# HDD DATA RECOVERY IN DIGITAL FORENSICS

## Lesson 1

SUMURI

EDRTOOLS
for Digital Forensics & Data Recovery

SPEAKER:

LUCA MARELLA

DATA RECOVERY TEACHER AT EDR TOOLS

# Why this training?

In these training sessions we'll discover how a Hard Drive works physically and logically. This information is not easily available on the internet but is vital in order to understand how to diagnose or even understand if a drive was tampered to prevent access to the data area

# Topics

**Lesson topics:**

- HARD DRIVE PARTS AND FUNCTIONS
- ELECTRONIC BOARD
- MECHANICAL PARTS
- MAGNETIC HEADS POSITIONING SYSTEM
- HOW ARE BITS STORED
- MAGNETIC RECORDING METHODS

# HARD DRIVE PARTS AND FUNCTIONS

HDDs are an example of mechatronics, where electronics and mechanics are fused together.

Understanding how the interfacing of mechanics by electronics works allows us to understand the possible causes of data loss, as well as possible anti-forensics techniques to prevent a forensic investigation

# HARD DRIVE PARTS AND FUNCTIONS

We will start by dividing the HDD into 2 main parts:

HDA - Head Disk Assembly

PCBA - Printed Circuit Board Assembly

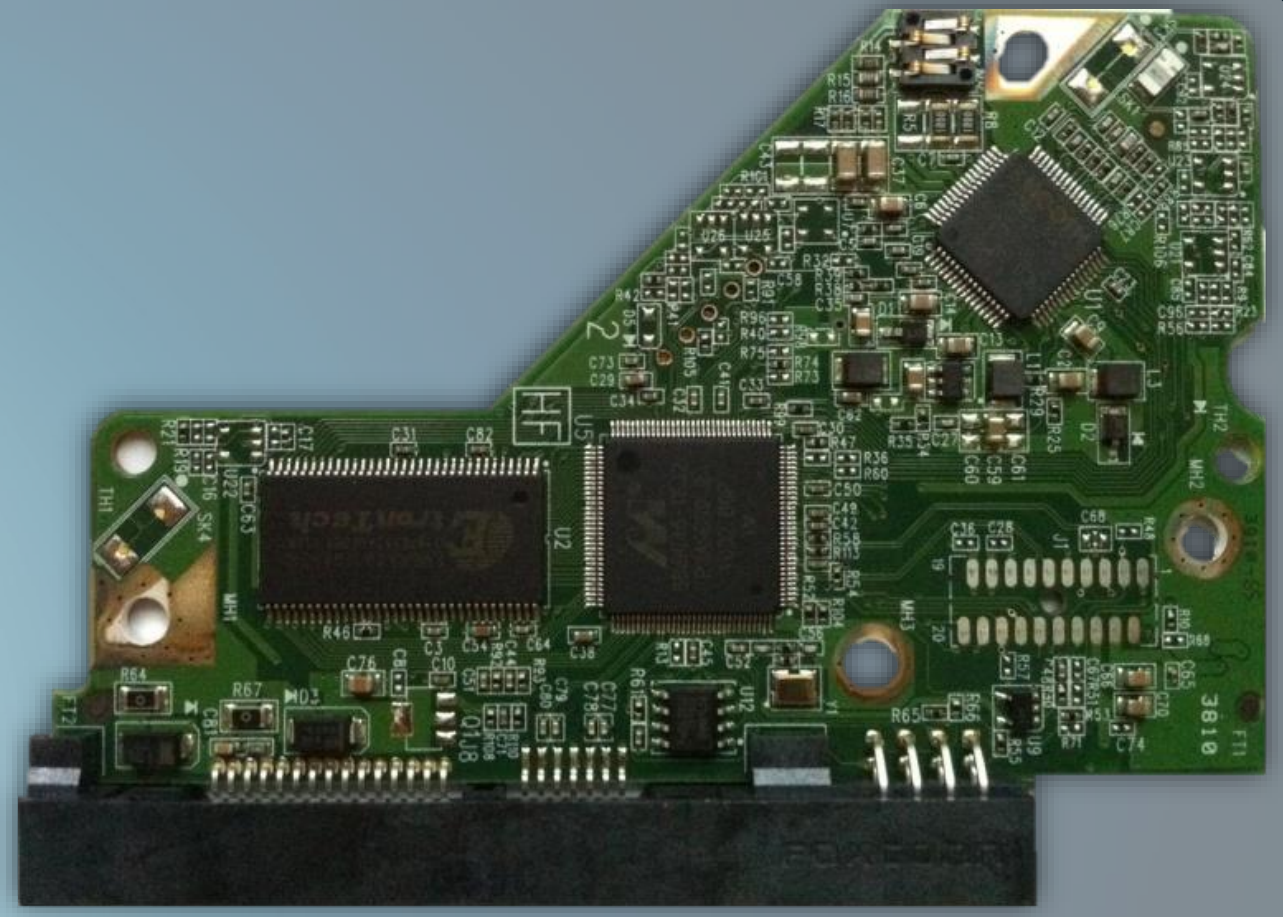
SUMURI

EDRTOOLS for Digital Forensics & Data Recovery

# HARD DRIVE PARTS AND FUNCTIONS

**PCBA:**

Is the mainboard, its aim is to make the drive load its own firmware and communicate with the PC through a controller



SUMURI

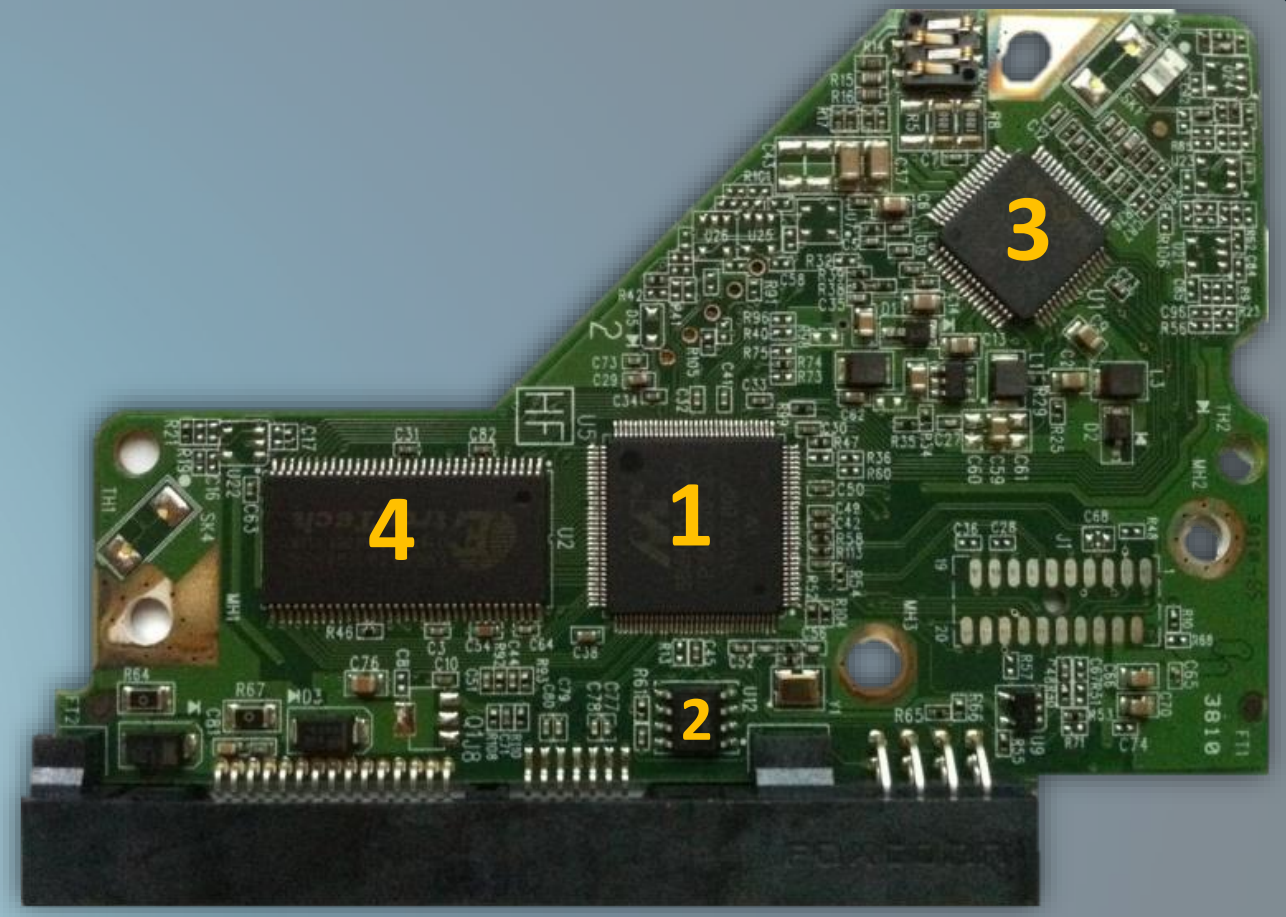
EDRTOOLS for Digital Forensics & Data Recovery

# HARD DRIVE PARTS AND FUNCTIONS

**PCBA:**

Main components

1. MCU
2. ROM
3. SPINDLE CONTROLLER
4. BUFFER

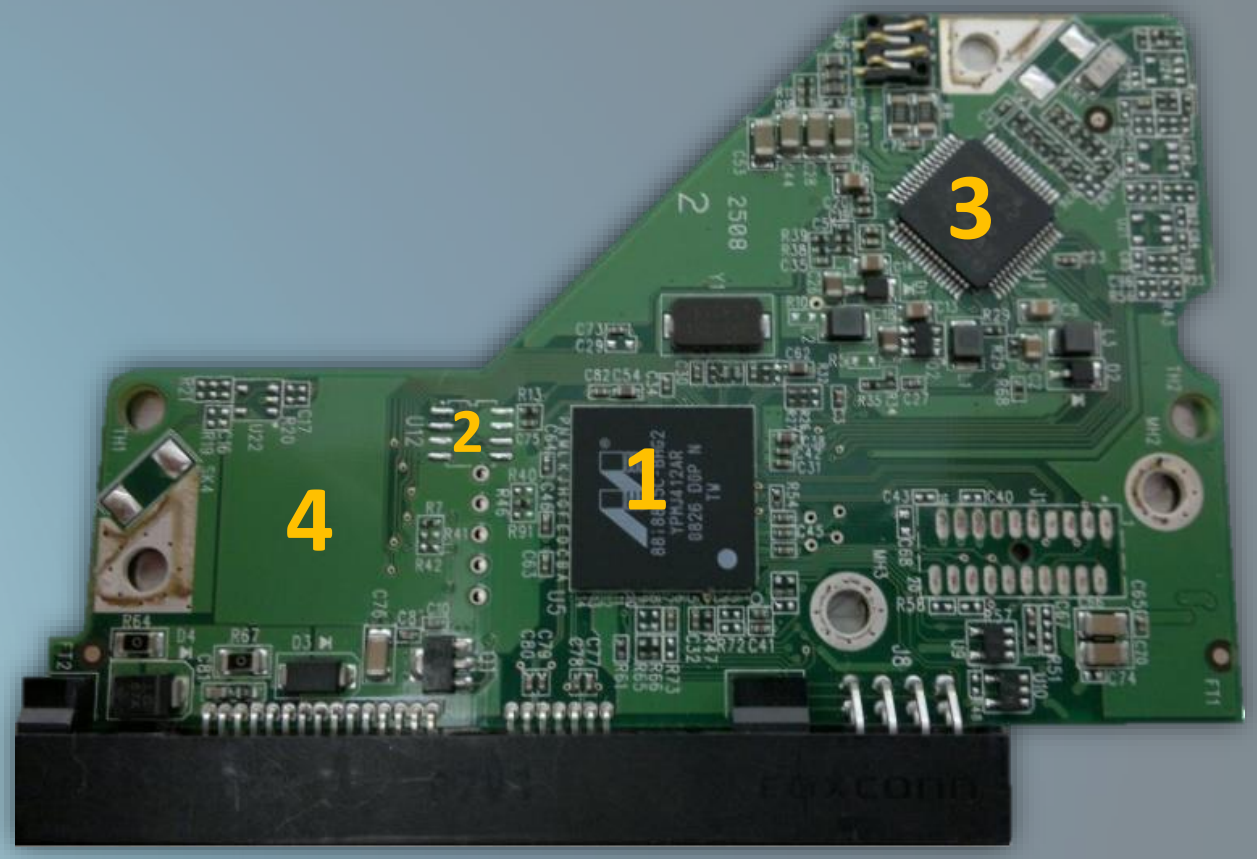


# HARD DRIVE PARTS AND FUNCTIONS

**PCBA:**

Main components

1. MCU
2. ROM
3. SPINDLE CONTROLLER
4. BUFFER



SUMURI

EDRTOOLS for Digital Forensics & Data Recovery

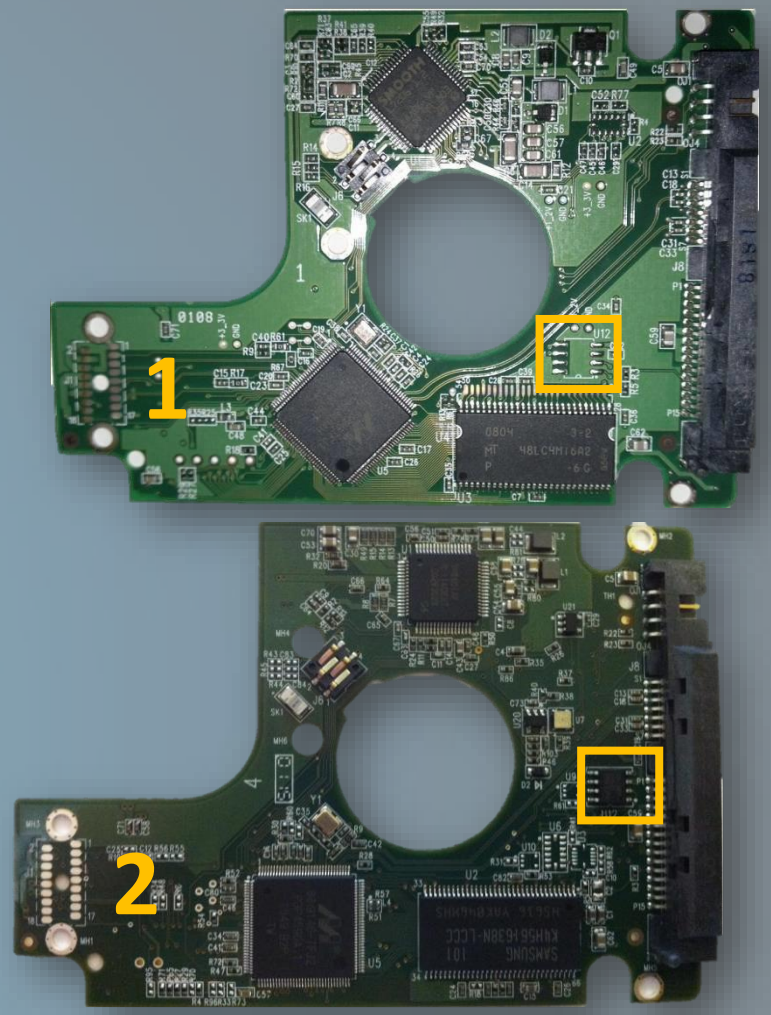
# HARD DRIVE PARTS AND FUNCTIONS

**PCBA:**

EMBEDDED VS EXTERNAL ROM

[1] Western digital laptop drive embedded rom

[2] Western digital laptop drive external rom

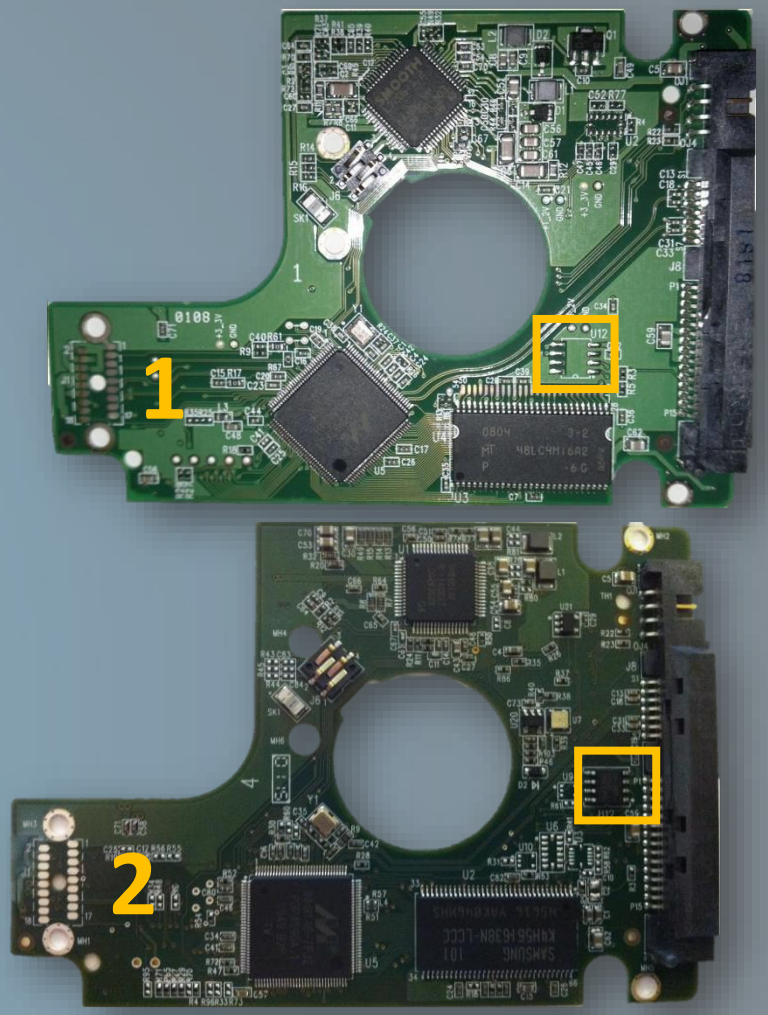


# HARD DRIVE PARTS AND FUNCTIONS

**ROM:**

Inside a ROM chip we can find

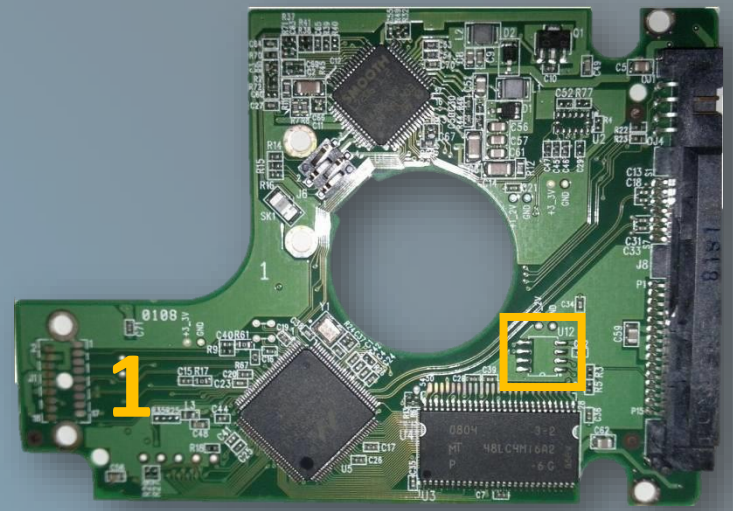
- Code
- Modules
  - Adaptive data
  - Head map
  - Boot flags
  - Techno overlay modules
  - Modules directories

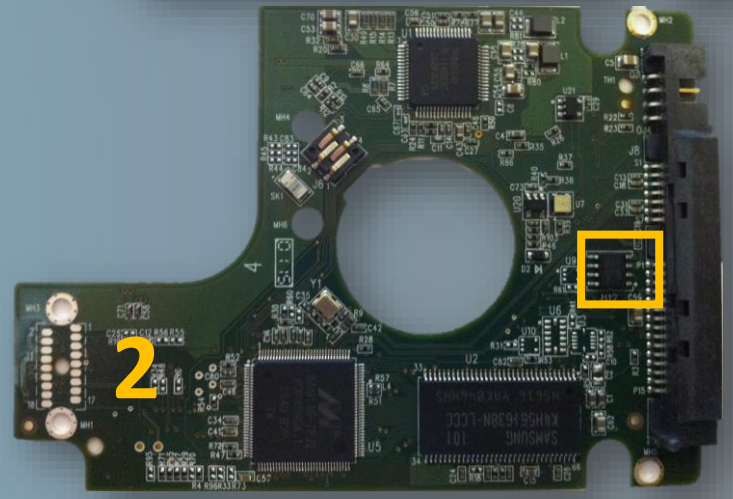


# HARD DRIVE PARTS AND FUNCTIONS

**ROM:**

- Is ROM worthy to analyze?
- Which kind of data can be stored?
- Should ROM be tampered with?
- Is ROM somehow hashed in standard forensic acquisition?



SUMURI

EDRTOOLS
for Digital Forensics & Data Recovery

# HARD DRIVE PARTS AND FUNCTIONS

**HDA:**

Includes the external case with all the magnetic and mechanical parts

SUMURI

EDRTOOLS for Digital Forensics & Data Recovery

# HARD DRIVE PARTS AND FUNCTIONS







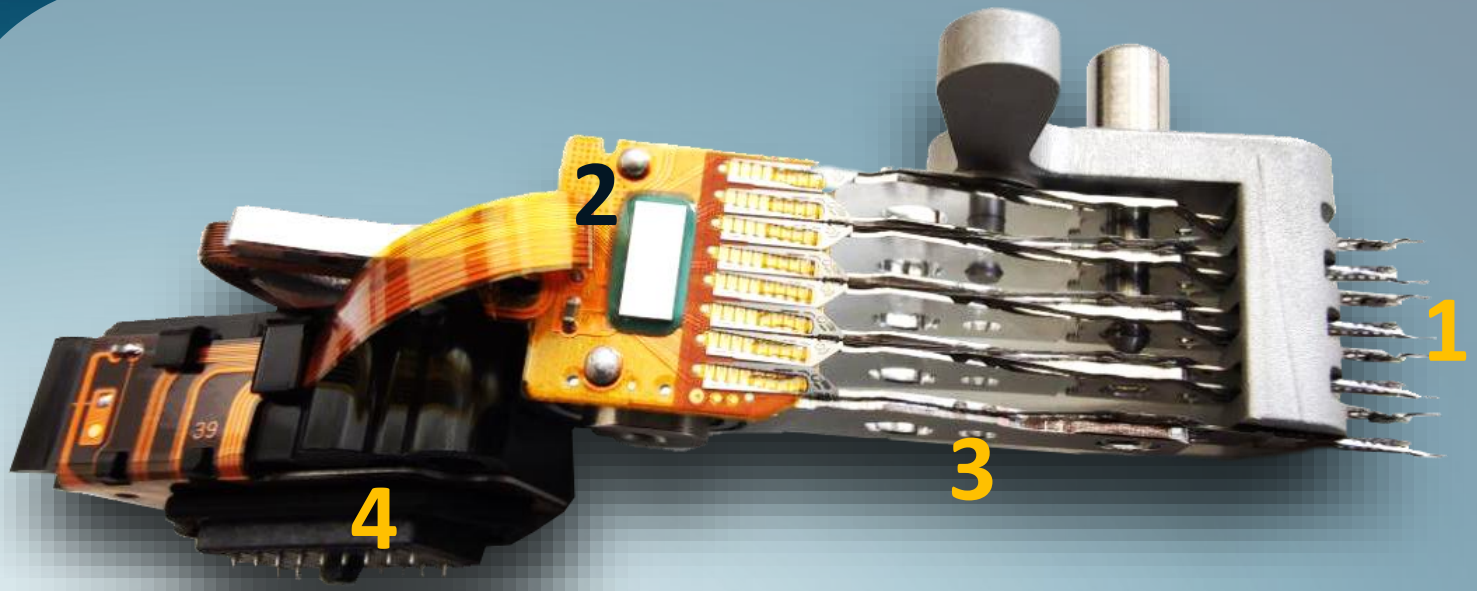

**HDA:**

1. SPINDLE MOTOR
2. AIR FILTER
3. HEAD STACK
4. BOTTOM MAGNET
5. TOP MAGNET
6. SPACERS
7. HEAD RAMP

SUMURI

EDRTOOLS for Digital Forensics & Data Recovery

# HARD DRIVE PARTS AND FUNCTIONS

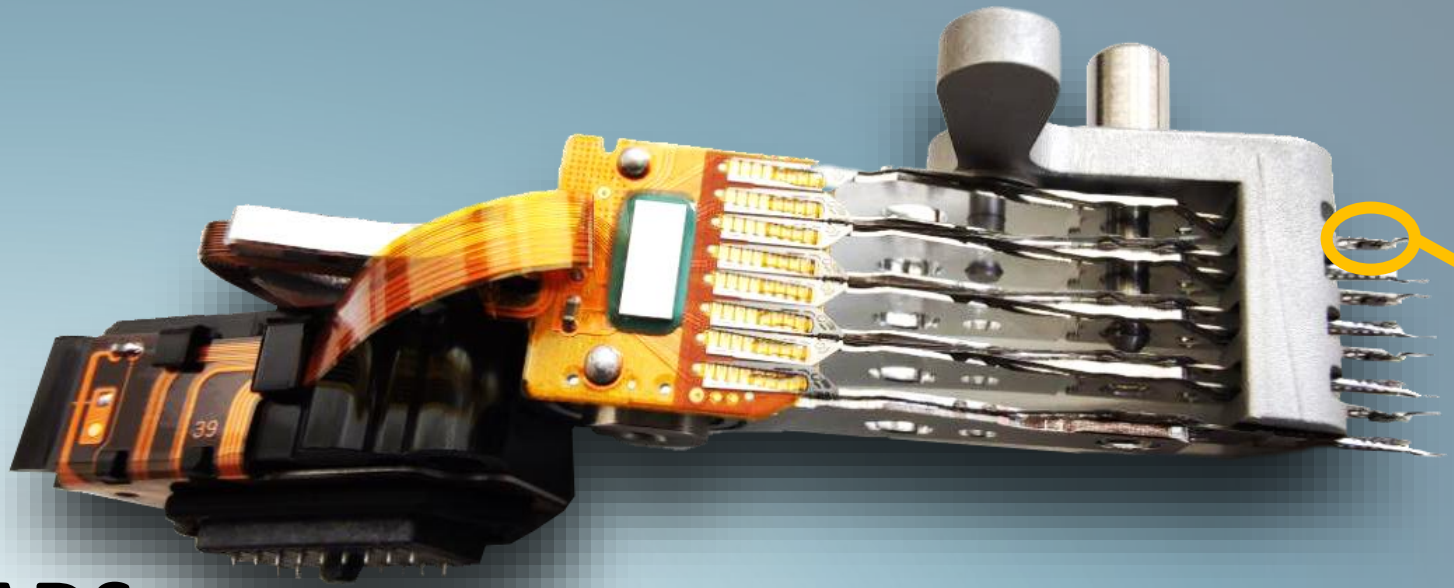


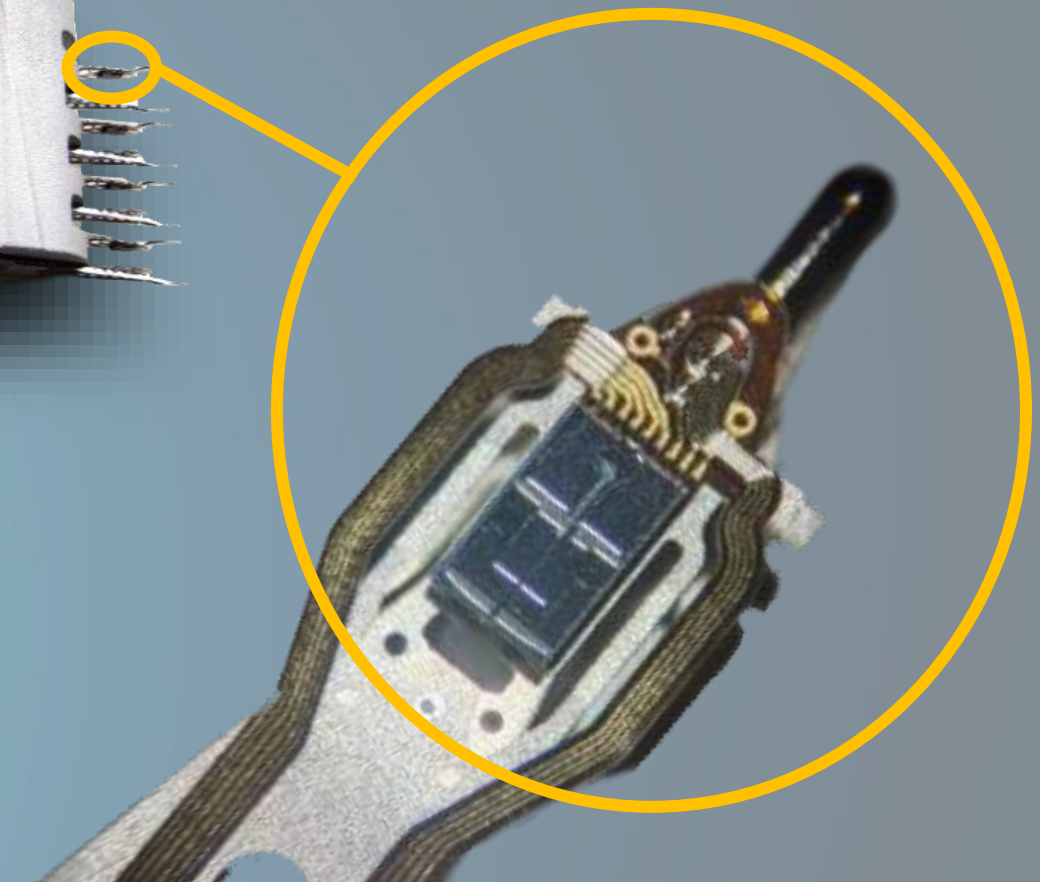


## HEAD STACK

1. R/W heads
2. Preamp chip
3. Head sliders
4. Head stack connector
5. VCM Voice Coil Motor

# HARD DRIVE PARTS AND FUNCTIONS





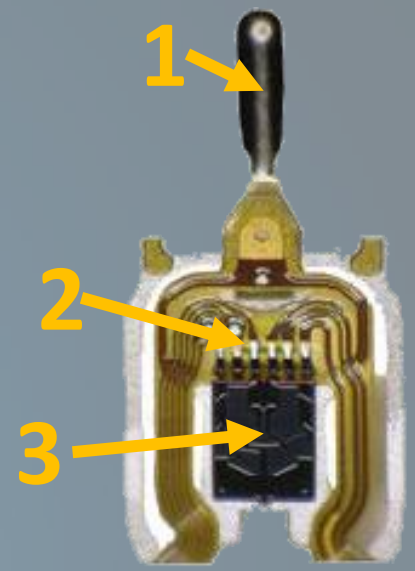
**HEADS:**

Read element and write element

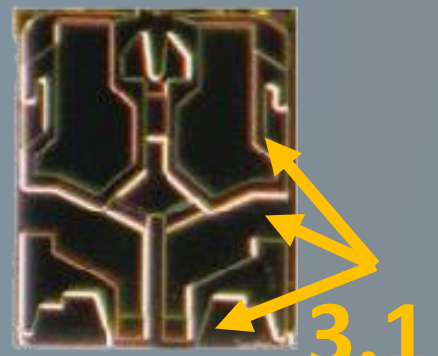
# HARD DRIVE PARTS AND FUNCTIONS

## Head (A)

1. Load/unload tip
2. Reader/writer/heater connectors
3. Read/write element
    1. Air bearing contour
4. Micro actuator





# HARD DRIVE PARTS AND FUNCTIONS

**The HDD is not sealed.**

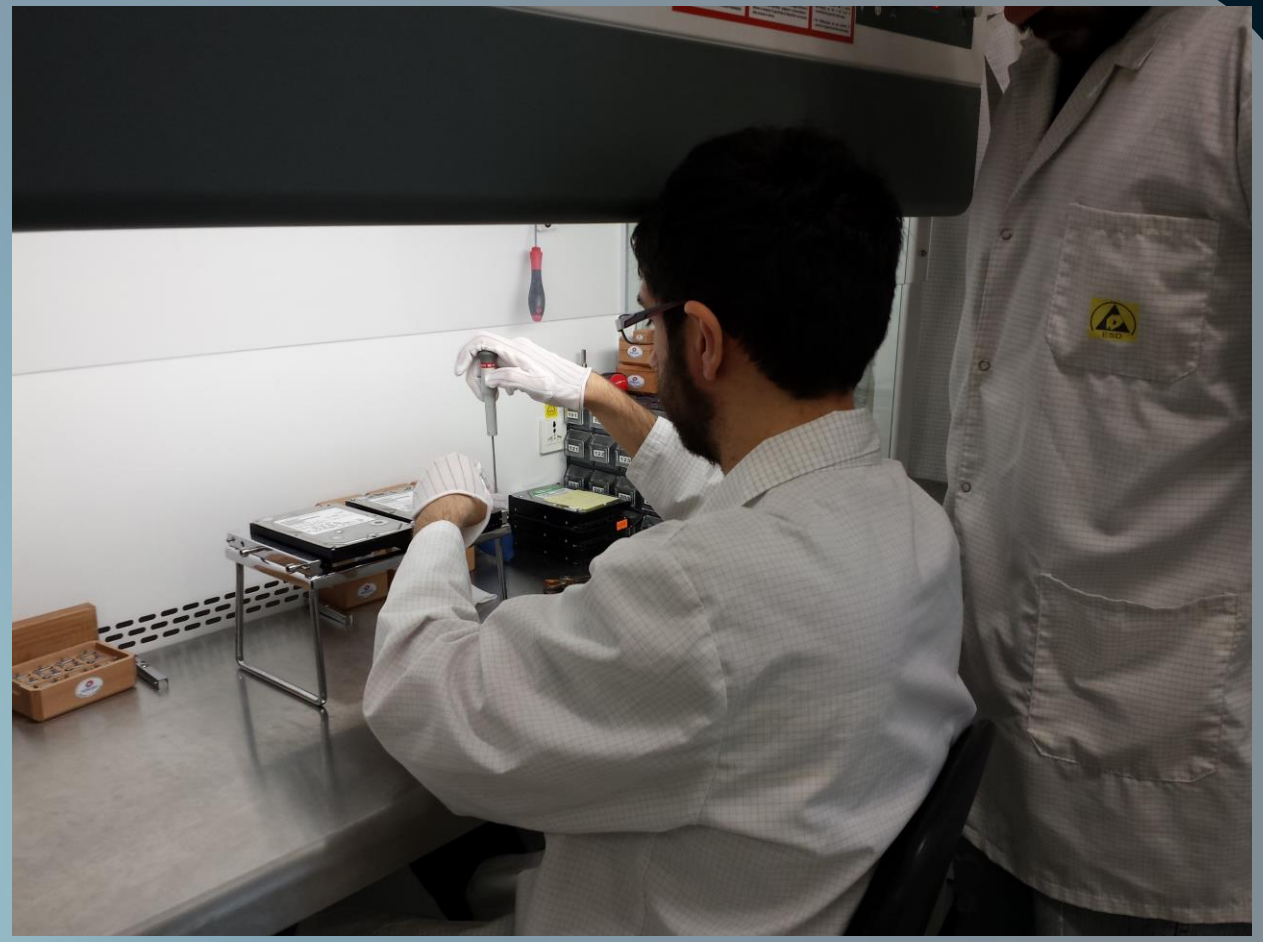
- Air is needed to let the heads “fly” over the platters
- Air must be filtered


# HARD DRIVE PARTS AND FUNCTIONS

**Importance of clean environment**

To open an HDD we need to work in a clean environment, such as a flow laminar clean bench.

We normally use an ISO5 flow hood.



SUMURI

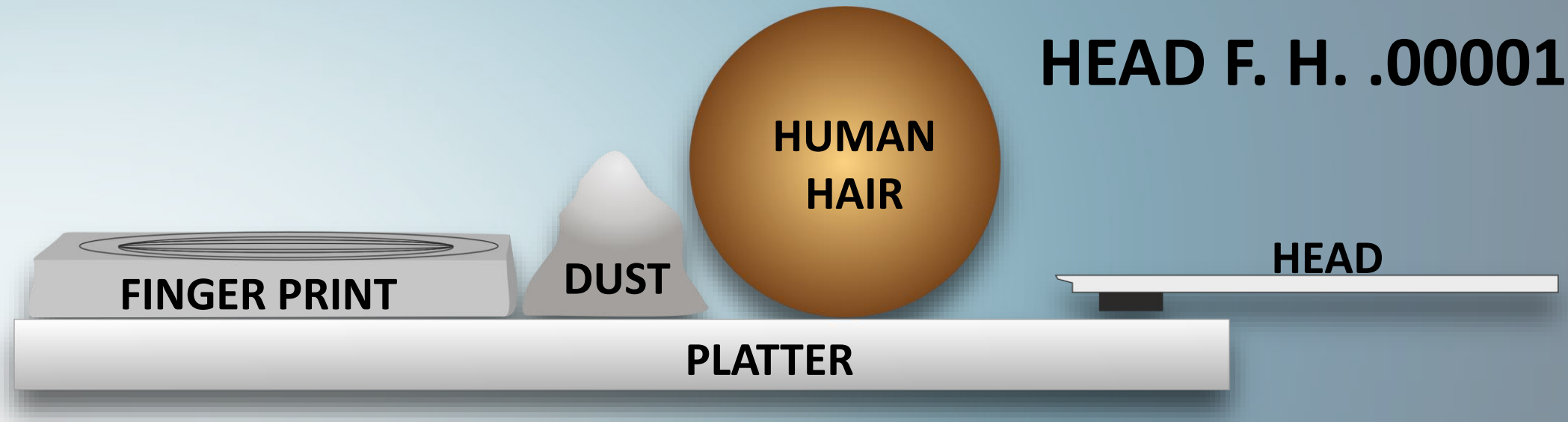
EDRTOOLS for Digital Forensics & Data Recovery

# HARD DRIVE PARTS AND FUNCTIONS

## CONTAMINATION VS FLIGHT HEIGHT

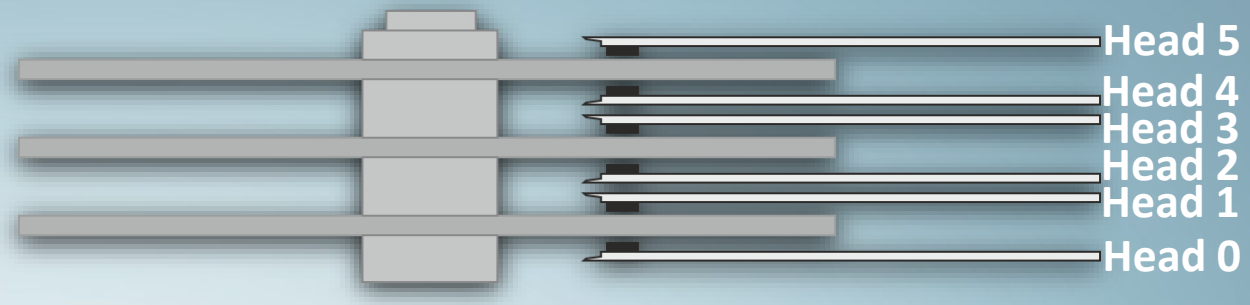
FINGER PRINT .00062 in.
DUST PARTICLE .0015 in.
HUMAN HAIR .003

**HEAD F. H. .000015 in.**

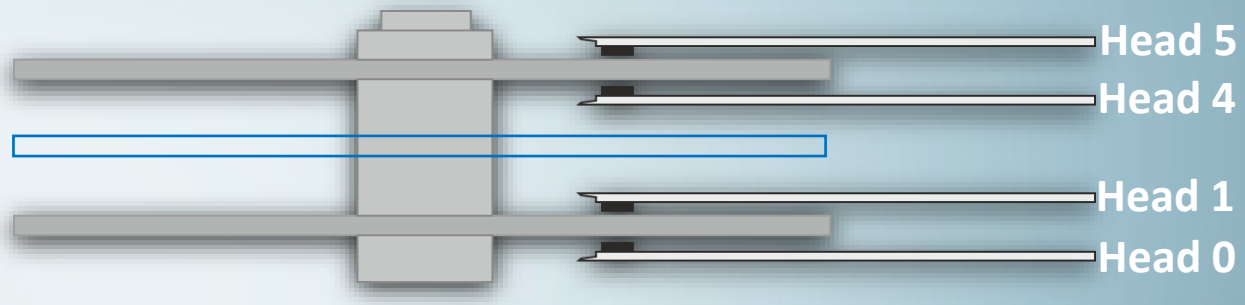


# HARD DRIVE PARTS AND FUNCTIONS

## Positioning system : Head map




Head map:
Heads number 6
Physical 0,1,2,3,4,5
Logical 0,1,2,3,4,5



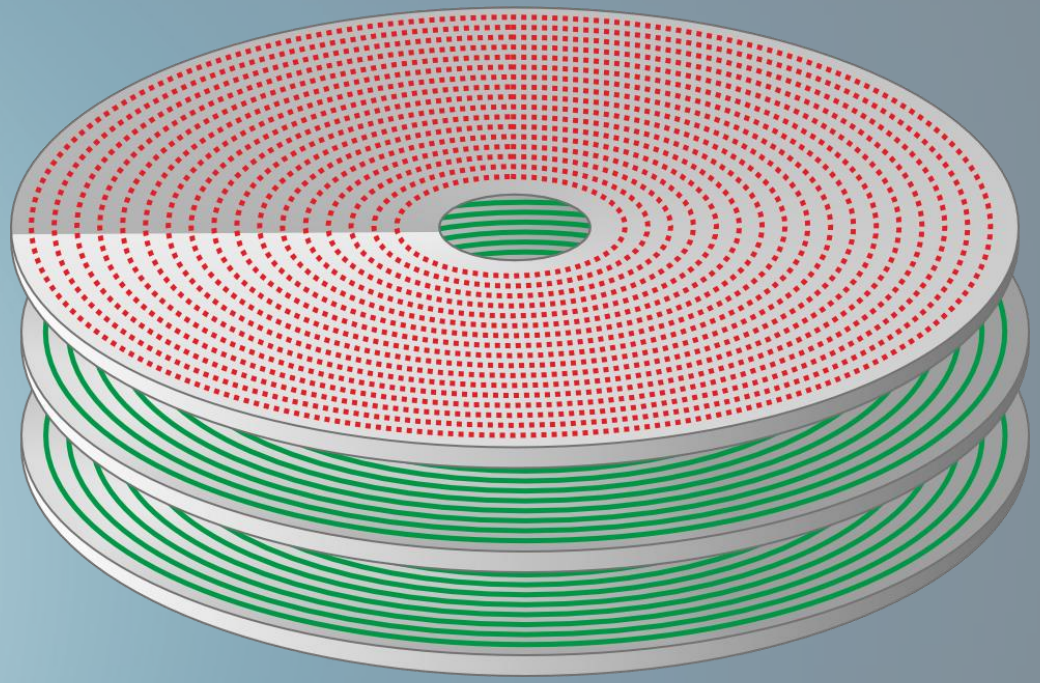

Head map:
Heads number 4
Physical 0,1,4,5
Logical 0,1,2,3

# HARD DRIVE PARTS AND FUNCTIONS

## Positioning system :

SERVO INFO

EMBEDDED



SUMURI

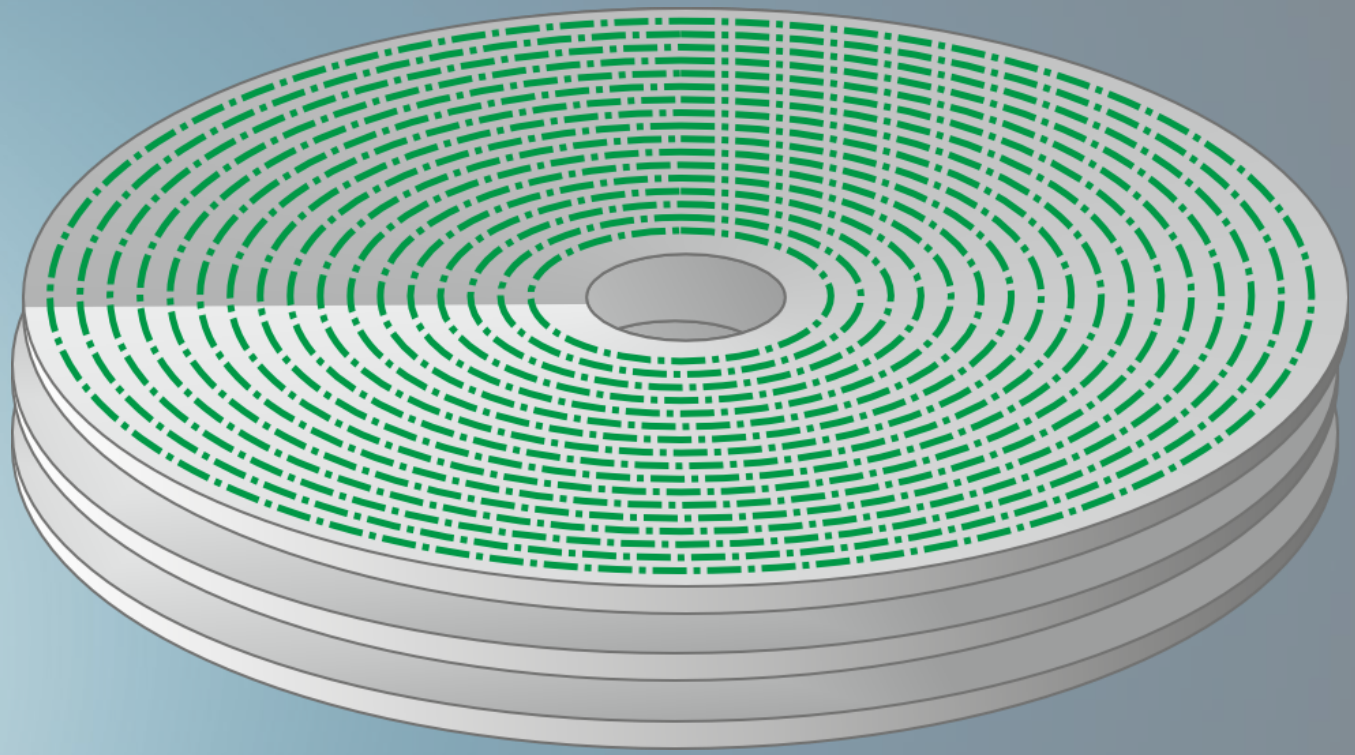
EDRTOOLS for Digital Forensics & Data Recovery

# HARD DRIVE PARTS AND FUNCTIONS

## Positioning system :

SERVO INFO

SECTOR LEVEL



# HARD DRIVE PARTS AND FUNCTIONS

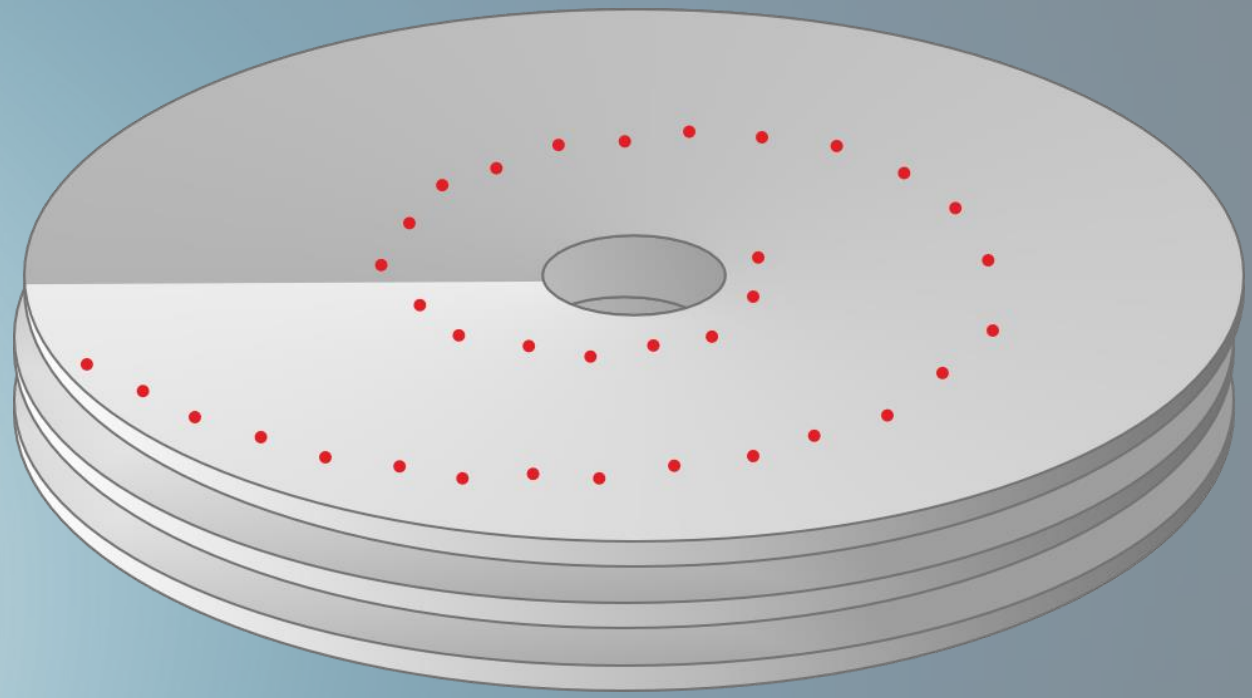
## Positioning system :

SERVO INFO

SPIRAL

WITH RELOCATION

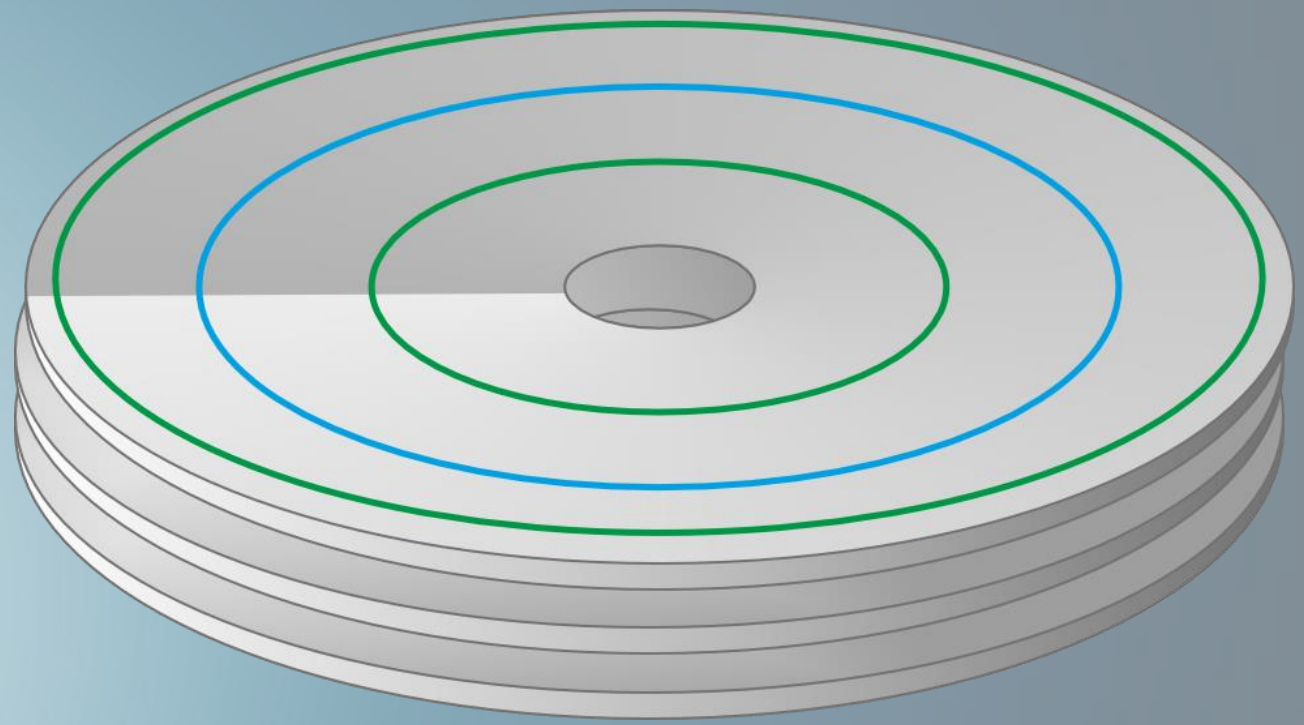
Servo flaw list



# HARD DRIVE PARTS AND FUNCTIONS

## Positioning system :

ID, OD AND S.A.



# HARD DRIVE PARTS AND FUNCTIONS

## Positioning system :

Understanding heads positioning system is important to make a first diagnosis of a disk based on head stack behavior and noises.

# HARD DRIVE PARTS AND FUNCTIONS

## HDD noises:

TOSHIBA LAPTOP DRIVE SPINDLE FAILURE

SEAGATE DESKTOP DRIVE SPINDLE FAILURE

SEAGATE LAPTOP DRIVE HEADS FAILURE (NOT ALL)

SEAGATE 7200.10 ALL HEADS FAILED

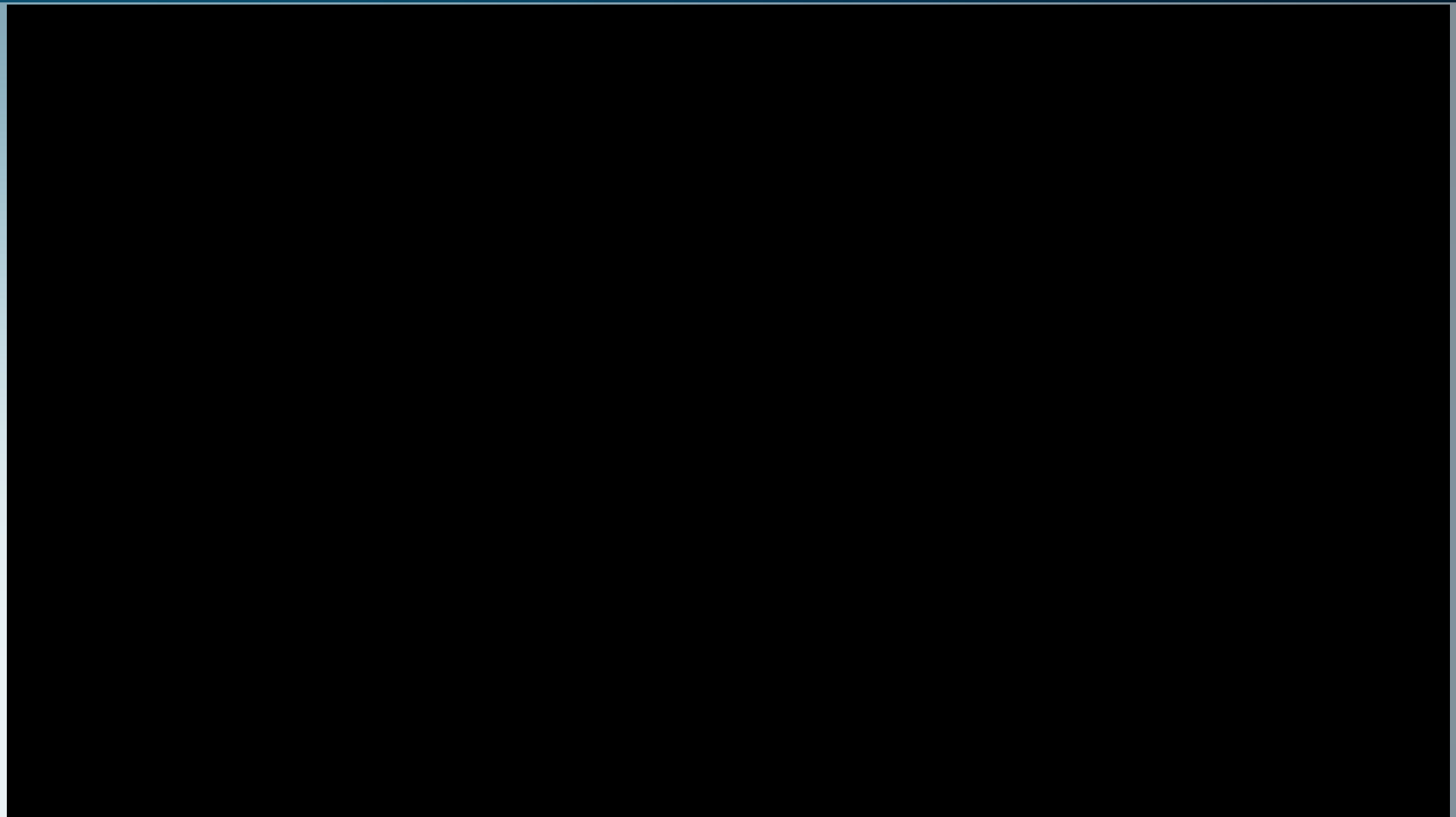
# HARD DRIVE PARTS AND FUNCTIONS

## POWER ON SEQUENCE:

PCB – MCU execute internal ROM boot loader and external or embedded ROM
PCB – Spindle motor controller start spin operations
HDA – Spindle motor spins up
PCB – Checks RPM to unlatch heads
HDA – head stack unlatch (vcm)
HDA – Heads calibrate position (servo info)
HDA – Heads move to firmware area and load full firmware
PCB – HDD ready state

***POWER ON VIDEO***

# HARD DRIVE PARTS AND FUNCTIONS



SUMURI

EDRTOOLS
for Digital Forensics & Data Recovery

# HARD DRIVE STORING DATA

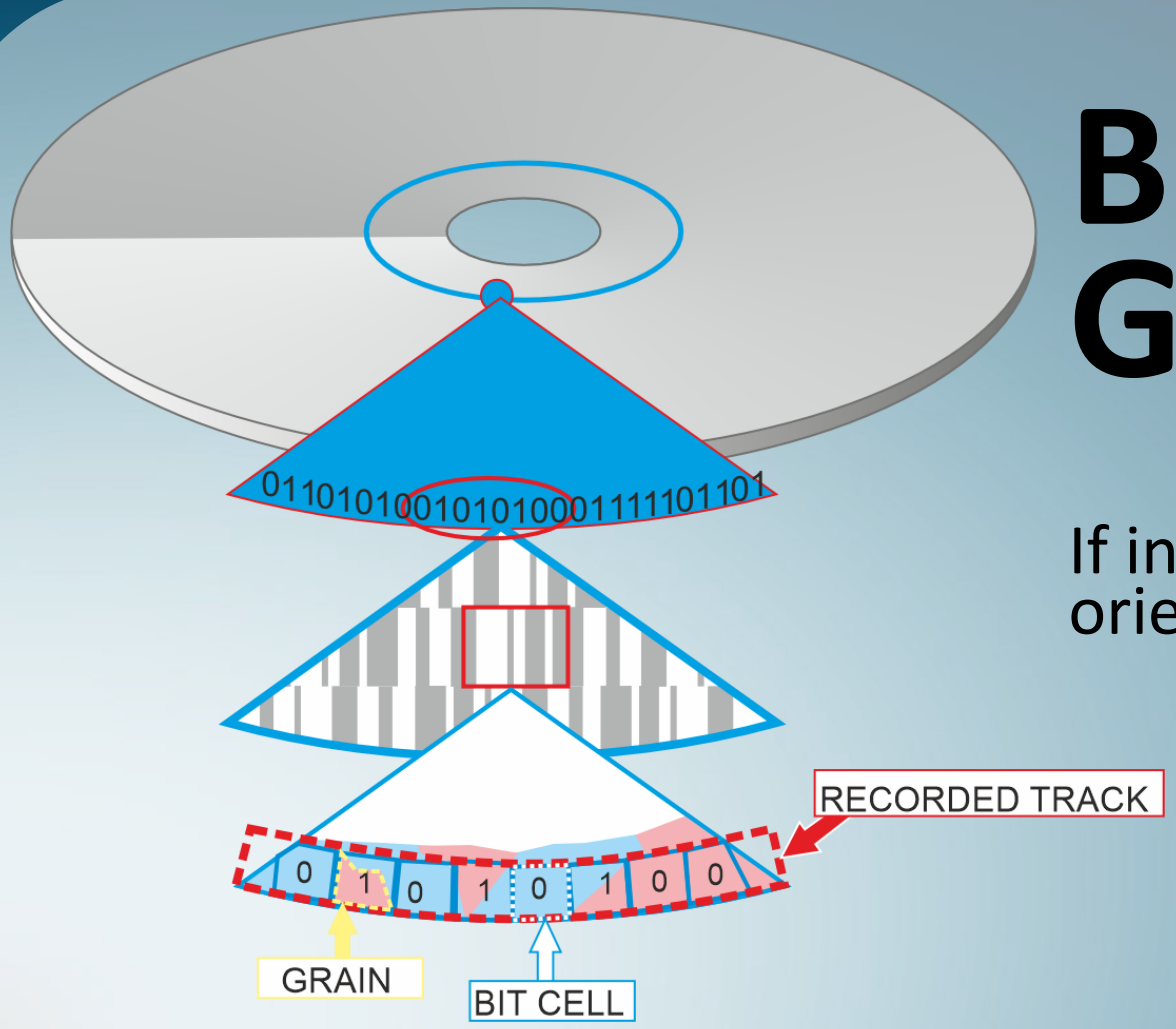
## MAGNETIC RECORDING PRICIPLE:

A drive writes data by passing electrical currents through an electromagnet (the drive head), generating a magnetic field that is stored on the medium.

A bit cell is the magnetic coating smallest part, in each one there are many tiny magnetic grains. These grains are randomly created during the deposition of the magnetic film.

If all grains in a bit cell are magnetized in the same polarity, it is said to be storing a binary ‘0’. On the other hand, a bit cell where a transition of magnetization takes place is considered as storing a binary ‘1’

# HARD DRIVE STORING DATA




## BIT CELLS AND GRAINS:

If in a bit cell all the grains have the same orientation is a 0 otherwise is a 1

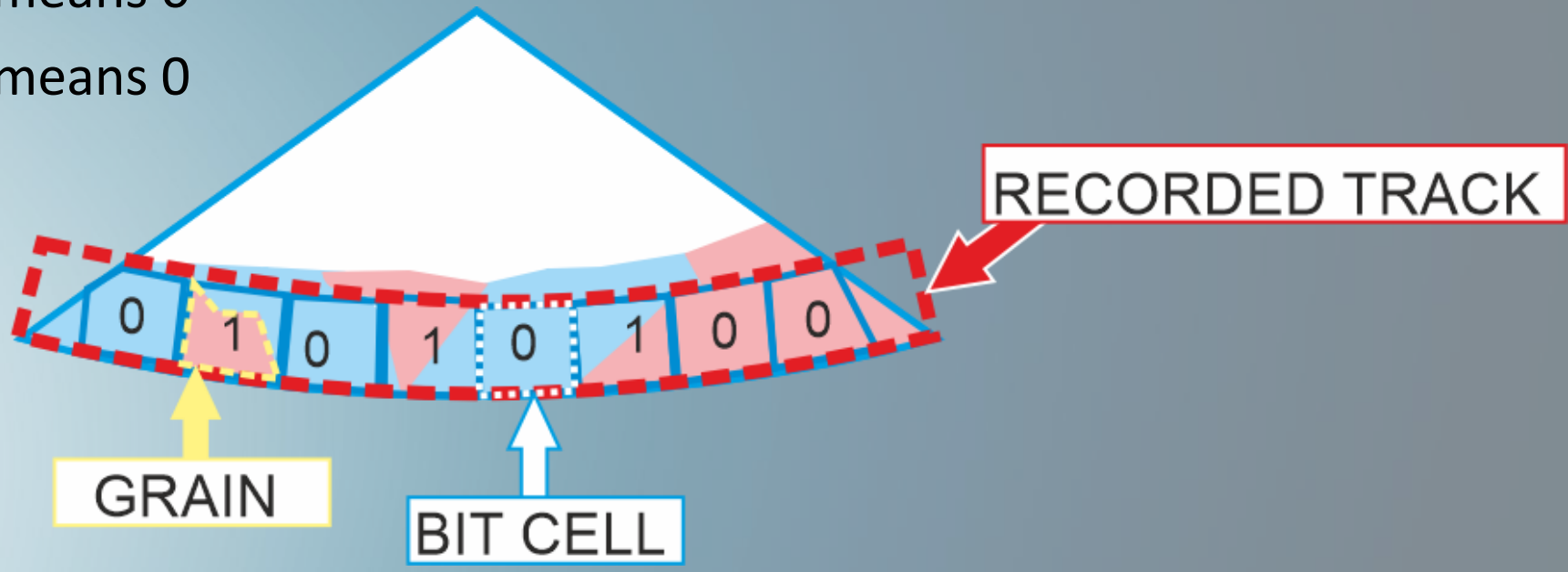
# HARD DRIVE STORING DATA

## BIT CELLS AND GRAINS:

To set a bit to value 0 we need to have all the grains in a bit cell having the same orientation (among them)

All the grains N→ S means 0

All the grains S→ N means 0



# HARD DRIVE STORING DATA

## DATA ERASURE BY OVERWRITING:

DoD data erasure

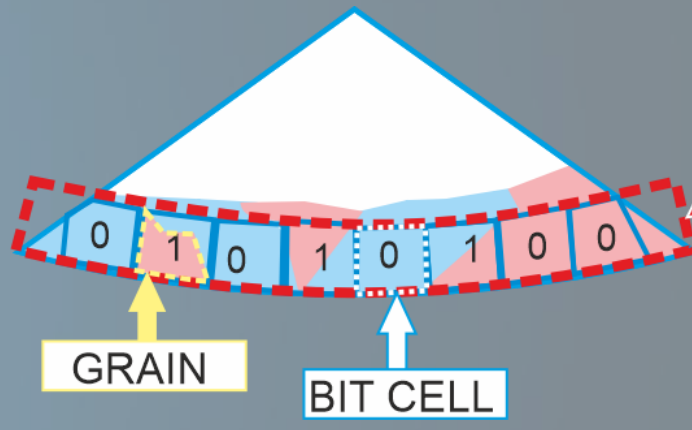
The Department of Defense 5220.22-M uses three overwrites, in 2001, the DoD 5220.22-M ECE method, a 7-pass version of the standard, was published. It runs DoD 5220.22-M twice, and an additional pass (DoD 5220.22-M (C) Standard) in between.

Nevertheless, the three-pass method is still its standard implementation. The DoD 5220.22-M data wipe method involves the following passes:

Pass 1: Writes a zero and verifies the write.

Pass 2: Writes a one and verifies the write.

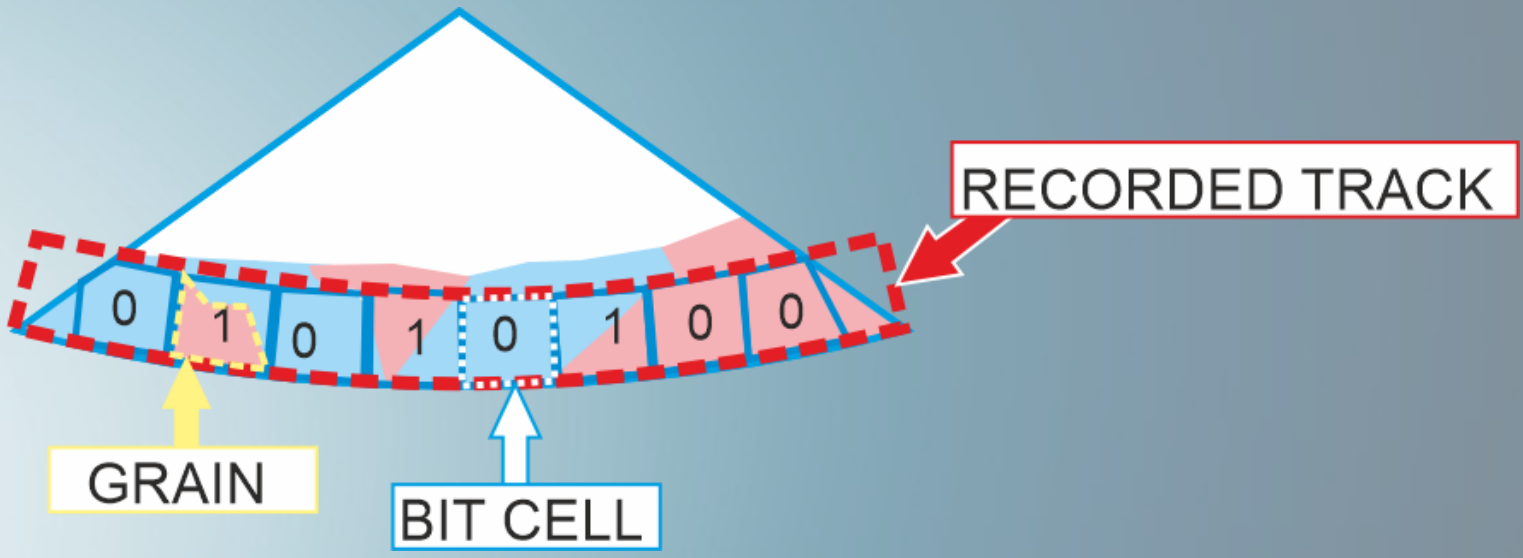
Pass 3: Writes a random character and verifies the write.



# HARD DRIVE STORING DATA

## DoD DATA ERASURE:

- Why 7 passes to erase with different patterns?
- Is it possible to recover overwritten Data?
- Difference between deleted files and wiped data/files



# THANK YOU FOR YOUR ATTENTION

SUMURI

EDRTOOLS
for Digital Forensics & Data Recovery

**Next lesson's topics:**

- ACTUAL AND NEAR FUTURE TECHNOLOGIES
- TRANSLATING PHYSICAL SECTORS TO LOGICAL SECTORS
- LBA ADDRESSING CREATION
- FACTORY TESTS AND SECTOR MAPS
- BAD SECTORS RELOCATIONS
- FIRMWARE AREA ON PLATTERS