NLECTC NIJ

Criminal Justice
Electronic Crime Technology
Center of Excellence

Evaluation of Mac Marshal™ Version 2.0.3

EVALUATION REPORT

September 2011

NIJ Electronic Crime Technology Center of Excellence
550 Marshall St., Suite B
Phillipsburg, NJ 08865
www.ECTCoE.org

NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O'Leary, CFCE, DFCP
Russell Yawn, CFCE
Laurie Ann O'Leary
Donald Stewart, CFCE
Randy Becker, CFCE
Mark Davis, Ph.D.
Victor Fay-Wolfe, Ph.D.
Chester Hosmer
Michael Terminelli

Table of Contents

Introduction **1**

Overview **3**

Product Information 3

Product Description 3

Special Features 4

Target Customers 4

Law Enforcement Applications 4

Evaluation and Testing of Mac Marshal™ **5**

Test Bed Configuration 5

Mac PowerBook G4 5

MacBook Air 5

Download and Installation of Mac Marshal 5

Test 1 – Running Mac Marshal Field Edition on OS X 10.4 6

Test 2 – Mac Marshal Forensic Edition 10

Test 3 – Performing Live Analysis of OS X 10.6.7 13

Conclusion **17**

Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ Research, Development, Testing & Evaluation (RDT&E) process.

The NIJ RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. The rigorous process has five phases:

- **Phase I: Determine technology needs principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropiate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit http://www,justnet.org).
- **Phase II: Develop technology program plans to address those needs. A multiyear research program is created to address the needs identified in Phase I.** One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary, and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions**. Appropriate solicitations are developed. Grantees are selected through an open, competitive, peer-reviewed process. Grants are awarded and the grantee and the NIJ program manager then work collaboratively to develop the solutions.
- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. After adoption, the solution's impact on practice is evaluated. During the testing and evaluation process, performance standards and guides are developed as appropriate to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides.
- **Phase V: Build capacity and conduct outreach.** To ensure that the new tool or technology benefits practitioners, NIJ publishes guides and standards and provides technology assistance to second adopters.[1]

The High-Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making.

The NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process. This process addresses the high-priority needs for criminal justice technology to protect the public, ensure officer safety, confirm the guilty and protect the innocent, improve the efficiency of justice and enable informed decision-making.

[1] *National Institute of Justice High-Priority Criminal Justice Technology Needs,* March 2009, NCJ 225375.

Overview

Apple Mac OS X is quickly becoming a popular operating system. Historically, the majority of digital forensic examinations performed on computers by state and local law enforcement were Windows based. With the increasing popularity of Apple-branded desktops and laptops, law enforcement is facing a new challenge of processing these machines in search of digital evidence. Many of the popular forensic examination suites can perform some functions on an imaged OS X hard drive; however, user-specific data to the Apple Mac OS X is often difficult to interpret. Furthermore, performing a live analysis on a Apple Mac OS X is limited in support. Mac Marshal™, is designed by Cyber Security Technologies to address these needs. From the Cyber Security Technologies website[2]:

> "The increasing popularity of Apple Macintosh hardware, particularly using Intel x86 compatible processors, provides new challenges for forensic investigators. The complexity of these investigations is compounded by the ability of modern Macs to run multiple operating systems, such as Windows or Linux, utilizing dual-boot via Apple's Boot Camp software or in a virtual machine such as Parallels or VMware Fusion. Mac Marshal automates the identification of the operating environment of the Mac OS X-based system, and automates the extraction of usage information left by the operating system and Mac OS X applications. Mac Marshal's unique implementation of the capability to use the Spotlight search functionality is invaluable in speeding searches for files based upon sophisticated content or metadata criteria."

Product Information

Mac Marshal was developed by ATC-NY, as subsidiary of Architecture Technology Corporation that specializes in research and product development in computer security and digital forensics.

Mac Marshal has been designed as two separate products, Mac Marshal Forensics Edition, and Mac Marshal Field Edition. Mac Marshal forensic and field editions are designed to be identical, with the exception of requiring an install for the Forensic Edition and the portability of the Field Edition.

Forensic Edition is an installed program on an Apple Mac OS X computer, and Field Edition is run from a USB Stick. Forensic Edition is free to state and local law enforcement. Mac Marshal Field Edition is $199 USD to U.S. law enforcement personnel. For commercial uses of either product, they can be purchased through Cyber Security Technologies.

Product Description

The following is the product description taken from the two products' datasheets[3]:

> "Mac Marshal Forensic Edition automates the analysis of Mac OS X disk images. It scans the image, automatically detects Mac, Windows, and other operating systems and virtual machine images, then provides the investigator with analysis tools that extract Mac OS X-specific forensic evidence, including data left by Apple's Mail, Safari, and iChat applications and many more."

[2]http://www.cyberstc.com/products_mac.asp
[3]http://www.macmarshal.com/index.php/support

"Mac Marshal Field Edition automates the analysis of live Macintosh systems and Mac OS X disk images. It scans the file system and extracts Mac OS X-specific forensic evidence, including data left by Apple's Mail, Safari, and iChat applications and many more. When run live on the suspect machine, Mac Marshal gathers valuable volatile information that would normally be lost during the seizure process. Mac Marshal Forensic Edition 2.0 is a software tool that runs on a forensic investigator's Mac workstation to automatically analyze a Mac disk image."

"Mac Marshal follows forensic best practices and maintains a detailed log file of all activities it performs. It produces reports in RTF, PDF, and HTML formats, and runs on Mac OS X-based analysis machines."

Special Features

The following is a list of features of Mac Marshal Forensic Edition taken from the product's website:

- Analyzes Mac OS X and dual-boot disk and partition images in multiple formats.
- Analyzes configuration and log files from common OS X applications, such as Mail, Safari, iChat and Address Book.
- Performs rapid searches using Spotlight file metadata.
- Gathers comprehensive machine usage information.
- Lists detailed information about every iPod and iPhone that has been connected to the machine.
- Detects VMWare, VirtualBox & Parallels virtual machines.
- Detects and analyzes FileVault-encrypted user directories.
- Supports dd, EnCase, FTK, AFF and Apple disk images.
- Maintains an audit trail and generates detailed reports, System Configuration and Swap File/Hibernation File acquisition tools. (This lets the examiner see things like past WiFi access points the computer was associated with, whether there's a Time Machine backup drive, etc.).
- Image thumbnail browser for previewing large numbers of image files.

In addition, the following features are included in Mac Marshal Field Edition:

- **Physical Memory acquisition:** Gathers a snapshot of RAM before you shut the computer down.
- **Live State acquisition tools:** Allows you to examine the volatile state of a live machine, such as running processes, current screenshot and list of active network connections, before seizing it.

Target Customers

Mac Marshal Forensics Edition is free (Field Edition is $199) to U.S. law enforcement by arrangements with NIJ. Mac Marshal is also available for purchase to the private sector and law enforcement from outside of the United States.

Mac Marshal is designed to allow a digital forensics investigator to acquire evidence from any Mac OS X platform. Any investigator that may be interested in examining Mac platforms may find this tool useful.

Law Enforcement Applications

Mac Marshal is designed to assist state and local law enforcement with the analysis of Mac OS computers.

Evaluation and Testing of Mac Marshal™

Test Bed Configuration

Mac PowerBook G4

This PowerBook is maintained at the Tulsa Digital Forensics Center. Its operating system is Mac OS X version 10.4.11. It contains a 1.5 GHz Power PC G4 processor and 1.25 GB DDR SDRAM for memory.

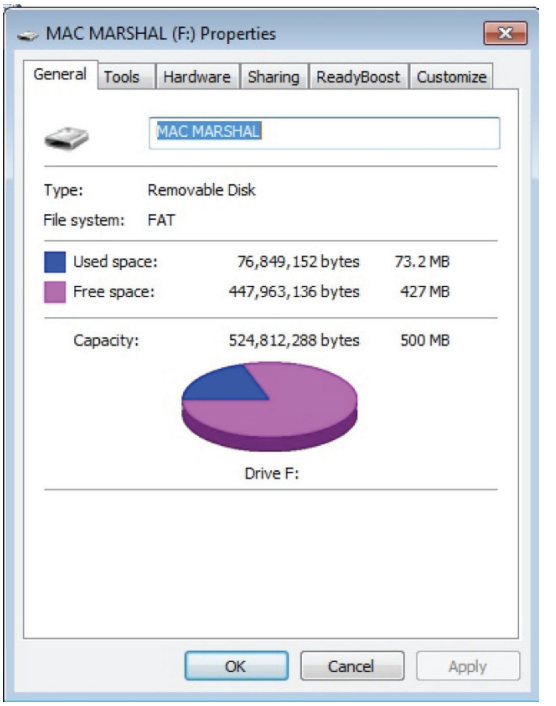
MacBook Air

The MacBook Air is personally owned by a member of the review team. Its operating system is Mac OS X version 10.6.7. It contains a 2.13 GHz Intel Core Duo Processor, and 4GB of memory and a 256GB solid state hard drive.

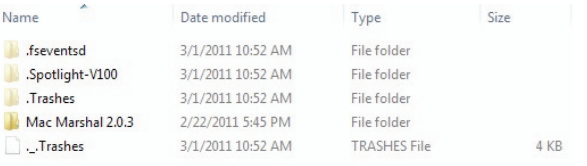
Download and Installation of Mac Marshal

ATC-NY was contacted to evaluate Mac Marshal. After some e-mail exchange, ATC-NY shipped Mac Marshal Field Edition to the reviewer. ATC-NY also provided an e-mail containing a link to download Mac Marshal Forensic Edition and a software key. During this process it was discovered that Mac Marshal Forensic Edition could only be installed on one machine per license. The Field Edition would allow for review on multiple platforms with only one license.

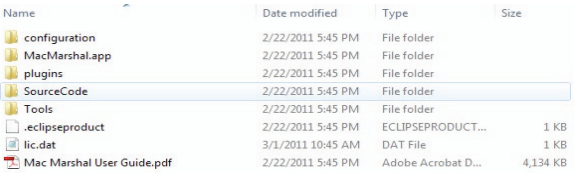
On receiving the Mac Marshal Field Edition USB Drive from ATC-NY, staff plugged it into a Windows 7 workstation to review the contents of the drive. Using the right-click-> properties in Windows on the USB Drive reported that the drive was ~500MB.



The USB Drive (automatically mounted by Windows as “F:” on this system) was selected and the folder contents were displayed.



The “Mac Marshal 2.0.3” folder was selected and the contents displayed. (The folders “.fseventsd,” “.Spotlight-V100” and “.Trashes” are system folders added by Mac OS X and were not reviewed.)



The "Mac Marshal folder" contained the "Mac Marshal User Guide.pdf." This guide was printed and reviewed. The guide contains a well-written detailed description of the use of Mac Marshal Forensic Edition and Mac Marshal Field Edition, including step-by-step instructions and screenshots. The guide was easy to read and follow.

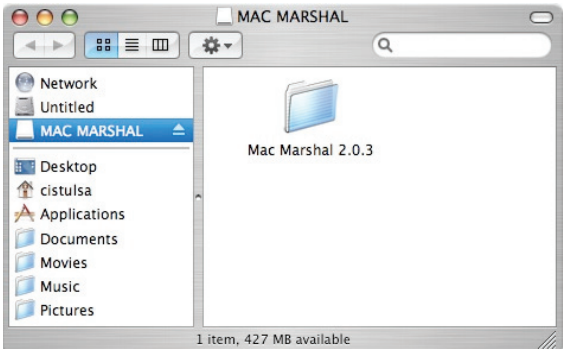
Based on information from the guide, it is obvious that Mac Marshal was designed to run in Mac OS X. The tests were performed on those operating systems.

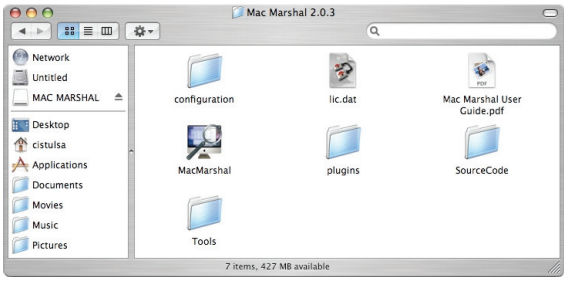
Test 1 – Running Mac Marshal Field Edition on OS X 10.4

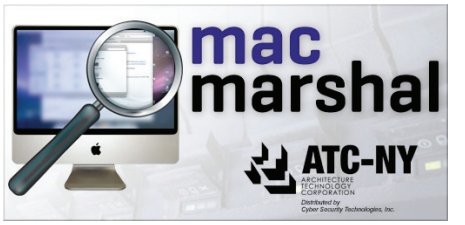
This test is designed to test Mac Marshal Field Edition on a Powerbook running OS X 10.4. No additional configuration was performed on this laptop. This test is designed to be the equivalent of running Mac Marshal Field Edition on an OS X machine with no prior knowledge of the contents of the system.

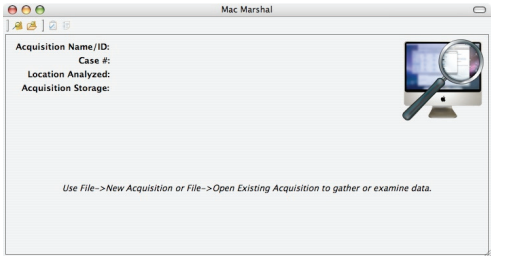
The following steps were performed:

1. The Powerbook OS X 10.4 test machine was plugged into a wall outlet.
2. The Powerbook was then powered on by pressing the power button. The Macbook booted into the operating system and displayed the desktop. The test machine reported that it could not connect to any of its known wireless networks and asked if the user would like to join another wireless network in range. "No" was selected.
3. The Mac Marshal Field Edition USB drive was inserted in the USB port of the Powerbook. A "MAC MARSHAL" icon appeared on the desktop. Double-clicking this icon opened a file browser with a folder labeled "Mac Marshal 2.0.3." Double-clicking this folder revealed another file listing, including the Mac Marshal executable file. Double-clicking this icon loaded Mac Marshal on the Powerbook.

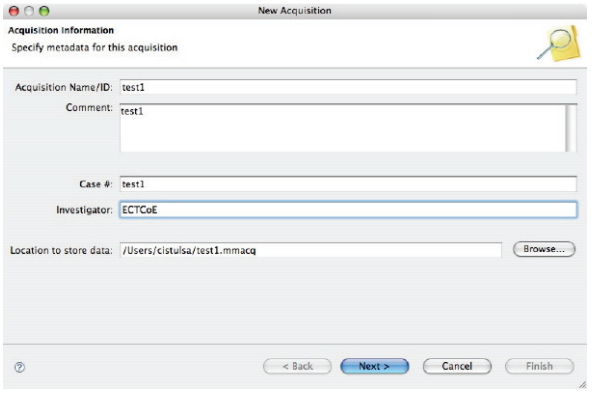




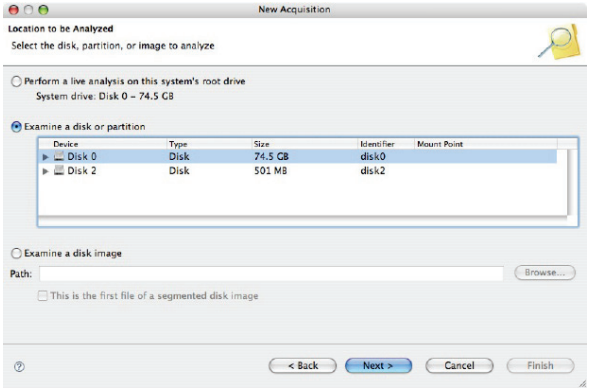




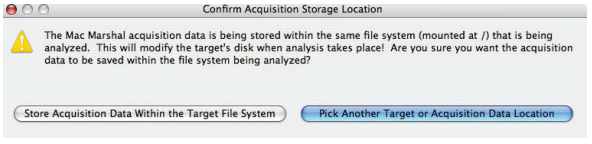
4. Selected "File->New Acquisition."
5. Completed the following form as detailed in the screen shot below.



6. Mac Marshal then scanned for local drives and displayed the screen below. “Examine a disk of partition was selected” and “Disk 0” highlighted.

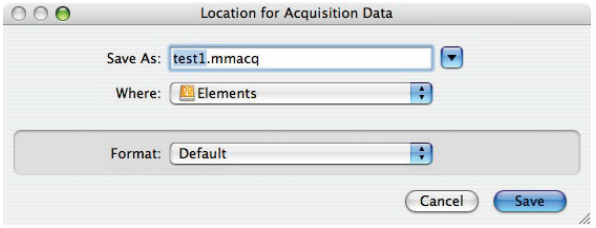


7. After clicking next, Mac Marshal gave this warning screening indicating that the storage of the case was on the same drive that was being examined. “Pick Another Target or Acquisition Data Location” was selected. Mac Marshal was closed.

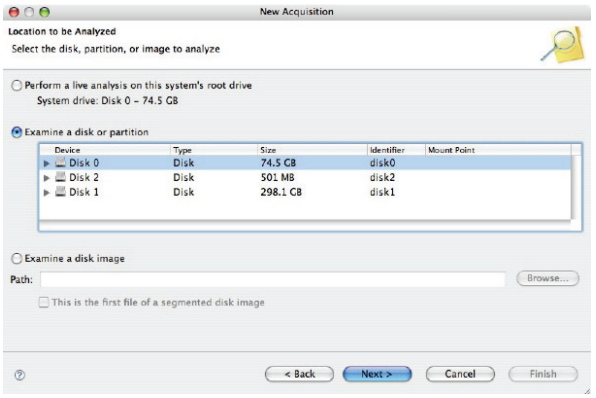


8. At this point, another external USB Hard Drive (named “Elements”) was attached to the Power-book. Once the operating system mounted the external USB hard drive, an icon appeared on the desktop.

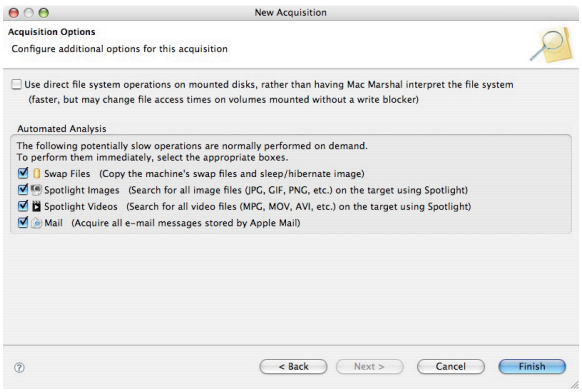
9. Once the USB Hard Drive was mounted, Mac Marshal was loaded again. This time on the “File Acquisition” screen, the browse button was “clicked” and a location on the External USB Hard Drive was selected.



10. Once again, “Hard Drive 0” was selected and “Next” was clicked.

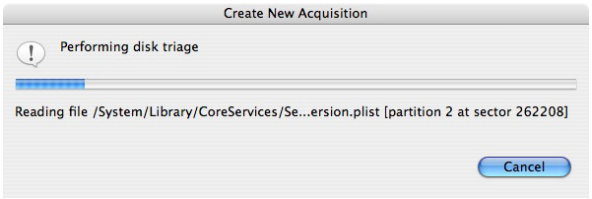


11. The next screen allowed the user to select what type of "Automated Analysis" was to be performed on the system. Given the warning that Mac Marshal may change file access times if using the "Direct File system Operations on mounted disk," this was left unchecked. The rest of the items were checked and "Finish" was clicked.



12. Mac Marshal then required the user to "Authenticate" by typing the user's password.

13. Mac Marshal then brought up a status screen of "Create New Acquisition" with a status bar to indicate its progress. This process was started at 3:41 p.m. and completed at 3:47 p.m.. (~6 minutes).



14. The next screen was displayed, and the "Mac OS X [Live]" disk was selected, and "Disk Triage" was clicked.

15. At this point, many categories of data could be selected to be examined including:

- Triage Info.
- Swap Files.
- System Config.
- Recent Items.
- Address Book.
- Preview.
- Mail.
- QuickTime Player.
- iPod/iPhone.
- iChat.
- Safari.

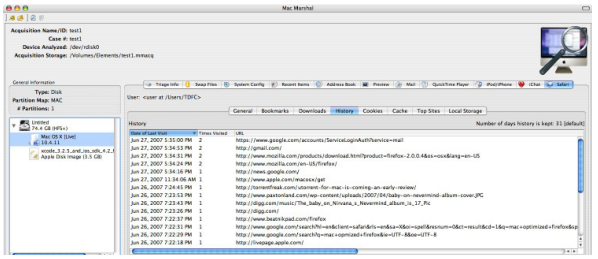
On clicking on "Safari," several categories were displayed, titled as follows:

- General.

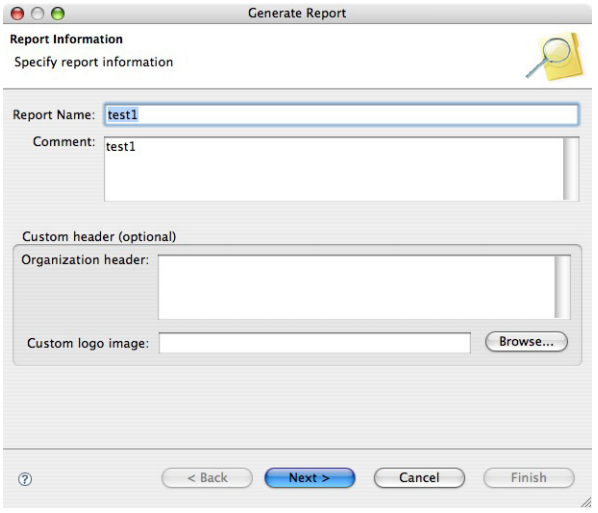
- Bookmarks.
- Downloads.
- History.
- Cookies.
- Cache.
- Top Sites.
- Local Storage.

This screen was very wide and went off the screen. To select all of the categories, the window had to be dragged sideways.

16. Since no data was intentionally placed on this computer for this review, many of these categories did not display any information. However, some information about the prior use of this laptop, most notably Safari information including bookmarks, cache and cookies, was captured.

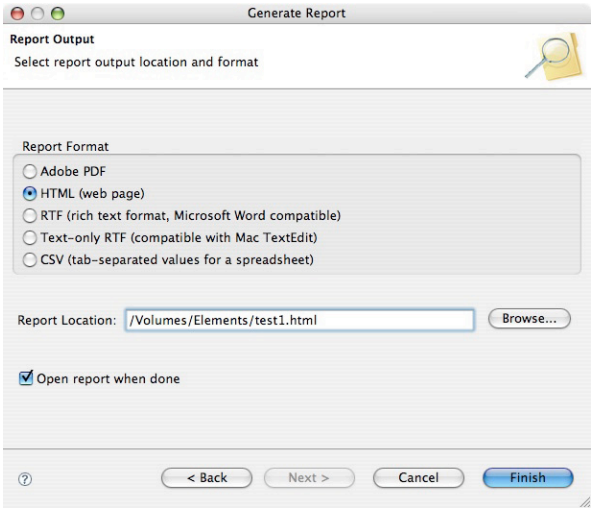


17. At this point the “Create Report” icon was clicked. The following screen was displayed. No additional information was entered and “Next” was clicked.

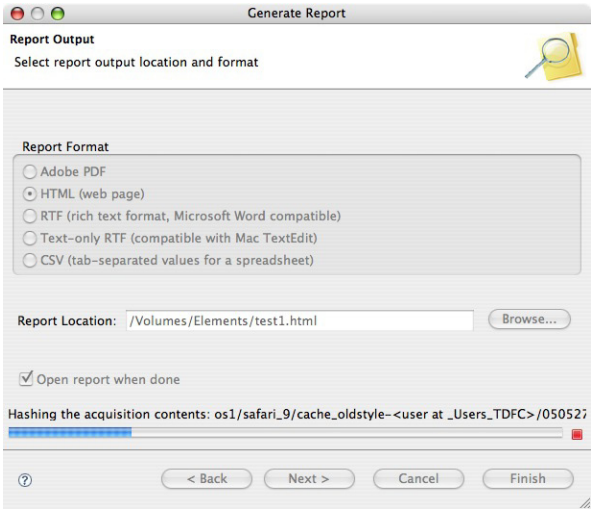


18. The report generator then allowed the user to select what to include in the report. “xcode_3.2.5_and_ios_sdk_4.2_final.dmg” were unchecked. (This is the iOS development platform and is a known good file, and quite large, so it was not to be included in the report). “Include audit log” was checked and “Next was clicked.”

19. The report generator then asked what format to use to create the report. “HTML (web page)” was selected, and the location was selected to be on the external USB hard drive. “Finish” was clicked.

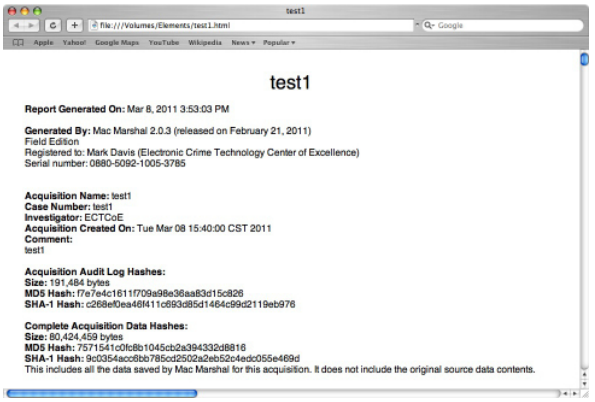


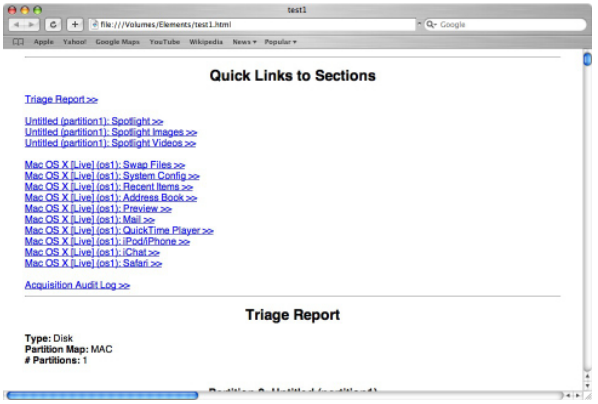
20. This process started another status bar that indicated many of the report items were being hashed.



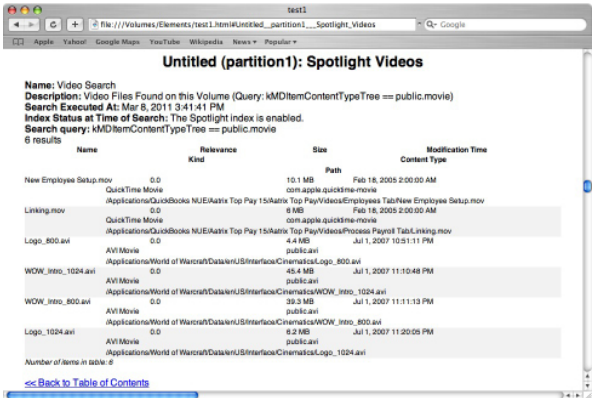
21. After about 30 seconds, the report was opened in Firefox automatically. It was determined this was configured as the default browser for this machine.

22. This report contained several bookmarks representing the sections seen earlier with the tool.





23. Clicking one the sections brings up that particular part of the report, in the case illustrated here, "Spotlight Videos."



24. The report was closed.

25. Mac Marshal was then closed.

Note: During this entire process, screenshots were being captured to "/users/TDFC/ScreenShots/" for the purposes of this report. Data contained in the report may reflect these screenshots. These screenshots were then copied to the external USB hard drive to be transferred to the report writing computer.

In this test the tool performed as expected. While there was not much data on this seldom used Powerbook to create interesting results, the tool acquired the drive and displayed some information. The report generation was simple and easy to read. The only difficulties encountered performing this test were that the case needed to be saved to a drive other than the one that was being examined, and that the live preview screen was quite wide and somewhat difficult to navigate. Having to save a case to a separate drive is a safeguard against overwriting potential evidence. Other than these extremely minor issues the tool performed quickly and efficiently, and was easy to use.

Test 2 – Mac Marshal Forensic Edition

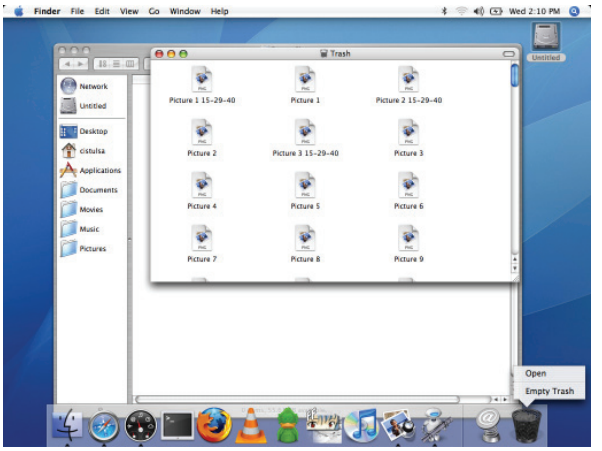
This test was performed to determine any differences between Mac Marshal Field Edition and Mac Marshal Forensic Edition. According to the website and documentation, Mac Marshal Field Edition is identical to Mac Marshal Forensics Edition with the exception of being portable, able to run on multiple machines per license and able to capture the live information of a running system. Prior to this test, an e-mail from ATC-NY was obtained that contained a link to the Mac Marshal Forensic Edition install and a key for Mac Marshal Field Edition.

In the following test, the same steps as Test 1 were performed. Screenshots were only to note any significant differences between the two products. This test was also performed on the Powerbook G4 running OS X 10.4.

The following steps were performed:

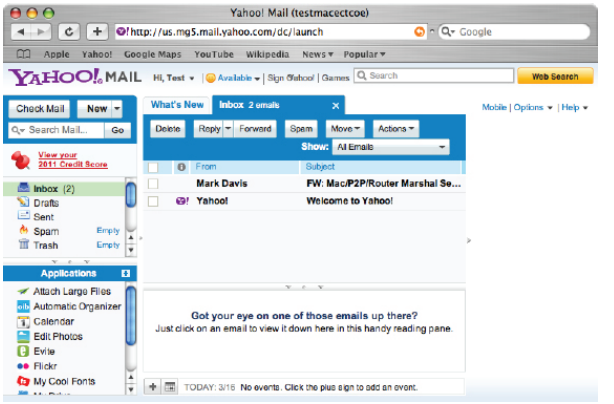
1. The Powerbook G4 was plugged into a wall outlet.

2. The Powerbook G4 was then booted by pressing the power button.

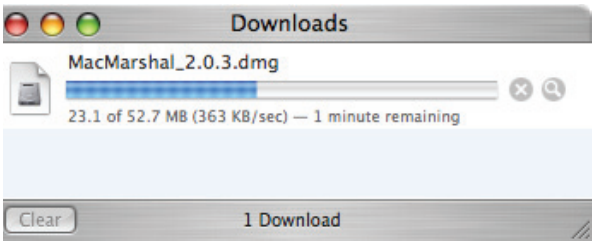


3. The folder “/users/TDFC/Screenshots” was opened. All files were selected and the “File->Move to Trash” option was selected. The Trash Can item was then selected by holding the mouse button and using the “Empty Trash” option.

4. The Powerbook G4 was then connected to a Ethernet cable, and assigned a static IP address on network interface “en0.” Safari was opened and www.yahoo.com was browsed to. “Sign up” was selected and test account named “TestMacEctcoe” was created. The install e-mail containing the links to the downloads and the keys was then forwarded to this account. This screenshot is not displayed in order to preserve the integrity of the keys using for testing



5. The e-mail was opened and the link to MacMarshal_2.0.3.dmg was selected. This started the download to the Powerbook G4. Once completed, this action created an icon on the desktop and opened the following window.

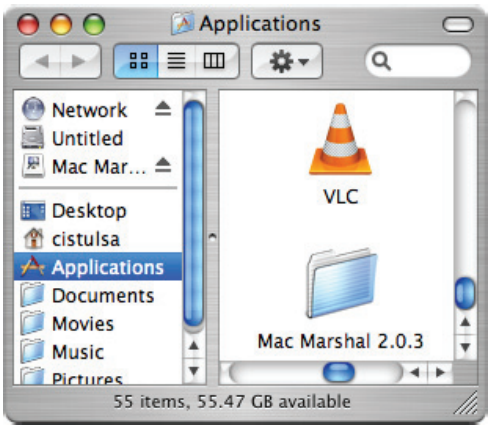


6. “Install Mac Marshal” was selected. This launched the installer screen. “Continue” was selected.

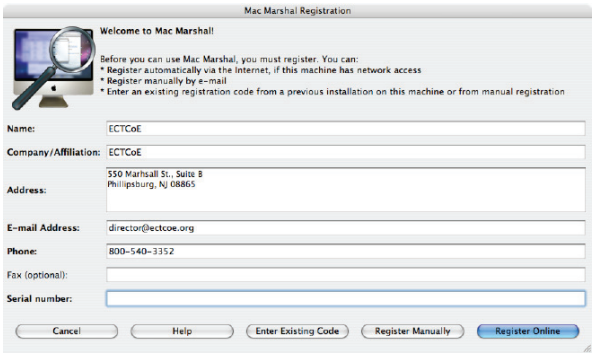
7. This ran the Mac Marshal Installer. All default options were selected and the screens were clicked through selecting “Next” at each stage. The install screen then appeared with a status bar indicating the installation progress. After about 10 seconds, the “Finish Up” screen was displayed. “Close” was selected.

8. From the menu “Go->Application” was selected. After browsing to the bottom of this window the Mac Marshal folder was displayed.

9. The folder was selected and the contents displayed. “Mac Marshal” was double clicked.



10. After the initial splash screen, the “Mac Marshal Registration” screen was displayed. The screenshot shows the values entered. The serial number from the e-mail was used and was not captured in the screenshot. “Register Online” was then selected.

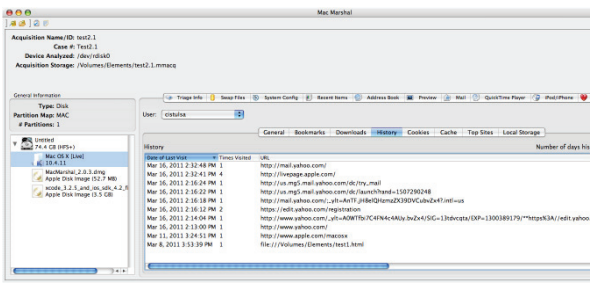


11. The “Registration Successful” screen was displayed. “Ok” was selected.

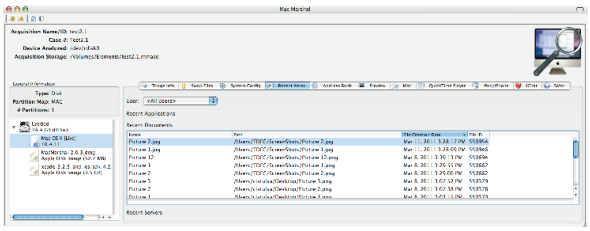
12. At this point, the same screens that appeared with the field edition were displayed. A new case was created identical to all of the steps in Test 1, using “Test 2” for any entries of “Test 1.”

13. The same occurrence about not saving the case to the drive to be analyzed occurred. The external USB hard drive was then connected and selected to save the case. All other steps performed were identical to Test 1. The test took a comparable amount of time to Test 1 to analyze the file system.

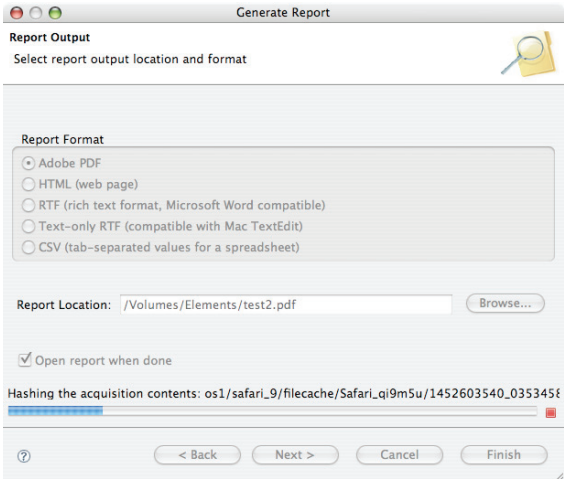
14. After completion, the same disk triage was selected, the “Safari” tabbed browsed to and “History” was selected. This screen displayed the connections to yahoo.com used during the installation of Mac Marshal Forensic Edition as expected. All of the other screens appeared similar to the results of Test 1.

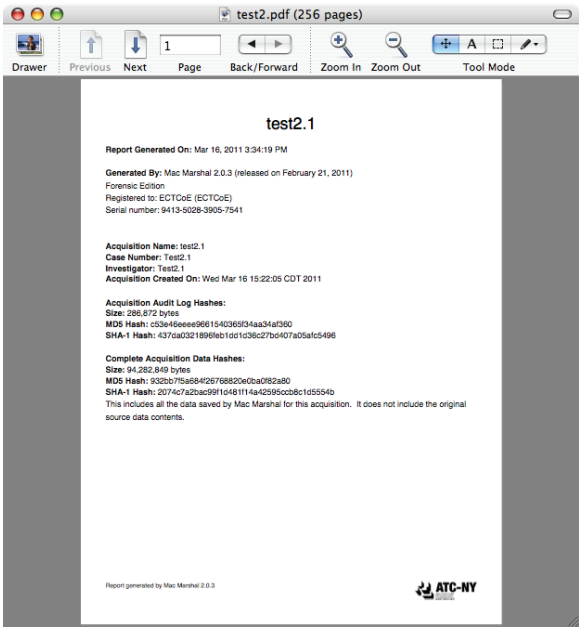


15. Screenshots that were viewed recently on this Powerbook as a result of this testing were found under the recent items tab.



16. A report was created, this time selecting the "Adobe PDF" format. This report was saved to the external USB hard drive as "Test2."





17. The screenshots taken during this test were then also copied to the external USB hard drive for inclusion in this report.

18. Mac Marshal was closed and the Powerbook G4 shutdown.

19. The screen and operation of this test were identical to the Mac Marshal Field Edition with the exception of the initial installation procedures.

It should be noted that this was not a proper forensics examination of this computer. Mac Marshal Forensic Edition should be installed on an OS X-based forensics examination computer, and any evidence or drives to be examined should be connected to the forensic examination machine using the proper write blocking precautions. This test was designed to simply test the functionality of Mac Marshal Forensic Edition. Because it is free to law enforcement, agencies that have access to an OS X-based forensic examination machine could benefit greatly from the use of this tool.

Test 3 – Performing Live Analysis of OS X 10.6.7

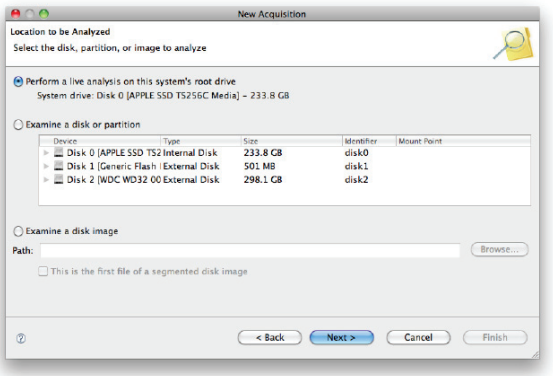
This test is designed to test the live analysis portion of Mac Marshal Field Edition on a Macbook Air running OS X 10.6.7. This test also differs from the previous test in that it is being performed on an OS X computer housing an Intel-based processer. No additional configuration was performed on this laptop. This test is designed to be the equivalent of running Mac Marshal Field Edition on an OS X machine will no prior knowledge of the contents of the system. Screenshots will only be included where steps or results differ from previous tests (splash screens, etc.) and to show results on this Macbook Air.

For this test the following steps were performed:

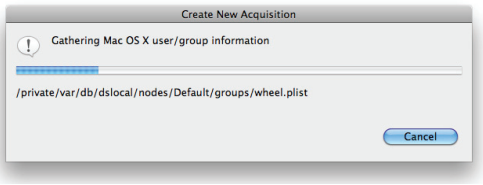
1. The Macbook Air was powered on by pressing the power button. The desktop was displayed. The Macbook Air displayed a list of available wireless networks. This window was closed without selecting a wireless network. The Airport (wireless card) on this Macbook was then disabled.

2. The Mac Marshal USB stick was plugged into the Macbook Air. The Mac Marshal Icon appeared on the desktop. Double-clicking this icon opened a window displaying the Mac Marshal folder. Double-clicking this folder displayed the Mac Marshal executable. This icon was double clicked. The Mac Marshal splash screen was displayed. “File->New acquisition” was selected. The “New Acquisition” screen was displayed and completed as shown in the screen shot. “Next” was selected.

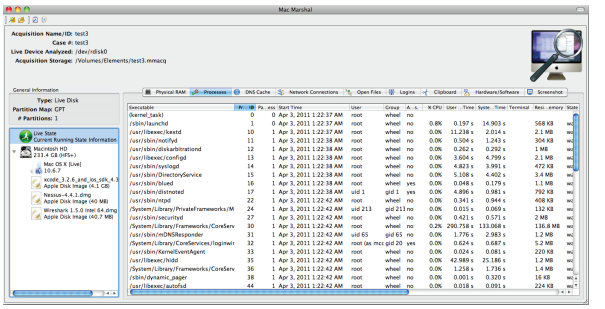
3. On the next screen, “Perform a live analysis on this system’s root drive” was selected by default. “Next” was selected.

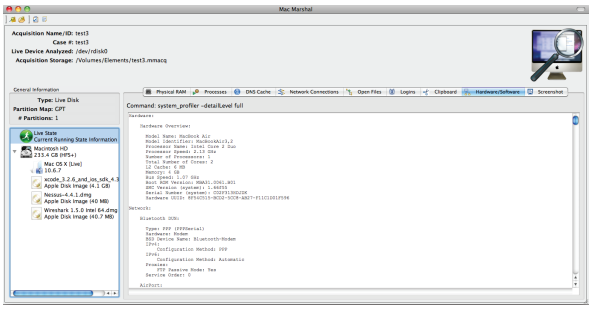


4. On the next screen all options minus the “Use direct file system operations on mounted disks” were selected and “Finish” was clicked. This process started at 1:33 p.m. and completed at 1:47 p.m.

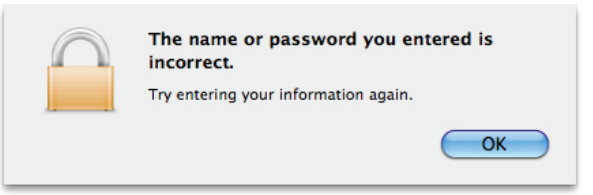


5. The results screen was displayed. The system asked for the user password to perform privilege actions. “Live State” was selected and several of the screens including “Processes,” “DNS Cache,” “Open Files,” “Logins” and “Hardware/Software” were browsed through. All of these screens displayed accurate information about the running state of the Macbook Air.

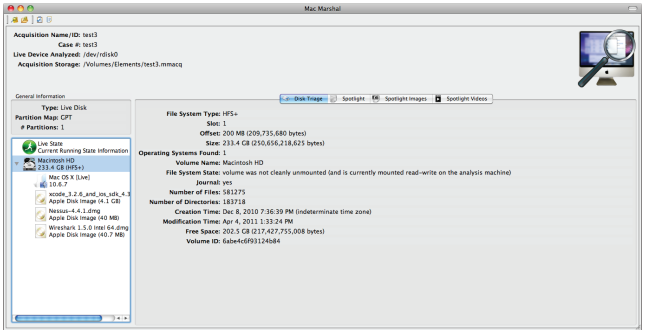


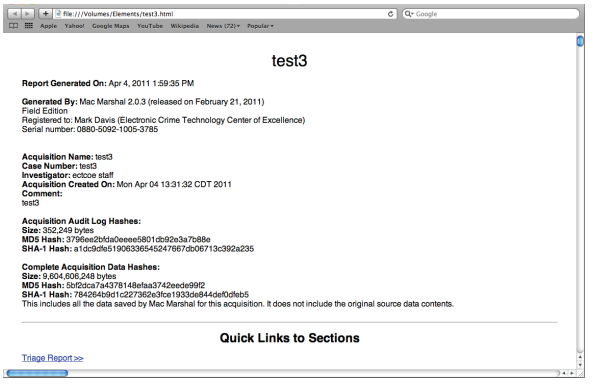


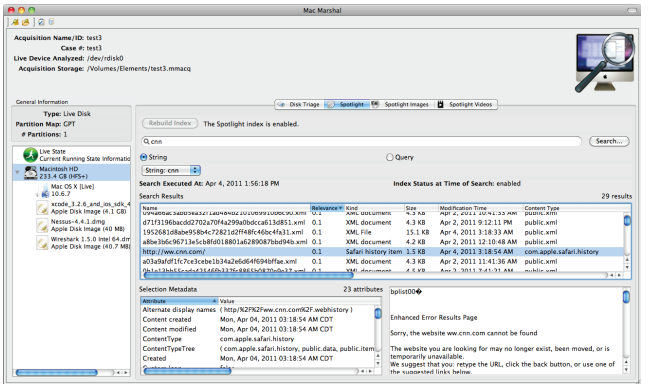
6. “Macintosh HD” was then selected. A bad password was intentionally entered. This resulted in the system asking for the password again. The correct password was then entered.

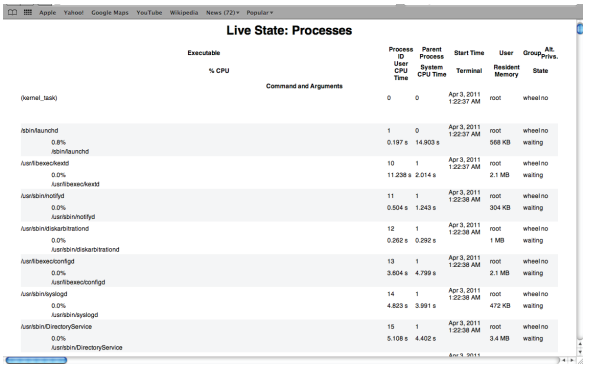


7. The spotloght search tab was selected. In the search criteria “cnn.com” was entered and the search was performed. The results were reviewed and an entry of this machine browsing to cnn.com was found as expected.

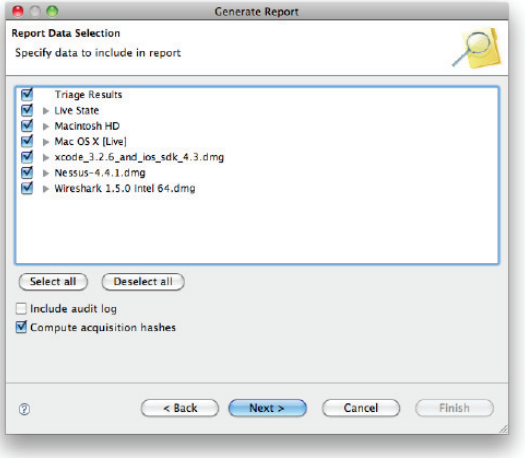




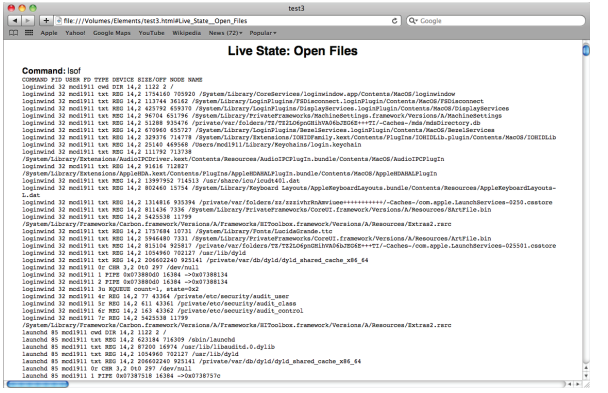




8. The generate report button was selected. The following selection criteria was used.



9. The report was then viewed for accuracy. A few screenshots of the report are included below.



In this test, the tool performed as expected. The tool was able to caputre information from a Mac OX X 10.6.7 system (at the time of this writing, the latest Mac OS X available from Apple). The tool did require a password to examine the hard drive. The tool was easy to use and navigate, a live search was performed easily and all of the live system information reviewed was deemed accurate.

Conclusion

In the three tests, Mac Marshal performed as expected. Several times it required the user to enter the system password to access information. The information the tool gathered was well displayed and easy to read, which would enable a law enforcement agent to quickly interpret the OS X-specific data on the machine. Mac Marshal Forensic Edition would either require a dedicated OS X-based forensics examination machine, or a request for a new license to examine each and every case. Mac Marshal Field Edition, at $199 USD, is a very cost-efficient way to have a tool that could examine multiple OS X-based machines.