There & Back Again

Full-stack Reverse Engineering of the Original Microsoft **Xbox**

by markus 'doom' gaasedelen

4000 hours

over about 3 years

2021 → 2024


XBOX
HALO

whoami

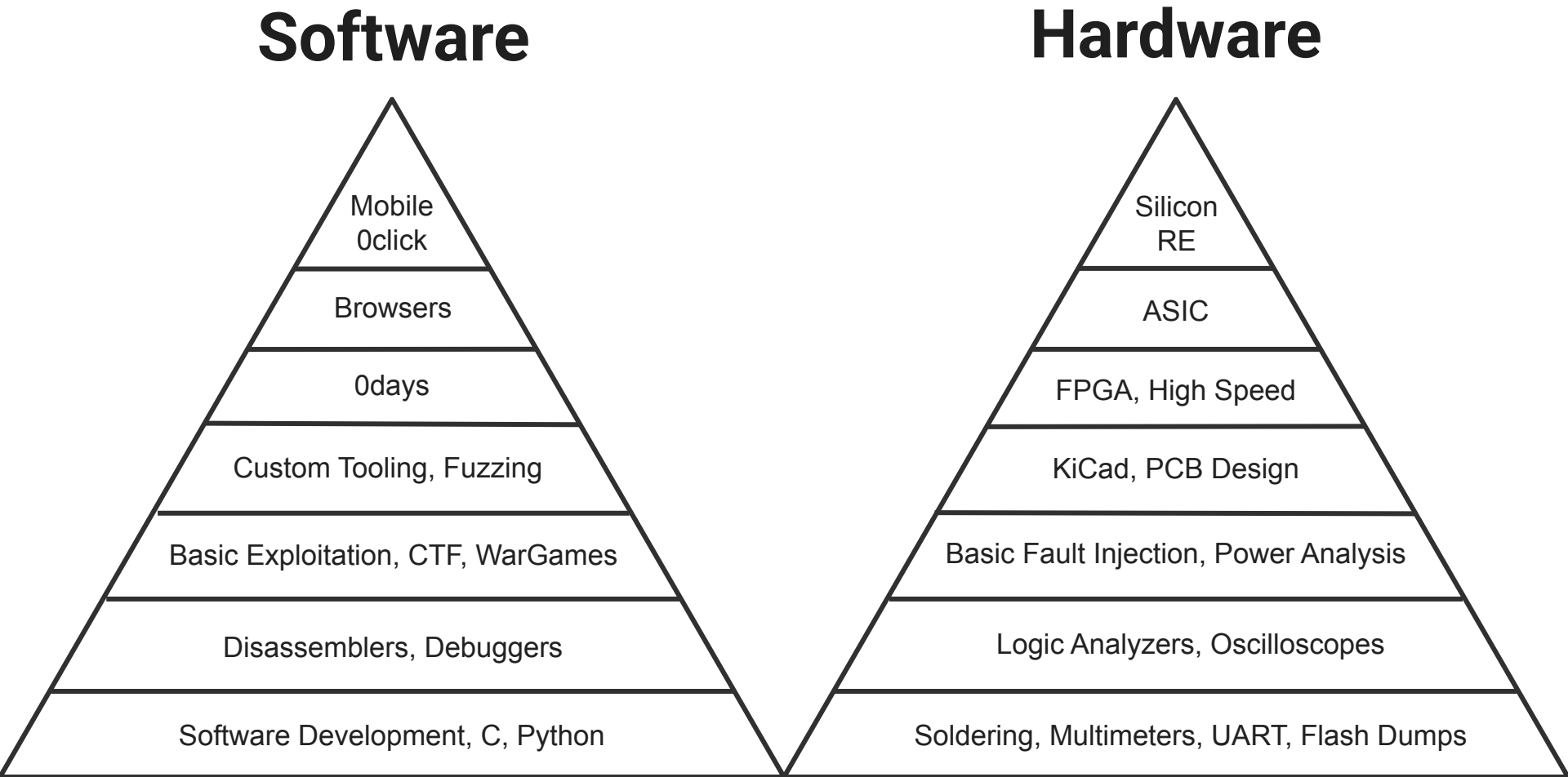
- **Markus Gaasedelen**
  - doom
- **Principal, Security Research**
  - Reverse Engineering
  - Software Exploitation
- **Co-founder of RET2 Systems**
  - est. 2017

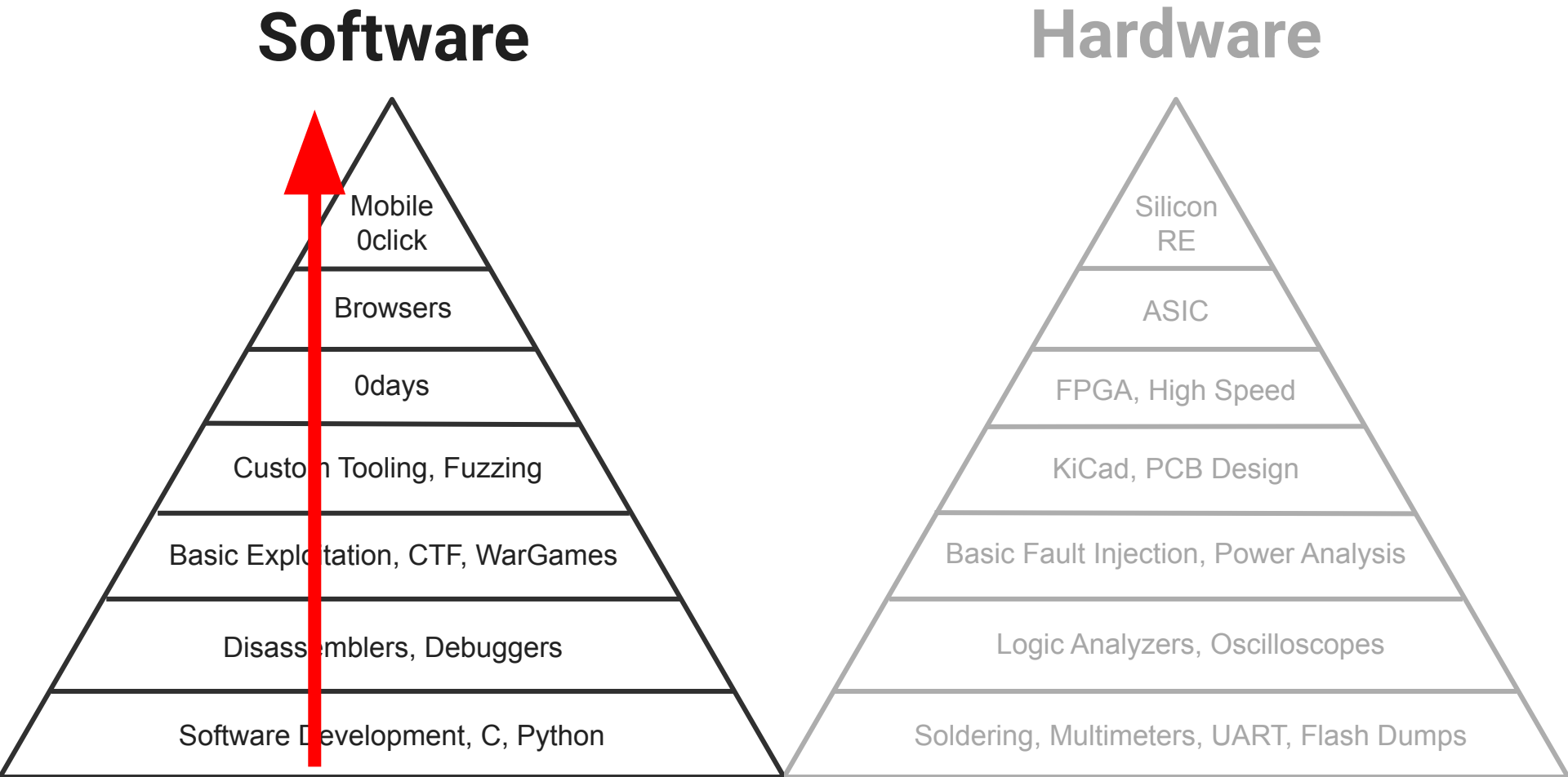
The Layman's Guide to Zero-Day Engineering

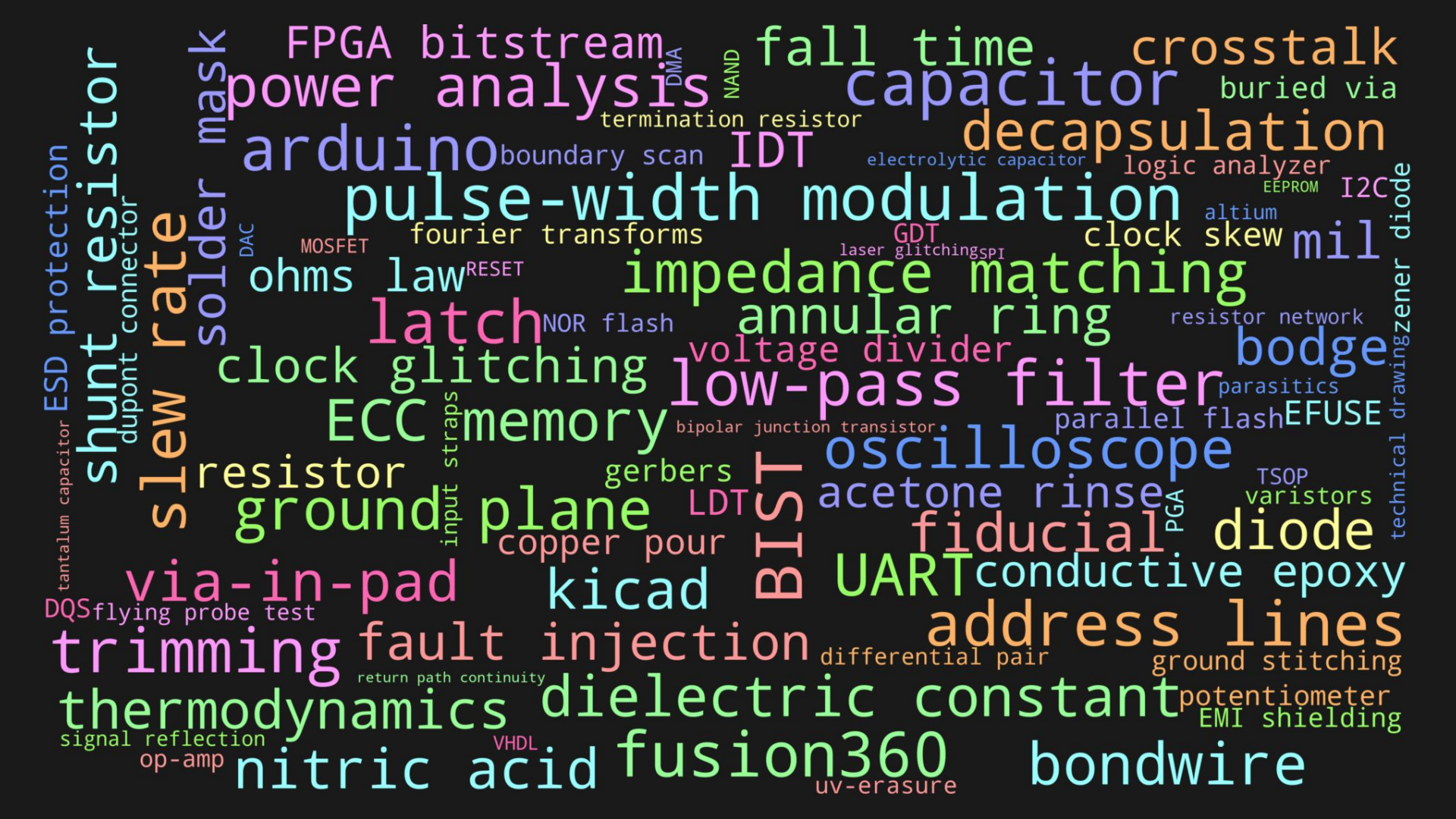
Demystifying the exploit development lifecycle

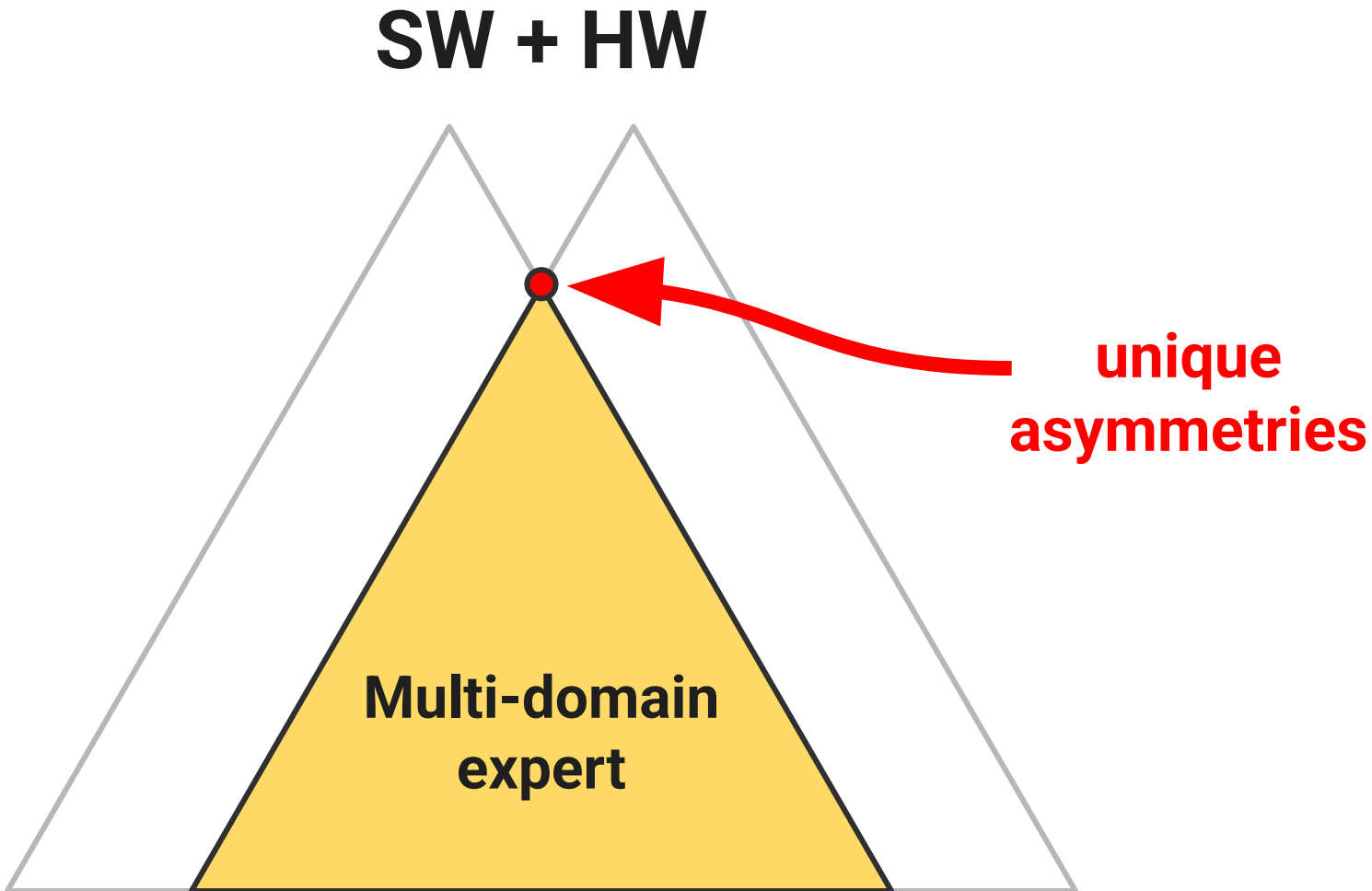
gaasedelen & itszn

RET2 SYSTEMS


Software
Mobile
0click
Browsers
0days
Custom Tooling, Fuzzing
Basic Exploitation, CTF, WarGames
Disassemblers, Debuggers
Software Development, C, Python
Hardware
Silicon
RE
ASIC
FPGA, High Speed
KiCad, PCB Design
Basic Fault Injection, Power Analysis
Logic Analyzers, Oscilloscopes
Soldering, Multimeters, UART, Flash Dumps


Software
Mobile
0click
Browsers
0days
Custo n Tooling, Fuzzing
Basic Explo tation, CTF, WarGames
Disass mblers, Debuggers
Software D evelopment, C, Python
Hardware
Silicon
RE
ASIC
FPGA, High Speed
KiCad, PCB Design
Basic Fault Injection, Power Analysis
Logic Analyzers, Oscilloscopes
Soldering, Multimeters, UART, Flash Dumps


FPGA bitstream
fall time
crosstalk
power analysis
capacitor
buried via
DMA
NAND
termination resistor
decapsulation
arduino
boundary scan
IDT
electrolytic capacitor
logic analyzer
EEPROM
I2C
pulse-width modulation
altium
shunt resistor
solder mask
fourier transforms
GDT
clock skew
mil
MOSFET
laser glitching
SPI
DAC
ohms law
RESET
impedance matching
zener diode
ESD protection
dupont connector
latch
NOR flash
annular ring
resistor network
slew rate
voltage divider
bodge
clock glitching
low-pass filter
parasitics
ECC memory
parallel flash
EFUSE
input straps
bipolar junction transistor
technical drawing
oscilloscope
resistor
gerbers
TSOP
acetone rinse
varistors
ground plane
LDT
PGA
fiducial
diode
BIST
copper pour
UART
conductive epoxy
tantalum capacitor
via-in-pad
kicad
address lines
DQS
flying probe test
trimming
fault injection
differential pair
ground stitching
return path continuity
thermodynamics
dielectric constant
potentiometer
EMI shielding
signal reflection
VHDL
op-amp
nitric acid
fusion360
bondwire
uv-erasure


SW + HW
unique
asymmetries
Multi-domain
expert

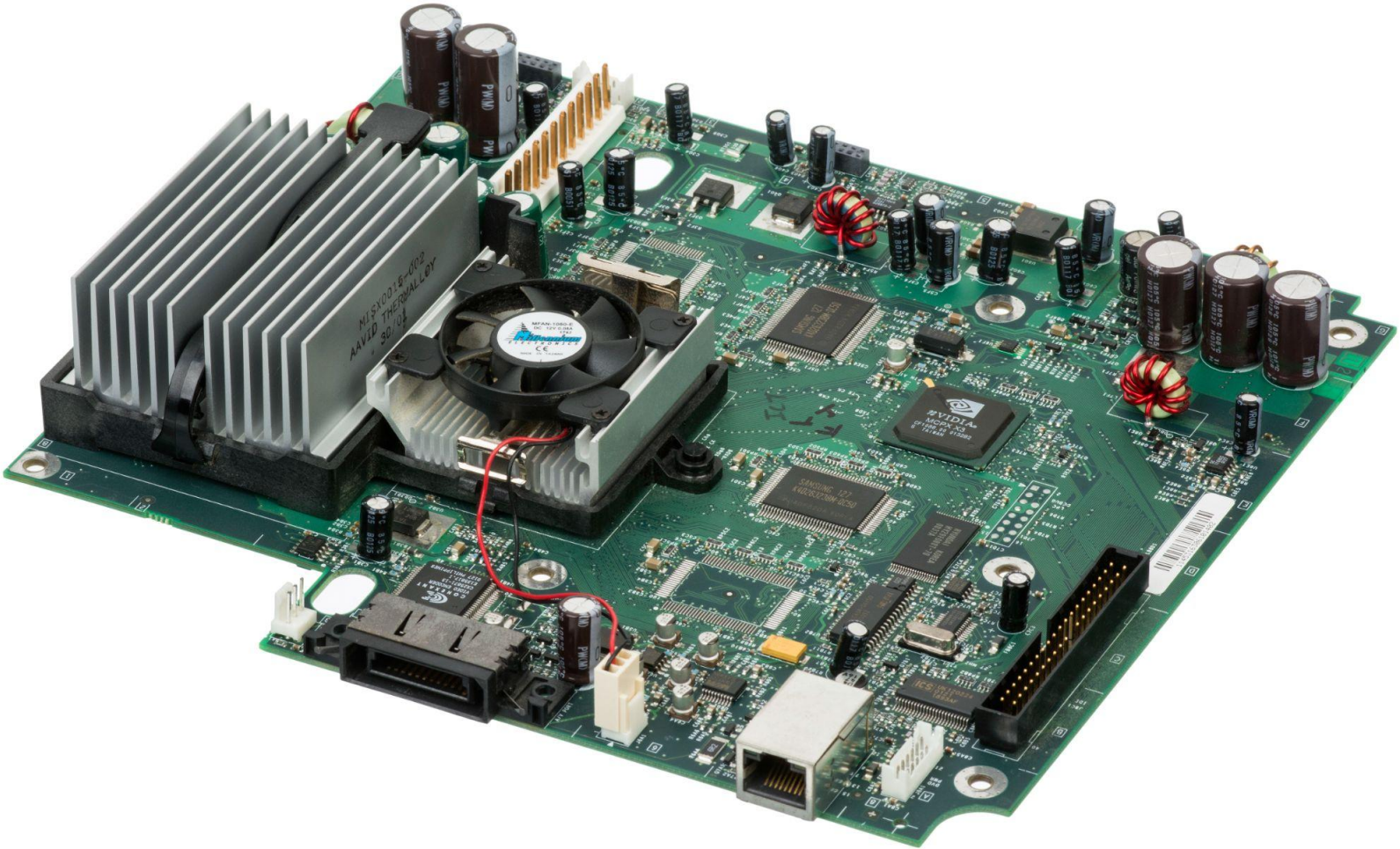
Agenda

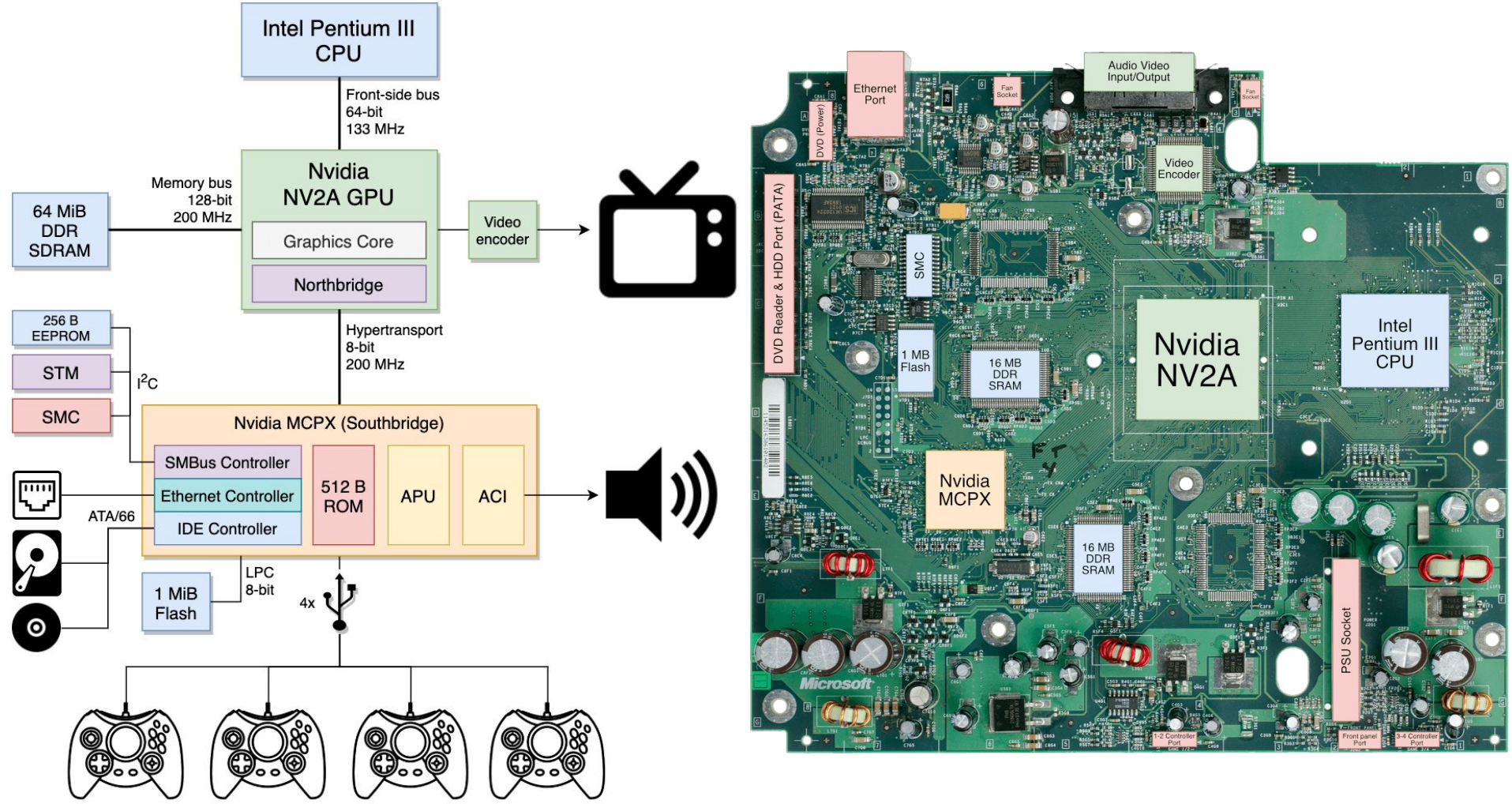
- ~~**Prologue**~~
- **Xbox**
  - Background & Resources
  - Basic Hardware Hacking
  - Basic Hardware Engineering
  - Bill Gates' Secret Bondwire
  - PIC16 / SMC Research
  - CPU Interposers
- **Epilogue**

The 'Original' Microsoft Xbox, 2001


HALO
COMBAT EVOLVED


XBOX
WARNING
DISCONNECT POWER TO XBOX
Part No :X06603-006
Western Digital
Microsoft

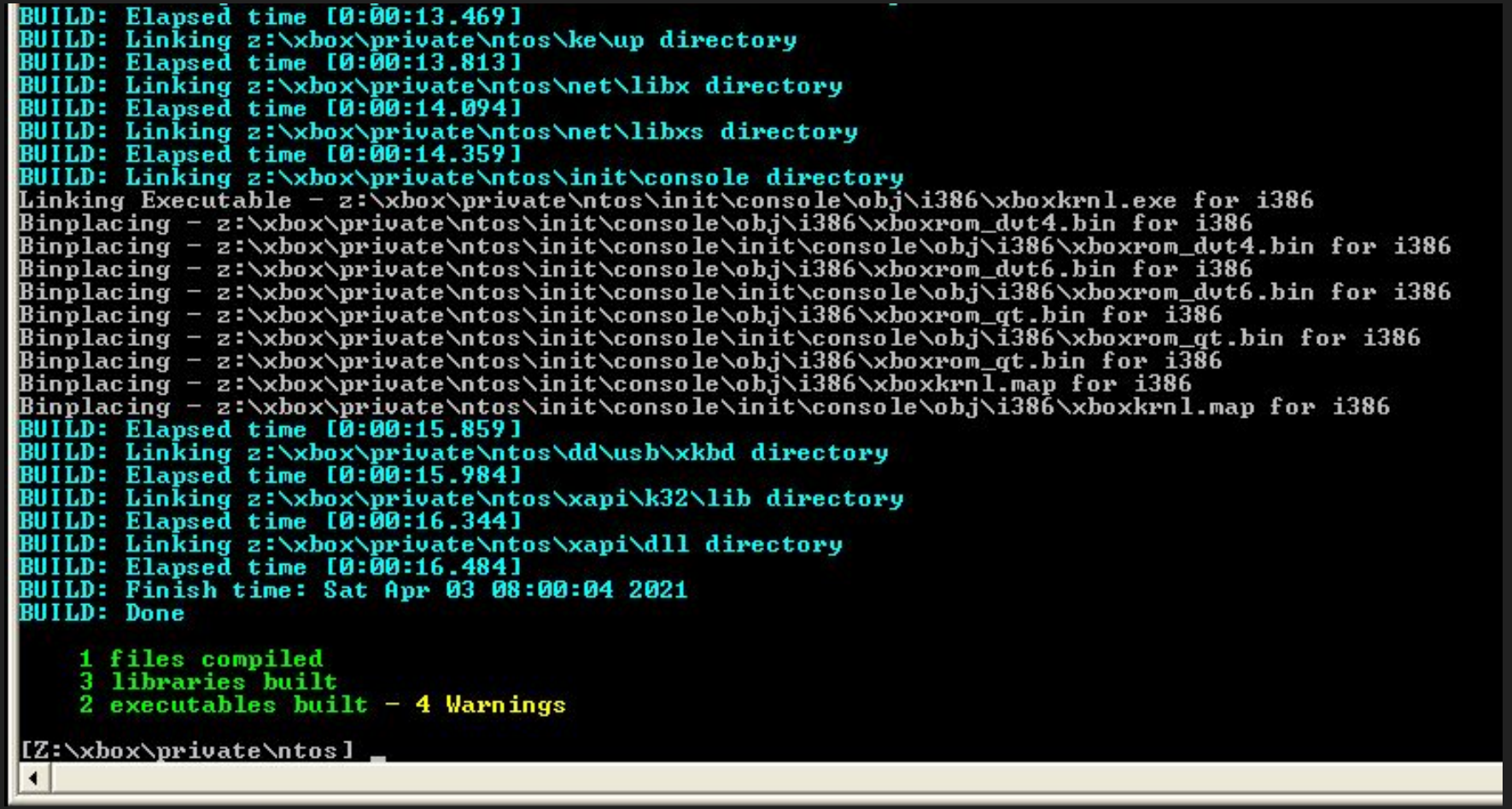

NVIDIA


Intel Pentium III CPU
Front-side bus
64-bit
133 MHz
Nvidia NV2A GPU
Graphics Core
Northbridge
Memory bus
128-bit
200 MHz
64 MiB DDR SDRAM
Video encoder
Hypertransport
8-bit
200 MHz
256 B EEPROM
STM
SMC
I²C
Nvidia MCPX (Southbridge)
SMBus Controller
Ethernet Controller
IDE Controller
512 B ROM
APU
ACI
ATA/66
1 MiB Flash
LPC
8-bit
4x
Ethernet Port
Audio Video Input/Output
DVD (Power)
Fan Socket
Video Encoder
DVD Reader & HDD Port (PATA)
SMC
1 MB Flash
16 MB DDR SRAM
Nvidia NV2A
Intel Pentium III CPU
Nvidia MCPX
16 MB DDR SRAM
PSU Socket
Microsoft
1-2 Controller Port
Front panel Port
3-4 Controller Port


ONE FOR BABIES
Burnett • Tudor
The Secret Garden
HARPER
TRACY KIDDER
WINNER OF THE PULITZER PRIZE
THE SOUL OF A NEW MACHINE
BACK BAY BOOKS
HACKING THE XBOX
BUNNIE
NO STARCH PRESS
PoC || GTFO II
THE GHIDRA BOOK
EAGLE AND NANCE

Leaked Technical Resources

- **Complete Source Tree Leak -- HOLY GRAIL**
  - Microsoft.OriginalXbox.Repo.zip -- April 2002, the '4400' leak (1.2gb)
- **Retail Motherboard Schematics**
  - Launch, XBLADE, Tuscany (PDFs)
- **Xbox Hardware Design Specification**
  - v0.91, v1.00, v1.02 (PDFs)
- **Official Xbox SDK's used by Game Developers**
  - XDK 5849.17 being the 'final' one
- **Misc 'confidential' datasheets / design documents ...**


BUILD: Elapsed time [0:00:13.469]
BUILD: Linking z:\xbox\private\ntos\ke\up directory
BUILD: Elapsed time [0:00:13.813]
BUILD: Linking z:\xbox\private\ntos\net\libx directory
BUILD: Elapsed time [0:00:14.094]
BUILD: Linking z:\xbox\private\ntos\net\libxs directory
BUILD: Elapsed time [0:00:14.359]
BUILD: Linking z:\xbox\private\ntos\init\console directory
Linking Executable - z:\xbox\private\ntos\init\console\obj\i386\xboxkrnl.exe for i386
Binplacing - z:\xbox\private\ntos\init\console\obj\i386\xboxrom_dvt4.bin for i386
Binplacing - z:\xbox\private\ntos\init\console\init\console\obj\i386\xboxrom_dvt4.bin for i386
Binplacing - z:\xbox\private\ntos\init\console\obj\i386\xboxrom_dvt6.bin for i386
Binplacing - z:\xbox\private\ntos\init\console\init\console\obj\i386\xboxrom_dvt6.bin for i386
Binplacing - z:\xbox\private\ntos\init\console\obj\i386\xboxrom_qt.bin for i386
Binplacing - z:\xbox\private\ntos\init\console\init\console\obj\i386\xboxrom_qt.bin for i386
Binplacing - z:\xbox\private\ntos\init\console\obj\i386\xboxrom_qt.bin for i386
Binplacing - z:\xbox\private\ntos\init\console\obj\i386\xboxkrnl.map for i386
Binplacing - z:\xbox\private\ntos\init\console\init\console\obj\i386\xboxkrnl.map for i386
BUILD: Elapsed time [0:00:15.859]
BUILD: Linking z:\xbox\private\ntos\dd\usb\xkbd directory
BUILD: Elapsed time [0:00:15.984]
BUILD: Linking z:\xbox\private\ntos\xapi\k32\lib directory
BUILD: Elapsed time [0:00:16.344]
BUILD: Linking z:\xbox\private\ntos\xapi\dll directory
BUILD: Elapsed time [0:00:16.484]
BUILD: Finish time: Sat Apr 03 08:00:04 2021
BUILD: Done
1 files compiled
3 libraries built
2 executables built - 4 Warnings
[Z:\xbox\private\ntos]

Retail BIOS Timeline

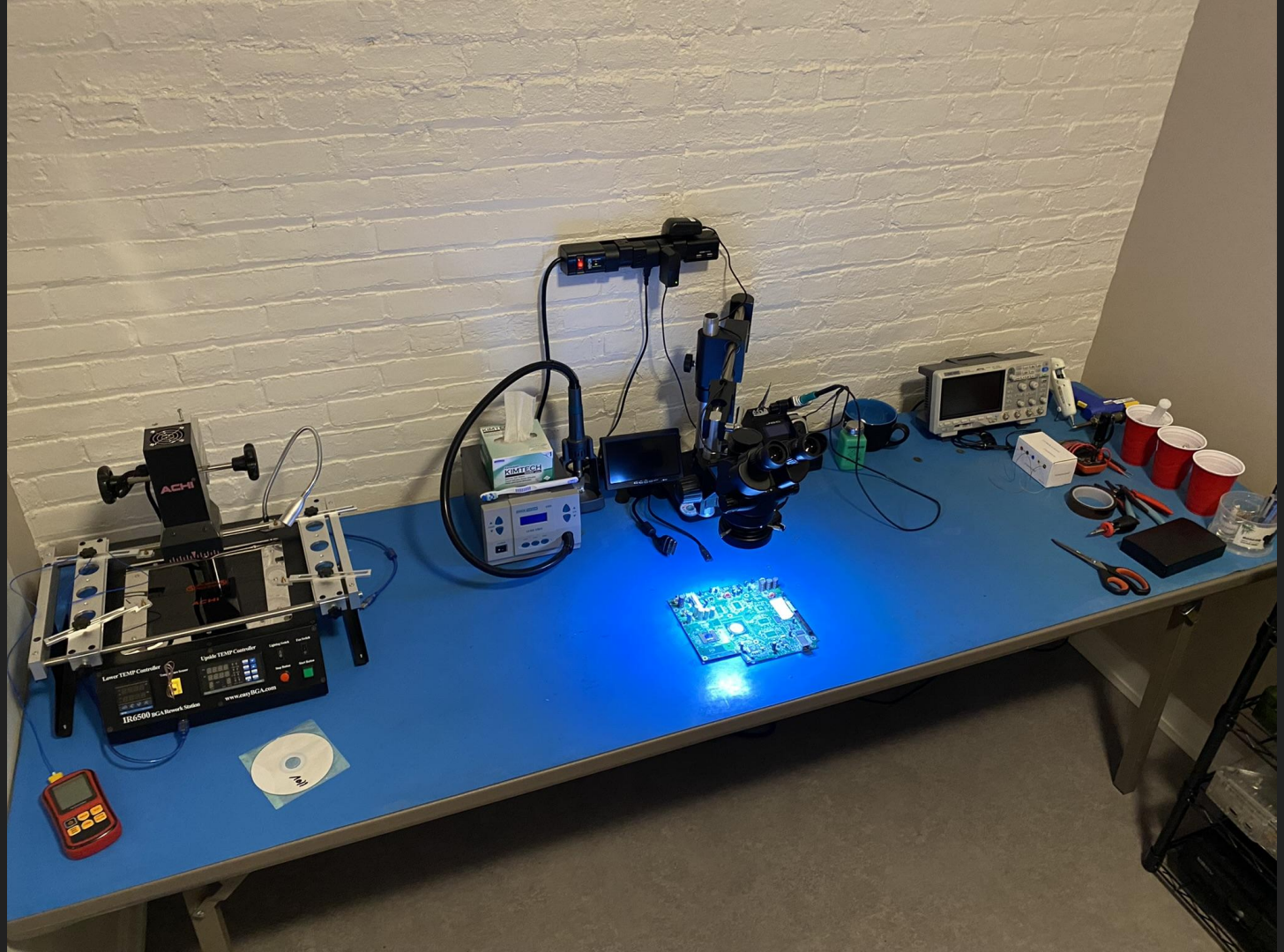
- 3944 - September 2001
- 4034 - October 2001
- 4817 - July 2002
- 5101 - October 2002
- 5530 - April 2003
- 5713 - August 2003
- 5838 - December 2003

Retail BIOS Breakdown

- **Xbox Flash ROM - 256kb**
  - ~8kb for HW initialization logic ('xcodes')
  - ~24kb for bootloader(s) (bldr32 / preldr32 or '2bl' / 'fbl')
  - ~224kb for encrypted+compressed Kernel & Boot Animation (xboxkrnl.exe)
    - ~600kb decompressed
      - 200kb Kernel, 400kb for the boot animation (DirectX)
    - NT-based, heavily pared down Windows 2000 Kernel

- **512 byte 'secret' bootrom**
  - Establishes the 'chain of trust'
  - Burned into the MCPX silicon
  - First x86 instructions executed out of CPU reset

Basic Hardware Hacking


ACHI
Lower TEMP Controller
Upside TEMP Controller
IR6500 BGA Rework Station
www.easyBGA.com
KIMTECH

Recommended Lab Equipment

- **Trinocular microscope -- $500**
- **Soldering station -- $125**
- **Hot air station -- $150**
- **Misc tools -- $125**
  - Micro cutter, Tweezers
  - iFixit Mako Driver Kit
  - Grinding pen
  - Multimeter
- **Supplies -- $100**
  - Kester solder, leaded 63/37
  - STIRRI-V3-TF flux (syringe)
  - Kimtech wipes, cotton q-tips
  - 99% isopropyl alcohol
  - 3-mil nitrile gloves
  - 30awg wire kit

$1000 USD

Trinocular microscope, double boom

(Eakins, AmScope, etc)

$272.54 ~~$332.36~~ 18% off

Tax excluded, add at checkout if applicable.

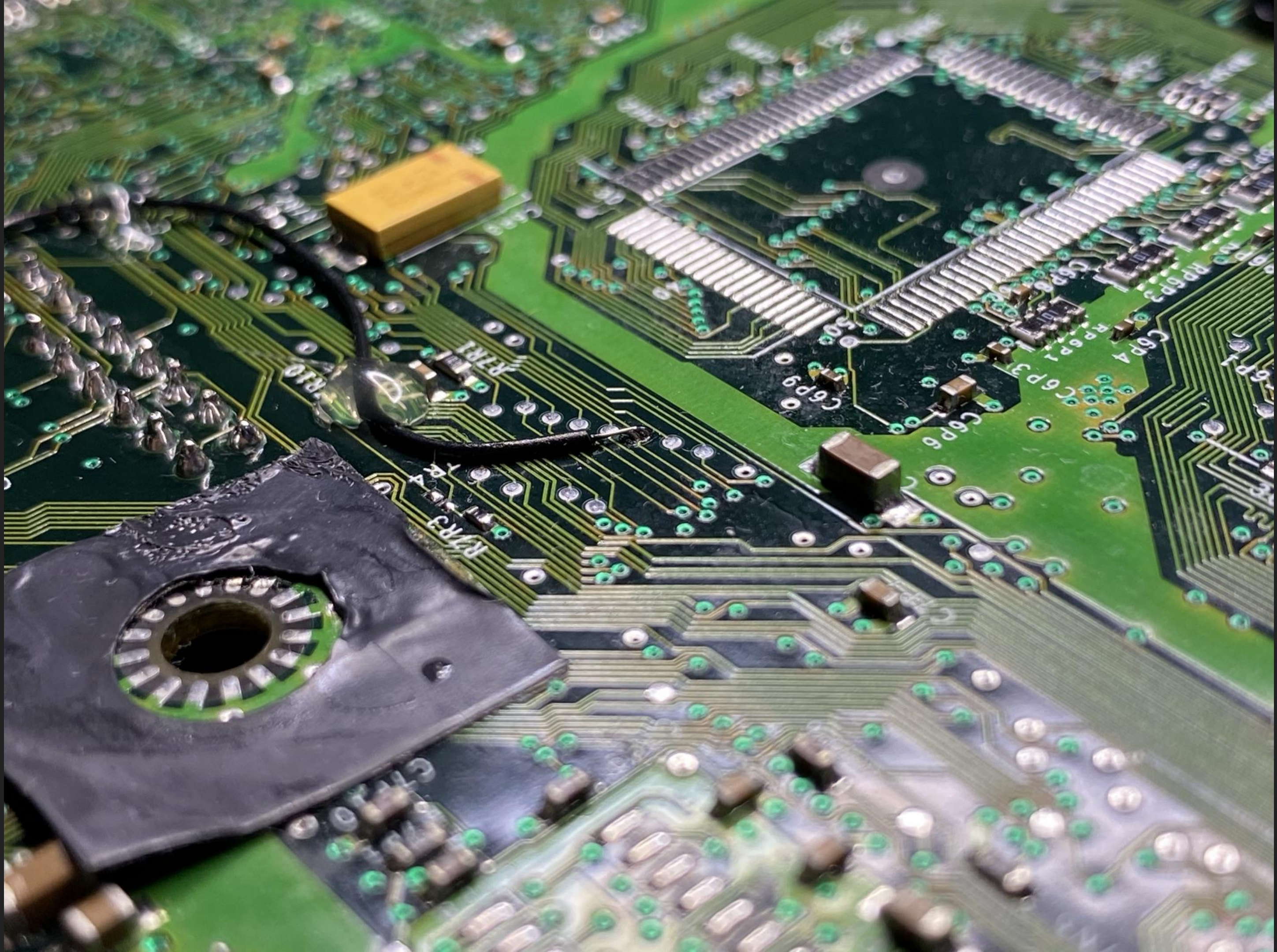
up to 4 x $68.14 with no interest

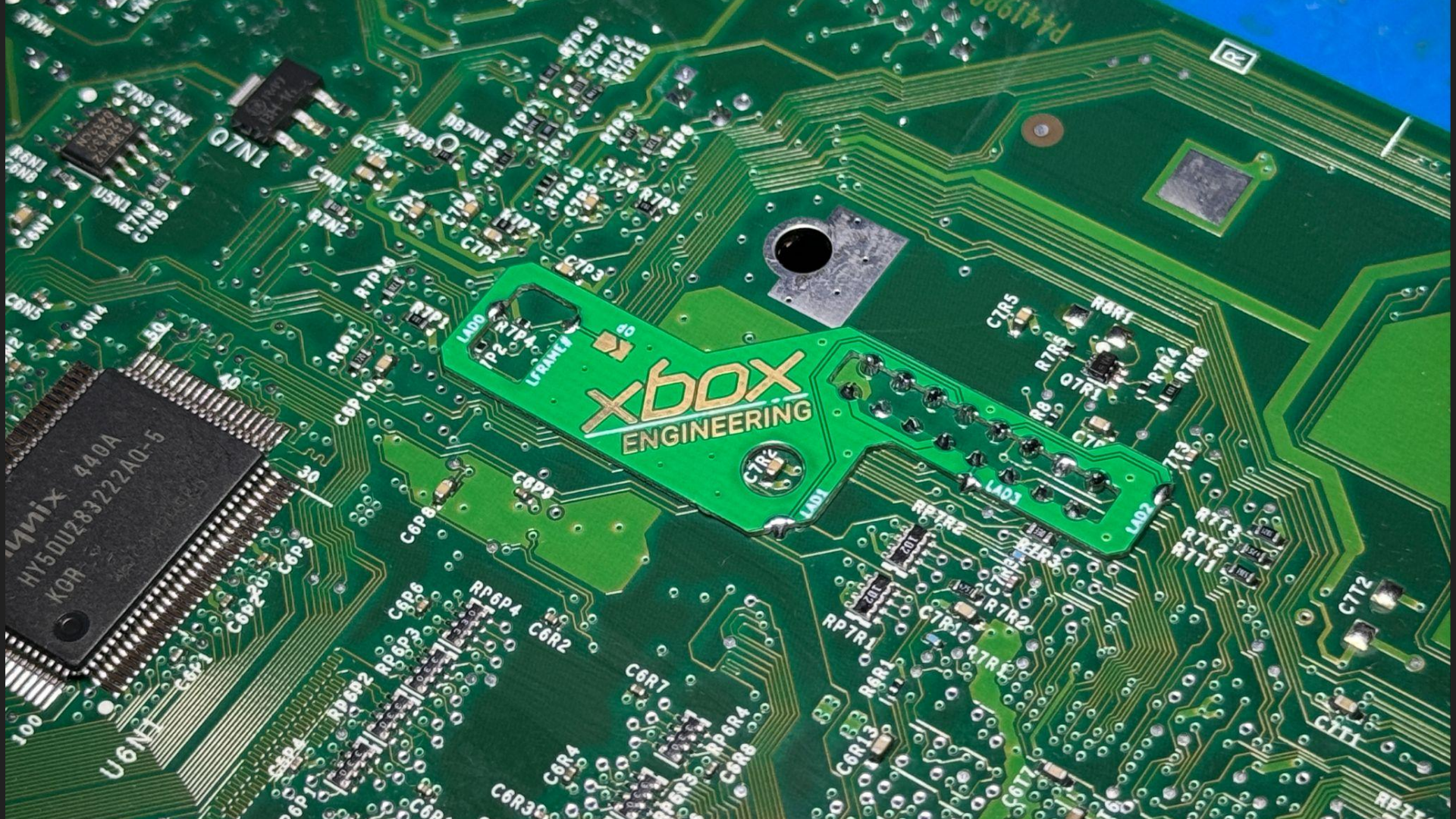
3.5X 90X 180X Simul-Focus Double Boom Stand Trinocular Stereo Zoom Microscope 48MP 55MP 2K 4K HDMI VGA USB Camera For PCB Repair

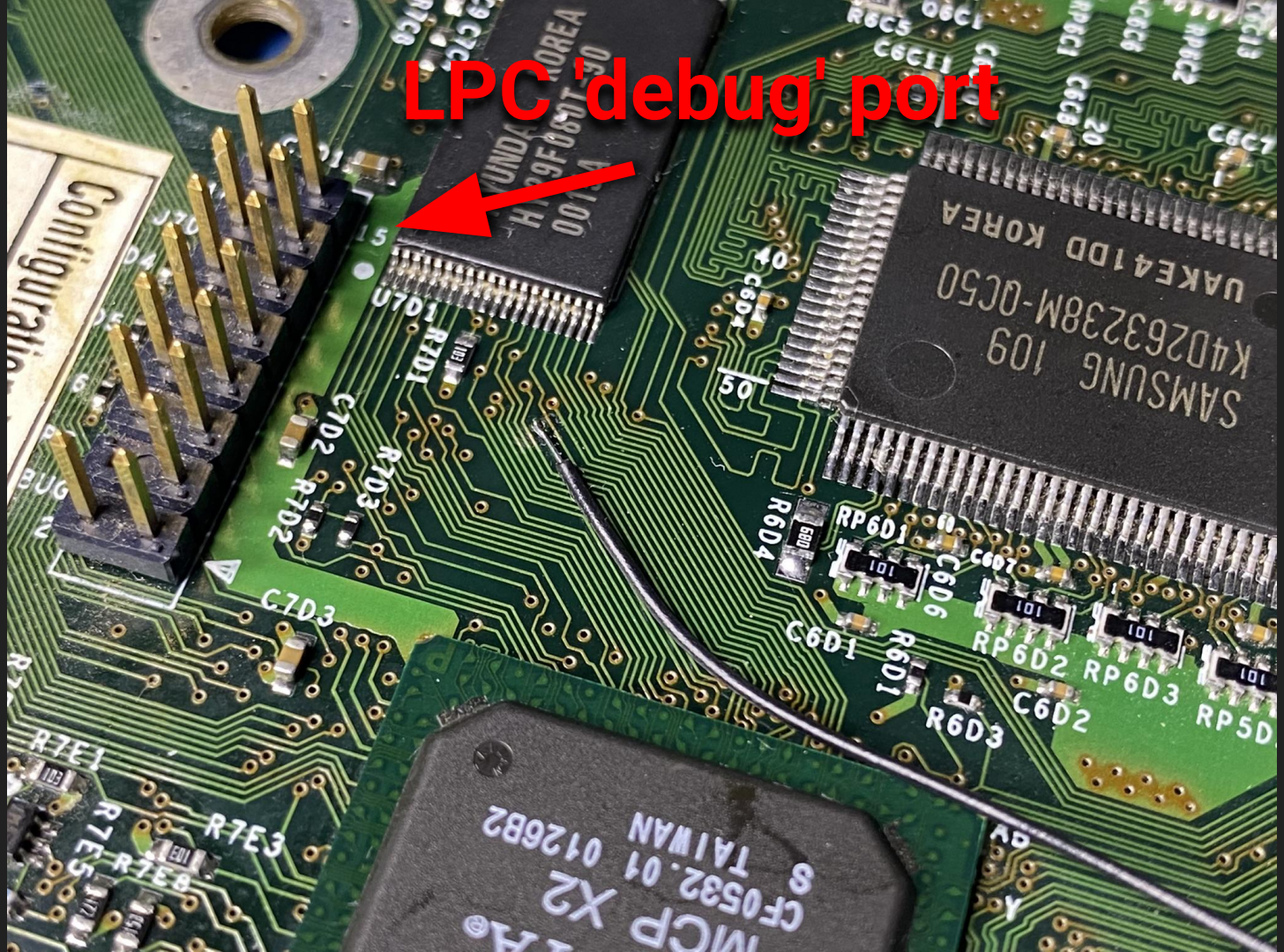
4.3 3 Reviews | 24 sold

Color: B HDMI VGA Camera

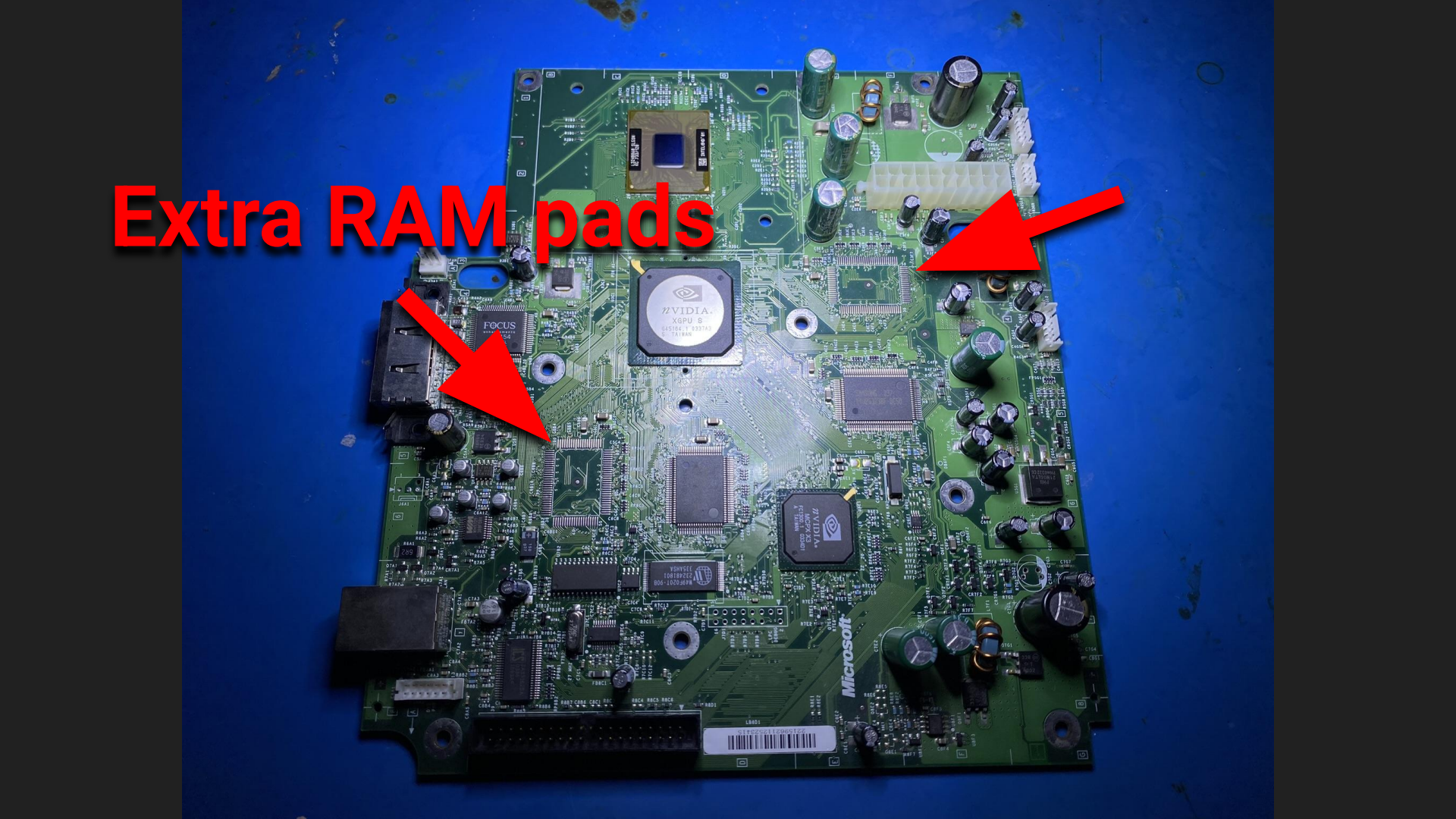
+$250 shipping

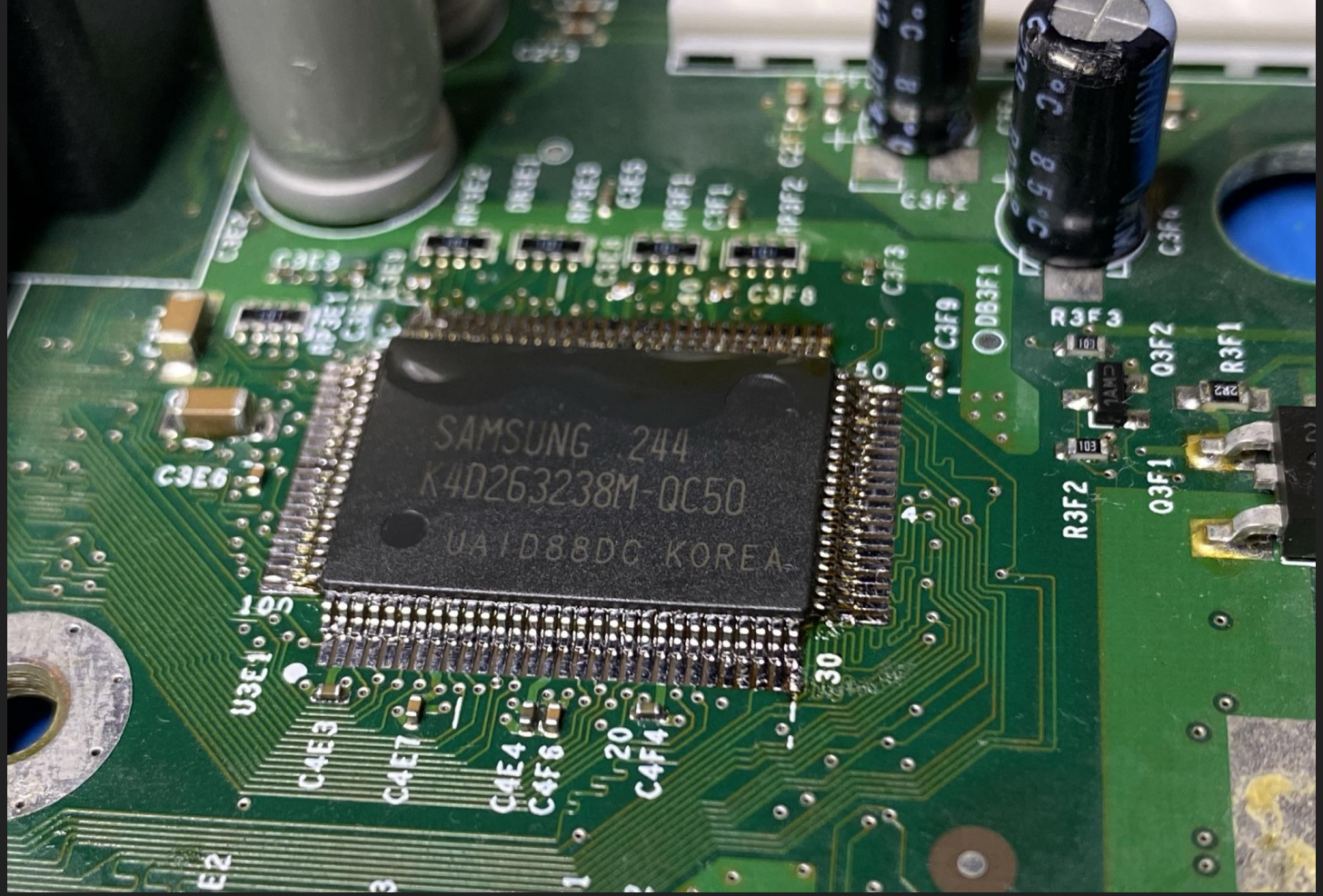

C6P9
C6P6
C6P3
C6P4
R7R3


xbox
ENGINEERING
LAD0
LFRAME#
LAD3
LAD1
LAD2
hynix
HY5DU283222AO-5
U6N1
Q7N1
U5N1

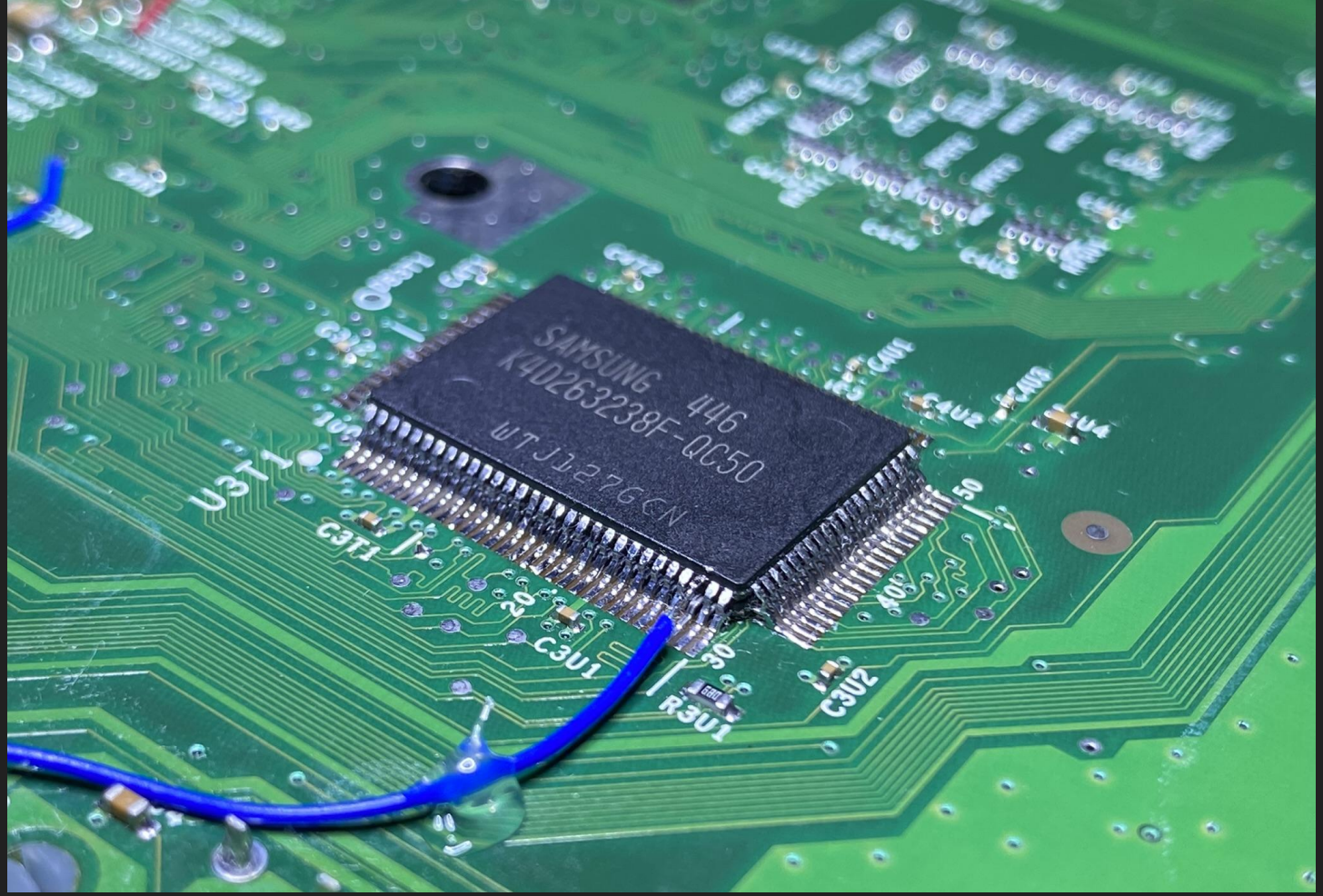

LPC 'debug' port

https://github.com/Ryzee119/OpenXenium


Extra RAM pads
NVIDIA
XGPU
FOCUS
Microsoft

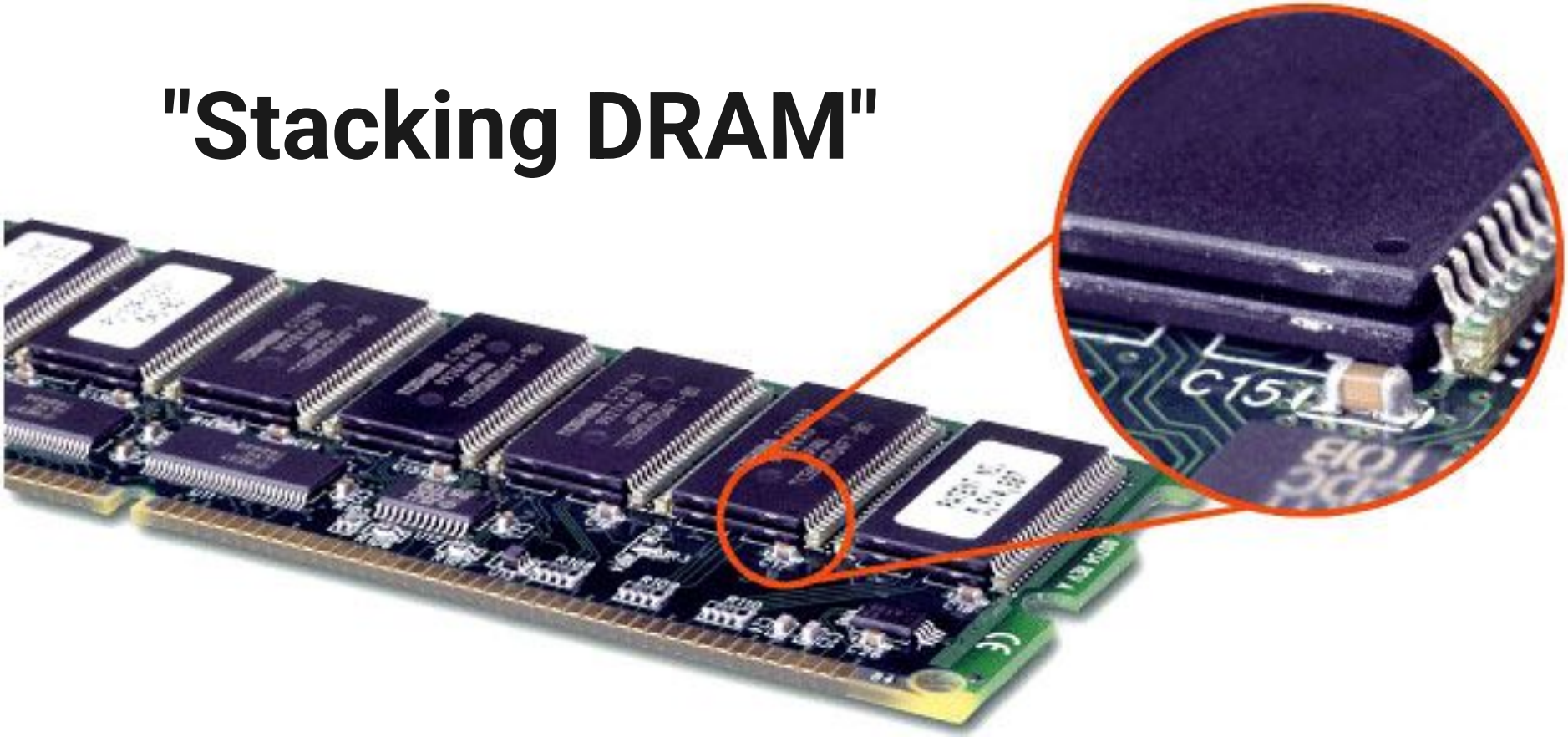


64mb → 128mb RAM upgrade



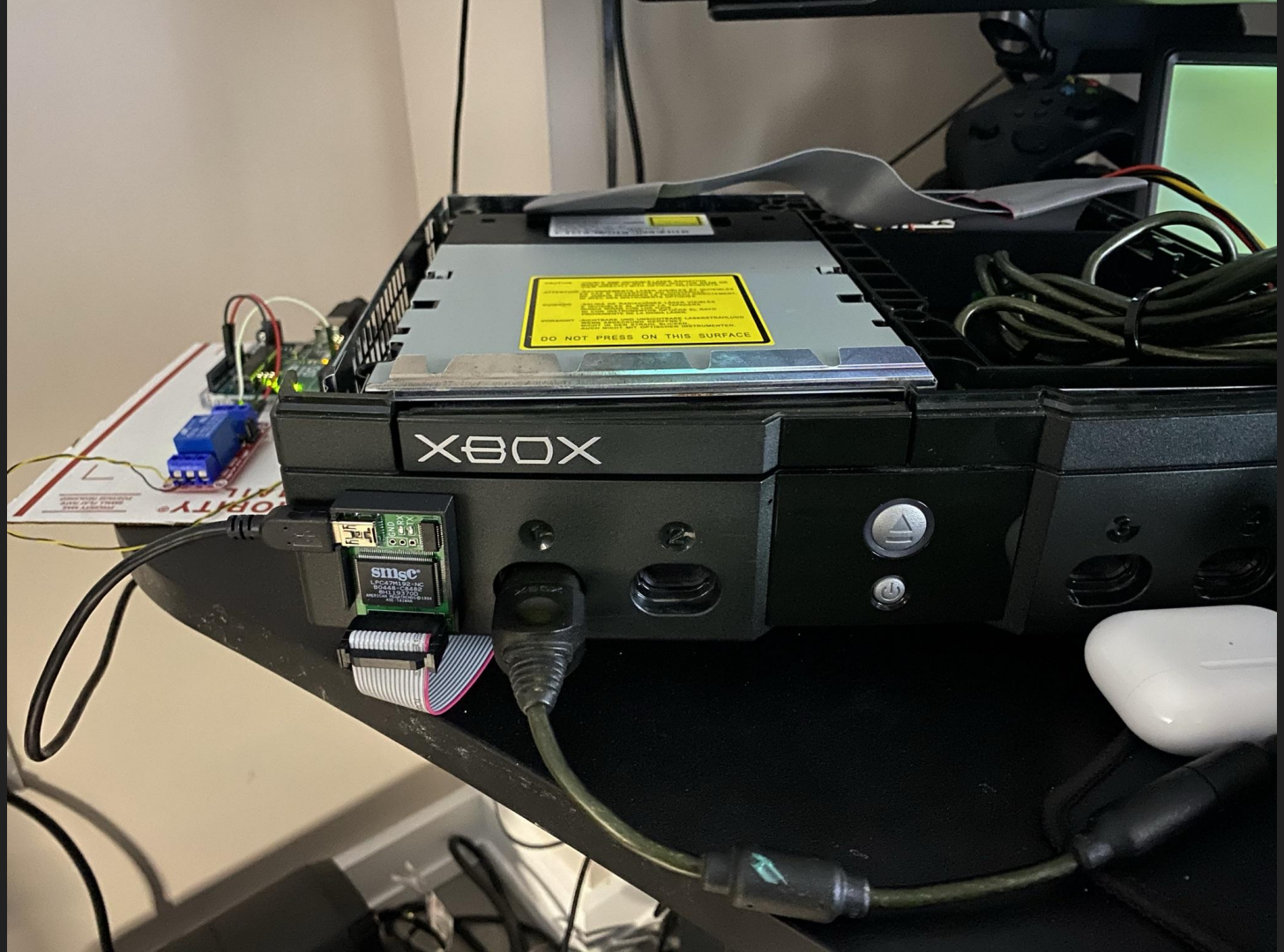
Stacking RAM chips (on rev 1.6)

"Stacking DRAM"



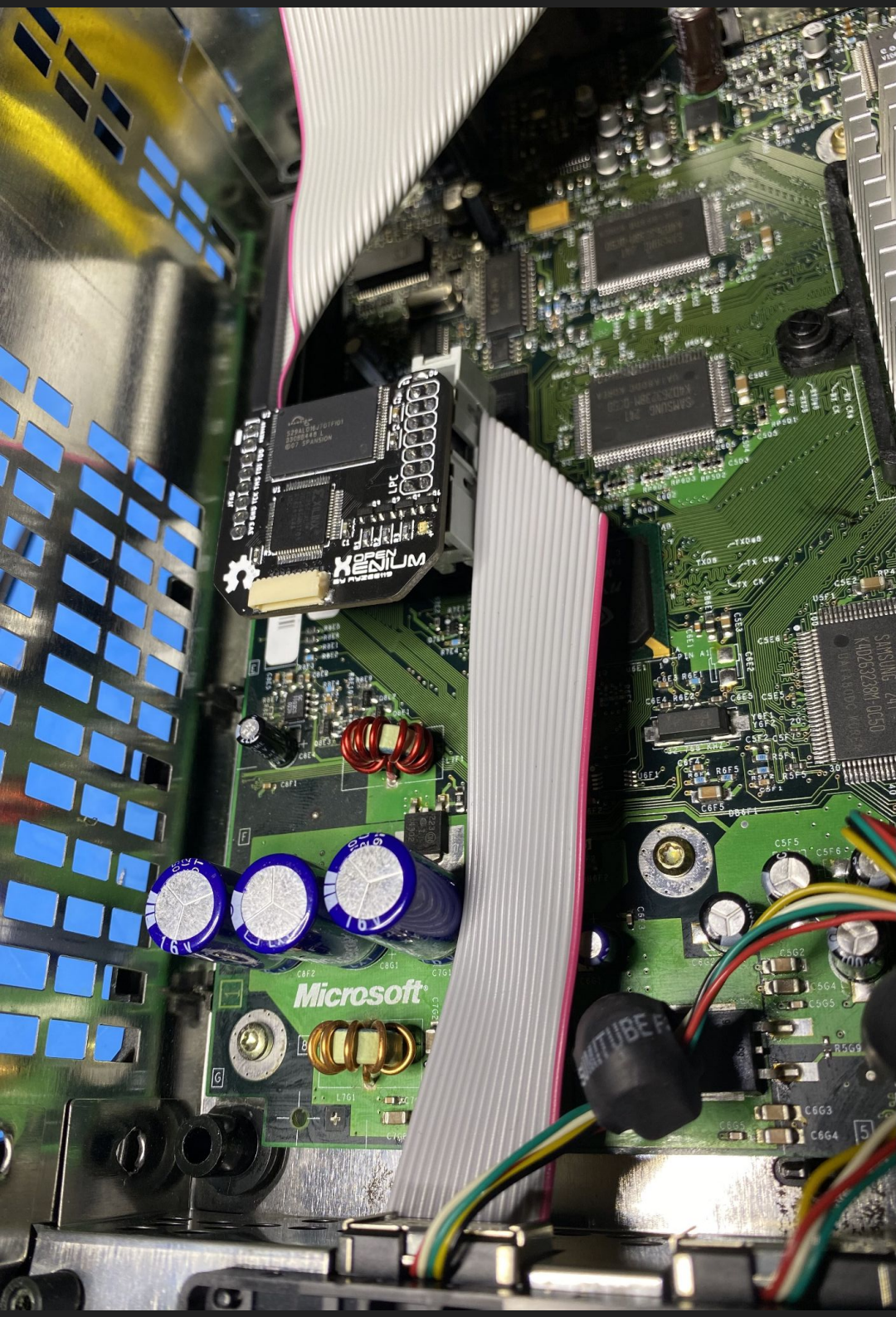
https://bit-tech.net/reviews/tech/memory/the_secrets_of_pc_memory_part_2/7/

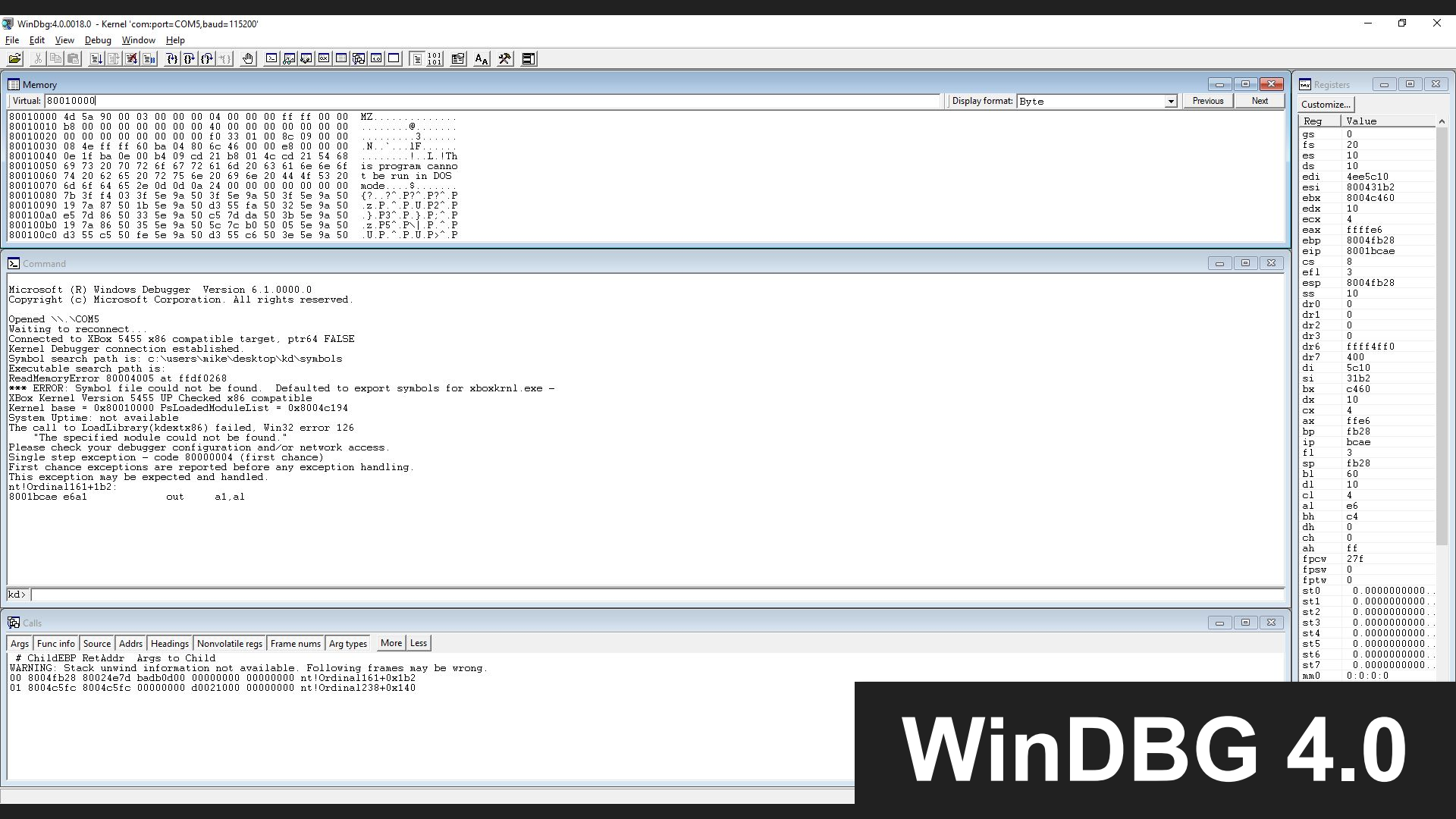
Basic Hardware Engineering

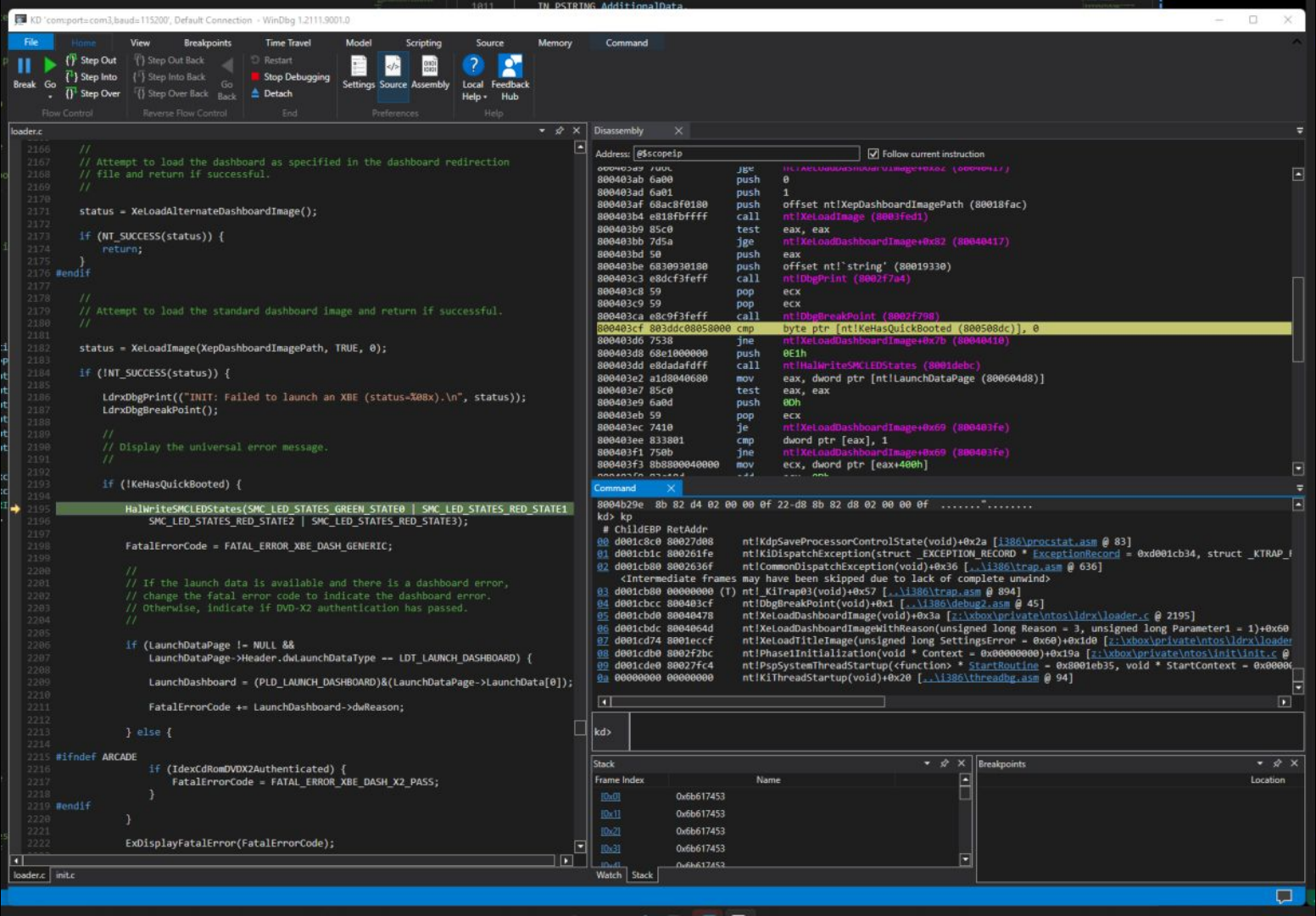

XBOX
DO NOT PRESS ON THIS SURFACE
SMSC

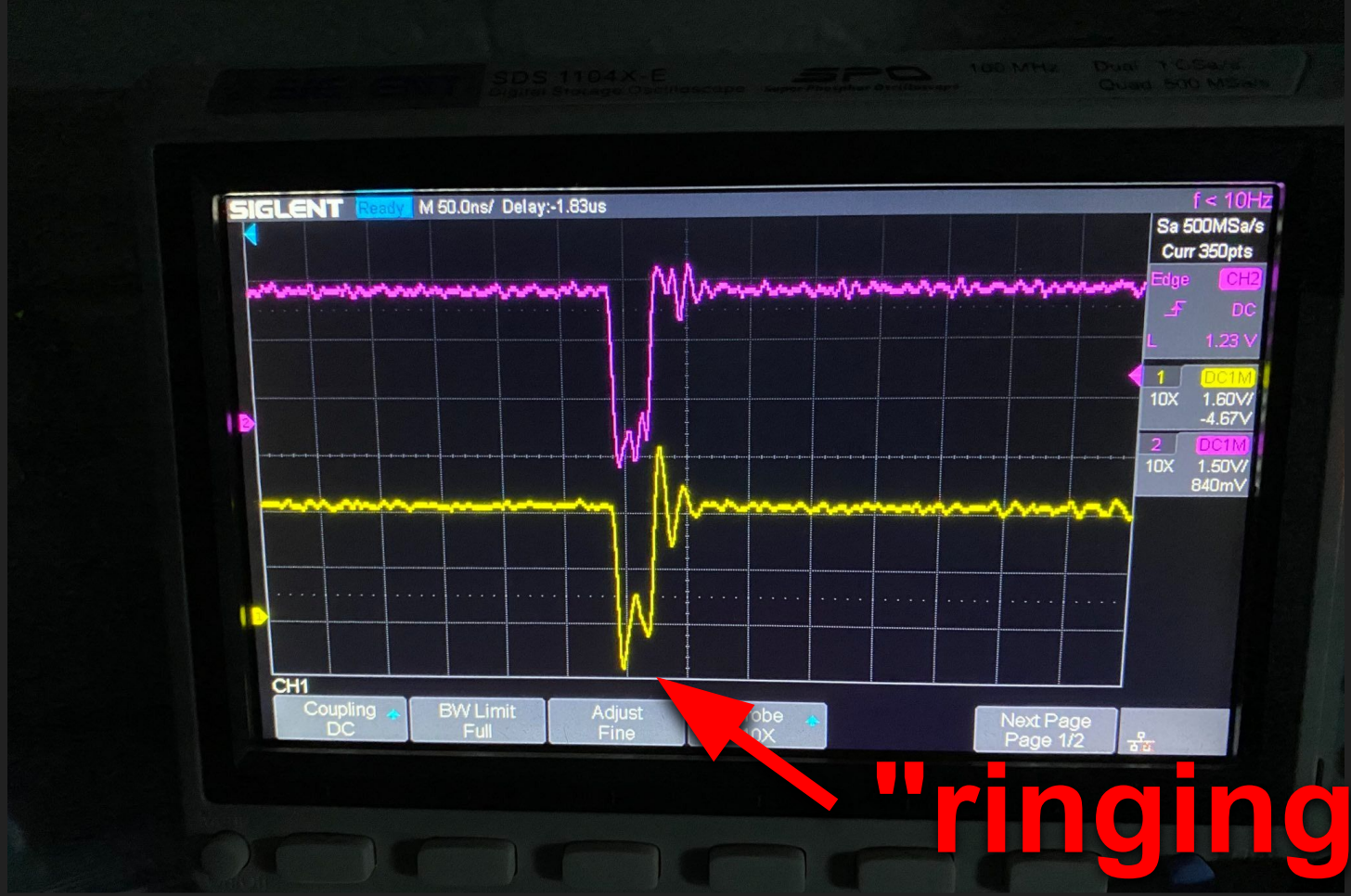
Xbox Serial USB Adapter

https://github.com/XboxDev/serial-usb-adapter


OPEN XENIUM
Microsoft

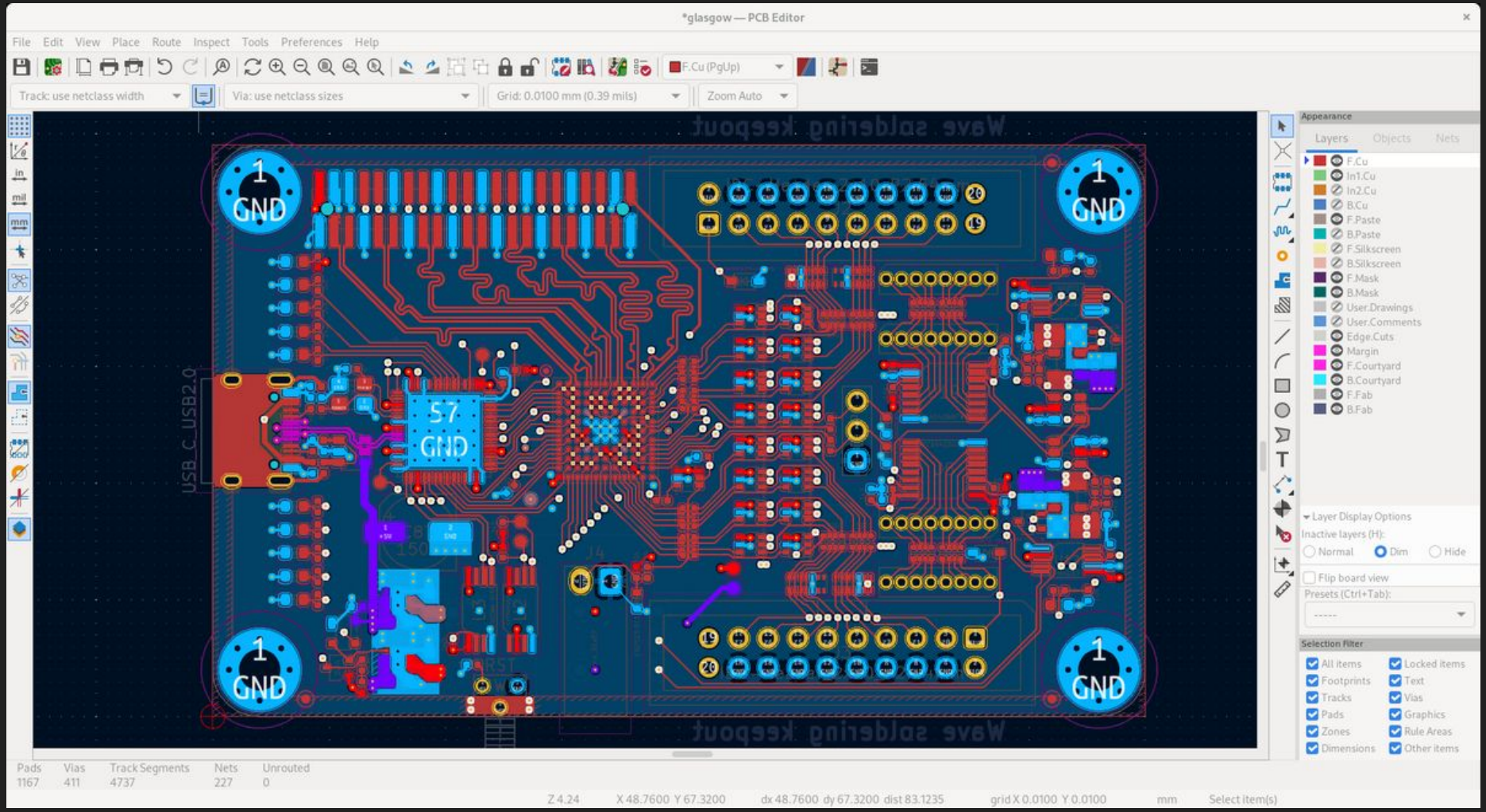

WinDbg:4.0.0018.0 - Kernel 'com:port=COM5,baud=115200'
File Edit View Debug Window Help
Memory
Virtual: 80010000
Display format: Byte
Previous
Next
80010000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
80010010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@.......
80010020 00 00 00 00 00 00 00 00 f0 33 01 00 8c 09 00 00 ....3......
80010030 08 4e ff ff 60 ba 04 80 6c 46 00 00 e8 00 00 00 .N..`...lF......
80010040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th
80010050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
80010060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS
80010070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$.......
80010080 7b 3f f4 03 3f 5e 9a 50 3f 5e 9a 50 3f 5e 9a 50 {?..?^.P?^.P?^.P
80010090 19 7a 87 50 1b 5e 9a 50 d3 55 fa 50 32 5e 9a 50 .z.P.^.P.U.P2^.P
800100a0 e5 7d 86 50 33 5e 9a 50 c5 7d da 50 3b 5e 9a 50 .}.P3^.P.}.P;^.P
800100b0 19 7a 86 50 35 5e 9a 50 5c 7c b0 50 05 5e 9a 50 .z.P5^.P\|.P.^.P
800100c0 d3 55 c5 50 fe 5e 9a 50 d3 55 c6 50 3e 5e 9a 50 .U.P.^.P.U.P>^.P
Command
Microsoft (R) Windows Debugger Version 6.1.0000.0
Copyright (c) Microsoft Corporation. All rights reserved.
Opened \\.\COM5
Waiting to reconnect...
Connected to XBox 5455 x86 compatible target, ptr64 FALSE
Kernel Debugger connection established.
Symbol search path is: c:\users\mike\desktop\kd\symbols
Executable search path is:
ReadMemoryError 80004005 at ffdf0268
*** ERROR: Symbol file could not be found. Defaulted to export symbols for xboxkrnl.exe -
XBox Kernel Version 5455 UP Checked x86 compatible
Kernel base = 0x80010000 PsLoadedModuleList = 0x8004c194
System Uptime: not available
The call to LoadLibrary(kdextx86) failed, Win32 error 126
"The specified module could not be found."
Please check your debugger configuration and/or network access.
Single step exception - code 80000004 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
nt!Ordinal161+1b2:
8001bcae e6a1 out a1,al
kd>
Calls
Args Func info Source Addrs Headings Nonvolatile regs Frame nums Arg types More Less
ChildEBP RetAddr Args to Child
WARNING: Stack unwind information not available. Following frames may be wrong.
00 8004fb28 80024e7d badb0d00 00000000 00000000 nt!Ordinal161+0x1b2
01 8004c5fc 8004c5fc 00000000 d0021000 00000000 nt!Ordinal238+0x140
Registers
Customize...
Reg Value
gs 0
fs 20
es 10
ds 10
edi 4ee5c10
esi 800431b2
ebx 8004c460
edx 10
ecx 4
eax ffffe6
ebp 8004fb28
eip 8001bcae
cs 8
efl 3
esp 8004fb28
ss 10
dr0 0
dr1 0
dr2 0
dr3 0
dr6 ffff4ff0
dr7 400
di 5c10
si 31b2
bx c460
dx 10
cx 4
ax ffe6
bp fb28
ip bcae
fl 3
sp fb28
bl 60
dl 10
cl 4
al e6
bh c4
dh 0
ch 0
ah ff
fpcw 27f
fpsw 0
fptw 0
st0 0.0000000000..
st1 0.0000000000..
st2 0.0000000000..
st3 0.0000000000..
st4 0.0000000000..
st5 0.0000000000..
st6 0.0000000000..
st7 0.0000000000..
mm0 0:0:0:0
WinDBG 4.0

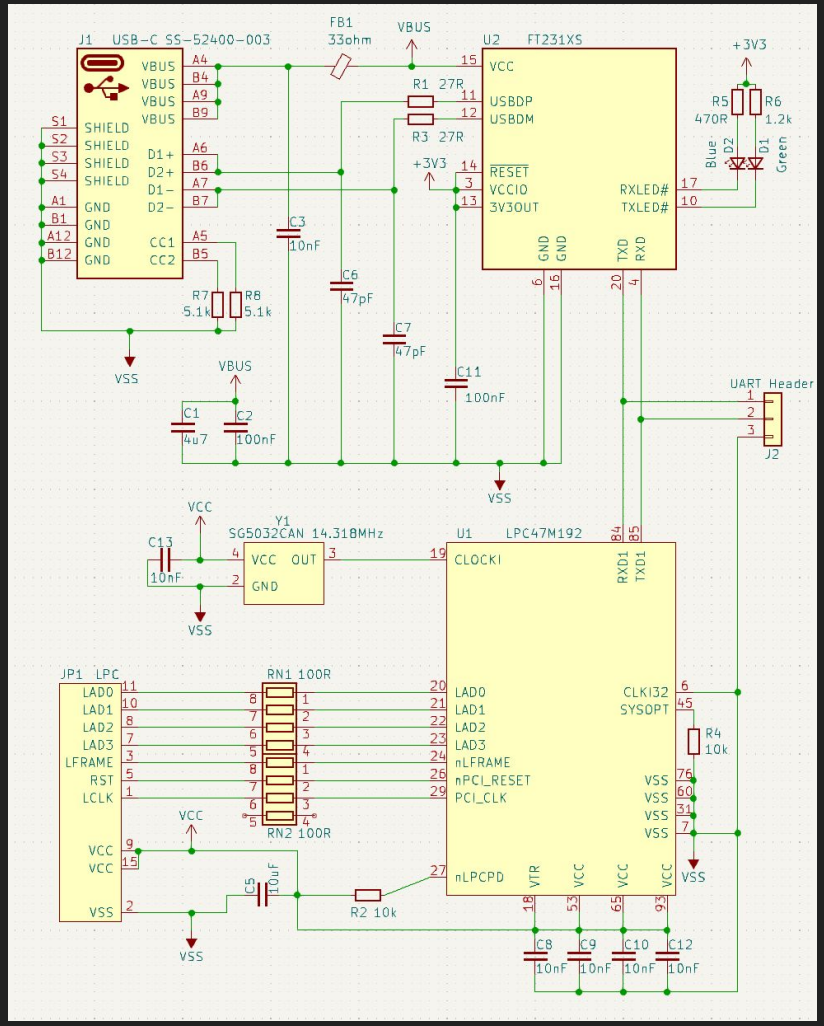

KD 'com:port=com3,baud=115200', Default Connection - WinDbg 1.2111.9001.0
File
Home
View
Breakpoints
Time Travel
Model
Scripting
Source
Memory
Command
Break
Go
Step Out
Step Into
Step Over
Step Out Back
Step Into Back
Step Over Back
Go Back
Restart
Stop Debugging
Detach
Settings
Source
Assembly
Local Help
Feedback Hub
Flow Control
Reverse Flow Control
End
Preferences
Help
loader.c
// Attempt to load the dashboard as specified in the dashboard redirection
// file and return if successful.
status = XeLoadAlternateDashboardImage();
if (NT_SUCCESS(status)) {
return;
}
#endif
// Attempt to load the standard dashboard image and return if successful.
status = XeLoadImage(XepDashboardImagePath, TRUE, 0);
if (!NT_SUCCESS(status)) {
LdrxDbgPrint(("INIT: Failed to launch an XBE (status=%08x).\n", status));
LdrxDbgBreakPoint();
// Display the universal error message.
if (!KeHasQuickBooted) {
HalWriteSMCLEDStates(SMC_LED_STATES_GREEN_STATE0 | SMC_LED_STATES_RED_STATE1 |
SMC_LED_STATES_RED_STATE2 | SMC_LED_STATES_RED_STATE3);
FatalErrorCode = FATAL_ERROR_XBE_DASH_GENERIC;
// If the launch data is available and there is a dashboard error,
// change the fatal error code to indicate the dashboard error.
// Otherwise, indicate if DVD-X2 authentication has passed.
if (LaunchDataPage != NULL &&
LaunchDataPage->Header.dwLaunchDataType == LDT_LAUNCH_DASHBOARD) {
LaunchDashboard = (PLD_LAUNCH_DASHBOARD)&(LaunchDataPage->LaunchData[0]);
FatalErrorCode += LaunchDashboard->dwReason;
} else {
#ifndef ARCADE
if (IdexCdRomDVDX2Authenticated) {
FatalErrorCode = FATAL_ERROR_XBE_DASH_X2_PASS;
}
#endif
}
ExDisplayFatalError(FatalErrorCode);
loader.c
init.c
Disassembly
Address: @$scopeip
Follow current instruction
800403ab 6a00 push 0
800403ad 6a01 push 1
800403af 68ac8f0180 push offset nt!XepDashboardImagePath (80018fac)
800403b4 e818fbffff call nt!XeLoadImage (8003fed1)
800403b9 85c0 test eax, eax
800403bb 7d5a jge nt!XeLoadDashboardImage+0x82 (80040417)
800403bd 50 push eax
800403be 6830930180 push offset nt!`string' (80019330)
800403c3 e8dcf3feff call nt!DbgPrint (8002f7a4)
800403c8 59 pop ecx
800403c9 59 pop ecx
800403ca e8c9f3feff call nt!DbgBreakPoint (8002f798)
800403cf 803ddc08058000 cmp byte ptr [nt!KeHasQuickBooted (800508dc)], 0
800403d6 7538 jne nt!XeLoadDashboardImage+0x7b (80040410)
800403d8 68e1000000 push 0E1h
800403dd e8dadafdff call nt!HalWriteSMCLEDStates (8001debc)
800403e2 a1d8040680 mov eax, dword ptr [nt!LaunchDataPage (800604d8)]
800403e7 85c0 test eax, eax
800403e9 6a0d push 0Dh
800403eb 59 pop ecx
800403ec 7410 je nt!XeLoadDashboardImage+0x69 (800403fe)
800403ee 833801 cmp dword ptr [eax], 1
800403f1 750b jne nt!XeLoadDashboardImage+0x69 (800403fe)
800403f3 8b8800040000 mov ecx, dword ptr [eax+400h]
Command
8004b29e 8b 82 d4 02 00 00 0f 22-d8 8b 82 d8 02 00 00 0f ....".........
kd> kp
ChildEBP RetAddr
00 d001c8c0 80027d08 nt!KdpSaveProcessorControlState(void)+0x2a [i386\procstat.asm @ 83]
01 d001cb1c 800261fe nt!KiDispatchException(struct _EXCEPTION_RECORD * ExceptionRecord = 0xd001cb34, struct _KTRAP_
02 d001cb80 8002636f nt!CommonDispatchException(void)+0x36 [..\i386\trap.asm @ 636]
<Intermediate frames may have been skipped due to lack of complete unwind>
03 d001cb80 00000000 (T) nt!_KiTrap03(void)+0x57 [..\i386\trap.asm @ 894]
04 d001cbcc 800403cf nt!DbgBreakPoint(void)+0x1 [..\i386\debug2.asm @ 45]
05 d001cbd0 80040478 nt!XeLoadDashboardImage(void)+0x3a [z:\xbox\private\ntos\ldrx\loader.c @ 2195]
06 d001cbdc 8004064d nt!XeLoadDashboardImageWithReason(unsigned long Reason = 3, unsigned long Parameter1 = 1)+0x60
07 d001cd74 8001eccf nt!XeLoadTitleImage(unsigned long SettingsError = 0x60)+0x1d0 [z:\xbox\private\ntos\ldrx\loader
08 d001cdb0 8002f2bc nt!Phase1Initialization(void * Context = 0x00000000)+0x19a [z:\xbox\private\ntos\init\init.c @
09 d001cde0 80027fc4 nt!PspSystemThreadStartup(<function> * StartRoutine = 0x8001eb35, void * StartContext = 0x0000
0a 00000000 00000000 nt!KiThreadStartup(void)+0x20 [..\i386\threadbg.asm @ 94]
kd>
Stack
Frame Index
Name
0x0
0x6b617453
0x1
0x6b617453
0x2
0x6b617453
0x3
0x6b617453
Breakpoints
Location
Watch
Stack

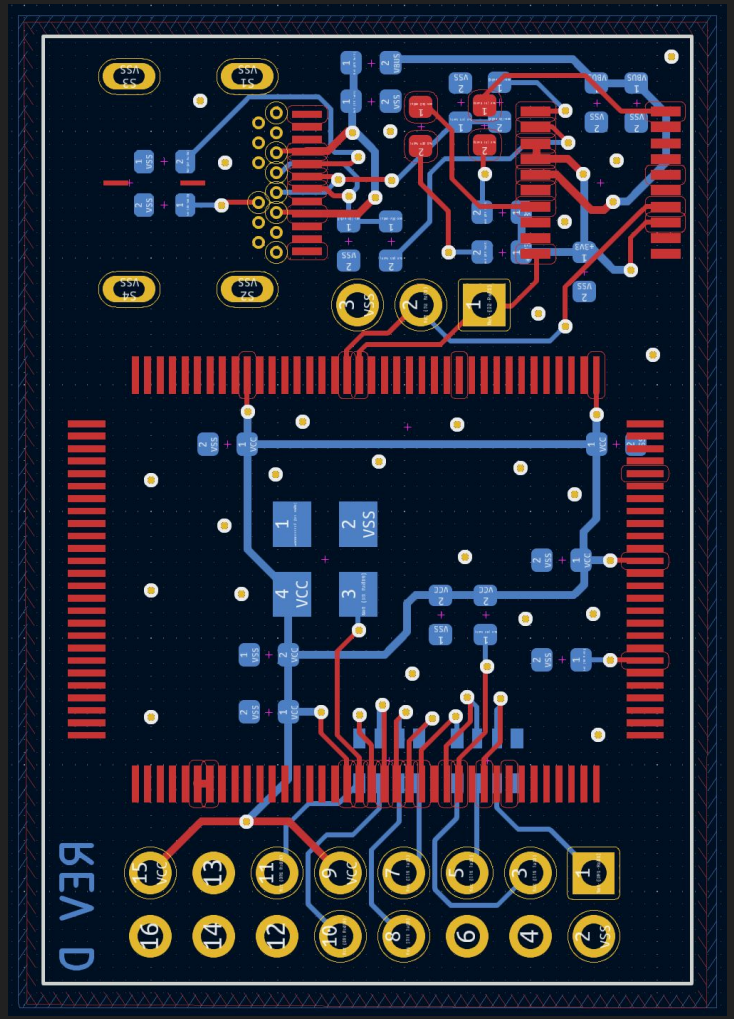


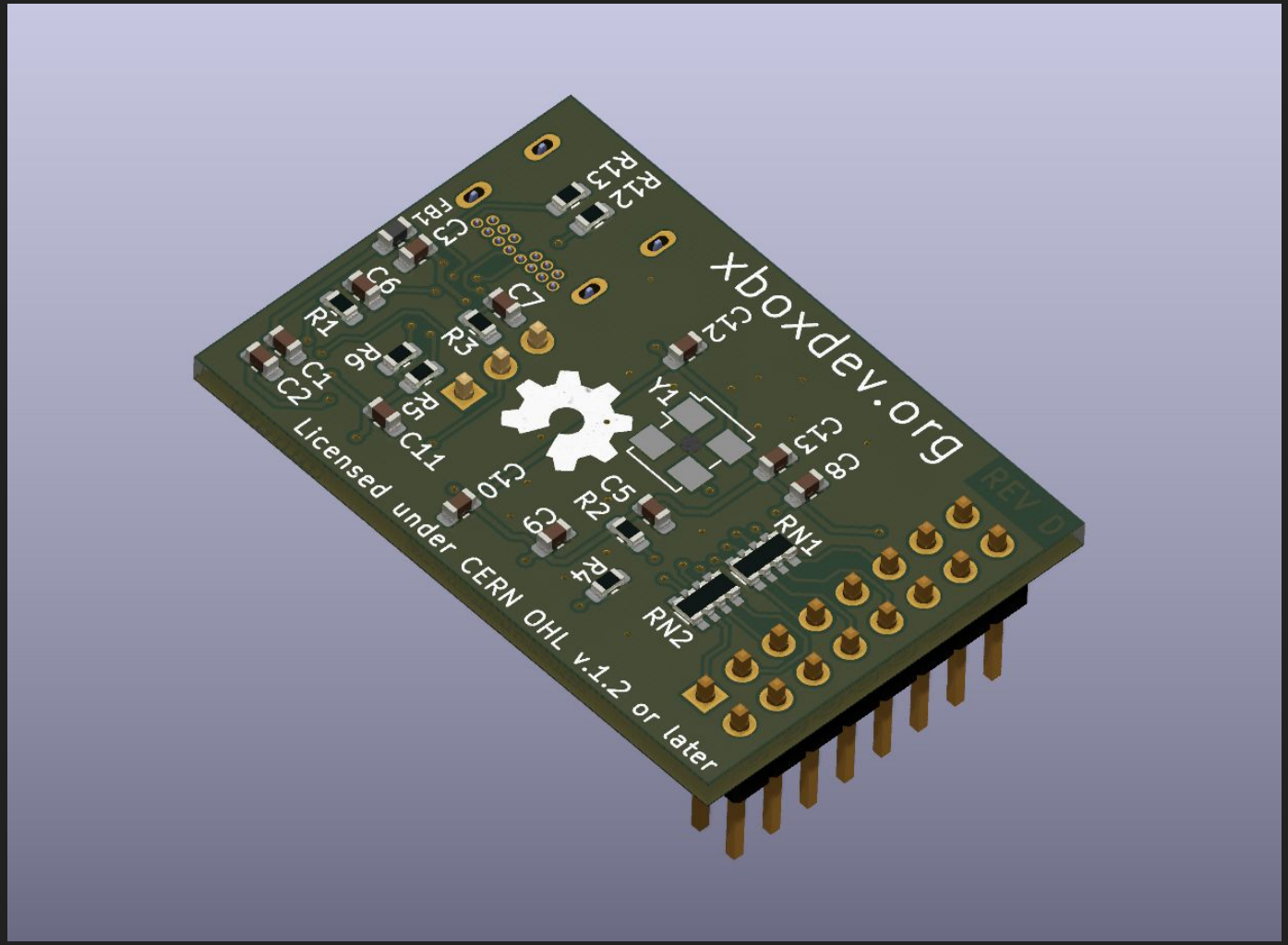
https://github.com/XboxDev/serial-usb-adapter/issues/6

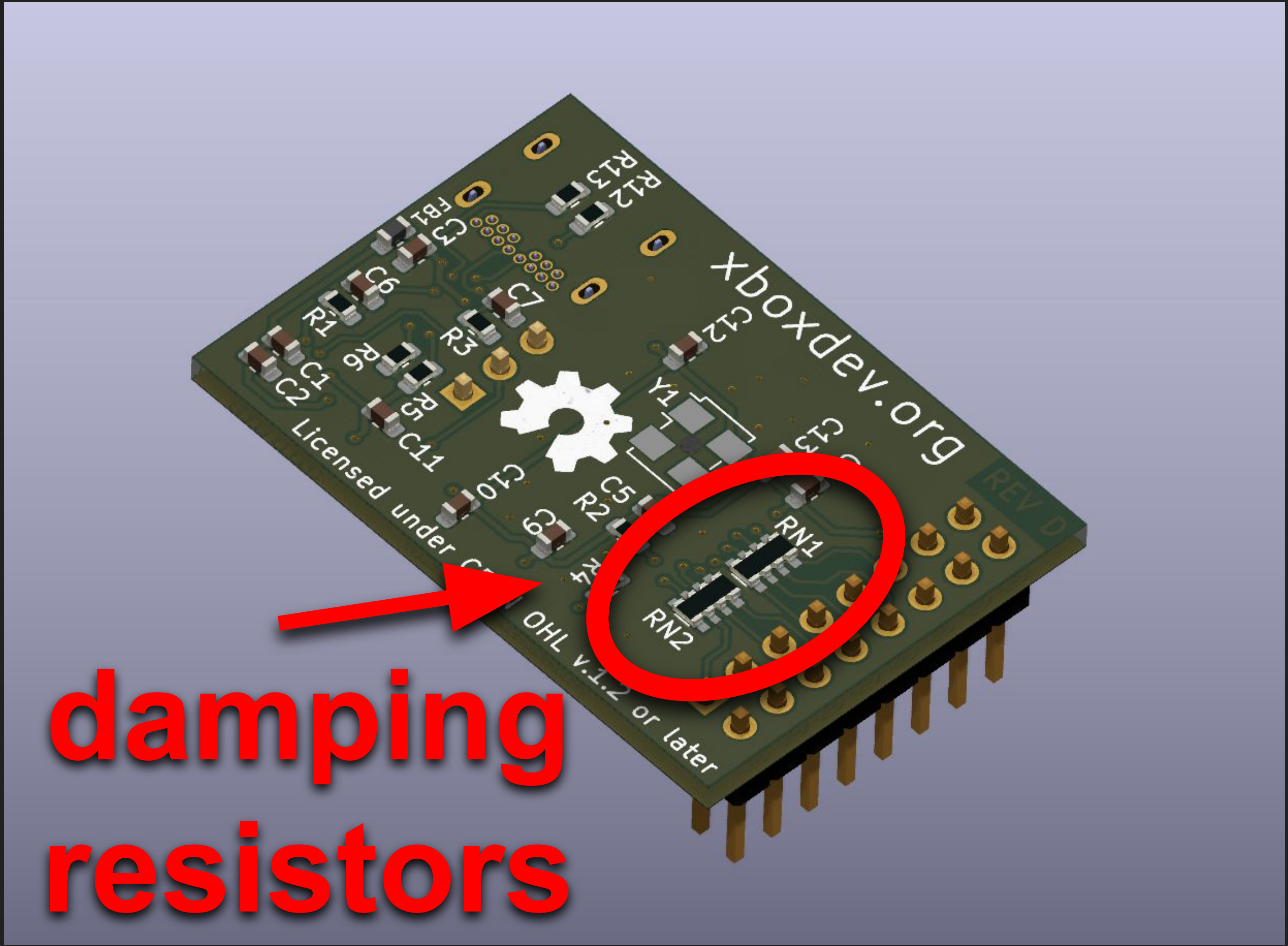

KiCad

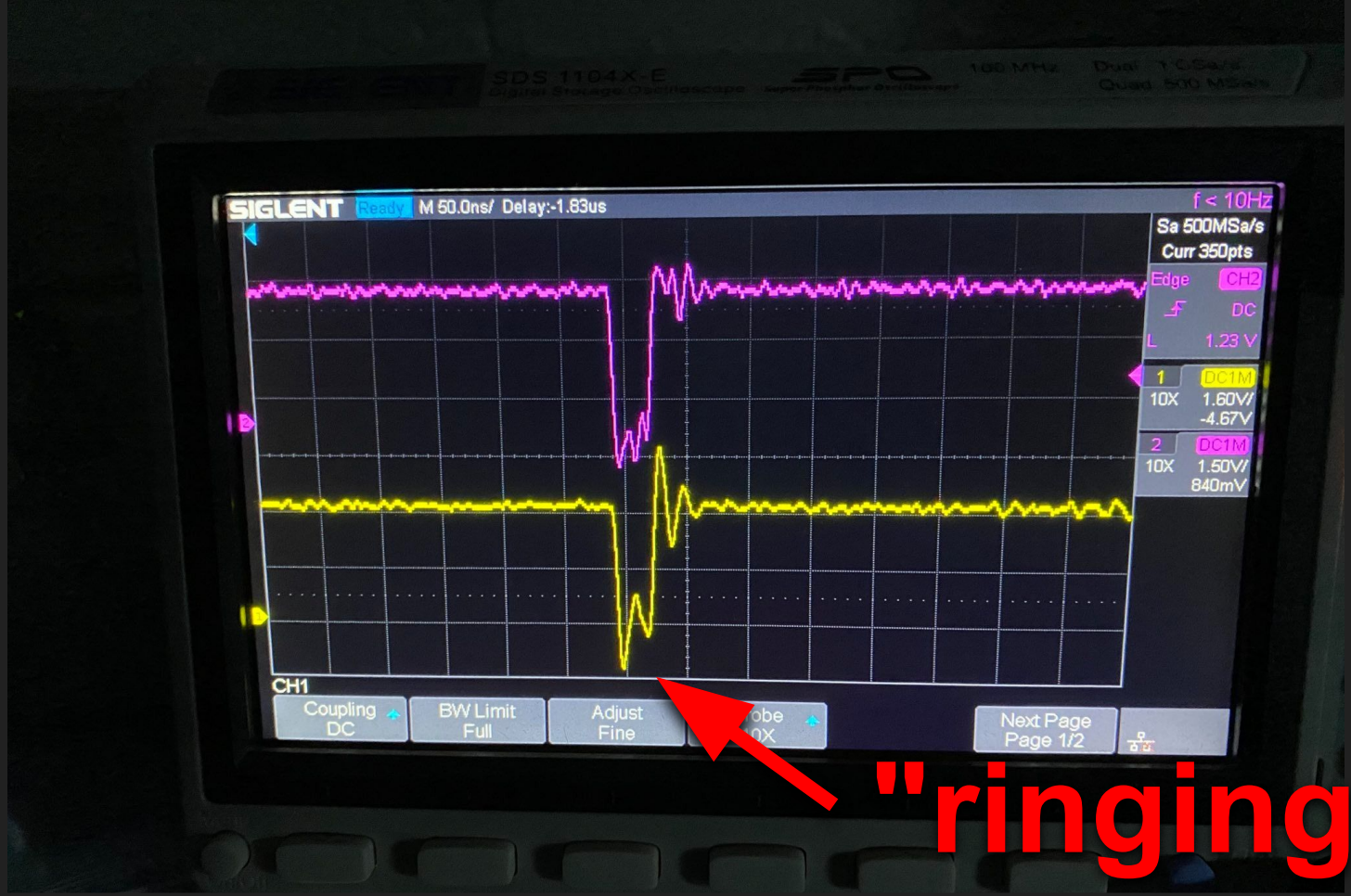

*glasgow — PCB Editor
File Edit View Place Route Inspect Tools Preferences Help
Track: use netclass width
Via: use netclass sizes
Grid: 0.0100 mm (0.39 mils)
Zoom Auto
F.Cu (PgUp)
Appearance
Layers Objects Nets
F.Cu
In1.Cu
In2.Cu
B.Cu
F.Paste
B.Paste
F.Silkscreen
B.Silkscreen
F.Mask
B.Mask
User.Drawings
User.Comments
Edge.Cuts
Margin
F.Courtyard
B.Courtyard
F.Fab
B.Fab
Layer Display Options
Inactive layers (H):
Normal Dim Hide
Flip board view
Presets (Ctrl+Tab):
Selection Filter
All items
Locked items
Footprints
Text
Tracks
Vias
Pads
Graphics
Zones
Rule Areas
Dimensions
Other items
GND
USB_C_USB2.0
Pads 1167
Vias 411
Track Segments 4737
Nets 227
Unrouted 0
Z 4.24
X 48.7600 Y 67.3200
dx 48.7600 dy 67.3200 dist 83.1235
grid X 0.0100 Y 0.0100
mm
Select item(s)


J1 USB-C SS-52400-003
VBUS
VBUS
VBUS
VBUS
SHIELD
SHIELD
SHIELD
SHIELD
GND
GND
GND
GND
A4
B4
A9
B9
A6
B6
A7
B7
A5
B5
B1
A12
B12
D1+
D2+
D1-
D2-
CC1
CC2
FB1
33ohm
U2 FT231XS
VCC
USBDP
USBDM
RESET
VCCIO
3V3OUT
GND
GND
TXD
RXD
RXLED#
TXLED#
R1 27R
R3 27R
+3V3
R5
470R
R6
1.2k
Blue
D2
D1
Green
C3
10nF
C6
47pF
C7
47pF
C11
100nF
R7
5.1k
R8
5.1k
C1
4u7
C2
100nF
UART Header
J2
Y1
SG5032CAN 14.318MHz
C13
10nF
U1 LPC47M192
CLOCKI
RXD1
TXD1
CLKI32
SYSOPT
LAD0
LAD1
LAD2
LAD3
nLFRAME
nPCI_RESET
PCI_CLK
nLPCPD
VTR
VSS
JP1 LPC
RST
LCLK
RN1 100R
RN2 100R
R4
10k
R2 10k
C5
10uF
C8
10nF
C9
10nF
C10
10nF
C12
10nF


REV D

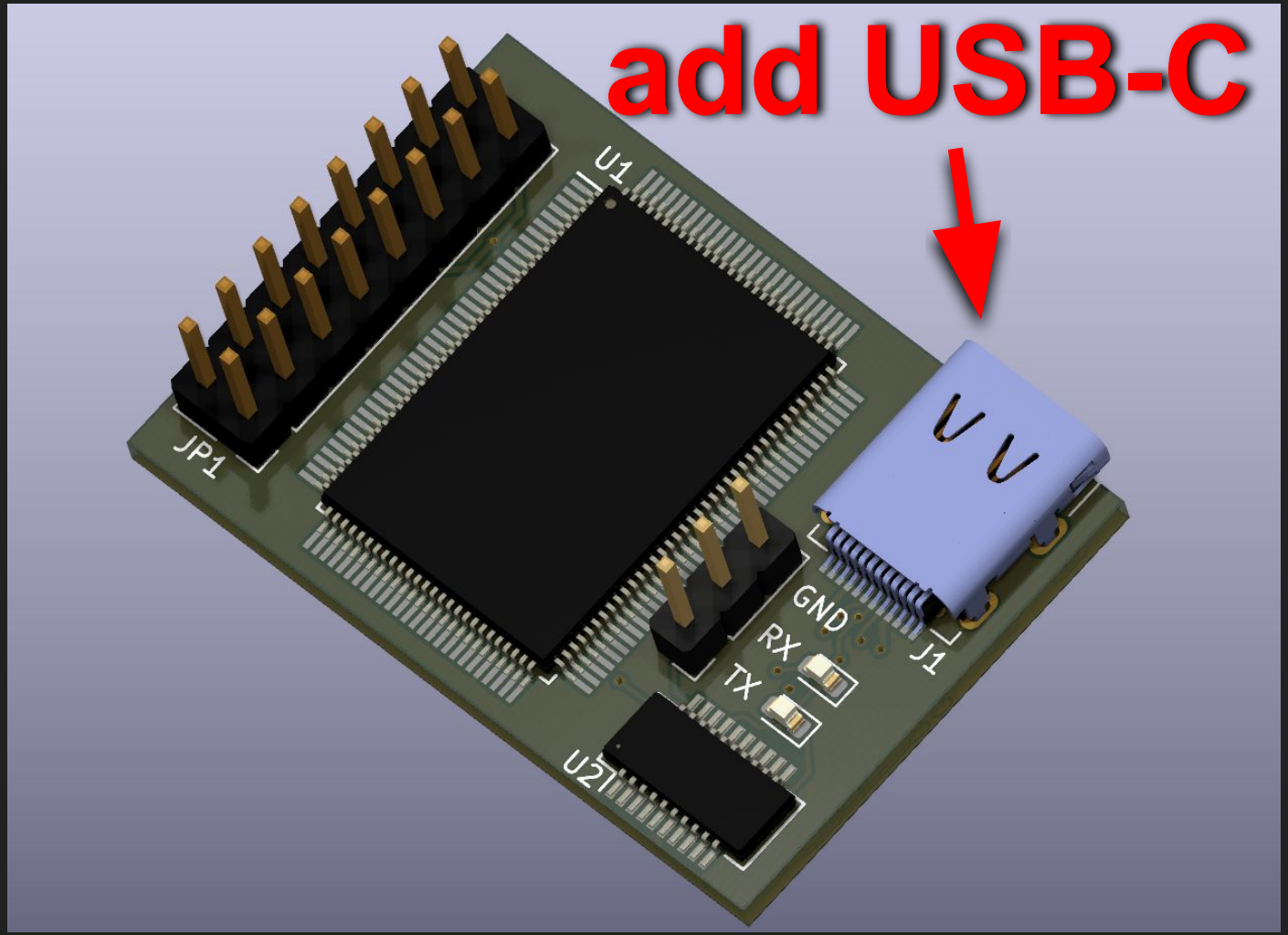

xboxdev.org
REV D
Licensed under CERN OHL v.1.2 or later
R13
R12
FB1
C3
C6
C7
R1
R3
C12
C1
R6
C2
R5
Y1
C11
C13
C8
C10
C5
R2
C9
RN1
R4
RN2

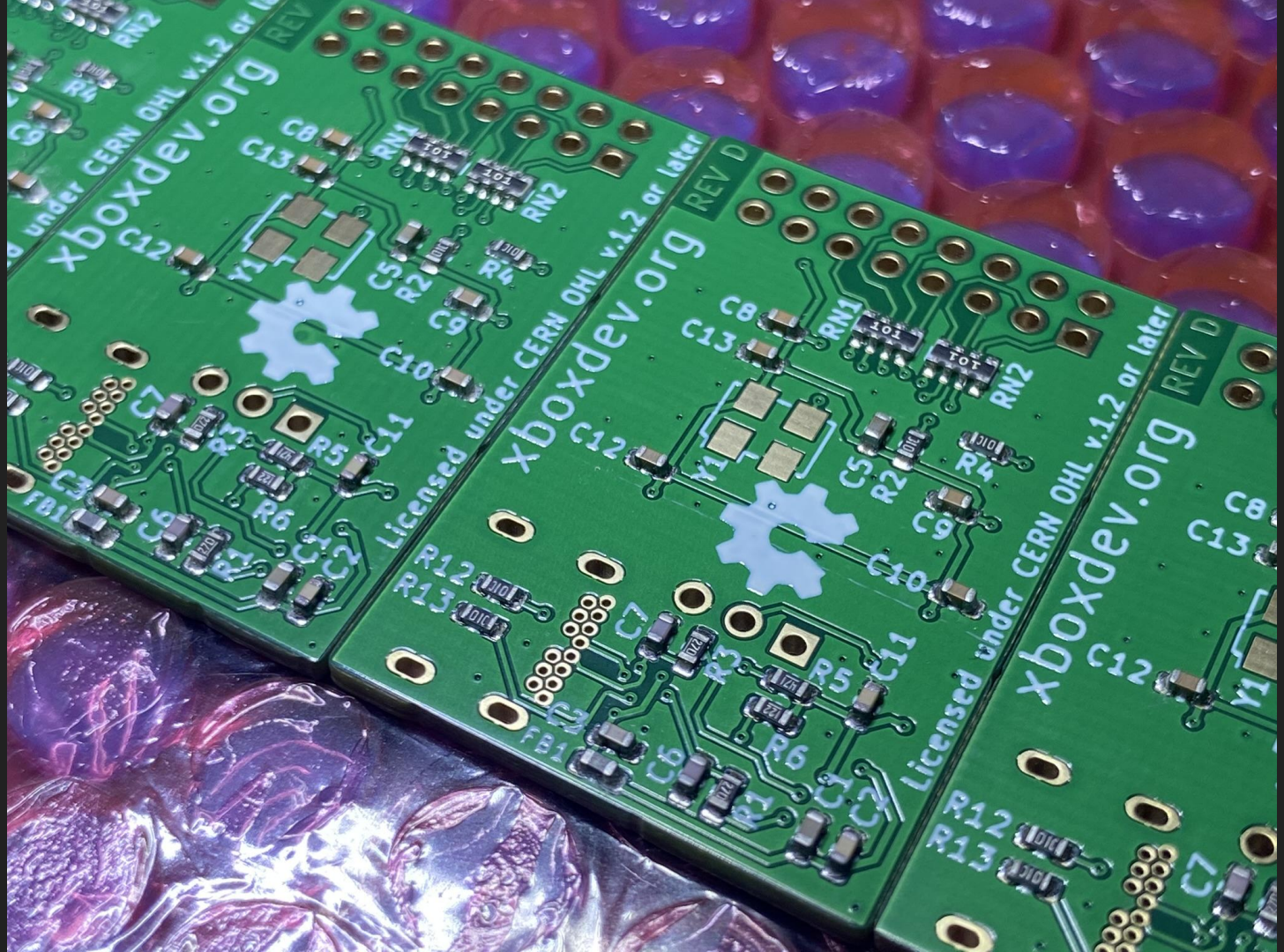

damping resistors
xboxdev.org
RN1
RN2
OHL v.1.2 or later
REV D



https://github.com/XboxDev/serial-usb-adapter/issues/6

https://github.com/XboxDev/serial-usb-adapter/issues/6


add USB-C
U1
JP1
GND
RX
TX
J1
U2


xboxdev.org
REV D
Licensed under CERN OHL v.1.2 or later
C8
C13
RN1
RN2
C12
Y1
C5
R2
R4
C9
C10
C7
R3
R5
C11
R6
C1
C2
C6
R1
FB1
R12
R13

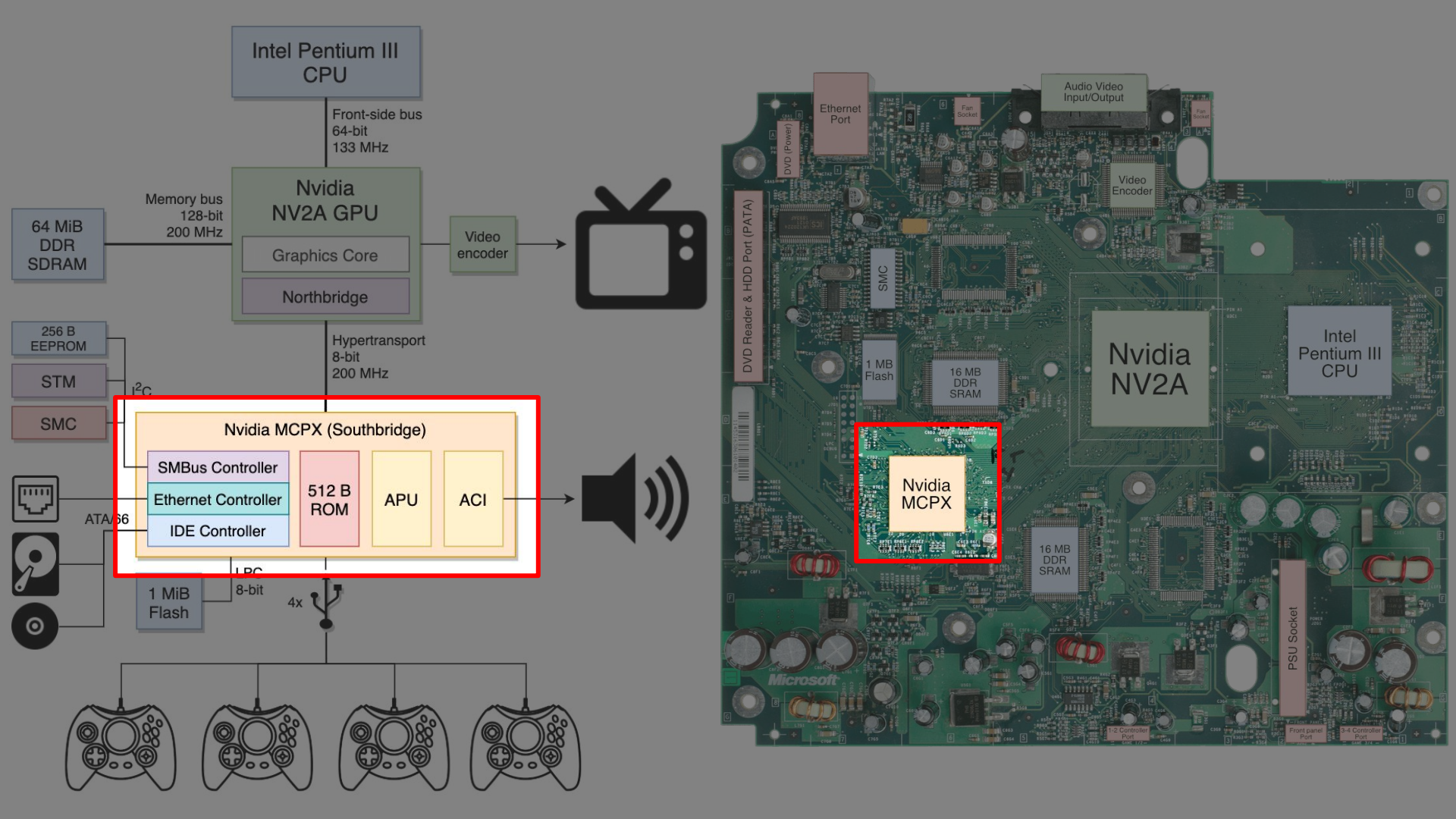

smsc
LPC47M192-NC
B0423-C8482
8H117696A
AMERICAN MEGATRENDS © 1994
ASE-TAIWAN
J1
GND
RX
TX
JP1

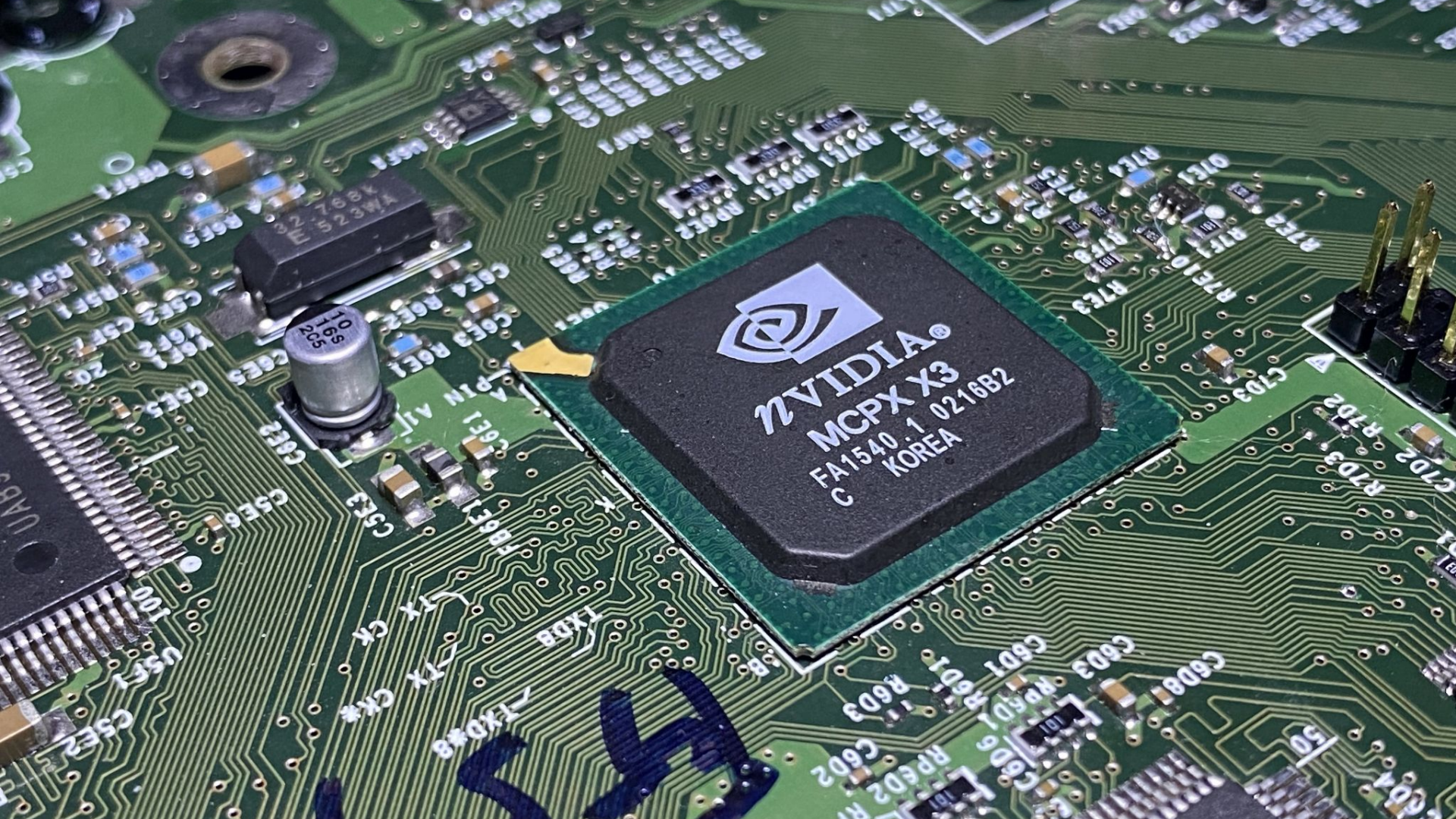

XBOX
smsc
LPC47M192-NC
B0423-C8482
8H117696A
AMERICAN MEGATRENDS ©1994
ASE-TAIWAN
GND
RX
TX
J1
U2

Basic Hardware Engineering

- **Modify an existing, open-source KiCad project**
  - Schematic Editing
  - PCB Layout Editing
  - Footprint / Symbol Editing
  - Generate Gerber files
- **Get PCBs manufactured (JLCPCB)**
  - Optionally, purchase partial PCB Assembly services
- **Experiment with Oscilloscopes and Logic Analyzers**

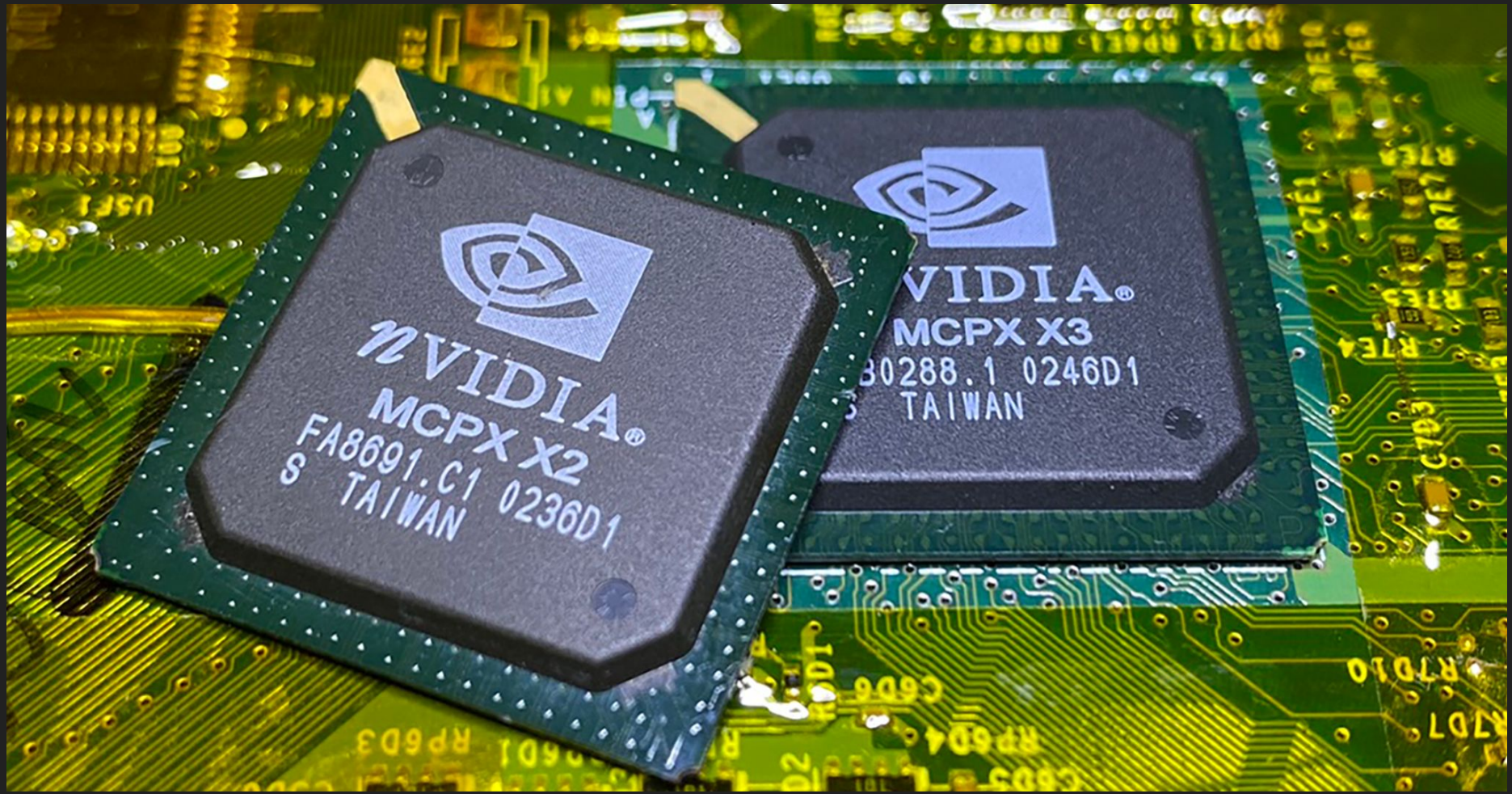
Bill Gates' Secret Bondwire


Intel Pentium III CPU
Front-side bus 64-bit 133 MHz
Memory bus 128-bit 200 MHz
64 MiB DDR SDRAM
Nvidia NV2A GPU
Graphics Core
Northbridge
Video encoder
Hypertransport 8-bit 200 MHz
256 B EEPROM
STM
SMC
I²C
Nvidia MCPX (Southbridge)
SMBus Controller
Ethernet Controller
IDE Controller
512 B ROM
APU
ACI
ATA/66
LPC 8-bit
1 MiB Flash
4x
Ethernet Port
Audio Video Input/Output
DVD (Power)
Fan Socket
Video Encoder
DVD Reader & HDD Port (PATA)
SMC
1 MB Flash
16 MB DDR SRAM
Nvidia NV2A
Intel Pentium III CPU
Nvidia MCPX
16 MB DDR SRAM
PSU Socket
Microsoft
1-2 Controller Port
Front panel Port
3-4 Controller Port


NVIDIA
MCPX X3
FA1540.1 0216B2
C KOREA

NVIDIA MCPX (Southbridge)

- **"Media Communication Processor"**
- **Handles Peripheral I/O (USB, IDE, Networking, Flash…)**
- **Contains "secret" retail bootrom (x86) fed to CPU**
  - Establishes the chain of trust


VIDIA
MCPX X2
FA8691.C1 0236D1
S TAIWAN
VIDIA
MCPX X3
80288.1 0246D1
TAIWAN


MCPX X2
MCPX X3
TAIWAN
TAIWAN


XBOX
DEBUG KIT
XBOX
DEVELOPMENT KIT
XBOX

MCP-1™

Media Communication Processor (South Bridge)

PRELIMINARY CONFIDENTIAL INFORMATION

8.0 XMode Operation

XMode is a Microsoft specific feature that can only be enabled via internal bond pads.

8.1 Bonding Options

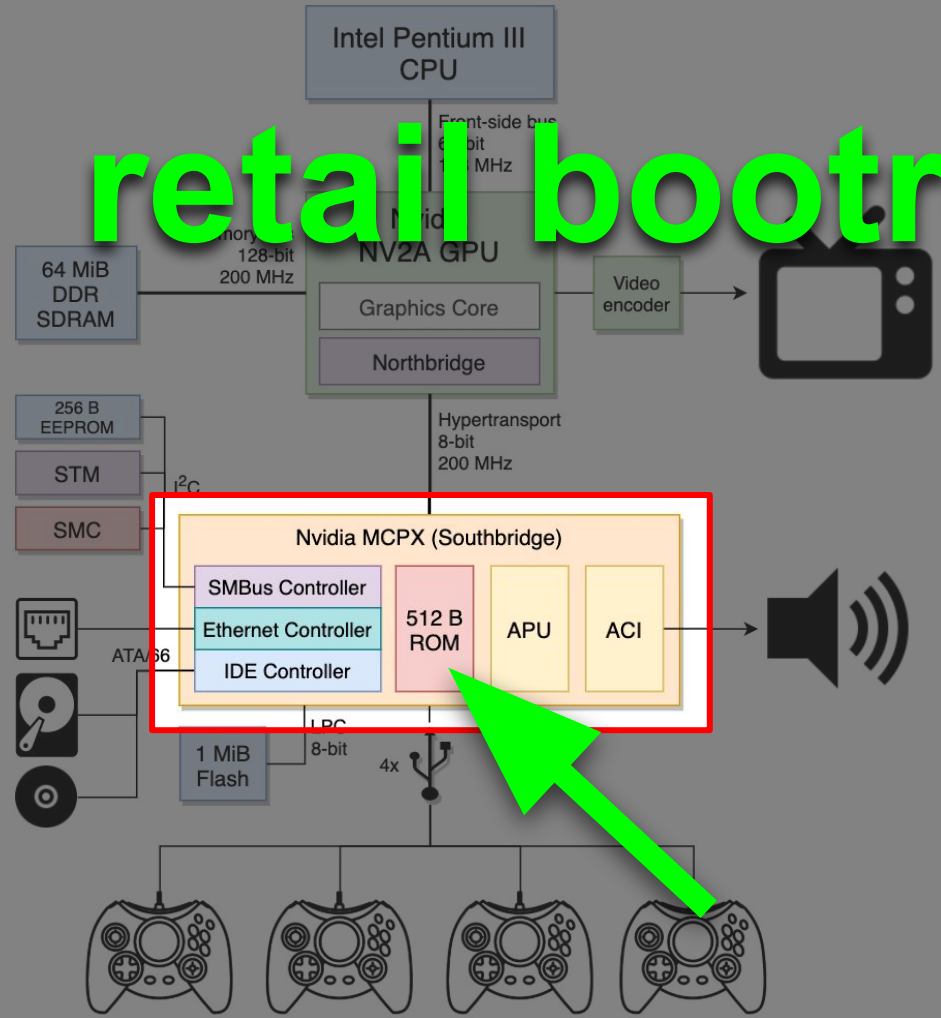
MCP1 uses the following Bonding Options:

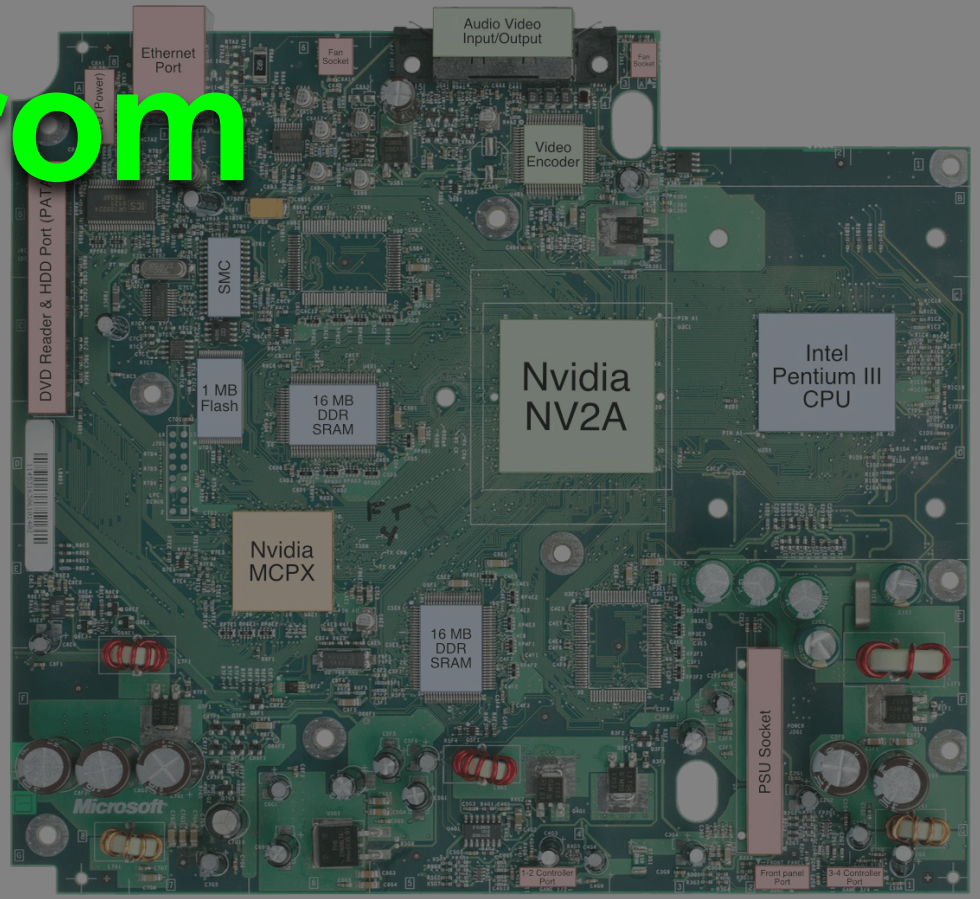
Pin Strap	Function	Bonded Value
XBox Mode[1:0]	XBox Functionality	00 – PC-Mode
		01 – X-Mode; PCI Bus; Internal ROM Disabled
	XM2	10 – X-Mode; ROM Bus; Internal ROM Disabled;
	XM3	11 – X-Mode; ROM Bus; Internal ROM Enabled;

The bond pads are powered off of the VDD3 ring.

Note: Xbox Mode[0] is available as a pin during the prototyping stage.

retail bootrom





8.0 XMode Operation

XMode is a Microsoft specific feature that can only be enabled via internal bond pads.

8.1 Bonding Options

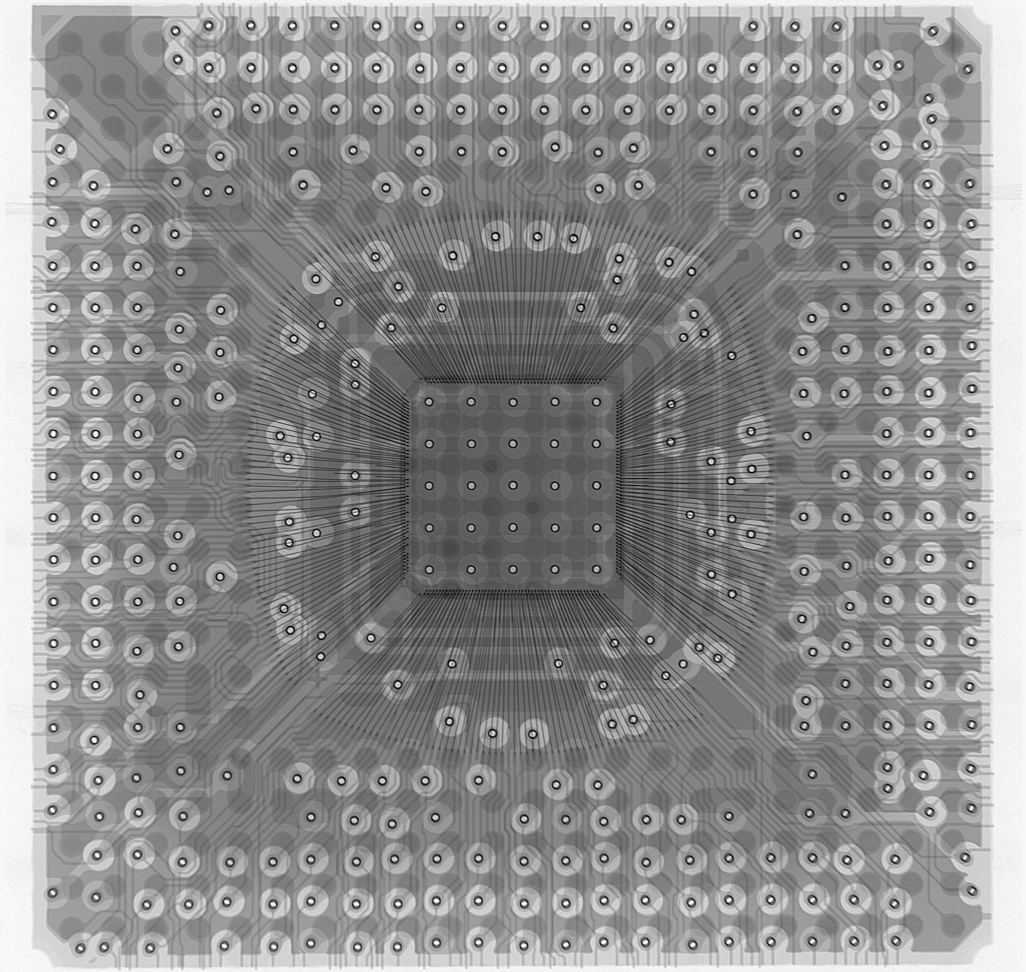
MCP1 uses the following Bonding Options:

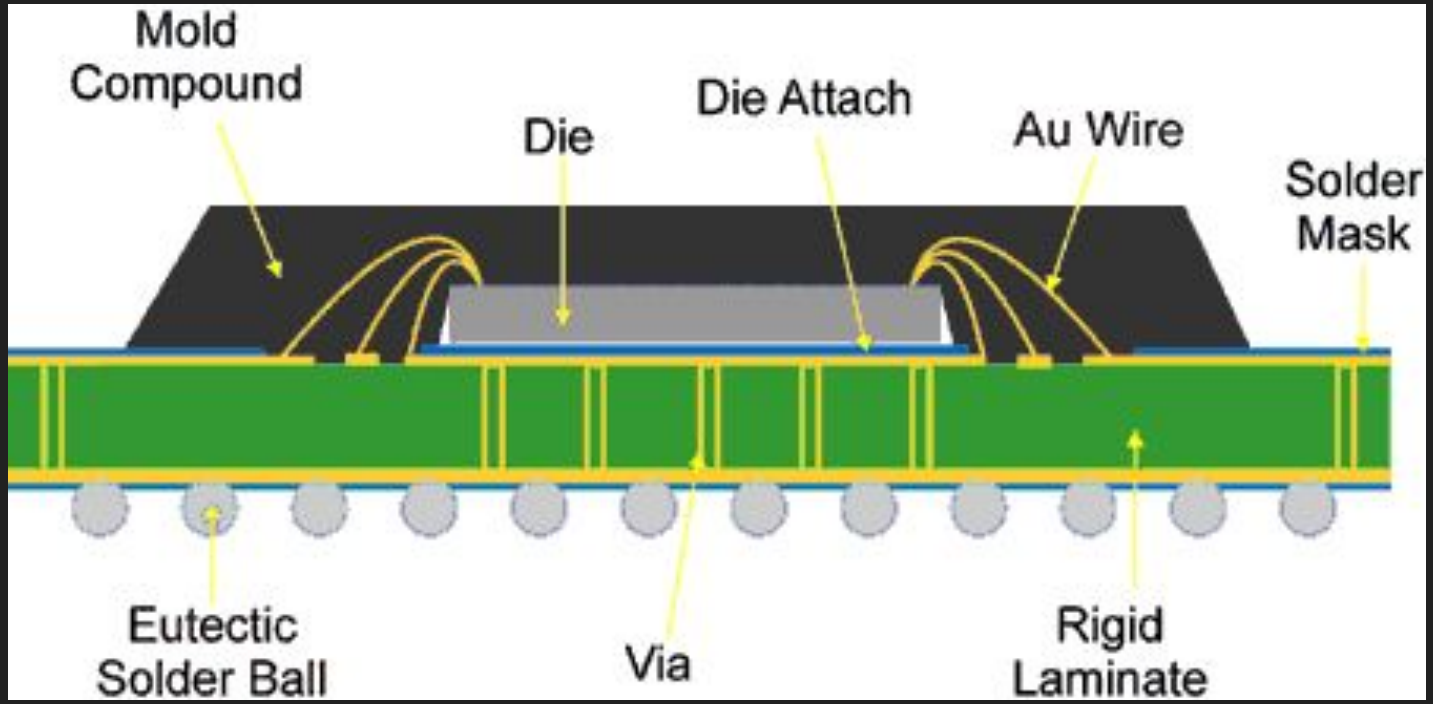
Pin Strap	Function	Bonded Value
XBox Mode[1:0]	XBox Functionality	00 – PC-Mode
		01 – X-Mode; PCI Bus; Internal ROM Disabled
	XM2	10 – X-Mode; ROM Bus; Internal ROM Disabled;
	XM3	11 – X-Mode; ROM Bus; Internal ROM Enabled;

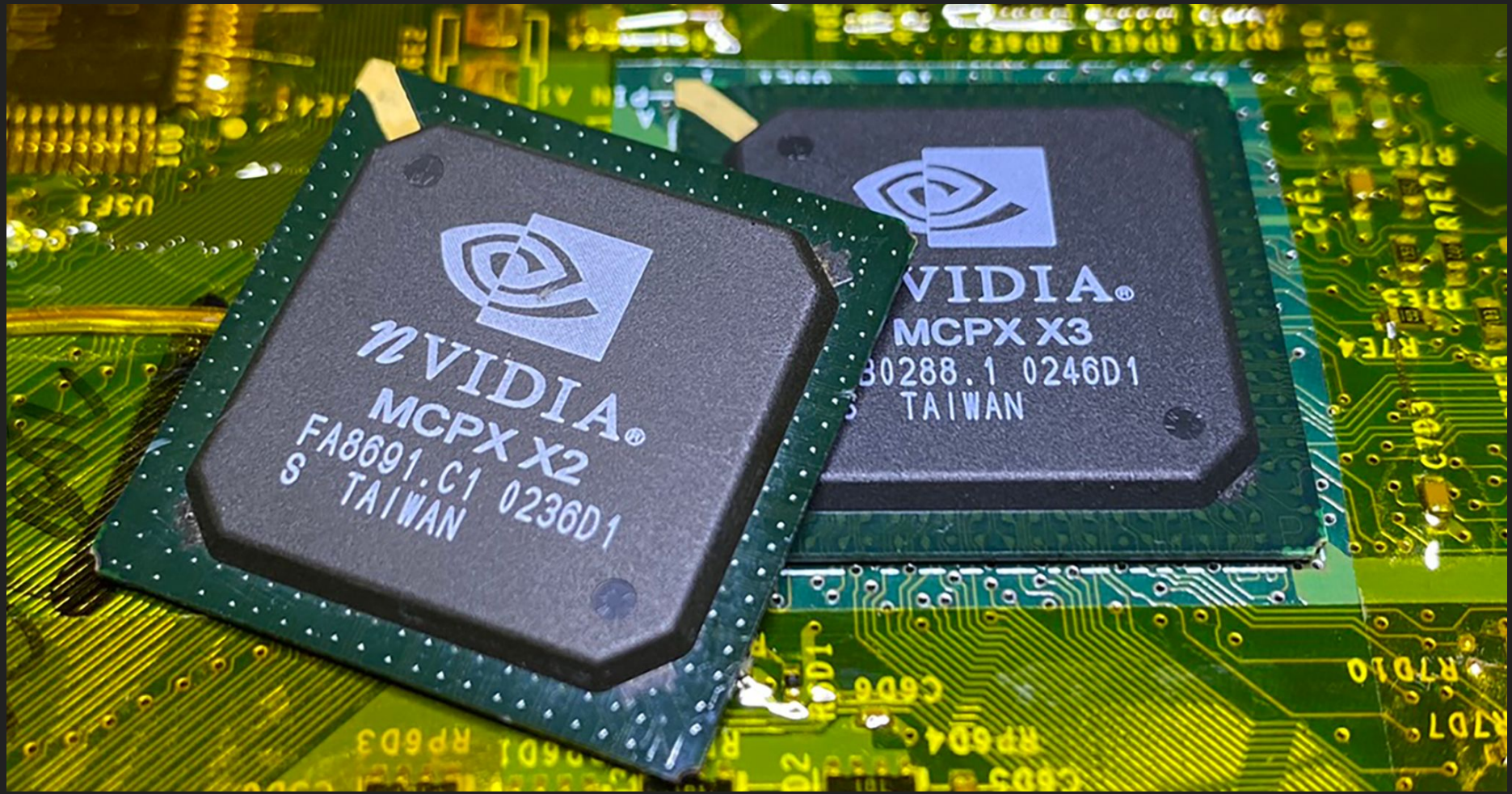
The bond pads are powered off of the VDD3 ring.

Note: Xbox Mode[0] is available as a pin during the prototyping stage.

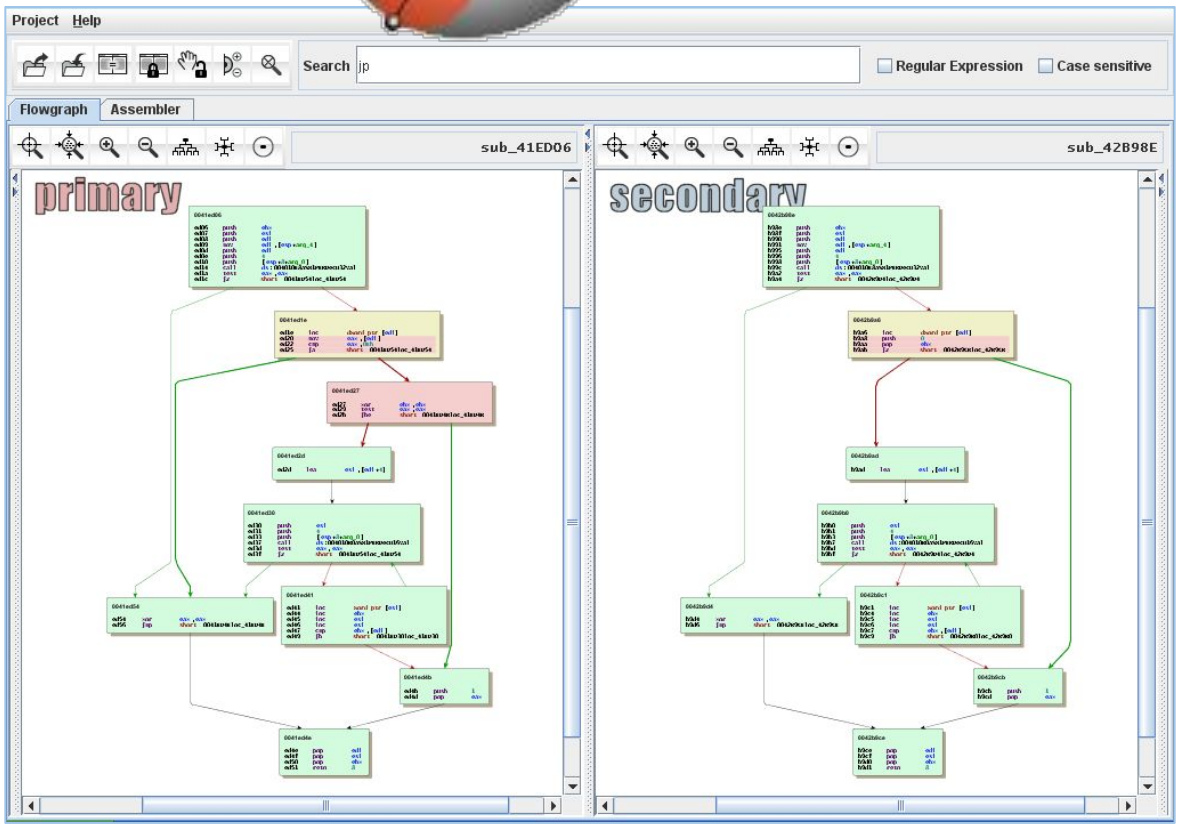

nVIDIA®
MCPX X3
FH6396.1 0513D3
C KOREA

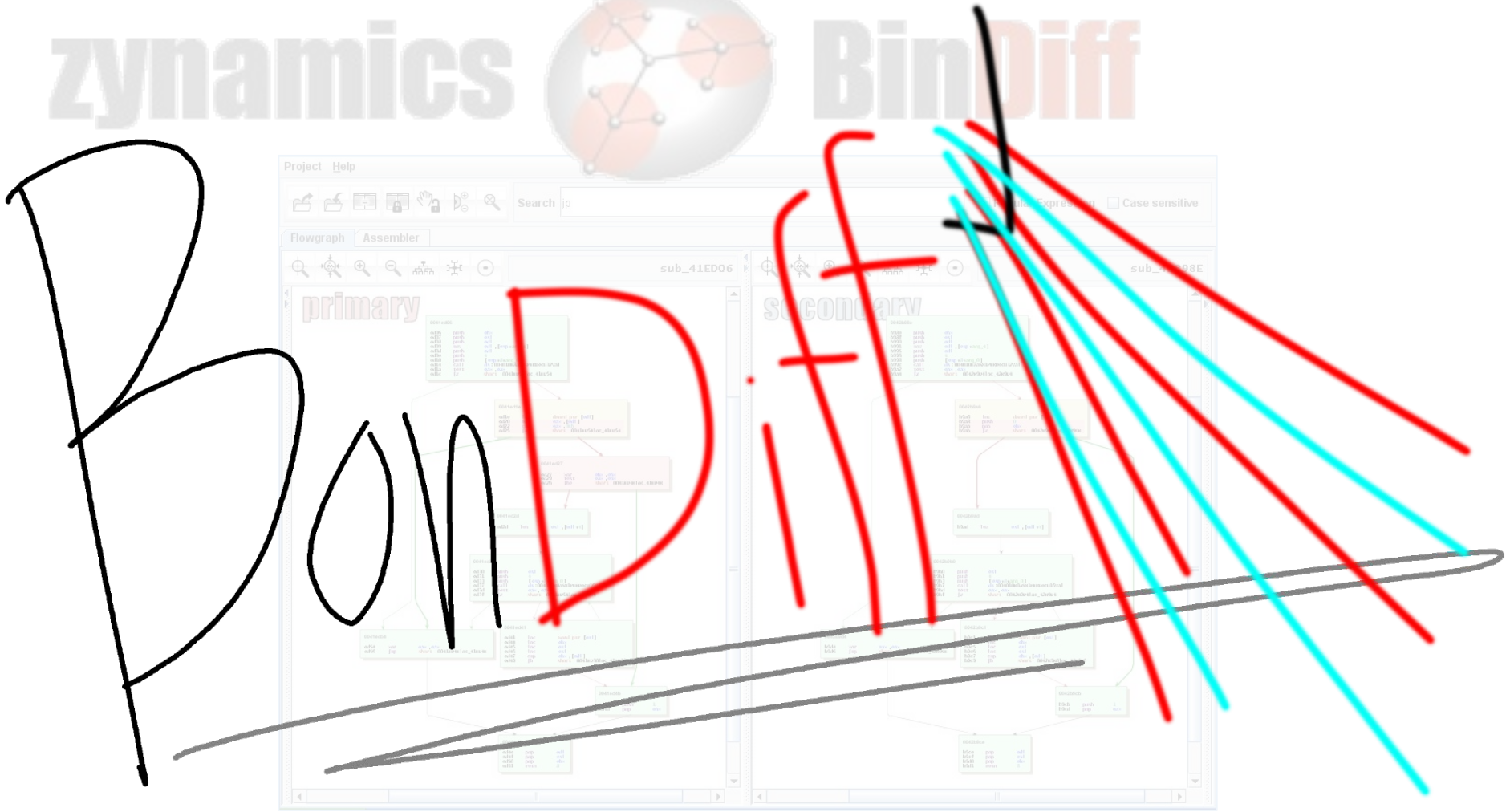


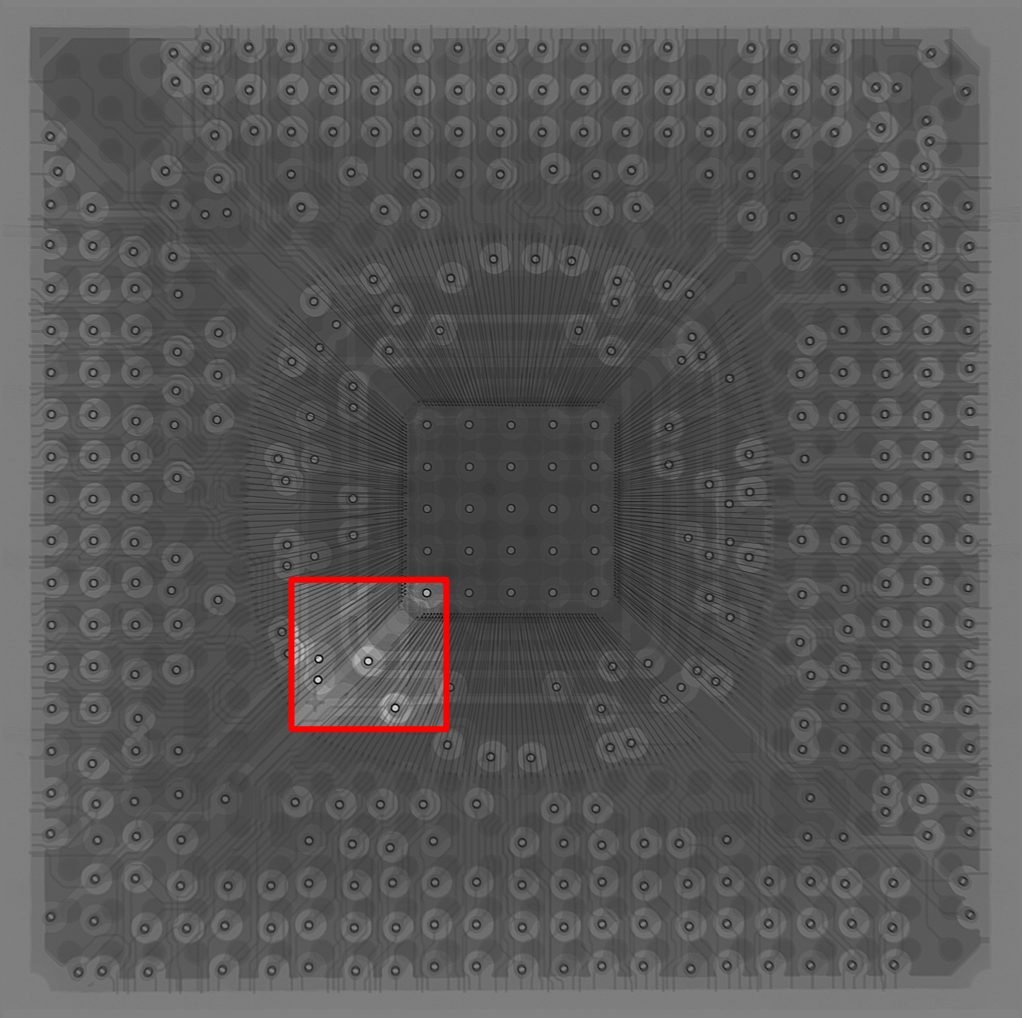

Mold
Compound
Die
Die Attach
Au Wire
Solder
Mask
Eutectic
Solder Ball
Via
Rigid
Laminate

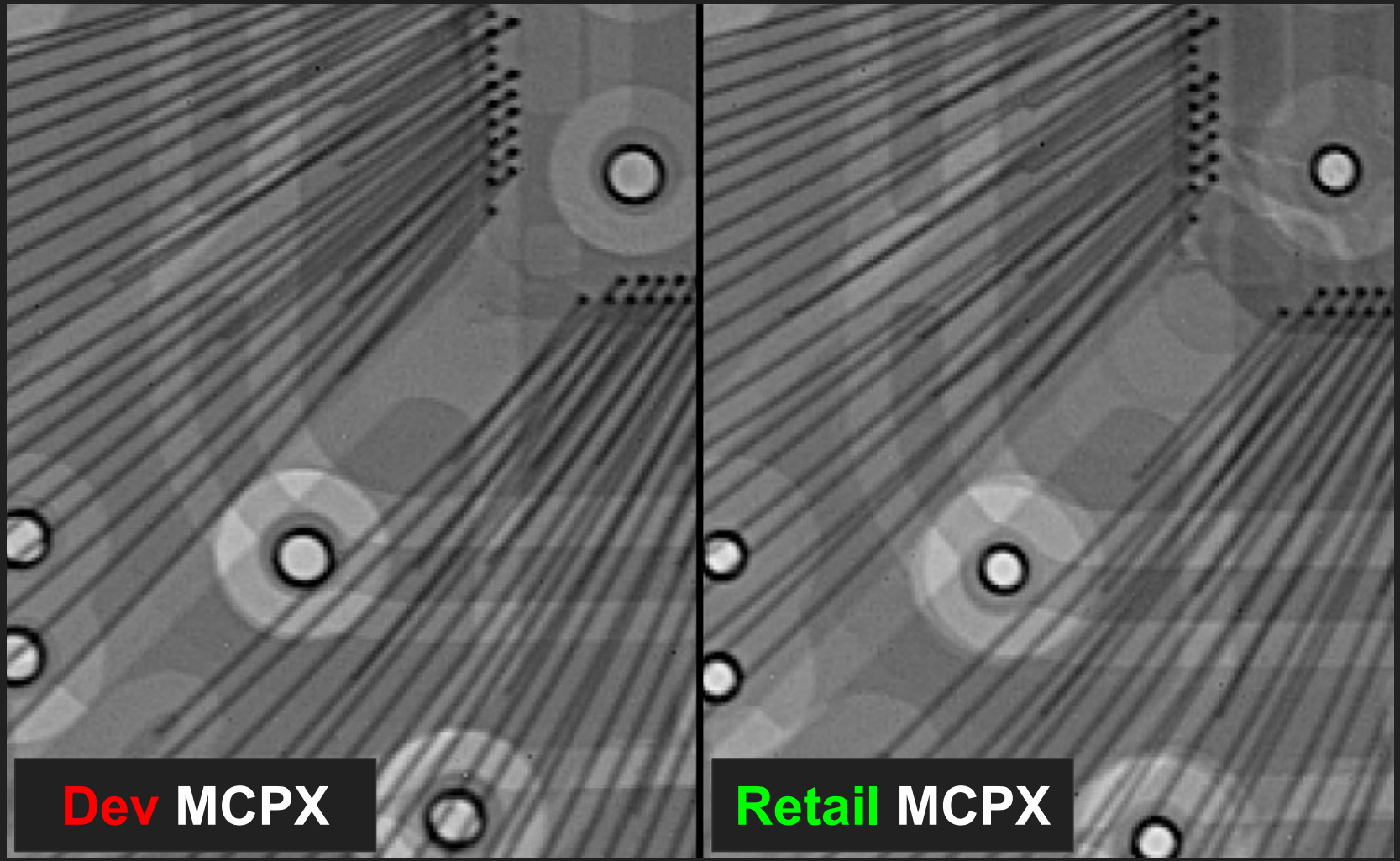

VIDIA
MCPX X2
FA8691.C1 0236D1
S TAIWAN
VIDIA
MCPX X3
80288.1 0246D1
TAIWAN

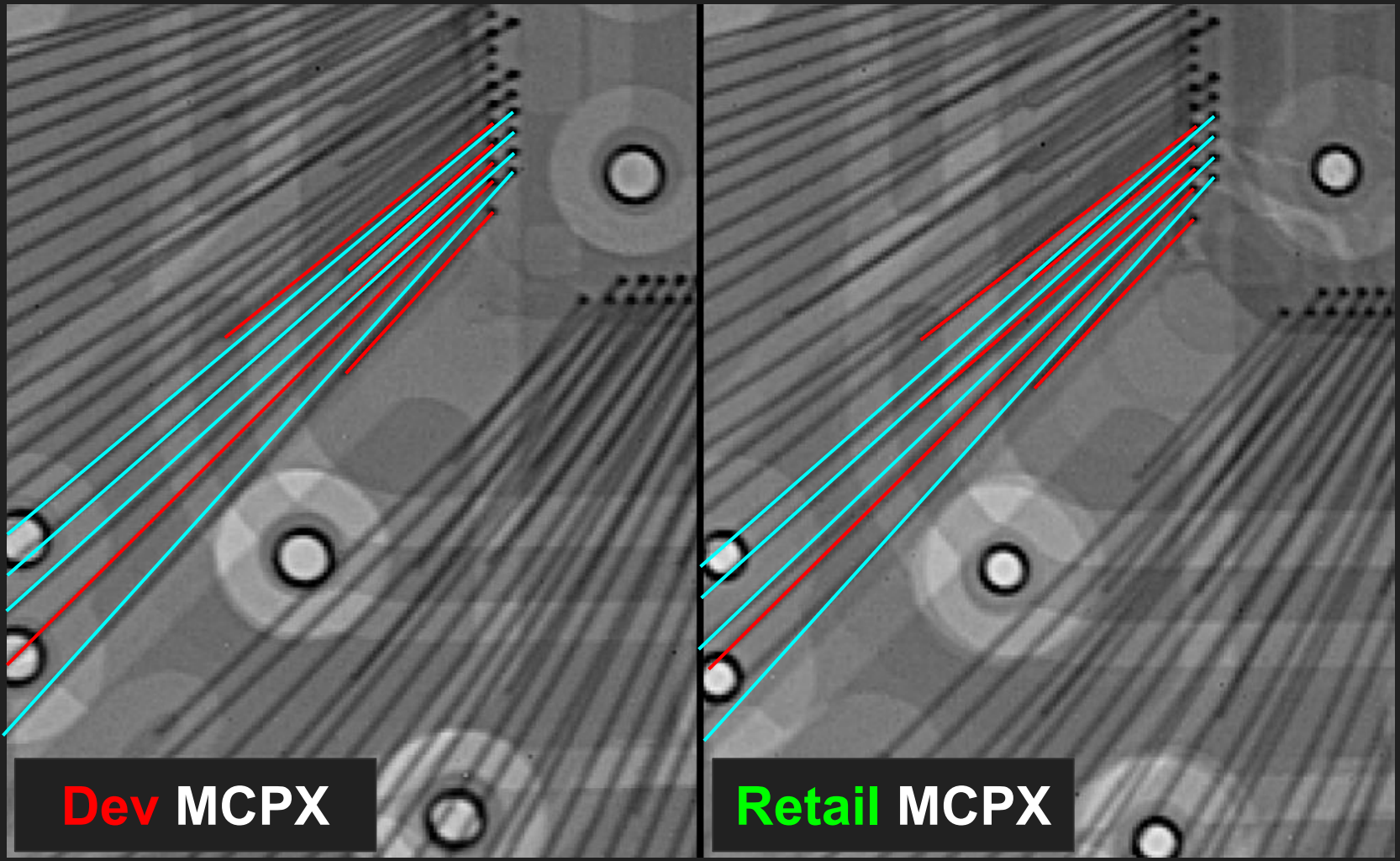
zynamics BinDiff

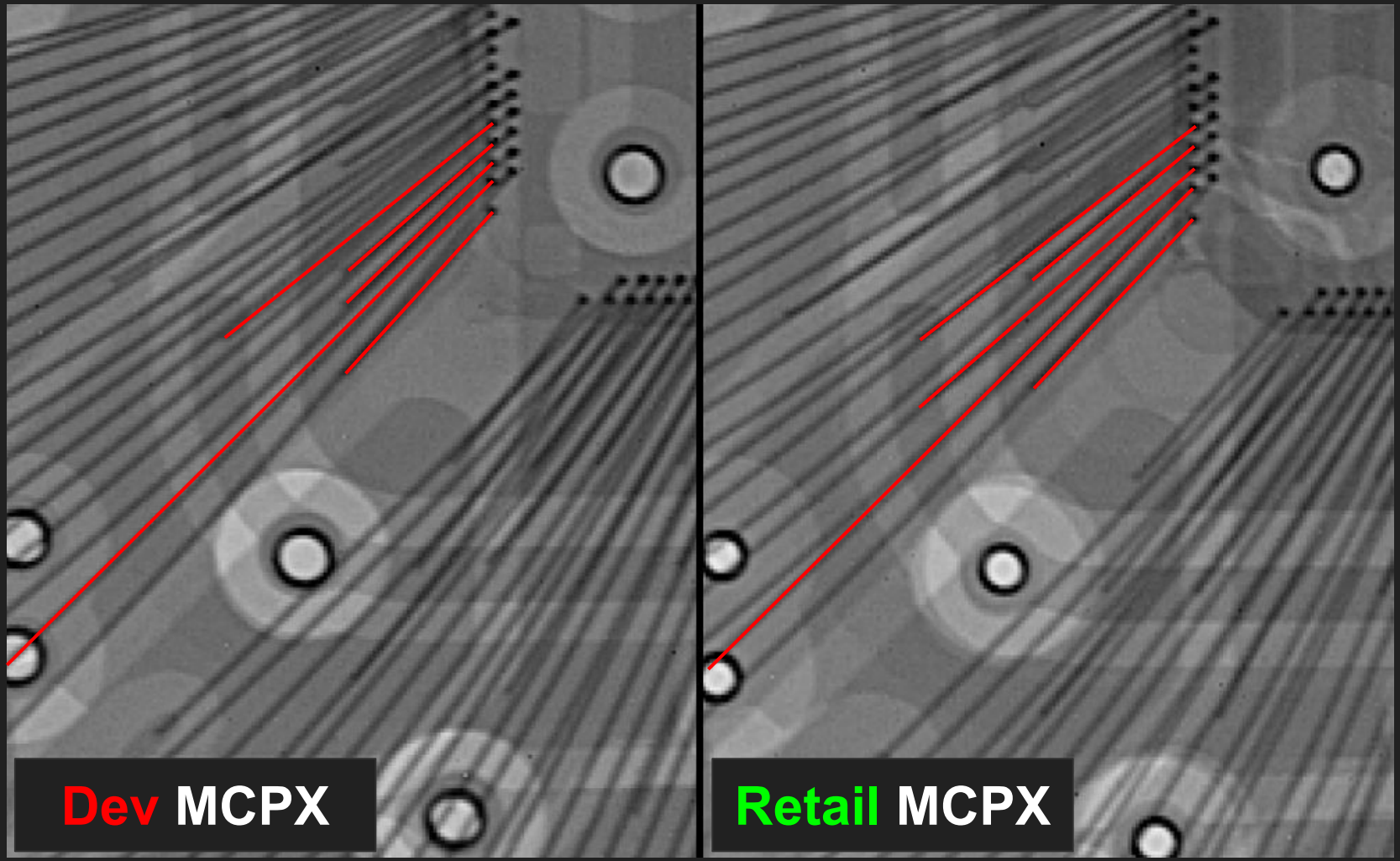


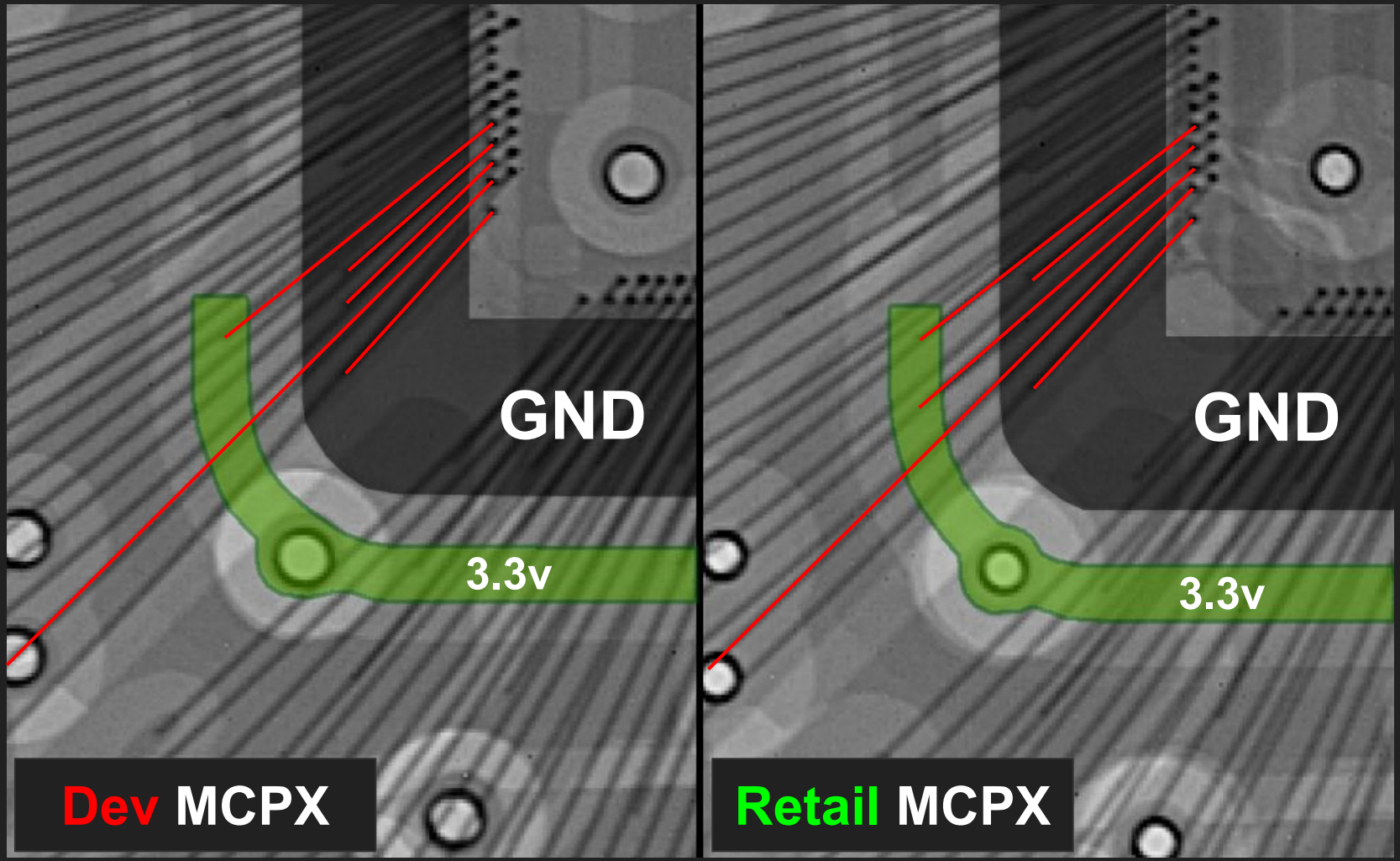

zynamics BinDiff
BinDiff
Project Help
Search
Case sensitive
Flowgraph
Assembler
primary
secondary

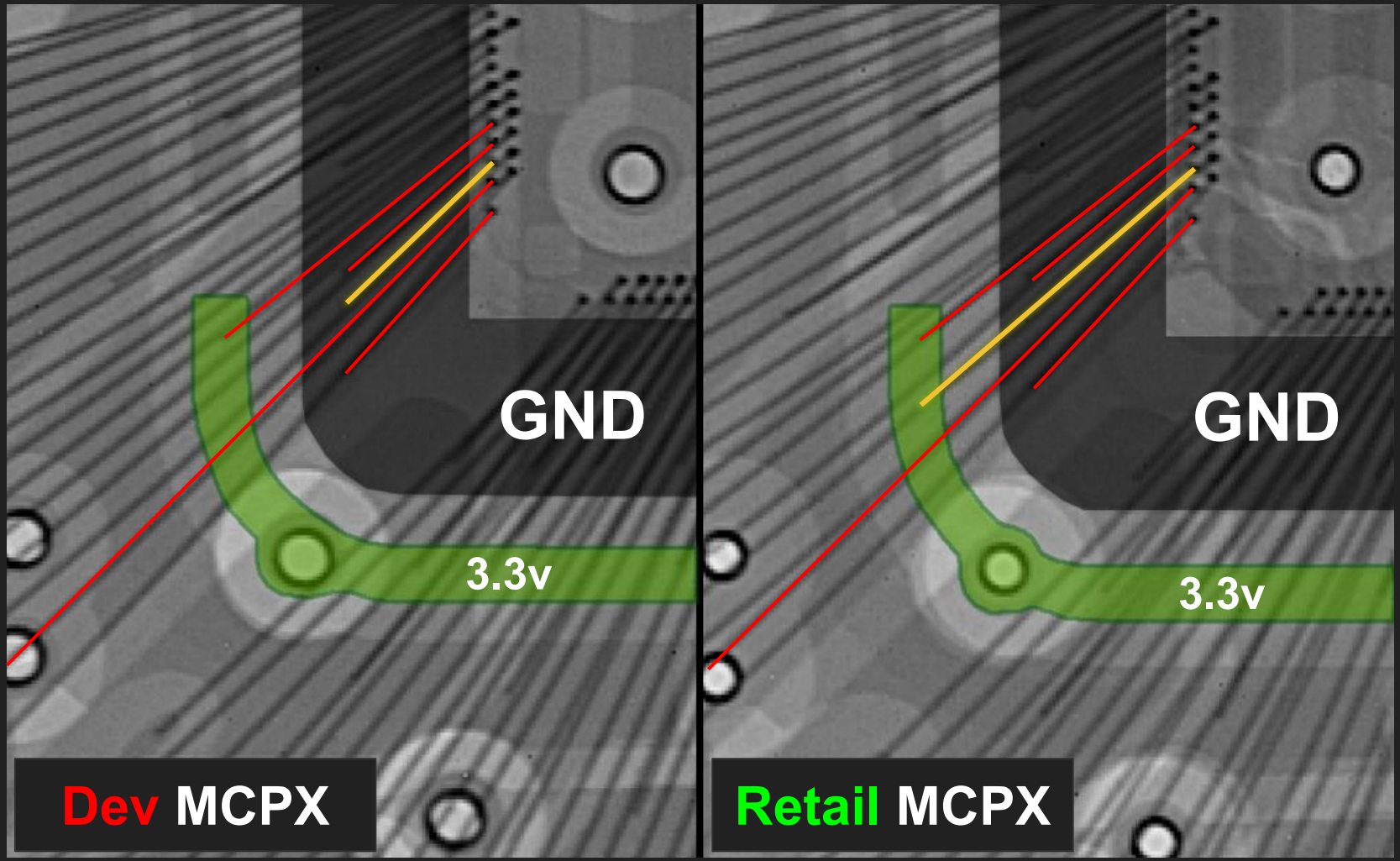


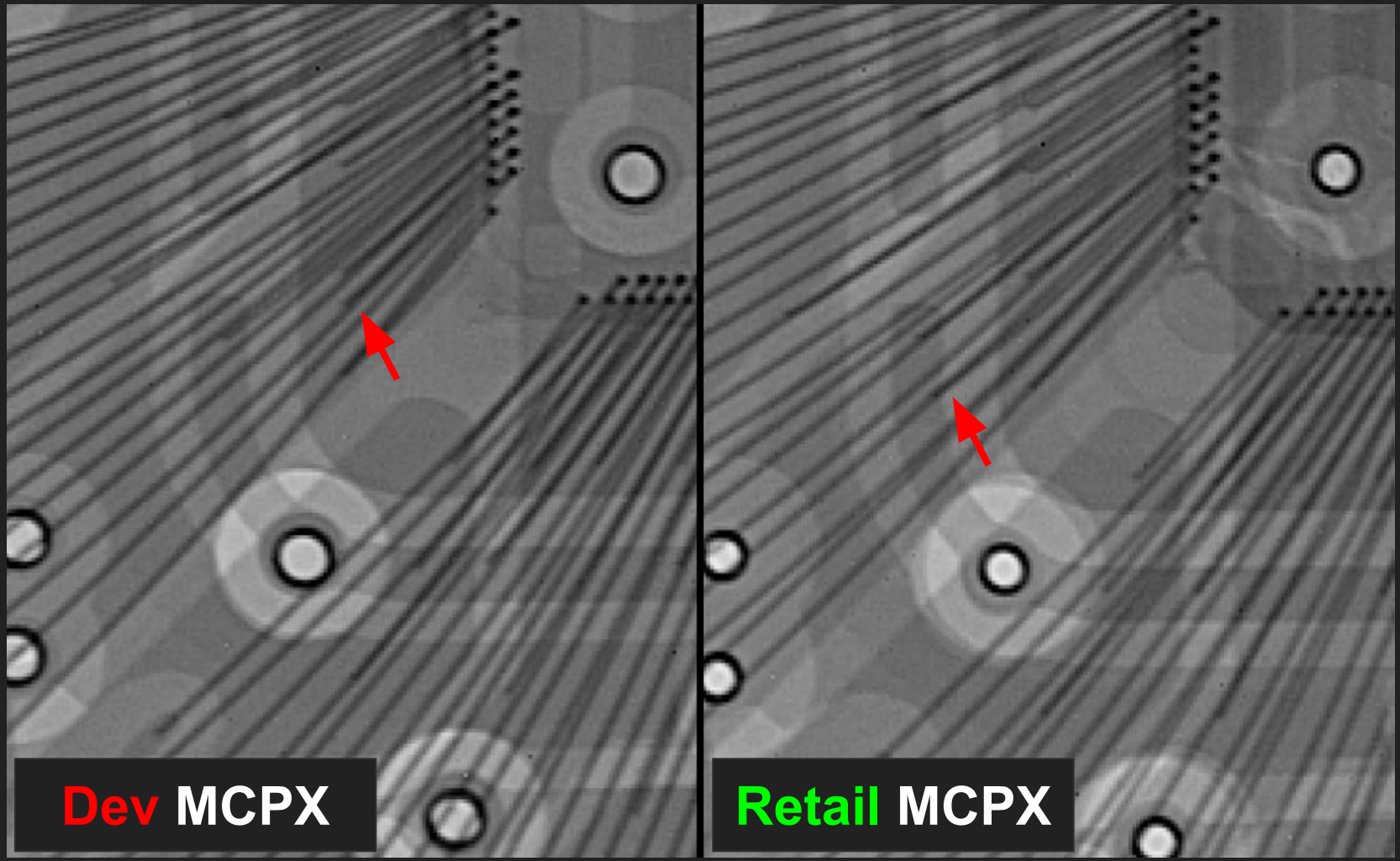

Dev MCPX
Retail MCPX


Dev MCPX
Retail MCPX

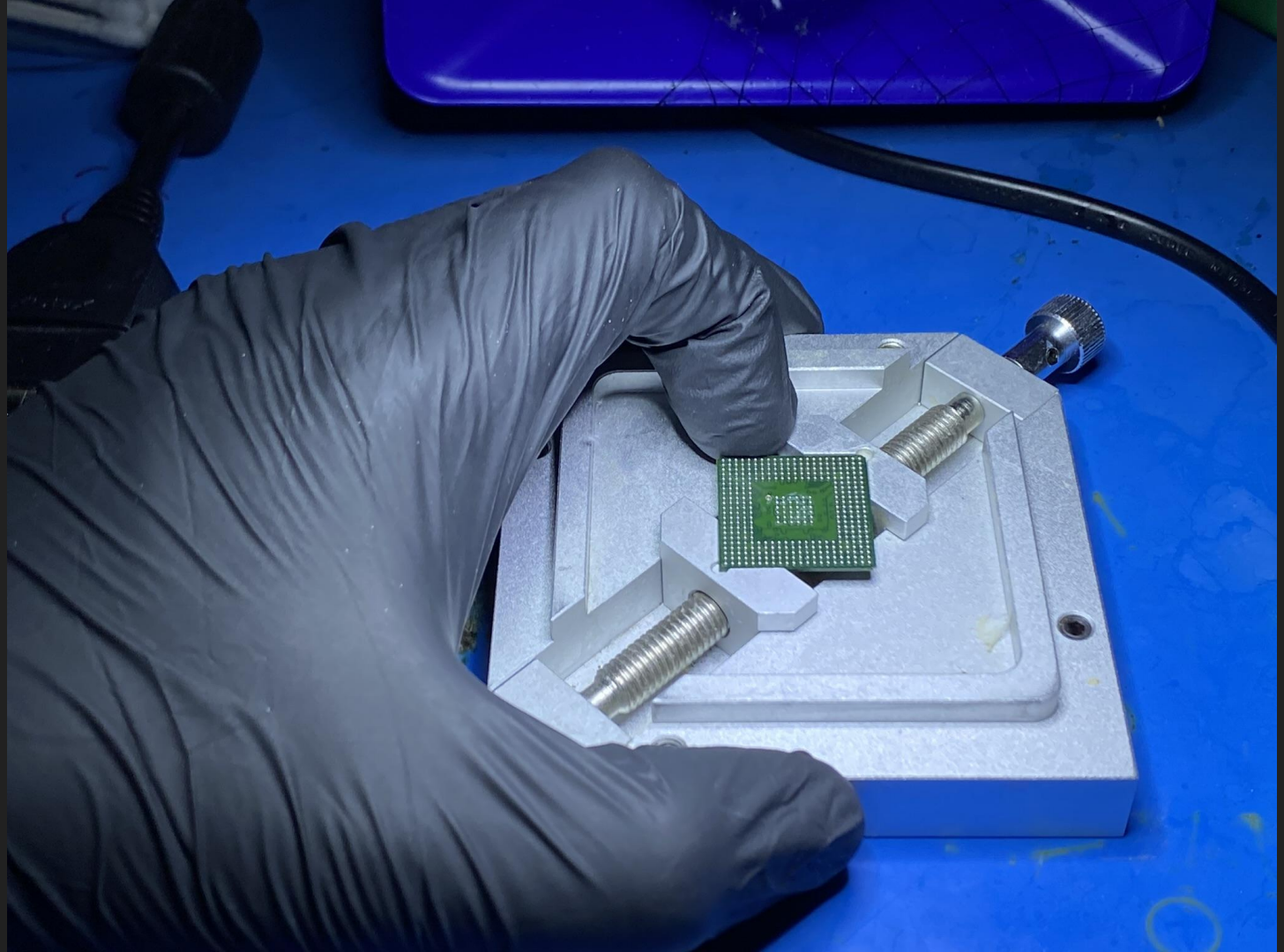

Dev MCPX
Retail MCPX

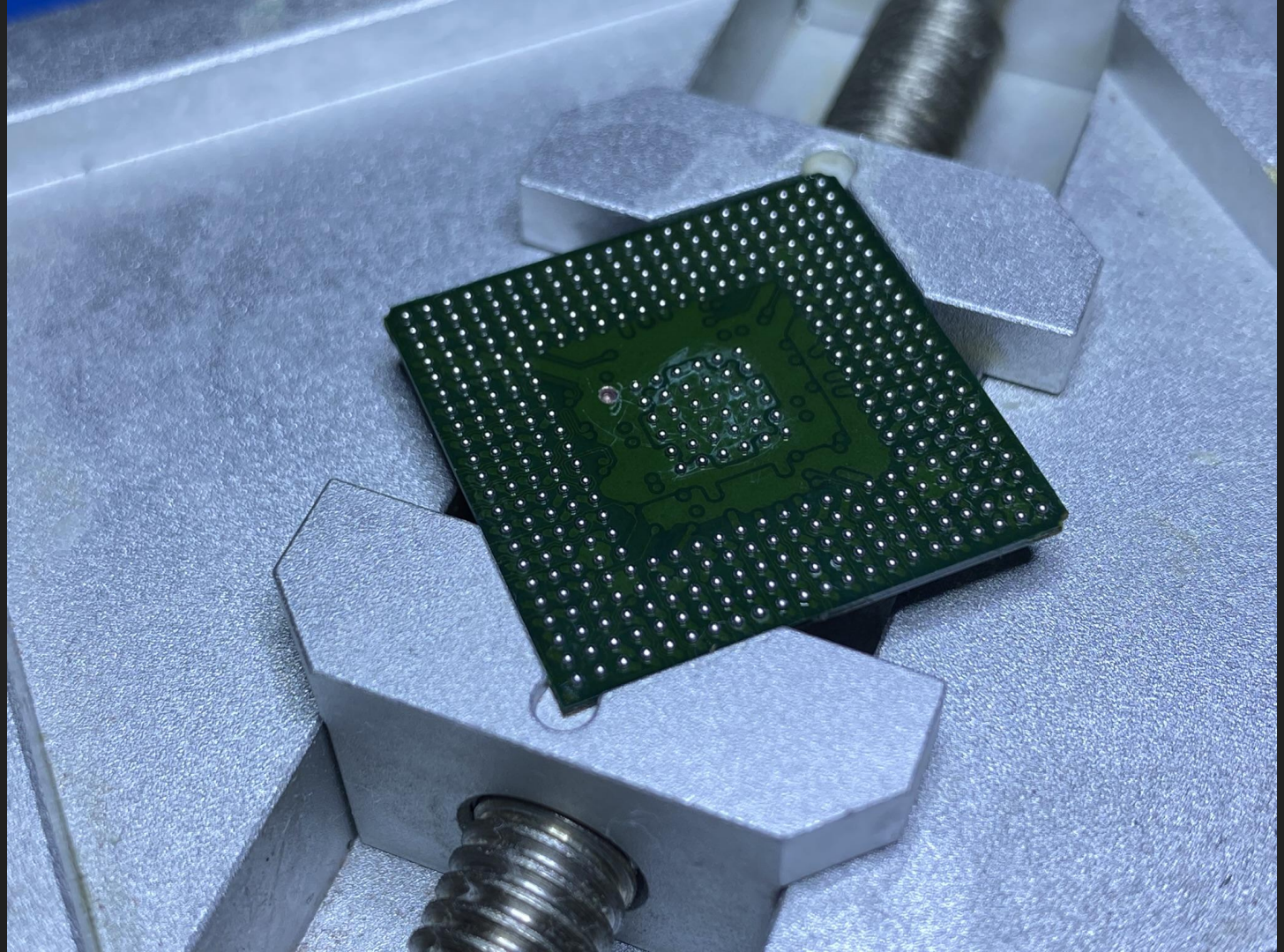

GND
3.3v
Dev MCPX
GND
3.3v
Retail MCPX

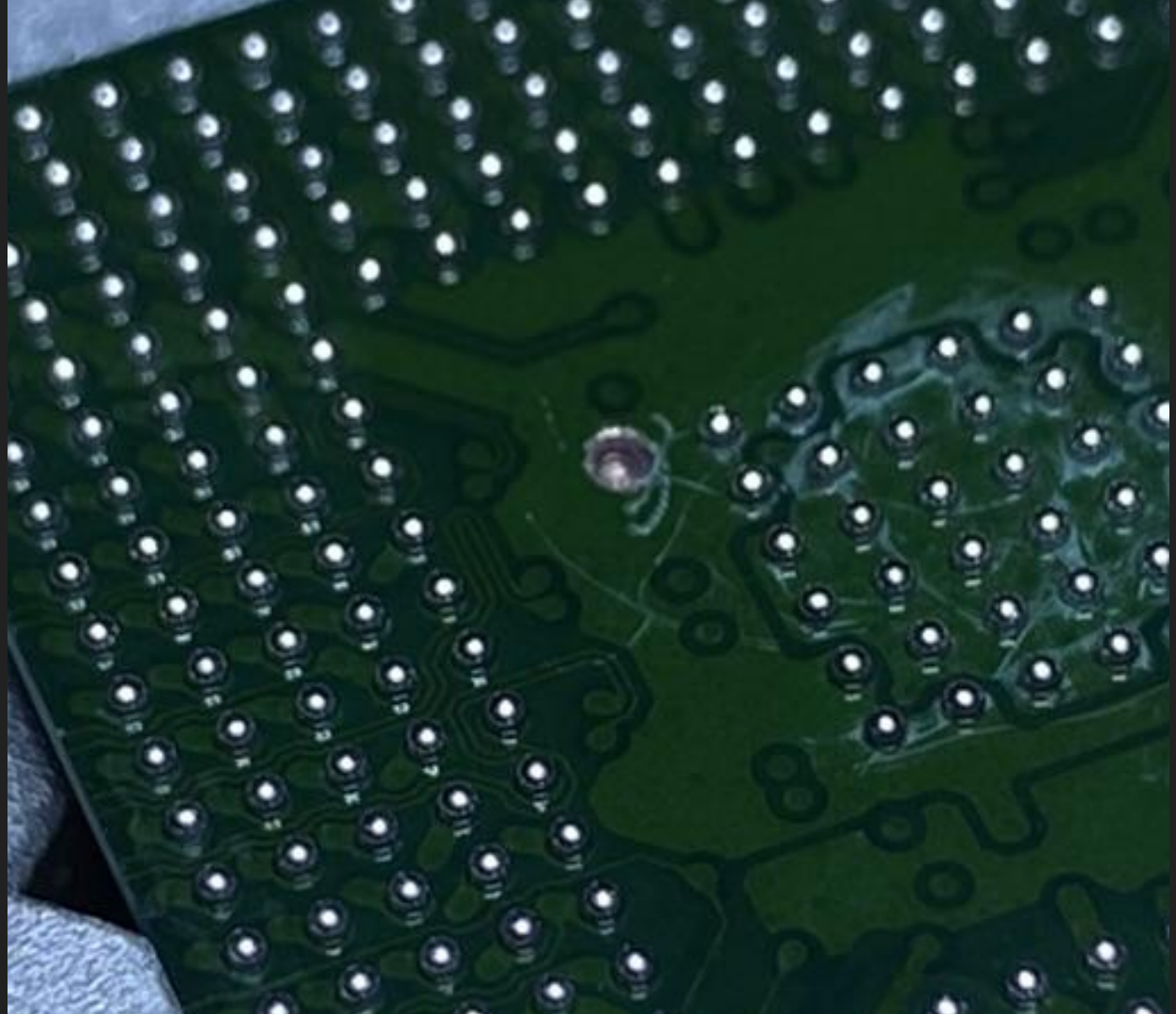

GND
3.3v
Dev MCPX
GND
3.3v
Retail MCPX

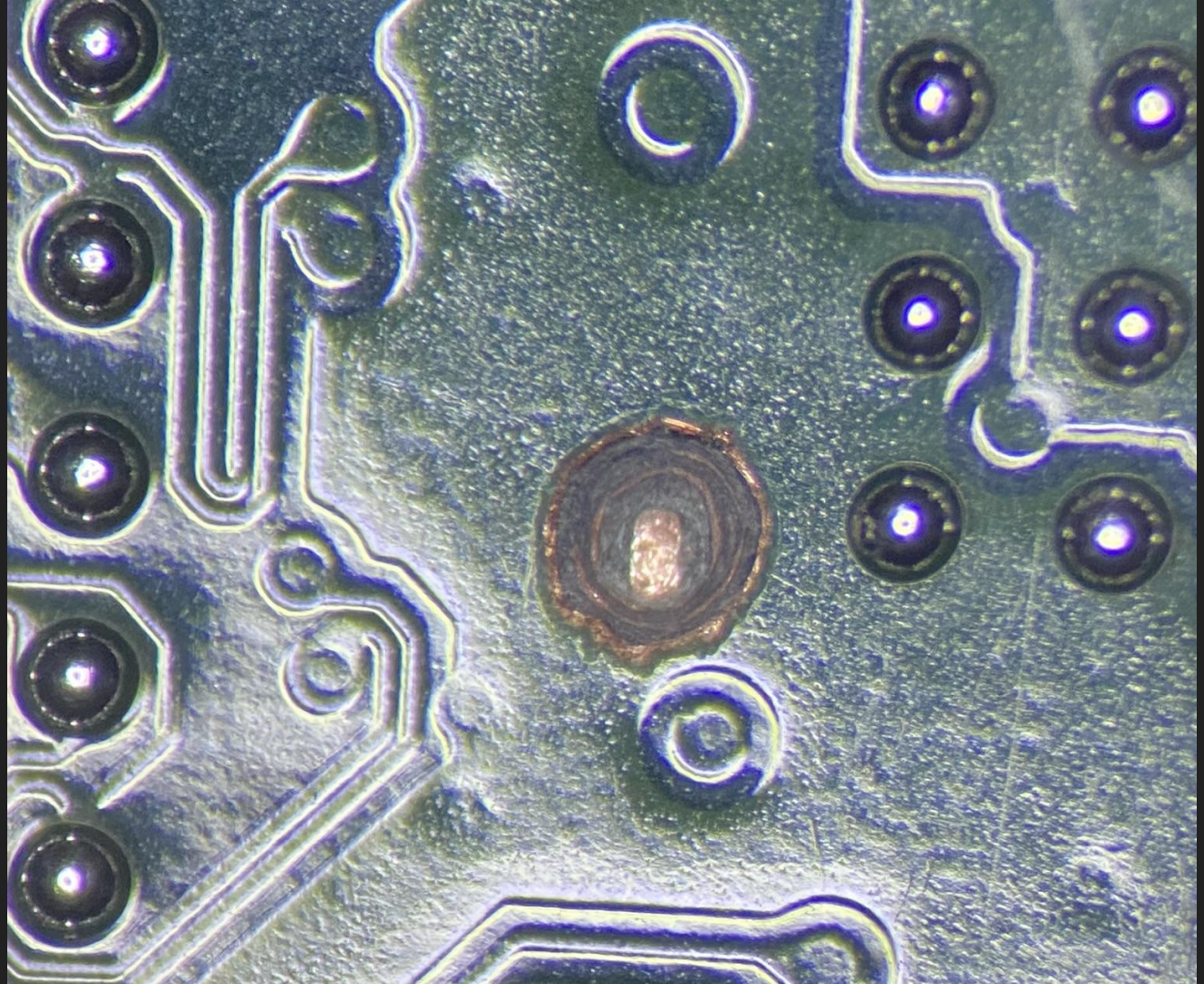

Dev MCPX
Retail MCPX

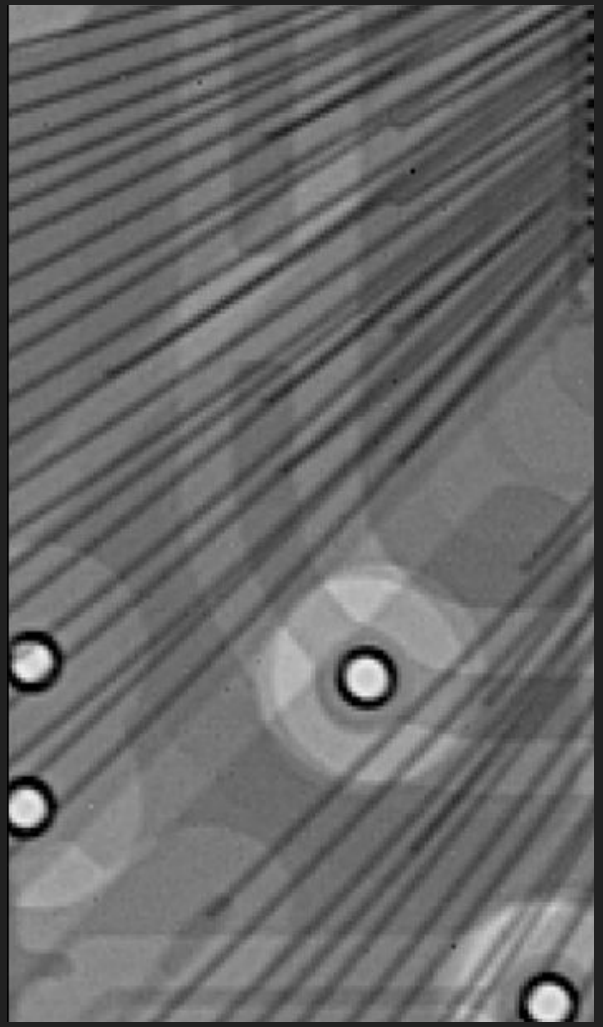
The Dig

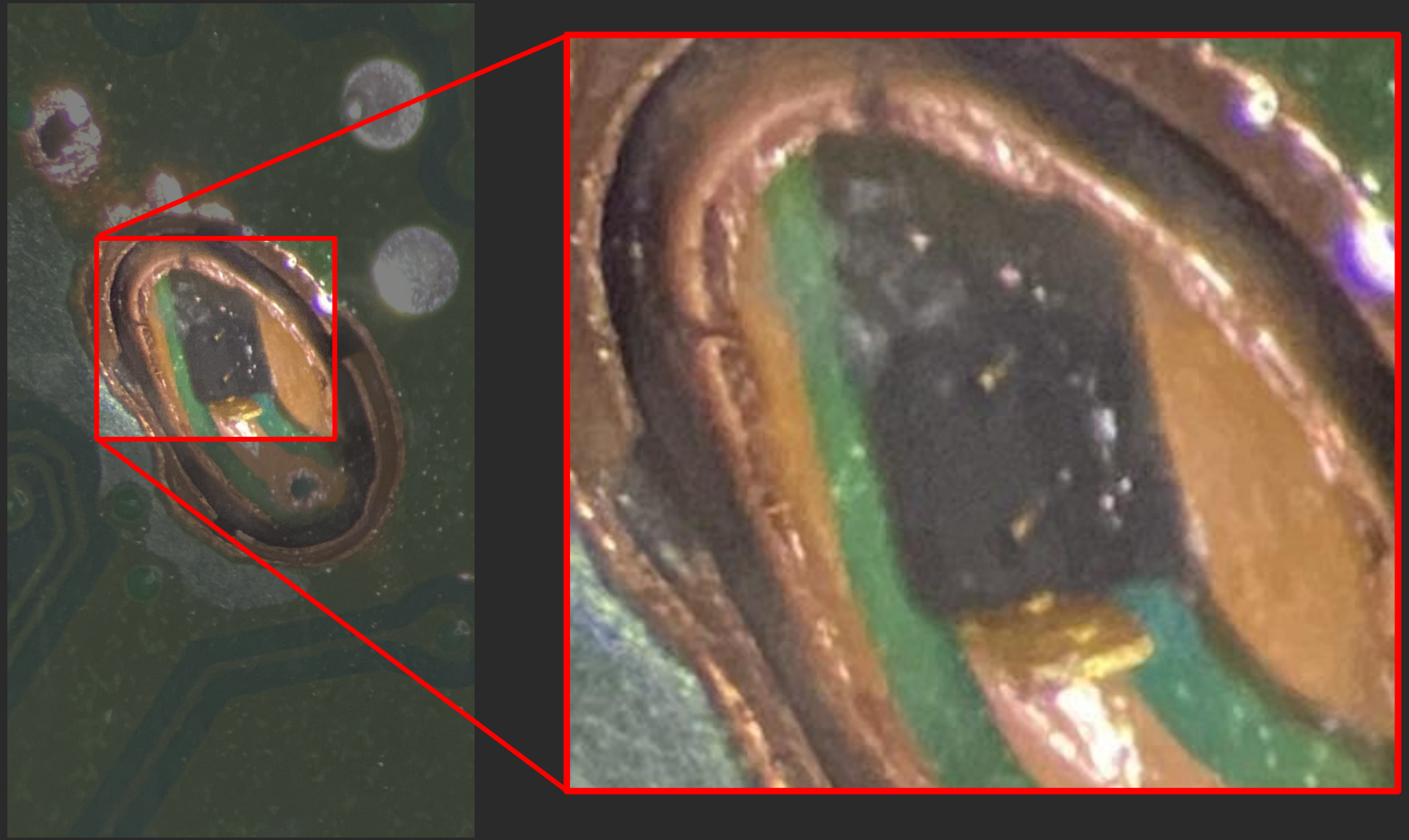




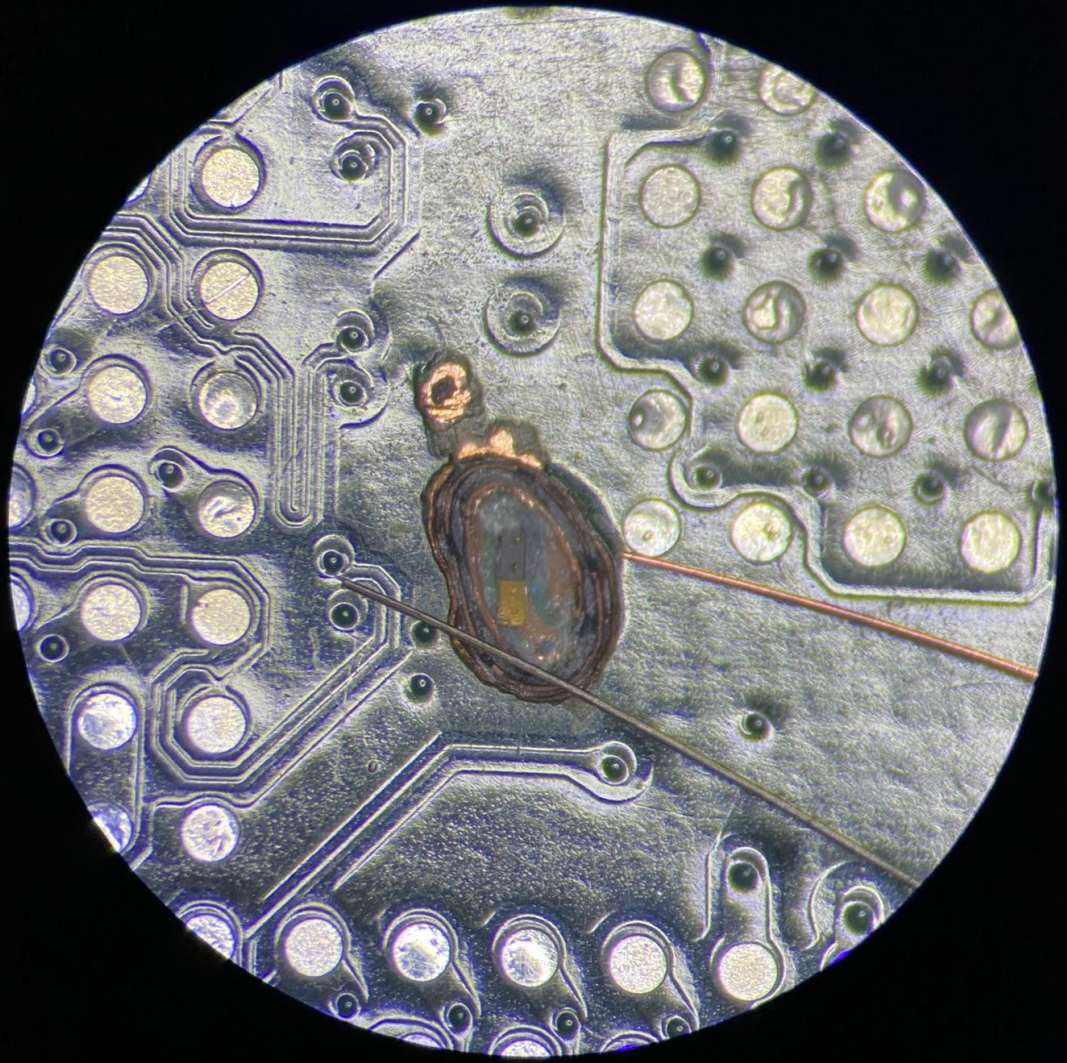








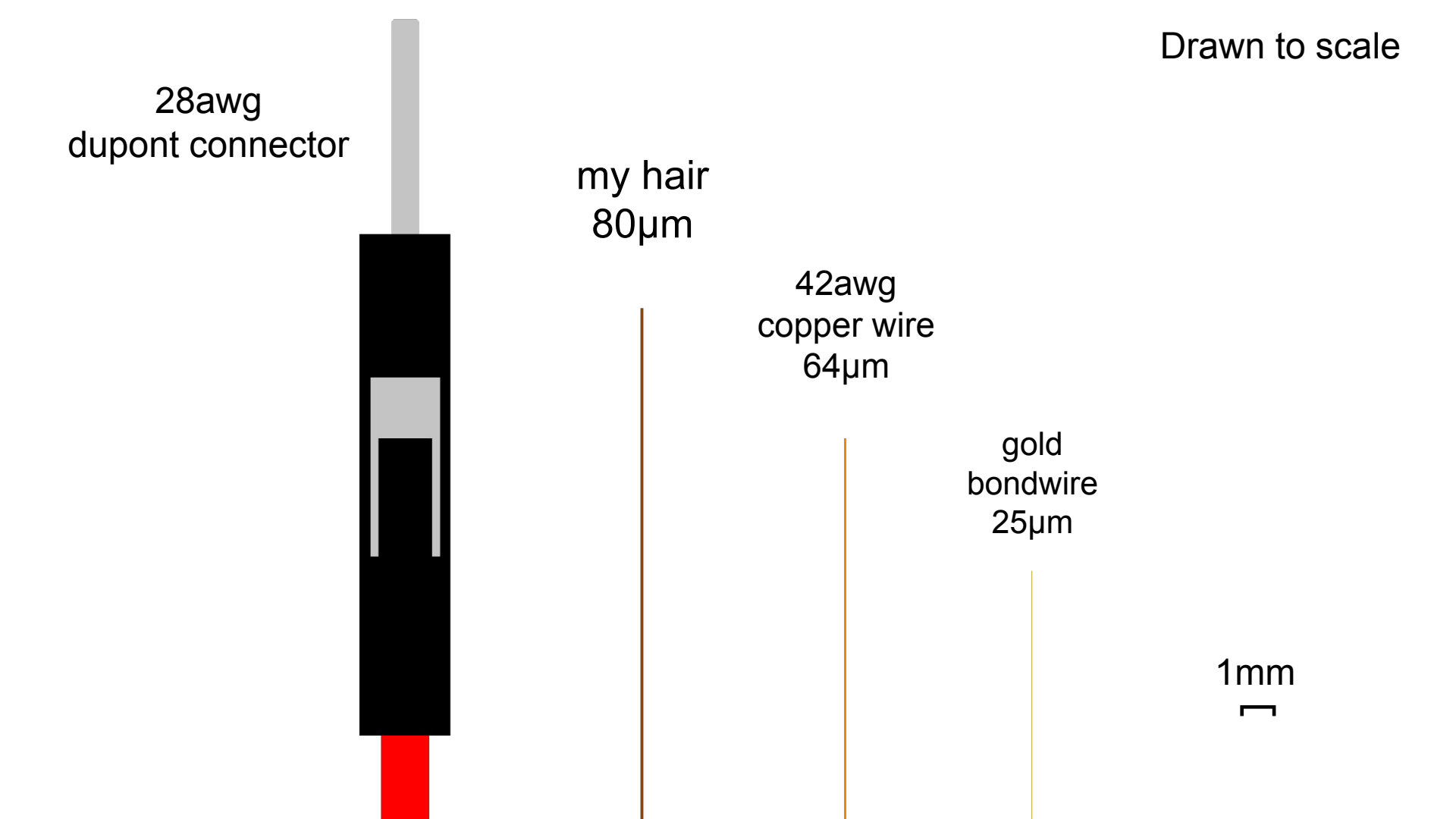

?
enable secret rom?



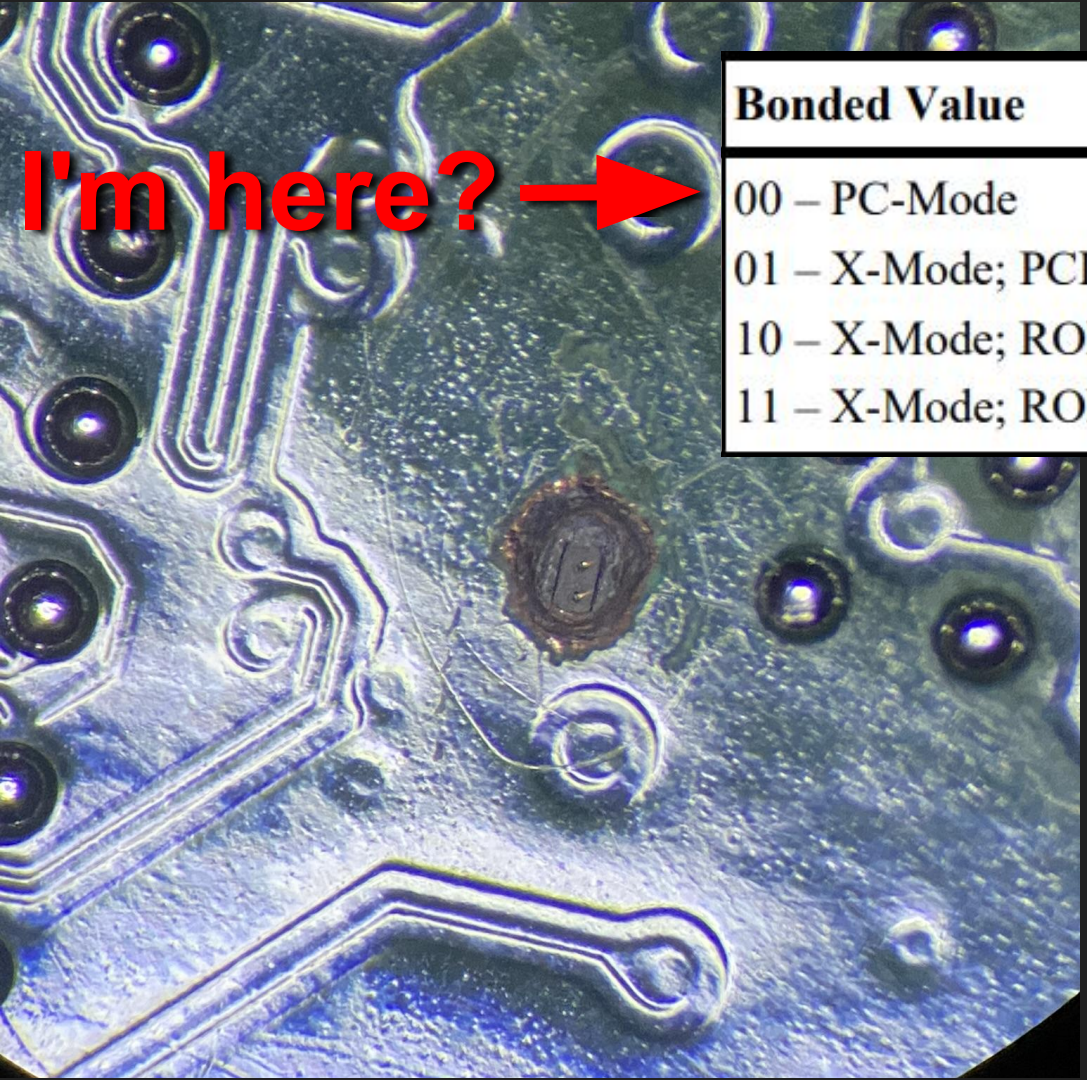
my hair
80µm

42awg
copper wire
64µm

gold
bondwire
25µm

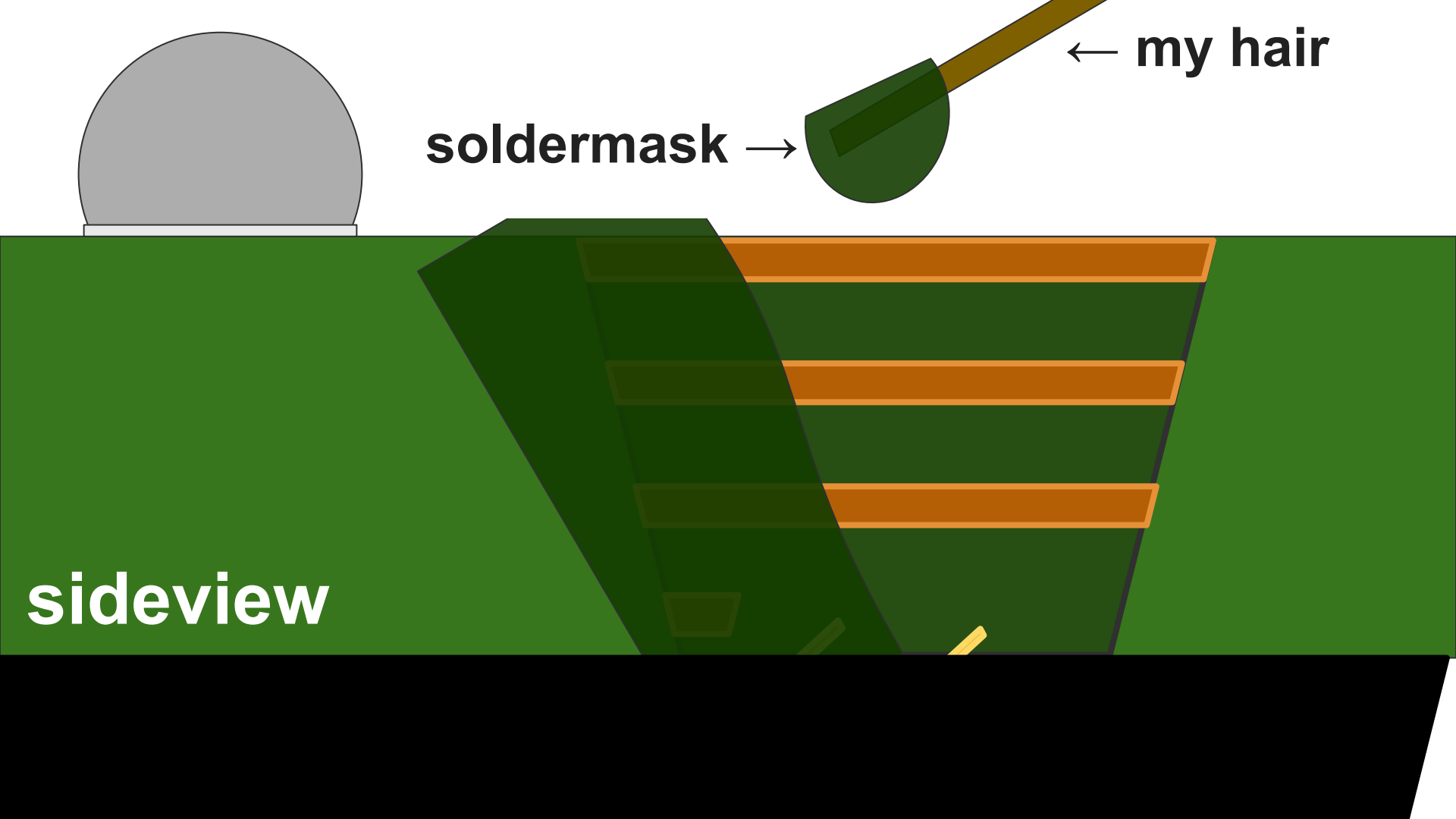

Drawn to scale
28awg
dupont connector
my hair
80µm
42awg
copper wire
64µm
gold
bondwire
25µm
1mm

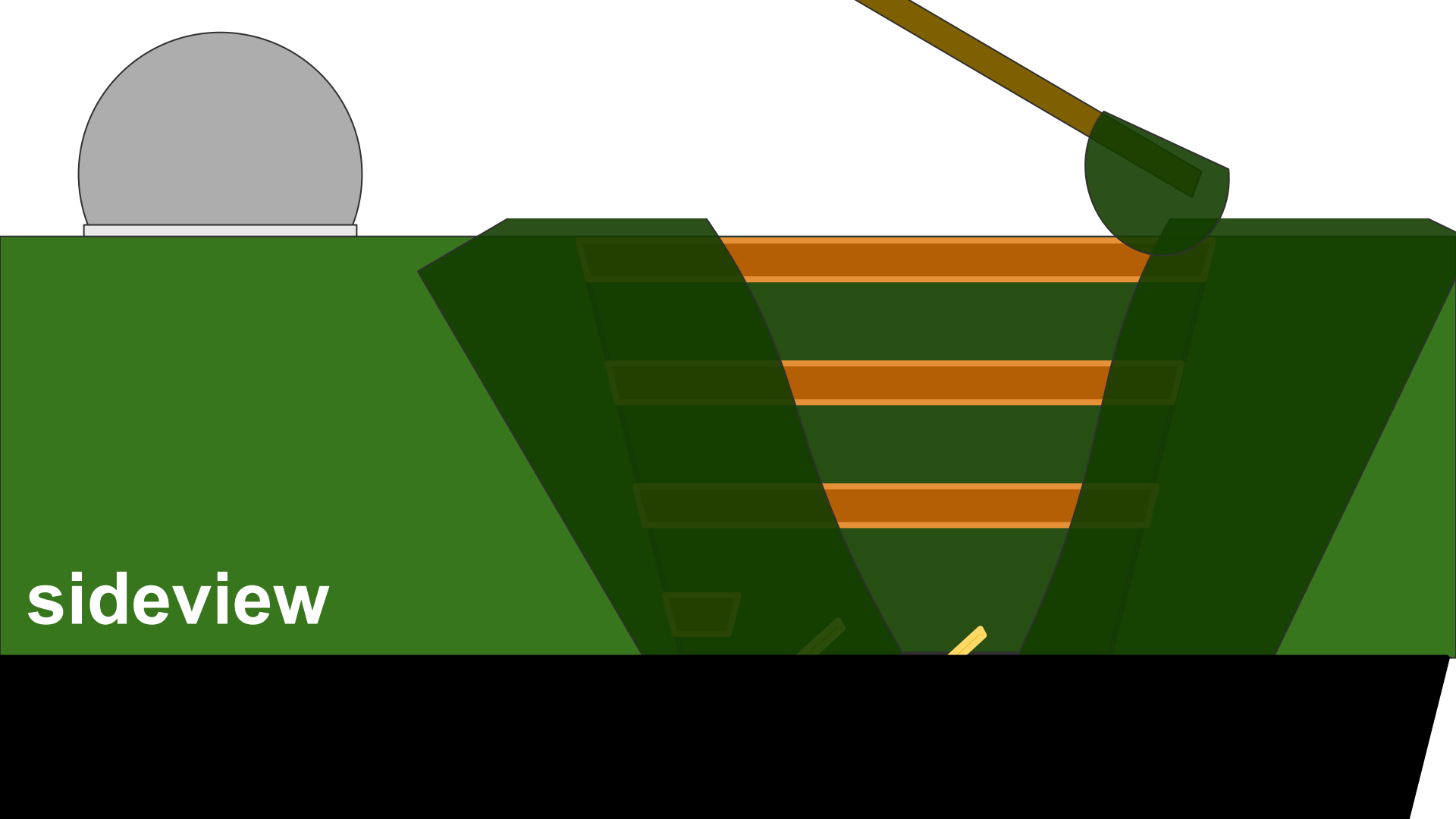
The Bodge

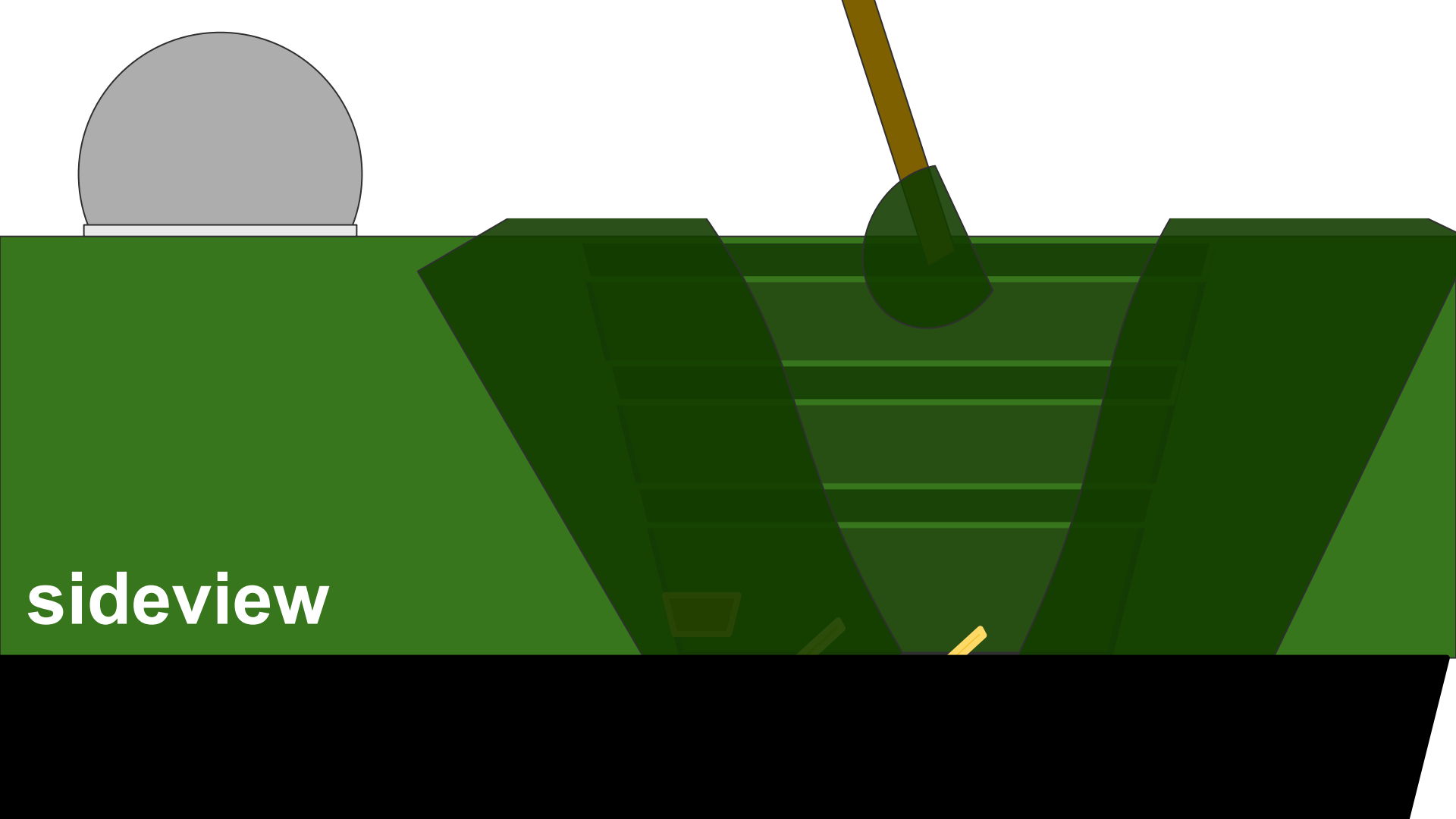


Bonded Value
00 – PC-Mode
01 – X-Mode; PCI Bus; Internal ROM Disabled
10 – X-Mode; ROM Bus; Internal ROM Disabled;
11 – X-Mode; ROM Bus; Internal ROM Enabled;

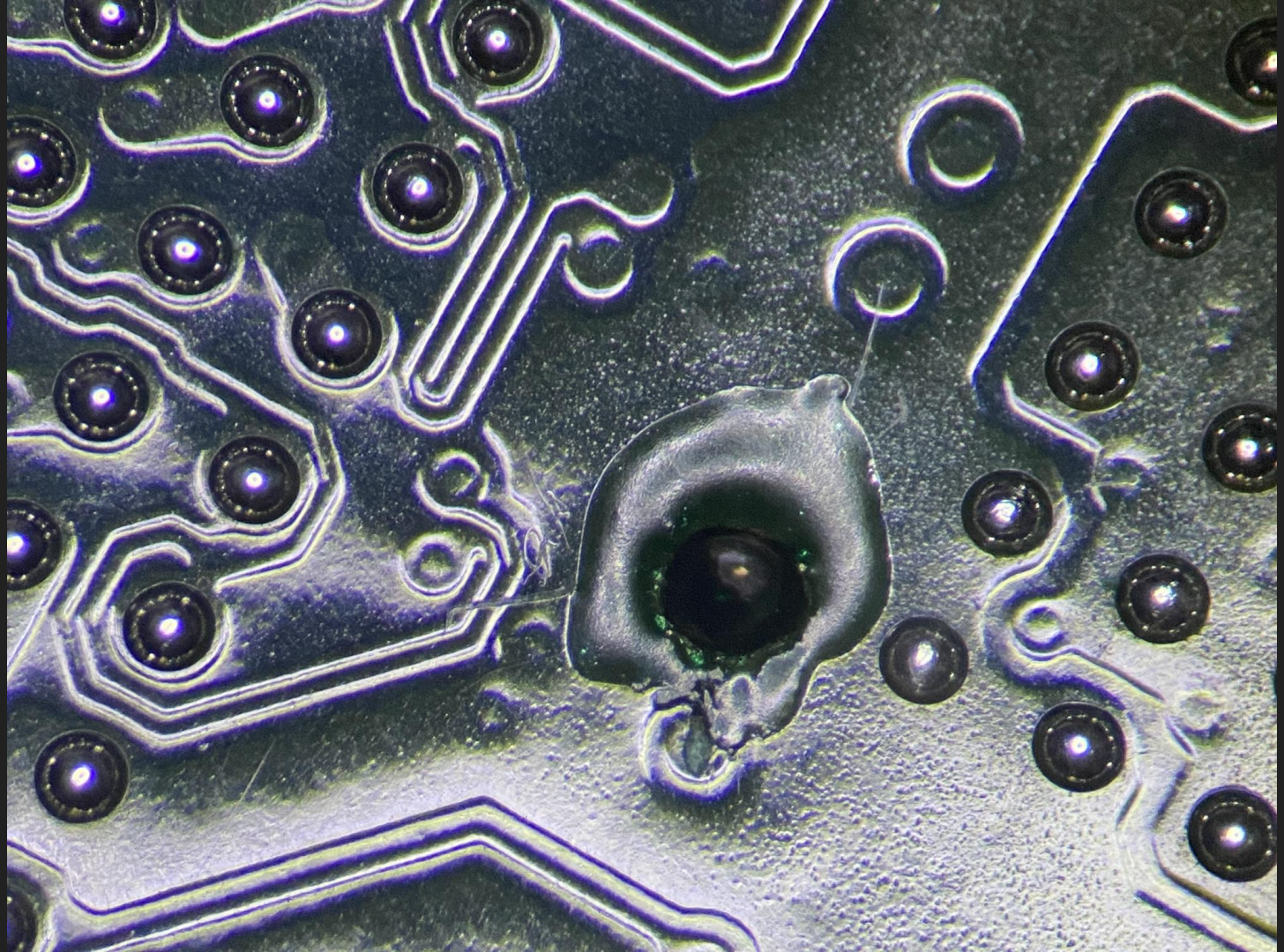

sideview


← my hair
soldermask →
sideview

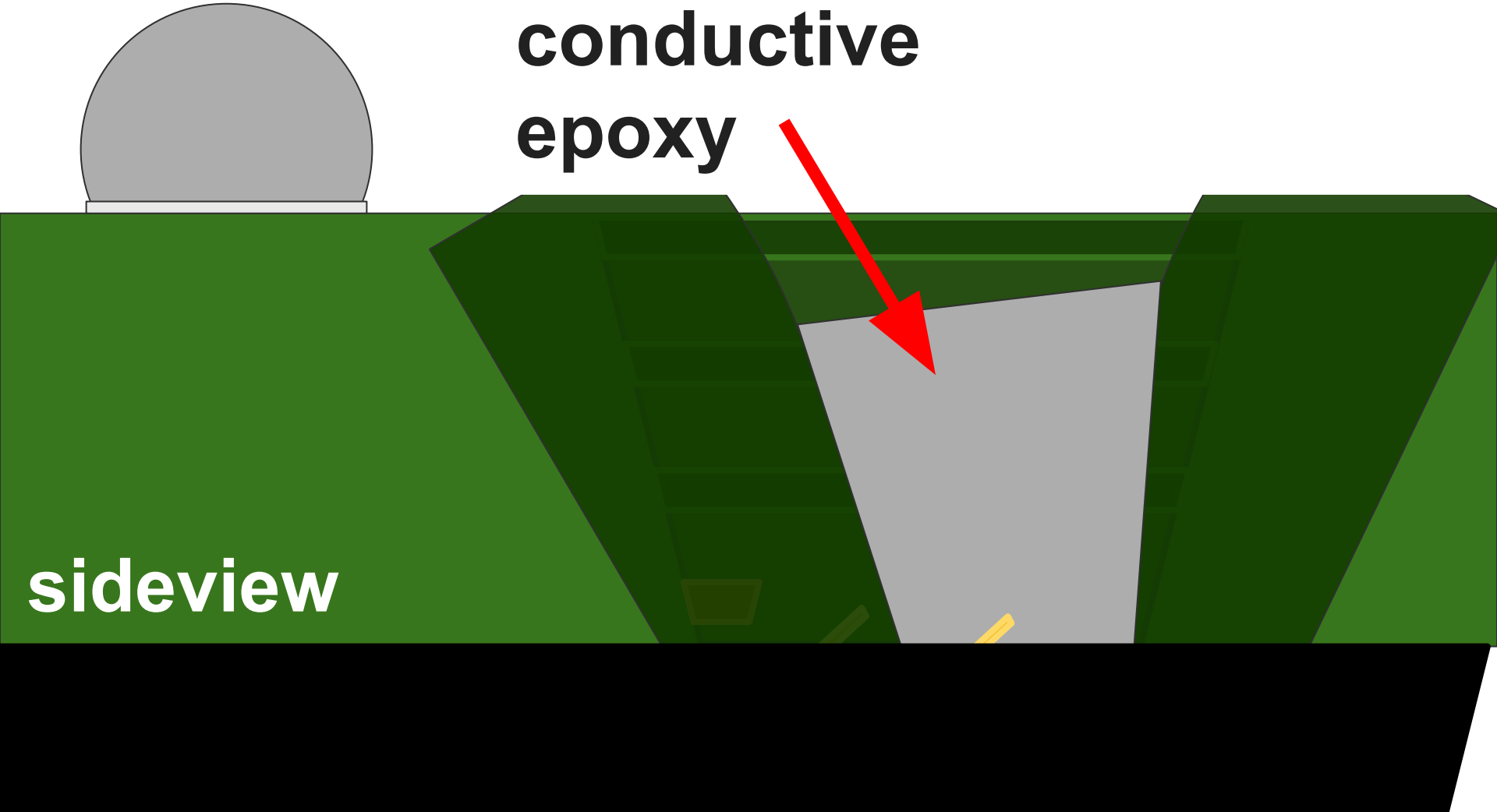

sideview

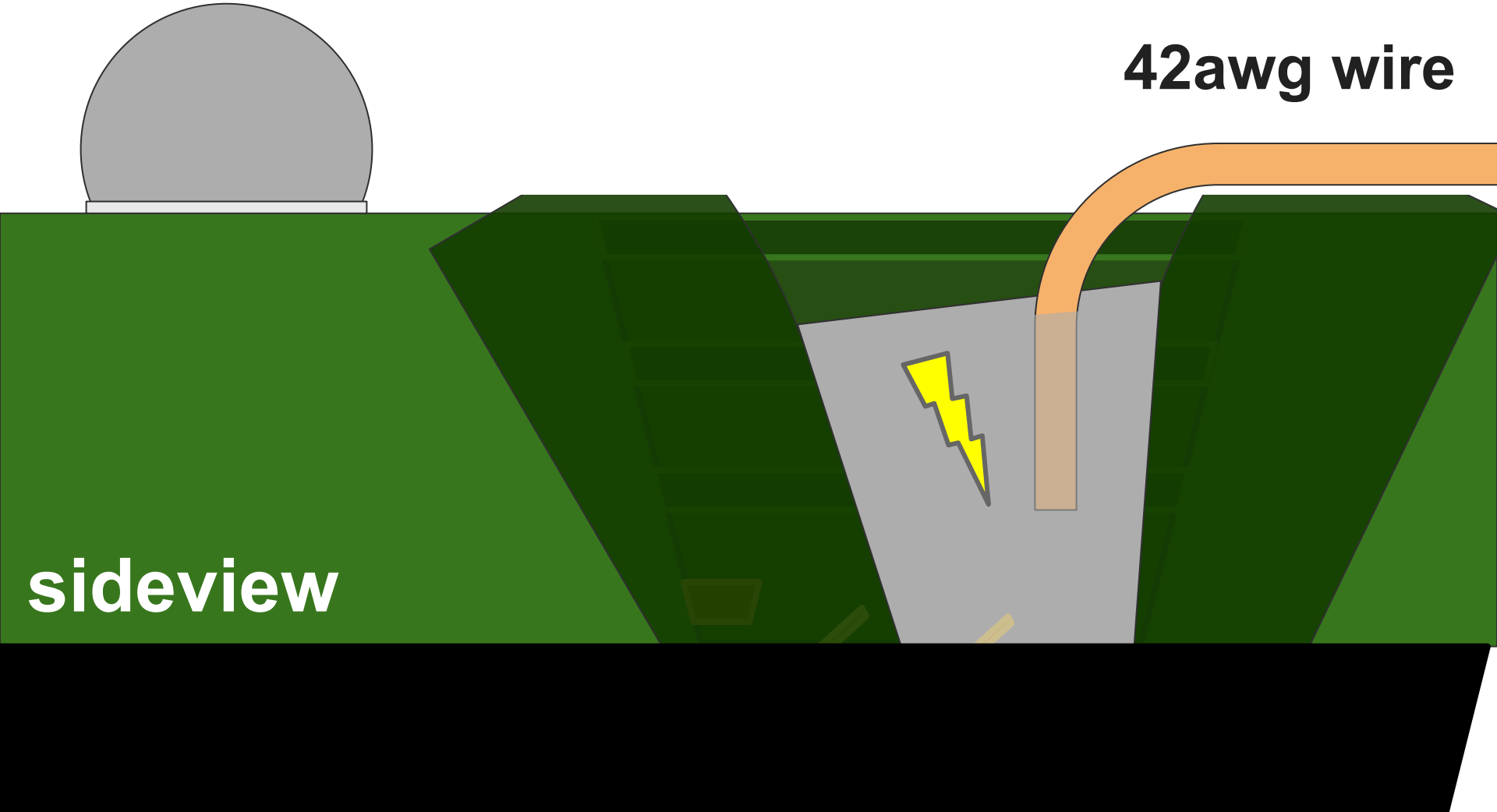

sideview

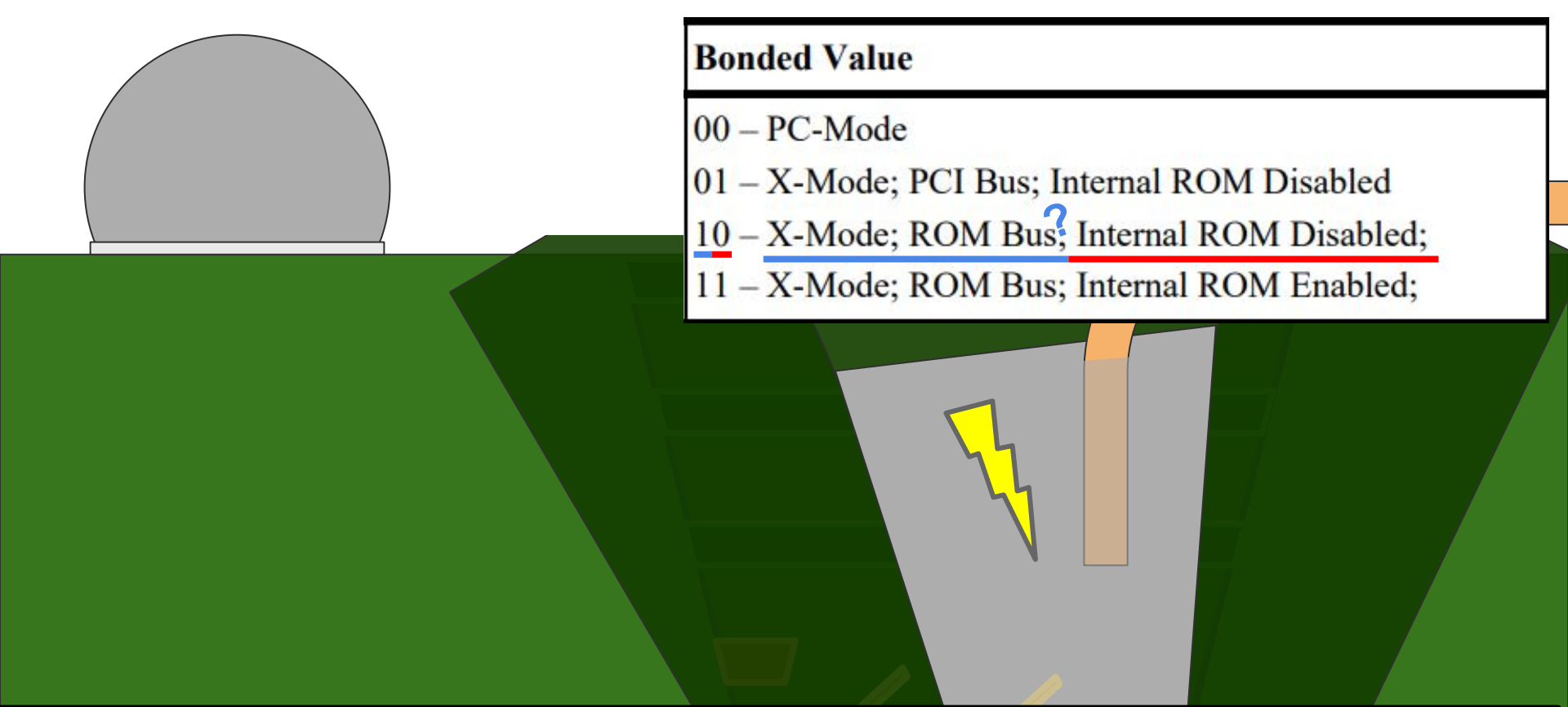

sideview

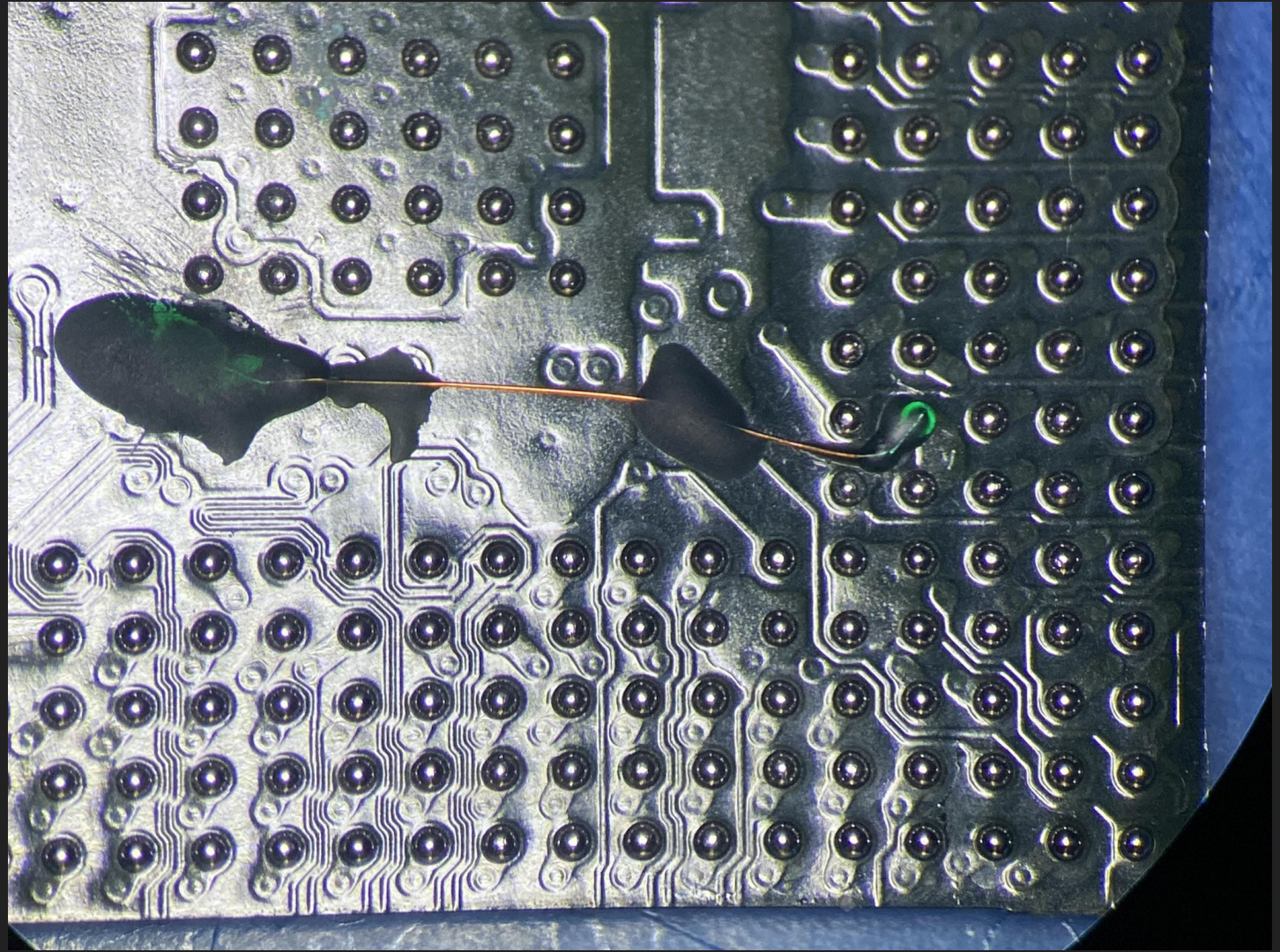


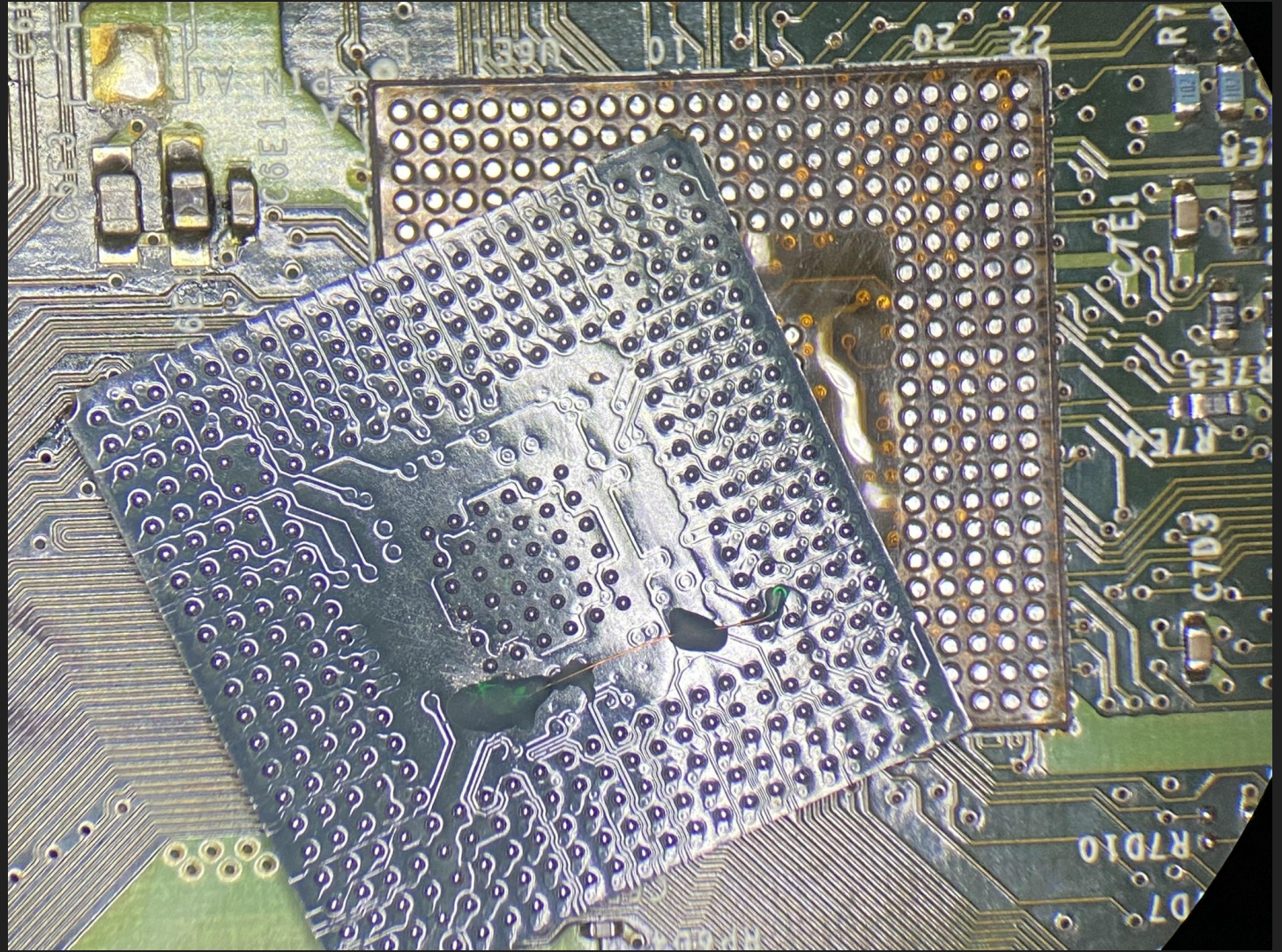

sideview

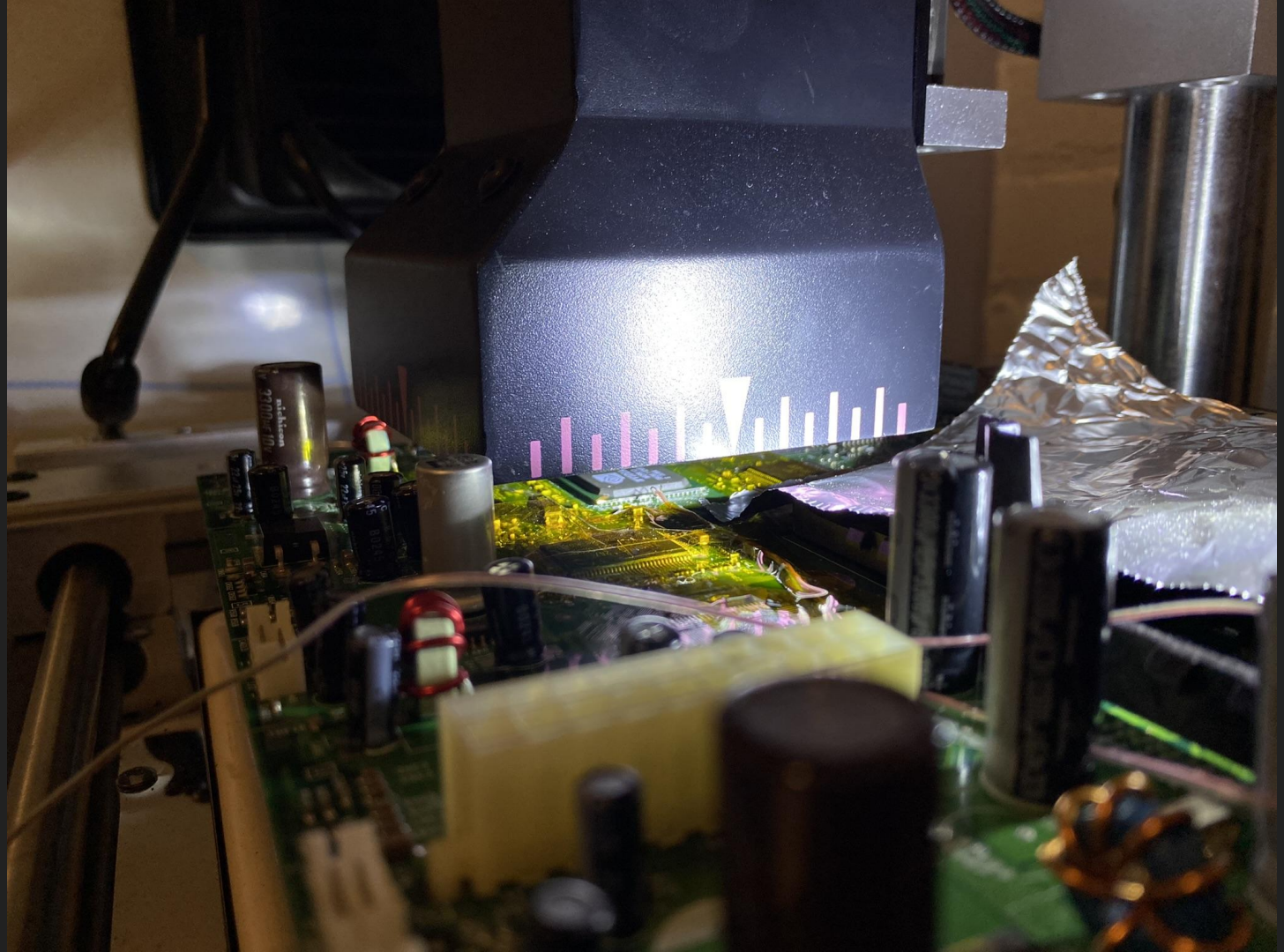

conductive
epoxy
sideview

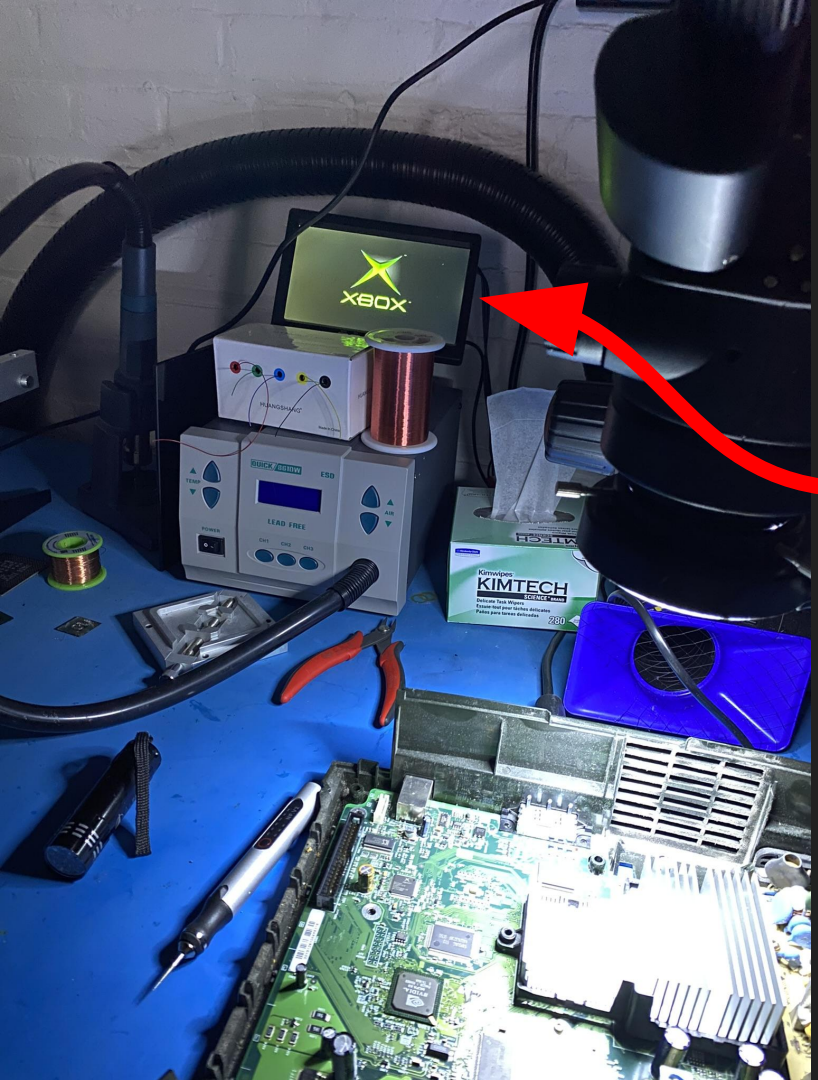

42awg wire
sideview


Bonded Value
00 – PC-Mode
01 – X-Mode; PCI Bus; Internal ROM Disabled
10 – X-Mode; ROM Bus; Internal ROM Disabled;
11 – X-Mode; ROM Bus; Internal ROM Enabled;
?
floating… as 0v?!
hoping it disables rom.
?
3.3v

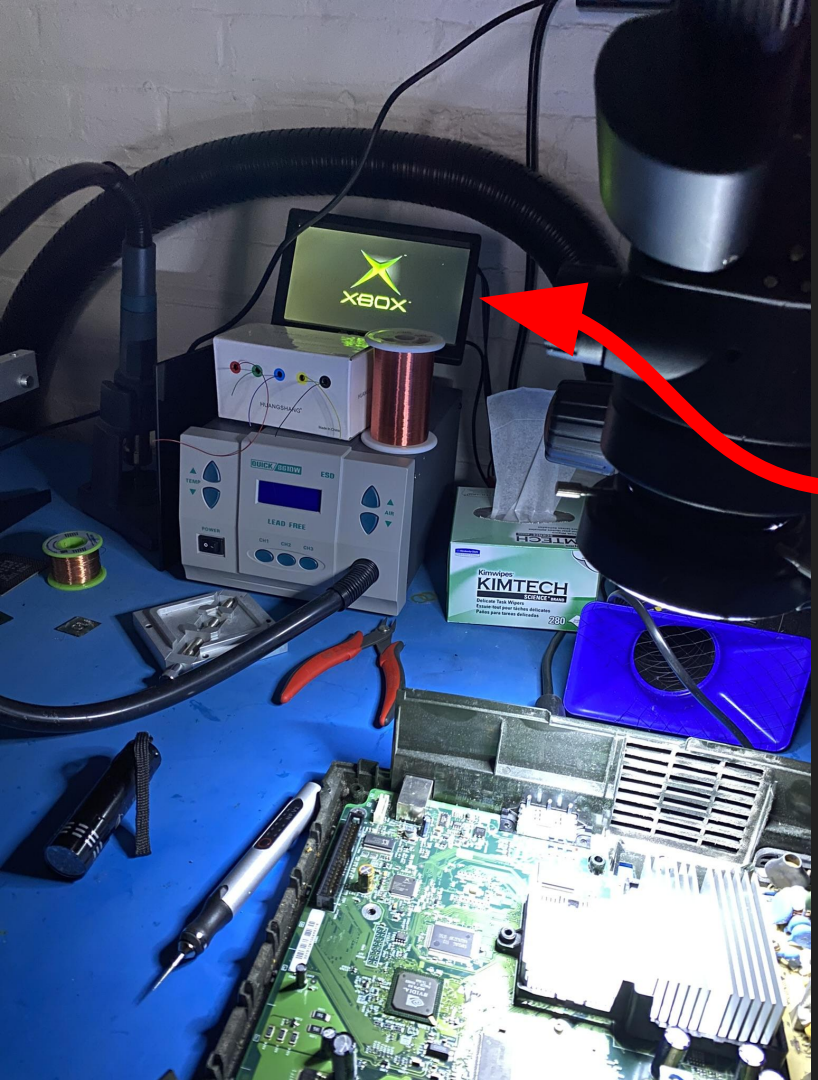








THE SYSTEM STILL BOOTS😱😱😱

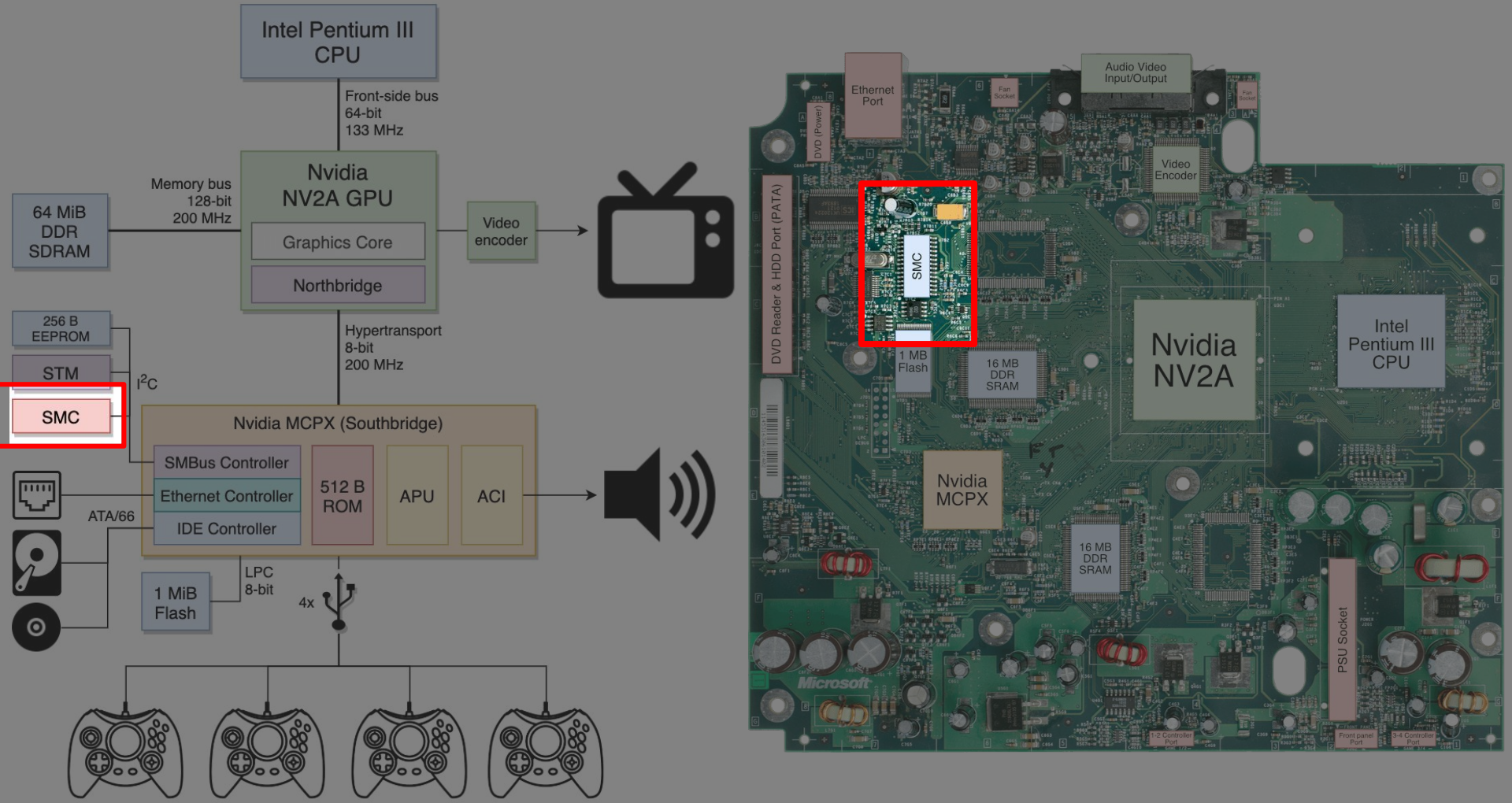


THE SYSTEM STILL BOOTS😱😱😱

... in retail mode.. 💢

fail..

System Management Controller


Intel Pentium III CPU
Front-side bus 64-bit 133 MHz
Memory bus 128-bit 200 MHz
64 MiB DDR SDRAM
Nvidia NV2A GPU
Graphics Core
Northbridge
Video encoder
Hypertransport 8-bit 200 MHz
256 B EEPROM
STM
SMC
I²C
Nvidia MCPX (Southbridge)
SMBus Controller
Ethernet Controller
IDE Controller
512 B ROM
APU
ACI
ATA/66
LPC 8-bit
1 MiB Flash
4x
Ethernet Port
Audio Video Input/Output
DVD (Power)
Fan Socket
Video Encoder
DVD Reader & HDD Port (PATA)
SMC
1 MB Flash
16 MB DDR SRAM
Nvidia NV2A
Intel Pentium III CPU
Nvidia MCPX
16 MB DDR SRAM
PSU Socket
Microsoft
1-2 Controller Port
Front panel Port
3-4 Controller Port

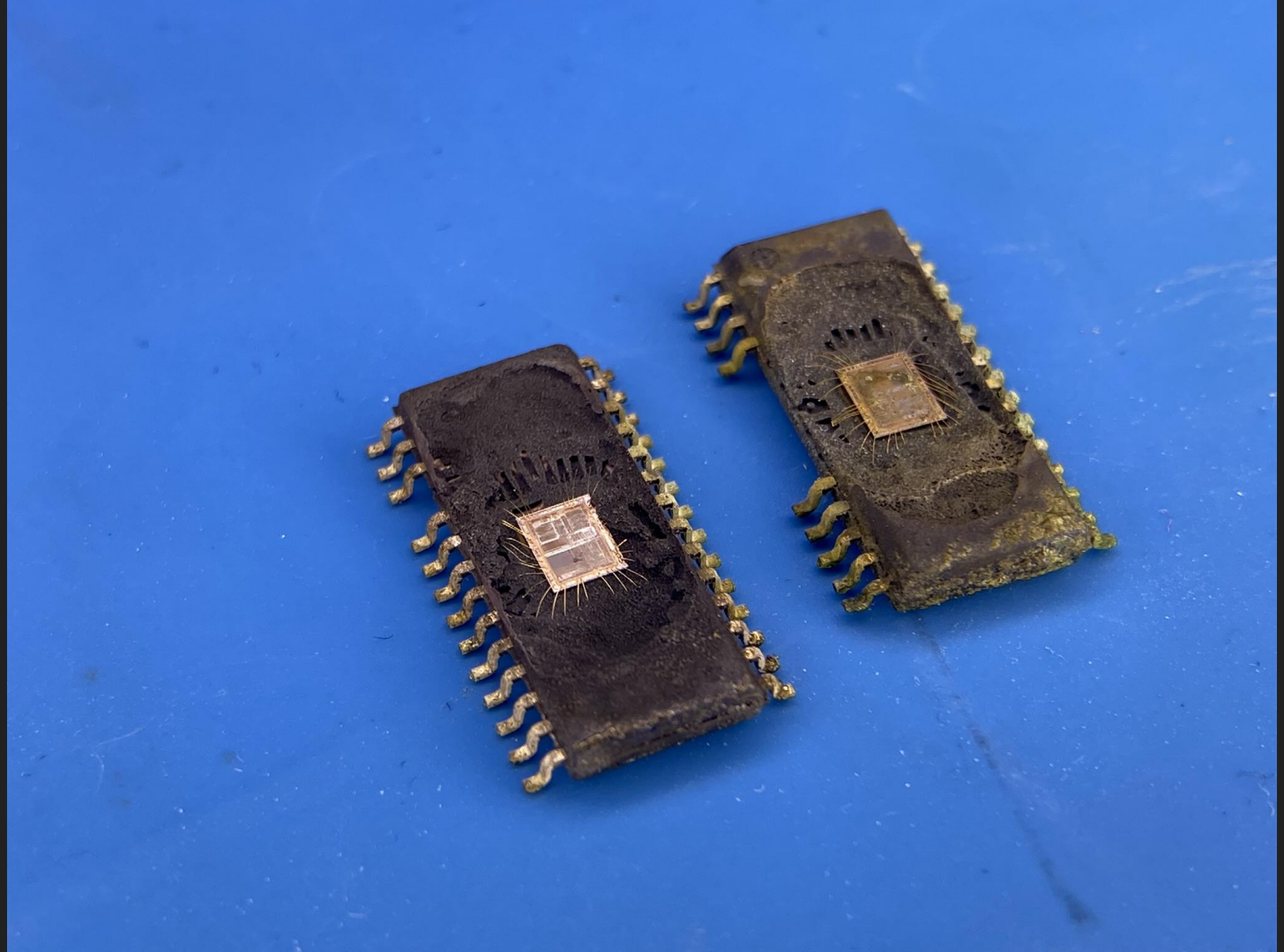
SMC - PIC16LC63A

- **System Management Controller**
  - Monitor power / eject button presses
  - Monitor DVD tray state signals
  - Drive fan PWM
  - Front panel LED
  - "SMC Challenge" / Boot security check

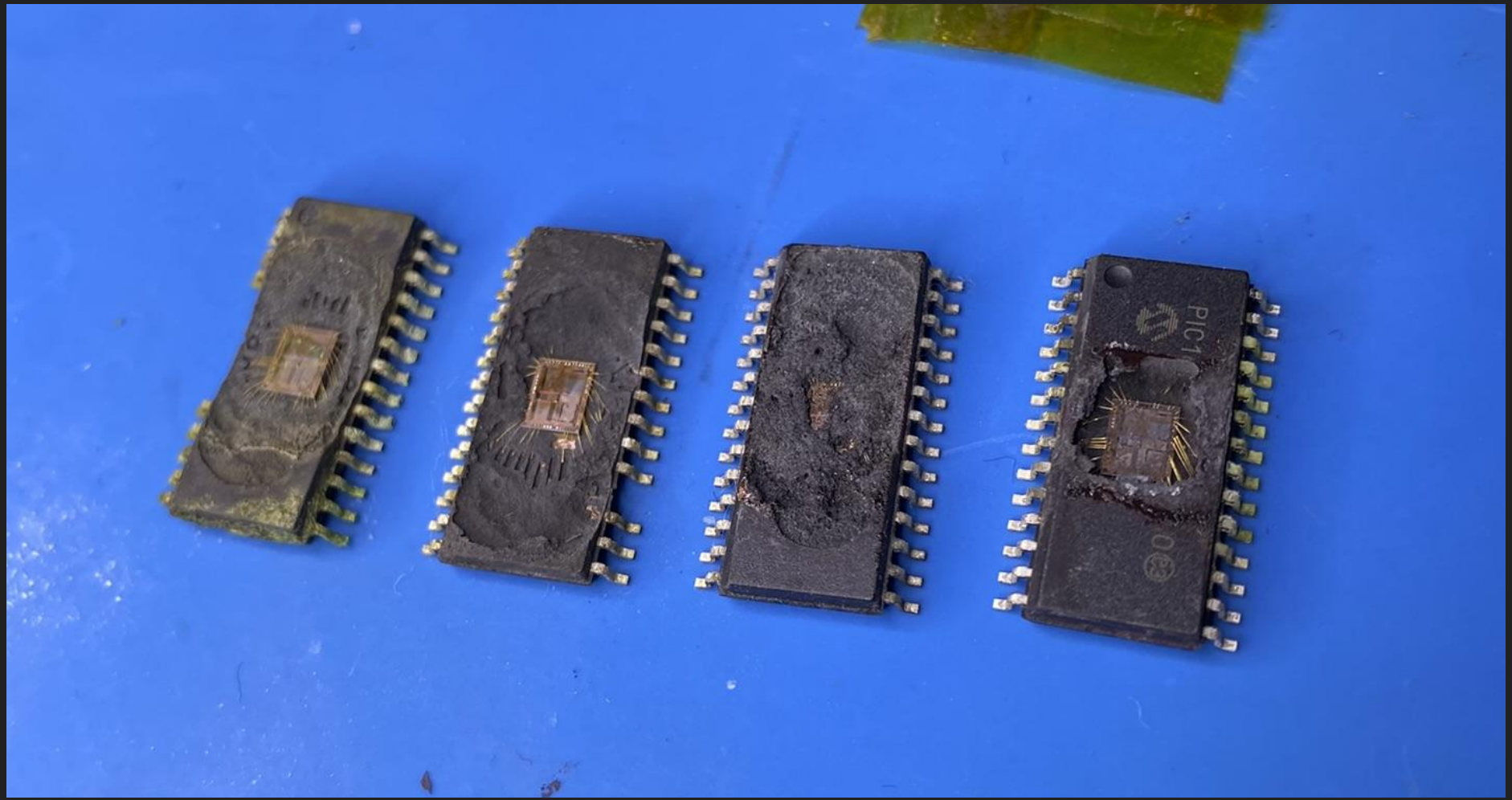
- **4KB of code - still undumped!**
  - Subtle differences between dev and retail SMC
  - **Good challenge to learn silicon RE!**

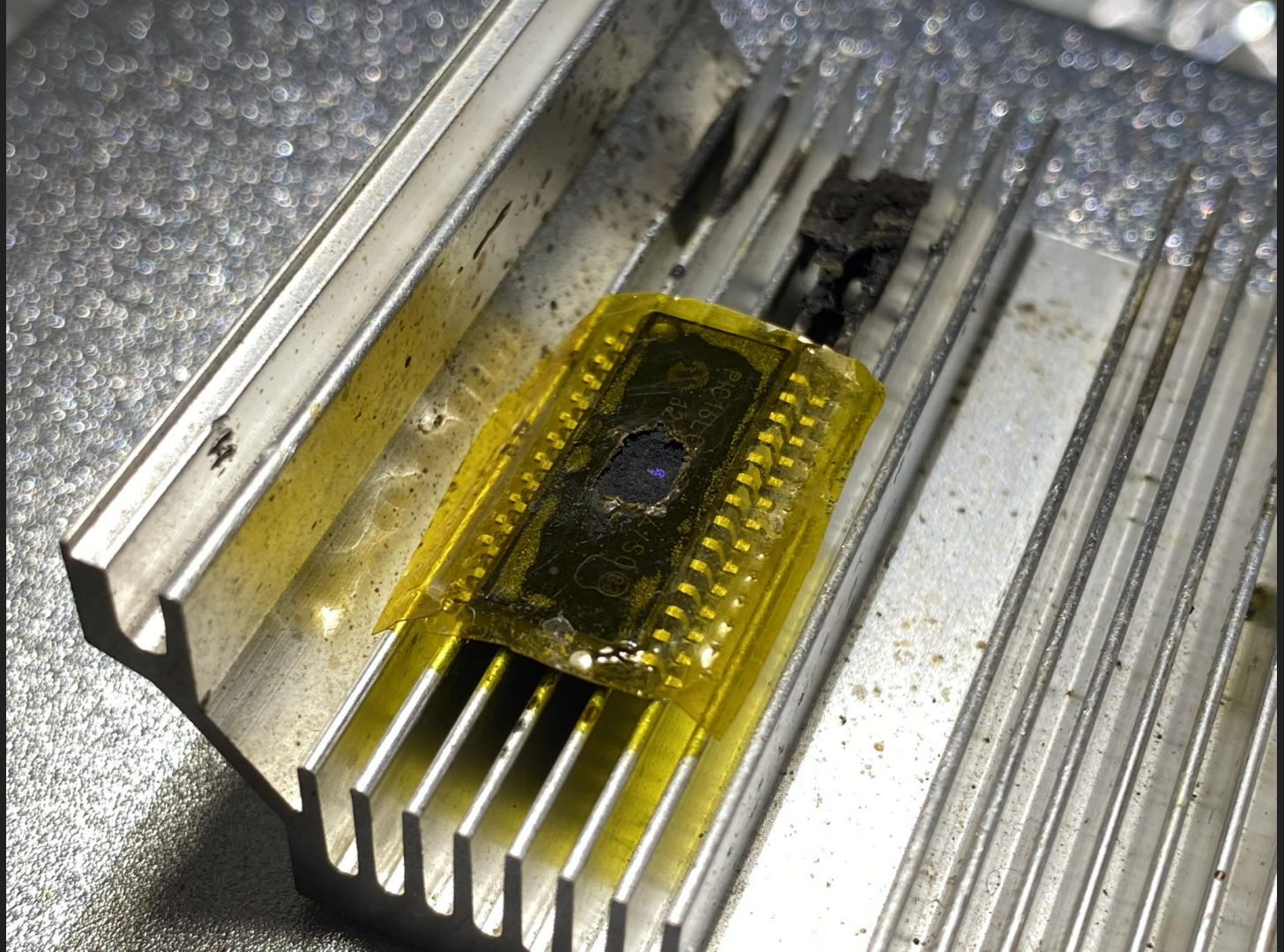
- **Glitch, and UV-Erasure Resistant?**
  - https://web.archive.org/web/20081222042941/http://www.flylogic.net/blog/?p=21


PIC16LC63A-04/SO
0229JF7
SMC_P01
POW
RUN
USB
XGecu Pro
IC

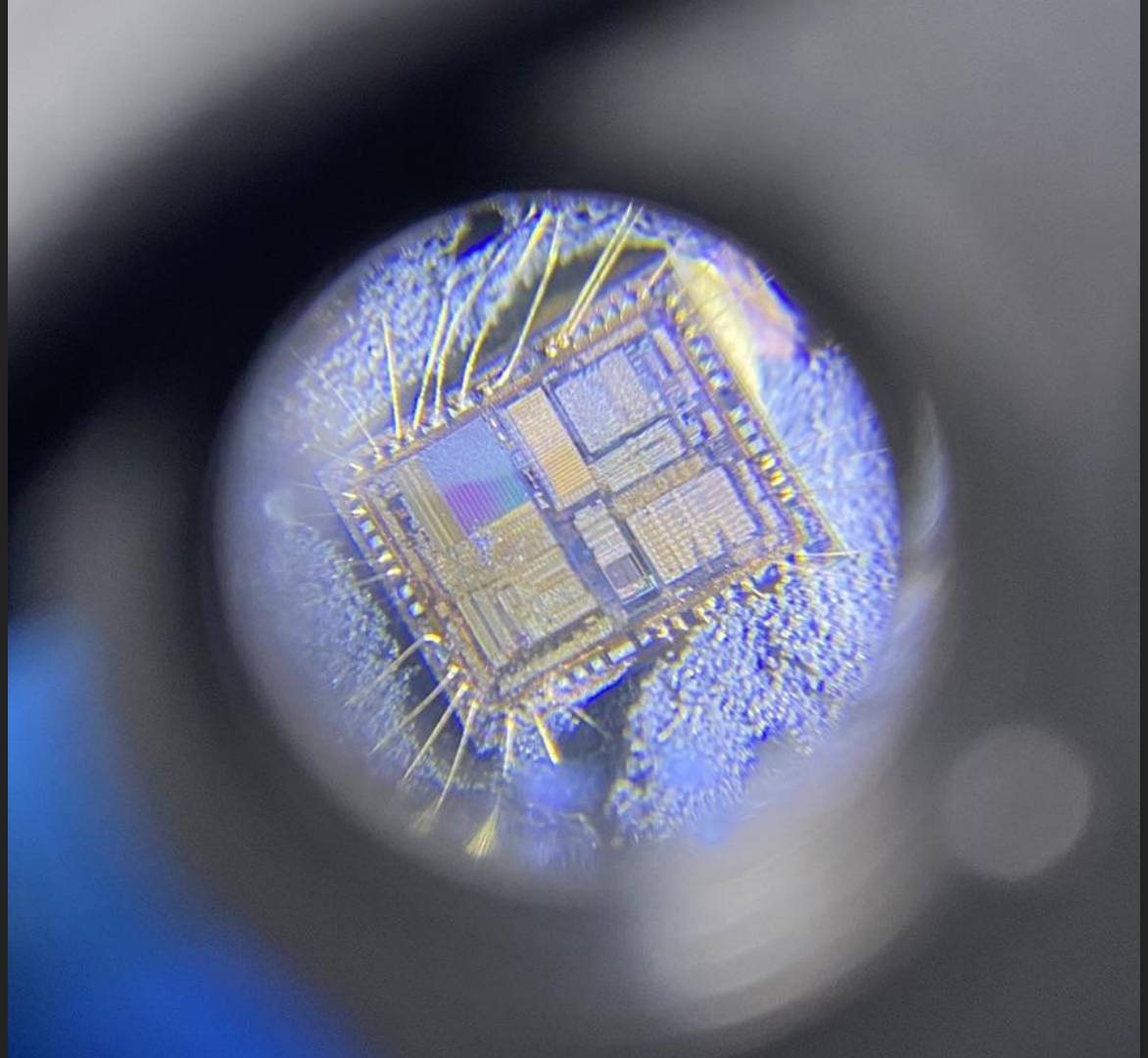


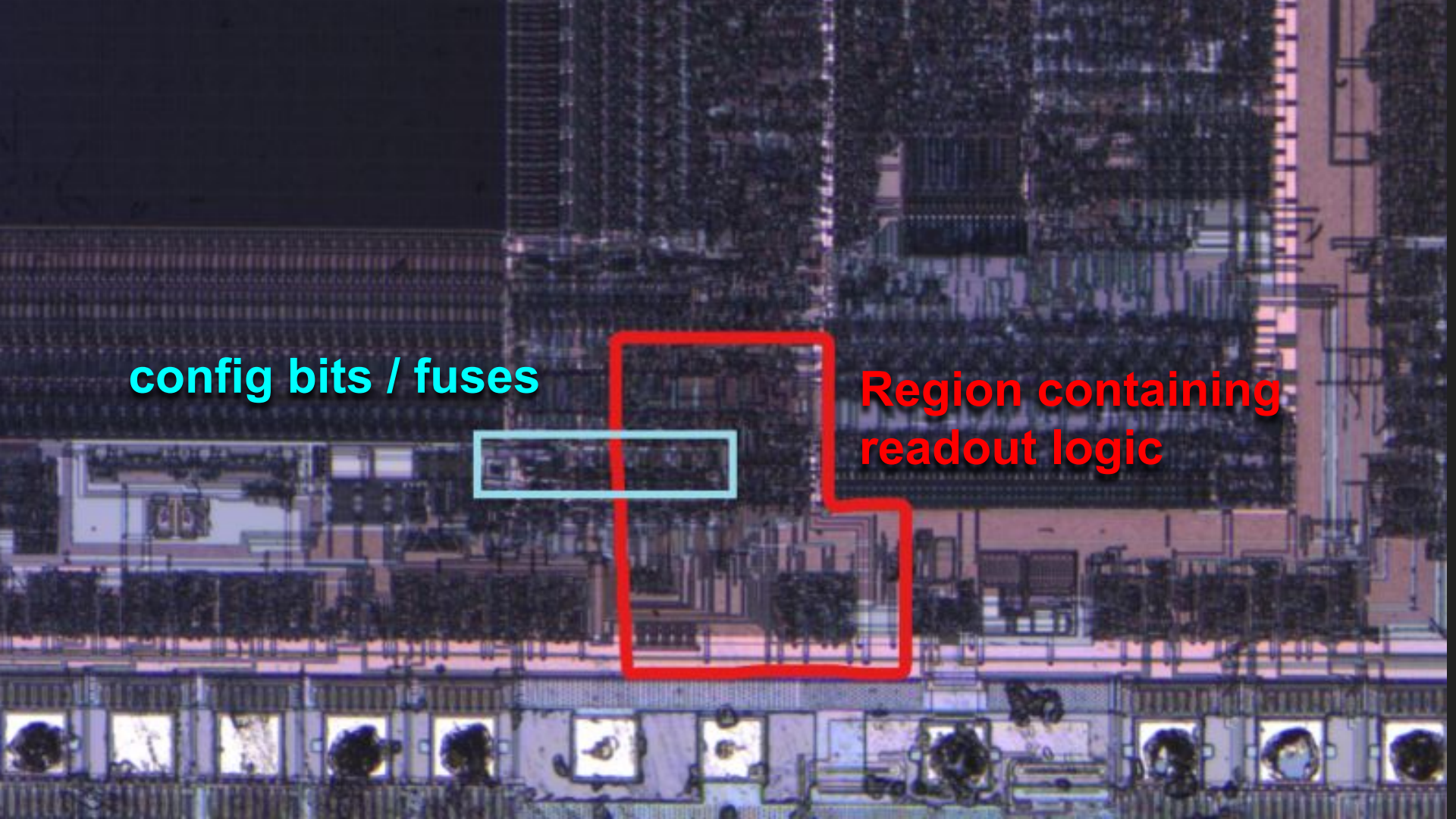
SH-2
MAGNETIC STIRRER

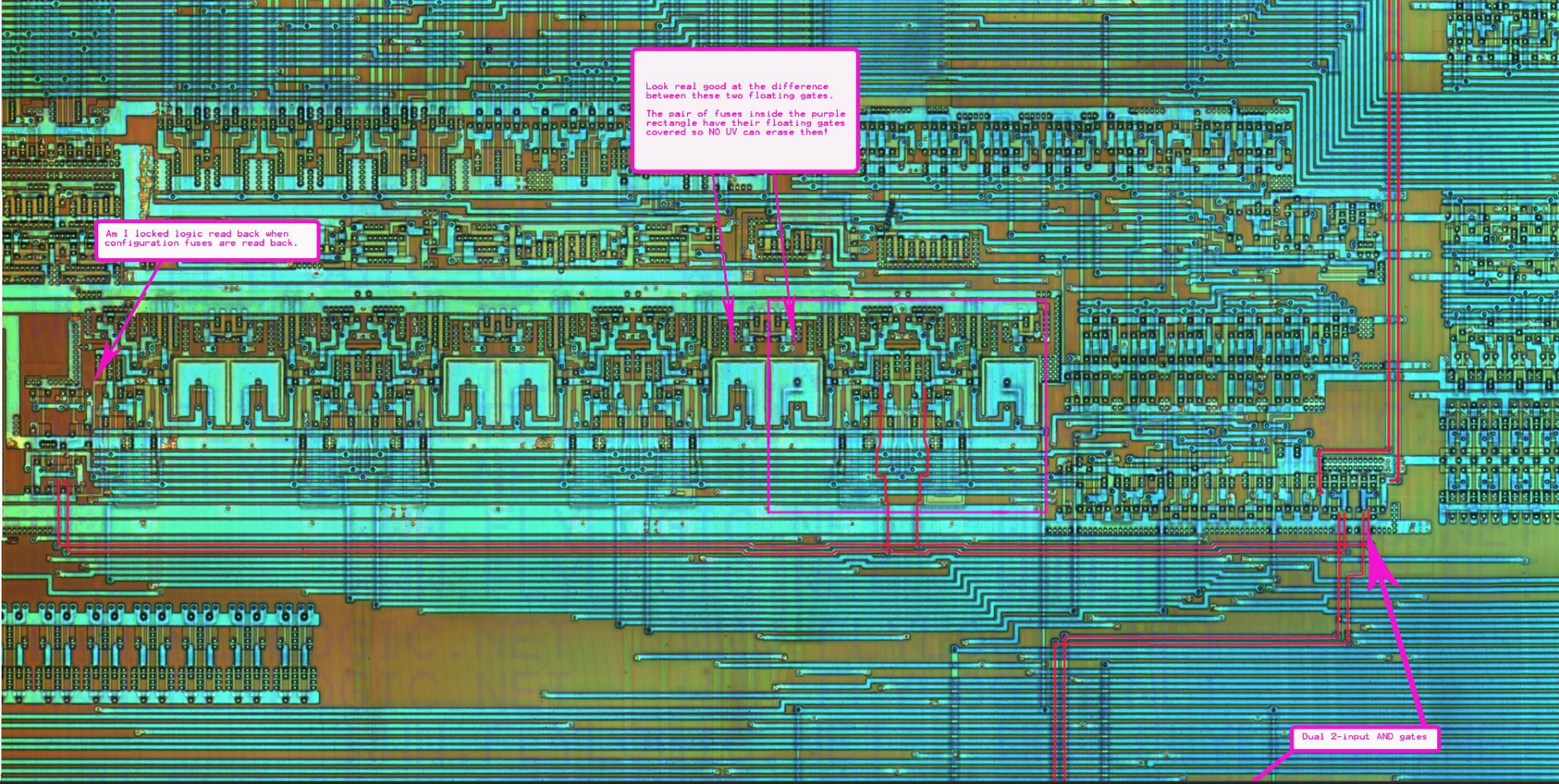

PIC1



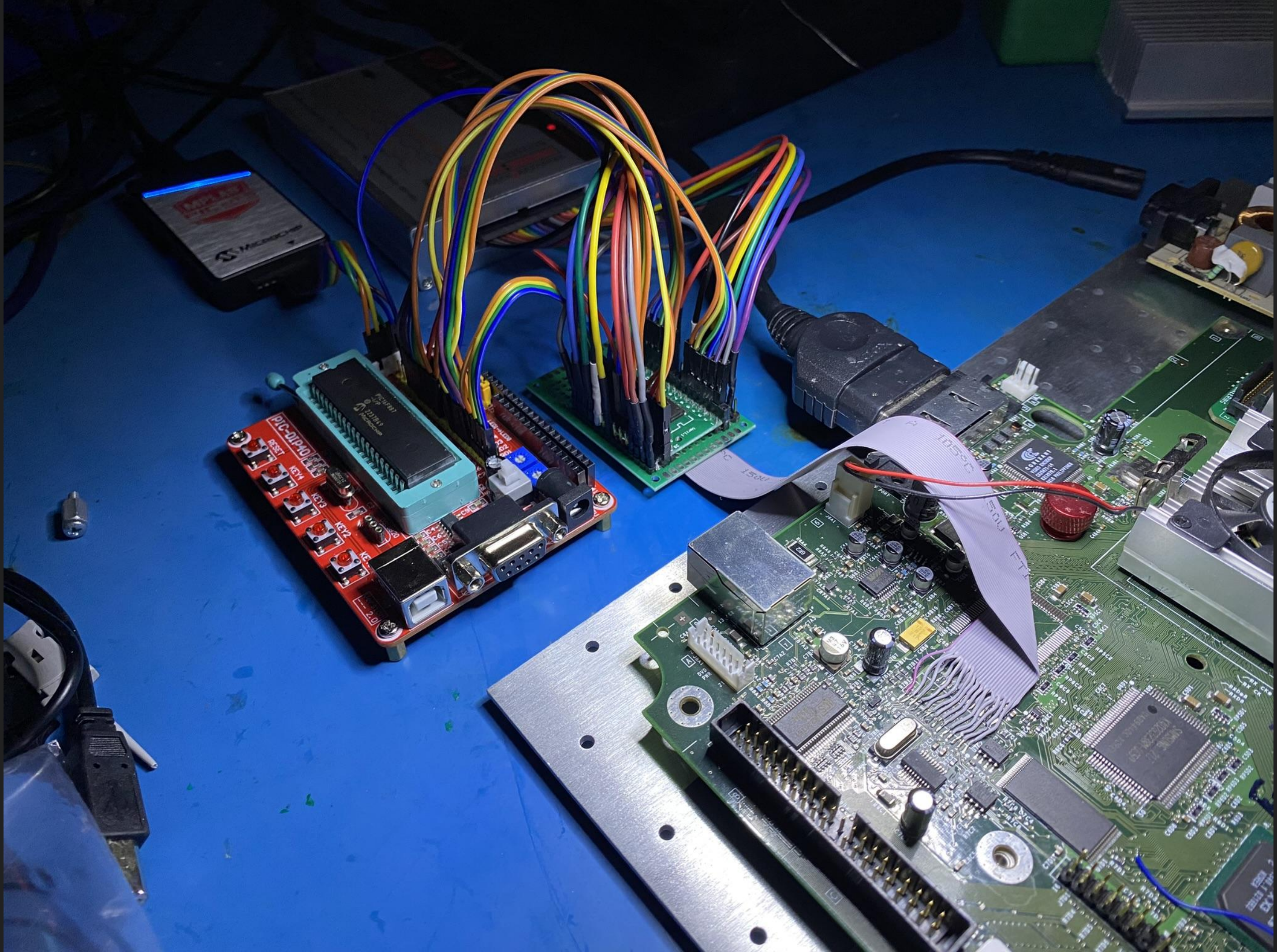

PIC16L
12
/SO



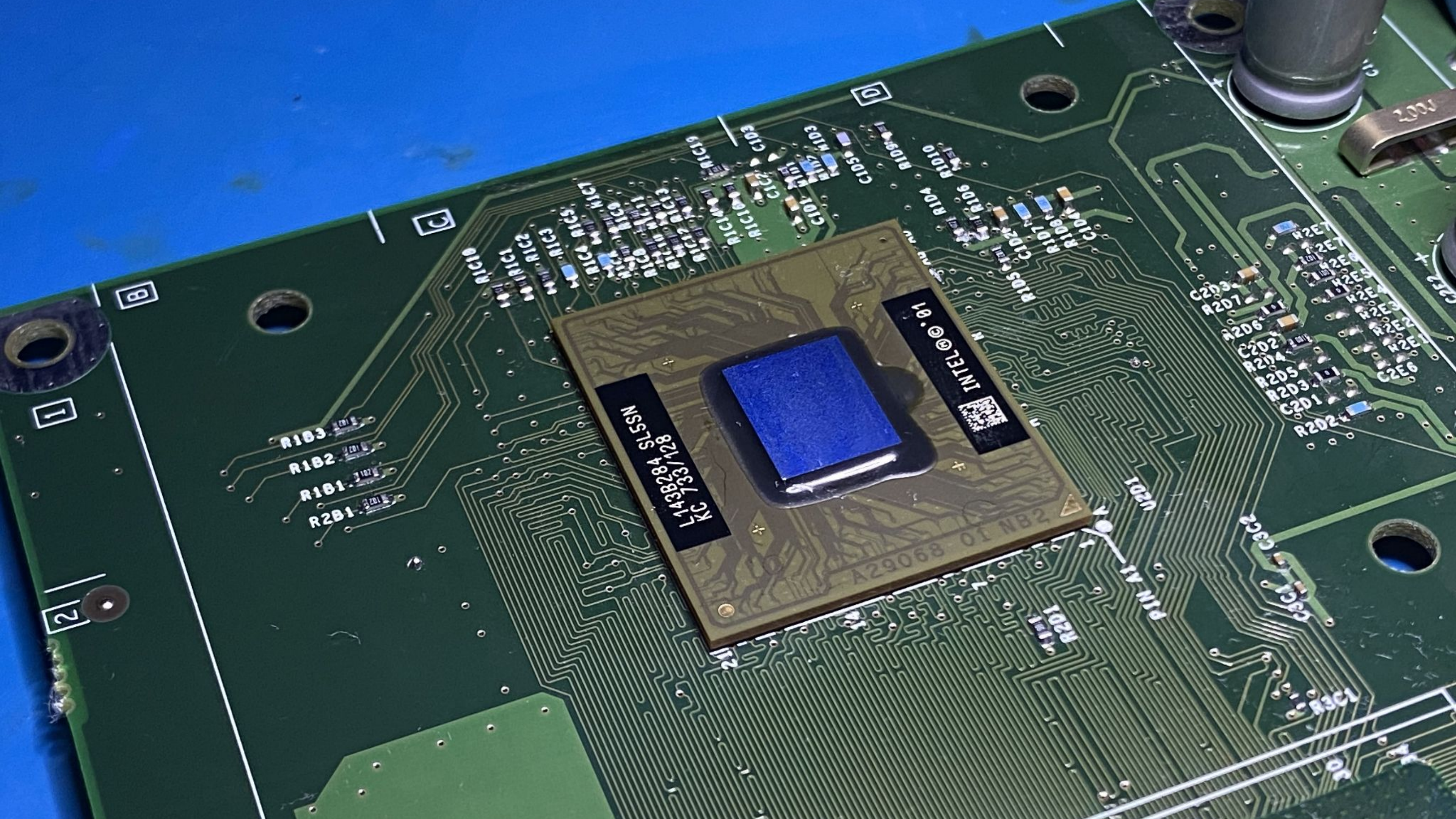

config bits / fuses
Region containing
readout logic



https://web.archive.org/web/20081222042941/http://www.flylogic.net/blog/?p=21



CPU Interposers


L143B284 SL5SN
KC 733/128
INTEL© '01
A29068 01 NB2
PIN A1

Xbox CPU

- **Retail Xbox CPU - 180nm Coppermine (SL5SN)**
  - 733mhz core
  - 133mhz fsb
  - 128kb L2 cache
  - 1.7 volts
  - BGA2 / Micro-PGA2

FriendTech
Gaming upgrades & more.

Categories
- DreamX (Gaming)
- DreamX (Entertainment)
- Xbox System Upgrades
- Xbox Upgrade Peripherals
- Xbox Skins
- Gaming-Fever

Articles
New Articles (0)
All Articles (5)
DreamX Comparison Charts (2)
Xbox Upgrades & Trade-In Rebates (2)
Gaming-Fever (1)

What's New?

USB Conversion Cable for Xbox
$4.95

Quick Find

DreamX-1480

$579.00

Excellent as a High-End Media Center, Games Emulator, and for Linux on the Xbox

Click to enlarge

(1) **New Intel 1400MHz Celeron CPU**
(2) 1480/740MHz Switchable Speed
(3) **Memory Upgraded to 128MB**
(4) **Pre-Modded (with Media Key installed)**
(5) **120GB Hard Drive + Media Center software**
(6) DreamX HDTV and A/V Cable included, for Component and S-Video Support
(7) Dolby 5.1 and DTS 5.1 Surround Sound with Optical Fiber Audio Port
(8) DVD Remote Control + USB Receiver
(9) Xbox to USB Converter (for connecting an optional wireless keyboard & mouse)
(10) Extra heatsink and heat conductive chain for improved heat dissipation
(11) Rubber Pedestal Feet
(12) New External Skin

200GB HDD Upgradability*
No support for Xbox Live!**
DVD movie playback requires XBMC***

Includes $100 Trade-In Rebate Coupon

Features Comparison Chart

Shopping Cart
0 items

FAQ Categories
DreamX (13)
Xbox System Upgrades (7)
FriendTech MCE (2)
Shipping (1)
Support & Service (5)

Latest FAQs
What will a modchip upgrade allow me to do?
How do I back up my games to the DreamX hard disk drive?
Do you offer a 512MB memory upgrade for retail Xboxes?

Notifications
Notify me of updates to **DreamX-1480**

Tell A Friend
Tell someone you know about this product.


http://www.upgrade123.com/catalog/product_info.php?products_id=65
Go
13 captures
10 Oct 2004 - 19 Dec 2021
SEP
OCT
10
2004
DEC
2003
2005
About this capture
FriendTech
Gaming upgrades & more.
Categories
DreamX (Gaming)
DreamX (Entertainment)
Xbox System Upgrades
Xbox Upgrade Peripherals
Xbox Skins
Gaming-Fever
Articles
New Articles (0)
All Articles (5)
DreamX Comparison Charts (2)
Xbox Upgrades & Trade-In Rebates (2)
Gaming-Fever (1)
What's New?
USB Conversion Cable for Xbox
$4.95
Quick Find
DreamX-1480
$579.00
Excellent as a High-End Media Center, Games Emulator, and for Linux on the Xbox
(1) New Intel 1400MHz Celeron CPU
(2) 1480/740MHz Switchable Speed
(3) Memory Upgraded to 128MB
(4) Pre-Modded (with Media Key installed)
(5) 120GB Hard Drive + Media Center software
(6) DreamX HDTV and A/V Cable included, for Component and S-Video Support
(7) Dolby 5.1 and DTS 5.1 Surround Sound with Optical Fiber Audio Port
(8) DVD Remote Control + USB Receiver
Click to enlarge
Shopping Cart
0 items
FAQ Categories
DreamX (13)
Xbox System Upgrades (7)
FriendTech MCE (2)
Shipping (1)
Support & Service (5)
Latest FAQs
What will a modchip
Trade-In Rebate Coupon
Tell A Friend
Tell someone you know about this product.
(1) New Intel 1400MHz Celeron CPU
(2) 1480/740MHz Switchable Speed
(3) Memory Upgraded to 128MB

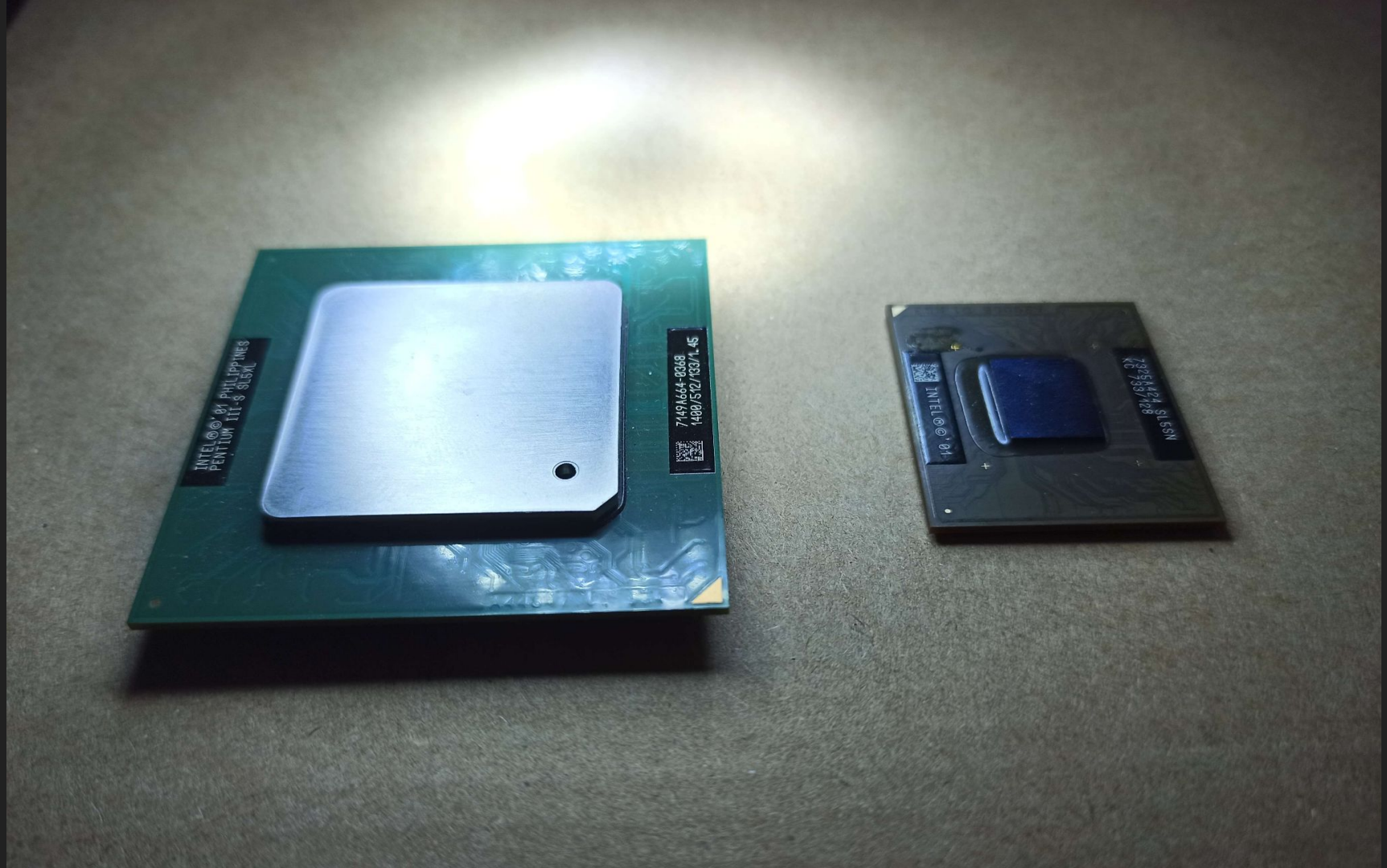
Xbox CPU Comparison

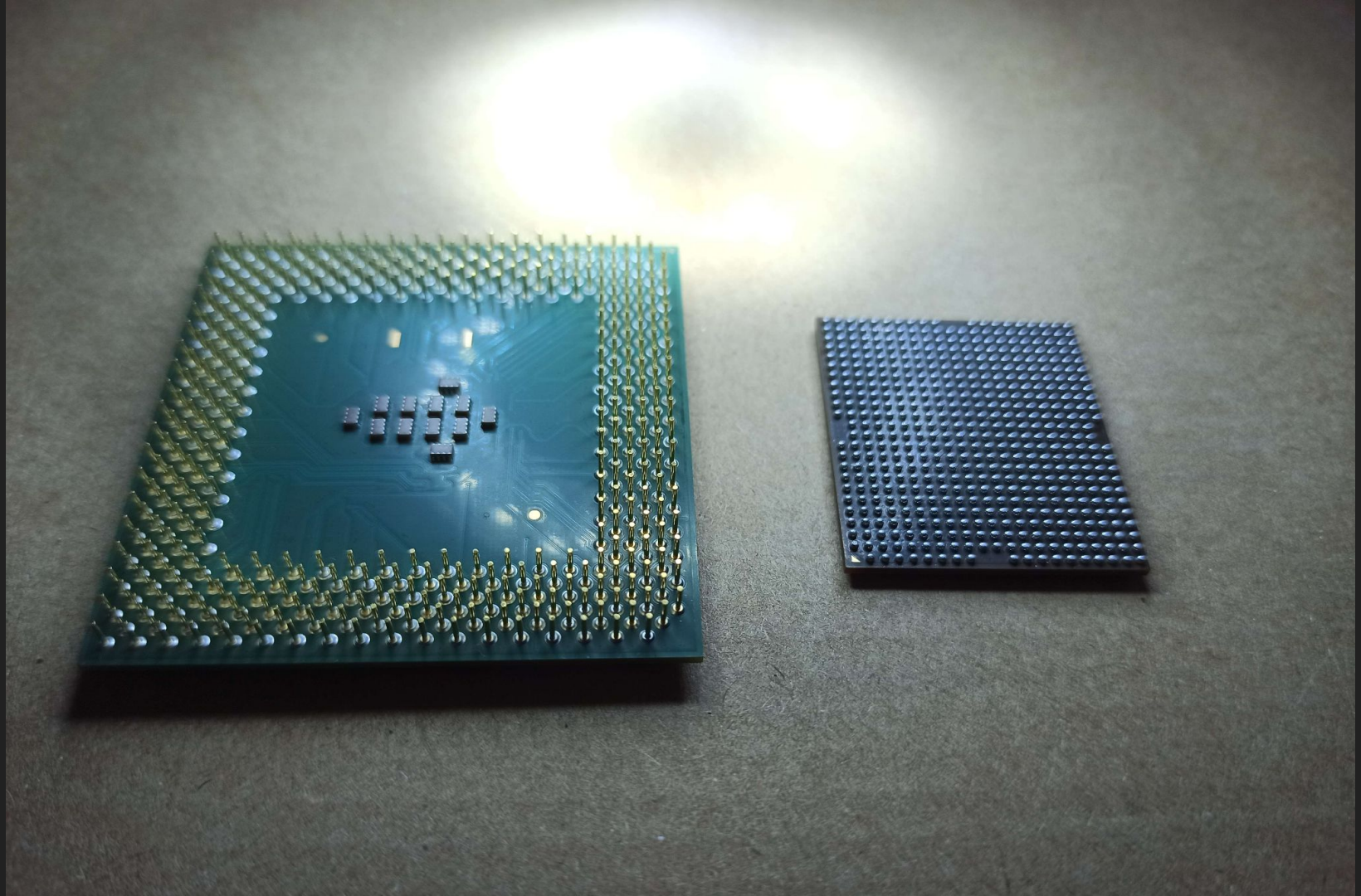
- **Retail Xbox CPU - 180nm Coppermine (SL5SN)**
  - 733mhz core
  - 133mhz fsb
  - 128kb L2 cache
  - 1.7 volts
  - BGA2 / Micro-PGA2

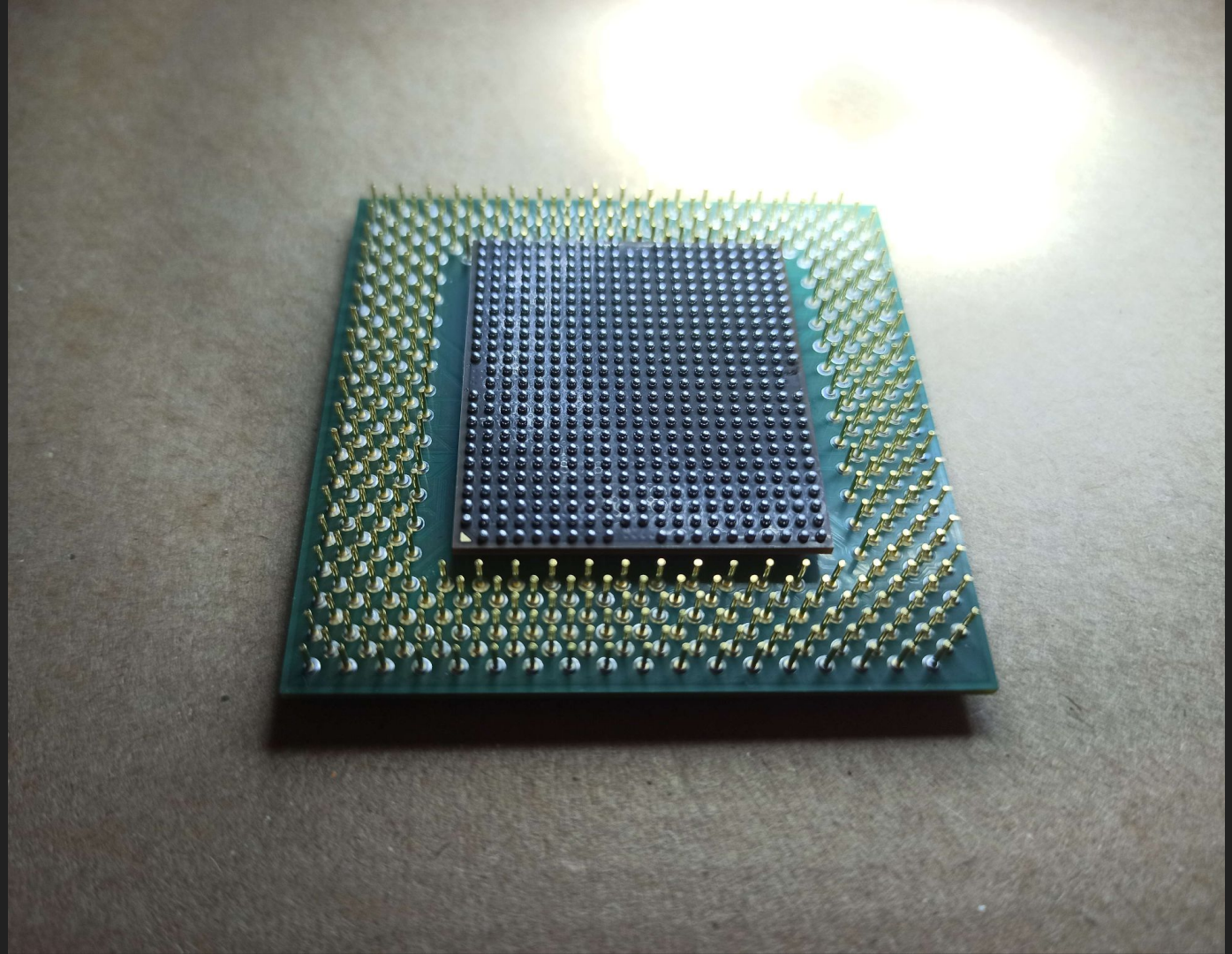
- **Upgraded CPU - 130nm Tualatin-S (SL6BY)**
  - 1400mhz core (+90%)
  - 133mhz fsb
  - 512kb L2 cache (+300%)
  - 1.45 volts
  - Socket 370 / PGA370

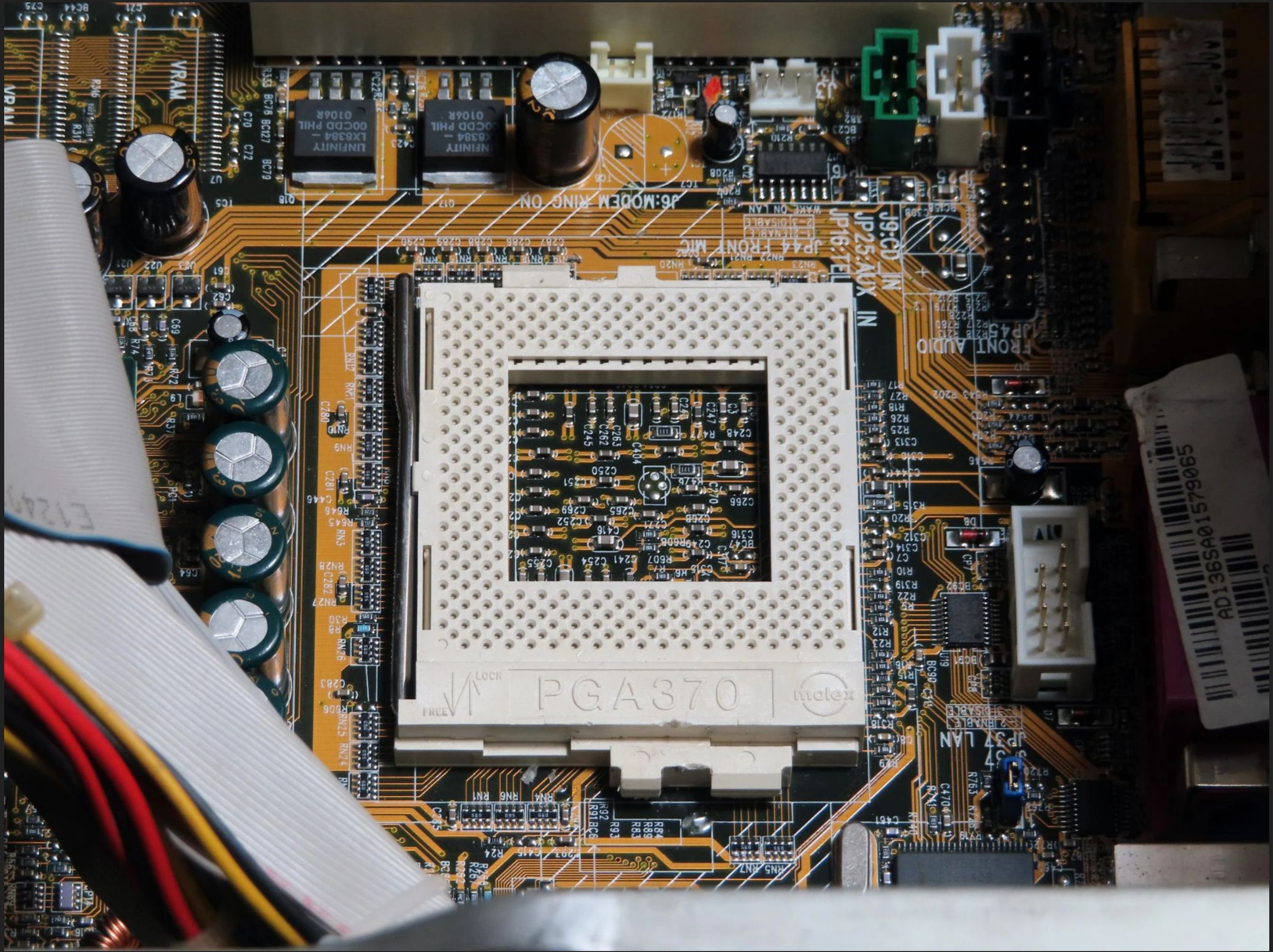
Xbox CPU Comparison

- **Retail Xbox CPU - 180nm Coppermine (SL5SN)**
  - 733mhz core
  - 133mhz fsb
  - 128kb L2 cache
  - 1.7 volts
  - BGA2 / Micro-PGA2
- **Upgraded CPU - 130nm Tualatin-S (SL6BY)**
  - 1400mhz core (+90%)
  - 133mhz fsb
  - 512kb L2 cache (+300%)
  - 1.45 volts
  - Socket 370 / PGA370


INTEL©'97 PHILIPPINES
PENTIUM III-S SL5XE
7149A664-0368
1400/512/133/1.45
INTEL©'01
SL5SN






PGA370
molex


PGA370
molex
INTEL®©'01 MALAY
900/128/100/1.75V
Q147A759-0242
CELERON SL633
JP37 LAN
AUDIO
JP44 FRONT MIC
WAKE ON LAN
J6:MODEM
LINFINITY
LX8384 —
00CDD PHIL
0106R

BGA2 → PGA370 CPU Interposer

US 20050282621A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2005/0282621 A1**

(43) **Pub. Date: Dec. 22, 2005**

Hu

(54) **CPU UPGRADING ADAPTER FOR A MICROSOFT XBOXTM GAME MACHINE**

(76) Inventor: **Ta-Shin Hu**, Sanchung City (TW)

Correspondence Address:
NIKOLAI & MERSEREAU, P.A.
900 SECOND AVENUE SOUTH
SUITE 820
MINNEAPOLIS, MN 55402 (US)

(21) Appl. No.: **10/645,383**

(22) Filed: **Aug. 21, 2003**

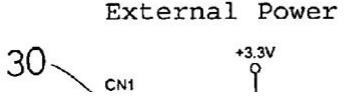
Publication Classification

(51) **Int. Cl.**[7] **A63F 9/24**; G06F 19/00

(52) **U.S. Cl.** **463/23**

(57) **ABSTRACT**

A CPU upgrading adapter for an XBOX game machine is composed of a circuit board on which a socket frame and a switched are electrically connected. When the original CPU is removed from a motherboard of the XBOX game machine, the CPU upgrading adapter is then mounted on the motherboard to receive a new high speed upgrading CPU. Such an upgrading CPU is chosen from an Intel© Pentium-III-S™ CPU, a Pentium-III™ CPU or a Celeron™ CPU.



"CPU upgrading adapter for a Microsoft XboxTM game machine, Patent # US 2005 / 0282621 A1"

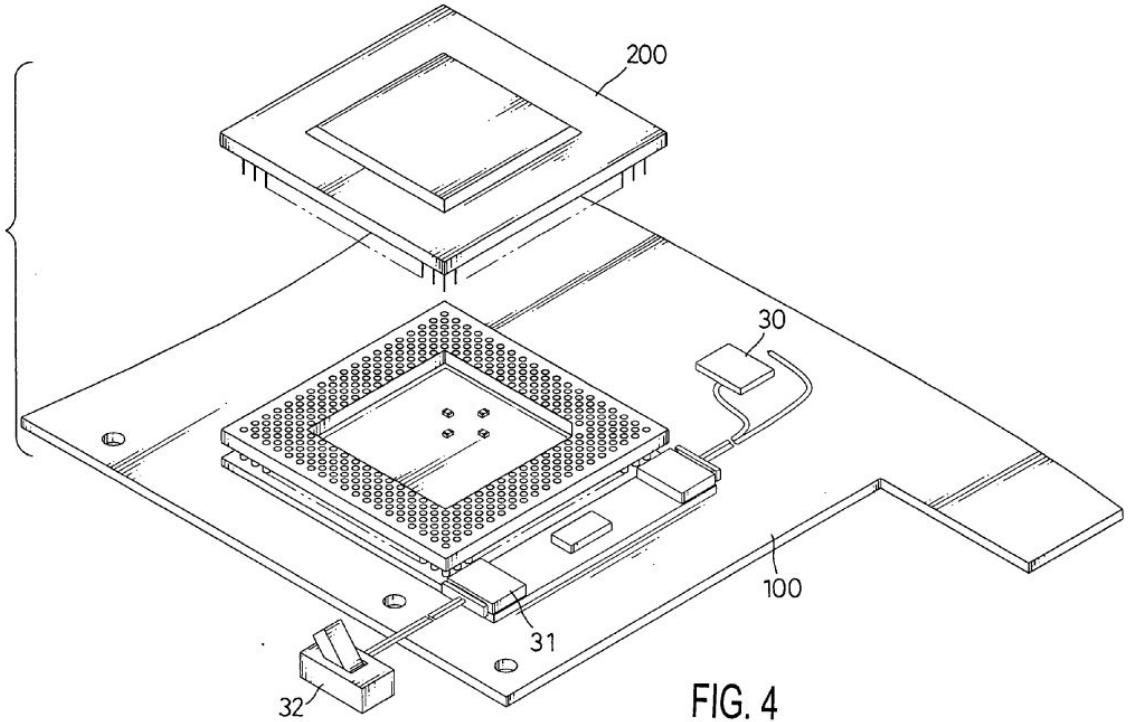


FIG. 4

"CPU upgrading adapter for a Microsoft XboxTM game machine, Patent # US 2005 / 0282621 A1" (Page 4)

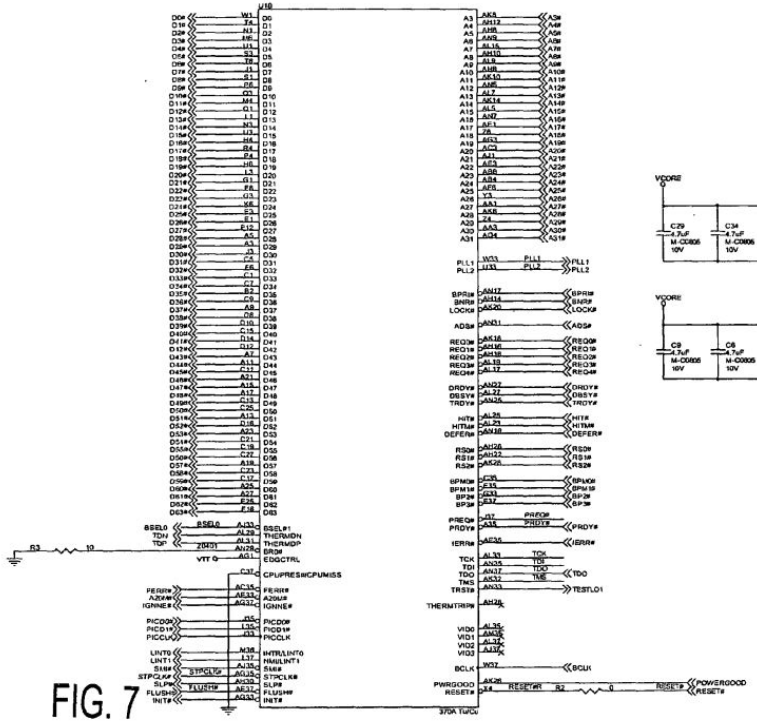


FIG. 7

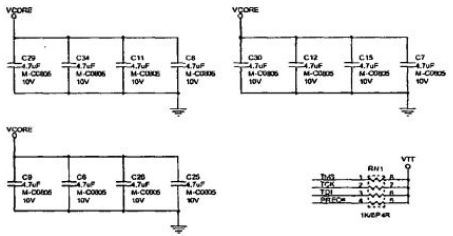
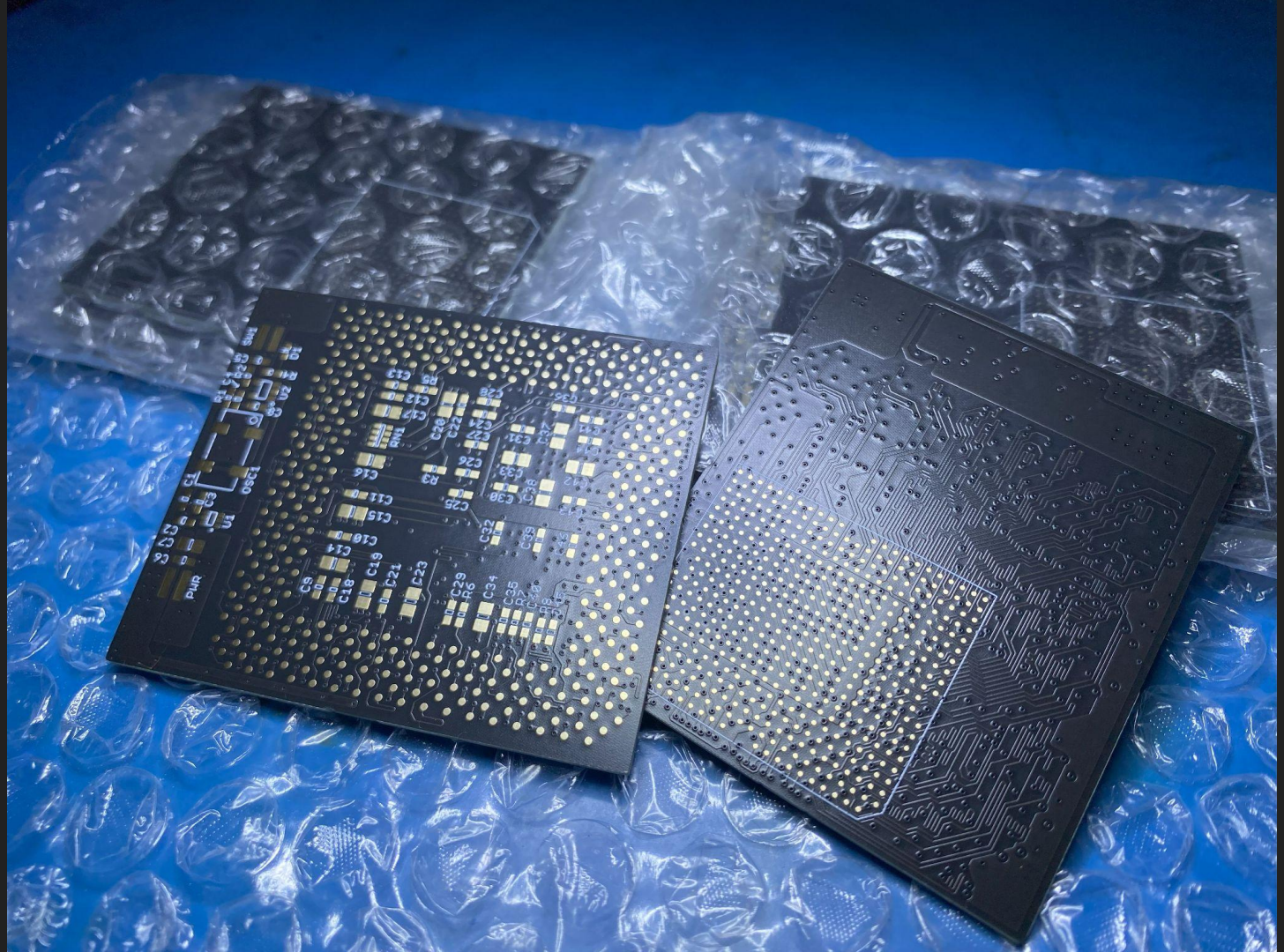
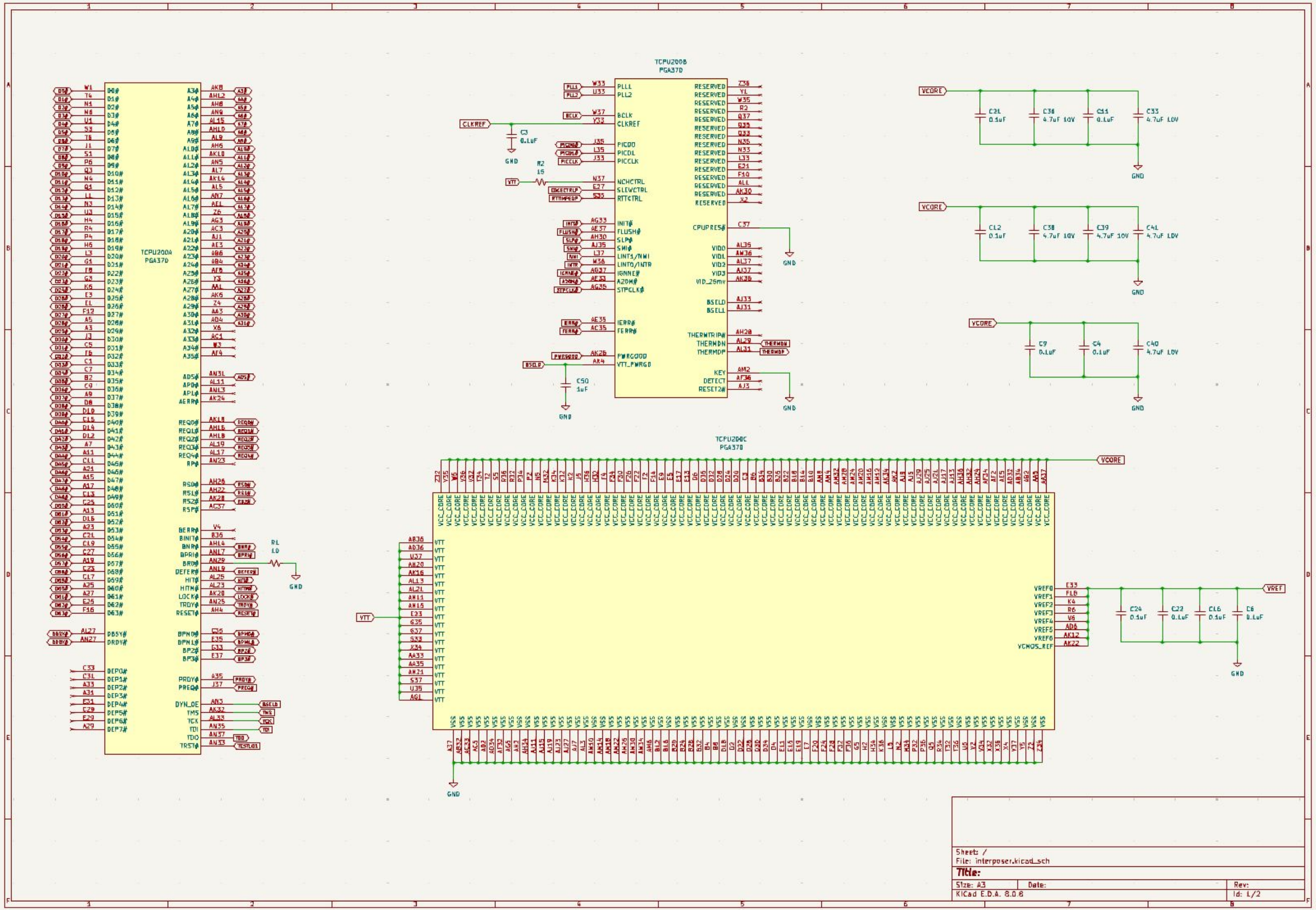
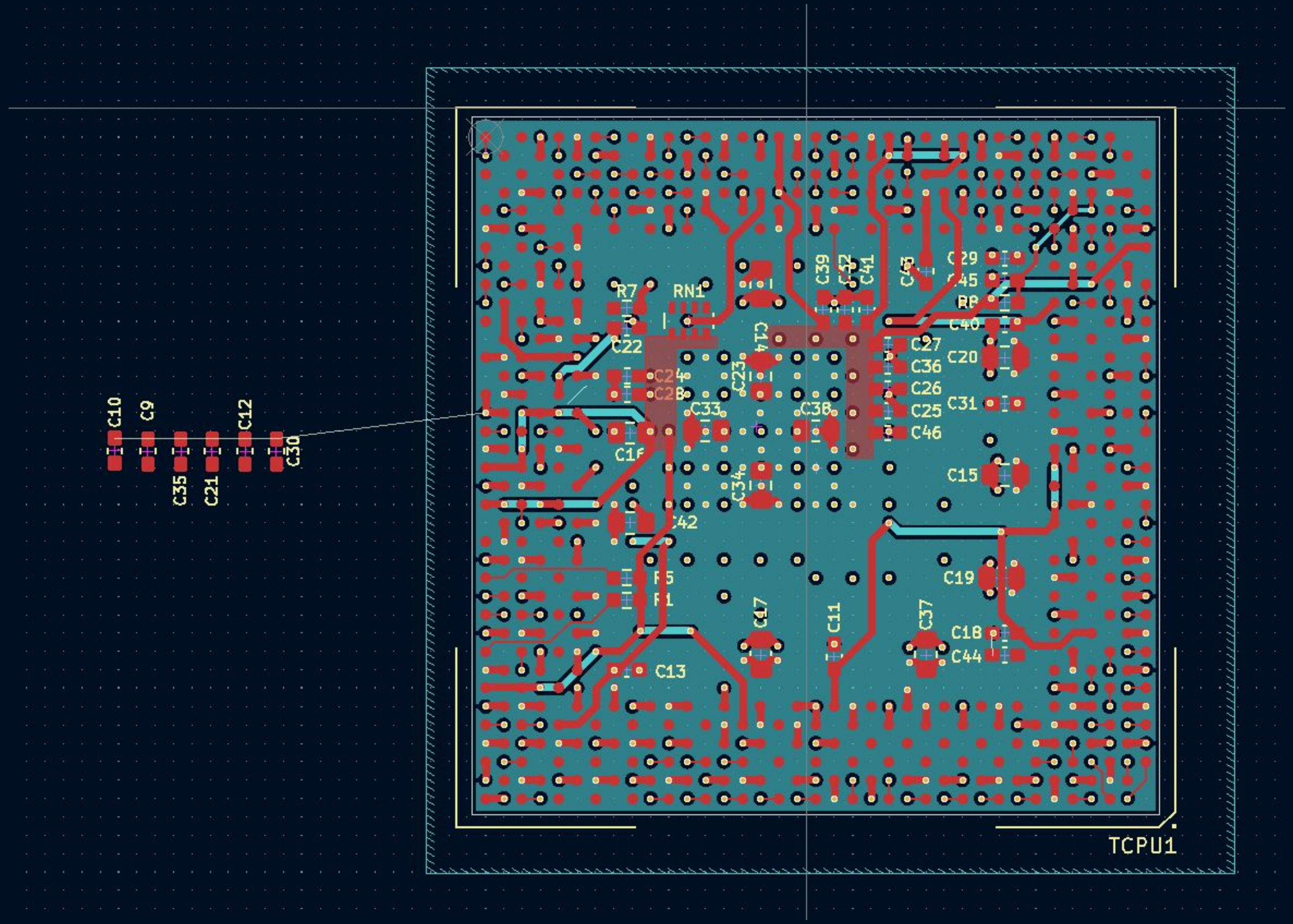


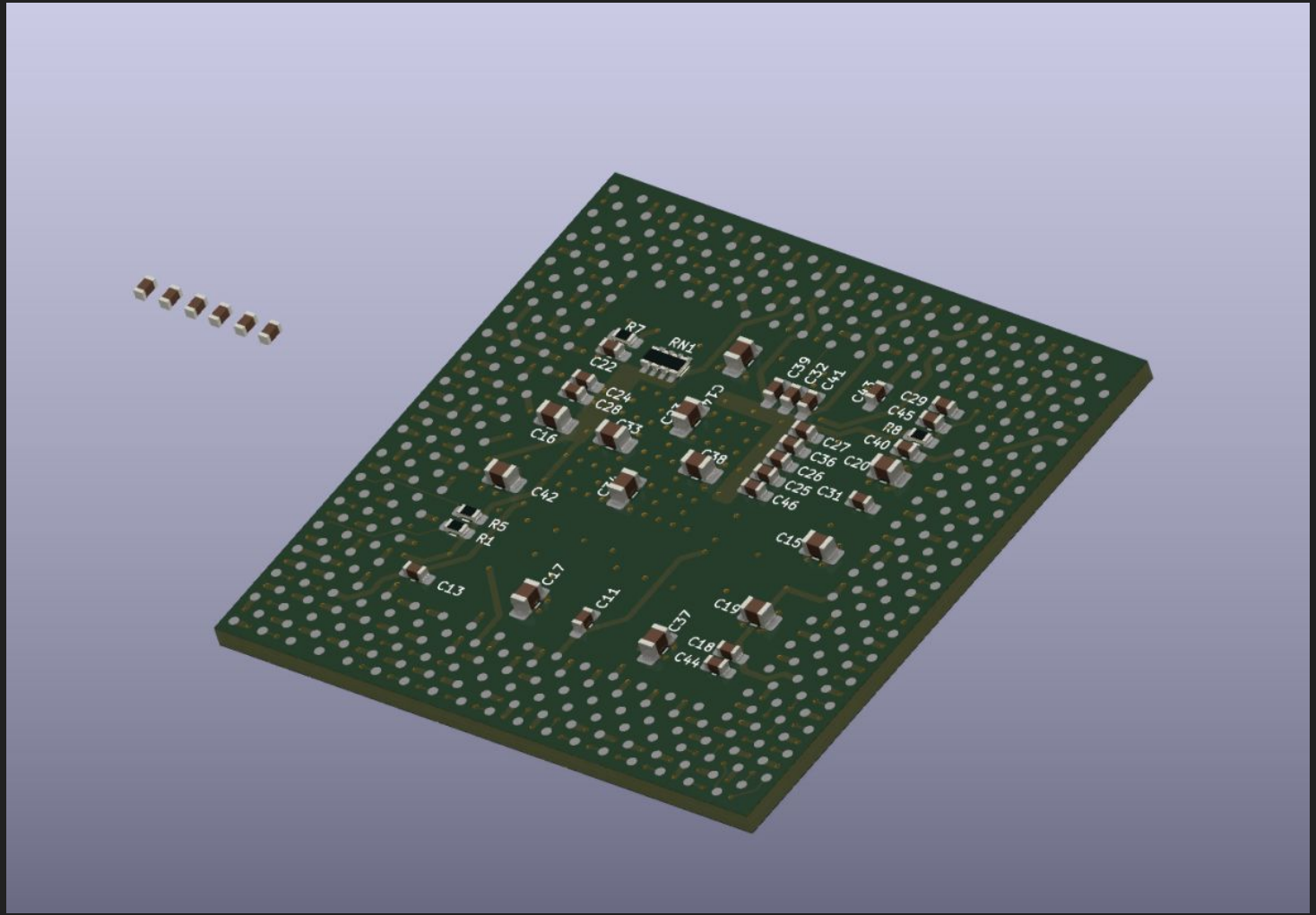
FIG. 12

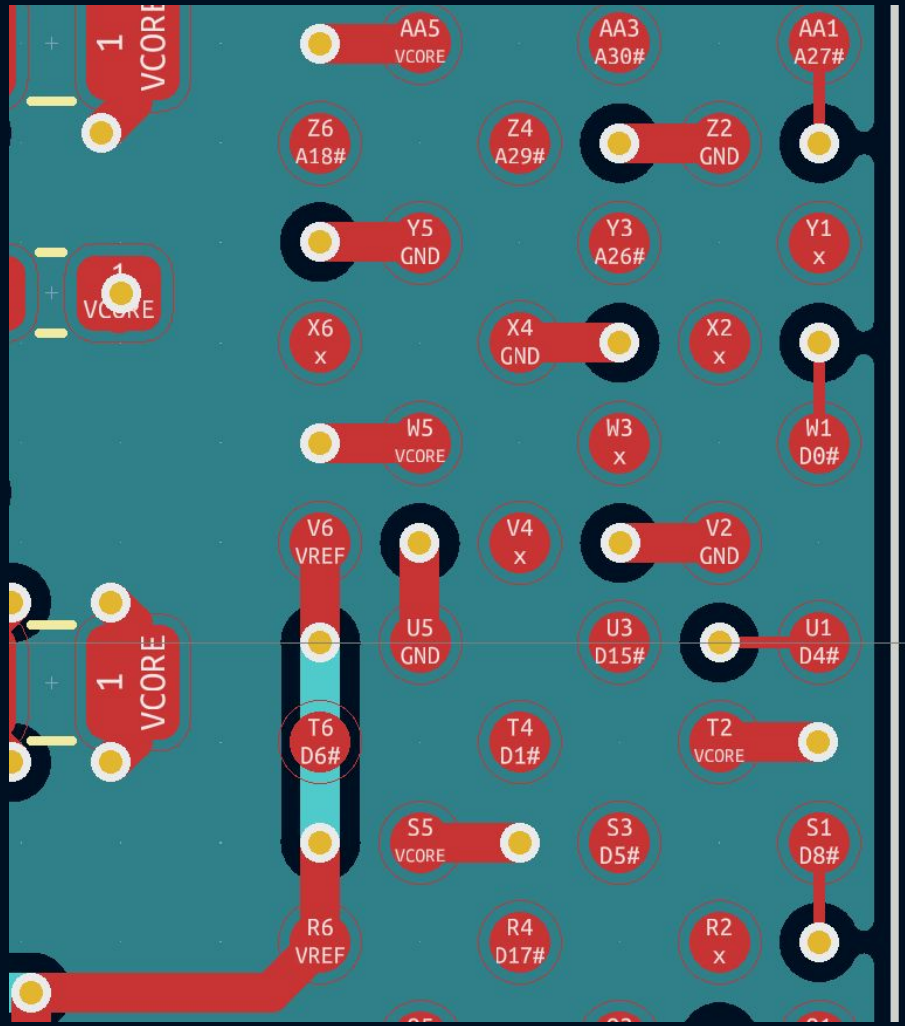
"CPU upgrading adapter for a Microsoft XboxTM game machine, Patent # US 2005 / 0282621 A1" (Page 7)


PWR


TCPU200A
PGA370
TCPU200B
PGA370
TCPU200C
PGA370
CLKREF
VTT
VCORE
VREF
GND
C31 0.1uF
C36 4.7uF 10V
C11 0.1uF
C33 4.7uF 10V
C12 0.1uF
C38 4.7uF 10V
C39 4.7uF 10V
C41 4.7uF 10V
C9 0.1uF
C4 0.1uF
C40 4.7uF 10V
C3 0.1uF
C50 1uF
C24 0.1uF
C22 0.1uF
C16 0.1uF
C6 0.1uF
R1 10
R2 15
Sheet: /
File: interposer.kicad_sch
Title:
Size: A3
Date:
Rev:
KiCad E.D.A. 8.0.8
Id: 1/2


C10
C9
C12
C35
C21
C30
R7
RN1
C22
C24
C28
C33
C23
C14
C39
C12
C41
C43
C29
C45
RP
C40
C27
C36
C26
C25
C46
C20
C31
C38
C16
C15
C34
C42
R5
R1
C19
C17
C11
C37
C18
C44
C13
TCPU1


R7
RN1
C22
C24
C28
C16
C42
R5
R1
C13
C17
C41
C37
C18
C44
C19
C15
C46
C25
C26
C36
C27
C20
C40
R8
C45
C29
C31


AA5
VCORE
AA3
A30#
AA1
A27#
Z6
A18#
Z4
A29#
Z2
GND
Y5
GND
Y3
A26#
Y1
x
X6
x
X4
GND
X2
x
W5
VCORE
W3
x
W1
D0#
V6
VREF
V4
x
V2
GND
U5
GND
U3
D15#
U1
D4#
T6
D6#
T4
D1#
T2
VCORE
S5
VCORE
S3
D5#
S1
D8#
R6
VREF
R4
D17#
R2
x
1
VCORE

timing analysis. However, simulation results at the device pins may be used later to correlate simulation performance against actual system measurements.

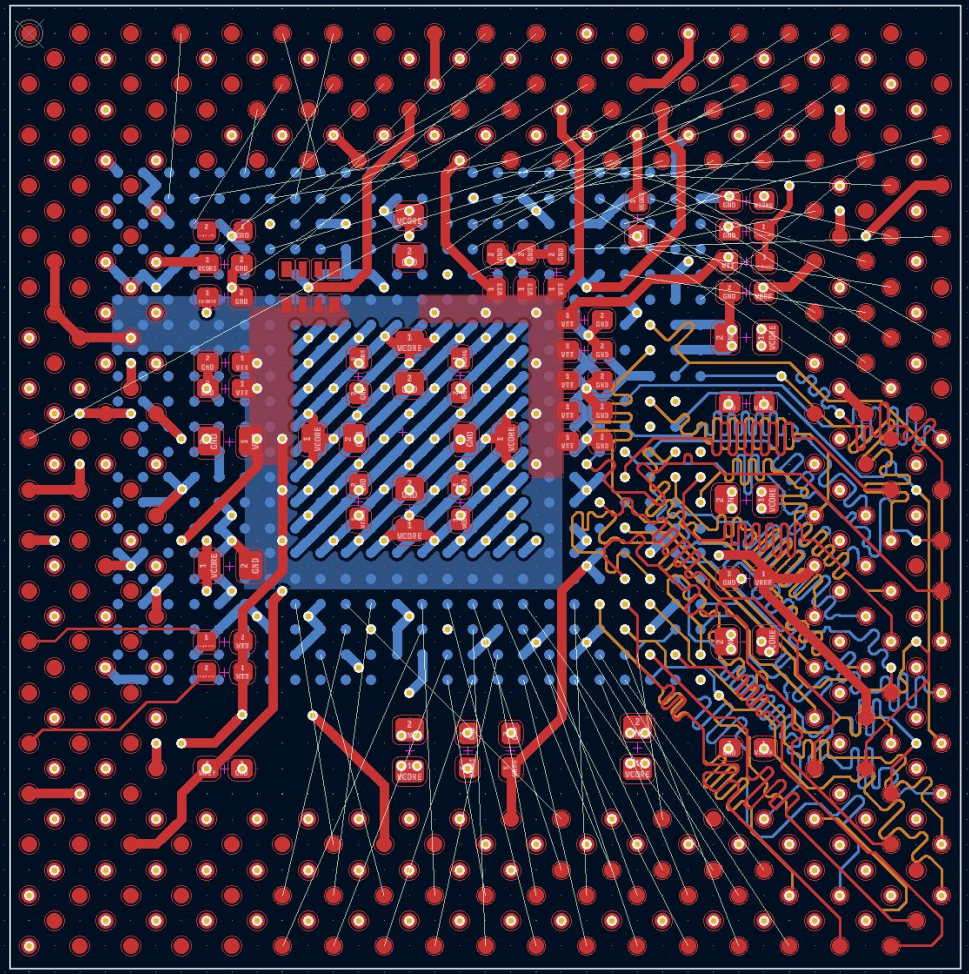
Intel® Pentium® III Processor with 512KB L2 Cache DP I/O buffer models are available from the Intel Developer website.

3.6 Trace Routing

The following guidelines should be followed when routing the AGTL host bus signal traces:

- Traces should have an impedance of 60Ω +/- 15%
- The nominal trace width should be 5 mils.
- The L0 and L1 lengths in Table 3-5 should be matched to within 0.25 inches.
- Minimize the number of vias and layer transitions.

3.7 Layout Rules for AGTL Signals



timing analysis. However, simulation results at the device pins may be used later to correlate simulation performance against actual system measurements.

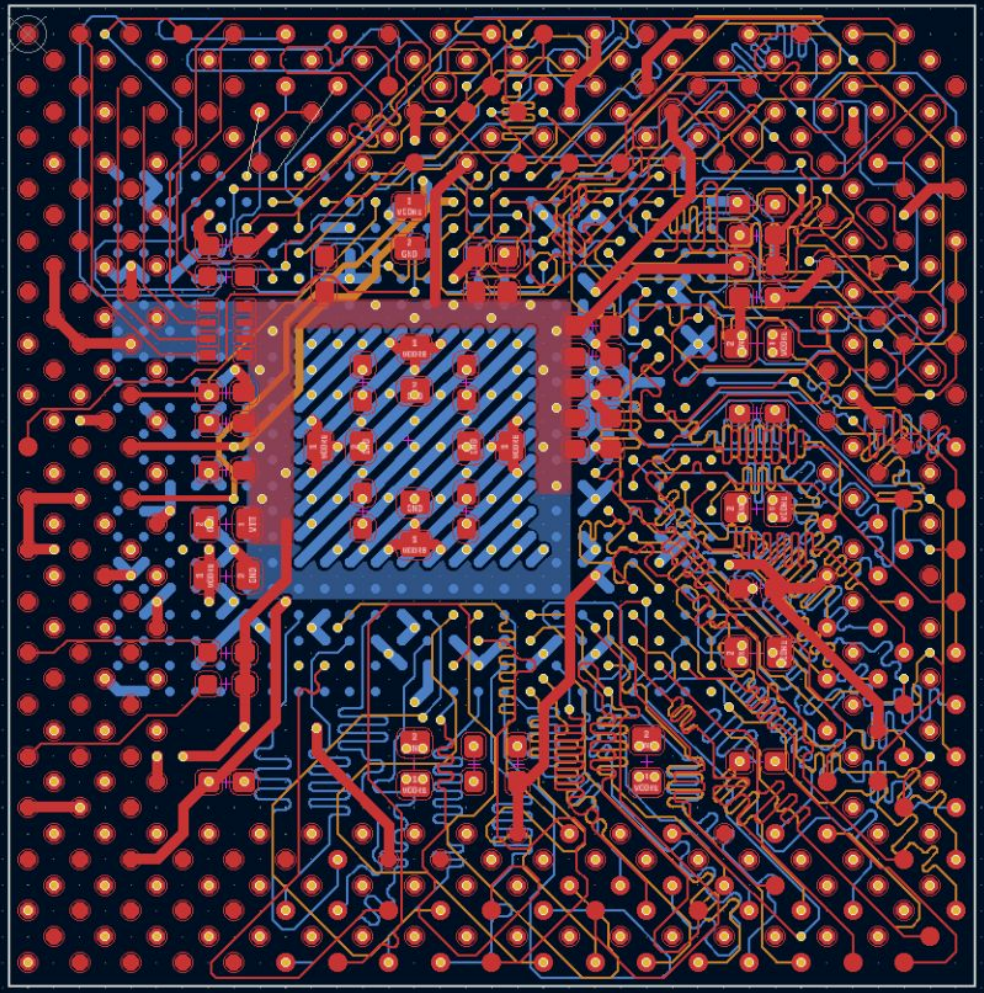
Intel® Pentium® III Processor with 512KB L2 Cache DP I/O buffer models are available from the Intel Developer website.

3.6 Trace Routing

The following guidelines should be followed when routing the AGTL host bus signal traces:

- Traces should have an impedance of 60Ω +/- 15%
- The nominal trace width should be 5 mils.

VTTPWRGD	• Pull-up to VTT through 1 kΩ resistor and connect to VTTPWRGD circuitry. See Section 4.2.6.
VREF [6:0]	• Connect to VREF voltage divider made up of 75 Ω and 150 Ω 1% resistors connected to VTT. Processor VREF must be able to be separate from chipset VREF. • Decoupling Guidelines: —4 ea. (minimum) 0.1 µF in 0603 package placed within 500 mils of VREF pins
VTT	• Connect AH20, AK16, AL13, AL21, AN11, AN15, G35, G37, AD36, AB36, Y34, AA33, AA35, AN21, F23, S33, S37, U35, and U37 to VRM



timing analysis. However, simulation results at the device pins may be used later to correlate simulation performance against actual system measurements.

Intel® Pentium® III Processor with 512KB L2 Cache DP I/O buffer models are available from the Intel Developer website.

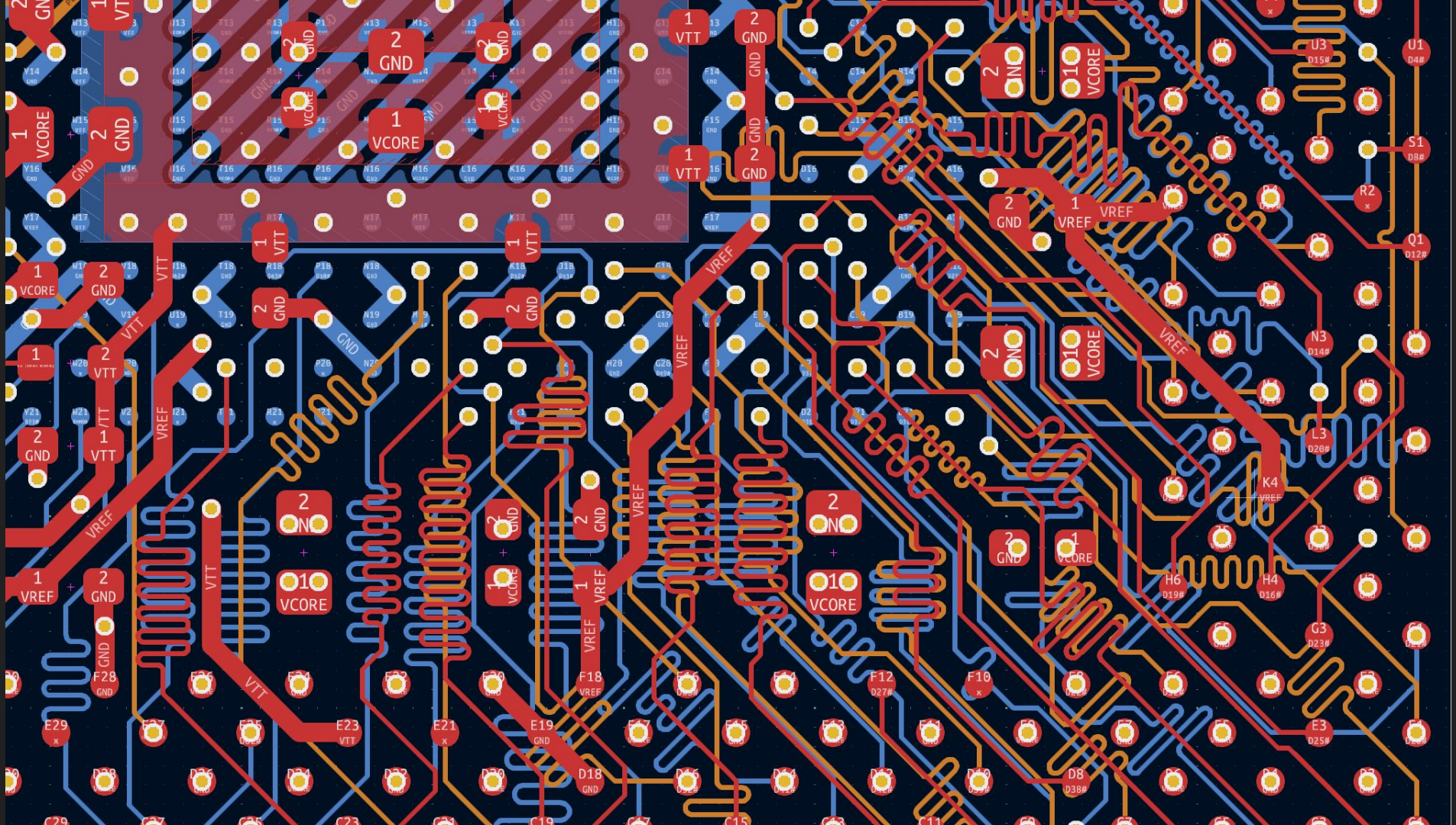
3.6

The following

- Traces s
- The nom

- Plan to place V_{REF} resistor divider pairs at the Intel 440 PCIset components. No V_{REF} divider is needed at the processors as V_{REF} is generated locally on the Pentium II processor from V_{TT}.
- Closely control the characteristic line impedance, Z_0 (50Ω to 80Ω).
- A PCB signal velocity of 1.6 to 2.2 ns/ft should be used.

VTTPWR	Using a PWRGD timings the Pe analog 50 Ω 1% le to be each ag
VREF [6	—4 ea. (minimum) 0.1 µF in 0603 package placed within 500 mils of VREF pins
VTT	• Connect AH20, AK16, AL13, AL21, AN11, AN15, G35, G37, AD36, AB36, Y34, AA33, AA35, AN21, F23, S33, S37, U35, and U37 to VRM


VCORE
VTT
VREF
GND

package, shared by 13 to 19 resistors (for 14- and 20-pin components). These packages generally have too much inductance to maintain the voltage/current needed at each resistive load. Intel recommends using discrete resistors, resistor networks that have separate power/ground pins for each resistor, or working with a resistor network vendor to obtain resistor networks that have acceptable characteristics.

5.0. MORE DETAILS AND INSIGHTS

5.1. Textbook Timing Equations

The textbook equations used to calculate the propagation rate of a signal in a PCB are the basis for spreadsheet calculations for timing margin. These equations are:

Equation 7. Intrinsic Impedance

$$Z_0 = \sqrt{\frac{L_0}{C_0}}$$

Equation 8. Stripline Intrinsic Propagation Speed

$$S_{0\_STRIPLINE} = 1.017 * \sqrt{\varepsilon_r}$$

Equation 9. Microstrip Intrinsic Propagation Speed

$$S_{0\_MICROSTRIP} = 1.017 * \sqrt{0.475 * \varepsilon_r + 0.67}$$

Equation 10. Effective Propagation Speed

$$S_{EFF} = S_0 * \sqrt{1 + \frac{C_D}{C_0}}$$

Equation 11. Effective Impedance

Equation 12. Distributed Trace Capacitance

$$C_0 = \frac{S_0}{Z_0}$$

Equation 13. Distributed Trace Inductance

$$L_0 = Z_0 * S_0$$

Where (for Equation 7 through Equation 13):

S_0 = The speed of the signal on an unloaded PCB. This is referred to as the board propagation constant.

S_0 MICROSTRIP and S_0 STRIPLINE = The speed of the signal on an unloaded microstrip or stripline trace on the PCB.

Z_0 = The intrinsic impedance of the line and is a function of the dielectric constant (ε_r), the line width, line height and line space from the plane(s). The equations for Z_0 are not included in this document. See the *MECL System Design Handbook* by William R. Blood, Jr. for these equations.

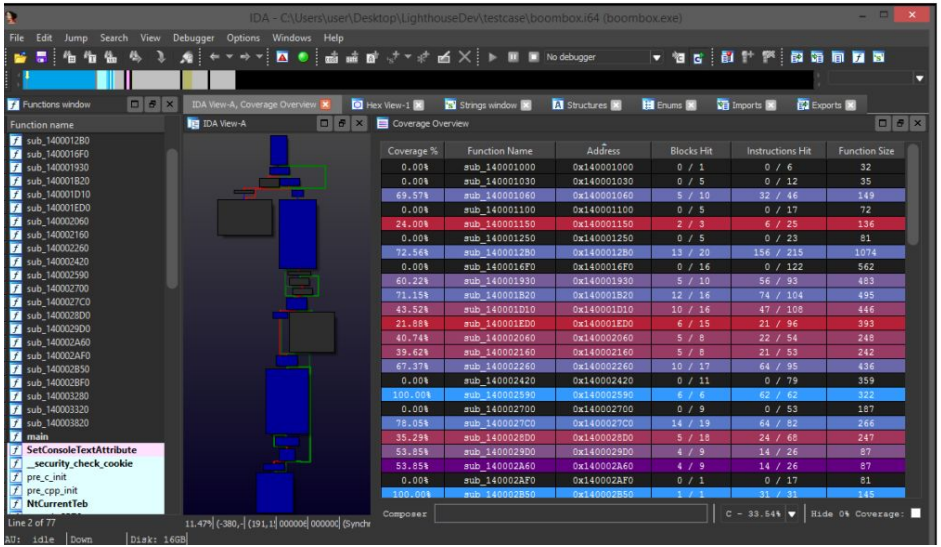
C_0 = The distributed trace capacitance per unit length of the network.

L_0 = The distributed trace inductance per unit length of the network.

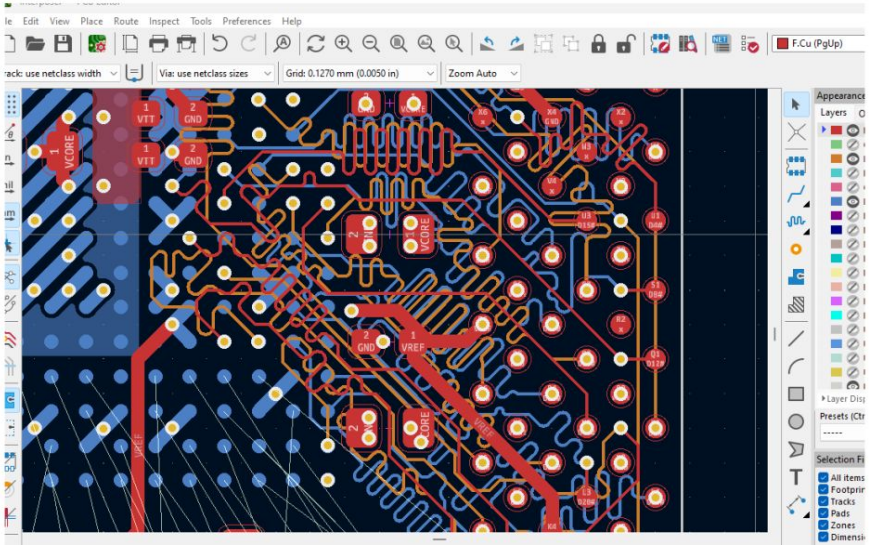
C_D = The sum of the capacitance of all devices and stubs divided by the length of the network's trunk, not including the portion connecting the end agents to the termination resistors.

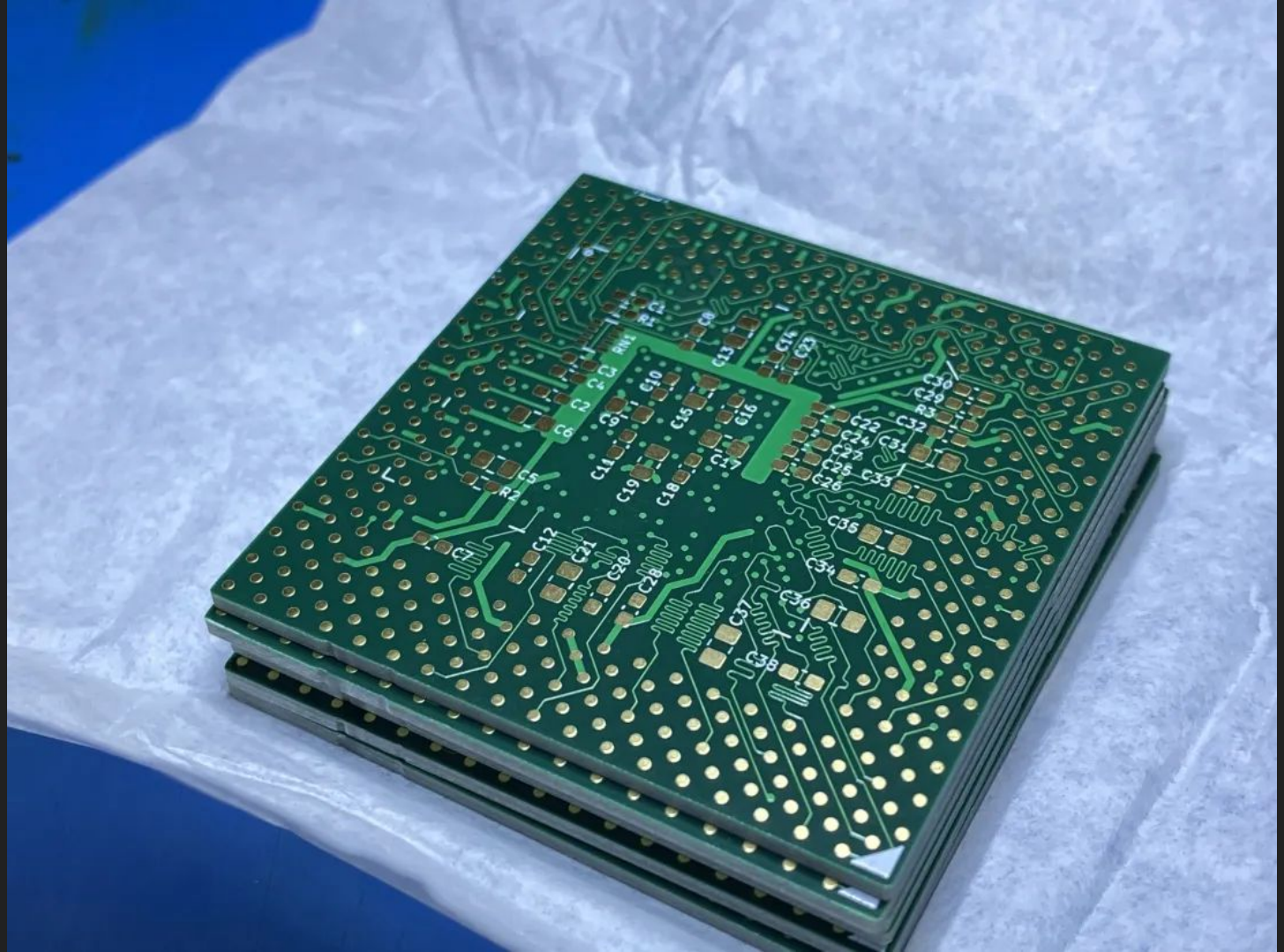
S_{EFF} and Z_{EFF} = The effective propagation constant and impedance of the PCB when the board is "loaded" with the components.

how it started



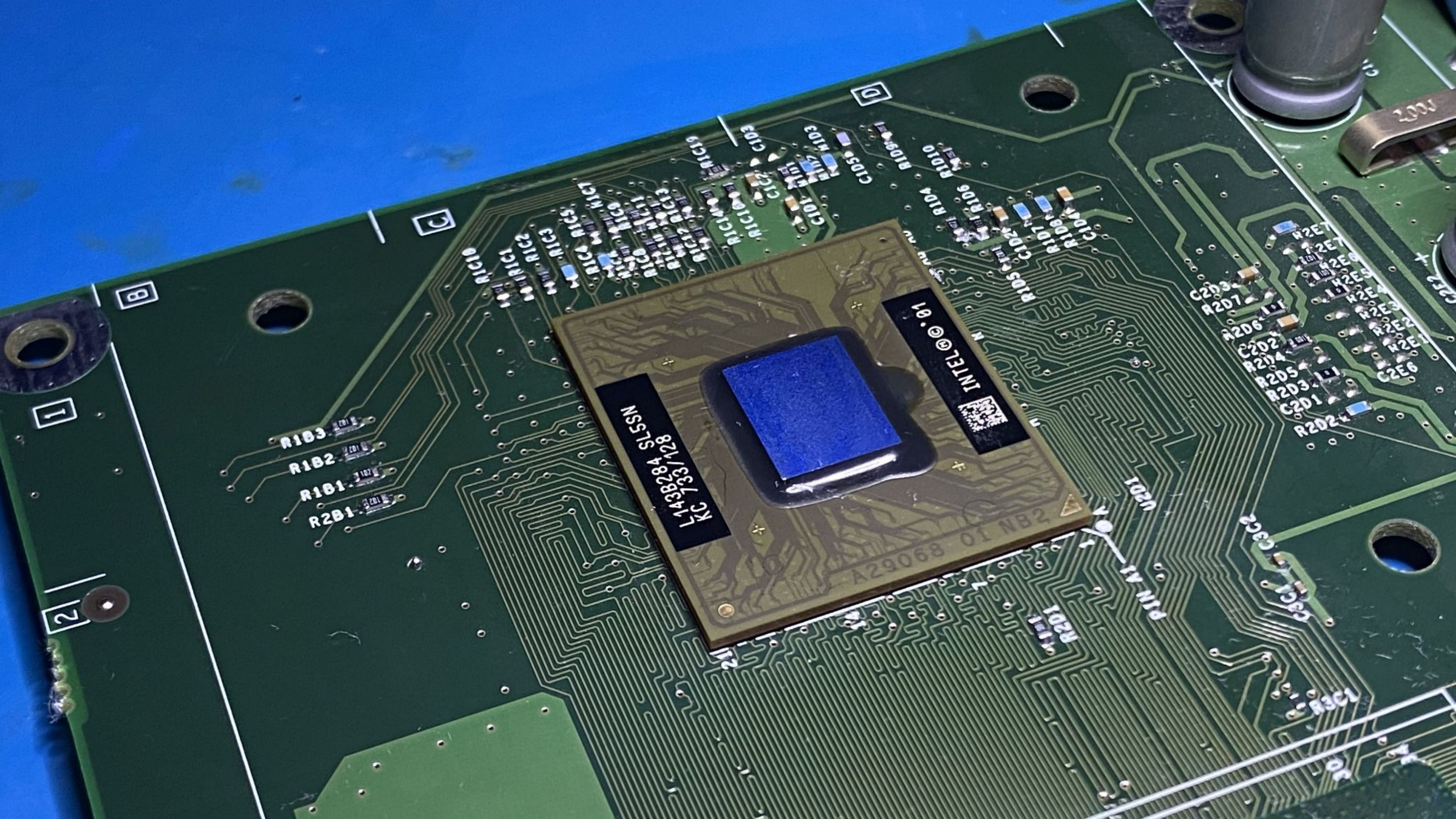
how it's going

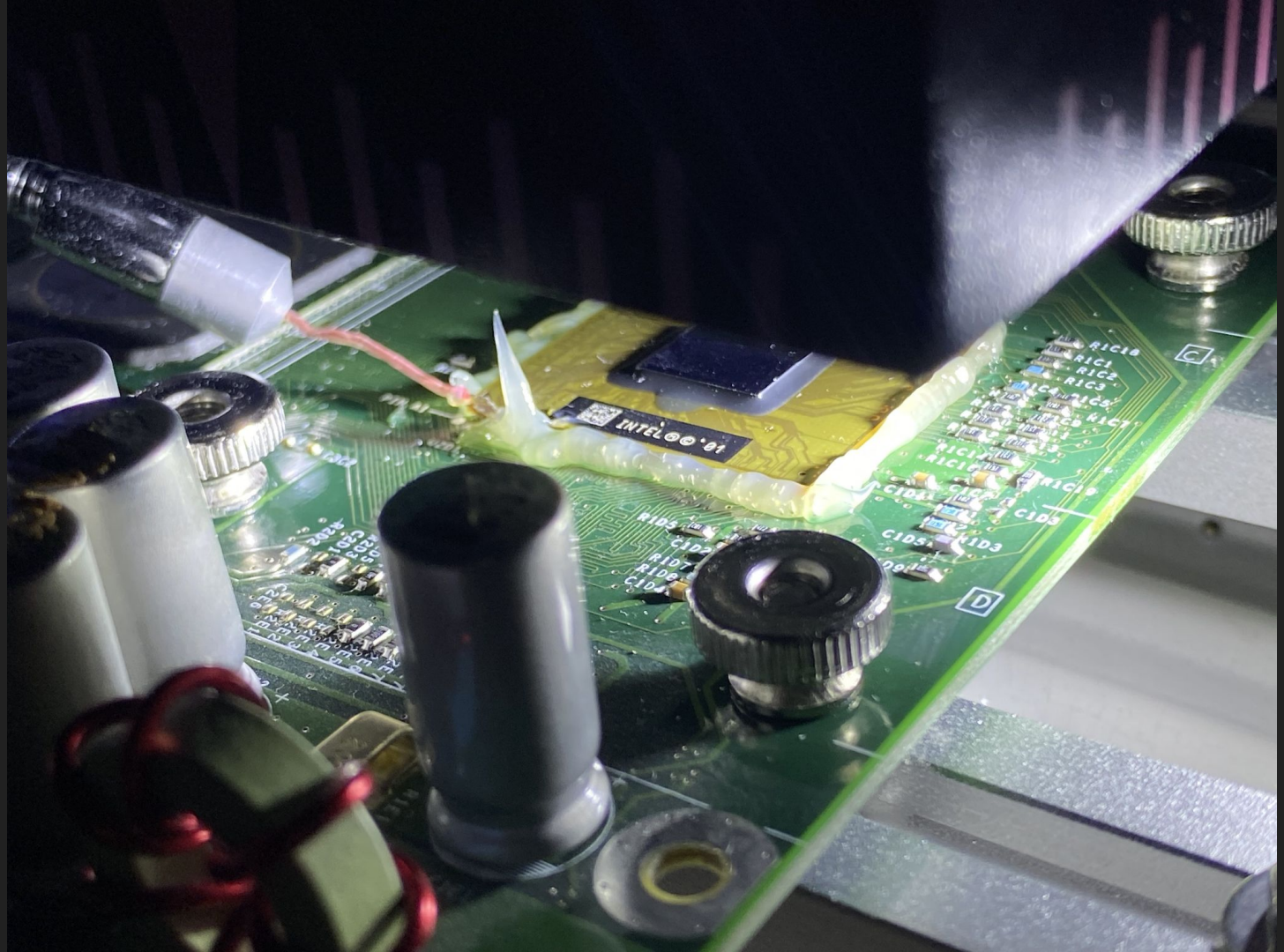


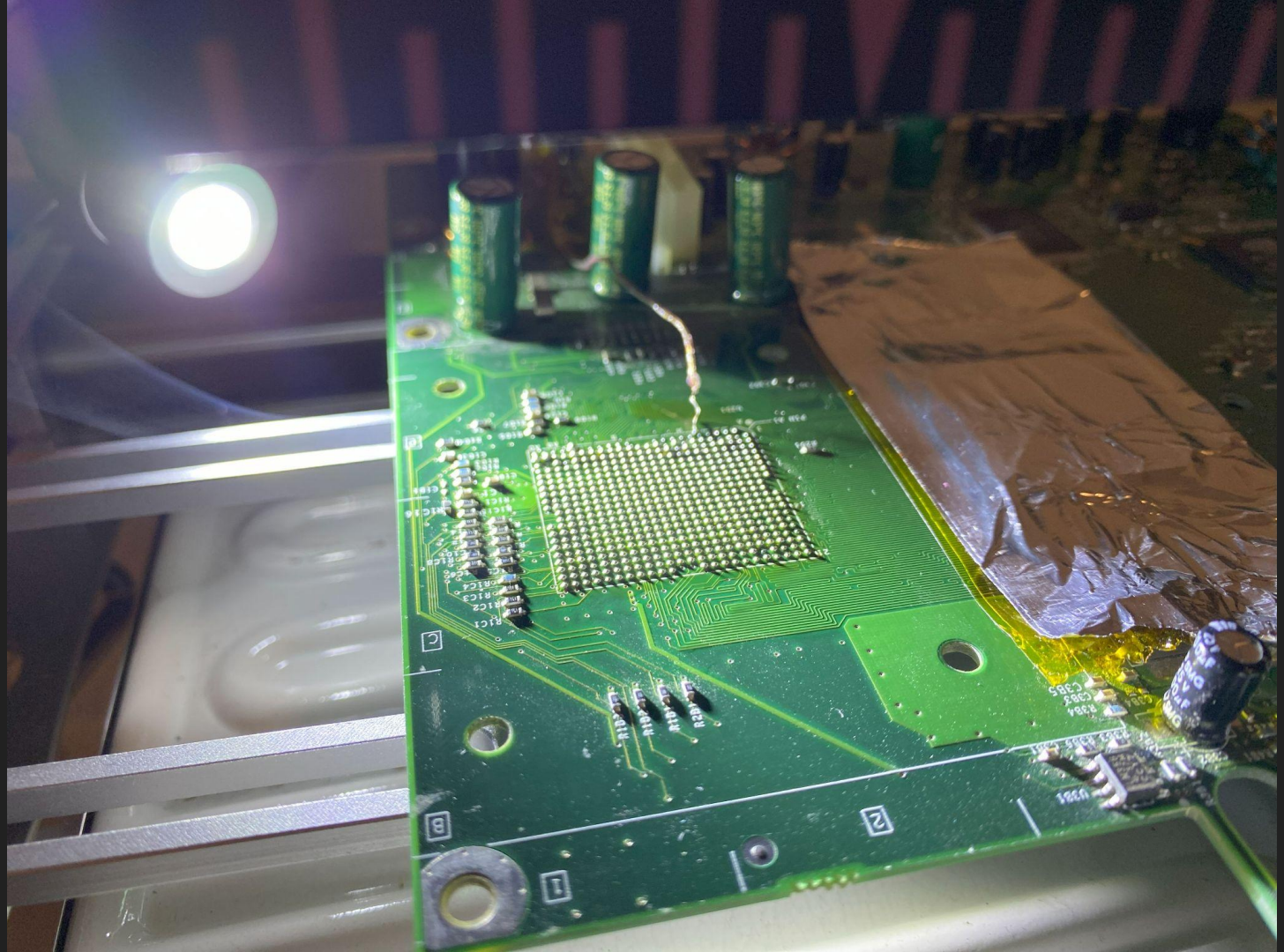

C1
R1
RN1
C8
C13
C16
C3
C30
C29
R3
C32
C22
C24
C31
C27
C25
C33
C26
C35
C34
C36
C37
C38
C2
C4
C10
C9
C15
C16
C6
C14
C17
C5
R2
C19
C18
C7
C12
C21
C20
C28

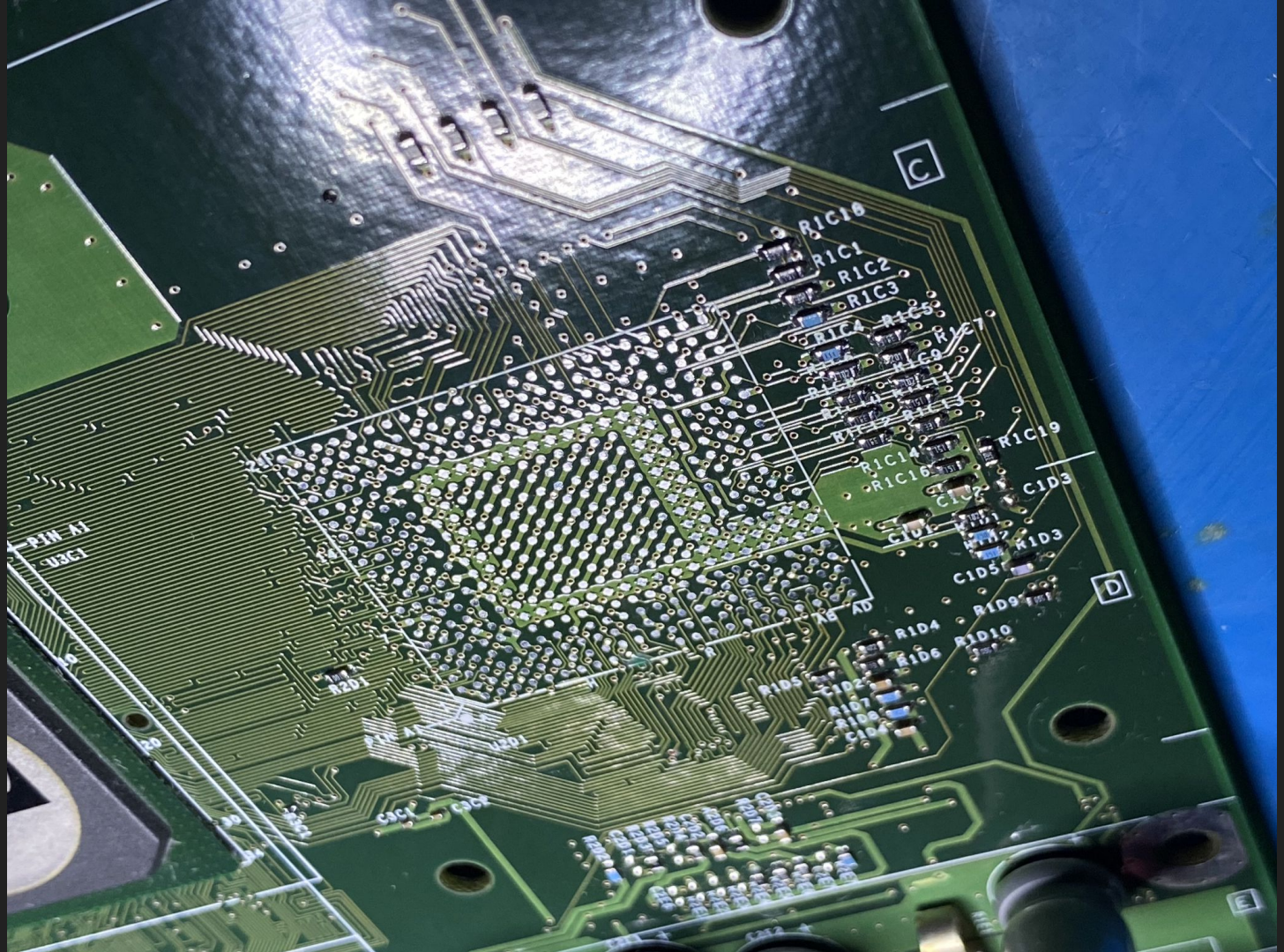
The Install

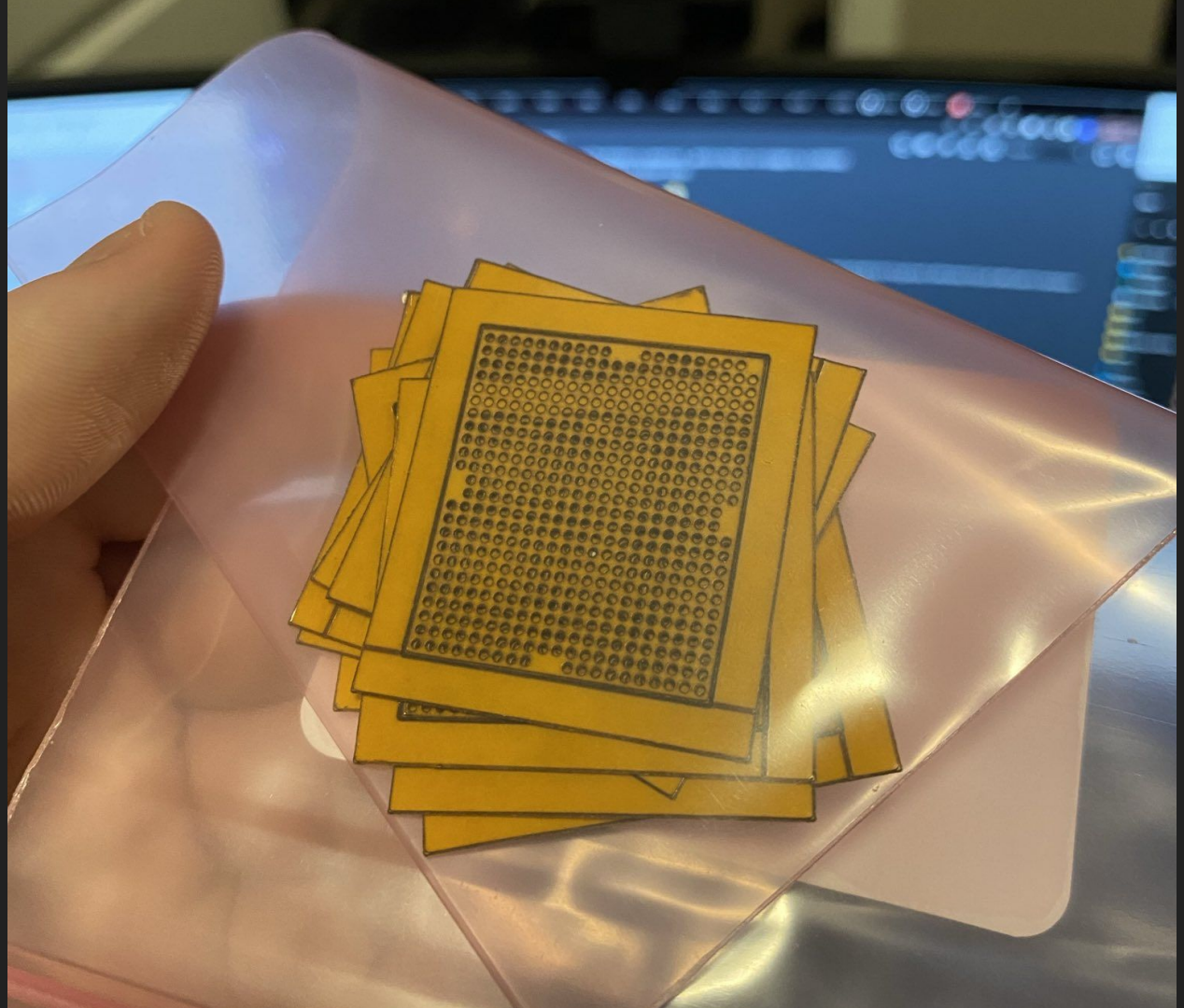

NVIDIA
XGPU
FOCUS
Microsoft

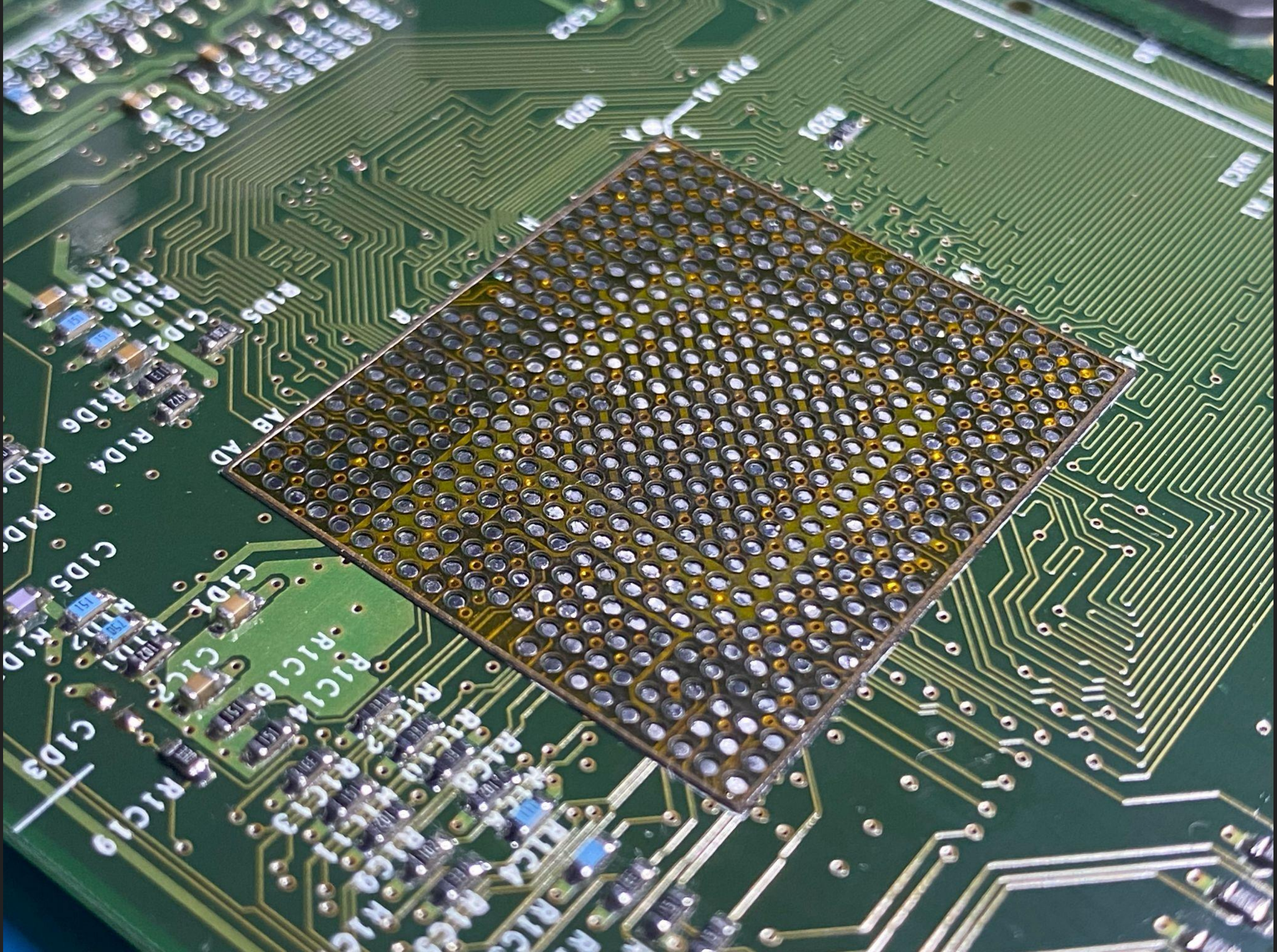

L143B284 SL5SN
KC 733/128
INTEL®©'01
A29068 01 NB2
R1B3
R1B2
R1B1
R2B1
PIN A1
U2D1


INTEL©©'01

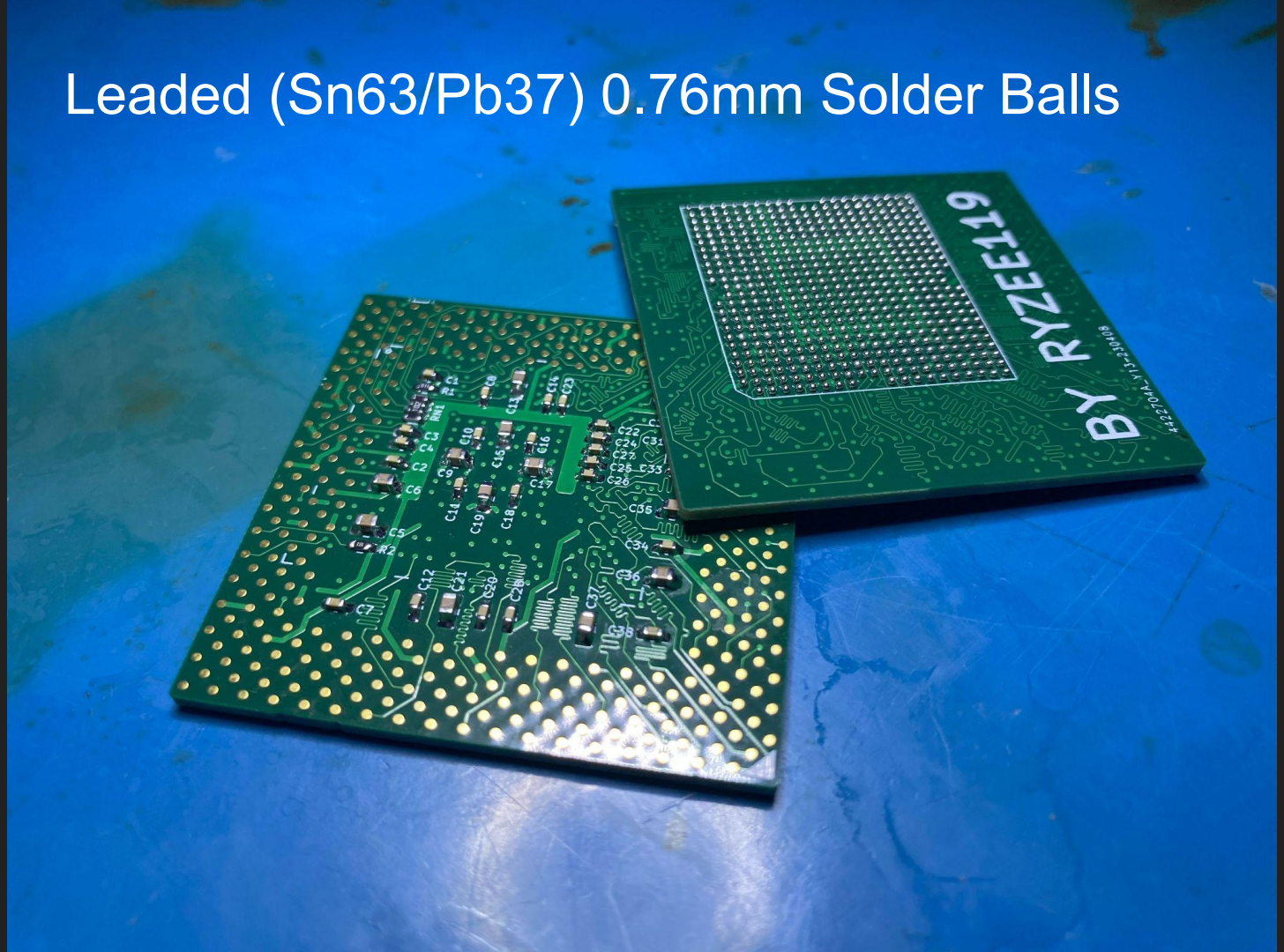


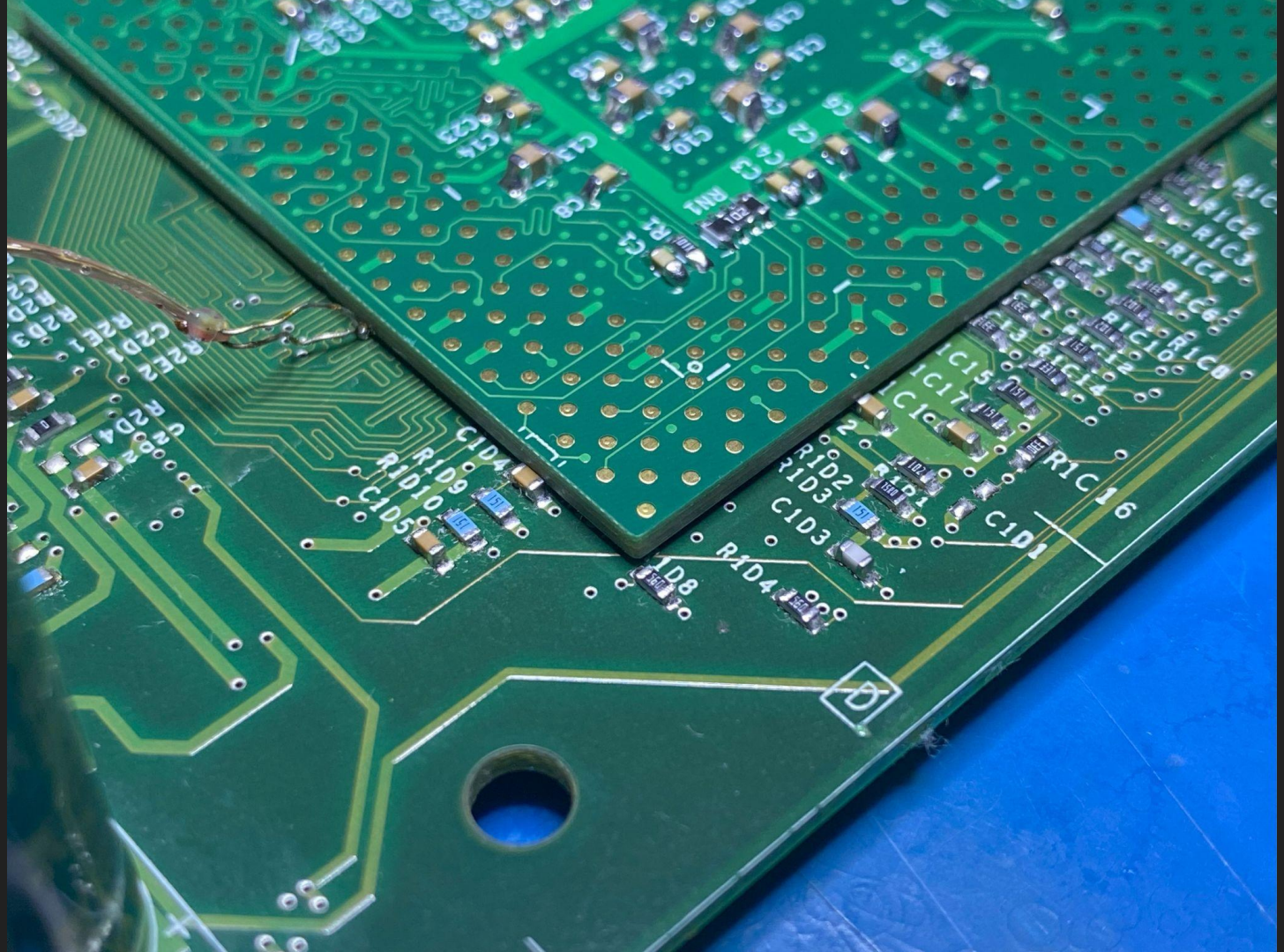

C
D
R1C16
R1C1
R1C2
R1C3
R1C4
R1C5
R1C7
R1C9
R1C14
R1C16
R1C19
C1C2
C1D3
C1D1
R1D3
C1D5
R1D9
R1D4
R1D6
R1D10
R1D5
C1D2
R1D7
R1D8
C1D4
PIN_A1
U3C1
R2D1
U2D1
C9C1
C9C2



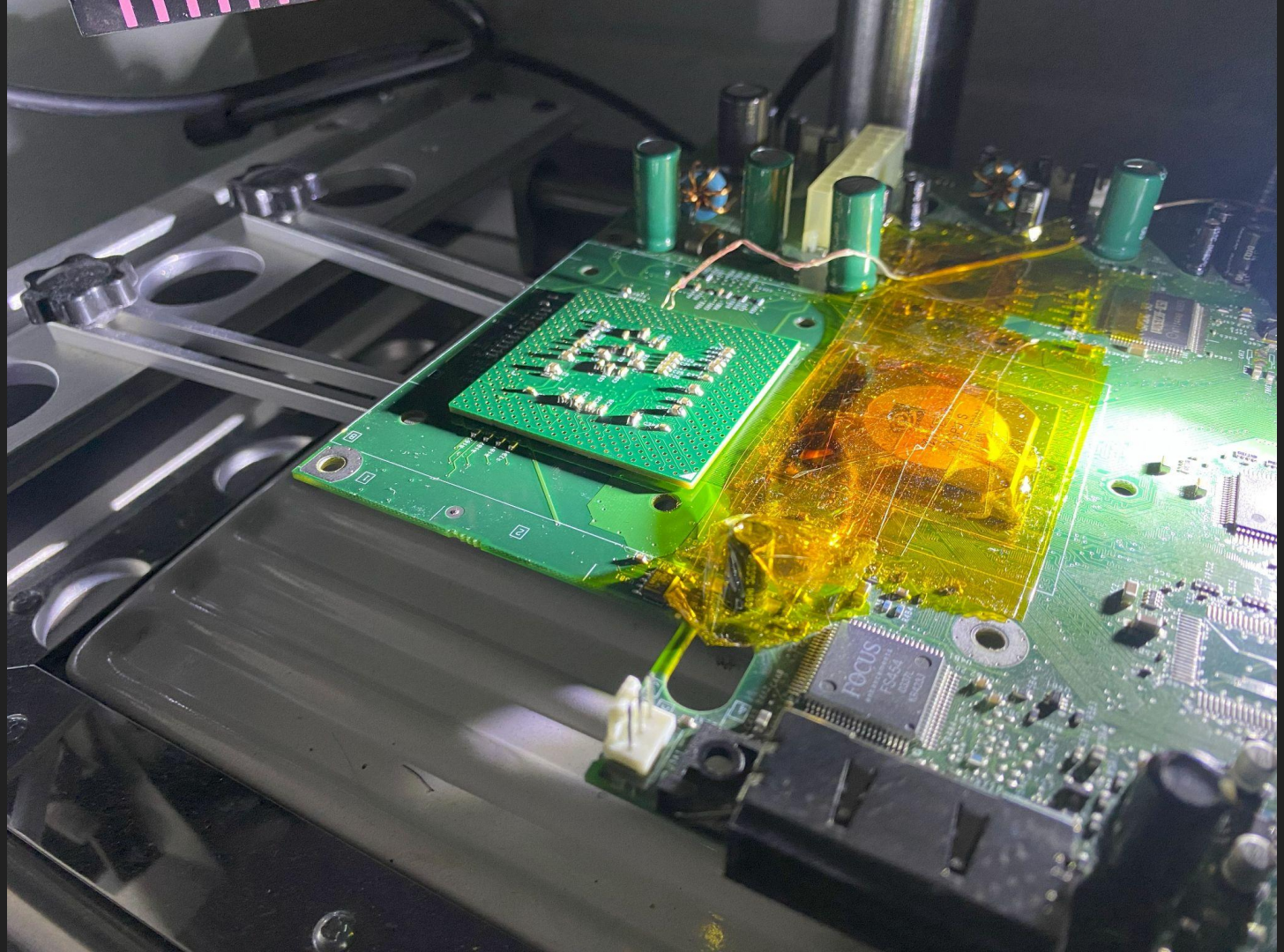

R1D5
C1D2
R1D7
R1D8
C1D4
R1D6
R1D4
AB
AD
C1D5
C1D1
R1C16
R1C14
C1C2
C1D3
R1C19

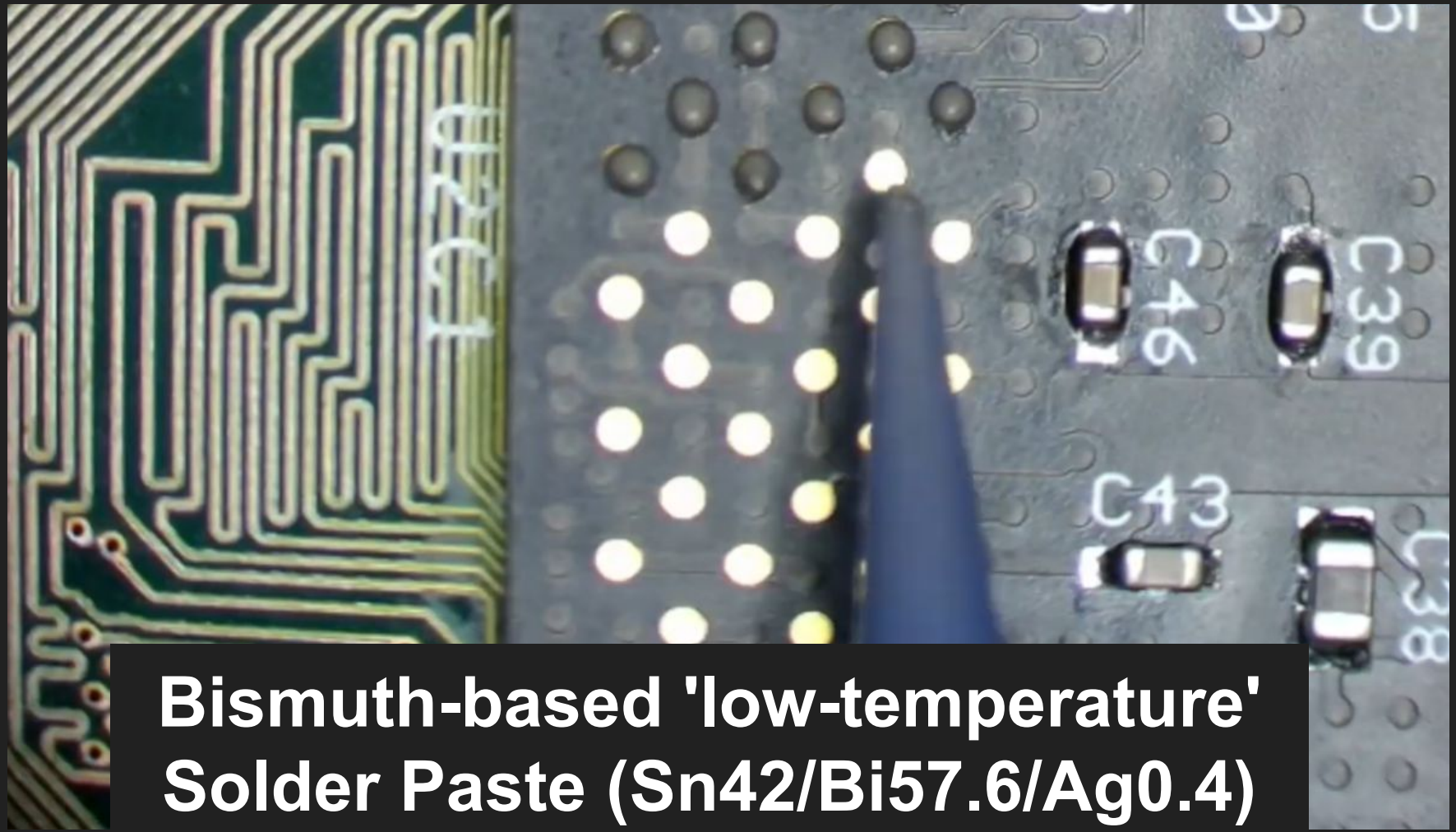
Leaded (Sn63/Pb37) 0.76mm Solder Balls



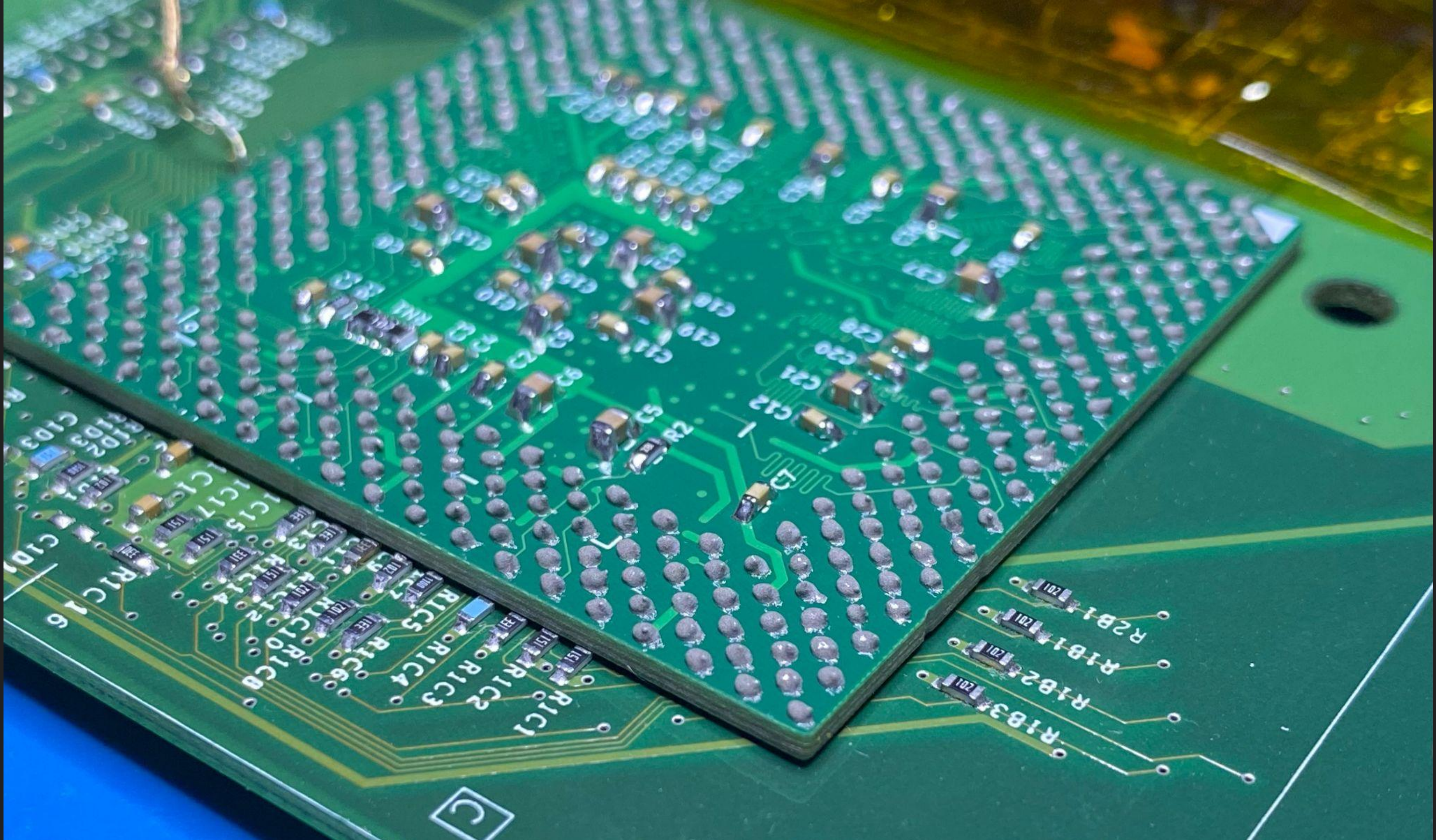

C1D4
R1D9
R1D10
C1D5
R1D8
R1D2
R1D3
C1D3
R1D4
C1D1
R1C16


ACHI
Lower TEMP Controller
32
180
Upside TEMP Controller
20
35
6
Lighting Switch
Fan Switch
Stop Button
Start Button
www.easyBGA.com


Focus

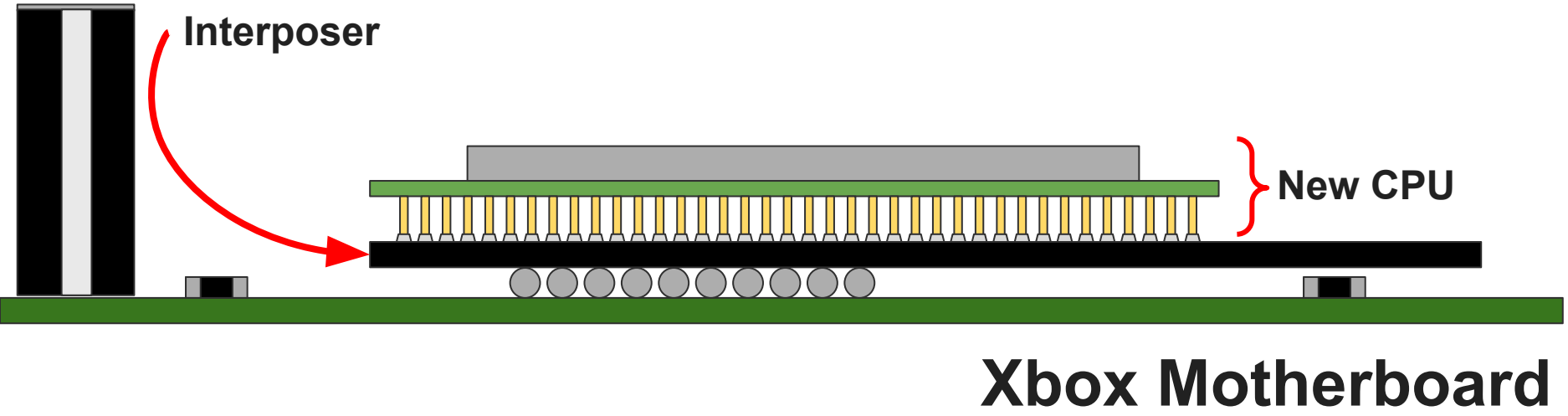


Bismuth-based 'low-temperature' Solder Paste (Sn42/Bi57.6/Ag0.4)

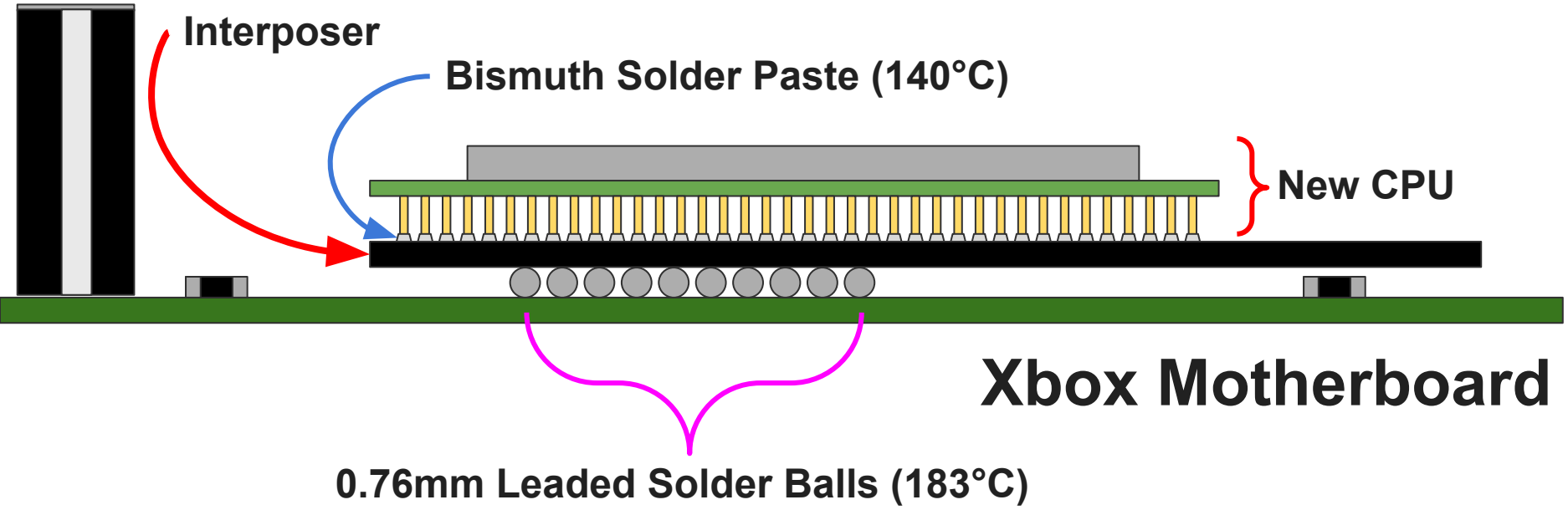

R2B1
R1B1
R1B2
R1B3
RIC1
RIC2
RIC3
RIC4
RIC5
C5
R2
C12


R281
R181
R182
R183

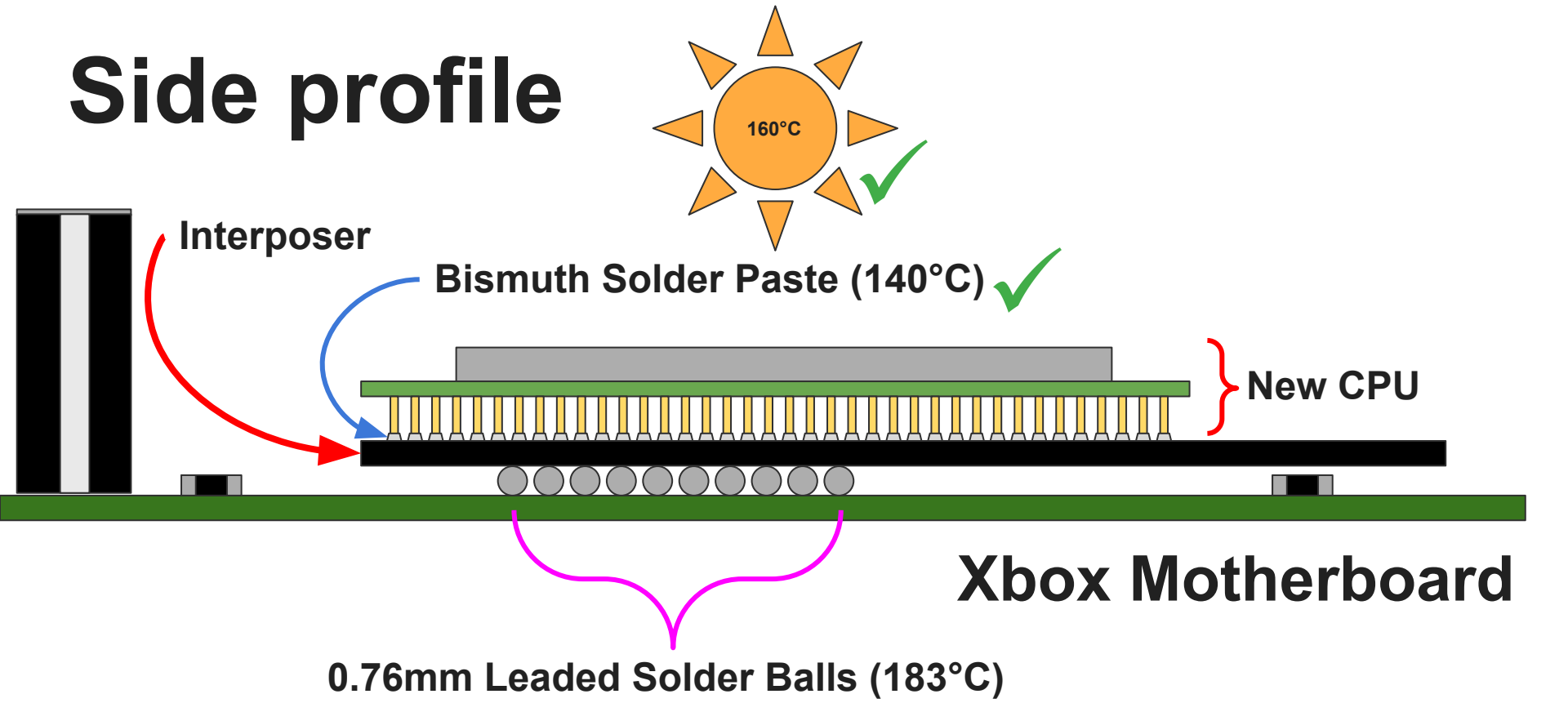
Side profile



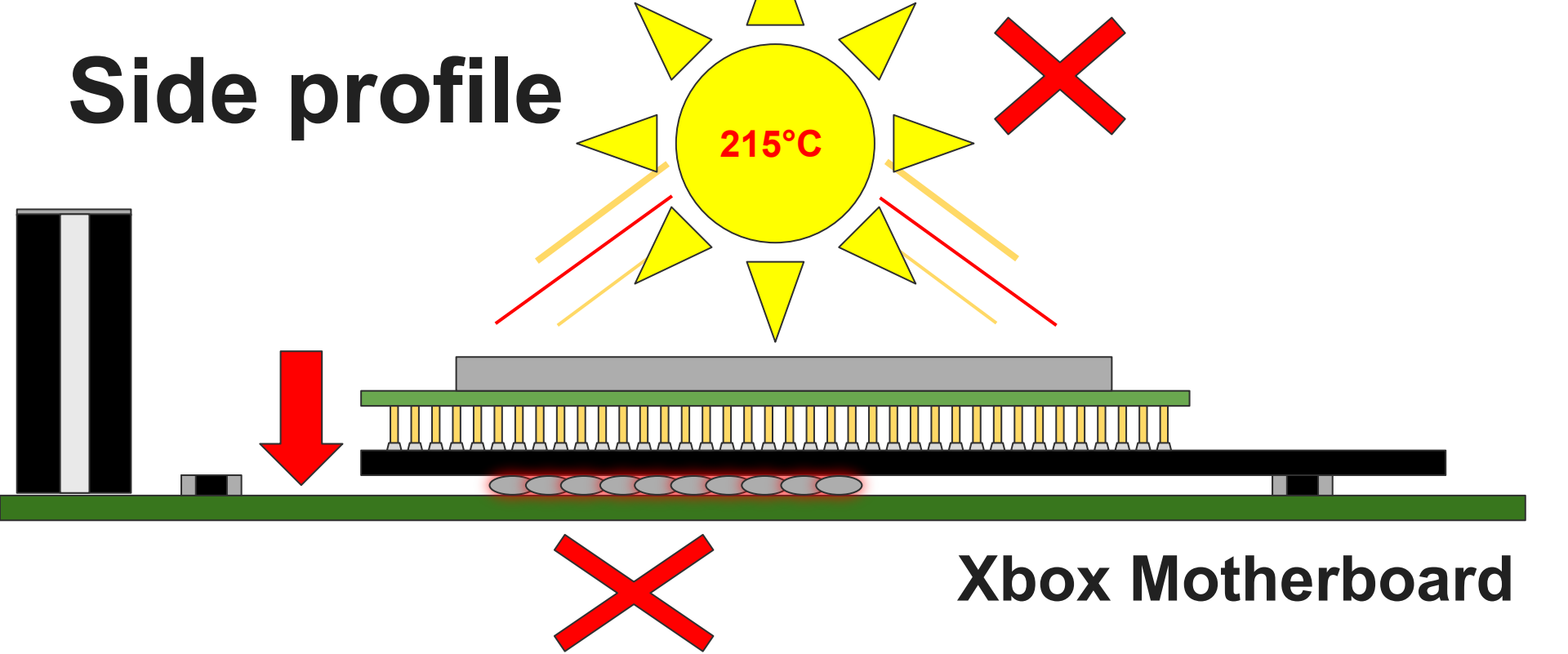
Side profile



Side profile

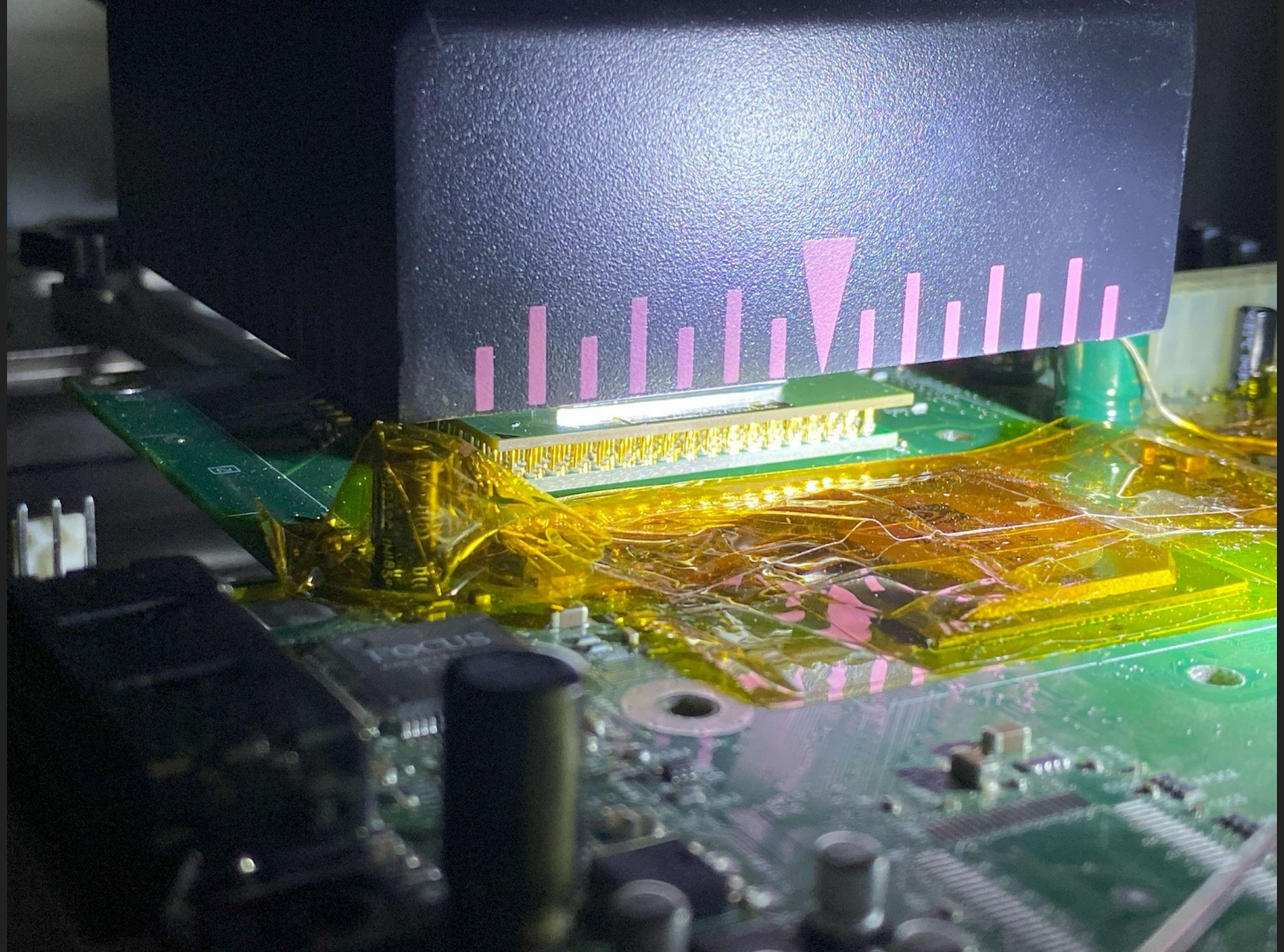


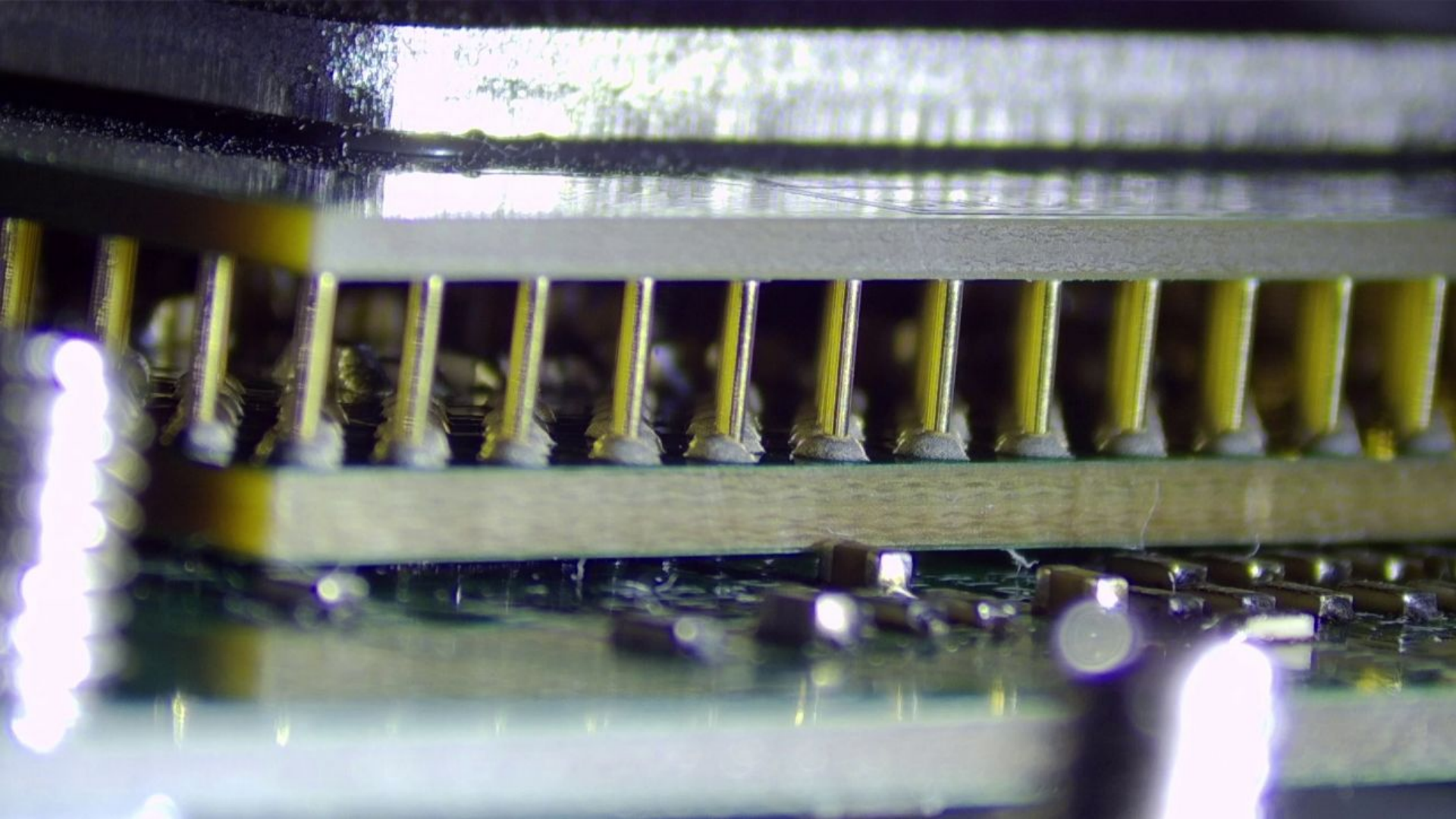
Side profile

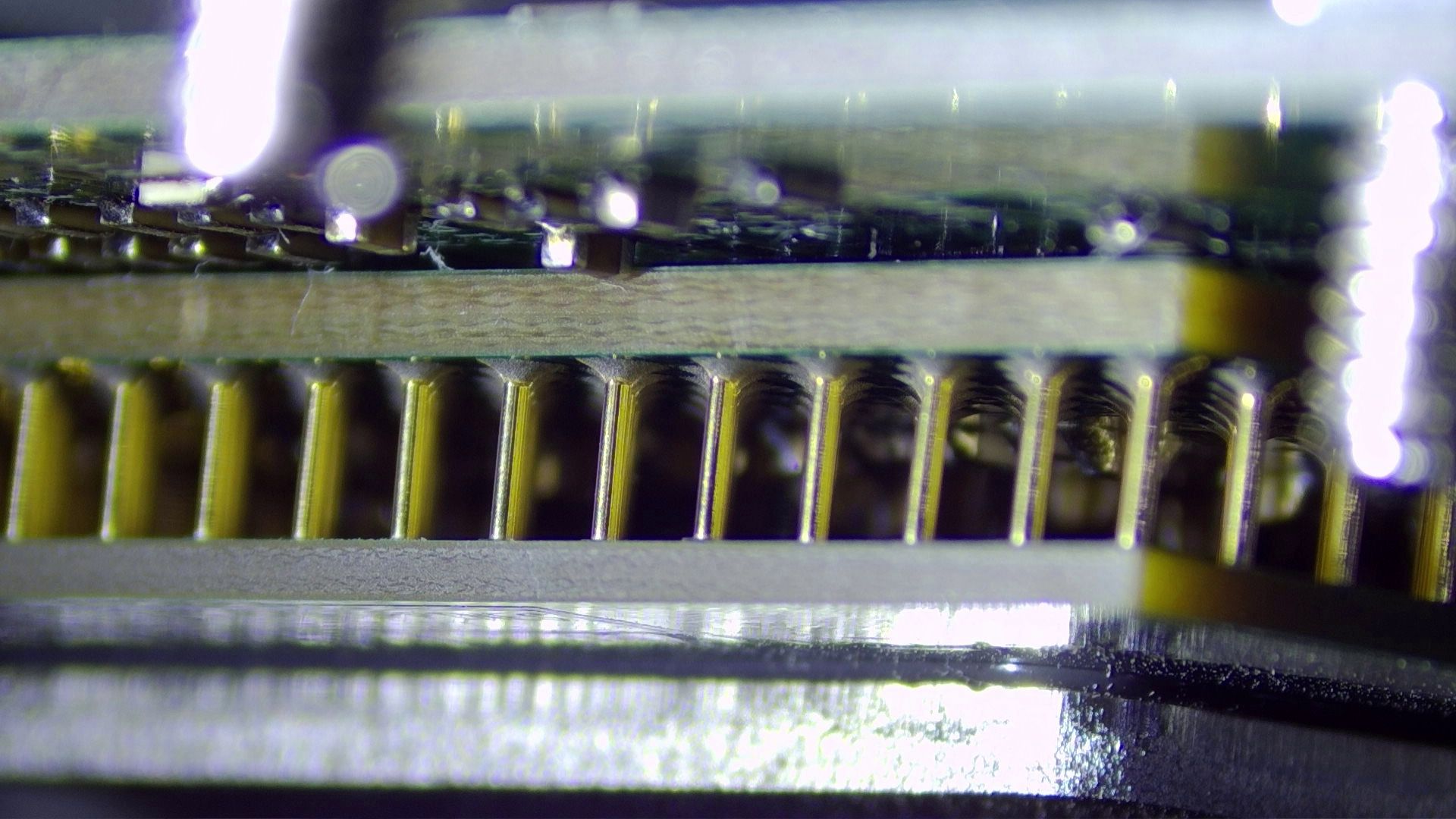


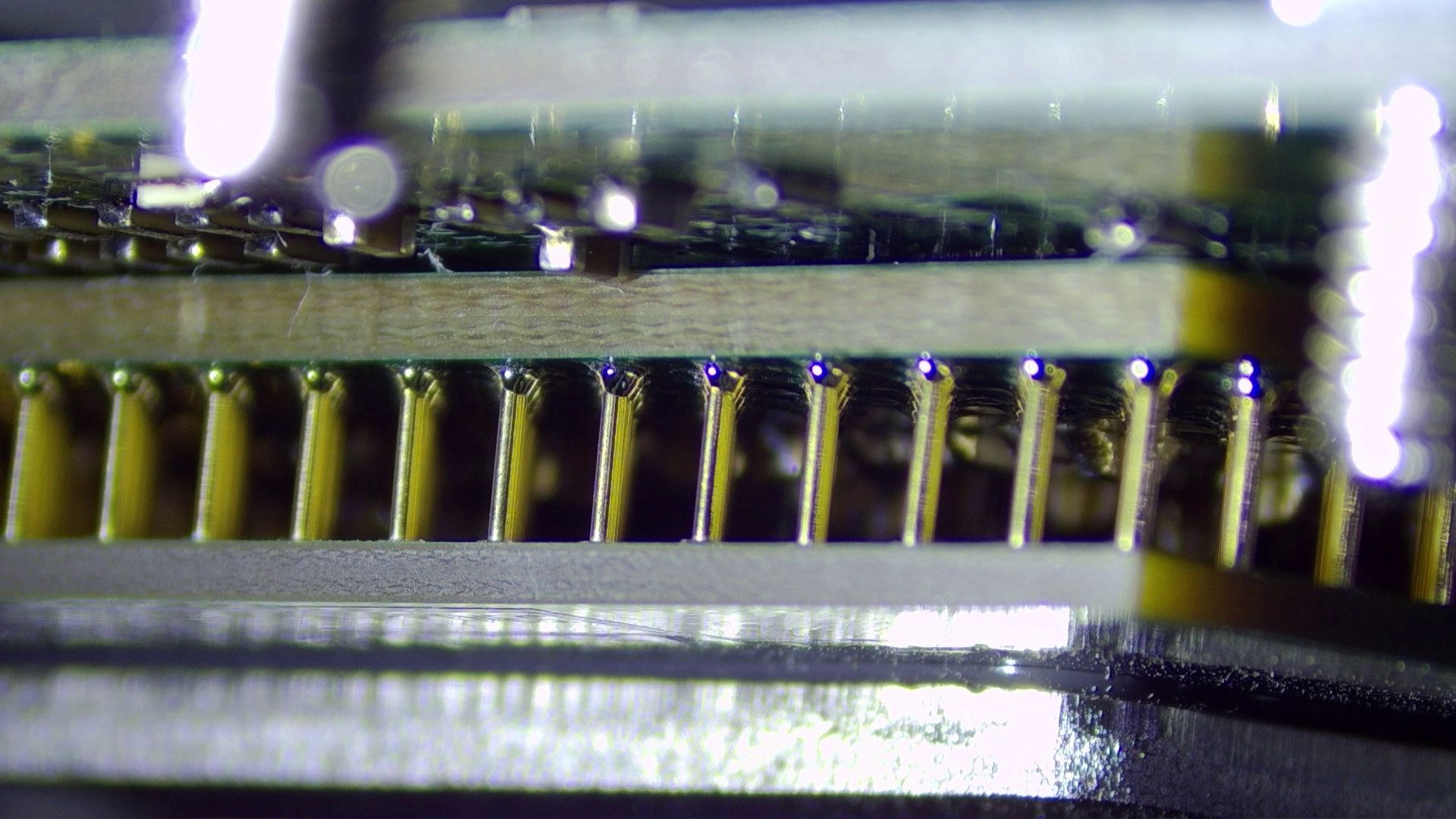
bridging BGA balls under interposer


ACHI
PSOFt
22:32:21
Set Point 36°C
UpsideTEMP Controller
www.easyBGA.com





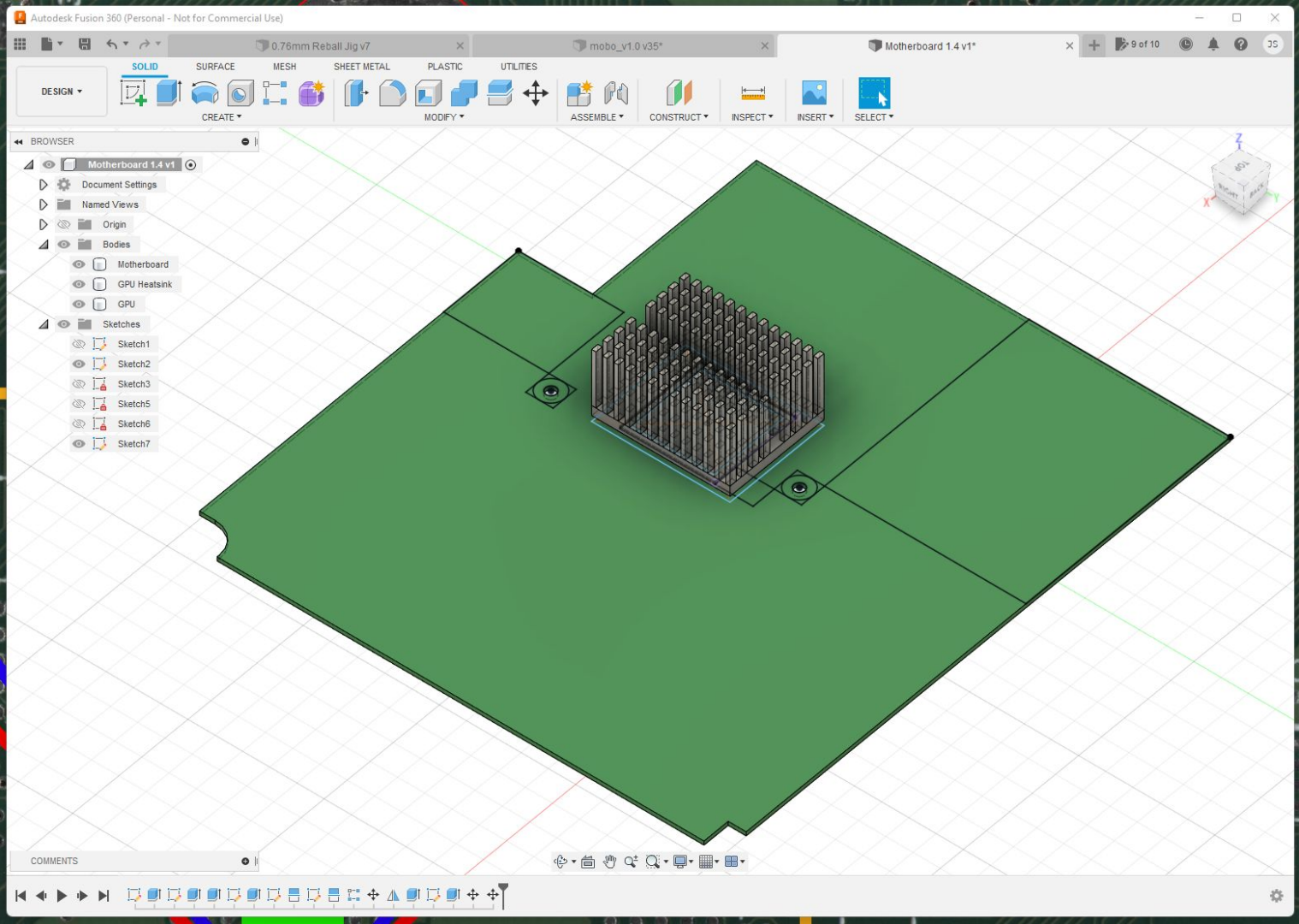


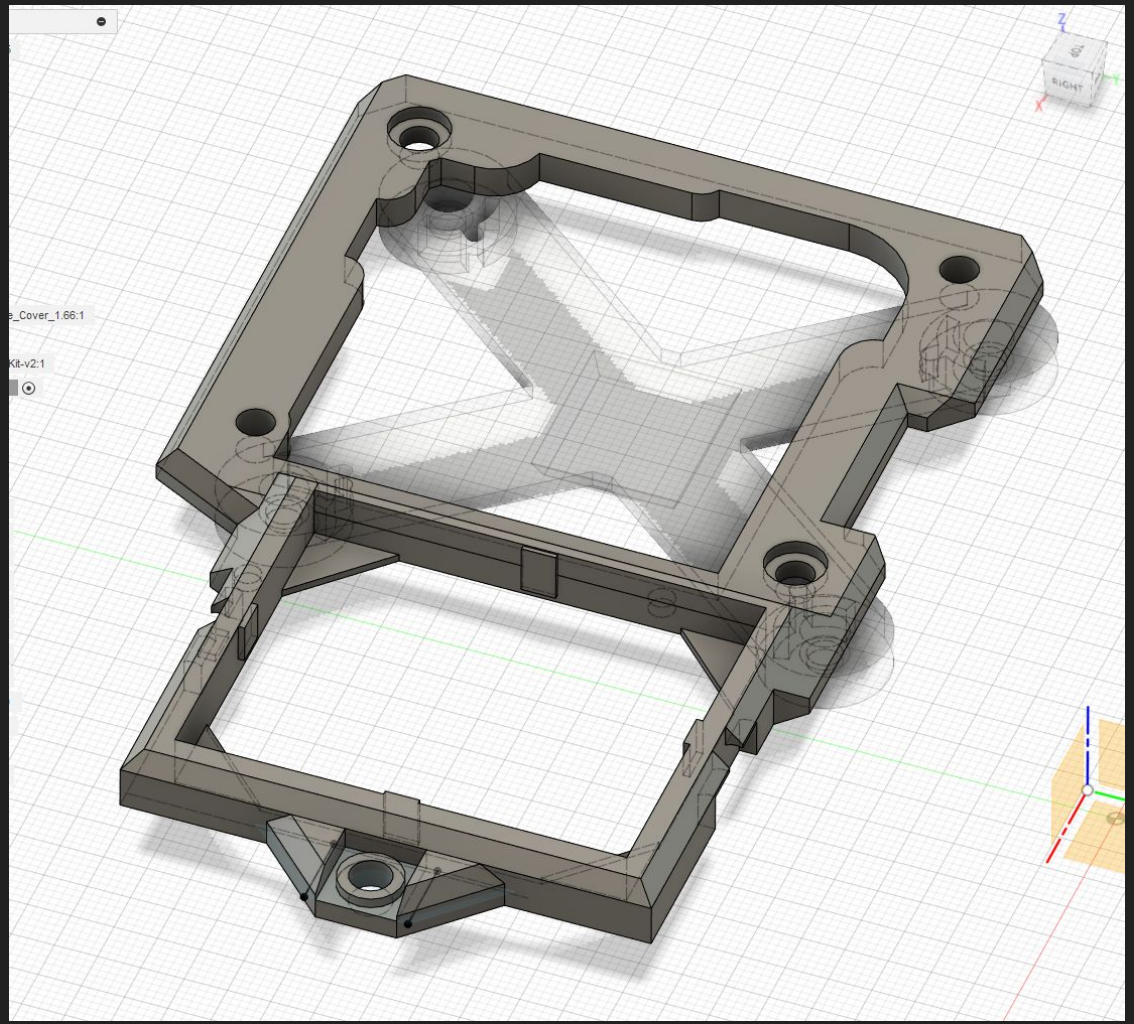


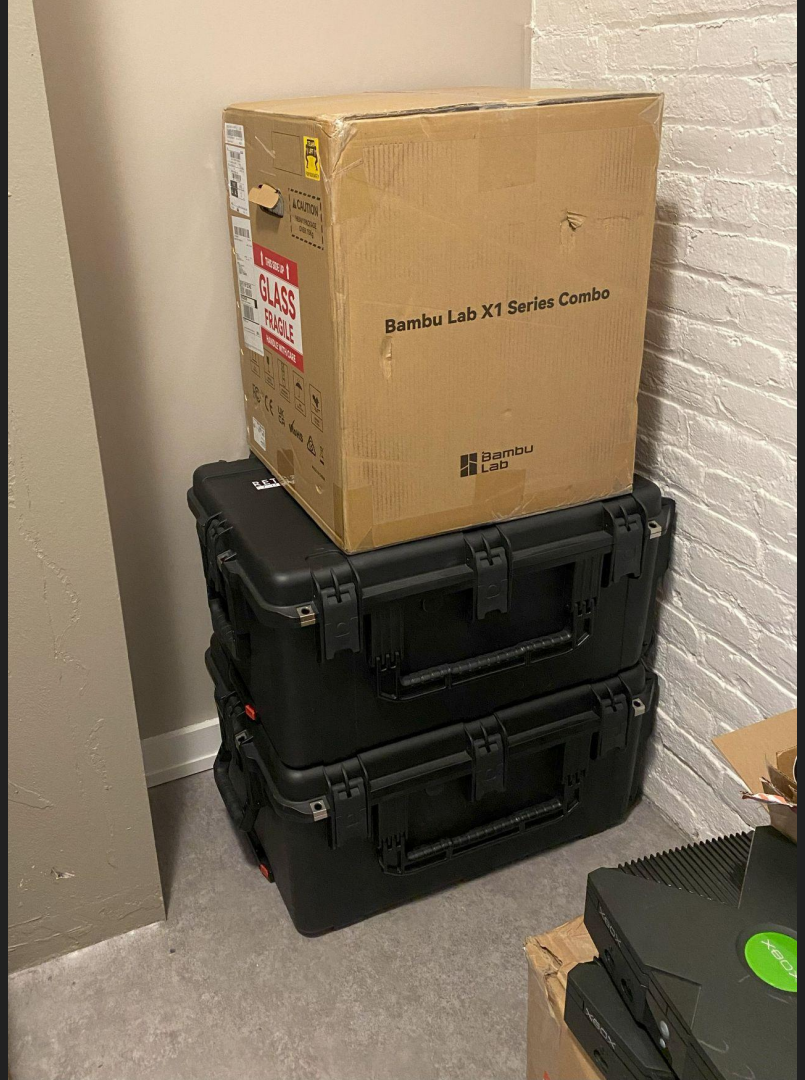

Q217A393-0322
1400/512/133/1.45
PIN A1
nVIDIA®
XGPU S


KIMTECH
XBOX

wait… how do I cool this thing?


Autodesk Fusion 360 (Personal - Not for Commercial Use)
0.76mm Reball Jig v7
mobo_v1.0 v35*
Motherboard 1.4 v1*
DESIGN
SOLID
SURFACE
MESH
SHEET METAL
PLASTIC
UTILITIES
CREATE
MODIFY
ASSEMBLE
CONSTRUCT
INSPECT
INSERT
SELECT
BROWSER
Motherboard 1.4 v1
Document Settings
Named Views
Origin
Bodies
Motherboard
GPU Heatsink
GPU
Sketches
Sketch1
Sketch2
Sketch3
Sketch5
Sketch6
Sketch7
COMMENTS


e_Cover_1.66:1
Kit-v2:1
RIGHT


Bambu Lab X1 Series Combo
GLASS
FRAGILE
Bambu Lab


AMS
X1 Carbon


FOCUS
FS454
NVIDIA
XGPU S
TAIWAN


SAMSUNG 340
K4D26323RF-DC50

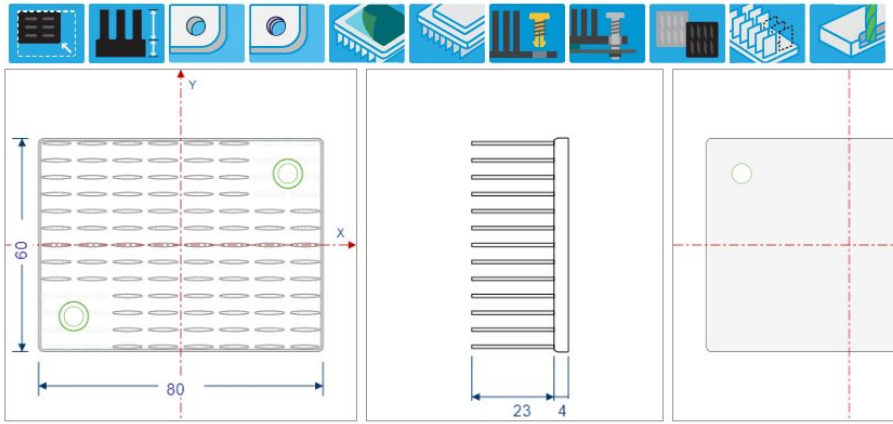
ALPHA Your partner for thermal solutions

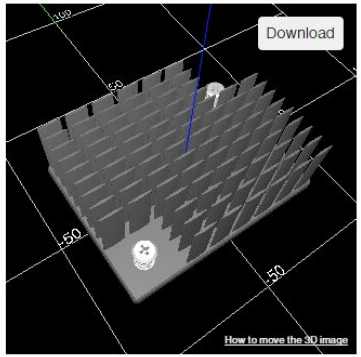
Search Login

Online Heat Sink Customization

Customization options for LPD6080

1. Specify Customization | 2. Input contact information | 3. Review | 4. Submit Request





Estimated price(US$)

Quantity	Price
1	127.55
5	35.23
10	24.22
50	10.11
100	8.14
200	Quote

Finalize

Customization Summary [Units:mm]

Change Height/Thickness — Fin height 23 — Base thickness 4

Add Shoulder Screws and Springs

Hole Location

ID	X	Y
1	-30	-20
2	30	20

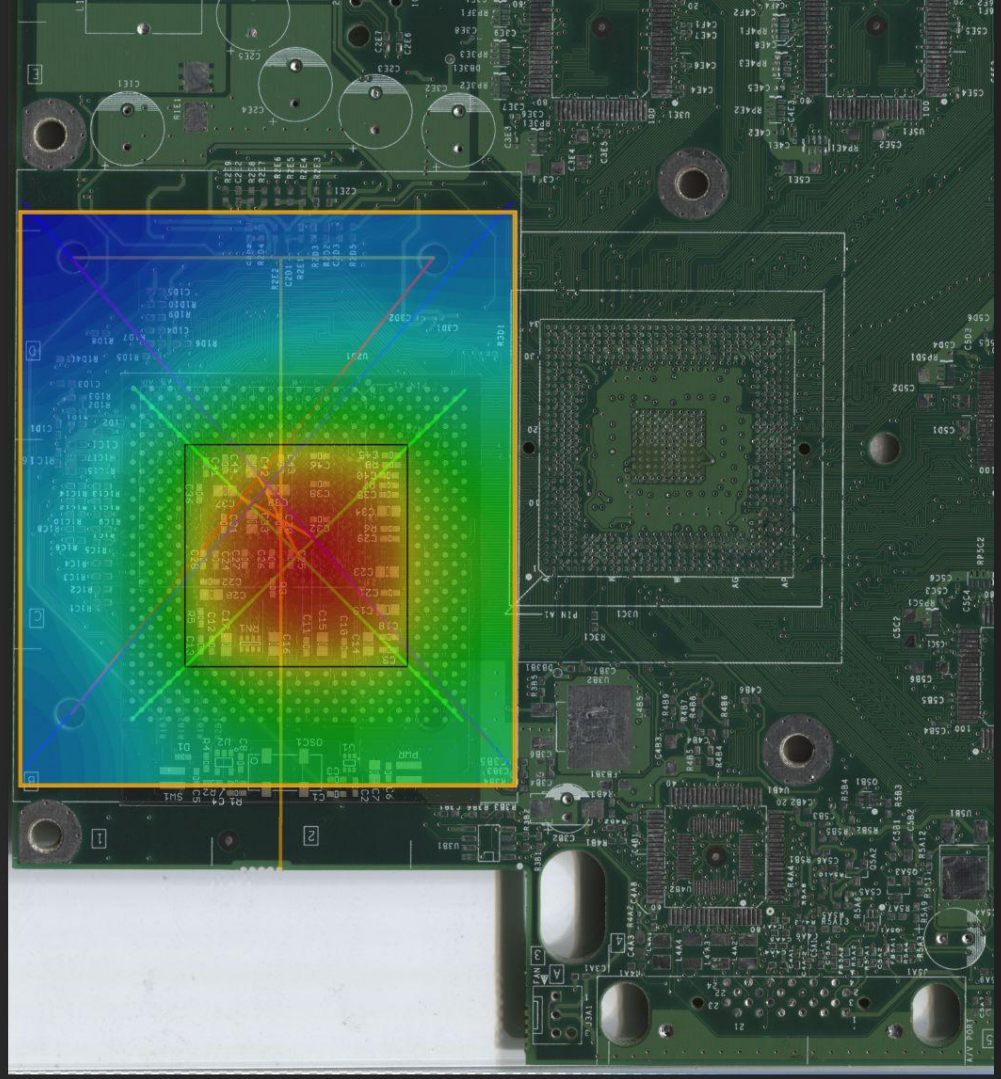
Selection Condition

Chip Info.

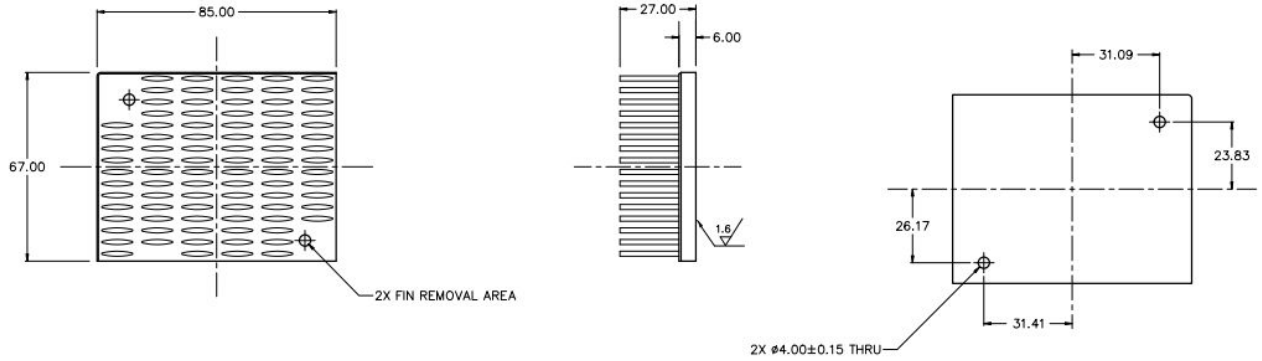
Chip Height	9
Vertical	31
Horizontal	31

Board Thickness		1.6		
Height Limit		36		
Allowable Load (N)(kgf)(lbf)	Min	9.81	1	2.2
	Max	9999	9999	9999
Attachment Method		ON the PCB surface		
PCB Hole Diameter		4		

Shoulder screw	SS-19-4.8-M3-7		
Spring	S001YJ52		
Working Load (N)(kgf)(lbf)	29.4	3.0	6.6
Pressure (N/mm2)(kgf/cm2)(psi)	0.03	0.31	4.44
Thread Protrusion(T.P.)	5.40		

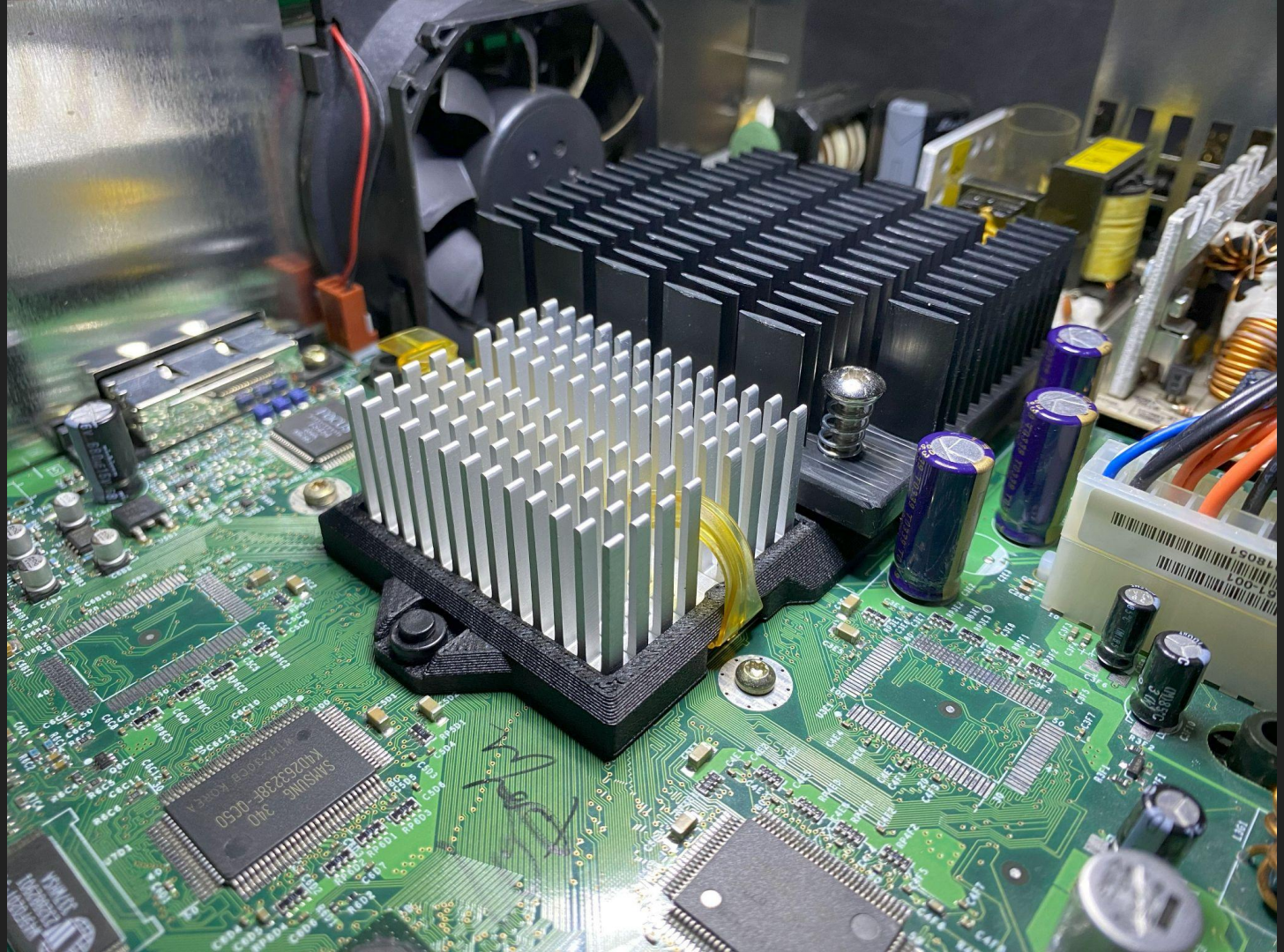


REVISIONS				
REV	DATE	DESCRIPTION	CHG	APPR

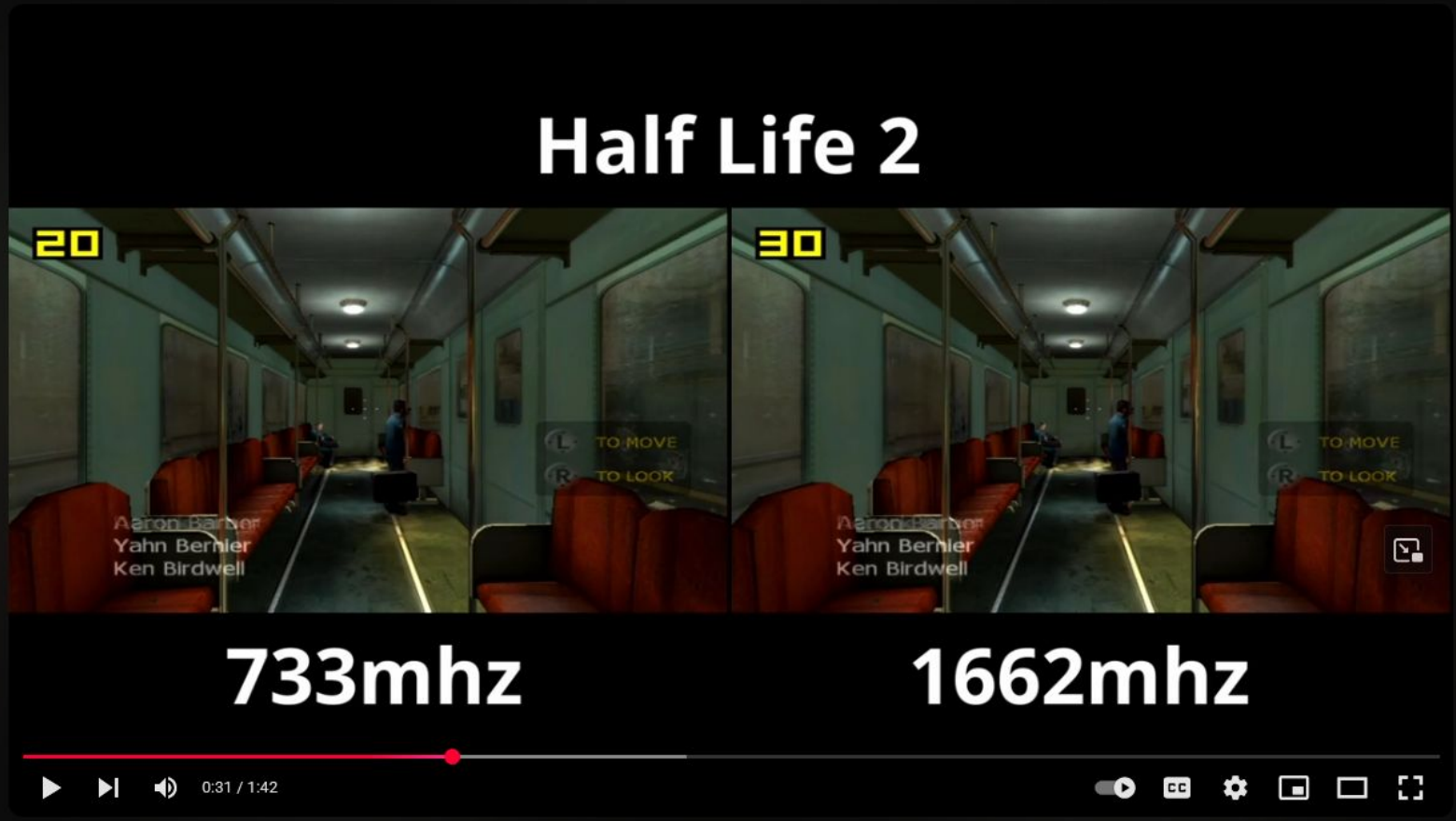


NOTES : UNLESS OTHERWISE SPECIFIED
1. INTERPRET DIMENSIONS AND TOLERANCES PER ANSI Y14.5M.
2. ALL DIMENSIONS ARE IN MILLIMETERS [INCHES].
3. MATERIAL : ALUMINUM 6063
4. FINISH : BLACK ANODIZE
5. TOLERANCES :
   .XX ±0.254 [.010]
   .XXX ±0.127 [.005]
   ANGLES ± 1°
6. REMOVE ALL BURRS AND BREAK SHARP EDGES. UNSPECIFIED CORNER R0.5 MAX OR C0.5 MAX.
7. A BEND OF THE FIN: THE FINS MUST NOT CONTACT.
8. FIN REMOVAL MARKS MAX 0.3MM
9. BASED ON ALPHA STANDARD HEAT SINK W100-45W

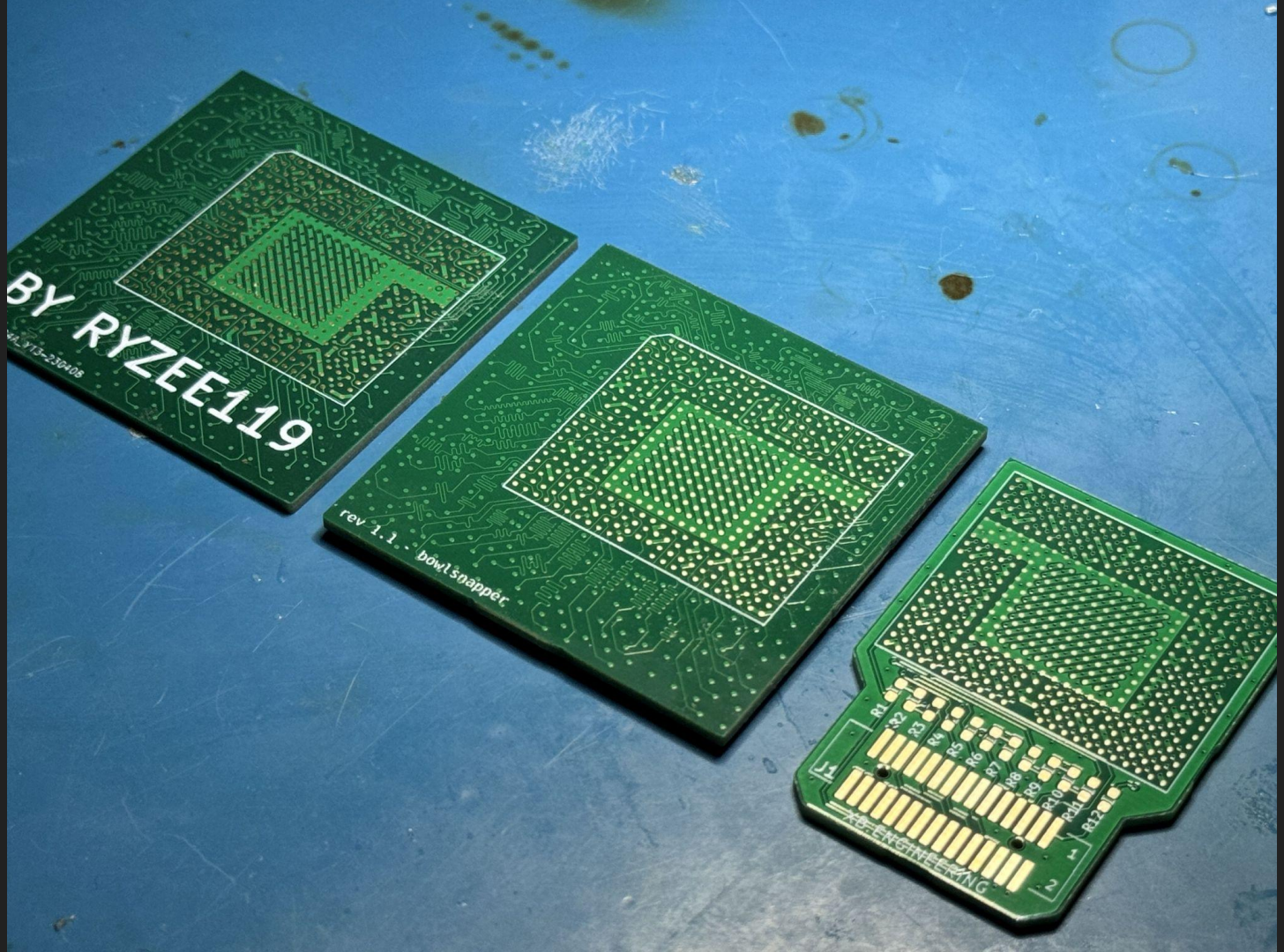
ITEM	PART NO.	PART NAME	REMARK	Q'TY
ALPHA CO.,LTD.			CSTMR'S PART NO.	
		MATERIAL NOTE 3,4	NAME W6785-27BM-RA8	
SCALE 1 : 1		APPR & CHCK G.SUMMERFIELD	PART NO. & DWG NO. S08FSQ03	REV
DATE JAN 19, 2023		DSGN & DWG G.SUMMERFIELD	RDCTN:	LOFF:


SAMSUNG 340
KM0263280F-QC50
KOREA


30
TO MOVE
TO LOOK
Gautam Babbar
Ted Backman
PC/AV
MENU
XBOX



Half Life 2 - Original Xbox CPU Upgrade Comparison


BY RYZEE119
rev 1.1
bowlsnapper
J1
J2
R1
R2
R3
R4
R5
R6
R7
R8
R9
R10
R11
R12
KBD ENGINEERING


J1
R1
R2
R3
R4
R5
R6
R7
R8
R9
R10
R11
R12
1
2
XB.ENGINEERING

x86 JTAG Debugging

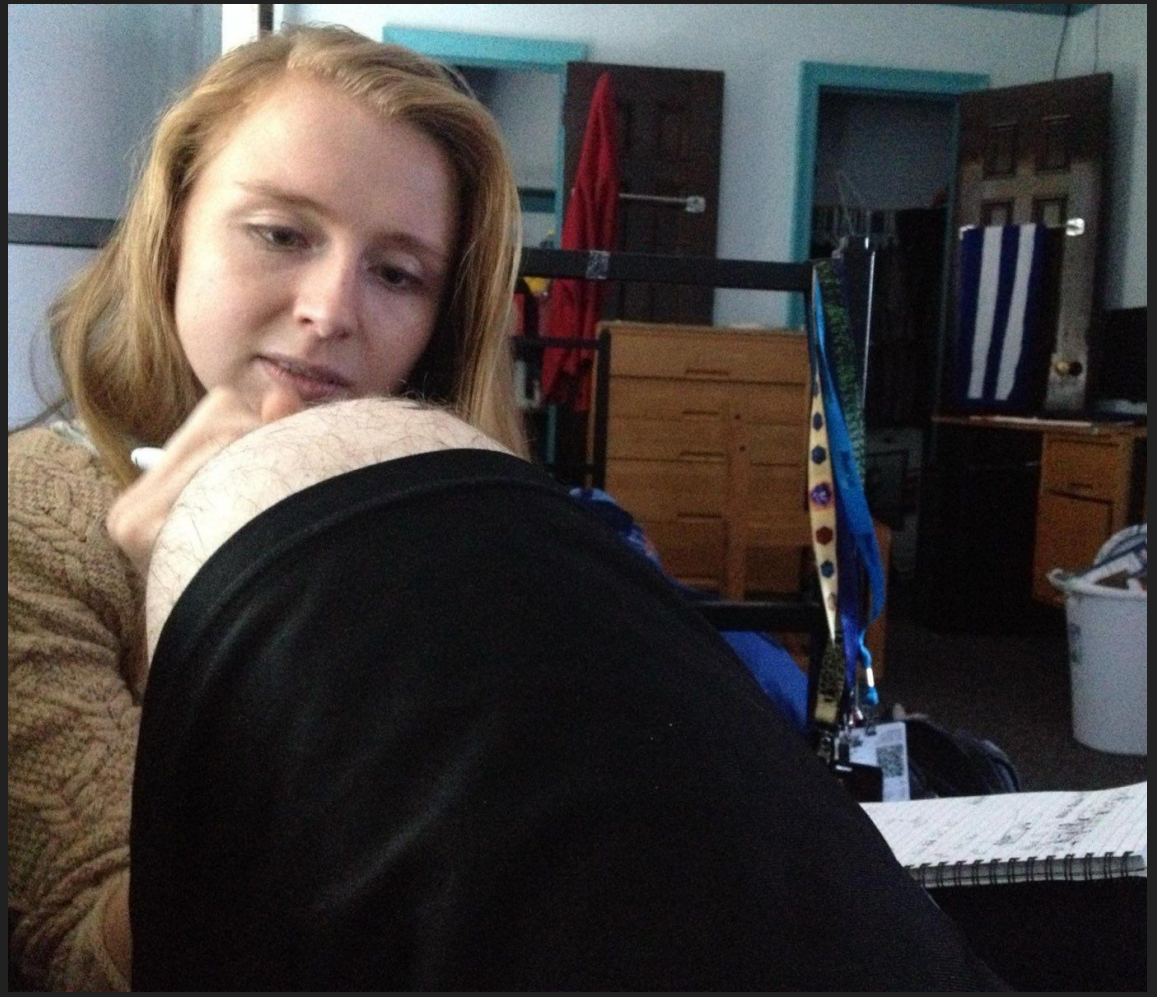
https://blog.ret2.io/2023/08/09/jtag-hacking-the-original-xbox-2023/

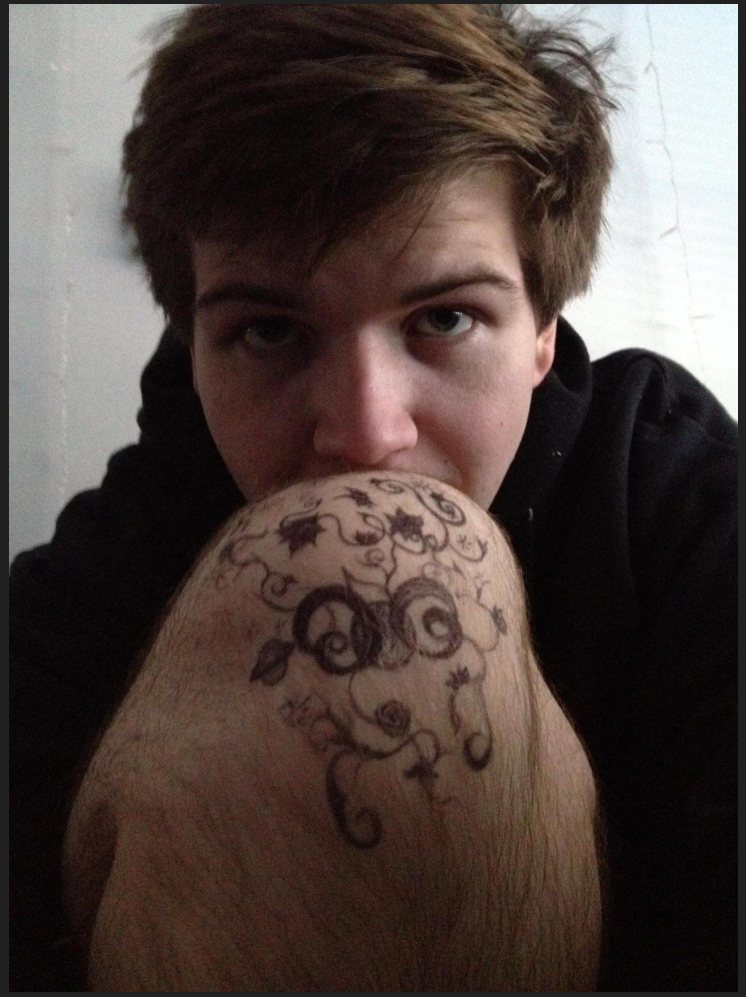
bunnie 7/14/23, 3:33 AM

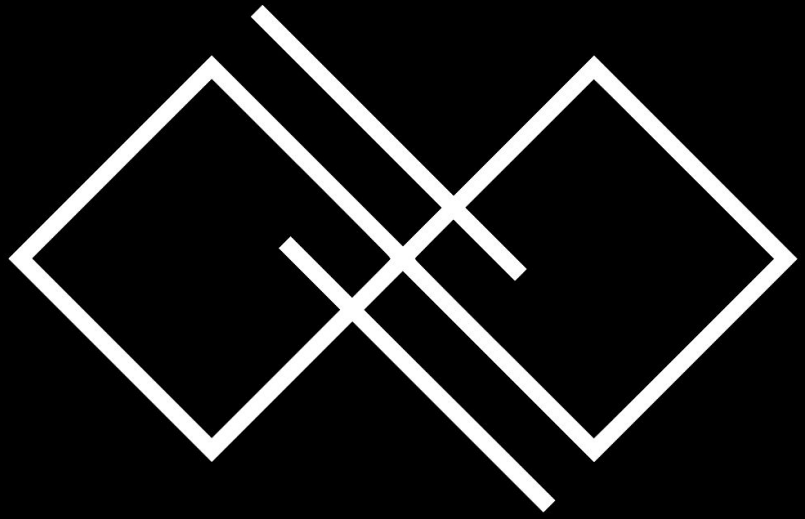
oh wow. the PCB interposer is genius.

Epilogue


HAPPY
BIRTHDAY
Cyber Missile
A visualization
?: is 0x15
21 in hex?
Yes → !!







RET2

SYSTEMS

MARGIN

RESEARCH


Last day at microsoft :D


last day at Trail of Bits
101 PARK AVE
New York, NY
MORE

Sophia “quend” d’Antoine was an amazing woman, researcher, and friend. She sat at the heart of the RPISEC family and was an important part of our story.

Her individual grace and ambition was felt across the industry. She inspired and touched so many lives.

Sophia’s vision and passion will continue to be the cornerstone of our collective aspirations.

1993 - 2024


WINIX


RET2
SYSTEMS
the woods are lovely,
dark, and deep. but
i have promises
to keep, and
miles to go
before i sleep.
- robert frost

Conclusions

- **Be ambitious, ignorance is bliss**
- **Hug your friends**
- **Special acknowledgements**
  - grimdoomer, xbox7887, 404, dustin, x, loser, mborgerson, libby, ryzee119, andy, disco, Insignia folks, haxar, prehistoricman, frank, archive.org, fish

thanks

doom@aol.com

DO YOU HAVE THIS BOARD?

(A1 / EVT)

$5000 USD Bounty