[TEKNIK]

PROBLEMS OF THE DIGITAL AGE: DIGITAL FORENSICS AND DATA RECOVERY

Vinny Dunne

Data Recovery, Digital Forensics and Electronics lead technician.

Business owner.

Importance of DFIR and DR today

DFIR

- It is essential in the modern world, as criminals increasingly use technology to commit crimes.
- Its importance lies in the resolution of cybercrimes and the protection of sensitive data.

DATA RECOVERY

- It is essential in today's era, providing the crucial ability to restore lost information, ensuring operational continuity, and mitigating the consequences of events such as technical failures, accidental loss, or cyber attacks.
- Additionally, it is also applied in the investigation of security incidents, the recovery of lost data, and the protection of the integrity of digital information.

1

DFIR

DIGITAL FORENSICS AND INCIDENT RESPONSE

"Multidisciplinary field that employs techniques from computer science, law, and investigative procedures to collect, analyze, and preserve electronic evidence in order to solve and prevent cybercrimes

Objectives and scope

- Its main objectives include the collection of digital evidence, determination of responsibilities, and prevention of future incidents.
- Its scope covers areas such as cybercrime, computer security, and data recovery.

"

El tiempo pone cambios. Estamos entrando en la época digital. Ni peor ni mejor: distinta

- José Mugica, Ex-presidente de Uruguay

- Analysis of malware on smartphones and mobile phones (Anti-Malware Services).
- Investigation of routes and data storage in Remotely Piloted Aircraft (Drones).
- Identity theft or impersonation.
- Unfair competition investigation.
- Computer sabotage.
- Crimes against intellectual or industrial property.
- Discovery and disclosure of secrets, industrial espionage, etc.
- Investigation and analysis of computers involved in legal disputes or trials under chain of custody.
- Violation of confidentiality or company policies.
- Breach of privacy rights and communication rights in the workplace.
- Investigation of inappropriate computer use during working hours.
- Chat, file, and web browsing history, or any other form of electronic communications.
- Unauthorized access to computer systems.
- Investigation of data deletion, theft of computer data, and information leakage.
- Recovery of data stored on any device or in the cloud.
- Origin of email and instant messaging messages.
- Logs and traces of communications via email and instant messaging.
- Detection of hidden microphones and cameras (Electronic sweep services)

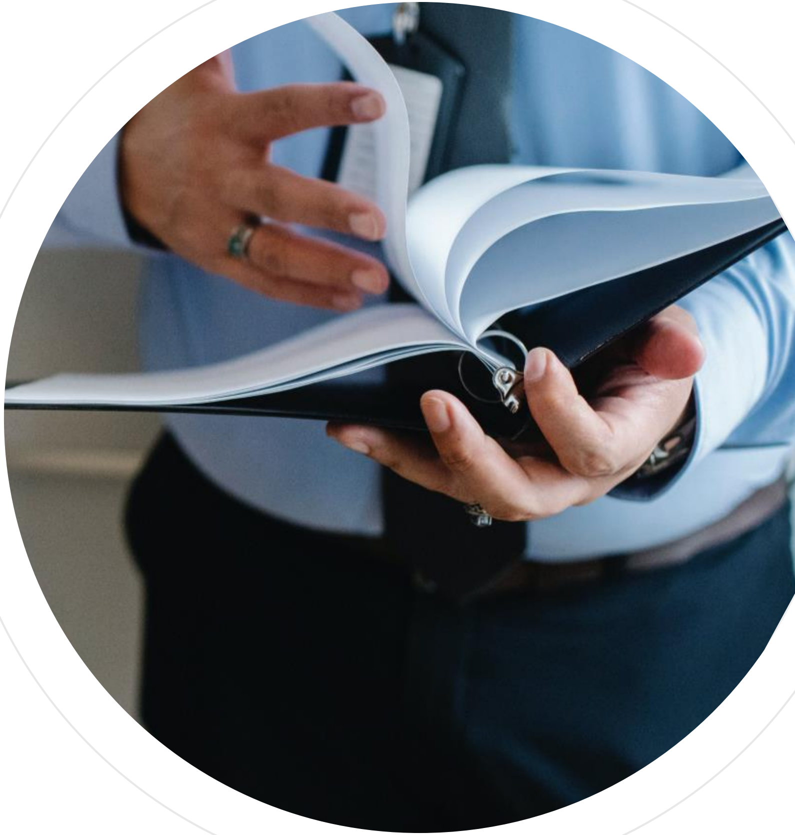
Scenarios

Forensic investigation process

1. CASE STUDY
2. EVIDENCE ADQUISITION
3. ADQUISITION ANALYSIS
4. REPORT

1. Case study

- Main Pillar
- Understanding of the Legal Context
- Interviews with Affected Parties
- Identification of Potential Evidence
- Risk Assessment

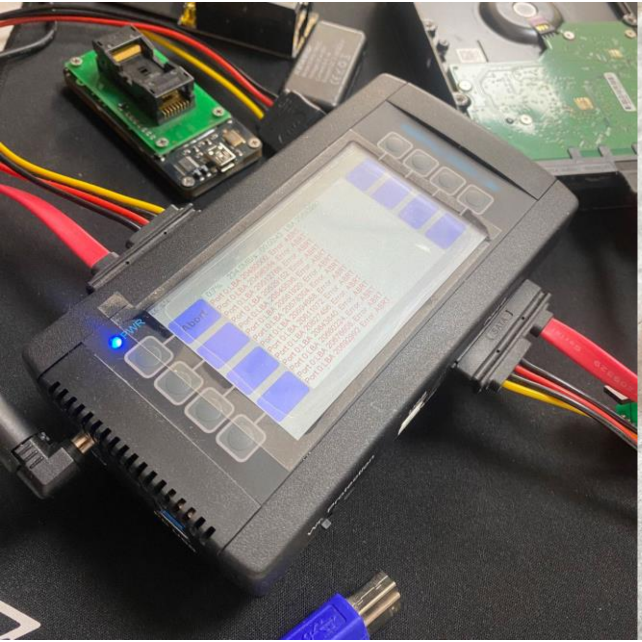


2. Adquisition

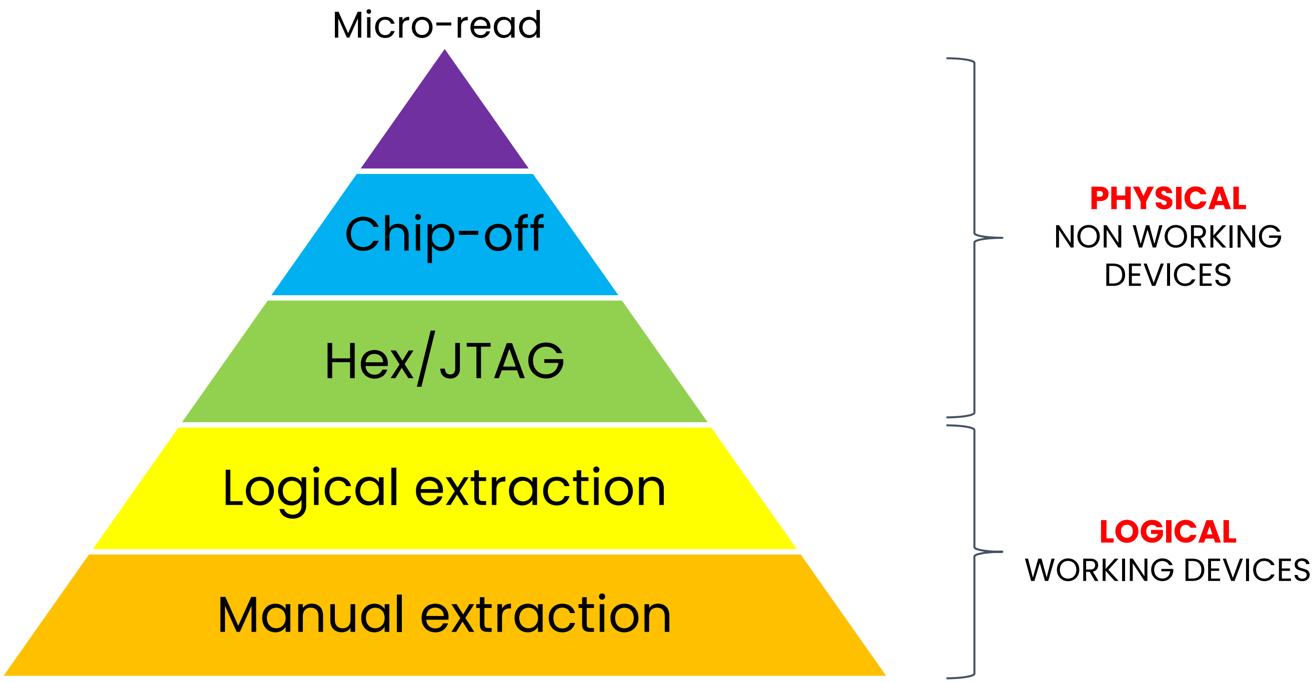
- Collecting evidence
- Copies
- Mobiles: physical/logical
- Chain of custody → **HASH**
- Must be reproducible

POLICíA MUNICIPAL
UDALTZAINGOA
PAMPLONA · IRUÑA

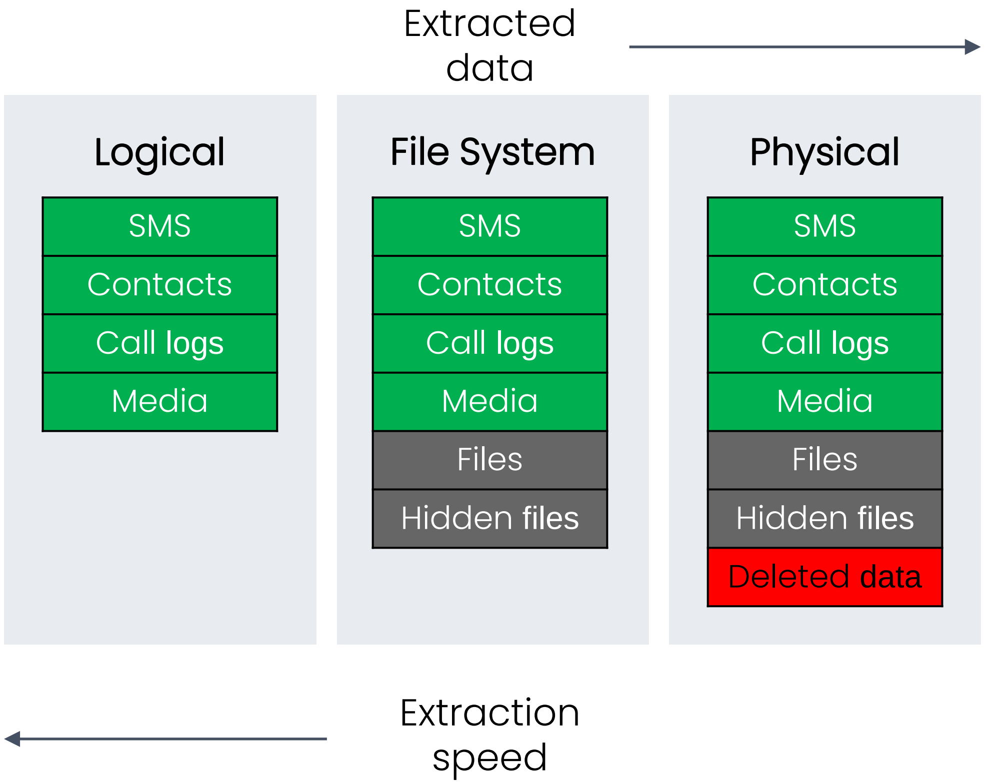
Forensic Workstation



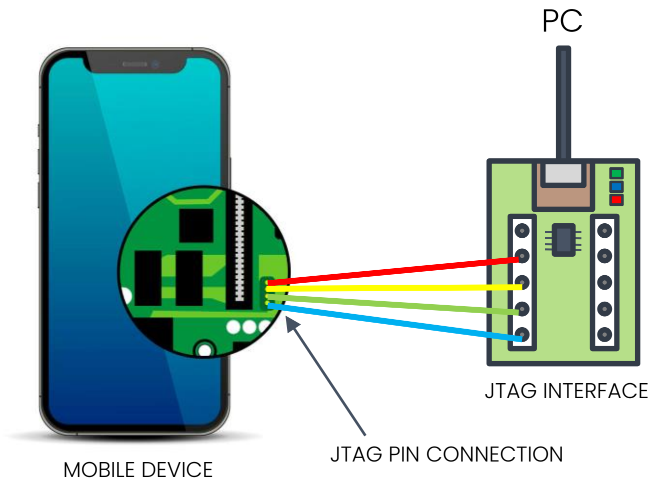
Portable solutions



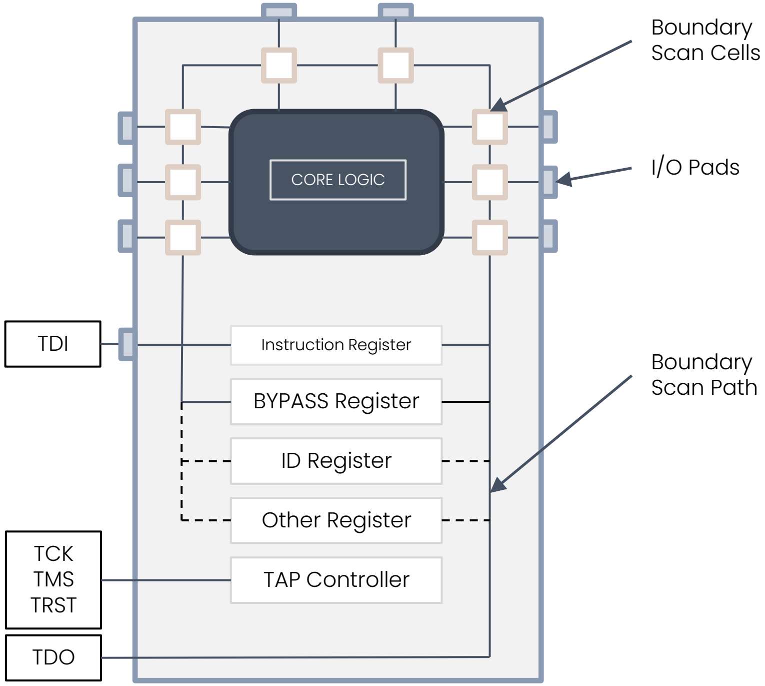
Extraction (mobile devices)



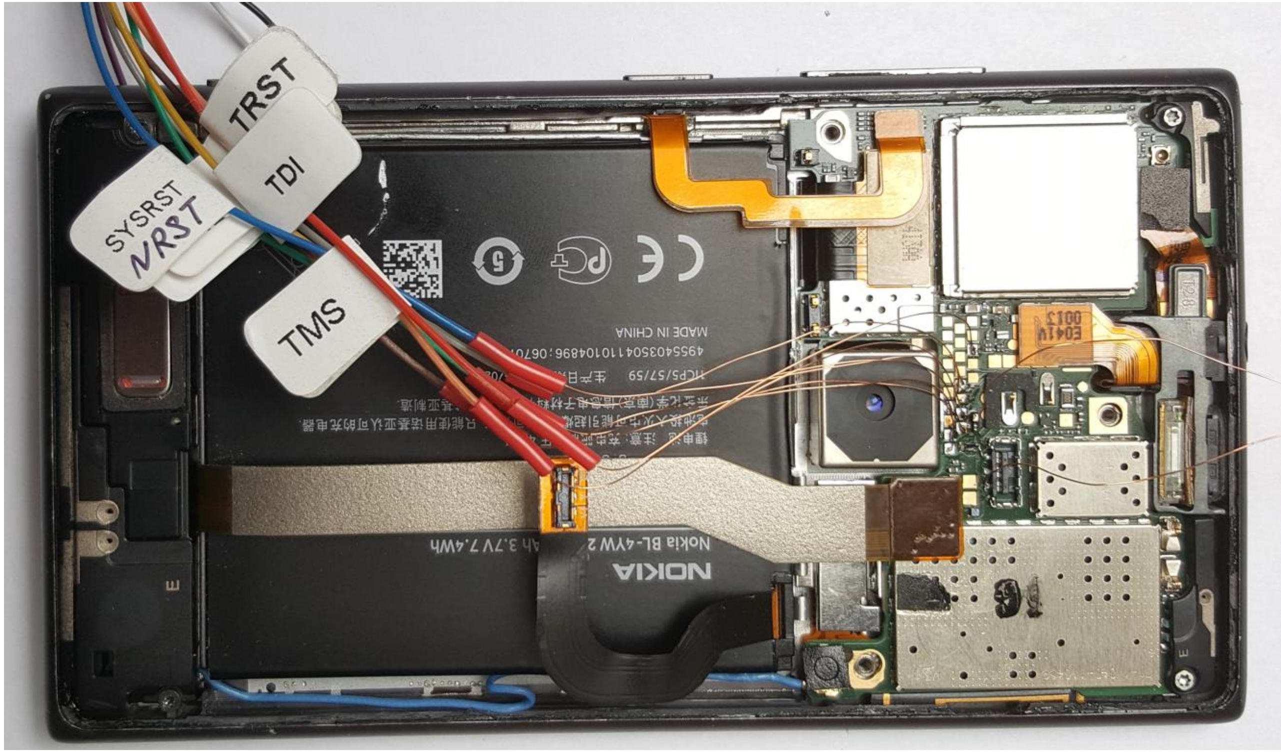
Extraction (mobile devices)



Required pins	Optional:
• TDI	• TRST
• TDO	• RTCK
• TCK	• GND
• TMS	• VCC



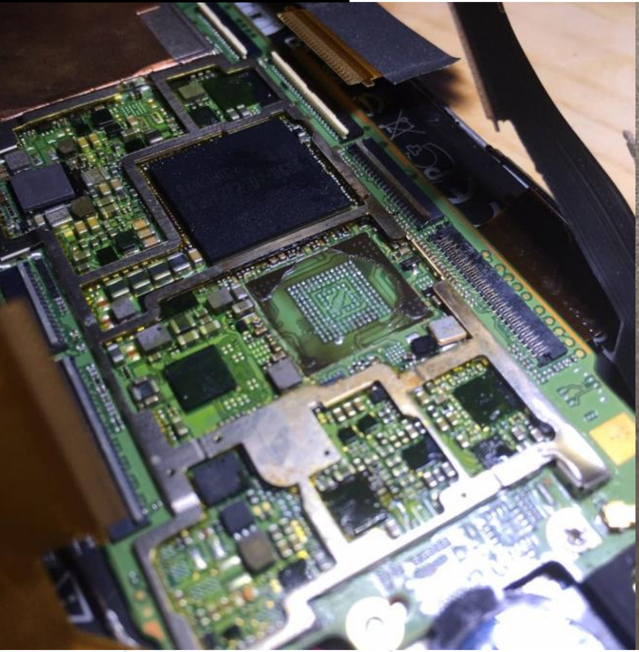
JTAG

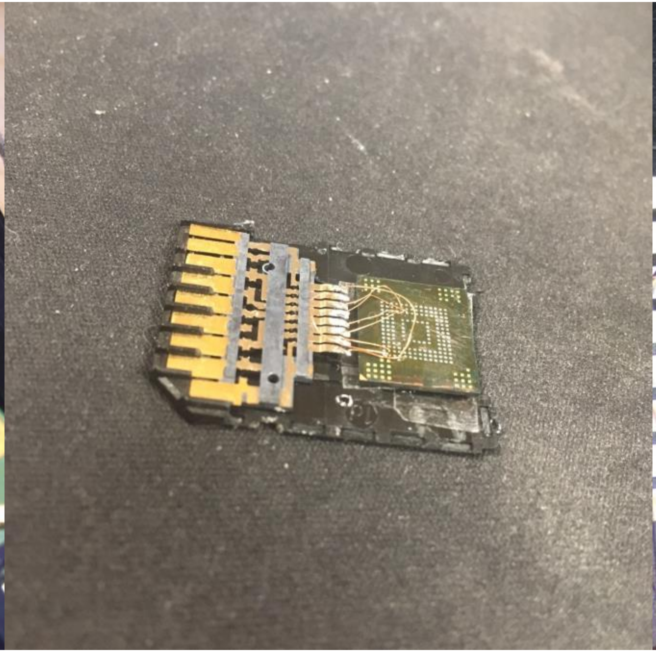


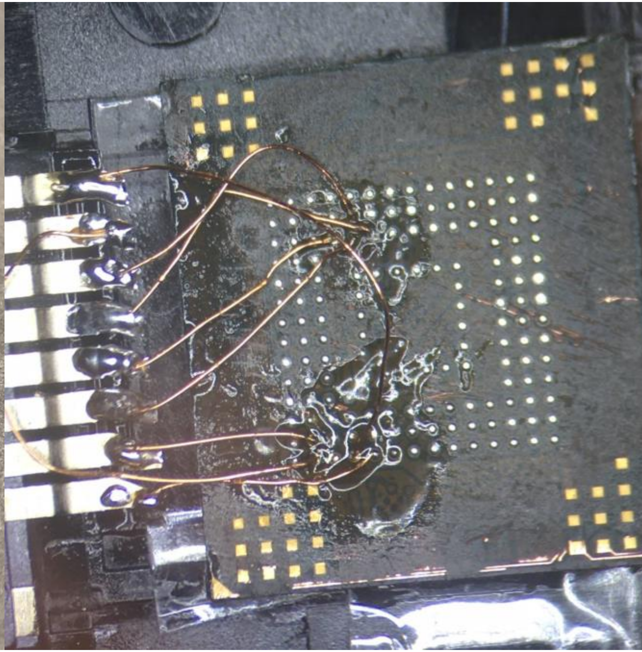
Source: packt

JTAG

HTC M8 (eMMC)

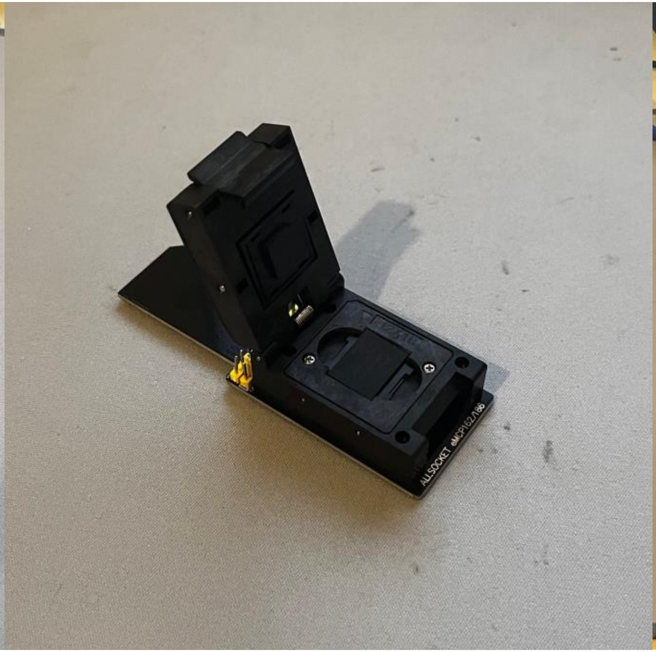






Chip-off #01

Unbranded phone (eMCP)



Chip-off #02

It is the result of a cryptographic function through a mathematical algorithm that transforms any arbitrary block of data into a series of characters with a fixed length.

Regardless of the length of the input data, the output hash value will always have the same length

$$H : U \to M$$
$$x \to h(x)$$

HASH

HEX DUMP

00000000	54 45 4B 4E 49 4B	TEKNIK

MD5: 0ED4D6C6175378B65CE2E87B7220CBF3

SHA-1: CF9EDA0B9DE7B82E7B7C13F8ADE2DC91912D4CBD

SHA-256:

EE1A30EDB70A4FEF77213C31CDC604D326356FBE676C54F60C6263CFC7DEE5EE

HASH

3. Analysis

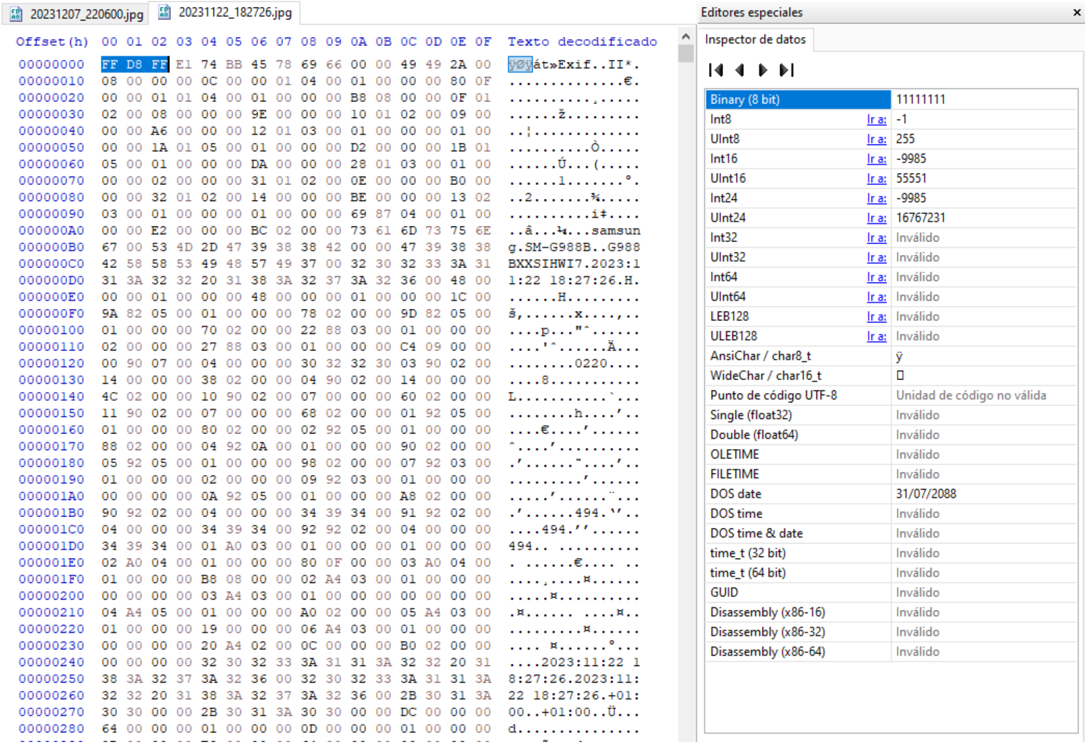
- Examine collected data
- Identify patterns
- Recover hidden information
- Data carving
- Reconstruction of events
- Establish timeline

- Almost all files have start and end identifiers or file signatures (headers/footers)
- Some have headers and no footers, or footer is not important for recovery
- Some of them have none at all, which can be an identifier (emails or TXT files)

JPG	FF D8 …	FF D9
PDF	25 50 44 46 …	25 25 45 4F 46
GIF	47 49 46 38 …	00 3B
DOC	D0 CF 11 E0 A1 B1 1A E1…	File struc. Based.

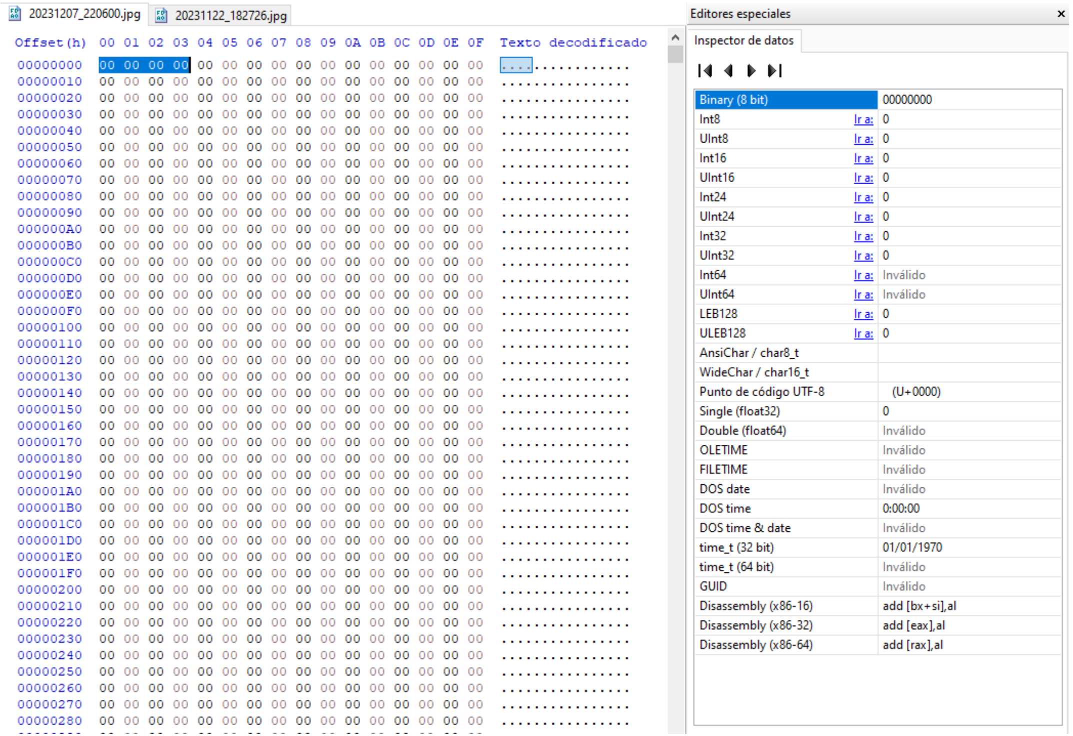
DATA CARVING

Healthy image



DATA CARVING

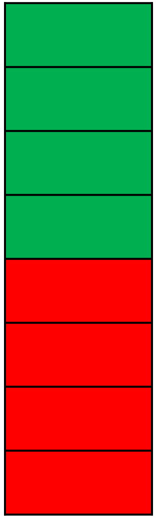
Empty image



DATA CARVING

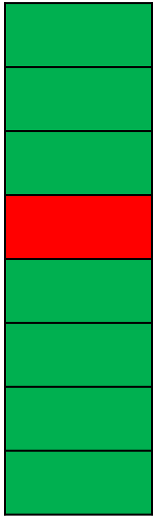
Hex table

Healthy image



Hex table

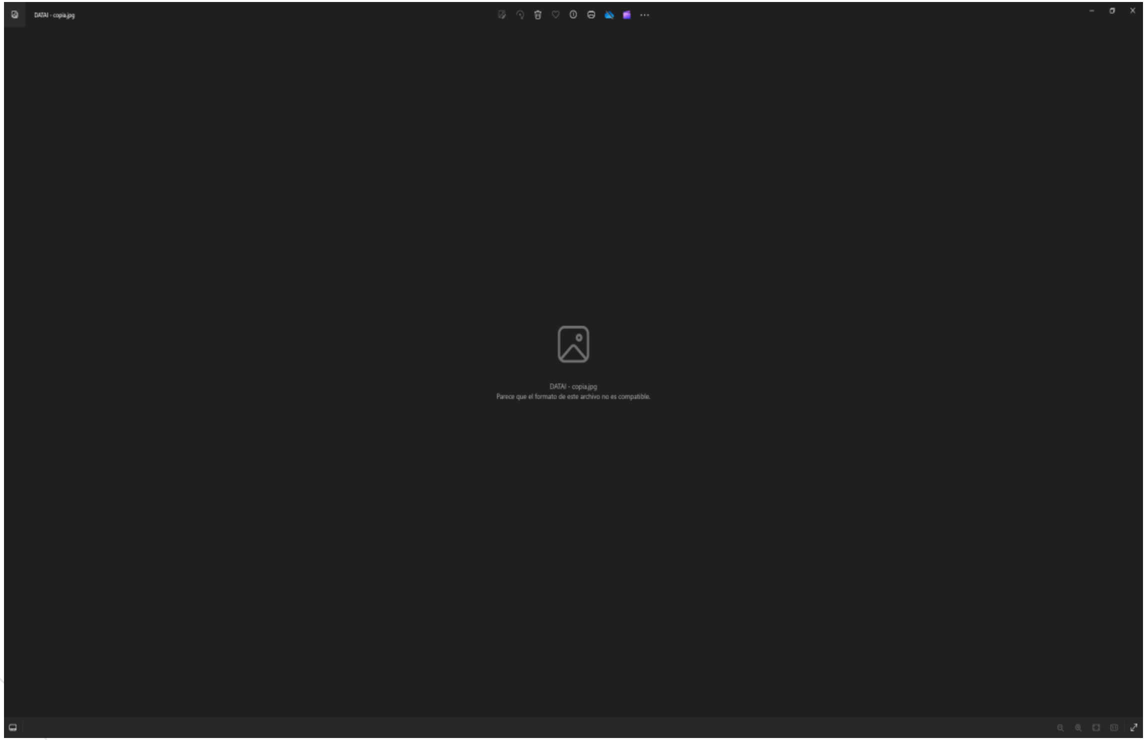
Barely damaged



Hex table

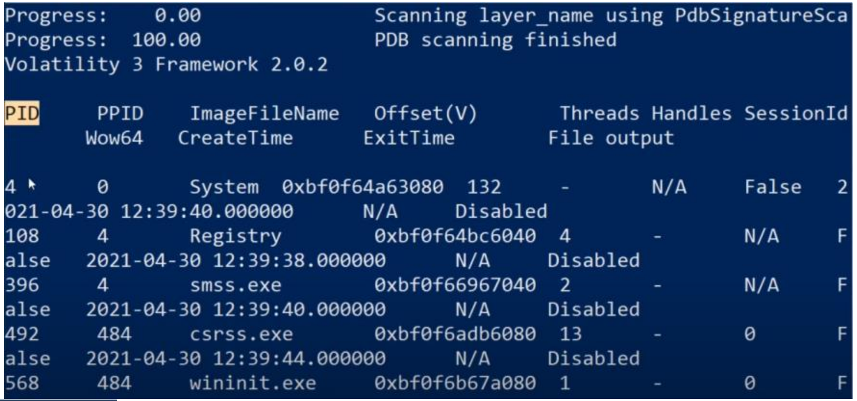
Badly damaged

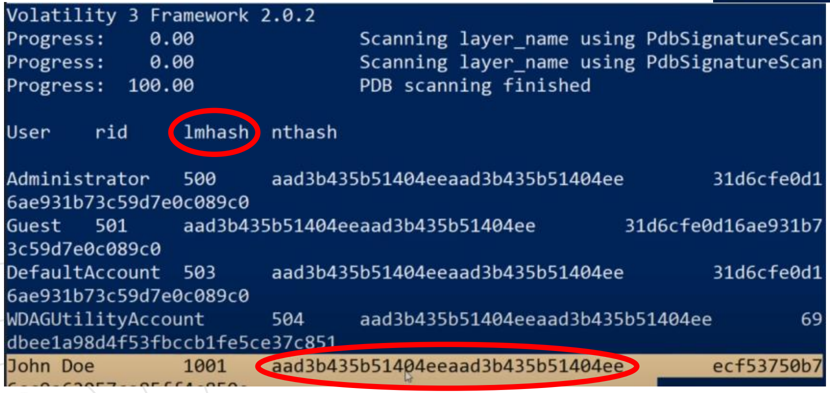
Hex table



Corrupt

Process list



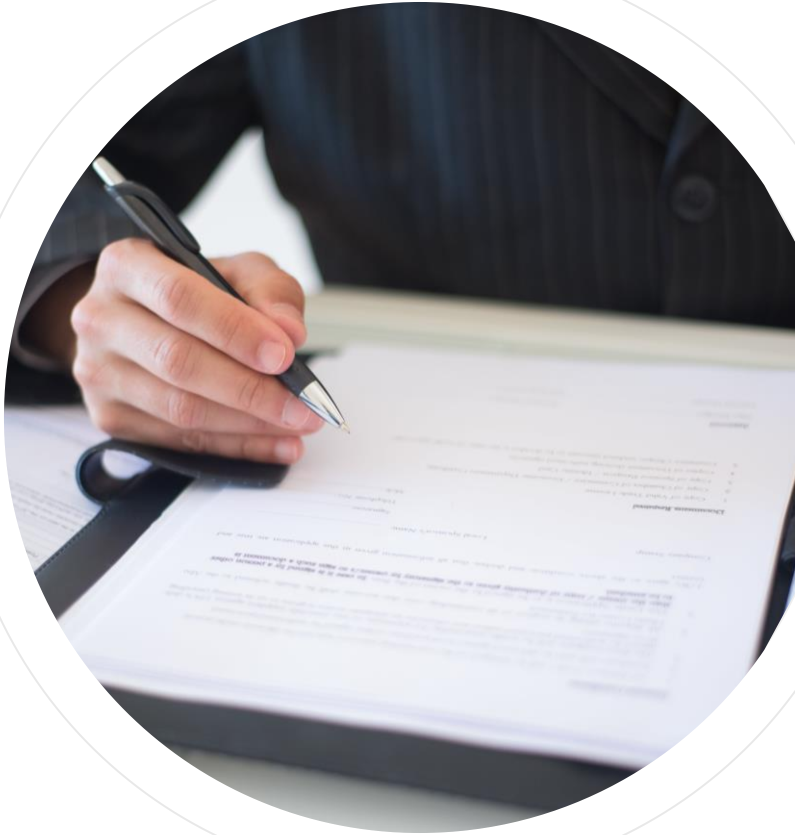


User passwords

DATA CARVING (RAM)

4. Report

- UNE 197010/2015
- Objectives/scope
- Methodology
- Additional documentation
- Conclussions
- Clear, precise, and supported by solid evidence



1

DIANA QUER

- Went missing 22nd August 2016
- Body retrieval 31st December 2017

iPhone 6
iOS 9

Chrono: Diana Quer

2016 | AUG | SEP | OCT | NOV | 2017 | APR | JUL | AUG | DEC | 2018 | JAN

22 AUG: Goes missing
23 AUG: Search

6 SEP
Phone positioning

27 OCT
Phone discovery

Mid NOV: vehicles identification
30 NOV statement

19 APR Dismissal

5 JUL
Phone unlock

22 AUG
Reconstruction

29 DEC
Attempted kidnapping

30 DEC
Confession

31 DEC
Body retrieval

11 JAN
Autopsy

2

MARTA DEL CASTILLO

- Went missing 24th January 2009
- Her body has not been found yet

LAZARUS

Motorola U9
Linux / Java

3

"LA MANADA"

- Events: 7th July 2016

LG G3S

iPhone 5

Vodafone Smart First 6

LG L9 II

Google Nexus 5

2

Data Recovery

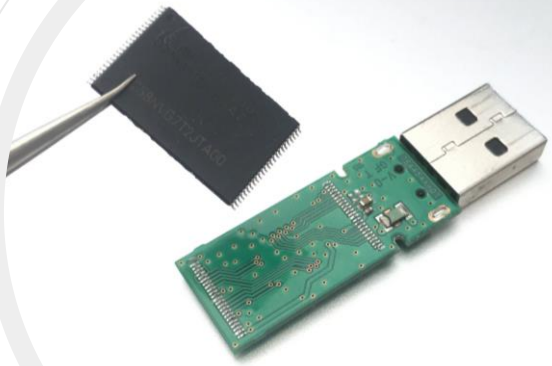
" **Set of procedures used to access information stored on a digital medium that, for various reasons, is not accessible conventionally**

Scenarios

- Accidental deletion
- Data corruption
- Disk formatting
- System failure
- Attacks, malware, virus/ransomware
- Physical damage to the device

Storage media

- Tapes
- HDD/SSD disks
- RAID/NAS/Servers systems
- USB drives
- Memory cards
- Mobile devices



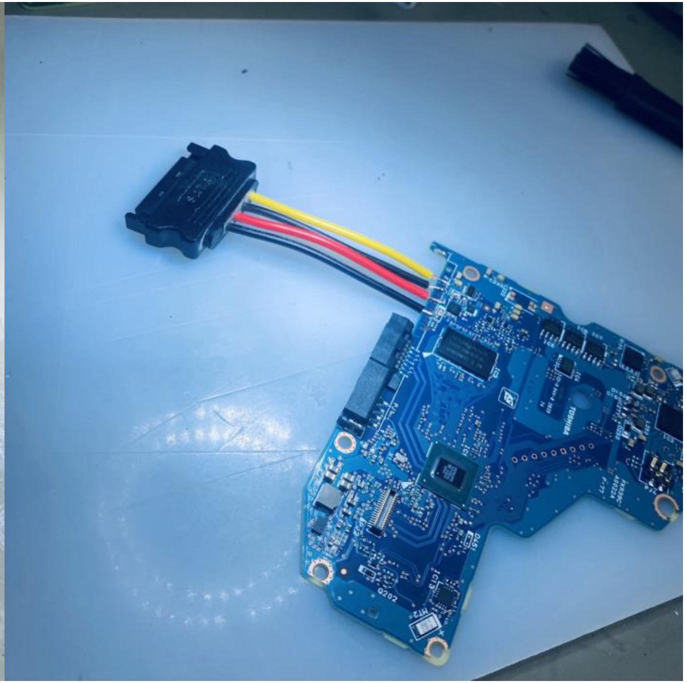
Common cases

- Basic logical
- Advanced logical
- Electronic fault
- Media or firmware issues
- Physical

Problems

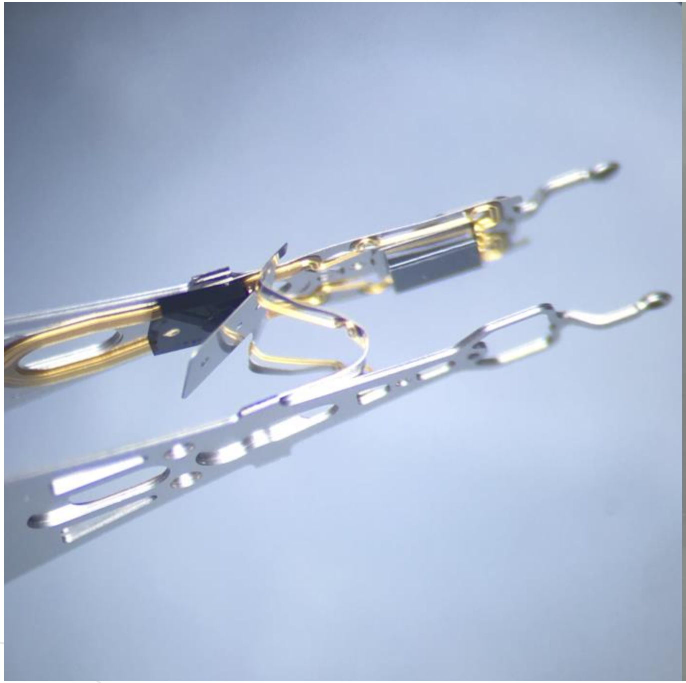
- + Density/+ Heads
- Helium drives
- Scarcity of old drives
- Searching for donors
- Time consuming

HDD

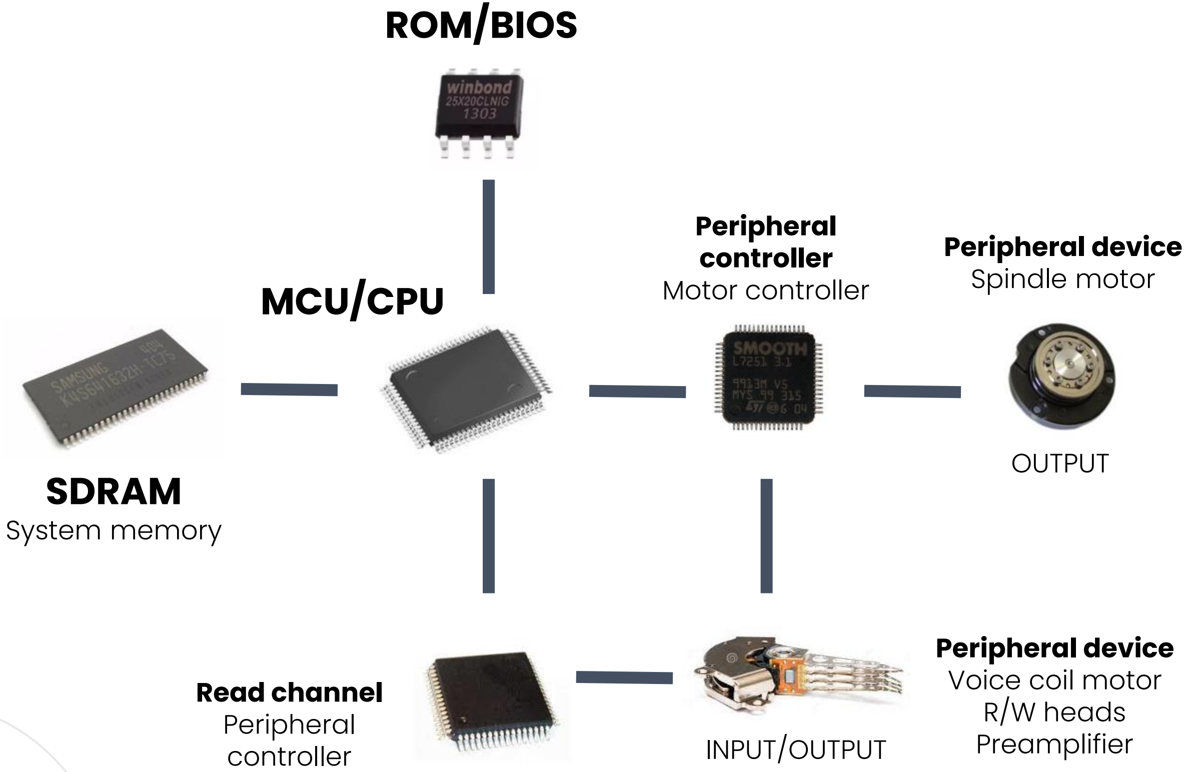


HDD (helium drive)

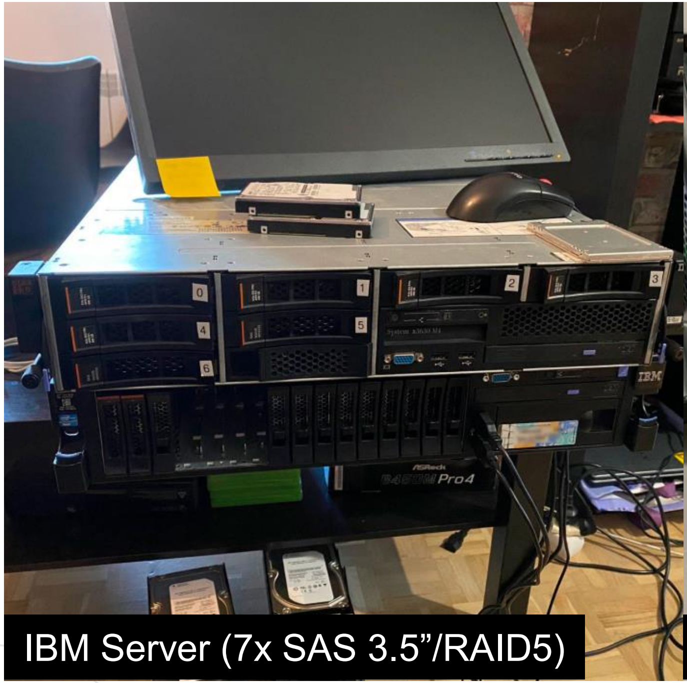
HDD (head swap)



HDD (head assy/PCB)


ROM/BIOS
MCU/CPU
SDRAM
System memory
Peripheral controller
Motor controller
Peripheral device
Spindle motor
OUTPUT
Read channel
Peripheral controller
INPUT/OUTPUT
Peripheral device
Voice coil motor
R/W heads
Preamplifier

HDD (PCB)



IBM Server (7x SAS 3.5”/RAID5)

4x SATA 3.5”/RAID5

RAID

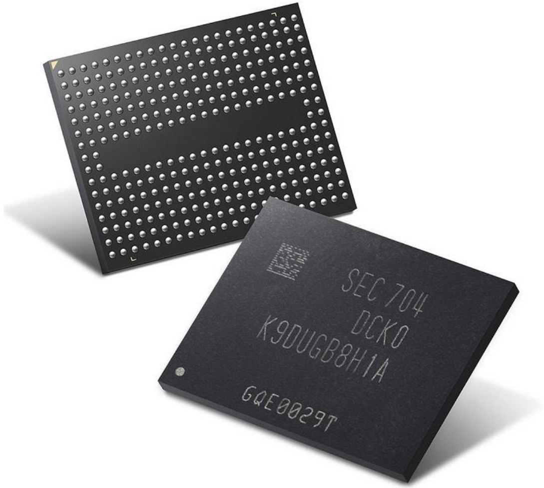
Common cases

- Mild media issues
- Electronic, controller and/or memory degradation
- Physical

Problems

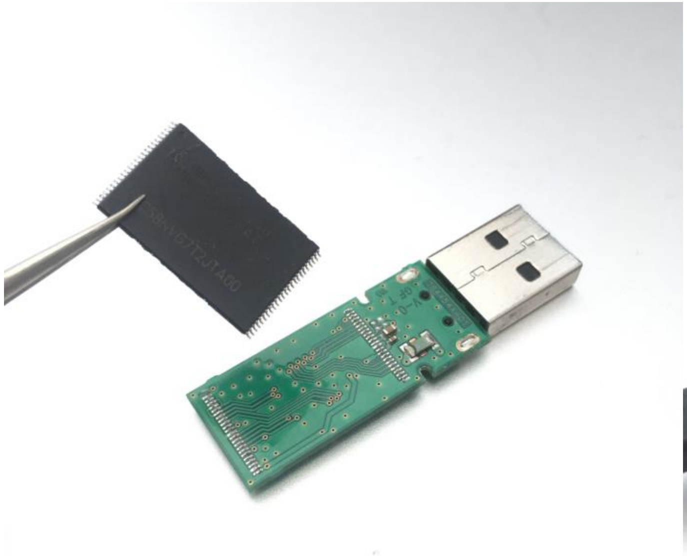
- No support
- Encrypted drives (SED)
- Scarcity of old drives
- Searching for donors

SSD



Chip-off method

Flash devices



USB flash drive

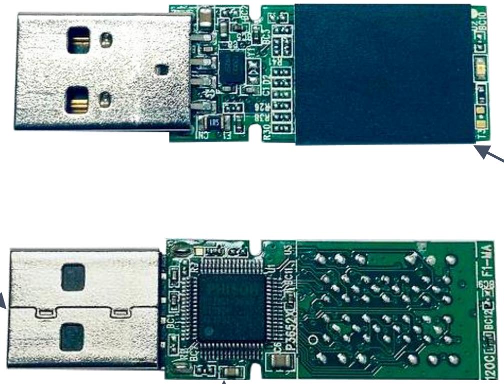
"

1. Flash device structure
2. Types of chips
3. How data is stored
4. Bit errors
5. Encryption in flash drives
6. How this is usefull in DFIR
7. Steps during recovery

- → USB
- → SD/CF/MS
- → SSD*

- → Main firmware
- → Service structures
- → Mixed user data

1. Flash device structure



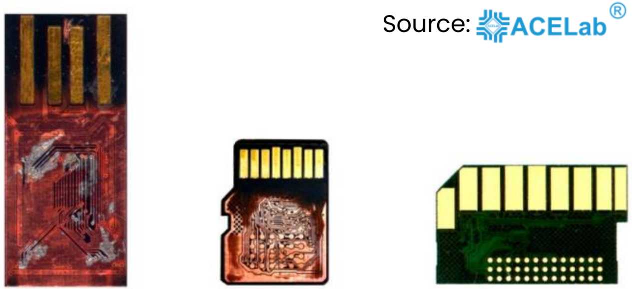
NAND:
TC58NVG5D2ELA48
BGA52 4GB X8 MLC
24 bit ECC for each
1024 bytes is required

Interface: USB

Controller: PS2251-33

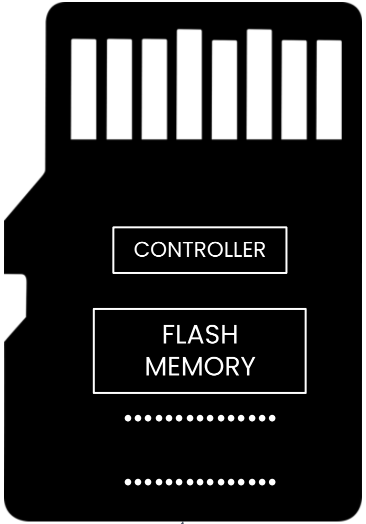
SMT: surface mount technology

Source: ACELab®



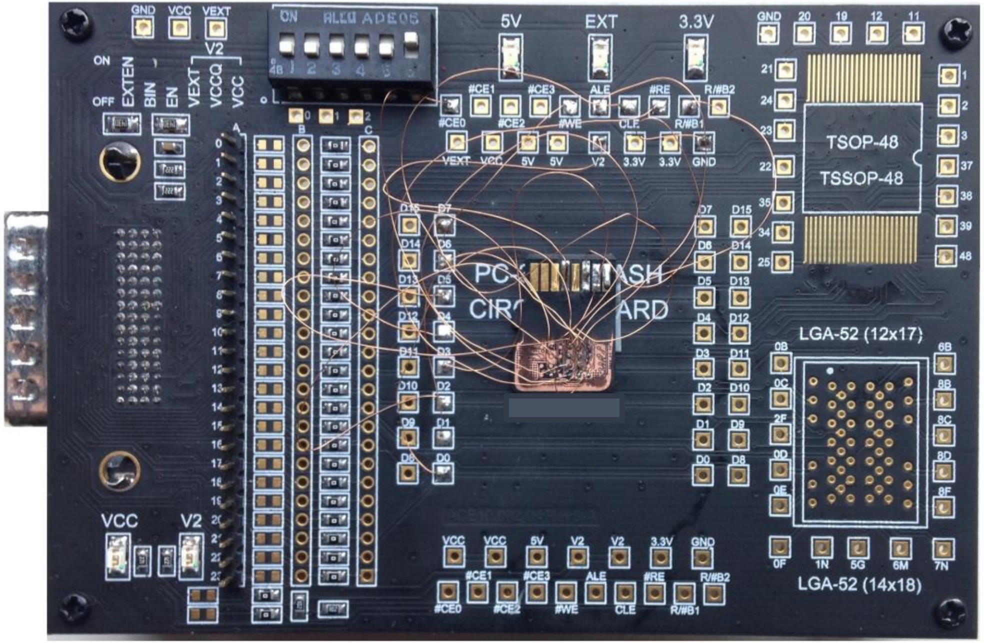
USB microSD SD

- Unified structure of the NAND flash device
- All components integrated into a single chip



Technological pins

Monolith



Data recovery: NAND protocol

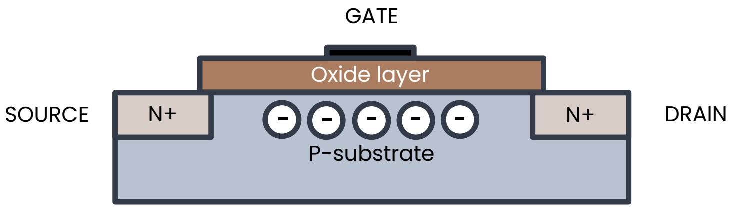
SLC: Single Level Cell
MLC: Multi Level Cell
TLC: Triple Level Cell
QLC: Quad Level Cell

QUALITY

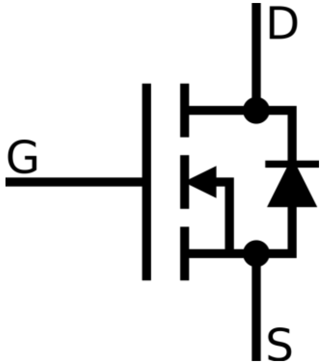
SLC	0	1														
MLC	00	01	10	11												
TLC	000	001	010	011	100	101	110	111								
QLC	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

PRICE

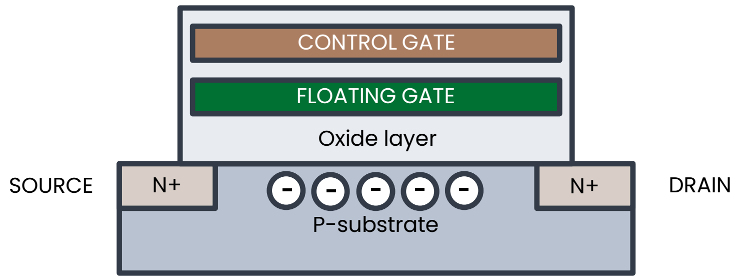
2. Types of chips

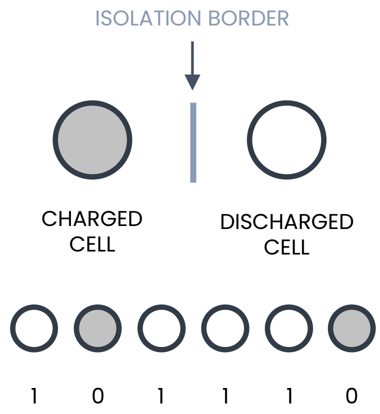


ON	1
OFF	0



3. How data is stored: the N-mosfet

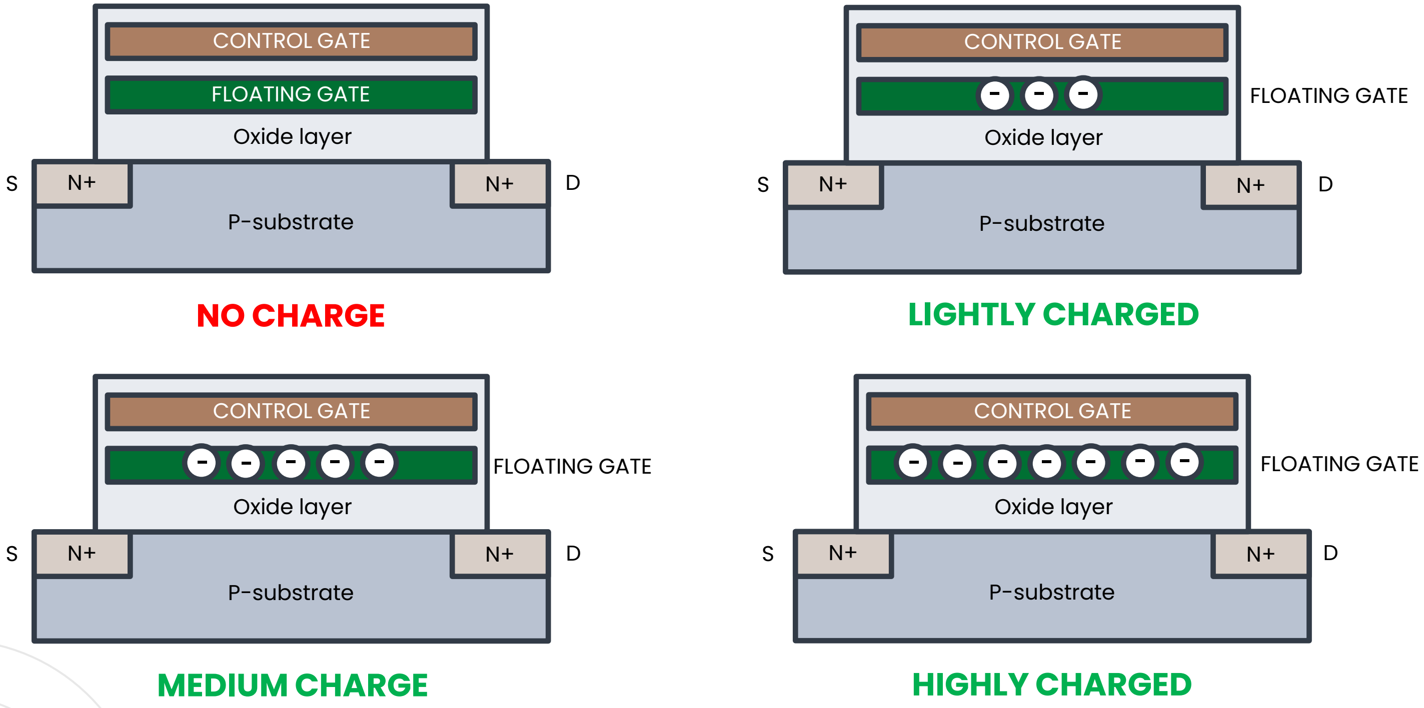




↓ V for Reading
↑ V for Erasing/Writing

- Degradation of isolation border
- Charge leakage

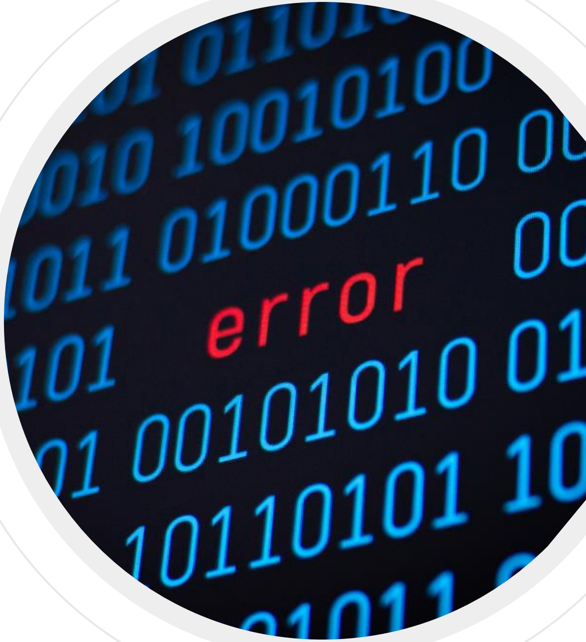
3. How data is stored (SLC)

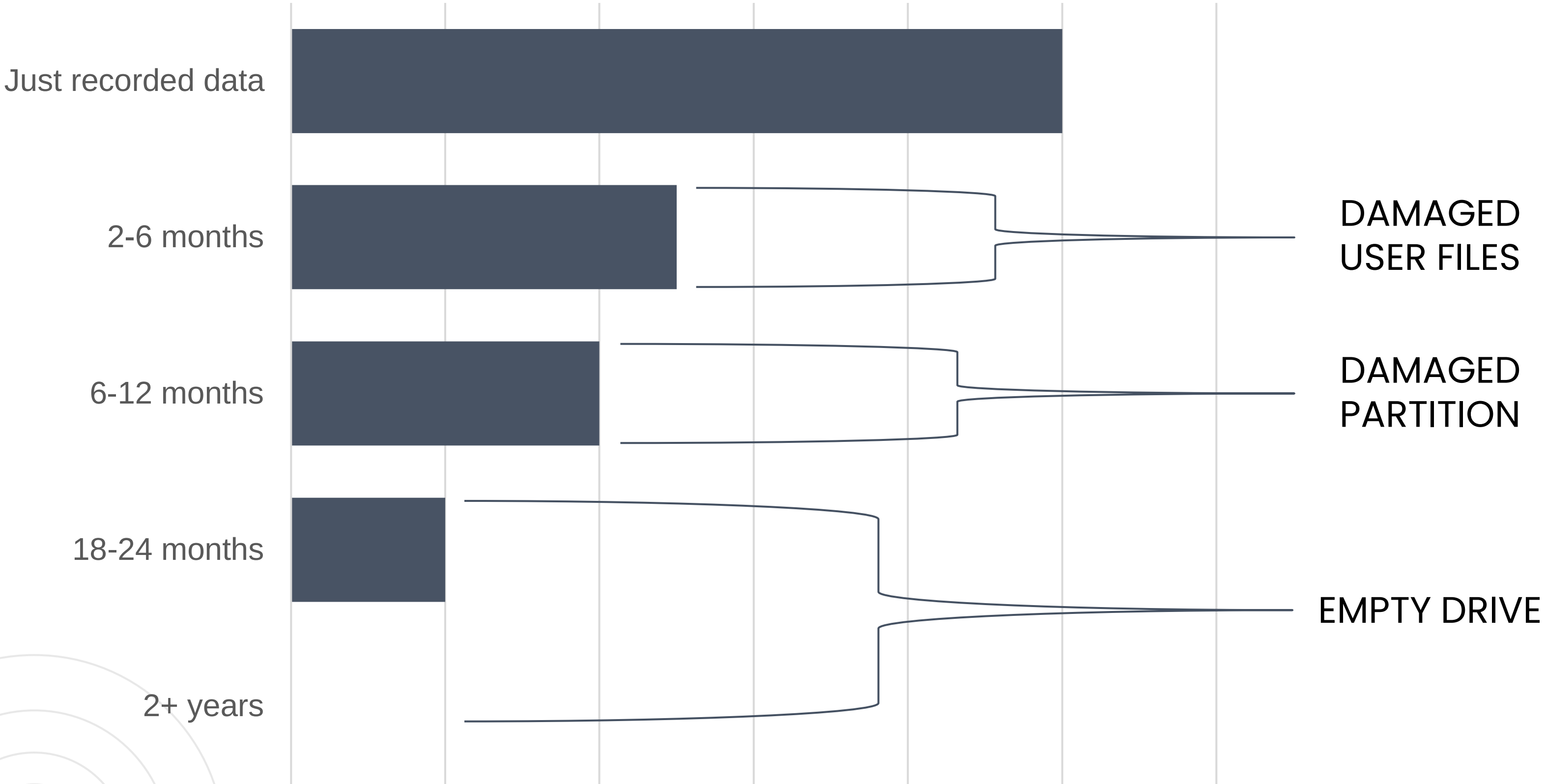


3. How data is stored (MLC)

4. Bit Errors in memory chips

- Bad quality NAND
- Charge leakage
- Damaged Temp/Volt table
- Compression of data
- Small process node
- Wear leveling/Block erase





Charge leakage

DEFAULT VALUES

Temp	VCC
-20°C	3V
20°C	3.3V
80°C	3.6V

NORMAL READING

POSSIBLE SHIFT

Temp	VCC
-20°C	3.3V
20°C	3.6V
80°C	3.9V

READING WITH ERRORS

Temperature/Voltage table

Reading errors

Freeze spray

Hot air

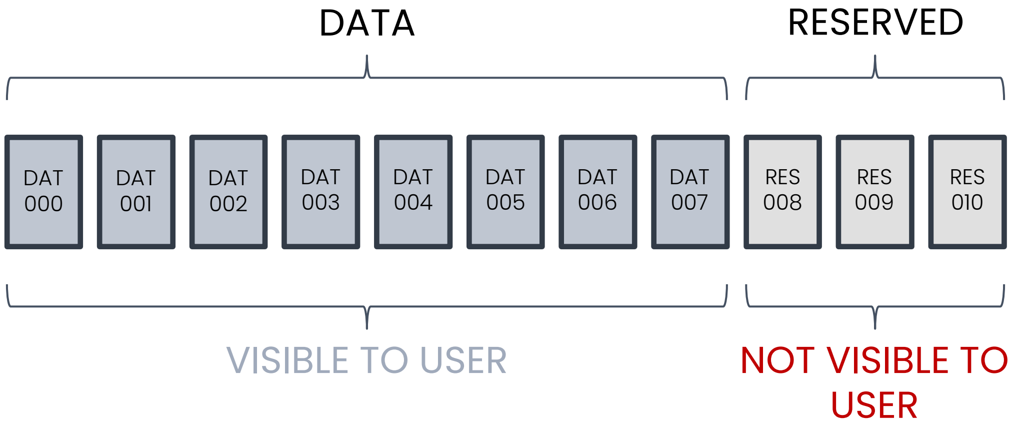
Used for error reading

5. Encryption in flash drives

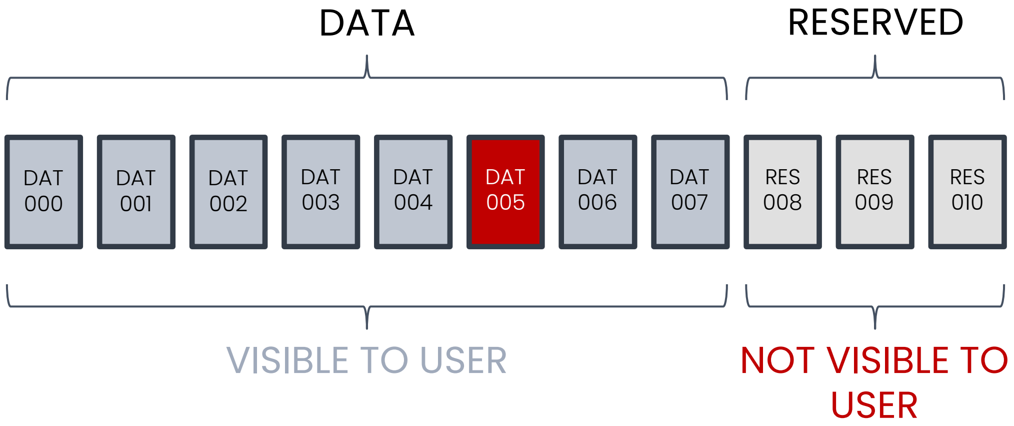
- Hardware encryption by Flash controller
- Software encryption on partition (Bitlocker/Filevault/other)
- XOR

6. How is this useful in DF

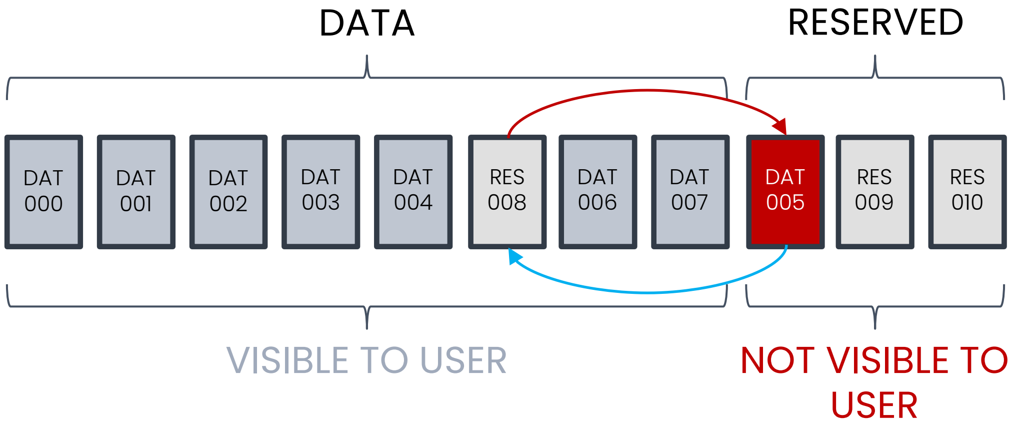
- We have access to **unadressed space** in the memory chip
- Deleted files or formatted drives can be recoverable



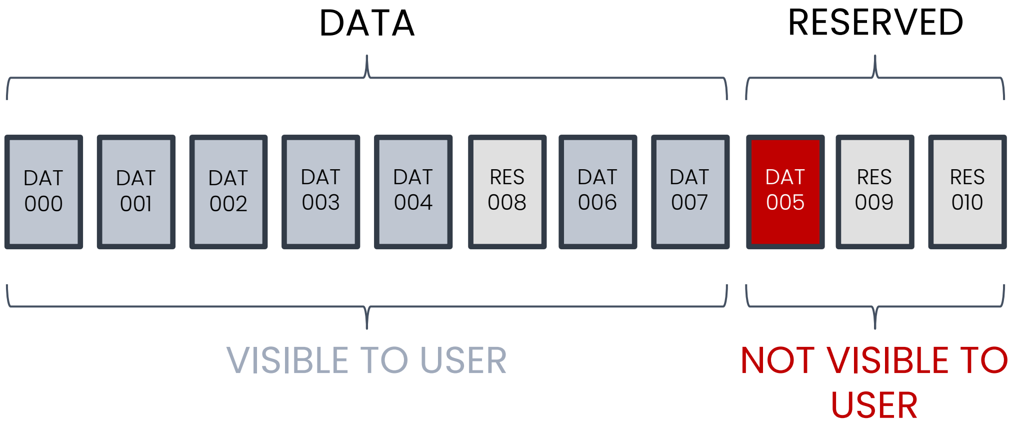
NAND based drive



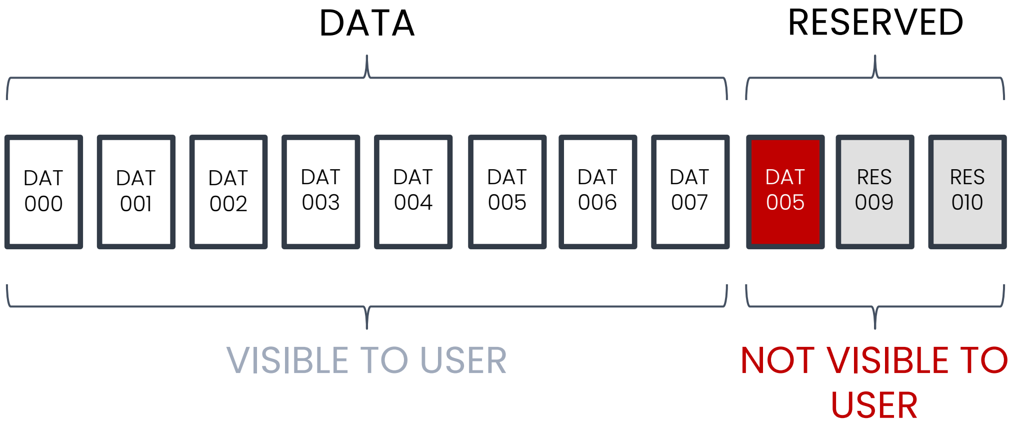
NAND based drive



NAND based drive



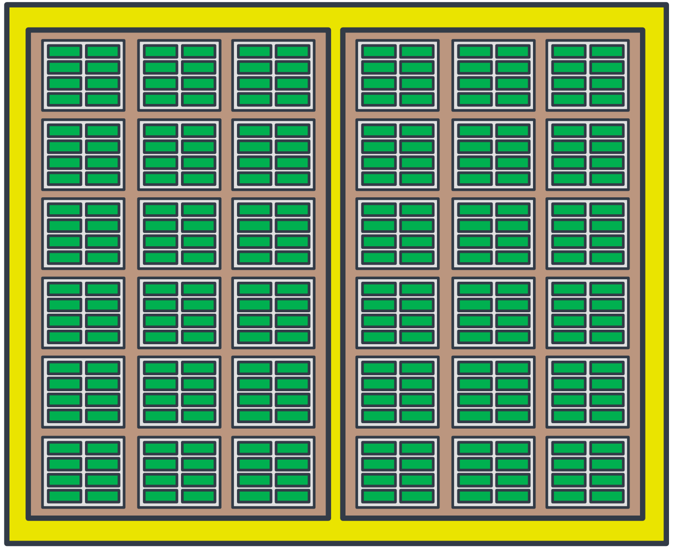
NAND based drive



NAND based drive

Chip-off recovery

1. DESOLDER CHIP(S)
2. IMAGE READING (DUMP)
3. FIX ECC/XOR/BAD COLUMNS
4. RE-READ

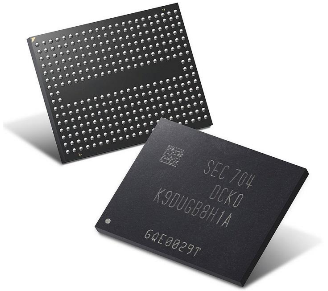


BLOCK

PAGE

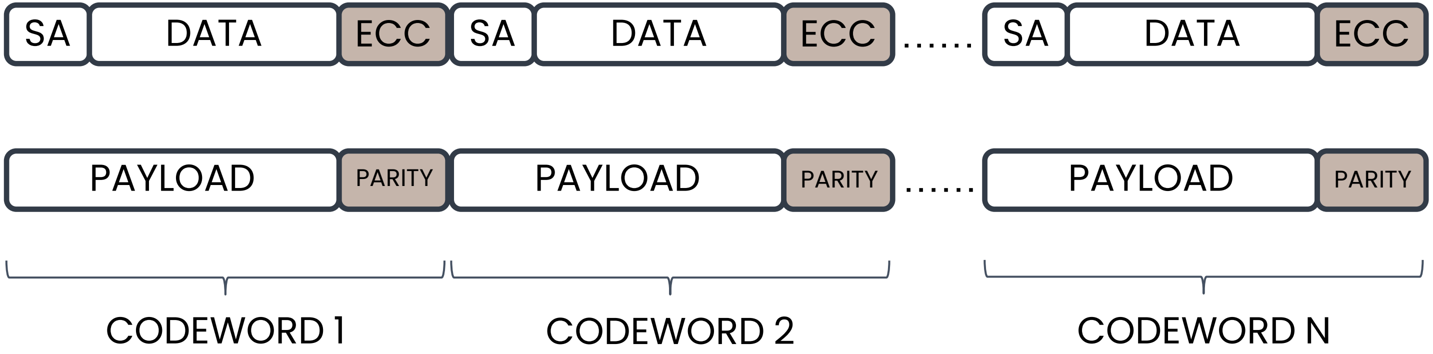
PLANE

DIE



NAND flash die layout

SPARE AREA, DATA AREA, ECC AREA



CODEWORD: Controller model, Page size, ECC size, Number of Codewords

Page/ ECC structure (payload/parity)

Error Correction Codes (ECC) are algorithms used to add additional information (**parity bits**) to stored data.

These additional bits enable the detection and correction of errors when reading the data.

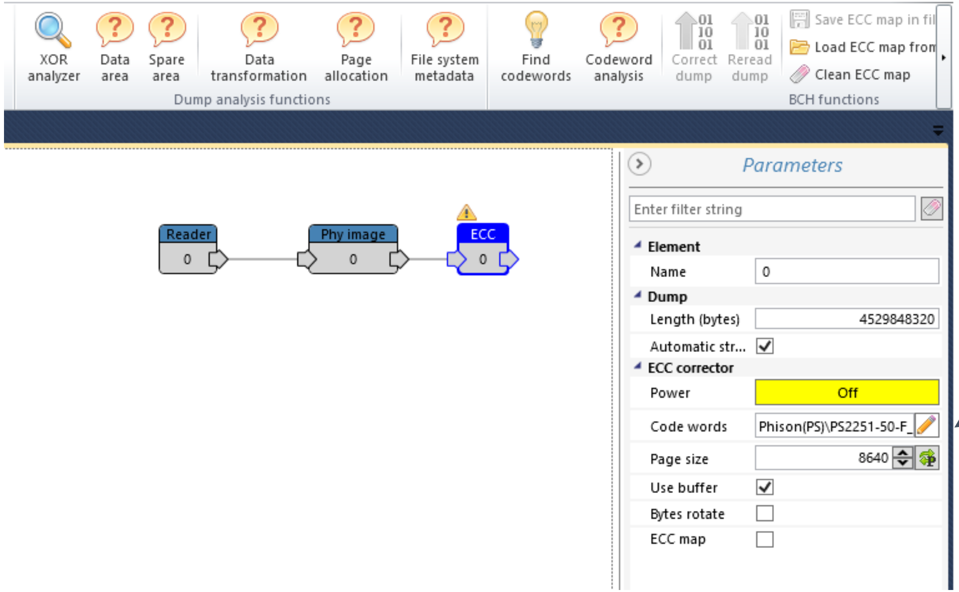
The **BCH ECC codes** are frequently utilized in flash storage devices. The BCH algorithm is customizable and comes with a specific set of parameters. These parameters are pre-configured in the controller's firmware and vary from one model to another. **If the controller becomes damaged**, the parameter information is lost; however, **ECC checksums persist** within each page of the NAND chip.

ECC

We use a BCH decoder designed to correct errors in data by utilizing the available ECC checksums. This ECC-based error correction algorithm can be implemented on the physical image after it has been extracted

This process is very time consuming

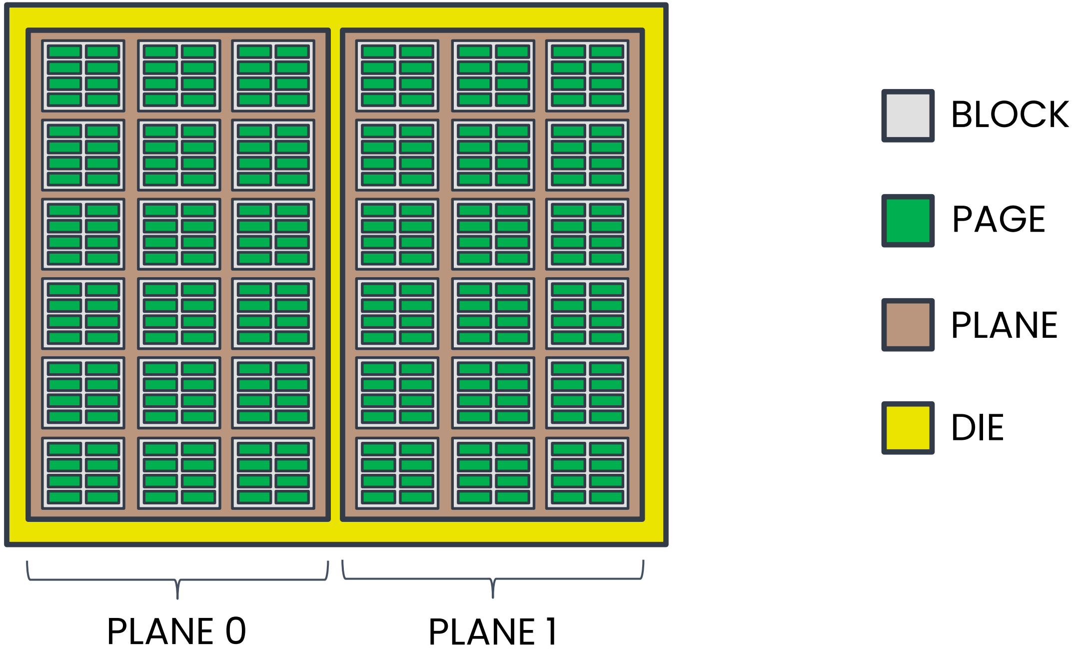
ECC



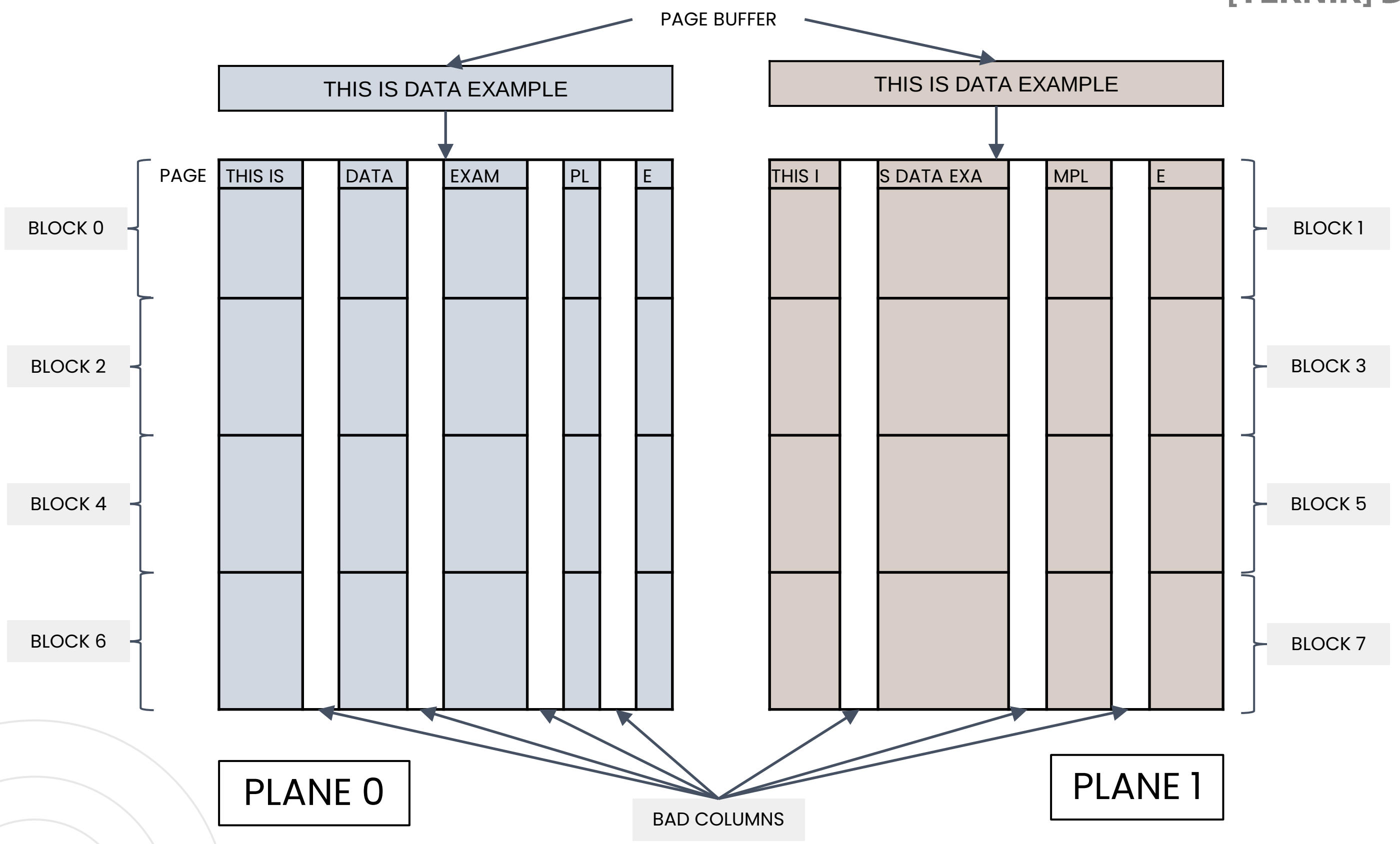
Autodetect or search in database (if lucky)

Phison controller

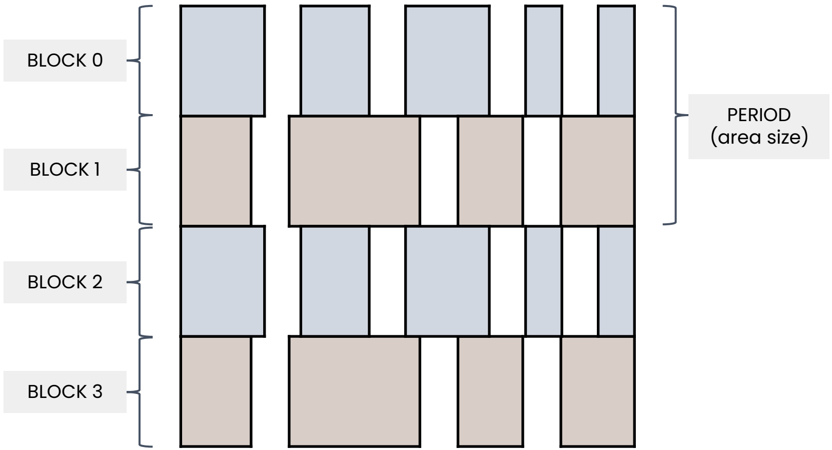
Page of flash memory



NAND flash die layout

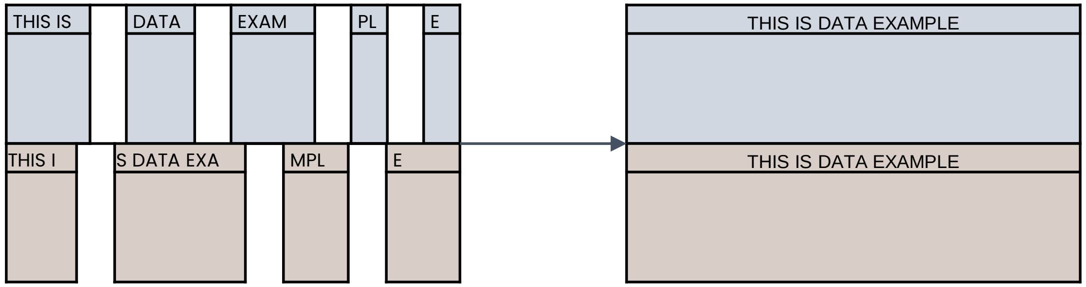

PAGE BUFFER
THIS IS DATA EXAMPLE
THIS IS DATA EXAMPLE
PAGE
THIS IS
DATA
EXAM
PL
E
THIS I
S DATA EXA
MPL
E
BLOCK 0
BLOCK 2
BLOCK 4
BLOCK 6
BLOCK 1
BLOCK 3
BLOCK 5
BLOCK 7
PLANE 0
PLANE 1
BAD COLUMNS

Bad columns



PHYSICAL IMAGE

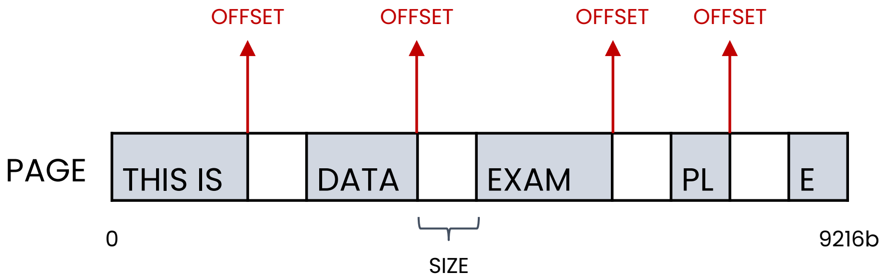
Bad columns



PHYSICAL IMAGE WITH BAD COLUMNS

PHYSICAL IMAGE WITHOUT BAD COLUMNS

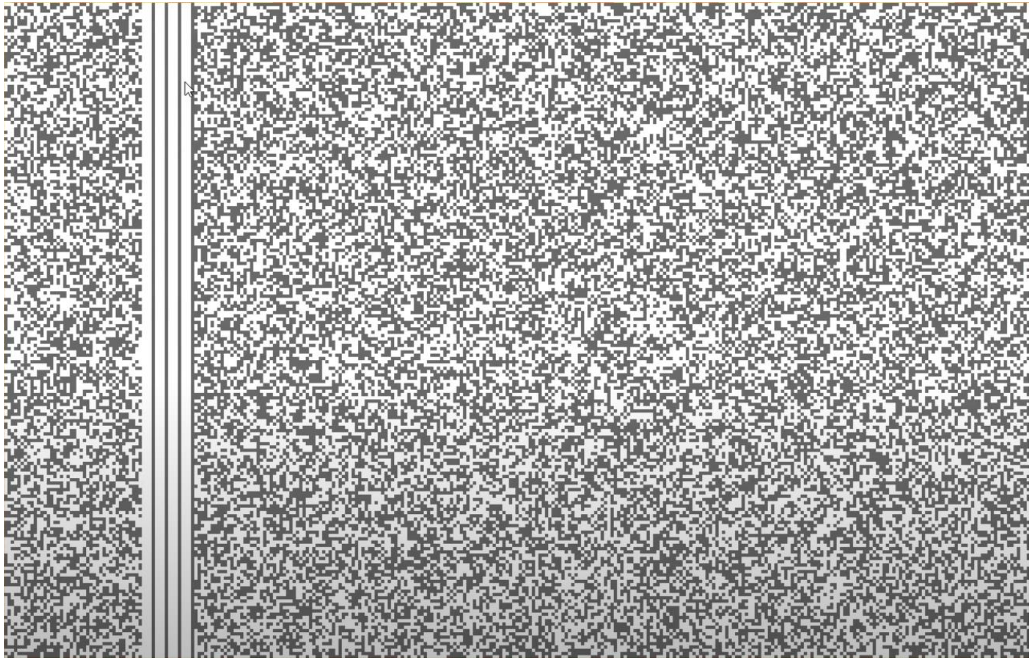
Bad columns



It’s necessary to determine the location, size and number of Bad columns within one page of each plane. Location is offset of bad column from the beginning of page. Bad Column size expressed in bytes. Number determines number of offsets from the beginning of page, that must be added in order to cut Bad Column defects.

Bad columns

Bad columns

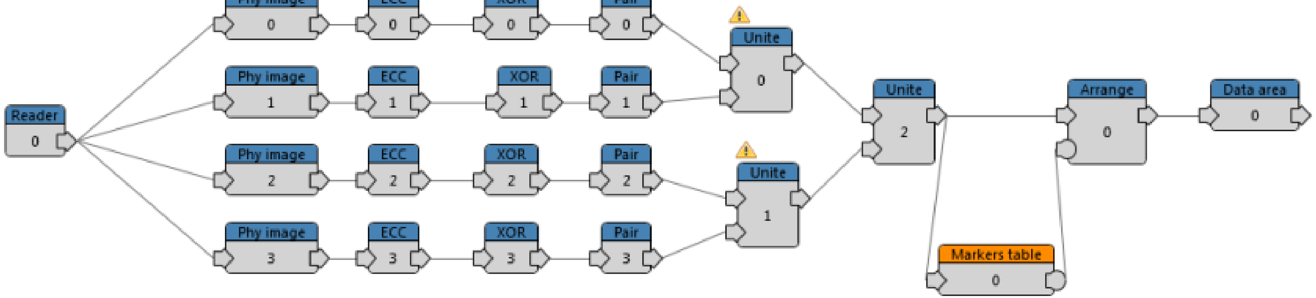


Bad columns

Modern flash controllers employ scrambling algorithms during the data recording process in flash memory. A typical implementation of a scrambler involves the generation of a unique scrambling (XOR) key by the controller, which is then combined with the data through an XOR gate/operation.
This occurs for every data block/page before it is written into the flash memory.

Generally, the XOR key is specific to a particular controller model. However, there are instances where similar controllers may use different XOR keys, and different controllers may use the same key. Unlike encryption, **scrambling is not implemented for security purposes**; instead, it eliminates data patterns that modern NAND chips struggle to store effectively due to charge leakage from adjacent cells. **It serves as a data-integrity measure** rather than a security measure.

XOR scrambling


Phy image
0
ECC
0
XOR
0
Pair
0
Unite
0
Phy image
1
ECC
1
XOR
1
Pair
1
Reader
0
Unite
2
Arrange
0
Data area
0
Phy image
2
ECC
2
XOR
2
Pair
2
Unite
1
Phy image
3
ECC
3
XOR
3
Pair
3
Markers table
0

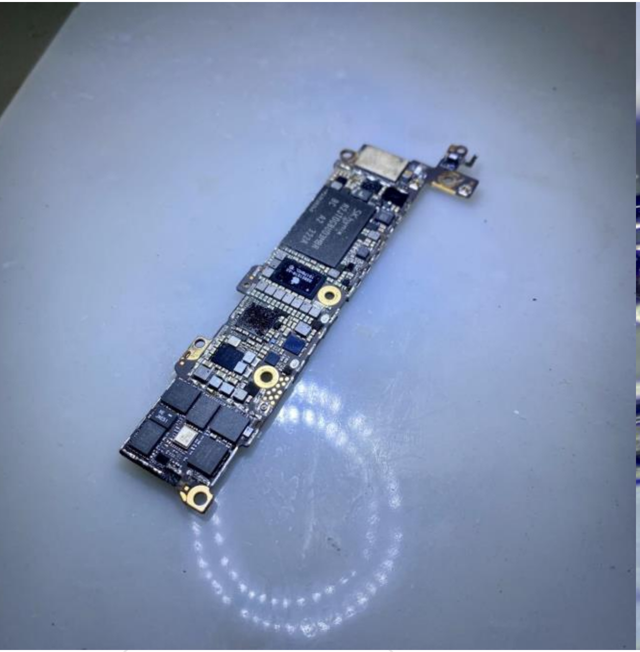
Assembly

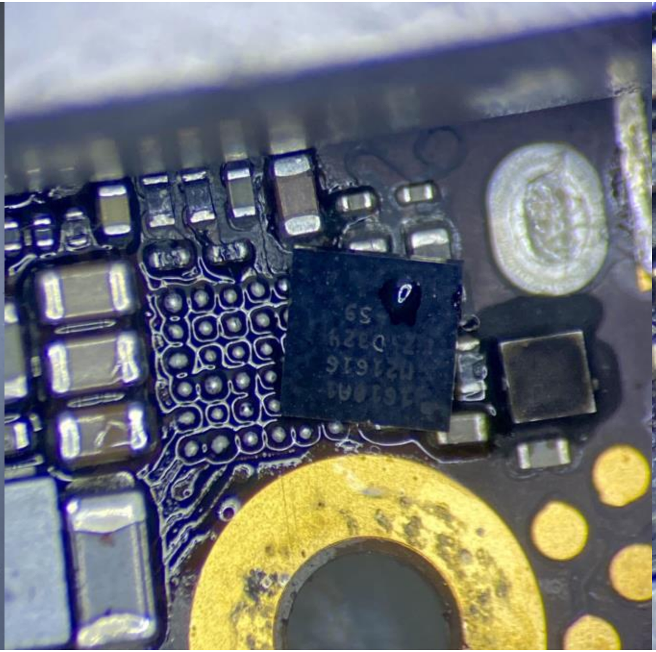
3

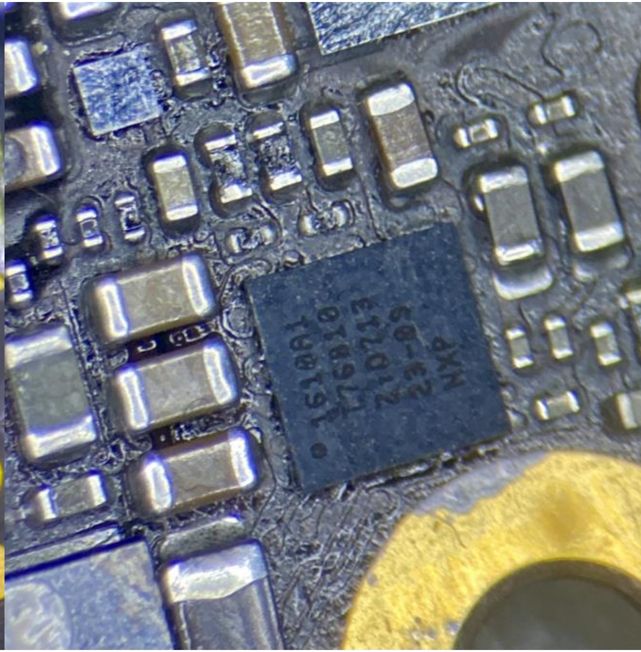
Extra Resources

Phones

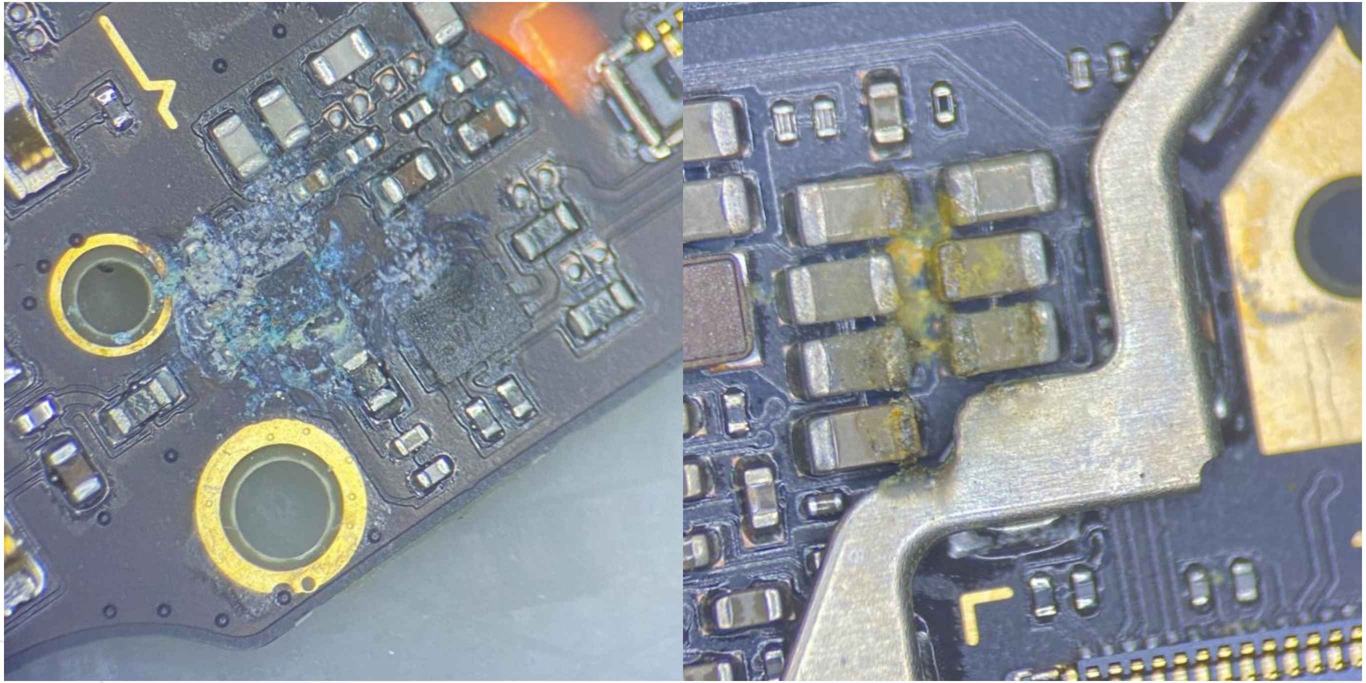

Tel: 848 880 028 | info@teknik.eus
[TEKNIK]
Empresa líder Navarra
[TEKNIK]
Repair Group
Digital
Forensics &
Data Recovery
sta web usa cookies propias y de terceros para mejorar la experienci
e navegación y ofrecerte contenidos interesantes mediante el análisi
de tus hábitos de navegación. Si continúas navegando, consideramos
que aceptas su uso. Puedes cambiar la configuración u obtener más
información en nuestra Política de Cookies.
Aceptar
Política de cookies



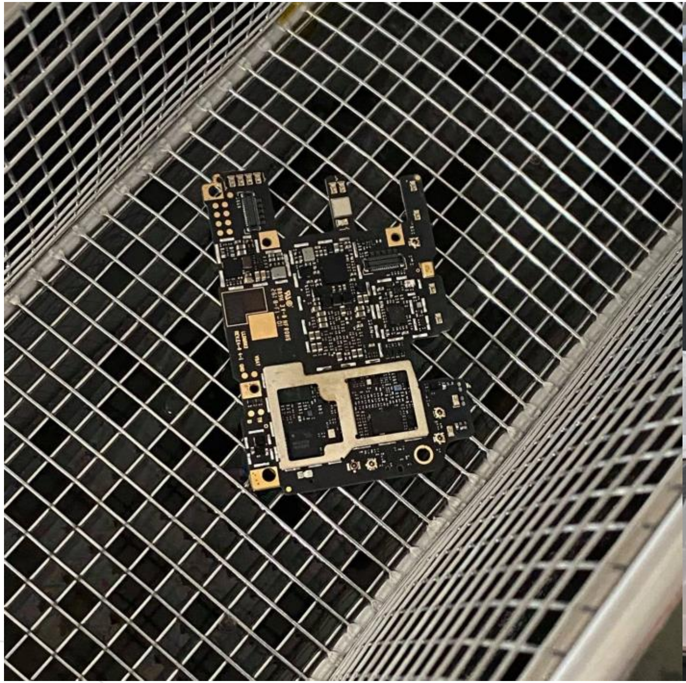




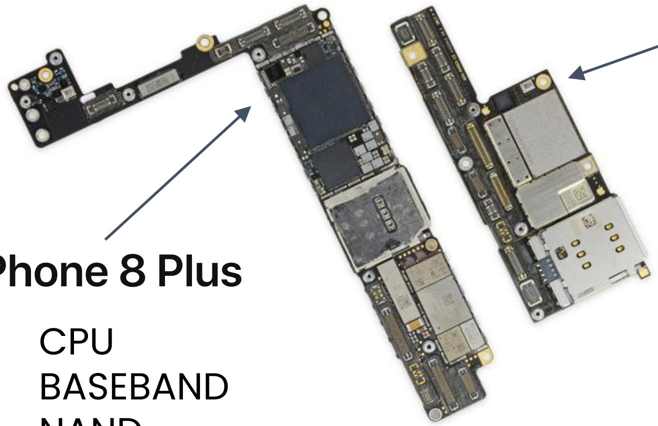
iPhone SE (liquid damage)



Xiaomi Mi A2 (liquid damage)



Xiaomi Mi A2 (EDL mode)



iPhone 8 Plus

- CPU
- BASEBAND
- NAND
- EEPROM

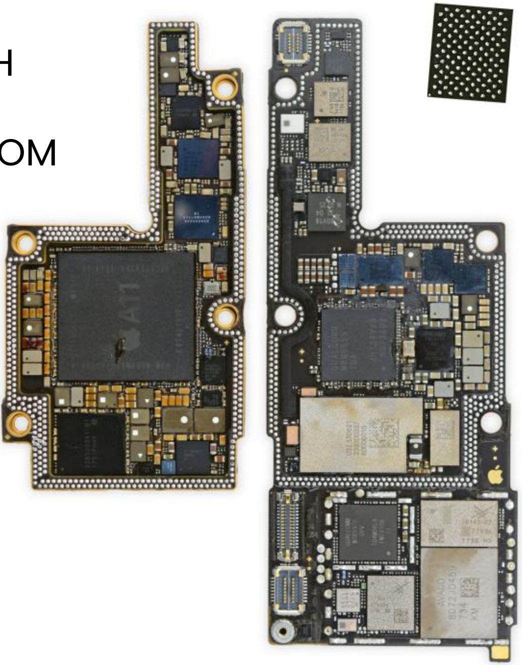
iPhone X

Bottom board:

- NFC
- WIFI/BLUETOOTH
- BASEBAND
- BASEBAND EEPROM

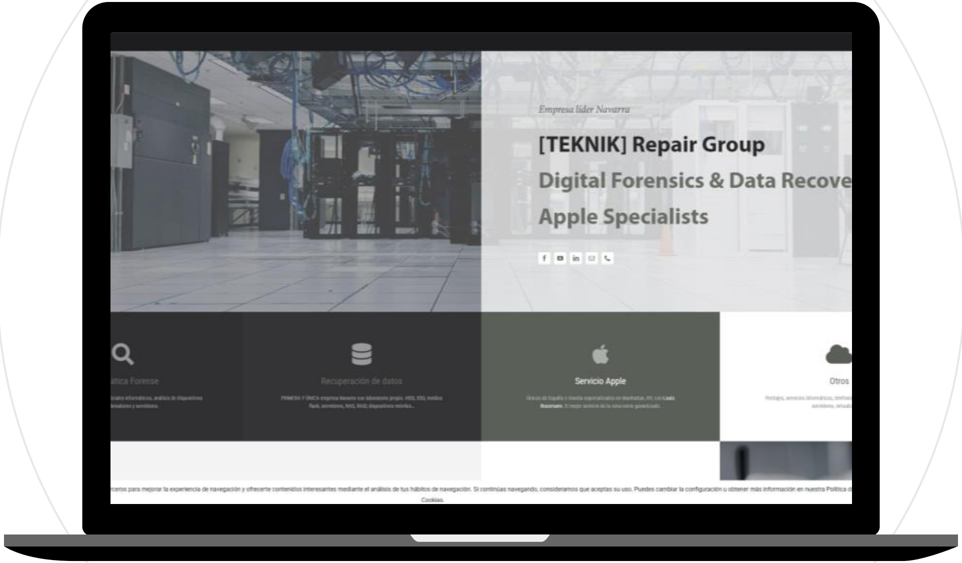
Top board:

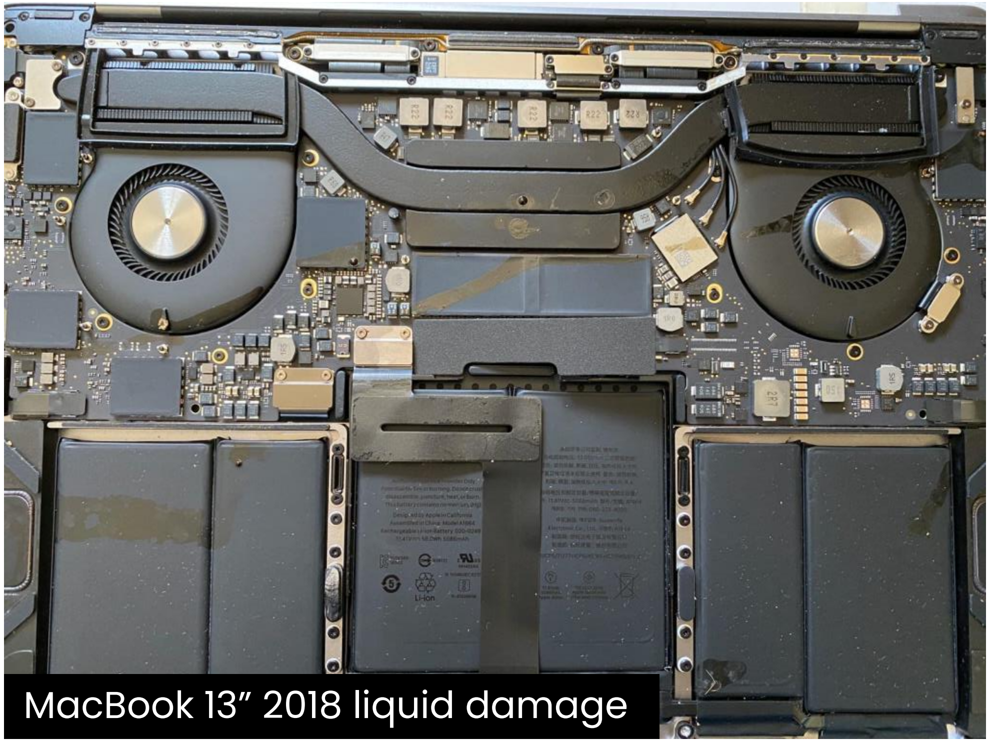
- CPU
- LOGIC EEPROM
- NAND



Chip swap

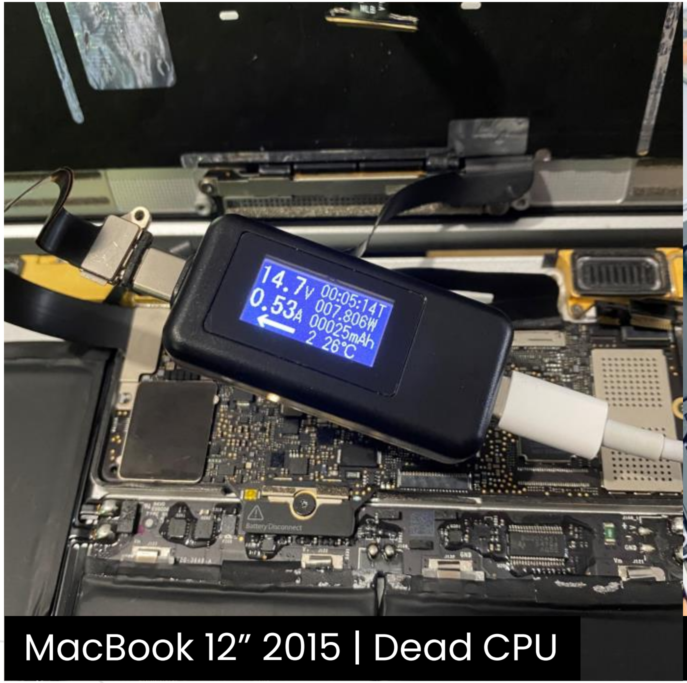
Laptops


Empresa líder Navarra
[TEKNIK] Repair Group
Digital Forensics & Data Recove
Apple Specialists
Recuperación de datos
Servicio Apple
Otros



MacBook 13” 2018 liquid damage

MacBook



MacBook 12” 2015 | Dead CPU


MacBook Pro M1 2021

MacBook

Honorable mention: Louis Rossmann

- Pioneer right to repair activist
- **Joe Biden** signed an executive order directing the Federal Trade Commission to draft new regulations limiting device manufacturers' ability to restrict independent repairs of their products.
- In 2022, got the first bill passed in Colorado. In 2023, we saw two more bills pass in Minnesota & California.
- Has been supported by millions of people and the entire electronics community, including Apple co-Founder: **Steve Wozniak**

Thanks!

Any questions?

You can find me at

info@teknik.eus