OFFZONE
2022

Recovering encrypted data from damaged media

}{отт@бь)ч Tehhi

DC78182

Moscow, August, 25-26, 2022

Legend

Quest report:

During a counter-terrorist operation, the special forces obtained some data carriers, which contain data that would compromise the activities of the terrorist group.

The media includes a memory stick and a hard drive. Since the operation was carried out with the use of brutal physical force, the data carriers were damaged.

Data storage device

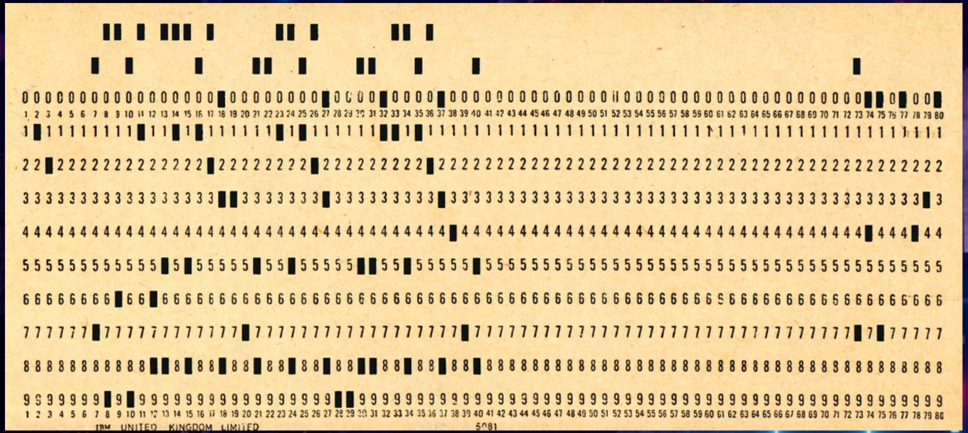
Recording principles:

- Mechanical
- Magnetic
- Electrostatic
- Optical

Mechanical

Knots

Text



Punchcard

Magnetic

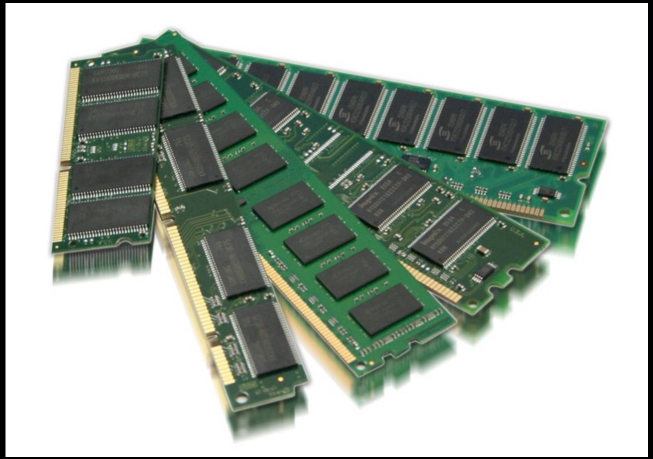
Magnet wire

Tapes

Floppy

Hard disk

Electrostatic

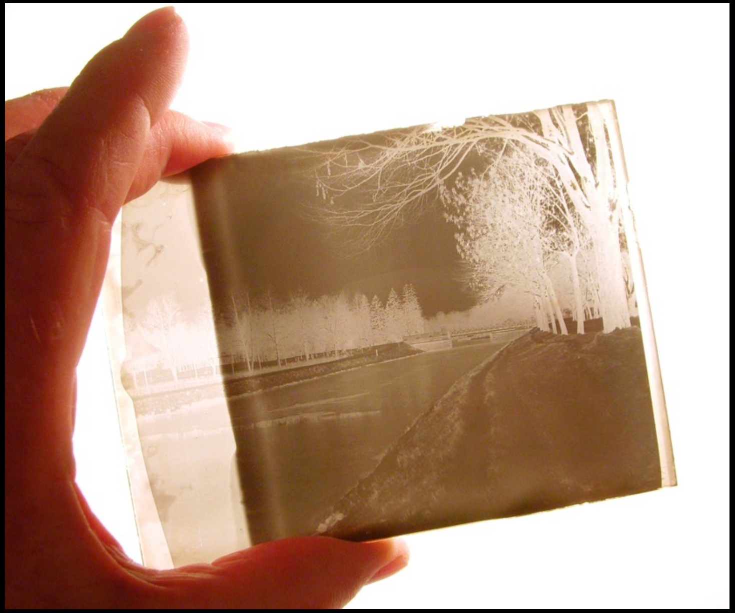


DRAM

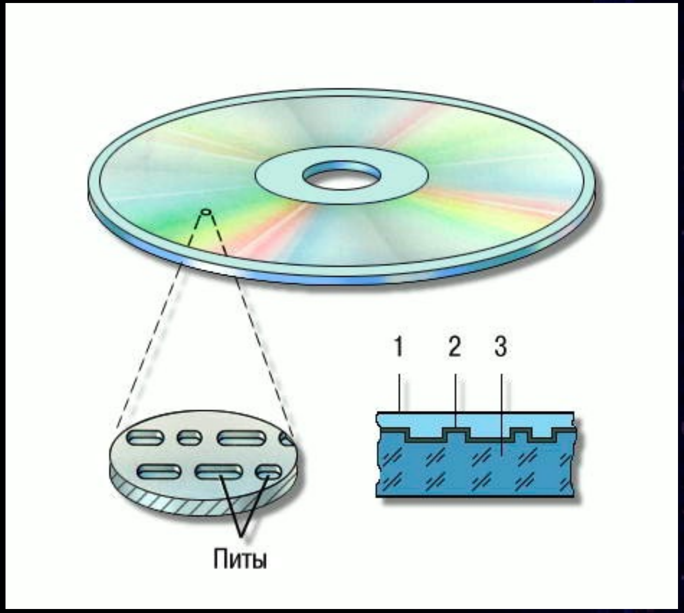
FLASH

SSD

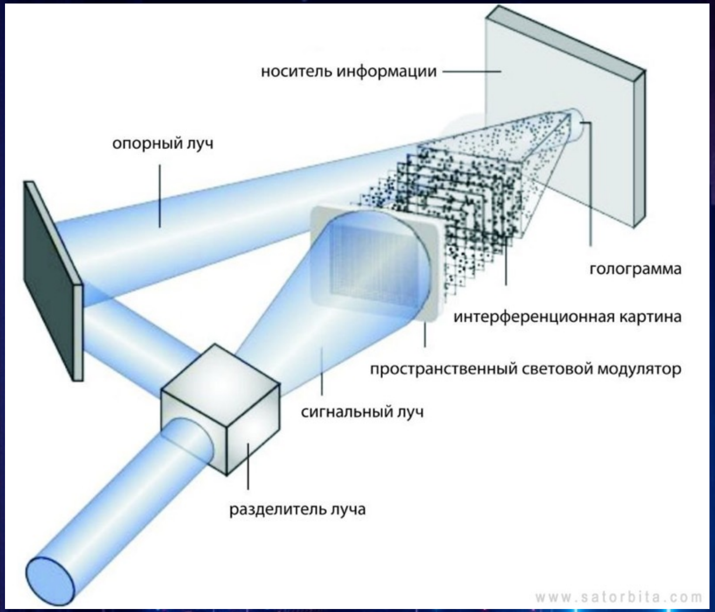
Optical



Photo



CD/DVD

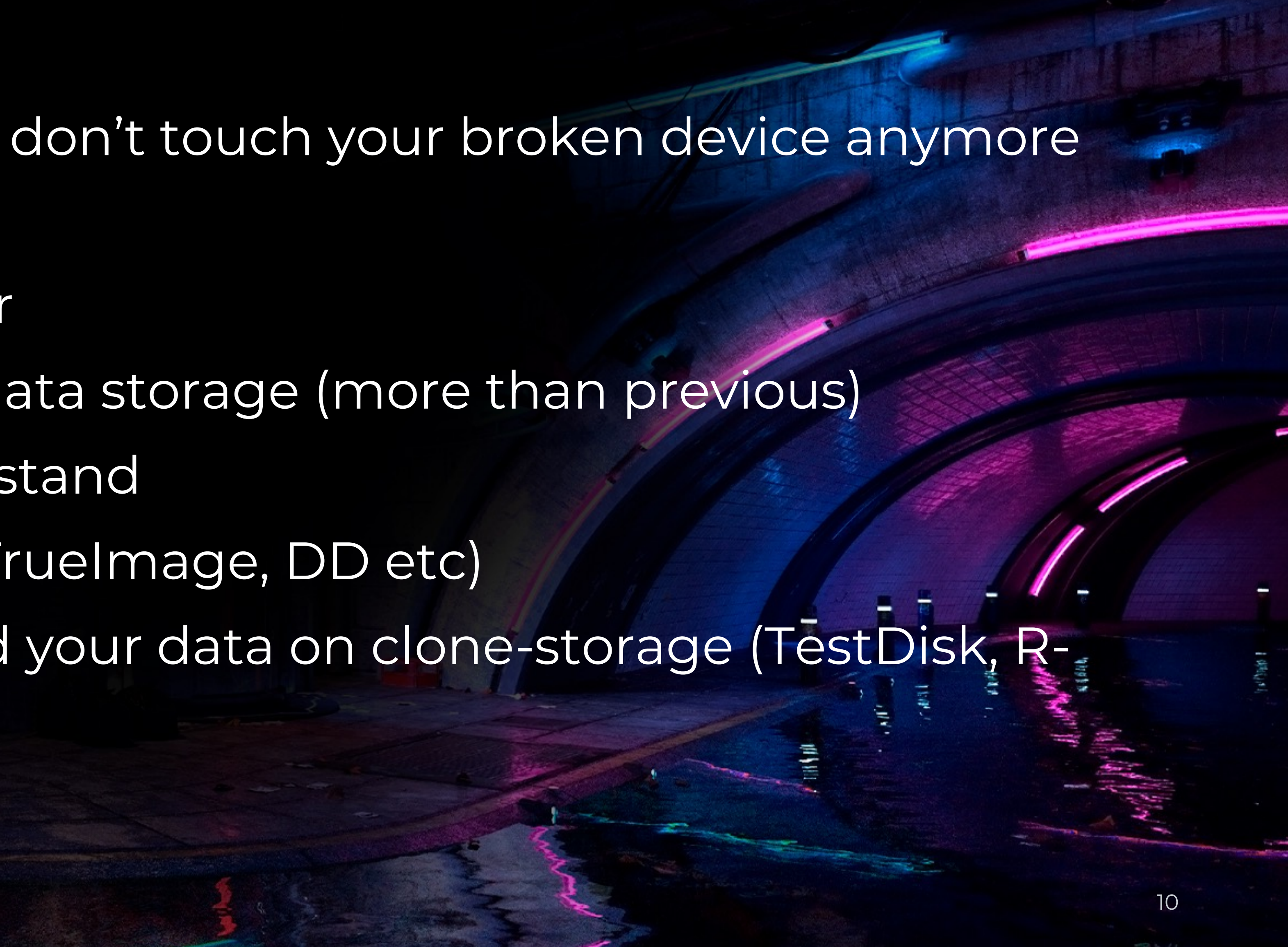


Holography

What causes Physical Media Damage?

- Mechanical damage
- Temperature
- Chemical damage
- Ionizing radiation
- Electromagnetic radiation
- High-intensity light source
- Human factor
- ETC

DATA RECOVERY



- Turn off your device. And don’t touch your broken device anymore
- Why it was damaged?
- Find and prepare a donor
- Prepare a new working data storage (more than previous)
- Assemble Data recovery stand
- Create a clone (Acronis, TrueImage, DD etc)
- Choose software and find your data on clone-storage (TestDisk, R-Studio etc)
- Crypto? No way…

Turn off your device
and don’t touch your broken device anymore

Necessary to prevent information corruption process

Why it was damaged?

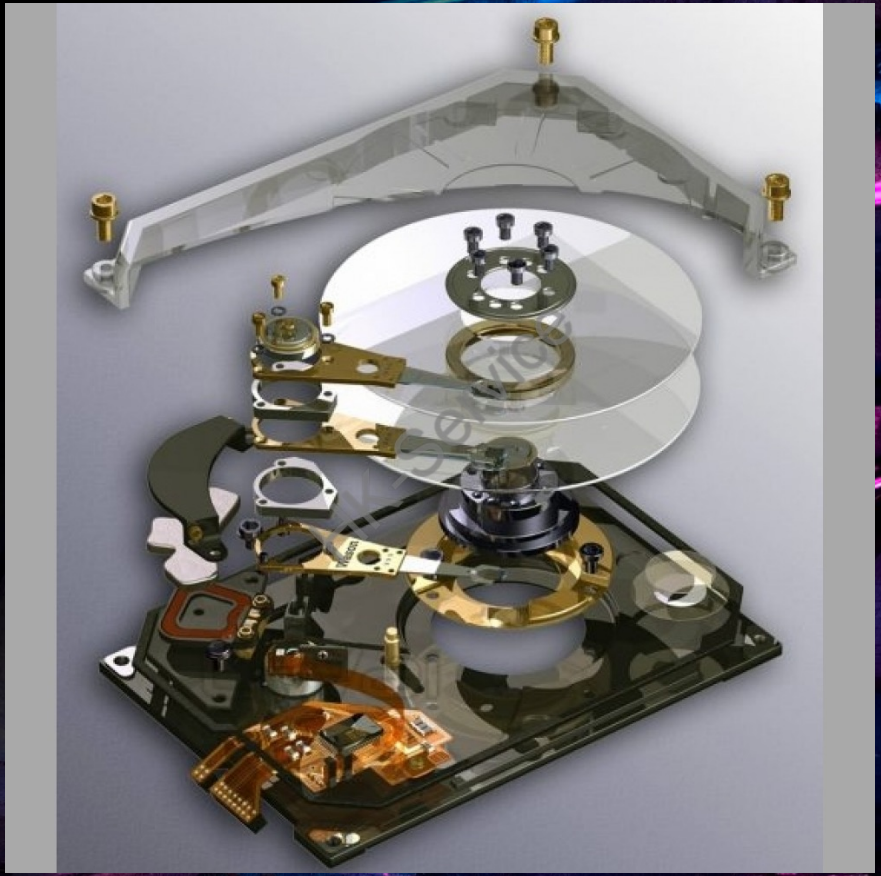
A clear understanding of the cause of information corruption makes it possible to understand what needs to be done to restore it

Find and prepare a donor

How to choose it?

- Ideally, the donor should be from the same lot as the damaged carrier
- or use a donor of an identical series, compatible in software and having a compatible package

An incompatible donor can lead to the complete destruction of information (erasing the HDD translator, erasing data in solid-state storage media, etc.)



Prepare a new working data storage (more than previous)

You have only one chance to clone your data, so

Don’t screw up

Data recovery stand

Soldering station with a kit of tools

Multimeter

Adapter

Programmer

Create a clone

Choosing software, remember that it’s main tasks are:

- byte-by-byte reading of the damaged storage medium with all errors
- writing the read data to a new medium "byte for byte"

Example: Acronis, TrueImage, DD

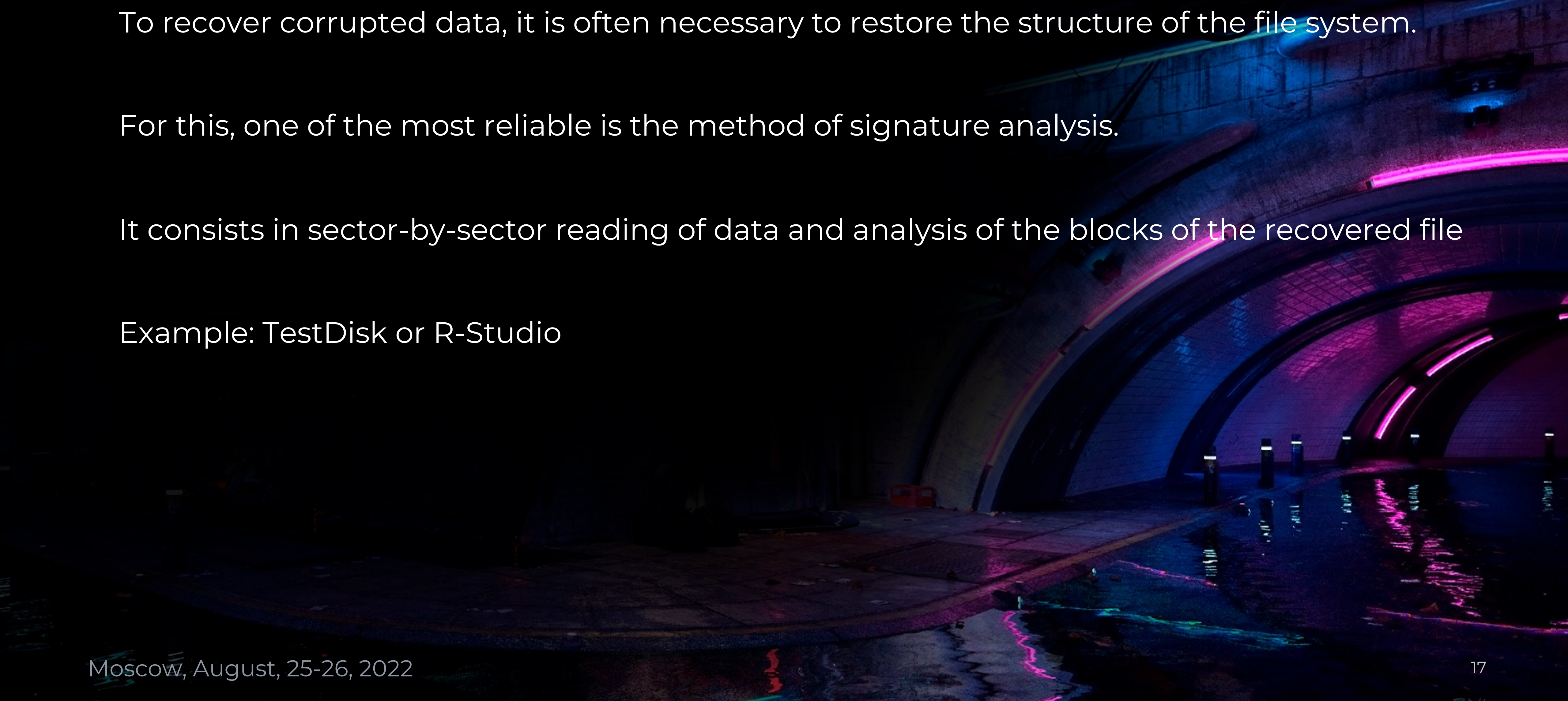
Find your data

To recover corrupted data, it is often necessary to restore the structure of the file system.

For this, one of the most reliable is the method of signature analysis.

It consists in sector-by-sector reading of data and analysis of the blocks of the recovered file

Example: TestDisk or R-Studio



Crypto? No way...

- End-to-end on-the-fly encryption with file system emulation
- Container could be: a file, a partition of a storage medium, an entire storage medium
- Container could be hidden (allows to implement the principle of true negation)
- Encryption key could be: a password, a token, a file, a system account

Example: TrueCrypt, VeraCrypt BitLocker etc

Thank you!

OFFZONE 2022

@dc78182