Check for updates

Received: 6 July 2023 | Revised: 14 September 2023 | Accepted: 9 October 2023

DOI: 10.1002/wfs2.1507

PERSPECTIVE

WIREs FORENSIC SCIENCE WILEY

The importance of digital evidence strategies

Graeme Horsman

Cranfield Forensic Institute, Cranfield University, Bedford, UK

Correspondence
Graeme Horsman, Cranfield Forensic Institute, Cranfield University, Bedford, UK.
Email: graeme.horsman@cranfield.ac.uk

Edited by: Kim-Kwang Raymond Choo, Editor

Abstract

As the complexity of digital forensic work continues to grow, and the demands and pressures placed on practitioners to complete their investigatory commitments remain, methods for conducting effective and efficient work are of paramount importance. To combat examination challenges any investigating team requires two fundamental and linked components; those conducting DF examinations should develop (1) a digital evidence strategy (DES) that outlines an effective investigative approach, and, (2) deploy it using appropriate tools and techniques. While these should be considered as a pair, arguably as tools have become more comprehensive and more akin to "*suites*," there is a real risk that tools themselves are being considered an "*examination strategy*," bypassing the need for investigative forethought. Given this concern, through the vehicle of an example deconstructed hypothetical forensic examination process, this work discusses the relationship between DESs and digital forensic tools, and the importance of both.

This article is categorized under:

Digital and Multimedia Science > Cybercrime Investigation

KEYWORDS

digital evidence, digital forensics, investigation, strategy, tools

1 | INTRODUCTION

Over the last 20 years, digital forensic (DF) examinations have become significantly more complex (James & Gladyshev, 2013; Jarrett & Choo, 2021; Vincze, 2016). Driven by the pace of technological change (Karie & Venter, 2015) and its availability to the masses at an affordable price, practitioners now face a diverse range of challenging case types, often with large volumes of data in need of review (Quick & Choo, 2016; Rappert et al., 2022). In addition, there is a need to complete this work at a pace that fits with any applicable criminal justice system's frequently congested schedule (Horsman & Sunde, 2022). The pressure to conduct and conclude investigations swiftly is somewhat understandable given the need for timely justice and the role and impact that forensic evidence can have on judicial decision making. However, practitioners must be wary of compromising the quality of their investigative work in order to increase the speed that they are doing it. To combat these examination challenges an investigating team requires two fundamental and linked components; those conducting DF examinations should develop (1) a digital evidence strategy (DES) that outlines an effective investigative approach

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.
© 2023 The Authors. *WIREs Forensic Science* published by Wiley Periodicals LLC.

and attempts to limit the chance of missing relevant digital data and, (2) execute it using appropriate tools and techniques (Horsman, 2022). This combined approach helps to ensure any available digital data is identified and processed properly and efficiently in order to address all relevant investigative inquiries. However, despite the suggested importance of these two elements, while narratives surrounding DF tool developments and capabilities are somewhat common, discussions concerning the need for DESs are somewhat sparse.

It is suggested that an effective DES is a fundamental part of any DF examination as it helps to maximize the chance of relevant data being captured and simultaneously reduces the likelihood of this data being missed. Those involved in any inquiry where digital evidence may exist should not disregard the need to create a DES at the start of their investigation. While the importance of having a DES in place at the start of any examination seems obvious and something that should be considered a critical piece of the investigative "*jigsaw puzzle*," it may not always be formally and robustly addressed during the DF examination process by an investigative team or examining practitioner. Instead, with the advent of multifaceted "*tool suites*" that offer many examination features and abilities, it is suggested that now there is a real risk that the DF tools themselves are being considered the "*examination strategy*," given the extensive examination-coverage that some can be preconfigured to offer.

While it is acknowledged that DF tools are a fundamental part of the DF investigative process, they cannot be the only factor driving how an examination is conducted. A solely tool-driven examination strategy can be problematic. Instead, an evaluation of the investigative tasks required to address any of the needs of an inquiry successfully should first be conducted (the DES), and only then should tools and techniques that are appropriate for carrying out this work be identified, configured, and deployed. DF tools must not be used without first determining what their role in a DF examination is, why they are being used, and what inquiry-relevant questions their use is attempting to address. It is conceivable that any examination approach that is solely tool-driven and takes place without an overarching DES can give rise to a number of problems that can impact both the thoroughness of an investigation and its efficiency, as well increasing the potential for compromising any defendant's data-privacy (Horsman, 2022; ICO, 2020, 2021; Privacyinternational.org, 2018). In addition, it at best begins to omit the use of a practitioner's "investigative skills and mindset," and at worst disregards the need for it, possibly in favor of blindly casting the "*data collection and processing net*" indiscriminately wide in the hope of capturing as much inquiry-relevant data as possible, rather than undertaking an appropriately targeted examination.

Through the vehicle of an example deconstructed hypothetical DF examination process, this work discusses the relationship between DESs and DF tools.

2 | THE RELATIONSHIP

The development of an investigative strategy is a key priority in any investigation (National Centre for Policing Excellence, 2006) as it helps those tasked with conducting any inquiries to plan for and identify appropriate investigative actions (College of Policing, 2022). In the field of DF, for inquiries that involve or are believed to involve digital devices or digital data, a DES should be developed and followed. A DES is defined by Horsman (2022, p. 117) as follows:

> 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.

When simplified, a DES outlines a plan for conducting an effective investigation of digital devices. A DES can be deployed in capacities ranging from describing practices linked to crime scene attendance (including but not limited to tasks such as device identification and collection, scene management and scene processing), or, for outlining a DF examination strategy for a device's contents. The latter or these two scenarios is the focus here. While a DES must be considered dynamic and changeable throughout the course of an inquiry to meet any subsequently identified needs, it should be initially developed prior to its start and set out those processes needed to address all of its initially recognized requirements. A DES should determine a course of investigative conduct that is appropriate and

25739468, 2024, 1, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1507 by Test, Wiley Online Library on [28/02/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

defensible, and part of this requires the identification of tools and techniques that are both suitable for deployment and meet the needs of the investigation, including deciding how they should be used (their remit/configuration) (Horsman, 2022).

In some cases, a DES may recognize that certain investigative questions cannot be addressed given currently available capabilities and knowledge. As a result, it may acknowledge instead the need to pare back to a position that is achievable. Where this discrepancy exists between what is needed to conduct a thorough DF examination and what is viable, this must be recognized within a DES rather than disregarded or ignored. In some cases, a tool may partially fulfill an investigative requirement, but additional work may be needed by a practitioner to manually interrogate and interpret data in order to identify and understand data that their tools cannot effectively process. The limits of any digital investigation should not be defined entirely by the capability of any available tools alone, and practitioners must be prepared to work beyond any tool's stated functionality if required.

Despite the importance of DESs, it is suggested that their role as part of DF investigation preparation and planning could start to be eroded. We have now reached a point in DF where the tools we purchase are rarely "single function" (tools that offer a single or limited number of defined functions), and more akin to a "suite," with potentially hundreds of configurable capabilities are provided. As a result, it is suggested that tool-suites are now beginning to encroach on the role of a DES, and starting to look more like an "investigative strategy" themselves given the plethora of functionality that they offer a practitioner.

2.1 | Tool-driven strategies

Hunton (2011, p. 64) notes that "a structured and rigorous assessment stage will not only assist investigators to gain a much richer understanding of the illicit activities surrounding a cybercrime but also support the formulation of any hypothesis relevant to guiding the technical evidence recovery." A distinction must be drawn between planning and evaluating the needs of an investigation, and the task of examining data using tools; where the former should influence the latter. Only once an extensive review has been conducted of the investigative scenario as a whole, and its requirements, can the most appropriate tools and techniques be determined (Hunton, 2011). It has been previously stressed that in many cases, individual tools cannot meet all of the needs of a digital investigation, where instead tool-collaboration is often required (Guo et al., 2009), and tool-selection and configuration must be guided by the identified needs of the investigation. Tools and techniques are not a strategy, they are used to fulfill any investigative strategy. Roux et al. (2012, 2022) emphasizes the need for those conducting forensic science to develop strategies which drive and determine the use of appropriate technologies, tools and techniques. The up-front strategic evaluation of any given case helps to ensure that the forensic processes and practices that are chosen and deployed are ethical, justifiable and meeting the requirements of any client (Cook et al., 1998; Jackson & Jones, 2009).

A DES should examine a case's requirements to provide a strategic investigative approach that is targeted, viable and one that has been critically evaluated and considered to have the highest chance of addressing any inquiry-relevant questions effectively. It should define what hypothetical "investigative success" looks like and outline a path to achieving this, which may involve identifying specific tools or tool-configurations that are required to complete necessary tasks. While a DES encapsulates tool usage and how they should be used it must recognize when work beyond a tool's existing capability is required and understand that any available tool's limits may fall short of what is required for the case and plan for how to address this scenario. Conversely, this work coins tool-driven strategies as those that involve the use of a tool or tool-suite without significant forethought of investigative requirements, where any results obtained define the extent and boundary of any investigative work. Work beyond what a tool has been configured to do (recover, parse, etc.) may be disregarded or not even considered, where in essence, the remit of the examination matches the remit of any chosen tool, and nothing further. Informally, this approach can in some cases involve gathering/processing as much data as a tool can provide, followed by a "*sift and see*" approach to this dataset.

The fundamental difference between a DES and tool-driven investigative strategy is that a DES evaluates and defines all of the investigative conduct required to address the needs of a given inquiry. Multiple data-examination options may exist but the believed (following evaluation and review) best course of conduct is suggested, and the strategy may be dynamic. In contrast, a tool-driven strategy may be more linear in nature, where regardless of any investigative requirements, a deployed tool's remit will either identify or miss inquiry-

25739468, 2024, 1, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1507 by Test, Wiley Online Library on [28/02/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

relevant content, and data beyond a tool's configured ability may not be considered or even disregarded. A chosen tool may simply be deployed because it is that organization's primary examination tool, or it may be their only tool, and in turn it could be deployed in similar ways in multiple cases regardless of the offense type or surrounding circumstances. It is argued that the likelihood of missing relevant data during a DF examination is increased when following this work's definition of a tool-driven strategy as opposed to an examination conducted following a DES.

It is foreseeable that tool-driven investigative strategies are now being deployed in place of DESs given that many tool-suites offer and automate data processing and recovery en masse, and the demand for case results to be delivered at speed. This may give the perception that strategic examination approaches and the need for a "*digital investigative mindset*" to find and recover relevant data are no longer required, replaced instead with a mentality that may align with an approach of "*throwing everything*" at any captured data hoping that any tools will capture and present any available evidence. With this in mind, it is worth noting that while multiple tool-vendor training courses exist, there are few training packages that focus on digital investigative approaches and strategies. As a result, there is arguably a real risk that the DF field is failing to acknowledge the need for investigative skills and instead prioritizing the acquisition of technical tool-driving skill sets.

In order to highlight the "DES-tool relationship" a deconstructed hypothetical examination process is discussed in Section 3. Through this vehicle, the intention is to emphasize the value of a DES and potential limitations with tool-driven strategies and a reliance on them.

3 | A DECONSTRUCTED EXAMINATION

There are four key components as part of representing a hypothetical deconstructed DF examination to consider; available data, inquiry-relevant data, DESs and, tools and techniques, with each discussed in turn.

3.1 | Available data

For any given digital examination, a practitioner has access to a hypothetical "pot" of data that is both available and accessible. This data forms the initial target of their investigation and they can and should plan for how they are going to examine it. In many cases, the total volume of available data will be much greater than the size of any data considered relevant to an inquiry (Horsman et al., 2014), emphasizing the need for strategic approaches that can sift and identify content appropriately. Often, the majority of available data will arguably be redundant and non-relevant. In regards to currently available data, there are three positions here that must be emphasized.

1. *"Currently" available data*: Any initial dataset that is currently available to the practitioner may reduce or expand in size overtime as more relevant sources are identified, or if restrictions over the use of any data come into force. In some cases, data that is linked to an inquiry will not be available at the time of an initial examination, but may subsequently become available following the seizure of devices later down the line, or as an investigation expands its remit. A DES should identify sources that are not currently available but are relevant to an inquiry and plan for if access to them is acquired. Alternatively, it should also recognize and plan for any impending data restrictions that might come into force and have an impact on the ability to address inquiry-relevant questions during an examination.
2. *Data we know we cannot get*: Beyond the realms of the available data exists data that an investigative team may know they cannot get access to in order to examine—non-available data. Examples include service-related data where access to it is refused by the service provider. While this may be frustrating, these non-accessible sources should not be ignored, but acknowledged in case any situation around data-access changes.
3. *Data we do not know is available*: Finally, in any investigation there is a risk that data is available to the investigative team but they are unaware of its existence. It is difficult to plan for these scenarios, but in reality, any existing dataset being investigated may not be "everything" that could be available, emphasizing the need to thoroughly evaluate the potential for available and legally accessible data to support an inquiry.

25739468, 2024, 1, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1507 by Test, Wiley Online Library on [28/02/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

3.2 | Inquiry-relevant data

While the data available for examination may be substantial in size, as noted, those parts of it that are of value to an inquiry may be less so. Inquiry-relevant data is data that has an impact on an investigative team or practitioner's understanding of an event or impact on their decision making regarding how a case progresses through the investigative process. Inquiry-relevant data can exist both within the data that is available for investigation and outside of this dataset. Where inquiry-relevant data is not currently available, its existence may be known about or remain unidentified, similar to the positions noted above in Section 3.1.

One of the principal aims of any digital investigative strategy is to identify all of the available inquiry-relevant data while limiting interaction with and the collection of any redundant data, so far as practically possible.

3.3 | Developing a DES

Following consideration of available and inquiry-relevant data, it is suggested that most DF examinations commence with data apportioned in a way that is comparable to Figure 1 (to note—the sizes of the diagrammatic sections is not intended to be representative of data apportioned quantities, merely a visual representation). It is at this point that the impact and implications of DESs and tool deployment can be seen.

A DES should define conduct that provides maximum coverage of all available inquiry-relevant data, while attempting to limit interaction with redundant content. It aims to define conduct that does this as efficiently and effectively as possible, taking into account available capability. Figure 2 represents the application of a DES to the start of a DF examination. First, it should be noted that any DES is likely to identify data types that are, and are not relevant to an inquiry—it is never a perfect science and a realistic approach should be taken here and expectations managed. A good DES cannot be considered a silver bullet solution for any investigation, but it should increase the quality of any investigative practices undertaken. DES development should be influenced by surrounding case information and intelligence; however, it must be remembered that while there may be a reasonable belief that information of a certain type may help a given inquiry, until it is actually identified and reviewed, its true value will remain unknown. For that reason, no DES is likely to be 100% successful in its identification of relevant-only information. DESs must balance the need to determine the presence or absence of likely inquiry-relevant information against the need for efficiency and to maintain a defendant's privacy so far as is practicable. Given that a DES should also look at the case-requirements overall, it is possible that a DES may identify some of the data that may not currently be in the available dataset as being relevant. In addition, a DES may consider data of a certain type to be inquiry-relevant; however, it may never actually exist.

In a worst-case scenario, a DES may fail to define the need for investigative conduct that would subsequently have led to the identification of relevant case-content. This has the potential to be missed evidence.

The construction of a DES should never be compromised due to limited resources, only its deployment. For example, where only certain tool capabilities are available for a practitioner, the boundaries of their DES should not be defined by these capabilities, it should continue to define what is required for investigative success—this is merely the boundary of what is achievable under the current operational circumstances. Instead, the DES should forward the need to address such investigative requirements, but acknowledge that what is achievable in reality may fall short of this.

A DES is important as it sets out a "road map" of suitable investigative actions that must be followed. Achieving these actions is partly done through the use of appropriate tools.

3.4 | Introducing tools

In any examination, tools and techniques should be introduced to facilitate the successful deployment of a DES. In an ideal situation, tools should address all and only those requirements of the DES; however, in reality this is not always achievable. Figure 3 visualizes the introduction of tools and techniques into a hypothetical digital examination. To note, the size of each section is not representative of the size of the category it shows, it is merely for illustrative purposes.

Achieving a perfect overlap between a DES, tools and techniques and inquiry-relevant is the aim in all cases. This scenario could lead to the recovery of all available inquiry-relevant data, but it is difficult to achieve. However, beyond this, it is feasible that any deployed tools will also recover/return data that is non-relevant and beyond the scope of the

25739468, 2024, 1, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1507 by Test, Wiley Online Library on [28/02/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

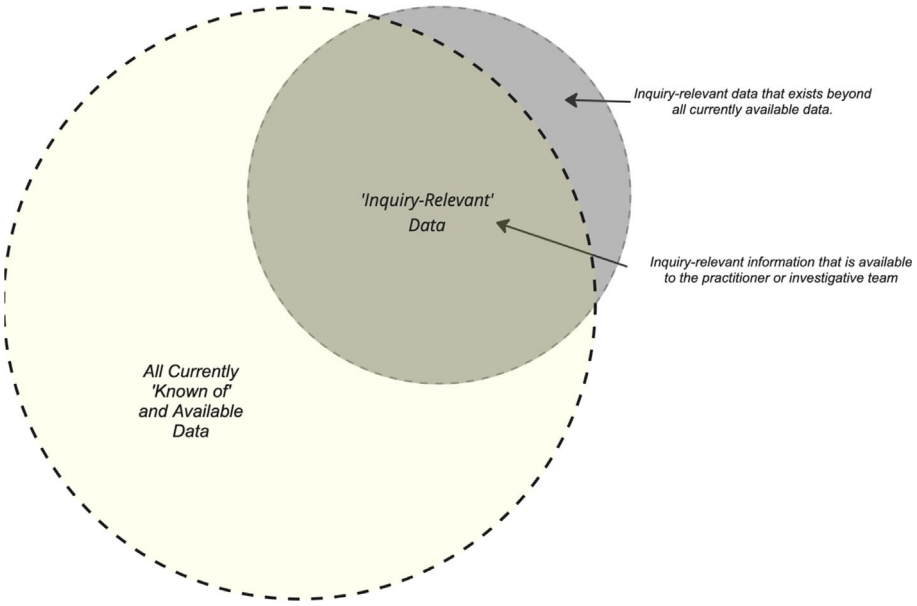

FIGURE 1 Apportioned data at the start of a DF examination.

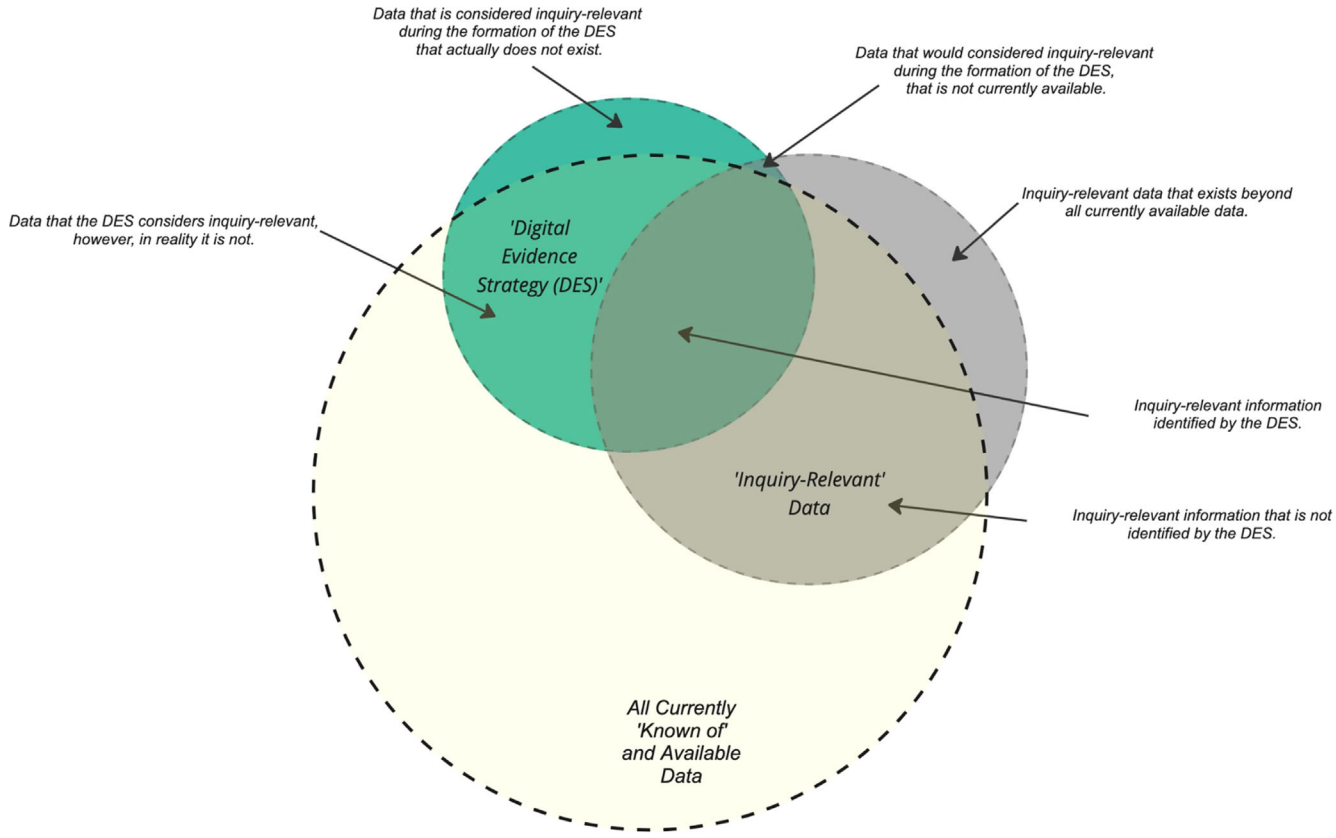

FIGURE 2 The deployment of a DES.

DES due to the way that it has been configured and deployed. This may be when a tool is configured to recover/parse identify data "too widely." Conversely, it is viable that a tool could recover/return data that is inquiry-relevant but was not envisaged within the development of the DES but on review of the data, it is subsequently deemed of interest. Again, a tool may have been configured too widely, but be fortunate in terms of recovering evidential information.

25739468, 2024, 1, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1507 by Test, Wiley Online Library on [28/02/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

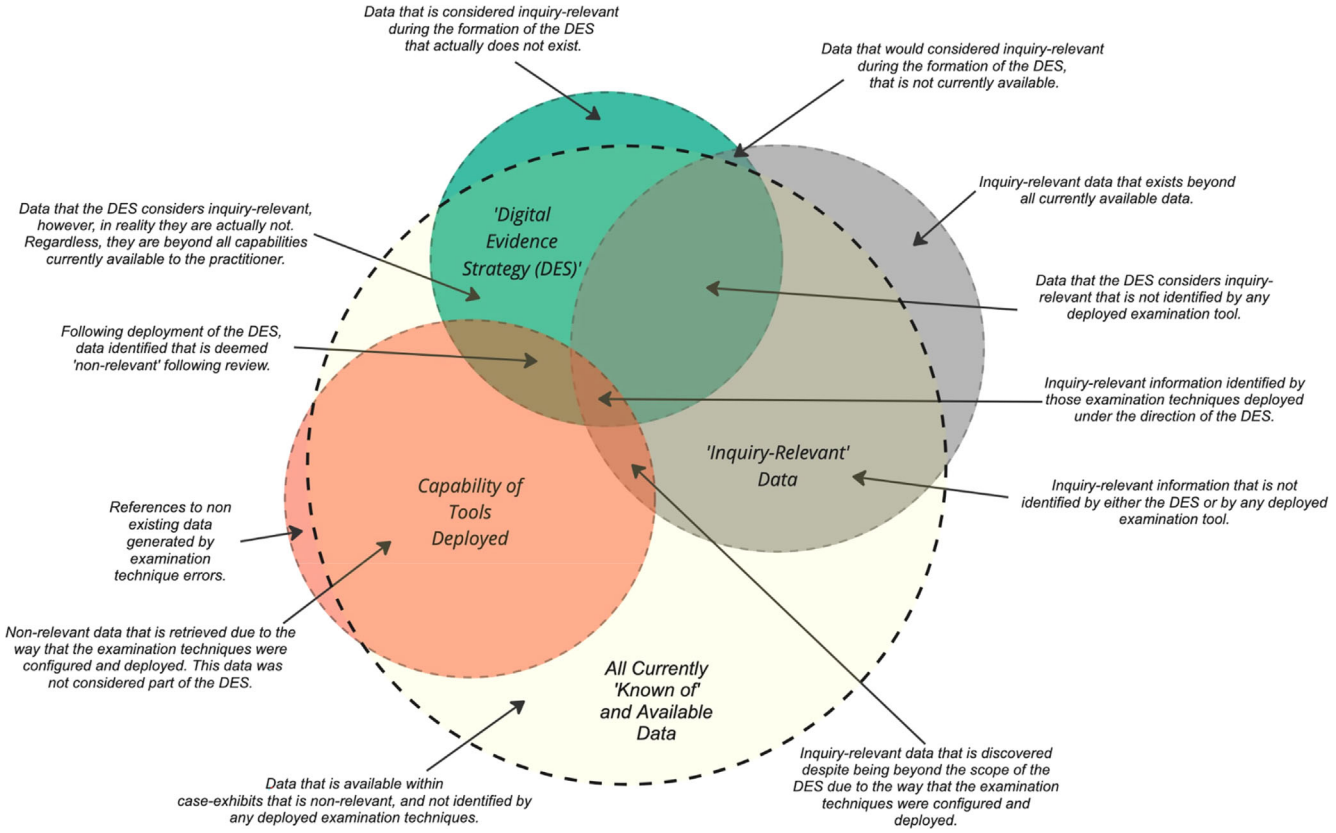

FIGURE 3 Introducing tools and techniques into a hypothetical digital examination.

Finally, and while unlikely in the majority of cases, tools and techniques may return references to non-existing data generated by examination technique errors.

3.4.1 | Two positions of unease

It is impossible to say for sure, but it is likely that in some digital investigations, not all of the available inquiry-relevant information will be found. It is considered that there are two circumstances when this will arise.

1. *Data that the DES considers inquiry-relevant that is not identified by any deployed examination tool*: In this scenario, a DES has identified certain data that is of investigative value, but either (1) they do not have tools and techniques available to them that can acquire, access, retrieve or parse this data (a "capability limitation"), or (2) they have with the ability to access, retrieve or parse this data, but they have been misconfigured. While it is easy to discuss these scenarios in hypothetical terms, yet in reality, it may not be possible to verify the existence of this relevant subset of data, given if we could then they would not remain unidentified.
2. *Inquiry-relevant information that is not identified by either the DES or by any deployed examination tool*: This scenario is similar to that noted above; however where above, consideration of the relevance and potential need to seek this data has at least been given by the DES, here it has not. Therefore, none of the investigative team even considered this data to exist and the currently deployed tools and techniques have not captured it.

4 | A FOCUS ON TOOLS

In all case work, a DF practitioner must choose the right tools for the job (Kiper, 2018) where a good DES defines a course of investigative conduct that any chosen tools must follow. DF tools are there to provide and enhance both

25739468, 2024, 1, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1507 by Test, Wiley Online Library on [28/02/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

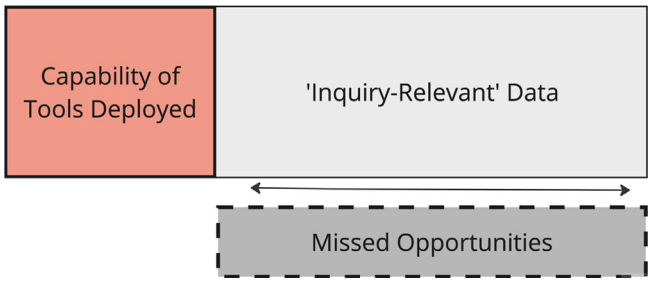

FIGURE 4 Tool limits and missed opportunities.

examination capability and performance and whether we like it or not, a practitioner's investigative ability in some cases will be constrained by the tools that they have access to. For example, in some cases, tools may provide access to or decode data that otherwise may not be achievable or practicable to do without them. While practitioners are the driving force behind any examination, the tools they use facilitate them to do their job. In any instance, it is not just a case of picking the right tool for a given task, but due to the complexity and array of functionalities offered by many modern DF tools, there is also a need to determine a tool's required configuration.

It is important for practitioners to recognize that those tools available to them are there to facilitate the deployment of their DES, they are not the DES. A DES proposes a series of investigative questions, and outlines those tools/techniques that may provide answers to them. A DES sets out the approaches that are believed to be required to effectively interrogate all available and relevant digital devices and data in order to answer any investigative questions about the surrounding circumstances of a case and achieve "success." This is achieved following a critical evaluation of all available and relevant case information, as well as an accumulation of the collective experience and knowledge of members of the investigative team. Constructing a DES is a logical, methodical and comprehensive process that also takes into account legal, ethical and professional implications when trying to conduct an examination. It is argued that this process cannot be disregarded.

In reference to Figure 3, one of the jobs of a DES is to describe a strategy that aligns with as much of the inquiry-relevant content that exists in a case. In an ideal scenario a DES describes a series of investigative tasks that if conducted correctly, all inquiry-relevant will be identified. In order to address these tasks, DF tools are often required. In this sense, a DES is a guide for how tools and techniques should be used. With this in mind, practitioners and investigative teams should resist the temptation to let any given tool(s) drive an examination strategy, in absence of a DES. Tool-driven strategies assume that the capability of any tool(s) deployed will be sufficient for meeting the needs of an examination. In some cases they may do so, but there is a risk that this approach fails to recognize what the actual needs of an inquiry are, instead in favor of simply deploying a tool regardless as to whether it is appropriate to do so or not. A DES determines the tools to be used, the tools do not determine the investigative strategy.

4.1 | A tool should not limit a strategy

A practitioner should also remember that the capability of their available tools does not always limit the extent of their examination. While in some cases, specifically in relation to tools for data-access, limitations can prevent further inquiries from taking place, it is sometimes possible to work beyond tools that are for searching, parsing and recovery. Practitioners should assess the capability of their tools and techniques and determine whether they can satisfy their investigative requirements. Where they cannot, they should assess whether it is possible and feasible to work beyond them and "*deploy themselves*" and their skills and knowledge to carry out further exploratory and interpretive work. One of the main concerns surrounding tool-driven strategies and the deployment of tools in general is the consensus that a practitioner's ability to undertake a DF examination is limited to what their tools can do or their configuration of them.

In some situations, the extent of their tools' ability or how they have configured it may only provide access to a subset of all available inquiry-relevant data (see Figure 4).

A failure to consider that any tool may have stopped short of what is required leaves a series of missed opportunities in the form of data which may impact an investigative team's understanding of events, case outcomes and decision making. While arguably it may provide comfort to practitioners to stay within their tools abilities, and in some cases, this may

25739468, 2024, 1, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1507 by Test, Wiley Online Library on [28/02/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

be all that is required, they must be able to work beyond when it is necessary, and at the very least consider the need to do so. One of the concerns surrounding tool-driven strategies is that it arguably becomes easy to forget what an investigation requires and instead, determine this to be simply the extent of what a tool has been configured or is capable of doing.

5 | CONCLUDING THOUGHTS

A DES is evidence of investigative competence, showing that the practitioner/investigator has an understanding of the circumstances of any alleged incident or offense and how to conduct a proper investigation of it. It is argued that tool-driven strategies do not offer evidence to the same extent and in turn can lead to examination practices falling short of what is required. When conducting a DF examination, investigative teams should consider the relationship between DESs and their tools and ensure that however they are approaching their work, they understand the benefits of ensuring appropriate strategic examination practices are in place. As a field, we must ensure that investigative skills and decision making are ranked as highly and considered as valuable as the ability to drive any tool. DF is an investigative science requiring those that practice it to have the ability more than just computing skills.

AUTHOR CONTRIBUTIONS

Graeme Horsman: Investigation (lead); methodology (lead); writing – original draft (lead); writing – review and editing (lead).

CONFLICT OF INTEREST STATEMENT

The author declares no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Graeme Horsman https://orcid.org/0000-0002-0685-0650

RELATED WIREs ARTICLES

Forming an investigative opinion in digital forensics

REFERENCES

College of Policing. (2022). *Managing investigations*. https://www.college.police.uk/app/investigation/managing-investigations

Cook, R., Evett, I., Jackson, G., Jones, P., & Lambert, J. (1998). A model for case assessment and interpretation. *Science & Justice*, *38*(3), 151–156. https://doi.org/10.1016/S1355-0306(98)72099-4

Guo, Y., Slay, J., & Beckett, J. (2009). Validation and verification of computer forensic software tools—Searching function. *Digital Investigation*, *6*, S12–S22.

Horsman, G. (2022). Digital evidence strategies for digital forensic science examinations. *Science & Justice*, *63*(1), 116–126.

Horsman, G. (2022). Defining principles for preserving privacy in digital forensic examinations. *Forensic Science International: Digital Investigation*, *40*, 301–350.

Horsman, G., Laing, C., & Vickers, P. (2014). A case-based reasoning method for locating evidence during digital forensic device triage. *Decision Support Systems*, *61*, 69–78.

Horsman, G., & Sunde, N. (2022). Unboxing the digital forensic investigation process. *Science & Justice*, *62*(2), 171–180.

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review*, *27*(1), 61–67. https://doi.org/10.1016/j.clsr.2010.11.001

ICO. (2020). *Mobile phone data extraction by police forces in England and Wales*. https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

ICO. (2021). *Guide to law enforcement processing*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

Jackson, G., & Jones, P. (2009). Case assessment and interpretation. In A. Moenssens & A. Jamieson (Eds.), *Wiley encyclopedia of forensic science* (Vol. 2, pp. 483–496). John Wiley & Sons.

James, J. I., & Gladyshev, P. (2013). *Challenges with automation in digital forensic investigations*. arXiv preprint arXiv:1303.4498.

Jarrett, A., & Choo, K. K. R. (2021). The impact of automation and artificial intelligence on digital forensics. *WIREs Forensic Science*, *3*(6), e1418.

Karie, N. M., & Venter, H. S. (2015). Taxonomy of challenges for digital forensics. *Journal of Forensic Sciences*, *60*(4), 885–893.

25739468, 2024, 1, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1507 by Test, Wiley Online Library on [28/02/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Kiper, J. R. (2018). *Pick a tool, the right tool: Developing a practical topology for selecting digital forensics tools* (pp. 1–24). SANS Institute-Information Security Reading Room.

National Centre for Policing Excellence. (2006). *Murder investigation manual*. https://library.college.police.uk/docs/APPREF/murder-investigation-manual-redacted.pdf

Privacyinternational.org. (2018). *Digital stop and search: How the UK police can secretly download everything from your mobile phone*. https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile

Quick, D., & Choo, K. K. R. (2016). Big forensic data reduction: Digital forensic images and electronic evidence. *Cluster Computing*, *19*, 723–740.

Rappert, B., Wilson-Kovacs, D., Wheat, H., & Leonelli, S. (2022). Evincing offence: How digital forensics turns big data into evidence for policing sexual abuse. *Engaging Science, Technology, and Society*, *8*(3), 8–30.

Roux, C., Bucht, R., Crispino, F., De Forest, P., Lennard, C., Margot, P., Miranda, M. D., NicDaeid, N., Ribaux, O., Ross, A., & Willis, S. (2022). The Sydney declaration—Revisiting the essence of forensic science through its fundamental principles. *Forensic Science International*, *332*, 111182.

Roux, C., Crispino, F., & Ribaux, O. (2012). From forensics to forensic science. *Current Issues in Criminal Justice*, *24*(1), 7–24.

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*(2), 183–194.

How to cite this article: Horsman, G. (2024). The importance of digital evidence strategies. *WIREs Forensic Science*, *6*(1), e1507. https://doi.org/10.1002/wfs2.1507

25739468, 2024, 1, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1507 by Test, Wiley Online Library on [28/02/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

https://dspace.org/

The importance of digital evidence strategies

Horsman, Graeme

2024-01
Wiley
https://doi.org/10.1002/wfs2.1507
Horsman G. (2024) The importance of digital evidence strategies. Wiley Interdisciplinary Reviews: Forensic Science, Volume 6, Issue 1, January/February 2024, Article number e1507

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