Using MD5 Hash

Feb 2017

Okay, so MD5 Hash isn't strictly a Linux thing, but I do see it used more in Linux systems than in Windows, so I have put it in the Linux Section.

What is MD5?

MD5 which stands for Message Digest algorithm 5 is a widely used cryptographic hash function that was invented by Ronald Rivest in 1991. The idea behind this algorithm is to take up a random data (text or binary) as an input and generate a fixed size “hash value” as the output. The input data can be of any size or length, but the output “hash value” size is always fixed.

What is MD5 Used For?

MD5 is a hash value that is stored along with a file on the internet, say on a web (WWW) or FTP server. When you download the file (lets say it's a new Linux .ISO file) you can also download the MD5 Hash file.

Whatever you download, you will have two files, the actual data file, and an MD5 Hash file.

```
-rw-r--r--. 1 root root 85063755 Feb  3 03:27 LinuxISO.gz
-rw-r--r--. 1 root root       33 Feb  3 03:27 LinuxISO.tar.gz.md5
```

If you look at the .md5 file contents, there will be a hash value.

```
3213fe6869acbf1b7d4945f2edd9fe3b
```

How to use MD5 Hash

Now that you have downloaded your Data file and MD5 Hash file, and checked the MD5 Hash value, you can verify the MD5 Hash value from Linux.

From the command line, in the folder where your downloaded files are, use the following syntax:

```
md5sum filename

So for or example:

md5sum LinuxISO.tar.gz
3213fe6869acbf1b7d4945f2edd9fe3b  LinuxISO.gz
```

Now compare the MD5 Hash value you just generated, with the downloaded MD5 Hash, if they match, then the integrity of the download is good, if they differ then you may have some file corruption.