CHAMPLAIN COLLEGE

LCDI

The Senator Patrick Leahy Center for Digital Investigation

Tool Comparison

Team Lead: Megh Shah
Researched by: David Paradise

175 Lakeside Ave, Room 300A
Phone: 802/865-5744
Fax: 802/865-6446
http://www.lcdi.champlin.edu

Published Date

Disclaimer:

Contents

Introduction

This project will be benchmarking three digital forensic tools: EnCase v7.04.01, FTK, and Imager v3.1.1.8, as well as the SANS SIFT Workstation v2.14. The tools will be tested on a mid-tier desktop computer in order to create a base line of how time effective they are and how well the computer can run the tasks. The purpose of benchmarking these tools is to evaluate how they run on a mid-tier computer as compared to a desktop built specifically for forensic work. We used a Virtual Machine to show the amount of memory used during the test.

Background:

EnCase:

EnCase is a computer forensics tool designed by Guidance Software. It is an industry accepted tool used in numerous investigations by law enforcement and private companies. EnCase is used to acquire, analyze, and report on evidence. The program creates an .E01 image file when acquiring hard drives, which is the standard format for EnCase. When acquiring a hard drive, the investigator can either do a physical or logical acquisition. Physical acquisition is the process of imaging the entire drive and seeing all data on it, including items that have been deleted and hidden files. Logical acquisition is when the image is viewed in the same format as the computer file system. EnCase also verifies the drive image with the original drive using MD5 and SHA1 hash values and checksums.

FTK Imager:

FTK Imager is a commercial forensic imaging software distributed by AccessData. The program creates images from hard drives and other types of storage devices. FTK can create images in four different file formats: .E01, SMART, AFF, and Raw. These images can be one file or be split into segments that can be constructed later on. When the file is split into segments, the files can be moved and stored in several locations.

SANS SIFT Workstation:

The SANS Investigative Forensic Toolkit (SIFT) is a VMware image that has forensic tools pre-installed. It is compatible with image formats such as .E01, AFF, and Raw. The forensic toolkit has specific guidelines in place to secure the integrity of the evidence, such as formatting evidence as read only by attaching it to a particular type of device. SIFT supports Windows, Mac and Linux, along with each of their file systems. The toolkit includes many different pieces of software such as The Sleuth Kit, log2timeline, Foremost/Scalpel, Wireshark and Autopsy.

Purpose and Scope:

The intent of this project is to see how well these programs run on a mid-tier desktop and if we can force a crash of the program. A mid-tier desktop is a computer with average specifications, such as 8 gigs of RAM and a fairly modern processor. The information gathered during this project can be used by anyone in the digital forensics field when deciding whether to buy a high end, expensive desktop to run these programs as compared to their current machine.

For this project, we are using our own Fire II Hard Drive. Fire II is from a previous project in which a 250GB Drive was partitioned with the Windows, Mac, and Linux operating systems. Within those partitions, there is generated data that can be used for a multitude of tests, in this case using the 250GB as a baseline and searching the drive for common files.

Research Questions:

What is the average time for acquisition, verification, and imaging of a hard drive (250GB)?

Is there any way to force a crash of a specific program? If so, how?

Terminology:

Image – The copy of a hard drive that is compressed into one file.

Acquisition – The viewing of the image in a program such as Encase in order to gather data and information.

Data Compression – When the information from a hard drive or other form of storage is compressed together to take up less space on the computer.

Verification – The information on the image is checked with the original information on the hard drive to make sure nothing was altered.

Methodology

We started the project running a desktop with an Intel Core 2 Quad CPU and 8GB of RAM. The computer ran a 64-bit Windows 7 Enterprise edition operating system with Service Pack 1. The computer was given the final name of Lcdi-testing01.

After set-up was complete, we were given a 250GB internal hard drive containing Fire. Fire was the result a previous project where information was generated on a hard drive from Windows, Mac, and Linux. Our team utilizes this hard drive when working on other forensic research projects in order to set a base line. Using this hard drive, we can create an image to test all the programs using the same example.

Most computers will have programs that will lengthen the time it takes to image the drive, so we decided to use the Fire II drive to comply with time constraints.

Equipment Used

Lcdi-testing01 – Desktop computer used to run the tests.

Write Blocker – Used to make sure no information is written back to the drive and to keep the tests forensically secure. Connected to Lcdi-testing01 via mini USB to USB.

Fire Drive – The hard drive that will be imaged for testing purposes (250GB Seagate Barracuda 7200).

EnCase v7.04.01 – Acquisition and verification of the hard drive and keyword searching.

FTK Imager v3.1.1.8 – Acquisition and verification of the hard drive.

VMware Workstation 10 – Used to access SANS SIFT Workstation.

SANS SIFT Workstation – Acquisition and verification of the hard drive.

Programs to stress memory:

PRTK – A Decryption and Password Cracking Software by AccessData

PC Mark7 – A Windows PC Benchmarking tool

Prime 95 – Used for stress testing the system such as using RAM.

Table 1: Physical Equipment

Item	Identifier	Size/Specification
Test Computer	*LCDI-testing01*	*8GB RAM (4GB in VMWare), Intel Core 2 Quad !9450 @2.66GHz processor, 1TB storage.*
Test Disk	*FIRE-01*	*250GB Internal Storage Drive, Seagate Barracuda, 7200 RPM, Firmware 3.ADA, SATA*
Write Blocker	*Write Blocker 11*	*Forensic Ultra dock V.4*

Analysis

Our analysis consists of many tests that are specific to each program. For example, in Encase 7 we took an image of a drive and tested how long it would take to acquire the information, the verification time of the image, and a search for very common files to task the system. Next in FTK Imager, a simpler imaging program, we tried imaging the Fire II drive in two different ways to retrieve more information, such as changing compression levels. Finally with SANS SIFT Workstation, we used the bundled FTK Imager to see if it was faster or slower to image the drive rather than the standalone program, and tested the verification of the image using the same process.

Results

Throughout our testing, multiple applications were running in tandem with the forensic software in order to simulate a work environment and crash the programs.

The initial tool used was Encase Version 7.04.01. Our first test was a simple acquisition that took the information directly from the hard drive and displayed it in EnCase for us to view. We ran YouTube through Internet Explorer in the background to take up additional processing. The second test was the verification of the acquired data to make sure that the information pulled was not altered. We also ran a search for multiple file types while running as many programs as possible to force a crash. With the final test, a keyword search was performed looking for the common letters “ac.”

We then proceeded to use FTK Imager Version 3.1.1.3. We attempted to image the drive twice, once with only Internet Explorer running and another time with various programs on the background. Both tests were done using a write blocker with a USB connection when imaging. With the first test, we did not compress the image, whereas we utilized a level five compression with the second image.

The final tool used was SANS SIFT Workstation Version 2.14. SIFT is a forensic image that is run though the VMWare Workstation. While the computer is using 8GB of RAM, VMWare is only using 4GB of that RAM. Two tests were done with SIFT, one test that imaged and verified the drive and the one that solely verified the drive.

Below is a table of how much memory each program utilized during testing.

Application Memory Usage with Encase	Application Memory Usage with FTK Imager	Application Memory Usage with VMWare
First Test Internet explorer W/Youtube – 158,860 K EnCase – 37,384 K	First Test FTK – 25,896 K Internet Explorer – 72,202 K	First Test VMware - 46,892 K
None	Second Test Firefox – 221,000 K Flash Player – 133,424 K PCMark7 – 58,268 K	Second Test VMware – 39,028 K
Third Test EnCase – 825,968 K Prtk – 101,532 K Firefox – 84,140 K PCMark7 – 69,920 K Vmware – 29,608 K FTK – 22,484 K FTK Imager – 13,904 K Prime95 – 1,613,376 K	None	None

Conclusion

Most of the tests that we performed were done successfully, with only a few minor inconveniences. For EnCase V7.04.01, we recorded that it took 2 hours and 25 minutes to acquire data from the 250 Gigabyte hard drive and another hour and 14 minutes to verify that the data shown was indeed the same as on the hard drive. We also did a keyword search that took an hour and 19 minutes and only had minimal issues, such as the occasional slow down while going through the results. For FTK Imager V3.1.1.3, the imaging of the hard drive on level 0 compression and level 5 compression were both approximately 3 hours 18 minutes. In SANS SIFT Workstation V.2.14, the first test to image and verify the drive failed to complete, although this was not a crash. The second test of just the verification took roughly 9 hours to complete.

Our other intent through our testing was to see if we could force a crash by running a large number of programs simultaneously. During the first EnCase test, Internet Explorer was the only running program, with a YouTube video playing in the browser. This did not cause any problems. During the third test of the keyword search, several programs were running, including PRTK, Firefox, PC Mark7, VMware, FTK, FTK Imager and Prime 95. Although all of these programs were running, EnCase did not crash. While the second test was running on FTK Imager, we had Firefox running with YouTube and a flash game as well as PC Mark7. Firefox crashed about 40 minutes into the test, which was then restarted, and crashed again at 2 hours 20 minutes. Neither EnCase nor FTK Imager crashed during testing.

Further Work

There is room for potential additional research in the future. Initially, we were supposed to be working with 16 and 32 Gigabyte memory systems, but as neither the system nor the tools crashed in an 8 Gigabyte environment, we did not see the value in going further at this time. If our team was to explore this field further, we could test average times for imaging, acquisition, and verification on computers with different amounts of memory. These tests would be to view the difference, if any, in the output of the system process, and the amount of time taken in imaging and using different tools simultaneously. We could also work on processing E01s from over the network using similar tools to report any changes in the process.

References

SANS Investigative Forensics Toolkit. (2013, May 12). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/SANS_Investigative_Forensics_Toolkit

Forensic Toolkit. (2013, November 22). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Forensic_Toolkit

Prime95. (2013, November 17). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Prime95

EnCase. (2013, November 24). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/EnCase