Reversing Microsoft Visual C++ Part II: Classes, Methods and RTTI

~~Thursday, September 21 2006 15:56.06 CDT~~

Author: igorsk **# Views:** 122311

Abstract

Microsoft Visual C++ is the most widely used compiler for Win32 so it is important for the Win32 reverser to be familiar with i
the compiler-generated glue code helps to quickly concentrate on the actual code written by the programmer. It also helps in
the program.

In part II of this 2-part article (see also: Part I: Exception Handling), I will cover how C++ machinery is implemented in MSVC
functions, RTTI. Familiarity with basic C++ and assembly language is assumed.

Basic Class Layout

To illustrate the following material, let's consider this simple example:

```
class A
{
  int a1;
public:
  virtual int A_virt1();
  virtual int A_virt2();
  static void A_static1();
  void A_simple1();
};

class B
{
  int b1;
  int b2;
public:
  virtual int B_virt1();
  virtual int B_virt2();
};

class C: public A, public B
{
  int c1;
public:
  virtual int A_virt2();
  virtual int B_virt2();
};
```

In most cases MSVC lays out classes in the following order:

- 1. Pointer to virtual functions table (_vtable_ or _vftable_), added only when the class has virtual methods and no sui
  reused.
- 2. Base classes
- 3. Class members

Virtual function tables consist of addresses of virtual methods in the order of their first appearance. Addresses of overloaded
functions from base classes.

Thus, the layouts for our three classes will look like following:

```
class A size(8):
    +---
 0  | {vfptr}
 4  | a1
    +---

A's vftable:
 0  | &A::A_virt1
 4  | &A::A_virt2

class B size(12):
    +---
 0  | {vfptr}
 4  | b1
 8  | b2
    +---

B's vftable:
 0  | &B::B_virt1
```

Article Comments

Write Comment / View Complete Comments

Username	Comment Excerpt	Date
cl001	[b][url=http://lululemonsales.webs.com/]Lululem...	Monday, May 6 201
julyDragon919	Hi! you ve just made me smile! i was having ...	Tuesday, August 7 2
Shine	good article£¬by what method do you trace it?	Thursday, August 4
martinkro	great artical ,thank you!!	Tuesday, July 19 20
EliteKnites	i have some doubts on this.. typeid is returnin...	Tuesday, May 10 20
EliteKnites	Thank you so much.. this paper gives a clear cu...	Tuesday, May 10 20
qxsl2000	it seems like c++ object hierarchy to be decomp...	Wednesday, March
roczhang	Great paper. I have took almost two days to wan...	Thursday, March 3 2
tcljg2008	very very good!	Saturday, Decembe
hwwh1999	Mark and study	Saturday, Septembe
FloydTammie31	Houses are quite expensive and not everyone can...	Sunday, September
Externalist	I've also read this some time ago but never rea...	Thursday, January 2
Sirmabus	[url=http://www.openrce.org/blog/view/1344/Clas...	Thursday, January 2
Sirmabus	Thanks the vtable finder/namer script functiona...	Wednesday, Decem
dnix	wonder whether these structures found by these ...	Tuesday, August 19
igorsk	Well, I was disassembling c1xx to check how it ...	Friday, September 2
MohammadHosein	actually didnt read the whole article yet , but...	Friday, September 2
linestyle	great work!!:)	Thursday, Septembe