

Not quite what you are looking for? You may want to try:

- [An MD5 Function Compatible with PHP](#)
- [Exploiting MD5 collisions \(in C#\)](#)

[highlights off](#)

8,535,913 members and growing! (60,442 online)

jash.liao ▼ 537 Sign out



[Home](#) [Articles](#) [Quick Answers](#) [Discussions](#) [Learning Zones](#) [Features](#) [Help!](#) [The Lounge](#) [MD5](#)

» [Languages](#) » [C / C++ Language](#) » [General](#)



MD5 File Creation and Verification

Licence [CPOL](#)
First Posted **4 Jan 2009**
Views **26,913**
Bookmarked **24 times**

See Also

- [More like this](#)
- [More by this author](#)

By [Shaheer Abdulrahiman](#) | 4 Jan 2009

[VC6](#) [VC7](#) [VC7.1](#) [VC8.0](#) [WinXP](#) [Win2003](#) [Vista](#) [C++](#) [C++/CLI](#) [C](#) , ...

A tool for creating/verifying MD5 files

[Article](#) [Browse Code](#) [Stats](#) [Revisions \(3\)](#) [Alternatives](#)

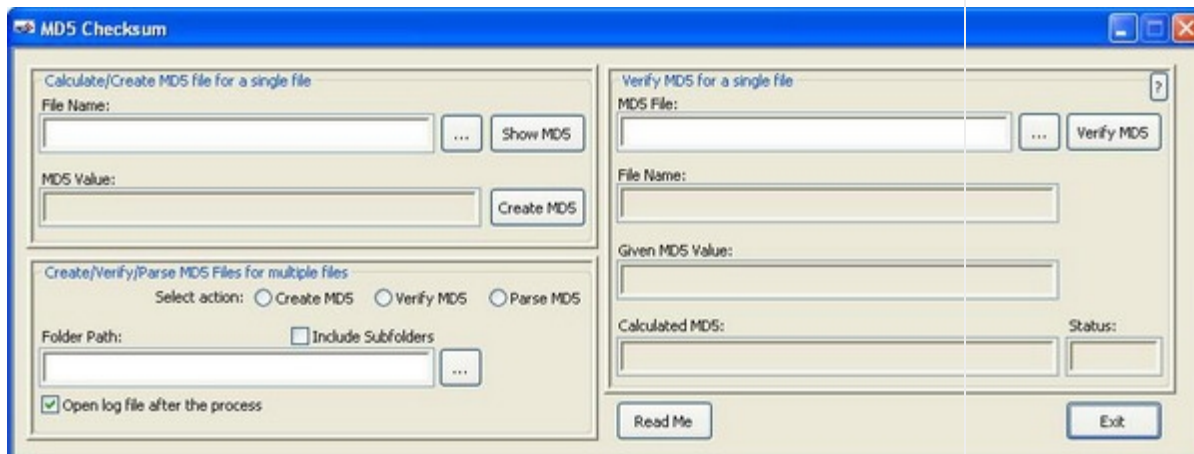


2.85 (7 votes)



Download source - 83.22 KB

[Add your own alternative version](#)



Introduction

In cryptography, **MD5** (Message-Digest algorithm 5) is a widely used, partially insecure cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), **MD5** has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An **MD5** hash is typically expressed as a 32 digit hexadecimal number.

For more information regarding **MD5**, [click here](#).

Background

This tool is for calculating/verifying **MD5** value of an EXE or

The basic function in this tool is as follows. This function will accept the EXE "FileName" and will return the MD5 value in "MD5". Anyone can use this function in his/her code to get the MD5 value. Just copy and paste this function in your code. You should include the header `<wincrypt.h>`.

[Collapse](#) | [Copy Code](#)

```
int CalculateMD5(CString FileName, CString &MD5)
{
    const size_t StringSize = FileName.GetLength() + 1;
    size_t CharactersConverted = 0;

    char *file = new char[StringSize];
    //char file[1024];
    wcstombs_s(&CharactersConverted, file,
        FileName.GetLength()+1, FileName, _TRUNCATE);

    int i, j;
    FILE *fInput;
    MD5Context md5Hash;
    unsigned char bBuffer[4096];
    unsigned char b;
    char c;

    if(!CryptStartup())
    {
        MessageBoxW(0, L"Could not start crypto library",
            L"MD5", MB_ICONERROR);
        return 0;
    }

    fInput = fopen(file, "rb");
    if(!fInput)
    {
        MessageBoxW(0, L"Failed to open - Invalid File",
            L"MD5", MB_ICONERROR);
        CryptCleanup();
        return 0;
    }

    memset(&md5Hash, 0, sizeof(MD5Context));
    MD5Init(&md5Hash);
    while(!feof(fInput)){
        unsigned int nCount = fread(bBuffer, sizeof(unsigned char),
            4096, fInput);
        MD5Update(&md5Hash, bBuffer, nCount);
    }
    MD5Final(&md5Hash);

    fclose(fInput);
    //printf("\nChecksum of '%s' is: ", argv[1]);
    char *Value = new char[1024];int k = 0;
    for(i = 0; i < 16; i++)
    {
        b = md5Hash.digest[i];
        for(j = 4; j >= 0; j -= 4)
        {
            c = ((char) (b >> j) & 0x0F);
            if(c < 10) c += '0';
            else c = ('a' + (c - 10));
            //printf("%c", c);
            Value[k] = c;
            k++;
        }
    }
    Value[k] = '\0';
    CryptCleanup();

    //CString cString;
```



Internet Components for every Major Protocol.









www.nsoftware.com



DOWNLOAD NOW

Related Articles

- [An MD5 Function Compatible with PHP](#)
- [Exploiting MD5 collisions \(in C#\)](#)
- [Use Windows Crypto API to calculate a MD5 string.](#)
- [How To: Hash Data Using MD5 and SHA1](#)
- [Duplicate Files Finder](#)
- [Good Bye MD5](#)
- [MD5 in ASP.NET](#)
- [ReHash - A console-based hash calculator](#)
- [Cyclic Redundancy Check \(CRC32\) HashAlgorithm](#)
- [Calculating MD5 Checksum](#)
- [Create md5 Hash-code using Assemblies in SQL Server 2005](#)
- [The FileDigest program and the C++ implementation of some Message-Digest algorithms](#)
- [MD5 Hash SQL Server Extended Stored Procedure](#)

```
delete file;
delete Value;
return 1;
}
```

History

- 3rd January, 2009: Initial post

License

This article, along with any associated source code and files, is licensed under [The Code Project Open License \(CPOL\)](#)

About the Author

Shaheer Abdulrahiman



Software Developer
India
Member



Article Top

Rate this: *Poor* ☐ ☐ ☐ ☐ ☐ *Excellent*

- Strategy Pattern
- MD5 Hash Calculator Pocket PC 2003/Windows CE 4.x
- Web Service Authentication
- Get MD5 and SHA-1 (SHA1) of any file
- Using hashlib++ for easily creating cryptographic checksums such as SHA1 and MD5
- Emulating PBEWithMD5AndDES Encryption under .NET

The Daily Insider

30 free programming books
Daily News: [Signup now.](#)

Comments and Discussions

Search this forum

Go

☐ Profile popups

Noise

Medium

Layout

Normal

Per

page

25

Update

Refresh

First Prev Next

MD5 Source in C++

MD5 is obsolete

Re: MD5 is obsolete

My vote of 2

牛B

Re: 牛B

Re: 牛B

Re: 牛B

none

wim ton

TobiasP

zengkun100

Member 4599072

baijun1982

Enjon CHEN

haohui

23:54 28 Feb '09

18:09 6 Jan '09

3:44 7 Jan '09

11:58 6 Jan '09

23:16 4 Jan '09

14:01 5 Jan '09

18:48 6 Apr '10

0:24 28 Oct '10

 Joke  Rant  Admin

Use Ctrl+Left/Right to switch messages, Ctrl+Up/Down to switch threads,
Ctrl+Shift+Left/Right to switch pages.

[Permalink](#) | [Advertise](#) | [Privacy](#) | [Mobile](#)

Web04 | 2.5.120302.2 | Last Updated 3 Jan 2009

Article Copyright 2009 by Shaheer Abdulrahiman
Everything else Copyright © [CodeProject](#), 1999-2012
[Terms of Use](#)

Layout: [fixed](#) | [fluid](#)