investigation. As a result, the importance of a practitioner correctly forming judgements regarding data traces cannot be emphasised enough.

Interpreting the meaning of digital data is a complex and multifaceted process. When forming an interpretative opinion of a data trace, practitioners can generally operate in one of three main 'modes'; '*technical', 'investigative*' and '*evaluative*' (Willis et al., 2015; Forensic Science Regulator, 2021), where this work will focus on the formation of investigative opinions, what this means in practice and the ways in which it can be achieved. This work will discuss the process of forming an investigative opinion when underpinned through the reconstruction and testing of a suspect system, coined here as 'reconstructive testing'. Section 2 discusses what an investigative opinion is where Section 3 outlines a three stages approach to formalising the investigative opinion generation process. Finally, conclusions are drawn.

2 Investigative opinions

Following the deployment of their strategy, a DFS practitioner will in many cases be presented with pieces of digital information that *may* have relevance to their investigation (following *'tool hits'* - the results of any forensic software's automated search, file/data recovery or data parsing functionality), or identify such information following a manual system examination which they have conducted. Regardless of the method, at this point, the DFS practitioner is presented with what can be considered '*potential digital evidence*' - data that may be of value to the current inquiry but its relevance is not yet fully understood. Before this data can be deemed *actual* digital evidence within the remit of any current examination, its presence on a suspect device must be understood at a technical level, and its value to the inquiry must be determined, either as a form of inculpatory or exculpatory evidence. Once this process is complete, a practitioner may form an

'*investigative opinion*' of the data, where reference is drawn to the Forensic Science Regulator for clarity on what this means (Forensic Science Regulator, 2021 at p.7):-

> 'In investigative mode, experts generate possible explanations to account for their scientific observations'. In regards to the investigation of digital data which may have apparent relevance, ….sometimes we don't know something is relevant until we know everything about it. - we might form an investigative assumption. For example, keyword hit to a phrase...may seem relevant due to the context, but we need to know more about it before its classed as 'relevant'

Guidance regarding the formation of opinion has recently been provided by the Forensic Science Regulator (2021) in England and Wales to support those conducting this type of forensic work. An investigative opinion is created to explain an observation (Jackson et al., 2006; Jackson and Jones, 2009), where in noting the need to express any possible explanations for an observation, Jackson et al., (2014) highlight that it may not be possible to acknowledge every potential instance. Efforts to be as comprehensive as possible should be made. The formation of an investigative opinion arguably straddles the interpretation and evaluation stages of the typical DF investigative workflow where practitioners try to understand the underlying meaning of any identified content.

It is suggested that a practitioner can form an investigative opinion regarding any specific data found on a suspect device once they have undertaken the following two tasks:-

1. Interpret the technical meaning of the data as far as is possible (what it may be, where it could have come from and what process may be responsible for its presence on the system); then,
2. Determine the contextual value and investigative relevance of the data to the current inquiry.

These two tasks may seem deceptively simple, however, when their complexity is unpacked, the formation of an investigative opinion requires a methodological approach to ensure that any conclusions reached are reliable. When attempting to interpret the technical meaning of any potentially relevant data for the purpose of forming an investigative opinion in DFS, this task can arguably be achieved in three ways (Horsman, 2019b):-

1. *Past case precedents*: A practitioner can seek to rely upon how any specific data type has been interpreted in past cases (if such interpretations are known-good) and utilise this information to help form their investigative opinion in the current case. These past cases may be those which the practitioner has previously worked upon or external cases where access has been granted (providing in either instance, any previous investigative opinions have been formed robustly).

2. *Published and peer-reviewed material*: Where, published, peer-reviewed and accepted material documents the specific data type which is the subject of their current examination in relevant detail, a practitioner may seek to utilise this information to help form their investigative opinion in the current case.

3. *Testing*: A practitioner may seek to reconstruct and test the specific scenario surrounding the data type (i.e. try to recreate and understand the events which may have caused the data to be present on the suspect's system) in order to establish its potential meaning.

Focus here will remain on instances where the practitioner deems it necessary to undertake reconstructive testing as a method of interpreting potentially relevant data and form an investigative opinion of it.

2.1 The process

Before commencing the interpretive process for any given data trace, a practitioner must understand their role within an investigation. Where they are expected to report solely upon technical facts, then the formation of an investive opinion may not be appropriate. Similarly, the process of forming investigative opinions should not be confused with that of forming expert evaluative opinions. Therefore a practitioner must understand their remit and responsibilities and conduct their work in accordance with these, where both different organisations and jurisdictions may have specific requirements.

The proposed formalised process for forming an investigative opinion via reconstructive testing is outlined in Figure 1. As noted in Section 2, DFS practitioners often commence an examination of a suspect device with procedures designed to sift its resident digital data in an effort to highlight those specific data traces which may potentially support a given inquiry (Beebe et al., 2011; Horsman et al., 2014). This should be driven by a case assessment which determines the requirements of the case and investigating authority (Cook et al., 1998). For each potentially evidential data trace, to form an investigative opinion of it which is as a result of reconstructive testing, a three-stage process is proposed.

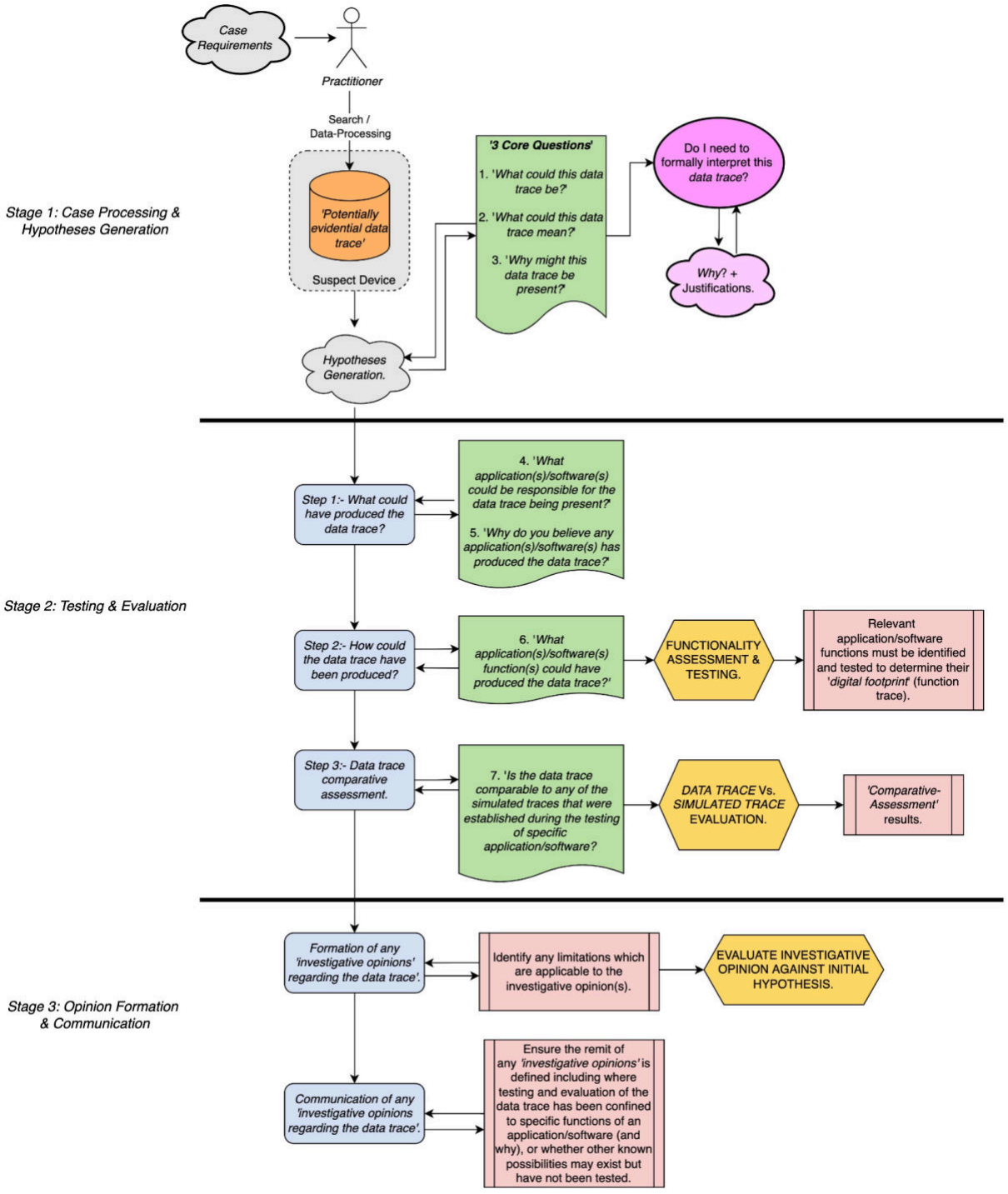


FIG 1 - Forming an investigative opinion system reconstruction and testing

2.2 Stage 1: Case Processing & Hypotheses Generation

It should be emphasised here that the proposed framework for the formation of an investigative opinion commences from the point at which data traces have been provided following the deployment of data acquisition and processing techniques. This work operates on the assumption that these stages have been undertaken effectively and appropriately in line with any inquiry undertaken, placing practitioners at the point in which they are ready to determine the potential relevance and value of any highlighted data trace. However, practitioners must be aware that if issues occur at these earlier stages, their ability to form a reliable investigative opinion of any data trace subsequently found may be impacted, for example if a chosen acquisition method is flawed or its ability misunderstood by a practitioner. In addition, poor investigative decision making and strategy development and bias are also a concern in relation to DF, and could lead to incomplete dataset being made available for review and interpretation by the practitioner (Sunde and Dror, 2019). When forming an investigative opinion of a data trace, it must not just be evaluated in isolation, any relevant procedural and case factors should also be taken into consideration.

Following processing procedures deployed on data extracted from any suspect device(s), all resulting outcomes (highlighted files, keyword hits etc.) require initial assessment by the practitioner to determine their potential investigative worth and whether it is necessary to examine them further. These instances are coined here as '*data traces*', and for each brought to the attention of the practitioner, an investigative hypothesis should be generated regarding their potential evidential value to the inquiry, and to determine whether they should be examined in further detail and how best to proceed with the examination of them. Information regarding what the data trace could be, what it could mean, and the act that created it may at this point be unknown, partially unknown or unavailable. It is also necessary to state that in some cases, a data trace type may be known to the practitioner where through past experience or knowledge they are able to explain its relevance and meaning, potentially negating the requirement for reconstructive testing.

At this stage for data traces that are not fully understood, the practitioner will deploy abductive reasoning as part of their hypothesis generation process given that only limited information may likely be known regarding the data trace or uncertainty exists (i.e. the data trace's current form and location on a suspect system) (Jackson, 2011; Walton, 2014). As stated by Jackson (2006 at p.36), 'abductive reasoning follows a process of generating likely explanations, testing these with new observations and eliminating or re-ranking the explanations...allowing the practitioner to reach their 'best bet' to explain the observations'. This approach commences with the generation of a hypothesis that may be the most logical or probable given the information which is known at the time and a practitioner's experience and knowledge may facilitate this process (Jackson, 2011; Walton, 2014). In any given scenario it is assumed that a practitioner will never be in a position of 'complete unknown' in relation to any given data trace, where even in cases of a 'data trace type' never being witnessed before, surrounding case information, experience and the ability to conduct preliminary research should provide the practitioner with the ability to form an initial hypothesis regarding what it could be and mean. This may be refined following the discovery of new knowledge following any testing.

To support the hypothesis generation process with regards to any data trace, practitioners, and where appropriate those involved in the wider investigation team, should consider an assessment of any data trace using the following three core questions:-

1. '*What could this data trace be?*':- A practitioner should first consider what the digital trace could be. In some cases, this may be straightforward (particularly in reference to known file-types), but this question becomes more difficult when offence-indicative data is identified in forms such as log files relating to software whose functionality is not well understood at the time of the examination by the practitioner, or forensic community. In these instances, an initial assessment (scoping research) of the software's purpose may inform the hypothesis generation process. Practitioners may derive initial hypotheses such as '*the data trace could be an internet history record*', or '*the*

data trace could be a record of the suspect device communicating with the victim X's device' taking into account the current state of the data trace and any of its available metadata. Or alternatively, whilst the practitioner may not have encountered the data trace before, they may seek to develop inferences regarding it from past experiences and knowledge that they might consider to be analogous or informative. In turn, it must be hypothesised that there may be multiple potential explanations for what a data trace could be, and each requires exploration in order to determine the viability of each. When considering what a data trace could be, a practitioner should observe the circumstances of the suspect device and information surrounding the data trace to inform the hypothesis generation process.

This is an obvious question at face value, and all practitioners to some degree will address this when they encounter a data trace, however, practitioners are encouraged to take a formal methodical approach to assessing meaning. The result of this assessment of meaning will directly impact upon later parts of the interpretative process as incorrect tools/processes may be selected if all potential meaning is not considered or a data trace is misunderstood.

2. '*What could this data trace mean?*':- A practitioner should consider all of the potential meanings that a data trace could have in relation to a given inquiry. A practitioner should consider that in some cases a data trace may have multiple meanings and therefore each may need to be evaluated. In doing this, a practitioner should take into account the type of data trace present and its location on a system. Consider an example of relevant data traces found in a web browser cache. Such data traces could mean the user viewed the image, that it has appeared on the screen (while scrolling in a browser for instance) or that the image may have been cache as part of a website visit but never have been seen by the user (Horsman, 2018). A failure to consider the viability of each meaning means that an incomplete opinion of a data trace may be offered which may compromise any inquiry moving forward.

3. '*Why might this data trace be present?*':- A practitioner should consider what could have caused the data trace to be present on the system. This includes not just what software/application may have created it, but also what specific functionality within it may have been responsible. This will also support a practitioner in determining point 2 above. In some cases, multiple acts can lead to a specific data trace being created, therefore meaning can not always be determined as 'singular', where operating under such a belief can lead to trace misinterpretation. A practitioner should consider and evaluate all (so far as is practical) potential digital actions which could be responsible for the presence of the data trace and how these scenarios might be tested.

   To establish why a data trace may be present on a system, a practitioner may need to conduct a wider investigation in regards to any suspect-system setup. This may include determining whether any similar or duplicates of the data trace may exist in other areas of the system which may support their interpretation of meaning, or if any additional metadata may be available which describes it. In relation to illegal imagery investigations, an example may include ascertaining whether thumbnail versions of any relevant imagery exist which may indicate how an image has been interacted with on a system. This may allow a practitioner to form a more robust opinion of the data trace and its presence by increasing their understanding of how the system has been interacted with.

When considering what a data trace could be, its meaning and the reason for its presence, practitioners should ensure both inculpatory and exculpatory considerations are given to ensure all possible interpretative avenues are explored. Further, a practitioner should also deliberate as to what a data trace could not be, and consider the impact of this upon any future work and opinion-generation process. By addressing the above three core questions a practitioner should be in a position to hypothesise as to the potential value that a data trace may have to the current investigative inquiry. At this point, the practitioner is required to determine

whether the data trace requires further exploration and all of the work required to form a robust investigative opinion of it, and therefore justify the time and resources which will be required to do this. Those data traces which are hypothesised as of potential value to an inquiry should proceed to Stage 2 of the investigative opinion formation process where testing and evaluation should be undertaken (discussed in Section 2.3).

It should be noted that in some cases, a practitioner may hypothesise that a data trace is unlikely to be of value to an inquiry, and opt to not explore it further. This is perhaps controversial given that such a decision occurs possibly before the full potential evidential remit of the data trace is fully understood, but is reflective of operational reality where often, not every piece of data will be scrutinised due to time and resource limitations (Pollitt, 2013). If large quantities of data traces exist (for example, consider the scenario where large numbers of keyword hits are returned following a search) a practitioner must prioritise which digital traces to explore further. Ideally, attempts to formally interpret all digital-traces present should be made, but in practice, this is not always feasible. Practitioners will often have to make a decision as to which digital traces are most likely to address the current investigative inquiry and therefore should be subject to formal testing and evaluative processes. Those which are deemed non-relevant may not be explored further, and justification for this decision should be documented. It is important to note that when assessing the value of a data trace, this should be done by considering it as both an inculpatory and exculpatory source of potential evidence. Those data traces which are hypothesized as likely relevant should proceed to Stage 2 of the investigative opinion process.

2.3 Stage 2: Testing & Evaluation

Stage 2 is designed to test those hypotheses generated in Stage 1 regarding any specific data traces, requiring the practitioner to establish valid conclusions based upon both available facts, and through undertaking reconstructive testing. Reconstructive testing involves the systematic exploration of any application/software found on a suspect device and its associated functions, which is speculated as being

responsible for the presence of a specific data trace or linked to it, in order to ascertain how it operates and any digital footprint it creates following its use. This includes an evaluation of any specific functions of any application/software which is suspected as being linked with the data trace following user interaction or via any autonomous functionality that it may possess. Any testing should be conducted under the same conditions found to be present within the actual suspect case (same operating system, same version of software etc.).

The goal of reconstructive testing is to engage relevant functions of any software/application believed to be responsible for the data trace found on the suspect system, in a test environment in order to create '*simulated traces*'. A simulated trace is defined by Jaquet-Chiffelle and Casey (2021 p.9) as 'a special case of Tangible Trace where the Event of interest is provoked by the scientists in a controlled environment and can be repeated.'. These simulated traces are then evaluated and compared with the suspect system data trace in order to ascertain whether any tested software/application may have been responsible for it - a comparative analysis of both traces is performed. For clarity, both the terms 'data trace' and 'simulated trace' are defined.

> *Data trace*: The term data trace has already been acknowledged in Section 2.2, however for clarity and formal definition, it refers to any piece of data or file (often found on a suspect's seized device) which may have the potential to be of value to the investigative inquiry taking place. Data traces require evaluation and interpretation before their evidential value can be known.

> *Simulated trace*: The term simulated trace refers to the digital data generated and stored on a system under test conditions following the execution of a specific function from a specific application/software during the process of reconstructive testing. Effective testing may allow simulated traces to be attributable to a specific, or subset of an application/software's functions.

Whilst a practitioner may seek to develop an investigative opinion subconsciously with regards to the value of a data trace found on a suspect device and what it could mean, it is suggested that this reasoning process be formally defined and followed to prevent or reduce the chance of systematic errors occurring. It is important that investigative opinions are not generated from unsound information or in some cases no information at all - a '*hunch or guess*'. Similar concerns include the 'overwhelming evidence principle' - *everything points at outcome A, and therefore that must be the result*, and finally, unfounded conclusions - '*I just know that's what it means*'. Even if such approaches lead to the correct investigative opinion of a data trace, the value of this evidence is at risk of being undermined if thorough scrutiny of the practitioner's reasoning highlights that it is based upon such non-rigorous interpretive processes. The formation of an investigative opinion must be based upon reliable and methodical processes and principles which have been deployed in a way that allows a rigorous assessment of any potentially relevant data trace, and this should be evidencable. Formalising the investigative opinion generation process helps to guard against bias (Sunde and Dror, 2019), by preventing a practitioner from concluding upon a data trace without evaluating the reliability of their processes first, as unsafe case outcomes can be reached via poorly defined and deployed methodologies.

In Stage 2, practitioners will face three steps as part of the process of testing their initial hypotheses regarding any data trace found during their examination of a suspect device. These are outlined as follows:

Step 1 - What could have produced the data trace?:- The 'producer' of the data trace here refers to the software/application present on a suspect device that could have been or is suspected to be responsible for the data trace being produced and present on a suspect system. For example, where data trace *D* is found in application *A's* app folder on mobile *M*, *A* may be initially considered the producer of *D* on *M*. In order to begin to interpret the meaning of any data trace, establishing what may have produced it is a fundamental first step. A practitioner will begin by assessing the location of the data trace on the suspect system where

in some cases it may reside within regions known to be attributable to a specific piece of software or application. In such cases, the practitioner may suspect the software/application as being the producer of the data trace and may proceed to evaluate if it could have produced it and how - discussed in Step 2. Practitioners who are uncertain as to what may have produced a specific data trace may proceed to identify multiple viable 'producers', where each may require exploration.

Finally, it may not be possible to establish a potential producer of a data trace, a particular challenge with data traces that are present in areas such as unallocated space. In these cases, it may not be possible to proceed with the reconstructive testing process as insufficient knowledge may be available from which to base a reconstructed scenario, where an almost endless amount of possibilities may exist. As a result, a practitioner may offer an investigative opinion that is based upon the limited available data trace information and suggest possible hypothetical reasoning behind its existence. Here a practitioner may also proceed to reconstruct a hypothetical scenario based purely on their knowledge and experience in order to demonstrate a potential possible technical reason for the data trace's presence. However, in such cases, it is important to ensure that the limitations of this form of investigative opinion and the assurances which can be placed upon it are effectively communicated and that it is treated with caution as such acts amount only to speculation, yet may still have informative value.

Given the time and resources required for effective reconstructive testing, a practitioner should evaluate their belief that a certain application/software is a producer of a potentially relevant data trace, and ensure that their decision is reliability underpinned and justifiable. Once all potential producers are identified, a practitioner should seek to determine which of their functionality may have led to the data trace's production - Step 2.

Step 2 - How could the data trace have been produced?:- Any software/application identified as a suspected producer of a relevant data trace during Step 1 must have its functionality evaluated. The practitioner must

address the question - '*what application(s)/software(s) function(s) could have produced the data trace?*', and to do this, the software/application must undergo a '*functionality assessment*'. A functionality assessment involves identifying what any producer software/application can do in terms of functions available to the user, what this means in terms of a 'digital course of conduct' and how any user of it can engage them. A practitioner must consider both surrounding data trace metadata and the circumstances of the given case in order to evaluate which functionalities could be responsible for the data trace and therefore require testing and evaluation. This includes determining what activity type and level may have been engaged by the suspect and the likely corresponding function (Henseler and de Poot, 2020), for example, whether a function is engaged via a deliberate button press/device integration, or whether activity is gathered passively.

The complexity of many software/applications means that it will not be feasible to test every function that a piece of software/application offers its users, therefore in some cases, the practitioner will be required to make a strategic assessment as to which functionalities are likely to create a simulated trace comparable to the data trace found on the suspect system. This decision should be based on any initial considerations of the structure of the original data trace that a practitioner may have, reference to the suspect actions from which the inquiry concerns, and surrounding case intelligence. For example, if a suspect is believed to have downloaded specific content, then functions that provide a user with the ability to download content may be considered a primary focus for reconstructive testing. Where it is not possible to identify a specific function, a full system test may be required, where each application/software function is systematically tested.

Following a functionality assessment, the practitioner must seek to engage those functions identified as potentially responsible for producing the data trace on a suspect device. The aim is to simulate those functions in-use, in an environment comparable to that of the suspect device where the suspect data trace originated from, in order to generate a 'simulated trace' (defined in section 2.3) which is attributable to a

specific application/software function. For those suspected producer software/applications, available setup and configuration information should be ascertained from the suspect system in order to support the construction of the testing environment. The design and deployment of effective reconstructive testing environments in DFS is a complex task, where support and in-depth discussion as to approaching this task is offered by Horsman (2019b) as this work does not intend to cover how to test appropriately - this is a separate topic. When reconstructive testing, it is not always necessary to mimic the exact substance of the data trace found on the suspect system (i.e. send the exact same text, download the exact same picture when testing etc.), where the validity of the test process lies with engaging the function in the same way procedurally. For example, where a data trace is suspected to be generated from application 'A' downloading a file, reconstructive testing should focus on 'A's' download function and how to exhaustively test it. Comparable test data (format, size etc.) in most cases will be sufficient to generate a reliable test case.

Following the completion of reconstructive test processes, both the original suspect data trace and any generated simulated traces must be compared and evaluated - this is Step 3.

Step 3 - data trace comparative assessment (DTCA):- A DTCA attempts to address the question - '*is the suspect data trace comparable to any of the simulated traces which were identified during the testing of a specific application/software and its functions?*'. This process involves an evaluation of both the data trace and the simulated trace, followed by a comparison of their data structure. A comparative assessment of the data trace and the simulated trace is a task that requires a methodical approach to be adopted, where the practitioner must also determine what comparative criteria they will use as part of the DTCA. The result of any DTCA can lead to the following outcomes.

Match: It is suggested that as a minimum, both the data trace and simulated trace must have comparative metadata and be structurally similar if they are considered to be a viable match. For each match (i.e. both

trace-types have comparable metadata and structure), the practitioner may consider that it is technically conceivable within the current digital scenario depicted on the suspect device that a data trace could have been created by the 'producer' software/application identified and the specific function which was tested and responsible for the comparable simulated trace. Establishing a trace-match is not always straightforward due to the complexity of many applications where interpretative inconsistencies may result in some scenarios (Forensic Science Regulator, 2020).

No-match: It is important to note that an investigative opinion is not just formed regarding what a data trace could be, but also what it may unlikely be - a '*no-match*' scenario. A no-match describes a situation where the data trace and simulated trace do not share comparable metadata and structure, either in part or full. If both trace-types do not share comparable characteristics a practitioner may proceed to form an investigative opinion that addresses what a suspect data trace is unlikely to be or mean.

Following all DTCAs a practitioner can begin to construct and communicate their investigative opinion.

2.4 Stage 3: Opinion Formation & Communication

Stage 3 focuses on the formation of any 'investigative opinion' regarding the data trace following the underpinning work carried out in Stage 2. As noted above, an investigative opinion is an explanation for a given observation (Jackson et al., 2006; Jackson and Jones, 2009; Jackson et al., 2014) - here, an explanation as to what a data trace may (or may not) be and mean, within the context of the inquiry, given attempts to reconstruct those actions which may have been responsible for its presence on the suspect system, and what a practitioner has learned from this process. In formulating their investigative opinion, the practitioner should evaluate their findings against their initially generated hypotheses in Stage 1. The practitioner must also clearly outline any limitations of the processes undertaken as part of the formation of the investigative opinion, including limitations in testing and those functionalities/scenarios which have not been explored, and why. If reconstructive testing for a specific data trace has not been possible (either due to the nature of

the trace or lack of available resources), this must be declared. The practitioner must evaluate any limitations and determine the impact these may have on their ability to formulate their investigative opinion regarding a specific data trace. It is important to enforce that the investigative opinions not only provide explanations for a possible cause and meaning of a data trace on a system but also potentially rule out certain causative actions. This process can lead to the formation of opinions that may describe both what a data trace could be and mean, as well as determine what it is unlikely to be and mean.

When communicating an investigative opinion, the practitioner must ensure that it is clear how the investigative opinion has been formed (Tart, 2020), where in the case of reconstructive testing, those formal methodologies deployed must be described either in any report formally, or be documented in any contemporaneous notes and be available for scrutiny if requested. Therefore emphasis is not only on how the opinion itself is communicated but also on how the practitioner has arrived at such a position.

3 Conclusions

This work has offered a formal methodology for the use of reconstructive testing to support the formulation of an investigative opinion in DFS in relation to suspect device data traces. Investigative opinions are frequently used by practitioners in DFS to convey the possible meaning and value of any potentially relevant data traces found as part of their examination of suspect devices. For quality assurance purposes, this process requires formalisation to ensure consistency in the formation of these opinion-types when testing is deployed and to ensure that they are procedurally valid and evidentially sound. It is suggested that the 3 Stage approach outlined here offers support and guidance to practitioners when undertaking this work by transparently defining those tasks which a practitioner should look to engage with if they are to reach an investigative opinion where testing has been involved, which is procedurally robust and scientifically valid.

It must be noted that the suggested approach here is a guide for practitioners, where the effective formation of robust investigative opinions still relies upon the practitioner and their technical and investigative ability

to construct effective testing and interpretation in the field of DF. This work aims to bring structure to the investigative opinion formation process but it cannot misinterpretations of data from occurring due to limitations in a practitioner's knowledge and ability. Future work is required to evaluate practices currently deployed by practitioners when forming investigative opinions in order to ascertain and evaluate these processes, develop best practices and identify any areas of concern.

References

Beebe, N.L., Clark, J.G., Dietrich, G.B., Ko, M.S. and Ko, D. Post-retrieval search hit clustering to improve information retrieval effectiveness: Two digital forensics case studies. Decision Support Systems 2011; 51(4):732-744.

Casey, E. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011.

Cook, R., Evett, I.W., Jackson, G., Jones, P.J. and Lambert, J.A. A model for case assessment and interpretation. Science and Justice 1998; 38(3):151-156.

Forensic Science Regulator. 'Forensic Science Regulator Guidance Method Validation in Digital Forensics' 2020 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

Forensic Science Regulator. 'Forensic Science Regulator Codes of Practice and Conduct Development of Evaluative Opinions' 2021 Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/960051/FSR-C-118_Interpretation_Appendix_Issue_1__002_.pdf'

Henseler J. and C.J. de Poot. The Potential of Digital Traces in Providing Evidence at Activity Level 2020 Available at: https://dfrws.org/wp-content/uploads/2020/06/2020_USA_pres-the_potential_of_digital_traces_in_providing_evidence_at_activity_level-1.pdf

Horsman, G. Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. Computers & Security 2018; 73: 294-306.

Horsman, G., Laing, C. and Vickers, P. A case-based reasoning method for locating evidence during digital forensic device triage. Decision Support Systems 2014;61:69-78.

Horsman, G., 2018. I didn't see that! An examination of internet browser cache behaviour following website visits. Digital Investigation, 25, pp.105-113.

Horsman, G. Tool testing and reliability issues in the field of digital forensics. Digital Investigation 2019; 28: 163-175.

Horsman, G. Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. Digital Investigation 2019b; 28:146-151.

Jackson, G., Jones, S., Booth, G., Champod, C. and Evett, I.W. The nature of forensic science opinion--a possible framework to guide thinking and practice in investigations and in court proceedings. Science & justice: journal of the Forensic Science Society 2006; 46(1):33-44.

Jackson, G. and Jones, P.J. Case assessment and interpretation. 2009; Wiley encyclopedia of forensic science.

Jackson, G. The Development of Case Assessment and Interpretation (CAI) in Forensic Science 2011 (Doctoral dissertation, University of Abertay Dundee).

Jackson, G., Aitken, C.G.G. and Roberts, P. Case assessment and interpretation of expert evidence: guidance for judges, lawyers, forensic scientists and expert witnesses. 2014; Royal Statistical Society.

Jaquet-Chiffelle, D.O. and Casey, E., 2021. A formalized model of the Trace. Forensic Science International, 327, p.110941.

Marshall, A.M. and Paige, R. Requirements in digital forensics method definition: Observations from a UK study. Digital Investigation 2018; 27: 23-29.

National Institute of Standards and Technology. 'Computer Forensics Tool Testing Program (CFTT)' 2019 Available at: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

Pollitt, M.M. Triage: A practical solution or admission of failure. Digital Investigation 2013; 10(2): 87-88.

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

Reedy, P. Interpol review of digital evidence 2016-2019. Forensic Science International 2020: Synergy.

Reid, C.A. and Howes, L.M. Communicating forensic scientific expertise: An analysis of expert reports and corresponding testimony in Tasmanian courts. Science & Justice 2020; 60(2):108-119.

Reith, M., Carr, C. and Gunsch, G. An examination of digital forensic models. International Journal of Digital Evidence 2002; 1(3):1-12.

Sunde, N. and Dror, I.E. Cognitive and human factors in digital forensics: problems, challenges, and the way forward. Digital investigation 2019; 29:101-108.

Tart, M. Opinion evidence in cell site analysis. Science & justice: journal of the Forensic Science Society 2020; 60(4):363-374.

Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R. and Watson, T. Quality standards for digital forensics: Learning from experience in England & Wales. Forensic Science International: Digital Investigation 2020; 32:200905.

van Zandwijk, J.P. and Boztas, A. The phone reveals your motion: Digital traces of walking, driving and other movements on iPhones. Forensic Science International: Digital Investigation 2021; 37:301170.

Walton, D. Abductive reasoning. 2014 University of Alabama Press.

Willis, S.M., McKenna, L., McDermott, S., O'Donell, G., Barrett, A., Rasmusson, B., Nordgaard, A., Berger, C.E.H., Sjerps, M.J., Lucena-Molina, J.J. and Zadora,G. ENFSI guideline for evaluative reporting in forensic science. 2015; European Network of Forensic Science Institutes.

Forming an investigative opinion in digital forensics

Horsman, Graeme

2022-05-09

Horsman G. (2022) Forming an investigative opinion in digital forensics. WIREs Forensic Science, Volume 4, Issue 6, November/December 2022, Article number e1460
https://doi.org/10.1002/wfs2.1460