

Scientific Data Recovery Methods and Solutions in Optics Discs and HDDs

Abdulkadir ÖZDEMİR

Konya Cyber Crime Branch Office

Şaban GÜLCÜ

Necmettin Erbakan University

Introduction

In the history of humanity from the earliest times to the recent past, the source of power; physical strength was evaluated on the basis of land size or numerical value. In today's conditions, power has become equivalent to knowledge. When we look at the world states which are called "superpowers" it is seen that one of the reasons why they are called by this name is that they have advanced technologies based on information. The concept of data is the general name given to any unprocessed raw data. Institutions, organizations, and individuals prefer digital media (HDD - SSD - flash memory, etc.) as a data storage medium, for reasons such as not occupying physical space, providing ease of access, and fast processing. Even today, it is observed that cloud storage methods are used more and more widely. As the amount of data created in daily life increases, the areas where this data will be stored will increase in direct proportion. The increase in data storage units and their widespread use will indirectly increase the possibility of digital data loss in different places, people, and time zones. The bit is the smallest unit used to store data in information systems. Bit expression also comes from the Binary digit. Data loss is mentioned when some or all of the data expected to be interpreted by the information system cannot be processed/understood. If the scaling of the bad effects of individual or corporate digital data loss is to be made; the losses of individuals due to digital data loss are generally higher in moral value, while the losses of institutions or organizations due to digital data loss are higher in monetary value. According to the IBM Security and Ponemon Institute, they have determined the costs incurred by data loss due to data breaches in the last 5 years as follows (IBM Security and Ponemon Institute, 2021):

- Average of 3.62 million USD for 419 companies in 13 countries in 2017,
- Average of 3.86 million USD for 447 companies in 15 countries in 2018,
- Average of 3.92 million USD for 507 companies in 16 countries in 2019,
- Average of 3.86 million USD for 524 companies in 17 countries in 2020,
- Average of 4.24 million USD for 537 companies in 17 countries in 2021.

When digital data loss events are examined, it is seen that data loss occurs mainly

due to exposure to various effects. These various effects are divided into software, hardware, and semi-hardware problems. Software malfunctions are cases where the required information cannot be accessed even though the digital recording medium is intact and the device containing the recording medium is also in working condition. Hardware failures, on the other hand, are the types of failures that differ according to the environment in which the data is recorded, but basically, it is used to express the situations where the data recording environment does not work (Özdemir and Gülcü, 2021). Semi-hardware failures are failures caused by software (firmware) embedded in the hardware in data recording units. In this study, software and hardware-based failures will be examined.

Data Storage Units

Data is a general name given to unprocessed pieces of raw information stored in the form of signals or bit strings carried in digital media (Durak, 2011). Data are stored in information systems in two ways: permanent (non-volatile) and temporary (volatile). Volatile memories hold data when electrical current (power) is present, they cannot hold data if power is lost. Data storage units by access options it is divided into two according to the options to offer local and remote connections. What is meant by the storage media accessed by local connection, is the access of a user to devices containing optical devices, magnetic and flash memory that can be directly connected to the motherboard of the information system. By means of a storage medium accessed by remote connection, it is possible to connect to the storage unit in an information system, either wired or wirelessly, from the local network or over the internet. The information system, which is connected via a remote connection, offers a local storage environment, considering the storage environment it offers to the user. Meanwhile, as a result of the widespread use of the internet with portable devices such as mobile phones and tablets, it has increased the use of cloud storage very quickly, as it allows it to be accessed regardless of location and time (Keskin et al., 2020). Data storage units have different features from each other in terms of connection interface, packaging/production format, and data recording technique. Digital data in storage units; magnetic, optical, and semiconductor (electronic) media are stored. Storage media containing data are classified according to certain criteria. This classification is presented in Figure 1 as an infographic. Detailed information about these storage units will be given under the relevant headings (Özdemir, 2022).

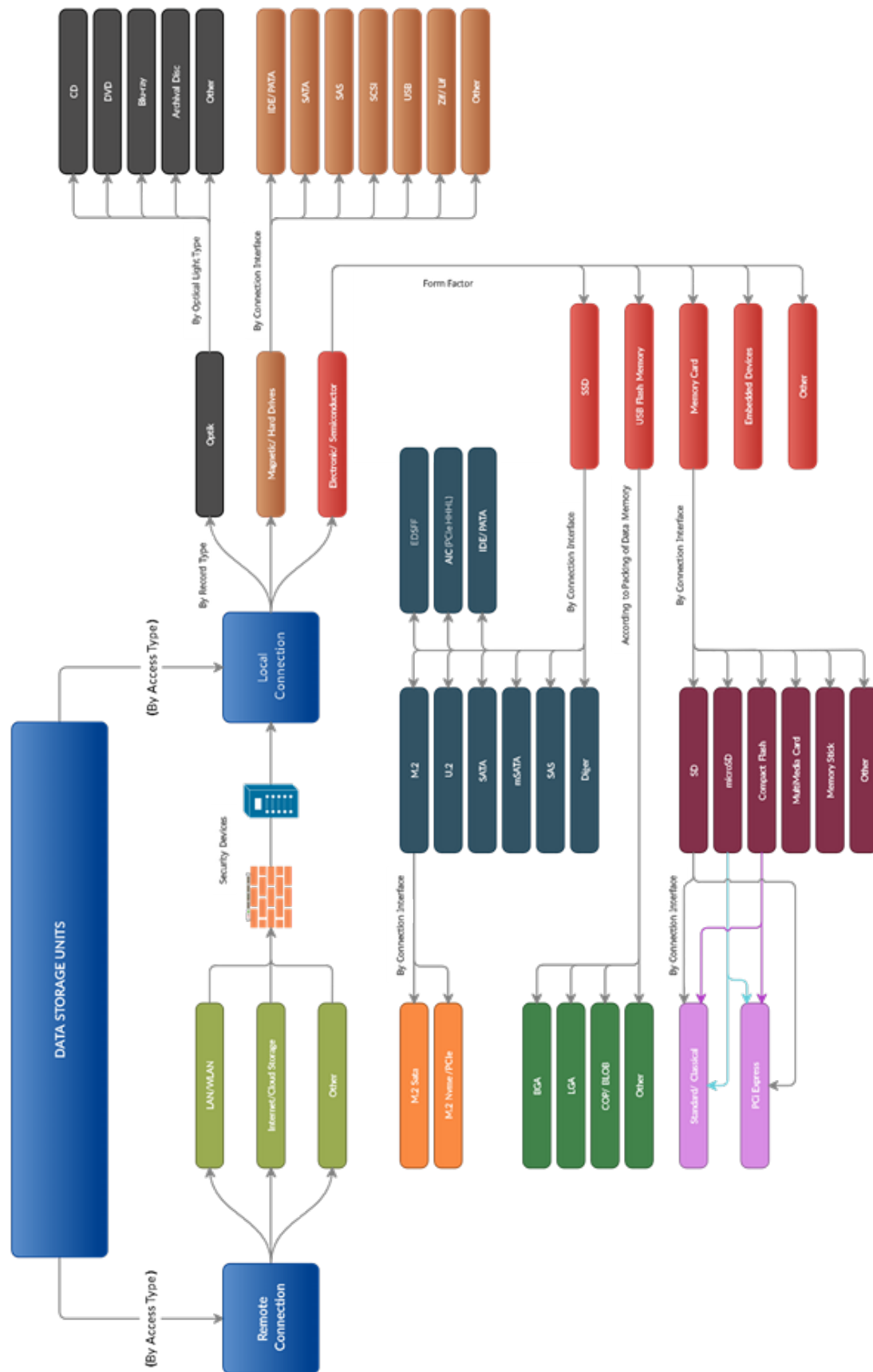


Figure 1. Data storage units and their classification

Data to Your Loss Causes of Causation and Data Recovery Methods

Data loss occurs when digital data cannot be accessed/used in normal ways for various reasons. It is also called data recovery when the reasons that cause data loss are determined and the necessary interventions are eliminated by using special hardware and software. These various reasons are generally; data hiding, deletion, corruption, encryption; breaking, burning, mechanical or electronic failure of data-hosting equipment; hardware (firmware) corruption, inability to be used by the device, etc. can be exemplified. These reasons can be natural, accidental, or sabotage. In Figure 2, the results of the research conducted by “Ontract Data” company in 2003 and “DeepSpar Data Recovery Systems” company obtained from 50 data recovery companies in 14 countries in 2007 regarding the causes of data loss are presented.

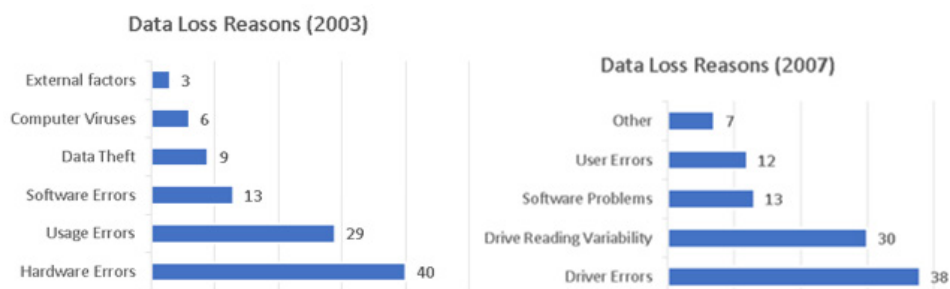


Figure 2. Causes of data loss (David, 2000; DeepSpar Data Recovery Systems, 2007))

Cloud storage or other structures (Das, Nas, San) or the problems caused by these are systemic failures, if these are ignored, data loss situations usually occur in data recording units. For example, the corruption of a disk in the device using Raid levels affects the entire structure. If the problem on this disk is resolved, the entire structure will be ready for use again. However, devices such as Das, Nas, and San offer the end user a logical space (volume) by using various parameters on the disks. If the device itself is corrupted, the data will not be accessible (except for Raid 1), since the logically presented structure will not be available. If the parameters used while creating this structure are created (simulated) software, only the data will be accessed.

Data recovery operations are subject to various classifications according to the method used or the type of digital material tampered with. The classification of data recovery methods in the literature is made according to the “cause of the failure” and “data recording technology” (Güllüce and Benzer, 2015). The main purpose during the data recovery process is to eliminate the reason why the user cannot access the data. The problems encountered in data recovery and how their solutions are carried out will be tried to be explained by using visual examples as much as possible. If the term in the solution methods is to be explained;

Raw Recovery: It is also called recovery or File carving. When the hexadecimal structure of the files in the data recording medium is examined, it is seen in Table 1 different types of files have different headers and some files have a footer in addition to the header.

Table 1. Headers and Footers of Files (Exterro Inc., 2021; Kessler, 2022)

File Extension	File Description	Signature (Header)	footer
(\$MFT)	Windows MFT Records	46 49 4c 45 30 00	
(FAT1)	FAT32 File Allocation table	F8 FF FF 0F FF FF FF 0F	
apk	Android Archive File	50 4B 03 04	
doc	MS Office Word document	EC A5 C1 00	
docx	MS Office 2007 documents	50 4B 03 04 14 00 06	
jpg/jpeg	JFIF/JPEG Image file	FF D8 FF E0 00 10 4A 46 49 46	FF D9
mp3	MPEG-1 Audio Layer 3 audio file	49 44 33	
mp4	MPEG-4 Video Files	00 00 00 18 66 74 79 70 33 67 70 35	
mov	Apple Quicktime movie file	00 00 00 20 66 74 79 70 4D 34 41 20	
pdf	Adobe Portable Document Format	25 50 44 46	0D 25 25 45 4F 46 0D
psd	Adobe Photoshop Image File	38 42 50 53	81 FF 81 FF 91 FF 81 FF F9 FF
rar	WinRAR v3 Compressed Archive File	52 61 72 21 1A 07 00 CF	
	WinRAR v5 Compressed Archive File	52 61 72 21 1A 07 01 00	
xls	MS Office Excel Spreadsheet	FD FF FF FF	45 78 63 65 6C 2E 53 68 65 65 74 2E 38 00 F4 39 B2 71
xlsx	MS Office 2007 documents	50 4B 03 04 14 00 06	
zip	WinZIP compressed archive	57 69 6E 5A 69 70	

This header and footer information, which enables files to be distinguished from each other, is called file signature. Data recovery and forensic software read/scan the data recording medium from beginning to end. During this scan, the process of recovering files or file system structures based on the signatures (header-footer) of the files and the clustering information (cluster) they use in the data recording medium is called raw recovery. If data recovery software can't access the clustering information and they didn't use sequential clustering from the files (in the fragment), the files will not be fully recovered. Therefore, the priority of the data recovery software used should be to recover the file system structures (MFT, FAT1, VBR, etc.) (Özdemir, 2022).

File-based recovery: Raw recovery is performed for one or a few files, not all files.

File repair: It is the process of removing the corruption or damage with software if the "recovered" files are corrupted or damaged as a result of raw recovery or file-based recovery.

In general, although it is tried to collect the malfunctions under certain headings, it should be known that the cause of each malfunction is different and the solutions will be different depending on this.

Software Data Loss and Solutions

Software data loss is defined as the situation where the requested files cannot be opened/viewed/used while accessing the normally working digital storage unit, where there is no physical failure.

Many users believe that their files are permanently deleted by simply moving their files to the recycle bin and then emptying the recycle bin. But there are two types of deletion. Figure 3 and we have two buttons named “button1” and “button2” on our form, after changing the text of “button1” to “Delete button2” Click Add event “button2.Visible=false;” Let’s write.

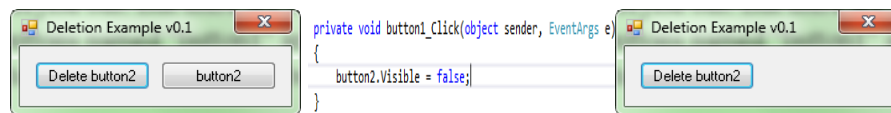


Figure 3. For the deletion example, form design, button typing is done with code and button

“Delete button2” in Figure 3 clicked, it will be seen that the button labeled “button2” has disappeared. The action done here is only to prevent “button2” from being displayed on the form. This is how the files are deleted from the computer. When a “Delete” command is given to the file system by the user, the file system provides the user with the illusion that the file has been deleted by simply making the file invisible (inaccessible) as shown above. As it can be understood, the button is not really deleted here, it is only hidden from the user, the first type of deletion is the case that it is not shown to the user while the data is still on the disk.

A question may come to mind: when files are deleted, the amount of free space on the disk increases, how would this amount of free space appear if there was no real deletion? Before answering this question, the concepts of allocated and unallocated space should be explained. In file systems, the disk areas where the user’s files are stored are called reserved space, and the areas marked as empty in the file system that the user can use to save new files are called unallocated space.

The second type of deletion is permanent deletion (wipe-data erasure) In addition to the deletion process described above, it is the process of writing FF or 00 or different hexadecimal values on the sectors where the data is located. In such cases, data recovery is not possible even if data recovery procedures are applied. Some of the software data recovery software are CDRoller, Disk Doctors, Easeus Data Recovery Wizard, File Scavenger, Flash Extractor, PC-3000, R- Studio, Recover MyFiles, Rusolut, Softcenter Image Explorer. This software can recover files that are consciously or unconsciously deleted by viruses, information system attacks or users, disk partitions damaged or deleted for any reason, file-based corruption, and data loss as a result of hardware or

system crashes. It can also retrieve deleted data and configuration information from RAID disks.

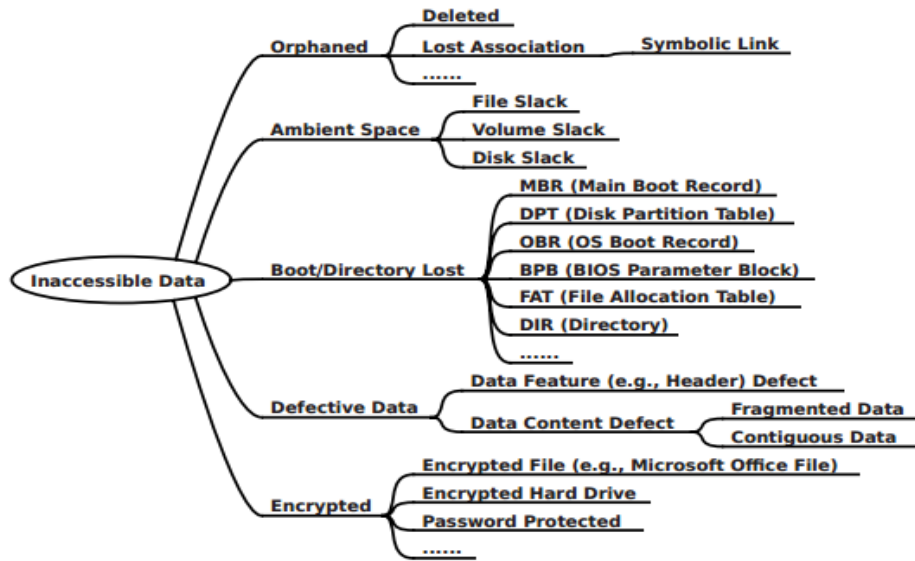


Figure 4. Classification of data according to inaccessibility (Guo and Slay, 2010)

If the software problems and their solutions are exemplified, the following examples can be given;

- * Corruption of the file system, the deletion or corruption of the files of the filing system, and the inaccessibility of data and files as a result of the disk becoming Figure 5).

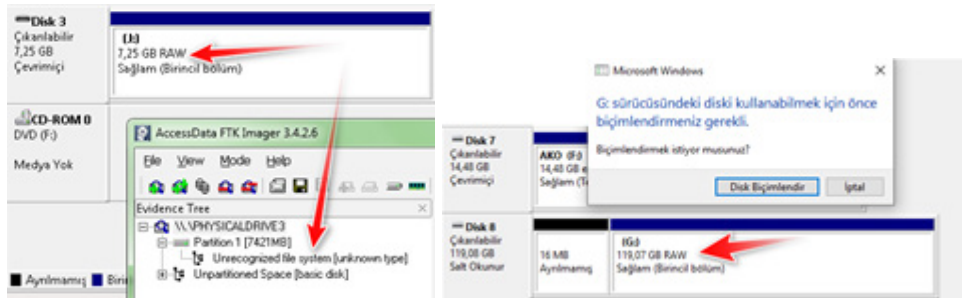


Figure 5. Device instances with a RAW file system

- Raw with data recovery software to access data on drives in this state Recovery or file type-based scanning is required. As an alternative method, try again to access the drive with a Unix-based operating system. The chkdsk commands should not be used without a forensic copy/image of the device.
 - This problem is usually caused by static electricity, care should be taken when connecting data loggers to the computer system.
- * If the drive letter cannot be assigned to the drive by the operating system, the operating system cannot logically show the drive to the user:

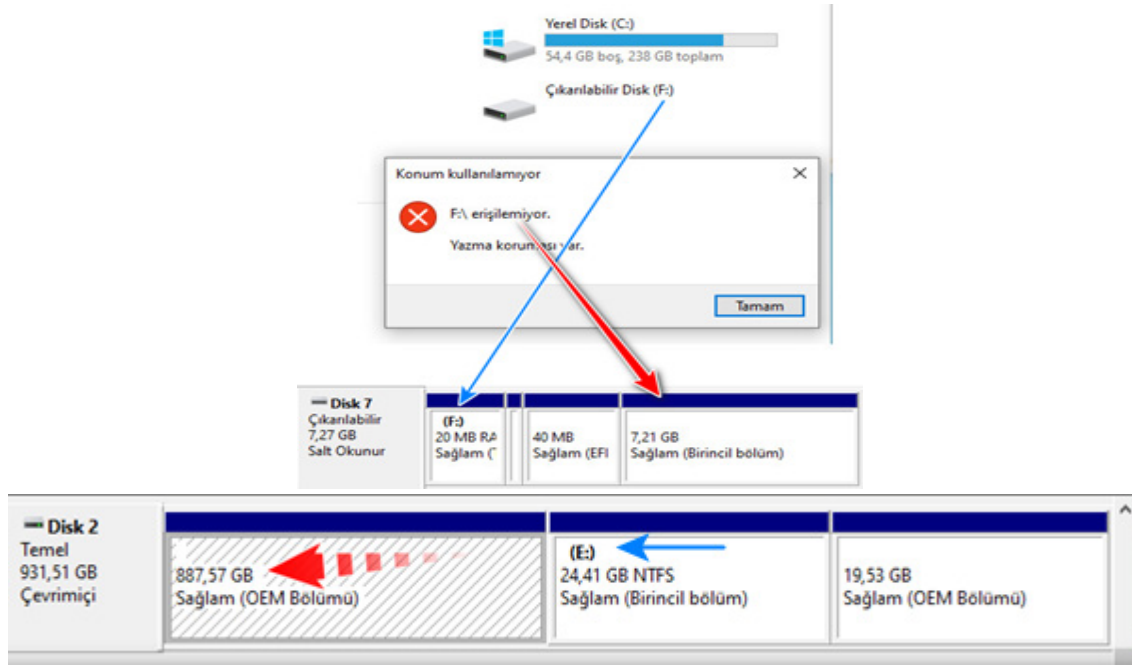


Figure 6. Examples of devices that cannot be assigned a drive letter

- The solution is provided by assigning drive letters to the drives in this situation from the disk management.
- * Encryption of the data recording medium: It can be done deliberately by the user (BitLocker, FileVault, TrueCrypt, etc.) as well as the measures taken to protect the devices themselves from unauthorized access.

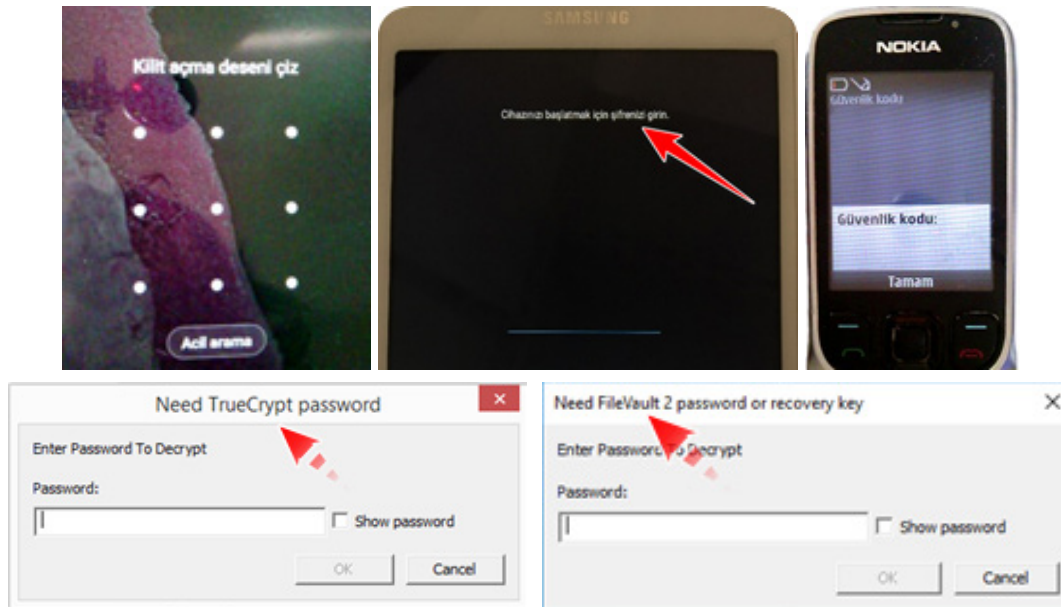


Figure 7. Encrypted device examples

- * The surest way to recover data from devices in this situation is to learn the password. If it is not possible to learn the password;
- Manual password attempt
 - Special software used (Passware Kit Mobile, PC-3000 Mobile, Cellebrite Ufed 4PC, Oxygen Forensics, Magnets By means of

Axiom, etc.) the pattern should be skipped/deactivated or closed physical forensic copy should be taken,

- Again, with such software, a brute force (brute-force) attack should be done.
- * Crashing during updating of operating systems or for any other reason:

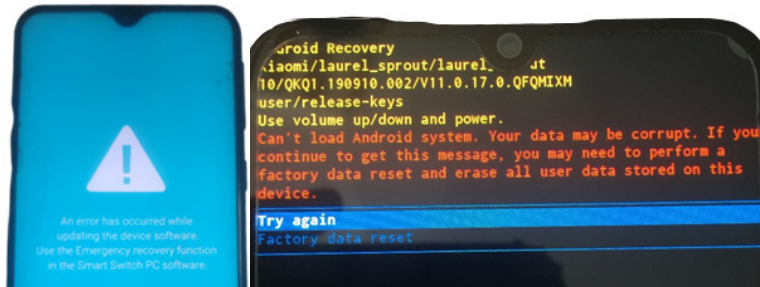


Figure 8. Examples of devices crashing during OS update

- * If the device used by the hardware in this situation is a computer, the data can be safely recovered by inserting the disk in the device into a different computer system. There are passwords set in Windows user accounts that do not prevent data recovery or access, data can be accessed by connecting a storage unit to a different computer.

If the device is a mobile device;

- Stock rom loading,
- Taking a physical copy of the device with forensic software,
- Recovery options offered by forensic software can be used.
- * Partition table corruption: These tables are corrupted due to sudden voltage changes, power cuts, etc.

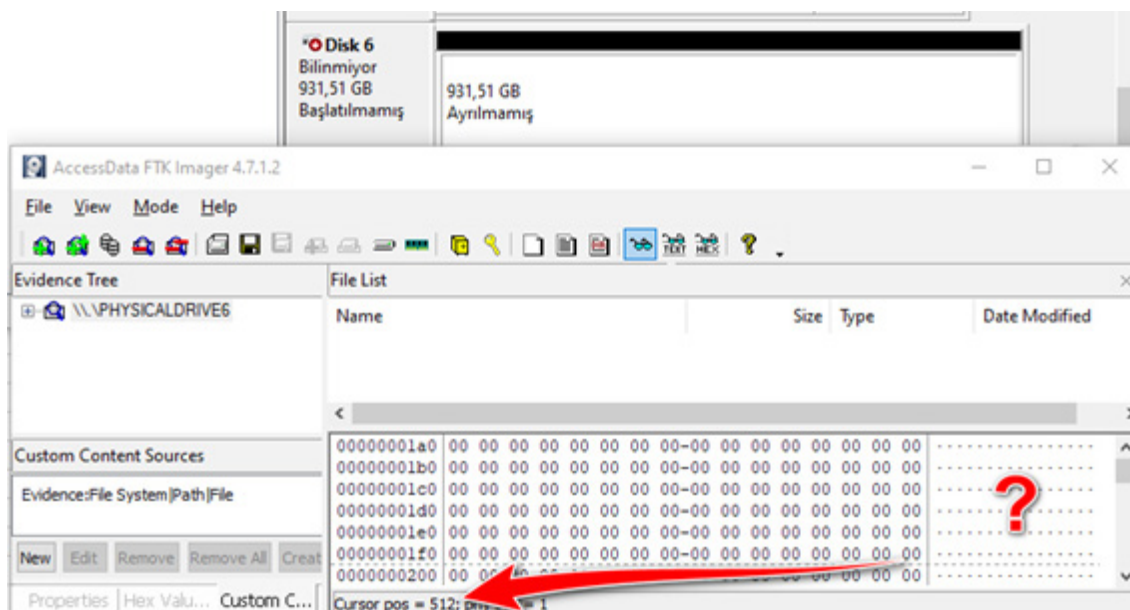


Figure 9. Partition table corrupted disk

- Raw with data recovery software to access data on drives in this state the file

system structures should be found by recovering. Or file-based recovery should be done.

- * During data recovery, the files do not come completely or not at all due to the scattered (fragment) records on the disk: As can be seen in Figure 10, it is seen that the first of the “recovered” files consists of 4 parts, and the other photo can be recovered in half.

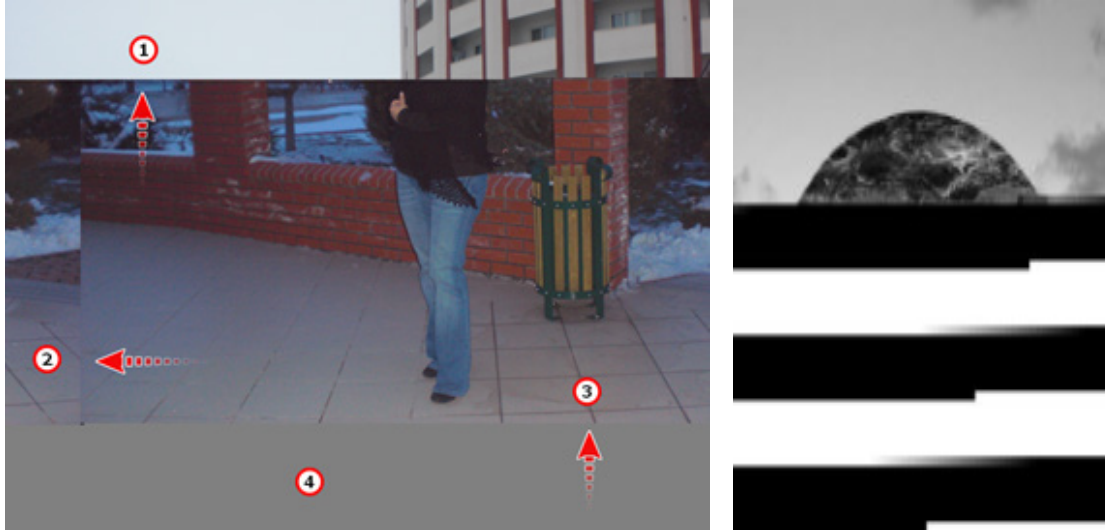


Figure 10. Fragmented files not coming in full

- That the software in which this process is performed recovers the file system structures and recovers the files on the disk hierarchically (tree structure) over it, or it is necessary to try alternative software.
- * File corruptions: deliberate or accidental power cuts during file operations (move, copy, delete), not using the remove hardware option.

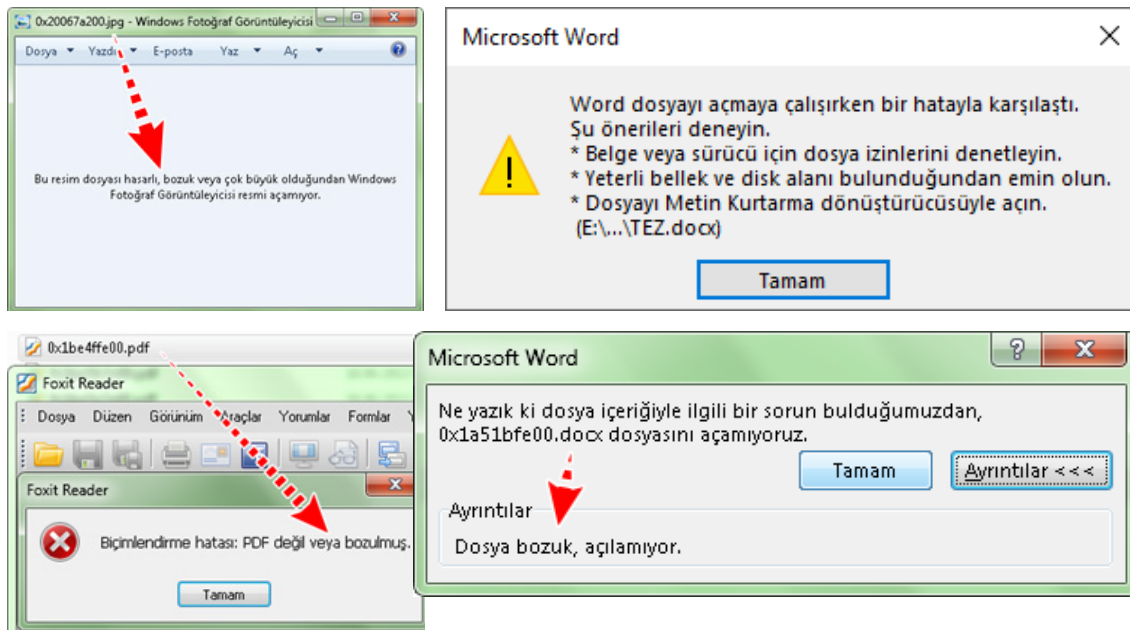


Figure 11. Examples of corrupt files

- If the methods described in Figure 10 cannot be obtained, a positive result can

be obtained as a result of searching the temporary (.tmp) files created according to the file type (such as automatic save for office files) if an automatic backup is made while working with the relevant file on the computer. If the positive result is still not achieved, file repair (corrupt file repair) software (eg S2 Recovery Tools) should be tried on the recovered file. In Figure 12, pre- and post-repair images of a broken video part are presented.

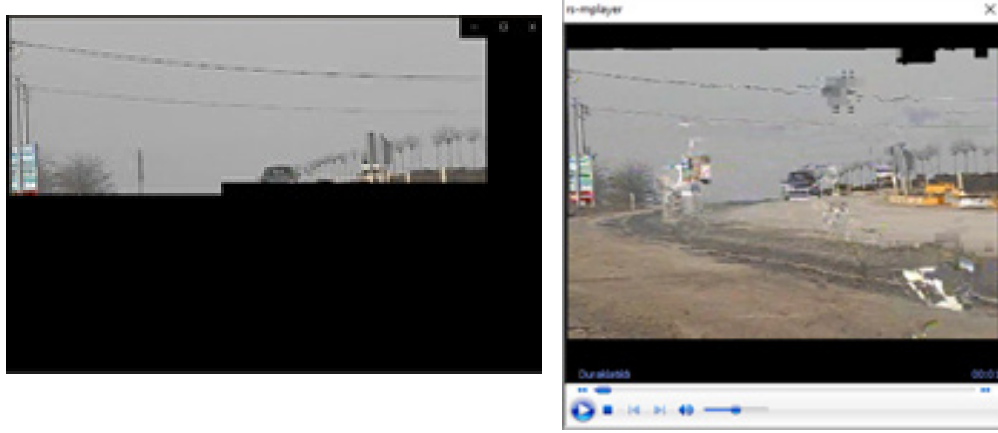


Figure 12. Repaired video example

- * Intentional encryption of files or encryption by viruses (ransomware):

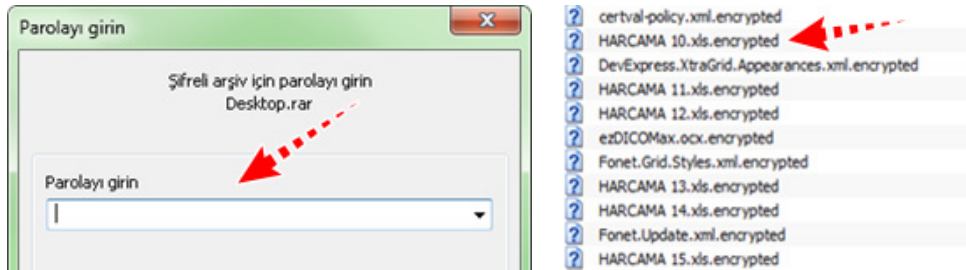


Figure 13. Encryption on files

- The surest way to recover data from files in this situation is to learn the password of the file. If it is not possible to learn the password, a brute force attack should be made by means of special software (Passware Kit Forensic, Hashcat, John the Ripper, etc.) If it is a Ransomware attack, developed software should be used to decrypt this Ransomware (MalwareHunterTeam, 2022; No More Ransom, 2022) or shadow copies (Shadow Copy - ShadowExplorer) should be used.
- * To access data as a result of burning the motherboard of the Nas device:



Figure 14. Inability to access data due to corruption of Nas device

- After detecting the Raid level on the Nas device (Raid0), software that can create software Raid in the computer environment (PC-3000 Express RAID System, UFS Explorer, Raid Reconstructor, R - Studio, Softcenter the build must be rebuilt with Raid Explorer, etc.).
- * Permanent wiping of data by users or viruses:
- * In such a case, data recovery is not possible.

Hardware Data Loss

In the previous titles, the software and hardware structures of data storage units were mentioned in detail. The mentioned components ensure the healthy operation of the data storage unit. If one or more of these components fail, the device will not work and data will be lost.

Hardware data losses; These refer to the situations in which the data recording unit does not work in any way as a result of exposure to natural disasters (earthquake, flood, landslide, fire), environmental factors (electrical fluctuation, static electricity, electromagnetic effect) or sabotage (throwing into acid, crushing, breaking, throwing into water). In short, it refers to all kinds of internal or external factors that will prevent the operation of the data recording medium. The aforementioned factors that the data logger is exposed to may have developed in accordance with the natural flow of life or may have been consciously carried out by a user or a cybercriminal. According to Figure 2, hardware data loss is seen as a 40% and 38% problem.

Data Loss in Optical Discs (Media) and Solutions

Since recording discs using optical write-reading technology do not have any casing or frame to protect them from external factors, they can be easily damaged.

Before moving on to the solutions, let's explain the terms to be used in the solutions:

Intervention With Electron Microscopy: It is to obtain a data stream from the images obtained from the scanned parts of an optical disc using an electron microscope, and then to interpret the data obtained with software specially developed for this work

(Jarolim, 2016).

Tagging Intervention: It is the fixation of the cracked part of an optical disc with a crack with a paper tape or label. The point to be considered here is that the adhesive property of the tape or label to be used should not be too strong. Otherwise, the coating of the pasted surface may be removed.

Filling Process: It is the use of specially developed optical disc cleaning and filling devices (Disc Body) to fill the scratches on the surface if it is deeply scratched on the optical disc.

Sanding Process: If there are not very deep scratches on the optical disc, these parts can be moistened and the data can be accessed by gently rubbing with very fine sandpaper (2000+) without causing new scratches.

Intervention With a Laser: The damaged part of the broken optic disc is cut with a laser from the broken places. Subsequently, a piece of a solid blank optical disc of the same size is laser cut and replaced with the slice removed from the previous optical disc. It should be adhered to the reflective face to reflect the light. It should be noted that there is no residue and level difference (Kara, 2013).

Heat Treatment Application: If the optic disc has taken a concave shape, a device (LCD Screen) capable of applying heat treatment and vacuuming an optical disc is placed on the separator. It is to wait for the optical disc to take its original shape by placing a suitable weight on the optical disc.

Cleaning Process: If the reading side of the optical disc is dirty, it is the process of first cleaning the solid dirt on it by holding it under water and then cleaning the sticky or water-removable dirt on it with isopropyl alcohol or cologne with the help of a cotton ball.

If the hardware problems specific to optical discs are to be exemplified;

- * If the surface of the optical disc is dirty:



Figure 15. Dirty and cleaned optical disc surface

- The disc surface should be cleaned.
- * Cracked optic disc:



Figure 16. A crack in the optic disc

- Cleaning and labeling processes should be applied to the disc surface.

* Fracture of the optic disc:



Figure 17. Fracture of the optic disc

- Disk surface cleaning and laser intervention should be done.

* Light scratches on the optical disc:



Figure 18. There are light scratches on the optical media

- The disc surface should be sanded and then cleaned.

* Having deep scratches on the optical disc



Figure 19. Having deep scratches on the optical disc

- The disc surface should be filled and cleaned afterward.

* Error during data recording to optical disc



Figure 20. Error during data recording to optical disc

- Data recovery should be attempted by trying alternative brands of optical disc readers.

* Wear of the reflective surface of the optical disc



Figure 21. Wear of the reflective surface of the optical disc

- The worn dimple should be covered with a material that will reflect light.

* Optical laser burning of the optical disc



Figure 22. Optical laser burning of the optical disc

- Data recovery should be attempted by trying alternative brands of optical disc readers.

* Distortion of the physical shape of the optical disc



Figure 23. Example of a physically deformed optical disc

- Heat treatment should be applied.

In cases of overwriting or deleting the unlogged optical media, software data recovery operations should be performed by making a logical copy of the optical media. In addition, in case the optical disc is not recognized by the optical disc reader, alternative brand optical disc readers should be tried and data recovery should be tried.

Data Loss and Solutions on Hard Drives

Data loss for hard drives; Printed circuit board failures, electronic components on the printed circuit board, motor malfunctions as a result of the disc being kept unused/ forgotten for a long time, deformation in the flex cable that provides the motor power connection, the pad available for the read/write heads on the printed circuit board to perform their necessary functions. Dirt/abrasion of the 's, scratches/scrapes on the

surface (platter), not being able to read the modules as a result of firmware (firmware) failure, inability to function as a result of contamination of the read/write heads, sticking of the read/write heads to the disk plate (platter), breakage of the read/write heads, etc. occurs in such cases (Schroeder and Gibson, 2007).

Before moving on to the solutions, let's explain the terms to be used in the solutions:

Repairing The Device: It refers to the normal operation of the device by eliminating the software or physical malfunctions that prevent the data recording medium from working normally.

Donors: The basic components (printed circuit board, hard disk assembly) that make up a data recording environment and one or more of the parts that make up the subunits of these components (electronic components on the printed circuit board, read/write head, engine) are compatible and healthy working data. It is the process of taking the defective data from the recording unit to the recording unit. Data logger manufacturers (except Seagate) do not perform data recovery operations other than production. Therefore, there is no valid method/recipe to find a 100% compatible donor for the data registers. There is no publication or documentation of the manufacturers on this subject. Instead, documentation or blog posts published by data recovery companies and companies selling data recovery tools are used, but the criteria shown are not met. It is also stated that there is no 100% guarantee of finding a donor. The best donor device is exactly the same except for the serial number.

Donor Search for The Printed Circuit Board (PCB): If the power connection of the disc is made and no sound or movement is felt from the disc, it is considered as the source of the fault. Donor search should be done by finding the relevant number on the card and searching for the donor card according to that number (Donor Drives LLC, 2012). Example card numbers according to brands are presented in (HDDZone, 2010). As can be seen from the examples, PCB numbers are in different standards and locations according to brands. An alternative method is to search for donors by identifying the manufacturing family of the hard disk (Figure 25). In addition, when the donor of the defective printed circuit board is found, it is often not sufficient to replace the cards directly. The chip on the card must also be carried in the rom, which contains the hardware software (firmware) that ensures the healthy operation of the hard disk. If there is no physical defect on the PCB, no sound is heard from the disc and no movement is felt, the source of the fault is the PCB.



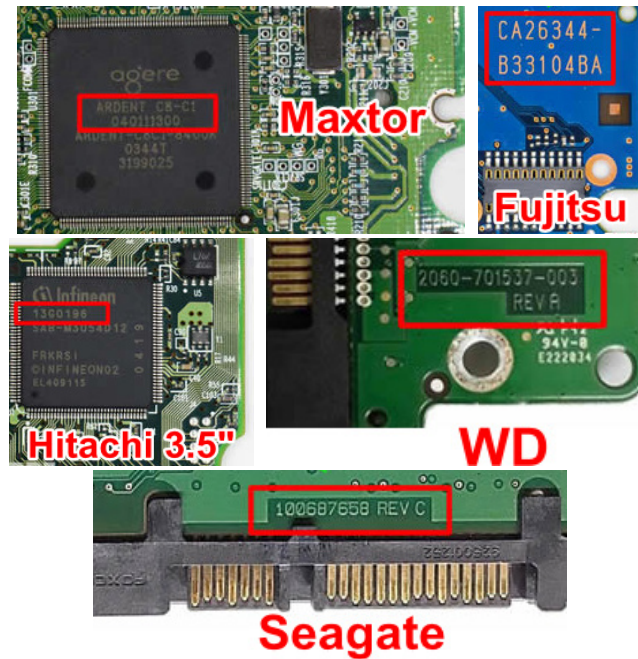


Figure 24. Criteria to be searched according to PCB brands

<i>Western Digital</i>		
Minimum PCB requirements	The middle characters in the second part of the model information. These characters indicate the family information to which the disc belongs. (Family ID)	WD6400AAKS-65 A7 B0 WD10TMVW-11 ZSM S1
<i>Seagate (Barracuda / F3 Mimarisi)</i>		
Minimum PCB requirements	Seagate brand drives produced before 2008 were produced with this architecture. There is no need to change ROM on these discs. Most likely a chip transfer will be required.	ST9640320AS ST31000528AS
<i>Toshiba</i>		
Minimum PCB requirements	Chip Transfer is required in most cases.	MK3265GSX MK1017GAP
<i>Samsung</i>		
Minimum PCB requirements	Chip transfer / swap or similar services may be required for new models.	HA250JC HM120JI SV0602H

Figure 25. Compatibility criteria for PCBs (Güllüce and Benzer, 2015)

Donor Search for Read/Write Heads and Motor: Although it is the easiest type of malfunction to detect, it is the most difficult compared to other types of malfunctions due to the highest level of operation sensitivity. This is because the read/write heads work very close to the platter. The main symptom is unusual noise from the disc. If there is such a malfunction in the disc, it is the sound of “squeaking”, “click- knock”, and “pop-pop” when the power is supplied to the disc. These sounds vary according to the brand and model of the disc and the type of malfunction (head sticking, head breaking, etc.). These sounds created by the discs are cataloged according to their brands and types, from the website of the Hdd Guru community ([files.hddguru.com/download/Hard Disk Clicking Noise/](http://files.hddguru.com/download/Hard-Disk-Clicking-Noise/)) can be listened to. In cases where there is no sound but no data can be received, to test whether the heads are sound or not, they should be connected to advanced hardware that can send disc manufacturer-level signals regardless of the operating system, and through the software of these hardware (Atola, Deeppsar,

Dolphin Data, MRT Lab, PC 3000, Salvation Data, etc.) should be tested with head test commands. Sometimes it may not come at all. In addition, sometimes these sounds can occur when an incompatible PCB is attached to the disc.

Donor for printed circuit board Similar to the criteria, a donor compatible with the defective disc is sought. It is shown by coloring on the photographs of the discs that the criteria are higher than on the printed circuit board. Donor Example discs with marked criteria are presented in Figure 26.

RED – Strictly required.

ORANGE – High priority.

YELLOW - Medium priority.

GREEN - Low priority.



Figure 26. Donor sample discs with marked (Donor Drives LLC, 2012)

Also, one of the best ways to find a good donor is to look at the preamp for Seagate and the microjog for WD. However, this is very difficult to do because it does not have the software and hardware to enable end users to see these values.

Preamp/microjog values match, there's a good chance the heads are compatible. When you give the command "ctrl + l" (L) from the terminal for Seagate or "View Rom Info"

for WD disks, many values on the ROM will be displayed about the disk. One of them is the Preamtype value. For Seagate, for example, these values are “CC 16” or “B2 03” or “CA 05”. To be a donor, at least the first two characters must match.

Head changes are in a dust-free clean room (clean room) cleaned with HEPA filters. It is performed by moving the head from the healthy disk to the defective disk in special areas called room). Special equipment is used for these changes.



Figure 27. Outer parking head replacement

To SATA Convert:

In hard disks with USB interface;

- The disc cannot be recognized by computers when power is on,
- Failure to fix the faults in the data paths with socket replacement,
- More commands can be run through the Sata interface,
- Since data recovery software (PC-3000, MRT, etc.) used with advanced data recovery hardware needs a Sata connection interface to send basic level commands such as ATA and PIO, disks must be converted to a Sata interface.

There are two ways to access USB disks with the Sata interface:

By looking at the production diagram (datasheet) of the controller, after determining which of the paths to the controller are Sata buses, the first method is to solder those paths to the SATA socket. Soldering operations should be done from the back of the capacitors at the input of the USB - SATA bridge circuit, according to the bus outputs, as shown in Figure 28 for the electrical connection, after the USB cable is attached to the PCB, the multimeter is brought to the diode mode (buzzer). After one end of the probe is touched from the USB cable end to the 5V pin, it is determined which point it corresponds to on the PCB. When the same process is done in the ground connection, the electrical pins on the PCB are also detected.

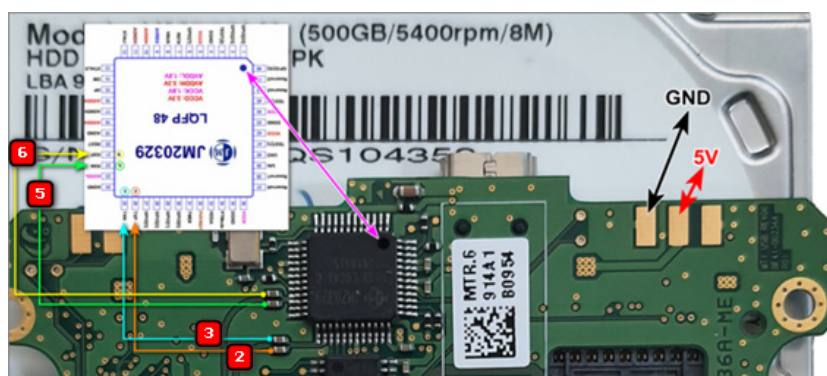


Figure 28. Soldering points when converting USB disk to Sata

To move the rom or replace it with a compatible PCB by writing the rom data. The list of compatible PCBs that can be used for Toshiba, Samsung, and WD brand USB disks is presented in Table 2.

Table 2. USB and SATA PCB Compatibility List (ACELab Europe s.r.o., 2014; Jared, 2016a; 2016b)

	USB PCB No	Sata PCB No.			USB PCB No	Sata PCB No.
SAM-SUNG	100725482	100720903			701605	701499
	100760718	100720903			701615	701499
	100740633	100739392			701635	701572
	100765396	100767980			701650	701499
	BF41-00300A	BF41-00306A			701675	701672, 701609, 771672
	BF41-00365A	BF41-00354A			701737	771692, 771692
	BF41-00373A	BF41-00354A			771754	701692
	BF41-00325A	BF41-00315A			771754	701692, 771692
	BF41-00357A	BF41-00315A			771761	771692
	BF41-00282A	BF41-00249B			771801	771823
	BF41-00311A	BF41-00315A			771814	771820
	BF41-00231B	BF41-00157A			771817	771820
					771859	771852
TOSHIBA	G3448A	G003235B, G003235C		WESTERN DIGITAL	771939	771959
	G003309A	G003235B, G003235C			771949	771959, 771939
	G003296A	G003138A, G003235C			771961	771960, 771933, 771939, 771959
	G003250A	G003138A			771962	771931, 771959
	G003054A	G002825A			771964	771983
	G3959A	G3918A			800038	800025
	G003189A	G003138A			800041	800022
	G4330A	G4311A			800067	800065
	G0034A	G4311A			800069	800066
	G0039A	G4311A			810003	800065
	G003296A	G003138A			810012-000	800022-002
	G003309A	G003235B				
	G3711A	G3235C				

SSDs with M.2 or other interfaces to convert to Sata, special converter cards must be used as presented in Figure 29.



Figure 29. SSD conversion cards with (Acelab Europe s.r.o., 2022)

The following examples of hardware problems for the hard disk can be given;

- * Contamination of pads to motor or read/write heads:



Figure 30. Contamination of pads going to a motor or read/write heads

- Related pads fiberglass should be cleaned with a pencil or eraser.

- * Breaking the hard disk bus:

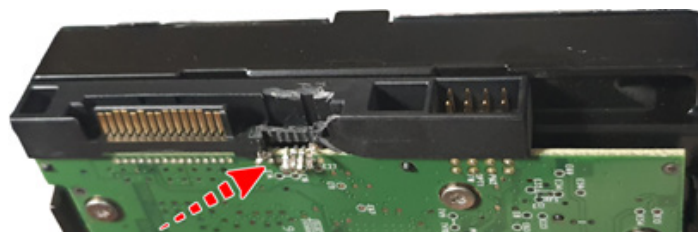


Figure 31. Breaking the data path

- The PCB can be changed (with the rom) as well as only the temporary connections to the buses can be soldered.

- * Breaking of circuit elements from PCB:

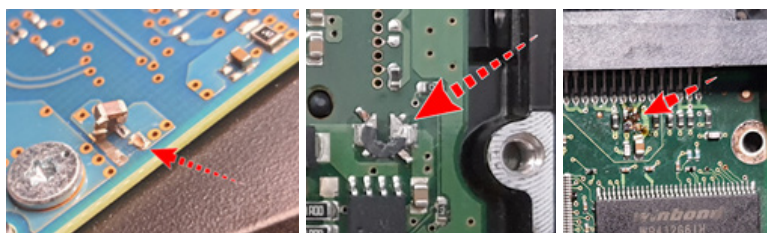


Figure 32. Breaking of circuit elements from PCB

- If the part can fulfill its function, it should be soldered, if it cannot fulfill its function, the donor should be provided.

- * Loss of function of parts on the PCB:

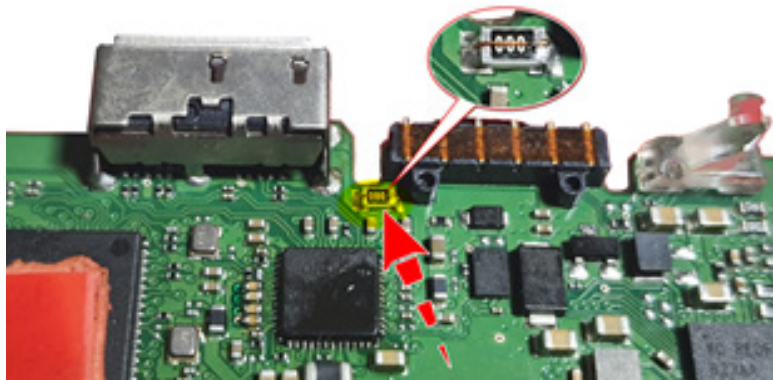


Figure 33. PCB with broken fuse resistor

- It is necessary to eliminate the malfunctions of the electronic parts on the PCB. Figure 33 how to bypass the fuse resistor using a jumper to repair it.

- * Path break in PCB:

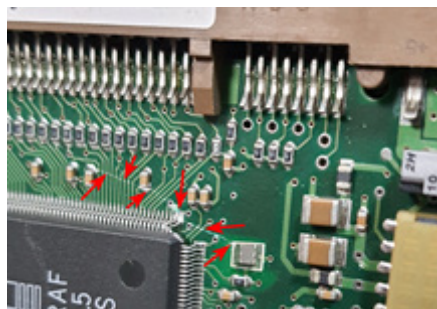


Figure 34. Example of path break in PCB

- If the PCB can be repaired, it should be performed using jumpers, if it is beyond repair, the PCB should be replaced by obtaining a donor.

- * Crushing PCB or HDD metal case:

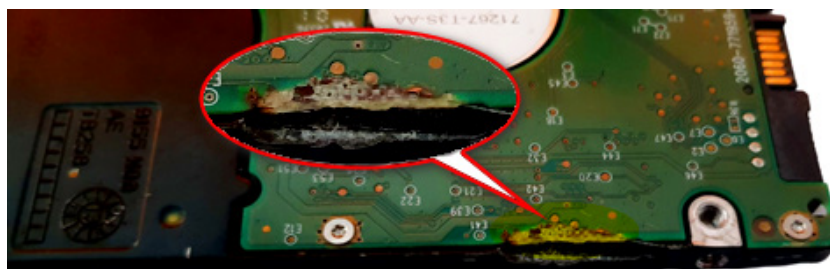


Figure 35. Crushing PCB or HDD metal case

- The donor should be obtained, the ROM should be moved and the PCB should be replaced.

- * Combustion of parts on the PCB:

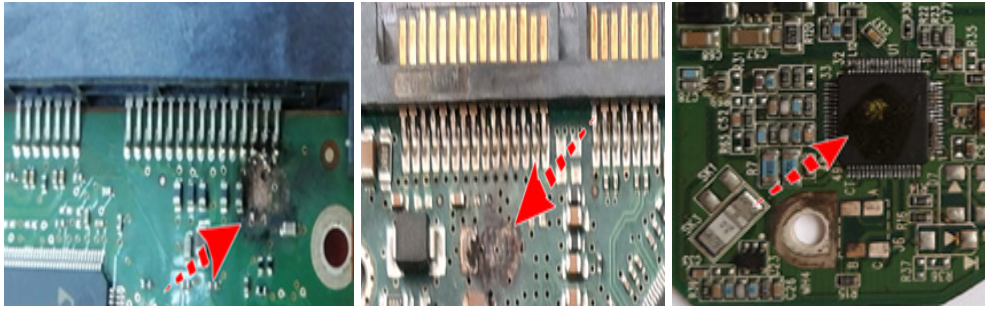


Figure 36. Part burn-in on PCB

- The burnt part(s) should be replaced by obtaining a donor. TVS diodes often burn out due to sudden voltage changes.

* Pin to the motor not touching the pad:

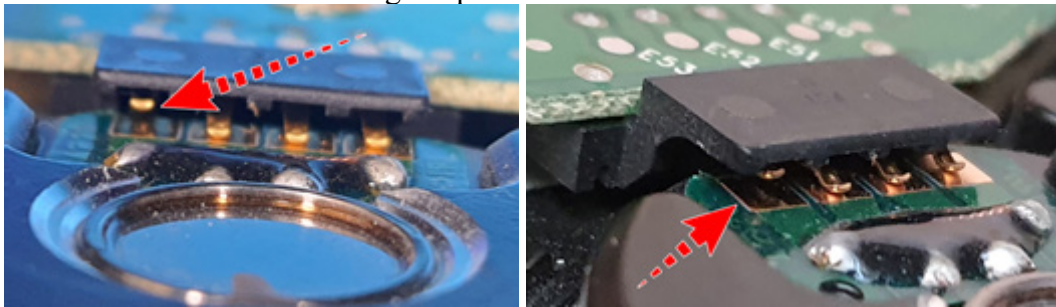


Figure 37. Pin to motor pad contact

- The pins pad should be touched.

* Failure of read/write heads:

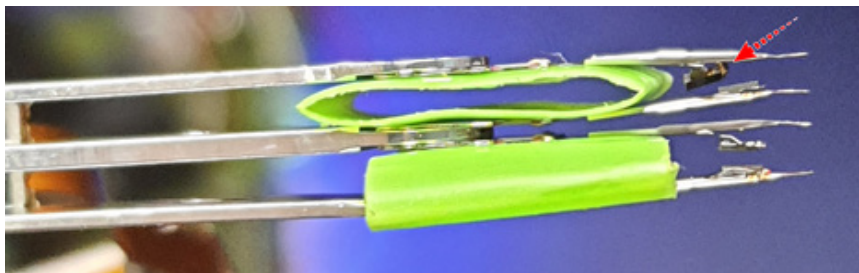


Figure 38. Failure of read/write heads

- A donor read/write head should be used.

* Formation of internal path break in PCB as a result of crushing:



Figure 39. Internal path break in PCB as a result of bending

- The donor should be obtained, the ROM should be moved and the PCB should be replaced.

* Loss of read/write head:

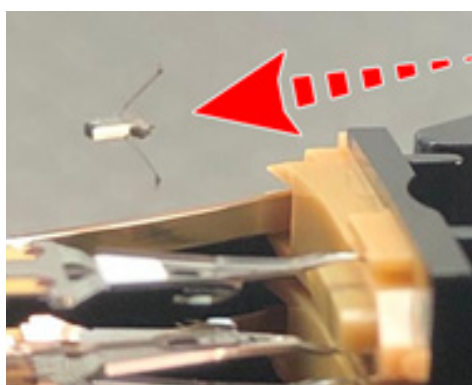


Figure 40. Break of read/write head to the platter

- A donor read/write head should be used.

* Hard disk USB socket clogged:

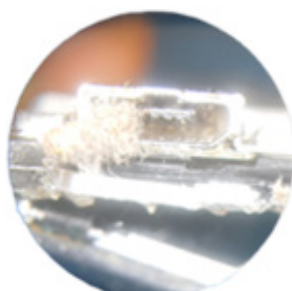


Figure 41. The hard disk USB socket clogged

- The socket must be cleaned.

* Sticking of read/write heads:

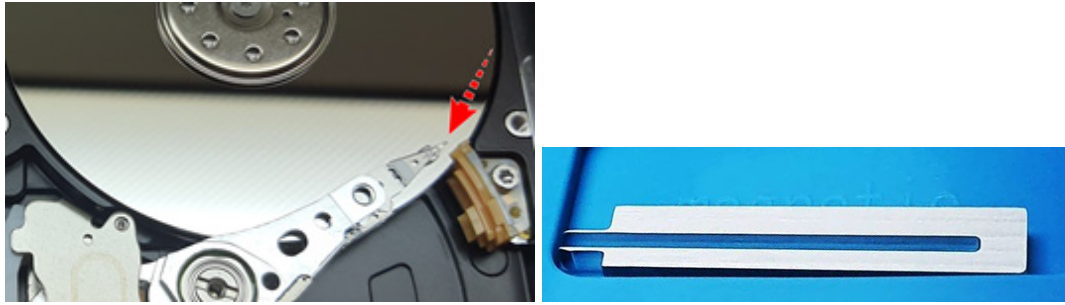


Figure 42. Adhesion of read/write heads and head spacer

- Head snapping/sticking is usually caused by the absence of airflow, or the motor not turning. Head sticking also occurs when a circuit element on the PCB is electrically burned. Sticking heads should be transported to the park using the head spacer presented in Figure 42. An alternative and risky method is to pull the read/write heads to the park by turning the read/write head clockwise while the platter is turned counterclockwise.

* Breaking of the power cables to the motor:

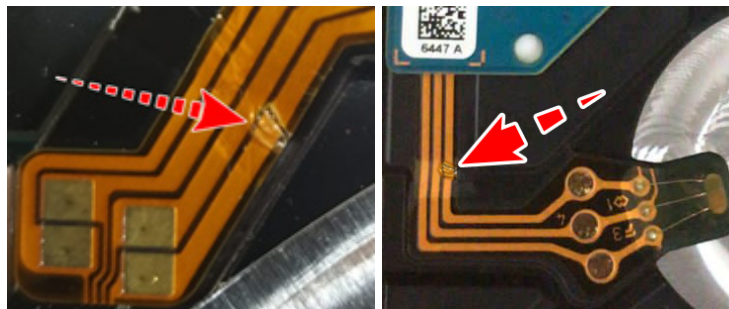


Figure 43. Breaking the power cable to the motor

- The power cable must be soldered or soldered with a jumper.
- * HDD with scratched plate and broken read/write head

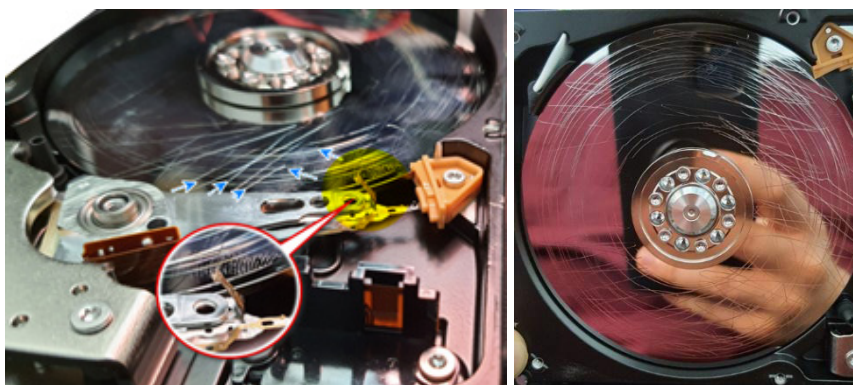


Figure 44. HDD with scratched plate and broken head

- Heads should be replaced by obtaining a donor, and data from the lower surface of the scratched plate and other plates should be tried.

* Contamination of read/write heads

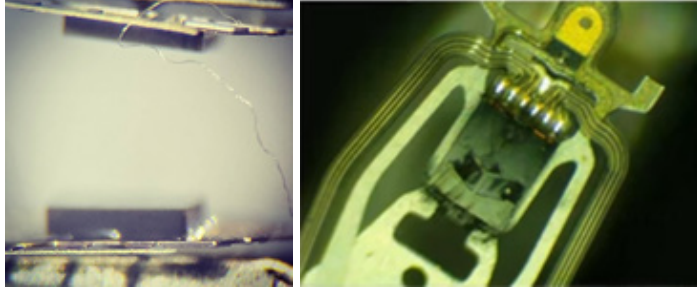


Figure 45. Contamination of read/write heads (Tri-State Data Recovery & Forensics LLC, 2020; ACELab Europe s.r.o., 2021)

- A donor read/write head should be used. As an alternative and risky procedure, it can be cleaned with isopropyl alcohol under a microscope.
- * The disc is exposed to a natural disaster or sabotaged:



Figure 46. Hdd inside burnt DVR device

- If the heat did not affect the plates of the disc, the plates and rum should be transported by obtaining a donor.
- * Unable to access the disk from the USB interface:

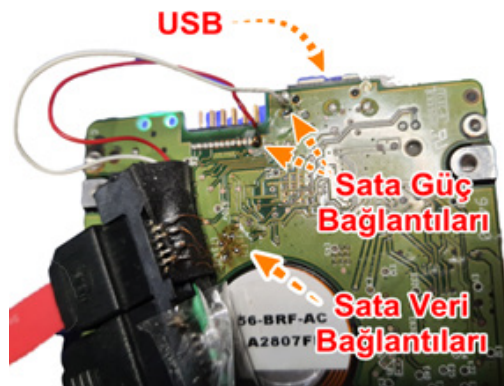


Figure 47. Example of SATA bus made to disk with bad USB socket

- Compatible Sata PCB must be used or converted to Sata.
- * PCB that will block/redirect the electric current:



Figure 48. Presence of materials that will block the electric current in the PCB

- Relevant material needs to be removed from the PCB.
- * Local scratches on disc platters:

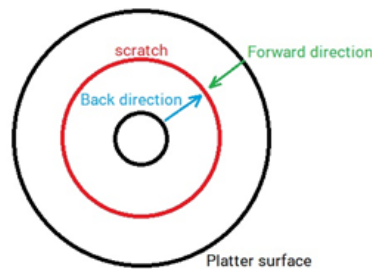


Figure 49. Presence of materials to prevent electric current in (Acelab Europe s.r.o., 2018)

- In the parts where there is regional scratching (red line), a forward reading should be started from the first sector of the disk via the data recovery software, and a backward reading should be made from the last sector of the disk when the parts with regional scratching come. In this way, the scratched region will be skipped and the heads will not be damaged during reading.
- * Intervention by non-specialists:

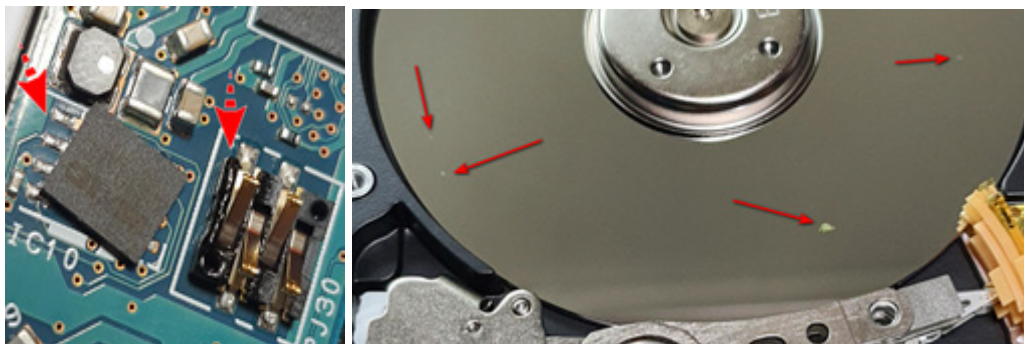


Figure 50. Intervention by non-experts

- If the intervened parts are still intact, the operation of the device is done correctly, if the parts do not work, a donor should be obtained.
- Intentional breakage of the printed circuit board:



Figure 51. Intentional breakage of the printed circuit board

- Donor printed circuit board must be provided, and the rom on the original board should be moved to the donor board.

* Physical damage to the disk



Figure 52. Physical damage to the disk (Recovery HDD, 2018)

- If the platters of the disc are not damaged, the platters should be moved to the donor disk.
- Failure of the motor to rotate the plates:
 - PCB of the disc and there is no audible sound, if the disc does not rotate despite the power supply, it is necessary to talk about a motor failure. It occurs when the engine oil in old-generation hard drives that have not been used for a long time loses its function. If the engine is heated with a hot air gun, the engine oil will regain its former functionality. Alternatively, the platters should be moved to a donor hard disk.

After the data recovery processes from 190 optical devices, which we performed on optical media and whose detailed information is given in Table 3, it was observed that data was recovered from 146 of them and data could not be recovered from 44 of them.

Table 3. Optical Disk Data Recovery Research Results

Problem	Type	Number of Optical Discs	Action Taken	Is data recovered?
Unable to copy files	CD	6	File-based forensic copying	Yes
	DVD	18		

Crack	CD	1	Labeling	Yes
Lightly scratched and stained	CD	22	Cleaning	Yes
	DVD	12		
Moderate scratches and stains	CD	29	Filling and Cleaning	Yes
	DVD	24		
Deep scratch	CD	5	Sanding and Cleaning	Yes
	DVD	8		
Deformity	CD	1	Heat treated	Yes
	DVD	2		
Unable to Read Data	DVD	18	Reading with a different reader	Yes
Broken	CD	5	Cleaning, Sanding, Filling	No
	DVD	2		
	Blu-ray	4		
Reflective part removed	CD	6		
	DVD	4		
Very deep scratch	CD	1		
	DVD	6		
Coated with glue	CD	11		
	DVD	5		

The detailed information of 338 data recovery processes that we performed on hard disks and solid state disks is given in Table 4. 137 of them are hardware problems. 29 of them are hardware and semi-hardware problems. 23 of them are hardware and software problems. 86 of them are semi-hardware problems. 2 of them are semi-hardware and software problems. It has been observed that 61 of them are software. During the 338 data recovery processes we performed, when the methods described above were applied, it was observed that 284 data were recovered.

Table 4. Types Of Failures Encountered In Data Recovery Operations

Fault Type	MOQ
Hardware	137
Hardware and semi-hardware	29
Hardware and software	23
Semi-hardware	86
Semi-hardware and software	2
Software	61
Total	338

Table 5. General Data Recovery Status

Situation	MOQ
Data recovery done	284
Data recovery not possible	54
Total	338

Table 6. Data Recovery Only in Hardware Failures

Situation	MOQ
Data recovery done	79
Data recovery not possible	54
Total	133

Table 7. Types of Hardware Failures by Brands

Brand/ Fault Type	HGST	Hita- chi	Ki- oxia	Sam- sung	Sea- gate	Sk Hy- nix	Toshi- ba	WD	To- tal
Head failure	2	4		13	29		5	21	71
Head weakening				4	9		3	5	21
engine failure				1	5		4	1	11
PCB failure	1		1	6	9	3	2	5	23
Platter failure							2		1
USB socket corruption								1	1
Burnt								1	1
Total	3	4	1	23	52	1	12	33	129

Table 8. Data Recovery Only in Case of PCB Failures

Situation	MOQ
Data recovery done	18
Data recovery not possible	7
Total	23

Table 9. Data Recovery in Head Failures

Situation	MOQ
Data recovery done	39
Data recovery not possible	37
Total	76

A converter board has been developed to ensure that HDDs or M.2 SSDs with failed USB interfaces can be accessed via the Sata interface. The image of this developed card is presented in Figure 53.

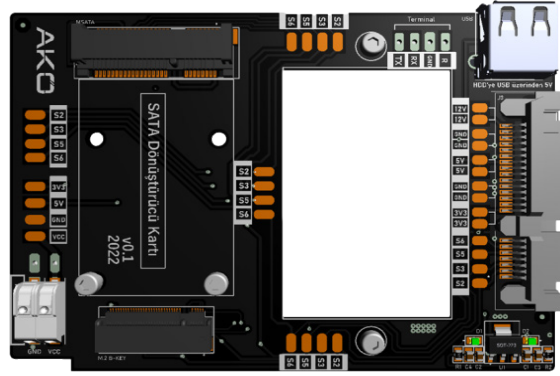


Figure 53. The card we developed for access from the Sata interface

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

- To enable msata conversion,
- To enable M.2 – B Key SSD conversion,
- To ensure the safety of soldered card connection cables,
- To provide terminal connection to disks when necessary,
- Apart from these, converting SSDs that can be converted to Sata,
- To facilitate the soldering process and facilitate the transport of the soldered board,
- A converter board has been developed to provide socket connections for 1.8”, 2.5”, and 3.5” hard disks with broken power or data sockets.

The root cause of problems with optical discs is problems with the optical disc surface. If these problems are listed;

- * The surface of the optic disc is dirty,
- * The optical laser burns the optical disc,
- * Fracture or cracking of the optic disc,
- * Distortion of the physical shape of the optical disc,
- * An error occurred during data recording to the optical disc,
- * It can be listed as light or deep scratches on the optical disc.

The main causes of problems in hard disks are the electronic circuit elements on the PCB, the motor, and the read/write heads.

The main ones are listed;

- * All kinds of reasons that prevent electrical conductivity, such as deterioration or fragmentation of circuit elements on the PCB,
- * All kinds of motor-related reasons prevent the rotation of the platters and the platters,
- * It can be summarized as any reason that prevents the read/write heads from functioning.

Process Steps to Follow During Data Recovery

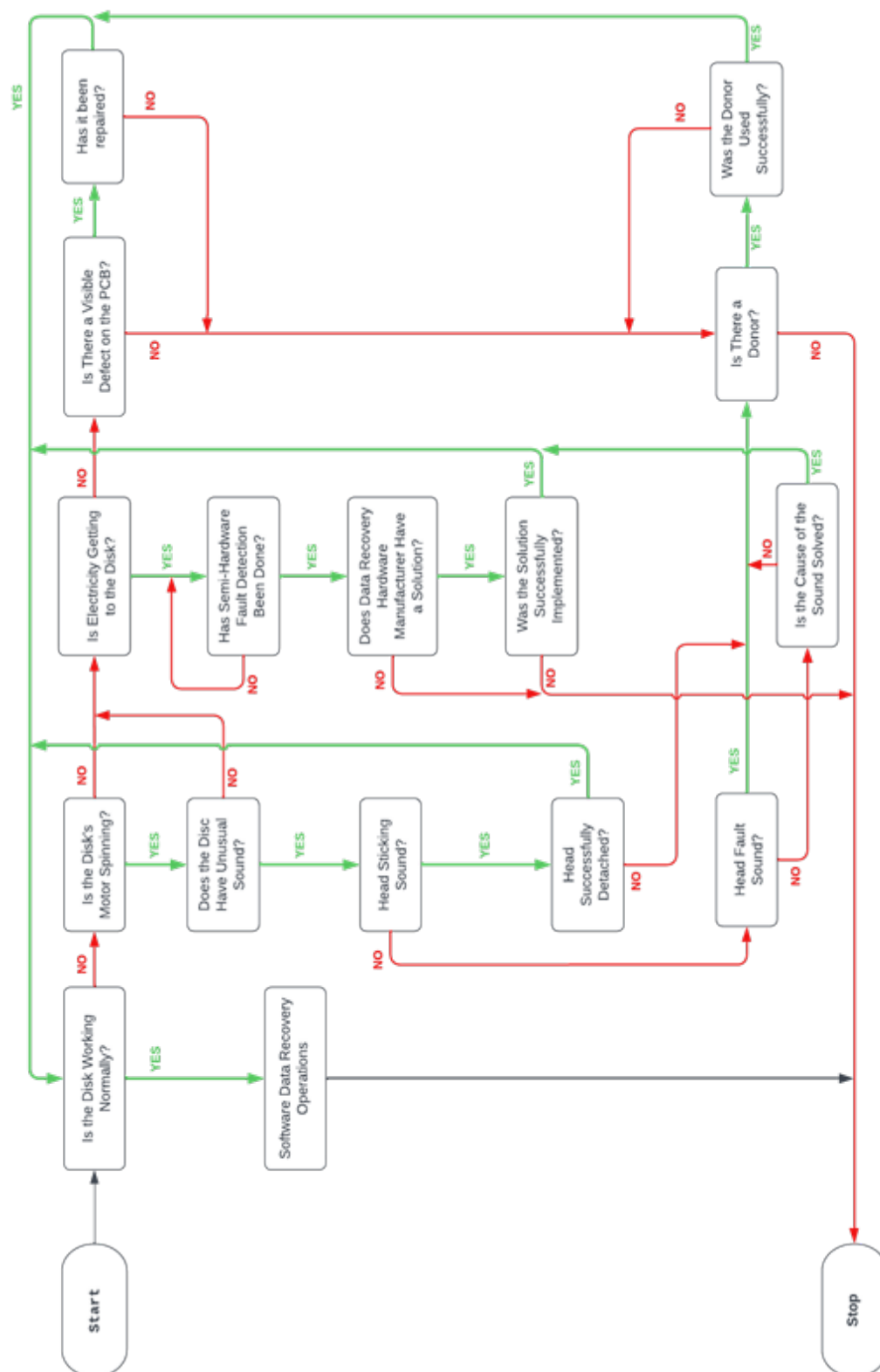


Figure 54. Data Recovery Steps on Hard Drives

References

- ACELab Europe s.r.o., 2014, List of compatible SATA PCB for 2,5" USB drives, <https://forum.ancelab.eu.com/viewtopic.php?f=155&t=8376>:
- Acelab Europe s.r.o., 2018, PC-3000 Data Extractor. Practical advices and Settings Menu Dive In, <https://blog.ancelab.eu.com/pc-3000-data-extractor-practical-advices-settings-menu.html>:
- ACELab Europe s.r.o., 2021, ACE Lab Webinar on the Modern Challenges in Data Recovery & Digital Forensics, <https://www.youtube.com/watch?v=47eXzxZk-0E>:
- Acelab Europe s.r.o., 2022, PC-3000 Product Catalogue for Digital Forensics.
- David, M. S., 2000, The cost of lost data, *Storage Manag. Solut.*, 4 (6), 60–61.
- DeepSpar Data Recovery Systems, 2007, Data Loss and Hard Drive Failure: Understanding the Causes and Costs, <http://www.deepspar.com/wp-data-loss.html>:
- Donor Drives LLC, 2012, Hard Drive Circuit Board Replacement Guide or How To Swap HDD PCB, www.donordrives.com/pcb-replacement-guide:
- Durak, R., 2011, Araştırma Yöntem Ve Teknikleri, <https://atauni.edu.tr/yuklemeler/e6d32be6d3b1ad4dae5f6cc23165e2da.pdf>:
- Exterro Inc., 2021, Custom Carvers, <https://support.exterro.com/support/solutions/articles/69000765593-custom-carvers>:
- Guo, Y. and Slay, J., 2010, Data Recovery Function Testing for Digital Forensic Tools, *Advances in Digital Forensics VI*, Berlin, Heidelberg, 297-311.
- Güllüce, Y. Z. and Benzer, R., 2015, Hard Disk Failure And Data Recovery Methods In Computer Forensic, *International Journal of Human Sciences*, 12 (1), 206-225
- HDDZone, 2010, Hard Drive PCB Replacement Guide, www.hddzone.com/conditions.html:
- IBM Security and Ponemon Institute, 2021, Cost of a Data Breach Report.
- Jared, 2016a, Samsung USB to SATA PCB Compatability, www.data-medics.com/forum/threads/samsung-usb-to-sata-pcb-compatability.1438:
- Jared, 2016b, Toshiba USB to SATA Guide, www.data-medics.com/forum/threads/toshiba-usb-to-sata-guide.1305/:
- Jarolím, J., 2016, Reconstruction Of Data From Damaged Cd/Dvd, Master Thesis, Brno University Of Technology.
- Kara, Ş., 2013, Evaluation Of The Achievements Of Data Recovery Methods, Master Thesis, Firat University.
- Keskin, N., Kiran, A. N., Eğdemir, F. K. and Eren, T., 2020, Multicriteria Decision Making Methods and Service Provider Selection to Cloud Information Security Requirements, *International Journal of Information Security Engineering*, 6 (1), 45-60.
- Kessler, G., 2022, Gck's File Signatures Table, https://www.garykessler.net/library/file_sigs.html:
- MalwareHunterTeam, 2022, IDRansomware, <https://id-ransomware.malwarehunterteam.com/>:

No More Ransom, 2022, Decryption Tools, www.nomoreransom.org/en/decryption-tools.html:

Özdemir, A. and Gülcü, Ş., 2021, Causes Of Digital Data Loss And Data Recovery Methods, *2nd International 5 Ocak Congress on Applied Sciences*.

Özdemir, 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).

Recovery HDD, 2018, Atropelado sim senhor... www.instagram.com/p/BoxTBRPIKbV/:

Schroeder, B. and Gibson, G., 2007, Disk Failures in the Real World: What Does an MTTF of 1, 000, 000 Hours Mean to You?, p.

Tri-State Data Recovery & Forensics LLC, 2020, www.instagram.com/p/CGGW131jvQQ/: [22.06.2022].

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, **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, **ORCID:** 0000-0001-7714-8861.

Similarity Index

The similarity index obtained from the plagiarism software for this book chapter is 7%.

To Cite This Chapter:

Özdemir, A. & Gülcü, Ş. (2022). Scientific Data Recovery Methods and Solutions in Optics Discs and HDDs. In S. Kocer & O. Dundar (Eds.), *Current Studies in Basic Sciences, Engineering and Technology* (pp. 224-257). ISRES Publishing.