COMPUTER FORENSICS FOR COMPUTER-BASED ASSESSMENT: THE PREPARATION PHASE

R. Laubscher[1], M.S. Olivier[2], H.S. Venter[3], D.J. Rabe[4], J.H.P. Eloff [5]

[4]Stellenbosch University, CIS department

Information and Computer Security Architectures (ICSA) Research Group

Department Computer Science

University of Pretoria

[1](rut@ma2.sun.ac.za)

[2](http://mo.co.za)

[3](hventer@cs.up.ac.za)

[4](castor@ma2.sun.ac.za)

[5](eloff@cs.up.ac.za)

When conducting a computer-based assessment, several infringements of assessment regulations could arise. Examples are illegal communication (e.g. by email, web, cell phone), hiding of computer objects with the aim of accessing or utilizing it, impersonation of another learner and presenting the project of another learner. If infringement is suspected, a computer forensic investigation should be launched. Almost no academic institution has a computer forensic department that can assist with a computer forensic investigation and therefore the responsibility rests upon the lecturer.

The purpose of this project is to apply forensic principles to a computer-based assessment environment in order to facilitate the identification and prosecution of any party that contravenes assessment regulations. The aim of the current paper is to consider the nature of a forensic ready computer-based assessment environment in more detail. This nature is derived from established computer forensic principles. In particular the focus is on the forensic process to determine the policies, procedures, processes and types of tools that should be present in such an environment. The computer-based assessment forensic process proposed in an earlier paper consists of four phases: 1) preparation of the environment, 2) collection of evidence, 3) analysis of evidence and 4) reporting the findings. The current paper will focus on the first step.

The utilization of different forensic tools for evidence collection and analysis used for cross-checking namely a key logger, CCTV camera, audit logs and a report of logins, will facilitate identification of any party that contravenes assessment regulations. The primary tool proposed in this paper is the key logger. The proposed process forms the backbone of the forensic process.

Computer-based assessment, privacy, computer forensic process, computer evidence, forensic readiness and key logger.

COMPUTER FORENSICS FOR COMPUTER-BASED ASSESSMENT: THE PREPARATION PHASE

1 INTRODUCTION

When conducting a computer-based assessment at an educational institution, several infringements of assessment rules could arise. Examples are illegal communication (e.g. by email, web, cell phone), hiding of computer objects with the aim of accessing or utilizing it, impersonation of another learner and presenting the project of another learner. If infringement is suspected, a computer forensic investigation should be launched. Almost no academic institution has a computer forensic department that can assist with a computer forensic investigation, and therefore the responsibility rests upon the lecturer.

The purpose of this project is to apply computer forensic principles to a computer-based assessment environment enabling the identification and prosecution of any party who contravenes assessment regulations. In previous work Laubscher et al (2005a) considered the application of forensics on the entire assessment process from a high level. The aim of the current paper is to consider the nature of a forensic ready computer-based assessment environment in more detail. In particular we will focus on the forensic process to determine the policies, processes, infrastructure and types of tools that should be present in such an environment.

The remainder of this paper is structured as follows: Section 2 provides an overview of previous work. Section 3 describes the computer forensic requirements for computer-based assessments. Section 4 discusses some privacy issues. Requirements regarding policies are discussed in section 5. Section 6 discusses the forensic tools for the computer-based assessment forensic process. Section 7 elaborates on the first phase of the computer-based forensic process, by proposing sub phases within the preparation phase. Sections 3, 4, 5, 6 and 7 form the main contribution of the current paper. The conclusions and future research are presented in section 8.

2 PREVIOUS WORK

Notwithstanding with security measures in place (for example the presence of invigilators, access control, and authentication), the risk for dishonest behaviour in computer-based assessments is high, because learners find innovative methods to violate assessment regulations or break through the already installed computer security controls. Fraud in paper-based assessment environments is already hard to prove where dishonest learners typically employ physical aids. In a computer-based assessment environment, many such possible aids become invisible: sending and receiving email, utilising a cell phone via Bluetooth, and accessing storage media by wireless (or inconspicuously wired) means are hard to notice during normal invigilation — and the illicit use of such technologies is in all likelihood harder to prove to a disciplinary committee after the assessment.

One of the academic responsibilities of a lecturer is to certify that each learner has mastered the subject area to the degree reflected in the marks awarded. This implies a dual duty for an assessment invigilator. On the one hand the invigilator must provide an environment in which the learner can be treated according to his or her right to privacy during the assessment session,

enabling the candidate to complete the assessment with as few distractions as possible. On the other hand the invigilator must also be able to determine, beyond reasonable doubt, which resources, legitimate and illicit, were used to complete the assessment.

The computer forensic process proposed in an earlier paper (Laubscher et al, 2005a) consists of four phases: 1) preparation of the environment, 2) collection of evidence, 3) analysis of evidence and 4) reporting of findings. The first step of the computer-based assessment forensic process is to provide a controlled assessment environment. Institutional policies should be in place prior to the assessment, preferably when learners commence their studies. A policy should permit monitoring of electronic activities, even if it means justifiable invasion of the privacy of the learner. The learner will be required to sign an acceptance of the policy and to give consent to be monitored and investigated if a possible contravention is detected. It is the **first step** that constitutes the focus of the current paper.

In order to provide the context for the work contributed by this paper, a brief overview of the forensic process together with the relevant phases, described in earlier work (Laubscher et al, 2005a) is given.

During the **first phase** (preparation) the controlled environment will be prepared prior to the assessment. The activities include: casting all computers with a previously set-up computer image, activation of the key logger software, logs and CCTV camera and verification that the time and dates of all computers are correct and identical. On arrival of the learners, the invigilators randomly allocate learners to computer workstations and announce the assessment regulations (also included in the question paper). The learners sign consent to be monitored (with key loggers and CCTV camera) for the purpose of evidence collection for possible misconduct.

In the **second phase** (evidence collection) the computer-based assessment is conducted. The main tools for collecting digital evidence are key loggers capturing the learner's keyboard and mouse actions and logs recording electronic activities. Additionally, an invigilator monitors the login activities frequently by generating reports indicating the following details: user names, workstation identity and date and time stamps. The invigilator will save these reports for electronic evidence to a file. The motivation for this is to detect, as soon as possible, if a learner attempts to impersonate another user. More than one invigilator should be present in the computer lab where the assessment is conducted. The CCTV camera records all activities within the computer lab during the computer-based assessment.

The **third phase** (analysis) in the proposed forensic process starts after completion of the assessment. Back-ups of all files (i.e. key logger files, logs, login reports and final assessments of learners) should be made to a separate computer or other trusted computer storage media. This computer or computer media should be write-protected and virus free. This computer could also be cast from the initial virus-free computer. The learner's access rights, issued for the submitted assessment on the network, should be revoked. This is important for the chain-of-custody, to protect the evidence data against modification or deletion. All accesses to the data after preservation must be traceable for the chain-of-custody. Only then will the CCTV camera, the key logger and logs be disabled. The videotape and other computer storage media should be tagged, bagged and then locked away in a secure locker.

An initial systematic scanning of all electronic evidence collected will be analysed for suspected activities that transgresses the assessment's regulations. It is possible to confirm deviations found in one evidence source, by cross checking with the other sources of evidence. If dishonesty is suspected, a comprehensive computer forensic analysis will be conducted. In the **fourth phase** (reporting) the findings will be reported to the examination board and authorities.

The purpose of the proposed four-phase process is to collect different types of evidence for analysis which act as indicators that regulations have been transgressed. Confirmation could be achieved by cross-checking the different sources of evidence. This forms the basis of proving that dishonesty has been committed during the computer-based assessment.

3 COMPUTER FORENSIC REQUIREMENTS FOR COMPUTER-BASED ASSESSMENT

The academic environment, where the forensic process will be executed, is different from traditional crime scenes for the following reasons: the potential crime domain is controlled, the initial investigator is not necessarily a forensic expert and the identification and investigation of misconduct should be dealt with in a very short time-span. It is very important to detect any suspected behaviour in a computer-based assessment as quickly and accurately as possible, because the assessment should be evaluated, moderated and the results published within a limited time.

In this section the following identified forensic requirements for computer-based assessments are discussed: forensic readiness, time synchronization, permissions to investigate or collect evidence, adhering to legal requirements, permissions to monitor computer behaviour, digital evidence controls, forensically sound investigation, chain-of-custody and forum for monitoring of the forensic process.

3.1 Forensic readiness

"Forensic readiness can be seen as the ability of an organization to maximize its potential to use digital evidence when required" (Rowlingson, 2004). Although digital forensic investigations are commonly employed as a post-event response to a serious information security or criminal incident (Rowlingson, 2004), when forensics is used to its potential, it can provide both pre- and post event benefits (Armstrong, 2002). If an Academic institution is not forensically ready, then the necessary evidence, either exists, and hopefully is found by the digital forensic investigation, or it does not exist at all and a suspect (learner) cannot be charged and prosecuted (Rowlingson, 2004). Activation of key loggers, a CCTV camera and audit logs, during the preparation phase of the computer-based assessment forensic process, could enhance the potential to have useful digital evidence in case of misconduct.

A controlled environment, such as the computer-based assessment environment, makes it easier to collect evidence compared to other crimes committed from unknown sources and by unknown criminals. Forensic readiness is enhanced because the following are known information in a controlled environment encountered with computer-based assessments: personal information concerning the potential criminals (id number, name, logon name, student number), time-slot, known sources and the possible origin (workstation number) of the misconduct. Although certain

new procedures will be necessary to implement forensic readiness, it should not entail a whole new set of procedures. Forensic readiness may be achieved through enhancement of existing policies, such as data retention, incident response, information security, and crime prevention. Policies will be discussed in Section 5.

3.2 Time synchronization

Boyd & Forster (2004) suggests that special care should be taken to ensure the *authentication* and *integrity* of the time and date stamps of the objects in evidence collection. Electronic documents will only stand up in court if the *who*, *what* and *when* they represent are unassailable (Tan, 2001). In the preparation of the computer lab, before the computer-based assessment commences, the CMOS time on each workstation and the server could be verified and synchronised in relation to actual time, obtainable using radio signal clocks or via the Internet using reliable time-servers. In order to protect the learners from changing the time and date on the workstation or server, no write-access to settings should be given to the learners.

3.3 Permission to investigate or collect evidence

Usually after detecting that a crime is committed, the law enforcers should issue a search warrant, before the investigation could commence. Computer-based assessment forensics needs permission to collect evidence and analyse the evidence even before one suspect's misconduct. Nelson et al (2004:15) state that **well-defined policies** give computing investigations and forensic examiners the authority to conduct private investigations such as those where learners infringe assessment regulations. The executive management of the Academic institution should define and limit who is authorized to conduct an initial forensic analysis and request a more comprehensive forensic investigation and analysis to avoid trivial or inappropriate investigations.

3.4 Adhering to legal standards

Infringement of assessment regulations fall in the category of **non-liturgical** investigation: one that is not foreseen to be taken to trial or involve litigation. However, one should always conduct the investigation using the same procedures as if you are going to trial (Marcella & Greenfield, 2002:19).

The treatment of electronic evidence in court is still a new area with regard to the admissibility of computer-produced evidence (Brungs & Jamieson, 2005). Computer-generated data such as logs is **not hearsay**. Computer-stored records that a person generates are subject to the governing hearsay evidence (Marcella & Greenfield, 2002:264). To qualify as a business-record exception to the hearsay rule, a person must have created the computer-stored records, and the records must be original. Federal Rules of Evidence treat printouts of digital files and bit-stream image copies as original evidence.

3.5 Permission to monitoring computer behaviour

One of the primary tools employed for evidence collection for a computer-based assessment is a key logger. A key logger (software or hardware implemented) records all keyboard and mouse actions. This monitoring process results in invasion of the learner's right to privacy: a personal profile could be built for a specific learner. Special consideration should be given to a person's right to privacy; especially if that right is invaded. The question to be answered: is it fair? Given the importance of this requirement, we devote Section 4 to the answering of this question.

3.6 Digital evidence controls

According to Ashcroft (2001) electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device. Electronic evidence is fragile and can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve and examine this type of evidence. Once the evidence is collected, precise backups of the media containing the evidence should be made and stored in a secure locker or on a secure server, together with the documentation. Sealing the electronic files with hash functions could protect the evidence from tampering.

For the computer-based assessment the sources of evidence will be the file(s) created by the key logger, the tape of the CCTV camera, the logs, the login reports and the assessment submitted. A high degree of redundancy will exist among evidence sources, which can help to verify the accuracy of the evidence, by cross-checking, in the evidence analysis phase.

3.7 Forensically sound investigation

"The first step to convince a jury that only the suspect could have committed the fraudulent transaction, is to ensure that the investigation is **forensically sound**: the investigation process must be documented and be repeatable" (Melia, 2002) and its results verifiable (Holley, 2000). For computer-based assessments a checklist could be utilized to ensure that all steps in the proposed forensic process are followed. Proper documentation of all forensic activities should also be recorded on a pre-designed form, indicating when, how and by whom the activity is completed.

3.8 Chain-of-custody

Nelson et al (2004:30) state that **chain-of-custody** refers to the route that evidence takes from the time you find it until the case is closed or goes to court. The admissibility of evidence will depend upon the chain-of-custody protocols (Feldman, 2001). First, one must be able to demonstrate that no information has been added or altered. This could be achieved through write-protecting and virus-checking the media containing the evidence. Secondly, you will need to demonstrate to the authorities what is purported to be a complete copy of a specific medium, in fact, what it purports to be. Make an image copy (bit-by-bit, sector-by-sector). Finally, you must show the court that a recognized and reliable copying process was used. Use recognised software to copy and save the evidence. To preserve the chain-of-custody document the following: where, when and by whom evidence is discovered and collected; where, when and by whom evidence is handled or examined; who had custody of the evidence, during what period and how was it stored?

3.9 Forum to monitor the forensic process

To protect the investigator from being subjective, we suggest that the learner is provided with an unbiased forum to raise concerns and ensure the integrity of the process. It would be viable to establish an **ethics committee** that could act as a mediator. It is further suggested that the committee consists of the following members: learner representative(s), person(s) with legal background, technical person(s) with IT experience, and person(s) who could evaluate the ethics issues and the integrity of the process. It is proposed that this committee will give permission for a more comprehensive investigation for evidence only if it is really required to do so. Learners should also have the right to ask permission from the committee to bring in their own IT specialist to validate the integrity of the investigation.

4 PRIVACY ISSUES

The invasion of the learner's privacy due to monitoring will be discussed from different viewpoints: legal, ethical and social acceptability.

4.1 Legal viewpoint

"The Interception Act prohibits the interception of communications, but allows for numerous exceptions to this prohibition. A communication may be intercepted with the consent of any party to that communication, or in terms of a direction issued by a judge" (Buys, 2004:252). To meet this legal requirement, the learners should know that they will be monitored and give written consent. Warn learners through various media: study guides, warning banners on all computer screens owned by the institution, online policy documents or paper-copies of policy documents and educating learners. Learners should give written consent to be monitored for the duration of the computer-based assessment.

4.2 Social viewpoint

Although key loggers and the CCTV camera monitor learners' actions or behaviour, the degree of intrusion of privacy is less compared to monitoring by several (human) invigilators. Invigilation usually entails observation of learners and their actions in a manner that could be considered privacy invasive in other contexts. Close monitoring by a computer could be more socially acceptable than monitoring by a human being.

4.3 Ethics viewpoint

According to Hartman (2001) simply knowing that someone knows personal information (for example typing speed and logical reasoning patterns by monitoring the sequence and type of actions selected) about you can feel invasive or violating. The strong invasiveness of the key logger could result in embarrassment of a learner. Monitoring is done beyond what is technically required and could raise ethics questions. In future a more in-depth discussion on the ethics issues will have to follow. A less invasive technology for collection of evidence could possibly be investigated.

5 POLICIES

An acceptable policy is considered generally *admissible evidence* (Pemble, 2003). Policies should be published and enforced by management. Published institution policies provide the line of authority to conduct internal forensic investigations (Nelson et al, 2004:15). The **line of authority** states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to the evidence. Another way an **institution** can avoid litigation is to display a **warning banner** on its computer screens. A warning establishes authority for conducting an investigation. By displaying a strong, well-worded warning banner, an organization does not need to obtain a search warrant or court order (Nelson et al, 2004:16).

Academic institutions do have assessment policies. If the assessment policy document of the institution does not yet include computer-based assessment regulations, the policy should be updated. To meet the computer forensic requirements institutional policies should be established or updated to address the following issues: monitoring electronic communication, privacy, recording evidence, protecting the evidence, utilization of recorded evidence, retention of evidence, destroying evidence, line of authority and request for full forensic investigation. The learners and all employees (also those involved in forensic investigation) should also sign a document acknowledging that they are aware of, understand and will adhere to institutional policies.

6 EVIDENCE COLLECTION TOOLS

The proposed forensic process employs a key logger to record primary evidence for a potential infringement of assessment regulations. Traditional key loggers record every keystroke and mouse action made by the computer user on which it was activated. Current key loggers have extended functions and record all computer activity: web sites visited, applications accessed, keystrokes, files and folders accessed, etc.

Logs create evidence by capturing the nature and duration of the transaction through time and date stamps of the logon sessions and by verifying that the suspected violator's unique user id and password were used to initiate these logon sessions (Melia, 2002).

Activate the key logger and logs when preparing the computer lab for the assessment. This captures the actions of the person preparing the lab for the assessment and could be used to verify the reliability and integrity of the evidence captured for learners. Even the CCTV camera should be activated when the computer lab is prepared prior to the commencement of the computer-based assessment. In this way the computer-based assessment forensic process should be more reliable and authentic.

7 SUB PHASES OF THE PREPARATION PHASE

For structuring purposes, the first phase (**preparation**) of the computer-based assessment forensic process could be divided into the following sub phases: 1) implementing a forensic readiness programme, 2) initial preparation of the computer lab, 3) preparing the computer lab for the

assessment and 4) final preparatory activities in presence of learners before commencing with the assessment. A discussion of each sub phase follows.

7.1 Implementing a forensic readiness programme

One of the key requirements for the forensic process is **forensic readiness** as discussed in Section 3.1 An Academic institution could follow the ten steps proposed by Rowlingson (2004) in implementing a forensic readiness programme: 1) define the scenarios that require digital evidence, 2) identify available sources and different types of potential evidence, 3) determine the evidence requirement, 4) establish a capability for securely gathering legally admissible evidence to meet the requirement, 5) establish a policy for secure storage and handling of potential evidence, 6) ensure monitoring is targeted to detect and deter major incidents, 7) specify circumstances when escalation to a full formal investigation should be launched, 8) train staff in incident awareness, 9) document an evidence-based case describing the incident and its impact and 10) ensure legal review to facilitate action in response to the incident.

7.2 Initial preparation of the computer lab

If software such as Deep Freeze is used to protect computers, then technical support time will be reduced or eliminated (http://www.amtsoft.com/deepfreeze/). Each restart eradicates all changes and resets the computer to its original state, right down to the last byte. It can protect several hundreds or thousands of computers across a distributed LAN, WAN or over the Internet. For the controlled environment needed for a computer-based assessment, once in the beginning of a semester or year or term (depending on the need), properly set up the computer lab. Thereafter utilize software (e.g. Deep Freeze) to reset the computers to the original (secure and virus-free) state before any computer-based assessment commences.

7.3 Preparation of the computer lab for the computer-based assessment

As already mentioned in Section 6, all monitoring devices (key logger and CCTV camera) and logs should already be activated in the first (preparation) phase of the computer-based assessment forensic process. An authorized person should prepare the lab for the assessment and verify the security and integrity of the lab, computers and software loaded. Do this as closely as possible to the computer-based assessment (may be within the 24 hours prior to the assessment). As mentioned in Section 7.2, utilize software to reset the computers to the original state (secure and virus free). Load any required documents, test the computers and software, check the time and date stamps and search for and eliminate all interference (human, electronic or signal). A cell phone noise generator could be installed to assist in identifying attempts to communicate via a cell phone.

Thereafter, the lab should be physically locked, the key kept in a safe locker and opened only by an authorised person when the computer-based assessment commences. Record **every preparation activity** on the appropriate document. This includes documenting the *what*, *when* and by *whom* of all activities.

7.4 Final preparatory activities in presence of learners

In the computer laboratory, on arrival of the learners, workstations should be randomly assigned to the learners. Even the workstation position number should be recorded on the appropriate documentation. The CCTV camera will also contain evidence of the presence of learners and their seat numbers. Then the learners should sign consent to permit the utilization of key logger tools to monitor computer actions. Learners should be referred to the assessment regulations (either on a paper-based document or electronic document) before the assessments starts.

8 CONCLUSION

In a nutshell, implementation of a forensic readiness programme at an Academic institution could assist in actively collecting potential evidence that facilitates the identification and prosecution of any party that contravenes assessment regulations. The ten steps as mentioned in Section 7.1 could be applied with more detail to shed more light on forensic readiness activities for computer-based assessment forensics. Several steps were already discussed: the scenario, available sources of evidence, how to treat evidence, monitoring and privacy issues, legal issues, policies and setting the scene before the commencement of the assessment.

The aim with the research project is to **establish standards** and **procedures** for computer-based assessment forensics. This paper's contribution focuses on the identification of forensic requirements for computer-based assessments and the preparatory activities, within the first phase of the forensic process, to meet some of the identified requirements. Others requirements will only be met in other phases of the forensic process (summarised in Section 2).

The proposed forensic process could be highly labour intensive and will delay the results of the computer-based assessment. To overcome this burden, human intervention should be restricted to the minimum in the computer forensic process. The forensic process should be automated as far as possible. In a following paper from this research project the focus is on the role of key loggers for evidence collection in the computer-based assessment forensic process (Laubscher et al, 2005c). In that work results are reported after an explorative experiment testing a key logger on a computer-based assessment. The main problem identified is the volume of data captured. Future research will have to investigate or develop methods to automate the analysis on the data with the aim of reducing the initial analysis time and effort.

9 REFERENCES

Ashcoft, J. 2001. *Electronic Crime Scene Investigation: A Guide for First Responders*. U.S. Department of Justice. National Institute of Justice.

Armstrong, I. 2002. Computer Forensics: Detecting the Imprint. *SC Magazine*, August 2002.

Brungs, A. & Jamieson, R. 2005. Identification of legal issues for computer forensics. *Information Systems Management,* Spring.

Boyd, C. & Forster, P. 2004. Time and date issues in forensic computing – a case study. *Digital Investigation*, 13 Jan.

Buys, R. 2004. *Cyber law. The law of the Internet in South Africa*. Van Schaik Publishers.

Feldman, J.E. 2001. *Computer Forensics Inc: Collecting and Preserving Electronic Media*. [Online]. Available: http://www.forensics.com [24.02.2005].

Hartman, L.P. 2001. Technology and ethics: Privacy in the workplace. Business and society Review, 106:1–27.

Holley, J. 2000. Computer Forensics: Market Survey. *SC Magazine*, September 2000.

Laubscher, R, Rabe, D.J, Olivier, M.S, Eloff, J.H.P & Venter, H.S. 2005a. Applying computer forensic principles in evidence collection and analysis for a computer-based programming assessment. IFIP WG 11.9 First International Digital Forensics Conference, Orlando Florida, Feb 2005.

Laubscher, R, Rabe, D.J, Olivier, M.S, Venter, H.S, & Eloff, J.H.P. 2005c. The role of key loggers in computer-based assessment forensics. Work in progress.

Marcella, A.J. & Greenfield, R.S. 2002. *Cyber forensics. A field manual for collecting, examining, and preserving evidence of computer crimes*. Auerbach Publications.

Melia, J. 2002. Linkin' Logs to Fraud: The secret to a successful Computer Fraud investigation is Proper Logging and Audit-Trail Reports. *Security Management*. [Online]. Available: http://www.securitymanagement.com/library/001335.html [30.03.2005].

Nelson, B., Phillips, A., Enfinger, F., & Steuart, C. 2004. *Guide to Computer forensics and Investigations*. Course Technology.

Pemble, M. 2003. Monitoring and Investigations. *Computer Fraud and Security,* Vol. 2003:7, July.

Rowlingson, R. 2004. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence,* Vol. 2:3, Fall.

Stephenson, P. 2003. Using evidence effectively. *Computer Fraud & Security*. Vol. 2003:3.

Tan, J. 2001. Forensic Readiness. [Online]. Available: http://www.atstake.com/research/reports/acrobat/atstake_forensic/readiness.pdf [30.03.2005].