



## CHIP-OFF DIGITAL FORENSICS

# THE MYTH ABOUT DATA DELETION

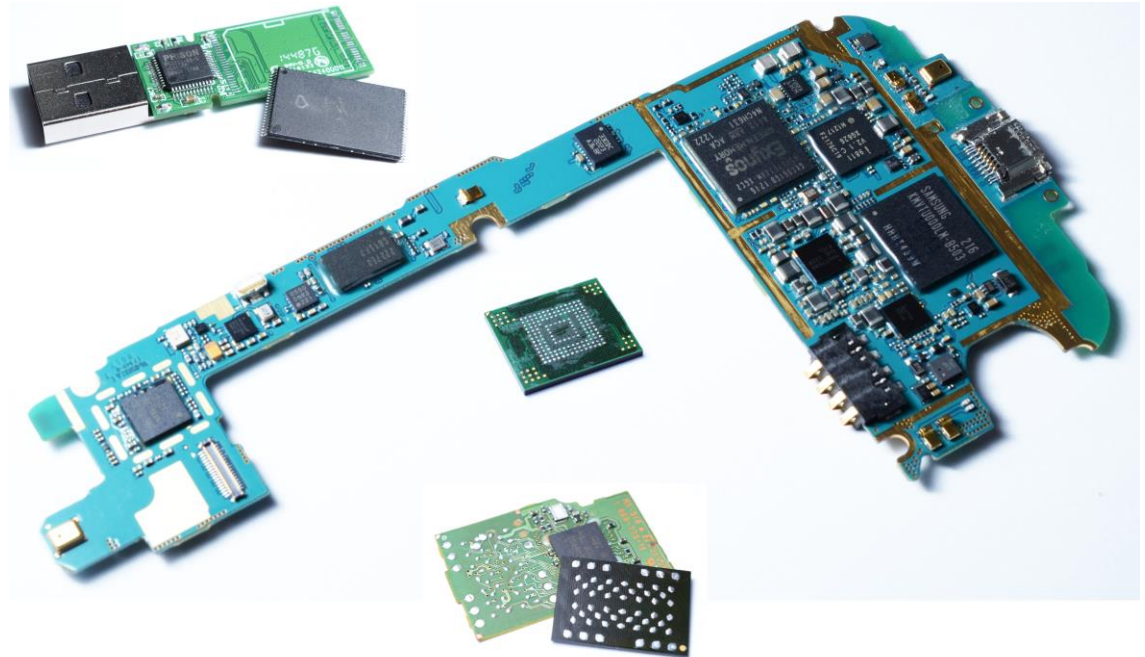
# NAND FLASH STORAGE



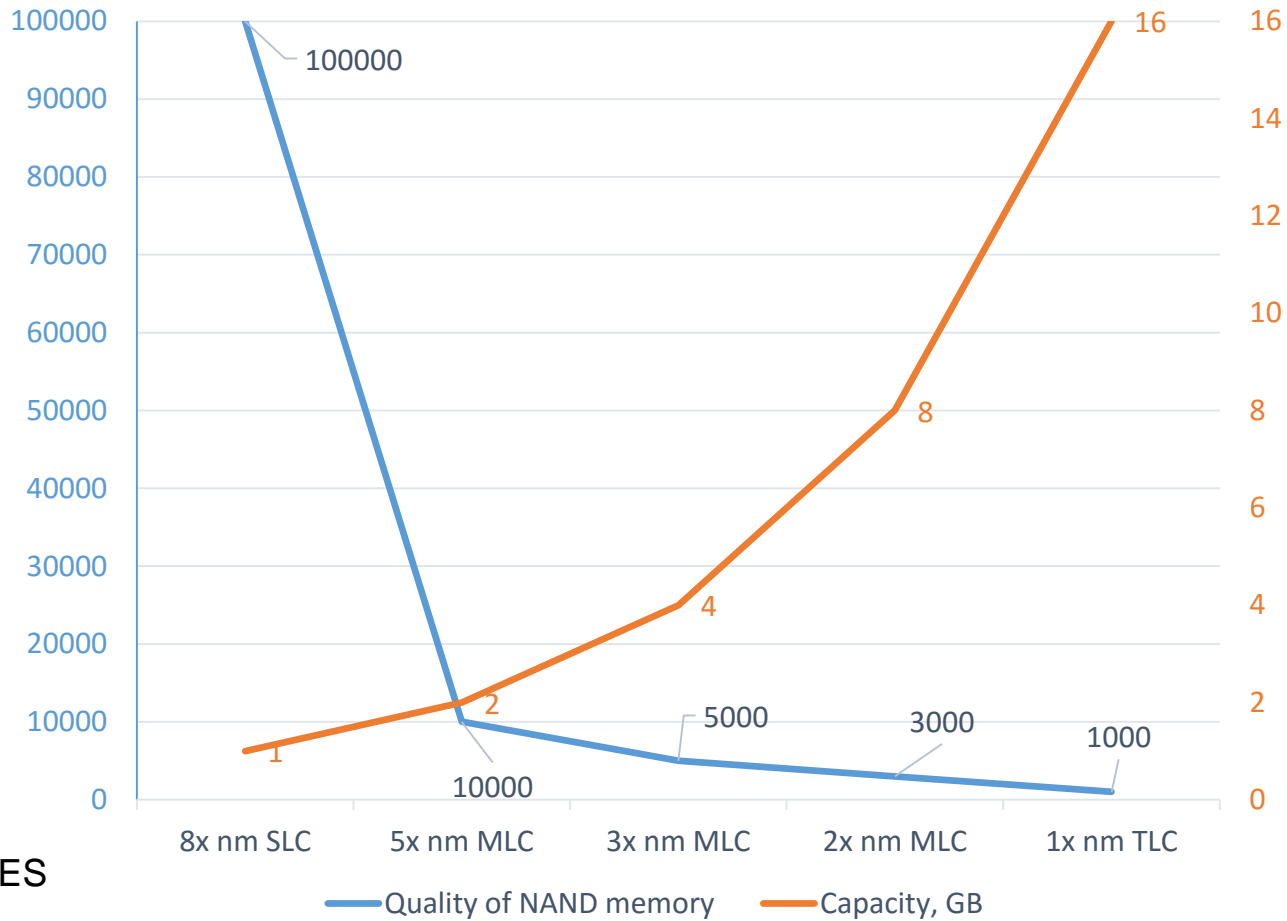
- USB pendrives
- Smartphones
- Tablets
- Memory cards (SD, microSD, CF, etc)
- Solid State Drives
- Digital voice recorders
- GPS devices
- Other devices

# NAND & eMMC CHIPS

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



# NAND MEMORY ENDURANCE



## ERASE CYCLES

SLC NAND – up to 100'000

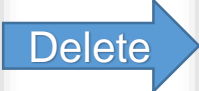
MLC NAND – up to 10'000

TLC NAND – up to 1500

# DELETE OPERATION ON FILE SYSTEM LAYER

OLD **INVISIBLE** VERSION OF DATA ON PHYSICAL NAND LAYER

2E 20 20 20	20 20 20 20	20 20 20 20	20 20 20 20	00 30 7B 38	...
A4 48 A4 48	01 00 7C 38	A4 48 DC 92	00 00 00 00	...	...
2E 2E 20 20	20 20 20 20	20 20 20 10	00 30 7B 38	...	...
A4 48 A4 48	00 00 7C 38	A4 48 00 00	00 00 00 00	...	...
41 41 00 6C	00 63 00 6F	00 72 00 0F	00 48 6D 00	...	...
69 00 63 00	72 00 6F 00	00 00 00 00	FF FF FF FF	...	...



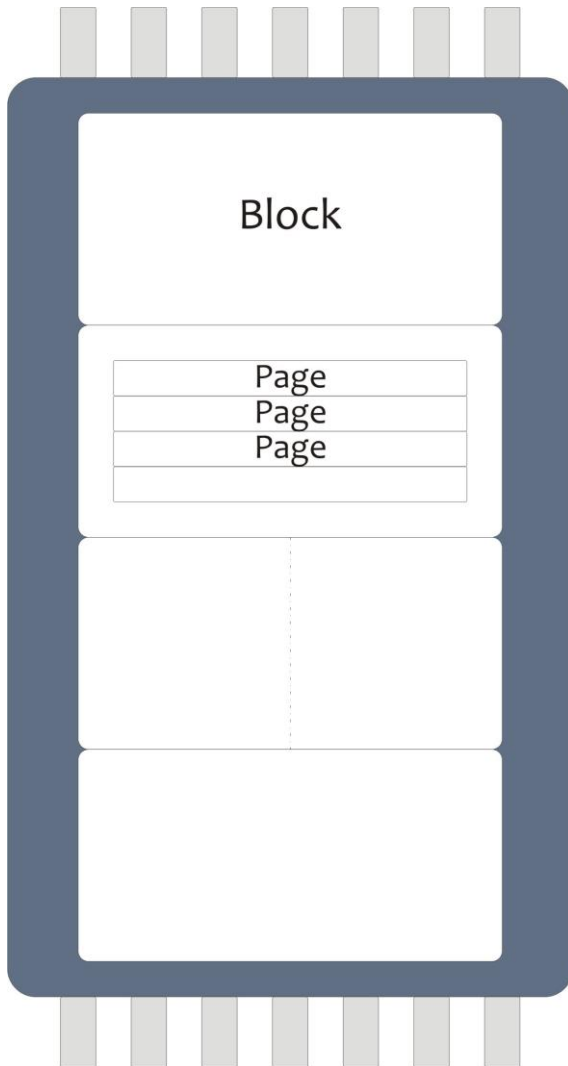
<b>E5</b> 2E 20 20	20 20 20 20	20 20 20 10	00 30 7B 38	...	...
<b>E5</b> A4 48 A4	48 01 00 7C 38	A4 48 DC 92	00 00 00 00	...	...
<b>E5</b> 2E 2E 20	20 20 20 20	20 20 20 10	00 30 7B 38	...	...
<b>E5</b> A4 48 A4	48 00 00 7C 38	A4 48 00 00	00 00 00 00	...	...
<b>E5</b> 41 00 6C	00 63 00 6F	00 72 00 0F	00 48 6D 00	...	...
<b>E5</b> 69 00 63	00 72 00 6F	00 00 00 00	FF FF FF FF	...	...
<b>E5</b> 4C 43 4F	52 4D 7E 31	20 20 20 10	00 33 7B 38	...	...
<b>E5</b> A4 48 A4	48 01 00 09 80	48 47 DD 92	00 00 00 00	...	...
<b>E5</b> FF 68 00	00 00 FF FF FF	FF FF FF 0F	00 8A FF FF	...	...
<b>E5</b> FF FF FF	FF FF FF FF	FF FF 00 00	FF FF FF FF	...	...
<b>E5</b> 02 28 00	65 00 63 00	63 00 34 00	0F 00 8A 32 00	...	...
<b>E5</b> 62 00 29	00 5F 00 34	00 2E 00 00	00 62 00 63 00	...	...
<b>E5</b> 01 41 00	6E 00 79 00	6B 00 61 00	0F 00 8A 33 00	...	...
<b>E5</b> 37 00 33	00 5F 00 34	00 33 00 00	00 32 00 30 00	...	...
<b>E5</b> 41 4E 59	4B 41 33 7E 31	42 43 48 20	00 70 7B 38	...	...
<b>E5</b> A4 48 B1	48 01 00 FA A6	6B 47 EB 92	51 06 00 00	...	...
<b>E5</b> 00 00 FF	FF FF FF FF	FF FF 00 00	FF FF FF FF	...	...
<b>E5</b> 41 00 6E	00 79 00 6B	00 61 00 0F	00 6A 33 00	...	...
<b>E5</b> 37 00 33	00 5F 00 34	00 33 00 00	00 32 00 30 00	...	...
<b>E5</b> 41 4E 59	4B 41 33 7E 32	42 43 48 20	00 75 7B 38	...	...
<b>E5</b> A4 48 A4	48 01 00 41 65	C9 46 EC 92	A4 0B 00 00	...	...
<b>E5</b> 41 43 00	68 00 69 00	70 00 73 00	0F 00 33 42 00	...	...
<b>E5</b> 61 00 6E	00 6B 00 00 00	FF FF 00 00	FF FF FF FF	...	...
<b>E5</b> 43 48 49	50 53 42 7E 31	20 20 20 10	00 79 7B 38	...	...
<b>E5</b> A4 48 A4	48 01 00 19 B5	28 48 ED 92	00 00 00 00	...	...
<b>E5</b> 42 62 00	63 00 68 00	00 00 FF FF 0F	00 6F FF FF	...	...
<b>E5</b> FF FF FF	FF FF FF FF	FF FF 00 00	FF FF FF FF	...	...
<b>E5</b> 01 44 00	33 00 34 00	36 00 39 00	0F 00 6F 5F 00	...	...
<b>E5</b> 34 00 31	00 36 00 30	00 5F 00 00	00 38 00 2E 00	...	...
<b>E5</b> 44 33 34	36 39 5F 7E 31	42 43 48 20	00 9A 7B 38	...	...
<b>E5</b> A4 48 A4	48 01 00 4A 63	66 45 F6 92	C8 0B 00 00	...	...

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.



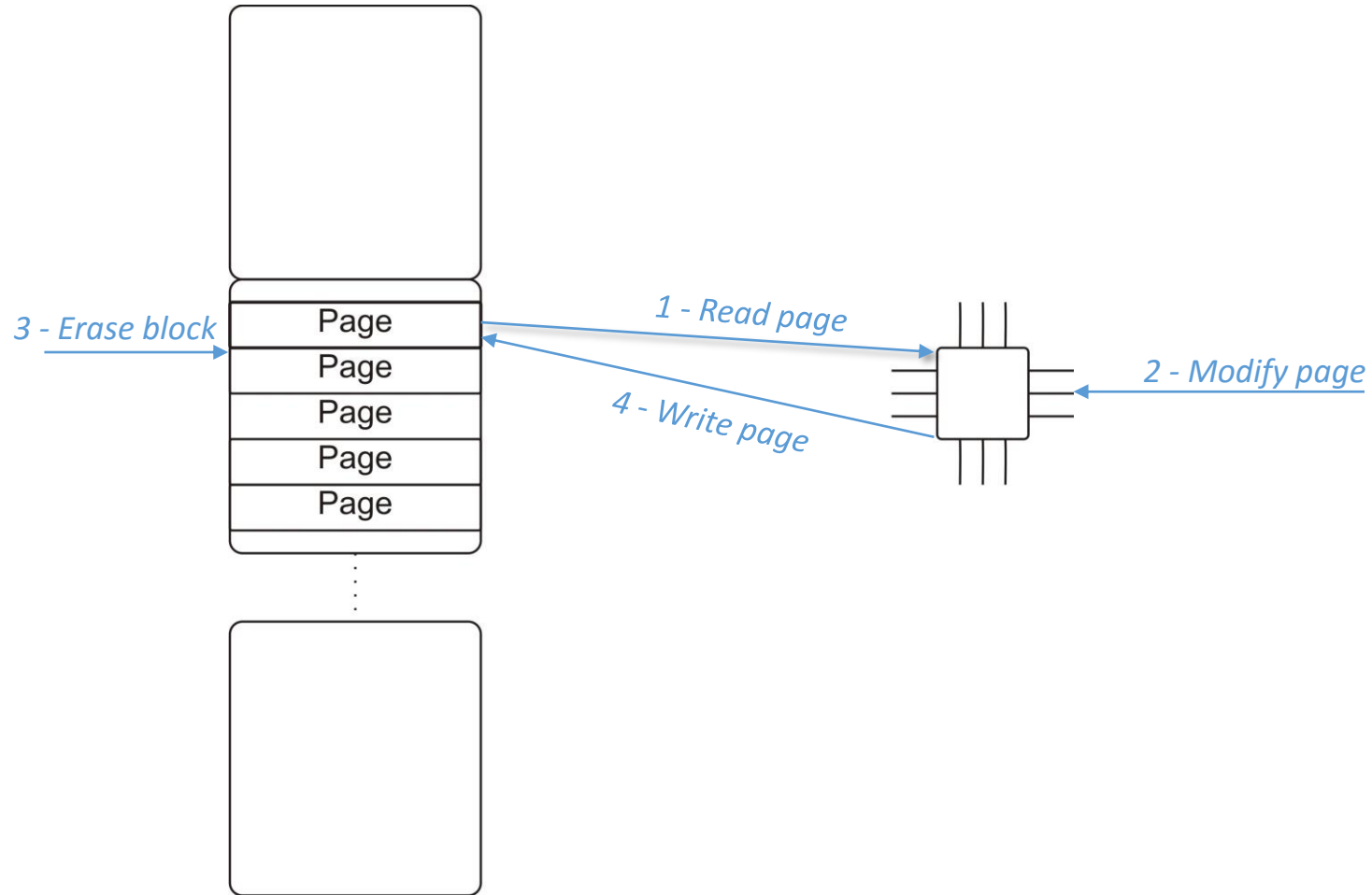
# PHYSICAL STRUCTURE OF NAND MEMORY



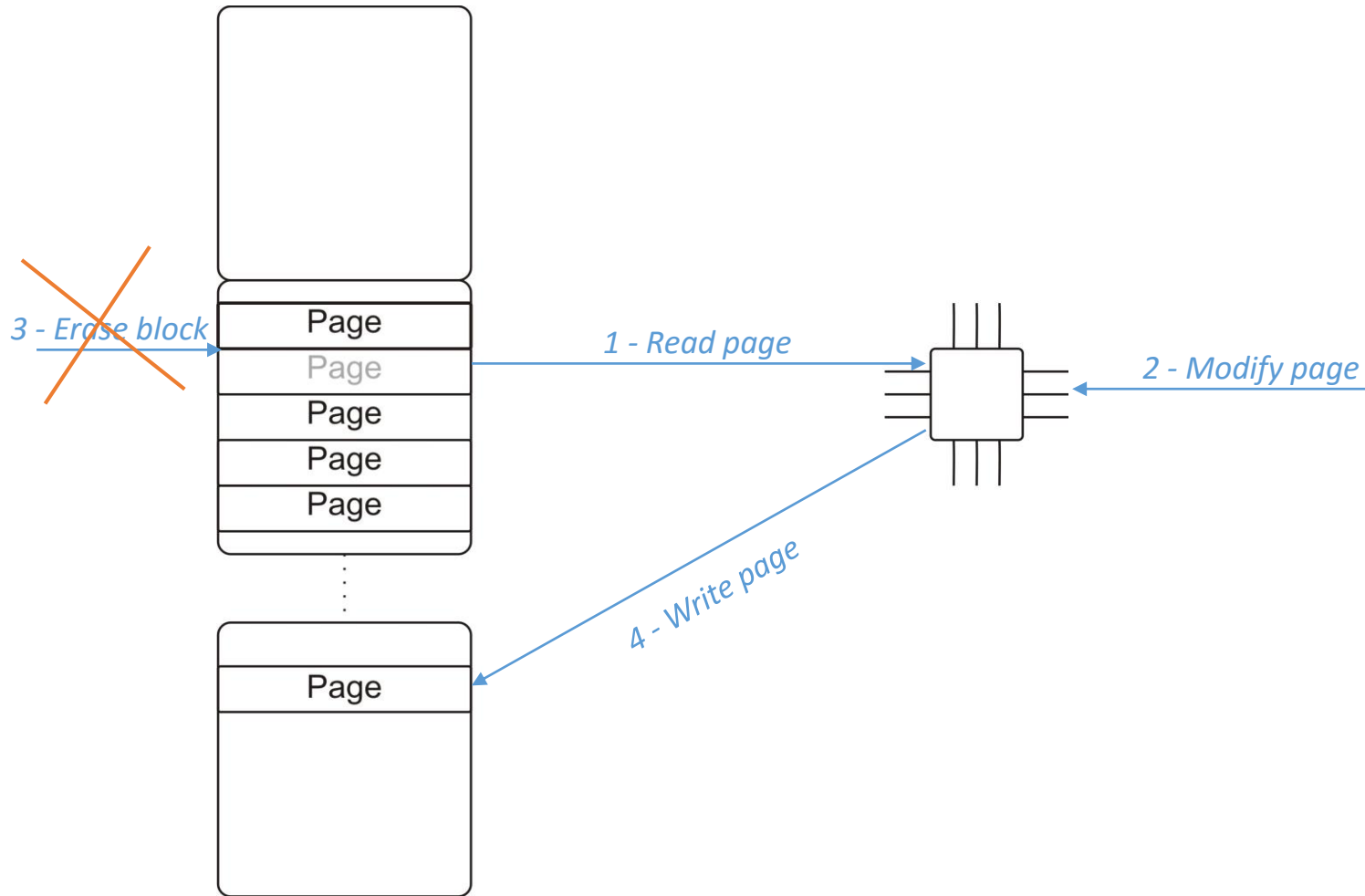
Block is a minimal unit of ERASE operation

Page is a minimal unit of READ/WRITE operation

# DATA MODIFICATION IN NAND. IN THEORY



# DATA MODIFICATION IN NAND. ON PRACTISE





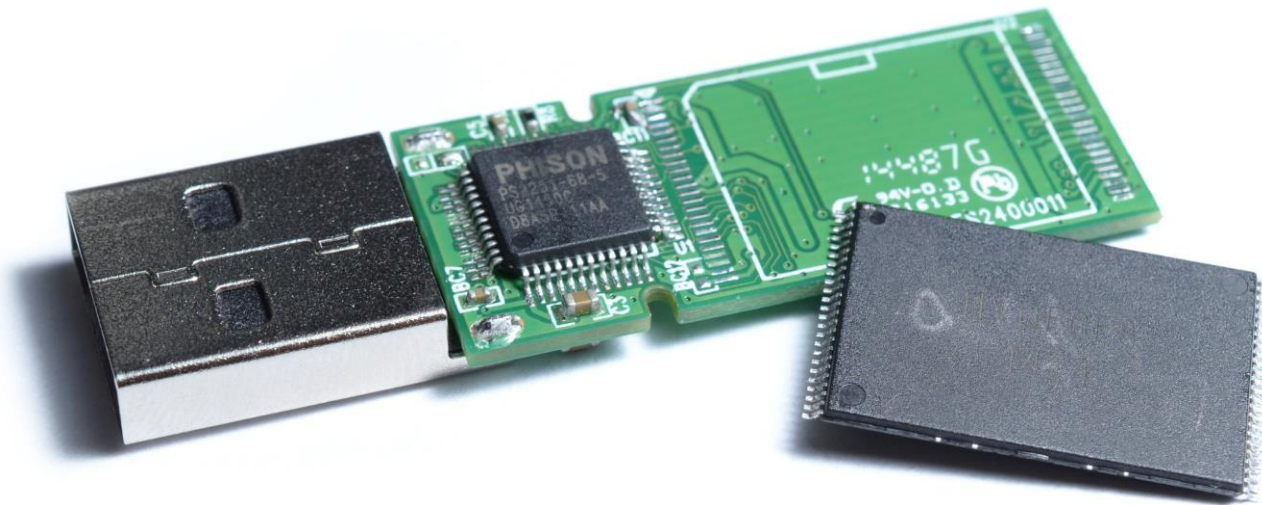
# CASE STUDY

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

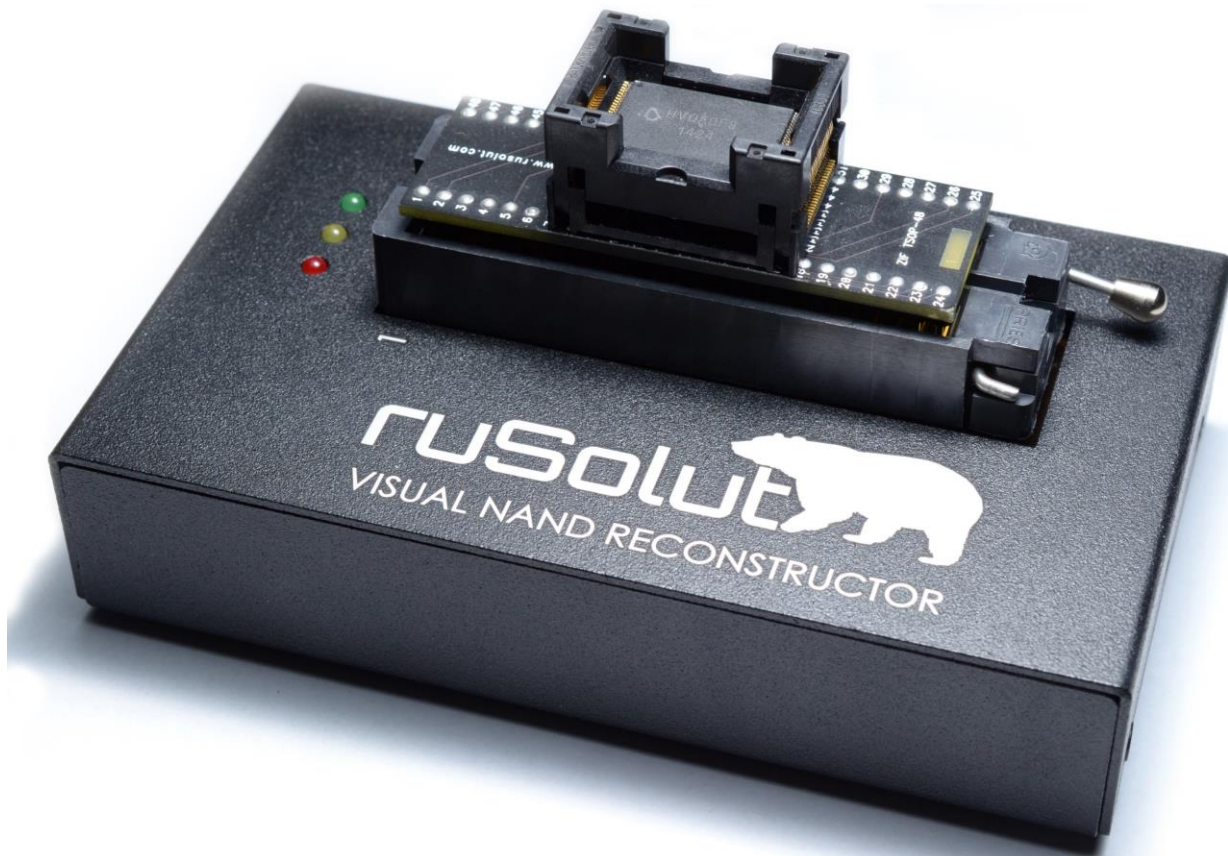
**Evidence collected:** Pendrive where he has probably copied stolen files

**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.



# CHIP-OFF NAND IMAGE EXTRACTION PROCESS



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

The screenshot displays the Visual NAND Reconstructor software interface, which is used for converting physical NAND flash images into logical images. The interface is divided into several main sections:

- Workspace:** Contains a workflow diagram with the following steps: **Phy image** (0) → **Inversion** (0) → **Pair** (0) → **Markers table** (0) → **Arrange** (0) → **Data area** (0). A **Markers table** (0) block is also shown below the main flow.
- Parameters:** A configuration panel for the selected element, including:
  - Enter filter string
  - Element: 0
  - Identifier: 0
  - List creator: ReCreate
  - Translation ta...: ReCreate
  - List creator by markers: Edit structure
  - Bank structure: Bank
  - Bank position: [Dropdown]
  - Block structure: Block
  - LBN position: 514,515
  - Header posi...: 512
  - Test1 position: [Dropdown]
  - Test2 position: 516,517
  - Page structure: Page
  - LPN position: 513
  - Commands: 10 ..
- Data area 0:** A file explorer view showing the contents of the logical image. The root directory contains a **Dump** folder with a list of files and folders, including:
  - 003.jpg
  - 0309
  - 230309
  - CORE
  - DIAMOND
  - ELPIDA
  - epexergasias
  - foto\_watch
  - KOTIS
  - Recycled
  - SUUNTO
  - EEPA
  - FAT0
  - FAT1

The interface also includes a toolbar with various functions like **Delete**, **Copy**, **Add physical images**, **Open physical images**, **Insert area**, **Skip area**, **Cut area**, **Remove bad columns**, **Show table**, and **Grid**. A sidebar on the left provides **Elements** and **Block list operations**, including **Reader**, **Physical image**, **ECC**, **Inversion**, **XOR**, **Pair**, **Separate**, **Unite**, **Rotate**, **Offsets**, **Arrange blocks**, **Data area**, and **Edit**, **Bit verifier**.

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

Visual NAND Reconstructor

Case Navigator Dump viewer Hex viewer

Hex view Bitmap view Structure view Records view Save all Save selected

Markers table 0 Workspace

Use	Bank	LBN	Header	Test2	Address	LB	RB
<input checked="" type="checkbox"/>	00	1000	FF	FFFF	0004C50000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1001	50	FFFF	00152C4000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1002	50	FFFF	00148F8000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1003	50	FFFF	000858C000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1004	50	FFFF	0007590000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1005	50	FFFF	001D850000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1006	50	FFFF	001C2A8000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1007	50	FFFF	0013A04000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1008	50	FFFF	001F950000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1009	50	FFFF	0017C88000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	100A	50	FFFF	001C488000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	100B	50	FFFF	000BD3C000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	100C	FF	FFFF	0004CD4000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	100D	FF	FFFF	000ECA0000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	100E	FF	FFFF	001C434000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	100F	FF	FFFF	001D958000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1010	FF	FFFF	0002520000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1011	FF	FFFF	001C224000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1012	FF	FFFF	00058B0000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1013	FF	FFFF	000A818000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1014	FF	FFFF	0000CE4000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1015	50	FFFF	00158F4000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1016	50	FFFF	0016A7C000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1017	50	FFFF	001DE80000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1018	50	FFFF	001F740000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1019	FF	FFFF	0013350000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	101A	50	FFFF	001BD90000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	101B	50	FFFF	0012D20000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	101C	50	FFFF	0003C54000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	101D	50	FFFF	0006300000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	101E	50	FFFF	00099A8000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	101F	50	FFFF	000EA9C000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1020	50	FFFF	0006618000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1021	50	FFFF	001E00C000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1022	50	FFFF	00170AC000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1023	50	FFFF	00141C0000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1024	50	FFFF	001EBE8000	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	00	1025	50	FFFF	001CBF0000	<input type="checkbox"/>	<input type="checkbox"/>

Block markers

LPN	Address
FF	0004C50000
FF	0004C50210
FF	0004C50420
FF	0004C50630
FF	0004C50840
FF	0004C50A50
FF	0004C50C60
FF	0004C50E70
FF	0004C51080
FF	0004C51290
FF	0004C514A0
FF	0004C516B0
FF	0004C518C0
FF	0004C51AD0
FF	0004C51CE0
FF	0004C51EF0
FF	0004C52100
FF	0004C52310
FF	0004C52520
FF	0004C52730
FF	0004C52940
FF	0004C52B50
FF	0004C52D60
FF	0004C52F70
FF	0004C53180
FF	0004C53390
FF	0004C535A0
FF	0004C537B0
FF	0004C539C0
FF	0004C53BD0
FF	0004C53DE0
FF	0004C53FF0
FF	0004C54200
FF	0004C54410
FF	0004C54620
FF	0004C54830
FF	0004C54A40
FF	0004C54C50

Page markers


```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0004C50000 FA BE 00 7C BF 00 7A B9 00 01 FC 0E 1F 0E 07 F3
0004C50010 A5 EA 16 7A 00 00 BB BE 7B 33 C9 80 3F 80 75 06
0004C50020 FE C5 8B F3 EB 07 80 3F 00 75 02 FE C1 83 C3 10
0004C50030 81 FB FE 7B 72 E5 83 F9 04 74 0B 81 F9 03 01 74
0004C50040 0A BB A5 7A EB 2C BB 87 7A EB 27 8B 4C 02 8B 14
0004C50050 B8 01 02 B8 00 7C CD 13 73 05 EB BC 7A EB 13 2E
0004C50060 B1 FE 7D 3D 55 AA 74 05 BB BC 7A EB 05 EA 00 7C
0004C50070 00 00 2E 8A 07 3C 00 74 0C 53 BB 07 00 B4 0E CD
0004C50080 10 5B 43 EB ED EB FE 4E 6F 20 62 6F 6F 74 61 62
0004C50090 6C 65 20 70 61 72 74 69 74 6F 6E 20 69 6E 20 74
0004C500A0 61 62 6C 65 00 49 6E 76 61 6C 69 64 20 50 61 72
0004C500B0 74 69 74 6F 6E 20 74 61 62 6C 65 00 49 6E 76 61
0004C500C0 6C 69 64 20 6F 72 20 64 61 6D 61 67 65 64 20 42
0004C500D0 6F 6F 74 61 62 6C 65 20 70 61 72 74 69 74 69 6F
0004C500E0 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C500F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C501A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C501B0 00 00 00 00 00 00 00 00 00 BF 63 39 C6 00 00 01
0004C501C0 01 00 06 0F E0 5F 20 00 00 E0 BF 1E 00 00 00
0004C501D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C501E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C501F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0004C50200 00 00 EF FF 00 00 4E DD E8 5A 1A AA 26 7F E3 74
..na..N3mZ.Ga rt
```

Position 0x0 from 0x800

Address: 80019456 Selected:

Event log explorer

Last active selection: address 80019456 selected



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.

The screenshot displays the Visual Nand Reconstructor interface. The main window shows a dump of a FAT file system. The left pane contains a 'Block markers' table with columns for Use, Bank, LBN, Header, Test2, Address, LB, and RB. The right pane shows a 'Page markers' table with columns for LPN and Address. The central pane displays a hex dump of the data, with the following text visible:

```
0002310840 2E 20 20 20 20 20 20 20 20 20 20 20 10 00 1E 2C 98
0002310850 9A 3A 9A 3A 00 00 2D 98 9A 3A 27 08 00 00 00 00
0002310860 2E 2E 20 20 20 20 20 20 20 20 20 10 00 1E 2C 98
0002310870 9A 3A 9A 3A 00 00 2D 98 9A 3A 00 00 00 00 00 00
0002310880 42 A1 03 A3 03 20 00 2E 00 6D 00 0F 00 18 64 00
0002310890 62 00 00 00 FF FF FF FF FF FF 00 00 FF FF FF FF
00023108A0 01 45 00 6C 00 70 00 69 00 64 00 0F 00 18 61 00
00023108B0 20 00 32 00 30 00 30 00 32 00 00 00 95 03 A5 03
00023108C0 45 4C 50 49 44 41 7E 31 4D 44 42 20 00 23 2C 98
00023108D0 9A 3A A3 3C 00 00 1A 72 A3 3C 28 08 00 90 DB 01
00023108E0 42 20 00 74 00 65 00 73 00 74 00 0F 00 27 2E 00
00023108F0 6D 00 64 00 62 00 00 00 FF FF 00 00 FF FF FF FF
0002310900 01 95 03 A4 03 99 03 9A 03 95 03 0F 00 27 A4 03
0002310910 95 03 A3 03 20 00 95 03 A5 03 00 00 A1 03 A9 03
0002310920 84 92 88 89 84 92 7E 31 4D 44 42 20 00 70 30 98
0002310930 9A 3A 29 3C 00 00 AF 56 29 3C F7 0E 00 00 0D 04
0002310940 42 2E 00 6D 00 64 00 62 00 00 00 0F 00 88 FF FF
0002310950 FF FF FF FF FF FF FF FF FF FF 00 00 FF FF FF FF
0002310960 01 95 03 A4 03 99 03 9A 03 95 03 0F 00 88 A4 03
0002310970 95 03 A3 03 20 00 95 03 A5 03 00 00 A1 03 A9 03
0002310980 84 92 88 89 84 92 7E 32 4D 44 42 20 00 AB F2 4D
0002310990 04 3B 83 3C 00 00 71 53 83 3C EB 20 00 80 D7 00
00023109A0 43 B1 03 C0 03 BF 03 B3 03 32 00 0F 00 EA 30 00
00023109B0 31 00 30 00 2E 00 78 00 6C 00 00 00 73 00 00 00
00023109C0 00 8F 8E 82 32 30 31 30 58 4C 53 20 00 9C 68 75
00023109D0 37 3A 98 3C 00 00 6B A0 42 3C 33 02 00 A2 63 00
00023109E0 42 A1 03 A3 03 20 00 2E 00 6C 00 0F 00 58 64 00
00023109F0 62 00 00 00 FF FF FF FF FF FF 00 00 FF FF FF FF
0002310A00 01 45 00 6C 00 70 00 69 00 64 00 0F 00 58 61 00
0002310A10 20 00 32 00 30 00 30 00 32 00 00 00 95 03 A5 03
0002310A20 45 4C 50 49 44 41 7E 31 4C 44 42 20 00 49 FC 71
0002310A30 A3 3C A3 3C 00 00 FD 71 A3 3C 3E 02 00 00 00 00
0002310A40 FD 2F EF BE 00 00 A2 2B FA B2 F9 16 B2 E7 28 9C
```

The right pane shows file metadata for 'ELPIDA.MDB' and 'ELPIDA.LDB'. The metadata includes fields such as Plane, Bank, Block, Page, Data area, Entry, Spare area, ECC, reserved space, Filename, File size, Extension, File Datestamp, File Timestamp, First file cluster num, LBN, test1, File attributes, and LPN.



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.

The screenshot displays the Visual Nand Reconstructor application. The main window is titled "Dump viewer" and shows a hex dump of data. The interface includes several panels:

- Block markers:** A table with columns for Use, Bank, LBN, Header, Test2, Address, LB, and RB. It lists various blocks, with some highlighted in blue.
- Page markers:** A table with columns for LPN and Address, listing page addresses.
- Hex viewer:** The central area showing hex data in columns (00-0F) and rows. A red box highlights a specific row of data.
- File attributes:** A panel on the right showing details for a file, including filename, extension, file attributes, file timestamp, and file size.
- File attributes table:** A table on the right showing a list of file attributes and their values, such as "Filename (E5 - deleted; 00 - unallocated) (1)", "Extension (3)", "File attributes (1)", "File Timestamp (2)", "File size (4)", etc.

The status bar at the bottom indicates the current selection: "Address: 36772032 Selected: 0".



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

Visual Nand Reconstructor

Case Navigator Dump viewer Hex viewer Structure viewer

Hex view Bitmap view Structure view Records view Save all Save selected

Markers table 0 Workspace

Use	Bank	LBN	Header	Test2	Address	LB	RB	LPN	Address
<input checked="" type="checkbox"/>	01	13A9	50	FFFF	003EC70000			4E	0002310000
<input checked="" type="checkbox"/>	01	13AA	FF	FFFF	0028488000			FF	0002310210
<input checked="" type="checkbox"/>	01	13AB	50	FFFF	0028A34000			FF	0002310420
<input checked="" type="checkbox"/>	01	13AC	FF	FFFF	002EB24000			FF	0002310630
<input checked="" type="checkbox"/>	01	13AD	FF	FFFF	002349C000			D0	0002310840
<input checked="" type="checkbox"/>	01	13AE	FF	FFFF	002C160000			D1	0002310A50
<input checked="" type="checkbox"/>	01	13AF	50	FFFF	003DA64000			D2	0002310C60
<input checked="" type="checkbox"/>	01	13B0	FF	FFFF	002D684000			D3	0002310E70
<input checked="" type="checkbox"/>	01	13B1	FF	FFFF	003F21C000			D4	0002311080
<input checked="" type="checkbox"/>	01	13B2	FF	FFFF	003D9E0000			D5	0002311290
<input checked="" type="checkbox"/>	01	13B3	FF	FFFF	0034878000			D6	00023114A0
<input checked="" type="checkbox"/>	01	13B4	FF	FFFF	0024414000			D7	00023116B0
<input checked="" type="checkbox"/>	01	13B5	FF	FFFF	0034B0C000			D0	00023118C0
<input checked="" type="checkbox"/>	01	13B6	FF	FFFF	0026724000			D1	0002311AD0
<input checked="" type="checkbox"/>	01	13B7	FF	FFFF	003D3B0000			D2	0002311CE0
<input checked="" type="checkbox"/>	01	13B8	FF	FFFF	0031A94000			D3	0002311EF0
<input checked="" type="checkbox"/>	01	13B9	FF	FFFF	003BD00000			D4	0002312100
<input checked="" type="checkbox"/>	01	13BA	FF	FFFF	003D6C8000			D5	0002312310
<input checked="" type="checkbox"/>	01	13BB	50	FFFF	003D95C000			D6	0002312520
<input type="checkbox"/>	00	1000	52	FFFF	0001BD8000			D7	0002312730
<input type="checkbox"/>	00	1041	52	FFFF	0002310000			F0	0002312940
<input type="checkbox"/>	00	1065	52	FFFF	0017760000			F1	0002312B50
<input type="checkbox"/>	00	1077	52	FFFF	0017448000			F2	0002312D60
<input type="checkbox"/>	00	13D9	50	FFFF	0015B04000			F3	0002312F70
<input type="checkbox"/>	00	31D9	50	FFFF	00049BC000			F4	0002313180
<input type="checkbox"/>	00	FFFF	4D	FFFF	0000528000			F5	0002313390
<input type="checkbox"/>	00	FFFF	50	FFFF	0002CD0000			F6	00023135A0
<input type="checkbox"/>	00	FFFF	FF	FFFF	000C57C000			F7	00023137B0
<input type="checkbox"/>	00	FFFF	FF	FFFF	0011568000			F8	00023139C0
<input type="checkbox"/>	00	FFFF	FF	FFFF	0013B90000			F9	0002313BD0
<input type="checkbox"/>	00	FFFF	4D	FFFF	0015E1C000			FA	0002313DE0
<input type="checkbox"/>	00	FFFF	FF	FFFF	002094C000			FB	0002313FF0
<input type="checkbox"/>	01	13B0	52	FFFF	0027E58000			FC	0002314200
<input type="checkbox"/>	01	FFFF	4D	FFFF	0021630000			FD	0002314410
<input type="checkbox"/>	01	FFFF	4D	FFFF	002EF44000			FE	0002314620
<input type="checkbox"/>	01	FFFF	FF	FFFF	0030CA8000			FF	0002314830
<input type="checkbox"/>	01	FFFF	FF	FFFF	0033F30000			DD	0002314A40
<input type="checkbox"/>	01	FFFF	FF	FFFF	003513C000			D1	0002314C50
<input type="checkbox"/>	01	FFFF	FF	FFFF	003513C000			D1	0002314C50

Block markers: 0002314A40, 0002314A50, 0002314A60, 0002314A70, 0002314A80, 0002314A90, 0002314AA0, 0002314AB0, 0002314AC0, 0002314AD0, 0002314AE0, 0002314AF0, 0002314B00, 0002314B10, 0002314B20, 0002314B30, 0002314B40, 0002314B50, 0002314B60, 0002314B70, 0002314B80, 0002314B90, 0002314BA0, 0002314BB0, 0002314BC0, 0002314BD0, 0002314BE0, 0002314BF0, 0002314C00, 0002314C10, 0002314C20, 0002314C30, 0002314C40

Page markers: 4E, FF, D0, D1, D2, D3, D4, D5, D6, D7, D0, D1, D2, D3, D4, D5, D6, D7, F0, F1, F2, F3, F4, F5, F6, F7, F8, F9, FA, FB, FC, FD, FE, FF, DD, D1

Address: 36784704 Selected: 0

Hex view: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  
2E 20 20 20 20 20 20 20 20 20 20 10 00 1E 2C 98  
9A 3A 9A 3A 00 00 2D 98 9A 3A 27 08 00 00 00 00  
2E 20 20 20 20 20 20 20 20 20 20 10 00 1E 2C 98  
9A 3A 9A 3A 00 00 2D 98 9A 3A 00 00 00 00 00 00  
42 A1 03 A9 03 20 00 2E 00 6D 00 0F 00 18 64 00  
62 00 00 00 FF FF FF FF FF FF 00 00 FF FF FF FF  
01 45 00 6C 00 70 00 69 00 64 00 0F 00 18 61 00  
20 00 32 00 30 00 30 00 32 00 00 00 95 03 A5 03  
45 4C 50 49 44 41 7E 31 4D 44 42 20 00 23 2C 98  
9A 3A A3 3C 00 00 A8 72 A3 3C 28 08 00 90 DB 01  
42 20 00 74 00 65 00 73 00 74 00 0F 00 27 2E 00  
6D 00 64 00 62 00 00 00 FF FF 00 00 FF FF FF FF  
01 95 03 A4 03 99 03 9A 03 95 03 0F 00 27 A4 03  
95 03 A3 03 20 00 95 03 A5 03 00 00 A1 03 A9 03  
84 92 88 89 84 92 7E 31 4D 44 42 20 00 7D 04  
9A 3A 29 3C 00 00 AF 56 29 3C F7 0E 00 00 07 30  
42 2E 00 6D 00 64 00 62 00 00 00 0F 00 88 FF FF  
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  
81 95 03 A4 03 99 03 9A 03 95 03 0F 00 88 A4 03  
95 03 A3 03 20 00 95 03 A5 03 00 00 A1 03 A9 03  
84 92 88 89 84 92 7E 32 4D 44 42 20 00 AB F2 4D  
04 3B 83 3C 00 00 71 53 83 3C EB 20 00 80 D7 00  
43 B1 03 C0 03 BF 03 B3 03 32 00 0F 00 EA 30 00  
31 00 30 00 2E 00 78 00 6C 00 00 00 73 00 00 00  
80 8F 8E 82 32 30 31 30 58 4C 53 20 00 9C 68 75  
37 3A 98 3C 00 00 6B A0 42 3C 33 02 00 A2 63 00  
42 A1 03 A9 03 20 00 2E 00 6C 00 0F 00 58 64 00  
62 00 00 00 FF FF FF FF FF FF 00 00 FF FF FF FF  
01 45 00 6C 00 70 00 69 00 64 00 0F 00 58 61 00  
20 00 32 00 30 00 30 00 32 00 00 00 95 03 A5 03  
45 4C 50 49 44 41 7E 31 4C 44 42 20 00 49 FC 71  
A3 3C A3 3C 00 00 A8 72 A3 3C 3E 02 40 00 00 00  
FD 2F EF BE 00 00 00 00 C9 E9 C4 8A 9C BC 48

Plane > Bank > Block > Page > Data area > Entry

- Filename (E5 - deleted; 00 - unallocated) (1) 0 - 0 1
- Filename (7) 1 - 7 7
- Extension (3) 8 - 10 3
- File attributes (1) 11 - 11 1
- reserved space (10) 12 - 21 10
- File Timestamp (2) 22 - 23 2
- File Timestamp (2) 24 - 25 2
- First file cluster num (2) 26 - 27 2
- File size (4) 28 - 31 4

Plane: 1107296256 as Plane  
Bank: 553649128  
Block: 540672 as Block  
Page: 528 as Page  
Data area: 512 as Data area  
Entry: 32  
Spare area: 16  
ECC: 10  
reserved space: 10  
Filename: 7  
File size: 4  
Extension: 3  
File Datestamp: 2  
File Timestamp: 2  
First file cluster num: 2  
LBN: 2  
test1: 2  
File attributes: 1  
Filename (E5 - deleted; 00 - unallocated): 1  
Header: 1  
LPN: 1

Position 0x7B1 from 0x800 Position 0x24 from 0x3FF

Event log explorer Last active selection: address 36784704 selected 0



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.

The screenshot displays the Visual Nand Reconstructor application interface. The main window is titled "Dump viewer" and shows a hex dump of data. The interface includes several panels:

- Case Navigator:** Contains icons for Hex view, Bitmap view, Structure view, Records view, Save all, and Save selected.
- Block markers:** A table with columns for Use, Bank, LBN, Header, Test2, Address, LB, and RB. It lists various memory blocks with their addresses and headers.
- Page markers:** A table with columns for LPN and Address, listing page numbers and their corresponding addresses.
- Hex Dump:** The central area showing a hex dump of data. The selected address is 36793152. The dump shows hex values and their corresponding ASCII characters, including "ELPIDA-1MDB" and "ELPIDA-1LDB".
- File Analysis Panel:** Located on the right, it shows a list of files with their attributes. The selected file is "Filename (E5 - deleted; 00 - unallocated) (1)". Other files listed include "Filename (7)", "Extension (3)", "File attributes (1)", "File Timestamp (2)", "First file cluster num (2)", and "File size (4)".
- File Properties Panel:** Located on the far right, it shows details for the selected file, including Plane, Bank, Block, Page, Data area, Entry, Spare area, ECC, reserved space, Filename, File size, Extension, File Datestamp, File Timestamp, First file cluster num, LBN, test1, File attributes, Filename (E5 - deleted; 00 - unallocated), Header, and LPN.



# 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.