README

How to quickly detect recent activities on your Mac OS X system? How to detect if someone attempted or succeeded to get an access to your Mac let in your hotel room during your dinner or party?

Just by analysing the system logs and files access dates with bash commands
(like grep, find, ls, stat, awk, etc.)

For example, to identify opened emails on July 8 from 8 am to 8:59 am:

*grep /Users/sudoman/Library/Mail/V2/IMAP-yyyy\@xxxx.domain.fr/INBOX.mbox/ -type f -name *.emlx -exec stat -f '%Sa %N' '{}' + |grep -i 'Jul 8 08:'|grep 2013*

Or to identify attempts to unlock session without success on July 8:
grep -i -B 9 'The authtok is incorrect.' /var/log/system.log|grep-i 'Jul 8'|grep 'Got user'|awk '{print$1,$2,$3,$9,$10}'

You can find a lot of others fun tricks commands here:
https://code.google.com/p/mac-security-tips/wiki/ALL_THE_TIPS

Proof of Concept in Python, ***CheckOut4Mac*** *[https://code.google.com/p/checkout4mac]*, has been developed in order to automate the search and identify malicious activities from 3 questions:
[1] When did you leave your hotel room? *eg: 22/6*
[2] At what time did you leave your hotel room? *eg: 22*
[3] How long did you leave your hotel room? *eg: 2*

CheckOut4Mac checks the following events for a specific date and/or specific hour:

[1]STARTUP ACTIVITIES
  [a]Startup dates
  [b]Stopping dates
  [c]Hibernation dates
  [d]Out of hibernation dates

[2]SESSION ACTIVITIES
  [a]Locked session dates
  [b]Attempt to unlock session without success
  [c]Unlocked session with success

[3]PHYSICAL CONNECTION ACTIVITIES
  [a]USB connections (last loading dates of USB extensions)
  [b]USB plugged devices
  [c]File system events (USB, mounting, etc.)
  [d]Firewire connections with another machine or storage media (last loading dates of Firewire extensions)
  [e]Firewire connections with another machine or storage media (activation of 'fw' interface)
  [f]Firewire connections to dump RAM (last loading dates of extensions IOFireWireSBP2/iPodDriver) just a supposition

[4]ESCALATION PRIVILEGES ACTIVITIES
  [a]Opened/Closed TTY terminals
  [b]ROOT commands executed with success
  [c]Attempt to execute commands with SUDO without success
  [d]User, password modification and creation

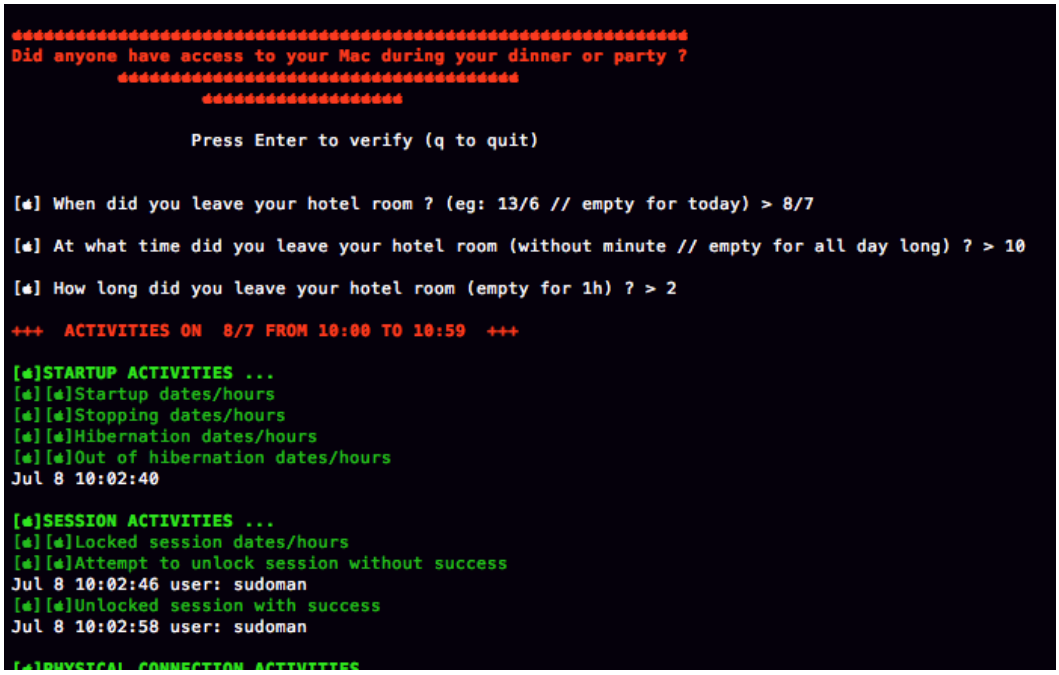
[5]APPLICATIONS ACTIVITIES
  [a]Opened applications (last access dates) => *not always with success (I search another solution)*

[6]FILES ACTIVITIES
  [a]Modified files (like autorun App, LaunchAgents or LaunchDaemons)
  [b]Added files (like trojan or malware App)
  [c]Accessed files (like your secret files)
  [d]Accessed Mails (last access dates)

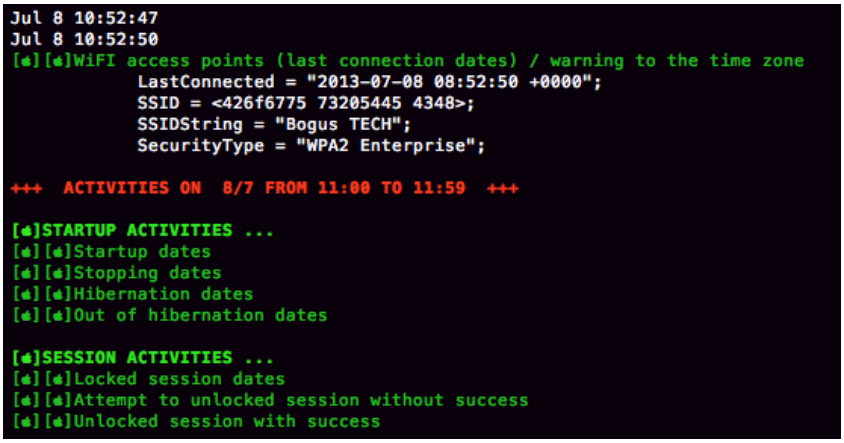
[7]NETWORK ACTIVITIES
  [a] Ethernet/WiFI connections (activation of 'enX' interface)
  [b] WiFI access points (last connection dates)

Features:
- Tested on Lion (10.7) and Mountain Lion (10.8)
- Analysis of current log files archive files (eg: /var/log/system.log, /var/log/system.log.7.bz2)
- Option -v allows to display launched commands
- Option -d allows to specify a date with format d/y or dd/yy without ask of the 3 questions
- Option -l, -s, -b allow to specify new log files path if you extract log manually

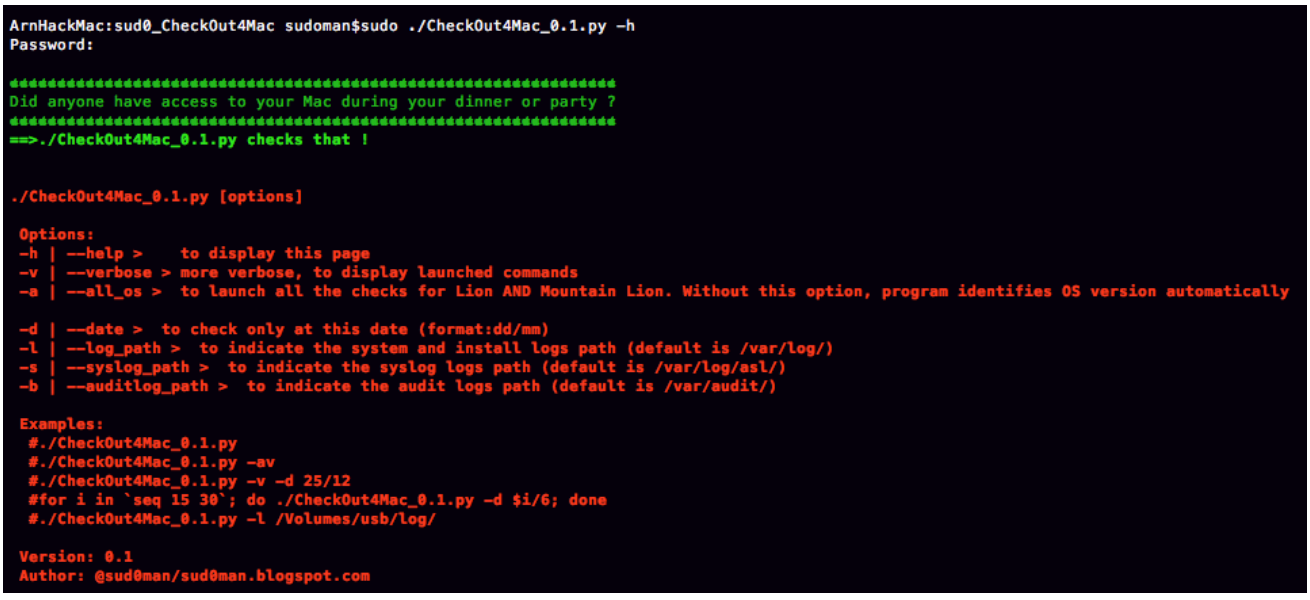
CheckOut4Mac launching and options:



First occurrence from 10:00 to 10:59



Second occurrence from 11:00 to 11:59



Before launching *CheckOut4Mac*:

```
##########################################
#PLEASE TO DEFINE USER VARIABLES TO DEFINE !!!
##########################################

# In first, you can disable controls just with comment #.
# All is into fct_all_dump() function.

# Secondly, you can custom a lot of dir and files

##########################################

#Check variables "path_grep", "path_egrep" and path_find into this file (search tag "to use your own grep, egrep and find" into the file")
# you can define your own grep, egrep and find for best performances (using of grep of gnu for example)

#timezone
timezone="utc+2"
#path where your applications are installed (.app)
path_applications = ["/Applications"]
maxdepth_find = "3"

#default log paths
var_log = "/var/log/"
path_to_syslog = "/var/log/asl/"
var_audit_log = "/var/audit/"

#define directories or files paths containing your secret informations (used to search if they have been read / do not use ~)
dir_secret_content=["/Users/sudoman","/tmp"]

#define dangerous directories or files paths if they have been modified (do not use ~)
dir_modify=["/Users/sudoman/Library/Preferences/com.apple.loginitems.plist","/etc/passwd","/Users/sudoman/Library/Caches"]

#define directories path wherein you want to check if files or directories have been added (do not use ~)
dir_add=["/System/Library/XPCServices/","/System/Library/LaunchAgents/","/Library/LaunchAgents/","/Users/sudoman/Library/LaunchAgents/","/Sy

#define paths containing your file in format .mbox (do not use ~)
path_to_mailbox=["/Users/sudoman/Library/Mail/V2/POP-test@pop.free.fr/INBOX.mbox/"]
#path_to_mailbox=["/Users/cilouze/Library/Mail/V2/IMAP-amalard\@mail.test.fr/"]
```

Please check paths and variables (into Check4Mac.py)

Limitations:

[1] Supported just “one” day by occurrence of *CheckOut4Mac*. If your search extends over several days, you have to re-launch one and/or several *CheckOut4Mac* occurrences. *CheckOut4Mac* detects this case and prints this message before continuing.

!! : Detection of analysis on several days, please launch an occurrence of CheckOut4Mac per day.
Press Enter to continue

If you want to launch *CheckOut4Mac* on several days, you can use the ‘for’ command:
 # for i in `seq 15 30`; do ./CheckOut4Mac_0.1.py -d $i/6; done

[2] Controls with tag “last access dates” between parentheses, use live files system and do not log files. So, warning to your interpretation if your system has been modified.

Screenshots:

```
+++  ACTIVITIES ON  8/7 FROM 00:00 TO 23:59  +++

[♦]STARTUP ACTIVITIES ...
[♦][♦]Startup dates/hours
[♦][♦]Stopping dates/hours
[♦][♦]Hibernation dates/hours
Jul 8 09:45:08
Jul 8 12:38:36
Jul 8 13:54:28
[♦][♦]Out of hibernation dates/hours
Jul 8 10:02:40
Jul 8 13:12:38
Jul 8 13:55:30

[♦]SESSION ACTIVITIES ...
[♦][♦]Locked session dates/hours
Jul 8 12:28:07
c[♦][♦]Attempt to unlock session without success
Jul 8 10:02:46 user: sudoman
^C[♦][♦]Unlocked session with success
Jul 8 10:02:58 user: sudoman
Jul 8 13:12:45 user: sudoman
```

Startup and session activities on July 8

```
Jul  8 14:13:25 ArnHackMac.local sudo[89143]:  sudoman : TTY=ttys010 ; PWD=/Users/sudoman/Dropbox/MAC_OS_X/sud0_CheckOut4Mac ; USER=root ; COMMAND=/usr/bin/syslog
8.G80.asl /var/log/asl/2013.07.08.U0.G80.asl /var/log/asl/2013.07.08.U0.asl /var/log/asl/2013.07.08.U205.asl /var/log/asl/2013.07.08.U503.asl
Jul  8 14:24:23 ArnHackMac.local sudo[91024]:  sudoman : 3 incorrect password attempts ; TTY=ttys001 ; PWD=/Users/sudoman ; USER=root ; COMMAND=/bin/bash
Jul  8 14:25:02 ArnHackMac.local sudo[91035]:  sudoman : TTY=ttys010 ; PWD=/Users/sudoman/Dropbox/MAC_OS_X/sud0_CheckOut4Mac ; USER=root ; COMMAND=/usr/bin/vim /va
Jul  8 14:25:38 ArnHackMac.local sudo[91046]:  sudoman : TTY=ttys010 ; PWD=/Users/sudoman/Dropbox/MAC_OS_X/sud0_CheckOut4Mac ; USER=root ; COMMAND=./CheckOut4Mac.p
Jul  8 14:28:56 ArnHackMac.local sudo[92213]:  sudoman : TTY=ttys010 ; PWD=/Users/sudoman/Dropbox/MAC_OS_X/sud0_CheckOut4Mac ; USER=root ; COMMAND=./CheckOut4Mac_0
[♦][♦]Attempt to execute commands with SUDO without success
Jul  8 14:24:23 ArnHackMac.local sudo[91024]:  sudoman : 3 incorrect password attempts ; TTY=ttys001 ; PWD=/Users/sudoman ; USER=root ; COMMAND=/bin/bash
[♦][♦]User, password modification and creation
```

Privileges escalation activities on July 8

```
[♦]NETWORK ACTIVITIES ...
[♦][♦]Network connections (based on DNS queries)
Jul 8 10:03:14
Jul 8 10:52:50
Jul 8 11:36:26
[♦][♦]Network disconnections (based on DNS queries)
Jul 8 10:02:41
Jul 8 10:52:15
Jul 8 11:36:07
[♦][♦]Ethernet connections (activation of 'en0' interface)
Jul 8 11:36:26
Jul 8 11:44:50
Jul 8 11:45:09
[♦][♦]WiFI connections (activation of 'en1' interface)
Jul 8 10:02:41
Jul 8 10:03:09
Jul 8 10:03:09
Jul 8 10:03:14
Jul 8 10:52:15
Jul 8 10:52:47
Jul 8 10:52:47
Jul 8 10:52:50
Jul 8 11:36:07
[♦][♦]WiFI access points (last connection dates) / warning to the time zone
            LastConnected = "2013-07-08 08:52:50 +0000";
            SSID = <426f6775 73205445 4348>;
            SSIDString = "Bogus TECH";
            SecurityType = "WPA2 Enterprise";
```

Network activities (Ethernet, WiFI, etc.) on July 8

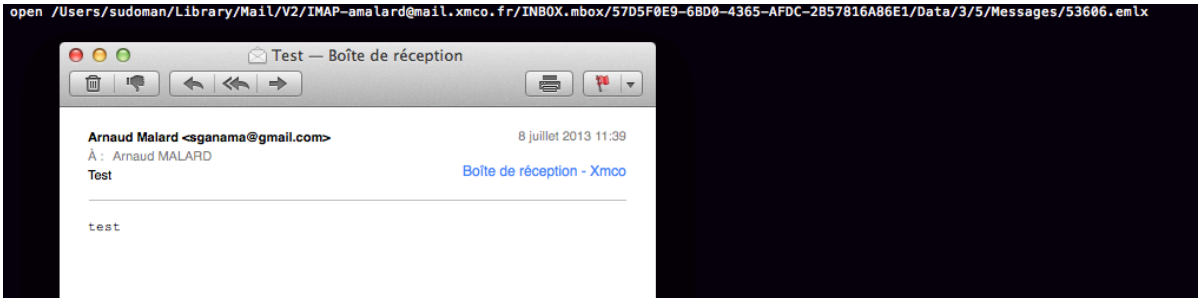
```
[♦]PHYSICAL CONNECTION ACTIVITIES ...
[♦][♦]USB connections (loaded USB extensions)
jul 8 10:03 IOUSBFamily.kext
jul 8 10:03 IOUSBMassStorageClass.kext
[♦][♦]USB plugged devices
Jul 8 10:03:15 => New plugged USB Device - USBMSC Identifier: 0x781(vendor) 0x5406(Device) - To identify the plugged device : external_bin/usb.ids

[♦][♦]File system events(USB, mounting, etc.)
Jul  8 10:03:16 ArnHackMac.local fseventsd[42]: check_vol_last_mod_time:XXX failed to get mount time (25; &mount_time == 0x109e12528)
Jul  8 10:03:16 ArnHackMac.local fseventsd[42]: log dir: /Volumes/RFID/.fseventsd getting new uuid: F70EE4EF-7A50-42EB-AF22-10BB6C86C0B3
Jul  8 10:03:16 ArnHackMac.local fseventsd[42]: disk logger: failed to open output file /Volumes/SoftDisk500/.fseventsd/fc0074742a62214a (No such f
entsd
Jul  8 10:03:16 ArnHackMac.local fseventsd[42]: failed to unlink old log file /Volumes/SoftDisk500/.fseventsd/fc0074742a62214a (No such file or dir
Jul  8 10:03:16 ArnHackMac.local fseventsd[42]: unmounting: failed to remove log dir /Volumes/SoftDisk500/.fseventsd (No such file or directory)
[♦][♦]Firewire connections with an other machine or storage media (loaded Firewire extensions)
jul 8 11:44 IOFireWireFamily.kext
jul 8 11:44 IOFireWireIP.kext
[♦][♦]Firewire connections with an other machine or storage media (activation of 'fw' interface)
Jul 8 11:44:50
[♦][♦]Firewire connections to dump RAM (loaded extensions IOFireWireSBP2/iPodDriver)
```

USB, Firewire activities on July 8

```
Jul  8 11:36:53 2013 /Users/sudoman/Pictures/screenshot/Capture d'écran 2013-07-08 à 11.39.50.png
[●][●]Accessed Mails (last access dates) / please to use command << open >> to read mbox files
Jul  8 11:07:47 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53380.partial.emlx
Jul  8 11:07:47 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53381.partial.emlx
Jul  8 11:36:43 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53405.emlx
Jul  8 11:07:47 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53419.emlx
Jul  8 11:07:47 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53429.emlx
Jul  8 11:08:58 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53547.emlx
Jul  8 11:35:18 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53550.emlx
Jul  8 11:08:48 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53551.emlx
Jul  8 11:09:00 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53566.emlx
Jul  8 11:39:06 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53567.emlx
Jul  8 11:39:02 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53578.emlx
Jul  8 11:08:38 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53588.emlx
Jul  8 11:39:06 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53592.emlx
Jul  8 11:40:53 2013 /Users/sudoman/Library/Mail/V2/IMAP-                INBOX.mbox/57D5F0E9-6BD0-4365-AFDC-2B57816A86E1/Data/3/5/Messages/53606.emlx
```

Accessed emails on July 8



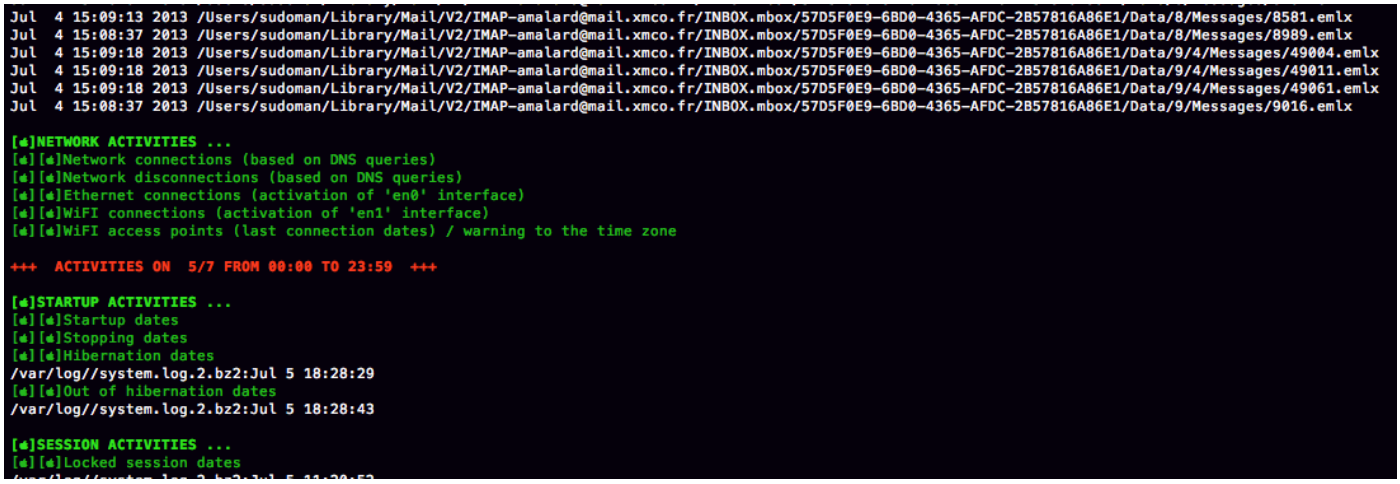
Opening of the selected email (with 'open' command)

```
[●]FILES ACTIVITIES ...
[●][●]Modified files (like autorun App, LaunchAgents or LaunchDaemons)
Jul  8 14:17:10 2013 /Users/sudoman/Library/Preferences/com.apple.loginitems.plist
[●][●]Added files (like trojan or malware App)
[●][●]Accessed files (like your secret files)
Jul  8 14:10:36 2013 /Users/sudoman/.bash_history
Jul  8 14:10:36 2013 /Users/sudoman/.bash_profile
Jul  8 14:28:25 2013 /Users/sudoman/.CFUserTextEncoding
Jul  8 14:28:11 2013 /Users/sudoman/.cups/lpoptions
Jul  8 14:13:49 2013 /Users/sudoman/.dropbox/aggregation.dbx
Jul  8 14:29:02 2013 /Users/sudoman/.dropbox/config.dbx
Jul  8 00:36:21 2013 /Users/sudoman/.dropbox/deleted.dbx
Jul  8 14:13:49 2013 /Users/sudoman/.dropbox/filecache.dbx
Jul  8 10:05:54 2013 /Users/sudoman/.dropbox/finderplugin/l/51da72e2
```

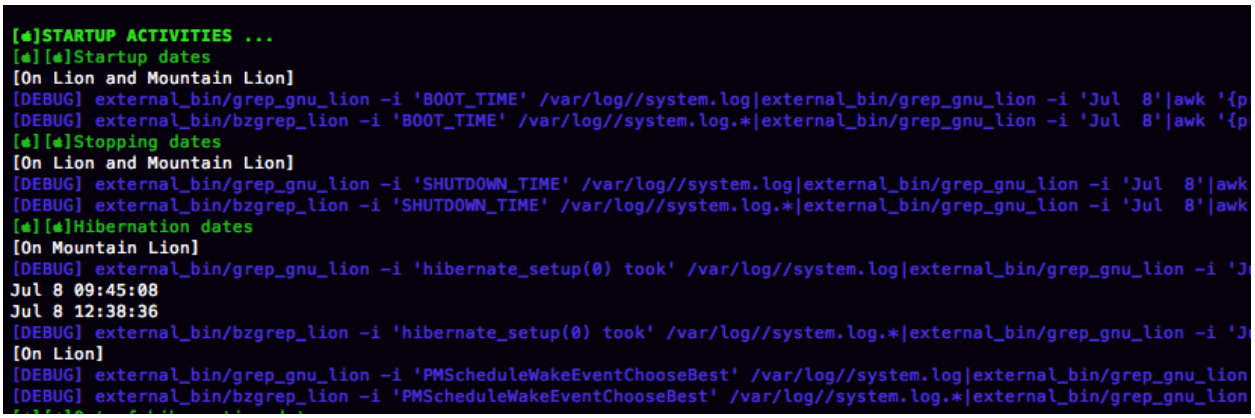
Accessed and modified files on July 4

```
[●]APPLICATIONS ACTIVITIES ...
[●][●]Opened applications (last access dates)
-rw-r--r--@ 1 sudoman staff 1676 8  14:16 /Applications/0xED.app/Contents/Info.plist
-rw-r--r--@ 1 sudoman admin 4375 8  14:16 /Applications/7zX.app/Contents/Info.plist
-rw-r--r--@ 1 sudoman admin 6201 8  14:16 /Applications/Adium.app/Contents/Info.plist
-rw-r--r-- 1 sudoman staff 2273 8  14:16 /Applications/AirParrot.app/Contents/Info.plist
-rw-r--r--@ 1 sudoman staff 2197 8  14:16 /Applications/AppCleaner.app/Contents/Info.plist
-rw-r--r-- 1 sudoman staff 2853 8  14:16 /Applications/ASCII Projektor.app/Contents/Info.plist
-rw-r--r--@ 1 sudoman admin 1750 8  14:16 /Applications/BadAssProxy.app/Contents/Info.plist
-rw-r--r--@ 1 sudoman admin 1572 8  14:16 /Applications/ClipMenu.app/Contents/Info.plist
-rw-r--r--@ 1 sudoman admin 1481 8  14:16 /Applications/Disk Arbitrator.app/Contents/Info.plist
-rw-r--r-- 1 sudoman admin 11284 8  14:16 /Applications/EagleFiler.app/Contents/Info.plist
-rw-r--r-- 1 sudoman admin 2015 8  14:16 /Applications/EasyFind.app/Contents/Info.plist
-rw-r--r-- 1 sudoman admin 8327 8  14:50 /Applications/Evernote.app/Contents/Info.plist
-rw-r--r--@ 1 sudoman admin 5487 8  14:47 /Applications/Firefox.app/Contents/Info.plist
-rw-r--r-- 1 sudoman staff 6378 8  14:16 /Applications/Fraise.app/Contents/Info.plist
-rw-r--r-- 1 sudoman admin 2009 8  14:16 /Applications/FreeMind.app/Contents/Info.plist
```

Opened applications on July 4



Read of logs files archive



Using of –v and –a option