

Unix/Linux dd Utility

Priscilla Oppenheimer

Unix/Linux dd Utility*

- Duplicate device, disk duplicator, data dump, whatever you want dd to mean
- Copies a chunk of data from one place to another
 - if = input
 - of = output
- Reads and writes data in block-sized chunks (default block size is 512 bytes)

*There are Windows versions too...

dd Example

- Create a disk image
- **dd if=/dev/disk0 of=case321.dd**
 - Copies all of disk0 to a file called case321.dd
- The disk image file will be mountable.
- The disk image file may be huge...

Output Destinations

- The output from dd can be a new file or another storage device
- Linux examples:
- **dd if=/dev/hda of=/mnt/hda.dd**
 - Copies the master ATA disk on the primary channel to a file
- **dd if=/dev/hda of=/dev/hdd**
 - Copies the master ATA disk on the primary channel to the slave AT disk on the second channel

dd Options

- `bs` - block size
- `count` - copy the number of blocks specified, then stop
- `skip` - count the blocks specified, skip them, then start copying
- `conv=noerror`, - prevent dd from stopping when it encounters an error
- `sync` - pad every input block to the buffer size

More dd Examples

- **dd if=/dev/disk0 count=1 of=case321.dmg**
 - Gets just one sector, possibly the boot sector (depending on what's on the disk)
- **dd if=/dev/disk0 skip=1 count=1 of=case321.dmg**
 - Gets the Partition Map on a Macintosh
- **dd if=/dev/disk0 skip=420000 count=3|xxd**
 - Shows a piece of evidence perhaps
 - Pipes to xxd hexdump utility
- **dd if=/dev/disk0 skip=420000 count=3|md5sum**
 - Pipes the results to md5sum to get a hash
 - Should have done this first probably...

dcfldd and dccidd

- U.S. Department of Defense's Cyber Crime Center created versions of dd that can calculate hashes of the data being copied
- dccidd is newer
 - Can calculate MD5, SHA-1, SHA-256
- **dcfldd if=/dev/hda of=/mnt/hda.dd bs=2k hashwindow=1M hashlog=/mnt/hda.hashes**

Do Try This at Home!

- Don't have Unix or Linux?
 - No problem (Use Penguin Sleuth Kit or other bootable Linux CD)
 - Includes The Sleuth Kit and other goodies.
- Don't have lots of hard drives lying around?
 - No problem (Image a USB thumb drive or your iPod while learning!)

Image a USB Thumb Drive

- **dd if=/dev/disk2 of=usbdrive.dmg**
- Look at it with TSK mmls utility
- Priscillas-Computer:/Applications/sleuthkit/sleuthkit-2.02/bin Priscilla\$
./mmls /Users/Priscilla/usbdrive.dmg
- DOS Partition Table
- Sector: 0
- Units are in 512-byte sectors
- | | Slot | Start | End | Length | Description | |
|---|------|-------|------------|------------|-------------|--------------------|
| • | 00: | ----- | 0000000000 | 0000000000 | 0000000001 | Primary Table (#0) |
| • | 01: | ----- | 0000000001 | 0000000031 | 0000000031 | Unallocated |
| • | 02: | 00:00 | 0000000032 | 0000250623 | 0000250592 | DOS FAT16 (0x06) |

Use dd to Break Out Partition

- **dd if=/Users/Priscilla/usbdrive.dmg
skip=32 count=250592
of=/Users/Priscilla/usbdrivePART1**

- Look at it with TSK fsstat utility

- Priscillas-Computer:/Applications/sleuthkit/sleuthkit-2.02/bin Priscilla\$./fsstat -f fat
/Users/Priscilla/usbdrivePART1

- FILE SYSTEM INFORMATION

- -----

- File System Type: FAT16

- OEM Name: MSWIN4.1

- Volume ID: 0x17e9242f

- Volume Label (Boot Sector): LEXAR MEDIA

- Volume Label (Root Directory):

iPod or Storage Device?

- Priscillas-Computer:/Applications/sleuthkit/sleuthkit-2.02/bin
Priscilla\$./mmls /Users/Priscilla/myipod
- MAC Partition Map
- Sector: 1
- Units are in 512-byte sectors

| • | Slot | Start | End | Length | Description |
|---|---------------------|------------|------------|------------|-------------|
| • | 00: ----- | 0000000000 | 0000000000 | 0000000001 | Unallocated |
| • | 01: 00 | 0000000001 | 0000000062 | 0000000062 | |
| | Apple_partition_map | | | | |
| • | 02: ----- | 0000000001 | 0000000003 | 0000000003 | Table |
| • | 03: ----- | 0000000004 | 0000000062 | 0000000059 | Unallocated |
| • | 04: 01 | 0000000063 | 0000065598 | 0000065536 | Apple_MDFW |
| • | 05: 02 | 0000065599 | 0007999486 | 0007933888 | Apple_HFS |

Free Forensics Tools

- [The Sleuth Kit](#)
- [Penguin Sleuth Kit bootable CD](#)
- [Helix bootable CD](#)
- [Auditor bootable CD](#)
- [dd for Windows](#)
- [Windows Forensics Acquisition Tools](#)