

Re: Locating procedures within an EXE

Source: <http://coding.derkeiler.com/Archive/Delphi/comp.lang.pascal.delphi.misc/2003-12/0922.html>

From: Martin Harvey (Demon Account) (martin_at__nospam_pergolesi.demon.co.uk)

Date: 12/22/03

Date: Mon, 22 Dec 2003 01:41:49 +0000

On Sun, 21 Dec 2003 01:29:28 -0800, Jamie
<jamie_5_not_valid_after_5@charter.net> wrote:

>*this is real native code generation here.*
>*we are not talking about VB or any other half wide language.*
>*there is no procedure/function name table in an EXE along with*
>*a list of entry points.*
>*you may find this in a DLL how ever.*
>*and i am not sure if the Export functions work in a EXE file..*
>*in any case you should not waste any more of your time trying to*
>*break down a EXE in that faction.*
>*simply putting it, EXE from Delphi is mostly pure CPU code., the only*
>*way you could even get some info would be to build your self a debugger*
>*that can scan the EXE file and generate CPU code looking for CALL*
>*statements.. i really don't think your looking to do that.*
>

Further to this – I actually suspect that Delphi executables contain a lot more symbol information in them than (for example) a C or C++ executable.

At the very least, you have all the RTTI information.

If the executable was build with Debug information (either Delphi debug info, of TD32 debug info), then you should have huge amounts of info about the type and size of everything.

The catch is, working out what the format of the information is, and being able to read it.

If it wasn't built with debug info, then you're pretty much stuck.

MH.