hardwear.io

Hardware Security Conference and Training

Hacking NAND Memory Pinout using Logic Analyzer

Alexander “Sasha” Sheremetov, Rusolut, Poland

RUSOLUT

WHO NEEDS THAT?

EVERYONE WHO HAS EVER WORKED WITH:

- PORTABLE STORAGE (CARDS, FLASHDRIVES, ETC)
- VEHICLE INFOTAINMENT SYSTEMS, ECUs, etc
- SMARTPHONES
- TABLETS
- DRONES
- ROUTERS
- WEARABLES/SMARTWATCHES
- LAPTOPS
- SOLID STATE DRIVES
- VOICE RECORDERS
- MULTIMEDIA PLAYERS
- SMART TV
- INTERNET OF THINGS

…AND MUCH MORE…

DIGITAL FORENSICS

SECURITY RESEARCHERS

DATA RECOVERY

VENDORS & INDUSTRY

TRANSPORTATION SAFETY BOARDS

WHY? BECAUSE WE WANT TO READ NAND MEMORY IN CASE IF:

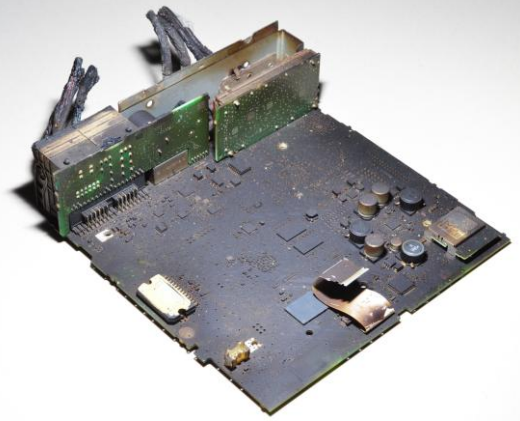
- Flash memory devices unrecognized by PC
- Secured/Locked flash media such as SD, eMMC, etc
- Damaged flash devices (fire, water, cracks)
- Recovery of data artefacts from non-erased blocks

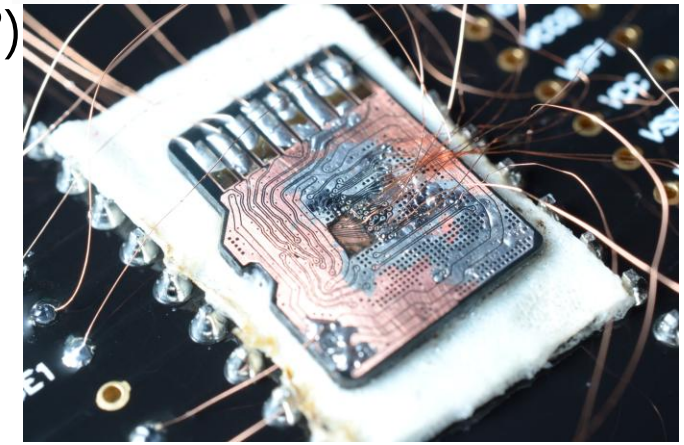
https://ieeexplore.ieee.org/document/9777707

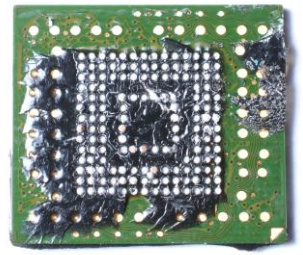
- Access every byte of the memory (hacking RPMB…?)

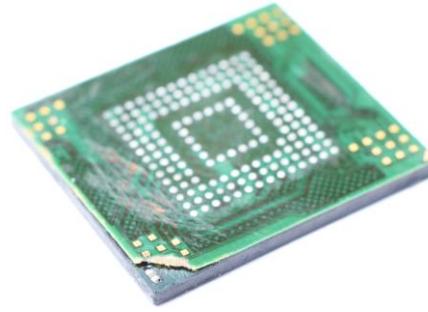
https://www.sciencedirect.com/science/article/pii/S2666281723002019

- Reverse engineering of FW/security/protocol layer

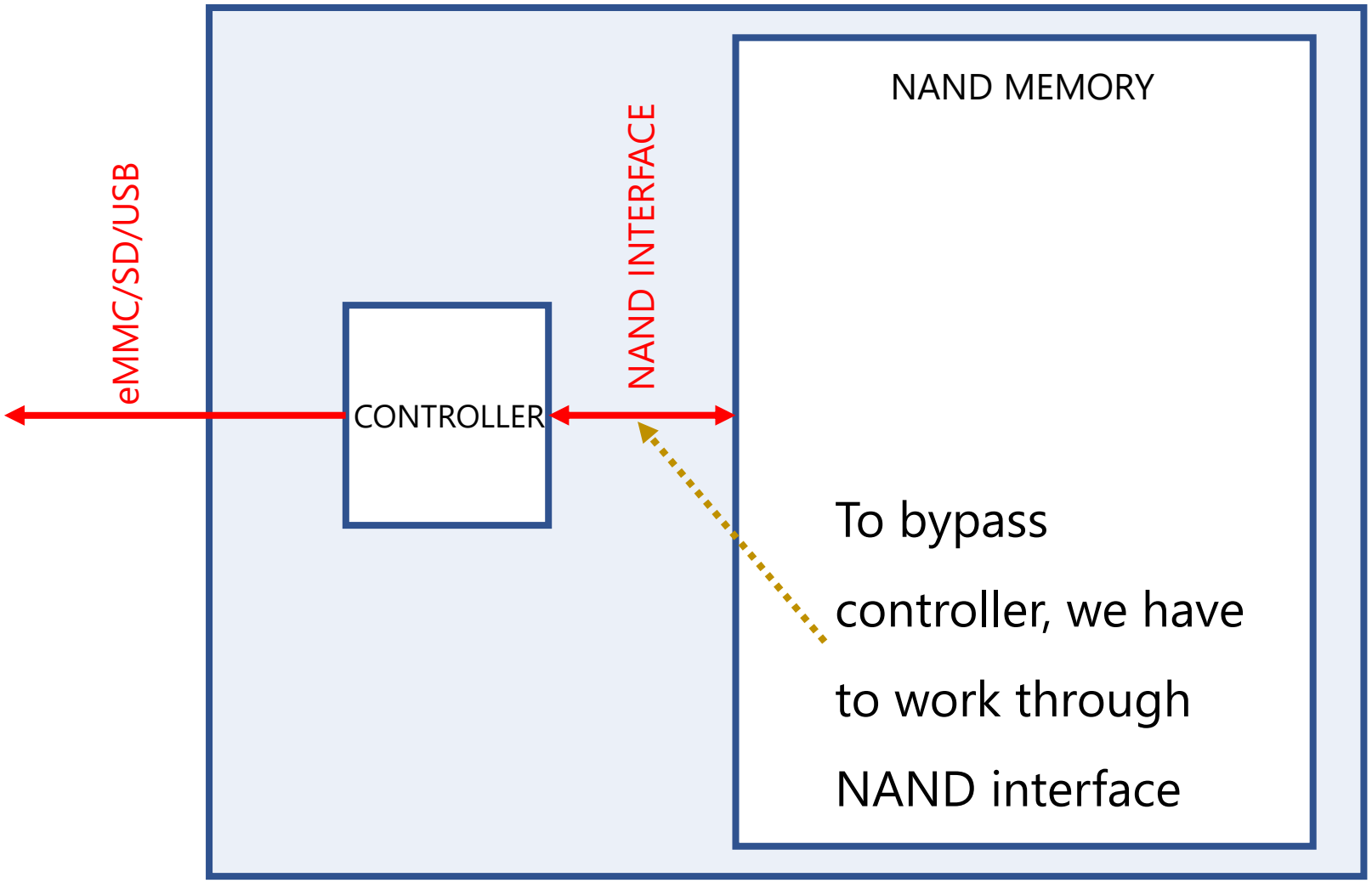


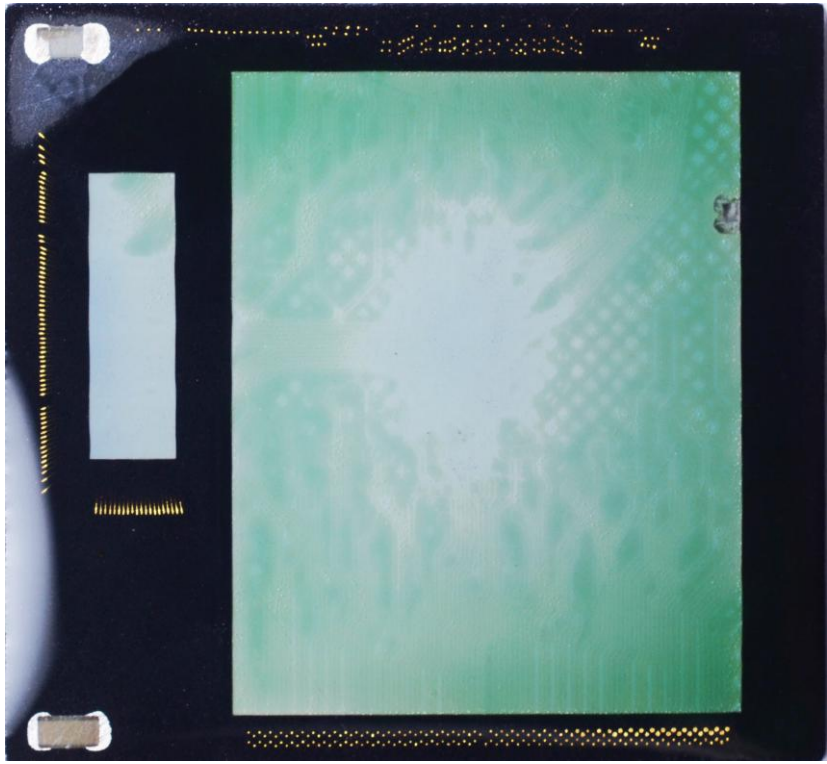




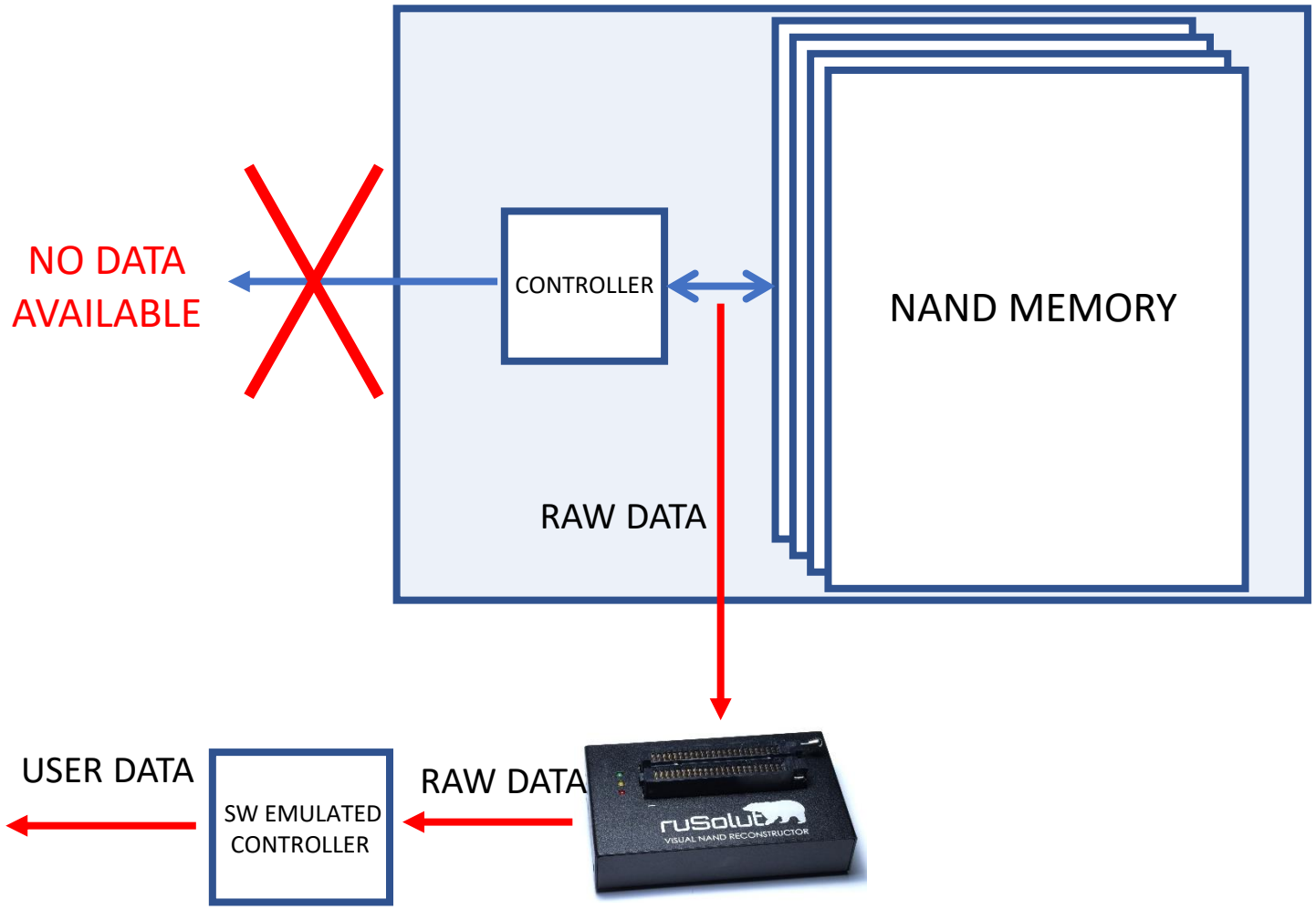


EMBEDDED NAND STRUCTURE





CHIP-OFF DATA ACQUISITION METHOD

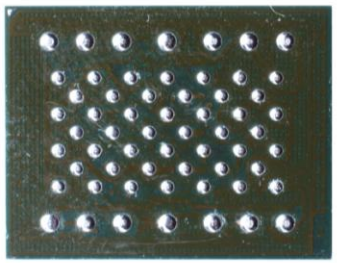


1. NAND memory connection
2. Physical image extraction
3. Controller emulation

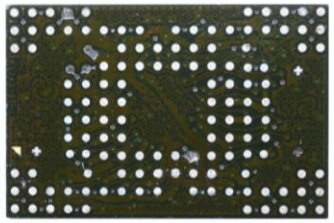
KNOWN PACKAGES OF NAND

TSOP48

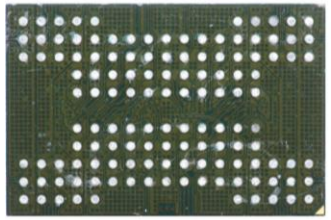
LGA52



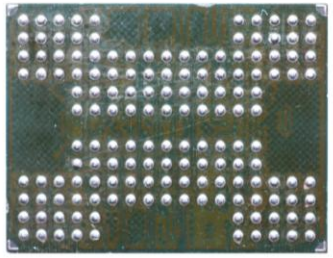
BGA154



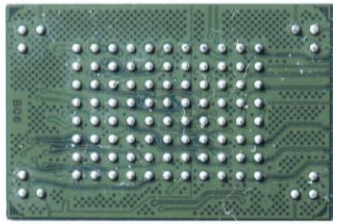
BGA132



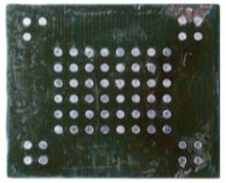
BGA152



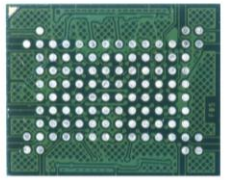
BGA100



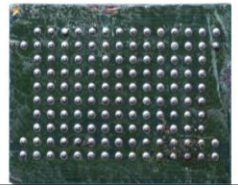
BGA63



BGA107



BGA137



EASY TO READ

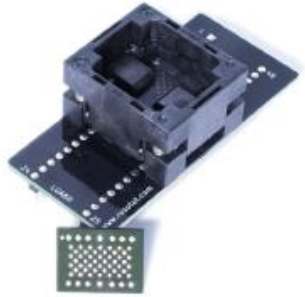
BGA152

BGA100

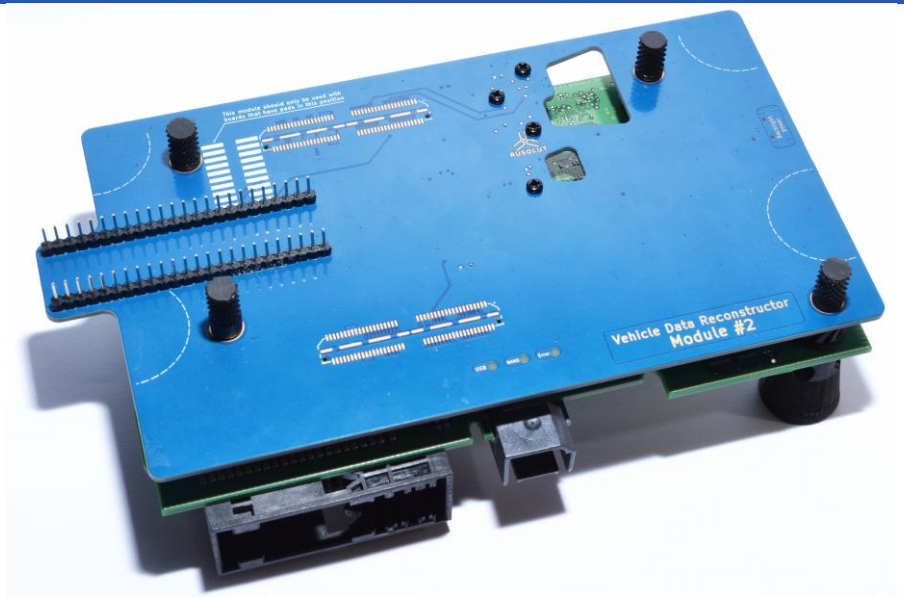
BGA132

BGA107

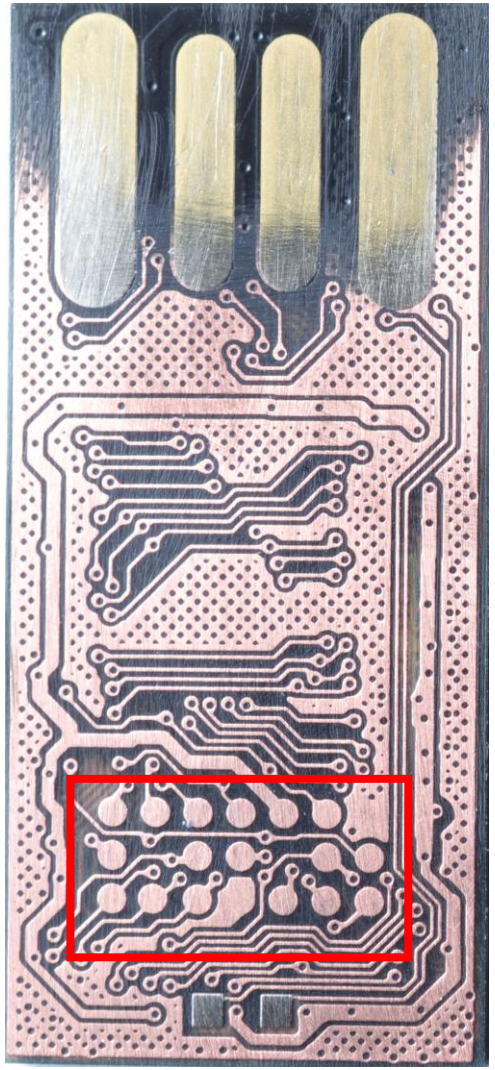
BGA137

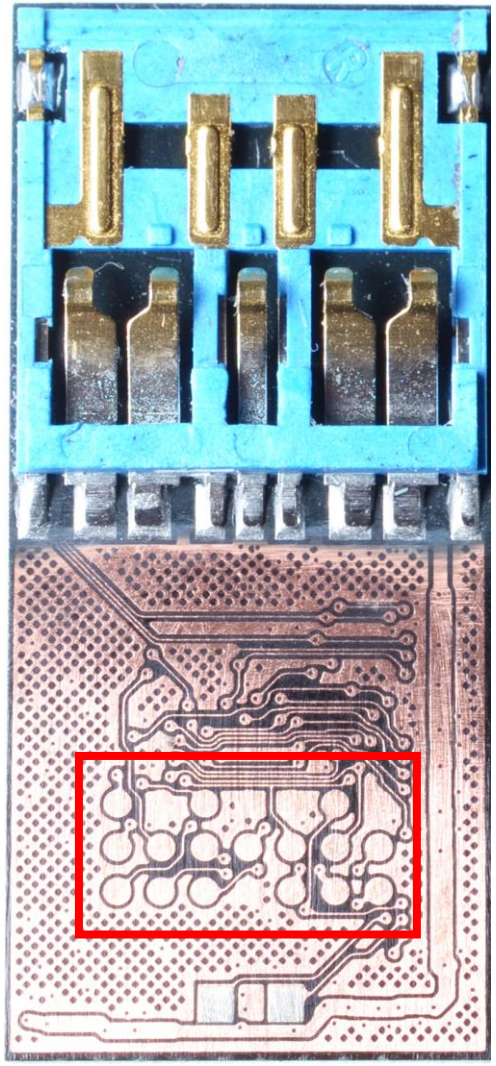


LGA60 (FOR TH58TFT1DFKLAVH AND ALIKE)

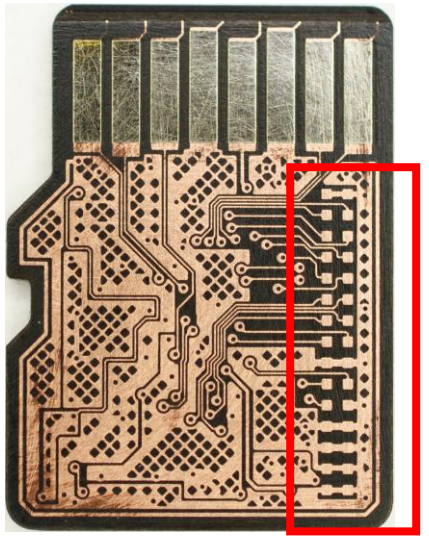


Technological pads of monolithic chips

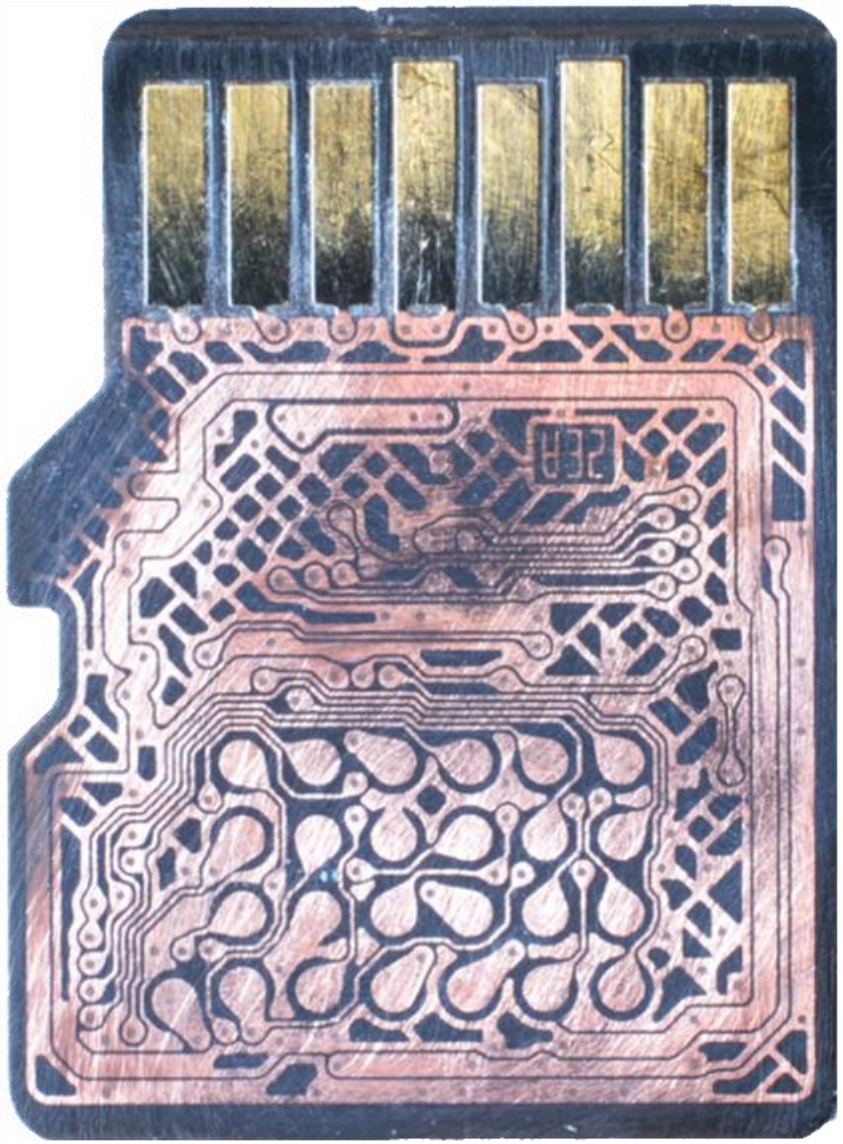


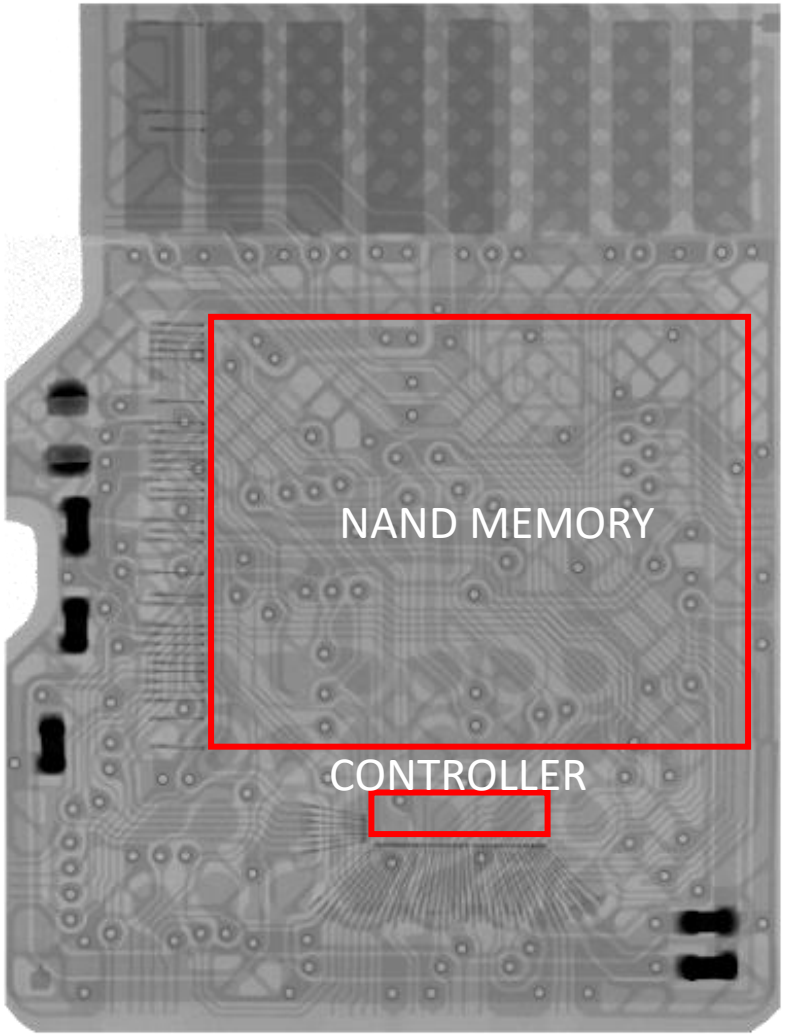


Pinout - ???

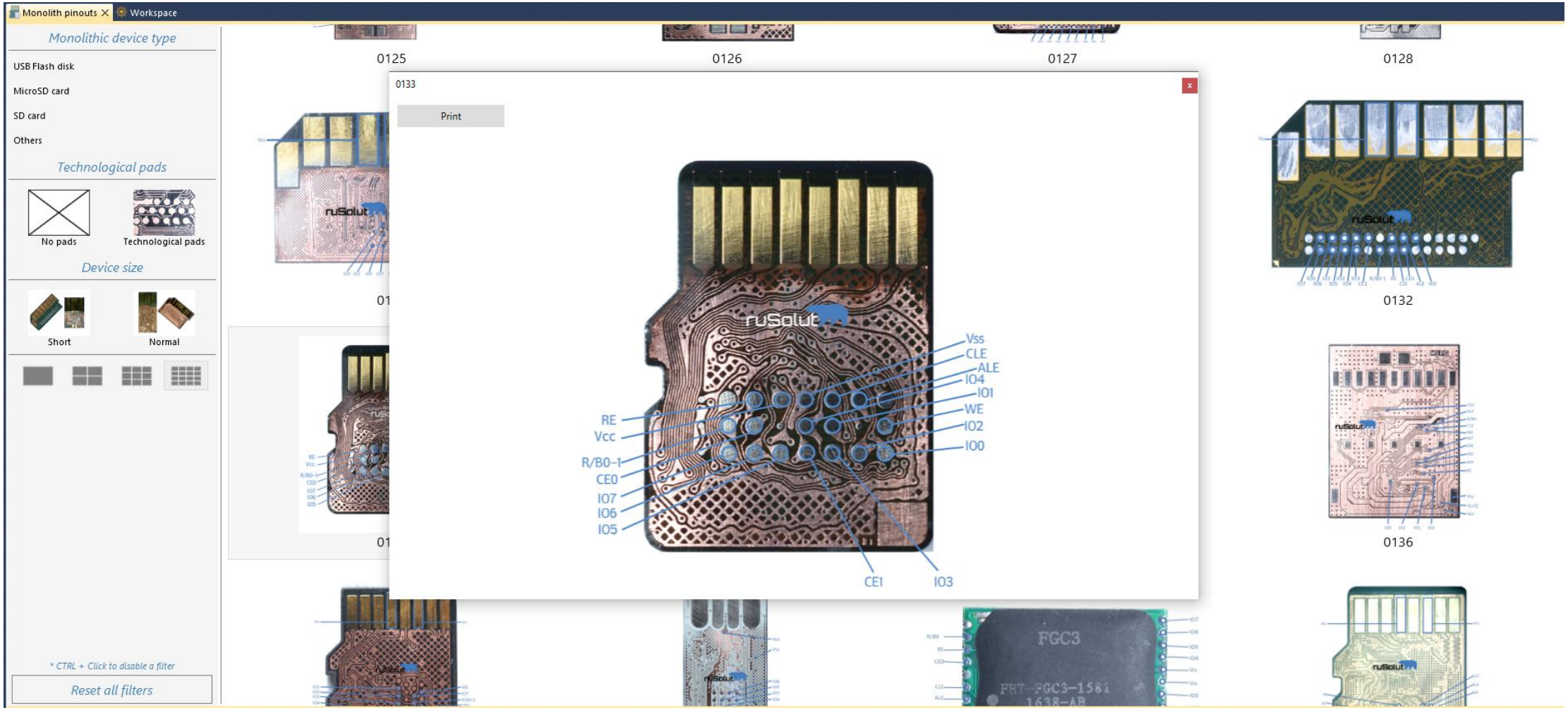


MicroSD inside

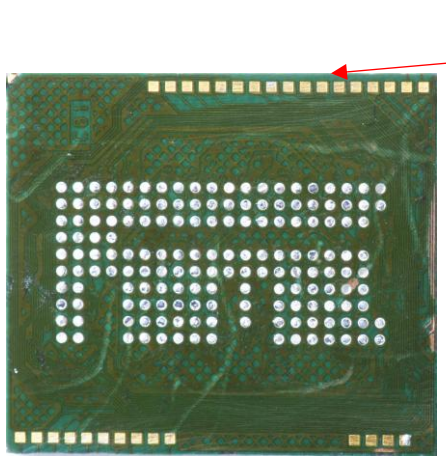


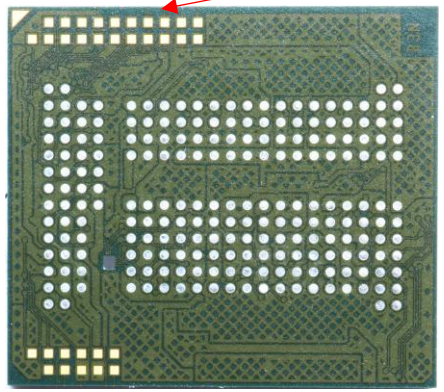


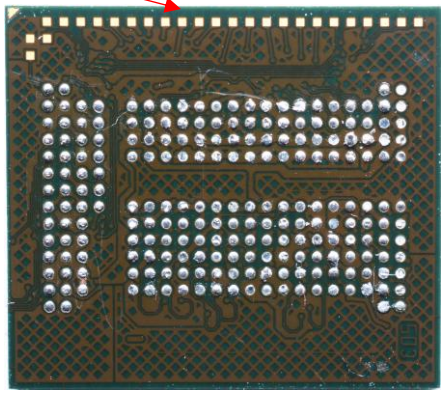
MicroSD inside

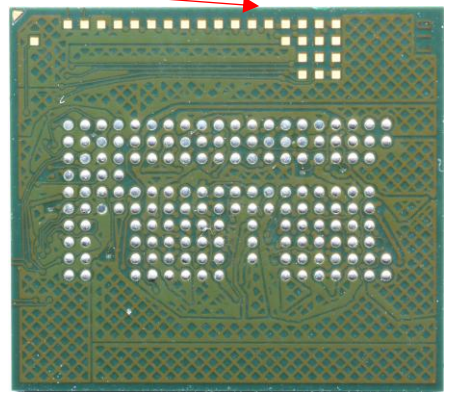


Technological pads of eMMC

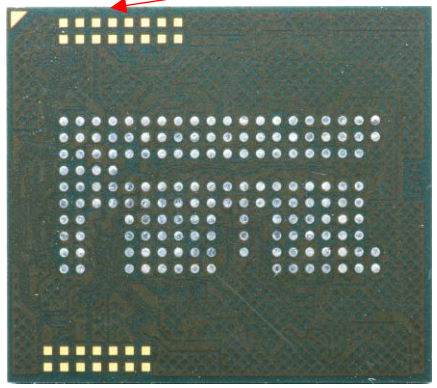


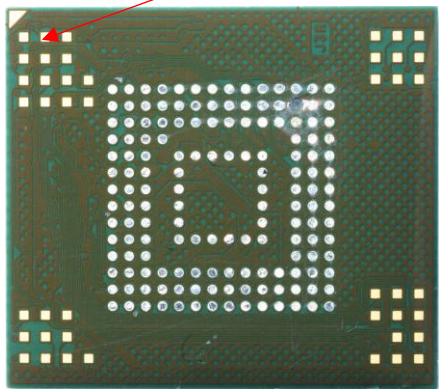


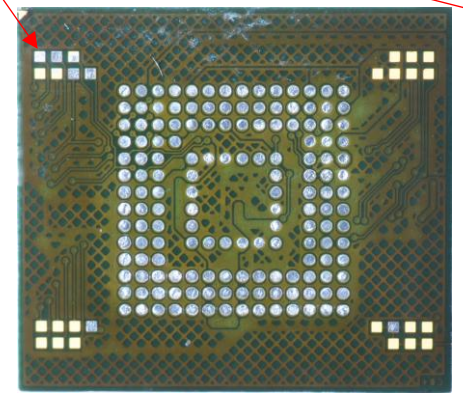


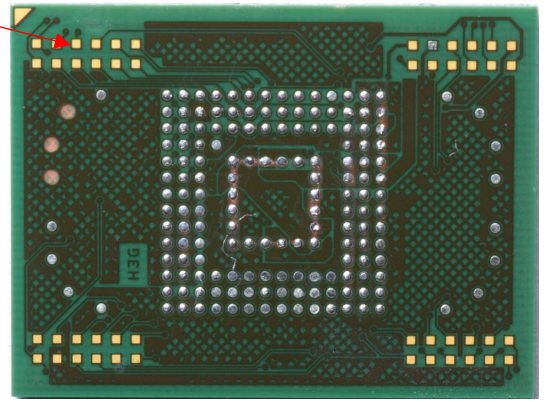


Pinout - ???

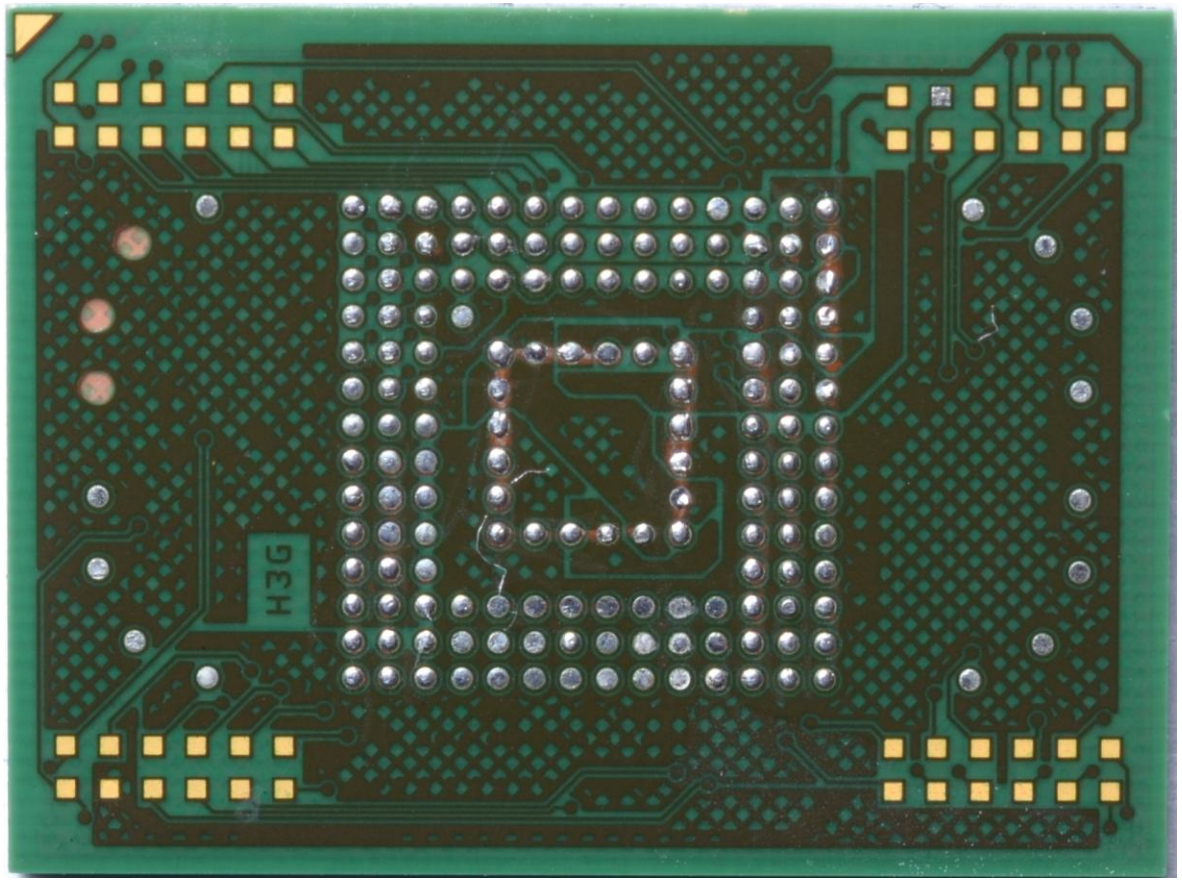


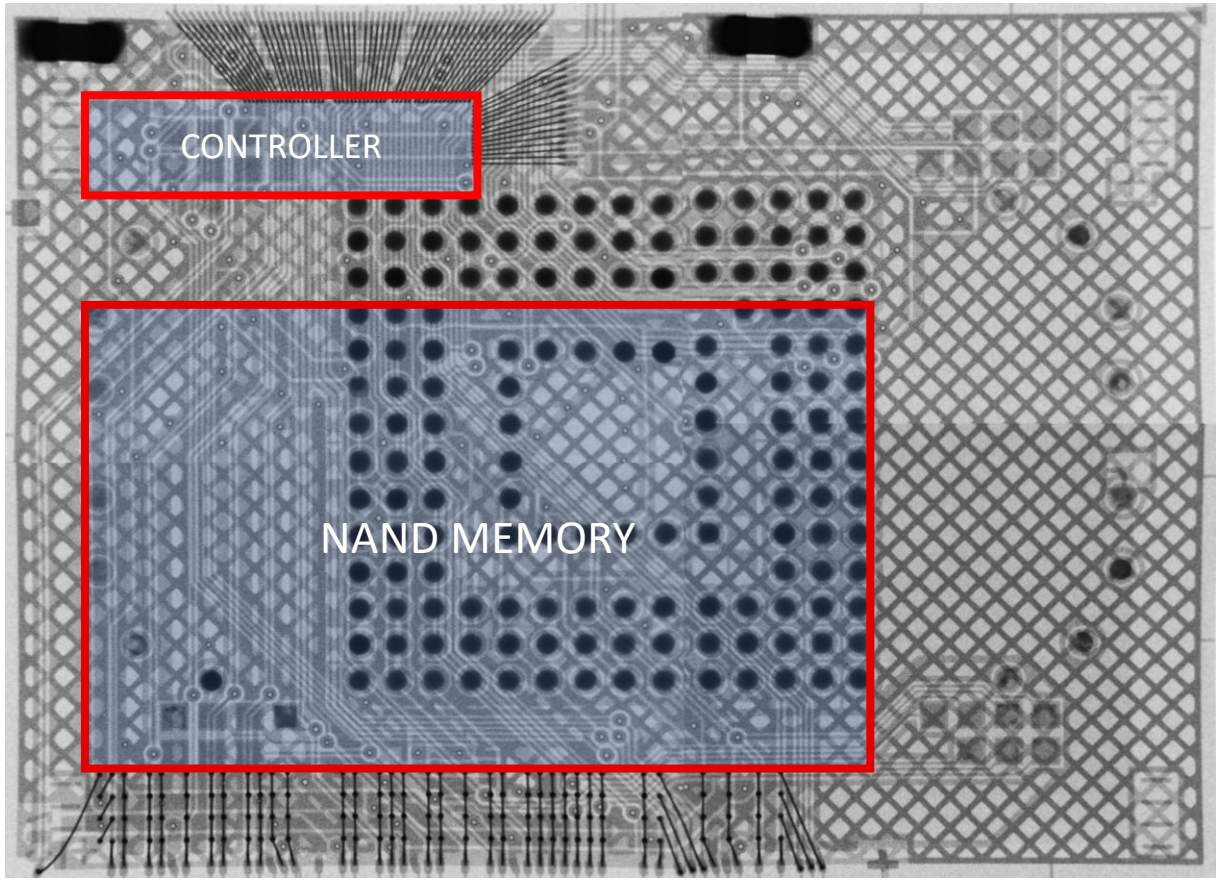






eMMC inside





NAND INTERFACE – TSOP48

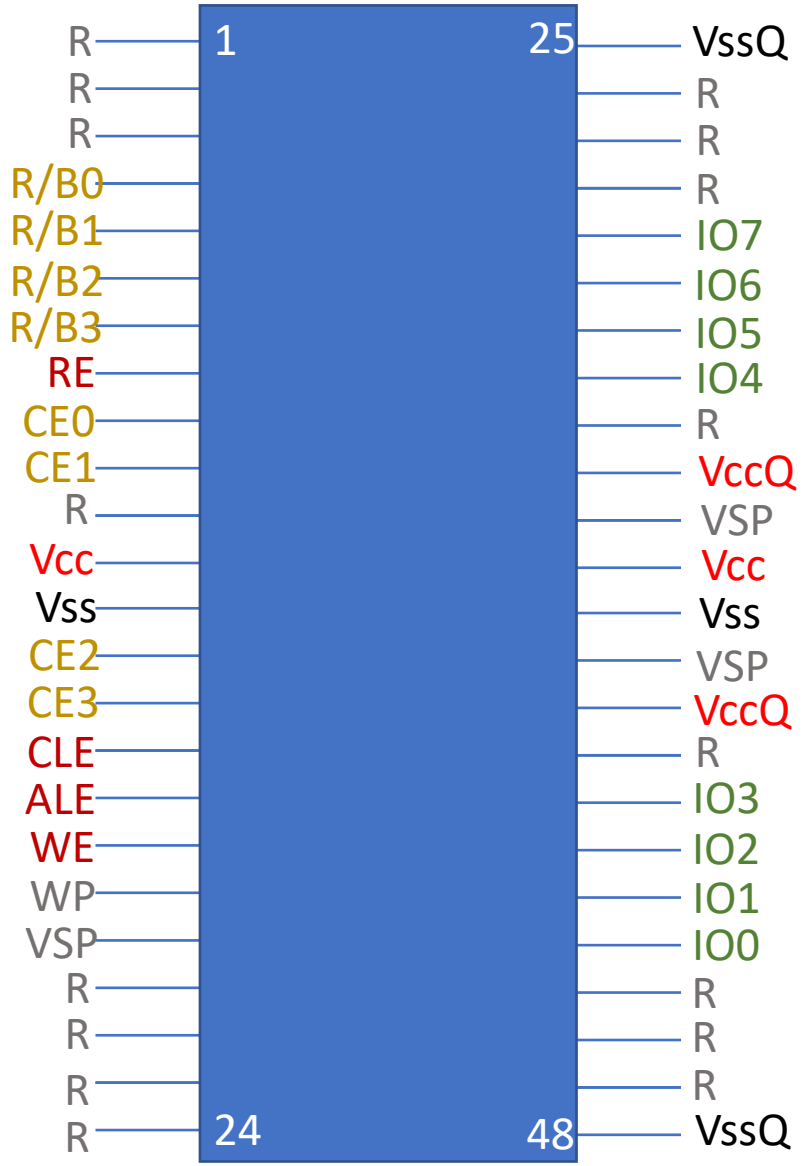
IO0…IO7 – Data bus

Vcc/VccQ – power 3,3 or 1,8 V

Vss/VssQ - Ground

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

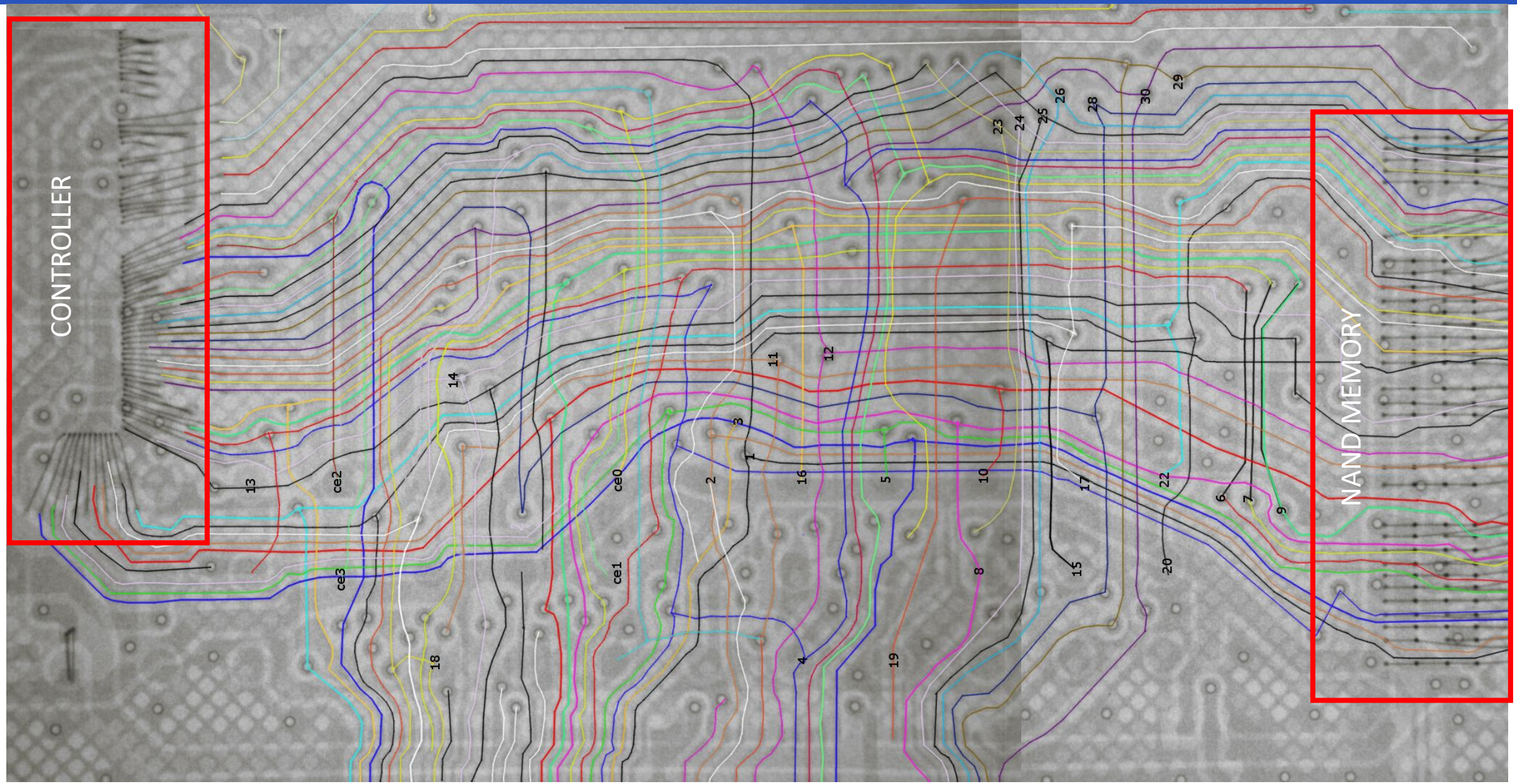
R/B0…R/B3 – Ready/Busy status
CE0…CE3 – Crystal enable



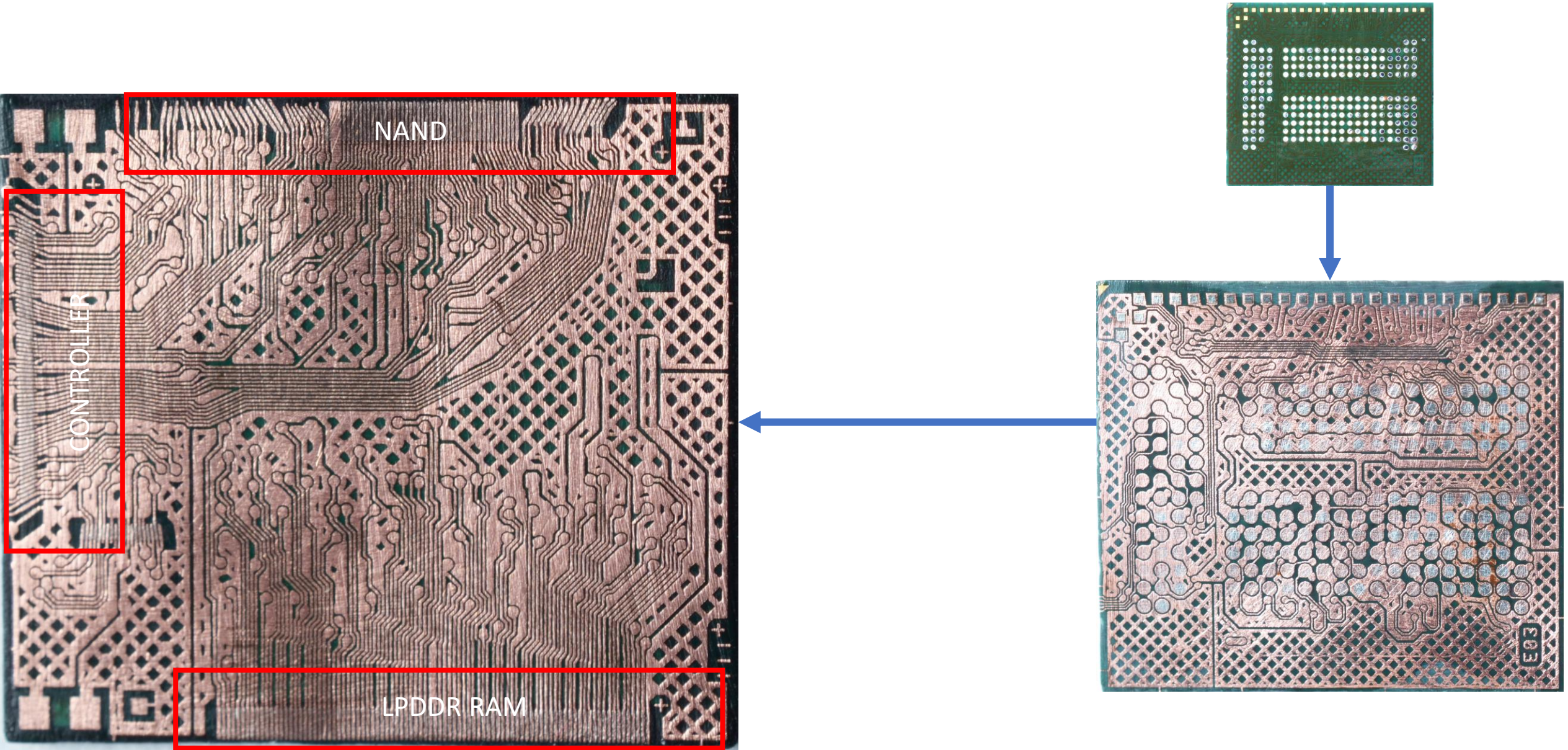
THREE MOST POPULAR METHODS OF UNKNOWN MEMORY PINOUT ANALYSIS

- XRAY inspection - schematics analysis ☹
- Layer dissection – schematics analysis 😐
- Logic analyzer – signal analysis ☺

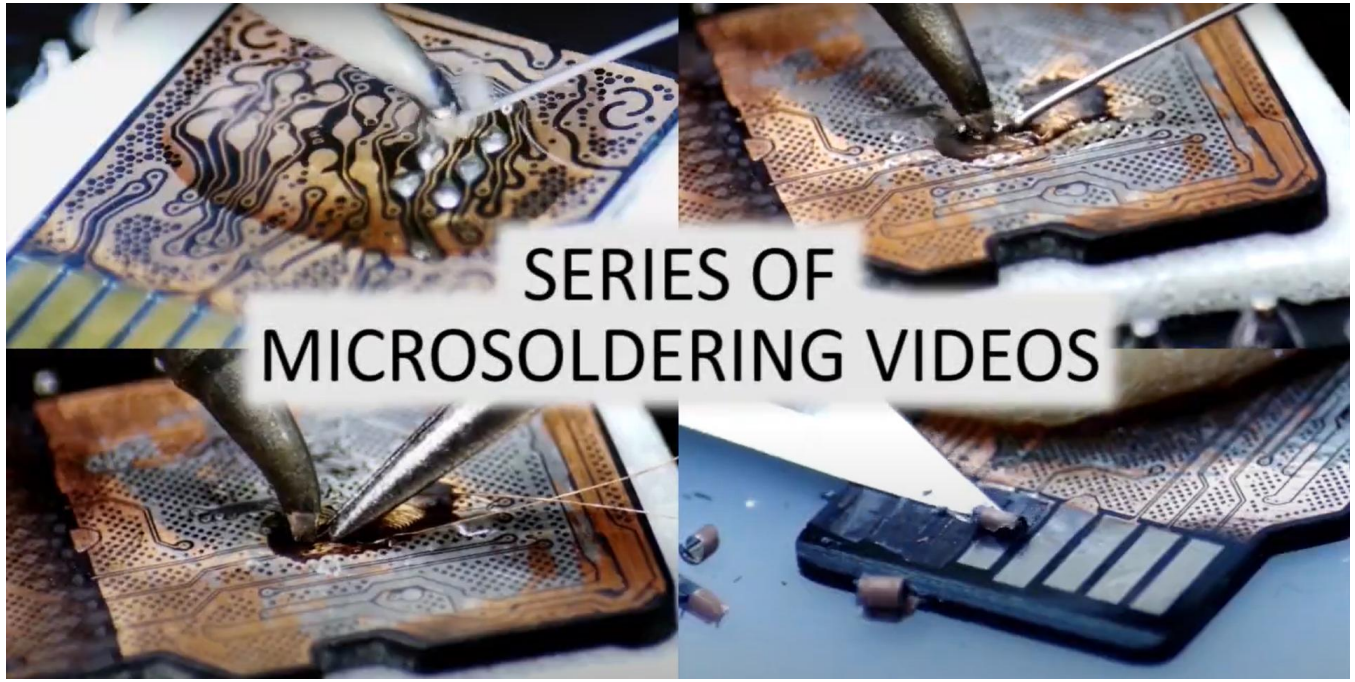
XRAY PINOUT ANALYSIS



LAYER DISSECTION – EASIER TO ANALYZE THAN XRAY

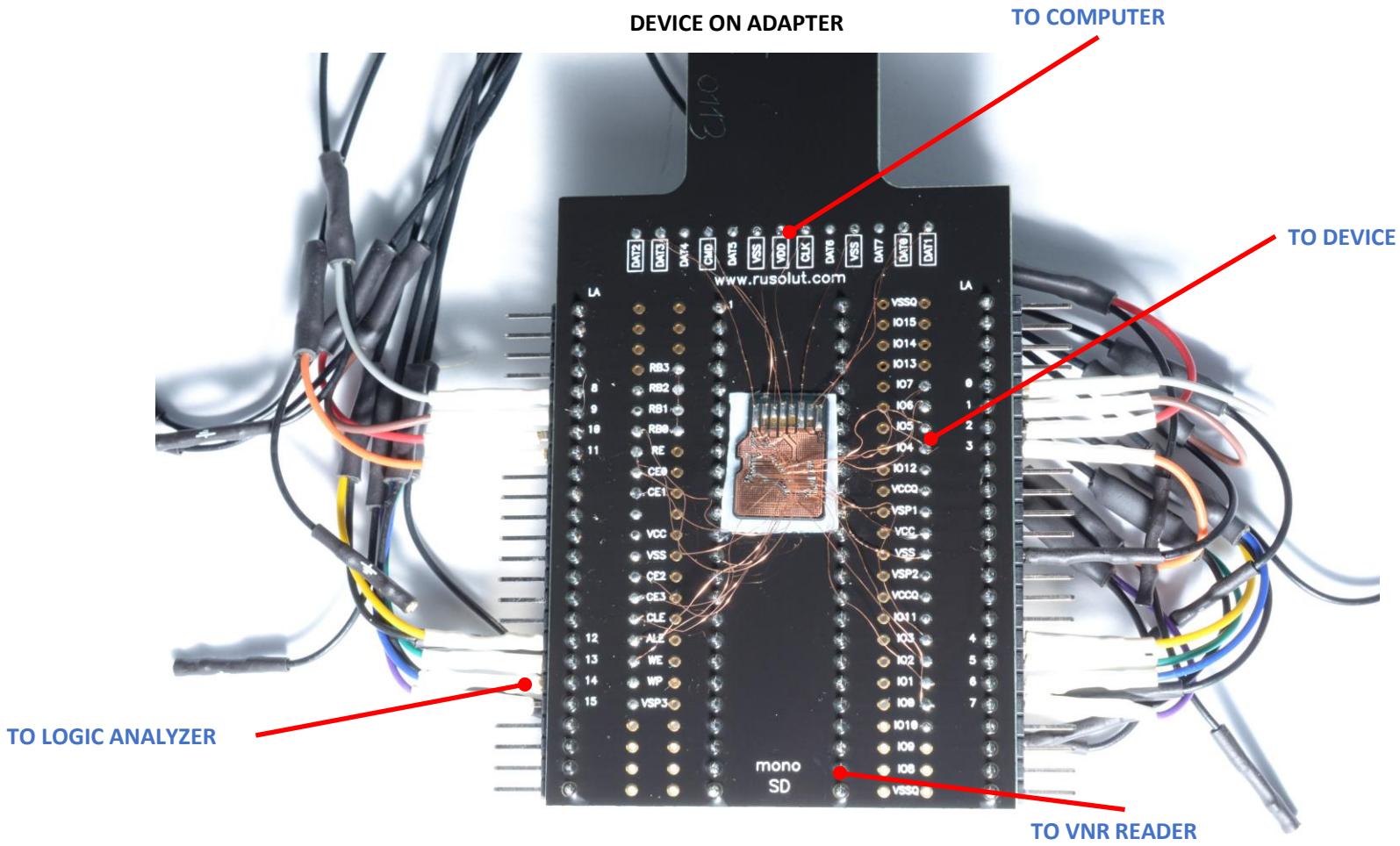


MICROSOLDERING MADE EASY ☺

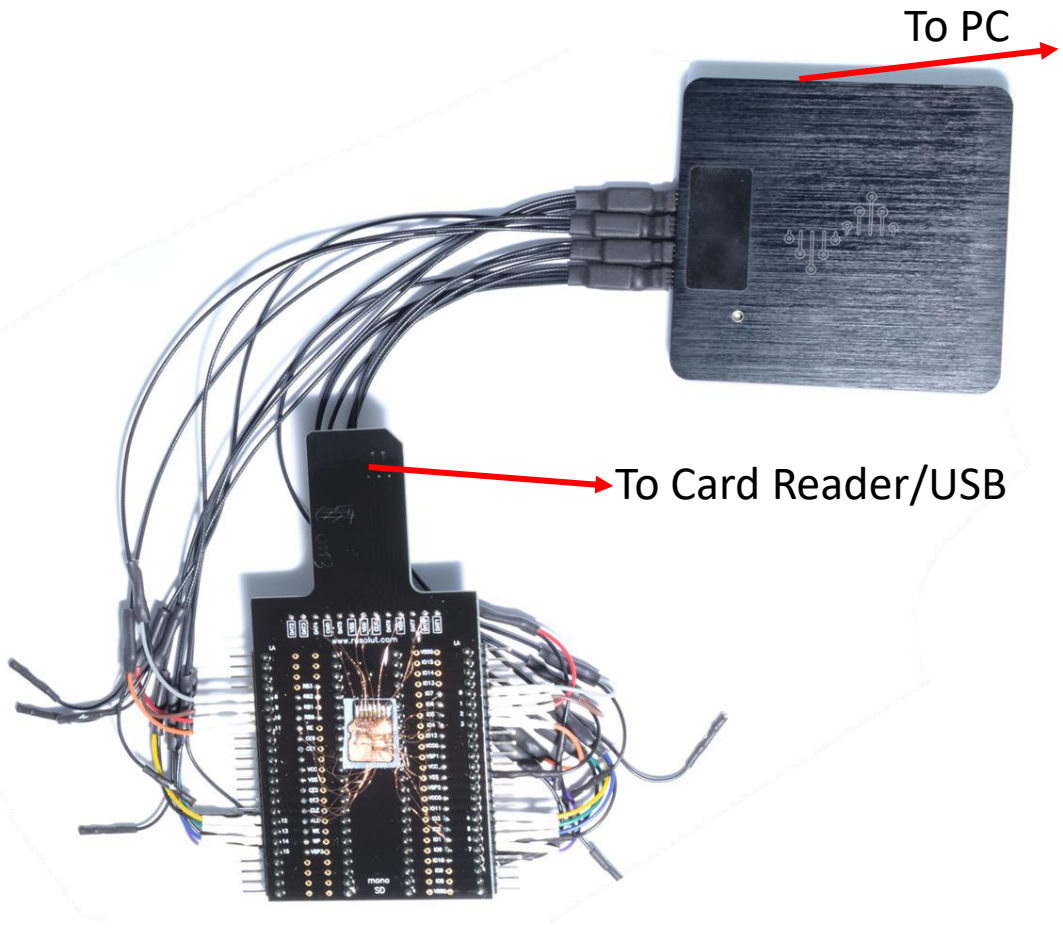


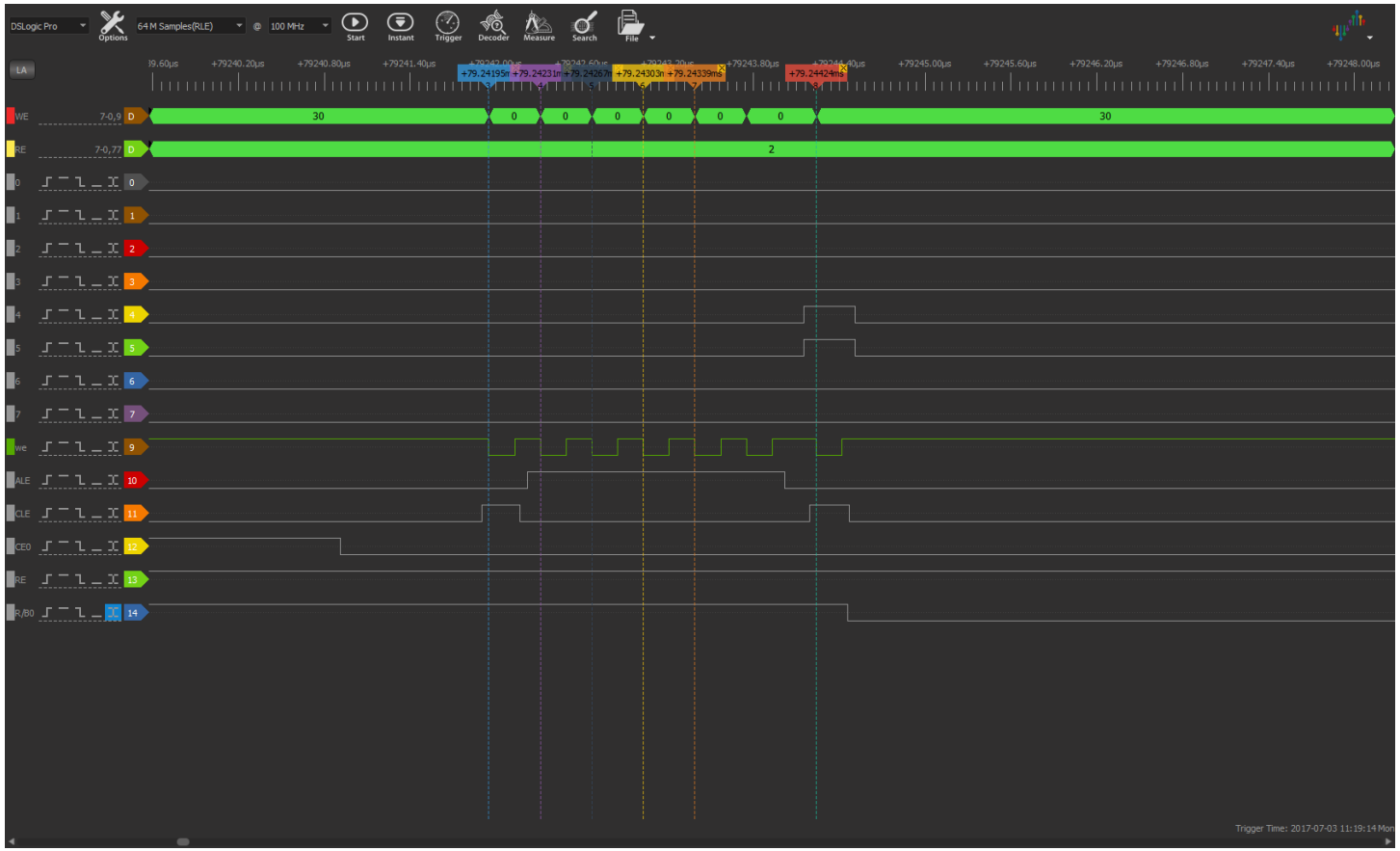
YouTube

SOLDER DEVICE TO ADAPTER

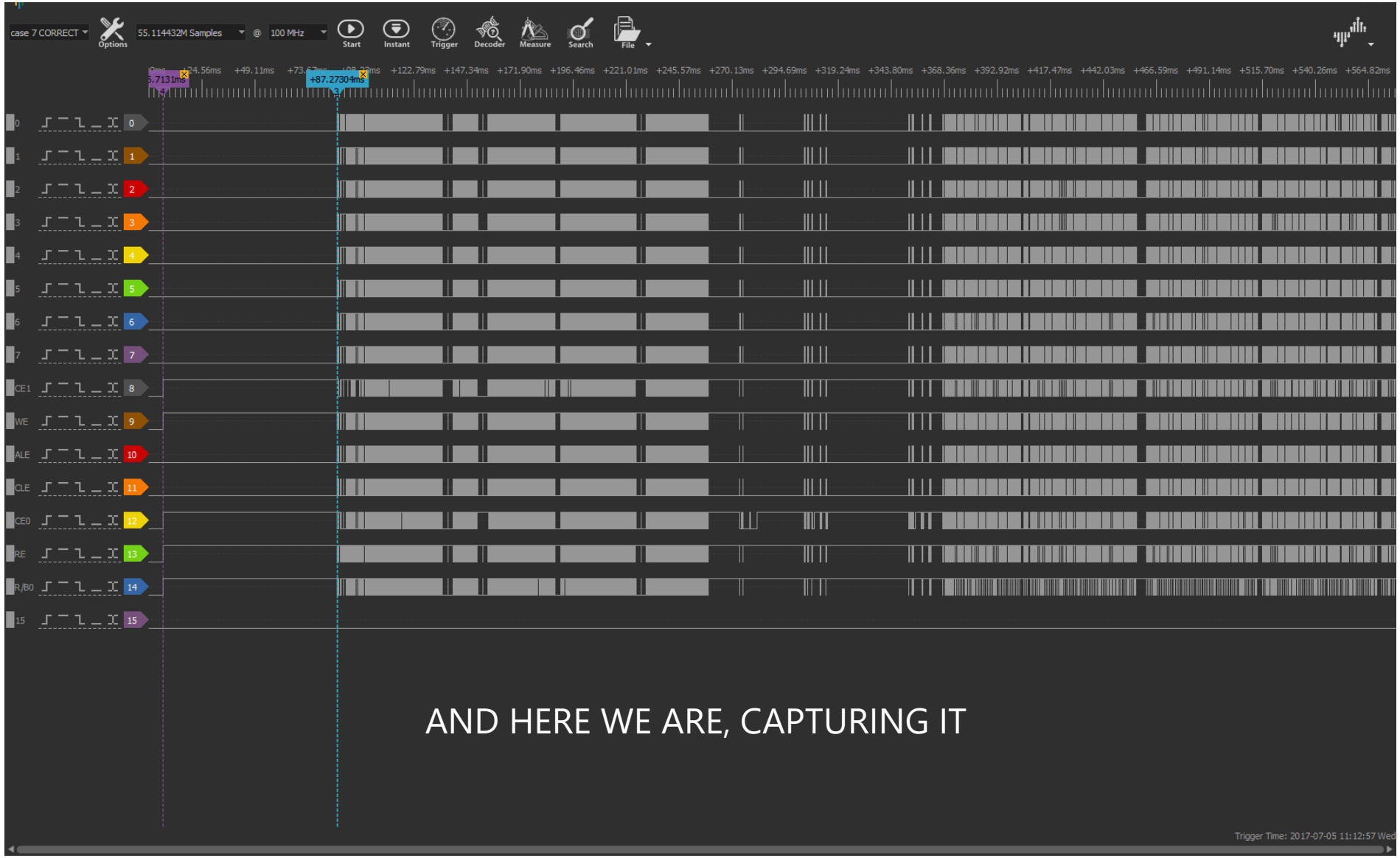


SIGNAL/PROTOCOL ANALYSIS WITH LOGIC ANALYZER

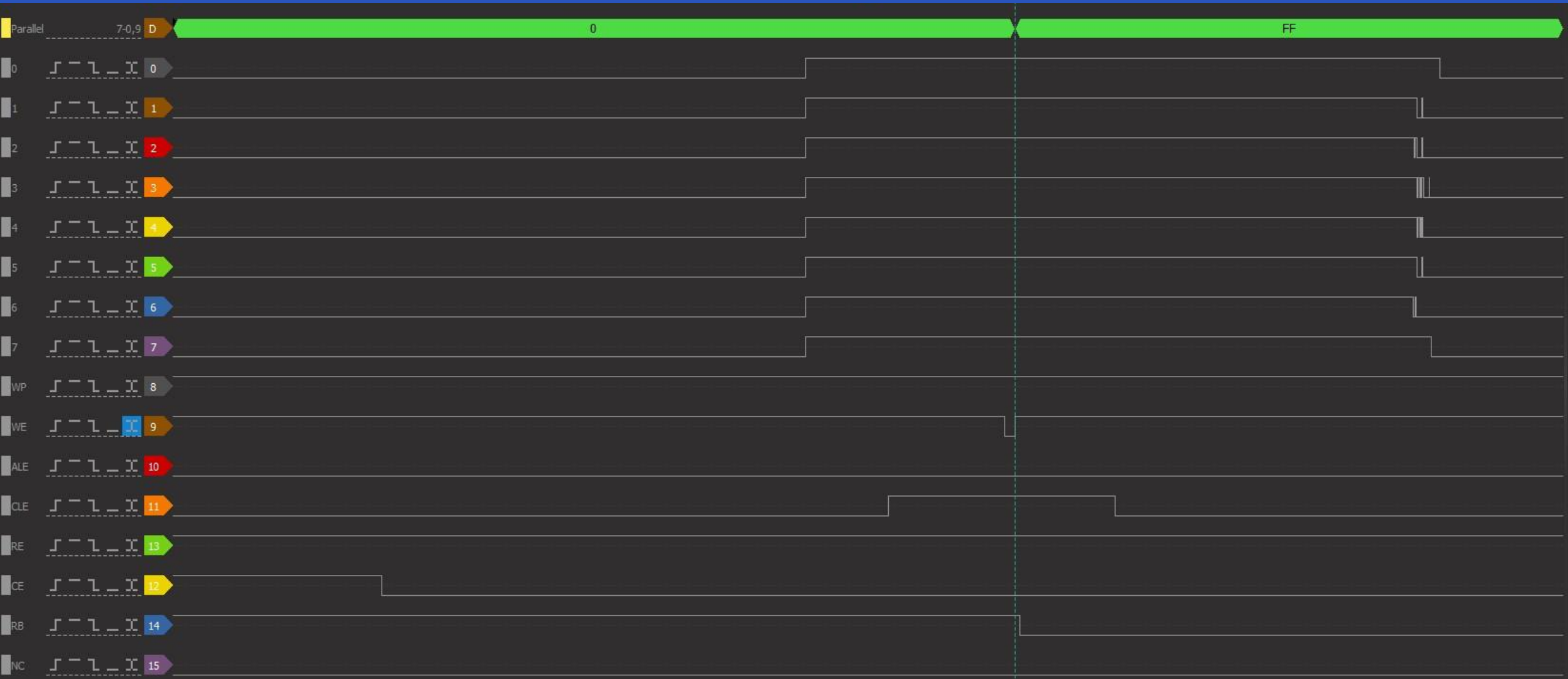




CONTROLLER READS SYSTEM DATA FROM NAND AFTER POWER UP

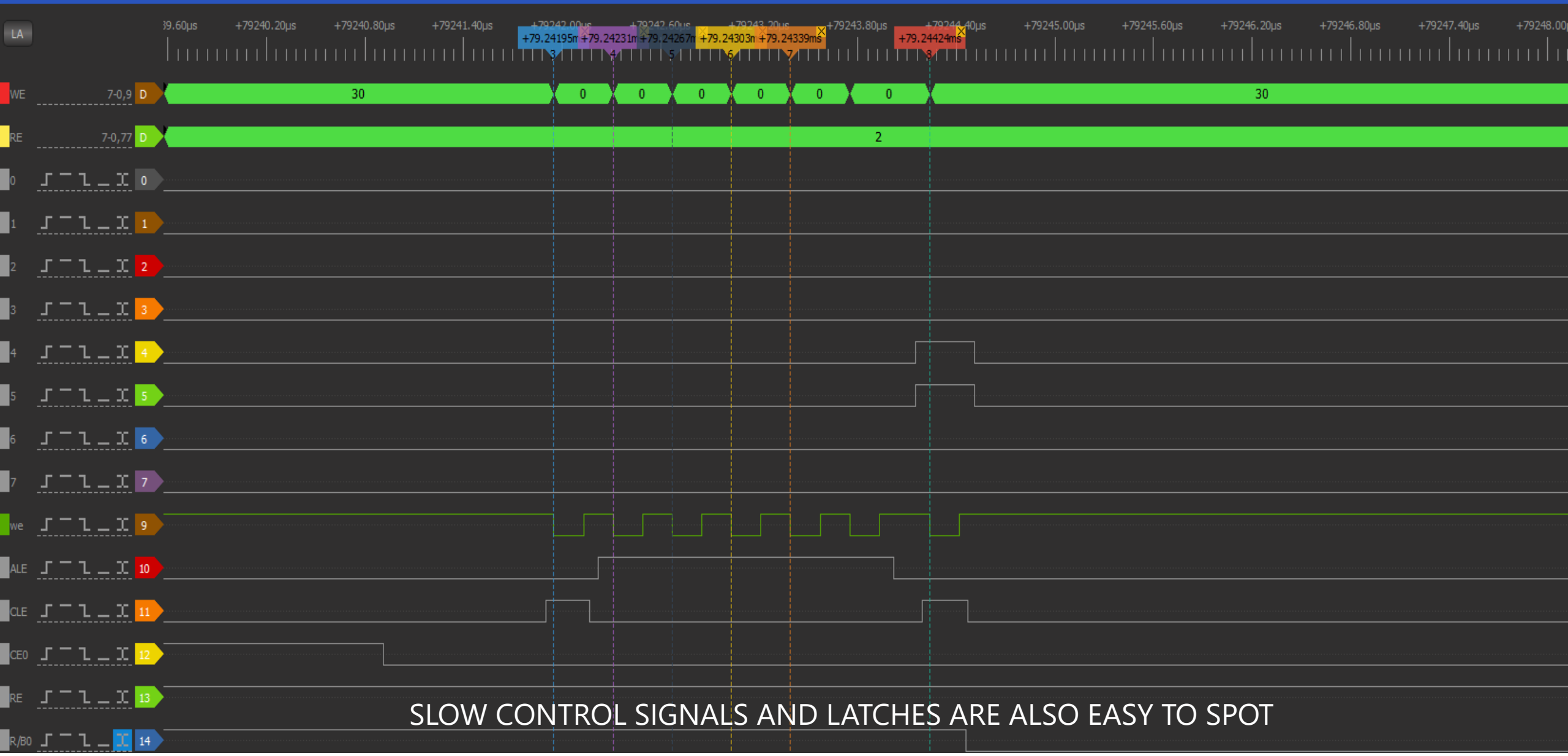


PATTERN ANALYSIS



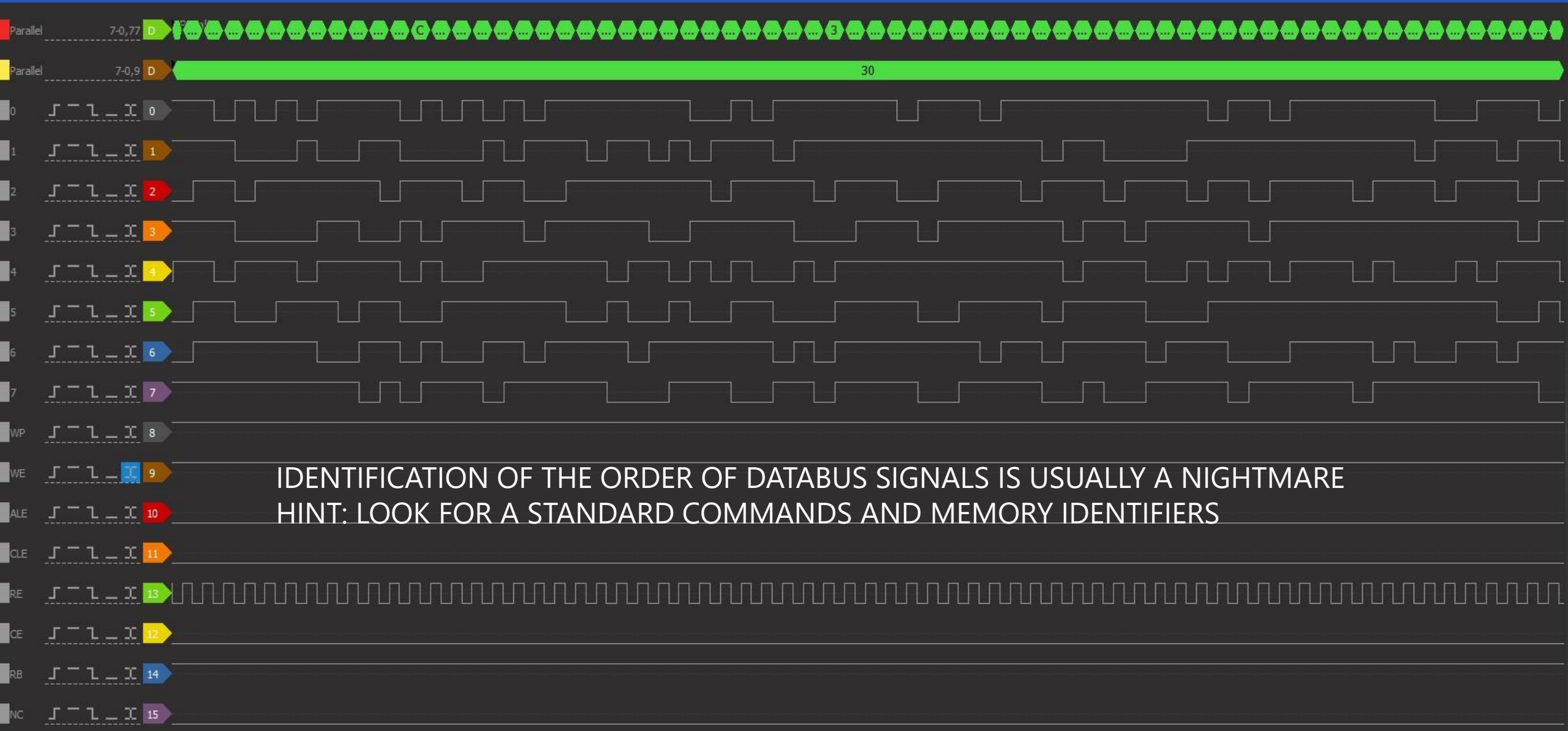
SLOW CONTROL SIGNALS ARE EASILY IDENTIFIABLE

PATTERN ANALYSIS



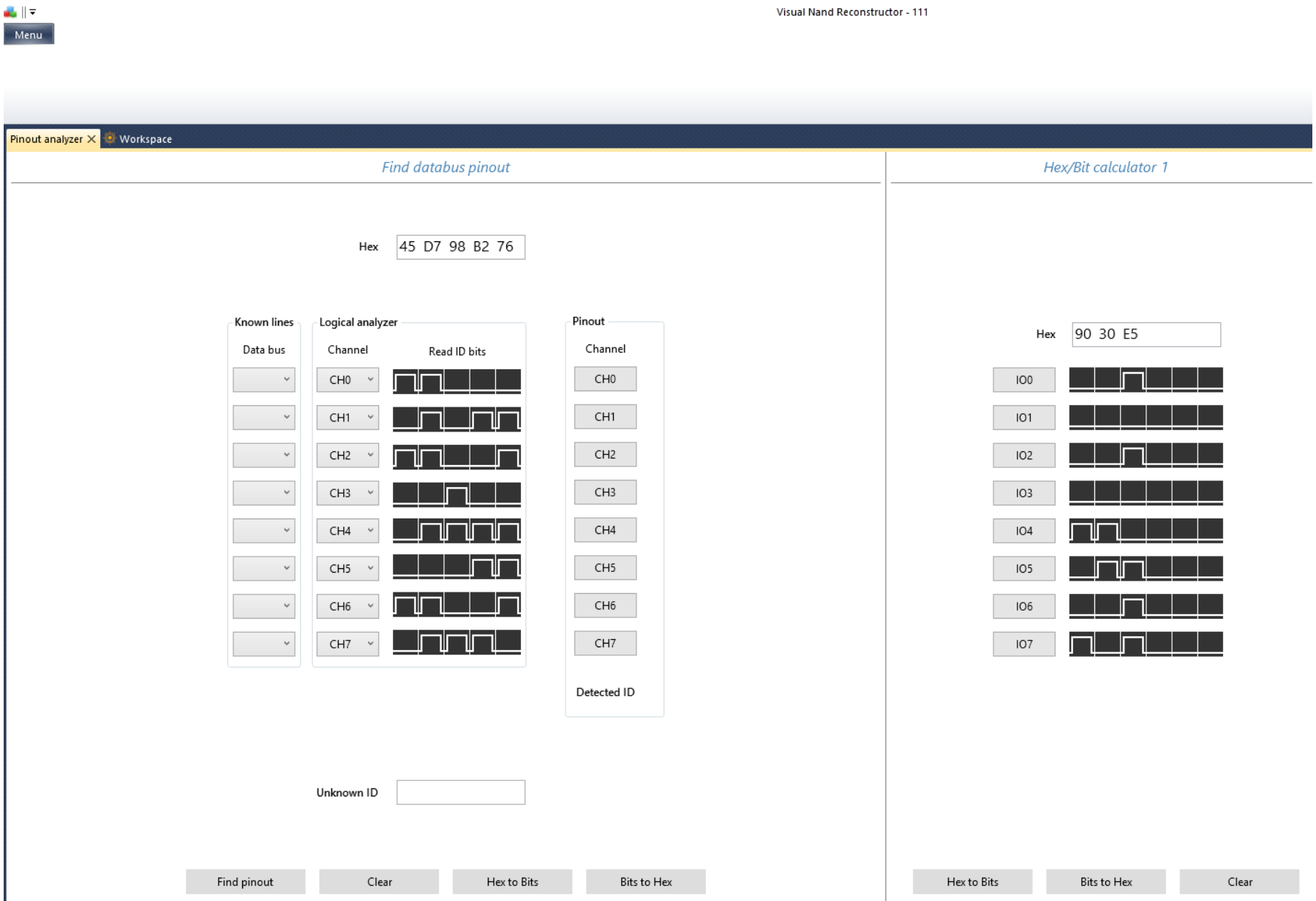
SLOW CONTROL SIGNALS AND LATCHES ARE ALSO EASY TO SPOT

PATTERN ANALYSIS

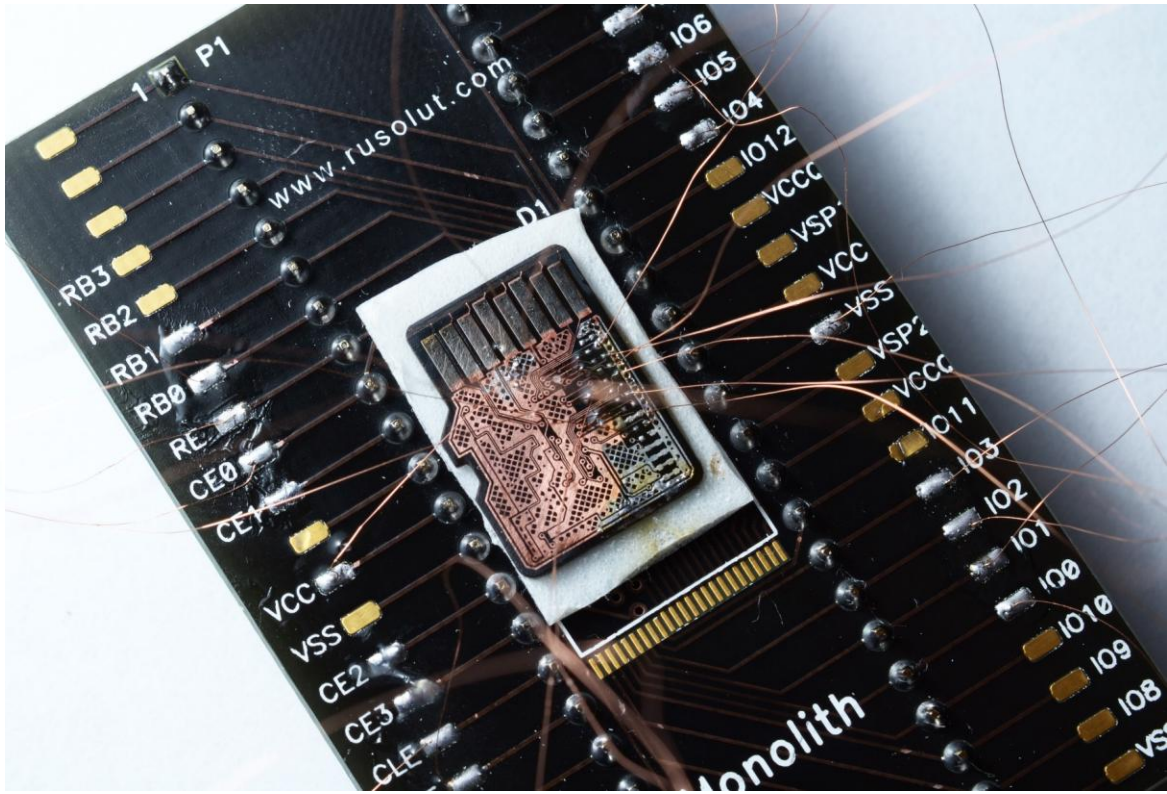


IDENTIFICATION OF THE ORDER OF DATABUS SIGNALS IS USUALLY A NIGHTMARE
HINT: LOOK FOR A STANDARD COMMANDS AND MEMORY IDENTIFIERS

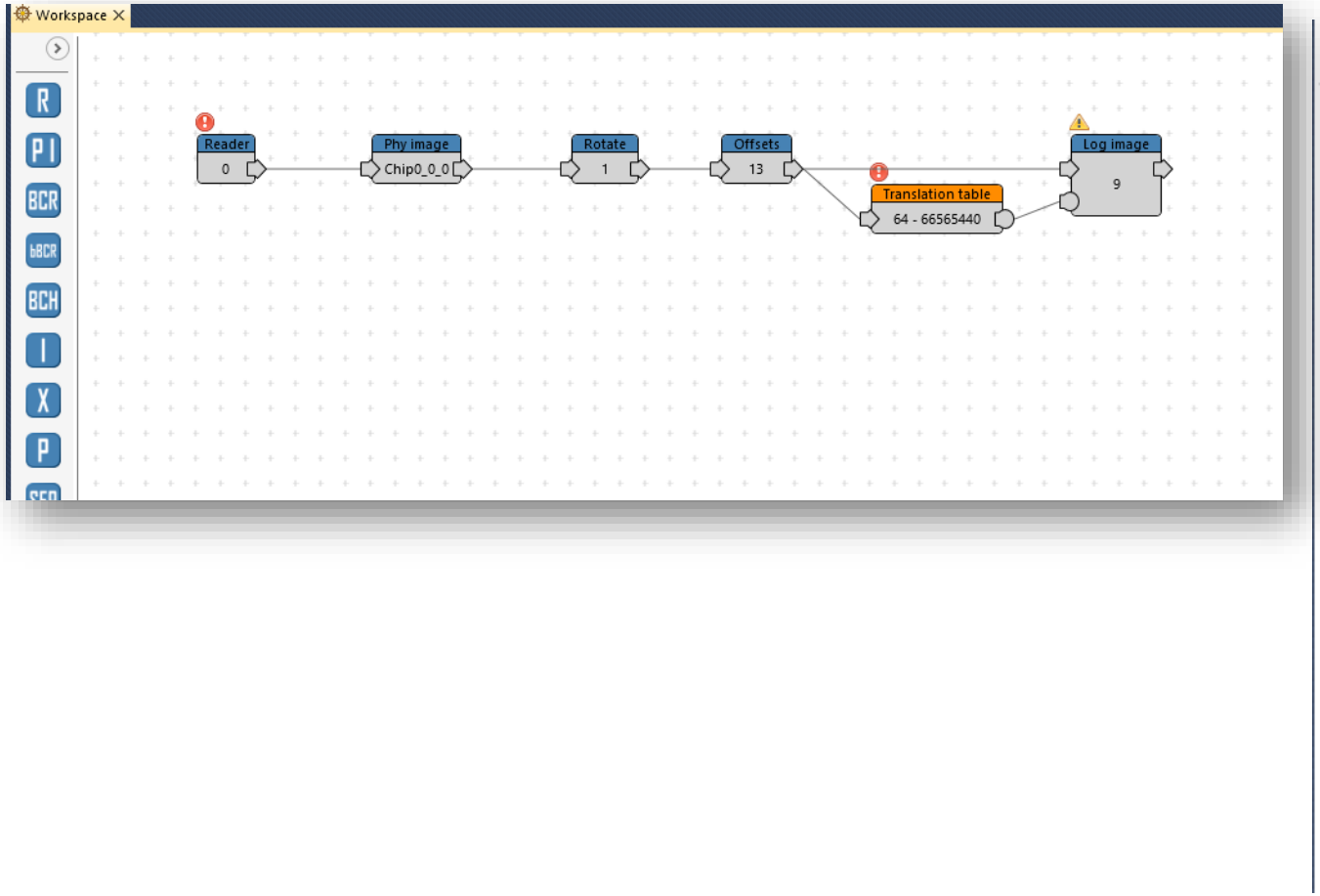
ONCE THE RIGHT PLACE WITH COMMANDS IS FOUND PINOUT CAN BE BRUTE FORCED

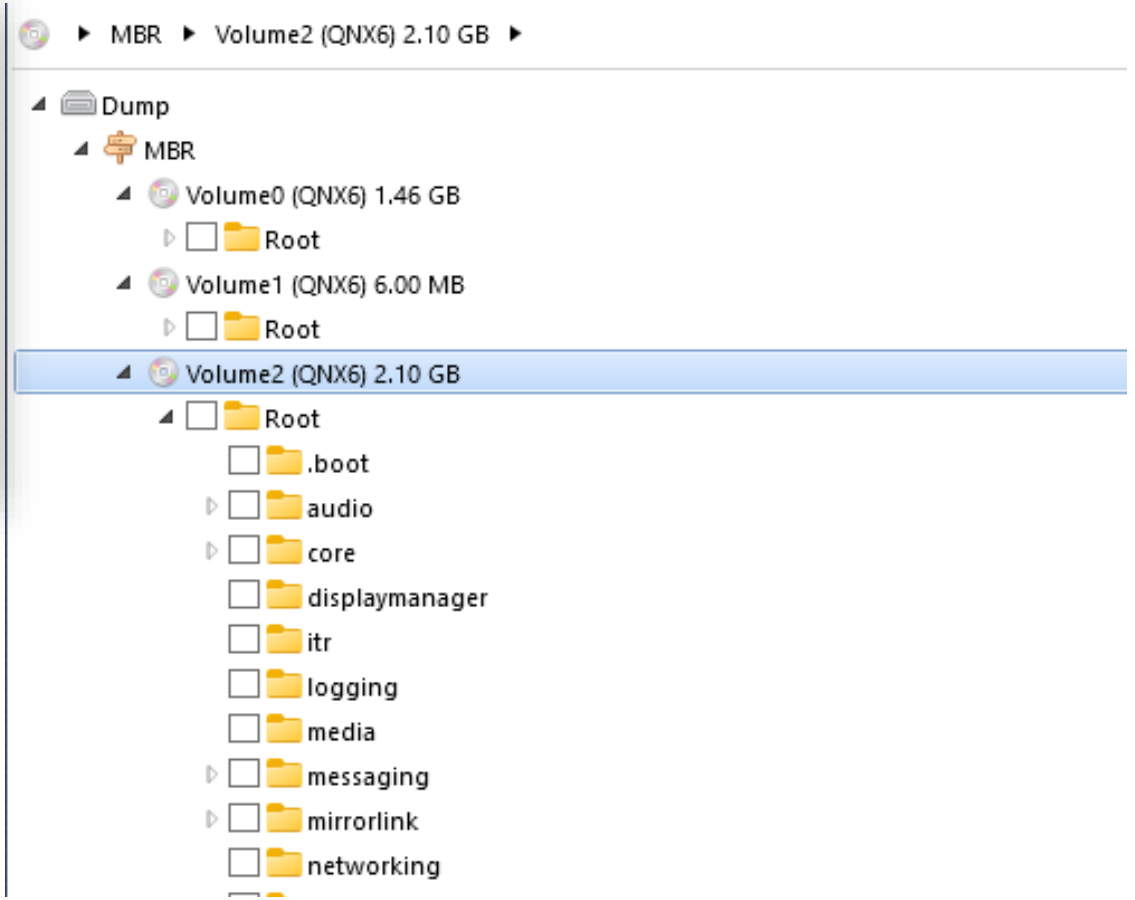


READ MEMORY AND GET DATA!



FILE SYSTEM RECONSTRUCTION





THANK YOU!

VISIT OUR BOOTH!

RUSOLUT