SWINBURNE UNIVERSITY OF TECHNOLOGY

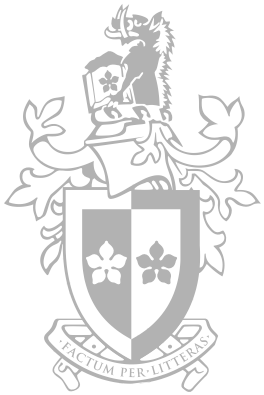
ICT30010 eForensic Fundamentals

Lecture 5

Disk and File Systems

Troy Pretty

Digital Forensic Analyst



SWINBURNE UNIVERSITY OF TECHNOLOGY

Outline and learning goals

- Disk geometry
- Partitions
- Multi-disk volumes
- Interface standards
- Data acquisition at disk level

Hierarchy of static data

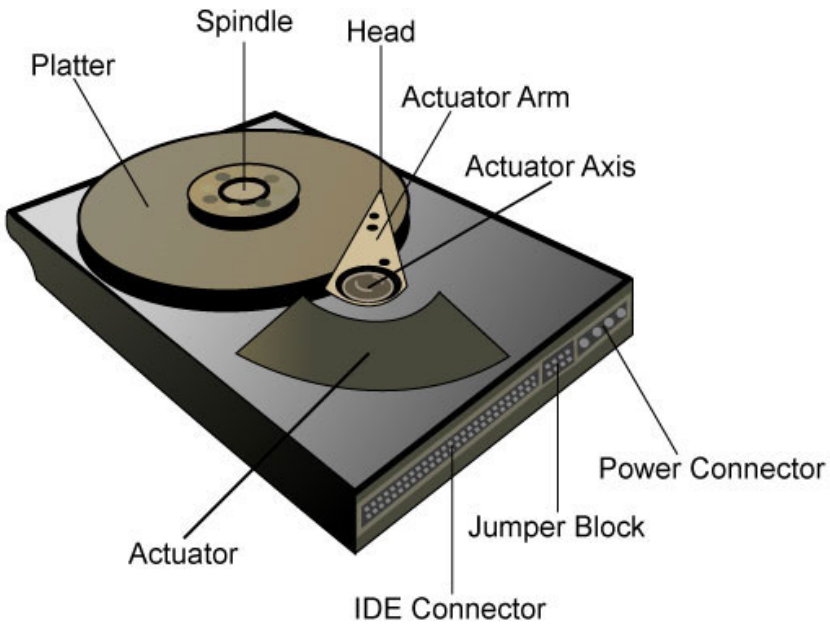
- Can acquire non-volatile data at different levels
  - Disk
  - Volume / Partition
  - File
  - Application
- At each level, information is lost
- General principle is to acquire data at the lowest level

Hierarchy of static data

- Often will acquire at the lowest level with direct disk copy but not always possible or necessary
  - Live application server, multi-user email or file server
- When acquired at low level need to interpret up to higher level
  - Eg looking for a particular picture file (.jpg, .gif etc)
  - Capturing a disk image requires tracing through the disk / partition / file / application structure until the picture file is obtained

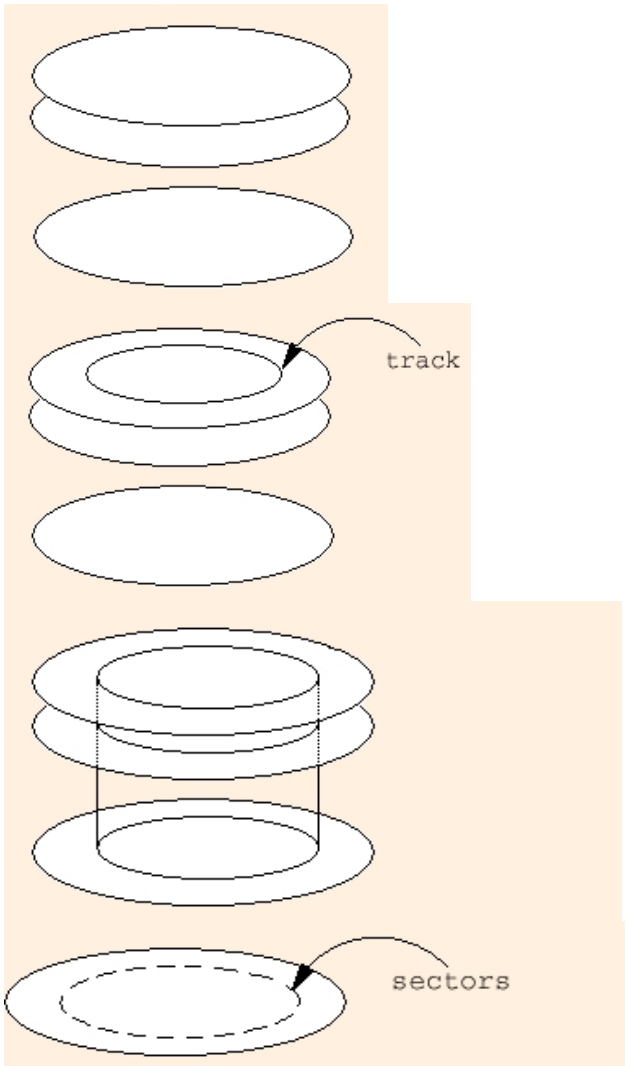
Spinning disk geometry

- Hard disk is made up of one or more circular platters stacked on each other and which spin at the same time
- The platters are read and written to and from heads at the end of actuators
- Each platter has two sides on which data can be stored



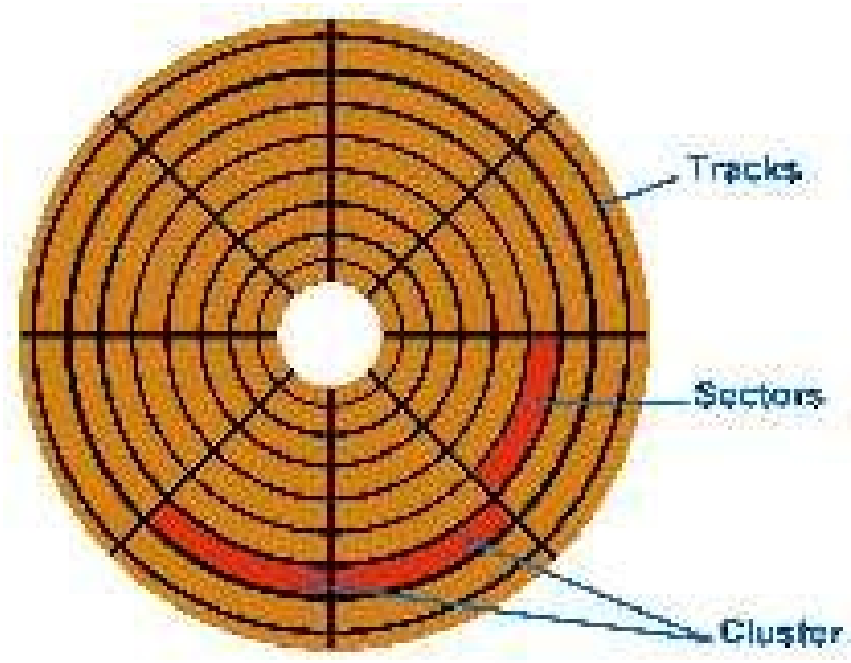
Spinning disk geometry (continued)

- Each side is divided into rings called tracks
- Tracks are numbered from 0 starting on the outside
- The same number track across all platters is a cylinder
- Pictures from http://www.rwc.uc.edu/koehler/comath/42.html



Spinning disk geometry (continued)

- Cylinders are numbered from 0 starting on the outside
- Each track is divided into sectors
- Sectors are typically 512 bytes in size
  - The smallest addressable unit on the hard disk
- Contiguous sectors form clusters

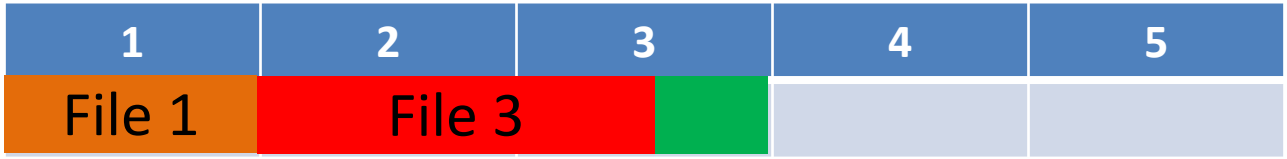


- picture from gorecovery.com

Flash based disk

- Mechanical disks increasingly being replaced wish flash based disks (SSD)
- Forensic Considerations
  - Flash chips can wear out over time
  - Wear levelling causes high data fragmentation
  - TRIM command actively overwrites unallocated space

Slack Space

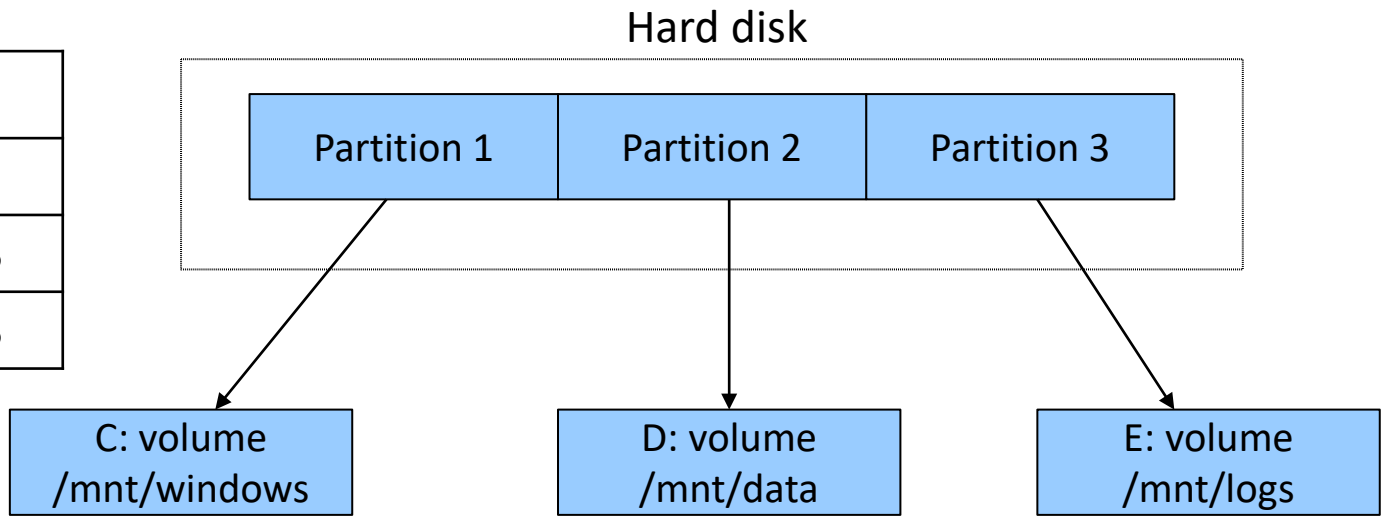


- File 1 is 512 bytes in size
- File 2 is 1024 bytes in size
- File 2 is deleted
- File 3 is 768 bytes in size, overwrites file 2
- 256 bytes of File 2 still exists and is recoverable

Partitions

- Sometimes used interchangeably with 'Volumes'
- Partition table points to a partition
- Partitions map to a volume (in Windows) or mount point/directory (in Unix)

START	END	TYPE
0	99	FAT
100	249	NTFS
300	599	NTFS

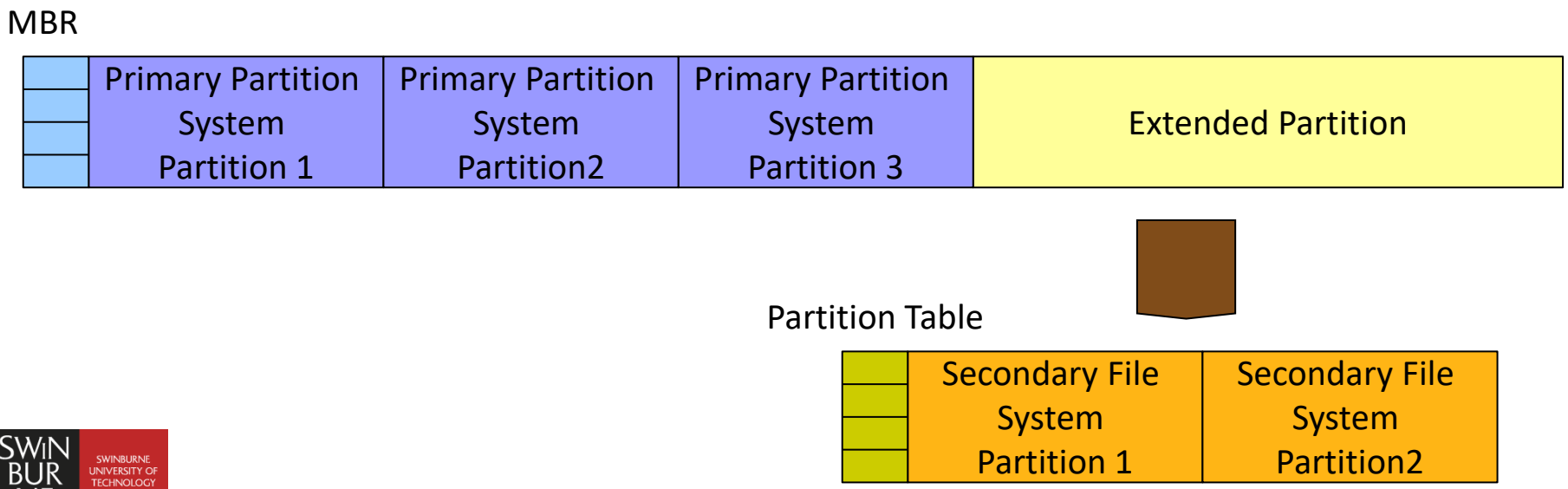


MBR Based Partitions

- A hard disk has one MBR (Master Boot Record)
- A MBR holds the Partition Table
- A partition contains a specific file system (e.g. FAT32 or NTFS)
- A partition is assigned a logical hard drive letter.
- MBR partition limited to 2TB

MBR Based Partitions

- MBR can describe up to 4 partitions
- Can have more than 4 by use of Extended partitions
- An extended partition may itself contain a partition table and up to two partitions one of which may be an extended partition



MBR Based Partitions

- FDISK –lu
  - 3 Primary Partitions

```
Disk /dev/sdc: 7.2 GiB, 7750287360 bytes, 15137280 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000654f4

Device     Boot   Start     End Sectors Size Id Type
/dev/sdc1          2048 2099199 2097152   1G  e W95 FAT16 (LBA)
/dev/sdc2       2099200 4196351 2097152   1G  e W95 FAT16 (LBA)
/dev/sdc3       4196352 6293503 2097152   1G  e W95 FAT16 (LBA)
```

  - 3 Primary, 1 Extended Partition

```
Disk /dev/sdc: 7.2 GiB, 7750287360 bytes, 15137280 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000654f4

Device     Boot   Start      End Sectors  Size Id Type
/dev/sdc1          2048  2099199 2097152    1G  e W95 FAT16 (LBA)
/dev/sdc2       2099200  4196351 2097152    1G  e W95 FAT16 (LBA)
/dev/sdc3       4196352  6293503 2097152    1G  e W95 FAT16 (LBA)
/dev/sdc4       6293504 15136767 8843264  4.2G  f W95 Ext'd (LBA)
/dev/sdc5       6295552  8392703 2097152    1G  e W95 FAT16 (LBA)
```

GPT Based Partition

- GUID Partition Table
  - Supported from Windows XP
    - 64 bit OS
    - Unified Extensible Firmware Interface (UEFI) BIOS
  - Increase partition size
    - 18 EB in Windows
  - Increased number of partitions
    - 128 in Windows

Multiple Disk Partitions

- Multiple disks are often used in servers and increasingly in desktops/laptops
  - Performance, reliability, scalability
- Main technologies are RAID and Disk Spanning
  - RAID – Redundant Array of Inexpensive Disks
  - Disk Spanning – Aggregating multiple disks into one volume (Sometimes “Just a Bunch of Disks” or JBOD)

RAID

- Goal is to make use of multiple disks for performance and/or reliability
- Depending on the priority (performance or reliability) individual files are 'striped' across multiple disks
- Different RAID configurations (RAID levels) achieve different goals
- May want to achieve very high data rates (RAID commonly used in video editing) or may want to have high reliability with (for example) hot swapping of faulty disks

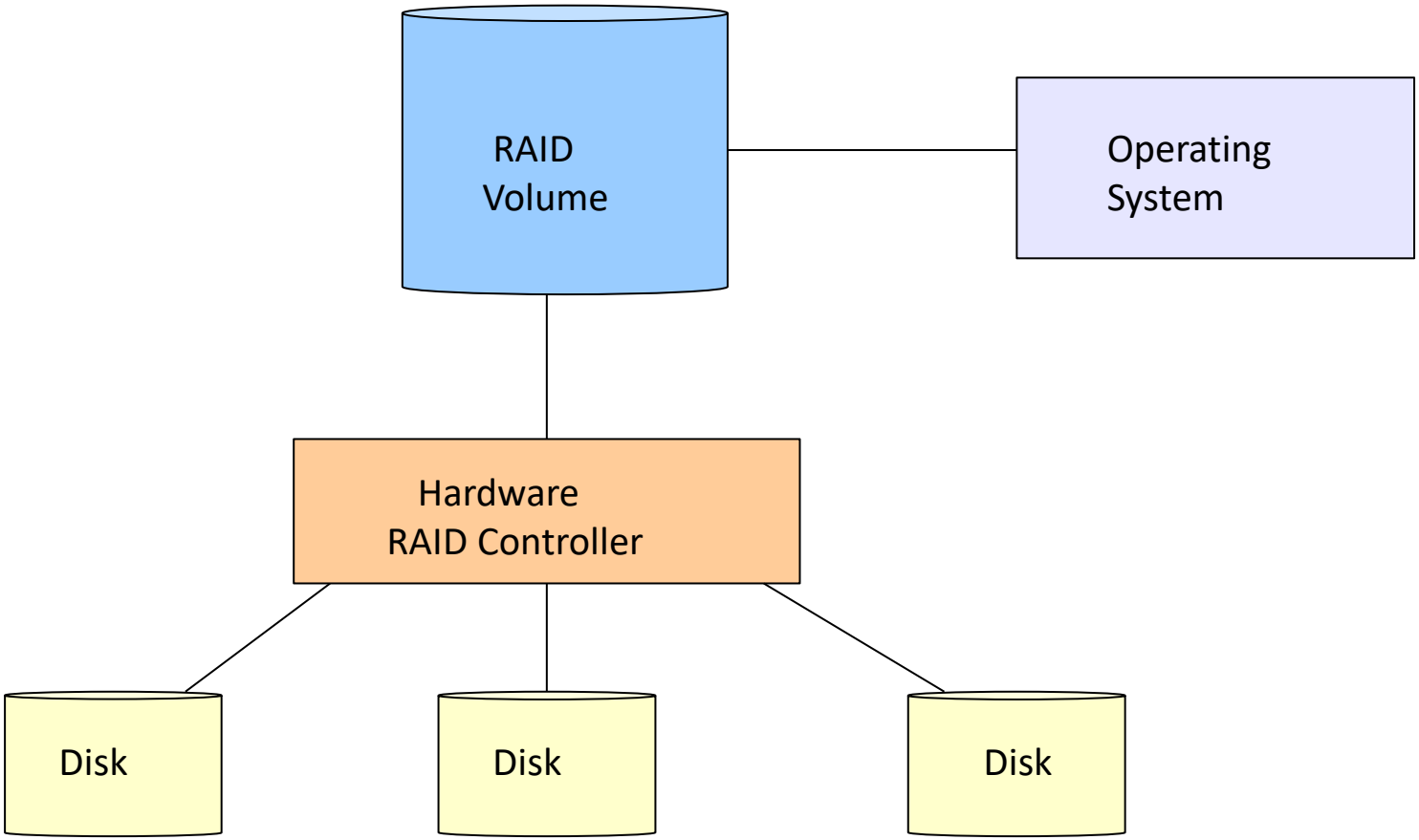
RAID Levels

RAID Level	Description
0	Data striped across the array in block sized chunks. Can provide very high performance but no additional reliability
1	Data is mirrored across two disks. Very reliable but no improvement on performance
2	Striping at bit level. Error correcting codes used across multiple disks. (rarely used)
3	Data striped across at least two disks and a dedicated parity disk. Striping is at byte level
4	Similar to RAID 3 except striping is based on blocks
5	Similar to RAID 4, except no dedicated parity disk. Each disk contains a mix of data and parity information.
6	Extends RAID 5 by adding an additional parity block.

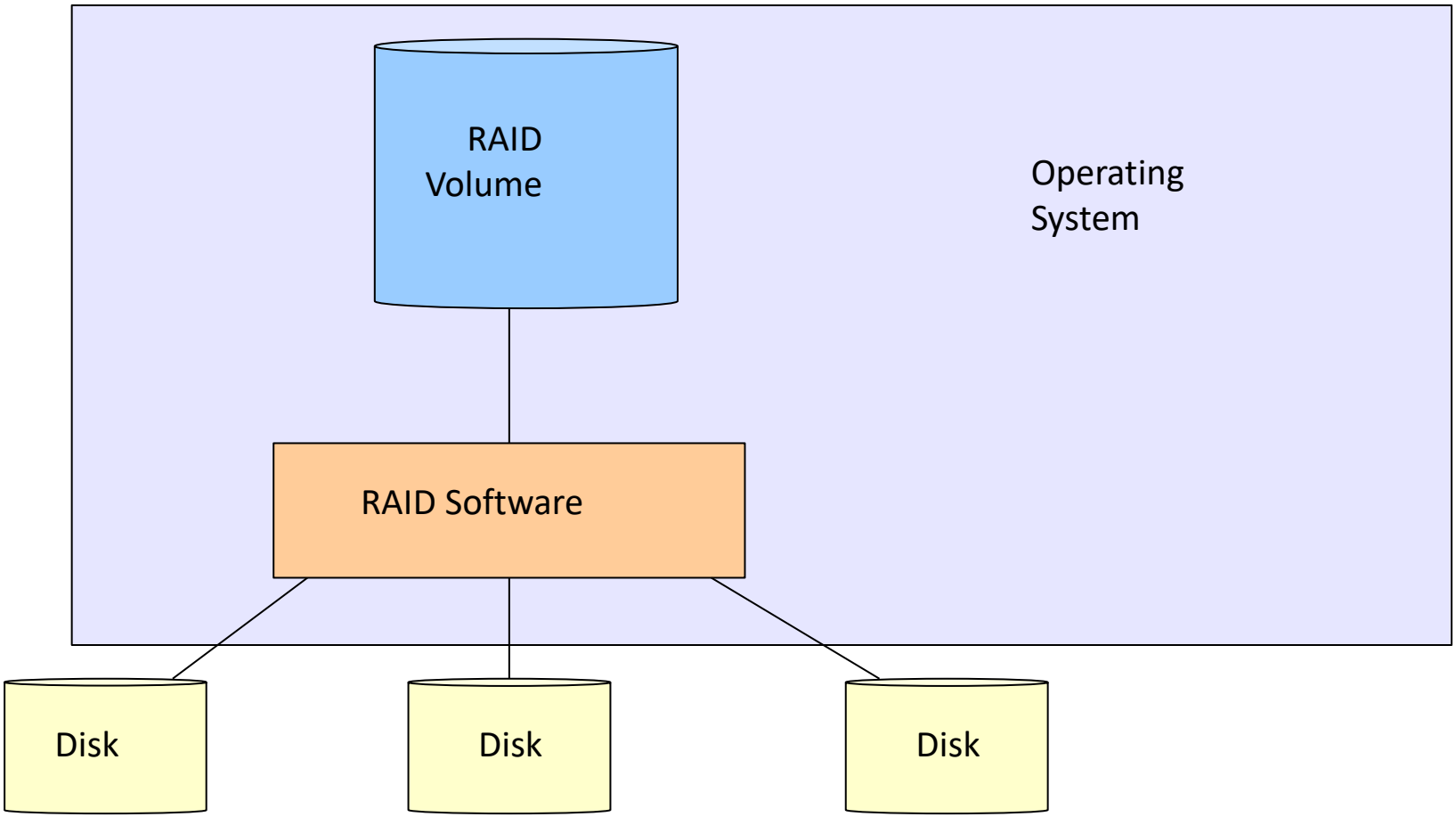
RAID

- Most commonly used RAID levels are 0, 1 and 5
  - Increasingly, RAID6 – same as 5 with two copies of parity information
- RAID can be implemented in hardware or software
  - Depending on which there are consequences for forensic acquisition
- Hardware RAID
  - Computer sees only the controller and not the individual disks
- Software RAID
  - Operating system manages disk access

Hardware RAID



Software RAID



RAID data acquisition

- Hardware RAID data acquisition
  - Easiest to acquire as if a single disk via the controller
  - Can be very large and very slow to acquire
    - May need another RAID system as the acquisition system
- If drivers for controller not available then only choice is to acquire data from each
- RAID data acquisition can be a difficult area

RAID data acquisition

- Software RAID data acquisition
  - Most operating systems offer some RAID capabilities
    - Linux, MS Windows, Apple OS X
  - Use a similar approach to hardware acquisition

Disk spanning

- Disk spanning makes multiple disks appear to be one large disk
- Most major operating systems support disk spanning
- Goal is to append disks to an existing storage space
- Logical volumes mapped onto multiple physical disks
- Again, simplest approach is to capture logical volume

Partition types

- Many partition types
- Important ones
  - FAT32 (Old Windows OS / Flash drives)
  - exFAT (Newer Flash Drives)
  - NTFS (Windows NT 3.1+)
  - EXT (Linux)
  - HFS / APFS (Mac OS X)
  - UFS (Unix)

Recovering deleted partitions

- A anti-forensic technique is to delete or reposition partitions
- Some tools exist to recover deleted partitions
- Essentially they look for characteristic strings and use that to reconstruct the partition structure
  - eg. FAT/NTFS file systems has the values 0x55 and 0xAA in bytes 510 and 511 of the first sector
  - Using similar pieces of information the partition can sometimes be recovered

Interface Standards

- AT Attachment (ATA/IDE)
  - Formulated by the T13 group of the International Committee on Information Standards Committee (INCITS)
  - Lots of ATA standards
    - ATA-1, ATA-3
    - ATA/ATAPI-4, ATAPI-6, ATAPI-7
- Small Computer Systems Interface (SCSI)
  - Formulated by the T10 group of INCITS
  - Again lots of SCSI standards
    - SCSI-1, SCSI-2, SCSI-3

ATA/IDE

- Advanced Technology Attachment interface / Integrated Disk Electronics
- AT specifies a number of commands issued by a controller contained on the motherboard
- Interface between controller and disk is called a channel
  - Connected by a 40 wire ribbon cable
- Refers to Master and Slave although neither controls or is controlled by the other
  - Specifies how attached to ribbon cable

ATA/IDE

- Serial ATA
  - Uses a serial rather than a ribbon cable to connect the controller to the disk
  - No difference as far as computer is concerned
  - No chaining of devices as in Parallel ATA

Picture from hardwaresecrets.com
(shows SATA on left, IDE on right)

SATA

- Each SATA drive is seen by the host as a master connected to the controller via its own channel
- Advantages of SATA
  - Less cumbersome cables than Parallel ATA
  - Simpler to configure (no slave configuration)

SCSI

- Main difference between SCSI and ATA is that SCSI does not have a controller on the disk
- SCSI defines a bus where different devices (not just hard disks) communicate with each other
- Many different cables and connectors
  - Serial
  - Parallel 8 bits
  - Parallel 16 bits (wide)
  - 50 pin, 68 pin connector

Fiber Channel

- Mainly used for storage area networks
  - Very high capacity over very short distances
  - Can run on twisted pair as well as fiber

USB

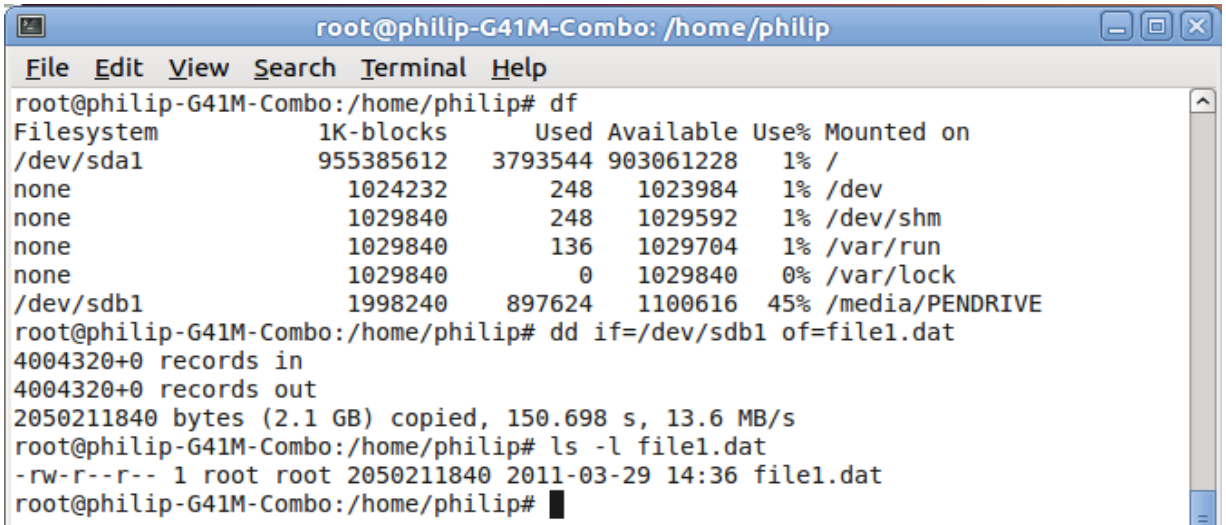
- Universal Serial Bus
  - Enables all manner of peripherals to be connected
  - Supplies power
- A number of different connectors
  - Type A and B most common
  - USB C is increasing in popularity

Data acquisition at disk level

- Data acquisition is usually done at the disk rather than the file level
  - Enables deleted files to be recovered (in most circumstances)
  - Some data may not be included within partitions
    - Eg DOS partitions do not use sectors 1 to 62
- Destination
  - Another device
  - Image file
  - An important issue is the size of the disk to be captured, particularly with multi-disk systems

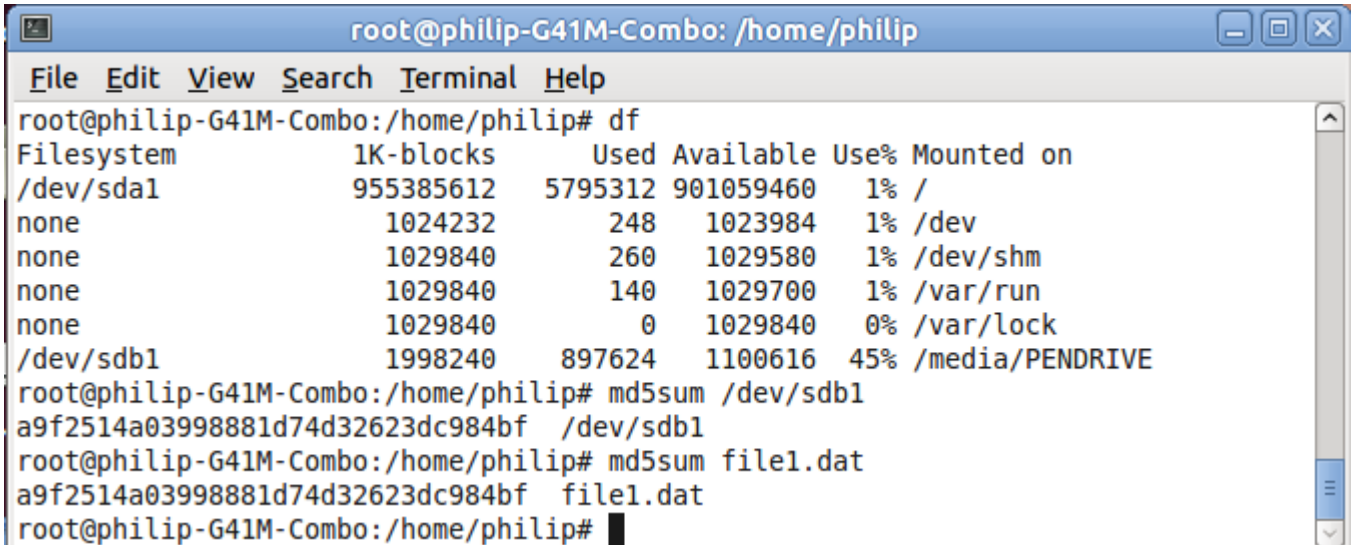
dd in Linux

- **dd** is a Low level but very useful technique for capturing an image of a disk
- A disk in Linux will have a mount point such as **/dev/sda1**
  - Can be identified using df
- Can be captured at the byte level using **dd**
  - "Forensic" versions of dd (dcfldd, dc3dd) include hashing, progress monitoring and error handling.



Data acquisition integrity

- Integrity of data captured is important
  - Need to demonstrate that data is unchanged
- Can be done using cryptographic hash functions
  - Takes a block of data and returns a fixed-size bit string
  - Any change to the original data will result in a significant change to the hash



SWINBURNE UNIVERSITY OF TECHNOLOGY

Hash Functions

- MD5 and SHA-1 most widely used hash functions
- MD5 described in RFC1321 (http://tools.ietf.org/html/rfc1321)
  - Splits digital object into 512 bit blocks
  - Calculates sub-hashes for each block
  - Sub-hashes then used as initialisation vector for next 512 block
- A single bit change in the digital object will, on average, cause 50% of the bits in the hash to be changed
- Some theoretical weaknesses in MD5 so SHA-1
- Hashing is one way, not possible to determine original data from the hash value

Hash functions

- Hash is the mathematical calculation of the data contained with a file
- File system dates and times relate to the file system only, they will not change the hash value of a file
- Hashing the same data will always return the same value
  - MD5(“BAT”) = 7ac04cf18b7606efb16ff9ecbca87825
  - MD5(“CAT”) = c01ae1a5f122f25ce5675f86028b536a
  - MD5(“BAT”) = 7ac04cf18b7606efb16ff9ecbca87825

Hash functions

- Hashing in forensics:
  - Ensures forensic processes have not modified data
  - Ensures chain of custody of evidence items
  - Helps to identify items of interest

Future of static storage technology

- Magnetic disk coming to the end of its 60 year dominance
  - Replaced by solid state drives
- Flash memory drives starting to rival hard drives in terms of capacity (if not price)
  - 512GB and 1TB common
- Advantages are robustness, i/o speed, low power consumption and size

Summary

- Examined the structure of disks
  - Geometry
  - Multi-disk volumes
  - Partitions
  - Slack space
  - Interfaces
  - Hashing