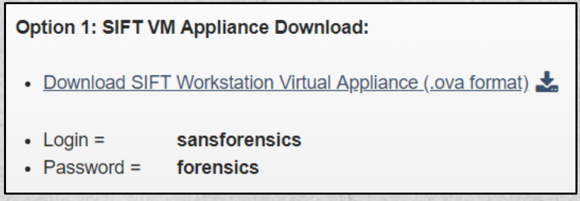
COMP 5350 / 6350
Digital Forensics

Storage Media Overview
Linux Forensics Commands

Forensics Testing Environment Setup

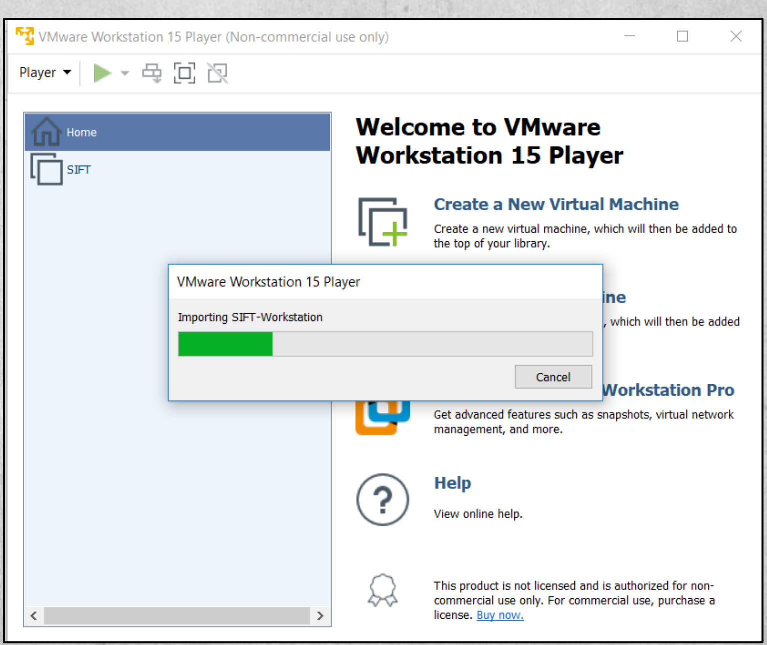
SIFT OVA Installation



Option 1: SIFT VM Appliance Download:

- Download SIFT Workstation Virtual Appliance (.ova format)

- Login = **sansforensics**
- Password = **forensics**



VMware Workstation 15 Player (Non-commercial use only)

Welcome to VMware Workstation 15 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

ine

, which will then be added

Workstation Pro

Get advanced features such as snapshots, virtual network management, and more.

Help

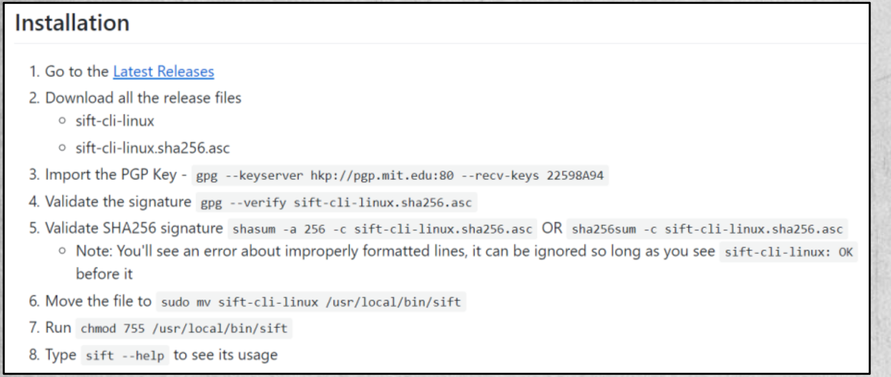
View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

VMware Workstation 15 Player

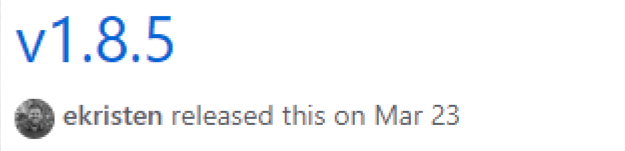
Importing SIFT-Workstation

SIFT CLI Installation



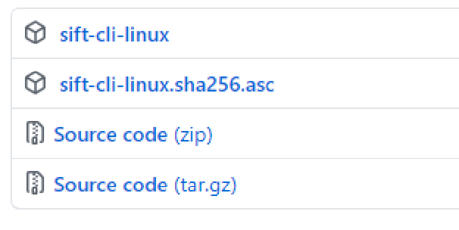
Installation

1. Go to the Latest Releases
2. Download all the release files
   - sift-cli-linux
   - sift-cli-linux.sha256.asc
3. Import the PGP Key - `gpg --keyserver hkp://pgp.mit.edu:80 --recv-keys 22598A94`
4. Validate the signature `gpg --verify sift-cli-linux.sha256.asc`
5. Validate SHA256 signature `shasum -a 256 -c sift-cli-linux.sha256.asc` OR `sha256sum -c sift-cli-linux.sha256.asc`
   - Note: You'll see an error about improperly formatted lines, it can be ignored so long as you see `sift-cli-linux: OK` before it
6. Move the file to `sudo mv sift-cli-linux /usr/local/bin/sift`
7. Run `chmod 755 /usr/local/bin/sift`
8. Type `sift --help` to see its usage



v1.8.5

ekristen released this on Mar 23



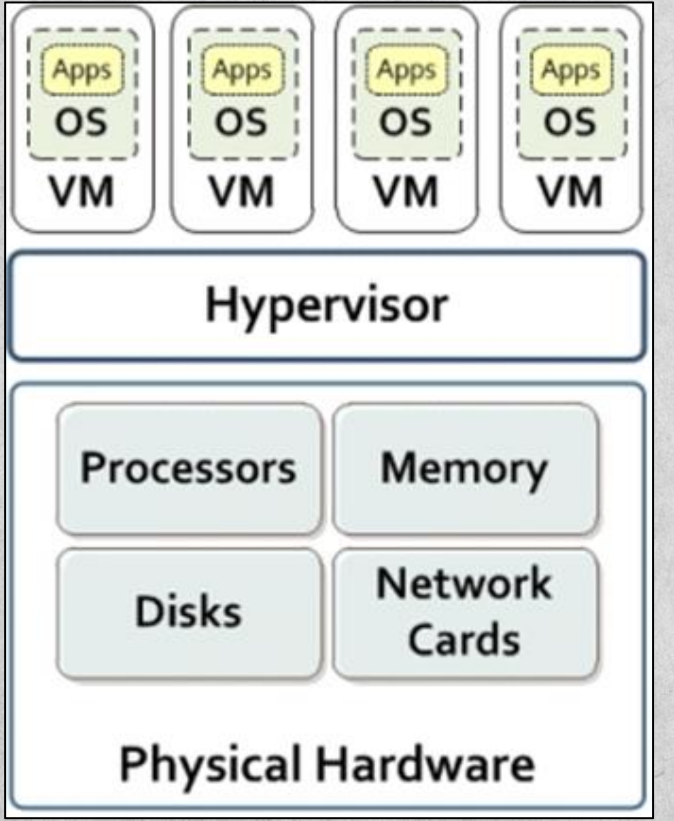
- sift-cli-linux
- sift-cli-linux.sha256.asc
- Source code (zip)
- Source code (tar.gz)

Virtualization

Virtualization Introduction

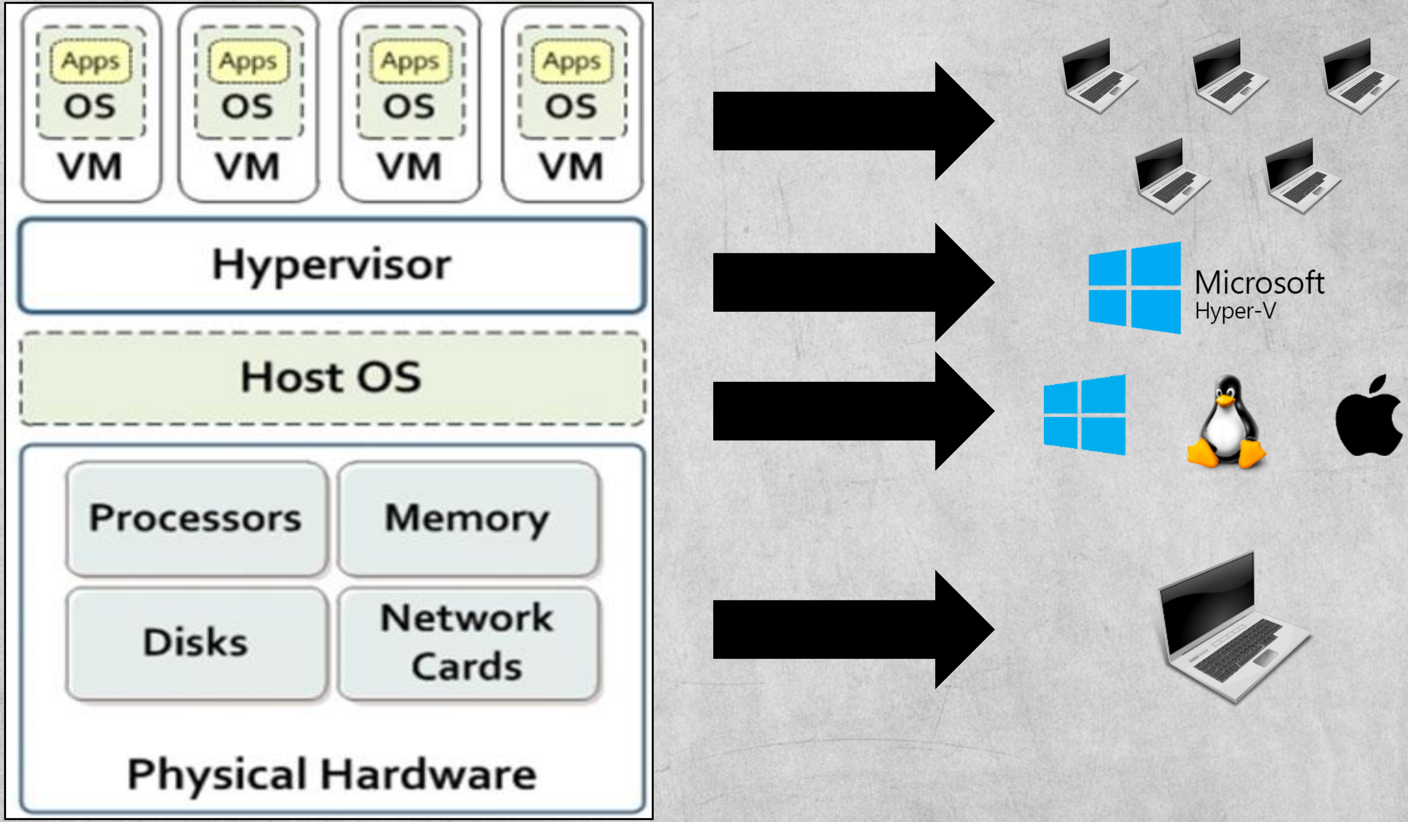
- Hypervisor - A software, firmware, or hardware solution that creates and runs virtual machines
- Hypervisors can be run in 2 different configurations:
  - ✓ Type I: Bare Metal
    - o Runs independent of the operating system
  - ✓ Type II: Hosted
    - o Dependent on the operating system
- Host – Hardware that a hypervisor runs on
- Guest – A virtual machine running on a hypervisor

Type I Hypervisor



vmware ESXi

Type II Hypervisor



Apps

OS

VM

Apps

OS

VM

Apps

OS

VM

Apps

OS

VM

Hypervisor

Host OS

Processors

Memory

Disks

Network Cards

Physical Hardware

Hypervisor Vendors

RED HAT VIRTUALIZATION

Hypervisor	Vendor	Type
ESX / ESXi*	VMWare	I
ZenServer	Citrix	I
Hyper-V	Windows	I
Workstation	VMWare	II
Player	VMWare	II
VirtualBox	Oracle	II

CITRIX XenServer

vmware

Microsoft Hyper-V

ORACLE VirtualBox

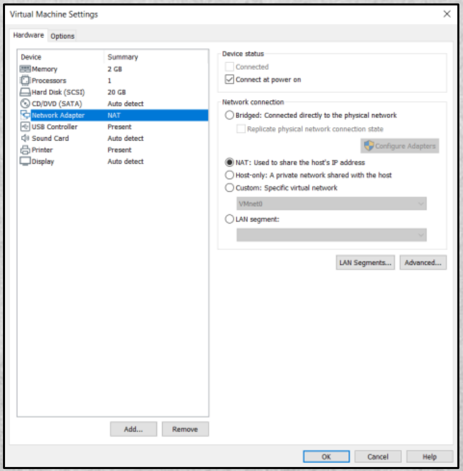
* Elastic Sky X

Virtualization Terms

- Provision
  - ✓ Allocation of host resources for a guest VM
- Clone
  - ✓ Replica of a VM’s for backup or operational purposes
- Snapshot
  - ✓ Image capture of a virtual machine
  - ✓ Allows rollback of VM’s due to corruption or misconfiguration
- Sandboxing
  - ✓ Separation of guest resources from external sources

Hypervisor Network Settings

- Hypervisors manage and allocate host and VM resources
  - ✓ Memory
  - ✓ Processors
  - ✓ Network Interfaces – Host Only, Bridged, NAT
  - ✓ USB Controller
  - ✓ Display



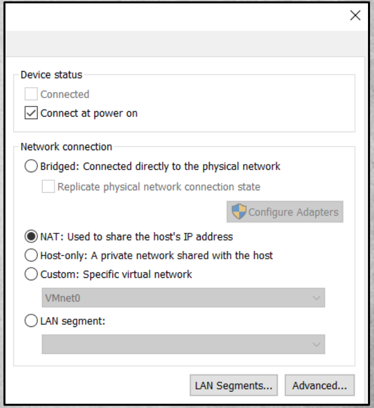
Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

□ Connected
☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
● NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
○ Custom: Specific virtual network
VMnet0
○ LAN segment:



Device status

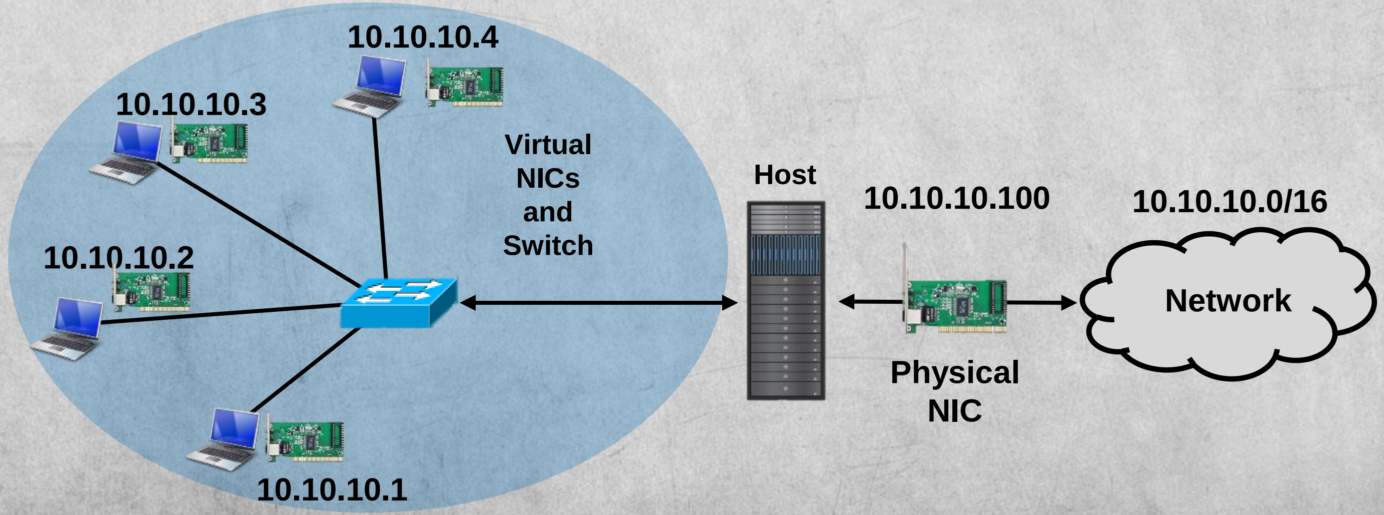
□ Connected
☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
● NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
○ Custom: Specific virtual network
VMnet0
○ LAN segment:

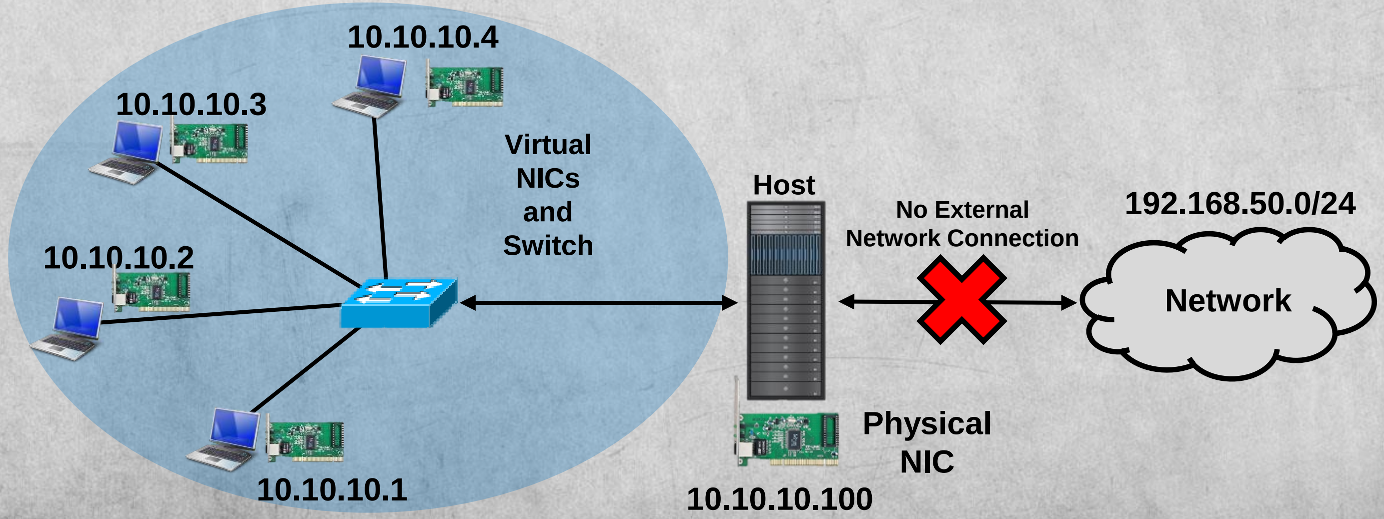
Bridged Network

- VM's and applications require direct network connections
- IP addressees assigned to guests coincide with the network that the physical NIC is communicating with
  - ✓ Static IP Assignment / DHCP



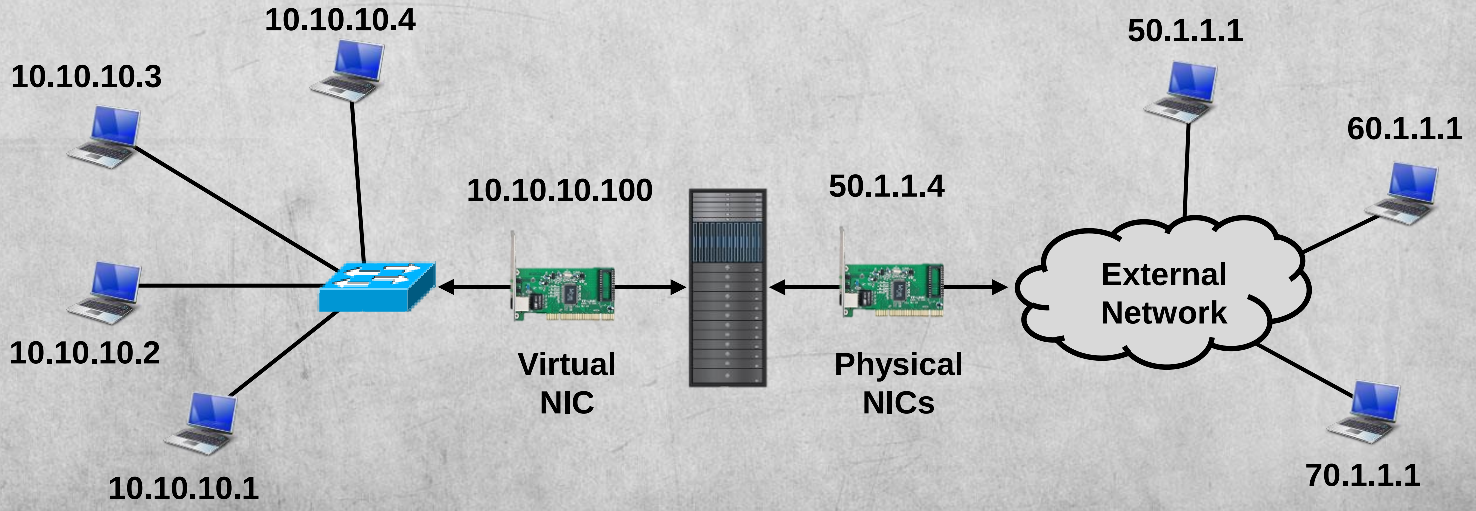
Host Only Network

- Some forensic applications require complete network isolation
  - ✓ Malware Analysis
  - ✓ Forensic Research
- IP addressees assigned to guests coincides only to the host IP network



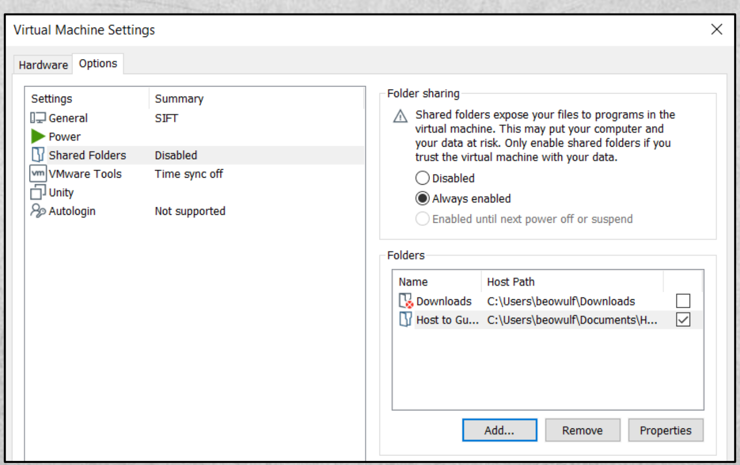
Network Address Translation

- NAT reduces the number of outward facing IP addresses in a traditional network and helps proxy internal IP traffic
- When assigned as a NAT network, guests will have there own internal IP structure while requests from external



Hypervisor Shared Directories

- When collecting forensic images from host to guest, it is advisable to create a shared directory
- Image size can be limiting if a shared directory is not available



Virtual Machine Settings

Settings	Summary
General	SIFT
Power	
Shared Folders	Disabled
VMware Tools	Time sync off
Unity	
Autologin	Not supported

Folder sharing

Shared folders expose your files to programs in the virtual machine. This may put your computer and your data at risk. Only enable shared folders if you trust the virtual machine with your data.

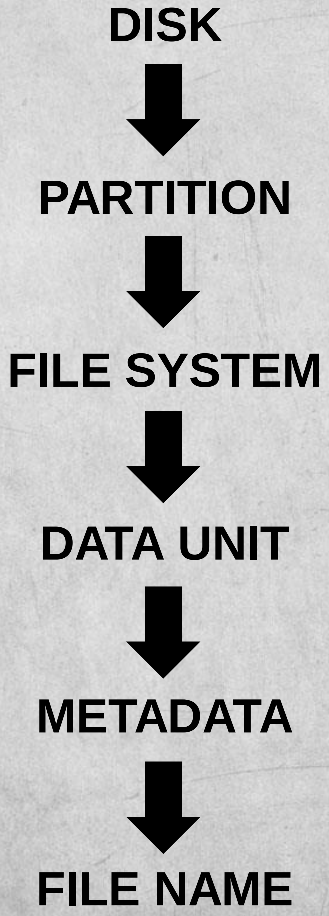
○ Disabled
● Always enabled
○ Enabled until next power off or suspend

Folders

Name	Host Path	
Downloads	C:\Users\beowulf\Downloads	□
Host to Gu...	C:\Users\beowulf\Documents\H...	☑

Introduction to
File System Abstraction

File System Abstraction



DISK

PARTITION

FILE SYSTEM

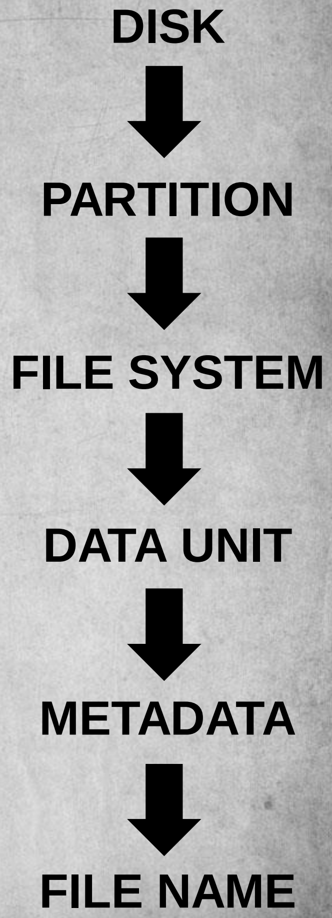
DATA UNIT

METADATA

FILE NAME

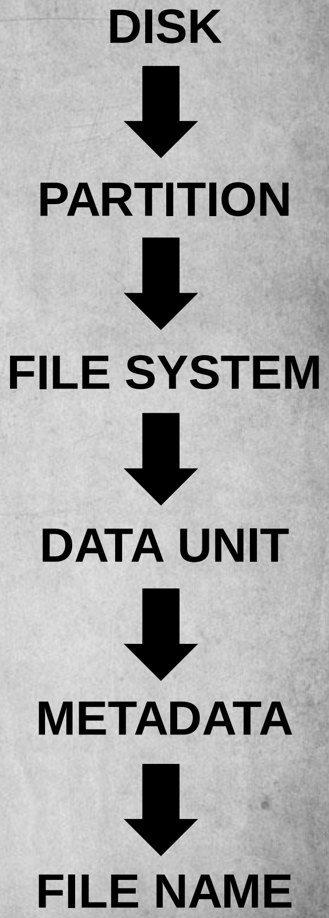
File System Abstraction

- Disk
  - ✓ Physical Storage Device
    - ○ SCSI
    - ○ SATA
    - ○ SD
- Partition
  - ✓ Logical separations for a disk
  - ✓ Partition: Single Disk
  - ✓ Volume: Multiple Disks
- File System
  - ✓ Defines partition file layout and metadata
  - ✓ Each partition / volume has a file system



File System Abstraction

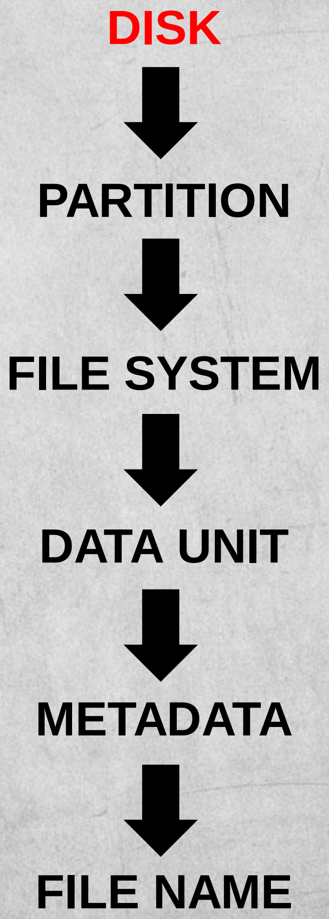
- File system model also includes:
  - ✓ Data Units
    - The smallest addressable data element
    - 512 bytes → 4 KB
  - ✓ Metadata
    - Data about data units
    - Windows
      - File ID
    - Linux
      - Inode
  - ✓ File Name
    - User space naming



DISK ↓ PARTITION ↓ FILE SYSTEM ↓ DATA UNIT ↓ METADATA ↓ FILE NAME

Storage Media Overview

File System Abstraction



DISK

PARTITION

FILE SYSTEM

DATA UNIT

METADATA

FILE NAME

Mass Storage Devices

- Mass storage divides into three main categories:
  - ✓ Magnetic Media
  - ✓ Non-Volatile Storage, Flash
  - ✓ Optical Media
- Mass storage devices have numerous device interfaces and communication protocols
  - ✓ SATA, eSATA, mSATA, IDE, NVME
  - ✓ USB-X, Thunderbolt

Magnetic Media

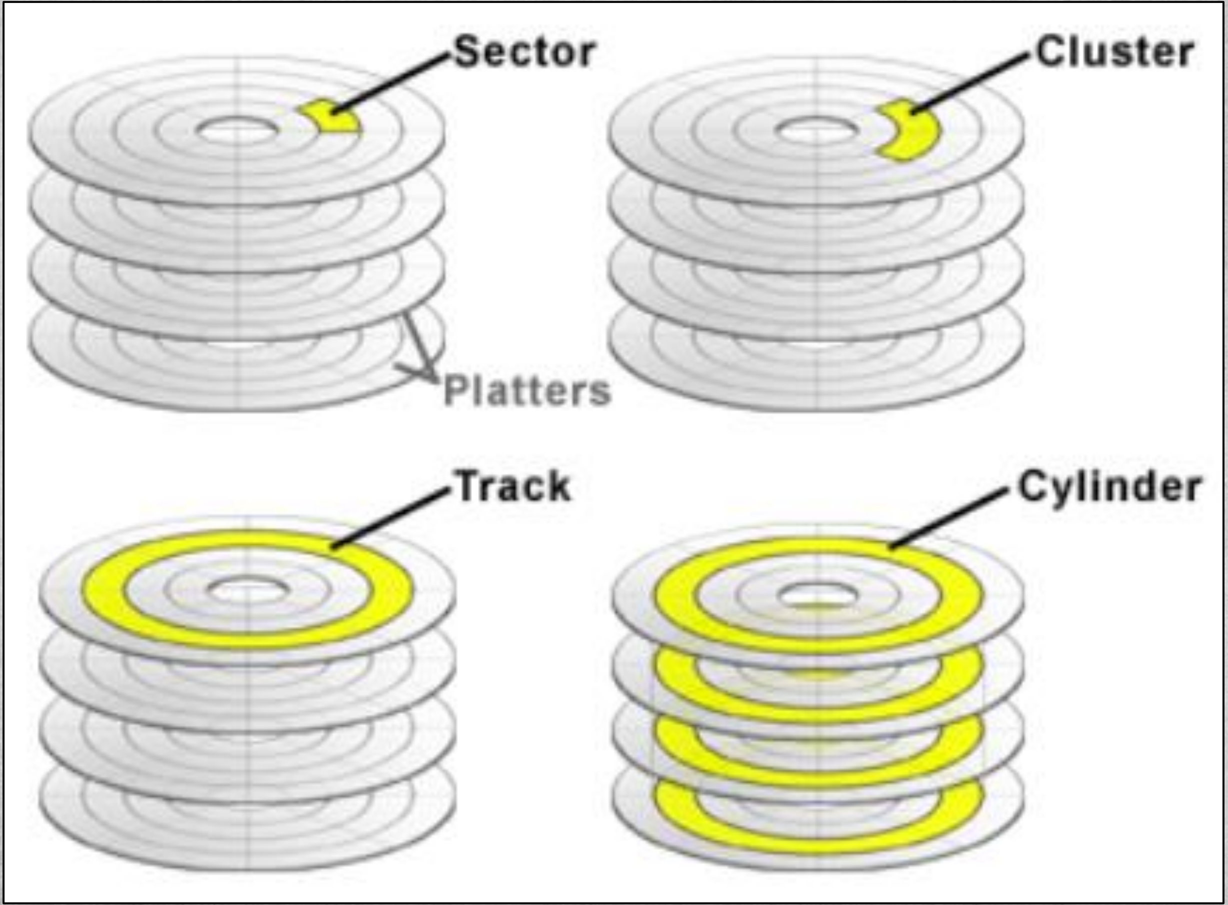
Magnetic Tapes

- Generally used for backup and archiving purposes
- Provide stable media that for long-term offline storage
- Sequential read and write, no random access
- Read and written with SCSI commands
- Once written to, each archive is marked with an end of Data (EOD) marker

Hard Disk Drives

- Traditional hard disks depend on physical geometry
  - ✓ Platter, Track, Cluster, Sector
- Storage is based on Logical Block Addresses (LBA)
- Sectors are the smallest addressable data element
  - 512 bytes → 4 KB (4Kn)
- File deletion only unlinks references to data
- Hard disk drives have “Host Protected Areas” that are inaccessible to users

Hard Disk Drive Geometry



Hard Disk Drive Forensics

- Forensic considerations when dealing with magnetic media
  - ✓ Physical vs. Logical Disks
    - Physical – Geometry
    - Logical – Partitions / Volumes
  - ✓ Address Mapping
    - Cylinder-Head-Sector (CHS)
    - Logical Block Address (LBA)
      - Physical sectors are assigned logical values creating virtual addresses for disk access
      - Hard drives have fixed address schemes between logical and physical blocks
  - ✓ Unallocated space
    - Can contain previously written data

Hard Drive Capacity

LBA 78165360

78,165,360 Sectors

×

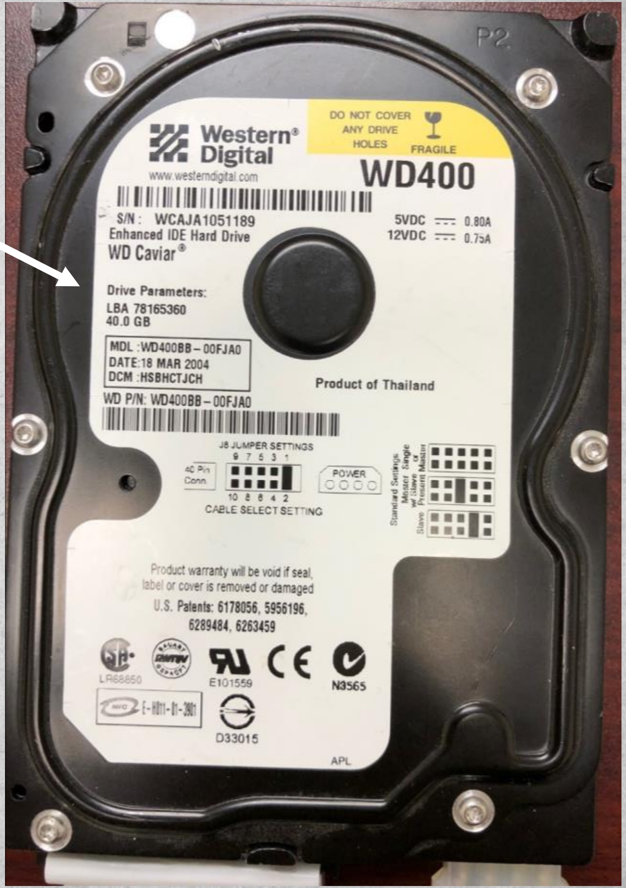
512 Bytes / Sector

40,020,664,320 Bytes

÷

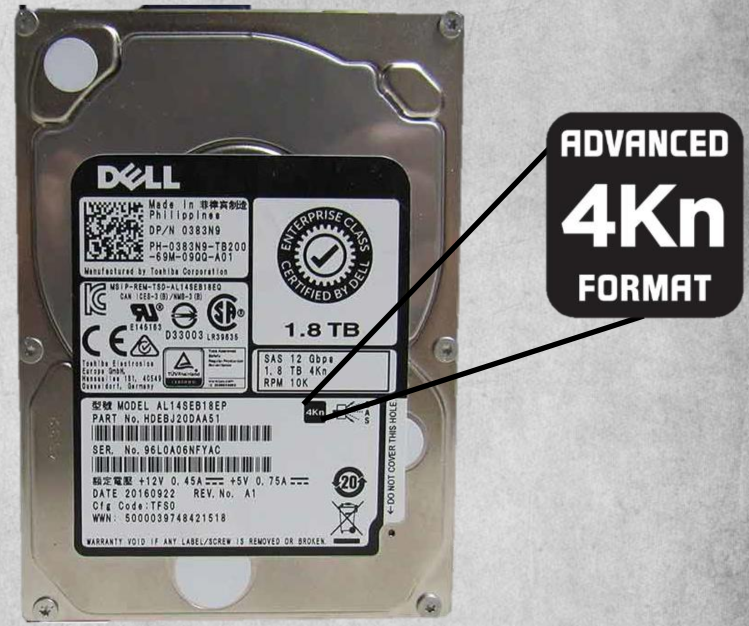
1,073,741,824 Bytes / GiB

37.3 GiB



Advanced Format 4Kn

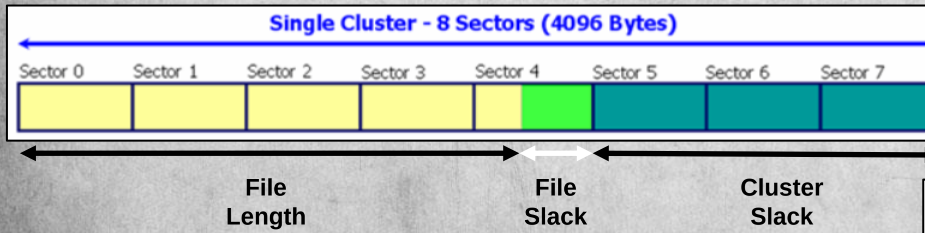
- International Disk Drive Equipment and Materials Association (IDEMA) Developed a standard to move sectors from 512 to 4096 bytes
- Most vendors started moving to the new standard in 2009, but many disks still emulate 512-byte sectors
  - ✓ 512e



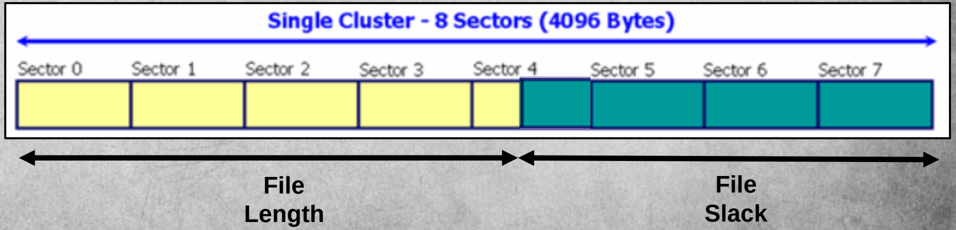
4Kn Disk Forensic Considerations

- 4Kn disks can cause difficulties in image acquisition due to several factors
  - ✓ Western Digital Advanced Format 512e disk offsets
  - ✓ Automated sector alignment
- When using 4Kn enabled disks, RAM slack and File Slack are the same since sectors are 4 KB versus 512 bytes

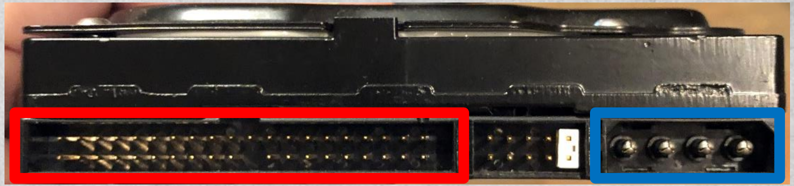
Sector – 512 bytes



Sector – 4KB



Hard Disk Drive Connectors



Integrated Drive Electronics

Molex Power

Non-Volatile Storage

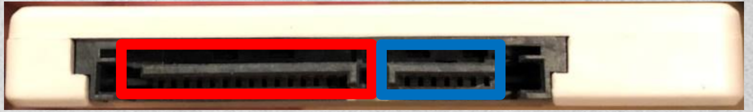
Solid State Drives

- Flash Erase Electrically Erasable Programmable Read-Only Memory (Flash) does not suffer from traditional hard disk wear
- Solid state storage devices can use AND, NOR, or NAND gates but usually NAND due to capacitance efficiencies
- TRIM command clears unallocated blocks
- SSD's are usually configured with Self-Monitoring, Analysis, and Reporting Technology (SMART)

Solid State Drive Connectors

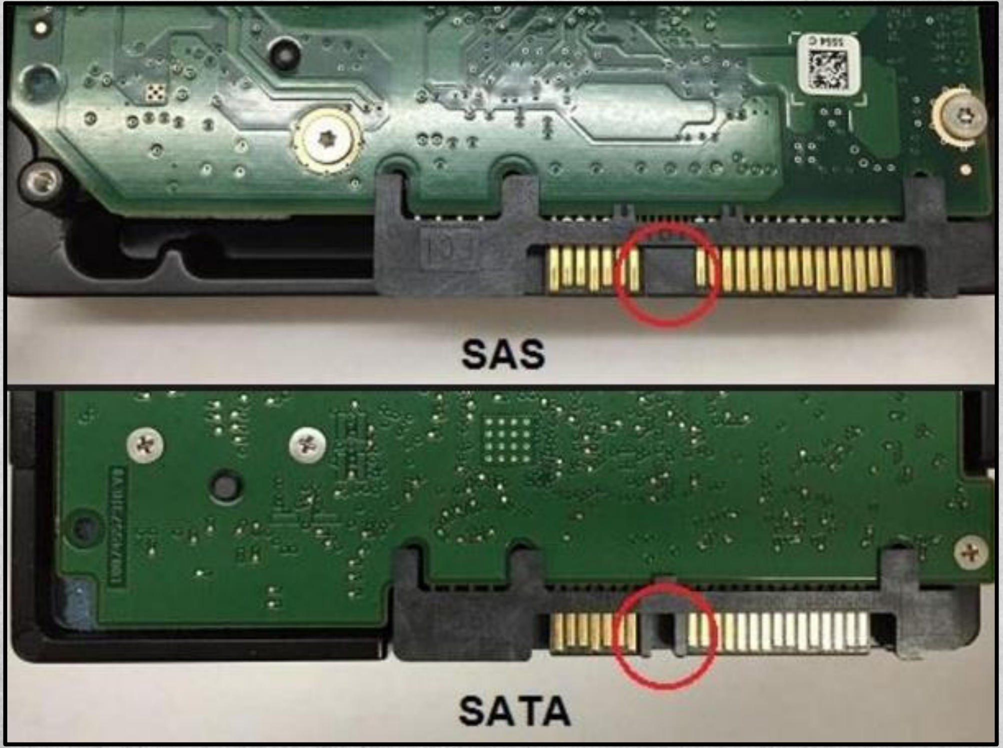
KingDian
S100
KingDian SSD 2.5"
WARNING!
Contains parts susceptible to damage by Electro-Static Discharge(ESD) Product Warranty will be VOID if label is removed
Implementation standard : Q/JDSJ 001-2017
PN: S100 16GB
SN:S101200000008536
6 935515 100027
Made in China

SATA Power



Serial Advanced Technology Attachment

SAS vs. SATA



Serial Attached Small Computer System Interface

Serial Advanced Technology Attachment

Solid State Drive Forensics

- Some forensics considerations to account for when analyzing non-volatile storage
  - ✓ Unallocated space
    - o Unlike hard disk drives, unallocated space in SSD’s are erased with TRIM to prepare for future writes which hinders data recovery
  - ✓ Address Mapping
    - o Unlike standard hard disk drives, SSD’s use dynamic addressing of logical to physical blocks

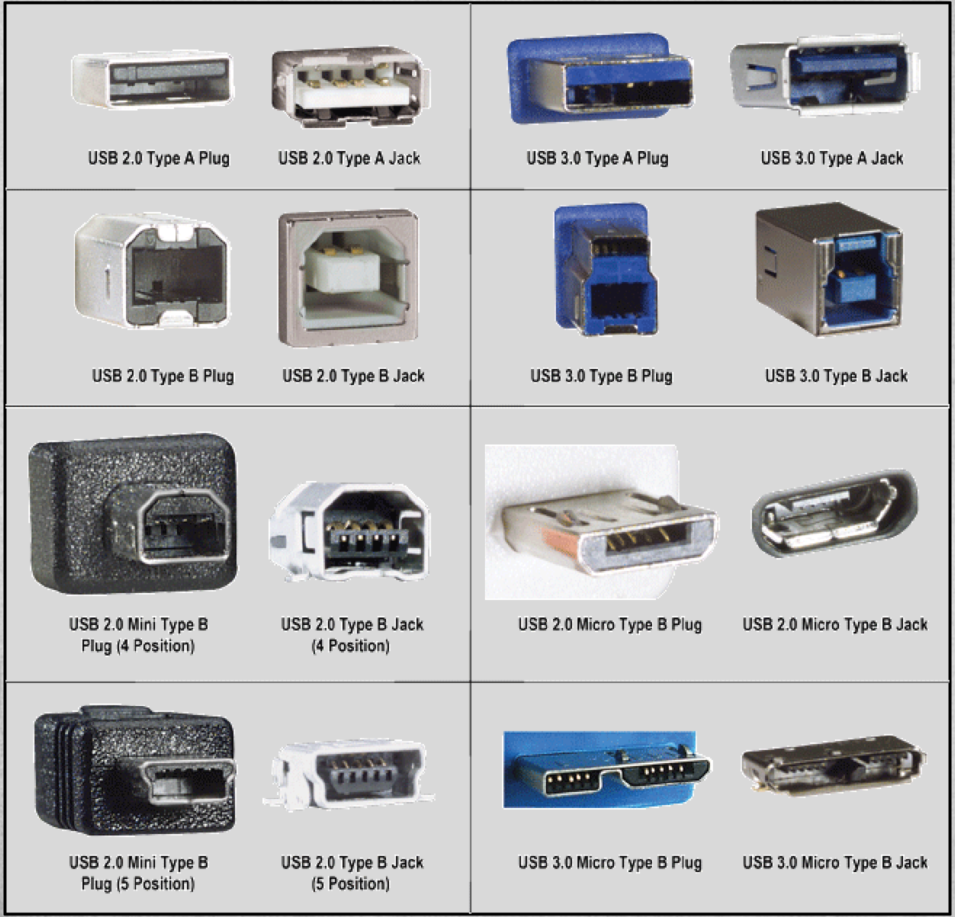
USB Flash Drives

- Universal Serial Bus is a NAND / NOR based storage technology
- USB flash drives can be formatted with most common file systems:
  - FAT
  - exFAT
  - NTFS
  - extX

USB SCSI Protocols

- USB accesses storage devices with two modes:
  - ✓ Bulk Only Transport (BOT) mode
    - o Legacy mode that sends data and commands sequential over the same channel lower
  - ✓ USB Attached SCSI Protocol (UASP) mode
    - o Advanced mode that sends multiple data and commands in parallel over multiple channels
    - o Higher performance over BOT mode and improves:
      - Asynchronous Processing
      - Improved Task Control
    - o Also known as:
      - USB3 Boost / Turbo / Extreme

USB Connectors


USB 2.0 Type A Plug
USB 2.0 Type A Jack
USB 3.0 Type A Plug
USB 3.0 Type A Jack
USB 2.0 Type B Plug
USB 2.0 Type B Jack
USB 3.0 Type B Plug
USB 3.0 Type B Jack
USB 2.0 Mini Type B Plug (4 Position)
USB 2.0 Type B Jack (4 Position)
USB 2.0 Micro Type B Plug
USB 2.0 Micro Type B Jack
USB 2.0 Mini Type B Plug (5 Position)
USB 2.0 Type B Jack (5 Position)
USB 3.0 Micro Type B Plug
USB 3.0 Micro Type B Jack

USB Flash Drive Forensic

- Flash drives can be configured with any filesystem depending on application
  - ✓FAT / exFAT / NTFS
  - ✓HFS
  - ✓extX
- Potential hiding techniques will be dependent on file system used
- USB flash drives are coded with:
  - ✓Vendor ID (VID)
  - ✓Product ID (PID)

Removable Memory Card Types

- Removable memory cards have multiple formats
  - ✓xD
    - Extreme Digital

  - ✓M2 / µSD
    - Memory Stick Micro / Micro Secure Digital

  - ✓PRO – Duo Pro
    - Sony proprietary

  - ✓MMC / SD
    - MultiMediaCard / Secure Digital

  - ✓CF
    - CompactFlash

Removable Memory Card Readers

Optical Storage Media

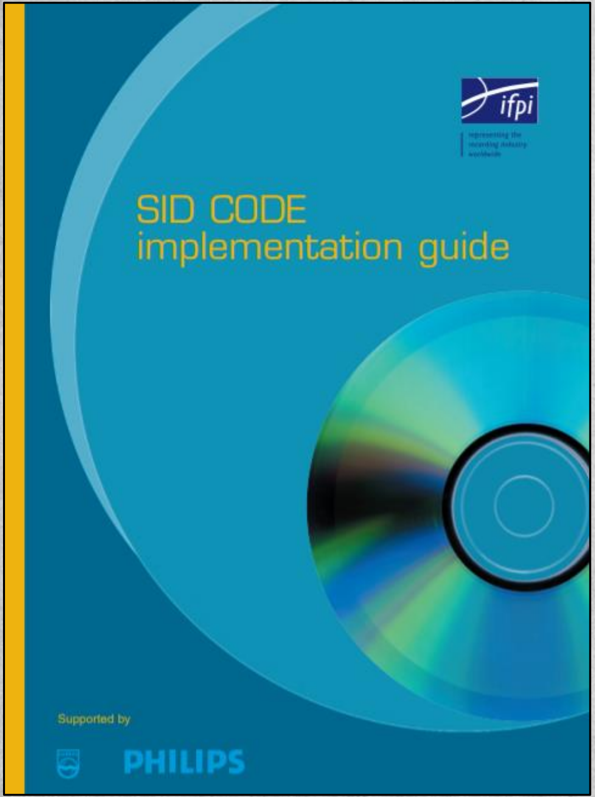
Compact Disc

- Common CD standards:
  - ✓ CD-DA – Compact Disc – Digital Audio
    - o IEC 60908 – Audio Recording – CD Digital Audio System
  - ✓ CD-ROM – Compact Disc – Read Only Memory
    - o IEC 10149 – Information Technology CD-ROM
  - ✓ CD-R – Compact Disc – Recordable (Single Write)
  - ✓ CD-RW – Compact Disc – Re-Writable (Multiple Writes)

CD-ROM File Systems

- Some of the more common CD-ROM file systems include:
  - ✓ High Sierra Format (HSF)
    - o Original PC CD-ROM standard
  - ✓ ISO 9660
    - o Updated HSF for Cross-Platform CD-ROM’s
  - ✓ Joliet
    - o ISO 9660 Extensions for Win 95+
  - ✓ Hierarchical File System (HFS)
    - o Macintosh CD-ROM standard
  - ✓ Rock Ridge
    - o ISO 9660 Extensions for Portable Operating System Interface (POSIX)
  - ✓ El Torito
    - o Bootable Disk Standard

Source Unique Identifiers



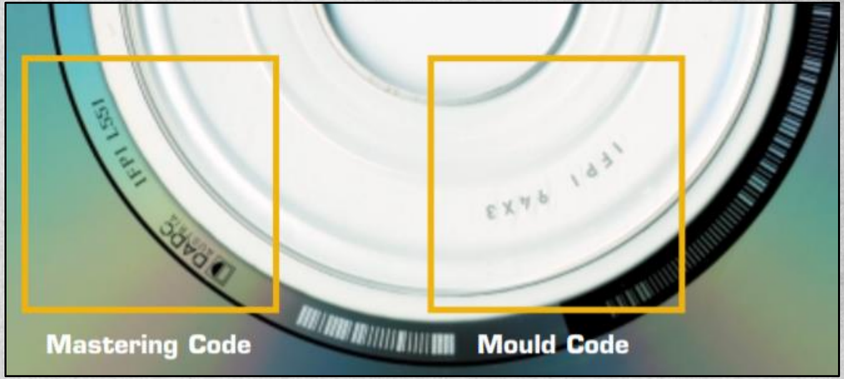
ifpi

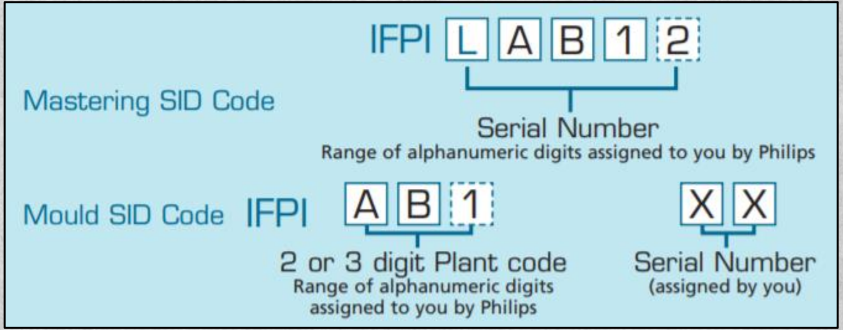
representing the recording industry worldwide

SID CODE
implementation guide

Supported by

PHILIPS





Mastering SID Code IFPI L A B 1 2

Serial Number
Range of alphanumeric digits assigned to you by Philips

Mould SID Code IFPI A B 1 X X

2 or 3 digit Plant code
Range of alphanumeric digits assigned to you by Philips

Serial Number
(assigned by you)

SID Code Reference

Digital Versatile Discs

- Single of double sided with 120-mm diameter by 1.2-mm thickness and composed of 2048-byte sectors and can be configured with Digital Rights Management (DRM) protection measures included encryption

- DVD standards have similarities to CD standards namely:
  - ✓ DVD-Video
  - ✓ DVD-ROM
  - ✓ DVD-R – DVD Recordable (Single Write)
  - ✓ DVD-RW – DVD Re-Writable (Multiple Writes)

Digital Versatile Discs

- In contrast to CD standards, DVD standards also include:
  - ✓ DVD-RAM
    - Written to and erased repeatedly, but only accessed with a DVD-RAM drive
  - ✓ DVD+R
    - DVD Recordable (Single Write)
  - ✓ DVD+RW
    - DVD Re-Writable (Multiple Writes)

- DVDs use Universal Disk Format (UDF) filesystem
  - ✓ Replacement for ISO9660

Blue-Ray Discs

- Just like CD and DVD discs, blue-ray has 2048-byte sectors
- Blue-Ray disc (BD) types:
  - ✓ BD-ROM
  - ✓ BD-R – Blue-Ray Recordable (Single Write)
  - ✓ BD-RE - Blue-Ray Re-Writable (Multiple Write)
  - ✓ BD-XL - Blue-Ray Double Capacity Re-Writable (Multiple Write)
- Just like DVDs, blue-ray discs use UDF file system and can be configured with DRM protections including encryption

Optical Storage Forensics

- Optical disks contain 2048-byte sectors that can be read directly and without the need of a write blocker

- In contrast to other storage media, optical media utilizes unique identifiers
  - ✓ International Federation of Phonographic Industry (IFPI)
  - ✓ Source Unique Identifier (SID)
    - Physical disc stamp indicating production facility
  - ✓ Recorder Identification Code (RIC)
    - Links a burned CD to the drive that created it

Additional Storage Media

Additional Media Types

Mini-SATA (mSATA)

M.2

Micro SATA (uSATA)

Non-Volatile Memory Express (NVME)

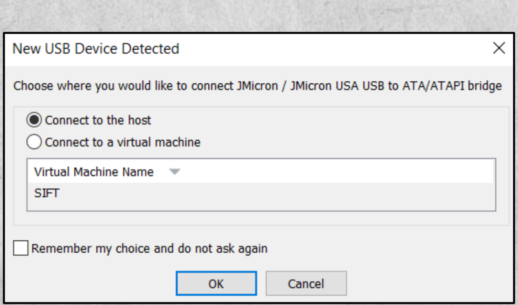
NVME Forensic Considerations

- Although NVME-based disks are block devices, they cannot be accessed in the same method as a SCSI-based disk since the protocols are different
  - ✓ /dev/sdX vs. /dev/nvmeXnX
- NVME use is relatively new and there have been additions to write-blockers to collect NVME-based disk images

Media Detection and Configuration

External Media Detection

- Connect drive to host
- Connect drive to guest
- Available devices
- Auto mount vs. read only
- Write blocking

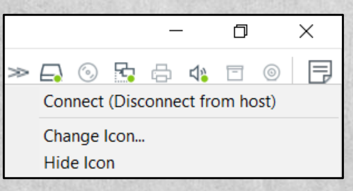

New USB Device Detected

Choose where you would like to connect JMicron / JMicron USA USB to ATA/ATAPI bridge

● Connect to the host
○ Connect to a virtual machine

Virtual Machine Name
SIFT

□ Remember my choice and do not ask again



Media Detection and Access

- With an initial introduction to media complete, we will now evaluate forensics tools built into SIFT Workstation
- The following Linux locations and commands provide information about attached media:

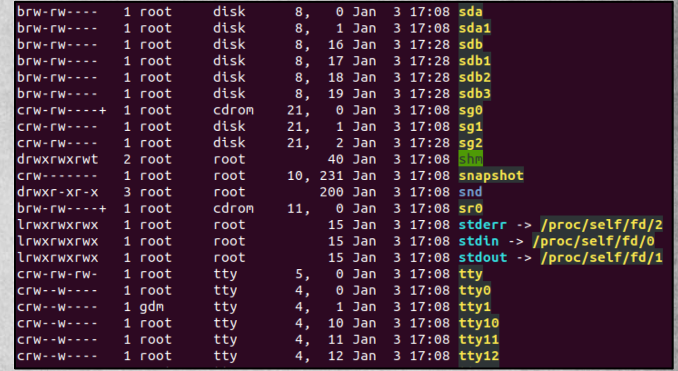
- ✓ /dev
  - Device file repository
- ✓ dmesg
  - Kernel level driver messages
- ✓ lsblk
  - List block devices
- ✓ blockdev
  - Block device system calls
- ✓ lsscsi
  - List SCSI disk attributes
- ✓ lsusb
  - List USB buses
- ✓ fdisk
  - Disk format
- ✓ df
  - Disk space
- ✓ hdparm
  - Display and set drive parameters
- ✓ hexdump (xxd)
  - Dump file contents in hex

/dev

- /dev directory contains device drivers
  - ✓ Additional information is available in /sys

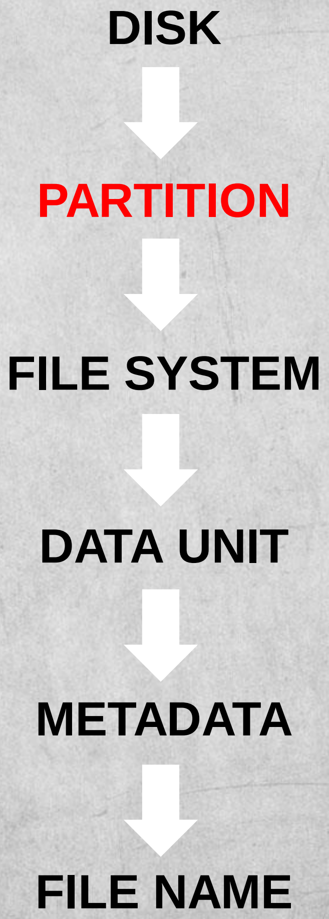
- Devices are characterized as either:
  - ✓ Character devices – c
    - ○ ttyX – Terminal
    - ○ snapshot – System memory snapshot
  - ✓ Block Devices – b
    - ○ loopX – Loopback device
    - ○ sdX – SCSI disk device
    - ○ nvmeXnX – NVME disk device

- Linux Allocated Devices Reference



```
brw-rw----   1 root     disk      8,   0 Jan  3 17:08 sda
brw-rw----   1 root     disk      8,   1 Jan  3 17:08 sda1
brw-rw----   1 root     disk      8,  16 Jan  3 17:28 sdb
brw-rw----   1 root     disk      8,  17 Jan  3 17:28 sdb1
brw-rw----   1 root     disk      8,  18 Jan  3 17:28 sdb2
brw-rw----   1 root     disk      8,  19 Jan  3 17:28 sdb3
crw-rw----+  1 root     cdrom    21,   0 Jan  3 17:08 sg0
crw-rw----   1 root     disk     21,   1 Jan  3 17:08 sg1
crw-rw----   1 root     disk     21,   2 Jan  3 17:28 sg2
drwxrwxrwt   2 root     root          40 Jan  3 17:08 shm
crw-------   1 root     root     10, 231 Jan  3 17:08 snapshot
drwxr-xr-x   3 root     root         200 Jan  3 17:08 snd
brw-rw----+  1 root     cdrom    11,   0 Jan  3 17:08 sr0
lrwxrwxrwx   1 root     root          15 Jan  3 17:08 stderr -> /proc/self/fd/2
lrwxrwxrwx   1 root     root          15 Jan  3 17:08 stdin -> /proc/self/fd/0
lrwxrwxrwx   1 root     root          15 Jan  3 17:08 stdout -> /proc/self/fd/1
crw-rw-rw-   1 root     tty       5,   0 Jan  3 17:08 tty
crw--w----   1 root     tty       4,   0 Jan  3 17:08 tty0
crw--w----   1 gdm      tty       4,   1 Jan  3 17:08 tty1
crw--w----   1 root     tty       4,  10 Jan  3 17:08 tty10
crw--w----   1 root     tty       4,  11 Jan  3 17:08 tty11
crw--w----   1 root     tty       4,  12 Jan  3 17:08 tty12
```

File System Abstraction



DISK

PARTITION

FILE SYSTEM

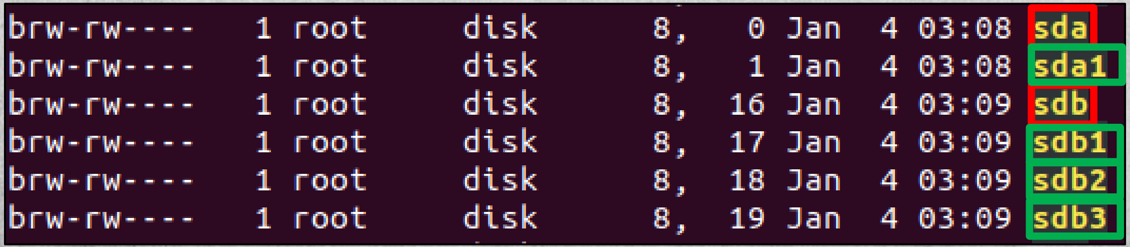
DATA UNIT

METADATA

FILE NAME

Disks and Partitions

- The file system abstraction layer identifies disks and associated partitions
- SCSI device files listing disks and partitions
  - Disks
    - /dev/sda – First Disk
    - /dev/sdb – Second Disk
  - Partitions
    - /dev/sda1 – First Disk, First Partition
    - /dev/sdb1 – Second Disk, First Partition
    - /dev/sdb2 – Second Disk, Second Partition
    - /dev/sdb3 – Second Disk, Third Partition

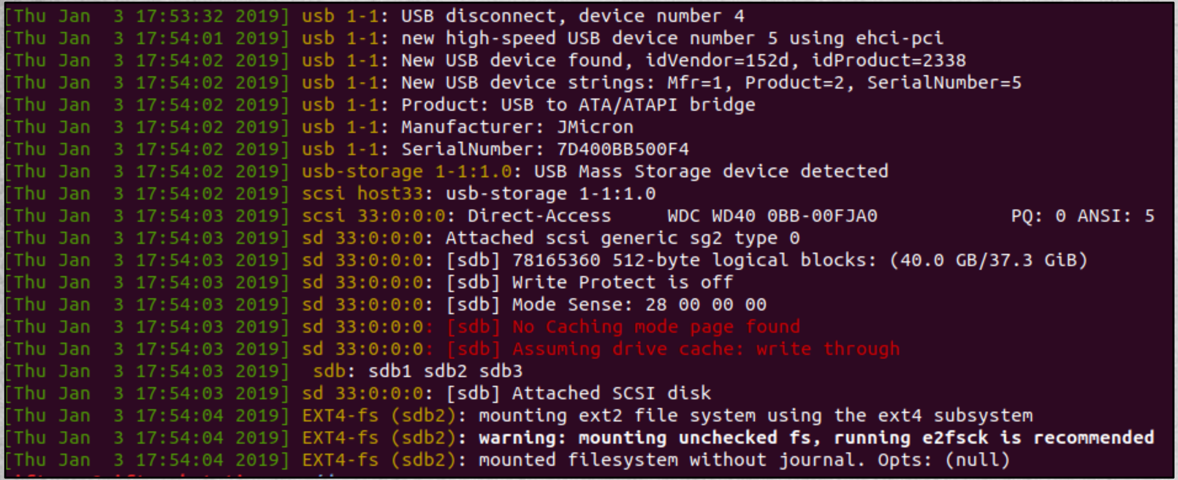


```
brw-rw----   1 root     disk      8,   0 Jan  4 03:08 sda
brw-rw----   1 root     disk      8,   1 Jan  4 03:08 sda1
brw-rw----   1 root     disk      8,  16 Jan  4 03:09 sdb
brw-rw----   1 root     disk      8,  17 Jan  4 03:09 sdb1
brw-rw----   1 root     disk      8,  18 Jan  4 03:09 sdb2
brw-rw----   1 root     disk      8,  19 Jan  4 03:09 sdb3
```

dmesg

- Print or control the kernel ring buffer which is responsible for recording kernel level driver messages
- All system changes can be displayed in real time
- Examples:
  - ✓ dmesg
    - o Displays kernel level driver messages
  - ✓ dmesg -T | grep sd
    - o Displays messages relative to disk events with local time and filters on scsi disk devices

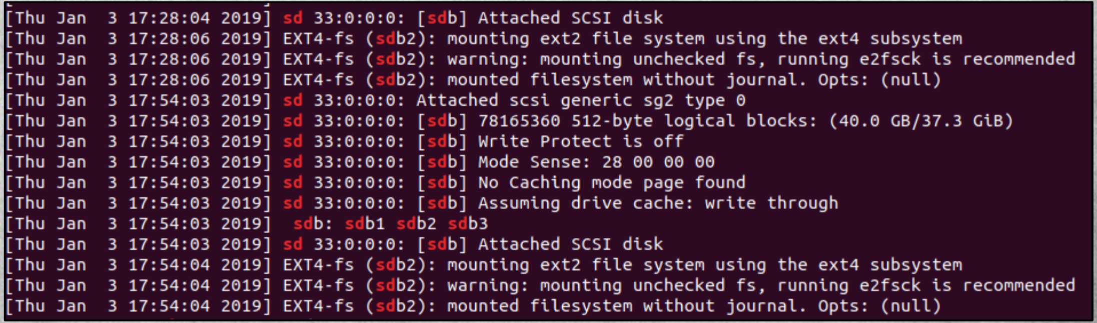
dmesg – Time and Drive Information



```
[Thu Jan  3 17:53:32 2019] usb 1-1: USB disconnect, device number 4
[Thu Jan  3 17:54:01 2019] usb 1-1: new high-speed USB device number 5 using ehci-pci
[Thu Jan  3 17:54:02 2019] usb 1-1: New USB device found, idVendor=152d, idProduct=2338
[Thu Jan  3 17:54:02 2019] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=5
[Thu Jan  3 17:54:02 2019] usb 1-1: Product: USB to ATA/ATAPI bridge
[Thu Jan  3 17:54:02 2019] usb 1-1: Manufacturer: JMicron
[Thu Jan  3 17:54:02 2019] usb 1-1: SerialNumber: 7D400BB500F4
[Thu Jan  3 17:54:02 2019] usb-storage 1-1:1.0: USB Mass Storage device detected
[Thu Jan  3 17:54:02 2019] scsi host33: usb-storage 1-1:1.0
[Thu Jan  3 17:54:03 2019] scsi 33:0:0:0: Direct-Access     WDC WD40 0BB-00FJA0          PQ: 0 ANSI: 5
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: Attached scsi generic sg2 type 0
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] 78165360 512-byte logical blocks: (40.0 GB/37.3 GiB)
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Write Protect is off
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Mode Sense: 28 00 00 00
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] No Caching mode page found
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Assuming drive cache: write through
[Thu Jan  3 17:54:03 2019]  sdb: sdb1 sdb2 sdb3
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Attached SCSI disk
[Thu Jan  3 17:54:04 2019] EXT4-fs (sdb2): mounting ext2 file system using the ext4 subsystem
[Thu Jan  3 17:54:04 2019] EXT4-fs (sdb2): warning: mounting unchecked fs, running e2fsck is recommended
[Thu Jan  3 17:54:04 2019] EXT4-fs (sdb2): mounted filesystem without journal. Opts: (null)
```

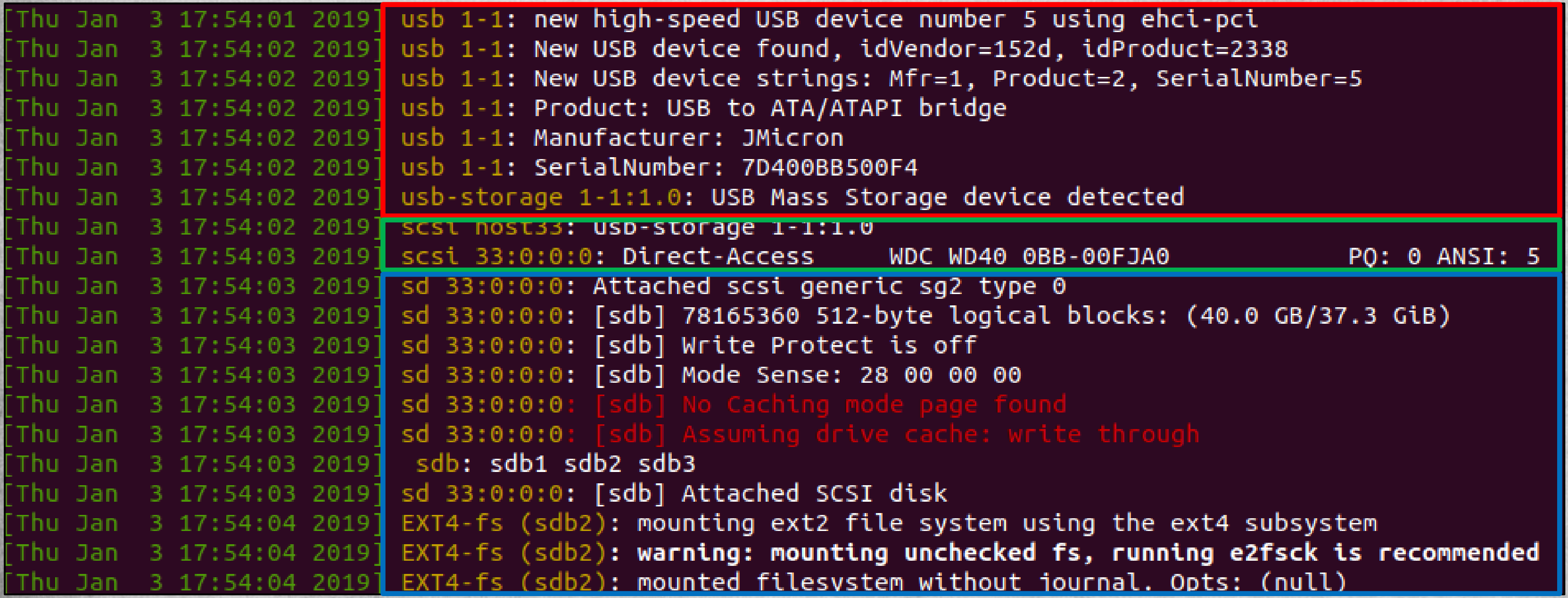
dmesg -T

dmesg –T | grep sd



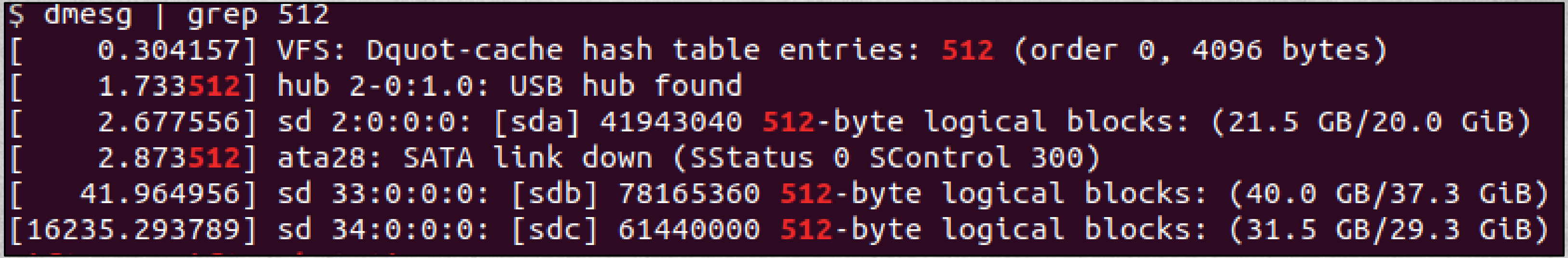
```
[Thu Jan  3 17:28:04 2019] sd 33:0:0:0: [sdb] Attached SCSI disk
[Thu Jan  3 17:28:06 2019] EXT4-fs (sdb2): mounting ext2 file system using the ext4 subsystem
[Thu Jan  3 17:28:06 2019] EXT4-fs (sdb2): warning: mounting unchecked fs, running e2fsck is recommended
[Thu Jan  3 17:28:06 2019] EXT4-fs (sdb2): mounted filesystem without journal. Opts: (null)
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: Attached scsi generic sg2 type 0
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] 78165360 512-byte logical blocks: (40.0 GB/37.3 GiB)
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Write Protect is off
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Mode Sense: 28 00 00 00
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] No Caching mode page found
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Assuming drive cache: write through
[Thu Jan  3 17:54:03 2019]  sdb: sdb1 sdb2 sdb3
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Attached SCSI disk
[Thu Jan  3 17:54:04 2019] EXT4-fs (sdb2): mounting ext2 file system using the ext4 subsystem
[Thu Jan  3 17:54:04 2019] EXT4-fs (sdb2): warning: mounting unchecked fs, running e2fsck is recommended
[Thu Jan  3 17:54:04 2019] EXT4-fs (sdb2): mounted filesystem without journal. Opts: (null)
```

dmesg Event Order



```
[Thu Jan  3 17:54:01 2019] usb 1-1: new high-speed USB device number 5 using ehci-pci
[Thu Jan  3 17:54:02 2019] usb 1-1: New USB device found, idVendor=152d, idProduct=2338
[Thu Jan  3 17:54:02 2019] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=5
[Thu Jan  3 17:54:02 2019] usb 1-1: Product: USB to ATA/ATAPI bridge
[Thu Jan  3 17:54:02 2019] usb 1-1: Manufacturer: JMicron
[Thu Jan  3 17:54:02 2019] usb 1-1: SerialNumber: 7D400BB500F4
[Thu Jan  3 17:54:02 2019] usb-storage 1-1:1.0: USB Mass Storage device detected
[Thu Jan  3 17:54:02 2019] scsi host33: usb-storage 1-1:1.0
[Thu Jan  3 17:54:03 2019] scsi 33:0:0:0: Direct-Access     WDC WD40 0BB-00FJA0            PQ: 0 ANSI: 5
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: Attached scsi generic sg2 type 0
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] 78165360 512-byte logical blocks: (40.0 GB/37.3 GiB)
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Write Protect is off
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Mode Sense: 28 00 00 00
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] No Caching mode page found
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Assuming drive cache: write through
[Thu Jan  3 17:54:03 2019]  sdb: sdb1 sdb2 sdb3
[Thu Jan  3 17:54:03 2019] sd 33:0:0:0: [sdb] Attached SCSI disk
[Thu Jan  3 17:54:04 2019] EXT4-fs (sdb2): mounting ext2 file system using the ext4 subsystem
[Thu Jan  3 17:54:04 2019] EXT4-fs (sdb2): warning: mounting unchecked fs, running e2fsck is recommended
[Thu Jan  3 17:54:04 2019] EXT4-fs (sdb2): mounted filesystem without journal. Opts: (null)
```

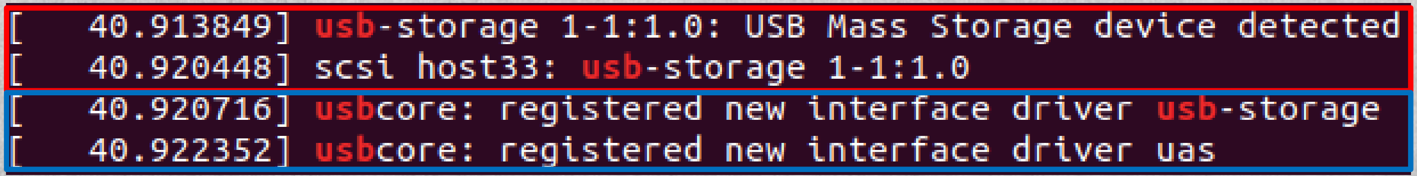
dmesg – Sector Sizes



```
$ dmesg | grep 512
[    0.304157] VFS: Dquot-cache hash table entries: 512 (order 0, 4096 bytes)
[    1.733512] hub 2-0:1.0: USB hub found
[    2.677556] sd 2:0:0:0: [sda] 41943040 512-byte logical blocks: (21.5 GB/20.0 GiB)
[    2.873512] ata28: SATA link down (SStatus 0 SControl 300)
[   41.964956] sd 33:0:0:0: [sdb] 78165360 512-byte logical blocks: (40.0 GB/37.3 GiB)
[16235.293789] sd 34:0:0:0: [sdc] 61440000 512-byte logical blocks: (31.5 GB/29.3 GiB)
```

dmesg - USB BOT vs. UASP Mode

- USB BOT Interface
  - ✓ usb-storage
- USB UASP Interface
  - ✓ uas
- The legacy BOT mode does not affect forensic collection or device hashes



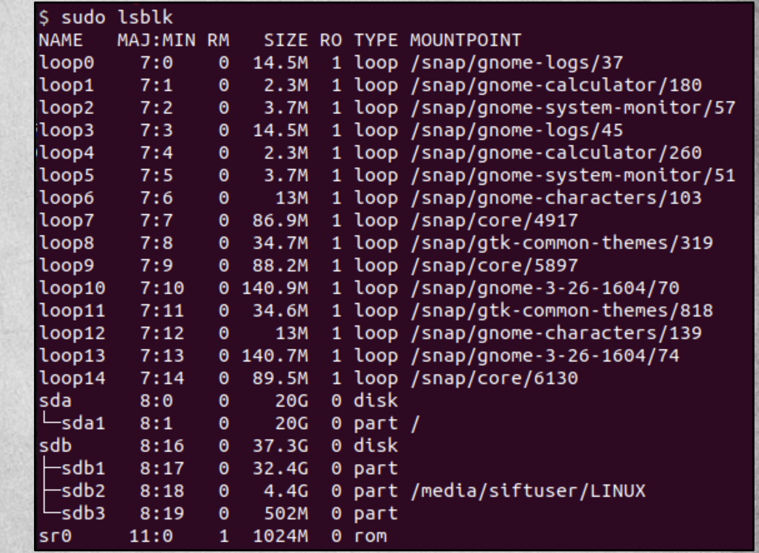
```
[   40.913849] usb-storage 1-1:1.0: USB Mass Storage device detected
[   40.920448] scsi host33: usb-storage 1-1:1.0
[   40.920716] usbcore: registered new interface driver usb-storage
[   40.922352] usbcore: registered new interface driver uas
```

BOT

UASP

lsblk

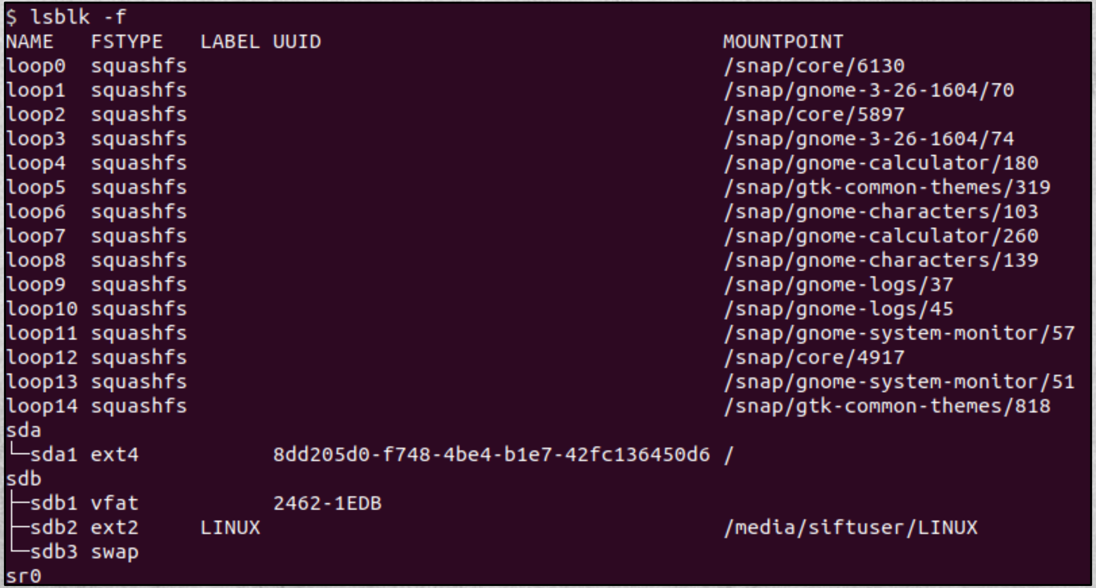
- lsblk lists all available block devices
- Reads the sysfs filesystem and udev database
- If udev is not available or lsblk is compiled without udev it reads LABELs, UUIDs and filesystem types from the block device
- Root permissions are necessary
  - ✓ sudo lsblk
- Lists all block devices, except RAM disks, in a tree-like format by default



```
$ sudo lsblk
NAME    MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
loop0     7:0    0  14.5M  1 loop /snap/gnome-logs/37
loop1     7:1    0   2.3M  1 loop /snap/gnome-calculator/180
loop2     7:2    0   3.7M  1 loop /snap/gnome-system-monitor/57
loop3     7:3    0  14.5M  1 loop /snap/gnome-logs/45
loop4     7:4    0   2.3M  1 loop /snap/gnome-calculator/260
loop5     7:5    0   3.7M  1 loop /snap/gnome-system-monitor/51
loop6     7:6    0    13M  1 loop /snap/gnome-characters/103
loop7     7:7    0  86.9M  1 loop /snap/core/4917
loop8     7:8    0  34.7M  1 loop /snap/gtk-common-themes/319
loop9     7:9    0  88.2M  1 loop /snap/core/5897
loop10    7:10   0 140.9M  1 loop /snap/gnome-3-26-1604/70
loop11    7:11   0  34.6M  1 loop /snap/gtk-common-themes/818
loop12    7:12   0    13M  1 loop /snap/gnome-characters/139
loop13    7:13   0 140.7M  1 loop /snap/gnome-3-26-1604/74
loop14    7:14   0  89.5M  1 loop /snap/core/6130
sda       8:0    0    20G  0 disk
└─sda1    8:1    0    20G  0 part /
sdb       8:16   0  37.3G  0 disk
├─sdb1    8:17   0  32.4G  0 part
├─sdb2    8:18   0   4.4G  0 part /media/siftuser/LINUX
└─sdb3    8:19   0   502M  0 part
sr0      11:0    1  1024M  0 rom
```

lsblk – Filesystem Information

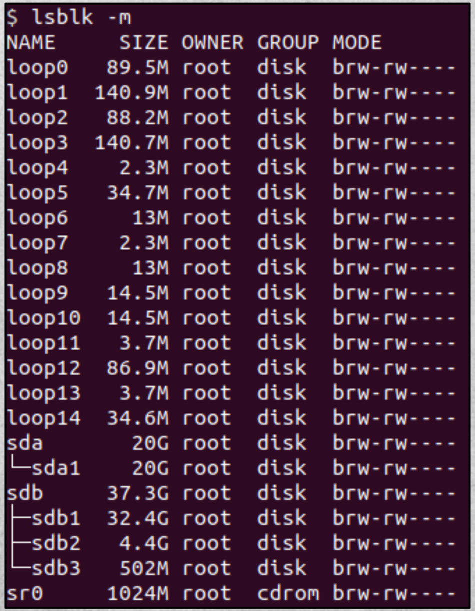
- lsblk –f lists all currently mounted filesystems
- Output for partition is shown as a tree



```
$ lsblk -f
NAME   FSTYPE   LABEL UUID                                 MOUNTPOINT
loop0  squashfs                                            /snap/core/6130
loop1  squashfs                                            /snap/gnome-3-26-1604/70
loop2  squashfs                                            /snap/core/5897
loop3  squashfs                                            /snap/gnome-3-26-1604/74
loop4  squashfs                                            /snap/gnome-calculator/180
loop5  squashfs                                            /snap/gtk-common-themes/319
loop6  squashfs                                            /snap/gnome-characters/103
loop7  squashfs                                            /snap/gnome-calculator/260
loop8  squashfs                                            /snap/gnome-characters/139
loop9  squashfs                                            /snap/gnome-logs/37
loop10 squashfs                                            /snap/gnome-logs/45
loop11 squashfs                                            /snap/gnome-system-monitor/57
loop12 squashfs                                            /snap/core/4917
loop13 squashfs                                            /snap/gnome-system-monitor/51
loop14 squashfs                                            /snap/gtk-common-themes/818
sda
└─sda1 ext4           8dd205d0-f748-4be4-b1e7-42fc136450d6 /
sdb
├─sdb1 vfat           2462-1EDB
├─sdb2 ext2     LINUX                                      /media/siftuser/LINUX
└─sdb3 swap
sr0
```

lsblk – Device Owner, Group, and Mode

- lsblk -m lists device owners, groups, and modes
- Modes shows permissions for owners, groups, and world



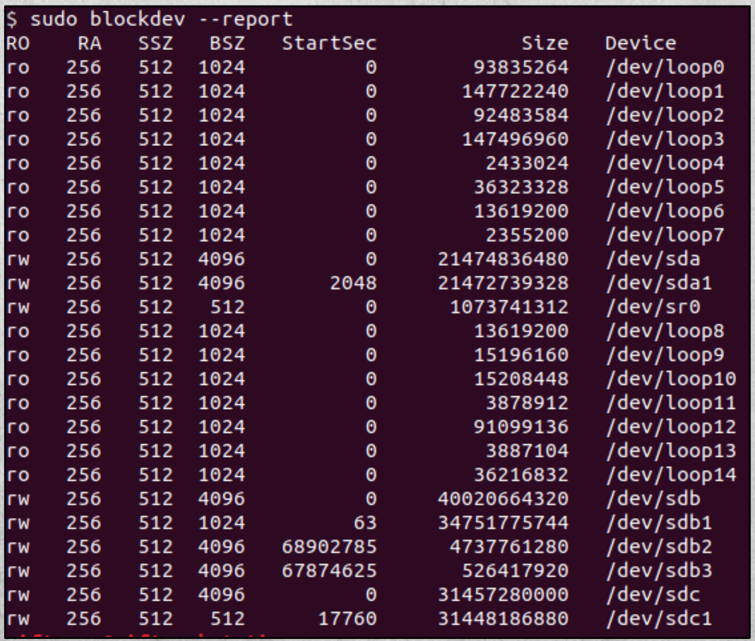
```
$ lsblk -m
NAME      SIZE OWNER GROUP MODE
loop0    89.5M root  disk  brw-rw----
loop1   140.9M root  disk  brw-rw----
loop2    88.2M root  disk  brw-rw----
loop3   140.7M root  disk  brw-rw----
loop4     2.3M root  disk  brw-rw----
loop5    34.7M root  disk  brw-rw----
loop6      13M root  disk  brw-rw----
loop7     2.3M root  disk  brw-rw----
loop8      13M root  disk  brw-rw----
loop9    14.5M root  disk  brw-rw----
loop10   14.5M root  disk  brw-rw----
loop11    3.7M root  disk  brw-rw----
loop12   86.9M root  disk  brw-rw----
loop13    3.7M root  disk  brw-rw----
loop14   34.6M root  disk  brw-rw----
sda        20G root  disk  brw-rw----
└─sda1     20G root  disk  brw-rw----
sdb      37.3G root  disk  brw-rw----
├─sdb1   32.4G root  disk  brw-rw----
├─sdb2    4.4G root  disk  brw-rw----
└─sdb3    502M root  disk  brw-rw----
sr0     1024M root  cdrom brw-rw----
```

blockdev

- blockdev is a system call directly to block devices
- blockdev switches include:
  - ✓ --getalignoff
    - Get alignment offset
  - ✓ --getfra
    - Get filesystem readahead in 512-byte sectors
  - ✓ --getsize64
    - Print device size in bytes.
  - ✓ --rereadpt
    - Reread partition table
  - ✓ --report
    - Create a report of all block devices

blockdev Report

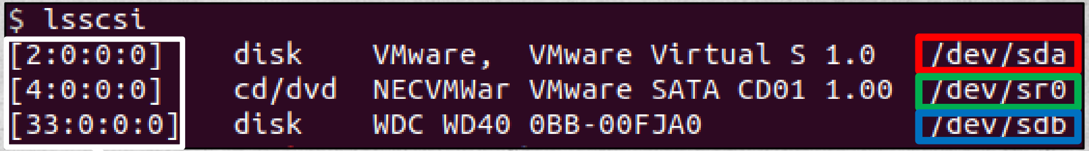
- Reports read only status, sector size, block size, starting sectors, and overall disk size



```
$ sudo blockdev --report
RO    RA   SSZ   BSZ   StartSec            Size   Device
ro   256   512  1024          0        93835264   /dev/loop0
ro   256   512  1024          0       147722240   /dev/loop1
ro   256   512  1024          0        92483584   /dev/loop2
ro   256   512  1024          0       147496960   /dev/loop3
ro   256   512  1024          0         2433024   /dev/loop4
ro   256   512  1024          0        36323328   /dev/loop5
ro   256   512  1024          0        13619200   /dev/loop6
ro   256   512  1024          0         2355200   /dev/loop7
rw   256   512  4096          0     21474836480   /dev/sda
rw   256   512  4096       2048     21472739328   /dev/sda1
rw   256   512   512          0      1073741312   /dev/sr0
ro   256   512  1024          0        13619200   /dev/loop8
ro   256   512  1024          0        15196160   /dev/loop9
ro   256   512  1024          0        15208448   /dev/loop10
ro   256   512  1024          0         3878912   /dev/loop11
ro   256   512  1024          0        91099136   /dev/loop12
ro   256   512  1024          0         3887104   /dev/loop13
ro   256   512  1024          0        36216832   /dev/loop14
rw   256   512  4096          0     40020664320   /dev/sdb
rw   256   512  1024         63     34751775744   /dev/sdb1
rw   256   512  4096   68902785      4737761280   /dev/sdb2
rw   256   512  4096   67874625       526417920   /dev/sdb3
rw   256   512  4096          0     31457280000   /dev/sdc
rw   256   512   512      17760     31448186880   /dev/sdc1
```

lsscsi

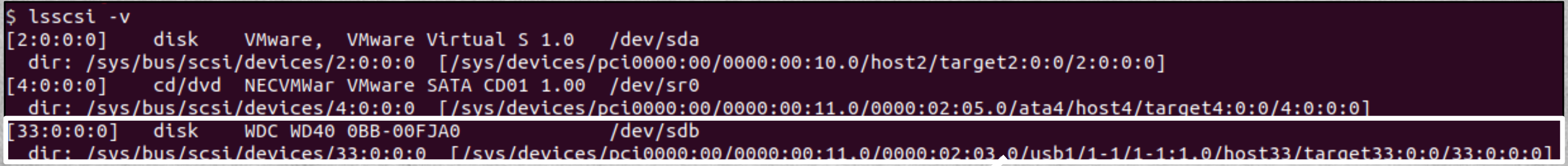
- While lsblk shows all block devices the use of lsscsi shows SCSI specific device attributes
  - ✓ Disks
  - ✓ Printers



```
$ lsscsi
[2:0:0:0]    disk    VMware,  VMware Virtual S 1.0   /dev/sda
[4:0:0:0]    cd/dvd  NECVMWar VMware SATA CD01 1.00  /dev/sr0
[33:0:0:0]   disk    WDC WD40 0BB-00FJA0             /dev/sdb
```

SIFT Drive
SCSI CD-ROM
External Drive

[Host Adapter ID:SCSI Channel:ID:Logical Unit Number]

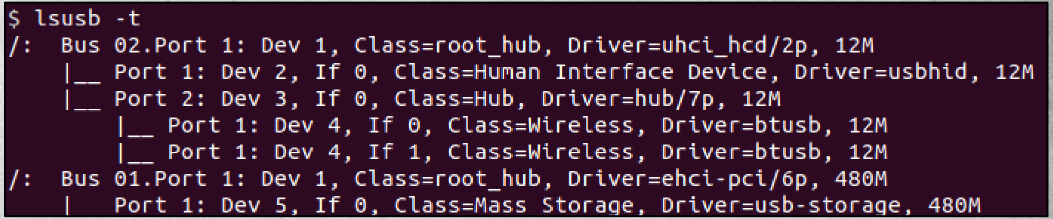


```
$ lsscsi -v
[2:0:0:0]    disk    VMware,  VMware Virtual S 1.0   /dev/sda
  dir: /sys/bus/scsi/devices/2:0:0:0  [/sys/devices/pci0000:00/0000:00:10.0/host2/target2:0:0/2:0:0:0]
[4:0:0:0]    cd/dvd  NECVMWar VMware SATA CD01 1.00  /dev/sr0
  dir: /sys/bus/scsi/devices/4:0:0:0  [/sys/devices/pci0000:00/0000:00:11.0/0000:02:05.0/ata4/host4/target4:0:0/4:0:0:0]
[33:0:0:0]   disk    WDC WD40 0BB-00FJA0             /dev/sdb
  dir: /sys/bus/scsi/devices/33:0:0:0  [/sys/devices/pci0000:00/0000:00:11.0/0000:02:03.0/usb1/1-1/1-1:1.0/host33/target33:0:0/33:0:0:0]
```

dir: /sys/bus/scsi/devices/33:0:0:0

lsusb

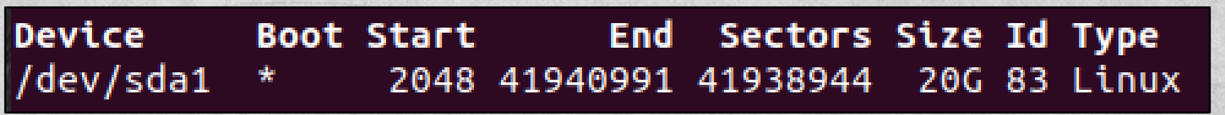
- Utility for displaying information about USB buses in the system and the devices connected to them
- Switch examples:
  - ✓ lsusb -v
    - Verbose output
  - ✓ lsusb -s 001
    - Show only devices in a specified bus
  - ✓ lsusb -t
    - Dump physical USB device hierarchy as a tree



```
$ lsusb -t
/:  Bus 02.Port 1: Dev 1, Class=root_hub, Driver=uhci_hcd/2p, 12M
    |__ Port 1: Dev 2, If 0, Class=Human Interface Device, Driver=usbhid, 12M
    |__ Port 2: Dev 3, If 0, Class=Hub, Driver=hub/7p, 12M
        |__ Port 1: Dev 4, If 0, Class=Wireless, Driver=btusb, 12M
        |__ Port 1: Dev 4, If 1, Class=Wireless, Driver=btusb, 12M
/:  Bus 01.Port 1: Dev 1, Class=root_hub, Driver=ehci-pci/6p, 480M
    |   Port 1: Dev 5, If 0, Class=Mass Storage, Driver=usb-storage, 480M
```

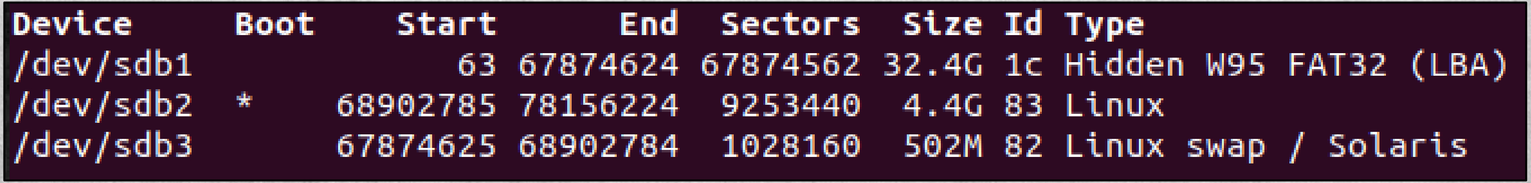
fdisk

- fdisk, short for format disk, is a tool that lists, creates, and manipulates disk partition tables
- Each partition displays start and end sectors which identifies where data for that partition reside



```
Device     Boot Start      End  Sectors Size Id Type
/dev/sda1  *     2048 41940991 41938944  20G 83 Linux
```

Single Partition

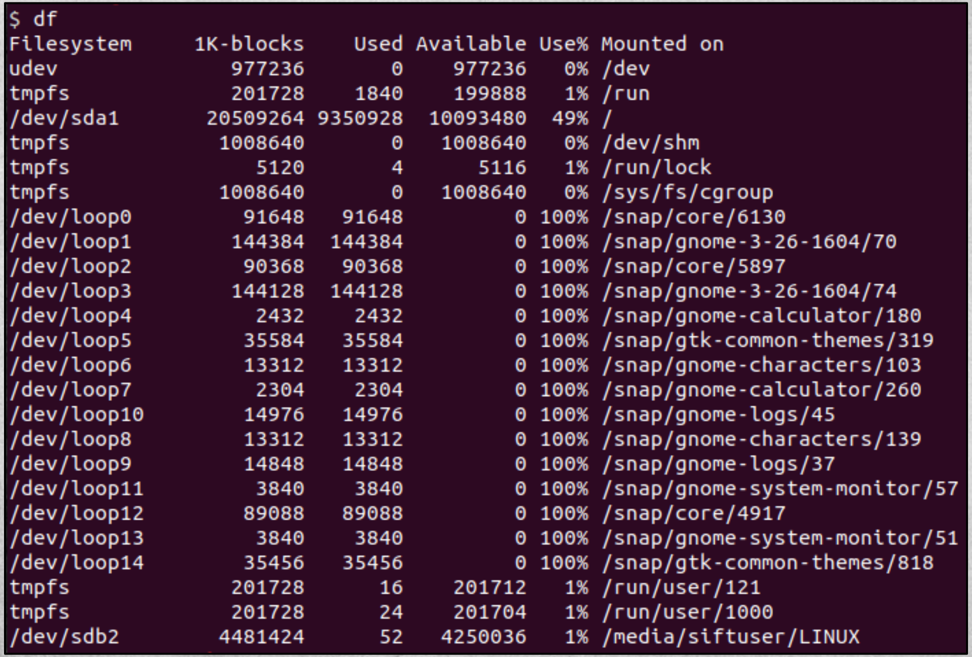


```
Device     Boot    Start      End  Sectors  Size Id Type
/dev/sdb1             63 67874624 67874562 32.4G 1c Hidden W95 FAT32 (LBA)
/dev/sdb2  *    68902785 78156224  9253440  4.4G 83 Linux
/dev/sdb3       67874625 68902784  1028160  502M 82 Linux swap / Solaris
```

Multiple Partition

df

- df displays file system disk space usage

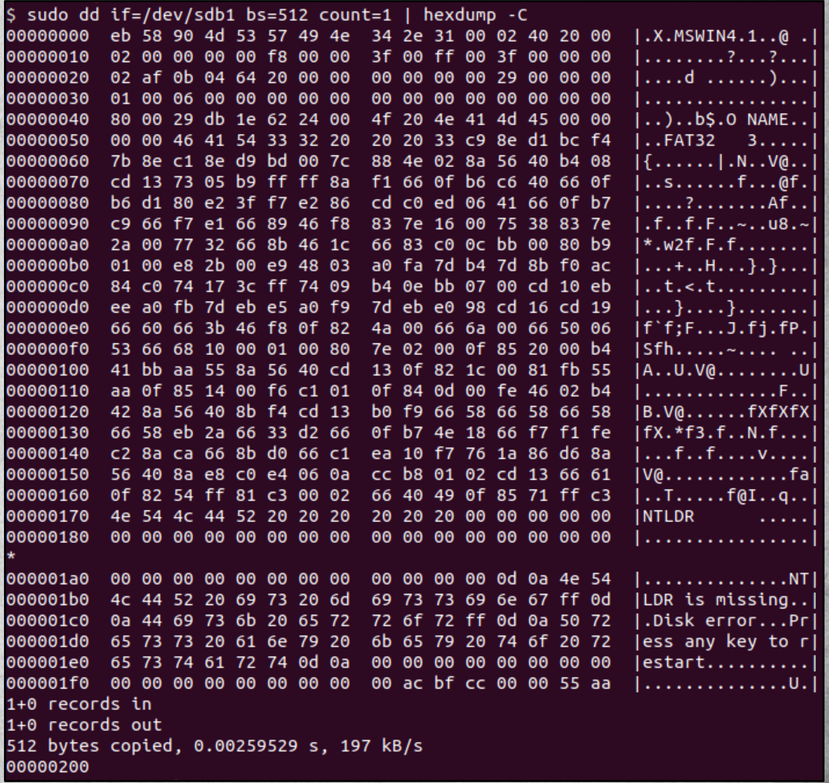


```
$ df
Filesystem     1K-blocks    Used Available Use% Mounted on
udev              977236       0    977236   0% /dev
tmpfs             201728    1840    199888   1% /run
/dev/sda1       20509264 9350928  10093480  49% /
tmpfs            1008640       0   1008640   0% /dev/shm
tmpfs               5120       4      5116   1% /run/lock
tmpfs            1008640       0   1008640   0% /sys/fs/cgroup
/dev/loop0         91648   91648         0 100% /snap/core/6130
/dev/loop1        144384  144384         0 100% /snap/gnome-3-26-1604/70
/dev/loop2         90368   90368         0 100% /snap/core/5897
/dev/loop3        144128  144128         0 100% /snap/gnome-3-26-1604/74
/dev/loop4          2432    2432         0 100% /snap/gnome-calculator/180
/dev/loop5         35584   35584         0 100% /snap/gtk-common-themes/319
/dev/loop6         13312   13312         0 100% /snap/gnome-characters/103
/dev/loop7          2304    2304         0 100% /snap/gnome-calculator/260
/dev/loop10        14976   14976         0 100% /snap/gnome-logs/45
/dev/loop8         13312   13312         0 100% /snap/gnome-characters/139
/dev/loop9         14848   14848         0 100% /snap/gnome-logs/37
/dev/loop11         3840    3840         0 100% /snap/gnome-system-monitor/57
/dev/loop12        89088   89088         0 100% /snap/core/4917
/dev/loop13         3840    3840         0 100% /snap/gnome-system-monitor/51
/dev/loop14        35456   35456         0 100% /snap/gtk-common-themes/818
tmpfs             201728      16    201712   1% /run/user/121
tmpfs             201728      24    201704   1% /run/user/1000
/dev/sdb2        4481424      52   4250036   1% /media/siftuser/LINUX
```

Viewing Raw Disk Data

- To properly analyze disk images, data, and metadata good understanding of partition composition is needed
- Numerous tools can be used to view raw disk data
  - ✓ dd
  - ✓ hexdump
  - ✓ xxd

One sector of the FAT32 disk



```
$ sudo dd if=/dev/sdb1 bs=512 count=1 | hexdump -C
00000000  eb 58 90 4d 53 57 49 4e  34 2e 31 00 02 40 20 00  |.X.MSWIN4.1..@ .|
00000010  02 00 00 00 00 f8 00 00  3f 00 ff 00 3f 00 00 00  |........?...?...|
00000020  02 af 0b 04 64 20 00 00  00 00 00 00 29 00 00 00  |....d ......)...|
00000030  01 00 06 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000040  80 00 29 db 1e 62 24 00  4f 20 4e 41 4d 45 00 00  |..)..b$.O NAME..|
00000050  00 00 46 41 54 33 32 20  20 20 33 c9 8e d1 bc f4  |..FAT32   3.....|
00000060  7b 8e c1 8e d9 bd 00 7c  88 4e 02 8a 56 40 b4 08  |{......|.N..V@..|
00000070  cd 13 73 05 b9 ff ff 8a  f1 66 0f b6 c6 40 66 0f  |..s......f...@f.|
00000080  b6 d1 80 e2 3f f7 e2 86  cd c0 ed 06 41 66 0f b7  |....?.......Af..|
00000090  c9 66 f7 e1 66 89 46 f8  83 7e 16 00 75 38 83 7e  |.f..f.F..~..u8.~|
000000a0  2a 00 77 32 66 8b 46 1c  66 83 c0 0c bb 00 80 b9  |*.w2f.F.f.......|
000000b0  01 00 e8 2b 00 e9 48 03  a0 fa 7d b4 7d 8b f0 ac  |...+..H...}.}...|
000000c0  84 c0 74 17 3c ff 74 09  b4 0e bb 07 00 cd 10 eb  |..t.<.t.........|
000000d0  ee a0 fb 7d eb e5 a0 f9  7d eb e0 98 cd 16 cd 19  |...}....}.......|
000000e0  66 60 66 3b 46 f8 0f 82  4a 00 66 6a 00 66 50 06  |f`f;F...J.fj.fP.|
000000f0  53 66 68 10 00 01 00 80  7e 02 00 0f 85 20 00 b4  |Sfh.....~.... ..|
00000100  41 bb aa 55 8a 56 40 cd  13 0f 82 1c 00 81 fb 55  |A..U.V@........U|
00000110  aa 0f 85 14 00 f6 c1 01  0f 84 0d 00 fe 46 02 b4  |.............F..|
00000120  42 8a 56 40 8b f4 cd 13  b0 f9 66 58 66 58 66 58  |B.V@......fXfXfX|
00000130  66 58 eb 2a 66 33 d2 66  0f b7 4e 18 66 f7 f1 fe  |fX.*f3.f..N.f...|
00000140  c2 8a ca 66 8b d0 66 c1  ea 10 f7 76 1a 86 d6 8a  |...f..f....v....|
00000150  56 40 8a e8 c0 e4 06 0a  cc b8 01 02 cd 13 66 61  |V@............fa|
00000160  0f 82 54 ff 81 c3 00 02  66 40 49 0f 85 71 ff c3  |..T.....f@I..q..|
00000170  4e 54 4c 44 52 20 20 20  20 20 20 00 00 00 00 00  |NTLDR      .....|
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000001a0  00 00 00 00 00 00 00 00  00 00 00 00 0d 0a 4e 54  |..............NT|
000001b0  4c 44 52 20 69 73 20 6d  69 73 73 69 6e 67 ff 0d  |LDR is missing..|
000001c0  0a 44 69 73 6b 20 65 72  72 6f 72 ff 0d 0a 50 72  |.Disk error...Pr|
000001d0  65 73 73 20 61 6e 79 20  6b 65 79 20 74 6f 20 72  |ess any key to r|
000001e0  65 73 74 61 72 74 0d 0a  00 00 00 00 00 00 00 00  |estart..........|
000001f0  00 00 00 00 00 00 00 00  00 ac bf cc 00 00 55 aa  |..............U.|
1+0 records in
1+0 records out
512 bytes copied, 0.00259529 s, 197 kB/s
00000200
```

Host Protected Area

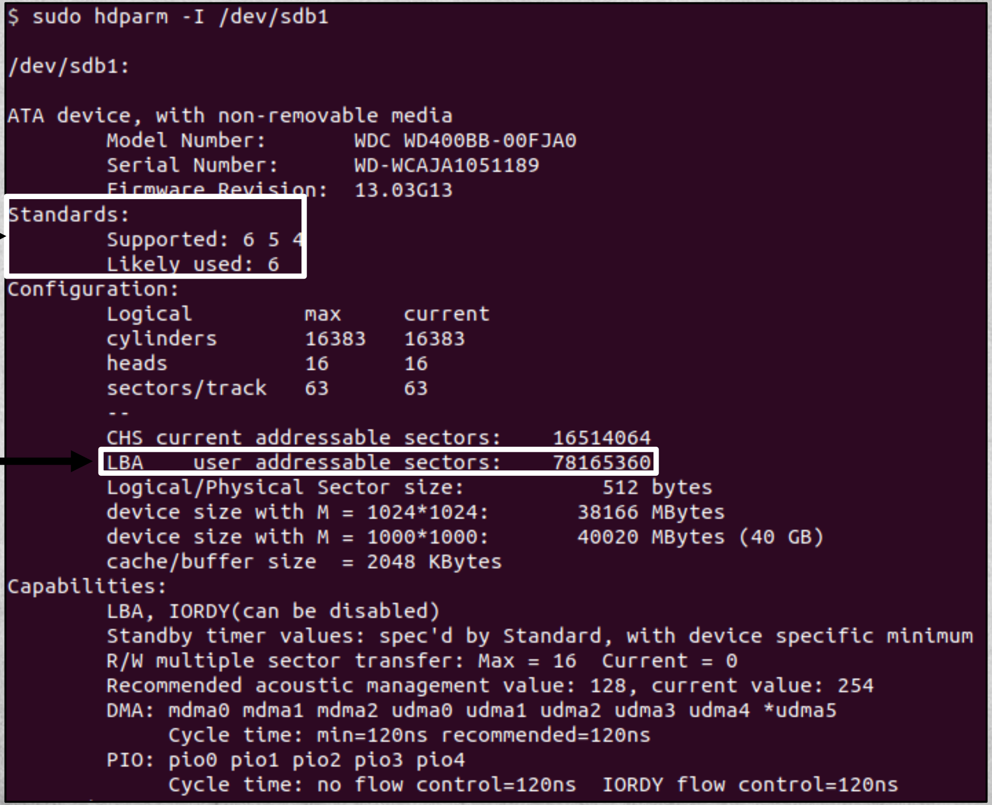
- Introduced in ATA/ATAPI-4 standard that allowed system vendors to allocate reserved space outside of the BIOS & OS
- HPA examples include:
  - ✓ Disk Utilities
  - ✓ System Recovery Data
  - ✓ Diagnostic Tools
  - ✓ Boot Sector Code
- The operating system does not have access to HPA and requires firmware

Device Configuration Overlay

- Introduced in ATA/ATAPI-6 standard that allows controls of disk features and made it easier to provide disk support and drive replacement across multiple vendors
- If used with HPA, DCO must be established first
- When conducting a forensics analysis, it is important to identify HPA and DCO usage as it has been used to hide malicious code and data
  - ✓ dmesg
  - ✓ hdparm

hdparm

- hdparm shows and sets hard disk parameters



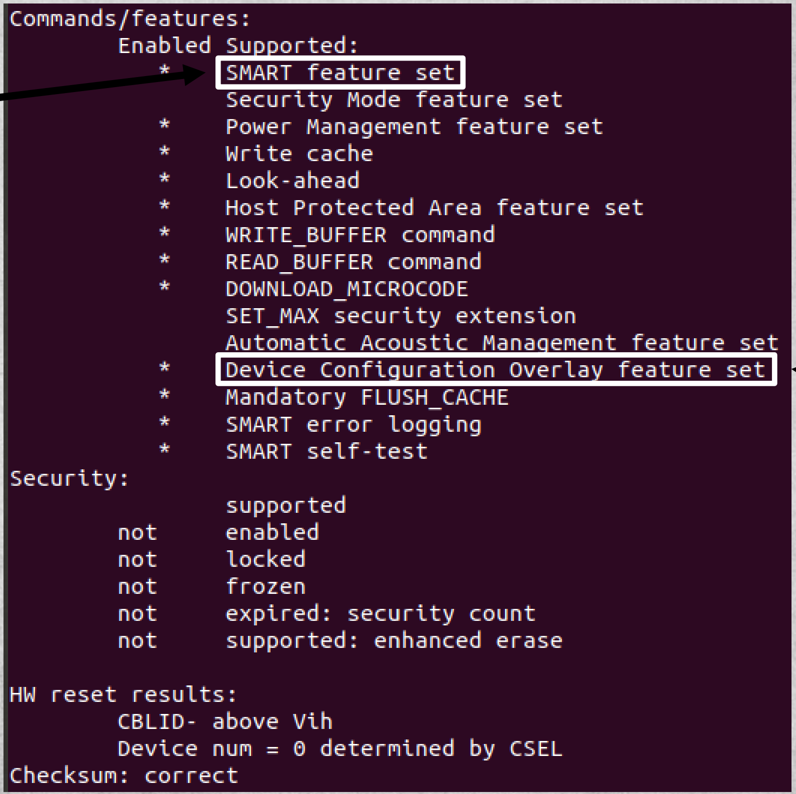
```
$ sudo hdparm -I /dev/sdb1

/dev/sdb1:

ATA device, with non-removable media
        Model Number:       WDC WD400BB-00FJA0
        Serial Number:      WD-WCAJA1051189
        Firmware Revision:  13.03G13
Standards:
        Supported: 6 5 4
        Likely used: 6
Configuration:
        Logical         max     current
        cylinders       16383   16383
        heads           16      16
        sectors/track   63      63
        --
        CHS current addressable sectors:    16514064
        LBA    user addressable sectors:    78165360
        Logical/Physical Sector size:           512 bytes
        device size with M = 1024*1024:       38166 MBytes
        device size with M = 1000*1000:       40020 MBytes (40 GB)
        cache/buffer size  = 2048 KBytes
Capabilities:
        LBA, IORDY(can be disabled)
        Standby timer values: spec'd by Standard, with device specific minimum
        R/W multiple sector transfer: Max = 16  Current = 0
        Recommended acoustic management value: 128, current value: 254
        DMA: mdma0 mdma1 mdma2 udma0 udma1 udma2 udma3 udma4 *udma5
             Cycle time: min=120ns recommended=120ns
        PIO: pio0 pio1 pio2 pio3 pio4
             Cycle time: no flow control=120ns  IORDY flow control=120ns
```

ATA/ATAPI-6 Standard

Logical Block Addressing

hdparm – Disk Features

Self-Monitoring Analysis and Reporting Technology



```
Commands/features:
        Enabled Supported:
           *    SMART feature set
                Security Mode feature set
           *    Power Management feature set
           *    Write cache
           *    Look-ahead
           *    Host Protected Area feature set
           *    WRITE_BUFFER command
           *    READ_BUFFER command
           *    DOWNLOAD_MICROCODE
                SET_MAX security extension
                Automatic Acoustic Management feature set
           *    Device Configuration Overlay feature set
           *    Mandatory FLUSH_CACHE
           *    SMART error logging
           *    SMART self-test
Security:
                supported
        not     enabled
        not     locked
        not     frozen
        not     expired: security count
        not     supported: enhanced erase

HW reset results:
        CBLID- above Vih
        Device num = 0 determined by CSEL
Checksum: correct
```

DCO Set

Disk Image Demo

References

- https://kb.digital-detective.net/display/BLADE1/File+System+Data+Recovery
- https://www.quora.com/What-is-the-port-difference-between-SSD-SAS-and-SSD-SATA
- https://www.slideshare.net/xabean/controlling-usb-flash-drive-controllers-expose-of-hidden-features
- https://usb-ids.gowdy.us/read/UD
- http://www.learnlinux.org.za/courses/build/internals/ch08s04.html
- http://www.ibm.com/developerworks/websphere/techjournal/1506_dejesus/1506_dejesus-trs.html
- https://www.sweetscape.com/010editor/manual/EditingDrives.htm
- https://thewirecutter.com/reviews/best-sd-card-readers