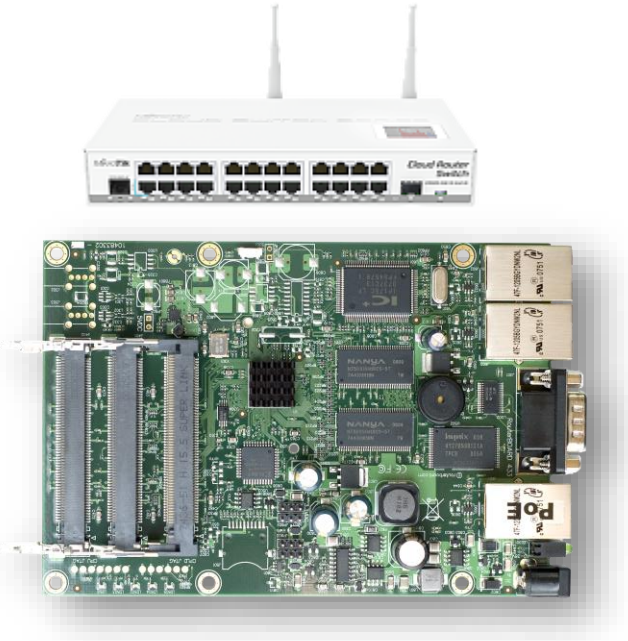
Forensic analysis of flash memory using X-RAY and Logic Analyzer

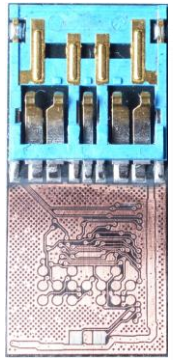
Rusolut, Poland

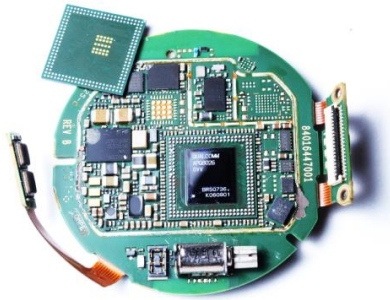
ruSolut
Data Investigation & Recovery Technology

PTXXI 2022 IV Konferencja Naukowa
PRZESTĘPCZOŚĆ TELEINFORMATYCZNA XXI WIEKU

EMBEDDED DEVICES







DIGITAL FORENSICS IS FAR BEHIND THE MODERN TECH

- It’s not just computer or mobile forensics anymore.
- The digital and IoT evolution is extremely rapid.
- Tons of digital evidence is missed/ignored
- HW vendors are not obliged to cooperate and they usually don’t
- Modern hardware is “multi-layered”, so multiple vendors involved
- Reverse engineering is by far one of the very few solutions

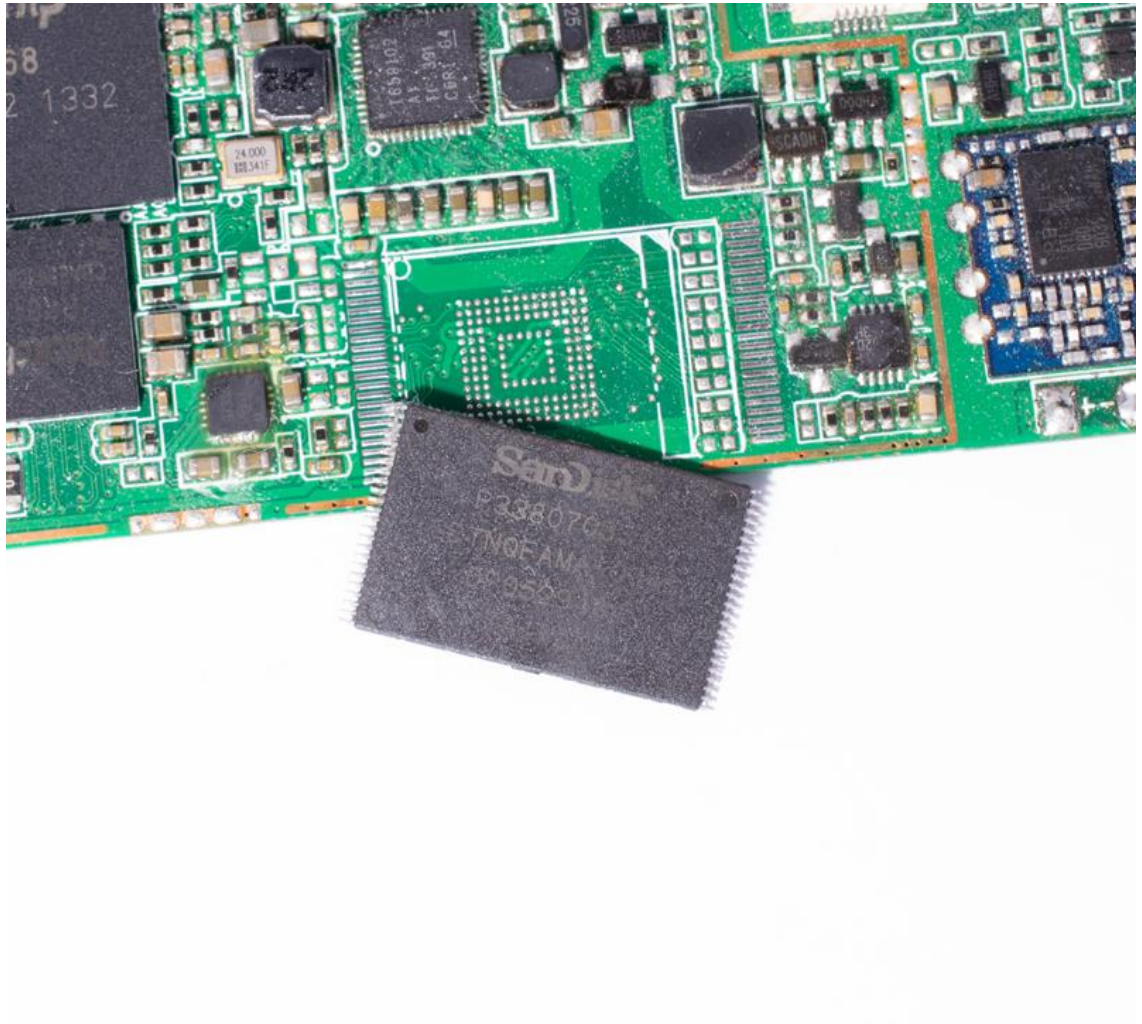
IN MOST EMBEDDED DEVICES DATA STORED IN NON-VOLATILE FLASH MEMORY

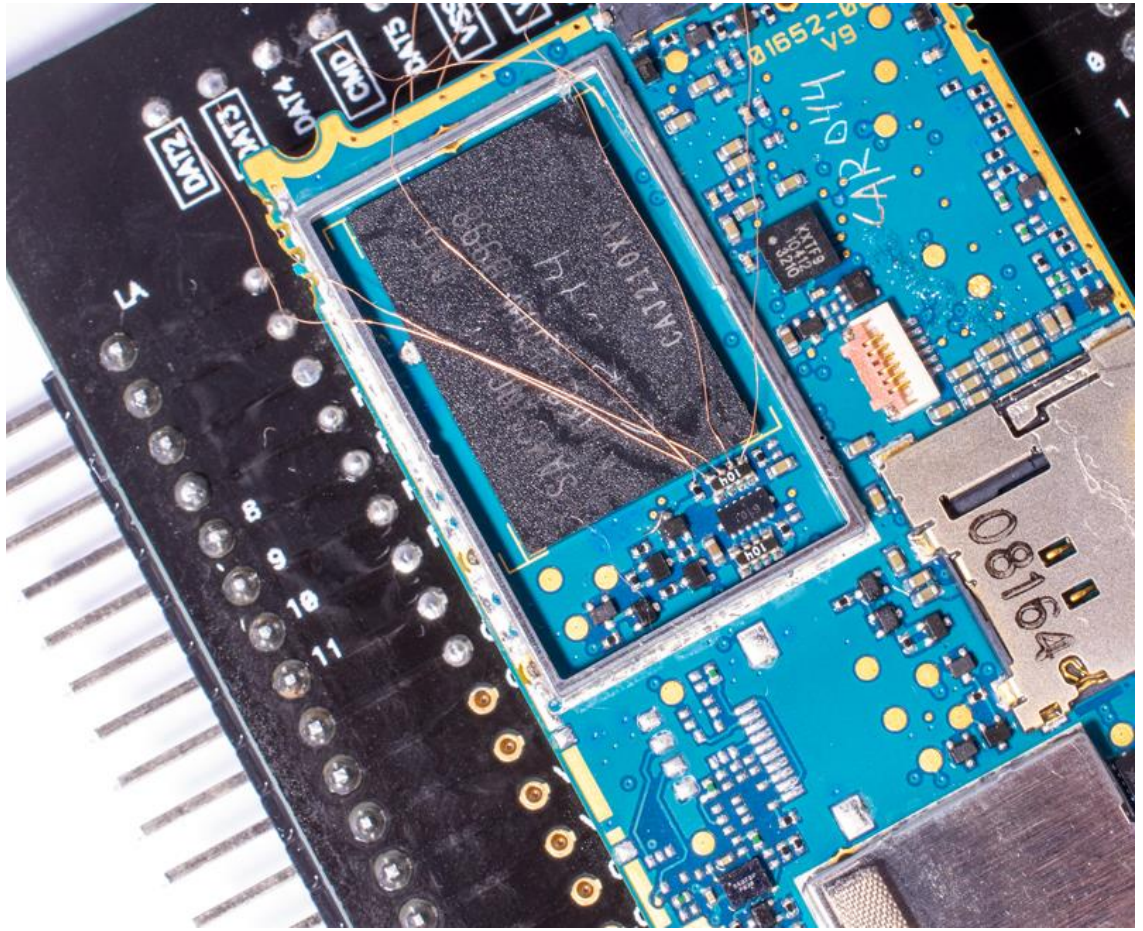
- Serial Flash, FeRAM (SPI, I2C interfaces)
- Parallel NOR/NAND flash (CFI interface)
- **NAND flash (NAND interface)**

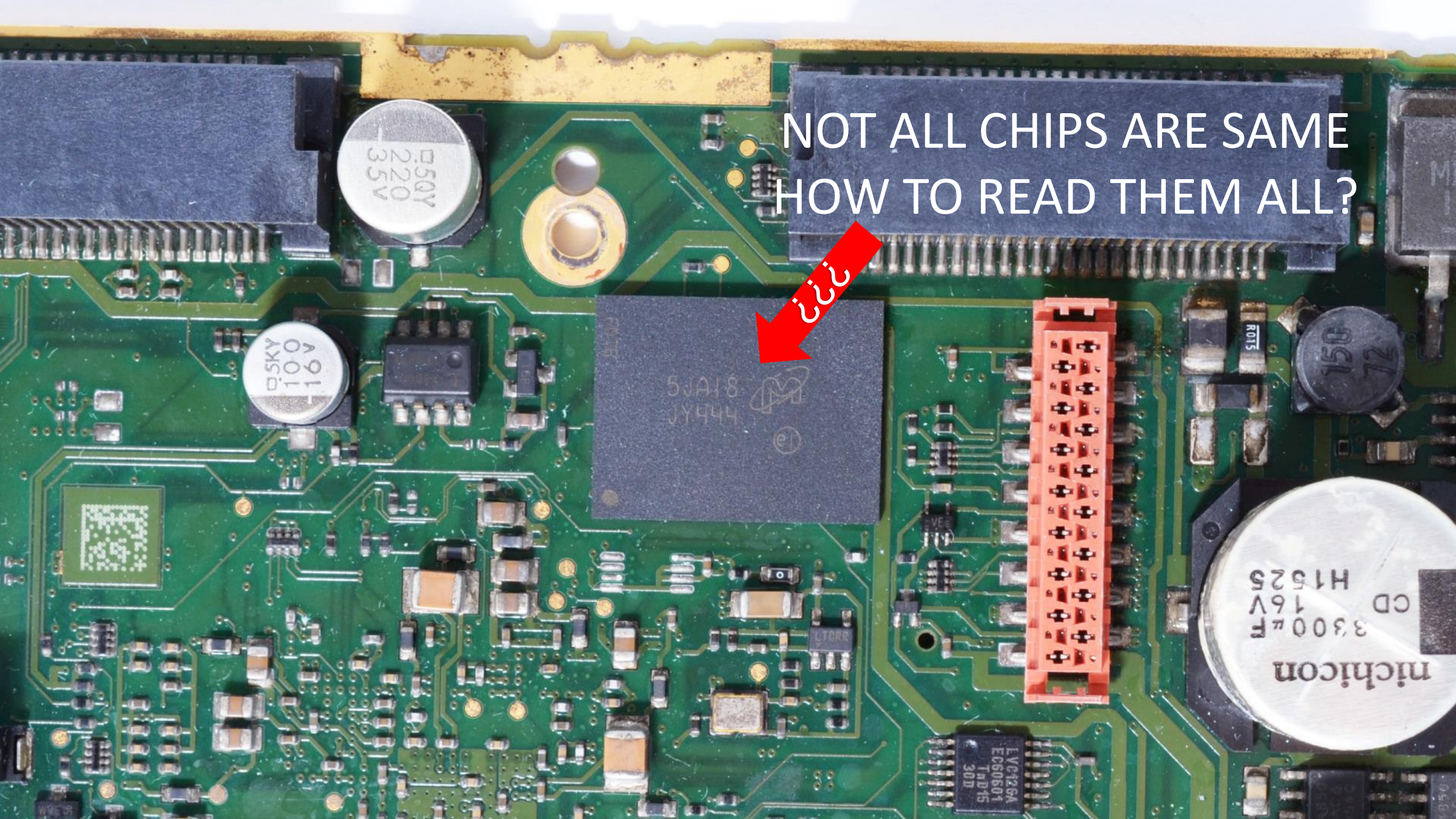
WHEN DATA EXTRACTION DIRECTLY FROM MEMORY CHIP IS THE ONLY SOLUTION?

- Devices where standard interface isn’t working/disabled
- Physically broken devices
- Non-working devices/corrupted FW
- Embedded devices w/o external interface
- Proprietary interface
- Extraction of erased data
- Locked eMMC chips and SD cards

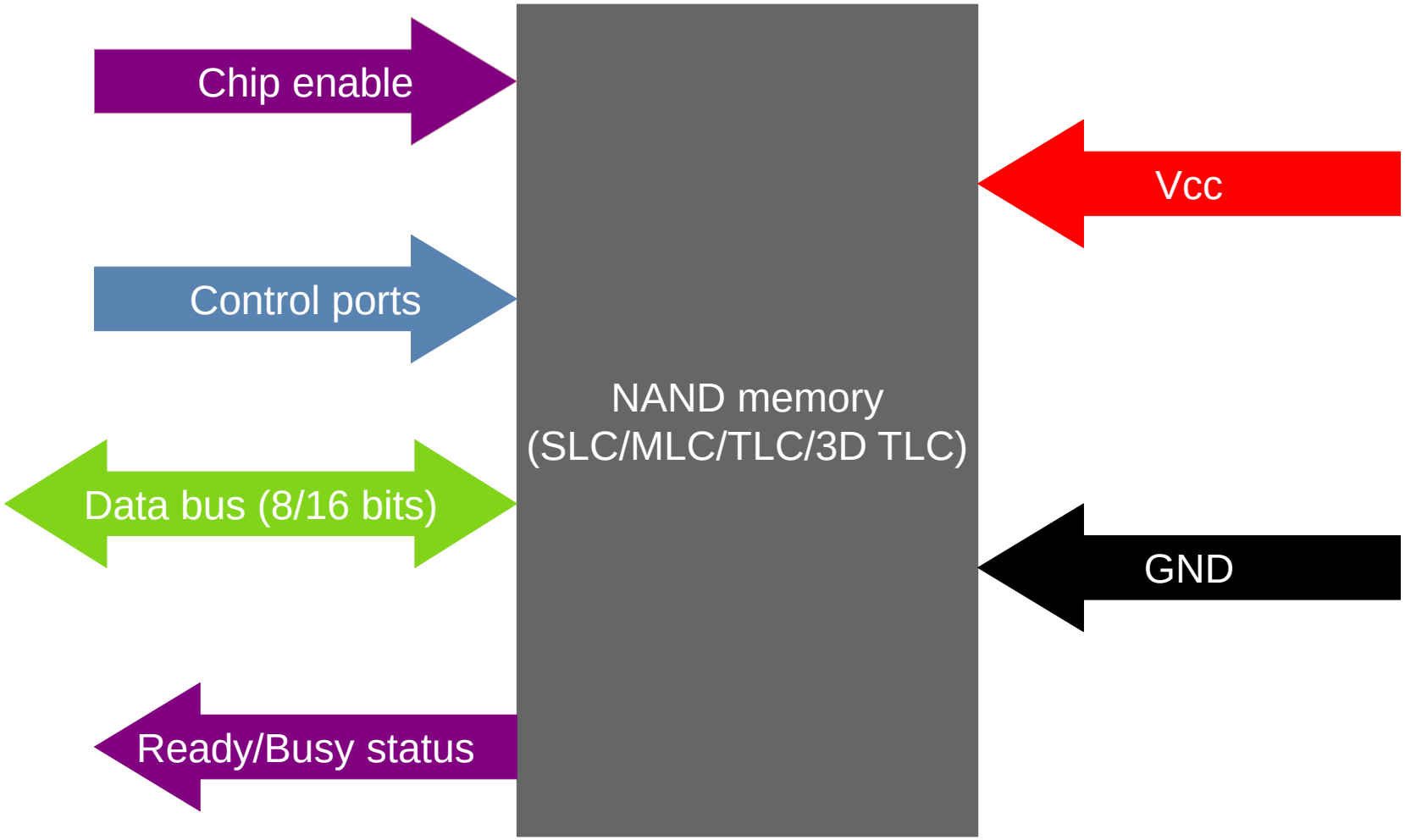
DIRECT FLASH MEMORY ACCESS CHIP-OFF OR ON-CHIP



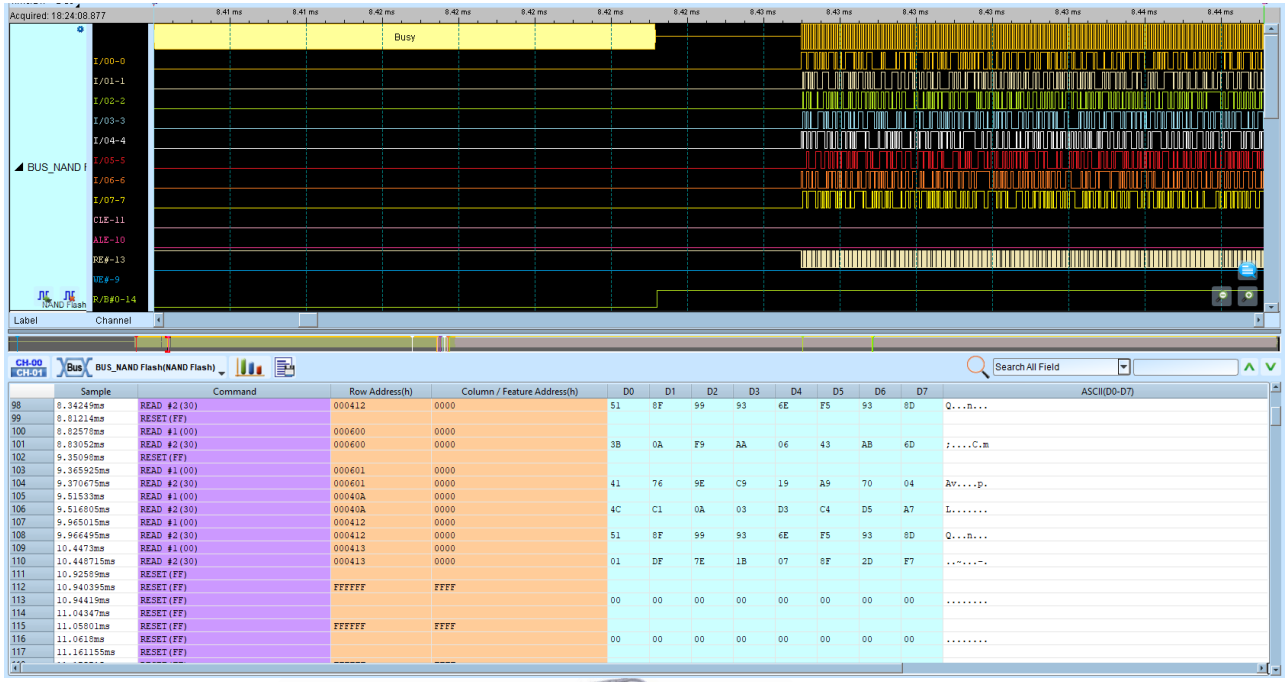



NOT ALL CHIPS ARE SAME
HOW TO READ THEM ALL?
¿¿¿
5JA18
JY444
nichicon

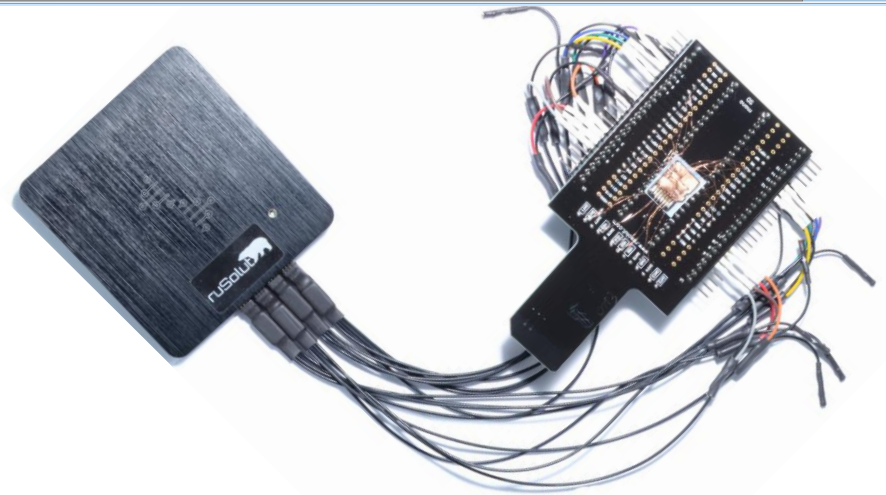
NAND INTERFACE



LOGIC ANALYZER & XRAY

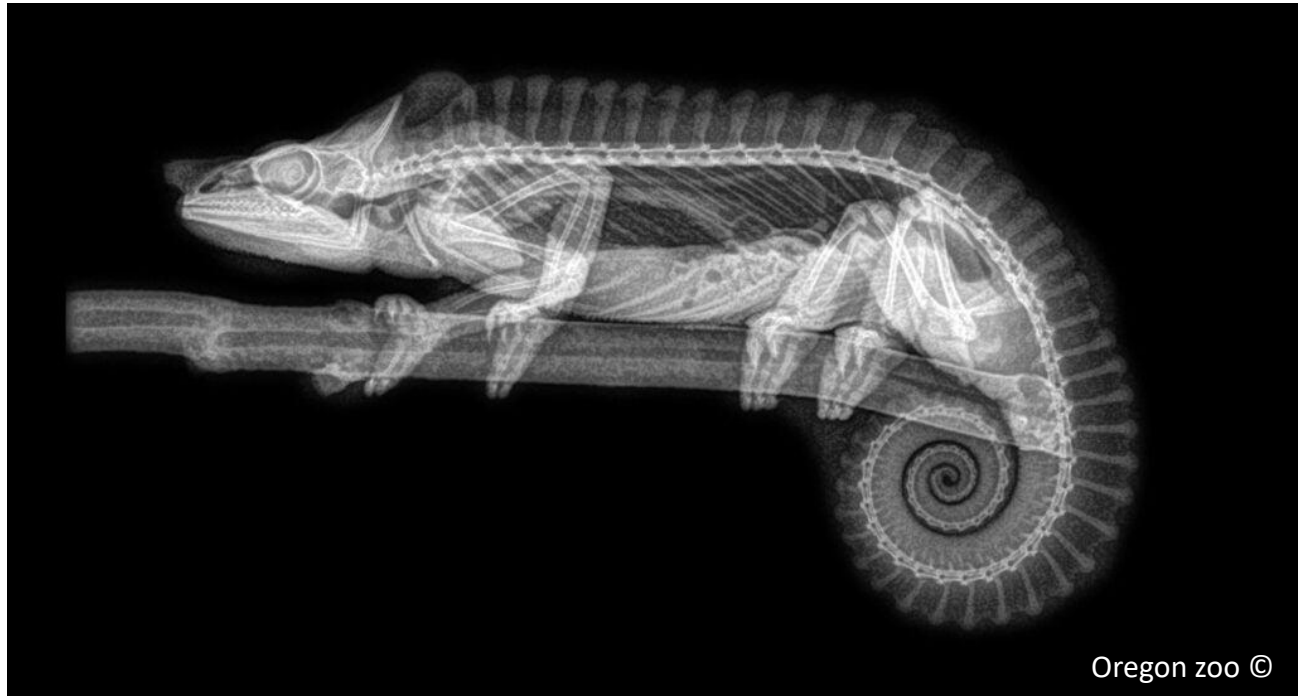


	Sample	Command	Row Address(h)	Column / Feature Address(h)	D0	D1	D2	D3	D4	D5	D6	D7	ASCII(D0-D7)
98	8.34249ms	READ #2(30)	000412	0000	51	8F	99	93	6E	F5	93	8D	Q...n...
99	8.81214ms	RESET(FF)											
100	8.82578ms	READ #1(00)	000600	0000									
101	8.83052ms	READ #2(30)	000600	0000	3B	0A	F9	AA	06	43	AB	6D	;....C.m
102	9.35098ms	RESET(FF)											
103	9.365925ms	READ #1(00)	000601	0000									
104	9.370675ms	READ #2(30)	000601	0000	41	76	9E	C9	19	A9	70	04	Av....p.
105	9.51533ms	READ #1(00)	00040A	0000									
106	9.516805ms	READ #2(30)	00040A	0000	4C	C1	0A	03	D3	C4	D5	A7	L.....
107	9.965015ms	READ #1(00)	000412	0000									
108	9.966495ms	READ #2(30)	000412	0000	51	8F	99	93	6E	F5	93	8D	Q...n...
109	10.4473ms	READ #1(00)	000413	0000									
110	10.448715ms	READ #2(30)	000413	0000	01	DF	7E	1B	07	8F	2D	F7	..~...-.
111	10.92589ms	RESET(FF)											
112	10.940395ms	RESET(FF)	FFFFFF	FFFF									
113	10.94419ms	RESET(FF)			00	00	00	00	00	00	00	00	....
114	11.04347ms	RESET(FF)											
115	11.05801ms	RESET(FF)	FFFFFF	FFFF									
116	11.0618ms	RESET(FF)			00	00	00	00	00	00	00	00	....
117	11.161155ms	RESET(FF)											

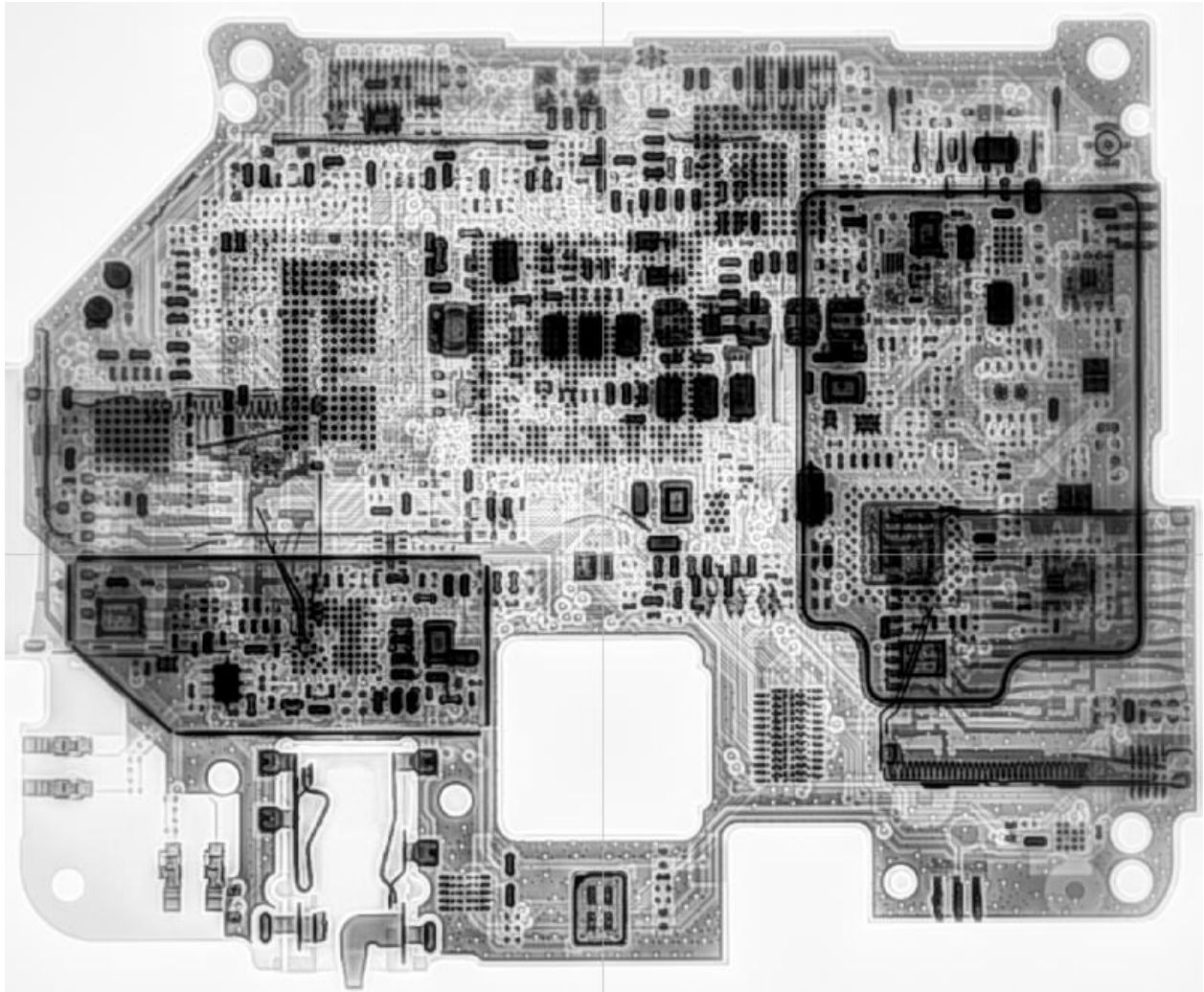


WHAT CAN YOU DO WITH XRAY?

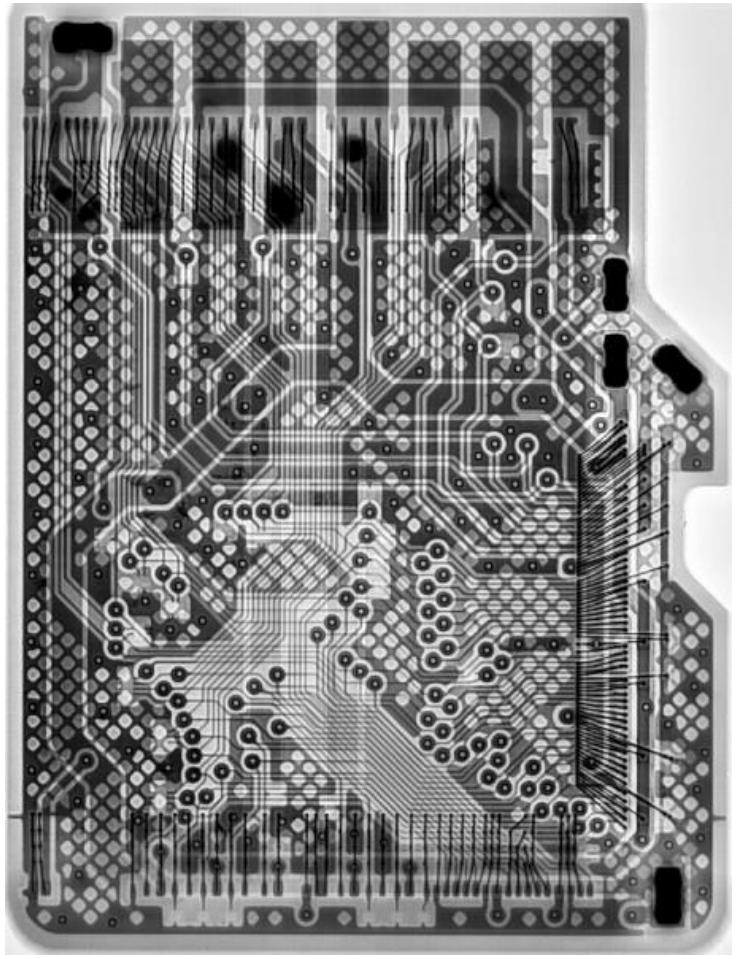
- Structural analysis of device
- Damage assessment
- PCB-to-chip analysis of traces
- **Helps to build flash memory pinout**

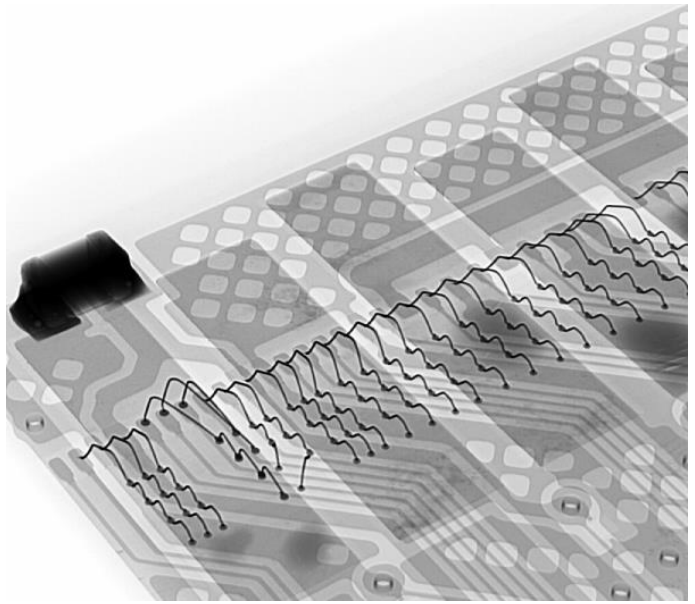


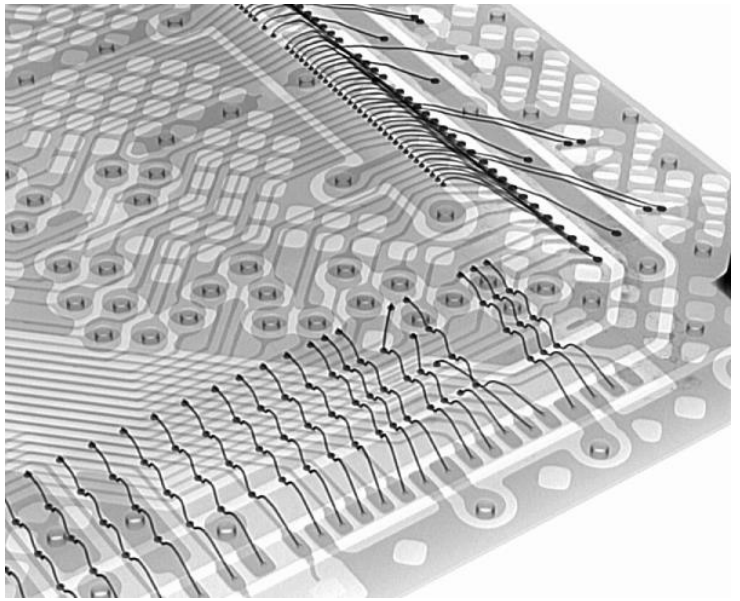
STRUCTURAL ANALYSIS OF DEVICE

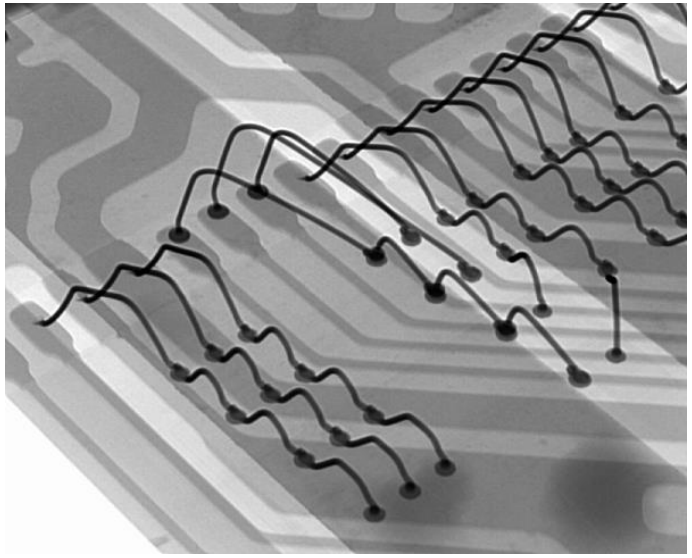


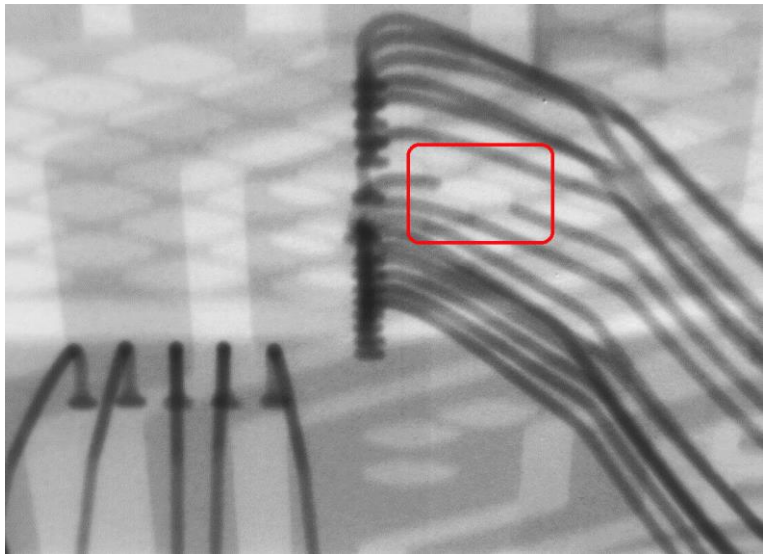
DAMAGE ASSESSMENT



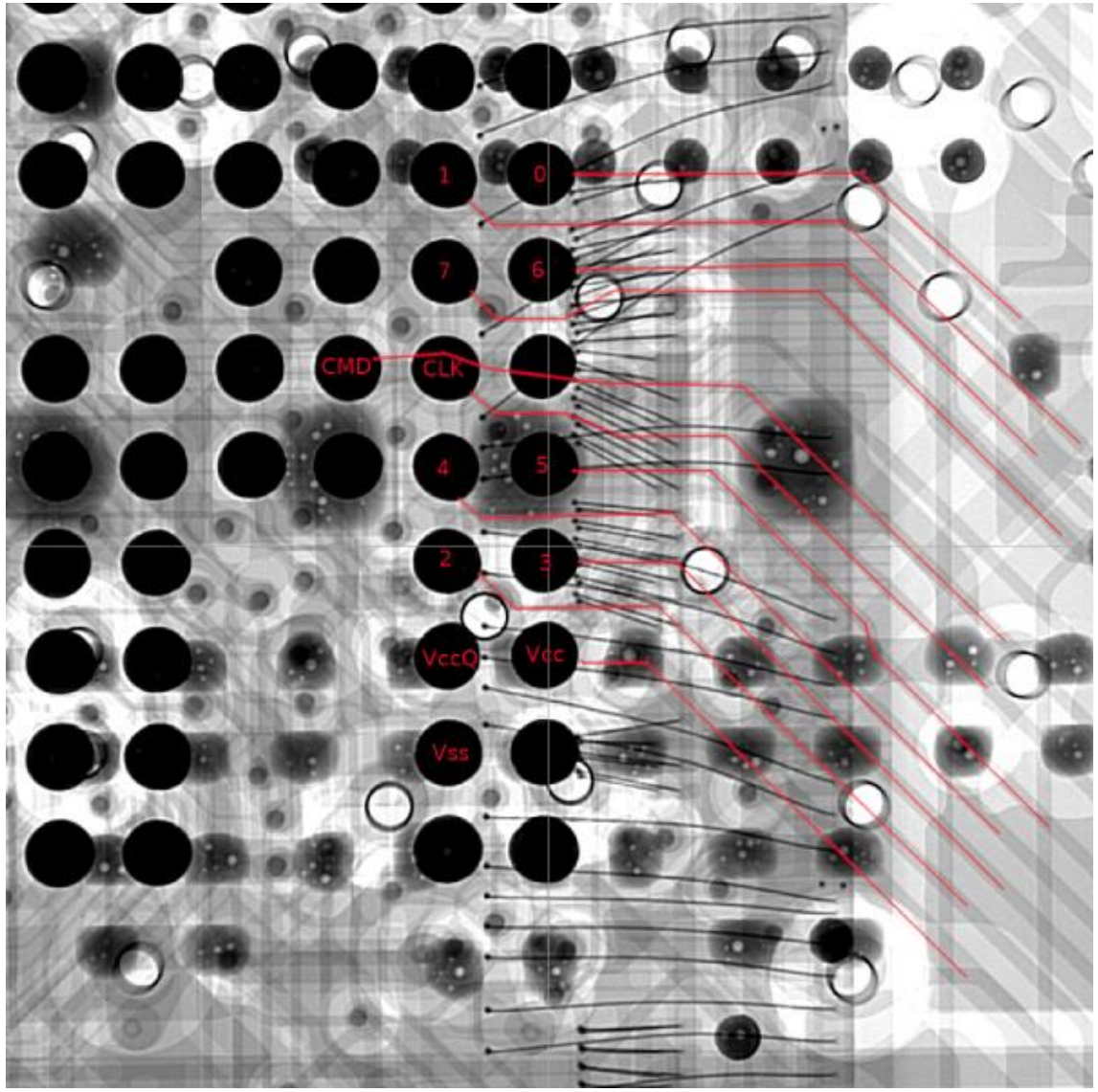




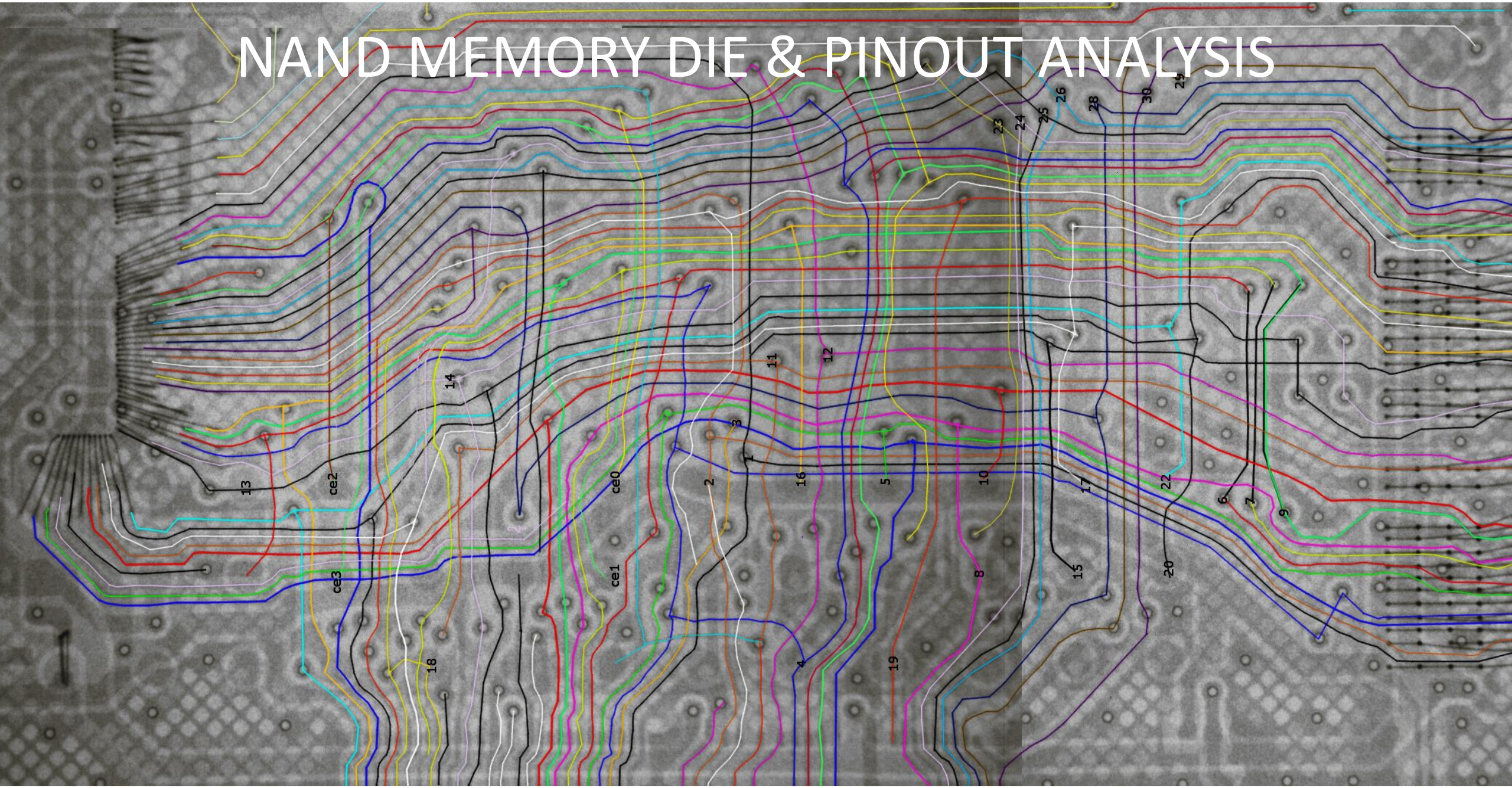




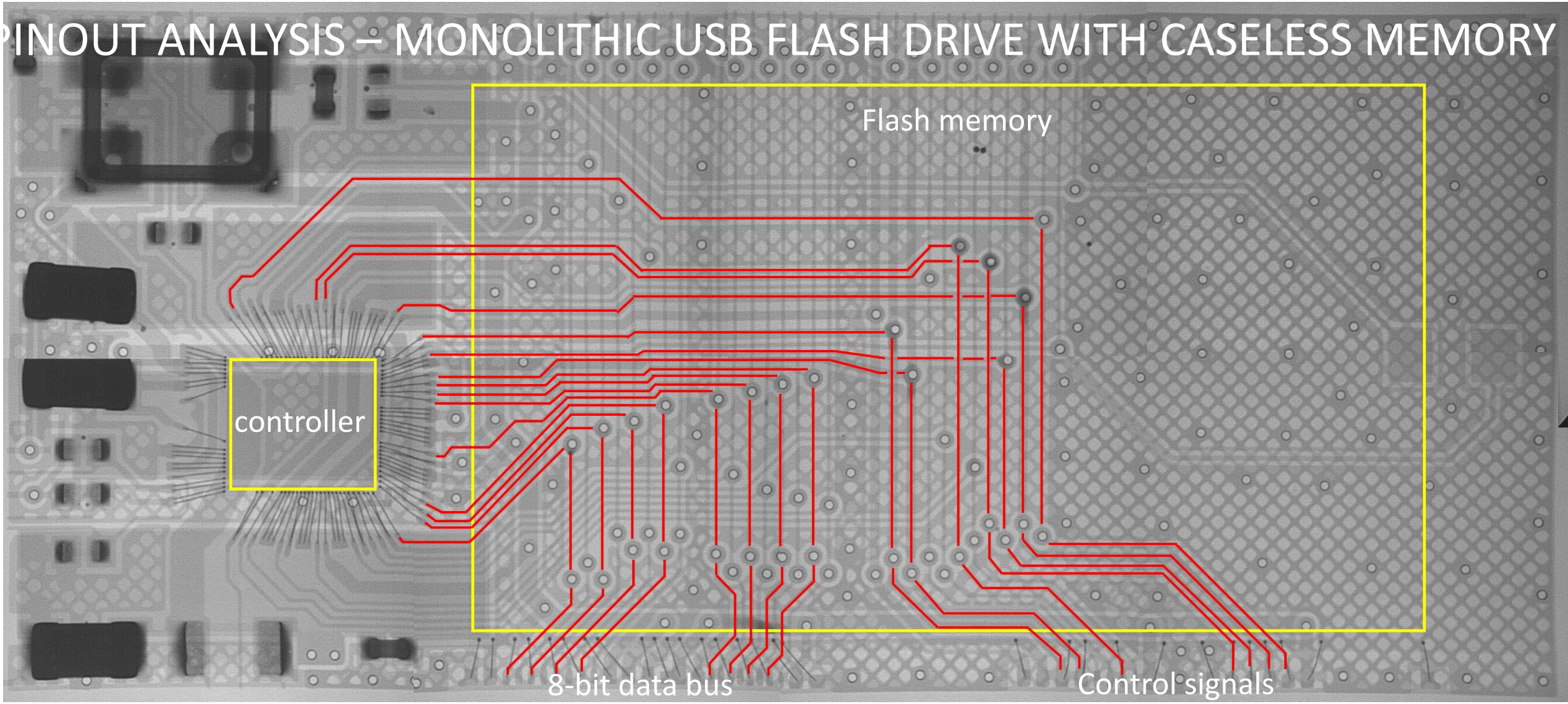
PCB-CHIP ANALYSIS OF MEMORY TRACES



NAND MEMORY DIE & PINOUT ANALYSIS



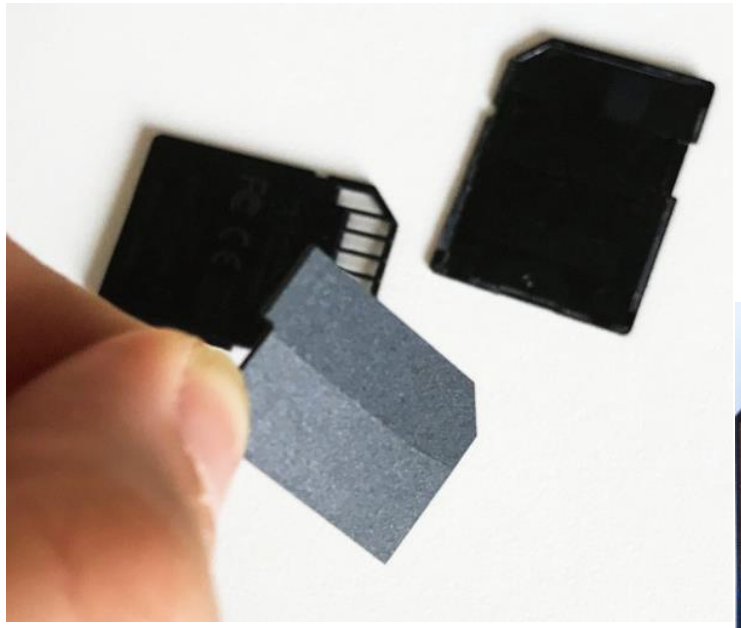
PINOUT ANALYSIS – MONOLITHIC USB FLASH DRIVE WITH CASELESS MEMORY

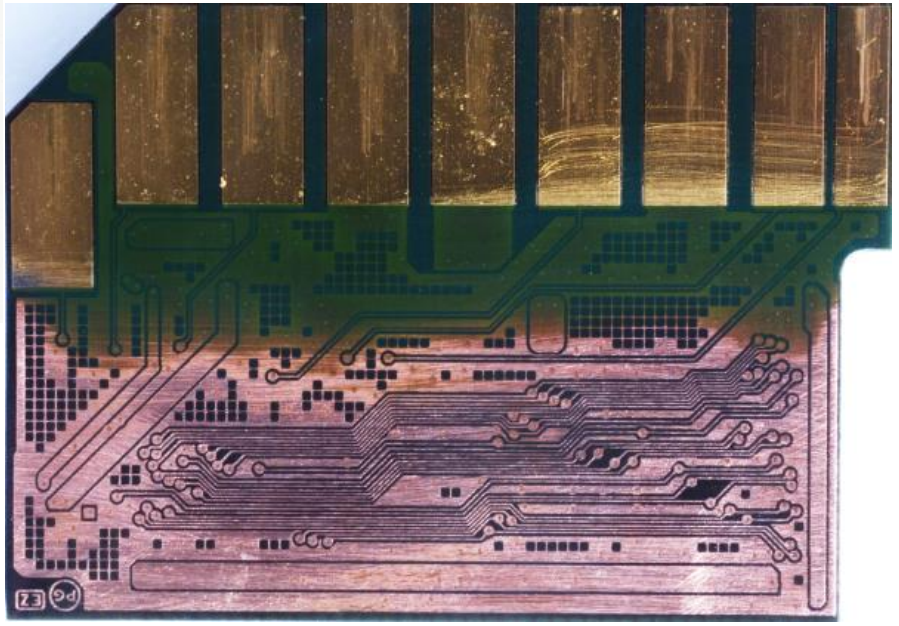


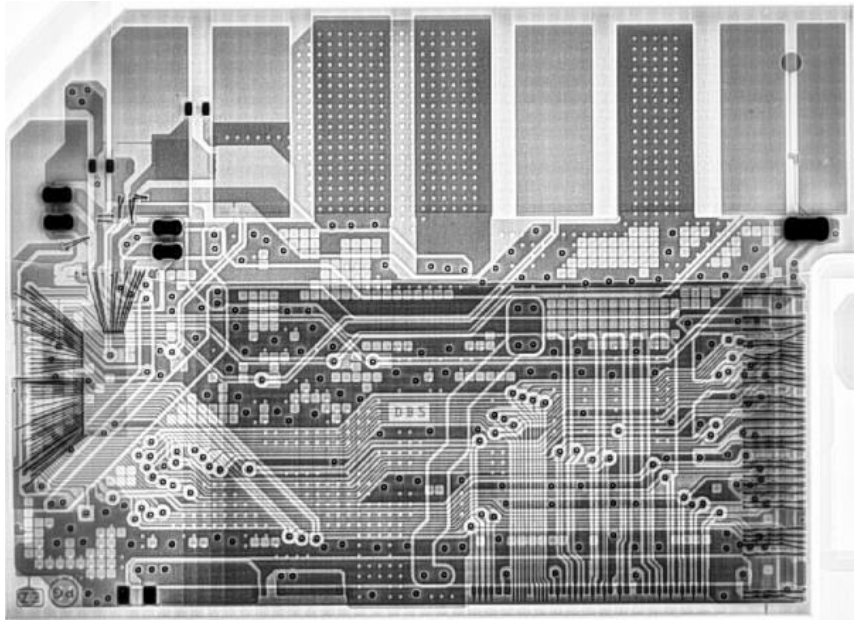
PINOUT ANALYSIS

- Find power lines and GNDs – they are thick
- Find 8 (16) similar tracks – it’s data bus
- The rest is control signals. It takes a bit of practise to be able to recognize their order

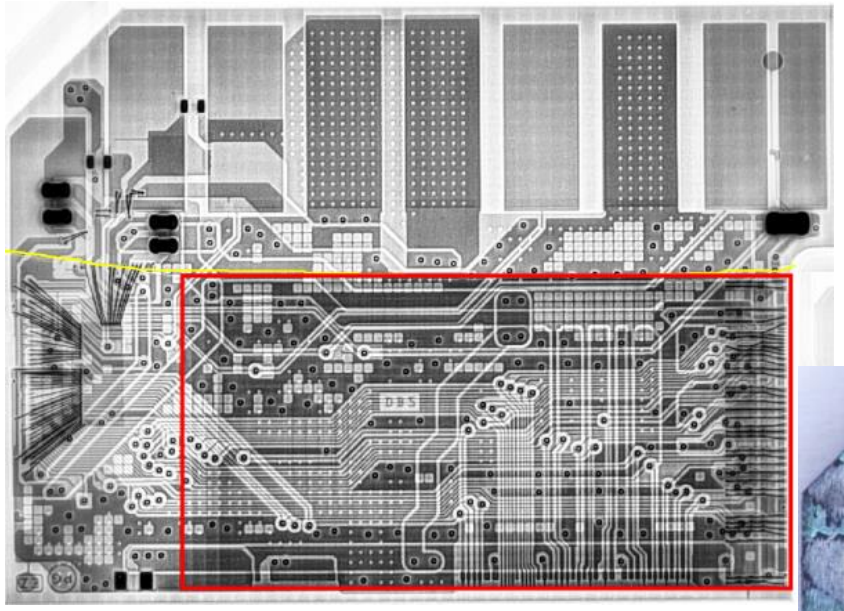
REAL LIFE CASE

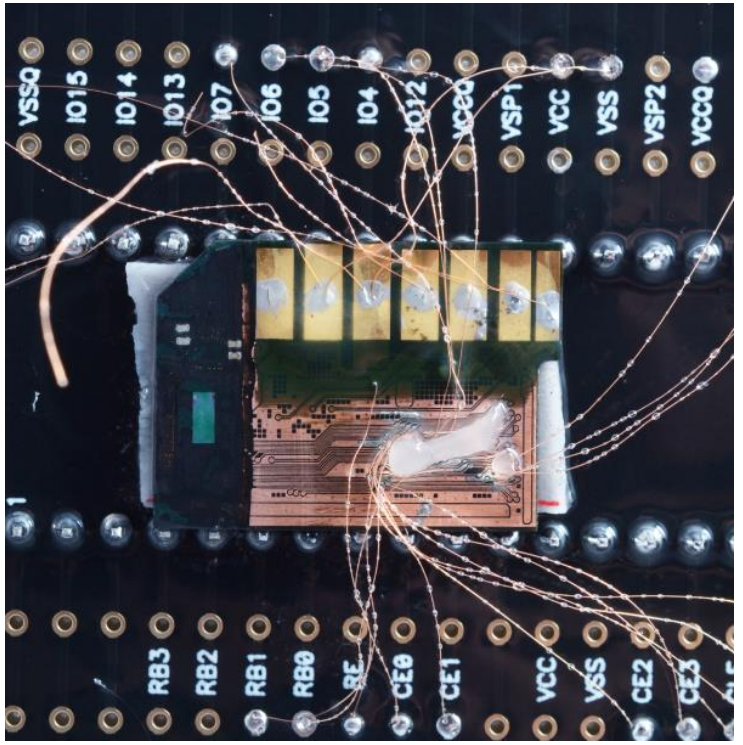






WIRED UP

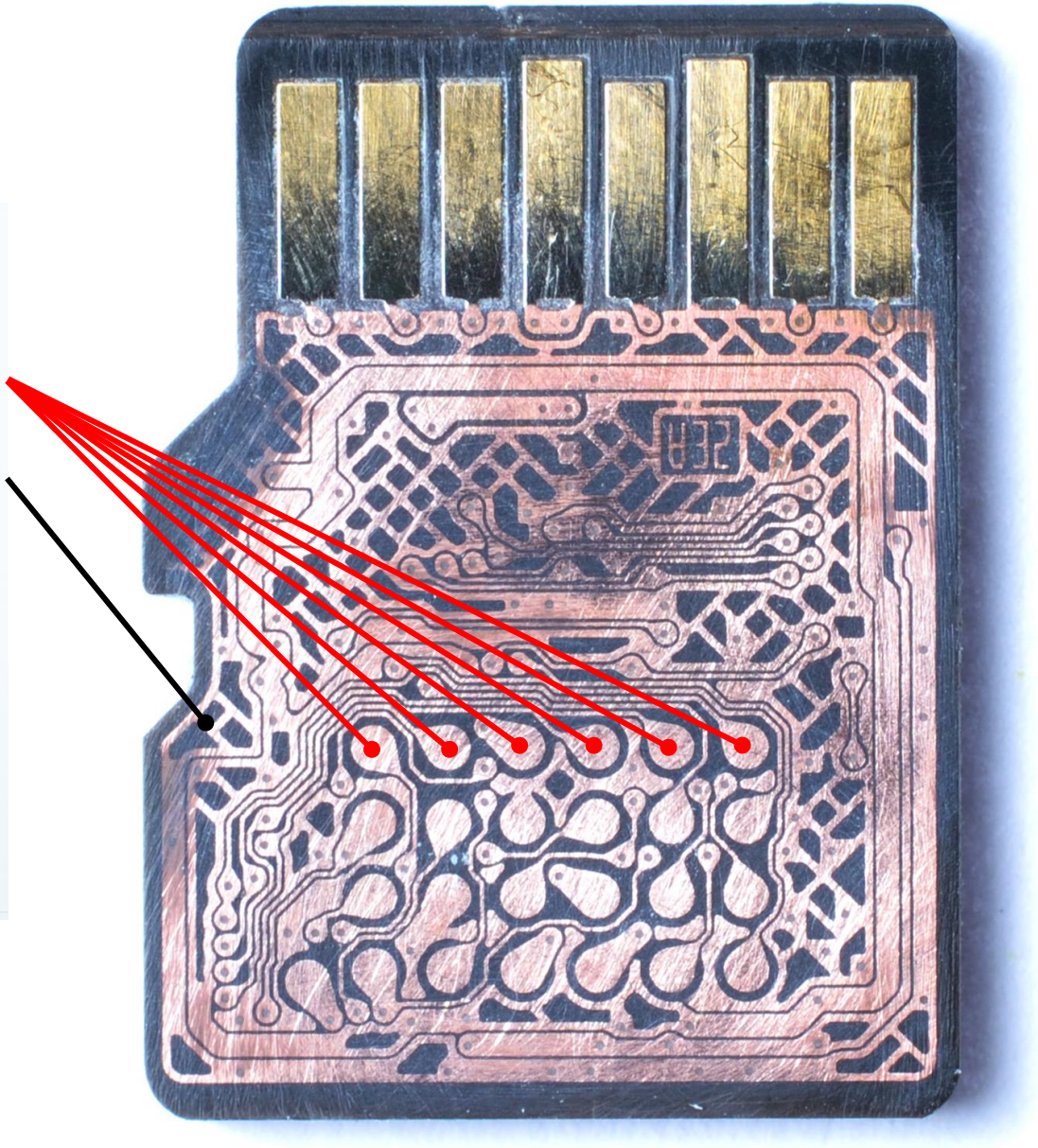



VSS0
IO15
IO14
IO13
IO7
IO6
IO5
IO4
IO12
VCC0
VSP1
VCC
VSS
VSP2
VCCQ
RB3
RB2
RB1
RB0
RE
CE0
CE1
VCC
VSS
CE2
CE3

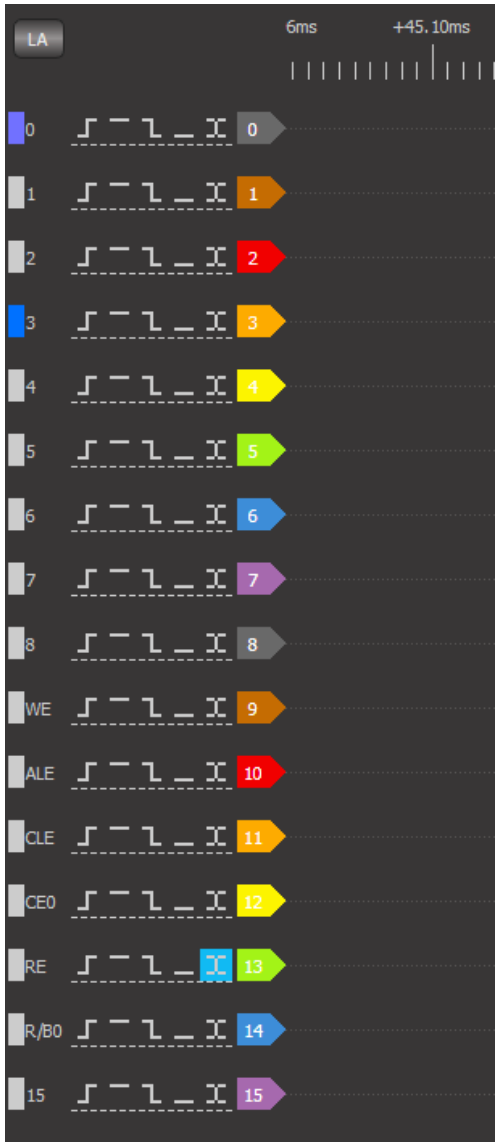
LOGIC ANALYZER, WHY?

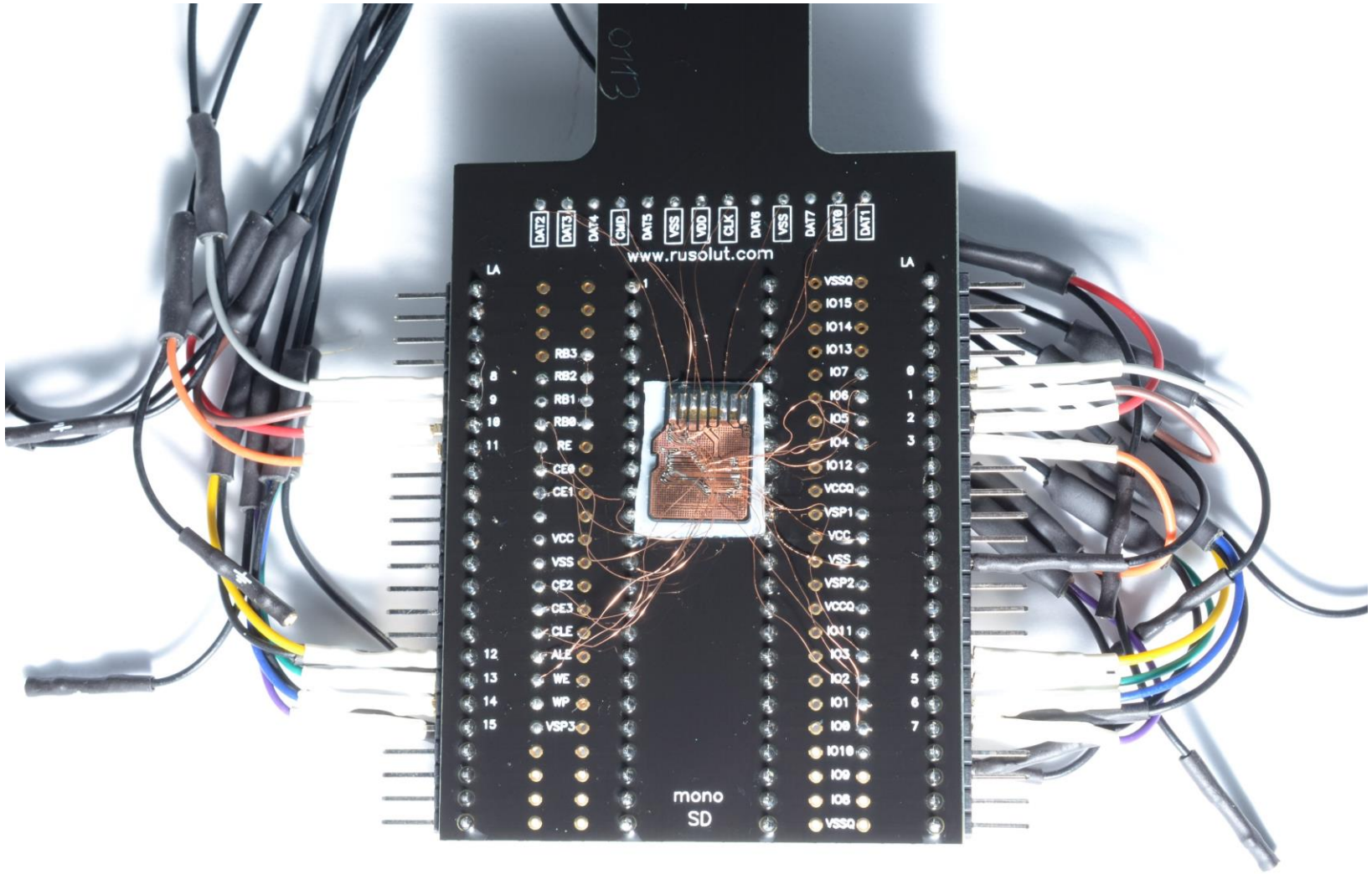
- The basic tool for man-in-the-middle signal analysis in the digital data transfer channel
- Unknown pinout of the memory analysis
- Real time data sniffing (passwords, parameters, etc)
- Unknown protocol of communication (commands, register addresses, etc)

DEFINE THE SCOPE OF WORK



INITIAL RANDOM WIRING TO LOGIC ANALYZER





THE BASIC KNOWLEDGE OF INTERFACE IS REQUIRED

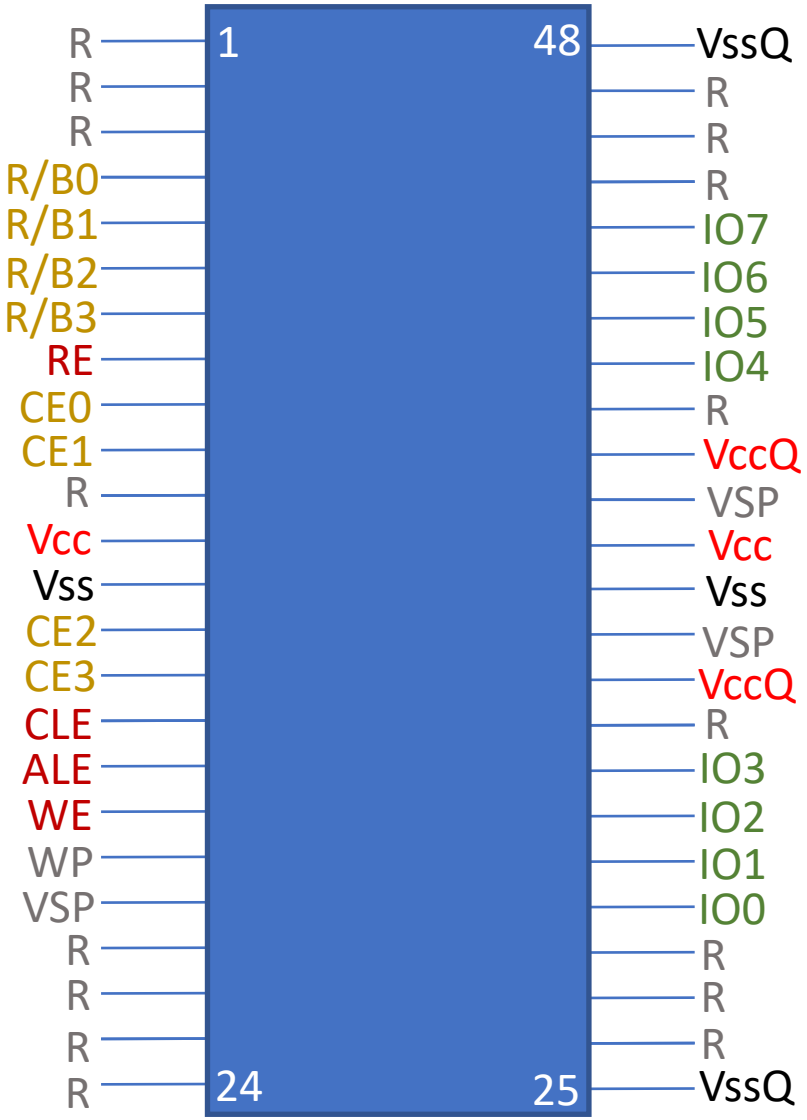
IO0…IO7 – Data bus

Vcc/VccQ – power 3,3 ... 1,8 V

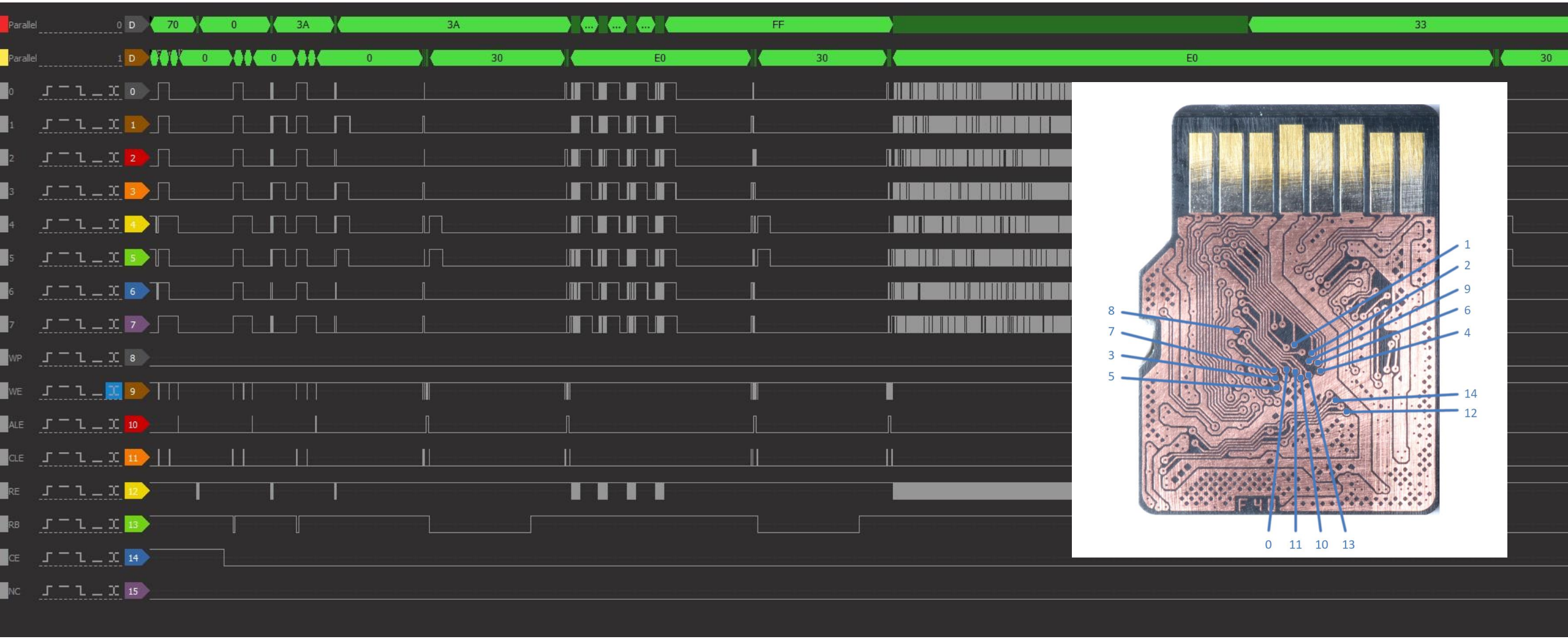
Vss/VssQ - Ground

CLE – Command latch enable
ALE – Address latch enable
RE – Read enable
WE – Write enable

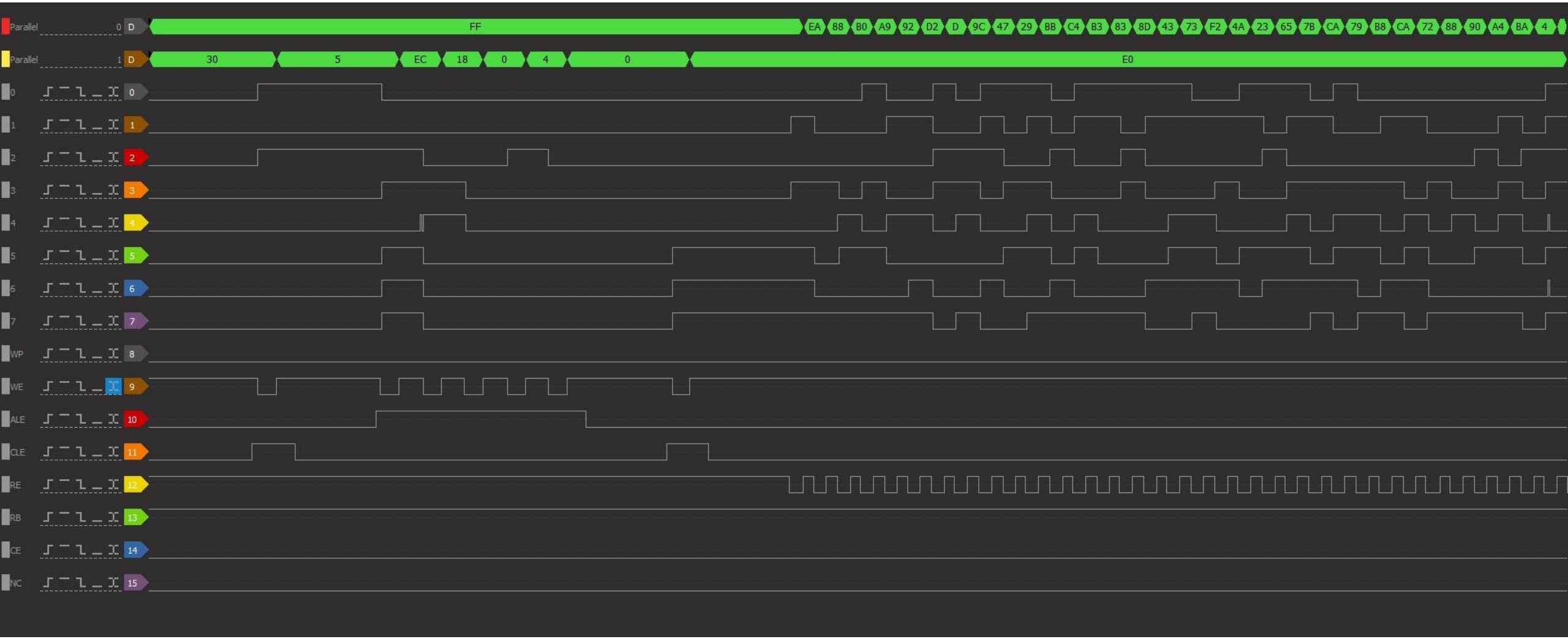
R/B0…R/B3 – Ready/Busy status
CE0…CE3 – Crystal enable



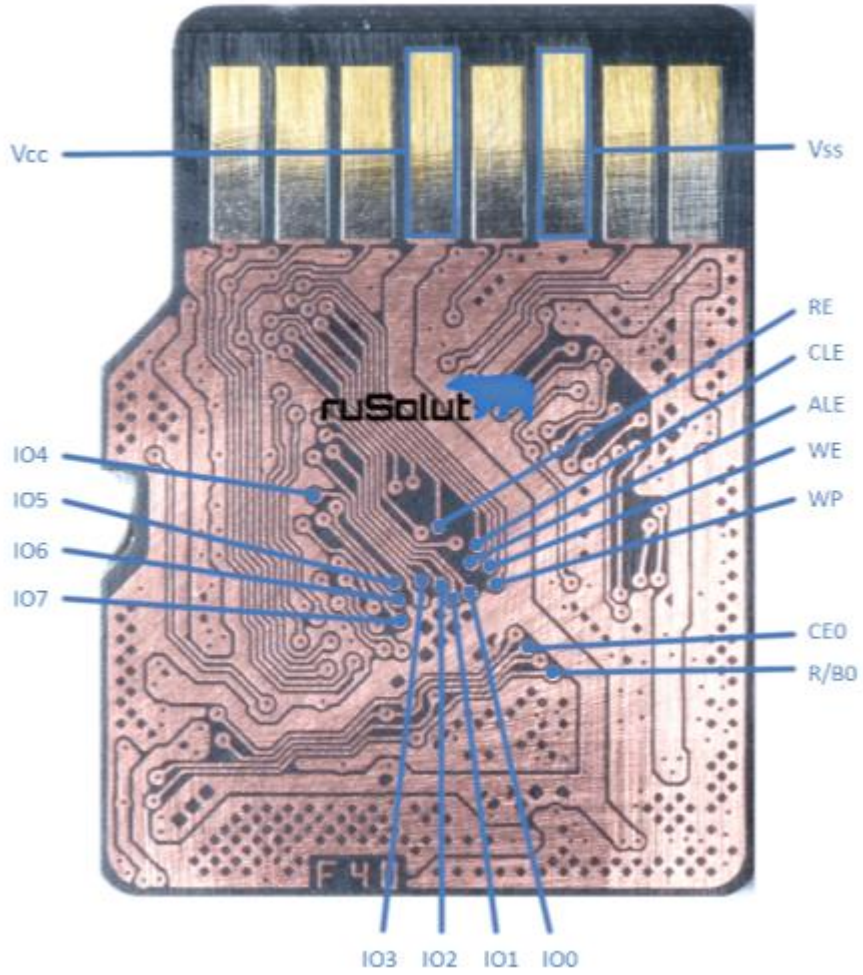
POWER UP YOUR “PATIENT” DEVICE AND READ THE SIGNALS



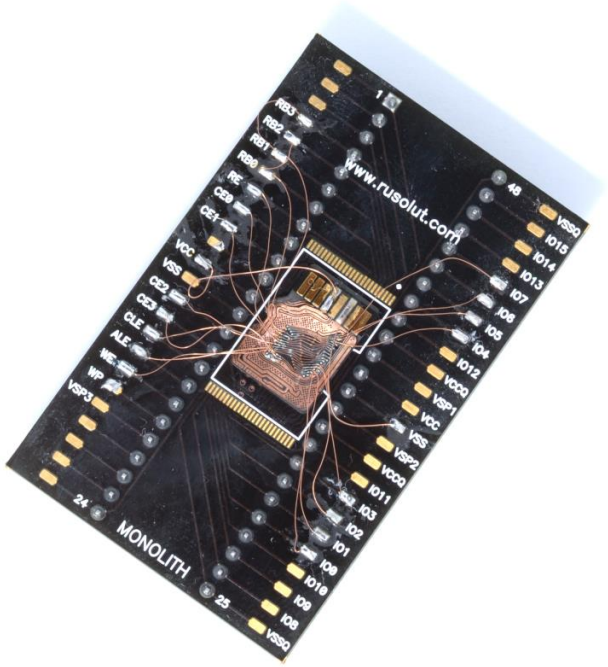
FIND SIGNAL PATTERNS AND IDENTIFY ALL THE SIGNALS OF THE PROTOCOL



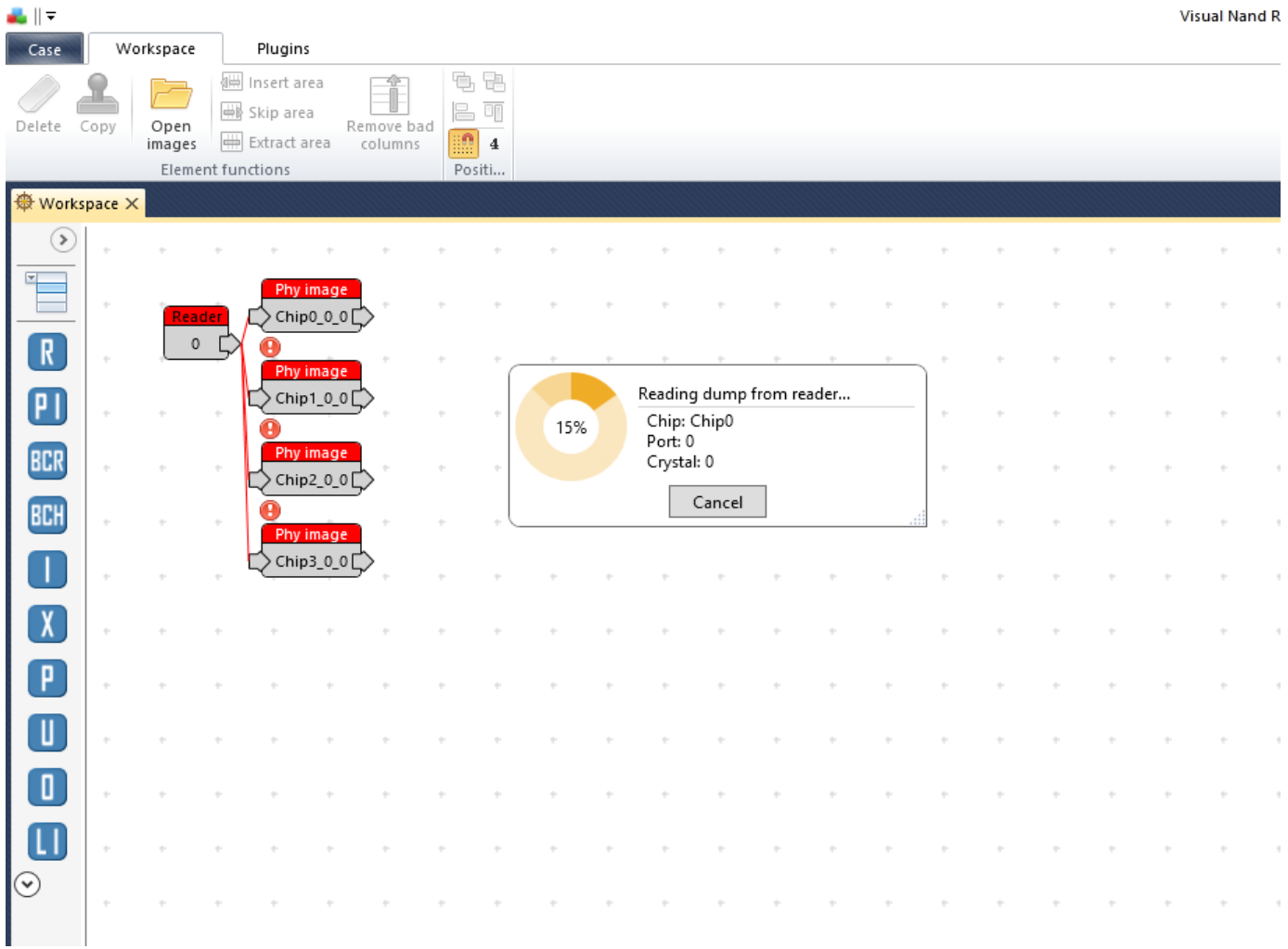
PINOUT IS FOUND



ONCE PINOUT IS FOUND - CONNECT DEVICE TO READER



READ THE DUMP, ANALYZE IT AND GET THE DATA



THANK YOU!

We have next session tomorrow
with case studies!

SASHA@RUSOLUT.COM