

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	1
Evaluation and Testing of Mac Marshal™	5
Test Bed Configuration	ō
Mac PowerBook G4	ō
MacBook Air	ō
Download and Installation of Mac Marshal	ō
Test 1 – Running Mac Marshal Field Edition on OS X 10.4	3
Test 2 – Mac Marshal Forensic Edition 10)
Test 3 – Performing Live Analysis of OS X 10.6.7	3
Conclusion	7

Introduction

he 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 appropriate 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.

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

Overview

pple 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 website2:

"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' datasheets³:

"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."

²http://www.cyberstc.com/products_mac.asp ³http://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.

Name	Date modified	Туре	Size
.fseventsd	3/1/2011 10:52 AM	File folder	
.Spotlight-V100	3/1/2011 10:52 AM	File folder	
.Trashes	3/1/2011 10:52 AM	File folder	
🌗 Mac Marshal 2.0.3	2/22/2011 5:45 PM	File folder	
	3/1/2011 10:52 AM	TRASHES File	4 KB

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.)

Name	Date modified	Туре	Size
loconfiguration	2/22/2011 5:45 PM	File folder	
MacMarshal.app	2/22/2011 5:45 PM	File folder	
🎉 plugins	2/22/2011 5:45 PM	File folder	
SourceCode	2/22/2011 5:45 PM	File folder	
🍌 Tools	2/22/2011 5:45 PM	File folder	
.eclipseproduct	2/22/2011 5:45 PM	ECLIPSEPRODUCT	1 KB
ic.dat	3/1/2011 10:45 AM	DAT File	1 KB
🔁 Mac Marshal User Guide.pdf	2/22/2011 5:45 PM	Adobe Acrobat D	4,134 KB

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 stepby-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.
- 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.
- 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.



MAC MARSHALL









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

- New Acquisition

 Acquisition information

 Specify metadata for this acquisition

 Acquisition Name/ID:

 test1

 Comment:

 test1

 Investigator:

 ECTCOE

 Location to store data:

 /Users/clstulsa/test1.mmacg

 Browse....
- Mac Marshal then scanned for local drives and displayed the screen below. "Examine a disk of partition was selected" and "Disk 0" highlighted.

Decation to be Ai Select the disk, Perform a liv System dr Examine a di Device Device Device	nalyzed partition, or image e analysis on this sy ve: Disk 0 – 74.5 G sk or partition	to analyze ystem's root drive 8				×
Perform a liv System dr Examine a di Device Device Dis	e analysis on this s ve: Disk 0 – 74.5 G sk or partition	ystem's root drive B				
Examine a di	sk or partition					
Device						
	k 0	Type Disk	Size 74.5 CB	Identifier disk0	Mount Point	
► 🖾 Dis	k 2	Disk	501 MB	disk2		
O Examine a di	sk image					
Path:						Browse
This is	the first file of a se	gmented disk ima	ge			

 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.

00	Confirm Acquisition	Storage Location
The Mac Marsh analyzed. This data to be save	aal acquisition data is being stored witt s will modify the target's disk when and ed within the file system being analyze	hin the same file system (mounted at /) that is being alysis takes place! Are you sure you want the acquisition d?
	And With the Transfer File Contain	Rick Apathon Target on Acquisition Data Location

 At this point, another external USB Hard Drive (named "Elements") was attached to the Powerbook. Once the operating system mounted the external USB hard drive, an icon appeared on the desktop.



 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.

000		Location for Acquis	ition Data
	Save As:	test1.mmacq	
	Where:	Elements	÷
	Format:	Default	•
			Cancel Save

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

0	0		New Acquisition			
Locatio	on to be Analyzed					0
Select	the disk, partition, o	sk, partition, or image to analyze				X
O Per	form a live analysis o	n this system's root	drive			
	System drive: Disk 0 -	- 74.5 GB				
• Ex	amine a disk or partiti	on				
	Device	Туре	Size	Identifier	Mount Point	
	Disk 0	Disk	74.5 CB	disk0		
	Disk 2	Disk	501 MB	disk2		
OEx	amine a disk image					
Path:						Browse
	This is the first file	of a segmented dis	k image			
		or a segmentee on	in things			
1			(< Back)	(Next >)	Cancel	Finish

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.

00	New Acquisition	
Acquisition Options		
Configure additional options fo	r this acquisition	X
Use direct file system operat	ons on mounted disks, rather than having Mac Marshal interpret the file syste	em
(faster, but may change file	access times on volumes mounted without a write blocker)	
Automated Analysis		
The following potentially slow To perform them immediately	operations are normally performed on demand. select the appropriate boxes.	
🗹 📋 Swap Files (Copy the n	achine's swap files and sleep/hibernate image)	
Spotlight Images (Sear	h for all image files (JPG, GIF, PNG, etc.) on the target using Spotlight)	
Spotlight Videos (Searc	h for all video files (MPG, MOV, AVI, etc.) on the target using Spotlight)	
Mail (Acquire all e-mai	messages stored by Apple Mail)	
3	< Back Next > Cancel (Finish

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

		Authenticate
	To perform requires th	n privileged actions, Mac Marshal Prep nat you type your password.
	Name:	TDFC
	Password:	
► Details		
?		Cancel OK

 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).



- 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.

· O Nac Marshal		
4 4 2 0		
Acquisition Name/ID: tost1		
Case #: test1		
Device Analyzed: (dev/rdisk0		
Acquisition Storage: /Volumes/Elements	/test1.mmacq	
General Information	- Trage Info 🚦 Swap Tries 🗿	Spann Carlig 👔 Room Iams 🛞 Adduss Book 🕱 Prodes 🛞 Mall 💮 QuickTine Nayor 🕼 Pool/Phone 😝 (Chat 🖬 Safar)
Type: Disk		
Partition Map: MAC	User: <user at="" tdfc="" users=""></user>	
# Partitions: 1		General Bookmarks Downloads History Cookies Cache Top Sites Local Storage
V State (Billion)	History	Number of days history is kept: 31 [defa
Mar (DLX [Live]	Clate of Last Valt + Tires Valted	UPL UPL
10.4.11	Jun 27, 2007 5:35:00 PM 2	https://www.geogle.com/accounts/ServiceLoginAath?service+mail
xcode_3.2.5_and_iss_sdk_4.2.5	Jun 27, 2007 5:34:53 PM 2	http://gmail.com/
Apple Disk Image (3.5 G8)	Jun 27, 2007 5:34:31 PM 2	http://www.mozila.com/products/download.html/product=firefox=2.0.0.4&ss=osx8/ang=en=US
	Jun 27, 2007 5:54:24 PM 2	http://www.mozila.com/en-US/Tirefs#/
	Jun 27, 2007 5:54 16 PM 1	NEp //news.googe.com/
	Jun 27, 2007 11:54:06 AM 1	NEp //www.apple.com/mackex/git
	Jun 26, 2007 7:24:45 PM 1	NED //Damentriess.com/utament-hor-insc-it-comise_bi-ebie
	Jun 26, 2007 72353 PM 1	http://www.partonana.com/wp-content/uprace/2007/04/baty-on-neverming-assim-coverge.
	Jun 26, 2007 7 23 43 PM 1	http://digg.com/music/ine_baby_on/Nivana_s_Nevernine_accur_is_1/_inc
	Jun 26, 2007 7:23:26 PM 1	http://digition/
	Jun 26, 2007 7:22:37 PM 1	http://www.bashkpad.com/ineex
	Jun 20, 2007 7 22 31 PM 1	nttp://www.googe.com/searchmientocenne-searchmise-entose-Adol=Spell&reshuth=OEct=result&cd=L&q=maz+optimized+Finehocdsp
	Jun 26, 2007 7 22 29 PM 1	NIP //www.google.com/searchig=mac+opmized+tretox8xe=UTF-8
	200 20, 2007 C 2218 PM 1	under 1 (sowellingen weiten vormal)

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

00		Ger	nerate Report		
Report Informa Specify report	tion information				P
Report Name:	test1				
Comment:	test1				
Custom head	der (optional) header:				
Custom loge	o image:				Browse
(?)		Back	Next >	Cancel	Finish

- 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."
- 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.

Generate Report	
ocation and format	P
nat, Microsoft Word compatible)	
mpatible with Mac TextEdit)	
ed values for a spreadsheet)	
olumes/Elements/test1.html	Browse
done	
< Back Next > Ca	ncel Finish
	Cenerate Report ccation and format mat, Microsoft Word compatible) mpatible with Mac TextEdit) ed values for a spreadsheet) olumes/Elements/test1.html done ca

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

$\Theta \cap \Theta$	Generate Report	
Report Output Select report output	P	
Report Format		
Adobe PDF		
• HTML (web page	:)	
ORTF (rich text fo	rmat, Microsoft Word compatible)	
O Text-only RTF (compatible with Mac TextEdit)	
O CSV (tab-separa	ted values for a spreadsheet)	
Report Location: //	/olumes/Elements/test1.html	Browse
Open report whe	n done	
Hashing the acquisition	on contents: os1/safari_9/cache_oldstyle- <u< td=""><td>iser at _Users_TDFC>/050527</td></u<>	iser at _Users_TDFC>/050527
0	< Back Next > C	ancel Finish

- 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.

Image: The control of the control o	000						testl			
the second	4 -> 0	+	🖻 file:///Volu	mes/Elemen	ts/test1.htm	1			* Q,- Google	
<section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	Apple	Yahoo!	Google Maps	YouTube	Wikipedia	News # P	opular v			
<section-header><pre>bests prove the sevent business and the sevent b</pre></section-header>										
<pre>test i test i test</pre>							toott			
Raper Generated On: Mar R, 2011 253:00 PM Banerated Dy: Mar Marshall 201 (viewsand on February 21, 2011) To El dialon: Banerated Dy: Mar Marshall 201 (viewsand on February 21, 2011) The Summer: Will Banerated Dy: Marshall Banerated Resultation Creation Marshall Conference on Summer							lesti			
Banchard Day Banchard 2.0.1 (released on Fachuary 2.1, 2011) The Table Table Table Science	Report	Genera	ated On: Ma	r 8, 2011 :	3:53:03 PM	4				
Fried Edam (Registered b: Mark: Devis (Electronic Column Echnology Center of Excellence) Sensi number: 0809-0902-1005-3783 Acquisition Name: sensi Case Number: sensi Case Number: sensi Case Number: sensi Network of the Sensition Name: sensitic Network of the Sensition Name: sensitic Name: sensitic Name:	Canara	ted Bu	Mac Marsh	al 2 0 2 (m	lassed or	Eeboueeu	91 90111			
Tagister dis Mark Davis (Electronic Crime Technology Center of Excellence) Sequitation Name: Iself Sare Number: Iself Sare	Field Ed	tition	. Midu Midron	ai 2.0.0 (re	ileased of	rebibaly	21,2011)			
and a minimum a monoport of the second of th	Registe	red to: I	Mark Davis (Electronic	Crime Te	chnology	Center of Exc	ellence)		
<text><text><text><text><text></text></text></text></text></text>	oenai n	uniber.	0000-0082-	1005-376						
Case Number: lead of the second of the Mar 00 15:40:00 CST 2011 Acquisition Created On: Tue Mar 00 15:40:00 CST 2011 Comment: Watt Mar Mark Comment: Base: 00:40:40:00 protects DMT Hash: c:RobertowsdWatt 1:60:00:00:20180:00:00:00:00:00:00:00:00:00:00:00:00:0	Acquie	ition N	ame-leet1							
<pre>https://www.initian.com/i</pre>	Case N	umber	: test1							
Comment: Watt Section Audit Log Isabate: Section Audit	Investig	gator: E	ECTCoE	Tue Mar O	15-40-00	CST 201				
testi See ei alue alue alue alue alue alue alue alue	Comme	ent:			10.10.00	001 201				
Acquisition Audit Log Patients: Weis 1993. Weissing 77: 54: 51: 1170 2003:05: 1146: 05: 05: 05: 05: 05: 05: 05: 05: 05: 05	test1									
State:::::::::::::::::::::::::::::::::::	Acquis	ition A	udit Log Ha	shes:						
SNA-1 Heah: ::2684cteas4811.1055385ci1464c9942119eb976 Compares Acquisitions BMS Heah: ::277 STATUS Bit 0465cc5202aeb5205ede0055e469d5 SNA-1 Heah: ::26054acob520aeb6250aeb6250e46055e469d5 SNA-1 Heah: ::26054acob520aeb6250aeb6250e46055e469d5 SNA-1 Heah: :26054acob520aeb6250aeb6250e46055e469d5 SNA-1 Heah: :26054acob520aeb6250aeb6250e46055e469d5 SNA-1 Heah: :26054acob520aeb6250aeb6250e46055e469d5 SNA-1 Heah: :26054acob520aeb6250aeb6250e46055e469d5 SNA-1 Heah: :26054acob520aeb6250aeb6250e46055e469d5 SNA-1 Heah: :26054acob520aeb6250aeb6250e46055e469d5 SNA-1 Heah: :26054acob520aeb6250e46055e469d5 SNA-1 Heah: :26054acob520aeb6250e46055e469d5 SNA-1 Heah: :26054acob520e46055e469d5 SNA-1 Heah: :26054acob520e46055e4664 SNA-1 Heah: :26054acob520e46055e4664 SNA-1 Heah: :26054acob520e46055e46665 SNA-1 Heah: :26054acob520e4666566666 SNA-1 Heah: :26054acob520666666666666666666666666666666666666	Size: 19 MD5 Ha	91,484 i ssh; f74	bytes 7e4c1611f7	09a98e36	aa83d15d	826				
Complete Acquisition Data Nations: See: 2024.492 Mail: Mail: Mail: Sec: 2024.402 Mail: 2024.2024.2024.2024.2024.2024.2024.2024	SHA-1	Hash:	268ef0ea46	14110693	d85d1464	c99d2119	eb976			
Site: B0.42.43b types MS Healt: S7371 foldbit 0.04bcbc3.83443324814 SHA-TI Mait: Sec054.accebb 78bcb250242e8b20e4e0055e46903 This includes all the data assed by the kannhait for this acquisation. It does not include the original source data contents.	Comple	ete Aco	uisition Dat	a Hashes						
May Hank: "Christian Characterian Scheduler: "Christian Characterian Charatterian Charatterian Characterian Characterian C	Size: 80	0,424,4	59 bytes							
This includes all the data saved by Max Manshal for this acquisition. It does not include the original source data contents.	SHA-1	Hash: (20354acc6	bb785cd2	502a2eb5	2c4edc05	5e469d			
	This inc	ludes a	II the data s	aved by M	ac Marsha	I for this a	equisition. It d	oes not include	the original source data contents.	
test					_					
test										
tot Triage Report Section										
Image: Display: The second	0						test1			
Apple Value See get Mays Year Method Water Culcic Links to Sections Trigge Reports United (particina): Society Musica as United (particina): Society Musica as Marc 26 X Livel (onl: Synath Ress All	> C	+	€ file:///Volur	nes/Elemen	ts/test1.htm	l.			* Q+ Google	
Cluck Links to Sections Trige Reportse United (partition): Spotight se United (partition): Spotight Insges se United (partition): Statist se United (partition): Chains se United (p	Apple	Yahoo!	Google Maps	YouTube	Wikipedia	News + Po	opular 🔻			
Cluck Links to Sections										
Inited Report to: Inited Control Scotlight to: Inited Control Scotlight Name Sites of Inited Control Scotlight Name Sites of Rec OX X.LVel Contl: Synate Sites or Rec OX X.LVel Contl: Synate Sites or Rec OX X.LVel Contl: Providence Rec OX X.LVel Contl: Solation se Rec OX X.LVel					Qu	ick Li	nks to Se	ctions		
Index Conductors Index Conductors Index Conductors Social Provided Conductors Soci	Maga D	lonot -	2							
Initial granition 1: Social in mage 2:> Initial granition 1:: Social 2:: Initial granition 1:: Initian 1::	meye r	iepon 2	2							
Interest pointerior in Sporting Historia Sec Interest pointerior in Sporting Historia Sec Interest Pointerior Interest Marc OS X, Livel (point): System Cooling sec Marc OS X, Livel (point): Research Historia Sec Marc OS X, Livel (point): Marcine Player sec Marc OS X, Livel (point): Could Sime Player sec Marc OS X, Livel (point): Chartise Marc OS X, Livel (point): Chartise Marc OS X, Livel (point): Salari sec Marc OS X, Livel (point): Sa	Intitled	(partitic	n1): Spotlig	ht 22						
Ana: C6 X . Lve] (dd1): Swap, Files >> Bac C6 X . Lve] (dd1): System Config >> Bac C6 X . Lve] (dd1): Address Book >> Bac C6 X . Lve] (dd1): Address Book >> Bac C6 X . Lve] (dd1): Mal >> Bac C6 X . Lve] (dd1):	Intitled	(partitic	n1): Spotig	ht Videos	22					
Nex CB2 Livel_ion1: Syntem Cardig see Mex CB2 Livel_ion1: Recent liment see Mex CB2 Livel_ion1: Address Book see Mex CB2 Livel_ion1: Address Book see Mex CB2 Livel_ion1: Address Book see Mex CB2 Livel_ion1: Charts me Mex CB2 Livel_ion1: Charts see Mex CB2 Livel_ion1: Status see Mex CB2 Livel_ion2: Status see	tee OP	V D have	Londh Dura	. Elles						
Idea CB X, Livel, Joint J. Reisent Items iso Idea CB X, Livel, Joint J. Address Book isos Idea CB X, Livel, Joint J. Address Idea CB X, Livel, Joint J. PoulfPone as Idea CB X, Livel, Joint J. Reisent as Idea CB X, Livel, Joint J. Shaft as Kequisition Audit Log as Triage Report Type: Disk Triage Report Partison Hap: IAAC Partison Hap: IAAC	Aac OS	X Live	1 (os1): Swa	em Config	22					
Mar Colo Line Line Line Particular Solutions Mar Colo Line Line Line Line Particular Solutions Mar Colo Line Line Line Line Line Marson Mar Colo Line Line Line Line Line Line Marson Mar Colo Line Line Line Line Line Line Line Marson Marco Sal Line Line Line Line Line Line Line Line	Aac OS	X [Live	(os1): Rece	ent Items a	2					
Ider CB X LL Veil (coli): Metal con Ider CB X LL Veil (coli): Doubt Time Payer con Ider CB X LL Veil (coli): Post Home con Ider CB X LL Veil (coli): Salati con Ider CB X LL Veil (coli): Con Ider CB X LL Veil (co	Aac OS	X Live	1 (os1): Addr 1 (os1): Prev	iew >>>	22					
Mac Cas X, Lue Joint, Cauck Time Physics> Mac Cas X, Lue Joint, Prodifforms >> Mac Cas X, Lue Joint, Prodifforms >> Mac Cas X, Lue Joint, Prodifforms >> Mac Cas X, Live Joint, Salari >> Mac Cas X, Live Joint, Prodifforms >> Triage Report Type: Disk Triage Report Partision Map: MAC Partisions : 1	fac OS	X [Live	(os1): Mail	22						
Mac CS X [Live] (os1): Shaft as localistics Audit Log as Triage Report Vps: Disk antition Map: MAC Partitions 1	fac OS	X Live	(os1): Quic	APhone ~	yer >>					
Acquisition Audi Log 200 Acquisition Audi Log 200 Triage Report Partition Map: MAC Partition : 1	Mac OS	X [Live	(os1): iCha	122	-					
Incusition Audit Log >> Triage Report Vpe: Disk Partition Map: MAC Partitions: 1	Aac OS	X [Live] (os1): Safa	fi.22						
Triage Report Specification Map: MAC Partitions 1	Acquisit	ion Aud	it Log >>							
ype: Disk artition Mag: MAC Partitions: 1						Tria	ge Repo	rt		
Partition Map: MAC # Partitions: 1	Type: D	isk								
# Paruuons: I	Partition	Map:	MAC							
	Partiti	ons: 1								
Bendid an B. Harddan d (a solid and)					-					

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

Anala Valuat d	mania Mana	Take Willingdia New	a Bandara		and south	
Apple Tanoor G	oogie waapa iros	Intitled (new	this at . Ca	allia he M	Ideas	
		Untitled (par	ution i): sp	otlight v	ideos	
Name: Video Sea	arch					
Description: Vid	eo Files Found	on this Volume (Qu	ery: kMDitemConte	entTypeTree	== public.movie)	
Index Status at 1	ime of Search	The Spotlight inde	v is enabled			
Search query: kl	MDitemConten	TypeTree == public	movie			
6 results		anyporteo paone				
Name		Relevance	Size		Modification Time	
		Kind			Content Type	
New Employee Cotyo			10.1 MB	Path Exh 18 1	005 3 00 00 AM	
rese criticities perch.	QuickTime Movie		com apple o	uicklime-movie	000 £.00 00 PM	
	(Applications/Qui	okBooks NUE/Aatrix Top P	ay 15/Aatrix Top Pay/Vic	deos/Employees 1	Tab/New Employee Setup mov	
Linking.mov	0.0		6 MB	Feb 18, 2	005 2:00:00 AM	
	QuickTime Movie	1	p.elqqa.moo	uickime-movie		
	Applications/Qui	okBooks NUEWatrix Top P	hay 15/Aatrix Top Pay/Vie	deos/Process Pay	roll Tab.Linking.mov	
Logo_800.avi	AVI Marvin		4.4 MB	Jul 1, 200	7 10:51:11 PM	
	/Anninetions/Wo	rid of Warran Data and ISI	Interface Cinematical or	an 800 avi		
WOW_Intro_1024.avi	0.0		45.4 MB	Jul 1, 200	7 11:10:48 PM	
	AVI Movie		public.avi			
	(Applications/Wo	rid of Warcraft/Data/enUS/	Interface/Cinematics/W0	W_Intro_1024.av	1	
WOW_INNO_800.avv	0.0		39.3 MB	Jul 1, 200	7 11:11:13 PM	
	/Annihestions/Min	dd of Warrah Dataiani IRI	Interface Cinematics MIC	W Inter BOD and		
Logo_1024.avi	0.0		6.2 MB	Jul 1, 200	7 11 20:05 PM	
	AVI Movie		public.avi			
	(Applications/Wo	rid of Warcraft/Data/anUS/	Interface/CinematicsLog	0_1024.avi		
Number of items in tab	ha: 6					

- 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 safe-guard 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.

000		🗑 Trash		
Network	Picture 1 15-29-40	Picture 1	Picture 2 15-29-40	0
Desktop	Picture 2	Picture 3 15-29-40	Picture 3	
Applications Documents Movies	Picture 4	Picture 5	Picture 6	
Music Pictures	Refuter 2	Return R	Picture 9	
				Open
C)) 4 F

 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

\varTheta \varTheta 🔿 Yahoo! Mail (testmacectcoe)	
C + Ofhttp://us.mg5.mail.yahoo.com/dc/launch	
🛱 Apple Yahoo! Google Maps YouTube Wikipedia News 🔻 Popular 🕶	
YAHOO! MAIL HI, Test - Sign Orthool Games Q. Search	Web Search
Check Mail New - What's New Inbox 2 emails × Mobile	Options • Help •
Qv Search Mail Go Delete Reply T Forward Spam Move Actions T	
Show: Al Emaile -	
2011 Credit Score From Subject	
Mark Davis FW: Mac/P2P/Router Marshal Se	
S Drafts Velcome to Yahoo!	
E Sent	
M Spam Empty	
III Irash Emply	
Applications EI	
Attach Large Files	
alb Automatic Organizer	
Got your eye on one of those emails up there?	
Edit Photos	
G Evite	
•• Flickr	
D My Cool Fonts	

 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.

00	Downloads	
	MacMarshal_2.0.3.dmg	
	23.1 of 52.7 MB (363 KB/sec) — 1 minute rem	naining
_	_	
Clea	1 Download	11.

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

 \bigcirc



Mac Marshal User Guide.pdf

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.

	The software was successfully installed
 Introduction License Select Destination Installation Type Install Finish Up 	Mac Marshal has been successfully installed! When using the software for the first time, you will be prompted to register it. You will need a serial number for the registre@macmarshal.com. Registration can be performed on-line, if this machine is connected to the Internet, or can be done by e-mail; simply follow the prompts when you first run Mac Marshal.

 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.

888		Mac Marshal
a a] 2 5		
Acquisition Name/ID: tost2:1 Case #: Test2:1 Device Analyzed: /dev/rdisk0 Acquisition Storage: /Volumes/Elements/	test2.1.mmacq	
General Information	Tringe brie 1 Swap files	🖏 System Config 👔 Recert Name 🐑 Address Book 🗰 Proving 🍙 Hall 🔅 QuickTime Foyer 🚱 Poul/Phone 🐐
Type: Disk Partition Map: MAC # Partitions: 1	User: cistulta	
Y SUbsted 74.4 CB (HFS+)	History	Carneral associations Downloads History Cookies Cache Tep Sites Local Storage
Mac OS X [Lve]	Oate of Last Visit Times Visiter	a lunc
Austral 22.2.1.4mg Apple Dok Inge (15.7.MD acote, 3.2.5.and (no. set), 4.2, 8 Apple Dok Inge (15.5.08)	Mar 16, 2011 232-45 MM 1 Mar 16, 2011 232-41 FM 4 Mar 16, 2011 232-41 FM 4 Mar 16, 2011 23-162 FM 1 Mar 16, 2011 23-163 FM 1 Mar 16, 2011 23-163 FM 1 Mar 16, 2011 23-164 FM 1 Mar 16, 2011 23-21 00 FM 1 Mar 11, 2011 324-51 FM 1 Mar 6, 2011 33-31 FM 1	WD [//most as application] WD [/most and with a second with multi-status 1307(2014) WD [/most application convol/minuteshare 1307(2014) WD [/most application], and with multi-status 2019(Calcular Constitution WD [/most application], and with multi-status 2019(Calcular Constitution) WD [/most application], and with multi-status 2019(Calcular Constitution), and with multi- tatus 2019(Calcular Constitution).

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

000		Mac Horohal		· · · · · · · · · · · · · · · · · · ·
a 😕 🛛 🖸 🖸				
Acquisition Name/ID: test2.1				
Case #: Test2.1				
Device Analyzed: (devird)/k0				
Acquisition Storage: /volumes/Elements	Jtest2.1.mmacc			1.
Sourced Information	Ge Trapins () to	a Ties 🛞 Apress Cardig (g) Benerg Bener (Cardig Cardina Benerg B	teviev 🐨 Ket 🛞 guerdine tever. 🖓	Neghter 👹 Kim 🔓 Ser
Type: Disk				
	and a second second	10		
Partition Map: MAC	EDDE: KANE UDDERSY	180		
4 Pertitions: 1	Recent Applications			
Partition Hap NVC Partitions: 1 Prototod	Recent Applications Recent Documents			
Partition Map MAC Partition: 1 The Control of Control The Control of Control Mark Control	Recent Applications Recent Documents	Test.	the Courtan Steel y The	n
Partitions: 1	Recent Applications Recent Documents Recent Documents Name Potane 2 jag	Ten Alters (TBC) formefinats (Patters 2.jpg	114 General-Gener + 754 Nar 11, 2011 1:28-17 PM 553	Ka
Partition Max. MAC # Partitions: 1 * State (Critical) Max 653 (Bio) (Critical) Max 653 (Bio) (Critical) Max Max Max Max Max Max Max Max Max Max	Recent Applications Recent Documents Nove Potane 2 jag Potane 1 jag	nes Alvers/TBEC/EconorStatic/Fisture 2.jpg Alvers/TBEC/EconorStatic/Fisture 2.jpg	The Construct Street y The New 11, 2011 1028 (2019), 550 New 11, 2011 1028 (2019), 550	n 166 146
Purdiene Map. MAC. 4 Partitione: 1 ▼	Recent Applications Recent Applications Recent Documents Name Portume Type Portume Type Portume T2	Part Name, TBPC/AnnuerStank, Pintawa Dyng Alama, TBPC/AnnuerStank, Pintawa Dyng Alama, TBPC/AnnueStank, Pintawa Dyng	Th Creater State v This New 11, 2011 1028 (2004) 553 New 11, 2011 1028 (2004) 553 New 8, 2011 1026 (2004) 553	n Ma Ma Sa
Public Map. MAC.	Recent Applications Recent Applications Recent Documents Name Pritage 2 jung Pritage 1 2 Pritage 1	New (THE C/Constructions (Picture 2 (pg) News (THE C/Constructions (Picture 2 (pg) News (THE C/Constructions (Picture 2 (pg) News (THE C/Constructions (Picture 2 (pg) (News (THE C/Constructions (Picture 2 (pg))	Ter-Charan-Date V Tain War 11, 2011 33.51.7 BW 553 554 Mar 11, 2011 3.36.60 PW 553 554 Mar A, 2011 3.96.11 PM 515 554 Mar A, 2011 3.96.11 PM 515 554	n Mile Mile Mile Sile Sile Sile
Ruttlem Map, MAC # Partitions: 1 ▼	Recent Applications Recent Applications Recent Documents Dates Printee 2 Japa Printee 12 Printee 12 Printee 12 Printee 2	feet Alaren, THE Concerdinate, Philaren Dyng Alaren, THE Concerdinate, Philaren Dyng Alaren, THE Concerdinate, Philaren Dyng Alaren, THE Concerdinate, Philaren Dyng Alaren, THE Concerdinate, Philaren Dyng	The Desire 1: Set N Thir No. 11. 2011 1: 20.81 2 ML Set Set No. 11. 2011 1: 20.60 ML Set No. 4. 2011 1: 20.60 ML No. 4. 2011 1: 20.60 ML Set No. 4. 2011 1: 20.60 ML No. 4. 2011 1: 20.60 ML Set No. 4. 2011 1: 20.60 ML	n 660 1046 664 660
Publice Map. Not.	Recent Applications Recent Applications Recent Documents Recent Documents Recent Partner 2 jung Recent 2 Recent 2 Recent 2 Recent 3	The Allows THE Conservation of the set of any Allows THE Conservation of the set	The One on Steet The Mar 11, 2011 13:81:00 458 Mar 11, 2011 13:80:00 550 Mar A, 2011 13:00:11:00 550 Mar A, 2011 13:00:01:00 550 Mar A, 2011 13:00:01:00 550 Mar A, 2011 13:00:01:00 550 Mar A, 2011 13:00:01:00:01:00 550 Mar A, 2011 10:01:01:01:01:01 560 Mar A, 2011 10:01:01:01:01:01 560	n Med Med 604 667 660 729
Redition Maps XXX 4 Pertitions XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Recent Applications Recent Applications Recent Documents Lowe Patture 2.j Patture 12 Patture 1 Patture 2 P	Terr Allward, TBE C / Konner Konst, Minister D Jarg Allward, Tu Link Jarg, Minister, Minister D Jarg Allward, Tu Link Jarg, Minister, Minister D Jarg	The Owner's Steet In Mar. 11, 2611 1324 (2004) 555 Mar. 2001 1326 (2004) 555 Mar. 2001 1326 (2004) 556 Mar. 2001 1326 (2004) 556 Mar. 2001 1326 (2004) 556 Mar. 2001 1326 (2004) 556 Mar. 2001 1326 (2004) 556 Mar. 2001 1327 (2004) 556 Mar. 2001 1326 (2004) 556 Mar. 2001 1327 (2004) 556 Mar. 2001 1327 (2004) 556 Mar. 2001 1327 (2004) 556	n he6 he6 660 667 729 729 1

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

$\Theta \cap \Theta$	Generate Report	
Report Out Select rep	tput port output location and format	P
Report Fo	ormat	
• Adobe	e PDF	
OHTML	L (web page)	
O RTF (r	rich text format, Microsoft Word compatible)	
O CSV (t	(tab-separated values for a spreadsheet)	
(-		
Report Lo	ocation: /Volumes/Elements/test2.pdf	Browse
✓ Open i	report when done	
Hashing the	e acquisition contents: os1/safari 9/filecache/Safari o	i9m5u/1452603540_0353458
_		
?	< Back Next > (0	Cancel Finish
00	🖹 test2.pdf (256 pages)	0
-&		
Drawer Pr	Previous Next Page Back/Forward Zoom In Zoo	m Out Tool Mode
	test2.1	
	Report Generated On: Mar 16, 2011 3:34:19 PM	
	Generated By: Mac Marshal 2.0.3 (released on February 21, 2011) Forensic Edition	
	Registered to: ECTCoE (ECTCoE) Serial number: 9413-5028-3905-7541	
	Acquisition Name: test2.1 Case Number: Test2.1	
	Acquisition Created On: Wed Mar 16 15:22:05 CDT 2011	
	Acquisition Audit Log Hashes: Size: 286,872 bytes	
	MD5 Hash: c53e46eeee9661540365/34aa34af360 SHA-1 Hash: 437da0321896leb1dd1d36c27bd407a05afc5496	
	Complete Acquisition Data Hashes: Size: 94.282,849 bytes	
	MD5 Hash: 932bb7f5a684f26768820e0ba0f82a80 SHA-1 Hash: 2074c7a2bac99f1d481f14a42595ccb8c1d5554b	
	This includes all the data saved by Mac Marshal for this acquisition. It does no source data contents.	t include the original
	Designment in the Manhol 202	
	responsigor research by 1988 (MB21948) 4.0.0	ALC-NY

- 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:

 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.
- On the next screen, "Perform a live analysis on this system's root drive" was selected by default. "Next" was selected.



 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.

Create New Acquisition	
() Gathering Mac OS X user/group information	
/nrivate /var/dh/dsloral/nodes/Default/nrouns/wheel plist	
, privace) var juby usiocal, nodes, benancy groups, micer, prise	
	Cancel

 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.





 "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.

\bigcirc	The name or password you entered is incorrect.
	Try entering your information again.
	ОК

 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.

800	Mac Marshal
A 🖉 🛛 🖓 🖗	
Acquisition Name/ID: test3 Case #: test3 Live Device Analyzed: /dev/rdisk0 Acquisition Storage: /Volumes/Eleme	ns, fret3 mmarq
General Information	San Data Traper 2 Southalt 198 Southalt Insaes 🖬 Southalt Viteos
Type: Live Disk Partition Map: CPT # Partitions: 1	File System Type: H5+ Sile: 1 Sile: 20 Micro 2018 (2010 235 (40) here)
Uve State Current Running State Information	Size 213. C@ 120,656.218,623 bytes) Operating Systems Found: 1
233.4 GB (HF5+) Mac OS X (Live) 10.6-7	Volume Name: Macintosin HU File System State: volume was not cleanly unmounted (and is currently mounted read-write on the analysis machine) Journal: yes
xcode_3.2.6_and_ios_sidk_4.3 Apple Disk Image (4.1 GB)	Number of Files: 581275 Number of Directories: 183718
Apple Disk Image (40 MB)	Creation Time: Dot 8, 2010 / 305 yr MI (indoterinatio time zone) Modification Time: Apr 4, 2011 1:33:24 PM Free Space: 202 5 GI (217427, 755,008 bytes)
A the	Valuma ID: 6abrte(69)124014



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

00		Generate Report	
Report Data Se Specify data t	lection o include in report		P
✓ Triage ✓ ► Live Sti ✓ ► Macint ✓ ► Mac O: ✓ ► xcode ✓ ► Nessus ✓ ► Wiresh	Results atte osish HD S.X [Live] 3.2.6_and_ios_sdk i=4.4.1.dmg ark 1.5.0 Intel 64.dm	4.3.dmg	
Select all Include au Compute a	Deselect all dit log cquisition hashes		
0	C < Ba	ick Next >	Cancel Finish

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

> + offie:///Volumes/Elements/test3.html		Qr Google
III Apple Yahoo! Google Maps YouTube Wikipe	dia News (72) + Popular +	
	toot2	
	lesio	
Report Generated On: Apr 4, 2011 1:59:35 P	м	
Generated By: Mac Marshal 2.0.3 (released o	n February 21, 2011)	
Field Edition Registered to: Mark Davis (Electronic Crime T	rehableau Conter of Excellence)	
Serial number: 0880-5092-1005-3785	criticiogy Center of Excellence)	
Acquisition Name: test3		
Case Number: test3		
Acquisition Created On: Mon Apr 04 13:31:3	2 CDT 2011	
Comment: test3		
Acquisition Audit Log Hashes: Size: 352 249 bytes		
MD5 Hash: 3796ee2bfda0eeee5801db92e3a	7b88e	
SHA-1 Hash: a1dc9dfe51906336545247667c	b06713c392a235	
Complete Acquisition Data Hashes:		
Size: 9,604,606,248 bytes MD5 Hash: 5bf2dcs7a4378148afas3742aade	2002	
SHA-1 Hash: 784264b9d1c227362e3fce1933	de844def0dfeb5	
This includes all the data saved by Mac Marsh	al for this acquisition. It does not include the original sou	rce data contents.
	Quick Links to Costions	
	QUICK LINKS TO SECTIONS	
Triage Report >>		

Apple Yahoot Google Maps	YouTube Wikipedia News (72) * Popular *					
	Live State: Processes					
	Live State. Frocesses					
	Executable	Process	Parent Process	Start Time	User	Group Alt.
	% CPU	User CPU Time	System CPU Time	Terminal	Resident Memory	State
	Command and Arguments			Apr 3 2011		
(vernel_task)		•	•	1:22:37 AM	root	wheelno
/sbin/launchd		1	0	Apr 3, 2011 1:22:37 AM	root	wheelno
0.8%		0.197 s	14.903 s		568 KB	waiting
Asribexeckextd		10	1	Apr 3, 2011	root	wheelno
0.0%		11.238 s	2.014 s	12237 AM	2.1 MB	waiting
Just/libexec/kextd				Apr 3, 2011		
Asistemnotityd		11	1 242 6	1:22:38 AM	204 KB	wheelno
Jusrisbin/hotilyd		0.004 2	1.240 8		004160	making
Ausr/sbin/diskarbitrationd		12	1	Apr 3, 2011 1:22:38 AM	root	wheelno
0.0%		0.262 s	0.292 s		1 MB	waiting
Astribexecton1gd		13	1	Apr 3, 2011	root	wheelno
0.0%		3.604 s	4.799 s	122.00 Pm	2.1 MB	waiting
Austrilibexec/configd				Apr 3, 2011		wheelee
0.0%		4.823 s	3.991 s	1:22:38 AM	472 KB	waiting
Jusrisbin/syslogd						
Asr/sbin/DirectoryService		15	1	1:22:38 AM	root	wheelno
0.0% Justishin/Directon/Service		5.108 s	4,402 5		3.4 MB	waiting
				Anr 9 9011		

C

)

0	9 \Theta	test3		
	▶ + ≷n	c://Volumes/Elements/test3.html#Live_State_Open_Files C Qr Coogle		
m	III Apple Y	aboo! Google Maps YouTube Wikipedia News(72)* Popular*		
		Line Obstan Onen Films		
		Live State: Open Files		
	Command:	sof	- 1	
	COMMAND FID U	HER FD TYPE DEVICE SIZE/OFF NODE NAME		
	loginwind 32	nod1911 owd DIR 14,2 1122 2 /		
	loginwind 32	mod1911 txt REG 14,2 1754160 705920 /Eystem/Library/CoreServices/loginwindow.app/Contents/MacOS/loginwindow		
	loginwind 32	nod1911 txt REG 14,2 113744 36162 /System/Library/LoginPlugins/FSDisconnect.loginPlugin/Contents/MacOS/FSDisconnect		
	loginwind 32	nod1911 txt #80 14,2 423792 459370 /8ysten/Library/LoginFlugins/DisplayServices.loginFlugin/Contents/MacOS/DisplayServices		
	loginvind 32	holi911 txt REG 14,2 96/04 651796 /System/Library/PrivateFrameworks/RachineBettings.tramework/Versions/A/MachineBettings		
	loginwind 32	nod911 txt REG 14,2 51288 935476 /private/var/folders/TE/TELDeprElinVA085JEGE+++TI/-Caches-/mds/mdsDirectory.db		
	loginvind 32	holiyi txt kau 14,2 5/0960 555/2/ /system/library/logins/sereiservices.iogin/ingin/contents/secos/sereiservices		
	loginvind 32	holiyii txt kuu 14,2 3293/6 /14/18 /System Library Excensions/ Contents/Pingins/ Contents/Pingin/Contents/Madds/ Contents/Madds/ Contents/Pingins/ Contents/ Pingins/ Contents/		
	loginging 32	Neisii tat kao 14,2 25140 485988 /08015/101511/Library/Meyonains/10311.Anyonain		
	/System/Libra	mainten der som kapp statten i var kapp (ontents/Besources/BudioIDCP) vols. kundle/Contents/BeoG/AudioIDCP) unte		
	loginging 12	wed1011 +v+ DBG 14 2 01616 712827		
	/System/Libra	ry/Extensions/AppleHDA.Kext/Contents/PlugIns/AppleHDABALFlugIn.burdle/Contents/MecOS/AppleHDABALFlugIn		
	loginwind 32	nod1911 txt REG 14.2 13997952 714513 /usr/share/icu/icudt401.dat		
	loginwind 32	nod1911 txt REG 14,2 802460 15754 /System/Library/Keyboard Layouts/AppleNeyboardLayouts.bundle/Contents/Resources/AppleNeyboardLayouts-		
	L.dat			
	loginwind 32	nod1911 txt REG 14,2 1314816 935394 /private/var/folders/zz/zzzivhrRnAmviuee++++++++/-Caches-/com.apple.LaunchServices-0250.csstore		
	loginwind 32	nod1911 txt REG 14,2 811436 7336 /System/Library/PrivateFrameworks/CoreUI.framework/Versions/A/Resources/SArtFile.bin		
	loginwind 32	mod1911 txt REG 14,2 5425538 11799		
	/System/Libra	ry/Trameworks/Carbon.framework/Vermions/A/Frameworks/Eramework/Vermions/A/Resources/Extras2.rsrc		
	loginvind 32	hod yn i tet kau 14,2 i 137694 10731 Aynteen Librery Fonte Libradaurende tet		
	loginvind 32	Religit the sec 14,2 System claim claimer y religion claimer and concern religion with very solution of the second s		
	loginvind 32	<pre>Notifit tot Map 14,2 81104 9281/ /private/war/ioiders/ta/ta2asphumin/wardshowt+++1/-caches-/com.apple.Launchservices-02591.csscore example1 as mm 14 2 10/460 20112 /cssc/ide/d</pre>		
	loginging 12	maleri te pol 1 / 2 205000 0011 /nrive/na//h//dv/d/dv/d shared rache v85 54		
	logingind 32	mod1011 0r CHB 3.2 010 207 /dev/tull		
	logingind 32	mol1911 1 FTFE 0x07388040 16184 ->0x07388134		
	losinwind 32	mcd1911 2 FIFE 0x073880d0 16384 ->0x07388134		
	loginwind 32	ncd1911 3u XQUEUE count=1, state=0x2		
	loginwind 32	mod1911 4r RBG 14,2 77 43364 /private/etc/security/audit_user		
	loginwind 32	nod1911 5r RED 14,2 611 43361 /private/etc/security/audit_class		
	loginwind 32	mod1911 6r MEG 14,2 163 43362 /private/eto/security/audit_control		
	loginwind 32	mod1911 7r REG 14,2 5425538 11799		
	/System/Libra	ry/Frameworks/Carbon.framework/Vermions/A/Frameworks/Effoolbox.framework/Vermions/A/Remources/Extram2.rmr		
	Launond 85 no	ligit Own DIM 14,2 1122 2 /	- 1	
	Lounond 85 no	11711 ERE 650 1476 663164 (18997 /SDUIN/IBUIN/BU 11811 ERE 880 14 5 07061 16978 /SDUIN/IBUIN/BUIN/BU	- 1	
	launced 05 EC	AND THE MEN AND THE CAN'S AND A AND AND AND AND AND AND AND AND A		
	launchd 45 pc	anna an	- 1	
	launchd 85 no	1911 0r CHB 3.2 010 297 /dev/ml1	1	
	launchd 85 no	11911 1 PTPR 0x07387518 16384 ->0x07387570		
-				

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.