Storage Forensics 1

A Top Down Approach

Recap

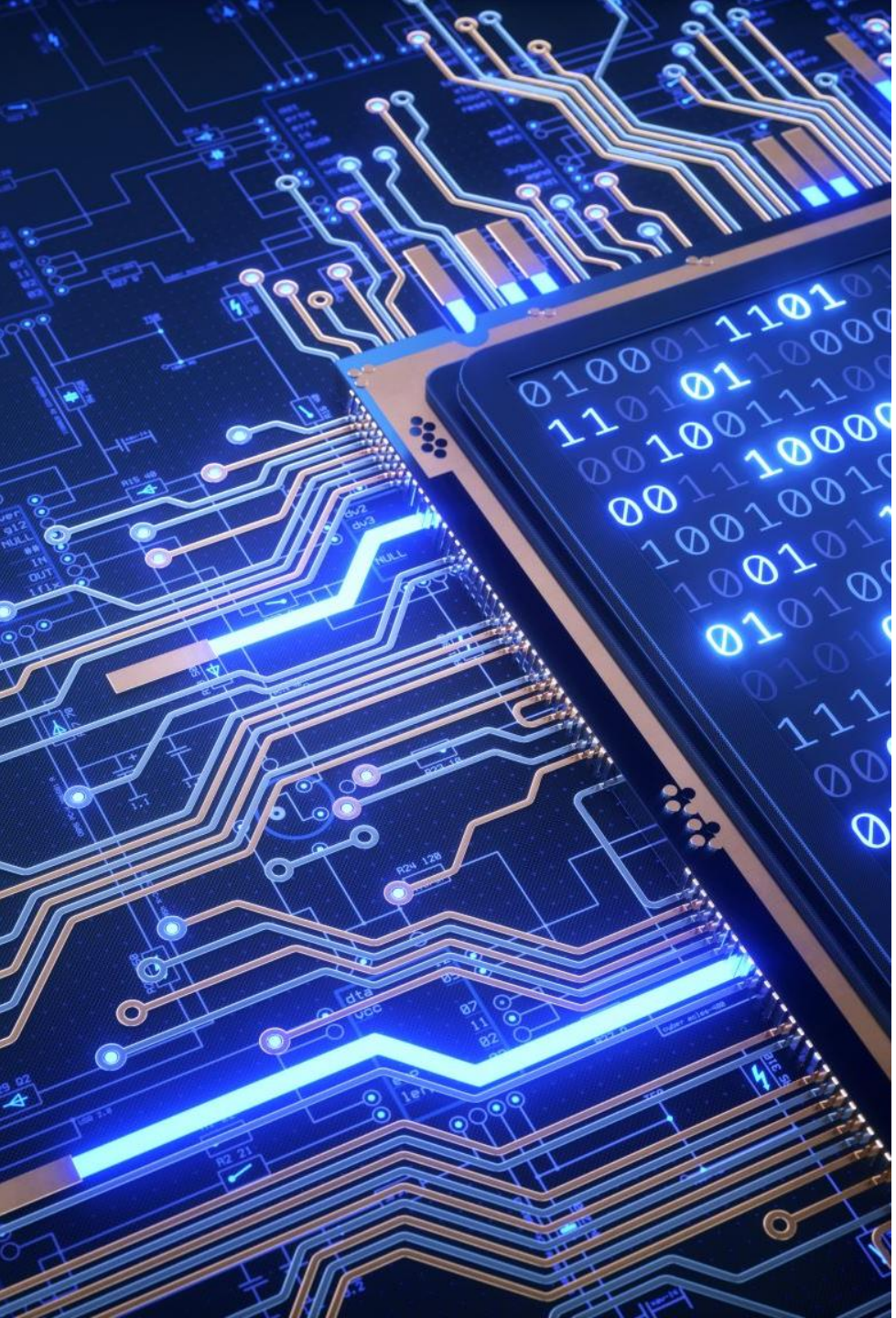
- The potential sources for our Digital Forensics data is practically limitless
- We use Forensic images in Forensics
- Those are not pixel data picture, rather “snaphots” of data on a machine
- Bitstream VS Backup
- We distinguish between Live and Static Acquisition
- Data can come from outside of the “computer”
- We make 2 copies and validate our results on Static acquisition

Difference between forensics on a magnetic hard disk vs an SSD

In a nutshell

What are we going to discuss here?

- Relevant Forensics concepts
- Basic operation of most common HDD and SDD, as we need to understand them, to be able to work with them.
- What do these differences in operation translate to data recovery and forensics in general? (At an abstract level)
- What is out there in terms of technology.
- Your options for engaging with the drives.



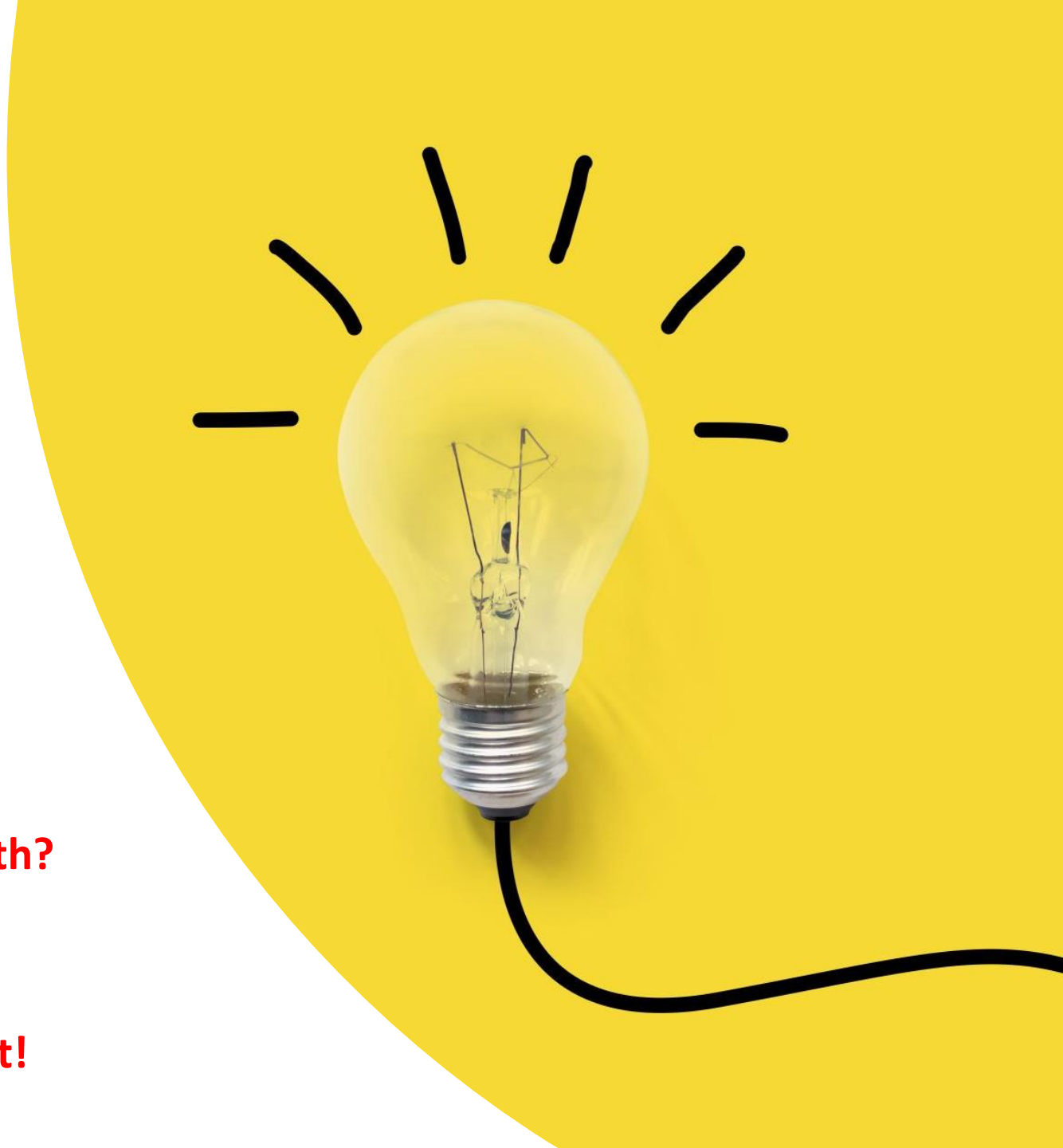
TL;DR

Solid-state drives (SSD) are predominantly being used as storage devices these days.

- Most digital devices like: desktop computers, laptops, tablets and smart phones use SSDs.
- SSD **uses flash** memory to store data.
- Unlike “traditional” hard drives, it is comparably harder to recover deleted data from SSDs (The “Why” Is discussed later)
- This means it consequently impacts digital investigations detrimentally.
- No, HDD as a technology is far from dead and replaced by SSDs

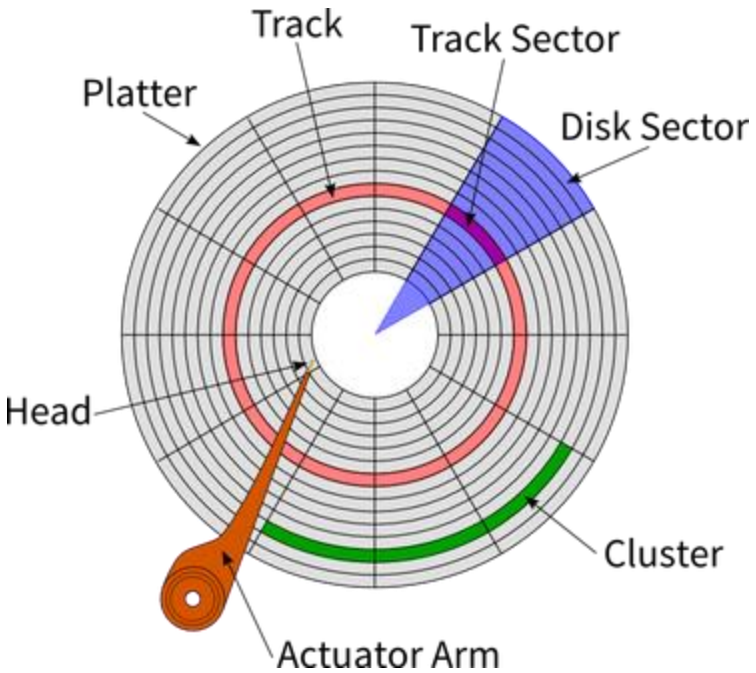
SSD VS HDD, the test (Which of the technology comes to your mind?)

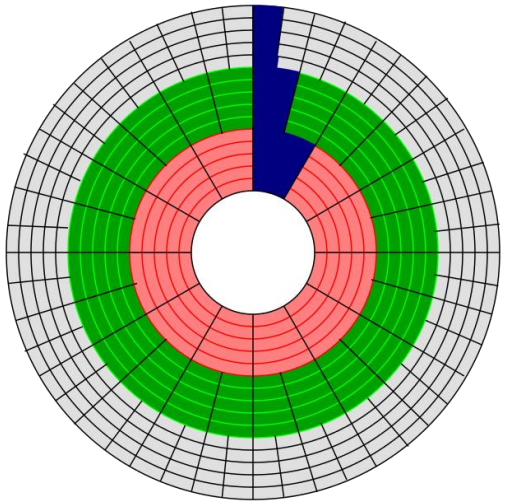
• Magnetic Disks	• **HDD**
• Quantum Tunnelling!	• **SSD**
• NAND	• **SSD**
• SLC,QLC, PLC	• **SSD**
• NVME	• **SSD**
• SATA	• **HDD, SSD**
• 3D	• **Technically both?**
• Lasers	• **Lasers! HAMR**
• RPM	• **HDD**
• TLA	• **Both have a lot!**



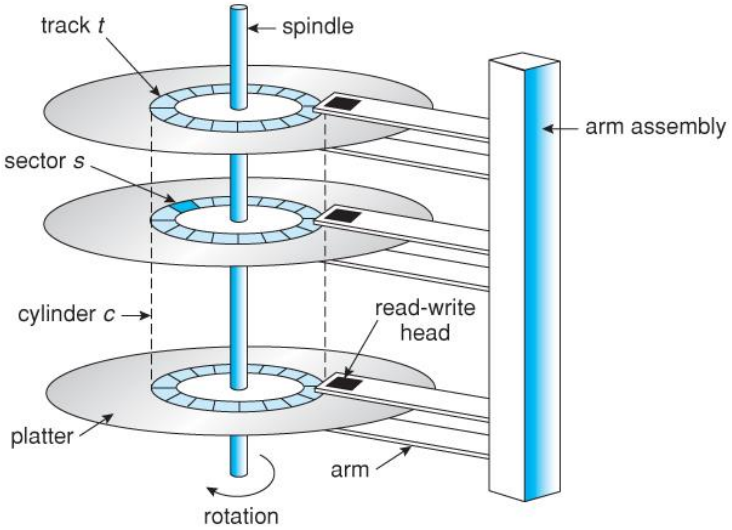
Background

- Every kind of information that can be stored on a computer is represented at some point as a pattern of 1s and
- 0s, for the purposes of computation and storage. These 1s and 0s are, however, merely a convenient
- Interpretation for human use – not a physical reality.
- Let's check out how HDDs do this VS the SSDs!





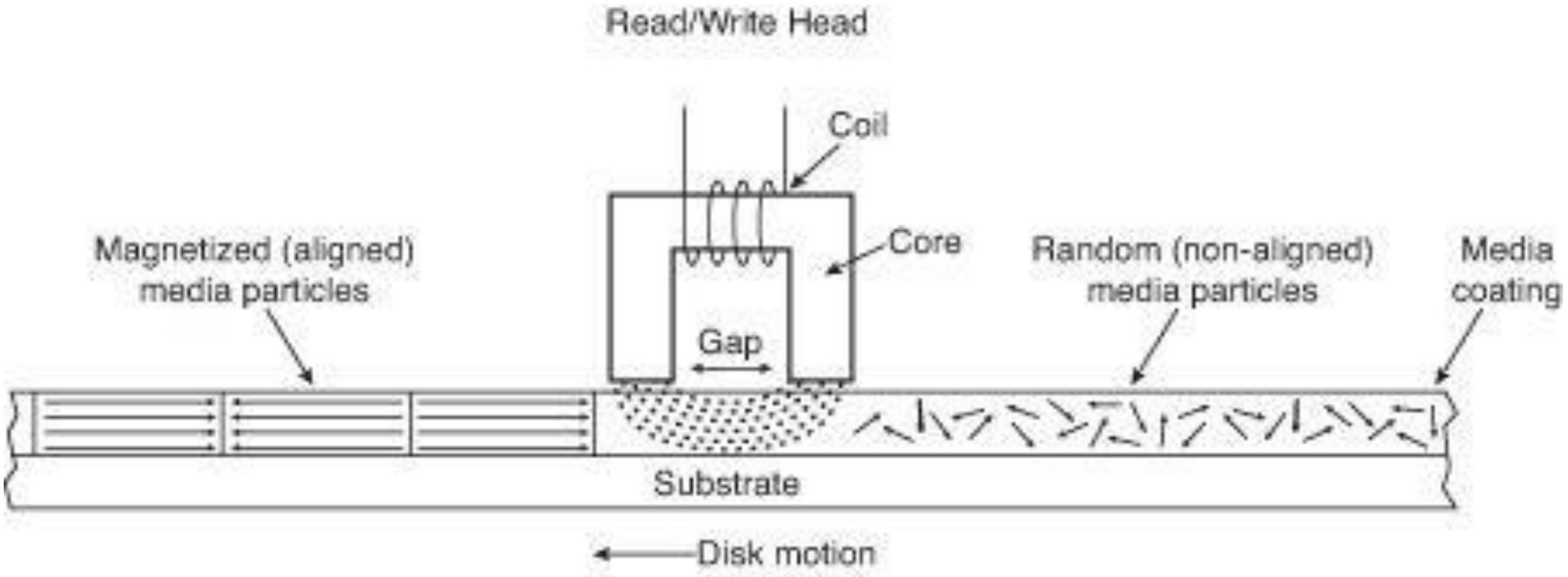
Sector 0

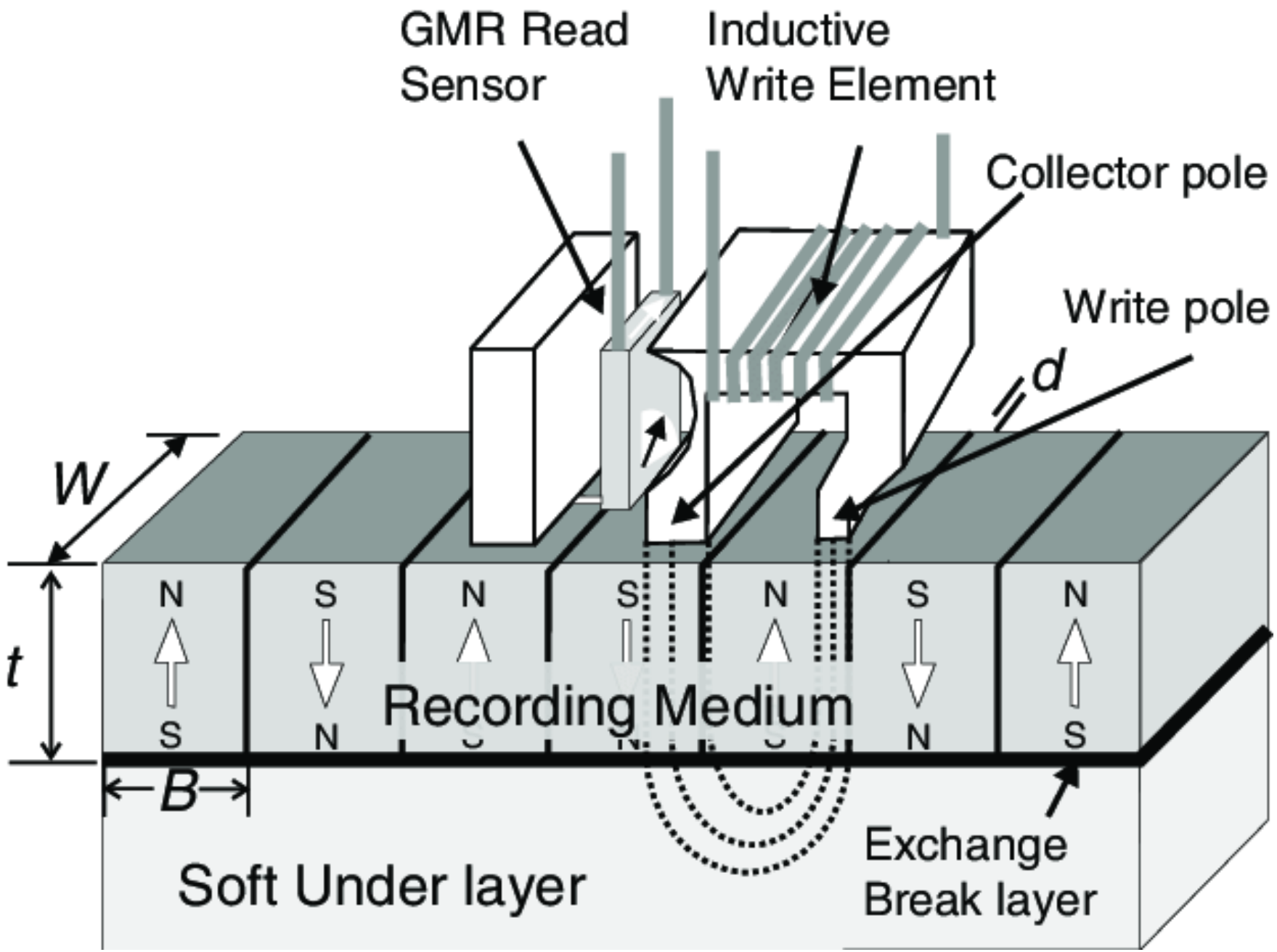


Disk technology - Magnetic

This image purely exists because HDDs record magnetic Flux changes and that made me think of the Flux Capacitor!

The platter. What is this exactly?


Read/Write Head
Coil
Core
Magnetized (aligned)
media particles
Gap
Random (non-aligned)
media particles
Media
coating
Substrate
Disk motion


GMR Read
Sensor
Inductive
Write Element
Collector pole
Write pole
d
W
t
N
S
N
S
N
S
N
S
N
S
N
S
Recording Medium
B
Soft Under layer
Exchange
Break layer

Disk technology – Important to remember

- Data stored in sectors of size 4KiB (512bytes on old (<2010) disks)
- The term block is also sometimes used, but block is an OS specific term in this context (normally 4KiB though)
- Data is addressed at sector level and stored in sector sized chunks
- Data is addressed using LBA at the OS/driver level and converted to something else like (Cylinder-head-sector (CHS)) by the disk firmware

How SSDs Are Different?

"If I had asked people what they wanted, they would have said faster horses." - Henry Ford

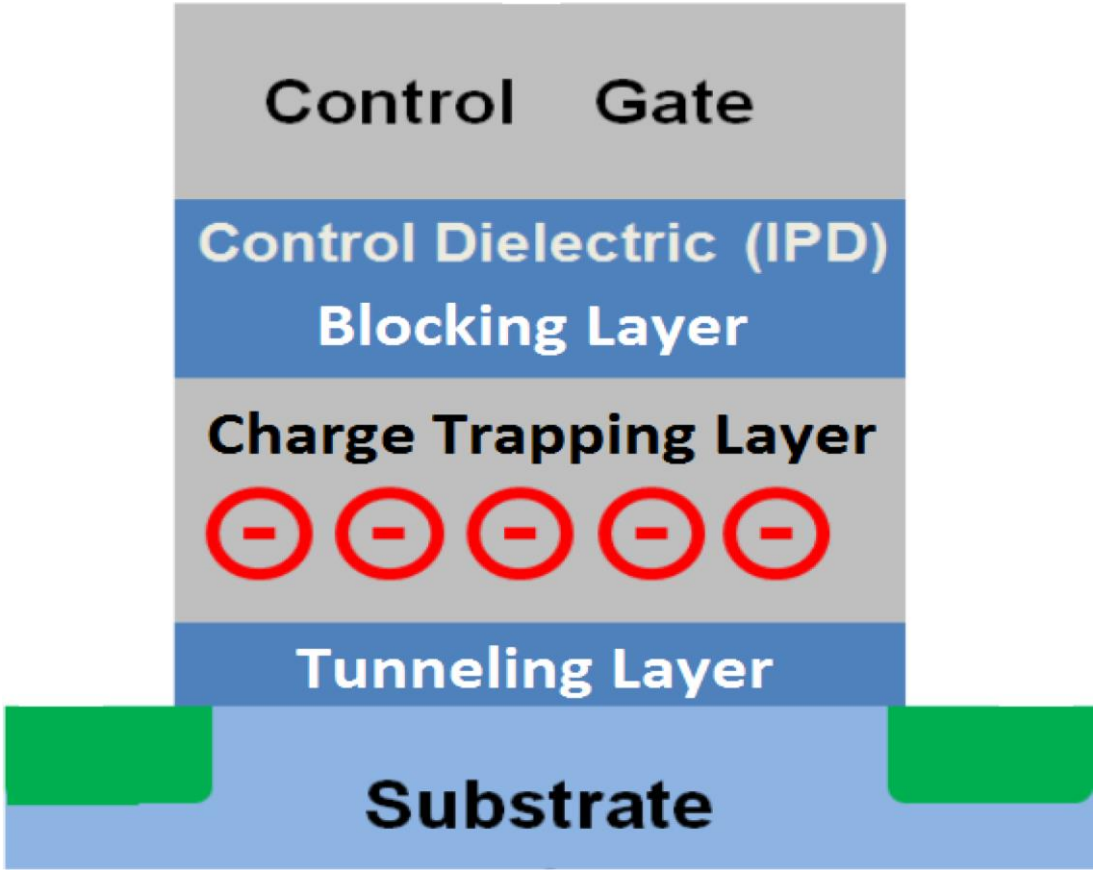
NAND Flash arrays

Before We can Understand Forensics, We need to understand the inner workings for some more detail

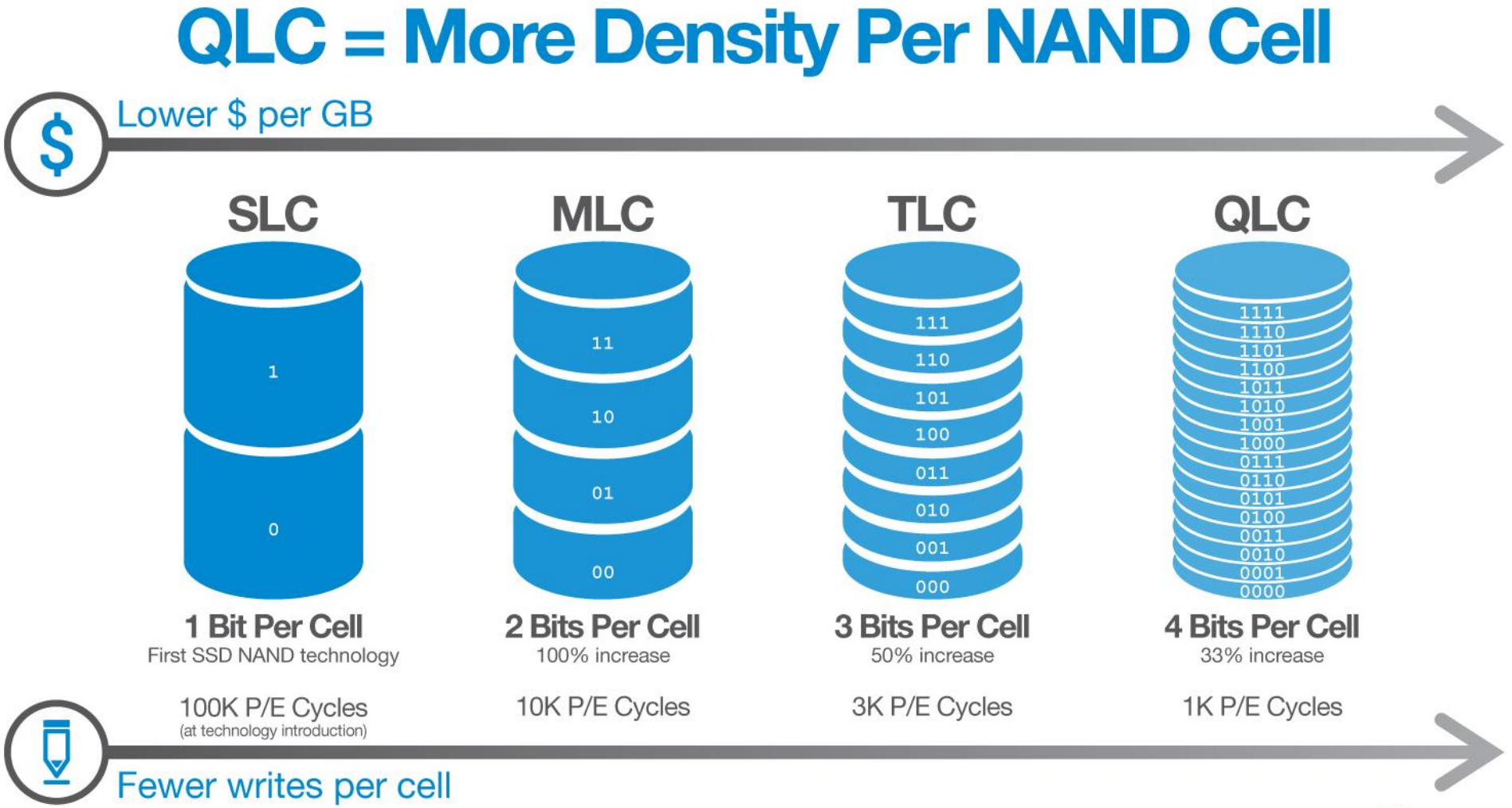
- It's a Micron 64L 3D QLC having 2GB Dram Cache, 2000GB Storage
- Endurance : 400TBW
- Controller : Silicon Motion SM2263EN
- NVM Express Connection

3D Charge Trap NAND Flash Memories

- We are trapping electrons (And keeping them in place for 10 years)
- Uses the power of Quantum physics!

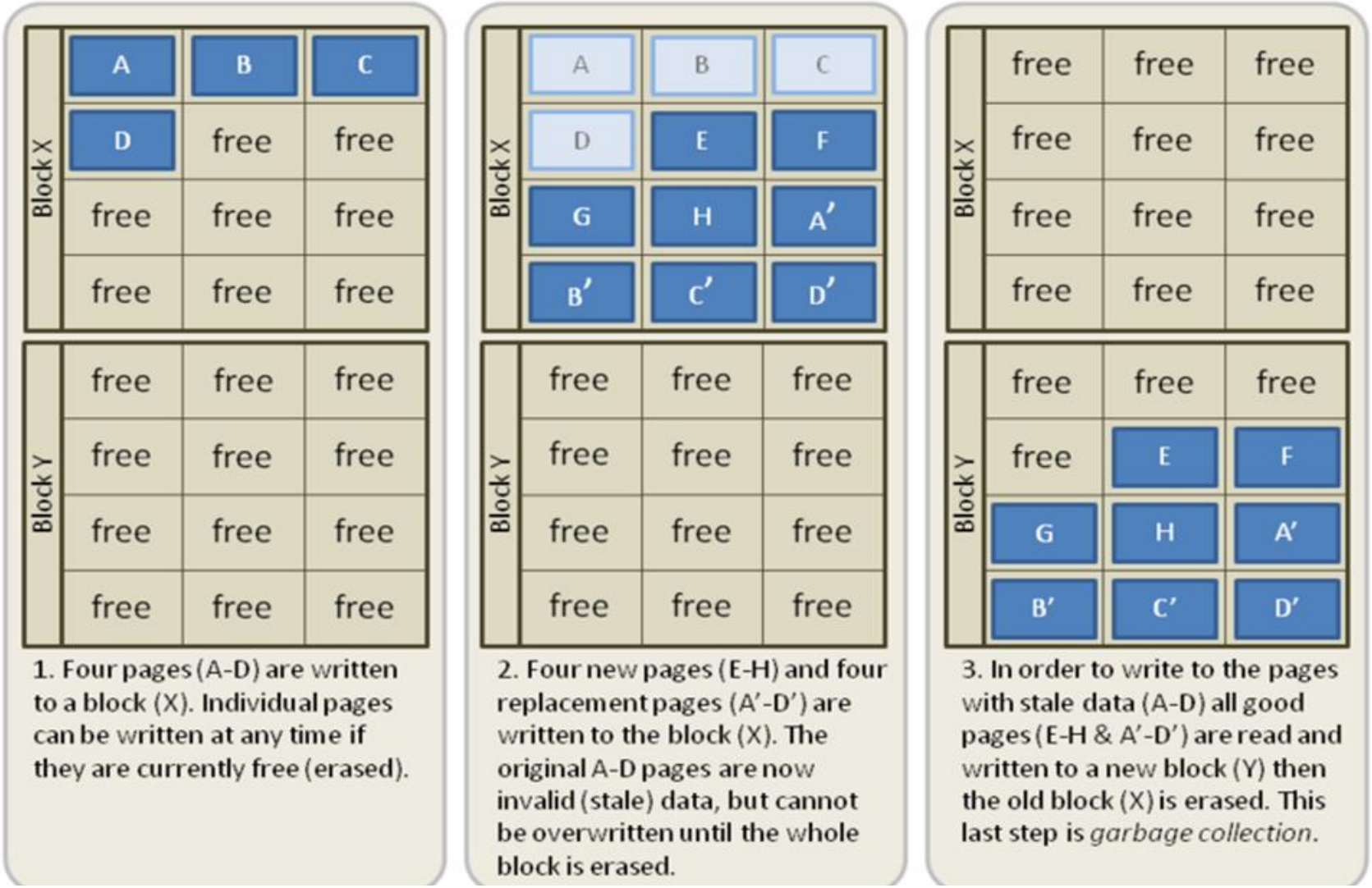


The Key Difference between Density



Reads, Writes, and Erasure

- Reads Data in Pages
- Writes Data in Pages to free
- **Can only erase by Blocks**
- **Cells Have Limited Life**



This leads to interesting properties

- Control of SSDs is very complex compared to HDDs

SSDs will need to employ tricks like :

- Wear Levelling
- Garbage Collection
- Over Provisioning
- TRIM

All of which impact the data recovery from these drives.

This also mean
s SSDs are potentially destroying/ altering data actively because:

- Over Provisioning
- Flash Translation Layer (Another built in Abstract to LBA(Logical Block Adressing))
- Constant Wear Levelling
- Constant Automatic Garbage Collection
- Self corrosion(The process of destroying evidence because of the above)
- Encryption in Hardware!

SSD Wear levelling Details

Every time you use a part of an SSD, it degrades. Use it too much and it stops working

If left unchecked, this could lead to Data corruption

The firmware controller of an SSD implements wear levelling to prevent this. At quite moments, frequently used data is moved to less worn parts of the SSD.

Care is taken to make sure that data isn’t moved unnecessarily, but wear levelling is still a constant process

This can mean that there are multiple copies of the data on the SSD, but only one that the OS knows about

Disk technology – SSD - corrosion

- Modern SSDs in modern OSes can suffer from forensic data corrosion through use of the TRIM command for SSDs
- If we are continually making copies of everything, every time we need to rewrite then that could leave lots of dirty pages around (esp as erasing takes time)
- We are probably copying data that isn't valid any more as all pages are copied
- TRIM allows the OS to mark a page as "no longer needed" and TRIMmed pages will not be copied during an overwrite
- Because the garbage collection is running constantly, as is wear levelling, this means that deleted data will get physically removed from the SSD in a relatively short period of time!
- Fortunately(??) not all consumer drives implement TRIM properly

We just did an image of a new drive, Questions We need to ask then?

- Admissible?
- Trustable?
- What Are the processes to recover?
- Will it change at a later stage?

What are our options as Forensic Scientist in 2021?

The good:

- Imaging Devices are catching up
- Processes are catching up
- Needs more care in the process, and people are working on solutions continuously

The "Keep in mind"

- Should be considered as a grey area as far of forensic recovery and legal validation are concerned
- Past data and data blocks can be deleted without any warning

Things we did not mention, but you should explore

- NVME – The connection standard and how it makes forensic recovery different
- Optane- What is it? How does it operate?
- Issues Soldered on formats of SSDs that come with modern laptops
- What about devices like Phones?

Additional Reading/ References

- Inside Solid State Drives (SSDs) Second Edition /Springer/
- Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? DOI: 10.15394/jdfsl.2010.1078