



## MEGA: A Tool for Mac OS X Operating System and Application Forensics

*By*

**Rob Joyce, Judson Powers, Frank Adelstein**

*Presented At*

The Digital Forensic Research Conference

**DFRWS 2008 USA** Baltimore, MD (Aug 11<sup>th</sup> - 13<sup>th</sup>)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

**<http://dfrws.org>**

# Mac Marshal: A Tool for Mac OS X Operating System and Application Forensics

Rob Joyce, Judson Powers, Frank Adelstein

ATC-NY

A Subsidiary of Architecture Technology Corporation

Digital Forensic Research Workshop

August 12 2008



# The Problem

- ▶ Crime labs see 5-10% Mac OS X systems
  - Market share between 8% (US) and 20-45% (edu)
- ▶ Investigators are ill-equipped to handle OS X
  - Imaging software, low-level file details, etc.
- ▶ Few existing tools gather and analyze higher level OS X-specific forensic data
- ▶ Intel-based OS X systems often run Windows



# Mac Marshal

- ▶ Build a set of simple, command-line OS X tools and a graphical front-end
  - Operate on disk images ('dead' forensics)
  - Live forensics also possible
- ▶ Gather data in a forensically-sound manner (audit logging, hashing results, etc.)
- ▶ Disseminate to LE free of charge



# Benefits

- ▶ Quicker triage of Mac disk images
- ▶ Visibility of OS X-specific evidence that may otherwise be overlooked
  - OS-level features provide a wealth of data that other operating systems do not
  - Smaller forensic labs may not have Mac experts on staff



# Benefits

- ▶ Standardized forensic procedures and report generation
  - Uniform ability to gather evidence
  - Simplifies court acceptance of results
- ▶ Auditable operation via logging and small low-level tools



# Mac Marshal Foundation

- ▶ Use established modules & methods from ATC-NY P2P Marshal™ and OnLineDFS™
- ▶ Use Brian Carrier's SleuthKit for disk image parsing
  - Allows Mac Marshal to read EnCase, FTK, and dd images
  - Revised SleuthKit HFS+ code
- ▶ Plug-in model to add file analysis support (new apps, data-gathering techniques, etc.)

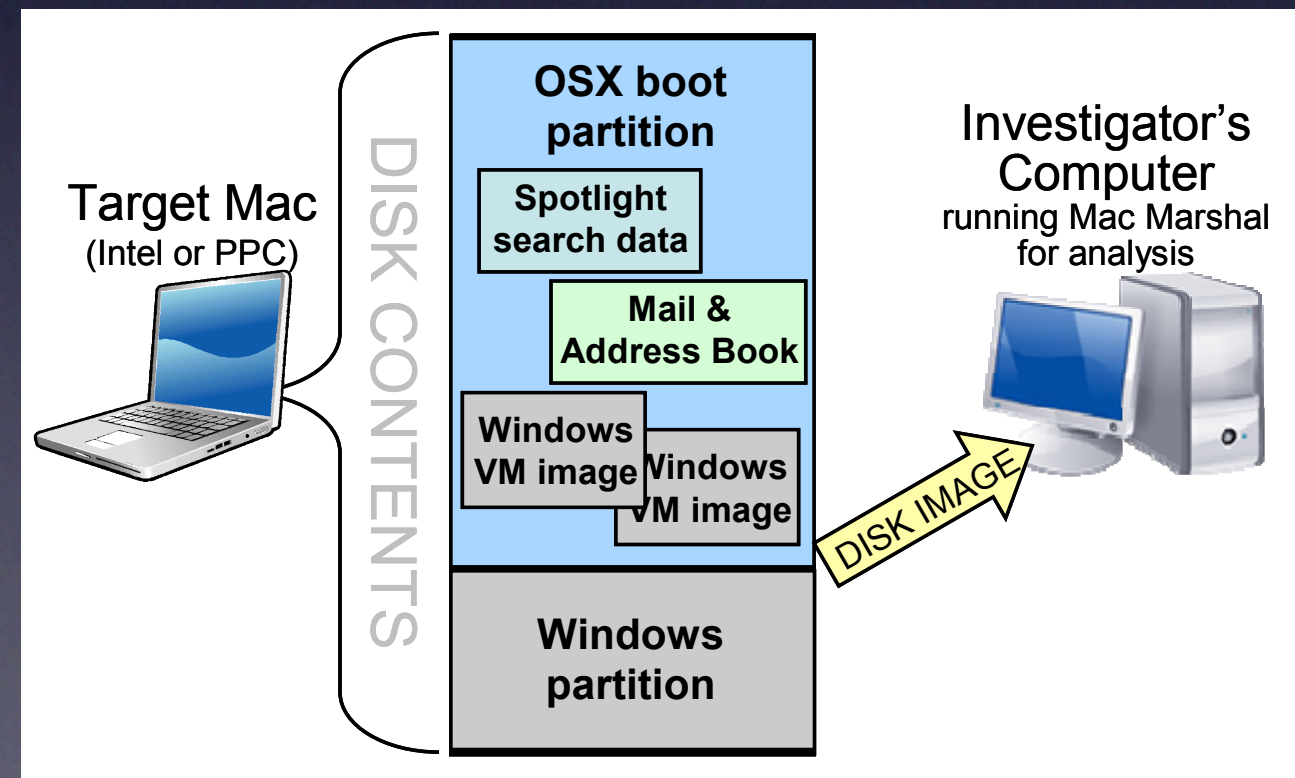


# Triage Step

- ▶ Dual-boot, VM image detection
  - Points investigator to installed OS image(s) on the disk
  - Investigator will then use tools of choice for the relevant operating systems (e.g., a Windows tool for Boot Camp)

- ▶ Encrypted home directories (FileVault)

- Integrate existing tools for rapid testing against a dictionary of potential passwords





# OS X Partition Analysis

Within a particular partition identified during triage, we can analyze:

- ▶ Spotlight search engine data
- ▶ Application-written data



# Spotlight Analysis

- ▶ Spotlight is the file indexing and search engine built in to Mac OS X 10.4 & 10.5
- ▶ Index includes metadata and content of many file types (images, Word docs, e-mail messages, audio/video metadata, appointments, contacts, etc.)
- ▶ For investigators, Spotlight metadata should be treated as advisory—the absence of a file from Spotlight is not exculpatory



# Spotlight Tech Details

- ▶ Spotlight index for a volume is stored at the root of that volume
  - Only the indices for currently-mounted volumes are available
  - Only root can read the index
- ▶ File metadata is searchable even on unindexed volumes
- ▶ Available metadata is based on a file's type “hierarchy” (data → image → JPEG)



# Metadata Fields

- ▶ Common metadata fields include:

  - kMDItemContentType*

  - kMDItemKind*

  - kMDItemURL*

  - kMDItemUsedDates* (list of last access dates)

- ▶ Image files also include:

  - kMDItemAcquisitionMake* (e.g., “NIKON CORPORATION”)

  - kMDItemAcquisitionModel* (e.g., “NIKON D70”)

- ▶ Safari adds:

  - kMDItemWhereFroms* (URL from which file was downloaded)



# Spotlight Searches

- ▶ OS X includes command-line Spotlight utilities

```
mdfind -onlyin /Volumes/Suspect  
"(kMDItemAcquisitionModel == 'NIKON D70') &&  
(kMDItemContentCreationDate >=  
$time.this_year)"
```

- ▶ Mac Marshal includes a command-line utility (spquery) that gives more detailed output
- ▶ Non-indexed volumes can be mounted read-only with a shadow file to allow indexing



# Spotlight in Mac Marshal

The screenshot shows the Mac Marshal application window. At the top, it displays acquisition details: "Acquisition Name/ID: Test Acquisition for DFRWS", "Case #: 1532", "Device Analyzed: /dev/rdisk0", and "Acquisition Storage: /Users/rob/Documents/MEGAtest/TestDfrws.mmacq". A magnifying glass icon is in the top right corner.

Below the acquisition details, there are three tabs: "Disk Triage", "Spotlight" (which is selected), and "Spotlight Images".

On the left side, under "General information", there is a table with the following data:

Type	Disk
Partition map	GPT
Number of partitions	1

Below this, a tree view shows the contents of "Rob's Laptop HD" (148.7 GB, HFS+). The contents include:

- Mac OS X 10.5.4
- Parallels VM image (18.5 GB)
- VMWare VM image (4 GB)
- jimtest.sparseimage (79.1 MB)
- sparseimage (88.1 MB)
- Parallels-Desktop-56...-Mac-en 12-04-46.dmg (88.1 MB)
- Parallels-Desktop-5600-Mac-en.dmg (88.1 MB)
- Parallels-Desktop-5608-Mac-en.dmg (87.9 MB)
- test\_fat.dmg (100 MB)
- test\_ufs.dmg (100 MB)
- DarkSideDVDA.dmg

The main area displays search results for the query "joyce". The "String" radio button is selected. The results table shows 357 results. The selected item is "DFRWS 2008 Agenda".

Name	Relevance	Kind	Size	Modification
Rob Joyce	0.1	Address Book Person Data	1.1 KB	Jul 22, 20
Rob Joyce	0.1	Address Book Person Data	3.4 KB	Jul 22, 20
hfs.c	0.1	C Source File	63.8 KB	Jul 27, 20
DFRWS 2008 Agenda	0.1	Safari history item	7.6 KB	Aug 6, 20
MacMarshalDFRWS	0.1	Keynote Document		Aug 7, 20
Marisa on 2007-11-01 at 18.34	0.553	Chat transcript	4.9 KB	Nov 1, 20
Marisa on 2007-11-02 at 12.55	0.553	Chat transcript	3.7 KB	Nov 2, 20
Marisa on 2007-11-02 at 17.26	0.553	Chat transcript	13.2 KB	Nov 2, 20

Below the search results, the "Selection metadata" section shows 25 attributes for the selected item:

Attribute	Value
FSOwnerUserID	501
FSSize	7777
FSTypeCode	0
Kind	Safari history item
LastUsedDate	Wed, Aug 06, 2008 04:30:29 PM EDT
URL	http://www.dfrws.org/2008/program.shtml
UsedDates	( Wed, Aug 06, 2008 12:00:00 AM EDT )



# OS X Application Data

(current support)

## ▶ Safari (web browser)

- Bookmarks, recent searches, history, cookies, last session
- Cache (files and/or SQLite database)
- ~~Form auto-fill~~ (encrypted via Keychain)

## ▶ iChat (IM client)

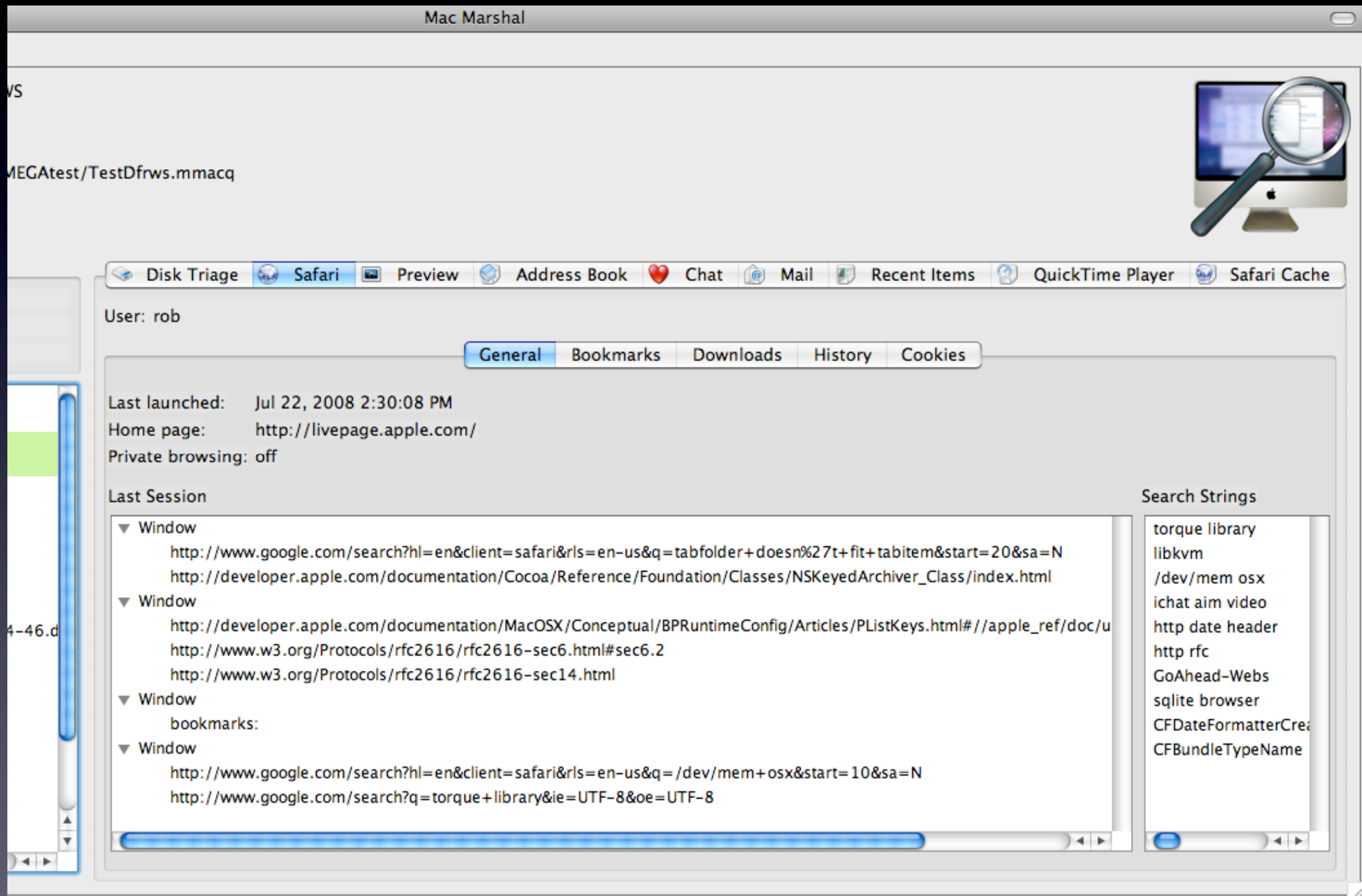
- Buddy lists, chat logs if available

## ▶ Address Book entries

## ▶ Finder recent items



# Mac Marshal App Data





# Future App Data Support

- ▶ Mail: recent addresses, messages
- ▶ iPhoto: metadata, key words, ratings, comments
- ▶ iTunes: serial number for last-connected iPod, iTunes store account
- ▶ iCal: calendar data



# Current Status

- ▶ Development ongoing, funded by National Institute of Justice (NIJ) through July 2009
- ▶ Beta version available shortly (limited audience)
- ▶ Free to law enforcement
- ▶ Version 1 near the end of 2008, training TBD



# Questions?