

Don't be helpless: You can find information, too, if you try

 devblogs.microsoft.com/oldnewthing/20080613-00

June 13, 2008



Raymond Chen

Here's a question that floated past my view:

Anybody know if there exists a library for computing MD5 hashes from unmanaged code? MSDN has information about .NET classes, but nothing about the unmanaged side.

Hm, let's see.

```
C:\Windows SDK\Include> grep MD5 *.h
wincrypt.h:#define ALG_SID_MD5 3
wincrypt.h:#define ALG_SID_SSL3SHAMD5 8
wincrypt.h:#define CALG_MD5 (ALG_CLASS_HASH | ALG_TYPE_ANY |
ALG_SID_MD5)
wincrypt.h:#define CALG_HUGHES_MD5
(ALG_CLASS_KEY_EXCHANGE|ALG_TYPE_ANY|ALG_SID_MD5)
wincrypt.h:#define CALG_SSL3_SHAMD5 (ALG_CLASS_HASH | ALG_TYPE_ANY |
ALG_SID_SSL3SHAMD5)
wincrypt.h:#define KP_PRECOMP_MD5 24
wincrypt.h:#define szOID_RSA_MD5RSA "1.2.840.113549.1.1.4"
wincrypt.h:#define szOID_RSA_MD5 "1.2.840.113549.2.5"
```

Wow, those hits sure look promising. Perhaps a search on [Windows Live](#) or [Google](#)¹ will turn up something. Oh hey, how about that, [sample code](#).

Exercise: Use this exact same technique to answer [this commenter's question](#) on how the C# `++` operator works. Hint: Since this is a question about the C# language, [the C# language specification](#) would be a good starting point.

Exercise: Use this technique to answer [this commenter's question](#) on how to connect to a process as a debugger.

Footnotes

¹ [OH MY GOD I LINKED TO GOOGLE.](#)

[Raymond Chen](#)

Follow

