8.8.1

DATA INTEGRITY – MD5 CHECKSUM

(EZ MD5 CREATOR)

Laboratory Overview

Objective

At the end of this lab students will be able to create a MD5 message digest, or “Fingerprint” of a data file.

Information for Laboratory

A. Students will utilize Easy MD5 Creator
B. Students will utilize Windows notepad text editor

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Easy MD5 Creator should be installed on each student computer. This file may be found as a separate listing in the External Links section of this blackboard course.

Estimated Completion Time

60 Minutes

MD5 Checksum

MD5 was developed by Professor Ronald L. Rivest of MIT, the “R” in “RSA” security.

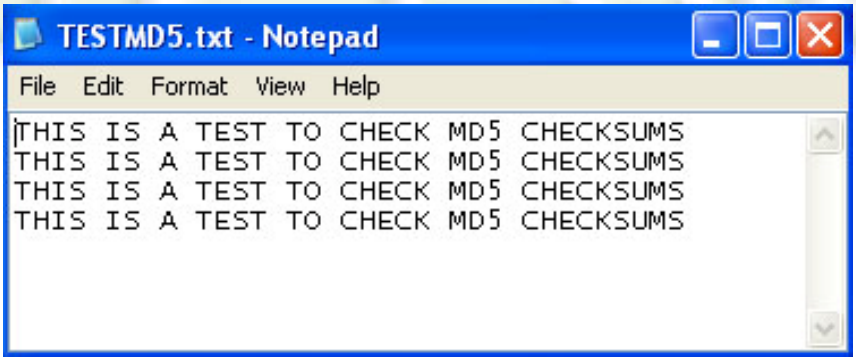
The MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is said that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

In essence, MD5 is a way to verify data integrity, and is much more reliable than standard checksum and many other commonly used methods.

MD5 Checksum Software – using Easy MD5 Creator

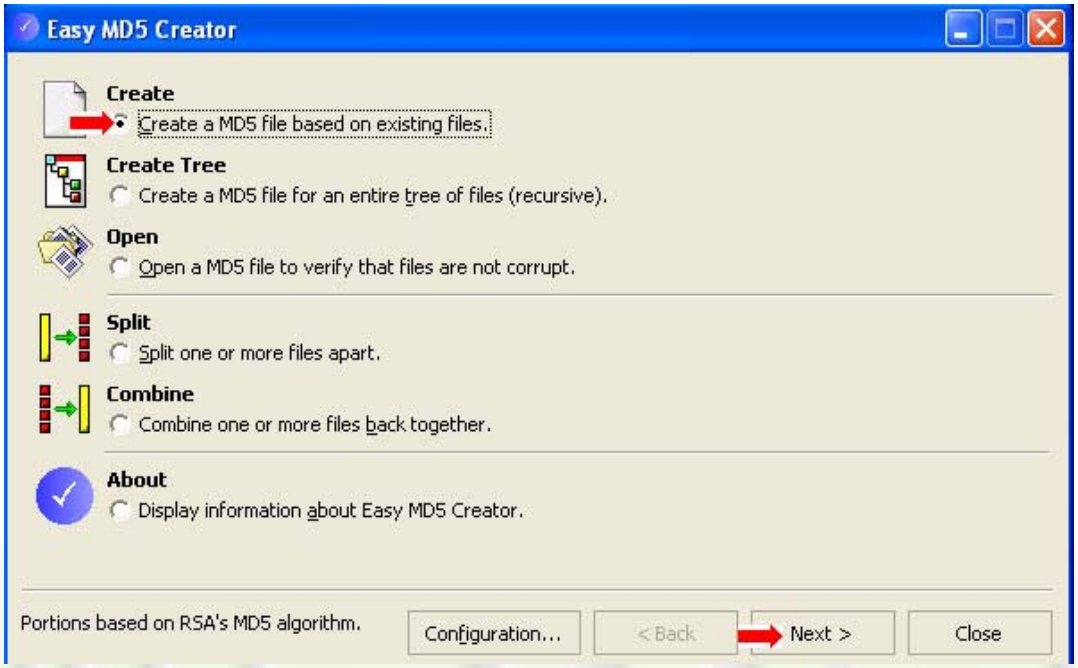
Step 1: Create a test file

Open windows notepad, Click START, All Programs, Accessories, Notepad. Type 4-5 lines of text and save the file as TESTMD5.txt. Your file should look something like this.

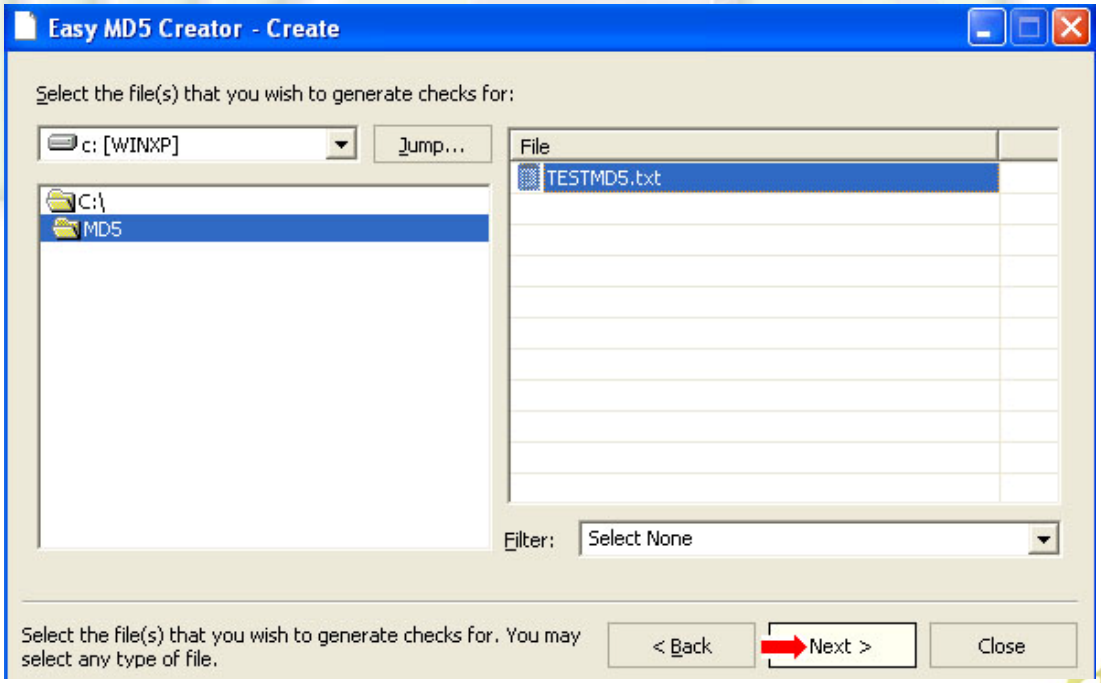


Step 2: Creating a MD5 Hash file

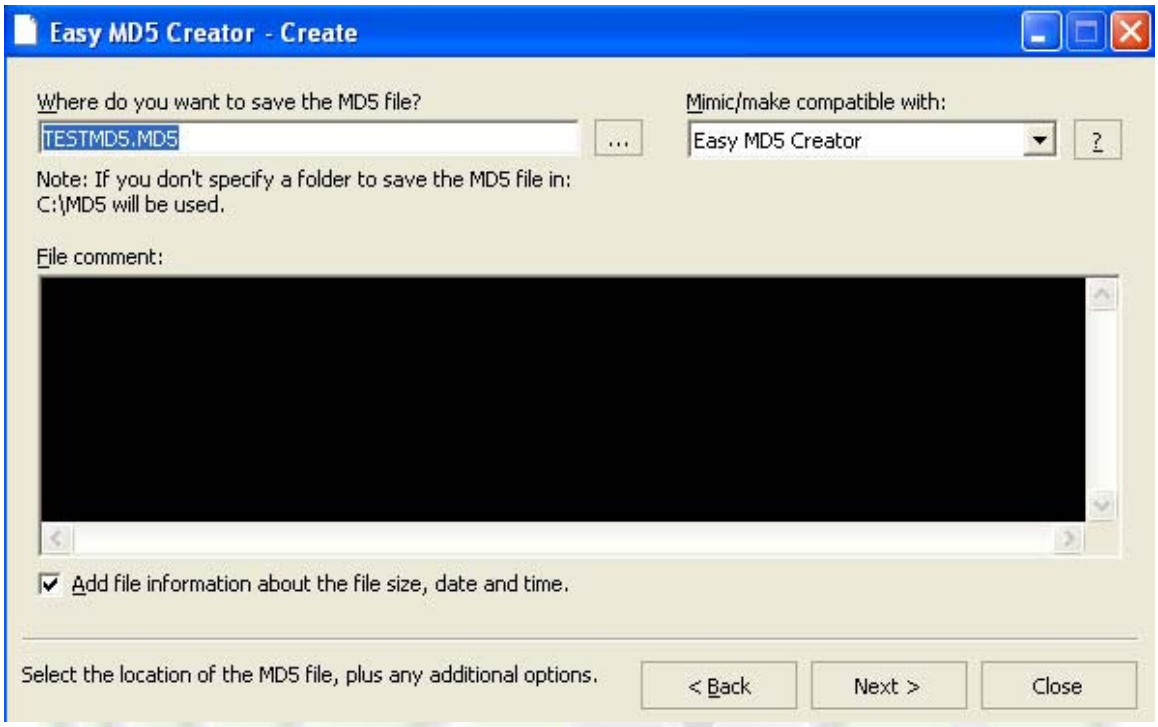
Open Easy MD5 Creator, and choose the option, Create a MD5 file based on existing files and click Next.



Browse the computer on the left side to locate TESTMD5.txt. Select the file TESTMD5.txt to create a MD5 checksum file. Click on TESTMD5.txt to highlight it, and click Next.



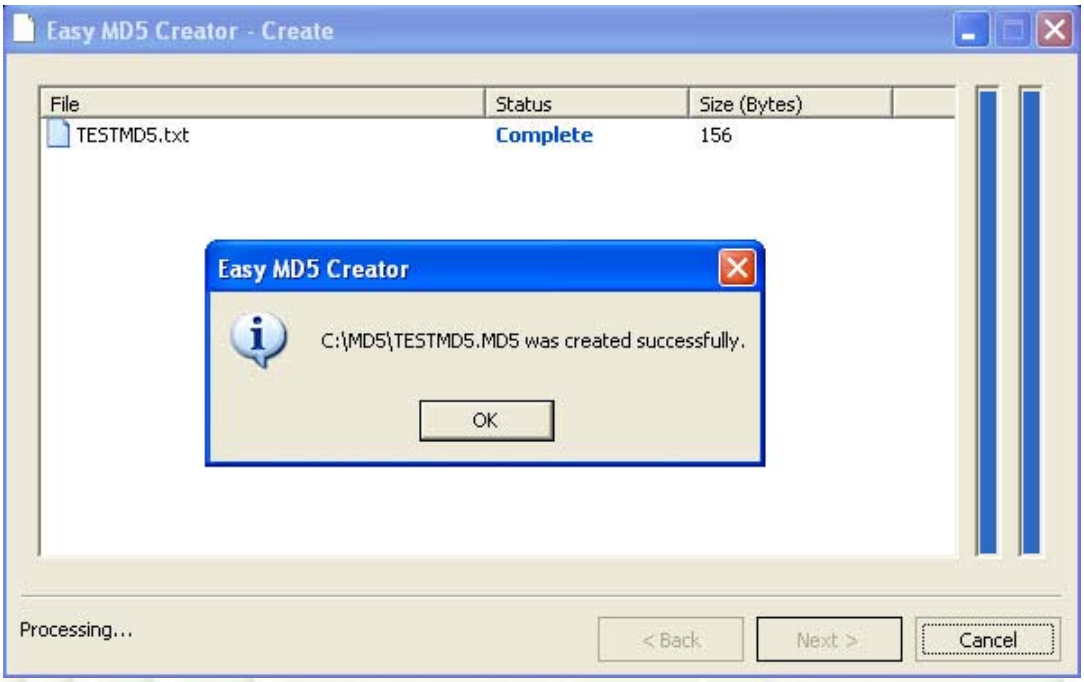
Step 3: Save your MD5 Hash file



Take note of where on the computer you are saving the file. In the example above, it is being save to C:\MD5\TESTMD5.MD5

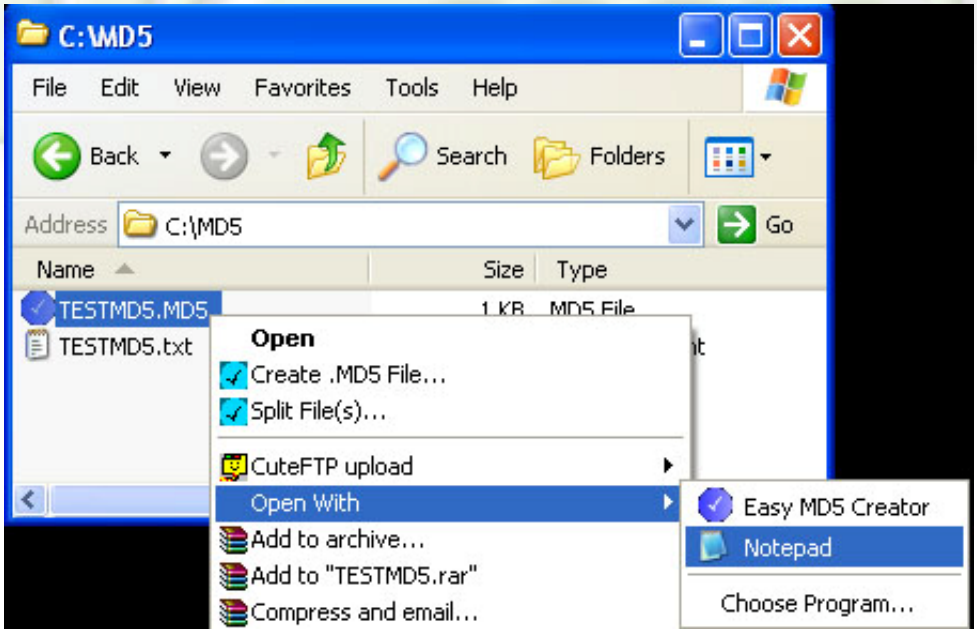
Check to see that the Add file information about file size, date and time box is checked, and click Next.

A dialog box should open showing that your file was created successfully, and the directory path will be listed. Click OK, and close the Easy MD5 program.

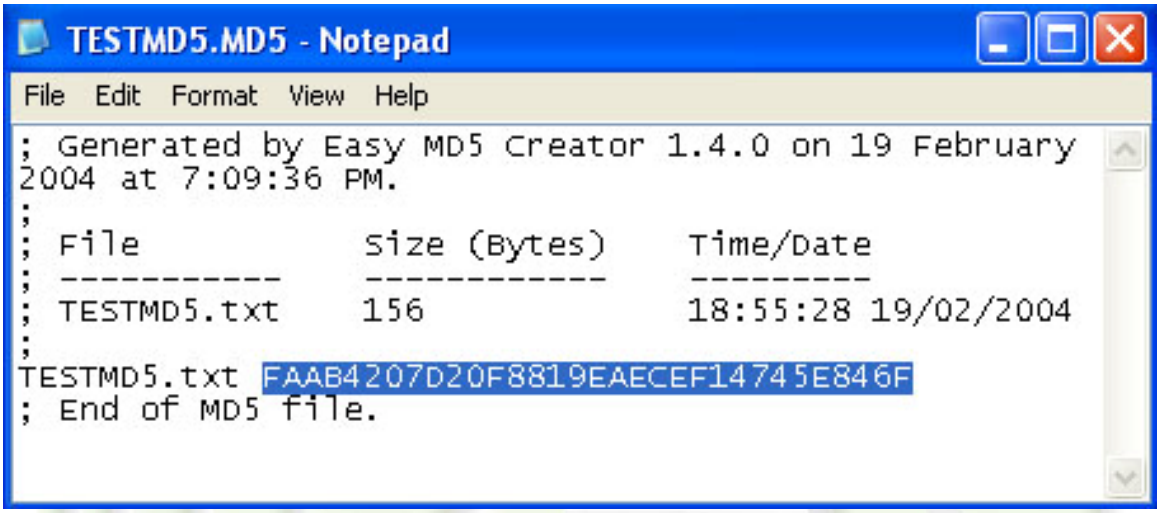


Step 4: Analyze the MD5 file

Using Windows explorer, locate your TESTMD5.MD5 file. Right click on the file, and choose the option, open with, the choose notepad if available, or choose program. Then choose notepad.

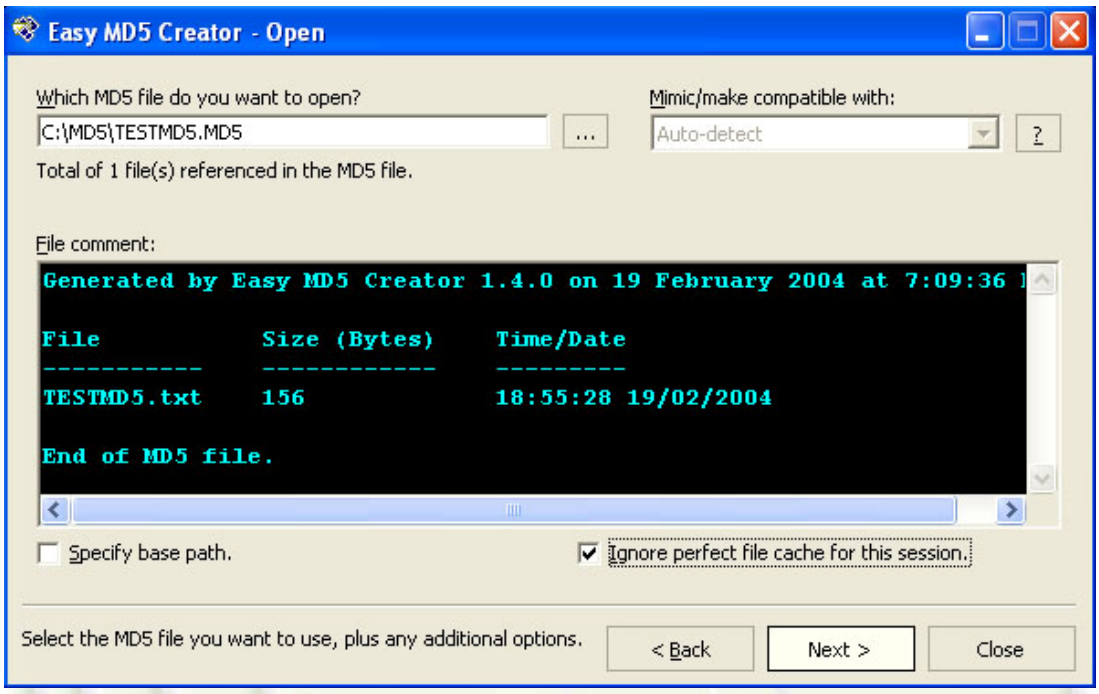


When opened, your TESTMD5.MD5 file should look like the example below. The highlighted text FAAB4207D20F8819EAECEF14745E846F is the MD5 Checksum Value computed from the MD5 Algorithm. Remember, your checksum may be different if your text file is different than the example.

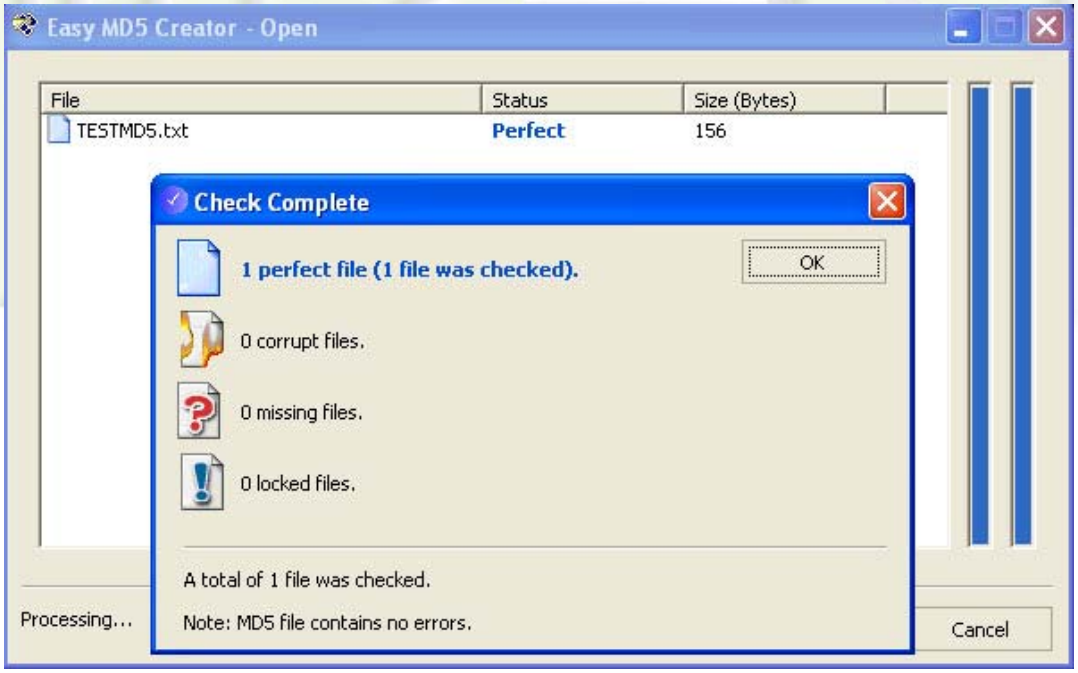


Step 5: Testing the accuracy of the MD5 Hash

Close Notepad. Double click on the TESTMD5.MD5 file to launch Easy MD5 Creator. TESTMD5.MD5 will be loaded and ready to verify against your original file. Make sure the box Ignore perfect file cache for this session is checked, and click Next.

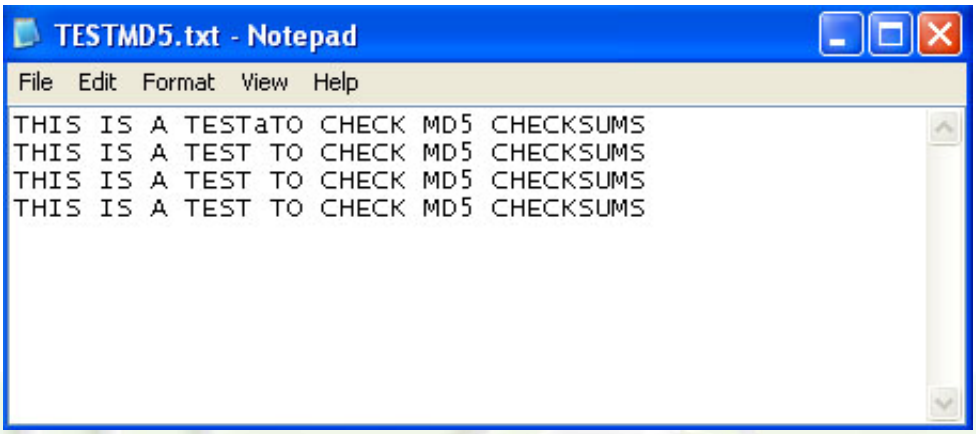


The original data file that is specified in the TESTMD5.MD5 will be re-run through the MD5 Algorithm, and both checksums will be compared.



Step 6: Modifying the original data

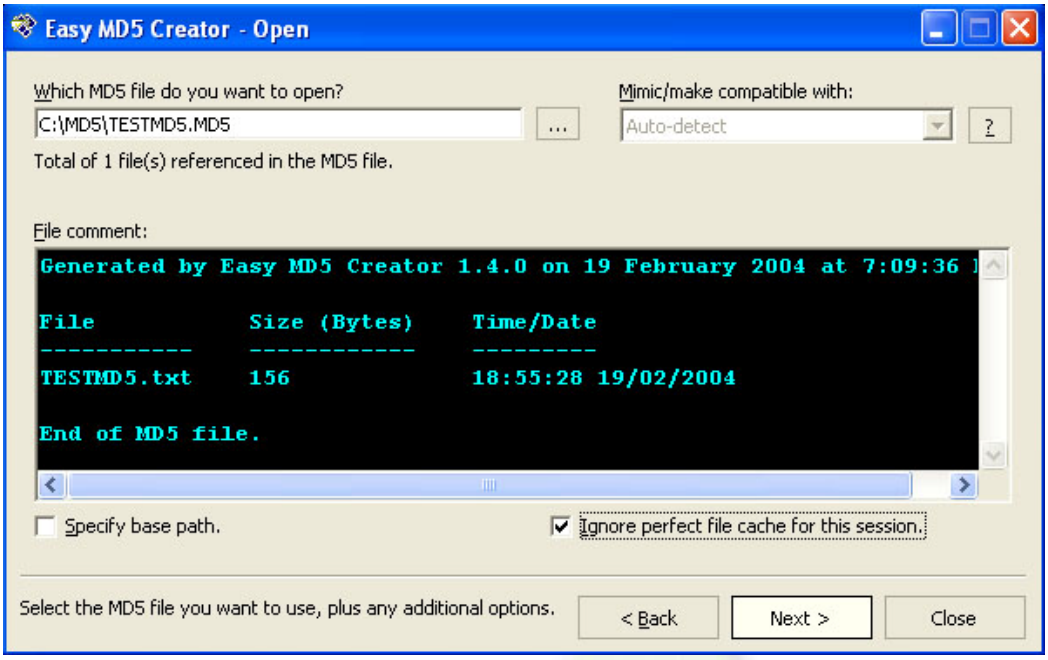
Open the original file TESTMD5.txt with notepad. Make at least one change to the file, and save your changes. Close and reopen the file to verify that changes were made.



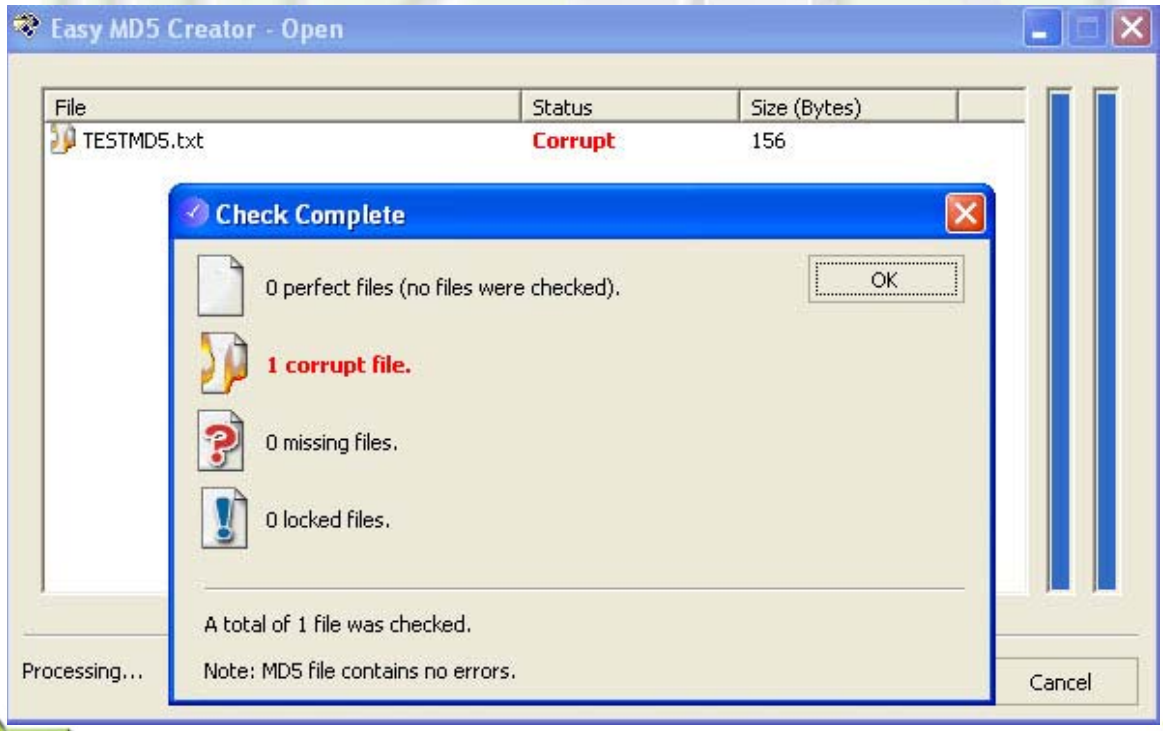
For the example, the letter a was inserted in between TEST and TO. This changes the file, and should create a different MD5 checksum value than the original file.

Step 7: Checking the modified file against the MD5 Checksum from the original file

Close Notepad. Double click on the TESTMD5.MD5 file to launch Easy MD5 Creator. TESTMD5.MD5 will be loaded and ready to verify against your original file. Make sure the box Ignore perfect file cache for this session is checked, and click Next.



The TESTMD5.txt data file is re-run through the MD5 Algorithm, and both checksums will be compared. Since this time, the TESTMD5.txt file has been modified, or corrupted, the MD5 checksum compare fails, and the file is shown to be corrupt.



Analysis

1) For which applications is MD5 Checksums best suited?

2) After working with these utilities, what about MD5 Checksums do you feel you should study further? Why?

3) Why would you use MD5 checksums for Internet file downloads?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More…

Read RFC 1321 ftp://ftp.rfc-editor.org/in-notes/rfc1321.txt

Appendix:

This lab was developed using Easy MD5 Creator Version 1.4.

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).