One Location to Rule Them All

mac4n6
Artifacts Location

Pasquale Stirparo
SANS DFIR Summit – Prague 2014
$whoami

- Pasquale Stirparo
  - MSc Computer Engineering, Ph.D. candidate at KTH – Royal Institute of Technology

- GCFA, GREM, OPST, OWSE, ECCE

- Mobile Security and Digital Forensics Engineer, Founder @ SefirTech

- Email: pstirparo@gmail.com
- Twitter: @pstirparo
mac4n6

• Officially launched last year... at SANS DFIR Prague 2013 :-)
• What: place for mac4n6 enthusiasts
• Why? Few reasons:
  o I’m an Apple geek
  o Tons of information sources for Windows, much less for OS X
  o Fragmentation of the resources and information:
    • Hundreds of blogs where to look for
    • Many repositories of papers and presentations
    • Several books where to start looking for the location of interesting artifacts

• https://code.google.com/p/mac4n6/
• https://groups.google.com/d/forum/mac4n6
OMG, another DFIR mailinglist???
Artifacts Location: what is this all about?

• Creating one single point of collection for OS X and iOS artifacts location

• Collect information for each artifact, not just a path!

• Main goal: reusable format
  o “machine parsable” and “human readable/writable”
  o reusable by any application, library, etc. (am I too optimistic?)
  o the effort is centralized and made only once
<table>
<thead>
<tr>
<th><strong>Artifact</strong></th>
<th><strong>Name</strong></th>
<th><strong>Labels</strong></th>
<th><strong>Path</strong></th>
<th><strong>Notes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>iCloud</td>
<td>Accounts</td>
<td>Users, applications, cloud, account</td>
<td>/Users/$USERNAME/Library/Application Support/Cloud/Accounts/</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariMainDir</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Safari/*</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariHistory</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Safari/history.sk</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariLastSession</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/SafariLastSession.plist</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariLocalStorage</td>
<td>Users, applications, browsing, db</td>
<td>/Users/$USERNAME/Library/SafariLocalStorage/*</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariLocalStorage</td>
<td>Users, applications, browsing, db</td>
<td>/Users/$USERNAME/Library/SafariLocalStorage/*</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariTopSites</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Safari/TopSites.plist</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariWebpageIcons</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Safari/WebpageIcons.plist</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariCacheDir</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Caches/com.apple.Safari/*</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariCache</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Caches/com.apple.Safari/*</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariCacheExtensions</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Caches/com.apple.Safari/Extensions/*</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariWebPreviews</td>
<td>Users, applications, browsing, img</td>
<td>/Users/$USERNAME/Library/Caches/com.apple.Safari/Webpage Previews/*</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariCookies</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Cookies/Cookies.binarycookies</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariPreferences</td>
<td>Users, applications, browsing, plist</td>
<td>/Users/$USERNAME/Library/Preferences/com.apple.Safari.plist</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariExtensionPreferences</td>
<td>Users, applications, browsing, plist</td>
<td>/Users/$USERNAME/Library/Preferences/com.apple.Safari.Extensions.plist</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariCacheBookmarks</td>
<td>Users, applications, browsing, img</td>
<td>/Users/$USERNAME/Library/Caches/Bookmark/*</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariCacheHistory</td>
<td>Users, applications, browsing, img</td>
<td>/Users/$USERNAME/Library/Caches/Metadata/Safari/Bookmarks/*</td>
<td></td>
</tr>
<tr>
<td>Safari</td>
<td>OSXSafariTemporaryImages</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Caches/com.apple.Safari/*</td>
<td></td>
</tr>
<tr>
<td>Firefox</td>
<td>OSXFirefoxDir</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Application Support/Firefox/*</td>
<td></td>
</tr>
<tr>
<td>Firefox</td>
<td>OSXFirefoxProfiles</td>
<td>Users, applications, browsing</td>
<td>/Users/$USERNAME/Library/Application Support/Firefox/Profiles/*</td>
<td></td>
</tr>
</tbody>
</table>
Artifacts Library

**OSXLaunchDaemons**
- **name**: OSXLaunchDaemons
- **doc**: Launch Daemons files
- **collectors**:
  - **collector_type**: FILE
  - **args**:
    - **path_list**:
      - /Library/LaunchDaemons/*
      - /System/Library/LaunchDaemons/*
- **labels**: [System, plist]
- **supported_os**: [Darwin]

**OSXiOSBackupInfo**
- **name**: OSXiOSBackupInfo
- **doc**: iOS device backup information
- **collectors**:
  - **collector_type**: FILE
  - **args**:
    - **path_list**:
      - /Users/$USERNAME/Library/Application Support/MobileSync/Backup/$BACKUP_FOLDER/info.plist
- **labels**: [Users, ios, backup, plist]
- **supported_os**: [Darwin]
Mac OS X 10.9 - Artifacts Location

Contents [hide]

1 SYSTEM ARTIFACTS
   1.1 Autorun Locations
   1.2 System Logs
   1.3 System Preferences
   1.4 System Settings and Information
   1.5 Sleep/Hibernate and Swap Image File
   1.6 Kernel Extension
   1.7 Software Installation
   1.8 System Info Misc.

2 USER ARTIFACTS
   2.1 Autorun Locations
   2.2 Users
   2.3 User Directories
   2.4 Preferences
   2.5 Logs
   2.6 iDevice Backup
   2.7 Preferences

3 APPLICATIONS ARTIFACTS
   3.1 iCloud
   3.2 Skype
   3.3 Safari
   3.4 Firefox
   3.5 Google Chrome
   3.6 Mail
   3.7 Misc.
   3.8 Networking

4 External Links
Audit Log

/private/var/audit/*

Installation log

It contains install date of system, as well as date of system and software updates

/private/var/log/install.log

System Preferences

System Preferences files

/Library/Preferences/*

Global Preferences

It contains Global Preferences information such as the local time zone, geographical coordinates, etc.

/Library/Preferences/.GlobalPreferences.plist

Software Update

Plst describing last attempt and last successful attempt at updating OS X software

/Library/Preferences/com.apple.SoftwareUpdate.plist
Current sources

- GRR “Darwin” Artifacts
- Plaso
- OSX Auditor
- OSX Collector
- Pac4Mac
- Related blog posts and... some of my own juice

Current numbers:
- 72 unique iOS artifacts
- 110 unique “verified” OS X 10.9 artifacts locations
- Hundred more almost ready to be released, stay tuned!!!
I Want You
One Location to Rule Them All... thank you