WHEN MACS GET HACKED

Sarah Edwards
@iamevltwin
oompa@csh.rit.edu
mac4n6.com

CURRENT THREATS:

Suspicious Use	Insider Threat	Data Exfiltration
Keylogger	Ad-Click Malware	Information Stealer
Phishing	Backdoors	Commercial Spyware

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

CURRENT THREATS: FLASHBACK

- Infected 600,000+ systems
- $10,000/day ad-click revenue for attackers
- Java Vulnerabilities
- Fake Adobe Flash Installer
- Drive-by-Download
  - Compromised Wordpress Blogs

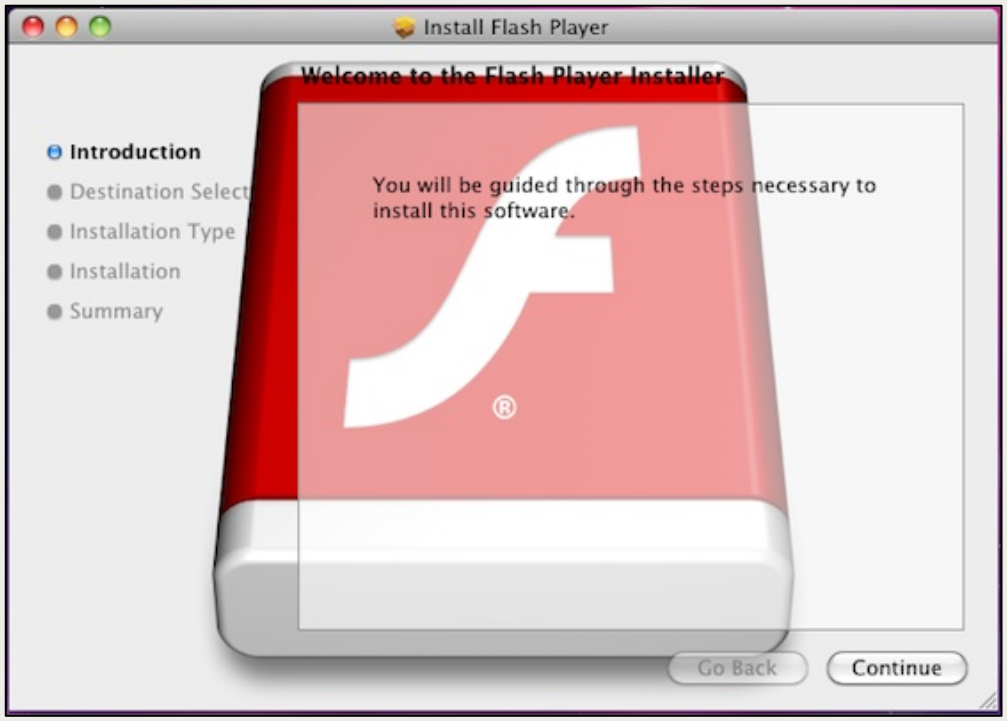


Image Source: http://www.cultofmac.com/124840/new-flashback-os-x-trojan-is-in-the-wild-and-it-can-kill-os-xs-anti-malware-scams/

CURRENT THREATS: COINTHEIF / STEALTHBIT

- Installed Browser Extensions in Safari and Chrome
- "Pop-Up Blocker"
- Snoops browser traffic for Bitcoin credentials (and other interesting data)
- Sends data to C2 Server

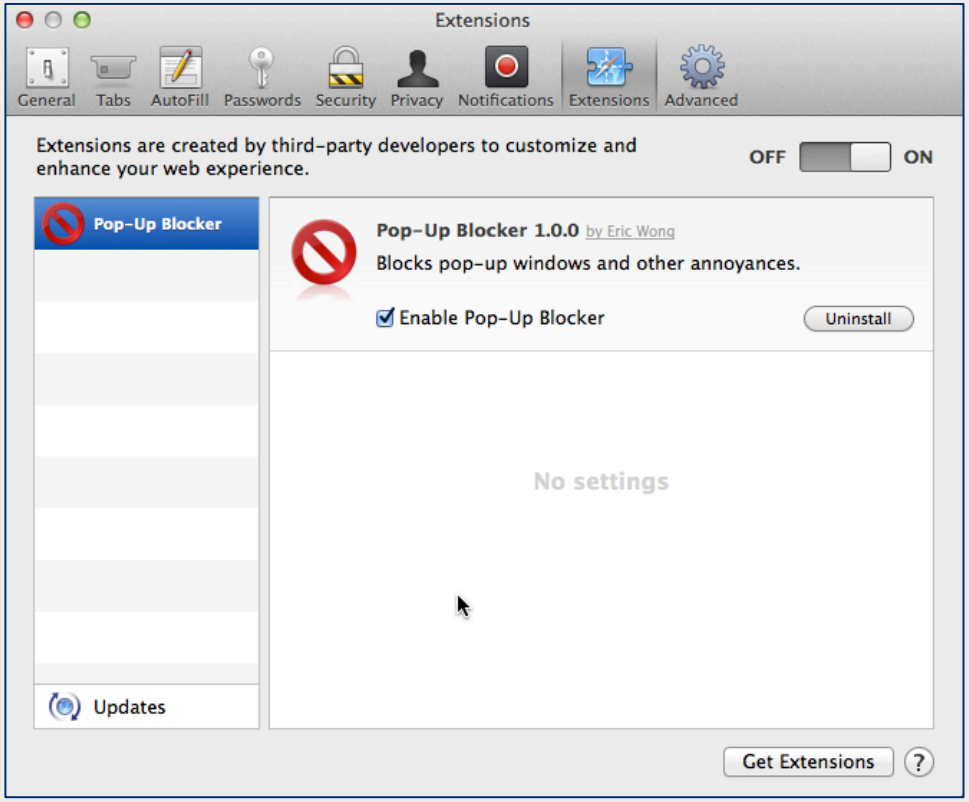


Image Source: http://www.thesafemac.com/wp-content/uploads/2014/02/CoinThief-extension.png

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

CURRENT THREATS: WIRELURKER

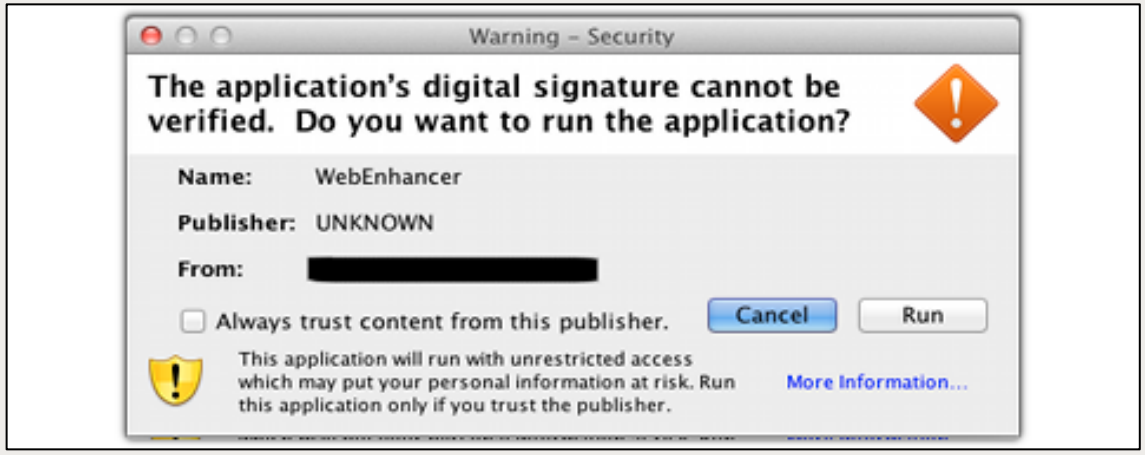
- Repackaged & Trojanized 3rd Party OS X Applications on Maiyadi App Store (Chinese)
- Infects connected iOS devices via OS X using dynamically generated malicious apps
  - Jailbroken and non-jailbroken
- Persistence via LaunchDaemon
- Uses Open Source Software libimobiledevice to monitor for USB connections

WIRELURKER INFECTED APPLICATION	NUMBER OF DOWNLOADS
The Sims 3	42,110
International Snooker 2012	22,353
Pro Evolution Soccer 2014	20,800
Bejeweled 3	19,016
Angry Birds	14,009
Spider 3	12,745
NBA 2K13	11,113
GRID	10,820
Battlefield: Bad Company 2	8,065
Two Worlds II Game of the Year Edition	6,451

Image Source: https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

CURRENT THREATS: CRISIS / MORCUT

- Rootkit & Spyware
- Arrives as AdobeFlashPlayer.jar
  - WebEnhancer.class
- Cross-platform (Windows!)
- Backdoor Access: Screenshots, keylog, webcam, location, microphone, files, IM data, etc.

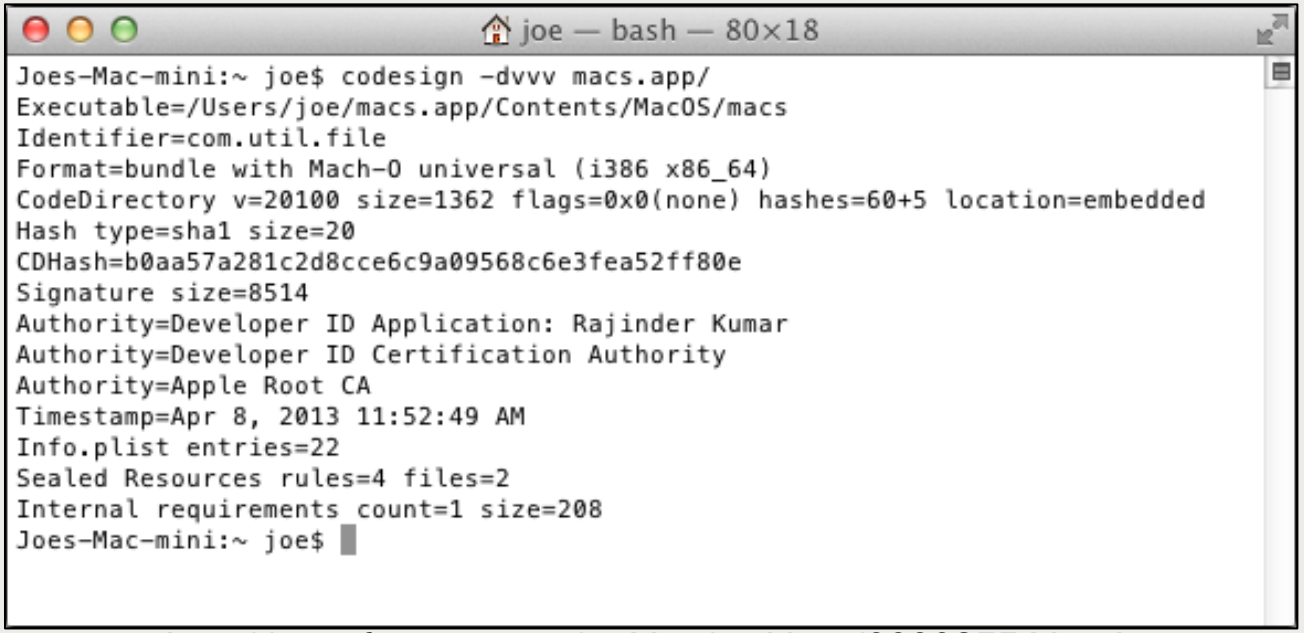


http://nakedsecurity.sophos.com/2012/07/25/mac-malware-crisis-on-mountain-lion-eve/

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

CURRENT THREATS: KITM

- Found on Angolan activist's system at Oslo Freedom Forum
- Backdoor
- Takes periodic screenshots
- Signed with Apple Developer ID



http://www.f-secure.com/weblog/archives/00002554.html

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

INCIDENT RESPONSE

What

- System Information
- Network Data
- Users Logged On
- Running Processes
- Open Files
- Memory Analysis

Why

- Collect Volatile Data
- Triage Analysis
- Dead-Box Analysis
- Encryption

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

INCIDENT RESPONSE: DATA COLLECTION COMMANDS

System Information

- `date`
- `hostname`
- `uname –a` – Kernel & Architecture Info
- `sw_vers` – OS X Version

Network Information

- `ifconfig` – Network Configuration
- `netstat –an` – Active network connections
- `lsof –i` – Network connections by process
- `netstat –rn` – Routing Table
- `arp –an` – ARP Table

Open Files – `lsof`

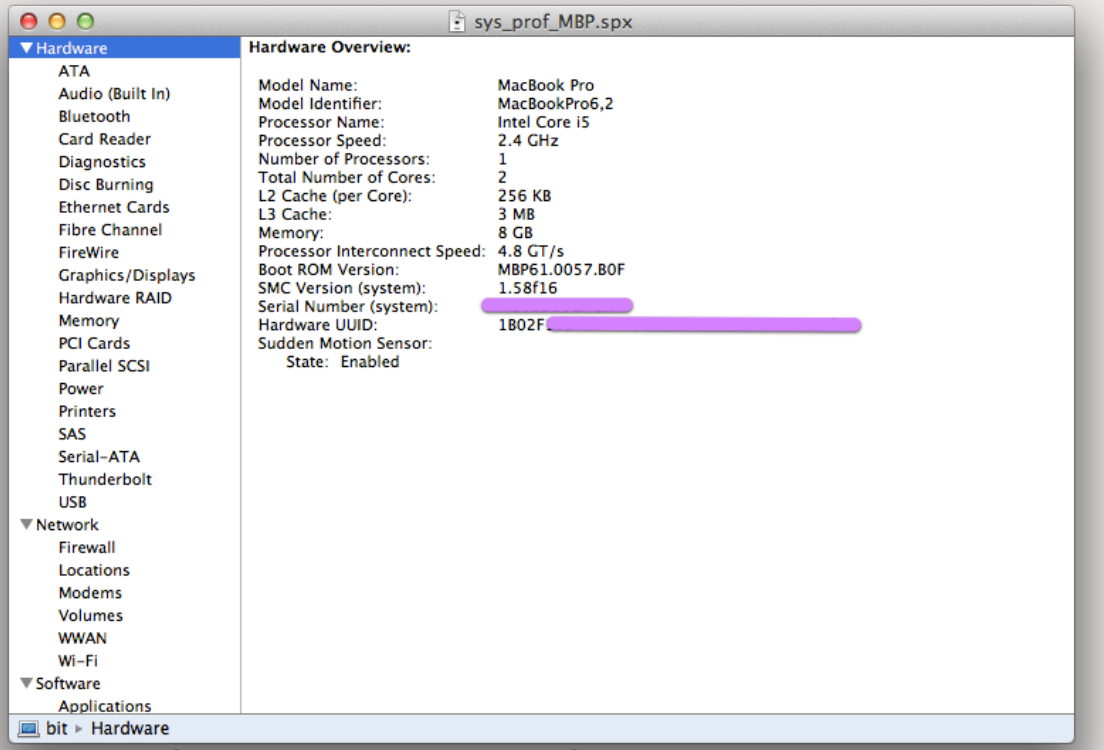
Logged on users – `who –a`, `w`

Process List – `ps aux`

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

INCIDENT RESPONSE: SYSTEM INFORMATION

- `system_profiler -xml -detaillevel full > /Volume/IR_CASE/sys_prof_MBP.spx`
- Open in “System Information.app”
- Contains:
  - Hardware Information
  - USB Information
  - Network Information
  - Firewall Settings
  - Mounted Volumes
  - System Information
  - Applications
  - Kernel Extensions
  - Log Data



oompa@csh.rit.edu | @iamevltwin | mac4n6.com

MEMORY COLLECTION & ANALYSIS

Collection

- OSXpmem
- MacQuisition
- Recon

Analysis

- Volatility
- Rekall

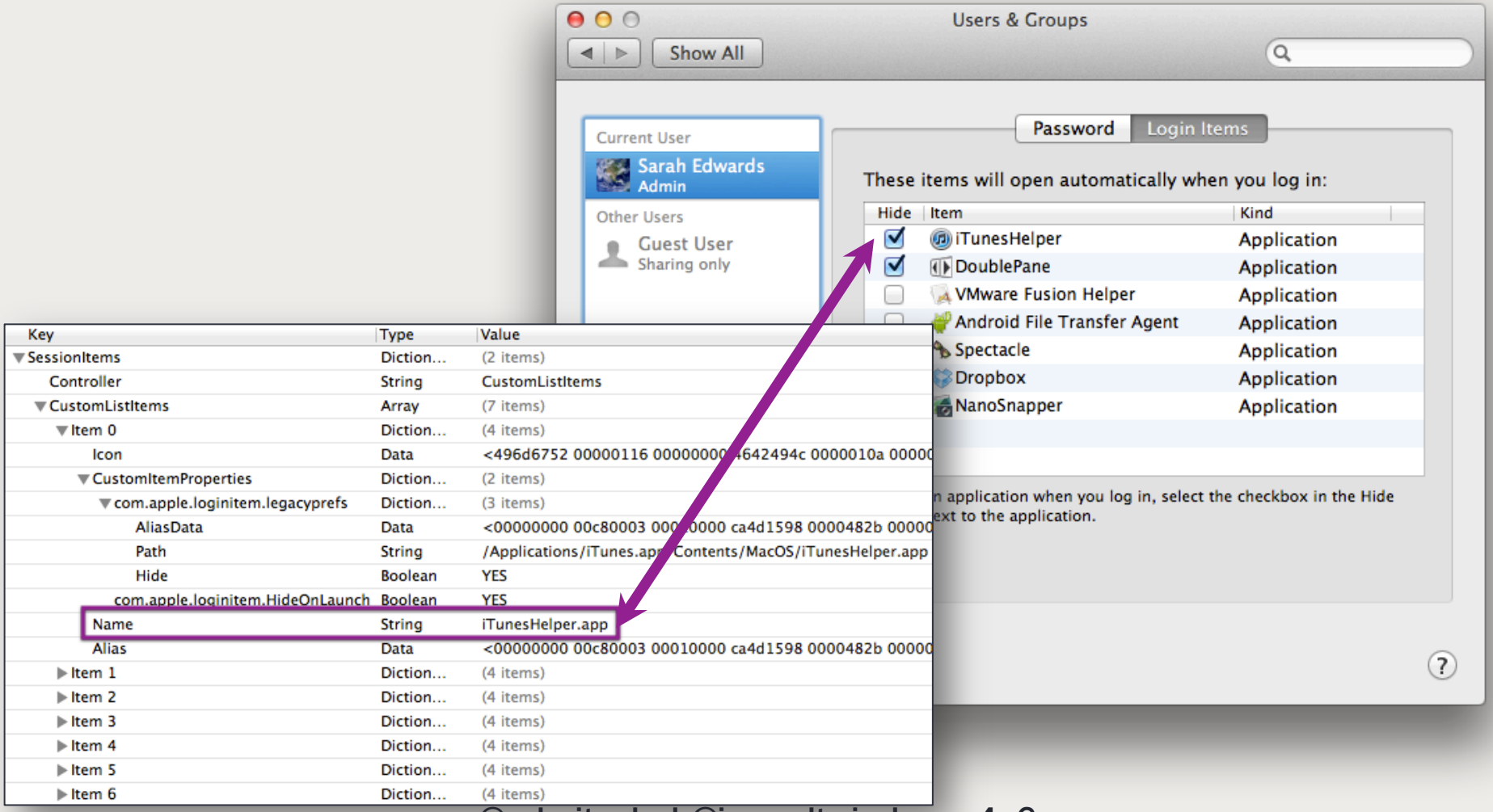
oompa@csh.rit.edu | @iamevltwin | mac4n6.com

MAC AUTORUNS

AUTORUNS: LOGIN ITEMS

- Launched when user logs into system via GUI
- Location:
  - ~/Library/Preferences/com.apple.loginitems.plist
  - <application>.app/Contents/Library/LoginItems/

AUTORUNS: LOGIN ITEMS EXAMPLE



oompa@csh.rit.edu | @iamevltwin | mac4n6.com

AUTORUNS: LAUNCH AGENTS & DAEMONS

- Preferred Method
- Introduced in 10.4 (w/launchd)
- Property List File
- Popular with current Mac malware
- Reference: TN2083

AUTORUNS: LAUNCH AGENTS

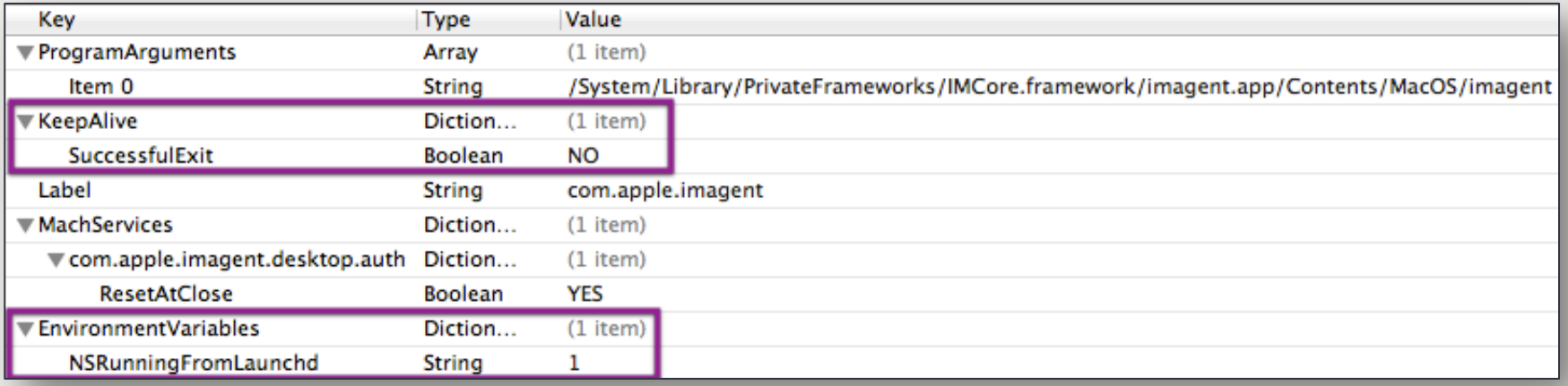
- Agent – Background User Process
  - Can access user home directory
  - May have GUI (limited, if at all)
- Location:
  - /System/Library/LaunchAgents/
  - /Library/LaunchAgents/
  - ~/Library/LaunchAgents

AUTORUNS: LAUNCH AGENTS EXAMPLES

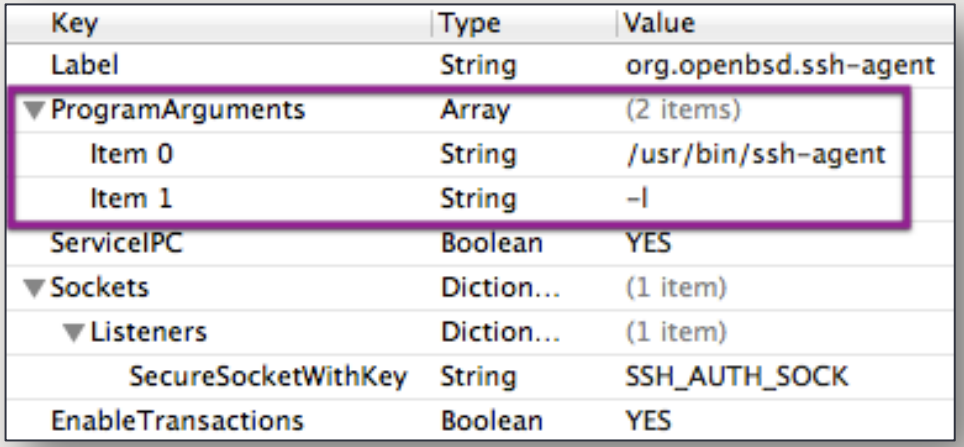
```
com.apple.AOSNotificationOSX.plist
com.apple.AddressBook.SourceSync.plist
com.apple.AddressBook.abd.plist
com.apple.AirPortBaseStationAgent.plist
com.apple.AppStoreUpdateAgent.plist
com.apple.AppleGraphicsWarning.plist
com.apple.BezelUI.plist
com.apple.CoreLocationAgent.plist
com.apple.DictionaryPanelHelper.plist
com.apple.DiskArbitrationAgent.plist
com.apple.Dock.plist
com.apple.FTCleanup.plist
com.apple.FileSyncAgent.PHD.plist
com.apple.FileSyncAgent.iDisk.plist
com.apple.Finder.plist
com.apple.FontRegistryUIAgent.plist
com.apple.FontValidator.plist
com.apple.FontValidatorConduit.plist
com.apple.FontWorker.plist
com.apple.KerberosHelper.LKDCHelper.plist
com.apple.LaunchServices.lsboxd.plist
com.apple.NetworkDiagnostics.plist
com.apple.PCIESlotCheck.plist
com.apple.PreferenceSyncAgent.plist
com.apple.PubSub.Agent.plist
com.apple.ReclaimSpaceAgent.plist
com.apple.RemoteDesktop.plist
com.apple.ReportCrash.Self.plist
com.apple.ReportCrash.plist
com.apple.ReportGPURestart.plist
com.apple.ReportPanic.plist
com.apple.ScreenReaderUIServer.plist
com.apple.ServiceManagement.LoginItems.plist
com.apple.SubmitDiagInfo.plist
com.apple.SystemUIServer.plist
com.apple.TMLaunchAgent.plist
com.apple.TrustEvaluationAgent.plist
com.apple.UserEventAgent-Aqua.plist
com.apple.UserEventAgent-LoginWindow.plist
com.apple.UserNotificationCenterAgent-LoginWindow.plist
com.apple.UserNotificationCenterAgent.plist
com.apple.VoiceOver.plist
com.apple.WebKit.PluginAgent.plist
com.apple.ZoomWindow.plist
com.apple.alf.useragent.plist
com.apple.aos.migrate.plist
com.apple.bluetoothUIServer.plist
com.apple.btsa.plist
com.apple.cfnetwork.AuthBrokerAgent.plist
com.apple.cookied.plist
com.apple.coredata.externalrecordswriter.plist
com.apple.coreservices.appleid.authentication.plist
com.apple.coreservices.uiagent.plist
com.apple.csuseragent.plist
com.apple.cvmsCompAgent_i386.plist
com.apple.cvmsCompAgent_x86_64.plist
com.apple.distnoted.xpc.agent.plist
com.apple.familycontrols.useragent.plist
com.apple.findmymacmessenger.plist
com.apple.fontd.useragent.plist
com.apple.gssd-agent.plist
com.apple.helpd.plist
com.apple.iCalPush.plist
com.apple.iChat.Theater.plist
com.apple.imagent.plist
com.apple.imklaunchagent.plist
com.apple.imtranscoderagent.plist
com.apple.imtransferagent.plist
```

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

AUTORUNS: LAUNCH AGENTS EXAMPLES



Key	Type	Value
▼ ProgramArguments	Array	(1 item)
Item 0	String	/System/Library/PrivateFrameworks/IMCore.framework/imagent.app/Contents/MacOS/imagent
▼ KeepAlive	Diction…	(1 item)
SuccessfulExit	Boolean	NO
Label	String	com.apple.imagent
▼ MachServices	Diction…	(1 item)
▼ com.apple.imagent.desktop.auth	Diction…	(1 item)
ResetAtClose	Boolean	YES
▼ EnvironmentVariables	Diction…	(1 item)
NSRunningFromLaunchd	String	1



Key	Type	Value
Label	String	org.openbsd.ssh-agent
▼ ProgramArguments	Array	(2 items)
Item 0	String	/usr/bin/ssh-agent
Item 1	String	-l
ServiceIPC	Boolean	YES
▼ Sockets	Diction…	(1 item)
▼ Listeners	Diction…	(1 item)
SecureSocketWithKey	String	SSH_AUTH_SOCK
EnableTransactions	Boolean	YES

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

AUTORUNS: LAUNCH DAEMONS

- Daemon – Background System Process
- Location:
  - /System/Library/LaunchDaemons
  - /Library/LaunchDaemons

AUTORUNS: LAUNCH DAEMONS EXAMPLE

```
Fri Apr 13 03:15:00 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 Capac
/dev/disk1                         698Gi  431Gi  267Gi    62
localhost:/YNU-3NIWZFYxg8rbEqggLJ  698Gi  698Gi    0Bi   100

Network interface status:
Name  Mtu   Network       Address            Ipkts Ierrs     
lo0   16384 <Link#1>                        38376     0     
lo0   16384 localhost   fe80:1::1          38376     -     
lo0   16384 127           localhost        38376     -    38376     -     -
lo0   16384 ip6-localho ::1                38376     -    38376     -     -
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 37611065     0 105742931     0     0
en1   1500  bit.local   fe80:5::9227:e4ff 37611065     - 105742931     -     -
en1   1500  192.168.1     bit              37611065     - 105742931     -     -
fw0   4078  <Link#6>    e8:06:88:ff:fe:d5:5d:08        0     0        0     0     0
p2p0  2304  <Link#7>    02:27:e4:f8:e6:5f      0     0        0     0     0
vmnet 1500  <Link#8>    00:50:56:c0:00:01      0     0        0     0     0
vmnet 1500  172.16.73/24  172.16.73.1          0     -        0     -     -
vmnet 1500  <Link#9>    00:50:56:c0:00:08      0     0        0     0     0
vmnet 1500  192.168.158   192.168.158.1        0     -        0     -     -

Local system status:
 3:15  up 3 days,  8:06, 4 users, load averages: 0.55 0.57 0.56

-- End of daily output --
```

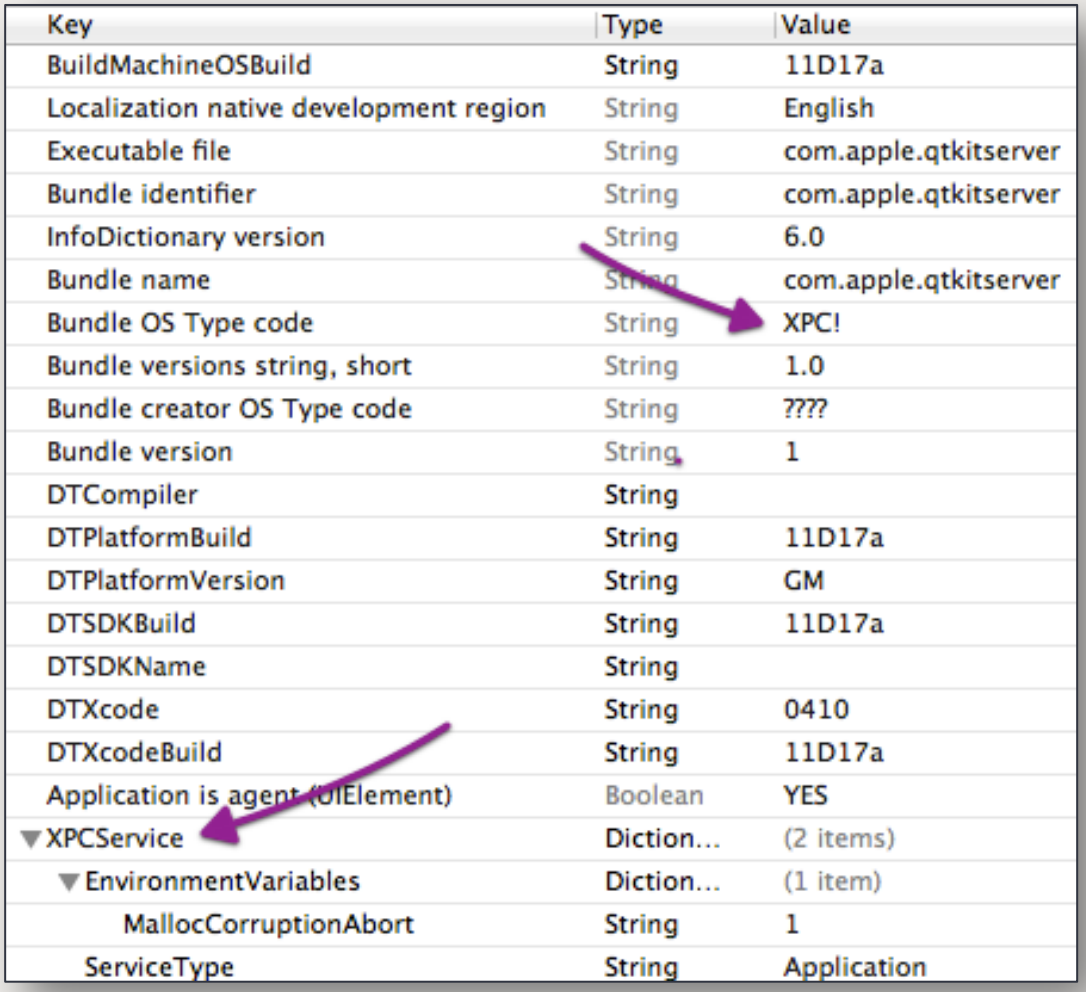
Key	Type	Value
Label	String	com.apple.periodic-daily
▼ ProgramArguments	Array	(2 items)
Item 0	String	/usr/sbin/periodic
Item 1	String	daily
LowPriorityIO	Boolean	YES
Nice	Number	1
▼ StartCalendarInterval	Diction...	(2 items)
Hour	Number	3
Minute	Number	15
AbandonProcessGroup	Boolean	YES

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

AUTORUNS: XPC SERVICES

- Privilege Separation & Stability
- Sandboxed Environment
- Runs in user context
- Services a single application
- Location:
  - Application Bundle: /Contents/XPCServices/
  - /System/Library/XPCServices/

AUTORUNS: XPC SERVICES EXAMPLE



Key	Type	Value
BuildMachineOSBuild	String	11D17a
Localization native development region	String	English
Executable file	String	com.apple.qtkitserver
Bundle identifier	String	com.apple.qtkitserver
InfoDictionary version	String	6.0
Bundle name	String	com.apple.qtkitserver
Bundle OS Type code	String	XPC!
Bundle versions string, short	String	1.0
Bundle creator OS Type code	String	????
Bundle version	String	1
DTCompiler	String	
DTPlatformBuild	String	11D17a
DTPlatformVersion	String	GM
DTSDKBuild	String	11D17a
DTSDKName	String	
DTXcode	String	0410
DTXcodeBuild	String	11D17a
Application is agent (UIElement)	Boolean	YES
▼ XPCService	Diction…	(2 items)
▼ EnvironmentVariables	Diction…	(1 item)
MallocCorruptionAbort	String	1
ServiceType	String	Application

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

AUTORUNS: MALWARE EXAMPLES

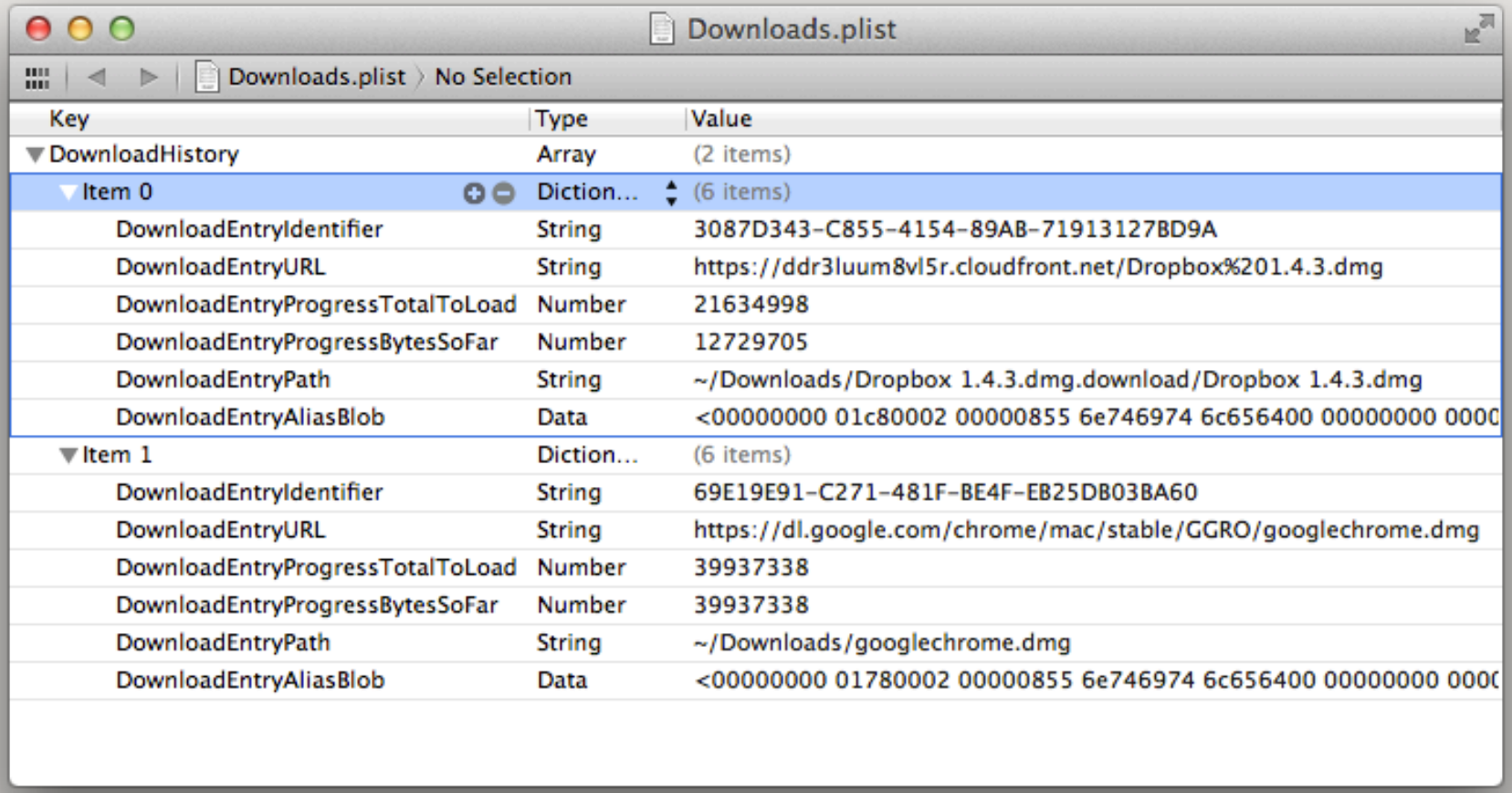
Flashback	• ~/Library/LaunchAgents/com.java.update.plist • References .jupdate in user's home directory.
CoinThief	• ~/Library/LaunchAgents/ com.google.softwareUpdateAgent.plist • References like-named executable in same directory.
KitM	• Login Item to start macs.app Application
Crisis	• With Admin Privileges… • /System/Library/Frameworks/Foundation.framework/ XPCServices/com.apple.mdworker_server.xpc
Janicab	• Entry in Crontab for runner.pyc

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

INTERNET HISTORY

INTERNET HISTORY: SAFARI - DOWNLOADS

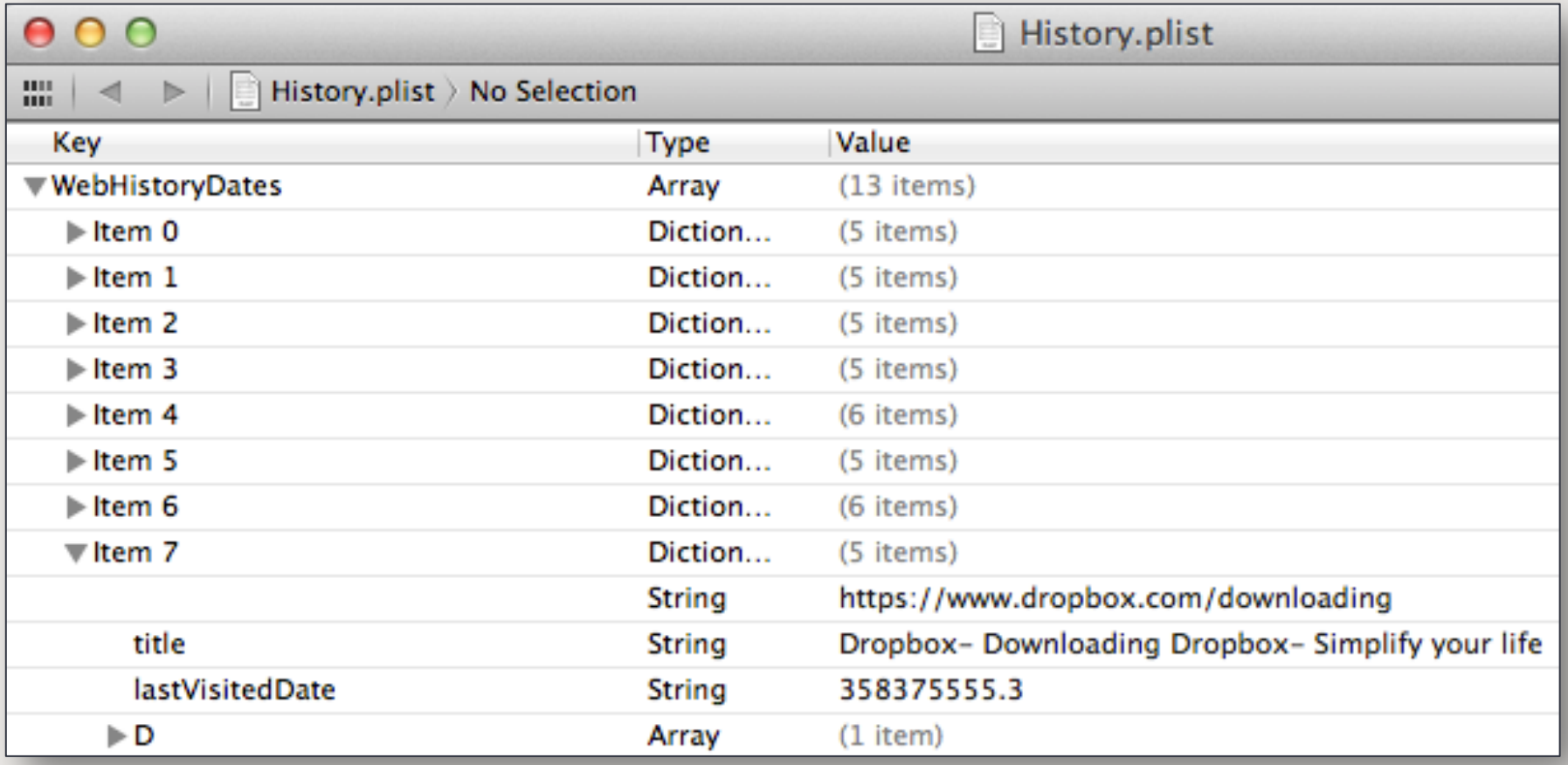
- ~/Library/Safari/Downloads.plist



Key	Type	Value
▼DownloadHistory	Array	(2 items)
▼Item 0	Diction…	(6 items)
DownloadEntryIdentifier	String	3087D343-C855-4154-89AB-71913127BD9A
DownloadEntryURL	String	https://ddr3luum8vl5r.cloudfront.net/Dropbox%201.4.3.dmg
DownloadEntryProgressTotalToLoad	Number	21634998
DownloadEntryProgressBytesSoFar	Number	12729705
DownloadEntryPath	String	~/Downloads/Dropbox 1.4.3.dmg.download/Dropbox 1.4.3.dmg
DownloadEntryAliasBlob	Data	<00000000 01c80002 00000855 6e746974 6c656400 00000000 0000
▼Item 1	Diction…	(6 items)
DownloadEntryIdentifier	String	69E19E91-C271-481F-BE4F-EB25DB03BA60
DownloadEntryURL	String	https://dl.google.com/chrome/mac/stable/GGRO/googlechrome.dmg
DownloadEntryProgressTotalToLoad	Number	39937338
DownloadEntryProgressBytesSoFar	Number	39937338
DownloadEntryPath	String	~/Downloads/googlechrome.dmg
DownloadEntryAliasBlob	Data	<00000000 01780002 00000855 6e746974 6c656400 00000000 0000

INTERNET HISTORY: SAFARI - HISTORY

- ~/Library/Safari/History.plist

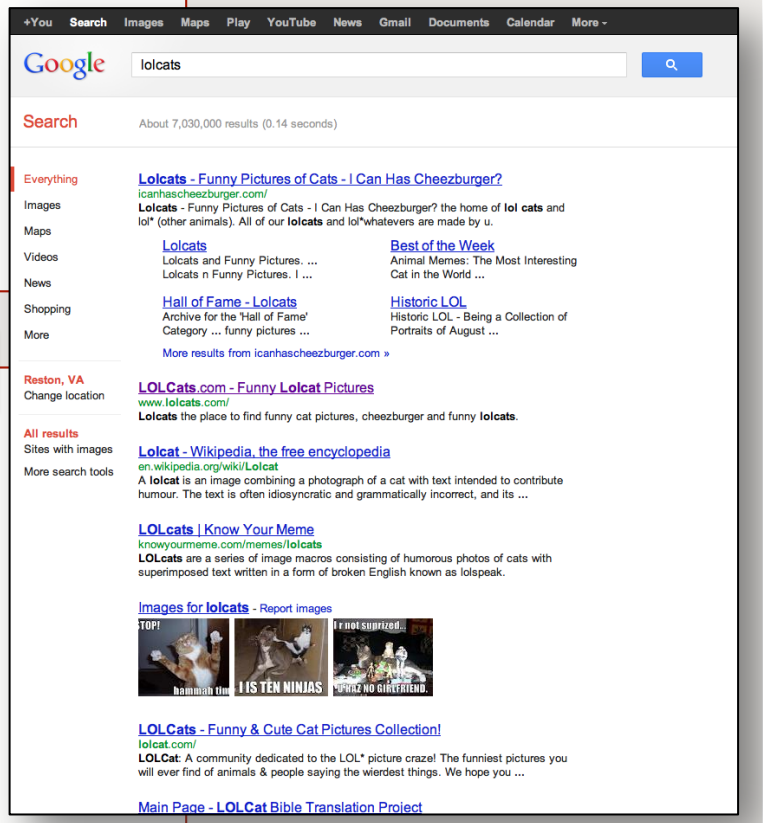


oompa@csh.rit.edu | @iamevltwin | mac4n6.com

INTERNET HISTORY: SAFARI - CACHE

~/Library/Caches/com.apple.Safari/Webpage Previews/

- Directory containing JPEG & PNG images of webpages.
- May be used to see a webpage taken from a snapshot in time.



~/Library/Caches/com.apple.Safari/Cache.db

- SQLite Database
- Download Cache Files
- Originating Location
- Download Date
- May contain evidence of:
  - Malicious code, redirects, phishing, etc.

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

TEMPORARY & CACHE DIRECTORIES

TEMP & CACHE DIRECTORIES: /TMP, JAVA TEMP & CACHE

- /tmp & /var/tmp
- /Users/<user>/Library/Caches/Java/tmp
- /Users/<user>/Library/Caches/Java/cache
  - IDX, JAR Files
  - Open Cache in /Applications/Utilities/Java Preferences.app

BRIAN BASKIN'S (@BBASKIN) IDX PARSER

- https://github.com/Rurik/Java_IDX_Parser
- Windows Executable
- or…
- Python Script!

```
nibble:CEIC2013 sledwards$ python idx_parser.py 68b1b3cd-5249d485.idx
Java IDX Parser -- version 1.3 -- by @bbaskin

IDX file: 68b1b3cd-5249d485.idx (IDX File Version 6.03)

[*] Section 2 (Download History) found:
URL: http://192.168.1.134/adobe.jar
IP: 192.168.1.134
<null>: HTTP/1.1 200 OK
content-length: 1124562
last-modified: Fri, 07 Dec 2012 05:21:22 GMT
content-type: application/java-archive
date: Wed, 06 Mar 2013 21:23:11 GMT
server: Apache/2.2.22 (Unix) DAV/2 mod_ssl/2.2.22 OpenSSL/0.9.8r
deploy-request-content-type: application/x-java-archive

[*] Section 3 (Jar Manifest) found:
Manifest-Version: 1.0
Created-By: 1.6.0_24 (Sun Microsystems Inc.)

Name: WebEnhancer.class
SHA1-Digest: 55gPOWmd1lIgDYdOF2EXCTPRpyU=

Name: mac
SHA1-Digest: fvpEryer0UCRvrcUIOyvQTWj4Vs=

Name: win
SHA1-Digest: f6fErxOtG88SsYClqc8kYTSFYIw=
```

TEMP & CACHE FILES: EXAMPLES

Flashback

- Mach-O Binary – /tmp/.sysenter
- Java Cache Files
  - rh-3.jar
  - cl-3.jar

Imuler

- /tmp/.mdworker
- /tmp/CurlUpload

MacControl

- /tmp/launch-hs – Bash Script
- /tmp/launch-hse - Malware
- /tmp/file.doc – Decoy Word Doc

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

EMAIL

EMAIL:
APPLE MAIL

- ~/Library/Mail/V2/MailData/
  - Accounts.plist – Mail Account Information

Key	Type	Value
AccountsVersion	Number	6
▶ DeliveryAccounts	Array	(2 items)
▼ MailAccounts	Array	(4 items)
▶ Item 0	Diction…	(8 items)
▼ Item 1	Diction…	(25 items)
AccountName	String	CSH
AccountPath	String	~/Library/Mail/V2/IMAP-oompa@mail.csh.rit.edu
AccountType	String	IMAPAccount

EMAIL: APPLE MAIL

- Directories for each email account.
  - Nested messages and attachment directories.
  - File Types: mbox & emlx
- Mailboxes
  - ~/Library/Mail/V2/

```
Attachments//435/1.2:
total 32
drwxr-xr-x  3 oompa  staff    102 May 10 16:55 .
drwxr-xr-x  5 oompa  staff    170 May 10 16:55 ..
-rw-r--r--@ 1 oompa  staff  13524 May 10 16:55 image001.jpg

Attachments//435/1.3:
total 32
drwxr-xr-x  3 oompa  staff    102 May 10 16:55 .
drwxr-xr-x  5 oompa  staff    170 May 10 16:55 ..
-rw-r--r--@ 1 oompa  staff  15868 May 10 16:55 image002.png
```

```
bit:Data oompa$ pwd
/Users/oompa/Library/Mail/V2/IMAP-oompa@mail.csh.rit.edu/INBOX.mbox/0223CBB8-8F52-487D-9F90-C87F2F6701C4/Data
bit:Data oompa$ ls -la
total 16
drwx------   11 oompa  staff    374 May 17 21:37 .
drwx------    4 oompa  staff    136 May 17 21:37 ..
-rw-r--r--@   1 oompa  staff   6148 May 17 21:38 .DS_Store
drwx------    3 oompa  staff    102 May 10 19:36 0
drwx------    5 oompa  staff    170 May 22 21:07 1
drwx------    4 oompa  staff    136 May 10 16:55 2
drwx------    4 oompa  staff    136 May 10 16:56 3
drwx------    4 oompa  staff    136 May 10 16:56 4
drwxr-xr-x    3 oompa  staff    102 May 10 17:10 6
drwxr-xr-x   54 oompa  staff   1836 May 17 21:37 Attachments
drwx------  990 oompa  staff  33660 May 28 14:46 Messages
```

EMAIL:
APPLE MAIL - ATTACHMENTS

"Saved"

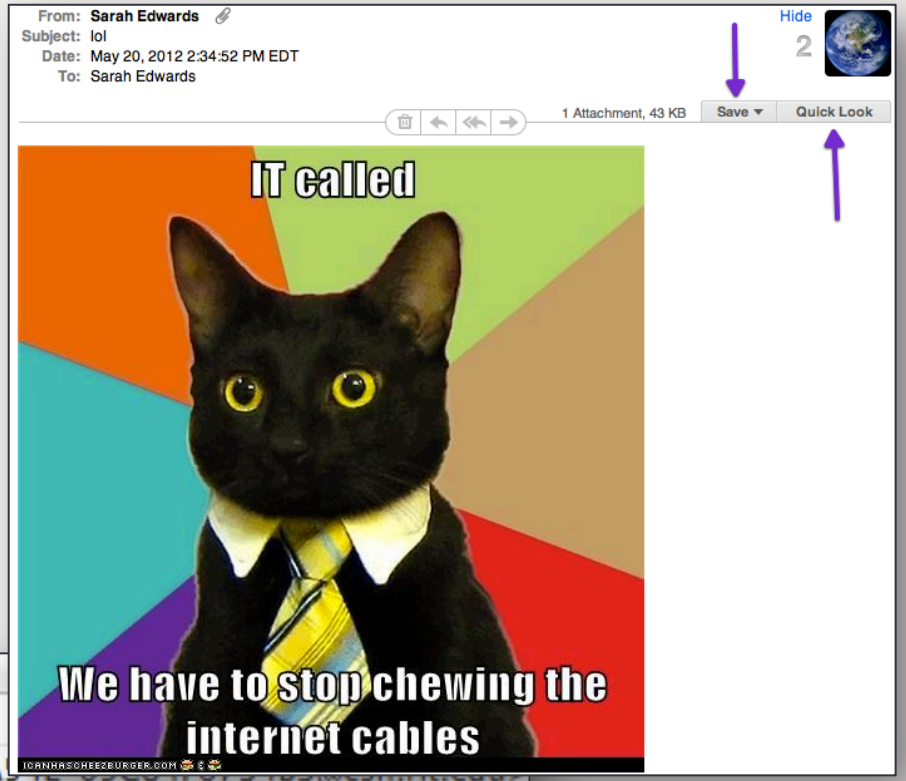
- ~/Downloads

"QuickLook"

- ~/Library/Mail Downloads/

Metadata (10.8-)

- ~/Library/Mail/V2/MailData/OpenedAttachments.plist or OpenedAttachmentsV2.plist



Key	Type	Value
▼ Item 0	Diction...	(5 items)
MessageID	String	<F86B9649-1F9A-4779-A
ModDate	Date	May 12, 2012 5:04:13 PM
OpenedDate	Date	May 12, 2012 5:04:13 PM
PartNumber	String	2
Path	String	/Users/oompa/Library/Mail Downloads/photo.JPG

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

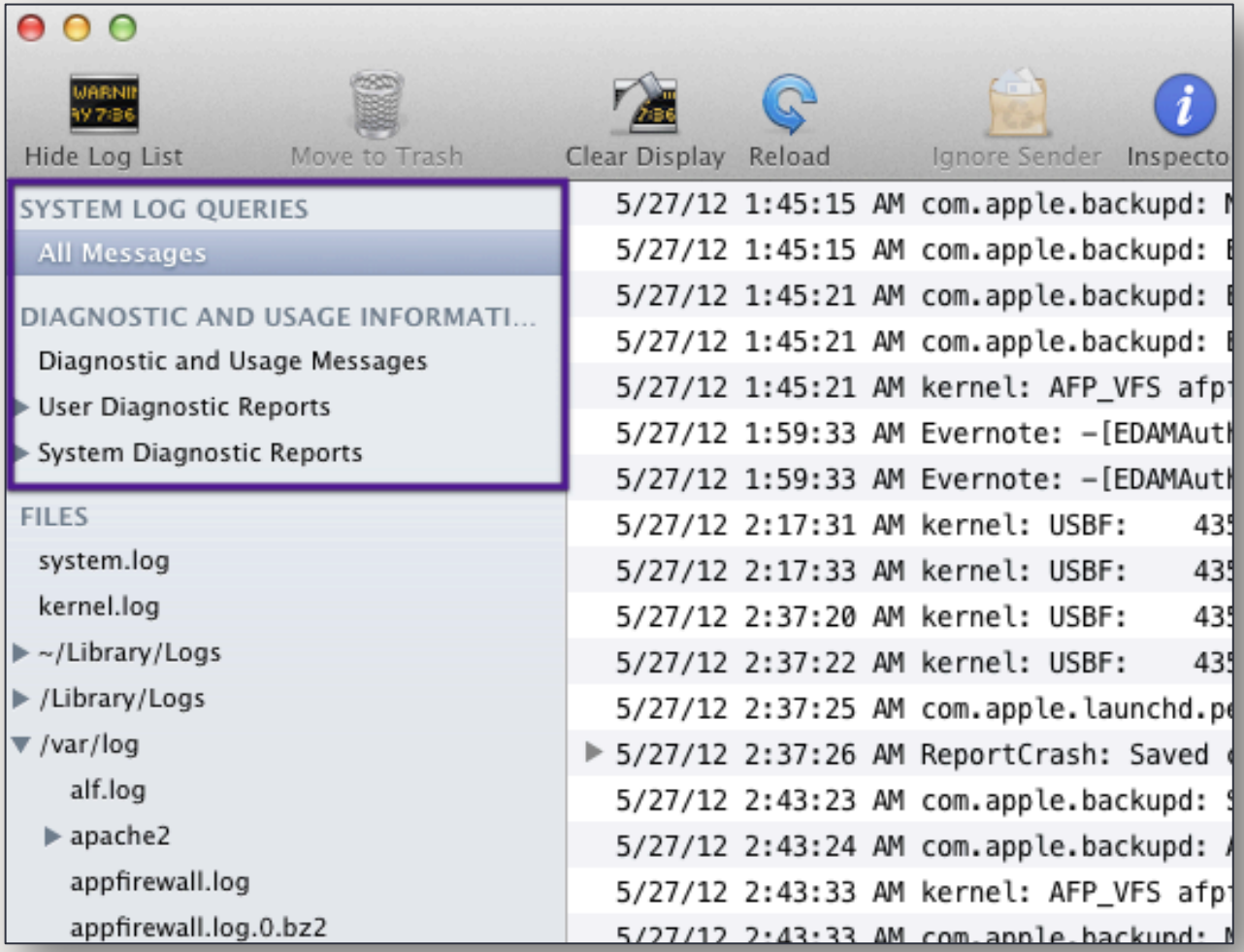
LOG ANALYSIS

LOG ANALYSIS: APPLE SYSTEM LOGS

- Location: /private/var/log/asl/ (>10.5.6)
- syslog “replacement”
- View using Console.app or `syslog` command
- Filename Format: YYYY.MM.DD.[UID].[GID].asl

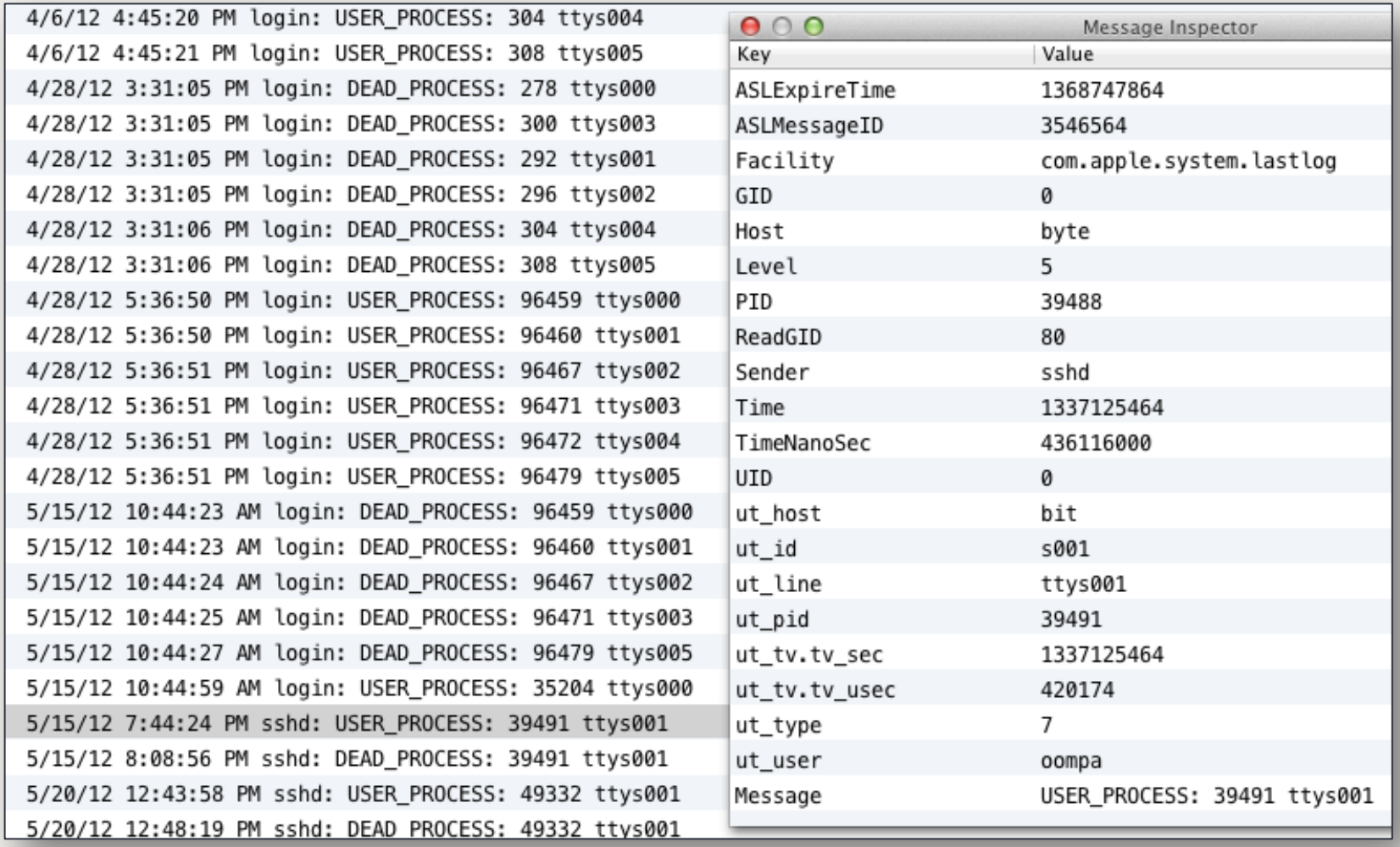
```
-rw-------+ 1 root  wheel  93522 May 22 23:45 2012.05.22.G80.asl
-rw-------+ 1 root  wheel   8696 May 22 23:45 2012.05.22.U0.G80.asl
-rw-------+ 1 root  wheel  24612 May 22 23:45 2012.05.22.U501.asl
-rw-------+ 1 root  wheel   3720 May 22 22:45 2012.05.22.U89.asl
-rw-------+ 1 root  wheel  87101 May 23 23:45 2012.05.23.G80.asl
-rw-------+ 1 root  wheel   9245 May 23 23:45 2012.05.23.U0.G80.asl
-rw-------  1 root  wheel    864 May 23 21:57 2012.05.23.U0.asl
-rw-------+ 1 root  wheel  18556 May 23 23:35 2012.05.23.U501.asl
-rw-------+ 1 root  wheel   5680 May 23 23:45 2012.05.23.U89.asl
-rw-------+ 1 root  wheel  92582 May 24 23:45 2012.05.24.G80.asl
-rw-------+ 1 root  wheel   9122 May 24 23:45 2012.05.24.U0.G80.asl
-rw-------+ 1 root  wheel  17707 May 24 23:28 2012.05.24.U501.asl
-rw-------+ 1 root  wheel   5680 May 24 23:45 2012.05.24.U89.asl
-rw-------+ 1 root  wheel  92416 May 25 23:45 2012.05.25.G80.asl
```

LOG ANALYSIS: CONSOLE.APP



oompa@csh.rit.edu | @iamevltwin | mac4n6.com

LOG ANALYSIS: CONSOLE.APP



oompa@csh.rit.edu | @iamevltwin | mac4n6.com

LOG ANALYSIS: SYSLOG COMMAND

- `syslog –d asl/`

```
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
```

LOG ANALYSIS:
syslog –T utc –F raw –d /asl

- [ASLMessageID 3555356]
- [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]

LOG ANALYSIS: AUDIT LOGS

- Location: /private/var/audit/
- BSM Audit Logs
- StartTime.EndTime
- YYYYMMDDHHMMSS.YYYYMMDDHHMMSS

```
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
```

LOG ANALYSIS:
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>
```

LOG ANALYSIS:
USER LOGINS & LOGOUTS - /VAR/LOG/SYSTEM.LOG

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
```

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
```

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
```

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

LOG ANALYSIS:
PRIVILEGE ESCALATION - /VAR/LOG/SYSTEM.LOG

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

LOG ANALYSIS: 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

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

LOG ANALYSIS: /VAR/LOG/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
-----
```

VOLUME ANALYSIS

VOLUME ANALYSIS: SYSTEM.LOG & DAILY.LOG

```
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
```

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

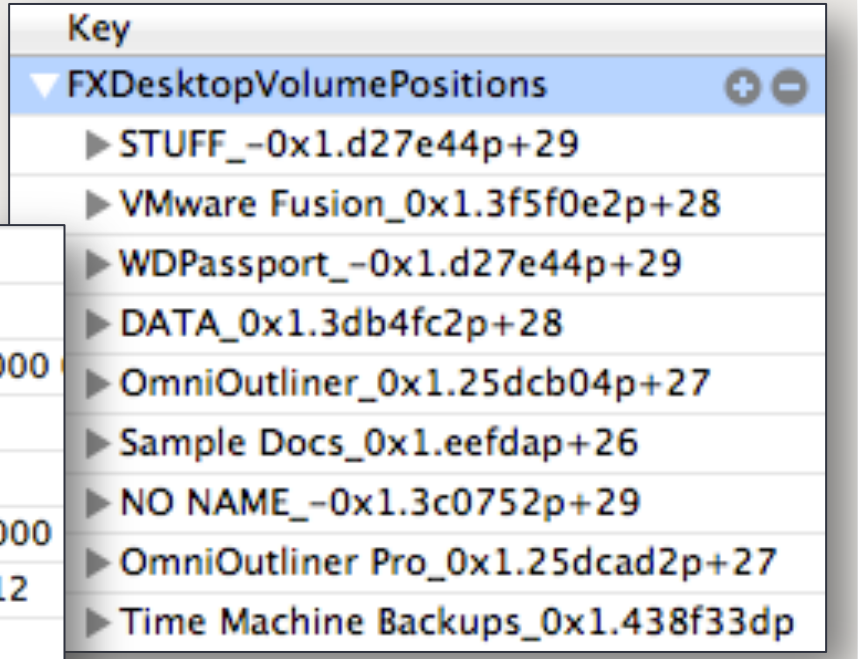
VOLUME ANALYSIS: KERNEL.LOG (10.8+ - SYSTEM.LOG)

- Search for “USBMSC”
- Serial Number, Vendor ID, Product ID, Version

```
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
```

VOLUME ANALYSIS:
~/LIBRARY/PREFERENCES/COM.APPLE.FINDER.PLIST

- FXDesktopVolumePositions
- FXRecentFolders (10 most recent)



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

oompa@csh.rit.edu | @iamevltwin | mac4n6.com

ANTIVIRUS

ANTIVIRUS: FILE QUARANTINE

- Introduced in 10.5
- Quarantines downloaded files
- Applications (Browsers, Email, etc)
- Weaknesses
  - Files on USB drives
  - Applications that do not implement File Quarantine

ANTIVIRUS:
FILE QUARANTINE EVENTS DATABASE

10.7+

- ~/Library/Preferences/
  com.apple.LaunchServices.QuarantineEvents.V2

10.6

- ~/Library/Preferences/
  com.apple.LaunchServices.QuarantineEvents

ANTIVIRUS: FILE QUARANTINE

- Quarantine Events – LSQuarantineEvent Table

Key	Example Data
LSQuarantineEventIdentifier	68F08939-EF7F-4326-BDA3-810542E43579
LSQuarantineTimeStamp	358820762.0
LSQuarantineAgentBundleIdentifier	com.google.Chrome
LSQuarantineAgentName	Google Chrome
LSQuarantineDataURLString	http://ash.barebones.com/TextWrangler_4.0.dmg
LSQuarantineSenderName	*NULL*
LSQuarantineSenderAddress	*NULL*
LSQuarantineTypeNumber	0
LSQuarantineOriginTitle	*NULL*
LSQuarantineOriginURLString	http://www.barebones.com/products/textwrangler/
LSQuarantineOriginAlias	*NULL*

ANTIVIRUS: EXTENDED ATTRIBUTES

- Command: `xattr`
- Quarantine
- Metadata:
  - kMDItemWhereFroms
- Disk Images
- FinderInfo
- TextEncoding
- Preview UI State
- Resource Fork
- DropBox
- Etc.

```
bit:Downloads oompa$ xattr -xl TextWrangler_4.0.dmg
com.apple.diskimages.fsck:
00000000  A1 52 D4 F1 FC 10 76 E8 A6 EB E3 EB 73 3F 8F A1  |.R....v.....s?..|
00000010  46 83 68 3C                                      |F.h<|
00000014
com.apple.diskimages.recentcksum:
00000000  69 3A 31 34 39 33 37 34 39 20 6F 6E 20 33 39 38  |i:1493749 on 398|
00000010  31 45 32 45 36 2D 30 43 41 43 2D 33 41 33 45 2D  |1E2E6-0CAC-3A3E-|
00000020  42 45 31 44 2D 39 30 44 35 38 33 46 38 39 41 35  |BE1D-90D583F89A5|
00000030  44 20 40 20 31 33 33 37 31 32 37 39 36 34 20 2D  |D @ 1337127964 -|
00000040  20 43 52 43 33 32 3A 24 45 36 41 31 34 31 31 34  | CRC32:$E6A14114|
00000050
com.apple.metadata:kMDItemWhereFroms:
00000000  62 70 6C 69 73 74 30 30 A2 01 02 5F 10 2D 68 74  |bplist00..._.-ht|
00000010  74 70 3A 2F 2F 61 73 68 2E 62 61 72 65 62 6F 6E  |tp://ash.barebon|
00000020  65 73 2E 63 6F 6D 2F 54 65 78 74 57 72 61 6E 67  |es.com/TextWrang|
00000030  6C 65 72 5F 34 2E 30 2E 64 6D 67 5F 10 2F 68 74  |ler_4.0.dmg_./ht|
00000040  74 70 3A 2F 2F 77 77 77 2E 62 61 72 65 62 6F 6E  |tp://www.barebon|
00000050  65 73 2E 63 6F 6D 2F 70 72 6F 64 75 63 74 73 2F  |es.com/products/|
00000060  74 65 78 74 77 72 61 6E 67 6C 65 72 2F 08 0B 3B  |textwrangler/..;|
00000070  00 00 00 00 00 00 01 01 00 00 00 00 00 00 00 03  |................|
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6D  |...............m|
00000090
com.apple.quarantine:
00000000  30 30 30 31 3B 34 66 62 32 66 34 31 64 3B 47 6F  |0001;4fb2f41d;Go|
00000010  6F 67 6C 65 20 43 68 72 6F 6D 65 3B 36 38 46 30  |ogle Chrome;68F0|
                                                          |8939-EF7F-4326-B|
                                                          |DA3-810542E43579|
                                                          ||com.google.Chro|
                                                          |me|
00000052
```

```
-rw-r--r--@  1 oompa  staff   18041097 May 11 20:01 Rdio.dmg
-rw-r--r--@  1 oompa  staff    5416932 May 15 20:26 TextWrangler_4.0.dmg
-rw-r--r--@  1 oompa  staff  188900306 May 11 19:22 VMware-Fusion-4.1.2-683185-light.dmg
-rw-r--r--@  1 oompa  staff   39937338 Apr 30 15:30 googlechrome.dmg
```

oompa@csh.rit.edu | @iamevltwin

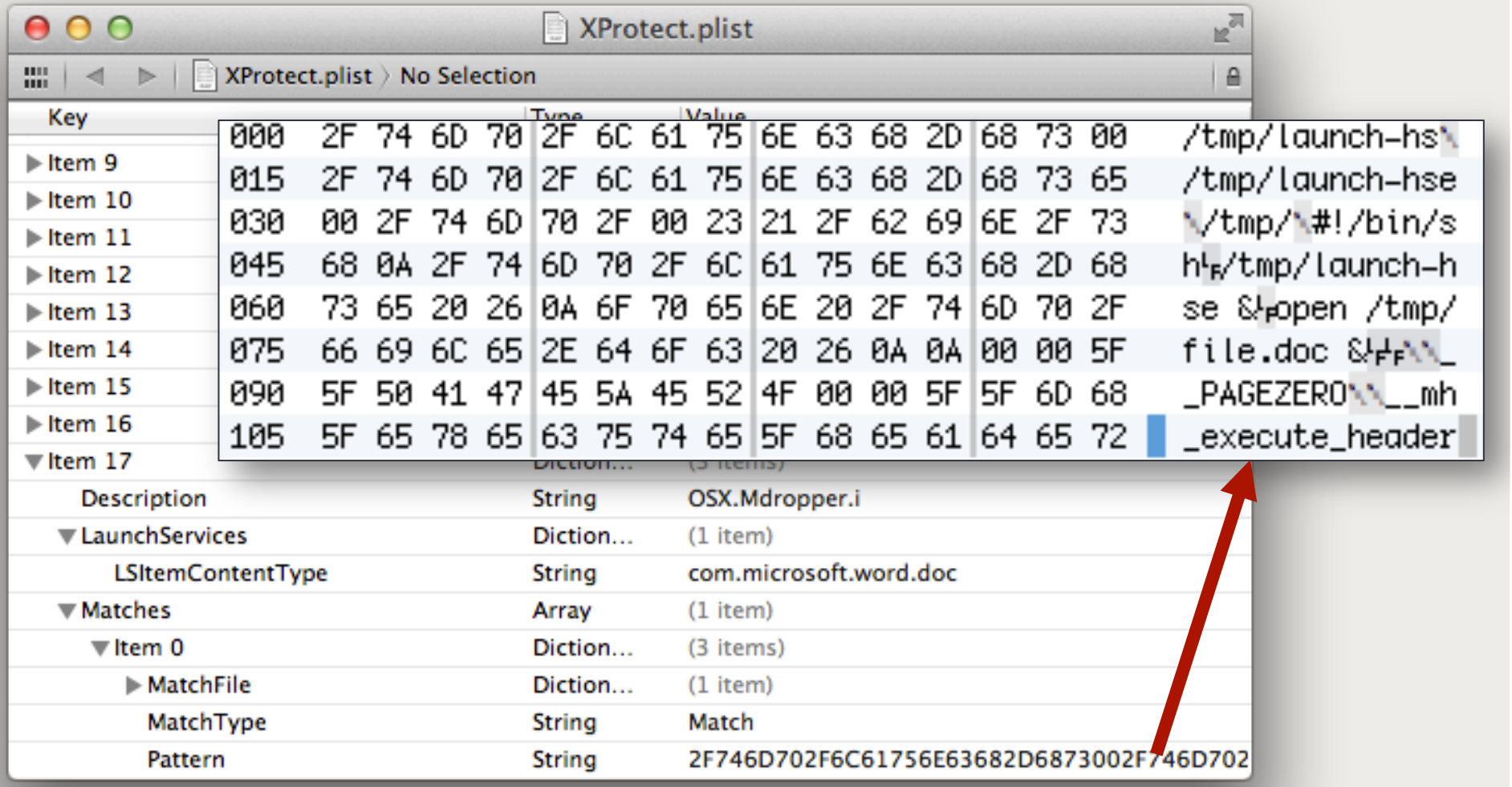
ANTIVIRUS: EXTENDED ATTRIBUTES

com.apple.quarantine	Related Key in QuarantineEvents Database
4fb2f41d	LSQuarantineTimeStamp
Google Chrome	LSQuarantineAgentName
68F08939-EF7F-4326-BDA3-810542E43579	LSQuarantineEventIdentifier
com.google.Chrome	LSQuarantineAgentBundleIdentifier
com.apple.metadata:kMDItemWhereFroms	
http://ash.barebones.com/TextWrangler_4.0.dmg	LSQuarantineDataURLString
http://www.barebones.com/products/textwrangler/	LSQuarantineOriginURLString

ANTIVIRUS: XPROTECT

- /System/Library/CoreServices/CoreTypes.bundle/Contents/Resources
  - XProtect.meta.plist
    - Last Update Date & Version
  - XProtect.plist
    - AV Signatures
- Weaknesses
  - Apple updates it, sometimes.
  - Very few signatures on blacklist
  - No Heuristics
  - Only checks “quarantined” files

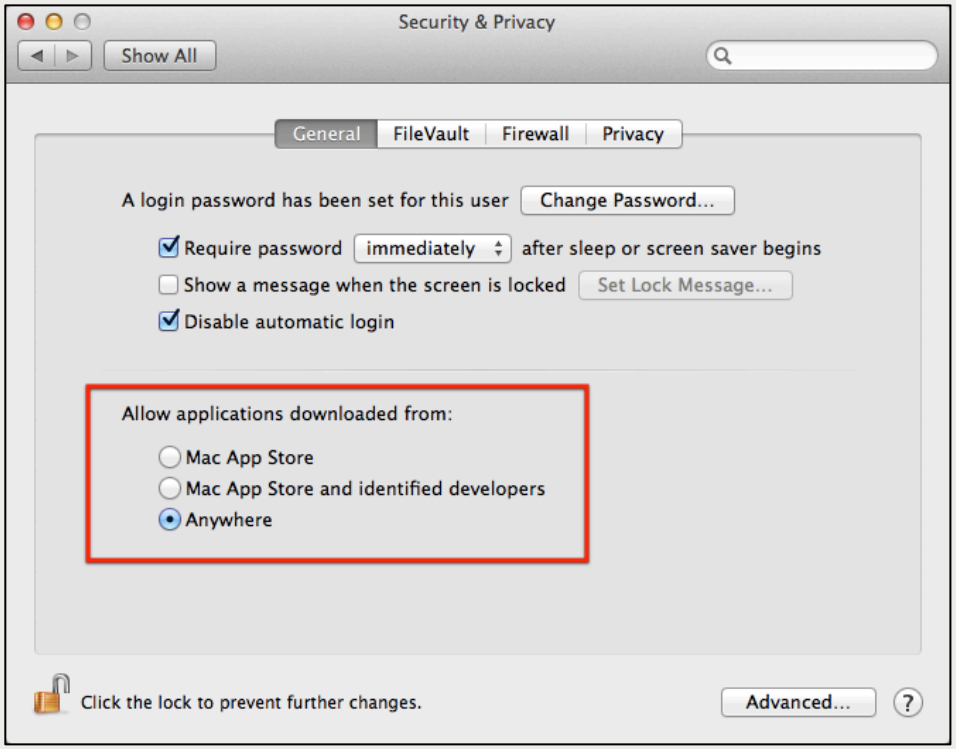
ANTIVIRUS: XPROTECT



oompa@csh.rit.edu | @iamevltwin | mac4n6.com

ANTIVIRUS: GATEKEEPER

- Introduced in 10.7.5
- Security Settings
  - Mac App Store
    - Users can only run apps from the store.
  - Mac App Store & Identified Developers
    - Default Setting
    - Users can only run software signed using Apple Developer ID
  - Anywhere
    - Users can run anything from anywhere



oompa@csh.rit.edu | @iamevltwin | mac4n6.com

OTHER FILES

OTHER FILES: KERNEL EXTENSIONS

- Dynamically loaded executable code in kernel space
  - Low Level Device Drivers
  - Network Filters
  - File Systems
  - …keyloggers?

```
MBP:Extensions oompa$ pwd
/System/Library/Extensions
MBP:Extensions oompa$ ls -la | grep "logKext"
drwxr-xr-x    3 root  wheel   102 Nov 19  2009 logKext.kext
```

```
76    0 0xffffff7f81340000 0xa000     0xa000     com.apple.driver.AppleMCCSControl (1.0.24) <55 9 7 5 4 3 1>
77    0 0xffffff7f81214000 0x5000     0x5000     com.apple.driver.AppleUpstreamUserClient (3.5.9) <55 9 8 7 5 4 3 1>
78    1 0xffffff7f813e5000 0xa4000    0xa4000    com.apple.driver.DspFuncLib (2.1.1f12) <67 66 5 4 3 1>
79    0 0xffffff7f81489000 0xaf000    0xaf000    com.apple.driver.AppleHDA (2.1.1f12) <78 67 65 64 57 55 6 5 4 3 1>
81    1 0xffffff7f80f67000 0x5000     0x5000     com.apple.kext.triggers (1.0) <7 6 5 4 3 1>
82    0 0xffffff7f80f6c000 0x9000     0x9000     com.apple.filesystems.autofs (3.0) <81 7 6 5 4 3 1>
83    0 0xffffff7f81631000 0x5000     0x5000     com.vmware.kext.vmmemctl (0068.29.96) <7 5 4 3 1>
85    0 0xffffff7f81637000 0xa000     0xa000     com.vmware.kext.vmhgfs (0068.29.96) <5 4 3 1>
88    0 0xffffff7f80802000 0x4000     0x4000     com.fsb.kext.logKext (2.3) <25 4 3>
```

OTHER FILES: BASH HISTORY

- ~/.bash_history
- File not written until session logout
  - Each terminal window is a login session
- 500 Entries by default
- Incident Response Tip:
  - Run the ‘history’ command for the logged in user.

WHEN MACS GET HACKED

Sarah Edwards
@iamevltwin
oompa@csh.rit.edu
mac4n6.com