Science & Justice, Volume 63, Issue 1, January 2023, pp. 116-126
10.1016/j.scijus.2022.11.004

Digital evidence strategies for digital forensic science examinations

Abstract
Given the size and complexity of many digital forensic science device examinations, there is a need for practitioners to formally and strategically determine a course of conduct which allows them to undertake the most robust and efficient examination possible. This work outlines both the need for practitioners to have a digital evidence strategy (DES) when tackling any given examination scenario, how to construct one and the concerns which exist when no formal DES is in place. Approaches to DES development are examined and the context to which they should be deployed are analysed, with focus being on the use of DESs at the *examination/processing* stage of the investigative workflow. Finally, a 'DES skeleton' is offered to guide practitioners as they seek to create their own DES.

Keywords: Digital Evidence; Strategy; Examination; Digital Forensics; Investigation

1 Introduction
It is well recognised that through increased ownership of, and engagement with technology, digital data now describes in detail many events in a device owner's life [1]. As a result, there is increasing reliance placed upon the data stored on digital devices as part of many criminal investigation processes by criminal justice systems due to their investigative inquiries [2][3][4]. Those involved in the investigation of crime where digital devices are suspected to contain pertinent information are tasked with extracting, sifting and interpreting device-content in order to ascertain whether inquiry-relevant data exists. This is traditionally done in digital forensic units (DFUs) or via outsourcing private sector organizations by specialist practitioners, however we are now witnessing an expansion of these responsibilities to roles which exist on the forensic-periphery, including front line police and crime scene investigators who are now performing preliminary digital-device examinations [5]. This is demonstrated with the use of so called 'cyber-kiosks' for mobile phone extraction and examination [6]. Regardless of the position, the task of examining a digital device is far from straightforward due to both the complexity of the device's data, and the large (and increasing) volume of it [7].

Digital evidence has now affirmed itself as a core evidence-type for criminal investigators to utilise as they seek to understand suspect behaviours in many cases. As a result, it should come as no surprise that a growing need for digital forensic science (DFS) device examinations [3] has led to well publicised backlogs and case delays [8][9] with the College of Policing noting that the examination of digital devices is often a primary reason for long bail times being granted [10]. Coping with this demand requires a combination of effective resourcing, and effective resource deployment. Effective resourcing requires sustained and appropriate investment, a discussion which is reserved for governmental authorities [11] where some advancements and acknowledgement have been made in England and Wales [12][3]. Effective resource deployment requires the use of investigative strategies that are designed to ensure all available resources are both effectively and efficiently utilised - a focus of discussions here.

1.1 Strategy & digital forensic science
Although it may be considered the job of any practitioner, analyst or officer to examine all data present on a device they are tasked with investigating, in many cases this approach is neither feasible or conducive to efficient case management [13]. Many devices can contain hundreds

Published by Elsevier. This is the Author Accepted Manuscript issued with: Creative Commons Attribution Non-Commercial No Derivatives License (CC:BY:NC:ND 4.0).
The final published version (version of record) is available online at DOI:10.1016/j.scijus.2022.11.004. Please refer to any applicable publisher terms of use.

of thousands of files, where many may bear little or no evidential value [14]. In contrast, data which is pertinent to an inquiry may often form only a small subset of the entire contents of a device, with identification of this dataset important to the success of the investigation [14]. Whilst the methodological processing of every single piece of data on a device is likely to yield high success rates of pertinent data identification, it is a practice that in many cases would take too long to undertake, impacting upon the delivery of effective justice within a requisite time frame. Despite such a statement appearing controversial, it is arguably reflective of the challenge faced by the DFS field as it seeks to balance the competing interests of undertaking thorough and robust forensic examinations against the needs of a criminal justice system and its requirement to be economical. As a result, strategic examination approaches are arguably preferable and needed for quality assurance and maintenance.

If we consider a hypothetical and generic high-level DFS investigative workflow, the following stages typically exist:- *data acquisition, examination/processing, analysis and interpretation*, and finally, the *communication of findings* [15][16]. Each stage maintains its own complexities, however one of the greatest challenges faced by those investigating digital devices lies at the *examination/processing* stage - where data is sifted in pursuit of relevant content. It is here that strategic decisions are made in regards to how to process the contents of a device, consisting of '*where to look*', and '*what to look for*', whilst managing the risk of potentially missing relevant content vs. the need for timely results. This task is sometimes referred to as '*data-screening*' [17], with the process sharing a similar purpose to that of triage [18], and is done in an effort to try and highlight only data which a practitioner is likely to interpret as being of value to a current inquiry.

If we consider that a practitioner may not have the time or resources to examine a device in its entirety (arguably a task which is becoming less feasible to consider) [19], then decisions must be made which define how a practitioner is to pursue finding inquiry-relevant data on a device within a suitable time frame [20][21][22]. In 2007, the Association of Chief Police Officers [23, p.1] stated that 'a digital evidence strategy must form an integral part of the wider investigative process', and it should outline those investigative processes that a practitioner intends to undertake following robust planning and evaluation. These procedures are the backbone of the forensic examination process, as failure to identify relevant content at this stage may mean that such information may never be discovered and taken into consideration as part of an interpretation of any alleged offence. The need for strategic approaches to device-investigations remains great where *ad hoc* approaches may lack the necessary rigour required to guarantee acceptable case outcomes.

In any criminal scenario, investigative decisions carry an inherent risk in regards to their impact on case outcomes and therefore the quality of these must be evaluated and their impact managed, if possible. DFS examinations are no exception, where it is important that any investigative decision making is underpinned with robust information, technical understanding and justifiable motivation. In all cases, those conducting an examination of a digital device (or multiple) in line with a given inquiry, should only do so following the development of a digital evidence strategy (DES) which defines how an examination is to be conducted and the reasons for doing so. Such investigative strategies are designed to maximise evidence recovery and reduce error [24], with ACPO confirming this importance.

> '*It is important that investigators develop appropriate strategies to identify the existence of digital evidence and to secure and interpret that evidence throughout their investigation*' [21, p.9].

The need for, and development of appropriate crime investigation strategies has long since been acknowledged by law enforcement, where founding examples of guidance for supporting this process include the National Centre for Policing Excellence's [47] 'Murder Investigation Manual. Yet arguably, in relation to inquiries involving digital devices and data specifically, there is currently less formal guidance available for those conducting these investigations to support the construction of an investigative strategy. Despite the requirement for DESs and the important role they should play in the undertaking of effective DFS examinations, there arguably remains limited dedicated literature and formalised guidance discussing their function, development and deployment. As a result, the quality and use of DESs in practice may be widely divergent or in worst-case scenarios, absent from the investigative workflow, raising questions about quality assurance and control mechanisms. This work outlines both the need for practitioners to have a DES when tackling any given examination scenario and the concerns which exist when no formal DES is in place. Approaches to DES development examined and the context to which they should be deployed are analysed, with focus being on the use of DESs *examination/processing* stage of the investigative workflow. Finally, a 'DES skeleton' is offered to guide practitioners as they seek to create their own DES.

2 What is a 'Digital Evidence Strategy'

As per ACPO -

> 'Due to the volume and complexity of data stored on digital devices, it is not possible or desirable to extract all data held on a device for review by investigators. Instead, a forensic strategy needs to be formulated to enable the examination to be focused on the relevant data' [21, p.11].

It is important to recognise that in many cases, the forensic examination of a digital device must not just be effective, but also efficient - i.e. any results must be produced within a time frame that fits with the requirements of the wider investigative process, particularly where court deadlines are set [19]. This trade-off arguably provides an uncomfortable conflict of interest as many will agree that quality should never be compromised in pursuit of speed or quantity of output, particularly given the gravity of forensic evidence and the subsequent reliance which is often placed upon it. However operational-reality requires an acceptable balance to be struck. The delivery of effective and efficient DFS examinations is, and will remain a challenge for those involved in this field, where it is recognised that in some cases there may not be any viable technological '*quick fixes*' or '*go to's*'. Tools which go beyond data-gathering, parsing and display, and actively support data interpretation are arguably a future goal, where machine learning and AI techniques are beginning to be explored [25]. However, we are not yet in a position to rely solely on such computational methods for improving examination quality and productivity, and therefore many of the traditional methods for processing data in a DFS examination (keyword searching, file identification & recovery etc) will continue to be a staple of the investigative workflow.

Achieving high-quality DFS examinations is arguably only partially dependent on the tools which are used, where greater impact stems from the ways in which an investigating

practitioner deploys their tools. In essence, having specific capability afforded by a tool does not guarantee a satisfactory case outcome, rather, this is often dictated by how the practitioner chooses to deploy this capability. For this reason, it is suggested that greater emphasis needs to be placed on the development of strategic investigative approaches which define how a practitioner should or intends to carry out their examination from the outset, within each specific case scenario. If we consider that finite resources may be available, prior planning and the evaluation of all available and relevant information can support the practitioner to strategically determine a pathway for undertaking the most robust and efficient examination possible. This approach advocates that practitioners outline a DES for each case they are involved in.

The Oxford Learner's Dictionary [26] defines a strategy as '*a plan that is intended to achieve a particular purpose*' where in the context of a criminal inquiry where one or more digital devices are involved and subject to examination, strategy-development is a complex task. It is argued that practitioners must develop a DES prior to commencement of any formal DFS examination processes, where here, a DES is defined as.

> '*An agreed, defensible, and dynamic plan that identifies those investigative actions which are deemed both proportionate and necessary to establish the potential existence and meaning of any available and relevant digital information that can assist with any/all reasonable lines of inquiry. This plan must define and justify the scope of any investigative actions, outline all known procedural limitations and risks which could impact upon the success of a case outcome and how they will be managed/mitigated, along with consideration of applicable legal, ethical and professional factors.'*

Given the importance of the role that DESs should play, this definition requires unpacking, where it is necessary to highlight its key elements.

2.1 'Agreed, defensible, and dynamic'

Any DES should have the following three fundamental traits.

Agreed: A DES must be agreed by all parties that are involved in the forensic examination of any digital devices, and by those who form part of the wider investigative team [23]. In some cases, this process may be straightforward, particularly where the DES is collaboratively constructed by all parties, and therefore explicit awareness naturally exists. As the conduct of the DFS practitioner directly impacts those seeking the results of their examination, it is important that those commissioning the forensic work are aware of those tasks and investigative directions being pursued, and the reasons which underpin them. In essence, the DES must meet the requirements of the client. Therefore the practitioner is under an obligation to develop an appropriate DES and communicate its remit and implications to the surrounding investigatory team prior to it being deployed [23]. Regular communication between the DFS practitioner and those appropriate persons is important at all stages of the investigation workflow and a DES must not just be agreed at the outset, but remain in a state of agreement throughout the investigation. Therefore where changes in examination direction may be considered, communication of these proposals must be made and justified, and agreement must be sought, it cannot be considered to be implied [21].

Defensible: Any DES should outline the course of investigative conduct which is to be taken by the practitioner and therefore this conduct must be defensible if questions arise regarding its appropriateness. As part of defending a DES, it must be transparently defined and available for scrutiny by others if and when required.

Dynamic: Any effective DES must be one which can adapt to changes and investigative direction brought about through the discovery of new case knowledge, as and when this may occur. DESs are created at the outset of an investigation where at this stage often only a subset of case-relevant information is known and utilised to inform its development. As a result, as any examination progresses and a practitioner's understanding of the scenario improves, it may be appropriate in some instances to deviate from an originally planned investigative course of conduct in order to achieve a suitable case-outcome [27]. This need for flexibility is acknowledged by ACPO [21].

> 'The forensic strategy should be regularly reviewed to take account of any changes in the direction of the investigation, which may occur as a result of digital forensic examination (for example, finding emails identifying a co-conspirator) or investigations elsewhere (a witness identifying another person as being of interest to the investigation)' [21, p.11].

A DES must consider how any changes to the originally planned investigation may be handled and communicated appropriately.

2.2 'Investigative actions'

In reference to '*investigative actions*', this includes all actions which a practitioner or those part of the investigating team consider appropriate (see section 2.3 for a discussion on 'proportionate and necessary') in order to ascertain the presence of any data which may be evidential. It is at this point where it must be considered that any DES must take into consideration which stages of the investigative workflow it is designed to govern. For simplicity, DESs are likely to be required in two contexts - '*at scene*' and '*in lab*'.

At scene: Any 'scene' where an inquiry is taking place requires a DES to ensure all available digital investigative opportunities are accounted for and where it is deemed appropriate, collected and/or subjected to forensic examination (either there, or through submission into the investigative process) [28]. Where scene attendance is predetermined, the development of a DES may be easier, allowing preemptive measures to be taken and subject to thorough scrutiny and refinement. Whilst in many cases a DES will not be able to account for all potential eventualities, preemptive development can ensure that many use cases are prepared for. Yet, not all criminal inquiries are planned, where some may be ad-hoc. In such instances, requiring the impromptu development of a DES, where those at scene should on arrival be continuously assessing for evidential opportunities [29].

The development of *at-scene* DESs is not the focus of this work.

In-lab: DESs for in-lab device examination may cover stages including device acquisition through to reporting, however the focus of discussions in this work will remain on DES developed for the examination/processing of data on a device. In this capacity, a DES must define those 'investigative actions' which are appropriate for use in the identification of any

relevant digital data which may be stored on a device and those actions designed to carry out this task. Often investigative actions involve the use of computational techniques which are designed to identify relevant digital data structures and types which a practitioner will then proceed to evaluate and interpret their value in regards to the given inquiry. Any DES must outline which investigative actions are being deployed and why.

2.3 'Proportionate and necessary'

A DES must consider the impact that those actions defined within it could have upon those subject to, or part of the wider investigation. DFS examinations are intrusive by their nature and therefore managing their impact upon those involved should be considered an important function and purpose of a DES. A DES must describe actions which are both proportionate for any inquiry for which it relates to [21], and that these actions are necessary in order to achieve an effective case outcome. This is a challenge for the development of a DES as the extent to which an investigation may be required to pursue may not always be known from the outset. Therefore DES development must operate incrementally through a series of hypothetical '*locked gates*', exposing any suspect to more invasive processes incrementally, where the need to do so is evaluated and deemed necessary. This approach prevents the '*overprocessing*' of data from occuring, helping to preserve the privacy of those involved where possible. In addition, only deploying proportionate and necessary processes helps to ensure available resources are used efficiently and not deployed superfluously.

2.4 'Potential existence and meaning'

The proposed DES definition also emphasises that the practitioner/investigation team must plan for both establishing the existence of potentially relevant data, and for proceeding to determine its meaning. In all cases, before any digital-trace found on a device can be considered relevant to an inquiry, it must be understood as to what it is, and its context. Therefore a DES must not just focus on finding potentially relevant information, but also set out how the value of this information is to be determined and how this may govern or influence any further line of inquiry. This interpretation process may occur at both a technical level (what is the data and why is it present on a system? etc.) and at the investigation level (what does this data mean in regards to our inquiry?). Further, a practitioner must consider the client's expectation and whether they are considering reporting at a technical, investigative or evaluative level [30]. Collaboration between all members of the investigating team 'will ensure that the significance of any reviewed data is not misunderstood. For example, when reviewing keyword hits which exist in deleted files, the significance of a hit's location may need explanation from a digital forensic practitioner.' [21, p.12].

2.5 'Any available and relevant digital information'

As per ACPO:-

> 'It is not practically possible to examine every item of digital data and clear tasking is needed to ensure that the digital forensic practitioner has the best chance of finding any evidence which is relevant to the investigation' [21, p.11].

A DES must plan to acknowledge any digital evidence sources (devices, service provider retained data etc.) and assess their availability and relevance. In terms of availability, a DES must determine from the outset whether the digital data/source is actually available for investigation, both physically and legally, before pursuing a course of conduct which may

ultimately be resource-wasteful. In turn, the DES must set out practices for determining the relevance of any digital information prior to it being subject to any investigative process [31]. All efforts should be made to ensure non-relevant information remains outside of an investigation, not only as an examination of this content is a waste of available resources, but also leads to potential unnecessary privacy intrusion [32]. In all cases, a DES will aim to identify all available data which is of potential evidential value, but achieving this in reality in all cases is unlikely. It is unlikely that all DESs will be 100% effective in all cases, but they should aim to be. In some cases, the identification of 100% of available information may not be required in order for events to be ascertained, therefore where prosecuting thresholds exist, these must be understood and it made clear if they have been met.

2.6 'Can assist with any/all reasonable lines of inquiry'

What is a reasonable line of inquiry is a matter to be determined by the investigation team [33], where both initial lines of inquiry to be pursued must be considered, and those which may become apparent as a result of further investigatory work. An 'investigator needs to properly consider the nature and purpose of the digital examination. The investigator must be clear on what priorities are placed on the examination as it may well be that key information needs to be found in order to preserve evidence that may exist elsewhere' [21, p.11]. The investigating team also need to be aware of any legal obligations which they are subject to when considering all reasonable lines of inquiry (see for example, the Criminal Procedure Rules Part 19 for those operating in England & Wales). A DES must consider the potential existence of both inculpatory and exculpatory information, and outline strategies which evidence the consideration of both.

Practitioners are under an obligation to examine devices for both exculpatory and inculpatory evidence, regardless of their position or role (prosecution/defence). Examination techniques must not just focus on identifying data which sits within one of those categories, and instead, screening must be deployed in a way which will identify any case-relevant material which may be present. Failure to do this through poor data-processing results in an ineffective investigative process and potential miscarriages of justice. There are many factors which can impact a practitioner's ability to develop effective data-processing approaches including cognitive bias [34][35], where formal structured guidance may help to try and mitigate such risks.

2.7 'Define and justify the scope of any investigative actions, outline all known procedural limitations and risks which could impact upon the success of a case outcome'

A DES must address the scope of the work - what will the investigation physically do, and justify any processes. Conversely, where there are known factors which may limit the success of an investigation or pose a risk to it, the DES must acknowledge these and outline how they will be managed/mitigated, if possible. In addition, such limiting factors must be accepted by the investigating team before the DES is brought into action.

2.8 'Consideration of applicable legal, ethical and professional factors'

Finally, any DES must consider the legal, ethical and professional implications of the actions which it sets out [36] and how it will operate within a suitable space. Advice from available legal teams should be sought to confirm that any defined actions are lawful. Organisational best practices and government guidelines may outline acceptable conduct in terms of ethical

and professional considerations, and adherence should be sought and evidenced in all instances.

A DES is a deceptively simple concept which when fully appreciated requires both time and effort to be instigated if it is to play an effective role. The importance of a DES cannot be understated as they act as the underpinning quality assurance structure for DFS examinations to be built upon, where this can only be fully appreciated when the implications of conducting investigatory work without a DES are considered.

3 When you don't have a formal digital evidence strategy

In 2012, Garfinkel et al., [37, p.50] stated that 'the dramatic growth of storage capacity and network bandwidth is making it increasingly difficult for forensic examiners to report what is present on a piece of subject media'. Almost 10 years later, this challenge remains. A DFS practitioner's primary task is to identify content on a device which is relevant to a given inquiry. If we assume that in many cases, it is unlikely that the DFS practitioner will be in a position which permits them to examine every file on a device (for example, if there are deadlines which must be met), then whether they formally recognise it or not, they are strategically determining where on a system to look, and what to look for. It may be common for practitioners to subconsciously decide upon these factors, taking influence from case intelligence and experience, and therefore creating an *ad hoc* informal DES.

As with all DFS investigations, there remains a risk of failing to identify information which may be of relevance, practitioners should ensure that their investigative approaches are unpinned by a defined and robust DES which has been fully evaluated prior to its deployment. A lack of a formally defined DES does not guarantee failure, but it arguably increases the chance of a poor outcome through potential inadequate consideration of all the needs of an investigation. Failure to formally define a DES prior to conducting a forensic examination creates the following investigative concerns.

1. *Inconsistency*:- Investigative approaches which are defined on an *ad hoc* basis are likely to be done so inconsistently. Consider two hypothetical cases involving similar inquiries based upon the same offence-type, where it could be argued that similar examination approaches are required. Where no formally defined DES exists which denotes an appropriate course of examination conduct under these circumstances, differing levels of investigative scrutiny may be deployed in each. Such a position may lead to a varying standard of case outcomes in scenarios where it would be expected that similar forensic workflows are deployed, which ultimately would lead to similar results. Whilst this may be a concern for a single practitioner who receives two such hypothetically similar cases, possibly months apart, the concern also exists where two such hypothetically similar cases are received at different organisations. Arguably it should not matter which practitioner examines a device or where the device is examined, any two cases with comparable offence-traits should be subject to the same level of investigative scrutiny, if such levels are considered appropriate and the best course of available action. By failing to define and utilise DESs, inconsistent practice is indirectly encouraged, and any available best practice are unlikely to be captured and reused.

2. *Habitual processing*: In absence of a formally defined and case-specific DES, a practitioner may fail to tailor their investigative approaches to the case in question appropriately. As a result they may be in danger of reverting subconsciously to an investigative approach based upon the sentiment of '*I've always done it that way, therefore it is fine*'. Whilst this may not always be a bad approach, practitioners must be aware that digital offences evolve over time and therefore investigative approaches must be consistently evaluated to determine whether they remain a valid course of action. Whilst Reddy [19] states that 'most proposed methods for speeding up digital evidence examination are based on the assumption that relevant information will be found in similar locations where it has been found in other cases' [19, p.491], in reality, such approaches risk being caught out by unexpected or unknown changes in the data subject to scrutiny. Formally defining a DES prior to commencing an examination encourages scrutiny of the suitability of any proposed practices, whilst helping to break the chain of any autonomous conduct which might otherwise have been deployed without evaluation of its fitness for purpose.

3. *Comprehensiveness*: A defined DES does not guarantee a comprehensive digital forensic investigation (consider poorly defined DESs or well-defined DESs which through a lack of feasible foresight are unable to identify data), however arguably they help to prevent inadequate performance through planning and evaluation. Any examination which commences in absence of a clear strategy with defined goals risks the practitioner misunderstanding the alleged offence scenario and available data, potentially leading to poor case outcomes.

4. *Barriers to evaluation*: In all cases, the ability to evaluate any investigative work which is proposed to be undertaken is key for quality control and assurance purposes. Where the investigative work has been driven by an informally defined strategy, it is arguably more difficult for a third party to ascertain what an investigating practitioner has done and their motives behind it. Whilst to some degree, a practitioner's contemporaneous notes may support this process providing they are maintained to an adequate level of depth and quality, it may not always be guaranteed. A transparent DES permits for proactive scrutiny of what is proposed and retrospective scrutiny following a case completion, allowing a third party to address the following:-

    a. *What a practitioner has done/proposes.*
    b. *What a practitioner has not done.*
    c. *Motivations and justification for their proposed examination conduct.*

    The evaluation of a DES also supports the detection of error, both pre and post examination.

5. *Inculpatory & exculpatory*: Practitioners are often under a legal duty to identify and report upon data (where it exists) which is both inculpatory and exculpatory, regardless of their role or employer. Whilst this duty is codified, it may be difficult to ascertain in practice whether a practitioner has given consideration to all such lines of enquiry. A DES which is formally defined must consider appropriate investigative approaches for the potential existence of both inculpatory and exculpatory evidence types and evidence that measures have been taken to determine whether this content may exist

within a given examination. In absence of this, any proof that both forms of evidence have been considered may simply lie with taking a practitioner's word that they have given due thought to this.

6. *Accountability*: A formal DES also acts as a contract of service between the practitioner/investigatory team and the client, outlining not only the acts which are deemed appropriate, but also that these actions have been evaluated and accepted by all parties. Deviations from the DES, if not communicated and agreed, may indicate malpractice.

7. *Inefficiency*: In many cases it is inevitable that some parts of a DES will lead to non-evidential data or areas of a system from being queried, where the aim is to limit these circumstances - a task of precision and recall [14]. Where no DES is present, there may be a risk of the practitioner losing sight of the goal of the investigation and overworking an examination through redundant process usage.

4 Approaching an examination & DES development

Whilst sections 2 and 3 have considered what a DES is and the concerns surrounding the absence of one in case examinations, section 4 outlines the challenges of DES development. From the outset it is necessary to state that the following discussion concerns the development of a DES for the *examination/processing* of digital data from a device under forensic examination conditions. DES development for other parts of the DFS workflow are outside this work's intended remit.

To contextualise DES development for the *examination/processing* of data, it is first necessary to outline the purpose of this stage. Agarwal et al., [38, p.119] acknowledge that the examination stage is 'designed to facilitate the visibility of evidence' - to try and find it and make it available to the practitioner. Any data acquired at this stage then moves to the analysis and interpretation phase, where a practitioner will make a decision regarding the evidential worth of any piece of data. One of the primary reasons that DES development provides such a challenge at the *examination/processing* stage to practitioners is their potential inability to observe and make judgements with regards to any data which a device contains on '*face value*'. The intangible nature of digital data means that specialist software and hardware is required in order to access and evaluate any digital data present on a device - once the examination process has begun. Whilst in some cases, the physical device itself may be evidential, often it is the data that is contained within it that is considered the focus of an inquiry.

To '*see*' this data, i.e. to find it, understand its structure, format and begin to interpret its meaning, practitioners require specialist tools to allow them to find, visualise and access it. To place this in context, a suspect device may have its content extracted using forensically accepted processes, where for simplicity of debate, we will reference this extraction as a forensic 'image' of a device's content. To see the contents of this image, specialist software is required to parse and display the data structures contained within it. Whilst this software may offer the practitioner the ability to look at everything it contains, limited available resources may restrict the practitioner to the deployment of techniques and methodologies which attempt to 'target' any relevant data. Here lies the challenge. A DES can be considered a formal outline of how a practitioner is going to approach a device-examination prior to its commencement,

yet foresight of the type of data which may be case-relevant and therefore influence their conduct could be limited.

Initially a DES for any given case may be constructed based upon a practitioner's knowledge and experience of the offence-type being investigated, any surrounding case intelligence which may be available or in some cases if time has permitted, an initial preview of a device to take place [21]. The latter arguably provides the greatest insight and support for DES development, however in some cases it may not be feasible to undertake. The intangible nature of digital data acts means that there is a hypothetical '*line of sight*' barrier for the practitioner and their construction of a DES, i.e. they often can't physically see what the data is in order to make decisions as to how to deal with it. This 'barrier' may be partially unblinded by surrounding case intelligence or a preliminary cursory preview of the device allowing relevant forensic techniques to be deployed to target specific data which is likely to identify evidential data, termed here as '*investigative-insight*' (see Figure 1). However the full extent of a device's content will remain unknown until an investigation has taken place.

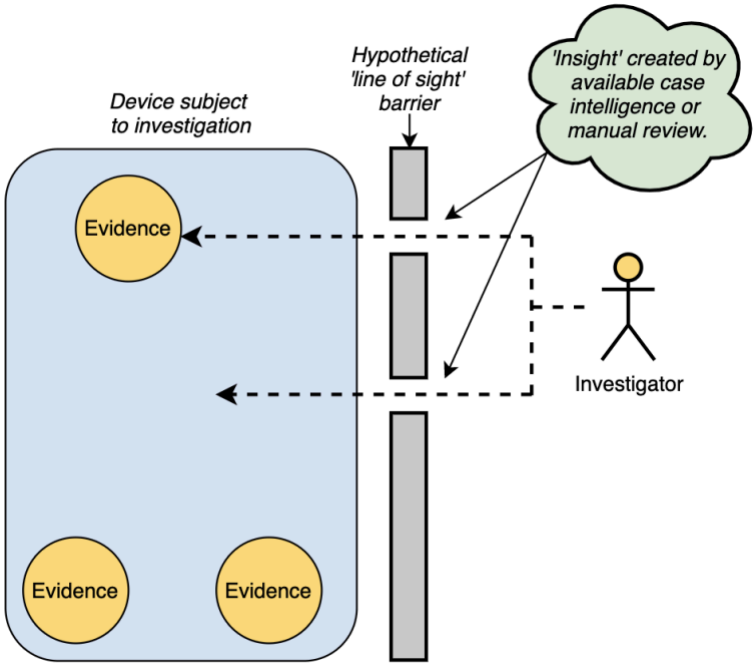

Figure 1: Developing a DES to target evidence on a device.

When building a DES, there are two fundamental components to consider, first, the 'investigative mode' which the practitioner intends to operate in, and second, the screening/processing/recovery techniques they seek to deploy.

4.1 Investigative modes

It is suggested that there are three ways, termed here as 'investigative modes' that a practitioner may approach their examination of a device in (or via a hybrid of multiple), with each discussed below.

4.1.1 The 'Informed Bread Crumb Trail'

In some cases, a practitioner, when informed by case intelligence, will be in a position to commence their examination in a specific part of a system or in pursuit of a specific digital-trace. Case intelligence may note the specific existence of this information (for example, a

report provided by a victim) or that it is likely or believed to exist on a device (for example, in cases where a third party may have observed the digital trace and reported this to the police). In either instance, the full extent of an alleged set of events may not be known, but a practitioner may commence their examination by identifying any '*known*' digital trace - referred to here as the '*principle digital trace*' (see Figure 2). This may be achieved through the manual traverse of a system and collection of data, or through the deployment of a process designed to target that specific digital trace. Once/if discovered a practitioner will evaluate the meaning and value of the principle digital trace which may connect to or indicate additional digital traces of relevance on a system, allowing a practitioner to deploy relevant techniques to explore such possibilities [54]. It is for this reason, this approach is considered the '*Informed Bread Crumb Trail*', where practitioners may be made aware of the start of what may be a hypothetical chain of evidential data which drives their examination decision making.

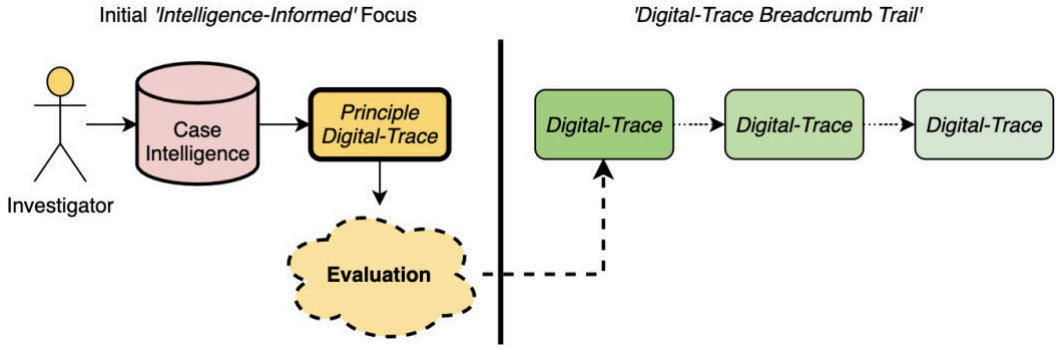

Figure 2: 'Informed Bread Crumb Trail'

4.1.2 The Offence-driven approach

Offence-driven strategies may not be informed by surrounding case intelligence, instead by the characteristics of any specific suspected offence-type. In some cases, a device may be seized as part of a reasonable line of inquiry into the suspected commission of a specific offence type [48], but insight as to the details of those acts carried out on a specific device could be limited. In these cases, a practitioner may determine the potential legal remit of the suspected offence [49] and hypothesise as to what digital actions and traces may be present should a suspect have/have not committed the offence. Practitioners may then deploy data processing techniques which allows them to gather potentially relevant digital traces which must then be reviewed, evaluated and a decision made as to whether they are of value to the inquiry being carried out (see Figure 3). Offence-driven approaches to analysis have been highlighted by Rogers [50] and Al Mutawa, N et al., [51] and may entail what Abdalla et al., [53] suggest as looking at 'obvious locations for evidence' .

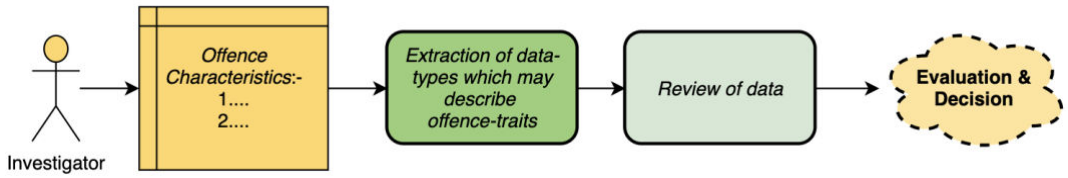

Figure 3: The 'offence-driven approach'

4.1.3 The 'jump in and see'

Some examination approaches may take the '*jump in and see*' approach. In such cases, a practitioner will hypothesise as to where inquiry-relevant data could be stored (should it exist)

on a device or in a dataset, where such initial decisions may be based upon a practitioner's experience alone. At which point, a practitioner may proceed to look through a system making '*on the fly*' decisions as to the relevance of data and how this could influence future investigative actions. In addition, a set of pre-defined processing tasks could be deployed that cover common areas of a system that may contain traces of relevant activity [51]. 'Jump in and see' approaches may be deployed where limited case intelligence exists and the suspected offence is of a type too generic to offer obvious digital traces of relevance to be determined and therefore searched for (see Figure 4).

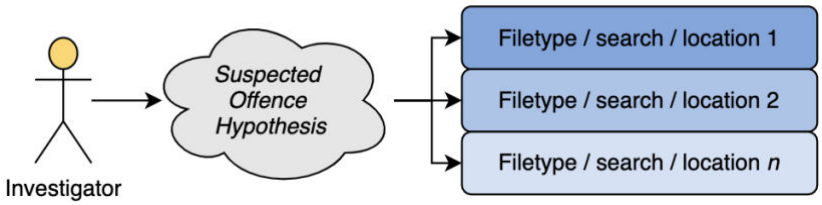

Figure 4: The 'jump in and see'

It is likely artificial to consider that any one practitioner in a given case will approach their examination solely within the confines of one of the aforementioned investigative modes. Instead, a practitioner may start their work in such a specific investigative mode then where appropriate move between them. An investigative mode can form the foundation for building a DES and provide structure to the practitioner's examination approach, even in '*jump in and see*' approaches. Practitioners will likely never be in a position to create a DES that will consistently target all evidence in every case, where often, a DES is a practitioner's formalised, and where possible informed, '*best guess*' as to how to effectively examine a device. However, by understanding the investigative mode(s) that a practitioner deems appropriate, a DES can be formed which can support the practitioner when working in this way.

In addition to the practitioner's chosen investigative mode, the practitioner will likely also deploy techniques which will 'screen' the data for relevant content, and this examination conduct must be described within a DES.

4.2 Data screening/processing/recovery

Given that large volumes of data are present in many cases and in an effort to process this, practitioners will often deploy computational data-screening/processing/recovery techniques as part of their examination practices [52]. The purpose of these processes is to target any subset of data which may exist on a device that is deemed most likely to contain information of evidential value. These techniques often include but are not limited to:-

1. The utilisation of keyword search techniques to identify potentially relevant files and data-content. Where a 'search hit' exists, depending on the search criteria used there may be a high likelihood of the data being relevant to a case, and this content is then subject to practitioner review [7].

2. Sorting file contents into a chronological representation (timelining) in order to target data which is relevant to the time of a specific known or suspected evidential event. For example, consider only viewing internet history from between two specific known

dates where a suspect is known to have been using a device [39].

3. The identification of known files or file types either through an analysis of their internal structure, location or via hash matching algorithms. Hash matching techniques are widely ustilised in cases of child abuse imagery [40].

4. The recovery of known file structures which may not be readily available (for example, deleted file recovery).

Screening/processing/recovery investigative techniques aim to reduce the quantity of data that a practitioner must interpret by targeting information which is of a type which may be relevant to an inquiry. However, as with any process which attempts to automatically sift and identify useful data, risks exist regarding their configuration and deployment. The setup of any of this group of techniques ultimately determines their success in highlighting relevant data. Incorrect configurations (either through error or lack of case insight) may lead to processes that do not capture evidential data as it may exist outside of the defined procedural-remit. If the technique is functioning correctly (for simplicity of discussion, let's assume it is), then this issue lies fundamentally with the practitioner and their ability to use these capabilities effectively.

Data-screening is a practice which has been developed through necessity and has limited formalisation of best practice. Given the reliance placed upon screened results, concerns lie with the deployment of inconsistent investigative practices in this context [41]. A lack of structured regulatory oversight and planning could mean that inconsistency in the way that data-screening techniques are deployed is likely to exist. As a consequence, there is a real risk that varying standards of data-screening practices exist, compromising the quality of this practice both within an organisation and geographically. There is a need to understand existing data-screening practices in the digital investigation context and to evaluate their deployment. This includes both at a technical level (how effective are the approaches at screening data) and at a procedural level (are data-screening approaches being correctly deployed). Current academic and operational research is yet to establish the circumstances which are appropriate for data-screening in an investigative context and the decisions which are taken prior to and during its deployment.

Effective data-screening processes can reduce case investigation times and increase the efficiency of an examination process if used effectively. In contrast, ineffective device screening can lead to missed information and incorrect investigative decisions, delaying casework or in some instances leading to the failure to deliver justice [42]. Any approach which seeks the use of computational methods to automate data sifting, even at a basic level, increases the risk of data being missed or mis-categorized as part of this process. This can sometimes be due to prioritising methods that aim to quickly get results rather than be thorough in their scrutiny of case data [43]. Data-screening now plays a prominent and important role in the digital device investigative process, but poor practices can lead to unacceptable and dangerous outcomes, and as this practice is and will remain an important tool for those investigating digital data, it is important that it is done appropriately.

A DES must define the remit of any proposed screening/processing/recovery techniques, their configuration and information influencing this, underpinning motivation, and be subject to a suitability-evaluation. Doing so aims to both formalise the process of deploying 'data

screening' mechanisms and also helps to define repeatable and consistent practice. This importance cannot be understated as often screening/processing/recovery techniques dictate the subset of data which is both discovered and subject to scrutiny. Data missed due to the inadequate use of screening/processing/recovery may compromise an investigation as the existence of it may never be acknowledged by a practitioner (see Figure 5).

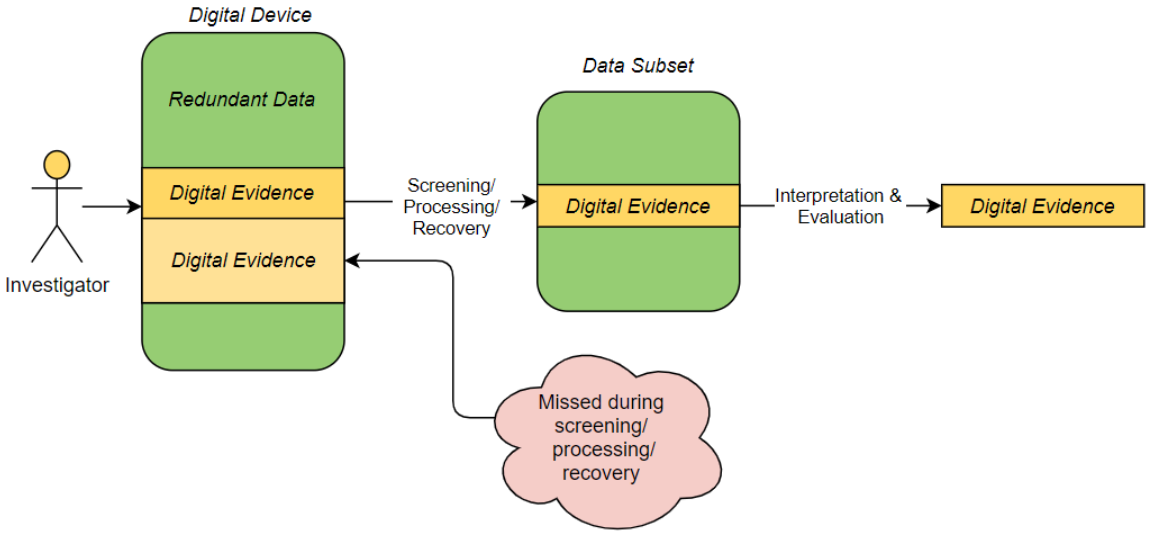

Figure 5: Data reduction via screening/processing/recovery techniques leading to missed data.

5 A DES Skeleton

To support the creation of a DES, the following 'skeleton' is offered which intends to help any investigating team by ensuring all necessary investigative questions and processes are identified and addressed. A DES should be considered a transparent record of investigative conduct and the third part of a triad of key case documentation (the first being a practitioner's contemporaneous notes and second, any generated statement/report). Whilst DESs will to some degree be bespoke to the case in which they apply making it impossible to develop a single holistic DES, it is possible to identify categories of information which must form part of it.

The following DES skeleton shown in figure 6 is influenced by the strategic foundations set out in the Case Assessment and Interpretation (CAI) model [44], and sets out 7 components which a DES must contain. Each component must be addressed in the construction of a DES, which must then be subject to evaluation regarding its suitability.

DES Skeleton:-

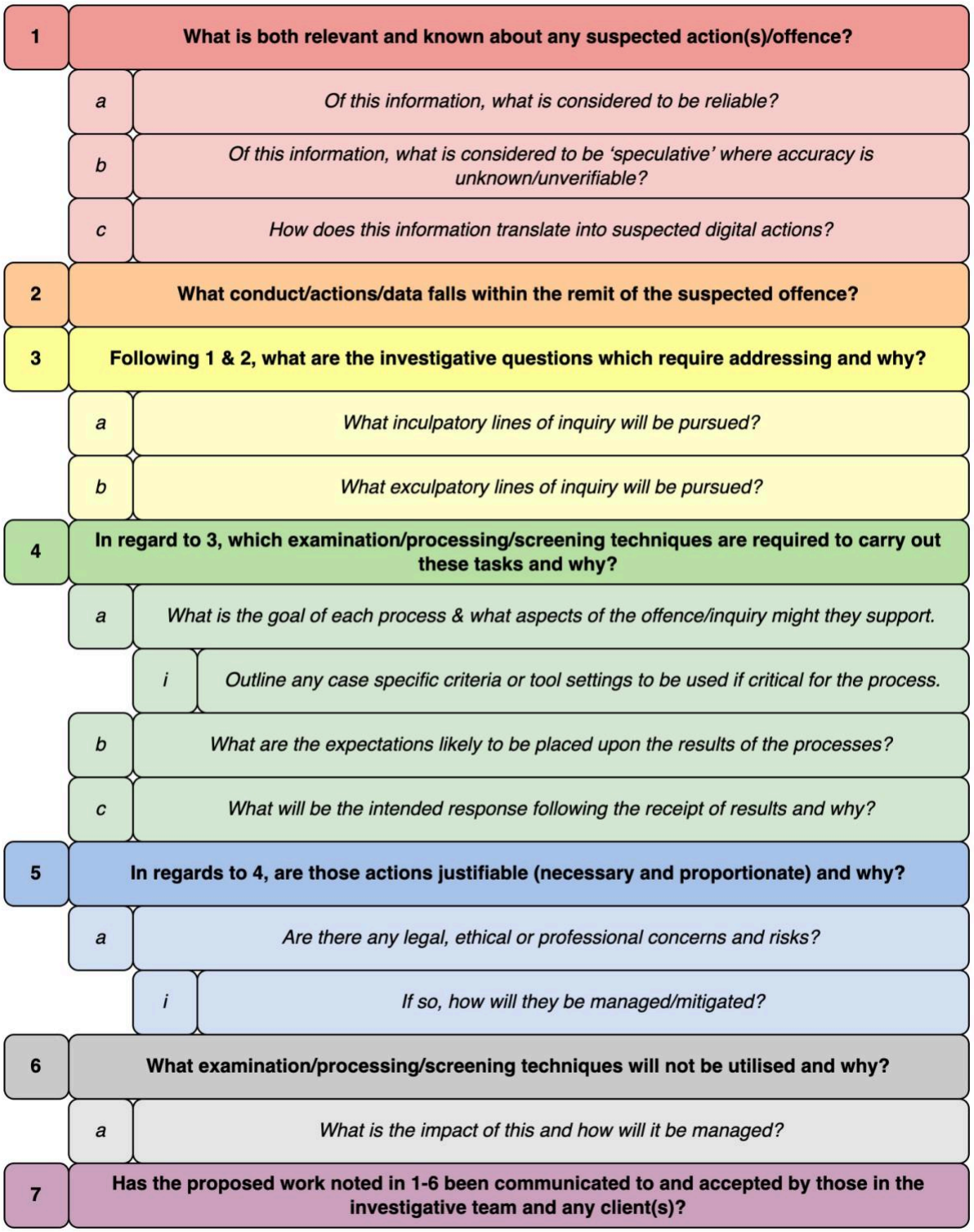

Figure 6: A DES Skeleton

Under (1), emphasis is placed upon the need for only relevant information as concern has sometimes been expressed about the potential for 'extraneous information' compromising the objectivity of scientific examinations and findings [44, p.61][45]. Here the DES must record what information that the investigating team seeks to rely upon as part of the development of their examination practices. This information should be assessed in terms of its reliability in order to manage the risk of overreliance upon, particularly if it is unconfirmed or considered

speculative as the investigation team must evaluate what it could mean in terms of digital trace evidence being present on a system. Misinterpretation of any r*elevant and known* suspected actions could lead to the inappropriate use of an investigative mode or screening/processing/recovery technique.

Under (2) the investigating team must establish the legal remit of the alleged offence and provide their interpretation of it, including what digital events/actions they believe would fall within its confines - taking into consideration information established at (1). Doing so will illustrate the actions that a practitioner will target as part of the examination and also establish whether they are in position to operate in an 'offence-driven' investigative mode, or whether insufficient information is available.

Under (3), the investigating team must consider the investigative questions which require addressing and why, influenced by stages 1 & 2. These may be generated from victim/defendant admissions or statements, or take an offence-based focus, i.e. '*did 'x' download 'y*'. It is important that examination processes are designed to provide an answer to these, otherwise a lack of focus may result in an inability to address the key purpose of the investigation - to determine whether a specific course of action has occurred.

Under (4) the investigating team are required to propose a course of examination conduct that is intended to address those questions in (3). Here, sufficient detail is required regarding both the physical processes and the belief in their need/suitability for the task. The use of any screening/processing/recovery techniques must be defined in full, including their configuration and reliance upon key information (for example, keyword search criteria established from (1)). The practitioner should outline what they expect to obtain from such processes (if successful/unsuccessful) and how this will influence future examination decisions.

Under (5) the investigating team must confirm that those examination actions under (4) are proportionate and necessary for the investigation in question and that any legal, ethical or professional concerns and risk have been acknowledged and managed/mitigated - and how. This must be a proactive approach as it may not be possible to retrospectively rectify any breaches post-examination. Anderson et al [55] note that 'digital evidence strategies allow investigators to set parameters such as time frames that are proportionate to the facts and assist in overcoming the challenges presented by the large volume of data stored on digital devices and associated storage services. The use of Digital Evidence Strategies allows the examination of digital devices to be both targeted and proportionate and streamline the forensic process'. Developing a proportionate and necessary DES can be a challenge, as any investigative requests made of forensic staff by officers in charge of a case could be excessive. This may be possibly due to a misunderstanding of the technology involved, the inability to fully understand how any digital evidence may support their inquiries, or, changes in stance in regards to policy and procedures involved in investigations. For the latter, examples may include changes to guidance regarding privacy preservation [56] and approaches to data extraction from devices for specific offence-types [57]. Therefore it is important to ensure open and clear channels of dialog are maintained in order to ensure that the remit of any DES is deemed appropriate by all parties and the underpinning reasons for it are agreed and understood.

Under (6) the investigating team as part of defining the examination scope, outline those actions which will not be undertaken. Whilst it is impossible to account for every eventuality, here focus is predominantly on highlighting and justifying the omission of actions which may seem controversial or being expected to have occurred. For example, if specific keyword criteria or the recovery of specific file types is to be excluded from an examination for legal/privacy reasons, this must be noted. Doing so ensures that any examination limitations are formally noted, and provides acknowledgement and justification for doing so, preventing any future case evaluation for inferring that this was an examination error or flaw.

Under (7), those responses to stages 1-6 must be agreed by all parties involved in the investigation. Agreement must be formally evidenced only once there is a recognition of understanding of the DES.

5.1 Discussion

The DES skeleton is a support mechanism for investigation teams to define the conduct of their examination formally, prior to its commencement at a time when it can be evaluated for suitability and refined without impacting an examination. A DES will not guarantee a quality examination of a device takes place, but it will arguably improve the likelihood that a robust investigation takes place due to scrutiny of practice which it should be subject to. DFS must move away from ad hoc examination approaches and bolster the formalisation of its procedures, ensuring that they are transparent, uncompromising and accurate. The DES process not only encourages investigating teams to think about an appropriate course of examination conduct within a given set of circumstances, it is also evidence of the underpinning motivations and decision making which has led to this undertaking.

DESs should be seen as a formalization of best practice for the particular scenario in which it has been created for - i.e. the DES should outline the best way that any given device can and should be examined within those resources available. Whilst a DES will be bespoke to each case in which it applies, DES-reuse may be viable where similar circumstances exist (case types of the same offence type etc.). This may take place internally to an organisation, and cross-community DES sharing should not be ruled out. Creating DESs prior to an examination is not only a quality assurance and control mechanism, but also a way of harmonising practices across the DFS field. DFS examinations are complex entities and those inoperational roles must begin to standardise how they approach this task. Doing so not only improves consistency of practice, but supports performance evaluation and incremental best practice development as there is a formal record of the strategic approaches which practitioners are deploying. In absence of a DES, there may be no formal documentation of the reasoning and approaches taken by a practitioner during an examination, bar the interpretation of their contemporaneous notes which may not contain strategy-level details.

Rappert et al [58] noted that DFS practitioners feel ‘tension between providing quality examinations and making good progress with their queue of cases’. It has long since been noted that a lack of resources in this field has led to backlogs and pressures being placed upon DFS staff to ensure cases are progressed in good time. All those involved in a given case want an effective and efficient case outcome, but the demand for quick results cannot come at the cost of the quality or appropriateness of any investigative work taking place [59]. Formalising a DES in every case is a time consuming process, therefore it must be managed to prevent it becoming a burden. The DES creation process must be seen as an important

part of the overall investigative process as an effective DES may save both time and resources in the long run by ensuring an effective and efficient examination is conducted. DES creation should also be a process that seeks input from as many of the wider investigative team as possible to ensure that its suitability is evaluated by all those involved in a case. Further, such incluitivty may help to prevent disagreements with it.

It is recognised that under already pressurized conditions, adding to the existing workload of an investigatory team may deter engagement with such tasks, however, it must be stressed that a DES should be considered an important and necessary process. It not only attempts to ensure an effective examination takes place, if the DES development process is genuinely engaged with properly, it also protects those involved in the examination by evidencing an objective, lawful and justifiable course of conduct.

Emphasis must be placed on the evaluation element of DES building to prevent it from becoming a token gesture process. Given that the DES is an accepted, indirect contract of conduct that those in the investigating team agree to adhere to, it is important that those actions described within it are scrutinised - particularly if a DES is designed by a single investigating practitioner. The DES must evidence an effective strategy for the case under examination, and this requires engagement in peer review processes [46]. Any created DES that is not subject to a suitability-evaluation defeats the purpose of this process and risks being inadequate.

6 Conclusions

This work has discussed the concept of the DES, what it is and why it is needed. The complexity of DFS device examination has now arguably called for the need for the use of formalised strategic examination approaches which are appropriate and justifiable. DESs created by investigating teams are proposed as a method of enhancing examination quality control by introducing formality and rigour into this process. The DES skeleton has been offered which provides an outline for investigating teams to utilise as they seek to define their own DESs. Future work involves assessing the uptake of formalising the DES process and evaluation of the decision making involved.

References

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

2. Home Office (2016) ‘Forensic Science Strategy’ Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/506683/54493_Cm_9217_Forensic_Science_Strategy_Print_ready.pdf (Accessed: 4 April 2021)

3. Forensic Capability Network, 2020. ‘Digital Forensic Science Strategy’ Available at: https://www.fcn.police.uk/sites/default/files/2020-07/Digital%20Forensic%20Science%20Strategy%20EMAIL%20VERSION%20ONLY.pdf (Accessed: 25 February 2020)

4. Police Service of Northern Ireland (2020) ‘Digital Strategy to 2020 and Beyond’ Available at: https://www.psni.police.uk/globalassets/inside-the-psni/our-departments/finance-and-support-services/ics/digital-strat-2020/psni-digital-strategy-a4-document-v9.2.3-external.pdf (Accessed: 4 April 2021)

5. Collie, J. and Overill, R.E., 2020. DEEP: Extending the Digital Forensics Process Model for Criminal Investigations. Athens Journal of Sciences, 7(4), pp.225-240.

6. Police Scotland (2021) ‘Cyber Kiosks’ Available at: https://www.scotland.police.uk/about-us/police-scotland/specialist-crime-division/cybercrime-investigations-and-digital-forensics/cyber-kiosks/ (Accessed: 4 April 2021)

7. Quick, D. and Choo, K.K.R., 2014. Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation, 11(4), pp.273-294.

8. Casey, E., Ferraro, M. and Nguyen, L., 2009. Investigation delayed is justice denied: proposals for expediting forensic examinations of digital evidence. Journal of forensic sciences, 54(6), pp.1353-1364.

9. Lillis, D., Becker, B., O'Sullivan, T. and Scanlon, M., 2016. Current challenges and future research areas for digital forensic investigation. arXiv preprint arXiv:1604.03850.

10. Home Office, 2021. Pre-charge bail: An overview of the evidence. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/952065/PCB_evidence_review_FINAL.pdf (Accessed: 4 April 2021)

11. Horsman, G., 2020. Opinion: Does the field of digital forensics have a consistency problem?. Forensic Science International: Digital Investigation, p.300970.

12. Transforming Forensics Programme, (2018) ‘BUSINESS CASE – TF DIGITAL. Doc No: G960-TFP-KBR-PRG-AD-BUC-0042’ Available at: https://www.npcc.police.uk/NPCCBusinessAreas/ReformandTransformation/SpecialistcapabilitiesmainSpecialistCapabilitiesProgrammeTransformingForensi.aspx (Accessed: 5 April 2021)

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

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

15. Köhn, M., Olivier, M.S. and Eloff, J.H., 2006, July. Framework for a Digital Forensic Investigation. In ISSA (pp. 1-7).

16. Kyei, K., Zavarsky, P., Lindskog, D. and Ruhl, R., 2012, October. A review and comparative study of digital forensic investigation models. In International conference on digital forensics and cyber crime (pp. 314-327). Springer, Berlin, Heidelberg.

17. Chen, L., Xu, L., Yuan, X. and Shashidhar, N., 2015, February. Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges. In 2015 International Conference on Computing, Networking and Communications (ICNC) (pp. 1132-1136). IEEE.

18. Overill, R.E., Silomon, J.A. and Roscoe, K.A., 2013. Triage template pipelines in digital forensic investigations. Digital Investigation, 10(2), pp.168-174.

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

20. Richard III, G.G. and Roussev, V., 2006. Next-generation digital forensics. Communications of the ACM, 49(2), pp.76-80.

21. Association of Chief Police Officers (2012) 'ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence for Digital Evidence' Available at: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed: 14 April 2021)

22. Kao, D.Y., Wu, N.C. and Tsai, F., 2020, February. A Triage Triangle Strategy for Law Enforcement to Reduce Digital Forensic Backlogs. In 2020 22nd International Conference on Advanced Communication Technology (ICACT) (pp. 1173-1179). IEEE.

23. Association of Chief Police Officers (2007) 'Good Practice Guide for Computer-Based Electronic Evidence' Available at: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf (Accessed: 14 April 2021)

24. Page, H., Horsman, G., Sarna, A. and Foster, J., 2019. A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn?. Science & justice, 59(1), pp.83-92.

25. Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N.A. and Scanlon, M., 2020, August. SoK: exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-10).

26. Oxford Learner's Dictionary (2021) 'Strategy' Available at: https://www.oxfordlearnersdictionaries.com/definition/english/strategy?q=strategy (Accessed: 4 April 2021)

27. Rogers, M., 2003. The role of criminal profiling in the computer forensics process. Computers & Security, 22(4), pp.292-298.

28. ILAC (2014) 'ILAC G19:08/2014 PUBLISHED' Available at: https://ilac.org/latest_ilac_news/ilac-g19082014-published/ (Accessed: 4 April 2021)

29. Gehl, R. and Plecas, D., 2017. Strategic Investigative Response. Introduction to Criminal Investigation: Processes, Practices and Thinking.

30. Forensic Science Regulator (2021) 'Forensic Science Regulator Codes of Practice and Conduct Development of Evaluative Opinions' 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 (Accessed: March 1 2021)

31. Horsman, G., 2021. The COLLECTORS ranking scale for 'at-scene' digital device triage. Journal of Forensic Sciences, 66(1), pp.179-189.

32. Information Commissioner's Office (2020) 'Mobile phone data Extraction by police forces in England and Wales' Available at: https://ico.org.uk/media/about-the-ico/documents/2620093/ico-investigation-mpe-england-wales-202106.pdf

33. Crown Prosecution Service, (2018) 'A guide to "reasonable lines of enquiry" and communications evidences' Available at: https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence.

34. Sharevski, F., 2015. Rules of professional responsibility in digital forensics: A comparative analysis. Journal of Digital Forensics, Security and Law, 10(2), p.3.

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

36. Leong, R.S., 2006. FORZA–Digital forensics investigation framework that incorporate legal issues. digital investigation, 3, pp.29-36.

37. Garfinkel, S., Nelson, A.J. and Young, J., 2012. A general strategy for differential forensic analysis. Digital Investigation, 9, pp.S50-S59.

38. Agarwal, A., Gupta, M., Gupta, S. and Gupta, S.C., 2011. Systematic digital forensic investigation model. International Journal of Computer Science and Security (IJCSS), 5(1), pp.118-131.

39. Hargreaves, C. and Patterson, J., 2012. An automated timeline reconstruction approach for digital forensic investigations. Digital Investigation, 9, pp.S69-S79.

40. Roussev, V., 2009. Hashing and data fingerprinting in digital forensics. IEEE Security & Privacy, 7(2), pp.49-55.

41. Horsman, G., 2020. Opinion: Does the field of digital forensics have a consistency problem?. Forensic Science International: Digital Investigation, 33, p.300970.

42. Boast, K., Harriss, L. 2016 'Digital Forensics and Crime' Available at: https://post.parliament.uk/research-briefings/post-pn-0520/

43. Casey, E., 2019. The chequered past and risky future of digital forensics. Australian journal of forensic sciences, 51(6), pp.649-664.

44. Jackson, G., Aitken, C. and Roberts, P., 2015. Case assessment and interpretation of expert evidence. Guidance for judges, lawyers, forensic scientists and expert witnesses. Practitioner guide, (4).

45. Willis, S., McKenna, L., McDermott, S., O'Donell, G., Barrett, A., Rasmusson, B., Nordgaard, A., Berger, C., Sjerps, M., Lucena-Molina, J. and Zadora, G., 2015. Strengthening the Evaluation of Forensic Results Across Europe (STEOFRAE), ENFSI guideline for evaluative reporting in forensic science.

46. Sunde, N. and Horsman, G., 2021. Part 2: The Phase-oriented Advice and Review Structure (PARS) for digital forensic investigations. Forensic Science International: Digital Investigation, 36, p.301074.

47. National Centre for Policing Excellence's., 2006 Murder Investigation Manual. Available at: https://www.npcc.police.uk/documents/FoI%20publication/Disclosure%20Logs/Crime%20%20FOI/2011/073%2011%20Att%2001%20of%201%20Murder%20Investigation%20Manual.pdf

48. Horsman, G., 2022. When is a line of inquiry 'reasonable'?-a focus on digital devices. Australian Journal of Forensic Sciences, pp.1-12.

49. Agarwal, A., Gupta, M., Gupta, S. and Gupta, S.C., 2011. Systematic digital forensic investigation model. International Journal of Computer Science and Security (IJCSS), 5(1), pp.118-131.

50. Rogers, M., 2003. The role of criminal profiling in the computer forensics process. Computers & Security, 22(4), pp.292-298.

51. Al Mutawa, N., Bryce, J., Franqueira, V.N., Marrington, A. and Read, J.C., 2019. Behavioural digital forensics model: Embedding behavioural evidence analysis into the investigation of digital crimes. Digital Investigation, 28, pp.70-82.

52. Beebe, N.L. and Clark, J.G., 2005. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), pp.147-167.

53. Abdalla, S., Hazem, S. and Hashem, S., 2007. Guideline model for digital forensic investigation.

54. Harbawi, M. and Varol, A., 2017, April. An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In 2017 5th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-6). IEEE.

55. Anderson, P., Sampson, D. and Gilroy, S., 2021, September. Digital investigations: relevance and confidence in disclosure. In ERA forum (pp. 1-13). Springer Berlin Heidelberg.

56. Horsman, G., 2022. Defining principles for preserving privacy in digital forensic examinations. Forensic Science International: Digital Investigation, 40, p.301350.

57. College of Police 2021. Extraction of material from digital devices Available at: https://www.college.police.uk/app/extraction-material-digital-devices/extraction-material-digital-devices

58. Rappert, B., Wheat, H. and Wilson-Kovacs, D., 2021. Rationing bytes: managing demand for digital forensic examinations. Policing and Society, 31(1), pp.52-65.

59. Wilson-Kovacs, D., 2019. Effective resource management in digital forensics: An exploratory analysis of triage practices in four English constabularies. Policing: an international journal, 43(1), pp.77-90.

https://dspace.org/

Digital evidence strategies for digital forensic science examinations

Horsman, Graeme

2023-01
Elsevier
https://doi.org/10.1016/j.scijus.2022.11.004
Horsman G. (2023) Digital evidence strategies for digital forensic science examinations. Science & Justice, Volume 63, Issue 1, January 2023, pp. 116-126

Downloaded from a DSpace repository. https://dspace.org/