Forensic Science International 316 (2020) 110486

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

Digital transformation risk management in forensic science laboratories

Eoghan Casey[*], Thomas R. Souvignet

School of Criminal Sciences, Faculty of Law, Criminal Justice and Public Administration Batochime, University of Lausanne, Switzerland

ARTICLE INFO

Article history:
Available online 3 September 2020

Keywords:
Forensic science
Digital transformations
Forensic laboratories
Forensic preparedness
Forensic digital preparedness
Risk management
ISO/IEC 17025

ABSTRACT

Technological advances are changing how forensic laboratories operate in all forensic disciplines, not only digital. Computers support workflow management, enable evidence analysis (physical and digital), and new technology enables previously unavailable forensic capabilities. Used properly, the integration of digital systems supports greater efficiency and reproducibility, and drives digital transformation of forensic laboratories. However, without the necessary preparations, these digital transformations can undermine the core principles and processes of forensic laboratories. Pertinent examples of problems involving technology that have occurred in laboratories are provided, along with opportunities and risk mitigation strategies, based on the authors' experiences. Forensic preparedness concentrating on digital data reduces the cost and operational disruption of responding to various kinds of problems, including misplaced exhibits, allegations of employee misconduct, disclosure requirements, and information security breaches. This work presents recommendations to help forensic laboratories prepare for and manage these risks, to use technology effectively, and ultimately strengthen forensic science. The importance of involving digital forensic expertise in risk management of digital transformations in laboratories is emphasized. Forensic laboratories that do not adopt forensic digital preparedness will produce results based on digital data and processes that cannot be verified independently, leaving them vulnerable to challenge. The recommendations in this work could enhance international standards such as ISO/IEC 17025 used to assess and accredit laboratories.

1. Introduction

Forensic science laboratories are becoming more reliant on computers and data for both administrative and analytical operations. These technological advances create new opportunities and risks for all forensic disciplines, not only to digital evidence [1]. With proper preparation and management, forensic laboratories can employ technology effectively to improve performance and quality, while mitigating the associated risks. However, many forensic laboratories do not understand the subtlety and expertise required to manage risks of digital transformation, inadvisedly treating it as simply a technical component of existing quality management processes. Forensic laboratories that fail to realise the need for forensic digital preparedness to actively manage risks associated with digital transformations are vulnerable to significant expense, disruption and liability when problems arise.

Forensic laboratories rely on technology for much more than communication and routine business functions. Sophisticated equipment for processing chemical and biological materials are operated using computers and save results in digital form. Mass spectrometers, DNA analysis systems, and other laboratory equipment save their results in raw data files. Digital evidence is processed using specialized hardware and software, although not all forensic laboratories have integrated this new discipline. Forensic laboratories are using computerized case management systems for tracking treatment of all evidential exhibits and forensic results. Automated systems with artificial intelligence are being used to support forensic analysis. In reality, digital transformations are well underway, and forensic laboratories require a robust strategy to manage the associated risks and realize the opportunities.

`Digital Transformations` – utilizing digital technology to make existing processes more efficient and effective, and to develop new solutions to emerging problems.

[*] Corresponding author.
E-mail addresses: eoghan.casey@unil.ch (E. Casey), thomas.souvignet@unil.ch (T.R. Souvignet).

http://dx.doi.org/10.1016/j.forsciint.2020.110486

This increased dependence on digital technology creates risks and opportunities for forensic laboratories. Potential pitfalls include loss of data needed to perform forensic analysis, errors in analysis of physical traces (e.g., DNA, fingerprint, face) caused by computer hardware or software, ability to tamper with raw data files generated by laboratory equipment, and incorrect information input into laboratory information management systems (LIMS). Possible benefits are traceability and integrity of traces, reliability and reproducibility of results from information extracted from traces and stored as raw data, and use of artificial intelligence to support forensic analysis.

Lessons can be learned from the digital forensic domain, including forensic digital preparedness and accreditation challenges. Primary challenges encountered by digital forensic laboratories adopting quality standards include [2]:

- Inaccurate or insufficient information in technical records, including chain of custody, and no mechanism to detect subsequent changes to records.
- Problems with the security of information technology systems and the backup processes of data.
- Missing or insufficiently detailed procedures for treating digital data, and personnel not following documented procedures consistently.
- Lack of robust quality checking mechanisms, and issues with validation of methods.

This paper presents risks and opportunities associated with digital transformation of forensic laboratories, providing examples based on the authors' experiences. Examples have been anonymized, as the intention is to illustrate general lessons learned rather than critique specific laboratories. This work then presents forensic digital preparedness, a set of recommendations to help laboratories navigate risks associated with digital transformations, including mishandled exhibits, allegations of employee misconduct, and disclosure requirements. The role of digital forensic capabilities and expertise in risk management of digital transformations in laboratories is discussed. This work culminates with broader implications for international standards used to assess and accredit laboratories such as ISO/IEC 17025.

2. Risks and remedies

Many processes in forensic laboratories have become digitalized, including information management systems and software running analysis equipment. These systems serve crucial functions in modern forensic laboratories, but have associated risks that must be managed.

2.1. Data retention

The computer systems used to store the generated data files (raw and processed) can encounter problems that lead to loss of information.

Data Loss

A forensic laboratory performed DNA analysis of a crime scene sample relevant to a multiple homicide and death penalty case, but did not retain a copy of the raw data files. To comply with a court order to provide the defense with original raw data, it was necessary to perform costly forensic data recovery on the computer used to perform the original processing of DNA. A customized software utility was created to automatically search the computer hard drive for all fragments of the relevant raw data and reconstruct the original files. The resulting files were tested and validated with DNA analysis software. [3]

Under certain circumstances, the original data files can be recovered from hard disks using digital forensic methods, which can be costly and time-consuming. Even when digital data is retained, it is malleable and subject to undetected alterations of content or metadata. Lack of proper data retention processes makes it more difficult, sometimes impossible, to recover original data files and verify their integrity.

Generally, normal backup processes do not have the fidelity of digital forensic preservation mechanisms. To manage the risks of data loss and undetected alterations, traditional data retention practices in forensic laboratories can be updated to employ digital forensic preservation methods. Specifically, as part of routine data retention processes, digital forensic preservation of original data (raw and processed) and associated metadata (filesystem timestamps) allows the integrity of data to be verified more easily when there is a problem or inquiry. For instance, original files and associated metadata can be forensically preserved using the Advanced Forensic Format (AFF4) which is open source and cross platform. The following command and output demonstrates how this method can be implemented on any type of computer system with a single command that can be part of a routine or automated process to forensically preserve all raw data files in a specified directory on a laboratory computer and generate a unique identifier for the digital evidence container for evidence management purposes [4,5].

```
  % aff4.py -cr s1-001-10April2020.aff4 RAWdata/s1-
001
  Creating AFF4Container: file://s1-001-10April2020.
aff4
  <aff4://c293153c-a317-4927-b1eb-6e3a5008ad0f>
  Adding: RAWdata
  Adding: RAWdata/s1-001/s1-001-sequence.sld
  Adding: RAWdata/s1-001/s1-001-processed.pdf
  Adding: RAWdata/s1-001/s1-001-ref.params
  Adding: RAWdata/s1-001/s1-001.RAW
```

This digital forensic preservation process captures file system metadata and automatically computes MD5 and SHA1 cryptographic hash values of the acquired data for integrity verification purposes as the following excerpt shows. These hash values are commonly used in digital forensic tools to enable future verification that the acquired data have not been altered since they were forensically preserved. The preserved metadata can also be useful for assessing the authenticity of the acquired data, including the original file name, size and creation timestamp.

```
  % aff4.py -m s1-000-10April2020.aff4
  ... EDITED FOR BREVITY...
  <aff4://c293153c-a317-4927-b1eb-6e3a5008ad0f/
RAWdata/s1-001/s1-000.RAW>
  a aff4:FileImage,
  aff4:Image,
  aff4:ImageStream;
  aff4:birthTime       “2020-04-10T22:41:03.949269
+02:00”^x̂sd:dateTime;
  aff4:hash     “1d2f7ff1ea563ceb6d2da0e168e90587-
”^flaff4:MD5,
  “427bc17e608fc493f0e2b3fed8fa55-
b36862ac31”^flaff4:SHA1;
  aff4:lastAccessed    “2020-04-10T22:41:08.708498
+02:00”^x̂sd:dateTime;
  aff4:lastWritten     “2020-04-10T22:41:05.290019
+02:00”^x̂sd:dateTime;
  aff4:originalFileName    “RAWdata/s1-001/s1-000.
RAW”^x̂sd:string;
  aff4:recordChanged   “2020-04-10T22:41:07.694584
+02:00”^x̂sd:dateTime;
  aff4:size 276196936.
```

In addition, AFF4 assigns a unique identifier to the acquired data to support evidence management and provenance tracking.

2.2. Evidence integrity

The data files generated by laboratory equipment and stored on computers can be altered afterwards accidentally or intentionally.

Data Alteration

To conceal specific information in test results, data files stored on laboratory computers were altered. Some alterations were detectable within the digital file, while others were not detected using available verification software. As a result, it was difficult to determine the full scope and specific impact of the alterations.

The motivation for editing data files (raw and processed) might be to cover up mistakes, conceal unfavorable results (corruption), facilitate prosecution (bias), or inflate laboratory metrics (performance) [6]. Forensic laboratory personnel might modify data to remove traces of contamination they considered to be insignificant, such as traces of investigators operating an evidential smartphone after the device was seized. Depending on the type of data and the method of modification, it might be possible to detect the alteration. However, some alterations may be undetectable using existing verification tools, making it more difficult to determine that modifications were made.

Normal backup processes, and even digital forensic preservation such as described in the previous section using AFF4, are not tamperproof because data can be forged to replace retained data, and a computer system can be backdated to make it seem to have occurred sometime in the past. Lack of a tamperproof chain of custody of primary data sources in a forensic laboratory makes it more difficult, sometimes impossible, to authenticate original data files that form the basis of forensic findings and reported results.

To manage the risks of inadvertent alteration and intentional tampering, traditional provenance tracking practices in forensic laboratories must be updated to employ digitalized chain of custody ledger solutions [7,8]. These digitalized chain of custody mechanisms can be implemented in a way that is tamperproof and independently verifiable.

2.3. Digital traceability

Forensic laboratories are increasingly using a laboratory information management system (LIMS) to record information about the full lifecycle of evidence in a forensic laboratory including submission, chain of custody, and results. A typical LIMS uses databases to store and organize information about each item of evidence at different stages of its treatment in the laboratory.

A LIMS is invaluable for keeping track of the growing amount of evidence and associated processes and results in forensic laboratories. As a result, such systems are considered essential for laboratory accreditation under standards such as ISO/IEC 17025. However, these systems can have weaknesses, including data entry errors, programming bugs, and system administrator bypass of access controls.

LIMS Weaknesses

Results of drug tests were routinely recorded in a LIMS, and normal users of the system could only create new records and view existing records. However, a system administrator was able to alter records using his higher level access, bypassing the security control mechanisms of a LIMS. The LIMS maintained an audit log of all normal user activities, but did not log system administration level actions.

To manage these risks of undetected or unattributed alterations to LIMS data, it is necessary to require unique user accounts for all actions and to maintain detailed electronic audit logs. These audit logs must include including successful actions, not only failed or blocked actions. Specifically, all transactions must be recorded (additions, alterations, deletions), and all computer system usage, such as logons and executed commands. In particular, system administrator accounts should be strictly protected (e.g., two-factor authentication) and monitored (e.g., sudo logging and process accounting). All audit logs must be preserved in a forensically sound manner in anticipation of their use as digital evidence in a legal matter. Applying digital forensic preservation and digitalized chain of custody on logs generated by LIMS and supporting computer systems can be an efficient way to enhance LIMS traceability.

2.4. Computer system malfunction

Forensic laboratories increasingly depend on computers to operate equipment for extracting information from biological and chemical samples (Fig. 1).

The computer systems used to operate laboratory equipment can malfunction, introducing errors in forensic analysis.

Hardware Issues

Unbeknownst to administrators, a few DNA analysis systems in a forensic laboratory were operated by computers with slightly different hardware than the standard configuration. This seemingly minor difference caused read errors which resulted in erroneous reference data being accessed on the DNA analysis systems. As a result, incorrect reference data were used in some cases, and the forensic analysis had to be repeated. This demonstrates that a seemingly unrelated problem with computer used to operate equipment for performing laboratory processes can cause incorrect results.

This example demonstrates that seemingly minor changes to underlying computer systems can interfere with traditional forensic processes. Although validation of computer systems can be covered under existing laboratory management processes, the subtleties of computer hardware and software configurations and interactions must not be underestimated.

2.5. Automation complexity and pitfalls

In forensic contexts, use of automated systems, including those with artificial intelligence (AI) and machine learning (ML), support

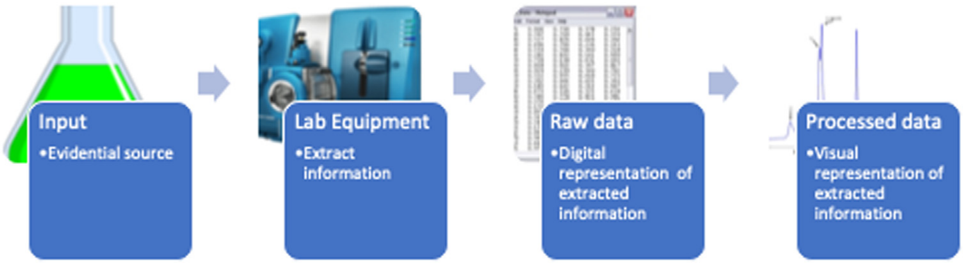
Input
•Evidential source
Lab Equipment
•Extract information
Raw data
•Digital representation of extracted information
Processed data
•Visual representation of extracted information

Fig. 1. Generalized depiction of laboratory equipment creating digital output.

analysis performed by human specialists who interpret the results. Although such automation can help maintain consistency and increase efficiency in forensic analysis, there are several major limitations that must be guarded against. Automated systems can have bugs that produce incorrect results, which can have serious consequences in a forensic context [9]. In addition, automated AI/ML systems can introduce bias due to poorly selected training datasets, and can lead to misinterpretations when the results are not fully understood [10]. When automated AI/ML systems are used to support investigation and forensic analysis, such as comparison of faces in digital video or photographs, algorithmic false positives can lead to incorrect results.

Concerns about Reliability and Human Rights

An independent study of six facial recognition technology test deployments performed by the London Metropolitan Police Service (MPS) found a high number of false positives. In total, only eight out of 46 automatically generated potential face recognition “matches” that were considered and evaluated by a human were deemed to be correct. The eight verified correct matches were determined by some form of confirmation such as through a street-based identity check [11]. The study paid particular attention to the risks of such technology interfering with fundamental human rights, including privacy violations and discrimination due to algorithmic bias relating to sex, race, or ethnicity.

Any automated system can have some false positives and false negatives, which demands that human analysts are in the loop to manage the risks of something important being overlooked or misinterpreted. Good practice here can also help deal with the risk of contextual bias. An automated system supporting forensic analysis should offer sequential unmasking capabilities [12].

Ultimately, automated systems supporting forensic analysis should integrate forensic requirements, risk management and privacy, i.e., forensic-by-design.

`Forensic-by-design` – integrating forensic preparedness principles and practices into the system engineering lifecycle, including risk management, incident handling, forensic principles and legal compliance [13].

However, such forensic-by-design is not common practice at the moment and there are growing concerns about the unreliability and invasiveness of such technologies for criminal investigation purposes. Some cities in California are strictly controlling the acquisition and utilization of *any electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group [14]*.

Forensic laboratories must be prepared to address concerns about reliability, privacy and discrimination associated with use of technology for processing data, particularly AI/ML systems for data analysis.

3. Digital reinforcement of forensic science principles

Core principles and processes in forensic laboratories can be bolstered using technology while increasing the efficiency and quality of services. These core principles include authenticity and integrity, reliability and reproducibility, quality and efficiency. In addition, intelligent application of digital technology can create new opportunities to deal with crime in digitalized society.

3.1. Authenticity and integrity

Digital transformation of forensic laboratories can enhance the traceability of traces. Existing computerized systems for processing physical and digital evidence typically provide a digital audit trail and its treatment throughout its lifecycle in the forensic laboratory. Alterations to data files (raw and processed) might be detectable using the digital traces that are created routinely during the processing of exhibits in a forensic laboratory. In some situations, to authenticate data files and associated results, it is necessary to perform contextual analysis, including digital forensic analysis of the original data and metadata.

Contextual Reconstruction

Questions arose about the results of some samples processed by a laboratory. In order to assess the reported results, the raw data was recovered from analysis systems along with processed results. The information from these files was compared with details recorded in the LIMS system, and discrepancies were found. However, audit logs in the LIMS system were found that corresponded with the original data. Timestamps of the original data files and the LIMS system were also examined to determine contemporaneous activities versus later changes.

It is advisable not to leave evidence authentication to chance. With properly protected audit trail and data file integrity mechanisms (preferably automated), a digitalized chain of custody can be maintained from intake to return or archival, providing valuable insights into laboratory operations and helping protect against undetected mistakes and forensic fraud. Some forensic laboratories have adopted bar code scanning and RFID labels to mark and track exhibits throughout their lifecycle. Some forensic laboratories use secure storage to retain raw data files. Some laboratories are developing enhanced methods for maintaining provenance information using blockchain-based systems [7,8].

With such automated provenance tracking mechanisms in place, every deliverable that a forensic laboratory produces could include the associated electronic chain of custody details as an appendix to demonstrate proper handling. Providing this provenance information in a standardized format such as CASE[1] enables receiving organizations to integrate the information into their information management systems and detect potential inconsistencies more easily, and even automatically.

3.2. Reliability and reproducibility

Forensic science practices demand that the data, methods, tools and analysis are described in sufficient detail that they can be carried out again with the same results.

Digital transformations can support reproducibility of processing by documenting all phases of the evidence lifecycle in the forensic laboratory, as well as reproducibility of analysis by providing others with original data to perform independent analysis. Some software developers also provide a standalone application for viewing the results of forensic processes, enabling others to verify forensic analysis without requiring them to purchase licenses for the specific software and/or version.

Reproducibility of Forensic Analysis

In an investigation involving various computers and mobile devices, multiple parties needed to perform an in-depth review of the results produced by a forensic laboratory. To save cost and time, the forensic laboratory provided the multiple parties with a complete package of data and viewing software necessary to perform in-depth review. Using this approach, all parties could assess the reliability of the evidence and results without having to purchase specialized equipment and software, or to run time consuming data processing operations that had already been performed by the laboratory.

The expanding decentralisation of forensic capabilities is driving the need for data and analysis results to be transferred securely between systems and organisations that is fully traceable,

[1] https://caseontology.org.

if not completely repeatable. This trend raises the importance of international standards for harmonization of forensic methods and data formats.

3.3. Quality and efficiency

Technological advances enable forensic laboratories to process evidence more quickly while maintaining quality. Forensic laboratories can manage the systems that they rely on for processing evidence in order to standardize the processing and output. The National Institute of Standards and Technology (NIST) Computer Forensic Tool Testing (CFTT) program publishes open access test reports for software commonly used in digital forensic laboratories, detailing both capabilities and limitations. The European Network of Forensic Science Institutes (ENFSI) and the US DoD Cyber Crime Center (DC3) also perform tool validation and testing, and provide the results to law enforcement agencies. Similar validation and testing should be applied to computers and software used to operate traditional forensic equipment. As discussed in Section 2.4, such validation must be alert for seemingly insignificant changes that can create major errors in traditional forensic processes. Furthermore, the validation of AI/ML based software is an important and complex undertaking that must be performed by an independent entity or consortium. This level of control helps improve the consistency and quality of results from forensic laboratory processes.

Validation and Change Control

A forensic laboratory routinely validated and tested equipment, and maintained strict change control procedures for computers used to process evidence. Every aspect of the systems was covered, including the specific hardware, firmware, and software versions. Validation of the forensic processes was performed on the specific systems, and any issues could be recognized and dealt with before causing further problems.

3.4. Forensic-by-design automation

Forensic laboratories are developing new automated systems, including those with AI/ML capabilities, to analyze data and to gain understanding of crime in ways that were previously not feasible [15,10].

Forensic Artificial Intelligence

Electronic portable devices, based on near-infrared spectroscopy and supported by machine learning, have been developed to test drugs rapidly. These devices could be useful for producing a full profile of the substance tested in the field and transfer the data to a computerized repository in the laboratory for further analysis [16]. Such a repository could be useful for tracking drug trends in a region, and quickly detecting a problem such as an epidemic.

The value of forensic laboratories can be extended to more proactive intelligence-led approaches based on knowledge extracted from repetitions found in crime [15]. To manage the associated risks, systems supporting such intelligence-based solutions should be forensic-by-design, abiding by forensic principles and human rights, including privacy and nondiscrimination. Forensic-by-design includes traceability, encryption, and impossibility even for system administrators to access private information.

4. Digital transformation risk management

This section describes the recommendations in Table 1 for managing risks of digital transformation of forensic laboratories. Forensic laboratories need to prepare for matters such as lost evidence, being audited or investigated, and responding to civil lawsuits. In the digital forensic domain, the practice of forensic preparedness has been developed to manage risks associated with computer use and misuse.

`Forensic preparedness` – involves specification of a policy that lays down a consistent approach, detailed planning against typical (and actual) audit or investigative scenarios that an organisation faces, identification of (internal or external) resources that can be deployed as part of those plans, identification of where and how the associated digital evidence can be gathered that will support investigation and a process of continuous improvement that learns from experience [17].

Lack of forensic preparedness increases the risks of problems going undetected and of ineffective response after a problem is detected. A reactive approach is costly and disruptive, including the need to find and retain external digital forensic expertise. Forensic preparedness enhances business continuity and contingency planning, putting organizations in a better position to detect and investigate problems and manage the associated risks [18,19]. These issues and remedies apply equally to all forensic laboratories, including those within private enterprises.

It is important to note that this road-map does not cover of cyberattacks, which require additional digital forensic preparations such as incident response procedures and expertise.

4.1. Curated digital information

A fundamental aspects of being prepared from a digital forensic perspective is knowing where key data sources are located, and ensuring that they contain the minimum data necessary to support business needs and meet legal requirements.

The purpose of curating digital information is to reduce the amount of time required to access and examine relevant data, thus

Table 1
Road-map for digital transformation risk management.

Risk	Recommendation	Sect
Not knowing what data exist	Develop a digital evidence map documenting where needed data, logs and provenance details are located and how they will be preserved in a forensic manner.	4.1
Not having a plan	Institute policies and procedures that govern the roles, responsibilities and expected actions during an inquiry.	4.2
Missing data and metadata	Implement an automated digital forensic preservation process of primary data sources.	4.3
Lack of traceability	Maintain and forensically preserve detailed electronic audit logs of all computer system usage and database transactions.	4.4
Lack of data integrity	Tamperproof digitalized chain of custody ledger to support authentication of data files and audit logs.	4.5
Lack of practice	Use audit logs and digitalized chain of custody records for routine purposes to ensure that the logs are monitored and used regularly.	4.6
Insufficient validation	Validate computer-reliant forensic processes whenever there are changes to hardware or software configurations.	4.7
Black-box automation	Evaluate automated systems at three levels performance, understandability, and scientific interpretation.	4.8
Lack of digital forensic support	Engage digital forensic expertise in preparation for problems, and to assist with dealing with problems that arise in a forensic laboratory.	5

reducing the interruption of business continuity and the overall cost to the forensic laboratory. Minimizing interruptions in forensic laboratories is essential for criminal justice, and some countries require annual testing of business continuity plans, with guidance from ISO 22313:2012 (Societal security – Business continuity management systems – Guidance) [20].

Curating digital information entails identifying all computer-reliant processes and then augmenting data sources to facilitate authentication of digital evidence (Fig. 2). When curating digital information, it is also important to eliminate extraneous data in order to avoid inordinately large repositories that are costly and time consuming to search or produce [21].

Forensic laboratories cannot rely solely on system administrators to curate digital information sources because these individuals are primarily concerned with system performance and security, and have limited experience with forensic preparedness. To ensure that forensic preparation will withstand scrutiny, it is advisable to involve experienced digital forensic practitioners in the process.

An important aspect of this forensic preservation process is to have a data management policy that specifies how long data will be maintained. For instance, a data management strategy is to erase the original files after they are forensically preserved, to avoid having to perform a costly and time-consuming forensic preservation and examination of every computer in the laboratory whenever there is a problem. Data retention decisions must take into account applicable national laws and regulations of the country.

> One of the most useful tools that investigators can have is a map indicating where evidence is located on a network – a digital evidence map. Such a map is even more useful when it specifies how long digital evidence remains on the network and references procedures for collecting the evidence. [22]

4.2. Established processes and procedures

Having documented processes to handle common audit and investigative scenarios puts forensic laboratories in a stronger position to respond in an organised, efficient and effective manner. Effective forensic preparedness requires clear oversight, authorizations, responsibilities, expected actions, desired results, and restrictions. For example, who will gather needed data from various sources in the forensic laboratory (LIMS, computers, backups), how they will perform these tasks, and under whose authority of supervision.

The purpose of documented processed and procedures is to ensure a more organized and efficient response and to reduce the risk of mistakes and oversights, thus limiting the associated disruption, liability, and cost for forensic laboratories.

These procedures include preservation of digital data with minimal disruption to business continuity and forensic laboratory operations. Proper preservation of digital data supports investigative, forensic, legal, and regulatory requirements, and can help a forensic laboratory defend against any subsequent civil litigation. Preservation is vastly simplified when forensic preparations are already in place.

Forensic laboratories should periodically test these processes and procedures to ensure they work as expected.

4.3. Data integrity

Manufacturers of laboratory equipment focus on the intended use of their systems, rather than potential misuses. Although manufacturers have some ability to check that output data is well formed, they cannot detect all types of alteration or corruption. Therefore, forensic laboratories cannot rely solely on the manufacturers of equipment to detect alteration or corruption of their output data. A straightforward mechanism for assuring the integrity of data is to generate cryptographic hash values of files, as demonstrated in Section 2.1. Using a digital forensic preservation method such as AFF4 provides more robust data integrity and evidence management. The integrity information can be stored in a LIMS system along with other pertinent details for an evidence item, or in a tamperproof digitalized chain of custody ledger.

4.4. Strategic audit logging

Forensic laboratories need to pay careful attention to maintaining chain of custody, including generating and protecting audit logging and mechanisms to ensure the authenticity and integrity of data in LIMS and generated files (raw and processed).

Ready access to audit logs allows faster response to problems and more comprehensive assessment of the scope of a problem, thereby helping reduce the associated interruption and cost. When

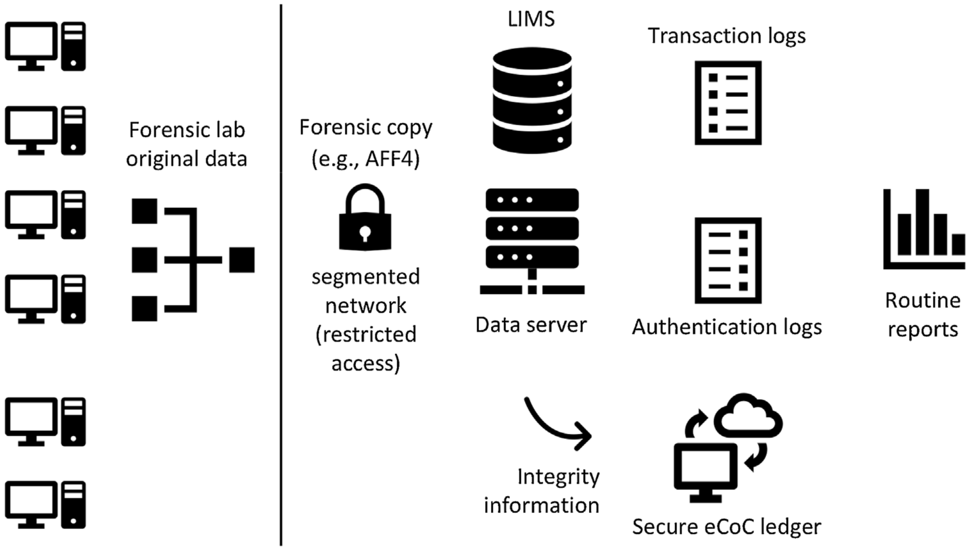

Fig. 2. Example digital evidence map for forensic laboratories.

a problem occurs in a forensic laboratory, it is advisable to make a forensic copy of all audit logs, preserving them as a source of evidence for further analysis. In some situations, it might also be necessary to restore older audit logs from backup to obtain a complete view of relevant activities.

Under certain conditions, system administrator level access can be used to bypass many protections and access controls on computer systems. Therefore, additional measures are needed to maintain the integrity of data in forensic laboratories such as maintaining integrity records contemporaneously as discussed in the next section.

4.5. Data authentication

To enable authentication of data, forensic results and audit logs, some forensic laboratories print hard copies of certain data to maintain paper records for future comparison with digital information. Another approach is to archive copies of the original digital data on read-only storage media.

Authentication can be enhanced with tamperproof digitalized chain of custody ledger using blockchain infrastructure as referenced above.

Given the importance of temporal information for data authentication, it is important for clocks on all computer systems to be automatically synchronized with a single timesource and timezone.

Some laboratories are adopting the CASE specification to represent digital forensic information, including provenance details, in a standardised form and maintain provenance of exhibits throughout their lifecycle in forensic laboratories [23]. Data marking is an integral part of CASE, supporting data protection for privacy and security purposes [24].

4.6. Regular use or review of data and processes

A common mistake that organizations make is to configure data retention and logging and only examine the information after a problem occurs. As a result, problems are registered in preserved data and audit logs but are not observed by anyone in the organization.

Routinely relying on the curated data sources, or at least reviewing them to ensure that those responsible are familiar with using and interpreting them, have effective tools for examining them, and promptly notice and resolve failures or errors such as malfunctioning data retention processes, corrupt data, incomplete records and incorrect time stamps [25].

4.7. Test and validation

When deploying new automated capabilities to support forensic analysis, it is necessary to test and validate the system to determine its reliability and limitations. Finding and mitigating problems in such systems is non-trivial and requires a systematic approach and specialized expertise [26]. Forensic laboratories have the necessary knowledge and structure to manage quality and risk of complex processes, which can be extended to encompass automated AI/ML systems [15].

4.8. Effective use of automation

One way to mitigate the risks associated with automation to support forensic analysis is to realize the value of human expertise. A study of facial comparison found that the optimal results were obtained when forensic expertise was combined with state-of-the-art face recognition technology [27].

However, when automated systems are not designed with core forensic principles in mind, lacking transparency, there is a risk of the black-box effect [10]. To manage this risk, forensic laboratories need to ensure that all automated processes they rely on produce forensic results, including AI/ML based systems, can be explained by the laboratory specialists. Limitations of automated systems, including possible false-positives and false-negatives, should be documented to manage risks of errors, omissions and misuse.

To address the risk of incorrect decisions based on automated systems, it is necessary for such systems to function well at three levels: performance, understandability, and scientific interpretation [28]. It is important to address these issues as part of forensic preparedness, before a problem occurs. Such preparations will put forensic laboratories in a stronger position to defend decision based on an automatic system and explain the underlying logic.

5. Role of digital forensic expertise

Success in managing risks associated with digital transformations in forensic laboratories depends on the qualifications and experience of the personnel performing the digital forensic processes.

Although there are ongoing efforts to harmonize digital evidence and forensic science [1], some forensic laboratories are currently unable to integrate digital forensic science, due to division of responsibilities or unavailability of resources and expertise. To help manage the risks associated with digital transformations, forensic laboratories can engage external digital forensic expertise to help develop forensic digital preparedness and respond to problems. It is most effective to arrange this prior to a problem occurring.

When a problem occurs, it can be larger than the organization initially realises. Forensic preparedness makes it easier to determine the full scope of the problem, and manage the potential damage more effectively. However, even with perfect preparation, there are usually unexpected challenges in any digital investigation. When the people dealing with a problem are not properly trained in digital forensic science, there is an increased risk of misunderstanding and misinterpretation. Even when they perform their work impeccably, unclear explanation can cause decision makers to miscomprehend digital forensic conclusions [29]. The knowledge and experience required effective forensic analysis and evaluation of digital evidence should not be underestimated [30].

Furthermore, digital forensic analysis can reveal weaknesses in forensic laboratory operations, and digital forensic expertise can help continuously improve forensic processes [31].

6. Quality assurance considerations

The forensic preparedness measures discussed above not only help laboratories respond more effectively and efficiently to problems, they also help improve quality assurance and auditability. A digital evidence map, digitally strengthened chain of custody ledger, and strategic audit logging, provide more detail and transparency into the handling of exhibits in forensic laboratories, and enables more effective problem detection and response.

It is also inadvisable to use the forensic laboratory LIMS to manage evidence of an investigation into its own problems. Therefore, forensic laboratories need to have a separate system for maintaining documentation, incident details, and evidence provenance, and other information that needs to be recorded during investigation of an incident.

This raises the question of whether there is a need to incorporate the digital transformation risk mitigation measures discussed in this paper into standards for accreditation such as ISO

17025:2017 (General requirements for the competence of testing and calibration laboratories).

6.1. Current requirements

Validation within forensic laboratories must include the underlying technology, including their hardware and software configuration, access control (security), and auditability. Each time there is a significant change in hardware or software, routine tests and validation should be performed against known datasets to determine whether expected results are produced.

Nevertheless, according to authors' experiences with laboratories both in Europe and the U.S., even ISO 17025 accredited laboratories do not always perform a validation process for each major release of every software application used for forensic analysis. This lack of rigour can be explained by the difficulty to trigger significant changes but is most of the time due to time saving reasons.

Moreover, if the ISO 17025 standard requires information management systems to be validated, the current version still states that "*commercial off-the-shelf software in general use within its designed application range can be considered to be sufficiently validated*" [32]. This large exception raises questions about existence and quality of validation processes performed by system providers. Some laboratories might also consider only validating internal systems.

6.2. Possible improvements

To overcome the limits related to validation cost of commercial software, independent bodies could share their validation results, following the digital forensic tool testing approach taken by NIST and DC3.

The need for such validation and testing does not only apply to systems used to process exhibits. More attention could be given to validation of LIMS systems, including their reliability, security, and auditability. Forensic laboratories should also ensure that access controls are in place on LIMS and secure storage systems to prevent unauthorized alteration or deletion. This issue could be address with clearer wording in quality standards such as ISO 17025 or in the the international guidance document ILAC G19.

The risks of oversights and misinterpretations are growing as more complex automated systems being used for forensic purposes lack forensics-by-design. To mitigate the associated risks forensic laboratories need to implement additional measures that govern proper operation and use of automated systems.

Quality standards such as ISO 17025 could be further refined by adding specific requirements for forensic digital preparedness described in this paper.

7. Conclusions

Forensic laboratories that fail to seriously confront digital transformations risk management will suffer significant disruption and expense when problems arise. To mitigate these risks, forensic laboratories must strengthen their forensic digital preparedness and ensure that technology abides by core principles and processes, i.e., authenticity and integrity, reliability and reproducibility, and quality and efficiency. Laboratories should also consider applying forensic digital preparedness to their email and other administrative systems. As much as feasible, the recommendations in this paper are "enable and forget" (until a problem occurs). An initial investment in forensic preparation can return repeated benefits by reinforcing forensic principles as noted in Section 3, and by reducing expenses and business disruption each time a problem arises.

In brief, laboratories should take forensic digital preparedness steps before a problem arises, and consider involving digital forensic specialists with experience in forensic laboratory operations. When a problem occurs, follow documented processes and procedures for responding to such incidents. If a plan does not exist, create one and implement it methodically. Know where sources of relevant digital data are, and take steps to preserve them properly. Forensic preservation of data includes original files and backups, as well as audit logs. Perform a thorough scope assessment to determine the full extent of the problem. Document all actions taken in response to the problem.

It would be generally beneficial to require LIMS and other digitalized processes in forensic laboratories to be forensic-by-design. The recommendations in this paper provide a foundation for forensic laboratories to develop requirements that system providers should fulfill.

With proper forethought and preparation, forensic laboratories can employ technology and advanced data analytics to enhance existing services and create new services, while respecting fundamental human rights.

Applying their existing knowledge and structures, forensic laboratories are in a strong position to effectively manage quality and risk of digital transformations.

Authors' contributions

Conception and design of study: Eoghan Casey, Thomas Souvignet

Drafting the manuscript: Eoghan Casey, Thomas Souvignet

Approval of the version of the manuscript to be published: Eoghan Casey, Thomas Souvignet.

Acknowledgements

Our deepest gratitude to Christophe Champod, Timothy Bollé, Francesco Servida, and Hannes Spichiger for their collaboration and insights. We are also thankful for the peer reviewers' recommendations which improved this work.

References

[1] M. Pollitt, E. Casey, D.-O. Jaquet-Chiffelle, P. Gladyshev, A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence, Tech. Rep., The Organization of Scientific Area Committees for Forensic Science, 2018, doi:http://dx.doi.org/10.29325/OSAC.TS.0002 January.

[2] G. Tully, N. Cohen, D. Compton, G. Davies, R. Isbell, T. Watson, Quality standards for digital forensics: learning from experience in England & Wales, FSI Digit. Investig. 32 (2020).

[3] J. Reust, R. Sommers, Identification and Reconstruction of Deleted, Fragmented DNA Digital Files, (2008) . https://www.aafs.org/wp-content/uploads/ProceedingsWashingtonDC2008.pdf.

[4] M. Cohen, S. Garfinkel, B. Schatz, Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow, Digit. Investig. 6 (2009) S57–S68, doi:http://dx.doi.org/10.1016/j.diin.2009.06.010 the Proceedings of the Ninth Annual DFRWS Conference. http://www.sciencedirect.com/science/article/pii/S1742287609000401.

[5] B.L. Schatz, Wirespeed: extending the aff4 forensic container format for scalable acquisition and live analysis, Digit. Investig. 14 (2015) S45–S54, doi:http://dx.doi.org/10.1016/j.diin.2015.05.016 the Proceedings of the Fifteenth Annual DFRWS Conference. http://www.sciencedirect.com/science/article/pii/S1742287615000614.

[6] J. Bidgood, Chemist's Misconduct is Likely to Void 20,000 Massachusetts Drug Cases, New York Times, 2017. https://www.nytimes.com/2017/04/18/us/chemist-drug-cases-dismissal.html.

[7] X. Burri, E. Casey, T. Bollé, D.-O. Jaquet-Chiffelle, Chronological independently verifiable electronic chain of custody ledger using blockchain technology, FSI Digit. Investig. 32 (2020).

[8] D.-O. Jaquet-Chiffelle, E. Casey, J. Bourquenoud, Tamperproof Timestamped Provenance Ledger Using Blockchain Technology, FSI Digital Investigation 33 (2020) June 2020, https://doi.org/10.1016/j.fsidi.2020.300977.

[9] D. Murray, Queensland Authorities Confirm 'miscode' Affects DNA Evidence in Criminal Cases, (2015) . March https://www.couriermail.com.au/news/

queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b.

[10] G. Margagliotti, T. Bollé, Machine learning & forensic science, Forensic Sci. Int. 298 (2019) 138–139, doi:http://dx.doi.org/10.1016/j.forsciint.2019.02.045. http://www.sciencedirect.com/science/article/pii/S0379073819300726.

[11] P. Fussey, D. Murray, Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, (2019) . , July http://repository.essex.ac.uk/24946/.

[12] R. Koppl, Strategic choice in linear sequential unmasking, Sci. Justice 59 (2) (2019) 166–171, doi:http://dx.doi.org/10.1016/j.scijus.2018.10.010. http://www.sciencedirect.com/science/article/pii/S1355030618300777.

[13] N. Ab Rahman, W. Glisson, Y. Yang, K.-K. Choo, Forensic-by-design framework for cyber-physical cloud systems, IEEE Cloud Comput. 3 (2016) 50–59, doi:http://dx.doi.org/10.1109/MCC.2016.5.

[14] S. COIT, Acquisition of Surveillance Technology Ordinance, (2019) . , May https://sfbos.org/sites/default/files/o0107-19.pdf.

[15] E. Casey, O. Ribaux, C. Roux, The kodak syndrome: risks and opportunities created by decentralization of forensic capabilities, J. Forensic Sci. 64 (1) (2019) 127–136, doi:http://dx.doi.org/10.1111/1556-4029.13849.

[16] F. Coppey, A. Bécue, P. Esseiva, Providing illicit drugs results in five seconds using ultra-portable NIR technology: an opportunity for forensic laboratories to cope with the trend toward the decentralization of forensic capabilities, Forensic Sci. Int. (2020).

[17] CESG, Good Practice Guide No. 18 Forensic Readiness, UK National Technical Authority for Information Assurance, 2016 October.

[18] A. Johnston, J. Reust, Network intrusion investigation – preparation and challenges, Digit. Investig. 3 (3) (2006) 118–126, doi:http://dx.doi.org/10.1016/j.diin.2006.08.001. http://www.sciencedirect.com/science/article/pii/S1742287606000922.

[19] M. Elyas, A. Ahmad, S.B. Maynard, A. Lonie, Digital forensic readiness: expert perspectives on a theoretical framework, Comput. Secur. 52 (2015) 70–89, doi:http://dx.doi.org/10.1016/j.cose.2015.04.003. http://www.sciencedirect.com/science/article/pii/S0167404815000449.

[20] G. Tully, Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System, (2017) . , October https://www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct.

[21] E. Casey, Digital evidence maps – a sign of the times, Digit. Investig. 4 (1) (2007) 1–2, doi:http://dx.doi.org/10.1016/j.diin.2007.01.004. http://www.sciencedirect.com/science/article/pii/S1742287607000060.

[22] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition, (2011) Waltham, MA, USA.

[23] E. Casey, S. Barnum, R. Griffith, J. Snyder, H. van Beek, A. Nelson, Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language, J. Digit. Investig. 22 (2017) 14–45, doi:http://dx.doi.org/10.1016/j.diin.2017.08.002.

[24] E. Casey, M.A. Biasiotti, F. Turchi, Using Standardization and Ontology to Enhance Data Protection and Intelligent Analysis of Electronic Evidence, (2017) . http://users.umiacs.umd.edu/oard/desi7/papers/EC.pdf.

[25] E. Casey, C. Daywalt, A. Johnston, Chapter 4 – intrusion investigation, in: E. Casey, C. Altheide, C. Daywalt, A. de Donno, D. Forte, J.O. Holley, A. Johnston, R. van der Knijff, A. Kokocinski, P.H. Luehr, T. Maguire, R.D. Pittman, C.W. Rose, J.J. Schwerha, D. Shaver, J.R. Smith (Eds.), Handbook of Digital Forensics and Investigation, Academic Press, San Diego, 2010, pp. 135–206, doi:http://dx.doi.org/10.1016/B978-0-12-374267-4.00004-5. http://www.sciencedirect.com/science/article/pii/B9780123742674000045.

[26] D.A. Taylor, J.-A. Bright, J. Buckleton, Commentary: a “source” of error: computer code, criminal defendants, and the constitution, Front. Genet. 8 (2017) 33, doi:http://dx.doi.org/10.3389/fgene.2017.00033.

[27] P.J. Phillips, A.N. Yates, Y. Hu, C.A. Hahn, E. Noyes, K. Jackson, J.G. Cavazos, G. Jeckeln, R. Ranjan, S. Sankaranarayanan, J.-C. Chen, C.D. Castillo, R. Chellappa, D. White, A.J. O'Toole, Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms, Proc. Natl. Acad. Sci. 115 (24) (2018) 6171–6176, doi:http://dx.doi.org/10.1073/pnas.1721355115. https://www.pnas.org/content/115/24/6171.full.pdf.

[28] T. Bollé, E. Casey, M. Jacquet, The role of evaluations in reaching decisions using automated systems supporting forensic analysis, FSI Digit. Investig. 34 (2020) August 2020 https://doi.org/10.1016/j.fsidi.2020.301016.

[29] E. Casey, Trust in digital evidence, Digit. Investig. 31 (2019) 200898, doi:http://dx.doi.org/10.1016/j.fsidi.2019.200898. http://www.sciencedirect.com/science/article/pii/S2666282519300647.

[30] E. Casey, Standardization of forming and expressing preliminary evaluative opinions on digital evidence, FSI Digit. Investig. 32 (2020) 200888, doi:http://dx.doi.org/10.1016/j.fsidi.2019.200888. http://www.sciencedirect.com/science/article/pii/S1742287619303147.

[31] E. Casey, B. Nikkel, Forensic analysis as iterative learning, in: M.M. Keupp (Ed.), The Security of Critical Infrastructures Risk, Resilience and Defense, Springer, San Diego, 2020.

[32] ISO, Iso/iec 17025:2017 General Requirements for the Competence of Testing and Calibration Laboratories, (2005) .