

Re: Enumerating 32-bit modules from 32-bit processes in WOW64

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2005-06/msg00180.htm>

- *From:* "Ivan Brugiolo [MSFT]" <ivanbrug@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 14 Jun 2005 07:59:03 -0700
-

I will try very briefly to summarize how a 32-bit process is loaded.

- an EPROCESS is created, with the 32bit process `flag` set
- the image is mapped in the new address space
- the 64bit ntdll.dll is loaded
- the 64-bit ntdll.dll realizes this is a wow64 process
- it then loads the wow64 modules (wow64, wow64bin, wow64cpu) and the wow64 modules runs the cpu simulation loop (let's not argue on this name for now)
- the cpu simulation loop loads the 32-bit ntdll.dll, that carries on process initialization as usual.
- during (32-bit) process initialization, ntdll loads the other modules (from SysWoW64)

NtDll.dll is treated specially, given its role in process initialization. So, to summarize, there are 2 list of modules for a 32-bit process under wow, and, 64-bit tlist.exe pointed to a 32-bit process clearly shows that.

The paths are always consistent for the "half of the world" that uses them. Unless you disable redirection, opening `c:\windows\system32` from a 32-bit process will effectively go to `c:\windows\SysWOW64`, that is the correct result from the point of view of the 32-bit process. Opening `c:\windows\syswow64` is again correct for a 32-bit process.

However, as 64-bit process can be 32-bit aware, and, opening `c:\windows\syswow64\xxx.dll` will really open the 32-bit binary, and that may be expected and wanted, since 64-bit processes can be designed to be aware of the wow64 subsystem, while the converse is not necessarily true.

—

This posting is provided "AS IS" with no warranties, and confers no rights. Use of any included script samples are subject to the terms specified at <http://www.microsoft.com/info/copyright.htm>

Re: Enumerating 32-bit modules from 32-bit processes in WOW64

"Philip Sloss" <stuff@xxxxxxxx> wrote in message
news:uBYP2IOcFHA.3120@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
> "Jochen Kalmbach [MVP]" <nospam-Jochen.Kalmbach@xxxxxxxx> wrote in
message
> news:OxMdiXKcFHA.3504@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>
>> Maybe the the fact that some names have the sysWow64 path inside the
>> names is because of the way the DLL is loaded (maybe is it is indirectly
>> loaded, the OS will have to find the correct one... and then it will use
>> the sywow64-directory). But this is just a assumption.
>
> Hi Jochen,
>
> I think that's a good assumption that this has to do with compatibility.
> This is one of those cases where I didn't find the "backwards
compatibility
> directive" to be an intuitive thing. And looking at a list of loaded
> modules for a couple of apps, the DLLs that point to "system32" do seem to
> be ones that tend to be loaded explicitly rather than implicitly. The
core
> Win32 libraries point to syswow64 (KERNEL, USER, GDI), as do a few others.
> NTDLL points to system32, but then that library is probably a special
case.
> The libraries that I'm loading explicitly (wtsapi32, iphlapi,
> ws2_32/wsock32) point to system32.
>
> I'll probably invest a little time to check this out in more detail, but
> this behavior may prove to be useful if it provides an indication (even
it's
> not a guarantee) of how a 32-bit DLL was loaded.
>
> Thanks,
>
> Philip Sloss
>
>

• *Follow-Ups:*

- ◆ [Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)
 ◇ From: Philip Sloss

• *References:*

- ◆ [Enumerating 32-bit modules from 32-bit processes in WOW64](#)
 ◇ From: Philip Sloss
- ◆ [Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)

Re: Enumerating 32-bit modules from 32-bit processes in WOW64

◇ *From:* Jochen Kalmbach [MVP]

◆ **[Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)**

◇ *From:* Philip Sloss

◆ **[Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)**

◇ *From:* Jochen Kalmbach [MVP]

◆ **[Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)**

◇ *From:* Philip Sloss

◆ **[Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)**

◇ *From:* Jochen Kalmbach [MVP]

◆ **[Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)**

◇ *From:* Philip Sloss

- Prev by Date: **[Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)**
- Next by Date: **[Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)**
- Previous by thread: **[Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)**
- Next by thread: **[Re: Enumerating 32-bit modules from 32-bit processes in WOW64](#)**
- Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**