THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 3 | Number 3 Article 3

2008

An Evaluation of Windows-Based Computer Forensics Application Software Running on a Macintosh

Gregory H. Carlton
California State Polytechnic University

An Evaluation of Windows-Based Computer Forensics Application Software Running on a Macintosh

Gregory H. Carlton
California State Polytechnic University
ghcarlton@csupomona.edu

ABSTRACT

The two most common computer forensics applications perform exclusively on Microsoft Windows Operating Systems, yet contemporary computer forensics examinations frequently encounter one or more of the three most common operating system environments, namely Windows, OS-X, or some form of UNIX or Linux. Additionally, government and private computer forensics laboratories frequently encounter budget constraints that limit their access to computer hardware. Currently, Macintosh computer systems are marketed with the ability to accommodate these three common operating system environments, including Windows XP in native and virtual environments. We performed a series of experiments to measure the functionality and performance of the two most commonly used Windows-based computer forensics applications on a Macintosh running Windows XP in native mode and in two virtual environments relative to a similarly configured Dell personal computer. The research results are directly beneficial to practitioners, and the process illustrates affective pedagogy whereby students were engaged in applied research.

Keywords: Computer Forensics, Macintosh, EnCase, FTK, Digital Forensics, Workstation Validation, Forensic Application Software

1. INTRODUCTION

Computer forensics is a dynamic and rapidly growing field, and as with any field experiencing changing conditions, practitioners are faced with a number of challenges to keep up with the current requirements (Volonino et al. 2007). Clearly, one factor concerning computer forensics regards capabilities to utilize contemporary technology while maintaining the ability to examine the variety of operating environments that exist in today's market (Nelson et al. 2008). Another factor facing computer forensics examiners concerns limited budget constraints with regards to equipping their forensic laboratories. Additionally, computer forensics examiners must ensure that their equipment function properly, as they must attest to the authenticity of the data analyzed and validate their findings (Volonino et al. 2007).

Given the conflicting goals of increasing the flexibility and performance of

computer equipment while reducing costs, one can logically deduce the advantage gained from the ability to utilize contemporary computer forensic application software from a single, hardware platform that can function properly in the variety of operating environments common today. Of course, prior to gaining this advantage of a single workstation capable of running contemporary forensics application software and operating in multiple operating system environments, this hardware must be tested to validate its functionality (Volonino et al. 2007).

This study conducted a series of experiments to determine the extent to which a Macintosh computer system performs while running the most popular computer forensics application software. These experiments were designed to measure the functionality and performance of a variety of tasks by comparing a personal computer running Windows XP natively to a Macintosh (Mac) running Windows XP in native mode and in two virtual environments.

The results of this study are beneficial to practitioners concerned with equipping their labs, as the experiment results include empirical functionality and performance measures. Additionally, this study illustrates successful research conducted within the "learn by doing" approach at a polytechnic university.

2. CONTEMPORARY FORENSICS COMPUTING ENVIRONMENTS

Current computer forensics examinations involve a wide variety of components, consisting of computer hardware, operating system environments, and computer forensics application software. Although there are many variations of hardware involved in digital forensics, including devices such as, personal data assistants (PDA) and cell phones, this study focuses on computer forensics concerning microcomputer workstations.

Each of these components is discussed below, first with a discussion on operating system environments in Section 2.1, then by a discussion on microcomputer hardware in Section 2.2, and then followed by a discussion of the most popular computer forensics application software in Section 2.3.

2.1 Operating system environments

There are three major operating system environments currently in common use on microcomputers (Nelson et al. 2008). The most widely used operating system environment in use is Microsoft's Windows, and the two versions of it currently available are Windows XP and Windows Vista. Although Vista was introduced as the replacement for XP, the market has not fully embraced this newer version of Windows, with compatibility issues listed among reasons cited for the market resistance (Griffith 2008). For example, the two most common Windows-based computer forensics application software products discussed in Section 2.3 were not initially supported on Vista; however, this limitation has recently been resolved.

Following the large market share enjoyed by Windows is OS-X, which runs exclusively on Apple's Macintosh computer systems. OS-X is touted by Apple as having a user-friendly, graphical user interface (GUI) that is actually a shell that runs on a UNIX kernel. The current version of OS-X supports a Boot Camp utility that provides the ability to run multiple operating systems in native mode, including the XP and Vista versions of Windows and Linux. Additionally, applications that run under OS-X allow Windows XP to run in a virtual environment within the protected shell of OS-X.

Behind the two leading commercial, proprietary operating systems for microcomputers are various implementations of open source Linux operating systems (Griffith 2008). Although the market shares of these operating systems are relatively small, computer forensics examiners must be prepared to recognize and analyze data from any of these popular operating systems.

2.2 Micro-computing hardware

Virtually all of the microcomputers on the market today are based on Intel, or compatible chipsets, as Apple migrated the Mac to an Intel chip in 2006 ("Apple to Use Inter Microprocessors Beginning in 2006" 2005). The Macintosh computers are exclusively manufactured by Apple, and although they contain Intel chips that are compatible with those found in IBM-compatible personal computers (PC), Macs' processors include proprietary code which affectively prohibits OS-X from running on non-Apple hardware.

In addition to OS-X requiring this proprietary code within Mac processors, the end user license agreement for OS-X presents another barrier prohibiting individuals from legally running OS-X on clone hardware. While some websites post information concerning hacks to enable OS-X to perform on clone microcomputers, forensic computer examiners that disregard ethical and legal barriers are not likely to be well received as expert witnesses in legal matters (Pash 2007).

Given the similarity between the hardware of PCs and Macs and the ability of Macs to run the Windows operating system while the proprietary code within Mac chips prohibit PCs from running OS-X, it appears that the Macintosh has an advantage in flexibility; however, measurable experiments are necessary to empirically determine the extent of functionality and performance of Macs relative to PCs. The following section presents the most popular computer forensic application software, and testing this software provides us with an interesting and relevant set of measurements to compare the functionality and performance between PC and Mac platforms.

2.3 Forensic application software

There are numerous computer forensics application software products currently on the market designed to run on individual microcomputer workstations. Each of these products is targeted toward a single operating environment, such as

Windows, OS-X, or some flavor or UNIX/Linux. Within this study, we assumed that each application will function properly when run in its native environment; otherwise, market forces will naturally eliminate the product. Our objective within this study was to evaluate the most popular computer forensics application software running on a workstation whose operating environment was not its native environment.

According to a recent study, the two most widely used computer forensics application software products are EnCase by Guidance Software and Forensics Toolkit (FTK) by AccessData (Carlton 2007). Additionally, both EnCase and FTK run exclusively on the Windows family of operating systems. There are other computer forensics application software products in use on Windows operating systems, as well as, applications and tools for UNIX/Linux and Macintosh's OS-X operating systems; however, their overall market share is relatively small compared to EnCase and FTK.

In this study, we were not concerned with evaluating the applications designed for OS-X since OS-X will not run on non-Apple hardware, as discussed in Section 2.2 above. Similarly, we were not concerned with testing Linux applications and tools, as their usage within the computer forensics market is minimal and it appears less problematic for Linux to run properly on PCs and Macs than does Windows. This decision will be expanded upon within the discussion on limitations of this study in section 5.5.

In summarizing our observations regarding operating system environments, microcomputer workstations, and computer forensics application software, we recognize that the most widely used computer forensics application software runs exclusively under the Windows family of operating systems. Also, the Macintosh is marketed touting the capability of running OS-X, Windows, and UNIX/Linux operating systems, whereas, due to proprietary code within Macintosh processors, OS-X will not perform on non-Apple hardware. Given these observations, we were interested in studying the functionality and performance of the most widely used computer forensics application software designed for Windows performing on a Macintosh computer system; therefore we limited this study to an evaluation of EnCase and FTK, and we conducted a series of experiments, as defined in Section 5 of this report.

3. FORENSICS LABORATORY BUDGET CONSTRAINTS

Regardless of whether a forensics laboratory is a private or government facility, financial resources are required to equip the lab with the computer hardware and software necessary to perform their forensic analyses. Although some forensics examiners may prefer to specialize in selected areas, such as cases involving a particular operating system, forensic examiners must be aware that any single, physical storage medium could contain data from multiple operating systems (Nelson et al. 2008). Therefore, it is beneficial for forensics examiners to equip their labs with the equipment necessary to

function in the variety of environments they are likely to encounter, such as the three operating environments discussed in Section 2.1.

Recognizing that it is beneficial for a forensics laboratory to have computer equipment capable of functioning in the major operating environments and understanding that procuring computer hardware requires limited financial resources, it is straightforward to extend this logic to conclude that it will be beneficial to have a forensics workstation in the laboratory that is capable of running the three major operating environments.

4. EXPERIMENTS

To determine whether the two most common computer forensics software applications function properly when run on a Macintosh computer system, we conducted a number of experiments in multiple hardware and operating environments. The following sections discuss the hardware we used to conduct these experiments, the different operating environments, and the specific application software tests we performed within each operating environment. After describing our tests, we present the results of our experiments and discuss limitations of this study.

4.1 Hardware

Our primary goal of this study is to evaluate the functionality and performance of a Macintosh computer system running the two most common forensics software applications. We selected two similarly configured microcomputer workstations to use in our comparison, with one being a PC and the other a Mac. Both computers had the similar central processing units (CPU), random access memory (RAM), bus speeds, and disk storage capacity. The specifications of these computers are presented in Table 1 Computer hardware. The PC represents a control unit from which we can measure the performance of the Mac.

Table 1. Computer hardware

	Dell Notebook	Mac Mini
CPU	Intel Core Duo T2300 1.66 GHz	Intel Core Duo T2300 1.66 GHz
Bus	667 MHz	667 MHz
RAM	DDR2 2GB (2x1GB) 667MHz	DDR2 2GB (2x1GB) 667MHz
Chipset	945GM rev 03	945GT rev 03
HDD	Hitachi SATA 150 GB, NCQ support, 8MB cache	Seagate SATA 150 GB, NCQ support, 8MB cache

As shown in Table 1 Computer hardware, the specifications of the Dell Notebook PC and the Mac Mini were virtually identical, with the exception of the hard disk drive brands. We were aware that faster, more powerful CPU

models were offered by both hardware suppliers; however, the similarities between the two systems we selected were sufficient to perform tests from which we can establish a meaningful comparison.

Table 2. SiSoftware Sandra benchmark summary

	Test	Dell	Mac
CPU	Dhrystone ALU	9916MIPS	10145MIPS
	Whetstone iSSE3	8105MFLOPS	8289MFLOPS
HDD	Index	26.69 MB/s	27.76 MB/s
	Random Access	19 ms	15 ms
RAM	Int Buff'd iSSE2	3.50 GB/s	3.48 GB/s
	Float Buff'd iSSE2	3.51 GB/s	3.47 GB/s

To determine the extent of performance similarity between the Dell PC and the Mac prior to conducting our forensics application software experiments, we conducted a series of performance benchmarks on both computer systems, and the results are summarized in Table 2 SiSoftware Sandra benchmark summary and Table 3 Geekbench benchmark summary.

The Intel Macintosh benchmarks were performed running Windows XP using the Boot Camp facility, as it represents a native-mode instance of the operating system, thus providing a more direct comparison between the two computer systems. Additionally, higher values indicated in Tables 2 and 3 represent better performance, except for the hard disk random access times.

Table 3. Geekbench benchmark summary

Test	Dell	Mac
Geekbench score	1781	1828
Integer	2039	2150
Floating Point	1822	1854
Memory	1367	1346
Stream	1571	1579

4.2 Testing environments

Using the hardware described in the preceding section, we established four testing environments from which we measured the functionality and performance of our experiments. The first testing environment, representing our experimental control, utilized the Dell PC, and we configured it with Windows XP Professional, 32bit version, Service Pack 3. The second testing environment utilized the Mac configured with its Boot Camp utility to run Windows XP Professional, 32 bit version, Service Pack 3 in native-mode, and the other two environments ran Windows XP in virtual-mode on the Mac using VMware Fusion and Parallels Desktop 3.0 for Mac respectively. Prior to testing, we disabled the screen savers and power saving modes in each environment.

In establishing the three environments on the Mac, we partitioned a 20 GB

volume for the native-mode Windows XP operating system using Boot Camp. Additionally, we established 20 GB fixed images for each of the two virtual implementations of Windows. This allotment of 20GB for the each of the three Windows environments left only 3GB of free space on the HFS+ Mac volume, and this proved to be somewhat of a disadvantage for the Mac.

To remove residual data that might bias the test results, we performed a defragmentation process on the Dell PC and the Mac prior to conducting our experiments. This process illustrated one example of the disadvantage the Mac encountered as a result of the limited disk free space, as the defragmentation process failed to complete due to insufficient disk space. This problem could have been resolved by either installing a higher capacity disk drive, or installing only one of the three test environments concurrently.

It also must be noted that both virtual environments were configured to utilize only 1 GB of RAM. There were also two notable differences between the virtual environments. VMware's Fusion virtualized two cores within the CPU, whereas, Parallels Desktop virtualized only a singe core. Additionally, we performed our tests using VMware Fusion's patch of Windows XP, Service Pack 3, and at the time we performed these experiments, Parallels had not released a similar patch.

Overall, these four environments were configured in a manner that was balanced to the best of our ability given the time and equipment available to us. The following section identifies the tests we conducted using each of these four environments, and we found the results to be very interesting, as shown in Section 4.4.

4.3 Application tests

Our primary goal was to test the functionality and performance of the two most common computer forensics application software products, both of which function on Windows operating systems only, when run on a Macintosh computer system. To test this functionality, we identified sets of tasks regarding forensic application software installation, forensic data acquisition, forensic analysis, and forensic data wiping, and we measured the functionality and performance of each task performed using EnCase and FTK in each of the four test environments described in Section 4.2.

The first set of tests involved installing EnCase Forensic, version 5.05j on each of the four test environments. This test included copying the EnCase version 5.01 CD to the HDD, representing 167 MB of data. Then the version 5.05j updated was copied to the HDD, representing 6.6 MB. Next, HASP HL Device Driver 5.12 was installed in each environment, followed by the version 5.01 installation, and finally installing the EnCase version 5.05j update.

The second set of tests involved performing forensic data acquisition tasks in each environment with EnCase. Two storages were provided for these tests,

with one being a Maxtor 15.3 GB IDE disk drive and a 1 GB thumb drive. Two Tableau write blocking devices, one IDE and the other USB, were connected to the test environments *via* USB 2.0 connectors for the data acquisitions.

The third set of tests involved forensic analysis using EnCase to perform four tasks. The first task was a keyword search for "Info2," "NTFS," "Amazon," and "Hotmail." The second task was a grep (i.e., general regular expression) keyword search for the hexadecimal representation of a JPEG file header (e.g., FF D8 FF E0), and the third task was a grep expression for the data mask of a phone number. The final analysis task was an EnScript (i.e., a proprietary scripting language within EnCase) to identify unique e-mail addresses.

The fourth set of tests concerned forensics data wiping, and these tests consisted of using EnCase to wipe the Maxtor 15.3 GB hard disk and the 1 GB thumb drive. This set of tasks represents the final test using the EnCase application software.

Just as the first set of four tasks identified above utilized testing EnCase functions in each of the four test environments, the final set of three tasks utilize FTK performing the same functions identified in the first three sets of tasks above in each of the four test environments. The data wiping tasks were not duplicated using FTK, as that function was not available.

The FTK installation procedure involved first copying the data from the installation CD to the HDD, consisting of 435 MB. Next, dongle drivers version 1.5 were installed followed by CodeMeter Runtime 3.3. Next, FTK 1.71 was installed, then FTK Imager 2.5.3, FTK Registry Viewer 1.5.1, Known File Filter (KFF) Library, Password Recovery Toolkit (PRTK) 6.3.3, and finally License manager 2.2.2 was installed.

After FTK was installed in each of the four test environments, the forensics data acquisition tasks were performed using FTK Imager to acquire and verify the 15.3 GB HDD and the 1 GB thumb drive, and an additional test was performed within FTK to index the image.

Additionally, there were differences in the data analysis tests using FTK. As a result of indexing the images, the keyword search test was measured based on the number of search hits only, as the index allowed FTK to display the keyword search hits immediately. Also, FTK does not have the ability to run EnScripts; therefore, that test was not performed. However, the searches based on the regular expressions for the hexadecimal representation of a JPEG header and a phone number were performed and measured in terms of search results and the time to perform the tests in each of the four test environments.

The results of each test are presented in the following section.

4.4 The results of the experiments

First, we can summarize quickly that the functionality tests for every task in each environment passed, as every function tested provided the correct results with no errors or unusual conditions in any environment. This included the proper installation of the applications, correct MD5 hash values for disk images, identical vales of search hit results, and the completion of disk wiping with no errors.

The installation of EnCase onto the test environments included the task of first copying the EnCase CD to the HDD prior to the application installation. This task was performed as a result of our observation that the Mac Mini required an excessive amount of time to access the CD drive. By isolating the CD access from the process, we are able to better understand the performance issues across the test environments. This installation test functioned properly in all four environments with no errors or unusual circumstances in any of the environments; however, the performance results were interesting and somewhat surprising, as shown in Table 4. EnCase installation summary.

Table 4. EnCase installation summary

	Time format: mm:ss.0			
Installation Preparation	Dell	Boot Camp	WMware Fusion	Parallels Desktop
Copy CD to HDD	01:32.5	01:34.0	03:25.0	13:13.5
Copy update to HDD	00:00.5	00.00.5	00.04.0	00:01.5
Application Installation				
HASP Driver	00:06.0	00:15.5	00:14.0	00:04.5
EnCase 5.01	00:10.5	00:08.5	00:16.0	00:07.5
EnCase 5.05	00:05.0	00:05.0	00:10.5	00:05.0
Total Time				
Excluding copying CD	00:21.5	00:29.0	00:40.5	00:17.0
Including copying CD	01:54.5	02:03.5	04:09.5	13:32.0

It would not have surprised us if the two native-mode environments, the Dell and the Mac using Boot Camp, performed faster than the two virtual environments, VMware Fusion and Parallels. However, excluding the CD copying times, the Parallels environment performed the task the fastest, yet including the CD copying times, the Parallels environment performed the slowest.

The second set of tests performed using EnCase in each environment consisted of performing forensic data acquisitions of a 15.3 GB IDE hard disk and a 1 GB thumb drive. Performing the tasks in each environment resulted in the

correct MD5 hash values, and the performance measures are listed in Table 5 EnCase data acquisition.

Table 5. EnCase data acquisition

	Time format: hh:mm:ss			
Acquisition	Dell	Boot Camp	VmWare Fusion	Parallels Desktop
HDD	0:37:46	0:34:09	1:19:00	2:06:00
Thumb D	0:18:44	0:03:09	0:05:11	0:08:33
Thumb D (repeat)	0:18:45			
Dell Re-acquistion	Right Top	Right Bottom	Rear Left	Rear Right
Thumb D	0:03:05	0:03:05	0:03:05	0:03:05

The results of the EnCase forensic data acquisition of the 1 GB thumb drive provided some initial unexpected values, so we repeated our tests to confirm our results. Initially, the acquisition times of the thumb drive ranged from just over 3 minutes to about 8 ½ minutes on the three Mac environments; however it took 18 minutes and 44 seconds to complete on the Dell with the thumb drive plugged into the left USB port on the rear of the unit. The test was immediately repeated with a result of 18 minutes and 45 seconds. After reflecting on the results, we suspected that the operating system was not treating the port as a USB 2.0 device. We also recognized that the Dell computer had four USB ports, with two ports located on the right side of the unit and two ports located on the rear of the unit. On a later date, we conducted additional tests on each of the four USB ports, and the operating system recognized the thumb drive as a USB 2.0 device on each port yielding identical data acquisition times of 3 minutes and 5 seconds for each of the four ports, as shown in Table 5 EnCase data acquisition.

Table 6. EnCase data analysis

	Time format: hh:mm:ss			
Keyword Search	Dell	Boot Camp	VMware Fusion	Parallels Desktop
Keyword Search	0:13:52	0:11:53	0:12:32	0:15:36
GREP JPEG	0:11:45	0:11:41	0:13:33	0:18:02
Phone #	0:28:18	0:27:43	0:29:05	0:33:56
EnScript	1:09:44	1:11:25	1:13:32	1:21:34
Total	2:03:39	2:02:42	2:08:42	2:29:08

Summarizing the results of the EnCase data acquisition, it is clear that the two native-mode environments (i.e., Dell and Mac using Boot Camp) performed significantly better than the two virtual environments in the data acquisition tasks. This difference seems reasonable, as the native-mode environments directly access the hardware through their device drivers, whereas, the virtual environments will have to communicate through the hosting OS-X operating system before reaching the physical devices. It is also noteworthy to mention that the Mac running Windows XP in native-mode performed approximately 10% faster than the Dell in the hard disk acquisition task.

Similarly, as one might expect based on the preceding observation concerning hardware devices, the results of the data analysis tasks were much closer over all four environments, as they did not involve any hardware devices. From a functionality perspective, the data analysis tasks yielded identical results across all four environments, and the performance values are summarized in Table 6 EnCase data analysis.

Again, it is interesting that the Mac, running Windows XP in native-mode under Boot Camp, performed faster overall than the Dell, completing three of the four tasks faster. The Dell performed the EnScript task faster, but the Mac still performed faster when considering the total time to perform the four tasks. Neither virtual environment performed faster than the native-mode environments in any of the EnCase data analysis tasks.

The final test using EnCase involved wiping the 15.3 GB hard disk drive and the 1 GB thumb drive. Once again, the two native-mode environments significantly performed faster than the virtual environments, as was expected due to the physical devices involved. The results of these tasks are provided in Table 7 EnCase disk wiping.

Table 7. EnCase disk wiping

	Time format: hh:mm:ss			
Device	Dell	Boot Camp	WMware Fusion	Parallels Desktop
HDD	0:22:17	0:23:43	1:31:00	3:35:00
Thumb	0:08:32	0:08:42	0:13:11	0:20:05

The tests involving installing FTK were performed in a similar manner as the EnCase installation, as we first copied the data from the CD to the HDD to provide a richer set of installation measurements. There are more steps to the FTK installation process, thus the overall time to install FTK was greater than the EnCase installation. Table 8 FTK installation lists the results from the FTK installation process in each of the four test environments.

Table 8. FTK installation

	Time format: hh:mm:ss			
Installation Preparation	Dell	Boot Camp	WMware Fusion	Parallels Desktop
Copy CD to HDD	0:03:14	0:08:18	0:08:50	0:17:20
Application Installation				
Dongle drivers	0:00:26	0:00:24	0:00:31	0:00.31
CodeMeter	0:00:10	0:00:11	0:00:37	0:00:32
FTK 1.71	0:00:17	0:00:16	0:00:39	0:00:38
Imager 1.5.1	0:00:37	0:00:32	0:00:57	0:00:51
Reg Viewer	0:01:40	0:01:30	0:02:33	0:03:01
KFF Library	0:00.14	0:00:16	0:01:10	0:00:43
PRTK 6.3.3	0:00:33	0:00:34	0:01:57	0:02:07
License Mgr.	0:00:04	0:00:02	0:00:05	0:00:05
Total Time				
Excluding copying CD	0:04:01	0:03:45	0:08:29	0:08:28
Including copying CD	0:07:15	0:12:03	0:17:19	0:25:48

The FTK data acquisition tests yielded the identical MD5 hash values as did the EnCase data acquisition tests in all four environments. The FTK data acquisition performance results are shown in Table 9 FTK data acquisition. Similar to the results of the EnCase data acquisition, the two native-mode instances of Windows XP performed significantly better than the two virtual environments, as physical, secondary storage devices are utilized extensively in the data acquisition process.

Table 9. FTK data acquisition.

	Time format: hh:mm:ss			
Acquisition Verification	Dell	Boot Camp	VMware Fusion	Parallels Desktop
HDD	0:23:09	0:24:39	1:52:41	3:33:13
Thumb D	0:03:40	0:03:45	0:11:00	0:13:26

Following the FTK data acquisition tasks, we indexed both images, the 15.3 GB HDD and the 1 GB thumb drive, within FTK simultaneously. The image process completed successfully within each environment, and the index completion times are: 44 minutes and 4 seconds for the Dell, 45 minutes and 57 seconds for the Mac using Boot Camp, 1 hour, 1 minute and 46 seconds for the Mac using WMware Fusion, and 1 hour and 40 seconds for the Mac using Parallels Desktop. Again, we saw the native-mode environments performing better than the virtual environments. The two native-mode environments

completed the tasks within two minutes of each other with the Dell performing faster. Interestingly, in the virtual environments, the two environments completed the test within one minute and six seconds of each other with Parallels Desktop completing the task faster.

The data analysis tasks within FTK yielded an identical number of search hits within each test environment for each of the tests. The time to complete the regular expression searches for the hexadecimal representation of a JPEG file header and phone numbers are presented in Table 10 FTK search results.

Table 10. FTK search results

	Time format: hh:mm:ss			
Live Search	Dell	Boot Camp	VMware Fusion	Parallels Desktop
JPEG	0:07:38	0:08:34	0:09:30	0:08:52
Phone #	0:04:31	0:04:21	0:05:01	0:06:43

Although the results of the regular expression searches within FTK are much closer in terms of total time, this is largely to the small amount of time necessary to perform the task, as the percentages of time relative to the Dell are similar to other tests, with the two native-mode environments performing faster than the virtual environments. The total time to perform the two tests took 12% longer in the VMware Fusion environment and 21% longer in the Parallels Desktop environment relative to the Boot Camp environment, and 19% and 28% longer than the Dell respectively. However, the Boot Camp environment performed better than the Dell in one of the two searches while performing worse in the other search test. The Boot Camp environment required 12% longer to complete the search for JPEG file headers while performing the phone number search 4% faster than the Dell environment.

4.5 Limitations

This study conducted a series of experiments to measure the functionality and performance of the two most common computer forensics application software products, both of which function exclusively on the Windows family of operating systems, when run on a Macintosh computer system, and while the experiments were completed successfully, there are a number of limitations that must be recognized. First, while our study utilized similarly configured Dell and Macintosh computers in the experiments, a more extensive study using a variety of similarly configured sets of computers with varying CPU models should provide a better understanding from which results may be generalized.

A limitation that should be noted concerns a potential flaw in our research methods. While we often performed the experiments multiple times and

reported the average values, we were not consistent in the number of times in which we performed each experiment. On instances where we observed an operational flaw due to human error, we discarded those results and performed the experiment again.

Our study was also restricted by the relatively small amount of disk space available to the different Mac environments. This disk storage capacity concern might have been reduced had we conducted these tests independently, with only one environment configured on the Mac and then subsequently conducting the tests in another Mac environment after removing the prior environment. Another approach would be to simply utilize a larger capacity disk storage device on the Mac.

Our study tested EnCase Forensics version 5.05j and FTK version 1.71. While each of these releases represents the latest release available within their respective versions, both EnCase and FTK are currently available in newer versions. As of this time, EnCase offers version 6 and FTK offers version 2 of their software; however, these versions were not available to us for testing.

We also used relatively small capacity storage devices, by today's standards, in performing our tests. For example, the 15.3 GB hard disk we tested is small compared to 250 GB, 500 GB or 1 TB disks forensics examiners are likely to encounter in contemporary investigations. However, the smaller capacity disk drives used in this test is not thought to reduce the significance of our findings. We encourage interested researchers to perform these experiments on larger capacity disk drives, newer releases of the application software, and higher performance CPUs to improve the knowledge base in this field.

5. PEDAGOGY

This study was developed by a faculty member in the Computer Information Systems Department at Cal Poly Pomona, and the experiments were conducted by a group of six, senior undergraduate students who were completing a ten-week, senior project. In conjunction with Cal Poly Pomona's polytechnic pedagogy using our "learn by doing" approach, the students were highly engaged in conducting this research. Five of the six students have completed coursework in computer forensics; therefore, they were familiar with EnCase and FTK, and multiple members of the group have participated in intercollegiate computer forensics competitions.

The test environments and each of the tasks were specified by the faculty member, and the students conducted each experiment. Frequently, tasks were repeated to ensure reliability in the results, and average scores were reported in these instances. Also, the storage media used in the experiments were provided by the faculty member, as well as the write-blocking equipment, application software and dongles.

The Dell and the Mac computer systems used for the experiments were

provided by the students, and at least four of the students were experienced, Mac users. All of the students became engaged in the process of understanding differences between the operating system environments, and they conducted independent research to understand the internal workings of each environment.

The students interacted with the faculty member frequently during the ten week period. This interaction included ad-hoc and regularly scheduled meetings and e-mail correspondence. The ad-hoc meetings and e-mail messages consisted of students providing test results immediately upon completion of each test and questions concerning procedures or response formats. The regularly scheduled meetings occurred approximately every two weeks, and they consisted of formal project management meetings where the students provided PowerPoint presentations and written reports documenting their progress, findings and concerns, and they received additional instructions during these meetings. Upon the completion of the project, the students submitted a 242 page report to the faculty member that documented each task and included screen-shots and logs of their activities. Additionally, the raw data were made available to the faculty member for electronic storage.

The project was enthusiastically received by the students, and as other teams of senior project students learned of this project, several students approached the faculty member expressing envious comments toward those working on this study. Additionally, three of the members of the student team were offered computer forensics jobs by big-four consulting firms and another member of the team was offered employment at a government organization regarding computer forensics.

Overall, this study was a success when measured on two outcomes. First, as shown in the following section, this study reached a conclusion that should prove useful to practitioners in the field of computer forensics. Secondly, this study was a success when measured on the educational experience it provided to students in the field on computer forensics, as it provided an enjoyable project from which students demonstrated project management skills and teamwork while developing a richer understanding of computer forensics tools, operating system environments, and research methods.

Although this study does not claim to introduce new pedagogical methods, as student involvement in hands-on experiments have been successfully conducted for years, it does provide confirmation of these methods, and perhaps most importantly, this offers a valuable forum for validating digital forensics techniques.

6. CONCLUSION

The primary goals of this study were to test the functionality and performance of the two most common computer forensics application software products, both of which function on Windows operating systems only, when run on a

Macintosh computer system. All of the functions performed correctly in all four test environments; therefore, we concluded that the Mac is an acceptable tool for running EnCase and FTK application software. Concerning performance issues, the two environments running Windows XP in native-mode consistently performed better than did the virtual environments of Windows XP. Faster performance results between the Dell and the Mac using Boot Camp were divided, with the Dell performing faster on some tasks and the Mac performing faster on others.

Although the two virtual environments did sacrifice some performance, they also provided some benefits. These benefits include allowing users to switch between environments without rebooting and operating in a protected, virtual environment.

Along with our observations concerning the acceptable performance of the most popular, Windows-based computer forensics applications running on a Mac and recognizing the benefits of running multiple operating system environments in a computer forensics laboratory, we conclude that a Macintosh is a viable computer system for general usage by computer forensics examiners, and it is not necessary to utilize it only for specialized cases involving data stored on Macs.

We also think it will be beneficial for other researchers and software developers to continue to investigate new techniques for improving the virtual operating environments available on computer systems, including the Macintosh. Computer forensics examiners will benefit from having powerful, flexible workstations available from which they can conduct their analyses, and this technology offers promising opportunities.

AUTHOR BIOGRAPHY

Gregory H. Carlton is an Assistant Professor in the Computer Information Systems Department at California State Polytechnic University (i.e., Cal Poly Pomona). He earned his MBA and Ph.D. from the University of Hawaii. In addition to teaching courses in computer forensics at the undergraduate and graduate levels and conducting research in this field, he is also a practitioner with an active caseload. He is an EnCase Certified Examiner (EnCE), a member of the High Technology Crime Investigation Association (HTCIA), and he has provided expert testimony. More information is available at his website at http://www.csupomona.edu/~ghcarlton.

REFERENCES

"Apple to Use Intel Microprocessors Beginning in 2006" (2005), Apple, Worldwide Developer Conference, June 6, 2005, From http://www.apple.com/pr/library/2005/jun/06intel.html on 6/13/2008.

Carlton, G.H. (2007), A Protocol for the Forensic Data Acquisition of Personal Computer Workstations, ProQuest, Ann Arbor, Michigan, UMI 3251043.

Griffith, E. (2008), "OS Wars: The Battle for Your Desktop", PC Magazine, Vol. 27, No. 4, March 1, 2008.

Nelson, B., Phillips, A., Enfinger, F., and Stewart, C. (2008), Guide to Computer Forensics and Investigations, 3rd Ed., Thomson, Boston.

Pash, A. (2007), "Build a Hackintosh Mac for Under $800", Lifehacker, 11/13/2007, http://lifehacker.com/software/hack-attack/build-a-hackintosh-mac-for-under-800-321913.php, accessed 6/13/2008.

Volonino, L., Anzaldua, R., and Godwin, J. (2007), Computer Forensics Principles and Practices, Prentice Hall, Upper Saddle River, New Jersey.