Data Recovery from Aircraft Black Box

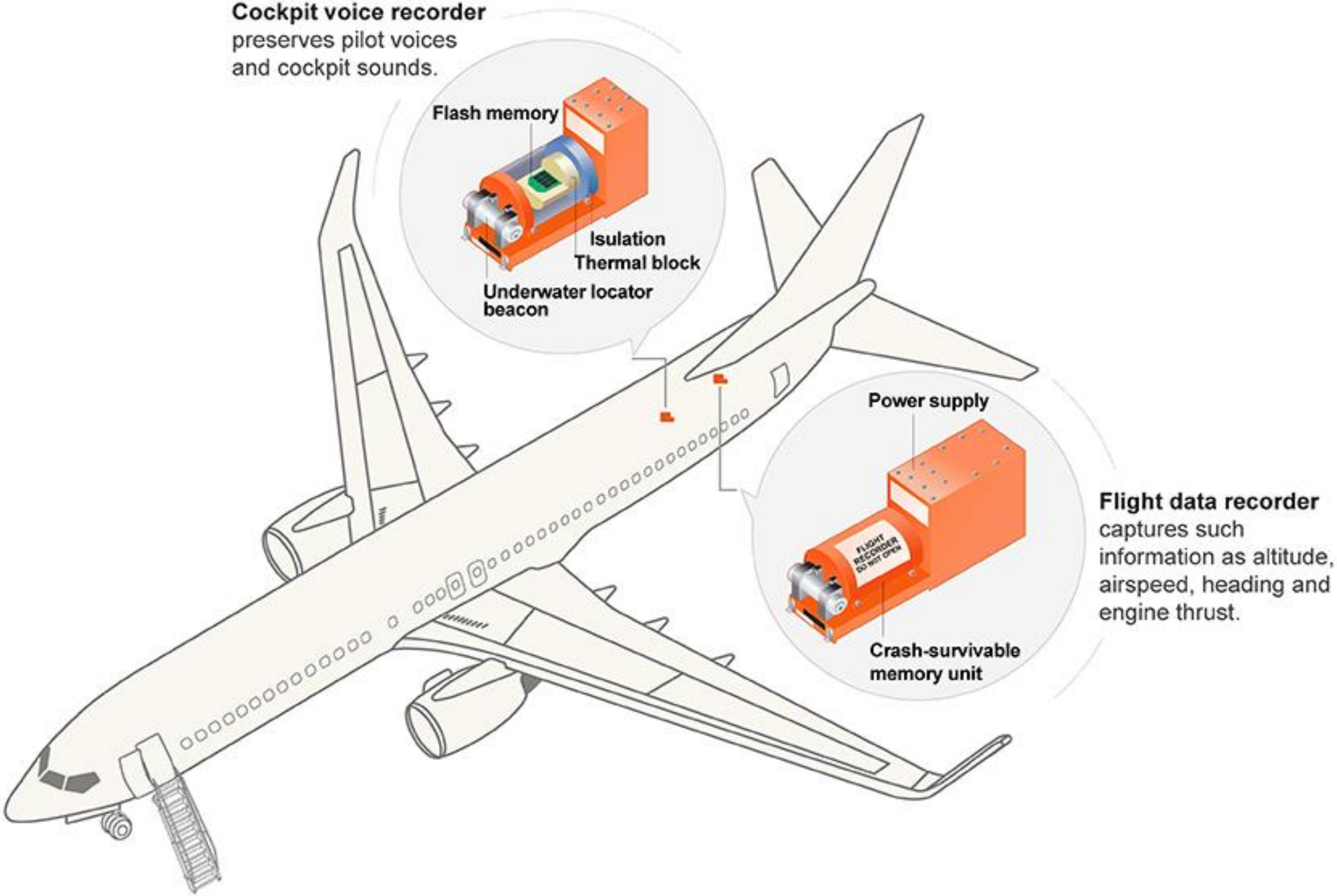
Michał Gmurek

ruSolut

June 5-8, 2023 | Wilmington, NC

Techno Security &
Digital Forensics
Conference

Data Recovery from Aircraft Black Box



Cockpit voice recorder preserves pilot voices and cockpit sounds.

Flash memory
Isulation
Thermal block
Underwater locator beacon

Flight data recorder captures such information as altitude, airspeed, heading and engine thrust.

Power supply
FLIGHT RECORDER DO NOT OPEN
Crash-survivable memory unit

D.T.MUX Sentinel™

Crash Protected System
from 32 to 128GB

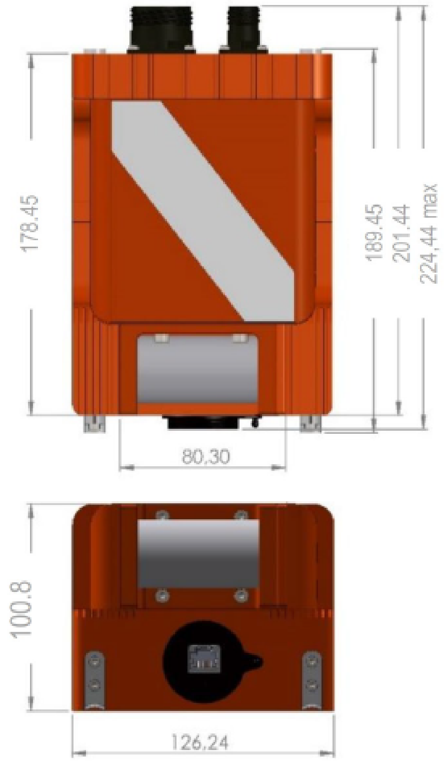
RTCA DO-160 vG TESTED

MILITARY MIL-STD 810G TESTED

Reference# SEN-XXX

MECHANICAL

	Specification	Remark
Size	189.5 (231.8 iRIPS /219.5 iEE) x 126.2 x 101 mm	D x W x H ± 1mm
Weight	≈ 3.30kg / 3.75kg ≈ 4.85kg	ED155/ ED112 iRIPS
Connectors	MIL-DTL-38999	Serie III
Mounting	ARINC 404	Customizable



ELECTRICAL

Input Voltage	28Vdc (16 to 36Vdc)
Power consumption	≈ 12 to 32 watts (28Vdc)
Power Interruption	≈ 200 to 800ms
Standard	MIL-STD-704F / DO-160

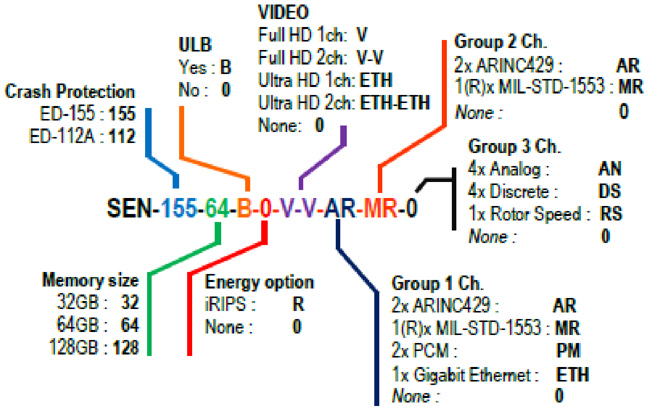
ENVIRONMENTAL

	Specification	Remark
Temperature	-40°C to 65°C	Operating
	-55°C to 90°C	Storage
Cooling	Passive	Convection
Humidity	95%	Non-Cond
Vibration	5Hz to 2KHz	6.29 g RMS
Shocks	20g 11ms	Operating
Acceleration	20g linear 3 axis	Operating
Altitude	+ 60,000 ft	Operating
Decompression	420Kpa/minute	Operating
MTBF	> 90,000 hours	Computed
EMI	DO-160	Rev G

STANDARD FUNCTIONALITY

	Specification
Gigabit Ethernet	Configuration/Control Data download and Streaming
Time synch	GPS Antenna input / Irig B / PTP v2
Voice	4x Audio channels
Recording	IRIG 106 Chapter 10 / DTMUX format
Sensors	Internal 3 Axis Gyro/ G force/ Pressure
COM port	RS-232 Configuration/Maintenance
Status	Status Led / Status output

SENTINEL PART NUMBER COMPOSITION



SEN-155-64-B-0-V-V-AR-MR-0

Crash Protection
ED-155 : 155
ED-112A : 112

Memory size
32GB : 32
64GB : 64
128GB : 128

ULB
Yes : B
No : 0

Energy option
iRIPS : R
None : 0

VIDEO
Full HD 1ch: V
Full HD 2ch: V-V
Ultra HD 1ch: ETH
Ultra HD 2ch: ETH-ETH
None: 0

Group 1 Ch.
2x ARINC429 : AR
1(R)x MIL-STD-1553 : MR
2x PCM : PM
1x Gigabit Ethernet : ETH
None : 0

Group 2 Ch.
2x ARINC429 : AR
1(R)x MIL-STD-1553 : MR
None : 0

Group 3 Ch.
4x Analog : AN
4x Discrete : DS
1x Rotor Speed : RS
None : 0

Environmental specifications

Environmental specifications

The equipment has been designed to meet the environmental specifications applicable to the installation limits as set forth in the version of RTCA/DO-160 in force at the time of certification.

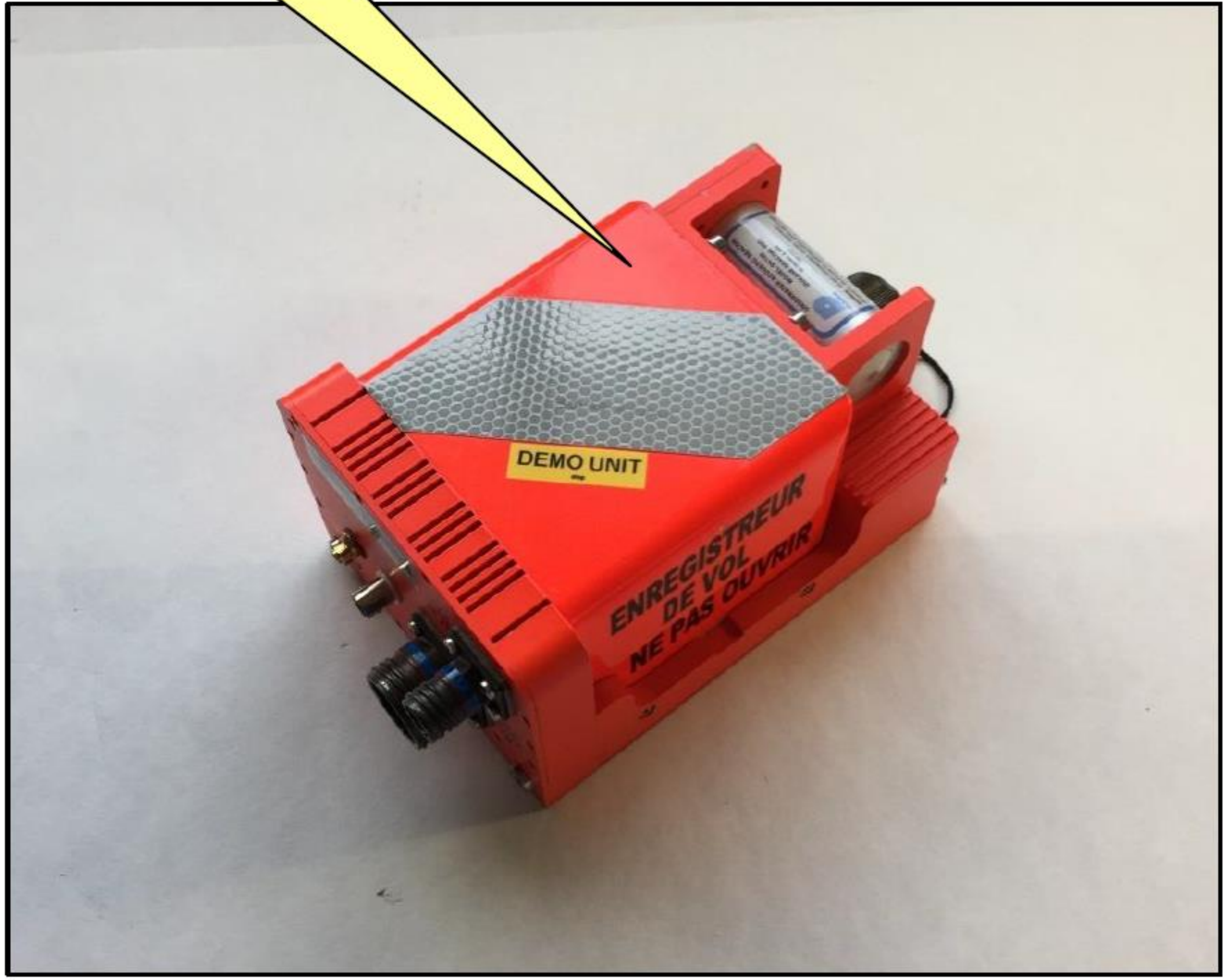
Sentinel Under High temperature fire test

Flight Recording Systems (ED-112), Survivability

- Impact: 3400 Gs, 6.5ms, All Axes
- Pin Penetration: 500 lb., 10 ft.(1/4 in. Pin)
- Static Crush: 5000 lb, 5 min All Axes
- Low Temp Fire: 260�C, during 10 hours
- High Temp Fire: 1,100� C, during 60 Min
- Sea Water Immersion: 30 Days
- Deep Sea Pressure: 20,000 ft., 24 Hrs.
- Fluid Immersion: Various Fluids, 48 Hrs.

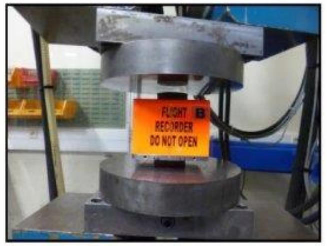
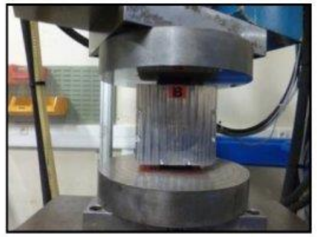
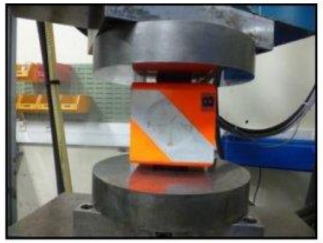
Qualification/Certification

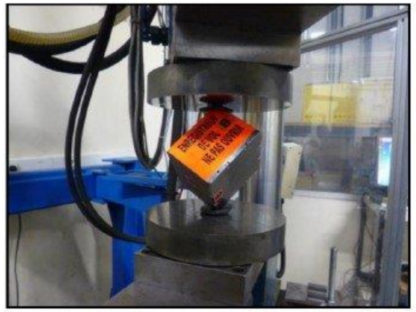
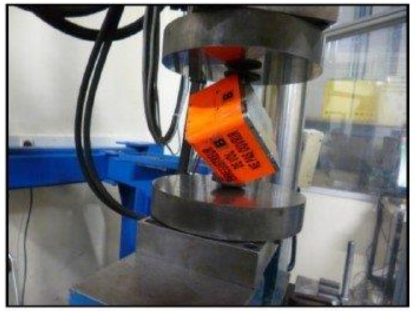
Sentinel "ED-112 type" meets the requirements as specified in the Minimum Operational Performance Specification (MOPS) for flight recording systems ED-112. The system also outperforms many of the crash survival requirements in the Minimum Operational Performance Specification for Crash Protected Airborne Recorder Systems ED-112.

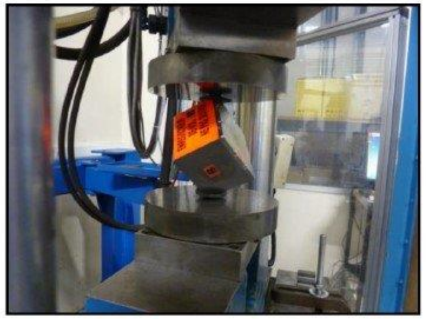
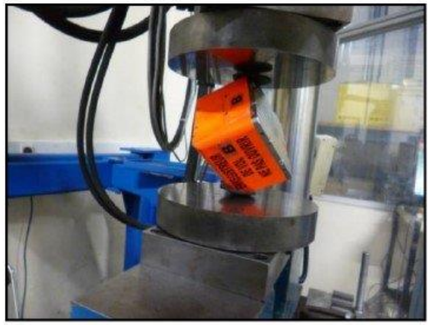


Crash Protected Memory Block

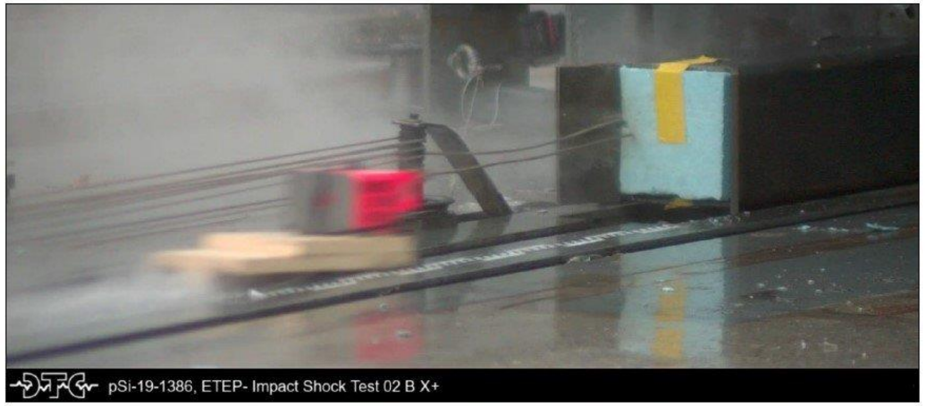
Hydraulic press test

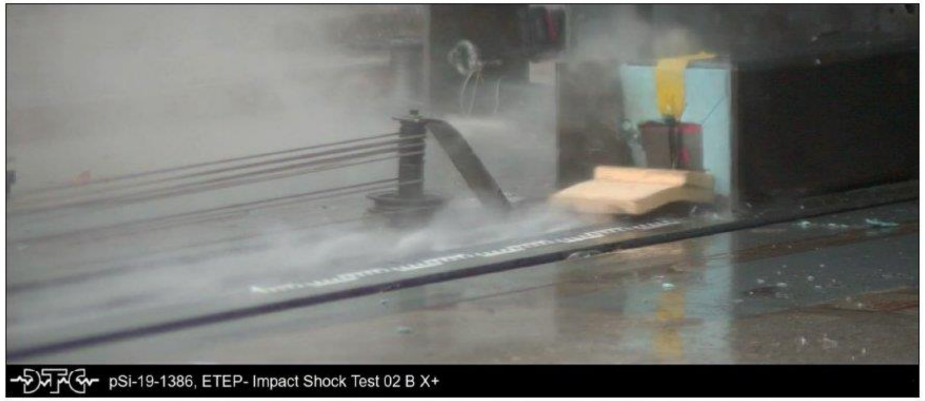
		

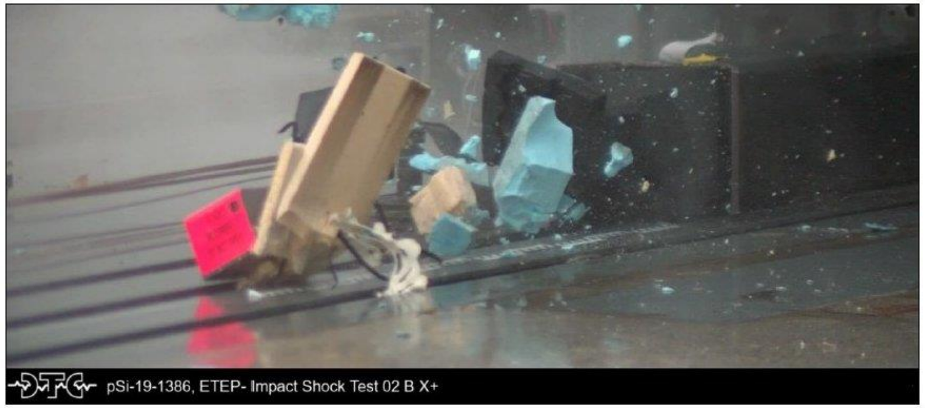
	
Diagonal 1	Diagonal 2

	
Diagonal 3	Diagonal 4

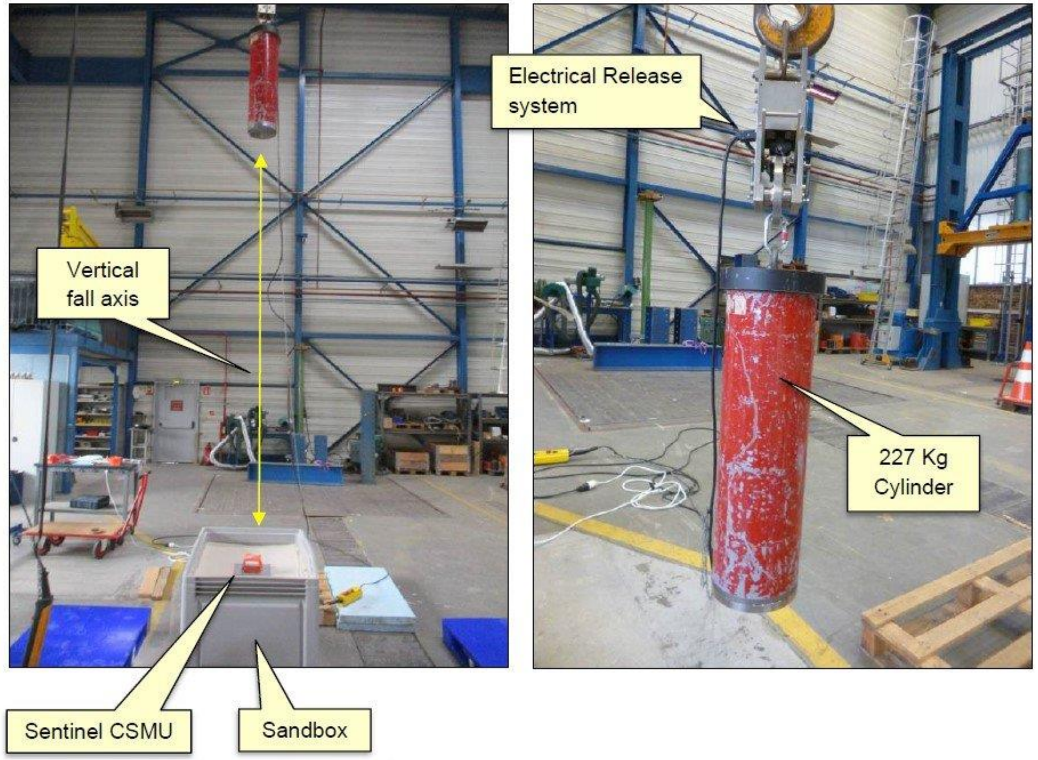
Crash test

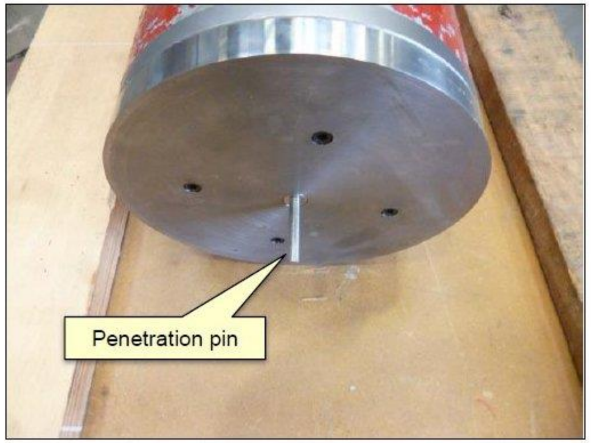

pSi-19-1386, ETEP- Impact Shock Test 02 B X+


pSi-19-1386, ETEP- Impact Shock Test 02 B X+

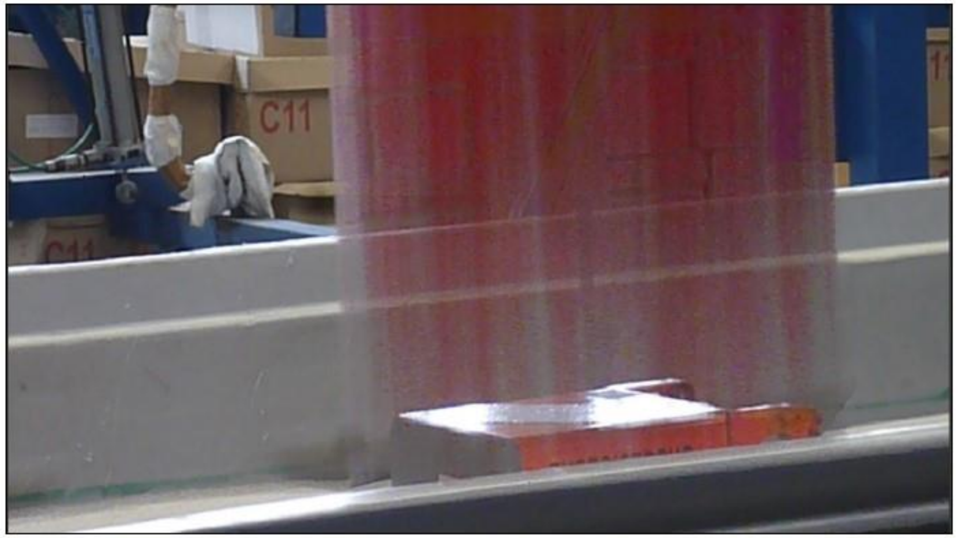

pSi-19-1386, ETEP- Impact Shock Test 02 B X+

Impact test

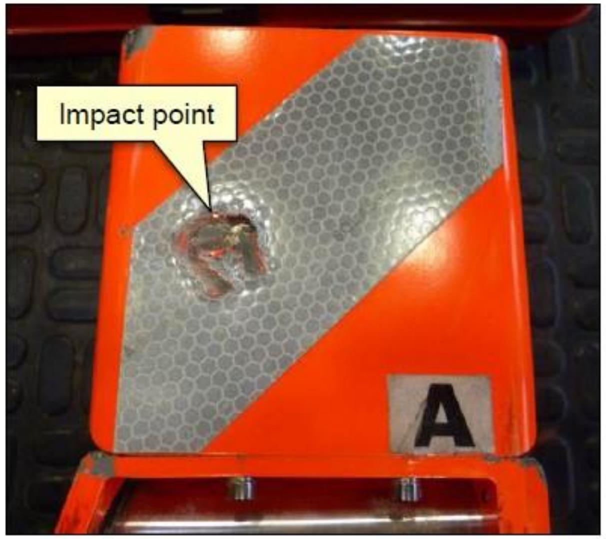

Electrical Release system
Vertical fall axis
227 Kg Cylinder
Sentinel CSMU
Sandbox


Penetration pin

Steel plate

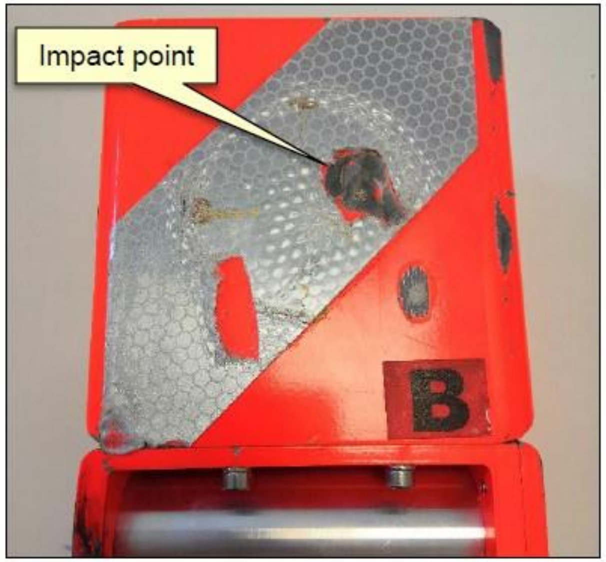


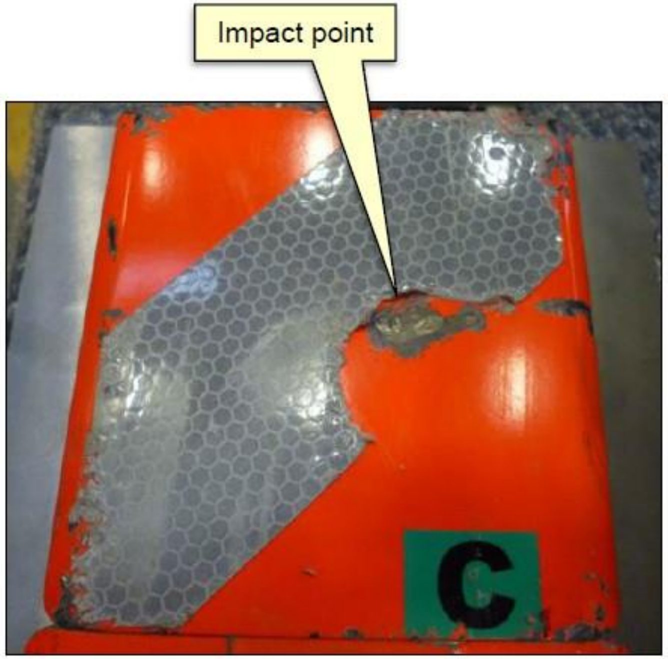
Mechanical crash test results



CSMU “A”, “B” and “C” has successfully pass test sequence, no penetration or deformation of structure has been noted for each one.

🗎 Note:
Data contained inside robust memory are not analyzed before end of test sequence.





High pressure test

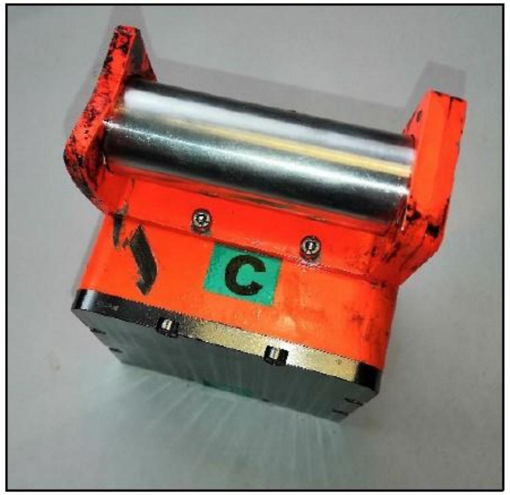
IFREMER is a French institute that undertakes research and expert assessments to advance knowledge on the oceans and their resources, monitor the marine environment and foster the sustainable development of maritime activities.

For more information consult Ifremer website: https://wwz.ifremer.fr/en/

The Sentinel CPM is placed in hyperbaric chamber during 24 hours at 625 Bar, in saltwater to simulate a depth of 6000m. The materials used to protect the recording medium have been shown to be unaffected by sea water (Titanium …)

Pictures Laboratory: IFREMER France (La-Seyne sur-Mer)

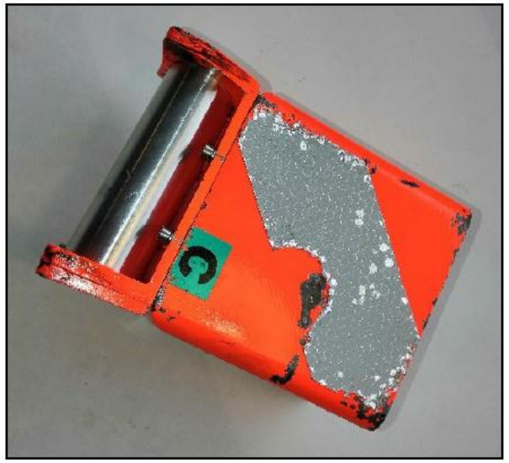
Sentinel CSMU Structure

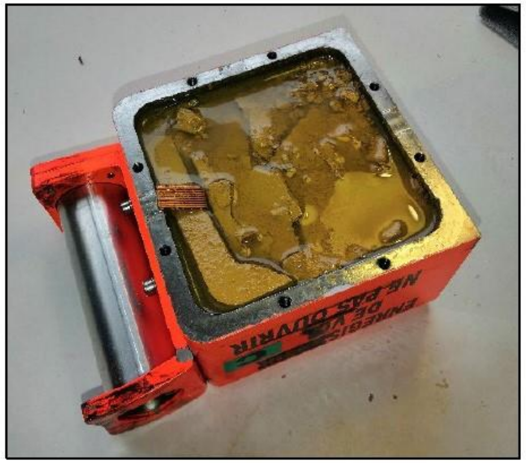


This test must determinate if the crash protected memory Sentinel can resist to an equivalent depth of 6 000 m (20 000 feet).

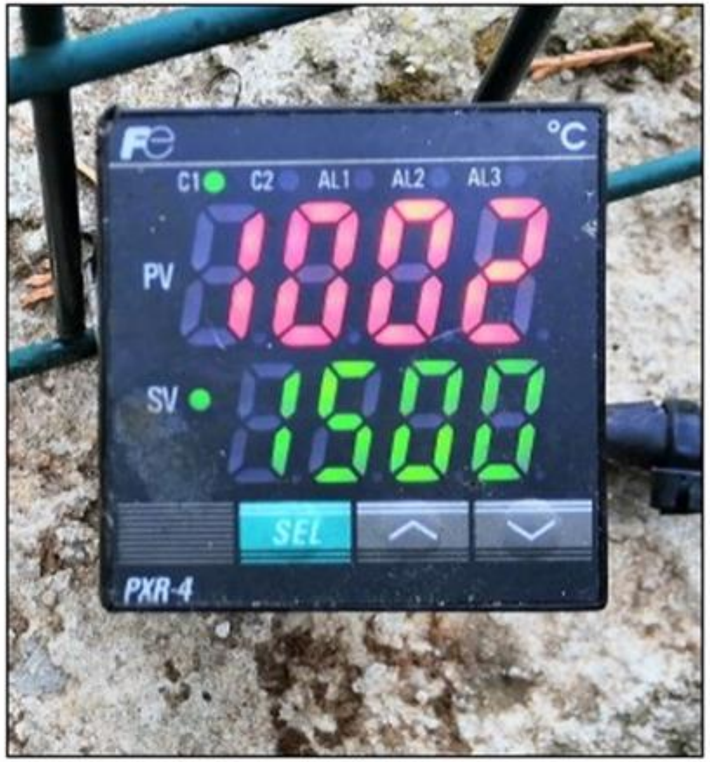
We no detected any change of the Sentinel CPM structure after 24 hours at 625 Bar.

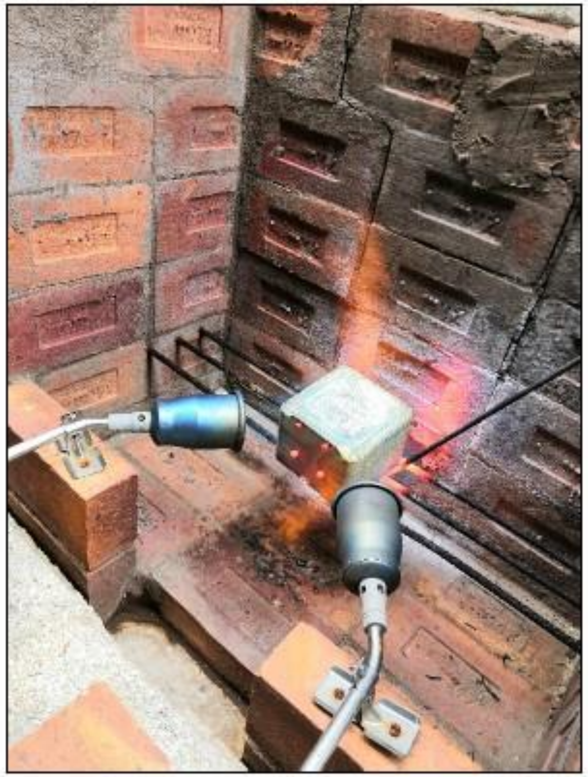
After this test in laboratory we don’t note any deformation of the structure, and the structure is remains in **full integrity.**

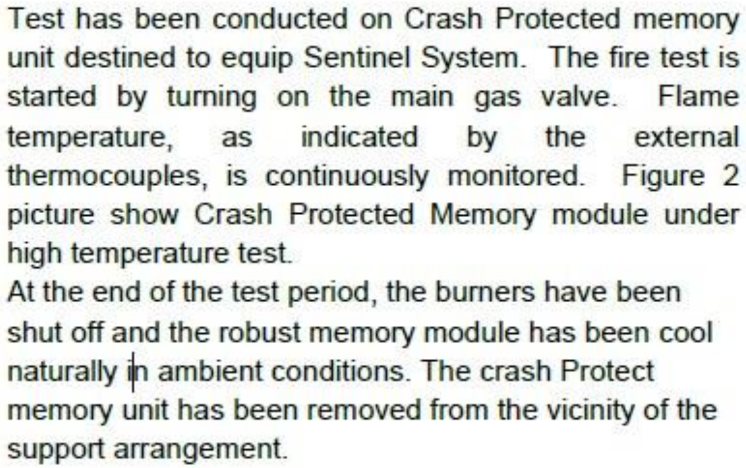




High temperature test



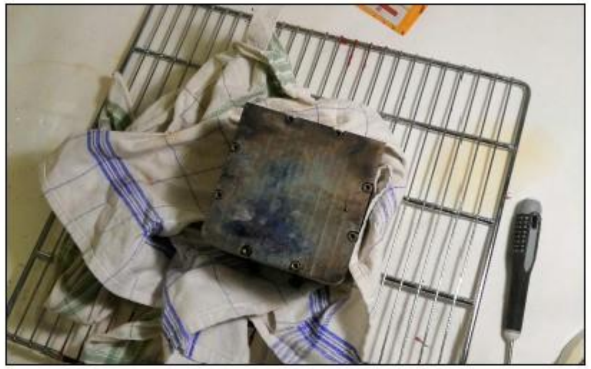




Test has been conducted on Crash Protected memory unit destined to equip Sentinel System. The fire test is started by turning on the main gas valve. Flame temperature, as indicated by the external thermocouples, is continuously monitored. Figure 2 picture show Crash Protected Memory module under high temperature test.

At the end of the test period, the burners have been shut off and the robust memory module has been cool naturally in ambient conditions. The crash Protect memory unit has been removed from the vicinity of the support arrangement.

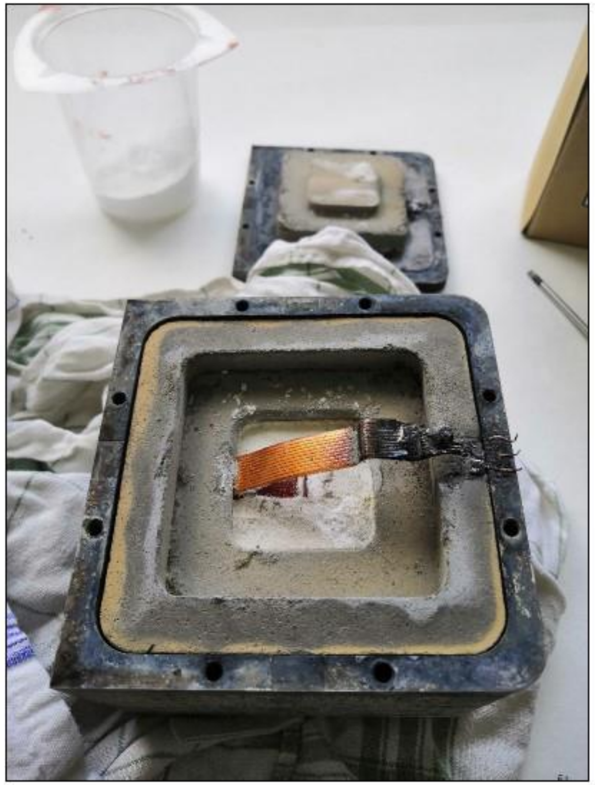
High temperature test results

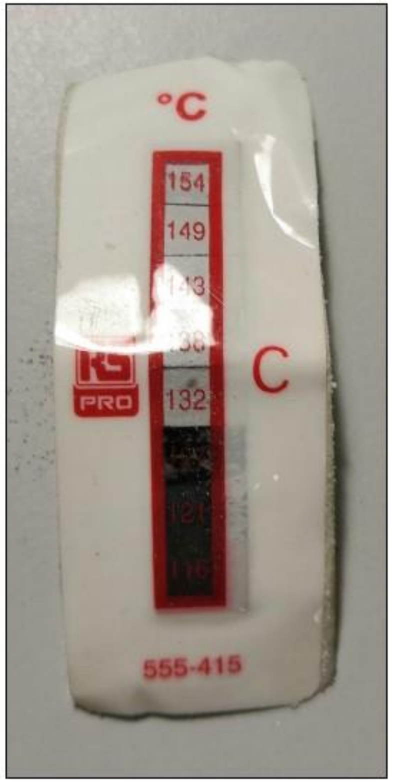


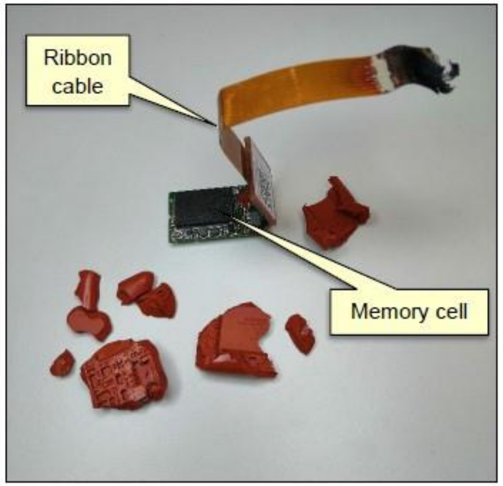
The unit is progressively put back to room temperature (natural cooling) the time is approximatively 3 hours before being able to go for opening process.

we don't notice any deformation of the structure and the structure is in **full integrity**. Bright orange paint has disappeared.

Reached temperature inside enclosure up to 132°C







After the test sequence has been performed, this test pattern shall be readily recoverable to establish that the bit error rate defined in Chapter 2-4 has not been exceeded.

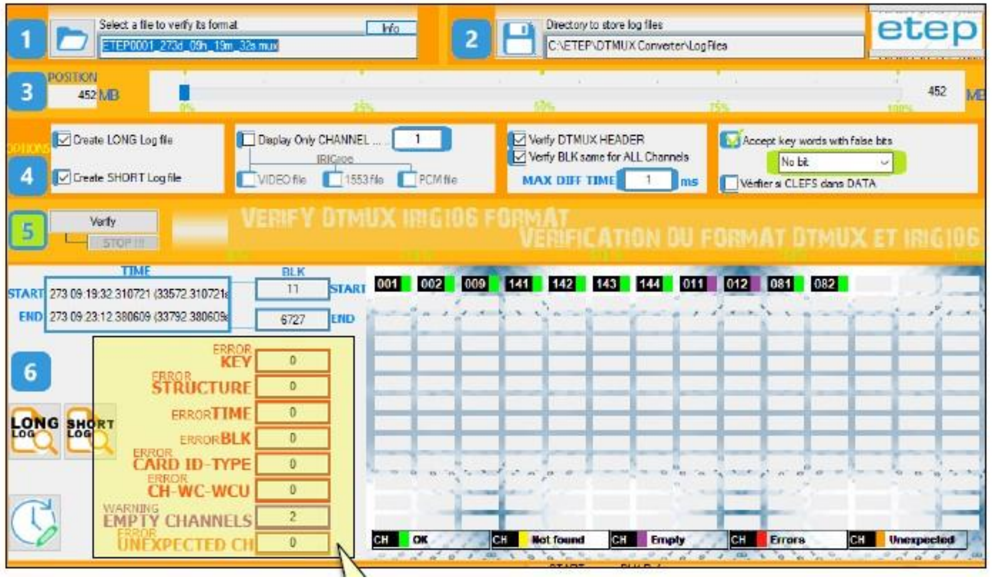
After this test the Sentinel crash protected memory is open to verify if the PCB did not damaged and if the data is still readable. After remove of all insulation protection (Ceramic, white powder material and red silicon protection), we examine the memory PCB.

Solid state drive integrity

After a visual inspection, we no detect any damages on solid state drive circuit.

The memory unit was tested to verify if the data is in full integrity.

The data is in full integrity and no present any error.



1 Select a file to verify its format: ETEP0001_273d_09h_19m_32s.mux

2 Directory to store log files: C:\ETEP\DTMUX Converter\Log Files

3 POSITION 452 MB — 452 MB

4 OPTIONS

☑ Create LONG Log file

☑ Create SHORT Log file

☐ Display Only CHANNEL ... 1

☐ VIDEO file ☐ 1553 file ☐ PCM file

☑ Verify DTMUX HEADER

☑ Verify BLK same for ALL Channels

MAX DIFF TIME 1 ms

☑ Accept key words with false bits: No bit

☐ Vérifier si CLEFS dans DATA

5 VERIFY DTMUX IRIG106 FORMAT — VERIFICATION DU FORMAT DTMUX ET IRIG106

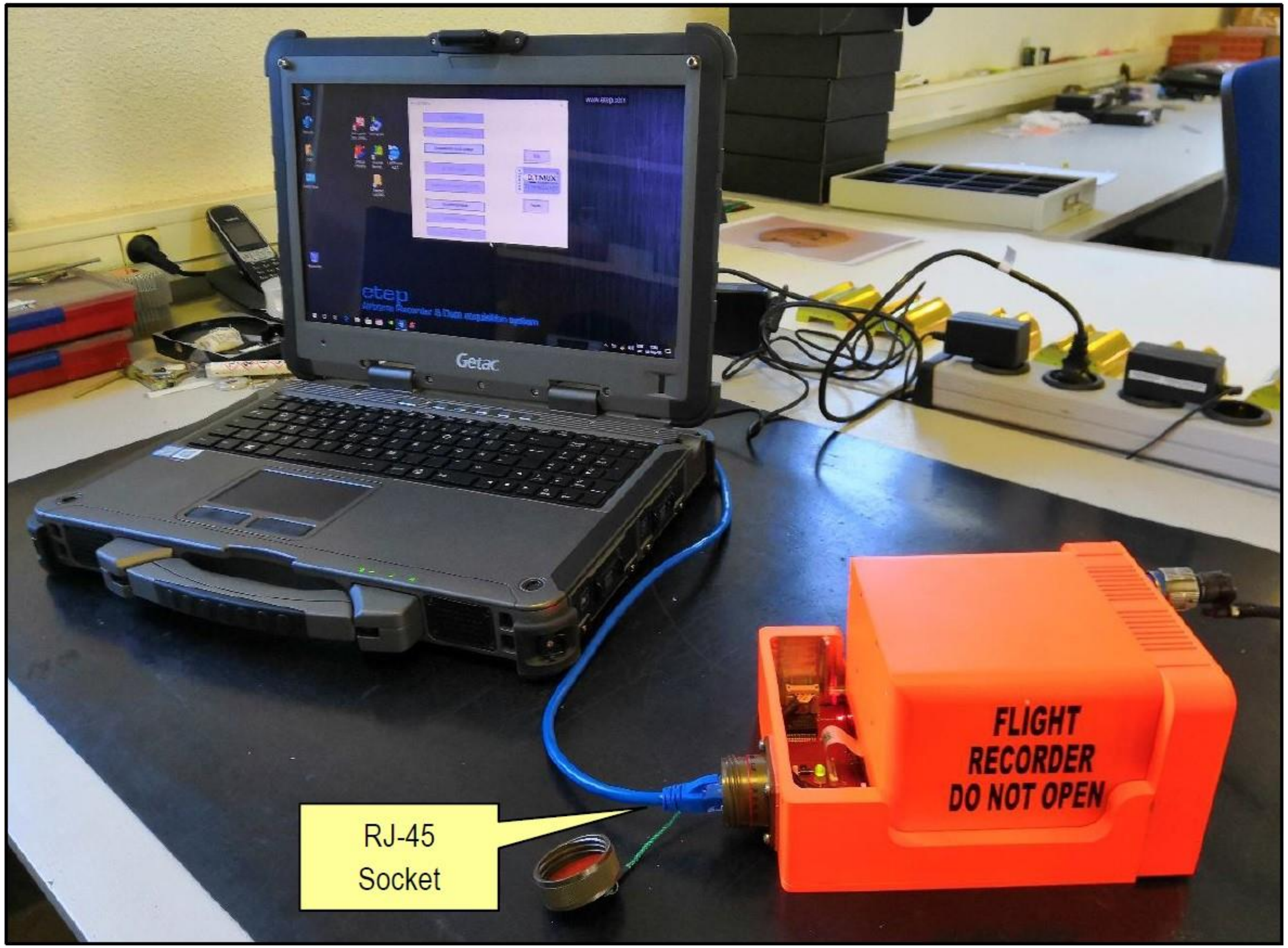
	TIME	BLK
START	273 09:19:32.310721 (33572.310721	11
END	273 09:23:12.380609 (33792.380609	6727

Channels: 001, 002, 009, 141, 142, 143, 144, 011, 012, 081, 082

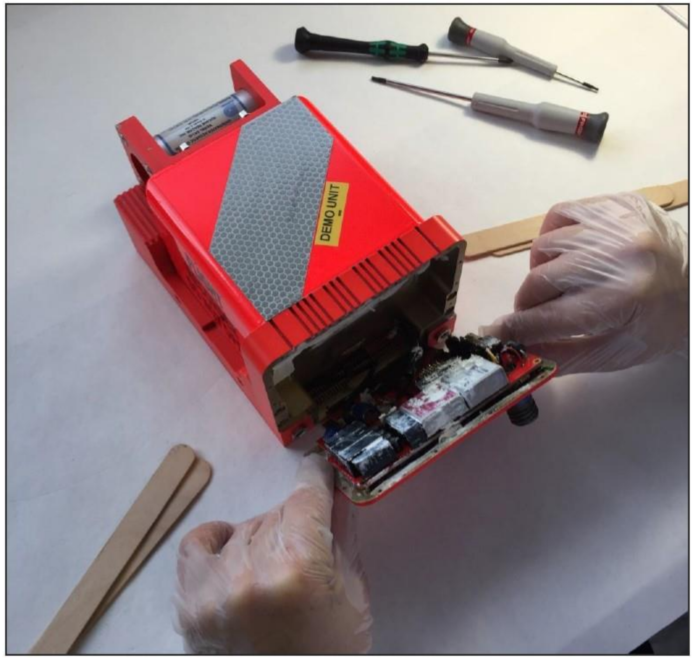
6

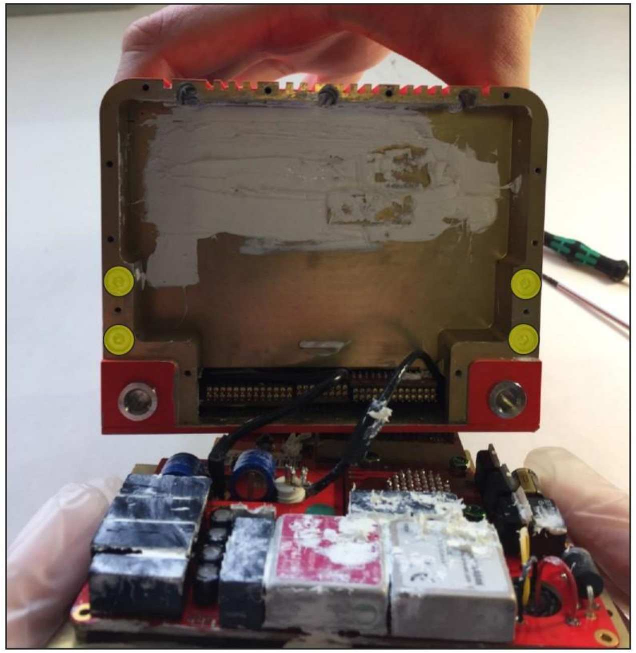
ERROR KEY	0
ERROR STRUCTURE	0
ERROR TIME	0
ERROR BLK	0
ERROR CARD ID-TYPE	0
ERROR CH-WC-WCU	0
WARNING EMPTY CHANNELS	2
ERROR UNEXPECTED CH	0

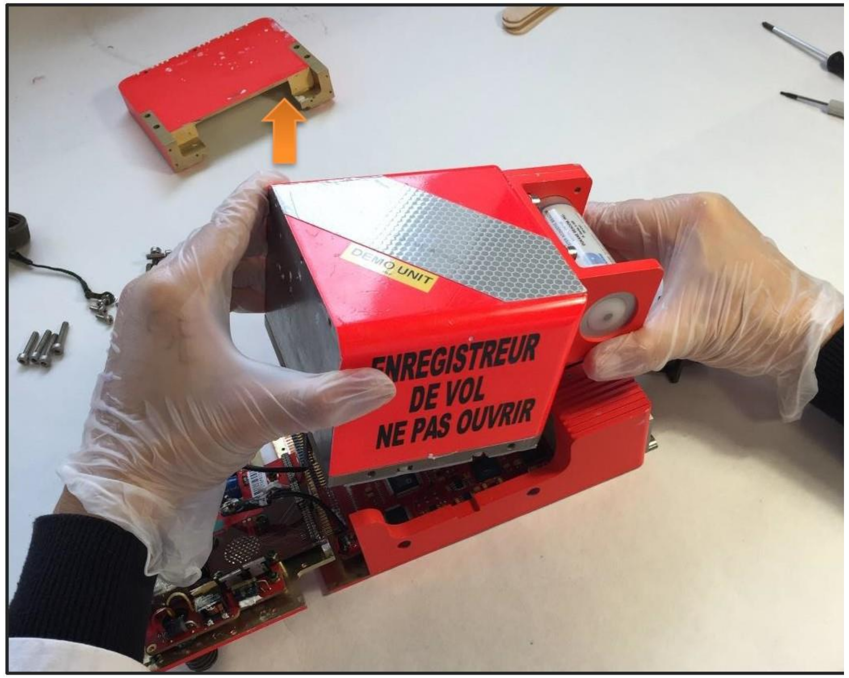
Data extraction via external interface

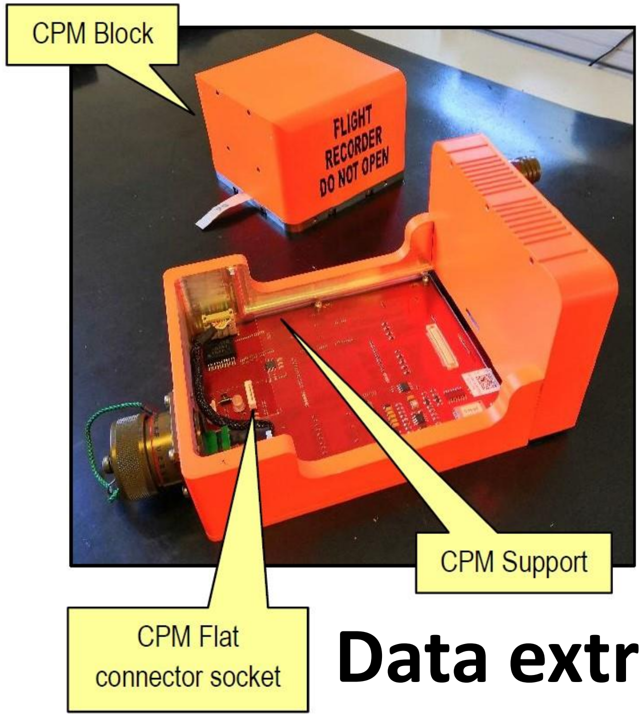


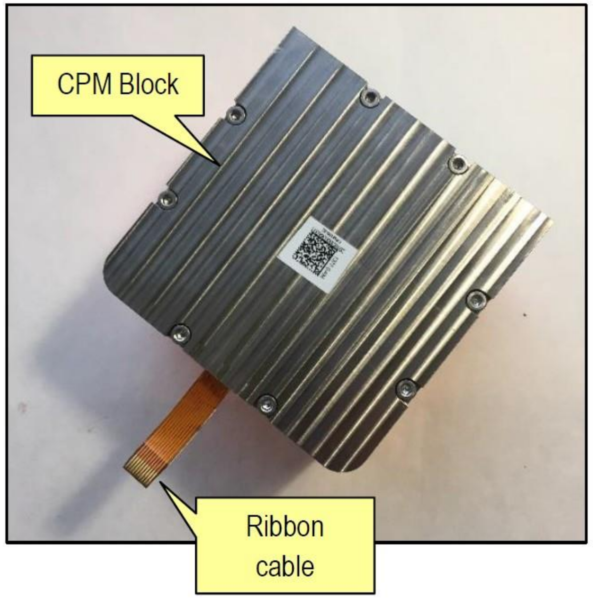
RJ-45
Socket



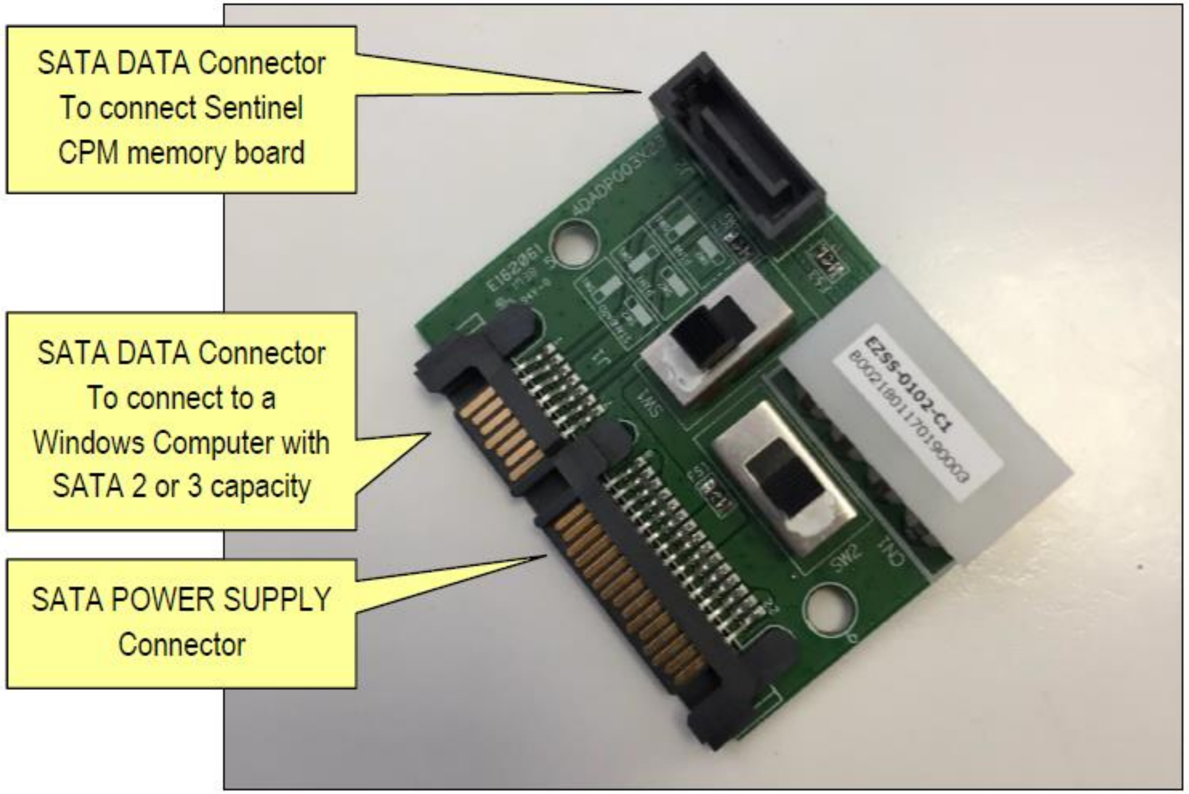


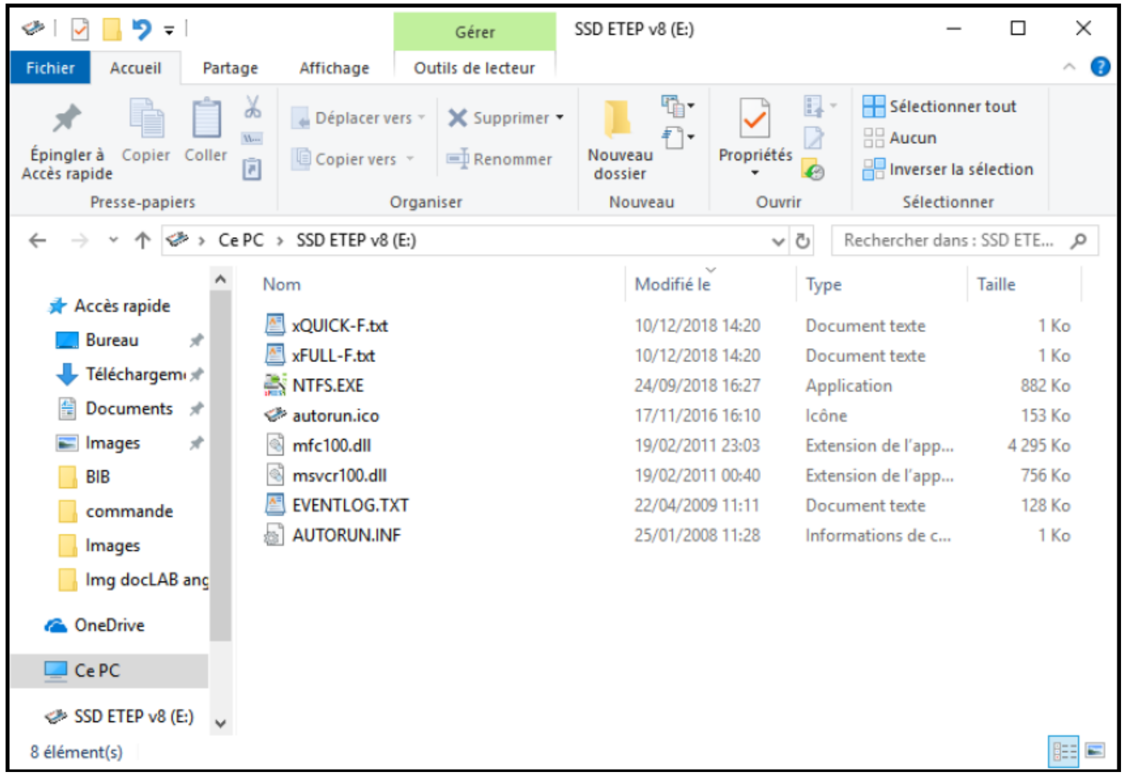






Data extraction via internal SATA

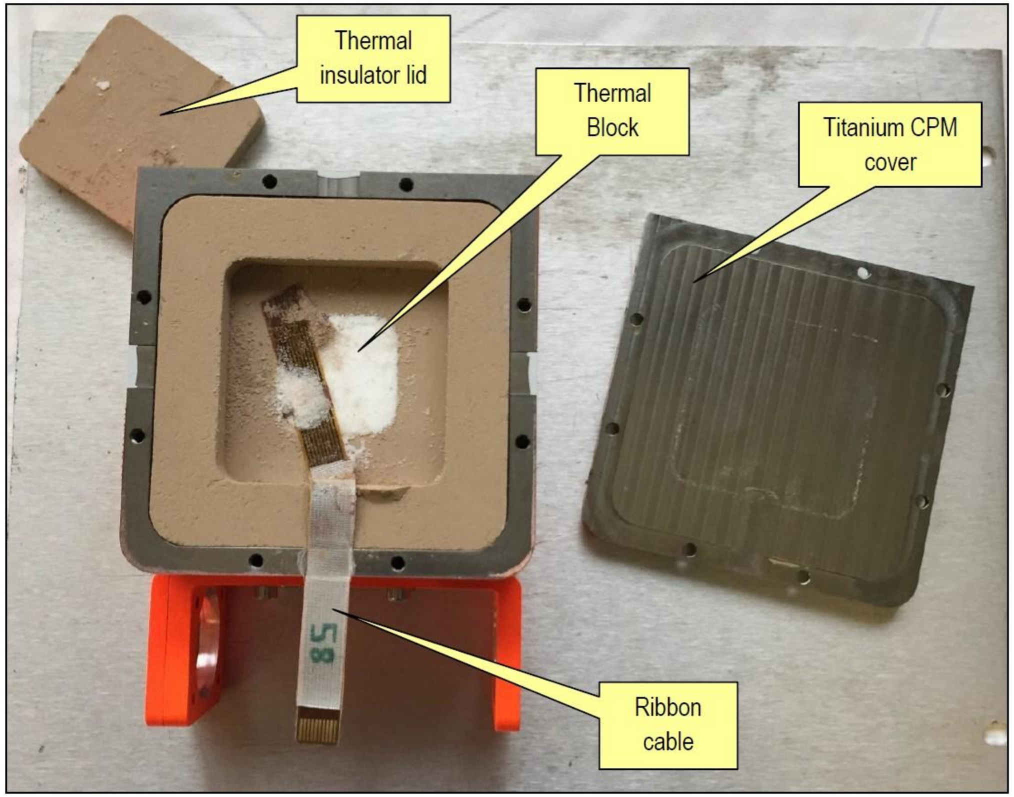


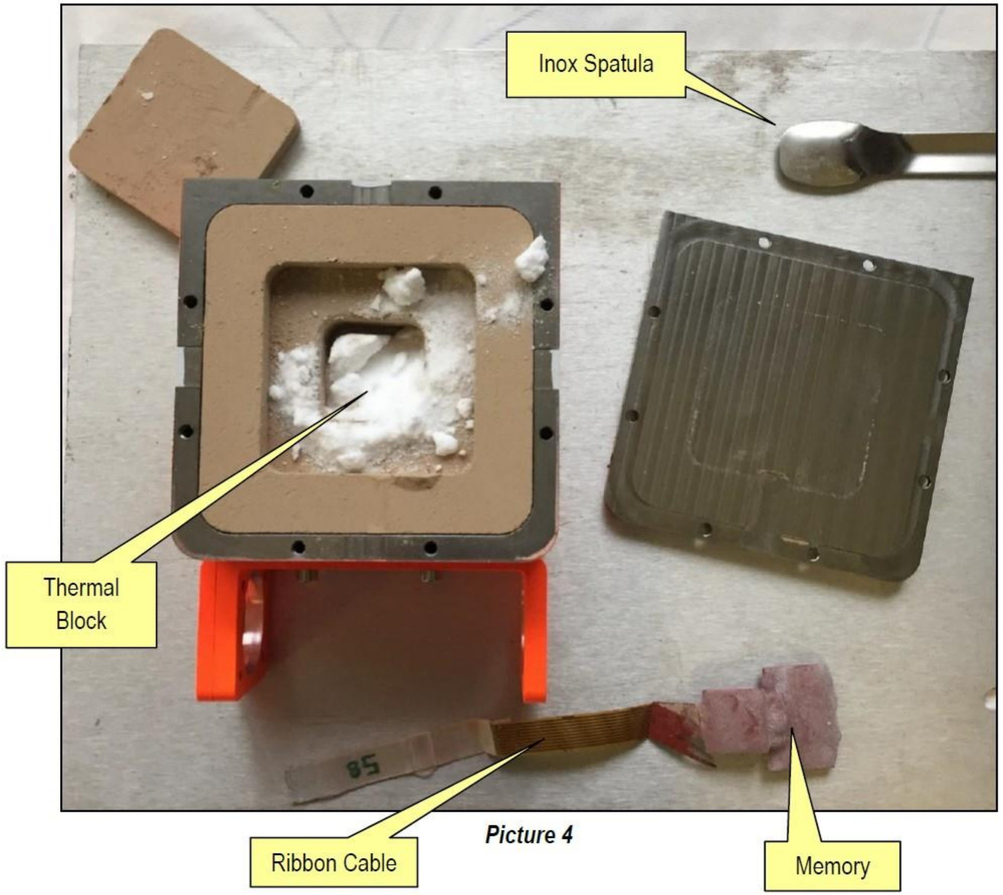


Nom	Modifié le	Type	Taille
xQUICK-F.txt	10/12/2018 14:20	Document texte	1 Ko
xFULL-F.txt	10/12/2018 14:20	Document texte	1 Ko
NTFS.EXE	24/09/2018 16:27	Application	882 Ko
autorun.ico	17/11/2016 16:10	Icône	153 Ko
mfc100.dll	19/02/2011 23:03	Extension de l'app...	4 295 Ko
msvcr100.dll	19/02/2011 00:40	Extension de l'app...	756 Ko
EVENTLOG.TXT	22/04/2009 11:11	Document texte	128 Ko
AUTORUN.INF	25/01/2008 11:28	Informations de c...	1 Ko

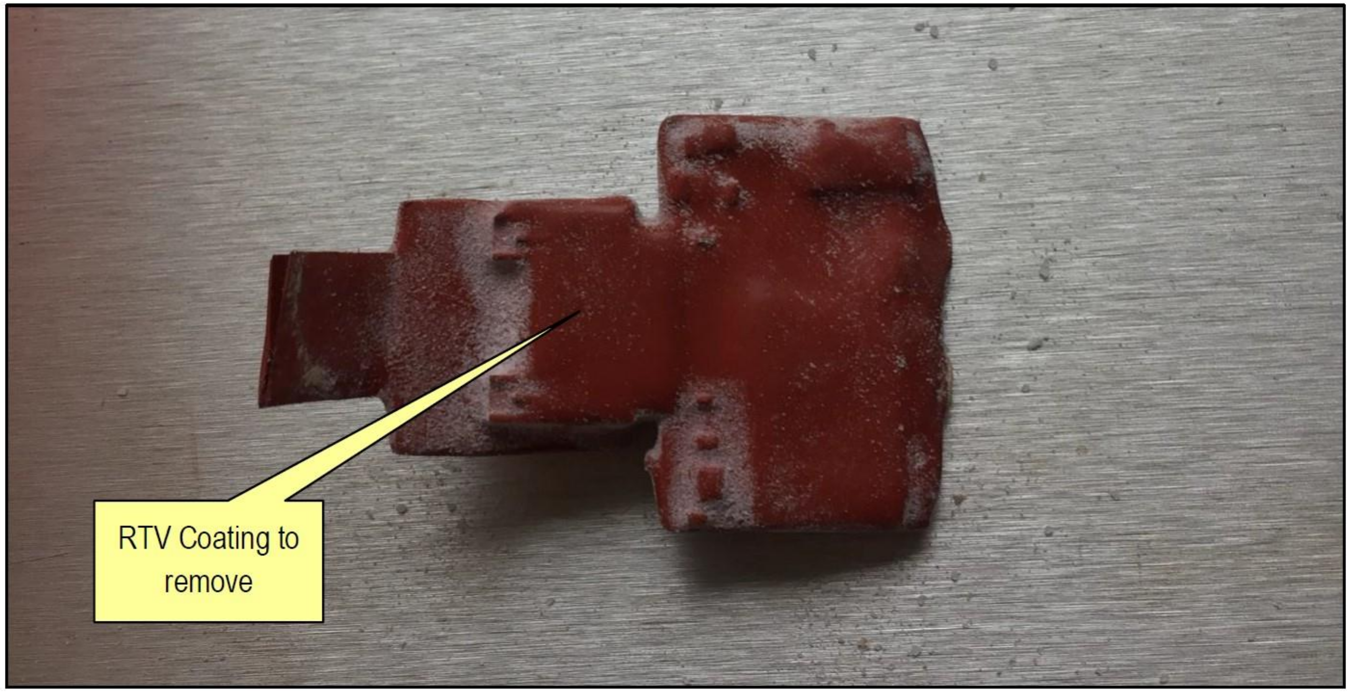
Real-world test...

When everything else fails...chips usually don't

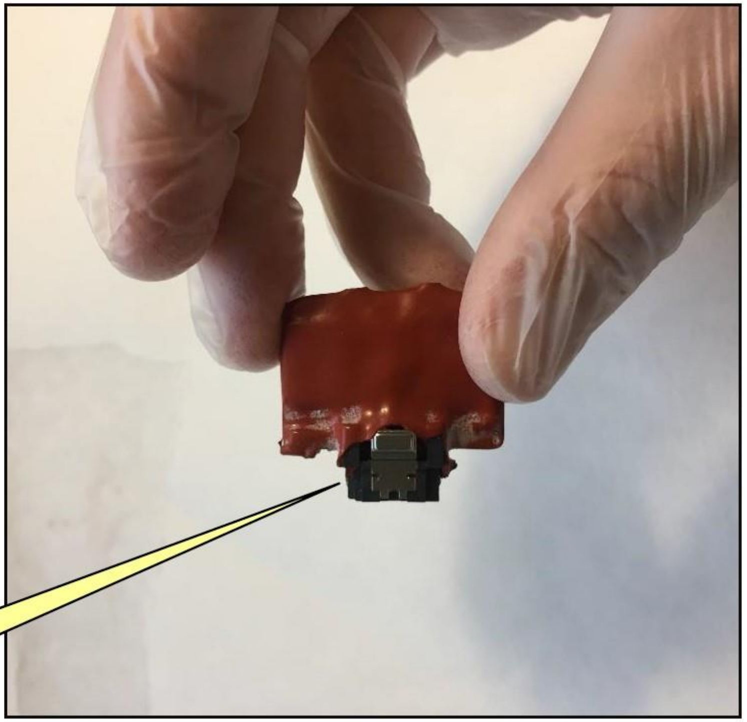




Picture 4

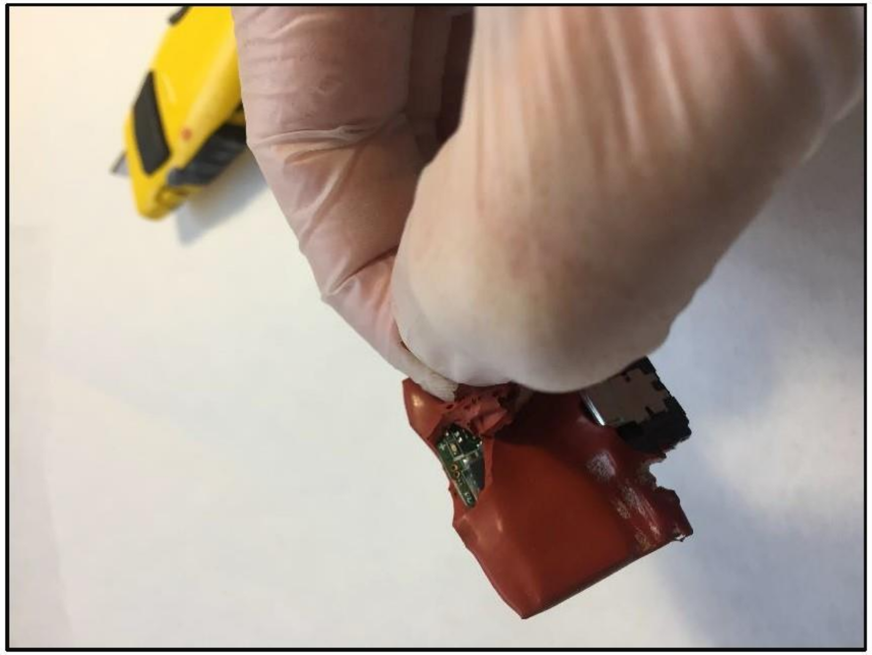


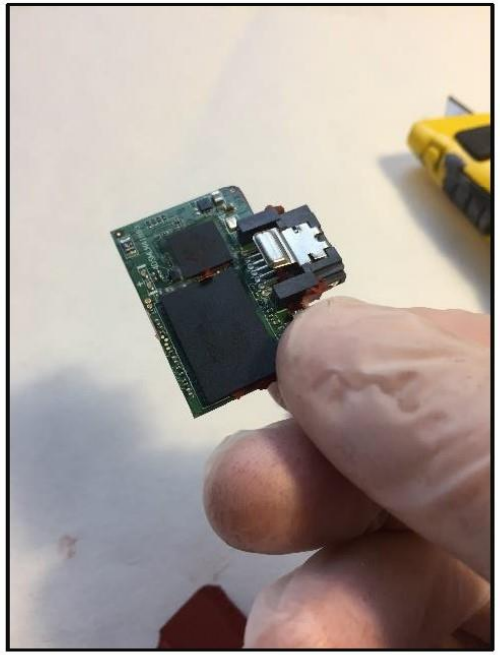
RTV Coating to remove

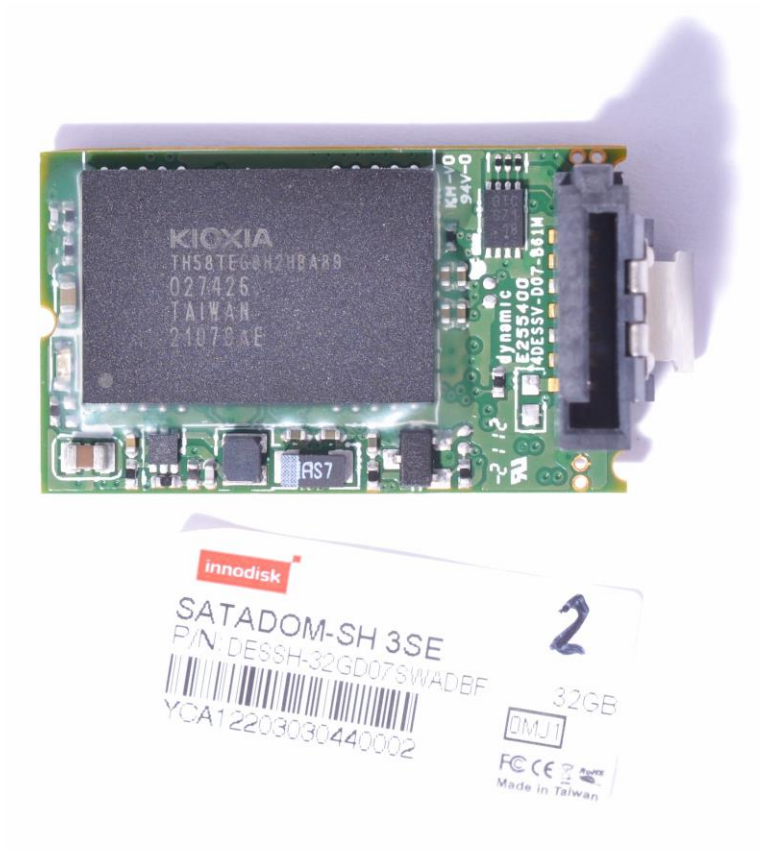


SATA Connector

FORTUNATULY, real-world crash conditions are rare occassion, we were not able to get our hands on damaged device

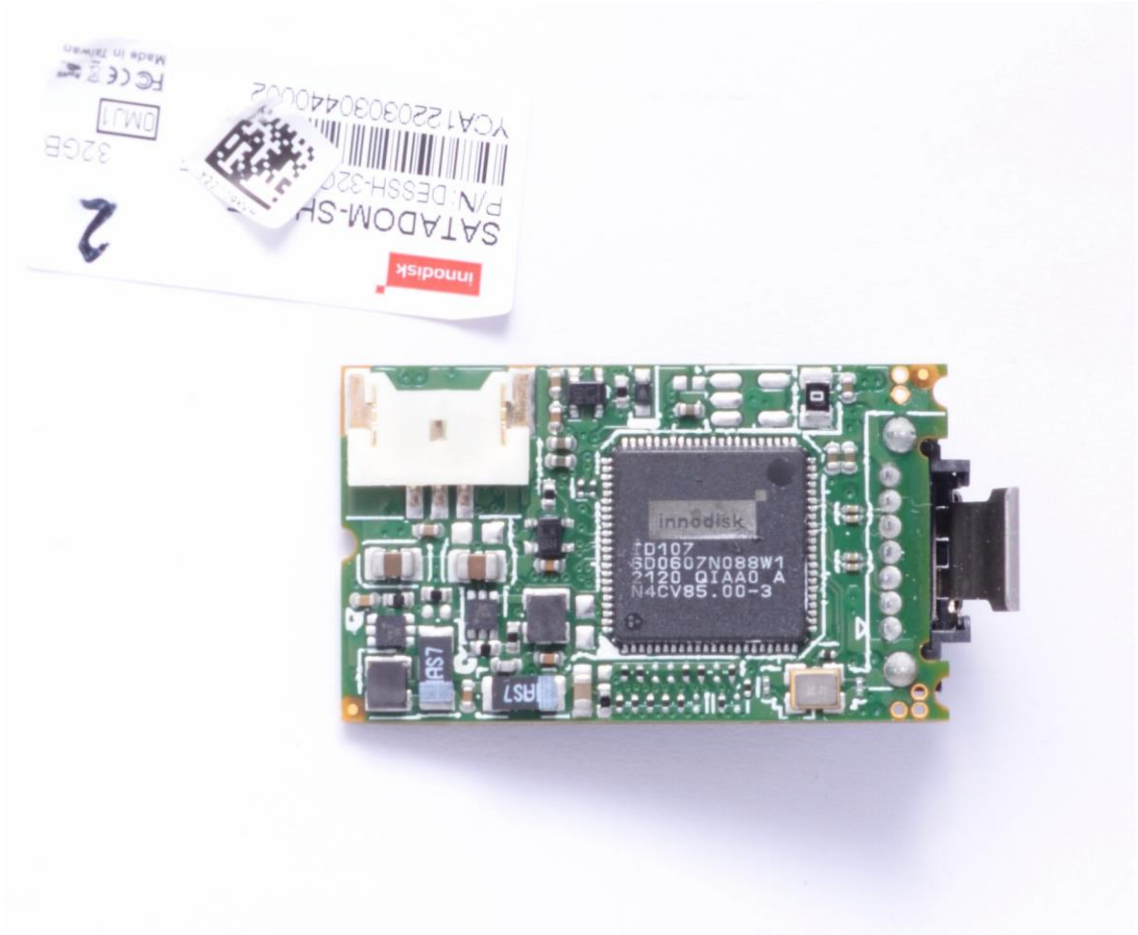






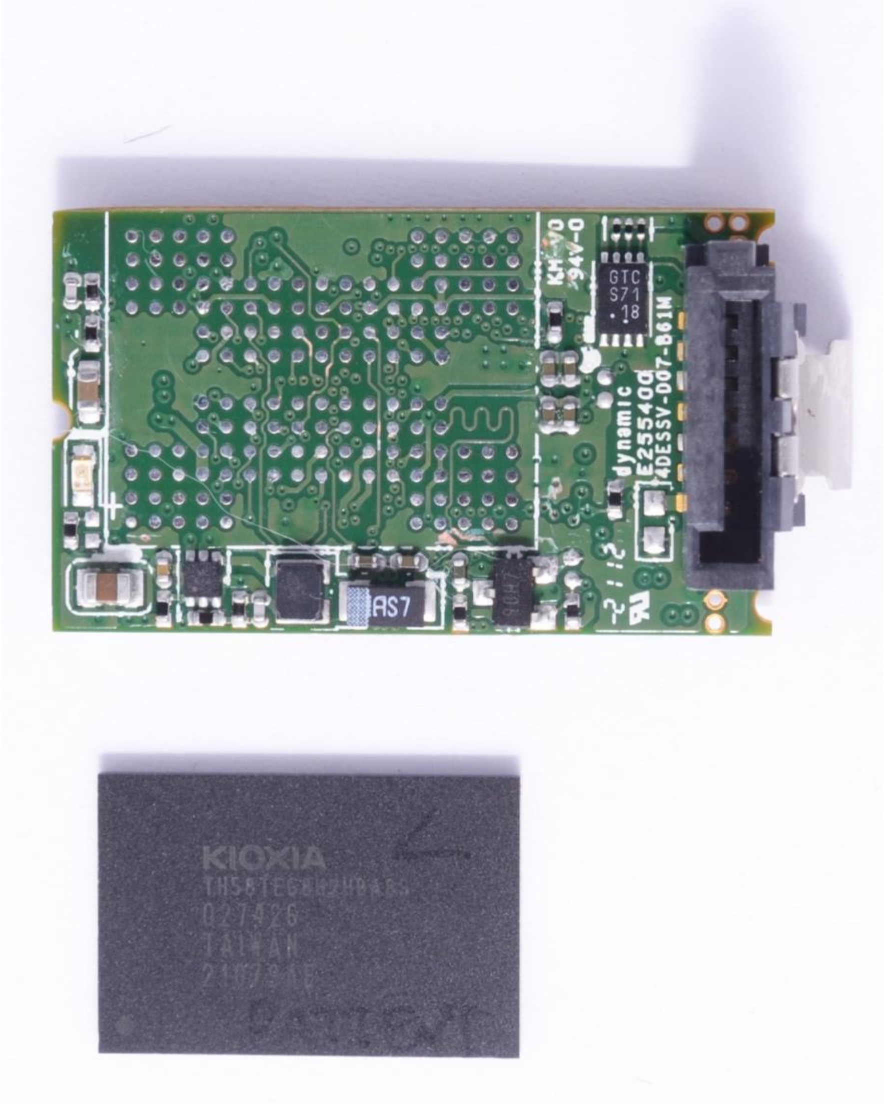
On this side of PCB we can spot NAND memory chip made by Kioxia (Toshiba) with the model name TH58TEG8H2HBA-89

On the other side of PCB we can see the microcontroller

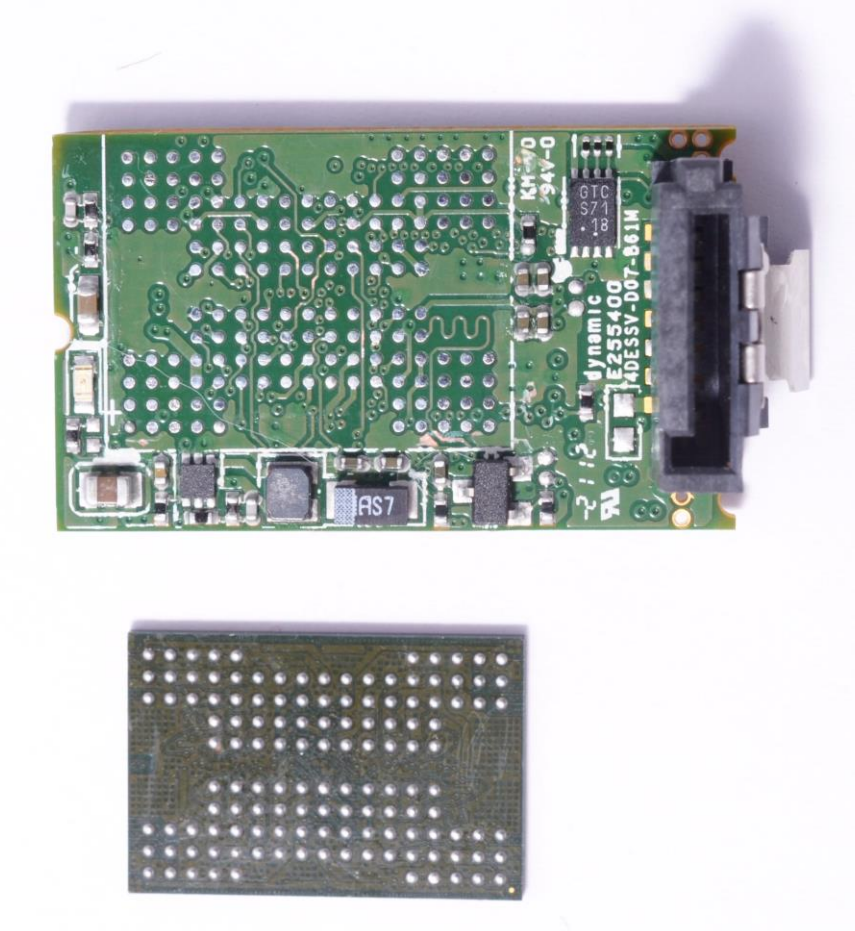


Unsoldered NAND memory – top view

The memory chip was removed from the PCB for further reading using InfraRed rework station and thermal profile of Tmax = 240C (Tdelta ~ 3C/s)



Unsoldered NAND memory – ball view

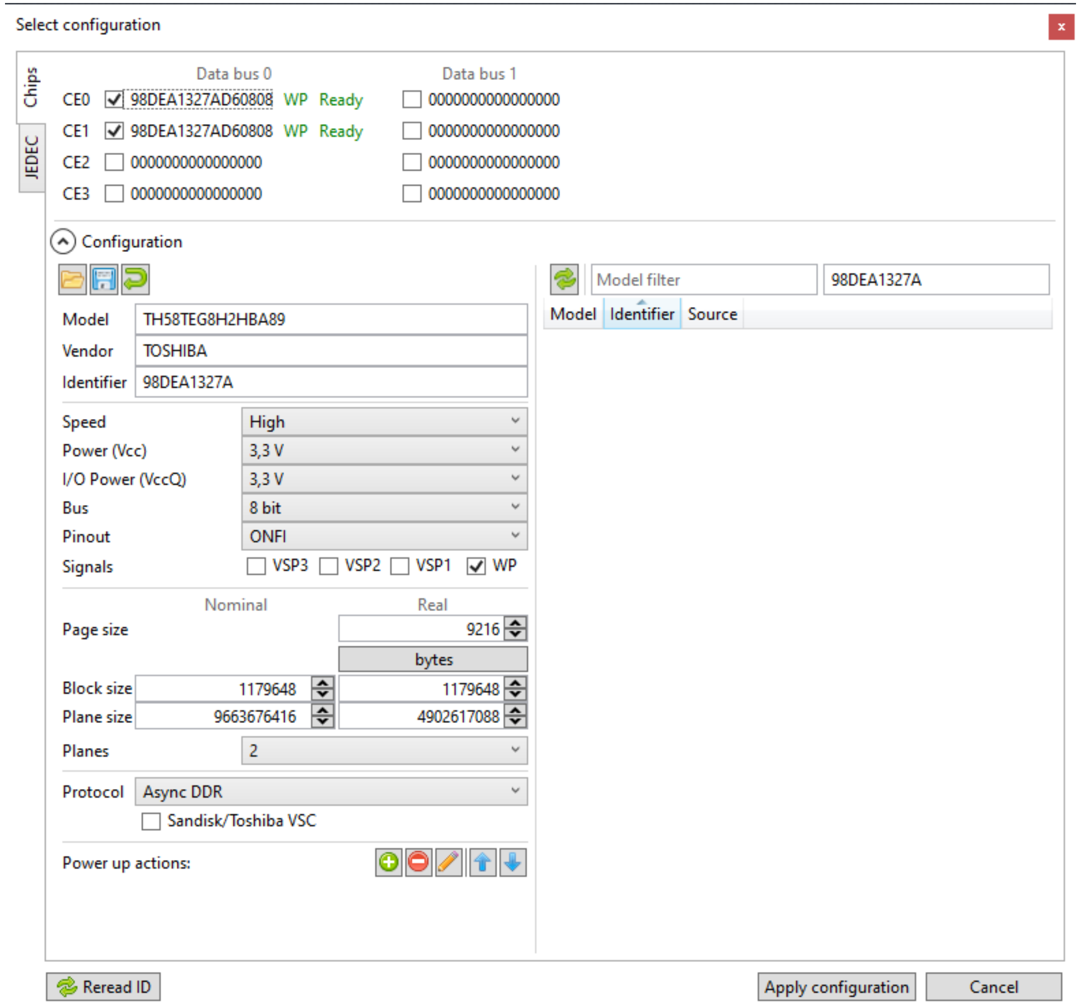


The NAND memory has BGA-132 package which is classics for high-capacity memory chips.
The pads of NAND memory chip have been cleaned with solder wick and then isopropyl alcohol.

Chip connected to VNR Reader

We used Visual Nand Reconstructor Reader from Starter kit in couple with BGA132 adapter from Standard kit for memory chip reading.

Chip identification



	Data bus 0			Data bus 1
CE0	☑ 98DEA1327AD60808	WP	Ready	□ 0000000000000000
CE1	☑ 98DEA1327AD60808	WP	Ready	□ 0000000000000000
CE2	□ 0000000000000000			□ 0000000000000000
CE3	□ 0000000000000000			□ 0000000000000000

Model filter: 98DEA1327A

Model: TH58TEG8H2HBA89
Vendor: TOSHIBA
Identifier: 98DEA1327A

Speed: High
Power (Vcc): 3,3 V
I/O Power (VccQ): 3,3 V
Bus: 8 bit
Pinout: ONFI
Signals: □ VSP3 □ VSP2 □ VSP1 ☑ WP

	Nominal	Real
Page size		9216 bytes
Block size	1179648	1179648
Plane size	9663676416	4902617088

Planes: 2

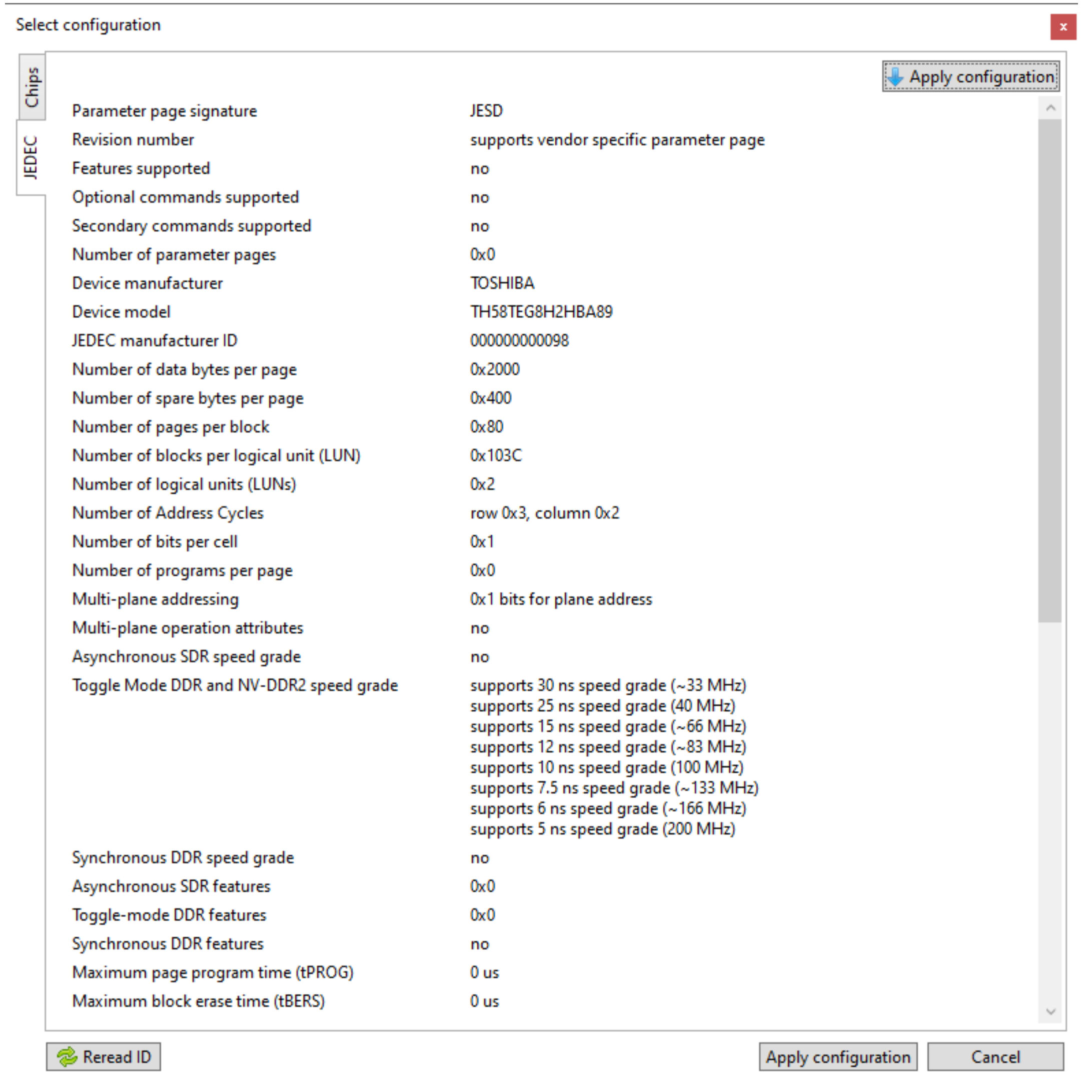
Protocol: Async DDR
□ Sandisk/Toshiba VSC

The first step before physical image reading is reading memory chip’s ID.

The chip model identifier is 98DEA1327A which belongs to Toshiba/Kioxia manufacturer

The memory chip has multi-die structure and we were able to identify 4 dies/crystals in single package.

JEDEC data

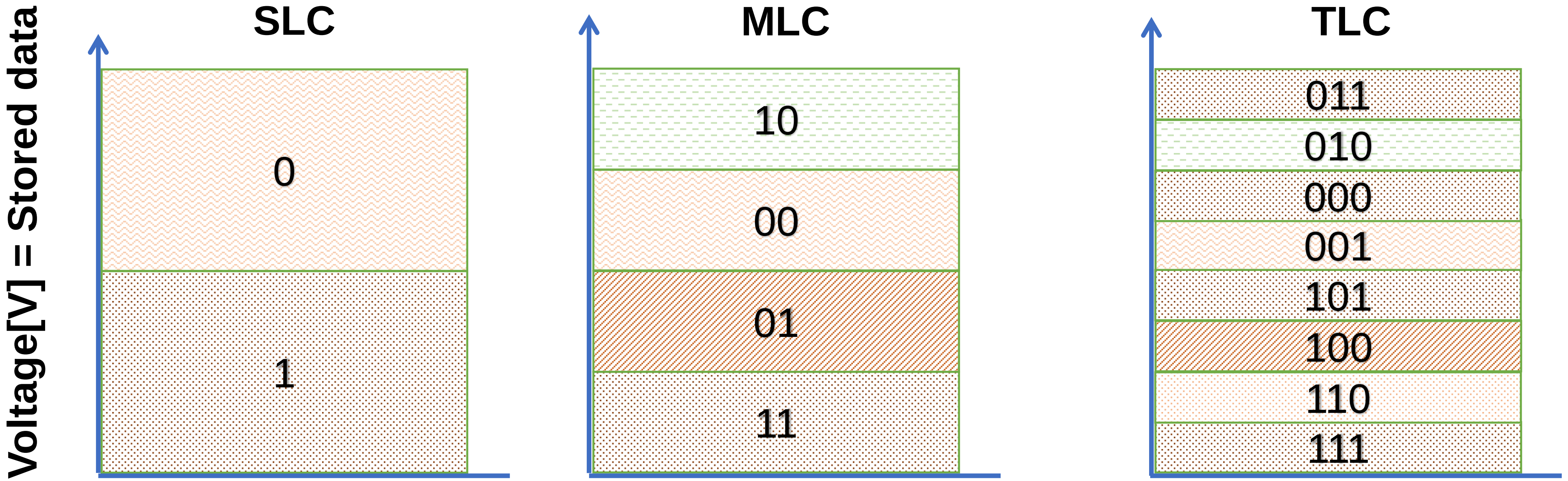


Parameter page signature	JESD
Revision number	supports vendor specific parameter page
Features supported	no
Optional commands supported	no
Secondary commands supported	no
Number of parameter pages	0x0
Device manufacturer	TOSHIBA
Device model	TH58TEG8H2HBA89
JEDEC manufacturer ID	000000000098
Number of data bytes per page	0x2000
Number of spare bytes per page	0x400
Number of pages per block	0x80
Number of blocks per logical unit (LUN)	0x103C
Number of logical units (LUNs)	0x2
Number of Address Cycles	row 0x3, column 0x2
Number of bits per cell	0x1
Number of programs per page	0x0
Multi-plane addressing	0x1 bits for plane address
Multi-plane operation attributes	no
Asynchronous SDR speed grade	no
Toggle Mode DDR and NV-DDR2 speed grade	supports 30 ns speed grade (~33 MHz) supports 25 ns speed grade (40 MHz) supports 15 ns speed grade (~66 MHz) supports 12 ns speed grade (~83 MHz) supports 10 ns speed grade (100 MHz) supports 7.5 ns speed grade (~133 MHz) supports 6 ns speed grade (~166 MHz) supports 5 ns speed grade (200 MHz)
Synchronous DDR speed grade	no
Asynchronous SDR features	0x0
Toggle-mode DDR features	0x0
Synchronous DDR features	no
Maximum page program time (tPROG)	0 us
Maximum block erase time (tBERS)	0 us

This NAND chip has special JEDEC parameter page that shows basic information about the memory.

As we can see from report:
Number of bits per cell = 1,
which means that memory chip has **SLC architecture, and it is the best choice for the applications where reliability is a KEY factor.**

NAND memory cell architectures

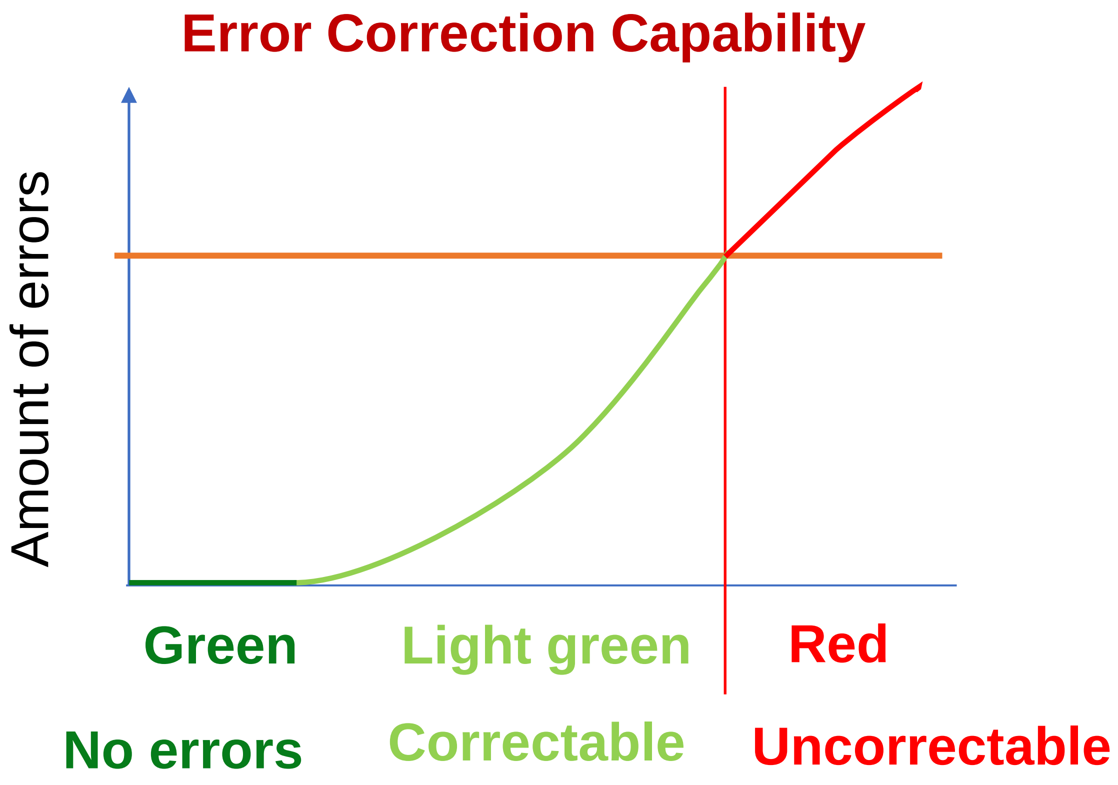


1 Bit Per Cell
2 Levels
100,000 P/E Cycles

2 Bits Per Cell
4 Levels
10,000 P/E Cycles

3 Bits Per Cell
8 Levels
1,000 P/E Cycles

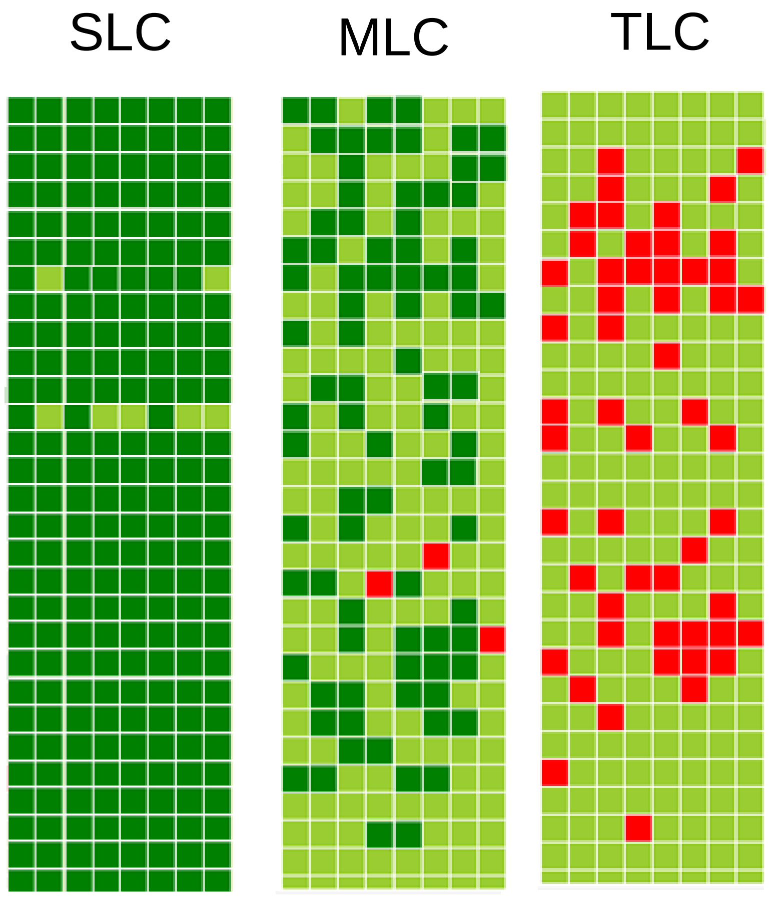
Bit errors in NAND



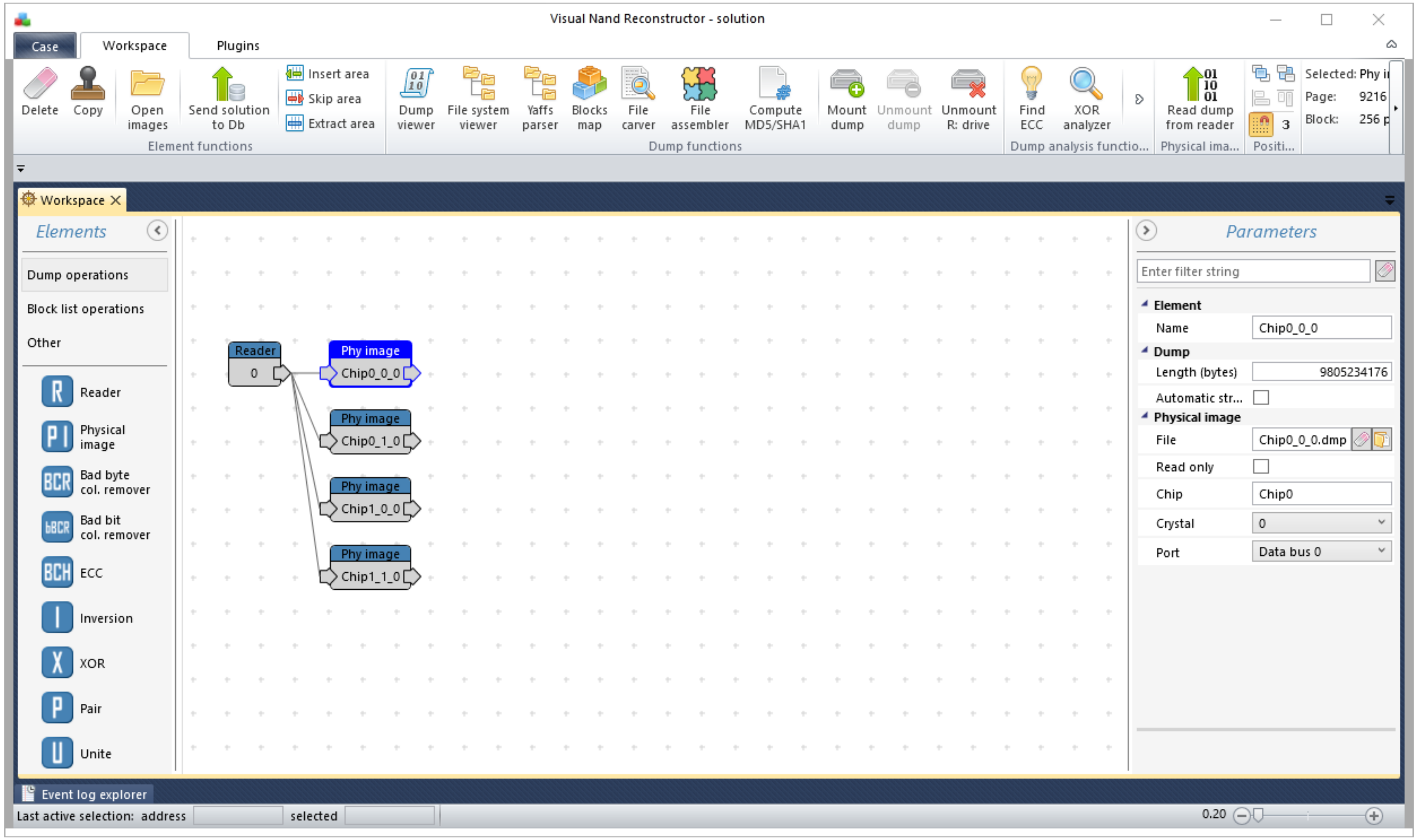
Green — No errors

Light green — Correctable

Red — Uncorrectable



Physical image extraction from NAND

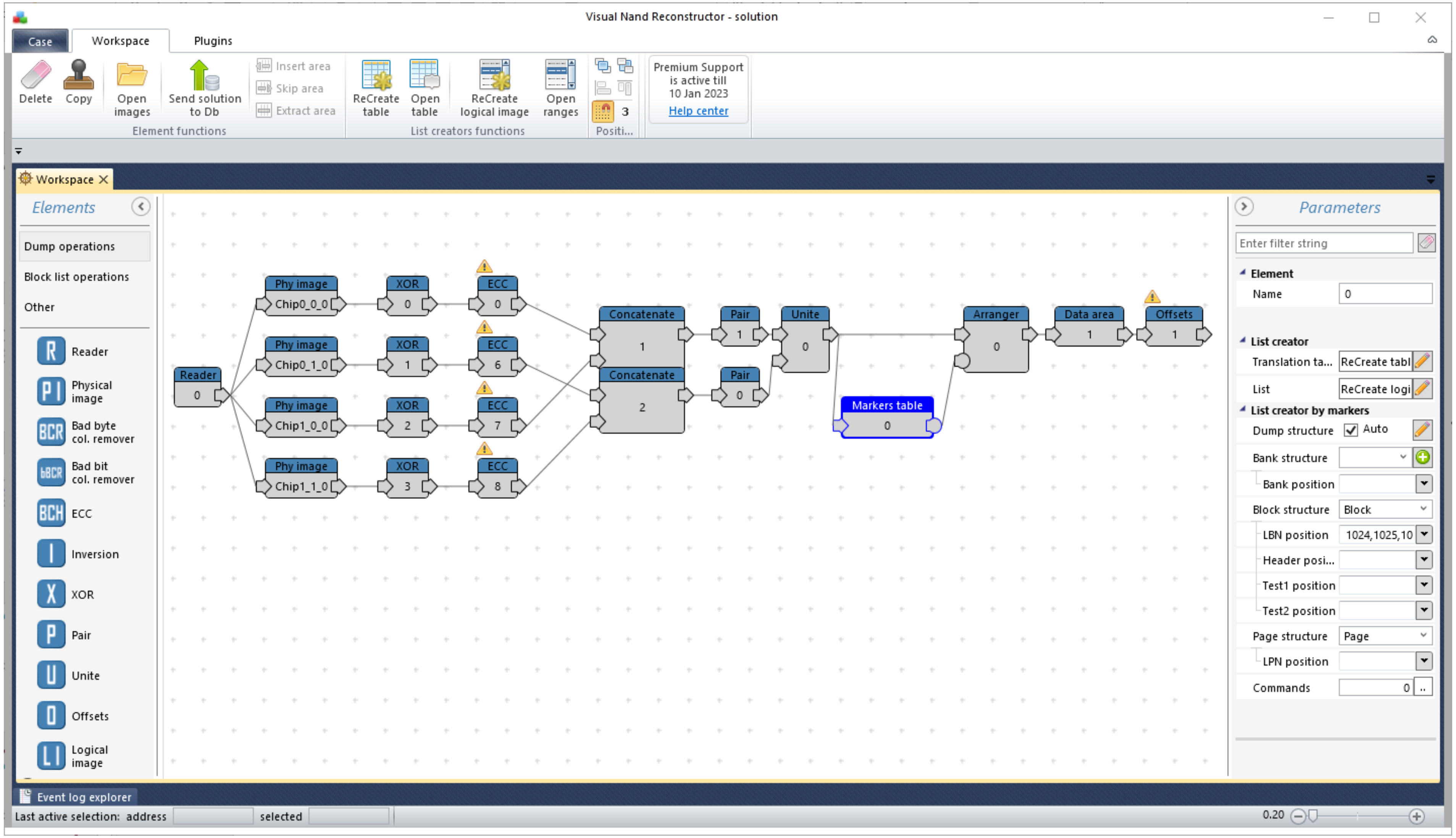


Element
Name: Chip0_0_0
Dump
Length (bytes): 9805234176
Automatic str... □
Physical image
File: Chip0_0_0.dmp
Read only □
Chip: Chip0
Crystal: 0
Port: Data bus 0

We used Visual NAND Reconstructor for memory chip reading and physical image processing.

In total 4 dumps/physical images were extracted out of the NAND.

Reconstruction of controller’s workflow



Element

Name: 0

List creator

Translation ta...: ReCreate tabl

List: ReCreate logi

List creator by markers

Dump structure: ☑ Auto

Bank structure:

Bank position:

Block structure: Block

LBN position: 1024,1025,10

Header posi...:

Test1 position:

Test2 position:

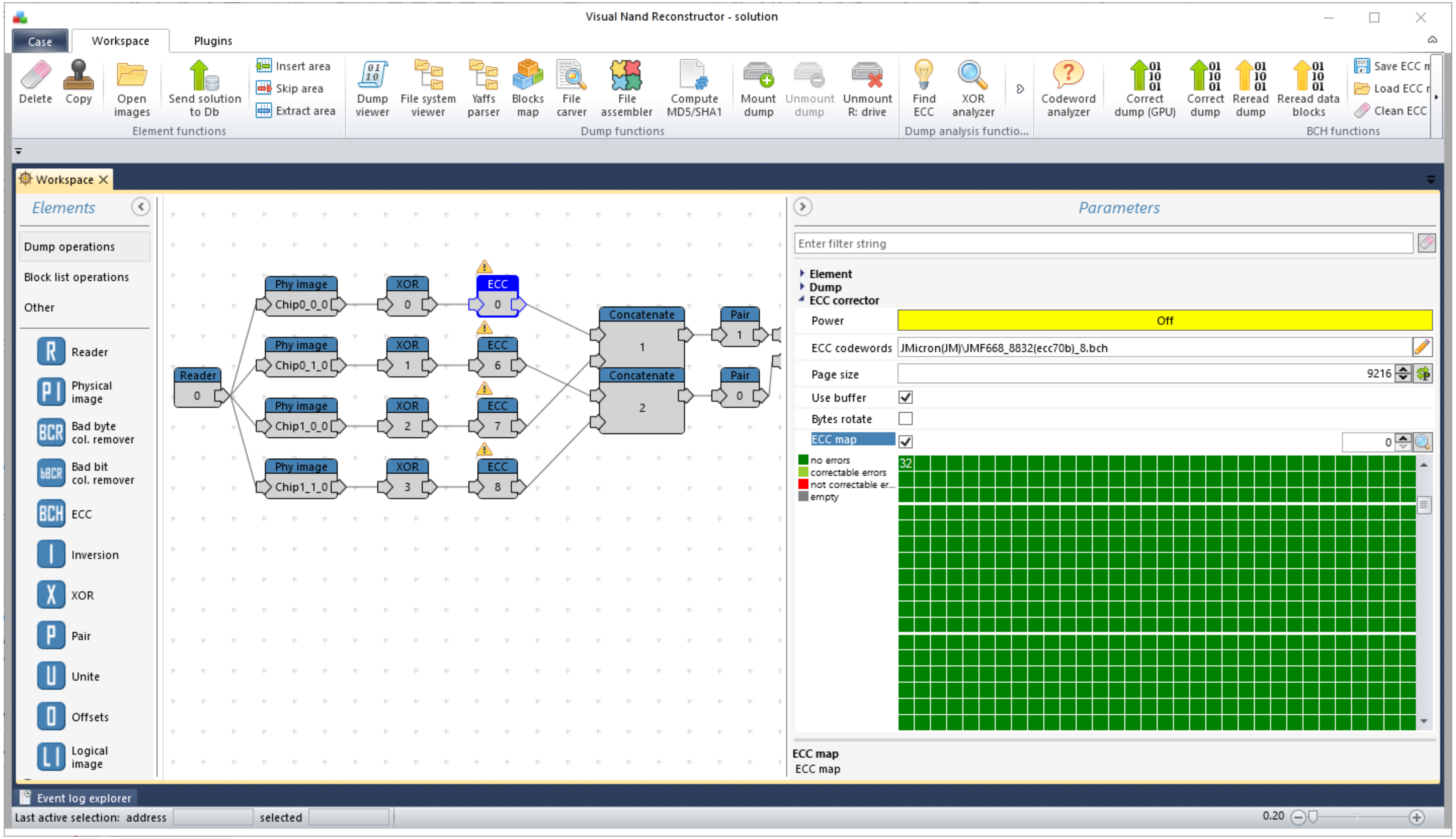
Page structure: Page

LPN position:

Commands: 0

Physical image has been converted to logical image through controller’s emulation process

ECC algorithm for bit error correction has been found and errors got corrected



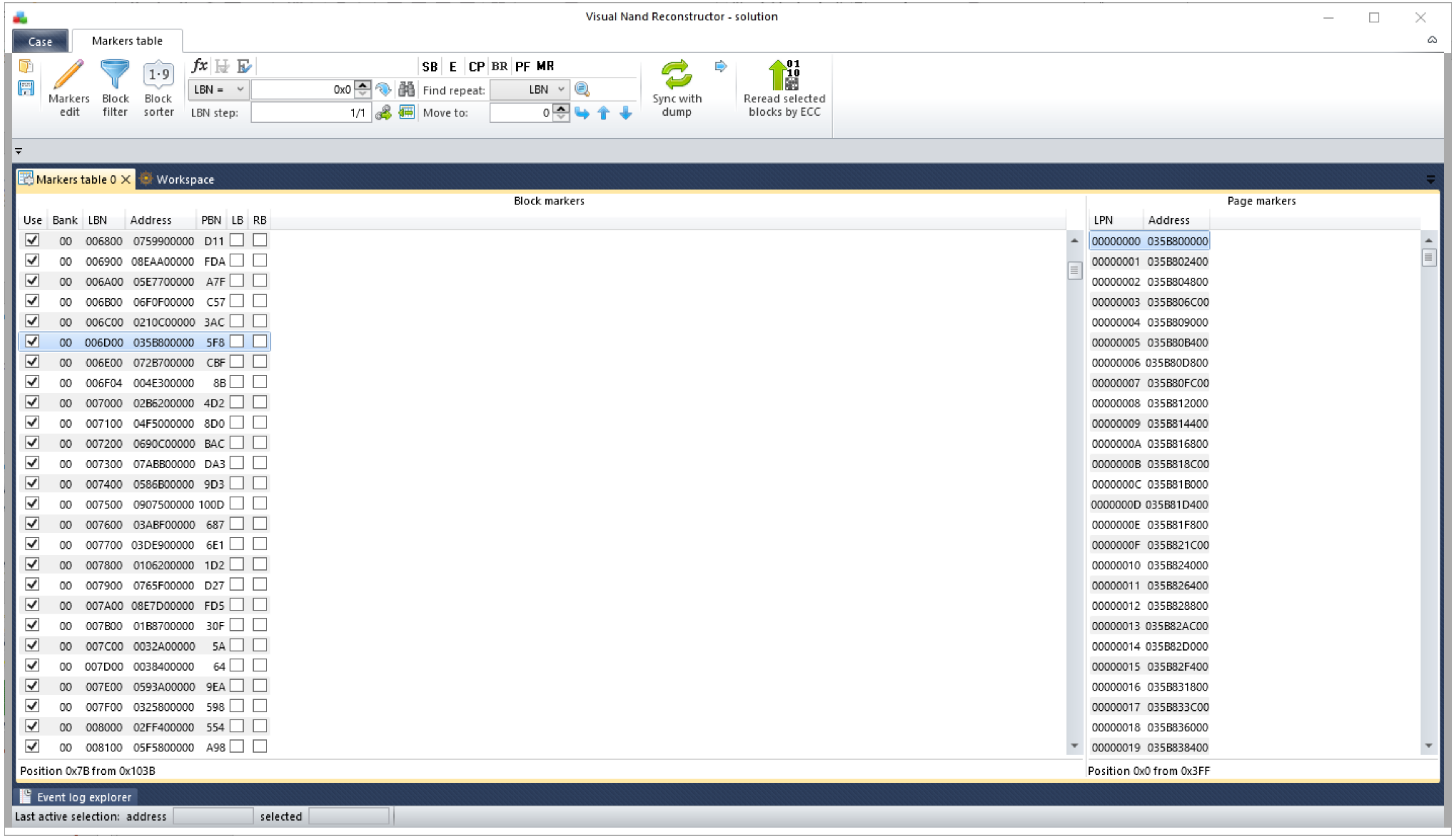
Visual Nand Reconstructor - solution

ECC corrector

Power	Off
ECC codewords	JMicron(JM)\JMF668_8832(ecc70b)_8.bch
Page size	9216
Use buffer	☑
Bytes rotate	□
ECC map	☑ 0

🟩 no errors
🟩 correctable errors
🟥 not correctable er...
⬛ empty

Block translation



LBN = 0x0

LBN step: 1/1

Find repeat: LBN

Move to: 0

Block markers

Use	Bank	LBN	Address	PBN	LB	RB
☑	00	006800	0759900000	D11	☐	☐
☑	00	006900	08EAA00000	FDA	☐	☐
☑	00	006A00	05E7700000	A7F	☐	☐
☑	00	006B00	06F0F00000	C57	☐	☐
☑	00	006C00	0210C00000	3AC	☐	☐
☑	00	006D00	035B800000	5F8	☐	☐
☑	00	006E00	072B700000	CBF	☐	☐
☑	00	006F04	004E300000	8B	☐	☐
☑	00	007000	02B6200000	4D2	☐	☐
☑	00	007100	04F5000000	8D0	☐	☐
☑	00	007200	0690C00000	BAC	☐	☐
☑	00	007300	07ABB00000	DA3	☐	☐
☑	00	007400	0586B00000	9D3	☐	☐
☑	00	007500	0907500000	100D	☐	☐
☑	00	007600	03ABF00000	687	☐	☐
☑	00	007700	03DE900000	6E1	☐	☐
☑	00	007800	0106200000	1D2	☐	☐
☑	00	007900	0765F00000	D27	☐	☐
☑	00	007A00	08E7D00000	FD5	☐	☐
☑	00	007B00	01B8700000	30F	☐	☐
☑	00	007C00	0032A00000	5A	☐	☐
☑	00	007D00	0038400000	64	☐	☐
☑	00	007E00	0593A00000	9EA	☐	☐
☑	00	007F00	0325800000	598	☐	☐
☑	00	008000	02FF400000	554	☐	☐
☑	00	008100	05F5800000	A98	☐	☐

Position 0x7B from 0x103B

Page markers

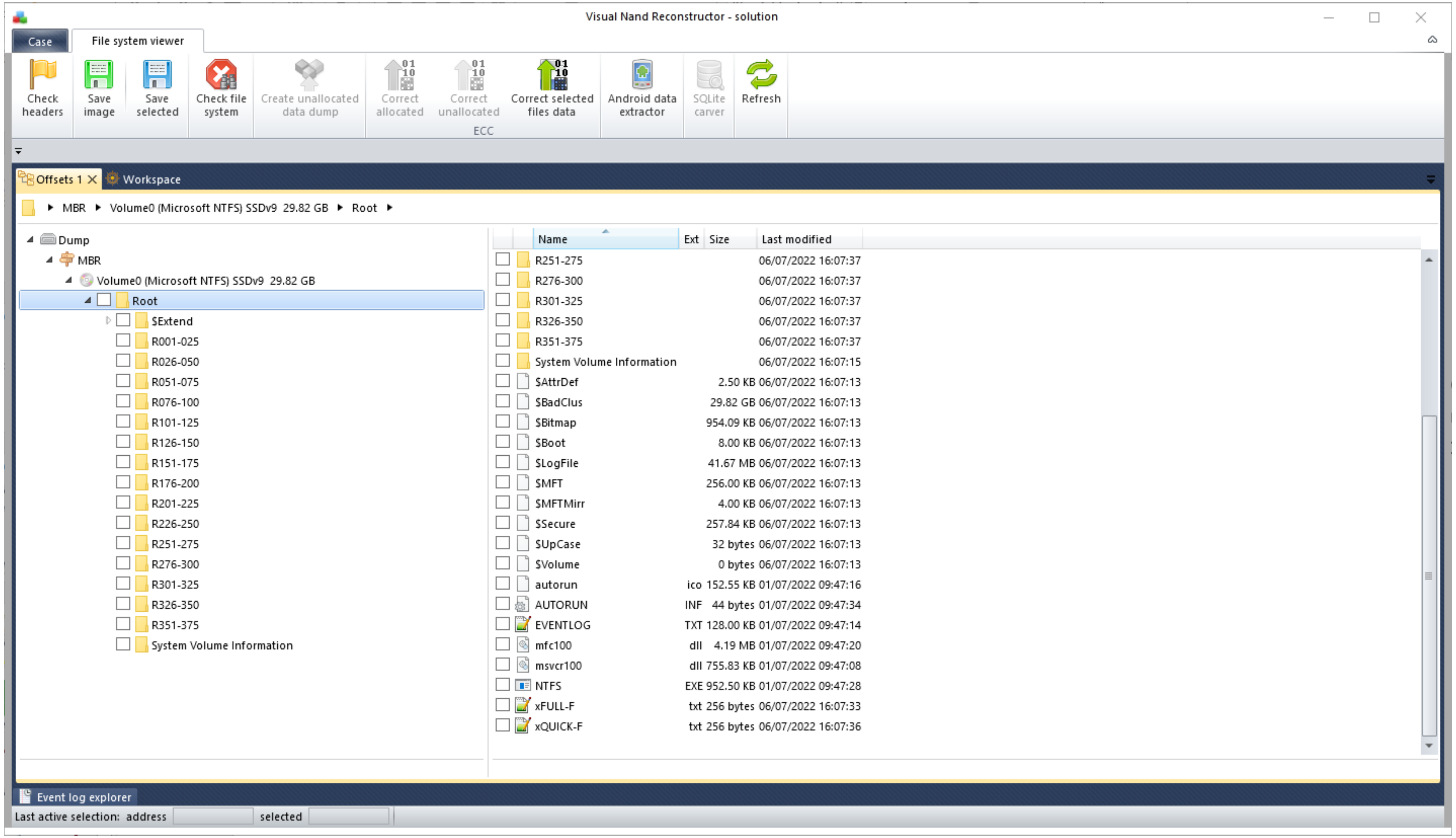
LPN	Address
00000000	035B800000
00000001	035B802400
00000002	035B804800
00000003	035B806C00
00000004	035B809000
00000005	035B80B400
00000006	035B80D800
00000007	035B80FC00
00000008	035B812000
00000009	035B814400
0000000A	035B816800
0000000B	035B818C00
0000000C	035B81B000
0000000D	035B81D400
0000000E	035B81F800
0000000F	035B821C00
00000010	035B824000
00000011	035B826400
00000012	035B828800
00000013	035B82AC00
00000014	035B82D000
00000015	035B82F400
00000016	035B831800
00000017	035B833C00
00000018	035B836000
00000019	035B838400

Position 0x0 from 0x3FF

Last active selection: address selected

Blocks have been properly reorganized according to the logical block number (LBN)

File system reconstructed from NAND ph.image



MBR ▸ Volume0 (Microsoft NTFS) SSDv9 29.82 GB ▸ Root ▸

- Dump
  - MBR
    - Volume0 (Microsoft NTFS) SSDv9 29.82 GB
      - □ Root
        - □ $Extend
        - □ R001-025
        - □ R026-050
        - □ R051-075
        - □ R076-100
        - □ R101-125
        - □ R126-150
        - □ R151-175
        - □ R176-200
        - □ R201-225
        - □ R226-250
        - □ R251-275
        - □ R276-300
        - □ R301-325
        - □ R326-350
        - □ R351-375
        - □ System Volume Information

	Name	Ext	Size	Last modified
□	R251-275			06/07/2022 16:07:37
□	R276-300			06/07/2022 16:07:37
□	R301-325			06/07/2022 16:07:37
□	R326-350			06/07/2022 16:07:37
□	R351-375			06/07/2022 16:07:37
□	System Volume Information			06/07/2022 16:07:15
□	$AttrDef		2.50 KB	06/07/2022 16:07:13
□	$BadClus		29.82 GB	06/07/2022 16:07:13
□	$Bitmap		954.09 KB	06/07/2022 16:07:13
□	$Boot		8.00 KB	06/07/2022 16:07:13
□	$LogFile		41.67 MB	06/07/2022 16:07:13
□	$MFT		256.00 KB	06/07/2022 16:07:13
□	$MFTMirr		4.00 KB	06/07/2022 16:07:13
□	$Secure		257.84 KB	06/07/2022 16:07:13
□	$UpCase		32 bytes	06/07/2022 16:07:13
□	$Volume		0 bytes	06/07/2022 16:07:13
□	autorun	ico	152.55 KB	01/07/2022 09:47:16
□	AUTORUN	INF	44 bytes	01/07/2022 09:47:34
□	EVENTLOG	TXT	128.00 KB	01/07/2022 09:47:14
□	mfc100	dll	4.19 MB	01/07/2022 09:47:20
□	msvcr100	dll	755.83 KB	01/07/2022 09:47:08
□	NTFS	EXE	952.50 KB	01/07/2022 09:47:28
□	xFULL-F	txt	256 bytes	06/07/2022 16:07:33
□	xQUICK-F	txt	256 bytes	06/07/2022 16:07:36

Last active selection: address selected

We have been able to successfully reconstruct file system for this SSD, and solution should generally work on all devices with same controller, NAND and capacity.

Conclusion:
The SLC memory chip used in this device is very reliable. Even in the critical scenario of thermal damage, there’s still high chance of successful data recovery. As long as memory chip is not cracked physically, the flight recorder is failproof.
Controller’s data translation algorithm was fully reverse engineered and logical image was reconstructed.
It can be fed to the vendor’s software for the flight accident data extraction.

Most of the black box pictures and testing materials were kindly provided by Etep
www.etep.com

Thank you!

Visit our booth 107 for more details and experience.