Science & Justice, Volume 62, Issue 5, September 2022, pp. 515-519
DOI: 10.1016/j.scijus.2022.07.006

That tool is rubbish!...or is it?

Abstract
Digital forensic practitioners often utilise a range of tools throughout their casework in order to access, identify and analyse relevant data, making them a vital part of conducting thorough, efficient and accurate digital examinations of device content and datasets. Whilst their importance cannot be understated, there is also no guarantee that their functionality is free from error, where similarly, no practitioner can 100% assure that their performance is flawless. Should an error occur during an investigation, assuming that it has been identified, then determining the cause of it is important for the purposes of ensuring quality control in both the immediate investigation and for longer term practice improvements. Perhaps anecdotally, a starting position in any postmortem review of an error may be to suspect that those tools used may be at fault, where recent narratives and initiatives have enforced the need to evaluate all tools prior to them being used in any live investigation. Yet, in addition, an error may occur as a result of a practitioner's investigative conduct. This work discusses the concept of 'fault-attribution', focusing on the roles of the forensic tool and practitioner, and provides a series of guidelines for determining responsibility for an investigative error.

Keywords: Digital forensics; Tools; Investigation; Error

1 Introduction
'*A bad workman blames his tools*' - an English proverb that considers poor performance and the potential for it to be attributed to any equipment being used to undertake a task, rather than the skills of those conducting the work [1]. In most instances where this description is used, it likely stands to provide an oversimplification and possibly misleading reason as to why any problem has occurred. This is due to the fact that in almost all cases and contexts, the level of success and quality of any work carried out is impacted by a number of factors beyond a simple consideration of whether any tool being used has 'worked'. Despite this, an individual may initially and autonomously consider the tools they have used to be at fault for any error in the work produced, rather than weaknesses in their own investigative approaches, particularly if these approaches had been subjected to review, and had subsequently been agreed as a form of their organisation's best practice. It should be noted that it is not being insinuated that practitioners who do so are being subconsciously negligent and trying to absolve themselves of any potential liability for a fault or limitation in their capability. Instead, merely that it is likely that a strong belief that their working practices are robust understandably exists in such cases - after all processes that are vetted and agreed should instil confidence in their use, leaving arguably a natural instinct to question any tool used. In these instances, the evaluation of any tools used may offer an acceptable starting point for determining the cause of a fault but it cannot be the only quality assurance and control mechanism deployed, where all aspects of any investigative procedure used should be assessed for the presence of any deficiencies that could have led to an error.

In the context of the field of digital forensics (DF), practitioners are reliant on their forensic tools which allow them to conduct and complete their defined investigation workflows with tasks including data access and acquisition, data searching, and, artefact parsing and display. Whilst DF tools do not '*do*' the forensic work for the practitioner as expert knowledge is still required in multiple areas of the investigative process beyond the ability to operate a tool, they still play a fundamental role by helping the practitioner as they aim to complete a thorough,

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.2022.07.006. Please refer to any applicable publisher terms of use.

robust and efficient examination. To contextualise this point, the practitioner may use a tool to either find, parse and present information for review, however, any decisions regarding the suitability of any tool for this task, the interpretation of any results it provides and the determination of any relevance of this data sits with the practitioner. A tool does not decide what data is of investigative-worth, but it does provide the practitioner with an opportunity to do this.

1.1 A 'correctly functioning' tool

Those operating in all fields do so with the hope that any tools they are using function correctly, with the DF discipline being no different, where some attention needs to be given to what exactly '*correctly functioning*' means. Here, reliance is placed upon any tool creator/vendor to determine this. It is suggested that a tool functions correctly when it conducts those tasks that its creator/vendor states it can do to any potential users, accurately, which are often described within and therefore bound by a contractual agreement (software licensing agreement), when operated within a set specific parameters as defined by the creator/vendor. Therefore, a tool's creator/vendor can be considered the central component to establishing when a tool is 'correctly functioning', as it is their description of their tool's capability that defines this remit. Simply put, a tool creator/vendor defines what their tool does, and, the conditions that this performance can be expected. Where the practitioner operates the tool within its stated conditions for performance and the tool does not accurately perform those tasks that the creator/vendor contracted that it is capable of, the tool is not functioning correctly.

When considered in this way, 'correctness' requires an evaluation of what a tool does against what a tool has been stated to do. Approaching this task in this way requires the practitioner to adopt a cautious stance when relying upon the creator/vendor's statements of tool functionality in order to then determine a tool's 'correctness' and to make sure that they fully understand them. In extreme cases, a tool could be defined by its creator/vendor to conduct a task which may in real-terms be erroneous or technically inaccurate, yet in such scenarios the tool itself would be performing as it was intended to do - arguably correctly. Similarly, the extent to which a task is completed by a tool may not be defined in enough detail, leaving a practitioner with ambiguity as to how far a tool '*must go*' before it is considered to be operating correctly (i.e. parse one or all fields of a specific log file).

Given their importance, DF tools have been the focus of recent narratives concerning examination quality assurance and the need to develop processes that can validate the accuracy of any results they provide [2]. Despite the heavy reliance placed on such tools to conduct forensic work, the field must not adopt a stance that always considers the tools themselves to be the determinative factor between a hypothetical '*good*' and '*bad*' examination. In reality, they are simply one variable amongst many that can impact the quality of any work forensic conducted. With this in mind, it is argued that given the scrutiny that DF tools are receiving, there is a need to provide direction regarding if and when a tool may have fault attributed to it.

Should an investigative issue occur, clarity is required as to whether and when any fault lies with the tool being used, with the practitioner conducting the work, or, with any wider investigative processes and procedures being deployed. This helps to ensure that an appropriate course of action is taken that safeguards the reliability of any results provided in the immediate case. In addition, determining and understanding the cause of an error

improves examination quality control and assurance on a wider scale, both in the short and long term by helping to understand the examination conduct taking place. If practitioners and organisations can determine the source of an error, efforts can be made to understand why this has occurred and the processes that can be put in place to safeguard against similar occurrences in future practice.

This article debates the concept of fault attribution in DF, focusing on the roles of the practitioner and any tool used with an aim to provide support for those conducting fault assessments.

2 Tools

In DF, both the examining practitioner(s) and the tools they use play a major role in the investigative process, where each can have an impact on the overall quality and reliability of any results obtained. Whilst the practitioner (with guidance from their wider investigative team and their organisation) is often responsible for the design and deployment of an effective digital evidence strategy which will inevitably include the examination and interpretation of relevant data, their chosen tools should support them to conduct these tasks. Often, practitioners and their organisations (through defined and approved best practices) are responsible for their choice and deployment of tools for use in their casework, no one else. These tool-focussed decisions are often fundamental to ensuring a robust and effective examination takes place, free from issue or concern. Whilst this is the aim, in some cases, tool errors may still occur. It also goes without saying that the implications caused by errors present in any criminal investigative process (particularly if undetected) have the potential to be severe for all parties involved. The prevention, or at worst the mitigation of error is paramount to ensuring appropriate quality standards are maintained, however, in some cases this may not be successfully achieved and problems still occur.

In regards to DF and the types of fault which may occur, where an investigative issue, error, omission or limitation has been established, the identification of its cause is necessary. This is not only for appropriate responsibility for the event to be associated with it, but also to ensure that the cause of it is fully understood, a solution to the immediate issue is defined and, preventative measures are put in place to stop future occurrences. It should be stressed that fault attribution is not part of a ‘blame game’, instead, it serves as a valid and important part of quality control and assurance mechanisms in all forensic sciences disciplines. As a result, this article poses the following question - ‘*if a fault occurs, how do we determine who or what it should be attributed to?*’. With this in mind, we consider that in some cases there may be a need to conduct fault-attribution processes, where here we will focus on two areas, the investigating practitioner and, their tools. Whilst it is appreciated that errors can stem from beyond these two entities, discussions here will remain confined and focused on these parties due to the primary role they both have in the investigative process.

When approaching the task of fault attribution, this work suggests that there are four principles to consider when attempting to determine whether the practitioner and/or any wider investigative procedure or, the tools they have used are the cause of any fault. These principles are intended to offer structure and support to those involved in fault attribution processes and to help those conduct the classification of fault types in a consistent way through their definition.

2.1.1 'Understanding' functionality

Fundamental to DF casework is the need for all practitioners to know and understand the tools and any of their functions which they intend to use, prior to deploying them in any real-world capacity. By '*know and understand*', it is suggested that the practitioner must be aware of the purpose and impact of the tool/function in regards to their given dataset (in essence, '*what is the tool/function doing?*'), the remit and limitations of it, and, how to invoke it correctly within their current investigative scenario. Put simply, the practitioner must '*get to know their tool properly*' so that they appreciate what it is supposed to do, and this requires an investment in time and effort to allow the practitioner to evaluate any tool/function thoroughly. Any tool's functionality must be determined and objectively evidenced prior to its use; a practitioner should not assume the suitability and use of a tool solely because they think they know what the tool/function does. Whilst a practitioner may understand the general premise of a tool or tool suite, in actuality, they must acquire in-depth knowledge of its ability, remit and how to use it, not only for the purposes of quality assurance but crucially to mitigate potential error following the tool's misuse. Achieving this requires the practitioner to both engage with relevant tool training and, conduct their own evaluation and testing of any tool that is planned to be used. Failure to fully understand a tool/function can hinder reliable fault attribution from taking place - simply put, it is argued that to determine the occurrence of a fault, one must first understand what correct performance looks like. Understanding a tool's functionality helps to prevent blame for any assumed fault from being misplaced with the tool itself. This may be due to a practitioner misunderstanding what the tool is designed to do within the given circumstances that they are deploying it, leading to the underlying issue being masked and a failure to prevent future occurrences of it. A fundamental part of attributing fault to a specific cause is the ability to assess and determine when the performance of any entity at potential fault has deviated from, or fallen below an acceptable level of performance. With DF, it is impossible to determine when the tool or function has performed erroneously if the remit of its acceptable performance is unknown. As a result, the first principle for tool-fault-attribution is defined.

> *Principle 1: Fault cannot be reliably attributed to a tool or any of it's functions if the remit of its acceptable performance is not fully known and understood.*

Simply put, a practitioner may struggle to justify blaming a tool for the occurrence of any fault if they do not know what the tool should or should not have been doing in the first instance. However, it is also recognised that the task of understanding a DF tool is not always an easy one as many are complex, closed source, multifaceted constructs wherein the case of 'tool-suites', the number of available functions can run into the hundreds. In these instances, it may not be feasible to decipher all of a tool's capability, but as a minimum, both those functions intending to be invoked (primary functions - i.e. search/recovery processes) as well as those that may have a direct impact upon any results (secondary functions - i.e. results display/filtering), must be understood. This task should not be placed solely on the shoulders of the practitioner and vendor support is encouraged.

The vendor of any tool must help the practitioner recognise and understand what their product does and does not do. Where a tool's functionality is vaguely described by its creator/vendor, the chance of a practitioner failing to fully understand the tool's operational remit and functionality is increased. In such cases, tool/function 'documentation-vagueness' may place the practitioner at an impasse, raising questions as to whether they should use a tool which

has not been properly described, or whether the burden of determining the remit of its functionality lies with them and their need and ability to thoroughly test it prior to its use. In an ideal situation, a tool's accompanying documentation should support the practitioner, but they must recognise that in some cases it is unlikely provide the level of detail required for evaluating all possible relevant scenarios. For example, documentation may not be revised following a tool incurring minor updates, or where a tool's target data may have updated (i.e. a new operating system version is released or the software version from which an artefact has originated from has changed). In contrast, if a tools documentation is comprehensive, a practitioner should also exercise some caution as to prevent overreliance on it and blindly follow instruction without first evaluation its procedures themselves. This means in reality a combination of both good documentation and an independent functionality assessment of the tool will by the practitioner will be needed prior to its use.

2.1.2 Invoking capability

A practitioner must be able to invoke any function of a tool they intend to use in the way that any tool's creator/vendor designed it to be invoked. In this sense, the 'correct' way to engage a tool's function is the way that its creator/vendor designed it to be used. This requires a thorough exploration and acknowledgement of any tool's configuration options as the ability to engage any function may not always be straightforward or obvious, where fault derived from a misconfigured tool must not be mistaken for a tool error. With this in mind, there is a caveat to consider, and that involves a tool error occurring when the practitioner is operating their tool in line with explicit tool vendor training or guidance which is subsequently found to be incorrect - technically an error of the tool vendor. Many tools now offer extensive levels of configurability, where the field has moved away from a one size fits all process for tackling all available data, towards a more strategic and targeted approach. This is of benefit to the practitioner; it allows them to deploy a digital evidence strategy that is proportionate and necessary for any case in question. However, it requires greater knowledge of the tool's configurability in order to ensure that the remit of its operation is both recognised and deemed appropriate for the investigative scenario that it is intended for deployed. A practitioner may know how they need a tool to function, but they also must be capable of making it function in their desired way. This requires help from the vendor where it is argued that they maintain some responsibility to provide resources that guide those using their tools in a way that allows them to invoke their tool's functionality effectively.

Fault via tool-misconfiguration is a concern as it is unlikely to be easily detectable, particularly if any evaluation of a fault is being conducted by the practitioner who operated the tool in the first instance. In addition, misconfigured tools may not always raise 'error-warnings' which alert the practitioner, as any fault may not technically occur during the tools run time. Rather, the result of the operation could be considered 'faulty' (returned data may not be as the practitioner intended) due to the practitioner's erroneous setup of the tool (for example, a search process may not return all available data due to user configured restrictions or filters which could have been applied by mistake or misunderstanding). Provided a tool performs in line with its known and described relevant settings, the onus for making the tool to perform in any expected way lies with the practitioner and their ability to correctly configure it, raising the second principle for tool-fault-attribution.

Principle 2: Tool-misconfiguration by the user is not the fault of the tool if there are resources (documentation/training) available that describe how to correctly operate it.

Finally, we must be careful so as to not absolve the practitioner of fault-liability where no resources for a tools correct operation exist. As previously noted, an under-documented tool must be approached with caution and practitioners cannot excuse themselves of fault occurring as a result of them operating a tool incorrectly due to not being able to determine a tool's correct operating procedures. It is unlikely that any practitioner would consider this stance.

2.1.3 Tool Capability

Any tool's performance cannot be evaluated until its stated capability is first identified and understood. Whilst this may seem obvious, it is necessary to acknowledge that a tool cannot be benchmarked against what a practitioner thinks it does or should do - tools cannot be held accountable for the absence of a function if it doesn't explicitly state that it offers such capability. A tool cannot be assumed to have a function, nor is it arguably viable for tool vendors to list every non-functionality that their tool may have, and indeed, what a tool 'can't do' may be obvious at times. In some instances, a vendor may helpfully state specific limitations which are known and fall within an area likely to be of value to the practitioner's knowing (and this conduct should be encouraged), but these cases are likely to be restricted (for example, if a tool is known to be unable to examine data type 'A' but can process similar data type 'B'). In all cases, a practitioner should start by only assuming a tool's capability if it is explicitly stated, requiring an assessment of the tool vendor's documentation and contracted statements.

Bhat et al's., [2] study of anti-forensic measure detection provides a recent example of the challenges in this area. Here, it is suggested that an expected response from The Sleuth Kit (TSK) in regards to the deployment of secure deletion measures is that it should inform the practitioner about the presence of possible secure deletion having occurred. Yet TSK offers no such functionality. Perhaps it is in this case unfair to expect the tool to do something it does not itself claim to do. Alternatively, and as noted above, perhaps it could be argued that the tool should have stated this limitation, given it may be useful to the practitioner to prevent it from being used in this capacity, however, such a stance makes it difficult to draw the line as to how far a vendor must go with regards to stating their tool's limitations. If we consider hypothetical fault attribution in a case where potential secure deletion traces were not flagged by TSK, but were present in the available data, it is suggested that 'fault' (being the failure to detect these traces) can only viably lie with the practitioner. TSK cannot be held accountable for failing to do something that it never stated it would - a principle which applies in many aspects of legal operations.

Put simply, if the practitioner requires functionality 'A', yet their tool states that only functionality 'B' is provided, then it must be initially assumed that functionality 'A' is not provided. It may subsequently be discovered that functionality 'A' may be available (for example, a provided data parsing algorithm appears to work on other data outside of the stated documentation), but the practitioner must proceed with caution as unstated functionality may not have been tested by the vendor or not intended to be part of the originally contracted for tool. A

practitioner must know their tools and what they are capable of, leading to the third principle of tool-fault-attribution.

> *Principle 3: A tool/function cannot be at fault for failing to do something, or incorrectly doing something that is outside of its expressly stated capability.*

2.1.4 Tool Suitability

Provided a tool performs accurately and in line with its intended configuration, the suitability of the tool for any investigative task must be determined by the practitioner. This requires the practitioner to identify whether a tool/function can successfully complete the task that they intend to use it for. A tool deployed in an unsuitable environment which ultimately leads to an investigative error/issue cannot be held at fault. Arguably, fault here is as a result of poor investigative decision making and strategy development on the part of the practitioner. Determining suitability can be challenging for all of the issues noted in Sections 2.1.1 - 2.1.3, however, the practitioner and their organisation will have the final decision as to when and where to deploy a specific tool. As a result, the fourth principle for tool-fault-attribution is offered.

> *Principle 4: A tool/function is not at fault for any error/issue/ommission which occurs as a result of it being deployed in an investigative scenario for which it is unsuitable for use. The suitability of a tool or tool function is for the practitioner to determine on a case-by-case basis.*

Consider the scenario where a tool is chosen to examine data from a version of a software application that is not explicitly supported by the tool (no declarations of support are offered by the tool creator/vendor for the given investigative circumstances). A tool may be assumed by the practitioner to offer investigative support because it has the capability of examining previous versions of the software application, however the latest iteration of the software may contain structural changes in its underlying data, which may lead to the tool not identifying and recovering relevant records. If the tool was not explicitly designed for use when investigating this version of the software application, then it is not suitable for use in this investigative scenario. Here, it is argued that a tool that does not state that it has support for the task it has been used for is not at fault.

In some cases determining a tool/function's suitability may be straight forward, where in others, more complex issues may need debating. If a dispute regarding tool-fault-attribution arises with specific reference to suitability, an independent party may be required to evaluate the circumstances of the case.

3 So when is a tool at fault?

Taking into account the aforementioned four principles for tool-fault-attribution, it is necessary to consider when a tool can be considered to be responsible for any fault, issue, omission or investigative error that arises. It is suggested that in order to determine that fault should be attributed to a tool/function, the following guidance should be applied:-

1. The tool explicitly states or contracts with its user that it provides function 'A', and;

2. The remit of ‘A’ is defined and declared by the vendor including an acknowledgement of any limitations via the information provided by the tool’s vendor/documentation, and;
3. The performance of ‘A’ when properly tested (or used) within its defined functionality-remit is shown to be inaccurate.

When simplified, fault can be attributed to a tool when it fails to perform in a way which it the tool vendor states that it should and proceeds to contract with the practitioner and the organisation on this basis. On face value, it may be assumed that this is easy to determine, however, the practitioner must consider whether they can objectively evidence the discrepancy they believe they have seen between the tool’s actual performance and the tool-vendor’s stated performance. Any ambiguity surrounding a tool’s expected performance as described within vendor documentation may in reality produce grey areas for fault attribution.

3.1 Grey areas

Practitioners will likely note that not all of the tools that they may seek to use maintain robust documentation which describes their functionality in a level of detail that would allow them to definitively determine when it is not performing as it should. Some tools may generically define their functionality whilst failing to describe it in full (consider a tool that states that it can process database ‘*d*’ but omits to parse and report all available fields, only providing those which the vendor believes to be of likely interest to the practitioner. Or where App ‘*a*’ is supported, but it is not clear which versions of ‘*a*’ or how many of the App’s artefacts are included in the examination package). This may cause an inability to fault-attribute, as whilst the general ‘*capability*’ of a tool may be establishable, the full remit of it could lack clear definition. In this case, there is no way of identifying where a tool’s functionality was intended to stop, and therefore what remains outside of it. Attributing fault requires any tool to be explicit in defining what it does - a task for the vendor. A vendor who fails to do this creates a grey area of uncertainty, where the practitioner remains unsure as to whether the tool is going to conduct the function in the way that they would like, limiting their ability to determine when the tool has not performed as expected. In turn, vagueness in the definition of tool capability provides the vendor with a greater remit for absolving themselves of liability for an error - albeit it is unlikely that any vendor would seek to adopt this position, rather many would be grateful of the acknowledgement of a tool fault and seek to correct it as soon as practicable.

Vendors should also consider the language they use to name and describe their tool’s functions to avoid confusion and the potential for functionality to be ‘assumed’ by the practitioner. Whilst such actions could lead to error on the part of the practitioner, clearly described tool functions could also help to prevent such issues from occurring. There is no standard naming convention for tools in the field of DF, where different vendors may name their tool’s functions differently from one another, despite fundamentally being the same technical process. Perhaps here lies a recommendation, that where possible, tool vendors in the DF field should consider harmonising the terminology that they use to describe their tools’ functions in order to help practitioners. Such a requirement would require vendor collaboration and agreement, but achieving this would arguably improve the clarity of every tools functionality. Doing so would not be possible for vendor-bespoke process, however, it may be possible that processes that are fundemtnally the same across vendors could be described in consistent ways.

Vendors must be aware that practitioners must understand what each vendor's naming conventions mean in regards to their tool and try to support their understanding. Ultimately, the practitioner must refrain from inferring any functionality due to the naming conventions used by a tool at face value, or from assumed experiences with other tools without first checking.

3.1.1 The testing challenge

A practitioner cannot assume that their chosen tool functions correctly. In some circumstances and particularly in the case of 'off the shelf' purchased tools, performance may likely occur as expected, but there is no guarantee. In fact, many vendors have stated in their licencing agreements that they cannot ensure that no errors in their product exist [4]. Whilst this is not ideal, it is a position which reflects the complexity of tool development in DF and that it may be unreasonable to never expect to encounter tools which fail to work completely as expected. Tool evaluation for error prevention is a task that both the vendor and the practitioner must share, where good practice dictates that a tool's performance is evaluated by the practitioner prior to its real-world deployment. Ensuring tool evaluation is correctly conducted is key to supporting reliable tool-fault-attribution. Here, procedures such as dual-tool verification, whilst not a guaranteed solution, can help to support the tool test and fault identification processes [6]. In such cases, a tools expected or actual performance can be benchmarked against another for the purposes of evaluation.

4 Final thoughts

Fundamentally, it is important to determine the difference between a tool error and an error occurring as a result of the practitioner's chosen investigative behaviour so that an appropriate course of action can be taken. In cases of an established tool error, formal obligations will be placed upon the vendor to try and fix any discovered issue, where in most cases this would likely be welcomed and addressed as soon as possible. In regards to practitioner error, blame naturally lies with the practitioner and their ability to competently conduct a DF examination and use the tools that they have access to effectively, in the appropriate investigative scenarios. Additional training may be required and greater awareness needed to ensure appropriate future investigative conduct is used in future cases. Further, the imposition of relevant ISO standards on organisations operating in DF and the subsequent development of relevant and robust processes and procedures for evidence adherence to these standards, it is likely that methodologies for fault prevention and fault finding are improved as a result. Whilst it may appear harsh, even where fault occurs as a result of a tool's error, the practitioner is not totally absolved of liability as now there is an expectation that tools are tested prior to their use, placing a high burden responsibility upon their shoulders as well as a substantial workload. It is important that those in DF consider the challenges of appropriate tool usage where practitioners must understand both what their tool does and how to use it properly, so as to avoid investigative issues occurring as a result of poor tool deployment. Addressing these points should never be an afterthought.

References

1. Lexico, 2021. 'a bad workman always blames his tools' Available at: https://www.lexico.com/definition/a_bad_workman_always_blames_his_tools (Accessed: 30 April 2021)

2. Forensic Science Regulator, 2020. ‘Forensic Science Regulator Guidance Method Validation in Digital Forensics’ Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/921392/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf (Accessed: 30 April 2021)
3. Bhat, W.A., AlZahrani, A. and Wani, M.A., 2021. Can computer forensic tools be trusted in digital investigations?. Science & Justice, 61(2), pp.198-203.
4. 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. Science & Justice, 58(6), pp.433-440.
5. Forensic Science Regulator, 2020. ‘Forensic Science Regulator Guidance Method Validation in Digital Forensics’ Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/921392/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf (Accessed: 30 April 2021)
6. Horsman, G., 2019. Tool testing and reliability issues in the field of digital forensics. Digital Investigation, 28, pp.163-175.



https://dspace.org/

That tool is rubbish!...or is it?

Horsman, Graeme

2022-08-05
Elsevier
https://doi.org/10.1016/j.scijus.2022.07.006
Horsman G. (2022) That tool is rubbish!...or is it?, Science & Justice, Volume 62, Issue 5, September 2022, pp. 515-519

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