

Using md5deep to calculate hashes

Overview: In this exercise, students learn to compute a hash on a file. There are some additional exercises on using md5deep.



Instructor Notes Begin

Importance [1-10]: 9

Goal: Students learn to compute hashes.

Assessment: Ensure the student knows how to open a command prompt and is able to browse to a directory from the prompt. The student should be able to compute the hash of a file.

Instructor Notes End



Open a command prompt by clicking “Start-->Run” and then typing “cmd.exe.”

Browse to the location where your files are located using the “cd” command.

Type “dir” once you are in the directory and you should see a listing similar to the one below:

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\pfeiffersec\md5deep-3.9.2>dir
Volume in drive C has no label.
Volume Serial Number is F49B-B7EA

Directory of C:\Documents and Settings\pfeiffersec\md5deep-3.9.2

08/21/2011  09:34 AM    <DIR>          .
08/21/2011  09:34 AM    <DIR>          ..
08/21/2011  09:30 AM             16,776 CHANGES.TXT
07/25/2011  07:46 PM             19,492 COPYING.TXT
07/25/2011  07:46 PM              2,265 FILEFORMAT.TXT
07/25/2011  07:46 PM            115,200 hashdeep.exe
07/25/2011  07:46 PM              9,963 HASHDEEP.TXT
07/25/2011  07:46 PM           104,448 hashdeep64.exe
07/25/2011  07:46 PM             59,904 md5deep.exe
07/25/2011  07:46 PM             12,767 MD5DEEP.TXT
07/25/2011  07:46 PM             52,736 md5deep64.exe
07/25/2011  07:46 PM             62,976 sha1deep.exe
07/25/2011  07:46 PM             56,832 sha1deep64.exe
07/25/2011  07:46 PM             68,096 sha256deep.exe
07/25/2011  07:46 PM             62,464 sha256deep64.exe
07/25/2011  07:46 PM             67,584 tigerdeep.exe
07/25/2011  07:46 PM             60,416 tigerdeep64.exe
07/25/2011  07:46 PM            81,920 whirlpooldeep.exe
07/25/2011  07:46 PM            71,168 whirlpooldeep64.exe
               17 File(s)          925,007 bytes
               2 Dir(s)  16,930,140,160 bytes free

C:\Documents and Settings\pfeiffersec\md5deep-3.9.2>_
```

Illustration 1: Directory listing of the md5deep-3.9.2 contents

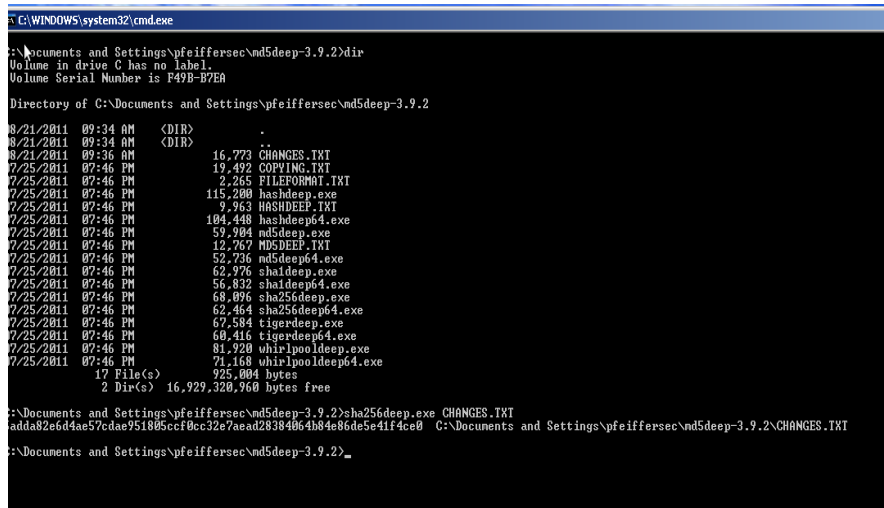
This provides a listing of the hash functions available in the hashdeep suite.

We'll use sha256deep.exe for this exercise. To compute the hash it is as simple as typing:

```
sha256deep.exe <filename>
```

where <filename> is the name of the file you want to hash. In this example, we'll compute the hash of the file "CHANGES.TXT" by typing:

```
sha256deep.exe CHANGES.TXT
```



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\pfeiffersec\nd5deep-3.9.2>dir
Volume in drive C has no label.
Volume Serial Number is F49B-B7EA

Directory of C:\Documents and Settings\pfeiffersec\nd5deep-3.9.2

08/21/2011 09:34 AM <DIR>          .
08/21/2011 09:34 AM <DIR>          ..
08/21/2011 09:36 AM             16,773 CHANGES.TXT
07/25/2011 07:46 PM             19,492 COPYING.TXT
07/25/2011 07:46 PM              2,265 FILEFORMAT.TXT
07/25/2011 07:46 PM            115,200 hashdeep.exe
07/25/2011 07:46 PM              9,963 HASHDEEP.TXT
07/25/2011 07:46 PM            104,448 hashdeep64.exe
07/25/2011 07:46 PM             59,904 md5deep.exe
07/25/2011 07:46 PM             12,767 MD5DEEP.TXT
07/25/2011 07:46 PM            52,736 md5deep64.exe
07/25/2011 07:46 PM            62,976 sha1deep.exe
07/25/2011 07:46 PM            56,832 sha1deep64.exe
07/25/2011 07:46 PM            68,096 sha256deep.exe
07/25/2011 07:46 PM            62,464 sha256deep64.exe
07/25/2011 07:46 PM            67,584 tigerdeep.exe
07/25/2011 07:46 PM            60,416 tigerdeep64.exe
07/25/2011 07:46 PM            81,920 whirlpooldeep.exe
07/25/2011 07:46 PM            71,168 whirlpooldeep64.exe
               17 File(s)          925,004 bytes
                2 Dir(s)  16,929,320,960 bytes free

C:\Documents and Settings\pfeiffersec\nd5deep-3.9.2>sha256deep.exe CHANGES.TXT
5adda82e6d4ae57cdae951805ccf0cc32e7aead28384064b84e86de5e41f4ce0 C:\Documents and Settings\pfeiffersec\nd5deep-3.9.2\CHANGES.TXT
C:\Documents and Settings\pfeiffersec\nd5deep-3.9.2>
```

The result is: 5adda82e6d4ae57cdae951805ccf0cc32e7aead28384064b84e86de5e41f4ce0

As long as the file CHANGES.TXT never changes, the hash should always be the same whether you compute the hash on Windows XP, Windows 7, Windows 2008, Mac OS X, Linux, etc.

Extra exercise.

This is a very basic method of computing a hash on all files within a directory to determine if a file has changed. This method should not be used for full production use for file integrity monitoring. The Learn SIA course will discuss other tools that are designed for full production use of monitoring the integrity of files and directories on your system in later lessons.

In the same directory where the md5deep folder was extracted, run the command:

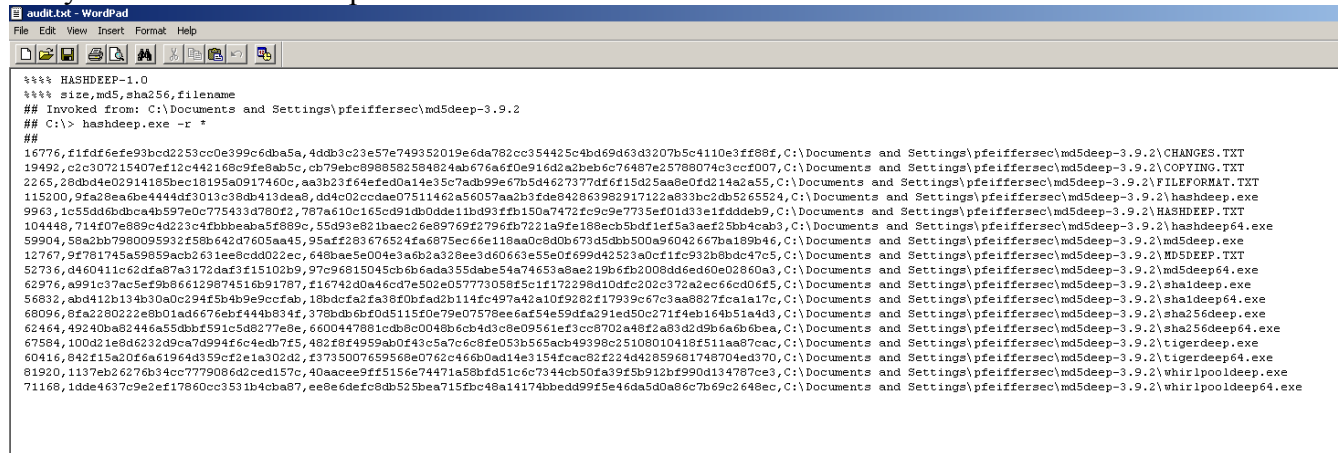
```
hashdeep.exe -r * > ..\audit.txt
```

The "-r" is recursive meaning it will compute the hash of all files in all subdirectories beneath the folder path you specified. The "*" is used to indicate we are only computing the hashes in the current directory (and if there were additional folders within this directory, it would compute the hashes for those too). The ">" sign is used to redirect the output of the command into the file "audit.txt."

After you execute the command above, open the file using wordpad with the command:

```
write ..\audit.txt
```

and you should see the output.



Now, close the file audit.txt and open the file “CHANGES.TXT” and change anything in the file. Add a letter, a space, or delete something. Then “Save” and close the file. Now we'll use the “audit.txt” file to determine if anything has changed. Run the command:

```
hashdeep.exe -r -vv -a -k ..\audit.txt *
```

What is the output?

Run the command:

```
hashdeep.exe -h
```

to determine what the options (or switches) “-a”, “-vv”, and “-k” mean.

What does each switch mean?

-a = _____

-v = _____

-k = _____