ERA Forum (2021) 22:587–599
https://doi.org/10.1007/s12027-021-00687-1

ARTICLE

Digital investigations: relevance and confidence in disclosure

Philip Anderson[1] · **Dave Sampson**[1] · **Seanpaul Gilroy**[2]

Accepted: 7 September 2021 / Published online: 21 September 2021

Abstract
The field of digital forensics has grown exponentially to include a variety of digital devices on which digitally stored information can be processed and used for different types of crimes. As a result, as this growth continues, new challenges for those conducting digital forensic examinations emerge. Digital forensics has become mainstream and grown in importance in situations where digital devices used in the commission of a crime need examining. This article reviews existing literature and highlights the challenges while exploring the lifecycle of a mobile phone examination and how the disclosure and admissibility of digital evidence develops.

Keywords Digital investigations · Disclosure · Relevance · Transparency · Fair trial

1 Introduction

1.1 Digital evidence

Owen and Thomas define forensics as the use of science to provide facts in the process of identifying, recovering and reconstructing evidence [1]. Therefore, the aim of computer or digital forensics can be described as the preservation, identification, extraction, interpretation, and presentation of computer data which can be used by a court of law [2]. Digital forensic evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter, to help jurors establish the

✉ P. Anderson
philip.anderson@northumbria.ac.uk

1 Dept. of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne, UK

2 Newcastle upon Tyne, UK

facts of the case and to support or refute legal theories of the case. Traditional acquisition tools produce an image that is a duplicate of the original media. The image will include all regions of the original media, even those that are blank, unused, or irrelevant to the investigation. It will also include large portions devoted to operating systems of third-party applications and programs supplied.

1.2 Digital investigation guidelines and standards

The Association of Chief Police Officers (ACPO) guide to good practice during digital investigations fundamentally consists of four principles. These guiding 'principles' are relied upon by digital investigators, police officers and staff, and those working within the private sector. Lallie and Pimlott [3] identify the use of the four key principles within Digital Forensic Investigations, highlighting their adoption as part of any standard investigation not only within the UK but within most of Europe. The four ACPO principles are as follows:

- Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
- Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to [4].

The first two principles might seem contradictory, but they have been developed in such a way that adherence will not impede a digital investigation. Many cases, especially involving smartphones, dictate that evidence cannot be secured or analysed without any changes being made. Hence, the second principle allows for changes to be made by a competent individual. If this principle was not present in the guidelines, many investigations could not be completed while maintaining compliance. Consequently, the admissibility of any presented evidence could quickly be called into question by the opposition in court [4].

At the same time that these guidelines were being published by the ACPO, the National Institute for Standards and Technology released their official recommendations for best practice in the field of digital forensics. The NIST guidelines provided an extensive set of recommendations for forensic examiners carrying out forensic investigations at the time. The publication includes both investigative models and principles, as well as practical knowledge that can be directly applied to various challenges during an investigation [5].

In addition to the ACPO Principles and NIST guidelines, Digital Forensic Investigators in the UK faced a new set of regulatory guidelines around investigative methods and tools. The UK Forensic Science Regulator introduced ISO17025, a nationally recognised laboratory standard for the testing and validation of methods and

tools which became a mandatory accreditation for Digital Forensic labs in 2017 [6]. ISO17025 details the technical and quality requirements that forensic labs must abide by, such as when a forensic practitioner conducts a method that does not conform to the standard [5]. If a digital forensic unit is not accredited under ISO17025, or they use a method that has not been assessed by the United Kingdom Accreditation Service (UKAS) for its conformance with ISO17025, they must detail their non-conformance when presenting their evidence.

In the same way that other forms of evidence need to be handled appropriately, there are several standards and industry guidelines to be considered while interacting with digital evidence. Since the relevant publications have now been implemented for many years, a failure to adhere will likely cause a dispute of admissibility during its presentation in a courtroom.

More recently the College of Policing [7] developed its own set of guidelines around the examination of digital devices, the 'Associate Professional Practice' guidance in the form of 10 principles. When writing the principles, the College of Policing acknowledges the consideration of a report by the Information Commissioners Office, relevant legislation, and a recent Court of Appeal judgments to ensure police officers and staff obtain evidence from digital devices fairly and lawfully while maintaining an individual's right to privacy and a fair trial.

1.3 Digital crimes: smartphones

The landscape of digital crime has been drastically changed by the widespread popularity of smartphones, with an increasing number of mobile devices being involved in criminal investigations. The underlying technology is rapidly evolving and has presented a new set of challenges for digital forensics investigators [8]. Over the last 20 years, various eras of mobile forensics have been identified which reflect the state of the discipline at that time. These stages consist of the early era pre-2007, at the first turning point for smartphone popularity. 2011-2013 saw the rapidly increasing popularity of smartphones across the globe, with further inclusions within the criminal investigations setting. Finally, 2014 onwards saw the exponential increase in smartphone usage in computer crime [9]. Smartphones are potentially very valuable within a forensic investigation, due to the wealth of data they can hold regarding user activity and events [10].

2 Examination of digital devices

As the field of Digital Forensics grows and forensic software providers enhance their capability for recovering data from digital devices, the complexity of these examinations increases. Whilst this is prevalent across the entire field of digital forensics, it is arguably most prevalent in the forensic examination of mobile devices such as mobile phones, tablets, and satellite navigation systems due to the complexities and challenges posed during such investigations.

2.1 Digital forensic lifecycle

A model will typically be structured into several stages, each of which contains the appropriate methodologies to be used across the investigation's timeline. Different methodologies store the relevant actions to be taken during a stage of an investigation. These models are generic so that they can be adapted to guide a broad range of scenarios. Since our digital landscape has drastically changed, older models need to be adapted along with the development of new frameworks. Recent developments in digital forensics models have focused on specific areas of the discipline, such as creating models for smartphone forensics. Newer research aims to modernise process models to mimic the advancements in digital forensics [11].

To understand the complexities, those involved in the disclosure of digital data must understand the lifecycle of a Digital Forensic Investigation. Whilst the lifecycle may vary between organisations across the globe, the fundamental lifecycle often used remains very similar and comprises of several key stages [12].

1. *Identification* – Stage one involves investigators identifying sources of information; this could be from an array of digital devices including computers, mobile phones, tablets, and SIM cards.
2. *Preservation* – Stage two involves investigators safeguarding electronic information and preserving the crime scene.
3. *Collection* – Stage three involves investigators collecting the devices from the crime scene. Once collected they are then responsible for extracting the data from the device and creating a forensic copy, where possible in a forensically sound manner maintaining evidential integrity.
4. *Analysis* – Once the data has been successfully extracted, the investigator is then responsible for conducting an analysis of the recovered data; this could include an analysis of both system- and user-generated information which may be useful and assist in drawing conclusions.
5. *Reporting* – The final stage involves the investigator generating a report documenting the result of their analysis of the digital data. This also ensures that a third party is able to repeat their actions and obtain the same results where required.

2.2 Mobile phone forensics

The mobile phone market has a number of different vendors, such as Apple, Samsung, and Huawei, all of which fight to dominate the market. These different vendors' devices often store data in different ways and have a variety of operating systems alongside proprietary file systems. These variables themselves present an ongoing challenge the field of Digital Forensics and as a result, the field must constantly adapt to ensure that new emerging technologies can be collected, analysed, and reported upon [13].

During the collection stage, the Digital Forensic Investigator can employ several techniques to extract data from mobile devices, as outlined in Fig. 1 [14]:

Whilst all methods of extraction may not be possible for every model of device, it is common practice that a single mobile phone device may be subjected to several different extraction types to maximise forensic opportunities by extracting all of the

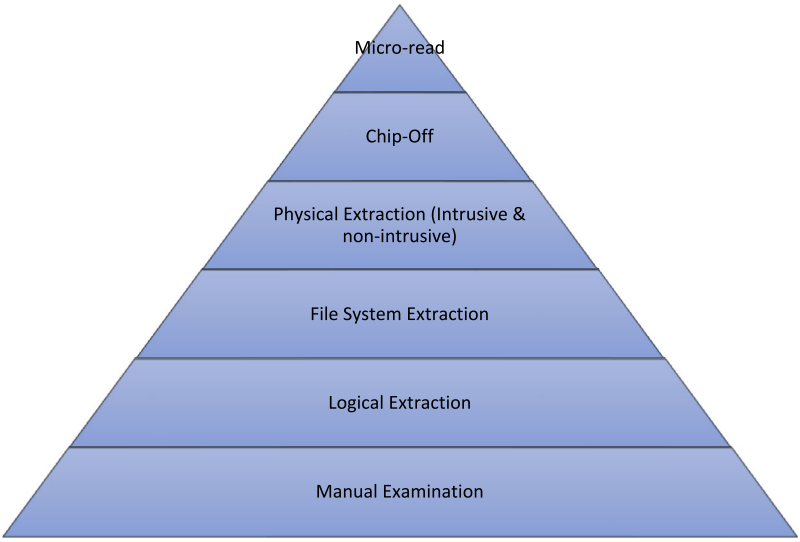

Fig. 1 Mobile Phone Extraction Pyramid

required data. It is the responsibility of the allocated Digital Forensic Investigator to understand these techniques and identify the most suitable on a case-by-case basis.

2.3 Case study

To fully understand the problems posed when dealing with disclosure in Digital Forensics, the case study documented below follows a basic submission to a Digital Forensic Unit as part of an ongoing homicide investigation. As part of this case study, the investigation team have submitted a single mobile device to their local Digital Forensic Unit for examination. Digital Forensic Investigations present several unique challenges to investigators. In an attempt to overcome these challenges, investigators often employ the use of Digital Evidence Strategies, also commonly known as Digital Investigative Strategies [4]. The Association of Chief Police Officers highlights several key stages when developing a Digital Investigative Strategy [4]:

- Data Capture and search and seizure at crime scenes;
- Data Examination;
- Data Interpretation;
- Data Reporting;
- Interview of Witness and Suspects.

Digital Evidence strategies allow investigators to set parameters such as time frames that are proportionate to the facts and assist in overcoming the challenges presented by the large volume of data stored on digital devices and associated storage services [15]. The use of Digital Evidence Strategies allows the examination of digital devices to be both targeted and proportionate and streamline the forensic process.

The submission contains a Digital Evidence Strategy which requests the following key data from the device:

- SMS/MMS Messages
- Incoming & Outgoing Call Data
- Pictures & Videos

It is widely recognised within the field of Digital Forensic Investigations that investigators have a variety of forensic tools at their disposal that can be used throughout the extraction and analysis stage of the investigation [15].

The Digital Forensic Investigator allocated to the case may have utilised forensic *"Tool A"* to conduct the following forensic extractions of the device:

- Logical
- File system

During a review of the two forensic extractions undertaken using forensic *"Tool A"*, it may become apparent to the Digital Forensic Investigator that the SMS messages required by the investigation team were not recovered, and again this is not uncommon when conducting an examination of mobile devices as highlighted by the Crown Prosecution Service [16]. As a result, they may opt to use forensic *"Tool B"* to conduct a further two extractions in an attempt to recover the required SMS messages:

- Logical Extraction
- File System

Both "Tool A" and "Tool B" may have failed to recover the SMS messages required by the investigation team; this is not a fault with the software but instead a limitation of the forensic software for that given device.

To further complicate matters, device support across forensic tools differs heavily and as a result "Tool C" may offer a more complex type of extraction such as a Physical, as outlined within the Mobile Phone Extraction Pyramid, which both "Tool A" and "Tool B" did not offer. As part of this case study, consider that the physical extraction conducted by "Tool C" successfully recovered the required SMS messages. As a result of the above extractions the Digital Forensic Investigator now has the below extractions ready to report upon:

- Logical (Obtained using forensic tool A)
- File System (Obtained using forensic tool A)
- Logical (Obtained using forensic tool B)
- File System (Obtained using forensic tool B)
- Physical (Obtained using forensic tool C)

Digital Forensic Investigators often merge multiple mobile phone extractions; this provides the Digital Forensic Investigator with the ability to produce a unified report (such as PDF or Excel) for the investigation team to review as part of "Stage 5: Reporting" [17].

Merging forensic extractions has several different benefits, including reducing the amount of time spent reviewing numerous extraction types as well as removing duplicate records. A logical, file system, and physical extraction may recover the same SMS 3 times; merging the records would ensure that the investigation team are only required to review this a single time, ultimately leading to more streamlined investigations - beneficial in today's world of "big data" [16].

As Digital Forensic Investigators and legal practitioners, robust procedures must be developed and maintained into department Quality Management Systems to ensure that data held as part of the Digital Forensic Investigation is disclosed correctly. Forensic tools store data in proprietary formats which can often only be accessed by the use of forensic tools which require specialist training; disclosing this data presents us with the challenge of interpreting it away from Digital Forensic Laboratories.

3 Principles of disclosure

The disclosure regime in England and Wales is governed by the Criminal Procedure and Investigations Act (CPIA) 1996 [18]. According to guidelines published by the Attorney General, the CPIA 1996 "aims to ensure that criminal investigations are conducted in a fair, objective and thorough manner" [19]. Further, the guidelines acknowledge that "[a] fair trial is the proper object and expectation of all participants in the trial process. Fair disclosure to the accused is an inseparable part of a fair trial" [20]. This explicit link between effective disclosure and the fair trial rights of the accused mean that failures of disclosure by the prosecution can have serious implications under Article 6 European Convention on Human Rights (ECHR [21]).

> "Fairness ordinarily requires that any material held by the prosecution which weakens its case or strengthens that of the defendant, if not relied on as part of its formal case against the defendant, should be disclosed to the defence. Bitter experience has shown that miscarriages of justice may occur where such material is withheld from disclosure. The golden rule is that full disclosure of such material should be made." - House of Lords, *R v H and C* [22].

CPIA 1996 endeavours to set standards and procedures to regulate the investigation process and manage the recording and retention of all material found or generated in the course of an investigation. Core roles and responsibilities are defined with regulatory duties to achieve the desired outcomes.

In *R v Malook* [23] the England and Wales Court of Appeal held that the duty to record applies not only to material evidence seized by the police during an investigation but equally to "documentation produced by the police in the course of investigations in contradistinction to pre-existing material seized by a police force." Further, the court held that "Proper record-keeping in an investigation is essential to the integrity of an investigation, to public confidence in police investigations and the proper administration of justice [24].

All investigators have a responsibility to carry out the duties imposed under CPIA 1996, including recording relevant information and retaining records of the information and other material from the outset of the investigation. The most important of these responsibilities is for an investigator to pursue all reasonable lines of enquiry, whether these point towards or away from a suspect. What is reasonable in each case will depend on the particular circumstances. For example, where the material is held on a computer, it is for the investigator to decide which material on the computer it is reasonable to enquire into, and in what manner. Material may be relevant to an investigation if it appears that it has some bearing on any offence under investigation or

any person being investigated, or on the surrounding circumstances of the case unless it is incapable of having any impact on the case [25].

The officer in charge of an investigation is responsible for directing and focusing the investigation, setting the parameters for the lines of enquiry. They are also responsible for ensuring that there are proper processes and procedures in place in the investigation for the recording of information and retaining records of other material. Some information will be used in the prosecution and will form the evidence of the case. The remaining information is referred to as unused material. This material is relevant to the case but is not being used as part of the prosecution evidence presented to the Court.

The disclosure officer [26] will have responsibility for ensuring that material generated during an investigation is properly recorded on a Schedule of Unused Material [27]. The revised Code of Practice to the CPIA 1996 requires that the disclosure officer should ensure that each item of material is listed separately on the schedule and is numbered consecutively. The description of each item should make clear the nature of the item and should contain sufficient detail to enable the prosecutor to decide whether they need to inspect the material before deciding whether or not it should be disclosed [28].

CPIA 1996 establishes a disclosure test that requires the prosecution to disclose any unused material that might reasonably be considered capable of undermining the prosecution case or of assisting the case for the accused [29]. The police and CPS in England and Wales are independent of each other, but each depend on the other performing their respective disclosure obligations. When a charge is brought against a person, the prosecution must serve the evidence that it will rely on in court to prove its case. The prosecution also has an initial disclosure duty which obliges the prosecutor to disclose to the defendant any unused material that satisfies the disclosure test. The prosecution's duty to disclose material is determined by the application of s.3 CPIA 1996. The disclosure of sensitive material [30] may be withheld on public interest grounds under a Public Interest Immunity (PII) application. In *R v H* [31] Lord Bingham of Cornhill eruditely summarised the operation of PII in the following terms: "Circumstances may arise in which material held by the prosecution and tending to undermine the prosecution or assist the defence cannot be disclosed to the defence, fully or even at all, without the risk of serious prejudice to an important public interest."

All parties, the investigator, the disclosure officer, and the prosecutor have a continuing duty to keep disclosure under review throughout the life of a case. As a part of the defence case, they serve a defence statement setting out the nature of the defence and request any material which could reasonably assist their case. This request is incorporated within the ongoing evaluation of the material held.

Disclosure of digital evidence fits within the framework of CPIA 1996; in principle the digital data is material. The challenge lies in the volume of the digital data and the additional challenges this raises in the identification of relevant data, as well as the ethical challenge posed by the processes to accessing and interpreting the data. As stated by Alison Saunders DPP – "while the principles remain unchanged, our working practices have had to respond to several significant developments... Criminal justice system-wide initiatives and, other changes, such as the unprecedented rise in

the volume of digital material created in criminal investigations, could not easily have been foreseen, and a fundamental review of the manual (CPIA 1996) has been undertaken" [32].

4 The disclosure challenges

Identification – To support the compiling of a Disclosure Management Document to facilitate a robust digital disclosure procedure the early creation of a digital strategy is required within every investigation. This can then be used as a guide and a rationale for the seizure and more importantly the non-seizure of digital items. Some devices' non-seizure can be dictated by the sheer volume of the device or the volatile nature of the data. Other devices' non-seizure may be mandated in respect of a victim's device, or subjectively in each case, for example following the onsite triage of a child's laptop to eliminate it from the enquiries due to its necessity for educational support or other reasons.

Historically, all digital devices would be seized for evaluation and potential examination as a matter of course. This process is still valid if it is justified and documented. But the modern digital world requires a more efficient digital data seizure approach. What are the relevant lines of the enquiry of the investigation and, within that, what are the date parameters? The validity of the seizure of a computer base unit stored and undisturbed for a significant period at a scene where the alleged offending has occurred in a recent timeframe would appear disproportionate to the investigation. For this issue, there is not a default answer, it is in certain circumstances acceptable to seize all digital media. But with this they should also expect to have to justify their course of actions, explain the relevance of the items to the investigation, and state what they intend to do with the items. If the intention is to not submit them for examination, then surely the question should be asked – why seize them in the first place? Similarly, the seize-all policy cannot be applied to complainants' and witnesses' digital devices. The right of privacy of an individual must be balanced against the suspect's right to a fair trial. The examination of complainants' and witnesses' devices must be done with their informed consent. They need to be fully aware of how the device is going to be examined, the data desired to be extracted, and to what ends that information is to be interrogated and shared. This requirement needs to follow the relevant lines of enquiry of the investigation, with the owner informed that it is not always possible to extract the exact data as required and that data outside of the requirement may need to be extracted to allow for further investigation and recovery of the relevant material [33].

Preservation and collection – Data is volatile and the historic storage of data on a single hard drive connected to a single device is of a rapidly disappearing era. In the modern home, there is now a myriad of digital devices utilising wireless and mobile network connectivity to provide the always-on requirement of contemporary society. This presents a new world of challenges to the safe and secure presentation of data. Volatile data is any kind of data that is available while a digital device is powered on and could be lost once the machine is turned off. The capturing of live data may contain information that through correct collection and analysis may become evidence

within an investigation that may be critical. Similarly, cloud data storage can often be split across multiple different devices and infrastructures, resulting in evidence being difficult to find and, more importantly, to preserve in an efficient timeframe. Once identified, the evidence must be recovered and preserved in a forensically sound manner. Data storage has the potential to be so vast that acquisition for analysis becomes unreasonable; this requires a different approach to examining the preserved data in situ and presents a greater need for all investigating bodies on both sides of a case to streamline the analysis process by agreeing on common requirements to feed the data interrogation.

The examination and analysis of digital media does not change data but identifies from within the data what is deemed relevant. This can be a fraught process with some digital material initially assessed as irrelevant data on its own merit, but this data may be metadata [34] with the ability to add value and substance to other identified relevant data. This can be very relevant and making the initially disregarded data significant to an investigation. As the disclosure process itself is a live ongoing process throughout an investigation, the review and identification of relevance within digital material must be fluid and adaptable. Collaboration is key to allow for all parties to have a thorough understanding of what digital material is held and, when lawfully allowed an understanding of the content of the digital material so that all parties are fully informed of the material's relevance and value to their investigation. The agreement of search parameters and search definitions supported by how the searching is to be completed is seldom reached in a timeframe which would allow the process to be completed, reviewed, and where necessary challenged. Search parameters cannot be set so wide as to fail to reduce the data sets being examined or so narrow as to yield minimal content. Within digital data, there is the potential for a person's whole life to be laid bare in a raw format. Uncontrolled access to this data cannot be granted due to the necessity of protecting the individual's right to a private life. The data should be accessed in a manner that allows for the examination of relevant information only, not - as is currently the case when a significant date in the criminal justice process approaches and acts as a trigger – in a manner giving unfettered access in contravention of CPIA 1996.

5 Conclusions

Digital evidence poses significant challenges and continues to grow in size, complexity and importance. In recent years, investigations involving digital devices have exponentially increased to include many and varied types of digital devices on which digitally stored information can be stored and processed. As a result of this, digital evidence has been presented in a growing number of criminal and civil court cases over the last decade. Because of how digital evidence is obtained, examined, analysed, and presented in court, it is often challenged, with parties contesting how the digital device was acquired or arguing that it was examined and analysed ineffectively.

Digital evidence must meet the same standards as other scientific and technical evidence in order to be admissible in court. Standards and guidelines are a necessary requirement to ensure that the courts and legal system are safeguarded from poor

digital evidence. The recent ISO17025 standard, however, does not directly assess an individual's expertise and competence, instead, it addresses the competency of the digital forensic lab and the tools used to conduct digital device examination. In some instances, digital evidence is omitted on the basis that it was obtained incorrectly or examined ineffectively.

In the United Kingdom, various laws and rules govern the admissibility of digital evidence in courts. Understanding how digital evidence is obtained affects how judges and juries weigh the importance of this evidence when it is presented in court. It could be said that to fairly and impartially assess the value of digital evidence, judges and juries should understand the basic functions of digital devices, such as computers and the software from which any evidence is extracted.

The use of Digital Evidence Strategies within a Digital Forensic Examination is becoming increasingly more important and offers a useful tool to investigators to assist with the disclosure of Digital Evidence. Whilst these strategies are dynamic and may change as the investigation progresses, they ensure that the examination is targeted and proportionate. If during the course of an investigation new lines of enquiry are identified, the Digital Evidence Strategy could be altered to include them, for example through further keyword searches across the raw data.

Due to the complex nature of Digital Forensic Investigations, it is vital that all parties collaborate in order to ensure that Digital Evidence is disclosed in the correct manner. Investigation teams may only receive tailored reports such as PDF or Excel documents that have been produced as part of the supplied Digital Evidence Strategy. The Digital Forensic team will retain the raw case files generated during the "collection" and "analysis" stage of the lifecycle which is likely to contain a wealth of data in comparison to the tailored reports. These raw case files often require commercial forensic tools and specialist training to analyse and interpret so that reports can be produced; ensuring that these raw case files are disclosed during an investigation is therefore vital "to ensure that criminal investigations are conducted in a fair, objective and thorough manner" [35]. A robust system should be employed to ensure that all material during the forensic examination is disclosed correctly.

The uncontrolled access to and examination of digital devices is correctly being challenged by society as a breach of privacy. The modern mobile phone contains a link or direct access route to every part of an individual's life from banking to social media profiles and beyond. New regimes and requirements are emerging and proving additional challenges to the seizure and examination of such devices. This requirement will grow and, as it is initially tested within the criminal justice system, will raise further exacting considerations for both disclosure and beyond.

The success of the disclosure process is fundamental to underpinning confidence in the criminal justice system. The defined structures and processes of the disclosure regime are in principle robust and correct but they need to be constantly reviewed in order to keep pace with the continually changing digital landscape and must be correctly applied by all parties. Collaboration is key across all interested parties in order to enable a fair trial to be held with appropriate interrogation of the disputed facts within an investigation, supported by the knowledge that all parties have a fundamentally clear awareness of all other data held. A disclosure process has to be adopted early in order for it to be successful. Any delay results in an ongoing process

of catch-up, which has consequences at each stage of the criminal justice process which can and do culminate in failings by one or all parties at a critical evidential stage, to the detriment of all involved.

References

1. Owen, P., Thomas, P.: An analysis of digital forensic examinations: mobile devices versus hard disk drives utilising ACPO & NIST guideline. Digit. Investig. **8**(2), 135–140 (2011). https://doi.org/10.1016/j.diin.2011.03.002
2. Dixon, P.D.: An overview of computer forensics. IEEE Potentials **24**(5), 7–10 (2005). https://doi.org/10.1109/MP.2005.1594001.
3. Lallie, H., Pimlott, L.: Applying the ACPO principles in public cloud forensic investigations. J. Digit. Forensics, Secur. Law **7**(1), 71–85 (2012). https://commons.erau.edu/jdfsl/vol7/iss1/5?utm_source=commons.erau.edu%2Fjdfsl%2Fvol7%2Fiss1%2F5&utm_medium=PDF&utm_campaign=PDFCoverPages. Accessed 24 May 2021
4. ACPO Good Practice Guide for Digital Evidence. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. Accessed 23 May 2021
5. Jansen, W., Ayers, R.: Guidelines on cell phone forensics. NIST Special Publication 2007;800:101. https://www.govinfo.gov/content/pkg/GOVPUB-C13-bd12c48cccb6fefb73982be53dea84c4/pdf/GOVPUB-C13-bd12c48cccb6fefb73982be53dea84c4.pdf. Accessed 12 July 2021
6. Barmpatsalou, K., Damopoulos, D., Kambourakis, G., Katos, V.: A critical review of 7 years of Mobile Device Forensics. Digit. Investig. **10**(4), 323–349 (2013). https://www.sciencedirect.com/science/article/pii/S1742287613001096. Accessed 4 July 2021
7. College of Policing: *ISO-17025 Extraction of material from digital devices* (2021). https://www.app.college.police.uk/app-content/extraction-of-material-from-digital-devices/. Accessed 12-30 July 2021
8. Quick, D., Choo, K.: Digital forensic intelligence: data subsets and Open Source Intelligence (DFINT+OSINT): a timely and cohesive mix. Future Gener. Comput. Syst. **78**, 558–567 (2018). https://www.sciencedirect.com/science/article/pii/S0167739X16308639. Accessed 4 July 2021
9. Chernyshev, M., Zeadally, S., Baig, Z., Woodward, A.: Mobile forensics: advances, challenges, and research opportunities. IEEE Secur. Priv. **15**(6), 42–51 (2017). https://ieeexplore.ieee.org/abstract/document/8123468. Accessed 4 July 2021
10. Mahalik, H., Bommisetty, S., Skulkin, O., Tamma, R.: Practical Mobile Forensics 3rd edn. pp. 1–5. Packt Publishing Ltd., Birmingham (2018)
11. Du, X., Le-Khac, N., Scanlon, M.: Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service (2017). ArXiv preprint, arXiv:1708.01730. Accessed 4 July 2021
12. The Digital Forensic Process. https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.1. Accessed 9 July 2021
13. Lillis, D., Becker, B.A., O'Sullivan, T., Scanlon, M.: Current Challenges and Future Research Areas for Digital Forensic Investigation (online) (2016). https://arxiv.org/pdf/1604.03850.pdf. Accessed 10 July 2021
14. SWDGE Best Practice for Mobile Phone Forensics. https://athenaforensics.co.uk/wp-content/uploads/2019/01/SWGDE-Best-Practices-for-Mobile-Phone-Forensics-021113.pdf Accessed 10 July 2021
15. 10 Challenges in Mobile Forensics (n.d.). https://www.t3k.ai/allgemein-en/10-main-challenges-in-mobile-forensics2/. Accessed 10 July 2021

16. Disclosure - a guide to "reasonable lines of enquiry" and communications evidence (2018). https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence. Accessed 27 July 2021
17. Cellebrite Release Notes – Version 5.0 (2016). https://cf-media.cellebrite.com/wp-content/uploads/2017/07/UFED_5.0_ReleaseNotes.pdf. Accessed 10 July 2021
18. Criminal Procedure and Investigations Act 1996 c.25. https://www.legislation.gov.uk/ukpga/1996/25/contents. Accessed 9 July 2021
19. Attorney General's Office, Attorney General's Guidelines on Disclosure, December 2013, para.1. https://www.gov.uk/government/publications/attorney-generals-guidelines-on-disclosure-2013. Accessed 9 July 2021
20. Attorney General's Office, Attorney General's Guidelines on Disclosure, December 2013, page 4, para 7. https://www.gov.uk/government/publications/attorney-generals-guidelines-on-disclosure-2013. Accessed 9 July 2021
21. Article 6 European Convention on Human Rights. https://www.echr.coe.int/Documents/Convention_ENG.pdf. Accessed 9 July 2021
22. House of Lords, *R v H and C* [2004] UKHL 3. https://publications.parliament.uk/pa/ld200304/ldjudgmt/jd040205/hc-1.htm. Accessed 9 July 2021
23. *R v Malook* [2011] EWCA Crim 254. https://www.bailii.org/ew/cases/EWCA/Crim/2011/254.html. Accessed 9 July 2021
24. *R v Malook* [2011] EWCA Crim 254, [35]. https://www.bailii.org/ew/cases/EWCA/Crim/2011/254.html. Accessed 9 July 2021
25. Section 3(1)(a) of the CPIA,1. https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence. Accessed 9 July 2021
26. Section 3(1)(a) of the CPIA,2. https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence. Accessed 9 July 2021
27. Form MG6C, see CPS Disclosure Manual (revised 14th Dec. 2018), Chap. 6 and NPCC, CPS, National Disclosure Standards, March 2019. https://www.cps.gov.uk/sites/default/files/documents/legal_guidance/National-Disclosure-Standards-2018.pdf. Accessed 9 July 2021
28. Revised Code of Practice to the CPIA 1996 (s.23(1)), para 6.11. https://www.gov.uk/government/publications/criminal-procedure-and-investigations-act-code-of-practice. Accessed 9 July 2021
29. Criminal Procedure and Investigations Act 1996, s.3 (as amended by Criminal Justice Act 2003 (c.44)). https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence. Accessed 9 July 2021
30. Revised Code of Practice to the CPIA 1996 (s.23(1)), para 6.14. https://www.gov.uk/government/publications/criminal-procedure-and-investigations-act-code-of-practice. Accessed 9 July 2021
31. *R v H* [2004] UKHL 4. https://publications.parliament.uk/pa/ld200607/ldjudgmt/jd070228/rvh-4.htm. Accessed 9 July 2021
32. Crown Prosecution Service and National Police Chiefs' Council - Action on Disclosure. https://www.cps.gov.uk/sites/default/files/documents/legal_guidance/Disclosure%20Manual_0.pdf. Accessed 9 July 2021
33. NPCC – Data Processing Notice DPNb - Witness information sheet. https://news.npcc.police.uk/resources/dpnb-witness-information-sheet. Accessed 9 July 2021
34. Metadata – Practice direction 31b Disclosure of electronic documents. Para 28. https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31/pd_part31b. Accessed 28 July 2021
35. Attorney General's Guidelines on Disclosure. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf. Accessed 28 July 2021