SACJ 30(1) July 2018
Research Article

A Digital Forensic Readiness Architecture for Online Examinations

Ivans Kigwana, H.S. Venter

Department of Computer Science, University of Pretoria, South Africa

ABSTRACT
Some institutions provide online courses to students to ease the courses' workload. Online courses can also be convenient because the online course content management software conducts marking of tests and examinations. However, a few students could be willing to exploit such a system's weaknesses in a bid to cheat in online examinations because invigilators are absent. Proactive measures are needed and measures have to be implemented in order to thwart unacceptable behaviour in situations where there is little control of students' conduct. Digital Forensic Readiness (DFR) employs a proactive approach for an organisation to be forensically prepared for situations where there is little control over people. This can be achieved by gathering, storing and handling incident response data, with the aim of reducing the time and cost that would otherwise be spent in a post-event response process. The problem this paper addresses is that, at the time of writing this paper, there existed no known DFR architecture that can be used to collect relevant information for DFR purposes, specifically in the course of an online examination, as described in the standard published by the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC) (ISO/IEC 27043:2015) for incident investigation principles and processes. Due to the lack of DFR architecture, the authors propose an Online Examination Digital Forensic Readiness Architecture (OEDFRA) that can be used to achieve DFR when online examinations are conducted. This architecture employs already existing DFR techniques, discussed in the study, to help educational institutions achieve DFR in online examinations. This architecture, (OEDFRA), when implemented, will be tested in future research in order to confirm its contribution to the field of DFR.

Keywords: digital forensics, digital forensic readiness, online examination architecture, online examination fraud, digital evidence, cheating in online tests

Categories: • **Security and privacy** ∼ **security services** • *Security and privacy* ∼ *authentication*

Email:
Ivans Kigwana ivans.kigwana@gmail.com,
H.S. Venter hventer@cs.up.ac.za

Article history:
Received: 27 February 2017
Accepted: 11 April 2018
Available online: 10 July 2018

1 INTRODUCTION

Technology has become a part of our daily lives and the way in which we handle and execute duties. Many educational institutions offer technology-related educational programmes but even the non-technology programmes have some aspect of technology attached to them-for instance writing and submission of assignments electronically, as well as writing online examinations. This

Kigwana, I. and Venter, H.S. (2018). A Digital Forensic Readiness Architecture for Online Examinations. *South African Computer Journal 30*(1), 1–39. https://doi.org/10.18489/sacj.v30i1.466

SACJ is a publication of the South African Institute of Computer Scientists and Information Technologists. ISSN 1015-7999 (print) ISSN 2313-7835 (online).

technology of online education is often known as e-learning (Welsh, Wanberg, Brown, & Simmering, 2003). Most institutions use e-learning as a way of saving time and money spent on stationery and manpower in the form of invigilators (Welsh et al., 2003; Clark & Mayer, 2016). Another major reason for employing e-learning is the attempt to reduce students' cheating during paper-based examinations. Serving students with questions in a different order in an e-learning environment discourages students from eavesdropping on the screen of another student. However, some students still find ways and opportunities to cheat during online examinations, without being caught. This is, in some cases, caused by the fact that some students are used to face-to-face interaction with their lecturers and when faced with the challenge of having study material delivered online, some find it hard to cope with the pressure and resort to cheating [3]. Regardless, even when a student is caught cheating during an examination, there might not be sufficient potential evidence to prove that the student committed such an offense and without such information, the student's wrongdoing might go unpunished. This situation currently presents itself because there are no proper procedures that can be used to collect digital information that can be used as potential digital evidence for the purposes of a disciplinary hearing into examination cheating.

The use of digital devices, internet usage in educational institutions and because students have easy access to the internet, made it easy for some students to exploit the situation when writing online examinations (Renard, 1999). When there are no invigilators where an examination takes place, the situation is worse because students may use the opportunity to cheat without being observed. However, in the past there were cases where students have been caught cheating during online examinations even when invigilators were present (King, Guyette Jr, & Piotrowski, 2009). Some students, though, get away with cheating during online examinations and with lack of the necessary potential digital evidence, any allegations by an invigilator that students were indeed cheating, are often treated as hearsay since there would be no evidence to back up the allegations, apart from the invigilator's word. However, some studies have shown that hearsay is also evidence (Spencer, 2014). The authors believe that using hearsay evidence can be argued.

Educational institutions that use e-learning have tried to make it harder for students to cheat during online examinations, however, current efforts prove to be unsuccessful in most cases (Hylton, Levy, & Dringus, 2016). It should be noted that detecting online examination fraud requires proper laid down procedures that should be followed when collecting potential digital evidence that can be used in a disciplinary hearing. However, the process of gathering information that can be used as potential evidence to convict a student of cheating can prove to be very difficult and even impossible if no proper procedures exist.

In this research, the authors propose an Online Examination Digital Forensic Readiness Architecture (OEDFRA) that can be used to achieve Digital Forensic Readiness (DFR) in online examinations. Educational institutions would be able to successfully convict students, in case of suspicion of online examination cheating which require a Digital Forensic Investigation (DFI), by using architecture such as OEDFRA.

The remainder of this paper is organised as follows: Section 2 discusses the background of the study of this paper. This is followed by Section 3 that gives a discussion of how ISO/IEC 27043:2015 is mapped to the OEDFRA. After this, Section 4 discusses the proposed architecture

for achieving DFR in online examinations, which is followed by preliminary results in Section 5 then a critical evaluation of this study follows in Section 6. Lastly, in Section 7, the authors conclude and mention future work to be conducted for this study.

2 BACKGROUND

In this section, the authors present an overview on Digital Forensics (DF), Digital Forensic Readiness (DFR) and fraud in online examinations. Since the architecture proposed is based on Online Examination Fraud (OEF), different sections of the Digital Forensic Investigation (DFI) processes, together with DFR as published in the ISO/IEC 27043:2015 international standard, are also reviewed. The authors review these four key areas particularly, because the proposed architecture follows the ISO/IEC 27043:2015 process of carrying out DFR during a DFI.

2.1 Digital forensics

Digital forensics, sometimes referred to as "computer forensics", started to evolve in the 1970s (Kohn, Eloff, & Eloff, 2013). During that time, DFIs mainly involved financial fraud. Currently, DF is being used to solve most cybercrimes and is not limited to financial fraud (Garfinkel, 2010). Examples of such cybercrimes include—but are not limited to—online identity theft, hacking, theft of company secrets etc. The National Institute of Standards and Technology (NIST) defines digital forensics as a process involving the identification, collection, examination, extraction, analysis and reporting of information as evidence (Kent, Chevalier, Grance, & Dang, 2006). While conducting this process, it is vital that the integrity of the information being extracted digitally from the computing device be adequately preserved or maintained. In the first Digital Forensic Research Workshop (DFRWS) held in 2001, Palmer (2001) defined DF as

> the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources, for the purpose of facilitating the reconstruction of events.

Due to the fact that an online user leaves behind a trail of information about his/her activities when digital devices are used, different DF tools can be used to reconstruct events and attain potential evidence from these devices in case an investigation is to be carried out. Even though a trail of information is left behind, DF investigators often carry out an investigation after the fact, i.e., reactively. The ISO/IEC 27043:2015 (2015c) international standard, for instance, provides investigators with a general standard that can be followed when conducting a formal digital forensic investigation. When these formalised steps and processes are followed correctly, chances of presenting admissible digital evidence about OEF to a disciplinary committee, increases substantially. In the next section, the authors take a closer look at DFR, which complements the area of DF in a proactive manner, and subsequently forms the main focus area of this study.

https://doi.org/10.18489/sacj.v30i1.466

2.2 Digital forensic readiness

Digital forensic readiness (DFR) is a precautionary or proactive measure put in place for a DFI, i.e., having DF measures in place before a crime is potentially committed. This means any organisation with DFR capability has the ability to support and provide enough potential digital evidence to an entity tasked with the duty of handling the DFI process, since the organisation would have gathered enough potential digital forensic information in advance of an incident. To achieve this, the organisation has to follow established guidelines involving a DFR process, as published in the ISO/IEC 27043 international standard (2015c).

Rowlingson (2004) defined DFR as "the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation." This requires an investigation process architecture, which recognises both the readiness and the investigation phases, to ensure that the processes and setup support such an investigation (Carrier & Spafford, 2003).

Most educational institutions now offer online examinations to their students, sometimes as a substitute to traditional paper-based examinations, especially for distance learners. Other reasons for employing online examination systems are to reduce on stationery costs and to avoid the cases of examination cheating that are mostly known to happen in traditional paper-based examinations. However, numerous recent threats to online examinations evolved, such as OEF. Other threats, among others related to OEF, include examination leakage through possible hacking, denial of service attacks and Trojan Horses (Furnell & Karweni, 2001; Dawson, 2016).

As mentioned earlier, achieving DFR in any organisation can be possible if an internationally recognised standard like ISO/IEC 27043 (2015c) is followed. Therefore, in this study, the authors use this international standard as a basis for their study and also show the reader, how ISO/IEC 27043 can be used to achieve DFR in online examinations, as explained in the next section.

2.3 International standardisation in DF: ISO/IEC 27043:2015

The international standards organisation (ISO) is a body that focuses on developing and publishing international standards in a very wide range of subject areas. One of those areas is information technology and security techniques, in which the area of digital forensics is included. Currently, there are numerous international standards that exist with a specific focus on DF. Some of these standards include:

1. ISO/IEC 27037:2012—Guidelines for identification, collection, acquisition and preservation of digital evidence(International Standards Organization, 2012),

2. ISO/IEC 30121:2015—Governance of digital forensic risk framework (International Standards Organization, 2015d),

3. ISO/IEC 27041:2015—Guidance on assuring suitability and adequacy of incident investigative method (International Standards Organization, 2015a),

4. ISO/IEC 27042:2015—Guidelines for the analysis and interpretation of digital evidence (International Standards Organization, 2015b) and also

5. ISO/IEC 27043:2015—Incident investigation principles and processes (International Standards Organization, 2015c).

In this study, the authors' focus is on ISO/IEC 27043:2015 and how it can be applied in online examinations to achieve DFR. The reason behind selecting to use ISO/IEC 27043:2015 among other options is due to the fact that it is the only international standard, among the current standards, that includes detailed guidelines on the implementation of DFR as a process. However, the standard is generic in the sense that it does not specifically address how DFR can be applied to OEF. Therefore, since this entire study is centered on DFR, the authors chose this standard as a basis for their study in order to extend DFR to OEF.

ISO/IEC 27043 is an international standard that provides guidelines and procedures, which are based on generic architectures for any incident investigation process across various investigation scenarios that involve digital evidence examination (International Standards Organization, 2015c). This standard also provides an overview of the entire digital incident investigation process, without necessarily providing specific details within each of the digital investigation processes, as covered in ISO/IEC 27043. Among the processes presented in this standard is the DFR process. Figure 1 represents the flow of the ISO/IEC 27043 digital investigation process.

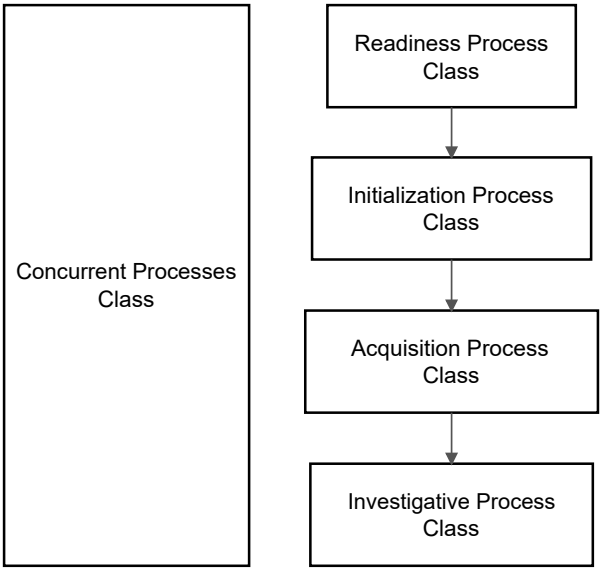

Figure 1: Digital investigation process classes (International Standards Organization, 2015c)

The digital investigation process classes, as shown in Figure 1, constitute the standard digital forensic investigation process according to ISO/IEC 27043:2015 international standard. The reader should note that the dotted lines around the Readiness Process Class indicate that it is the main focus of this study. Another reason for the use of dotted lines is that, according to

ISO/IEC 27043:2015, it is an optional process that does not necessarily have to be part of the reactive DFI process. The next section discusses the background of the fourth key area of this study, which relates to online examination fraud.

2.4 Online examination fraud

Online Examination Fraud (OEF) relates to cheating during an online examination, usually by students. Online examination forensics is a new investigation area in digital forensics, coined by the authors. In other words, online examination forensics refers to the discipline that utilises a DF process applied to OEF.

Students use various methods to cheat in online examinations. Some practices have existed for many years but never received much research attention. One example of OEF practice, referred to here as impersonation, exists where a student attends an online examination on behalf of another student. Other forms of OEF are still new, since they arise from the exploitation of advancements in technology, for instance, checking the Hypertext Mark-up Language (HTML) code that might contain the possible answers (Kigwana & Venter, 2016).

Tips on how to secure online examinations and prevent against OEF are presented by Freifeld (2013). He provides scenarios of how students cheat in online examinations. He discusses a situation that happened in China in 2012 where over 1500 people were suspected of selling transmitters and earpieces to students with the aim of helping them to cheat during online examinations.

Different factors, for instance, time pressure and high course demands, often compel some students to succumb to these kinds of OEF behaviours (Sterngold, 2004). Isolation experienced by students, such as distance-learning students taking online examinations or programmes—usually increases stress levels among these students, contrary to what their fellow students, who have a face-to-face interaction with their lecturers, experience (Gibbons, Mize, & Rogers, 2002). For this reason, 1998 argue that students who engage with lecturers actively are less likely to involve themselves in examination malpractices. Scanlon (2003) believes that this problem is not about to disappear any time soon, since some educational institutions lack the necessary manpower and experience to manage and maintain transparency in online examinations.

To further elaborate on the issue of OEF, Table 1 shows some of the techniques that students use to cheat in online examinations. Two columns are shown: the middle column represents methods that are known to happen in online examinations and other methods that strictly happen in paper-based examinations are shown in the column on the right. This study concentrates on techniques used in online examinations.

From Table 1 it is evident that more attention needs to be put on securing online examinations. This is evident by the number of ticks (which are significantly more than those in paper-based examinations), which show that there are more ways of cheating in online examinations than in traditional paper-based examinations. Most of these techniques of cheating involve the use of digital devices. This can also explain why there is a need for DFR in online examinations, just in case there is suspicion of students cheating in online examinations.

Table 1: Techniques of cheating in online and paper-based examinations

Techniques	Online examinations	Paper-based examinations
Accessing online content	✓	
Screen share	✓	
Opening new pages in separate tabs/pages	✓	
Inspecting element/HTML code	✓	
Using programmable devices	✓	✓
Using an impersonator	✓	✓
Switching computers during an examination	✓	
Bribing the invigilators	✓	✓
Using in-ear radio devices	✓	✓

In the next section, a brief reference is made to some of the laws that cover digital forensic information and its use in judicial proceedings, since OEF has a definite legal connotation.

2.5 Legal perspective on potential digital forensic evidence

Different countries or jurisdictions have different requirements on the legality of information that can potentially be used as digital evidence. The practice of gathering information for purposes of detecting and acting on OEF, however, may infringe on privacy and interception of communication laws if no proper measurements are followed to protect personal information. The following Acts define the rules of admissibility and legality of digital evidence in South Africa, USA and UK (amongst others) respectively:

1. The Protection of Personal Information (POPI) Act of South Africa (2013a),
2. Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) of South Africa (2013b),
3. The Electronic Communication and Transaction (ECT) Act of South Africa (2006),
4. Stored Communications Act (SCA) of USA (2009) and
5. The UK's Association of Chief Police Officers (ACPO) (2012).

The SCA (Scolnik, 2009) notes that accessing an electronic device for purposes of gathering information without authorisation is against the law. However, The Electronic Communications Privacy Act (ECPA) (2012) of the USA notes that any electronic information or digital evidence that has been intercepted and all electronic records thereof must be collected to help in any prosecution process in the judicial system. The POPI Act of South Africa gives a constitutional right to information privacy by protecting personal information. However, chapter 4 of the same Act legalises the interference to private information in cases that involve national security (2014).

Although the interception of online examination data might not necessarily be seen as private information threatening national security, a case can be made that private information divulged during an online examination was for the purposes of suspected OEF and not for blatant infringement of privacy. RICA is used to enforce the interception and monitoring of all communications in South Africa. Also, an exemption to the interference of private information is made in this case if it involves national security, as well as for the prosecution or detection of offenses (2013b), which, in the case of this research, include OEF.

These Acts cannot be ignored when conducting DFR for the purpose of OEF detection and prosecution. However, these Acts do make room for conducting DFR under certain conditions, such as when there might be suspicion that a crime might be committed. It should be stressed that not all students are automatically suspected of committing examination fraud; however, incorporating the paradigm of DFR during online examinations would ensure that evidence would be available in the case that a student is suspected of OEF. Therefore, if used properly, these Acts will allow such measures of information interference to be carried out only if the students are aware that they are monitored for the said purpose. It is possible to make students aware of this practice by for example, letting them sign an institution's policy agreement/contract. This policy agreement/contract should state that students agree to be subjected to monitoring during the course of online examinations. When such legal requirements are met and proper procedures, as outlined in ISO/IEC 27043, are followed, the success rate of convicting students for OEF by using such DFR practices in online examinations, is likely to increase significantly.

The next section discusses the application of the ISO/IEC 27043 international standard to online examinations in order to achieve DFR.

3 APPLYING DIGITAL FORENSICS READINESS IN ONLINE EXAMINATIONS USING ISO/IEC 27043:2015

As previously explained and illustrated in Figure 1, the main focus of this study is in the readiness process class and how it can be applied to online examinations to achieve digital forensic readiness. This is further discussed in detail in the sections to follow.

3.1 Overview of the Readiness Process Class

Referring to processes under the readiness process class, the authors refer to those processes that need to be covered by the educational institution so that, in an event of suspicion of OEF that would require a DFI, such an institution has the ability to maximise its potential to make use of digital evidence while minimising the time and cost of a conventional reactive DFI (International Standards Organization, 2015c; Rowlingson, 2004). The ISO/IEC 27043 standard mentions four aims as to why an organisation (such as an educational institution in the case of this research) would need digital investigation readiness processes, namely:

1. To maximise the potential use of digital evidence;

2. To minimise the costs incurred when carrying out a DFI either directly to the organisation's system, or related to the system's services;

3. To minimise interference with and prevent interruption of the organisation's business processes;

4. To preserve the current level of information security of systems within the organisation (2015c).

To further enlighten the reader on how the ISO/IEC 27043:2015 international standard fits into this study, the standard breaks down the readiness process class into groups. In the next section, the authors provide an explanation of each of the three groups in the readiness processes class and also provide a graphical representation of these process classes in Figure 2.

3.2 Readiness Process Groups

The readiness process group in ISO/IEC 27043:2015 comprise three main groups namely; planning process group, implementation process group and assessment process group. However, as shown previously, in Figure 1, there are processes that run alongside these process groups, from the start to when the assessment finishes. These are known as concurrent processes. A detailed explanation for each process group and concurrent processes can be found in ISO/IEC 27043:2015 (2015c).

As seen in Figure 2, all process groups are iterative, meaning that any stage in the process groups, it is possible for one to return to the previous process. For instance, imagine during the assessment process an investigator notes that certain pre-incident analysis measures were not properly implemented in the implementation process group, the investigator would then need to go back to the implementing pre-incident analysis process to make the necessary changes. Take a scenario where a student wants to submit their online examination after they finished writing their online examination. According to the authors' proposed architecture, a pre-analysis of the examination about to be submitted, has to be performed. The pre-analysis process compares answers from the student's examination with answers existing in the answers database in order to detect if answers from the answer database might have been compromised in some or other way. However, when testing the OEF forensic system, the developers/administrators of this forensic system might realise that, even when the similarity index of students' answers might be above a certain threshold (indicating that a student might have copied from another student sitting next to him/her, or that the database might have been compromised in some or other way), no red flag is raised by the system when indeed a flag should have been raised by the system. Such a situation might be the result of an implementation error or configuration error of the DFR system. Usually, when an error appears, it could mean a valid request was made from the user's (student's) workstation but the server refuses to accept the request due to lack of permission to access the requested resource. Another reason can be due to short timeout duration during the pre-analysis process (step 30 of Figure 8, shown later) when the system is still checking for the similarity index. Therefore, this will require the responsible parties to go back to the implementation processes in order to rectify this problem.

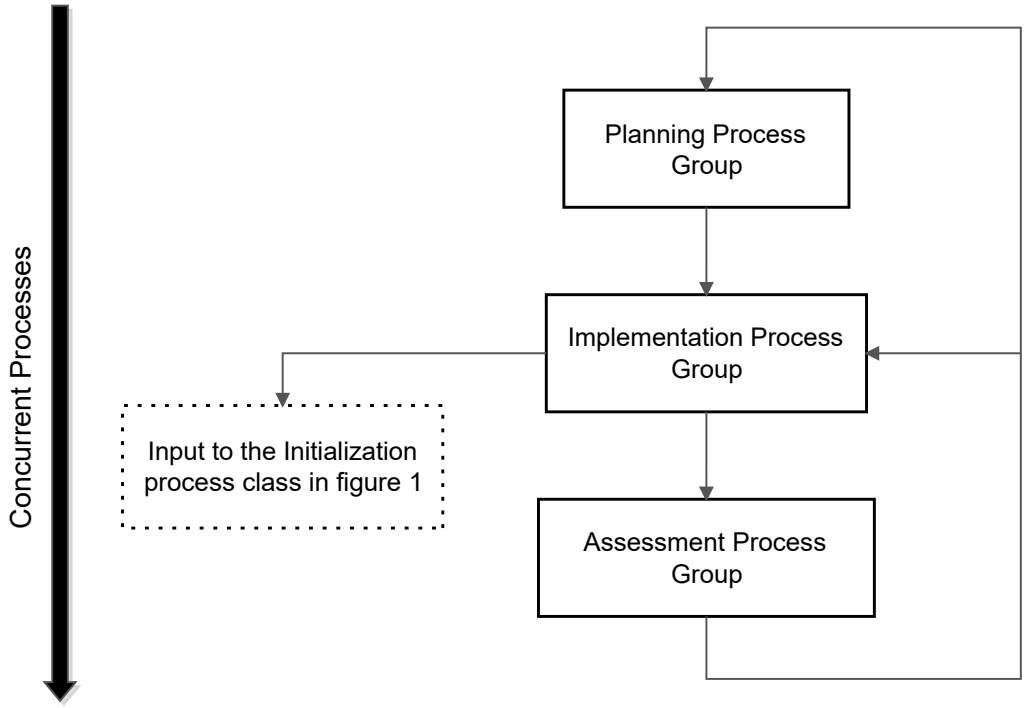

Figure 2: Overview of Readiness Process Group

Another scenario might be that, during the planning phase, the implementer notice that plans made during the planning phase are not in line with the required DFR requirements and/or principles spelled out by the educational institution. One can then go back to the planning phase to make the necessary adjustments. Consider for instance, the educational institution might categorically state in a policy that no sensitive information (like a student password) should be captured in plain text as part of the potential digital evidence. Another policy example might be that the institution states that all gathered information should be grouped in correct file formats to ease identification. If at some stage this is not the case, one can go back to the planning process phase to correct this problem.

To further understand what happens in each process group, each of the groups is broken down into steps and explained in detail in relation to OEF.

3.2.1 Concurrent Process

Concurrent processes, presented in Figure 2, refer to processes that happen alongside the non-concurrent processes. These processes can happen in no particular order, unlike the non-concurrent processes that are sequential. For instance, with non-concurrent processes, the implementation process group cannot go ahead unless processes in the planning process group have been accom-

https://doi.org/10.18489/sacj.v30i1.466

plished. The main reason why concurrent processes are needed is to make sure that all potential digital evidence is admissible in legal proceedings. Without these concurrent processes, there is a risk that the digital evidence might not be admissible. The reason might be improper handling and documentation of the digital evidence. The ISO/IEC 27043:2015 standard mentions six concurrent processes (2015c);

1. Obtaining authorisation: This process simply means that before any information gathering can be done, the party intending to gather such information needs to get permission from the institution's authorised personnel/office responsible for the administration and management of online examinations.

2. Documentation: All gathered digital information representing potential digital evidence needs to be clearly documented and easily distinguishable from one another.

3. Managing information flow: The flow of information from one stage to other needs to be well taken care of to make sure no digital information is compromised in the process.

4. Preserving chain of custody: All digital evidence that is gathered needs to be clearly marked from the point it was gathered, who gathered the evidence, the process of gathering it and when it was gathered, transportation of such evidence, analysis and disposition of such evidence.

5. Preserving digital evidence: This process deals with making sure that all gathered evidence is preserved through hashing, to maintain its integrity. If the integrity of gathered evidence is doubtable, such evidence faces a risk of being inadmissible in a disciplinary hearing.

6. Interaction with the physical investigation: This process deals with how gathered evidence is collected physically from an investigation scenario (incident scene).

3.2.2 Planning Process Group

All the planning relating to how data is gathered happens in this process group. Activities involved in this planning process group include the following:

1. Scenario definition: this process involves identifying scenarios where digital evidence can be required. In this study, the scenario where digital evidence is required will be during the course of writing the online examination. In case there is any suspicion that online examination fraud took place, there is sufficient information that can be used to acquire potential digital evidence.

2. Identifying sources of potential digital evidence: in this process, all sources where potential digital evidence can be captured from are identified, for instance, keystrokes from the keyboard, mouse movement and workstation memory, and storage on which the online examination is written. Evidence can also be captured from surveillance cameras, if there are any in the examination room.

3. Planning pre-incident gathering, storage and handling of potential digital evidence: in this process, the educational institution is required to define ways of how pre-incident information gathering, storage and handling will be conducted. This means that measures need to be put in place to define what kind of data needs to be captured and a risk assessment has to be performed pertaining to all data that will be captured in the process. It is the institution's responsibility that all collected data conforms to principles governing a digital investigation process; else such data might not be admissible in a disciplinary hearing or a court of law. Also, while gathering data, the institution is obliged to protect the privacy of its students and abide by the laws governing its jurisdiction.

4. Planning pre-incident analysis: in this process, procedures of how data representing potential digital evidence are defined and clearly spelled out. For this process to be a success, the institution is required to have a system, such as a monitoring system, that is able to detect incidents as they happen. For instance, having a log processing system would enable most data to be captured in form of logs. The main aim is to detect incidents. Therefore, this system needs to show exactly how the incident is detected and what behaviour constitutes an incident. For example, if a student logs into the system three times without any success, the system should be able to report this incident promptly, since it might be an indication of an intruder trying to access the system.

5. Planning incident detection: in this process, the institution needs to stipulate what actions need to be performed when an incident of online examination fraud is detected. Still using the same example as mentioned in the planning pre-incident analysis process (i.e., miss-entering a password several times), the system should lock out the student immediately after making more than a certain number of failed login attempts. The system should send an alert to the server about the incident, showing on which specific workstation the incident occurred. In the meantime, this information is forensically logged for DFR purposes.

6. Defining system architecture: it is in this process that all system architecture is defined, including all the applications that will be used to capture data, the network on which the readiness system and online examination system will be hosted on, all required software that will run on the online examination workstations and the DFR server. All these need to be in line with the output results from the previously-mentioned readiness processes.

3.2.3 Implementatation Process Group

This process group includes the entire processes specific to implementing all plans mentioned in the planning process group. These include;

1. Implementing system architecture: in this process, the system architecture that was planned in the planning process group is implemented. This process includes installation of relevant software that is required for the smooth running of online examinations and also software to be used to capture data representing potential digital evidence. This includes, among others,

implementing the hardware such as workstations and the required peripherals, surveillance cameras, network equipment and server equipment. Policies that will be followed when implementing DFR measures need to be spelled out clearly at this stage before the readiness process can be instantiated across the entire institution.

2. Implementing pre-incident gathering, storage and handling of potential digital evidence: in this process, the educational institution is required to implement pre-incident gathering, storage and analysis of all data that represents potential digital evidence, as mentioned in the planning of pre-incident gathering, storage and handling of potential digital evidence phase in the planning process group. Activities that happen in this process include installation of forensic logging software that will gather data representing potential digital evidence (including timestamps of when each log entry was taken). Devices required at this stage include biometric readers and surveillance cameras installed inside the examination rooms.

3. Implementing pre-incident analysis: in this process, the institution should implement pre-incident analysis of all data representing potential digital evidence, as mentioned in the planning process group. Here, the required applications that detect incidents and send alerts to the server need to be properly implemented. The output generated in this process is in the form of detected incidents during the course of the online examination. These incidents might include, among others, failed login attempts, attempts to open new tabs or web browsers (if more than one browser exists on the same system), and attempts to use forbidden external drives on the examination system.

4. Implementing incident detection: in this process, the institution is required to implement incident detection as mentioned in planning incident detection in the planning process group. This process depends mainly on input received from implementing pre-incident analysis of all data represented in the potential digital evidence process. Since any incident detection is dependent on analysis performed, it is, at this stage that system designers of the forensic monitoring system need to decide which data is deemed relevant to the DFI process. In this study, data such as attempts to install prohibited external peripherals, detection of a high similarity index between answers submitted by the student and answers already in the examination database, can be crucial during an investigation. Therefore, this type of data can be forwarded to the next stage of the DFI process. In this same process, the institution is required to spell out guidelines, clearly stating what constitutes an event, to be recognised as an incident. At this stage, there is a fine line between DFR processes and the actual digital investigation. This is due to the fact that, without an incident, no investigation can be conducted and an event has merely declared an incident. This process is the link between the readiness process class and the incident detection process that forms the first process in the initialisation process class. The reader is reminded that this was illustrated in Figure 2, using dotted lines.

3.2.4 Assessment Process Group

In this process group, the institution and/or responsible bodies within the institution, perform an assessment of the generated results from the implementation process group. These results are then compared to the initial aims set out by the institution for wanting to achieve DFR in online examinations. It is at this stage that all legal matters relating to captured data are reviewed and settled to make sure no individual rights relating to personal information are violated, all captured data is within the laws of the given jurisdiction in which the educational institution resides, all DF principles within that specific jurisdiction are followed and all the other architectures and procedures mentioned earlier are adhered to. If all these aspects are reviewed and in good standing with the legal realm, all gathered data representing potential digital evidence stands a good chance of being admissible in a disciplinary hearing or a court of law. If all plans are carefully made and implemented in the right way by following correct procedures and all assessments are done properly, it is possible for an educational institution to achieve DFR in online examinations.

Note that DFR is implemented before the potential crime is committed, i.e., DFR follows a proactive approach. DF, however, is carried out after the crime has been committed and, hence, follows a reactive approach. The focus of this study, which is DFR, entails all processes that happen before and during the course of the online examination, to the point when the student submits the online examination and leaves the examination room. This study aims to find ways of how best to prepare educational institutions that make use of online examinations to achieve DFR. Achieving DFR means less time is spent gathering digital evidence in a reactive manner to be used in an investigation. In this fashion, costs of gathering such data are severely reduced, mainly due to the amount of time that is saved.

The following section discusses the proposed DFR architecture for online examinations.

4 ONLINE EXAMINATION DIGITAL FORENSIC READINESS ARCHITECTURE

This section presents the proposed online examination digital forensic readiness architecture (OEDFRA), following the ISO/IEC 27043 international standard. The proposed architecture can help educational institutions achieve DFR by making use of the DFR process, as stated in ISO/IEC 27043. According to the Oxford dictionary, an architecture is defined as "the conceptual structure and logical organisation of a computer or computer-based system" (Oxford Dictionaries, n.d.). In this study, the proposed architecture is broken down into several main processes. To represent these processes, the authors first provide a high-level view of the architecture, which acts as a guideline to the extended architecture, in the section that follows.

4.1 High-level architecture

Figure 3 is a representation of the high-level view of the proposed OEDFRA. This architecture is designed following the ISO/IEC 27043 international standard titled "Incident investigation principles and processes".

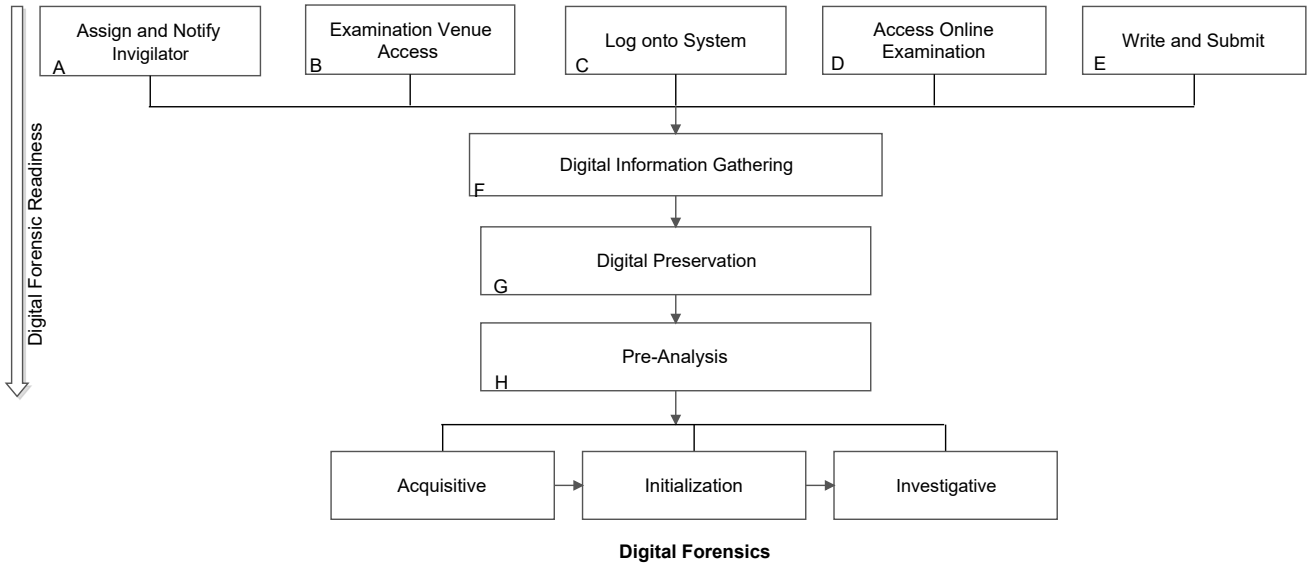

Figure 3: High-level view of the OEDFRA

Figure 3 shows the main processes of the proposed architecture labelled A to H. These processes (A to H) are the main focus of this study that makes up the OEDFRA. A detailed analysis of the last three processes (Acquisitive, Initialisation and Investigative), which fall outside the DFR process class (see Figure 1), can be found in the ISO/IEC 27043:2015 international standard (2015c) and is adopted exactly as such. Process A concerns assigning and notifying invigilators of their duties. Process B is a representation of the access control mechanism to the examination venue through means of authentication. There are different ways of authenticating users, for instance, biometric authentication like fingerprint scanning, usernames and passwords, Personal Identification Numbers (PINs) and smart card readers, and others which are some of the most commonly used methods of authentication. From the authors' perspective, they recommend the use of multifactor authentication methods. Multifactor authentication consists of a number of verification methods where each method adds an extra layer of security to the system by making use of—in addition to the username and password—something that only the user of the system knows and that the user has at hand (SecurEnvoy, 2017; TechTarget, 2017). In this study, the multifactor authentication methods chosen involve the use of a username and password, an access card (token) and fingerprint biometrics to authenticate a user's identity. Unlike other methods where students can easily exchange their personal information (like a username and password, as well as an access card) with another student, it is not easy to exchange a biometric authentication method, thereby adding an extra of layer of security, which effectively limits chances of impersonation.

Students and invigilators have to be authenticated first before they can gain access to the examination venue. For the purposes of this study, use of access cards and fingerprint biometrics

have been chosen as the preference by the authors, since such a system of authentication (multi-factor authentication) is nowadays commonly used at many institutions around the world. After successful authentication, students and invigilators should then have access to the examination venue, from where students can proceed to their individual workstations. As soon as the student reaches their workstation, they each log into the system at process C and, if the login attempt is successful, then they should have access to the online examination at process D. A student can then start answering the examination questions during process E and when a student finishes writing, they can submit their examination online.

When the examination is finished, the invigilator and student can sign out of the examination room using the biometric system. Fingerprint features are captured digitally by the system. During all these processes (from process A to process E), digital information is collected and preserved forensically for DFR purposes, in the case that a DFI might be required (i.e., should there be suspicion of a student cheating during the examination). Processes A to E are each discussed in detail in the sections to follow. Processes F, G and H are, however, not discussed separately because these are continuous processes that make up the overall OEDFRA and, therefore, they are discussed alongside processes A to E and represented as steps 36, 37 and 38 in Figures 4 to 9, in the sections to follow.

A certain number of techniques are used during the process to capture data, using the OEDFRA, to represent potential digital evidence. These techniques have been identified by the authors in previous research (Freifeld, 2013) and are presented in a summarised form in Table 2, alongside the respective data that will be captured by each technique. These techniques are labelled from T1 to T8, which are interpreted as “Technique 1” to ”Technique 8” respectively.

In the next section, the authors discuss each process of the high-level architecture, as shown in detail, Figure 3.

https://doi.org/10.18489/sacj.v30i1.466

Table 2: Summary of DFR techniques and information provided by each (from Kigwana and Venter (2016))

DFR technique	Description	Information to be captured
T1	Multifactor authentication (*Username, password, access card and biometrics*)	Name of the person and ID number on access card Fingerprint features Venue ID Timestamp (date/time)
T2	Surveillance cameras	Video footage Venue ID Timestamp of footage (date/time) IP address of camera Camera ID
T3	Key Logging	Keystroke Timestamp
T4	PC Activity Logging	Accessed Timestamp
T5	Mouse Activity Logging	Mouseclicks Timestamp
T6	Background screen recording	All PC activity footage
T7	Webcam recording	Individual footage of PC user
T8	Browser Logging	Browser log Timestamp

https://doi.org/10.18489/sacj.v30i1.466

4.2 Detailed view of the OEDFRA

In this section, the authors discuss the different processes of the proposed OEDFRA in detail. For each process, first, the authors illustrate the process in a figure followed by a detailed discussion of this process.

4.2.1 Assign and Notify Invigilator

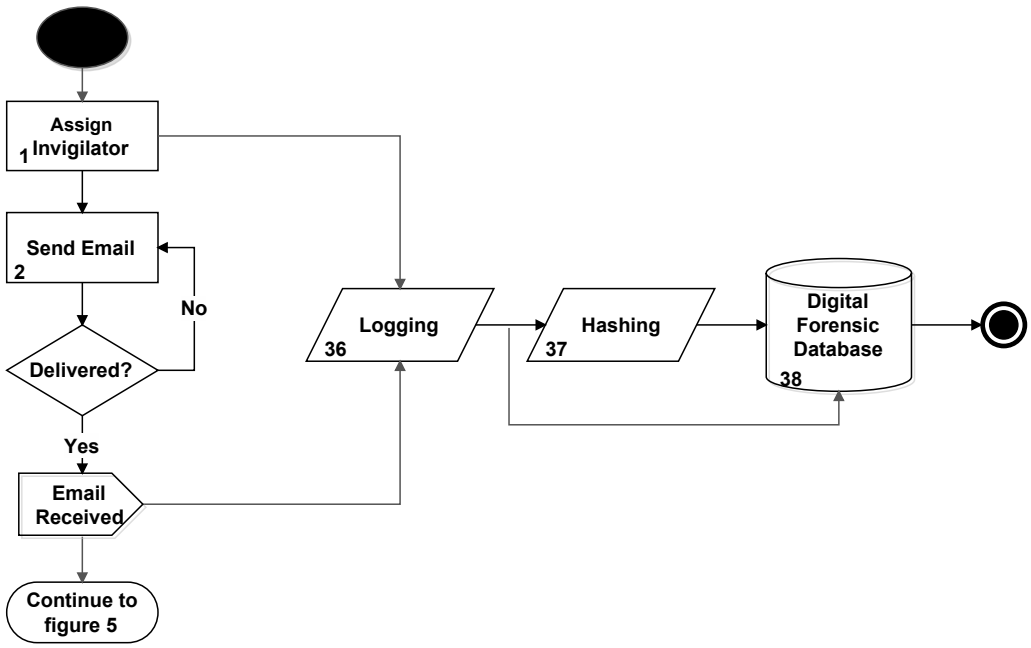

Figure 4: Assign and Notify Invigilator

Figure 4 is a representation of the first process, i.e., process A—Assign and Notify Invigilator. During this process, the invigilators are automatically assigned to examination venues by the system, from a pool of registered invigilators (at step 1 in Figure 4). Each assigned invigilator is notified of their upcoming duties through an email - in step 2. The email is sent out by the system administrator, who has to make sure that each invigilator receives the email. When the system signals receipt, it shows that the email was successfully sent and received at the recipient's end. In case the email is not delivered, the system has to resend the email until it is sent and received.

All this information in the different steps is captured by the system in step 36 and digitally preserved for DFR purposes in step 38, in case there is need for a digital forensic investigation later. A hash is also created in step 37 to protect the integrity of the captured information.

One should note that steps 36, 37 and 38 appear in all the other detailed diagrams. This is due to the fact that these three steps handle the capturing and preservation of data that can later

be used as potential digital evidence at all the five main processes (processes A to E), as seen in Figure 3. However, since the steps in the complete diagram, where all five processes are merged into one figure (Figure 9), is labelled from 1 to 38, the 3 mentioned steps (steps 36, 37 and 38) are labelled as such in Figures 4 to 8.

In the next section, the authors present a detailed diagram of Process B.

4.2.2 Invigilator and Student Venue Access Authentication

In this section, the parts of the multifactor authentication methods used to access the examination venue is presented. Note that the numbering of steps continues chronologically from the previous figure. This practice is applied in all successive figures.

Process B - (Invigilator and Student Venue Access Authentication) starts at step 3, which represents the student or invigilator going to the examination venue. In step 4, the first DFR technique labelled T1, i.e., access card and fingerprint biometric authentication, is activated just before the invigilator or student swipes their access card and also scans their fingerprint, at step 5. T1 is responsible for capturing both fingerprint features and access card details of the student or invigilator, for digital forensic readiness purposes. It is assumed that, prior to this process of biometric authentication, all students' biometric fingerprint data had been enrolled by relevant authorities of the university. When a student scans their fingerprint at the examination venue, that information is used as a reference for matching students' fingerprint features with what is stored in the institution's database.

The system, therefore, verifies whether or not the card used to swipe at the entrance and the scanned fingerprint belongs to the same person as registered on the institution's database. If the authentication is successful, the individual is granted access to the examination venue, in step 7. However, before that happens, T2, which represents the activation of surveillance cameras, in step 6, is activated to start recording all movements or activities in the examination room.

If the authentication is not successful, the system checks if it is a 3rd unsuccessful attempt, which probably indicates that an unauthorised user is attempting password guesses. If three unsuccessful attempts have not yet been detected, the individual will be allowed to retry by swiping their access card and scanning their fingerprint again, at step 8. However, if it is a 3rd unsuccessful attempt, the system will automatically block the individual, at step 9. The blocked person will have to ask the system administrator to reset their credentials on the system at step 10 before they can try to gain access to the venue, at step 5. Three unsuccessful attempts probably denote a student not being registered on the system. In such a case, a student may be required to register on the system first. If this is the case, it is also handled at step 10.

https://doi.org/10.18489/sacj.v30i1.466

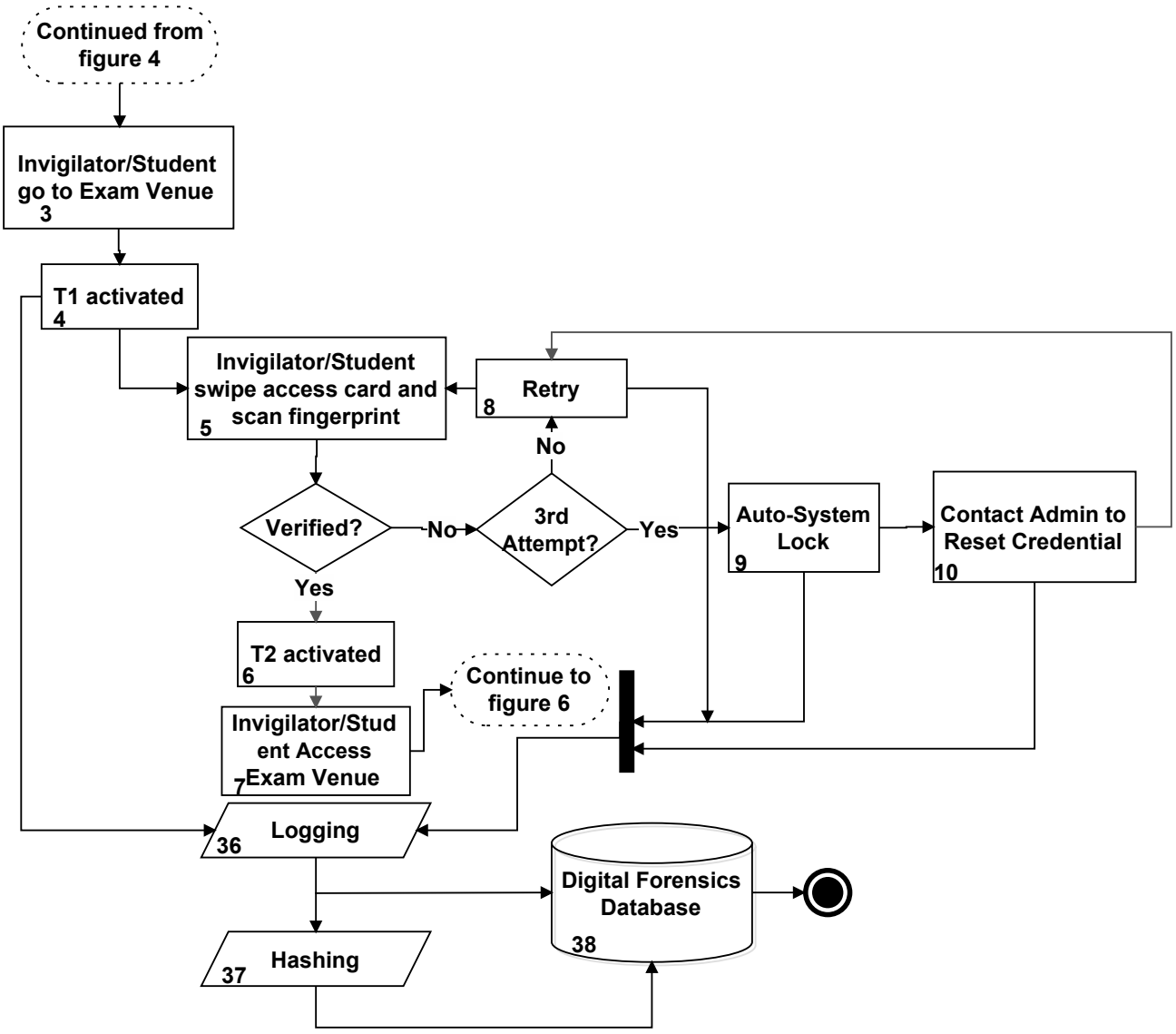

Figure 5: Invigilator and student venue access authentication

https://doi.org/10.18489/sacj.v30i1.466

When all information has been logged and preserved, at steps 36 to 38, this represents an end to process B. In the next section, the authors illustrate process C.

4.2.3 Log onto System (Workstation)

Figure 6, which is process C—log onto system, shows the process of logging onto the system (workstation) by the student before starting the online examination.

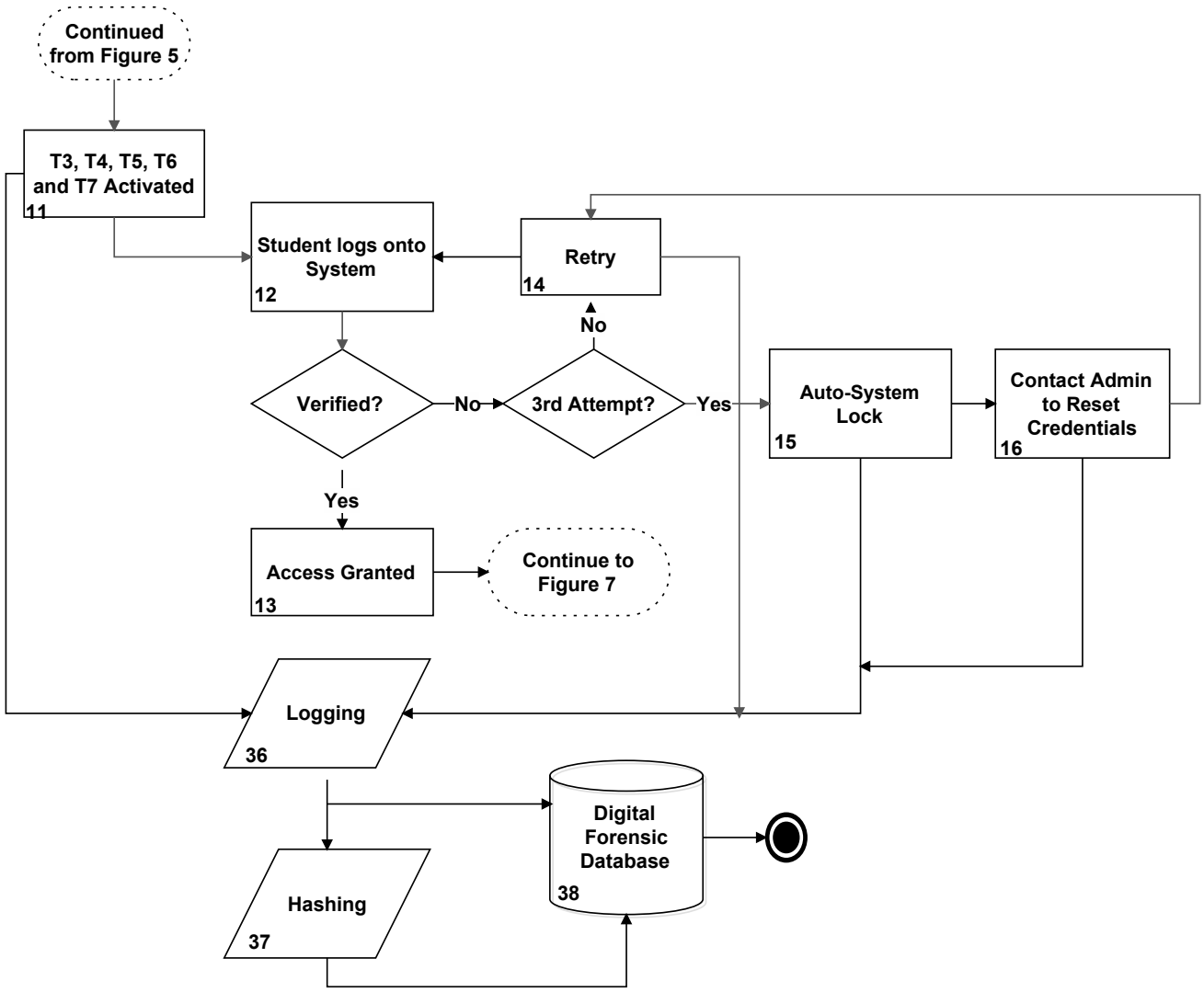

Figure 6: Student logs onto system

Before a student takes up a workstation and tries logging onto the system, five different DFR techniques are activated to start collecting data. These techniques include: keylogging (T3), PC

https://doi.org/10.18489/sacj.v30i1.466

activity logging (T4), mouse activity logging (T5), background screen recording (T6) and webcam recording (T7), as shown in step 11 of Figure 6. Visual data collected for DFR purposes at this stage, using T6 and T7 in Figure 6 and T2 in Figure 5), is a recommendation by the authors. However, for purposes of this study, it is not considered to be in the final implementation process because the authors had only limited access to computational resources during the study.

The student logs onto the system (workstation) with their username and password, in step 12. If the student enters wrong login details, access is denied and the login prompt reappears, as seen in step 14 of Figure 6, until correct details are entered. This applies only if the student did not make three unsuccessful login attempts. Three unsuccessful login attempts mean that the system will automatically lock the student out, as seen in step 15. The student will subsequently have to contact the system administrator at step 16. If a student successfully logs on to the system, then they are granted access to the system. This is shown in step 13.

In the next section, the authors illustrate the fourth stage (Process D).

4.2.4 Access Online Examination

In this section, the authors present a detailed view of process D—Access to the online examination in Figure 7.

Students proceed to open up the online examination browser and log into the examination. Here, browser logging, step 17, as another DFR technique, comes into play and it is represented as T8 in Figure 7.

When a student clicks on the online examination browser, shown in step 18, another login prompt is activated. This login attempt shows that a student attempted to open the examination. It can also act as an attendance register since it shows the student's presence and attempts to answer the examination. A student has a maximum of three login attempts to gain access to the examination, after which the system will automatically lock them out if all login attempts have failed, as seen in steps 21 and 22. If there are no login problems for the student, they are granted access to the examination and can go ahead to open the examination, as shown in step 19.

While the student attempts answering questions set in the examination, information from the time the student opens the browser to when they have access to the examination, including successful and unsuccessful login attempts, are logged and stored in the digital forensic database for future reference, as depicted in processes 36 to 38. In the next section, the authors illustrate the fifth stage of the high-level diagram, labelled as process E.

https://doi.org/10.18489/sacj.v30i1.466

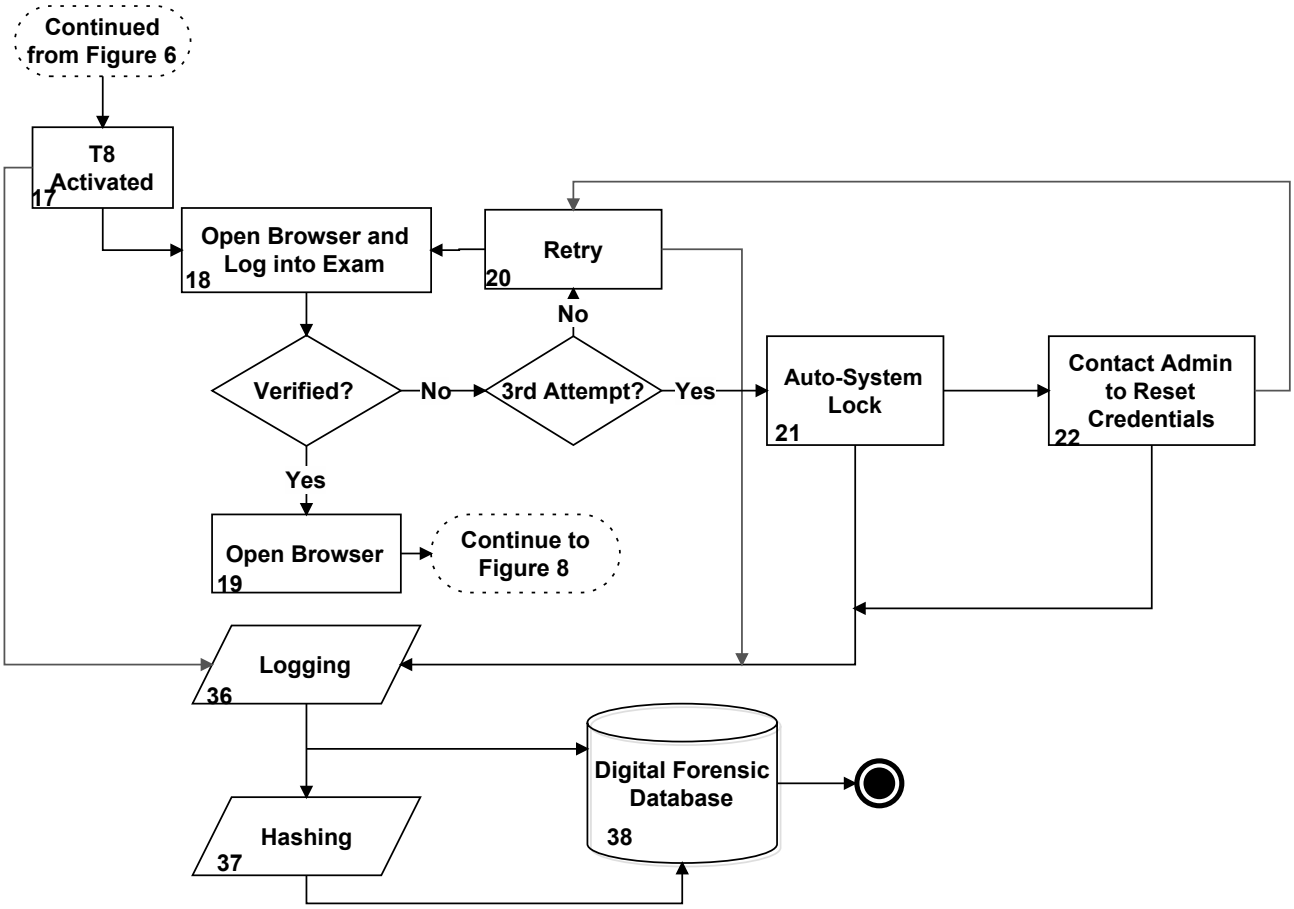

Figure 7: Access to Online Examination

https://doi.org/10.18489/sacj.v30i1.466

4.2.5 Write and Submit Examination

In Figure 8, process E—Write and submit examination—is discussed in detail.

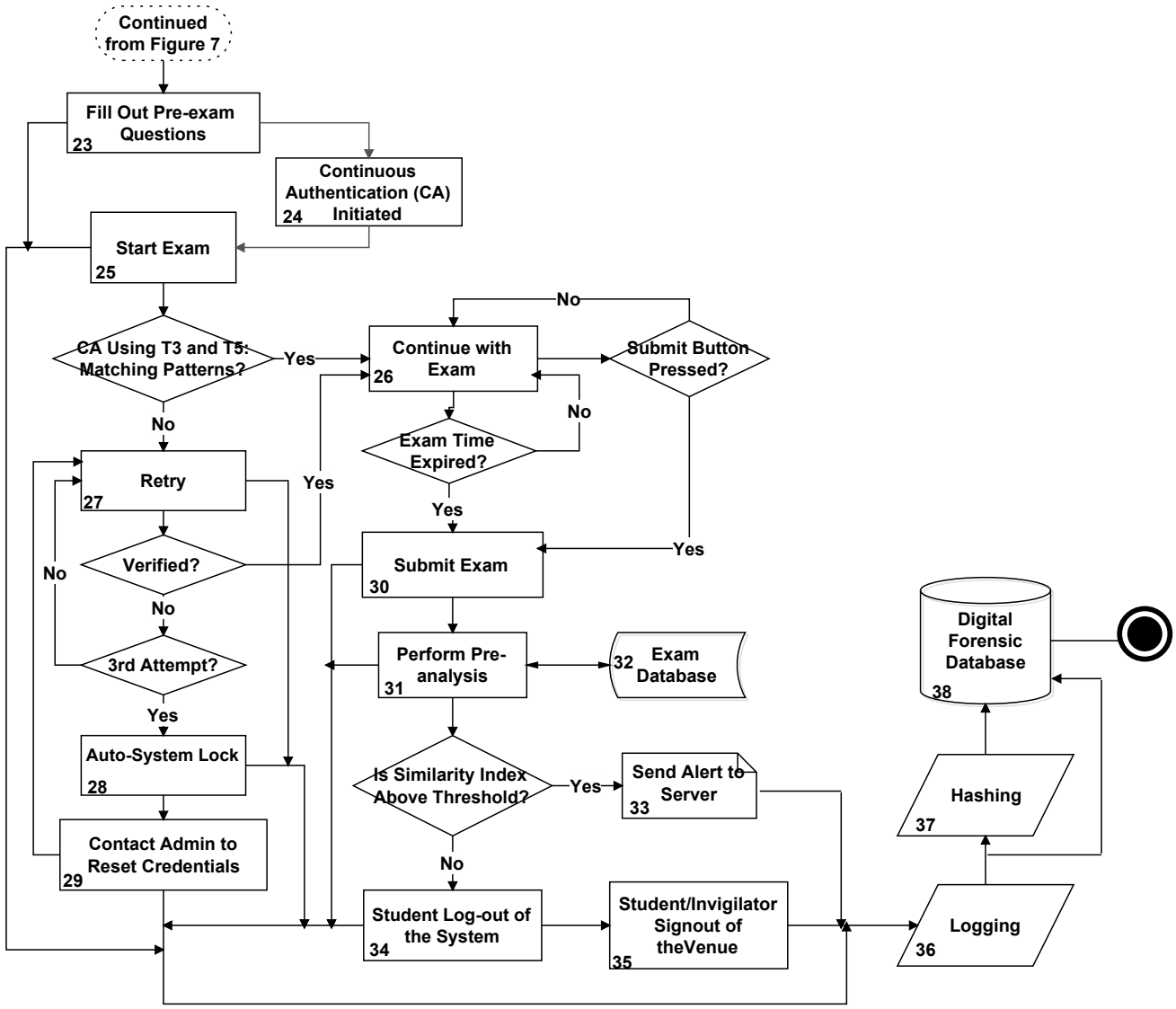

Figure 8: Write and Submit Examination

The process represented in Figure 8 starts by students filling out random questions, at step 23, before they actually start writing the examination. The purpose for this is to gather data about a student's typing habits and use of the mouse. Since the authors are using keystroke dynamics (Monrose & Rubin, 1997; Shepherd, 1995) and mouse movement dynamics as the chosen method of Continuous Authentication (CA) (Ramu & Arivoli, 2013), this information is

vital for the system to work. From this stored data, the system will keep testing the data against the student's behaviour on the workstation during the course of the examination. That is why the authors introduced step 23 in this architecture. At this step, students are asked pre-examination questions in a random order. The questions involve tying out their responses and multiple choice selections meaning they need to use the keyboard and mouse at a certain point. This is the point where the system gathers information about the student's typing dynamics and their use of the mouse. Once that information is captured and stored, CA is triggered by step 24. In the meantime, once the student answers all the questions, they can start writing the examination at step 25. The reader should note that step 24 is a background step, so the student will not know they are being authenticated until the system detects mismatching patterns, based on their typing or mouse activity. This method of CA uses an adaptive delimiter, meaning there is no fixed threshold of time intervals of when the system does the CA. This is done so as to avoid issues that may arise when a fixed delimiter is used. For instance, in the case of a fixed delimiter with a 10-minute threshold, it means every 10 minutes the system authenticates the student. However, problems might arise that, in the case that, within those 10 minutes, a student is inactive on the workstation, the delimiter will still attempt to authenticate the student as though they were still active. On the other hand, the adaptive delimiter will take into account the shortest time the student was inactive (among other inactive sessions) during step 23 and use that as the best case scenario of how long a student "rests" when using a workstation. The delimiter will set a threshold for CA based on each individual student's habits, unlike a fixed delimiter that has a fixed threshold for all students. If a mismatch is detected, the system will automatically lock the student out and the student will be required to re-log in to the system for verification. The student goes through the same verification process as before. Three consecutive failed login attempts will prompt the system to lock the student out at step 28. This would require help from the system administrator to allow the student to access the examination workstation at step 29, if they were still the legitimate student. If the system detects no mismatching typing patterns or mouse movement patterns, the student continues with the examination in step 26.

When a student finishes the examination by pressing a button to indicate that they would like to submit the examination, the system will be directed to step 30 to enable a student to submit their examination. Alternatively, if the examination time allowed has also elapsed, the system will redirect the student to submit the examination.

From that stage, the system will perform a pre-analysis of the student's answers in step 31 by cross-checking their answers with answers in the examination answer database in step 32. This is a pre-analysis check for similarities between what the student wrote and what is stored in the database of that written by other students. The authors do not expand on the specifics of the similarity index. Any suitable similarity index can be employed here. If the similarity index is above a specific similarity threshold, the system will send a red flag to the server at step 33. Raising such a red flag can indicate that, for example, a student might have copied an answer from the screen of a neighbouring student. There could also be a require help from the system administrator to allow the student to access the examination workstation at step 29, if they were still the legitimate student. If the system detects no mismatching typing patterns or mouse

movement patterns, the student continues with the examination in step 26.

When a student finishes the examination by pressing a button to indicate that they would like to submit the examination, the system will be directed to step 30 to enable a student to submit their examination. Alternatively, if the examination time allowed has also elapsed, the system will redirect the student to submit the examination.

From that stage, the system will perform a pre-analysis of the student's answers in step 31 by cross-checking their answers with answers in the examination answer database in step 32. This is a pre-analysis check for similarities between what the student wrote and what is stored in the database of that written by other students. The authors do not expand on the specifics of the similarity index. Any suitable similarity index can be employed here. If the similarity index is above a specific similarity threshold, the system will send a red flag to the server at step 33. Raising such a red flag can indicate that, for example, a student might have copied an answer from the screen of a neighbouring student. There could also be a require help from the system administrator to allow the student to access the examination workstation at step 29, if they were still the legitimate student.

If the system detects no mismatching typing patterns or mouse movement patterns, the student continues with the examination in step 26.

When a student finishes the examination by pressing a button to indicate that they would like to submit the examination, the system will be directed to step 30 to enable a student to submit their examination. Alternatively, if the examination time allowed has also elapsed, the system will redirect the student to submit the examination.

From that stage, the system will perform a pre-analysis of the student's answers in step 31 by cross-checking their answers with answers in the examination answer database in step 32. This is a pre-analysis check for similarities between what the student wrote and what is stored in the database of that written by other students. The authors do not expand on the specifics of the similarity index. Any suitable similarity index can be employed here. If the similarity index is above a specific similarity threshold, the system will send a red flag to the server at step 33. Raising such a red flag can indicate that, for example, a student might have copied an answer from the screen of a neighbouring student. There could also be an address on which the examination was answered and submitted, timestamp of when the examination was submitted and the time when the student logged out of the system, are logged by the system in step 36 and preserved for future reference through storage in a digital forensic database in step 38. A hash is created for this information, in step 37, and stored alongside the preserved information, in a digital forensic database.

Now that the five main processes, processes A to E, have been discussed in detail, they are merged into one diagram that make-up the overall OEDFRA. This is shown in Figure 9.

https://doi.org/10.18489/sacj.v30i1.466

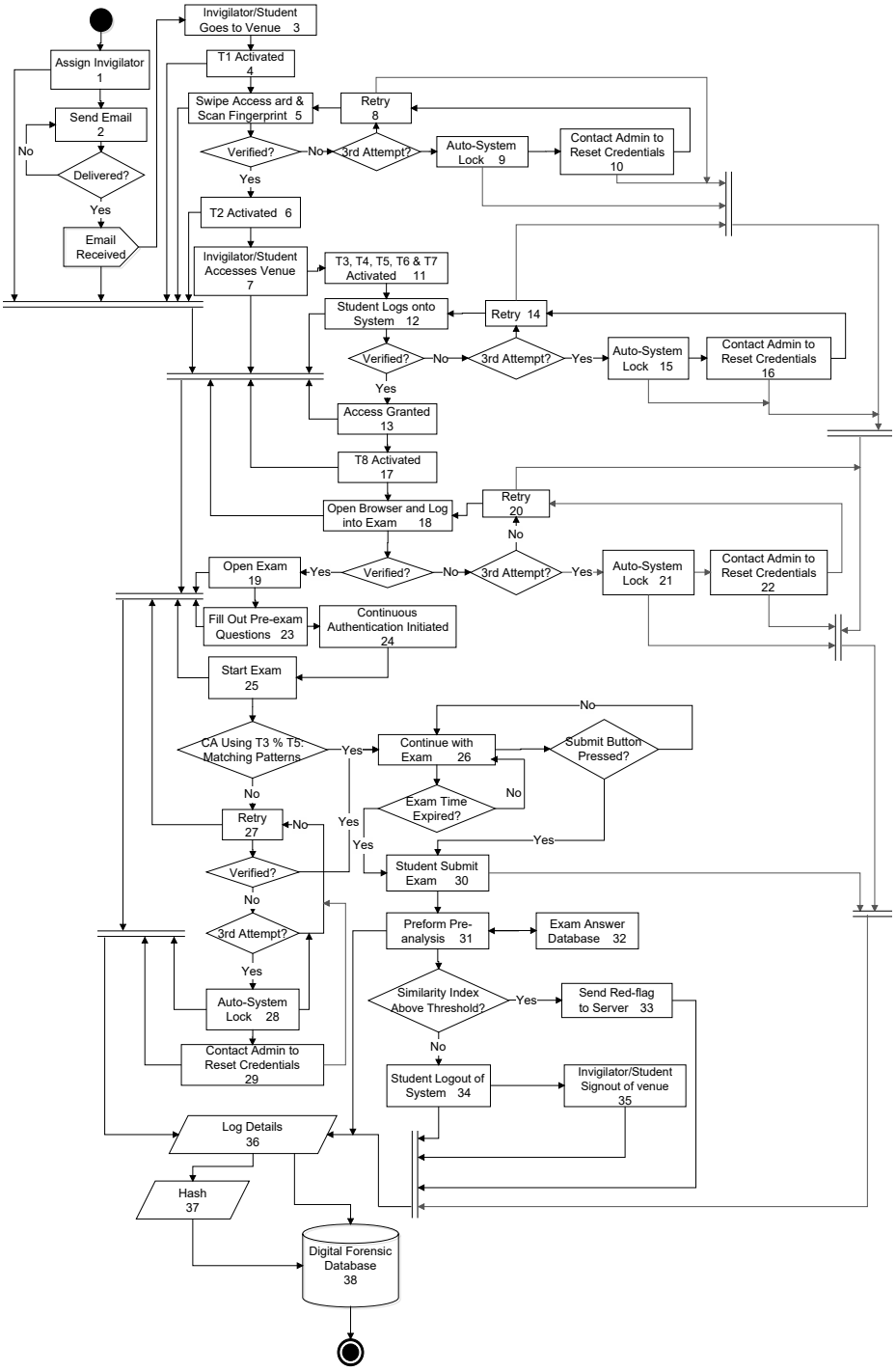

Figure 9: Detailed online examination digital forensic architecture

https://doi.org/10.18489/sacj.v30i1.466

In the next section, the authors present the preliminary results obtained from testing the proposed OEDFRA. Please note that these results are not conclusive. These results were obtained while the system was still under its initial stages of development. However, for purposes of this paper, the authors thought it would be interesting to show the reader what has been achieved so far. Further system analysis, implementation and testing is to be done once all the implementation stages, as per ISO/IEC 27043, are covered carefully, one stage after the other, together with further input from different stakeholders within the department of computer science.

5 PRELIMINARY RESULTS

These are some of the results that were obtained at the early stages of implementing the proposed Online Examination Digital Forensic Readiness Architecture (OEDFRA). Although the overall architecture has undergone more changes since then, these results are still valid as the changes to the proposed architecture do not impact in any way the results shown in the following section.

5.1 Assigning invigilators

In this section, the authors show how the invigilator (named moderator) is added to the Digital Forensic Readiness (DFR) system in Figure 10. The figure shows the invigilator's details such as username, email address, cell phone number, date of registration (the date the invigilator was added to the system) and the status. "Status" in this case refers to an invigilator who has or has not been assigned a task. If the status is "active", it means the invigilator has been assigned a task and if "inactive" the invigilator has not been assigned one. In this specific figure, the status of the named invigilator is "inactive", which means the invigilator has not been assigned to any specific examination yet. Also, at the time this result was obtained, the authors were still testing the email-sending module that is supposed to notify the invigilator of his or her specific duties therefore, this module does not appear in this paper.

To activate the invigilator, the "activate" button under the attribute "Action" is clicked on. An email will then be sent to the invigilator notifying him or her of their duties and all the necessary details they need to know. This includes details such as the time of the examination, examination venue and the likely number of students to expect on that day.

In the next section, the authors show briefly in Figure 11 how the examination questions appear from the database side. This figure is just an example of what a simple examination would look like. This was used for testing purposes and does not, in any way, reflect what the normal examination set by the university looks like.

https://doi.org/10.18489/sacj.v30i1.466

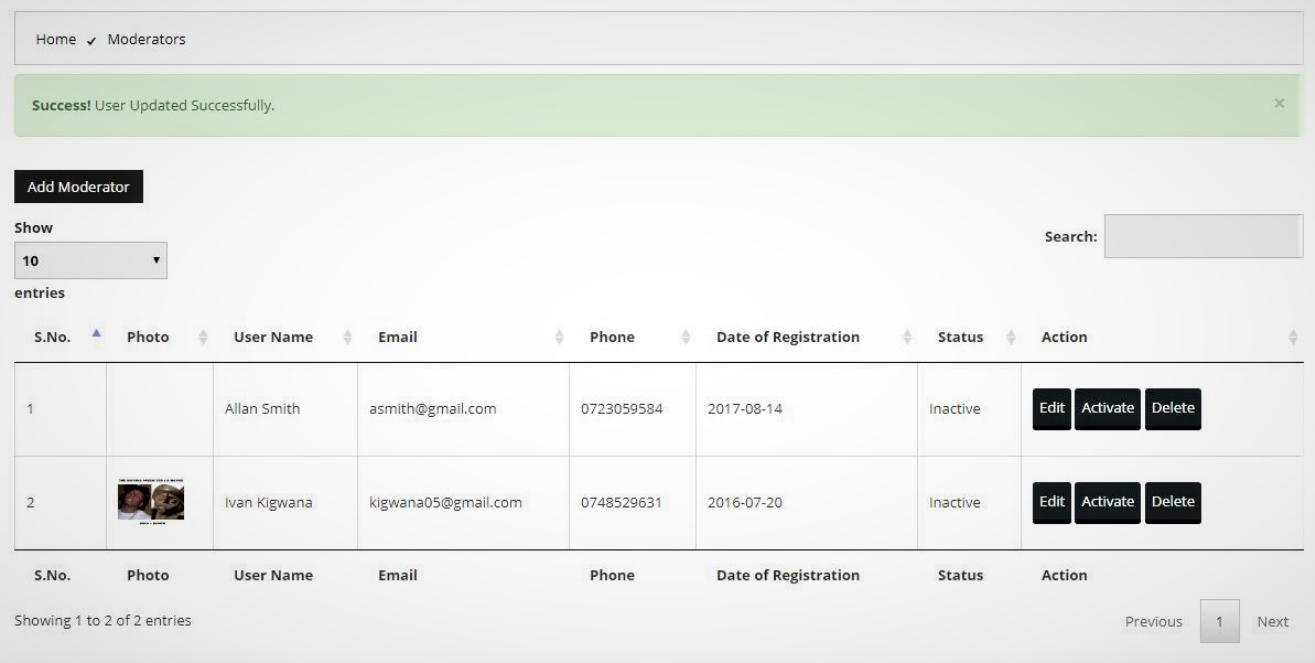

Figure 10: Assigning invigilators

	questionid	subjectid	questiontype	totalanswers	question	answer1	answer2	answer3	answer4	answer5
Edit Copy Delete	1	1	SingleAnswer	4	What does binary mean?	Means 10	Means 9	2 united states	2 states	
Edit Copy Delete	2	1	SingleAnswer	4	Who is the father of Computer Science?	Bill Gates	Steve Jobs	Mark Zuckerberg	Alan Turing	
Edit Copy Delete	3	3	SingleAnswer	4	1+1	11	10	2	6	
Edit Copy Delete	4	3	SingleAnswer	4	x*x=	2x	X	chromosomes	x squared	
Edit Copy Delete	5	2	SingleAnswer	4	Hyphothesis test includes	K1 and K2	X and Y	Ho and Ha	A or B	
Edit Copy Delete	6	2	SingleAnswer	4	What is the probability of a human flying?	0	10	100	1	

Figure 11: Overview of the examination questions

https://doi.org/10.18489/sacj.v30i1.466

5.2 Overview of examination questions

Figure 11 is an overview of the sample examination questions that were used to test the DFR system. "Question ID" shows the number of questions in that specific examination; "subject ID" is the right answer to the question being asked; "question type" shows whether the question is a single answer question, a multiple answer question or an open-ended question, i.e., a structured question requiring a student to write down the answer in essay format. "Total answers" is the total number of possible choices a student can choose from for their answer. In this case, all questions had four possible answers. "Question" is the asked question in detail and Answer 1, Answer 2, Answer 3 and Answer 4 are the choices the student could choose from to respond to the question.

The next section shows how student details are stored in the digital forensic database after students submit their examination.

5.3 Submitted examination

	id	userid	email	username	quiz_id	score	total_questions	dateoftest	timeoftest
Edit Copy Delete	1	4	new@user.com	New User	1	0	1	2016-09-09	16:05
Edit Copy Delete	2	4	new@user.com	New User	1	0	1	2016-09-09	16:17
Edit Copy Delete	3	4	new@user.com	New User	1	0	1	2016-09-09	16:36
Edit Copy Delete	4	4	new@user.com	New User	1	0	1	2016-09-09	16:48
Edit Copy Delete	5	4	new@user.com	New User	1	0	1	2016-09-15	02:16
Edit Copy Delete	6	4	new@user.com	New User	1	0	1	2016-09-16	01:30
Edit Copy Delete	7	4	new@user.com	New User	1	0	1	2016-09-16	01:55
Edit Copy Delete	8	4	new@user.com	New User	1	0	1	2016-09-16	02:06

Figure 12: Submitted examination

In Figure 12, the authors show information that is stored in the database after the students have submitted the examination. An "ID" is automatically generated by the database system showing the number of entries at the time. "User ID" shows the workstation ID where the examination was submitted from. In this example, the authors only used one workstation throughout the initial testing phase; therefore, only "user ID 4" appears in Figure 12. "Email" is the email address of the student who submitted the test and "username" is the name of the student who submitted the test.

When this system is fully implemented, the email address (as it appears in Figure 12) will be changed to reflect the email address the student used when registering with the university. The "username" will then be the student's student number. The "quiz_ID" is the identifier for that specific examination; the "score" symbolises the total score of the student at the time the

examination was submitted; "total questions" is the number of questions the student attempted to answer in the examination and "date of test" is the date the examination was written.

In the next section, the authors will show information that was captured from the keyboard on the workstation during the examination time.

5.4 Keyboard activity information

+ Options

	id	uid	keys	ip_address	timestamp	hash
Edit Copy Delete	24	4	H	196.249.56.248	2016-09-21 21:38:25	efd2b1c7fb8849ee8792dfa06000b39df20d4754
Edit Copy Delete	23	4	m	196.249.56.248	2016-09-21 21:32:26	efd2b1c7fb8849ee8792dfa06000b39df20d4754
Edit Copy Delete	22	4	m	196.249.56.248	2016-09-21 21:28:28	efd2b1c7fb8849ee8792dfa06000b39df20d4754
Edit Copy Delete	21	4	k	196.249.56.248	2016-09-21 21:28:27	efd2b1c7fb8849ee8792dfa06000b39df20d4754
Edit Copy Delete	20	4	6	196.249.56.248	2016-09-21 21:26:55	19657bffeb8ee09d72b7ef6a23471e76bc48a6a2
Edit Copy Delete	19	4	7	196.249.56.248	2016-09-21 21:26:55	ec018985d961bac71e6cab983c03252509e79ef7
Edit Copy Delete	18	4	8	196.249.56.248	2016-09-21 21:26:55	28518a2f42fdf85fccb438ebcaf2cefa1907a615
Edit Copy Delete	17	4	9	196.249.56.248	2016-09-21 21:26:54	bfb9e3cf76a569a959fb1c54ad8d8a74802acc1d
Edit Copy Delete	16	4	0	196.249.56.248	2016-09-21 21:26:51	efd2b1c7fb8849ee8792dfa06000b39df20d4754
Edit Copy Delete	15	4	½	196.249.56.248	2016-09-21 21:26:50	efd2b1c7fb8849ee8792dfa06000b39df20d4754
Edit Copy Delete	14	4	½	196.249.56.248	2016-09-21 21:26:45	efd2b1c7fb8849ee8792dfa06000b39df20d4754
Edit Copy Delete	13	4	H	196.249.56.248	2016-09-21 21:25:46	efd2b1c7fb8849ee8792dfa06000b39df20d4754
Edit Copy Delete	25	4	S	196.249.56.248	2016-09-21 21:38:27	efd2b1c7fb8849ee8792dfa06000b39df20d4754
Edit Copy Delete	26	4	6	196.249.56.248	2016-09-21 21:38:30	19657bffeb8ee09d72b7ef6a23471e76bc48a6a2
Edit Copy Delete	27	4	l	196.249.56.248	2016-09-21 21:38:38	efd2b1c7fb8849ee8792dfa06000b39df20d4754

Figure 13: Keyboard activity information

In Figure 13, the authors present keystroke activity during the time of answering the examination. The "ID" is the number of entries in the database at the time. For some reason, the entries in this figure are not in order. "U ID" is the workstation ID that was assigned to the online examination workstation on which this specific testing phase took place. As discussed in Figure 12, this testing was done on one workstation; therefore, it is the same workstation ID as in Figure 12. "Keys" are the specific keyboard keys that were pressed when attempting to answer the examination questions; "IP address" shows the IP address of the workstation at the time this examination was taken. The IP address, workstation ID and the student's email address (in Figure 12) are solid digital information because this information places the student at that workstation at the time the examination was written.

https://doi.org/10.18489/sacj.v30i1.466

"Timestamp" shows the time the examination commenced from that specific workstation and the hash is meant to protect the integrity of this digital information in case this information is required in the future for any reason, including an investigation into possible examination fraud. If, at any point, the hash is different from the initial hash function that was created, then this information cannot be used as potential digital evidence, because its integrity cannot be relied upon anymore. If, however, the information was not tampered with, the hash will stay the same. This means the information is still valid as potential digital evidence and can be used in a disciplinary hearing into online examination fraud.

Although the results are inconclusive at this stage, these results show that it is possible to achieve DFR in online examinations. More testing is still required on this system and when that is done, a fully completed prototype publication will be released.

In the next section, the authors present an evaluation of the proposed OEDFR architecture.

6 EVALUATION OF THE PROPOSED ARCHITECTURE

In this section, the authors discuss how the proposed OEDFRA can be applied towards achieving DFR in online examinations. The contribution of the OEDFRA is that it focusses mainly on refining the DFR planning and preparation process, as described by ISO/IEC 27043:2015, for online examination fraud. In the next section, the authors discuss the evaluation of the proposed architecture in detail.

6.1 Evaluation of the OEDFRA

DFR applications deployed in this proposed architecture are used to capture information from students writing the examinations, some of which include private information. A student might perceive the capturing of their information as an act of invasion of their privacy. However, since this architecture will be used in a university or educational environment where the institution has the right to institute its own policy rules and regulations governing online examinations, this can be spelt out clearly to students in the form of "online examination rules and regulations" or as part of the university policies, to which the student needs to sign consent. Also, since this information, i.e., the recorded DFR data, is used strictly for legal purposes and is only accessible by authorised personnel, for instance digital forensic investigators, the institution can use this to defend its decision for capturing such data from students. Beyond the university's jurisdiction, there are laws and Acts (RSA Department of Justice, 2013a, 2013b; Scolnik, 2009; Association of Chief Police Officers, 2012; Doyle, 2012) that allow for the capture of sensitive information from an individual only if that information is required by law enforcement agencies and it is to be used in courts of law or any other disciplinary committees. This does not constitute an infringement of a student's right to privacy unless such information can lead to a criminal conviction, for instance, OEF against a student, in a disciplinary hearing.

The architecture presented shows that, by using proper procedures to capture information for DFR purposes, sufficient forensic preparedness can be achieved from information that has been

digitally preserved. The authors believe that in case there is an incident that has been detected, the institution's authorities responsible for online examination regulations, together with digital forensic investigators and perhaps witnesses, such as invigilators and fellow students, should refer to the institution's policies and procedures on handling potential digital evidence data, before a DFI process is formally initiated.

The authors emphasise that having such architecture in place can contribute greatly towards achieving DFR in an online examination environment. From this, digital forensic investigators are able to extract enough data and information that can be used in a disciplinary hearing into online examination fraud. Such extracted potential digital evidence can easily be admissible evidence when needed. For this, the task of data analysis would be eased, especially when using forensically-ready data that had been captured and adequately preserved.

As part of the authors' continuation to evaluate the proposed architecture, the authors studied some of the related work by other scholars, as far as online examination fraud is concerned and the solutions they proposed. This is explained in the next section and related to the proposed OEDFRA.

6.2 Related work

In this section, a continuation of the evaluation is presented in form of related work from other scholars. A comparison is made between what other researchers have done and what the authors of this paper have proposed.

Ramu and Arivoli (2013) proposed a framework of authentication in online examinations using biometrics. The authors of this study proposed this framework as an alternative for traditional paper-based examinations. In their study, the authors investigated existing potential threats in authenticating students who do online examinations. This is due to the fact that in most online examination settings, there is no face-to-face interaction when a student is submitting their examination, so it is not easy to tell if the registered student indeed completed the examination themselves or they had outside help. The authors later analyzed the benefits and limitation of existing approaches as far as student authentication is concerned. From that point, the authors proposed their framework. The proposed framework uses a multi-modal authentication mechanism to secure examinations through the use of keystroke dynamics and knowledge-based authentication. This was a great contribution but the benefit of our approach over this approach is that authentication using keystroke dynamics constitute one component of the whole system. Ramu and Arivoli's framework does not take into account any element of digital forensic readiness nor did it follow any specific international digital forensic standard when it was designed. Where there is any allegation that a student indeed received outside help while writing the examination and the university needs to prove its case, such information cannot be used as potential digital evidence, because the evidence integrity is unreliable.

Impara, Kingsbury, Maynes, and Fitzgerald (2005) proposed a way of detecting cheating in computer adaptive tests using data forensics. The authors of this paper mentioned different ways of how cheating can occur, for instance, using forbidden materials like cheat sheets, text messaging,

collusion and, worse, by teacher or invigilator involvement to help students pass tests through substituting wrong answers with correct ones, among other methods. From that angle, the authors proposed using data forensics to detect examination fraud using aberrance indicators (unusual response times and unusual response patterns). In their work, the authors observed aberrance by taking into account inconsistencies an examination taker demonstrates when answering test questions in a manner different from demonstrated behavior and knowledge. The authors gave an example of inconsistencies that may arise, for instance, in the amount of time taken to respond to test questions and also the student's answer selection that is inconsistent when compared to other tests taken by the same student. The solutions provided by these authors yielded great results (Impara et al., 2005), however, in their study, the authors do not mention whether they followed any international digital forensic standard when carrying out this study or when making their propositions. Also, the authors did not mention what happens to the data collected from students. They do not mention whether this data is stored in a forensically-sound manner or stored as is, without any regard to its integrity. In our study, maintaining the integrity of all collected digital information, while following a well-known international standard, is crucial in giving our contribution an upper-hand, compared to what Impala, Kingsbury, Maynes et al did.

Burke (2009) conducted a study that involved procedures of preserving the integrity of online examinations or testing. In his work, the author proposed procedures to defend against unauthorised access to online examinations. These procedures catered for both live examination assessments and also a continuous external check of processes, to make sure procedures put in place to manage the security of the tests are still working. This was achieved by use of what the author called "web patrols", which was supported by data forensic audits. These web patrols were deployed to search internet sites for any potential security breaches, for instance, brain dump sites, pirate sites and any other sites that inappropriately provide access to educational content to anyone via the internet. These web patrols, together with data forensic algorithms, were tasked to look for inconsistencies and variations that would be unlikely to happen under normal conditions. For instance, fast response rates and high correct answer rates, could indicate that someone had access to answers prior to doing the test. This was a great study with good findings; however, similar to other researchers mentioned earlier, the author did not take into account any international digital forensic standard when conducting his research. He also does not mention how he intends to protect the integrity of all information captured using the data forensic algorithm, does not mention what happens when there is a suspicion that a student committed fraud, whether the system lock out the student, or whether the student is allowed to continue with the test. However, in our study, we followed the process of ISO/IEC 27043 and also provided a way of protecting the integrity of captured information, which is required for forensic analysis.

Other authors who proposed a solution to online examination fraud include Rodchua, Yiadom-Boakye, and Woolsey (2011), who proposed a system for student verification in online examinations as a way to improve quality and integrity of distance learning. These researchers proposed a model to support integrity and quality of online assessments. Their model makes use of facial recognition, video surveillance and computer access restriction software, all incorporated into a

system to minimise unauthorised entry. However, these researchers, too, did not follow an international standard, nor did they apply any DF capabilities in their work, which makes it hard to use their digital information as viable potential digital evidence.

Beck (2014), Nixon (2004) and Siyao and Qianrang (2011) all carried out studies in online examination cheating and how best it can be resolved. However, one thing they all have in common is that none of these studies followed any international digital forensic standard when being carried out. Also, they did not include any digital forensics aspect in their studies while conducting online examinations involving digital devices.

There was literature on other, similar studies but the authors picked the ones that were discussed, as we were of the opinion that those were the most noteworthy studies, apart from ours, conducted in the field.

In a nutshell, our contribution in this study can be used as an enhanced solution to already existing solutions as far as cheating in online examinations is concerned. The existing solutions are good, however, most of them did not follow proper DF guidelines and all of them (those mentioned in this specific study) did not follow any recognised international standard whilst being designed and/or implemented. In this study, the authors followed the ISO/IEC 27043:2015 international standard when designing the proposed architecture. All DFR steps and guidelines, as mentioned in the standard, were followed in this study, to make it more likely that any potential digital evidence captured, following our architecture, is much more likely to be admissible in legal proceedings or a disciplinary hearing. Table 3 is a summary of the comparison made from other researchers' work to our study in this paper. The ✓ represents "Yes" and the x represents "No".

Table 3: Comparison of other researchers' findings and our study

Authors	**Abbreviated topic**	**Applied DF**	**Applied DFR**	**Followed Intl Std**
Ramu and Arivoli (2013)	Biometric-based online examination authentication	x	x	x
Impara, Kingsbury, Maynes, and Fitzgerald (2005)	Detecting cheating in computer adaptive tests using data forensics	✓ (Data forensics)	x	x
Burke (2009)	Preserving the integrity of online testing	✓ (Data forensics)	x	x
Rodchua, Yiadom-Boakye, and Woolsey (2011)	Student verification for online assessments	x	x	x
Beck (2014)	Model to predict online cheating	x	x	x
Nixon (2004)	Cheating in cyberspace	x	x	x
Siyao and Qianrang (2011)	Anti-cheating strategy of online exams	x	x	x
Kigwana and Venter (2016)	A digital forensic readiness architecture for online exams	✓	✓	✓ (ISO/IEC 27043:2015)

7 CONCLUSION AND FUTURE WORK

This paper proposed architecture for gathering digital information that can be used for DFR purposes in an online examination environment, through the OEDFRA.

The contribution made by the paper shows that it is possible to gather digital forensic-ready data and/or information for legal purposes using different techniques, as mentioned in the paper. These techniques are used to collect potential digital evidence admissible in a disciplinary hearing concerned with online examination fraud.

The OEDFRA can be used by educational institutions to be forensically well prepared for when there is suspicion of online examination fraud and a need for a DFI into the matter when the need arises. The authors showed how online examinations face a lot of challenges, most of which deal with examination cheating and the fact that there exists no DFR architecture for gathering potential digital evidence in an online examination environment.

As part of the authors' future work, the plan is to implement the current architecture as a prototype and to thoroughly test it at an educational institution. In addition, the further aim is to develop the architecture into a standardised architecture to support different online examination systems, to enable DFR processes in all online examination environments.

References

Association of Chief Police Officers. (2012). ACPO Good Practice Guide for Digital Evidence. Last accessed 01 Jul 2018. Retrieved from http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Beck, V. (2014). Testing a model to predict online cheating—Much ado about nothing. *Active Learning in Higher Education*, *15*, 65–75. https://doi.org/10.1177/1469787413514646

Burke, E. (2009). Preserving the integrity of online testing. *Industrial and Organizational Psychology*, *2*, 35–38. https://doi.org/10.1111/j.1754-9434.2008.01104.x

Carrier, B. & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*, 1–20.

Clark, R. C. & Mayer, R. E. (2016). *E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning*. John Wiley & Sons Inc. https://doi.org/10.1002/9781119239086

Crown, D. F. & Spiller, M. S. (1998). Learning from the literature on collegiate cheating: A review of empirical research. *Journal of Business Ethics*, *17*, 683–700.

Dawson, P. (2016). Five ways to hack and cheat with bring-your-own-device electronic examinations. *British Journal of Educational Technology*, *47*, 592–600. https://doi.org/10.1111/bjet.12246

Doyle, C. (2012). Privacy: An overview of the electronic communications privacy act. Last accessed 01 Jul 2018. Retrieved from https://fas.org/sgp/crs/misc/R41733.pdf

Freifeld, L. (2013). Securing exams against fraud. Last accessed 30 Jun 2018. Retrieved from http://www.trainingmag.com/content/securing-exams-against-fraud

Furnell, S. & Karweni, T. (2001). Security issues in online distance learning. *Vine*, *31*, 28–35. https://doi.org/10.1108/03055720010803998

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Forensic Research Workshop*, *7*, S64–S73. https://doi.org/10.1108/03055720010803998

Gereda, S. (2006). The electronic communications and transactions act. In L. Thornton (Ed.), *Telecommunications law in South Africa*. STE.

Gibbons, A., Mize, C. D., & Rogers, K. L. (2002). That's my story and I'm sticking to it: Promoting academic integrity in the online environment. Last accessed 30 Jun 2018. Retrieved from https://eric.ed.gov/?id=ED477016

Hylton, K., Levy, Y., & Dringus, L. P. (2016). Utilizing webcam-based proctoring to deter misconduct in online exams. *Computers & Education*, *92*, 53–63. https://doi.org/10.1016/j.compedu.2015.10.002

Impara, J. C., Kingsbury, G., Maynes, D., & Fitzgerald, C. (2005). Detecting cheating in computer adaptive tests using data forensics. In Proceedings of the Annual Meeting of the National Council on Measurement in Education and the National Association of Test Directors, Montreal, Canada, 2005.

International Standards Organization. (2012). ISO/IEC 27037:2012—Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence. Last accessed 30 Jun 2018. Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381

International Standards Organization. (2015a). ISO/IEC 27041:2015—Information technology—Security techniques—Guidance on assuring suitability and adequacy of incident investigative method. Last accessed 30 Jun 2018. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27041:ed-1:v1:en

International Standards Organization. (2015b). ISO/IEC 27042:2015—Information technology—Security techniques—Guidelines for the analysis and interpretation of digital evidence. Last accessed 30 Jun 2018. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en

International Standards Organization. (2015c). ISO/IEC 27043:2015—Information technology—Security techniques—Incident investigation principles and processes. **D**OI?

International Standards Organization. (2015d). ISO/IEC 30121:2015—Information technology—Governance of digital forensic risk framework. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:30121:ed-1:v1:en

Kebande, V. R. & Venter, H. S. (2014). A cloud forensic readiness model using a botnet as a service. In Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014) (pp. 23–32).

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. NIST Special Publication.

Kigwana, I. & Venter, H. (2016). Proposed high-level solutions to counter online examination fraud using digital forensic readiness techniques. In Proceedings of the 11th International Conference on Cyber Warfare and Security: ICCWS2016 (p. 407).

King, C. G., Guyette Jr, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *Journal of Educators Online*, *6*, n1.

Kohn, M. D., Eloff, M. M., & Eloff, J. H. (2013). Integrated digital forensic process model. *Computers & Security*, *38*, 103–115. https://doi.org/10.1016/j.cose.2013.05.001

Monrose, F. & Rubin, A. (1997). Authentication via keystroke dynamics. In Proceedings of the 4th ACM conference on Computer and communications security, (pp. 48–56). Association for Computing Machinery. https://doi.org/10.1145/266420.266434

Nixon, M. (2004). Cheating in cyberspace: Maintaining quality in online education. *AACE Journal*, *12*, 85–99.

Oxford Dictionaries. (n.d.). Architecture—Definition of architecture in English by Oxford Dictionaries. Last accessed 30 Jun 2018. Retrieved from https://en.oxforddictionaries.com/definition/architecture

Palmer, G. (2001). A road map for digital forensics research—Report from the first Digital Forensics Research Workshop (DFRWS). Last accessed 01 Jul 2018. Retrieved from http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

Ramu, T. & Arivoli, T. (2013). A framework of secure biometric based online exam authentication: An alternative to traditional exam. *International Journal of Scientific and Engineering Research*, *4*(11), 52–60.

Renard, L. (1999). Cut and paste 101: Plagiarism and the net. *Educational Leadership*, *57*, 38–42.

Rodchua, S., Yiadom-Boakye, G., & Woolsey, R. (2011). Student verification system for online assessments: Bolstering quality and integrity of distance learning. *Journal of Industrial Technology*, *27*.

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, *2*, 1–28.

RSA Department of Justice. (2013a). Protection Of Personal Information Act.

RSA Department of Justice. (2013b). Regulation of Interception of Communication and Provision of Communication-Related Information Act.

Scanlon, P. M. (2003). Student online plagiarism: How do we respond? *College Teaching*, *51*, 161–165.

Scolnik, A. (2009). Protections for electronic communications: The stored communications act and the fourth amendment. *Fordham Law Review*, *78*.

SecurEnvoy. (2017). What is 2FA? Last accessed 30 Jun 2018. Retrieved from https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm

Shepherd, S. (1995). Continuous authentication by analysis of keyboard typing characteristics. In Proceedings of the European Convention on Security and Detection, Brighton, UK, 1995 (pp. 111–114). https://doi.org/10.1049/cp:19950480

Siyao, L. & Qianrang, G. (2011). The research on anti-cheating strategy of online examination system. In Proceedings of the 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011, (pp. 1738–1741).

Spencer, J. (2014). *Hearsay evidence in criminal proceedings*. Bloomsbury.

Sterngold, A. (2004). Confronting plagiarism: How conventional teaching invites cyber-cheating. *Change: The Magazine of Higher Learning*, *36*, 16–21.

TechTarget. (2017). Two-factor authentication (2FA). Last accessed 30 Jun 2018. Retrieved from http://searchsecurity.techtarget.com/definition/two-factor-authentication

Welsh, E. T., Wanberg, C. R., Brown, K. G., & Simmering, M. J. (2003). E-learning: Emerging uses, empirical results and future directions. *International Journal of Training and Development*, *7*, 245–258. https://doi.org/10.1046/j.1360-3736.2003.00184.x