Chapter 9

APPLYING FORENSIC PRINCIPLES TO COMPUTER-BASED ASSESSMENT

R. Laubscher, D. Rabe, M. Olivier, J. Eloff and H. Venter

Abstract A computer forensic investigator investigates computer crime. Currently only a few academic institutions have a computer forensic department and, therefore, the investigative responsibility (in case of contravention of assessment regulations for computer-based assessments) rests upon the lecturers.

The purpose of our project is to apply computer forensic principles to a computer-based assessment environment to facilitate the identification and prosecution of any party that contravenes assessment regulations. This paper is the first step in that project; its purpose is to consider the nature of such an environment. This nature is derived from the established computer forensic principles. In particular, we focus on the forensic process to determine the policies, procedures and types of tools that should be present in such an environment. The intention of the paper is not to consider any of the issues raised in detail, but to consider the process from a high level. The utilization of different tools, namely a key logger, CCTV camera, audit log and a report of logins, facilitates the identification of any party that contravenes assessment regulations. The proposed process consists of four phases: preparation of the environment, collection of evidence, analysis of evidence, and reporting findings.

Keywords: Computer-based programming assessment, forensic process, key logging

1. Introduction

In learning to program, the greatest amount of time is devoted to working on the computer. As Wyer and Eisenbach [11] pointed out, it is more appropriate to test programming skills by means of a computerized assessment than by means of a paper-based assessment. Examples of risks that could arise in a computer-based assessment are: hidden pre-written code with the aim to copy or access the code during the

assessment, electronic communication with the aim of exchanging solutions or tips, impersonation of another learner (knowing the other user's login name and password) and presenting the programming project of another learner under this learner's name (masquerading). Even with security measures in place (e.g., the presence of invigilators, access control and authentication), the risk of contravention of assessment regulations is high, because learners find innovative methods to violate assessment regulations or bypass security controls.

Currently only a few academic institutions have a computer forensic department that is able to investigate suspected assessment misconduct. Computer forensic departments are emerging in the financial sector, but are likely to remain uncommon in academic institutions. Therefore the responsibility of conducting a computer forensic investigation will rest on the lecturer – in particular, the collection and analysis of the required computer evidence. After an investigation is completed, the investigation report could be presented to the examination board and authorities, and may lead to a court case.

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. An assessment invigilator (or commissioner) has a dual duty to fulfill. On the one hand the invigilator must provide an environment in which the learner can be treated with his/her right to privacy during the assessment to enable 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 develop a programming project.

The purpose of our project is to apply forensic principles to a computerized assessment environment in order to facilitate the identification and prosecution of any party that contravenes assessment regulations. This paper is the first step in that project; its purpose is to consider the constituent elements of such an environment. These elements are derived from established computer forensic principles. In particular we will focus on the forensic process to determine the policies, procedures and types of tools that should be present in such an environment. The intention of the paper is not to consider in detail any of the issues raised, but to consider the process from a high level.

The remainder of this paper is structured as follows. Section 2 defines the relevant terminology. Section 3 describes the computer forensic process in a computerized assessment environment. Sections 4, 5, 6 and 7 elaborate on the four phases of the assessment forensic process. Section 8 presents the conclusions and recommendations.

2. Relevant Terminology

Computer Forensics: The goals of computer forensics are to conduct a structured investigation to determine exactly what happened and who was responsible, and to perform the investigation so that the results are useful in a criminal proceeding [6] (p. 292). In our case, the possible culprits are known and the crime domain is restricted.

In a forensically sound methodology, no changes are made on data from the original evidence; the evidence is preserved in a pristine condition [5]. It should also not matter who completes the examination of media, which tools are used and which methods employed – the same results should always be obtained.

Key Logging Tools: Key loggers record every keystroke and mouse action performed by the user of the computer on which these tools are activated. Examples of key logger software are: KeyCapture [9], Powered Keylogger, Handy Keylogger, Stealth Keylogger and Perfect Keylogger [8]. The emphasis is on the key logger as primary source for evidence collection and the other tools (CCTV camera and audit logs) as secondary sources.

Audit Logs: The general notion of an audit log is appealing for use in an assessment environment. In practice, however, an audit log may be difficult to handle, owing to the volume of data and analysis effort required. To overcome this problem, we suggest that a backup of the audit log is made and then cleared before the computer-based programming assessment commences. Only transactions within the specific computer-based programming assessment time-slot should be recorded for forensic investigation purposes.

3. Proposed Computer Forensic Process

For the purposes of this research the following prerequisites are assumed to establish a controlled computer-based programming assessment environment: there are at least two invigilators, of which the programming lecturer is one, learners complete the assessment on randomly assigned (by the lecturer) workstations that are not connected to the Internet, the assessment starts and ends at a specific time, network access is restricted to a designated folder for each learner (with appropriate access rights), learners are not able to observe any other screens and casting of a previously set-up computer is utilized in order to ensure identical configurations on each workstation.

According to Holley [5], a computer forensic investigation is a four-step process conducted after a crime has been reported and a subpoena issued. The first step is to identify which computer media may contain

evidence. The second step is to preserve the digital data because they are fragile. The third step is to analyze the data by conducting an examination either directly on the image or to use the image to make another copy of the media to be examined. The final step is to report the findings to decision-makers for action.

According to Armstrong [1], when forensics is used to its full potential, it can provide both pre- and post-event benefits. The computer forensics process we are proposing for computer-based programming assessment also consists of four phases: preparation of the environment, evidence collection, analysis, and reporting findings.

During the first phase the controlled environment is prepared prior to the assessment. The activities are casting all computers with a previously set-up computer, disabling Internet connections, activating key logger software, audit log and CCTV camera, verifying that the time and dates of all computers are correct and identical, announcing assessment regulations, and obtaining the consent of learners for evidence collection.

In the second phase the computer-based programming assessment starts. Key loggers capture the learner's keyboard and mouse actions and the electronic activities are recorded in the audit log. Login activities must be monitored frequently by generating a report indicating details of all users logged onto the network. For the duration of the assessment session, the CCTV camera records all activities within the computer laboratory.

The third phase in the forensic process starts after the completion of the assessment. Back-ups of all files (i.e., key logger files, audit log, login reports, programming projects of learners) are made on a separate computer or other trusted computer-storage media. Only then are the CCTV camera, key logger and audit log disabled. Next, an initial systematic scanning of all electronic evidence collected should be conducted and analyzed for suspected activities that transgresses regulations for the assessment. 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 forensic analysis must be conducted.

In the fourth phase, the findings are 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 transgression of regulation has been committed in the computer-based programming assessment. The comprehensive forensic investigation lies beyond the scope of this paper. Now that an overview

of the process has been given, the following sections elaborate on each of the phases.

4. Phase I: Preparation for Evidence Collection

Preparation for evidence collection starts prior to the assessment. When a computer cast is done from a previously set-up computer, all workstations start with an identical image to prevent learners from hiding pre-written code or programs. Care must be taken to ensure that the computer from which the cast is created is virus free. The presence of viruses increases the complexity of the burden of proof. Next, a CCTV camera, audit log and key logger are activated for every workstation. The CCTV camera is used for surveillance (who sits where), the audit log records network transactions, and the key logger monitors the specific workstation.

Workstations must be assigned to learners upon their arrival. The learners should sign consent forms to permit the utilization of key logger tools to monitor all keyboard and mouse actions. An institutional policy should be in place and explained to the learners upon registering at the institution; they should also sign a document acknowledging that they understand the policy and will adhere to it.

Other important issues in the preparation phase are discussed in the following subsections: assessment regulations, legal issues, and time and date stamps.

Assessment Regulations: Examples of assessment regulations and instructions include a prohibition of communication between candidates in the assessment room as well as a prohibition on the use of supporting material (blank paper, books, notes, calculators, cellular phones and other electronic equipment) in the assessment room. Regulations specific to computer-based assessment usually explicitly prohibit electronic communication between candidates themselves and electronic communication between candidates and other external people. Electronic access to digital documents is restricted to those explicitly specified in the assessment paper.

Legal Issues: Obviously, invasion of privacy is a serious legal issue. To overcome the privacy issue, it is necessary to ensure that there are written institutional policies stating the rights of the institution or auditors to access and review all data on the institution's computers and related media and peripherals at any time, and to monitor all actions while using the facilities to ensure compliance with institutional policy [2].

Time and Date Stamps: Evidence collection relies extensively on time and date stamps of objects. Boyd and Forster [3] suggest that special care should be taken to ensure the authentication and integrity of the time and date stamps of the objects. Before the assessment starts, the CMOS time on each workstation and the server should be verified and synchronized in relation to actual time, obtainable using radio signal clocks or via the Internet using reliable time-servers. Learners should not have write access to the time settings.

5. Phase II: Evidence Collection

During the assessment, further monitoring activities may be applied to enhance evidence collection and analysis. Protection should be in place to ensure that learners could not bypass the key logging process, disable it or tamper with the log file. The captured keystrokes and mouse clicks should be written to a predetermined file on the server, protected by access control to ensure its authenticity and integrity. Masquerading will be confirmed if login attempts of more than one user are recorded for the same file.

Impersonation of learners during computer-based assessment could be identified if the lecturer frequently monitors login activity and writes the evidence to a separate file. Alternatively, the evidence will also be in the audit log. The advantage of monitoring logins during the session is that a learner could be caught in the act of impersonation.

6. Phase III: Analysis of Collected Evidence

After the submission of the final version of the programming project, five steps remain in the proposed computer forensic process: preserving computer media, de-activating logging devices, conducting an initial analysis of the collected evidence, conducting a comprehensive analysis of the evidence, and reporting findings.

Analysis should be conducted on exact copies of the media. Reliable backup copies should be created for investigations of key logger files, the audit log, the file containing the login reports, and the learners' final programming projects. These files should be inaccessible to the learners or any other person or object. A message digest (MD) could be calculated for the evidence data, providing a seal and encasing it so that any change is apparent [7] (p. 76).

It is necessary to verify that the final project submitted is the learner's legitimate and own work, created during the assessment. For this purpose it should be verified that non-permitted objects were not accessed or copied during the assessment, no electronic communications occurred

between the learner and another person, one learner did not impersonate another learner, and the learner did not employ other tools, e.g., program generators, during the session.

Two processes are involved in evidence analysis: (i) an initial search for possible dishonesty, seeking clues that indicate communication, copying or accessing non-permitted files, and (ii) a comprehensive analysis when there is a possibility of dishonesty.

The initial analysis strategy involves replaying the learner's key strokes and mouse clicks. This is performed on a workstation that is in a "clean state" (configured similar to workstations at the beginning of the assessment session). Replaying the key strokes and mouse clicks should therefore result in the same file(s) that were submitted by the candidate. Further analysis is required of any differences are found between the submitted file(s) and those created during the replay.

The initial analysis could be concluded by scanning the audit log for all disk accesses and broadcast messages, and by viewing the last entry in the file which reports the logins to confirm that all learners have logged in only once at the beginning of the assessment.

The final phase in the forensic process is to report the findings to the decision-makers, i.e., the examination board and authorities. The reporting of findings, discussed in the following section, is crucial to the forensic process.

7. Phase IV: Reporting Findings

All the forensic activities and the evidence collected should be documented with precision and accuracy. The report must be written in a clear and concise manner and should be understandable to non-technical people.

Of course, underlying all of these activities is "chain-of-custody." This refers to the proposition that evidence once captured or seized must be accounted for from that time onward [10]. Throughout the investigation, analysis and report preparation, the chain-of-custody must be provably kept intact. Feldman [4] recommends that to preserve the chain-of-custody, it is necessary to demonstrate that no information has been added or altered. This can be accomplished by write protecting and virus checking all media, and calculating and signing a message digest.

8. Conclusions

The purpose of our project is to apply forensic principles to a computerized assessment environment to facilitate the identification and prosecution of any party that contravenes assessment regulations. In a con-

trolled assessment environment it is easier to identify any party that contravenes assessment regulations. An institutional policy should permit monitoring of electronic activities, even if this means invasion of the privacy of the learner. The learner should be required to sign an acceptance of the policy and to give consent to be monitored and investigated if a possible contravention is detected.

The utilization of tools for evidence collection and analysis (cross-checking), i.e., key logger, CCTV camera, audit log and report of logins, facilitates the identification of any party that contravenes assessment regulations. The forensic process consists of four phases: preparation of the environment, collection of evidence, analysis of evidence, and reporting findings. The proposed analysis methods are conducted manually, but future research will lead to an automated process. The approach should be applicable to any type of computer-based assessment.

References

[1] I. Armstrong, Computer forensics: Detecting the imprint, *SC Magazine*, August 2002.

[2] M. Bigler, Computer forensics, *Internal Auditor*, vol. 57(1), p. 53, 2000.

[3] C. Boyd and P. Forster, Time and date issues in forensic computing: A case study, *Digital Investigation*, vol. 1(1), pp. 18-23, 2004.

[4] J. Feldman, Collecting and preserving electronic media, Computer Forensics Inc., Seattle, Washington, 2001.

[5] J. Holley, Market survey: Product review, *SC Magazine*, September 2000.

[6] W. Kruse and J. Heiser, *Computer Forensics: Incident Response Essentials*, Addison-Wesley Longman, Amsterdam, The Netherlands, 2001.

[7] C. Pfleeger and S. Pfleeger, *Security in Computing*, Prentice Hall, Upper Saddle River, New Jersey, 2003.

[8] S.T. Ltd., Top ten key loggers in review (www.keylogger.org).

[9] W. Soukoreff and S. Mackenzie, KeyCapture (www.dynamicservices.com/~will/academic/textinput/keycapture), 2003.

[10] H. Wolfe, Computer forensics, *Computers and Security*, vol. 22(1), pp. 26-28, 2003.

[11] M. Wyer and S. Eisenbach, LEXIS: An exam invigilation system, *Proceedings of the Fifteenth Conference on Systems Administration*, 2001.