

Information Technology Security Guide
Lead Agency Publication G2-008



Computer Forensics:

A Guide for IT Security Incident Responders

Technical Security Branch
Technical Operations
Royal Canadian Mounted Police
Issued: May 2008

Disclaimer of Responsibility

This publication has been prepared by the RCMP for the use of departments or agencies in the Government of Canada. The publication is informal and limited in scope. It is not an assessment or evaluation and does not represent an endorsement of any sort by the RCMP. The material in it reflects the RCMP's best judgment in light of the information available to it at the time of preparation. Any use a third party makes of this publication, or any reliance on or decisions made based on it, are the responsibility of such third parties. The RCMP accepts no responsibility for damages, if any, by any third party as a result of decisions or actions based on this publication.

Copyright 2008 Government of Canada, Royal Canadian Mounted Police (RCMP)
1200 Vanier Parkway, Ottawa, Ontario, Canada, K1A 0R2

This publication may be reproduced verbatim, in its entirety, without charge, for educational and personal purposes only. However, written permission from the RCMP is required for use of the material in edited or excerpted form, or for any commercial purpose.

TABLE OF CONTENTS

- 1 Introduction 1**
 - 1.1 Purpose..... 1
 - 1.2 Assumptions 2
- 2 Problem Overview 2**
- 3 Best Practices..... 2**
 - 3.1 Incident Handling and Response 2
 - 3.2 Detection of Computer Security Incidents..... 3
 - 3.3 Law Enforcement Involvement..... 4
 - 3.3.1 Pre-Law Enforcement Actions 4
 - 3.3.2 Contacting Law Enforcement 5
 - 3.4 Legal Considerations 6
 - 3.4.1 Evidence..... 6
 - 3.4.2 Rules of Evidence 6
 - 3.4.3 Chain of Custody 7
- 4 Conclusion 8**

1 Introduction

IT security incidents and computer related crimes have become increasingly common occurrences in the workplace. Law enforcement is called upon to deal with the latter every year. Not every computer incident, however, is an actual crime. Theoretically, Government of Canada departmental IT security personnel should handle all IT security incidents deemed violations of the Departmental Security Policy (DSP). Where the incident is, or appears to be, criminal in nature, federal government departments and agencies must consult law enforcement as soon as possible. However, since the priority for law enforcement is crime, it is beneficial for all parties involved that departments are reasonably certain a crime has been committed before it is reported.

At the moment a suspicious behaviour or incident has been identified, IT security incident responders must be ready to react to the situation quickly and effectively to contain the damage, communicate the situation to appropriate parties, implement the necessary countermeasures, restore the affected service, and, finally, perform a post-incident review to verify the effectiveness of current incident response processes and procedures. In order to facilitate an appropriate response to IT security incidents, it is important to document how all the aforementioned steps will be followed. Thus, the creation of a formal “incident response plan” or procedure should prove to be extremely valuable, serving as guidance both prior to, and in response to, IT security incidents.

During preparation of the plan or procedure, it is important to think about how computer forensics integrates with each of the steps mentioned above from the moment an incident is detected to post-incident analysis. For example, the “restoration of service” step in particular, could have profound effects on a criminal investigation if certain precautions are not observed. In order to keep computer forensics in mind during the preparation or revision of an incident response plan, it is important to have a better understanding of what “computer forensics” really means.

“Computer forensics” can be described as the “preservation, identification, extraction, documentation and interpretation of computer data.”¹ When searching for materials on the subject, several other terms may be considered synonymous such as data forensics, network forensics and digital forensics. However, some may argue the differing terminologies could imply a more focused, or specialized, area of analysis.

“Computer forensics is now an established set of disciplines and the very high standards in place for preserving material from personal computers creates high expectations of other forms of digital evidence, including those from large corporate systems and networks, across the Internet and the emerging families of personal digital assistants (PDA), mobile phones and portable media units.”²

For the sake of this document, we prefer to use the quote above to define and generalize “computer forensics” since it implies other systems, devices or networks are included as possible sources for evidence and forensic analysis.

1.1 Purpose

This document is intended to provide first responders such as IT security and/or administrative personnel with technical guidance as it relates to IT security incident response and computer forensics. Federal government departments and agencies may use this guide to develop and/or update IT security incident response plans or procedures. Up-to-date incident response plans, or procedures, and documentation can play an important role when IT security personnel are required to hand-over incident investigations, which appear “criminal” by nature, to law enforcement without compromising or damaging the digital

evidence. This guide will help to clarify the definition of computer crime, provide an overview of law enforcement involvement and legal considerations, recommend best practices for IT incident response, and other related information.

This guideline is intended to be preliminary in nature. It is not intended to be a detailed treatment and may be updated periodically as forensic methodologies and best practices evolve.

1.2 Assumptions

Departmental Security Policy (DSP) – This document assumes that the department is compliant with Treasury Board Secretariat’s *Management of Information Technology Security (MITS)* Standard and has a departmental security policy in place. The DSP should outline specific details regarding topics such as monitoring of network usage, acceptable use of computing resources, audit policies and more.

Departmental Incident Response Policy – This document also assumes that the department has established linkage to Public Safety Canada’s Canadian Cyber-Incident Response Centre (CCIRC) and has an incident response plan in place. This is a policy/plan to be implemented in the event of a computer security incident.

2 Problem Overview

Computer crimes have become a regular subject in the news headlines. As common as these incidents may be, it is likely that violations of departmental Acceptable Use Policies (AUPs) are even more common. Although it can be assumed crimes are always violations of a department’s AUP, on the flip-side, violations of departmental security policy are not always crimes. Herein lies the problem.

What happens when an incident is discovered and it is unclear as to whether a law has been broken? Computer forensics is a task best left to properly trained professionals, especially when there is an expectation that evidence uncovered during the investigation may end up in a court of law. At the same time, law enforcement units are often already dealing with a heavy workload and cannot be called out to investigate every incident that may only be violations of the DSP and not a crime. Reasonably dealing with this dilemma is discussed in this guide. This document outlines the best practices a department or agency can implement to ensure the preliminary investigations of IT security incidents go smoothly.

3 Best Practices

3.1 Incident Handling and Response

Incident response involves having standardized methods for responding to incidents of all sorts. In this case, the plan will deal specifically with IT security incidents. During incidents like these, it is important to assume the worst and downgrade the situation from there. In accordance with MITS’ Operational Security Standard, departments must have an IT Security Coordinator to manage information security incidents and report them to upper management.³ All federal departments must also have incident response plans in place. Individuals responsible for responding to these events must take detailed notes of actions taken to discover, mitigate and investigate an incident.⁴

One of the most important reasons for taking such detailed notes is many incidents that are actually serious in nature often start out as innocuous system abnormalities. A small glitch may turn out to be only the tip of the iceberg. Suspected policy violations can quickly turn into full-blown crimes. The key here is that as soon as an incident is determined to be a crime, law enforcement must be contacted. At this point

in time, the internal investigation should cease immediately until advice from law enforcement has been sought. This step is to avoid compromising the investigation in any way and also to avoid the possibility of breaking the law during the course of the investigation.

3.2 Detection of Computer Security Incidents

Initially, one of the most important aspects of incident response is how an IT security incident will be detected. Without detection there can be no way to know that an unauthorized event has taken place on the network. The incident that kicks off an initial investigation may be completely innocuous and can be as simple as abnormal system or network performance. In the end, the key is to treat even abnormal system behaviour as suspicious and this means taking care when collecting information (evidence) about the problem. If the system is treated carefully and a crime is discovered, it will be less likely that the crime scene has been altered. If the incident turns out to be benign, the investigator is in a better position to resolve the problem and has better notes from which to work.

However, to be able to detect these abnormalities one needs to know the normal operating parameters. To know this, IT personnel must carry out preparatory work in advance of a computer security incident. It is necessary to document the behaviour of the systems, devices, operating systems and networks with which one works each day. Aside from detecting computer security incidents, this will also allow personnel to determine if there are other problems occurring. Creating these thresholds can be done in several ways and/or areas:

- Set-up baseline installations for each group of systems
 - Document which operating system patches are installed, which third party software is installed and if it is patched. Also document any non-standard configurations on the systems.
- Baseline the system performance (know what sort of performance is normal/abnormal)
- Baseline the system usage (know what sort of load is normal/abnormal)

Other methods for detecting incidents and attacks include calls from attentive users to the help desk. Users are often some of the first people to notice that something is no longer working properly or that a system is exhibiting abnormal behaviour. MITS (s.14.2) stresses that it is important for departments to train their help desk staff on how to respond to security incidents.⁵ When users call in with information about an incident, the help desk must have documented response procedures that explain which IT security personnel to notify and what instructions to provide the caller.

Another very common method for detecting IT security incidents is to make use of technologies that monitor systems and networks for security breaches. Detection tools create alerts, such as log files, alert emails and other sorts of notices to draw attention to something that may be a problem. There are many types of devices and applications that can perform these duties. They include but are not limited to:

- Firewalls (log files)
- Routers (log files)
- Host Intrusion Detection Systems (HIDS)
- Network Intrusion Detection Systems (NIDS)
- File Hashing Programs (programs that pre-compute hashes for critical system files and allows you to validate the hashes after an incident)

In compliance with MITS, Section 17 states that departments must, at the very least, have an audit log function in all their IT systems.⁶ High-risk systems must be better protected. This involves implementing

real-time, automated, incident detection devices or applications. The implementation of these different types of defences is, however, subject to applicable laws and policies.

3.3 Law Enforcement Involvement

Law enforcement involvement in a computer security incident investigation can be a complex issue. Sometimes it will lead to a preference not to involve the police. Historically, the initial response to a security violation may not include reporting the matter to the police. However, it should be noted that law enforcement agencies can provide numerous advantages such as:

- Provide technical data, hacker profiles, file signatures and hash values
- Provide legal options for a criminal case
- Provide IT security guidelines and best practices
- Coordinate Internet Service Provider (ISP) cooperation
- Develop targeted operational activity (based on high numbers of reported incidents)
- Track down a suspect
- Statistical analysis of trends, vulnerabilities and criminal methods leading to the development of new and/or improved countermeasures

In accordance with Treasury Board Secretariat's *Government Security Policy (GSP)*, as soon as an incident has been determined to be a crime, the law enforcement agency of proper jurisdiction must be called.⁷ Depending on the type of threat or incident (e.g. a threat to national security), the department or agency may be required to notify other agencies such as CSIS and Public Safety Canada.⁸

3.3.1 Pre-Law Enforcement Actions

In most cases, a computer security incident investigation begins with the technical personnel on-site. This is the logical first step since they are responsible for the systems and their security. Since it would be very difficult, if not impossible, for law enforcement to get involved in reacting to every detected incident (not yet deemed a "crime"), it can be expected some investigative work will have to be performed by technical staff.

The key point is to investigate the suspect system only to the extent strictly necessary to determine if police involvement is required. This is especially true if it is already clear that the problem is security related. The personnel performing this initial examination must take notes of everything they do and touch. Each page of the notes should be signed and dated. These notes will be invaluable should the incident be escalated to a criminal investigation.

The steps taken during this initial phase of the investigation will always vary depending on the situation and the type of system(s) analyzed. Unfortunately, maintaining a comprehensive list of DOs and DON'Ts is not feasible as the list would be constantly changing to account for evolving technologies and methodologies.

The best way to understand basic computer forensic principles and methodologies is to attend formal hands-on training courses in the subject area. These courses and seminars can be found across Canada and the United States. They can provide basic to advanced training, an understanding of important forensic and legal concepts and hands-on experience analyzing sample systems.

Since many forensic training providers are based in the United States, it is important to remember that while the basics of computers and their functions remain the same, the differences between Canadian and

American law can be significant. What may be considered a computer crime in one country may not necessarily be considered a crime in the other.

These training courses also cover the use of a variety of forensic tools that can be used to analyze a suspect system. Today there are many companies that offer forensic toolkits for conducting investigations and gathering evidence for presentation in court. There are also many open-source programs available.

The key issue when selecting a toolkit to use is the credibility it is seen to have in court. Guidance Software's EnCase and AccessData's Forensic Tool Kit (FTK) are two of the more common toolkits used by investigators. Both applications are considered acceptable in Canadian and American courtrooms. As well, both companies offer proprietary training and certification for investigators to assure proper use of the toolkits.

Today, computer crimes keep law enforcement personnel very busy. Once an incident has been deemed a crime, and the department or agency has called to report the incident, there is a possibility the response by law enforcement will not be immediate to the site. If there is a risk crucial data may be lost or compromised before law enforcement arrive, it may be necessary for the department or agency to take preventive and immediate action. An example of this type of situation would be when there is a need to acquire volatile data from a suspect system before it is altered or destroyed.

- Volatile data – Data that will be lost or changed in a short period of time or when the system power is lost (turned off). Examples of this would be the memory in a computer system (system RAM) or operational data held by routers.

Clearly, there is a need to acquire this type of data from memory before it is altered or lost. The memory could be storing evidence of actions taken on the system, or information regarding processes running in memory at the time of the incident. If there is a situation when volatile data might be lost if not acquired immediately, and police officers are not able to attend immediately, then the systems administrator or technical security personnel should acquire and preserve that information for law enforcement to analyze.

The technical staff should document exactly what they are doing in writing. Thus, the data and the written notes can be efficiently handed over to police when they arrive. In some circumstances, police must work with the “best evidence” obtainable. It may not be ideal but it may be the best available for the situation at hand. In the end, it is important to remember that police forces exist to help. If in doubt, err on the side of caution.

The United States National Institute of Standards & Technology has written an extensive document for IT staff operating as the first-line of response during a computer incident. For further information and material please refer to their guide, *First Responders Guide to Computer Forensics: Advanced Topics*.⁹

3.3.2 Contacting Law Enforcement

Contacting law enforcement is a decision that needs to be made by the victim. Every incident is different and the need for police involvement may become clear at different points during each investigation.

In some cases, it is difficult to distinguish between incidents considered “criminal” versus DSP violations. Sometimes it is obvious that a crime has been or is being committed. Other times, it is not as clear and a professional, with knowledge of the *Criminal Code*, should be consulted. Federal government departments experiencing a computer security incident requiring police involvement should contact the appropriate RCMP Integrated Technological Crime Unit (ITCU). These units are located in the major

centres across Canada. Any suspected criminal activity/incident uncovered by any other agency should be reported to the police service of local jurisdiction.

Upon contacting the police, be prepared to provide details of the suspected criminal activity/incident. If all the facts are at hand, it will make it easier to determine if police involvement is required. Should the police be attending, be available to provide information.

The police will need to see all of the notes taken. Be aware that the police may need to seize the originals as evidence so it is a good idea to photocopy them first. System log files may also be requested. Whereby specific dates and times of an incident are key, such as log files, it would be a good idea to have the files printed. If possible, highlight the areas of concern--this will make them easier to locate. The information you provide police when they initially attend can determine the direction and scope of the investigation. Be prepared!

3.4 Legal Considerations

For the sake of this document, “computer crimes” can be defined as criminal acts involving a computer or network. However, in terms of computer forensics, digital evidence can also be used to support the prosecution of other criminal offences. The following sections in the *Criminal Code of Canada* outline the specific acts in relation to computers, networks and data that are considered criminal in Canada.

- s.326 – Theft of telecommunications service
- s.342.1 – Unauthorized use of a computer
- s.342.2 – Possession of device to obtain computer service
- s.430.1.1 – Mischief in relation to data

3.4.1 Evidence¹⁰

When dealing with computer forensics and computer crime investigations, the term “evidence” has the following meaning: “Any information related to an incident in physical or binary (digital) form that may be used to support or prove the facts of an incident.” The concept of “best evidence” refers to evidence that most closely matches the original or real evidence. This can be original media or it may be the most forensically sound copy of the data (a bit-stream copy) available.

Sometimes law enforcement agencies have to make do with best evidence. This is often the case when an initial investigation is handed over to police. The police would also be dealing with best evidence if a live system capture had been performed prior to the arrival of police to the crime scene. Therefore, it becomes important to understand police requirements for preliminary investigations and evidence handling so as to be able to provide the officers with the best possible evidence from which to work.

3.4.2 Rules of Evidence¹¹

The rules of evidence are very precise and exist to ensure that evidence is properly acquired, stored and unaltered when it is presented in the courtroom. The rules require digital evidence to be:

- **Authentic** – The integrity and chain of custody of the evidence must be intact.
- **Complete** – All evidence supporting or contradicting any evidence that incriminates a suspect must be considered and evaluated. It is also necessary to collect evidence that eliminates other suspects. One must not only be able to prove that it was the accused who committed the crime but also that the crime was not committed by anyone else.

- **Reliable** – Evidence collection, examination, analysis, preservation and reporting procedures and tools must be able to replicate the same results over time. The procedures must not cast doubt on the evidence’s authenticity and/or on conclusions drawn after analysis.
- **Believable** – Evidence should be clear, easy to understand and believable. The version of evidence presented in court must be linked back to the original binary evidence otherwise there is no way to know if the evidence has been fabricated.

It is just as important to follow the rules of evidence in non-criminal computer forensics investigations for two reasons. First, non-criminal investigations can also end up in court. For example, a departmental security policy violation may lead to an employee dismissal. This employee, in turn, may eventually file a wrongful dismissal suit against the department. The evidence becomes critical to ensure the dismissal stands up in court.¹² Having a policy to backup the decision to dismiss is also important. It is a document the department can refer to as proof that the employee was aware they were violating the rules.

Second, a preliminary investigation can uncover criminal activity. Once an incident is deemed criminal, any and all work done to that point must measure up to Canadian legal standards to ensure evidence is admissible and to ensure the investigation has not been compromised.

In March 2000, the G8 put forward a set of proposed principles for procedures relating to digital evidence. These principles provide a solid base from which to work during any examination done before law enforcement attends.

- **G8 Principles – Procedures Relating to Digital Evidence¹³**
 - When dealing with digital evidence, all general forensic and procedural principles must be applied.
 - Upon seizing digital evidence, actions taken should not change that evidence.
 - When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
 - All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved, and available for review.
 - An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
 - Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

This set of principles can act as a solid foundation. However, as one principle states, if someone must touch evidence they should be properly trained. Training helps reduce the likelihood of unintended alteration of evidence. It also increases one’s credibility in a court of law if called to testify about actions taken before the arrival and/or involvement of the police.

3.4.3 Chain of Custody¹⁴

Chain of custody refers to the tracking of evidence items from the scene of a crime to the item’s presentation in a legal proceeding. Maintaining the chain of custody in cases where there is a strong reliance on digital evidence is critical. Digital evidence can be easily altered and a break in the chain of custody would undoubtedly compromise the evidential weighting in a criminal case. It is critical to know where evidence has been at all times from the moment of acquisition until the time it is presented in court.¹⁵ It is always the preference of law enforcement agencies that evidence not be touched before they attend, however, this is not always possible as previously discussed. In such cases, all actions taken by non-law enforcement personnel need to maintain the chain of custody, along with observing the rules of evidence.

4 Conclusion

Security-related investigations are complex situations requiring patience, technical expertise and knowledge of the law. They are the types of problems that should be tackled by an individual who has experience in the field. This is especially true if the incident is believed to be a crime. Technical personnel who will be responsible for responding to incidents within their departments or agencies should pursue computer forensics training. This will ensure a certain basic level of competence when dealing with an initial examination. It will also lessen the likelihood of basic mistakes being made during an analysis of the system in question.

If it is preauthorized by DSP and determined to be appropriate, technical staff, preferably following guidance from a police expert, may acquire data or information from a suspect system. This should only be done to the extent that is strictly necessary. All actions must be noted in detail and the notes should be signed and dated. Copies of these notes must be given to police attending the scene at a later time.

Should a crime be suspected or confirmed, leaving the system alone and contacting the law enforcement agency of proper jurisdiction is the best approach. The police will provide guidance on the intricacies of forensics and Canadian criminal law.

Forensic methodologies and technologies change constantly and this makes an already complex field of expertise one in which it is hard to remain current. However, by taking recognized forensics courses and maintaining a willingness to involve experts in law and computer forensics during an investigation, there is a greater chance investigations will go smoothly and will result in a positive outcome for those involved.

The RCMP will continue to update this document as best practices, tools and methodologies evolve.

¹ Warren G. Kruse and Jay G. Heiser, *What Exactly is Computer Forensics?* (June 2004) at 1, online: IT Observer <<http://www.ebcvg.com/articles.php?id=220>>

² Peter Sommer, *Directors and Corporate Advisors' Guide to Digital Investigations and Evidence* (September 2005) at 9, online: Information Assurance Advisory Council <<http://www.iaac.org.uk/Default.aspx?tabid=65>>.

³ Treasury Board Secretariat, *Operational Security Standard: Management of Information Technology Security* (14 April 2004) at 3, online: Treasury Board Secretariat <http://www.tbssct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp>.

⁴ *Ibid.* at 15.

⁵ MITS s14.2

⁶ *Ibid.* s17

⁷ Treasury Board Secretariat, *Government Security Policy* (1 February 2002) at 11, online: Treasury Board Secretariat <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp>.

⁸ *Ibid.* at 11.

⁹ The NIST document can be found here: <http://www.cert.org/archive/pdf/05hb003.pdf>

¹⁰ Communications Security Establishment, *Government of Canada Information Infrastructure Protection: Computer Forensics – Concept of Operations* (Ottawa: Cinnabar Networks Inc., 2004) at 17.

¹¹ *Ibid.* at 18.

¹² National Infrastructure Security Coordination Center, “An Introduction to Forensic Readiness Planning,” (May 2005) at 3, online: NISCC <<http://www.niscc.gov.uk/niscc/docs/re-20050621-00503.pdf>>.

¹³ International Organization on Computer Evidence, “G8 Proposed Principles for the Procedures Relating to Digital Evidence” (March 1998) at 1, online: National Center for Forensic Science <<http://ncfs.org/documents/ioce2002/reports/g8ProposedPrinciples.pdf>>.

¹⁴ *Supra* note 5 at 18.

¹⁵ *Supra* note 1 at 26-27.