Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
The risks for digital evidence

After the discussion of quality assurance in digital evidence, the question of the future naturally follows. Some leaders in the field have made the disturbing observation that the overall quality of digital forensic examination is declining, and the comprehension of cybercrime is diminishing. This reliable observation appears to be in conflict with the simultaneous improvement in the general public’s knowledge of technology and its attendant utility irrespective of the level of economic development. Further, such a decline is occurring at a time when all communities are becoming more dependent on technology and therefore individuals are generating more digital traces representing the thoughts, behaviours and actions that might be used in evidence in any proceedings. This decline is a great concern as the consequences of errors and omissions in forensic science result in miscarriages of justice, and dangerous criminals will continue to be at large to perpetrate further crimes against persons and organisations [1]. The public rightfully expects that its justice system will continuously improve in meeting the needs of the community and to have confidence in the evidence that might be presented.

The increasing quantity, diversity, diffusion, structural intricacy and complexity in the use of data, sometimes referred to as the oil of the 21st century, make it increasingly difficult for the digital forensic examiner to find the most investigatively useful information. Attorneys and judges are struggling to learn how to evaluate and interpret digital forensic results and the intimate and detailed nature of digital traces raises privacy concerns that must be considered in all stages of the data preservation, examination and reporting processes.

The situation is further compounded by competing demands to follow methodical, scientific practices and to respond in shorter time frames yet deal with the dual challenges of growth in cybercrime and the increasing volume of data in the lake. In addition, organisations and first responders are increasing their demand for decentralised forensic capabilities (e.g. at the crime scene) and for correlation capabilities to identify emerging trends and seriality. The calls on digital evidence are multiple and complex.

In its early history, digital forensic practitioners considered the data from devices as fact-based evidence with little consideration given to evaluation of alternative interpretations. This approach still persists today to a significant degree with the effect of denying the scientific basis to the field. To this day, there is still a significant volume of debate about what aspects of digital forensics are or are not science and some forensic science publications still do not recognise digital forensics as a forensic discipline.

The risks in digital forensics are adequately addressed as technical and interpretive errors which, therefore, continue to be ongoing challenges. Practitioners generally have an inadequate understanding of the operation of hardware and software that leads to a flawed interpretation of the analysis of data. Consequently, practitioners rely heavily on tools to process data without due regard to the limitations and inherent errors within the tools. The inadequate understanding of practitioners resulting in the
consequent overreliance on commercial tools and vendor training is exacerbated by the highly dynamic technical and operational environments of rapidly evolving technology and the increased prevalence of digital technology used in the conduct of criminal activity. There are numerous cases where incorrect conclusions, false accusations and misinterpretation of data have led to poor investigational and court outcomes.

Treating the field as fact based, rather than a scientific discipline, is useful in certain circumstances. It is useful when the data are to be used as information to assist in investigations, including developing the investigation hypothesis and subsequent fact checking. It is also useful to locate additional data sources or to find potential suspects or victims. Given that digital traces can be altered or parsed incorrectly by the tools and digital forensic results can be open to interpretation and, therefore, misinterpretation, the assumption that digital forensics is based on fact is dangerous, especially when used as evidence rather than investigative information or for intelligence. Some courts have recognised that digital forensics is not fact-based evidence and have questioned the validity of digital forensic reports due to the absence of demonstrable scientific validity in the analytical process.

The future risks to digital forensics arise in several areas including, but not limited to:

- Application to many contexts including investigations, military, critical infrastructure protection and intelligence operations, with each context treating digital evidence differently and developing context-specific standard procedures. To transfer knowledge and processes from one context to another, for example, from an intelligence purpose to a criminal investigation purpose, without due consideration can lead to a flawed interpretation of findings.
- Decentralisation, including the deployment of advanced digital forensic techniques by persons with limited knowledge, can result in errors and the lost opportunities for broader visibility across the crime environment and to compare multiple crimes. Forensic intelligence is a function of forensic science that is becoming increasingly favoured by many organisations, with some excellent results being realised. Digital forensics lends itself very well to a forensic intelligence function, but if examinations are being conducted in a decentralised environment, it is unlikely that the data will be captured in the consolidated repository and merged with other forensic information, therefore it will be unavailable to fulfil the intelligence function.
- Dynamism of the field with new technology and devices, such as the Internet of Things, outpaces the scientists’ ability to understand the new technology that they are likely to encounter in case work.
- Growth in case and data volumes continues at massive rates that greatly outstrips the capacity of organisations to manage and to adjust. For most organisations, the ability to purchase digital forensics tools and equipment is compromised as it is often referred to as ‘computer equipment’ or similar and is therefore subject to organisation- or government-wide procurement policies, including approval by the IT manager. The requirement to follow such processes compromises the ability of digital forensic teams to respond to emerging issues and can comprise the selection of best fit for purpose.
- Knowledge management and information sharing within the digital forensics community and between groups within the justice system and only sporadically applied within forensic organisations.
The risks for digital evidence

- Poor quality management with many of the processes used in digital forensics occurring outside of a quality framework that increases the risk of errors and omissions.
- Privacy is, rightly, becoming an increasing concern. Governments and businesses can access huge amounts of personal and private data, but the tension between privacy and digital forensics is complex. Recent examples include the ongoing tension between the US Department of Justice, who seeks a ‘backdoor’ to Apple’s iPhone encryption while Apple seeks to maintain a secure device for its users; and, the promotion of tracking and contact apps by the governments of several countries as a part of their response to COVID-19, but concern by citizens that it is a movement towards a permanent state of surveillance. Ignoring privacy concerns of the community at large may result in the limitation of utility of digital evidence through the means of regulation and legislation.

Some steps are being taken to address the risks. The United States Scientific Working Group on Digital Evidence (SWGDE) has developed an error mitigation approach that will identify each potential source of error encompassing technology and human factors. There is some overlap with ISO 17020 and ISO 17025 that are used for the basis of forensic accreditation. It is important to emphasise that error mitigation analysis involves testing and validation of digital forensic tools, but it does not deal with the evaluation of evidence and mitigation of bias.

Work is being undertaken to harmonise forensic science and digital forensics. The Digital Media Scientific Area Committee (of the National Institute of Standards and Technology, Organisation of Scientific Area Committees) has developed a forensic science framework for digital traces with a view to it being applied to other disciplines. The framework is based on scientific reasoning that addresses defined questions of authentication, identification, classification, reconstruction and evaluation in a broad range of legal contexts.

To mitigate the risk created by the potential loss of knowledge in digital forensics, knowledge management strategies can be implemented:

- The scope of forensic examination can be determined by the purpose to which it is being applied and then conducted to the extent that is appropriate for that purpose. Generally speaking, there are three tiers of forensic examination that are applied (triage, preliminary examination and in-depth examination) in practice which will indicate the extent of resources that are to be directed to the task at hand.
- Digital forensic knowledge can be codified in automated solutions.
- The digital forensic community can construct a collaborative knowledge exchange including multidisciplinary conferences and structured knowledge management systems (such as instructional documents and videos).
- Organisations can designate forensic advisors, who specialise in digital forensics, to liaise with and guide investigators and to provide appropriate contextual information for examiners.
- Forensic intelligence teams that specialise in digital forensics.
- Interoperability and automation, for example, the ability to combine the results of multiple tools that are used to extract information from all data sources will significantly improve the efficiency and effectiveness of an investigation and facilitate verification and the sharing of information.
Several initiatives are under development in multiple organisations including the support of forensic intelligence capabilities. Organisations will continue to be challenged as some of the developments in digital forensic capabilities are progressing at a pace that far exceeds that at which forensic science can adapt [1].

Reference

[1] E. Casey, The chequered past and risky future of digital forensics, Aust. J. Forensic Sci. 51 (6) (2019) 649–664.