

Reverse Engineering Mac Malware

Sarah Edwards

@iamevtwin

mac4n6.com

Scope & Agenda

Malware Triage

~20% Static, ~80% Dynamic

No Assembly

Agenda:

- Static Analysis
 - File Types
 - Analysis Tools
- Dynamic Analysis
 - Virtualization
 - Application Tracing
 - Analysis Tools
- Analysis Examples

Static Analysis

Locate & Extract the Executable Files

File Types:

- Application Bundles
- Mach-O
- PKG Files

Tools:

- MachOView
- lipo
- Strings || srch_strings
- nm
- codesign
- Hopper

Locate the Malware

Application Bundle (*.app)

PKG File

Mach-O Executable

...

Office Document

ZIP Archive

JAR File

...others...

Application Bundle

Directory

Contents:

- Info.plist (*required*)
 - Configuration Information
- Executable (*required*)
 - Located anywhere in bundle
- MacOS Directory
 - Executable may be in here too!
- Resources Directory
 - Supporting Files

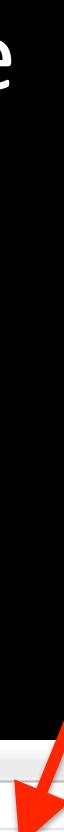
```
Safari.app/
└── Contents
    ├── Info.plist
    ├── MacOS
    ├── PkgInfo
    ├── Resources
    └── _CodeSignature
        └── version.plist
```

```
Dashboard.app/
└── Contents
    ├── Info.plist
    ├── MacOS
    │   └── Dashboard
    ├── PkgInfo
    ├── Resources
    │   └── Dashboard.icns
    └── _CodeSignature
        └── CodeResources
            └── version.plist
```

Application Bundle Crisis Sample

- Executables:
 - IZsROY7X.-MP
 - lUnsA3Ci.Bz7
 - mWgpX-al.8Vq
- Kernel Extension =
6EaqyFfo.zIK.kext

Key	Type	Value
▼ Information Property List	Dictionary	(11 items)
Localization native development region	String	English
Executable file	String	IZsROY7X.-MP
Bundle identifier	String	com.apple.mdworker-user
InfoDictionary version	String	6.0
Bundle name	String	mdworker-user
Bundle OS Type code	String	APPL
Bundle creator OS Type code	String	????
Bundle version	String	1.0
Main nib file base name	String	MainMenu
Principal class	String	NSApplication
NSUIElement	String	1



```
jlc3V7we.app/
└─ Contents
  └─ Info.plist
  └─ MacOS
  └─ Resources
    └─ 6EaqyFfo.zIK.kext
      └─ Contents
        └─ Info.plist
        └─ MacOS
          └─ 6EaqyFfo.zIK
            └─ Resources
  └─ IZsROY7X.-MP
  └─ WeP1xpBU.wA-
  └─ eiYNz1gd.Cfp
  └─ krfhIqFRqIqxU8x6eqo68hVjjq.gai
  └─ krfhIqFRxIqxU8x6eqojjUo8jq.gai
  └─ krfhIqFjqIqxU8x6e68UoHoQqq.gai
  └─ krfhIqFjqIqxU8x6e68eqUxHjq.gai
  └─ krfhIqFjqIqxU8x6e6hFUee6qq.gai
  └─ krfhIqFjqIqxU8x6e6hFVVVFVjq.gai
  └─ krfhIqFjqIqxU8x6e6hVDRHjq.gai
  └─ krfhIqFjqIqxU8x6e6hVhU8Zqq.gai
  └─ krfhIqFjqIqxU8x6e6hjFQqRjq.gai
  └─ krfhIqFjqIqxU8x6e6hxQ6joqq.gai
  └─ krfhIqFjqIqxU8x6e6hxqjhDjq.gai
  └─ krfhIqFjqIqxU8x6eFFVHeFDqq.gai
  └─ krfhIqFjqIqxU8x6eFUR8FZZjq.gai
  └─ krfhIqFjqIqxU8x6eFVHoHHhjq.gai
  └─ krfhIqFjqIqxU8x6eFVx6QRFqq.gai
  └─ krfhIqFjqIqxU8x6eFqDFDHZjq.gai
  └─ krfhIqFjqIqxU8x6eFqHjoUxqq.gai
  └─ krfhIqFjqIqxU8x6eFxZDhDRqq.gai
  └─ krfhIqFjqIqxU8x6eFxj6qQxqq.gai
  └─ krfhIqFjqIqxU8x6exU6jejojq.gai
  └─ krfhIqFjqIqxU8x6exUQhFhZqq.gai
  └─ krfhIqFjqIqxU8x6exUUHHHxqq.gai
  └─ krfhIqFjqIqxU8x6exUjFQVVjq.gai
  └─ krfhIqFjqIqxU8x6exUojDZ8qq.gai
  └─ krfhIqFjqIqxU8x6exoF8VUjjq.gai
  └─ krfhIqqRqIqxU8x6eqojjUo8jq.gai
  └─ lUnsA3Ci.Bz7
  └─ mWgpX-al.8Vq
  └─ mdworker.flg
  └─ q45tyh
```

PKG File

eXtensible ARchiver
(XAR) Archive

Flashback used a fake
“FlashPlayer-11-
macos.pkg” Installer



PKG Files

List & Extract the Malware

```
nibble:malware sledwards$ xar -t -v -f FlashPlayer-11-macos.pkg
-rw-r--r--    alis/wheel          729 2011-10-06 09:09:44 Distribution
drwxr-xr-x    alis/wheel          0 2011-10-06 09:09:44 Resources
drwxr-xr-x    alis/wheel          0 2011-10-06 09:09:44 Resources/en.lproj
-rw-r--r--    alis/wheel        128522 2011-07-22 14:18:25 Resources/en.lproj/background
drwxr-xr-x    alis/wheel          0 2011-10-06 09:09:44 license.pkg
-rw-r--r--    alis/wheel          267 2011-10-06 09:09:44 license.pkg/PackageInfo
-rw-r--r--    alis/wheel        35129 2011-10-06 09:09:43 license.pkg/Bom
-rw-r--r--    alis/wheel          115 2011-10-06 09:09:43 license.pkg/Payload
-rw-r--r--    alis/wheel        32942 2011-10-06 09:09:43 license.pkg/Scripts
```

```
nibble:malware sledwards$ unar FlashPlayer-11-macos.pkg -o flashback_extract/
FlashPlayer-11-macos.pkg: XAR
  license.pkg/ (dir)... OK.
  license.pkg/PackageInfo (267 B)... OK.
  license.pkg/Bom (35129 B)... OK.
  license.pkg/Payload (115 B)... OK.
  license.pkg/Scripts (32942 B)... OK.
  Resources/ (dir)... OK.
  Resources/en.lproj/ (dir)... OK.
  Resources/en.lproj/background (128522 B)... OK.
  Distribution (729 B)... OK.

Successfully extracted to "flashback_extract/FlashPlayer-11-macos".
```

PKG Files

List & Extract the Malware

```
nibble:license.pkg sledwards$ file *
Bom:      Mac OS X bill of materials (BOM) file
PackageInfo: ERROR: line 163: regex error 17, (illegal byte sequence)
Payload:   gzip compressed data, from Unix
Scripts:   gzip compressed data, from Unix
```



```
nibble:license.pkg sledwards$ unar -r Payload
Payload: Gzip
Payload... OK.
Successfully extracted to "./Payload-1".
nibble:license.pkg sledwards$ unar -r Scripts
Scripts: Gzip
Scripts... OK.
Successfully extracted to "./Scripts-1".
```



```
nibble:license.pkg sledwards$ unar -r Payload-1
Payload-1: Cpio
./ (dir)... OK.
./license (0 B)... OK.
Successfully extracted to "Payload-1-1".
nibble:license.pkg sledwards$ unar -r Scripts-1
Scripts-1: Cpio
./ (dir)... OK.
./postinstall (99268 B)... OK.
Successfully extracted to "Scripts-1-1".
```

PKG Files

List & Extract the Malware

- *-1 (First unar - gzip)
- *-1-1 (Second unar - cpio)

```
nibble:license.pkg sledwards$ file *
Bom:      Mac OS X bill of materials (BOM) file
PackageInfo: ERROR: line 163: regex error 17, (illegal byte sequence)
Payload:   gzip compressed data, from Unix
Payload-1:  ASCII cpio archive (pre-SVR4 or odc)
Payload-1-1: directory
Scripts:   gzip compressed data, from Unix
Scripts-1:  ASCII cpio archive (pre-SVR4 or odc)
Scripts-1-1: directory
nibble:license.pkg sledwards$ file Payload-1-1/*
Payload-1-1/license: empty
nibble:license.pkg sledwards$ file Scripts-1-1/*
Scripts-1-1/postinstall: Mach-O universal binary with 2 architectures: [x86_64: Mach-O 64-bit
x86_64 executable] [i386: Mach-O i386 executable]
```

Mach-O Binaries

- Executable Format used on OS X
- Universal (Fat) Binaries
- File Signatures:
 - 0xCAFEBAE – Fat binary
 - 0xFEEDFACE – 32-bit
 - 0xFEEDFACF – 64-bit
 - 0xCEFAEDFE – 32-bit, Little Endian
 - 0xCFFAEDFE – 64-bit, Little Endian

32-Bit/Little Endian

```
nibble:jlc3V7we.app sledwards$ file IZsR0Y7X.-MP
IZsR0Y7X.-MP: Mach-O i386 executable
```

```
0000000: cefa edfe 0700 0000 0300 0000 0200 0000 .....
0000010: 2300 0000 5412 0000 8500 0001 0100 0000 #...T....
0000020: 3800 0000 5f5f 5041 4745 5a45 524f 0000 8...__PAGEZERO..
0000030: 0000 0000 0000 0000 0010 0000 0000 0000 .....
```

Mach-O Binaries

Universal/Fat Binaries

```
00000000: cafe babe 0000 0002 0100 0007 8000 0003 .....  
00000010: 0000 1000 0000 60e8 0000 000c 0000 0007 .....`.....  
00000020: 0000 0003 0000 8000 0000 5e24 0000 000c .....^.$.  
00000030: 0000 0000 0000 0000 0000 0000 0000 0000 .....
```

Intel 32 & 64-bit

```
nibble:jlc3V7we.app sledwards$ file mWgpX-al.8Vq  
mWgpX-al.8Vq: Mach-O universal binary with 2 architectures: [x86_64: Mach-O 64-bit x86_64  
executable] [i386: Mach-O i386 executable]
```

Universal – PowerPC & Intel 32-bit

```
nibble:malware sledwards$ file MacKontrol  
MacKontrol: Mach-O universal binary with 2 architectures: [ppc_7400: Mach-O ppc_7400 executable]  
[i386: Mach-O i386 executable]
```

Universal/Fat Binary File Info

lipo

Review Architecture Details:

- `-info <file>`
- `-detailed_info <file>`

```
nibble:malware sledwards$ lipo -info MacKontrol
Architectures in the fat file: MacKontrol are: ppc7400 i386
nibble:malware sledwards$ lipo -detailed_info MacKontrol
Fat header in: MacKontrol
fat_magic 0xcafebabe
nfat_arch 2
architecture ppc7400
    cputype CPU_TYPE_POWERPC
    cpusubtype CPU_SUBTYPE_POWERPC_7400
    offset 4096
    size 44852
    align 2^12 (4096)
architecture i386
    cputype CPU_TYPE_I386
    cpusubtype CPU_SUBTYPE_I386_ALL
    offset 49152
    size 50692
    align 2^12 (4096)
```

Universal/Fat Binary File Info

lipo

Extract Binaries:

- **-extract <architecture type>**
- **-output <output file>**

```
nibble:malware sledwards$ lipo -extract i386 -output MacKontrol_i386 MacKontrol  
nibble:malware sledwards$ file MacKontrol_i386  
MacKontrol_i386: Mach-O universal binary with 1 architecture: [i386: Mach-O i386 executable]
```

MachOView - Mach Header

sourceforge.net/projects/machoview/

The screenshot shows the MachOView application interface. On the left is a tree view of file contents, and on the right is a table of Mach header fields.

Tree View (Left):

- Executable (X86) [SDK10.6 Target10.5]
 - Mach Header
 - Load Commands
 - Section (__TEXT,__text)
 - Assembly
 - Section (__TEXT,__symbol_stub)
 - Symbol Stubs
 - Section (__TEXT,__stub_helper)
 - Assembly
 - Section (__TEXT,__cstring)
 - C String Literals
 - Section (__TEXT,__const)
 - Section (__TEXT,__unwind_info)
 - Section (__TEXT,__eh_frame)
 - Call Frame 0x53EE0

Offset	Data	Description	Value
00000000	FEEDFACE	Magic Number	MH_MAGIC
00000004	00000007	CPU Type	CPU_TYPE_I386
00000008	00000003	CPU SubType	
	00000003		CPU_SUBTYPE_I386_ALL
0000000C	00000002	File Type	MH_EXECUTE
00000010	00000023	Number of Load Commands	35
00000014	00001254	Size of Load Commands	4692
00000018	01000085	Flags	
	00000001		MH_NOUNDEFS
	00000004		MH_DYLDLINK
	00000080		MH_TWOLEVEL
	01000000		MH_NO_HEAP_EXECUTION

Executables Strings

strings || srch_strings

Extract all strings:

- ASCII Strings
 - `strings -a`
- Unicode Strings (The Sleuth Kit)
 - `srch_strings -a -t`

```
mBackdoorPath
mKext32Path
mKext64Path
mServiceLoaderPath
setMBackdoorPath:
setMKext32Path:
setMKext64Path:
setMSLIplistPath:
setMServiceLoaderPath:
setMExecFlag:
isLion
isLeopard
disableSetugidAuth
enableSetugidAuth
unloadKext
loadKextFor64bit:
dropExecFlag
makeSuidBinary:
isBackdoorPresentInSLI:
createLaunchAgentPlist:forBinary:
c16@0:4@8@12
createSLIplistWithBackdoor
removeBackdoorFromSLIplist
addBackdoorToSLIplist
```

MachOView - Strings

sourceforge.net/projects/machoview/

The screenshot shows the MachOView application interface. The title bar reads "IZsROY7X.-MP". Below the title bar are two tabs: "RAW" and "RVA", with "RVA" being the active tab. A search bar is located at the top right. The main window is divided into two sections: a tree view on the left and a table view on the right.

Tree View (Left):

- Executable (X86) [SDK10.6 Target10.5]
 - Mach Header
 - Load Commands
 - Section (_TEXT, __text)
 - Section (_TEXT, __symbol_stub)
 - Section (_TEXT, __stub_helper)
 - Section (_TEXT, __cstring)
 - C String Literals
 - Section (_TEXT, __const)
 - Section (_TEXT, __ unwind_info)
 - Section (_TEXT, __eh_frame)
 - Section (_DATA, __dyld)
 - Section (_DATA, __nl_symbol_ptr)
 - Section (_DATA, __la_symbol_ptr)
 - Section (_DATA, __data)
 - Section (_DATA, __cfstring)
 - Section (_DATA, __const)
 - Section (_OBJC, __message_refs)
 - Section (_OBJC, __cls_refs)
 - Section (_OBJC, __class)
 - Section (_OBJC, __meta_class)
 - Section (_OBJC, __instance_vars)
 - Section (_OBJC, __inst_meth)
 - Section (_OBJC, __symbols)
 - Section (_OBJC, __module_info)

Offset	Data	Description	Value
000497C7	6D4261636...	CString (length:13)	mBackdoorPath
000497D5	6D4B65787...	CString (length:11)	mKext32Path
000497E1	6D4B65787...	CString (length:11)	mKext64Path
000497ED	6D5365727...	CString (length:18)	mServiceLoaderPath
00049800	7365744D4...	CString (length:17)	setMBackdoorPath:
00049812	7365744D4...	CString (length:15)	setMKext32Path:
00049822	7365744D4...	CString (length:15)	setMKext64Path:
00049832	7365744D5...	CString (length:17)	setMSLIPlistPath:
00049844	7365744D5...	CString (length:22)	setMServiceLoaderPath:
0004985B	7365744D4...	CString (length:13)	setMExecFlag:
00049869	69734C696...	CString (length:6)	isLion
00049870	69734C656...	CString (length:9)	isLeopard
0004987A	646973616...	CString (length:18)	disableSetugidAuth
0004988D	656E61626...	CString (length:17)	enableSetugidAuth
0004989F	756E6C6F6...	CString (length:10)	unloadKext
000498AA	6C6F61644...	CString (length:17)	loadKextFor64bit:
000498BC	64726F704...	CString (length:12)	dropExecFlag
000498C9	6D616B655...	CString (length:15)	makeSuidBinary:
000498D9	697342616...	CString (length:23)	isBackdoorPresentInSLI:
000498F1	637265617...	CString (length:33)	createLaunchAgentPlist:forBinary:
00049913	633136403...	CString (length:12)	c16@0:4@8@12
00049920	637265617...	CString (length:26)	createSLIPlistWithBackdoor
0004993B	72656D6F7...	CString (length:26)	removeBackdoorFromSLIPlist
00049956	616464426...	CString (length:21)	addBackdoorToSLIPlist

Display Symbols

nm

- Variable and Function Names
- Crisis Example:
 - “nm IZsROY7X.-MP”

```
000576b8 S _gAgentCrisis
000576c0 S _gAgentCrisisApp
000576bc S _gAgentCrisisNet
000545d0 D _gBackdoorID
00057698 S _gBackdoorName
000545f0 D _gBackdoorSignature
0005769c S _gBackdoorUpdateName
00054580 D _gConfAesKey
000576a0 S _gConfigurationName
000576a4 S _gConfigurationUpdateName
00057690 S _gControlFlagLock
00054620 D _gDemoMarker
000576a8 S _gInputManagerName
000545b0 D _gInstanceId
000576c4 S _gIsDemoMode
000576ac S _gKext32Name
000576b0 S _gKext64Name
00054550 D _gLogAesKey
00054664 D _gMemCommandMaxSize
00054668 D _gMemLogMaxSize
00054640 D _gMode
0005466c D _gMyXPCName
000576d4 S _gOSBugFix
000576cc S _gOSMajor
000576d0 S _gOSMinor
00057688 S _gOriginalDesktopImage
00057694 S _gSessionKey
000576dc S _gSharedMemoryCommand
000576e0 S _gSharedMemoryLogging
000576c8 S _gSkypeQuality
0005768c S _gSuidLock
000576e4 S _gUtil
00054690 D _gVersion
000576b4 S _gXPCName
000074e1 T _getActiveWindowInfo
00007c87 T _getBSDProcessList
00006f5f T _getHostname
00010ceb T _getRootDomain
00007b3f T _getSystemSerialNumber
```

MachOView - Symbols

sourceforge.net/projects/machoview/

The screenshot shows the MachOView application interface. The title bar reads "IZsROY7X.-MP". The left sidebar contains a tree view of symbols:

- Section (_DATA, __const)
- ▶ Section (_OBJC, __message_refs)
- ▶ Section (_OBJC, __cls_refs)
- ▶ Section (_OBJC, __class)
- ▶ Section (_OBJC, __meta_class)
- ▶ Section (_OBJC, __instance_vars)
- ▶ Section (_OBJC, __inst_meth)
- ▶ Section (_OBJC, __symbols)
- ▶ Section (_OBJC, __module_info)
- ▶ Section (_OBJC, __cls_meth)
- ▶ Section (_OBJC, __property)
- ▶ Section (_OBJC, __class_ext)
- ▶ Section (_OBJC, __category)
- ▶ Section (_OBJC, __cat_inst_meth)
- ▶ Section (_OBJC, __protocol)
- ▶ Section (_OBJC, __cat_cls_meth)
- ▶ Section (_OBJC, __image_info)
- ▶ Function Starts
- ▼ Symbol Table
 - Symbols
- ▼ Dynamic Symbol Table
- External Relocations
- Indirect Symbols
- String Table

The main pane displays a table of symbols:

Offset	Data	Description	Value
0005D8CC	00000B7F	String Table Index	_gAgentCrisis
0005D8D0	0F	Type	
	0E		N_SECT
	01		N_EXT
0005D8D1	0F	Section Index	15 (_DATA, __common)
0005D8D2	0000	Description	
0005D8D4	000576B8	Value	358072 (\$+48)
0005D8D8	00000B8D	String Table Index	_gAgentCrisisApp
0005D8DC	0F	Type	
	0E		N_SECT
	01		N_EXT
0005D8DD	0F	Section Index	15 (_DATA, __common)
0005D8DE	0000	Description	
0005D8E0	000576C0	Value	358080 (\$+56)
0005D8E4	00000B9E	String Table Index	_gAgentCrisisNet
0005D8E8	0F	Type	
	0E		N_SECT
	01		N_EXT
0005D8E9	0F	Section Index	15 (_DATA, __common)
0005D8EA	0000	Description	
0005D8EC	000576BC	Value	358076 (\$+52)
0005D8F0	00000BAF	String Table Index	_gBackdoorID
0005D8F4	0F	Type	

Hopper - hopperapp.com

File: IZsROY7X.hop

Labels Strings

Search

Tag Scope

- RCSMSharedMemory
- RCSMTaskManager
- RCSMUtils
- RESTNetworkProtocol

-[RCSMUtils copyWithZone:]
-[RCSMUtils retain]
-[RCSMUtils retainCount]
-[RCSMUtils release]
-[RCSMUtils autorelease]
-[RCSMUtils isLeopard]
-[RCSMUtils isLion]
-[RCSMUtils executeTask:withArguments:waitUntil...]
-[RCSMUtils removeBackdoorFromSLIList]
-[RCSMUtils createSLIListWithBackdoor]
-[RCSMUtils isBackdoorPresentInSLI:]
-[RCSMUtils openSLIList]
-[RCSMUtils makeSuidBinary:]
-[RCSMUtils dropExecFlag]
-[RCSMUtils init]
+[RCSMUtils allocWithZone:]
+[RCSMUtils sharedInstance]
-[RCSMUtils setMBackdoorPath:]
-[RCSMUtils mBackdoorPath]
-[RCSMUtils setMKext32Path:]
-[RCSMUtils mKext32Path]
-[RCSMUtils setMKext64Path:]
-[RCSMUtils mKext64Path]
-[RCSMUtils setMSLIListPath:]
-[RCSMUtils mSLIListPath]
-[RCSMUtils setMServiceLoaderPath:]
-[RCSMUtils mServiceLoaderPath]
-[RCSMUtils setMExecFlag:]
-[RCSMUtils mExecFlag]
-[RCSMUtils disableSetuidAuth]
-[RCSMUtils enableSetuidAuth]
-[RCSMUtils unloadKext]
-[RCSMUtils loadKextFor64bit]
-[RCSMUtils createLaunchAgentPlist:forBinary:]
-[RCSMUtils saveSLIListAtPath:]
-[RCSMUtils searchSLIListForKey:]
-[RCSMUtils addBackdoorToSLIList]

0x00005384 mov dword [ss:esp+0xc], eax
0x00005388 lea eax, dword [ds:esi-0x5cd+cfstring__sbin_kextload]
0x0000538e mov dword [ss:esp+0x8], eax ; @"/sbin/kextload"
0x00005392 jmp 0x523c
; endp

===== BEGINNING OF PROCEDURE =====

- [RCSMUtils createLaunchAgentPlist:forBinary:]

0x00005397 push ebp
0x00005398 mov ebp, esp
0x0000539a push ebx
0x0000539b push edi
0x0000539c push esi
0x0000539d sub esp, 0x5c
0x000053a0 call 0x53a5
0x000053a5 pop esi
0x000053a6 mov eax, dword [ds:esi-0x53a5+cls_NSMutableDictionary] ; XREF=-[RCSMUtils createLaunchAgentPlist:forBinary:]
0x000053a7 mov ecx, dword [ds:esi-0x53a5+objc_msg_dictionaryWithCapacity_] ; @selector(dictionaryWithCapacity:)
0x000053a8 dword [ss:esp+0x4], ecx
0x000053b2 mov dword [ss:esp], eax
0x000053b6 mov dword [ss:esp+0x8], 0x1
0x000053b9 mov dword [ss:esp+0x8], var_88, eax
0x000053c1 call imp_symbol_stub_objc_msgSend
0x000053c6 mov dword [ss:bp-0x68+var_88], eax
0x000053c7 call imp_symbol_stub_getuid
0x000053c9 test eax, eax
0x000053ce jne 0x54f6

0x000053d6 mov eax, dword [ds:esi-0x53a5+cls_NSBundle]
0x000053dc mov ecx, dword [ds:esi-0x53a5+objc_msg_mainBundle] ; @selector(mainBundle)
0x000053e2 mov dword [ss:esp+0x4], ecx
0x000053e6 mov dword [ss:esp], eax
0x000053e9 call imp_symbol_stub_objc_msgSend
0x000053ee mov ecx, dword [ds:esi-0x53a5+objc_msg_bundlePath] ; @selector(bundlePath)
0x000053f4 mov dword [ss:esp+0x4], ecx
0x000053fb call imp_symbol_stub_objc_msgSend
0x00005400 mov edx, dword [ds:esi-0x53a5+cfstring_library_Preferences] ; @selector(rangeOfString:)
0x00005406 lea edx, dword [ds:esi-0x53a5+objc_msg_rangeOfString_] ; @selector(rangeOfString:)
0x0000540c mov dword [ss:esp+0x8], edx
0x00005410 mov dword [ss:esp+0x4], ecx
0x00005414 mov dword [ss:esp], eax
0x00005417 call imp_symbol_stub_objc_msgSend
0x0000541c cmp eax, 0xffffffff
0x00005421 je 0x57e5

0x00005427 mov eax, dword [ds:esi-0x53a5+cls_NSBundle]
0x0000542d mov ecx, dword [ds:esi-0x53a5+objc_msg_mainBundle] ; @selector(mainBundle)
0x00005433 mov dword [ss:esp+0x4], ecx
0x00005437 mov dword [ss:esp], eax
0x0000543a call imp_symbol_stub_objc_msgSend
0x0000543f mov ecx, dword [ds:esi-0x53a5+objc_msg_bundlePath] ; @selector(bundlePath)
0x00005445 mov dword [ss:esp+0x4], ecx
0x00005449 mov dword [ss:esp], eax
0x0000544c call imp_symbol_stub_objc_msgSend
0x00005451 mov ecx, dword [ds:esi-0x53a5+objc_msg_rangeOfString_] ; @selector(rangeOfString:)
0x00005457 lea edx, dword [ds:esi-0x53a5+cfstring_Users_] ; @"/Users/"
0x0000545d mov dword [ss:esp+0x8], edx
0x00005461 mov dword [ss:esp+0x4], ecx
0x00005465 mov dword [ss:esp], eax
0x00005468 call imp_symbol_stub_objc_msgSend
0x0000546d cmp eax, 0xffffffff
0x00005472 je 0x57e5

Instruction Encoding
Format
Comment
Colors and Tags
Area RCSMUtils
Address RCSMUtils
Block
Procedure
Manage Tags
Is Referenced By
Address instruction
Remove Reference Add Reference
Have Reference To
Address instruction
Remove Reference Add Reference
Procedure
12 basic blocks
Basic Block
Input Regs: esp
Killed Regs: eax ecx esp esi eip
Predecessors

Address 0x5397, Segment __TEXT, -[RCSMUtils createLaunchAgentPlist:forBinary:] + 0, Section __text, file offset 0x4397

Code Signed Binaries

`codesign -dvvv <*.app or Mach-O>`

```
nibble:Documents sledwards$ codesign -dvvv OSX_Kitmos_A_39FAA22EB9D6B750EC345EFCB38189F5
Executable=/Users/sledwards/Documents/OSX_Kitmos_A_39FAA22EB9D6B750EC345EFCB38189F5
Identifier=com.util.file
Format=Mach-O thin (x86_64)
CodeDirectory v=20100 size=1362 flags=0x0(none) hashes=60+5 location=embedded
Hash type=sha1 size=20
CDHash=b0aa57a281c2d8cce6c9a09568c6e3fea52ff80e
Signature size=8514
Authority=Developer ID Application: Rajinder Kumar
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=Apr 8, 2013, 4:52:49 AM
Info.plist=not bound
Sealed Resources=none
Internal requirements count=1 size=208
```

KitM Sample = “Kumar In the Mac”

Dynamic Analysis

Virtualization

- XProtect
- Gatekeeper

Application Tracing

Analysis Tools (File, Process & Network)

- Dtrace
- Xcode Instruments
- fs_usage
- fseventer
- Activity Monitor
- procxp
- CocoaPacketAnalyzer
- Wireshark
- tcpdump
- lsock

Virtualization

Virtualization Tools

- VMware Fusion
- Parallels

Virtualization Issues

- Capable Versions - 10.7+ (10.6 Server)
- Xprotect & Gatekeeper

XProtect

Files	Weaknesses
<ul style="list-style-type: none">• /System/Library/CoreServices/CoreTypes.bundle/Contents/Resources• XProtect.meta.plist<ul style="list-style-type: none">• Last Update Date & Version (10.7 & 10.8)• Java Minimum Version & Blacklisted Plugins• XProtect.plist<ul style="list-style-type: none">• AV Signatures	<ul style="list-style-type: none">• Apple updates it...when they want to.• Very few signatures on blacklist.• No Heuristics• Only checks “quarantined” files<ul style="list-style-type: none">• com.apple.quarantine Extended Attribute• Mac Threats Only

```
nibble:Downloads sledwards$ ls -l xmount-0.5.0-x86_64.pkg
-rw-r--r--@1 sledwards staff 909305 Dec 24 07:40 xmount-0.5.0-x86_64.pkg
nibble:Downloads sledwards$ xattr -plx com.apple.quarantine xmount-0.5.0-x86_64.pkg
com.apple.quarantine:
00000000  30 30 32 31 3B 35 32 62 39 38 30 62 30 3B 47 6F  10021;52b980b0;GoI
00000010  6F 67 6C 65 5C 78 32 30 43 68 72 6F 6D 65 3B 36  logle.x20Chrome;6I
00000020  46 35 41 38 46 44 30 2D 34 33 31 34 2D 34 45 44  1F5A8FD0-4314-4ED1
00000030  33 2D 42 44 30 45 2D 45 32 33 44 35 37 33 33 38  13-BD0E-E23D573381
00000040  34 45 35                                         14E5I
```

XProtect Signature by Hash

SHA256: c6b0f2b35deaab5a85d039fa142a4ecef495391f15bf26e9b9cc338eb3f202d

File name: sig

Detection ratio: 8 / 49

Analysis date: 2014-02-13 18:04:47 UTC (3 weeks ago)

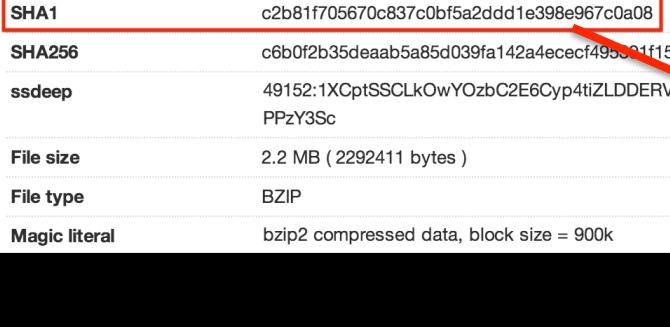
 1  0

[Analysis](#) [Additional information](#) [Comments 1](#) [Votes](#)

File identification

MD5	26d5f81486e4588990a126d51ad5140a
SHA1	c2b81f705670c837c0bf5a2ddd1e398e967c0a08
SHA256	c6b0f2b35deaab5a85d039fa142a4ecef495391f15bf26e9b9cc338eb3f202d
ssdeep	49152:1XCptSSCLkOwYOzbC2E6Cyp4tiZLDDERV6 PPzY3Sc
File size	2.2 MB (2292411 bytes)
File type	BZIP
Magic literal	bzip2 compressed data, block size = 900k

“Identity” Key = SHA1 Hash



Item 2	Dictionary (3 items)
Description	String OSX.CoinThief.B
LaunchServices	Dictionary (1 item)
LSItemContentType	String com.apple.application-bundle
Matches	Array (1 item)
Item 0	Dictionary (2 items)
MatchType	String MatchAny
Matches	Array (2 items)
Item 0	Dictionary (3 items)
Identity	Data <c2b81f70 5670c837 c0bf5a2d dd1e398e 967c0a08>
MatchFile	Dictionary (1 item)
NSURLNameKey	String .sig
MatchType	String Match
Item 1	Dictionary (3 items)
Identity	Data <02e24315 7dbc8803 a364e941 0a5c41b3 6de64c95>
MatchFile	Dictionary (1 item)
NSURLNameKey	String .sig
MatchType	String Match

XProtect

Signature by Launch Service & Pattern

▼ Item 20	Dictionary	(3 items)
Description	String	OSX.Mdropper.i
▼ LaunchServices	Dictionary	(1 item)
LSItemContentType	String	com.microsoft.word.doc
▼ Matches	Array	(1 item)
▼ Item 0	Dictionary	(3 items)
▼ MatchFile	Dictionary	(1 item)
NSURLTypelIdentifierKey	String	com.microsoft.word.doc
MatchType	String	Match
Pattern	String	2F746D702F6C61756E63682D68
 000 2F 74 6D 70 2F 6C 61 75 6E 63 68 2D 68 73 20 /tmp/launch-hs 015 2F 74 6D 70 2F 6C 61 75 6E 63 68 2D 68 73 65 /tmp/launch-hse 030 00 2F 74 6D 70 2F 00 23 21 2F 62 69 6E 2F 73 /tmp/\#!/bin/s 045 68 0A 2F 74 6D 70 2F 6C 61 75 6E 63 68 2D 68 h/tmp/launch-h 060 73 65 20 26 0A 6F 70 65 6E 20 2F 74 6D 70 2F se &open /tmp/ 075 66 69 6C 65 2E 64 6F 63 20 26 0A 0A 00 00 5F file.doc &FFNN 090 5F 50 41 47 45 5A 45 52 4F 00 00 5F 5F 6D 68 _PAGEZERO_NN_mh 105 5F 65 78 65 63 75 74 65 5F 68 65 61 64 65 72 _execute_header		

Disable XProtect

Delete/Edit XProtect Files ...or...

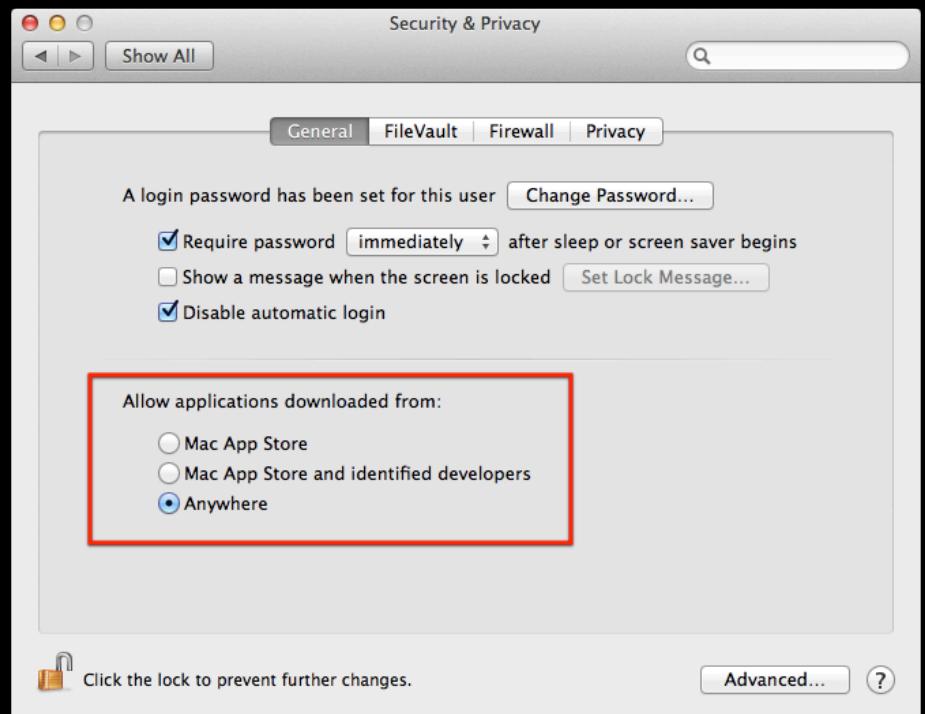
Remove com.apple.quarantine Extended Attribute

- `xattr -d com.apple.quarantine <filename>`



Gatekeeper

- Introduced in 10.7.5
- Anti-malware Feature
- Application Execution Restrictions
- Security Settings
 - Mac App Store
 - Users can only run apps from the store.
 - Mac App Store & Identified Developers
 - Default Setting (10.8+)
 - Users can only run software signed using Apple Developer ID
 - Anywhere
 - Default Setting (10.7.5)
 - Users can run anything from anywhere



Disable Gatekeeper

- Permanent: Change to “Allow Applications Downloaded From:” to “Anywhere” ...or...
- Case-by-case basis: Control+Click Application



Application Tracing

“Trace” program execution, file system events, network communications for use in troubleshooting.

Low-level logging

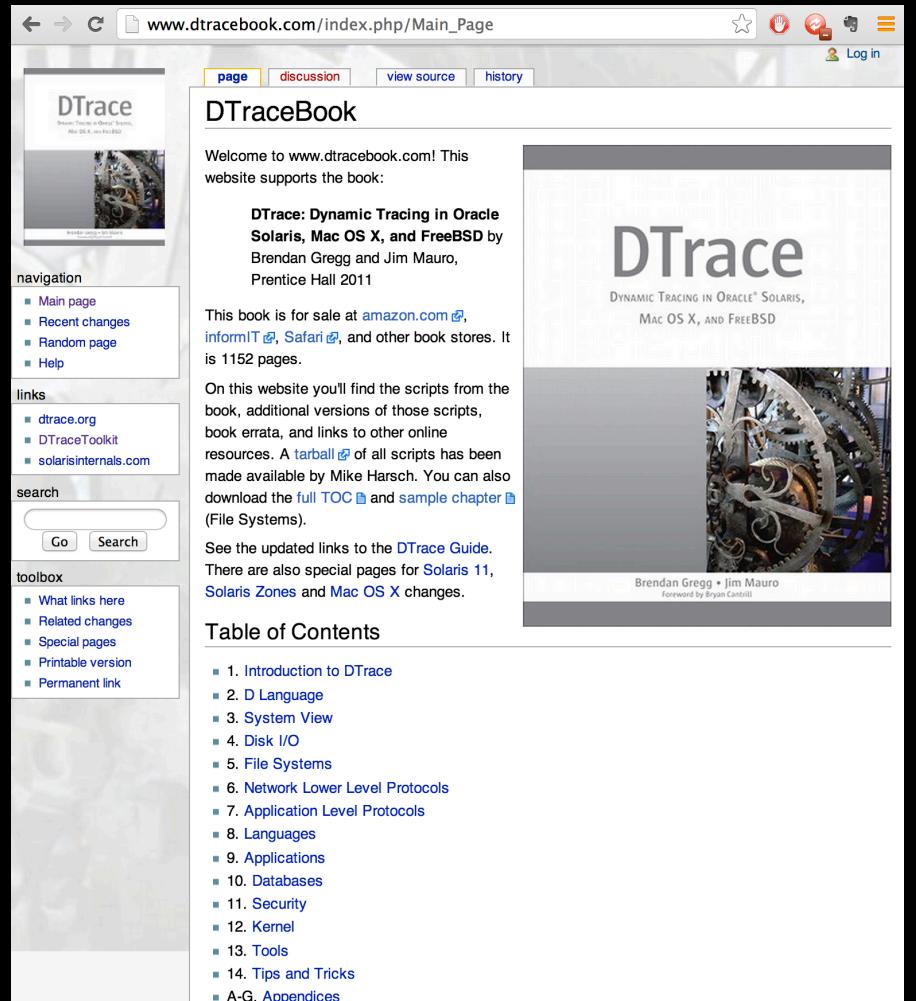
Verbose

Very useful for reverse engineering!

Tools: Dtrace, fs_usage, Xcode Instruments

Dtrace

- Troubleshooting Utility
- Designed by Sun Microsystems (Originally for Solaris)
- Added to OS X in 10.5
- Captures data from:
 - CPU
 - Memory
 - Network
 - File System
 - Processes
- Uses D Language (awk-ish)
- dtracebook.com
- man –k dtrace



Dtrace Example

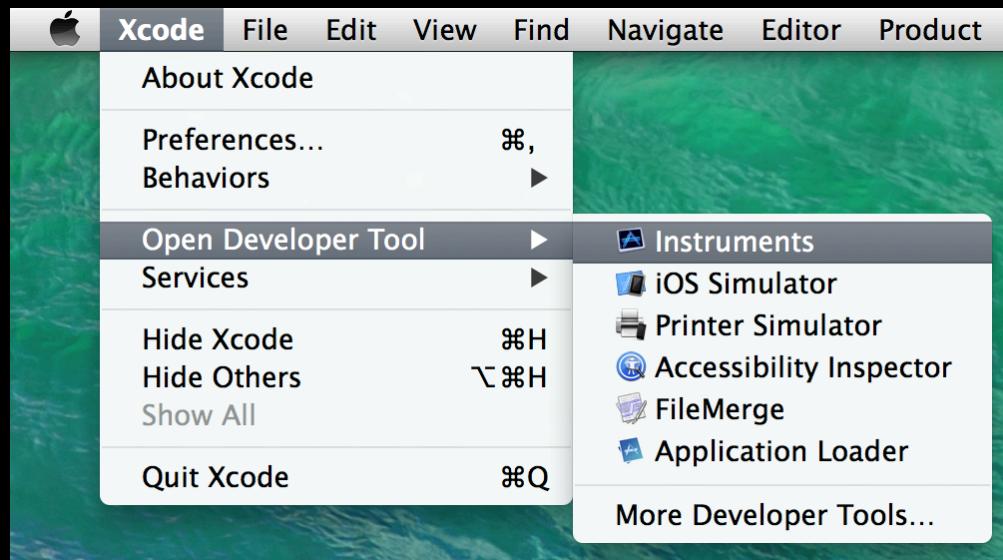
- Files Opened by Process
- Example from dtracebook.com (filebyproc.d)

```
dtrace -n 'syscall::open*:entry { printf("%s %s", execname, copyinstr(arg0)); }'
```

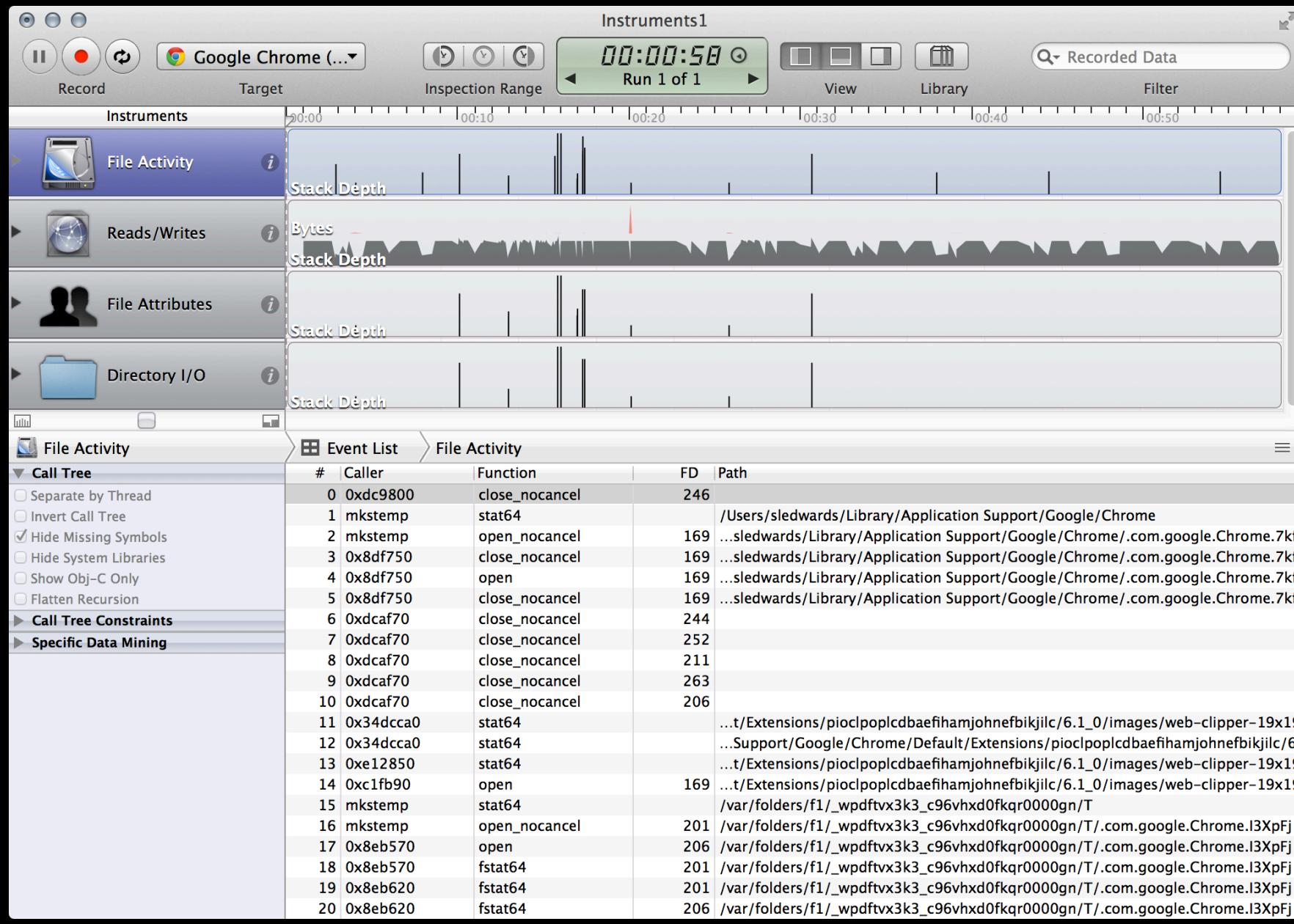
```
nibble:/ sledwards$ sudo dtrace -n 'syscall::open*:entry { printf("%s %s", execname, copyinstr(arg0)); }'
dtrace: description 'syscall::open*:entry' matched 4 probes
CPU      ID          FUNCTION:NAME
 0    937          open_nocancel:entry kextd //private/var/run/installd.commit.pid
 1   151          open:entry mds_stores .
 1   151          open:entry mds_stores .
 0   937          open_nocancel:entry Google Chrome /Users/sledwards/Library/Application Support/Google/Chrome/Default/.com.google.Chrome.WWGUaH
 0   151          open:entry Google Chrome /Users/sledwards/Library/Application Support/Google/Chrome/Default/.com.google.Chrome.WWGUaH
 1   151          open:entry mds /Users/sledwards/Library/Application Support/Google/Chrome/Default/TransportSecurity
 3   151          open:entry mds_stores .
 0   937          open_nocancel:entry Mail /etc/hosts
 2   937          open_nocancel:entry Mail /etc/hosts
 0   151          open:entry mdworker /Users/sledwards/Library/Application Support/Google/Chrome/Default/TransportSecurity
```

Xcode Instruments

- Installed with Xcode (Xcode Tools)
- Apple Developer: Instruments User Guide
- GUI Tracing Application



Xcode Instruments



File Analysis

Dtrace

- filebyproc.d
- opensnoop
- losnoop
- creatbyproc.d

fs_usage

fseventer

File Analysis – Files Opened By Process

Dtrace - filebyproc.d

- CPU – CPU that received event
- ID – Dtrace Probe ID
- FUNCTION:NAME – Dtrace Probe Name
- Remaining – Process/Pathname

```
Cliffs-Mac:~ cliffstoll$ sudo filebyproc.d
Password:
dtrace: script '/usr/bin/filebyproc.d' matched 4 probes
CPU      ID          FUNCTION:NAME
 1        151          open:entry touch /dev/dtracehelper
 1        151          open:entry touch test.txt
 1        151          open:entry Dock /Users/cliffstoll/Applications
 1        151          open:entry Dock /Users/cliffstoll
 1        151          open:entry Dock /Users/cliffstoll
 1        151          open:entry Finder /Users/cliffstoll
 0        151          open:entry mdworker /dev/dtracehelper
 0        151          open:entry mdworker /dev/autofs_nowait
 0        151          open:entry mdworker /Users/cliffstoll/.CFUserTextEncoding
 0        151          open:entry mdworker /dev/autofs_nowait
 0        151          open:entry mdworker /Users/cliffstoll/.CFUserTextEncoding
 0        937          open_nocancel:entry mdworker /etc/localtime
 0        937          open_nocancel:entry mdworker /System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/
 0        937          open_nocancel:entry mdworker /System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/
 0        151          open:entry mdworker /System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/
 0        151          open:entry mdworker /Library/Preferences/SystemConfiguration/com.apple.Boot.plist
 0        151          open:entry cfprefsd /Users/cliffstoll/Library/Preferences/ByHost/com.apple.SpotlightServer.000c29f9c093.plist
 0        151          open:entry cfprefsd /Users/cliffstoll/Library/Preferences/ByHost/com.apple.SpotlightServer.000c29f9c093.plist
```

File Analysis – Files Opened

Dtrace - opensnoop

- UID – User ID
- PID – Process ID
- COMM – Process Command Name
- FD – File Descriptor
- PATH – File Path

```
Cliffs-Mac:~ cliffstoll$ sudo opensnoop
UID      PID  COMM           FD  PATH
501      663  bash            3  .
501     1209  open            4  /System/Library/CoreServices/SystemVersion.plist
501     1209  open            4  /usr/bin
501     1209  open            4  /usr/bin
501     1209  open            4  /usr/bin/open
501     1209  open            4  ./vol/16777218/78/open/..namedfork/rsrc
501     1209  open            3  /dev/dtracehelper
501     1209  open            3  .
501     1209  open            4  /Library/Application Support/CrashReporter/SubmitDiagInfo.domains
501     1209  open            4  /dev/random
501     1209  open            4  /dev/random
501     1209  open            4  /System/Library/CoreServices/CoreTypes.bundle/Contents/Library/AppExceptions.bundle/Exceptions.plist
501     1209  open            4  /private/var/db/launchd.db/com.apple.launchd.peruser.501/overrides.plist
501     1209  open            5  /private/var/db/launchd.db/com.apple.launchd.peruser.501/overrides.plist
501     1209  open            4  /System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/Exceptions.plist
 0     13  taskgated         3  /Applications/TextEdit.app
 0     13  taskgated         3  /Applications/TextEdit.app/Contents
 0     13  taskgated         3  /Applications/TextEdit.app/Contents/Info.plist
 0     13  taskgated         3  /Applications/TextEdit.app/Contents/MacOS/TextEdit
 0     13  taskgated         5  /Applications/TextEdit.app/Contents/MacOS/TextEdit
 0     13  taskgated         3  /Applications/TextEdit.app/Contents/Info.plist
501    181  Dock             31 /Applications/TextEdit.app
```

File Analysis – Files Opened

Dtrace – opensnoop -a

- -a = All Data
 - TIME – Timestamp (Relative Microsecond Counter)
 - STRTIME – String Timestamp (Local System Time)
 - UID – User ID
 - PID – Process ID
 - FD – File Descriptor
 - ERR – Errno Value (See errno.h)
 - PATH – File Path
 - ARGS – Argument List

```
Cliffs-Mac:~ cliffstoll$ sudo opensnoop -a
TIME      STRTIME          UID    PID   FD  ERR  PATH                ARGS
22505562387  2014 Mar 22 13:44:34  501   1410   4   0  /dev/dtracehelper  cat\0
22505597664  2014 Mar 22 13:44:34  501   1411   4   0  /dev/dtracehelper  groff\0
22505629896  2014 Mar 22 13:44:34  501   1413   4   0  /dev/dtracehelper  less\0
22505549462  2014 Mar 22 13:44:33  501   1405   3   0  /usr/lib/libxcselect.dylib man\0
22505549975  2014 Mar 22 13:44:33  501   1405   3   0  /dev/dtracehelper  man\0
22505552023  2014 Mar 22 13:44:33  501   1405   3   0  /usr/share/locale/en_US.UTF-8/LC_CTYPE man\0
22505552291  2014 Mar 22 13:44:33  501   1405   3   0  /usr/share/locale/en_US.UTF-8/LC_MESSAGES/LC_MESSAGES man\0
22505552381  2014 Mar 22 13:44:33  501   1405   3   0  /private/etc/man.conf man\0
22505552985  2014 Mar 22 13:44:34  501   1405  -1   2  /usr/share/xcode-select/xcode_dir_path man\0
22505553120  2014 Mar 22 13:44:34  501   1405  -1   2  /usr/share/man/html1/ man\0
22505553195  2014 Mar 22 13:44:34  501   1405   4   0  /usr/share/man/man1/ man\0
22505554577  2014 Mar 22 13:44:34  501   1405   4   0  /usr/share/man/man1/opensnoop.1m man\0
```

File Analysis - Files Read/Written by Process

Dtrace - iosnoop

- UID – User ID
- PID – Process ID
- D – Direction (Read/Write)
- BLOCK – File System Block for Operation
- SIZE – Operation Size
- COMM – Process Command Name
- PATHNAME – File Path

```
Cliffs-Mac:~ cliffstoll$ sudo iosnoop
UID  PID D    BLOCK  SIZE      COMM PATHNAME
 0    1 W  22281784  4096  launchd ??/asl/2014.03.21.G80.asl
 0    1 W  22281768  4096  launchd ??/asl/2014.03.21.U0.G80.asl
 0    1 W  16515088  4096  launchd ??/asl/StoreData
 0    1 W    35040   8192  launchd ??/<unknown (NULL v_parent>/<unknown (NULL v_name)>
 0    1 W    36256   8192  launchd ??/<unknown (NULL v_parent>/<unknown (NULL v_name)>
 0    1 W    36720   8192  launchd ??/<unknown (NULL v_parent>/<unknown (NULL v_name)>
```

File Analysis – Files Created by Process

Dtrace – creatbyproc.d

- CPU – CPU ID
- ID – Process ID
- FUNCTION:NAME – Dtrace Probe Name
- Remaining – Command/Application & File Path

```
nibble:Documents sledwards$ sudo creatbyproc.d
dtrace: script '/usr/bin/creatbyproc.d' matched 1 probe
CPU      ID          FUNCTION:NAME
 0        151          open:entry Google Chrome /Users/sledwards/Library/Application Support/Google/Chrome/Default/Local Storage
 1        151          open:entry Google Chrome /Users/sledwards/Library/Application Support/Google/Chrome/Default/Local Storage/http_www.rdio.com_0.localstorage-journal
 1        151          open:entry Google Chrome /Users/sledwards/Library/Application Support/Google/Chrome/Default/Local Storage/http_www.rdio.com_0.localstorage-journal
 0        151          open:entry Google Chrome /Users/sledwards/Library/Application Support/Google/Chrome/Default/Local Storage/http_www.rdio.com_0.localstorage-journal
 0        151          open:entry Google Chrome /Users/sledwards/Library/Application Support/Google/Chrome/Default
 0        151          open:entry man /dev/dtracehelper
 0        151          open:entry tbl /dev/dtracehelper
 0        151          open:entry cat /dev/dtracehelper
 0        151          open:entry Google Chrome /var/folders/f1/_wpdftvx3k3_c96vhxd0fkqr0000gn/T/.com.google.Chrome.LcnDaW
 1        151          open:entry sh /dev/dtracehelper
 1        151          open:entry sh /dev/tty
 1        151          open:entry cat /usr/share/man/man1/creatbyproc.d.1m
 1        151          open:entry troff /dev/dtracehelper
 1        151          open:entry less /dev/tty
 1        151          open:entry grotty /dev/dtracehelper
 1        151          open:entry Google Chrome /var/folders/f1/_wpdftvx3k3_c96vhxd0fkqr0000gn/T/.com.google.Chrome.hEiMHy
 2        151          open:entry Google Chrome /Users/sledwards/Library/Application Support/Google/Chrome/Default/Cookies-journal
```

File Analysis

fs_usage

Very Verbose

Native to OS X

`fs_usage -w -f <filter>`

Filters:

- `pathname` – File Path Events
- `filesystem` – File System Events
- `exec` – New and Spawning Process Events
- `diskio` – Disk Input/Output Events
- `cachehit` – Cache Hits
- `network` – Network Events

File Analysis – Pathname Events

`fs_usage -f pathname`

- Columns
 - Timestamp
 - Call
 - File Descriptor (F=##)
 - [ERRNO] – Error Code
 - File Path
 - Time Interval (W = Wait Time)
 - Process Name
- Calls of Interest
 - `getattrlist` – Get file system attributes
 - `getxattr` – Get extended attribute
 - `setattrlist` – Set file system attribute
 - `stat64, lstat64` – Get file status
 - `open` – Open/Create File
 - `mkdir, rmdir` – Make/Remove a directory

File Analysis - Pathname Events

```
fs_usage -w -f pathname
```

```
08:05:21.631155  getattrlist /Applications/  
Messages.app      0.000011    Dock.513976
```

```
08:05:21.006391  open F=135 (R____) /Users/  
slewards/Library/Application Support/  
Google/Chrome/Default/Local Storage  
0.000022    Google Chrome.7460
```

File Analysis – Disk I/O Events

`fs_usage -f diskio`

- Columns
 - Timestamp
 - Call
 - Disk Block (D=##)
 - Byte Count (B=##)
 - Disk
 - File Path
 - Time Interval (W = Wait Time)
 - Process Name
- Calls of Interest
 - WrMeta – Write Metadata
 - WrData – Write Data
 - RdData – Read Data
 - PgIn – Page In
 - PgOut – Page Out

File Analysis – Disk I/O Events

`fs_usage -w -f diskio`

```
08:15:54.847585      WrMeta[AT3]      D=0x01471e78
B=0x2000  /dev/disk1  /Users/sledwards/Library/
Mail/V2/IMAP-sledwards@imap.gmail.com/[Gmail].mbox/
Trash.mbox/65AE84E4-7606-4E45-BC3F-E5E3398FDCE0/
Data/0/7/Messages  0.000262 W launchd.207
```

```
08:15:55.005800      WrData[AT1]      D=0x125f2870
B=0x1000  /dev/disk1  /Users/sledwards/Library/
Application Support/Google/Chrome/Default/Local
Storage/http_www.rdio.com_0.localstorage-journal
0.000169 W Google Chrome.7458
```

File Analysis fseventer

fernlightning.com

GUI Application

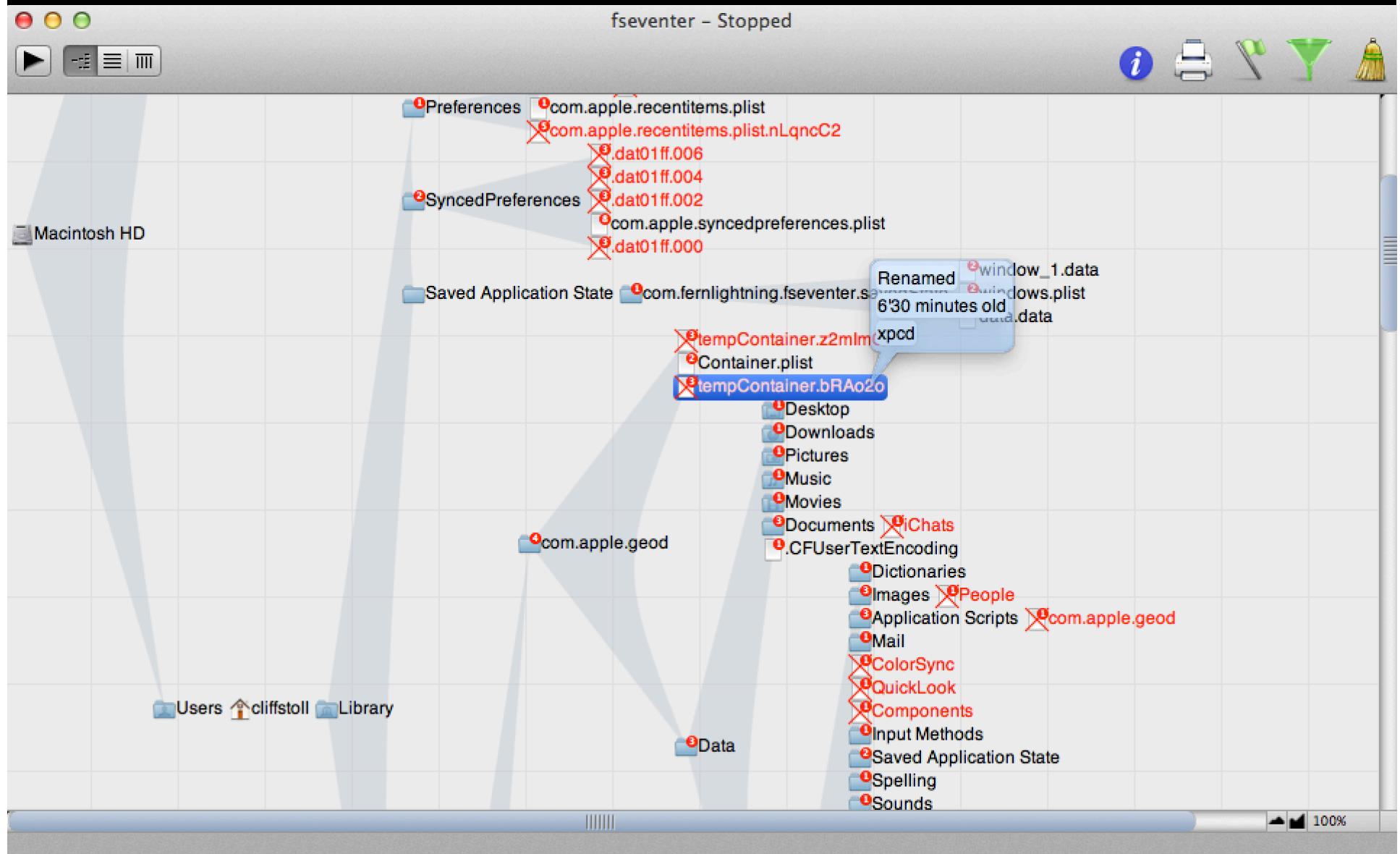
Different Views:

- Graphical “Tree” View
- Table View

Filtering

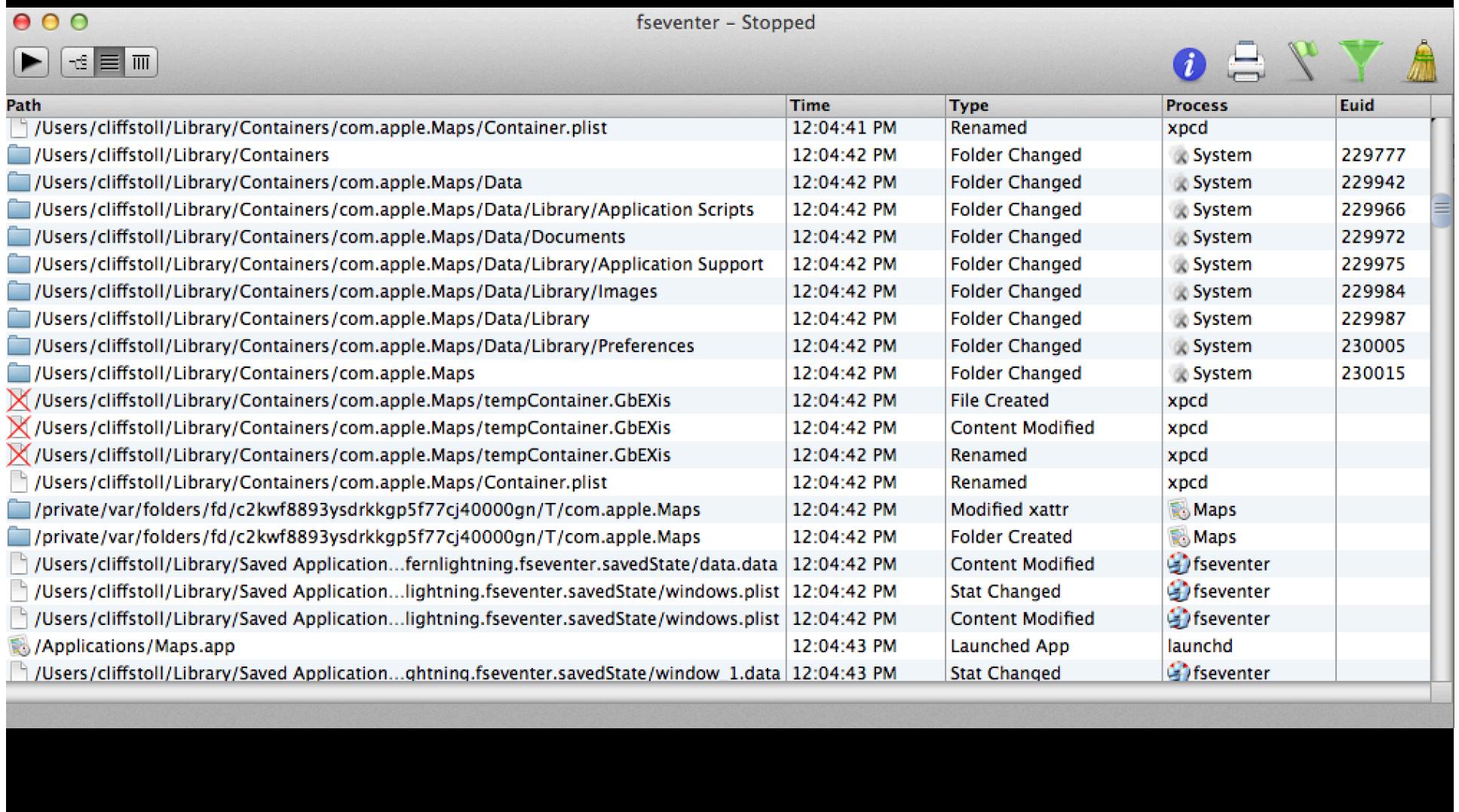
Save Output to Text File

File Analysis - fseventer



File Analysis - fseventer

fseventer – Stopped



The screenshot shows the fseventer application window titled "fseventer – Stopped". The window contains a table of file system event logs. The columns are: Path, Time, Type, Process, and Euid. The table lists numerous events, primarily related to the com.appleMaps container and its subfolders, such as Container.plist, Data, Library, and Preferences. Other events include file creation, modification, and renaming by processes like xpcd, System, Maps, and fseventer, with Euids ranging from 229777 to 230005. A few events are marked with a red X icon.

Path	Time	Type	Process	Euid
/Users/cliffstoll/Library/Containers/com.appleMaps/Container.plist	12:04:41 PM	Renamed	xpcd	
/Users/cliffstoll/Library/Containers	12:04:42 PM	Folder Changed	System	229777
/Users/cliffstoll/Library/Containers/com.appleMaps/Data	12:04:42 PM	Folder Changed	System	229942
/Users/cliffstoll/Library/Containers/com.appleMaps/Data/Library/Application Scripts	12:04:42 PM	Folder Changed	System	229966
/Users/cliffstoll/Library/Containers/com.appleMaps/Data/Documents	12:04:42 PM	Folder Changed	System	229972
/Users/cliffstoll/Library/Containers/com.appleMaps/Data/Library/Application Support	12:04:42 PM	Folder Changed	System	229975
/Users/cliffstoll/Library/Containers/com.appleMaps/Data/Library/Images	12:04:42 PM	Folder Changed	System	229984
/Users/cliffstoll/Library/Containers/com.appleMaps/Data/Library	12:04:42 PM	Folder Changed	System	229987
/Users/cliffstoll/Library/Containers/com.appleMaps/Data/Library/Preferences	12:04:42 PM	Folder Changed	System	230005
/Users/cliffstoll/Library/Containers/com.appleMaps	12:04:42 PM	Folder Changed	System	230015
✗ /Users/cliffstoll/Library/Containers/com.appleMaps/tempContainer.GbEXis	12:04:42 PM	File Created	xpcd	
✗ /Users/cliffstoll/Library/Containers/com.appleMaps/tempContainer.GbEXis	12:04:42 PM	Content Modified	xpcd	
✗ /Users/cliffstoll/Library/Containers/com.appleMaps/tempContainer.GbEXis	12:04:42 PM	Renamed	xpcd	
✗ /Users/cliffstoll/Library/Containers/com.appleMaps/Container.plist	12:04:42 PM	Renamed	xpcd	
/private/var/folders/fd/c2kwf8893ysdrkkgp5f77cj40000gn/T/com.appleMaps	12:04:42 PM	Modified xattr	Maps	
/private/var/folders/fd/c2kwf8893ysdrkkgp5f77cj40000gn/T/com.appleMaps	12:04:42 PM	Folder Created	Maps	
/Users/cliffstoll/Library/Saved Application...fernlightning.fseventer.savedState/data.data	12:04:42 PM	Content Modified	fseventer	
/Users/cliffstoll/Library/Saved Application...lightning.fseventer.savedState/windows.plist	12:04:42 PM	Stat Changed	fseventer	
/Users/cliffstoll/Library/Saved Application...lightning.fseventer.savedState/windows.plist	12:04:42 PM	Content Modified	fseventer	
✗ /Applications/Maps.app	12:04:43 PM	Launched App	launchd	
/Users/cliffstoll/Library/Saved Application...qhtning.fseventer.savedState/window_1.data	12:04:43 PM	Stat Changed	fseventer	

File Analysis - fseventer

fseventer - Stopped

Any of the following are true

path includes

Path	Time	Type	Process	E...
/Users/cliffstoll/Library/Containers/com.apple.Preferences/com.apple.HIToolbox.plist	12:04:43 PM	File Created	xpcd	
/Users/cliffstoll/Library/Containers/com.apple.geod/Container.plist	12:04:43 PM	Renamed	xpcd	
✗ /Users/cliffstoll/Library/Containers/com.apple.Library/Preferences/com.apple.GEO.plist	12:04:43 PM	File Created	xpcd	
✗ /Users/cliffstoll/Library/Containers/com.apple.ByHost/com.apple.GEO.000c29f9c093.plist	12:04:43 PM	File Created	xpcd	
/Users/cliffstoll/Library/Containers/com.apple.Library/Preferences/com.apple.Maps.plist	12:04:44 PM	File Created	cfprefsd	
/Users/cliffstoll/Library/Containers/com.apple.Library/Preferences/com.apple.Maps.plist	12:04:44 PM	Chown	cfprefsd	
✗ /Users/cliffstoll/Library/Containers/com.apple.Preferences/com.apple.Maps.plist.NzSmbtL	12:04:44 PM	File Created	cfprefsd	
✗ /Users/cliffstoll/Library/Containers/com.apple.Preferences/com.apple.Maps.plist.NzSmbtL	12:04:44 PM	Chown	cfprefsd	
✗ /Users/cliffstoll/Library/Containers/com.apple.Preferences/com.apple.Maps.plist.NzSmbtL	12:04:44 PM	Chown	cfprefsd	
✗ /Users/cliffstoll/Library/Containers/com.apple.Preferences/com.apple.Maps.plist.NzSmbtL	12:04:44 PM	Content Modified	cfprefsd	
✗ /Users/cliffstoll/Library/Containers/com.apple.Preferences/com.apple.Maps.plist.NzSmbtL	12:04:44 PM	Renamed	cfprefsd	
/Users/cliffstoll/Library/Containers/com.apple.Library/Preferences/com.apple.Maps.plist	12:04:44 PM	Renamed	cfprefsd	
/Users/cliffstoll/Library/Containers/com.apple.geod/Container.plist	12:04:45 PM	Renamed	xpcd	
/Users/cliffstoll/Library/SyncedPreferences/com.apple.syncedpreferences.plist	12:04:47 PM	Renamed	511 (exited?)	
/Users/cliffstoll/Library/SyncedPreferences/com.apple.syncedpreferences.plist	12:04:47 PM	Chown	511 (exited?)	
✗ /Users/cliffstoll/Library/Preferences/com.apple.recentitems.plist.nLqncC2	12:04:47 PM	File Created	cfprefsd	
✗ /Users/cliffstoll/Library/Preferences/com.apple.recentitems.plist.nLqncC2	12:04:47 PM	Chown	cfprefsd	
✗ /Users/cliffstoll/Library/Preferences/com.apple.recentitems.plist.nLqncC2	12:04:47 PM	Chown	cfprefsd	
✗ /Users/cliffstoll/Library/Preferences/com.apple.recentitems.plist.nLqncC2	12:04:47 PM	Content Modified	cfprefsd	
✗ /Users/cliffstoll/Library/Preferences/com.apple.recentitems.plist.nLqncC2	12:04:47 PM	Renamed	cfprefsd	
/Users/cliffstoll/Library/Preferences/com.apple.recentitems.plist	12:04:47 PM	Renamed	cfprefsd	
/Users/cliffstoll/Library/SyncedPreferences/com.apple.syncedpreferences.plist	12:04:47 PM	Renamed	511 (exited?)	
/Users/cliffstoll/Library/SyncedPreferences/com.apple.syncedpreferences.plist	12:04:47 PM	Chown	511 (exited?)	

Process Analysis

Dtrace

- execsnoop
- newproc.d

fs_usage

procxp

Activity Monitor

Process Analysis – Snoop New Processes

Dtrace – newproc.d

- Timestamp
- Process ID
- Parent Process ID
- Architecture = 32b/64b
- Command & Arguments / Application

```
nibble:Documents sledwards$ sudo newproc.d
2014 Mar 25 07:55:13 2137 <151> 32b  /Applications/Microsoft Office 2011/Office/Office365Service.app/Contents/MacOS/Office365Service
2014 Mar 25 07:55:17 2138 <151> 64b  /System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/A/Support/md
worker -s mdworker -c MDSImporterWorker -m <...>
2014 Mar 25 07:55:50 2142 <151> 64b  /Applications/Notes.app/Contents/MacOS/Notes
2014 Mar 25 07:55:50 2143 <37> 64b  /System/Library/Frameworks/CoreServices.framework/Frameworks/OSServices.framework/Versions/A/Support/S
FLIconTool com.apple.recentitems RecentApplications
2014 Mar 25 07:55:50 2144 <151> 64b  /System/Library/Frameworks/OpenGL.framework/Versions/A/Libraries/CVMCompiler 3
2014 Mar 25 07:55:51 2145 <1> 64b  xpcproxy /System/Library/Frameworks/Security.framework/Versions/A/XPCServices/XPCKeychainSandboxCheck.x
pc/Contents/MacOS/XPCKeychainSandb (...)

2014 Mar 25 07:55:51 2146 <1> 64b  com.apple.iCloudHelper
2014 Mar 25 07:55:51 2146 <1> 64b  xpcproxy /System/Library/PrivateFrameworks/AOSKit.framework/Versions/A/XPCServices/com.apple.iCloudHelp
er.xpc/Contents/MacOS/com.apple.iC (...)

2014 Mar 25 07:55:51 2145 <1> 64b  com.apple.security.XPCKeychainSandboxCheck
2014 Mar 25 07:56:23 2157 <2154> 64b  troff -Wall -mtty-char -mandoc -c -Tascii
2014 Mar 25 07:56:23 2148 <420> 64b  man ifconfig
2014 Mar 25 07:56:43 2161 <37> 64b  /System/Library/Frameworks/CoreServices.framework/Frameworks/OSServices.framework/Versions/A/Support/S
FLIconTool com.apple.recentitems RecentApplications
2014 Mar 25 07:56:43 2159 <420> 64b  open -a TextWrangler
2014 Mar 25 07:56:43 2160 <151> 32b  /Applications/TextWrangler.app/Contents/MacOS/TextWrangler
```



Process Analysis - New Processes

Dtrace – execsnoop

- TIME – Relative Timestamp
- STRTIME –Timestamp (String)
- PROJ – Project ID
- UID – User ID
- PID – Process ID
- PPID – Parent Process ID
- ARGS – Program/Application

nibble:Documents sledwards\$ sudo execsnoop -a	TIME	STRTIME	PROJ	UID	PID	PPID	ARGS
	1580104042	2014 Mar 25 08:06:08	0	501	2249	420	cat
	1581769527	2014 Mar 25 08:06:10	0	501	2250	420	xxd
	1584611113	2014 Mar 25 08:06:12	0	501	2252	151	TextWrangler
	1584576058	2014 Mar 25 08:06:12	0	501	2251	416	open
	1584848351	2014 Mar 25 08:06:13	0	501	2253	37	SFLIconTool
	1593140847	2014 Mar 25 08:06:21	0	501	2254	151	cookied
	1595461967	2014 Mar 25 08:06:23	0	0	2256	2255	find
	1595448068	2014 Mar 25 08:06:23	0	501	2255	416	sudo
	1611400046	2014 Mar 25 08:06:39	0	501	2257	412	man
	1611442879	2014 Mar 25 08:06:39	0	501	2257	412	man
	1611462816	2014 Mar 25 08:06:39	0	501	2267	2263	grotty
	1611462074	2014 Mar 25 08:06:39	0	501	2266	2263	troff
	1611457535	2014 Mar 25 08:06:39	0	501	2265	2264	less
	1611450569	2014 Mar 25 08:06:39	0	501	2262	2260	cat
	1611451542	2014 Mar 25 08:06:39	0	501	2263	2259	groff
	1611452923	2014 Mar 25 08:06:39	0	501	2261	2259	tbl

Process Analysis – New Processes

`fs_usage -f exec`

- Columns
 - Timestamp
 - Call
 - Pathname
 - Time Interval (W = Wait Time)
 - Process Name
- Calls of Interest:
 - `execve` – New Process
 - `posix_spawn` – Spawned Process

Process Analysis - New Processes

fs_usage -w -f exec

```
20:53:48.539284  posix_spawn /Applications/0xED.app/  
Contents/MacOS/0xED 0.000270 launchd.777421
```

```
20:54:04.592903  execve /usr/bin/man 0.000175 bash.777569
```

```
20:54:04.600445  posix_spawn /bin/sh 0.000165 man.777569
```

```
20:54:04.603848  execve /usr/bin/tbl 0.000224 sh.777573
```

```
20:54:04.604053  execve /usr/bin/groff 0.000173 sh.777574
```

Process Analysis – Real-time Processes

procxp

CLI Process Explorer (for Mac)

Scroll/sort processes via keys

Click Enter for more info on process

www.newosxbook.com/index.php?page=downloads

```

08:19:51 Up 53:56.00 Load Average: 1.29 1.34 1.29
CPU: 2/2 active <Unable to get processor information>
RAM: 900M Free + 1146M Used (Active: 673M + Inactive: 268M + Wired: 204M Comp: 0M) 1M purgeable
      Memstatus: 89 Comp: 0M + Decom: 0M File: 1255M Anon: 475M Throttled: 0M
Swap: 1024M Free + 0M Used (enc)
Pkts: TX: 614/53K (0 bytes/sec) RX: 995/150K (0 bytes/sec)
Unable to get Power Source information

```

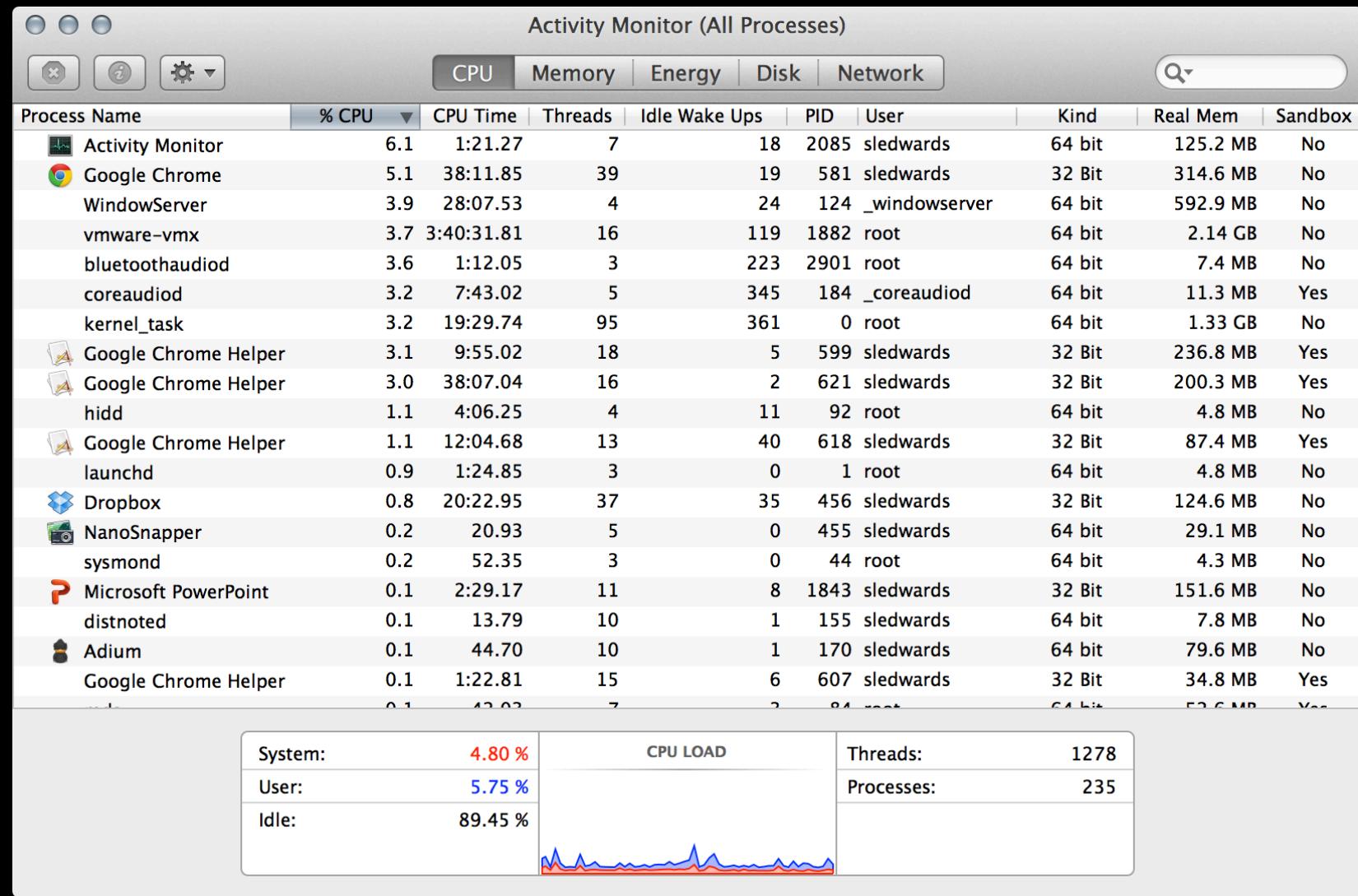
PID	PPID	UID	TTY	COMMAND	PRI	#TH	VSS	RSS	S	STIME	TIME	CPU	FDS	DISK
439	243	501	268435	procexp.univers	31	2/1	2398M	14M	R	08:19:33	00.57	8	3	8K
438	1	501	none	QuickLookSatell	4	5	3493M	18M	S	08:19:16	00.47	0	10	155K
437	166	501	none	quicklookd	4	4	2936M	9784K	S	08:19:16	00.21	0	19	782K
436	166	501	none	pbs	4	2	2390M	2564K	S	08:19:13	00.03	0	5	36K
434	166	501	none	cookied	31	2	2388M	1844K	S	08:19:09	00.01	0	5	0K
433	1	501	none	IMRemoteURLConn	4	3	2412M	5500K	S	08:19:08	00.03	0	11	32K
427	166	501	none	spindump_agent	4	2	2390M	2200K	S	07:28:16	00.02	0	5	8K
366	166	501	none	mdflagwriter	31	2	2389M	720K	S	24/02 22:28	00.00	0	5	16K
290	166	501	none	EscrowSecurityA	46	3	2440M	11M	S	24/02 21:53	00.08	0	5	73K
278	166	501	none	storeagent	31	3	2416M	9164K	S	24/02 21:47	00.88	0	11	490K
271	166	501	none	CloudKeychainPr	31	2	2388M	1924K	S	24/02 21:47	00.01	0	5	0K
267	166	501	none	vmware-tools-da	31	4	642M	6108K	S	24/02 21:47	06.20	0	8	8K
264	166	501	none	AppleIDAuthAgen	4	3	2390M	1936K	S	24/02 21:47	00.02	0	5	0K
262	166	501	none	helpd	31	2	2411M	4532K	S	24/02 21:47	00.02	0	5	0K
258	166	501	none	SocialPushAgent	31	2	2390M	5272K	S	24/02 21:47	00.02	0	5	16K
257	166	501	none	WiFiKeychainPro	4	2	2411M	2484K	S	24/02 21:47	00.04	0	5	24K
252	251	501	268435	bash	31	1	2385M	1204K	S	24/02 21:47	00.01	0	3	0K
248	247	501	268435	bash	31	1	2385M	1188K	S	24/02 21:47	00.01	0	3	0K
243	242	501	268435	bash	31	1	2385M	1204K	S	24/02 21:47	00.02	0	3	24K
238	1	501	none	com.apple.dock.	46	3	2437M	16M	S	24/02 21:47	00.20	0	5	416K
236	1	501	none	com.apple.WebKi	46	3	3455M	12M	S	24/02 21:47	00.15	0	10	121K
235	1	501	none	com.apple.webKi	46	2	3438M	10096	S	24/02 21:47	00.06	0	10	92K
232	166	501	none	accountsd	4	2	2416M	5704K	S	24/02 21:47	00.10	0	9	25K

2Process: 243 Name: bash Parent: 242 Status: runnable
 2Flags: 64-bit, called exec, has control tty, has controlling terminal, may suspend
 2UID: 501 RUID: 501 SVUID: 501
 2GID: 20 RGID: 20 SVGID: 20
 2Virtual size: 2385M (2501206016) Resident size: 1244K (1273856)
 2Time: 00.03 = 00.01 (User) + 00.02 (System)
 2Syscalls: 1749 Mach Traps: 118
 2Disk I/O: Read 8K Written: 16K
 2#Threads: 1 (Process has no workqueues)
 2(library and shared libraries)
 2(press T to display Thread Information)
 2Process Hierarchy:
 2 243 bash
 2 L 443 procexp.univers
 23 File descriptors: 3 files (press F for detailed information)

178	166	501	none	Terminal	47	7	2516M	40M	S	24/02 21:47	02.88	56	13	326K
176	166	501	none	tccd	4	2	2413M	3188K	S	24/02 21:47	00.06	0	6	8K
173	166	501	none	cfprefsd	4	4	2390M	1624K	S	24/02 21:47	00.32	0	5	967K
170	166	501	none	distnoted	31	2	2411M	2524K	S	24/02 21:47	00.17	0	5	0K

Process Analysis – Real-time Processes

Activity Monitor



Network Analysis

CocoaPacketAnalyzer

Wireshark

Tcpdump

Activity Monitor

lsock

Network Analysis - CocoaPacketAnalyzer

www.tastycocoabytes.com/cpa/

Untitled_3262014-083017.pcap

Select a filter predicate

Filter

ID	Source	Destination	Captured Length	Packet Length	Protocol	Date Received	Time Delta	Information
1	172.16.148.135	172.16.148.1	76	76	UDP	2014-03-26 08:30:20.006	0.000000	60895 > DOMAIN
2	172.16.148.1	172.16.148.135	70	70	ICMP	2014-03-26 08:30:20.007	0.001410	Destination unreachable...
3	172.16.148.135	172.16.148.1	98	98	ICMP	2014-03-26 08:30:20.639	0.633687	Echo request (Code=0)
4	172.16.148.1	172.16.148.135	98	98	ICMP	2014-03-26 08:30:20.640	0.633816	Echo reply (Code=0)
5	172.16.148.135	172.16.148.1	76	76	UDP	2014-03-26 08:30:21.041	1.035184	60895 > DOMAIN
6	172.16.148.1	172.16.148.135	70	70	ICMP	2014-03-26 08:30:21.041	1.035376	Destination unreachable...
7	172.16.148.135	172.16.148.1	98	98	ICMP	2014-03-26 08:30:21.641	1.635041	Echo request (Code=0)
8	172.16.148.1	172.16.148.135	98	98	ICMP	2014-03-26 08:30:21.641	1.635171	Echo reply (Code=0)
9	172.16.148.135	172.16.148.1	98	98	ICMP	2014-03-26 08:30:22.642	2.636535	Echo request (Code=0)
10	172.16.148.1	172.16.148.135	98	98	ICMP	2014-03-26 08:30:22.642	2.636602	Echo reply (Code=0)

Details | Values

- Packet
- Ethernet-Header
- IP-Header
- ICMP-Header

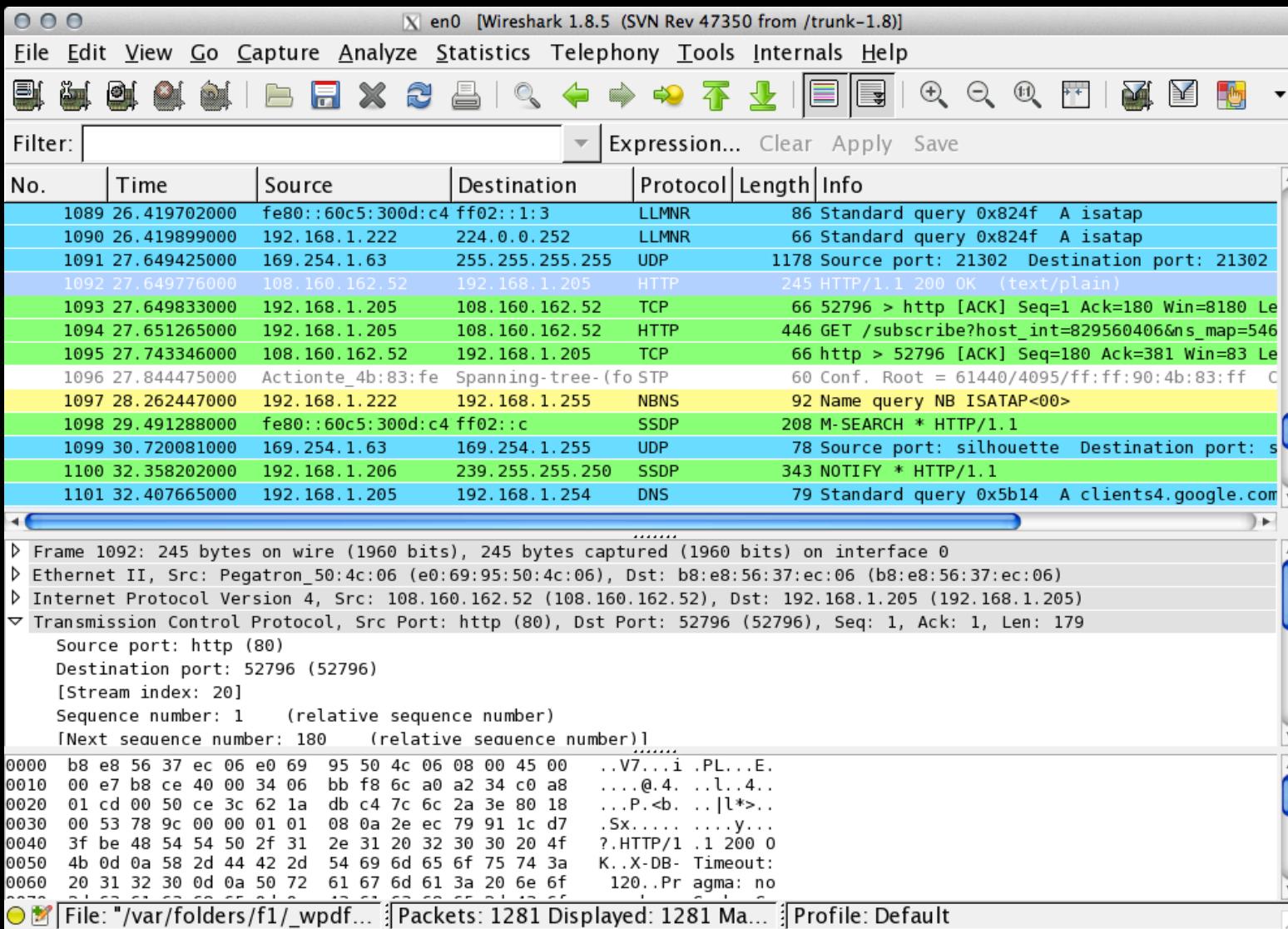
Length: 64 bytes
Type: 8 (Echo request)
Code: 0
Checksum: 0x91a8
Identifier: 0x9702
Sequence: 1

00: 00 50 56 C0 00 01 00 0C 29 F9 C0 93 08 00 45 00 00 54 B5 CA 00 00 40 01 00 00 AC 10 .PV.....).....E..T....@....
28: 94 87 AC 10 94 01 08 00 91 A8 97 02 00 01 53 32 C8 5D 00 09 C8 B7 08 09 0A 0B 0C 0DS2.].....
56: 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29!"#\$%&'@
84: 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 *+,-./01234567

Fileformat: 2.4 Snaplength: 65535 bytes Linktype: ETHERNET (DLT_EN10MB) Filesize: 5752 bytes Packets: 52 of 52 (1 selected)

Network Analysis – Wireshark

www.wireshark.org/download.html



Network Analysis

tcpdump

Without Content: `tcpdump -i en0 -n host #.#.#.#`

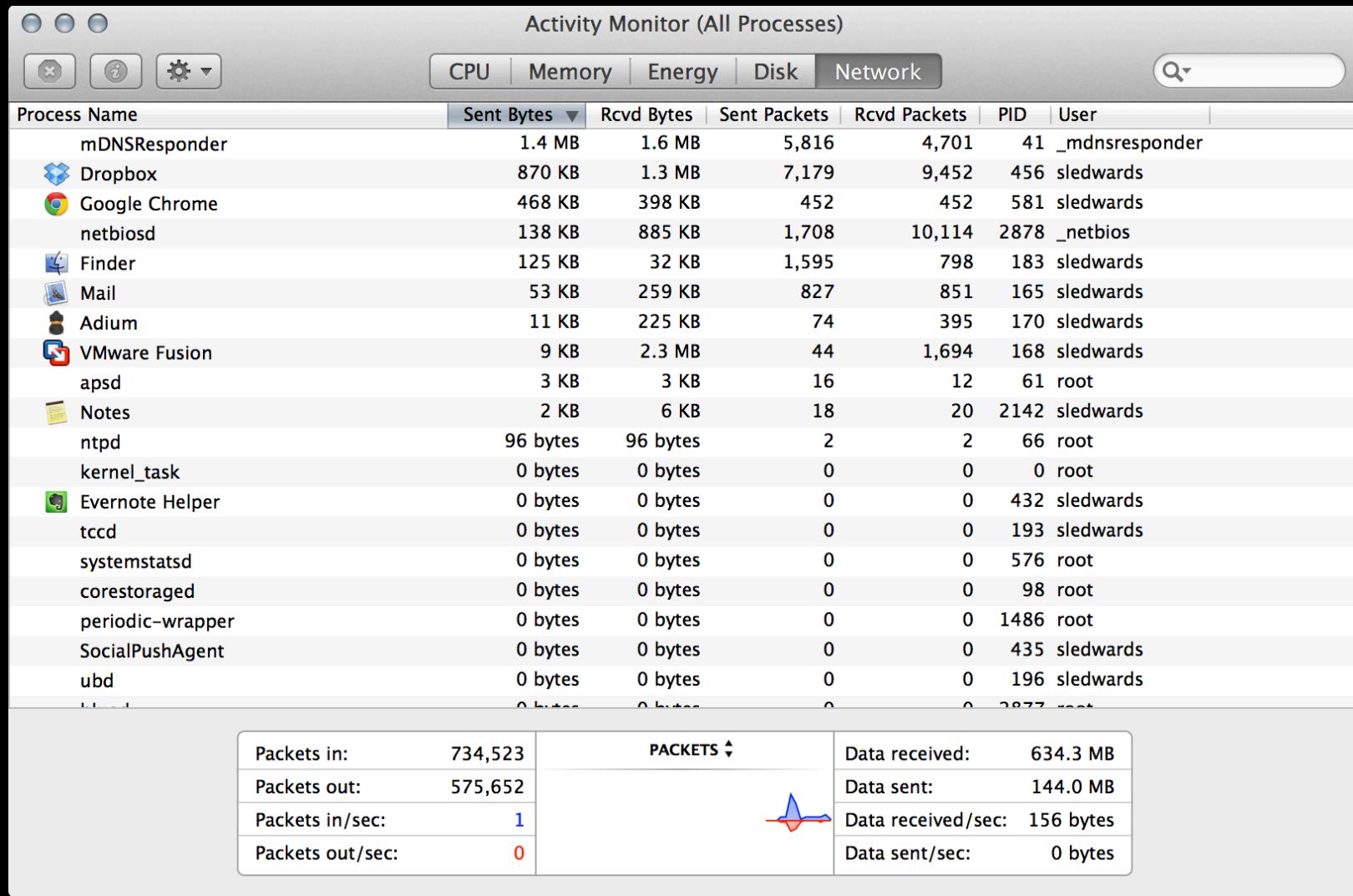
```
nibble:~ sledwards$ tcpdump -i en0 -n host 192.168.1.205
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 65535 bytes
16:26:16.626586 IP 192.168.1.205.53398 > 108.160.165.212.443: Flags [F.], seq 2979705787, ack 3210059276, win 8192, options [nop,nop,TS val 760117124 ecr 3433675004], length 0
16:26:17.202780 IP 192.168.1.205.52626 > 192.168.1.128.5001: Flags [P.], seq 222079171:222079481, ack 980612418, win 8192, options [nop,no p,TS val 760117699 ecr 2488032], length 310
16:26:17.202959 IP 192.168.1.205.52626 > 192.168.1.128.5001: Flags [P.], seq 310:382, ack 1, win 8192, options [nop,nop,TS val 760117699 ecr 2488032], length 72
16:26:17.204283 IP 192.168.1.128.5001 > 192.168.1.205.52626: Flags [.], ack 310, win 2641, options [nop,nop,TS val 2488537 ecr 760117699], length 0
```

With Content: `tcpdump -i en0 -n -X host #.#.#.#`

```
nibble:~ sledwards$ tcpdump -i en0 -n -X host 192.168.1.205
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en0, link-type EN10MB (Ethernet), capture size 65535 bytes
16:47:15.694066 IP 192.168.1.128.5001 > 192.168.1.205.52626: Flags [P.], seq 980659379:980659434, ack 222192319, win 2641, options [nop,no p,TS val 2614360 ecr 761370136], length 55
    0x0000: 4500 006b 9396 4000 4006 2259 c0a8 0180 E..k..@."Y....
    0x0010: c0a8 01cd 1389 cd92 3a73 acb3 0d3e 62bf .....:s...>b.
    0x0020: 8018 0a51 4fea 0000 0101 080a 0027 e458 ...Q0.....'.X
    0x0030: 2d61 9618 1703 0300 3235 192f 427b 51c0 -a.....25./B{Q.
    0x0040: c1af 1984 6097 41cc 95fd 6a45 92ac 8720 ....`A...jE....
    0x0050: 97e2 d240 9618 9489 8d4f 1325 8716 737d ...@.....0.%..s}
    0x0060: e191 16fe 457c 22c6 1e80 77 ....E!"...w
16:47:15.694134 IP 192.168.1.205.52626 > 192.168.1.128.5001: Flags [.], ack 55, win 8188, options [nop,nop,TS val 761370908 ecr 2614360], length 0
    0x0000: 4500 0034 d3a7 4000 4006 e27e c0a8 01cd E..4..@..~.....
    0x0010: c0a8 0180 cd92 1389 0d3e 62bf 3a73 acea .....>b.:s..
    0x0020: 8010 1ffc eeaе 0000 0101 080a 2d61 991c .....-a..
    0x0030: 0027 e458 .....'.X
```

Network Analysis

Activity Monitor



Network Analysis – lsof

www.newosxbook.com/index.php?page=downloads

Time	Local Addr	Remote Addr	If	State	PID	(Name)
14:39:03	fd85:971f:afda:26d4:f5c4:2bf:2800:b80:123	*.*			8	N/A
14:39:03	0.0.0.0:17500	*.*	0	N/A	596	(Dropbox)
14:39:03	0.0.0.0:52988	*.*	1	N/A	20	(syslogd)
14:39:03	fd85:971f:afda:26d4:f5c4:2bf:2800:b80:4500	*.*			8	N/A
14:39:03	fd85:971f:afda:26d4:f5c4:2bf:2800:b80:500	*.*			8	N/A
14:39:03	fe80::f5c4:2bf:2800:b80:123	*.*		8 N/A	66	(ntpd)
14:39:03	::1:4500	*.*	1	N/A	612	(racoon)
14:39:03	::1:500	*.*	1	N/A	612	(racoon)
14:39:03	127.0.0.1:4500	*.*	1	N/A	612	(racoon)
14:39:03	127.0.0.1:500	*.*	1	N/A	612	(racoon)
14:39:03	fe80::1:4500	*.*	1	N/A	612	(racoon)
14:39:03	fe80::1:500	*.*	1	N/A	612	(racoon)
14:39:03	192.168.1.205:4500	*.*	4	N/A	612	(racoon)
14:39:03	192.168.1.205:500	*.*	4	N/A	612	(racoon)
14:39:03	fe80::f5c4:2bf:2800:b80:4500	*.*		8 N/A	612	(racoon)
14:39:03	fe80::f5c4:2bf:2800:b80:500	*.*		8 N/A	612	(racoon)
14:39:03	0.0.0.0:64835	*.*	0	N/A	170	(Adium)
14:39:03	192.168.1.205:123	*.*	4	N/A	66	(ntpd)
14:39:03	fe80::1:123	*.*	1	N/A	66	(ntpd)
14:39:03	::1:123	*.*	1	N/A	66	(ntpd)
14:39:03	::61675	*.*	0	N/A	41	(mDNSResponder)
14:39:03	0.0.0.0:0	*.*	0	N/A	106	(airportd)
14:39:03	0.0.0.0:0	*.*	0	N/A	12	(UserEventAgent)
14:39:03	192.168.1.205:52377	23.195.92.166:443	4	ESTABLISHED	161	(Google Chrome)
14:39:03	192.168.1.205:51966	173.194.76.125:5222	4	ESTABLISHED	161	(Google Chrome)
14:39:03	192.168.1.205:51863	173.194.68.108:993	4	ESTABLISHED	163	(Mail)
14:39:03	192.168.1.205:51845	129.21.49.169:143	4	ESTABLISHED	163	(Mail)
14:39:03	127.0.0.1:26164	*.*	1	LISTENING	596	(Dropbox)
14:39:03	::1:631	*.*	1	LISTENING	1	(launchd)
14:39:20	192.168.1.205:52397	108.160.165.212:443	4	SYN_SENT	596	(Dropbox)
14:39:20	192.168.1.205:52398	108.160.165.212:443	4	SYN_SENT	596	(Dropbox)
14:39:21	192.168.1.205:52399	23.23.226.102:443	4	SYN_SENT	596	(Dropbox)

Malware Analysis Examples

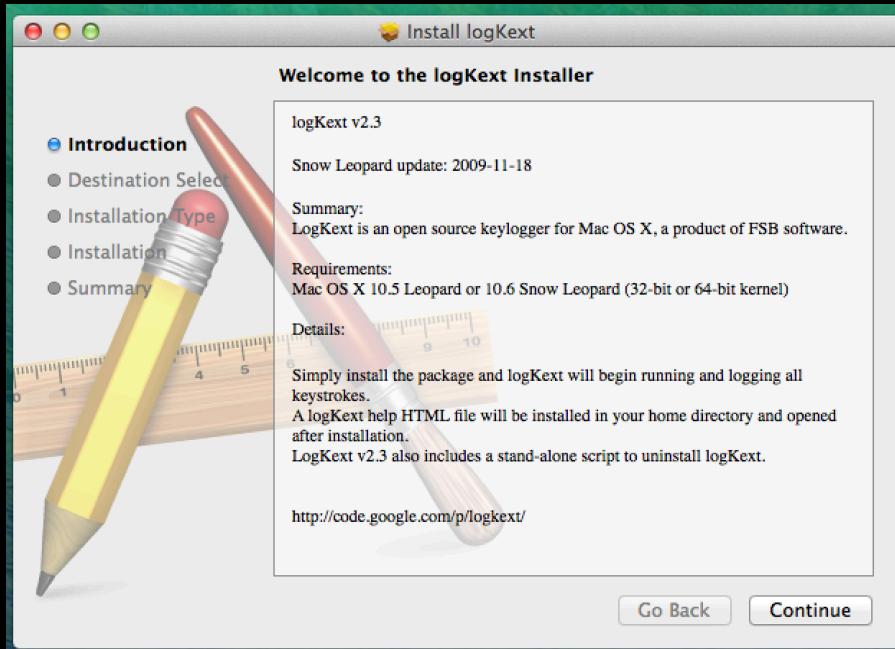
LogKext – Open Source Keylogger

- *.pkg Installer

Imuler – File/Screenshot Stealer

- *.app disguised as a photo

Example - LogKext



The screenshot shows a web browser window titled 'LogKext v2.2'. The address bar shows 'file:///LogKext%20Readme.html'. The page content is the 'logKext v2.2' README. It features a title 'logKext v2.2' and a 'Release Date: 2008-1-9'. Below this, there are sections for 'Summary', 'Requirements', 'How to get started', and 'Step 1: Finding the Terminal' and 'Step 2: Using the Terminal'. The 'Summary' section states: 'LogKext is a freeware keylogger for Mac OS X, a product of FSB software.' The 'Requirements' section specifies 'Mac OS X 10.4 or 10.5'. The 'How to get started' section explains that control and usage is through 'logKextClient'. The 'Step 1' and 'Step 2' sections provide instructions for using the terminal, including commands like 'sudo logKextClient' and the password prompt 'logKext password:'. A note at the bottom says: 'Type in your logKext password. The default password is "logKext". You will not see the password echoed to the screen as you type it.'

Example - LogKext newproc.d

```
2014 Apr  1 17:46:48 1445 <444> 64b  /bin/sh /tmp/  
PKInstallSandbox.82TjPW/Scripts/  
com.fsb.logkext.logkextExt.pkg.V8BqhR/postinstall /Users/  
cliffstoll/Desktop/logKext-2.3.pkg /System/Library/  
Extensions / /
```

```
2014 Apr  1 17:46:49 1457 <1445> 64b  /Library/Application  
Support/logKext/logKextKeyGen
```

```
2014 Apr  1 17:46:49 1458 <1445> 64b  /bin/launchctl  
load /Library/LaunchDaemons/logKext.plist
```

```
2014 Apr  1 17:46:49 1460 <1445> 64b  /usr/bin/open /  
LogKext Readme.html
```

Example - LogKext newproc.d

2014 Apr 1 17:46:48 1455 <1445> 64b /sbin/kextunload -b
com.fsb.kext.logKext

2014 Apr 1 17:46:49 1456 <1445> 64b /sbin/kextload /
System/Library/Extensions/logKext.kext

2014 Apr 1 17:46:49 1459 <1> 64b /Library/Application
Support/**logKext/logKextDaemon**

2014 Apr 1 17:47:00 1472 <897> 64b **login -pf cliffstoll**

2014 Apr 1 17:47:00 1473 <1472> 64b **-bash**

2014 Apr 1 17:47:11 1476 <1473> 64b **sudo logKextClient**

2014 Apr 1 17:47:11 1477 <1476> 64b **logKextClient**

Example - LogKext

fs_usage -f pathname

```
17:40:24.418176  getattrlist /Users/cliffstoll/Desktop/  
logKext-2.3.pkg 0.000004  Finder.7100
```

```
17:40:24.418285  setattrlist /System/Library/CoreServices/  
Installer.app 0.000012  Finder.7100
```

```
17:40:24.641275  open F=15 (RW_A_E) private/var/log/install.log  
0.000028  syslogd.30889
```

```
17:40:39.296222  statfs64 /Library/Application Support/logKext  
0.000021  mds.30953
```

```
17:40:39.296445  stat64 /System/Library/Extensions/logKext.kext  
0.000010  mds.30953
```

```
17:40:43.135053  setattrlist /LogKextUninstall.command 0.000014  
mds.31061
```

Example - LogKext

fs_usage -f pathname

```
17:40:58.946647  open F=3 (R_____)  /usr/bin/logKextClient  
0.000007  logKextKeyGen.31301
```

```
17:40:59.028515  open [ 2] (R_____)  /Library/Preferences/  
com.fsb.logKext.plist 0.000003  cfprefsd.31142
```

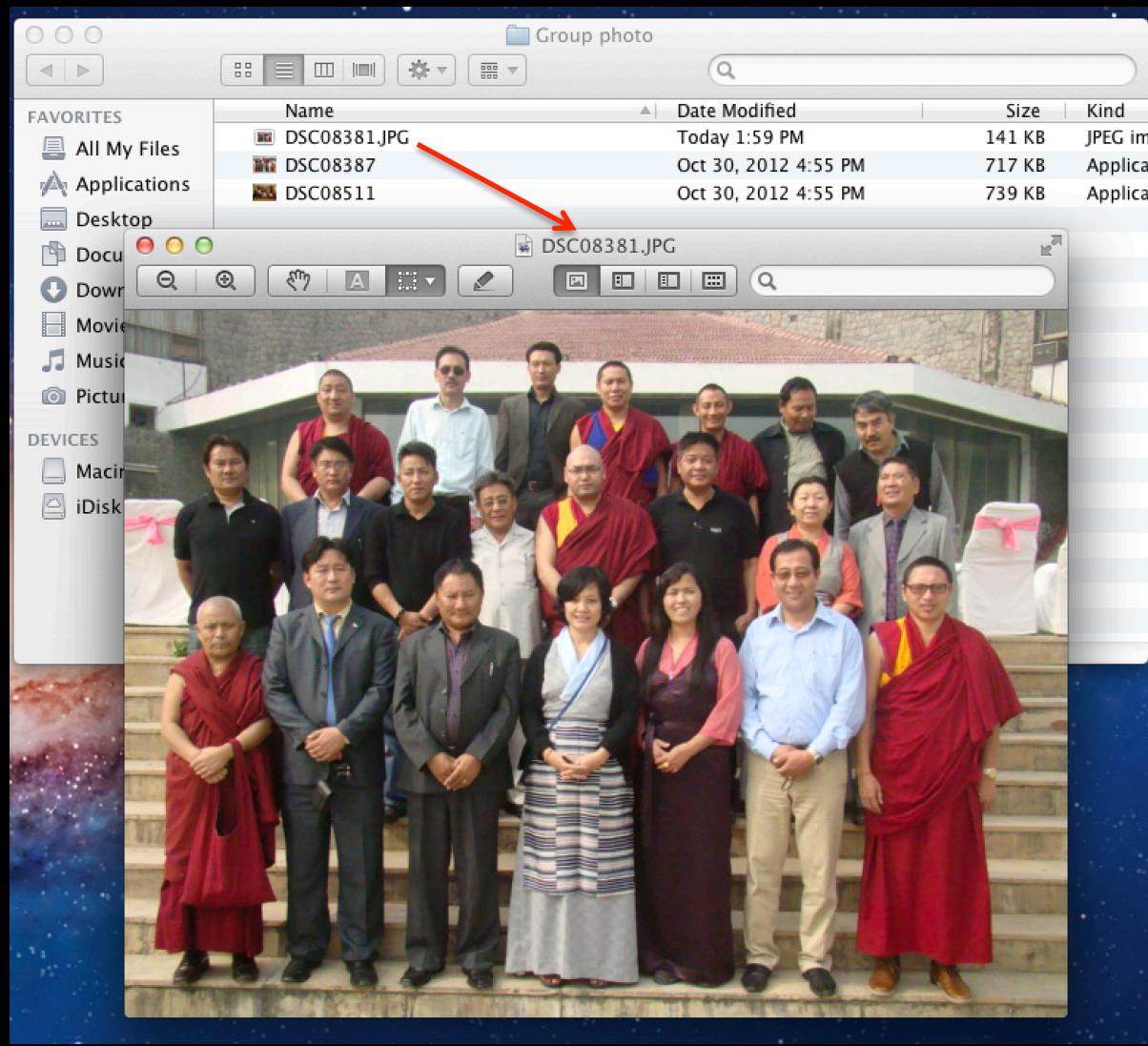
```
17:40:59.056241  statfs [ 2] /Library/Preferences/com.fsb.logKext  
0.000018  logKextDaemon.31319
```

```
17:40:59.190232  open F=11 (R_____)  /LogKext Readme.html 0.000007  
mds.31061
```

```
17:41:06.808873  open F=25 (_WC_T_)  /Users/cliffstoll/Library/  
Caches/Metadata/Safari/History/file:%2F%2F%2FLogKext  
%2520Readme.html.webhistory 0.000110  Safari.31520
```

```
17:41:31.191547  stat64 /usr/bin/logKextClient  
0.000007  sudo.31638
```

Example - Imuler



Example - Imuler fs_usage -f exec

```
Elwoods-Mac:~ elwoodblues$ sudo fs_usage -f exec
```

WARNING: Improper use of the sudo command could lead to data loss or the deletion of important system files. Please double-check your typing when using sudo. Type "man sudo" for more information.

To proceed, enter your password, or type Ctrl-C to abort.

Password:

14:17:50	posix_spawn	p/Group photo/DSC08381.app/Contents/MacOS/FileAgent	0.000641 W launchd
14:17:50	posix_spawn	/usr/libexec/taskgated	0.000338 W launchd
14:17:50	execve	OSServices.framework/Versions/A/Support/SFLIconTool	0.000371 coreservices
14:17:50	posix_spawn	/bin/sh	0.001594 W FileAgent
14:17:50	execve	private/tmp/Spotlight	0.000223 sh
14:17:50	posix_spawn	/bin/sh	0.003831 W FileAgent
14:17:50	execve	private/tmp/launch-ICS000	0.000232 sh
14:17:50	execve	/usr/bin/open	0.001563 W sh
14:17:51	execve	A/Support/lssave	0.002305 W coreservices
14:17:51	posix_spawn	/Applications/Preview.app/Contents/MacOS/Preview	0.003968 W launchd
14:17:52	execve	OSServices.framework/Versions/A/Support/SFLIconTool	0.000363 coreservices
14:17:52	posix_spawn	/bin/sh	0.001929 W FileAgent
14:17:52	execve	/bin/rm	0.000193 sh
14:17:52	posix_spawn	/usr/libexec/xpcproxy	0.005484 W launchd
14:17:52	execve	y.pboxd.xpc/Contents/MacOS/com.apple.security.pboxd	0.004930 W xpcproxy
14:17:53	execve	OSServices.framework/Versions/A/Support/SFLIconTool	0.000449 coreservices
14:17:53	posix_spawn	/usr/libexec/lsboxd	0.002383 W launchd
14:17:54	posix_spawn	s/OpenGLES.framework/Versions/A/Libraries/CVMCompiler	0.001632 W launchd

Example - Imuler fseventer [1]

📄	/Users/elwoodblues/Desktop/Group photo/DSC08381.JPG	1:59:54 PM	File Created	950 (exited?)
📁	/Users/elwoodblues/Library/Preferences/SDMHelpData/AppleExtra/English/HelpSDMIndexFile	1:59:54 PM	Folder Changed	System
📁	/Users/elwoodblues/Library/Saved Application State/com.fernlightning.fseventer.savedState	1:59:54 PM	Folder Changed	System
📁	/private/tmp	1:59:54 PM	Folder Changed	System
📄	/Users/elwoodblues/Desktop/Group photo/DSC08381.JPG	1:59:54 PM	Content Modified	950 (exited?)
📄	/private/tmp/DSC08381.JPG	1:59:54 PM	File Created	950 (exited?)
📄	/private/tmp/DSC08381.JPG	1:59:54 PM	Content Modified	950 (exited?)
████	/private/tmp/launch-ICS000	1:59:54 PM	File Created	950 (exited?)
████	/private/tmp/launch-ICS000	1:59:54 PM	Content Modified	950 (exited?)
████	/private/tmp/launch-ICS000	1:59:54 PM	Chown	950 (exited?)
✗	./.Spotlight-V100/Store-V2/552B9C16-9B3A-4E91-B1C4-9128412E64ED/journalAttr.6	1:59:54 PM	File Created	mds
████	/Users/elwoodblues/Library/LaunchAgents/ScheduledSync	1:59:54 PM	File Created	953 (exited?)
████	/Users/elwoodblues/Library/LaunchAgents/ScheduledSync	1:59:54 PM	Content Modified	953 (exited?)
📄	/Users/elwoodblues/Library/LaunchAgents/ScheduledSync.plist	1:59:54 PM	File Created	Spotlight
📄	/Users/elwoodblues/Library/LaunchAgents/ScheduledSync.plist	1:59:54 PM	Content Modified	Spotlight
████	/Users/elwoodblues/Library/LaunchAgents/ScheduledSync	1:59:54 PM	Chown	Spotlight
📄	/Users/elwoodblues/Library/LaunchAgents/ScheduledSync.plist	1:59:54 PM	Chown	Spotlight
📄	/Users/elwoodblues/Library/.confback	1:59:54 PM	File Created	Spotlight
📄	/Users/elwoodblues/Library/.confback	1:59:54 PM	Content Modified	Spotlight

Example - Imuler fseventer [2]

✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app	1:59:55 PM	Terminated App	System
✚ /Applications/Preview.app	1:59:56 PM	Launched App	launchd
✚ /Users/elwoodblues/Library/Saved Application State/com.apple.finder.savedState/window_14.data	1:59:55 PM	Stat Changed	Finder
✚ /Users/elwoodblues/Library/Saved Application State/com.apple.finder.savedState/window_14.data	1:59:55 PM	Modified xattr	Finder
✚ /Users/elwoodblues/Library/Saved Application State/com.apple.finder.savedState/data.data	1:59:55 PM	Content Modified	Finder
✚ /Users/elwoodblues/Library/Saved Application State/com.apple.finder.savedState/windows.plist	1:59:55 PM	Stat Changed	Finder
✚ /Users/elwoodblues/Library/Saved Application State/com.apple.finder.savedState/windows.plist	1:59:55 PM	Content Modified	Finder
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/Info.plist	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/MacOS/.cnf	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/MacOS/.confr	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/MacOS/.conft	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/MacOS/FileAgent	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/MacOS	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/PkgInfo	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/Resources/co.icns	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/Resources/English.lproj/InfoPlist.strings	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/Resources/English.lproj/MainMenu.nib	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/Resources/English.lproj	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents/Resources	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app/Contents	1:59:55 PM	Deleted	959 (exited?)
✗ /Users/elwoodblues/Desktop/Group photo/DSC08381.app	1:59:55 PM	Deleted	959 (exited?)

Example – Imuler tcpdump

- Beacons to “ouchmen.com”

```
13:47:04.202620 IP 172.16.148.1 > 172.16.148.136: ICMP 172.16.148.1 udp port 53 unreachable, length 36
 0x0000: 4500 0038 ccf6 0000 4001 2d24 ac10 9401 E..8....@.-$....
 0x0010: ac10 9488 0303 21f2 0000 0000 4500 0049 .....!.....E..I
 0x0020: e458 0000 ff11 56a0 ac10 9488 ac10 9401 .X....V.....
 0x0030: daa0 0035 0035 0000           ...5.5..
13:47:04.202647 IP 172.16.148.136.61721 > 172.16.148.1.53: 54710+ A? www.ouchmen.com. (33)
 0x0000: 4500 003d 6914 0000 ff11 0000 ac10 9488 E..=i.....
 0x0010: ac10 9401 f119 0035 0029 80e5 d5b6 0100 .....5.).....
 0x0020: 0001 0000 0000 0000 0377 7777 076f 7563 .....www.ouc
 0x0030: 686d 656e 0363 6f6d 0000 0100 01     hmen.com.....
13:47:04.202779 IP 172.16.148.1 > 172.16.148.136: ICMP 172.16.148.1 udp port 53 unreachable, length 36
 0x0000: 4500 0038 5461 0000 4001 a5b9 ac10 9401 E..8Ta..@.....
 0x0010: ac10 9488 0303 0b85 0000 0000 4500 003d .....E..=
 0x0020: 6914 0000 ff11 d1f0 ac10 9488 ac10 9401 i.....
 0x0030: f119 0035 0029 0000           ...5.)..
13:47:04.202807 IP 172.16.148.136.58918 > 172.16.148.1.53: 35328+ AAAA? www.ouchmen.com. (33)
 0x0000: 4500 003d d956 0000 ff11 0000 ac10 9488 E..=V.....
 0x0010: ac10 9401 e626 0035 0029 80e5 8a00 0100 .....&.5.).....
 0x0020: 0001 0000 0000 0000 0377 7777 076f 7563 .....www.ouc
 0x0030: 686d 656e 0363 6f6d 0000 1c00 01     hmen.com.....
```

Resources & References

Blogs

- “Reverse Engineering OS X” - reverse.put.as (@osxreverser)
- “Reverse Engineering Resources” - <http://samdmmarshall.com/re.html> (@dirk_gently)
- Hopper App Blog - hopperapp.tumblr.com (@hopperapp)

Resources

- Apple Developer Website
- man Pages

Malware Samples

- Contagio - contagiodump.blogspot.com
- VXShare - virusshare.com
- Open Malware - www.offensivecomputing.net
- Malwr - malwr.com

Contact me at: [@iamevl twin or \[oompa@csh.rit.edu\]\(mailto:oompa@csh.rit.edu\)](mailto:@iamevl twin)