

Xbox to 360

Modding Halo along the way.



// ibotpeaches

Name the Xbox - 1



Xbox - (November 2001)

Name the Xbox - 2



The Xbox Developer Kit (XDK) - (Feb 2000)

Name the Xbox - 3



Translucent "**Ice Blue**" Halo 2 Canadian Special Edition Xbox - (March 2005)

Name the Xbox - 4



Xbox 360 - (November 2005)

Name the Xbox - 5



Xbox 360 Launch Team Edition - (November 2005)

Name the Xbox - 6




Xbox 360 Slim - (June 2010)

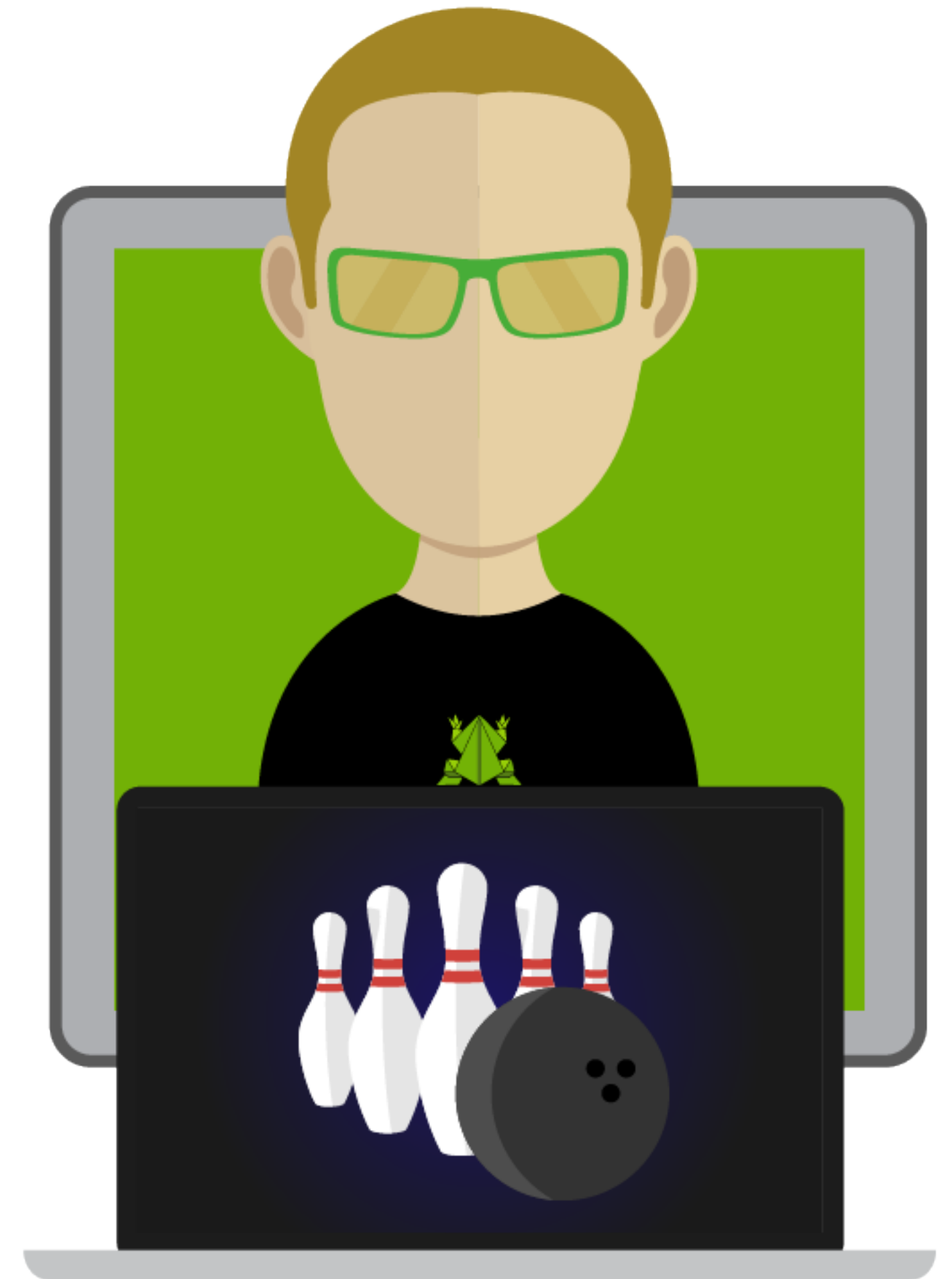
Name the Xbox - 7



Xbox 360 E - (June 2013)

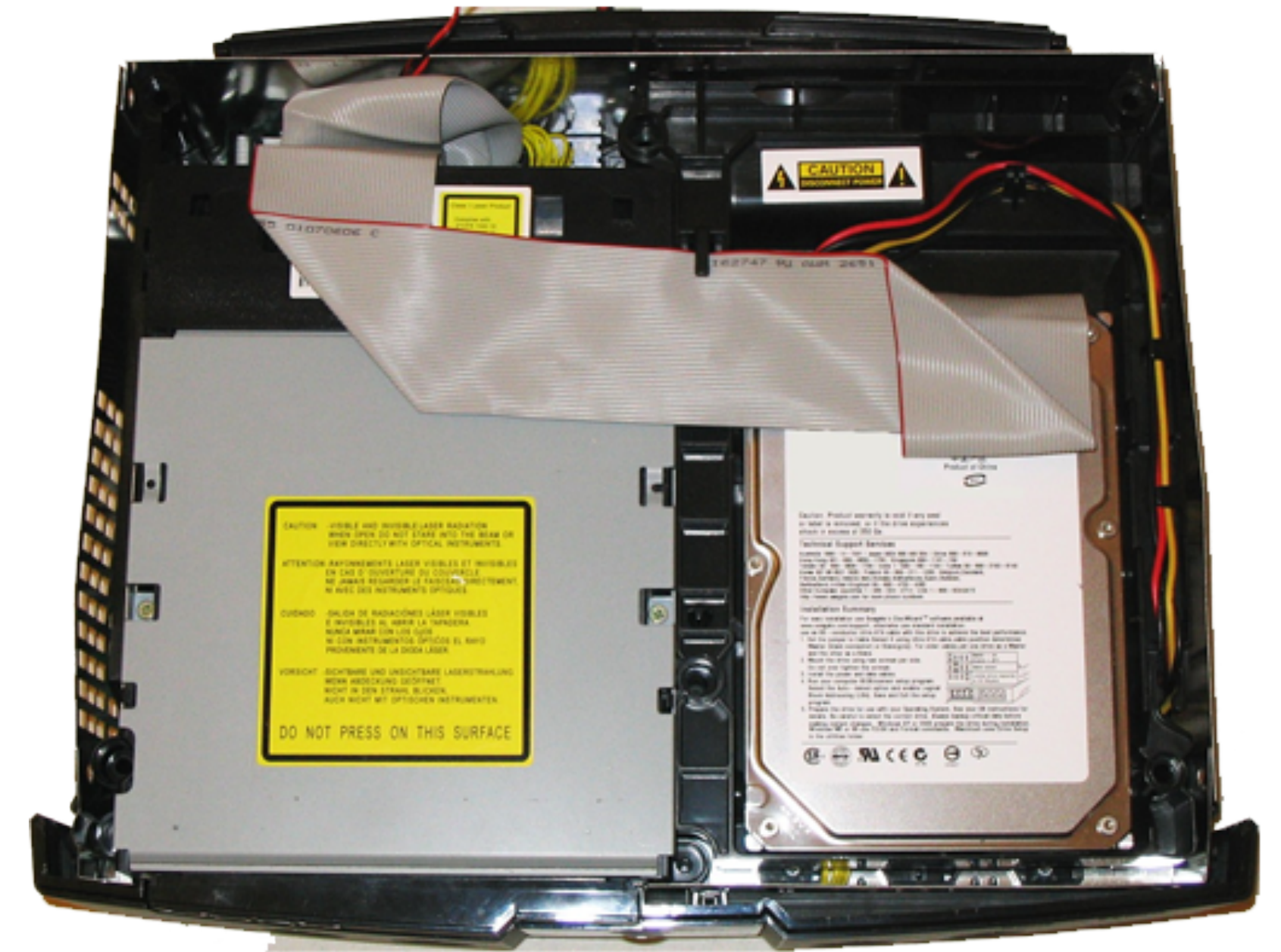
Who

- iBotPeaches 
- Connor Tumbleson (.com)
- Started in Halo
- Migrated to Android
- Now Web/PHP



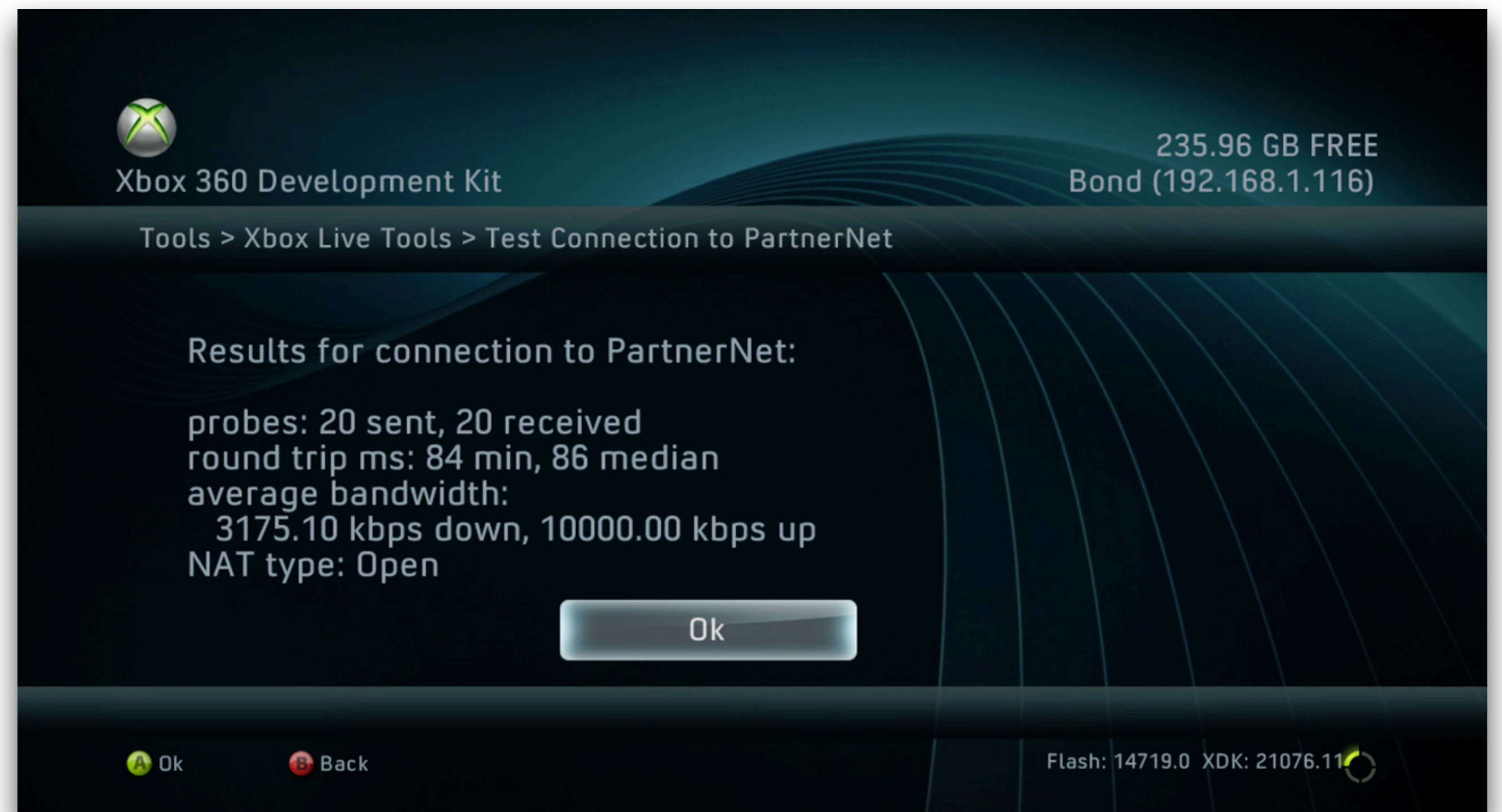
Refresh - Xbox

- Intel Pentium III 733 MHz CPU
- nVidia GeForce 3MX
- DVD Drive
- 8GB HDD
- 64MB RAM



Gameplan

- Softmod an Xbox
- Hardmod an Xbox
- “Mod” Halo
- Hardmod a 360
- “Mod” Halo



Softmod?

- Modify an xbox beyond intention
WITHOUT any hardware interaction.
- Or in web industry - a vuln.



What do you need?

- An affected game
- Transfer mechanism
 - Splinter Cell
 - Action Replay



How?

- Don't play
- Load a game save
 - A packed save



Game Saves - 101 - Xbox

- Two types - Roamable / “noroam”
- **noroam** - signed via game + xbox
- **roamable** - signed via game + constant
- 5C0733AE0401F7E8BA7993FDCD2F1FE0 (retail)
- 66810D3791FD457FBFA976F8A446A494 (debug)

The Market - **Action Replay**

- Buy
- Download
- Transfer
- Cheat
- Have Fun



Game Saves - Difficulty

- What to hash? - Not consistent
- Trial and error
 - Play/Save - Do nothing
 - Play/Save - Do 1 thing
- Compare/Contrast



The Bounty & 007

- \$100,000 bounty to softmod is up
 - Michael Robertson (MP3 / Lindows)
- Odd release
 - uudecode
 - 1st post

XboxHacker BBS ->General ->General Xbox Hacking & Modding

Pages: (5) ≤ **[1]** 2 3 4 5 ≥ (Go to first unread post)

Project B Solved!, Linux Project B solved!

« Next Oldest | Next Newest »

habibi_xbox

Posted: Mar 29 2003, 12:20 PM

Newbie
■

Group: Members
Posts: 1
Member No.: 8724
Joined: 29-March 03

Subject : Project B Solved !

Ladies and Gentlemen,

I'm happy to present the first solution found for the Xbox Linux Project B:
Here is a way to run Xbox Linux on an unmodded, unopened Xbox !

Inlcuded is a uuencoded zip file containing all the necessary files. Here is what you need:

- - You need an unmodded XBOX (not sure it works with modded bios)
- - You need the game 007 Agent Under Fire (*NOT* NIGHTFIRE, those are two different games!)
- - You need a way to transfer a save to a memory card (that is, xbox-save.com's hardware, or usb<>xbox cable + usb stick + xbox-save software, or you can use a standard memory card too if you can put files on it (with EvoX for instance).
- - You need to get the "Xbox Linux Live" small distro.

Got all this? Let's party!

The Technical - 007 Hack

- Buffer Overflow
- Decrypt the JPEG. Find the real hack.
- Disable write kernel protections
- Adapt public key. Make factorable
- Launch into modified XBE

The Limbo State

- In between worlds
- The auto-installer
- Dashes, BIOS, etc
- Now “soft-modded”



UnleashX

- Modded dashboard
- Launch Games
- Launch Apps
- Settings



Bert n Ernie

- Mysterious release
- Not obfuscated
- Two font files
 - Buffer Overflow
 - Thread Collision

```
;;this finds 2 exports in the pe header, HalWriteSMBusValue and XePublicKeyData
findexp :
        lea     edx, [ebp+(offset smb - offset getip)]
        mov     ecx, [edi+10h]
        mov     edi, [edi+1Ch]
        lea     edi, [esi+edi]

getexp :
        mov     eax, [edx]

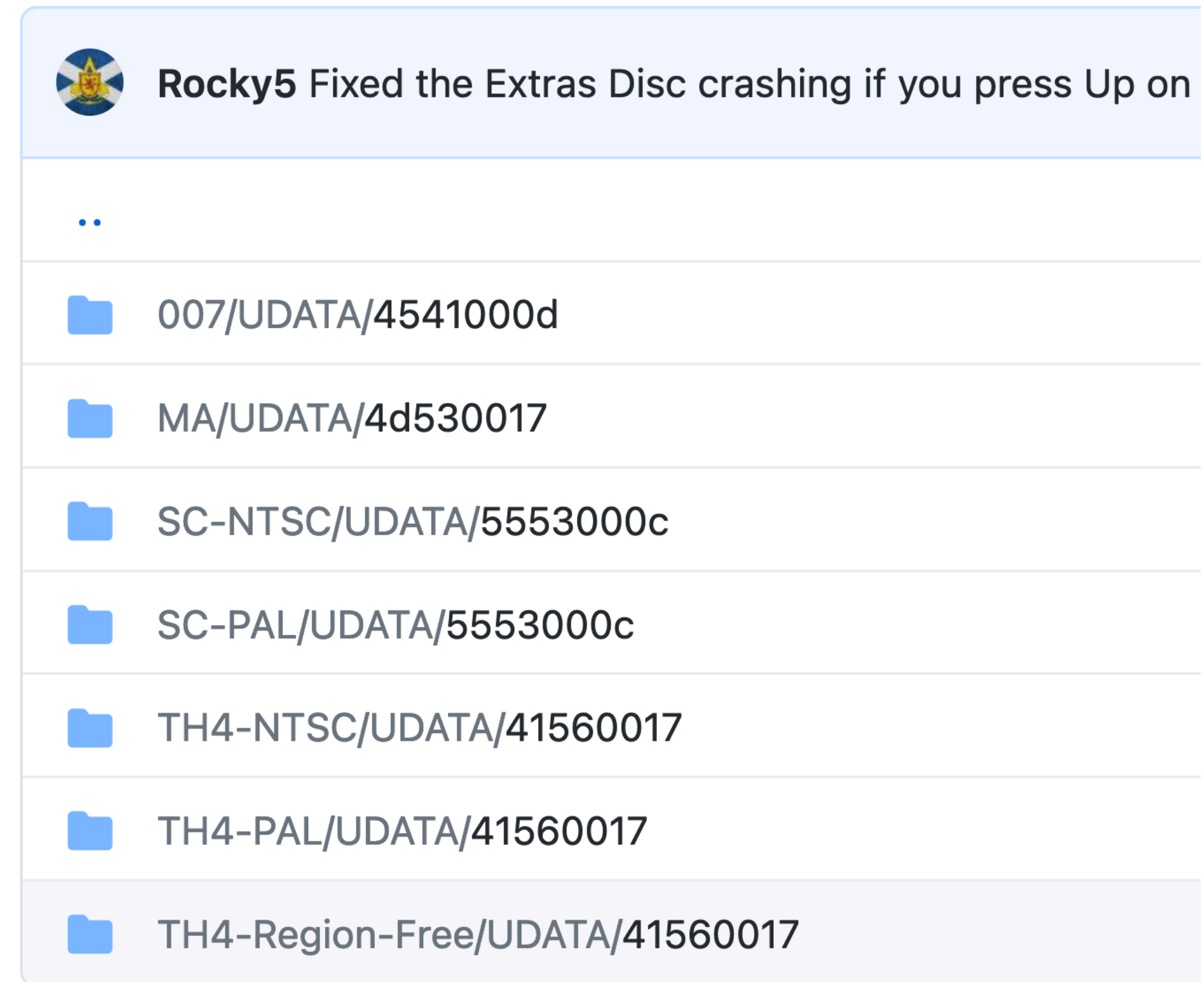
findaddr :
        or      eax, eax
        jz      short findkey
        sub     eax, ecx
        shl     eax, 2
        mov     eax, [edi+eax]
        or      eax, eax
        jz      short storeaddr
        add     eax, esi

storeaddr :
        mov     [edx], eax
        inc     edx
        inc     edx
        inc     edx
        inc     edx
        jmp     short getexp

;;;some data for use various places
path      db '\Device\Harddisk0\Partition2',0
file      db 'default.xbe',0
smb       dd 32h
key       dd 163h
          dd 0
```

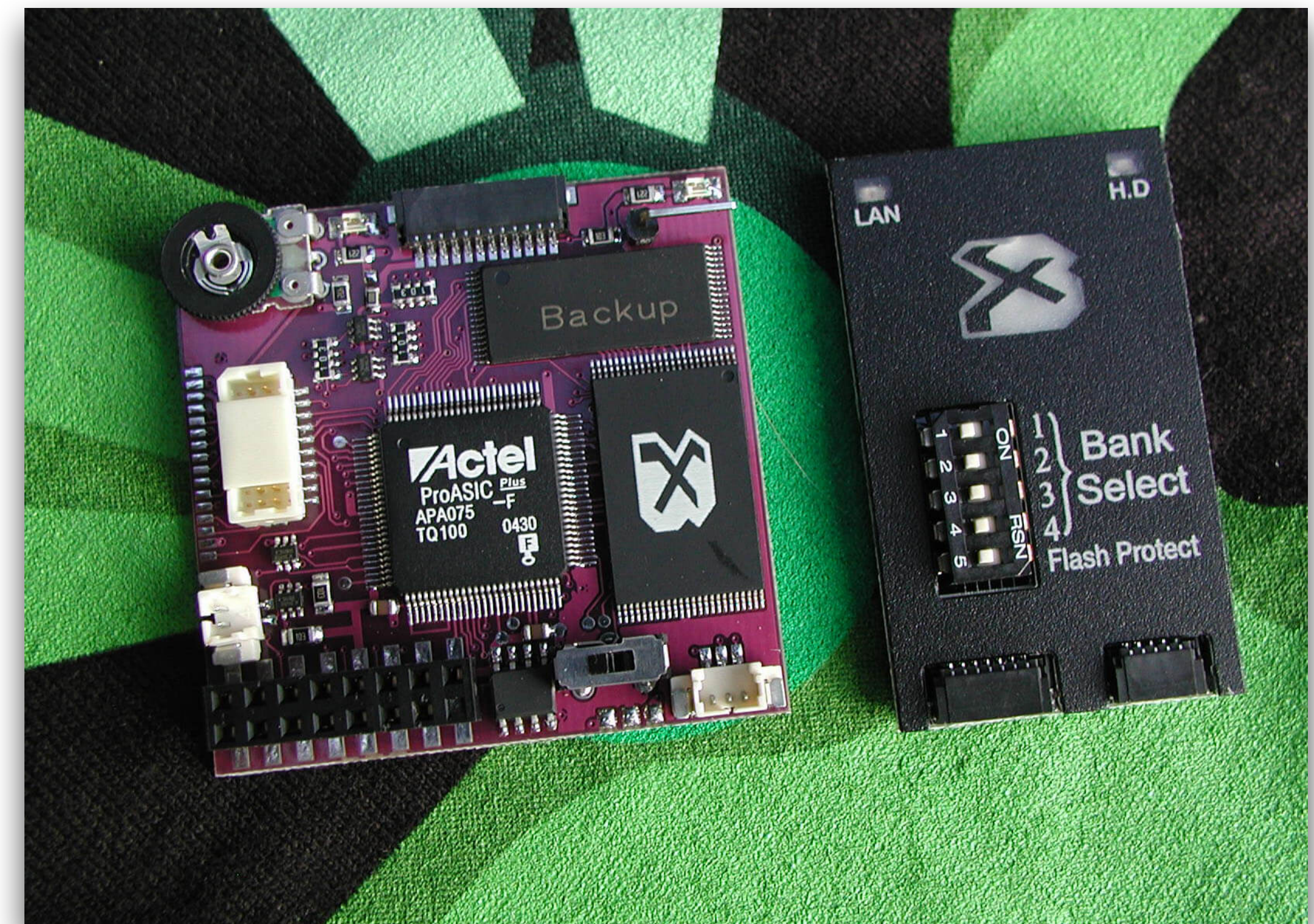
The SoftMod Saves

- James Bond: 007 Agent Under Fire
- Mech Assault
- Splinter Cell
- TonyHawk ProSkater 4
- Frogger



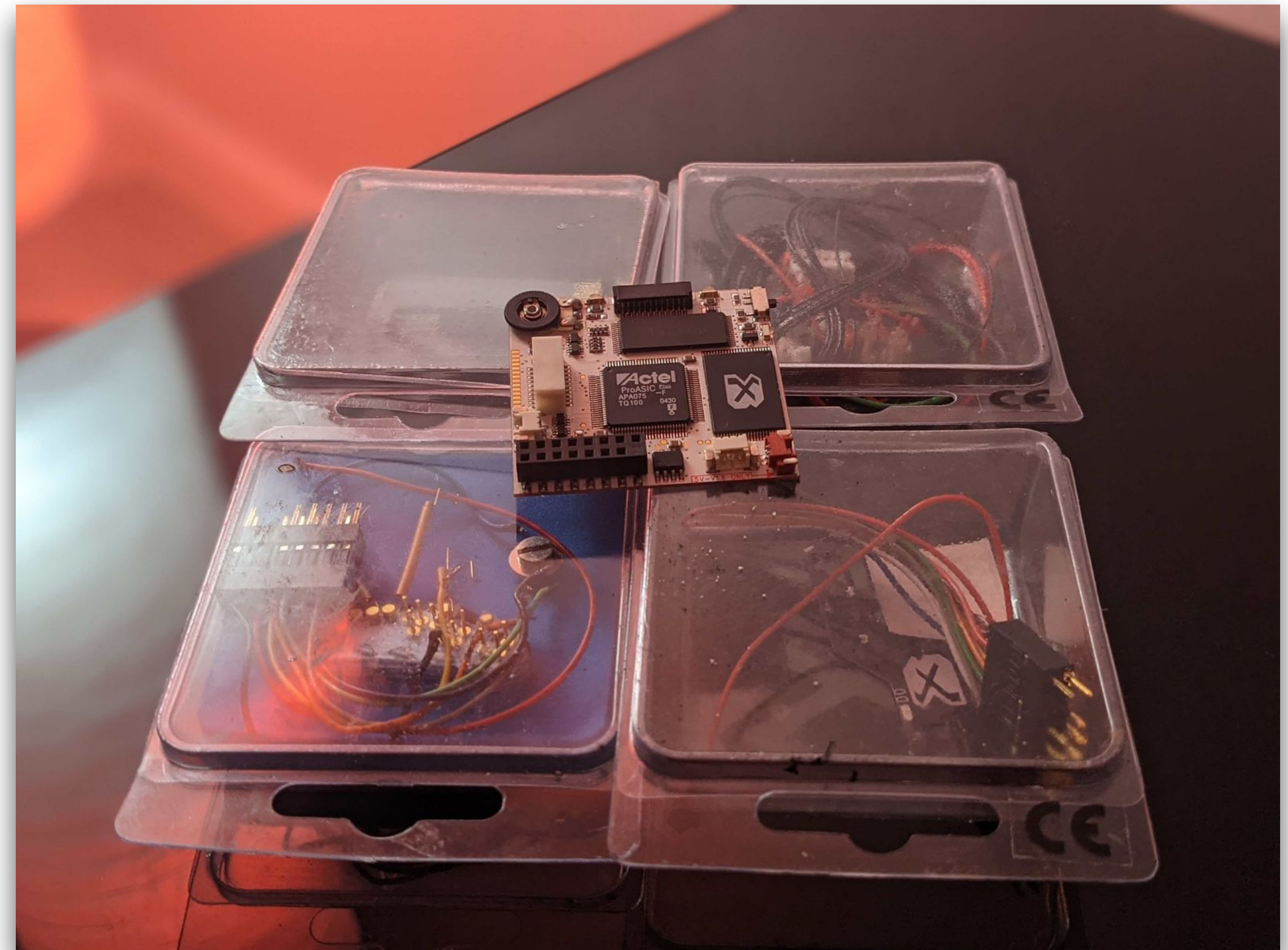
Hardmod?

- Modify an xbox beyond intention **WITH** some form of hardware.
- Modchip common.



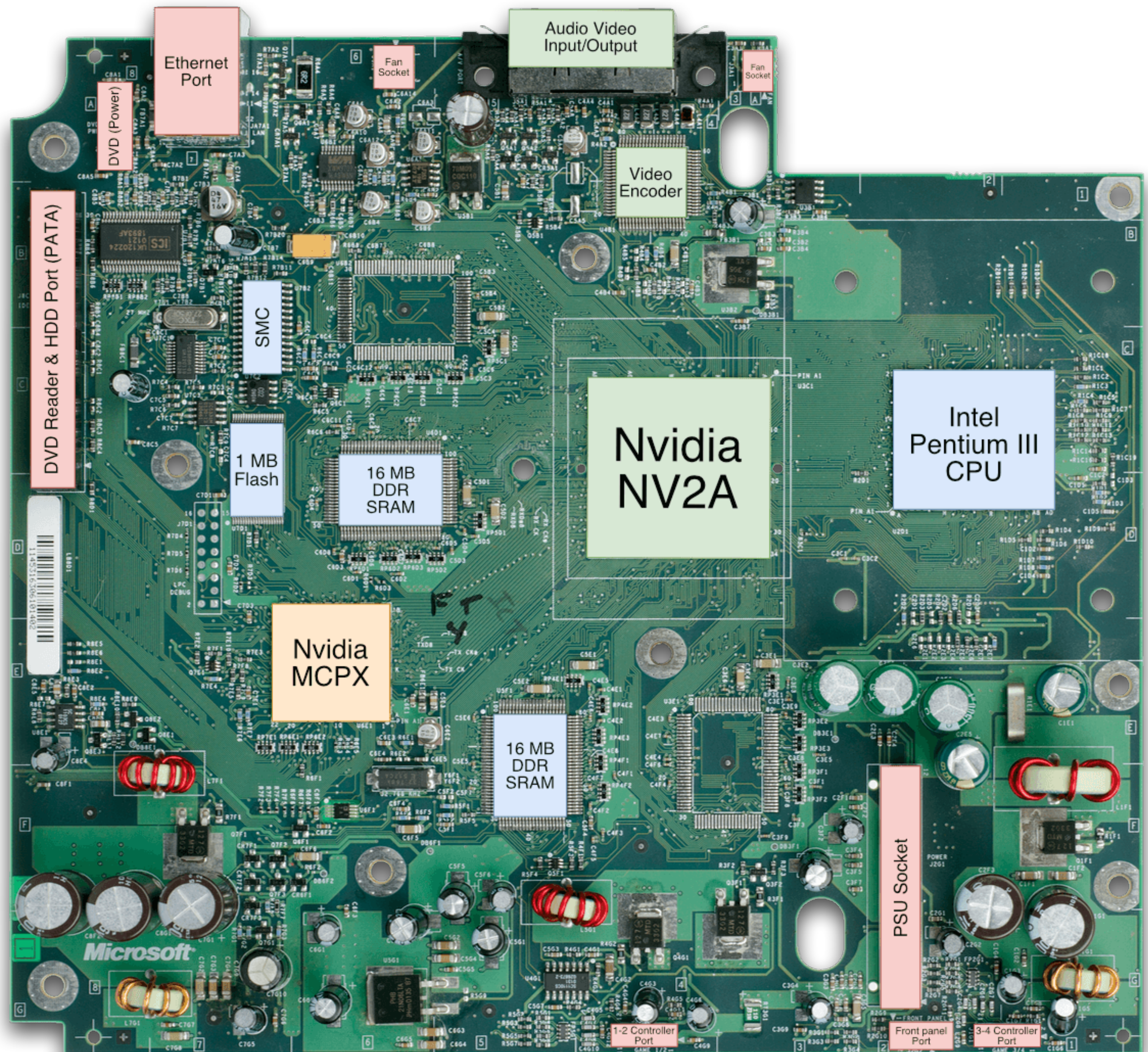
Hardmod Features

- Hardware Upgrades - HDD / RAM
- Custom BIOS
- Forgiving of errors



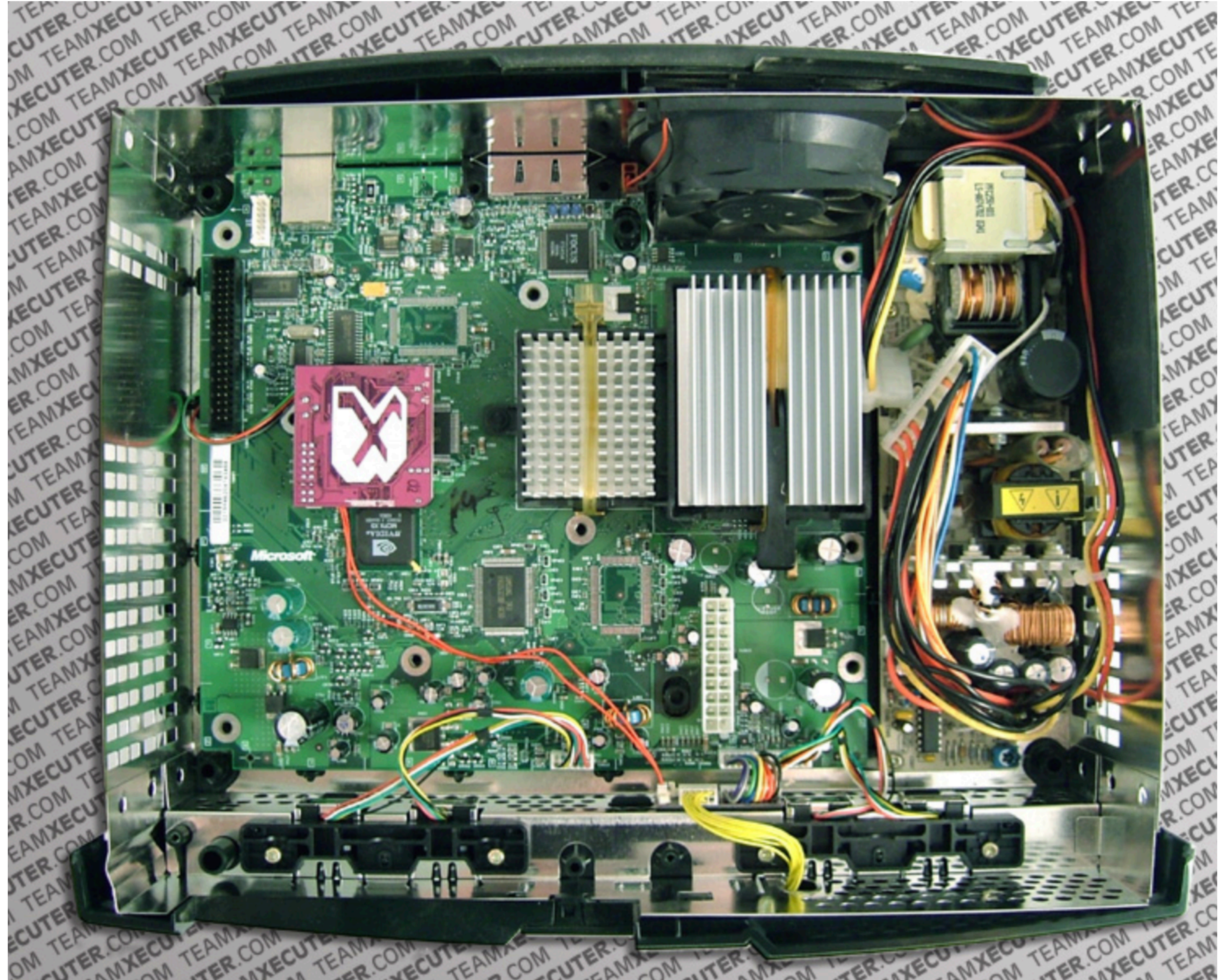
Motherboard

- MCPX
- SRAM (64mb)
- EEPROM



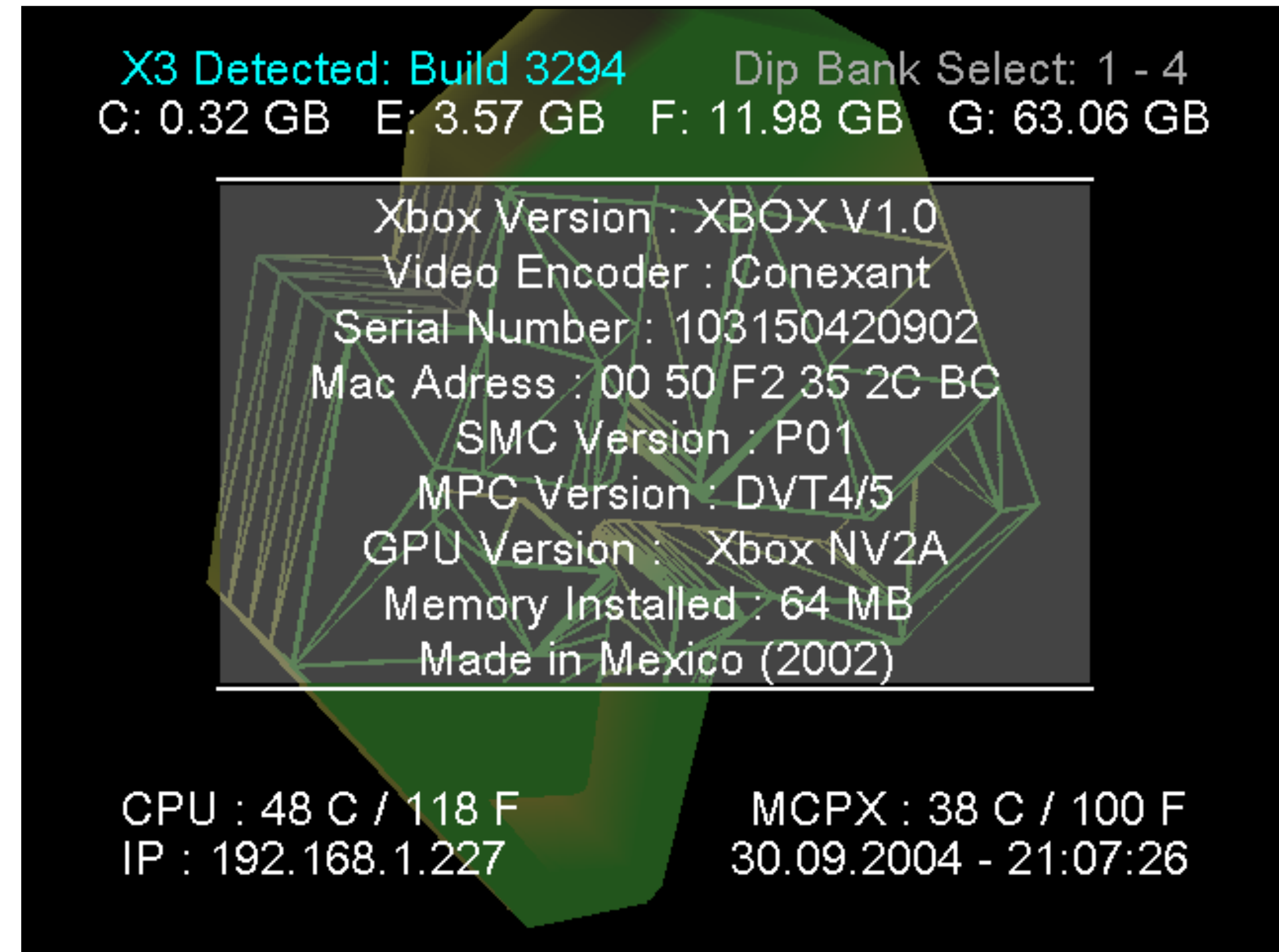
Soldering?

- LPC Port
- HDD LED
- LAN LED
- D0 (trick Ipc)



X3 Config Live - Xecuter

- ⦿ Settings everywhere
- ⦿ BIOS Flashing
- ⦿ FTP Server
- ⦿ Info dump / backups



Bank Settings

- 2MB Bank
- 256k (x8)
- 512k (x4)
- 1mb (x2)
- 2mb

Xecuter 3 Switch Bank Settings

- Note: switch 5 is flash protect. "ON" is protection enabled -

256k Banks



512k Banks



1MB - 2MB Banks



Modded Xbox

- Xecuter 3CE
- 500gb HDD
- Orange Case
- Blue Jewel



Debug BIOS

- Expands features to pair with XDK



XBMC

- You know it as “KODI” now.



Playing modded Halo 2

● Game Trainers - Yelo (xbox7887)

Yelo: Halo 2 (Xbox)

Post Reply



Search this topic...



1204 posts



1

2

3

4

5

...

61



Yelo: Halo 2 (Xbox)

by **xbox7887** » Thu Aug 17, 2006 6:28 pm

Yel-o (yell-oh) *noun*. blam engine hack project for all halo games of all platforms. *syn.* 1337

If you don't know how to use trainers, I suggest you check out www.xbox-scene.com or www.maxconsole.net for further information. Like always, I will not respond to questions already answered in this post and PMs requesting beta content will also be ignored. If you are experiencing problems with the trainer itself, fill out a bug report with a complete discription of what you were doing when it happened, otherwise I won't be able to help.

Along with the trainer, you must also transfer over the "config_v1.5.inc" file to "E:/TDATA/4D530064/". If you fail to do so the trainer will not function properly and immediately go into wireframe at the press of a button. Since I haven't gotten around to writing an editor for the trainer config file, if you would like to make your own changes, you can refer to the included "config_v1.5.txt" which maps out all values. Every combo and a few other options can be edited via the trainer config file. Feel free to share your edited config files in this topic. If it's good I will link it to the main page so others can download as well.

Note that some of the cinematic and lighting options are experimental so if you don't like them, don't use them 😊

- This trainer will only work with the [Xored ETM Launcher v2.2](#) (due to memory allocation issues) so be sure to download that before use.
- Please refer to [Aequitas' UST post](#) for all information regarding screencap recovery.
- If you are using a mac computer you will need to [download](#) a different deswizzler.
- You can grab source examples [here](#) and [here](#).
- Grab the config editor [here](#).
- Having trouble with UST? Try the [alternative](#).
- For those of you that have been complaining about the 1.1 update, Download Snave's mainmenu mod at the bottom of this post[url].



xbox7887



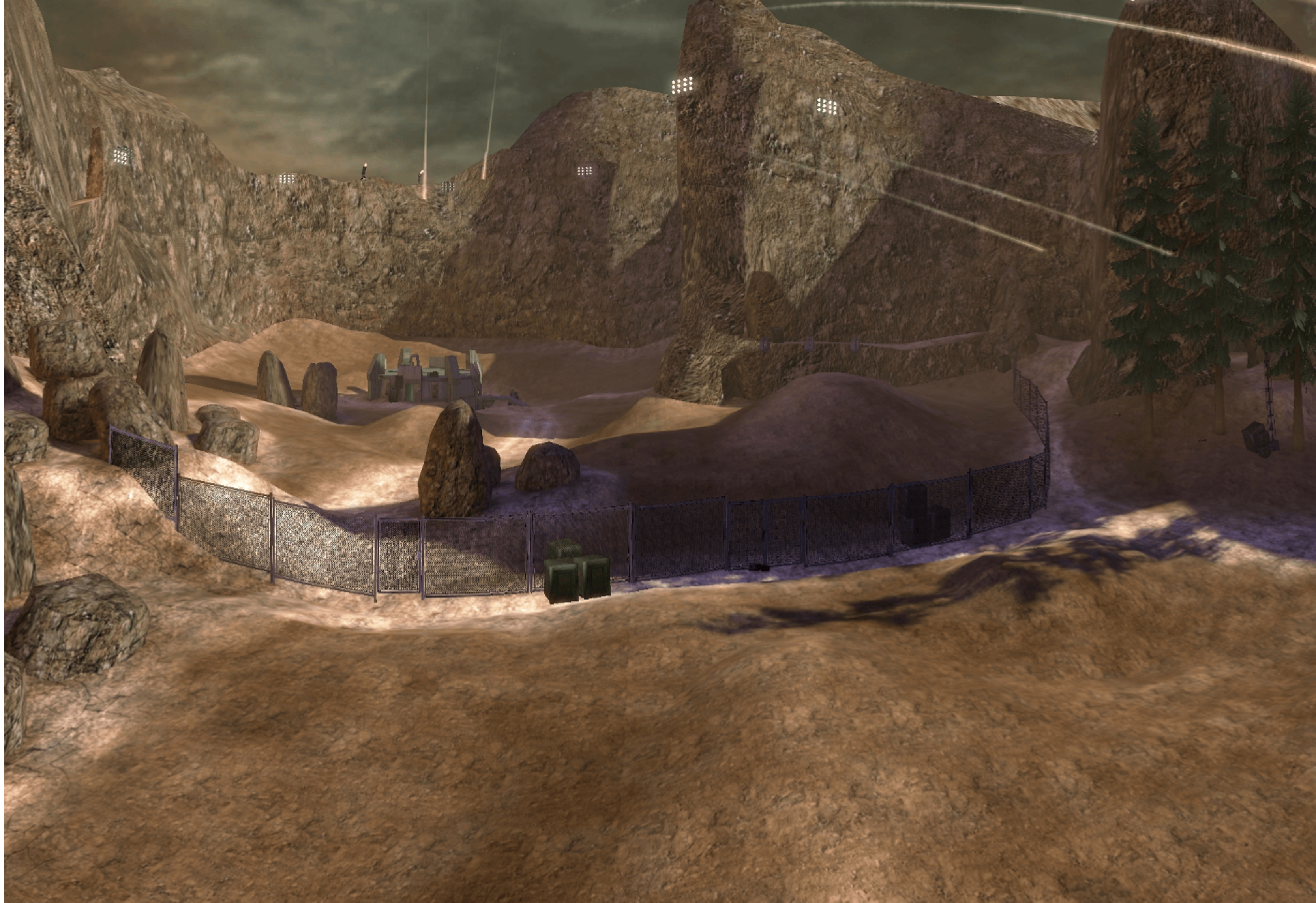
Posts: [2160](#)
Joined: Mon Dec 27, 2004 6:19 pm
Location: New Lenox, Illinois
Contact: [...](#)

Playing modded Halo 2

- AI, Camera, Screenshots

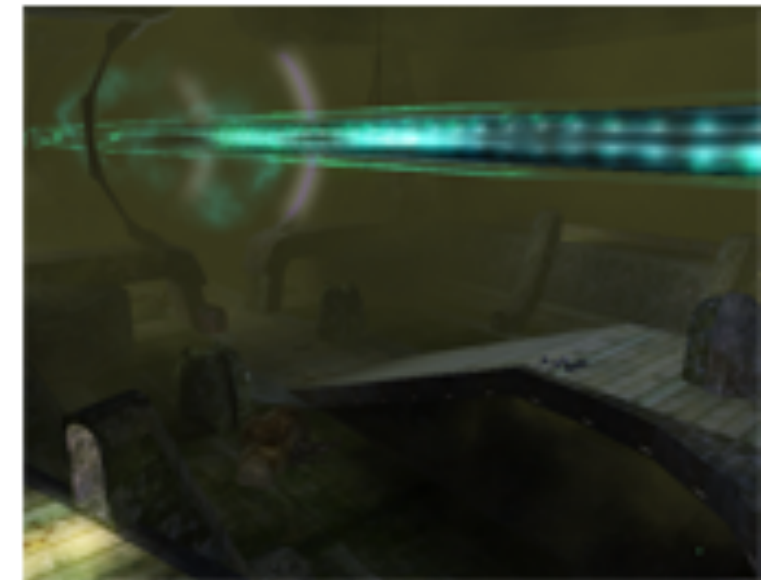
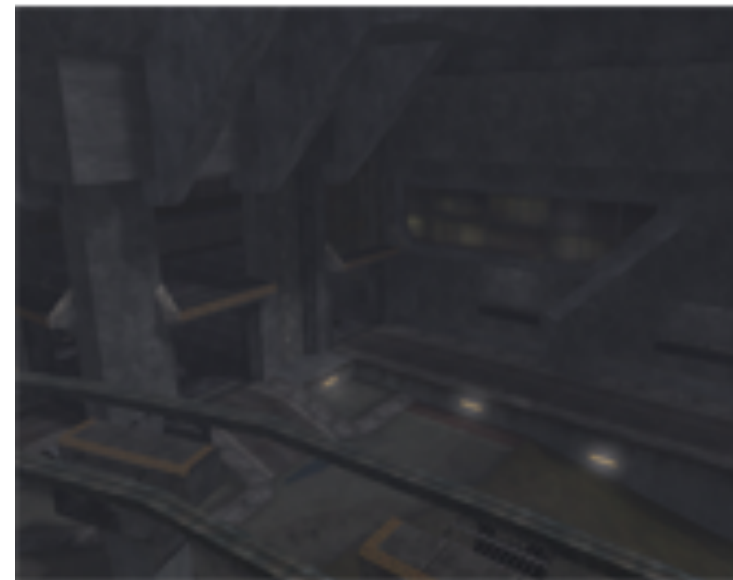
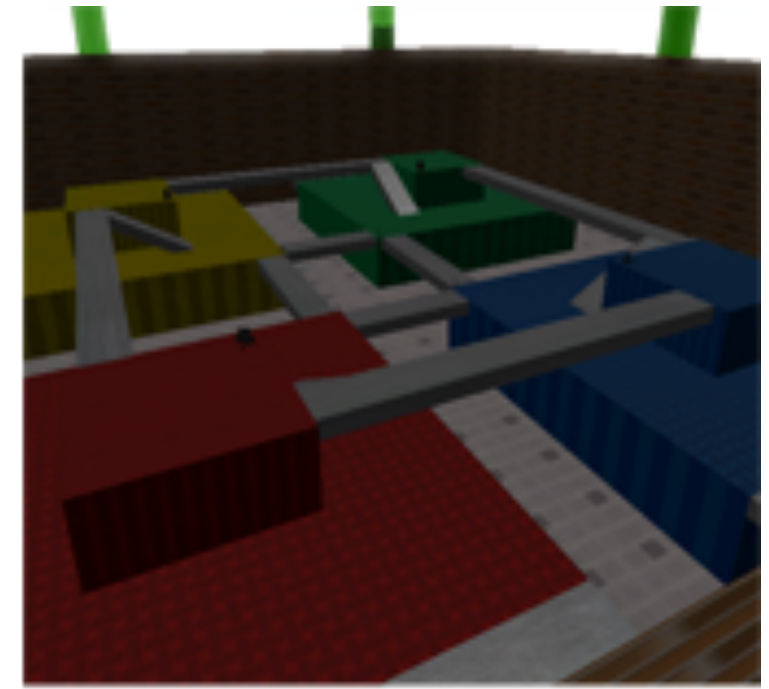
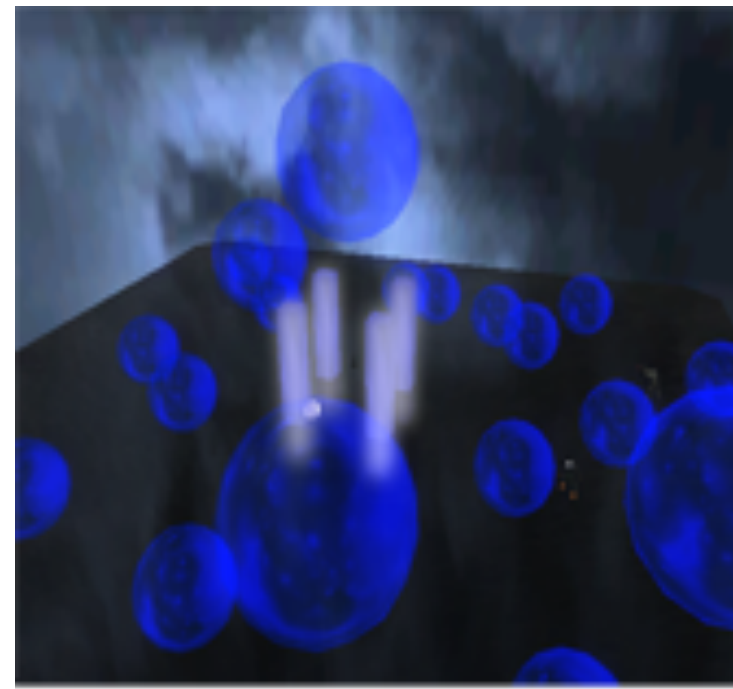


Halo 2 - Havok



Halo 2 Modding

- ◉ Racetracks
- ◉ Campaign ports
- ◉ Creative mods
- ◉ New models (weapons/vehicles)
- ◉ Alternative sandbox



Halo 2 Mappack - Phantom

4

XBOX

ISBN 0-7806-2041-0

7 94043 45772 2

ONLINE ENABLED

Phantom

90 maps

Made by: iBotPeaches

Cellmates
CaptainPoopFace

PLAYERS 1-4

SYSTEM LINK 2-16

ONLINE MULTIPLAYER

MEMORY UNIT 8 BLOCKS

HDTV 480P

VOICE

CUSTOM SOUNDTRACKS

TEMPLATE BY C.R.

FRIENDS

IN-GAME DOLBY DIGITAL

CONTENT DL

SCOREBOARD

Xbox Live System Requirements:

•High-Speed Internet Service (Cable or DSL)

•Internet Cable (not included)

•Subscription to Xbox Live service* (sold separately)

Performance may vary based on game, internet service speed, network activity, or capacity. Depending on you internet service connection or network configuration, additional hardware may be required. Most high-speed internet serviced will work with Xbox Live: some may not. Check with your service provider.

*Available in the 50 U.S., D.C., Canada & Puerto Rico. Subject to terms of use (see <http://www.xbox.com/live/legal>). Major credit card required. Xbox live not intended for kids under 13.

IMPORTANT! Read Instruction Manual for important safety and health information.

Dolby and the double-D symbol are trademarks of Dolby Laboratories. High Definition AV Pack or Advanced AV Pack requires the Dolby Digital. Sold separately. CF and the Coverflend logo are trademarks of coverflend.com and its associated affiliates. The ratings icon is a trademark of the Interactive Digital Software Association. Microsoft, Xbox and the Xbox Logo are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and / or in other countries. *Xbox Live only available in the U.S. and Canada. Use is subject to the xbox Live Terms of use. Major credit card required. Not intended for children under the age of 13.

MATURE

Blood And Gore
Mild Lyrics
Intense Violence

ESRB CONTENT RATING

Game Experience May Change During Online Play.

xbox

LIVE ONLINE ENABLED

Tokyo
MrBall

Phantom

MATURE

CONTENT RATED BY ESRB

Halo 2 Prank Mods

- Soccer Tourney
- Out of Town
- Friend on Team
- Bring Xbox
- Prank



Halo 2 Modding + Xbox

- ◉ Open research
- ◉ Many tools
- ◉ Forums on forums
- ◉ **Free!** (This will make sense later)



Why was the Xbox so hackable?

- Dash Vulnerabilities
 - Bert n Ernie
 - Fonts & Playlists
 - dashupdate.xbe (xbox live update)

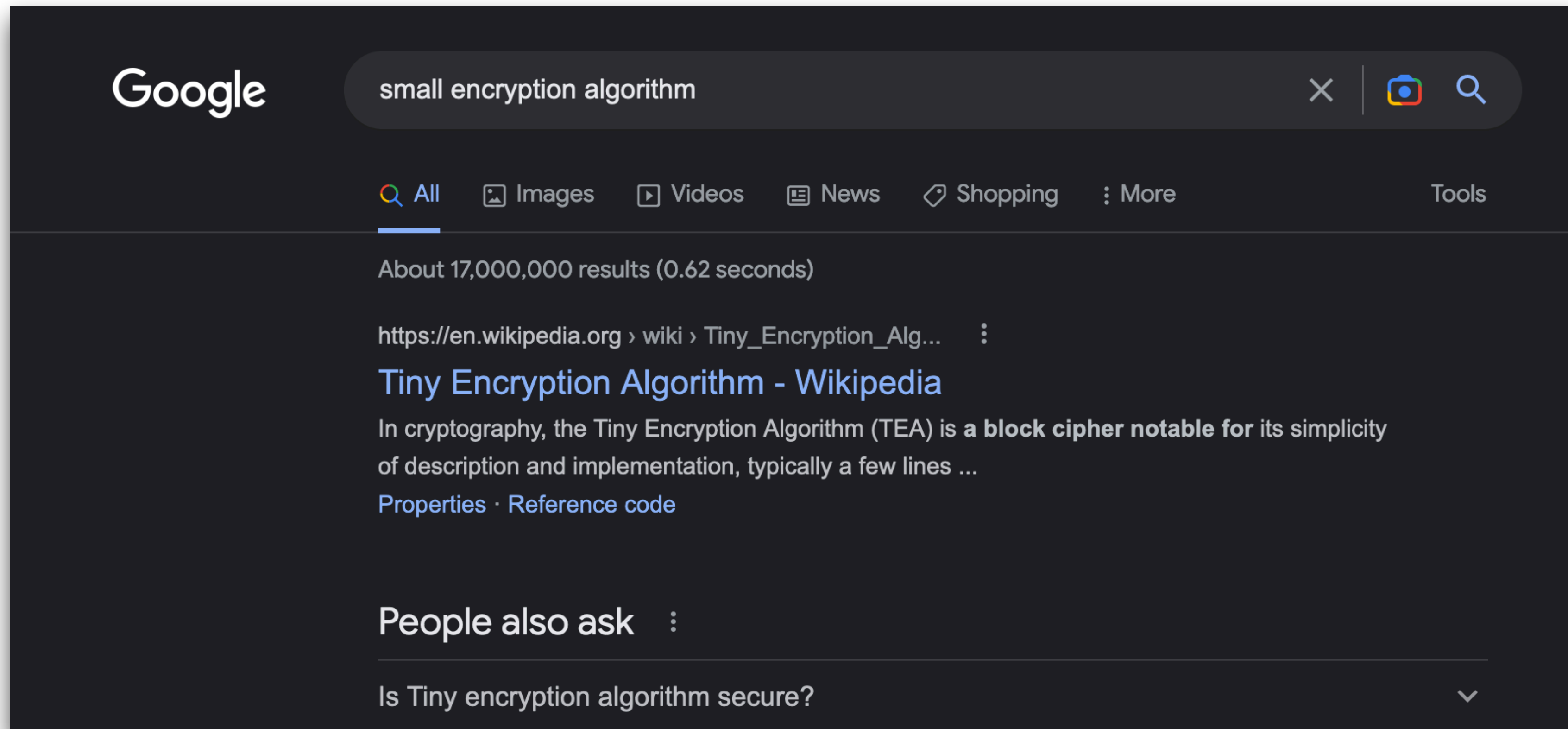


Why was the Xbox so hackable?

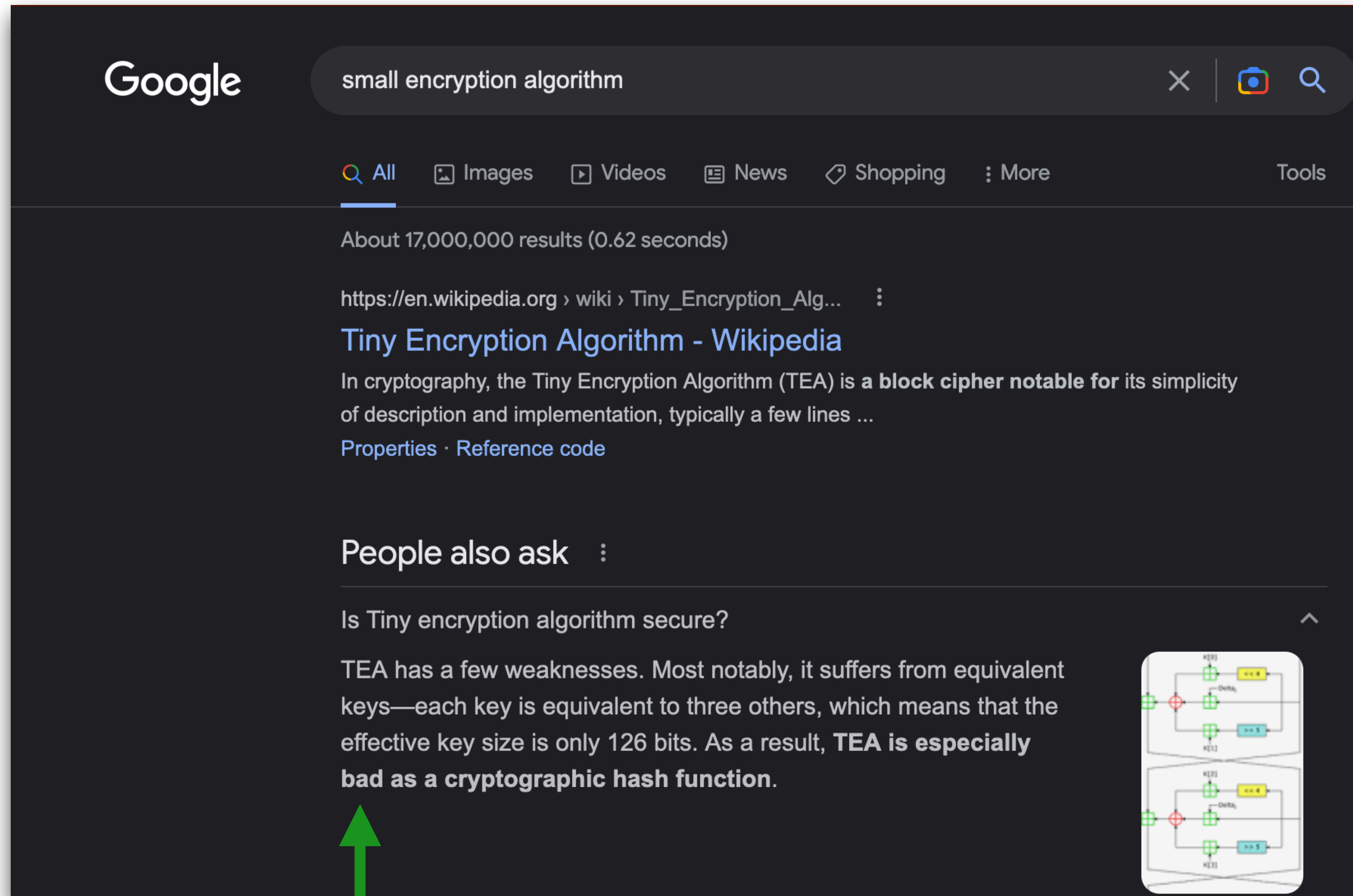
- Downgrade to **RC4**, from **RC5**
 - MCPX 1.0 only checks last few bytes.
- Rushed updates
 - Trashed chips (1.0)
 - 1.1 was also bugged.

Why was the Xbox so hackable?

- Swapping AMD to Intel late
- Tiny Encryption Algorithm (TEA)



Why was the Xbox so hackable?



The screenshot shows a Google search interface with the query "small encryption algorithm". The search results page displays "About 17,000,000 results (0.62 seconds)". The top result is from Wikipedia, titled "Tiny Encryption Algorithm - Wikipedia". The snippet describes TEA as a block cipher notable for its simplicity. Below the snippet, there are links for "Properties" and "Reference code". A "People also ask" section is visible, with the question "Is Tiny encryption algorithm secure?". The answer states that TEA has weaknesses, including equivalent keys, and is "especially bad as a cryptographic hash function." A green arrow points from the bottom left towards this text. To the right of the answer is a diagram of the TEA encryption process, showing two rounds of computation with subkeys and XOR operations.

Google

small encryption algorithm

Q All Images Videos News Shopping More Tools

About 17,000,000 results (0.62 seconds)

[https://en.wikipedia.org › wiki › Tiny_Encryption_Al...](https://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm)

Tiny Encryption Algorithm - Wikipedia


In cryptography, the Tiny Encryption Algorithm (TEA) is a **block cipher notable** for its simplicity of description and implementation, typically a few lines ...

[Properties](#) · [Reference code](#)

People also ask

Is Tiny encryption algorithm secure?

TEA has a few weaknesses. Most notably, it suffers from equivalent keys—each key is equivalent to three others, which means that the effective key size is only 126 bits. As a result, **TEA is especially bad as a cryptographic hash function.**

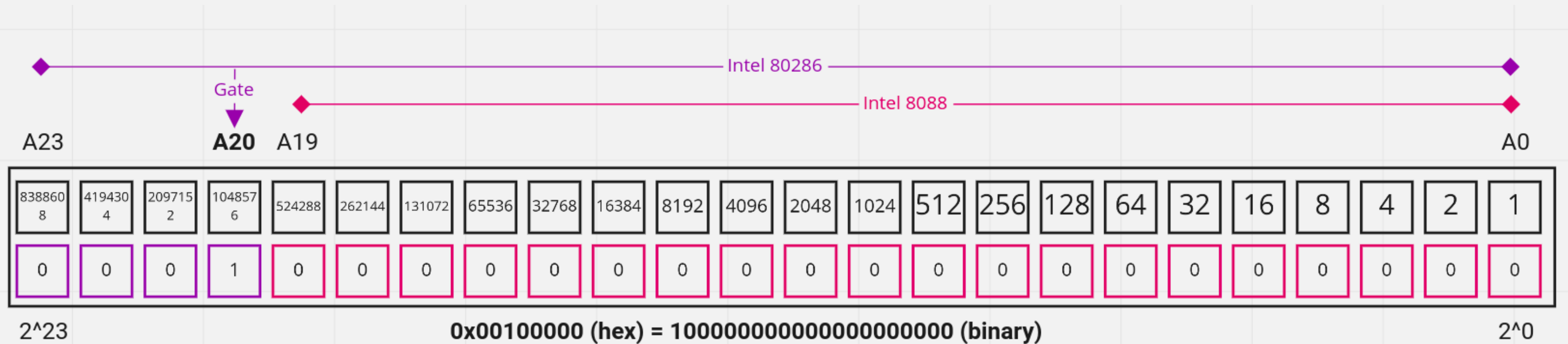


Why was the Xbox so hackable?

- Flash memory. LPC ports.
- Easy to connect to hardware
- CPU Wraparound - early Intel feature
- A20 Gate - Backward compatibility

A20 - Address Lines

- 16 bit processor
- 20 bit physical space
- So what about F800:8000?



A20 - Address Translation

segment:offset

0xF800:0x8000

$(\text{segment} * \text{shift}) + \text{offset}$

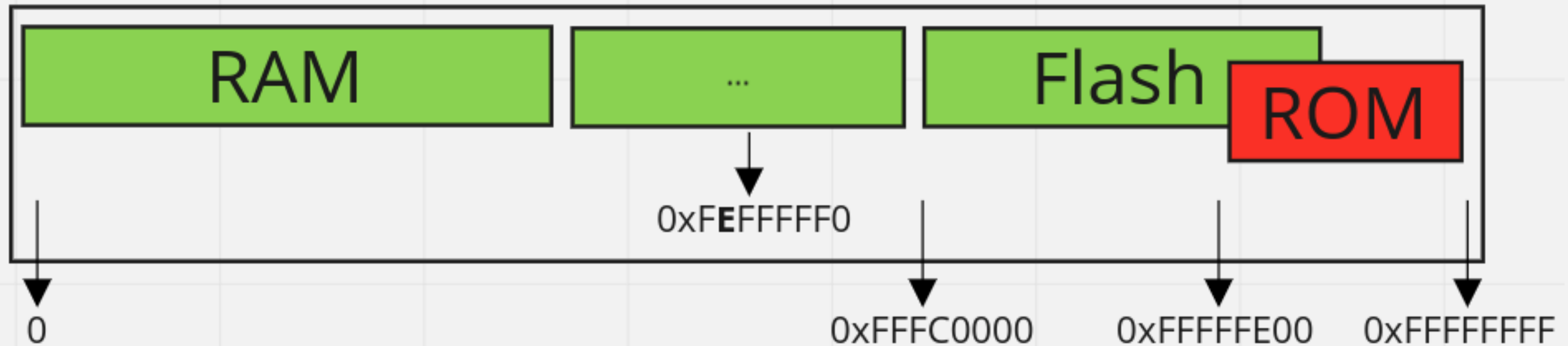
$(0xF800 * 0x10) + 0x8000$

physical address

0x00100000

A20 - The Nerd Details - Part 3

- *0x00100000* over 1MB oops.
- The 21st bit, A20 causes shift
- Bonus - Secret ROM still on!



The Next Generation



360 Time

- JTAG
- Test Kit
- Xenons
- Halo Edition
- Disc Format



Xbox 360 Teams & Homebrew

- Xbox-Linux Team (Xbox)
- Free60 Team (Xbox 360)
- Backward Compatibility
- Emulation
- XeLL (legal loader)



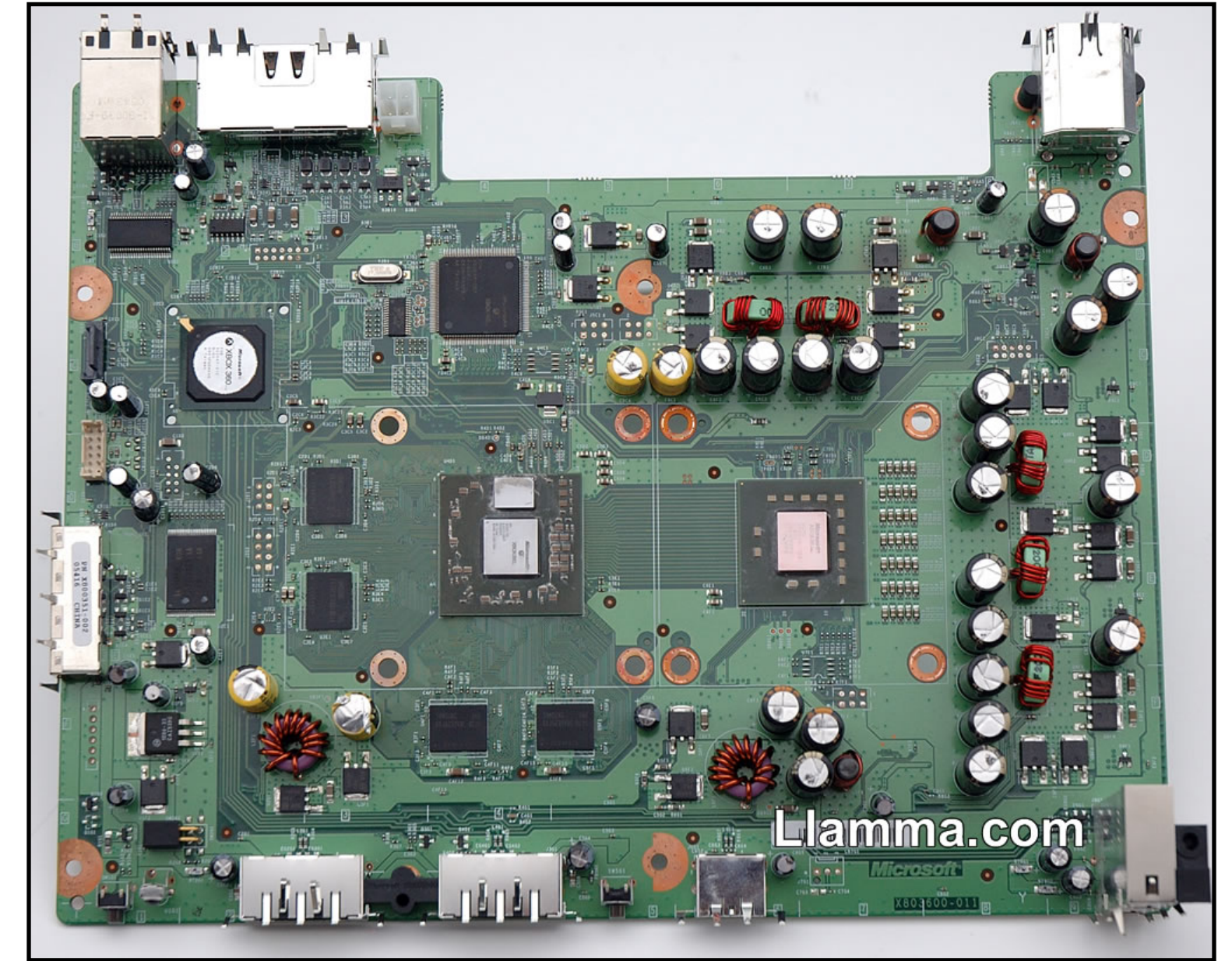
Xbox 360 - RRoD

- Sadness.
- \$1.2~ billion fix
- Balmer approved
- Mobo Revisions



Xbox 360 Codenames

- Xenon (RRoD)
- Zephyr (Added HDMI, RRoD Fix)
- Opus (Patched RRoD for Xenon)
- Falcon (New CPU + Cooler)
- Jasper (New GPU)
- Trinity / Corona / Winchester (Slim & E)



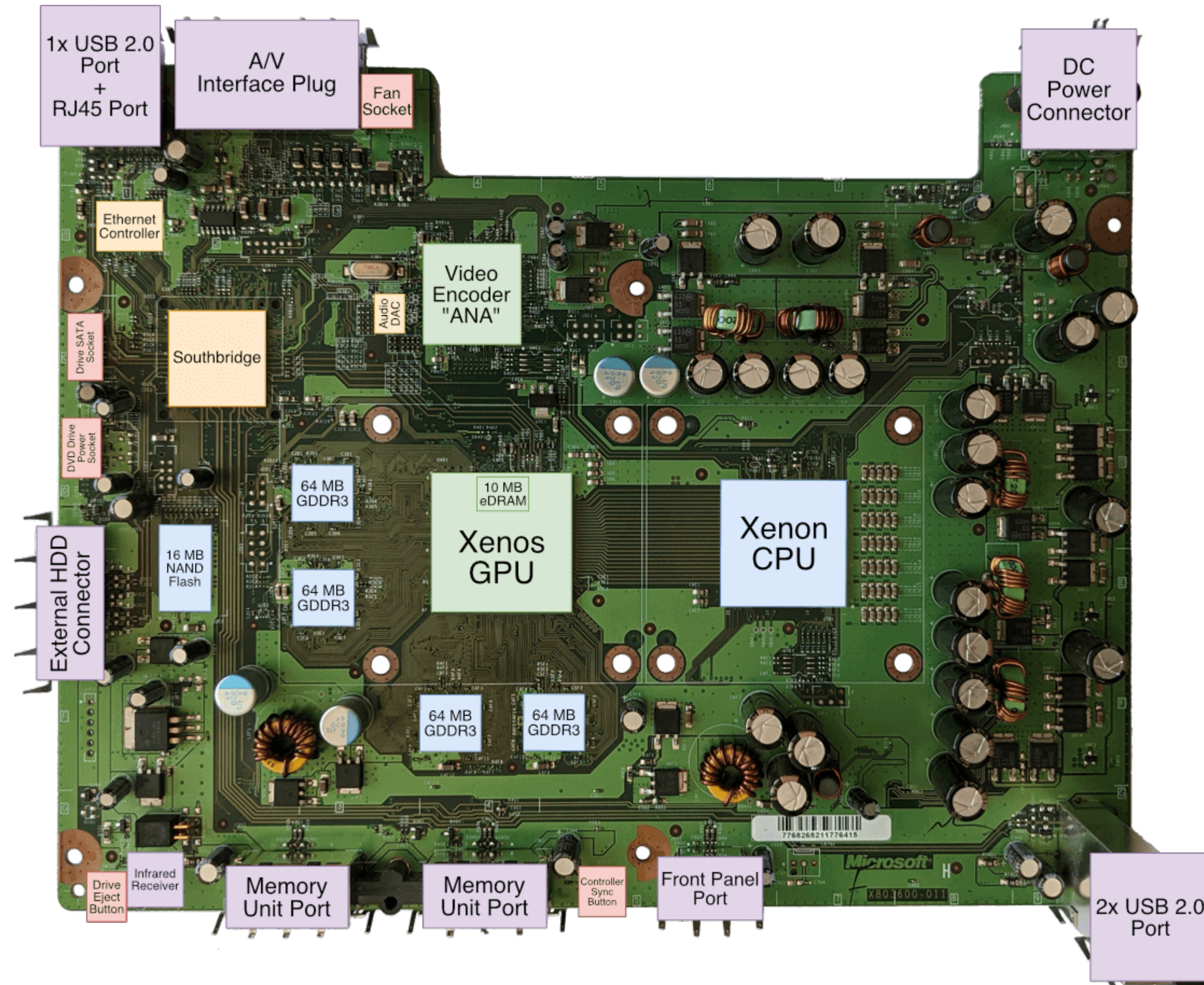
Xbox 360 Boot

- **1BL** - CPU ROM
- **CB (2BL)** - NAND - Preps MEM
- **CD** - Decrypts **CE** into RAM, checks
- **CF** - Decrypts patches, patches **CG**
- Boot patched kernel/dash



Xbox 360 Motherboard

- AES-128 (L2)
- CPU
- RAM
- SRAM



Xbox 360 eFuses

- Hardware level changes
 - Blown bit by bit
- 00-01: JTAG
- 02: 2BL
- 03-06: CPU
- 07-11: Counter

```
Fuseset 00: 110001111111111111
Fuseset 01: 01010101010110
Fuseset 02: 0100000000000000
Fuseset 03: 10011111101100000001011101000000001010101110100010100000000000
Fuseset 04: 10011111101100000001011101000000001010101110100010100000000000
Fuseset 05: 1101010101101001101110101101011010010101100011011011000000000000
Fuseset 06: 1101010101101001101110101101011010010101100011011011000000000000
Fuseset 07: 1111000000000000
Fuseset 08: 0000000000000000
Fuseset 09: 0000000000000000
Fuseset 10: 0000000000000000
Fuseset 11: 0000000000000000
```


Xbox 360 - Disc Security (XGD)

- **Xbox Game Disc 2/3**
- DVD Key derived from CPU Key
- Tricks Table of Contents for DVD player
- Security Sector validation
 - Intentionally invalid blocks to scan.
- XGD3 - Larger available space.

Early Mods - Xbox 360

- Security is tougher.
- Kits are the way.
 - Test/Demo Kits
 - Dev Kits
 - Stress Kits



\$\$\$ to Enter, \$\$\$ to Make

- Kits “obtained” and resold.
- Ranging \$200-\$2,000
- What is legal?
- Tough barrier of entry



XNA Test Kit

The First Hack

- ◉ Needed an old kernel
- ◉ Hotswap
- ◉ Modify KingKong
 - ◉ Since unencrypted
- ◉ Shader Exploit
 - ◉ DMA to RAM



Patch: CB 1920 Update

- Manufacturing Mode patch
 - Add CPU key for encrypting 4BL
- New discovery: **zero out** pairing mode
 - Land on any patch intended.

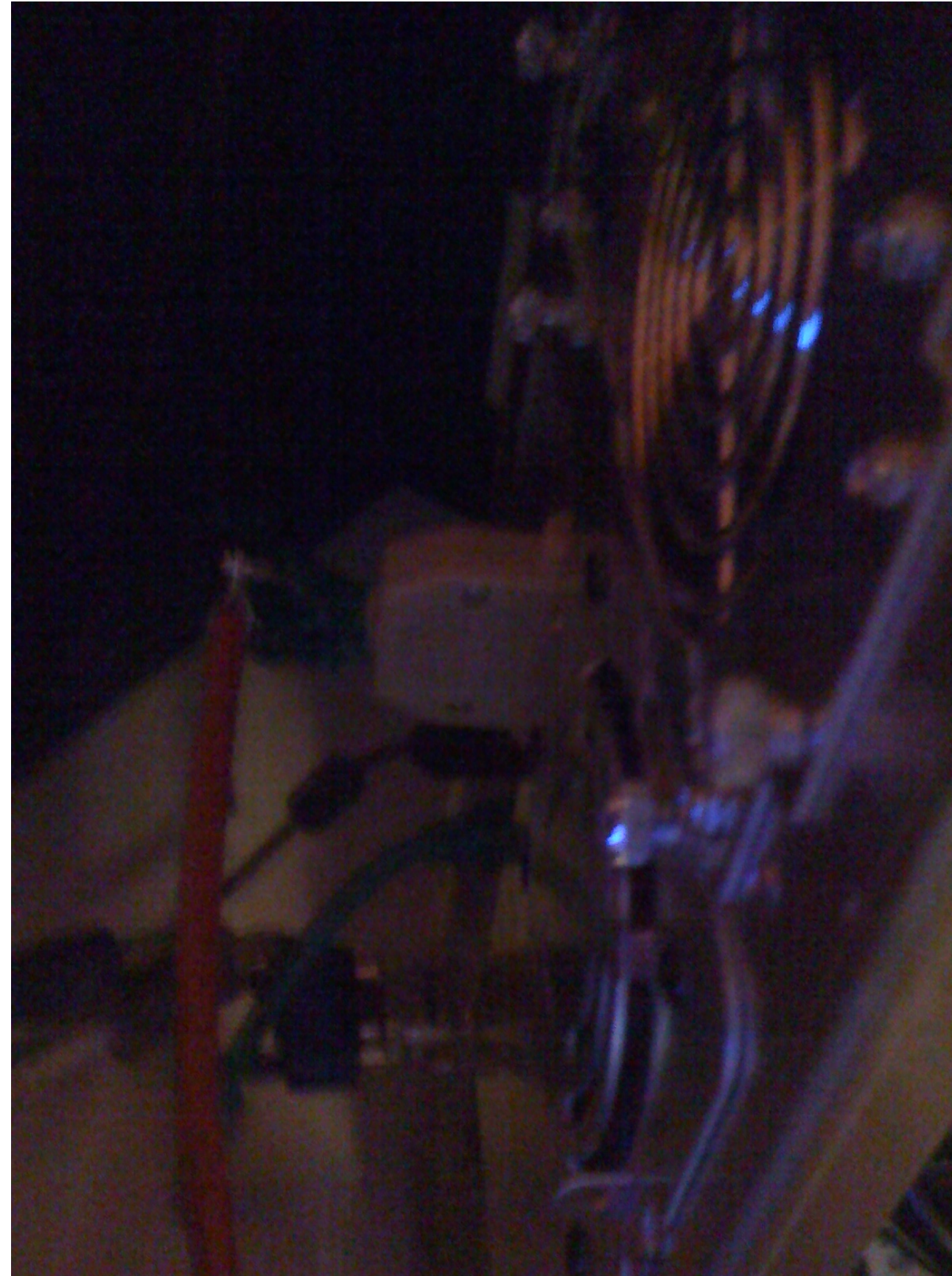
The Second Hack - SMC / JTAG

- Bridge some points - Soldering
- Dump your NAND - More Soldering
- Build the exploit
- Unsigned shader -> memory export
- Quite complex chained together

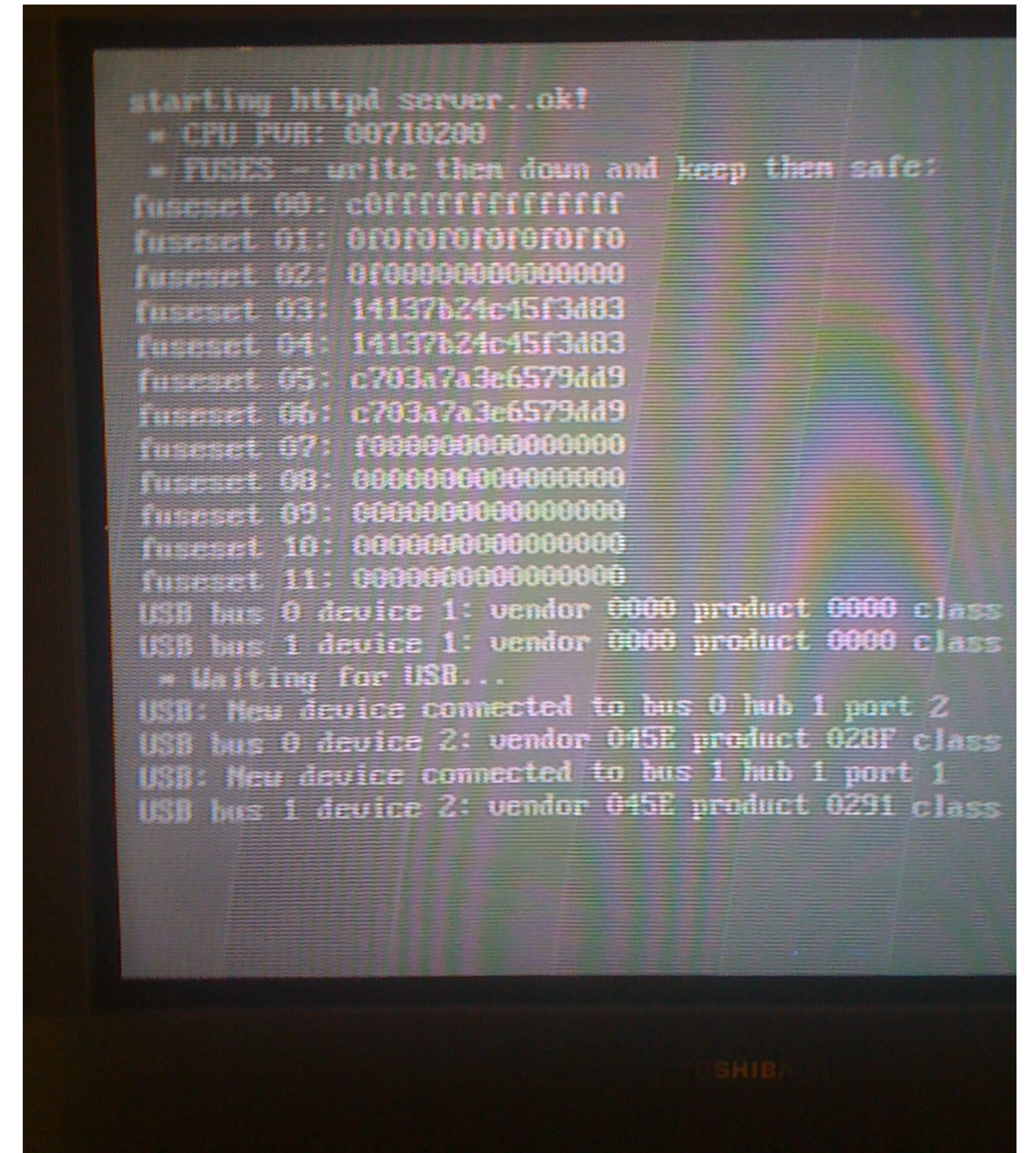
The Second Hack - SMC / JTAG



Attaching points



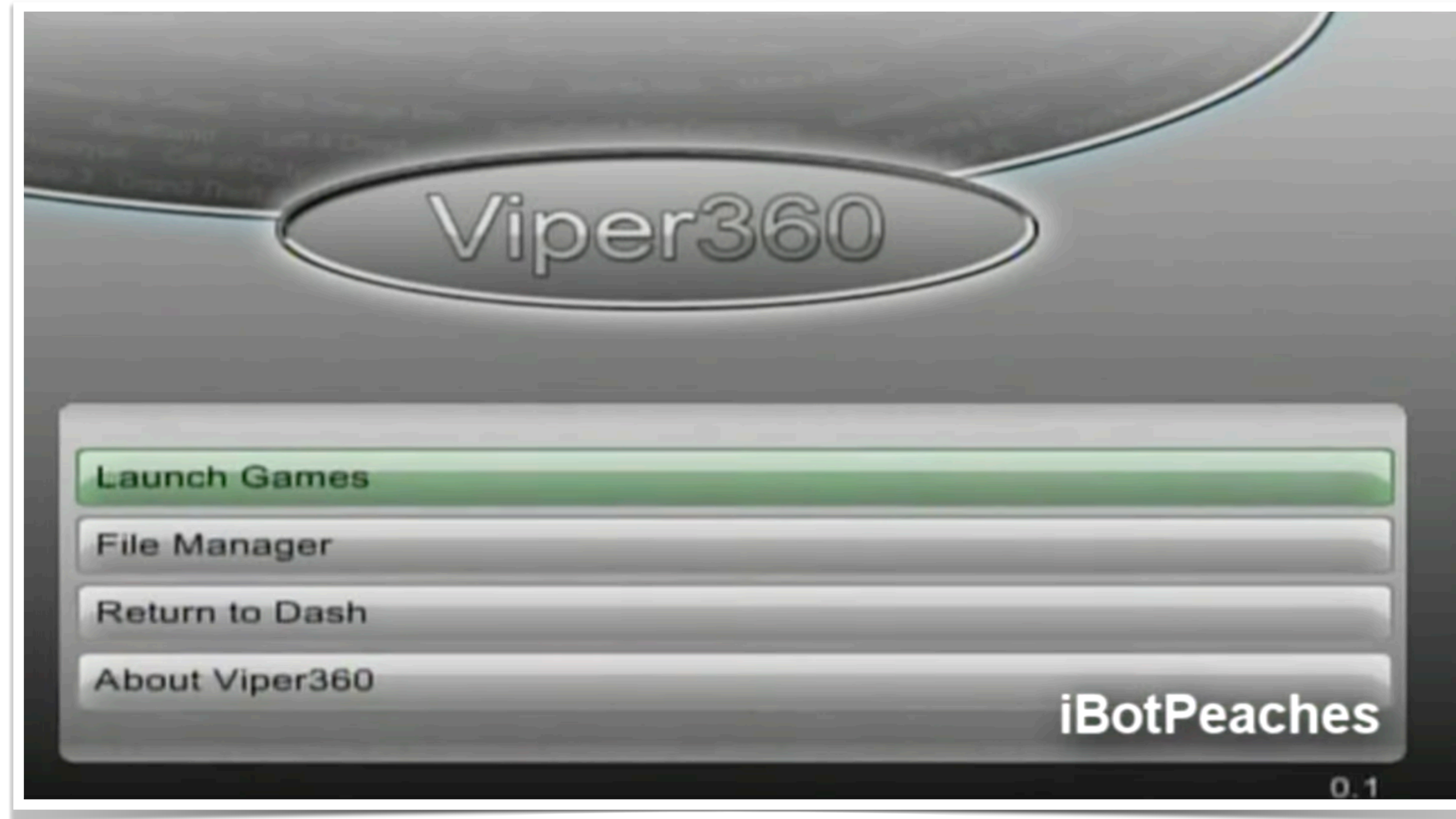
NAND Cable Built



Dumping your NAND

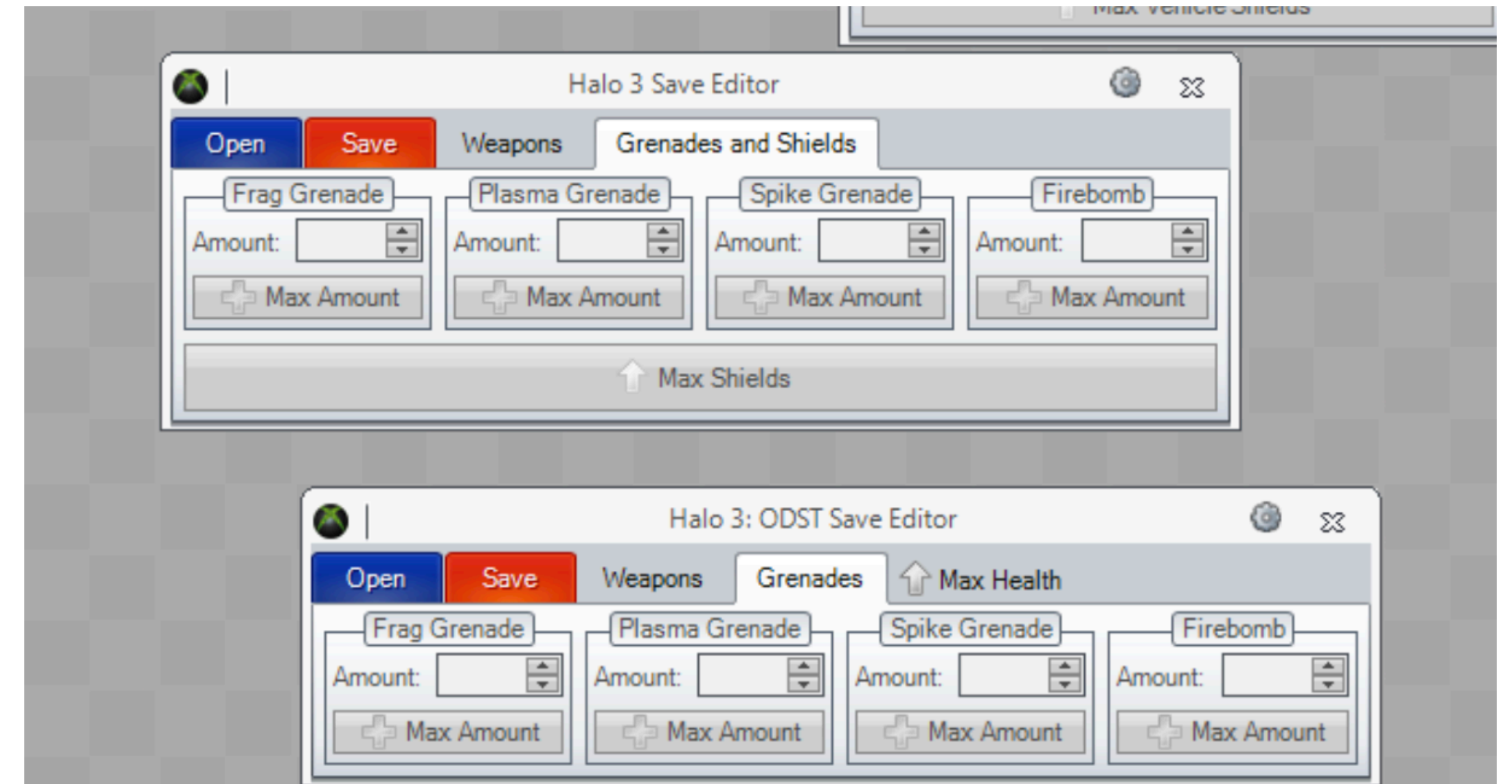
Early 360 Software

- Early homebrew
- File manager
- Apps on Dash
- Custom XEXs



“Scene” Competition

- Horizon vs Modio vs Valhalla
- Pay for save game exploits
- Modded COD lobbies, FIFA coins
- Escalates further
- :(

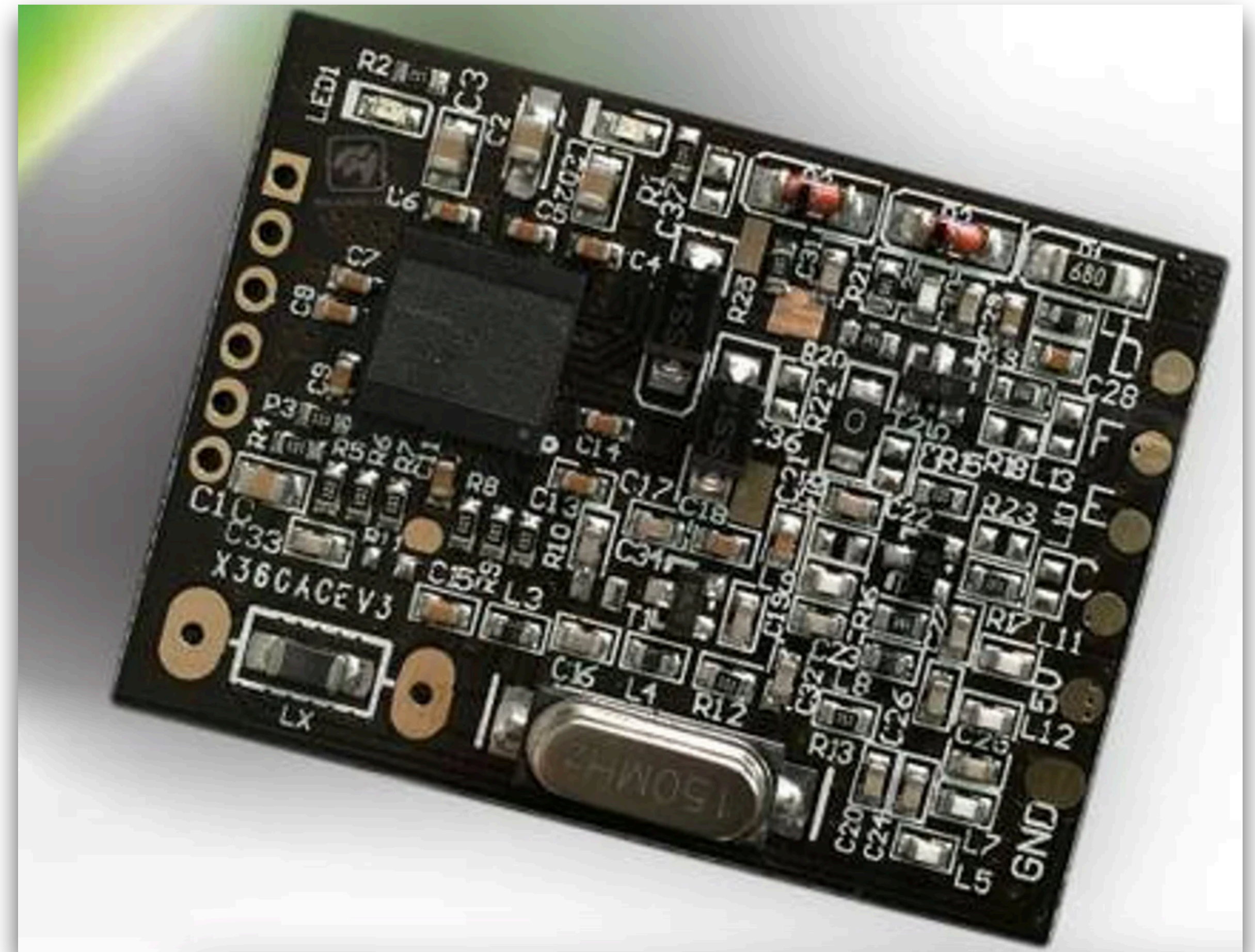


New method on Horizon - RGH

- **Reset Glitch Hack** - Any “fat” model.
- Dump your NAND
- Build exploit
- Slow CPU, Prevent Reset, Remove RRoD,
Glitch CB_A, Boot custom CB_B

RGH Hardware

- Hardware Help
- \$\$\$
- Automation to ease process



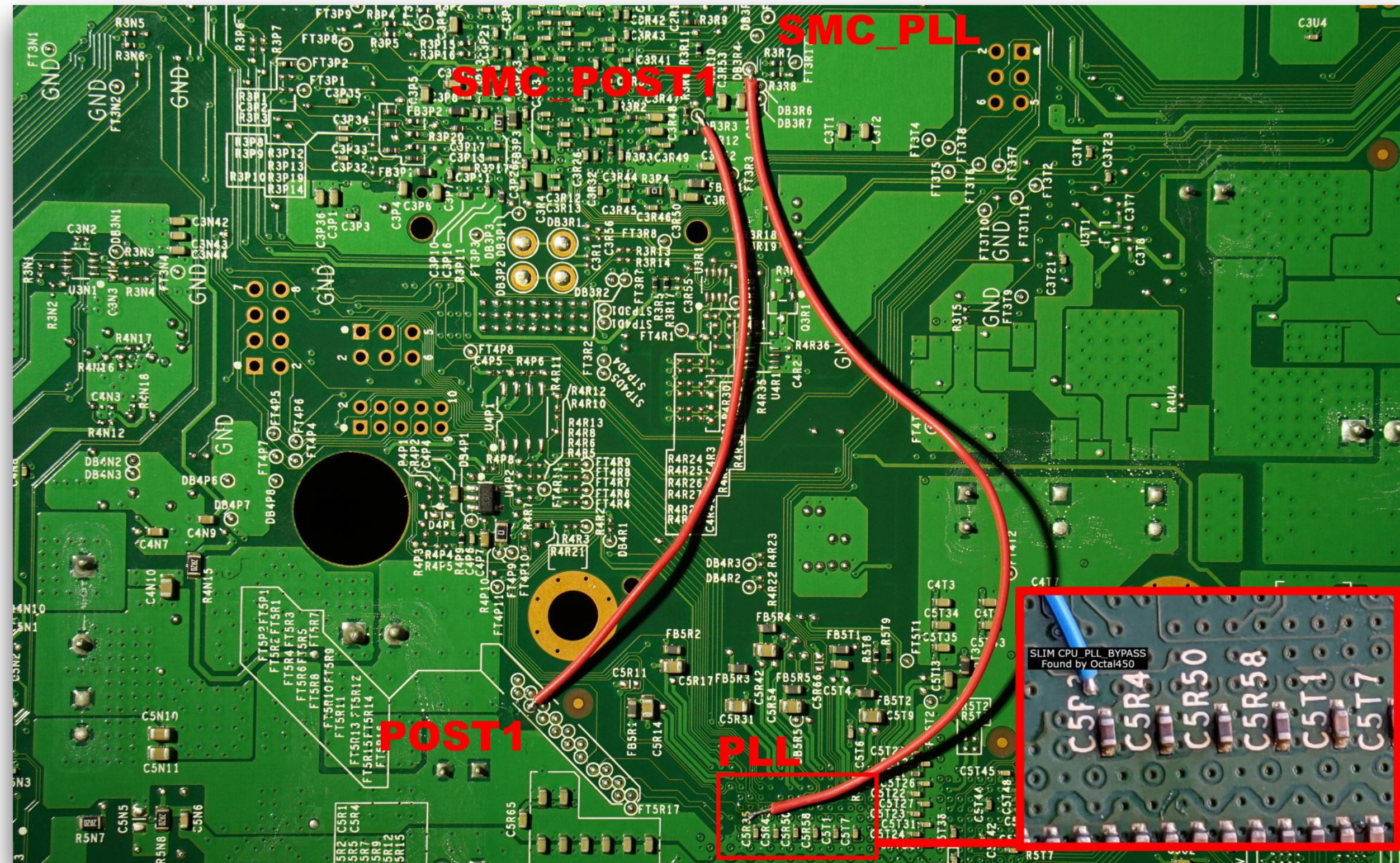
Winchester - Xbox 360 E

- Timing Fixes
 - No more POST OUT
 - Filters external disturbance
- **RGH** dead :(
- 3 years after discovery.



RGH3.0 - Arrival

- RGH all 360s!
- (except Winchester)



Modding Halo - 360

- Basic
- Swaps
- Assembly



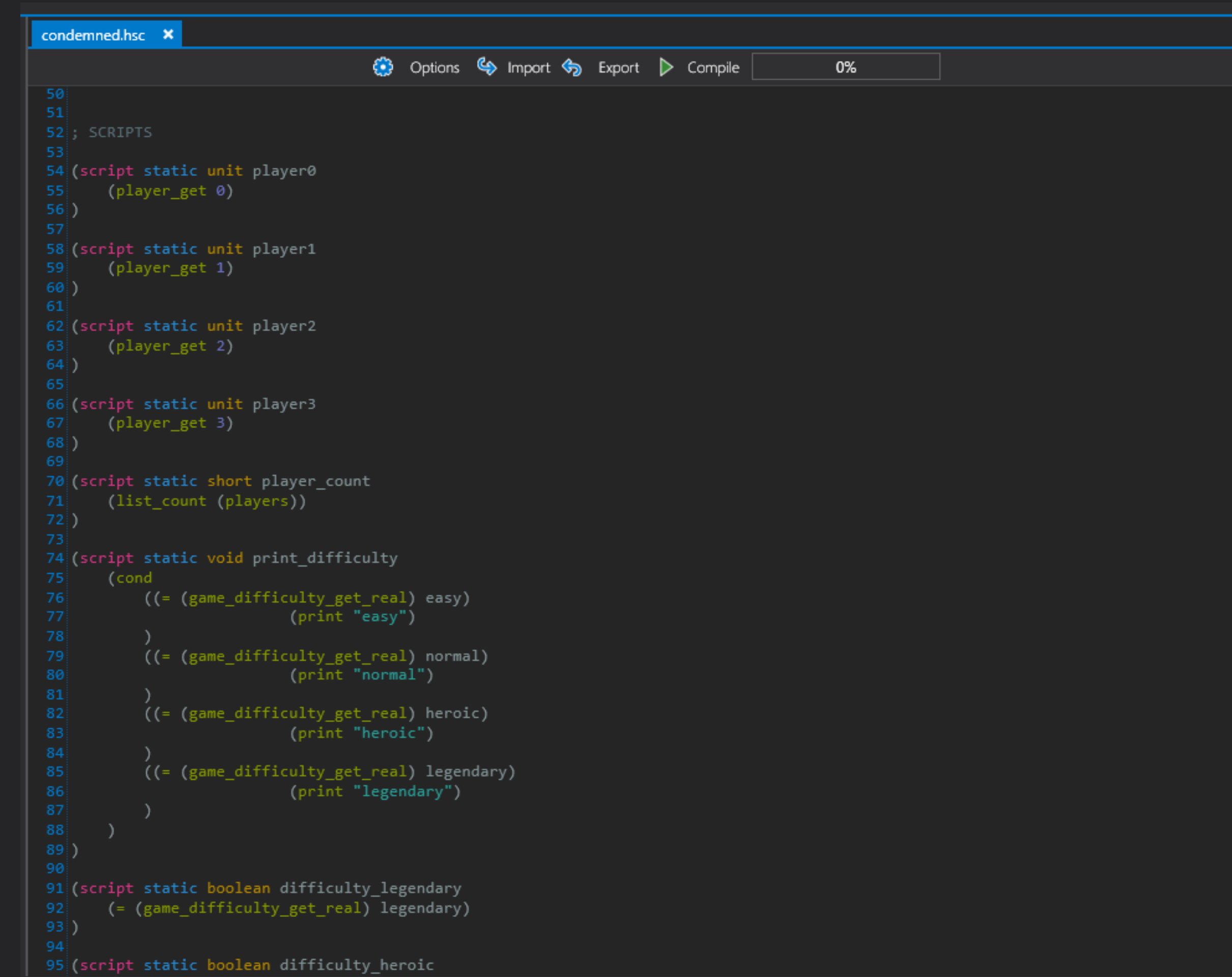
Modding Halo - 360

- Models
- Funny
- Localized



Gametypes & Map Scripts

- Megalo
- Sharing
- Creative
- Fileshares



The screenshot shows a code editor window with a single tab titled 'condemned.hsc'. The editor has a dark theme and a toolbar at the top with icons for Options, Import, Export, and Compile, along with a progress indicator showing '0%'. The code is written in a scripting language and is as follows:

```
50
51
52; SCRIPTS
53
54(script static unit player0
55    (player_get 0)
56)
57
58(script static unit player1
59    (player_get 1)
60)
61
62(script static unit player2
63    (player_get 2)
64)
65
66(script static unit player3
67    (player_get 3)
68)
69
70(script static short player_count
71    (list_count (players))
72)
73
74(script static void print_difficulty
75    (cond
76        ((= (game_difficulty_get_real) easy)
77            (print "easy")
78        )
79        ((= (game_difficulty_get_real) normal)
80            (print "normal")
81        )
82        ((= (game_difficulty_get_real) heroic)
83            (print "heroic")
84        )
85        ((= (game_difficulty_get_real) legendary)
86            (print "legendary")
87        )
88    )
89)
90
91(script static boolean difficulty_legendary
92    (= (game_difficulty_get_real) legendary)
93)
94
95(script static boolean difficulty_heroic
```


Halo "Scene" Shrinks

- ◉ Kits are expensive
- ◉ Hacks are complicated
- ◉ A lot is gated/\$\$
- ◉ H2 - 125k posts
- ◉ H3 - 24k posts
- ◉ Reach - 6k posts



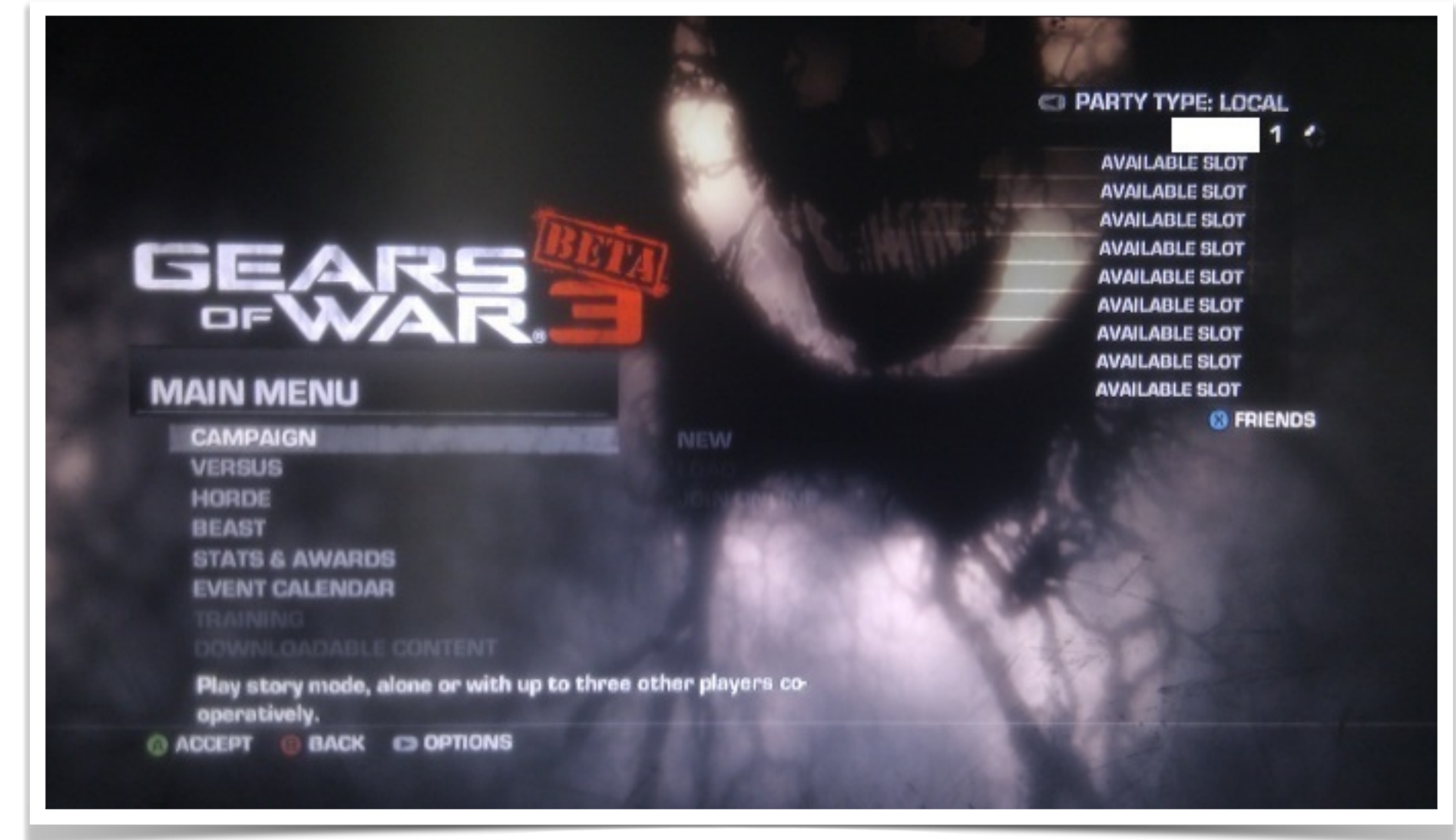
Time to move on...

- Bungie leaves Halo behind
- Newer consoles patching vulns
- HaloMods Drama
- Sad tale for a few
- Toxic community at times

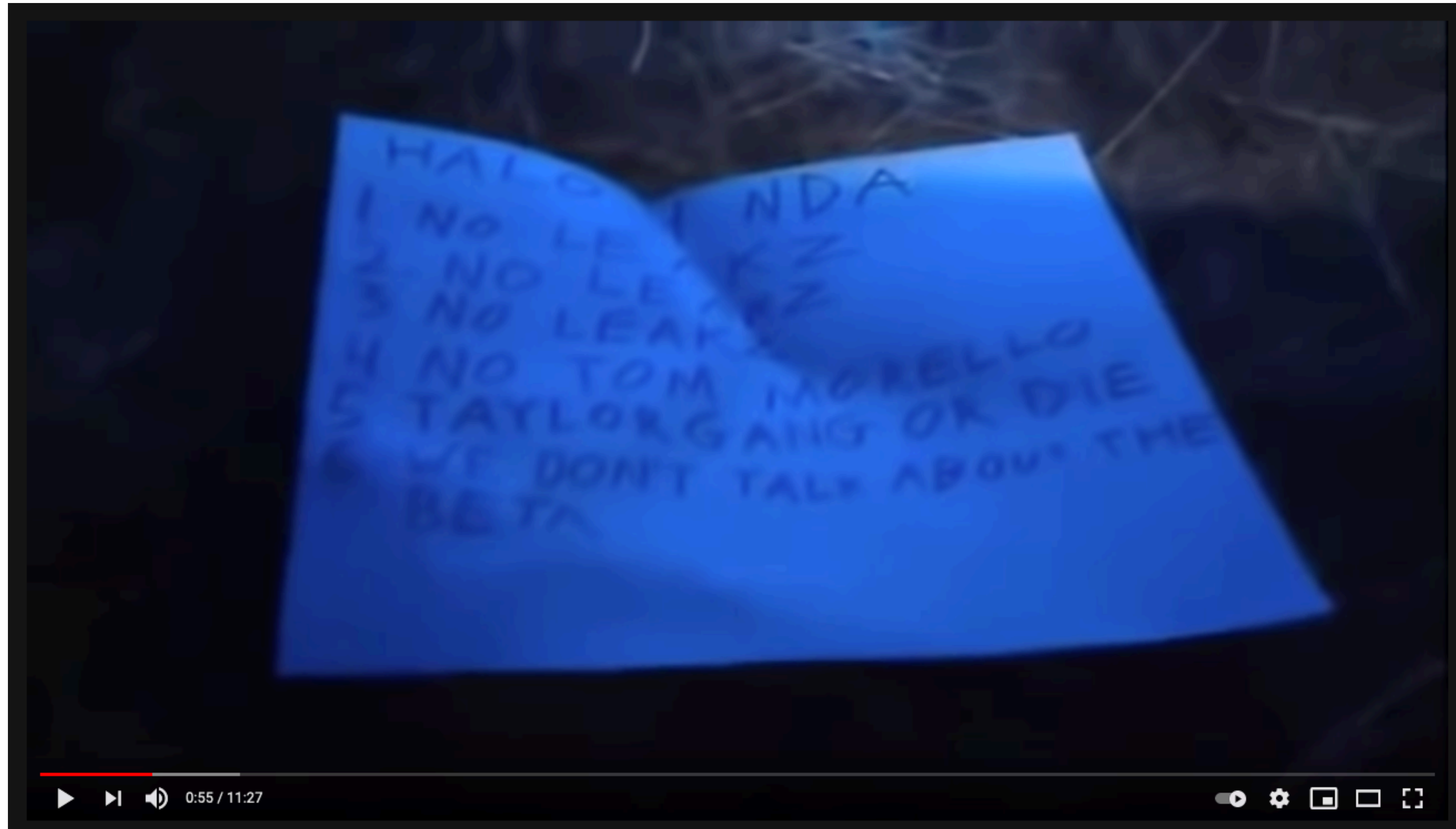


X360 Dark Market

- Keyvault Service
- Shadow Booting
- COD Infection Lobbies
- Piracy - PartnerNet (GOW3)
- The Barn Video



X360 Meme Market



NEW! Halo 4 Leaked Multiplayer Gameplay

X360 Security Recap

- eFuses (IBM)
- Console Certificate (RSA)
- 8498 Update - boot loader upgrade!
- XGD3 Disc Security
- STFS File Security (PIRS, LIVE, CON)

Hope! Halo MCC

- All Halos back!
- On PC!
- Modding reborn!
- Ehh Nope.
- **1185 days to fix**

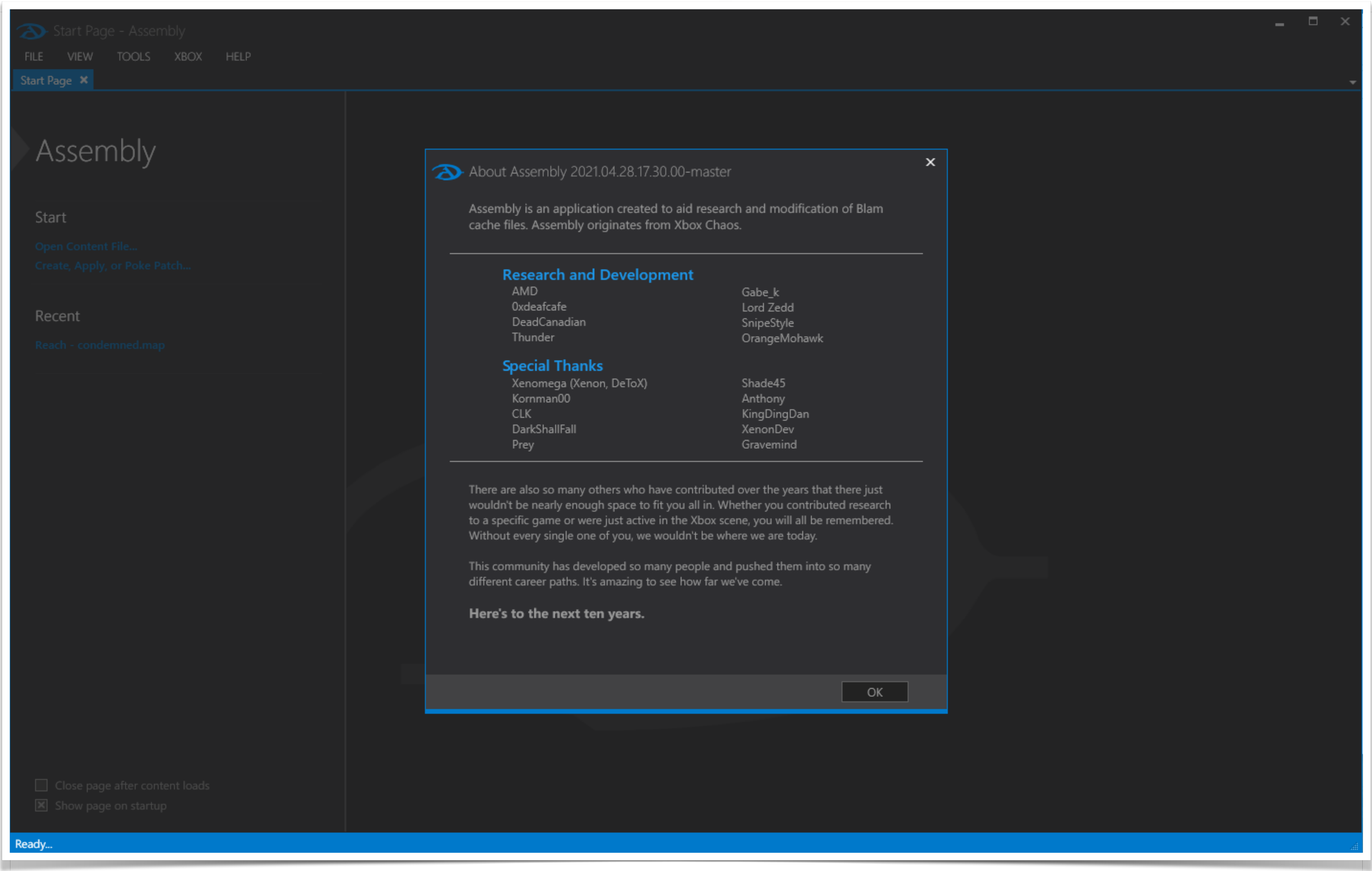
CONSOLES

A Status Update From Bonnie Ross on Halo: The Master Chief Collection

by Bonnie Ross Head of 343 Industries • Nov 25, 2014 @ 1:47am

On Nov 11th we released *Halo: The Master Chief Collection*. The goal being to create a tribute to Halo fans around the world, and to celebrate the Master Chief's debut on Xbox One. With the initial release of *Halo: The Master Chief Collection*, however, we have not delivered the experience you deserve. I personally apologize for this on behalf of us all at 343 Industries. Our team is committed to working around the clock until these issues are resolved.

Assembly - Multi-Generation Blam Engine Tool



At least it wasn't the PS3

- Hard-coded random number
- Root keys broken
- Everyone (geohot & fail0verflow) sued
- PSN offline for weeks

erk: 120 120 120 120
riv: 120 120 120 120
pub: 120 120 120 120
R: 8 120 120 120 120
n: E 120 120 120 120
K: E 120 120 120 120
Da: 120 120 120 120

~geohot

props to fail0verflow for the asymmetric half
no donate link, just use this info wisely
i do not condone piracy

Credits

- ◉ **Free60 / Xbox Linux** - Research
- ◉ **HaloMods** - Years of Halo
- ◉ **RemnantMods** - Post HaloMods
- ◉ **XboxChaos** - Assembly
- ◉ **JoeyBe11** - Hacking Me
- ◉ **Tural** - Banning Me

thanks

@iBotPeaches

connortumbleson.com