The Role of Key Loggers in Computer-based Assessment Forensics

R. LAUBSCHER, M.S. OLIVIER, H.S. VENTER, J.H.P. ELOFF
University of Pretoria
and
D.J. RABE
Stellenbosch University

When conducting a computer-based assessment in an educational environment, several infringements of assessment regulations could arise. Examples are, illegal communication (e.g. by e-mail, web or cell phone); hiding of computer objects with the aim of accessing or utilising it; impersonation of another student and presenting the assessment material (e.g. file containing answers of WebCT test, files that form part of a programming project) of another student. To determine beyond reasonable doubt that no infringement has taken place, various tools could be utilised. One such a tool, the key logger, is the subject of scrutiny for this study. Key loggers are considered a type of spyware. Spyware is software that gathers information secretly about a computer's use, usually installed without the user's consent or knowledge, and relays that information, also covertly, back to a third party. This paper reports the results of an explorative experiment applied to computer-based assessments with the aim to investigate the role of key loggers in computer-based assessment forensics. This exploratory experiment was conducted during computer-based assessments of different groups of students in different subjects. The results include a description of the set up of the controlled environment for the computer-based assessment, execution of the assessment with the accompanying data collection, preserving of the data, analysis of the data, effectiveness of the specific key logger in the forensic process and the conclusions derived from the data.

Categories and Subject Descriptors: K.3 [**Computing Milieux**]: Computers and Education; K.4.1 [**Computing and Society**]: Public Policy Issues – Abuse and crime involving computers; K.4.1 [**Computing and Society**]: Public Policy Issues – Privacy; K.4.2 [**Computing and Society**]: Social Issues – Abuse and crime involving computers; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – Invasive software; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – Unauthorized access
General Terms: Human factors, Management, Measurement, Performance, Reliability, Security
Additional Key Words and Phrases: computer-based assessment forensics, digital evidence collection

1. INTRODUCTION

In all educational institutions cheating by students are common and a sad reality. With the increased utilisation of computer-based assessments, the following question comes to mind: Have students indeed mastered the subject matter reflected in the marks obtained? Rowe [2004] asks a similar question: When students score well in computer-based assessment does that prove that they know the material? There is much cheating that is not caught.

When conducting a computer-based assessment at an educational institution several infringements of assessment regulations are possible. Examples are illegal communication (e.g. by e-mail, web or cell phone), hiding of computer objects with the aim of accessing or utilising it, impersonation of another student, and presenting the assessment material of another student. Rowe [2004] also mentions that students could use *spyware* to electronically sneak a look at how other students are answering questions during an assessment. Furthermore students could use spyware to electronically sneak a look at the activities of the person preparing electronic files for the assessment and password-protect the computer-based assessment. Students could also use software called *sniffers* to decipher the message packages of a local area network which contains fellow students' or the instructor's details and read their answers or passwords.

If infringement is suspected, a computer forensic investigation should be launched. It is assumed through general observation that there are currently no academic institutions that have a computer forensic department, which is able to investigate suspected assessment infringements. Therefore, the responsibility of conducting a computer forensic investigation, in particular the collection and analysis of the required computer evidence, in most cases will rest upon the lecturer.

Author Addresses:
R. Laubscher, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, Pretoria, 0002, South Africa; rut@ma2.sun.ac.za.
D.J. Rabe, Computer Information Systems Department, Stellenbosch University, Military Academy, Saldanha, 7395, South Africa ; castor@ma2.sun.ac.za.
M.S. Olivier, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, Pretoria, 0002, South Africa; martin@mo.ac.za.
H.S. Venter, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, Pretoria, 0002, South Africa; hventer@cs.up.ac.za.
J.H.P Eloff, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, Pretoria, 0002, South Africa; eloff@cs.up.ac.za.

This paper forms part of a research project on how to apply computer forensic principles to a computer-based assessment environment in order to identify and if necessary prosecute any party that contravenes assessment regulations. This would contribute to quality assurance in the subject and enhance the academic integrity of the educational institution. Previous work by Laubscher et al. [2005a] considers the application of forensics on the entire computer-based assessment process. In this paper the role of key loggers in computer-based assessment forensics will be investigated. The methodology followed is based on an explorative experiment where key logger software is installed on the workstations of the computer laboratory and activated for selected computer-based assessments.

The other aspects covered in this paper are as follows: an elaboration on key loggers and privacy concerns raised when monitoring human computer behaviour; an overview of the forensic process for computer-based assessments and forensic requirements for computer-based assessment forensics; a discussion of the explorative experiment for testing the performance of key loggers in the computer-based assessment forensic process; followed by the final conclusions and recommendations.

2. BACKGROUND

Key loggers, software or hardware implemented, record all keyboard and computer actions. The key loggers discussed in this paper are extensions of the general key loggers that only capture keyboard and mouse actions and could be employed extensively in computer-based assessment forensics. In this section, the negative connotations of key loggers are contrasted against their usability in the forensic process for computer-based assessment.

2.1 Key Loggers

Key loggers are considered a type of spyware which is commonly used to refer to software that, from a user's perspective, gathers information secretly about a computer's use, usually installed without the user's consent or knowledge, and relays that information, also covertly, back to a third party [Saroiu et al. 2004; Hinde 2004]. One of the main security threats of spyware is the ability to steal confidential information such as passwords [Hinde 2004]. Spyware succeeds because today's desktop operating systems make it simple to build and install such software [Saroiu et al. 2004]. Spyware could have a degrading effect on the system's processing capacity and can have a costly effect on bandwidth [Boldt et al. 2005]. The mentioned implications of spyware should therefore be considered carefully in the process of selecting forensic tools for evidence collection in computer-based assessment forensics.

In contrast to the mentioned negative connotations, key loggers could also capture valuable forensic evidence such as keystroke and mouse actions, access to applications, web pages, files and folders and screen shots. Examples of key logger software are KeyCapture [Soukoreff & Mackenzie, 2003], Computer WatchDog, SpectorSoft, eBlaster, Ghost Keylogger, KeyKatcher, Perfect Keylogger [Security Technology Ltd. 2003] and 007 Spy Software [E-Spy 2005]

The specific key logger chosen for this study is 007 Spy Software. It is a stealth computer monitoring software package that allows you to record all activities of computer users and automatically delivers logs. A valuable security feature of the 007 Spy Software is the password protection so that only an authorised user (i.e. a system administrator) may enable, disable or manipulate its settings.

The reason why this key logger software is chosen is because most computer actions can be detected. The 007 spy Software records not only keyboard and mouse actions, but also all applications executed and terminated, all documents opened and closed, all web sites browsed, all file and folder manipulations and takes screen shots at specified intervals just like a surveillance camera. In addition, it is easy to install and runs as an application and not as a service, which captures the user's initial logon password. It only captures intermediate passwords entered by the user while the key logger is activated. It is only possible to deactivate the key logger if its password is known and if the person logs in as a system administrator.

The data captured by the key loggers could be utilised in different ways for initial analysis in the forensic process for computer-based assessment: it could trigger alarms when certain web sites, applications, files or folders were accessed, or it could be an indication of a possible infraction due to the total file size and number of files recorded.

Tools used for collecting various types of evidence not only include key loggers, but also closed circuit television (CCTV) cameras, log files and the final submitted assessment material. Confirmation could be achieved by cross checking the different sources of evidence. This forms the basis of proving that dishonesty has been committed in the computer-based assessment. The key logger is the subject of scrutiny for this study.

2.2 Privacy

Although key loggers are useful for collecting digital evidence, this monitoring process results in invasion of the student's right to privacy: a personal profile could be built for a specific student. Special consideration should be given to a person's right to privacy; especially if that right is invaded. In Laubscher's et al. [2005b] discussion of the invasion of privacy from a legal, social and ethical acceptability viewpoint, the following should be considered: a student should give consent to be monitored, close monitoring by a computer could be more socially acceptable than monitoring by a human being, and monitoring done beyond what is technically required could raise ethical questions. It is a socially acceptable norm that a person will have to sacrifice, to a certain degree, the right to privacy when conducting an assessment.

To meet the computer forensic and privacy requirements, institutional policies should be established or updated to address the following issues: recording evidence, utilisation of recorded evidence, retention of evidence, destroying evidence, assessment infringements and electronic communication privacy. The students should also sign a document that they are aware of and will adhere to the institutional policies. The institution could also display warning banners on its computer screens to make computer users aware of the policy.

Warnings could be attached to notice boards in the computer centre to inform students of the activation of key loggers for capturing data for the duration of computer-based assessments. During assessment situations students should again give written consent to be monitored.

3. PREVIOUS WORK

In order to provide the context for this paper, a brief overview of the computer-based assessment forensic requirements and forensic process, described in earlier work [Laubscher et al. 2005a; Laubscher et al. 2005b], is given.

3.1 Forensic Requirements for Computer-based Assessment

The computer-based forensic requirements as identified by Laubscher et al. [2005b] are: forensic readiness, time synchronisation, permission to investigate or collect evidence, adhering to legal standards, permission to monitor computer behaviour, digital evidence controls, forensically sound investigation, chain-of-custody and an ethics committee to monitor the forensic process. This subsection will present a summary of some of these forensic requirements.

Forensic readiness could be demonstrated by maximising the potential to use digital evidence when required. This could partially be achieved by activation of forensic tools, prior to the computer-based assessment session (in the preparation phase). 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. The controlled assessment environment contributes positively to forensic readiness because the possible suspects, times and dates, resources, sources of evidence and the origin of the possible infringement are all known. Updated or newly established policies could streamline the forensic process.

Special care should be taken to ensure the *authentication and integrity* of the *time and date stamps* of collected evidence. Before the assessment starts the CMOS time on each workstation and the server should be verified and synchronised in relation to actual time, obtainable using radio signal clocks or via the Internet using reliable time-servers. Secure the time and dates on the workstation or server by restricting write-access for students to these settings.

In general if a crime is committed, law enforcers have to issue a search warrant before the investigation could commence. In the case of computer-based assessment forensics permission to collect evidence and analyse evidence is needed even before any transgression could be performed. Well-defined policies give computing investigations and forensic examiners the *authority to conduct private investigations* such as those where students infringe assessment regulations. The executive management of the academic institution should define and limit who is authorised to conduct an initial forensic analysis and request a more comprehensive investigation to avoid inappropriate investigations.

A *forensically sound investigation* implies that the investigation process must be documented and be repeatable. Checklists, indicating the required forensic actions, could help to ensure that predetermined processes and procedures are executed, contributing to a forensically sound investigation. The people preparing the assessment environment, invigilators for the assessment and the person(s) involved in the initial analysis of the collected data after the computer-based assessment, should complete necessary documentation.

For the *chain-of-custody* one must firstly be able to demonstrate that no information has been added or altered to the evidence. Secondly, one will need to demonstrate to the authorities what is purported to be a complete copy of a specific medium is in fact what it purports to be. Finally, one must demonstrate to a court of law that a recognised and reliable copying process was used.

To protect the investigator from being subjective, it is suggested that the student has access to an unbiased forum to raise concerns and ensure the integrity of the process. It was suggested that an *ethics committee* should be established to act as a mediator and it could consist of the following members: student 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.

3.2 The Forensic Process for Computer-based Assessment

The proposed forensic process for computer-based assessment consists of four phases: preparation of the environment, evidence collection, analysis of data and reporting the findings.

During the first phase (*preparation*) the controlled environment is prepared prior to the assessment. As indicated in previous work [Laubscher et al. 2005b], the first phase entails activities to provide forensic readiness for a computer-based assessment environment. The process for forensic readiness could be subdivided in the following subphases: readiness of documents, initial preparation of the computer lab, and preparation of the lab for the specific assessment and final readiness activities of the students before commencing with the assessment.

In summary, the first phase activities include casting of all computers with a previously set-up computer image (software such as DeepFreeze could be used to reduce technical support time), activation of the *key logger*, activating

logs and CCTV camera, and verification that the time and dates of all computers are correct and identical. On arrival of the students, the invigilators randomly allocate students to computer workstations and announce the assessment regulations. The students should give consent to be monitored (with *key loggers* and CCTV cameras) 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 firstly, *key loggers* used to capture the student's keyboard and mouse actions, and secondly, logs used to record electronic activities. In addition, 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 saves these reports for electronic evidence to a file. The motivation for this is to detect, as soon as possible, when a student attempts to impersonate another user. More than one invigilator should be present in the computer lab where the assessment is conducted. The CCTV cameras record 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 students) 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, and should also be casted from an initial virus-free computer. The student'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 collected electronic evidence should be analysed for suspected activities that transgress 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 should be conducted. In the fourth phase (*reporting*) the findings should be reported to the examination board and relevant authorities.

4. THE EXPLORATIVE EXPERIMENT

In every assessment situation the invigilators have dual responsibilities to fulfil: on the one hand they must provide an environment in which the student can be treated according to his or her right to privacy during the assessment session in order to complete the assessment with as few distractions as possible. On the other hand they must also be able to determine beyond reasonable doubt which resources, legitimate and illicit, were used to develop the final submitted assessment material. It is also very important to detect and deal with any suspected behaviour in a computer-based assessment as quickly as possible, because the assessment should be evaluated, moderated and the results published within a limited time. This section explains the following aspects of the experiment: purpose, hypothesis, equipment and methodology.

4.1 Purpose of the Experiment

The *objectives* of the experiment are to identify the types of infringement that can be identified successfully with the data captured by the key logger and the usability of the recorded data. Although, the challenge in the research project is to detect and prove every transgression, without falsely accusing someone of transgression, the aim with this experiment is not to prove accuracy, but rather to explore the usability of the tool and the nature and sufficiency of the data collected by the key logger.

4.2 Hypothesis

Key loggers capture *useful forensic data* enabling the identification and facilitating of the prosecution of any party who contravenes assessment regulations during a computer-based assessment.

4.3 Methodology

The explorative experiment was launched on two different first-year modules in the Computer Information Systems Department of the Military Academy (Saldanha). A group of twenty students from the Introduction to Programming (CIS114) module completed a computer-based assessment to develop a Java program. A group of ten students from the Computer Skills (CS114) module completed a computer-based assessment with ExamView [ExamView 2005]. Two extra students completed the assessments with instructions to commit computer-based assessment infringement. They were not registered for the module.

The key logger software was installed on the workstations in the CIS centre prior to the assessment. Students gave written consent to be monitored; the computer workstation position number and details of the student were also recorded on the written consent form. The invigilators assigned students randomly to workstations.

The CS114 assessment contained 30 multiple-choice questions with a time restriction of 15 minutes for the assessment. The CIS114 assessment was restricted to one hour for the development of a Java program. The CIS114 students were only allowed to utilise JCreator and the API documentation of Java. The CS114 students were only allowed to utilise ExamView to complete the computer-based assessment.

Workstation position number	Dishonesty	Folder size	No of files in folder	Result file sizes in KB					JPEG
				App	Files & Folders	Web	Screens	Keys	No of files
	Yes / No	MB							
A2	No	4.49	82	5	1	1	25	4	77
A3	No	2.1	38	3	1	2	2	3	34
A5	No	4.2	68	19	1	3	24	3	63
D1	Yes	1.21	46	12	1	3	21	11	40
D2	Yes	1.39	32	18	1	0	16	4	29
Total		13.12							
Average		2.624							

Table 1 Summary of file sizes for data captured in ExamView assessment

Workstation position number	Dishonesty	Folder size	No of file in folder	Result file sizes in KB					JPEG
				App	Files & Folders	Web	Screens	Keys	No of files
	Yes / No	MB							
C4	No	14.4	169	26	1	0	65	8	164
C5	No	8.73	116	5	2	0	41	9	111
C7	No	10.5	133	29	5	0	51	10	129
D1	No	11.3	125	13	3	3	51	13	120
D3	No	11.9	137	26	10	3	57	16	132
D4	No	13.5	149	27	7	0	61	18	144
D5	No	10.0	113	24	2	0	47	11	108
D6	No	10.6	118	18	3	2	49	11	113
D7	No	11.0	137	35	6	2	57	24	132
A1	Yes	0.852	22	8	9	2	9	3	18
A2	Yes	1.16	25	11	7	3	11	2	15
Total		114.382							
Average		10.4							

Table 2 Summary of file sizes for data captured in the Java programming assessment

5 RESULTS

For the explorative experiment the ***dependent variables*** (depend upon the actions of the specific student) were the folder size, number of files created and entries captured in html files. The ***independent variable*** (test different entities) was the students who completed the computer-based assessments. The ***constants*** (similar for all entities) were similar assessments for the different groups and similar conditions (time slot, similar computer workstations, equivalent programs e.g. ExamView and JCreator) under which the assessments were completed**.**

5.1 Type of Data Captured by the Key Logger

The key logger software logs five result files, represented as HTML files, and a varying number of JPEG files per workstation and can deliver the logs to a pre-determined destination. The result files log the following: file and folder manipulation, application accesses, web site visits, keystrokes and screen shots captured. Each file contains various entries associated with each category.

5.2 The File sizes of the data captured by Key Logger

The file sizes are remarkably smaller where infringement took place. A possible reason is that the students took short cuts and did not utilise the full session to complete the assessment. The duration of the Programming assessment was one hour and for the ExamView assessment 15 minutes. For the Programming assessment more screen shots were captured that resulted in an increase in folder size, number of JPEG files and number of entries in the file of screen shots.

The average folder size for the ExamView and Programming assessments was 2.624 MB (as shown in Table 1) and 10.4 MB (as shown in Table 2), respectively. The duration of ExamView of the assessment was 15 minutes. If 100 students will be assessed in an ExamView assessment of one hour, then the key logger will record approximately 1.496 GB (262.4 KB times 4) of data. The screen shots occupy most of this file space. To reduce the file size of the captured data, the setting of the key logger could be changed to capture screen shots at longer intervals and with lower intensity. From a forensic perspective this could be a less efficient choice, because possible evidence data could be lost (screen

shots not recorded due to time interval). There should be a balance between number of screen shots captured and accuracy of possible evidence collected in computer-based assessment forensics.

User@Time	ciscenter@2005-05-15 19:29:33
Action	Run
Application Name	Pegasus Mail
User@Time	ciscenter@2005-05-15 19:31:07
Action	Run
Application Name	Microsoft PowerPoint
User@Time	ciscenter@2005-05-15 19:31:07
Action	Open
Application Name	Microsoft PowerPoint - [LECTURE6]
User@Time	ciscenter@2005-05-15 19:31:30
Action	Close
Application Name	Microsoft PowerPoint - [LECTURE6]

Table 3 Example entries recorded in Application file

User@Time	ciscenter@2005-05-15 19:37:49
Site Name	Character (Java 2 Platform SE v1.4.2)
URL Address	file:///C:/j2sdk1.4.2_03/docs/api/index.html

Table 4 Example entries recorded in Web Sites visited file

5.3 Example Entries in Captured Data

The key logger records all computer actions and keyboard actions: no computer action is undetected. Even if a student manages to plug a flash disk into the USB port without the invigilator noticing the illegal action, as soon as the student attempts to access data on the flash disk, the key logger would record this action. Table 3 and 4 reflect extracts of entries recorded in the application and web-sites-visited html files. Table 3 has an example of data recorded in the application html file, indicating that a student illegally sent e-mail using Pegasus mail and opened a PowerPoint presentation for reference. From a forensic point of view, it is of importance to note that the date and time are also recorded as evidence data. The date and time stamps of all workstations should be synchronized before the assessment commences. Table 4 shows an example of an entry in the web-sites-visited html file indicating that a student accessed the Java documentation (this was a legal action).

6 DISCUSSION

The *objectives* of the experiment were to identify the types of infringement that can be identified successfully with the data captured by the key logger, the usability of the recorded data, the methodology for the initial forensic analysis of the recorded data and improvements or additional processes needed to complete the forensic analysis more efficiently. All types of infringements listed in the introduction could be identified with the data recorded by the key logger. Table 5 indicates the possible source file for recorded data that indicates transgression of the assessment regulations.

The data recorded by the key logger is sufficient and usable. More than enough data is recorded to identify and prove beyond reasonable doubt that an infringement has taken place. The main areas of concern are the volume of the recorded data and the tedious and time-consuming procedures necessary in the initial analysis of the recorded data.

There is currently no quick solution for the initial forensic analysis of the recorded data per student. A filtering process should filter the data recorded outside the time slot of the computer-based assessment. Once again, it is important to ensure that the dates and times are synchronised before the computer-based assessment commences. Word searches should be launched on the filtered data in an attempt to identify illegal computer actions e.g. e-mail communication, access to web sites, applications, files and folders.

Automation of the forensic analysis on the recorded computer-based assessment data could ensure timely publishing of results to the examination committee. This paper is the first step in the automation of the forensic process.

Type of infringement via digital medium	Possible source of identification
e-mail communication	Keystroke, application
Web communication	Keystroke, web site
Blue tooth communication	Applications
Wireless communication	Applications
Accessing electronic lecturing notes	Application, Files and folders
Accessing previous projects	Applications
Accessing slide show presentations	Applications
Accessing web sites	Web sites
Use of electronic storage media e.g. memory stick	Files and folders, Applications
Use of spyware	Applications
Use of sniffers	Applications

Table 5 Identification of possible source file for specific type of infringement

Other concerns are the performance degrading on the workstation where the key logger software is installed and the issue of invading the privacy of students due to monitoring. The forensic value added when key logger software is installed and activated during the computer-based assessment, however, outweighs the degree of performance degradation on the workstation.

7 CONCLUSION AND RECOMMENDATIONS

The experiment indicates that modern key loggers (monitoring of all computer behaviour opposed to only keyboard and mouse actions) are capable of capturing useful data that could be utilised as evidence in computer-based assessment forensics. The *007 Spy Software* key logger is capable of identifying the following types of infringement: electronic, web, blue tooth and wireless communication; illegal access to applications, web pages, files and folders; use of external storage media; use of spyware or sniffers.

The main concerns detected from the explorative experiment were the volume of the recorded data and performance degradation of the system on which it is activated. Future research will have to investigate methods to automate the analysis on the data with the aim of reducing the initial analysis time and effort. Possible filtering methods include text mining, data mining or self-organising maps [Fei et al. 2005].

This paper's main contribution to the field of digital forensics is the application of general digital forensic processes and principles to a specific application, namely computer-based assessments at academic institutions. By viewing, scrutinising, testing, and evaluating digital forensic processes and principles from different application perspectives, possible gaps and improvements could be identified in the broader digital forensic field.

Key loggers could also be utilised to collect possible evidence in other applications of digital forensics, specifically in the private sector domain (forensic cases that hopefully will not end in court). The data captured by key loggers could be analysed for indications of transgression of company regulations or policies. In future various other key loggers could be scrutinised and the link between key loggers and forensic software such as Encase could be investigated.

REFERENCES

BOLDT, M., CARLSSON, B. AND JACOBSSON, A. School of Engineering, Blekinge Institute of Technology, S-372 25 Ronneby, Sweden. 2005. *Exploring Spyware Effects*. psi.bth.se/mbo/exploring_spyware_effect-nordsec2004.pdf Accessed in May 2005.

E Spy SOFTWARE ONLINE. 2005. *007 Spy software*. http://www.e-spy-software.com. Accessed in May 2005.

EXAMVIEW. *Test generator*. 2005. http://www.examview.com/. Accessed May 2005.

FEI, B.K.L, ELOFF, J.H.P, OLIVIER, M.S AND VENTER, H.S. Computer Forensic Tools with self-organizing maps. *IFIP WG 11.9 First International Digital Forensics Conference*, Orlando Florida, Feb 2005.

HINDE, S. 2004. Spyware: the spy in the computer. *Computer Fraud and Security*. 2004, 12.

LAUBSCHER, R, RABE, D.J, OLIVIER, M.S, ELOFF, J.H.P, AND 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, OLIVIER, M.S, VENTER, H.S, RABE, D.J, AND ELOFF, J.H.P. 2005b. Computer Forensics for a Computer-based assessment: The preparation phase. Work submitted for a conference.

ROWE, N.C. 2004. Cheating in Online Student Assessment: Beyond Plagiarism. Online Journal of Distance Education Administration. http://www.cs.nps.navy.mil/people/faculty/rowe/dlcheat.htm

SARIOU, S, GRIBBLE, S.D, AND LEVY, H.M. 2004. Measurement and analysis of spyware in a university environment. *In Proceedings of the ACM.USENIX Symposium on Networked Systems Design and Implementation* (NSDI), San Fransisco, CA, USA, March 2004.

SECURITY TECHNOLOGY LTD. 2003. http://www.keylogger.org/progrm.cgi?id=1. Accessed on 9 Dec. 2004.
SOUKOREFF, W, AND MACKENZIE, S. KeyCapture. 18/07/2003.
http://www.dynamicservices.com/~will/academic/textinput/keycapture. Accessed on 24 Nov. 2004.

R Laubscher, MS Olivier, HS Venter, JHP Eloff and DJ Rabe, "The role of key loggers in computer-based assessment forensics," in J Bishop and DG Kourie (eds), *Research for a changing world - Proceedings of SAICSIT 2005*, 123-130, White River, South Africa, September 2005)