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)

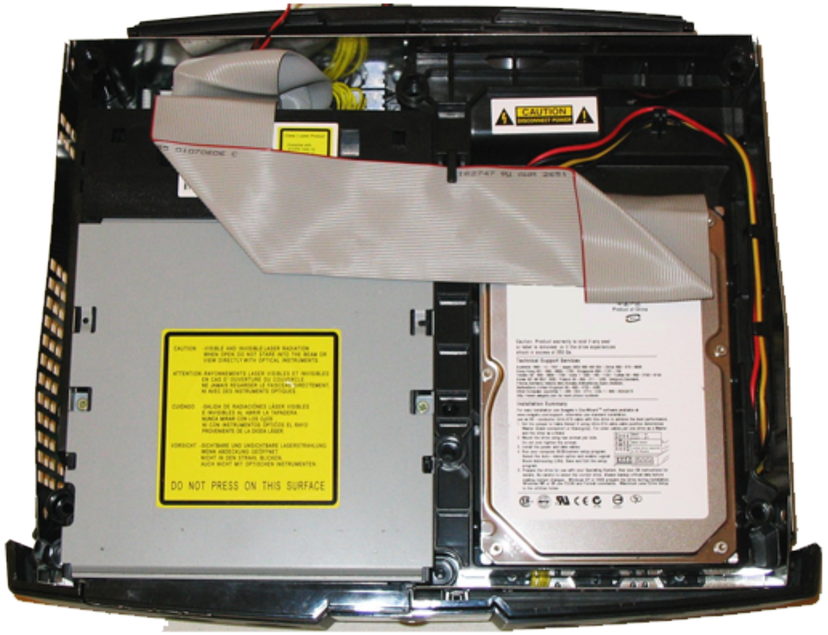
Who

- iBotPeaches
- Connor Tumbleson (.com)
- Started in Halo
- Moved to Android
- Now blog weekly



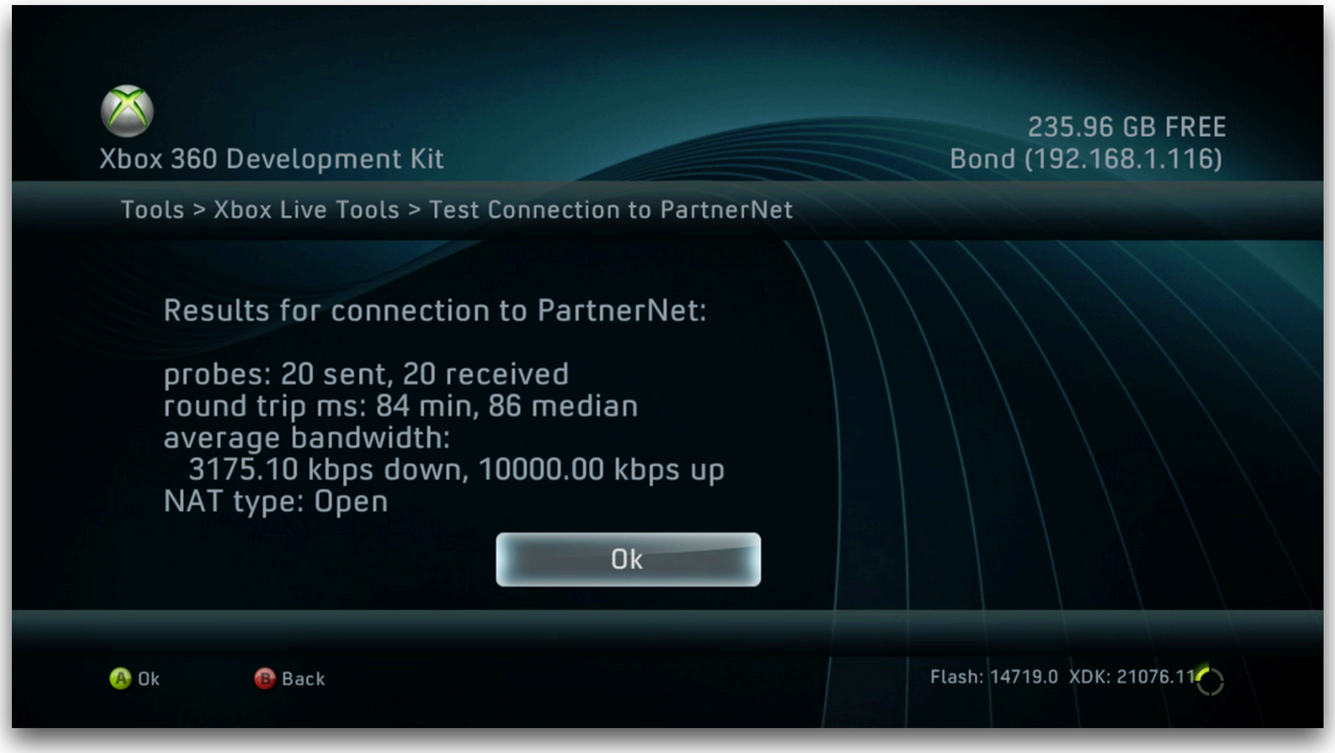
Refresh - Xbox

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



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 “special” 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
- Profit



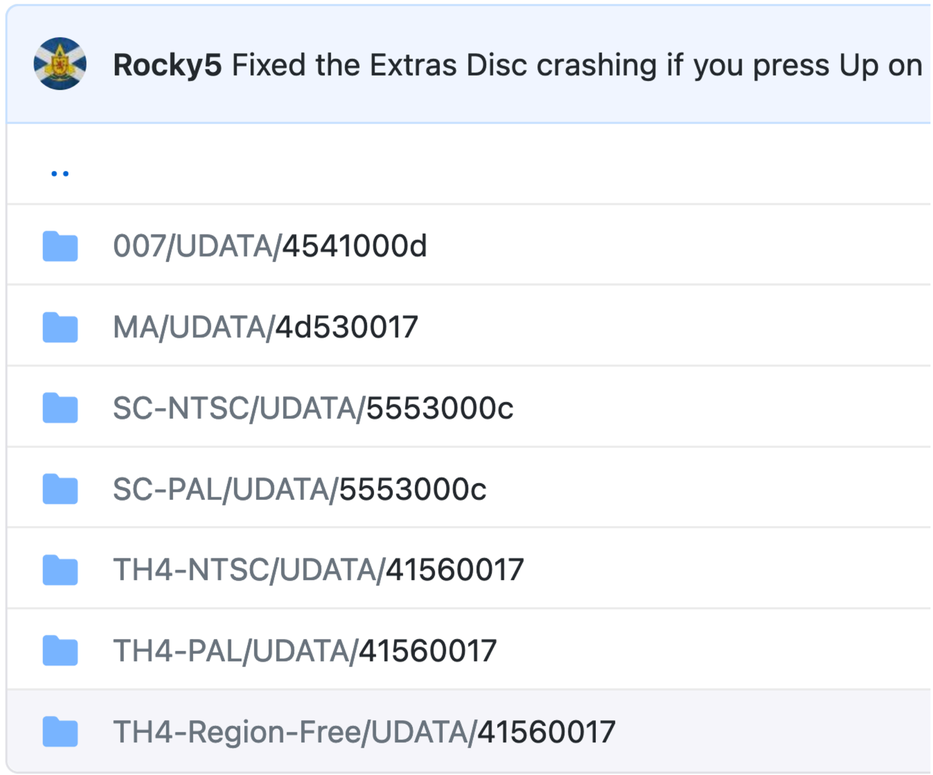
Game Saves - Difficulty

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



The SoftMod Saves

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

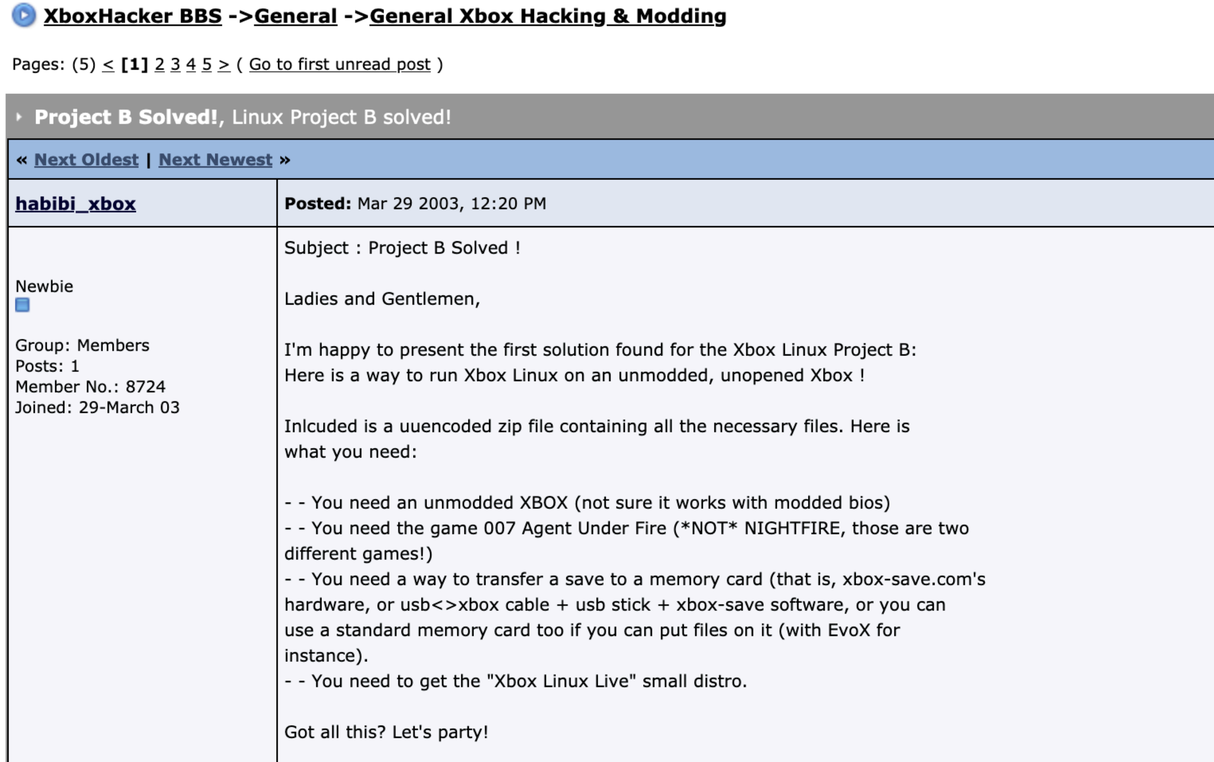


github.com/Rocky5/Xbox-Softmodding-Tool

The Bounty & 007

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

xboxhacker.net (dead)



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 Overview - 007 Hack



- Small little dat file
- An image is in it?

```
→  Downloads binwalk xbsavegame.dat

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
4224          0x1080          JPEG image data, JFIF standard 1.01

→  Downloads
```

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

xbox-linux.sourceforge.net/docs/007analysis.html

The Limbo State

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



SlaYers_EvoX_Auto-Installer_v2.7FINAL.pdf

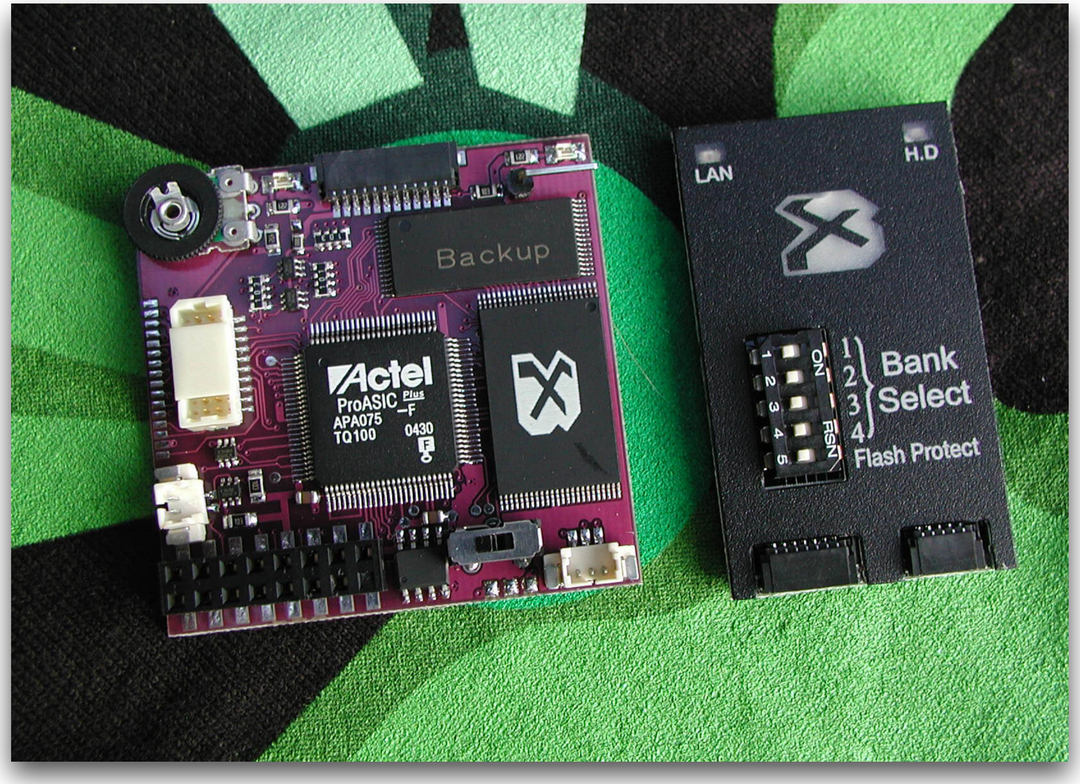
UnleashX

- Modded dashboard
- Launch Games
- Launch Apps
- Settings



Hardmod?

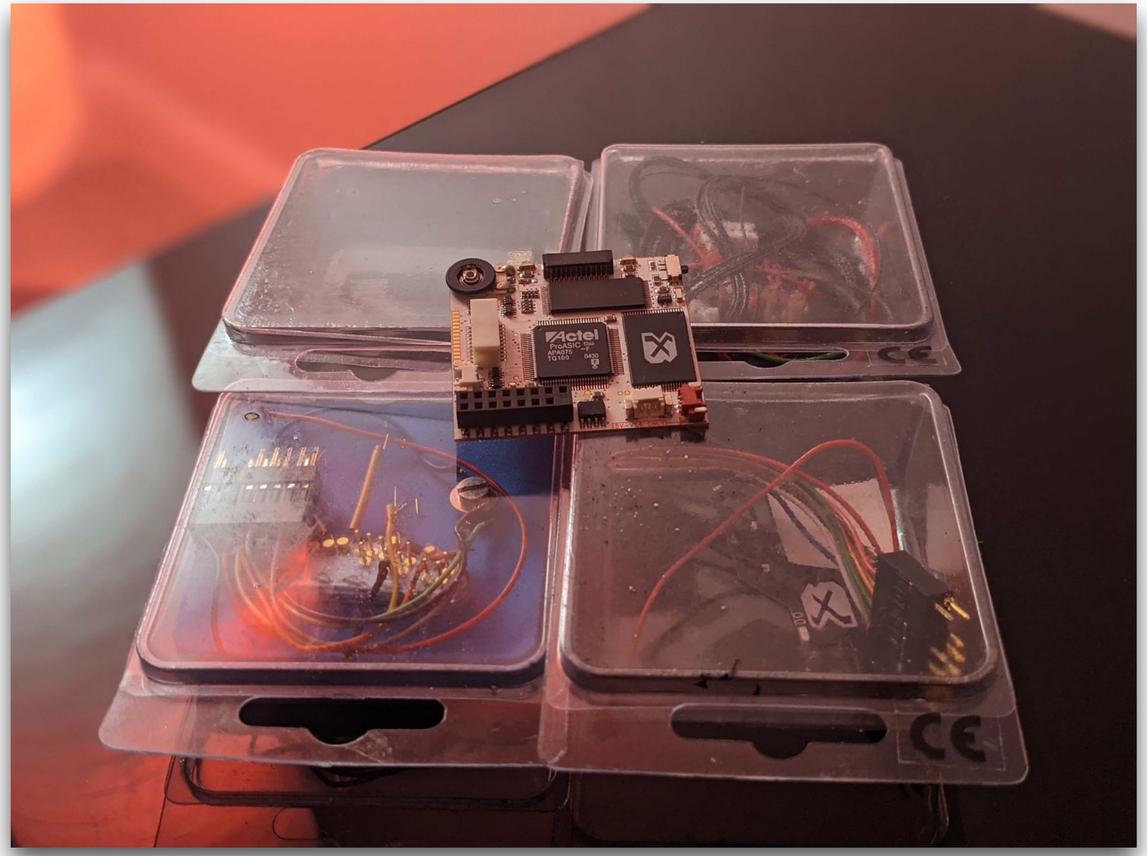
- Modify an xbox beyond intention WITH some form of hardware.
- Modchip common.



Xecuter X3

Hardmod Features

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



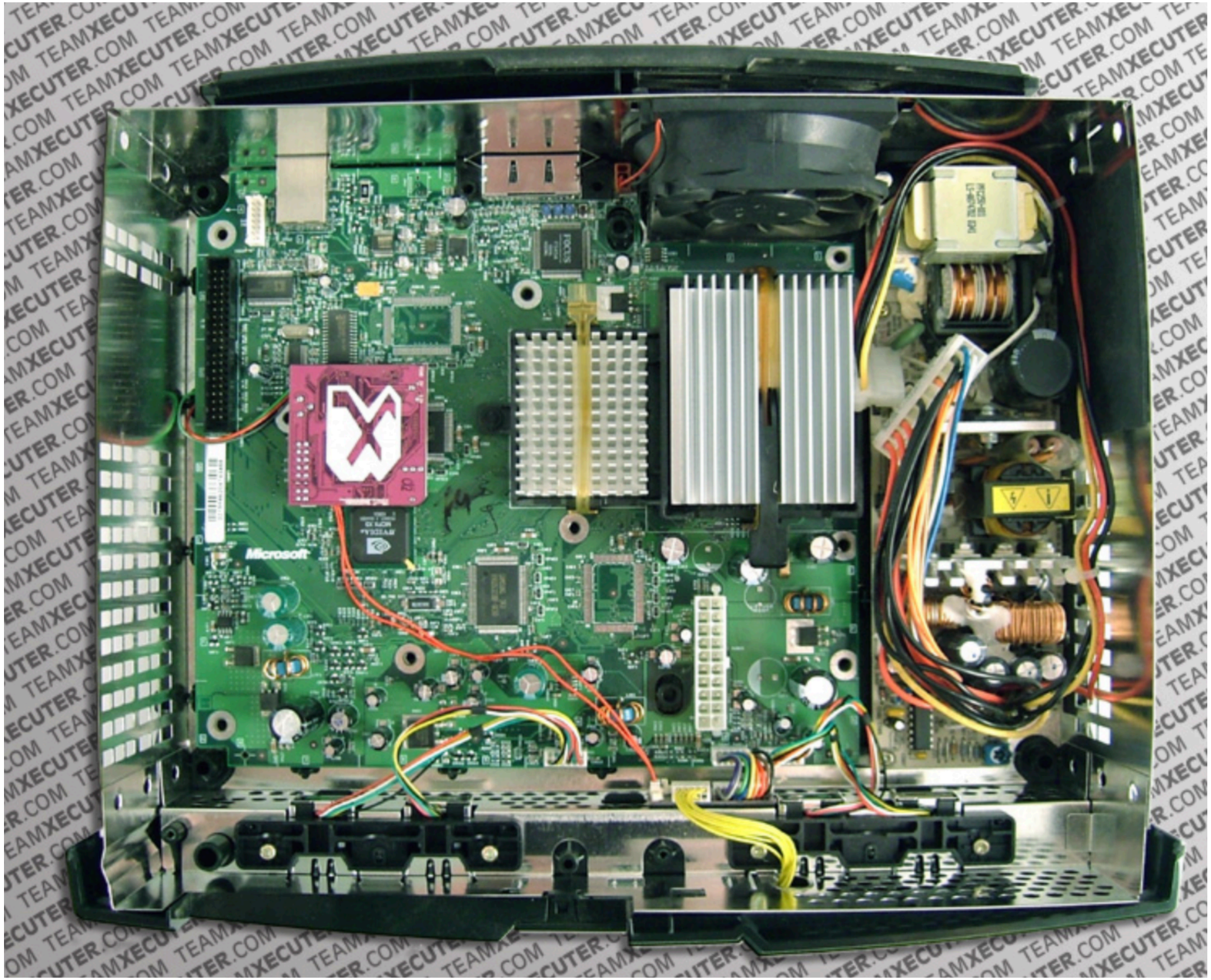
My Modded Xbox

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



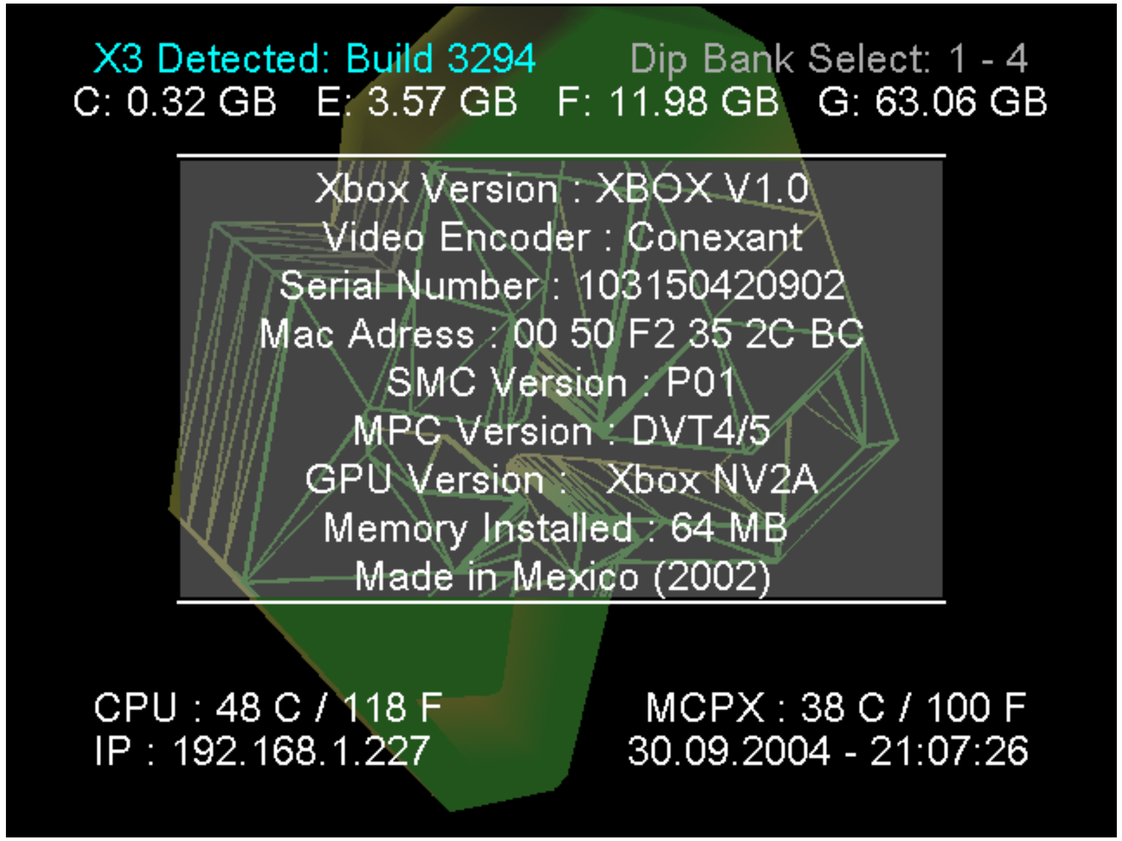
Soldering?

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



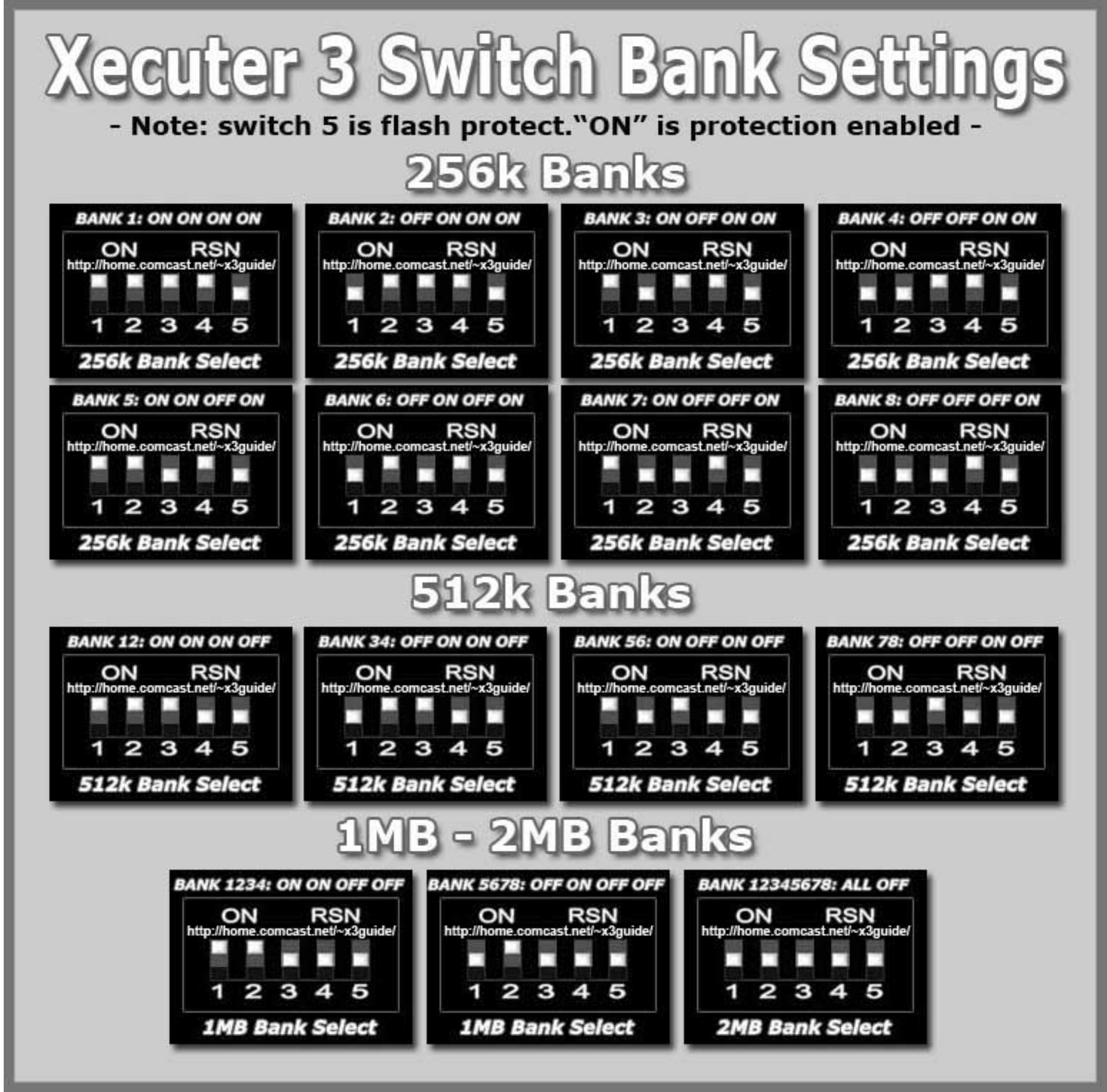
X3 Config Live - Xecuter

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



Bank Settings

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



Debug BIOS

- Expands features to pair with XDK





XBMC

- You know it as “KODI” now.



Bert n Ernie

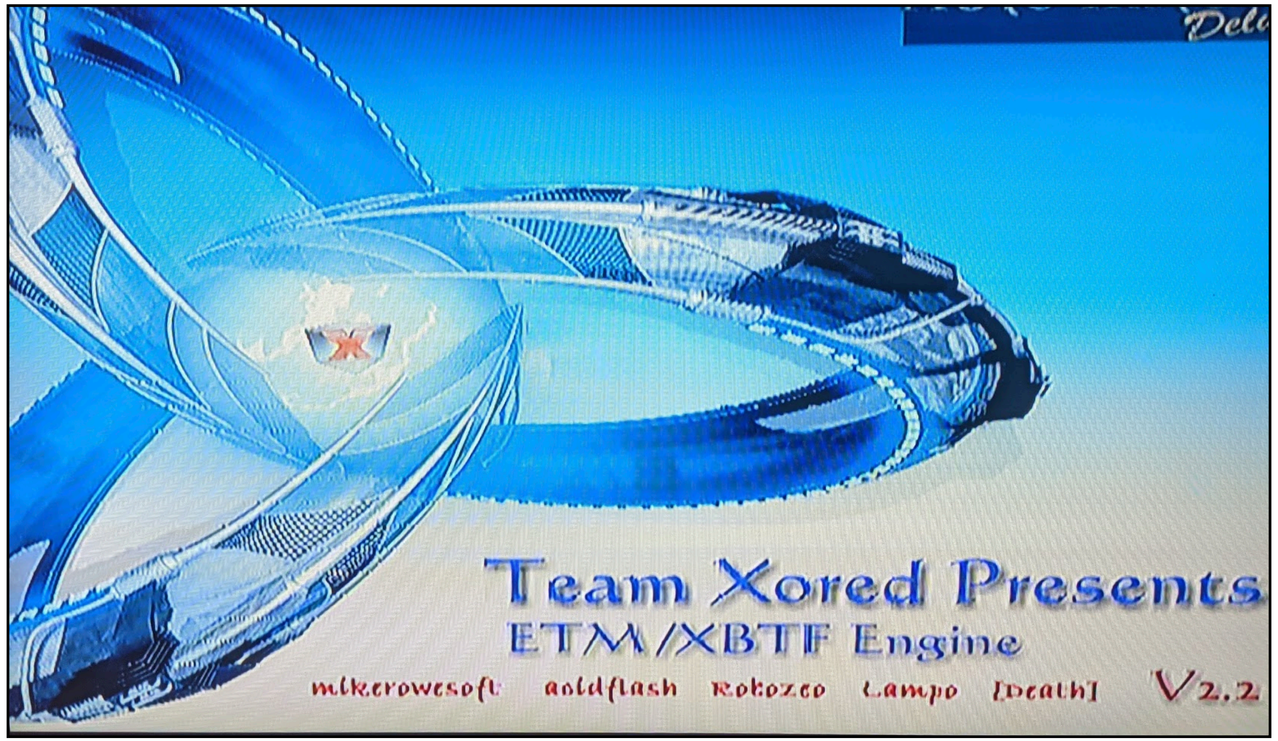
- Mysterious release
- Not obfuscated
- Two font files
  - Buffer Overflow
  - Thread Collision

```
;;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
```

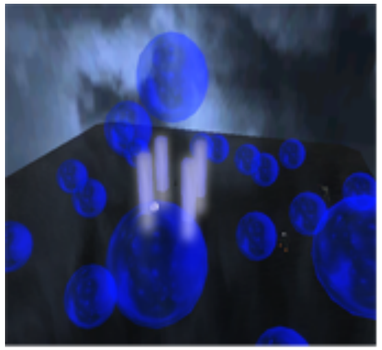
phoenix.maxconsole.com (dead)

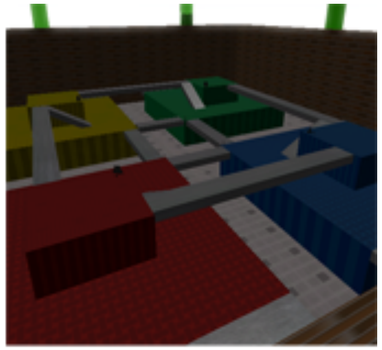
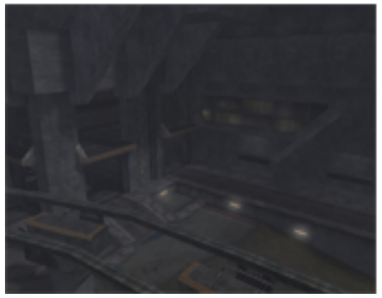
Playing modded Halo 2

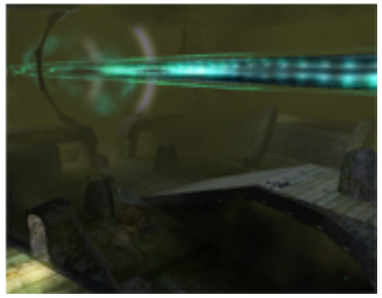
- Game Trainers - Yelo (xbox7887)
- Launching them - Xored



Halo 2 Modding

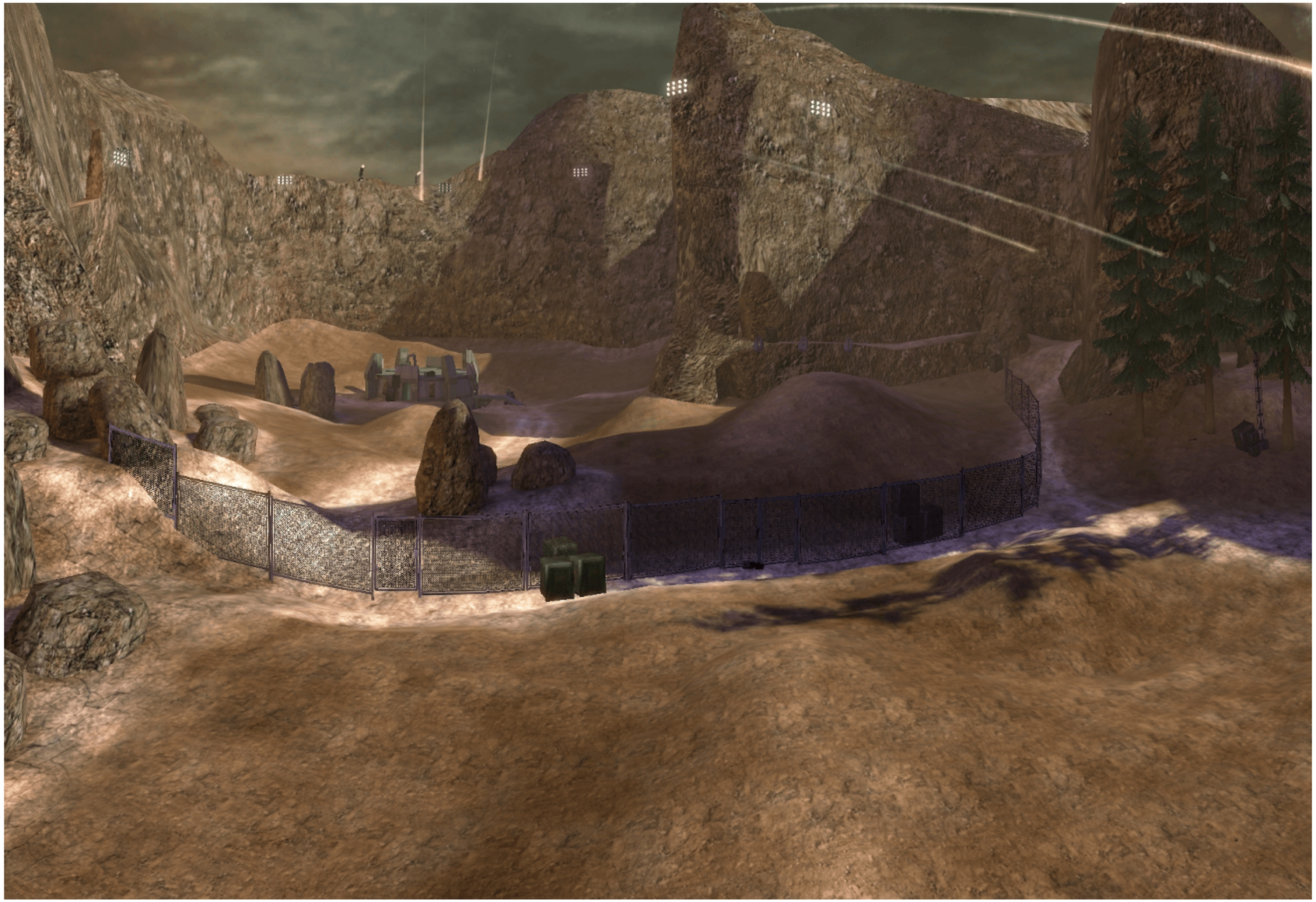




- Racetracks
- Campaign ports
- Creative mods
- New models (weapons/vehicles)
- Alternative sandbox

Halo 2 - Havok



Darkshallfall

Halo 2 Mappack - Phantom







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)



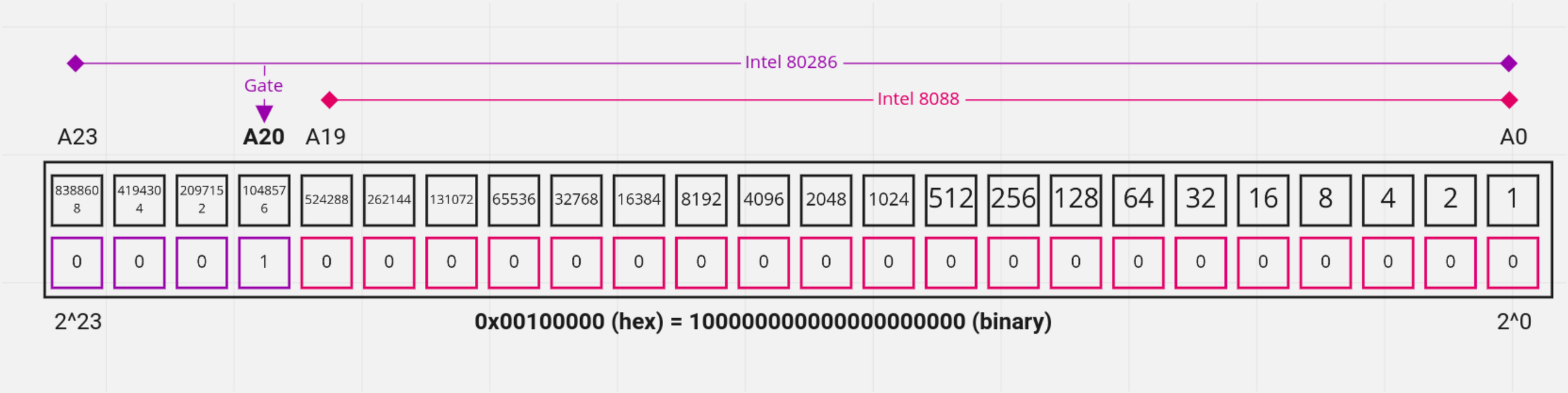
halomods.info (archived)

Why was the Xbox so hackable?

- Existing parts - quick build out (TEA)
- Bert n Ernie. Game Over.
- Rushed updates, Trashed chips (1.0)
- RC4 weak, RC5 was not ready
- Flash memory. LPC ports.
- A20 - early era IBM wraparound

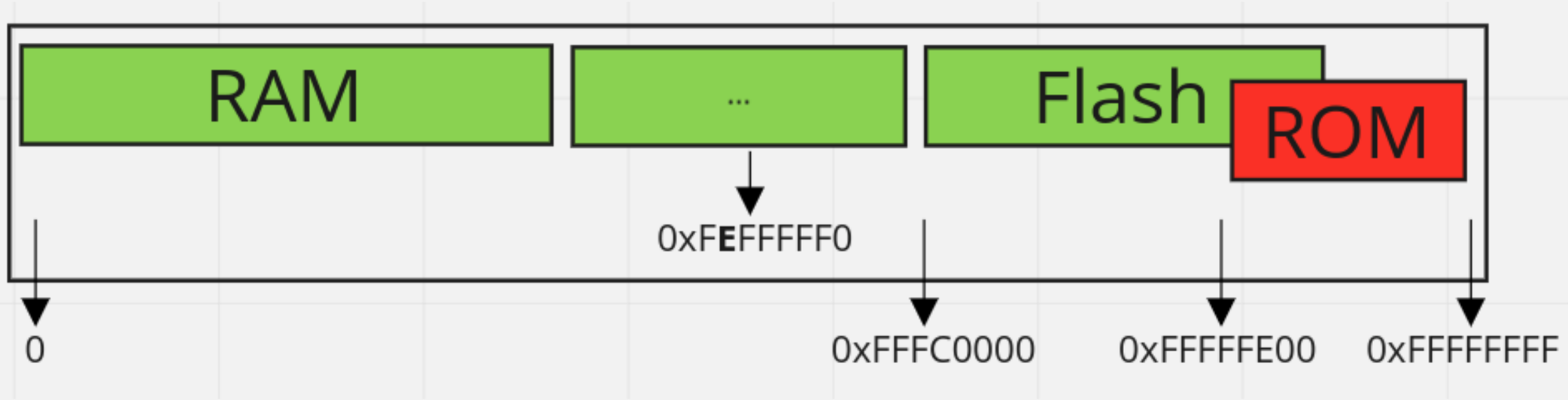
A20 - The Nerd Details

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



A20 - The Nerd Details - Part 2

- *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)



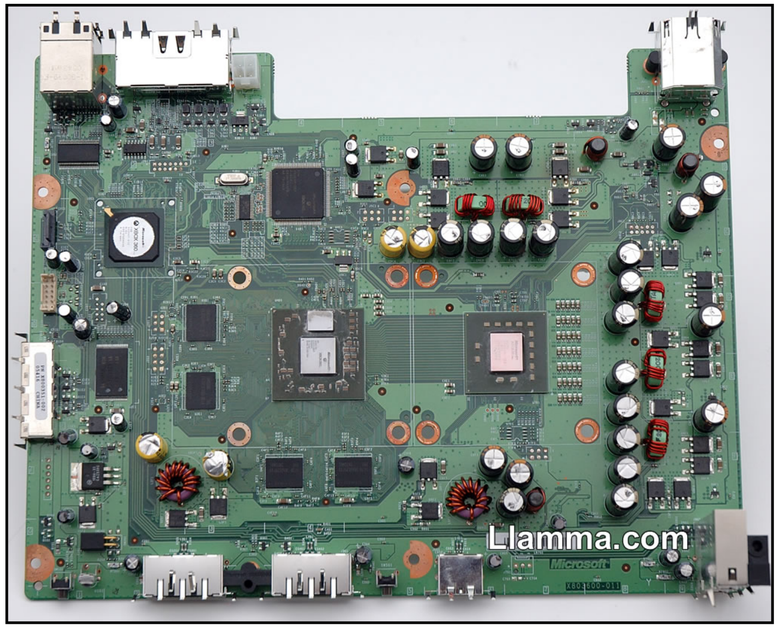
- Backward Compatibility
- Emulation
- XeLL (legal loader)

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)

Early Mods - Xbox 360

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



assemblergames.com (dead)

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



$$$ to Enter, $$$ to Make

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

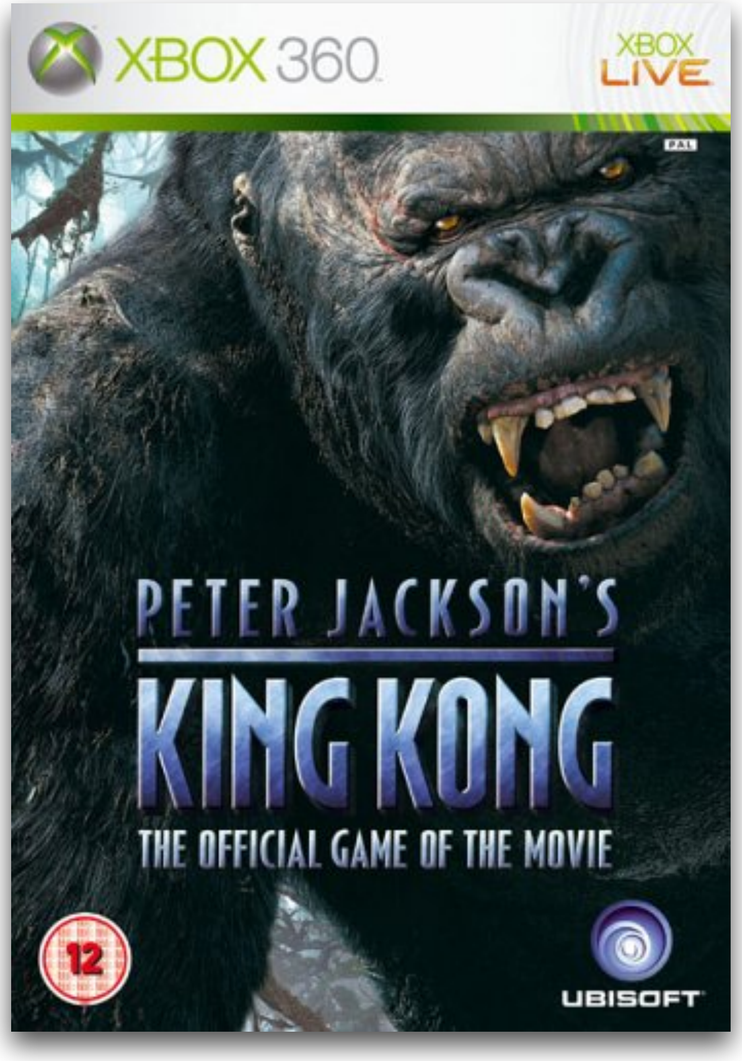


XNA Test Kit

assemblergames.com (dead)

The First Hack

- Needed an old kernel
- Hotswap
- Modify KingKong
- Serial Cable —> NAND



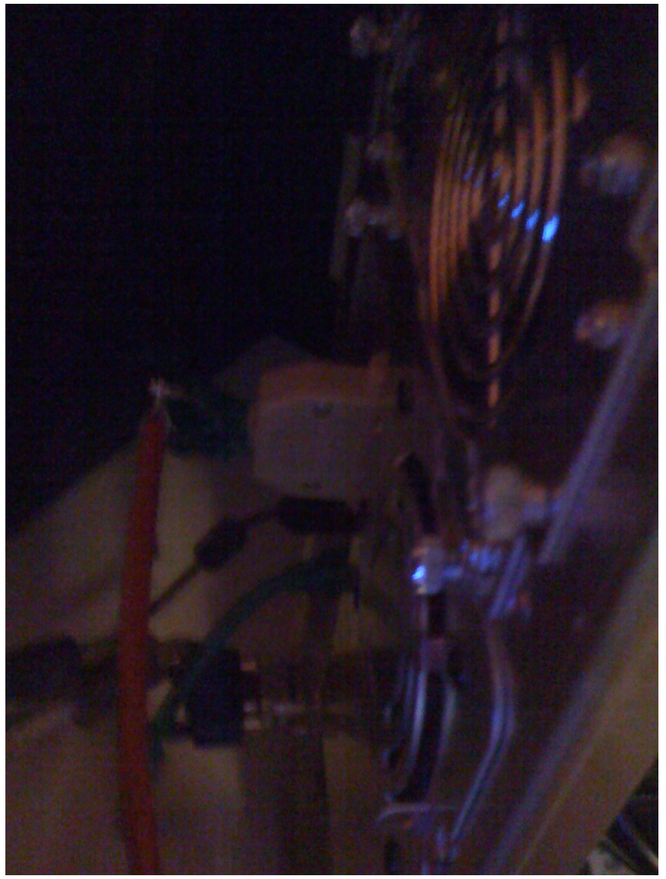
The Second Hack - SMC / JTAG

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

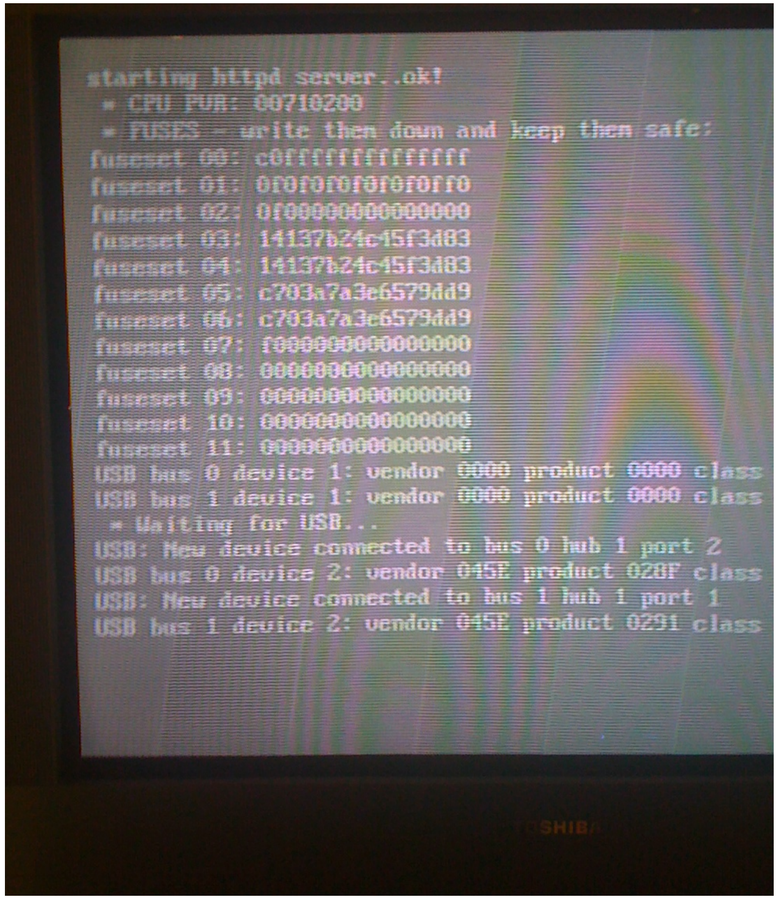
The Second Hack - SMC / JTAG



Attaching points



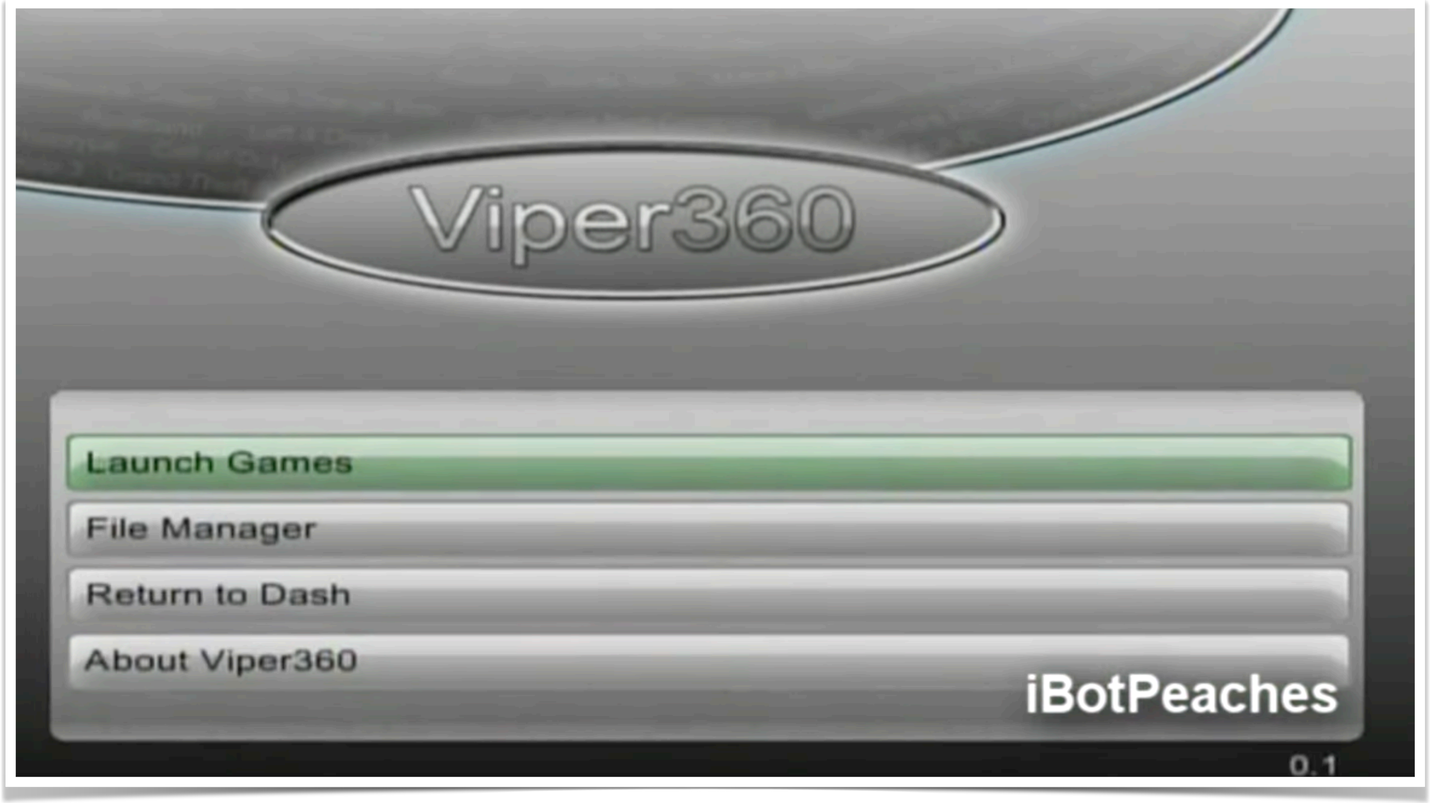
NAND Cable Built



Dumping your NAND

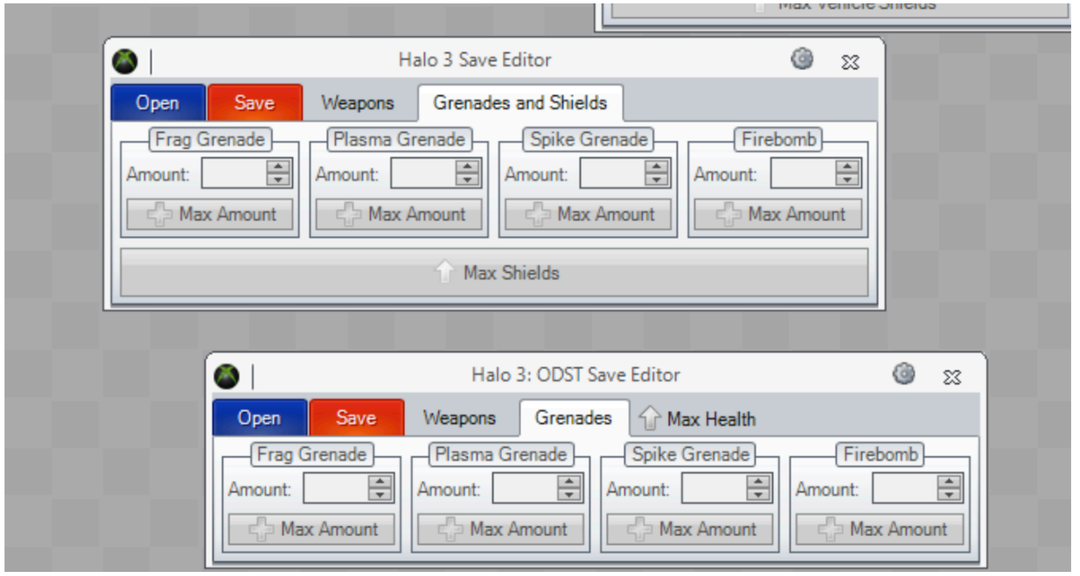
Early 360 Software

- 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

- **R**eset **G**litch **H**ack - Any “fat” model.
- Dump your NAND
- Build exploit
- Slow CPU, Prevent Reset, Remove RRoD, Glitch CB_A, Boot custom CB_B

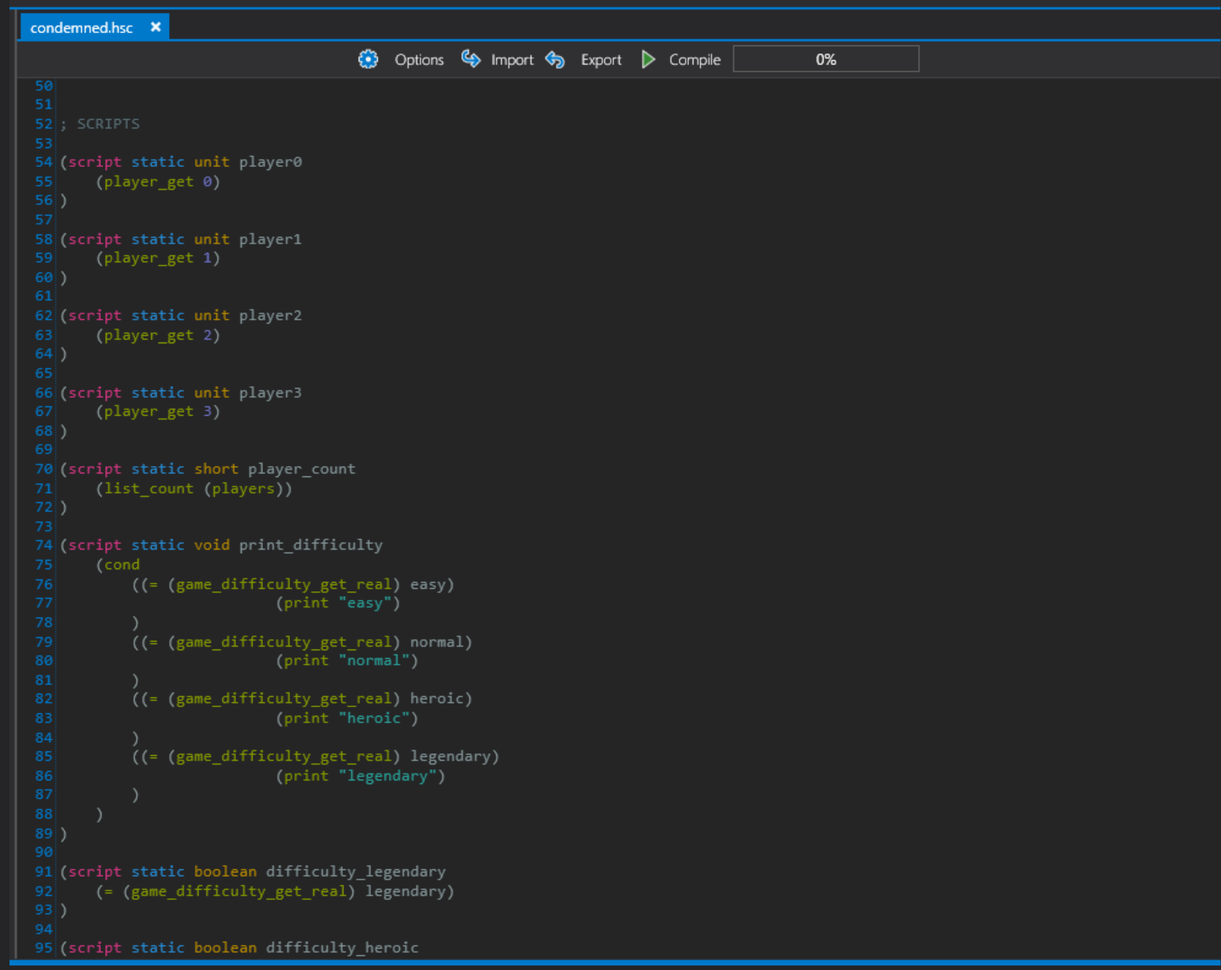
Modding Halo - 360

- Basic
- Swaps
- Assembly



Gametypes & Map Scripts

- Megalo
- Sharing
- Creative
- Fileshares



Halo “Scene” Shrinks

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

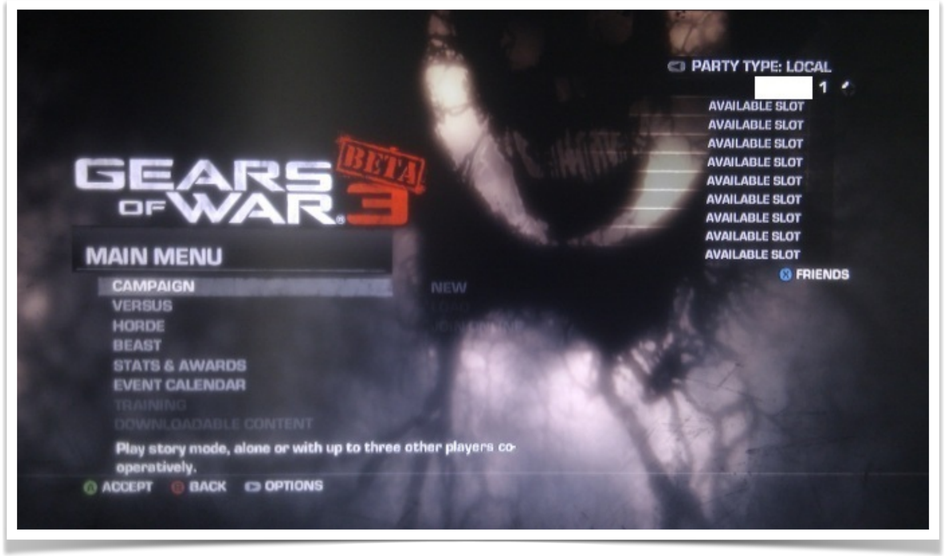


Time to move on…

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

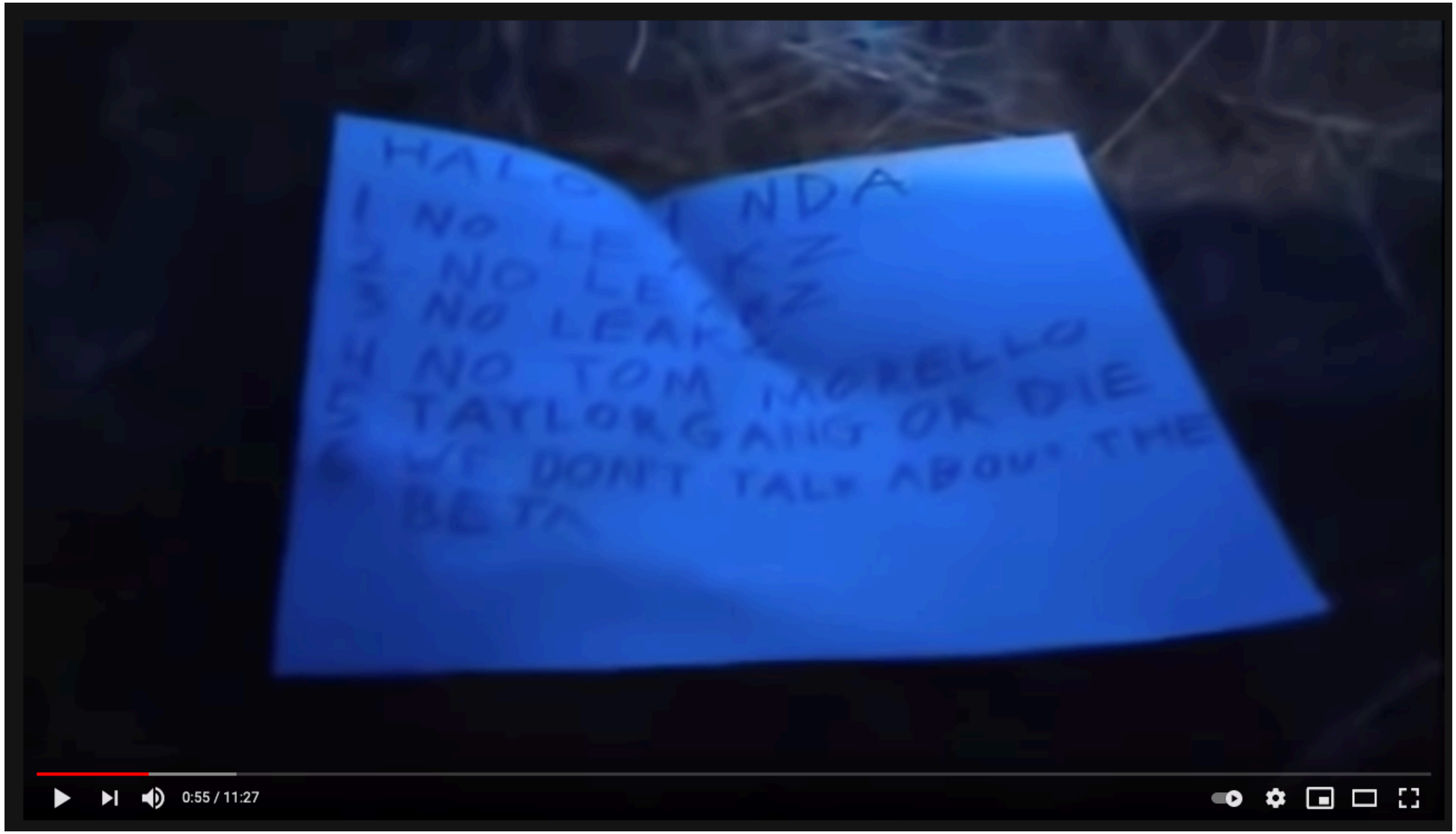


X360 Dark Market



- 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**



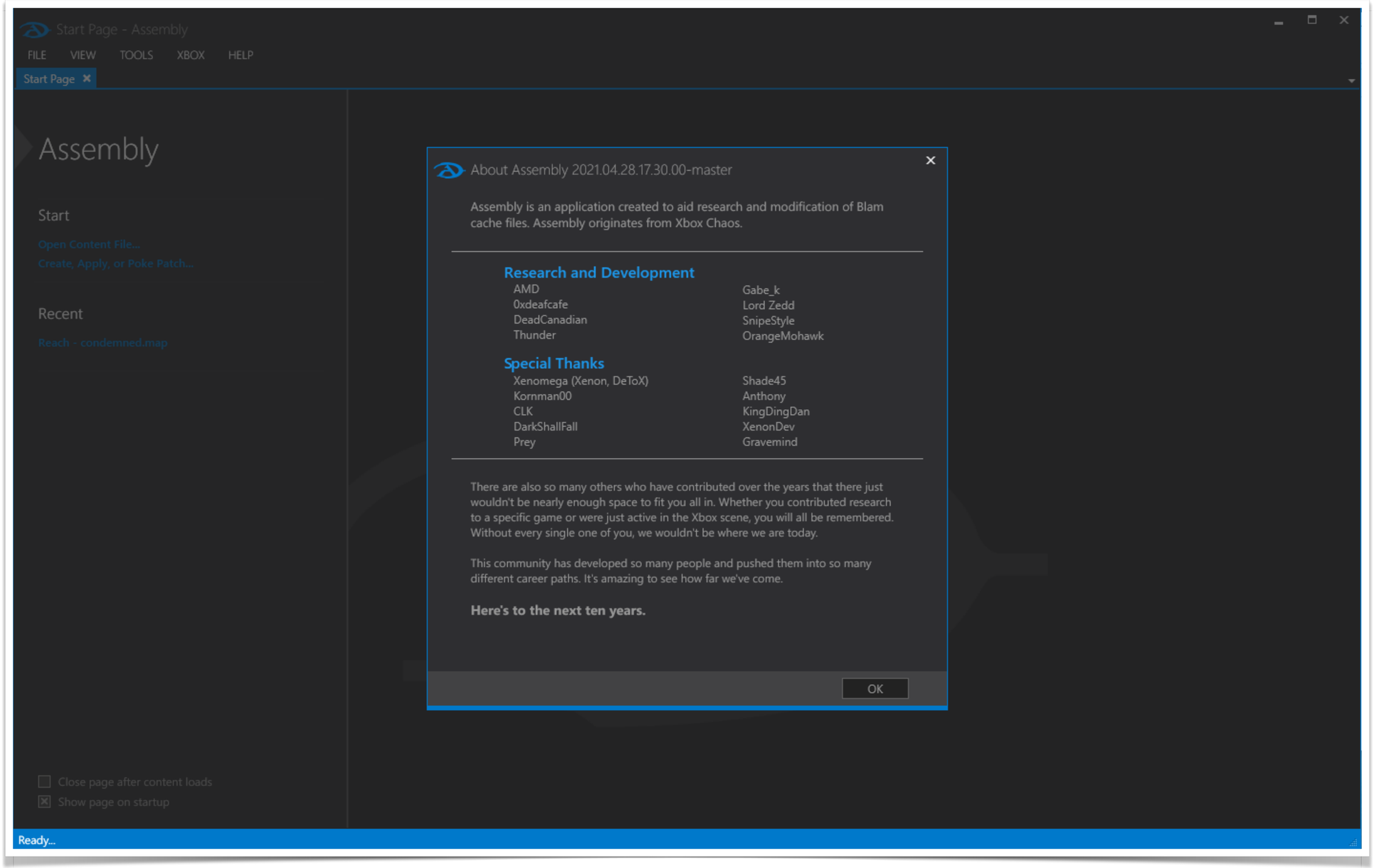
CONSOLES

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.

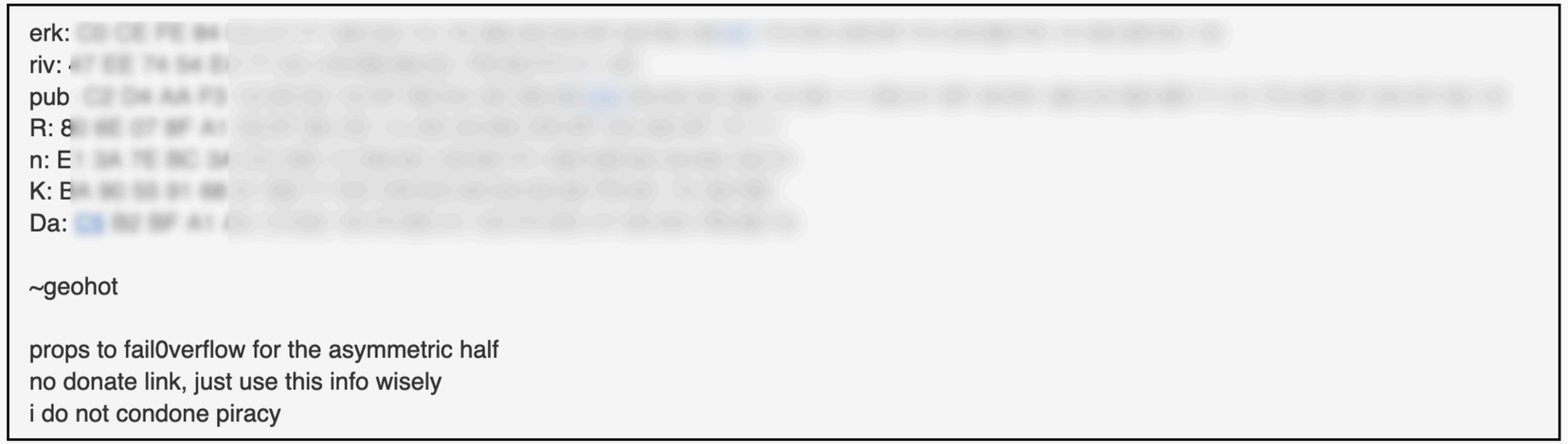
Assembly - Multi-Generation Blam Engine Tool



xboxchaos.com

At least it wasn’t the PS3

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



geohot.com (changed)

Credits

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

thanks

@iBotPeaches
connortumbleson.com