Forensic Science International: Digital Investigation 51 (2024) 301843



Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

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





Commentary:- Can I use that tool?

Graeme Horsman [1]

Cranfield University, College Rd, Cranfield, Wharley End, Bedford, MK43 0AL, UK

ARTICLE INFO

Keywords:
Digital forensics
Digital investigation
Digital evidence
Tools
Practitioners

ABSTRACT

The decision as to whether a given tool can be used for the purposes of conducting a digital forensic examination of a device and its data may seem straightforward, but it is not. As part of their work, practitioners must always seek to identify and use tools that are appropriate for their investigative tasks, deploy them reliably within an applicable scenario, and be able to trust and understand the results that they provide. Before they can begin to do this, they must first ask themselves the question - '*can I use that tool?*', where this work considers how a practitioner may begin to formulate an answer. By unpacking the hidden complexity of this question, it is suggested that five sub-questions must be explored by any practitioner when seeking to use a tool, namely - (1) '*what does that tool do?*'; (2) '*how do I use that tool?*'; (3) '*how does the tool do it?*'; (4) '*does the tool do it properly?*' and (5) '*should I use the tool?*'. This work discusses each in turn and the risks they pose to a practitioner.

1. Introduction

When conducting digital forensics (DF) examinations, practitioners are reliant upon specialist tools for searching, recovering and presenting digital traces, which they will subsequently review and evaluate for relevance (Dimpe et al., 2017; Sindhu et al., 2012). DF tools form a core part of the digital device investigative process (Carrier, 2002; Rafique et al., 2013), and whilst their importance cannot be understated, it is also necessary to note that the use of them should not be completely unfettered, and any determination of their suitability for a given task go without scrutiny. In all cases a practitioner must first decide whether any given tool 'can' be used, before they go ahead and deploy it within their casework; a task that is multifaceted (Barik et al., 2022). What we refer to here is not an attempt at the use of a tool in the physical sense (of course, bids to physically operate a tool can always be made), but instead, emphasis is placed upon the need for an upfront assessment of the appropriateness of a tool's use by a practitioner within their current investigative circumstances (Pernul, 2023). Therefore the question '*can I use that tool?*' is one that requires a practitioner to evaluate all of the factors that may lead to the use of a given tool in their DF examination being wrong, or the correctness of such a decision being subject to question. The DF field has long surpassed the point where it is deemed sensible or acceptable to deploy tools '*straight from their box*' without first assessing their accuracy and suitability for any task that their use is intended for (Brunty, 2023). Whilst evaluating a tool may seem simple, it is a job that actually maintains complexities which may be overlooked.

Within the field of DF there are multiple mainstream commercial tools in circulation, each containing many different, and complex functionality. In addition, Wu et al. (2020a), note that frequently, tools are produced and disseminated following published research. Choosing the right tool for the job is just as important in the domain of DF as it is in all other areas (Ramadhani et al., 2020) and as practitioners encounter or identify investigative 'gaps' within their DF examinations, it is often the case that they will seek to address these with any appropriate functionality offered by tools that they have available (European Committee for Standardization, 2022). Doing this has the potential to lead to a more comprehensive interrogation of any seized and acquired data, providing that whatever tool that is identified is suitable for use within the context of their investigative scenario (Lovanshi and Bansal, 2019). All practitioners must strive for what we consider '*safe tool usage*'; referring to an instance where a relevant tool is reliably and properly deployed within an applicable and appropriate scenario, and the results that it provides can be trusted and understood. Whilst this may seem obvious, it is not always easy to consistently and correctly make a correct assessment regarding when a particular tool can and should be used, and this decision process requires unpacking. In all cases, before using a tool, practitioners must start with raising an initial question of '*can I use that tool?*', and this work explores how they can begin to provide a reliable and defensible answer to this query.

E-mail address: graeme.horsman@cranfield.ac.uk.

[1] The author is responsible for all work in this article.

https://doi.org/10.1016/j.fsidi.2024.301843
Received 17 July 2024; Received in revised form 16 October 2024; Accepted 8 November 2024
Available online 17 November 2024
2666-2817/© 2024 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

2. Can I use that tool?

Any tool that is appropriate for a given exercise, deployed properly, and is trustworthy in terms of the results it produces can improve the robustness of a DF examination. Conversely, tools that are not suitable for a given task, flawed or used inappropriately can be detrimental and undermine the reliability of any forensic work conducted. Practitioners may opt to use a tool as part of their work due to its stated capability (or its performance metrics for a given task (Salih et al., 2023; Stanivuković et al., 2016; Dizdarević et al., 2020)), which may allow them to access and/or decode data that they may otherwise have not been able to do (European Committee for Standardization, 2022). Other factors driving a decision to use a particular tool include a practitioner's familiarity with a tool (both knowledge of it and training undertaken), their organisation's tool-budget, how easy a tool is to use (Karabiyik and Karabiyik, 2020; Wu et al., 2020b), or potentially the tool's popularity (Barik et al., 2022). Studies that consider the suitability of DF tools have focused on how well a tool performs under specific conditions - something that is more akin to a technical evaluation of a tools performance (see for example, Saleem et al. (2016), and Dimpe and Kogeda (Dimpe et al., 2019)), but omit a discussion of the 'non-tool performance' related technical factors that impact any decision regarding the appropriateness of using a tool. Often, and understandably, the ability to establish that a tool is going to function correctly is often a primary factor for its selection. Whilst a correctly functioning tool is vital, there should be more evaluation of a tools suitability for a given investigative task than just the fact that it 'works'. It is therefore necessary to distinguish the concept of tool evaluation from that of an assessment of tool selection suitability. The former aims to assess and understand how a tool performs when faced with specific conditions (Flandrin et al., 2014), where the latter is concerned with a wider appraisal of the tool, the practitioner and the investigative circumstances faced, in order to determine whether any selected tool offers the best solution for any examination task.

The task of determining whether to use a tool is deceptively simple (Karabiyik and Karabiyik, 2017), and as a result, this work proposes a formalisation of this decision process, coupled with the unpacking of its hidden complexity. By doing this, practitioners will benefit from

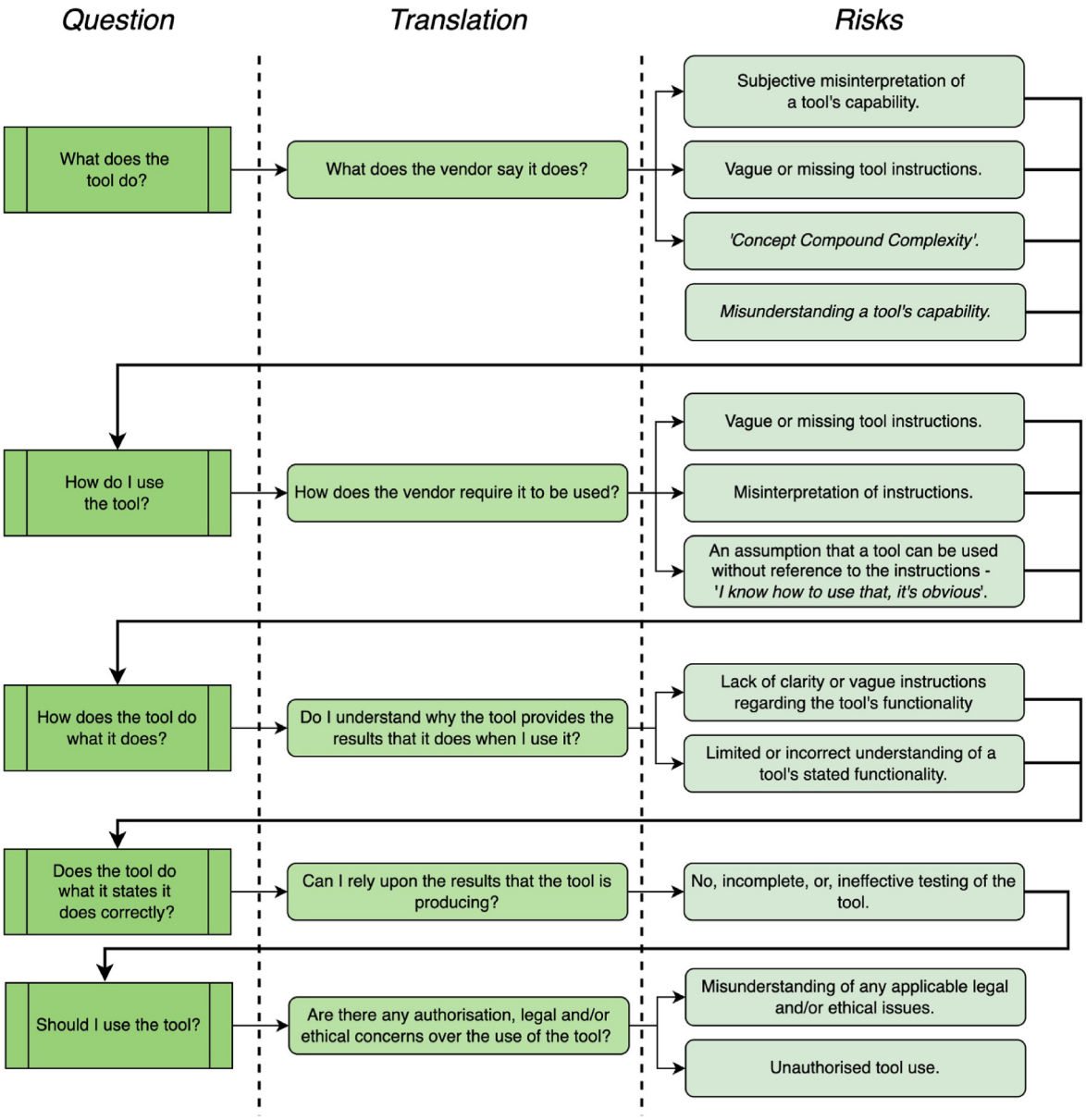


Fig. 1. Establishing when a tool can be used.

exposing the risks associated with considering whether to use a tool, allowing them to ensure they are acknowledged and addressed. With that in mind, it is considered that when deciding whether a tool should be used, a practitioner may consider five 'simple' questions, with five not so simple 'answers'.

2.1. Five questions that a practitioner may consider

When unpacking the question '*can I use that tool?*', there are five questions a practitioner should ask themselves, and answer:

1. 'What does that tool do?'
2. 'How do I use that tool?'
3. 'How does the tool do it?'
4. 'Does the tool do it properly?'
5. *'Should I use the tool?*'

Each of these five questions must first be translated in order to determine what they mean in reference to operational practices. Then, in answering these questions, practitioners must acknowledge and address their associated risks. Fig. 1 provides a breakdown of these five questions, and each are discussed in turn below.

2.1.1. Question 1 - *'What does that tool do?'*

Before a practitioner can begin to evaluate whether it is appropriate to use any given tool within an investigation, they must first determine what it does. This may seem an obvious question and in an operational environment, this question may look something akin to - "*can tool 'X' do task 'Y' that I require for my case*", and practitioners will frequently ask this in any multitude of scenarios. Whilst interpreting what this question is asking may seem straightforward, after all, practitioners should not (and possibly cannot) utilise any tool as part of their work if they do not know what it does, it actually maintains hidden complexity. When a practitioner begins to assess what a tool does, they must actually determine what any tool's vendor/creator defines as their tool's functionality, and the scope of it (Horsman, 2024a). Whilst a practitioner following subsequent testing may deem a tool has additional uses, the starting point lies at what the tool's vendor says their tool does, and practitioners themselves should refrain from extending a tool's scope of use if there are no grounds to base this on other than mere conjecture on their part (Horsman, 2024a).

If a practitioner does not know what a tool does, they should never deploy it in live casework and seek to utilise any results it provides. Being able to accurately determine any tool's functionality forms the basis of a practitioner's decision as to whether it is appropriate to use it within the bounds of their current investigative context. However, when determining what a tool does, there are four risks that may impact upon any final determination:

1. *Subjectivity*: Practitioners must be aware of their potential to misinterpret what a tool's capability is. Whilst in almost all cases a practitioner will need to evaluate any instructions provided with a tool in order to determine what it does, this evaluation naturally carries an element of interpretation and practitioners should be aware of their potential to misinterpret a tool's functionality and guard against it. A practitioner must start with what a tool's vendor/creator says it does, not what they think it could do, and without making conscious efforts to ensure these two concepts are distinguished from one another, it may be easy for the lines between the two to become blurred. This risk is heightened in cases where a tool's accompanying documentation remains vague or utilises capability statements that are wide-ranging and vulnerable to multiple different interpretations. The result of which may be the use of a tool by a practitioner in conditions which the tool is not appropriate for, or an expectation that a tool will perform in a way that it cannot.
2. *Vague/missing tool instructions*: Arguably, all tools must be accompanied with a robust set of instructions that both detail what the tool does, and help any potential users to operate it effectively. However, given the complexity of many DF tools, creating instructions which comprehensively document a tool's functionality, capability and constraints is a significant task. In reality, some tools may have user manuals which fall short of the detail required for a practitioner to fully understand what their capability is and how to use them. Practitioners must evaluate whether they are in a position (or can get to a position) where they are able to determine the extent of a tool's functionality and to be sure that it will suitably address their investigative requirements, before using it.
3. *'Concept Compound Complexity'*: Concept Compound Complexity (CCC) is a term coined here that relates to the need for complex investigative concepts utilised within a tool to be unpacked and thoroughly described if they are to be fully understood. Take for example, a tool that states that it is capable of carving for specific files; the concept of file carving is complex and to fully understand what the tool can do within the realm of 'file carving', the concept needs to be further unpacked and fully described by the tool's vendor (for example, does the tool only carve contiguous files? How is file fragmentation handled? How are compressed structures processed?). When tools engage with complex functionality, practitioners must take care when assessing the breadth of the functionality being offered, and not make any assumptions as to the extent of it. Being able to fully establish the remit of any tool's complex functions permits the practitioner to better address any uncertainty in regard to the results generated by a tool, and any implications arising from these. Perhaps a simpler illustrative example includes where a tool claims to be able to parse a specific artefact, but remains silent on which, or if all of the fields/attributes the artefact contains are included in any results that the tool provides to the user.
4. *Misunderstanding*: In all cases, a practitioner may simply misunderstand what a tool states that it does as a result of gaps or flaws in their own knowledge. This must be distinguished from a misinterpretation error.

Whilst it does not provide a perfect solution, arguably, some of the risk noted above can be mitigated through the production of suitably detailed tool documentation, and the subsequent thorough review of it by a potential tool user. Whilst it could be argued that vendor training may plug some of this gap, some tools do not have accompanying training, and even where training is available, quality documentation must still be available so practitioners can refer to it in the future, if needed.

2.1.2. Question 2 - *'how do I use that tool?'*

When we ask the question '*how do we use tool 'x'?*', what practitioners should be referring to is how the tool's vendor requires them to operate it. Only the tool vendor can define the conduct required for their tools to be effectively used - i.e. those configurations and specific scenarios required for the tool to perform as expected (Horsman, 2024a). Whilst a tool-user may identify subsequent ways to use a tool, for example, it may be determined that it can be used to parse artefacts beyond any versions of the artefact that are stated in the tool's documentation, the practitioner takes responsibility for extending the tool's scope of use. When addressing how a tool should be used, there are three main risks:

1. *Vague/missing tool instructions*: Similar to Question 1 above, vague or missing instructions that define how a tool should be configured and used pose a risk to the practitioner (Ramadhani et al., 2020). Where instructions fail to provide details regarding a tool's operational conditions and the necessary configurations and setup required for it to run successfully, a practitioner may seek to fill in these gaps via educated guesses. Practitioners may start to assume what a tool may do and how it does it based on what any 'functions' within a tool are

named by a vendor, arguably a risky approach. An improvement on this position lies with a practitioner determining how to use a tool following the testing of it under controlled conditions. All tools should be tested prior to use, but the testing conducted must be of sufficient quality. Arguably, there is less chance of using a tool incorrectly if the tool's vendor provides robust and correct instructions that describe how to use it properly.

2. *Misinterpretation of instructions*: As a starting point we will work from the assumption that all tools will maintain some form of instructions; instruction-less tools pose too great of a quality-risk to be used in a forensic capacity. Even when instructions are provided, a practitioner must decipher them correctly in order to deploy the tool appropriately. A tool vendor may define a correct standard operating procedure for their tool, but there remains a potential for any practitioner to fail to follow it correctly. Any instructions should be clear, concise and, as far as possible, remove the potential for them to be misinterpreted. If possible, the limitations of any tool should also be highlighted.
3. *An assumption that a tool can be used without reference to the instructions - 'I know how to use that, it's obvious'*: Practitioners must guard against assuming that they know how to use a tool without first making reference to its instructions. Reviewing tool instructions may not be an exciting task, but it is one that is important. In some cases it may be tempting to 'jump straight in' and use a tool. In others, a tool's menus and labels, or its high level stated functionality may encourage the perception that it is obvious as to how it should be used and deployed. Restraint from deploying a tool in such ways should be exercised and confirmation of how any tool should be deployed should be first sought.

2.1.3. Question 3 - 'How does the tool do it?'

All practitioners must understand how the tools that they are using do the things they do, and the results that they provide. Carvey (Harlan Carvey, 2009) coined the term 'Nintendo forensics' in reference to the need for practitioners to have the appropriate knowledge and skills before deploying tools. We also see similar activity referred to as 'push button forensics' (Horsman, 2019; Shavers and Zimmerman, 2013), the premise being that a tool is not 'magic' and therefore we cannot treat the results that it generates as being produced by such means; we must be sure what the tool is doing and why. This work is not discouraging the use of automation in regard to the processing of data, in fact it is becoming a crucial part of being able to handle the volume of data practitioners are now regularly experiencing in their cases. However, this need should not supersede the requirement to first understand how any such tools are conducting their work; placing blind faith in any tool's functionality maintains risk. We are in a position now where tools offer a plethora of functionality and Horsman (2024b) suggests that the tools themselves may be considered a strategy and therefore deployed with less rigour being applied as to what they are doing. Before tools can be used, practitioners need to understand what they are doing, and there are two main risks associated with doing this:

1. *Lack of clarity or vague instructions regarding the tool's functionality*: Limitations in respect of a tool's instructions remains a common theme, and in regard to how a tool is conducting its functions, vague descriptions may impact whether a practitioner can understand why it is producing the data that it does. Whilst it is recognised that understanding any underlying algorithms that a tool deploys is not easy, it is actually more likely that most never have an opportunity to try, as such details are not always observed in tool documentation. One must ask whether this should remain the norm (whilst also recognising intellectual property concerns and arguments), and in a time where greater scrutiny is being applied to the performance of tools, arguably, details of critical functionality would support and likely improve tool evaluation processes. Even at a high-level, some description of functionality should be provided by a tool in order for a fair assessment to be made as to when a tool is suitable for deployment and in what circumstances. Yet is it recognised that tool vendors may want to protect this information and prevent it from being shared with competitors.
2. *Limited or incorrect understanding of a tool's stated functionality*: In cases where a tool does provide a detailed description regarding how it conducts its functionality, a practitioner must be capable of understanding it. For example, a tool may provide details of the protocols and algorithms it uses when interacting with data, but to be able to evaluate whether they are suitable in the current investigative scenario, a practitioner must have the knowledge and skills to be able to understand it. The presence of detailed instructions outlining functionality does not guarantee the tool's suitability, more that it provides a chance to conduct a more rigorous evaluation of the tool's suitability for a given task.

2.1.4. Question 4 - 'Does the tool do it properly?'

Fundamental to all DF examinations is the requirement to utilise tools that are performing correctly (Brunty, 2023; Horsman, 2018, 2019; Beckett and Slay, 2007) raising the question to the practitioner - '*can I rely upon the results that the tool is producing?*'. This risk has been discussed in relative depth over recent years with documents describing both the need for method and tool validation and associated practices (Forensic Science Regulator, 2020) relevant to the task of determining whether a tool is performing properly in all cases. An assessment of whether a tool is performing correctly requires a practitioner to assess a tool's performance, where one main risk is associated:

1. *No, incomplete, or, ineffective testing of the tool*: Whilst we recognise the need to evaluate tools, and demonstrate that this has been done effectively, there is a risk that tools are used which have not been subject to any evaluative practices. Even if tool testing has been conducted, it must be comprehensive if the results of it are going to be relied upon when assessing whether a tool is performing accurately.

2.1.5. Question 5 - 'should I use the tool?'

Finally, even if a tool may appear suitable for the investigative circumstances that a practitioner requires it for, they need to consider whether they should use the tool. This requires first ensuring that they have the authorisation for using a tool from whomever is in a position to provide such permission, and this depends upon the circumstances of any case in question and potentially any laboratory accreditation governance like ISO/IEC 17025:2017. Organisational and laboratory practices may define who and how authority for the use of specific tools should be obtained. In addition, given the nature and scope of many DF examinations, and the range and extent of functionality that some tools maintain, it is necessary to ensure that it is both legal to deploy any tool with a set of given circumstances, and that it is ethical to do so (Ferguson et al., 2020). There are two main risks associated with this question:

1. *Misunderstanding of any applicable legal and/or ethical issues*: Investigative complexities and a fast moving technical and legislative landscape may make it difficult for practitioners to determine the legality of their conduct in relation to a tool. Whilst arguably in all cases, checks should be made as to the legality of any tool usage, if any potential legal issues are not obvious or understood, then unintentional tool-misuse may occur. Further, as we see developments with professional and ethical considerations and principles surrounding policing practices (College of Policing, 2024), it is important that practitioners are abreast of such developments and how they may impact the acceptability of tool usage.
2. *Unauthorised tool use*: A practitioner may not realise that the use of any given tool requires authorisation, or forget to confirm that the use of a tool is permitted. It may even be possible that a tool's use is incorrectly authorised.

3. Concluding thoughts

This work suggests that the assessment as to whether a tool can be used with an investigation requires systematic consideration of five core concepts. The aim is to help practitioners to evidence that they have conducted a thorough evaluation of the suitability of the tools they have utilised in their case work, those chosen are suitable for the examination task they have been used for, and any judicial processes can take confidence from the practitioner having done so. Whilst it is recognised that any decision as to whether to use a tool may need to be made quickly and be made based upon perceived functionality in an effort to immediately address the needs of any case work, recognition of the complexity involved with determining when a tool can be used is needed. By unpacking the decision to use a tool, revealing five core questions and their associated risks, a practitioner can begin to ensure that their use of a tool in any given circumstance is appropriate and effective. It is suggested that in all cases, a practitioner evaluates their answers to these five questions in order to justify any tool usage within their case work. As part of doing this, a practitioner may want to consider and evaluate the source/origin of a tool when deciding whether to use it. Whilst it is argued that the source of a tool alone is not necessarily a reason to not use it, an evaluation of a tool's source/origin may have an impact on a practitioner's ability to answer the aforementioned five questions and the level of reliability they feel they can attribute to their answers.

Conflicts of interest

No conflicts of interest to declare.

Data availability

No data was used for the research described in the article.

References

Barik, K., Abirami, A., Konar, K., Das, S., 2022. Research perspective on digital forensic tools and investigation process. Illum. Artif. Intell.Cybersecur. Forensic. 71–95.

Beckett, J., Slay, J., 2007. Digital forensics: validation and verification in a dynamic work environment. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE, 266a-266a.

Brunty, J., 2023. Validation of forensic tools and methods: a primer for the digital forensics examiner. Wiley Interdiscip. Rev.: Forensic Sci. 5 (2), e1474.

Carrier, B., 2002. Open Source Digital Forensics Tools: the Legal Argument.

College of Policing, 2024. Ethical policing principles. Available at: https://www.college.police.uk/ethics/code-of-ethics/principles.

Dimpe, P.M., Kogeda, O.P., 2017. Impact of using unreliable digital forensic tools. In: Proceedings of the World Congress on Engineering and Computer Science, 1, pp. 118–225.

Dimpe, P.M., Kogeda, O.P., 2019. A model for evaluating digital forensic tools. J. Eng. Appl. Sci. 14 (19), 7048–7058.

Dizdarević, A., Baraković, S., Baraković Husić, J., 2020. Examination of digital forensics software tools performance: open or not?. In: Advanced Technologies, Systems, and Applications IV-Proceedings of the International Symposium on Innovative and Interdisciplinary Applications of Advanced Technologies (IAT 2019). Springer International Publishing, pp. 442–451.

European Committee for Standardization, 2022. Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain. Available at: https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/RI/cwa17865_2022.pdf.

Ferguson, R.I., Renaud, K., Wilford, S., Irons, A., 2020. PRECEPT: a framework for ethical digital forensics investigations. J. Intellect. Cap. 21 (2), 257–290.

Flandrin, F., Buchanan, W.J., Macfarlane, R., Ramsay, B., Smales, A., 2014. Evaluating Digital Forensic Tools (DFTs).

Forensic Science Regulator, 2020. Method validation in digital forensics. Available at: https://assets.publishing.service.gov.uk/media/5f6ca608d3bf7f7231ac65e0/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf.

Harlan Carvey, 2009. Windows 7 and the future of forensic analysis. Available at: https://windowsir.blogspot.com/search?q=nintendo.

Horsman, G., 2018. "I couldn't find it your honour, it mustn't be there!"–Tool errors, tool limitations and user error in digital forensics. Sci. Justice 58 (6), 433–440.

Horsman, G., 2019. Tool testing and reliability issues in the field of digital forensics. Digit. Invest. 28, 163–175.

Horsman, G., 2024a. Sources of error in digital forensics. Forensic Sci. Int.: Digit. Invest. 48, 301693.

Horsman, G., 2024b. The importance of digital evidence strategies. Wiley Interdiscip. Rev.: Forensic Sci. 6 (1), e1507.

Karabiyik, U., Karabiyik, T., 2017. Digital Forensics Tool Selection with Multi-Armed Bandit Problem.

Karabiyik, U., Karabiyik, T., 2020. A game theoretic approach for digital forensic tool selection. Mathematics 8 (5), 774.

Lovanshi, M., Bansal, P., 2019. Comparative study of digital forensic tools. Data, Eng. Appl. 2, 195–204.

Pernul, G., 2023. Support tool selection in digital forensics training. In: Ubiquitous Security: Second International Conference, UbiSec 2022, Zhangjiajie, China, December 28–31, 2022, Revised Selected Papers. Springer Nature, p. 3.

Rafique, M., Khan, M.N.A., 2013. Exploring static and live digital forensics: methods, practices and tools. Int. J. Sci. Eng. Res. 4 (10), 1048–1056.

Ramadhani, E., Wahyuni, E.G., Pratama, H.R., 2020. Design of expert system for tool selection in digital forensics investigation. In: IOP Conference Series: Materials Science and Engineering, 852. IOP Publishing, 012137, 1.

Saleem, S., Popov, O., Baggili, I., 2016. A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis. Digit. Invest. 16, S55–S64.

Salih, K.M.M., Dabagh, N.B.I., 2023. Digital forensic tools: a literature review. J. Edu. Sci. 32 (1), 109–124.

Shavers, B., Zimmerman, E., 2013. X-ways Forensics Practitioner's Guide. Newnes.

Sindhu, K.K., Meshram, B.B., 2012. Digital forensic investigation tools and procedures. Int. J. Comput. Netw. Inf. Secur. 4 (4), 39.

Stanivuković, D.R., Ranđelović, D.M., 2016. Application of multiple criteria decision making in the selection of digital forensics software. Vojnotehnicki Glas. /Mil. Tech. Cour. 64 (4), 1083–1101.

Wu, T., Breitinger, F., O'Shaughnessy, S., 2020a. Digital forensic tools: recent advances and enhancing the status quo. Forensic Sci. Int.: Digit. Invest. 34, 300999.

Wu, T., Breitinger, F., O'Shaughnessy, S., 2020b. Digital forensic tools: recent advances and enhancing the status quo. Forensic Sci. Int.: Digit. Invest. 34, 300999.



https://dspace.org/

Commentary:- Can I use that tool?

Horsman, Graeme

2024-12-01
Elsevier
https://doi.org/10.1016/j.fsidi.2024.301843
Horsman G. (2024) Commentary:- Can I use that tool? Forensic Science International: Digital Investigation, Volume 51, December 2024, Article number 301843

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