Received: 29 July 2020 | Revised: 11 January 2021 | Accepted: 8 February 2021

DOI: 10.1002/wfs2.1417

ADVANCED REVIEW

WIREs FORENSIC SCIENCE WILEY

# Standardizing digital forensic examination procedures: A look at Windows 10 in cases involving images depicting child sexual abuse

**Graeme Horsman**

School of Health & Life Sciences, Teesside University, Middlesbrough, UK

**Correspondence**
Graeme Horsman, School of Health & Life Sciences, Teesside University, Middlesbrough, Tees Valley TS1 3BX, UK.
Email: graeme.horsman@googlemail.com

**Edited by:** Kim-Kwang Raymond Choo, Editor

**Abstract**

As a topic area, the need for the standardization of operational practices in digital forensics has seen much discussion. There are clear benefits for digital forensics if its procedures can be harmonized including increasing the reliability of the work produced by its practitioners, consistency of practice, and the potential for greater quality control, however, attaining standardization is a difficult task, and further work in this field is required. This work discusses the "standardization challenge" assessing both the need for standardization and the feasibility of achieving it. It is suggested that those actively contributing in this area should consider the development of models for defining operational practice which are *offence-specific*, *device-specific* and *operating system-specific*. To support this proposal, an example standard is offered and discussed which suggests and documents the minimum expected requirements for the examination of Windows 10 devices in cases involving images depicting child sexual abuse.

This article is categorized under:

Digital and Multimedia Science > Cybercrime Investigation

**KEYWORDS**

crime, digital forensics, investigation, quality, standards

## 1 | INTRODUCTION

The field of digital forensics (DF) is both one of the fastest-developing, and fastest-growing subbranches of forensic science (Home Office et al., 2018). The adoption of technology in almost all aspects of society has arguably led to an increasing requirement for digital-device analysis to be performed as part of criminal investigations worldwide, subsequently creating backlogs (Home Office et al., 2018; Mayor of London, 2019; Montasari & Hill, 2019; Quick & Choo, 2014; Scanlon, 2016; Thompson, 2019) where in some worst-case scenarios, device examination wait-times can be longer than 12 months (Mayor of London, 2019). The reliance now placed on digital evidence by criminal justice systems in many cases has led to concerns being raised with regards to both its quality and reliability (Grobler, 2012; Page et al., 2018; Sunde & Dror, 2019) and a lack of oversight and regulation of the DF field itself with regards to the definition and maintenance of standards (Tully, 2020). It is unlikely that the demand placed upon DF organizations and law

enforcement for the forensic examination of digital devices will lessen within the foreseeable future, where arguably, increased reliance on these services is likely to be observed. As a result, many DF practitioners and their organizations will continue to battle the "short turnaround times" which may be imposed by legal systems who themselves are attempting to deliver timely justice (Home Office et al., 2018). Given this challenge, it is important that the deployment of DF practices be controlled via the development and adherence to accepted standards (Grobler, 2012).

Casey (2019) notes "the consequences of errors and omissions in digital forensics include imprisoning innocent people, leaving dangerous criminals free to perpetrate additional crimes, and continuing victimization of the organizations and people targeted by offences." As a field with limited resources, it is important that those in DF whilst attempting to keep pace with the demands placed upon it, do not lose sight of the need to create, develop and enforce mechanisms for ensuring high-quality work is produced by its practitioners. In short, the field must not compromise quality in pursuit of the increased throughput of cases and resist adopting a "conveyor-belt" approach to case processing, instead prioritizing the transparency, validity and reliability of investigatory methods, ensuring that it operates as a dependable, consistent and responsible branch of forensic science. Calls made to harmonize the principles of DF with those of forensic science have been made, with perceived benefits including the strengthening of DF's "scientific foundations" (Casey, 2019; Jaquet-Chiffelle et al., 2018). In addition, the Forensic Science Regulator in England and Wales has stressed the need for the implementation of quality standards which offer a "systematic approach to scientific validity, competence and quality" across the forensic sciences (Tully, 2020). As legal systems increasingly look towards the DF field to support the reconstruction of criminal events through the investigation and interpretation of digital data, conduct and best practice within DF should be regulated to ensure that the work it undertakes is fit for purpose.

Arguably, across the DF field, there is an imminent need to increase consistency of practice via the adoption and use of accepted protocols, bringing with it the potential benefits of quality control (Horsman, 2020a, 2020b), but this is not the first time this opinion has been raised. In 2012, Grobler suggested that "standardisation within digital forensics has been a continuous struggle in terms of worldwide acceptance and creating common methodologies," where this remains true in 2020. Whilst some improvements have been made, the field is arguably still far from being satisfactorily governed. As techniques develop and capability expands, the reliability of these practices must be verified to prevent rogue practice from corroding confidence in this field (Grobler, 2012). The "standardization issue" in DF continues to be raised, not only by academics (Grobler, 2012; Karie et al., 2019; Mothi et al., 2020; Valjarevic & Venter, 2012a, 2012b) but also formally by those overarching bodies such as those with powers of oversight and governance, and with the push for the adoption of ISO accreditation in varying areas of practice (see, e.g., ISO17025 and 17020; Tully, 2020). In an ideal scenario, everyone who calls upon the services of DF should be entitled to the same level of service and the same level of quality in any product received, but in reality, there is a risk that this may not currently be the case (Horsman, 2020a, 2020b).

This work offers a discussion of the challenge of standardization in DF, critically evaluating both the need and feasibility of achieving it. A proposal is made for considering efforts which focus on the development of standard examination approaches which are *offence-specific*, *device-specific* and *operating system-specific*, in essence, taking into account the *offence* type under investigation and the platform subject to analysis. To demonstrate this idea, a standard operating procedure is offered for the DF examination of Windows 10 devices in cases involving imagery depicting child sexual abuse (IDCSA). This standard defines the minimum set of requirements and expectations placed upon a practitioner in an effort to define a quality-benchmark for investigatory practice, and in doing so, having the potential to harmonize practice.

## 2 | THE STANDARDIZATION CHALLENGE FOR DIGITAL FORENSICS

What may at first glance appear a simple concept, standardization is in-fact multifaceted with reference made to the definition offered by the U.K. government's Department for Business, Energy, and Industrial Strategy (2012).

> "Standardisation is the process of creating, issuing and implementing standards. A standard is a document, established by consensus and approved by a recognised body. It provides rules, guidelines or characteristics for activities or their results so that they can be repeated. They aim to achieve the greatest degree of order in a given context." (Department for Business, Energy, & Industrial Strategy, 2012)

In regards to DF, the field should strive for standardization in its entirety, as with it comes the harmonization of practice and both consistent and reliable outputs if any such agreed standards are correctly developed and adhered to. Yet the complexity of such a task means that in reality, it is very unlikely that this will ever be achieved, where even

standardization within a single laboratory environment comes with challenges (although it is common for standard operating procedures to be developed for specific practices (Bulbul et al., 2013). In certain geographical regions, the push for mandatory adherence to specific International Organization for Standardization (ISO) accreditation can be seen, where in England and Wales attempts are in place to establish "blanket-adherence" to ISO17025 by all DF organizations, in theory bringing with it an agreed level of consistent practice. Yet, this has been met with well-documented practitioner scrutiny, and questions as to whether it is the correct option for DF in its pursuit of standardization (ForensicFocus, 2017, 2018; Sommer, 2018), where the Forensic Science Regulator has noted concerns around a lack of compliance from DF organizations (Tully, 2020). Many external barriers have been raised in regards to evidencing adherence to such standards including cost and resourcing issues, and it is suggested that there remain those who "devote much time and energy to avoiding compliance, arguing against change and sticking to 'how we've always done it'" (Tully, 2020). It would appear that such statements are no longer considered justification for adopting methods which do not fall in line with any standard-based expectations (Tully, 2020). In addition, the "ISO 27K series" of standards exist (including 27037, 27042; ISO, 2020b), which attempt to define standards specific to DF.

This article wishes not to enter into the debate between "right" and "wrong" in relation to the specifics of ISO17025 and the position in England and Wales, but to stay within the generics of the standardization debate. As DF grows, becoming more complex both operationally, and through the development and use of a greater array of investigative techniques, standards increase in importance (Cargill, 2011), becoming a way for assuring quality (Hatto, 2013). Standards help to define a minimum and expected level of service delivery (Grobler, 2010) and codify best-practice. It is important to note that attaining standardization in any environment is a difficult and often resource-intensive process, yet the benefits it brings in regards to the cohesion of practice and assurance of quality means that it should be pushed for. However, when distilled, there are two suggested areas of challenge; developing a standard and then seeking the adoption of it.

Standard development itself maintains multiple stages to address with organizations such as ISO (2020) and BSI (2020a) offering independent and formal support. Tasks include identifying the problem area to be addressed by a standard and the standard's scope. Here, feasibility is a factor for consideration as in fields which contain multiple variables in need of control, the scope of any standardization attempt must arguably shrink if it is to achieve its goal. As a result, domains such as DF are arguably more likely to achieve true standardization within specific jurisdictions, for specific areas of the investigatory process, most likely for specific device types as opposed to field-wide harmonization on a grand scale. For example, Horsman et al. (2019) provide a standard operating procedure specific to router examinations at scene, in an effort to standardize approaches to the examination of these device-types, specific to scene-based scenarios. This may in part be due to the intricacies of policing and legal system requirements, forensic budgets and recognized training and procedural pathways within various different countries. Furthermore, the standard itself must identify the best practice which is to be followed and codify it in a way which allows it to be adhered to, or identify ways in which adherence can be evidenced (BSI, 2020b). This process of development requires not only a representative body of individuals who maintain appropriate domain-specific knowledge to be able to develop such standards, but also periods of consultation to allow field-wide input and a consensus of "fitness-for-purpose" (Hatto, 2013). The sheer volume of organization and effort required to bring all these elements together in a coherent and orderly manner is vast, and even if successful, buy-in from the targeted community must be sought and is not guaranteed.

Standards are also seen as "pervasive mechanisms of international governance" (Abbott & Snidal, 2001) and therefore for a standard to be of value, it must be adopted by those it is aimed at, within the spirit for which it was designed. Adoption of a standard by the community is an issue regardless as to whether it is enforced through legislation or suggested as voluntary, as in either case, individual discrepancies will always present themselves. Whilst standard development in most cases should consider periods of community consultation as part of its development, it does not always guarantee committed engagement. This is noted by Tully (2020) who suggests that practitioners or organizations "may grudgingly implement standards, but in a way that cripples their productivity and locks staff into rigid protocols, no matter what the case requires. Or they may devote much time and energy to avoiding compliance, arguing against change." In essence, standard-adoption represents a significant hurdle in the pursuit of standardization as in any given instance it is unlikely that a proposed standard will be met with wholesale agreement, and in some cases, it may cause short-term determinant to some that are then tasked with seeking adherence to it (e.g., change in practice or setup may be needed, requiring time and resource investment). That being said, it is important to note the difficulty attributed to meeting a standard should not in itself be used as an excuse for not meeting it as such a sentiment undermines the whole purpose of such mechanisms and their purpose of quality control.

It may be argued that in seeking to impose a standard, its acceptance to begin with does not have to be witnessed in the totality as markets demanding such services begin to indirectly police those operating within the field, directing

business towards those who have sought to adopt these measures. In essence, adherence to standardization becomes a business-critical decision and those who do not have it ultimately lose work. Regardless as to whether this approach is right or wrong, it is inevitable that in the absence of a legal requirement enforcing adherence, this pattern of activity will emerge. With this in mind, it is necessary to establish where the field of DF is in regards to standardization.

## 2.1 | Digital forensics and standardization

When considering the standardization issues in DF, it is perhaps best to draw reference to the typical investigative process (Agarwal et al., 2011). Figure 1 describes this process as six stages, digital evidence "collection," "handling," "acquisition," "analysis," "interpretation," and "reporting and presentation." In regards to standardization of the first three steps in this process, it is arguably the case that progress has been made with regards to the standardization of practices, albeit there is no overarching formal enforcement. Conceptually, there is an acknowledgement for the need for data preservation which begins at the collection phase of any investigation, requiring the appropriate handling of devices followed by data capture. Whilst there is no formal enforcement of a standardized approach, there is arguably acceptance of the need for such principles and a number of guidelines are available confirming this and outlining the accepted methods for achieving this (Association of Chief Police Officers', 2012; Interpol, 2019).

If we consider that at the collection and handling stages, digital device types can often be gathered into native groups (albeit some devices will be subject to bespoke standard operating practices), there are likely fewer variables which any process must tackle when considering standardization of these actions. Furthermore, acquisition methods pursue a common goal—to extract data from the device whilst maintaining its integrity. Traditionally, in computer-based evidence, hard disk imaging and the expert witness format (.E01) is what is preferred and whilst multiple tools are capable of carrying out this process, the. E01 format is well-defined. Yet now there is the added complexity of mobile device extraction terminology and the range of investigative extraction processes. These acquisition methods arguably require some harmonization in regards to their capability and description, but it is suggested that this is achievable with further collaboration between organizations and tool-vendors. As a result, even though the field is not there yet, it is greatest degree of standardization is suggested to occur in these three process-areas, and it is these stages where standardization on a grand scale is both feasible and closest being achieved.

In comparison, the stages of analysis and interpretation provide standardization challenges, where further work is required (Casey, 2020; Horsman, 2018; Sunde & Dror, 2019). Here, focus is on the practitioner and the methods which they use to access, parse, display and interpret digital data on a device, a set of acts which in most cases will be almost entirely self-determined by the investigating practitioner. This is often due in part to the number of different situations which can be present in any given examination as a result of the almost unlimited amount of actions which can be carried out on a digital device. Both these concepts are also multifaceted. The analysis of a device concerns the processing of an exhibit's data, taking into account not only tools used, but the practitioner's decision-making as to how those tools

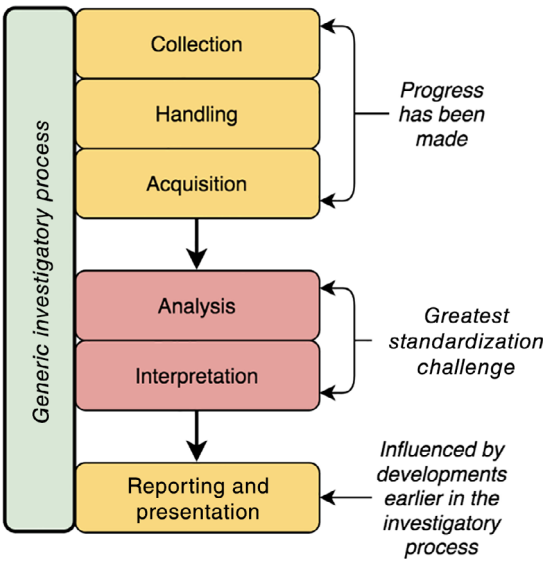


**FIGURE 1** Standardization mapped against the digital forensics investigative process

should be used. This involves the practitioner attempting to extract data from a device which is likely to be of value to an investigation. There are also the added elements of validation and verification in regards to any tools used and methods deployed. The field is yet to see field-wide standardized approaches for the analysis of device data and therefore continue to risk inconsistencies in practice and potential errors. Of equal concern and following device analysis, a DF practitioner must then seek to interpret the importance of any relevant data. Data interpretation in DF has received much recent debate (Casey, 2002, 2020; Horsman, 2018, 2019, 2020a, 2020b) and questions have been previously raised as to whether standardization is even possible at this phase of an investigation (Scholtz, 2010).

## 3 | MORE FOCUSED STANDARDIZATION ATTEMPTS

It would be incorrect to suggest that DF entirely lacks standardization as conceptually it exists in as many models, and standard operating procedures have been developed for various elements of the analysis process (Horsman et al., 2019; Mothi et al., 2020). However, much academic contribution, in terms of standardization concentrates on proposing generic standardized high-level investigative process models (see, e.g., Valjarevic & Venter, 2012a, 2012b; Sibiya et al., 2012; Lalla & Flowerday, 2010; Kebande & Ray, 2016). Such approaches do bring value to the community as they provide a foundation for concepts within an investigation to be expressed, that is, they outline the concepts that a practitioner should consider, where recommendations for standardizing DF workflows and the stages involved in this process are described. Yet they do not always offer stepwise detailed guidance required for an operational level. The problem that remains is sometimes these steps may provide a practitioner with "room for maneuver" and therefore potentially allow for the impression that standardization is in place when operationally, this may not be the case, and operational standardization is important for quality assurance (Amann & James, 2015). For example, such models may propose steps which include data collection or analysis, but possibly lack the fine-grained detail to truly standardize processes at a microlevel. As a result, multiple organizations may demonstrate data collection or analysis giving a high-level appearance of standardization, but below the surface, achieve this in different ways defeating the purpose of the standardization attempt. Of the few efforts which achieve this, Montasari's (2017) framework for data acquisition is possibly one of the closest to achieving this level of detail.

It is suggested that whilst all efforts to support standardization are valued, focus could be turned towards attempts to standardize parts of the investigative process in more detail. Whilst there are many proposed frameworks which outline a standardized investigatory process, the field requires further work which concentrates on standardizing those actions which occur within each stage.

### 3.1 | The proposed model: *Offence-specific*, *device-specific*, and *operating system-specific*

It is argued that in the pursuit of standardization, DF should increase focus on the development of procedures which are *offence-specific*, *device-specific*, and *operating system-specific* in their design. Justification for this approach is argued as follows:

#### 3.1.1 | Why an "*offence*-specific" approach?

Different digital *offence* types inherently maintain different evidential digital traits (Horsman et al., 2014; Silde & Angelopoulou, 2014). Therefore, standardization between different *offence* types where evidential traits may be different, could be a difficult task. Instead, where *offence*s of the same type may share similar evidential traits (e.g., illegal imagery cases will focus on media files), consistent approaches may be justifiable for replication across multiple cases of the same *offence*, and in turn, be achievable. Such thoughts may be considered in line with the concept of "digital profiling," where consistent behaviors found in specific crime types may allow standard investigative approaches to be adopted (Silde & Angelopoulou, 2014).

#### 3.1.2 | Why a device-specific and operating system-specific approach?

Similar to the reasoning noted above, operating systems and device types of the same type may perform consistently leading to the same data-types and structures being present across multiple cases where the same device and operating

system is in operation. Therefore, consistency is argued as more achievable when the underlying variables of device-type and operating system-type are in place. In contrast, whilst at a high-level, different operating systems may allow a user to achieve the same type of activity (such as opening a file and then maintaining records of this activity), they way they do this, and how this is recorded in the underlying structure of the operating system may be different between each one. Therefore, approaches specific to operating systems and devices are argued as being more likely to be consistently and effectively deployable.

Developed standards which consider these three criteria are arguably more fine-grained, allowing for potential effective scrutiny and evaluation of practices whilst being aligned to any operational requirements. Although it could be argued that such an approach may lead to standard "bloat" given the number of different combinations which could exist with regards to the three above noted variables, this should be considered against the perceived benefit. Examination standards defined for the specifics of an *offence* and the device it is alleged to have been carried out on arguably reduce the chance of evidence misinterpretation or omission as they are constructed with the characteristics of the *offence* and device in mind, along with legal and procedural requirements. Furthermore, they increase resource efficiency by preventing unnecessary processing tasks from being implemented, either by mistake or through a misunderstanding of the requirements of the investigation. However, developing standards with this level of detail is a difficult and time-consuming task.

To provide an example, this work offers a documented standardized process outlining a suggested proposal for the minimum investigatory requirements for investigation of IDCSA (other terms exist depending on the applicable jurisdiction) on devices running the Windows 10 operating system. It must be stressed that the proposed model defines a standard for the minimum requirements for investigations. Therefore, those interpreting this model should not view it as a definitive step-by-step guide, but that in all cases, the processes outlined in the model are considered core to the implementation of an effective examination. Whilst all investigations of this *offence* type will maintain some digital characteristics unique to the suspect under investigation (Horsman et al., 2014), degrees of commonality are also likely to be present, including modes of access to media and potentially the media itself. Furthermore, in all cases within a specific jurisdiction, applicable law will dictate those actions which in all cases must be present in order for an *offence* to be committed.

What the minimum standard model attempts to do is improve subpar examination conduct by defining a minimum level of acceptable investigatory practice—*these are the procedures that as a minimum should be undertaken*, where a failure to do so would be considered bad-practice. It is acknowledged that in some cases, adherence to these minimum standards may not be enough to effectively examine a given case and in such instances, requirements are then placed upon the practitioner to extend the remit of their investigation. The implementation of a minimum standard may seem controversial, but doing so considers the realistic implications of operational challenges where practitioners are now often unable to investigate all content on a device (Pollitt, 2013), where resourcing and time issues impact the level of detail afforded to an investigation. Whilst this may not sit well with everyone, DF now finds itself in an unfortunate position of in many cases having "too much data to review" and therefore strategic examination practices are required if it is to keep pace with the demands placed upon it. Whilst in some instances practitioners may have the ability or time to pursue further lines of enquiry or data revealed through those processes undertaken as part of the minimum standard may require it, it is argued that the proposed baseline of tasks provides a tradeoff between operational demands and the effective examination of a device. It is important to consider that there is little value in proposing methods which are too difficult or resource-intensive to operationally implement.

The proposed minimum standard is split into three stages, "processing digital data," "recovery/screening," and "analysis," adopting terminology and areas noted within the ISO17025 standard (Tulley, 2017). Together, the three stages define how a Windows 10 device should be processed including evidence types to be collected and parsed, the implementation of file recovery methods, keyword screening approaches and finally, the questions a practitioner must seek to address as part of their analysis and interpretation of data (see Figure 2).

## 3.2 | Processing digital data

This work adopts the definition of "processing digital data" from the Forensic Science Regulator's Codes of Practice and Conduct documentation which describes this act as—"the process of converting (e.g., extraction, organizing of data) digital data to produce meaningful information either by a manual or automated process to allow subsequent analysis to take place" (Tulley, 2017). Here, this is interpreted as those processes used by a practitioner to identify and extract

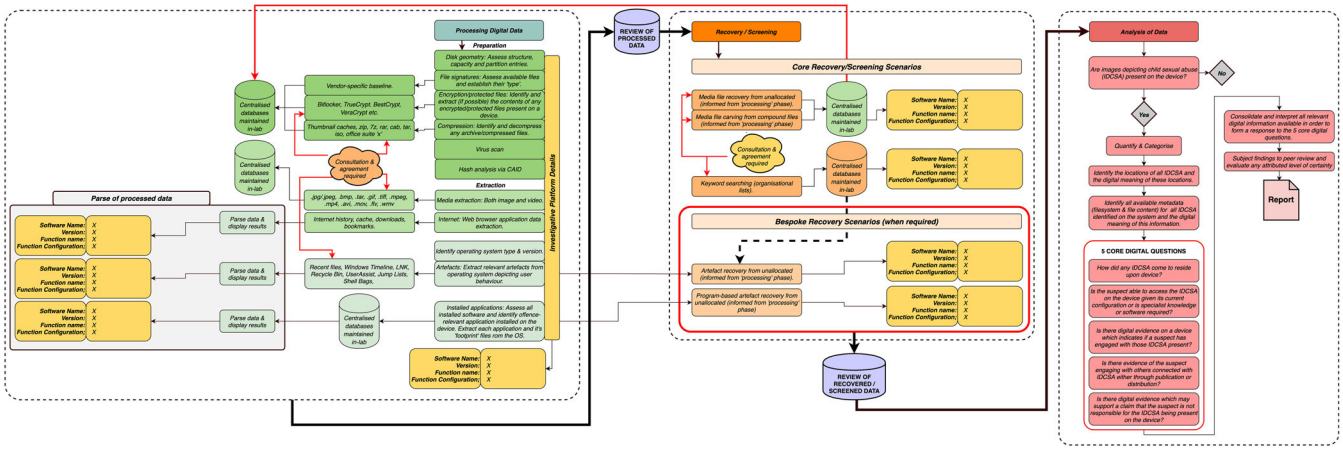


FIGURE 2 The proposed standard for the minimum requirements for examining Windows 10 devices as part of imagery depicting child sexual abuse investigations

digital data from a device, which may include subsequent data-parsing so that information can be viewed and interpreted at a later stage (notably, the "analysis" stage). As a result, processing involves the use of techniques or procedures to extract a subset of digital data from a device, which is either believed to contain information of value to an investigation or to refute an accusation. The processing digital data stage is split into two phases, *preparation* and *extraction*.

### 3.2.1 | Preparation phase

The preparation phase must be completed first and contains six tasks which should be undertaken on a target system which ensure the practitioner is in a position to correctly process data. These tasks are:

1. Carry out disk geometry checks, verifying structure, capacity and accessibility of data (consider device configuration overlay [DCO], host protected area [HPA]). This ensures that the practitioner understands what they do and potentially do not have access to, and any further procedures they may need to carry out to address these situations. In most cases, it is likely that disk geometry checks will raise few concerns.
2. Carry out file signatures analysis, assessing all files present on a device to establish their correct "type" prior to any subsequent processes being implemented for data collection or parsing, preventing missed information. This process should be implemented using an agreed signature database to prevent discrepancies in this process, yet such an approach will inevitably require additional cost and effort to maintain, and agreement across the field. When multiple vendor-specific databases are utilized, each should be vetted for inconsistencies and harmonized if possible (which in some cases may require the manual adding of signature information not already present). This will prevent discrepancies in results being witnessed by practitioners using different tools. File signature analysis should be undertaken prior to any data collection and review.
3. Identify the presence of encrypted content, protected files and encryption capability on a device. Whilst it is recognized that it is not possible to consider all encryption variants, it is proposed that as a minimum, Bitlocker, BestCrypt, 7zip encryption and VeraCrypt are considered. However, it is recognized that additional platforms may be identified, and therefore additions beyond this minimum standard should be contained within a central in-lab database.
4. Identify and decompress compound files, both compressed archives and operating system artifacts. As a minimum standard, the identification and processing of thumbnail caches, zip, 7z, rar, cab, tar, iso and office suite "x" files are suggested. This process may also identify subsequent protected/encrypted files (e.g., archives which are protected/encrypted). As with file signature analysis noted above, if vendor-specific databases are utilized for this process, harmonization is required to ensure consistency.

5. Virus scan the device image (mount and scan) appropriately to establish the presence or absence of any malicious software.
6. All files should be hashed and verified against the latest implementation of the child abuse image database (CAID; Home Office, 2018).

### 3.2.2 | Extraction

The extraction phase contains four tasks concerned with data extraction and in some cases subsequent parsing for later review.

1. Both video and image media should be identified and extracted from the system. Here we are concerned with live files. Consensus should be sought as to a baseline set of file types to be considered, mooted here as .jpg/.jpeg, .bmp, .tar, .gif, .tiff, .mpeg, .mp4, .avi, .mov, .flv, .wmv).
2. All available web browser application data should be identified and extracted from all browsers installed on the system.
3. Operating system and user account details should be confirmed, including version, installed data, shut down/accessed time, user account profiles and login information/password protection. Confirmation of the operating system version ensures relevant artifacts depicting user behavior can be extracted and parsed. It is proposed that as a minimum, Recent files, Windows Timeline (database). LNK, Recycle Bin, UserAssist, Jump Lists and Shell Bags are captured for review.
4. All installed applications must be assessed to identify any *offence*-relevant applications. Each identified application should have it is "digital footprint" extracted from the operating system.

### 3.2.3 | Consultation and agreement required

The proposed minimum standard takes a bold and likely controversial stance in regards to stating those media types, encryption formats and artifacts that should be considered a minimum standard for processing. Inevitably there will be those who disagree. It is argued that collectively they provide a minimum standard which should be considered and it is suggested that laboratories should consult and agree upon what they deem suitable as their minimum processing requirements as part of their operational practices and available resources. However, it must be stressed that any deviation from those suggested here should be in the direction of increasing the comprehensiveness of the process and anything less would arguably fall below what is argued here as a minimum.

### 3.2.4 | Parsing

Some of the artifacts extracted as part of the data processing stage require parsing in order to present their internal content in a form which allows a practitioner to interpret relevance. When data parsing software is used, the software's name, version, function name and function configuration should be recorded. As part of any standardization process, it is important that all available variables are consistently applied, where using the same piece of software for multiple tasks will not suffice. It is important that any software is consistently utilized and consistently configured in order to determine reliable outputs. It is also important that details regarding the investigative platform used to carry out the processing data stage are also recorded. Recording these details enables the consistent future practice and also the identification of any subsequent issues if errors in software are later discovered.

### 3.2.5 | Review of processed data

On completion of the "processing of digital data" stage, practitioners should review all available and parsed content. In some cases, this will provide sufficient information in order to be able to move to the "analysis of data" stage, but where

file recovery and screening is required, a practitioner should use information from the processed data stage to inform their investigatory approaches going forward. This is explained in Section 3.2.

## 3.3 | Recovery and screening

Unlike the definition afforded to the processing digital data stage, the Forensic Science Regulator's Codes of Practice and Conduct does not offer such a targeted one for these tasks. Therefore defined here, the recovery and screening stage of a device involves the use of tools for both file recovery and keyword searching. In some cases, file recovery and screening may not be necessary as either all available evidence may have been manually reviewed or mechanisms such as the Streamlined Forensic Reporting mechanisms are engaged (see discussion by the Crown Prosecution Service with regards to proportionate assessment and the volume of images on a device; Crown Prosecution Service, 2020). In addition, in some jurisdictions, charging decisions may be made which subsequently mean that it is not necessary for time to be invested in file recovery processes. Should recovery and screening of a device be necessary, there are two proposed applications of it.

### 3.3.1 | Core recovery and screening

Core recovery and screening processes concern media file recovery and keyword searching, where it is deemed necessary to engage these processes.

*Core media file recovery and carving from unallocated and compound files*

By default, media file recovery should be considered from unallocated regions of a device and from compound files (as some may not have been parsable during the "processing" stage). Core media file recovery should be informed by the data processing stage and therefore those agreed media file formats that are gathered from the system during "processing," should also be the target of any recovery process. Recovery information should be maintained in a laboratory database, however, it is likely that reliance will be placed upon vendor-generator recovery capability by practitioners. Should this be the case, laboratories should make sure that the recovery processes across each of the different tools in operation are harmonized and validated to ensure consistent performance. This does not just include ensuring that the same file formats are targeted but also that the processes are configured to process digital media in the same way. To that end, software versions and setups should be documented and where possible minimum standard configurations should be identified. All of the aforementioned issues also extend to any process aimed at carving media files from any compound files on a device which have not been parsable.

*Core keyword searching*

When a device is screened using keywords, screening should utilize a defined and agreed set of terms where organizations may maintain their own database of terms or utilize terms provided by child protection organizations. For the purpose of standardization, a minimum term-list should be identified and used to highlight the presence of any relevant information. Practitioners should then consider the use of case-specific terms if necessary as this is considered beyond the minimum standard. In addition, the configuration of the search must be standardized, specifically in cases where the search is used to screen activity records such as Internet history. Standardizing the screening process prevents errors created via tool misconfiguration or misunderstanding which could lead to missed "hits." A global (and comparable for multiple different tools) configuration standard should be defined and made available.

### 3.3.2 | Bespoke recovery scenarios (when required)

Bespoke recovery scenarios revolve around the use of file recovery procedures to recover OS and program-specific artifacts and should be informed by the results of the digital data processing stage. As recovery procedures can take long periods of time, it is important that bespoke recovery is only engaged where necessary and whilst it is included as part of the minimum standard, it is only engaged when required. Similar to core media file recovery, tool configuration must be standardized and defined.

### 3.4 | Analysis of data

The "analysis of data" stage involves the practitioner identifying any relevant processed, recovered and screened data in order to assess whether there is evidence of an *offence* being committed. The first step in the analysis stage is to determine whether IDCSA exist on the device and if so, to quantify and categorize them. If no IDCSA exist and all previous processing, recovery and screening procedures have been followed then the practitioner may take the option of classing the case as negative. For all categorized IDCSA, file location and available metadata should be collected in order to support a practitioner as they attempt to address "5 core digital questions" which are designed to support the practitioner in the structuring of their analysis of any findings.

#### 3.4.1 | Five core digital questions

It is proposed that the are five questions which the practitioner must address as part of their analysis of data in order to ensure that they provide a comprehensive analysis of the suspected *offence*:

1. *How did any IDCSA come to reside upon device?*: Practitioners should examine all processed and recovered data in an effort to establish the origin of any IDCSA and how they came to reside upon the suspect system. This may include establishing whether the IDCSA are made by the suspect or whether they have been introduced to the system via the Internet (downloaded or cached) or other methods (sent via email, etc.).
2. *Is the suspect able to access the IDCSA on the device given its current configuration or is specialist knowledge or software required?*: Questions of accessibility can be an important factor for establishing culpability (Crown Prosecution Service, 2020). Therefore, the practitioner should determine whether any IDCSA are in a system location which the suspect can access, or whether in order to access them they would receive specific tools or specialist knowledge (consider cached IDCSA which may specialist understanding of the cache and require specific software to parse data to retrieve any imagery). It also may prove relevant should an applicable defense be raised by a suspect.
3. *Is there digital evidence on a device which indicates if a suspect has engaged with any IDCSA present?*: Practitioners should consider digital evidence which indicates whether any IDCSA have been opened (executed), moved or interacted with on the system by a device user. This will involve examining a combination of the suggested Windows OS artifacts and any application-specific information if any relevant software is found to be installed upon the system. Establishing engagement is an important factor as it can support any counterclaims against a suspect who indicates that they were not aware of any IDCSA on their machine. In addition, a practitioner should consider who has access to a system, as where multiple device users are reported, attempts should be made to identify information which may link to a suspect. Consider password-protected user profiles, the time and date information surrounding IDCSA and access to other services which may link to a specific individual (e.g., logins to email accounts around the time IDCSA are created/accessed).
4. *Is there evidence of the suspect engaging with others connected with IDCSA either through publication or distribution?*: Practitioners must also establish whether a suspect is a possessor of IDCSA or whether they have escalated their involvement by distributing or publishing material. Furthermore, a suspect may have engaged with others in their sourcing of any material as opposed to passively downloading content, and therefore evidence of outside engagement may also reveal additional parties involved in a wider network.
5. *Is there digital evidence which may support a claim that the suspect is not responsible for the IDCSA being present on the device?*: Finally, practitioners should establish if any information exists on a system which may provide an alternative version of events from that which is suspected (Casey, 2018; Horsman, 2019, 2020a, 2020b). This is often referred to as an alternative hypothesis (Casey, 2018; Horsman, 2019, 2020a, 2020b).

Practitioner's should consolidate their interpretation of data and provide answers to the five questions, and seek sufficient peer review of the work they have undertaken as a mechanism for quality assurance (Horsman, 2019; Sommer, 2018).

## 4 | FINAL THOUGHTS

This work has outlined the challenges and benefits of standardization in DF before proposing an example standard for IDCSA investigations involving Windows 10 devices. It has been suggested that those who opt to propose models which

contribute to the knowledge base of standardization attempts in DF should look to focus on procedural areas which are *offence-specific*, *device-specific* and *operating system-specific*, which is the method followed here. In taking such a focused approach, arguably it allows greater control of the standardization implemented by a DF organization and a method for documenting and evidencing adherence to it. This brings with it greater potential quality control of the investigations which take place by practitioners. It is also acknowledged that taking this approach to every *offence* type for every device in which it could occur is difficult to sustain given the sheer amount of combinations which could present themselves. In addition, it is also acknowledged that platform and device updates—e.g., operating system service packs may impact such a framework to a minor degree, and such incremental changes are always going to challenge attempts at procedural standardization. Therefore, frequent evaluation of standardized approaches is needed in order to ensure it remains viable for use following any such updates. However, it is argued that this model could offer a skeleton structure which could be adopted and adapted in other *offence* and device combinations. Whilst the push for standardization is one which requires the investment of time and resources to achieve, it is argued that the benefits in the form of quality control and being able to evidence this, make it worth pursuing. If the field of DF is to ensure it continues to effectively support legal systems and law enforcement in their investigation of crime, mechanisms for standardization should be seen as a must, where encouragement should be given to those seeking to contribute approaches for achieving this.

## CONFLICT OF INTEREST

The author has declared no conflicts of interest for this article.

## ORCID

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

## REFERENCES

Abbott, K. W., & Snidal, D. (2001). International 'standards' and international governance. *Journal of European Public Policy*, *8*(3), 345–370.

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security*, *5*(1), 118–131.

Amann, P., & James, J. I. (2015). Designing robustness and resilience in digital investigation laboratories. *Digital Investigation*, *12*, S111–S120.

Association of Chief Police Officers'. (2012). *Good practice guide for computer-based electronic evidence*. Retrieved from https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

BSI. (2020a). *Home*. Retrieved from https://www.bsigroup.com/en-GB/

BSI. (2020b). *Standards matter to consumers*. Retrieved from https://www.bsigroup.com/LocalFiles/en-GB/consumer-guides/resources/BSI-consumer-brochure-standards-matter-to-consumers-UK-EN.pdf

Bulbul, H. I., Yavuzcan, H. G., & Ozel, M. (2013). Digital forensics: An analytical crime scene procedure model (ACSPM). *Forensic Science International*, *233*(1–3), 244–256.

Cargill, C. F. (2011). Why standardization efforts fail. *Journal of Electronic Publishing*, *14*(1).

Casey, E. (2002). Error, uncertainty and loss in digital evidence. *International Journal of Digital Evidence*, *1*(2), 1–45.

Casey, E. (2018). Clearly conveying digital forensic results. *Digital Investigation*, *24*, 1–3.

Casey, E. (2019). The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences*, *51*(6), 649–664.

Casey, E. (2020). Standardization of forming and expressing preliminary evaluative opinions on digital evidence. *Digital Investigation*, *32*, 200888.

Crown Prosecution Service. (2020). *Indecent and prohibited Images of children*. Retrieved from https://www.cps.gov.uk/legal-guidance/indecent-and-prohibited-images-children

Department for Business, Energy & Industrial Strategy. (2012). *Standardisation explained*. Retrieved from https://www.gov.uk/government/publications/standardisation/standardisation

ForensicFocus. (2017). *Challenges of ISO 17025 accreditation—Survey: Results*. Retrieved from https://www.forensicfocus.com/legal/challenges-of-iso-17025-accreditation-survey-results/

ForensicFocus. (2018). *ISO 17025 for digital forensics—Yay or nay*. Retrieved from https://www.forensicfocus.com/legal/iso-17025-for-digital-forensics-yay-or-nay/

Grobler, M. (2010). *Digital forensic standards: International progress*.

Grobler, M. (2012). The need for digital evidence standardisation. *International Journal of Digital Crime and Forensics*, *4*(2), 1–12.

Hatto, P. (2013). *Standards and standardisation: A practical guide for researchers*. European Commission-Directorate-General for Research & Innovation.

Home Office. (2018). *The Child Abuse Image Database (CAID)*. Retrevied from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759328/CAID_Brochure_May_2018_for_gov_uk.pdf

Home Office, Association of Police and Crime Commissioners, & National Police Chiefs' Council. (2018). *Forensics review*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/800447/Joint-review-of-forensics-provision-July-2018.pdf

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

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

Horsman, G. (2020a). Digital evidence certainty descriptors (DECDs). *Digital Investigation*, *32*, 200896.

Horsman, G. (2020b). Opinion: Does the field of digital forensics have a consistency problem? *Digital Investigation*, *33*, 300970.

Horsman, G., Findlay, B., & James, T. (2019). Developing a 'router examination at scene' standard operating procedure for crime scene investigators in the United Kingdom. *Digital Investigation*, *28*, 152–162.

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.

Interpol. (2019). *Global guidelines for digital forensics laboratories* Retrevied from https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

ISO. (2020). *Home*. Retrevied from https://www.iso.org/home.html

ISO. (2020b). *ISO/IEC 27037:2012(en)* Retrevied from https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

Jaquet-Chiffelle, D. O., Casey, E., Pollitt, M., & Gladyshev, P., (2018) *A framework for harmonizing forensic science practices and digital/multimedia evidence* (No. 0002). OSAC/NIST.

Karie, N. M., Kebande, V. R., Venter, H. S., & Choo, K. K. R. (2019). On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports*, *1*, 100008.

Kebande, V. R., & Ray, I. (2016). A generic digital forensic investigation framework for internet of things (IoT). In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 356–362). New York, NY: IEEE.

Lalla, H., & Flowerday, S. (2010). August. Towards a standardised digital forensic process: E-mail forensics. In *ISSA, Information Security South Africa Conference 2010, Sandton, South Africa*.

Mayor of London. (2019). *Backlog of mobile phones and computers awaiting forensic analysis*. Retrevied from https://www.london.gov.uk/questions/2019/12159#:~:text=Digital%20Forensics%20currently%20have%20approximately,will%20take%20over%2012%20months

Montasari, R. (2017). A standardised data acquisition process model for digital forensic investigations. *International Journal of Information and Computer Security*, *9*(3), 229–249.

Montasari, R., & Hill, R. (2019). Next-generation digital forensics: Challenges and future paradigms. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* (pp. 205–212). New York, NY: IEEE.

Mothi, D., Janicke, H., & Wagner, I. (2020). A novel principle to validate digital forensic models. *Digital Investigation*, *33*, 200904.

Page, H., Horsman, G., Sarna, A., & Foster, J. (2018). A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn? *Science & Justice*, *59*(1), 83–92.

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

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

Scanlon, M. (2016). August. Battling the digital forensic backlog through data deduplication. In *2016 sixth international conference on innovative computing technology (INTECH)* (pp. 10–14). New York, NY: IEEE.

Scholtz, J., (2010) *Towards an automated digital data forensic model with specific reference to investigation processes* (Doctoral dissertation). Auckland University of Technology).

Sibiya, G., Venter, H. S., Ngobeni, S., & Fogwill, T. (2012). Guidelines for procedures of a harmonised digital forensic process in network forensics. In *2012 information security for South Africa* (pp. 1–7). New York, NY: IEEE.

Silde, A., & Angelopoulou, O. (2014). A digital forensics profiling methodology for the cyberstalker. In *2014 international conference on intelligent networking and collaborative systems* (pp. 445–450). New York, NY: IEEE.

Sommer, P. (2018). Accrediting digital forensics: What are the choices? *Digital Investigation*, *25*, 116–120.

Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation*, *29*, 101–108.

Thompson, T. (2019). *Forensic delays 'deeply concerning' as case backlog grows*. Retrevied from https://www.policeprofessional.com/news/forensic-delays-deeply-concerning-as-case-backlog-grows/

Tulley, G. (2017). *Codes of practice and conduct*. Retrevied from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651966/100_-_2017_10_09_-_The_Codes_of_Practice_and_Conduct_-_Issue_4_final_web_web_pdf__2_.pdf

Tully, G. (2020). *Annual report*. Retrevied from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/877607/20200225_FSR_Annual_Report_2019_Final.pdf

Valjarevic, A., & Venter, H. S. (2012a). Harmonised digital forensic investigation process model. In *2012 Information Security for South Africa* (pp. 1–10). New York, NY: IEEE.

Valjarevic, A., & Venter, H. S. (2012b). Harmonised digital forensic investigation process model. In *2012 Information Security for South Africa* (pp. 1–10). https://doi.org/10.1109/ISSA.2012.6320441.

**How to cite this article:** Horsman G. Standardizing digital forensic examination procedures: A look at Windows 10 in cases involving images depicting child sexual abuse. *WIREs Forensic Sci*. 2021;e1417. https://doi.org/10.1002/wfs2.1417