ANALYSIS & CORRELATION OF MAC LOGS

Sarah Edwards
@iamevltwin
oompa@csh.rit.edu

WHY?

Volumes	Network	Location	User Activity
Backups	Software	System Information	System State
Printing	Temporal Changes	Bluetooth	Communication

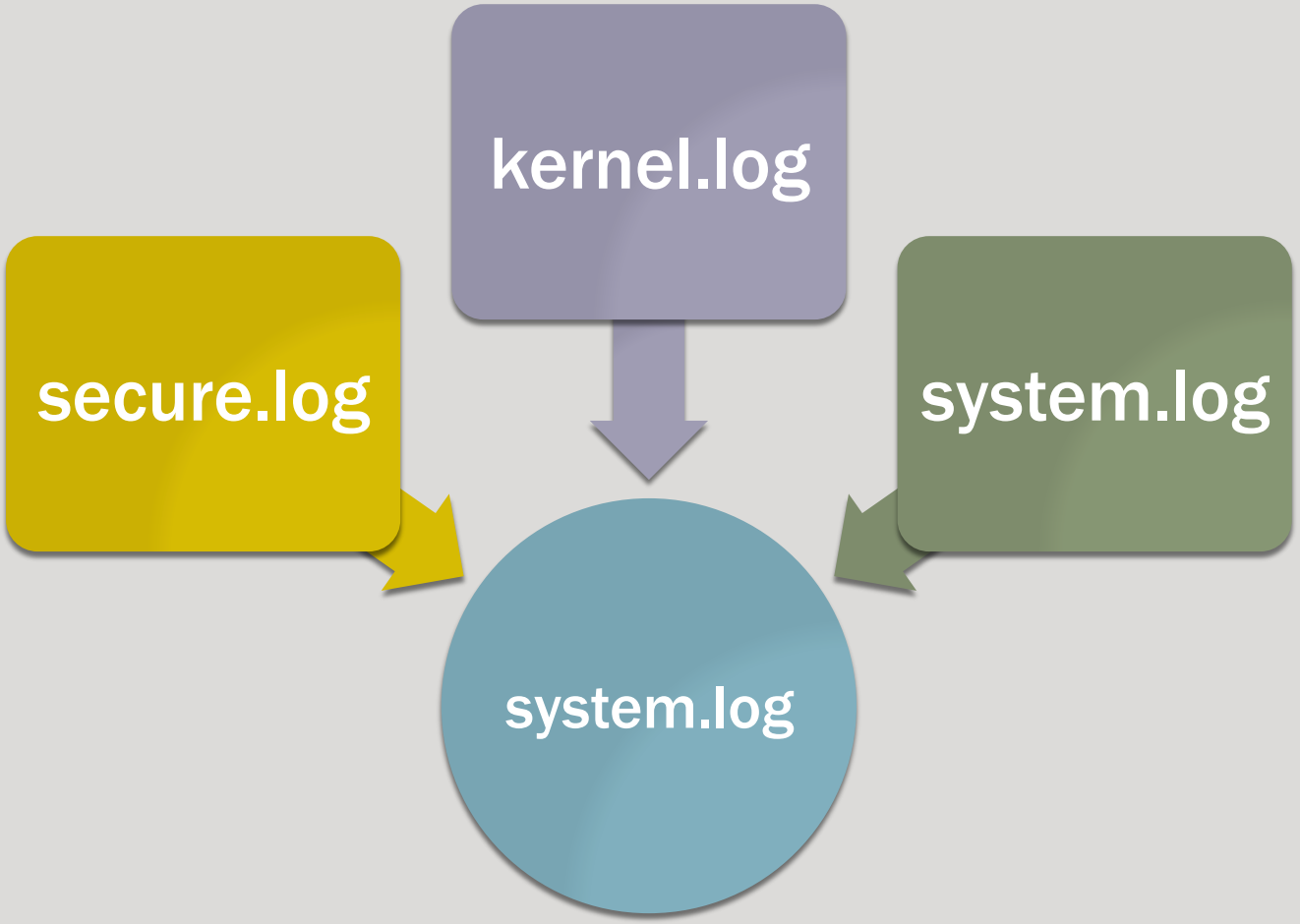
LOG BASICS

oompa@csh.rit.edu | @iamevltwin

GENERAL LOG LOCATION

System Logs	• /private/var/log • /Library/Logs
User Logs	• ~/Library/Logs
Application Specific	• /Library/Application Support/<app> • /Applications/ • /Library/Logs/

MAJOR LOG CHANGES IN 10.8+



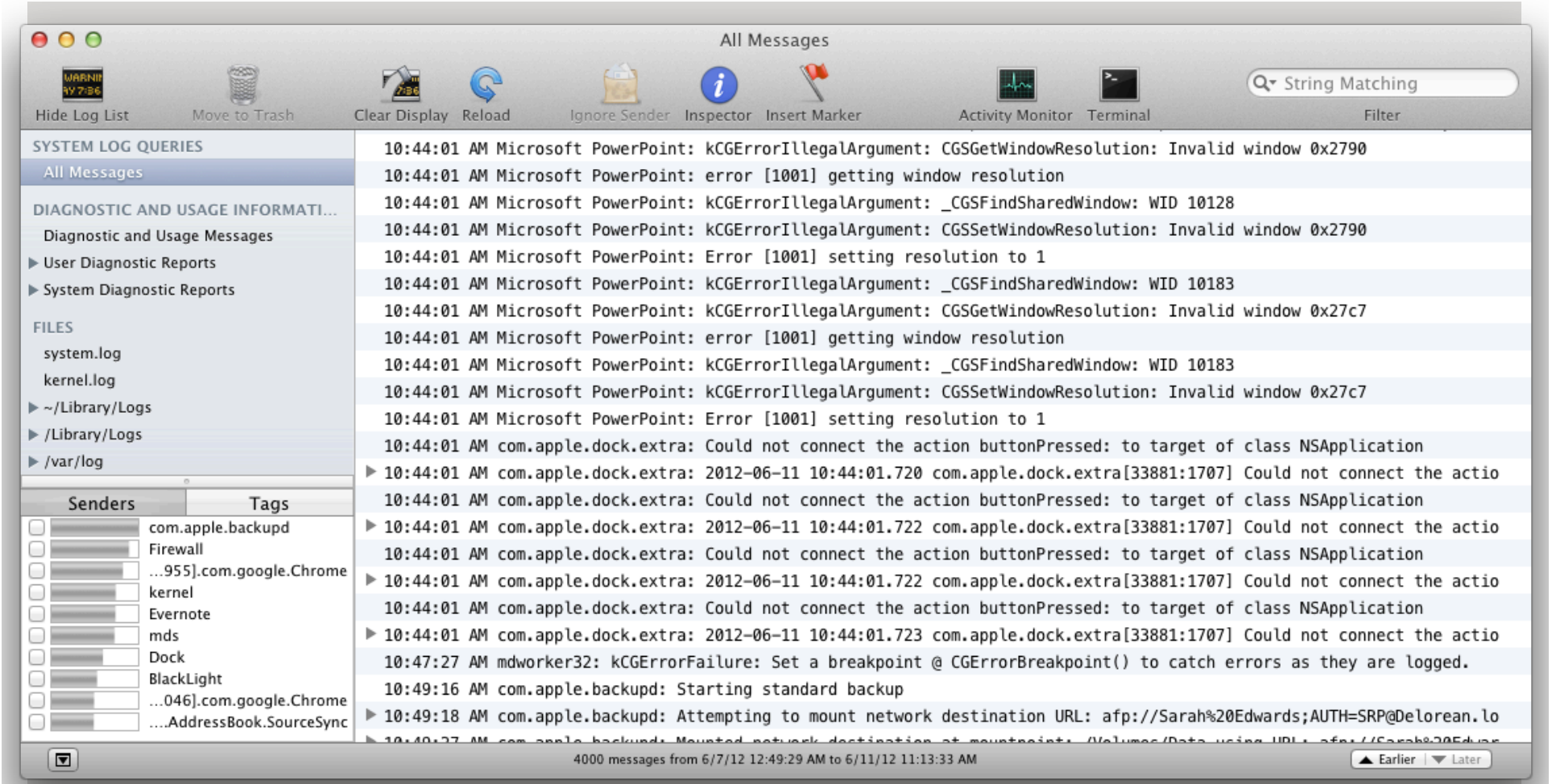
OS X LOG BASICS

- Tends to use Standard Unix Log Format
  - `MMM DD HH:MM:SS Host Service: Message`
- Most are in plaintext
- BZip2 (10.8-) or Gzip (10.9) Compression
  - Used for archival after log turnover

```
appfirewall.log
appfirewall.log.0.bz2
appfirewall.log.1.bz2
appfirewall.log.2.bz2
appfirewall.log.3.bz2
appfirewall.log.4.bz2
appfirewall.log.5.bz2
```

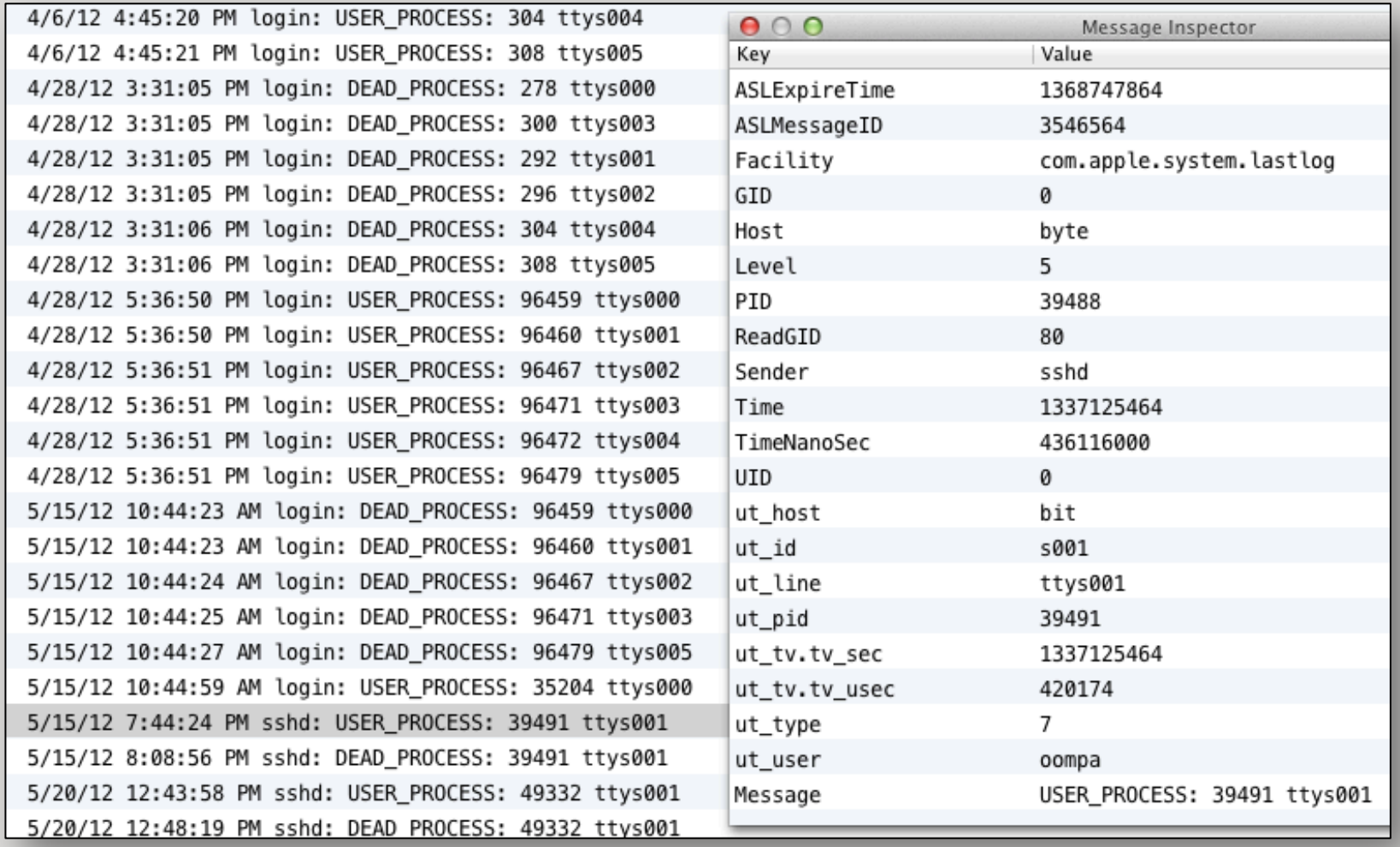
```
Apr 18 22:44:02 byte Firewall[89]: Stealth Mo
Apr 18 22:44:02 byte Firewall[89]: Stealth Mo
Apr 18 22:44:04 byte Firewall[89]: Stealth Mo
Apr 18 22:44:04 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:10 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:10 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:22 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:22 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:46 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:46 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 23:01:12 byte Firewall[89]: Stealth Mode connection attempt
```

CONSOLE.APP



oompa@csh.rit.edu | @iamevltwin

CONSOLE.APP: MESSAGE INSPECTOR



BZIP2 DECOMPRESSION

- Use `bzcat` or `gzcat` on OS X
  - (oldest -> newest)
  - **Bzip2** - system.log.7.bz2 -> system.log.0.bz2
  - **Gzip** - system.log.7.gz -> system.log.0.gz

1. `bzcat system.log.7.bz2 system.log.6.bz2 system.log.5.bz2 system.log.4.bz2 system.log.3.bz2 system.log.2.bz2 system.log.1.bz2 system.log.0.bz2 >> system_all.log`
2. `cat system.log >> system_all.log`

LOG NORMALIZATION

Correlate data in a single system or across multiple systems

Must know “originating” time zone for system

Timestamp Storage

- Apple System Log = UTC
- Most other logs (/var/log, ~/Library/Logs/) = Local System Time

Timestamp Output

- ASL Logs – `praudit` may output to local system time
- Use `export TZ="EST5EDT" command`
- Temporarily change time zone of terminal window

LOG RECOVERY

Logs get “removed” or “turned over”

GREP or keyword search for specific date/log formats.

- “May 18 23:17:15”
- “Thu May 31 19:35:35 EDT 2012”
- “ASL DB”
- “launchctl::Audit startup”
- “BZh91AY&SY”
- “1F8B08”

APPLE SYSTEM LOG

oompa@csh.rit.edu | @iamevltwin

APPLE SYSTEM LOG

- Location: /private/var/log/asl/ (>10.5.6)
- syslog “replacement” (Still uses syslog backend)
- View using Console.app or `syslog` command
- Binary Format – “ASL DB” Signature
- Log Turn Over - 7 Days, ~1 Year (utmp)

```
4153 4c20 4442 0000 0000 0000 0000 0002  ASL DB..........
0000 0000 0000 00f6 0000 0000 51a2 054b  ............Q..K
0000 0100 0000 0000 0003 6c3a 0000 0000  ..........l:....
0000 0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000 0000  ................
0001 0000 007b 6861 6e64 6c65 5f77 696c  .....{handle_wil
6c5f 736c 6565 705f 6175 7468 5f61 6e64  l_sleep_auth_and
5f73 6869 656c 645f 7769 6e64 6f77 733a  _shield_windows:
2072 656c 6561 7369 6e67 2061 7574 6877   releasing authw
2030 7837 6662 3562 6663 3034 3932 3028   0x7fb5bfc04920(
3230 3030 292c 2073 6869 656c 6420 3078  2000), shield 0x
3766 6235 6262 6365 6362 3130 2832 3030  7fb5bbcecb10(200
3129 2c20 6c6f 636b 2073 7461 7465 2033  1), lock state 3
```

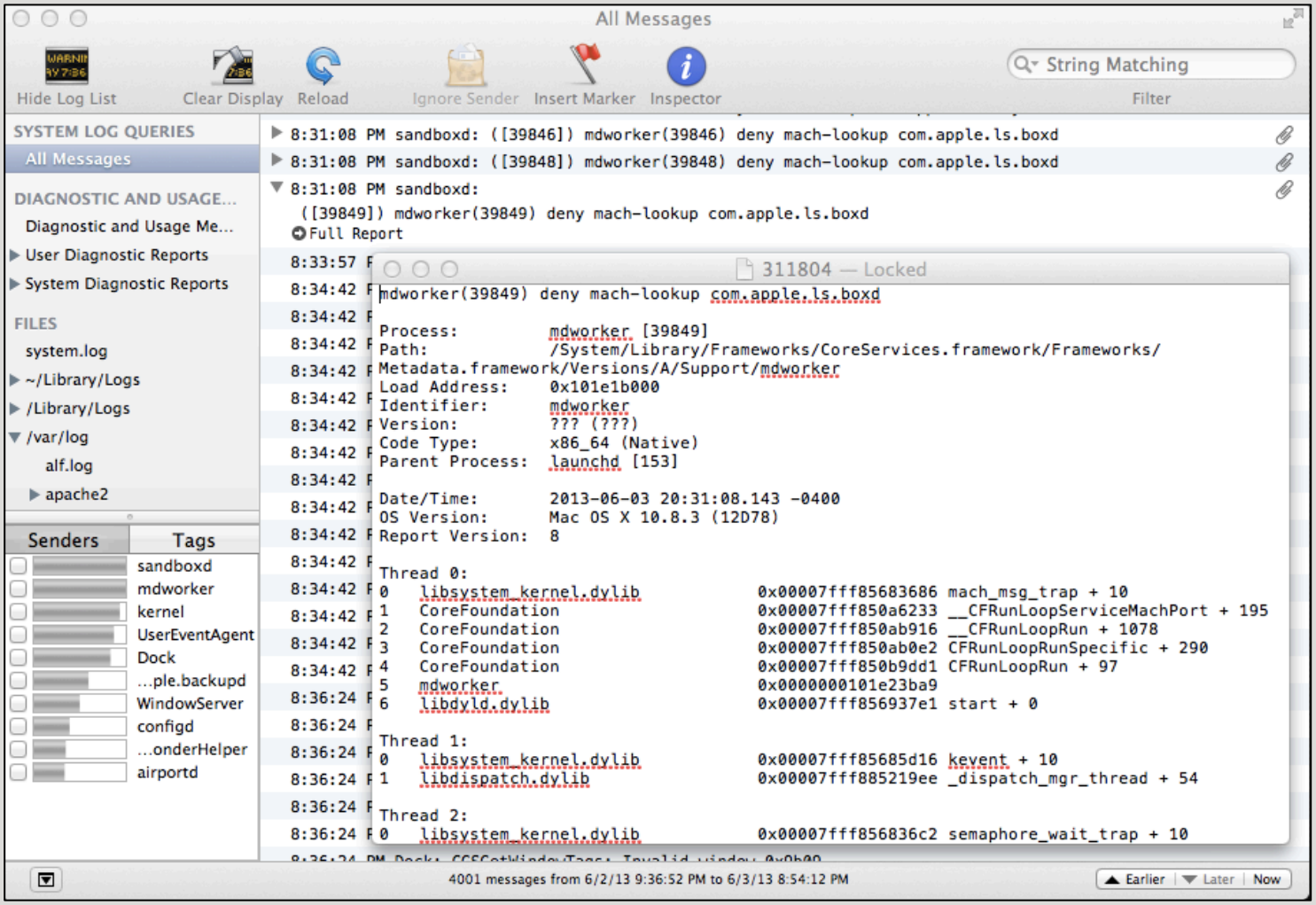
APPLE SYSTEM LOG FILE NAMES

- Filename Format: YYYY.MM.DD.[UID].[GID].asl
- BB – Best Before
- AUX - Auxiliary

```
nibble:AUX.2013.05.28 sledwards$ pwd
/var/log/asl/AUX.2013.05.28
nibble:AUX.2013.05.28 sledwards$ ls
281501  281597  281692  281790  281884
281503  281599  281698  281792  281886
281505  281604  281700  281794  281892
281511  281606  281702  281801  281894
281513  281608  281708  281803  281896
281515  281614  281710  281805  281902
281521  281616  281712  281810  281904
281523  281618  281718  281812  281906
281525  281624  281721  281814  281912
281531  281626  281723  281820  281914
```

```
May 28 23:57 2013.05.28.G80.asl
May 28 23:59 2013.05.28.U0.G80.asl
May 28 23:49 2013.05.28.U0.asl
May 28 22:15 2013.05.28.U501.asl
May 29 23:58 2013.05.29.G80.asl
May 29 23:58 2013.05.29.U0.G80.asl
May 29 22:45 2013.05.29.U0.asl
May 29 23:21 2013.05.29.U501.asl
May 30 23:57 2013.05.30.G80.asl
May 30 23:57 2013.05.30.U0.G80.asl
May 30 23:49 2013.05.30.U0.asl
May 30 22:41 2013.05.30.U501.asl
May 31 23:59 2013.05.31.G80.asl
May 31 23:59 2013.05.31.U0.G80.asl
May 31 22:52 2013.05.31.U0.asl
May 31 23:08 2013.05.31.U501.asl
Jun  1 23:59 2013.06.01.G80.asl
Jun  1 23:59 2013.06.01.U0.G80.asl
Jun  1 23:17 2013.06.01.U0.asl
Jun  1 21:45 2013.06.01.U501.asl
Jun  2 23:58 2013.06.02.G80.asl
Jun  2 23:58 2013.06.02.U0.G80.asl
Jun  2 23:06 2013.06.02.U0.asl
Jun  2 21:22 2013.06.02.U501.asl
Jun  3 20:08 2013.06.03.G80.asl
Jun  3 20:08 2013.06.03.U0.G80.asl
Jun  3 19:21 2013.06.03.U0.asl
Jun  3 10:57 2013.06.03.U200.asl
Jun  3 19:55 2013.06.03.U501.asl
May 28 23:56 AUX.2013.05.28
May 29 23:57 AUX.2013.05.29
May 30 23:56 AUX.2013.05.30
May 31 23:59 AUX.2013.05.31
Jun  1 23:58 AUX.2013.06.01
Jun  2 23:58 AUX.2013.06.02
Jun  3 20:08 AUX.2013.06.03
Mar 30 09:59 BB.2014.03.31.G80.asl
Apr 25 17:35 BB.2014.04.30.G80.asl
May 29 20:52 BB.2014.05.31.G80.asl
```

APPLE SYSTEM LOGS
AUXILIARY FILES



APPLE SYSTEM LOG RECORD FORMAT

```
5/7/13 9:27:03 PM login: DEAD_PROCESS: 97280 ttys002
5/7/13 9:27:03 PM login: DEAD_PROCESS: 97313 ttys004
5/7/13 10:03:36 PM login: USER_PROCESS: 98679 ttys002
5/9/13 7:04:01 PM login: USER_PROCESS: 4500 ttys004
5/9/13 7:04:01 PM login: DEAD_PROCESS: 4500 ttys004
5/9/13 9:13:38 PM login: USER_PROCESS: 4969 ttys004
5/10/13 6:18:21 PM login: DEAD_PROCESS: 4969 ttys004
5/10/13 9:00:19 PM login: USER_PROCESS: 7960 ttys004
5/10/13 9:10:51 PM login: DEAD_PROCESS: 7960 ttys004
5/16/13 10:29:47 PM login: USER_PROCESS: 25177 ttys004
5/16/13 10:29:59 PM login: DEAD_PROCESS: 76584 ttys003
5/16/13 10:36:26 PM login: USER_PROCESS: 37534 ttys003
5/18/13 10:23:22 PM login: DEAD_PROCESS: 76647 ttys000
5/18/13 10:23:22 PM login: DEAD_PROCESS: 91613 ttys001
5/18/13 10:23:22 PM login: DEAD_PROCESS: 25177 ttys004
5/18/13 10:23:22 PM login: DEAD_PROCESS: 98679 ttys002
5/18/13 10:23:22 PM login: DEAD_PROCESS: 37534 ttys003
5/18/13 10:23:26 PM loginwindow: DEAD_PROCESS: 55 console
5/18/13 10:25:07 PM loginwindow: USER_PROCESS: 59 console
5/18/13 10:25:08 PM login: USER_PROCESS: 236 ttys000
5/18/13 10:25:09 PM login: USER_PROCESS: 246 ttys001
5/18/13 10:25:09 PM login: USER_PROCESS: 254 ttys002
5/18/13 10:25:09 PM login: USER_PROCESS: 259 ttys003
```

Message Inspector

Key	Value
ASLExpireTime	1399856419
ASLMessageID	220267
Facility	com.apple.system.lastlog
GID	20
Host	nibble.blah
Level	5
PID	7960
ReadGID	80
Sender	login
Time	1368234019
TimeNanoSec	920375000
UID	0
ut_id	s004
ut_line	ttys004
ut_pid	7960
ut_tv.tv_sec	1368234019
ut_tv.tv_usec	918722
ut_type	7
ut_user	sledwards
Message	USER_PROCESS: 7960 ttys004

SYSLOG COMMAND

Output Format (-F)

- bsd
- std
- raw
- xml

Time Format (-T)

- sec
- local
- utc

File or Directory

- -f
- -d

```
sh-3.2# syslog -d asl/ | more
Mar 12 17:15:01 byte login[63585] <Notice>: USER_PROCESS: 63585 ttys003
Mar 15 01:41:32 byte login[48848] <Notice>: USER_PROCESS: 48848 ttys004
Mar 15 01:44:22 byte login[48905] <Notice>: USER_PROCESS: 48905 ttys005
Mar 15 01:52:19 byte login[48848] <Notice>: DEAD_PROCESS: 48848 ttys004
Mar 15 01:52:19 byte login[48905] <Notice>: DEAD_PROCESS: 48905 ttys005
Mar 15 01:52:21 byte login[48960] <Notice>: USER_PROCESS: 48960 ttys004
Mar 15 01:53:16 byte login[48960] <Notice>: DEAD_PROCESS: 48960 ttys004
Mar 15 01:53:18 byte login[50861] <Notice>: USER_PROCESS: 50861 ttys004
Mar 15 01:53:52 byte login[50861] <Notice>: DEAD_PROCESS: 50861 ttys004
Mar 15 01:53:53 byte login[52753] <Notice>: USER_PROCESS: 52753 ttys004
Mar 15 01:54:19 byte login[53625] <Notice>: USER_PROCESS: 53625 ttys005
```

syslog -T utc -F raw -d /asl

- [ASLMessageID 3553356]
- [Time 2012.05.28 19:39:32 UTC]
- [TimeNanoSec 887175000]
- [Level 5]
- [PID 908]
- [UID 0]
- [GID 20]
- [ReadGID 80]
- [Host byte]
- [Sender login]
- [Facility com.apple.system.utmpx]
- [Message DEAD_PROCESS: 908 ttys002]
- [ut_user oompa]
- [ut_id s002]
- [ut_line ttys002]
- [ut_pid 908]
- [ut_type 8]
- [ut_tv.tv_sec 1338233972]
- [ut_tv.tv_usec 886961]
- [ASLExpireTime 1369856372]

```
[ASLMessageID 23869] [Time 2013-03-17 20:12:49Z] [TimeNanoSec 649773000] [Level 5] [PID 21931] [
UID 0] [GID 20] [ReadGID 80] [Host nibble.blah] [Sender login] [Facility com.apple.system.utmpx]
 [Message DEAD_PROCESS: 21931 ttys003] [ut_user sledwards] [ut_id s003] [ut_line ttys003] [ut_pi
d 21931] [ut_type 8] [ut_tv.tv_sec 1363551169] [ut_tv.tv_usec 647288] [ASLExpireTime 1395173569]
[ASLMessageID 28599] [Time 2013-03-23 00:10:53Z] [TimeNanoSec 859756000] [Level 5] [PID 28503] [
UID 0] [GID 20] [ReadGID 80] [Host nibble.blah] [Sender login] [Facility com.apple.system.lastlo
g] [Message USER_PROCESS: 28503 ttys003] [ut_user sledwards] [ut_id s003] [ut_line ttys003] [ut_
pid 28503] [ut_type 7] [ut_tv.tv_sec 1363997453] [ut_tv.tv_usec 859054] [ASLExpireTime 139561985
3]
```

AUDIT LOGS

oompa@csh.rit.edu | @iamevltwin

AUDIT LOGS
/PRIVATE/VAR/AUDIT/*

Basic Security Module (BSM) Audit Logs

Binary Format

```
sh-3.2# xxd 20130307232230.20130308000749
0000000: 1400 0000 7d0b af67 0000 5139 2136 0000  ....}..g..Q9!6..
0000010: 02ed 7101 0000 0000 0000 0000 0007 7366  ..q...........sf
0000020: 6c61 6773 002d 0200 0000 0000 0b61 6d5f  lags.-.......am_
0000030: 7375 6363 6573 7300 2d03 0000 0000 000b  success.-.......
0000040: 616d 5f66 6169 6c75 7265 0024 ffff ffff  am_failure.$....
0000050: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000060: 0000 0000 0001 8703 0000 0000 0000 0000  ................
0000070: 2700 0000 0000 13b1 0500 0000 7d14 0000  '...........}...
0000080: 007d 0baf 6800 0051 392b d400 0003 e771  .}..h..Q9+.....q
0000090: 0100 0000 0000 0000 0000 0773 666c 6167  ...........sflag
00000a0: 7300 2d02 0000 0000 000b 616d 5f73 7563  s.-.......am_suc
00000b0: 6365 7373 002d 0300 0000 0000 0b61 6d5f  cess.-.......am_
00000c0: 6661 696c 7572 6500 24ff ffff ff00 0000  failure.$.......
00000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000e0: 0000 0187 0300 0000 0000 0000 0027 0000  .............'..
00000f0: 0000 0013 b105 0000 007d 1400 0000 7d0b  .........}....}.
0000100: af65 0000 5139 2bd5 0000 0000 7101 0000  .e..Q9+.....q...
0000110: 0000 0000 0000 0007 7366 6c61 6773 002d  ........sflags.-
0000120: 0200 0000 0000 0b61 6d5f 7375 6363 6573  .......am_succes
0000130: 7300 2d03 0000 0000 000b 616d 5f66 6169  s.-.......am_fai
0000140: 6c75 7265 0024 ffff ffff 0000 0000 0000  lure.$..........
0000150: 0000 0000 0000 0000 0000 0000 0000 0001  ................
0000160: 8705 0000 0000 0000 0000 2700 0000 0000  ..........'.....
0000170: 13b1 0500 0000 7d                        ......}
```

AUDIT LOGS – AUDIT TRAIL FILES

StartTime.EndTime

YYYYMMDDHHMMSS.YYYYMMDDHHMMSS

Other Filenames:

- “current”
- *.not_terminated
- *.crash_recovery

```
drwx------   8 root  wheel    272 May 28 15:22 .
drwxr-xr-x  29 root  wheel    986 May  9 21:39 ..
-r--r-----   1 root  wheel  48987 May 10 00:46 20120509232853.20120510044637
-r--r-----   1 root  wheel  57158 May 12 11:31 20120510204054.20120512153135
-r--r-----   1 root  wheel  92166 May 27 20:02 20120512153220.20120528000216
-r--r-----   1 root  wheel  20805 May 28 15:20 20120528000250.20120528192006
-r--r-----   1 root  wheel   4619 May 28 21:07 20120528192235.not_terminated
lrwxr-xr-x   1 root  wheel     40 May 28 15:22 current -> /var/audit/20120528192235.not_terminated
```

praudit -xn /var/audit/*

SU EXAMPLE:

```
<record version="11" event="user authentication" modifier="0"
time="Mon May 28 21:12:51 2012" msec=" + 41 msec" >
<subject audit-uid="501" uid="0" gid="20" ruid="501" rgid="20"
pid="552" sid="100004" tid="552 0.0.0.0" />
<text>Verify password for record type Users &apos;root&apos;
node &apos;/Local/Default&apos;</text>
<return errval="success" retval="0" />
</record>

<record version="11" event="user authentication" modifier="0"
time="Mon May 28 21:12:55 2012" msec=" + 449 msec" >
<subject audit-uid="501" uid="0" gid="20" ruid="501" rgid="20"
pid="554" sid="100004" tid="554 0.0.0.0" />
<text>Verify password for record type Users &apos;root&apos;
node &apos;/Local/Default&apos;</text>
<return errval="failure: Unknown error: 255" retval="5000" />
</record>
```

AUDIT LOG RECORDS

- Each record is made up of “tokens”

Header

```
<record version="11" event="user
authentication" modifier="0" time="Mon May 28
21:12:51 2012" msec=" + 41 msec" >
```

Subject

```
<subject audit-uid="501" uid="0" gid="20"
ruid="501" rgid="20" pid="552" sid="100004"
tid="552 0.0.0.0" />
```

Text

```
<text>Verify password for record type Users
&apos;root&apos; node &apos;/Local/
Default&apos;</text>
```

Return

```
<return errval="success" retval="0" />
```

Trailer

```
</record>
```

AUDIT LOG RECORD - TOKENS

Variable number of tokens

Subject Token

The ``subject'' token contains information on the subject performing the operation described by an audit record, and includes similar information to that found in the ``process'' and ``expanded process'' tokens. However, those tokens are used where the process being described is the target of the operation, not the authorizing party. A ``subject'' token can be created using au_to_subject32(3) and au_to_subject64(3).

Field	Bytes	Description
Token ID	1 byte	Token ID
Audit ID	4 bytes	Audit user ID
Effective User ID	4 bytes	Effective user ID
Effective Group ID	4 bytes	Effective group ID
Real User ID	4 bytes	Real user ID
Real Group ID	4 bytes	Real group ID
Process ID	4 bytes	Process ID
Session ID	4 bytes	Audit session ID
Terminal Port ID	4/8 bytes	Terminal port ID (32/64-bits)
Terminal Machine Address	4 bytes	IP address of machine

VOLUMES

oompa@csh.rit.edu | @iamevltwin

SYSTEM.LOG & DAILY.LOG SEARCH "/VOLUMES/"

```
May 19 08:58:23 bit fseventsd[20]: log dir: /Volumes/Time Machine Backups/.fseventsd getting new uuid: 5420A642-DE8C-4B90-B2B4-B948288F5E3F
May 19 16:52:30 bit fseventsd[20]: log dir: /Volumes/NO NAME/.fseventsd getting new uuid: DD64986D-F58C-407B-901B-5BD27104F062
May 23 20:10:35 bit fseventsd[20]: log dir: /Volumes/NO NAME/.fseventsd getting new uuid: 0D8CB03B-0691-4381-ACEF-8F7F421D12DF
May 26 14:01:03 bit fseventsd[20]: log dir: /Volumes/WDPassport/.fseventsd getting new uuid: CDCE4339-A254-4925-A909-97B4553BDAC1
May 26 15:40:38 bit fseventsd[20]: log dir: /Volumes/WDPassport/.fseventsd getting new uuid: D4FFFBA2-16A8-4CB3-88DE-327CDE1551EC
```

```
Fri May 11 17:12:29 EDT 2012

Removing old temporary files:

Cleaning out old system announcements:

Removing stale files from /var/rwho:

Removing scratch fax files

Disk status:
Filesystem                          Size   Used  Avail Capacity  Mounted on
/dev/disk0s2                       698Gi   22Gi  675Gi     4%    /
localhost:/35wJAmjuh-MSBDh6mJulon  698Gi  698Gi    0Bi   100%    /Volumes/MobileBackups
/dev/disk6s2                       107Mi  107Mi    0Bi   100%    /Volumes/Google Chrome
```

KERNEL.LOG & SYSTEM.LOG SEARCH "USBMSC"

- Serial Number, Vendor ID, Product ID, Version
- <=10.7 – This data is found in the kernel.log
- 10.8+ – This data resides in the system.log

```
Apr 25 12:27:11 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:32:31 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:47:29 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:49:43 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:52:46 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
Apr 25 12:53:37 Pro kernel[0]: USBMSC Identifier (non-unique): ABCDEF0123456789 0xe90 0x5 0x0
Apr 25 13:04:21 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 13:04:29 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
Apr 26 12:36:05 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 27 09:02:59 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
Apr 30 09:07:14 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
May  3 05:43:05 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
May  3 06:24:05 Pro kernel[0]: USBMSC Identifier (non-unique): SWOC22905731 0x1199 0xfff 0x323
May 24 11:22:43 Pro kernel[0]: USBMSC Identifier (non-unique): 000000009833 0x5ac 0x8403 0x9833
May 24 11:53:25 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
May 25 12:48:38 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
May 30 06:50:01 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
May 31 13:10:09 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
Jun  1 07:16:03 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
```

USBMSC - KERNEL.LOG & SYSTEM.LOG SYSTEM INFORMATION

```
Jun  3 11:11:53 bit kernel[0]: USBMSC Identifier (non-
unique): FBF1011220504638 0x90c 0x1000 0x1100
```

Flash Disk:

Capacity:	8.02 GB (8,019,509,248 bytes)
Removable Media:	Yes
Detachable Drive:	Yes
BSD Name:	disk2
Product ID:	0x1000
Vendor ID:	0x090c (Silicon Motion, Inc. - Taiwan)
Version:	11.00
Serial Number:	FBF1011220504638
Speed:	Up to 480 Mb/sec
Manufacturer:	USB
Location ID:	0xfd130000 / 5
Current Available (mA):	500
Current Required (mA):	500
Partition Map Type:	MBR (Master Boot Record)
S.M.A.R.T. status:	Not Supported
Volumes:	
BLACKBAG:	
Capacity:	8.02 GB (8,019,476,992 bytes)
Available:	7.87 GB (7,868,444,672 bytes)
Writable:	Yes
File System:	MS-DOS FAT32
BSD Name:	disk2s1
Mount Point:	/Volumes/BLACKBAG
Content:	DOS_FAT_32

SYSTEM.LOG
SEARCH “HFS:” OR “[UN]MOUNT”

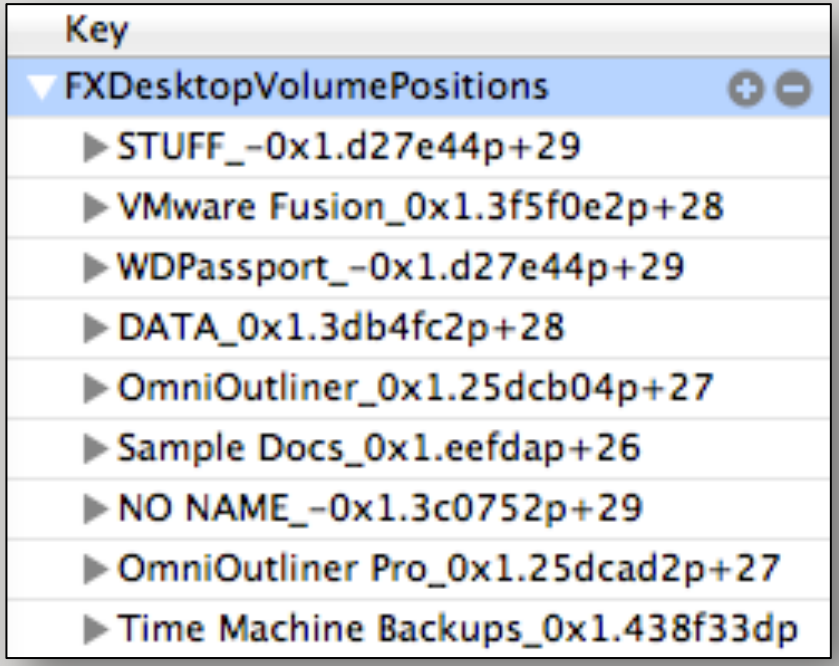
- Mounted Devices
- /dev/disk#s#
- Determine how long a volume was mounted

```
May 18 02:01:11 word kernel[0]: hfs: mounted Recovery HD on device disk0s3
May 18 02:01:11 word kernel[0]: hfs: unmount initiated on Recovery HD on device disk0s3
May 18 19:25:26 word kernel[0]: hfs: mounted Recovery HD on device disk0s3
May 18 19:25:27 word kernel[0]: hfs: unmount initiated on Recovery HD on device disk0s3
May 18 19:58:15 word kernel[0]: hfs: Removed 0 orphaned / unlinked files and 3 directori
May 18 19:58:15 word kernel[0]: hfs: mounted DATA on device disk3s2
May 18 20:34:41 word kernel[0]: hfs: unmount initiated on DATA on device disk3s2
May 18 22:30:01 word kernel[0]: hfs: mounted Recovery HD on device disk0s3
May 18 22:30:02 word kernel[0]: hfs: unmount initiated on Recovery HD on device disk0s3
```

~/LIBRARY/PREFERENCES/ COM.APPLE.FINDER.PLIST

- FXDesktopVolumePositions
- FXRecentFolders (10 most recent)
- Item 0 = Most Recently Accessed Item

▼ FXRecentFolders	Array	(10 items)
▼ Item 0	Diction…	(2 items)
file-bookmark	Data	<626f6f6b ac030000
name	String	STUFF
▼ Item 1	Diction…	(2 items)
file-bookmark	Data	<626f6f6b 3c030000
name	String	TechnoSecurity2012
▼ Item 2	Diction…	(2 items)
file-bookmark	Data	<626f6f6b 8c020000
name	String	oompa
▼ Item 3	Diction…	(2 items)
file-bookmark	Data	<626f6f6b c0020000
name	String	Dropbox

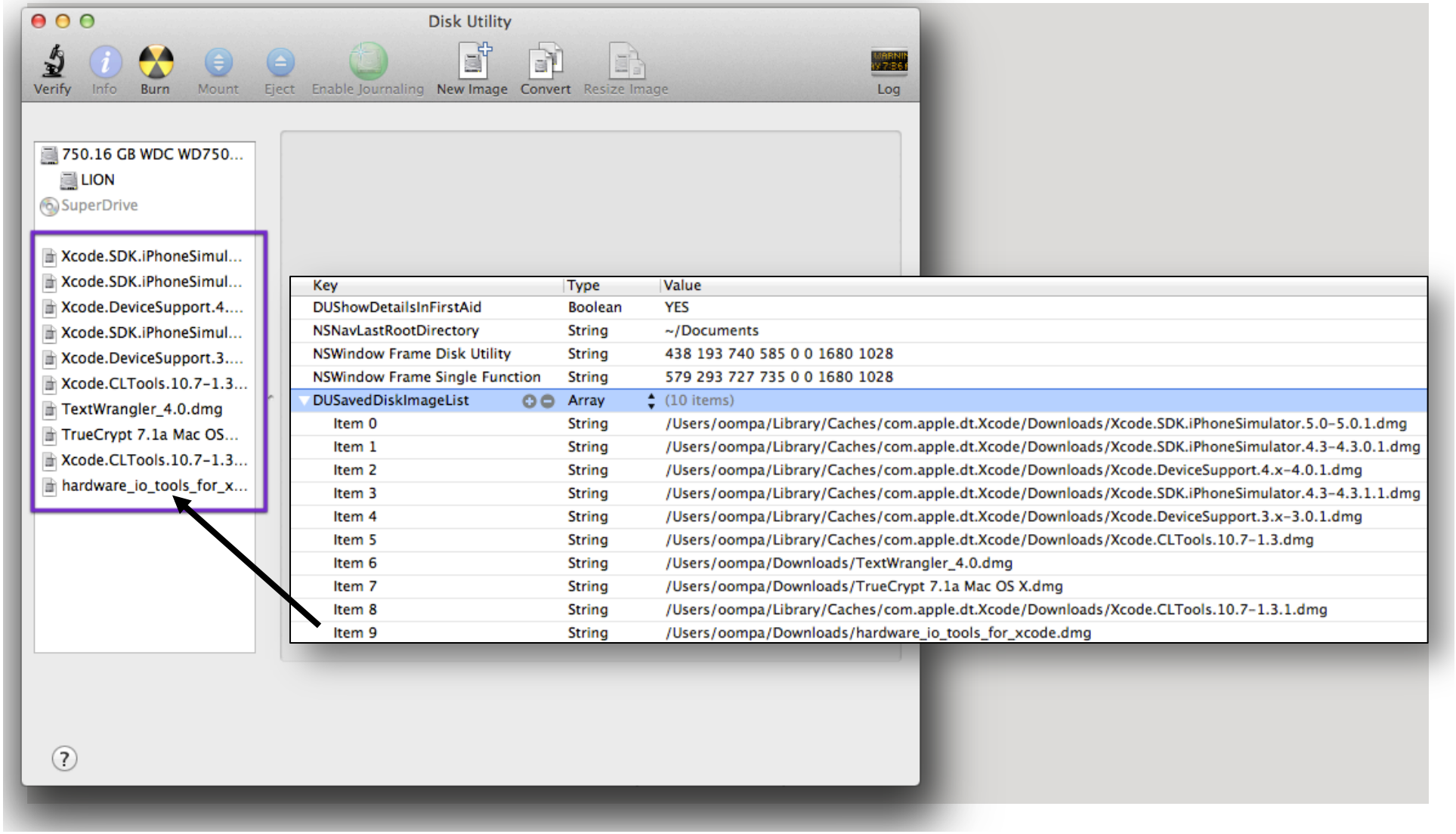


FINDER – DESKTOP VOLUMES
~/LIBRARY/PREFERENCES/ COM.APPLE.FINDER.PLIST

FXDesktopVolumePositions

▼ FXDesktopVolumePositions	Dictionary	(68 items)
▶ FAT32_WIN_-0x1.d27e44p+29	Dictionary	(4 items)
▶ MacQuisition	Dictionary	(4 items)
▶ PenTablet_0x1.5dd99bbp+28	Dictionary	(4 items)
▶ TextWrangler 4.0_0x1.517f6b7p	Dictionary	(4 items)
▼ HFS_APM_0x1.5aa61c9p+28	Dictionary	(4 items)
xRelative	Number	-166
ScreenID	Number	0
AnchorRelativeTo	Number	1
yRelative	Number	62
▶ Firefox_0x1.5423ffbp+28	Dictionary	(4 items)
▶ Useful Scripts_0x1.8b017bap+27	Dictionary	(4 items)
▶ Tiger_-0x1.7476c46p+29	Dictionary	(4 items)
▶ Microsoft Office	Dictionary	(4 items)
▶ MacResponse_0x1.561bebdp+28	Dictionary	(4 items)
▶ Untitled_0x1.55b30ddp+28	Dictionary	(4 items)
▶ TrueCrypt 7.1a_0x1.4e12977p+28	Dictionary	(4 items)
▶ BLACKBAG_-0x1.d27e44p+29	Dictionary	(4 items)
▶ HFS_GUID_0x1.5aa6206p+28	Dictionary	(4 items)
▶ Dropbox Installer_0x1.6978e77p	Dictionary	(4 items)
▶ STUFF_-0x1.d27e44p+29	Dictionary	(4 items)

~/LIBRARY/PREFERENCES/ COM.APPLE.DISKUTILITY.PLIST



~/LIBRARY/PREFERENCES/ COM.APPLE.SIDEBARLISTS.PLIST

Key	Type	Value
▼ favorites	Diction…	(7 items)
▶ CustomListProperties	Diction…	(2 items)
ShowRemovable	Boolean	YES
ShowHardDisks	Boolean	YES
ShowEjectables	Boolean	YES
▶ VolumesList	Array	(57 items)
ShowServers	Boolean	YES
Controller	String	VolumesList
▶ savedsearches	Diction…	(2 items)
▼ systemitems	Diction…	(7 items)
▶ CustomListProperties	Diction…	(1 item)
ShowRemovable	Boolean	YES
ShowHardDisks	Boolean	YES
ShowEjectables	Boolean	YES
▶ VolumesList	Array	(42 items)
ShowServers	Boolean	YES
Controller	String	VolumesList

▼ VolumesList	Array	(42 items)
▶ Item 0	Diction…	(4 items)
▶ Item 1	Diction…	(5 items)
▶ Item 2	Diction…	(3 items)
▶ Item 3	Diction…	(4 items)
▶ Item 4	Diction…	(5 items)
▶ Item 5	Diction…	(4 items)
▼ Item 6	Diction…	(3 items)
Alias	Data	<00000000 00b40003 00010000 cbc9d31f 0000482b
Name	String	Dropbox Installer
EntryType	Number	1027
▼ Item 7	Diction…	(3 items)
Alias	Data	<00000000 00a00003 00010000 cbc0e521 0000482b
Name	String	Google Chrome
EntryType	Number	1027
▼ Item 8	Diction…	(3 items)
Alias	Data	<00000000 00740003 00010000 ca50c8c2 0000482b
Name	String	DATA
EntryType	Number	517

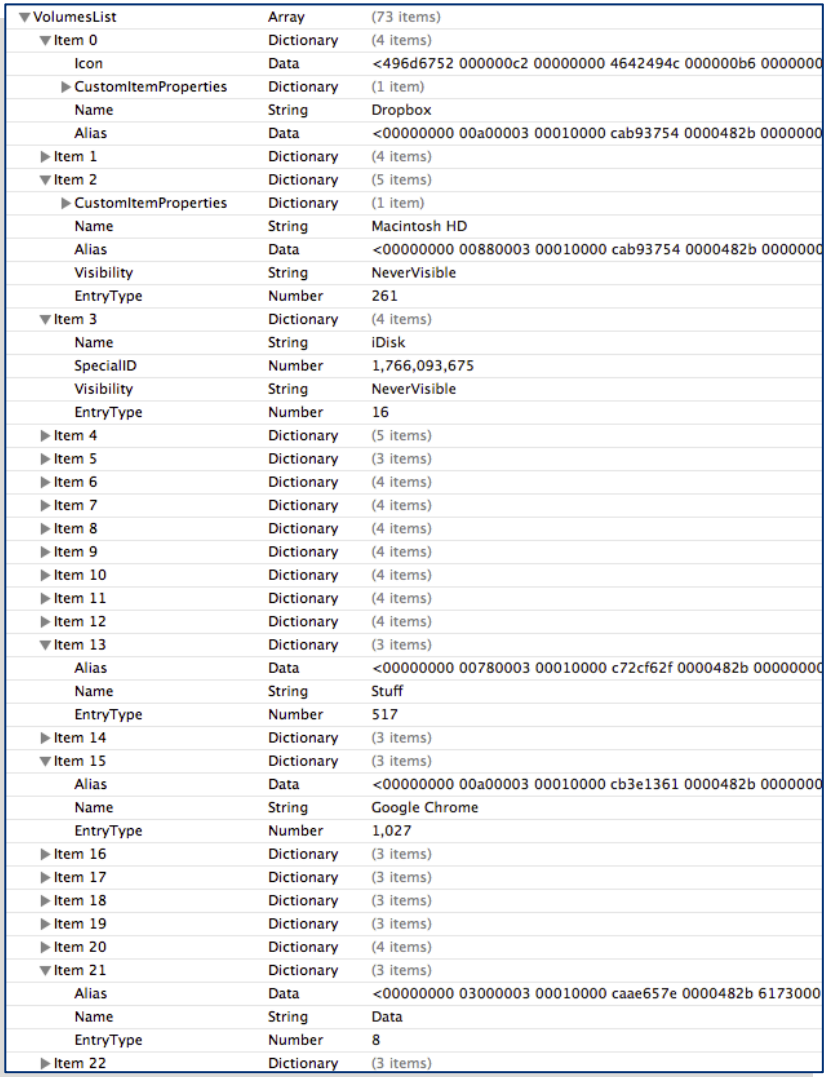
oompa@csh.rit.edu | @iamevltwin

FINDER SIDEBAR – FAVORITES & SYSTEM ITEMS
~/LIBRARY/PREFERENCES/COM.APPLE.SIDEBARLISTS.PLIST

▼ favorites	Dictionary	(7 items)
▼ CustomListProperties	Dictionary	(2 items)
com.apple.LSSharedFileList.VolumesListMigrated	Boolean	YES
com.apple.LSSharedFileList.Restricted.upgraded	Boolean	YES
ShowRemovable	Boolean	YES
ShowHardDisks	Boolean	YES
ShowEjectables	Boolean	YES
▶ VolumesList	Array	(73 items)
ShowServers	Boolean	YES
Controller	String	VolumesList

FINDER SIDEBAR – VOLUMES LIST ~/LIBRARY/PREFERENCES/ COM.APPLE.SIDEBARLISTS.PLIST

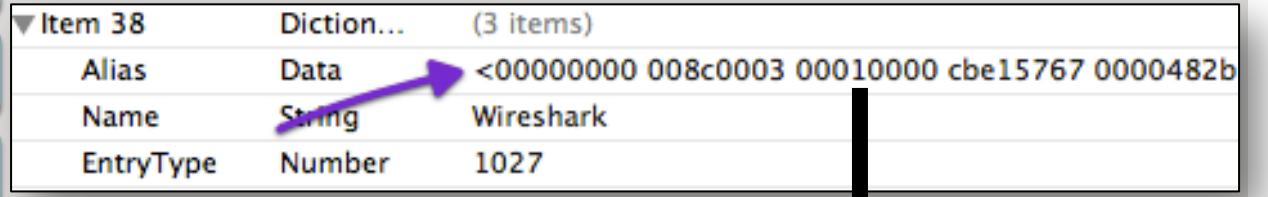
Volume EntryType	
8	• Time Machine (AFPFS), AFP File Shares, OSXFUSE Volumes
16	• Network Hard Drive, iDisk, “Computer”
128	• “iDisk”
261	• Hard Drive, Boot Hard Drive
515	• USB Flash, Time Machine Backups, Disk Image (HFS, MBR)
517	• USB Hard Drive (FAT/ExFAT/HFS+)
1024	• “Remote Disk”
1027	• Disk Image (Bzip, VAX COFF Executable), DVD
1029	• External HDD (NTFS)

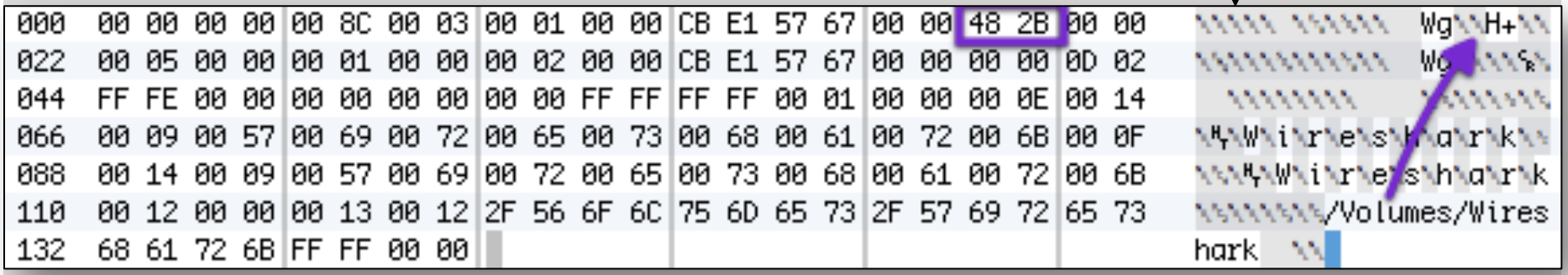


▼ VolumesList	Array	(73 items)
▼ Item 0	Dictionary	(4 items)
Icon	Data	<496d6752 000000c2 00000000 4642494c 000000b6 0000000
▶ CustomItemProperties	Dictionary	(1 item)
Name	String	Dropbox
Alias	Data	<00000000 00a00003 00010000 cab93754 0000482b 0000000
▶ Item 1	Dictionary	(4 items)
▼ Item 2	Dictionary	(5 items)
▶ CustomItemProperties	Dictionary	(1 item)
Name	String	Macintosh HD
Alias	Data	<00000000 00880003 00010000 cab93754 0000482b 0000000
Visibility	String	NeverVisible
EntryType	Number	261
▼ Item 3	Dictionary	(4 items)
Name	String	iDisk
SpecialID	Number	1,766,093,675
Visibility	String	NeverVisible
EntryType	Number	16
▶ Item 4	Dictionary	(5 items)
▶ Item 5	Dictionary	(3 items)
▶ Item 6	Dictionary	(4 items)
▶ Item 7	Dictionary	(4 items)
▶ Item 8	Dictionary	(4 items)
▶ Item 9	Dictionary	(4 items)
▶ Item 10	Dictionary	(4 items)
▶ Item 11	Dictionary	(4 items)
▶ Item 12	Dictionary	(4 items)
▼ Item 13	Dictionary	(3 items)
Alias	Data	<00000000 00780003 00010000 c72cf62f 0000482b 0000000
Name	String	Stuff
EntryType	Number	517
▶ Item 14	Dictionary	(3 items)
▼ Item 15	Dictionary	(3 items)
Alias	Data	<00000000 00a00003 00010000 cb3e1361 0000482b 0000000
Name	String	Google Chrome
EntryType	Number	1,027
▶ Item 16	Dictionary	(3 items)
▶ Item 17	Dictionary	(3 items)
▶ Item 18	Dictionary	(3 items)
▶ Item 19	Dictionary	(3 items)
▶ Item 20	Dictionary	(4 items)
▼ Item 21	Dictionary	(3 items)
Alias	Data	<00000000 03000003 00010000 caae657e 0000482b 6173000
Name	String	Data
EntryType	Number	8
▶ Item 22	Dictionary	(3 items)

VOLUME ALIAS DATA
VOLUME FORMAT

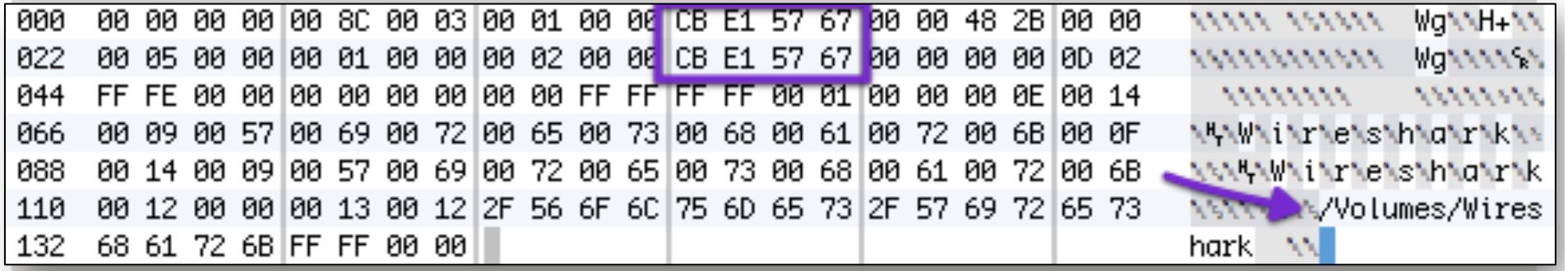
- BDxF - ExFAT
- BDIS – FAT32
- BDcu –UDF (DVD)
- NTcu - Unknown
- H+ - HFS





VOLUME ALIAS DATA
DATES & MOUNT POINT

- Volume Name
- Mount Point
- File Creation Time (HFS+ Date)
- May or may not be present
  - Only seen on H+ formatted disks
  - DMG
  - USB



APPLE FILING PROTOCOL (AFP) NETWORK SHARES – SEARCH "AFP_VFS"

```
Jun 15 21:00:01 nibble kernel[0]: AFP_VFS afpfs_mount: /Volumes/
Macintosh HD-1, pid 860
Jun 15 21:00:01 nibble kernel[0]: AFP_VFS afpfs_mount : succeeded
on volume 0xffffff80d5a33008 /Volumes/Macintosh HD-1 (error = 0,
retval = 0)
Jun 15 21:00:59 nibble kernel[0]: AFP_VFS afpfs_unmount: /Volumes/
Macintosh HD-1, flags 0, pid 879
Jun 15 21:00:59 nibble kernel[0]: AFP_VFS afpfs_unmount : We are
the last mnt/sbmnt using volume /Volumes/Macintosh HD-1
0xffffff80d5a33008
Jun 15 21:00:59 nibble kernel[0]: AFP_VFS afpfs_unmount : We are
the last volume using socket /Volumes/Macintosh HD-1
0xffffff80d5a33008
Jun 15 21:00:59 nibble kernel[0]: AFP_VFS afpfs_unmount :
afpfs_DoReconnect sent signal for unmount to proceed
```

SMB Shares are Similar

oompa@csh.rit.edu | @iamevltwin

NETWORK INFORMATION

oompa@csh.rit.edu | @iamevltwin

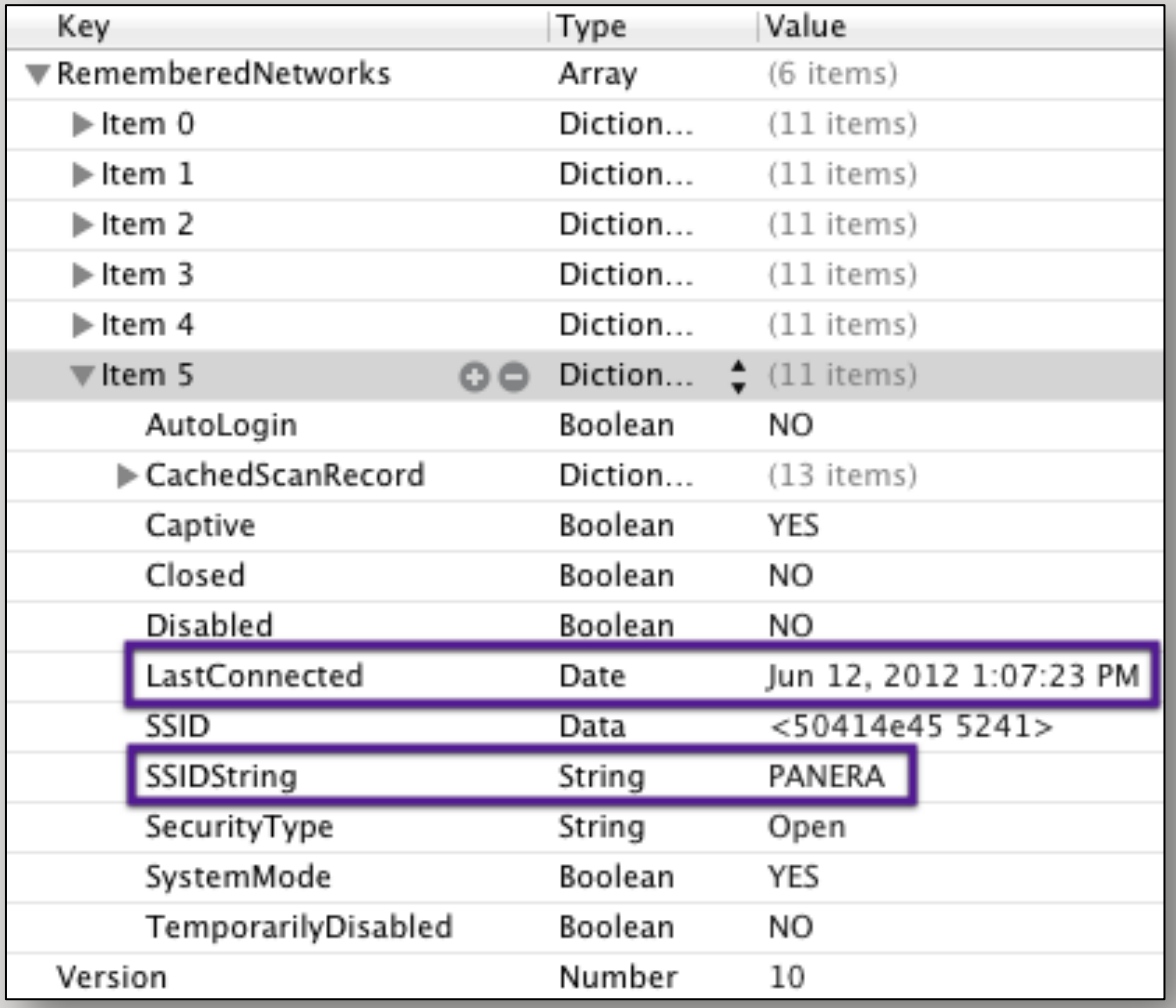
NETWORK CHANGES
SYSTEM.LOG – SEARCH "CONFIGD"

```
Jun 12 13:07:11 bit configd[16]: network configuration changed.
Jun 12 13:07:11 bit configd[16]: setting hostname to "bit.local"
Jun 12 13:07:11 bit configd[16]: network configuration changed.
Jun 12 13:07:28 bit configd[16]: network configuration changed.
```

SYSTEM.LOG
SEARCH “AIRPORTD”

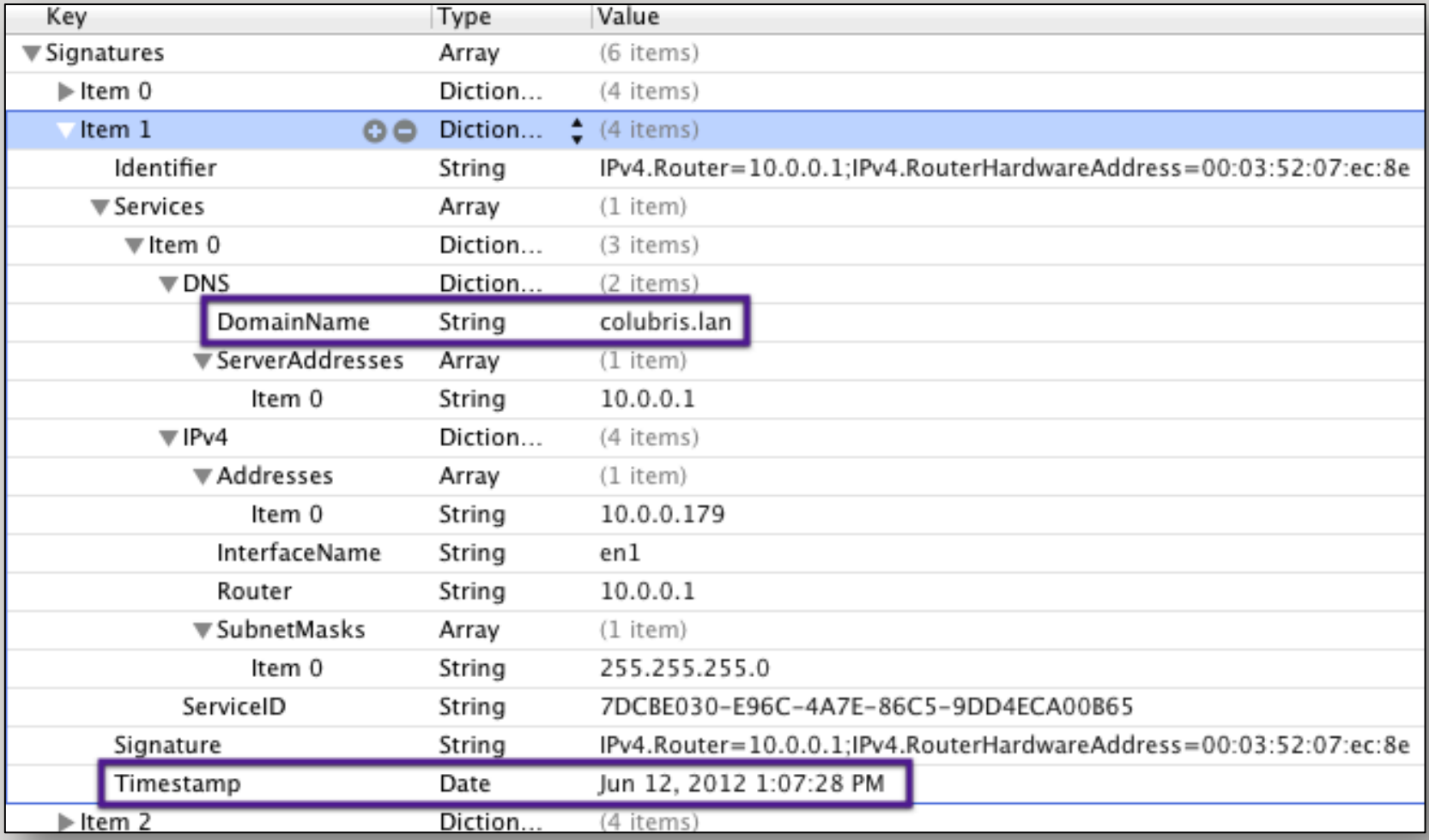
```
Jun 12 10:17:24 bit airportd[36]: _doAutoJoin: Already associated to “veyron”.
Bailing on auto-join.
Jun 12 11:43:17 bit airportd[3105]: _doAutoJoin: Already associated to “veyron”.
Bailing on auto-join.
Jun 12 13:07:24 bit airportd[3218]: _doAutoJoin: Already associated to “PANERA”.
Bailing on auto-join.
Jun 12 13:07:29 bit airportd[3218]: _doAutoJoin: Already associated to “PANERA”.
Bailing on auto-join.
Jun 12 14:51:42 bit airportd[3756]: _processSystemPSKAssoc: No password for
network <CWNetwork: 0x7f8083c189b0> [ssid=L.A. Boxing Customer WIFI,
bssid=00:21:29:d5:20:12, security=WPA/WPA2 Personal, rssi=-92,
channel=<CWChannel: 0x7f8085106d90> [channelNumber=6(2GHz),
channelWidth={20MHz}], ibss=0] in the system keychain
Jun 12 16:49:03 bit airportd[3769]: _doAutoJoin: Already associated to “veyron”.
Bailing on auto-join.
```

/LIBRARY/PREFERENCES/SYSTEMCONFIGURATION/ COM.APPLE.AIRPORT.PREFERENCES.PLIST



Key	Type	Value
▼ RememberedNetworks	Array	(6 items)
▶ Item 0	Diction…	(11 items)
▶ Item 1	Diction…	(11 items)
▶ Item 2	Diction…	(11 items)
▶ Item 3	Diction…	(11 items)
▶ Item 4	Diction…	(11 items)
▼ Item 5	Diction…	(11 items)
AutoLogin	Boolean	NO
▶ CachedScanRecord	Diction…	(13 items)
Captive	Boolean	YES
Closed	Boolean	NO
Disabled	Boolean	NO
LastConnected	Date	Jun 12, 2012 1:07:23 PM
SSID	Data	<50414e45 5241>
SSIDString	String	PANERA
SecurityType	String	Open
SystemMode	Boolean	YES
TemporarilyDisabled	Boolean	NO
Version	Number	10

/LIBRARY/PREFERENCES/SYSTEMCONFIGURATION/COM.APPLE.NETWORK.IDENTIFICATION.PLIST



Key	Type	Value
▼Signatures	Array	(6 items)
▶Item 0	Diction…	(4 items)
▼Item 1	Diction…	(4 items)
Identifier	String	IPv4.Router=10.0.0.1;IPv4.RouterHardwareAddress=00:03:52:07:ec:8e
▼Services	Array	(1 item)
▼Item 0	Diction…	(3 items)
▼DNS	Diction…	(2 items)
DomainName	String	colubris.lan
▼ServerAddresses	Array	(1 item)
Item 0	String	10.0.0.1
▼IPv4	Diction…	(4 items)
▼Addresses	Array	(1 item)
Item 0	String	10.0.0.179
InterfaceName	String	en1
Router	String	10.0.0.1
▼SubnetMasks	Array	(1 item)
Item 0	String	255.255.255.0
ServiceID	String	7DCBE030-E96C-4A7E-86C5-9DD4ECA00B65
Signature	String	IPv4.Router=10.0.0.1;IPv4.RouterHardwareAddress=00:03:52:07:ec:8e
Timestamp	Date	Jun 12, 2012 1:07:28 PM
▶Item 2	Diction…	(4 items)

NETWORK INFORMATION – CONFIGURATION

/LIBRARY/PREFERENCES/SYSTEMCONFIGURATION/ PREFERENCES.PLIST

▼ 29A1FDC6-B462-4518-...	Dictionary	(7 items)
▼ DNS	Dictionary	(1 item)
▼ ServerAddresses	Array	(0 items)
▼ IPv4	Dictionary	(1 item)
ConfigMethod	String	DHCP
▼ IPv6	Dictionary	(2 items)
ConfigMethod	String	Automatic
__INACTIVE__	Boolean	YES
▼ Interface	Dictionary	(4 items)
DeviceName	String	en0
Hardware	String	AirPort
Type	String	Ethernet
UserDefinedName	String	Wi-Fi
▼ Proxies	Dictionary	(2 items)
▼ ExceptionsList	Array	(2 items)
Item 0	String	*.local
Item 1	String	169.254/16
FTPPassive	Number	1
▼ SMB	Dictionary	(1 item)
NetBIOSName	String	nibble
UserDefinedName	String	Wi-Fi

▼ CE4DF79D-2811-444D-...	Dictionary	(7 items)
▼ DNS	Dictionary	(0 items)
▼ IPv4	Dictionary	(4 items)
▼ Addresses	Array	(1 item)
Item 0	String	192.168.123.123
ConfigMethod	String	Manual
Router	String	192.168.1.254
▼ SubnetMasks	Array	(1 item)
Item 0	String	255.255.255.0
▼ IPv6	Dictionary	(1 item)
ConfigMethod	String	Automatic
▼ Interface	Dictionary	(4 items)
DeviceName	String	en4
Hardware	String	Ethernet
Type	String	Ethernet
UserDefinedName	String	Thunderbolt Ethernet
▼ Proxies	Dictionary	(2 items)
▼ ExceptionsList	Array	(2 items)
Item 0	String	*.local
Item 1	String	169.254/16
FTPPassive	Number	1
▼ SMB	Dictionary	(0 items)
UserDefinedName	String	Thunderbolt Ethernet

NETWORK INFORMATION – DHCP ADDRESSES /PRIVATE/VAR/DB/DHCPCLIENT/LEASES/

```
bash-3.2# pwd
/private/var/db/dhcpclient/leases
bash-3.2# ls -l
total 16
-rw-r--r--  1 root  wheel  969 May 10 10:20 en0-1,b8:e8:56:37:ec:6
-rw-r--r--  1 root  wheel  927 Feb 18 20:48 en4-1,68:5b:35:91:1a:b5
bash-3.2# plutil -p en4-1\,68\:5b\:35\:91\:1a\:b5
{
  "LeaseStartDate" => 2014-02-19 01:39:52 +0000
  "RouterHardwareAddress" => <e0699550 4c06>
  "IPAddress" => "192.168.1.237"
  "LeaseLength" => 43200
  "RouterIPAddress" => "192.168.1.254"
  "PacketData" => <02010600 7a48b9f4 000d0000 00000000 c0a801ed c0a801fe 00000000 685b3591 1ab
50000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 0000000
0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00
000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000000
00 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 0
0000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 63825363 35010
536 04c0a801 fe330400 00a8c03a 04000054 603b0400 0093a801 04ffffff 001c04c0 a801ff03 04c0a801
fe0604c0 a801feff 00000000 00000000>
}
```

DETERMINE "HOME" NETWORK

com.apple.airport.preferences.plist

- "Item 0"
- SecurityType != OPEN
  - "OPEN" generally seen at wifi hotspots
  - Example: My home network is "WPA2 Personal"

system.log

- More entries than most others when "airportd" searched for.

LOCATIONAL DATA

oompa@csh.rit.edu | @iamevltwin

DETAILED TIMELINE
SYSTEM.LOG - SEARCH "AIRPORTD"

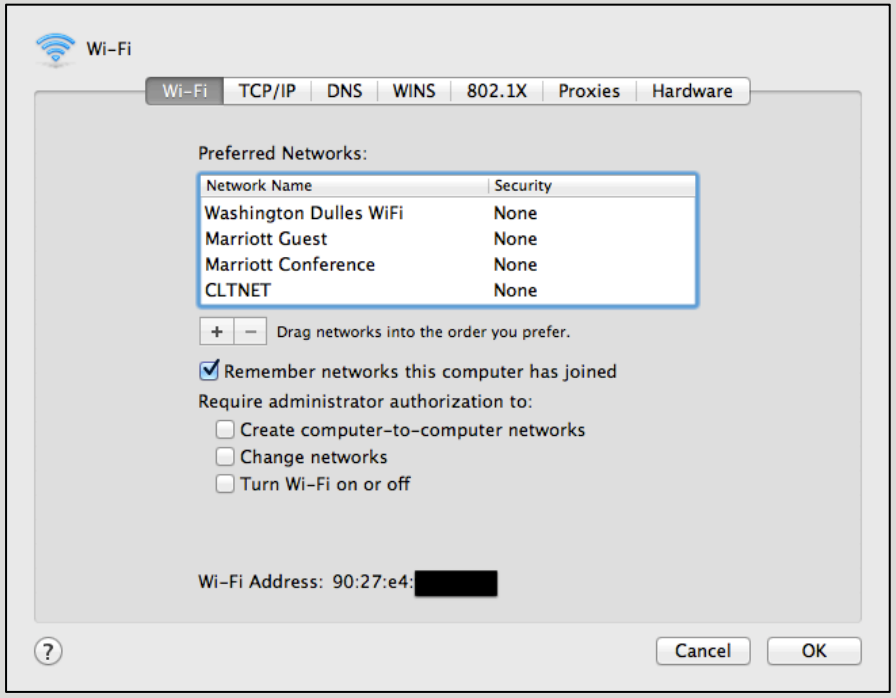
```
Jun  1 19:52:04 bit airportd[3492]: _doAutoJoin: Already associated to "veyron". Bailing on auto-join.
Jun  2 07:24:23 bit airportd[3848]: _doAutoJoin: Already associated to "Washington Dulles WiFi". Bailing on auto-join.
Jun  2 14:44:32 bit airportd[4944]: _doAutoJoin: Already associated to "Marriott Guest". Bailing on auto-join.
Jun  3 17:12:14 bit airportd[6538]: _doAutoJoin: Already associated to "Marriott Guest". Bailing on auto-join.
Jun  4 01:33:29 bit airportd[7841]: _doAutoJoin: Already associated to "Marriott Guest". Bailing on auto-join.
Jun  5 08:50:16 bit airportd[17054]: _doAutoJoin: Already associated to "Marriott Guest". Bailing on auto-join.
Jun  6 13:34:01 bit airportd[20160]: _doAutoJoin: Already associated to "Marriott Guest". Bailing on auto-join.
Jun  6 13:34:40 bit airportd[20160]: _doAutoJoin: Already associated to "Marriott Conference". Bailing on auto-join.
Jun  6 17:40:23 bit airportd[20286]: _doAutoJoin: Already associated to "CLTNET". Bailing on auto-join.
Jun  9 09:24:24 bit airportd[25724]: _doAutoJoin: Already associated to "veyron". Bailing on auto-join.
Jun 12 13:07:24 bit airportd[3218]: _doAutoJoin: Already associated to "PANERA". Bailing on auto-join.
Jun 12 16:49:03 bit airportd[3769]: _doAutoJoin: Already associated to "veyron". Bailing on auto-join.
```

oompa@csh.rit.edu | @iamevltwin

WIRELESS NETWORKS

/LIBRARY/PREFERENCES/SYSTEMCONFIGURATION/COM.APPLE.AIRPORT.PREFERENCES.PLIST

- Determine general location based upon SSID
- Last Connected Time
- Local System Time



oompa@csh.rit.edu | @iamevltwin

TRAVEL TIMELINE

oompa@csh.rit.edu | @iamevltwin

COUNTRY CODES - KERNEL.LOG & SYSTEM.LOG SEARCH “COUNTRY CODE”

```
Sep  1 17:42:13 MBP kernel[0]: en1: 802.11d country code set to 'AU'.
Sep  1 17:42:13 MBP kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 12 13 36 40 44 48
52 56 60 64 149 153 157 161 165
Sep  1 17:46:13 MBP kernel[0]: Auth result for: 00:26:b0:fe:76:74 MAC AUTH succeeded
Sep  1 17:46:13 MBP kernel[0]: AirPort: Link Up on en1
…
Aug  5 09:49:07 MBP kernel[0]: en1: 802.11d country code set to 'XO'.
Aug  5 09:49:07 MBP kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 36 40 44 48 52 56
60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
Aug  5 09:49:10 MBP kernel[0]: NVEthernet::setLinkStatus - Valid but not Active
Aug  5 09:49:10 MBP kernel[0]: NVEthernet::mediaChanged - Link is down
Aug  5 09:49:10 MBP kernel[0]: NVEthernet::setLinkStatus - Valid but not Active
Aug  5 09:49:13 MBP kernel[0]: en1: 802.11d country code set to 'US'.
Aug  5 09:49:13 MBP kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 36 40 44 48 52 56
60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
Aug  5 09:49:40 MBP kernel[0]: Auth result for: 00:0c:e5:0e:65:bd MAC AUTH succeeded
Aug  5 09:49:40 MBP kernel[0]: AirPort: Link Up on en1
…
Jun  5 12:08:49 MBP  kernel[0]: en1: 802.11d country code set to 'SE'.
Jun  5 12:08:49 MBP kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 12 13 36 40 44 48
52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
Jun  5 12:09:14 MBP kernel[0]: Auth result for: 88:f0:77:2f:75:70 MAC AUTH succeeded
Jun  5 12:09:14 MBP kernel[0]: AirPort: Link Up on en1
```

SYSTEM.LOG
SEARCH "HOSTNAME" (10.6)

```
Apr 27 19:34:55 205-168-25-116 configd[13]: setting hostname to
"205-168-25-116.dia.static.qwest.net
```

- DIA – Denver Airport Code
- 205.168.25.116 – Registered to "JOHN Q HAMMONS HOTEL MANAGEMENT"

```
Aug  2 18:37:07 wsip-70-164-159-4 configd[13]: setting hostname to
"wsip-70-164-159-4.lv.lv.cox.net"
```

- LV = Las Vegas?
- 70.164.159.4 – Registered to "Cox Communications Inc. NETBLK-LV-OHFC"

```
Jun  5 12:09:19 host-78-64-88-181 configd[13]: setting hostname to
"host-78-64-88-181.homerun.telia.com"
```

- 78.64.88.181 – Registered to Telia Network Services in Sweden

CORRELATE WITH…

- Photo EXIF Data
- Calendar
- Email Itineraries
- Internet History
- Travel Websites
- Search History

oompa@csh.rit.edu | @iamevltwin

USER ACTIVITY

oompa@csh.rit.edu | @iamevltwin

USER LOGINS / LOGOUTS

Local Terminal

- May 28 14:48:04 byte login[693]: USER_PROCESS: 693 ttys000
- May 28 14:48:07 byte login[698]: USER_PROCESS: 698 ttys001
- May 28 15:07:29 byte login[812]: USER_PROCESS: 812 ttys002
- May 28 15:07:51 byte login[812]: DEAD_PROCESS: 812 ttys002

Login Window

- May 28 12:42:23 byte loginwindow[66]: DEAD_PROCESS: 74 console
- May 28 14:28:04 byte loginwindow[66]: USER_PROCESS: 60 console

SSH

- May 28 15:15:38 byte sshd[831]: USER_PROCESS: 842 ttys002
- May 28 15:15:52 byte sshd[831]: DEAD_PROCESS: 842 ttys002

Screen Sharing

- 5/28/12 3:31:33.675 PM screensharingd: Authentication: SUCCEEDED :: User Name: Sarah Edwards :: Viewer Address: 192.168.1.101 :: Type: DH

LOG ANALYSIS MONTHLY.OUT

- Account Audit
- Monthly
- Uses `ac -p` command to calculate account time on system.
- "Accumulated connected time in decimal hours"

```
-- End of monthly output --

Wed Apr  4 09:15:54 EDT 2012

Rotating fax log files:

Doing login accounting:
          total     3678.85
          sledwards  3678.76
          root         0.09

-- End of monthly output --

Tue May  1 05:30:00 PDT 2012

Rotating fax log files:

Doing login accounting:
          total     4301.95
          sledwards  4301.77
          root         0.18

-- End of monthly output --

Fri Jun  1 06:46:13 PDT 2012

Rotating fax log files:

Doing login accounting:
          total     5047.22
          sledwards  5047.04
          root         0.18

-- End of monthly output --
```

PRIVILEGE ESCALATION

su

- 5/27/12 8:54:21.646 PM su: BAD SU oompa to root on /dev/ttys001
- 5/28/12 8:57:44.032 PM su: oompa to root on /dev/ttys000

sudo

- 5/27/12 8:48:15.790 PM sudo: oompa : TTY=ttys000 ; PWD=/Users/oompa/Documents ; USER=root ; COMMAND=/usr/bin/iosnoop

ACCOUNT CREATION

Audit Logs

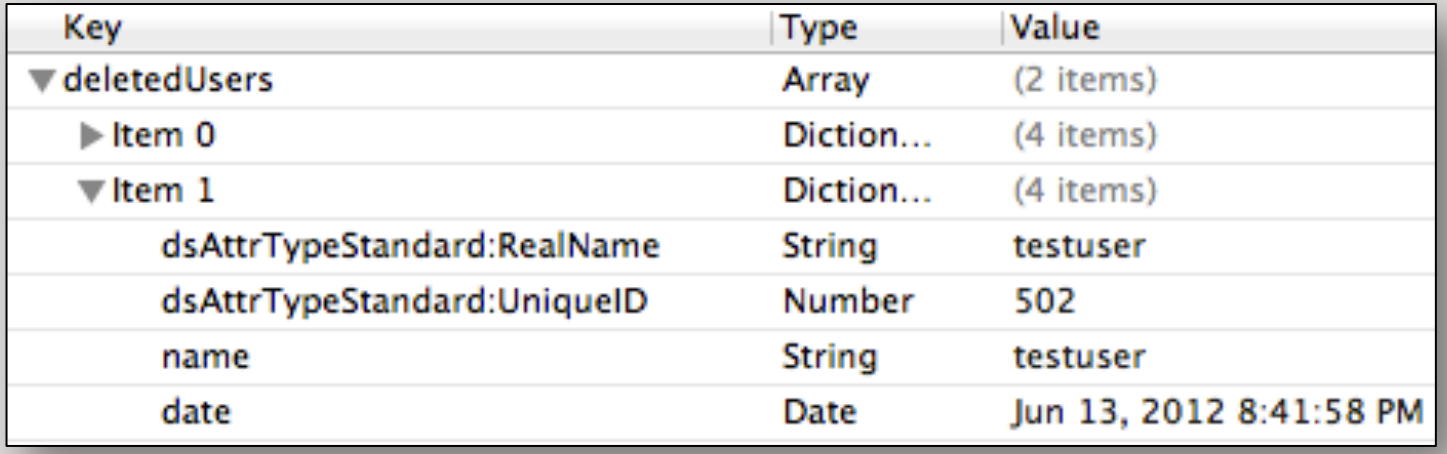
- <record version="11" event="**create user**" modifier="0" time="Mon May 28 21:25:49 2012" msec=" + 677 msec" >
  <subject audit-uid="501" **uid="501"** gid="20" ruid="501" rgid="20" pid="585" sid="100004" tid="585 0.0.0.0" />
  <text>Create record type Users '**supersecretuser**' node '/Local/Default'</text>
  <return errval="success" retval="0" />
  </record>

secure.log or system.log (10.8+)

- May 28 21:25:22 bit com.apple.SecurityServer[24]: UID 501 authenticated as user oompa (UID 501) for right 'system.preferences.accounts'

ACCOUNT DELETION

- /Library/Preferences/com.apple.preferences.accounts.plist



Key	Type	Value
▼ deletedUsers	Array	(2 items)
▶ Item 0	Diction…	(4 items)
▼ Item 1	Diction…	(4 items)
dsAttrTypeStandard:RealName	String	testuser
dsAttrTypeStandard:UniqueID	Number	502
name	String	testuser
date	Date	Jun 13, 2012 8:41:58 PM

```
<record version="11" event="delete user" modifier="0" time="Wed Jun 13 20:41:56
2012" msec=" + 322 msec" >
<subject audit-uid="501" uid="501" gid="20" ruid="501" rgid="20" pid="10717"
sid="100005" tid="10717 0.0.0.0" />
<text>Delete record type Users &apos;testuser&apos; node &apos;/Local/
Default&apos;</text>
<return errval="success" retval="0" />
</record>
```

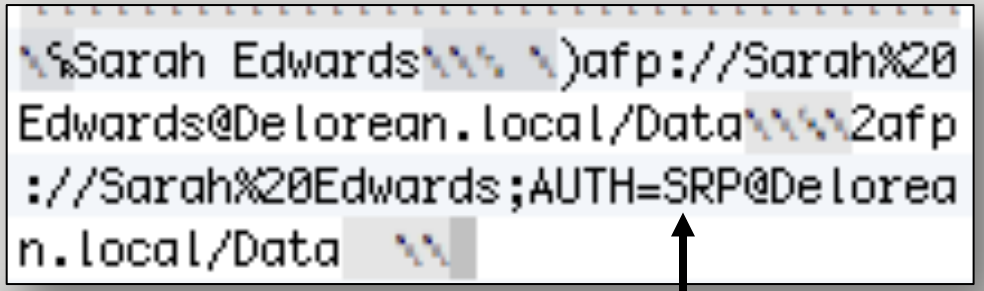
BACKUPS

oompa@csh.rit.edu | @iamevltwin

BACKUP LOG ENTRY
SYSTEM.LOG

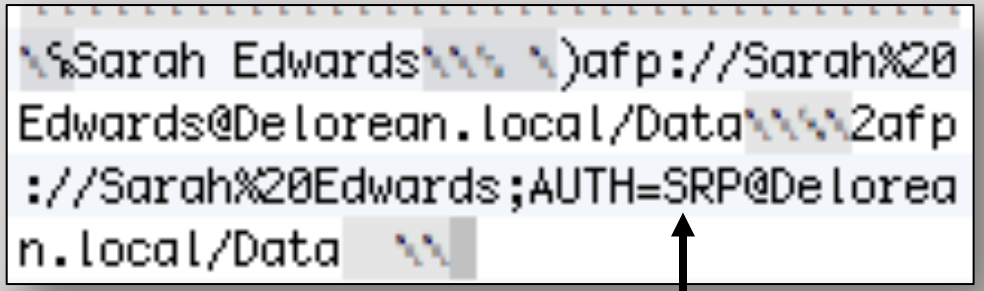
```
Jun 16 15:18:10 bit com.apple.backupd[1957]: Starting standard backup
Jun 16 15:18:10 bit com.apple.backupd[1957]: Attempting to mount network destination URL: afp://Sarah
%20Edwards;AUTH=SRP@Delorean.local/Data
Jun 16 15:18:19 bit com.apple.backupd[1957]: Mounted network destination at mountpoint: /Volumes/Data
using URL: afp://Sarah%20Edwards;AUTH=SRP@Delorean.local/Data
Jun 16 15:18:23 bit com.apple.backupd[1957]: QUICKCHECK ONLY; FILESYSTEM CLEAN
Jun 16 15:18:26 bit com.apple.backupd[1957]: Disk image /Volumes/Data/bit.sparsebundle mounted at: /
Volumes/Time Machine Backups
Jun 16 15:18:26 bit com.apple.backupd[1957]: Backing up to: /Volumes/Time Machine Backups/Backups.backupdb
Jun 16 12:19:00 bit com.apple.backupd[1957]: 100.0 MB required (including padding), 516.13 GB available
Jun 16 12:19:00 bit com.apple.backupd[1957]: Waiting for index to be ready (101)
Jun 16 12:22:08 bit com.apple.backupd[1957]: Copied 1115 files (26.1 MB) from volume LION.
Jun 16 12:22:09 bit com.apple.backupd[1957]: 1.23 GB required (including padding), 516.13 GB available
Jun 16 12:22:51 bit com.apple.backupd[1957]: Copied 971 files (1.1 MB) from volume LION.
Jun 16 12:22:57 bit com.apple.backupd[1957]: Starting post-backup thinning
Jun 16 12:23:43 bit com.apple.backupd[1957]: Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/
2012-05-19-004000 (21.3 MB)
Jun 16 12:24:22 bit com.apple.backupd[1957]: Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/
2012-06-08-004822 (87.3 MB)
Jun 16 12:25:11 bit com.apple.backupd[1957]: Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/
2012-06-10-002525 (168.2 MB)
Jun 16 12:25:11 bit com.apple.backupd[1957]: Post-back up thinning complete: 3 expired backups removed
Jun 16 12:25:11 bit com.apple.backupd[1957]: Backup completed successfully.
Jun 16 12:25:51 bit com.apple.backupd[1957]: Ejected Time Machine disk image.
Jun 16 12:25:51 bit com.apple.backupd[1957]: Ejected Time Machine network volume.
```

BACKUPS - /LIBRARY/PREFERENCES/ COM.APPLE.TIMEMACHINE.PLIST



Key	Type	Value
▶ FirmwareCheckDatesLion	Diction…	(1 item)
▶ HostUUIDs	Array	(1 item)
LocalizedDiskImageVolumeName	String	Time Machine Backups
BackupAlias	Data	<00000000 03e40002 00010444 61746100 0(
PreferencesVersion	Number	1
TimeCapsuleName	String	Delorean
RootVolumeUUID	String	3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D
FirmwareCheckDestinationAlias	Data	<00000000 03e40002 00010444 61746100 0(
AutoBackup	Boolean	YES
▶ DestinationVolumeUUIDs	Array	(1 item)

BACKUPS - /LIBRARY/PREFERENCES/ COM.APPLE.TIMEMACHINE.PLIST



Key	Type	Value
▶ FirmwareCheckDatesLion	Diction…	(1 item)
▶ HostUUIDs	Array	(1 item)
LocalizedDiskImageVolumeName	String	Time Machine Backups
BackupAlias	Data	<00000000 03e40002 00010444 61746100 0(
PreferencesVersion	Number	1
TimeCapsuleName	String	Delorean
RootVolumeUUID	String	3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D
FirmwareCheckDestinationAlias	Data	<00000000 03e40002 00010444 61746100 0(
AutoBackup	Boolean	YES
▶ DestinationVolumeUUIDs	Array	(1 item)

SNAPSHOTS - /VAR/DB/ COM.APPLE.TIMEMACHINE.SNAPSHOTDATES.PLIST

Key	Type	Value
▼ 3F6992A5-4151-37CC-BD67-C6556DA81FB1	Array	(60 items)
Item 0	Date	Oct 2, 2011 8:36:25 PM
Item 1	Date	Oct 15, 2011 11:34:12 AM
Item 2	Date	Oct 23, 2011 12:36:23 AM
Item 3	Date	Oct 30, 2011 12:21:28 AM
Item 4	Date	Nov 12, 2011 3:42:43 PM
Item 5	Date	Nov 19, 2011 9:12:42 AM
Item 6	Date	Nov 27, 2011 10:36:34 AM
Item 7	Date	Dec 4, 2011 8:43:46 AM
Item 8	Date	Dec 11, 2011 9:12:43 AM
Item 9	Date	Dec 18, 2011 10:27:37 AM
Item 10	Date	Dec 28, 2011 7:47:02 PM
Item 11	Date	Jan 4, 2012 5:49:49 PM
Item 12	Date	Jan 11, 2012 7:05:02 PM
Item 13	Date	Jan 18, 2012 6:35:38 PM

SOFTWARE

oompa@csh.rit.edu | @iamevltwin

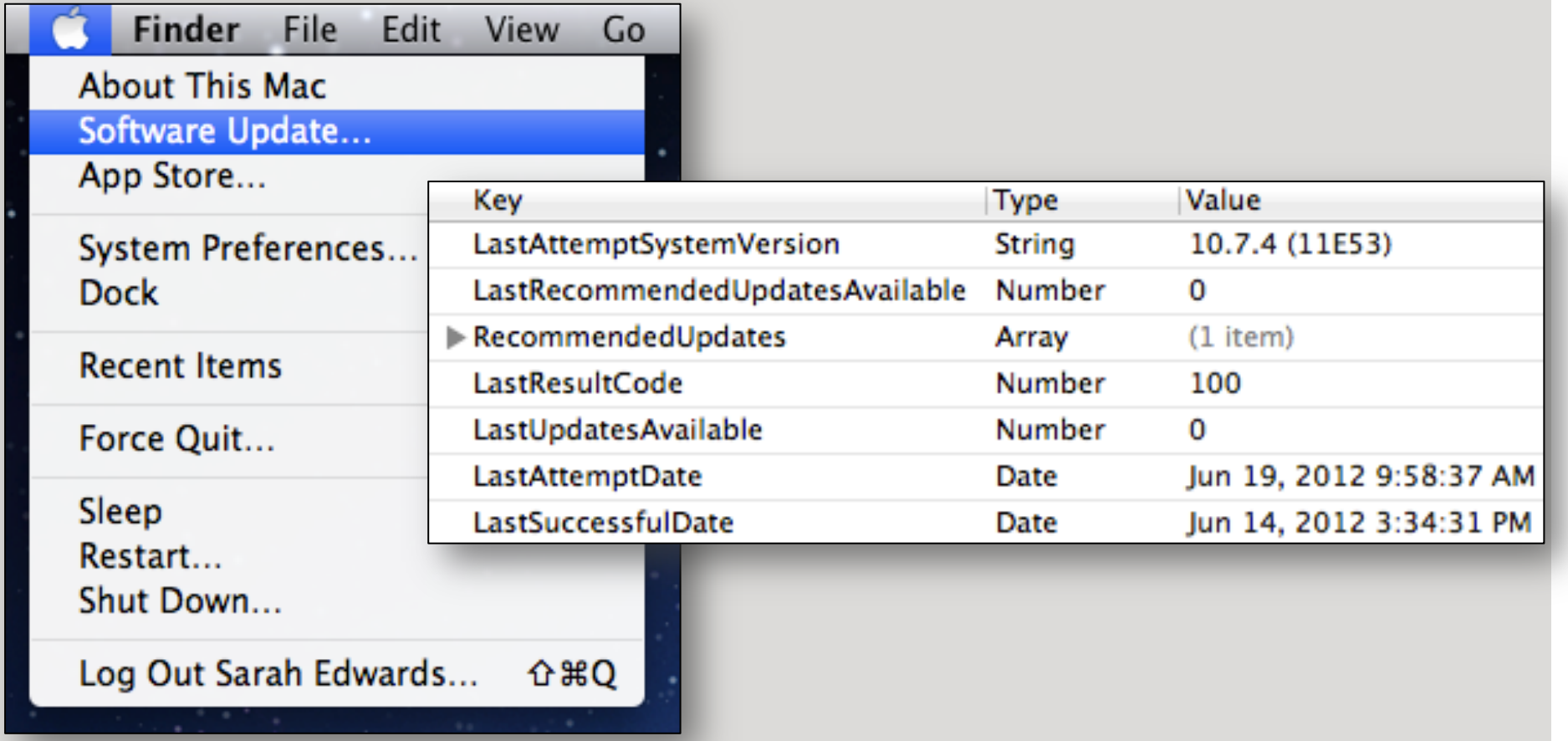
INSTALLED SOFTWARE
INSTALL.LOG – SEARCH “INSTALLED”

```
May  9 16:28:06 localhost OSInstaller[328]: Installed "Mac OS X" ()
…
May  9 19:56:21 bit installd[338]: Installed "Evernote" ()
May 10 00:45:34 bit installd[559]: Installed "Flashback malware removal tool" (1.0)
May 10 00:45:34 bit installd[559]: Installed "Mac OS X Update Combined" (10.7.4)
May 10 00:45:34 bit installd[559]: Installed "iTunes" (10.6.1)
May 10 00:46:33 bit installd[559]: Installed "Lion Recovery Update" (1.0)
May 10 16:51:51 bit installd[295]: Installed "Xcode" ()
May 10 16:55:55 bit installd[295]: Installed "iPhoto" ()
May 11 19:51:09 bit installd[4384]: Installed "Office 2011 14.1.0 Update" ()
May 14 18:31:44 bit installd[9572]: Installed "Java for OS X 2012-003" (1.0)
May 19 16:50:20 bit installd[20691]: Installed "TrueCrypt 7.1a" ()
May 19 17:17:25 bit installd[20847]: Installed "CCleaner" ()
May 19 17:32:19 bit installd[20847]: Installed "TextWrangler" ()
May 26 20:15:45 bit installd[39022]: Installed "The Unarchiver" ()
May 27 15:46:56 bit installd[41936]: Installed "Wireshark 1.6.8 Intel 64" ()
May 27 20:57:48 bit installd[514]: Installed "Microsoft Error Reporting for Mac" ()
May 27 20:59:41 bit installd[978]: Installed "Office 2011 14.2.2 Update" ()
```

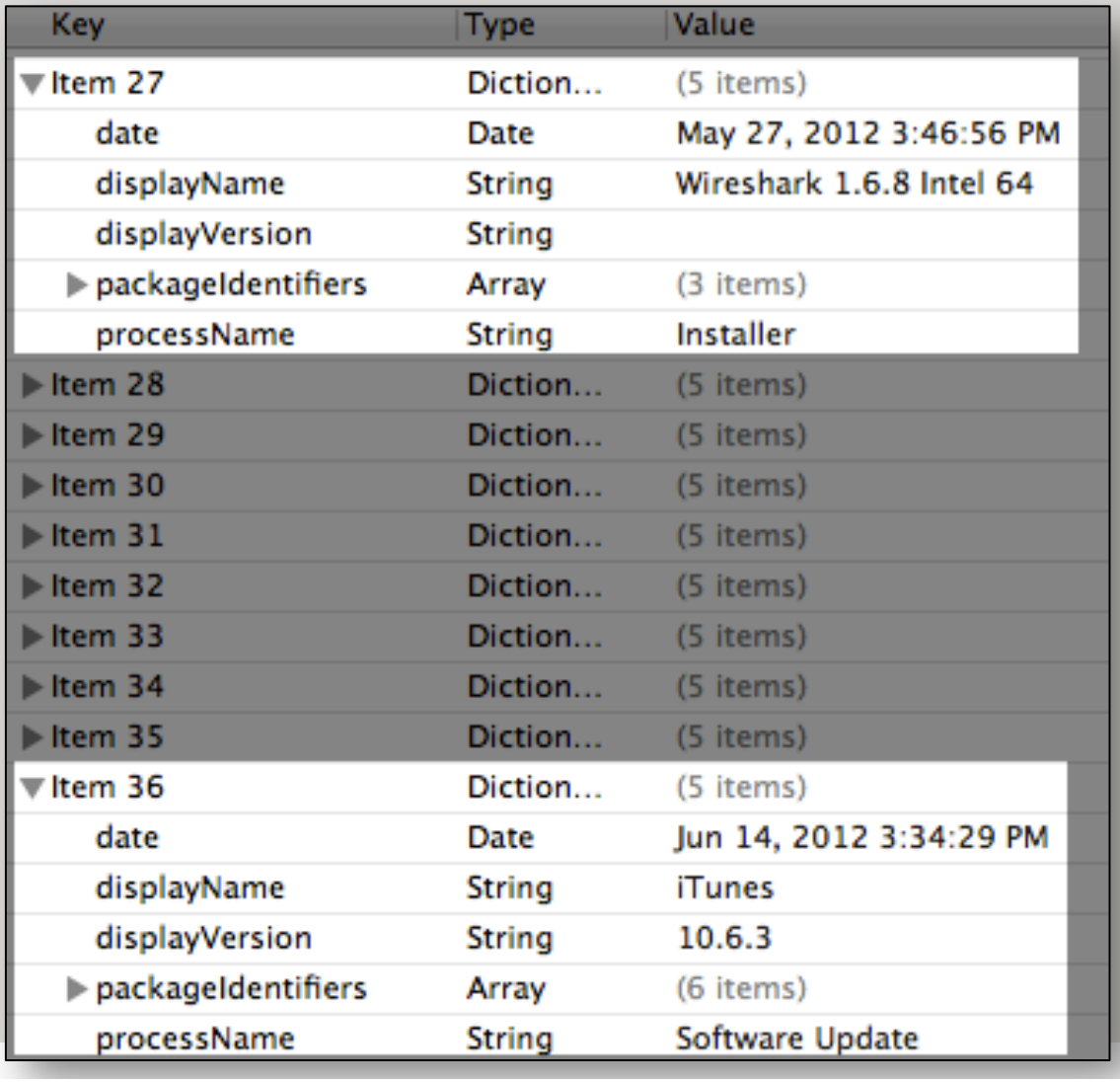
INSTALL DETAILS
INSTALL.LOG

```
May 27 11:59:03 MBP Installer[470]: logKext  Installation Log
May 27 11:59:03 MBP Installer[470]: Opened from: /Users/oompa/
Downloads/logKext-2.3.pkg
May 27 11:59:03 MBP Installer[470]: Product archive /Users/oompa/
Downloads/logKext-2.3.pkg trustLevel=100
May 27 11:59:17 MBP Installer[470]: InstallerStatusNotifications plugin
loaded
May 27 11:59:26 MBP runner[477]: Administrator authorization granted.
May 27 11:59:26 MBP Installer[470]:
================================================================================
=========
May 27 11:59:26 MBP Installer[470]: User picked Standard Install
May 27 11:59:26 MBP Installer[470]: Choices selected for installation:
…
May 27 12:01:34 MBP installd[481]: Installed "logKext" ()
May 27 12:01:35 MBP installd[481]: PackageKit: ----- End install -----
```

/LIBRARY/PREFERENCES/ COM.APPLE.SOFTWAREUPDATE.PLIST



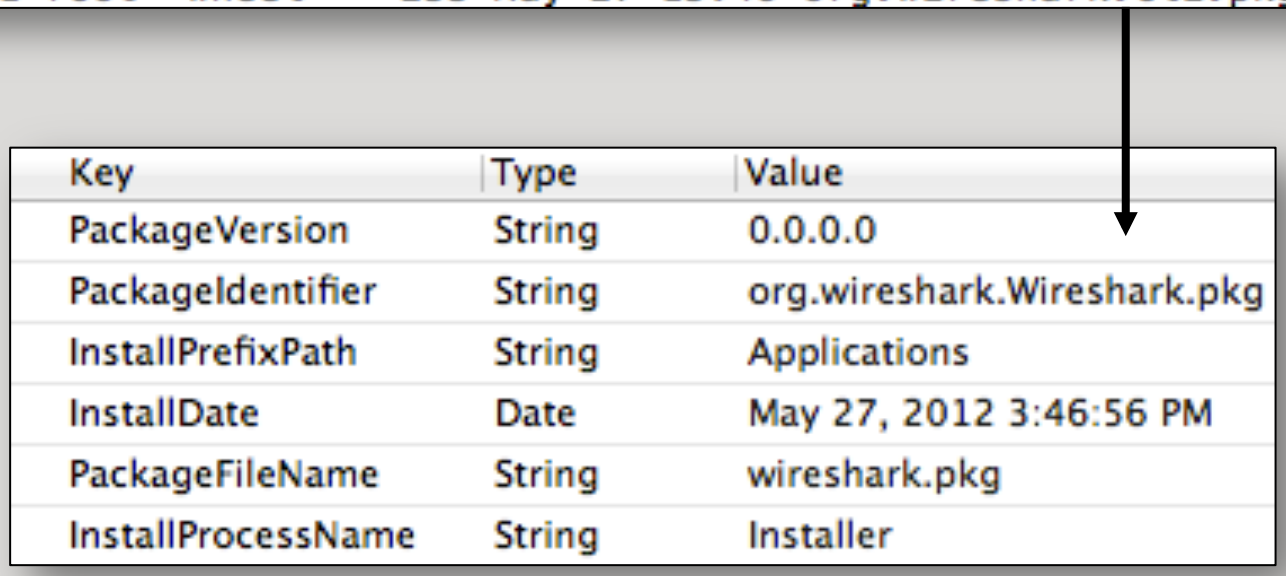
INSTALL HISTORY /LIBRARY/RECEIPTS/INSTALLHISTORY.PLIST



Key	Type	Value
▼ Item 27	Diction…	(5 items)
date	Date	May 27, 2012 3:46:56 PM
displayName	String	Wireshark 1.6.8 Intel 64
displayVersion	String	
▶ packageIdentifiers	Array	(3 items)
processName	String	Installer
▶ Item 28	Diction…	(5 items)
▶ Item 29	Diction…	(5 items)
▶ Item 30	Diction…	(5 items)
▶ Item 31	Diction…	(5 items)
▶ Item 32	Diction…	(5 items)
▶ Item 33	Diction…	(5 items)
▶ Item 34	Diction…	(5 items)
▶ Item 35	Diction…	(5 items)
▼ Item 36	Diction…	(5 items)
date	Date	Jun 14, 2012 3:34:29 PM
displayName	String	iTunes
displayVersion	String	10.6.3
▶ packageIdentifiers	Array	(6 items)
processName	String	Software Update

RECEIPT FILES
/VAR/DB/RECEIPTS/

```
-rw-r--r--  1 root  wheel  35290 May 27 15:46 org.wireshark.ChmodBPF.pkg.bom
-rw-r--r--  1 root  wheel    260 May 27 15:46 org.wireshark.ChmodBPF.pkg.plist
-rw-r--r--  1 root  wheel  62594 May 27 15:46 org.wireshark.Wireshark.pkg.bom
-rw-r--r--  1 root  wheel    256 May 27 15:46 org.wireshark.Wireshark.pkg.plist
-rw-r--r--  1 root  wheel  35138 May 27 15:46 org.wireshark.cli.pkg.bom
-rw-r--r--  1 root  wheel    255 May 27 15:46 org.wireshark.cli.pkg.plist
```



Key	Type	Value
PackageVersion	String	0.0.0.0
PackageIdentifier	String	org.wireshark.Wireshark.pkg
InstallPrefixPath	String	Applications
InstallDate	Date	May 27, 2012 3:46:56 PM
PackageFileName	String	wireshark.pkg
InstallProcessName	String	Installer

SYSTEM VERSION
INSTALL.LOG – SEARCH "BUILD:"

```
May  9 16:14:10 localhost Install Mac OS X Lion[339]: Running OS Build: Mac OS X 10.7 (11A511)
May  9 16:19:25 localhost OSInstaller[328]: Running OS Build: Mac OS X 10.7 (11A511)
May 11 19:23:47 bit Installer[3177]: Running OS Build: Mac OS X 10.7.4 (11E53)
May 11 19:40:47 bit Installer[3755]: Running OS Build: Mac OS X 10.7.4 (11E53)
May 11 19:49:02 bit Installer[4114]: Running OS Build: Mac OS X 10.7.4 (11E53)
May 13 13:47:00 bit Installer[3927]: Running OS Build: Mac OS X 10.7.4 (11E53)
May 19 16:50:11 bit Installer[20680]: Running OS Build: Mac OS X 10.7.4 (11E53)
May 27 15:46:39 bit Installer[41929]: Running OS Build: Mac OS X 10.7.4 (11E53)
May 27 20:57:17 bit Installer[495]: Running OS Build: Mac OS X 10.7.4 (11E53)
May 27 20:58:01 bit Installer[529]: Running OS Build: Mac OS X 10.7.4 (11E53)
Jun  9 09:28:18 bit Installer[299]: Running OS Build: Mac OS X 10.7.4 (11E53)
```

SYSTEM VERSION
KERNEL.LOG/SYSTEM.LOG – SEARCH "DARWIN"

```
Jul 22 06:49:23 localhost kernel[0]: Darwin Kernel Version 11.0.0: Sat Jun 18 12:56:35 PDT 2011;
root:xnu-1699.22.73~1/RELEASE_X86_64
Aug  8 21:43:11 localhost kernel[0]: Darwin Kernel Version 11.0.0: Sat Jun 18 12:56:35 PDT 2011;
root:xnu-1699.22.73~1/RELEASE_X86_64
Aug 20 20:21:18 localhost kernel[0]: Darwin Kernel Version 11.1.0: Tue Jul 26 16:07:11 PDT 2011;
root:xnu-1699.22.81~1/RELEASE_X86_64
Oct  5 06:59:00 localhost kernel[0]: Darwin Kernel Version 11.1.0: Tue Jul 26 16:07:11 PDT 2011;
root:xnu-1699.22.81~1/RELEASE_X86_64
Oct 12 19:36:33 localhost kernel[0]: Darwin Kernel Version 11.2.0: Tue Aug  9 20:54:00 PDT 2011;
root:xnu-1699.24.8~1/RELEASE_X86_64
Dec 30 19:21:03 localhost kernel[0]: Darwin Kernel Version 11.2.0: Tue Aug  9 20:54:00 PDT 2011;
root:xnu-1699.24.8~1/RELEASE_X86_64
Feb  2 20:05:19 localhost kernel[0]: Darwin Kernel Version 11.3.0: Thu Jan 12 18:47:41 PST 2012;
root:xnu-1699.24.23~1/RELEASE_X86_64
Apr  8 15:13:53 localhost kernel[0]: Darwin Kernel Version 11.3.0: Thu Jan 12 18:47:41 PST 2012;
root:xnu-1699.24.23~1/RELEASE_X86_64
May 10 19:35:18 localhost kernel[0]: Darwin Kernel Version 11.4.0: Mon Apr  9 19:32:15 PDT 2012;
root:xnu-1699.26.8~1/RELEASE_X86_64
```

SYSTEM INFORMATION & SYSTEM STATE

oompa@csh.rit.edu | @iamevltwin

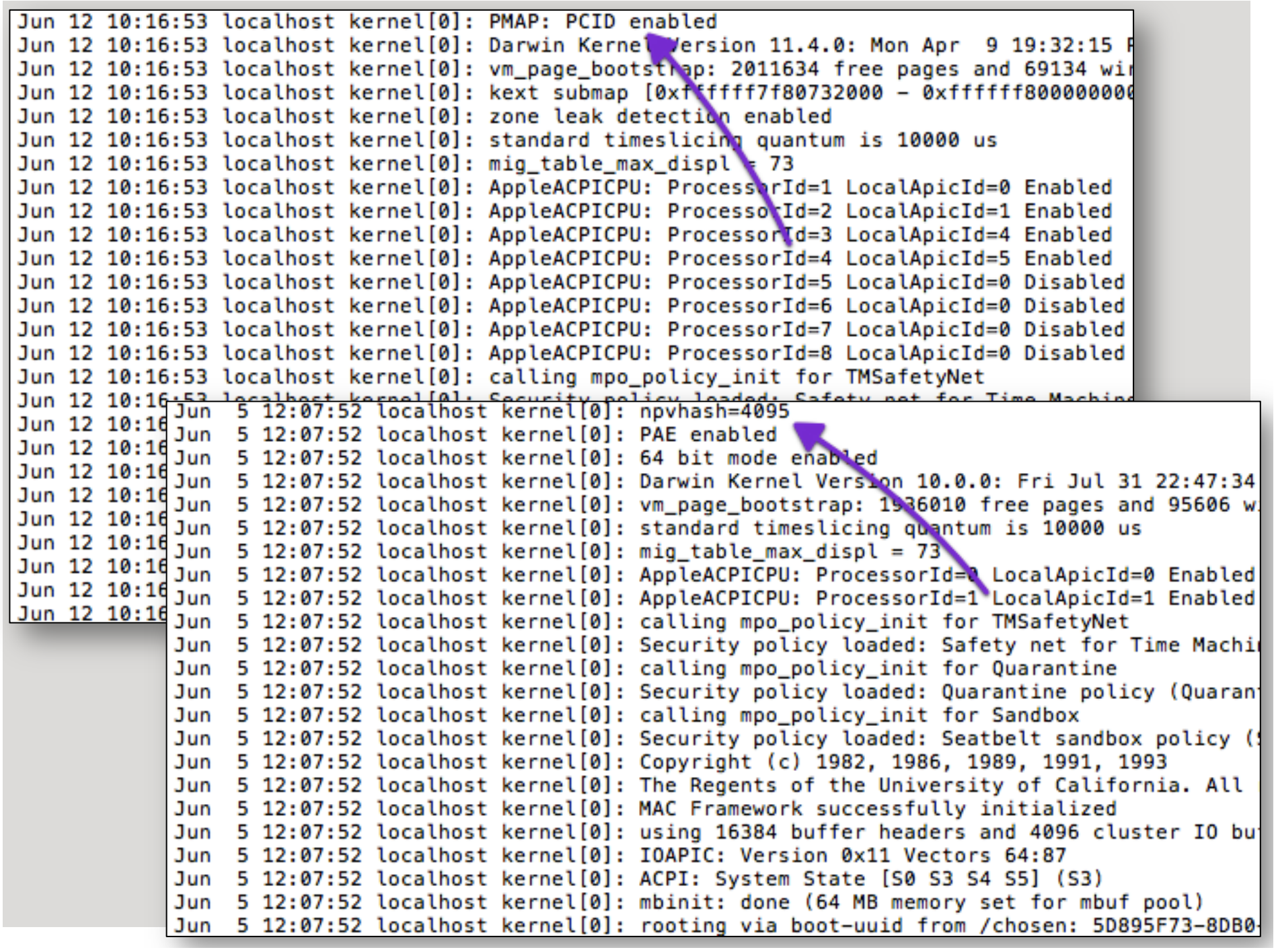
SYSTEM.LOG
BOOT, REBOOT & SHUTDOWN

```
May  9 16:28:48 localhost bootlog[0]: BOOT_TIME 1336606128 0
May 10 16:40:27 localhost bootlog[0]: BOOT_TIME 1336682427 0
May 12 11:32:16 localhost bootlog[0]: BOOT_TIME 1336836736 0
May 27 20:02:41 localhost bootlog[0]: BOOT_TIME 1338163361 0
May 28 15:22:30 localhost bootlog[0]: BOOT_TIME 1338232950 0
Jun  9 09:27:05 localhost bootlog[0]: BOOT_TIME 1339248425 0
Jun  9 10:15:56 localhost bootlog[0]: BOOT_TIME 1339251356 0
Jun  9 10:33:39 localhost bootlog[0]: BOOT_TIME 1339252419 0
Jun  9 09:27:05 localhost bootlog[0]: BOOT_TIME 1339248425 0
Jun  9 10:15:56 localhost bootlog[0]: BOOT_TIME 1339251356 0
Jun  9 10:33:39 localhost bootlog[0]: BOOT_TIME 1339252419 0
Jun 10 13:33:56 localhost bootlog[0]: BOOT_TIME 1339349636 0
Jun 12 10:16:35 localhost bootlog[0]: BOOT_TIME 1339510595 0
```

```
May 27 20:02:14 bit shutdown[42801]: halt by oompa:
May 27 20:02:14 bit shutdown[42801]: SHUTDOWN_TIME: 1338163334 903688
May 28 15:20:06 bit shutdown[2421]: halt by oompa:
May 28 15:20:06 bit shutdown[2421]: SHUTDOWN_TIME: 1338232806 702175
Jun  9 09:25:33 bit shutdown[25868]: halt by oompa:
Jun  9 09:25:33 bit shutdown[25868]: SHUTDOWN_TIME: 1339248333 887656
Jun  9 10:15:24 bit shutdown[546]: reboot by oompa:
Jun  9 10:15:24 bit shutdown[546]: SHUTDOWN_TIME: 1339251324 30856
Jun  9 10:21:53 bit shutdown[309]: halt by oompa:
Jun  9 10:21:53 bit shutdown[309]: SHUTDOWN_TIME: 1339251713 535787
Jun  9 09:25:33 bit shutdown[25868]: halt by oompa:
Jun  9 09:25:33 bit shutdown[25868]: SHUTDOWN_TIME: 1339248333 887656
Jun  9 10:15:24 bit shutdown[546]: reboot by oompa:
Jun  9 10:15:24 bit shutdown[546]: SHUTDOWN_TIME: 1339251324 30856
Jun  9 10:21:53 bit shutdown[309]: halt by oompa:
Jun  9 10:21:53 bit shutdown[309]: SHUTDOWN_TIME: 1339251713 535787
```

SYSTEM BOOT
KERNEL.LOG & SYSTEM.LOG

10.8+	• **Boot logging starts with** “`BOOT_TIME`”
10.7	• **Boot logging starts with** “`PMAP: PCID enabled`”
10.6	• **Boot logging starts with** “`npvhash=4095`”


Jun 12 10:16:53 localhost kernel[0]: PMAP: PCID enabled
Jun 12 10:16:53 localhost kernel[0]: Darwin Kernel Version 11.4.0: Mon Apr 9 19:32:15
Jun 12 10:16:53 localhost kernel[0]: vm_page_bootstrap: 2011634 free pages and 69134
Jun 12 10:16:53 localhost kernel[0]: kext submap [0xffffff7f80732000 - 0xffffff8000000000
Jun 12 10:16:53 localhost kernel[0]: zone leak detection enabled
Jun 12 10:16:53 localhost kernel[0]: standard timeslicing quantum is 10000 us
Jun 12 10:16:53 localhost kernel[0]: mig_table_max_displ = 73
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=1 LocalApicId=0 Enabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=2 LocalApicId=1 Enabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=3 LocalApicId=4 Enabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=4 LocalApicId=5 Enabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=5 LocalApicId=0 Disabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=6 LocalApicId=0 Disabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=7 LocalApicId=0 Disabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=8 LocalApicId=0 Disabled
Jun 12 10:16:53 localhost kernel[0]: calling mpo_policy_init for TMSafetyNet
Jun 5 12:07:52 localhost kernel[0]: npvhash=4095
Jun 5 12:07:52 localhost kernel[0]: PAE enabled
Jun 5 12:07:52 localhost kernel[0]: 64 bit mode enabled
Jun 5 12:07:52 localhost kernel[0]: Darwin Kernel Version 10.0.0: Fri Jul 31 22:47:34
Jun 5 12:07:52 localhost kernel[0]: vm_page_bootstrap: 1536010 free pages and 95606
Jun 5 12:07:52 localhost kernel[0]: standard timeslicing quantum is 10000 us
Jun 5 12:07:52 localhost kernel[0]: mig_table_max_displ = 73
Jun 5 12:07:52 localhost kernel[0]: AppleACPICPU: ProcessorId=0 LocalApicId=0 Enabled
Jun 5 12:07:52 localhost kernel[0]: AppleACPICPU: ProcessorId=1 LocalApicId=1 Enabled
Jun 5 12:07:52 localhost kernel[0]: calling mpo_policy_init for TMSafetyNet
Jun 5 12:07:52 localhost kernel[0]: Security policy loaded: Safety net for Time Machi
Jun 5 12:07:52 localhost kernel[0]: calling mpo_policy_init for Quarantine
Jun 5 12:07:52 localhost kernel[0]: Security policy loaded: Quarantine policy (Quaran
Jun 5 12:07:52 localhost kernel[0]: calling mpo_policy_init for Sandbox
Jun 5 12:07:52 localhost kernel[0]: Security policy loaded: Seatbelt sandbox policy
Jun 5 12:07:52 localhost kernel[0]: Copyright (c) 1982, 1986, 1989, 1991, 1993
Jun 5 12:07:52 localhost kernel[0]: The Regents of the University of California. All
Jun 5 12:07:52 localhost kernel[0]: MAC Framework successfully initialized
Jun 5 12:07:52 localhost kernel[0]: using 16384 buffer headers and 4096 cluster IO bu
Jun 5 12:07:52 localhost kernel[0]: IOAPIC: Version 0x11 Vectors 64:87
Jun 5 12:07:52 localhost kernel[0]: ACPI: System State [S0 S3 S4 S5] (S3)
Jun 5 12:07:52 localhost kernel[0]: mbinit: done (64 MB memory set for mbuf pool)
Jun 5 12:07:52 localhost kernel[0]: rooting via boot-uuid from /chosen: 5D895F73-8DB0-

SYSTEM BOOT - BOOT DEVICE KERNEL.LOG OR SYSTEM.LOG

```
May  9 16:29:10 localhost kernel[0]: rooting via boot-uuid
from /chosen: 3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D
May  9 16:29:10 localhost kernel[0]: Waiting on <dict
ID="0"><key>IOProviderClass</key><string ID="1">IOResources</
string><key>IOResourceMatch</key><string ID="2">boot-uuid-
media</string></dict>
May  9 16:29:10 localhost kernel[0]: Got boot device =
IOService:/AppleACPIPlatformExpert/PCI0@0/AppleACPIPCI/SATA@1F,
2/AppleIntelPchSeriesAHCI/PRT0@0/IOAHCIDevice@0/
AppleAHCIDiskDriver/IOAHCIBlockStorageDevice/
IOBlockStorageDriver/WDC WD7500BPKT-75PK4T0 Media/
IOGUIDPartitionScheme/Untitled@2
```

SYSTEM BOOT
BOOT UUID

```
nibble:SystemConfiguration sledwards$ diskutil list
/dev/disk0
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *500.3 GB   disk0
   1:                        EFI EFI                     209.7 MB   disk0s1
   2:          Apple_CoreStorage                        499.4 GB   disk0s2
   3:                 Apple_Boot Recovery HD            650.0 MB   disk0s3
/dev/disk1
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:                Apple_HFS Macintosh HD           *499.1 GB   disk1
nibble:SystemConfiguration sledwards$ diskutil info /dev/disk1
   Device Identifier:        disk1
   Device Node:              /dev/disk1
   Part of Whole:            disk1
   Device / Media Name:      Macintosh HD

   Volume Name:              Macintosh HD
   Escaped with Unicode:     Macintosh%FF%FE%20%00HD

   Mounted:                  Yes
   Mount Point:              /
   Escaped with Unicode:     /

   File System Personality:  Journaled HFS+
   Type (Bundle):            hfs
   Name (User Visible):      Mac OS Extended (Journaled)
   Journal:                  Journal size 40960 KB at offset 0x1238b000
   Owners:                   Enabled

   Content (IOContent):      Apple_HFS
   OS Can Be Installed:      Yes
   Recovery Disk:            disk0s3
   Media Type:               Generic
   Protocol:                 PCI
   SMART Status:             Not Supported
   Volume UUID:              2603DEB0-8EBD-36BD-A5F4-989446F8EE01

   Total Size:               499.1 GB (499082485760 Bytes) (exactly 974770480 512-Byte-Units)
   Volume Free Space:        126.6 GB (126555856896 Bytes) (exactly 247179408 512-Byte-Units)
   Device Block Size:        512 Bytes

   Read-Only Media:          No
   Read-Only Volume:         No
   Ejectable:                No

   Whole:                    Yes
   Internal:                 Yes
   Solid State:              Yes
   OS 9 Drivers:             No
   Low Level Format:         Not supported
```

```
Feb 13 11:00:23 localhost kernel[0]: rooting via boot-uuid from /chosen: 2603DEB0-8EBD-36BD-A5F4-989446F8EE01
Feb 13 11:00:23 localhost kernel[0]: Waiting on <dict ID="0"><key>IOProviderClass</key><string ID="1">IOResources</string><key>IOResourceMatch</key><string ID="2">boot-uuid-media</string></dict>
```

SYSTEM BOOT
MAC ADDRESSES

- Three different systems, boot from same HDD.
- Boot-UUID remains the same.
- MAC addresses change for each system.
- Correlate an HDD moving to/from systems.

```
Jun 14 17:41:59 localhost kernel[0]: rooting via boot-uuid from /chosen: 1FDCF218-B7EB-3BAC-9AD6-8498D0E2EA9D
Jun 14 19:50:26 localhost kernel[0]: rooting via boot-uuid from /chosen: 1FDCF218-B7EB-3BAC-9AD6-8498D0E2EA9D
Jun 14 20:33:38 localhost kernel[0]: rooting via boot-uuid from /chosen: 1FDCF218-B7EB-3BAC-9AD6-8498D0E2EA9D

Jun 14 17:42:22 Sarah-Edwardss-MacBook kernel[0]: yukon: Ethernet address 00:19:e3:3c:cb:7e
Jun 14 17:42:22 Sarah-Edwardss-MacBook kernel[0]: AirPort_AthrFusion21: Ethernet address 00:1b:63:c3:8d:1a
Jun 14 19:50:53 Sarah-Edwardss-MacBook kernel[0]: AirPort_Brcm4331: Ethernet address 28:cf:da:04:84:77
Jun 14 19:50:53 Sarah-Edwardss-MacBook kernel[0]: BCM5701Enet: Ethernet address 3c:07:54:03:65:20
Jun 14 20:34:12 Sarah-Edwardss-MacBook kernel[0]: BCM5701Enet: Ethernet address c4:2c:03:09:ca:fd
Jun 14 20:34:12 Sarah-Edwardss-MacBook kernel[0]: AirPort_Brcm43224: Ethernet address 90:27:e4:f8:e6:5f
```

KERNEL.LOG / SYSTEM.LOG
SLEEP CAUSE

```
May 26 17:27:02 MBP kernel[0]: Previous Sleep Cause: #
```

5	• Normal Sleep, Closed Laptop Lid
-60	• Unknown
0	• Hibernation

KERNEL.LOG / SYSTEM.LOG
WAKE REASON

`Jun  9 19:45:46 bit kernel[0]: Wake reason: <Message>`

RTC (Alarm)	• Wake on Demand, Bonjour Services - Real Time Clock
EC LID0, EC LID0 EHC2, EC.LidOpen, EC.LidOpen XHC1	• Laptop Lid
EHC1, EHC2	• Enhanced Host Controller - USB, Bluetooth, Wireless Devices
PWRB (User)	• Power Button
OHC1	• Open Host Controller - USB/Firewire, Mouse/Keyboard
? (User)	• Power Button from hibernation w/ no battery power
USB1	• Trackpad
EC.ACAttach (Maintenance), EC.ACDetach (Maintenance)	• Power Adapter

oompa@csh.rit.edu | @iamevltwin

KERNEL.LOG/SYSTEM.LOG SHUTDOWN CAUSE

```
Jul 23 17:08:52 localhost kernel[0]: Previous Shutdown Cause: #
```

0	• Battery Removal/Power Plug
3	• Hard Shutdown (Hold Power Button)
5	• Normal Shutdown/Reboot
-128	• Unknown
-60	• Unknown

DISK USAGE HISTORY
DAILY.LOG

```
Sun May 13 04:02:55 EDT 2012

Removing old temporary files:

Cleaning out old system announcements:

Removing stale files from /var/rwho:

Removing scratch fax files

Disk status:
Filesystem    Size   Used  Avail Capacity  Mounted on
/dev/disk1   698Gi  109Gi  588Gi    16%    /

Network interface status:
Name  Mtu   Network       Address            Ipkts Ierrs    Opkts Oerrs  Coll
lo0   16384 <Link#1>                        6641727     0  6641727     0     0
lo0   16384 localhost   fe80:1::1           6641727     -  6641727     -     -
lo0   16384 127           localhost         6641727     -  6641727     -     -
lo0   16384 localhost   ::1                 6641727     -  6641727     -     -
gif0* 1280  <Link#2>                             0     0        0     0     0
stf0* 1280  <Link#3>                             0     0        0     0     0
en0   1500  <Link#4>    c4:2c:03:09:ca:fd       0     0        0     0     0
en1   1500  <Link#5>    90:27:e4:f8:e6:5f 1823664     0  2065789     0     0
p2p0* 2304  <Link#6>    02:27:e4:f8:e6:5f       0     0        0     0     0
fw0   4078  <Link#7>    e8:06:88:ff:fe:d5:5d:08       0     0        0     0     0

Local system status:
 4:03  up 16:31, 2 users, load averages: 10.59 2.96 1.20
```

```
/dev/disk1   698Gi   109Gi   588Gi    16%    /
/dev/disk1   698Gi   123Gi   574Gi    18%    /
/dev/disk1   698Gi   172Gi   525Gi    25%    /
/dev/disk1   698Gi   181Gi   517Gi    26%    /
/dev/disk1   698Gi   181Gi   517Gi    26%    /
/dev/disk1   698Gi   180Gi   517Gi    26%    /
/dev/disk1   698Gi   180Gi   517Gi    26%    /
```

oompa@csh.rit.edu | @iamevltwin

PRINTING

oompa@csh.rit.edu | @iamevltwin

/VAR/LOG/CUPS/PAGE_LOG

- Printer Name
- User
- Job ID
- Date/Time
- Page Number
- Copies
- Job Billing
- Originating Hostname
- Job Name
  - “Print - .....”
- Media
  - “Letter”
- Sides
  - “one-sided” or “-”

```
Brother_HL_2170W_series oompa 1 [31/May/2012:20:26:31 -0400] 1 1 - localhost Print - Amazon.com - Returns Center Letter -
Brother_HL_2170W_series oompa 1 [31/May/2012:20:26:31 -0400] 2 1 - localhost Print - Amazon.com - Returns Center Letter -
Brother_HL_2170W_series oompa 2 [31/May/2012:20:27:39 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided
Brother_HL_2170W_series oompa 3 [01/Jun/2012:17:17:53 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided
Brother_HL_2170W_series oompa 4 [01/Jun/2012:17:26:25 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided
Brother_HL_2170W_series oompa 7 [01/Jun/2012:17:32:06 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided
Brother_HL_2170W_series oompa 8 [01/Jun/2012:17:38:37 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided
Brother_HL_2170W_series oompa 9 [14/Jun/2012:10:36:03 -0400] 1 1 - localhost Print - Platypus - Wikipedia, the free encyclopedia Letter -
Brother_HL_2170W_series oompa 9 [14/Jun/2012:10:36:03 -0400] 2 1 - localhost Print - Platypus - Wikipedia, the free encyclopedia Letter -
Brother_HL_2170W_series oompa 9 [14/Jun/2012:10:36:04 -0400] 3 1 - localhost Print - Platypus - Wikipedia, the free encyclopedia Letter -
```

/VAR/LOG/CUPS/ACCESS_LOG

- Hostname
- Group (-)
- User (-)
- Date/Time
- Method/Resource/Version
- Status Code
  - 200 = Successful
- Bytes in Request
- IPP Operation
  - “Create-Job”
  - “Send Document”
- IPP Status
  - “successful-ok”

```
localhost - - [01/Jun/2012:17:32:00 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 1243 Create-Job successful-ok
localhost - - [01/Jun/2012:17:32:00 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 166037 Send-Document successful-ok
localhost - - [01/Jun/2012:17:32:01 -0400] "POST / HTTP/1.1" 200 345 Set-Job-Attributes successful-ok
localhost - - [01/Jun/2012:17:38:31 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 1243 Create-Job successful-ok
localhost - - [01/Jun/2012:17:38:31 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 166037 Send-Document successful-ok
localhost - - [01/Jun/2012:17:38:32 -0400] "POST / HTTP/1.1" 200 345 Set-Job-Attributes successful-ok
localhost - - [14/Jun/2012:10:35:57 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 1267 Create-Job successful-ok
localhost - - [14/Jun/2012:10:35:57 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 570775 Send-Document successful-ok
localhost - - [14/Jun/2012:10:35:57 -0400] "POST / HTTP/1.1" 200 311 Set-Job-Attributes successful-ok
```

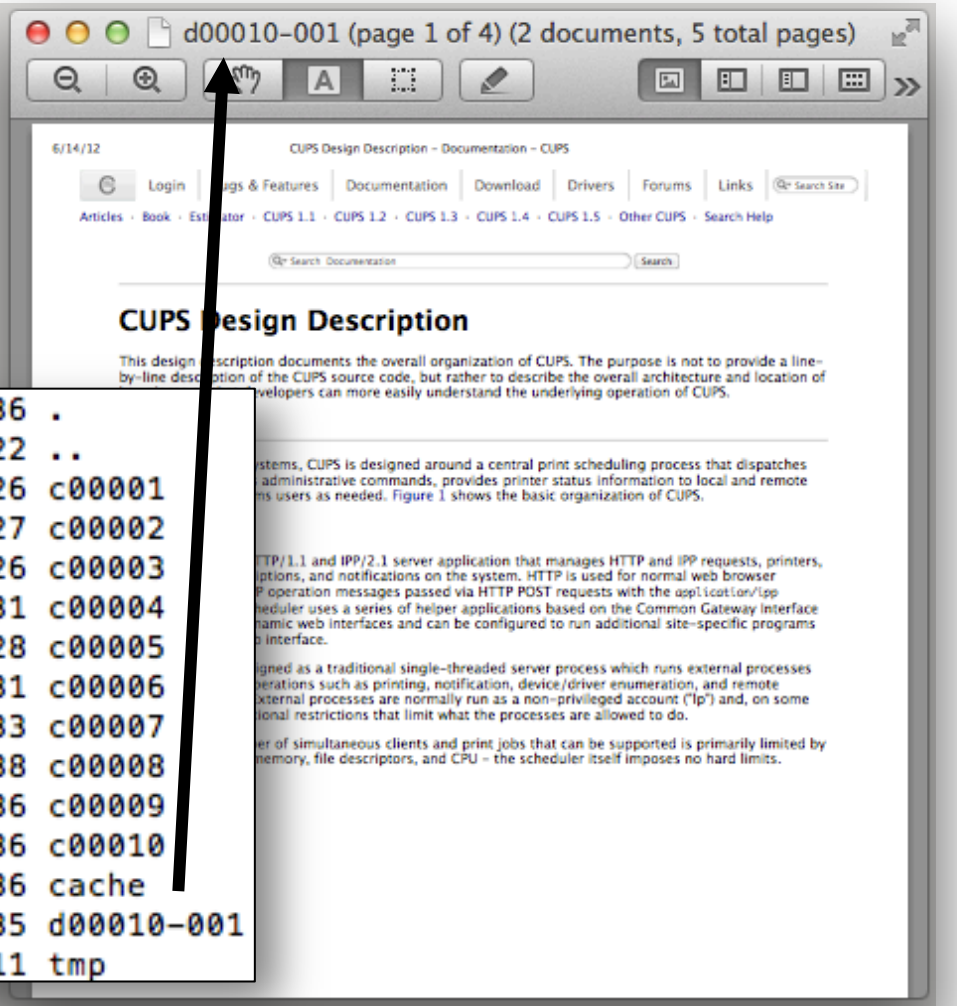
PRINTER CONTROL FILES /PRIVATE/VAR/SPOOL/CUPS

- Nine Printer Control Jobs (c#####)

```
sh-3.2# pwd
/private/var/spool/cups
sh-3.2# ls -la
total 72
drwx--x---  13 root  _lp     442 Jun 14 10:36 .
drwxr-xr-x   7 root  wheel   238 May  9 19:22 ..
-rw-------   1 root  _lp    1841 May 31 20:26 c00001
-rw-------   1 root  _lp    1883 May 31 20:27 c00002
-rw-------   1 root  _lp    1883 Jun  1 17:26 c00003
-rw-------   1 root  _lp    1883 Jun  1 17:31 c00004
-rw-------   1 root  _lp    1815 Jun  1 17:28 c00005
-rw-------   1 root  _lp     723 Jun  1 17:31 c00006
-rw-------   1 root  _lp    1883 Jun  1 17:33 c00007
-rw-------   1 root  _lp    1883 Jun  1 17:38 c00008
-rw-------   1 root  _lp    1873 Jun 14 10:36 c00009
drwxrwxr-x   8 root  _lp     272 Jun 14 10:46 cache
drwxrwx--T   2 root  _lp      68 Jun 19  2011 tmp
```

PRINTER DATA FILES /PRIVATE/VAR/SPOOL/CUPS

- Data Files (d#####)
- Removed immediately after successful print.
- PDF Files




```
drwx--x---  15 root  _lp       510 Jun 14 12:36 .
drwxr-xr-x   7 root  wheel      238 May  9 19:22 ..
-rw-------   1 root  _lp      1841 May 31 20:26 c00001
-rw-------   1 root  _lp      1883 May 31 20:27 c00002
-rw-------   1 root  _lp      1883 Jun  1 17:26 c00003
-rw-------   1 root  _lp      1883 Jun  1 17:31 c00004
-rw-------   1 root  _lp      1815 Jun  1 17:28 c00005
-rw-------   1 root  _lp       723 Jun  1 17:31 c00006
-rw-------   1 root  _lp      1883 Jun  1 17:33 c00007
-rw-------   1 root  _lp      1883 Jun  1 17:38 c00008
-rw-------   1 root  _lp      1873 Jun 14 10:36 c00009
-rw-------   1 root  _lp      1878 Jun 14 12:36 c00010
drwxrwxr-x   8 root  _lp       272 Jun 14 12:36 cache
-rw-r-----   1 root  _lp    608373 Jun 14 12:35 d00010-001
drwxrwx--T   2 root  _lp        68 Jun 19  2011 tmp
```

oompa@csh.rit.edu | @iamevltwin

TEMPORAL CHANGES & CONTEXT

oompa@csh.rit.edu | @iamevltwin

TIME CHANGES: GOING BACK IN TIME
SYSTEM.LOG

```
Jun 16 14:50:56 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] Invalidating
_selectedCityLayer
Jun 16 14:50:56 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good
cachedValue:1.000000
Jun 16 14:50:56: --- last message repeated 4 times ---
Jun 16 14:50:56 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] Invalidating
_selectedCityLayer
Jun 16 14:50:56 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good
cachedValue:1.000000
Jun 16 14:50:56: --- last message repeated 1 time ---
Jun 16 14:50:56 bit System Preferences[1828]: **** ERROR: -[GEOCityPickerView
_bindPublicToPrivateProperties] UI is already bounded
Jun 16 14:50:59 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good
cachedValue:1.000000
Jun 16 11:51:05: --- last message repeated 4 times ---
Jun 16 11:51:05 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] Invalidating
_selectedCityLayer
Jun 16 11:51:05 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good
cachedValue:1.000000
Jun 16 11:51:06 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] Invalidating
_selectedCityLayer
Jun 16 11:51:06 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good
cachedValue:1.000000
Jun 16 11:51:06 bit ntpd[1848]: proto: precision = 1.000 usec
```

TIME CHANGES:
TIME ZONE - /ETC/LOCALTIME

```
bit:etc oompa$ pwd
/etc
bit:etc oompa$ ls -l localtime
lrwxr-xr-x  1 root  wheel  39 Jun 16 11:51 localtime
-> /usr/share/zoneinfo/America/Los_Angeles
```

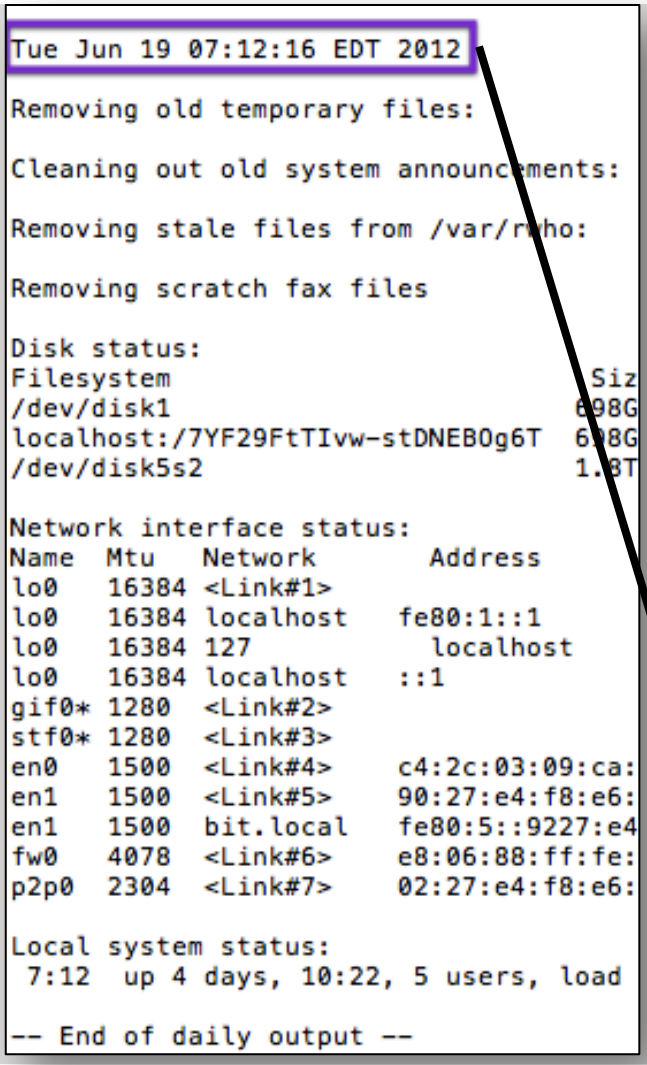
TIME CHANGES: BACK TO THE FUTURE SYSTEM.LOG (10.8-)

```
Jun 16 12:08:04 bit System Preferences[1914]: -[GEOWorldTimeZoneView
selectedCityLayer] all good  cachedValue:1.000000
Jun 16 12:08:04: --- last message repeated 1 time ---
Jun 16 12:08:04 bit System Preferences[1914]: **** ERROR: -
[GEOCityPickerView _bindPublicToPrivateProperties] UI is already
bounded
Jun 16 12:08:06 bit System Preferences[1914]: -[GEOWorldTimeZoneView
selectedCityLayer] all good  cachedValue:1.000000
Jun 16 15:08:09: --- last message repeated 9 times ---
Jun 16 15:08:09 bit System Preferences[1914]: WARNING: -
[GEOTimezoneHitMap fileNameAtLongitude:latitude:] no time zone area
found
Jun 16 15:08:13 bit System Preferences[1914]: -[GEOWorldTimeZoneView
selectedCityLayer] all good  cachedValue:1.000000
Jun 16 15:08:15: --- last message repeated 5 times ---
```

TIME CHANGES: BACK TO THE FUTURE AUTHD.LOG (10.9)

```
May 19 12:28:35 word com.apple.authd[36]: Succeeded
authorizing right 'system.preferences' by client '/System/
Library/PreferencePanes/DateAndTime.prefPane/Contents/
XPCServices/
com.apple.preference.datetime.remoteservice.xpc' [17859] for
authorization created by '/System/Library/PreferencePanes/
DateAndTime.prefPane/Contents/XPCServices/
com.apple.preference.datetime.remoteservice.xpc' [17859] (2,0)
May 19 12:28:35 word com.apple.authd[36]: Succeeded
authorizing right 'system.preferences.datetime' by client '/
System/Library/PreferencePanes/DateAndTime.prefPane/Contents/
XPCServices/
com.apple.preference.datetime.remoteservice.xpc' [17859] for
authorization created by '/System/Library/PreferencePanes/
DateAndTime.prefPane/Contents/XPCServices/
com.apple.preference.datetime.remoteservice.xpc' [17859]
(12,0)
```

TIME ZONE CHANGES
DAILY.LOG – SEARCH "2012"



```
Tue Jun 19 07:12:16 EDT 2012

Removing old temporary files:

Cleaning out old system announcements:

Removing stale files from /var/r
ho:

Removing scratch fax files

Disk status:
Filesystem                                Siz
/dev/disk1                                698G
localhost:/7YF29FtTIvw-stDNEBOg6T         698G
/dev/disk5s2                              1.8T

Network interface status:
Name  Mtu   Network       Address
lo0   16384 <Link#1>
lo0   16384 localhost   fe80:1::1
lo0   16384 127           localhost
lo0   16384 localhost   ::1
gif0* 1280  <Link#2>
stf0* 1280  <Link#3>
en0   1500  <Link#4>    c4:2c:03:09:ca:
en1   1500  <Link#5>    90:27:e4:f8:e6:
en1   1500  bit.local   fe80:5::9227:e4
fw0   4078  <Link#6>    e8:06:88:ff:fe:
p2p0  2304  <Link#7>    02:27:e4:f8:e6:

Local system status:
 7:12  up 4 days, 10:22, 5 users, load

-- End of daily output --
```

```
Tue Jun  5 08:50:04 EDT 2012
Wed Jun  6 10:17:44 EDT 2012
Thu Jun  7 08:15:09 EDT 2012
Fri Jun  8 03:15:00 EDT 2012
Sat Jun  9 09:24:18 EDT 2012
Sun Jun 10 09:19:00 EDT 2012
Mon Jun 11 04:01:17 EDT 2012
Tue Jun 12 04:06:51 EDT 2012
Wed Jun 13 08:26:34 EDT 2012
Thu Jun 14 08:47:03 EDT 2012
Fri Jun 15 19:13:34 EDT 2012
Sat Jun 16 11:00:19 EDT 2012
Sun Jun 17 07:57:40 PDT 2012
Mon Jun 18 05:34:50 PDT 2012
Tue Jun 19 07:12:16 EDT 2012
```

TEMPORAL CONTEXT

Carved & Extracted Files

May not contain context

- Year
- Time Zone

```
Jun 19 07:13:14 bit kernel[0]: PPTP domain init
Jun 19 07:13:16 bit kernel[0]: nd6_setmtu: new link MTU on ppp0 (1276) is too small for IPv6
Jun 19 07:13:42 bit kernel[0]: IOSurface: buffer allocation size is zero
Jun 19 07:19:55 bit kernel[0]: hibernate image path: /var/vm/sleepimage
Jun 19 07:19:55 bit kernel[0]: sizeof(IOHibernateImageHeader) == 512
Jun 19 07:19:55 bit kernel[0]: Opened file /var/vm/sleepimage, size 8589934592, partition base 0x0, maxio 400000 ssd 0
Jun 19 07:19:55 bit kernel[0]: hibernate image major 14, minor 0, blocksize 512, pollers 4
Jun 19 07:19:55 bit kernel[0]: hibernate_alloc_pages flags 00000000, gobbling 0 pages
Jun 19 07:19:55 bit kernel[0]: hibernate_setup(0) took 0 ms
Jun 19 07:19:55 bit kernel[0]: en1: BSSID changed to 00:19:07:96:03:10
Jun 19 07:19:55 bit kernel[0]: wlEvent: en1 en1 Link DOWN virtIf = 0
Jun 19 07:19:55 bit kernel[0]: AirPort: Link Down on en1. Reason 8 (Disassociated because station leaving).
```

DATE & TIME SEARCH
EPOCH & TIMESTAMP FORMATS

kernel.log/system.log

- Jun 19 09:20:16 bit kernel[0]: nspace-handler-set-snapshot-time: **1340112018**
- Jun 12 10:08:15 bit kernel[0]: RTC: maintenance alarm **2012/6/12 14:08:14**, sleep **2012/6/12 12:08:46**

system.log

- Jun 13 09:55:31 bit mtmd[64]: Set snapshot time:**1339595733** (current time:**1339595731**)
- Jun 12 10:16:35 localhost bootlog[0]: BOOT_TIME **1339510595** 0
- Jun 9 10:21:53 bit shutdown[309]: SHUTDOWN_TIME: **1339251713** 535787
- Jun 12 17:23:44 bit com.apple.backupd[4046]: Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/**2012-06-10-012553** (50.5 MB)
- Jun 12 10:17:42 bit [0x0-0x8008].com.google.Chrome[141]: **2012-06-12 14:17:42.785** Google Chrome Helper[196:207] Error received in message reply handler: Connection invalid

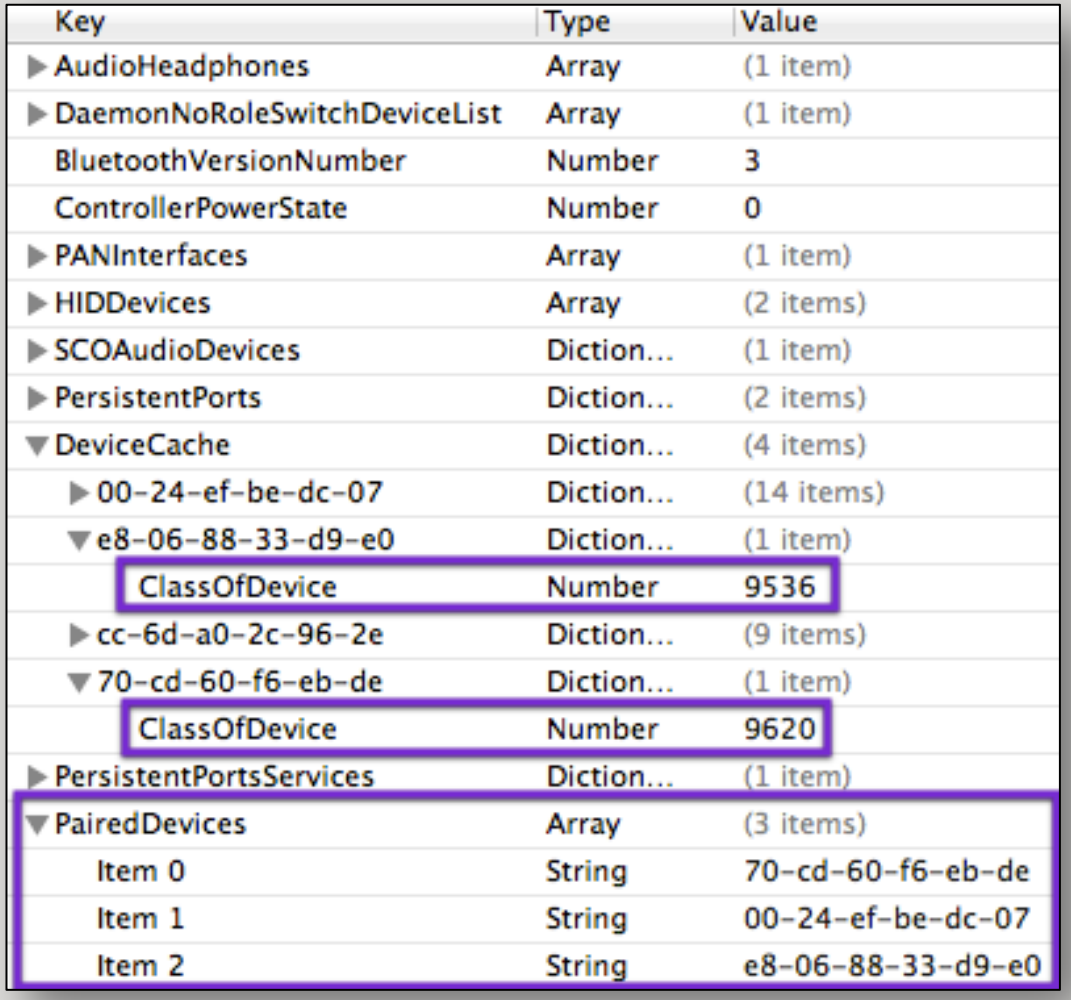
BLUETOOTH

oompa@csh.rit.edu | @iamevltwin

BLUETOOTH DEVICES
SYSTEM.LOG – SEARCH "BLUED"

```
Jun 17 09:36:26 bit com.apple.blued[3545]: link key found for
device: 70-cd-60-f6-eb-de
Jun 17 09:36:26 bit com.apple.blued[3545]: link key found for
device: e8-06-88-33-d9-e0
Jun 17 12:57:00 bit blued[3853]: Removing Bluetooth configured
device: 00-24-ef-be-dc-07
Jun 17 13:10:20 bit com.apple.blued[3853]: link key found for
device: 70-cd-60-f6-eb-de
Jun 17 13:10:20 bit com.apple.blued[3853]: link key found for
device: e8-06-88-33-d9-e0
```

/LIBRARY/PREFERENCES/ COM.APPLE.BLUETOOTH.PLIST (10.7)



Key	Type	Value
▶ AudioHeadphones	Array	(1 item)
▶ DaemonNoRoleSwitchDeviceList	Array	(1 item)
BluetoothVersionNumber	Number	3
ControllerPowerState	Number	0
▶ PANInterfaces	Array	(1 item)
▶ HIDDevices	Array	(2 items)
▶ SCOAudioDevices	Diction…	(1 item)
▶ PersistentPorts	Diction…	(2 items)
▼ DeviceCache	Diction…	(4 items)
▶ 00-24-ef-be-dc-07	Diction…	(14 items)
▼ e8-06-88-33-d9-e0	Diction…	(1 item)
ClassOfDevice	Number	9536
▶ cc-6d-a0-2c-96-2e	Diction…	(9 items)
▼ 70-cd-60-f6-eb-de	Diction…	(1 item)
ClassOfDevice	Number	9620
▶ PersistentPortsServices	Diction…	(1 item)
▼ PairedDevices	Array	(3 items)
Item 0	String	70-cd-60-f6-eb-de
Item 1	String	00-24-ef-be-dc-07
Item 2	String	e8-06-88-33-d9-e0

/LIBRARY/PREFERENCES/ COM.APPLE.BLUETOOTH.PLIST (10.8+)

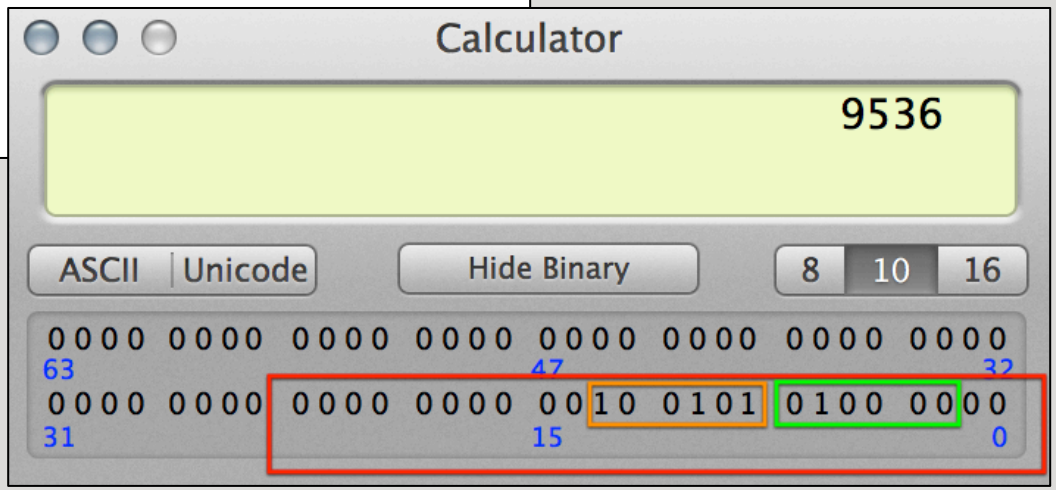
▼ 00-0d-44-bc-4d-81	Dictionary	(16 items)
LastServicesUpdate	Date	Dec 12, 2012 5:22:59 PM
ClockOffset	Number	13,678
Name	String	Logitech Boombox
LMPSubversion	Number	7,213
InquiryRSSI	Number	0
SupportedFeatures	Data	<8759ff9b fe8fffff>
LastNameUpdate	Date	Dec 6, 2012 7:12:43 AM
PageScanPeriod	Number	0
LMPVersion	Number	5
PageScanRepetitionMode	Number	1
LastInquiryUpdate	Date	Dec 15, 2012 11:02:52 AM
Services	Data	<040b7374 7265616d 7479
PageScanMode	Number	0
Manufacturer	Number	10
EIRData	Data	<11094c6f 67697465 6368
ClassOfDevice	Number	2,360,340

DETERMINE BLUETOOTH CLASS OF DEVICE

/SYSTEM/LIBRARY/FRAMEWORKS/IOBLUETOOTH.FRAMEWORK/HEADERS/

Bluetooth.h

```
//  Physical layout of the "class of device/service" field (see Bluetooth Assigned Numbers section 1.2):
//
//   2 2 2 2 1 1 1 1 1 1 1 1 1 1
//   3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0  <- Bit Transmission Order
//  +---------------+---------------+---------------+
//  |    octet 3    |    octet 2    |    octet 1    | <- Octet Transmission Order
//  +---------------+---------------+---------------+
//  <------ 11 bits ------>< 5 bits ><- 6 bits ->
//  +---------------------+---------+-----------+-+-+
//  |   Service Classes   | Major   |  Minor    | | |
//  +-+-+-+-+-+-+-+-+-+-+-+  Device |   Device  |0|0|
//  | | | | | | | |*|*|*| |   Class |    Class  | | |
//  +-+-+-+-+-+-+-+-+-+-+-+---------+-----------+-+-+
//    | | | | | | | |       |                     |
//    | | | | | | | |       + Limited Discoverable   +- Format Type
//    | | | | | | | +- Networking
//    | | | | | | +- Rendering
//    | | | | | +- Capturing
//    | | | | +- Object Transfer
//    | | | +- Audio
//    | | +- Telephony
//    +- Information
```



DETERMINE BLUETOOTH CLASS OF DEVICE

/SYSTEM/LIBRARY/FRAMEWORKS/IOBLUETOOTH.FRAMEWORK/HEADERS/

```
//
// Device Class Major
//

enum
{
    kBluetoothDeviceClassMajorMiscellaneous             = 0x00,     // [00000] Miscellaneous
    kBluetoothDeviceClassMajorComputer                  = 0x01,     // [00001] Desktop, Notebook, PDA, Organizers, etc...
    kBluetoothDeviceClassMajorPhone                     = 0x02,     // [00010] Cellular, Cordless, Payphone, Modem, etc...
    kBluetoothDeviceClassMajorLANAccessPoint            = 0x03,     // [00011] LAN Access Point
    kBluetoothDeviceClassMajorAudio                     = 0x04,     // [00100] Headset, Speaker, Stereo, etc...
    kBluetoothDeviceClassMajorPeripheral                = 0x05,     // [00101] Mouse, Joystick, Keyboards, etc...
    kBluetoothDeviceClassMajorImaging                   = 0x06,     // [00110] Printing, scanner, camera, display, etc...
    kBluetoothDeviceClassMajorWearable                  = 0x07,     // [00111] Wearable
    kBluetoothDeviceClassMajoToy                        = 0x08,     // [01000] Toy
    kBluetoothDeviceClassMajoHealth                     = 0x09,     // [01001] Health devices
    kBluetoothDeviceClassMajorUnclassified              = 0x1F,     // [11111] Specific device code not assigned
```

ICLOUD

oompa@csh.rit.edu | @iamevltwin

ICLOUD – LOGS
~/LIBRARY/LOGS/UBIQUITY/UBIQUITY.LOG

```
[ERROR]    36607b4ef66e2 [13/11/02 11:39:16.090] {195BBE38}
200.com.apple.ubiquity.SRConnection.callouts.0x7fa891c11a10 service_get_requested_path_status:344
can't find item for path '/Users/sledwards/Library/Mobile Documents/com~apple~TextEdit/Documents/
Untitled 2.rtf'
[warn]     36607b97c864e [13/11/02 11:39:16.166] {195BBE38} 200.fsevents update_item_unsafe:2763
unlocked! fields (change-id|root-id|local-rank|file-id|owner-id|last-editor-id|size|ea-size|
checksum|state|mod-time) of item i:0x0001000000000124 c:0x00010000000002fb rk:1658 p:
0x0005000000000112 r:0x0002000000000100 o:0x0001 le:0x00010000000002fb n:"Untitled 2.rtf" s:(meta|
hidden-ext) f:12409199 z:314 eaz:178 mt:1383406756 ct:1383406756 md:0644/-rw-r--r-- ck:
0197ac6b9b7de709b8574a59beefe0ac4e1d37ee3e  orig-s:(dead|hidden-ext)
[ERROR]    3660ad58f84ef [13/11/02 11:39:29.522] {195BBE38}
200.com.apple.ubiquity.SRConnection.callouts.0x7fa891c11a10 service_get_requested_path_status:344
can't find item for path '/Users/sledwards/Library/Mobile Documents/com~apple~TextEdit/Documents/
iCloudFTW.rtf'
[ERROR]    3660ad5da9978 [13/11/02 11:39:29.527] {195BBE38}
200.com.apple.ubiquity.SRConnection.callouts.0x7fa891c11a10 service_get_requested_path_status:344
can't find item for path '/Users/sledwards/Library/Mobile Documents/com~apple~TextEdit/Documents/
iCloudFTW.rtf'
```

ICLOUD – LOGS
~/LIBRARY/LOGS/UBIQUITY/UBIQUITY-DIGEST.LOG

```
[13/11/02 11:36:13.403] Sending 15 items to "iCloud"
[13/11/02 11:36:13.819] iCloud wants us to upload 7 items
[13/11/02 11:36:15.347] uploaded 'id:0x00010000000002e3' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:15.350] uploaded 'id:0x00010000000002e1' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:15.351] uploaded 'id:0x00010000000002e5' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:15.351] uploaded id:0x00010000000002dd to iCloud
[13/11/02 11:36:15.352] uploaded 'id:0x00010000000002e2' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:15.352] uploaded 'id:0x00010000000002ea' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:15.352] uploaded 'id:0x00010000000002e9' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:15.601] Received 15 item updates from "iCloud"
[13/11/02 11:36:26.401] Sending 15 items to "iCloud"
[13/11/02 11:36:26.553] iCloud wants us to upload 6 items
[13/11/02 11:36:27.831] uploaded 'id:0x00010000000002e1' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:27.835] uploaded 'id:0x00010000000002e5' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:27.837] uploaded 'id:0x00010000000002e9' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:27.837] uploaded 'id:0x00010000000002e2' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:27.838] uploaded id:0x00010000000002dd to iCloud
[13/11/02 11:36:27.838] uploaded 'id:0x00010000000002ea' in package 'id:0x00010000000002de' to iCloud
[13/11/02 11:36:29.188] Received 15 item updates from "iCloud"
[13/11/02 11:39:18.172] Sending 1 items to "iCloud"
[13/11/02 11:39:19.373] iCloud wants us to upload 1 items
[13/11/02 11:39:20.048] uploaded id:0x0001000000000124 to iCloud
[13/11/02 11:39:20.142] Received 1 item updates from "iCloud"
[13/11/02 11:39:31.648] Sending 2 items to "iCloud"
[13/11/02 11:39:31.760] Received 1 item updates from "iCloud"
```

ICLOUD – MOBILE DOCUMENTS ~/LIBRARY/MOBILE DOCUMENTS/

- ~/Library/Mobile Documents/
- Local Storage of iCloud Data & Documents
  - Keynote
  - Numbers
  - Pages
  - TextEdit
  - Notes
  - Preview
  - Passes

```
bash-3.2# pwd
/Users/oompa/Library/Mobile Documents
bash-3.2# tree -L 2 .
.
├── com~apple~Keynote
│   ├── Documents
│   └── iWorkPreviews
├── com~apple~Notes
│   └── Documents
├── com~apple~Numbers
│   ├── Documents
│   └── iWorkPreviews
├── com~apple~Pages
│   ├── Documents
│   └── iWorkPreviews
├── com~apple~Preview
│   └── Documents
├── com~apple~TextEdit
│   └── Documents
├── com~apple~TextInput
│   ├── Dictionaries
│   └── Documents
├── com~apple~mail
│   ├── Data
│   └── Documents
├── com~apple~shoebox
│   ├── Documents
│   └── UbiquitousCards
└── com~apple~system~spotlight
    └── mdlabels
```

FACETIME

oompa@csh.rit.edu | @iamevltwin

FACETIME – FACETIME ACCOUNT INFO
~/LIBRARY/PREFERENCES/ COM.APPLE.IMSERVICE.FACETIME.PLIST

▼ Root	Dictionary	(3 items)
▼ ActiveAccounts	Array	(1 item)
Item 0	String	6CE7388C-C134-45D1-BDD1-F176B5D5A34A
▼ Accounts	Dictionary	(1 item)
▼ 6CE7388C-C134-45D1-BDD1-F176B5D5A34A	Dictionary	(10 items)
AuthID	String	D:247[redacted]
LoginAs	String	E:oompa@csh.rit.edu
▼ AccountPrefs	Dictionary	(0 items)
▼ Profile	Dictionary	(5 items)
▼ ServerContext	Dictionary	(0 items)
Number	String	+1571[redacted]
ErrorCode	Number	-1
Status	Number	3
Region	String	R:US
▼ Registration	Dictionary	(2 items)
ErrorCode	Number	-1
Status	Number	5
AuthToken	String	KQXZV2XXXXXXba313b8ccab3414001aee7df8b
▼ Aliases	Array	(4 items)
▼ Item 0	Dictionary	(2 items)
Alias	String	oompa@csh.rit.edu
Status	Number	3
▶ Item 1	Dictionary	(2 items)
▶ Item 2	Dictionary	(2 items)
▶ Item 3	Dictionary	(2 items)
InvitationProtocolVersion	Number	21
ServerHost	String	init.ess.apple.com
▼ VettedAliases	Array	(4 items)
Item 0	String	iamevltwin@icloud.com
Item 1	String	[redacted]
Item 2	String	oompa@csh.rit.edu
Item 3	String	sledwards@gmail.com
▼ OnlineAccounts	Array	(1 item)
Item 0	String	6CE7388C-C134-45D1-BDD1-F176B5D5A34A

FACETIME LOG – INITIAL CONTACT (INCOMING/OUTGOING) ~/LIBRARY/LOGS/FACETIME.LOG

```
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Peers for this call (null)
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Is reinitiate: NO
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Received invite push from: +1571[redacted] (P:+1571[redacted]
type: video
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Conference ID:
0D91F56BF9FE0436F26CC7C5C3B94F1270CCB94B34E8BD1E
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Returning device support registration supported: YES
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] ConferenceDictionary: {
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Generated Properties: {
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Should call be allowed ? YES, isBlocked = NO
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Retargeting peer ID: P:+1571[redacted]  display ID:
+1571[redacted]  token: <e95bf1c2 186f22c5 3146e5a2 02835465 66a7d140 c360849a 92016843 a6df2eda>  cid:
0D91F56BF9FE0436F26CC7C5C3B94F1270CCB94B34E8BD1E
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Resulting peerInfo {
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Conference map after retarget: {
2014-05-08 21:46:41 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] All maps after retarget: {
2014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] respondToVCInvitationWithPerson: +1571[redacted]  properties:
2014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] All conference maps {
2014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Found peer ID: P:+1571[redacted] for display ID: +1571[redacted]
(Peer info: {
2014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Found token: <e95bf1c2 186f22c5 3146e5a2 02835465 66a7d140
c360849a 92016843 a6df2eda> for peer ID: P:+1571[redacted]
2014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Reponse dictionary: {
2014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Returning device support registration supported: YES
2014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Choosing callerID iamevltwin@[redacted] callerURI
mailto:iamevltwin[redacted] from aliases (
2014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default]   =>  Found account: IDSAccount: 0x7ffe31d060f0 [Service:
com.apple.ess  User: oompa@csh.rit.edu  ID: 3B49DCCC-0163-4B62-BEC9-82C4E354439E  Type: Apple ID  Active: YES  Registration Status:
Registered]
```

```
2014-05-19 11:09:09 -0400 [FaceTimeServiceSession(imagent:13311:YES):Default] requestVCWithPerson: +1571[redacted]  properties: {
2014-05-19 11:09:09 -0400 [FaceTimeServiceSession(imagent:13311:YES):Default] Sending invitation to: +1571[redacted]  from:
mailto:iamevltwin@[redacted]
2014-05-19 11:09:09 -0400 [FaceTimeServiceSession(imagent:13311:YES):Default] Returning device support registration supported: YES
2014-05-19 11:09:09 -0400 [FaceTimeServiceSession(imagent:13311:YES):Default] Choosing callerID iamevltwin@[redacted] callerURI
mailto:iamevltwin@[redacted] from aliases (
2014-05-19 11:09:09 -0400 [FaceTimeServiceSession(imagent:13311:YES):Default]   =>  Found account: IDSAccount: 0x7fdd696167c0 [Service:
com.apple.ess  User: oompa@csh.rit.edu  ID: 3B49DCCC-0163-4B62-BEC9-82C4E354439E  Type: Apple ID  Active: YES  Registration Status: Registered]
```

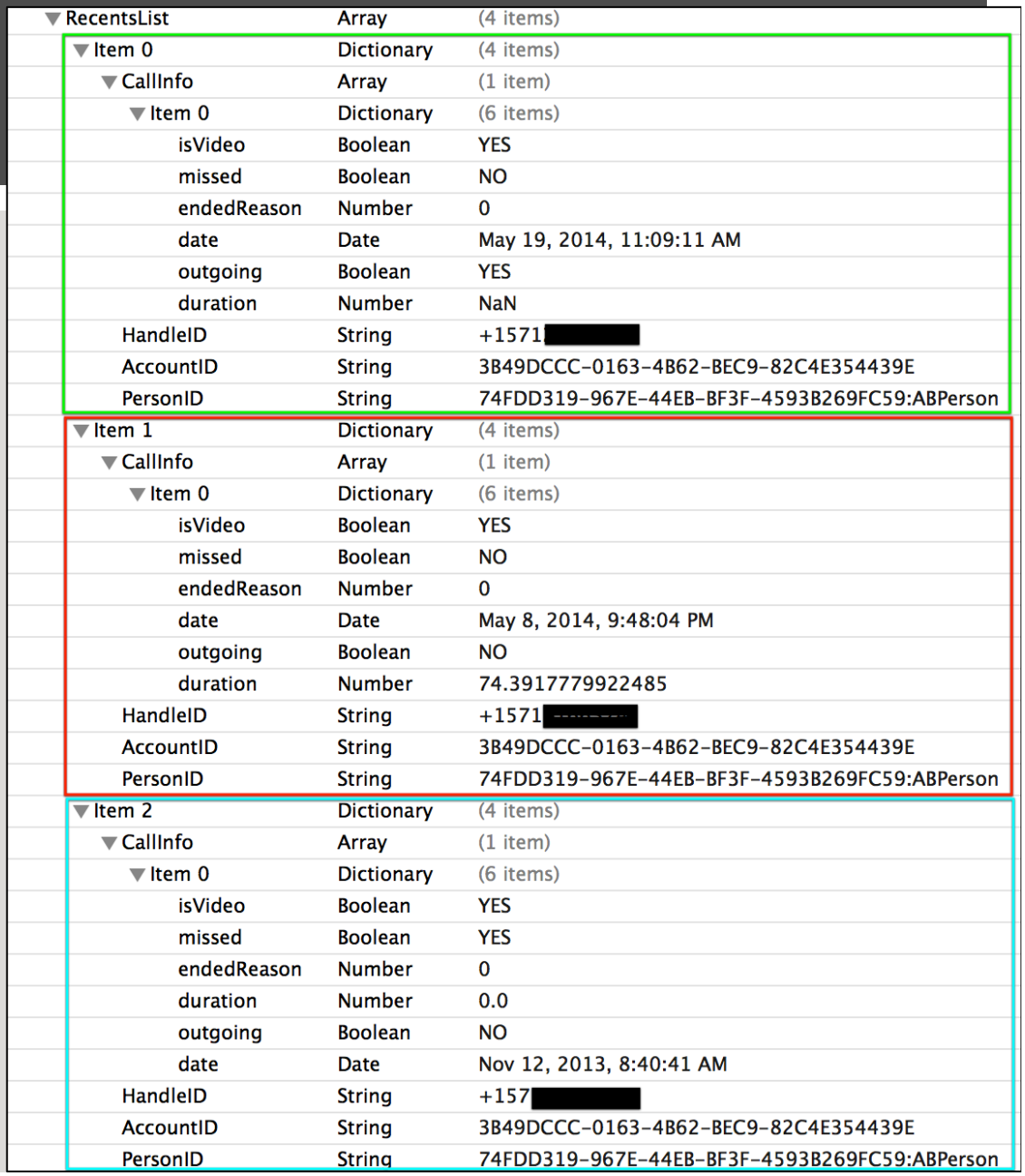
FACETIME LOG – ACCEPT/END CALLS ~/LIBRARY/LOGS/FACETIME.LOG

```
014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Sending accept to: +1571[redacted] for conference:
D91F56BF9FE0436F26CC7C5C3B94F1270CCB94B34E8BD1E
014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default]   =>  Returning topic: com.apple.ess
014-05-08 21:46:47 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default]   =>  Found account: IDSAccount: 0x7ffe31d060f0 [Service
om.apple.ess  User: oompa@csh.rit.edu  ID: 3B49DCCC-0163-4B62-BEC9-82C4E354439E  Type: Apple ID  Active: YES  Registration Status:
egistered]
```

```
2014-05-08 21:46:52 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Checking peers with peerID P:+1571[redacted] conferenceID
0D91F56BF9FE0436F26CC7C5C3B94F1270CCB94B34E8BD1E
2014-05-08 21:46:52 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] My GUID: E175D6B8-C670-441D-948A-F61769DCA884
2014-05-08 21:46:52 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Conference maps {
2014-05-08 21:46:52 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Looking for peer in map {
2014-05-08 21:46:52 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Peers (
2014-05-08 21:46:52 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Peer info {
2014-05-08 21:46:52 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Comparing P:+1571[redacted] to P:+1571[redacted]
2014-05-08 21:46:52 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Found display ID: +1571[redacted] for peer ID: P:+1571[redacted]
2014-05-08 21:46:52 -0400 [FaceTimeServiceSession(imagent:5040:YES):Default] Received relay cancel push from: +1571[redacted] (P:
+1571[redacted]
```

FACETIME – FACETIME RECENT CALLS

- ~/Library/Preferences/ByHost/com.apple.FaceTime.<GUID>.plist



RecentsList	Array	(4 items)
Item 0	Dictionary	(4 items)
CallInfo	Array	(1 item)
Item 0	Dictionary	(6 items)
isVideo	Boolean	YES
missed	Boolean	NO
endedReason	Number	0
date	Date	May 19, 2014, 11:09:11 AM
outgoing	Boolean	YES
duration	Number	NaN
HandleID	String	+1571[redacted]
AccountID	String	3B49DCCC-0163-4B62-BEC9-82C4E354439E
PersonID	String	74FDD319-967E-44EB-BF3F-4593B269FC59:ABPerson
Item 1	Dictionary	(4 items)
CallInfo	Array	(1 item)
Item 0	Dictionary	(6 items)
isVideo	Boolean	YES
missed	Boolean	NO
endedReason	Number	0
date	Date	May 8, 2014, 9:48:04 PM
outgoing	Boolean	NO
duration	Number	74.3917779922485
HandleID	String	+1571[redacted]
AccountID	String	3B49DCCC-0163-4B62-BEC9-82C4E354439E
PersonID	String	74FDD319-967E-44EB-BF3F-4593B269FC59:ABPerson
Item 2	Dictionary	(4 items)
CallInfo	Array	(1 item)
Item 0	Dictionary	(6 items)
isVideo	Boolean	YES
missed	Boolean	YES
endedReason	Number	0
duration	Number	0.0
outgoing	Boolean	NO
date	Date	Nov 12, 2013, 8:40:41 AM
HandleID	String	+157[redacted]
AccountID	String	3B49DCCC-0163-4B62-BEC9-82C4E354439E
PersonID	String	74FDD319-967E-44EB-BF3F-4593B269FC59:ABPerson

WHY?

Volumes	Network	Location	User Activity
Backups	Software	System Information	System State
Printing	Temporal Changes	Bluetooth	Communication

ANALYSIS & CORRELATION OF MAC LOGS

Sarah Edwards
@iamevltwin
oompa@csh.rit.edu