Macintosh Forensics

University of Utah

Sept 21, 2005

Derrick Donnelly, CTO
BlackBag Technologies
Rules of the game

- Make no changes to suspect system
- Document everything
- Document, document and then document some more...
- Take very good notes
- A case could take 2–3 years to go to court, your memory will never last
Data changes fast

- Under normal conditions as soon as an HFS partition mounts on your desktop, you will change your last modified date and time
- You want to avoid this, if you can’t document it
- You can use physical write-blockers or turn off diskarbitrationd (In Panther and Tiger)
Interesting commands

- Mount
- ls /dev/disk?
- ioreg –c “IOMedia”
- dd and dcfldd
- pdisk
- hdiutil pmap
- hdiutil attach
- Hdiutil attach /some/image.dmg –shadow
Disk Arbitration

- Diskarbitration is now the main process in Panther used to manage and mount disk partitions
- BBT has provided a GUI app to disable Diskarbitrationd similar to the autodiskmounting procedure in 10.1–10.2
- /etc/mach_init.d/diskarbitrationd.plist
Disk Arbitration

• `/etc/mach_init.d` directory example
Disk Arbitration

- Contents of diskarbitration.d.plist
- Contents in standard XML

```xml
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version='1.0'>
<dict>
  <key>ServiceName</key>
  <string>com.apple.DiskArbitration.diskarbitrationd</string>
  <key>Command</key>
  <string>/usr/sbin/diskarbitrationd</string>
  <key>OnDemand</key>
  <false/>
</dict>
</plist>
```

BlackBag1:/etc/mach_init.d/dornellid$
Disk Arbitration - Disabling

- Go to the /etc/mach_init.d Directory
  - cd /etc/mach_init.d
- Create a directory in /Library called DiskArb_Backup
  - sudo mdir /Library/DiskArb_Backup
- Copy diskarbitrationd.plist to DiskArb_Backup (Always make sure you have a backup before you remove the file)
  - sudo cp /etc/mach_init.d/diskarbitrationd.plist /Library/DiskArb_Backup
- Now you can remove (delete) the file
  - sudo rm /etc/mach_init.d/diskarbitrationd
- Once the file has been removed, you can Reboot the System

- To re-enable DiskArbitration reverse the process, copy the file (diskarbitrationd.plist back to /etc/mach_init.d

- Always make sure you make a Backup of diskarbitrationd.plist before you delete or move it
Diskarbitration

• When diskarbitration is off partitions do not get mounted automatically
• It is not a write-blocker, if you do something stupid you can change data on a suspect system
• You have to mount destination partitions manually
• You can also mount read-only
Open Firmware

- Use “Open Firmware Password” to set a password for your Open Firmware
- You can find this utility on the first CD of your Install CDs
- If a user sets the firmware password it may interfere with FireWire Target Mode
Open Firmware

• If you boot up and hold the “Option” key and you see this screen a firmware password has been set by the user.
Open Firmware

• Or the computer might continue to Boot as normal, if you see this you want to kill the power
Open Firmware

- Normal bootup screen
Open Firmware

• For proper FireWire target mode you should see the yellow FireWire logo
• If you hold down “Apple” + “Option” + “O” + “F” you will drop into the Open Firmware
Open Firmware

• To continue normal booting type:
  - mac–boot (you do not want to do this on a suspect system)

• To shutdown from open firmware type:
  - shut–down

• This can be handy if you just want to check the system time

• This process will not write to the drive
Open Firmware

• Notice you can see the system time from this screen
• Time will be in GMT

system time and date is: 16:25:21 04/08/2004
Imaging drives

- Standard dd command (suspect drive=/dev/disk1)
  ```
sudo dd if=/dev/disk1 bs=1024 conv=noerror,sync of=/evidence/Imagefile.dmg
  ```

- sudo dd if=/dev/disk1 bs=1024 conv=noerror,sync | split - -b2000m /evidence/Imagefile.
Working dcfldd

- sudo dcfldd if=/dev/disk1 hashwindow=0 conv=noerror,sync bs=1024 of=/evidence/imagefile.dmg
- Sudo dcfldd if=/dev/disk1 hashwindow=0 conv=noerror,sync bs=1024 | split - -b2000m /evidence/imagefile.
- Dcfldd has been updated now called dccidd (Supports sha1, sha-256)
Imaging Live systems

- Use rdisk entries (ls /dev/rdisk?)
- Rdisk = raw disk (buffered copy)
- Sudo dd if=/dev/rdisk0 conv=noerror,sync bs=1024 of=/evidence/imagefile.dmg
- Make sure you have enough space to image a full drive
- Lock your image files before mounting them with DiskCopy (DiskUtility)
Places to look for evidence

- Remember Mac OS X is a Unix based system
- Most user files are created and saved in the User’s home directory
- A Mac OS X System can have multiple users
Panther Built in Tools

• Always use find to search for large .dmg or sparse files
• You could be missing entire sub volumes
Panther Built in Tools

• Sort results by size, to find all the large disk images
Panther Built in Tools

• Click on the results to find the paths to the files in question
Open Source Solutions

• SleuthKit
  - Forensic Tools from Brain Carrier
  - Installation
    - Requirements:
      - Developer Tools
    - Available from www.sleuthkit.org

  - Use
    - For SleuthKit to see data, you need to manually break out the partitions.

• Autopsy
  - Graphical Front end to SleuthKit
• **Music only FAT 32 formatted**

```bash
Differential:/dev charnotachardioreg -c IOMedia+-o Apple iPod Media <class IOMedia, registered, matched, active, busy 0, retain count 10$

```
iPod (in ioreg)

```
"BSD Unit" = 2
"Ejectable" = Yes
"Content" = "FDisk_partition_scheme"
"Whole" = Yes

+-o IOMediaBSDClient <class IOMediaBSDClient, registered, matched, active, busy 0, retain count
+-o IOFDiskPartitionScheme <class IOFDiskPartitionScheme, !registered, !matched, active$
+-o Untitled 2@2 <class IOMedia, registered, matched, active, busy 0, retain count 9>  

|   |   |       | |   |       |       |   "Leaf" = Yes
|   |   |       | |   |       |       |   "Writable" = Yes
|   |   |       | |   |       |       |   "BSDMinor" = 9
|   |   |       | |   |       |       |   "PreferredBlockSize" = 512
|   |   |       | |   |       |       |   "PartitionID" = 2
|   |   |       | |   |       |       |   "BSDMajor" = 14
|   |   |       | |   |       |       |   "BSDDisk" = "disk2s2"
|   |   |       | |   |       |       |   "Size" = 4959843840
|   |   |       | |   |       |       |   "ContentHint" = "DOS_FAT_32"
|   |   |       | |   |       |       |   "Removable" = Yes
|   |   |       | |   |       |       |   "BSDUnit" = 2
|   |   |       | |   |       |       |   "Ejectable" = Yes
|   |   |       | |   |       |       |   "Content" = "DOS_FAT_32"
|   |   |       | |   |       |       |   "Whole" = No

```
Commercial Data Recovery

- FileSalvage SubRosa Soft
- DataRescue
- DiskWarrior
- Drive 10
- Tech Tool
MacQuisition Boot CD

- Image Mac systems without taking them apart
BlackBag Services

- Software Forensic Suite
- Forensic Hardware (Firebox)
  - IDE and SCSI Write Blocker using the Firewire bus
- Mac Forensic Training
  - (Local Santa Clara and Mobile Class)
- Forensic analysis consulting and Data Recovery
Mac Forensic Forum

- Join us on the Mac Forensic forum on Yahoo
  - http://groups.yahoo.com/group/macos_foresnics/
- The group is closed group mostly for Law enforcement
Contact

Derrick Donnelly
CTO, BlackBag Technologies

derrick@blackbagtech.com
408–844–8892
www.blackbagtech.com