Received: 5 July 2022 | Revised: 1 September 2022 | Accepted: 23 March 2023

DOI: 10.1002/wfs2.1487

PERSPECTIVE

WIREs FORENSIC SCIENCE WILEY

We're making a list and we're checking it twice, gonna find out what makes digital forensic examiners suffice

Sarah Morris[1] | **Melissa Hadgkiss**[2] | **Anne David**[1] | **John Guinness**[1] | **Charles Frewin**[1]

[1]University of Southampton, Southampton, UK

[2]Cranfield University, Cranfield, UK

Correspondence
Sarah Morris, University of Southampton, Southampton, UK.
Email: s.morris@soton.ac.uk

Edited by: Kim-Kwang Raymond Choo, Editor

Abstract

Digital forensic examinations have grown in breadth and depth at a currently unsustainable rate. Digital Investigations now feature in around 90% of criminal cases, demonstrating that digital evidence is crucial to forensic investigations. Due to the high number of cases, most law enforcement units have significant backlogs of devices waiting for analysis. As the field of Digital Investigation has grown, it is no longer solely related to criminal investigations, with the techniques also supporting civil, private, and corporate activities. Given the evident challenges, it is logical that more digital forensic experts are needed to keep pace with the field's complexities and demands. Identifying what characteristics and skills make a digital forensic expert enables an evaluation to ensure that any new staff are fit for purpose. There is a growth in academic, civil, corporate, and intelligence-based activity within the field. Each area defines their standards, field scope, and expertise level. Still, as any case has the potential to become a matter of criminal investigation, surely the focus needs to be on the standards required to ensure evidence is admissible for that purpose. As expertise levels can vary, it is also necessary to challenge the level at which an expert is defined and the implications of this decision. By identifying what makes an expert in this unique forensic science area, it is possible to explore the potential challenges the field faces in obtaining, retaining, and training staff.

This article is categorized under:

Digital and Multimedia Science > Cybercrime Investigation

KEYWORDS

data recovery, digital forensic expert, Digital Forensics

1 | INTRODUCTION

To define what makes a digital forensic examiner an expert, it is first necessary to consider defining the field and where it sits in relation to other disciplines. Numerous papers already describe the general field of Digital Forensics

(Slay et al., 2009). Still, there is a growing trend to refer to the collective field of Digital Forensics and Incident Response (DFIR; Farid, 2018). The authors of this paper believe DFIR are types of Digital Investigation; their reasoning for this is discussed in this section.

While Digital Investigation is a global occupation, the authors of this expert commentary are all primarily working on investigations within the United Kingdom. When discussing their view in this expert commentary, the views and angles taken will be based on established UK practitioners. Therefore, some policies and challenges will vary across different jurisdictions.

1.1 | Digital Forensics

A starting point is to look at the definition of Digital Forensics. Digital Forensics is an evolved term, originating from Forensic Computing, aimed to encompass the wide range of digital devices that could be investigated. The National Institute of Standards and Technology (NIST) defines *Digital Forensics* as "The application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data." At its core is the "forensic" aspect, which relates to the presentation of evidence in Court. Given the rise in digital devices, it is no surprise that around 90% of criminal cases involve digital evidence (House of Lords, 2019). A traditional digital forensic investigator applies digital forensic practice to extract and present evidence from a digital device concerning a criminal case. Therefore, given the significant number of digital device cases, digital forensic investigators are a crucial part of the justice system.

Criminal proceedings require a weighting of "beyond reasonable doubt", a high standard of proof. The information identified and presented by a digital forensic analyst in criminal proceedings may impact an individual's freedom. Therefore, digital forensic practices are typically the most rigorous standard for working with digital devices.

1.2 | Digital Forensics is a type of cyber security!

Having established how Digital Forensics is defined, next, we consider where the field sits in relation to other disciplines. In 2019, a University of Bristol-led consortium published the Cyber Security Body of Knowledge (known as CyBOK). CyBOK "codifies the foundational knowledge in Cyber Security for education and professional training." The CyBOK document (Version 1.1.1) contains a widely recognized collection of the 21 knowledge areas within Cyber Security and the scope of knowledge within them. The document was primarily overseen by UK-based academics and practitioners across various Cyber Security and related domains. In Chapter 9, Digital Forensics is documented. The definition provided within the Digital Forensics chapter focuses on "legal proceedings" (Martin et al., 2019). CyBOK Digital Forensics focuses on the traditional criminal focus of the field. In the remainder of the CyBOK document, other areas relevant to our description of Digital Investigation, such as computer security, privacy, and incident response, are covered.

The CyBOK project has included over 115 expert contributions and was funded by the National Cyber Security Program. Given the breadth of expertise in compiling this resource, it is clear that considerable thought and research was put into establishing each knowledge area. Therefore, the authors of this paper feel it is established that Digital Forensics is a subdiscipline of Cyber Security.

1.3 | Digital Investigation

Having established Digital Forensics sits within the broader field of Cyber Security, a review of the other knowledge areas within CyBOK suggested a broader synergy with other skillsets. Therefore, the authors suggest that Digital Forensics itself is part of a broader investigative skillset. We propose that Digital Investigation is Digital Forensics applied to broader society. Digital Investigation uses Digital Forensic skills and techniques to assist with a more comprehensive range of investigation types. For this paper and our ongoing activity, we define the aim of Digital Investigation as "To investigate digital devices and their associated data to provide intelligence, information, or evidence relating to system or user activity." This definition enables a wider variety of tools and techniques to suit the constraints and requirements of the investigation type.

Digital Investigation is still the process of preserving, identifying, and extracting data from any digital device. However, each investigator can adapt techniques and procedures to suit multiple investigation needs. Therefore, it is an expanding sector encompassing Digital Forensics, incident response, e-discovery, intelligence, digital archaeology, and device security. A critical feature of the field is that the results have a direct, immediate impact on the world. The real-time nature of this critical work puts additional pressure on an already stretched system, increasing the possibility of life-changing mistakes.

2 | FIELDS OF INVESTIGATION

Section 1 briefly outlined our case for the term Digital Investigation to mean a broader use and interpretation of a traditional digital forensic skillset. The phrase demonstrates its application in a wider variety of circumstances. Based on this case, we believe any criteria for expertise should apply to the broader use of the skillset as far as possible. Therefore, this section considers where the skillset could be applied. This section aims to demonstrate the broad application of digital forensic skillsets and related career pathways.

Table 1 illustrates a range of industries interested in investigating digital devices. Although the table is not exhaustive, it provides insight into the areas where the skills and procedures utilized in Digital Forensics can be adapted to meet similar needs. Recent public case examples are provided for each industry to give more background.

Archivists and historians have a growing interest in investigating digital devices, with a predominant focus on recovering data from older devices. This usage is likely to snowball, given how embedded technology has become in western society over the last few decades. Indeed, historians in the future may need to do their Digital Investigations of digital research as a standard part of their research activities. Although the industries listed in Table 1 are not exhaustive; they show a range of areas which use the same essential skillset. The criminal investigation activities map naturally to corporate and civil investigations, as they are all “investigations”. Incident response, security, and intelligence generally use the skillset, tools, and artifact locations to retrieve intelligence at speed to move forward activity.

Similarly, Media and Public Interest investigations focus on retrieving focused intelligence for use in their activities. However, these investigations may not have the same levels of (legal) data access and time frames. As shown in the table, recent cases cited over the past 3 years highlight the current relevance of these areas.

3 | CHALLENGES, CHALLENGES, CHALLENGES

Having defined the field and associated use cases across various industries, the next step is to examine the industry's current challenges. By defining the challenges, it will be possible to identify where responsibility for each challenge lies, with the individual, the organization, or the industry.

TABLE 1 Selection of industries interested in investigating digital devices.

Industries	Example areas of interest	Recent public case example
Archivists/historians	Data recovery, data validation	(Huges, 2021)
Civil	Divorce, copyright	(Yaffe-Bellany, 2022)
Corporate	Accessing information, trade secrets, grievance procedures, misuse of corporate resources, disciplinary procedures	(Van Natta, 2022)
Criminal	Child abuse, fraud, drug activity, murder, sexual assault	(Australian Federal Police, 2022)
Incident response	Protecting digital infrastructure, analyzing privacy/vulnerabilities, investigating postincident	(Kunert, 2022)
Intelligence/security	Counterterrorism, national security, organized crime, international criminal activities	(McEwen, 2022)
Media	Verifying sources and critical evidence, open-source intelligence, enhancing sources, recovering metadata and deleted information, tracing activity	(Paton Walsh, 2020) (Izadi, 2022)
Private	Protecting individual privacy	(O'Flaherty, 2022)
Public interest	National events, celebrity activities	(Wise, 2022)

The field has fought constant challenges from its inception, with examiners continually investigating the unknown with limited staff, skills, and equipment. Despite the array of support at their fingertips today, the field faces endless backlogs, a lack of examiners, and ever-changing technology.

3.1 | Overload

Digital Investigations now feature in around 90% of criminal cases in law enforcement, and other sectors have rapidly increased their Digital Forensics capability. This requirement has created the most demand we have ever seen for Digital Forensics examiners and an excessive number of investigations to process. This universal utilization of digital evidence has resulted in most examiners being consistently overloaded with work, facing extreme pressures and tight deadlines. Overloading is a significant issue in many surveys of examiners (Fahdi et al., 2013). Constant overloading can create a high-stress environment and a higher likelihood of errors and has continually been a challenge in Digital Forensics. Where resources permit, the industry continually recruits to manage the backlog and improve staff well-being. However, it is challenging to find experienced professionals suitable for the role with constant competition from other areas with universal demand.

3.2 | Training, development, and education

With such a high volume of investigations, it is even more challenging for companies to release staff and for individual examiners to find the time for training and development. The increased workload has created an environment with limited opportunities to maintain core knowledge and develop new skills. The high workload can make it very challenging for examiners to devote time to keeping up with ever-changing and evolving technology. Such demands can be incredibly overwhelming for new examiners learning the field. As with time, money can also be reduced in some regions of Digital Investigation, which can seriously restrict the amount of training available to examiners.

However, both training and education are critical parts of an examiner's introduction and development in the Digital Investigation field. Because of this demand, there are many course offerings from companies, vendors, and academia. However, there are vast differences in the outputs for focus, quality, cost, coverage, and technicality. Therefore, it is hard to assess these courses' actual accomplishments (Siewert, 2015). This significant disparity, coupled with no standard level of education, has meant that examiners are entering or developing in the field with different skill sets and understanding. Although being different is not bad, it can be challenging to assess each examiner's level of experience and knowledge based on education alone.

3.3 | Shortage of examiners

Historically, criminal casework was the primary area that utilized the digital forensic skillset. Digital Forensics skills are now utilized across multiple industries, so examiners have a universal demand (Karie & Karume, 2017). This demand has meant more significant opportunities, different career pathways and progression for examiners. It is easier for examiners to transfer to other roles than stay in traditional law enforcement posts. The limited compensation has caused challenges with staff retention and loyalty in some companies. With some industries offering extensive work packages and incentives, it has become difficult for other industries to compete in some instances.

3.4 | Development of technology

Technology has vastly changed throughout the history of Digital Forensics, which is even more concerning when considering the relatively short time frame. We have hundreds of different electronic devices, numerous operating systems, and continuous updates that examiners are fighting against (Caviglione et al., 2017). The range of technology has often meant that examiners are researching between casework commitments and outsourcing work to specialist examiners at a premium.

This challenge is also heavily affected by some examiners' reliance on tools with heavy automation and interpretation. However, tool vendors must also tackle the battle of updates and introducing new technology. Although the vendors may have better capabilities to research and update their tools, it is often a significant period after the release. Leaving examiners to their research or interpretation of the changes in artifacts, which they may not have the experience to complete. Therefore, the value and validity of these new artifacts need to be evaluated by an experienced practitioner.

Although keeping up with new technology is one challenge, examiners must also retain knowledge and skills with legacy equipment due to their regularity in cases. This retention is particularly relevant for more contemporary practitioners who may not have experienced interacting with older devices. Given the difficulties for a skilled technical practitioner to keep up with device changes, it is worrying to note that we expect the same ability to identify devices from general crime scene investigators who are not technology experts.

3.5 | Mental well-being

The nature of Digital Forensics means content can be extreme. Regular and prolonged exposure to explicit and harmful content is likely to toll examiners' mental well-being and health (Seigfried-Spellar, 2017). Although employers are now taking steps to ensure that mental health is protected. It is often not identified as a challenge within the industry. Previous sections have highlighted the difficulties of finding time for research and professional development. Therefore, it has unintentionally become the responsibility of each examiner to fit in these activities, often in their own time. Individuals should not be required to dedicate their time outside work to critical continued professional development. The requirement to do so means that not all examiners will have or be willing to give up this time, adding to workplace stress and tension. Workplaces need to provide adequate staffing and support to enable staff to meet the needs of their job within their contracted working hours at a safe and mentally sustainable level.

4 | WELL, WHAT DO I NEED?

Having defined the current significant challenges in the field, the authors now set out their criteria to be an expert. The requirements were developed based on the field definition and practitioner use cases from their previous experience. The criteria developed and the rationale is provided below.

4.1 | Subject specific skills

Digital Forensics is traditionally considered the field of presenting evidence relating to digital devices for use in Legal proceedings. However, the skill set of a digital forensic examiner is vastly adaptable and applicable to a range of activities. Focusing on the core skill set, we can see several skills a typical digital forensic investigator has; at a high level, we believe these to be:

- Read and interpret binary information.
- Acquire data from static and in-transit locations.
- Identify and work with a variety of storage media, partition schemes, file systems, operating systems, and data structures.
- Perform experimental research to aid gaps in knowledge for investigations and verification of tools.
- Select artifacts relevant to an investigation.
- Contextualize artifacts with the broader activity of the device(s).
- Validate findings using a dual tool approach.
- Record and present findings of the investigation.

Within the skills listed above, it is noted that different examiners will have different focuses within the above. Some examiners new to the field may focus on single skills such as acquiring storage media. Other examiners may focus on a particular type of investigation or device types, such as terrorism and vehicle analysis. However, an experienced digital forensic investigator will have the experience and capability to work across all points concerning their role.

4.2 | Personal characteristics/traits

Alongside the technical skills from the previous section, examiners require key personal characteristics to succeed (Craiger et al., 2007). These personal characteristics support and enhance the examiner's technical skillsets and often define how they will apply themselves to their role. We believe these characteristics are:

4.2.1 | Problem-solving

When working in Digital Forensics, problem-solving is essential as every task, operation, or case drills down to a "whodunit" like scenario needing to be solved through digital evidence. Although you may not need Scooby-Doo and the gang, examiners must be inquisitive, desire to question the unknown and not expect repetitive tasks.

To solve problems effectively in the field, examiners need good attention to detail to spot the nuggets of gold and a level of independence to work effectively alone. Examiners also need to admit when they do not know or do not have the capability.

4.2.2 | Adaptable (mental agility)

Due to the dynamic nature of Digital Forensics, examiners must be adaptable and quickly learn and process new material or skills. To be effective, examiners need a willingness to learn new skills and maintain knowledge in line with technological developments. Managing the additional work often means that examiners will need to have the ability to work under pressure, especially with the tight turnaround and high workloads. With this in mind, being resilient is also a characteristic supporting trait.

4.2.3 | Ethical

Examiners are often faced with complex scenarios that may invoke some personal responses or feelings. Due to the stringent nature of the field, examiners must remain professional and display correct ethical behavior. Maintaining these characteristics will ensure that examiners remain impartial and maintain proper conduct.

4.2.4 | Team player

Throughout an investigation cycle, different individuals with varying responsibilities will be involved, meaning examiners must be willing to work as part of a wider team. Although individual tasks may be completed alone, examiners must be willing to work toward a common goal and discuss it appropriately with other team members. Remember just as UK ACPO Principle 4 (Association of Chief Police Officers, 2011); in short, within an investigation, the boss is the boss, all the glory but all the responsibility!

4.3 | Experience

Binary data have two states. Our definition is a black or white, true or false, 0 or 1 state. However, categorizing the experience of a human being is a far more complex and a gray area. We propose that experience consists of three areas, Track record, professional memberships, and education/training. Each area on its own does not represent an experienced individual. Therefore, we propose the unique combination of each investigator's three elements that should be judged as a combined "experience" indicator. A breakdown of each area is provided below.

4.3.1 | Casework track record

The history and types of cases may potentially look different in each industry; however, a track record of activity is a favorable reflection of an examiner's capability. A good quality examiner will have some casework history in the field. This track record actively demonstrates how they can practically employ and evaluate their knowledge and skills in applicable real-world scenarios. Their track record is usually a key indicator and ultimate proof of the difference between an examiner, a good examiner, and a great expert. It also forms great "war stories" to share with other examiners, which serve as educational anecdotes.

4.3.2 | Training and education

Digital Forensics examiners must continually adapt to technology, which means continued professional development typically includes further training and education. Alongside knowledge gain, this development can potentially help bolster an examiner's experience by giving them formal certification as proof of understanding. However, due to the ever-changing nature of Digital Forensics, the increased volume of providers and content has caused various concerns with training and education, which are explored further below.

When selecting a potential course, the quality and content coverage can often be challenging to assess, especially with many providers available. This variety is often cited as a consistent issue in Digital Forensics (Sommer, 2011). Whilst some organizations have responded to publicize the expected learning outcomes openly, others reveal little information. Therefore, trying to understand the benefit, the potential knowledge gained, or the level of understanding can be hard to establish for both the student, employers and opposing experts. Even if this information is available, the depth and level of technicality taught can massively vary between providers (Gupta et al., 2022). Meaning people are often left working off general opinions or views of the provider's quality and standing in the field to assess the benefit of a qualification.

Previously when education was limited, providers were often selected because they were the most popular or well-known providers. The assumption being their popularity meant that their offering was the best. However, with hundreds of new providers and rapid content growth have invoked a potential exploration of standardizing or accrediting education and training courses (Akhgar et al., 2014). By establishing some form of control and ensuring the quality of the outputs. In the United Kingdom, the most popular type currently seen in the field is the National Cyber Security Centre (NCSC) certification for degrees and training courses. Courses that are successful in gaining this are verified and competent in delivering the proposed training or education. However, certification is based on the accreditor's desired criteria, which will not always meet everyone's requirements. Certification may also be based solely on limited written documentation, which can only provide a limited picture. Therefore, certification should be used as additional evidence of actual qualifications.

Due to the Digital Forensics skillset being utilized in other industries, it is becoming increasingly difficult to secure and retain academic or training staff to deliver courses (Lang et al., 2014). This shortage can lead to organizations forcing the delivery of weak content while trading off esteem indicators such as accreditation, popularity and known individuals in the field to gain business. In cases with limited staff, there is increased physical and mental health pressure on the team to deliver, which harms their well-being. Organizations often do not understand the challenges of delivering an up-to-date Digital Forensic offering, which can add to difficulties in obtaining appropriate resourcing and support. The authors propose that practitioners be more vocal in supporting those delivering their CPD content. Practitioners need to aid teachers in making themselves heard within their organization to ensure they get the support they need. After all, both are part of the same delicate ecosystem and rely upon each other. An investigator's or organization's reputation can be easily damaged by one bad course or case, so identifying and supporting suitable training offerings is critical.

Although training and education are essential in Digital Forensics, it is crucial to recognize the variety of educational backgrounds in the field. Being such a dynamic industry, some examiners have entered the field through non-traditional routes (Schroeder, 2005). Therefore, investigators may not have any previous or related degrees in the area. So, an assessment of qualifications alone is not a fair judgment of an examiner's competency.

These issues have demonstrated why relying on just qualifications to establish an examiner's understanding or experience is not a fair assessment. A more collective approach to an examiner's history and background, that is, qualifications, experience, and case record, provides greater insight into an examiner's professional standing in the field.

TABLE 2 Review of available professional membership requirements.

Organization	Membership levels	Qualification req.	Experience req.	Interview	References	Background check	Notes
The Institute of Cyber Digital Investigation Professionals (ICDIP)	Junior practitioner, practitioner, senior practitioner			X			Membership calculated from a competency-based assessment
Chartered Institute of Information Security (CIISec)	Affiliate and student						Entry point
	Accredited affiliate						Requires passing approved examination, apprenticeship, or course
	Associate		2+ years				
	Full membership		5–10 years in an information security role				
	Fellowship						Requires a nomination by either a CIISec Board member, full or fellow member
Chartered Society of Forensic Sciences	Student	Current full-time student in forensic science					
	Affiliate						Open to all, initial step in professional membership
	Associate	Graduated or studying at a postgraduate level	Less than 3 years				
	Member	Forensic-related undergraduate or postgraduate degree National qualification Approved other qualifications	Over 3 years				

TABLE 2 (Continued)

Organization	Membership levels	Qualification req.	Experience req.	Interview	References	Background check	Notes
	Fellow	Recognized academic qualifications in forensic science	Extensive experience and recognition				Requires membership for 3 years prior
BCS Chartered Institute for IT	Student	Studying an IT-related course					
	Associate		1 year		X		Curriculum vitae required
	Professional	Relevant qualification	5 years				Accredited degrees do not require proof of experience
	Fellow						IT leader or role model
International Association of Computer Investigative Specialists (IACIS)	Full-time students						
	Associate member					X	Aspiring members of the Digital Forensics community
	Regular member		Current or former full-time law enforcement, government employee, or contractor				

4.3.3 | Professional memberships

As forensics has evolved, many organizations have formulated professional memberships, from overarching forensics and IT to specific Digital Forensics offerings (Zahadat, 2019). Each provides a method of recognition of an examiner's professional standing. Table 2 reviews professional memberships, highlighting the substantial variation in requirements and focus. It is noted that some favor competency and experience, while others regard qualifications as higher or equal to experience. This variation is demonstrated by some organizations requiring examinations or assessments to show an examiner's competency and knowledge. Others are highly focused on Curriculum vitae. Therefore, comparing and understanding the value or standard of each examiner's professional membership can be difficult without evaluating the professional body itself.

5 | SO, AM I AN EXPERT?

This expert commentary has explored the field of Digital Forensics and identified that the skillset is multipurpose. After defining the field, the paper has explored both the challenges in working in the field and the requirements that must be placed on an individual to demonstrate their expertise. This revelation has led the authors to conclude that Digital Forensics is part of a broader field within Cyber Security, which we name Digital Investigation.

The Cambridge English Dictionary defines an expert as “a person with a high level of knowledge or skill relating to a particular subject or activity”. Based on this definition, we propose that being an expert in every avenue of Digital Investigation at a single point in time is impossible. The field is now too broad and constantly changing to have an elevated level of knowledge in all areas. We propose that the expertise of a digital investigator changes over time. An investigator with the criteria outlined in Section 4 can adapt and become suitably expert in the area required for each investigation as the need arises. We also suggest that experts who meet these criteria know their limitations and capability. Therefore, they would endeavor to stay within activities they could demonstrate a justification and competence to perform.

Although theoretical knowledge is a vital criterion of any digital investigator's expertise, it is the experience of applying that knowledge to investigations genuinely separates the novice from the expert in this field. Having an academic understanding of artifacts and processes does not prepare an investigator for the realities of working on a case. Indeed, while well-meaning theoretical models often do not meet an examiner's needs. They are difficult to translate into working practices. The authors of this document are predominantly active practitioners, and there is an argument that this may bias their view of expertise. There is also the argument that with an average field experience of over 10 years, they have prolonged experience in the field as it has rapidly evolved. Based on this experience, the authors note that those without casework experience often initially struggle with the challenges outlined in this paper and find adjusting to the limited resources, immense pressure, and viewing harmful material particularly difficult. This realization often results in a high drop-out rate, including those who leave the field and move out of law enforcement to other Digital Investigation roles. Conversely, those who join the field with an investigative background often struggle with performing rigorous scientific research and being able to build solutions to emerging problems. This insight leads the examiners to conclude it is a mix of academic understanding with practitioner casework experience leading to a successful expert career.

To survive in a constantly evolving field, an investigator must continually strive to stay up to date, question whether the activity is still the most appropriate, and remain hands-on. Like evolution has led to species adapting, so must the digital investigator. Therefore, in answer to the question, are you an expert? The answer is “it depends.” You may be an expert today on vehicle infotainment and next month on smart doorbells.

AUTHOR CONTRIBUTIONS

Sarah Morris: Conceptualization (equal); investigation (equal); methodology (equal); writing – original draft (equal); writing – review and editing (equal). **Melissa Hadgkiss:** Conceptualization (equal); investigation (equal); methodology (equal); writing – original draft (equal); writing – review and editing (equal). **Anne David:** Investigation (equal); methodology (equal); writing – review and editing (equal). **John Guinness:** Investigation (equal); methodology (equal); writing – review and editing (equal). **Charles Frewin:** Investigation (equal); methodology (equal); writing – review and editing (equal).

FUNDING INFORMATION

No external funding was utilized.

CONFLICT OF INTEREST STATEMENT

The authors have declared no conflicts of interest for this article.

DATA AVAILABILITY STATEMENT

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

ORCID

Sarah Morris https://orcid.org/0000-0002-9482-6270

RELATED WIREs ARTICLES

Forming an investigative opinion in digital forensics

REFERENCES

Akhgar, B., Bosco, F., & Staniforth, A. (2014). *Cyber crime and cyber terrorism investigator's handbook* (pp. 91–100). Syngress.

Association of Chief Police Officers (Ed.). (2011). *ACPO good practice guide for digital evidence* (5th ed., p. 6). Association of Chief Police Officers. https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf

Australian Federal Police. (2022). Sydney man charged with possessing and transmitting child abuse material. *Australian Federal Police*. https://www.afp.gov.au/news-media/media-releases/sydney-man-charged-possessing-and-transmitting-child-abuse-material

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The future of digital forensics: Challenges and the road ahead. *IEEE Security & Privacy*, *15*(6), 12–17. https://doi.org/10.1109/MSP.2017.4251117

Craiger, P., Ponte, L., Whitcomb, C., Pollitt, M., & Eaglin, R. (2007). Master's degree in digital forensics. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. IEEE.

Fahdi, M., Clarke, N., & Furnell, M. (2013). Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In *2013 Information Security for South Africa* (pp. 1–8). IEEE. https://doi.org/10.1109/ISSA.2013.6641058

Farid, H. (2018). Digital Forensics in a post-truth age. *Forensic Science International*, *289*, 268–269.

Gupta, K., Neyaz, A., Shashidhar, N., & Varol, C. (2022). Digital forensics lab design: A framework. In *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE.

House of Lords. (2019). Forensic science and the criminal justice system: a blueprint for change. HL Paper 333.

Huges, M. (2021). Retro collectors are uncovering hoards of old data. *WIRED UK*. https://www.wired.co.uk/article/vintage-computers-data

Izadi, E. (2022). This is how journalists figure out if all those Ukraine videos are real. https://www.washingtonpost.com/media/2022/03/02/ukraine-visual-forensics/

Karie, N., & Karume, S. (2017). Digital forensic readiness in organisations: Issues and challenges. *The Journal of Digital Forensics, Security and Law*, *12*, 48.

Kunert, P. (2022). Aon confirms it is investigating "cyber incident." *Theregister.com*. https://www.theregister.com/2022/03/01/aon_cyber_incident/

Lang, A., Bashir, M., Campbell, R., & DeStefano, L. (2014). Developing a new digital forensics curriculum. *Digital Investigation*, *11*, S76–S84.

Martin, A., Rashid, A., Chivers, H., Danezis, G., Schneider, S., & Lupu, E. (2019). *Introduction to CyBOK* (1st ed., pp. 290–300). The National Cyber Security Centre. https://www.cybok.org/media/downloads/Introduction_to_CyBOK.pdf

McEwen, A. (2022). Computer found in room of scots terror plan accused "held 1000s of hate images." *Daily Record*. https://www.dailyrecord.co.uk/news/scottish-news/computer-found-bedroom-scots-terror-25216152

O'Flaherty, K. (2022). The data game: What Amazon knows about you and how to stop it. *The Guardian*. https://www.theguardian.com/technology/2022/feb/27/the-data-game-what-amazon-knows-about-you-and-how-to-stop-it

Paton Walsh, N. (2020). Leaked documents reveal China's mishandling of the early stages of Covid-19 pandemic. *CNN*. https://edition.cnn.com/2020/11/30/asia/wuhan-china-covid-intl/index.html

Schroeder, S. (2005). How to be a digital forensic expert witness. In *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)* (pp. 69–85). IEEE. https://doi.org/10.1109/SADFE.2005.18

Seigfried-Spellar, K. (2017). Assessing the psychological well-being and coping mechanisms of law enforcement investigators vs. digital forensic examiners of child pornography investigations. *Journal of Police and Criminal Psychology*, *33*(3), 215–226.

Siewert, P. (2015). Certifications vs. experience. *Prodigital4n6.blogspot.com*. http://prodigital4n6.blogspot.com/2015/01/normal-0-false-false-false-en-us-x-none_41.html

Slay, J., Lin, Y., Turnbull, B., Beckett, J., & Lin, P. (2009). Towards a formalisation of digital forensics. *Advances in Digital Forensics V*, *306*, 37–47.

Sommer, P. (2011). Certification, registration and assessment of digital forensic experts: The UK experience. *Digital Investigation*, *8*(2), 98–105.

Van Natta, D. (2022). Cowboys paid $2.4M over cheerleader allegations. *ESPN.com*. https://www.espn.com/nfl/story/_/id/33231841/dallas-cowboys-paid-24-million-settle-cheerleaders-voyeurism-allegations

Wise, J. (2022). The DIY intelligence analysts feasting on Ukraine. *Intelligencer*. https://nymag.com/intelligencer/2022/03/the-osint-analysts-feasting-on-ukraine.html

Yaffe-Bellany, D. (2022). Remains of the day: Custody battles move on from kids and house to crypto. *dtNext.in*. https://www.dtnext.in/News/Business/2022/02/16002426/1343878/Remains-of-the-day-Custody-battles-move-on-from-kids-.vpf

Zahadat, N. (2019). Digital forensics, a need for credentials and standards. *The Journal of Digital Forensics, Security and Law*, *14*, 4–6.

How to cite this article: Morris, S., Hadgkiss, M., David, A., Guinness, J., & Frewin, C. (2023). We're making a list and we're checking it twice, gonna find out what makes digital forensic examiners suffice. *WIREs Forensic Science*, *5*(5), e1487. https://doi.org/10.1002/wfs2.1487