CF

(A) Garbage Collection:-

Goals is to enable the flash storage devices to have enough spare blocks so that whenever data must be written, the devices does not have to wait for a block to be erased & made available for the new data.

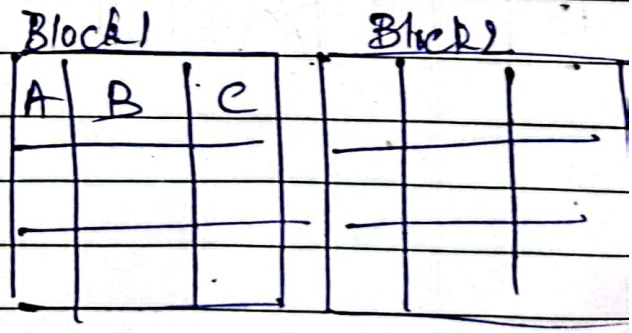
Modify data → Stored in pages → SSD writes → changes in new page → mark old page → modified data stored → Stale page.

In order to avoid → filling ~~stale page~~ → SSD → Stale page → Garbage collection.

Idle → SSD become → Garbage collection triggered

↳ Copying valid data → reserved block
leaving stale data → orginial block.

↳ Erasing 0s block → new available block

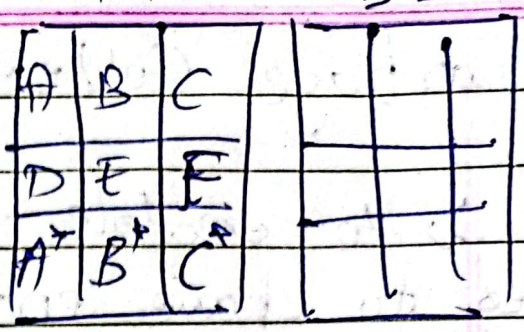


- Page A, B, C Block 1 active data.

- Remaining page free & available when new data written / stored

PAGE NO.:
DATE:

Data pages A, B & C B1
↓
Modified by A*, B* & C*



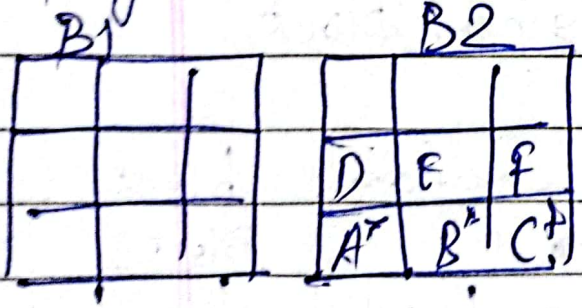
New Data → written page
D, E & F.

Page A, B, C → Marked invalid or stale
cannot be written → new data → unless entire B1 is erased.

- Garbage collection performed.

- Valid data D, E, F → A* B* C* → copied B2

- All page B1 → erased → available written new data.



(B) Trim.

Trim Command → ATA Interface (Advanced Technology Attachment)

Use your drive → changing & deleting information → SSD make sure invalid info. is deleted → space available for new info. → Trim tells SSD which pieces data can be erased.

Users perspective → data been deleted from a document → Bcuz the way SSD → read/write info. → data is not deleted → Drive → User's Command.

- Instead → Area SSD → contained data → marked as no longer used.
- Trim commands → tells drive → data can be removed.

- Benefits of Trim → time Saving → SSD drive erased data when computer is idle → rather using extra time → during write process → remove data no longer valid.

(C) Wear levelling:

Wear levelling → flash memory Controller feature that spread the wear & tear of data transfers and useage evenly across the NAND flash memory, making your SSD last longer.

Wear leveling → designed to extend → life of SSD → Solid State Storage → mode microchips → store data in blocks

Each block → tolerate → finite number of program/erase cycles → before becoming unreliable

- P/E Cycles → 4 type — Single level Cell Flash approx. 1,00,000 cycles — Multi LC Flash (approx 10,000-3500 cycles
- Triple LC flash → approx 5000 cycles
- Quad LC flash → approx 1000 - 100 cycles.

(2) What is GPT & MBR?

MBR (Master Boot Record) → Partition tyles,
GPT (GUID Partition Table) → 2 ways of storing Partitioning info.

- It Include where partition starts/end.
  - ↳ Operating System knows
  - ↳ Which sector belongs to each partition
  - ↳ which partition is bootable.
- Before Partitioning select GPT/MBR.

MBR's limitations.

↳ works with disks upto 2TB in size.
↳ Only supports upto 4 primary partitions.
↳ If you want more,
↳ Make one of your Primary partitions an "extended partition" & Create logical partitions.

MBR became the industry standard.
Used → Partitioning & booting from disks.

GPT →

- GUID → Globally Unique ID entities.
These are less chances that ID will be same globally.
- This is because, GUID a random string is used to create
- GPT → New standard — replacing MBR
- Associated with UEFI - (Unified Extensible Firmware Interface)
designed to replaced BIOS (basic Input/output System) & legacy.

Advantages →

↳ Drivers → much much larger
↳ Size Limit → depend on → OS and its fileSystems
↳ Allows Unlimited Partitions → Limit here will OS
↳ Windows allows upto 128 partitions on a GPT drive.

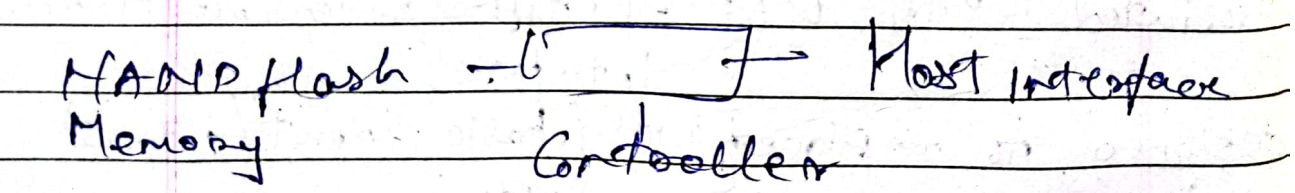
PAGE NO.:
DATE: / /

⑤ brief Note on SSD?

- Data Stored in flash memory.
- Storage device which is very fast.
- low power Consumption
- No moving parts like a memory stick
- Uses NAND or NOR gates based flash memory
- Directly reads from cell location so lower latency.
- No effect of magnetic field on SSD operation
- No heat production as no moving parts
- Better reliability and longer lifespan
- 100 times higher access speed wrt HDD

Architecture of SSD:

SSD is made of non-volatile NAND flash memory.



Types of SSD.

NOR SSD — cells connected parallel
- Complex Structure
- More wires
- Costlier.

NAND SSD — cells connected in series
- less Complex, lesser wires
- Better Chip density.

Advantages of SSD over HDD.

- Durability & Reliability of an SSD
- SSDs are faster than Hard Drives.
- Power & Energy Efficient.
- less weight and No Noise.
- More practical sizes/form factors.

Q) Ans – Digital forensics → retrieval, analysis & use of digital evidence → civil or criminal investigation.

- Digital Forensics → branch Forensics Science — recovery & investigation → material found — digital devices related to cybercrime.

types of Digital Forensics.

- Disk Forensics :- deals → extracting data — storage media — searching active, modified, deleted files: for eg: Hard drive use in cybercrime.
- Network Forensics: subbranch of Digital forensics — related to monitoring & analysis of computer network traffic.

For eg:- web server logs can be used to show when a suspect accessed information related to criminal activity.

Wireless forensics:- division of network forensics

Main aim — to offers tools need to collect & analyze — data from wireless network

For eg:- Wifi, Mobile.

Malware forensics:- branch deals — identification of malicious code — study payload, viruses, worms etc.

For eg Static, Hybrid, Dynamic Analysis.

Email Forensics:- Deals — recovery & analysis of emails — deleted emails, Calendars & contacts

For eg:- Email Header Analysis, Sender Mailer Fringerprint.

Memory Forensics:- Collecting data — system memory (system, registers, Cache, Rams) — Raw form — Carving the data from Raw dump.

For eg:- network connections, account credentials.

Mobile Phone Forensics :

deals - examination & analysis of mobile devices.

- helps retrieve phone, Sim Contacts, call logs, incoming, and outgoing SMS/MMS, Audio, video etc.

For eg :- Health App Data;

Database forensics :- study & examination of Database & their related metadata.

For eg : OS, Network forensics, Database Platform.

IOT Forensics :- practice of analyzing IOT devices to investigate crimes.

Foreg :- fitness trackers, smart appliances

Cloud Forensics :- Cloud forensic - amalgamation of all the different forensics.

For eg :- A company using cloud server might be the victim of a data breach or denial of the service incident.

PAGE NO.:
DATE: / /

⑤ Anti-forensics techniques.

Americans lost USD 4 billion to cyber attack in 2020

Anti-forensics — designed to prevent individuals — commit cyber attack being discovered.

Following are the Anti-forensics techq.

① Disk Wiping :-
deleting all data — Hard drive — Media storage device

Anti Forensics tools — erase the contents of drive — difficult for forensics analysts to recover the data.
- Drive wiper

② File Encryption :-

process of transforming readable data into an unreadable format using various encryption algo.

③ Steganography :-

hiding Message or files - another file
Anti-forensics tools like Hidder Tear & stego Watch used to hide information like image, audio, video etc.

④ Compression:
- used to reduce the size of file.
- Due to this it is difficult to view or decode.
- Antiforensic tools like WinZip & PKZip can compress files for this purpose.

⑤ Malware:- type of software designed to damage or disable computers and processes. Trojan horses are used to install malware on a computer while ransomware encrypts the contents of a drive, making it inaccessible to the user.

⑥ Process of Digital forensics are as follows (13)

↳ Identification:-
- First step in the forensics process
- includes things like - what evidence is present - where it is stored & how it is stored
- Electronic storage media → pens, computer, Mobile phones etc.

↳ Preservation:-
- data is isolated, secured, preserved.
- preventing people → using digital device
- so digital evidence is not tampered.

↳ Analysis :-

↳ investigation agent reconstruct fragments of data & draw conclusion based on evidence found.

— it take numerous iterations of night examination to support a specific crime theory

↳ Documentation :-

— record of all visible data must be created

— recreating the crime scene & reviewing it.

— involves proper documentation of crime scene like photographing, sketching & crime scene mapping.

↳ Presentation :-

Process of summarization & explanation of conclusions is done.

(7) HDD forensics.

- Easy to retrieve deleted data.
- Traditional forensic can be applied
- New data can be overwritten over existing data
- Data can be written nearly infinite times till there is a bad sector or physical damage
- Evidence is preserved.

SSD forensics

- Difficult to retrieve deleted data
- Data extraction not possible through HDD technique.
- Data can not be overwritten. Old data has to be erased, before writing fresh data.
- Data can be written finite number of times
- Evidence is destroyed.

(8) Data Recovery & Data Carving.

principle → file recovery of deleted files — based on the fact that Windows does not wipe the contents of the file when its being deleted.

- Instead — file system records — storing exact location — deleted file — disk is being marked — "deleted"

— Disk space — previously occupied — deleted filed — labeled as available — not overwritten with zeroes & other data.

— Carving — bit precise & sequential examination — entire content of Hard Drive

— Data Carving — Different from file recovery.

— file carving — raw data on the media — not connected — file system structure.

— Data Carving / file carving — forensic method — reassembling files — unallocated space in drive.

— Data Carving — based — characteristics signature / patterns.

— file recovery techniques — use of file system information — many files can be recovery

— FTK, EnCase, Foremost etc ...

(9.)

- Write blocker — permits read only access
- Data storage devices — without compromising the integrity of Data.

- Prevent any write access — hard Disk.

As per NIST (National Institute of Standards & Technology) general guidelines.

Write Blocker tool — not allow to protected drive — to changed.

- not prevent any operations to a drive — not protected

Write Blocker ← Hardware
Software

Hardware :- hardware blocker — device installed — runs software internally to itself — block write capability — computer to the device attached to the write blocker

Software :- Software Blocker — an application — run on OS — implement software Control — turn off — write capability - OS.

PAGE NO:
DATE: / . /

(10) Copying/.

-Disk cloning:-

-process of copying - content of a hard drive - other desired drive - uncompressed format - Disk cloning.
-Disk cloning software - enables - create one-to-one copy - one harddrive - another hard Drive.

Disk Imaging :- process of compressing - hard drive - including your OS - other data - form of image.
- Unlike disk clone - disk images - stored - single hard drive.

Disk Imaging	Disk cloning.
creates compressed file of your drive that is large in size can be restored later	uncompressed replica of your drive. If harddrive fails you can else the cloned Drive
DI is more flexible lets you create/schedule full, differential & incremental bit by bit backups of your hard drive.	DC is comparatively less flexible. You can only have one clone at a time. since cloning creats an exact copy of a hard Drive

Best suited when creating multiple Backups of your OS & encompassing file	Best suited when upgrading a hard drive or when you need a medium of recovery Eg:- when you have hard drive that is failing.

(11) IDE — Integrated Disk Electronics.
- Disk — uses IDE — IDE disks.
- Officially designated ATA, — informally called IATA
- ATA specification — T13 Technical Committee
= International Committee on Information Technology Standards.
- ATA disks — controller — built into — motherboard — modern System.
- Controller issues commands — 1/2 ATA disks — using ribbon cable
- Cable length max 18 inches & 40 pins.

ATA Standards.

ATA-1 - Single channel — 2 hard disks configured — master & slave.
- P I/O modes 0, 1 & 2.

ATA-2 :-
- called Enhanced IDE (EIDE)
- P I/O modes 3 & 4
- logical Block addressing.

PAGE NO.:
DATE: / /

ATA-3

- Improved - reliability - high speed transfers
- Self-Monitoring, Analysis & Reporting Technology Added.
- Introduced - password protection - better control drive access.

ATA/ATAPI-4

- known as Ultra DMA/33
- Added support for an 80-conductor, 40pin ribbon cable.
- Higher speed DMA transfer mode.

(2.)

- SCSI - Small Computer System Interface
- ATA - 40-44 pin Connectors → SCSI has - wide range - shapes & style.
- SCSI cable - more longer - ATA cables
- SCSI cannot connect more than 2 device.
- SCSI - (X) controller.

Type of SCSI

- Different version of SCSI - boil down - bits transferred - time.
- freq. of signals - or cable - what type of signals used.

- Older version SCSI — normal version
- wide version

- Normal version — 8 bit / time
- wide version — 16 bit / time.
- Newer system — 16-bit transfers.

- Second difference — SCSI version — speed signals in the cable.

Type	Freq	8bit	16-bit
SCSI	5MHz	5 MB/s	10 MB/s
Fast SCSI	10MHz	10MB/s	20MB/s
Ultra SCSI	20MHz	20MB/s	40MB/s
Ultra 2	40MHz	40MB/s	80 MB/s

(15.)

8 Ans — 1,2 point.

- Recover deleted & Hidden files.
  - ↳ file deleted / hidden — criminals
  - recovered — using Recovery tools
  - form imp forensic evidence.

↳ Can analyze almost all memory-based devices.

- Deleted files — cellphone, computer, USB, etc — can examined — Forensic data recovery.

↳ Finding Unknown.

- Patterns, links — sets of data
- connecting dots — uncover info.
- might not be initially considered
- Irrelevant — inaccessible — help in recovering unknowns.

↳ Preserves data integrity.

- Integrity — collected data — projected using write blocker
- helping in presenting — evidence in og state.