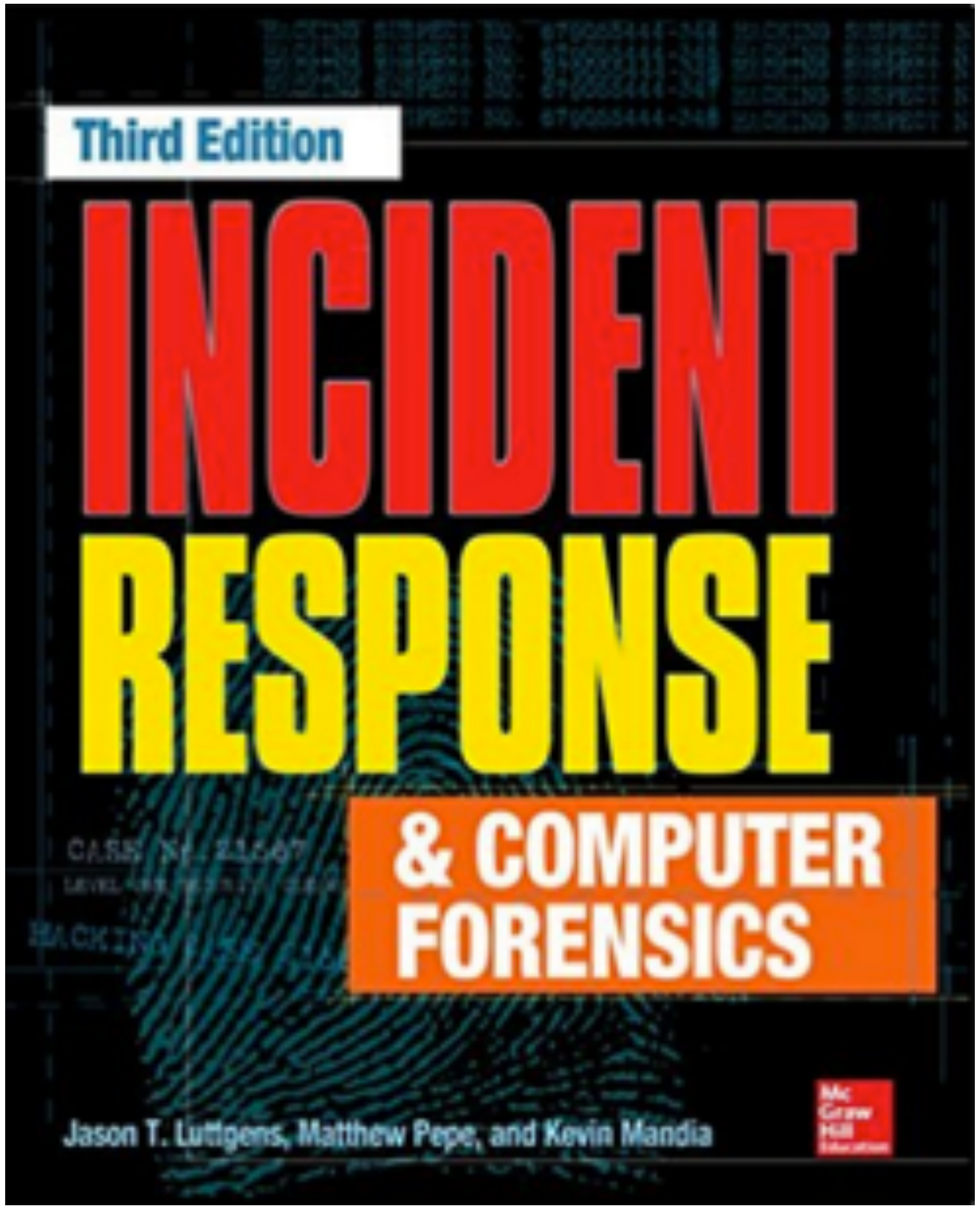
CNIT 121: Computer Forensics



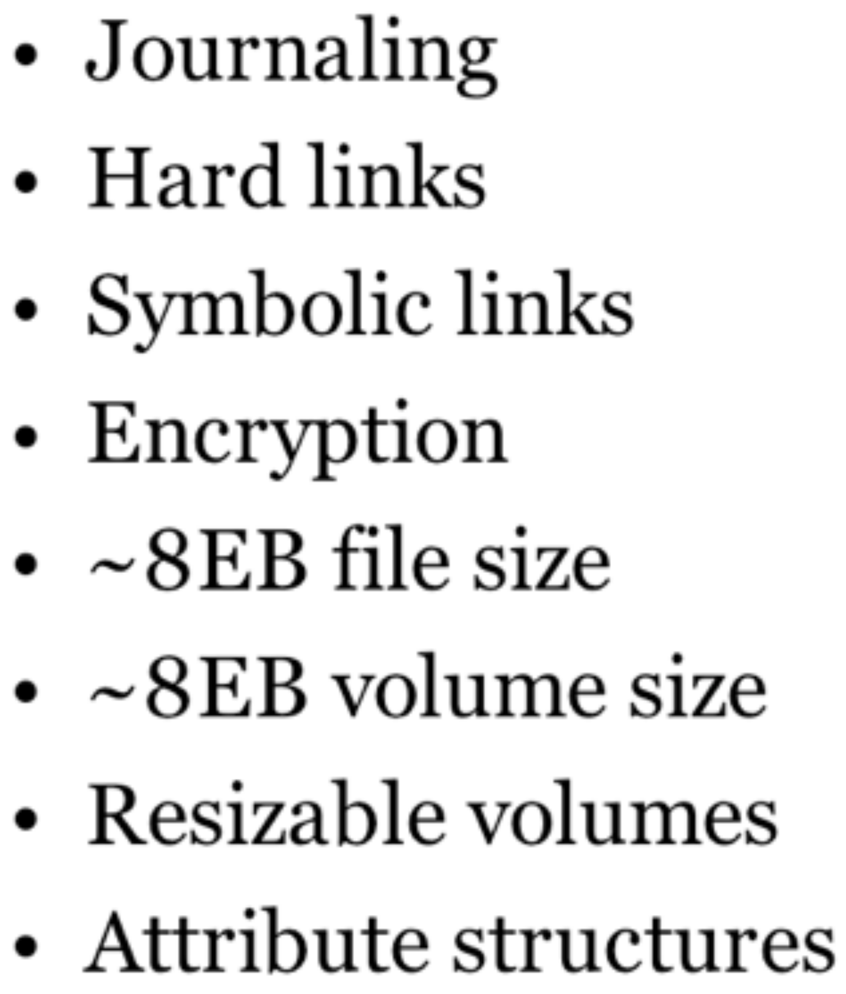
13 Investigating Mac OS X Systems

Topics

- The HFS+ file system
- Core operating system data
- Spotlight data
- System and application logging
- Application and system configuration

HFS+ and File System Analysis

- **Hierarchical File System features:**



- Journaling
- Hard links
- Symbolic links
- Encryption
- ~8EB file size
- ~8EB volume size
- Resizable volumes
- Attribute structures

Nine Structures

1. **Boot blocks**
2. **Volume header**
3. **Allocation file**
4. **Extents overflow file**
5. **Catalog file**
6. **Attributes file**
7. **Startup file**
8. **Alternate volume header**
9. **Reserved blocks**

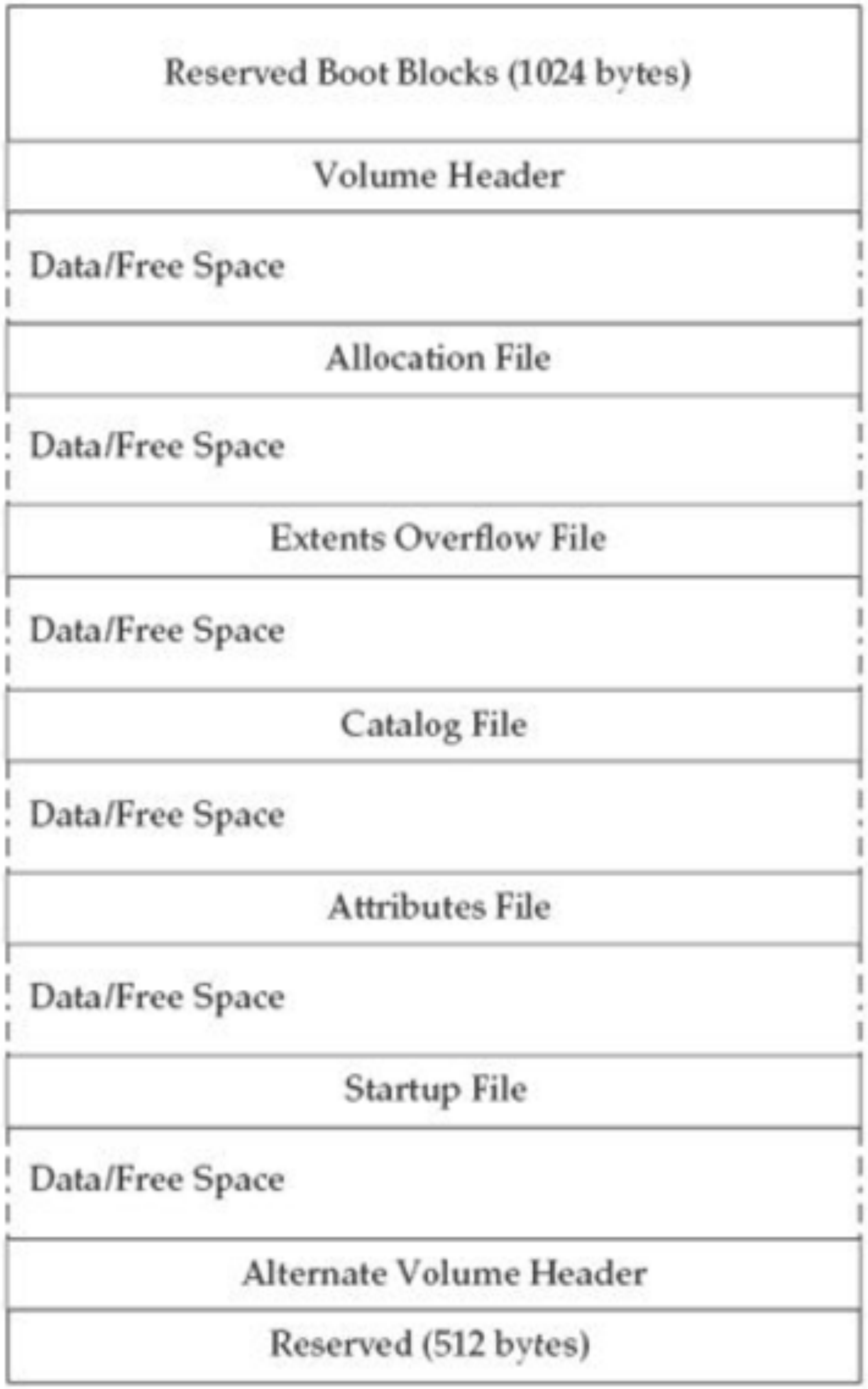
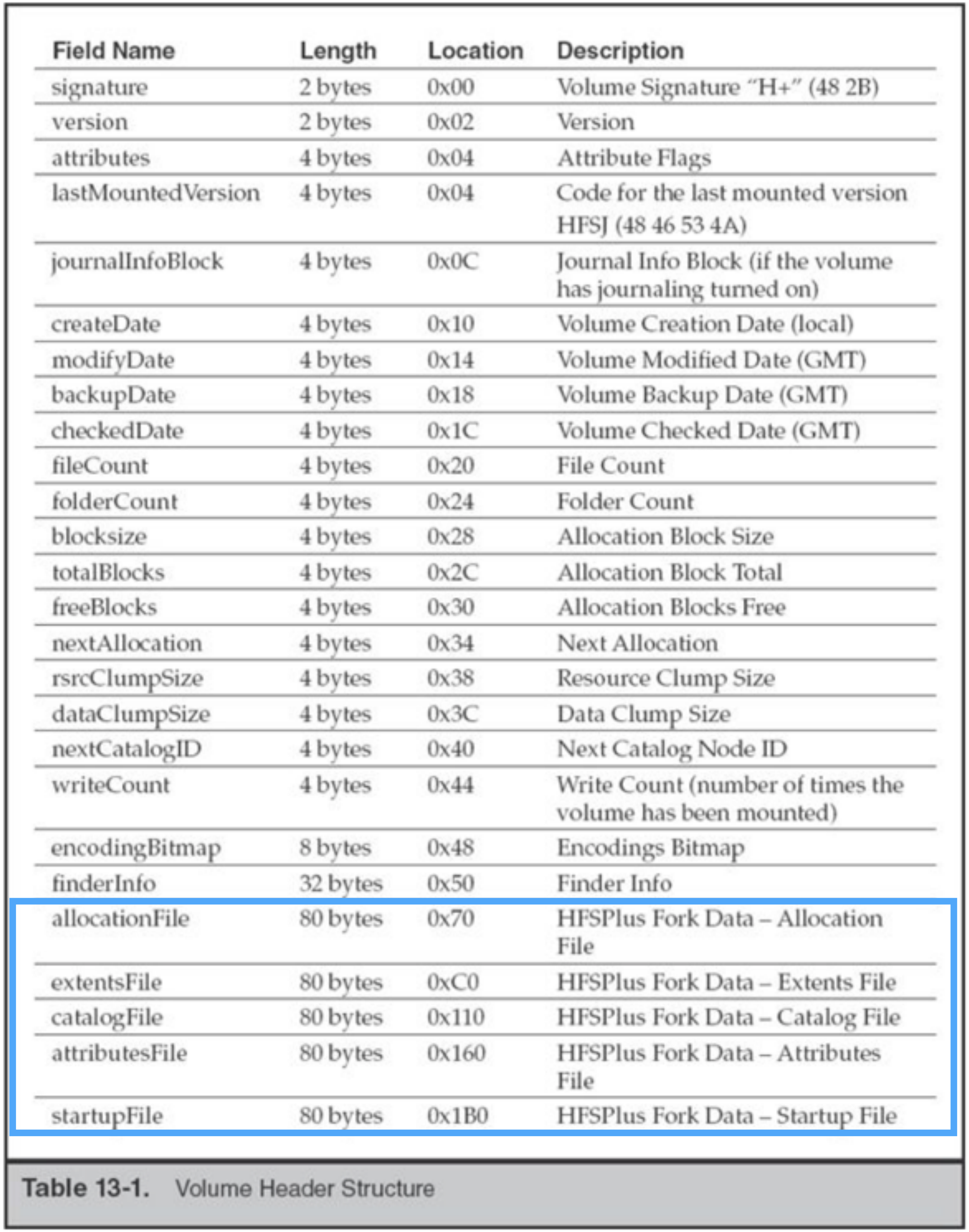


Figure 13-1. Anatomy of a disk

Nine Structures

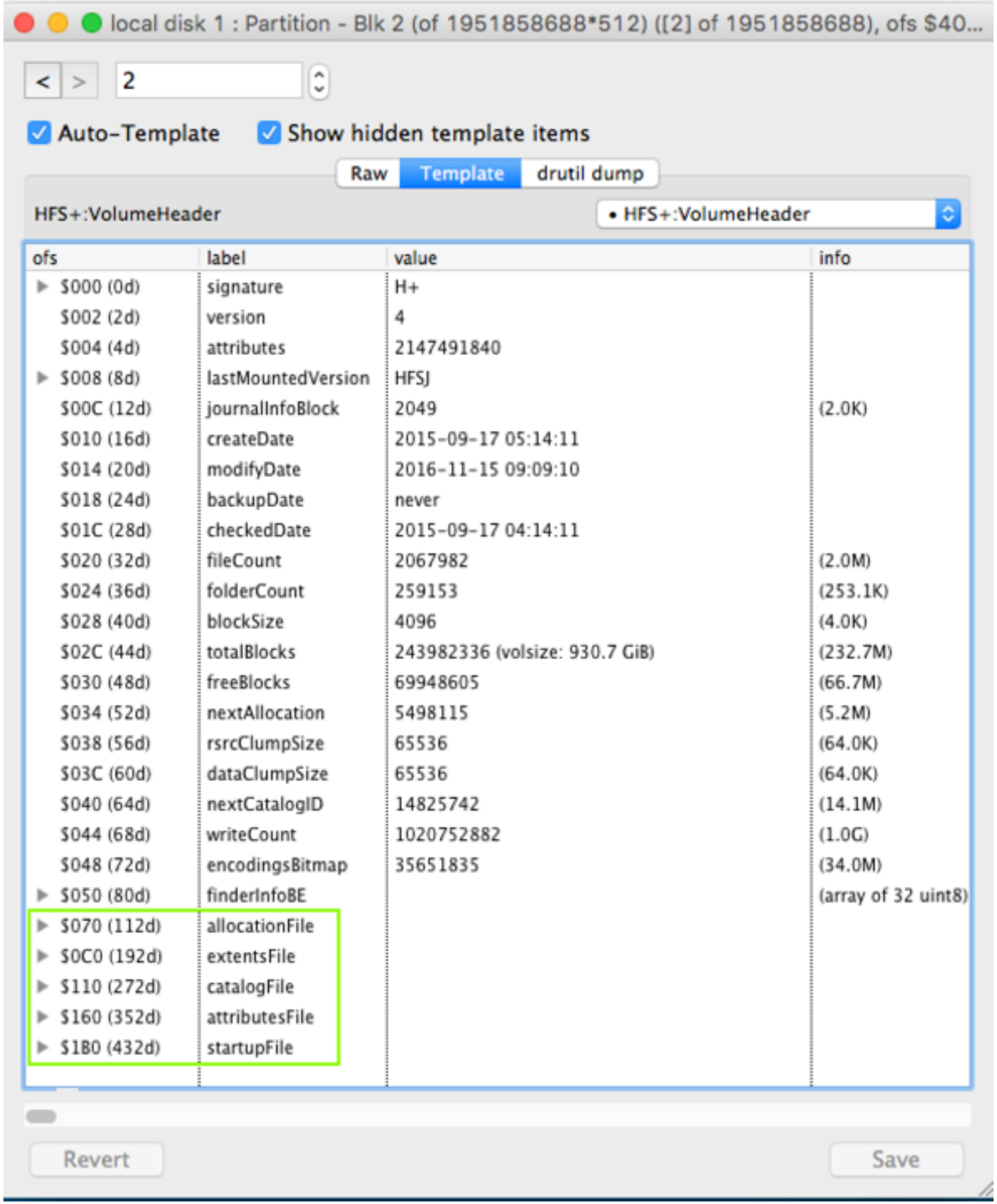
1. **Boot blocks**
   - **First 1024 bytes of volume**
   - **Typically empty on modern systems**
2. **Volume Header and Alternate Volume Header**
   - **Located 1024 bytes from the beginning of the volume**
   - **Information about the volume, including the location of other structures**



Field Name	Length	Location	Description
signature	2 bytes	0x00	Volume Signature "H+" (48 2B)
version	2 bytes	0x02	Version
attributes	4 bytes	0x04	Attribute Flags
lastMountedVersion	4 bytes	0x04	Code for the last mounted version HFSJ (48 46 53 4A)
journalInfoBlock	4 bytes	0x0C	Journal Info Block (if the volume has journaling turned on)
createDate	4 bytes	0x10	Volume Creation Date (local)
modifyDate	4 bytes	0x14	Volume Modified Date (GMT)
backupDate	4 bytes	0x18	Volume Backup Date (GMT)
checkedDate	4 bytes	0x1C	Volume Checked Date (GMT)
fileCount	4 bytes	0x20	File Count
folderCount	4 bytes	0x24	Folder Count
blocksize	4 bytes	0x28	Allocation Block Size
totalBlocks	4 bytes	0x2C	Allocation Block Total
freeBlocks	4 bytes	0x30	Allocation Blocks Free
nextAllocation	4 bytes	0x34	Next Allocation
rsrcClumpSize	4 bytes	0x38	Resource Clump Size
dataClumpSize	4 bytes	0x3C	Data Clump Size
nextCatalogID	4 bytes	0x40	Next Catalog Node ID
writeCount	4 bytes	0x44	Write Count (number of times the volume has been mounted)
encodingBitmap	8 bytes	0x48	Encodings Bitmap
finderInfo	32 bytes	0x50	Finder Info
allocationFile	80 bytes	0x70	HFSPlus Fork Data – Allocation File
extentsFile	80 bytes	0xC0	HFSPlus Fork Data – Extents File
catalogFile	80 bytes	0x110	HFSPlus Fork Data – Catalog File
attributesFile	80 bytes	0x160	HFSPlus Fork Data – Attributes File
startupFile	80 bytes	0x1B0	HFSPlus Fork Data – Startup File

Table 13-1. Volume Header Structure

iBored
Disk Editor
for
Mac


local disk 1 : Partition - Blk 2 (of 1951858688*512) ([2] of 1951858688), ofs $40...
<
>
2
Raw
Template
drutil dump
Revert
Save

☑ Auto-Template ☑ Show hidden template items

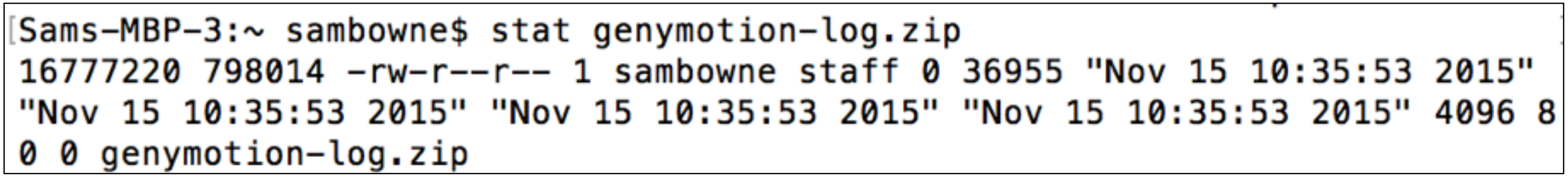
HFS+:VolumeHeader • HFS+:VolumeHeader

ofs	label	value	info
▶ $000 (0d)	signature	H+	
$002 (2d)	version	4	
$004 (4d)	attributes	2147491840	
▶ $008 (8d)	lastMountedVersion	HFSJ	
$00C (12d)	journalInfoBlock	2049	(2.0K)
$010 (16d)	createDate	2015-09-17 05:14:11	
$014 (20d)	modifyDate	2016-11-15 09:09:10	
$018 (24d)	backupDate	never	
$01C (28d)	checkedDate	2015-09-17 04:14:11	
$020 (32d)	fileCount	2067982	(2.0M)
$024 (36d)	folderCount	259153	(253.1K)
$028 (40d)	blockSize	4096	(4.0K)
$02C (44d)	totalBlocks	243982336 (volsize: 930.7 GiB)	(232.7M)
$030 (48d)	freeBlocks	69948605	(66.7M)
$034 (52d)	nextAllocation	5498115	(5.2M)
$038 (56d)	rsrcClumpSize	65536	(64.0K)
$03C (60d)	dataClumpSize	65536	(64.0K)
$040 (64d)	nextCatalogID	14825742	(14.1M)
$044 (68d)	writeCount	1020752882	(1.0G)
$048 (72d)	encodingsBitmap	35651835	(34.0M)
▶ $050 (80d)	finderInfoBE		(array of 32 uint8)
▶ $070 (112d)	allocationFile		
▶ $0C0 (192d)	extentsFile		
▶ $110 (272d)	catalogFile		
▶ $160 (352d)	attributesFile		
▶ $1B0 (432d)	startupFile		

Mac Timestamps

- **All in local time**
- **HFS+ Volume**
  - **Create date, modify date, backup date, checked date**
- **File**
  - **Access, modify, inode change, inode birth time (file creation)**

Stat Command

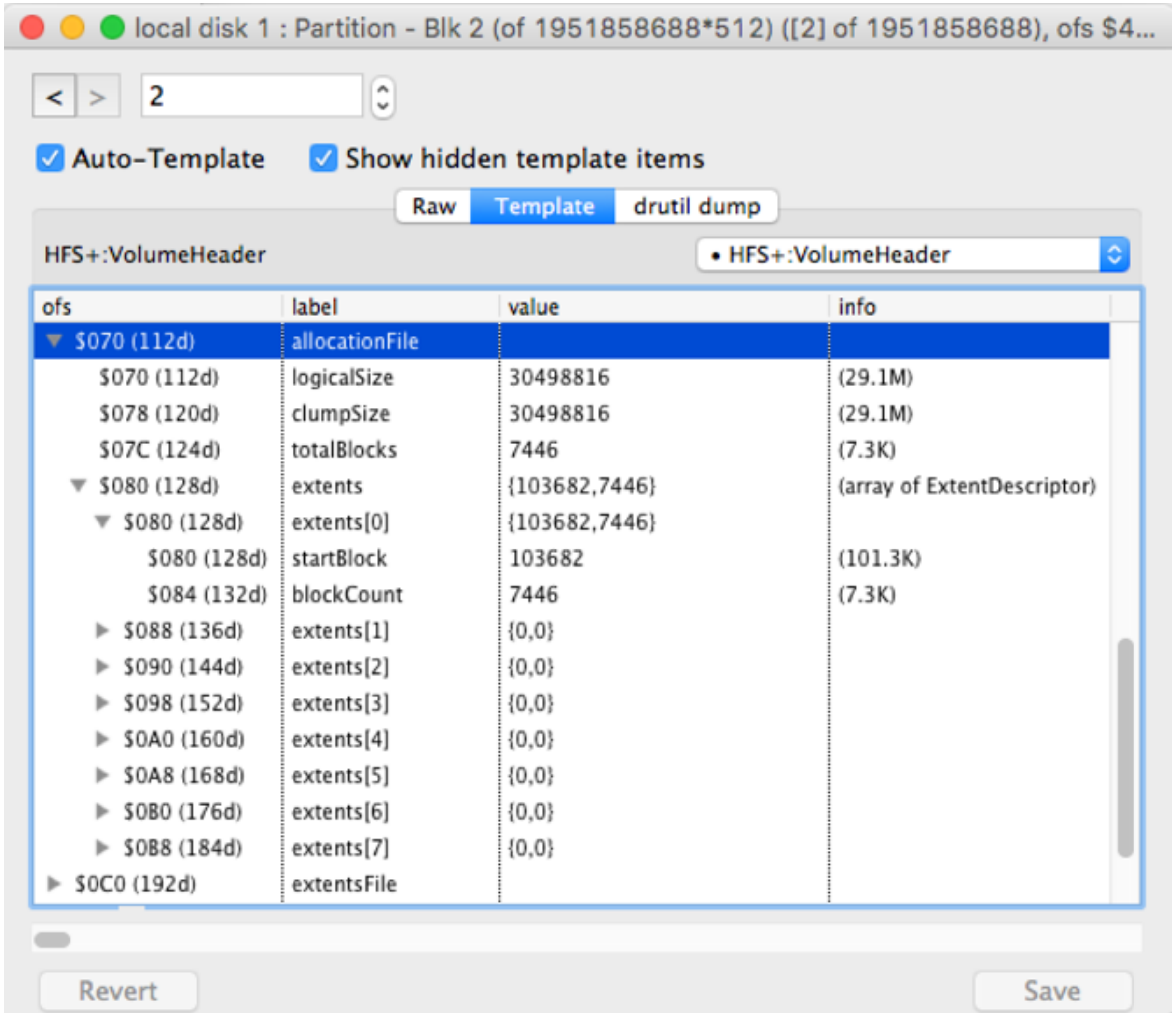


```
[Sams-MBP-3:~ sambowne$ stat genymotion-log.zip
16777220 798014 -rw-r--r-- 1 sambowne staff 0 36955 "Nov 15 10:35:53 2015"
"Nov 15 10:35:53 2015" "Nov 15 10:35:53 2015" "Nov 15 10:35:53 2015" 4096 8
0 0 genymotion-log.zip
```

- **Shows all four timestamps on Mac**

Allocation File

- **A bit for every block**
- **1 = in use**
- **0 = available**



local disk 1 : Partition - Blk 2 (of 1951858688*512) ([2] of 1951858688), ofs $4...

2

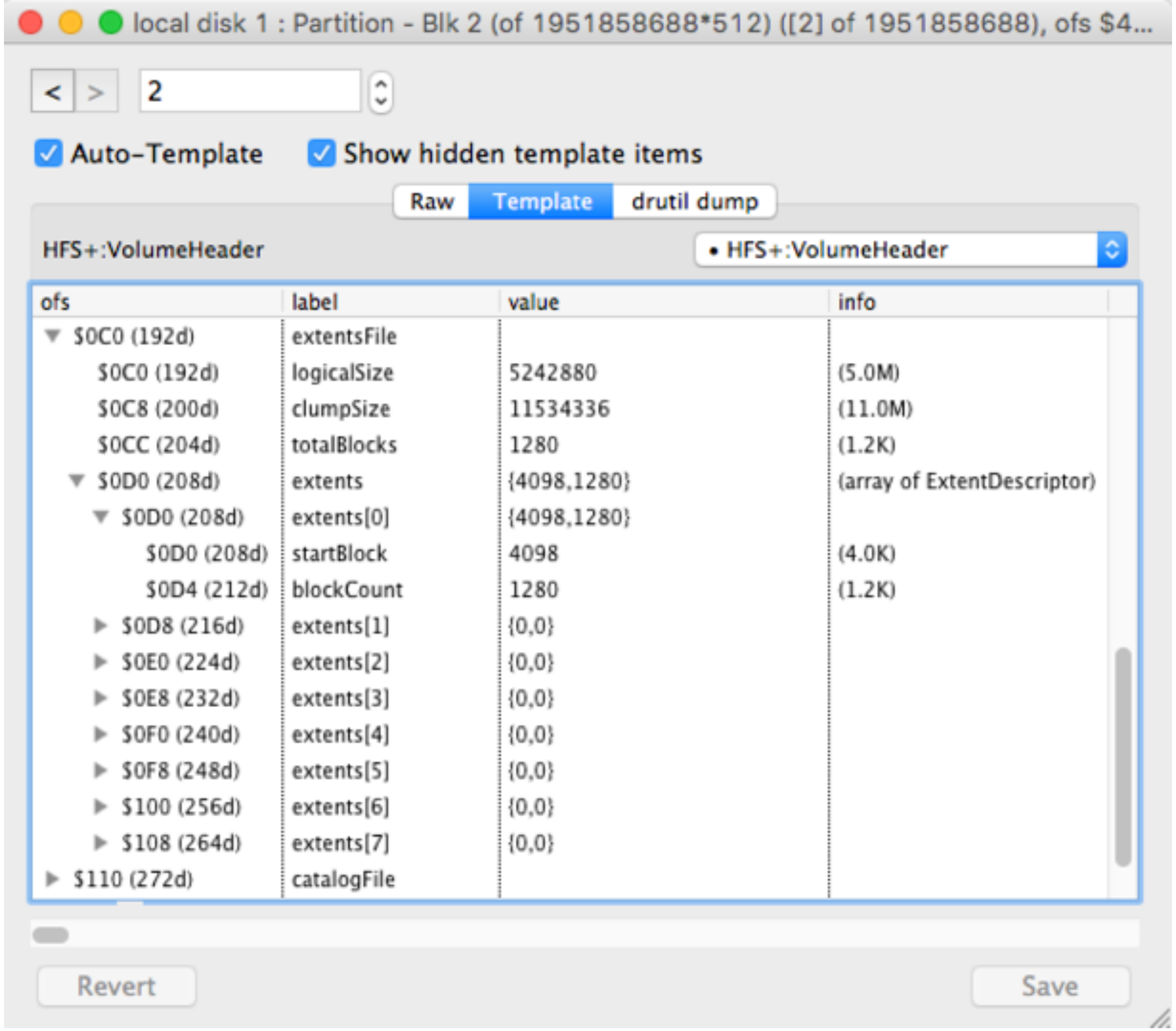
☑ Auto-Template ☑ Show hidden template items

HFS+:VolumeHeader

ofs	label	value	info
▼ $070 (112d)	allocationFile		
$070 (112d)	logicalSize	30498816	(29.1M)
$078 (120d)	clumpSize	30498816	(29.1M)
$07C (124d)	totalBlocks	7446	(7.3K)
▼ $080 (128d)	extents	{103682,7446}	(array of ExtentDescriptor)
▼ $080 (128d)	extents[0]	{103682,7446}	
$080 (128d)	startBlock	103682	(101.3K)
$084 (132d)	blockCount	7446	(7.3K)
▶ $088 (136d)	extents[1]	{0,0}	
▶ $090 (144d)	extents[2]	{0,0}	
▶ $098 (152d)	extents[3]	{0,0}	
▶ $0A0 (160d)	extents[4]	{0,0}	
▶ $0A8 (168d)	extents[5]	{0,0}	
▶ $0B0 (176d)	extents[6]	{0,0}	
▶ $0B8 (184d)	extents[7]	{0,0}	
▶ $0C0 (192d)	extentsFile		

Extents Overflow File

- **"Extents" are contiguous allocation blocks**



local disk 1 : Partition - Blk 2 (of 1951858688*512) ([2] of 1951858688), ofs $4...

2

☑ Auto-Template ☑ Show hidden template items

HFS+:VolumeHeader

• HFS+:VolumeHeader

ofs	label	value	info
▼ $0C0 (192d)	extentsFile		
$0C0 (192d)	logicalSize	5242880	(5.0M)
$0C8 (200d)	clumpSize	11534336	(11.0M)
$0CC (204d)	totalBlocks	1280	(1.2K)
▼ $0D0 (208d)	extents	{4098,1280}	(array of ExtentDescriptor)
▼ $0D0 (208d)	extents[0]	{4098,1280}	
$0D0 (208d)	startBlock	4098	(4.0K)
$0D4 (212d)	blockCount	1280	(1.2K)
▶ $0D8 (216d)	extents[1]	{0,0}	
▶ $0E0 (224d)	extents[2]	{0,0}	
▶ $0E8 (232d)	extents[3]	{0,0}	
▶ $0F0 (240d)	extents[4]	{0,0}	
▶ $0F8 (248d)	extents[5]	{0,0}	
▶ $100 (256d)	extents[6]	{0,0}	
▶ $108 (264d)	extents[7]	{0,0}	
▶ $110 (272d)	catalogFile		

Catalog File

- **Details hierarchy of files and folders in the system**
- **Each file and folder has a unique catalog node ID (CNID)**

Attributes File

- **Optional**
- **Used for *named forks***
  - **Additional metadata assigned to a file**
  - **Like Microsoft's Alternate Data Streams**
- **Stores origin of files from the Internet, and tags like "Green" and "Important"**

Startup File

- **Not used by Mac OS X**
- **Usually empty**

File System Services

- **Spotlight**
- **Managed Storage**

Spotlight

- **Metadata indexing and searching service**

- **Indexers examine the content of files to find keywords**

    - **Some index entire content, others only import metadata**

Spotlight

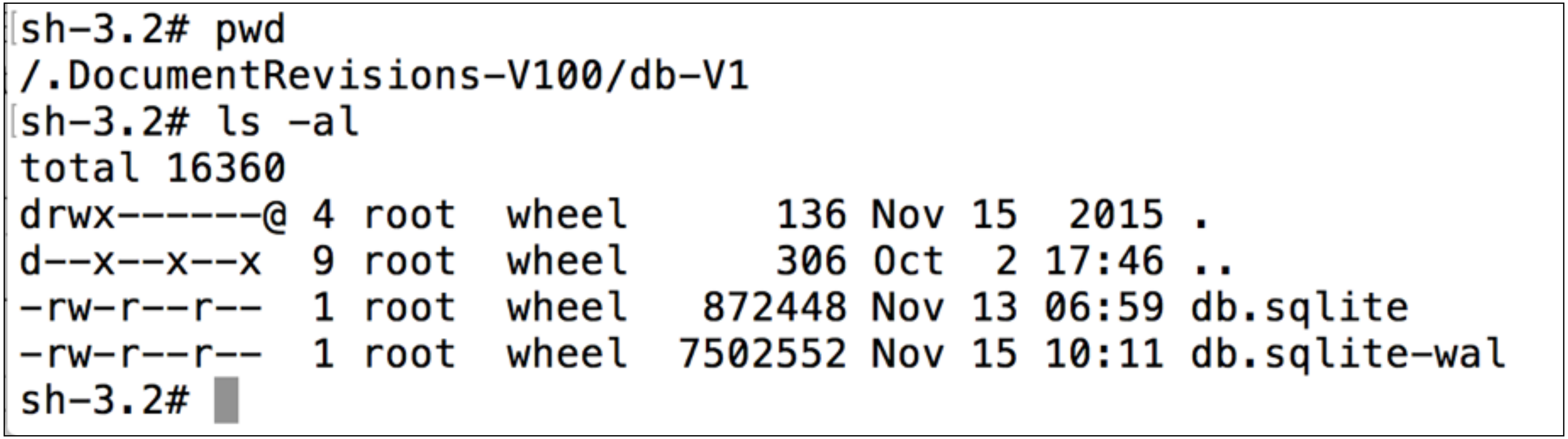
- Can be used to search a live system
- Not much use for a static acquisition
  - Indexes are deleted when a file is deleted
  - No tools are available to parse the data stored by the Spotlight indexer once it's extracted from a drive image

Managed Storage

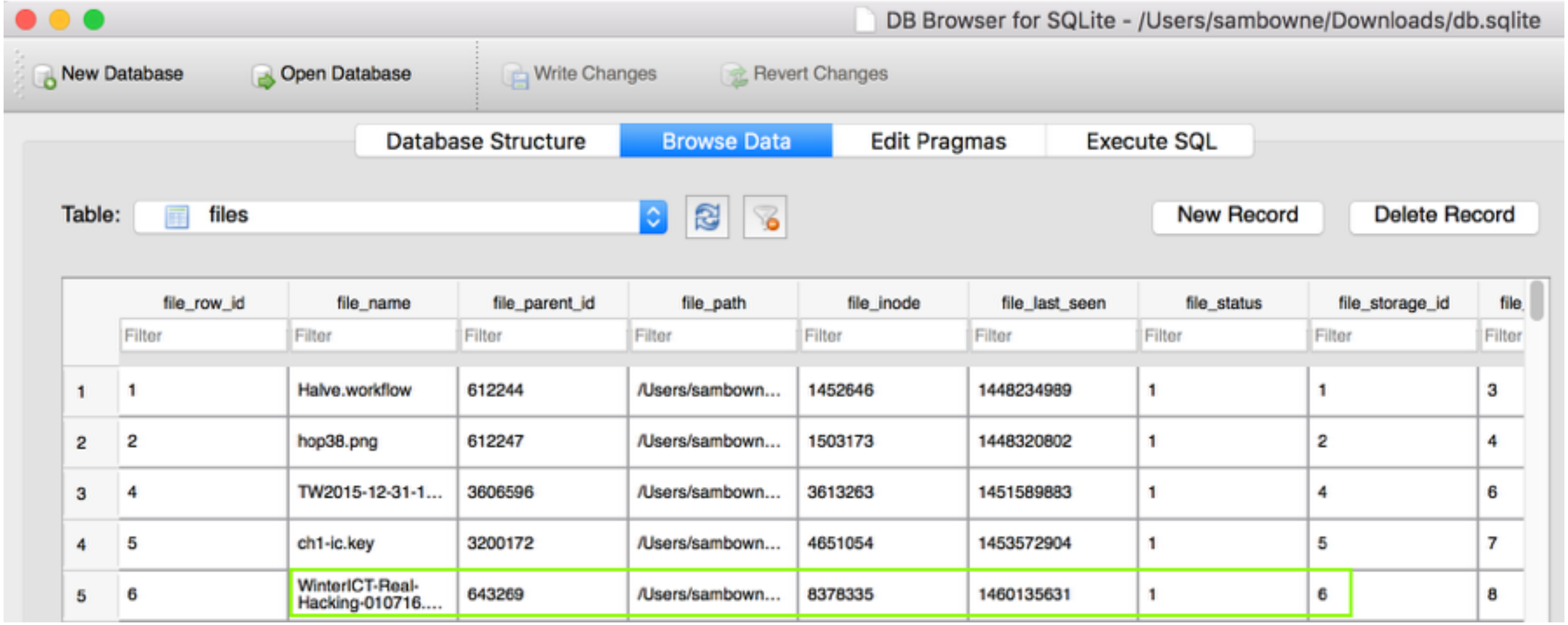
- New in Mac OS X Lion (10.7)
- Allows apps to continuously save data
- Uses daemon "revisiond"
- Saves data on volumes under the "hidden" directory
    - /.DocumentRevisions-V100

Capturing db Files

- **Copy them to another folder**
- **Originals are in use and won't open**
- **db.sqlite shows files used with timestamps**



```
[sh-3.2# pwd
/.DocumentRevisions-V100/db-V1
[sh-3.2# ls -al
total 16360
drwx------@ 4 root  wheel      136 Nov 15  2015 .
d--x--x--x  9 root  wheel      306 Oct  2 17:46 ..
-rw-r--r--  1 root  wheel   872448 Nov 13 06:59 db.sqlite
-rw-r--r--  1 root  wheel  7502552 Nov 15 10:11 db.sqlite-wal
sh-3.2# 
```



	file_row_id	file_name	file_parent_id	file_path	file_inode	file_last_seen	file_status	file_storage_id	file_
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	Halve.workflow	612244	/Users/sambown...	1452646	1448234989	1	1	3
2	2	hop38.png	612247	/Users/sambown...	1503173	1448320802	1	2	4
3	4	TW2015-12-31-1...	3606596	/Users/sambown...	3613263	1451589883	1	4	6
4	5	ch1-ic.key	3200172	/Users/sambown...	4651054	1453572904	1	5	7
5	6	WinterICT-Real- Hacking-010716....	643269	/Users/sambown...	8378335	1460135631	1	6	8

- **Consider the file with file_storage_id 6**

Generations

- **394 versions of that file saved**
- **With timestamps and other info.**

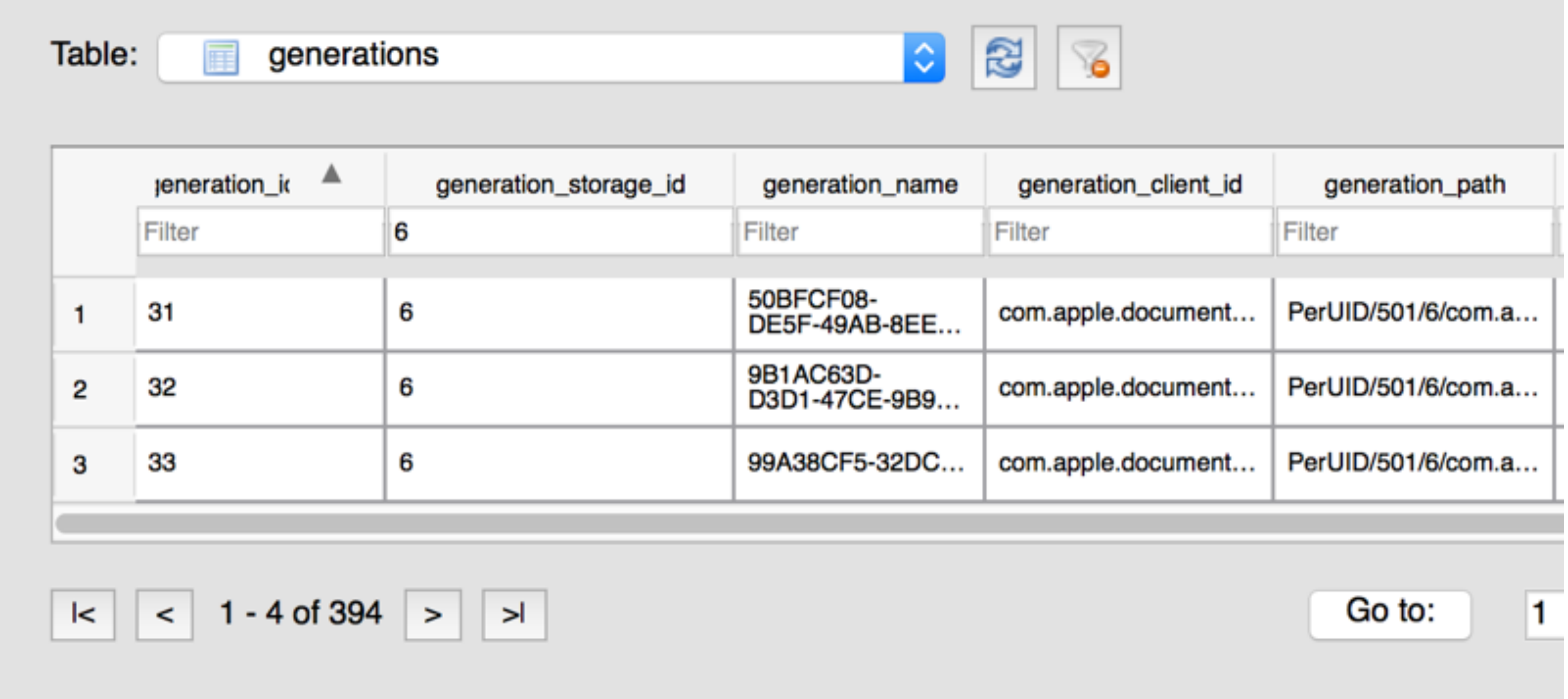


Table: generations

	ɪeneration_ic ▲	generation_storage_id	generation_name	generation_client_id	generation_path
	Filter	6	Filter	Filter	Filter
1	31	6	50BFCF08-DE5F-49AB-8EE...	com.apple.document...	PerUID/501/6/com.a...
2	32	6	9B1AC63D-D3D1-47CE-9B9...	com.apple.document...	PerUID/501/6/com.a...
3	33	6	99A38CF5-32DC...	com.apple.document...	PerUID/501/6/com.a...

1 - 4 of 394

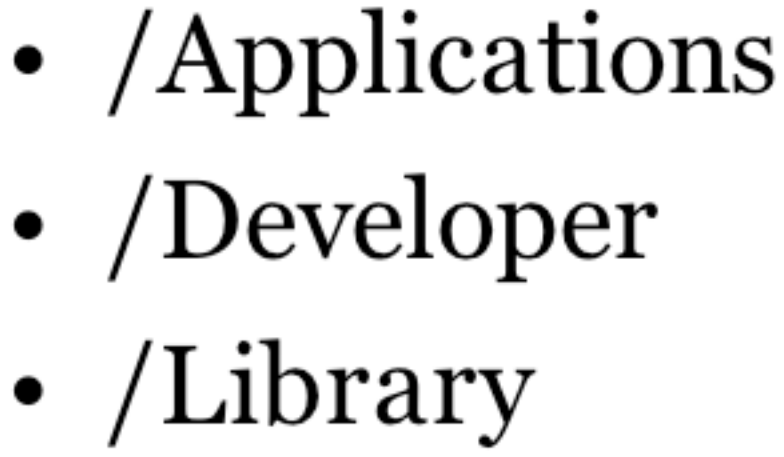
Core Operating System Data

File System Layout

- **Four domains for data classification**
  - **Local**
  - **System**
  - **Network**
  - **User**

Local Domain

- **Applications and configurations that are shared among all users of a system**
- **Administrative privileges required to modify data in this domain**
- **These directories are in the local domain:**



  - /Applications
  - /Developer
  - /Library

System Domain

- Data installed by Apple, and a few specialized low-level utilities

- Most useful domain for intrusion investigations because it contains the system logs

- Includes all the traditional Unix structures, all of which require administrative privileges to modify

  - /bin, /usr, /dev, /etc, and so on, also /System

Network Domain

- **Applications and data stored here is shared among a network of systems and users**
- **In practice, rarely populated with data**
- **Located under the /Network directory**

User Domain

- **Primary source of data for most other investigations**
- **Contains user home directories and a shared directory**
- **All user-created content and configurations will be found under /Users**
- **High-privilege and Unix-savvy users may break this model**

MacPorts Package Manager

- Lets you add BSD packages to your Mac
- Very useful
- Requires command-line developer tools
    - Link Ch 13b

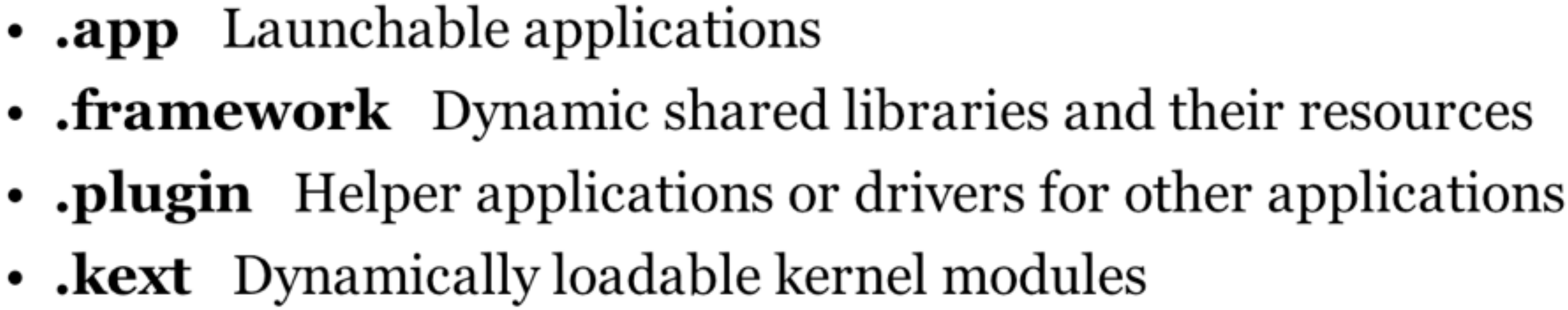
The Local Domain

/Applications

- **Nearly every installed application is here**
- **Application Bundles**
    - **Contain everything an application needs to run:**
    - **Executable code, graphics, configuration files, libraries, helper applications and scripts**

Application Bundles

- **Finder treats the bundle as a single file**
- **Most common extensions**

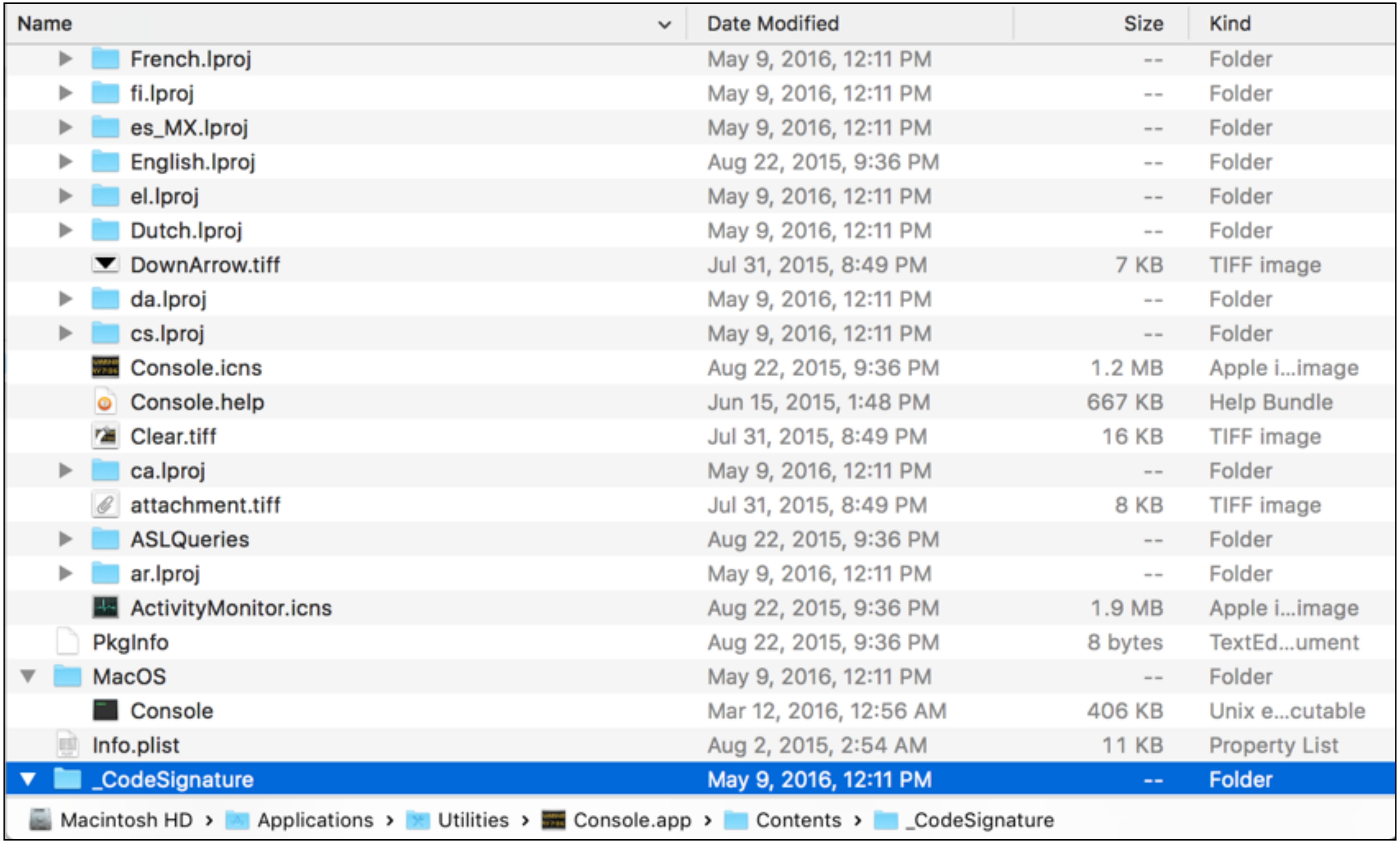


- **.app** Launchable applications
- **.framework** Dynamic shared libraries and their resources
- **.plugin** Helper applications or drivers for other applications
- **.kext** Dynamically loadable kernel modules

Inside the Bundle

- **Right-click, Show Package Contents**
- **Subdirectories**
  - **MacOS, Resources, Library, Frameworks, PlugIns, SharedSupport**
- **Developers can put anything in these directories**
- **VMware Fusion's Library folder contains command-line utilities to manage the VMware hypervisor**

Console App



Name	Date Modified	Size	Kind
French.lproj	May 9, 2016, 12:11 PM	--	Folder
fi.lproj	May 9, 2016, 12:11 PM	--	Folder
es_MX.lproj	May 9, 2016, 12:11 PM	--	Folder
English.lproj	Aug 22, 2015, 9:36 PM	--	Folder
el.lproj	May 9, 2016, 12:11 PM	--	Folder
Dutch.lproj	May 9, 2016, 12:11 PM	--	Folder
DownArrow.tiff	Jul 31, 2015, 8:49 PM	7 KB	TIFF image
da.lproj	May 9, 2016, 12:11 PM	--	Folder
cs.lproj	May 9, 2016, 12:11 PM	--	Folder
Console.icns	Aug 22, 2015, 9:36 PM	1.2 MB	Apple i...image
Console.help	Jun 15, 2015, 1:48 PM	667 KB	Help Bundle
Clear.tiff	Jul 31, 2015, 8:49 PM	16 KB	TIFF image
ca.lproj	May 9, 2016, 12:11 PM	--	Folder
attachment.tiff	Jul 31, 2015, 8:49 PM	8 KB	TIFF image
ASLQueries	Aug 22, 2015, 9:36 PM	--	Folder
ar.lproj	May 9, 2016, 12:11 PM	--	Folder
ActivityMonitor.icns	Aug 22, 2015, 9:36 PM	1.9 MB	Apple i...image
PkgInfo	Aug 22, 2015, 9:36 PM	8 bytes	TextEd...ument
MacOS	May 9, 2016, 12:11 PM	--	Folder
Console	Mar 12, 2016, 12:56 AM	406 KB	Unix e...cutable
Info.plist	Aug 2, 2015, 2:54 AM	11 KB	Property List
_CodeSignature	May 9, 2016, 12:11 PM	--	Folder

Macintosh HD › Applications › Utilities › Console.app › Contents › _CodeSignature

Package Contents

- **Contains additional metadata**
- **Time and date stamps show when the app was installed**
- **A good place to hide data**

/Developer

- **Used by XCode, Apple's development environment**
- **Until recently, all development tools, SDKs, documentation, and debugging tools were here**
- **Later versions of XCode moved the tools**
- **This directory may still be present on some systems**

/Library

- **/System/Library**
  - **App settings for the operating system**
- **/Library**
  - **Settings shared between users**
- **/Users/*username*/Library**
  - **User-specific settings**

Application Support

- **/Library/Application Support**
- **/User/*username*/Library/Application Support**
  - **Settings, caches, license information, and anything else desired by the developer**

Caches

- **/Library/Caches**
- **/User/*username*/Library/Caches**
  - **Temporary data for applications**

Frameworks

- /Library/Frameworks
- /System/Library/Frameworks
  - Drivers or helper applications, for applications
  - Usually nothing significant here

Keychains

- **/Library/Keychains**
- **/System/Library/Keychains**
- **/User/*username*/Library/Keychains**
  - **Passwords and certificates**
  - **Requires user's password to open**

Logs

- **/Library/Logs**
- **/User/*username*/Library/Logs**
  - **Application logs**
  - **Very important to review**

Preferences

- **/Library/Preferences**
- **/User/*username*/Library/Preferences**
  - **Application preferences, if the application allows a system API to manage them**
  - **Stored in .plist files**
  - **Comparable to the Software hive in Windows**

Receipts

- **/Library/Receipts**
- **/User/*username*/Library/Receipts**
  - **Files here are updated when an application is added to the system**
  - **InstallHistory.plist contains information about every application installed via the OS's installer or update framework**

WebServer

- **/Library/WebServer**
  - **Apache, installed on every copy of Mac OS X, is started when a user turns on Web sharing**
  - **This folder is Apache's Document Root**

File Types

- **Used by nearly every application**
- **Property lists (.plist)**
  - **Tools: plutil on Mac, "plist Explorer" on Windows**
- **SQLite databases**
  - **Tools: Firefox Plugin SQLite Manager, sqlitebrowser**

The System Domain

Traditional Unix Paths

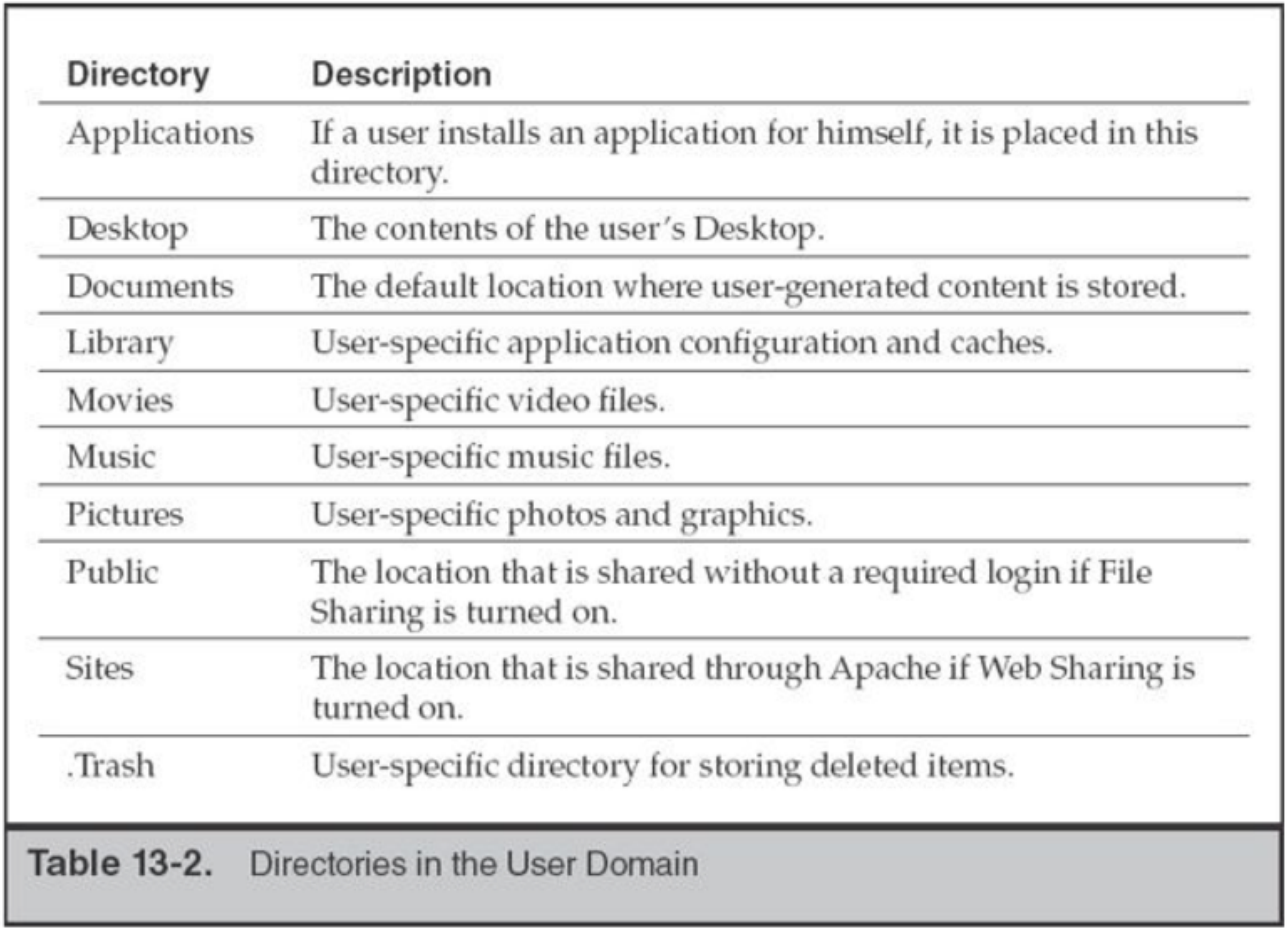
- **Some investigations are based entirely on data found here, such as log files**
- **/System directory is structured similarly to the /Library directory**
  - **Locations where applications maintain persistence**
  - **Requires administrator privileges to create or modify files**

Artifacts

- **System logs in /var/log**
- **Databases in /var/db**
- **Records of printed data in the CUPS log**
- **System sleep image**
- **Software imported using MacPorts or Fink, or compiled in place, may be in /opt**

The User Domain

User-Created Content



Directory	Description
Applications	If a user installs an application for himself, it is placed in this directory.
Desktop	The contents of the user's Desktop.
Documents	The default location where user-generated content is stored.
Library	User-specific application configuration and caches.
Movies	User-specific video files.
Music	User-specific music files.
Pictures	User-specific photos and graphics.
Public	The location that is shared without a required login if File Sharing is turned on.
Sites	The location that is shared through Apache if Web Sharing is turned on.
.Trash	User-specific directory for storing deleted items.

Table 13-2. Directories in the User Domain

Specific Sources of Evidence

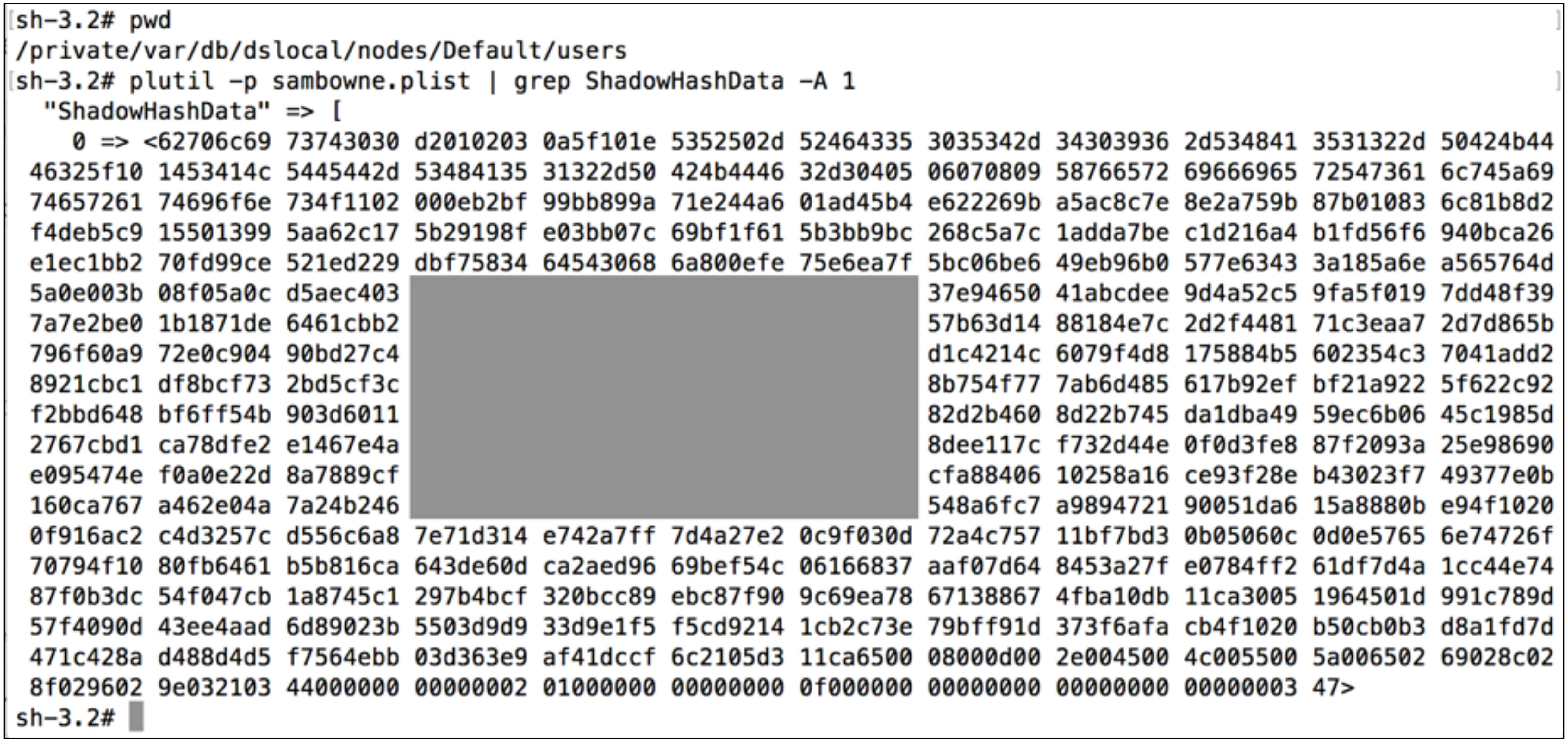
User and Service Configuration

- **Apple uses LDAP for enterprise management and Directory Services for local user management**
- **Directory Services doesn't use the traditional Unix files /etc/passwd and /etc/groups**
- **Data in SQLite databases and binary-formatted property lists**

The Evidence

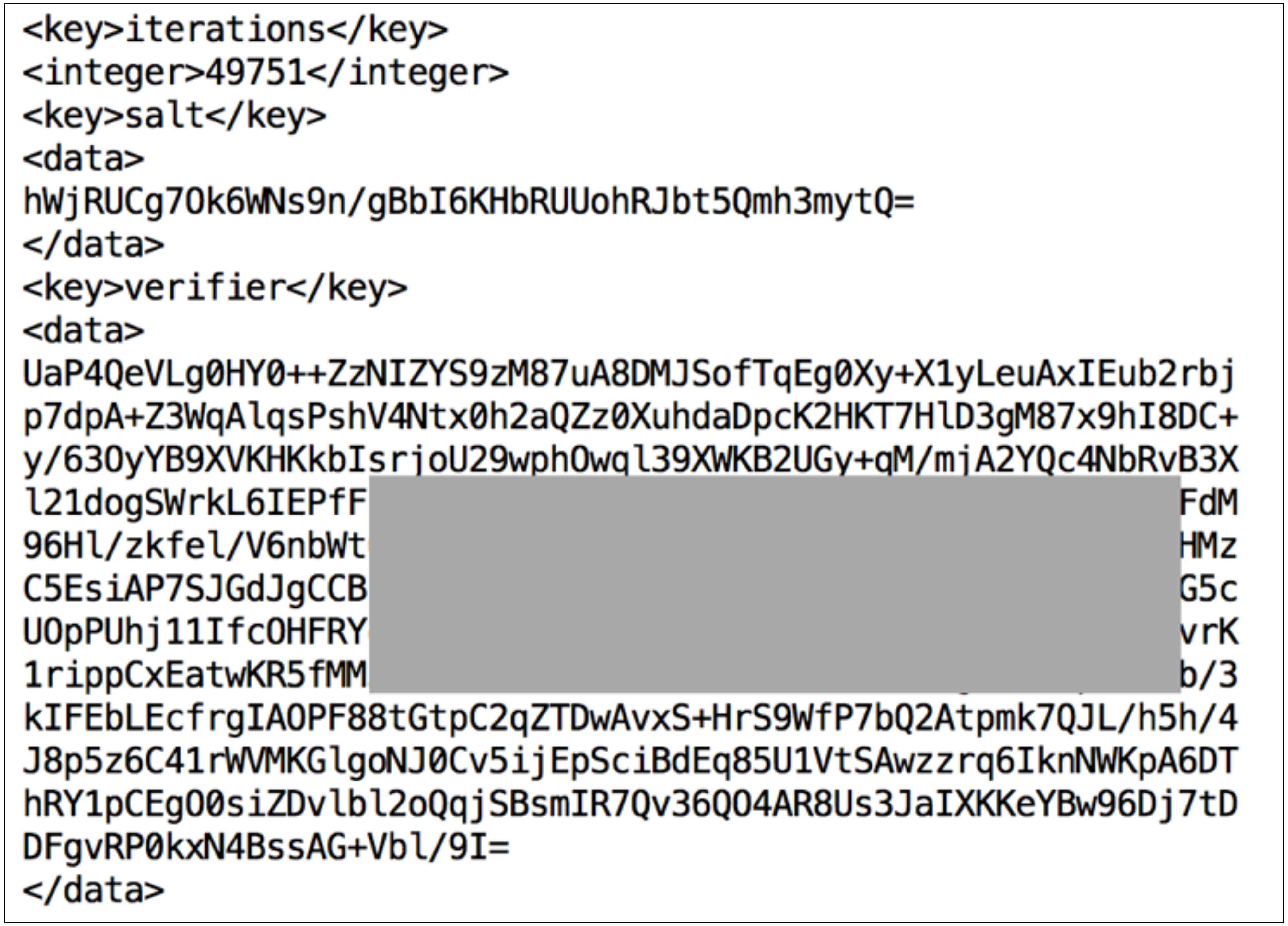
- Directory Service data is in /private/var/db/dslocal
- Databases (or nodes) for the local system are in the subdirectory nodes/Default
- My password hash is on the next slide
  - More info at links Ch 13c and 13d

Password Hash



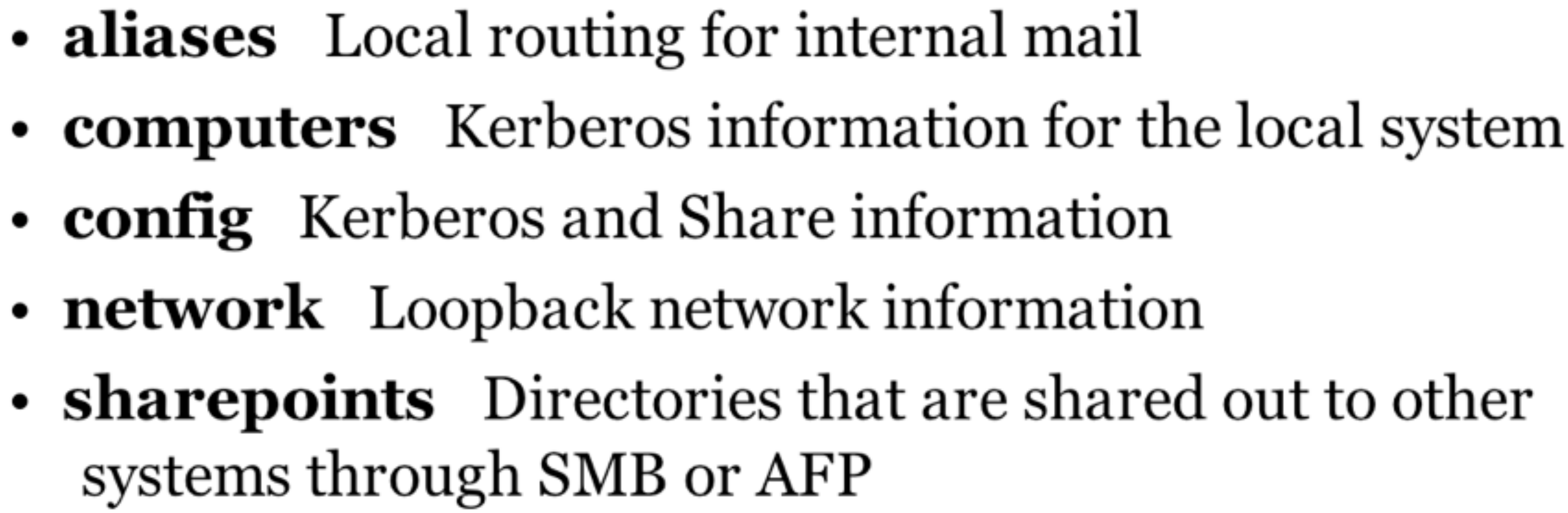
```
sh-3.2# pwd
/private/var/db/dslocal/nodes/Default/users
sh-3.2# plutil -p sambowne.plist | grep ShadowHashData -A 1
  "ShadowHashData" => [
    0 => <62706c69 73743030 d2010203 0a5f101e 5352502d 52464335 3035342d 34303936 2d534841 3531322d 50424b44
 46325f10 1453414c 5445442d 53484135 31322d50 424b4446 32d30405 06070809 58766572 69666965 72547361 6c745a69
 74657261 74696f6e 734f1102 000eb2bf 99bb899a 71e244a6 01ad45b4 e622269b a5ac8c7e 8e2a759b 87b01083 6c81b8d2
 f4deb5c9 15501399 5aa62c17 5b29198f e03bb07c 69bf1f61 5b3bb9bc 268c5a7c 1adda7be c1d216a4 b1fd56f6 940bca26
 e1ec1bb2 70fd99ce 521ed229 dbf75834 64543068 6a800efe 75e6ea7f 5bc06be6 49eb96b0 577e6343 3a185a6e a565764d
 5a0e003b 08f05a0c d5aec403 [redacted]                          37e94650 41abcdee 9d4a52c5 9fa5f019 7dd48f39
 7a7e2be0 1b1871de 6461cbb2                                     57b63d14 88184e7c 2d2f4481 71c3eaa7 2d7d865b
 796f60a9 72e0c904 90bd27c4                                     d1c4214c 6079f4d8 175884b5 602354c3 7041add2
 8921cbc1 df8bcf73 2bd5cf3c                                     8b754f77 7ab6d485 617b92ef bf21a922 5f622c92
 f2bbd648 bf6ff54b 903d6011                                     82d2b460 8d22b745 da1dba49 59ec6b06 45c1985d
 2767cbd1 ca78dfe2 e1467e4a                                     8dee117c f732d44e 0f0d3fe8 87f2093a 25e98690
 e095474e f0a0e22d 8a7889cf                                     cfa88406 10258a16 ce93f28e b43023f7 49377e0b
 160ca767 a462e04a 7a24b246                                     548a6fc7 a9894721 90051da6 15a8880b e94f1020
 0f916ac2 c4d3257c d556c6a8 7e71d314 e742a7ff 7d4a27e2 0c9f030d 72a4c757 11bf7bd3 0b05060c 0d0e5765 6e74726f
 70794f10 80fb6461 b5b816ca 643de60d ca2aed96 69bef54c 06166837 aaf07d64 8453a27f e0784ff2 61df7d4a 1cc44e74
 87f0b3dc 54f047cb 1a8745c1 297b4bcf 320bcc89 ebc87f90 9c69ea78 67138867 4fba10db 11ca3005 1964501d 991c789d
 57f4090d 43ee4aad 6d89023b 5503d9d9 33d9e1f5 f5cd9214 1cb2c73e 79bff91d 373f6afa cb4f1020 b50cb0b3 d8a1fd7d
 471c428a d488d4d5 f7564ebb 03d363e9 af41dccf 6c2105d3 11ca6500 08000d00 2e004500 4c005500 5a006502 69028c02
 8f029602 9e032103 44000000 00000002 01000000 00000000 0f000000 00000000 00000000 00000003 47>
sh-3.2#
```

Decoding the Password Hash



```
<key>iterations</key>
<integer>49751</integer>
<key>salt</key>
<data>
hWjRUCg7Ok6WNs9n/gBbI6KHbRUUohRJbt5Qmh3mytQ=
</data>
<key>verifier</key>
<data>
UaP4QeVLg0HY0++ZzNIZYS9zM87uA8DMJSofTqEg0Xy+X1yLeuAxIEub2rbj
p7dpA+Z3WqAlqsPshV4Ntx0h2aQZz0XuhdaDpcK2HKT7HlD3gM87x9hI8DC+
y/63OyYB9XVKHKkbIsrjoU29wphOwql39XWKB2UGy+qM/mjA2YQc4NbRvB3X
l21dogSWrkL6IEPfF [redacted] FdM
96Hl/zkfel/V6nbWt HMz
C5EsiAP7SJGdJgCCB G5c
UOpPUhj11IfcOHFRY vrK
1rippCxEatwKR5fMM b/3
kIFEbLEcfrgIAOPF88tGtpC2qZTDwAvxS+HrS9WfP7bQ2Atpmk7QJL/h5h/4
J8p5z6C41rWVMKGlgoNJ0Cv5ijEpSciBdEq85U1VtSAwzzrq6IknNWKpA6DT
hRY1pCEgO0siZDvlbl2oQqjSBsmIR7Qv36Q04AR8Us3JaIXKKeYBw96Dj7tD
DFgvRP0kxN4BssAG+Vbl/9I=
</data>
```

Other Configuration Options



- **aliases** Local routing for internal mail
- **computers** Kerberos information for the local system
- **config** Kerberos and Share information
- **network** Loopback network information
- **sharepoints** Directories that are shared out to other systems through SMB or AFP

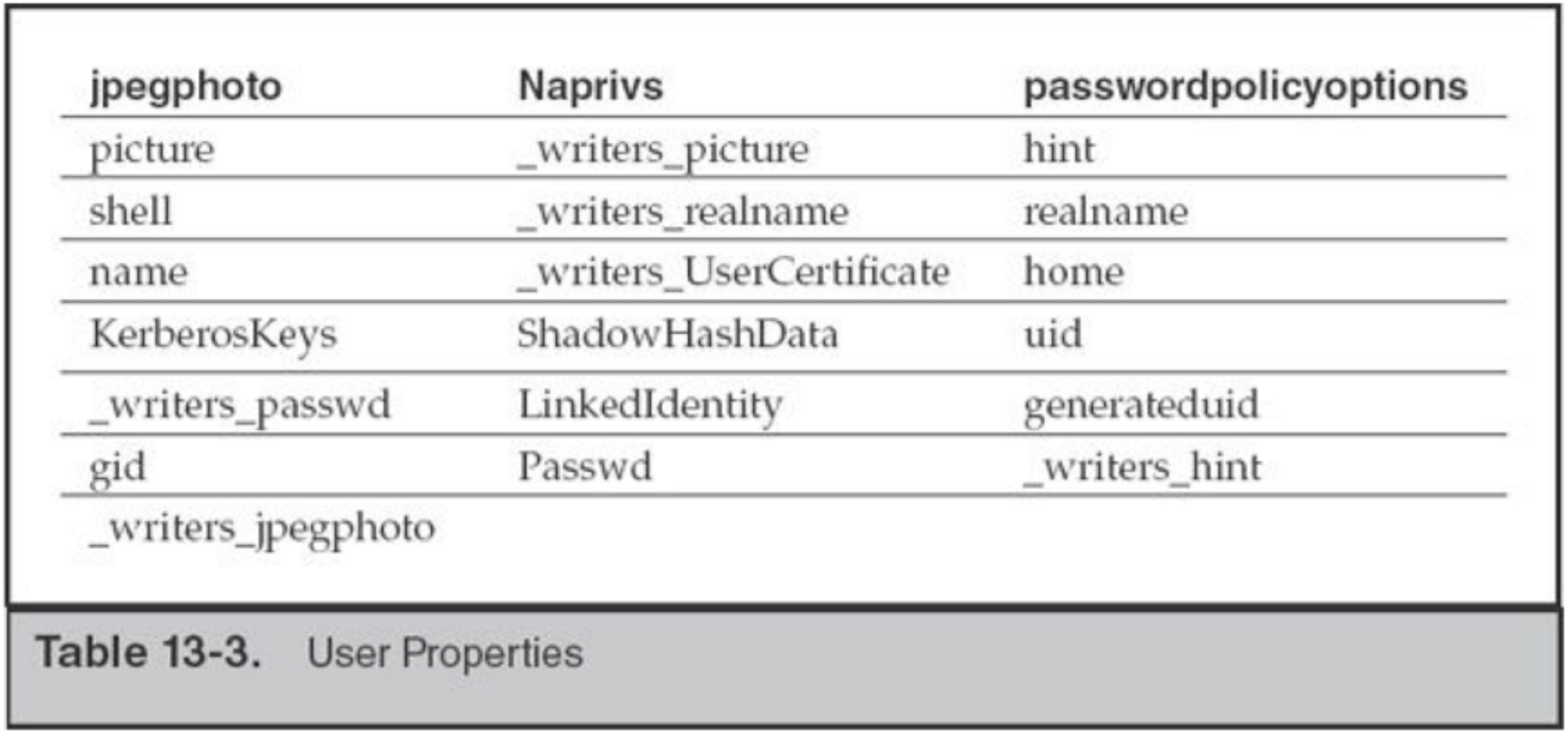
sqlindex

- In /private/var/db/dslocal
- Maintains creation and modification time for the plist files in the directory structure
- And information on the relationships between the data
- Automatically backed up to /private/var/db/dslocal-backup.xar (a gzip tar file)

Analysis of sqlindex

- **Shows when a share was created**
- **Whether an account existed,and its privilege level**

User Accounts



jpegphoto	Naprivs	passwordpolicyoptions
picture	_writers_picture	hint
shell	_writers_realname	realname
name	_writers_UserCertificate	home
KerberosKeys	ShadowHashData	uid
_writers_passwd	LinkedIdentity	generateduid
gid	Passwd	_writers_hint
_writers_jpegphoto		

Table 13-3. User Properties

Sharepoints

- Status of the share for
  - AFP (Apple Filing Protocol)
  - SMB (Server Message Block)
  - FTP (File Transfer Protocol)
- Sharepoint names and share path
- When the share was created

Trash and Deleted Files

- **/.Trashes** Volume-wide trash folder
- **~/.Trash** User-specific trash folder
- **/private/var/root/.Trash** Root user's trash folder

- **Files deleted from USB sticks go into a Trash folder on the stick, labeled by user ID, like**
  - **/Volumes/USBDRIVE/.Trashes/501**

System Auditing, Databases, and Logging

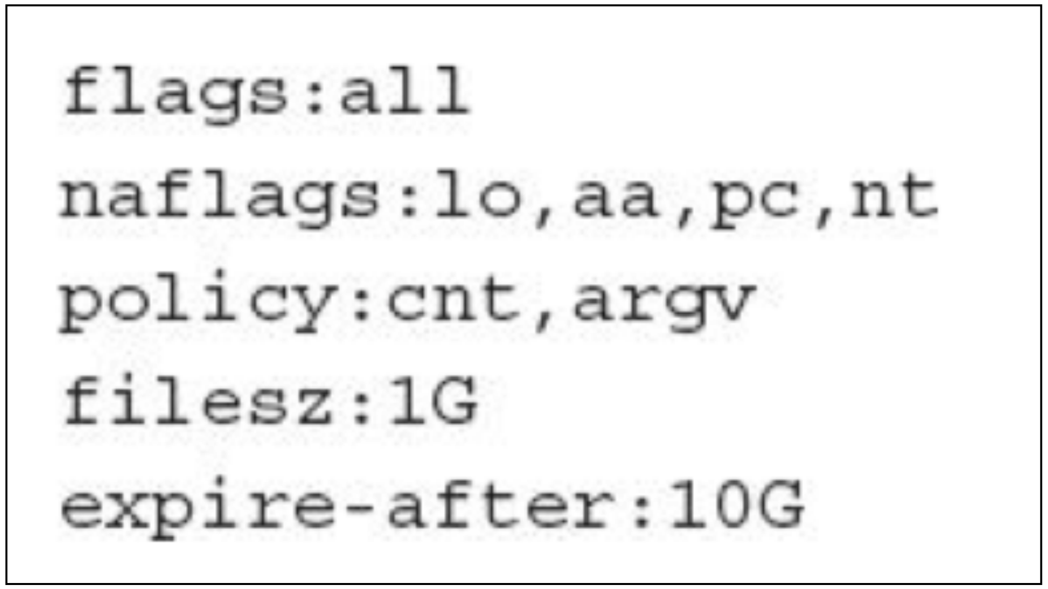
- **Open Source Basic Security Module (OpenBSM)**
  - **Powerful auditing system**
  - **Logs:**
    - **File access**
    - **Network connections**
    - **Execution of applications and their command-line options**

OpenBSM

- Default configuration doesn't save detailed information and is of limited use for IR
- Configuration files in /etc/security
  - Primary file is audit_control

OpenBSM

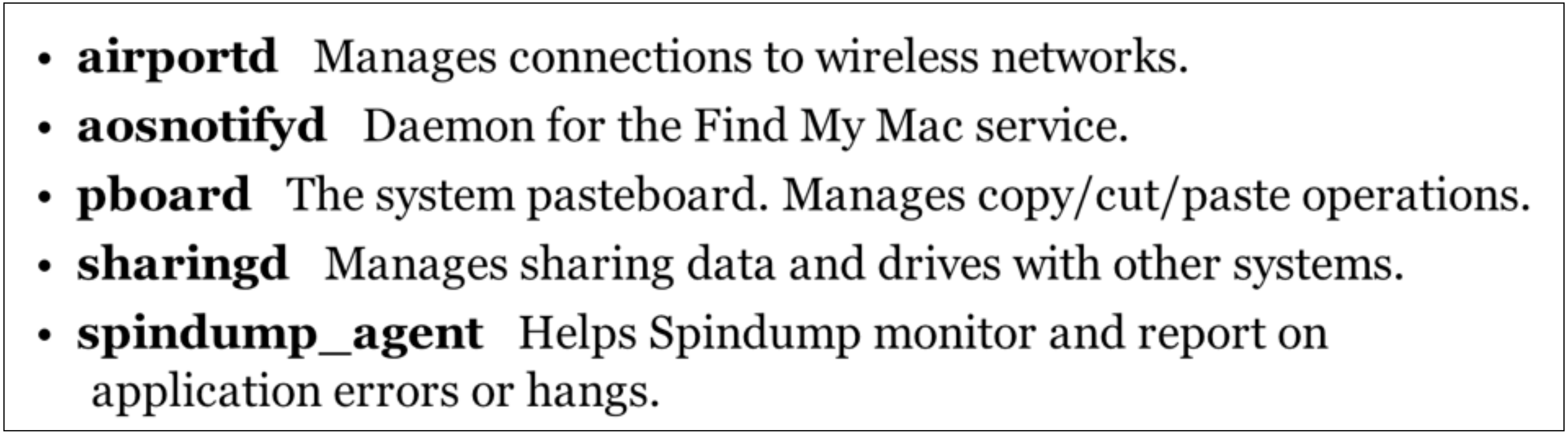
- **This configuration will log everything for all users, and**
  - **Login/logout, administrative events, processes, and network activity**



```
flags:all
naflags:lo,aa,pc,nt
policy:cnt,argv
filesz:1G
expire-after:10G
```

Helper Services

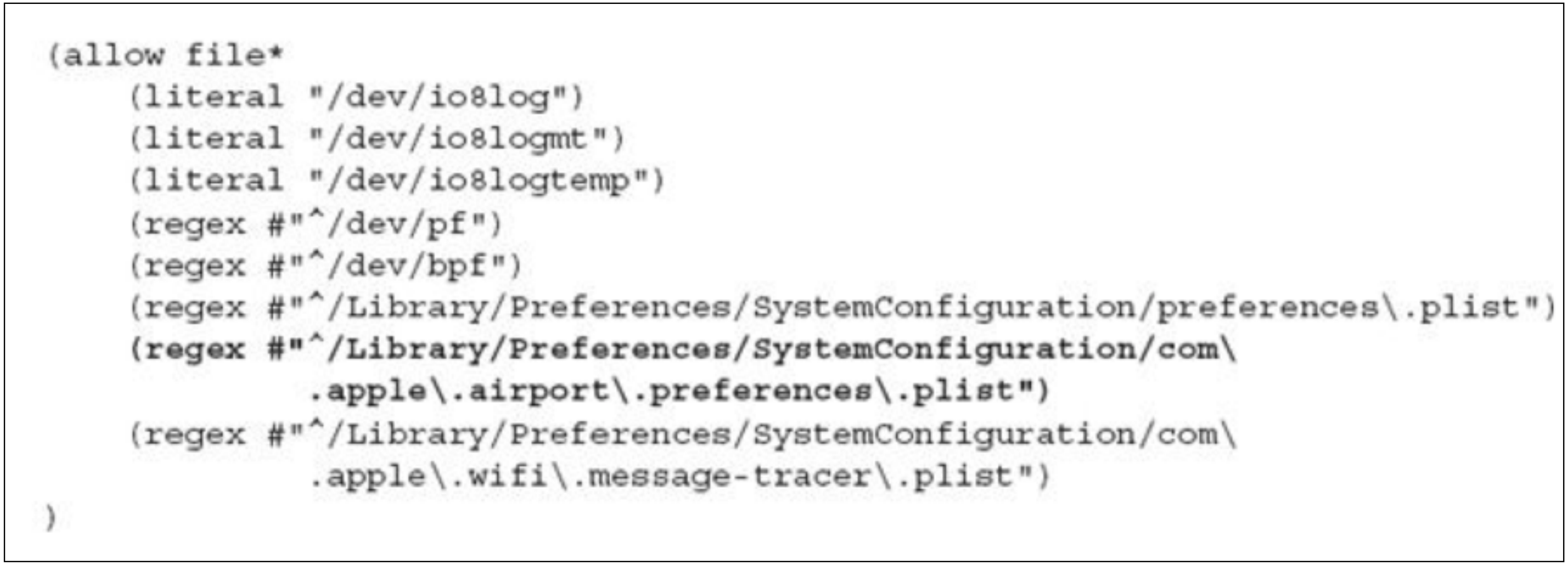
- **Run in background**
- **Track events or common data**
- **Maintain state with SQLite databases or property list**
- **Examples:**



- **airportd** Manages connections to wireless networks.
- **aosnotifyd** Daemon for the Find My Mac service.
- **pboard** The system pasteboard. Manages copy/cut/paste operations.
- **sharingd** Manages sharing data and drives with other systems.
- **spindump_agent** Helps Spindump monitor and report on application errors or hangs.

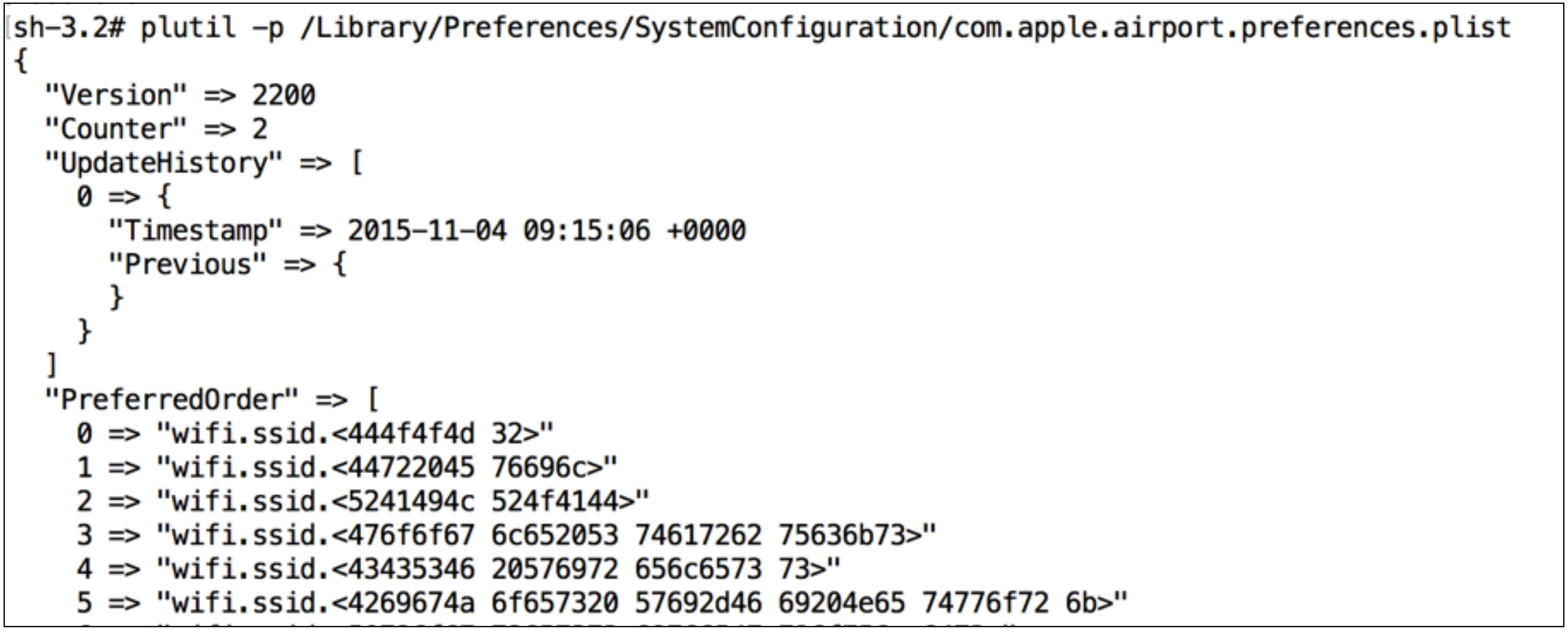
Airportd

- **Runs in an application sandbox**
- **Configured in /usr/share/sandbox**

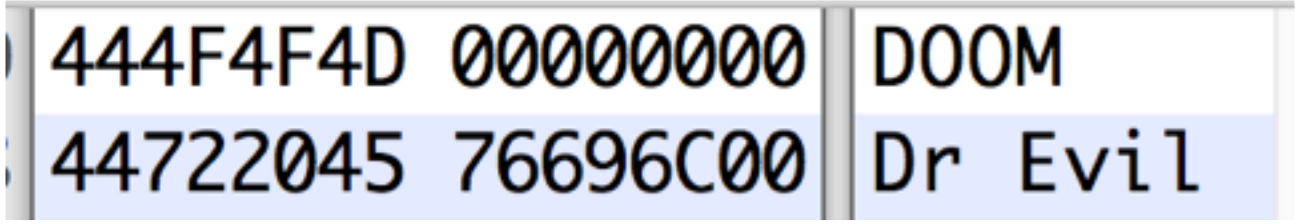


```
(allow file*
    (literal "/dev/io8log")
    (literal "/dev/io8logmt")
    (literal "/dev/io8logtemp")
    (regex #"^/dev/pf")
    (regex #"^/dev/bpf")
    (regex #"^/Library/Preferences/SystemConfiguration/preferences\.plist")
    (regex #"^/Library/Preferences/SystemConfiguration/com\
            .apple\.airport\.preferences\.plist")
    (regex #"^/Library/Preferences/SystemConfiguration/com\
            .apple\.wifi\.message-tracer\.plist")
)
```

Airportd Plist

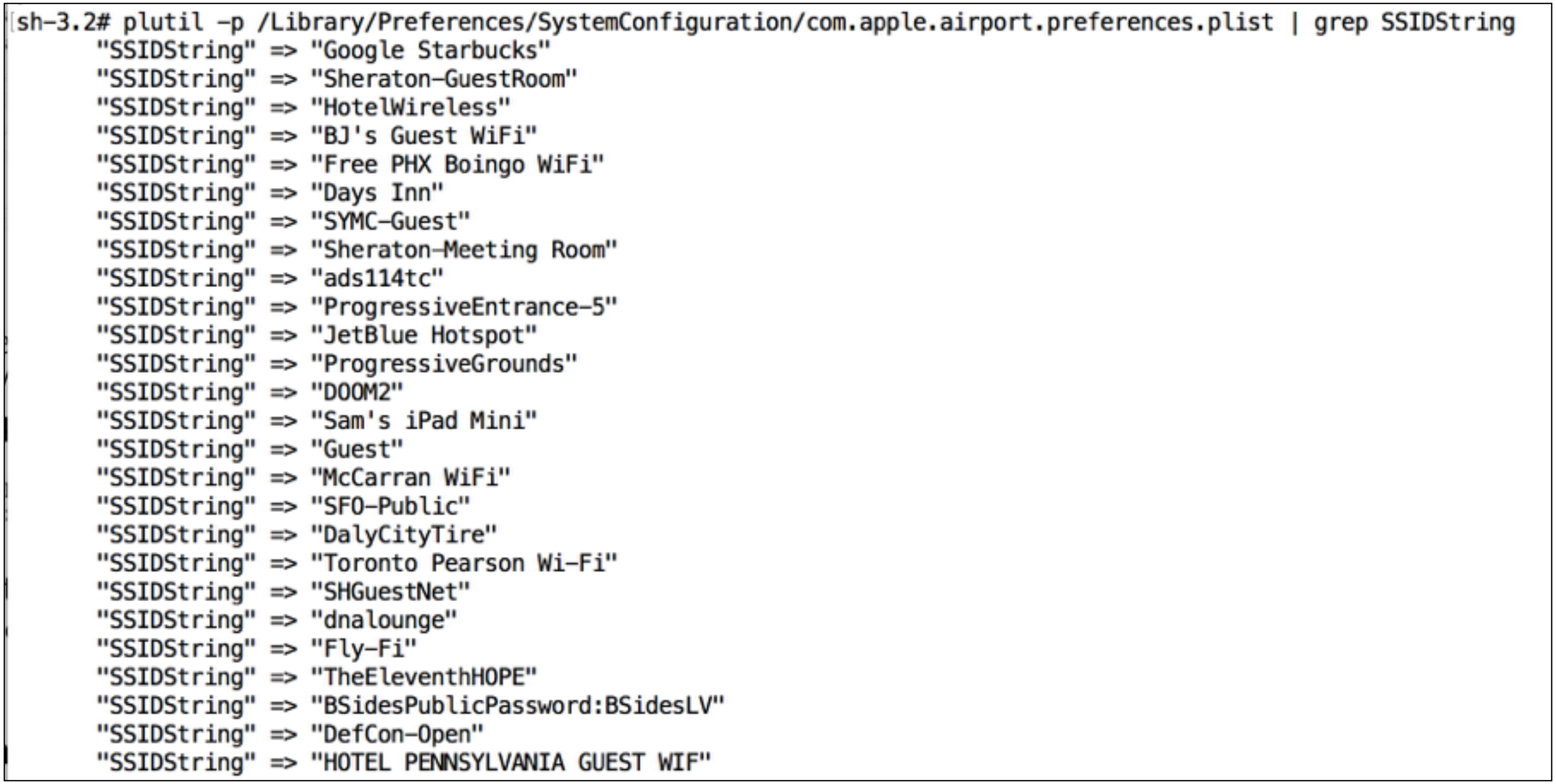


```
sh-3.2# plutil -p /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist
{
  "Version" => 2200
  "Counter" => 2
  "UpdateHistory" => [
    0 => {
      "Timestamp" => 2015-11-04 09:15:06 +0000
      "Previous" => {
      }
    }
  ]
  "PreferredOrder" => [
    0 => "wifi.ssid.<444f4f4d 32>"
    1 => "wifi.ssid.<44722045 76696c>"
    2 => "wifi.ssid.<5241494c 524f4144>"
    3 => "wifi.ssid.<476f6f67 6c652053 74617262 75636b73>"
    4 => "wifi.ssid.<43435346 20576972 656c6573 73>"
    5 => "wifi.ssid.<4269674a 6f657320 57692d46 69204e65 74776f72 6b>"
```



```
444F4F4D 00000000 | DOOM
44722045 76696C00 | Dr Evil
```

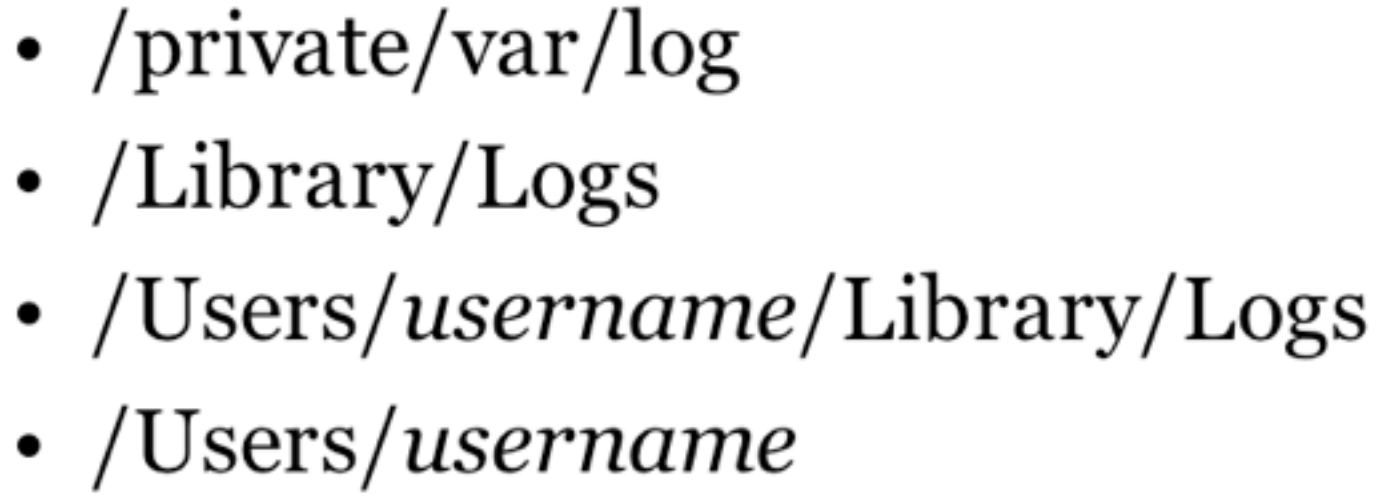
Networks



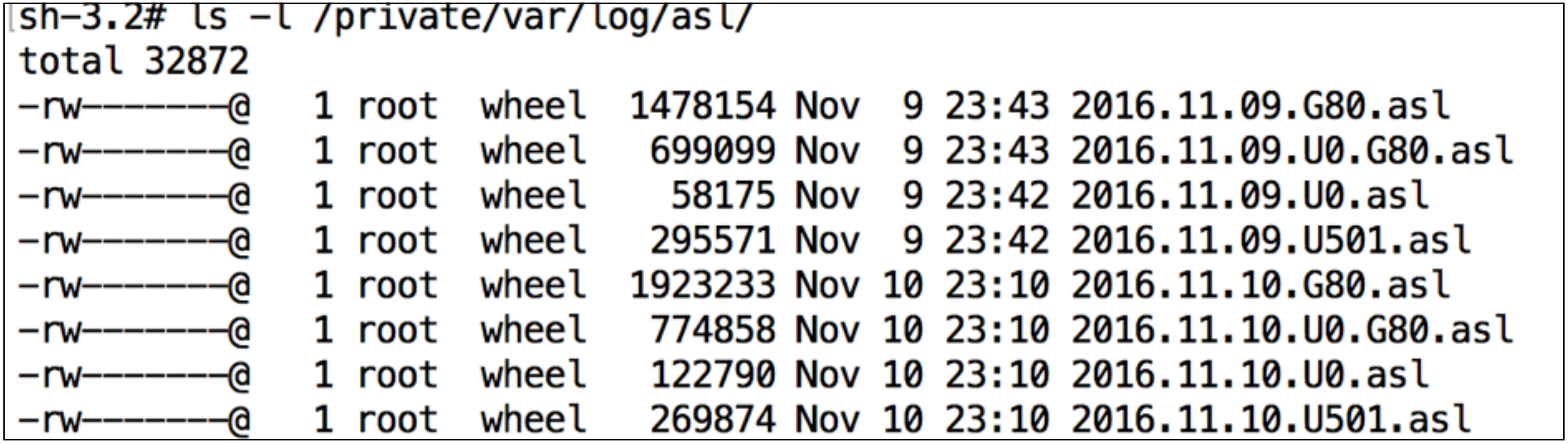
```
[sh-3.2# plutil -p /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist | grep SSIDString
      "SSIDString" => "Google Starbucks"
      "SSIDString" => "Sheraton-GuestRoom"
      "SSIDString" => "HotelWireless"
      "SSIDString" => "BJ's Guest WiFi"
      "SSIDString" => "Free PHX Boingo WiFi"
      "SSIDString" => "Days Inn"
      "SSIDString" => "SYMC-Guest"
      "SSIDString" => "Sheraton-Meeting Room"
      "SSIDString" => "ads114tc"
      "SSIDString" => "ProgressiveEntrance-5"
      "SSIDString" => "JetBlue Hotspot"
      "SSIDString" => "ProgressiveGrounds"
      "SSIDString" => "DOOM2"
      "SSIDString" => "Sam's iPad Mini"
      "SSIDString" => "Guest"
      "SSIDString" => "McCarran WiFi"
      "SSIDString" => "SFO-Public"
      "SSIDString" => "DalyCityTire"
      "SSIDString" => "Toronto Pearson Wi-Fi"
      "SSIDString" => "SHGuestNet"
      "SSIDString" => "dnalounge"
      "SSIDString" => "Fly-Fi"
      "SSIDString" => "TheEleventhHOPE"
      "SSIDString" => "BSidesPublicPassword:BSidesLV"
      "SSIDString" => "DefCon-Open"
      "SSIDString" => "HOTEL PENNSYLVANIA GUEST WIF"
```

System and Application Logging

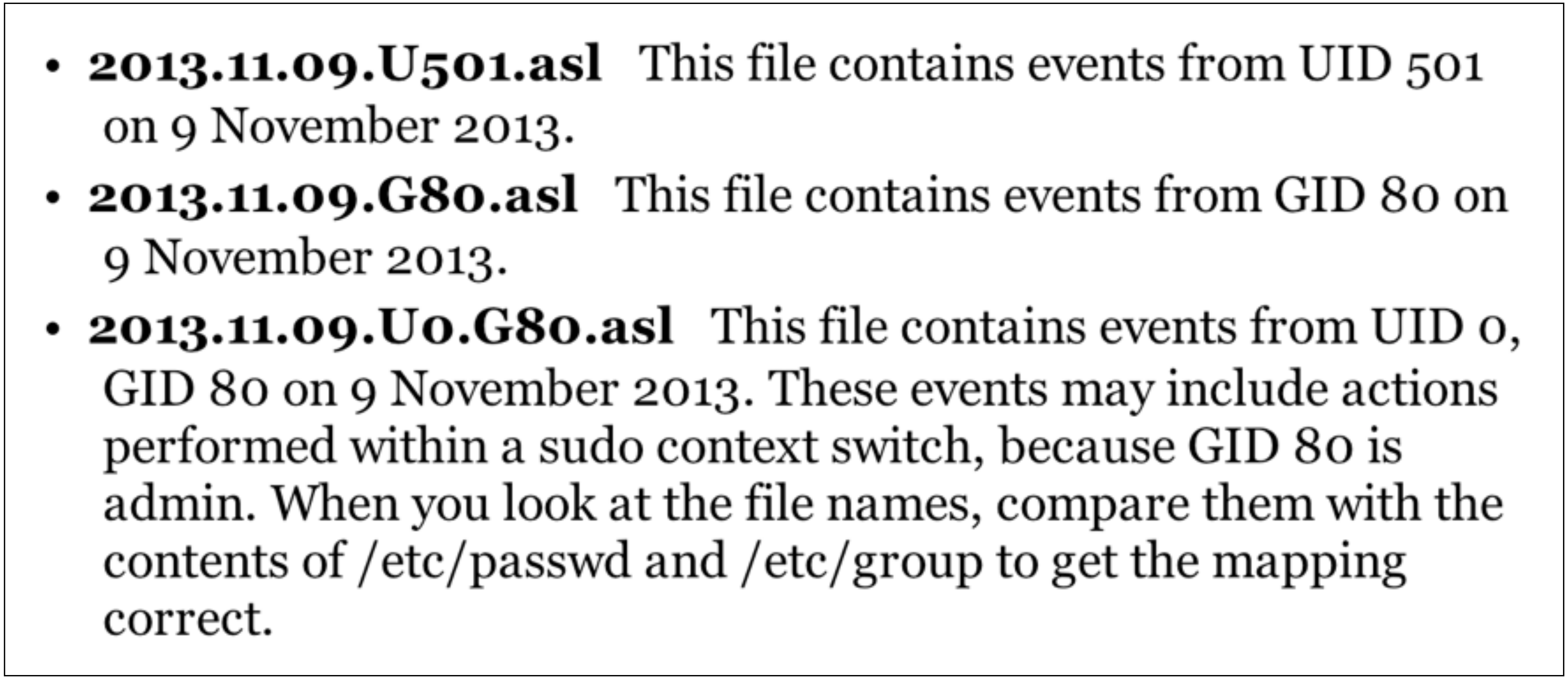
- **Many log and forensic artifacts in these folders**
- **Most are in plaintext, some are binary**



- /private/var/log
- /Library/Logs
- /Users/*username*/Library/Logs
- /Users/*username*

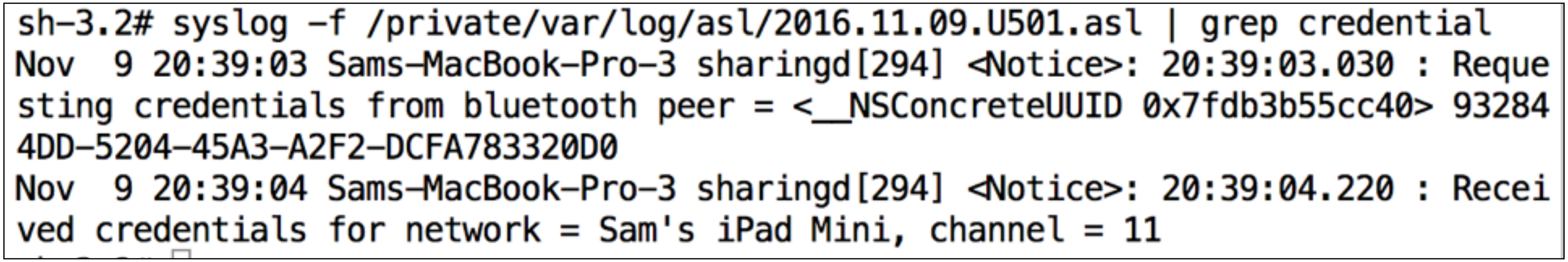


```
sh-3.2# ls -l /private/var/log/asl/
total 32872
-rw-------@  1 root  wheel  1478154 Nov  9 23:43 2016.11.09.G80.asl
-rw-------@  1 root  wheel   699099 Nov  9 23:43 2016.11.09.U0.G80.asl
-rw-------@  1 root  wheel    58175 Nov  9 23:42 2016.11.09.U0.asl
-rw-------@  1 root  wheel   295571 Nov  9 23:42 2016.11.09.U501.asl
-rw-------@  1 root  wheel  1923233 Nov 10 23:10 2016.11.10.G80.asl
-rw-------@  1 root  wheel   774858 Nov 10 23:10 2016.11.10.U0.G80.asl
-rw-------@  1 root  wheel   122790 Nov 10 23:10 2016.11.10.U0.asl
-rw-------@  1 root  wheel   269874 Nov 10 23:10 2016.11.10.U501.asl
```



- **2013.11.09.U501.asl** This file contains events from UID 501 on 9 November 2013.
- **2013.11.09.G80.asl** This file contains events from GID 80 on 9 November 2013.
- **2013.11.09.U0.G80.asl** This file contains events from UID 0, GID 80 on 9 November 2013. These events may include actions performed within a sudo context switch, because GID 80 is admin. When you look at the file names, compare them with the contents of /etc/passwd and /etc/group to get the mapping correct.

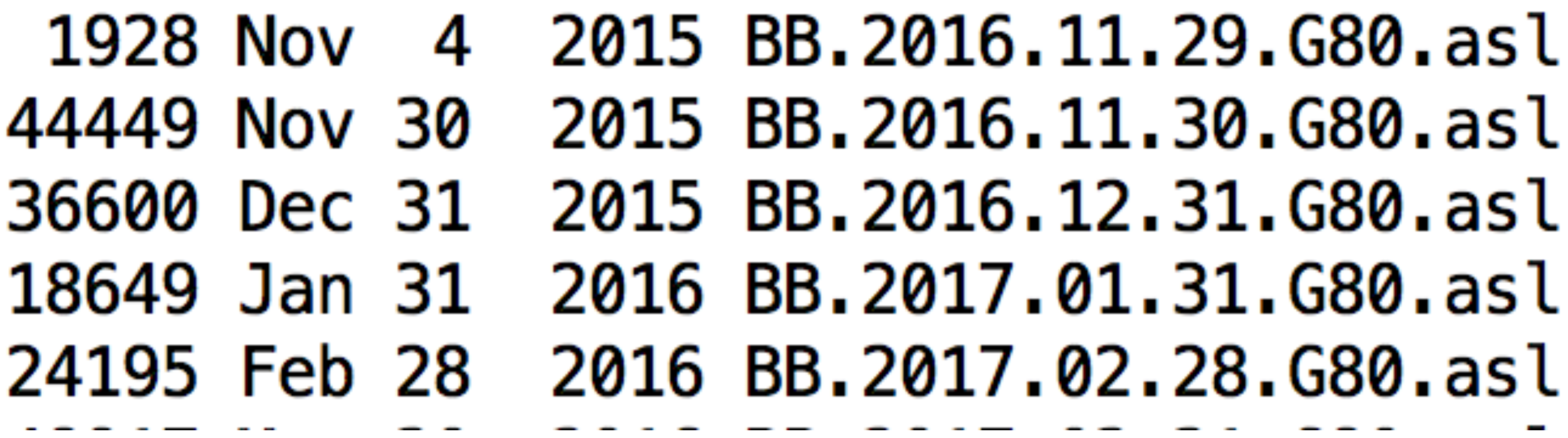
Read with Syslog



```
sh-3.2# syslog -f /private/var/log/asl/2016.11.09.U501.asl | grep credential
Nov  9 20:39:03 Sams-MacBook-Pro-3 sharingd[294] <Notice>: 20:39:03.030 : Reque
sting credentials from bluetooth peer = <__NSConcreteUUID 0x7fdb3b55cc40> 93284
4DD-5204-45A3-A2F2-DCFA783320D0
Nov  9 20:39:04 Sams-MacBook-Pro-3 sharingd[294] <Notice>: 20:39:04.220 : Recei
ved credentials for network = Sam's iPad Mini, channel = 11
```

Other ASL Log Files

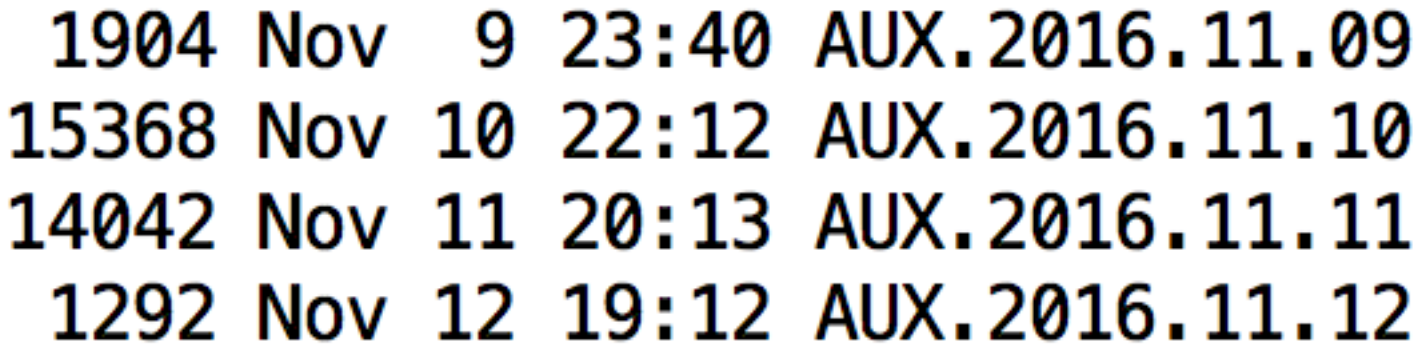
- **Filenames starting with BB**
  - **Authentication logs from long ago**
  - **Year is 1 year after the correct date**



```
 1928 Nov  4  2015 BB.2016.11.29.G80.asl
44449 Nov 30  2015 BB.2016.11.30.G80.asl
36600 Dec 31  2015 BB.2016.12.31.G80.asl
18649 Jan 31  2016 BB.2017.01.31.G80.asl
24195 Feb 28  2016 BB.2017.02.28.G80.asl
```

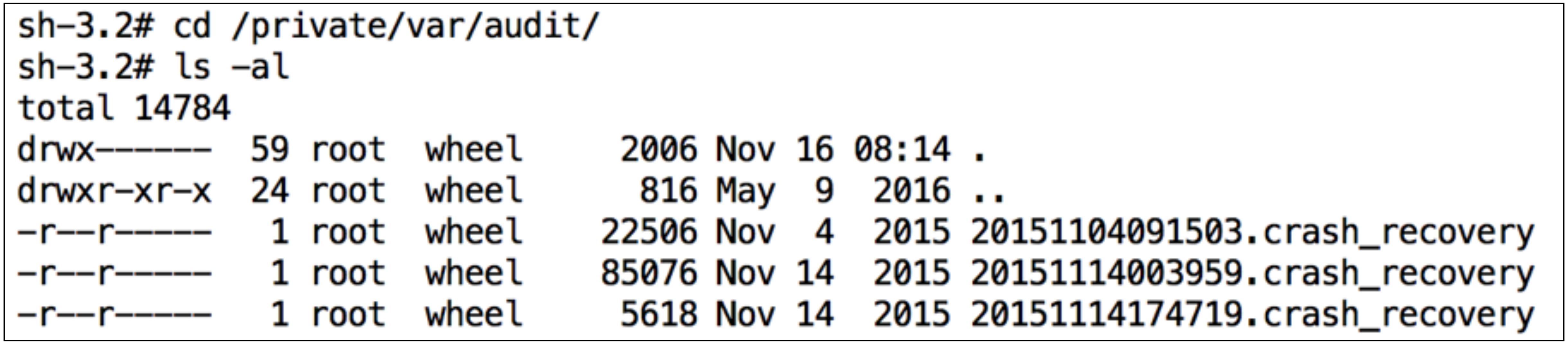
Other ASL Log Files

- **Filenames starting with AUX**
  - **Backtrace for crashed or abnormally terminated applications**
  - **Plaintext**



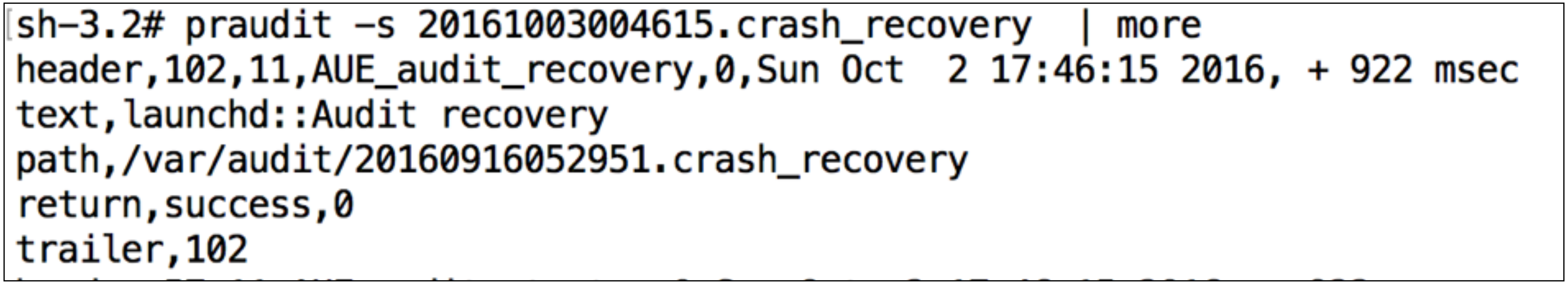
```
 1904 Nov  9 23:40 AUX.2016.11.09
15368 Nov 10 22:12 AUX.2016.11.10
14042 Nov 11 20:13 AUX.2016.11.11
 1292 Nov 12 19:12 AUX.2016.11.12
```

/private/var/audit



```
sh-3.2# cd /private/var/audit/
sh-3.2# ls -al
total 14784
drwx------  59 root  wheel    2006 Nov 16 08:14 .
drwxr-xr-x  24 root  wheel     816 May  9  2016 ..
-r--r-----   1 root  wheel   22506 Nov  4  2015 20151104091503.crash_recovery
-r--r-----   1 root  wheel   85076 Nov 14  2015 20151114003959.crash_recovery
-r--r-----   1 root  wheel    5618 Nov 14  2015 20151114174719.crash_recovery
```

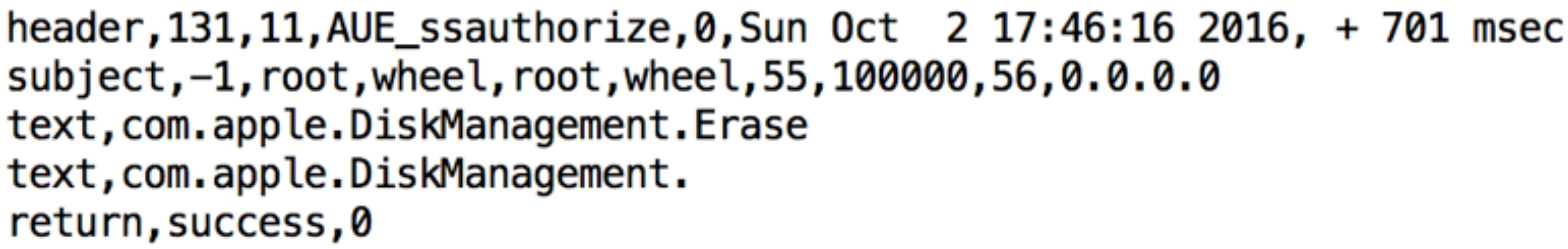
- **Read with praudit**



```
[sh-3.2# praudit -s 20161003004615.crash_recovery  | more
header,102,11,AUE_audit_recovery,0,Sun Oct  2 17:46:15 2016, + 922 msec
text,launchd::Audit recovery
path,/var/audit/20160916052951.crash_recovery
return,success,0
trailer,102
```

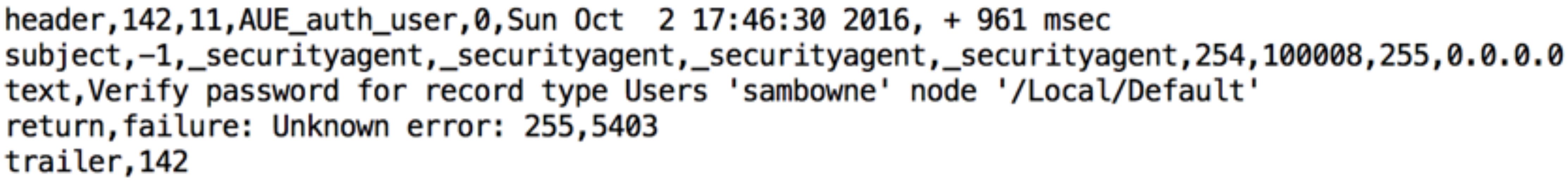
Example Log Entries

- **Erase flash drive**



```
header,131,11,AUE_ssauthorize,0,Sun Oct  2 17:46:16 2016, + 701 msec
subject,-1,root,wheel,root,wheel,55,100000,56,0.0.0.0
text,com.apple.DiskManagement.Erase
text,com.apple.DiskManagement.
return,success,0
```

- **Failed login attempt**



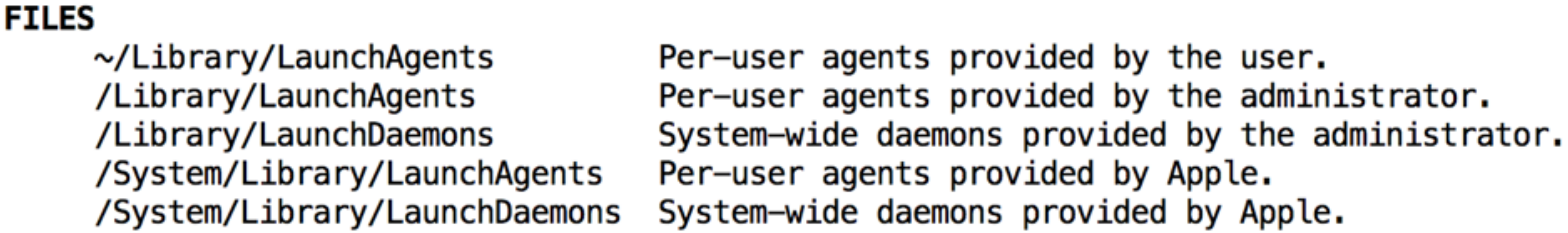
```
header,142,11,AUE_auth_user,0,Sun Oct  2 17:46:30 2016, + 961 msec
subject,-1,_securityagent,_securityagent,_securityagent,_securityagent,254,100008,255,0.0.0.0
text,Verify password for record type Users 'sambowne' node '/Local/Default'
return,failure: Unknown error: 255,5403
trailer,142
```

Interesting Items in Log

- **iCloud connection, Time Machine, iTunes**
  - **Indicates that there are backups of data on other devices**

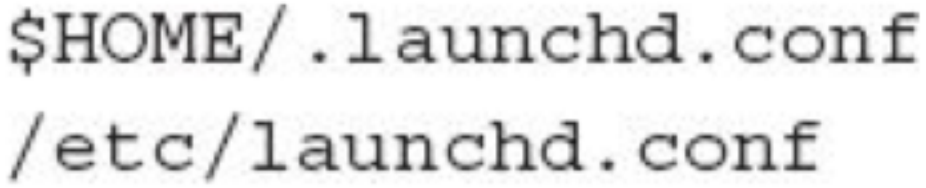
Scheduled Tasks and Services

- **Apple moved from cron to launchd**



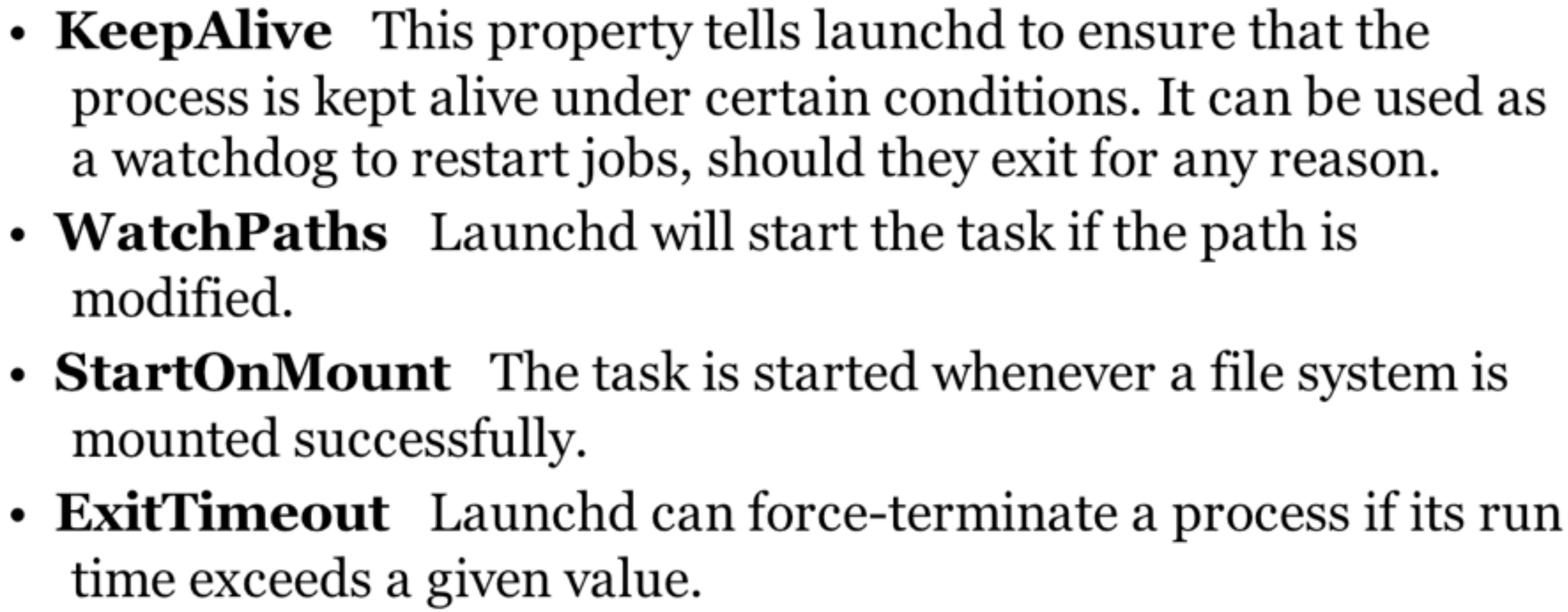
```
FILES
     ~/Library/LaunchAgents         Per-user agents provided by the user.
     /Library/LaunchAgents          Per-user agents provided by the administrator.
     /Library/LaunchDaemons         System-wide daemons provided by the administrator.
     /System/Library/LaunchAgents   Per-user agents provided by Apple.
     /System/Library/LaunchDaemons  System-wide daemons provided by Apple.
```

- **Commands to execute at startup**



```
$HOME/.launchd.conf
/etc/launchd.conf
```

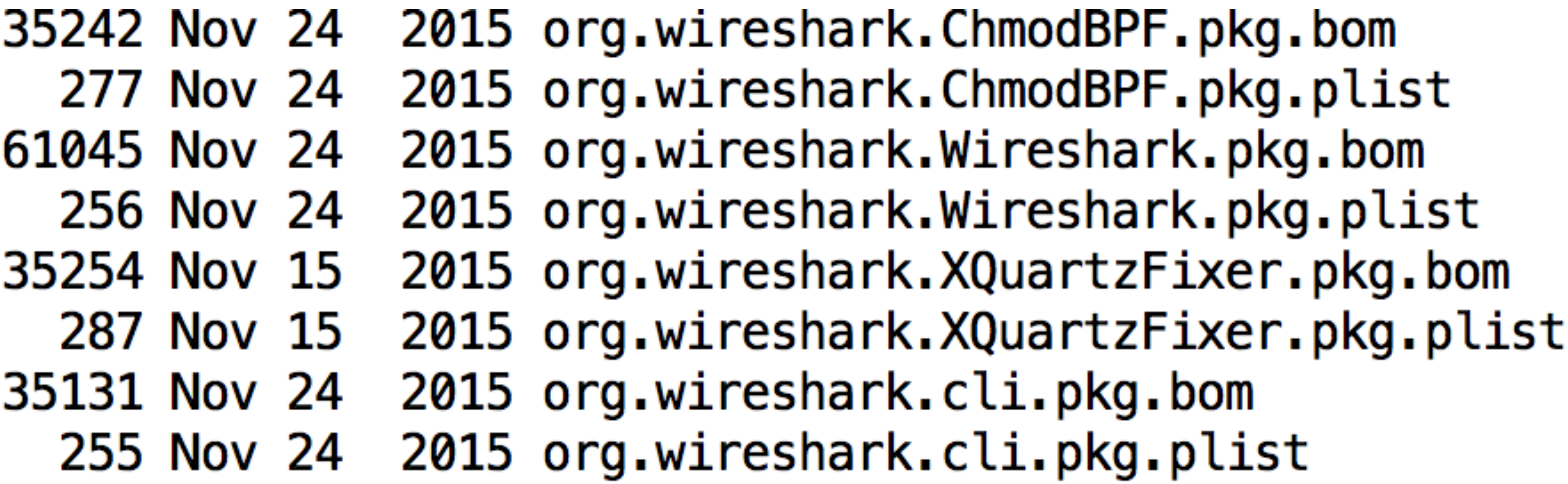
Properties for LaunchAgents



- **KeepAlive** This property tells launchd to ensure that the process is kept alive under certain conditions. It can be used as a watchdog to restart jobs, should they exit for any reason.
- **WatchPaths** Launchd will start the task if the path is modified.
- **StartOnMount** The task is started whenever a file system is mounted successfully.
- **ExitTimeout** Launchd can force-terminate a process if its run time exceeds a given value.

Application Installers

- **When an application is installed, two files are placed in /private/var/db/receipts**
  - **Bill of Materials (BOM) and plist**



```
35242 Nov 24  2015 org.wireshark.ChmodBPF.pkg.bom
  277 Nov 24  2015 org.wireshark.ChmodBPF.pkg.plist
61045 Nov 24  2015 org.wireshark.Wireshark.pkg.bom
  256 Nov 24  2015 org.wireshark.Wireshark.pkg.plist
35254 Nov 15  2015 org.wireshark.XQuartzFixer.pkg.bom
  287 Nov 15  2015 org.wireshark.XQuartzFixer.pkg.plist
35131 Nov 24  2015 org.wireshark.cli.pkg.bom
  255 Nov 24  2015 org.wireshark.cli.pkg.plist
```

Application Installers

- **BOM contains a complete inventory of files**
- **Plist contains install date, package identifier, and path access control lists**

What sources of evidence can I use for timeline analysis?

Artifact	Time-based Evidence Source
HFS+ directory entries	File Access, File Modify, Inode change, Inode Birth timestamps
Syslog and ASL entries	Entry generated time
Wireless connection logs	Entry generated time
Spotlight indexer	Created and modified timestamps
Cron jobs	Scheduled run time, previous run times in logs
OS install date	File Access, File Modify, Inode change, Inode Birth timestamps
Application install date	BOM files
OpenBSM entries	Entry generated time
Application plist files	File system metadata; dates tracked by the applications and set in their plist files
Document revisions	Revision creation dates
Document metadata	Dates stored by applications within certain types of data files

What services were running or what shares were available when the system was imaged?

Artifact	Evidence Source
Directory Services	List of SMB and AFP shares
Contents of /var/run	State files and PID files

What system information can I gather from a static image?

Artifact	Evidence Source
System host name	/Library/Preferences/SystemConfiguration/preferences.plist.
OS version information	/System/Library/CoreService/SystemVersion.plist.
IP addresses	If defined in the Network Preferences, /Library/Preferences/SystemConfiguration/preferences.plist. If configured for DHCP, /private/var/db/dhcpclient/leases/.
Date of OS install	File creation date of /private/var/db/.AppleSetupDone or the InstallDate value in /private/var/db/receipts/com.apple.pkg.InstallMacOSX.plist.
System time zone, connected printers (via color profiles)	/Library/Preferences/.GlobalPreferences.plist. Note that if the user allows Location Services to set the time zone, this file contains the latitude and longitude of the recent locations.

What sources of evidence can prove that a file was recently opened?

Artifact	Evidence Available
/Users/*username*/ Library/Preferences/ com.apple.recentitems.plist	The 10 most recently run applications, connected server information, and documents recently accessed by the user

What artifacts can provide evidence of deleted files?

Artifact	Evidence Available
/Users/*username*/.Trash	Items moved to Trash. If Trash has been emptied, this folder will be empty. Note that files removed outside of Finder are not moved to a Trash folder and are immediately unlinked.

What files are configured to maintain persistence (automatically run) upon bootup or user login?

Artifact	Evidence Available
/Library/LaunchAgents /System/Library/LaunchAgents ~/Library/LaunchAgents	Agents started by the system or per user
/Library/LaunchDaemons /System/Library/LaunchDaemons ~/Library/LaunchDaemons	Daemons started by the system or per user
/Library/StartupItems /System/Library/StartupItems	Legacy system startup items (predating launchd)

Who interactively logged on to a system? At what date(s) and time(s) did a given user log on to a system?

Artifact	Evidence Available
Authentication logs	Contents of /var/log/authd.log and ASL logs in /var/log/asl
File system	Creation of user profile directory (for example /Users/[username]) and associated subdirectories; configuration plists after interactive logon by an account
utmp data	The current logged-in users and the processes that are running