Xbox to 360 Security

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

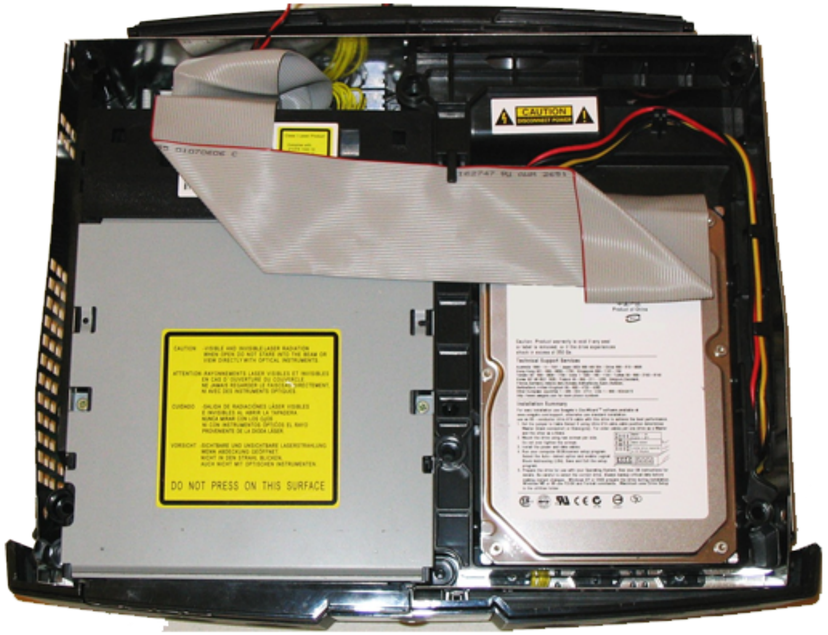
Xbox 360 E - (June 2013)

Who

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

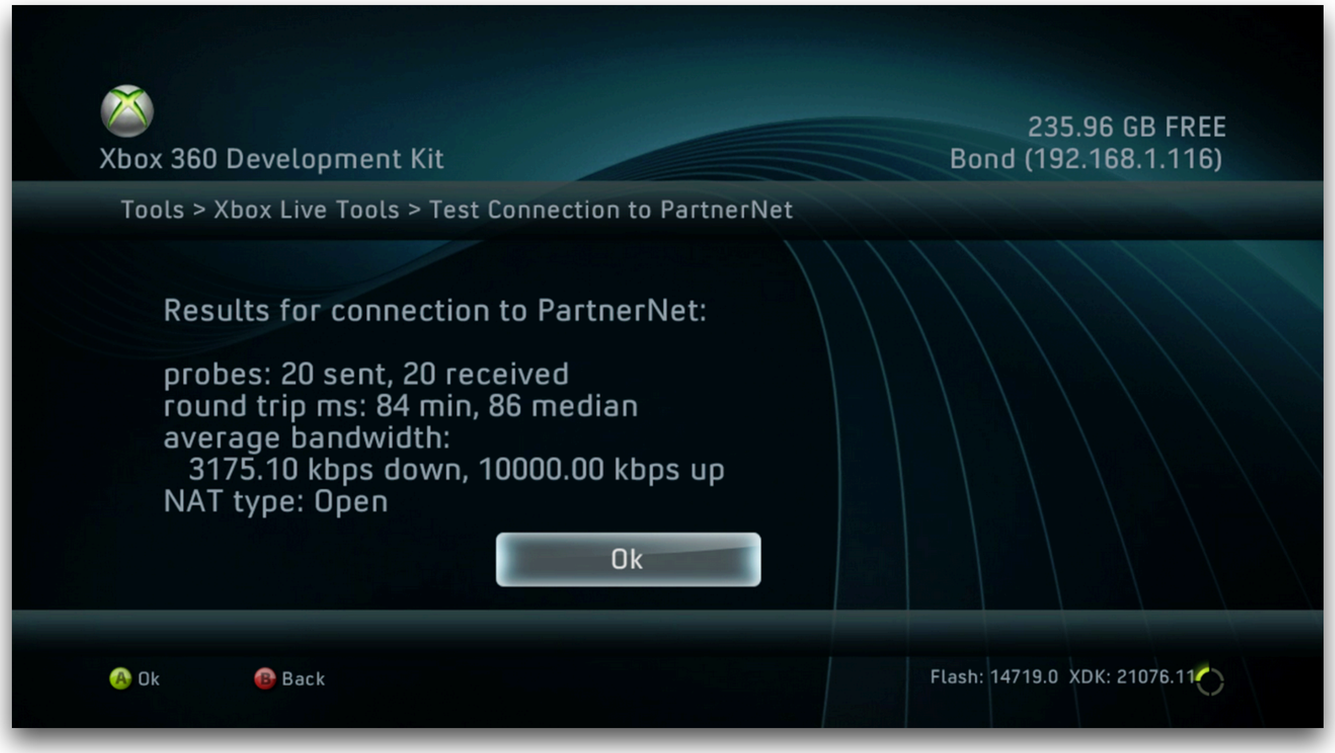
Refresh - Xbox

- Intel Pentium lll 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 did 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

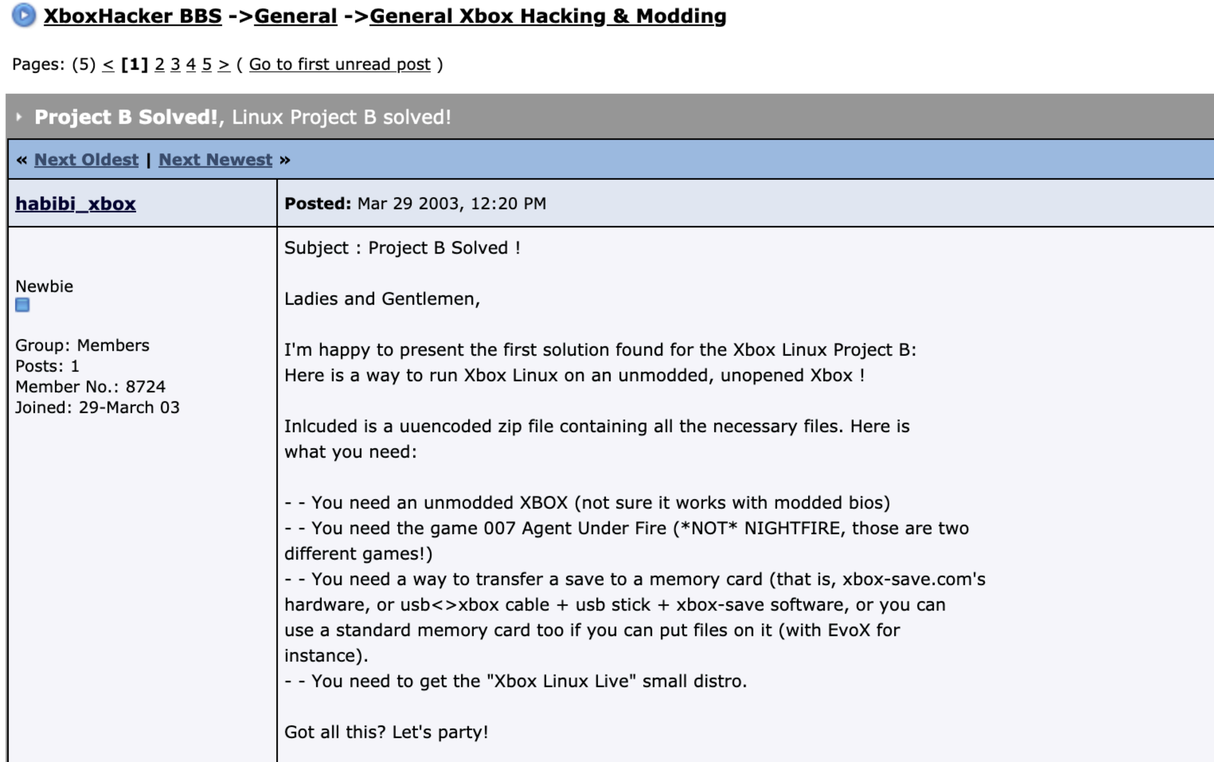
Game Saves - Difficulty

- 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.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 Bounty & 007

```
begin 644 007linux.zip
M4$L#!!0````(`#VR>2Y0Y7!)AP```/
L````*````9V%M96ED+FEN:8MV3\Q-
MC>7E\G2Q-3$U,30P,$CAY0K)
+,E)M75,3\TK40C-2TDM4G#++$KEY7))
+4ZV
M]<M72`'219D%)9GY>4#!Q))46UZNX,2RU!
2G2@3+-3<Q,P?(#4LMLC7@Y0I*
M30<J!['%R!PM$@9?
$&2`#B"F017BX_H.MLG?S]7*P4'$/=J.L"`%!
+`P0*
M`````#'!7HN`````````````````#P```%5$051!
+S0U-#$P,#!D+U!+`P0*
M`````#!`WHN`````````````````^````%5$051!
+S0U-#$P,#!D+S`P,#`P
M,#`P,#`P,"]02P,$%`````@`!!]X+ER'5B:/
`0``@`,``"D```!51$%402\T
M-30Q,#`P9"\P,#`P,#`P,#`P,#`O9&5F875L="Y
P871C:(MP<O4($'9MGW/U
M9QI[\V
(LKVW>LSF2MV[TE3TUPW[6Y[_[BK]../
G5.OW=)*<;6HODNV?=>:HT
MC7O;K+E7-/.>&;`5EK\]=W9YL-
M_P92-3SQ^*W:6L.;'1G-,F_!B>:_%M$><
M"S=??>^7^>/2U?@D6Y7]H9L?
[#C)=SIER]6I';$2RM9.LV:XO#@O**8SU>^2
M1]ZIE9JU2][4W*L_-
T^QB[]2_OHD[B_K[5KF6\;/7VB\]_COO/,+/
O9P<?RL
M.QG:L+7S:'N7O,AQ&>'[/7EVSG?
F<L67]RPO_CRI=GKW5L9?7.G)NVJD_.S]
MF^_W2'&L^VJ8FG_I$JM]4I^ISO[?.6Y/
C"RFS$A;W!3Q=,)SXW`[!@9&!AUV
M!@:&!@&&"D8&,*A@9&0`,3V8(0*KW?
ZN8&B`2A(!M@7D1&,3[P&:MX"9@>$"
MDE$^#)D,>0RE#!78-`P`8&5@.``,CH;_0$!
8]2@``5#R81``1:H`&(&(%FC:
M:0#234#<EVB\Y&O1\@_H7W[%:5_?'RO>(
<#`%!+`P0*`````"[@,$P"HRX
MTR(```B````*````%5$051!+S0U-#$P,#!
D+S`P,#`P,#`P,#`P,"]3879E
M365T82YX8GC__DX`80!M`&4`/0!'"$\`3@!
$`#H`(`!!`%4`1@`-``H`4$L#
M!!0````(`#9U>"ZYU!;"1P@``&D6```J````541!
5$$O-#4T,3`P,&0O,#`P
M,#`P,#`P,#`P+WAB<V%V96=A;64N9&%T[9
=[5!-G&L9G$@+!@B'A(E%*"8(B
MBIL@"`<0C0H(2$G"I2@7%1**@#2"*$&1(
&65BPBF@!71*C?)(%>%X%$344O4
M=5N+(!>AEG@!1I&+:%8NLU_PM-
KNL>=X]L_=4Y[DF2_SO>^\Y_W-EYDYL]T`
M@H@=/U]07#1:%)=;-
#WJ/)HRE/',PY&[?]JQ@3QG*Z'02$_8^*^24O
9I=?
M#)<7Z[H]ED=GR*Q,AELQUK6GV%
(])K94%Y@"3`;6`28!SP4Q;3!J`7\"/^=8
M$Y@(YC7`J`Y,`%8#Q@/
C@&$0@\"(0;.:U:QF]7\BEQW)WN^#^N&9<
=7_\
M\!&SFM5?1_]Y?6Q5SEX?
LYK57T/]JDUPRG."-@213&3F&#:-
D4QED]]A&"QT
M.A!/&/@>AB`G-_#C`<B45F_""6L&Q#4-
XIH2L;1>M0>)I?NGP%@JE@I5(RJ6
M1D[CA)*:EZ@)
(B')T5>(I"X1=4<DR_($YH@D_36Z")
%4HE9UB.1\'QJ/2!J4
M:,=,#HB&H'A#1,*XJ9HYCT-
EB*0&4E6@RU%[1!J*PPLE=2M0="9=5?
@:>A5L
M<]`%B.0"C&HB8K'TB"J)
(4,5B%A:,W.`+WH7D1+P^)GF:&"4L-"=@XC
T"9L@
MK,D1BP<:X8]CJR/-L-U2M:!Z#0-4;>A;-
G,5VS+`UK`0)?[*QD'M5&A=;]$Z
M$4FM&%T*TD?
1UM^A@5(D1-4[;@:M&:3TH38S:(._H?
6=POI^18/DJ"\B$:,H
M]@?`G!ST]'N`[1^Y>*`GHJJNR!
*TTX^>_`WSSP%5:_<V<!--POST BOX-->.`?
==![ZH)N`
MR_]D[0#@']<.H)6_0XM0_8./I[61((C5/_8-
#D*GN0Y!?NN9OLP@&UL;!IU.
MYP;1WU,0EQ>^+3YZU_*$4!
Z$M8)W>Q:HP`!
><4UVS0J"P)0UQ,=8K)GG(1]3
M/0];6UL_?!']%\(ZL(>0CH>KNRL$PS#D!
CX0-HW#G?.93DI(TS90$F[F!8][
M465?.Y4@LOM_LWS]YDVDB]-
HP].KV:DZGF/6MXJI?2\";]<-]A=-89CO"FL8
MDA\YH_G)'/=Z-U>KK+-KF?SD->WE?
I[+&@X-.XO9:$\;M1"XY2[X3NB
M%=*?,C@A?K[K6]:0NM&PJ<=)HI;
\P.:;*STUB9<R6[3QN.P+B:MM;6JD6M1Y
M!N+<Y[HTDY+B#O.EEHNL!.7G*@T7?
Y5[ZB0%OG6*/NG2YOBZ4SGB<-A)<
MO6?/W@>?JV/-(\-!
50]\J1I+2TE$<LO9Z'+X9<7Y*O#K0U98I$!
8\X%+2W
M[9[3ZI#XA-+IR;$#B-N&@1O7;X\?
(Q#79&>E<N;:]DDOG/=\I&/>G%]THNMT
MTW?55:6T97Z6%HM?;:CEF))U/
`*V**GS:9K02K:VD?6Z/
NVYYL9Z<PYO9KD>
M+&.N'7$)V/^M^_K$PHM^_I>W[>/P8B-
BJN7;(\D"?GA*4G2H#XL=$N07N)FP
M<!&.X1"7'!T5L\IUO>?GFD0-BC81?
\^:OKKK7YU6K?:K%$/.S78K'7YV,!YY
M*>\(9@9*)5=RSO1V]W9^D5=X_+*DL8']9
HN;"]/'FZV<G+X(]K<=JJ\[K>JW
M!!'?E!<GQN[F'TSZIBD_,QVE-LSI]AJ/
%SR]A=_1,T8JH3"@F@6:.A4ZQ^89
MX$5"K!M:!QF0R+KDN0:Z%%UP[N?
3[,QHQL:T]?05%G8L5U\?;U>OC0%AR=$!
M(0E;-GK%Y/,34@]FYV3[1YXH+
\PH2\[,3E<5@>=1J;1/:4PS,V9ZH%=@^D<+
MDT%D(N0$6>-A4PA'AO%D&+L.+8`@/
*SZOA-!70W&X35`T%H'PL%X'%Y=C4!X
M&P,!2(U,H*C3V+JF#.:VJ]8[4W+U%ZX]?
7<=)ZYV&!Q#556#WZ\X?!J,`&$
M:&0(!P03WH5@')E"P^NJZ3&8[&&L"]
("G>#(>#*T&JHZDV&!TTBW+2PL6AM@
MFJ=H3,\@^!
R^GB"Z7Q3:.AZ%4+@93[QD60N-
BDGLC>&U@;EQ6GS\DMSN!HUQ
M3:)ETLJQJHMIE?
P.;VJ]SB&.M4@@;Z%J5*=/<)XN^/[5[J)-
V\M[2J>R[-A9
MRS)/['(.>[%YR6?J#<\UU?=3#?=.M-
X*2W'18\%!CI41_WRF[\L5/23$<29]
MXE?=>31_5?4XG=MR<I_&[?P(?
*%Q9_'1(9O)BB>Y"BWZ[GQ[V^=G!
^Y_<3QH
M<F(BMN*^T8BWZ9'Z`_;-9XD0-'>=?
N=K15,CRA[XNZ"]Y4X;)>C3L]<+*!UQ
M+B*I8=B;VG\D]U@V7XD[M\FK/
+)*[C$4TVY]J?:'KDIE,L?AY/&Z*XY<1[.6
M$.GFFE0'BS-"!R]
+II9H`S^W(MQ9&%YFS\LN1GHC.=5[L'CKJ
]82UIZY'G
M+6I\EN)/,*P='7:J\%S]\
$;5N6WJNBDV'HS<J6OW_)/96L.?5?
GQEBB%9^H[
M@Z\FXQX$.K]TNLSLCW*)T"E0I$UFVAD
=BI7N2]8O2`DW'1TD#]=IM,@5O>=W
M>OR09!2J;]79)!M^G/'R%\?
%]>%'^6IUAXM_3+A78.,\'1%-]7;1\W.AG,_X
M21X++Q<D16RM+-
V@1CY`*EJ93RPSS+=-/E;J<.'$
[H:I2FU3(T7,LR.]EWJ]
M*?Z/OBUSJAC,ZMI?
6M(_<KG80#CTP)V0FCAZ1S#H%+S#B!
>M7YJC=-2R>&W3
MWN)1&T!Q:W0OV7ET]&S8A-
(_M:R#GJ+=E,6**O7SLNH=WS]XQ&/
W<=OF.4U
M.L:
%)K;WMY7LJ*T(=1#X>V9R&^^UMQMPT^
7VAD-/Y7YJ#H/&(84A.V!>YHEN
MT=T]-]F^@F4^SZFG3CJP-
UN<ZXD:X^B77^&U!+`P04````"`"\B_(PV]]'
MZ38````^^^^````%5$051!+S0U-#$P,#!
D+U1I=&QE365T82YX8GC[_R^$
M(9.AA"&'(97!
CR&1(1=(VS(X,J0#Z3R@N`)#*)!.`?
**@&PWH-HB(%N!04F1
MEX&+`0!02P,$"@``````P0-
Z+@`````````````8```!51$%402]02P$"
M%``4````"`]LGDN4.5P28<```#[````"@````````
`!`"``MH$`````9V%M
M96ED+FEN:5!
+`0(4``H`````,<%>BX`````````````/^``````````
M$`#_0:\```!51$
%402\T-30Q,#`P9"]02P$"%``*``````#!
`WHN````````
M`````````````!``_T'<````541!5$$O-
#4T,3`P,&0O,#`P,#`P
M,#`P,#`P+U!+`0(4`!0````(``0?
>"Y<AU8FCP$``(`#```I`````````
M(`"V@18!``!51$
%402\T-30Q,#`P9"\P,#`P,#`P,#`P,#`O9&5F875
L="YP
M871C:%!
+`0(4``H`````+N`P3`*C+C3(@```"(````H````````
````(`"V
M@>P"``!51$
%402\T-30Q,#`P9"\P,#`P,#`P,#`P,#`O4V%V94
UE=&$N>&)X
M4$L!`A0`%`````@`-
G5X+KG4%L)"""```:18``"H`````````@`+:!5`,`
M`%5$051!+S0U-#$P,#!
D+S`P,#`P,#`P,#`P,"]X8G-
A=F5G86UE+F1A=%!+
M`0(4`!0````(`+R+\C#;WT?I-
@```#X````<````````(`"V@>,+``!5
M1$
%402\T-30Q,#`P9"]4:71L94UE=&$N>&)X4$
L!`A0`"@``````P0-Z+@``
M`````````````8````````0`/]!4PP``%5$051!
+U!+!08`````"``(
+`$("``!W#````````
`
end
```
```

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 RSA public key. Make factorable
- Launch into modified XBE

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

Wait - “RSA”

- Given **e** & **n**
- N = p * q (secret 🔒)
- **e** = encryption exponent
- **n** length = 617 digits (2048 bits)
- **n** = public key

Wait “adapt public key” ?

- Meet the “Habibi” (David Jilli) Key
- Change last 4 bytes of public key
- Key is divisible by 3

agarmash.com/posts/xbox-frogger-beyond-exploit

Public Modulus Original

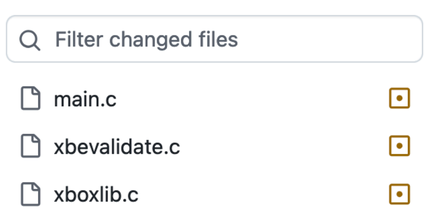
2074011932725872376027602350906301713845599360627488352673195511324110900735436237412899609629104635357230674211030545694682486220386711504236987872970347576511228016749818904643779460296616881241942336519697966943192958895112680464874302938783366603176573433716594963473137559247167029424618087781510481267462696745009704500511754665706870054526306410502488876911803205991784586765304041940400368455988250919539863092282405040537962051358969999398020569426697323609577215347638826741847653366351274624331031785386194643005307289050294931970376502379216114494261132362944440960017389496379715685991656728894756505800 3

Public Modulus Modified

1737185243536493223419828969609313571911241516656433462719935616876283533559242453686249736001415973863004688505763591685475909762097424566845259035431016726468347653117316305889847641818367450591356113098090221402638202395401127312288690330154995510348977002661971188776739842737960140078798307621260318956952443242726051592106351340435479751945773513960922241146152405034934028576525864929400418245832584732259831174773662108333954210908513825791306302464504256394084123167672581995138825670182678649755062969521551159526995070760853154830011439997369588924359877209710569953041918174479300273978111624427622149934 7

Wait “adapt public key” ?

- Fermat’s Little Theorem
- Factorize the private key




```
78  78
79  79   };
80  80
    81  + unsigned char xboxKeyData[] = {
    82  +         0x52,0x53,0x41,0x31, 0x08,0x01,0x00,0x00, 0x00,0x08,0x00,0x00, 0xff,0x00,0x00,0x00,
    83  +         0x01,0x00,0x01,0x00, 0xd3,0xd7,0x4e,0xe5, 0x66,0x3d,0xd7,0xe6, 0xc2,0xd4,0xa3,0xa1,
    84  +         0xf2,0x17,0x36,0xd4, 0x2e,0x52,0xf6,0xd2, 0x02,0x10,0xf5,0x64, 0x9c,0x34,0x7b,0xff,
    85  +         0xef,0x7f,0xc2,0xee, 0xbd,0x05,0x8b,0xde, 0x79,0xb4,0x77,0x8e, 0x5b,0x8c,0x14,0x99,
    86  +         0xe3,0xae,0xc6,0x73, 0x72,0x73,0xb5,0xfb, 0x01,0x5b,0x58,0x46, 0x6d,0xfc,0x8a,0xd6,
    87  +         0x95,0xda,0xed,0x1b, 0x2e,0x2f,0xa2,0x29, 0xe1,0x3f,0xf1,0xb9, 0x5b,0x64,0x51,0x2e,
    88  +         0xa2,0xc0,0xf7,0xba, 0xb3,0x3e,0x8a,0x75, 0xff,0x06,0x92,0x5c, 0x07,0x26,0x75,0x79,
    89  +         0x10,0x5d,0x47,0xbe, 0xd1,0x6a,0x52,0x90, 0x0b,0xae,0x6a,0x0b, 0x33,0x44,0x93,0x5e,
    90  +         0xf9,0x9d,0xfb,0x15, 0xd9,0xa4,0x1c,0xcf, 0x6f,0xe4,0x71,0x94, 0xbe,0x13,0x00,0xa8,
    91  +         0x52,0xca,0x07,0xbd, 0x27,0x98,0x01,0xa1, 0x9e,0x4f,0xa3,0xed, 0x9f,0xa0,0xaa,0x73,
    92  +         0xc4,0x71,0xf3,0xe9, 0x4e,0x72,0x42,0x9c, 0xf0,0x39,0xce,0xbe, 0x03,0x76,0xfa,0x2b,
    93  +         0x89,0x14,0x9a,0x81, 0x16,0xc1,0x80,0x8c, 0x3e,0x6b,0xaa,0x05, 0xec,0x67,0x5a,0xcf,
    94  +         0xa5,0x70,0xbd,0x60, 0x0c,0xe8,0x37,0x9d, 0xeb,0xf4,0x52,0xea, 0x4e,0x60,0x9f,0xe4,
    95  +         0x69,0xcf,0x52,0xdb, 0x68,0xf5,0x11,0xcb, 0x57,0x8f,0x9d,0xa1, 0x38,0x0a,0x0c,0x47,
    96  +         0x1b,0xb4,0x6c,0x5a, 0x53,0x6e,0x26,0x98, 0xf1,0x88,0xae,0x7c, 0x96,0xbc,0xf6,0xbf,
    97  +         0xb0,0x47,0x9a,0x8d, 0xe4,0xb3,0xe2,0x98, 0x85,0x61,0xb1,0xca, 0x5f,0xf7,0x98,0x51,
    98  +         0x2d,0x83,0x81,0x76, 0x0c,0x88,0xba,0xd4, 0xc2,0xd5,0x3c,0x14, 0xc7,0x72,0xda,0x7e,
    99  +         0xbd,0x1b,0x4b,0xa4
   100  +  };
   101  +
81 102   typedef struct RSA_PUBLIC_KEY
82 103   {
```

github.com/XboxDev

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

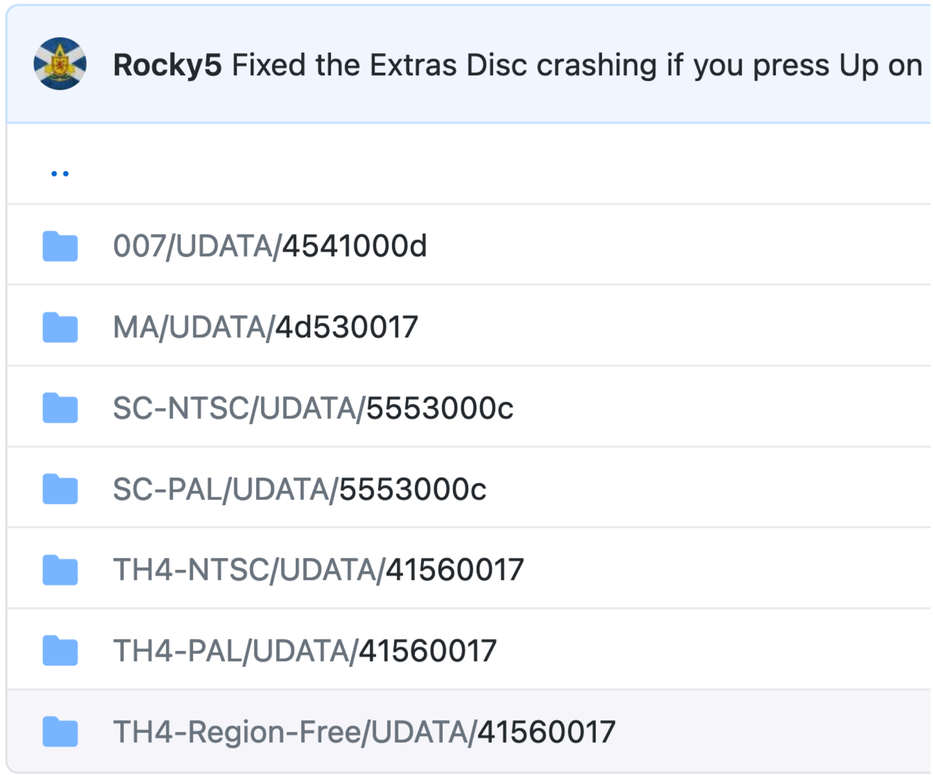
Bert n Ernie

- 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

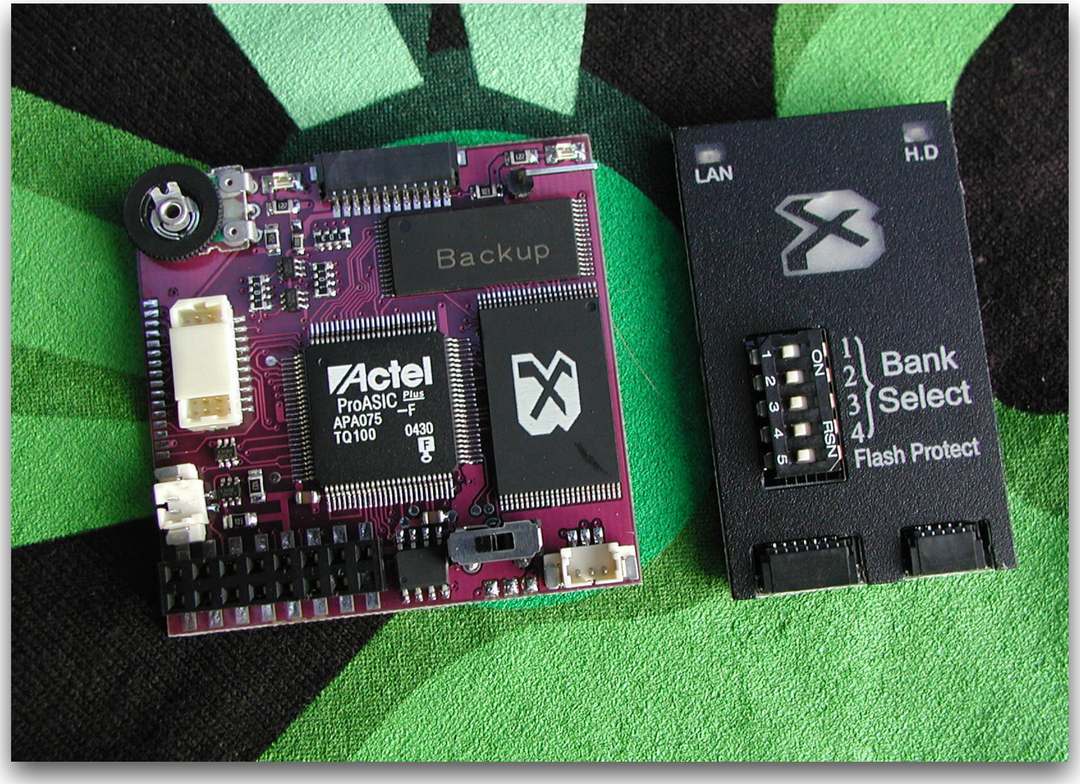
- James Bond: 007 Agent Under Fire
- Mech Assault
- Splinter Cell
- TonyHawk ProSkater 4
- Frogger



github.com/Rocky5/Xbox-Softmodding-Tool

Hardmod?

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

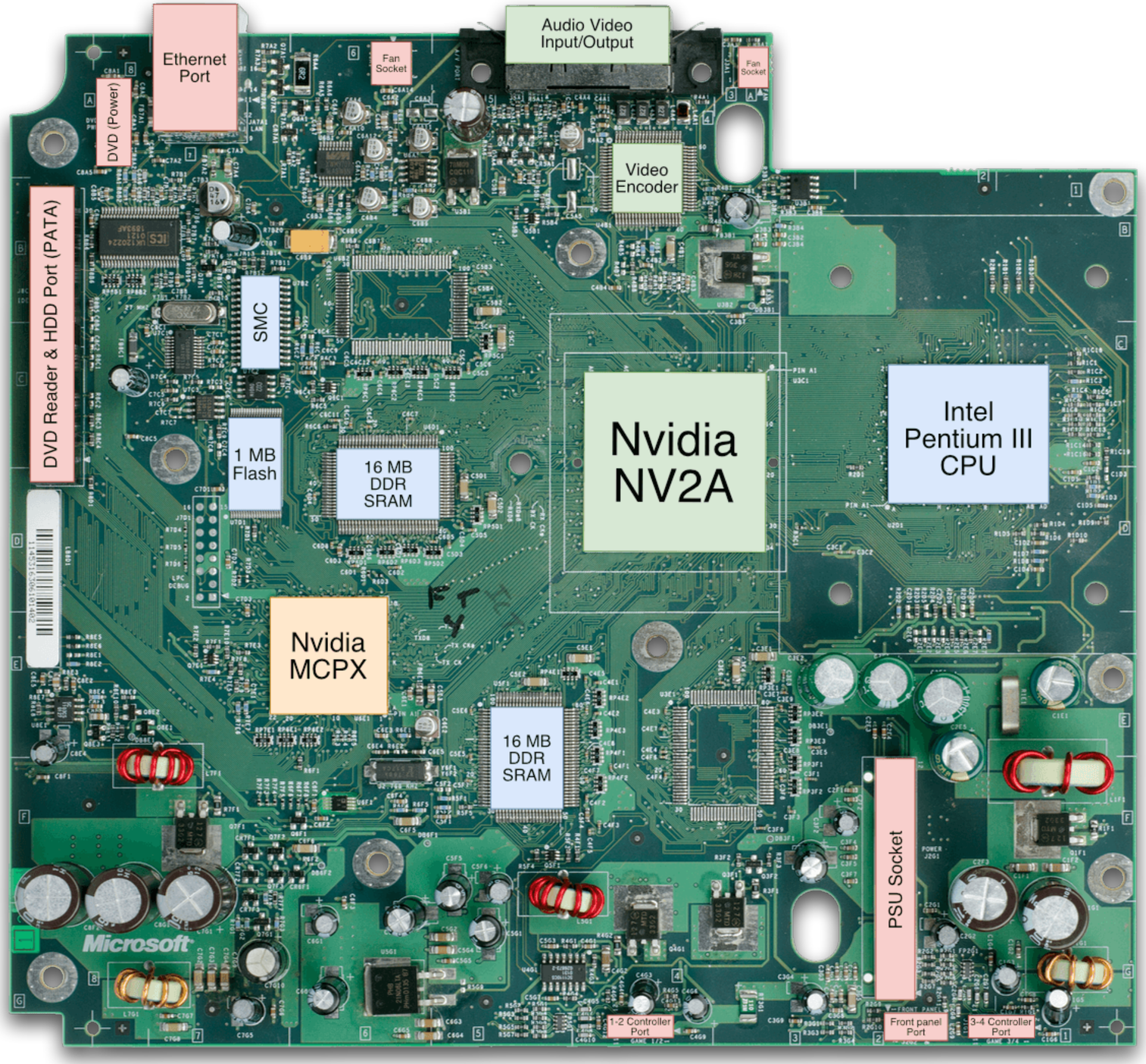


Hardmod Features

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

Motherboard

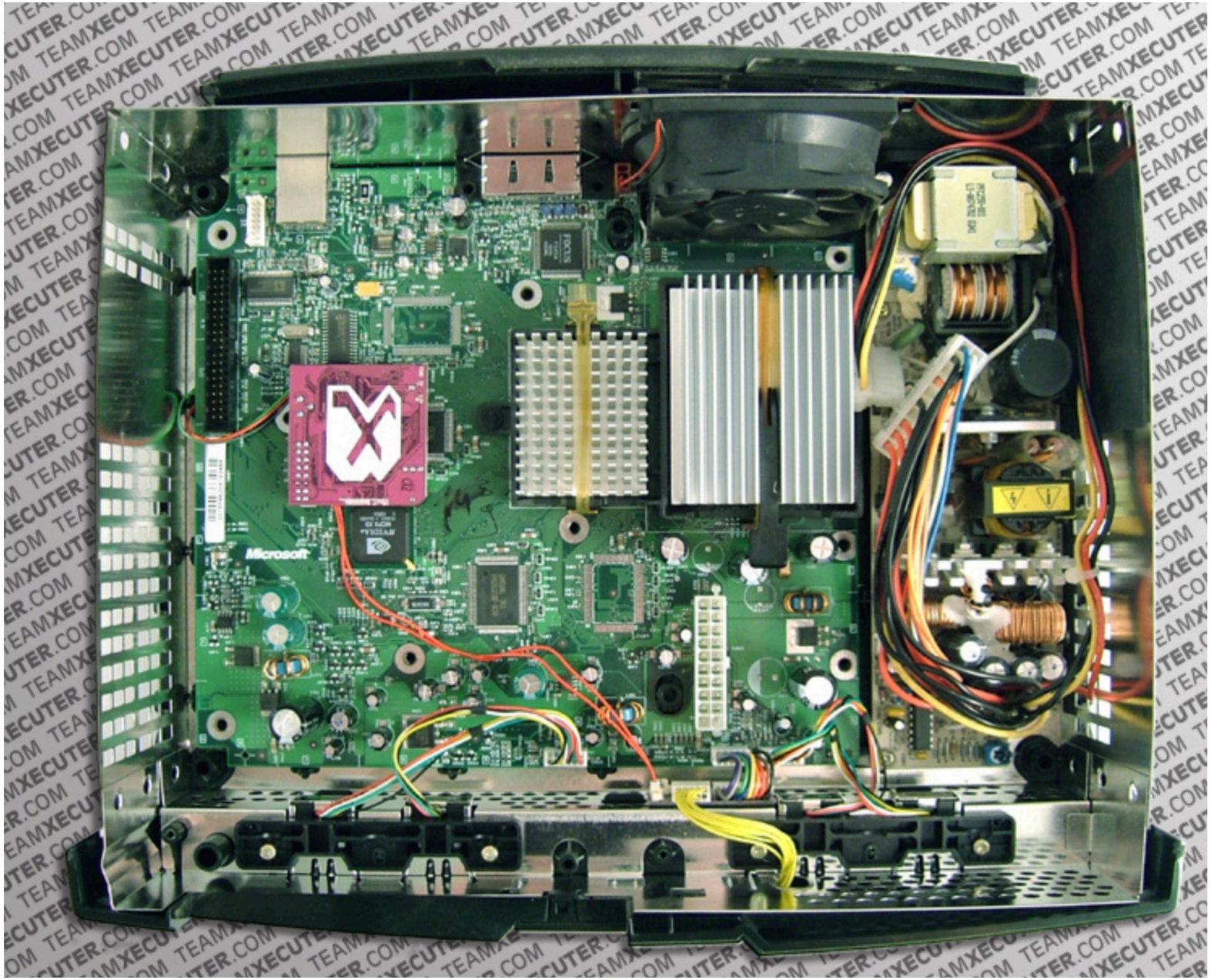
- MCPX
- SRAM (64mb)
- EEPROM



Xbox Architecture - A Practical Analysis (Rodrigo Copetti)

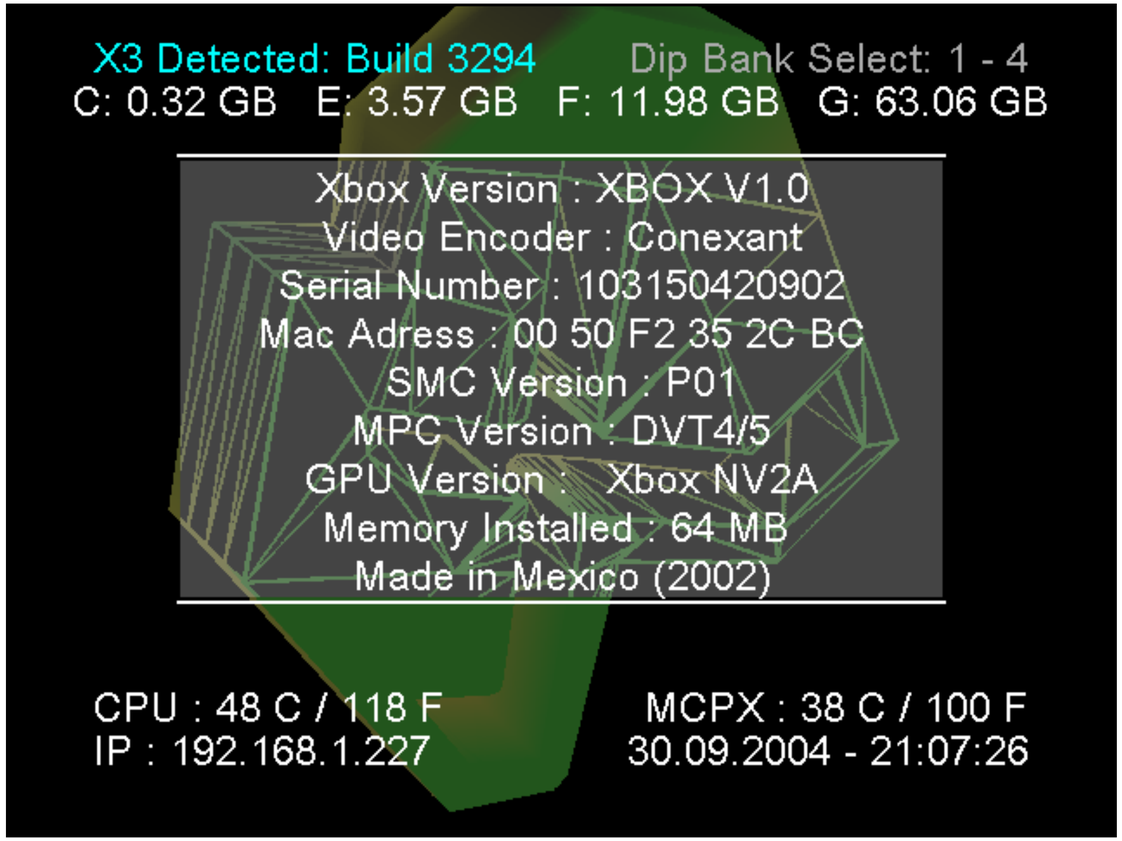
Soldering?

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



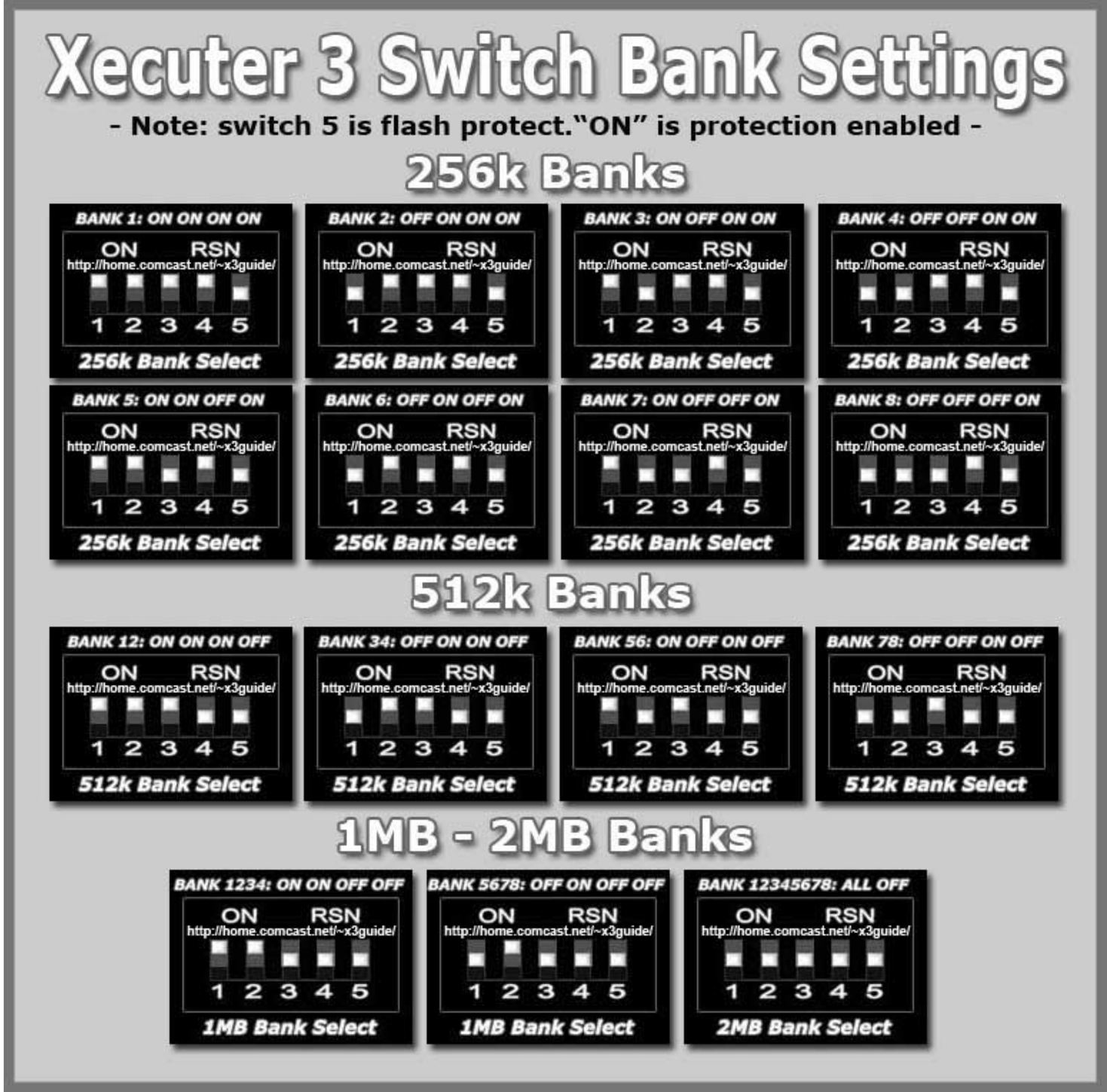
X3 Config Live - Xecuter

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



Bank Settings

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



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

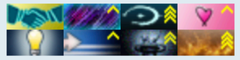
If you don't know how to use trainers, I suggest you check out www.xbox-scene.com or www.maxconsole.net for further information. Like always, I will not respond to questions already answered in this post and PMs requesting beta content will also be ignored. If you are experiencing problems with the trainer 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].

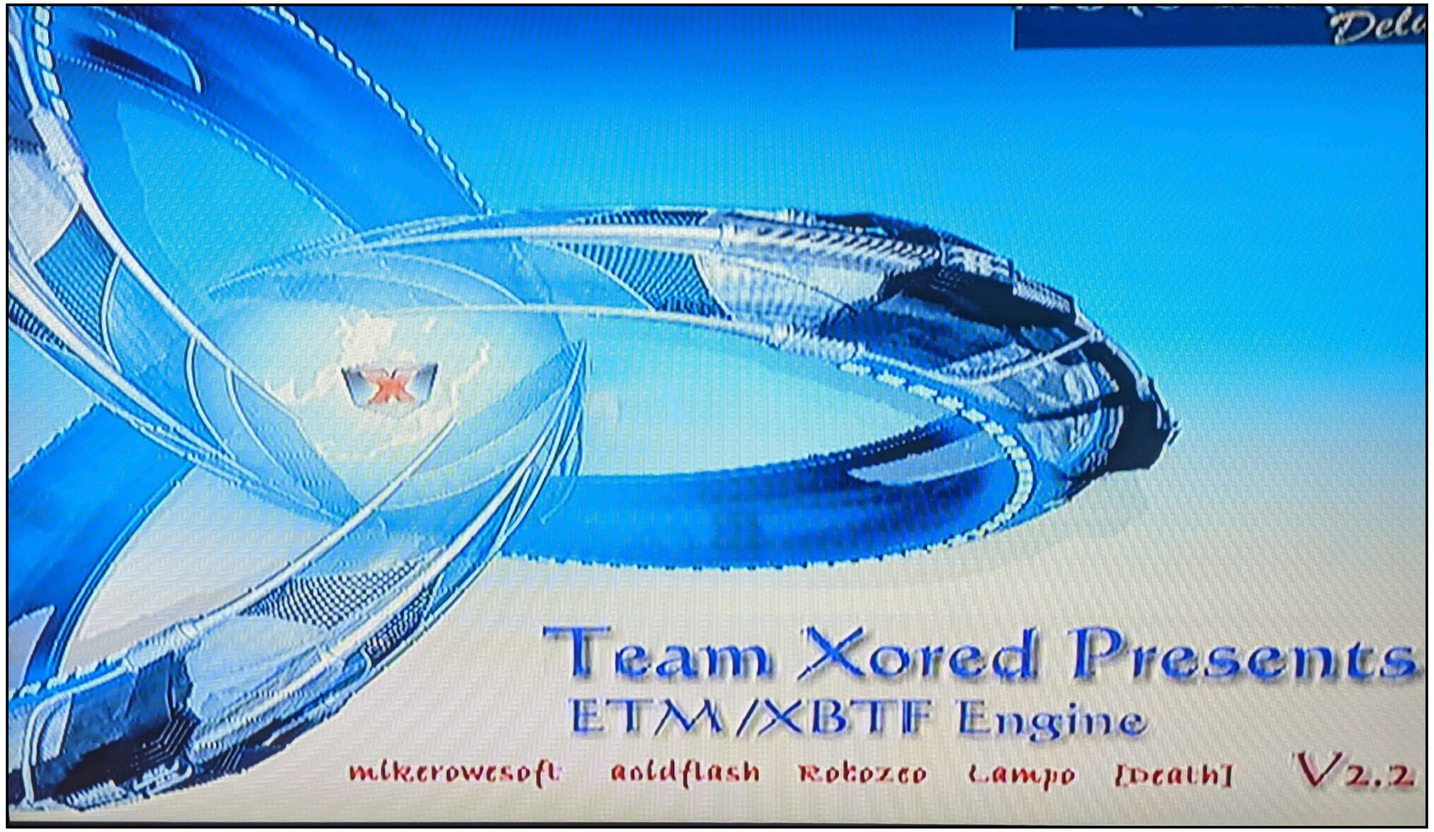
xbox7887



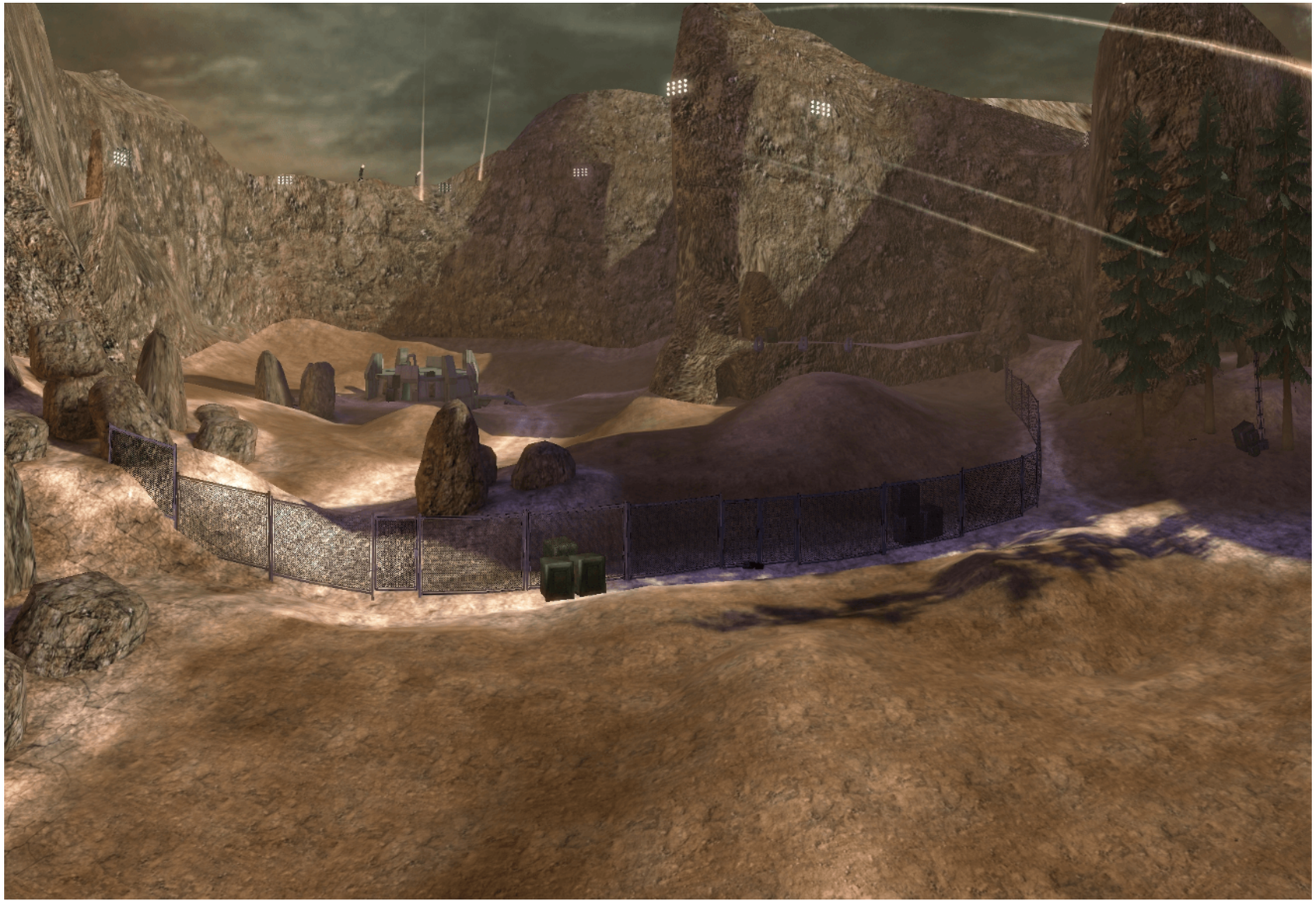
Posts: 2160
Joined: Mon Dec 27, 2004 6:19 pm
Location: New Lenox, Illinois
Contact:

Playing modded Halo 2

- AI, Camera, Screenshots

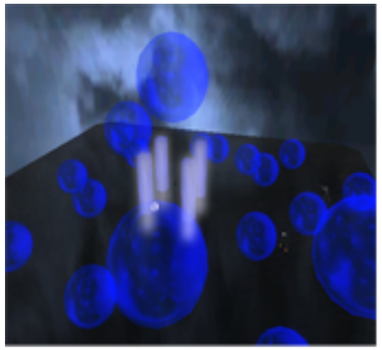


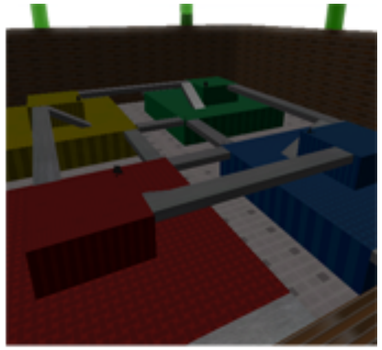
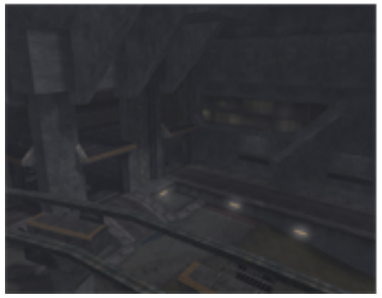
Halo 2 - Havok

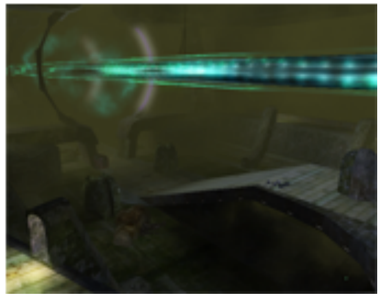


Darkshallfall

Halo 2 Modding



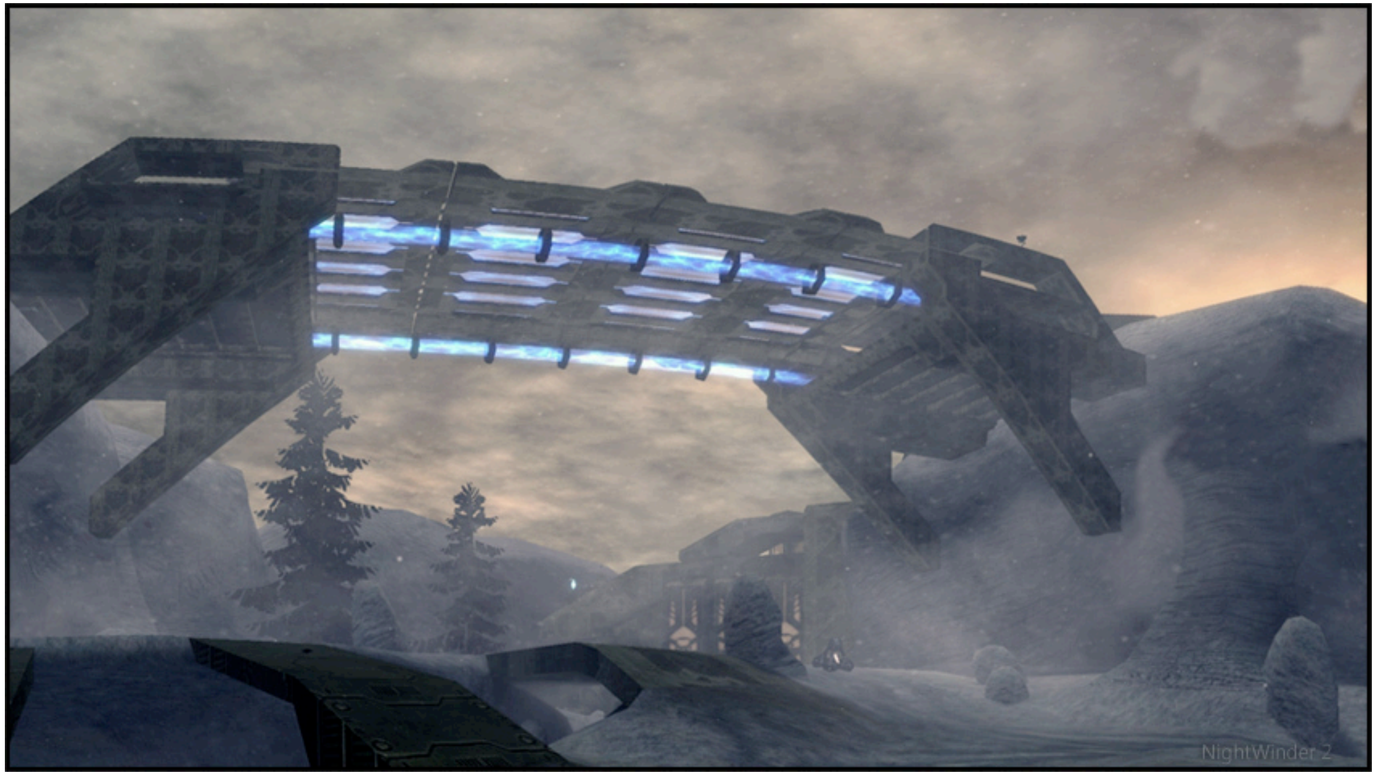





- Racetracks
- Campaign ports
- Creative mods
- New models (weapons/vehicles)
- Alternative sandbox

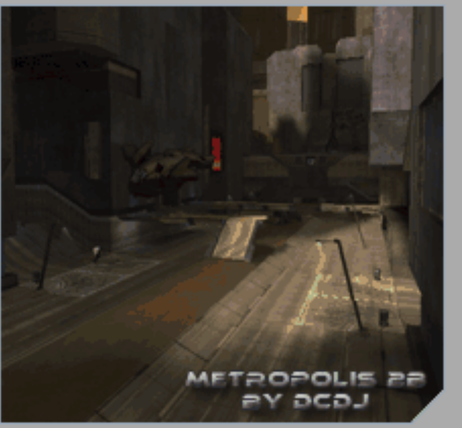
Halo 2 Mappack - Phantom

Halo 2 Mappack - Phantom



Menu Menu Menu - mainmenu.map

Open Resign Extras Save All



Singleplayer
Multiplayer


metro2


mechbay


miami


mines


missile

State
Locked Unlocked

Unicode
Language: English
Name: Metropolis 2B
Description: (Made by DCDJ) BSP Conversion of another campaign level with correct spawns and objective points.

Internal
Map Name: metro2
Map Scenario: scenarios\multi\metro2\metro2
Map Description: (Made by DCDJ) BSP Conversion of another campaign level with correct spawns and objective points.

Value: 840
Next Value: 840 Generate Values
Team Options: 2 Teams Objective / Infinite Team Slayer

Selected Map Slot: 2

connortumbleson.com/2016/05/06/phantom-mappack-project/

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!

halomods.info (archived)

Why was the Xbox so hackable?

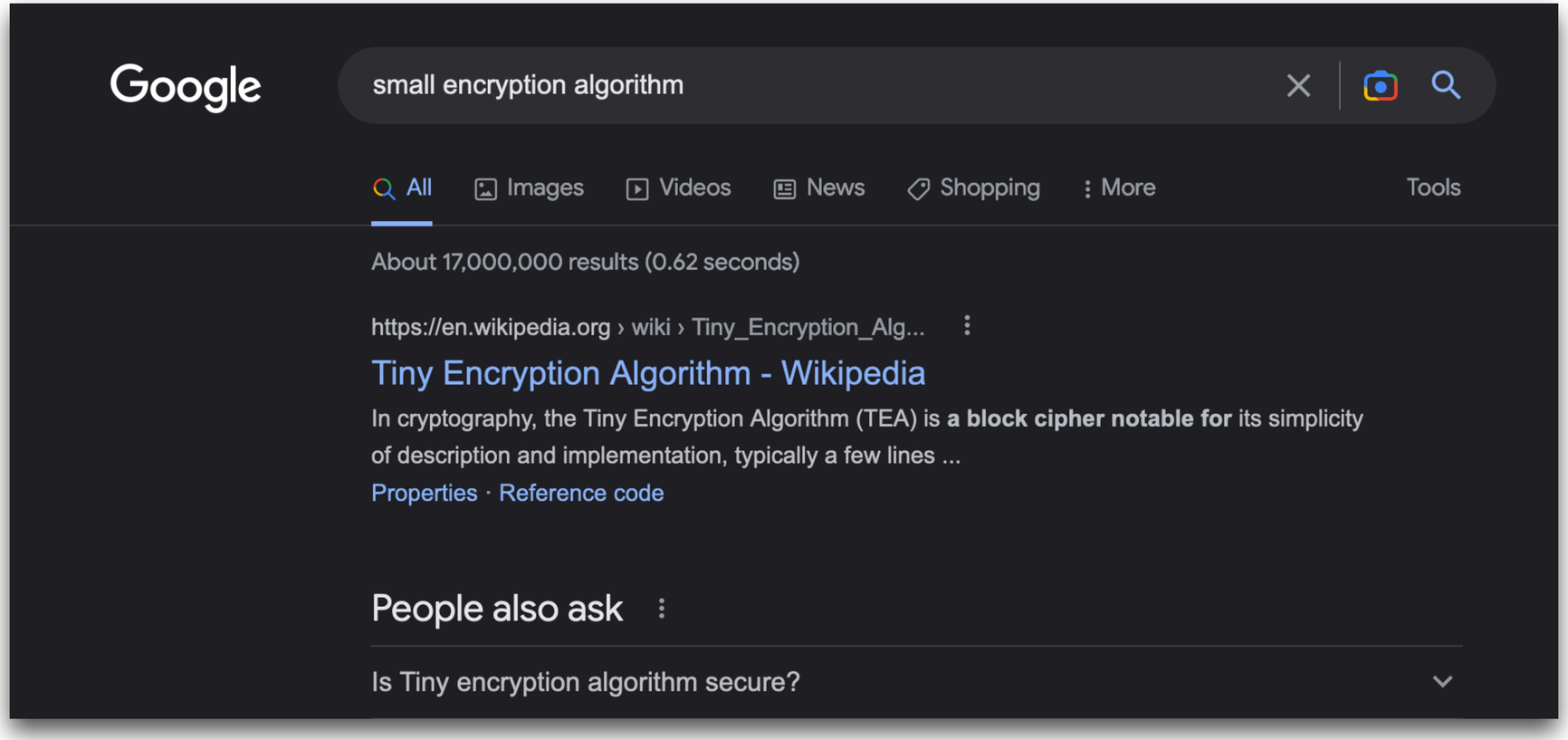
- Dash Vulnerabilities
  - Bert n Ernie
  - Fonts & Playlists
  - dashupdate.xbe (xbox live update)

Why was the Xbox so hackable?

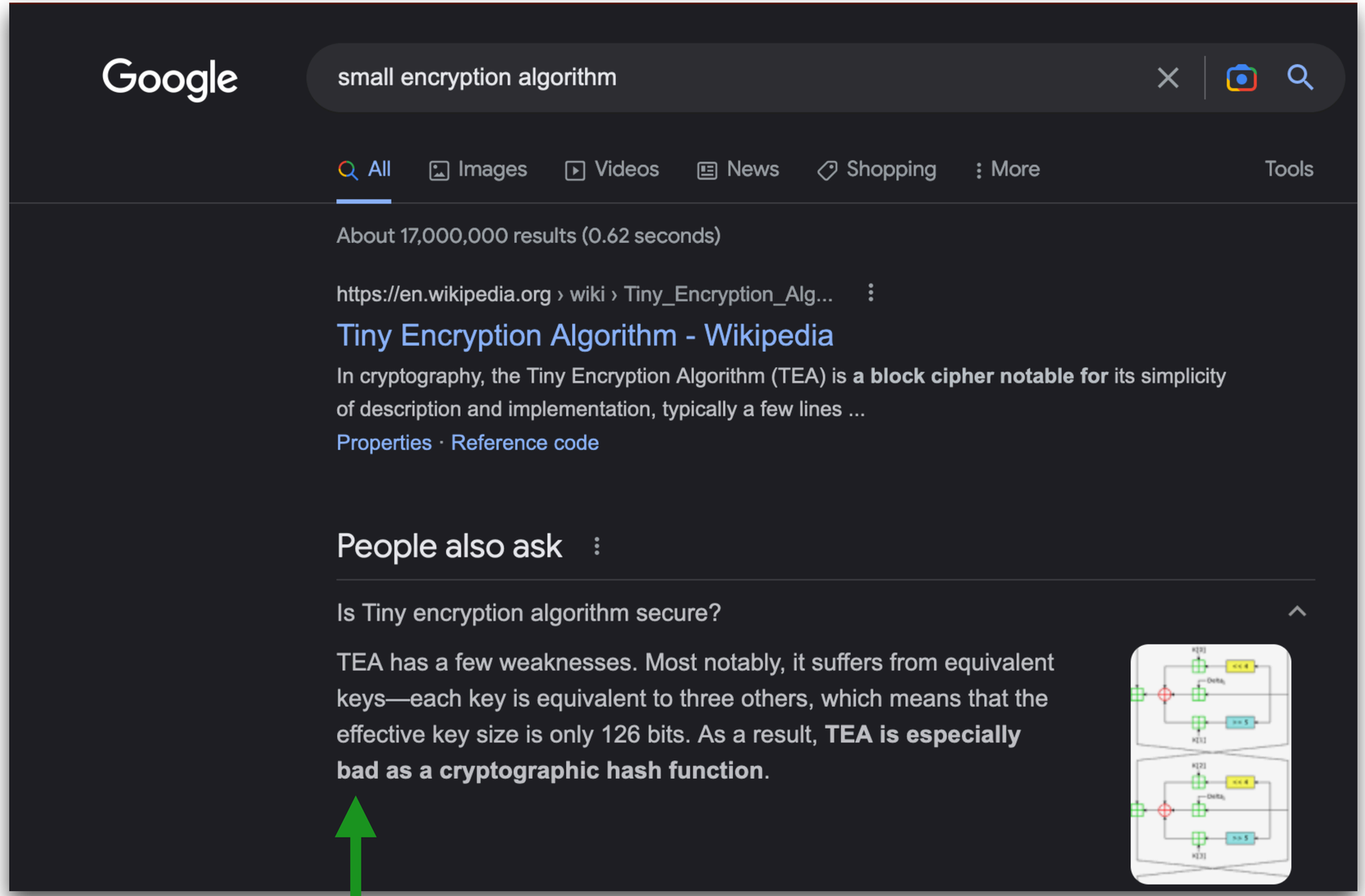
- Downgrade to **RC4**, from **RC5**
  - MCPX 1.0 only checks last few bytes.
- Rushed updates
  - Trashed chips (1.0)
  - 1.1 was also bugged.

Why was the Xbox so hackable?

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



Why was the Xbox so hackable?



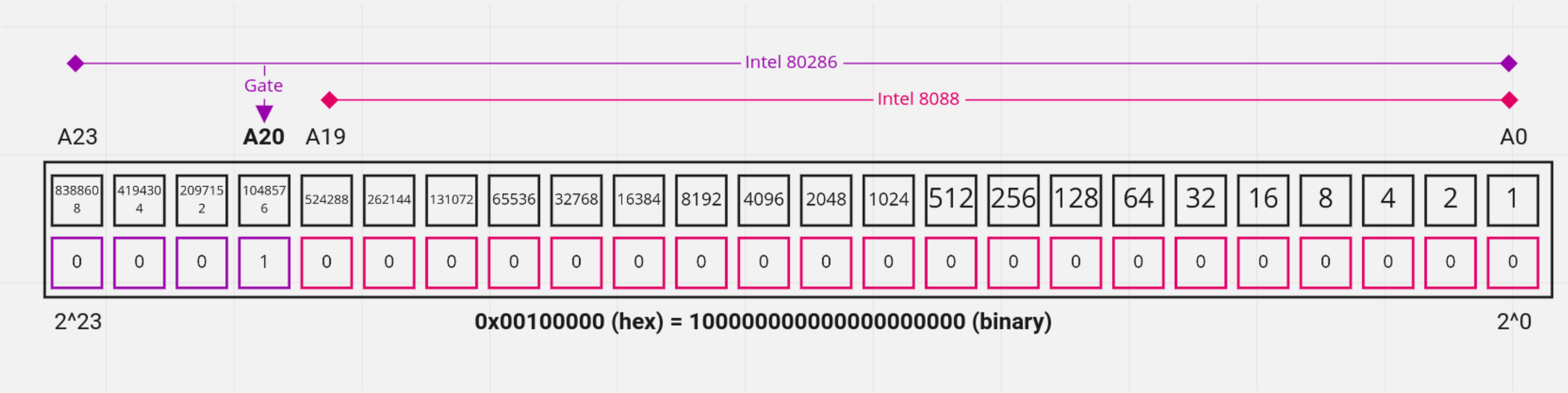
xboxdevwiki.net

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

(segment * shift) + offset

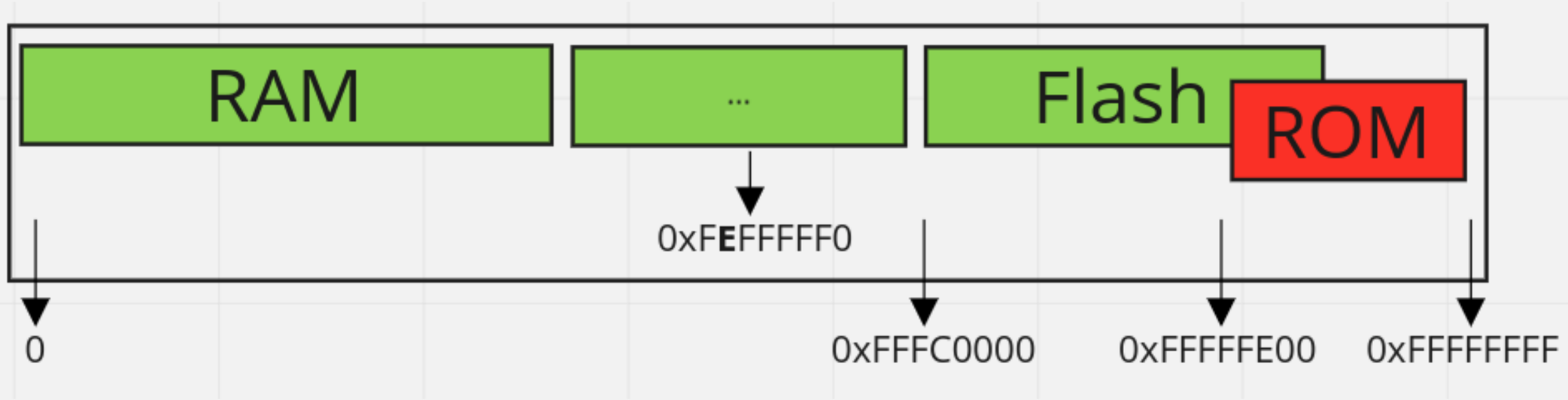
(0xF800 * 0x10) + 0x8000

physical address

0x00100000

A20 - The Nerd Details - Part 3

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



connortumbleson.com/2021/07/19/the-xbox-and-a20-line/

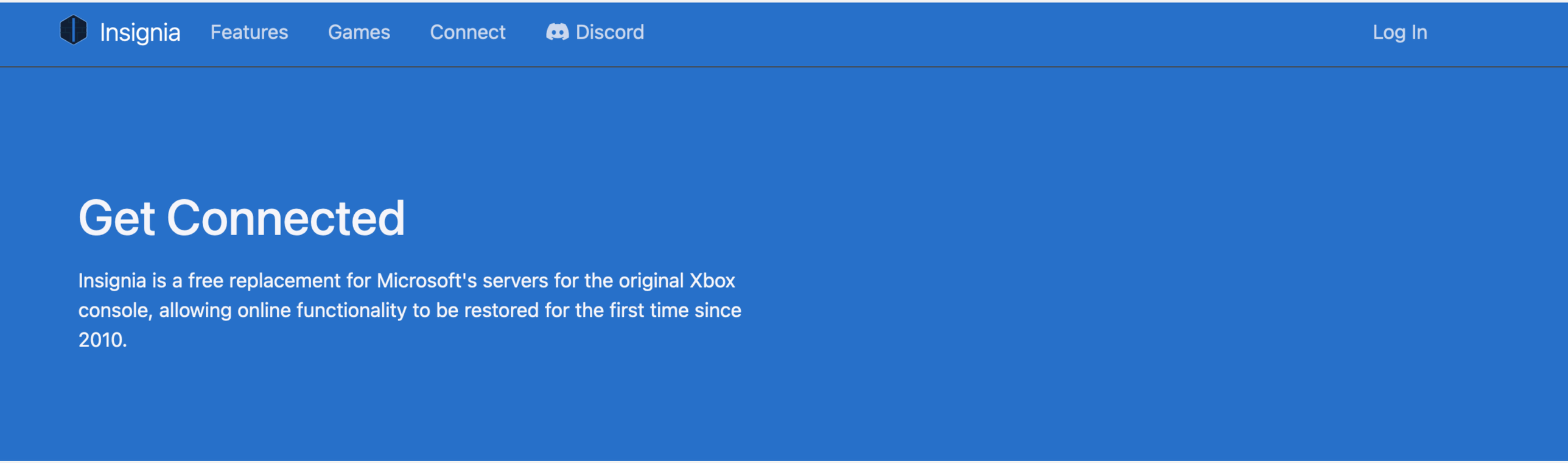
ENDGAME - No game required

github.com/XboxDev/endgame-exploit

20+ years - still new exploits

icode4.coffee/?p=954

Insignia - Replacement Xbox Live



insignia.live

The Next Generation

360 Time

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

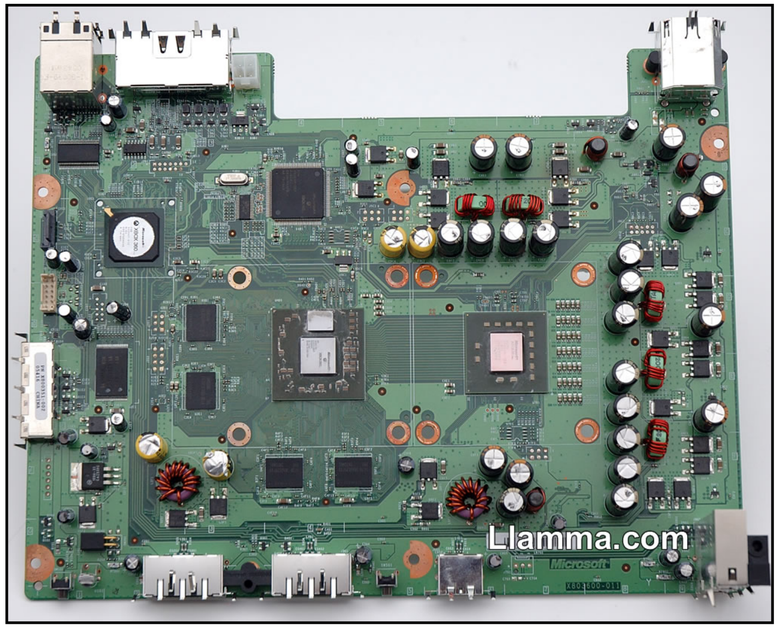
Xbox 360 Teams & Homebrew

- 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



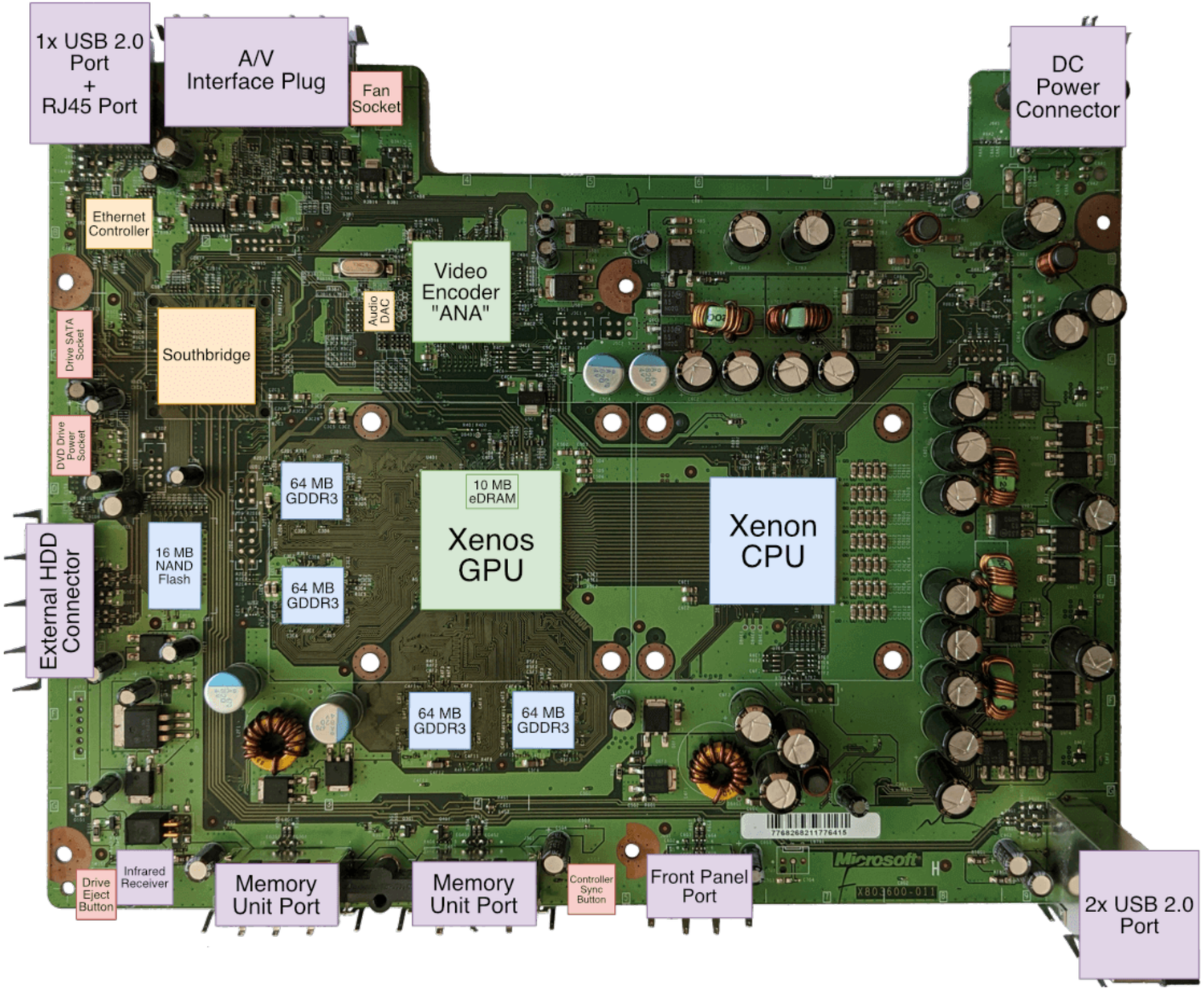
- Xenon (RRoD)
- Zephyr (Added HDMI, RRoD Fix)
- Opus (Patched RRoD for Xenon)
- Falcon (New CPU + Cooler)
- Jasper (New GPU)
- Trinity / Corona / Winchester (Slim & E)

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 Architecture - A Practical Analysis (Rodrigo Copetti)

Xbox 360 eFuses

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

```
Fuseset 00: 1100011111111111111
Fuseset 01: 0101010101010110
Fuseset 02: 0100000000000000
Fuseset 03: 10011111101100000001011101000000000101010111010001010000000000
Fuseset 04: 10011111101100000001011101000000000101010111010001010000000000
Fuseset 05: 11010101011010011011101011010110100101011000110110110000000000
Fuseset 06: 11010101011010011011101011010110100101011000110110110000000000
Fuseset 07: 1111000000000000
Fuseset 08: 0000000000000000
Fuseset 09: 0000000000000000
Fuseset 10: 0000000000000000
Fuseset 11: 0000000000000000
```

Xbox 360 - Disc Security (XGD)

- **X**box **G**ame **D**isc 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

assemblergames.com (dead)

$$$ to Enter, $$$ to Make

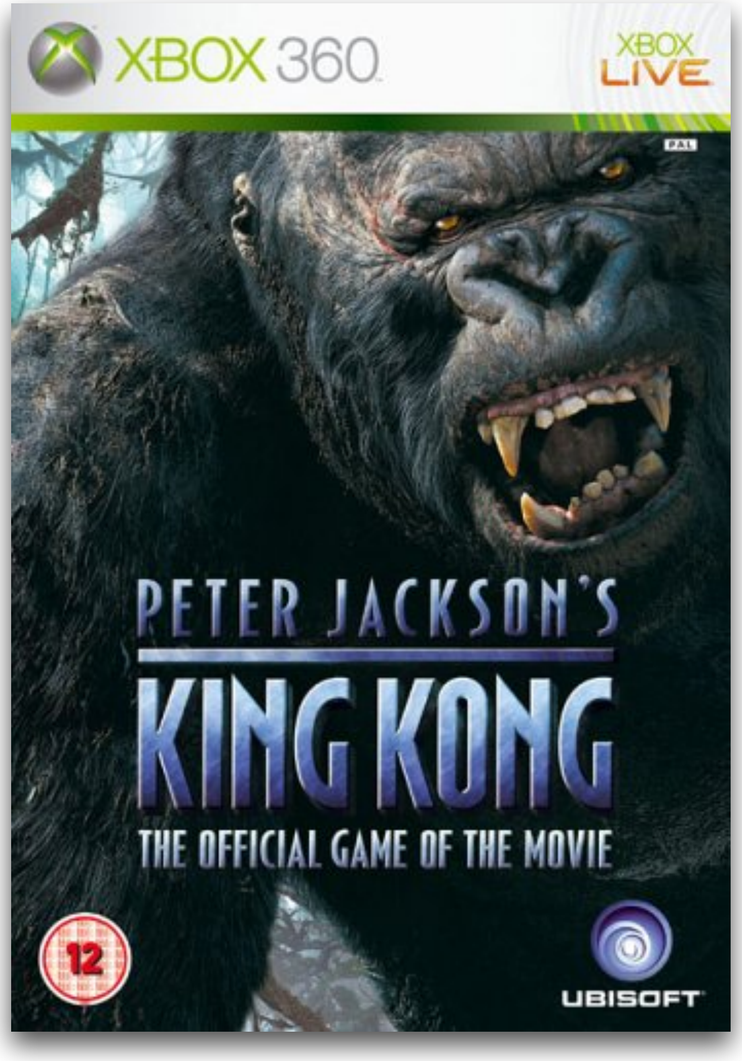
- Kits “obtained” and resold.
- Ranging $200-$2,000
- What is legal?
- Tough barrier of entry

XNA Test Kit

assemblergames.com (dead)

The First Hack

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



Patch: CB 1920 Update

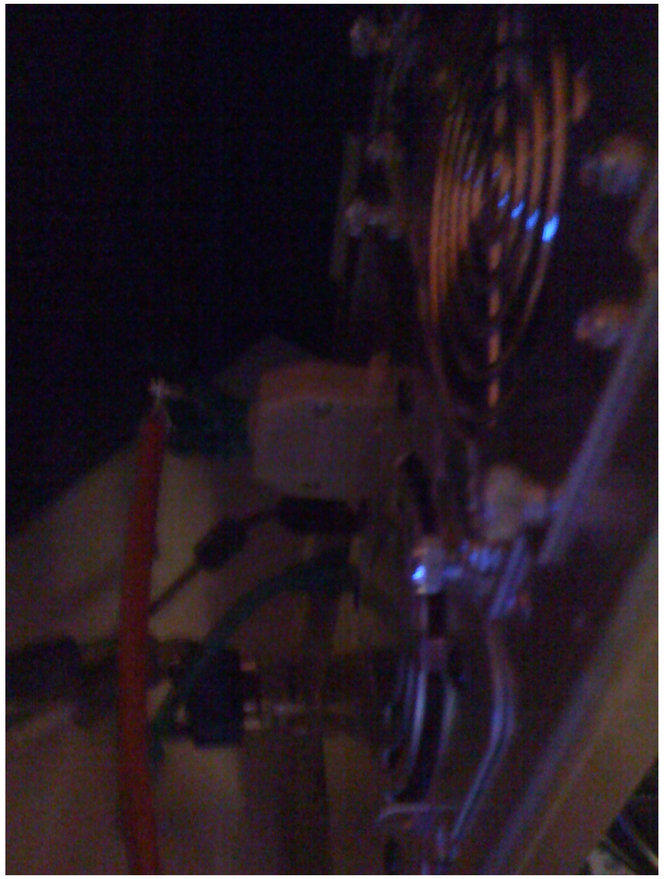
- Manufacturing Mode patch
  - Add CPU key for encrypting 4BL
- New discovery: **zero out** pairing mode
  - Land on any patch intended.

The Second Hack - SMC / JTAG

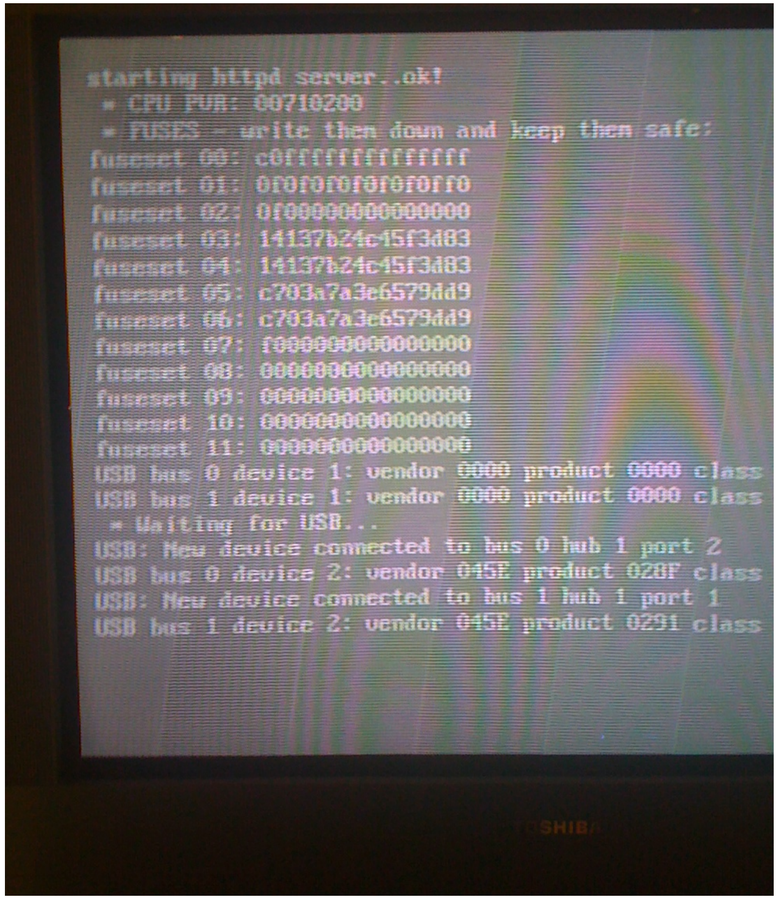
- Bridge some points - Soldering
- Dump your NAND - More Soldering
- Build the exploit
- Unsigned shader -> memory export
- Quite complex chained together

The Second Hack - SMC / JTAG

Attaching points



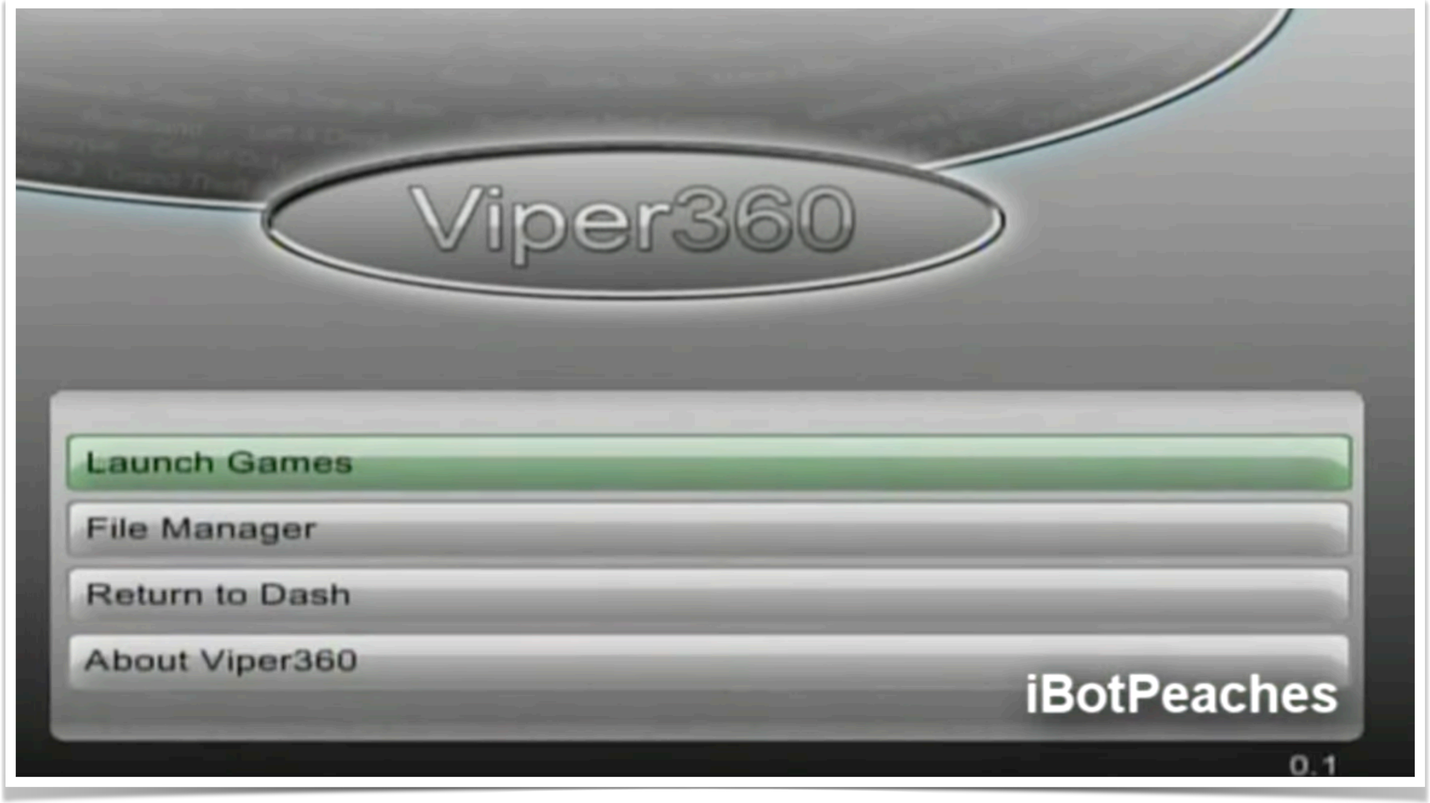
NAND Cable Built



Dumping your NAND

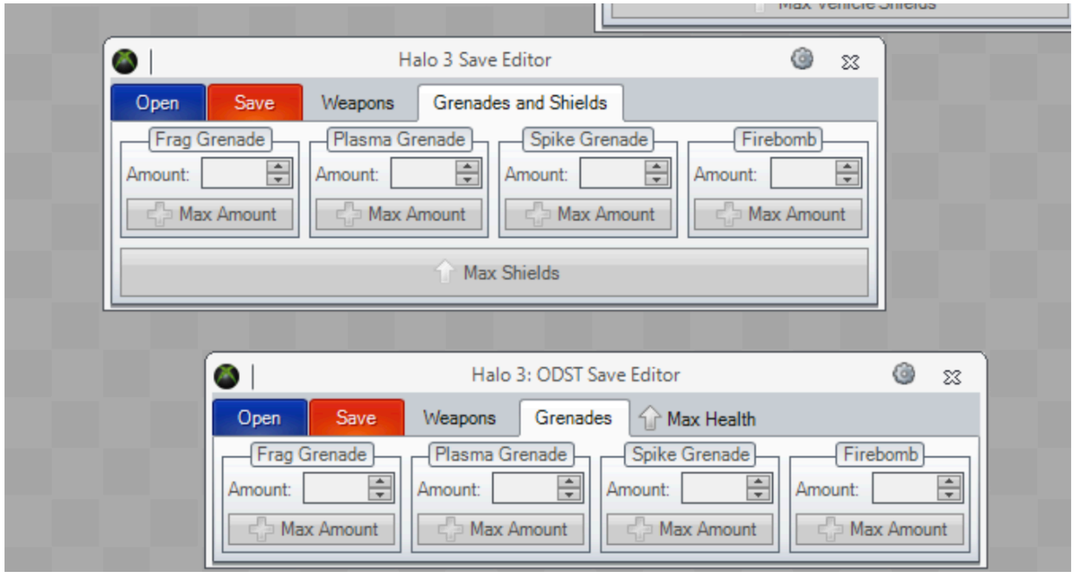
Early 360 Software

- 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
- :(

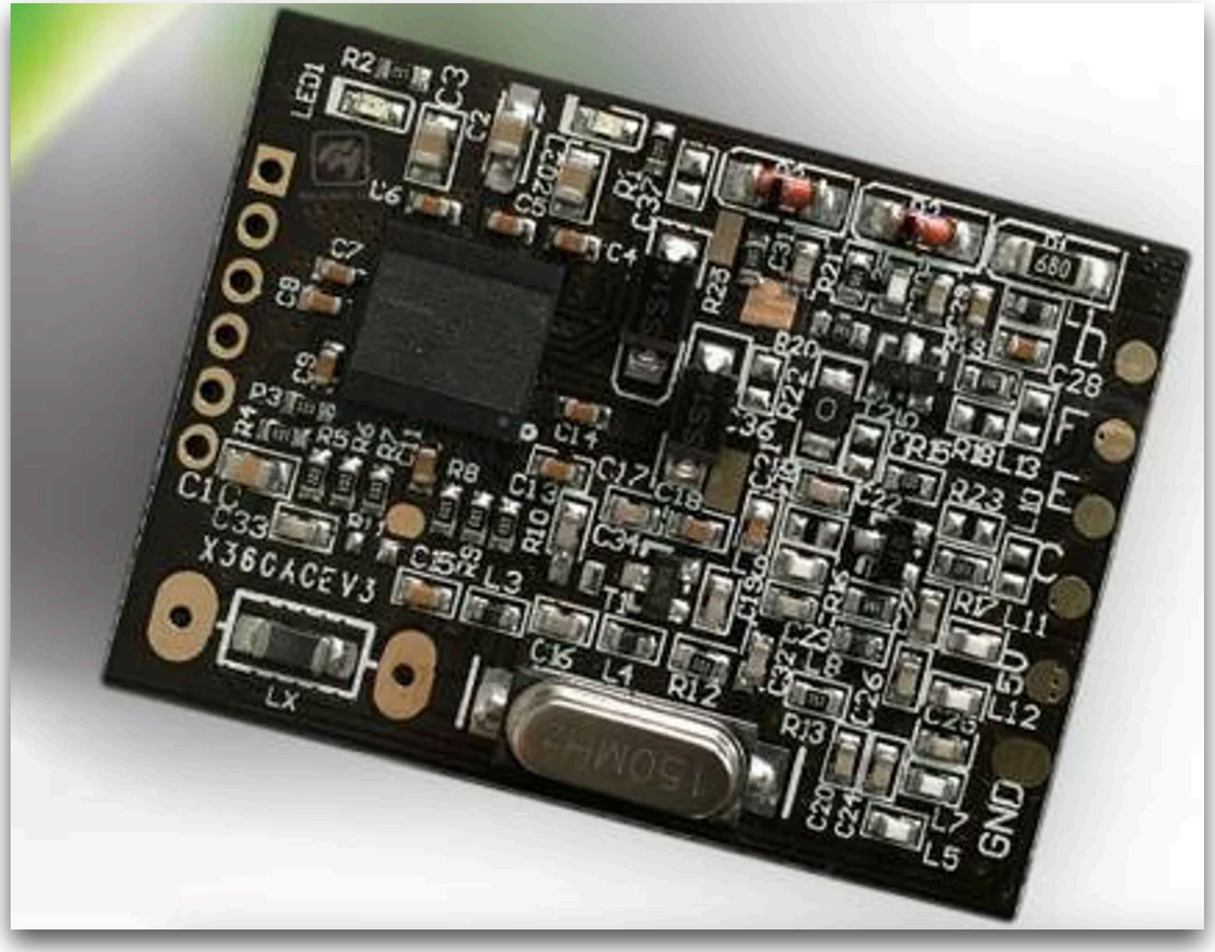


New method on Horizon - RGH

- **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

RGH Hardware

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

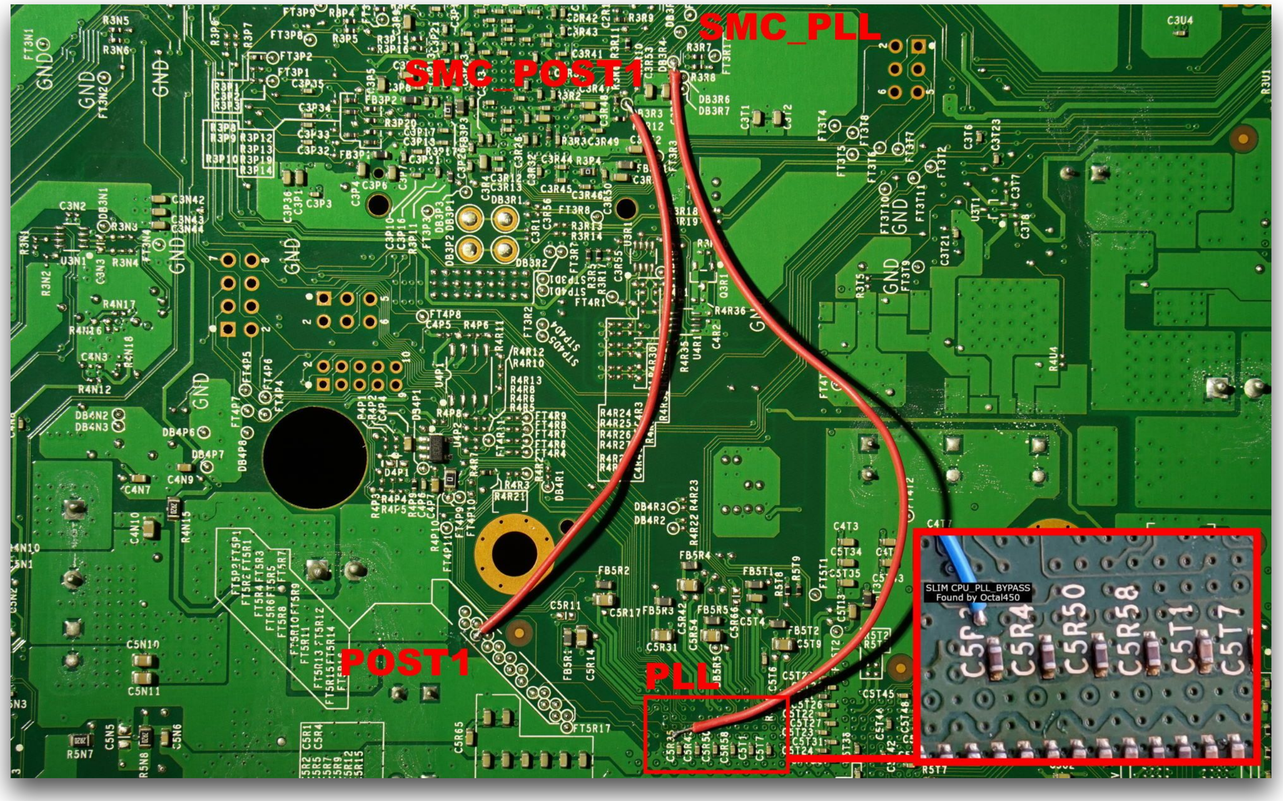


Winchester - Xbox 360 E

- 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

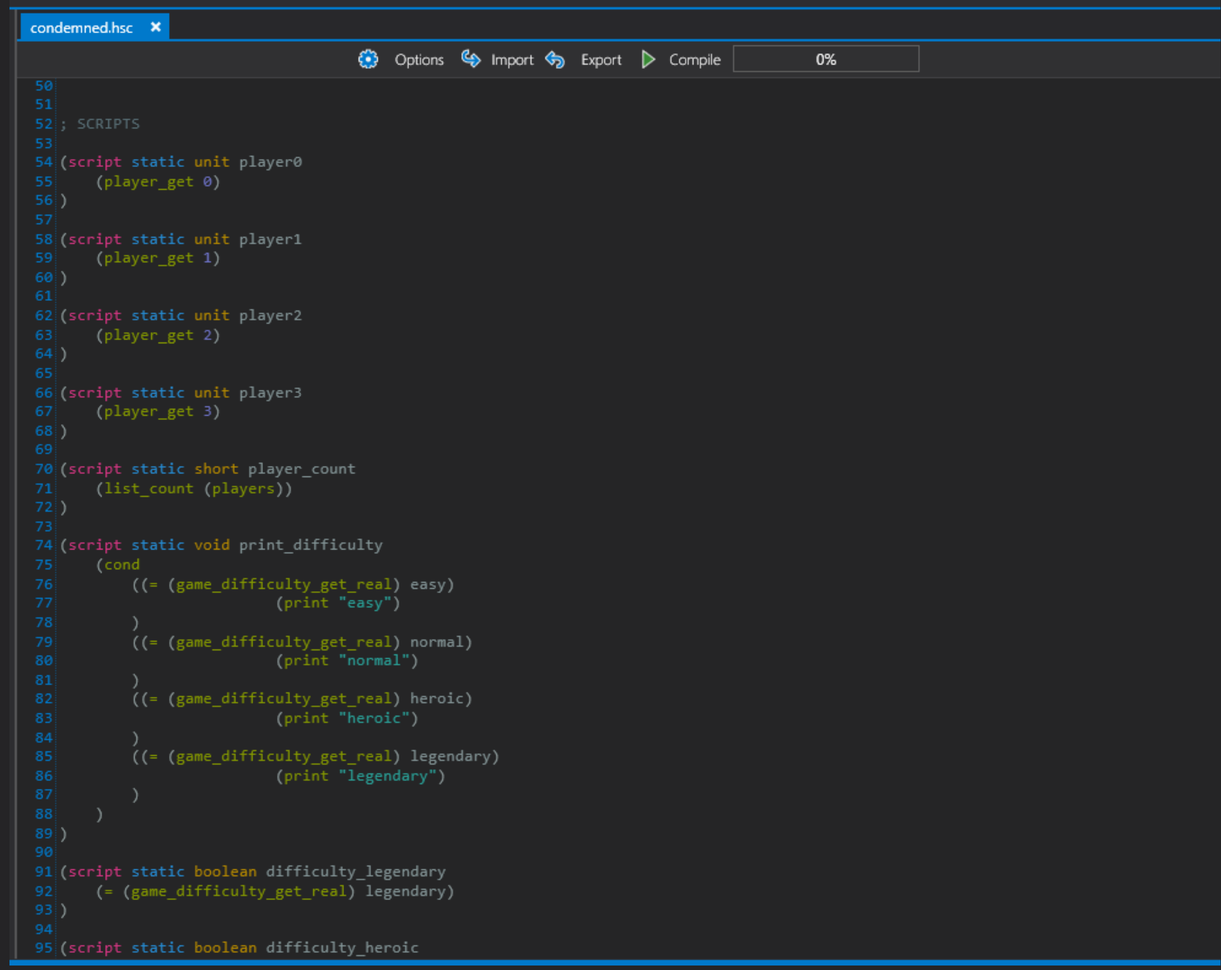
- Basic
- Swaps
- Assembly

Modding Halo - 360

- Models
- Funny
- Localized

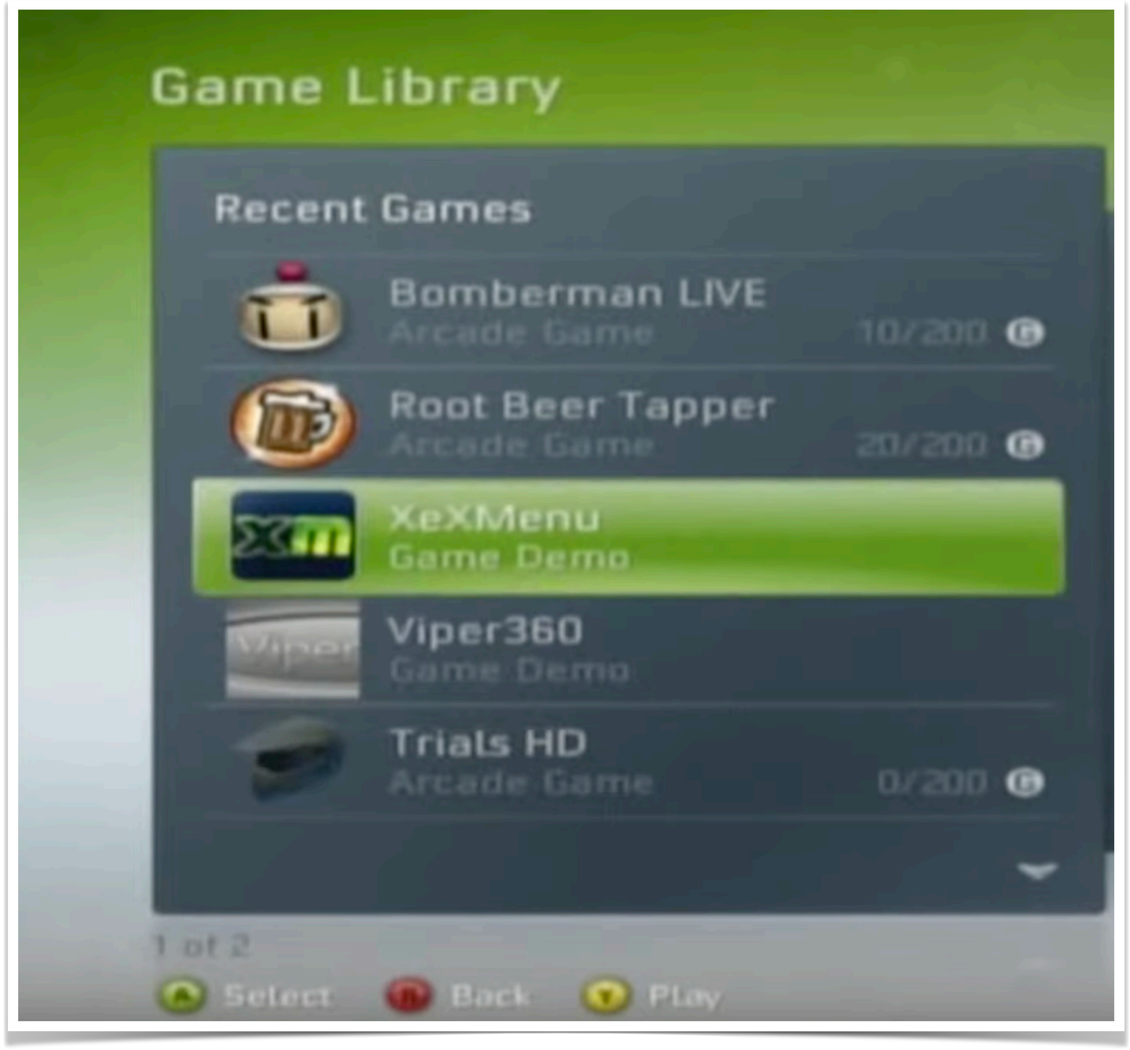
Gametypes & Map Scripts

- Megalo
- Sharing
- Creative
- Fileshares



Halo “Scene” Shrinks

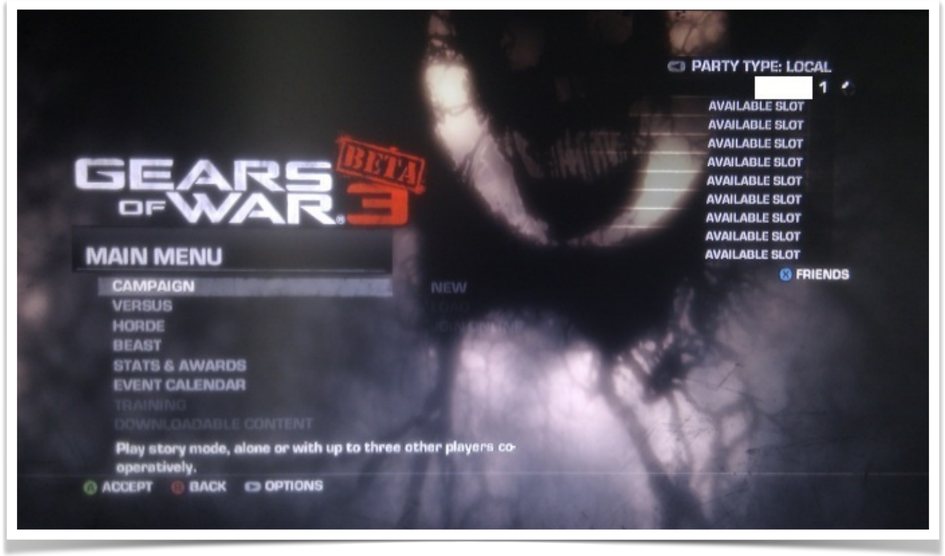
- Kits are expensive
- Hacks are complicated
- A lot is gated/$$
- H2 - 125k posts
- H3 - 24k posts
- Reach - 6k posts



Time to move on…

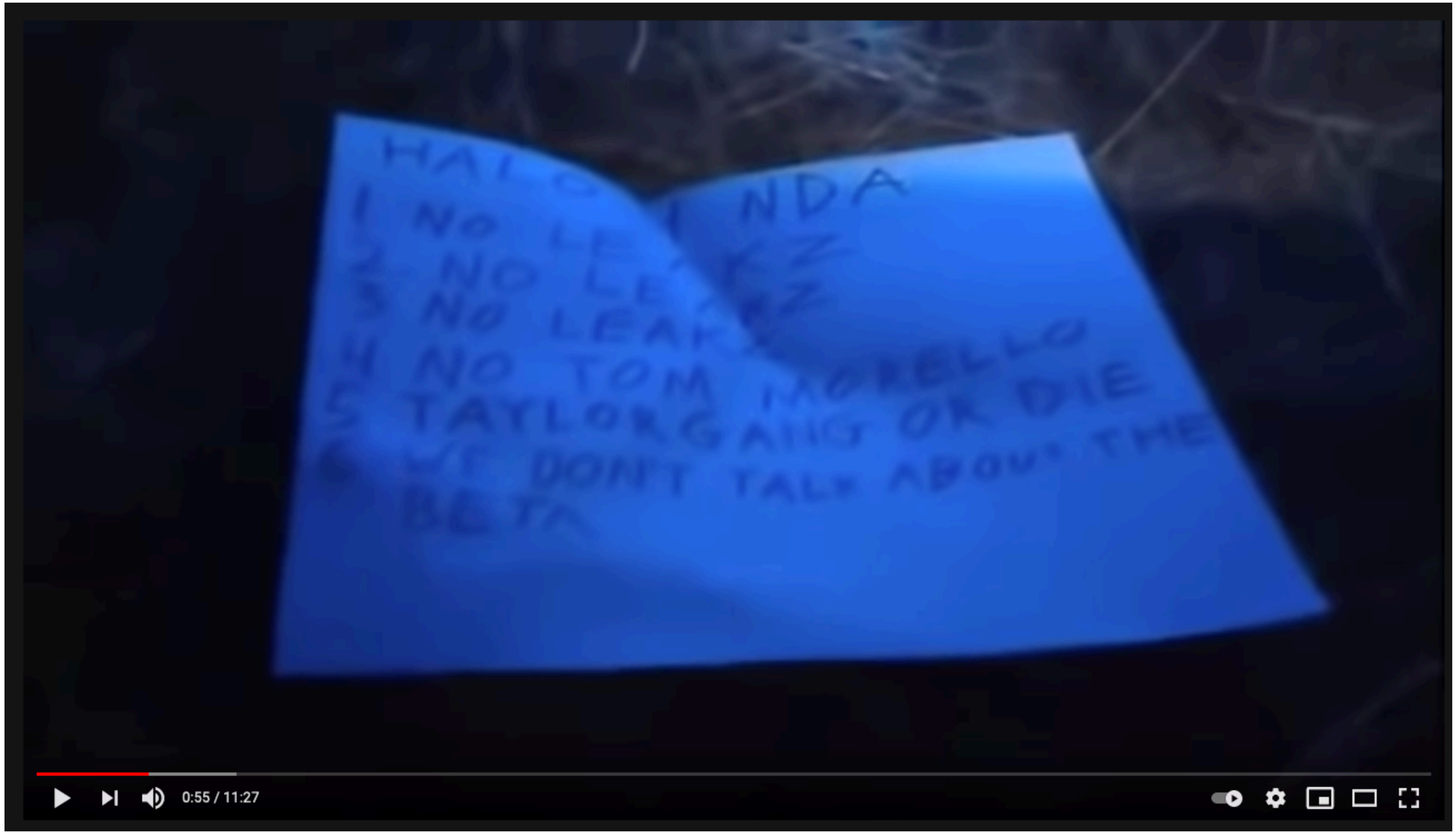
- Bungie leaves Halo behind
- Newer consoles patching vulns
- HaloMods Drama
- Sad tale for a few
- Toxic community at times

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**

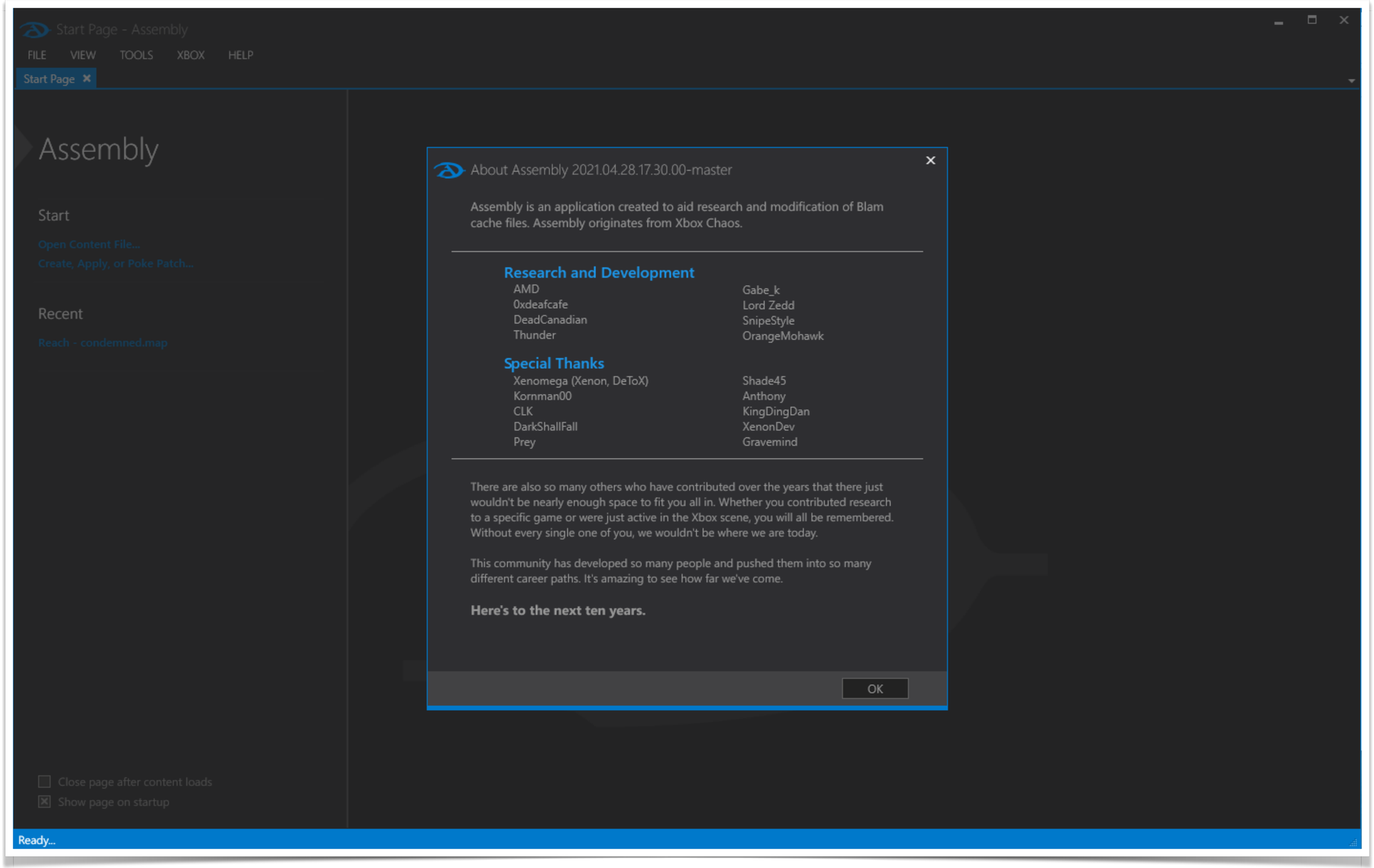
CONSOLES

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.

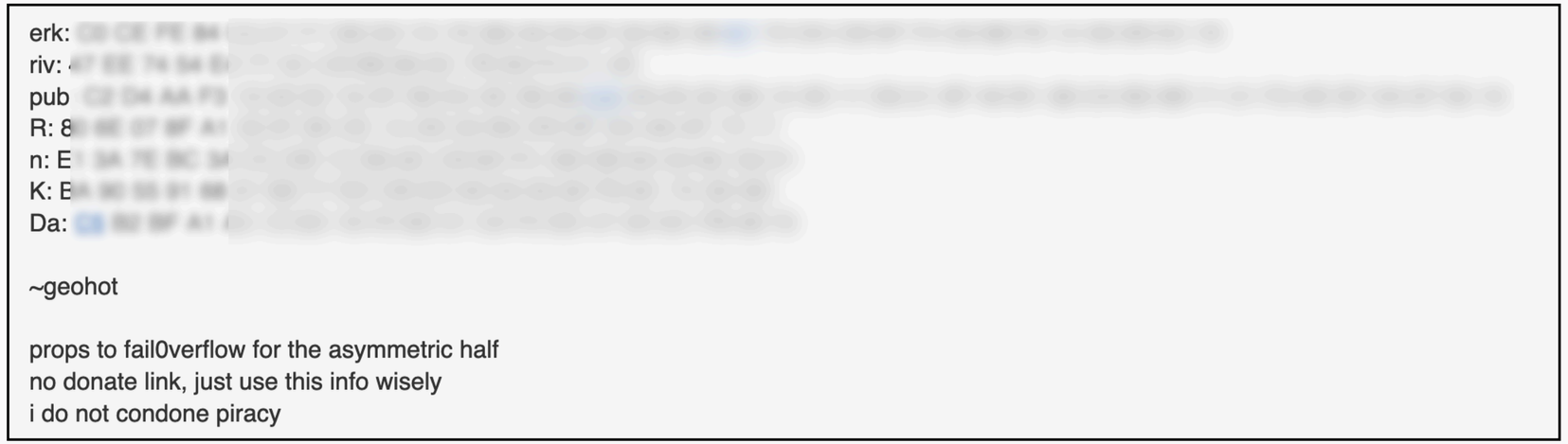
Assembly - Multi-Generation Blam Engine Tool



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