C L R C

CNSG/ P111/2004

RUTHERFORD APPLETON LABORATORY
BITD

COMPUTER AND NETWORKS SECURITY GROUP

Computer Misuse Investigation - Seizure and Examination Process

Matthew Joyce
September 2004

1.A INTRODUCTION

1.2 Overview of the process

1.2.1 Investigation Scope

This document describes the process for investigating the possible misuse of a computer system.

The process includes:

- How investigations are authorised
- How the seizure of evidence is authorised and conducted
- How examinations of seized computers and media are carried out
- An investigation report template

1.2.2 What this process does not include

This process does not include the HR process that accompanies a misuse investigation, including any disciplinary process.

1.2.3 Process roles

The process defines three key roles:

- The investigator: leads an investigation, directs an examiner, but does not directly view any seized computer or media.
- The examiner: seizes and searches computer media for evidence of misuse.
- The HR Case Officer: liases with investigator to ensure that the investigation answers any specific allegations that have been made and that enough detail is provided to bring an HR disciplinary process to a conclusion.

1.3 Audience for this document

- CCLRC HR staff conducting investigations
- CCRLC Information Security Officers
- CCLRC Staff performing investigator and examiner roles

1.4 Illegal material

For the purposes of this document, the term "illegal material" is defined as any indecent photograph or pseudo photograph of a child.

During an investigation an examiner may find illegal material and viewing that illegal material without a legitimate reason may be a criminal offence. The process

specifically incorporates procedures to allow an examiner who views illegal material during the course of an investigation, to clearly establish that they had a legitimate reason for doing so, for their viewing of the material to be recorded and corroborated by a second examiner and for further access to the material to be immediately prevented, pending handover of the investigation to the police. These steps are as agreed with Manches, CCLRC legal advisers.

The investigation process may uncover other material that is technically illegal, such as images that are obscene or outrage public decency or material that is being stored or transferred in breach of copyright, such as digital music or video files. This type of material is referred to as "unacceptable material" in this document. Storing or distributing such material using CCLRC systems is contrary to the CCLRC Acceptable Use Policy and will be pursued using CCLRC disciplinary procedures.

1.5 Applicability

This process wil be used when investigations are performed into misuse of CCLRC computer systems or networks by CCLRC staff or any other person.

2. ROLES

There are a number of roles defined in this process:

HR Case Officer	the HR representative who arranges the authorisation for seizure, takes part in the seizure and receives the report of the investigation.
CCLRC Information Security Officer	authorises investigations and seizure of evidence. Deputy for approving investigation requests is BITD Director or BITD Directors assigned deputy.
HR Director	authorises investigations and seizure of evidence.
Investigator	the senior member of staff who instructs the examiners, and liases with the HR Case Officer during the investigation process. This is normally the Information Security Officer.
Examiner	the technical member of staff who takes part in the seizure, examines the seized machine and media and prepares the report

The last two roles are specific to this investigation process and the requirements for the Investigator roles are as follows;

2.1 Investigator requirements

- Senior member of staff.
- Understanding of forensic processes and software.
- Ability to instruct examiners clearly what is being searched for.
- Understanding of the CCLRC policies & legal requirements surrounding seizure, investigations and illegal material.

2.2 Examiner requirements

- Experience of hard disk removal and installation.
- Understanding of disk formats.
- Understanding and experience of preserving evidence on computer media.
- Experience of forensic examination software.
- Understanding of common applications and data file formats.
- Methodical approach with understanding of why detailed handwritten logs are required and how to report back to investigator.

- Can perform seizures and examinations quietly and discretely.
- Willingness to examine machines that may have illegal material on them.

3. INVESTIGATION KICKOFF

3.1 Authorisation for an investigation to begin

Prior to an investigation beginning, authorisation must be given for the investigation to begin.

An Information Security Officer or an HR Case Officer can request that an investigation is performed. The request must be made to the HR Director or an assigned deputy and to the CCLRC Information Security Officer or an assigned deputy.

Written consent is required on paper or in email from both the HR Director and the Information Security Officer to begin the investigation.

When permission is given:

- An Investigator must be assigned.
- If an HR case officer is not already assigned, an HR case officer must now be assigned.

4. SEIZURE OF EVIDENCE

Seizing evidence is a serious step in an investigation and will only be taken when the matter being investigated cannot be resolved in any other reliable way.

1.1 Authorisation to seize computers or other evidence

In an investigation, it may be required to seize one or more computers and associated media such as CDROMs, floppy disks or magnetic tapes to examine for evidence.

The HR case officer or Investigator can request that evidence is seized. The request must be made to the HR Director or an assigned deputy and to the CCLRC Information Security Officer or an assigned deputy. Written consent on paper or in email is required from both the HR Director and the Information Security Officer before any evidence can be seized.

1.2 Remote examination of evidence

It is sometimes possible to remotely examine computers over a network, however this method is unreliable and unrepeatable. It is unreliable because it is possible for a user to configure a computer to hide evidence from a network search and it will also not uncover evidence that the user has stored on removable media, such as CD-R. It is unrepeatable because the computer remains in the possession of the user and if the users chooses to, they can remove or alter any evidence at any time and so a subsequent examination of the computer may not produce the same results.

Remotely examining a computer over a network is permitted if that examination is a precursor to seizing the computer for a full examination. However the results of a examination of a computer over a network are not to be used as the primary evidence in an investigation.

1.3 Seizure of non-CCLRC computers

CCLRC does not have authority to seize non-CCLRC computers. If a non-CCLRC computer is involved in a misuse incident, other means of investigating the incident will be used where possible, such as capturing and examining network traffic or examining audit logs on servers, firewalls and other network devices.

1.4 Seizure of shared computers

An investigation may show that evidence is stored on a shared computer, such as a networked file server. Seizing the shared computer without providing any alternative may cause unjustifiable disruption to users. In this case, there are two possibilities:

- Seize a backup of the shared computer to restore and examine the backup on a similar computer.
- Seize the shared computer.

- If the shared computer is a high impact system, the disaster recovery plan for that system will be used to provide users with a replacement service.

- If the shared computer is a low impact system, then the effect of the computer being seized is not significant.

Seizing a backup of the shared computer is preferred as it causes less disruption to users of the shared resource but allows the examination to continue.

If seizure of a shared resource is required, negotiation with the resource owner must take place, before an appropriate solution can be chosen. Seizing the shared computer will be necessary when illegal material has been discovered on a shared resource, as it is not possible for CCLRC to allow illegal material to continue to be available on a shared resource. In this case, the decision of what will be seized will be made by the police to whom the incident has been reported.

There may be other solutions that are feasible on a case-by-base basis.

5. PROCESS FOR SEIZURE OF EVIDENCE

1.5 The HR case officer and investigator agree what must be seized.

Rationale: Normally one or more computers are the evidence that must be seized. Occasionally additional media may need to be seized, such as CDROMs or floppy disks and this is dependent upon the nature of the investigation.

1.6 Permision for the seizure is requested.

Rationale: Seizing evidence is disruptive. Seizures must be performed with the authority of the HR Director and the CCLRC Information Security Officer.

1.7 The investigator decides how the evidence should be seized.

Rationale: The investigation may require that the staff member is unaware that their machine is being examined, in case the staff member destroys any incriminating material. If this is the case, the media from the machine should be seized and imaged overnight or over a weekend or any other period when the user if not present. A copy of the media may be replaced in the original machine. However it should be noted that this process is technically difficult and full seizure of a computer is preferred. If illegal material is believed to be involved, then a copy of the media must not be replaced in the original machine.

1.8 The investigator requests that staff are assigned to be examiners for this investigation.

Rationale: Examiners are assigned to investigations according to the likely material to be examined. There is a pool of staff who have the requisite technical skills to perform the role of examiners, however not all of those staff are prepared to examine material when there is a risk that illegal material may be viewed or when the material is simply pornographic.

1.9 The HR case officer identifies whether the evidence is in a shared office or a locked office and plans accordingly.

Rationale: If the evidence is in a locked office, then the HR case officer must arrange for access to the office. If the evidence is in a shared office, the HR case officer must be prepared to answer questions from other members of staff who might be present during the seizure.

1.10 The examiners are given at least 24 elapsed hours notice of the planned seizure time by the investigator.

Rationale: The examiners must be prepared to perform the seizure and have adequate notice.

1.11 The HR case officer arranges for the staff member being investigated to be removed from their office while the evidence is seized. <u>If the staff member is present when the seizure takes place, the examiners will refuse to seize the evidence.</u>

Rationale: The examiners who take part in seizing the evidence should remain anonymous to the staff member during the investigation. If the staff member knows who the examiners are, the staff member may contact them directly to discuss the case or to put pressure on the examiners. After the investigation, the examiners may have to provide face-to-face technical support to the staff member and this may be difficult if the staff member knows that the examiners were involved in the investigation.

1.12 The HR case officer and the examiner go to the location of the evidence

Rationale: The HR case officer must be present to answer any questions from other members of staff who are present during the seizure. The examiners will not answer questions from other members of staff.

1.13 Any computers to be seized are physically disconnected from the network.

Rationale: The computers are physically disconnected to prevent remote users from connecting to those computers and altering or deleting evidence.

1.14 A check is made of the processes running on the computers and any disk encryption software disabled, if possible.

Rationale: If any disk encryption software is found to be running, then if this is not disabled or reconfigured before the machine is turned off, the encrypted disk partitions or files may be irretrievable. It is preferred to use the disk encryption software to unencrypt disk partitions or files. If this cannot be done, then the users cooperation may be required to examine the machine.

1.15 Power to the computers is turned off.

Rationale: To turn the power off immediately is the only way to guarantee that information is preserved on the machine. Turning the power off will lose the contents of memory and may damage some application files. But to use the normal operating system halt procedures may trigger cleaning scripts or programs that automatically remove evidence.

1.16 Computers are removed to examination area.

Rationale: Any examination must take place in a dedicated location where access to any examined machines is limited to authorised staff and unauthorised staff cannot accidentally view the examined machine, in case illegal or obscene material is displayed on the monitor at the time.

6. EXAMINATION PROCESS

1.17 The examiner installs the media onto a standalone dedicated examination computer in a secure location.

Rationale: A standalone dedicated examination computer is used, so that any illegal material remains isolated on the examination computer, no network connections can be made to the examination computer and that machine may be returned to a known state after an examination. The examination computer should in a secure location where only authorised staff can access the computer or view the screen.

1.18 A copy of the original media is made. The original media will be stored securely and all examinations will be made on the copy of the original media.

Rationale: The original hard disk must be preserved in exactly the state that it was taken from the machine. It is not sufficient to rely on a forensic software package to make an image of the disk and to store the image, while working on the original media, as this process

1.19 The investigator gives instructions for the examination to the examiner.

Rationale: There is a separation of duties between the investigator and the examiner. The investigator may know the user involved and the circumstances leading to the investigation. The examiner does not necessarily need to know any details of the case, but is given a clear set of instructions of what is to be examined and what to look for.

1.20 The examiner takes hand written notes in an examination log of each action they perform.

Rationale: The examiner has to demonstrate that they conducted the examination in an orderly manner and that any findings are repeatable and reproducible.

1.21 If suspected illegal material is found, then the examiner will immediately stop the examination and summon a second examiner. The second examiner will read and countersign the first examiners examination log, including the date and time when they joined the examination.

Rationale: If suspected illegal material is found, then the examiner must demonstrate that they have a legitimate reason for showing or distributing the material. The second examiner will corroborate the recorded actions of the first examiner and confirm that the illegal material was discovered during a legitimate examination of another users computer. Offences under Section 1, subsection 1b or 1c of The Protection of Children Act 1978 or under Section 160 of the Criminal Justice Act allow a defence that a person has a legitimate reason for having an indecent photograph of a child in their possession or showing or distributing an indecent photograph of a child. This examination process is designed to allow each examiner to corroborate each other's legitimate reasons for possessing or showing any illegal material.

1.22 If either examiner believes that illegal material has been found, then the examination is halted, a record of the date and time made in the examination log. The police will then be informed, a note made of the date and time in the

examination log and both examiners will sign the log. The examination computer will be turned off immediately and all media will be handed over to the police who will continue the investigation. The examiners must not contact the investigator, HR or any other staff members until the police have given them permission to do so, as the police will conduct the investigation from that point onwards.

Rationale: When the police are called, all copies of the illegal material must be given to them, to avoid any illegal material remaining on site. Recording the date and time of finding the suspected illegal material and then the time of the report to the Police is necessary to show the report was timely.

1.23 The examiner reports the results of the examination to the investigator. If necessary, further examination steps may take place.

Rationale: The examiners role is limited to copying and searching the media and reporting the results to the investigator. The investigator communicates the results of the examination to the HR Case Officer, but does not view the material in question.

1.24 The investigator writes an investigation report, including summarised conclusions from the examiner report and attaches the examiner report as an annex. This investigation report is delivered to the HR Case Officer.

1.25 If required, the Investigator will ask the examiners to compile a sample of the evidence to present to a disciplinary panel. The investigator will present the evidence sample to the committee.

7. INVESTIGATION REPORT

The investigation report should take the following format:

Title page

CCLRC Misuse Investigation

User: *user name*

Date: *date of investigation report*

Investigator: *Investigator name and job title*

Computer: *computer identifier*

Section1: Investigation Summary

The summary describes the reasons for the investigation starting, a brief overview of the investigatory steps taken and a summary of the conclusions.

Section 2: Investigation Background

A detailed description of how the investigation was initiated, including who authorised the investigation. This must include the specific allegations that the investigation must investigate.

Section 3: Investigation Details

A thorough account of the investigation, including all details of any seizure of evidence that were performed.

Section 4: Investigation Conclusion

The conclusions from the investigation, including an opinion about each of the specific allegations that the investigation was asked to examine.

Annex A: Examiners report

If applicable, a copy of the technical report from the examiners.

8. INVESTIGATION WRAPUP

1.26 The original media, the examination notes and the results of the examination are securely archived.

Rationale: The original media must be stored in case another examination needs to be conducted. The examination notes and results must be stored in case a question arises about how the examination was conducted.

1.27 The mirrored media, any other media used during the examination and the examination computer are securely erased.

Rationale: If another examination is required, then another mirrored copy can be created from the original media. If illegal or incriminating material was discovered, then this must be securely erased from the mirrored disk, any temporary media used, and the media on the examination computer.

1.28 If access to the disk contents is required to retrieve data to allow other processes to continue, then data from the mirrored disk can by recorded onto CDROM and delivered back to the department. A copy of the data delivered to the document will be kept in case of any later disputes.

Rationale: The original media must remain archived as evidence, and the mirrored media must not be returned to the department as it may contain illegal or incriminating material that has not yet been discovered.

1.29 When the examination does not find any evidence, then with the permission of the investigator, all original media will be returned to the user, or if the user is unaware, the media will be securely erased.

Rationale: There is no reason to keep copies of media if the investigation found nothing.

1.30 When the examination does find evidence, then after the end of any proceedings (employment tribunal, civil case, etc.) and after any appeal period has lapsed, the media will securely erased or otherwise destroyed.

Rationale: It is necessary to keep the original evidence in case a re-examination is required.