Wii Homebrew

Running and writing software for the Wii

Peter Serwylo

peter@serwylo.com

Homebrew

Homebrew

Noun:

An alcoholic beverage (especially beer) made at home.

Jailbreaking (iOS)

Jailbreaking (iOS)

Rooting (Android)

Jailbreaking (iOS)
Rooting (Android)

In electronics: to enable use of a consumer electronics product not intended by the manufacturer through the exploitation of software hacks.

Who wants this?

Wii

Wii

PS3

Wii

PS3

PSP

Wii

PS3

PSP

NDS

Wii

PS3

PSP

NDS

etc...

Part 1) Examples

Part 1) Examples

Part 2) Breif History + Modding

Part 1) Examples

Part 2) Breif History + Modding

Part 3) Developing Homebrew

Part 1) Examples

(Hopefully not failing spectacularly...)

Part 2) Breif History + Modding

Tweezer Attack

(Team Twiizers)

Tweezer Attack

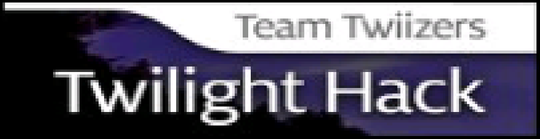
(Team Twiizers)

Obtained private kees from Wii memory to decrypt code from the game disk (I think)

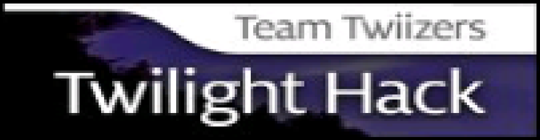
http://tinyurl.com/wii-tweezer

Exploits

Exploits



Exploits



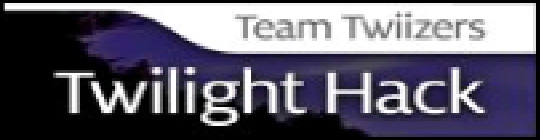
Exploits

Team Twiizers
Twilight Hack

Yu-Gi-OWNED!

bannerbomb

Exploits


Team Twiizers
Twilight Hack

Brawl
Smash
Stack

Yu-Gi-Owned!

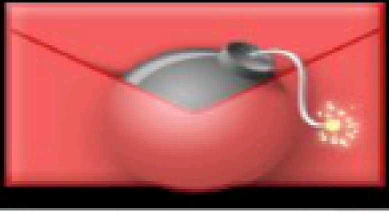
bannerbomb

Exploits

Team Twiizers
Twilight Hack
Brawl
Smash
Stack
Yu-Gi-OWNED!
bannerbomb
Team Twiizers & roto
Return of the Jodi
Team Twiizers
Indiana Pwns

Exploits

Team Twiizers
Twilight Hack

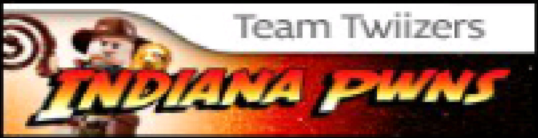


BRAWL
SMASH
STACK

Yu-Gi-OWNED!

bannerbomb

Team Twiizers & roto
RETURN OF THE JODI

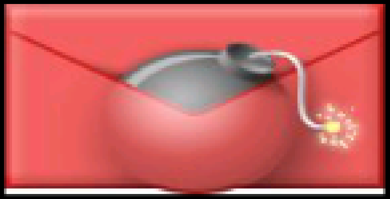

Team Twiizers
INDIANA PWNS

"When the game loads, you will be in Barnett College."

"When the game loads, you will be in Barnett College."
Walk to the Art Room (through the Courtyard),
approach the left character on the podium.

"When the game loads, you will be in Barnett College." Walk to the Art Room (through the Courtyard), approach the left character on the podium. When it zooms on him, choose the switch to option (two silhouettes, staggered, with an arrow pointing between them)."

http://please.hackmii.com



Wii

Is it Legal?

Homebrew vs Nintendo

Part 3) Developing Homebrew

Part 3) Developing Homebrew

1) Get devkitpro toolchain

devkitpro

devkitpro

GNU Compiler Tools...

devkitpro

GNU Compiler Tools...

...and a bunch of libraries and tools

Developing Homebrew

1) Get devkitpro toolchain

2) Setup dev environment

dev environment

dev environment

Copy example folder from devkitpro

dev environment

Copy example folder from devkitpro

Modify Makefile as required

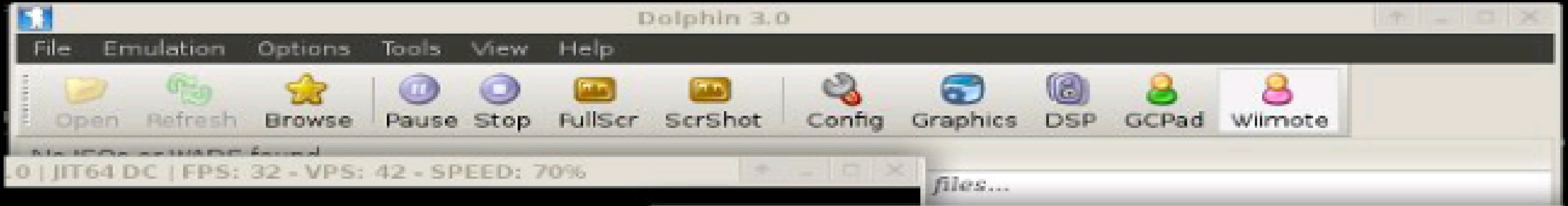
Developing Homebrew

1) Get devkitpro toolchain

2) Setup dev environment

3) Install emulator

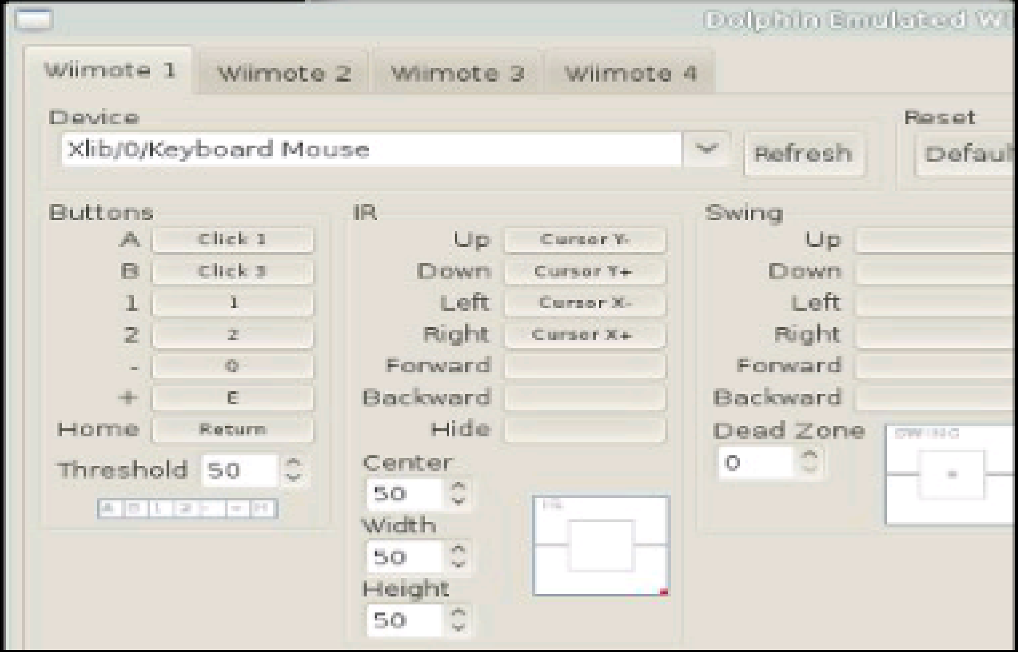
dolphin-emu



No ISOs or WADS found

0 | JIT64 DC | FPS: 32 - VPS: 42 - SPEED: 70%

files...



Device: Xlib/0/Keyboard Mouse

Buttons

A: Click 1
B: Click 3
1: 1
2: 2
-: 0
+: E
Home: Return
Threshold: 50

IR

Up: Cursor Y-
Down: Cursor Y+
Left: Cursor X-
Right: Cursor X+
Forward:
Backward:
Hide:
Center: 50
Width: 50
Height: 50

Swing

Up:
Down:
Left:
Right:
Forward:
Backward:
Dead Zone: 0

Developing Homebrew

1) Get devkitpro toolchain

2) Setup dev environment

Developing Homebrew

1) Get devkitpro toolchain

2) Setup dev environment

3) Install emulator

4) code...

Libraries

Portlibs (from devkitpro)

http://sourceforge.net/projects/devkitpro/files/portlibs/ppc/

Portlibs (from devkitpro)

http://sourceforge.net/projects/devkitpro/files/portlibs/ppc/

libpng / libjpeg

Portlibs (from devkitpro)

http://sourceforge.net/projects/devkitpro/files/portlibs/ppc/

libpng / libjpeg

freetype

zlib

Portlibs (from devkitpro)

http://sourceforge.net/projects/devkitpro/files/portlibs/ppc/

libpng / libjpeg

freetype

zlib

expat

Other Ported libs

http://wiibrew.org/wiki/List_of_development_tools#Ported_Libraries

Other Ported libs

http://wiibrew.org/wiki/List_of_development_tools#Ported_Libraries

SDL

```
screenMode - VIDEO_GetPreferredMode(NULL);
frameBuffer - MEM_K0_TO_K1(SYS_AllocateFramebuffer(screenMode)

VIDEO_Configure(screenMode);
VIDEO_SetNextFramebuffer(frameBuffer);
VIDEO_SetPostRetraceCallback(copy_buffers);
VIDEO_SetBlack(FALSE);
VIDEO_Flush();

fifoBuffer - MEM_K0_TO_K1(memalign(32,FIFO_SIZE));
memset(fifoBuffer, 0, FIFO_SIZE);

GX_Init(fifoBuffer, FIFO_SIZE);
GX_SetCopyClear(backgroundColor, 0x00ffffff);
GX_SetViewport(0,0,screenMode->fbWidth,screenMode->efbHeight,0,
GX_SetDispCopyYScale((f32)screenMode->xfbHeight/(f32)screenMod
GX_SetScissor(0,0,screenMode->fbWidth,screenMode->efbHeight);
GX_SetDispCopySrc(0,0,screenMode->fbWidth,screenMode->efbHeig
GX_SetDispCopyDst(screenMode->fbWidth,screenMode->xfbHeight);
GX_SetCopyFilter(screenMode->aa,screenMode->sample_pattern,GX_
GX_SetFieldMode(screenMode->field_rendering,((screenMode->viHeig

GX_SetCullMode(GX_CULL_NONE);
GX_CopyDisp(frameBuffer,GX_TRUE);
GX_SetDispCopyGamma(GX_GM_1_0);
...
```

```
SDL_Init( SDL_INIT_VIDEO )
atexit( SDL_Quit );
SDL_ShowCursor( SDL_DISABLE );
SDL_SetVideoMode( 640, 480, 16, SDL_DOUBLEBUF | SDL_HWSURFAC
```

Other Ported libs

http://wiibrew.org/wiki/List_of_development_tools#Ported_Libraries

SDL

Box2D / Bullet

Other Ported libs

http://wiibrew.org/wiki/List_of_development_tools#Ported_Libraries

SDL

Box2D / Bullet

etc...

Native Wii libs

Native Wii libs

libmii

Native Wii libs

libmii

libwiigui

Native Wii libs

libmii

libwiigui

libwiisprite

Native Wii libs

libmii

libwiigui

libwiisprite

etc...

GX

```
guMtxIdentity(model);
guMtxTransApply(model, model, -1.5f,0.0f,-6.0f);
guMtxConcat(view,model,modelview);
GX_LoadPosMtxImm(modelview, GX_PNMTX0);

GX_Begin(GX_TRIANGLES, GX_VTXFMT0, 3);
    GX_Position3f32( 0.0f, 1.0f, 0.0f);
    GX_Position3f32(-1.0f,-1.0f, 0.0f);
    GX_Position3f32( 1.0f,-1.0f, 0.0f);
GX_End();
```

```
glLoadIdentity();
glTranslatef(-1.5f,0.0f,-6.0f);



glBegin(GL_TRIANGLES);
    glVertex3f( 0.0f, 1.0f, 0.0f);
    glVertex3f(-1.0f,-1.0f, 0.0f);
    glVertex3f( 1.0f,-1.0f, 0.0f);
glEnd();
```

Debugging

Debugging

GDB over USB

USB Gecko

Debugging

GDB over USB

USB Gecko

discontinued...

Debugging

GDB over WiFi

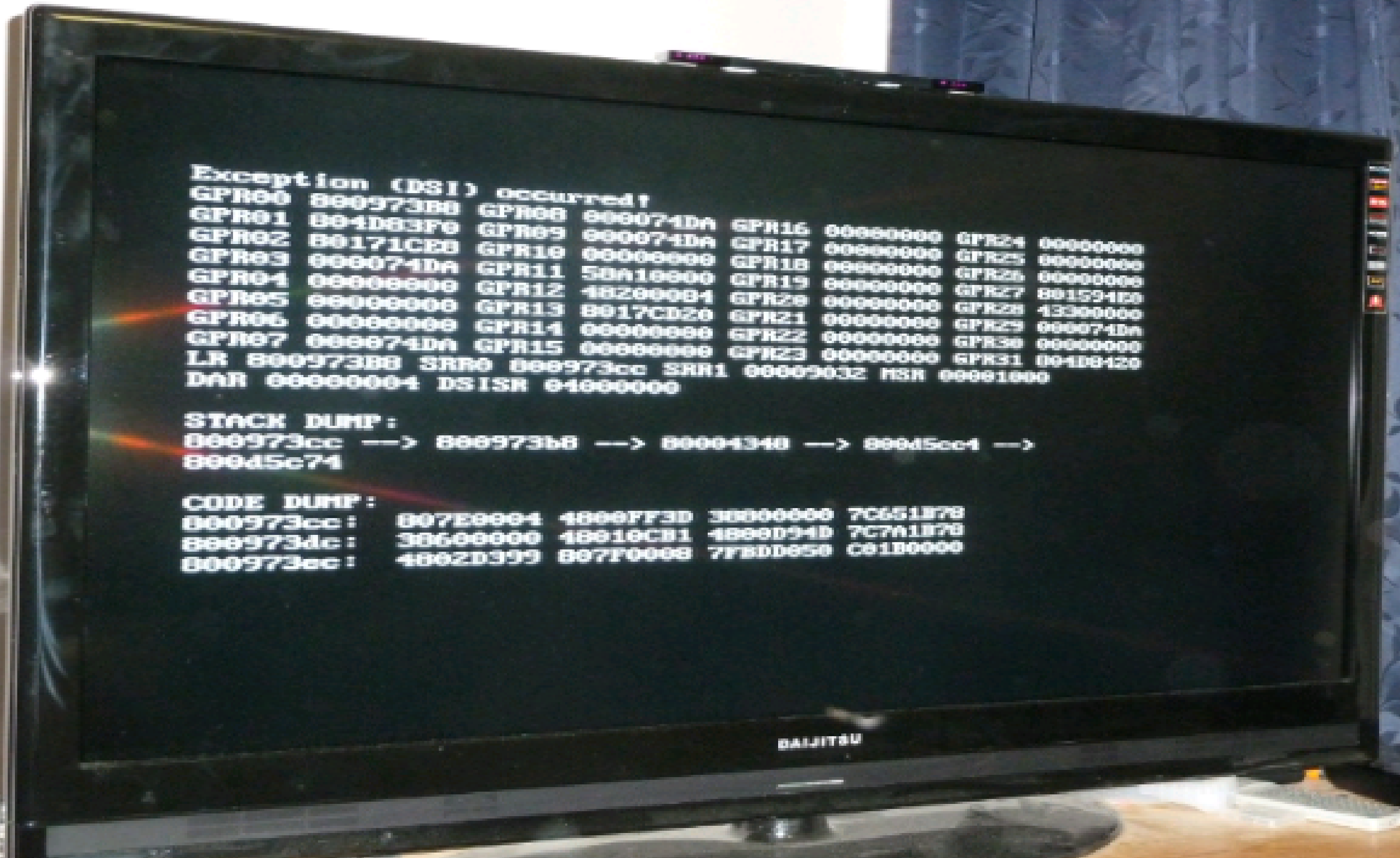
Debugging

printf() + binary search

dolphin-emu outputs to console

Debugging

```
exit(0)
```



```
Exception (DSI) occurred!
GPR00 800973B8 GPR08 000074DA GPR16 00000000 GPR24 00000000
GPR01 804D83F0 GPR09 000074DA GPR17 00000000 GPR25 00000000
GPR02 80171CE0 GPR10 00000000 GPR18 00000000 GPR26 00000000
GPR03 000074DA GPR11 58A10000 GPR19 00000000 GPR27 80159480
GPR04 00000000 GPR12 48200004 GPR20 00000000 GPR28 43300000
GPR05 00000000 GPR13 8017CD20 GPR21 00000000 GPR29 000074DA
GPR06 00000000 GPR14 00000000 GPR22 00000000 GPR30 00000000
GPR07 000074DA GPR15 00000000 GPR23 00000000 GPR31 804D8420
LR 800973B8 SRR0 800973cc SRR1 00009032 MSR 00001000
DAR 00000004 DSISR 04000000

STACK DUMP:
800973cc --> 800973b8 --> 80004340 --> 800d5cc4 -->
800d5c74

CODE DUMP:
800973cc:  807E0004 4800FF3D 38000000 7C651B78
800973dc:  38600000 48010CB1 4800D94D 7C7A1B78
800973ec:  4802D399 807F0008 7FBDD050 C81B0000
```

wiibrew.org

devkitpro.org