GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

S. Grace
Security Essentials Level One Practical

# Computer Incident Response and Computer Forensics Overview

## Introduction

When a compromise of security or an unauthorized/illegal action associated with a computer is suspected, it is important that steps are taken to ensure the protection of the data within the computer and/or storage media. The stored data is needed to determine the level of security compromise and location of potential evidence concerning the unauthorized or illegal act.

The initial response to a computer security incident may be more important than later technical analysis of the computer system because of the actions taken by incident response team members. Actions taken by the incident response team impact subsequent laboratory examinations of the computer and/or media. Of most importance is that the first responder act appropriately.

In the event of a suspected computer incident, care must be taken to preserve evidence in its original state. While it may seem that simply viewing files on a system would not result in alteration of the original media, opening a file changes it. From a legal sense, it is no longer the original evidence and may be inadmissible in any subsequent legal or administrative proceedings.

This paper will focus on the incident response and computer forensics on the personal or desktop computers. The incident response and forensic procedures and techniques for servers may additional knowledge and tools.

## Incident Response

Every organization should have an incident response team. This team may consist of one person in an organization or several persons. In the event of suspected computer crime or violations of user policies, the team should be activated. The team should have written procedures for incident response, including what conditions warrant calling in local and/or federal law enforcement authorities. Violations of user policies may result in administrative actions whereas suspected computer crimes may require that law enforcement authorities be called in. The incident team needs to protect evidence for either situation. For administrative actions, the procedures described in this paper may be sufficient. However, for suspected computer crimes, the law enforcement officials may instruct the incident team to wait for their arrival.

The activities/procedures for securing a suspected computer incident scene include

- Securing the scene
- Shutting down the computer

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Labeling the evidence
- Documenting the evidence
- Transporting the evidence
- Providing chain-of-custody documentation

The computer incident response team should keep in mind that what begins as a collection of evidence for violation of administrative policy violations may escalate into collection of evidence for more serious violations. The computer may have also been used to commit illegal activities that are subject to civil and/or criminal penalties. For example, a company incident response team may be seizing an employees computer to collect evidence for misuse of the Internet (excessive surfing and/or visiting porn sites) privileges and subsequently discover that the employee was using the company computer to develop and release damaging viruses and/or using it to hack into other computers. The later two uses of the employees' computer may result in civil/criminal prosecution. In order to properly handle the potential evidence, it must be assumed that the worst has occurred and that the potential evidence be treated appropriately.

The entire work area, office, or cubicle is a potential crime scene, not just the computer itself. The work area should be secured and protected to maintain the integrity of the scene and the storage media. While waiting for the official incident responder, no one should be allowed to touch the computer, to include shutting the computer down or exiting from any programs/files in use at the time or remove anything from the scene. All individuals at a scene should be known and briefly interviewed to determine their access to the computer and work area before asking them to leave.

Once initial security has been established, the scene should not be left unattended or unsecured until the processing of the scene is completed. Only those directly involved with the incident response should be allowed in the area. Notes should be maintained regarding how scene security was established to include the identification of persons at the scene.

Under no circumstances should anyone, with the exception of qualified computer forensics personnel, make any attempts to restore or recover information from a computer system. It is important to remember that that the data present within the storage media is potential evidence and should be treated accordingly. Any attempts to retrieve data by unqualified individuals should be avoided as these attempts could either compromise the integrity of the files or result in the files being inadmissible in legal or administrative proceedings.

Shut Down Procedures (reference: U.S. Department of Energy)

One of the most difficult decisions is dealing with power-down of a computer system in a manner that will not corrupt the integrity of the files. In most cases the type of operating system will be the key to powering down the computer. With some operating systems, merely pulling the power plug is preferred method. With other systems, disconnecting the power supply without allowing the operating system to initiate internal shutdown

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

could result in loss of files to hard drive crash. Potential evidence may reside in typical storage areas such as the spreadsheet, database or word processing files. However, potential evidence may also be in file slack, erased files, and Windows swap files (reference: Anderson, M). Potential evidence in these locations is usually in the form of data fragments and can be easily overwritten by booting the computer and/or running the operating system. When Windows starts, it can create new files and open existing files causing erased to potentially overwritten and data previously stored in the Windows swap file to be altered or destroyed. Windows 95 updated directory entries for files as a normal operating process. If word processing or other program files are opened and viewed, temporary files are created and overwritten by updated versions of files making potential evidence stored in these locations subject to loss.

The following table provides shutdown procedures for various operating systems (reference: U.S. Department of Energy).

| Operating System | Shut Down Procedures |
|---|---|
| MS DOS | • Photograph screen and document any programs running<br>• Pull power cord from wall |
| UNIX/Linux | • Photograph screen and document any programs running<br>• Right click to the menu<br>• From menu, click **Console**<br>• If root user prompt (#) not present, change user to root by typing **su –**<br>• If root password not available, pull power cord from the wall<br>• If password is available, enter it. At the # sign type **sync;sync;halt** and the system will shutdown<br>• Pull power cord from the wall |
| Mac | • Photograph screen and document any programs running<br>• Click **Special**<br>• Click **Shutdown**<br>• The window will tell you it is safe to turn off the computer.<br>• Pull power cord from the wall |
| Windows 3.X/95/98/NT | • Photograph screen and document any programs running<br>• Pull power cord from wall |

The incident response team should use the table above unless special circumstances warrant immediately pulling the power cord to the computer/central processing unit (CPU). Special circumstances would include were the suspect initiated a self-destruct program or is in the process of reformatting the storage media. If the computer was already shut down prior to arrival, no attempts should be made to power-on the CPU.

Properly Marking Computer, Media, and Cables for Transport

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

All connections and plugs should be labeled and marked for evidence prior to disassembly using tape and/or tags to mark each end. The configuration should be documented and photographed prior to removal. Storage media should be collected in the state that they were found. Write protect media according to the following table.

| **Media** | **Write protect by:** |
|---|---|
| 5 ¼ inch disks | Place tape over the notch |
| 3 ½ inch disks | Place the write protect tab in the open position |
| Cassette tapes | Remove the record tab. |
| Removable hard drives | Place tape over the notch |
| Cartridge tapes | Turn the dial until the arrow is aligned with "safe" mark or white dot is facing out. |

Documentation

Detailed notes should be maintained during all aspects of the scene processing. This not only includes the usual who, what, where, when but overall observations of the scene. A evidence/property document should contain entries with a description of the items (model and serial number), any visible markings present on the item, the condition of the item, the manner it was marked for evidence and the location from within the scene it was seized. Every item of evidence has its own characteristics, but should be identified in a manner it can be easily identified at a later date. Items should be collected as found and documented.

Handling and Transportation

It is important that computer equipment be handled gently. The CPU should, in particular, should be handled gently. The "parking" of the heads in the hard drive provides some protection, but should always be assumed to not be parked. Mishandling of the CPU could result in hard drive failure.

The ideal packing material for a CPU is the original factory container, however is rarely available. If original packing is not available, then the CPU should be packed and carried as it was set up. Avoid turning the CPU upside down or lying on its side during transport.

Diskettes have fragile magnetic media. If they are packed loosely and allowed to strike each other repeatedly during transit, the media could be damaged and the data lost.

When transporting a CPU, devices, or media, they should not be placed in a vehicle trunk or area where there will be drastic changes in temperature. The ideal place for transport would be on the rear seat, placed in a manner where the CPU will not fall during sudden stop/start or other maneuvers.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Preserving Electronic Evidence

The incident response team's primary duty is the collection and preservation of the evidence. The incident team must store and/or immediately turn over the collected evidence and documentation to qualified forensics technicians. The forensic technicians may be qualified in-house specialists, consultants, and/or law enforcement agencies.

The Forensic Evaluation Process

The follow discussion is an overview of what typical steps are taken by forensics technicians and what evidence/forensic computer programs are available. There are various things that must be done with a confiscated computer to protect and preserve the electronic evidence before conducting forensics evaluations. The first thing the forensic technician should do is to make a complete bit stream backup of all the computer data before it is reviewed or processed and to validate the accuracy of the bit stream backup. Essentially, a forensically sound examination is one conducted under such controlled conditions that it is completely documented, it is repeatable it's results are verifiable. A forensically sound methodology also changes no data on the original evidence, preserving it in pristine condition. There are various software programs available for making bit stream backups and several were reviewed in SC InfoSecurity Magazine (reference: Holley, 2000). This article presents results of comparison testing of several commercial products, including:

- Byte Back by Tech Assist
- Drive Image Pro by PowerQuest
- EnCase by Guidance Software'
- Linux "dd" by Red Hat
- Norton Ghost 2000 by Symantec
- SafeBack by New Technologies
- SnapBack DatArrest by Columbia Data Products

There is specialized forensics training (reference: New Technologies, Inc. A.; and reference: Key Computer Service, Inc. A.) classes that may include use of specialized software programs that perform various forensics tasks. The are a variety of vendors that provide their own suites of forensics software. The New Technologies Corporate Evidence Processing Suite (reference: New Technologies, Inc. B) includes:

- CRCND5: CRC (checksum) program that validates the contents of one or more files.
- DISKSIG: A CRC program that validates mirror image backup accuracy.
- FILELIST: A disk catalog tool used to evaluate computer use time lines.
- FILTER I: An intelligent fuzzy logic filter for use with ambient data.
- GETFREE: An ambient data collection tool used to capture unallocated data.
- GETSLACK: An ambient data collection tool used to capture file slack.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- GETTIME: A program used to document the system time and date on a computer seized as evidence.
- NTI-DOC: A documentation program for use in recording file dates, times and attributes.
- SEIZED: A program used to lock and secure evidence computers.
- SHOWFL: A program used to analyze the output of file list.
- Text Search Plus: A text search utility used to locate key strings of text and graphic files.

The Key Computer Service suite of forensics software (reference: Key Computer Service, Inc. B.) includes:

- WIPER - a disk utility that will completely erase all information on a logical or physical drive.
- LISTDRV – a utility that examines FAT12, FAT16, or FAT32 files to a comma-delimited and quotation mark-delimited file prepared for importation into a database program or a spreadsheet program for any desired manipulation, including deleted files if desired.
- CHKSUM – a disk utility that calculates a 64-bit checksum for a physical or logical disk drive.
- FREESECS – a disk utility which searches a specified logical drive for the unallocated or free space, and saves the information.
- DISKDUPE– an assembly language utility that makes an exact forensic copies of floppy diskettes.
- DATASNIFFER- a utility that can "carve" data or files from files or unused space (when recovered with a utility like FREESECS).

Although there are highly specialized forensics software programs available, old programs, such as MS-DOS, are also useful forensics tools. MS-DOS is used to copy floppies using the MS-DOS Diskcopy command. Other useful MS-DOS tools include "Debug," "Undelete," and "Unformat" (reference: Mendell, 2001).

The reader should note that from the description of these tools that performing forensic analysis should be done by a qualified/certified trained forensic technician. The author is reminded of the expression "a little knowledge is dangerous" and it certainly applies in this situation. In order to effectively protect electronic media for possible administrative and/or civil/criminal prosecutions, only qualified/trained/certified technicians should be conducting forensics evaluations.

In summary, the forensic examination of seized computers and media includes several important steps. The computer forensic specialist should perform these steps (reference: Robbins):

- Protect the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
- Recover all (or as much as possible) of discovered deleted files.
- Reveal (to the extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
- Access (if possible and if legally appropriate) the contents of protected or encrypted files.
- Analyze all possibly relevant data found in special (and typically inaccessible) areas of a disk. This includes but is not limited to what is called 'unallocated' space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as 'slack' space in a file (the remnant area at the end of a file, in the last assigned disk cluster, that is unused by current file data, but once again may be a possible site for previously created and relevant evidence).
- Print out an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data. Further, provides an opinion of the system layout, the file structures discovered, any discovered data and authorship information, any attempts to hide, delete, protect, encrypt information, and anything else that has been discovered and appears to be relevant to the overall computer system examination.
- Provide expert consultation and/or testimony, as required.

This paper has provided a broad overview of collecting and protecting potential evidence in a suspected violation of administrative or legal requirements involving a computer. Formal training should be received by all participating on an incident response team and only those certified computer forensics technicians should perform evidence collection from the media itself.

**References:**


Anderson, Michael R. "Computer Evidence Processing, The Third Step – Preserve the Electronic Crime Scene." New Technologies, Inc. URL: http://www.forensics-intl.com/art7.html (March 1, 2001).

Holley, James. "Computer Forensics." SCInfo Security Magazine. September 2000. URL: http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html #secure (March 1, 2001).

Key Computer Service, Inc. A "Computer Forensics Training Center." URL: http://www.cftco.com/index.htm (March 1, 2001).

Key Computer Service, Inc. B. "Computer Forensics Training Center." URL: http://www.cftco.com/utilities.htm (March 1, 2001).


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Mendell, Ronald L. "Computer Crime Investigator's Toolkit: Part I." Earthweb. 13 February, 2001. URL: http://www.earthweb.com/dlink.resource-jhtml.72.1084.|repository|softwaredev|content|article|2001|02|08|SDSPcrime1|SDSPcrime1~xml.0.jhtml?cda=true (March 1, 2001).

New Technologies, Inc. A. "3 Day Computer Forensics Training Course." New Technologies, Inc. URL: http://www.forensics-intl.com/forensic.html (March 1, 2001).

New Technologies, Inc. B. "Corporate Evidence Processing Suite" New Technologies, Inc. URL: http://www.forensics-intl.com/suite2.html (March 1, 2001).

Robbins, Judd. "An Explanation of Computer Forensics." URL: http://crime.about.com/newsissues/crime/gi/dynamic/offsite.htm?site=http%3A%2F%2Fknock-knock.com%2Fforens01.htm (March 1, 2001).

U.S. Department of Energy. "Computer Forensics Laboratory First Responder's Manual – Version 1." 30 January 2001.

© SANS Institute 2000 - 2002, Author retains full rights.