🏠 » **Languages** » **C / C++ Language** » **General**

MD5 File Creation and Verification

By **Shaheer Abdulrahiman** | 4 Jan 2009

Licence	CPOL
First Posted	**4 Jan 2009**
Views	**26,913**
Bookmarked	**24 times**

See Also

- More like this
- More by this author

VC6 VC7 VC7.1 VC8.0 WinXP Win2003 Vista C++ C++/CLI C , +

A tool for creating/verifying MD5 files

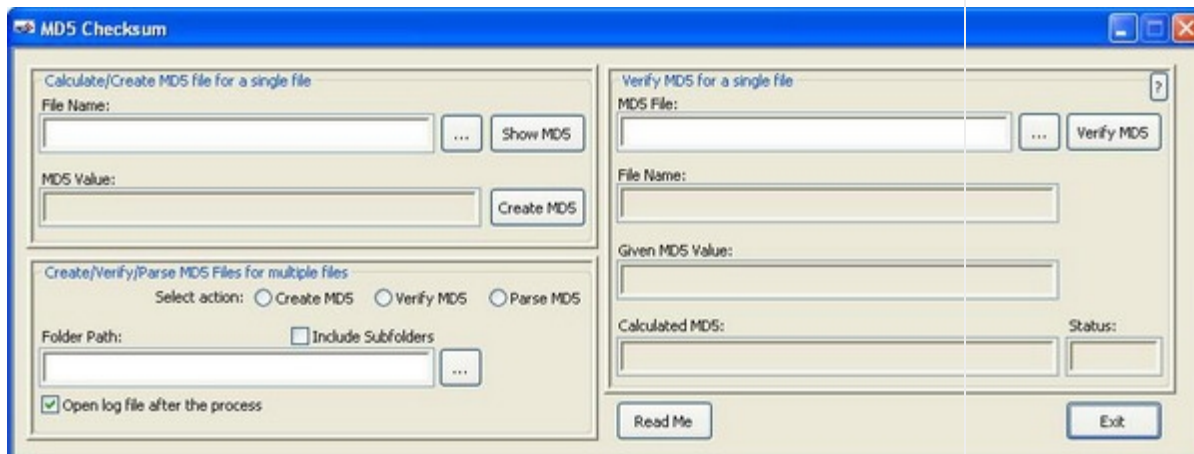**Article** | Browse Code | Stats | Revisions (3) | Alternatives

★★★☆☆   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

```cpp
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;
```

Related Articles

```
    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* Vote

Comments and Discussions

🗎 **New Message**

Search this forum   Go

☐ Profile popups   Noise [Medium ▾] Layout [Normal ▾] Per
                                    page [25 ▾] Update

                              Refresh   First Prev Next

🗎 **MD5 Source in C++** 📌   🗟 **none**   **23:54 28 Feb '09**

🗎 **MD5 is obsolete** 📌   🗟 **wim ton**   **18:09 6 Jan '09**

  🗎 Re: MD5 is obsolete 📌   🗟 TobiasP   3:44 7 Jan '09

🗎 **My vote of 2** 📌   🗟 zengkun100   **11:58 6 Jan '09**

🗎 **牛B** 📌   🗟 **Member 4599072**   **23:16 4 Jan '09**

  🗎 Re: 牛B 📌   🗟 baijun1982   14:01 5 Jan '09

    🗎 Re: 牛B 📌   🗟 Enjon CHEN   18:48 6 Apr '10

      🗎 Re: 牛B 📌   🗟 haohui   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