Final Project

CA-CYESN

Instructions:

1. Read all instructions.
2. Prepare needed files.
3. Write your program code.

Total_____ /60

Objective

The purpose of this project is to implement file hashes, compare file hashes, describe the usage and importance of file hashing, and define file integrity.

Required Material

- Customer-supplied desktop/laptop hardware system
- Windows 10 Professional installed
- MD5deep installed
- MD5deep may be obtained from https://sourceforge.net/projects/md5deep/files/md5deep/md5deep-4.3/md5deep-4.3.zip/download. or
- Download, extract, and move the MD5deep folder to your desktop.

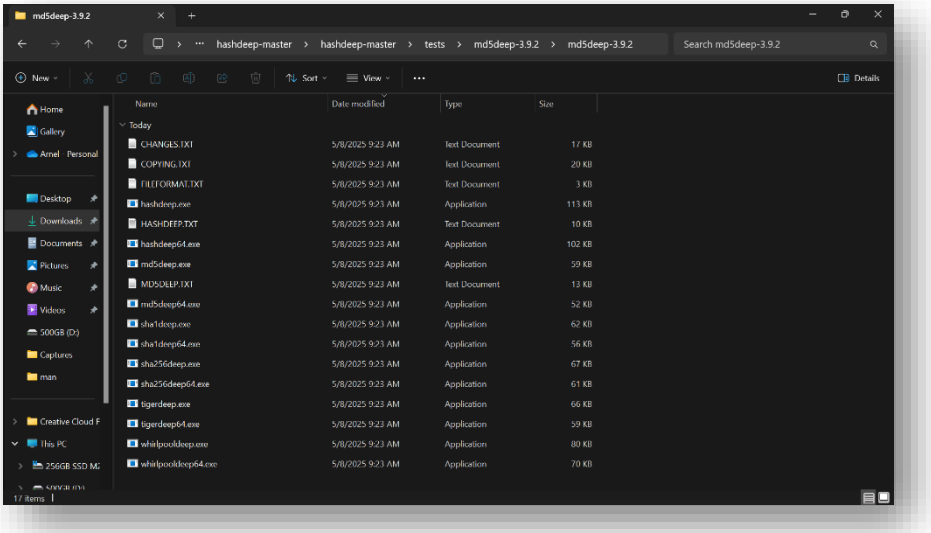
PROJECTS SPECI FICATIONS

Instructions

In this procedure, you will create and compare hashes. You will also tamper with the file to witness the differences in hashing, so you will better understand what ensuring file integrity really means.

Part1 1:

1. Power on your machine.
2. Log on to your computer using your administrative account.
3. Double-click the md5deep-4.3 folder, located on the desktop.
4. To help navigate which files are which, you will change the view option to show the file extensions of each file.
5. Click the View tab near the top left of the window and place a check in the box next to File Name Extensions; this will add the extensions to each file to help you navigate which files are which. **(Screenshot Required)**



6. Locate md5deep.exe, sha1deep.exe, and whirlpooldeep.exe.These will be the hash algorithms

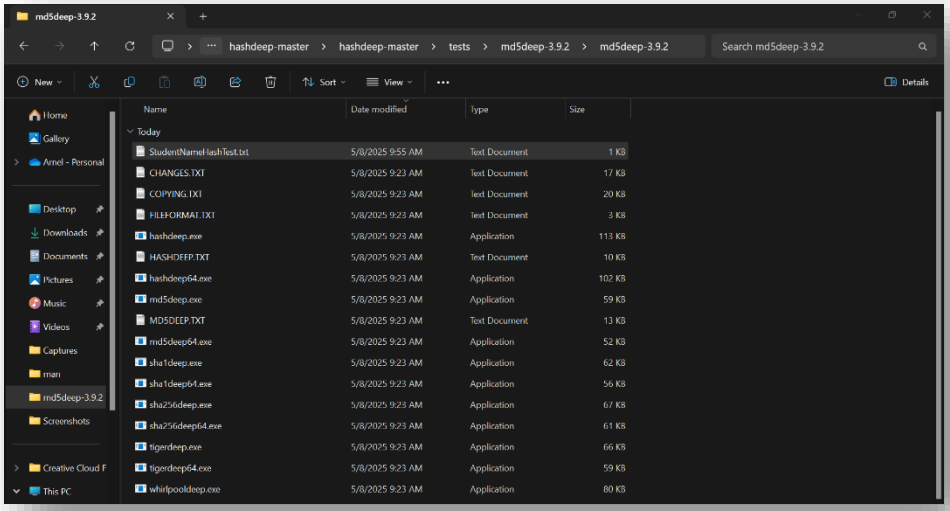
you will test.

Part 2:

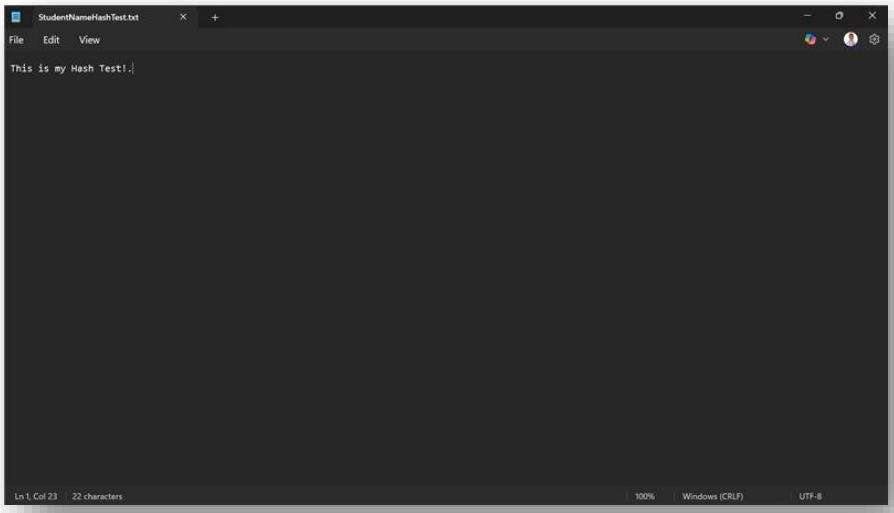
Creating a Test File

Create a test file in the same folder as the hash algorithms. Using the command line can be difficult if you are not familiar with it, so keeping the file in the same folder will create an easier environment to navigate.

1. Right-click any empty white space in the right pane.
2. Navigate to and select New ➢ Text Document.
3. You will be prompted to create a name for the new text document. Type **StudentNameHashTest** as the name. Notice the file is given a .txt extension. Press Enter to confirm. **(Screenshot Required)**



4. Double-click the **StudentNameHashTest.txt** file to open it in Notepad.
5. Type **This is my Hash Test!. (Screenshot Required)**



6. Click File, and then select Save to save the contents. Exit Notepad by clicking on the red X in the top-right corner of the window.

Part 3:

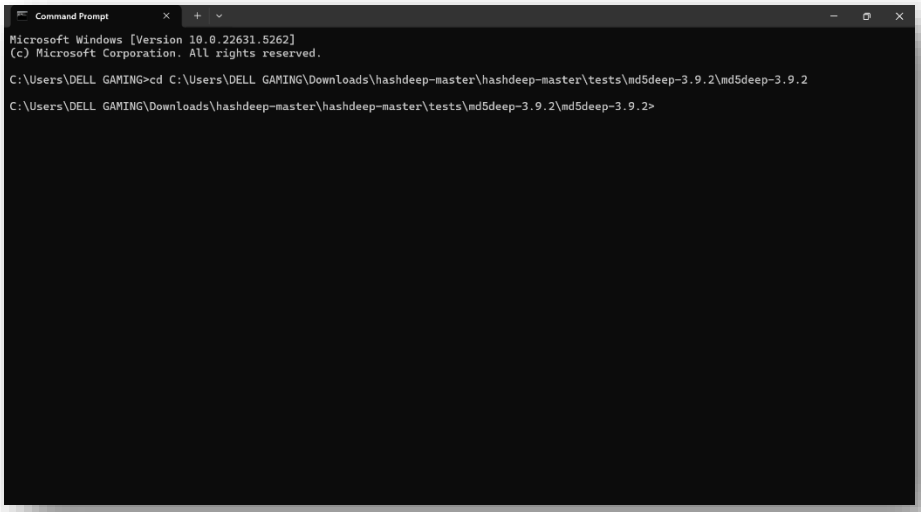
Creating Multiple Hashes

A hash is similar to a digital fingerprint. It is considered secure if it includes a fixed size, is unique, and cannot be reversed to reveal the original plaintext.

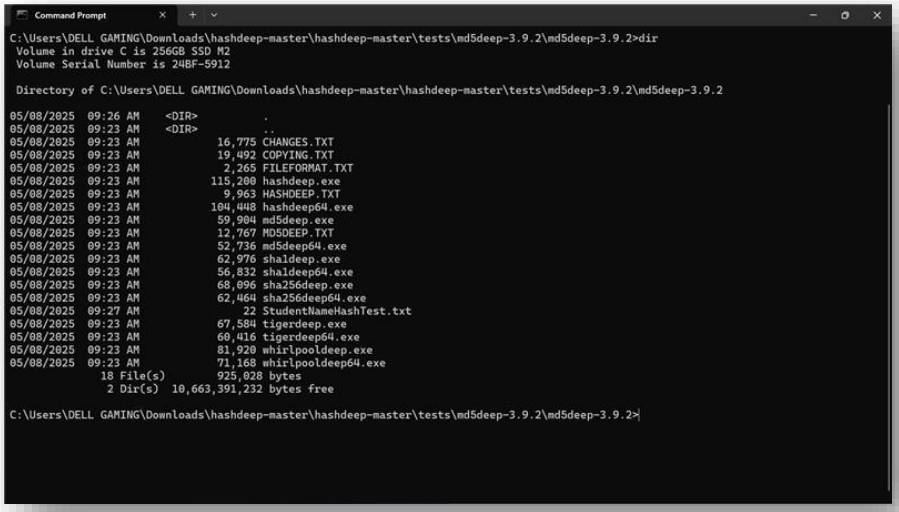
1. Leave the md5deep-4.3 folder open.

2. To locate the command prompt, type cmd in the embedded search bar and press Enter. The Command Prompt window will be launched.

3. You will need to change directories to be inside the md5deep-4.3 folder. Type cd C:\users\your account name\desktop\md5deep-4.3 and press Enter. You will be redirected to the folder **(Screenshot Required)**

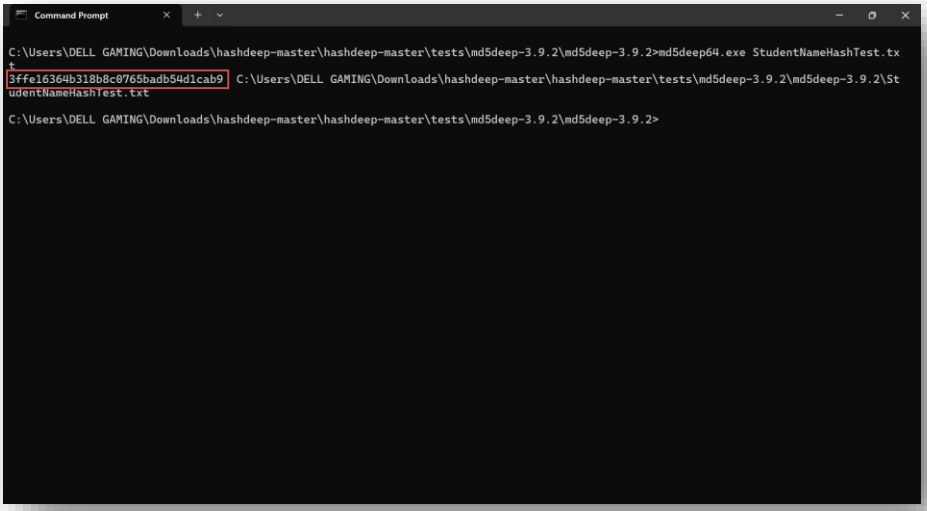


4. Now that the command prompt is located in the folder, you can view the contents by typing dir and pressing Enter. The contents of the folder will be displayed **(ScreenShot Required)**



Here you can see the same contents as within the Windows Explorer. Locate the hash algorithms you will be using, along with the StudentNameHashTest.txt file. Understand that to use these command-line tools you will need to type the entire filename with its associated extension.

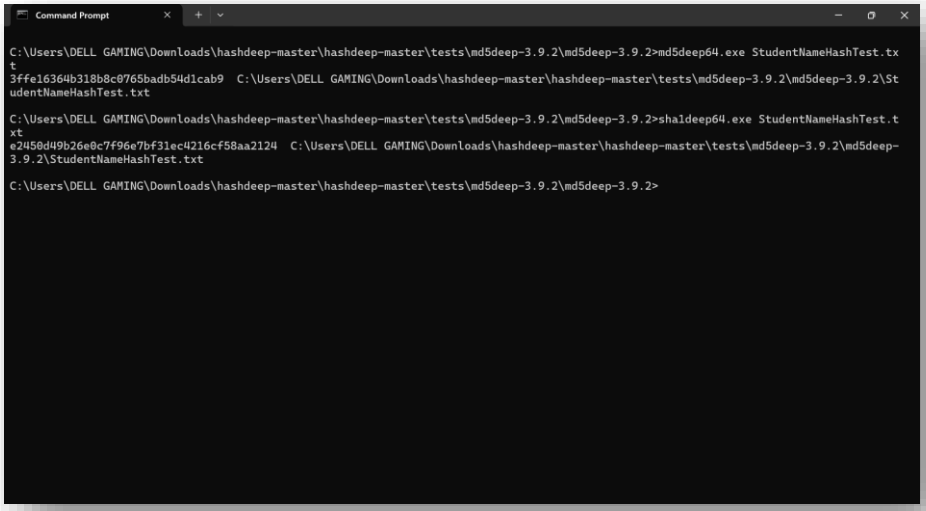
5. To create your first hash, type md5deep.exe StudentNameHashTest.txt. This tells the computer to use MD5 to create a hash of StudentNameHashTest.txt. Press Enter to create the hash**. (Screenshot Required)**



You should see a string of characters, as illustrated in the figure. This represents your file with the MD5 hash algorithm applied to it.

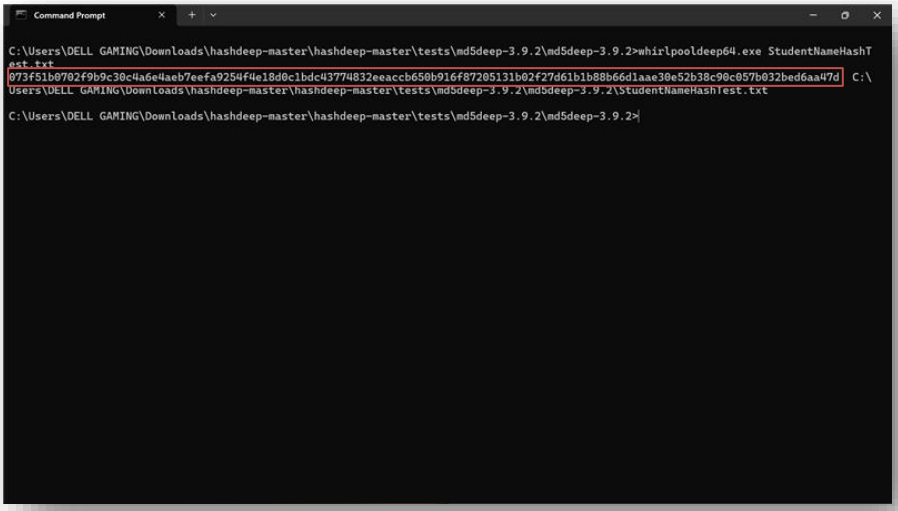
NOTE
You will receive an error if you attempt to use md5deep.exe on a 64-bit system. If you are currently using a 64-bit system, use md5deep64.exe. The same will be true for the following hash algorithms as well. Proper Hash output for 64-bit version is shown in Figure Below

6. Now type sha1deep.exe StudentNameHashTest.txt and press Enter, The string of numbers and letters represents your file with the Sha-1 hash algorithm applied to it. **(Screenshot Required)**



Notice that the hash output has more characters than the MD5 hash. The MD5 hash output is 128 bits, while the Sha-1 hash output is 160 bits. SHA (secure hash algorithm) is considered more secure.

7. Finally, type whirlpooldeep.exe StudentNameHashTest.txt and press Enter. This will use the Whirlpool hash algorithm on the text file. **(Screenshot Required)**



The Whirlpool hash algorithm employs an astounding 512-bit digest to the file, much larger than the previous two hashing algorithms.

Part 4:

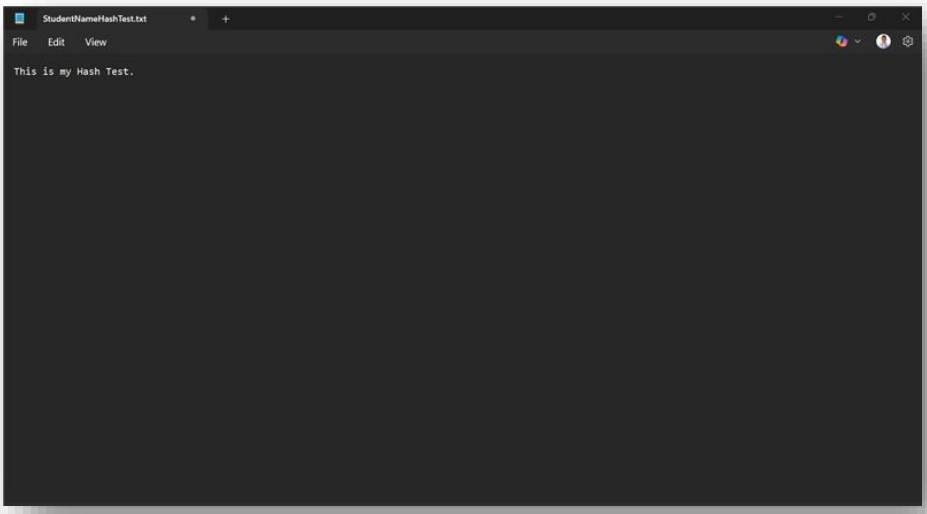
Tampering with a File

The purpose of the hash is verifying file integrity. Now let's tamper with the file in a minimal way so you can later attempt to discern the subtle difference.

1. Leave the Command Prompt window open and return to the Windows Explorer window with the md5deep-4.3 folder open.

2. Double-click the HashTest.txt file to open it. Notepad will launch.

3. Delete the exclamation point and insert a period. The contents should now read, This is my Hash Test., **(Screenshot Required)**



4. Click File and select Save to save the file. Exit Notepad by clicking on the red X in the top-right corner of the window.
5. Exit the Windows Explorer window by clicking on the red X in the top-right corner of the window.

Part 5:

Comparing Hash Values

You might think with such a subtle change to the contents of the file that a hash output might be similar. You will now discover the importance of hash output by comparing the before and after of the file hashes.

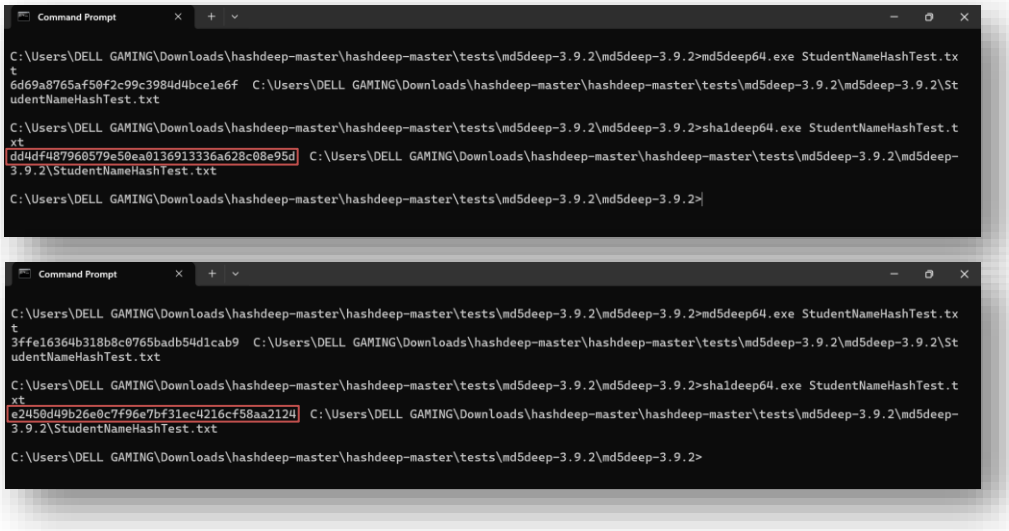
1. Return to the command prompt. You should be able to view the three previous hashes.
2. At the prompt, type md5deep.exe StudentNameHashTest.txt. This will create a hash of the newly tampered with HashTest file. Press Enter.

Is there a difference between your new hash and your previous hash?

Ans Yes

As comparing this hash to the first hash reveals a completely different set of characters. This verifies the file's integrity. (**Screenshot Required)**

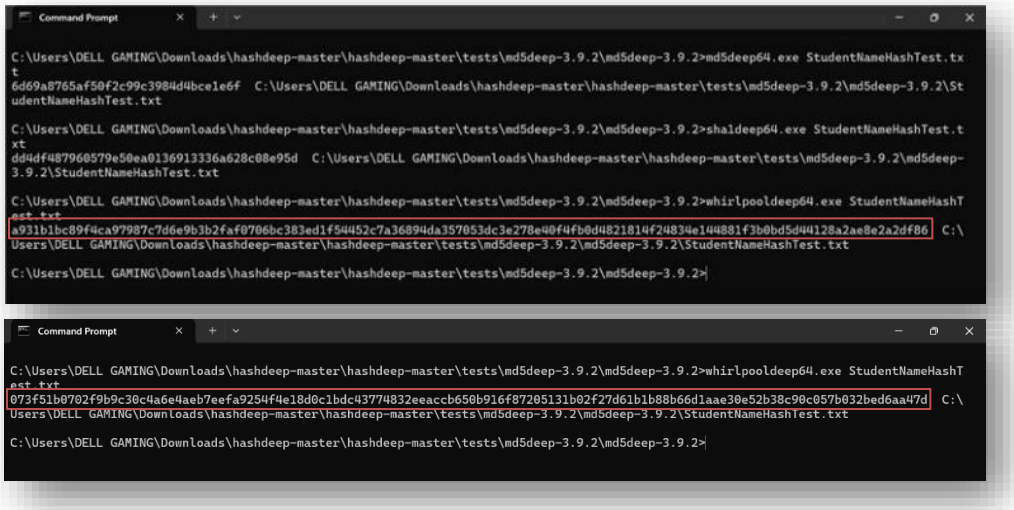
3. Type sha1deep.exe HashTest.txt and press Enter. The resulting hash will be displayed and should be different from the earlier hash **(Screenshot Required)**



When you compare your Sha-1 outputs, is there a difference?

Ans: Yes

4. Finally, type whirlpooldeep.exe HashTest.txt and press Enter.There should be a difference between the previous hash and the new hash. **(Screenshot Required)**



Is there a difference between your hashes?

Ans: Yes

5. Exit the command prompt by typing exit and pressing Enter.
6. Shut down the computer.

MARKING SCHEME

You will be graded on:

Project component	Points
Part 2	20
Part 3	20
Part 4	20
Part 5	20
The total number of possible points is :	100%