CHIP-OFF DIGITAL FORENSICS

THE MYTH ABOUT DATA DELETION

Sasha Sheremetov | Rusolut

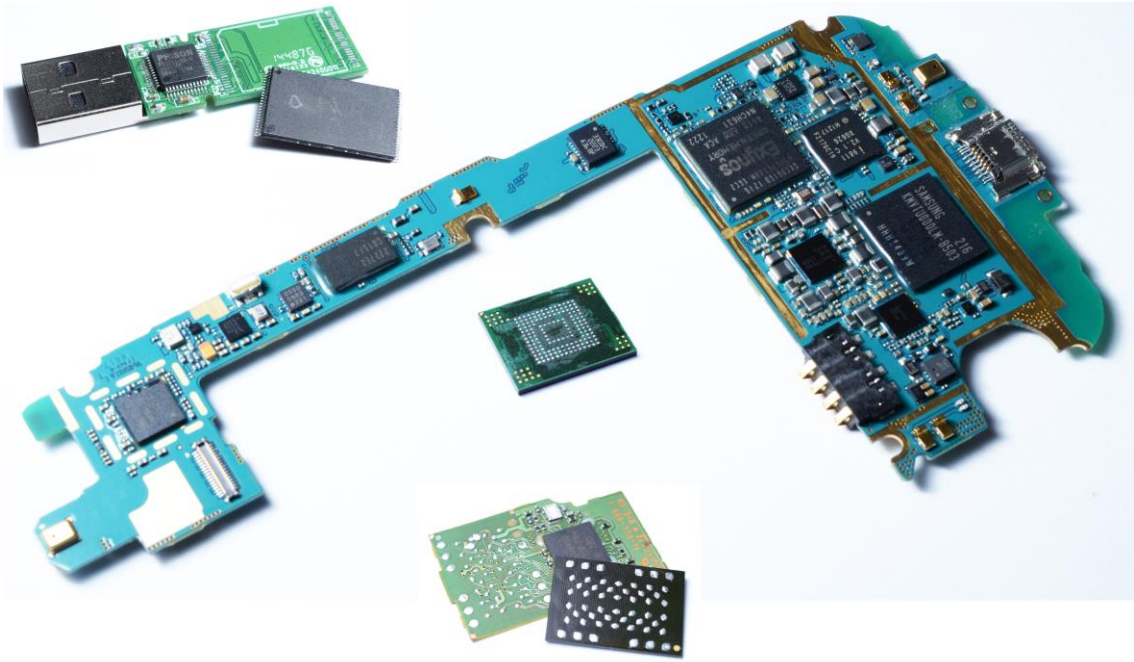
ruSolut

NAND FLASH STORAGE

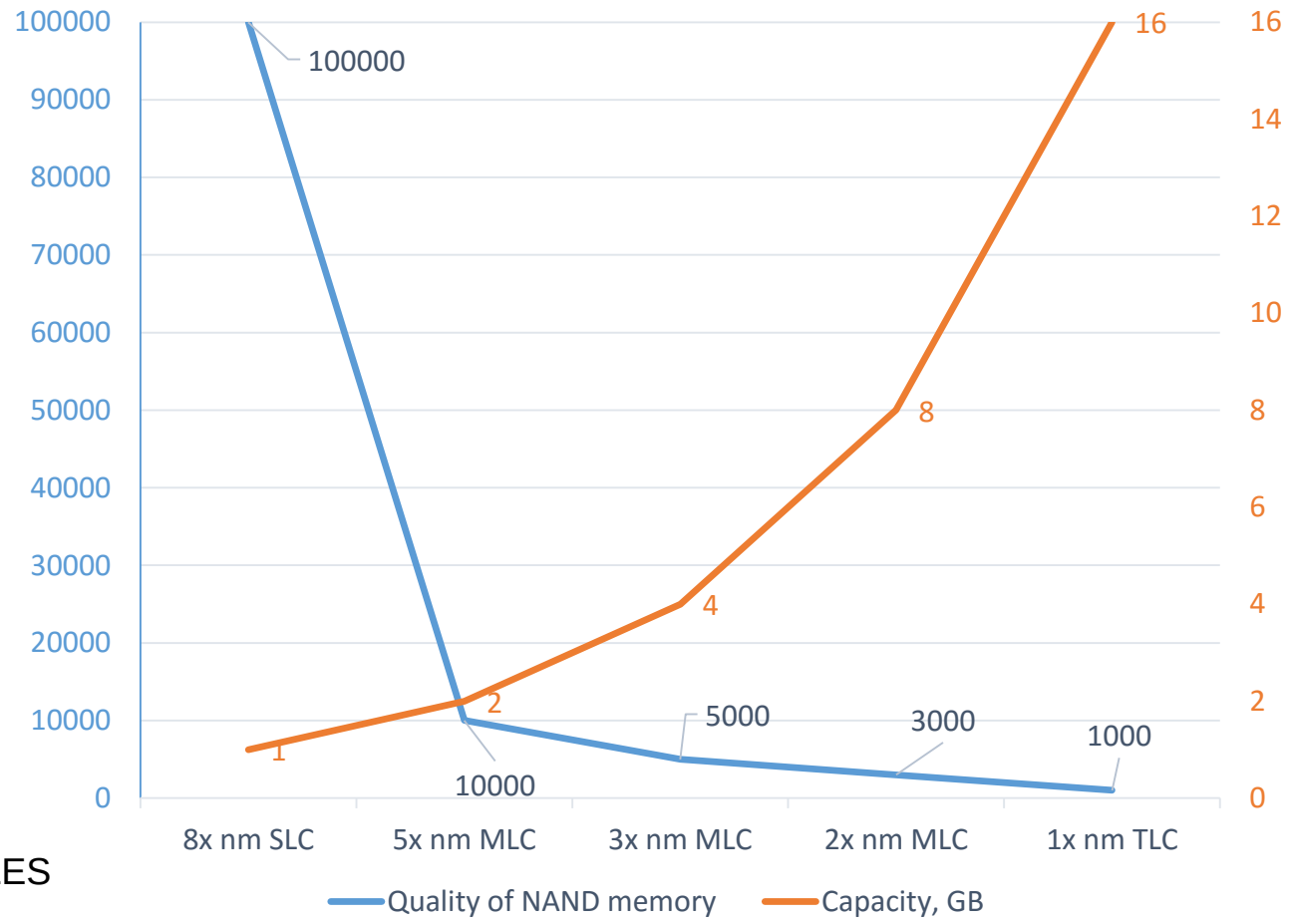
- USB pendrives
- Smartphones
- Tablets
- Memory cards (SD, microSD, CF, etc)
- Solid State Drives
- Digital voice recorders
- GPS devices
- Other devices

NAND & eMMC CHIPS

- TSOP48
- LGA52
- BGA169 eMMC
- BGA100
- BGA132
- BGA152
- BGA137
- BGA154
- BGA221



NAND MEMORY ENDURANCE

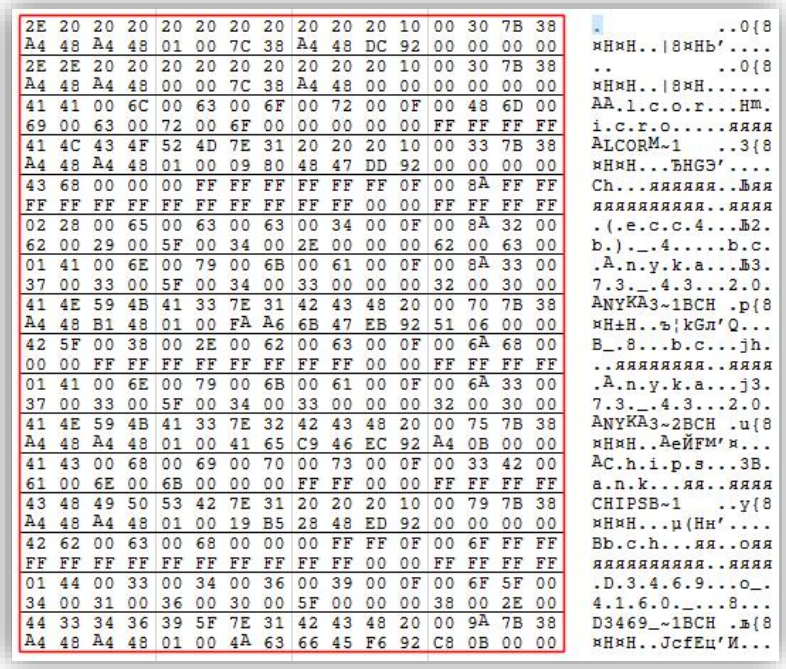


ERASE CYCLES

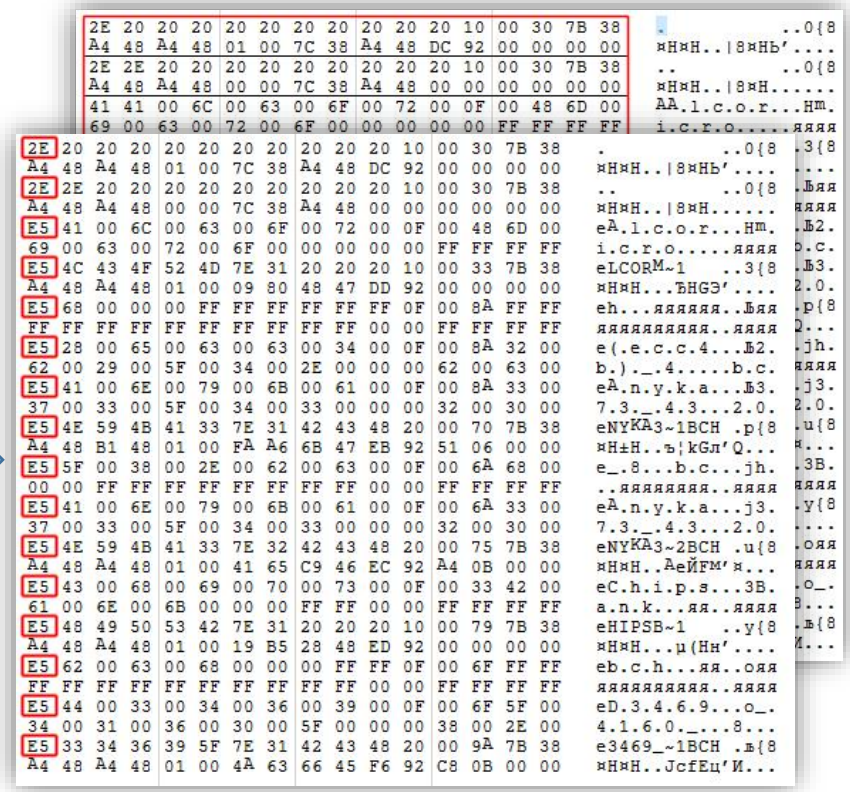
SLC NAND – up to 100’000
MLC NAND – up to 10’000
TLC NAND – up to 1500

DELETE OPERATION ON FILE SYSTEM LAYER

OLD INVISIBLE VERSION OF DATA ON PHYSICAL NAND LAYER



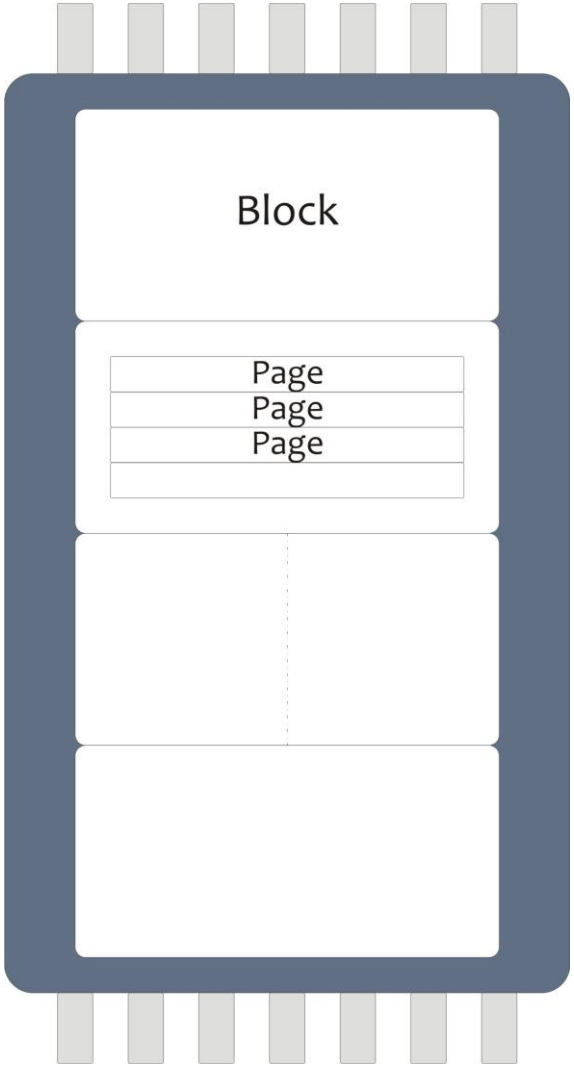
Delete



NEW VISIBLE VERSION OF DATA ON PHYSICAL NAND LAYER

Normally when the file is deleted, there's only metadata modified to make it invisible.
But in fact, there still old version of this metadata is stored in another NAND block.

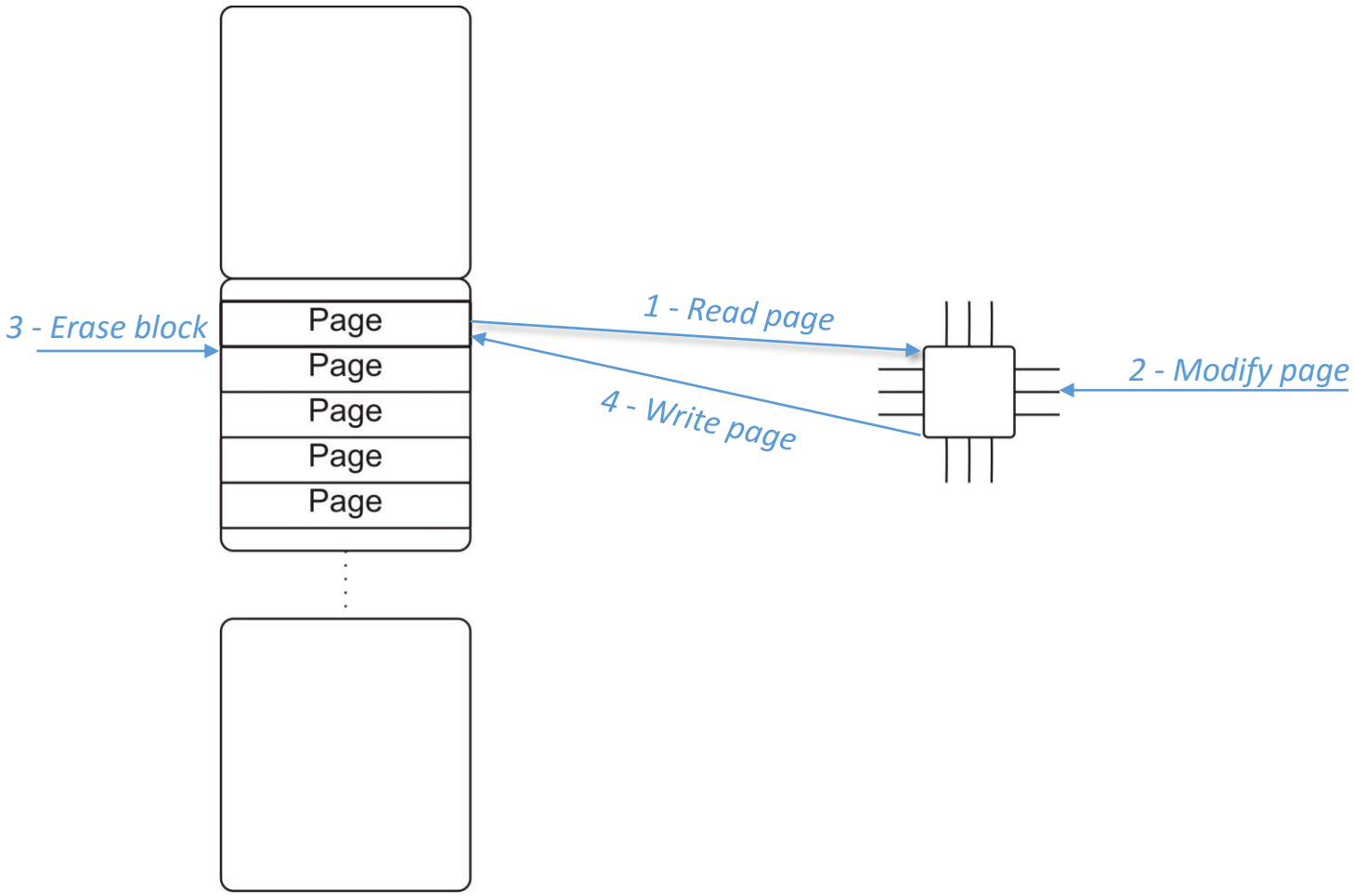
PHYSICAL STRUCTURE OF NAND MEMORY



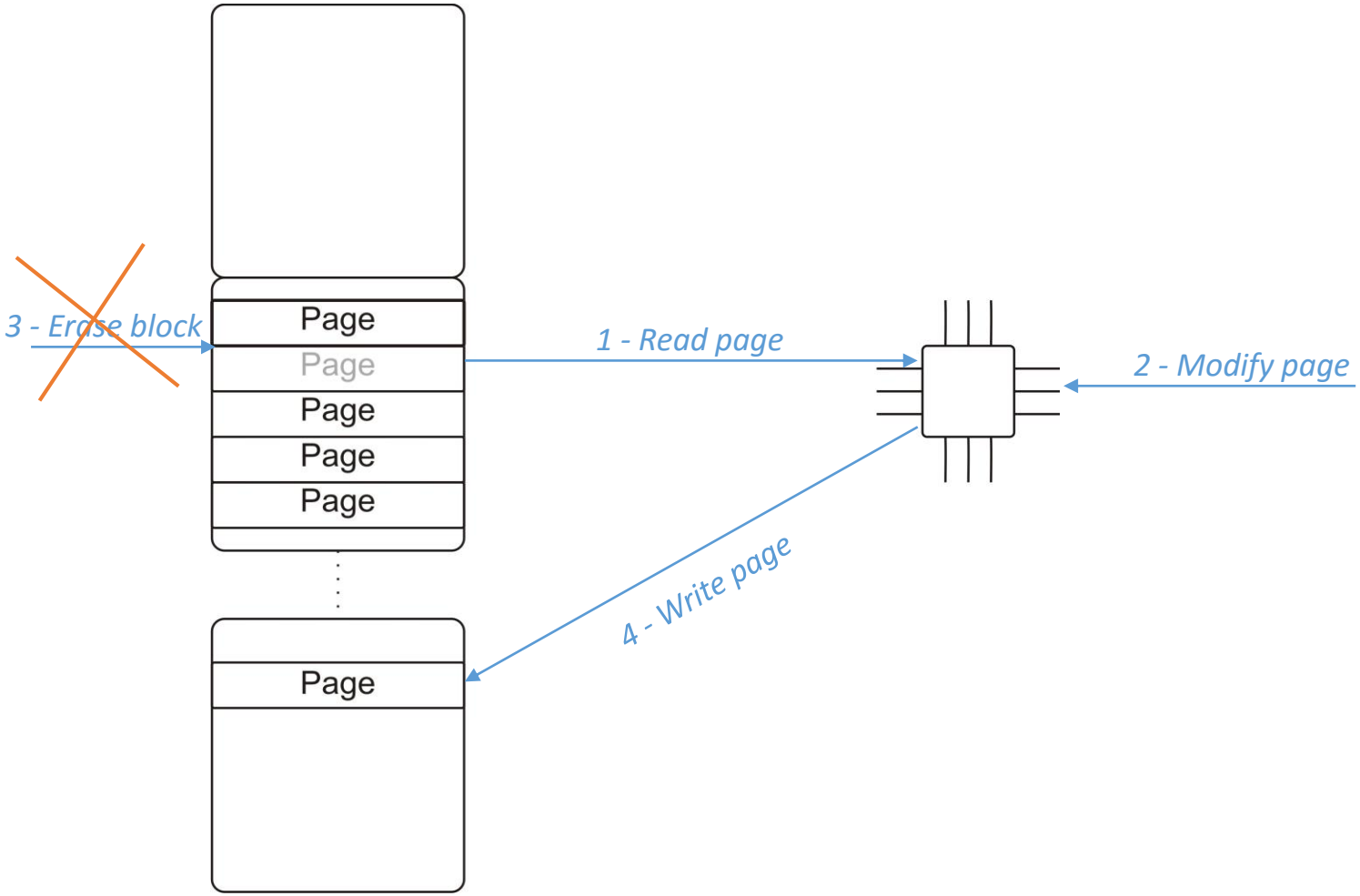
Block is a minimal unit of ERASE operation

Page is a minimal unit of READ/WRITE operation

DATA MODIFICATION IN NAND. IN THEORY



DATA MODIFICATION IN NAND. ON PRACTISE



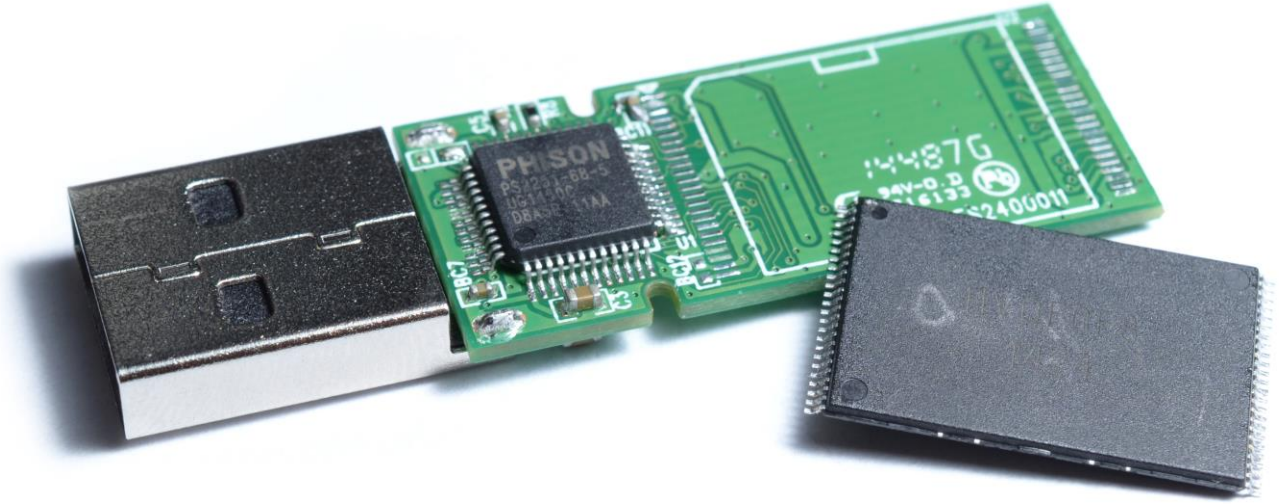
CASE STUDY

Scenario: The ex-employee of company is accused in stealing corporate's client database

Evidence collected: Pendrive where he has probably copied stolen files

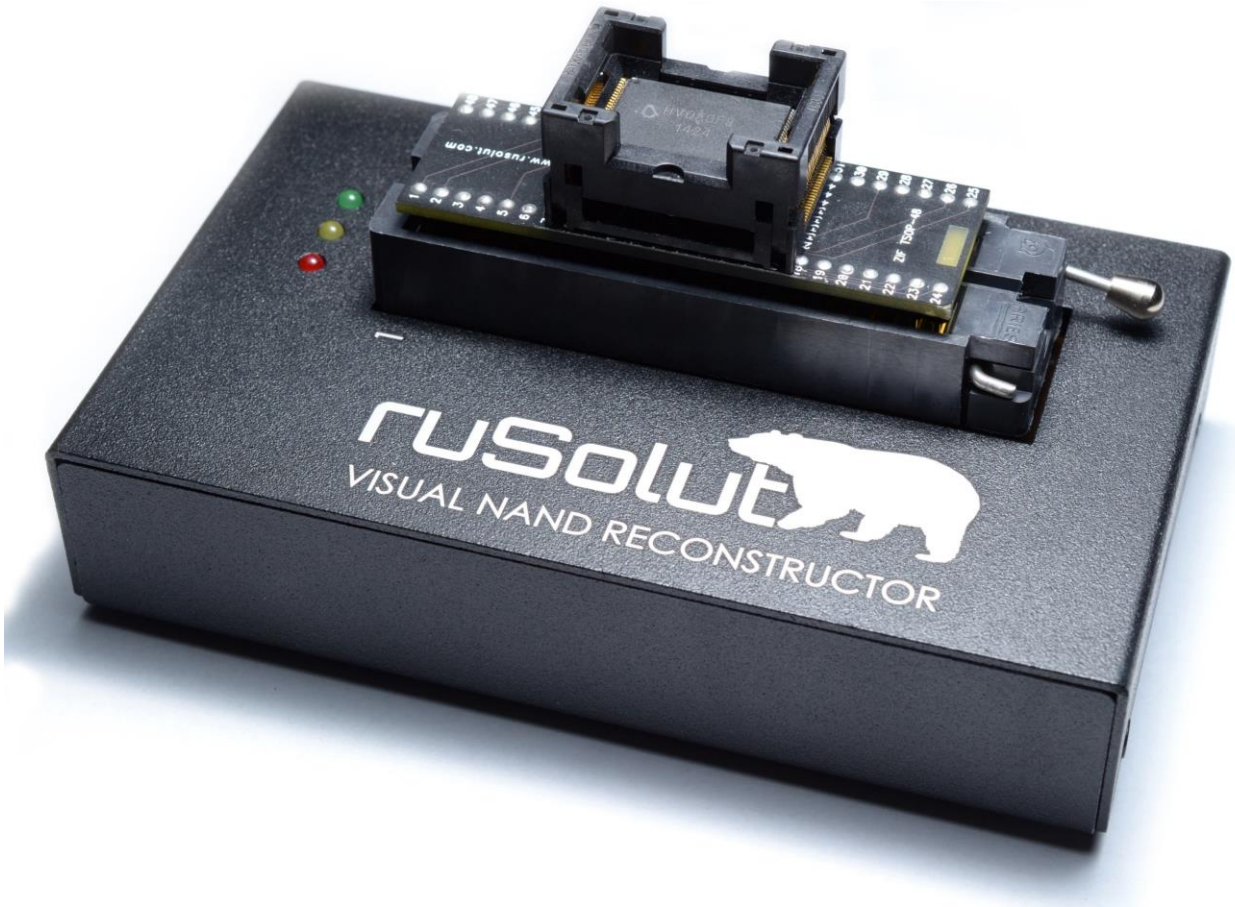
Goals: Find any traces or files related to database "ELPIDA"

Notes: No database files were found during classic forensic analysis.
Data is probably deleted and overwritten.



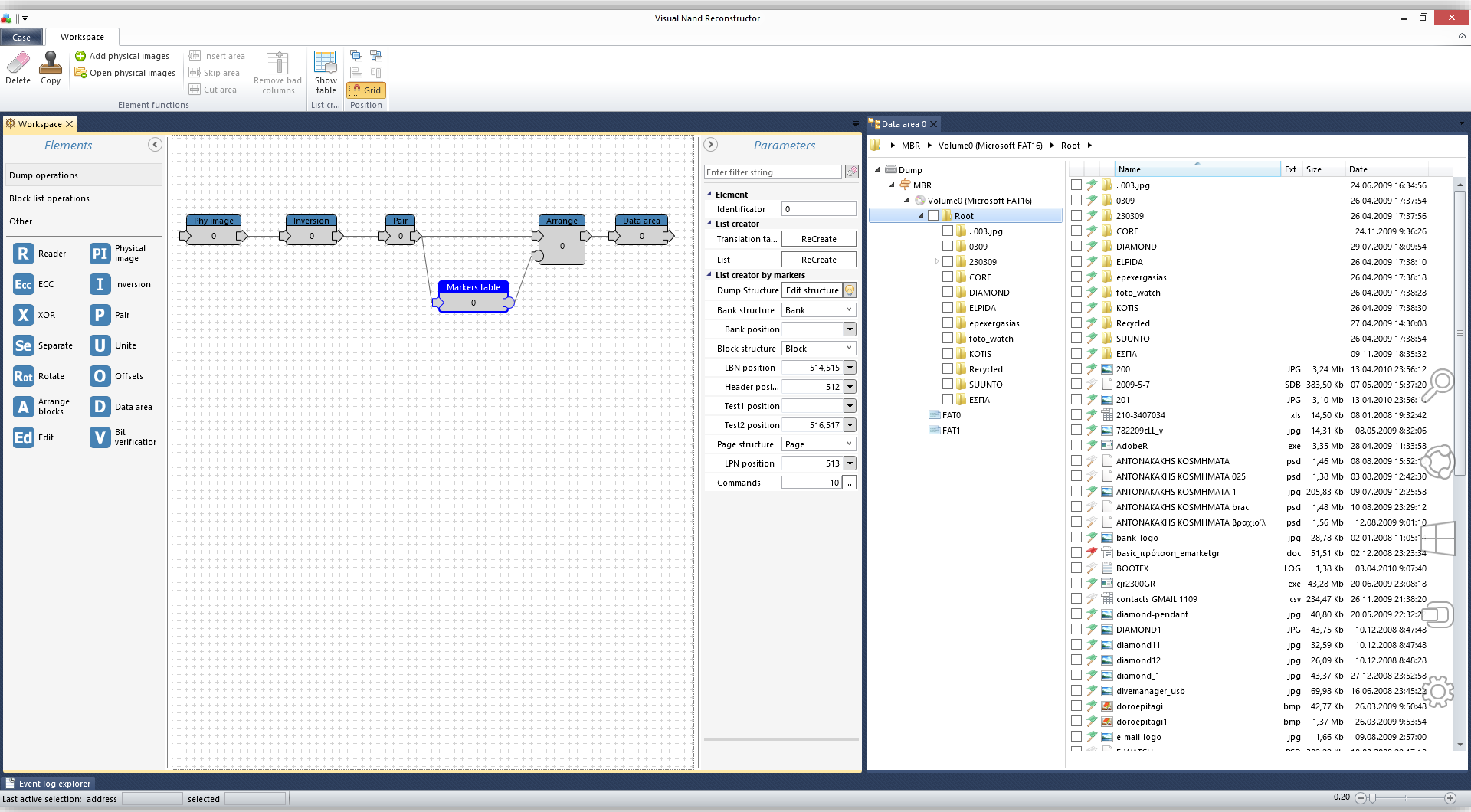
ruSolut

CHIP-OFF NAND IMAGE EXTRACTION PROCESS

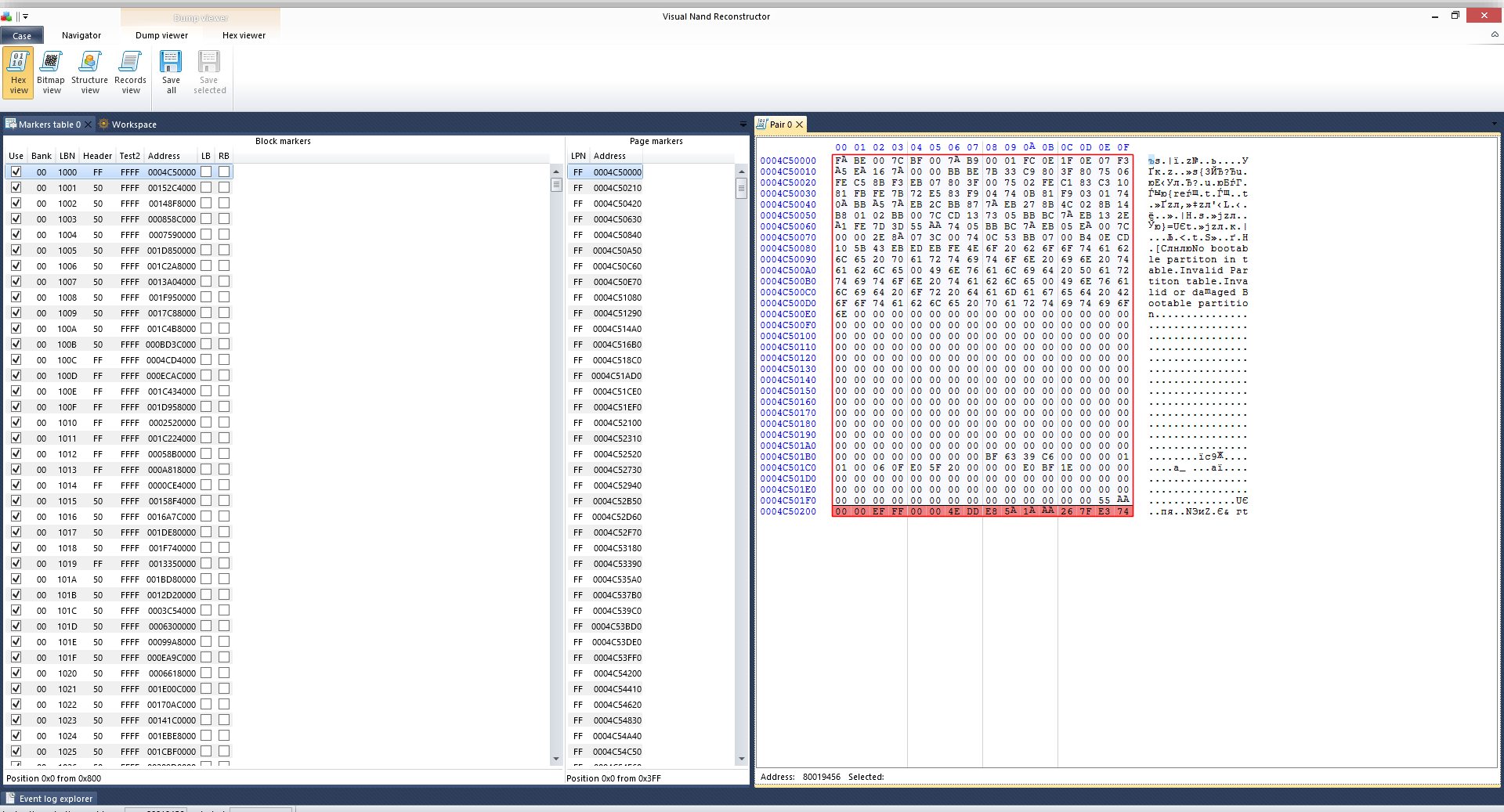


ruSolut

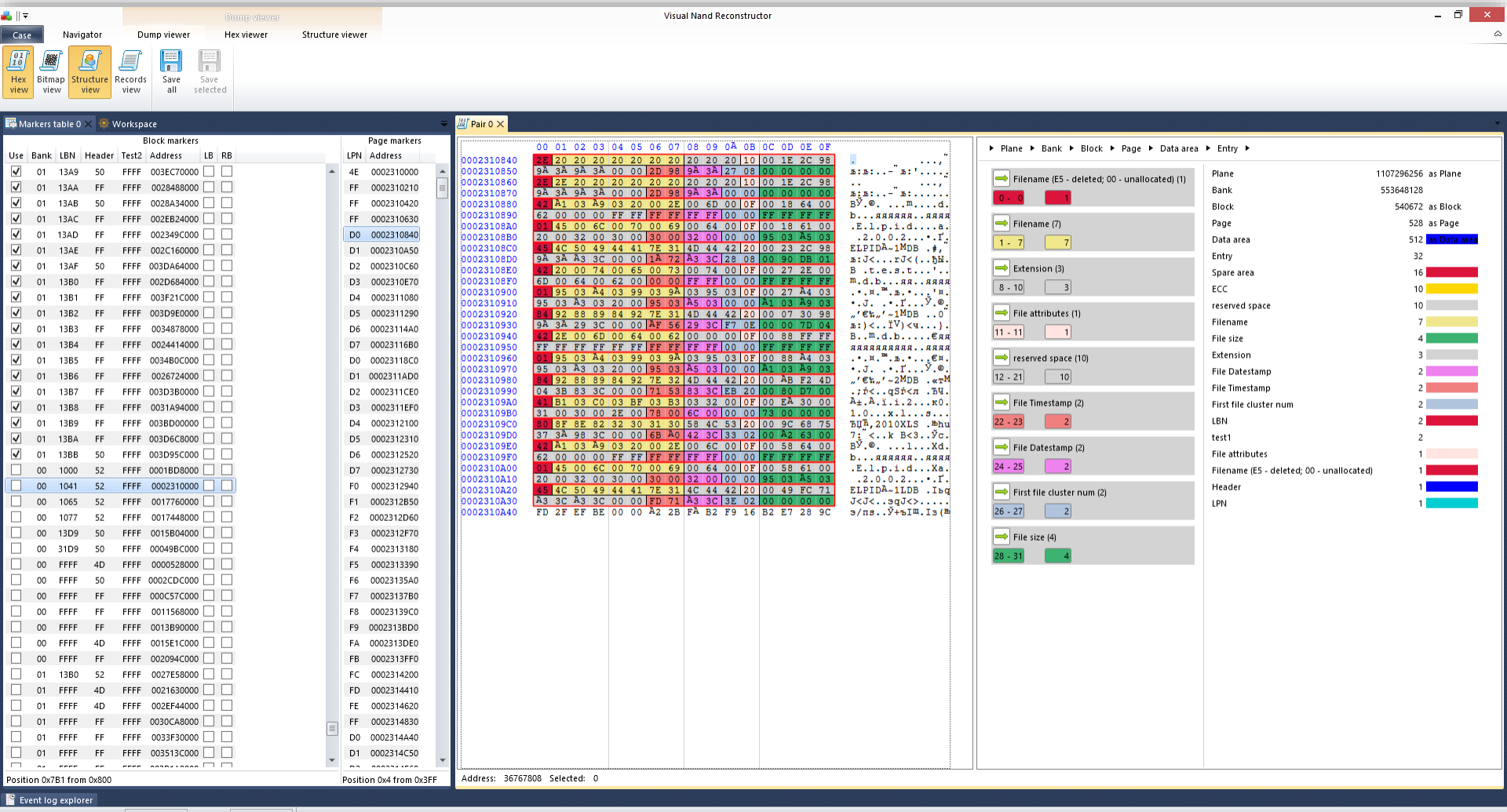
When physical image is extracted, it has to be transformed to logical image



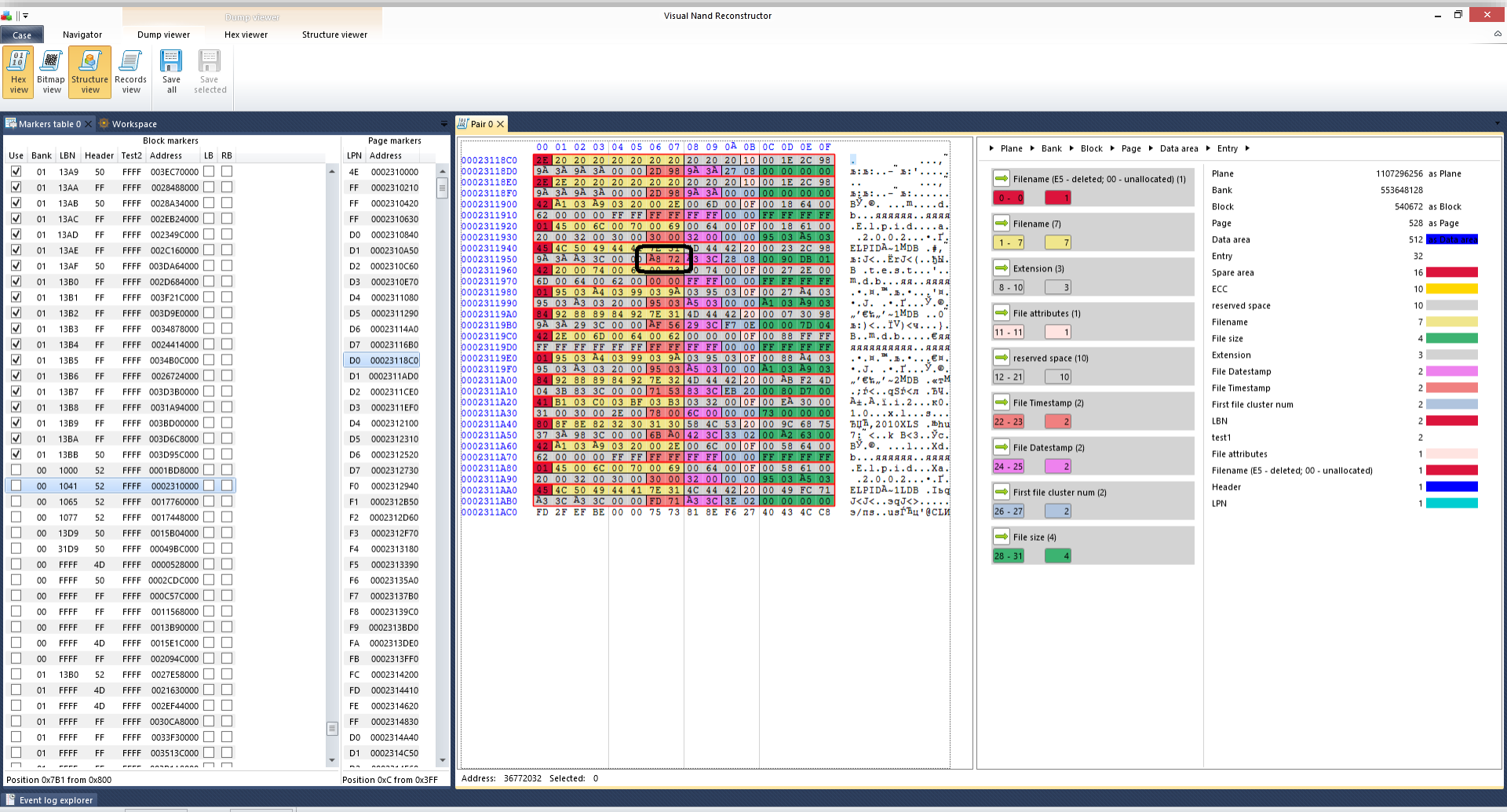
Here we see data blocks which shape logical image with file system



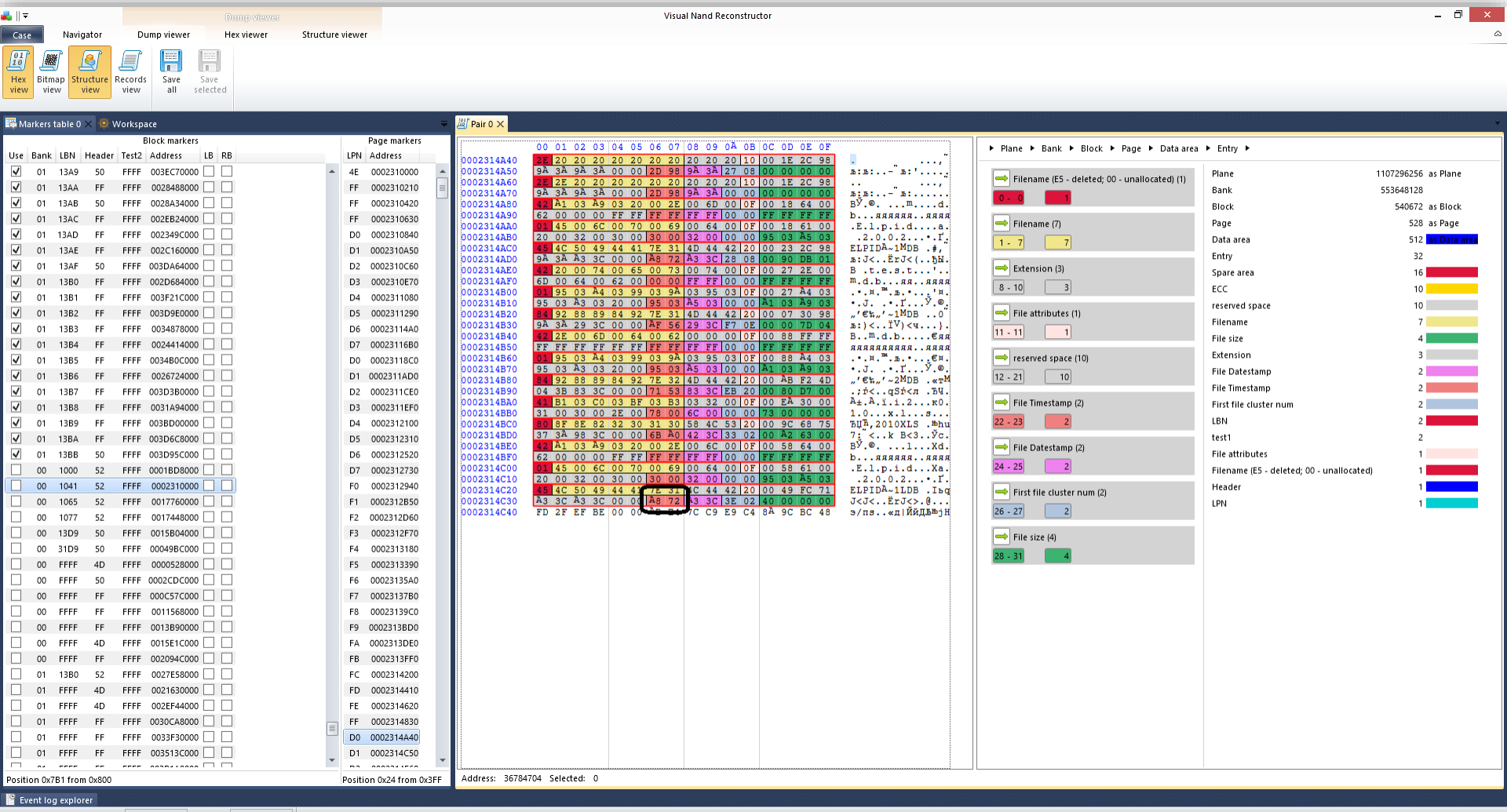
There are some other blocks beyond the range of data blocks, they are system and invisible outside interface. In one of those blocks we can find a fragments of file system's metadata, in particular - FAT folder. This FAT folder contains file record of "ELPIDA.MDB" and "ELPIDA .LDB" files. It proves existence of the stolen files on suspect's device.



In another copy of the page we can even see the history of file creation and modification. The blocks that contain pages with different versions of data are called “LOG block”, because they keep LOGs of data modification. In this page we can see that time stamp of “ELPIDA.MDB” was changed.

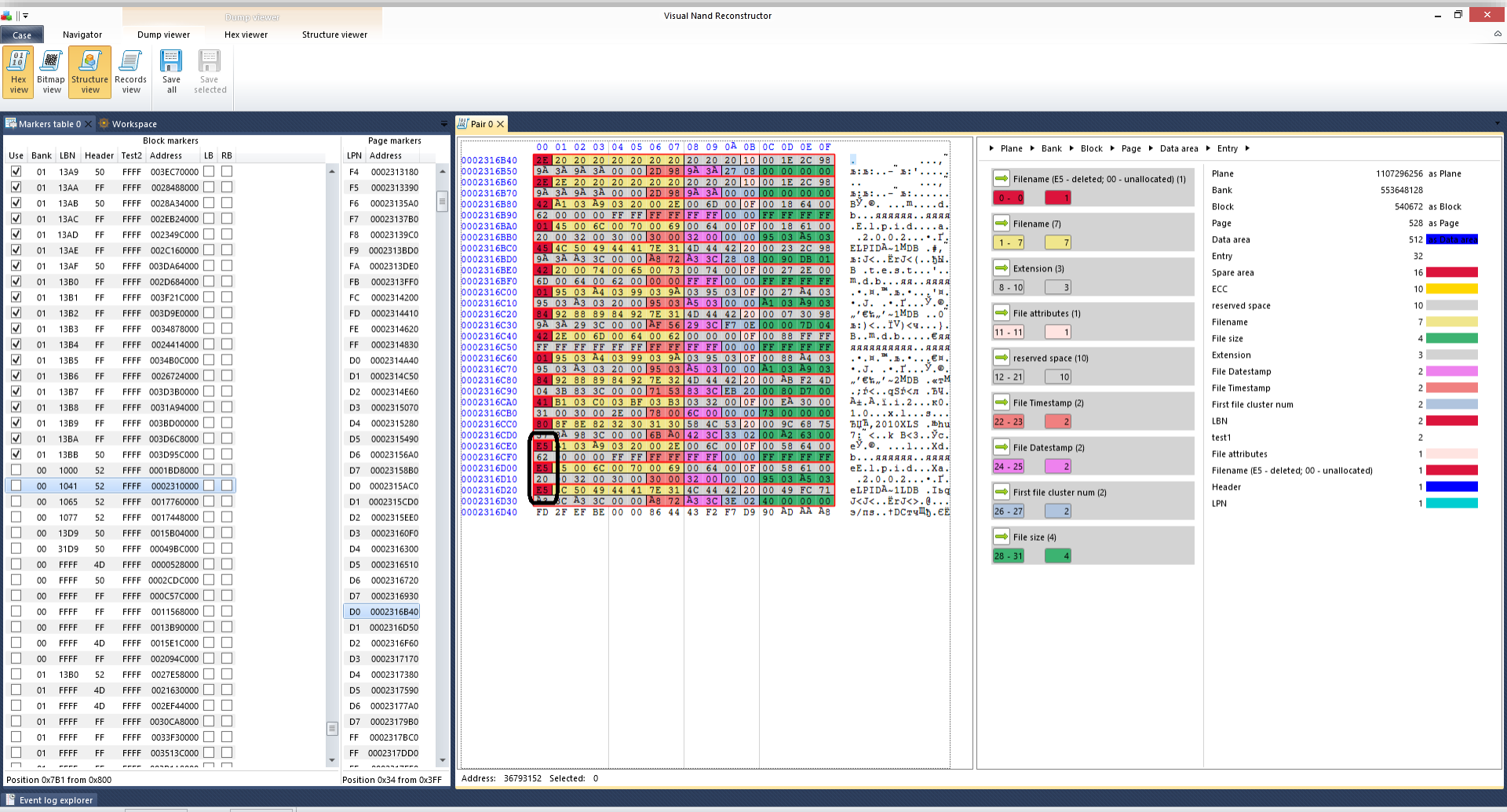


There are several copies of page with file system’s metadata. In this version we can see that timestamp of “ELPIDA.LDB” was changed.



ruSolut

In the latest versions of the page we can see that eventually files related to ELPIDA database were deleted. File recovery is not possible in this case, but the trace, the fact that this file was existing on device proves that files were actually stolen.



CONCLUSION

It is known fact that NAND Flash storage devices do not erase data when it’s deleted, during a period of time (until garbage collection algorithm eventually does it).

As we have just proven, chip-off data extraction and analysis is the only way to find 100% of user's data or data traces on flash device

This method is applicable for working and heavily damaged (non-working) flash devices that utilize NAND memory.

ruSolut