Video game hacking:

Breaking games and protecting ours

Lucas PARSY

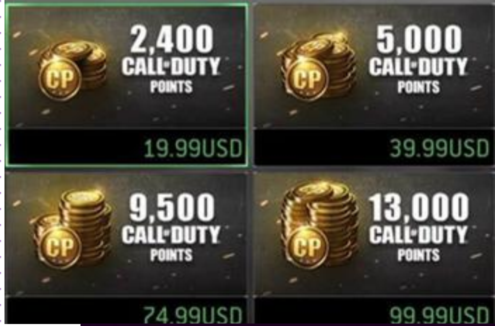
1

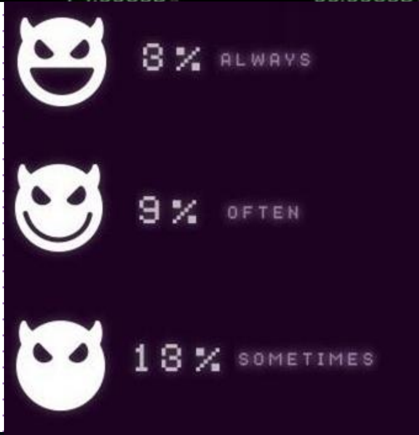
Overview of game hacking

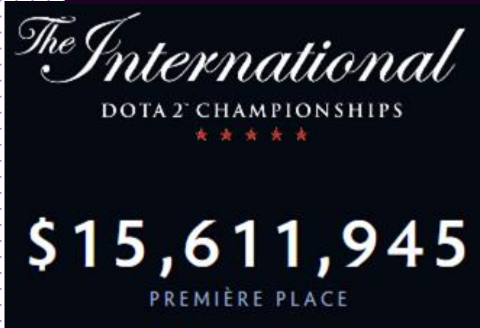
You know the rules and so do I

Serious Games

- 76 billions $ microtransactions in 2023
- 1 billion online games players
  37% admitted having cheated
- Competitions with enormous cashprizes







A whole world of video game hacks

Assets Extraction

ILSpy

Decompilation

Ghidra

Obfuscation

RenderDoc

GPU API

CE Autoassembler

Hooking

DLL Injection

Frida

Unity Explorer

Anti-cheat Bypass

Code Filter

Value detection

Memory scan

Debugging

Cheat Engine

Server checks

Multiplayer Pwn

Network interception

Burp

Message encryption

Registry Edit

System Slowdown

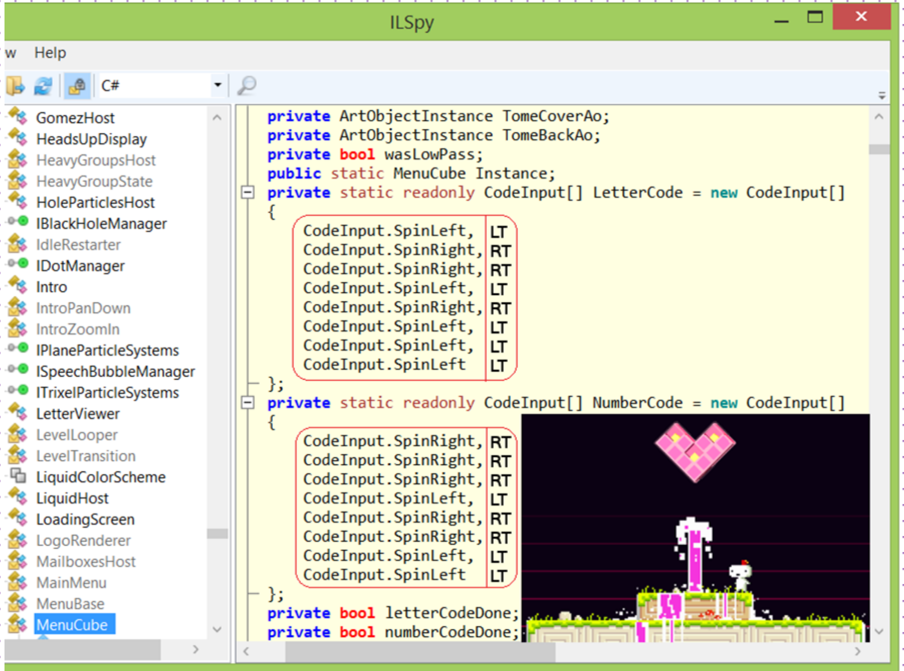
System edits

Clock modification

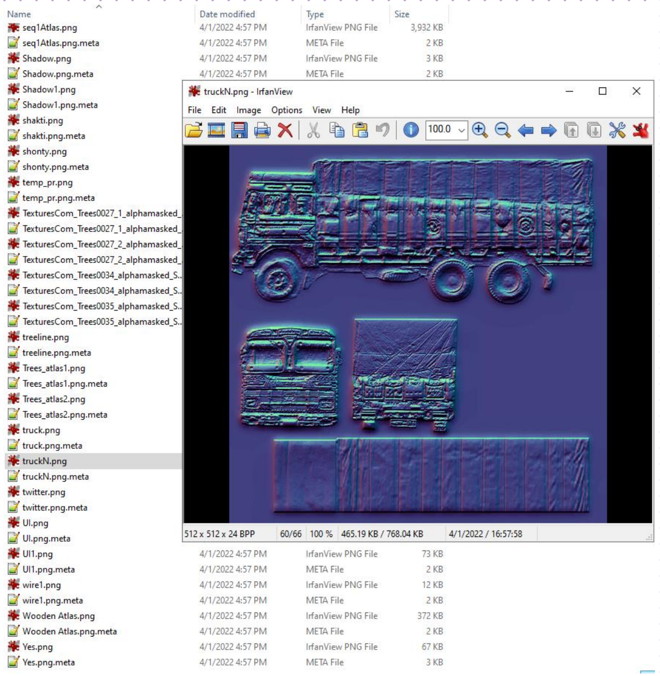
Savefile edit

A whole world of video game hacks

Unpack/ source code decompilation



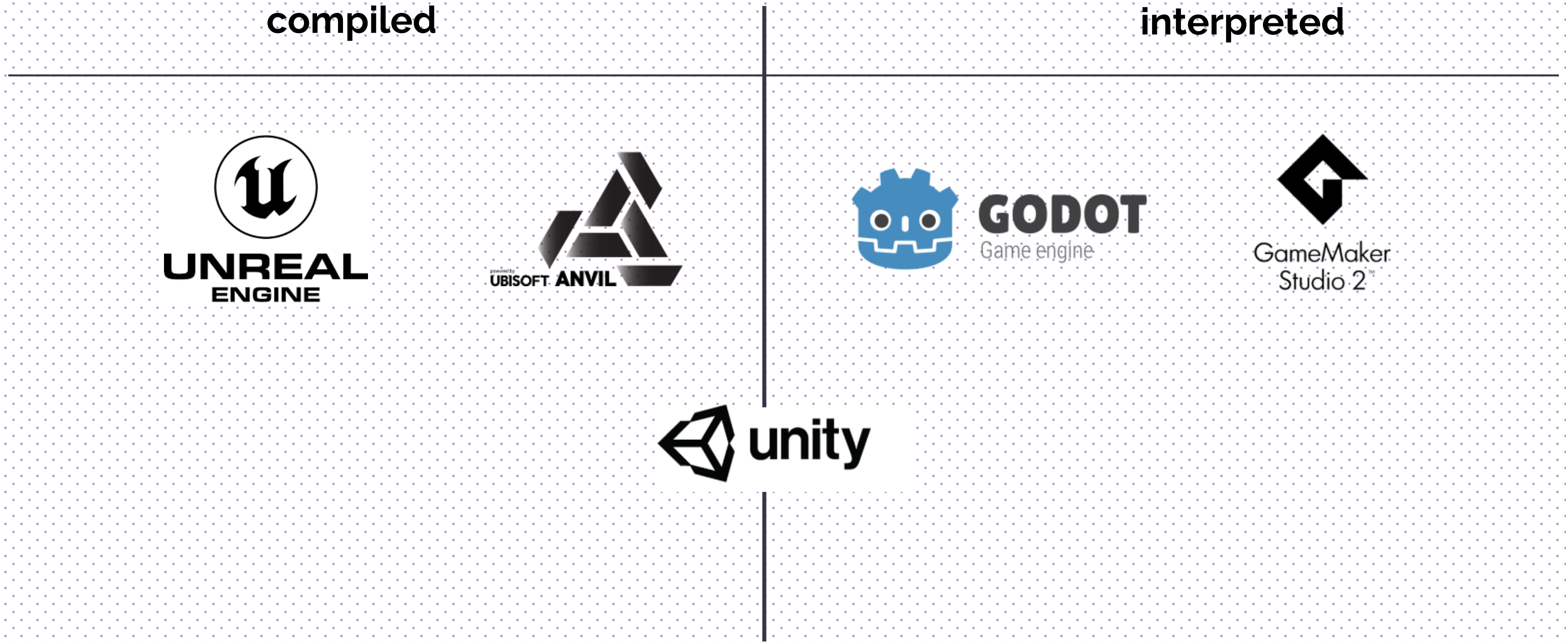
```
private ArtObjectInstance TomeCoverAo;
private ArtObjectInstance TomeBackAo;
private bool wasLowPass;
public static MenuCube Instance;
private static readonly CodeInput[] LetterCode = new CodeInput[]
{
    CodeInput.SpinLeft,   LT
    CodeInput.SpinRight,  RT
    CodeInput.SpinRight,  RT
    CodeInput.SpinLeft,   LT
    CodeInput.SpinRight,  RT
    CodeInput.SpinLeft,   LT
    CodeInput.SpinLeft,   LT
    CodeInput.SpinLeft    LT
};
private static readonly CodeInput[] NumberCode = new CodeInput[]
{
    CodeInput.SpinRight,  RT
    CodeInput.SpinRight,  RT
    CodeInput.SpinRight,  RT
    CodeInput.SpinLeft,   LT
    CodeInput.SpinRight,  RT
    CodeInput.SpinRight,  RT
    CodeInput.SpinLeft,   LT
    CodeInput.SpinLeft    LT
};
private bool letterCodeDone;
private bool numberCodeDone;
```



Name	Date modified	Type	Size
seq1Atlas.png	4/1/2022 4:57 PM	IrfanView PNG File	3,932 KB
seq1Atlas.png.meta	4/1/2022 4:57 PM	META File	2 KB
Shadow.png	4/1/2022 4:57 PM	IrfanView PNG File	3 KB
Shadow.png.meta	4/1/2022 4:57 PM	META File	2 KB
Shadow1.png			
Shadow1.png.meta			
shakti.png			
shakti.png.meta			
shonty.png			
shonty.png.meta			
temp_pr.png			
temp_pr.png.meta			
TexturesCom_Trees0027_1_alphamasked_			
TexturesCom_Trees0027_1_alphamasked_			
TexturesCom_Trees0027_2_alphamasked_			
TexturesCom_Trees0027_2_alphamasked_			
TexturesCom_Trees0034_alphamasked_S...			
TexturesCom_Trees0034_alphamasked_S...			
TexturesCom_Trees0035_alphamasked_S...			
TexturesCom_Trees0035_alphamasked_S...			
treeline.png			
treeline.png.meta			
Trees_atlas1.png			
Trees_atlas1.png.meta			
Trees_atlas2.png			
Trees_atlas2.png.meta			
truck.png			
truck.png.meta			
truckN.png			
truckN.png.meta			
twitter.png			
twitter.png.meta			
UI.png			
UI.png.meta			
UI1.png	4/1/2022 4:57 PM	IrfanView PNG File	73 KB
UI1.png.meta	4/1/2022 4:57 PM	META File	2 KB
wire1.png	4/1/2022 4:57 PM	IrfanView PNG File	12 KB
wire1.png.meta	4/1/2022 4:57 PM	META File	2 KB
Wooden Atlas.png	4/1/2022 4:57 PM	IrfanView PNG File	372 KB
Wooden Atlas.png.meta	4/1/2022 4:57 PM	META File	2 KB
Yes.png	4/1/2022 4:57 PM	IrfanView PNG File	67 KB
Yes.png.meta	4/1/2022 4:57 PM	META File	3 KB

A whole world of video game hacks

Unpack/ source code decompilation



A whole world of video game hacks

Method hooking

process

FRIDA

```
session = frida.attach("solitaire.exe")
script = session.create_script("""
   Interceptor.attach(ptr(FUNCTION_ADDRESS),
   {
      onEnter(args) {
         args[0] = ptr("1337");
      }
   });
""")
```

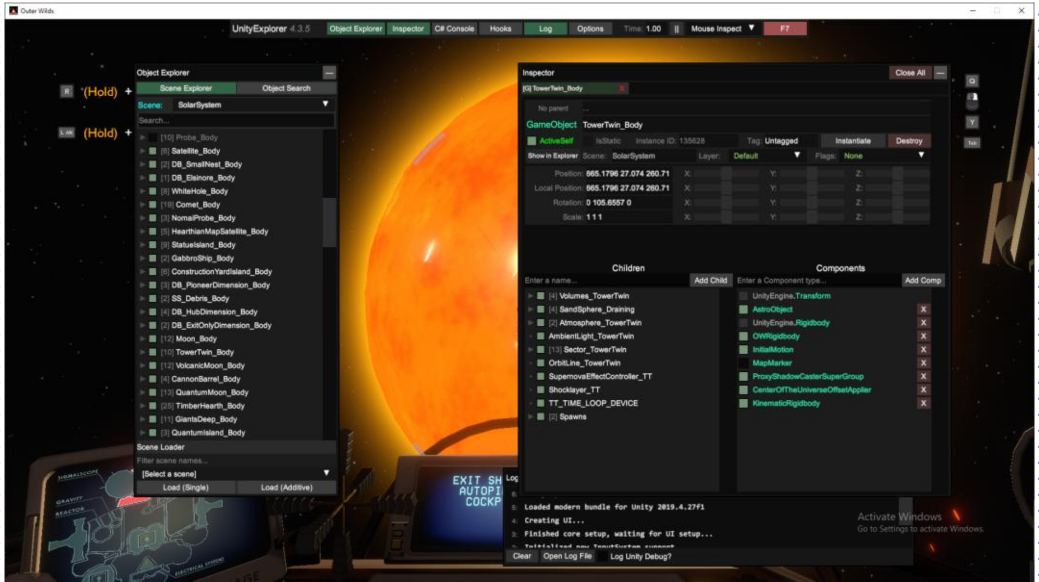
A whole world of video game hacks

Method hooking

Game Engine

process

BepInEx / MelonLoader



Scene: SolarSystem

- [10] Probe_Body
- [6] Satellite_Body
- [2] DB_SmallNest_Body
- [1] DB_Elsinore_Body
- [8] WhiteHole_Body
- [19] Comet_Body
- [3] NomaiProbe_Body
- [5] HearthianMapSatellite_Body
- [9] StatueIsland_Body
- [2] GabbroShip_Body
- [6] ConstructionYardIsland_Body
- [3] DB_PioneerDimension_Body
- [2] SS_Debris_Body
- [4] DB_HubDimension_Body
- [2] DB_ExitOnlyDimension_Body
- [12] Moon_Body
- [10] TowerTwin_Body
- [12] VolcanicMoon_Body
- [4] CannonBarrel_Body
- [13] QuantumMoon_Body
- [25] TimberHearth_Body
- [11] GiantsDeep_Body
- [3] QuantumIsland_Body

[G] TowerTwin_Body

No parent ...

GameObject TowerTwin_Body

ActiveSelf IsStatic Instance ID: 135628 Tag: Untagged

Show in Explorer Scene: SolarSystem Layer: Default Flags: None

Position: 665.1796 27.074 260.71 X: Y: Z:
Local Position: 665.1796 27.074 260.71 X: Y: Z:
Rotation: 0 105.6557 0 X: Y: Z:
Scale: 1 1 1 X: Y: Z:

Children:

- [4] Volumes_TowerTwin
- [4] SandSphere_Draining
- [2] Atmosphere_TowerTwin
- AmbientLight_TowerTwin
- [13] Sector_TowerTwin
- OrbitLine_TowerTwin
- SupernovaEffectController_TT
- Shocklayer_TT
- TT_TIME_LOOP_DEVICE
- [2] Spawns

Components:

- UnityEngine.Transform
- AstroObject X
- UnityEngine.Rigidbody X
- OWRigidbody X
- InitialMotion X
- MapMarker X
- ProxyShadowCasterSuperGroup X
- CenterOfTheUniverseOffsetApplier X
- KinematicRigidbody X

Log

```
6:
5: Loaded modern bundle for Unity 2019.4.27f1
4: Creating UI...
3: Finished core setup, waiting for UI setup...
```

A whole world of video game hacks

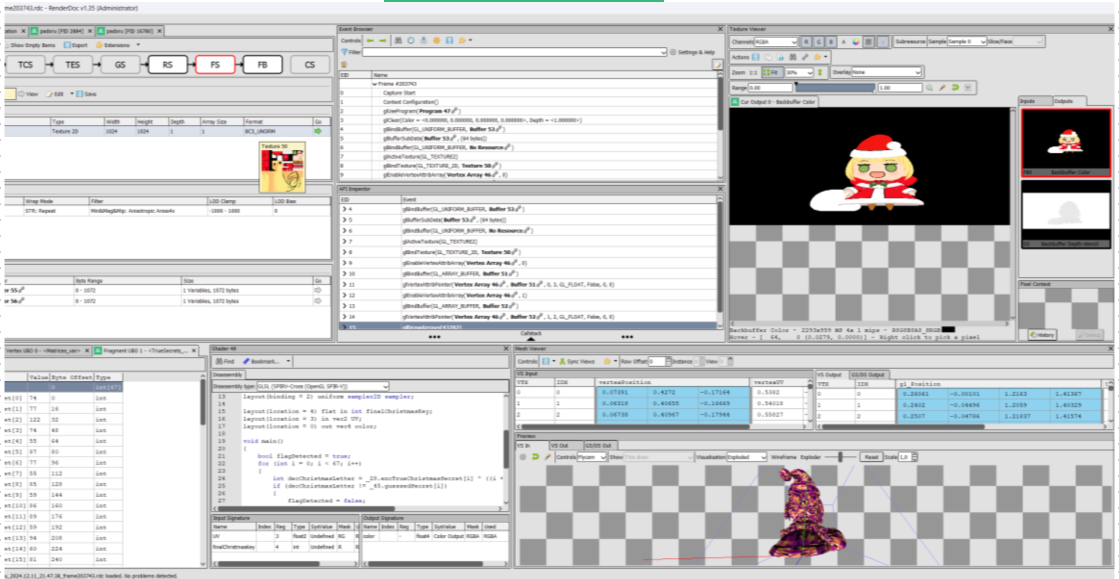
Method hooking

Game Engine

GPU Render

process

RenderDoc

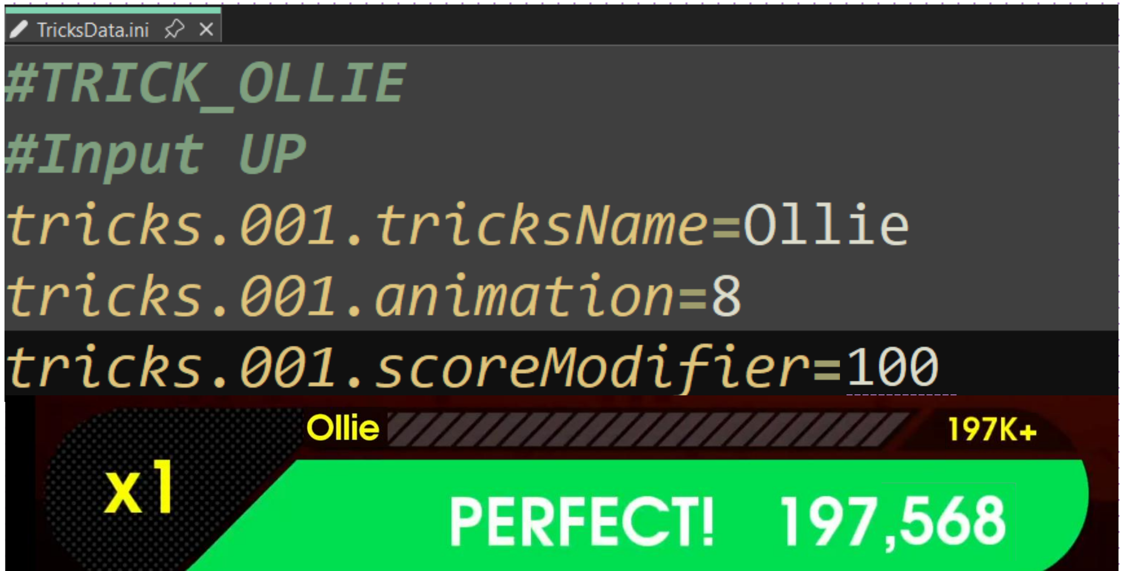


```
layout(binding = 2) uniform sampler2D sampler;

layout(location = 4) flat in int finalChristmasKey;
layout(location = 3) in vec2 UV;
layout(location = 0) out vec4 color;

void main()
{
    bool flagDetected = true;
    for (int i = 0; i < 67; i++)
    {
        int decChristmasLetter = _28.encTrueChristmasSecret[i] ^ ((i +
        if (decChristmasLetter != _45.guessedSecret[i])
        {
            flagDetected = false;
```

```
EID  Name
     Frame #203743
0    Capture Start
1    Context Configuration()
2    glUseProgram(Program 47)
3    glClear(Color = <0.000000, 0.000000, 0.000000, 0.000000>, Depth = <1.000000>)
4    glBindBuffer(GL_UNIFORM_BUFFER, Buffer 53)
5    glBufferSubData(Buffer 53, (64 bytes))
6    glBindBuffer(GL_UNIFORM_BUFFER, No Resource)
7    glActiveTexture(GL_TEXTURE2)
8    glBindTexture(GL_TEXTURE_2D, Texture 50)
9    glEnableVertexAttribArray(Vertex Array 46, 0)
```

A whole world of video game hacks

save games and config files editing


TricksData.ini

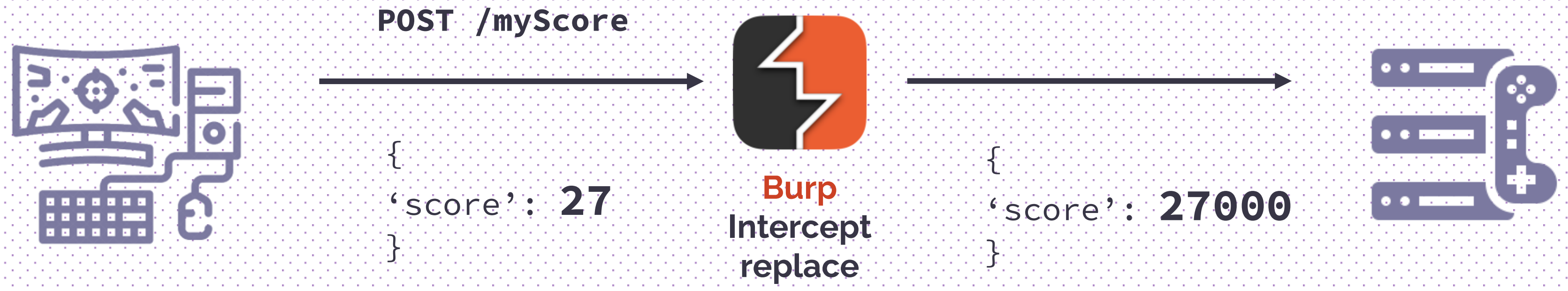
```
#TRICK_OLLIE
#Input UP
tricks.001.tricksName=Ollie
tricks.001.animation=8
tricks.001.scoreModifier=100
```

Procmon64

Finds files/registry keys used by a process

A whole world of video game hacks

Interception/modification of network packets



A whole world of video game hacks

Interception/modification of network packets

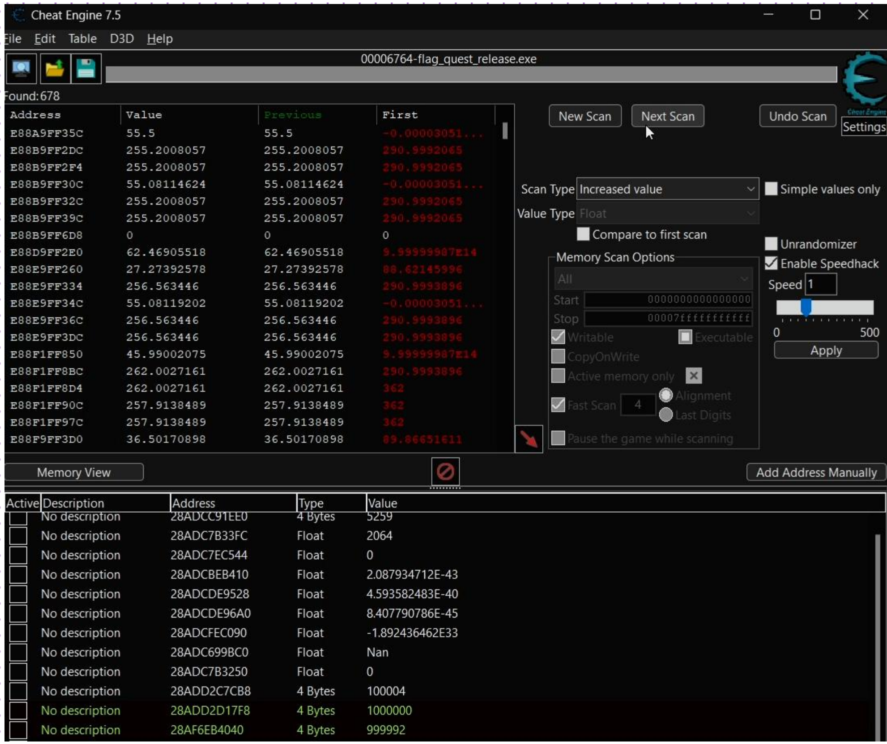
2

Hacking games with CheatEngine

"It's pronounced Aine jean"

Cheat Engine

- Memory scanner and debugger



Found:678

Address	Value	Previous	First
E88A9FF35C	55.5	55.5	-0.00003051...
E88B9FF2DC	255.2008057	255.2008057	290.9992065
E88B9FF2F4	255.2008057	255.2008057	290.9992065
E88B9FF30C	55.08114624	55.08114624	-0.00003051...
E88B9FF32C	255.2008057	255.2008057	290.9992065
E88B9FF39C	255.2008057	255.2008057	290.9992065
E88B9FF6D8	0	0	0
E88D9FF2E0	62.46905518	62.46905518	9.99999987E14
E88E9FF260	27.27392578	27.27392578	88.62145996
E88E9FF334	256.563446	256.563446	290.9993896
E88E9FF34C	55.08119202	55.08119202	-0.00003051...
E88E9FF36C	256.563446	256.563446	290.9993896
E88E9FF3DC	256.563446	256.563446	290.9993896
E88F1FF850	45.99002075	45.99002075	9.99999987E14
E88F1FF8BC	262.0027161	262.0027161	290.9993896
E88F1FF8D4	262.0027161	262.0027161	362
E88F1FF90C	257.9138489	257.9138489	362
E88F1FF97C	257.9138489	257.9138489	362
E88F9FF3D0	36.50170898	36.50170898	89.86651611

Scan Type: Increased value
Value Type: Float
Compare to first scan: ☐
Simple values only: ☐
Unrandomizer: ☐
Enable Speedhack: ✓
Speed: 1 (0 – 500) Apply

Memory Scan Options: All
Start: 0000000000000000
Stop: 00007fffffffffff
Writable: ✓ Executable: ☐
CopyOnWrite: ☐
Active memory only: ☐
Fast Scan: ✓ 4 — Alignment / Last Digits
Pause the game while scanning: ☐

Active	Description	Address	Type	Value
☐	No description	28ADCC91EE0	4 Bytes	5259
☐	No description	28ADC7B33FC	Float	2064
☐	No description	28ADC7EC544	Float	0
☐	No description	28ADCBEB410	Float	2.087934712E-43
☐	No description	28ADCDE9528	Float	4.593582483E-40
☐	No description	28ADCDE96A0	Float	8.407790786E-45
☐	No description	28ADCFEC090	Float	-1.892436462E33
☐	No description	28ADC699BC0	Float	Nan
☐	No description	28ADC7B3250	Float	0
☐	No description	28ADD2C7CB8	4 Bytes	100004
☐	No description	28ADD2D17F8	4 Bytes	1000000
☐	No description	28AF6EB4040	4 Bytes	999992

Cheat Engine

- Memory scanner and debugger
- **AutoAssembly and LUA scripting**

```
Hook :
retGetGamePlayers_o:
readmem( retGetGamePlayers, 6 )
mov [LocalPlayer],rax
mov rcx, [rax+30]
test rcx,rcx
je short @f
    mov [OakPlayerController],rcx
    mov rcx, [rcx+488]
    test rcx, rcx
        je short @f
        mov rcx, [rax+30]
        mov rcx, [rcx+1988]
        test rcx,rcx
        je short @f
            mov [OakDeveloperPerks],rcx
            test byte ptr [rcx+C8],40
            jne short @f
                or byte ptr [rcx+C8],40

@@:
jmp retGetGamePlayers+6
```

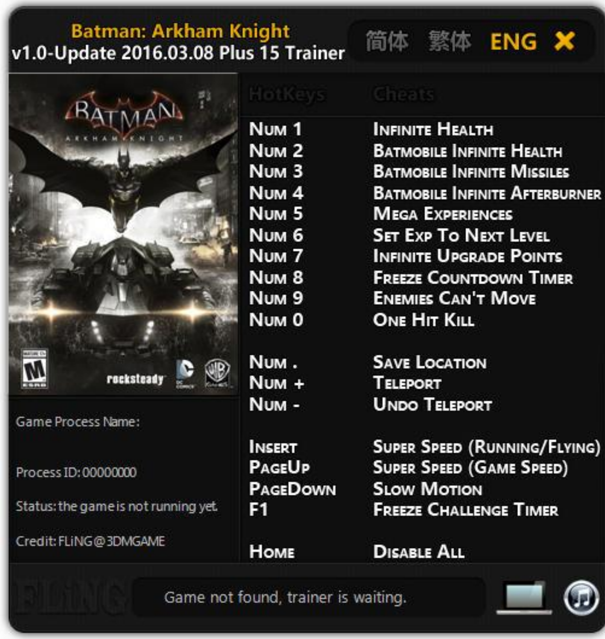
Cheat Engine

- Memory scanner and debugger
- **AutoAssembly and LUA scripting**

```
function AOBScanAA(script, symbol)
  local success,disableInfo = autoAssemble(script)
  if not success then return nil, disableInfo end -- disab
  local addr = getAddress(symbol)
  autoAssemble(script, disableInfo) -- disable script and
  return addr, 'success'
end

function AOBScanRegion(bytestr, start, stop)
  local script = ([[
  [ENABLE]
  aobscanregion(luaAOBScanRegionSymbol,%X,%X,%s)
  registersymbol(luaAOBScanRegionSymbol)
  [DISABLE]
  unregistersymbol(luaAOBScanRegionSymbol)
  ]]):format(getAddress(start), getAddress(stop), bytestr)
  return AOBScanAA(script, 'luaAOBScanRegionSymbol')
end

function AOBScanModule(bytestr, module)
  local script = ([[
  [ENABLE]
  aobscanmodule(luaAOBScanModuleSymbol,%s,%s)
  registersymbol(luaAOBScanModuleSymbol)
  [DISABLE]
  unregistersymbol(luaAOBScanModuleSymbol)
  ]]):format(module, bytestr)
  return AOBScanAA(script,'luaAOBScanModuleSymbol')
end
```

Cheat Engine

- Memory scanner and debugger
- AutoAssembly and LUA scripting
- **GUI ‘trainer’ generator**


Batman: Arkham Knight
v1.0-Update 2016.03.08 Plus 15 Trainer

简体 繁体 ENG

HotKeys	Cheats
Num 1	Infinite Health
Num 2	Batmobile Infinite Health
Num 3	Batmobile Infinite Missiles
Num 4	Batmobile Infinite Afterburner
Num 5	Mega Experiences
Num 6	Set Exp To Next Level
Num 7	Infinite Upgrade Points
Num 8	Freeze Countdown Timer
Num 9	Enemies Can't Move
Num 0	One Hit Kill
Num .	Save Location
Num +	Teleport
Num -	Undo Teleport
Insert	Super Speed (Running/Flying)
PageUp	Super Speed (Game Speed)
PageDown	Slow Motion
F1	Freeze Challenge Timer
Home	Disable All

Game Process Name:

Process ID: 00000000

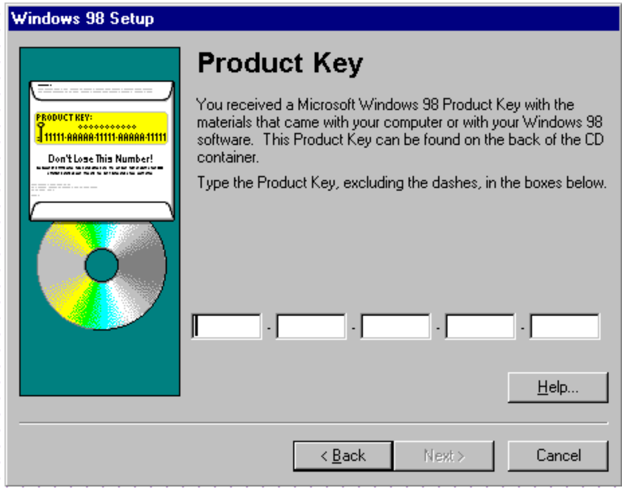
Status: the game is not running yet.

Credit: FLiNG@3DMGAME

Game not found, trainer is waiting.

CheatEngine

- Memory scanner and debugger
- AutoAssembly and LUA scripting
- GUI ‘trainer’ generator
- **Not limited to video games**

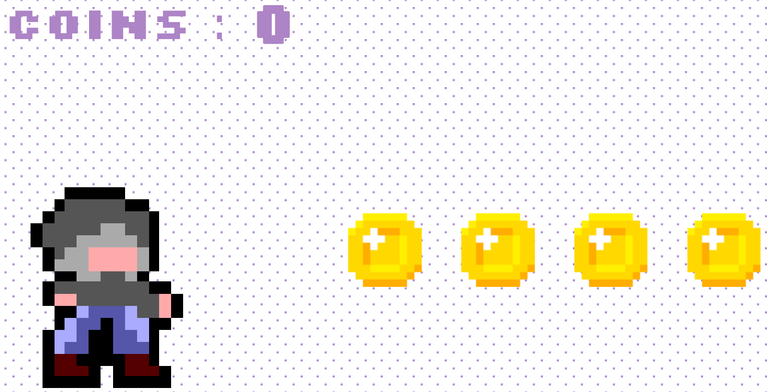

Windows 98 Setup

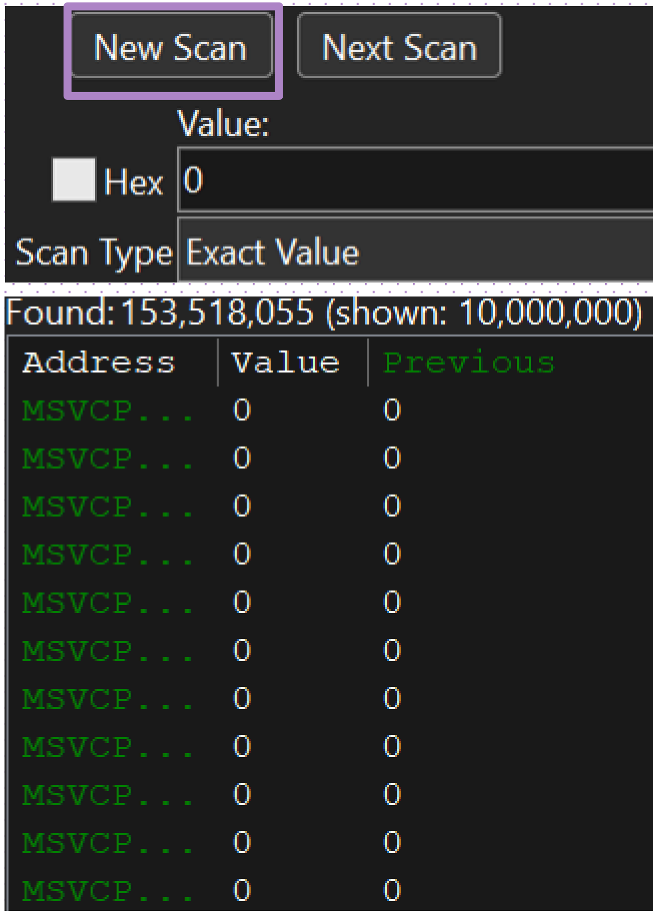
Product Key

You received a Microsoft Windows 98 Product Key with the materials that came with your computer or with your Windows 98 software. This Product Key can be found on the back of the CD container.

Type the Product Key, excluding the dashes, in the boxes below.

Finding values



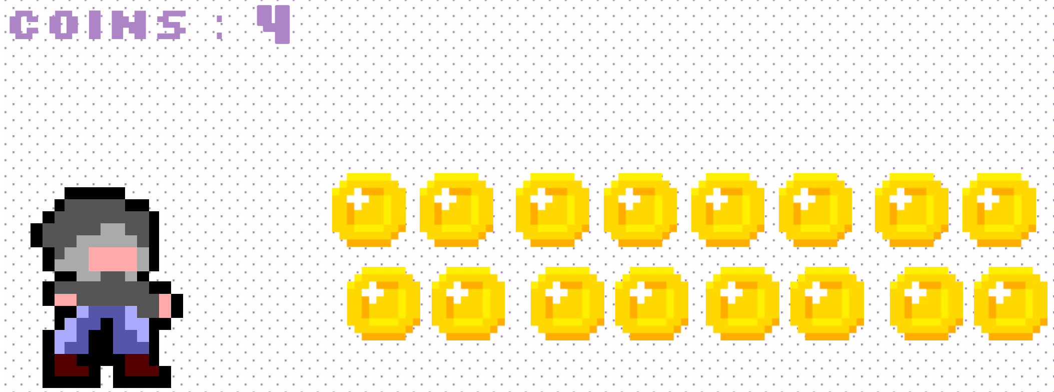


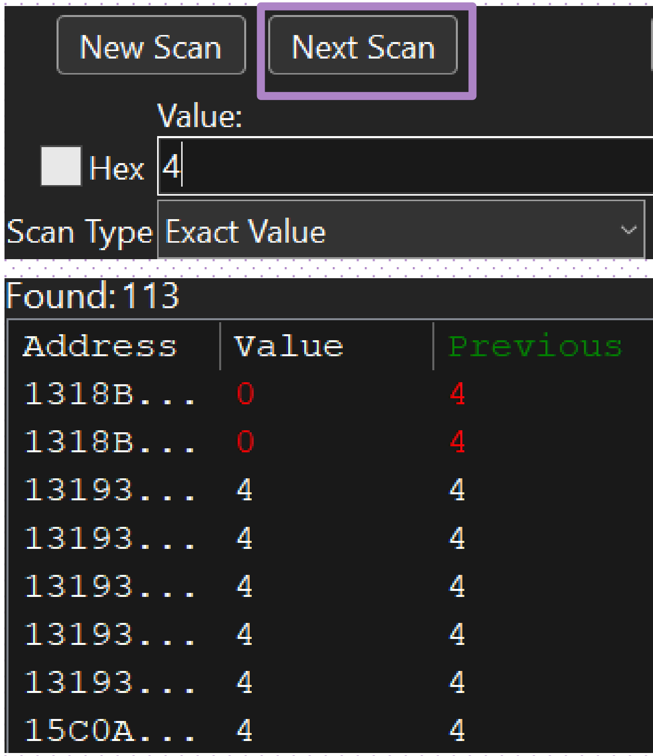
Value:
0
Scan Type Exact Value

Found: 153,518,055 (shown: 10,000,000)

```
Address      Value    Previous
MSVCP...     0        0
MSVCP...     0        0
MSVCP...     0        0
MSVCP...     0        0
MSVCP...     0        0
MSVCP...     0        0
MSVCP...     0        0
MSVCP...     0        0
MSVCP...     0        0
MSVCP...     0        0
MSVCP...     0        0
```

Finding values





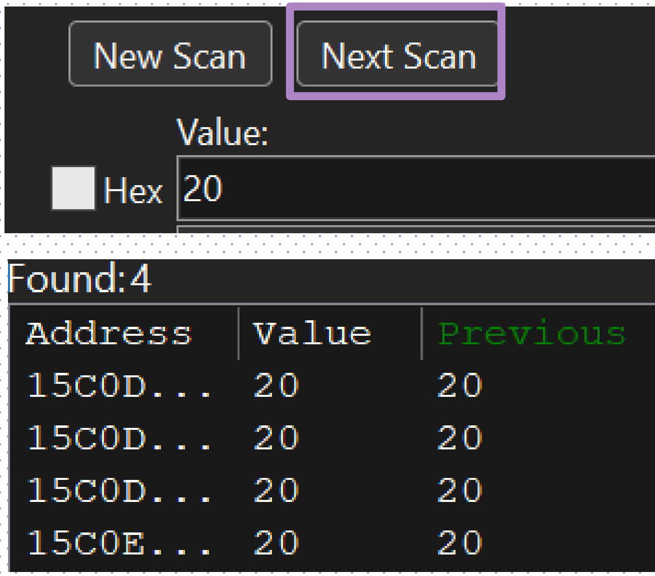
Value: 4

Scan Type Exact Value

Found: 113

```
Address      Value   Previous
1318B...     0       4
1318B...     0       4
13193...     4       4
13193...     4       4
13193...     4       4
13193...     4       4
13193...     4       4
15C0A...     4       4
```

Finding values

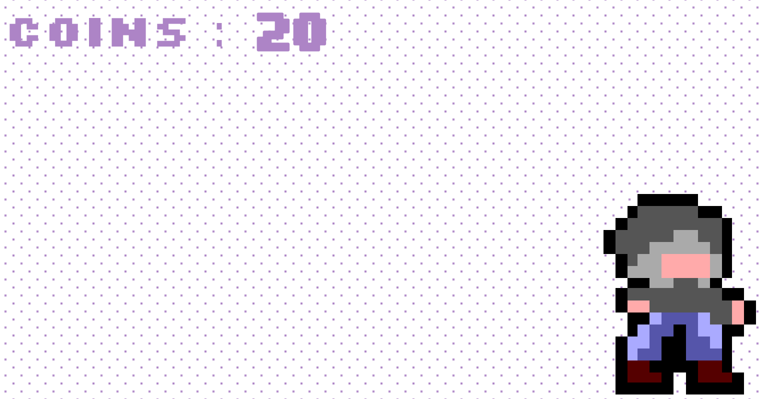


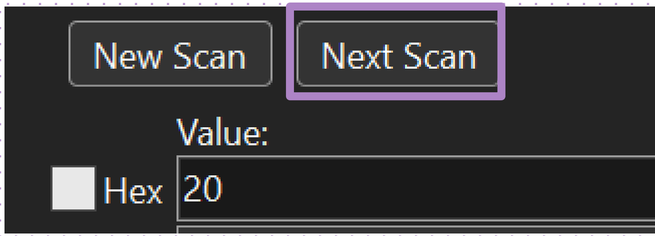
20

Found:4

```
Address      Value     Previous
15C0D...     20        20
15C0D...     20        20
15C0D...     20        20
15C0E...     20        20
```

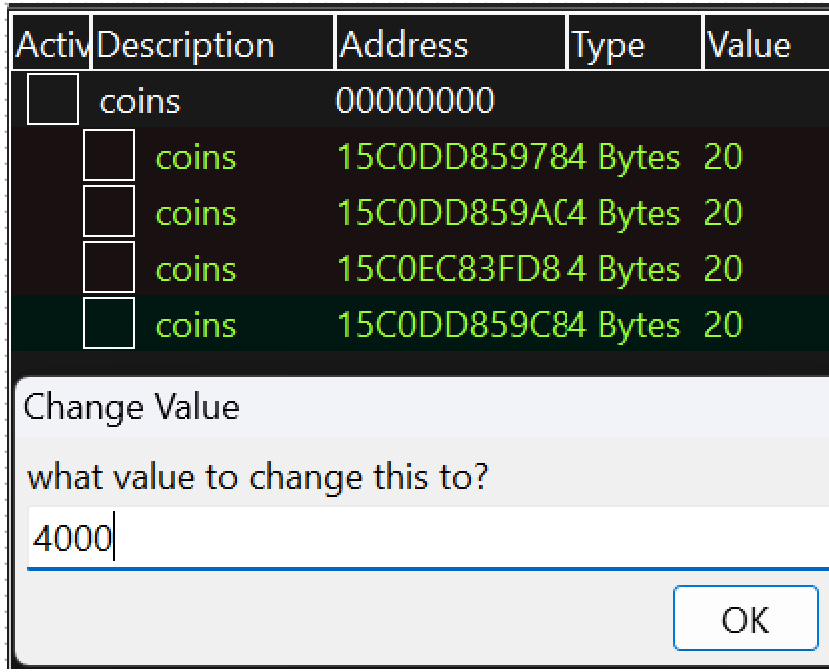
Finding values





Value:

Hex 20



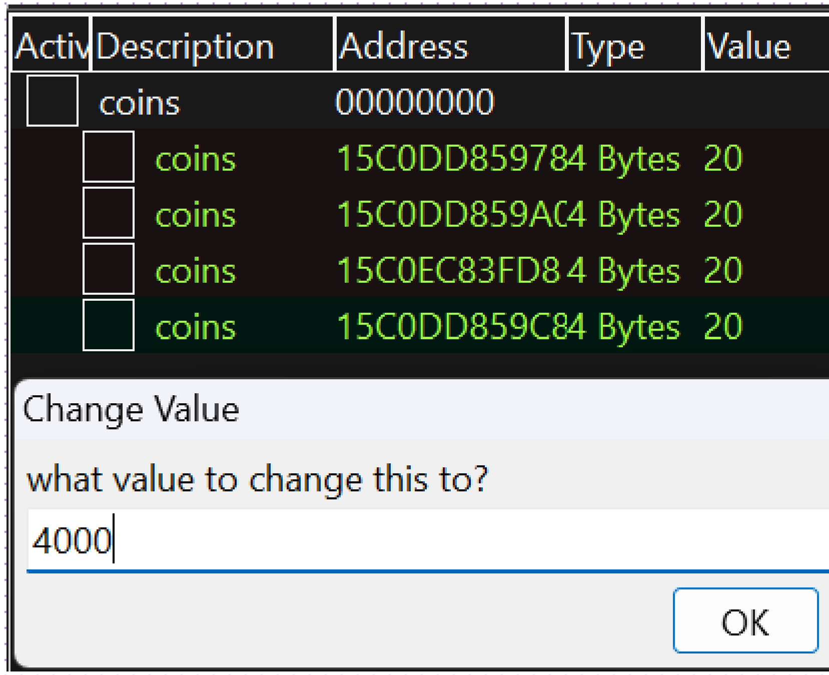
Activ	Description	Address	Type	Value
	coins	00000000		
	coins	15C0DD85978	4 Bytes	20
	coins	15C0DD859AC	4 Bytes	20
	coins	15C0EC83FD8	4 Bytes	20
	coins	15C0DD859C8	4 Bytes	20

Change Value

what value to change this to?

4000

Finding values



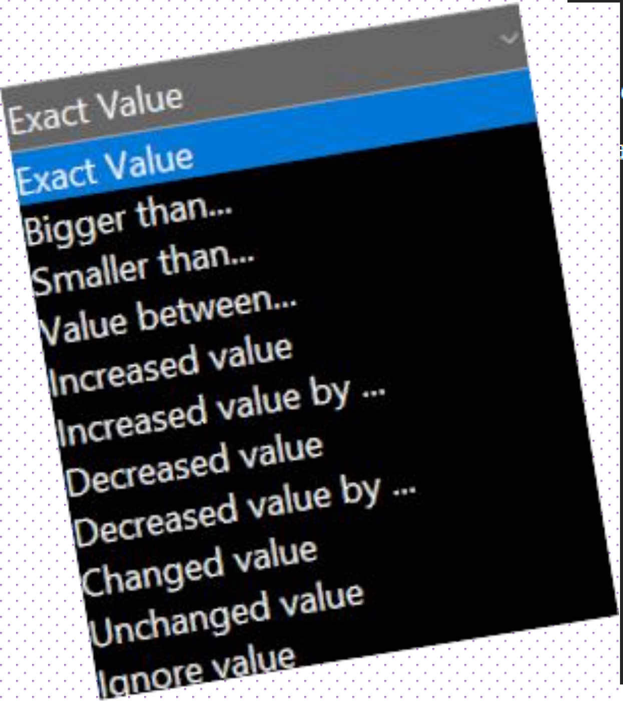
Activ	Description	Address	Type	Value
	coins	00000000		
	coins	15C0DD85978	4 Bytes	20
	coins	15C0DD859AC	4 Bytes	20
	coins	15C0EC83FD8	4 Bytes	20
	coins	15C0DD859C8	4 Bytes	20

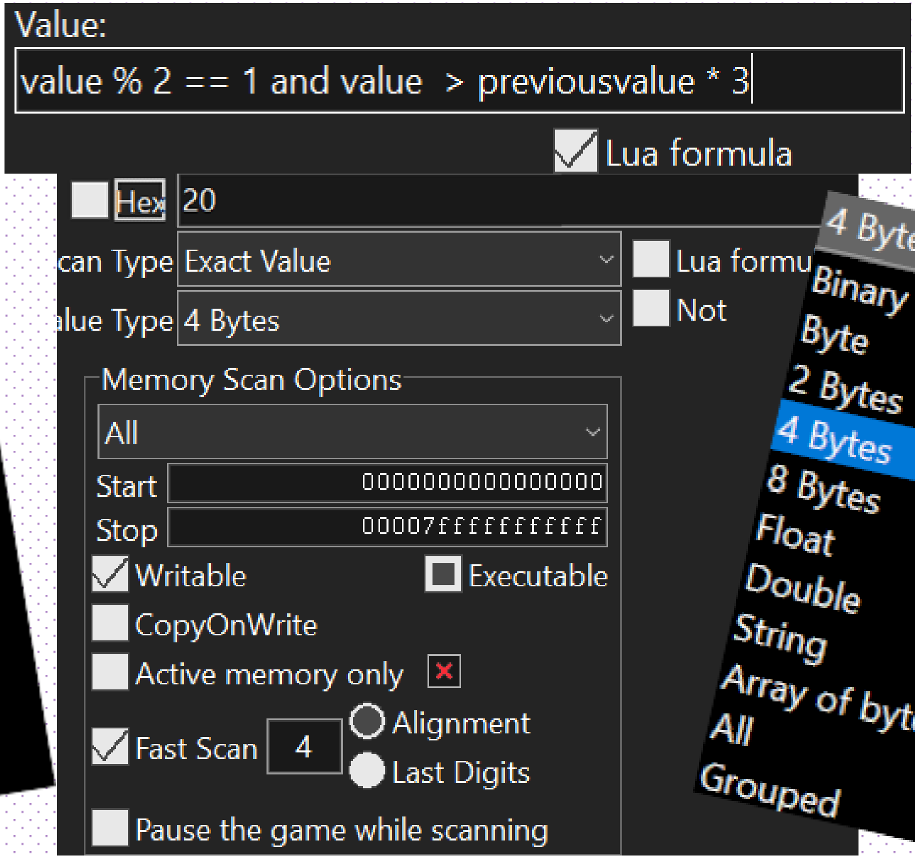
Change Value

what value to change this to?

4000

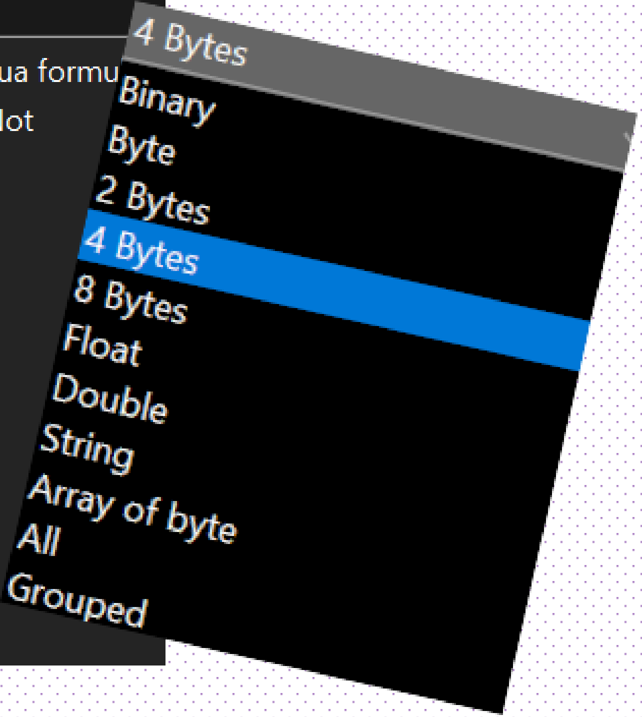
Finding values: advanced features




Value:
value % 2 == 1 and value > previousvalue * 3
[✓] Lua formula

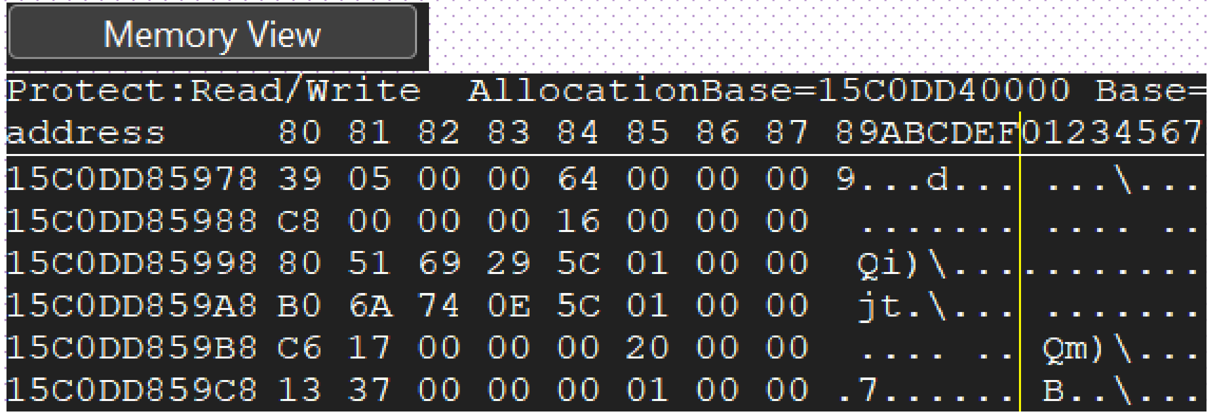
[ ] Hex 20
can Type Exact Value [ ] Lua formu
alue Type 4 Bytes [ ] Not

Memory Scan Options
All
Start 0000000000000000
Stop 00007fffffffffff
[✓] Writable [■] Executable
[ ] CopyOnWrite
[ ] Active memory only
[✓] Fast Scan 4 ( ) Alignment (●) Last Digits
[ ] Pause the game while scanning



Memory viewer

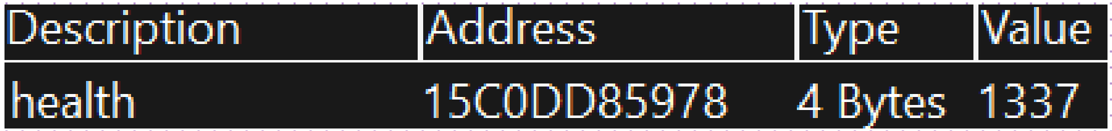
Description	Address	Type	Value
health	15C0DD85978	4 Bytes	1337



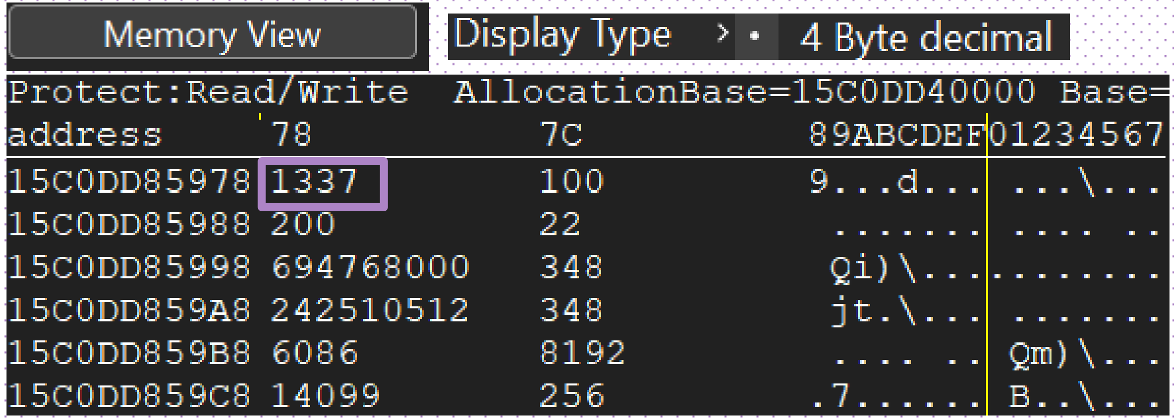
```
Protect:Read/Write  AllocationBase=15C0DD40000 Base=
address         80 81 82 83 84 85 86 87 89ABCDEF01234567
15C0DD85978 39 05 00 00 64 00 00 00 9...d... ...\...
15C0DD85988 C8 00 00 00 16 00 00 00  .......  .... ..
15C0DD85998 80 51 69 29 5C 01 00 00  Qi)\...........
15C0DD859A8 B0 6A 74 0E 5C 01 00 00  jt.\...  .......
15C0DD859B8 C6 17 00 00 00 20 00 00  .... .. Qm)\...
15C0DD859C8 13 37 00 00 00 01 00 00 .7...... B..\...
```

```
struct Player
{
    int health    = 1337;
    int ???       = ???;
    int ???       = ???;
}
```

Memory viewer



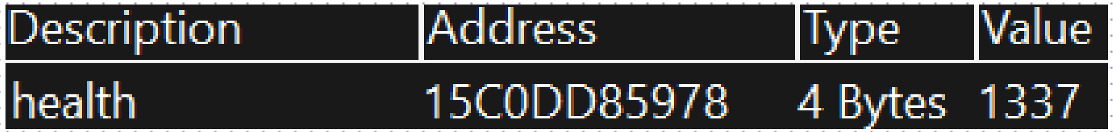
Description	Address	Type	Value
health	15C0DD85978	4 Bytes	1337



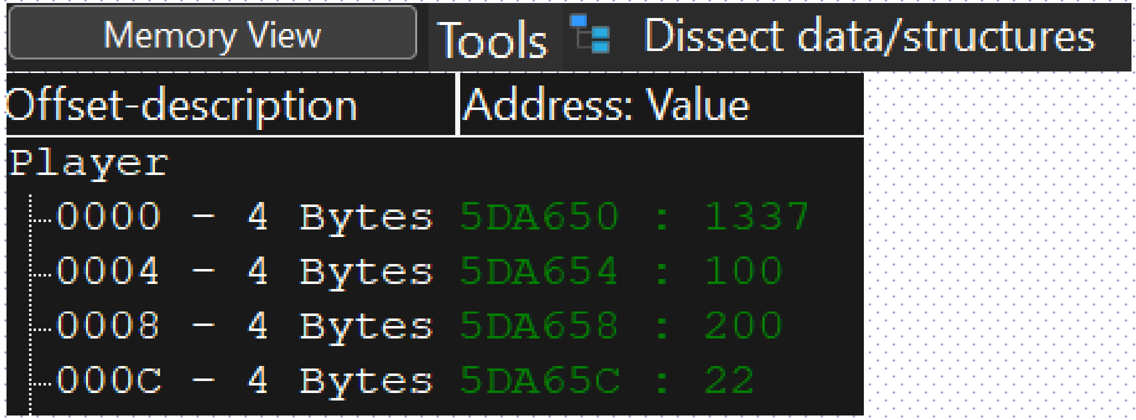
```
Protect:Read/Write  AllocationBase=15C0DD40000 Base=
address      78          7C           89ABCDEF01234567
15C0DD85978 1337         100          9...d... ...\...
15C0DD85988 200          22            ........ .... ..
15C0DD85998 694768000    348           Qi)\...........
15C0DD859A8 242510512    348           jt.\... .......
15C0DD859B8 6086         8192          .... .. Qm)\...
15C0DD859C8 14099        256          .7...... B..\...
```

```
struct Player
{
    int health   = 1337;
    int strength = 100;
    int defense  = 200;
}
```

Data structures



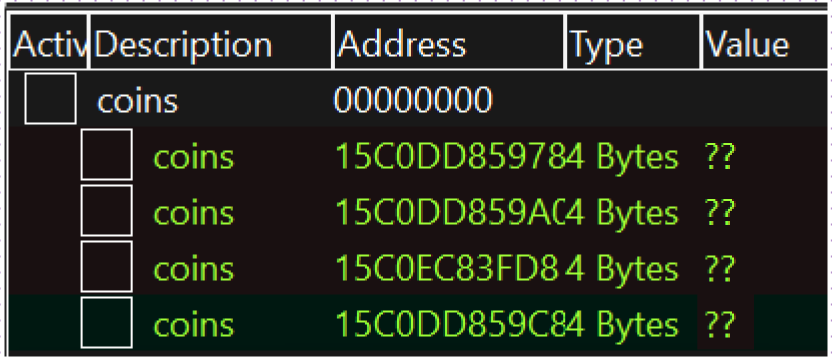
Description	Address	Type	Value
health	15C0DD85978	4 Bytes	1337



```
Offset-description          Address: Value
Player
 0000 - 4 Bytes 5DA650 : 1337
 0004 - 4 Bytes 5DA654 : 100
 0008 - 4 Bytes 5DA658 : 200
 000C - 4 Bytes 5DA65C : 22
```

```
struct Player
{
    int health   = 1337;
    int strength = 100;
    int defense  = 200;
}
```

Persisting memory addresses

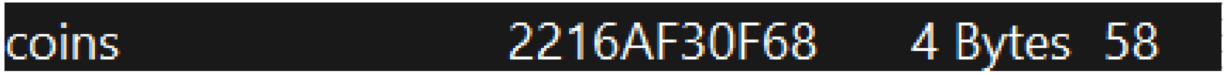


Activ	Description	Address	Type	Value
	coins	00000000		
	coins	15C0DD85978	4 Bytes	??
	coins	15C0DD859AC	4 Bytes	??
	coins	15C0EC83FD8	4 Bytes	??
	coins	15C0DD859C8	4 Bytes	??

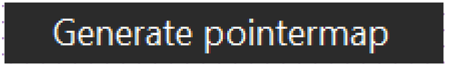
Reload game
Lose everything!

Persisting memory addresses

Solution: search *potentially* static addresses
search for all code that points to the address

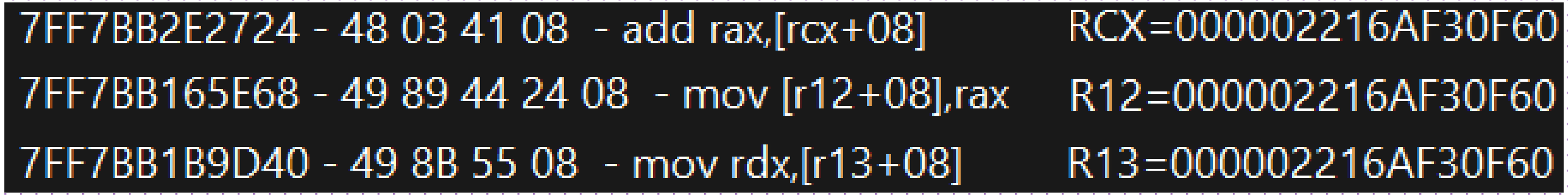


```
coins                    2216AF30F68     4 Bytes   58
```

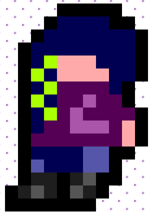


Recursive scan

```
op [(Address - 1) + 01]
op [(Address - 2) + 02]
op [(Address - 3) + 03]
…
```

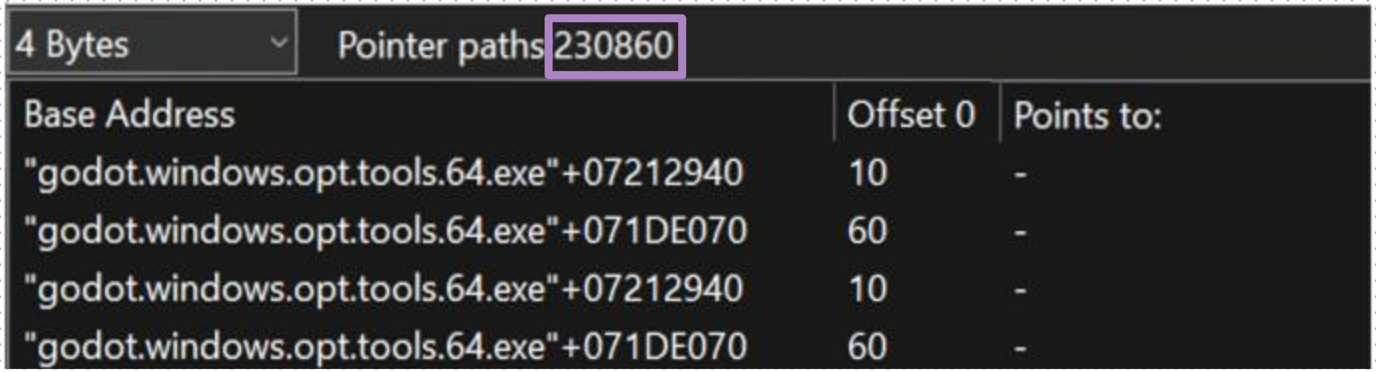


```
7FF7BB2E2724 - 48 03 41 08  - add rax,[rcx+08]        RCX=000002216AF30F60
7FF7BB165E68 - 49 89 44 24 08  - mov [r12+08],rax     R12=000002216AF30F60
7FF7BB1B9D40 - 49 8B 55 08  - mov rdx,[r13+08]        R13=000002216AF30F60
```



Persisting memory addresses

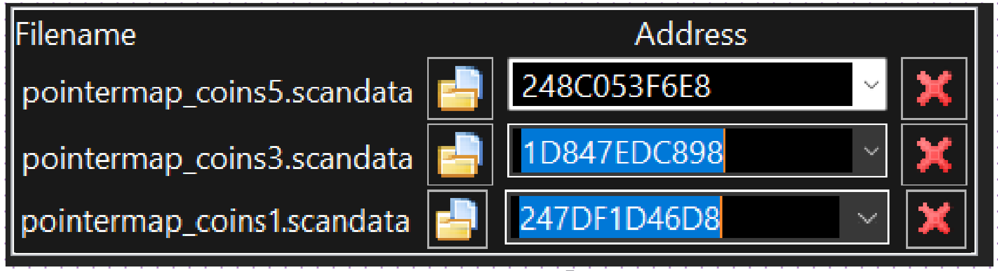
Problem: too many results!



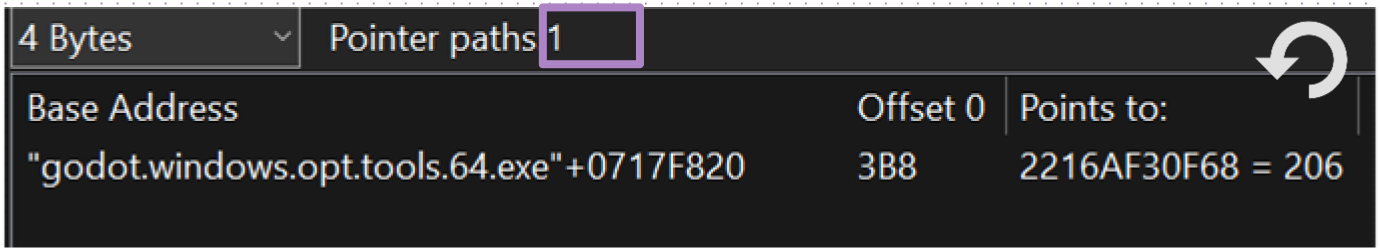
```
4 Bytes          Pointer paths 230860
Base Address                                   Offset 0   Points to:
"godot.windows.opt.tools.64.exe"+07212940     10         -
"godot.windows.opt.tools.64.exe"+071DE070     60         -
"godot.windows.opt.tools.64.exe"+07212940     10         -
"godot.windows.opt.tools.64.exe"+071DE070     60         -
```

Persisting memory addresses

solution: rescan, and compare results

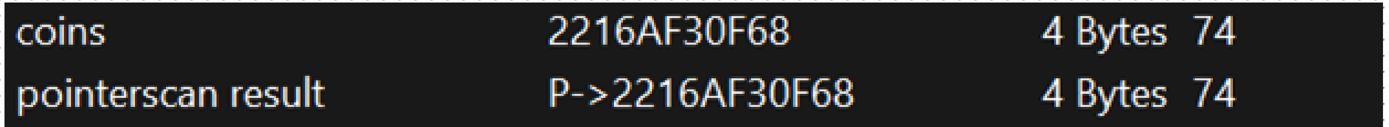


Filename	Address
pointermap_coins5.scandata	248C053F6E8
pointermap_coins3.scandata	1D847EDC898
pointermap_coins1.scandata	247DF1D46D8



4 Bytes   Pointer paths 1

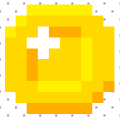
Base Address	Offset 0	Points to:
"godot.windows.opt.tools.64.exe"+0717F820	3B8	2216AF30F68 = 206

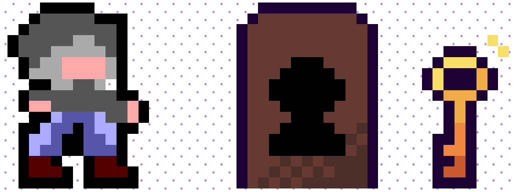


coins	2216AF30F68	4 Bytes	74
pointerscan result	P->2216AF30F68	4 Bytes	74

What if we don't search a value?

How to search for a condition?

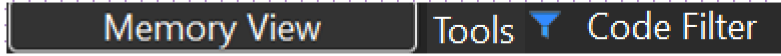


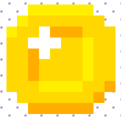


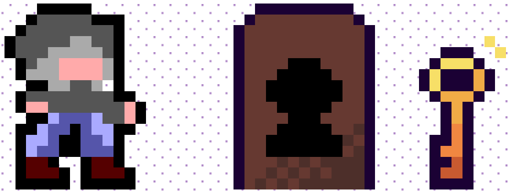
```
def player_move():
    if collision("coin"):
        coins += 1
    if collision("door"):
        if has_key:
            open_door()
    if button("down"):
        crouch()
```

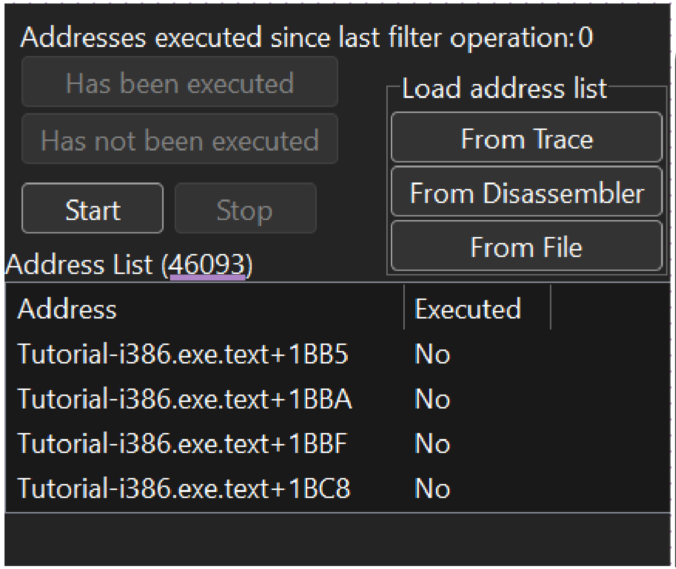
What if we don't search a value?

How to search for a condition?:
code filter





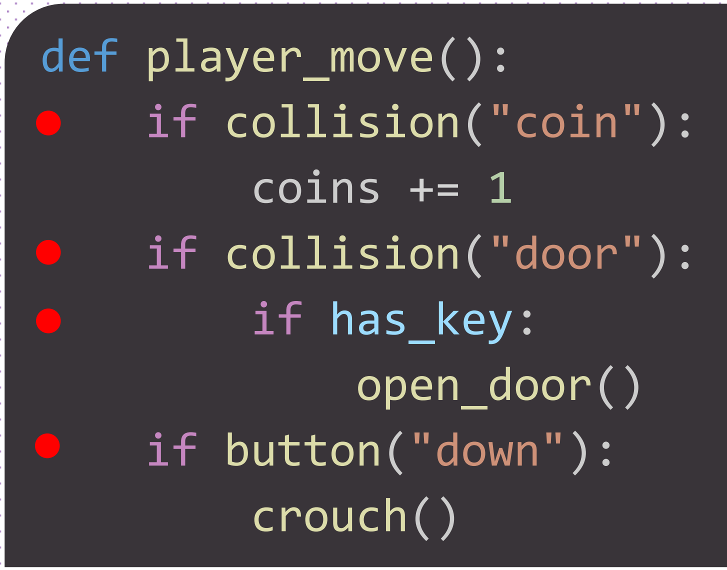




Addresses executed since last filter operation:0

Address List (46093)

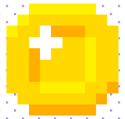
Address	Executed
Tutorial-i386.exe.text+1BB5	No
Tutorial-i386.exe.text+1BBA	No
Tutorial-i386.exe.text+1BBF	No
Tutorial-i386.exe.text+1BC8	No

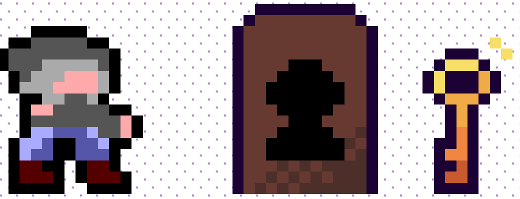


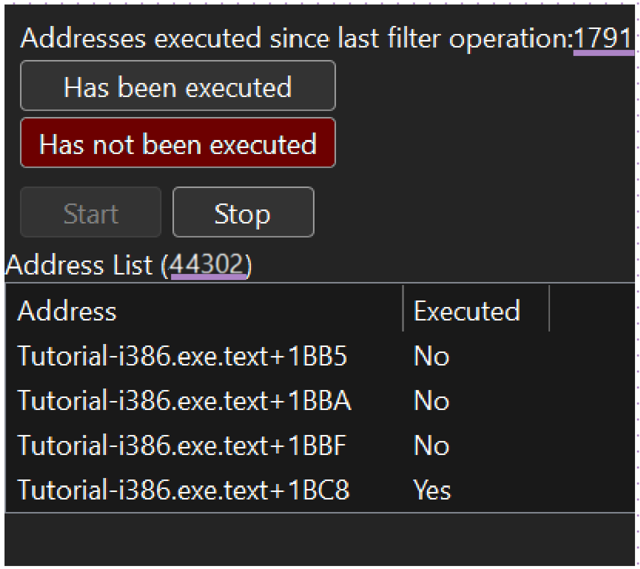
```
def player_move():
●   if collision("coin"):
        coins += 1
●   if collision("door"):
●       if has_key:
            open_door()
●   if button("down"):
        crouch()
```

What if we don't search a value?

How to search for a condition?:
code filter



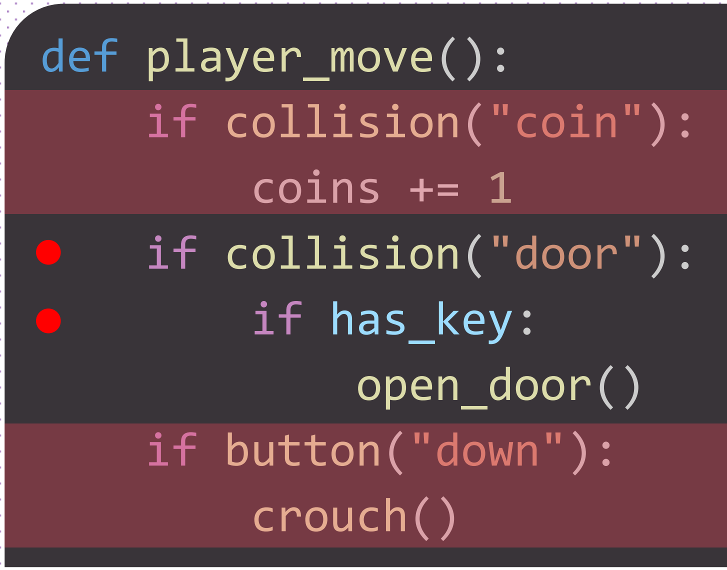




Addresses executed since last filter operation:1791

Address List (44302)

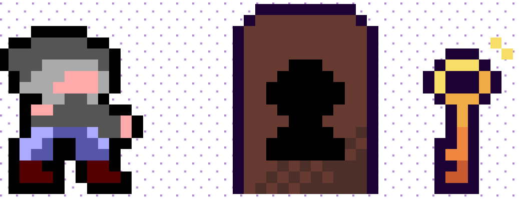
Address	Executed
Tutorial-i386.exe.text+1BB5	No
Tutorial-i386.exe.text+1BBA	No
Tutorial-i386.exe.text+1BBF	No
Tutorial-i386.exe.text+1BC8	Yes

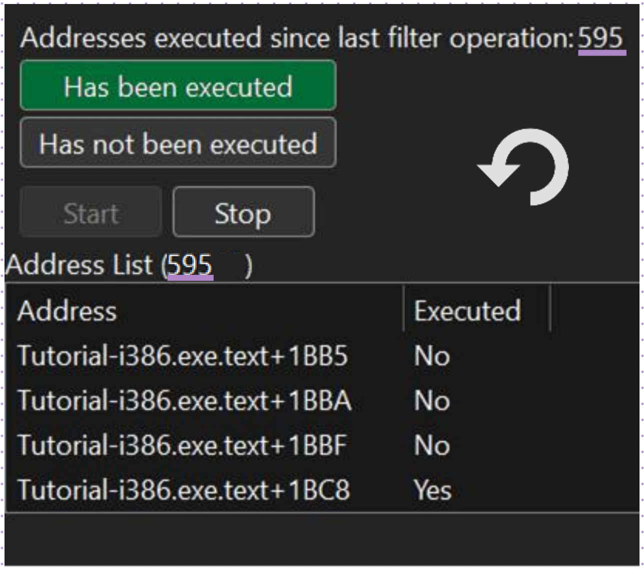


```
def player_move():
    if collision("coin"):
        coins += 1
●   if collision("door"):
●       if has_key:
            open_door()
    if button("down"):
        crouch()
```

What if we don't search a value?

How to search for a condition?:
code filter

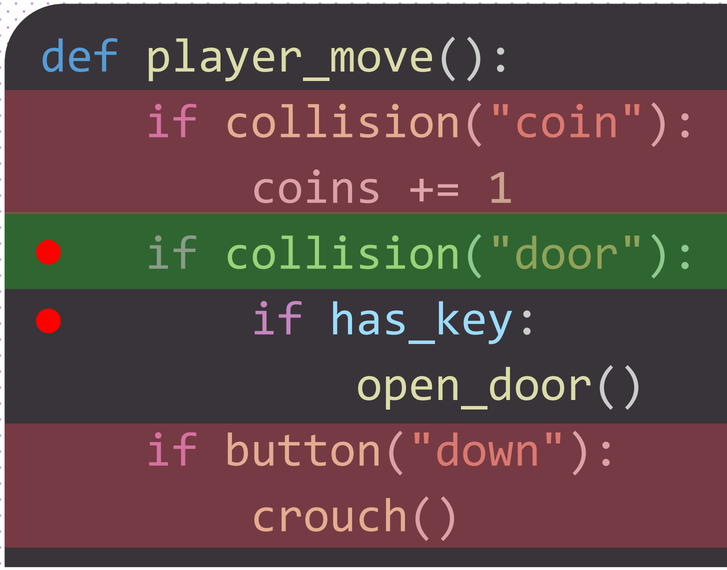




Addresses executed since last filter operation: 595

Address List (595)

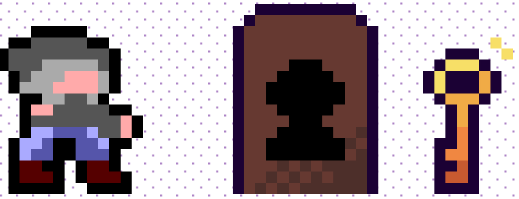
Address	Executed
Tutorial-i386.exe.text+1BB5	No
Tutorial-i386.exe.text+1BBA	No
Tutorial-i386.exe.text+1BBF	No
Tutorial-i386.exe.text+1BC8	Yes

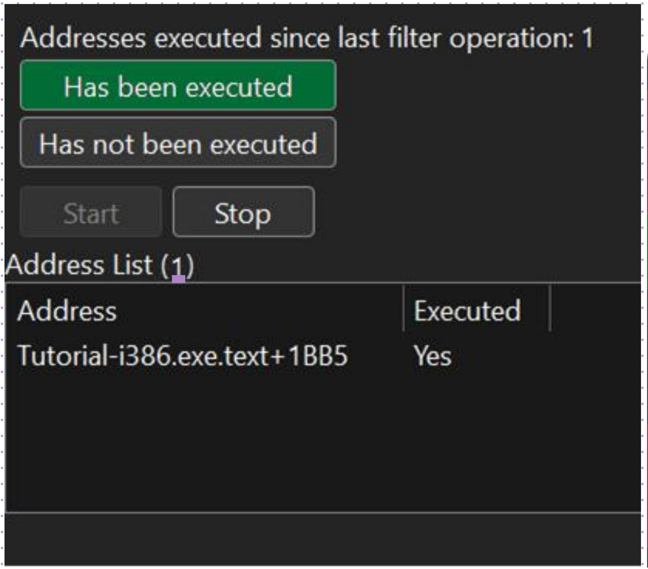


```
def player_move():
    if collision("coin"):
        coins += 1
●   if collision("door"):
●       if has_key:
            open_door()
    if button("down"):
        crouch()
```

What if we don't search a value?

How to search for a condition?:
code filter

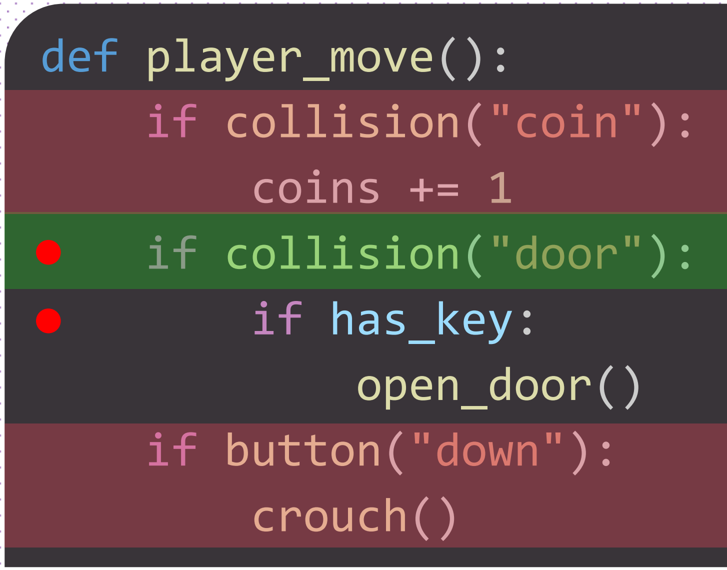




Addresses executed since last filter operation: 1

Address List (1)

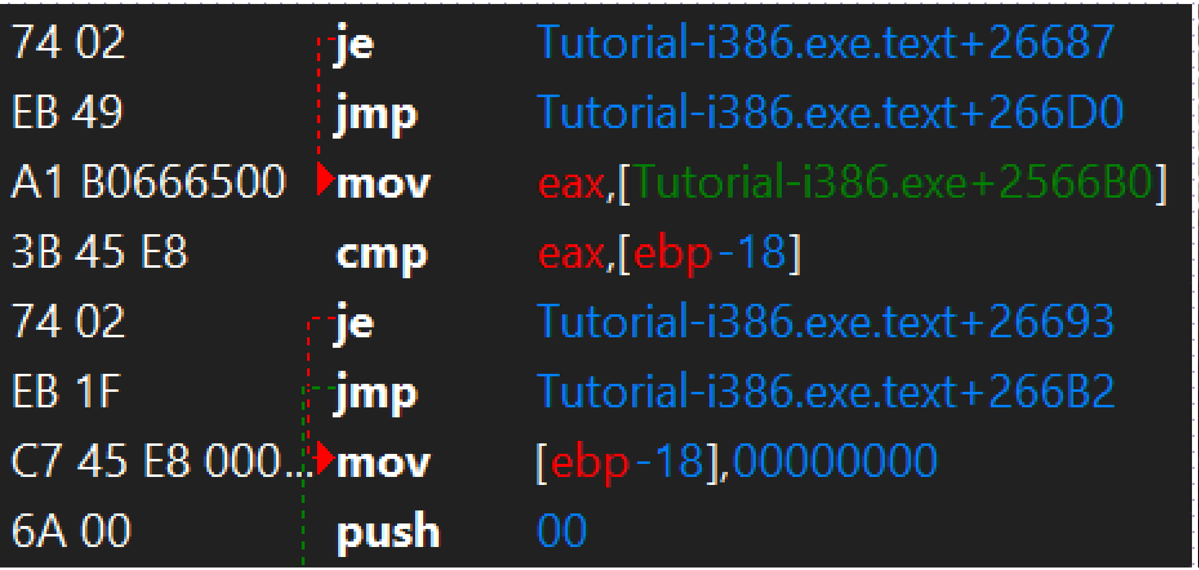
Address	Executed
Tutorial-i386.exe.text+1BB5	Yes



```
def player_move():
    if collision("coin"):
        coins += 1
●   if collision("door"):
●       if has_key:
            open_door()
    if button("down"):
        crouch()
```

Instruction patching

ASM, help!



```
74 02            je    Tutorial-i386.exe.text+26687
EB 49            jmp   Tutorial-i386.exe.text+266D0
A1 B0666500      mov   eax,[Tutorial-i386.exe+2566B0]
3B 45 E8         cmp   eax,[ebp-18]
74 02            je    Tutorial-i386.exe.text+26693
EB 1F            jmp   Tutorial-i386.exe.text+266B2
C7 45 E8 000...  mov   [ebp-18],00000000
6A 00            push  00
```

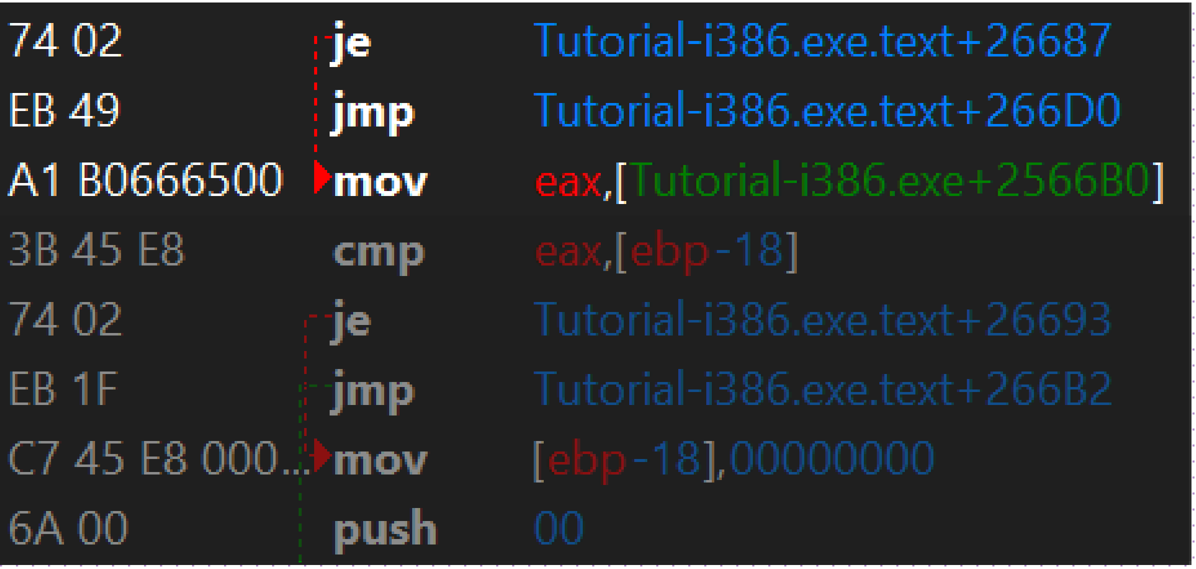
Instruction patching

ASM primer

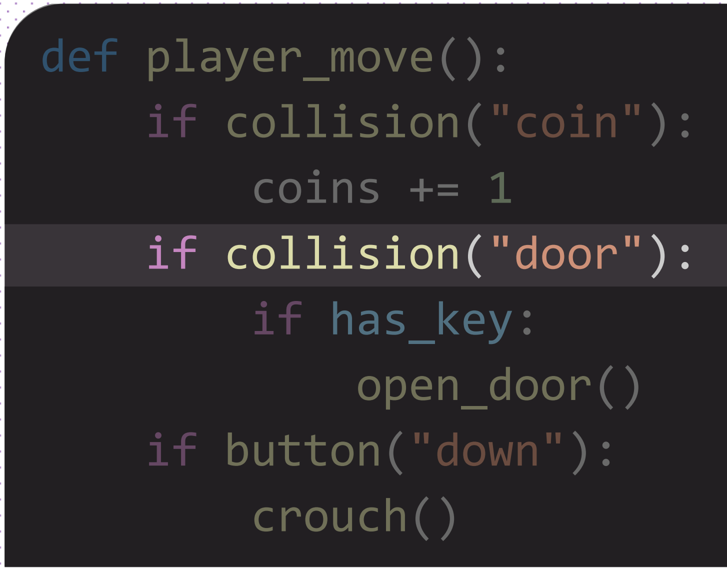
je	if ==
jne	if !==
jg	if >
jl	if <
add	+=
sub	-=
mov	x=y
nop	do nothing (padding)

Instruction patching

Replace the *has_key* condition



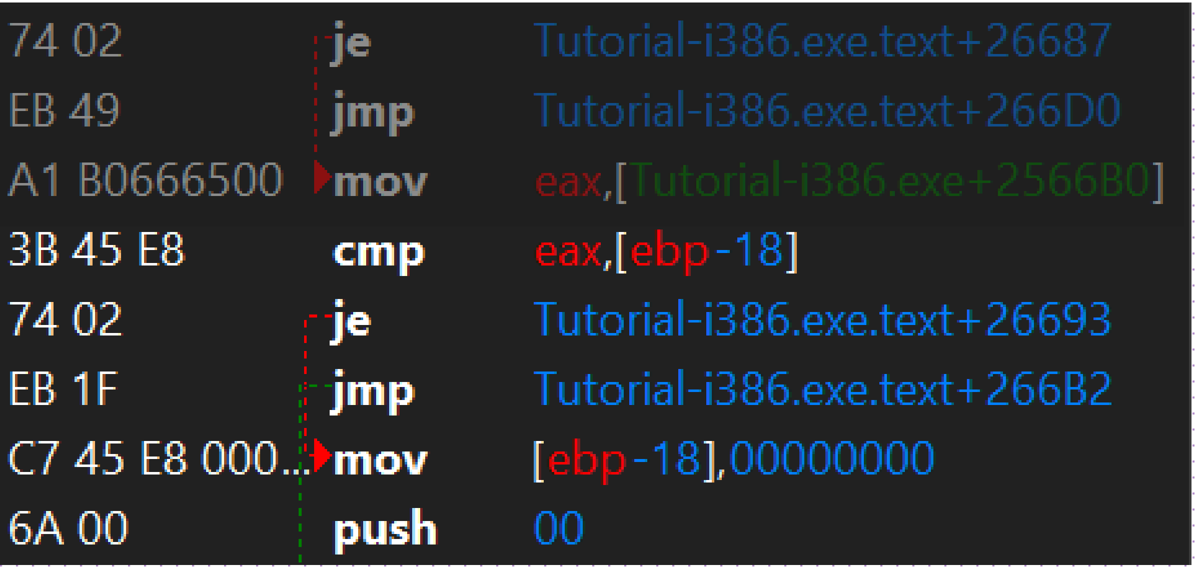
```
74 02          je    Tutorial-i386.exe.text+26687
EB 49          jmp   Tutorial-i386.exe.text+266D0
A1 B0666500    mov   eax,[Tutorial-i386.exe+2566B0]
3B 45 E8       cmp   eax,[ebp-18]
74 02          je    Tutorial-i386.exe.text+26693
EB 1F          jmp   Tutorial-i386.exe.text+266B2
C7 45 E8 000...mov   [ebp-18],00000000
6A 00          push  00
```



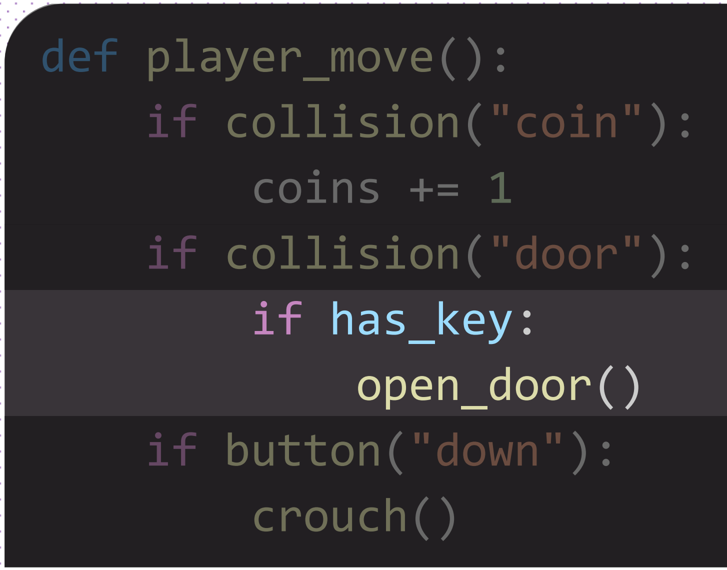
```
def player_move():
    if collision("coin"):
        coins += 1
    if collision("door"):
        if has_key:
            open_door()
    if button("down"):
        crouch()
```

Instruction patching

Replace the *has_key* condition



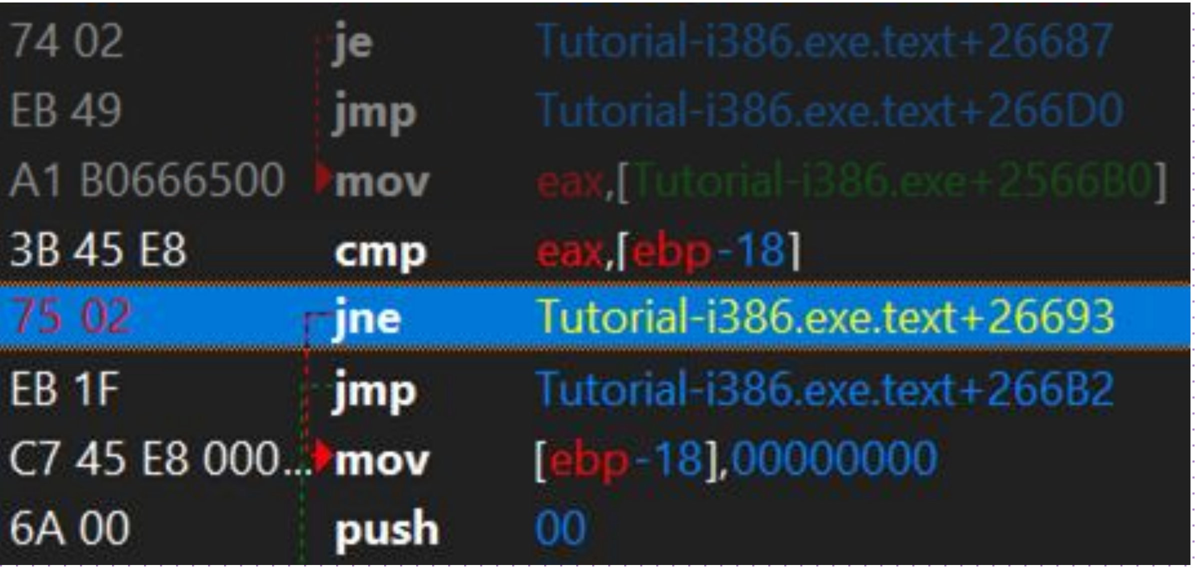
```
74 02            je    Tutorial-i386.exe.text+26687
EB 49            jmp   Tutorial-i386.exe.text+266D0
A1 B0666500      mov   eax,[Tutorial-i386.exe+2566B0]
3B 45 E8         cmp   eax,[ebp-18]
74 02            je    Tutorial-i386.exe.text+26693
EB 1F            jmp   Tutorial-i386.exe.text+266B2
C7 45 E8 000...  mov   [ebp-18],00000000
6A 00            push  00
```



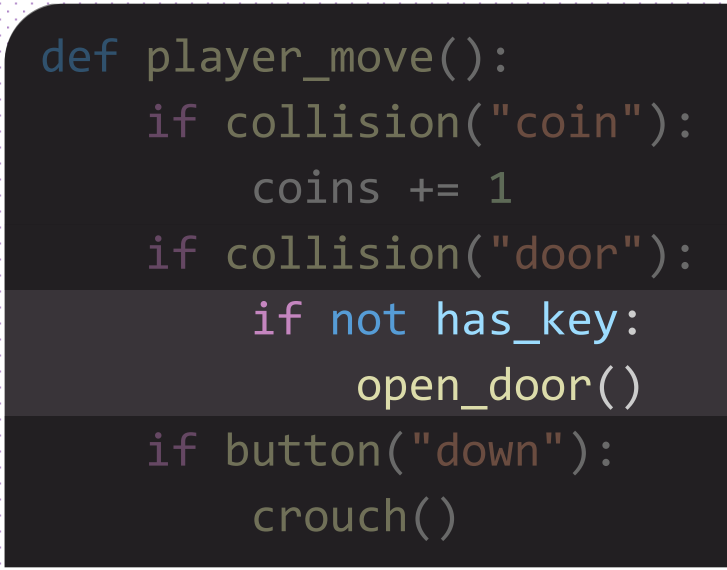
```
def player_move():
    if collision("coin"):
        coins += 1
    if collision("door"):
        if has_key:
            open_door()
    if button("down"):
        crouch()
```

Instruction patching

Replace the *has_key* condition



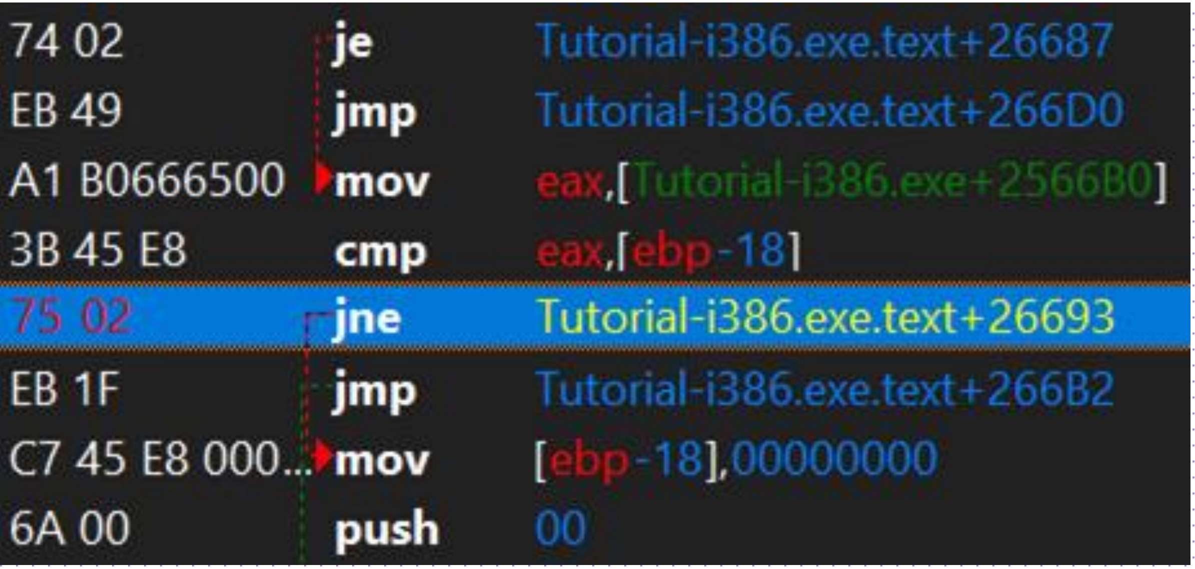
```
74 02             je    Tutorial-i386.exe.text+26687
EB 49             jmp   Tutorial-i386.exe.text+266D0
A1 B0666500       mov   eax,[Tutorial-i386.exe+2566B0]
3B 45 E8          cmp   eax,[ebp-18]
75 02             jne   Tutorial-i386.exe.text+26693
EB 1F             jmp   Tutorial-i386.exe.text+266B2
C7 45 E8 000...   mov   [ebp-18],00000000
6A 00             push  00
```



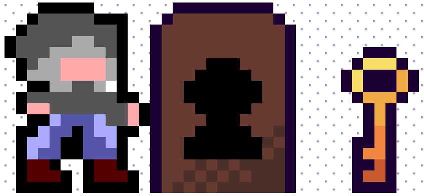
```python
def player_move():
    if collision("coin"):
        coins += 1
    if collision("door"):
        if not has_key:
            open_door()
    if button("down"):
        crouch()
```

Instruction patching

Replace the *has_key* condition

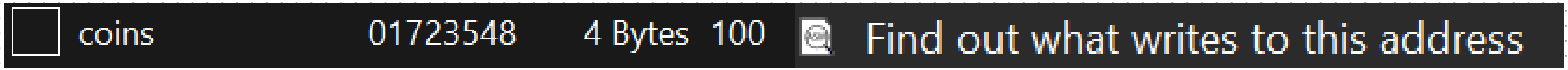


```
74 02           je    Tutorial-i386.exe.text+26687
EB 49           jmp   Tutorial-i386.exe.text+266D0
A1 B0666500     mov   eax,[Tutorial-i386.exe+2566B0]
3B 45 E8        cmp   eax,[ebp-18]
75 02           jne   Tutorial-i386.exe.text+26693
EB 1F           jmp   Tutorial-i386.exe.text+266B2
C7 45 E8 000... mov   [ebp-18],00000000
6A 00           push  00
```

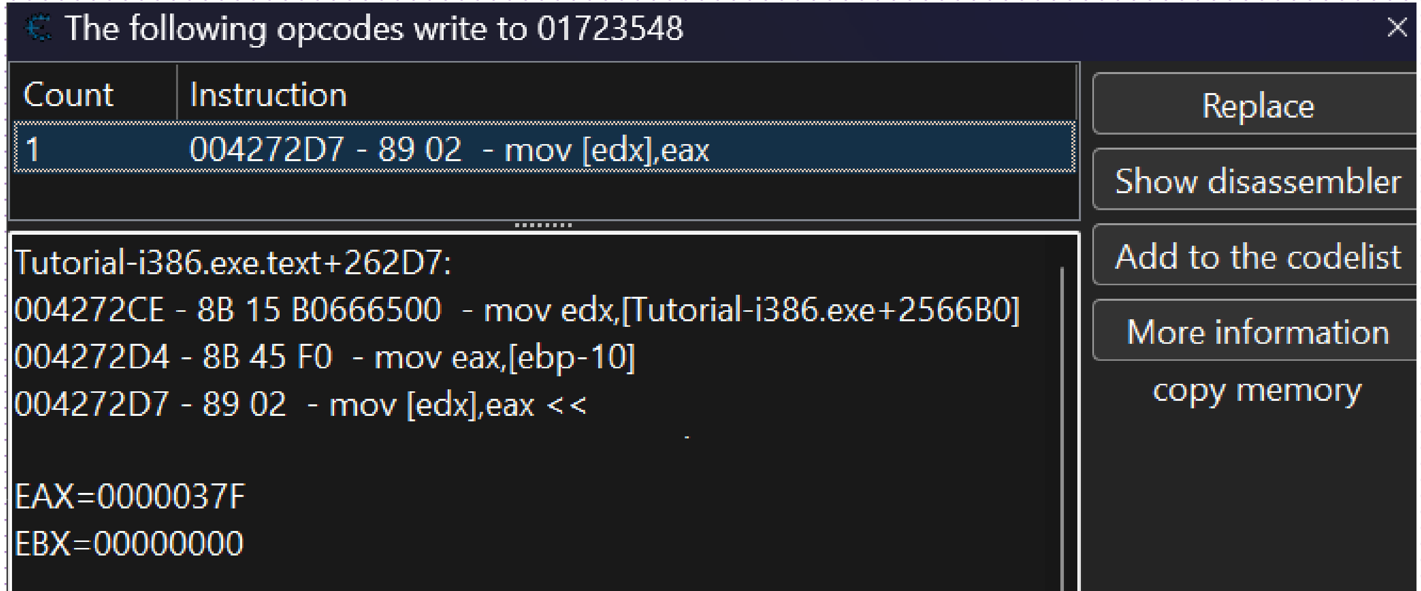


Instruction patching

What if we could do it from known memory addresses?



```
coins    01723548    4 Bytes  100
```



The following opcodes write to 01723548

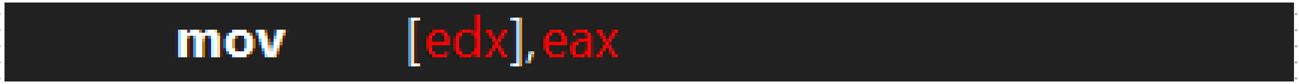
Count	Instruction
1	004272D7 - 89 02 - mov [edx],eax

```
Tutorial-i386.exe.text+262D7:
004272CE - 8B 15 B0666500  - mov edx,[Tutorial-i386.exe+2566B0]
004272D4 - 8B 45 F0  - mov eax,[ebp-10]
004272D7 - 89 02  - mov [edx],eax <<

EAX=0000037F
EBX=00000000
```

Instruction patching: problems

Less obvious instructions

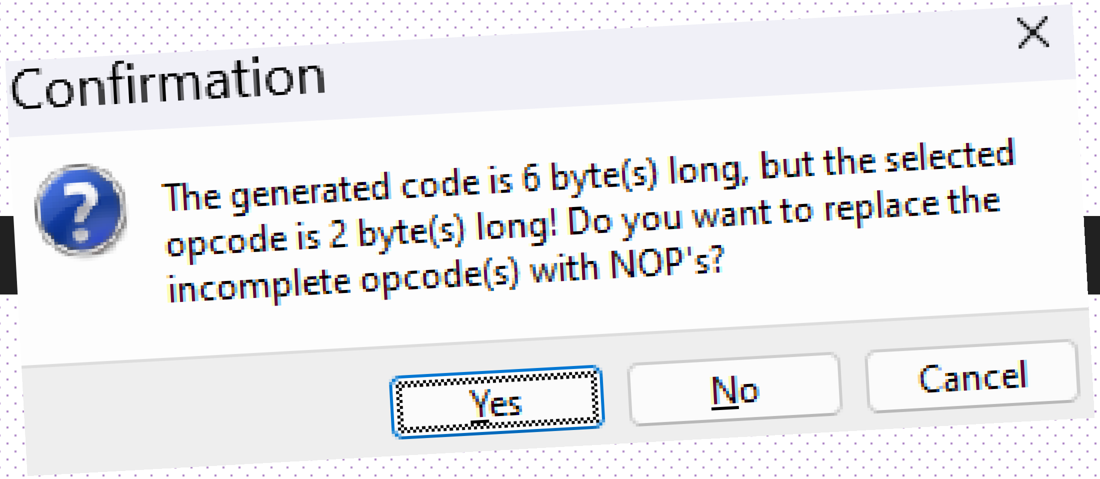
where **add** ?



```
mov         [edx],eax
```

Instruction patching: problems

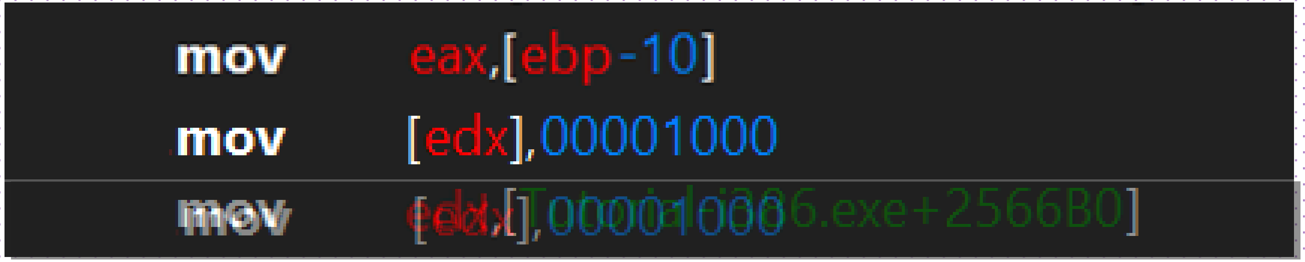
Instruction size clash



The generated code is 6 byte(s) long, but the selected opcode is 2 byte(s) long! Do you want to replace the incomplete opcode(s) with NOP's?

Instruction patching: problems

Instruction size clash
Where to add our code?



```
mov     eax,[ebp-10]
mov     [edx],00001000
mov     edx,[Tutorial-i386.exe+2566B0]
mov     [edx],00001000
```

Autoassemble

Solution: **auto assembler!**

- Auto-allocate memory
- Create complex methods
- Persisting and toggleable

```
[ENABLE]
alloc(newmem,2048)
label(return)
alloc(multiplier, 2)
registerSymbol(multiplier)




multiplier:
    dd (int)5

newmem:
mov eax, [edx]
add eax, [multiplier]
mov [edx],eax
mov eax, [Tutorial-i386.exe+2566B0]
jmp return

"Tutorial-i386.exe"+272D7:
jmp newmem
nop 2
return:

[DISABLE]
dealloc(multiplier)
unregisterSymbol(multiplier)

dealloc(newmem)
"Tutorial-i386.exe"+272D7:
db 89 02 A1 B0 66 65 00
```

Autoassemble

Solution: **auto assembler!**

- **Auto-allocate memory**

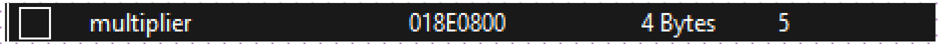
```
alloc(newmem,2048)
label(return)









newmem:
// your code here




jmp return

"Tutorial-i386.exe"+272D7: //original
jmp newmem                             address
nop 2
return:
```

Autoassemble

Solution: **auto assembler!**

- Auto-allocate memory

  manages labels, variables...



multiplier 018E0800 4 Bytes 5

```
alloc(newmem,2048)
label(return)
alloc(multiplier, 2)
registerSymbol(multiplier)




multiplier:
    dd (int)5

newmem:
mov eax, [edx]
add eax, [multiplier]


jmp return

"Tutorial-i386.exe"+272D7:
jmp newmem
nop 2
return:
```

Autoassemble

Solution: **auto assembler!**

- Auto-allocate memory
- **Create complex methods**

```
alloc(newmem,2048)
label(return)
alloc(multiplier, 2)
registerSymbol(multiplier)




multiplier:
    dd (int)5

newmem:
mov eax, [edx] //coins += multiplier
add eax, [multiplier]
mov [edx],eax
mov eax, [Tutorial-i386.exe+2566B0]
jmp return

"Tutorial-i386.exe"+272D7:
jmp newmem
nop 2
return:
```

Template -> Full Injection

Autoassemble

Solution: **auto assembler!**

- Auto-allocate memory
- Create complex methods
- **Persisting and toggleable**

```
[ENABLE]
alloc(newmem,2048)
label(return)
alloc(multiplier, 2)
registerSymbol(multiplier)




multiplier:
    dd (int)5

newmem:
mov eax, [edx]
add eax, [multiplier]
mov [edx],eax
mov eax, [Tutorial-i386.exe+2566B0]
jmp return

"Tutorial-i386.exe"+272D7:
jmp newmem
nop 2
return:

[DISABLE]
dealloc(multiplier)
unregisterSymbol(multiplier)

dealloc(newmem)
"Tutorial-i386.exe"+272D7:
db 89 02 A1 B0 66 65 00
```

Autoassemble

Solution: **auto assembler!**

- Auto-allocate memory
- Create complex methods
- **Persisting and toggleable**

```
[ENABLE]
alloc(newmem,2048)
label(return)
alloc(multiplier, 2)
registerSymbol(multiplier)




multiplier:
    dd (int)5

newmem:
mov eax, [edx]
add eax, [multiplier]
mov [edx],eax
mov eax, [Tutorial-i386.exe+2566B0]
jmp return

"Tutorial-i386.exe"+272D7:
jmp newmem
nop 2
return:

[DISABLE]
dealloc(multiplier)
unregisterSymbol(multiplier)

dealloc(newmem)
"Tutorial-i386.exe"+272D7:
db 89 02 A1 B0 66 65 00
```

Template -> AOB Injection

Autoassemble

Solution: **auto assembler!**

- Auto-allocate memory
- Create complex methods
- Persisting and toggleable

  Resist binary changes with AOB scans

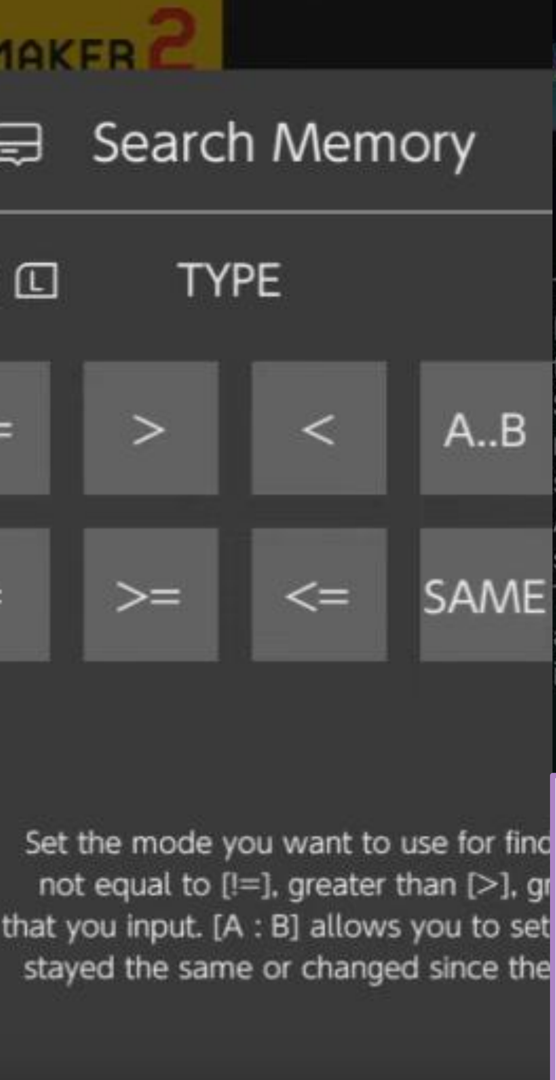
```
[ENABLE]
alloc(newmem,2048)
label(return)
alloc(multiplier, 2)
registerSymbol(multiplier)
registerSymbol(INJECT)
aobscanmodule(INJECT,Tutorial-i386.exe,
                89 02 A1 B0 66 65 00)

multiplier:
    dd (int)5

newmem:
mov eax, [edx]
add eax, [multiplier]
mov [edx],eax
mov eax, [Tutorial-i386.exe+2566B0]
jmp return

INJECT:
jmp newmem
nop 2
return:

[DISABLE]
dealloc(multiplier)
unregisterSymbol(multiplier)

dealloc(newmem)
INJECT:
db 89 02 A1 B0 66 65 00
unregistersymbol(INJECT)
```

Autoassemble

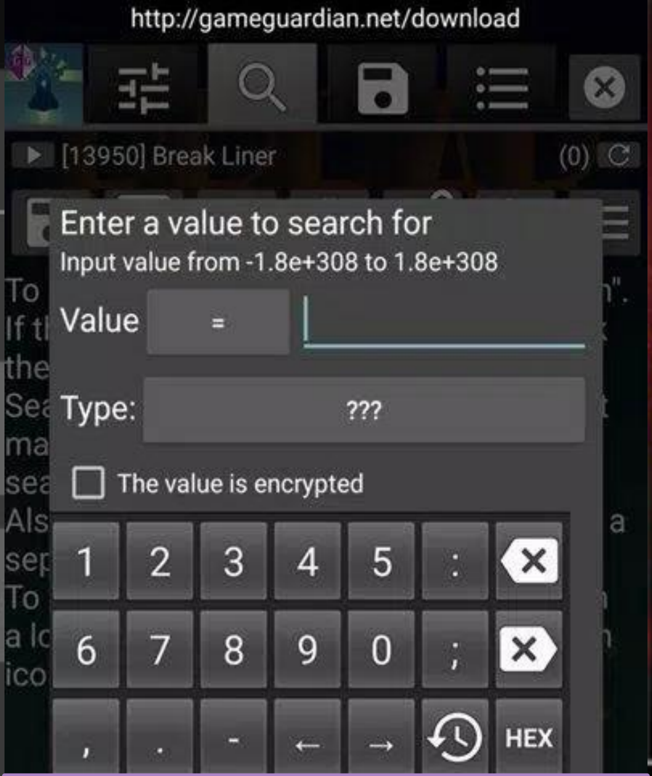
Solution: **auto assembler!**

- Auto-allocate memory
- Create complex methods
- Persisting and toggleable

```
[ENABLE]
alloc(newmem,2048)
label(return)
alloc(multiplier, 2)
registerSymbol(multiplier)
registerSymbol(INJECT)
aobscanmodule(INJECT,Tutorial-i386.exe,
                89 02 A1 B0 66 65 00)

multiplier:
    dd (int)5

newmem:
mov eax, [edx]
add eax, [multiplier]
mov [edx],eax
mov eax, [Tutorial-i386.exe+2566B0]
jmp return

INJECT:
jmp newmem
nop 2
return:

[DISABLE]
dealloc(multiplier)
unregisterSymbol(multiplier)

dealloc(newmem)
INJECT:
db 89 02 A1 B0 66 65 00
unregistersymbol(INJECT)
```



Set the mode you want to use for find
not equal to [!=], greater than [>], g
that you input. [A : B] allows you to set
stayed the same or changed since the


http://gameguardian.net/download

[13950] Break Liner (0)

Enter a value to search for
Input value from -1.8e+308 to 1.8e+308

Value: =

Type: ???

The value is encrypted

Equivalents on all platforms

Less advanced /
More complex to setup

POUR GAME BOY. ADVANCE & GAME BOY. ADVANCE SP
AR ACTION REPLAY
Inclus des codes exclusifs pour Pokémon ROUGE FEU
Inclus des codes exclusifs pour Pokémon VERT FEUILLE
Inclus des codes exclusifs pour Pokémon RUBIS
Inclus des codes exclusifs pour Pokémon SAPHIR
PRÉCHARGÉ AVEC PLUS DE 3000 CODES INCROYABLES
Tous les véhicules
Munitions Infinies
Personnages Supplémentaires
Vie Infinie
DECHAINE LA PUISSANCE POUR FINIR TES JEUX !

Next steps

code caves

unrandomizer

Float ASM

.1

Shared instructions

speedhack

LUA Autoclicker

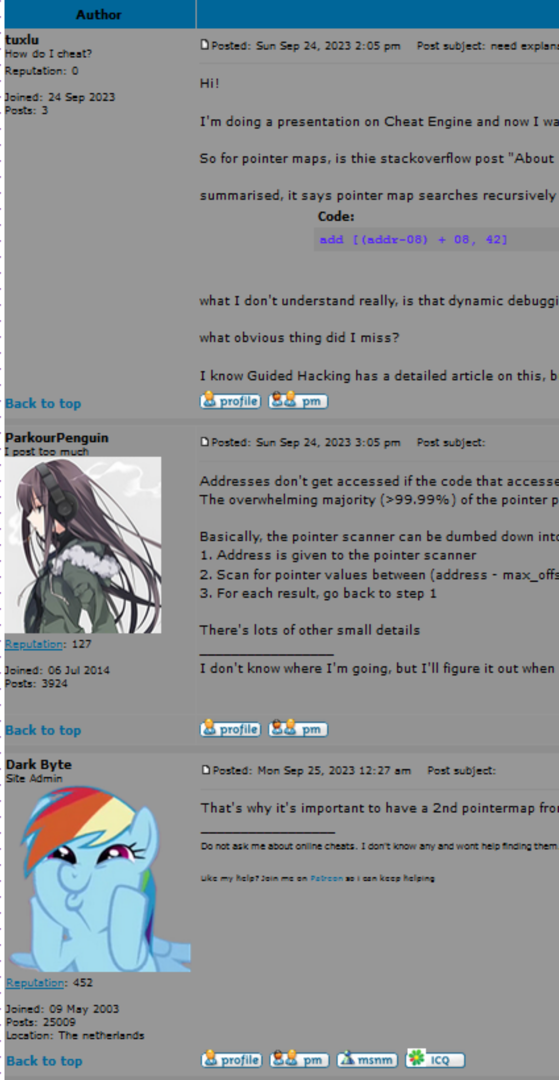
Trainer GUI

Multilevel pointers

->

Resources

- Cheat Engine Forums



Author

tuxlu
How do I cheat?
Reputation: 0

Joined: 24 Sep 2023
Posts: 3

Posted: Sun Sep 24, 2023 2:05 pm   Post subject: need explana

Hi!

I'm doing a presentation on Cheat Engine and now I wa

So for pointer maps, is thie stackoverflow post "About

summarised, it says pointer map searches recursively

Code:
```
add [(addr-08) + 08, 42]
```

what I don't understand really, is that dynamic debuggi

what obvious thing did I miss?

I know Guided Hacking has a detailed article on this, b

Back to top   profile   pm

ParkourPenguin
I post too much

Reputation: 127

Joined: 06 Jul 2014
Posts: 3924

Posted: Sun Sep 24, 2023 3:05 pm   Post subject:

Addresses don't get accessed if the code that accesse
The overwhelming majority (>99.99%) of the pointer p

Basically, the pointer scanner can be dumbed down into
1. Address is given to the pointer scanner
2. Scan for pointer values between (address - max_offs
3. For each result, go back to step 1

There's lots of other small details

____
I don't know where I'm going, but I'll figure it out when

Back to top   profile   pm

Dark Byte
Site Admin

Reputation: 452

Joined: 09 May 2003
Posts: 25009
Location: The netherlands

Posted: Mon Sep 25, 2023 12:27 am   Post subject:

That's why it's important to have a 2nd pointermap fro

____
Do not ask me about online cheats. I don't know any and wont help finding them.

Like my help? Join me on Patreon so i can keep helping

Back to top   profile   pm   msnm   ICQ

Resources

- Cheat Engine Forums
- **Youtube tutorials**
  By Stephen Chapman
  & Guided Hacking

No programming knowledge necessary!
HOW TO MAKE A TRAINER WITH CHEAT ENGINE!
CHEAT ENGINE TUTORIAL SERIES REFRESHER:
QUICK-SOLVE STEPS 2-9, FOR RETURNING CE USERS!
CHEAT ENGINE TUTORIAL SERIES PART 16:
DBVM AND ULTIMAP!
CHEAT ENGINE TUTORIAL SERIES PART 15:
ALL ABOUT XMM REGISTERS
WRITES TO/ACCESSES AN ADDRESS
CHEAT ENGINE TUTORIAL SERIES PART 13:
HOW TO FIND ADDRESSES AN INSTRUCTION WRITES TO!
CHEAT ENGINE TUTORIAL SERIES FOR PROS:
ADVANCED SCRIPTING AND ASSEMBLY, TRACER DEBUGGING, CODE REFACTORING, AND MORE!
SCANS DEMYSTIFIED!
ONE CHEAT: MANY SOLUTIONS!
CHEAT ENGINE TUTORIAL SERIES FOR PROS:
BACK-TRACING A SHARED INSTRUCTION FROM A VISUAL ADDRESS!

Resources

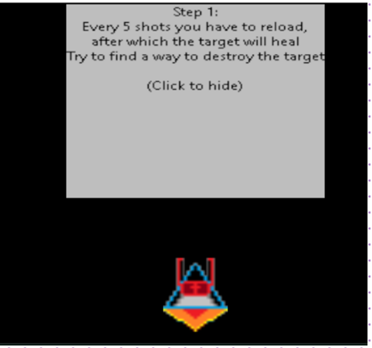
- Cheat Engine Forums
- Youtube tutorials
  By Stephen Chapman
  & Guided Hacking
- **Video game challenges!**

3

Creating a game for hackers

Shall we play a game?

past CtF games


Step 1:
Every 5 shots you have to reload,
after which the target will heal
Try to find a way to destroy the target

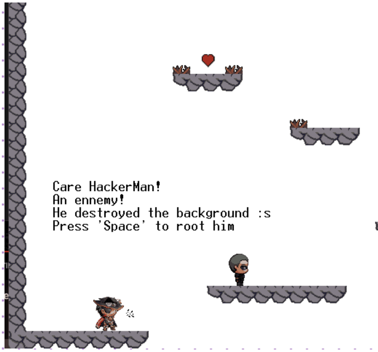
(Click to hide)

Cheat Engine
Built-in tutorial

```
#include "libGameLogic.h"

void Player::SetJumpState(bool b) {
    printf("[*] SetJumpState(%d)\n", b);
}
```

Pwn Adventure

Google CTF
Hackceler8


```
Care HackerMan!
An ennemy!
He destroyed the background :s
Press 'Space' to root him
```

Rootme's HackerMan

Released while working on my challenge!

Godot Engine

Free open source engine

Lightweight and fast iteration

Growing community

4

Protecting your game from hackers

No fun allowed

Protect your game

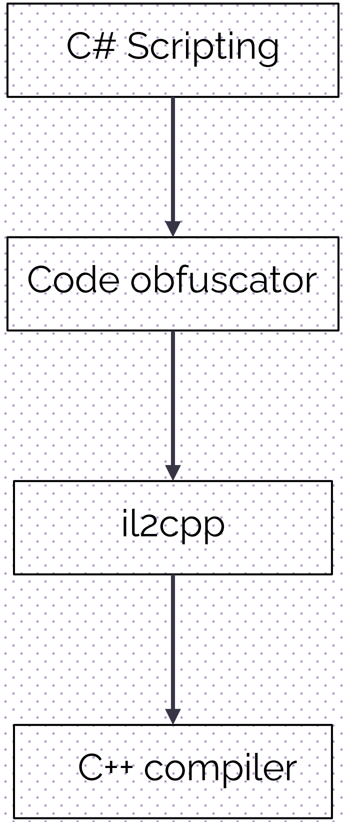
- Obfuscate values in memory

```
struct AntiCheatInt
{
    int projected;
    int r = rand();

    public int Value {
        get => (projected + r) / 3;
        set => projected = (value * 3) - r;
    }
}
```

Protect your game

- Obfuscate values in memory
- **Obfuscate binaries**

unity Code pipeline



```
void takeDamage(int amount)
```

```
void x1337(int zzcc)
```

```
extern MethodInfo
playerclass_x1337(int zzcc)
```

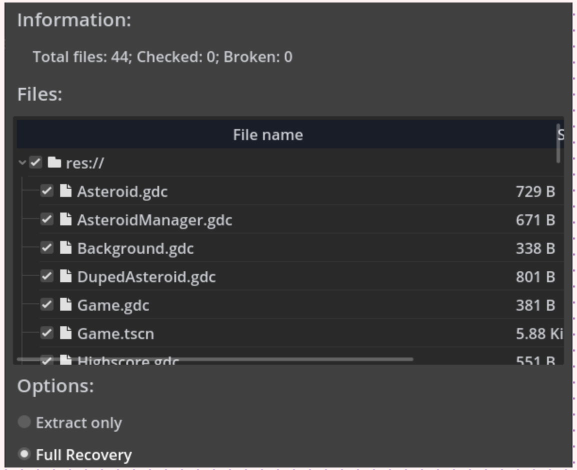
```
mov [r12+10],rcx
mov rax, [r13+08]
```

Protect your game : Godot

Interpreted language in
an open source format

Protect your game: Godot

Interpreted language in an open source format



```
Information:
  Total files: 44; Checked: 0; Broken: 0
Files:
                         File name
⌄ ✓ res://
    ✓ Asteroid.gdc                    729 B
    ✓ AsteroidManager.gdc             671 B
    ✓ Background.gdc                  338 B
    ✓ DupedAsteroid.gdc               801 B
    ✓ Game.gdc                        381 B
    ✓ Game.tscn                       5.88 Ki
    ✓ Highscore.gdc                   551 B
Options:
  ○ Extract only
  ● Full Recovery
```

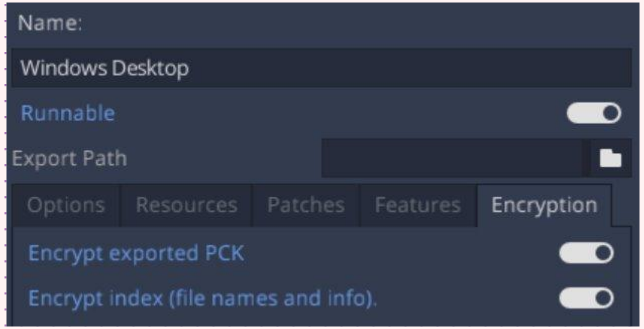
Entirely decompilable with GdsDecomp

Protect your game: Godot

Interpreted language in an open source format

Entirely decompilable with GdsDecomp

Game can be encrypted with an AES key

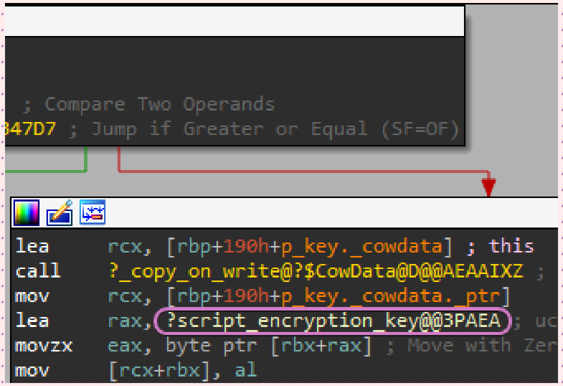


Name:
Windows Desktop
Runnable
Export Path
Options | Resources | Patches | Features | Encryption
Encrypt exported PCK
Encrypt index (file names and info).

Protect your game: Godot

Interpreted language in an open source format

Game can be encrypted with an AES key



```
 ; Compare Two Operands
347D7 ; Jump if Greater or Equal (SF=OF)
```

```
lea     rcx, [rbp+190h+p_key._cowdata] ; this
call    ?_copy_on_write@?$CowData@D@@AEAAIXZ ;
mov     rcx, [rbp+190h+p_key._cowdata._ptr]
lea     rax, ?script_encryption_key@@3PAEA ; uc
movzx   eax, byte ptr [rbx+rax] ; Move with Zer
mov     [rcx+rbx], al
```

Entirely decompilable with GdsDecomp

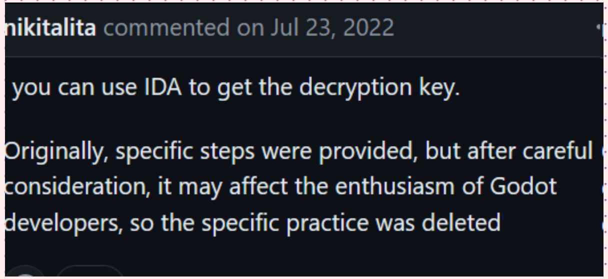
Key is extractible in the binary

Protect your game: Godot

Interpreted language in an open source format

Game can be encrypted with an AES key

GdsDecomp dev won't give hints on how to extract it



nikitalita commented on Jul 23, 2022

you can use IDA to get the decryption key.

Originally, specific steps were provided, but after careful consideration, it may affect the enthusiasm of Godot developers, so the specific practice was deleted

Entirely decompilable with GdsDecomp

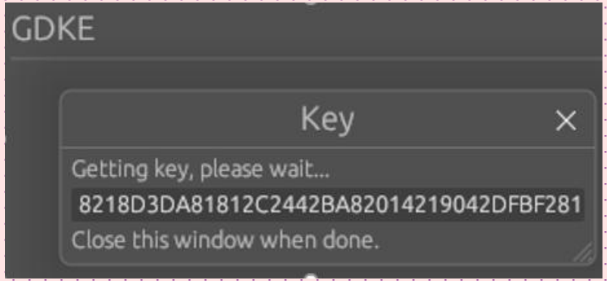
Key is extractible in the binary

Protect your game: Godot

Interpreted language in an open source format

Game can be encrypted with an AES key

GdsDecomp dev won't give hints on how to extract it



GDKE

Key

Getting key, please wait...

8218D3DA81812C2442BA82014219042DFBF281

Close this window when done.

Entirely decompilable with GdsDecomp

Key is extractible in the binary

Someone else made a tool for it: gdke

Protect your game: Godot

Interpreted language in an open source format

Game can be encrypted with an AES key

GdsDecomp dev won't give hints on how to extract it

Entirely decompilable with GdsDecomp

Key is extractible in the binary

Someone else made a tool for it: gdke

```
Vector<uint8_t> p_key = raw_key.reverse();

std::transform(p_key.begin(), p_key.end(),
p_xor_key.begin(), p_key.begin(),
std::bit_xor<uint8_t>());
```

We can patch a few lines of the engine to fool the tool

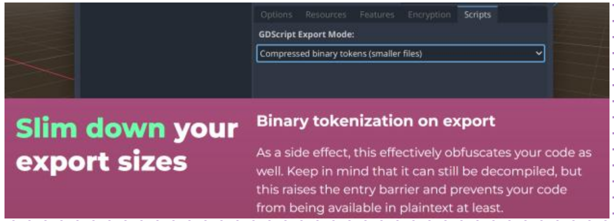
Protect your game: Godot

Interpreted language in an open source format

Game can be encrypted with an AES key

GdsDecomp dev won't give hints on how to extract it

We can patch a few lines of the engine to fool the tool


Options Resources Features Encryption Scripts

GDScript Export Mode:

Compressed binary tokens (smaller files)

Slim down your export sizes

Binary tokenization on export

As a side effect, this effectively obfuscates your code as well. Keep in mind that it can still be decompiled, but this raises the entry barrier and prevents your code from being available in plaintext at least.

Entirely decompilable with GdsDecomp

Key is extractible in the binary

Someone else made a tool for it: gdke

Always findable for a motivated hacker

Protect your game

- Obfuscate values in memory
- Obfuscate binaries
- Encrypt binaries and save files
- **Don’t trust the client:**
  check everything server side

I'd like to protect my game against reversers, make it harder to break my game
to deter script kiddies, easy hacks...
NOOO IT'S USELESS!
ENCRYPTION, OBFUSCATION, ANTI-CHEAT, ALL POINTLESS!
HACKERS GONNA HACK, YOUR GAME IS DOOMED, OPEN SOURCE IT ALREADY

Anti cheat Softwares

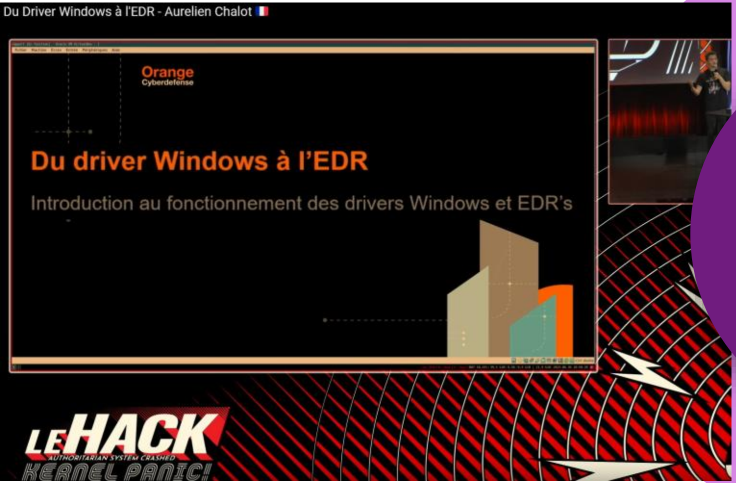
easy™ ANTI-CHEAT

DENUVO

BATTLEYE

V.A.C

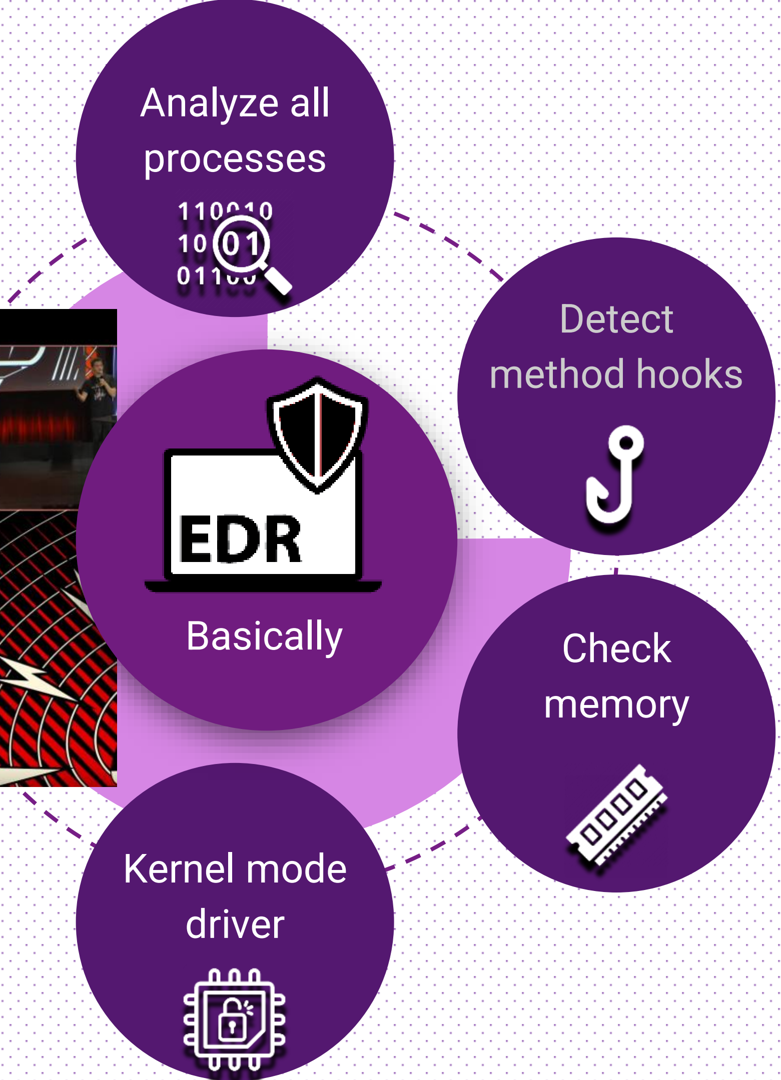
Anti cheat Softwares


Du Driver Windows à l'EDR - Aurelien Chalot 🇫🇷

Orange Cyberdefense

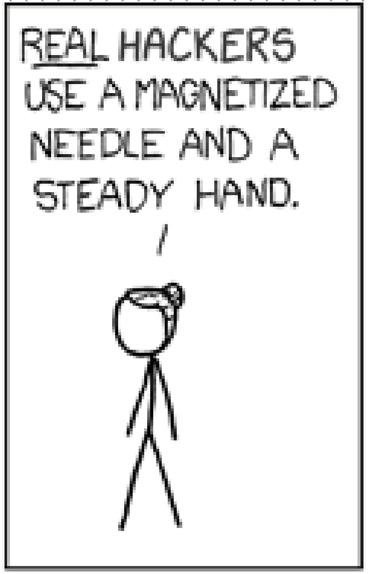
Du driver Windows à l'EDR

Introduction au fonctionnement des drivers Windows et EDR's



Advanced cheating: Undetectable.

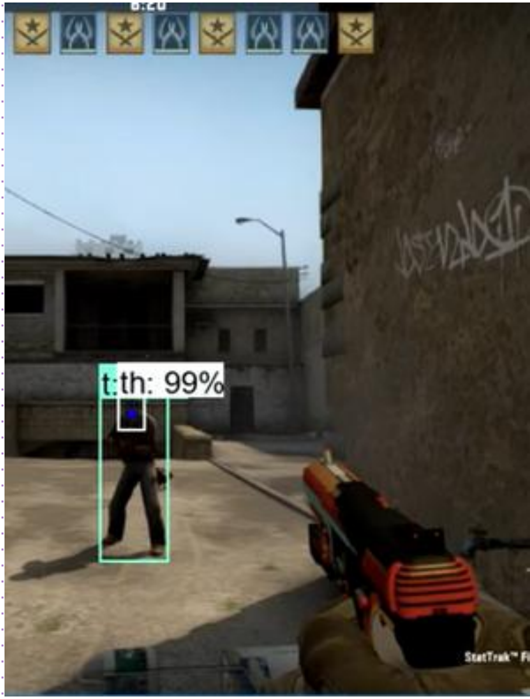
- Hardware level hacks, Harder to detect.



Advanced cheating: Undetectable.

- Hacks hardware,
  plus difficile à détecter.

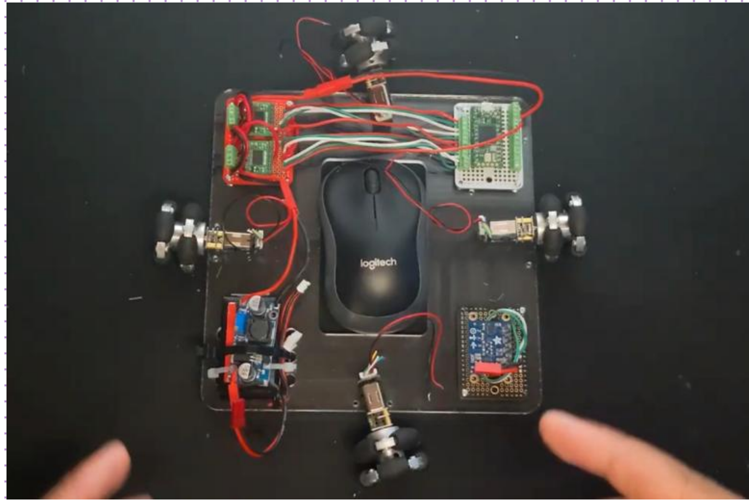
- **Screen reading tools (aimbot)**



Advanced cheating: Undetectable.

- Hardware level hacks,
  Harder to detect.

- **Screen reading tools (aimbot)**



Advanced cheating: Undetectable.

- Hardware level hacks,
  Harder to detect.

- Screen reading tools (aimbot)

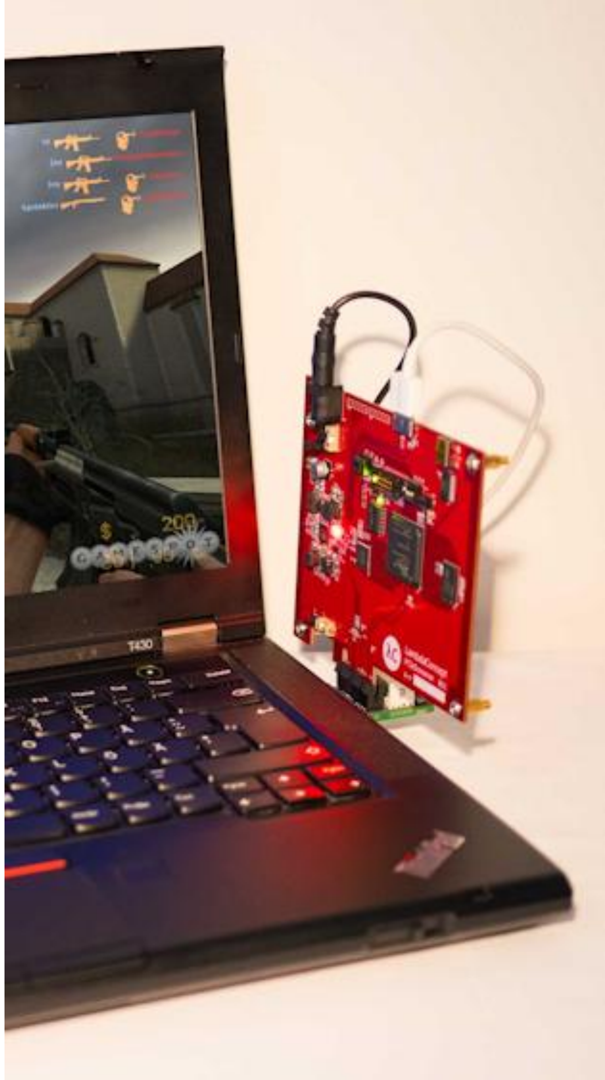
- **Online latency desynchronization**

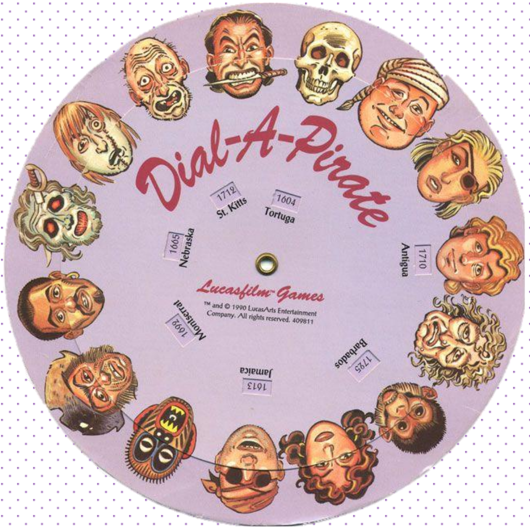
Advanced cheating: Undetectable.

- Hardware level hacks,
  Harder to detect.
- Screen reading tools (aimbot)
- **Online latency desynchronization**

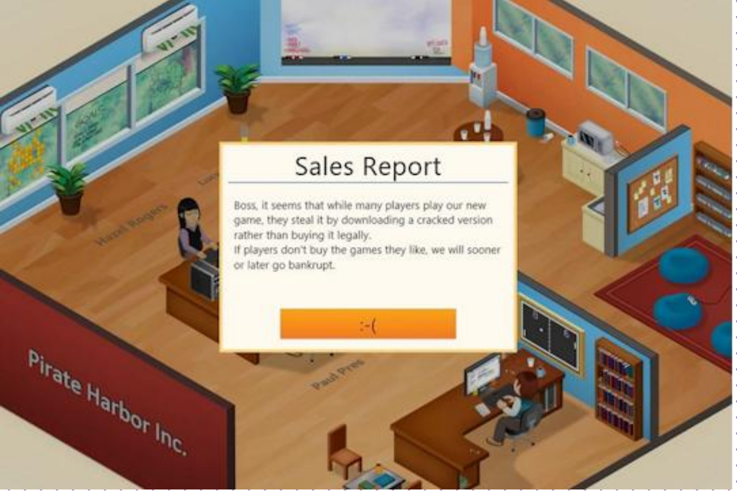
Advanced cheating: Undetectable.

- Hardware level hacks,
  Harder to detect.
- Screen reading tools (aimbot)
- Online latency desynchronization
- **Direct Memory Access via PCIE**





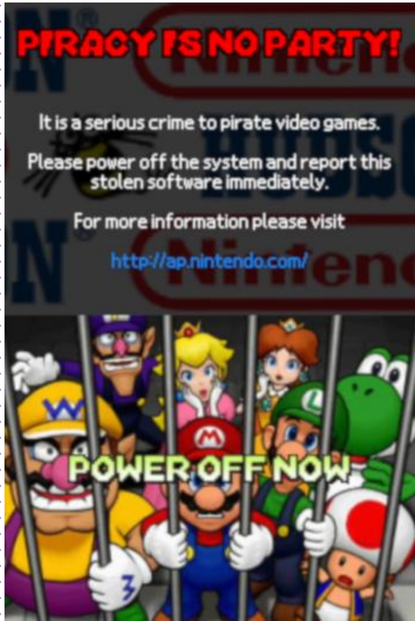
tuxlu.fr/talk_vghacking



Sales Report

Boss, it seems that while many players play our new game, they steal it by downloading a cracked version rather than buying it legally.
If players don't buy the games they like, we will sooner or later go bankrupt.

:-(



PIRACY IS NO PARTY!

It is a serious crime to pirate video games.

Please power off the system and report this stolen software immediately.

For more information please visit

http://ap.nintendo.com/

POWER OFF NOW

tuxlu.fr/talk_vghacking

thank you.

TXL