# Macintosh Forensics University of Utah

#### Sept 21, 2005



Derrick Donnelly, CTO BlackBag Technologies

1



# **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
- 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

BlackBag1:/etc/mach_init.d d	onnelld\$ cd /etc/mach_init.d	Į
BlackBag1:/etc/mach_init.d d	onnelld\$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 d	onnelld\$	
BlackBag1:/etc/mach_init.d d	onnelld\$	



### **Disk Arbitration**

- Contents of diskarbitrationd.plist
- Contents in standard XML

```
\Theta \Theta \Theta
                               Terminal — bash — 89x16
                                                                                           Z
<?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>
        _ckey>Command</key>
        <string>/usr/sbin/diskarbitrationd</string>
        _key>OnDemand</key>
        <false/>
</dict>
</plist>
BlackBag1:/etc/mach_init.d donnelld$
```



# **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\_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



# 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



- 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



 If you boot up and hold the "Option" key and you see this screen a firmware password has been set by





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





#### Normal bootup screen





#### 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

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.



- 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



- 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 updatednow 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) BlackBag Technologies Inc., © 2005



- 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

Search in: Specific places Add Remove	]
<ul> <li>Data</li> <li>Panther</li> <li>Panther Server</li> </ul>	
Search for items whose:	
Name Contains .dmg	$\odot \oplus$
	Search

BlackBag Technologies Inc., © 2005



# **Panther Built in Tools**

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

Desk 2/6/2004 Backup\_2.0.dmg

0	00	Search	Results for ".dmg"			$\bigcirc$
×		1	of 331 selected			6
	Name	Parent	Date Modified	Size ▼	Kind	
	ntfs2.dmg	Data	Nov 10, 2003, 4:40 PM	4.53 GB	disk image file	
3	panther_xcode_tools.dmg	Data	Sep 30, 2003, 9:26 AM	584 MB	disk image file	
	Example_2.dmg	Data	Oct 19, 2003, 9:22 PM	50 MB	disk image file	
	Example.dmg	Data	Oct 19, 2003, 9:22 PM	50 MB	disk image file	
	os9_bootable.dmg	Downloads	Oct 21, 2003, 11:17 AM	27 MB	disk image file	
3	os9_bootable.dmg	Downloads	Oct 21, 2003, 11:17 AM	27 MB	disk image file	
2	valuepackx10.1.dmg	All Microsoft	lun 23. 2002. 11:58 AM	24 MB	disk image file	Ψ.
			^			
ii:	E Desktop					
	📁 All Desks					



# **Panther Built in Tools**

#### Click on the results to find the paths to the files in question

$\Theta \Theta \Theta$	Search	Results for ".dmg"			$\bigcirc$
×	1	of 331 selected			٢
Name	Parent	Date Modified	Size ▼	Kind	
ntfs2.dmg	Data	Nov 10, 2003, 4:40 PM	4.53 GB	disk image file	0
panther_xcode_tools.dmg	Data	Sep 30, 2003, 9:26 AM	584 MB	disk image file	
🔎 Example_2.dmg	Data	Oct 19, 2003, 9:22 PM	50 MB	disk image file	
Example.dmg	Data	Oct 19, 2003, 9:22 PM	50 MB	disk image file	
os9_bootable.dmg	Downloads	Oct 21, 2003, 11:17 AM	27 MB	disk image file	
os9_bootable.dmg	Downloads	Oct 21, 2003, 11:17 AM	27 MB	disk image file	
valuepackx10.1.dmg	All Microsoft	lun 23. 2002. 11:58 AM	24 MB	disk image file	<b>T</b>
		^			

Data Example\_2.dmg

1



# **Open Source Solutions**

- SleuthKit
  - Forensic Tools from Brain Carrier
  - Installation
    - Requirements:
      - **Developer Tools**
    - Available from <u>www.sleuthkit.org</u>
  - Use
    - For SluethKit 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\$

			{
			"Writable" = Yes
			"BSD Minor" = 8
	Ī		Preferred Block Size" = 512
ÌÌ			"BSD Major" = 14
ÌÌ	Í		BSD Name" = "disk2"
ÌÌ	Í		"Size" = 5007744000
ÌÌ	Í		Content Hint" = ""
ÌÌ	Í		"Removable" = Yes
İİ	İ		"IOMediaIcon" =
• •	("(	CFBundleI	dentifier"="com.apple.iokit.IOStorageFamily","IOBundleRes\$



# iPod (in ioreg)

Ι		"BSD Unit" = 2
		"Ejectable" = Yes
		"Content" = "FDisk_partition_scheme"
		"Whole" = Yes
i	ÌÌÌ	
i	ÌÌÌ	+-o IOMediaBSDClient <class 0,="" active,="" busy="" iomediabsdclient,="" matched,="" registered,="" reta\$<="" th=""></class>
Í		+-o IOFDiskPartitionScheme <class !matched,="" !registered,="" active\$<="" iofdiskpartitionscheme,="" td=""></class>
Ì		+-o Untitled 2@2 <class 0,="" 9="" active,="" busy="" count="" iomedia,="" matched,="" registered,="" retain="">        </class>
`		"Leaf" = Yes
i	iii	"Writable" = Yes
i	ÌÌÌ	"BSD Minor" = 9
Í		"Preferred Block Size" = 512
Í	Î Î	Partition ID" = 2
Í		"BSD Major" = 14
Í	Î Î	"BSD Name" = "disk2s2"
		"Size" = 4959843840
		Content Hint" = "DOS_FAT_32"
Í	Î Î	"Removable" = Yes
		"BSD Unit" = 2
		"Ejectable" = Yes
Í	Î Î	Content" = "DOS_FAT_32"
		"Whole" = No
Í		
Ì		+-o IOMediaBSDClient <class \$<="" 0,="" active,="" busy="" iomediabsdclient,="" matched,="" registered,="" td=""></class>



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



### **MacQuisition Boot CD**

#### Image Mac systems without taking them apart

0	MacQuisition STEP 1 - Source Identification			
EP: 1 🗹 Full Acquisition		No Software RAID Detected		
ct all source devices from th	e following list: NOTE: BDrive=Boot Drive	Rescan Buses		
Device /dev/disk0 ATA FUJI /dev/disk1 OTHER A	Device Info SU MHT2080AT – 74.53 GB BDrive ple sparse disk image – 69.16 GB	Comments		
	O O MacQuisition	n STEP 3 – Case Information		
	STEP: 3 Case Information			
/ill be warned if you attemp	System Time: 5:17:09 PM Wednesday, M	ay 11, 2005 Ac	dditional Information	
	hh:mm:ss mm/	dd/yyyy	MacQuisition STEP 5 - Imaging /Status	Information
	Real Time: 4:56:54 PM - 5/1	1/2005 • Set	CTED. E	mormation
	Case Name:	Case ID: CASE_0001	Acquisition Log:	Input/Output Errors
	Location:	Exhibit ID: EXHIBIT 00	01 Hard Drive Capacity:	Reporting Options
			Case Comments: Source-Device:-/dev/disk0 ATA FUIITSU MHT2080AT - 74.53 GB BD	System Info
	Folder Name: CASE_2005-05-11_165651	Image File Name: IMAGE_000	1 Schrauge Viel Size: 80026361856 Bytes 156301488 Sectors	IOReg Info
			Destination_Partition_MountPoint:	Create SigFile
	Expert Options	Back	Destination Wath: /CASE_2005-05-11_165651/Images/IMAGE_0001	↓ ▼
			- 0	
			Programs information	
			Progress information	Back
			Progress information Start Time::	Back
			Progress information         Start Time:::-         Estimated Finish Time:::         Time Remaining:::	Back Cancel

BlackBag Technologies Inc., © 2005



# **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
- <u>http://groups.yahoo.com/group/maco</u> <u>s\_forensics/</u>
- <u>http://www.blackbagtech.com/forensi</u>
   <u>cs.html</u>
- The group is closed group mostly for Law enforcement





### Derrick Donnelly CTO, BlackBag Technologies <u>derrick@blackbagtech.com</u> 408-844-8892 www.blackbagtech.com