

Reverse Engineering

Week 3: C++, More Difficult Algorithms, Don't RE what you don't have to

John Berry, Sergey Bratus -- Dartmouth College -- Winter 2022



Overview

What & Why

- Function Pointers
 - You saw a little with the jump table for switches
- C++
 - With things like virtual functions and name mangling this is a different beast

Motivation

Cool RE

- http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf
- This example is more than just reverse engineering and their story is funny. They wanted to give a talk but the MBTA tried to silence them.
 - <https://www.discovermagazine.com/technology/mit-students-who-hacked-boston-subway-silenced-report-gets-out-anyway>
 - Streisand effect

Function Pointers

What & Why

- Like regular pointers but they point to executable code.
- Allows a programmer to dynamically select functions to execute
- Will show up in assembly as: *call <register>*

Function Pointers

```
#include <stdio.h>
#include <stdlib.h>
|
void even() { printf("Even\n"); }
void odd() { printf("Odd\n"); }

int main(int argc, char **argv)
{
    if (argc != 2) {
        exit(0);
    }

    void (*parity)() = NULL;

    int x = atoi(argv[1]);

    if (x % 2) {
        parity = &odd;
    } else {
        parity = &even;
    }

    parity();
}

return 0;
}
"function_pointer.c" 26L, 334C written
```

Function Pointer

Listing

| | | | | XREF[1]: | | |
|----------|-------------------------|------|------------------------------------|----------|-------------|--|
| | | | LAB_001011da | | | |
| 001011da | 48 c7 45 f8 00 00 00 00 | MOV | qword ptr [RBP + parity],0x0 | XREF[1]: | 001011ce(j) | |
| 001011e2 | 48 8b 45 e0 | MOV | RAX,qword ptr [RBP + argv] | | | |
| 001011e6 | 48 83 c0 08 | ADD | RAX,0x8 | | | |
| 001011ea | 48 8b 00 | MOV | RAX,qword ptr [RAX] | | | |
| 001011ed | 48 89 c7 | MOV | RDI,RAX | | | |
| 001011f0 | e8 8b fe ff ff | CALL | <EXTERNAL>::atoi | | | |
| 001011f5 | 89 45 f4 | MOV | dword ptr [RBP + arg1_val],EAX | | | |
| 001011f8 | 8b 45 f4 | MOV | EAX,dword ptr [RBP + arg1_val] | | | |
| 001011fb | 83 e0 01 | AND | EAX,0x1 | | | |
| 001011fe | 85 c0 | TEST | EAX,EAX | | | |
| 00101200 | 74 0d | JZ | LAB_0010120f | | | |
| 00101202 | 48 8d 05 | LEA | RAX,[even] | | | |
| | 80 ff ff ff | | | | | |
| 00101209 | 48 89 45 f8 | MOV | qword ptr [RBP + parity],RAX=>even | | | |
| 0010120d | eb 0b | JMP | LAB_0010121a | | | |
| | | | LAB_0010120f | XREF[1]: | 00101200(j) | |
| 0010120f | 48 8d 05 | LEA | RAX,[odd] | | | |
| | 8a ff ff ff | | | | | |
| 00101216 | 48 89 45 f8 | MOV | qword ptr [RBP + parity],RAX=>odd | | | |
| | | | LAB_0010121a | XREF[1]: | 0010120d(j) | |
| 0010121a | 48 8b 55 f8 | MOV | RDX,qword ptr [RBP + parity] | | | |
| 0010121e | b8 00 00 00 00 | MOV | EAX,0x0 | | | |
| 00101223 | ff d2 | CALL | RDX=>even | | | |
| 00101225 | b8 00 00 00 00 | MOV | EAX,0x0 | | | |

C++

What

- C++ has some features that make reverse engineering it bit more difficult
- Classes
 - Like structures but with functions, and more complicated rules of access
- Vftables
 - A Virtual Function Table is an array of function pointers for the virtual functions of a class.
- Polymorphism and Class Inheritance
 - Results in multiple vftables and a more complex organization of the data structure
- Constructors / Destructors

C++

Identification

- How to know if you are up against a C++ binary?
 - Lots of usage of RDI-relative addressing in g++-compiled binaries, RCX in Windows binaries.
 - Contains the *this* pointer when calling class functions
 - You may see some weird mangled functions names like:
 - `_ZStlslSt11char_traitslcERSt13basic_ostreamlcT_ES5_PKc`

C++

Demangling

- The mangled names mentioned earlier are not actually a C++ standard. Each C++ compiler has their own format
 - Wikipedia article on Name Mangling has good examples
- Fortunately, Ghidra, Binary Ninja, and IDA can all demangle mostly automatically

CodeBrowser: COSC169:/helloworld

C++

Demangling

Listing: helloworld

```
***** THUNK FUNCTION *****
thunk undefined frame_dummy()
    Thunked-Function: register_tm_clones
    AL:1 <RETURN>
frame_dummy
XREF[3]: Entry Point(*),
          _libc_csu_init:001012a9(c),
          00103d78(*)

001011a0 f3 0f 1e fa    ENDBR64
001011a4 e9 77 ff      JMP     register_tm_clones
                        ff ff
-- Flow Override: CALL_RETURN (CALL_TERMINATOR)

***** FUNCTION *****
undefined main()
AL:1 <RETURN>
Stack[-0xc]:4 local_c
Stack[-0x18]:8 local_18
main
XREF[4]: Entry Point(*),
          _start:001010e1(*), 00102040,
          001020f8(*)

001011a9 f3 0f 1e fa    ENDBR64
001011ad 55             PUSH    RBP
001011ae 48 89 e5       MOV     RBP,RSP
001011b1 48 83 ec 10   SUB    RSP,0x10
001011b5 89 7d fc       MOV    dword ptr [RBP + local_c],EDI
001011b8 48 89 75 f0   MOV    qword ptr [RBP + local_18],RSI
001011bc 48 8d 35       LEA    RSI,[s_Hello_world_00102005]
                        42 0e 00 00
001011c3 48 8d 3d       LEA    RDI,[std::cout]
                        76 2e 00 00
001011ca e8 c1 fe     CALL   <EXTERNAL>::std::operator<<
                        ff ff
001011cf 48 89 c2       MOV    RDX,RAX
001011d2 48 b8 05       MOV    RAX,qword ptr [-><EXTERNAL>::std::endl<char,std::char_traits<char>>]
                        f7 2d 00 00
001011d9 48 89 c6       MOV    RSI=><EXTERNAL>::std::endl<char,std::char_traits<char>>,RAX
001011dc 48 89 d7       MOV    RDI,RDX
001011df e8 bc fe     CALL   <EXTERNAL>::std::basic_ostream<char,std::char_traits<char>>::operator<<
                        ff ff
001011e4 b8 00 00       MOV    EAX,0x0
                        00 00
001011e9 c9             LEAVE
001011ea c3             RET

***** _static_initialization_and_destruction_0(int, int) *****
undefined __stdcall __static_initialization_and_destruct...
AL:1 <RETURN>
int    EDI:4 param_1
int    ESI:4 param_2
Stack[-0xc]:4 local_c
Stack[-0x10]:4 local_10
_Z41__static_initialization_and_destruction_0ii XREF[3]: _GLOBAL_sub_I_main:0010124a(c),
                                                _static_initialization_and_destruction_0
                                                XREF[2]: 001011f7(W),
                                                001011fd(R)
                                                001011fa(W),
                                                00101203(R)
001011eb f3 0f 1e fa    ENDBR64
001011ef 55             PUSH    RBP
```

C++

Classes

- You likely know what classes are already but what do they look like in memory?
- Let's take a look at a basic example

C++

Example

john@caesar: ~/recourse/week03

```
class Person {  
private:  
    std::string name;  
    int age;  
  
public:  
    virtual void setName( std::string name ) { this->name = name; };  
    virtual void setAge( int age ) { this->age = age; };  
    virtual std::string getName( void ) { return this->name; };  
    virtual int getAge( void ) { return this->age; };
```

}

2

2

2

2

9

2

2

6

2

2

2

"class_layout.hpp" 11L, 319C

5,0-1

All

C++

Example

```
#include <iostream>
#include "class_layout.hpp"

int main(int argc, char **argv)
{
    Person *bob = new Person;

    bob->setName("bob");
    bob->setAge(42);

    std::cout << "Name: " << bob->getName() << " Age: " << bob->getAge() << std::endl;

    return 0;
}
```

Cookies: A Segue

Not just bad for
your teeth

Listing: class_layout - (13 addresses selected)

```

undefined4     Stack[-0x5c]:4 local_5c          001013ae(*)
undefined8     Stack[-0x68]:8 local_68          XREF[1]: 00101336(W)
                                                       XREF[1]: 00101339(W)
                                                       main      XREF[7]: Entry Point(*),
                                                       _start:00101261(*), 0010204c,
                                                       001021f0(*), 001022b6(*),
                                                       001022c5(*), 001022d0(*)

00101329 f3 Of 1e fa    ENDBR64
0010132d 55             PUSH    RBP
0010132e 48 89 e5      MOV     RBP,RSP
00101331 53             PUSH    RBX
00101332 48 83 ec 58   SUB    RSP,0x58
00101336 89 7d ac      MOV     dword ptr [RBP + local_5c],EDI
00101339 48 89 75 a0   MOV     qword ptr [RBP + local_68],RSI
0010133d 64 48 8b      MOV     RAX,qword ptr FS:[0x28]
04 25 28
00 00 00
00101346 48 89 45 e8   MOV     qword ptr [RBP + local_20],RAX
0010134a 31 c0          XOR    EAX,EAX
0010134c bf 30 00      MOV     EDI,0x30
00 00

LAB_00101351           CALL   <EXTERNAL>::operator.new
00101351 e8 4a fe      ff ff
00101356 48 89 c3      MOV     RBX,RAX
00101359 48 89 df      MOV     RDI,RBX
0010135c e8 77 02      CALL   Person::Person
00 00
00101361 48 89 5d b8   MOV     qword ptr [RBP + local_50],RBX
00101365 48 8b 45 b8   MOV     RAX,qword ptr [RBP + local_50]
00101369 48 8b 00      MOV     RAX,qword ptr [RAX]
0010136c 48 8b 18      MOV     RBX,qword ptr [RAX]
0010136f 48 8d 45 b7   LEA    RAX=>local_51,[RBP + -0x49]
00101373 48 89 c7      MOV     RDI,RAX
00101376 e8 b5 fe      CALL   <EXTERNAL>::std::allocator<char>::allocator
ff ff
0010137b 48 8d 55 b7   LEA    RDX=>local_51,[RBP + -0x49]
0010137f 48 8d 45 c0   LEA    RAX=>local_48,[RBP + -0x40]
00101383 48 8d 35      LEA    RSI,[DAT_00102005]
7b 0c 00 00
0010138a 48 89 c7      MOV     RDI,RAX

try { // try from 0010138d to 00101391 has its CatchHandler @...
LAB_0010138d           CALL   <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::basic_string
0010138d e8 4e fe      ff ff
                                                       XREF[1]: 001022b8(*)
} // end try from 0010138d to 00101391
00101392 48 8d 55 c0   LEA    RDX=>local_48,[RBP + -0x40]
00101396 48 8b 45 b8   MOV     RAX,qword ptr [RBP + local_50]
0010139a 48 89 d6      MOV     RSI,RDX
0010139d 48 89 c7      MOV     RDI,RAX

try { // try from 001013a0 to 001013a1 has its CatchHandler @...
LAB_001013a0           CALL   RBX
001013a0 ff d3          CALL   RBX
                                                       XREF[1]: 001022bd(*)
} // end try from 001013a0 to 001013a1
001013a2 48 8d 45 c0   LEA    RAX=>local_48,[RBP + -0x40]
001013a6 48 89 c7      MOV     RDI,RAX
001013a9 e8 b2 fd      CALL   <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::~basic_string
ff ff
001013ae 48 8d 45 b7   LEA    RAX=>local_51,[RBP + -0x49]
001013b2 48 89 c7      MOV     RDT,RAX
= 62h      b
void * operator.new(ulong param_1)
undefined Person(Person * this)
undefined allocator(void)

```

Cookies: A Segue

Not just bad for
your teeth

CodeBrowser: COSC169:/class_layout

Listing: class_layout - (17 addresses selected)

| Address | OpCode | Operands | Description |
|----------|----------------------------|--|--|
| 00101405 | 48 89 c7 | MOV RDI,RAX | |
| 00101408 | ff d1 | CALL RCX | |
| 0010140a | 48 8d 45 c0 | LEA RAX=>local_48,[RBP + -0x40] | |
| 0010140e | 48 89 c6 | MOV RSI,RAX | |
| 00101411 | 48 89 df | MOV RDI,RBX | |
| 00101414 | e8 67 fd ff ff | CALL <EXTERNAL>::std::operator<< | try { // try from 00101414 to 00101460 has its CatchHandler @... |
| 00101419 | 48 8d 35 f0 0b 00 00 | LEA RSI,[s__Age:_00102010] | XREF[1]: 001022c7(*) |
| 00101420 | 48 89 c7 | MOV RDI,RAX | basic_ostream * operator<<(basic... |
| 00101423 | e8 68 fd ff ff | CALL <EXTERNAL>::std::operator<< | = " Age: " |
| 00101428 | 48 89 c3 | MOV RBX,RAX | basic_ostream * operator<<(basic... |
| 0010142b | 48 8b 45 b8 | MOV RAX,qword ptr [RBP + local_50] | |
| 0010142f | 48 8b 00 | MOV RAX,qword ptr [RAX] | |
| 00101432 | 48 83 c0 18 | ADD RAX,0x18 | |
| 00101436 | 48 8b 10 | MOV RDX,qword ptr [RAX] | |
| 00101439 | 48 8b 45 b8 | MOV RAX,qword ptr [RBP + local_50] | |
| 0010143d | 48 89 c7 | MOV RDI,RAX | |
| 00101440 | ff d2 | CALL RDX | |
| 00101442 | 89 c6 | MOV ESI,EAX | |
| 00101444 | 48 89 df | MOV RDI,RBX | |
| 00101447 | e8 c4 fd ff ff | CALL <EXTERNAL>::std::basic_ostream<char,std::char_traits<char>>::operator<< | undefined operator<<(basic_ostre... |
| 0010144c | 48 89 c2 | MOV RDX,RAX | |
| 0010144f | 48 8b 05 7a 2b 00 00 | MOV RAX,qword ptr [-><EXTERNAL>::std::endl<char,std::char_traits<char>>] | = 00105010 |
| 00101456 | 48 89 c6 | MOV RST=><EXTERNAL>::std::endl<char,std::char_traits<char>>,RAX | = ?? |
| 00101459 | 48 89 d7 | MOV RDI,RDX | |
| 0010145c | e8 4f fd ff ff | CALL <EXTERNAL>::std::basic_ostream<char,std::char_traits<char>>::operator<< | undefined operator<<(basic_ostre... |
| 00101461 | 48 8d 45 c0 | LEA RAX=>local_48,[RBP + -0x40] | |
| 00101465 | 48 89 c7 | MOV RDI,RAX | |
| 00101468 | e8 f3 fc ff ff | CALL <EXTERNAL>::std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::__basic_stri... | undefined ~basic_string(basic_st... |
| 0010146d | b8 00 00 00 00 | MOV EAX,0x0 | |
| 00101472 | 48 8b 4d e8 | MOV RCX,qword ptr [RBP + cookie] | |
| 00101476 | 64 48 33 0c 25 28 00 00 00 | XOR RCX,qword ptr FS:[0x28] | |
| 0010147f | 74 58 | JZ LAB_001014d9 | |
| 00101481 | eb 51 | JMP LAB_001014d4 | |
| 00101483 | f3 0f 1e fa | catch() { ... } // from try @ 001013a0 with catch @ 00101483 XREF[1]: 001022bf(*) | |
| 00101487 | ENDBR64 | | |
| 0010148a | 48 8d 45 c0 | MOV RBX,RAX | |
| 0010148e | 48 89 c7 | LEA RAX,[RBP + -0x40] | |
| 00101491 | e8 ca fc ff ff | MOV RDI,RAX | |
| 00101496 | eb 07 | CALL <EXTERNAL>::std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::__basic_stri... | undefined ~basic_string(basic_st... |
| 00101498 | f3 0f 1e fa | JMP LAB_0010149f | |
| 0010149c | ENDBR64 | | |
| 0010149e | 48 89 c3 | MOV RBX,RAX | |

Cookies: A Segue

Not just bad for
your teeth

CodeBrowser: COSC169:/class_layout

File Edit Analysis Graph Navigation Search Select Tools Window Help

I D U L F R V B

Listing: class_layout - (5 addresses selected)

| Address | OpCode | Operands | Description | XREF |
|--|----------------|---|--|---|
| 00101498 | f3 0f 1e fa | ENDBR64 | | XREF[1]: 001022ba(*) |
| 0010149c | 48 89 c3 | MOV RBX, RAX | | |
| 0010149f | 48 8d 45 b7 | LEA RAX, [RBP + -0x49] | | XREF[1]: 00101496(j) |
| 001014a3 | 48 89 c7 | MOV RDI, RAX | | |
| 001014a6 | e8 15 fd ff ff | CALL <EXTERNAL>::std::allocator<char>::~allocator | | undefined ~allocator(allocator<c...) |
| 001014ab | 48 89 d8 | MOV RAX, RBX | | |
| 001014ae | 48 89 c7 | MOV RDI, RAX | | |
| 001014b1 | e8 6a fd ff ff | CALL <EXTERNAL>::_Unwind_Resume | -- Flow Override: CALL_RETURN (CALL_TERMINATOR) | XREF[1]: 001022cd(*) undefined _Unwind_Resume() |
| 001014b6 | f3 0f 1e fa | ENDBR64 | catch() { ... } // from try @ 00101414 with catch @ 001014b6 | XREF[1]: 001022ca(*) |
| 001014ba | 48 89 c3 | MOV RBX, RAX | | |
| 001014bd | 48 8d 45 c0 | LEA RAX, [RBP + -0x40] | | |
| 001014c1 | 48 89 c7 | MOV RDI, RAX | | |
| 001014c4 | e8 97 fc ff ff | CALL <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::~basic_string(basic_st...) | | undefined ~basic_string(basic_st...) |
| 001014c9 | 48 89 d8 | MOV RAX, RBX | | |
| 001014cc | 48 89 c7 | MOV RDI, RAX | | |
| 001014cf | e8 4c fd ff ff | CALL <EXTERNAL>::_Unwind_Resume | -- Flow Override: CALL_RETURN (CALL_TERMINATOR) | undefined _Unwind_Resume() |
| 001014d4 | e8 f7 fc ff ff | CALL <EXTERNAL>::_stack_chk_fail | -- Flow Override: CALL_RETURN (CALL_TERMINATOR) | XREF[1]: 00101481(j) undefined _stack_chk_fail() |
| 001014d9 | 48 83 c4 58 | ADD RSP, 0x58 | | XREF[1]: 0010147f(j) |
| 001014dd | 5b | POP RBX | | |
| 001014de | 5d | POP RBP | | |
| 001014df | c3 | RET | | |
| ***** | | | | |
| * static_initialization_and_destruction_0(int, int) * | | | | |
| ***** | | | | |
| undefined | AL:1 | <RETURN> | | |
| int | EDI:4 | param_1 | | |
| int | ESI:4 | param_2 | | |
| undefined4 | Stack[-0xc]:4 | local_c | XREF[2]: 001014ec(W), 001014f2(R) | |
| undefined4 | Stack[-0x10]:4 | local_10 | XREF[2]: 001014ef(W), 001014f8(R) | |
| _Z41_static_initialization_and_destruction_0ii XREF[3]: _GLOBAL__sub_I_main:0010153f(c), _static_initialization_and_destruction_0 | | | | |
| 001014e0 | f3 0f 1e fa | ENDBR64 | | 00102054, 00102218(*) |
| 001014e4 | 55 | PUSH RBP | | |
| 001014e5 | 48 89 e5 | MOV RBP, RSP | | |
| 001014e8 | 48 83 ec 10 | SUB RSP, 0x10 | | |
| 001014ec | 89 7d fc | MOV dword ptr [RBP + local_c], param_1 | | |
| 001014ef | 89 75 f8 | MOV dword ptr [RBP + local_10], param_2 | | |
| 001014f2 | 83 7d fc 01 | CMP dword ptr [RBP + local_c], 0x1 | | |

001014d4 main CALL 0x001011d0

CodeBrowser: COSC169:/class_layout

C++

Allocation

Listing: class_layout - (10 addresses selected)

| Address | OpCode | Operands | Description | References |
|----------|----------------|---|----------------------|-------------------------------------|
| 00101329 | f3 0f 1e fa | ENDBR64 | | |
| 0010132d | 55 | PUSH RBP | | |
| 0010132e | 48 89 e5 | MOV RBP,RSP | | |
| 00101331 | 53 | PUSH RBX | | |
| 00101332 | 48 83 ec 58 | SUB RSP,0x58 | | |
| 00101336 | 89 7d ac | MOV dword ptr [RBP + local_5c],EDI | | |
| 00101339 | 48 89 75 a0 | MOV qword ptr [RBP + local_68],RSI | | |
| 0010133d | 64 48 8b | MOV RAX,qword ptr FS:[0x28] | | |
| | 04 25 28 | | | |
| | 00 00 00 | | | |
| 00101346 | 48 89 45 e8 | MOV qword ptr [RBP + cookie],RAX | | |
| 0010134a | 31 c0 | XOR EAX,EAX | | |
| 0010134c | bf 30 00 | MOV EDI,0x30 | | |
| | 00 00 | | | |
| 00101351 | e8 4a fe ff ff | CALL LAB_00101351 <EXTERNAL>::operator.new | XREF[1]: 001022b4(*) | void * operator.new(ulong param_1) |
| 00101356 | 48 89 c3 | MOV RBX,RAX | | |
| 00101359 | 48 89 df | MOV RDI,RBX | | |
| 0010135c | e8 77 02 | CALL Person::Person | | undefined Person(Person * this) |
| | 00 00 | | | |
| 00101361 | 48 89 5d b8 | MOV qword ptr [RBP + local_50],RBX | | |
| 00101365 | 48 8b 45 b8 | MOV RAX,qword ptr [RBP + local_50] | | |
| 00101369 | 48 8b 00 | MOV RAX,qword ptr [RAX] | | |
| 0010136c | 48 8b 18 | MOV RBX,qword ptr [RAX] | | |
| 0010136f | 48 8d 45 b7 | LEA RAX=>local_51,[RBP + -0x49] | | |
| 00101373 | 48 89 c7 | MOV RDI,RAX | | |
| 00101376 | e8 b5 fe ff ff | CALL <EXTERNAL>::std::allocator<char>::allocator | | undefined allocator(void) |
| 0010137b | 48 8d 55 b7 | LEA RDX=>local_51,[RBP + -0x49] | | |
| 0010137f | 48 8d 45 c0 | LEA RAX=>local_48,[RBP + -0x40] | | |
| 00101383 | 48 8d 35 | LEA RSI,[DAT_00102005] | | = 62h b |
| | 7b 0c 00 00 | | | |
| 0010138a | 48 89 c7 | MOV RDI,RAX | | |
| | | | | |
| 0010138d | e8 4e fe ff ff | CALL LAB_0010138d <EXTERNAL>::std::_cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::basic_string | XREF[1]: 001022b8(*) | undefined basic_string(char * pa... |
| | | | | |
| 00101392 | 48 8d 55 c0 | LEA RDX=>local_48,[RBP + -0x40] | | |
| 00101396 | 48 8b 45 b8 | MOV RAX,qword ptr [RBP + local_50] | | |
| 0010139a | 48 89 d6 | MOV RSI,RDX | | |
| 0010139d | 48 89 c7 | MOV RDI,RAX | | |
| | | | | |
| | | | | |

C++

Setting up the Vftable

Listing: class_layout - (18 addresses selected)

```

*****  

* Person::Person()  

*****  

undefined __thiscall Person(Person * this)  

    AL:1      <RETURN>  

    RDI:8 (auto)  this  

    Stack[-0x10]:8 local_10  

XREF[3]:  001015e4(W),  

          001015ef(R),  

          001015f6(R)  

_ZN6PersonC1Ev  

_ZN6PersonC2Ev  

Person::Person  

001015d8 f3 0f 1e fa  ENDBR64  

001015dc 55      PUSH   RBP  

001015dd 48 89 e5  MOV    RBP,RSP  

001015e0 48 83 ec 10 SUB   RSP,0x10  

001015e4 48 89 7d f8 MOV    qword ptr [RBP + local_10],this  

001015e8 48 8d 15 LEA    RDX,[PTR_setName_00103cf0]  

          01 27 00 00  

001015ef 48 8b 45 f8 MOV    RAX,qword ptr [RBP + local_10]  

001015f3 48 89 10 MOV    qword ptr [RAX],RDX=>PTR_setName_00103cf0  

001015f6 48 8b 45 f8 MOV    RAX,qword ptr [RBP + local_10]  

001015fa 48 83 c0 08 ADD   RAX,0x8  

001015fe 48 89 c7 MOV    this,RAX  

00101601 e8 ea fb CALL  <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::basic_string(void  

          ff ff  

00101606 90      NOP  

00101607 c9      LEAVE  

00101608 c3      RET  

00101609 0f      ??    0Fh  

0010160a 1f      ??    1Fh  

0010160b 80      ??    80h  

0010160c 00      ??    00h  

0010160d 00      ??    00h  

0010160e 00      ??    00h  

0010160f 00      ??    00h  

*****  

*           FUNCTION  

*****  

undefined __libc_csu_init()  

    AL:1      <RETURN>  

__libc_csu_init  

XREF[4]:  Entry Point(*),  

          _start:0010125a(*), 0010208c,  

          00102258(*)  

00101610 f3 0f 1e fa  ENDBR64  

00101614 41 57      PUSH   R15  

00101616 4c 8d 3d    LEA    R15,[__frame_dummy_init_array_entry]  

          ab 26 00 00  

0010161d 41 56      PUSH   R14  

0010161f 49 89 d6    MOV    R14,RDX  

00101622 41 55      PUSH   R13  

00101624 49 89 f5    MOV    R13,RSI  

00101627 41 54      PUSH   R12  

00101629 41 89 fc    MOV    R12D,EDI  

0010162c 55          PUSH   RBP  

0010162d 48 8d 2d    LEA    RBP,[__do_global_dtors_aux_fini_array_entry]  

          a4 26 00 00  

00101634 53          PUSH   RBX  

00101635 4c 29 fd    SUB   RBP,R15  

00101638 48 83 ec 08 SUB   RSP,0x8

```

001015f3 Person MOV qword ptr [RAX],RDX

C++

The Vftable

CodeBrowser: COSC169:/class_layout

File Edit Analysis Graph Navigation Search Select Tools Window Help

Listing: class_layout - (32 addresses selected)

| Address | Value | Type | Description |
|----------------------------------|--------------|-------------|--|
| 00103ce8 | 10 3d 10 | addr | Person::typeinfo |
| | 00 00 00 | | |
| | 00 00 | | |
| 00103cf0 | 46 15 10 | addr | Person::setName |
| | 00 00 00 | | |
| | 00 00 | | |
| 00103cf8 | 74 15 10 | addr | Person::setAge |
| | 00 00 00 | | |
| | 00 00 | | |
| 00103d00 | 90 15 10 | addr | Person::getName[abi:cxxl1] |
| | 00 00 00 | | |
| | 00 00 | | |
| 00103d08 | c2 15 10 | addr | Person::getAge |
| | 00 00 00 | | |
| | 00 00 | | |
| ***** | | | |
| * typeinfo for Person * | | | |
| ***** | | | |
| _ZTI6Person | | XREF[2]: | Entry Point(*), 00103ce8(*) |
| Person::typeinfo | | | |
| 00103d10 | 20 50 10 | addr | __cxxabiv1::__class_type_info::vtable |
| | 00 00 00 | | |
| | 00 00 | | |
| 00103d18 | 18 20 10 | addr | typeinfo-name |
| | 00 00 00 | | |
| | 00 00 | | |
| // | | | |
| // .dynamic | | | |
| // SHT_DYNAMIC [0x3d20 - 0x3f2f] | | | |
| // ram:00103d20-ram:00103f2f | | | |
| // | | | |
| _DYNAMIC | | | |
| 00103d20 | 01 00 00 | Elf64_Dy... | XREF[3]: 001001a0(*), 00103f30(*), _elfSectionHeaders::00000650(*) |
| | 00 00 00 | | |
| | 00 00 01 ... | | |
| 00103ef0 | 00 | ?? | 00h |
| 00103ef1 | 00 | ?? | 00h |
| 00103ef2 | 00 | ?? | 00h |
| 00103ef3 | 00 | ?? | 00h |
| 00103ef4 | 00 | ?? | 00h |
| 00103ef5 | 00 | ?? | 00h |
| 00103ef6 | 00 | ?? | 00h |
| 00103ef7 | 00 | ?? | 00h |
| 00103ef8 | 00 | ?? | 00h |
| 00103ef9 | 00 | ?? | 00h |
| 00103efa | 00 | ?? | 00h |
| 00103efb | 00 | ?? | 00h |
| 00103efc | 00 | ?? | 00h |
| 00103efd | 00 | ?? | 00h |
| 00103efe | 00 | ?? | 00h |
| 00103eff | 00 | ?? | 00h |
| 00103f00 | 00 | ?? | 00h |
| 00103f01 | 00 | ?? | 00h |
| 00103f02 | 00 | ?? | 00h |
| 00103f03 | 00 | ?? | 00h |
| 00103f04 | 00 | ?? | 00h |

DT_NEEDED - Name of needed library

C++

Setting up the Vftable

Listing: class_layout - (18 addresses selected)

```

*****  

* Person::Person()  

*****  

undefined __thiscall Person(Person * this)  

    AL:1      <RETURN>  

    RDI:8 (auto)  this  

    Stack[-0x10]:8 local_10  

XREF[3]:  001015e4(W),  

          001015ef(R),  

          001015f6(R)  

_ZN6PersonC1Ev  

_ZN6PersonC2Ev  

Person::Person  

001015d8 f3 0f 1e fa  ENDBR64  

001015dc 55      PUSH   RBP  

001015dd 48 89 e5  MOV    RBP,RSP  

001015e0 48 83 ec 10 SUB   RSP,0x10  

001015e4 48 89 7d f8 MOV    qword ptr [RBP + local_10],this  

001015e8 48 8d 15 LEA    RDX,[PTR_setName_00103cf0]  

          01 27 00 00  

001015ef 48 8b 45 f8 MOV    RAX,qword ptr [RBP + local_10]  

001015f3 48 89 10 MOV    qword ptr [RAX],RDX=>PTR_setName_00103cf0  

001015f6 48 8b 45 f8 MOV    RAX,qword ptr [RBP + local_10]  

001015fa 48 83 c0 08 ADD    RAX,0x8  

001015fe 48 89 c7 MOV    this,RAX  

00101601 e8 ea fb CALL   <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::basic_string(void  

          ff ff  

00101606 90      NOP  

00101607 c9      LEAVE  

00101608 c3      RET  

00101609 0f      ??    0Fh  

0010160a 1f      ??    1Fh  

0010160b 80      ??    80h  

0010160c 00      ??    00h  

0010160d 00      ??    00h  

0010160e 00      ??    00h  

0010160f 00      ??    00h  

*****  

*           FUNCTION  

*****  

undefined __libc_csu_init()  

    AL:1      <RETURN>  

__libc_csu_init  

XREF[4]:  Entry Point(*),  

          _start:0010125a(*), 0010208c,  

          00102258(*)  

00101610 f3 0f 1e fa  ENDBR64  

00101614 41 57      PUSH   R15  

00101616 4c 8d 3d LEA    R15,[__frame_dummy_init_array_entry]  

          ab 26 00 00  

0010161d 41 56      PUSH   R14  

0010161f 49 89 d6  MOV    R14,RDX  

00101622 41 55      PUSH   R13  

00101624 49 89 f5  MOV    R13,RSI  

00101627 41 54      PUSH   R12  

00101629 41 89 fc  MOV    R12D,EDI  

0010162c 55      PUSH   RBP  

0010162d 48 8d 2d LEA    RBP,[__do_global_dtors_aux_fini_array_entry]  

          a4 26 00 00  

00101634 53      PUSH   RBX  

00101635 4c 29 fd  SUB    RBP,R15  

00101638 48 83 ec 08 SUB   RSP,0x8

```

001015f3 Person MOV qword ptr [RAX],RDX

C++

Initializing the name string

Listing: class_layout - (16 addresses selected)

```

*****
* Person::Person()
*****
undefined __thiscall Person(Person * this)
    AL:1      <RETURN>
    RDI:8 (auto)  this
    Stack[-0x10]:8 local_10

    _ZN6PersonC1Ev
    _ZN6PersonC2Ev
    Person::Person

001015d8 f3 0f le fa    ENDBR64
001015dc 55              PUSH   RBP
001015dd 48 89 e5        MOV    RBP,RSP
001015e0 48 83 ec 10     SUB    RSP,0x10
001015e4 48 89 7d f8     MOV    qword ptr [RBP + local_10],this
001015e8 48 8d 15        LEA    RDX,[PTR_setName_00103cf0]
    01 27 00 00
001015ef 48 8b 45 f8     MOV    RAX,qword ptr [RBP + local_10]
001015f3 48 89 10        MOV    qword ptr [RAX],RDX=>PTR_setName_00103cf0
001015f6 48 8b 45 f8     MOV    RAX,qword ptr [RBP + local_10]
001015fa 48 83 c0 08     ADD    RAX,0x8
001015fe 48 89 c7        MOV    this,RAX
00101601 e8 ea fb ff ff CALL   <EXTERNAL>::std::__cxxl::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(void)

00101606 90              NOP
00101607 c9              LEAVE
00101608 c3              RET
00101609 0f              ??    0Fh
0010160a 1f              ??    1Fh
0010160b 80              ??    80h
0010160c 00              ??    00h
0010160d 00              ??    00h
0010160e 00              ??    00h
0010160f 00              ??    00h

*****
*          FUNCTION
*****
undefined __libc_csu_init()
    AL:1      <RETURN>
    __libc_csu_init

00101610 f3 0f le fa    ENDBR64
00101614 41 57            PUSH   R15
00101616 4c 8d 3d        LEA    R15,[__frame_dummy_init_array_entry]
    ab 26 00 00
0010161d 41 56            PUSH   R14
0010161f 49 89 d6        MOV    R14,RDX
00101622 41 55            PUSH   R13
00101624 49 89 f5        MOV    R13,RSI
00101627 41 54            PUSH   R12
00101629 41 89 fc        MOV    R12D,EDI
0010162c 55              PUSH   RBP
0010162d 48 8d 2d        LEA    RBP,[__do_global_dtors_aux_fini_array_entry]
    a4 26 00 00
00101634 53              PUSH   RBX
00101635 4c 29 fd        SUB    RBP,R15
00101638 48 83 ec 08     SUB    RSP,0x8

```

XREF[3]: 001015e4(W),
001015ef(R),
001015f6(R)
XREF[4]: Entry Point(*), main:0010135c(c),
00102084, 001021b0(*)

= 00101546
= 00101546

XREF[4]: Entry Point(*),
_start:0010125a(*), 0010208c,
00102258(*)

= 101320h
= 1012E0h

00101601 Person
CALL 0x001011f0

CodeBrowser: COSC169:/class_layout

C++ Calling a virtual function

File Edit Analysis Graph Navigation Search Select Tools Window Help

Listing: class_layout - (14 addresses selected)

| Address | OpCode | Operands | Description | References | Comments |
|----------|----------------------|--|--|-------------------------------------|----------|
| 0010132e | 48 89 e5 | MOV RBP,RSP | | | |
| 00101331 | 53 | PUSH RBX | | | |
| 00101332 | 48 83 ec 58 | SUB RSP,0x58 | | | |
| 00101336 | 89 7d ac | MOV dword ptr [RBP + local_5c],EDI | | | |
| 00101339 | 48 89 75 a0 | MOV qword ptr [RBP + local_68],RSI | | | |
| 0010133d | 64 48 8b | MOV RAX,qword ptr FS:[0x28] | | | |
| | 04 25 28 | | | | |
| | 00 00 00 | | | | |
| 00101346 | 48 89 45 e8 | MOV qword ptr [RBP + cookie],RAX | | | |
| 0010134a | 31 c0 | XOR EAX,EAX | | | |
| 0010134c | bf 30 00 | MOV EDI,0x30 | | | |
| | 00 00 | | | | |
| | | | | | |
| 00101351 | e8 4a fe ff ff | CALL <EXTERNAL>::operator.new | XREF[1]: 001022b4(*) | void * operator.new(ulong param_1) | |
| 00101356 | 48 89 c3 | MOV RBX,RAX | | | |
| 00101359 | 48 89 df | MOV RDI,RBX | | | |
| 0010135c | e8 77 02 00 00 | CALL Person::Person | | undefined Person(Person * this) | |
| 00101361 | 48 89 5d b8 | MOV qword ptr [RBP + bob_class],RBX | | | |
| 00101365 | 48 8b 45 b8 | MOV RAX,qword ptr [RBP + bob_class] | | | |
| 00101369 | 48 8b 00 | MOV RAX,qword ptr [RAX] | | | |
| 0010136c | 48 8b 18 | MOV RBX,qword ptr [RAX] | | | |
| 0010136f | 48 8d 45 b7 | LEA RAX=>local_51,[RBP + -0x49] | | | |
| 00101373 | 48 89 c7 | MOV RDI,RAX | | | |
| 00101376 | e8 b5 fe ff ff | CALL <EXTERNAL>::std::allocator<char>::allocator | | undefined allocator(void) | |
| 0010137b | 48 8d 55 b7 | LEA RDX=>local_51,[RBP + -0x49] | | | |
| 0010137f | 48 8d 45 c0 | LEA RAX=>local_48,[RBP + -0x40] | | | |
| 00101383 | 48 8d 35 7b 0c 00 00 | LEA RSI,[DAT_00102005] | | = 62h b | |
| 0010138a | 48 89 c7 | MOV RDI,RAX | | | |
| | | | try { // try from 0010138d to 00101391 has its CatchHandler @... | | |
| 0010138d | e8 4e fe ff ff | CALL <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::basic_string | XREF[1]: 001022b8(*) | undefined basic_string(char * pa... | |
| | | | } | | |
| 00101392 | 48 8d 55 c0 | LEA RDX=>local_48,[RBP + -0x40] | | | |
| 00101396 | 48 8b 45 b8 | MOV RAX,qword ptr [RBP + bob_class] | | | |
| 0010139a | 48 89 d6 | MOV RSI,RDX | | | |
| 0010139d | 48 89 c7 | MOV RDI,RAX | | | |
| | | | try { // try from 001013a0 to 001013a1 has its CatchHandler @... | | |
| 001013a0 | ff d3 | CALL RBX | XREF[1]: 001022bd(*) | | |
| | | | } | | |
| 001013a2 | 48 8d 45 c0 | LEA RAX=>local_48,[RBP + -0x40] | | | |
| 001013a6 | 48 89 c7 | MOV RDI,RAX | | | |
| 001013a9 | e8 b2 fd ff ff | CALL <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::~basic_string | | undefined ~basic_string(basic_st... | |
| 001013ae | 48 8d 45 b7 | LEA RAX=>local_51,[RBP + -0x49] | | | |
| 001013b2 | 48 89 c7 | MOV RDI,RAX | | | |
| 001013b5 | e8 06 fe ff ff | CALL <EXTERNAL>::std::allocator<char>::~allocator | | undefined ~allocator(allocator<c... | |
| 001013ba | 48 8b 45 b8 | MOV RAX,qword ptr [RBP + bob_class] | | | |
| 001013be | 48 8b 00 | MOV RAX,qword ptr [RAX] | | | |
| 001013c1 | 48 83 c0 08 | ADD RAX,0x8 | | | |
| 001013c5 | 48 8b 10 | MOV RDX,qword ptr [RAX] | | | |
| 001013c8 | 48 8b 45 b8 | MOV RAX,qword ptr [RBP + bob_class] | | | |
| 001013cc | be 2a 00 nn nn | MOV ESI,0x2a | | | |

C++

Calling a virtual function

CodeBrowser: COSC169:/class_layout

File Edit Analysis Graph Navigation Search Select Tools Window Help

Listing: class_layout - (2 addresses selected)

| Address | OpCode | Operands | Comments |
|--|----------------------|--|--|
| 0010132e | 48 89 e5 | MOV RBP, RSP | |
| 00101331 | 53 | PUSH RBX | |
| 00101332 | 48 83 ec 58 | SUB RSP, 0x58 | |
| 00101336 | 89 7d ac | MOV dword ptr [RBP + local_5c], EDI | |
| 00101339 | 48 89 75 a0 | MOV qword ptr [RBP + local_68], RSI | |
| 0010133d | 64 48 8b | MOV RAX, qword ptr FS:[0x28] | |
| | 04 25 28 | | |
| | 00 00 00 | | |
| 00101346 | 48 89 45 e8 | MOV qword ptr [RBP + cookie], RAX | |
| 0010134a | 31 c0 | XOR EAX, EAX | |
| 0010134c | bf 30 00 | MOV EDI, 0x30 | |
| | 00 00 | | |
| | | | |
| 00101351 | e8 4a fe ff ff | CALL <EXTERNAL>::operator.new | XREF[1]: 001022b4(*) |
| 00101356 | 48 89 c3 | MOV RBX, RAX | |
| 00101359 | 48 89 df | MOV RDI, RBX | |
| 0010135c | e8 77 02 00 00 | CALL Person::Person | |
| 00101361 | 48 89 5d b8 | MOV qword ptr [RBP + bob_class], RBX | |
| 00101365 | 48 8b 45 b8 | MOV RAX, qword ptr [RBP + bob_class] | |
| 00101369 | 48 8b 00 | MOV RAX, qword ptr [RAX] | |
| 0010136c | 48 8b 18 | MOV RBX, qword ptr [RAX] | |
| 0010136f | 48 8d 45 b7 | LEA RAX=>local_51,[RBP + -0x49] | |
| 00101373 | 48 89 c7 | MOV RDI, RAX | |
| 00101376 | e8 b5 fe ff ff | CALL <EXTERNAL>::std::allocator<char>::allocator | |
| 0010137b | 48 8d 55 b7 | LEA RDX=>local_51,[RBP + -0x49] | |
| 0010137f | 48 8d 45 c0 | LEA RAX=>local_48,[RBP + -0x40] | |
| 00101383 | 48 8d 35 7b 0c 00 00 | LEA RSI, [DAT_00102005] | |
| 0010138a | 48 89 c7 | MOV RDI, RAX | |
| | | | = 62h b |
| | | | |
| try { // try from 0010138d to 00101391 has its CatchHandler @... | | | |
| LAB_0010138d | e8 4e fe ff ff | CALL <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::basic_string | XREF[1]: 001022b8(*) undefined basic_string(char * pa... |
| } | | | |
| // end try from 0010138d to 00101391 | | | |
| 00101392 | 48 8d 55 c0 | LEA RDX=>local_48,[RBP + -0x40] | |
| 00101396 | 48 8b 45 b8 | MOV RAX, qword ptr [RBP + bob_class] | |
| 0010139a | 48 89 d6 | MOV RSI, RDX | |
| 0010139d | 48 89 c7 | MOV RDI, RAX | |
| | | | |
| try { // try from 001013a0 to 001013a1 has its CatchHandler @... | | | |
| LAB_001013a0 | ff d3 | CALL RBX | XREF[1]: 001022bd(*) |
| } | | | |
| // end try from 001013a0 to 001013a1 | | | |
| 001013a2 | 48 8d 45 c0 | LEA RAX=>local_48,[RBP + -0x40] | |
| 001013a6 | 48 89 c7 | MOV RDI, RAX | |
| 001013a9 | e8 b2 fd ff ff | CALL <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::~basic_string | undefined ~basic_string(basic_st...) |
| 001013ae | 48 8d 45 b7 | LEA RAX=>local_51,[RBP + -0x49] | |
| 001013b2 | 48 89 c7 | MOV RDI, RAX | |
| 001013b5 | e8 06 fe ff ff | CALL <EXTERNAL>::std::allocator<char>::~allocator | |
| 001013ba | 48 8b 45 b8 | MOV RAX, qword ptr [RBP + bob_class] | |
| 001013be | 48 8b 00 | MOV RAX, qword ptr [RAX] | |
| 001013c1 | 48 83 c0 08 | ADD RAX, 0x8 | |
| 001013c5 | 48 8b 10 | MOV RDX, qword ptr [RAX] | |
| 001013c8 | 48 8b 45 b8 | MOV RAX, qword ptr [RBP + bob_class] | |
| 001013cc | be 2a 00 nn nn | MOV ESI, 0x2a | |
| | | | |

001013a0 main CALL RBX

C++

Where is the age field?

Listing: class_layout - (3 addresses selected)

```

        undefined __thiscall setAge(Person * this, int param_1)
        AL:1      <RETURN>
        Person *  RDI:8 (auto)  this
        int       ESI:4      param_1
        undefined8 Stack[-0x10]:8 local_10
                                XREF[2]:  0010157c(W),
                                00101583(R)
                                XREF[2]:  00101580(W),
                                00101587(R)
                                XREF[4]:  Entry Point(*), 0010206c,
                                00102150(*), 00103cf8(*)

        undefined4 Stack[-0x14]:4 local_14

        _ZN6Person6setAgeEi
        Person::setAge
        00101574 f3 0f 1e fa  ENDBR64
        00101578 55      PUSH   RBP
        00101579 48 89 e5  MOV    RBP,RSP
        0010157c 48 89 7d f8  MOV    qword ptr [RBP + local_10],this
        00101580 89 75 f4  MOV    dword ptr [RBP + local_14],param_1
        00101583 48 8b 45 f8  MOV    RAX,qword ptr [RBP + local_10]
        00101587 8b 55 f4  MOV    EDX,dword ptr [RBP + local_14]
        0010158a 89 50 28  MOV    dword ptr [RAX + 0x28],EDX
                                XREF[4]:  Entry Point(*), 0010206c,
                                00102150(*), 00103cf8(*)

        0010158d 90      NOP
        0010158e 5d      POP    RBP
        0010158f c3      RET

 *****
 * Person::getName[abi:cxx11]()
 *****
 undefined __thiscall getName[abi:cxx11](Person * this)
        AL:1      <RETURN>
        Person *  RDI:8 (auto)  this
        undefined8 Stack[-0x10]:8 local_10
                                XREF[3]:  0010159c(W),
                                001015ac(R),
                                001015bb(R)
                                XREF[2]:  001015a0(W),
                                001015a4(R)
                                XREF[4]:  Entry Point(*), 00102074,
                                00102170(*), 00103d00(*)

        undefined8 Stack[-0x18]:8 local_18

        _ZN6Person6getNameB5cxx11Ev
        Person::getName[abi:cxx11]
        00101590 f3 0f 1e fa  ENDBR64
        00101594 55      PUSH   RBP
        00101595 48 89 e5  MOV    RBP,RSP
        00101598 48 83 ec 10  SUB    RSP,0x10
        0010159c 48 89 7d f8  MOV    qword ptr [RBP + local_10],this
        001015a0 48 89 75 f0  MOV    qword ptr [RBP + local_18],RSI
        001015a4 48 8b 45 f0  MOV    RAX,qword ptr [RBP + local_18]
        001015a8 48 8d 50 08  LEA    RDX,[RAX + 0x8]
        001015ac 48 8b 45 f8  MOV    RAX,qword ptr [RBP + local_10]
        001015b0 48 89 d6  MOV    RSI,RDX
        001015b3 48 89 c7  MOV    this,RAX
        001015b6 e8 95 fb  CALL   <EXTERNAL>::std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string undefined basic_string(basic_str...
          ff ff
        001015bb 48 8b 45 f8  MOV    RAX,qword ptr [RBP + local_10]
        001015bf c9      LEAVE
        001015c0 c3      RET
        001015c1 90      ??    90h
                                XREF[4]:  Entry Point(*), 00102074,
                                00102170(*), 00103d00(*)

 *****
 * Person::getAge()
 *****
 undefined __thiscall getAge(Person * this)
        AL:1      <RETURN>
        Person *  RDI:8 (auto)  this
        undefined8 Stack[-0x10]:8 local_10
                                XREF[2]:  001015ca(W),
                                001015ce(R)
                                XREF[4]:  Entry Point(*), 0010207c,

```

0010158a setAge
MOV dword ptr [RAX + 0x28],...

C++

Layout of bob

| | |
|------|---------|
| | + ----- |
| 0x00 | {vptr} |
| 0x08 | name |
| ... | |
| 0x28 | age |
| | + ----- |

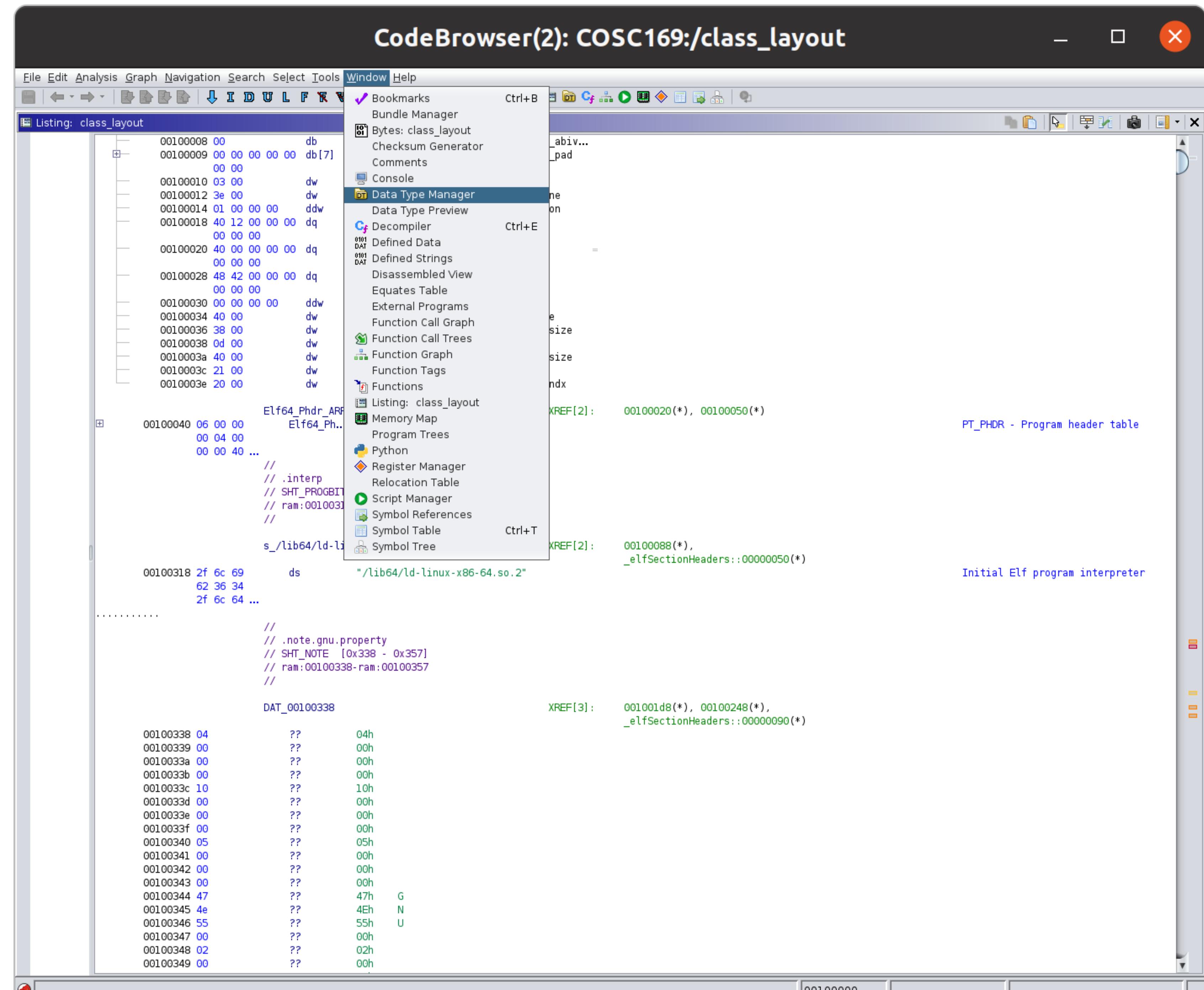
C++

Ghidra tip: Defining Data Types

- Up to this point we have only updated the disassembly with variable names but now we should start defining data types

C++

Open the Data Type Manager



CodeBrowser(2): COSC169:/class_layout

C++

Expand the Demangler

The screenshot shows the CodeBrowser interface with the title "CodeBrowser(2): COSC169:/class_layout". The main window displays assembly code for a C++ program, specifically the class layout of a Person object. The assembly code is shown in the central listing pane, with mnemonics like MOV, CALL, and LEAVE, and registers like RAX, RBP, and RSP.

The left sidebar contains a "Data Type Manager" with a tree view of data types. Under "std::class_layout", there is a "Demangler" folder which is currently selected. A context menu is open over a "Person" entry in this folder, with "Edit" highlighted. Other options in the menu include New, Copy, Cut, Delete, Paste, Rename, Export C Header..., Favorite, Display as Graph, Find Uses of, and Find Uses of Field... .

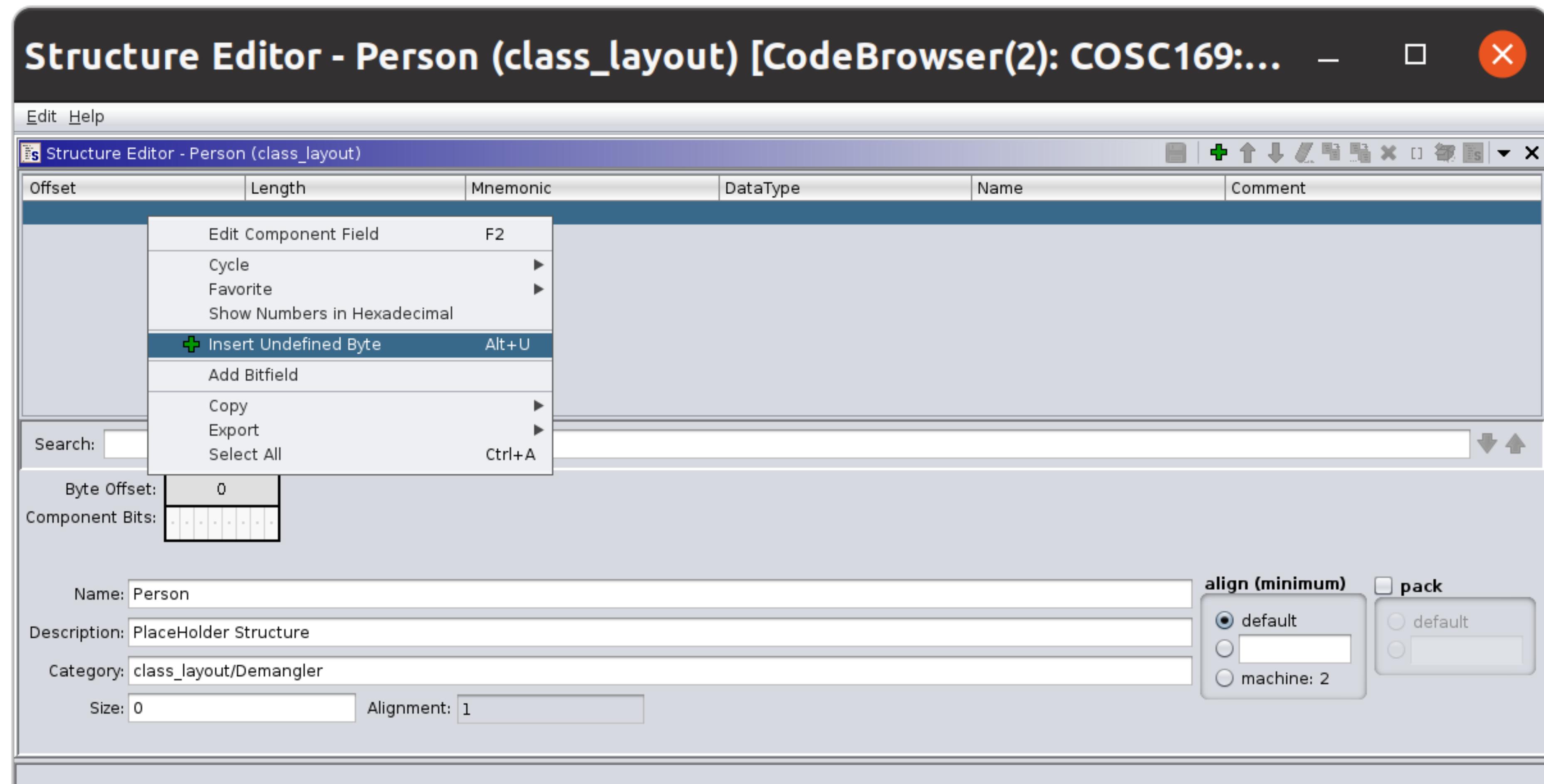
The right sidebar contains a "Functions - 59 items" table. The table lists various functions with their names, descriptions, and sizes. Some of the entries are:

| Name | Description | Function Size |
|-------------------------|-------------|---------------|
| _init | ... int ... | 27 |
| FUN_00101020 | ... unde... | 13 |
| _cxa_finalize | ... thun... | 11 |
| operator= | ... thun... | 11 |
| basic_string | ... thun... | 11 |
| ~basic_string | ... thun... | 11 |
| _cxa_atexit | ... thun... | 11 |
| operator<< | ... thun... | 11 |
| operator.new | ... thun... | 11 |
| operator<< | ... thun... | 11 |
| ~allocator | ... thun... | 11 |
| _stack_chk_fail | ... thun... | 11 |
| basic_string | ... thun... | 11 |
| basic_string | ... thun... | 11 |
| Init | ... thun... | 11 |
| operator<< | ... thun... | 11 |
| _Unwind_Resume | ... thun... | 11 |
| allocator | ... thun... | 11 |
| _start | ... unde... | 47 |
| deregister_tm_clo... | ... unde... | 34 |
| register_tm_clones | ... unde... | 51 |
| _do_global_dtors... | ... unde... | 54 |
| frame_dummy | ... thun... | 9 |
| main | ... unde... | 358 |
| _static_initializati... | ... unde... | 77 |
| _GLOBAL_sub_I_m... | ... unde... | 25 |
| setName | ... unde... | 46 |
| setAge | ... unde... | 28 |
| getName[abi:cxx11] | ... unde... | 49 |
| getAge | ... unde... | 21 |
| Person | ... unde... | 49 |
| _libc_csu_init | ... unde... | 101 |
| _libc_csu_fini | ... unde... | 5 |
| _fini | ... unde... | 13 |
| operator= | ... thun... | 1 |
| basic_string | ... thun... | 1 |
| endl<char, std::ch... | ... thun... | 1 |
| ~basic_string | ... thun... | 1 |
| _cxa_atexit | ... thun... | 1 |
| operator<< | ... thun... | 1 |
| operator<< | ... thun... | 1 |
| operator.new | ... thun... | 1 |
| operator<< | ... thun... | 1 |
| ~allocator | ... thun... | 1 |
| _stack_chk_fail | ... thun... | 1 |
| basic_string | ... thun... | 1 |
| basic_string | ... thun... | 1 |
| Init | ... thun... | 1 |
| _gxx_personality_v0 | ... thun... | 1 |
| operator<< | ... thun... | 1 |
| _ITM_deregisterTM... | ... thun... | 1 |

The bottom status bar shows the memory address 001015d8, the function name Person, and the instruction ENDBR64.

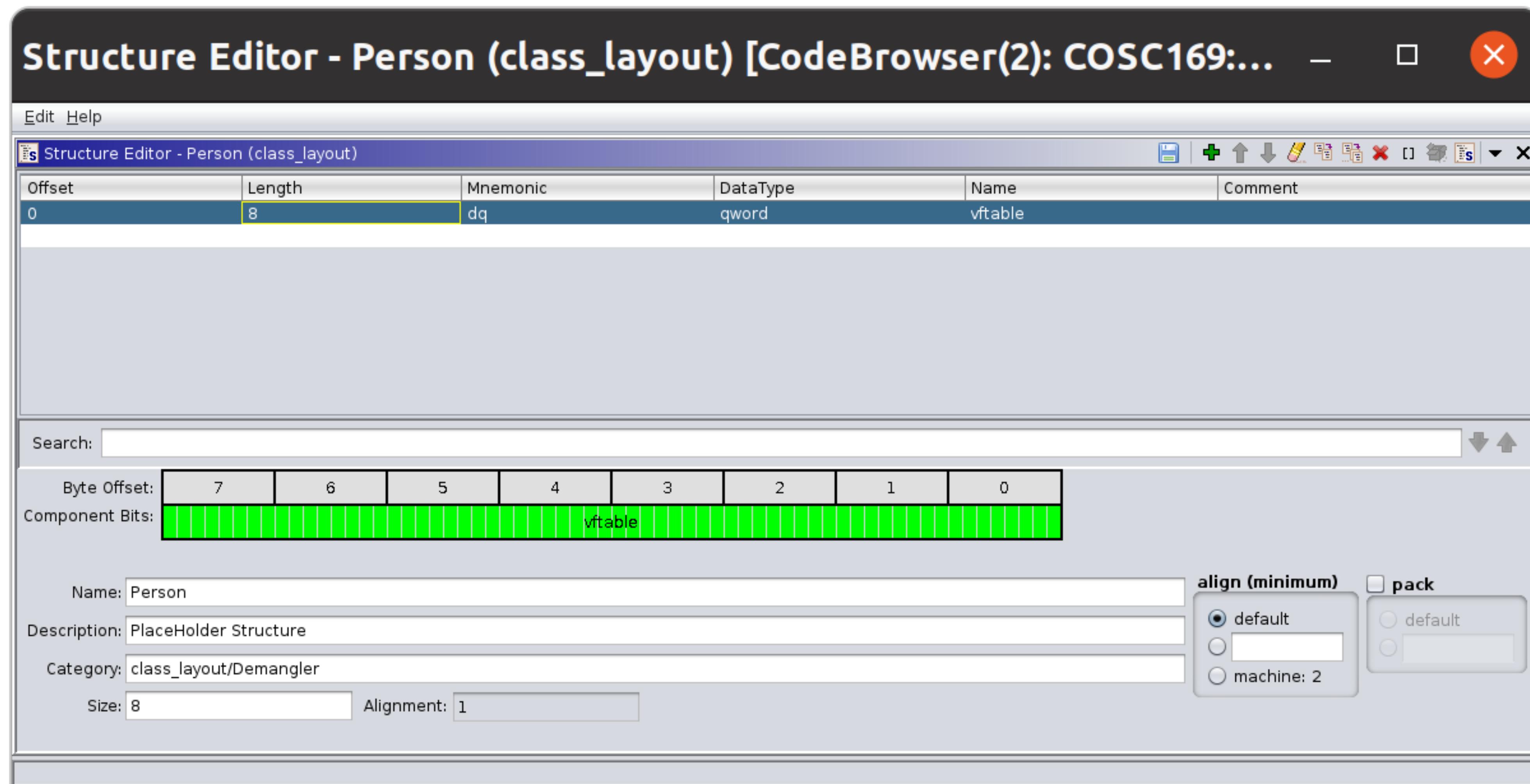
C++

Add an undefined byte (8x)



C++

Make it a qword and name it. The hot key is probably 'b'



C++

Add the remaining two fields then click the save icon

Structure Editor - Person (class_layout) [CodeBrowser(2): COSC169:...]

| Offset | Length | Mnemonic | DataType | Name | Comment |
|--------|--------|----------|---------------|---------|---------|
| 0 | 8 | dq | qword | vtable | |
| 8 | 32 | ??[32] | undefined[32] | name | |
| 40 | 4 | ddw | dword | age | |
| 44 | 4 | ddw | dword | padding | |

Byte Offset: 47 46 45 44 43 42 41 40 39 38 37 36

Component Bits: padding age name

Name: Person
Description: PlaceHolder Structure
Category: class_layout/Demangler
Size: 48 Alignment: 1

align (minimum) pack
 default

 machine: 2

C++

The Person struct will now be updated

CodeBrowser(2): COSC169:/class_layout

File Edit Analysis Graph Navigation Search Select Tools Window Help

Data Type Manager Listing: class_layout Functions - 59 items

Person

Alignment: 1 Length: 48

/* PlaceHolder Structure */

struct Person {

qword vtable

undefined[32] name

dword age

dword padding

} pack(disabled)

TerminatedCString

uleb128

ulong

undefined1

undefined4

undefined8

void

word

generic_clib_64

MOV THIS, RAX

CALL <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::basic_string

MOV RAX, qword ptr [RBP + local_10]

LEAVE

RET

?? 90h

* Person::getAge()

undefined __thiscall getAge(Person * this)

AL:1 <RETURN>

RDI:8 (auto) this

Stack[-0x10]:8 local_10

XREF[2]:

_ZN6Person6getAgeEv

Person::getAge

Entry Po: 00102190

001015c2 f3 0f 1e fa ENDBR64

001015c6 55 PUSH RBP

001015c7 48 89 e5 MOV RBP, RSP

001015ca 48 89 7d f8 MOV qword ptr [RBP + local_10], this

001015ce 48 8b 45 f8 MOV RAX, qword ptr [RBP + local_10]

001015d2 8b 40 28 MOV EAX, dword ptr [RAX + 0x28]

001015d5 5d POP RBP

001015d6 c3 RET

001015d7 90 ?? 90h

* Person::Person()

undefined __thiscall Person(Person * this)

AL:1 <RETURN>

RDI:8 (auto) this

Stack[-0x10]:8 local_10

XREF[3]:

_ZN6PersonC1Ev

_ZN6PersonC2Ev

Person::Person

Entry Po: 00102084

001015d8 f3 0f 1e fa ENDBR64

001015dc 55 PUSH RBP

001015dd 48 89 e5 MOV RBP, RSP

001015e0 48 83 ec 10 SUB RSP, 0x10

001015e4 48 89 7d f8 MOV qword ptr [RBP + local_10], this

001015e8 48 8d 15 LEA RDX, [PTR_setName_00103cf0]

01 27 00 00

001015ef 48 8b 45 f8 MOV RAX, qword ptr [RBP + local_10]

001015f3 48 89 10 MOV qword ptr [RAX], RDX=>PTR_setName_00103cf0

001015f6 48 8b 45 f8 MOV RAX, qword ptr [RBP + local_10]

001015fa 48 83 c0 08 ADD RAX, 0x8

001015fe 48 89 c7 MOV this, RAX

00101601 e8 ea fb CALL <EXTERNAL>::std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>>::basic_string

ff ff

00101606 90 NOP

00101607 c9 LEAVE

00101608 c3 RET

00101609 0f ?? 0Fh

0010160a 1f ?? 1Fh

0010160b 80 ?? 80h

0010160c 00 ?? 00h

0010160d 00 ?? 00h

Functions - 59 items

| Name | Function | Function Size |
|-------------------------|-------------|---------------|
| _init | ... int ... | 27 |
| FUN_00101020 | ... unde... | 13 |
| _cxa_finalize | ... thun... | 11 |
| operator= | ... thun... | 11 |
| basic_string | ... thun... | 11 |
| ~basic_string | ... thun... | 11 |
| _cxa_atexit | ... thun... | 11 |
| operator<< | ... thun... | 11 |
| operator<< | ... thun... | 11 |
| operator.new | ... thun... | 11 |
| operator<< | ... thun... | 11 |
| ~allocator | ... thun... | 11 |
| _stack_chk_fail | ... thun... | 11 |
| basic_string | ... thun... | 11 |
| basic_string | ... thun... | 11 |
| Init | ... thun... | 11 |
| operator<< | ... thun... | 11 |
| _Unwind_Resume | ... thun... | 11 |
| allocator | ... thun... | 11 |
| _start | ... unde... | 47 |
| deregister_tm_clo... | ... unde... | 34 |
| register_tm_clones | ... unde... | 51 |
| _do_global_dtors... | ... unde... | 54 |
| frame_dummy | ... thun... | 9 |
| main | ... unde... | 358 |
| _static_initializati... | ... unde... | 77 |
| _GLOBAL_sub_I_m... | ... unde... | 25 |
| setName | ... unde... | 46 |
| setAge | ... unde... | 28 |
| getName[abi:cxx11] | ... unde... | 49 |
| getAge | ... unde... | 21 |
| Person | ... unde... | 49 |
| _libc_csu_init | ... unde... | 101 |
| _libc_csu_fini | ... unde... | 5 |
| fini | ... unde... | 13 |
| operator= | ... thun... | 1 |
| basic_string | ... thun... | 1 |
| endl<char, std::ch... | ... thun... | 1 |
| ~basic_string | ... thun... | 1 |
| _cxa_atexit | ... thun... | 1 |
| operator<< | ... thun... | 1 |
| operator<< | ... thun... | 1 |
| operator.new | ... thun... | 1 |
| operator<< | ... thun... | 1 |
| ~allocator | ... thun... | 1 |
| _stack_chk_fail | ... thun... | 1 |
| basic_string | ... thun... | 1 |
| basic_string | ... thun... | 1 |
| Init | ... thun... | 1 |
| _gxx_personality_v0 | ... thun... | 1 |
| operator<< | ... thun... | 1 |
| _ITM_deregisterTM... | ... thun... | 1 |

C++

Results? Open the Decompilation of setAge

CodeBrowser(2): COSC169:/class_layout

File Edit Analysis Graph Navigation Search Select Tools Window Help

Listing: class_layout

Decompile: setAge - (class_layout)

00101552 48 89 7d f8 MOV qword ptr [RBP + local_10],this
00101556 48 89 75 f0 MOV qword ptr [RBP + local_18],param_1
0010155a 48 8b 45 f8 MOV RAX,qword ptr [RBP + local_10]
0010155e 48 8d 50 08 LEA RDX,[RAX + 0x8]
00101562 48 8b 45 f0 MOV RAX,qword ptr [RBP + local_18]
00101566 48 89 c6 MOV param_1,RAX
00101569 48 89 d7 MOV this,RDX
0010156c e8 cf fb CALL <EXTERNAL>::std::__cxxll::basic_string<char, std::char_traits<char>, std::allocator<char>>::append
ff ff
00101571 90 NOP
00101572 c9 LEAVE
00101573 c3 RET

* Person::setAge(int)

undefined _thiscall setAge(Person * this, int param_1)
AL:1 <RETURN>
RDI:8 (auto) this
ESI:4 param_1
Stack[-0x10]:8 local_10 XREF[2]: 0010157c(W),
00101583(R)
Stack[-0x14]:4 local_14 XREF[2]: 00101580(W),
00101587(R)

_ZN6Person6setAgeEi
Person::setAge XREF[4]: Entry Point(*), 0010206c,
00102150(*), 00103cf8(*)

00101574 f3 0f 1e fa ENDBR64
00101578 55 PUSH RBP
00101579 48 89 e5 MOV RBP,RSP
0010157c 48 89 7d f8 MOV qword ptr [RBP + local_10],this
00101580 89 75 f4 MOV dword ptr [RBP + local_14],param_1
00101583 48 8b 45 f8 MOV RAX,qword ptr [RBP + local_10]
00101587 8b 55 f4 MOV EDX,dword ptr [RBP + local_14]
0010158a 89 50 28 MOV dword ptr [RAX + 0x28],EDX
0010158d 90 NOP
0010158e 5d POP RBP
0010158f c3 RET

* Person::getName[abi:cxx11]()

undefined _thiscall getName[abi:cxx11](Person * this)
AL:1 <RETURN>
RDI:8 (auto) this
Stack[-0x10]:8 local_10 XREF[3]: 0010159c(W),
001015ac(R),
001015bb(R)
Stack[-0x18]:8 local_18 XREF[2]: 001015a0(W),
001015a4(R)

_ZN6Person7getNameB5cxx11Ev
Person::getName[abi:cxx11] XREF[4]: Entry Point(*), 00102074,
00102170(*), 00103d00(*)

00101590 f3 0f 1e fa ENDBR64
00101594 55 PUSH RBP
00101595 48 89 e5 MOV RBP,RSP
00101598 48 83 ec 10 SUB RSP,0x10
0010159c 48 89 7d f8 MOV qword ptr [RBP + local_10],this
001015a0 48 89 75 f0 MOV qword ptr [RBP + local_18],RSI
001015a4 48 8b 45 f0 MOV RAX,qword ptr [RBP + local_18]
001015a8 48 8d 50 08 LEA RDX,[RAX + 0x8]
001015ac 48 8b 45 f8 MOV RAX,qword ptr [RBP + local_10]
001015b0 48 89 d6 MOV RSI,RSI
001015b3 48 89 c7 MOV this,RAX

Decompile: setAge x Functions x

00101574 setAge ENDBR64

C++

Inheritance

- What if a class has a parent class from which it inherits?

We stopped here in class

C++ Inheritance

```
john@caesar: ~/recourse/week03
class Building {
private:
    int height;
    int width;
    std::string address;

public:
    virtual void setHeight( int height ) { this->height = height; }
    virtual void setWidth( int width ) { this->width = width; }
    virtual void setAddress( std::string address ) { this->address = address; }

    virtual int getHeight( void ) { return this->height; }
    virtual int getWidth( void ) { return this->width; }
    virtual std::string getAddress( void ) { return this->address; }
};

~
~
~
~
~
~
~
~

"building.hpp" 15L, 500C
```

C++ Inheritance

```
#include "building.hpp"

class House: public Building {
private:
    int rooms;
    int baths;

public:
    virtual void setRooms( int rooms ) { this->rooms = rooms; }
    virtual void setBaths( int baths ) { this->baths = baths; }

    virtual int getRooms( void ) { return this->rooms; }
    virtual int getBaths( void ) { return this->baths; }
};

~
~
~
~
~
~
~
~
~
```

C++ Inheritance

```
#include <iostream>
#include "house.hpp"

int main( int argc, char** argv)
{
    House *home = new House;

    home->setHeight(10);
    home->setWidth(10);
    home->setAddress("Nowhere");
    home->setRooms(4);
    home->setBaths(4);

    return 0;
}
```

```
~  
~  
~  
~  
~  
~  
~  
~
```

"inherit.cpp" 16L, 239C

john@caesar: ~/recourse/week03



4,0-1

All

C++ Short Lab

- Open the *inherit* binary in Ghidra and using a combination of static and dynamic analysis work out the memory layout of the class

C++ Short Lab: Results

CodeBrowser: COSC169:/inherit

File Edit Analysis Graph Navigation Search Select Tools Window Help

I D U L F R V B

Data Type Manager

Listing: inherit

Functions - 57 items

```

AL:1 <RETURN>
undefined AL:1 <RETURN>
House * RDI:8 (auto) this
int ESI:4 param_1
undefined8 Stack[-0x10]:8 local_10
undefined4 Stack[-0x14]:4 local_14

_ZNSHouse8setBathsEi
House::setBaths
0010154a f3 0f 1e fa ENDBR64
0010154e 55 PUSH RBP
0010154f 48 89 e5 MOV RBP,RSP
00101552 48 89 7d f8 MOV qword ptr [RBP + local_10],this
00101556 89 75 f4 MOV dword ptr [RBP + local_14],param_1
00101559 48 b8 45 f8 MOV RAX,qword ptr [RBP + local_10]
0010155d 8b 55 f4 MOV EDX,dword ptr [RBP + local_14]
00101560 89 50 34 MOV dword ptr [RAX + 0x34],EDX
00101563 90 NOP
00101564 5d POP RBP
00101565 c3 RET

*****
* House::getRooms()
*****
undefined __thiscall getRooms(House * this)
AL:1 <RETURN>
undefined undefined undefined8
House * RDI:8 (auto) this
Stack[-0x10]:8 local_10

_ZNSHouse8getRoomsEv
House::getRooms
00101566 f3 0f 1e fa ENDBR64
0010156a 55 PUSH RBP
0010156b 48 89 e5 MOV RBP,RSP
0010156e 48 89 7d f8 MOV qword ptr [RBP + local_10],this
00101572 48 b8 45 f8 MOV RAX,qword ptr [RBP + local_10]
00101576 8b 40 30 MOV EAX,dword ptr [RAX + 0x30]
00101579 5d POP RBP
0010157a c3 RET
0010157b 90 ?? 90h

*****
* House::getBaths()
*****
undefined __thiscall getBaths(House * this)
AL:1 <RETURN>
undefined undefined undefined8
House * RDI:8 (auto) this
Stack[-0x10]:8 local_10

_ZNSHouse8getBathsEv
House::getBaths
0010157c f3 0f 1e fa ENDBR64
00101580 55 PUSH RBP
00101581 48 89 e5 MOV RBP,RSP
00101584 48 89 7d f8 MOV qword ptr [RBP + local_10],this
00101588 48 b8 45 f8 MOV RAX,qword ptr [RBP + local_10]
0010158c 8b 40 34 MOV EAX,dword ptr [RAX + 0x34]
0010158f 5d POP RBP
00101590 c3 RET
00101591 90 ?? 90h

```

Filter:

Decompile: getRooms x Functions x

00101566 getRooms ENDBR64

Homework

- Difficult crackme written in C++
- The difficulty with this one is likely to be in figuring out the algorithm
- Determine what input will result in printing SUCCESS
- A small write-up describing the algorithm