

# Macintosh Forensics

# Mac Networkers Retreat

---

**Oct 30, 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 disk arbitration (In Panther and Tiger)



## Files/Folders created

- 560 files/folders can be created between boot-ups
- 10000–11000 files/folders can be created in a 24 hr period (Normal use)
- Temp files, plists, .DS\_Store, virtual memory, browser cache file, e-mail cache files, e-mail databases etc...



# Interesting commands

- Mount
- Is /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

```
Terminal — bash — 76x14
BlackBag1:/etc/mach_init.d donnell$ cd /etc/mach_init.d
BlackBag1:/etc/mach_init.d donnell$ ls
ATSServer.plist          diskarbitrationd.plist
DirectoryService.plist  distnoted.plist
KerberosAutoConfig.plist  fix_prebinding.plist
WindowServer.plist      kuncd.plist
configd.plist           lookupd.plist
coreservicesd.plist     notifyd.plist
BlackBag1:/etc/mach_init.d donnell$
```



# Disk Arbitration

- Contents of diskarbitrationd.plist
- Contents in standard XML

```
Terminal — bash — 89x16

<?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 donnell$
```





# 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 mkdir /Library/DiskArb_Backup`
- Copy diskarbitrationd.plist to DiskArb\_Back (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



## Warning!!!

- **Make sure you turn off FileVault or use a non FileVaulted user!!!!**
- **Added Oct 30, 2005 (Aptos, CA)**



# 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

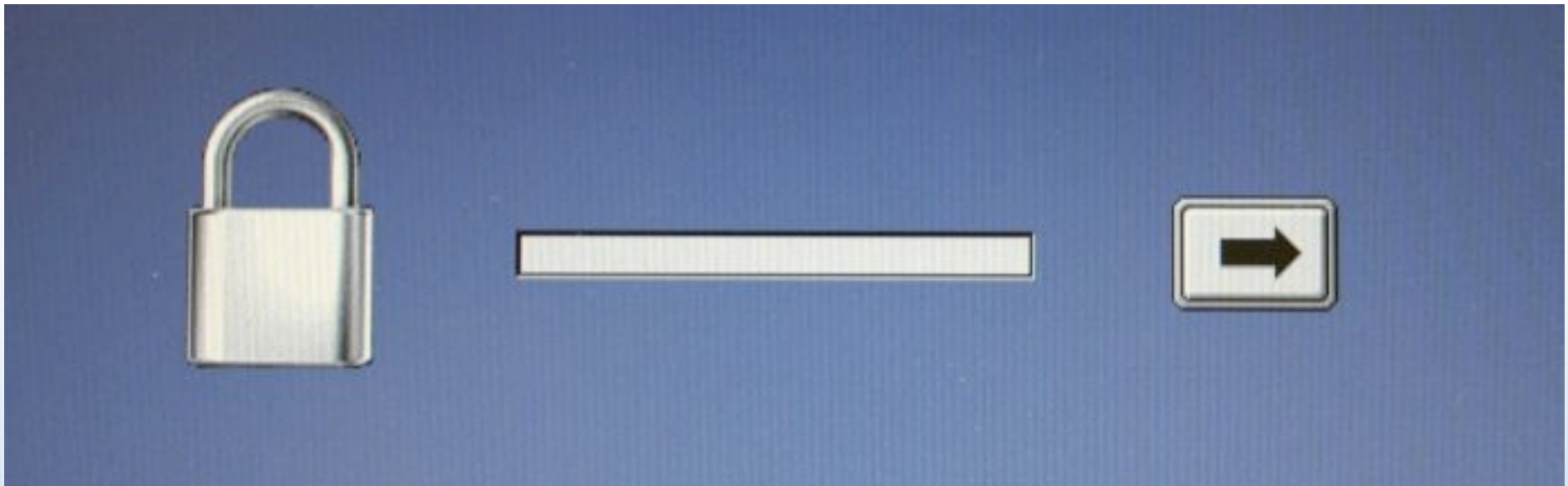


Open Firmware Password



# 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







# Open Firmware

- If you hold down “Apple” + “Option” + “O” + “F” you will drop into the Open Firmware

```
Apple PowerBook5,3 4.7.1f1 BootROM built on 09/04/03 at 13:39:26
Copyright 1994-2003 Apple Computer, Inc.
All Rights Reserved.

Welcome to Open Firmware, the system time and date is: 16:25:21 04/08/2004

To continue booting, type "mac-boot" and press return.
To shut down, type "shut-down" and press return.

ok
0 > _
```



# 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
```



# Looking for devices

- `ioreg -c "IOMedia"`
- `ioreg -l | more`
- `ioreg -c "IOMedia" | more`
- `ioreg -c "ATADeviceNub"`
  
- Is `/dev/disk?`
  - ◆ `/dev/disk0`     `/dev/disk1`



# Output from ioreg

```
• | | | +-o Hitachi IC25N080ATMR04-0 Media <class IOMedia, regis$
• | | | | {
• | | | | "Leaf" = No
• | | | | "Writable" = Yes
• | | | | "BSD Minor" = 0
• | | | | "IOBusyInterest" = "IOCommand is not serializable"
• | | | | "Preferred Block Size" = 512
• | | | | "BSD Major" = 14
• | | | | "BSD Name" = "disk0"
• | | | | "Size" = 80026361856
• | | | | "Content Hint" = ""
• | | | | "Removable" = No
• | | | | "IOMedialcon" = {"IOBundleResourceFile"="Internal.i$
• | | | | "BSD Unit" = 0
• | | | | "Ejectable" = No
• | | | | "Content" = "Apple_partition_scheme"
• | | | | "Whole" = Yes
• | | | | }
```

BlackBag Technologies Inc., © 2005



## ioreg -c "ATADeviceNub"

- | | | +-o ATADeviceNub@0 <class ATADeviceNub, registered, matched, active, busy 0, retain count 6>
- | | | | {
- | | | | "ata device type" = "ata"
- | | | | "unit number" = 0
- | | | | "IOUnit" = 0
- | | | | "socket type" = "internal"
- | | | | "device model" = "Hitachi IC25N080ATMR04-0"
- " | | | |
- | | | | "extended LBA capacity" = 156301488
- | | | | "device serial" = " MRG426K4GH031H"
- | | | | "device revision" = "MO4AAD0A"
- | | | | }
- | | | |



## 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)



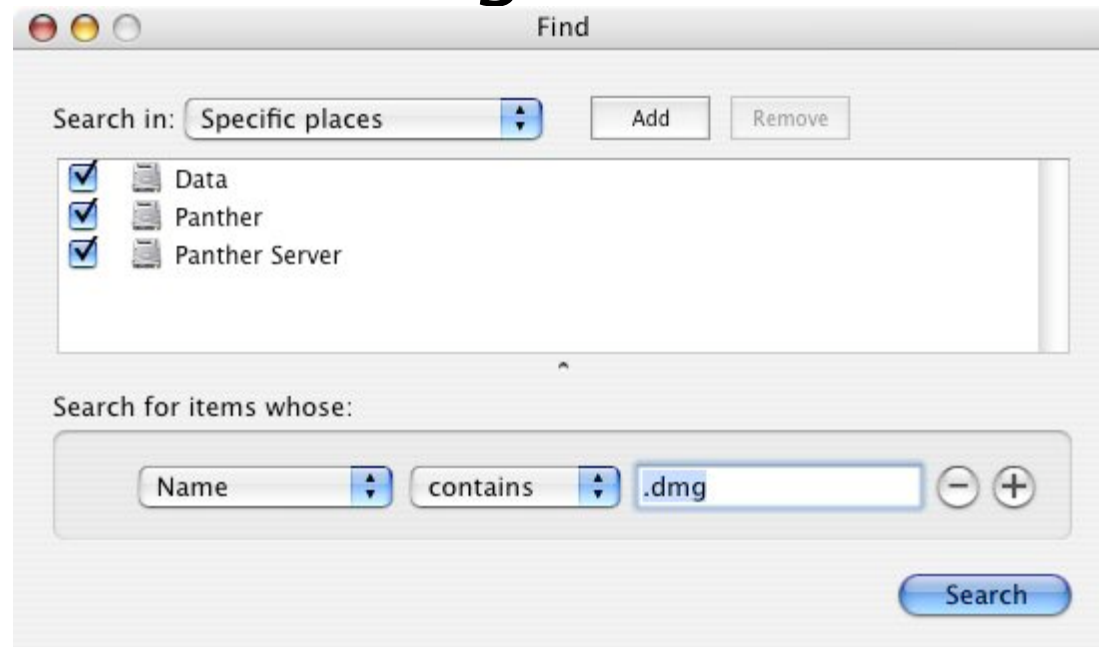
## Places to look for evidence

- 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

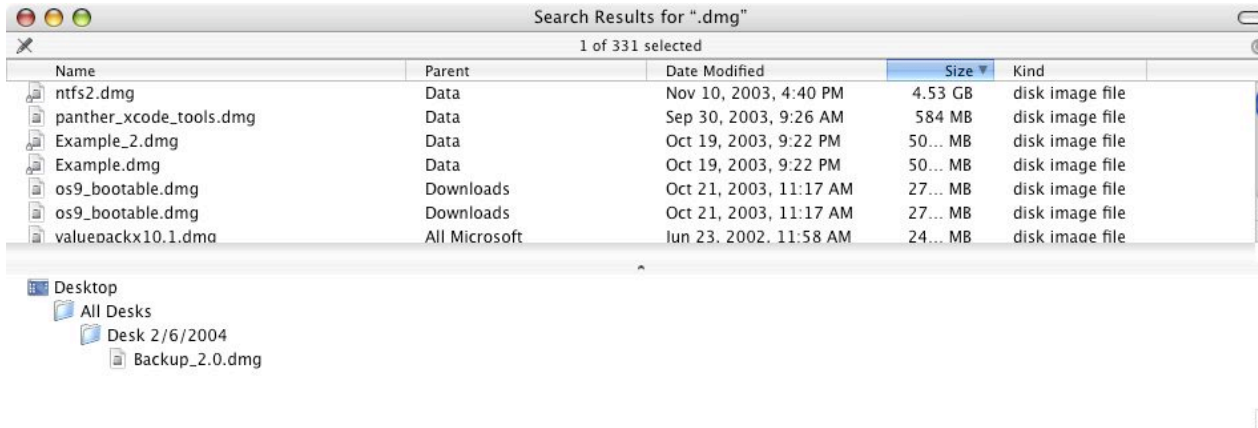
- Always use find to search for large .dmg or sparse files
- You could be missing entire sub volumes





# Panther Built in Tools

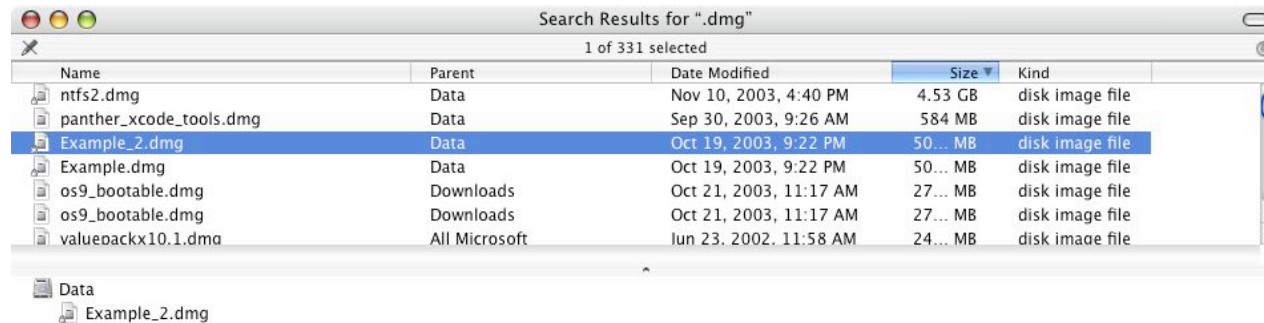
- Sort results by size, to find all the large disk images





# 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](http://www.sleuthkit.org)
  - ◆ Use
    - For SleuthKit to see data, you need to manually break out the partitions.
- Autopsy
  - ◆ Graphical Front end to SleuthKit



# iPod

- Music only FAT 32 formatted

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

```
| | | | | | | | {
| | | | | | | | "Leaf" = No
| | | | | | | | "Writable" = Yes
| | | | | | | | "BSD Minor" = 8
| | | | | | | | "Preferred Block Size" = 512
| | | | | | | | "BSD Major" = 14
| | | | | | | | "BSD Name" = "disk2"
| | | | | | | | "Size" = 5007744000
| | | | | | | | "Content Hint" = ""
| | | | | | | | "Removable" = Yes
| | | | | | | | "IOMediaIcon" =
| | | | | | | | {"CFBundleIdentifier"="com.apple.iokit.IOStorageFamily","IOBundleRes$
```



# iPod (in ioreg)

```
||| | ||| | | | | "BSD Unit" = 2
||| | ||| | | | | "Ejectable" = Yes
||| | ||| | | | | "Content" = "FDisk_partition_scheme"
||| | ||| | | | | "Whole" = Yes
||| | ||| | | | | }
||| | ||| | | | |
||| | ||| | | | | +-o IOMediaBSDClient <class IOMediaBSDClient, registered, matched, active, busy 0, reta$
||| | ||| | | | | +-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
||| | ||| | | | | | | "BSD Minor" = 9
||| | ||| | | | | | | "Preferred Block Size" = 512
||| | ||| | | | | | | "Partition ID" = 2
||| | ||| | | | | | | "BSD Major" = 14
||| | ||| | | | | | | "BSD Name" = "disk2s2"
||| | ||| | | | | | | "Size" = 4959843840
||| | ||| | | | | | | "Content Hint" = "DOS_FAT_32"
||| | ||| | | | | | | "Removable" = Yes
||| | ||| | | | | | | "BSD Unit" = 2
||| | ||| | | | | | | "Ejectable" = Yes
||| | ||| | | | | | | "Content" = "DOS_FAT_32"
||| | ||| | | | | | | "Whole" = No
||| | ||| | | | | | | }
||| | ||| | | | | | |
||| | ||| | | | | +-o IOMediaBSDClient <class IOMediaBSDClient, registered, matched, active, busy 0, $
```





# Commercial Data Recovery

- FileSalvage SubRosa Soft
- DataRescue, DataRescue II
- DiskWarrior
- Drive 10
- Tech Tool



# MacQuisition Boot CD

- Image Mac systems without taking them apart

The image displays three overlapping screenshots of the MacQuisition software interface, illustrating the process of imaging a Mac system.

**STEP: 1 - Source Identification**

Full Acquisition (checked). No Software RAID Detected.

Select all source devices from the following list: NOTE: BDrive=Boot Drive

Device	Device Info	Comments
<input type="checkbox"/> /dev/disk0	ATA FUJITSU MHT2080AT - 74.53 GB	BDrive
<input type="checkbox"/> /dev/disk1	OTHER Apple sparse disk image - 69.16 GB	

**STEP: 3 - Case Information**

Case Information

System Time: 5:17:09 PM Wednesday, May 11, 2005

Real Time: 4:56:54 PM 5/11/2005

Case Name: Case ID: CASE\_0001

Location: Exhibit ID: EXHIBIT\_0001

Folder Name: CASE\_2005-05-11\_165651 Image File Name: IMAGE\_0001

**STEP: 5 - Imaging/Status Information**

Acquisition Log:

Hard Drive Capacity:  
Case Comments:  
Source Device: /dev/disk0 ATA FUJITSU MHT2080AT - 74.53 GB BD  
Source Device Size: 80026361856 Bytes 156301488 Sectors  
Destination Device:  
Destination Partition MountPoint:  
Destination Path: /CASE\_2005-05-11\_165651/Images/IMAGE\_0001

Reporting Options:

- System Info
- IOReg Info
- Create SigFile

Progress Information:

Start Time: ---:--:--  
Estimated Finish Time: ---:--:-- Time Remaining: ---:--:--

Buttons: Back, Cancel, IMAGE



# 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\\_forensics/](http://groups.yahoo.com/group/macos_forensics/)
- <http://www.blackbagtech.com/forensics.html>
- The group is closed group mostly for Law enforcement



# Contact

Derrick Donnelly  
CTO, BlackBag Technologies

[derrick@blackbagtech.com](mailto:derrick@blackbagtech.com)

408-844-8892

[www.blackbagtech.com](http://www.blackbagtech.com)