Game Hacking with Rust

Target Audience

- You should know how to program
- Systems Programming basics

You need to download:

- AssaultCube
- Rust
- VSCode with Rust Analyzer extension

Source Code

Available here:

https://github.com/not-matthias/game-hacking-workshop

or

https://shorturl.at/jmqrV

About Rust

- Types: `i16` vs `u16`
- Functions: `fn foo(bar: u32) -> i16 {}`
- Variables: `let mut temp = 42;`
- Run with: `cargo r` or `cargo run`

What is a pointer?

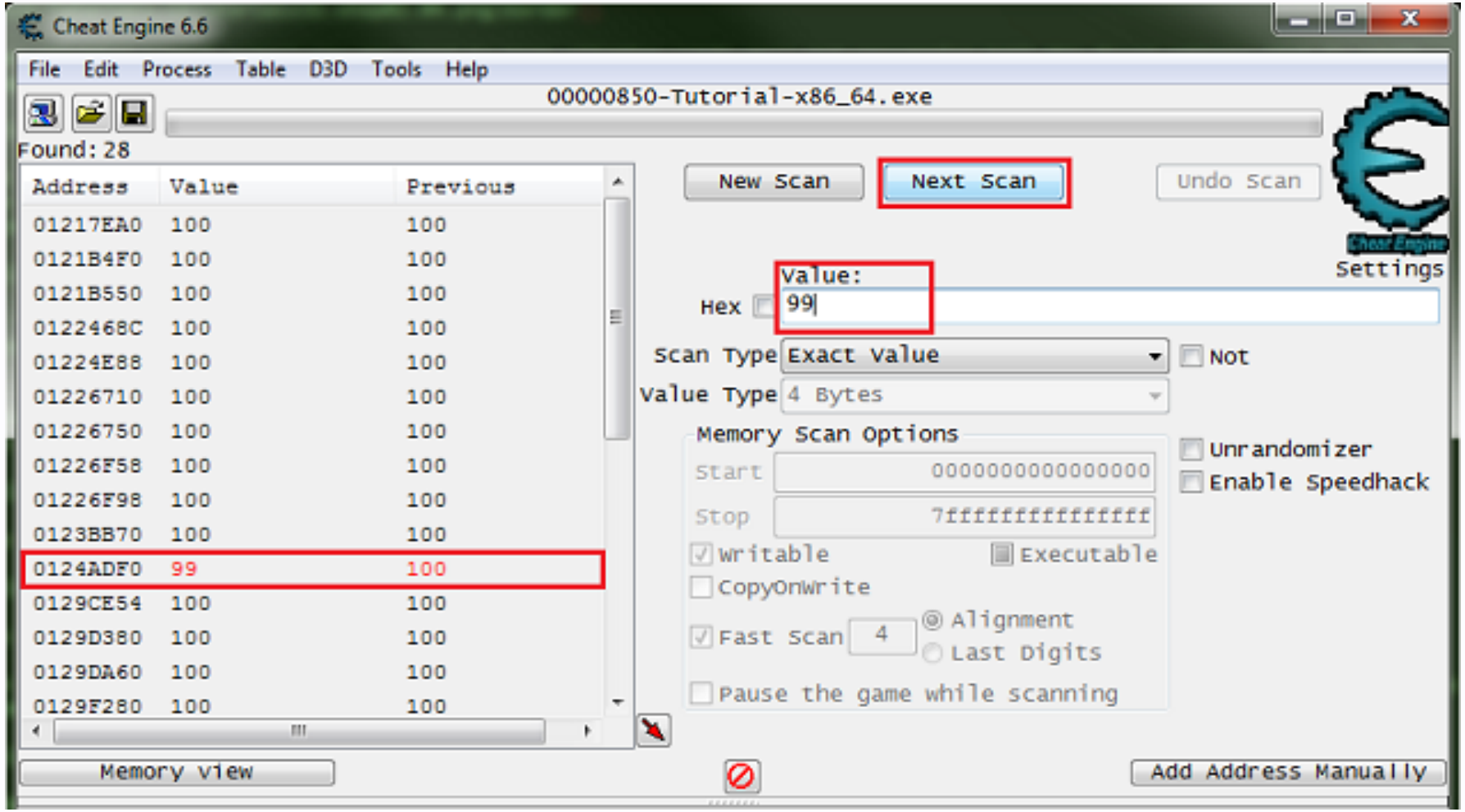
- Points to a memory location
- 64 Bit Process => 64 Bit pointers
- 32 Bit Process => 32 Bit pointers

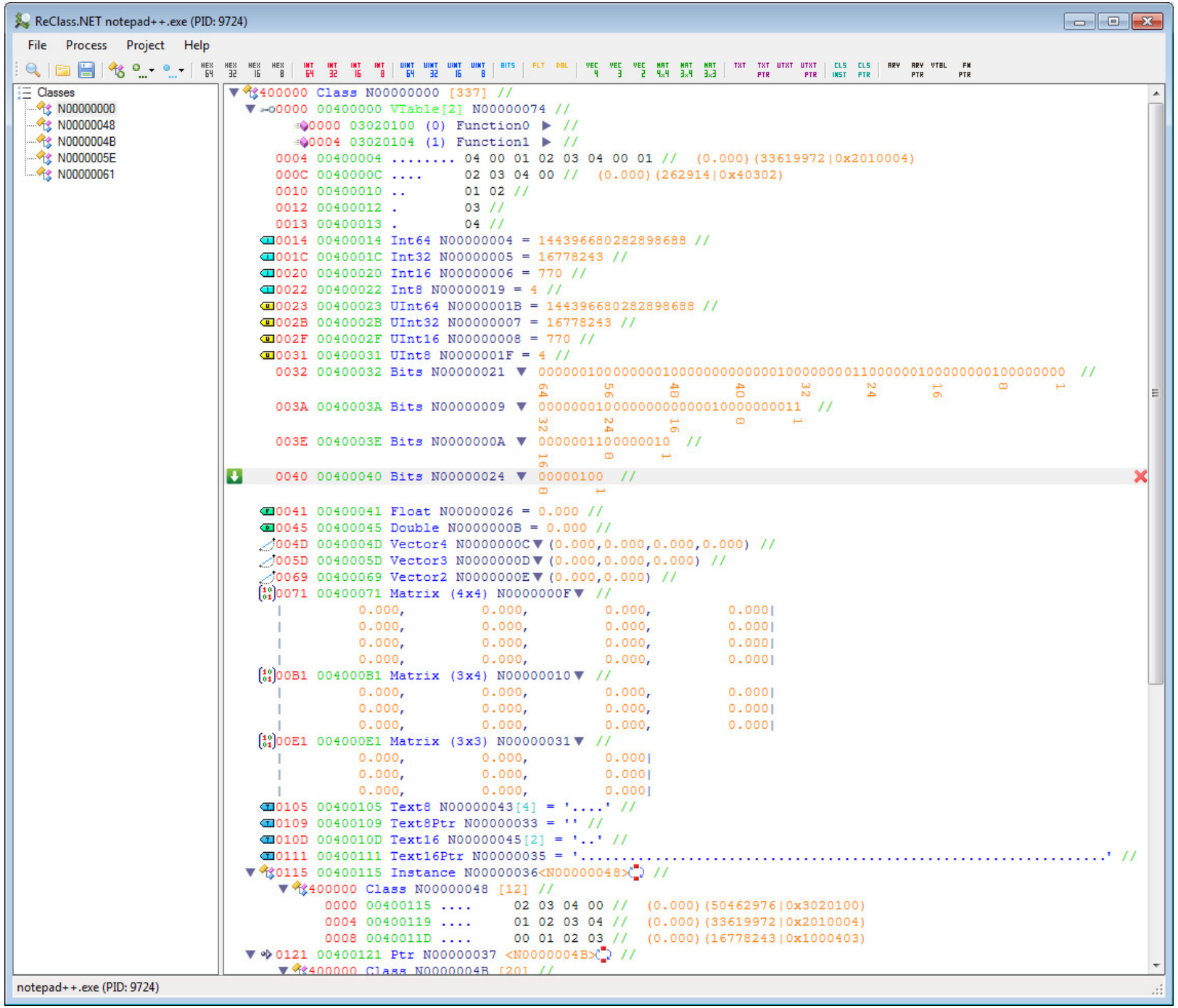
Let's get started

And this is just the start...

Useful tools

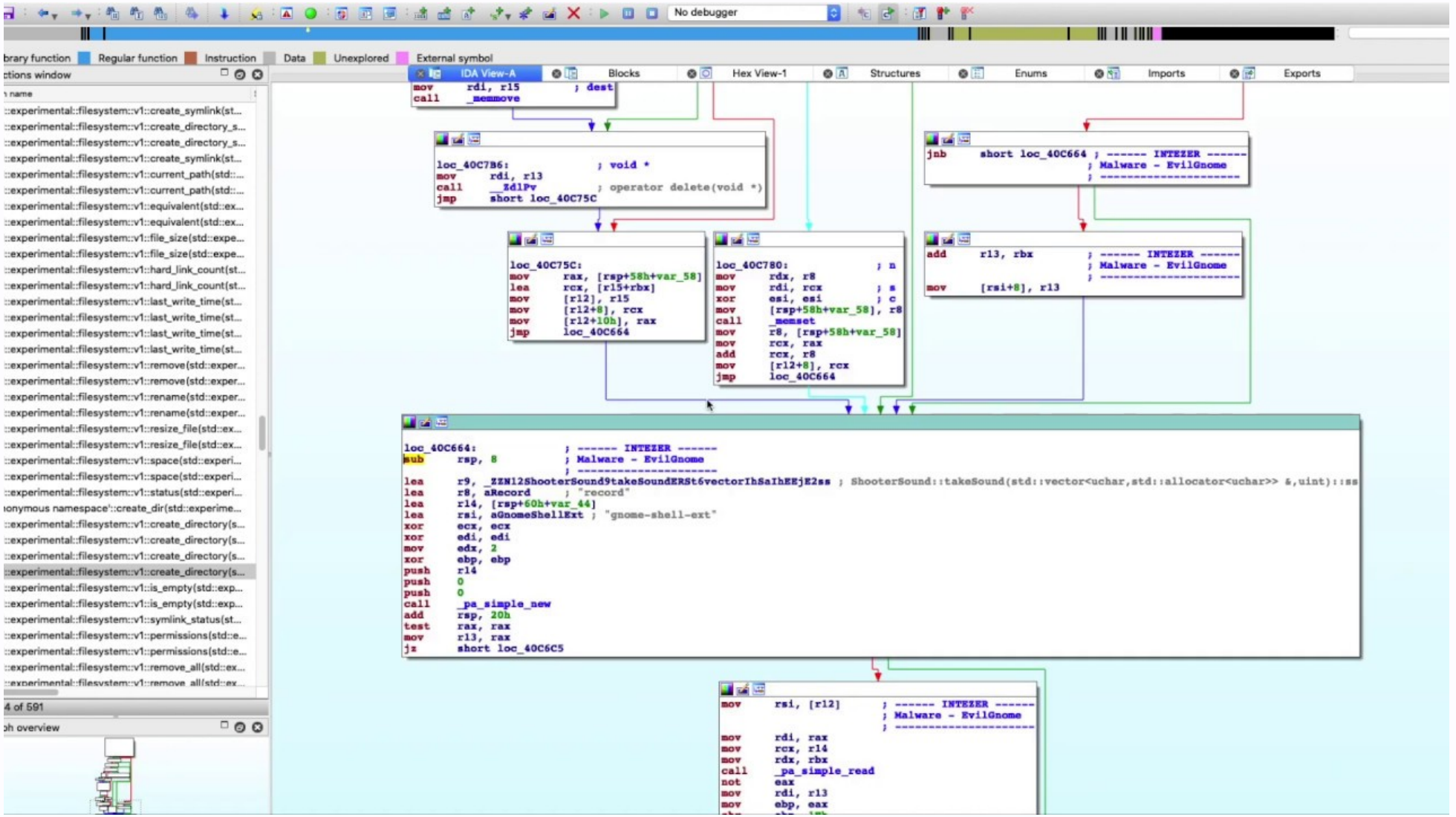
Cheat Engine

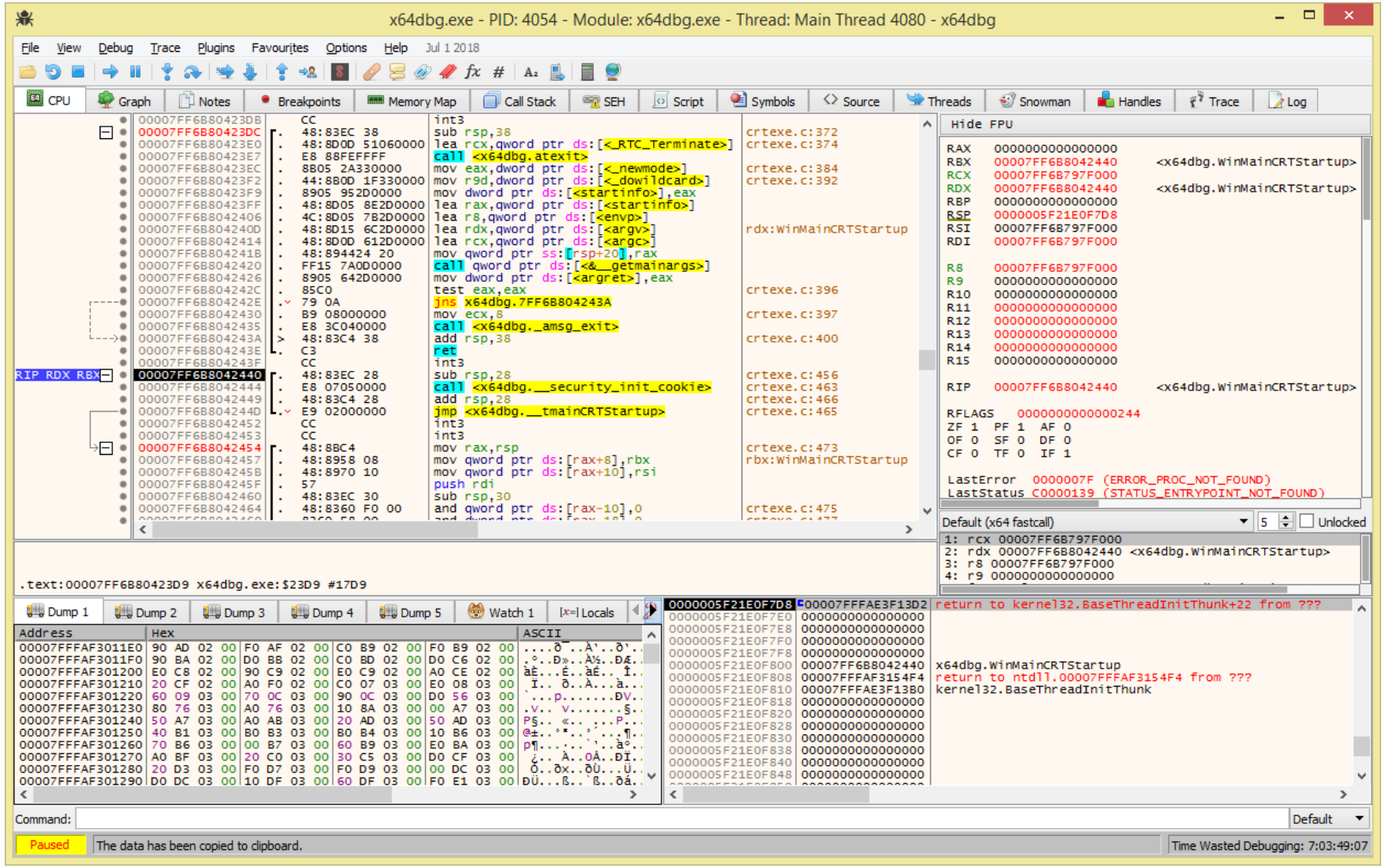



ReClass.NET notepad++.exe (PID: 9724)
File
Process
Project
Help
Classes
N00000000
N00000048
N0000004B
N0000005E
N00000061
notepad++.exe (PID: 9724)

Reclass

IDA


No debugger
Regular function
Instruction
Data
Unexplored
External symbol
IDA View-A
Blocks
Hex View-1
Structures
Enums
Imports
Exports
loc_40C7B6:
loc_40C75C:
loc_40C780:
loc_40C664:
jnb short loc_40C664 ; ------ INTEZER ------
; Malware - EvilGnome
add r13, rbx
mov [rsi+8], r13
lea r9, _ZZN12ShooterSound9takeSoundERSt6vectorIhSaIhEEjE2ss ; ShooterSound::takeSound(std::vector<uchar,std::allocator<uchar>> &,uint)::ss
lea r8, aRecord ; "record"
lea rsi, aGnomeShellExt ; "gnome-shell-ext"
call _pa_simple_new
call _pa_simple_read
jz short loc_40C6C5


x64dbg.exe - PID: 4054 - Module: x64dbg.exe - Thread: Main Thread 4080 - x64dbg
File View Debug Trace Plugins Favourites Options Help Jul 1 2018
CPU Graph Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source Threads Snowman Handles Trace Log
Hide FPU
RAX 0000000000000000
RBX 00007FF6B8042440 <x64dbg.WinMainCRTStartup>
RCX 00007FF6B797F000
RDX 00007FF6B8042440 <x64dbg.WinMainCRTStartup>
RBP 0000000000000000
RSP 0000005F21E0F7D8
RSI 00007FF6B797F000
RDI 00007FF6B797F000
R8 00007FF6B797F000
R9 0000000000000000
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00007FF6B8042440 <x64dbg.WinMainCRTStartup>
RFLAGS 0000000000000244
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
LastError 0000007F (ERROR_PROC_NOT_FOUND)
LastStatus C0000139 (STATUS_ENTRYPOINT_NOT_FOUND)
Default (x64 fastcall)
Unlocked
1: rcx 00007FF6B797F000
2: rdx 00007FF6B8042440 <x64dbg.WinMainCRTStartup>
3: r8 00007FF6B797F000
4: r9 0000000000000000
.text:00007FF6B80423D9 x64dbg.exe:$23D9 #17D9
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals
Address Hex ASCII
Command:
Default
Paused
The data has been copied to clipboard.
Time Wasted Debugging: 7:03:49:07

x64Dbg

More ideas

- Read enemy positions -> Radar or ESP
- Aimbot
- Movement Speed multiplier
- No Recoil / Spread

Anticheats

- EasyAntiCheat
- Battleye
- Vangard
- ...

Binary Analysis

- Deobfuscation
- Devirtualization
- ...

Recommended Resources

- gamehacking.academy
- unknowncheats.me
- github.com/hax-rs
- /r/ReverseEngineering
- Discord Servers
  - Rust RE
  - hax-rs
  - Reverse Engineering