

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:
 - I'm an Apple geek
 - Tons of information sources for Windows, much less for OS X
 - 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
 - “machine parsable” and “human readable/writable”
 - reusable by any application, library, etc. (am I too optimistic?)
 - the effort is centralized and made only once

Mac OS X Forensics Artifacts v0.1

File Edit View Insert Format Data Tools Help All changes saved in Drive

1 other viewer

Comments

Share

Mac OS X Forensics Artifacts v0.1

10 Arial 123 % \$

It

	A	B	C	D	
79	APPLICATIONS ARTIFACTS				
80	Artifact	Name	Labels	Path	Notes
81	iCloud				
82	iCloud Accounts	Accounts	Users, applications, cloud, account	/Users/\$USERNAME/Library/Application Support/iCloud/Accounts/	
83					
84	Skype				
85	Skype Directory	OSXSkypeMainDir	Users, applications, IM	/Users/\$USERNAME/Library/Application Support/Skype/*	Directory containing Skype use
86	Skype User profile	OSXSkypeUserProfile	Users, applications, IM	/Users/\$USERNAME/Library/Application Support/Skype/\$SKYPE_USERNAME/*	Directory containing Skype use
87	Skype Preferences and Recent Searches	OSXSkypePreferences	Users, applications, IM, plist	/Users/\$USERNAME/Library/Preferences/com.skype.skype.plist	Skype preferences and recent
88	Main Skype database	OSXSkypeDb	Users, applications, IM, db	/Users/\$USERNAME/Library/Application Support/Skype/\$SKYPE_USERNAME/Main.d	Database of contacts, SMS's, c
89	Chat Sync Directory	OSXSkypechatsync	Users, applications, IM	/Users/\$USERNAME/Library/Application Support/Skype/\$SKYPE_USERNAME/chatsyr	Directory containing chat logs
90					
91	Safari				
92	Safari Main Folder	OSXSafariMainDir	Users, applications, browsing	/Users/\$USERNAME/Library/Safari/*	
93	Safari Bookmarks	OSXSafariBookmarks	Users, applications, browsing, plist	/Users/\$USERNAME/Library/Safari/Bookmarks.plist	Plist listing default and user-ad
94	Safari Downloads	OSXSafariDownloads	Users, applications, browsing, plist	/Users/\$USERNAME/Library/Safari/Downloads.plist	Plist listing files downloaded us
95	Safari Installed Extensions	OSXSafariExtensions	Users, applications, browsing, plist	/Users/\$USERNAME/Library/Safari/Extensions/Extensions.plist	Plist describing installed Safari
96	"	"	Users, applications, browsing	/Users/\$USERNAME/Library/Safari/Extensions/*	Directory of Safari Extensions.
97	Safari History	OSXSafariHistory	Users, applications, browsing, plist	/Users/\$USERNAME/Library/Safari/History.plist	Plist listing Safari web browsing
98	Safari History Index	OSXSafariHistoryIndex	Users, applications, browsing	/Users/\$USERNAME/Library/Safari/HistoryIndex.sk	An index of Safari History allow
99	Safari Last Session	OSXSafariLastSession	Users, applications, browsing, plist	/Users/\$USERNAME/Library/Safari/LastSession.plist	A plist describing the state of S
100	Safari Local Storage Directory	OSXSafariLocalStorage	Users, applications, browsing, db	/Users/\$USERNAME/Library/Safari/LocalStorage/*	A directory for webpage-specifi
101	Safari Local Storage Database	OSXSafariStorageTracker	Users, applications, browsing, db	/Users/\$USERNAME/Library/Safari/LocalStorage/StorageTracker.db	A database listing the webpage
102	Safari Top Sites	OSXSafariTopSites	Users, applications, browsing, plist	/Users/\$USERNAME/Library/Safari/TopSites.plist	A Plist listing the webpages bel
103	Safari Webpage Icons Database	OSXSafariWebpagelcons	Users, applications, browsing, db	/Users/\$USERNAME/Library/Safari/Webpagelcons.db	A database containing saved w
104	Safari Cache Directory	OSXSafariCacheDir	Users, applications, browsing	/Users/\$USERNAME/Library/Caches/com.apple.Safari/*	A directory containing Safari-sp
105	Safari Cache	OSXSafariCache	Users, applications, browsing, db	/Users/\$USERNAME/Library/Caches/com.apple.Safari/Cache.db	A cache of data from visited we
106	Safari Extensions Cache	OSXSafariCacheExtensions	Users, applications, browsing	/Users/\$USERNAME/Library/Caches/com.apple.Safari/Extensions/*	A directory containing cached i
107	Safari Webpage Previews	OSXSafariWebPreviews	Users, applications, browsing, img	/Users/\$USERNAME/Library/Caches/com.apple.Safari/Webpage Previews/*	A directory containing images c
108	Safari Cookies	OSXSafariCookies	Users, applications, browsing	/Users/\$USERNAME/Library/Cookies/Cookies.binarycookies	Cookies from visited webpages
109	Safari Preferences and Search terms	OSXSafariPreferences	Users, applications, browsing, plist	/Users/\$USERNAME/Library/Preferences/com.apple.Safari.plist	Contains recent safari search s
110	Safari Extension Preferences	OSXSafariExtPreferences	Users, applications, browsing, plist	/Users/\$USERNAME/Library/Preferences/com.apple.Safari.Extensions.plist	Contains preferences of Safari
111	Safari Bookmark Cache	OSXSafariCacheBookmarks	Users, applications, browsing, img	/Users/\$USERNAME/Library/Caches/Metadata/Safari/Bookmarks/*	Each bookmark entry in Bookm
112	Safari History Cache	OSXSafariCacheHistory	Users, applications, browsing, img	/Users/\$USERNAME/Library/Caches/Metadata/Safari/History/*	Each website entry in History.p
113	Safari Temporary Images	OSXSafariTempImg	Users, applications, browsing, img	/Users/\$USERNAME/Library/Caches/com.apple.Safari/fsCachedData/*	It contains the images present/
114					
115	Firefox				
116	Firefox Directory	OSXFirefoxDir	Users, applications, browsing	/Users/\$USERNAME/Library/Application Support/Firefox/*	Directory containing user artifa
117	Firefox Profiles	OSXFirefoxProfiles	Users, applications, browsing	/Users/\$USERNAME/Library/Application Support/Firefox/Profiles/*	

[10.6] Snow Leopard [10.7] Lion [10.8] Mountain Lion [10.9] Mavericks [10.9] All-in-one

Artifacts Library


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

```
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]
```

Forensicswiki

Mac OS X 10.9 – Artifacts

forensicswiki.org/wiki/Mac_OS_X_10.9_-_Artifacts_Location



[Main Page](#)
[Categories](#)

▼ About
forensicswiki.org:
[Recent changes](#)
[Random page](#)

► [Tools](#)

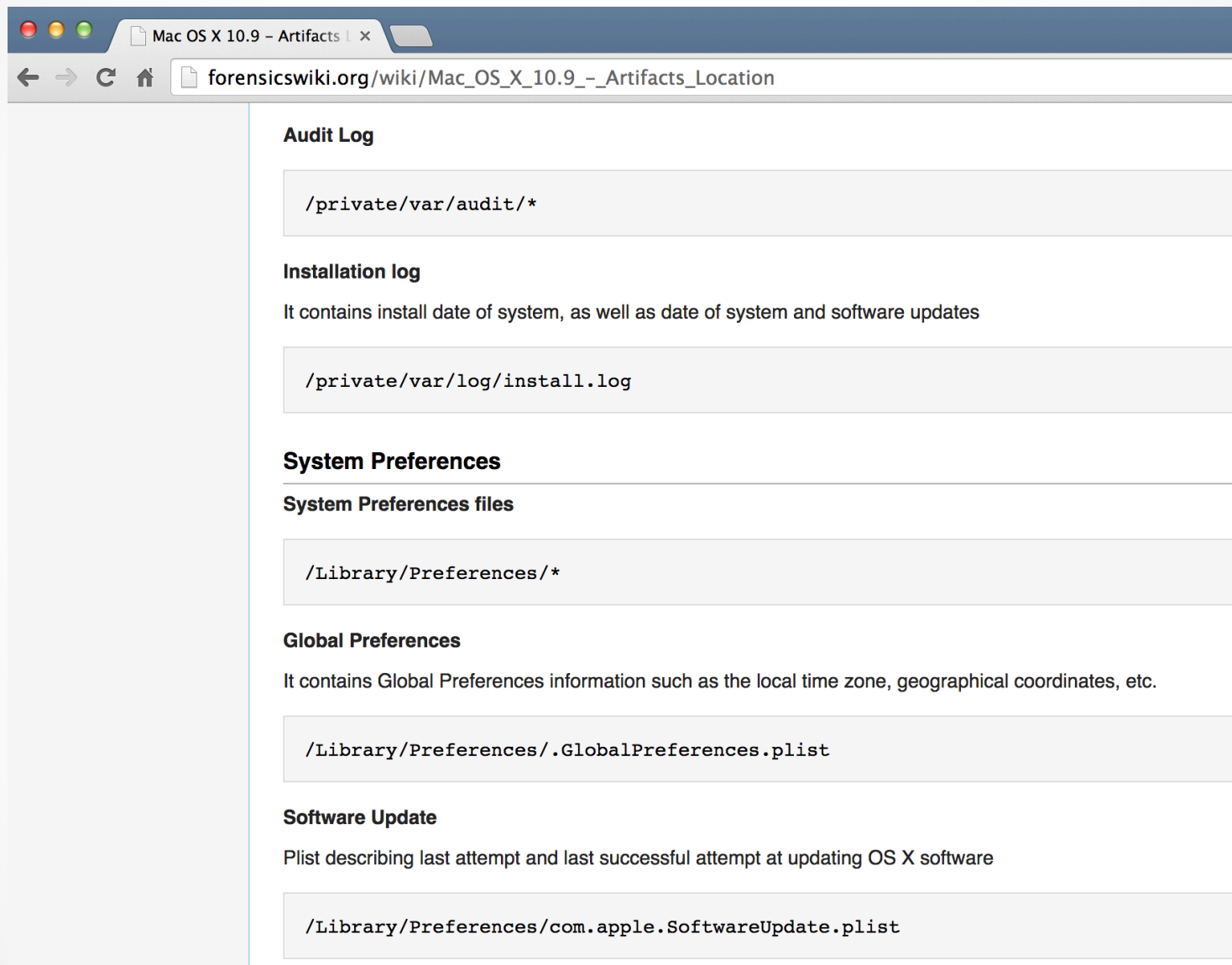
Page [Discussion](#)

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 Informations](#)
 - [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**

Forensicswiki



Current sources

- GRR “Darwin” Artifacts
- Plaso
- OSXAuditor
- OSXCollector
- 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

