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 11th - 13th)

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

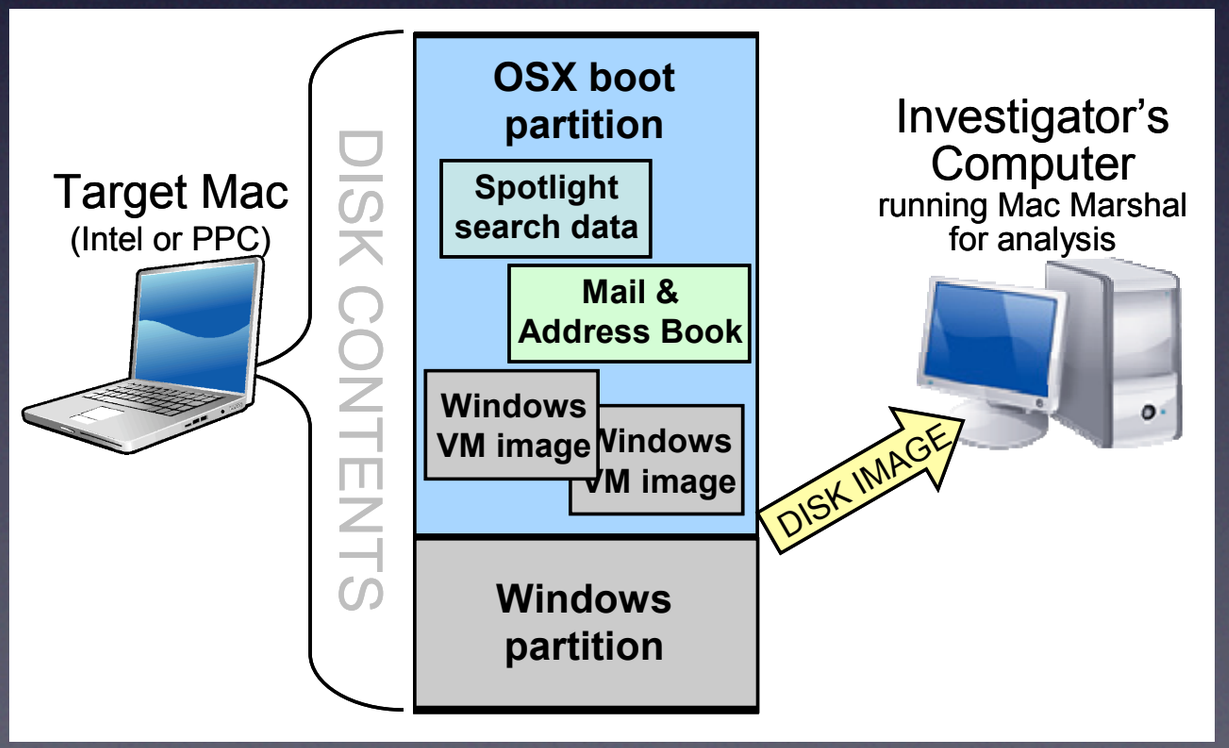
- Standardized forensic procedures and report generation
  - Uniform ability to gather evidence
  - Simplifies court acceptance of results
- Auditable operation via logging and small low-level tools

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 (File Vault)
  - 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)

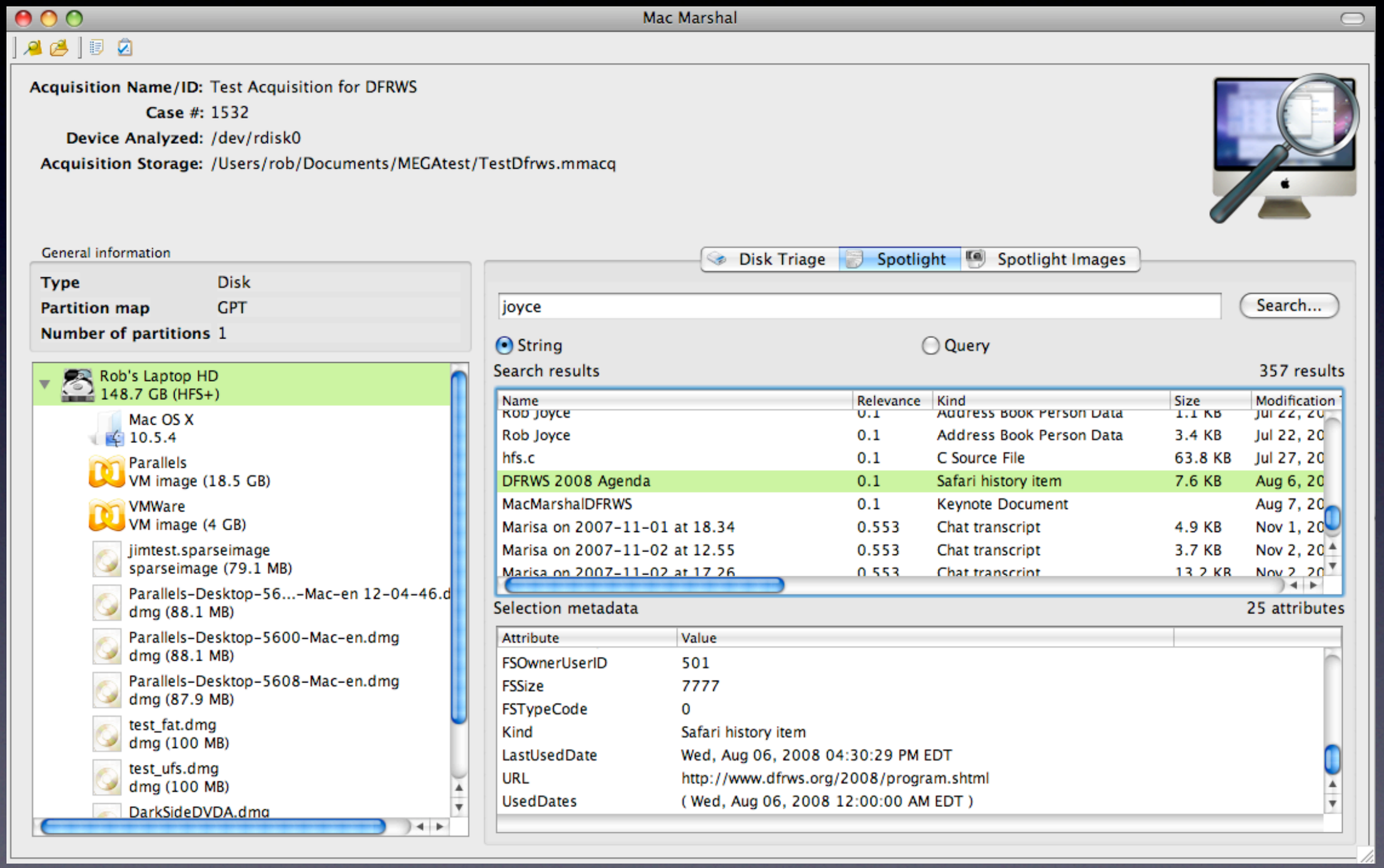
Spotlight Searches

- 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

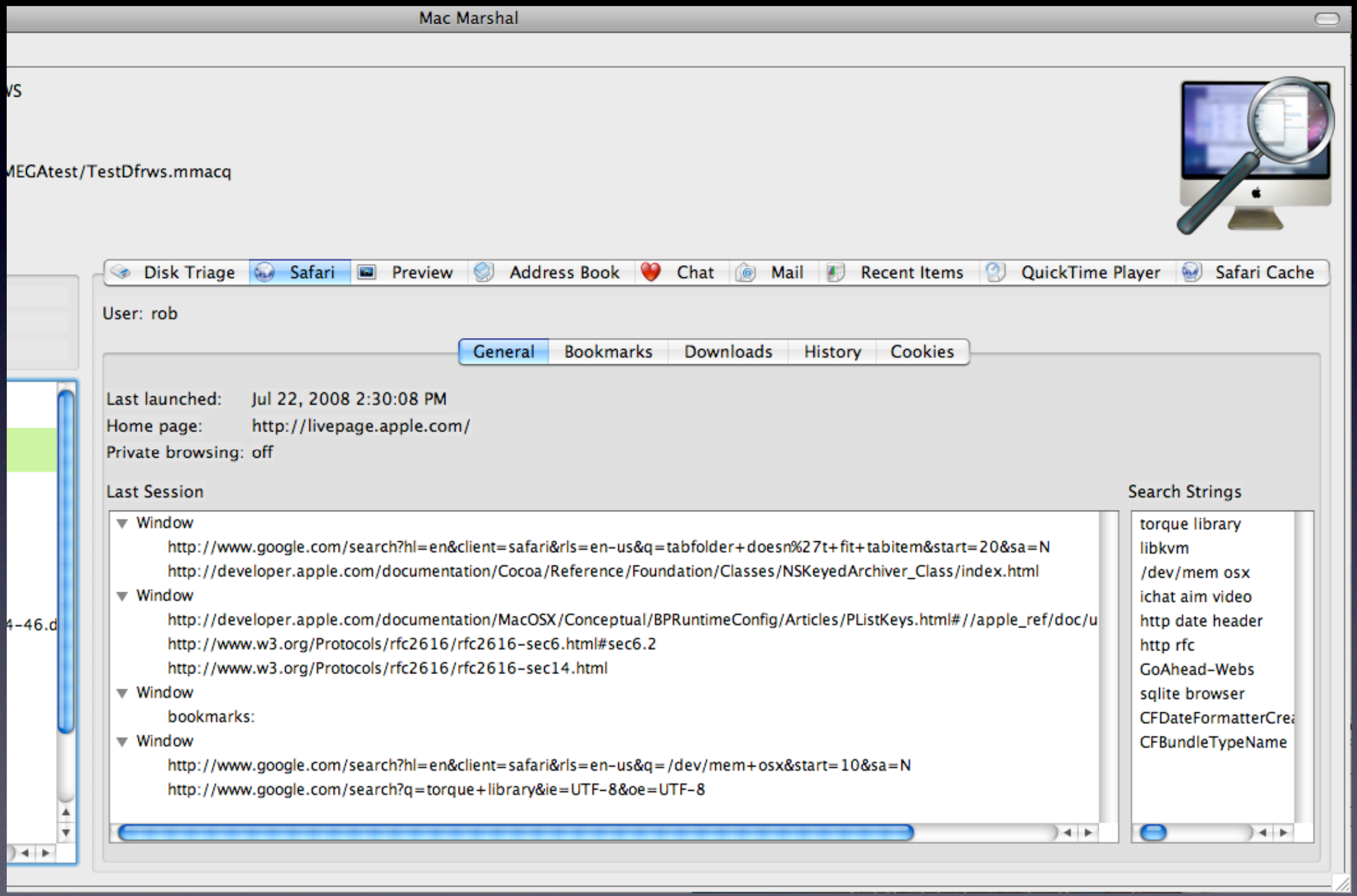
Spotlight in Mac Marshal



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?