

## Scientific Data Recovery Methods and Solutions in Devices using Flash Memory

**Abdulkadir ÖZDEMİR**

*Konya Cyber Crime Branch Office*

**Şaban GÜLCÜ**

*Necmettin Erbakan University*

### Introduction

Since devices using flash memory are used extensively in daily life, falling, crushing, breaking, and static electricity, etc. they can be overexposed and damaged. Due to their complex structure, data recovery in case of failure is much more difficult than hard disks.

There are two basic data recovery ways:

- The first way is to access the data by fixing/repairing the problem that prevents access to the data.
- The second way is the methods that will be used to access the data if the first method failed or the first method is not applicable. It is to access via Jtag/Isp/ protocols (On- Chip) without removing the data register unit, while the data chip is on the device.

If the data could not be reached with “On-Chip”,

- If the device is encrypted,
- If the device only has a data logger,
- The device has an interface different from the standard,
- The device’s firmware (firmware) is corrupted,
- The data cannot be accessed (corrupted) via the interface of the device, it is accessed from the eMMC or Nand interface by removing the data recording unit (Chip-Off ) from the device.

“On-Chip” and “Chip-Off” methods are available in the literature. It is expressed as direct access to (Rusolut Sp. z o.o., 2022).

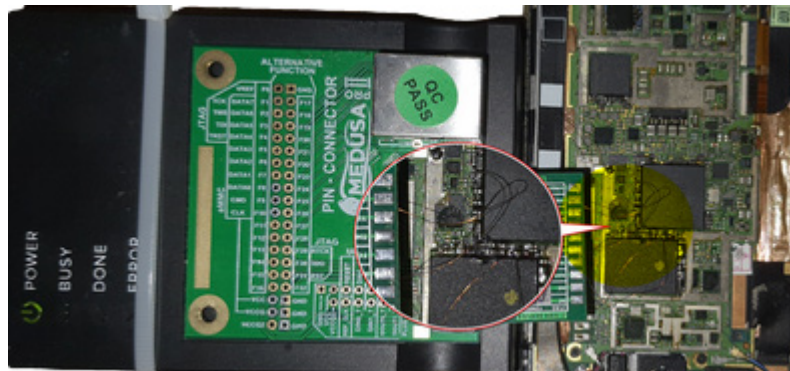
**Full Swap:** It is believed that the device’s controller and data chip (s) are intact, and if the donor is available, data can be accessed by moving the controller and data chip(s) to the donor device, this is called full swap.

**Jtag/ISP (On-Chip):** JTAG, Joint Test Action Group; ISP is short for In-System Programming. Industry standards are used to verify and test printed circuit boards after manufacture. Although the data recording medium works, if all data cannot be retrieved from the standard interface (physical copy) or if the device’s malfunction cannot be resolved, it is aimed to retrieve data using Jtag/ISP standards. Special devices and

sockets are used to enable this process to take place. During these operations, no part is removed from the printed circuit board of the data recording medium. It is performed by soldering the pinpoints on the Jtag/ISP device around the data chip and the technological test points (pinout) of the data recording medium. The read data of the mobile device is transferred to the computer environment via the USB connection (Johnson and Christie, 2009). Technological test points/pinout to be soldered using Jtag/ISP is provided by the device manufacturer or provided from open sources. Pin names to be soldered for Jtag/ISP are presented in Table 1 and a sample ISP-connected mobile phone printed circuit board is presented in Figure 1.

**Table 1.** Jtag, ISP, UFS Pin Names to Be Soldered

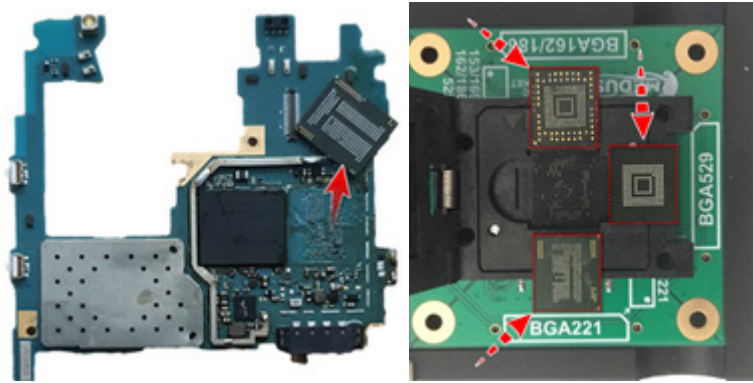
| Standard | Pin Names                                                                                  |
|----------|--------------------------------------------------------------------------------------------|
| JTAG     | Gnd, Vcc , Tdi , Tdo , Tclk , Tms , Rtcck , Trst                                           |
| ISP      | Gnd, Vcc (2.8V), Vccq (1.8), Clk , Cmd , D0                                                |
| UFS      | Gnd, Vcc (2.8V), Vccq (1.8), Txon (Dino_C), Txop (Dino_T), Rxon (Douto_C), Rxop ( Douto_T) |



**Figure 1.** Example of a device with an ISP connection

Rooting, Jailbreak, Download mode for mobile devices, EDL mode or closed physical, file system, etc. offered by forensic software. Data can also be recovered using methods (Doğanay, 2019).

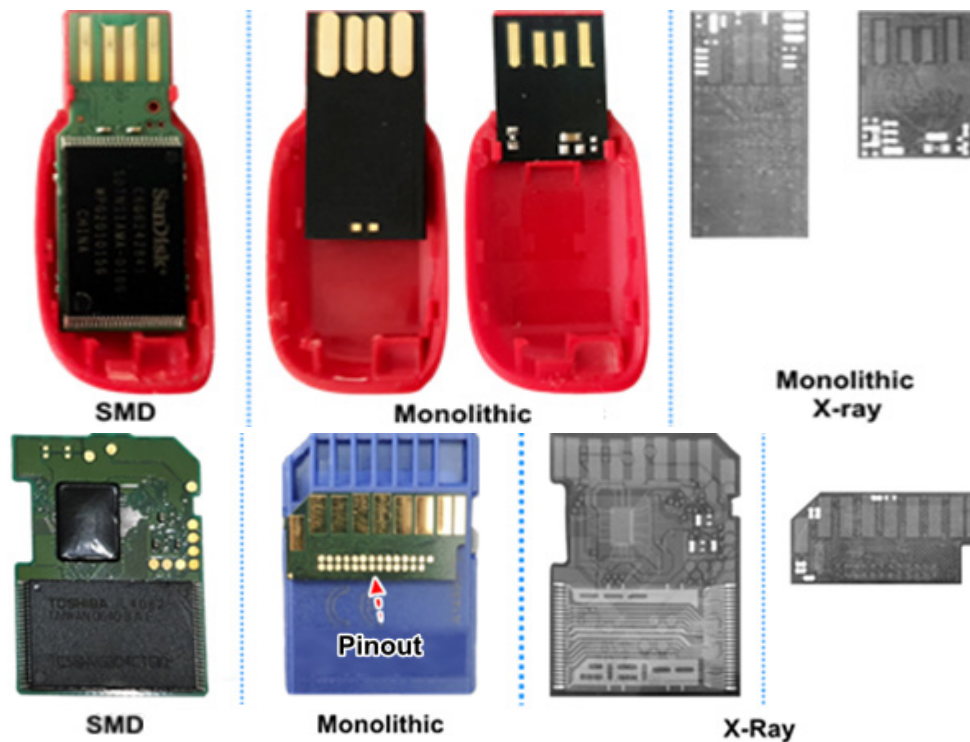
**Chip-Off:** The devices specially produced for these processes are called Box devices. Memory chips in a device are removed and placed with a special socket developed for these chips. After the socket is plugged into the Box device, the data read over the USB connection of the Box device is transferred to the computer environment. It is used as an alternative method in mobile devices using NAND memory if the data cannot be accessed by the previously mentioned methods. However, it should be used as a last resort (Özdemir and Gülcü, 2021). It is used on devices using the Android operating system and direct access to data can be provided up to the Android v6 version. On most devices after Android v6, the data is encrypted. In Figure 2, a chip-off phone (data chip is removed) and 3 different chip samples placed on the socket of the Box device, where the chips will be read, are presented.

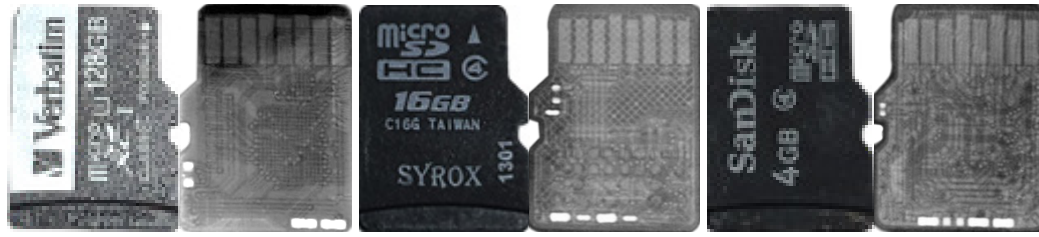


**Figure 2.** Three different data chips with a Chip-Off device

**Nand Interface:** According to whether the memory units are embedded or not, it is divided into memory using SMD components and memory with a monolithic structure. It is shown in Figure 3 through detailed examples.

Nand memory in the monolithic devices can be tested during the production phase whether it works correctly or not. These points are named pinout, technological pins, or technological contact points. Thanks to these points, memory manufacturers can test the robustness of the memories, while data recovery companies can perform data recovery operations using the same points. To recover data from the monolithic device, the signals specified in Table 2 must be soldered to the technological contact points/pinout (TTNs) in the data logger shown as an example in Figure 3 (Özdemir, 2022).



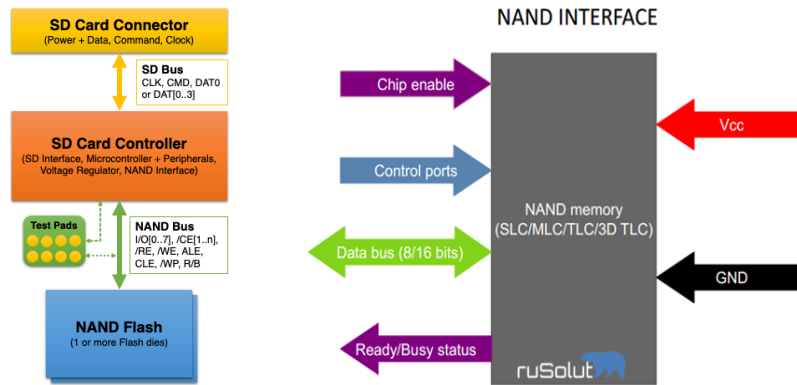


**Figure 3.** Examples of SMD and Solid type memory using NAND memory

**Table 2.** Nand Signals and Explanations (ONFI Workgroup, 2021)

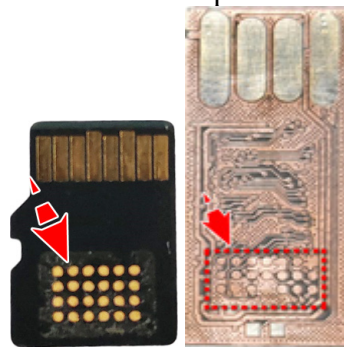
| Signal   | Input/Output | Signal Description                                                                                                                                                                                     |
|----------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ALE      | I            | Address Latch Enable is one of the signals used by the host to indicate the type of bus loop (command, address, data). When active, data can be written to an address.                                 |
| CE_x     | I            | Chip Enable signal activates the device. The activity of the signal is that the square wave is in a low position. If the signal is not active, the device is in standby mode.                          |
| CLE      | I            | Command Enable signal is one of the signals used by the host to indicate the type of bus loop (command, address, data). This signal should be low when writing commands to the command register.       |
| I/O 0-7  | I/O          | Inputs/Outputs is an 8-bit wide bidirectional port for receiving addresses, commands, and data to and from the device. (Data bus )                                                                     |
| I/O 8-15 | I/O          | Nand memory is 16 bits, the first I/O 0-7 is used in addition to I/O8-15.                                                                                                                              |
| NC       |              | No Connection                                                                                                                                                                                          |
| NU       |              | Not Usable                                                                                                                                                                                             |
| R        |              | Reserved for future use.                                                                                                                                                                               |
| R/B_x    | I/O          | Ready/Busy signal shows the status of device operation. When low, it indicates that a write, erase, or read (LUN) operation is in progress. It returns to the high state when the process is complete. |
| RE       | I            | Read Enable signal controls the serial data output from the device. When active (low) data is output from the device.                                                                                  |
| VCC      | I            | Power                                                                                                                                                                                                  |
| VDD      |              |                                                                                                                                                                                                        |
| GND      | I            | Ground                                                                                                                                                                                                 |
| VSS      |              |                                                                                                                                                                                                        |
| VSP      |              | Vendor Specific, the function of the signal is defined and specified by the NAND manufacturer.                                                                                                         |
| WE       | I            | Write Enable signal controls the capture of commands, addresses, and input data.                                                                                                                       |
| WP       | I            | Write Protect signal disables write to memory and erase operations. It is generally recommended to connect to VCC, but the port can also be connected                                                  |

Figure 4, the connection between the controller, Flash memory, and TTNs, where the data reading process passes from the flash memory to the controller and then to the computer environment via the USB interface.



**Figure 4.** The connection between controller, Flash memory and TTNs, and I/O status (Gin, 2020; Rusolut Sp. z o.o., 2022)

In light of this information, it will be concluded that the flash memory of the devices can be accessed via the USB interface as well as via TTNs. TTNs must be used for data recovery as we cannot access solid devices through their standard interfaces (over the controller). The TTNs of monolithic devices are either covered with a protective layer or covered with tape. To access TTNs, the protective layer above the TTN needs to be scraped with a fiberglass pen or sandpaper first 1000+ then 2000+, or the protective tape removed. If sanding is done by moistening, it does not remove dust and scraping takes place faster because the sandpaper will not clog. Figure 5 shows a micro SD memory card with the adhesive tape removed and a solid USB flash memory (UFD) with an etched coating. Also, TTNs of an SD card are presented in Figure 5.



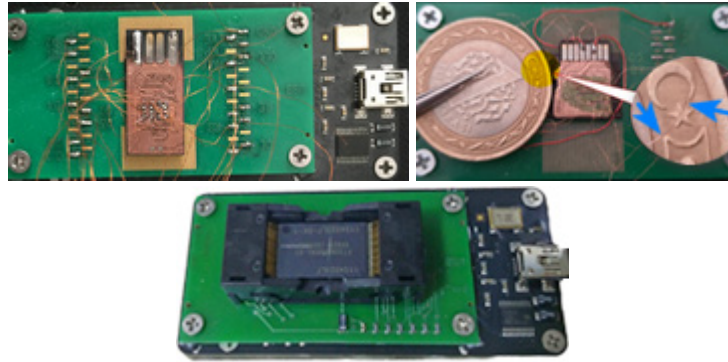
**Figure 5.** Tape - removed microSD and scraped UFD

This recovery process consists of 2 main stages:

**First Stage:** It is the process of making TTNs visible, soldering the signals on special equipment, or plugging them into sockets and reading this equipment as a dump (raw) to the computer over the USB connection.

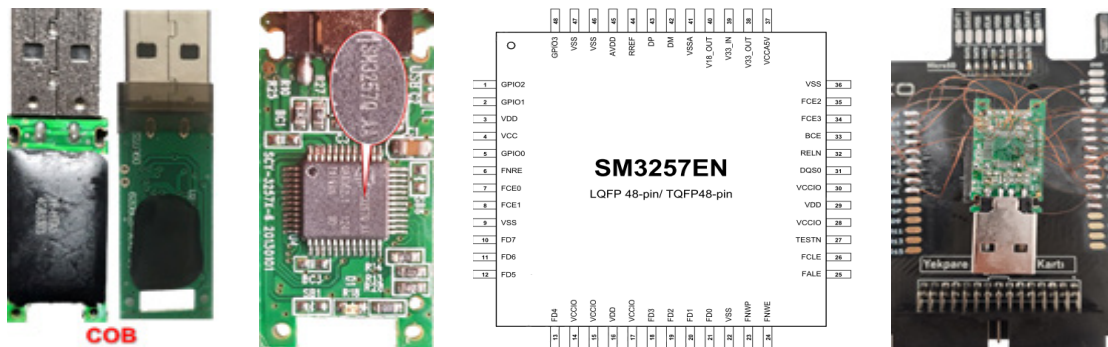
Data writing is through the USB interface to the controller and then to the flash memory. Data is recorded using structures (Abrasion compensation, Bad block management, Erase before writing restriction, etc.) in the Flash memory conversion layer within the controller. In other words, the controller writes data to the (Özdemir and Gülcü, 2021). Figure 6 with Nand connections, microSD, and a Tsop48 data chip placed in the socket. To understand the sensitivity of the jumpers (blue arrowhead) used in the soldering

processes, their photos were taken with 1TL.



**Figure 6.** Examples of devices with Nand connections

All detachable circuit elements (including the controller) on the device must be removed since the USB flash drives whose packaging type is Cob/Blob shown in Figure 7 are not memory units that can be removed or scraped to reveal TTNs. After disassembly, the controller's manual (datasheet) should be found. After learning the output signals of the pads where the controller's legs sit from this manual, the actions described above as the first operation should be performed.



**Figure 7.** With COB-type flash memory and its soldered Nand connections

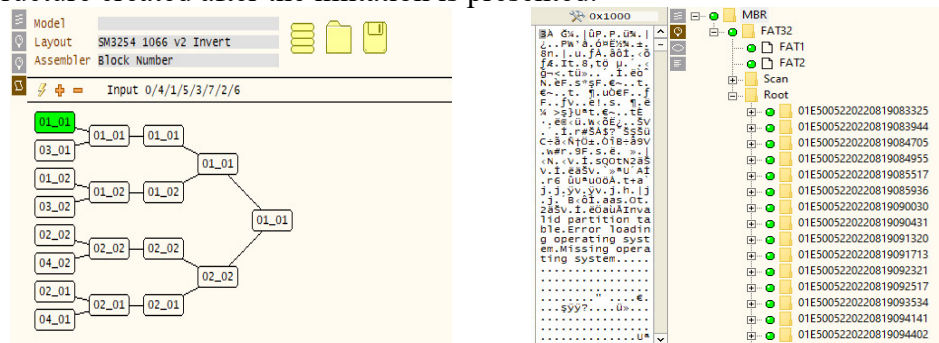
Nand Manufacturer brands according to their 3. According to the brands in this chart, Retry, power special reading settings such as mode must be performed. Power mod just Tsop is an enhanced option for reading chips (Özdemir, 2022).

**Table 3.** Nand Owned By Their Manufacturers ID

| ID | Brand   | ID | Brand   |
|----|---------|----|---------|
| 2C | Micron  | 98 | Toshiba |
| 45 | Sandisk | AD | Hynix   |
| 89 | Intel   | EC | Samsung |

**Second Stage:** The first step is to make sense of the raw data read through software (Flash Extractor, PC-3000 Flash, Rusolut) capable of data recovery from Nand devices. As an example, the first stage has been carried out and the imitation of the controller of

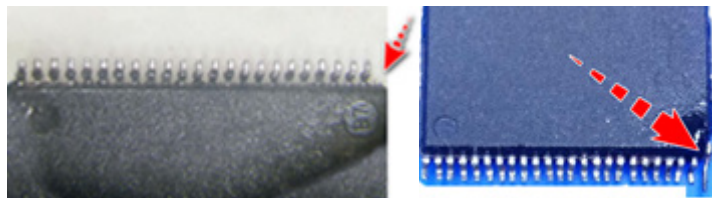
a CF card with 4 Tsop48 data chips in Figure 8 with Flash Extractor software and the tree structure created after the imitation is presented.



**Figure 8.** Imitation of the controller with Flash Extractor software and the tree structure formed as a result of this imitation

If hardware problems are to be exemplified;

- The legs of the data chip:



**Figure 9.** Example of tsop48 data chip legs breaking

- It must be repaired using the jumper.

\* Loss of USB busses:



**Figure 10.** USB bus break

- \* It must be repaired using the jumper.

\* Breaking the USB PCB:



**Figure 11.** Breaking the USB PCB

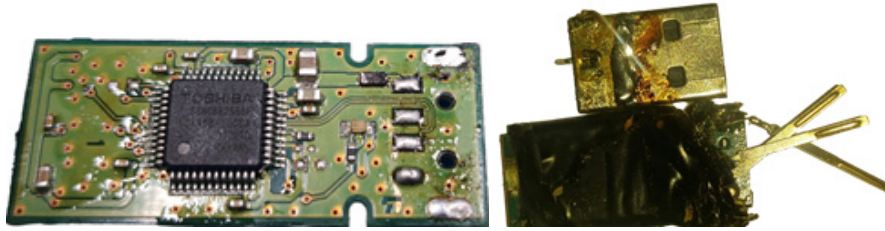
- Soldered to a solid USB socket.

- \* Breakdown of electronic circuit element:



**Figure 12.** Fragmentation/loss of circuit element

- Donor or it should be completed by finding the diagram and determining the circuit element.
- \* USB socket was broken:



**Figure 13.** USB socket broken

- Soldered to a solid USB socket.
- \* USB socket pins not touching:



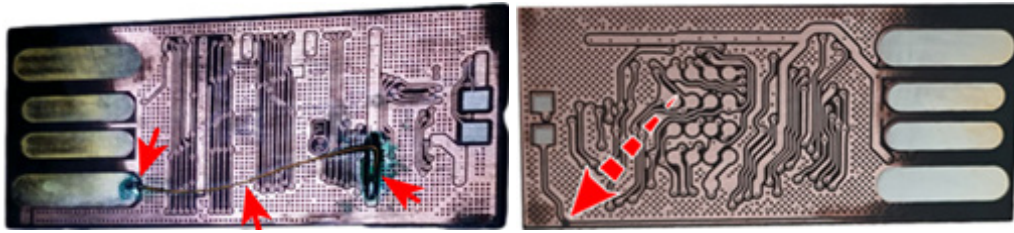
**Figure 14.** USB socket pins not touching

- Pins must be soldered.
- \* Deterioration of fuse resistor or capacitors:



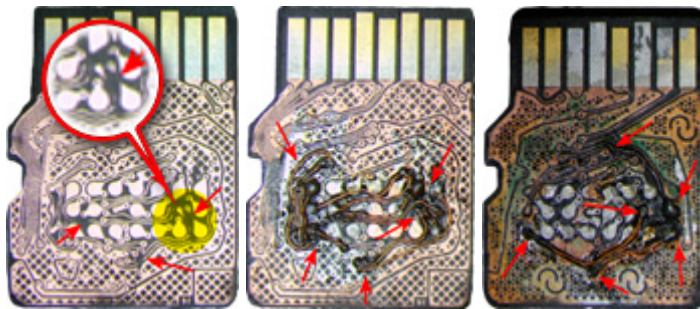
**Figure 15.** Bad fuse resistor

- The resistor must be changed or a jumper must be used. Capacitors must be replaced. Chip On or Chip If Repair Failed Off should be applied.
- \* Power (5V) not reaching memory or internal or surface bus being broken path:



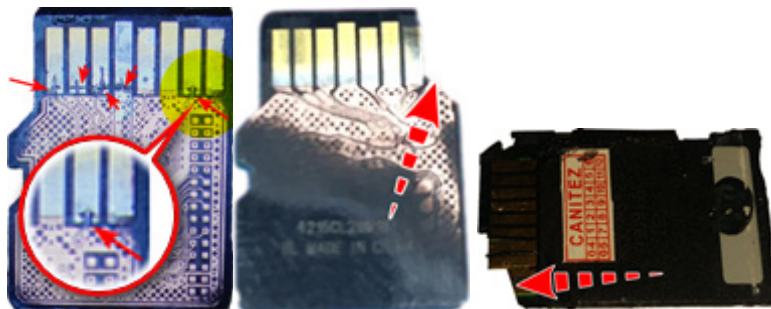
**Figure 16.** Internal and surface path break in USB flash memory

- Provided with the jumper or the broken path should be repaired.
- If the surface paths of the memory card are broken:



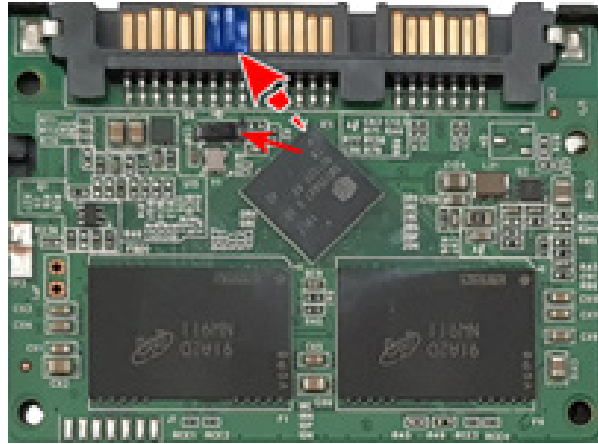
**Figure 17.** The paths of the memory card are broken

- \* Paths with jumpers must be repaired. Or it must be accessed from the Nand interface.
- \* Broken or broken memory card busses:



**Figure 18.** Broken or broken memory card busses

- Broken connections should be connected with a wire. Or by following the bus, the solder should be applied to the card reader by using the jumper from the last visible point.
- \* SSD data interface degradation and diode degradation:



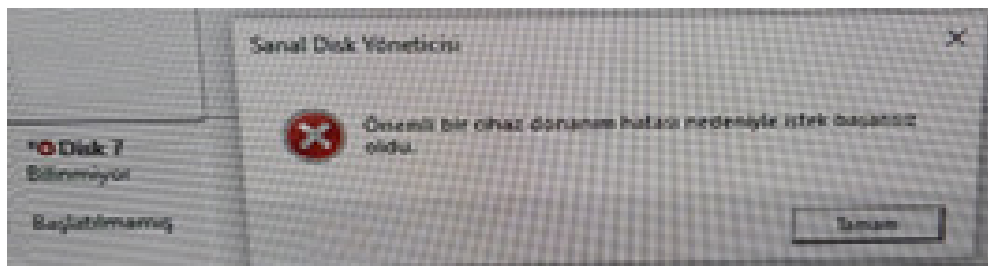
**Figure 19.** SSD data interface corruption

- The data interface should be repaired and the diode replaced or removed.
- \* Breakage of the circuit element on the SSD PCB:



**Figure 20.** Example of fragment breaking from SSD

- Soldered by detecting the circuit element by finding the donor or by finding the schematic.
- M.2 SSDs in the wrong socket:



**Figure 21.** Installing M.2 SSDs in the wrong socket

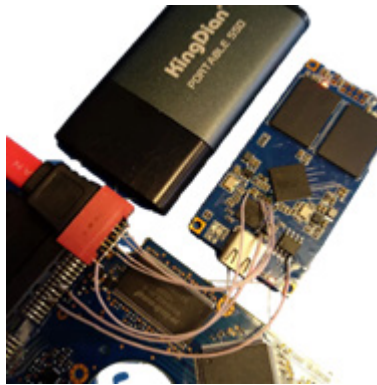
- Socket details Must be plugged into a shape-matched socket or reader
- \* Deterioration of circuit elements on the memory card PCB:



**Figure 22.** Deterioration of circuit elements on the memory card

- The donor must be found and the circuit element must be replaced.

\* USB socket not working:



**Figure 23.** Example of SSD with USB socket not working (Total-Recovery, 2022)

- The data must be accessed by performing the conversion to the Sata interface.

\* Failure of busses after liquid contact:



**Figure 24.** Bus not working after liquid contact with (ITHOPE s.r.o., 2021)

- M.2 disk that cannot be accessed from its default interface must be converted to SATA.

\* Physical environmental conditions of the environment where the data logger is located:



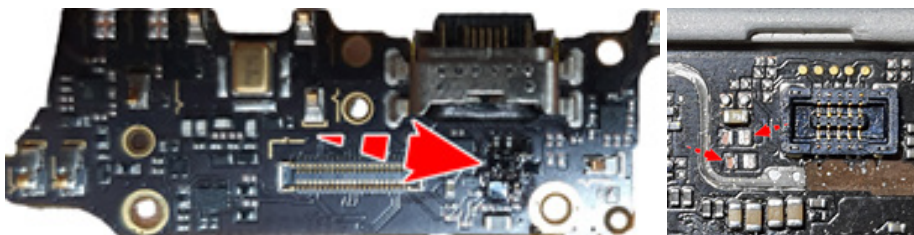
**Figure 25.** Example of a mouse biting the power cord

- The power cord must be replaced. Environmental conditions should be considered. From time to time, physical environments where data recording media are located should be checked.
- \* Breaking the data paths of mobile devices, breaking their sockets, breaking the socket pins, clogged the socket:



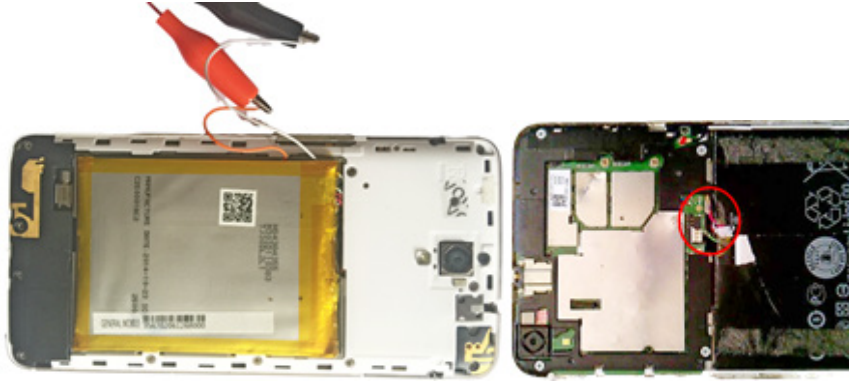
**Figure 26.** Socket failures in mobile devices

- Busses must be repaired with a jumper, breaks must be replaced with new sockets, and their blockages must be removed.
- \* Failure of circuit elements in the bus of mobile devices:



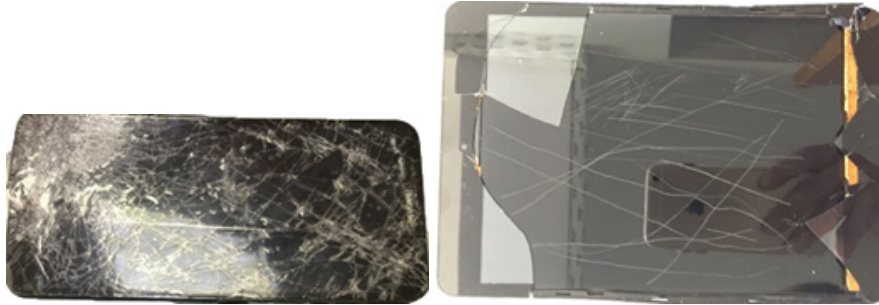
**Figure 27.** Malfunction of circuit elements in mobile devices

- \* The donor or the relevant part should be replaced by looking at its diagram.
- Battery deterioration of mobile devices:



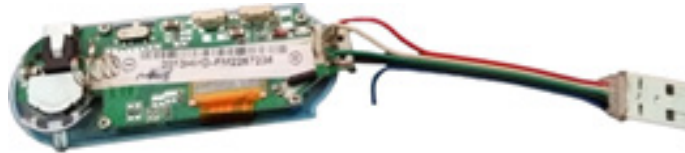
**Figure 28.** Battery deterioration of mobile devices

- External power must be supplied or a new battery must be installed.
- \* Cracked mobile screens:



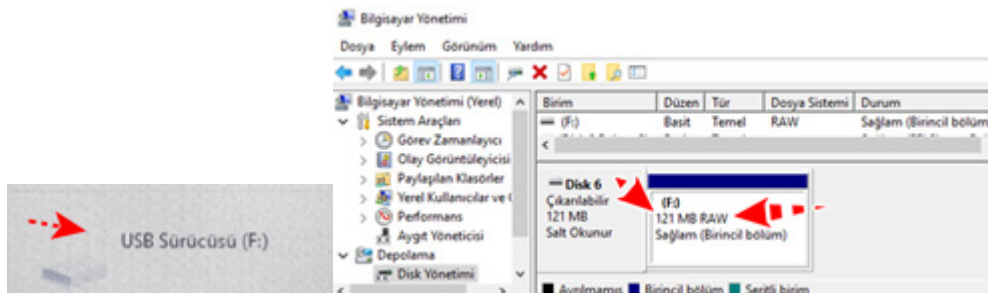
**Figure 29.** Cracked mobile screens

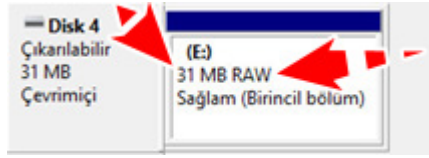
- The screen must be replaced.
- Malfunction of the socket of MP3 players:



**Figure 30.** Malfunction of the socket of MP3 players

- The socket must be replaced.
- \* USB flash drives or memory cards appear below their normal capacity:

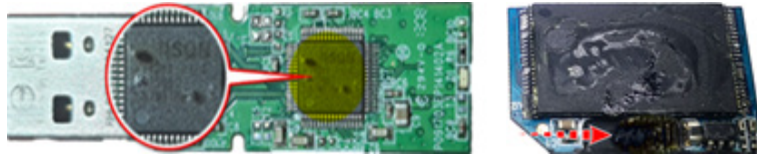




**Figure 31.** The appearance of the devices with hardware failures on the computer

- When there is a hardware failure in USB flash drives or memory cards or SSDs, as can be seen in Figure 31, they appear as an empty drive on my computer screen with a value below their normal capacity, such as “121MB” or “31MB”. It is necessary to access data on such devices using the Nand interface.

\* USB flash drive and memory card with damaged controller:



**Figure 32.** USB flash drive and memory card with damaged controller

- Requires access from the Nand interface.

\* Flash drive oxidized by liquid contact:



**Figure 33.** Oxidized USB flash drive

- Oxidation with isopropyl alcohol, if there is a faulty circuit element, it should be replaced. If the fault cannot be resolved, it must be accessed from the Nand interface.

\* Burnt memory card and memory cards with broken PCB:



**Figure 34.** Burnt memory card (Rusolut Sp. z o.o., 2014) and memory cards with broken PCB

- Chip-Off should be tried

- \* Excessive scraping of memory card surface:



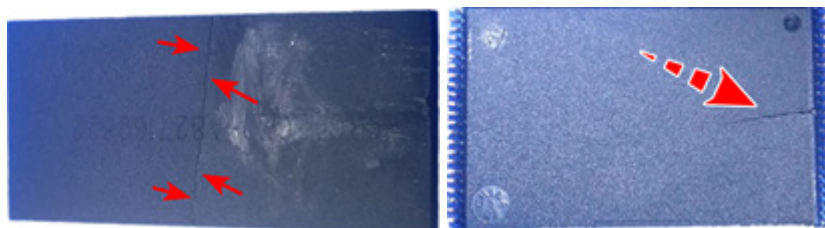
**Figure 35.** Excessive scraping of the memory card surface

- By being too scraped or physically damaged by the user to access TTNs. Access from the Nand interface should be attempted by taking X-rays and determining the exact locations of the TTNs.

- \* Memory card or data chip broken, cracked, or dented:



**Figure 36.** Examples of broken, cracked, and dented memory cards



**Figure 37.** Broken UFD and Tsop48 chip examples

- An X-ray of the memory unit should be taken. If there is no damage to the Nand memory, try to get data from the Nand interface. Generally, data recovery is not possible in cases where the memory unit is broken or crushed.

- \* Combustion of parts on SSD PCB:



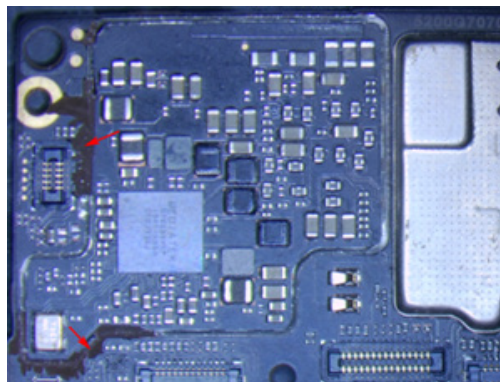
**Figure 38.** Burning parts on (DataSector, 2022)

- Data must be accessed from the Nand interface. As an alternative solution, a full replacement can be tried.
- \* A mobile device whose physical failure cannot be fixed:



**Figure 39.** An example of ISP applied to a mobile device whose physical failure cannot be repaired

- Data must be accessed by making an ISP. If inaccessible, it must be accessed from the Nand interface.
- \* Paths are broken or the protective coating has been removed on the PCB of the mobile device:



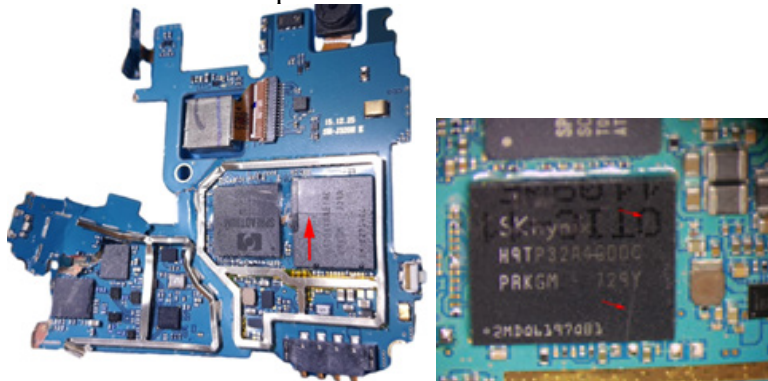
**Figure 40.** Remaining protective coating of mobile device PCB

- Jtag/ISP and then Chip-Off should be tried.
- \* Burnt cell phone:



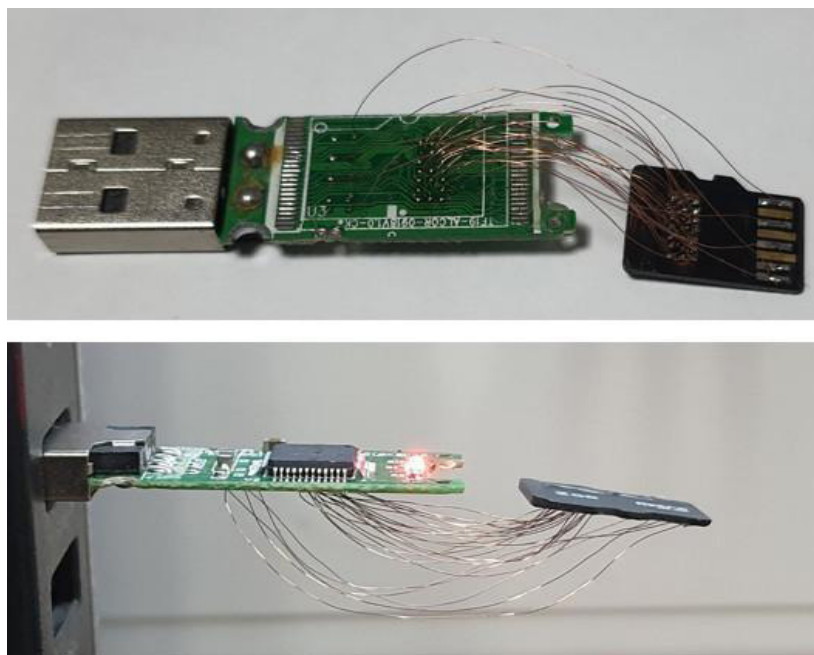
**Figure 41.** Burnt cell phone.

- Jtag/ISP and then Chip-Off should be tried.
- \* Mobile device PCB broken chip broken:



**Figure 42.** Mobile device PCB broken, chip broken

- An X-ray should be taken, if the Nand memory is not damaged, data should be obtained via Chip-Off or Nand interface.
- \* Breaking of data transmission legs of Usb Flash memory using a memory card as memory unit:



**Figure 43.** Breaking of data transmission paths

- If there are a few methods that can be used for data recovery processes;
  - » Bus reconnection can be achieved by molding the TTNs of the memory card.

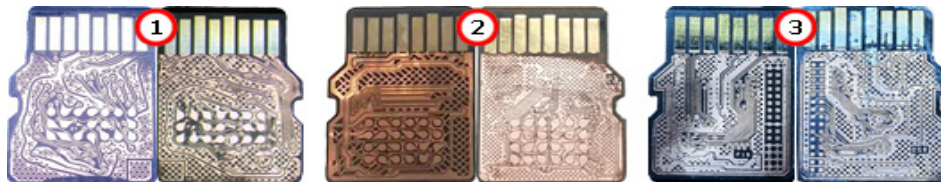
- » The TTNs of the USB Flash memory and the TTNs of the memory card can be soldered with wires.
- » The memory card can be accessed via the Nand interface (Chip-Off).

When TTNs are examined during data recovery operations on memory cards, species naming is shown in Table 4.

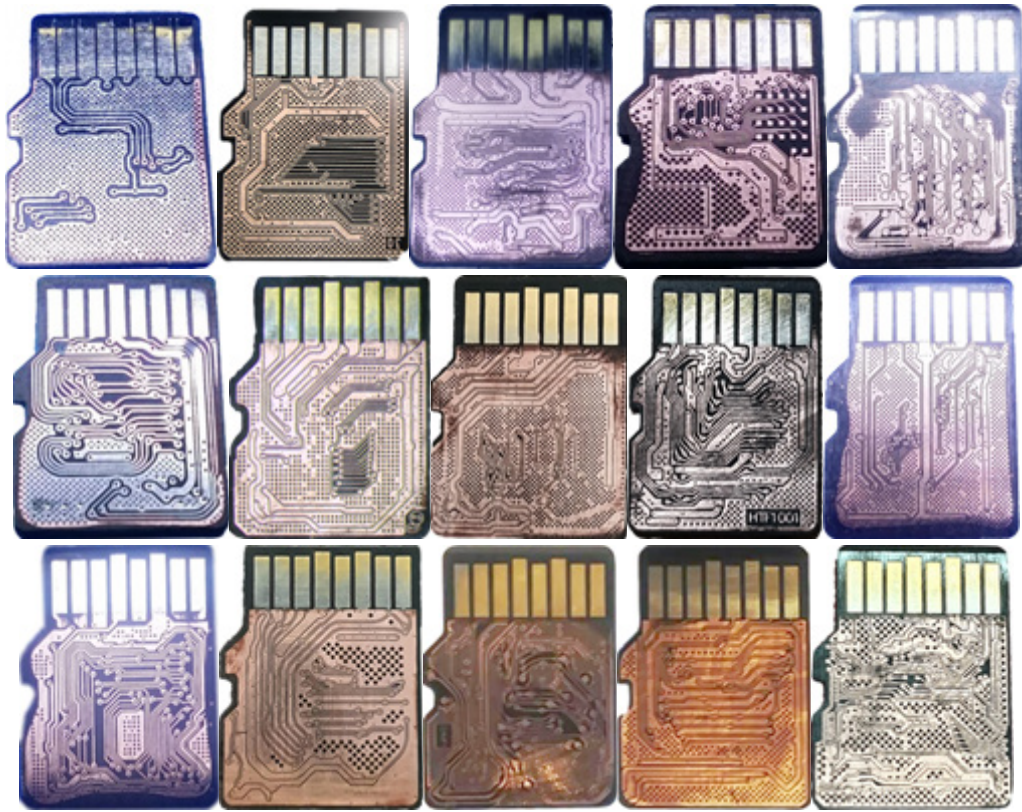
**Table 4.** Number of Encounters with TTN Types

| TTN Type | Number of Encounters | Sample Photo        |
|----------|----------------------|---------------------|
| 3x7      | 34                   | Figure 43– Number 1 |
| 4x6      | 52                   | Figure 43– Number 2 |
| 15x2     | 14                   | Figure 43– Number 3 |
| Other    | 72                   | Figure 44           |
| Total    | 172                  |                     |

As can be seen from this chart, common TTN types are 3x7, 4x6, and 15x2. It was thought that it would be useful to make an adapter for the most common type of micro SD memory cards to be read quickly as a dump using the Nand interface. Previously, it has been explained how to perform data recovery over the Nand interface. To access the memory over the Nand interface, the signal equivalents of the TTNs to be used must be known. On Micro SD memory cards, detailed information of which is presented in Table 4, it was observed that 102 were hardware and 66 were software. When the methods described above were applied, it was observed that 97 data were recovered. When examined for data recovery processes for these memory cards, it was seen that some of the TTNs were the same (Figure 44) and some were completely different from each other (Figure 45). Pages belonging to data recovery companies (Arvika Data Recovery, 2013; GreyD Lab, 2015; Rflashdata.com, 2016; RecuperoDatos.com, 2020) When TTNs would be checked, it would be seen that there are hundreds of cards with different TTNs.

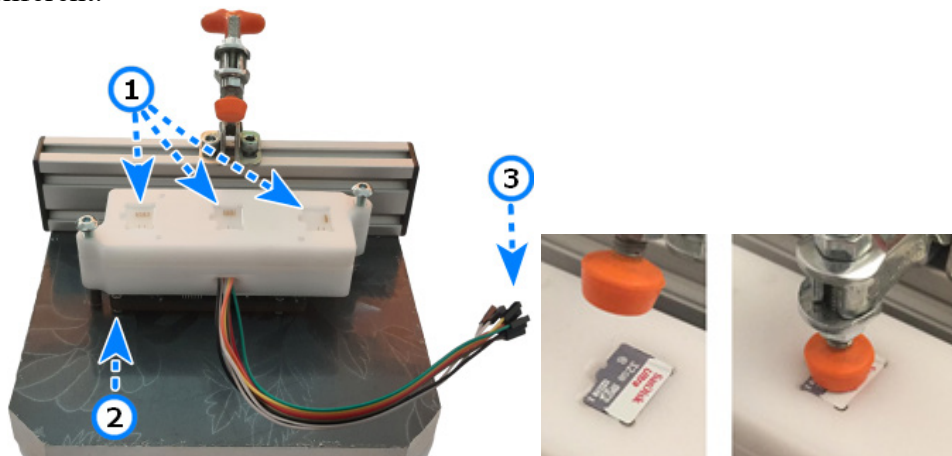


**Figure 44.** Same TTNs of different brands



**Figure 45.** Different TTNs of different brands

The points called technological touch points cannot be seen directly from the outside and are used for tests. The TTN variety is developed according to the Nand memory type, circuit elements, and data buses used by the vendors during production, and the signal information used in TTNs cannot be disclosed due to copyrights. Memory cards vary in capacity, application performance, speed, and data paths. Multi-level cell technologies are also used to ensure this diversity. Due to this diversity, it is understood from the x-ray images that the internal data paths of the cards and the circuit elements used are also different.



**Figure 46.** Completed adapter with all connections made

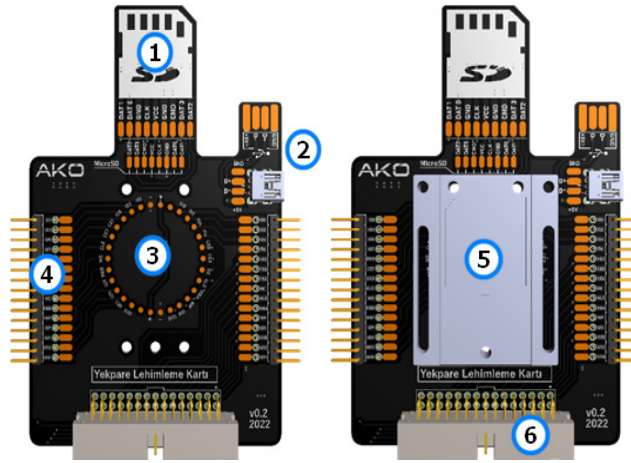
Thanks to this developed reader adapter;

\* Common TTNs, without the need for soldering, the memory card Figure 46 reading

process is performed very quickly through the Nand Reader hardware belonging to the Soft-Center Company to the part indicated with number 2.

- \* Figure 46 is also performed for the devices of other companies that produce data recovery equipment.
- \* With this adapter produced, the loss of time spent on the soldering process will be eliminated.
- \* During soldering, problems such as incorrect soldering, solder, and wire breaks that repeat the soldering process and cause time loss will be eliminated.
- \* The loss of foreign currency spent on foreign companies that carry out similar transactions will be prevented.

Flash memories are mentioned as other and not frequently encountered in Table 4 Nand interface.



**Figure 47.** Soldering board developed for memory cards and USB sticks

Thanks to this card, all of the operations listed below can be performed without the need for any other hardware (Figure 47).

- MicroSD memory cards with a standard data interface broken or pin disconnected can be soldered to the area indicated by number 1 and data can be retrieved.
- USB flash drives with broken sockets can receive data via USB interface 2.
- 3 or 4 can be used crosswise/mixed for soldering memory cards, memory packaging type Cop/Blob or solid USB flash drives to TTNs. In this way, narrow soldering operations, which are formed by overlapping jumpers during the soldering of TTNs, are facilitated.
- To perform the soldering operations, it is necessary to fix the relevant memory to the soldering board, for this, bidirectional tapes are used. With the soldering holders we have developed, the formation of residues of the bidirectional tape on the memory card and soldering card is prevented.

The double-sided tape is prevented from losing its adhesive property due to the heat of the soldering iron.

- Multicom Sp. Zo.o. Since an output compatible with the output of the soldering card produced by the company is provided, this equipment can still be used if this equipment is already available.

In summary, the absence of mechanical parts in devices using flash memory, compared to hard disks, prevents the occurrence of mechanical problems such as head and motor failures, which are frequently encountered in hard disks. However, since devices using flash memory are constantly carried in daily life (mobile phones, USB flash memory, memory card, etc.), they are more likely to encounter physical effects. Therefore, physical failures occur more than software failures compared to other storage units.

These failures are;

- Fractures/cracks in the data chip,
- In addition, breakage/deterioration of components (such as screen, touchscreen) that enable the device to be used,
- can be listed as all kinds of reasons that prevent electrical conductivity, such as deterioration and disintegration of circuit elements in PCBs.

The closer the physical failures in data recording environments to the unit where the data is stored, the higher the sensitivity and difficulty level in the recovery process. For example;

- 1- A USB flash memory socket is broken
- 2- access Nand data chip of same USB flash memory

If a comparison is made, it will take 5 minutes for the problem to be resolved by replacing the socket, the fault in number 1, and to reach the data. However, it will only take ~5 minutes to remove the data chip to fix the fault in number 2. Afterward, the data chip will be read raw, and the read data will be tried to be made meaningful by imitating the controller. Here, however, data recovery will take days, maybe weeks.

## Process Steps to Follow During Data Recovery

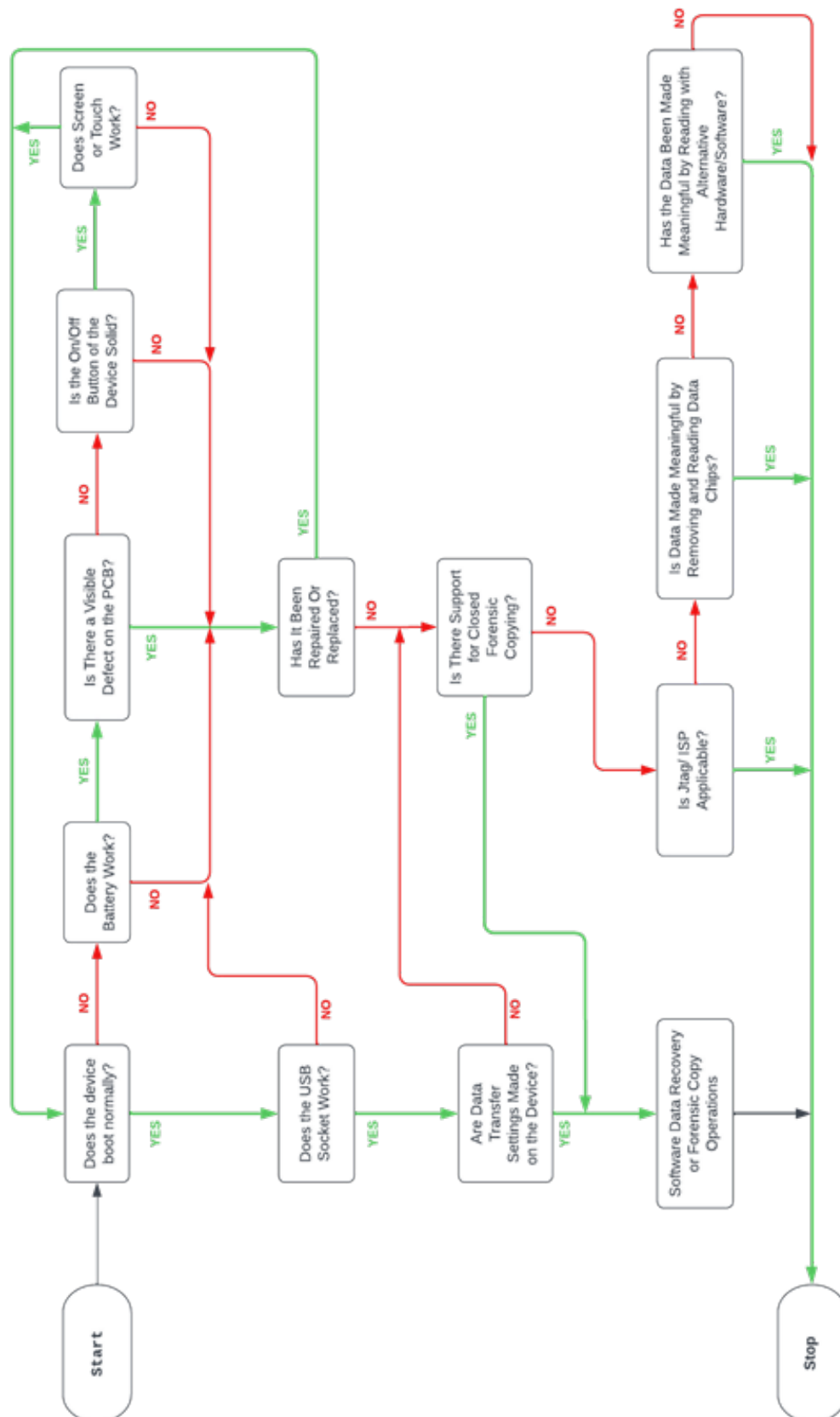
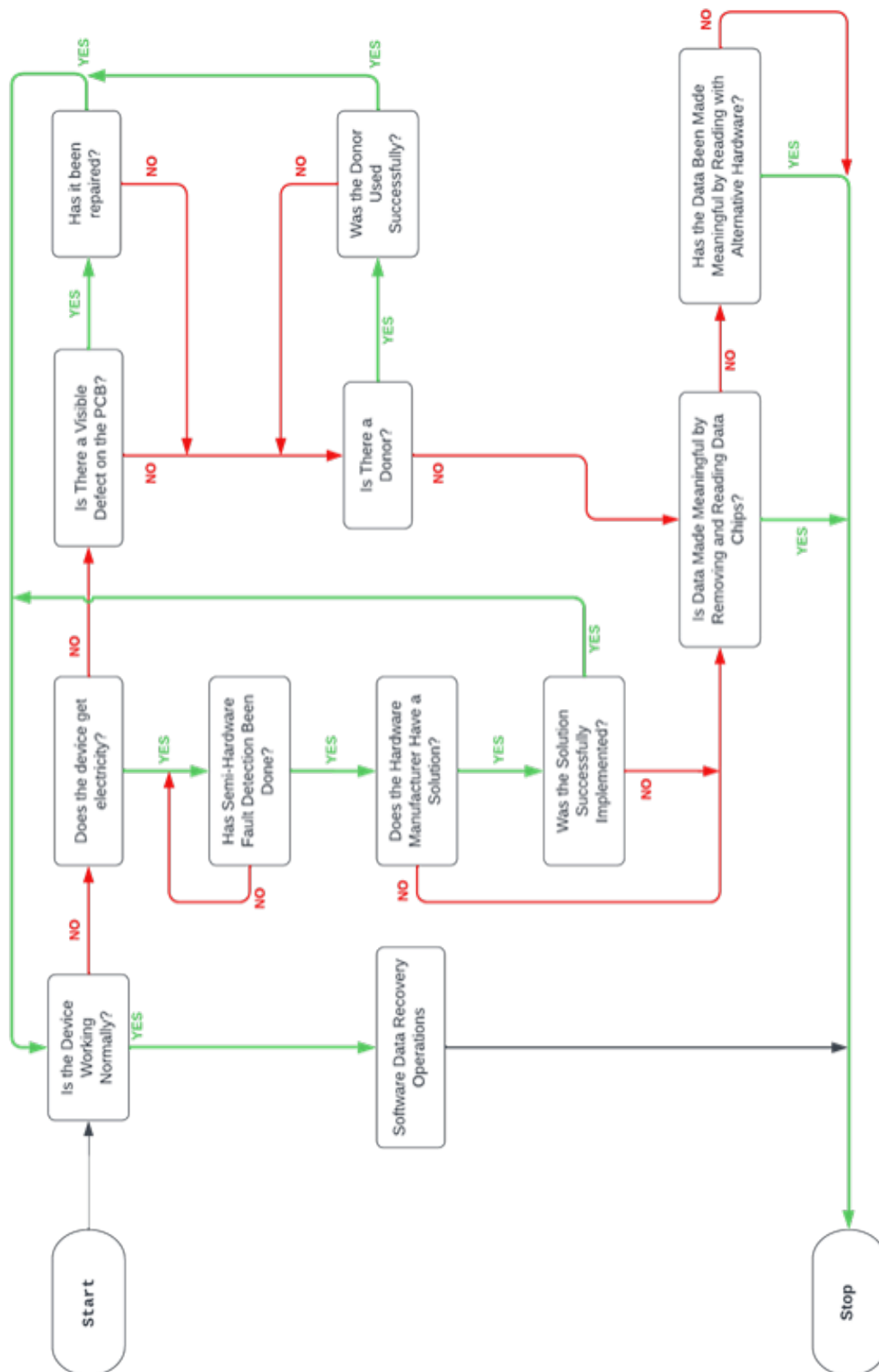


Figure 48. Data recovery steps from mobile devices



**Figure 49.** Data recovery steps from devices using flash memory

### Precautions to be Taken to Avoid Data Loss

- \* To use a power supply for hardware protection of the device in sudden power cuts.
- \* To provide grounding to protect the device from static electricity.
- \* Using a case/bag to weaken the effects of physical impacts such as hitting or falling.
- \* Position data storage units with moving parts so that they cannot be moved as much as possible.
- \* Disconnecting from the computer using the “remove hardware” option to avoid corrupting files during data transfer to an external data storage or editing of data on it.
- \* Anti-virus etc. to prevent data encryption or corruption caused by a virus. using security software.
- \* To provide physical security to protect the data logger from forensic events such as theft.
- \* To use data storage units by taking appropriate measures to protect the data recording unit from natural disasters.
- \* Make at least two backups, one of which is cloud storage, to prevent data loss that may occur consciously or unconsciously.

### References

- Arvika Data Recovery, (2013), Monolith Database <http://odzyskiwanie-danych.com.pl/monolith-database.html>.
- DataSector, (2022), Intel SSD, <https://www.instagram.com/p/Ce0XJk6DVvH/?hl=tr>.
- Doğanay, H. A., 2019, Evaluation Of The Legal Process And The Term Chain Of Custody With Actual Difficulties Against Investigation Of New Generation Mobile Devices In The Context Of The Importance Of Mobile Device Forensics, Master Thesis, Ankara University, Department of Interdisciplinary Forensic Sciences.
- Gin, J., (2020), Reverse-engineering and analysis of SanDisk High Endurance microSDXC card, <https://ripitapart.com/2020/07/16/reverse-engineering-and-analysis-of-sandisk-high-endurance-microsdxc-card/>.
- GreyD Lab, (2015), Монолиты, <http://greydcode.com/monolith.html>.
- ITHOPE s.r.o., (2021), SanDisk SSD U100, [www.instagram.com/p/CLPYC6gj8t9/?hl=tr](https://www.instagram.com/p/CLPYC6gj8t9/?hl=tr).
- Johnson, R. and Christie, S., (2009). JTAG 101 IEEE 1149.x and Software Debug.
- ONFI Workgroup, (2021), Open NAND Flash Interface Specification 5.0. Schmidt, K.-U.
- Özdemir, A. and Gülcü, Ş., (2021), Causes of Digital Data Loss and Data Recovery Methods, 2nd International 5 Ocak Congress on Applied Sciences.
- Ozdemir, A., (2022), Investigation of data recovery methods and development of auxiliary equipment for data recovery, Necmettin Erbakan University, The graduate school of natural and applied science (Master thesis).
- RecuperoDatos.com, (2020), Monolith Memories Database (MicroSD, SD, Pendrive), <https://datarecoveryhdd.com/monolith-database-microsd-sd-pendrive-cf>.

Rflashdata.com, (2016), Monolith Flash Database, <https://www.rflashdata.com/monolith-flash-database/>.

Rusolut Sp. z o.o., (2014), BurntSD.jpg, <https://rusolut.com/wp-content/uploads/2014/03/BurntSD.jpg>.

Rusolut Sp. z o.o., (2022), Forensic analysis of flash memory using X-RAY and Logic Analyzer. PTXXI 2022 IV Konferencja Naukowa Przestępczość Teleinformatyczna XXI Wieku.

Total-Recovery, (2022), <https://www.instagram.com/p/CaYlOyRjyW0/?hl>.

### About the Authors

**Abdulkadir ÖZDEMİR** is a police officer who has been working in Cyber Crime Branch Offices in different provinces since 2012. He has a master's degree in Computer Engineering from Necmettin Erbakan University. The main areas of work are digital data recovery, installation, and management of digital evidence inspection systems, malware analysis, and digital data inspection. He continues to work on various hardware and software developments to be used in digital evidence examination and data recovery processes.

**E-mail:** [by.akozeimir@gmail.com](mailto:by.akozeimir@gmail.com), **ORCID:** 0000-0002-6992-5170.

**Şaban GÜLCÜ** graduated from the Software Engineering Department of Vienna University of Technology with B.S. and M.S. degrees in 2005 and 2006, respectively. He received a Ph.D. degree in Computer Engineering Department from Selcuk University in 2017. He is an Assistant Professor at the Computer Engineering Department at Necmettin Erbakan University. His main research interests are neural networks, optimization algorithms, and software engineering.

**E-mail:** [sgulcu@erbakan.edu.tr](mailto:sgulcu@erbakan.edu.tr), **ORCID:** 0000-0001-7714-8861.

### Similarity Index

The similarity index obtained from the plagiarism software for this book chapter is 3%.

### To Cite This Chapter:

Özdemir, A. and Gülcü, Ş. (2022). Scientific Data Recovery Methods and Solutions in Devices using Flash Memory. In S. Kocer & O. Dundar (Eds.), *Current Studies in Basic Sciences, Engineering and Technology* (pp. 258-286). ISRES Publishing.