Forensics System Benchmark Proposal

Senator Patrick Leahy Center
for Digital Investigation

By: Frederick Morey & Neil Torpey
In Accordance With: Michael Wilkinson
2/11/12

Contents

1 Introduction

1.1 Research Statement

In the field of high performance computers there are millions of benchmarks and comparisons of different computers and parts but none of these benchmarks focus on digital forensics in comparison to hardware; we aim to change that.

1.2 Field of Research

Computer and Digital Forensics is a new field that is expanding rapidly with new technology and new methods. The rapid expansion of this field has made it difficult for companies to make hardware specifically for digital forensics. Most professional digital forensics computers or servers are extremely expensive. On the other hand, high powered home desktops, as of late, have been dropping in price but the machines themselves have been increasing in power. This is our main question; can a high powered desktop have the same amount of power and speed that the professionally built forensics machines offer.

1.3 Benchmark Overview

This benchmark is being developed to determine if it is better to buy a fully customized professional forensic computer at high dollar or if it is possible to buy a high powered desktop computer from a retail store for much cheaper and get the same or better performance. The test is also designed to find at what speed each forensic program runs on each system and which system runs the programs the fastest. Overall there are four steps to this benchmark. The first step is to gather basic information on the computer such as its hardware and operating system. The second step is a stability test. The programs used in digital forensics can be very CPU intensive for long periods of time; to test this; we will run a program and stress the CPU to 100% for a long period of time. The third step is basic benchmarking using PCMark7. Doing this allows us to compare computers to millions of others worldwide. The final and most important step is the forensic testing. We will run three different commonly used digital forensics programs that are used at the LCDI.

2 Overarching methodology

2.1 Stability testing

The reasoning behind stability testing is simple. We want to see if the system is able to run at high stress for long periods of time and still remain stable and not shutdown. This also tests to see if the cooling provided is enough to keep the CPU within operating temperatures. The results for this test are a simple pass/fail. If the system passed then the CPU temperature never hit the TjMax of the CPU (the maximum temperature a CPU can handle) and the system never crashed during the 6 hour run. The

two programs that will be used to test the system for stability are called Prime95 and CPU-Z.

2.2 Basic Benchmarking

There is one basic computer benchmark program that has been chosen that can be compared to computers all around the world. PCMark7 is an excellent program that tests all aspects of a computer. It runs many tests from 3D game previews to test the system but also image manipulation, video decoding, and many other aspects of the computer.

2.3 Forensics Testing

The software used for this section is Forensics Tool Kit (FTK), EnCase 6.19, & WinHex 16.1 SR-6. These three programs that are commonly used at the LCDI are the basis for our digital forensics evidence collecting and investigations. For FTK and EnCase there are two tests that will be conducted while for WinHex there is only one.

The first step when a drive is entered for examination is to make a forensic image of the drive using either EnCase or FTK. This is the first data point that will be recorded. The programs report the time it takes to image a drive in Days: Hours: Minutes: Seconds. The time will be recorded in only seconds and then when calculating the overall time it will be converted to minutes only. The drive used in this section is a 250GB 7200RPM Seagate SATA hard drive that will be imaged using a write blocker connected to the fastest interface the computer has access to.

The second aspect of this section is the time it takes to search the drive. Three searches will be performed with all three programs. Each of these searches will fulfill a different commonly seen result of forensics searches. The first of these three searches is the overload search. For this benchmark we will use each of the three programs to search a Windows 7 forensics image for the term “ew”. This will show the time it takes to do an overload search which is where there are more search hits than a normal search would produce. The second search is a normal search. For this benchmark we are using the search term “Fred” for our second search. This search does result in some hits but not nearly as many as our overload search. The final search is the failed search. The failed search is a search that returns no results. For this benchmark we are using the search term “ew5566965621398d” as our search term.

3 Data Collection

List of steps that make up the forensic benchmark:

3.1 Basic data collection:

Using free programs such as GPU-Z, CPU-Z and information included with the computer to record specifications such as the hardware and operating system the computer has. CPU-Z is a freeware application that provides extensive information on your computer's central processing unit. The software provides your processor's name and manufacturer, its core stepping and process, processor package, processor current core voltage, internal and external clocks, clock multiplier, partial overclock detection and more. GPU-Z is also a freeware program that displays the same type of information as CPU-Z but instead for the graphics card. (Graphic 3-1)

3.2 Stability Testing

Using a freeware program called Prime95 the system's processor will be stressed to 100% for 12 to 15 hours. Prime95 stresses the computer's processor to 100% by running a Lucas-Lehmer primality test which tests numbers to find Mersenne numbers. The maximum temperature the CPU reaches will be recorded using a free program called Core Temp which simply reads the core temperature from the CPU and reports it on the screen. (Graphic 3-2)

3.3 Basic Benchmarking

PCMark7 is a freeware program that is made to test CPU, graphics, HDD, and RAM performance. After running its multiple tests the program then presents a numeric rating or score of the computer. The overall score along with some specific scores of interest are recorded on the data sheet. (Graphic 3-3)

3.4 Forensic Testing

The main focus of the forensic testing is hard drives. Firstly a Seagate Barracuda hard drive that has been described above has been made the dedicated benchmark drive that will be imaged onto the test machine using Forensic Took Kit (FTK) and EnCase. With FTK there are two extra steps that the program takes that EnCase does not take when imaging a drive. These steps are counted on the data sheet as well. There is a predetermined .E01 file that was created and will be copied to each test system then searched using each program for three set quires outlined above. One search will produce an average number of hits, one will produce no hits, and the final will produce an overload of search hits. The times for each search and the overall time to image the drive are all recorded on the record sheet. (Graphic 3-4)

4 Analysis

After all the data is collected and placed in their respective places on the data sheet the overall score is automatically calculated by Excel. Excel automatically adds up the time it takes for each forensics program to run in a total time section for each program. This time is expressed in minutes. It then adds a total forensics time taken section and finally the overall score section. The overall score section is calculated by averaging the overall forensics times. (Graphics 3-4 and 4-0)

5 Graphics

5.1 Graphic 3-1

Computer Brand:	Custom Built		Dell
Computer Model:	Custom Built		XPS
CPU Name:	Intel Core i7 950		Intel Core 2 Quad Q9450
Number of Cores:	4 Physical 8 Logical		4 Physical 4 Logical
Core Name (architecture):	Bloomfeild		Yorkfeild
Core Speed (In MHz):	3207		2000
RAM amount (in Mb):	8192		6144
Ram Speed (in MHz):	534.6		400
Motherboard Name:	Asus Sabertooth X58		Dell 0PP150
Number of HDD's:	2		2
HDD 1 Brand and Model:	Western Digital Black		Seagate Barracuda
HDD 1 Size (in Gb):	931.51		232.83
HDD 2 Brand and Model:	Western Digital Black		Western Digital Black
HDD 2 Size (in Gb):	931.51		931.51
HDD 3 Brand and Model:	N/A		N/A
HDD 3 Size (in Gb):	N/A		N/A
HDD 4 Brand and Model:	N/A		N/A
HDD 4 Size (in Gb):	N/A		N/A
HDD 5 Brand and Model:	N/A		N/A
HDD 5 Size (in Gb):	N/A		N/A
Optical Drive Type:	DVD-RW		DVD-RW
Number of Video Cards:	1		2
Number of identical cards:	1		2
Card 1 Make:	nVidia		nVidia
Card 1 Model:	GeForce GTX 460 SE		9800 GT
Card 2 Make:	N/A		nVidia
Card 2 Model:	N/A		9800 GT
Operating System:	Windows 7 sp1		Windows 7 SP1

Two example system's data recorded on the data sheet

5.2 Graphic 3-2

Prime 95 6hr test pass (Y/N):	Yes	1	Yes
CPU TjMax (in °C)	100		90
Max CPU Temp in Prime95 (in °C):	82		59

Data collected from stress testing both computers listed in 3-1

5.3 Graphic 3-3

PCMark Overall Score:	3127		2002
Video Downscaling (in kB/s):	5732.43		1796.83
Image Manipulation (in Mpx/s):	9.34		6.5
Data Decrypting (in MB/S):	68.05		56.03
System Storage Windows Defender (in MB/S):	2.02		1.29

Scores recorded from PCMark7

5.4 Graphic 3-4

FTK HDD Image Time (sec):	12235.00		11334.00	
FTK Time to Verify HDD Image (sec):	2362.00		3806.00	
FTK HDD Indexing Time (sec) :	4342.00		4676.00	
FTK Failed Search Time (ew5566965621398d)(sec):	475.00		1207.00	
FTK Passing Search Time (Fred)(sec):	475.00		1273.00	
FTK Overload Search Time (ew)(sec):	9604.00		5134.00	
		FTK Total Time (min)		FTK Total Time (min)
		491.55		457.17
EnCase HDD Image Time (sec):	8940.00		8580.00	
EnCase Failed Search Time (ew5566965621398d) (sec):	494.00		1671.00	
EnCase Passing Search Time (Fred) (sec):	646.00		1634.00	
EnCase Overload Search Time (ew) (sec):	668.00		2109.00	
		Encase Total Time (min)		Encase Total Time (min)
		179.13		233.23
WinHex Failed Search Time (ew5566965621398d) (sec):	842.00		750.00	
WinHex Passing Search Time (Fred) (sec):	864.00		854.00	
WinHex Overload Search Time (ew) (sec):	870.00		1053.00	
		WinHex Total Time (min)		WinHex Total Time (min)
		42.93		44.28

Data collected from forensic testing along with total times for each program

5.5 Graphic 4-0

Total Fornesics Time (min)		Total Fornesics Time (min)
713.62		734.68
Overall Forensics Average		Overall Forensics Average
237.87		244.89

Overall Scores that Excel automatically calculates on the spreadsheet