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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

AN OVERVIEW OF DISK IMAGING TOOL IN COMPUTER FORENSICS

By Madihah Mohd. Saudi

(As part of the requirement of GSEC Examination)

Table of Contents

1. Objective.

2. Introduction.

3. Disk Imaging Definition.

4. Current Issues.

5. Recommended Solutions.

5.1 Never work on the original evidence.
5.2 Evidential integrity and security.
5.3 Presentation of evidence.
5.4 Rapidly increasing storage capacity.
5.5 Right job with the right tools.

6. Examples of Disk Imaging Tool.

7. Conclusion.

8. References.

© SANS Institute 2000 - 2005, Author retains full rights.

An overview of disk imaging tool in computer forensics

1. Objective

The objective of this paper is to educate users on disk imaging tool ; issues that arise in using disk imaging, recommended solutions to these issues and examples of disk imaging tool. Eventually the goal is to guide users to choose the right disk imaging tool in computer forensics.

2. Introduction

In solving computer crime cases, computer forensics is used to gather evidence, which will be analyzed and presented to a court of law to prove the illegal activity. It is important that when doing computer forensics no alteration, virus introduction, damages or data corruption occurs. In order to do a good analysis the first step is to do secure collection of computer evidence. Secure collection of evidence is important to guarantee the evidential integrity and security of information. The best approach for this matter is to use disk imaging tool. Choosing and using the right tool is very important in computer forensics investigation.

3. Disk Imaging Definition

A few forensics professionals and companies have illustrated disk imaging in various terms and definition. These are as quoted below:

Disk imaging as defined by Jim Bates, Technical Director of Computer Forensics Ltd, refers to:

"An image of the whole disk was copied. This was regardless of any software on the disk and the important point was that the complete content of the disk was copied including the location of the data. Disk imaging takes sector-by-sector copy usually for forensic purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered. It does not necessarily need the same geometry as the original as long as arrangements are made to simulate the geometry if it becomes necessary to boot into the acquired image."

Tech Assist, Inc. has defined disk imaging as following:

"Term given to creating physical sector copy of a disk and compressing this image in the form of a file. This image file can then be stored on dissimilar media for archiving or later restoration."

In simple words, disk imaging can be defined as to make a secure forensically sound copy to media that can retain the data for extended period.

Disk imaging is also one of the approaches for backup except that backup only copys the active file. In backup, ambient data will not be copied. This is an area where the most important source for the evidence could be found. Ambient data is a data stored in Windows swap file, unallocated space and file slack.

© SANS Institute 2000 - 2005 Author retains full rights.

The result of the analysis also can be duplicated to another media using disk imaging tool. A good imaging tool will not alter the original evidence. It can copy all the information from the drive and make the contents available for forensic analysis. Even ambient data that is inaccessible to the residental of operating system will be copied. From the definition of the disk imaging, many disk imaging tool has been invented. The first imaging tool was sold on 1991 by Computer Forensics Ltd where now sold under the trademark DIBS.

4. Current Issues

What is mainly concerns in disk imaging tool is whether can it produce a copy that is exactly same like the original? Users scare that if they use disk imaging tools, it might altered the layout of the copy and omits free and deleted space. In computer forensics, priority and emphasis are on accuracy and evidential integrity and security Doing analysis directly on original evidence might changes or alters the evidence. Due to that, it is essential to have a forensically sound of copy from original evidence.

Another issue is regarding internal verification. When done with imaging process, it is important to have one procedure or mechanism to determine that the evidence has not been altered or damaged. Internal verification is the only way to check the validity of the copy from the original drive.

In computer forensics, for cases that take years to be resolved, the evidence that has been imaged need to be stored into appropriate media. Appropriate media must be chosen to avoid any alteration or contamination of the evidence.

"During the last part of 1998, most computers on the market had hard drives of 6-8 gigabytes (GB). Very soon 13-27 GB hard drives will become the norm. By the end of 2000, we will be seeing 60-80 GB hard drives."
(As quoted from http://www.cybercrime.gov/freeh328.htm)

The problem arise from increasing of storage capacity is the need to do fast imaging especially when on-site or during emergency case. It needs a lot of time to do the imaging without using a correct tool. How does other products or technology help to do imaging process faster?

It can be difficult to explain the findings of computer evidence in a court especially to non-technical person. How can non-technical person understand findings of forensic analysis? The value of the evidence will ultimately depend on the way it is presented in court.

It is important to choose right tool in doing imaging process because we are interacting directly with the evidence. What criteria should be considered before buying or using disk imaging tool ? Accurate and dependable disk imaging tools are required in computer forensic investigation.

© SANS Institute 2000 - 2005 Author retains full rights.

5. Recommended solutions

Based on my analysis and observation, below are the recommended solutions regarding disk imaging tools issues.

5.1 Never work on the original evidence

Although it is easier to do analysis directly on original evidence it is not best practice in computer forensics. Evidence would be exposed to the risk of contamination. One of the cardinal rules in computer forensics is never work on the original evidence. Why? Because evidence is very fragile. Evidence must be handled properly and very easily destroyed. With only one strike on keyboard evidence could be accidentally destroyed or modified.

During computer forensic process, the risk of alterations, damage and virus introduction on evidence must be eliminated or minimized. In this situation, disk imaging tool can be used to make a bit-stream duplicate or forensically sound copy of an original disk. The best way to do analysis is on copy evidence. If something went wrong, everything can be done all over again. Every information that has been imaged must has no relationship or dependency on any hardware or software.

5.2 Evidential integrity and security

5.2.1 Internal Verification

For security consideration, internal verification should be made. It is used to verify the imaging procedures and to check if there are any changes during imaging process.

Disk imaging tool would generate log file. In log file it has all records of parameter of the process from disk geometry, interface health and packet checksums to case details such as date, time and analyst's name.

Checksums is one of the ways to check the validity of the copy from the original drive. It will apply an advanced mathematics algorithm to the information stored on a drive or file. The output of this mathematics will give a unique output. This means that we can compare between the original with the copy using the checksum. Same checksums between original and copy shows an exact copy has been produced. It is impossible and difficult to change the information on the drive without changing the checksums.

At present, some of the disk imaging tool use cyclical redundancy checksums (CRC) or MD5 checksums to ensure the integrity of the evidence.

DIBS has created one mechanism (internal verification) to ensure the copied data has not been altered and same as the original. It is known as Digital Integrity Verification and Authentication protocol (DIVA). Details about DIVA can be retrieve at http://www.forensic-

© SANS Institute 2000 - 2005 Author retains full rights.

computing.com/archives/diva.html

5.2.2. Evidence preservation

Electronic evidences might be altered or tampered without trace. Original copy should be placed in secure storage. Consider a situation when the victim claimed that if his computer is being taken, his business will suffer. As Jim Bates suggested (taken from Fundamentals of Computer Forensics) two forensically sound copies would help to solve this problem. Forensic investigation is done on one copy and another copy can be sealed in secure storage. When in doubt about evidence there is always another copy as reference.

The evidence that has been imaged, needs to be stored into appropriate media or reliable mass storage. Optical media can be use as the mass storage. It is reliable, fast, longer life span and reusable compared to CD-ROM or tape device that is slow and unreliable for accurate storage of evidential data. It also has limited life span. In five to ten years time this media may no be longer available for sale, degrade over time and evidence could at some point become no longer recoverable. In computer forensics some of the cases mat take more than two or three year to be solved. A secure storage space to store the original evidence is very important to avoid any contamination or alteration of data.

5.3 Presentation of evidence

It can be difficult to explain the findings of computer evidence in a court especially to non-technical person. The value of the evidence will ultimately depend on the way it is presented in a court. In court cases, even slightest doubt about the computer evidence makes the evidence invalid proof of any crime.

Result or report produce by the disk imaging tool must be easily understood either by non technical person or person from non computer literate background such as judges, jury and lawyers. Technical evidence should be presented in simple and precise way so that everyone in the court can understand the technical evidence presented.

5.4 Rapidly increasing storage capacity

The speed of imaging process varies based on number of factors such as physical state of the media and processor. In the past, to copy one computer to another, DISKCOPY command is used and it is very helpful due to small capacity storage. However presently where 60 GB is normal, disk imaging tools that could do fast imaging process is very important.

5.4.1 SmartSector Imaging

Many companies are introducing a new technology, which has the ability to make imaging process faster. PowerQuest Corporation has introduced a new technology called SmartSector imaging technology in their product, Drive Image Pro. File-by file imaging will read and copy each fragmented file. This will take longer time. Different from file-by-file technology,

© SANS Institute 2000 - 2005 Author retains full rights.

SmartSector imaging reads entire FAT for NTFS once, scan the disk and imaging only sector that have data allocated. This methodology helps speed up the imaging process. It eliminate any slow down and unaffected by file fragmentation on the hard disk.

5.5 Right job with the right tools

Nowadays many companies claim that they sell the best product for disk imaging purpose. A few suggestions or guidance in choosing the right tool are:

a. Disk imaging tool top level requirement (provided by National Institute of Standards and Technology) are:

- The tool shall make a bit-stream duplicate or an image of an original disk or partition on fixed or removable media.
- The tool shall not alter the original disk
- The tool shall be able to access both IDE and SCSI disks.
- The tool shall be able to verify the integrity of a disk image file
- The tool shall log I/O errors
- Provides good documentation

b. If necessary use the combination of different tools that has been developed independently which can help guarantee accuracy of the evidence.

c. Simple to use and quick to learn.

-This helps even non technical person to do imaging process without destroying the evidence especially in emergency case. User interactive that is well designed and interactive make the imaging process easier.

d. Provides fast imaging process.

-Technology such as SmartSector imaging helps to make imaging process faster. This is an additional requirement. When time is limited especially on-site and the need to conduct an initial analysis of drive contents, technology such as SmartSector is highly recommended.

e. Provides compression method, which helps to reduce the amount of space to store all the evidence files.

6. Examples of disk imaging tool

The SC InfoSecurity Magazine(September 2000) has provided a report on forensic tools evaluation. They found that Linux dd, SafeBack and SnapBack DatArrest as the best product to do fast and completely accurate copying of hard disks.

Below is a summary of disk imaging tool taken from a report on forensic tools evaluation from SC InfoSecurity Magazine, Pick of 2000,Computer Forensics and from my lab.

© SANS Institute 2000 - 2005 Author retains full rights.

Products / Features	Image file/internal verification	Imaged to appropriate media	Imaging SCSI / IDE drive	Copying sector -by sector / file-by-file
1.Safe Back Version 2.0	CRC checksum	Hard drive, tape, removable media	IDE drive	Sector- by- sector
2.SnapBack DatArrest Version 4.12	MD5 checksum	Hard drive, tape, removable media	SCSI drive	Sector- by- sector
Linux "dd" Version 7.0	MD5 checksum	Hard drive, tape, removable media	SCSI drive and IDE drive	Sector- by- sector and file-by-file
1.DIBS PERU (Portable Evidence Recovery Unit) 2. DIBS RAID (Rapid Action Imaging Device)	DIVA	Optical media	SCSI drive and IDE drive	Sector- by- sector

DIBS PERU : **www.dibsusa.com**
DIBS RAID : www.dibsusa.com
Linux "dd" : www.redhat.com
SafeBack :**www.forensics-intl.com**
SnapBack DatArrest : **www.cdp.com**

© SANS Institute 2000 - 2005 Author retains full rights.

6. Conclusion

Increasing number of computer crime means increasing demand for computer forensics services. In doing computer forensics investigation, choosing the right disk imaging tool is very important. There is no standard conformity of computer forensic imaging methodology or tool. This paper only provides guidance and suggestions regarding imaging tool. It should not be constructed as mandatory requirement.

One thing that we should bear in mind about disk imaging tool is, if the copy is not accurate as the original, then analysis may be flawed or incomplete, which may lead to unresolved cases. From time to time new technology and better imaging tools will be invented. It is really up to us to master appropriate tools so that it can be used effectively especially when emergency case happens. The next step after collection is the analysis and presentation of the evidence. Stick to the methodology and cardinal rules of computer forensics then analysis and presentation of the evidence so that the prime objective of computer forensics is met, which is to have the evidence accepted by the court of law.

7. References:

1.Holley, James. "Computer Forensics in the New Millennium." On-line SC InfoSecurity Magazine. September 1999. URL:http://www.scmagazine.com/scmagazine/1999_09/survey/survey.html

2. Holley,James. "Computer Forensics." On-line SC InfoSecurity Magazine. September 2000. URL: http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html

3. "Disk Imaging Tool Specification." Version 3.1.3. NIST(National Institute of Standards and Technology). 26 August 2001. URL: http://www.cftt.nist.gov/testdocs.html

4. "Ambient data defined." New Technologies Inc. 4 October 2000. URL : http://www.forensics-intl.com/def1.html

5. "Computer Forensics Definition." New Technologies Armor, Inc. 25 April 2001. URL: http ://www.forensics-intl.com/define.html

6. Heinonen,Daniel. "Computer Forensics-The Criminal Advantage." Version 0.1. 6 June 2001. URL: http://www.fineartforum.org/staff/daniel/compEvid01.pdf

7. "DIBS RAID-Rapid Action Imaging Device." DIBS USA, Inc. URL : http://www.dibsusa.com/

8. Bates,James. "DIVA Computer Evidence." International Journal of Forensic Computing. URL: http://www.forensic-computing.com/archives/diva.html

© SANS Institute 2000 - 2005 Author retains full rights.

9. "The History of Image Copying Technology." DIBS USA, Inc. URL : www.computer-forensics.com/history/welcome.html

10. "Byte Back Data Recovery and Computer Investigation Tool." Tech Assist, Inc. 2001. URL : http://www.toolsthatwork.com/byte.shtml#CLONE

11. "Drive Image Pro White Paper Exact Imaging for Fast Windows Deployment." PowerQuest Corporation. 2001. URL: http://www.powerquest.com/

12. "Products: SnapBack Live!: Product and Technology Comparison 1/15." Columbia Data Products, Inc. URL : http://www.snapback.com/snapback_live__-_product_and_t.html

13. "DIBS PERU (Portable Evidence Recovery Unit)." DIBS USA, Inc. URL : **http://www.dibsusa.com/products/peru.html**

14. Bates,Jim."Fundamentals of Computer Forensics." January / February 1997. URL : http://www.forensic-computing.com/archives/fundamentals.html

15. J.Freeh, Louis. March 28,2000. "Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime." URL : http://www.cybercrime.gov/freeh328.htm

16. Holley, James. "SC Info Security Magazine, Pick of 2000, Computer Forensics." 2000. URL: http://www.scmagazine.com/scmagazine/2000_12/testc/forensics.htm

17. Sheldon, Andrew. "Forensic Auditing, The role of Computer forensics in the corporate toolbox". URL: www.itsecurity.com/papers/p11.htm

© SANS Institute 2000 - 2005, Author retains full rights.