CHECKSUM Utilities for ‘hashing’ files (TAMPER DETECTION)

You just received a file from a friend over the internet...

How do you know the file you received has not been corrupted while being sent to you, whether over the internet, while being transferred to a thumb drive, or over the air via ham radio digital modes?

Or, how do you know it wasn’t intercepted and maliciously altered before being passed along to you?

To verify that a file you have received is genuine, uncorrupted, or has not been altered or tampered with (maliciously or inadvertently), there is a simple and free, but powerful tool, available called Checksum Utilities. They are free downloadable programs.

What does a checksum utilities do? They ‘hash’ files. Any computer file.
What does that mean? It means it determines a unique fingerprint made up of seemingly random letters and numbers for a particular file.
How? Encryption algorithms used to generate (or determine) the ‘hash’ (unique fingerprint) of a file.

If one single letter or punctuation mark has been removed or changed, if the file name is changed, if an image is re-sized or an effect added to it, if one space or hyphen is added to a sentence, even if one letter is changed to a bold font, or if one thousandth of a second is added or removed from an audio file, it will alter the hash of that file. You’ll know SOMETHING has changed from the original file.

This applies to audio files, movie files, text files, word documents, spreadsheets, etc.

This is important even over amateur radio when precise information must be correct, and lives are on the line. If a doctor is giving specific instructions about the type or amount of medication to give, if a stranded party needing rescue provides grid coordinates of their location, or if net schedule instructions for a specific time window or mode or frequency are being conveyed, the information must be exact. Not garbled. Not somewhat ‘mostly’ readable. It has to be perfect with no mistakes.

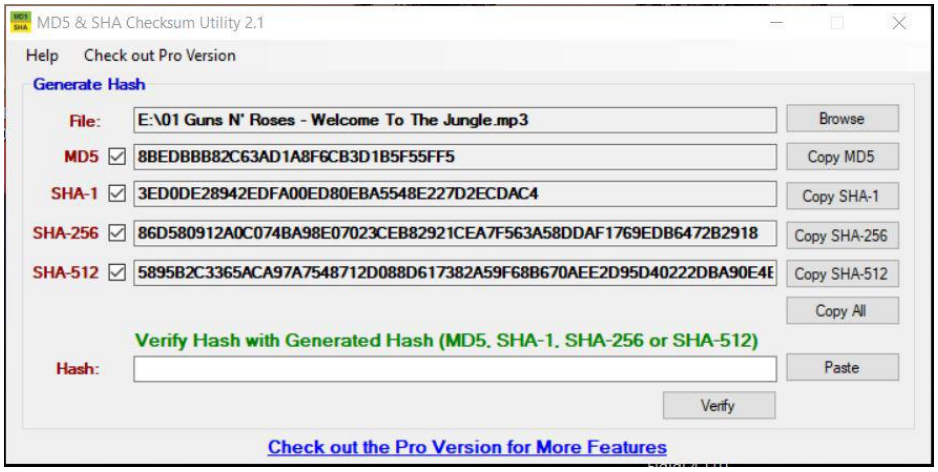
Also, hashes cannot be backward engineered. In other words, if a hash is intercepted computer forensics specialists cannot determine the contents or nature of the file simply by the hash (string of letters and numbers).

It looks like this: 3ed0de28942edfa00ed80eba5548e227d2ecdac4

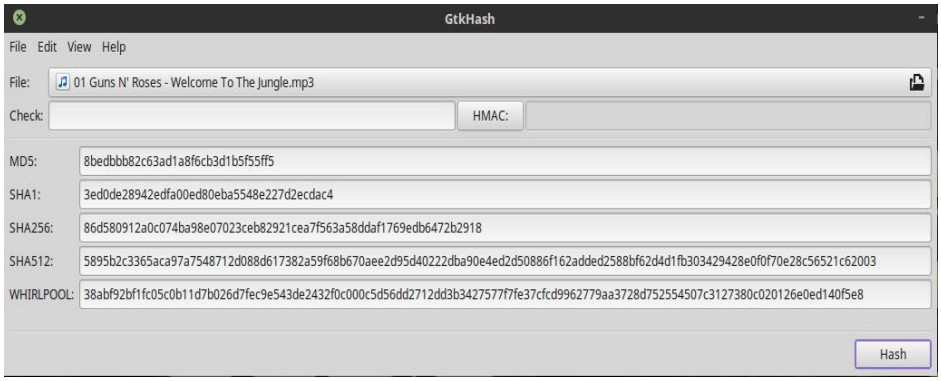
In the example below, an mp3 music file was used by dragging and dropping the file into the ‘File:’ box in the Checksum utility (program). Click the ‘create’ or ‘generate’ hash button and a hash for that file is created. Copy and paste the hash you wish to use (your choice) and send it to the other party. Then you would send your mp3 audio file to the other party. He should be able to drop the file into his Checksum utility and the hash that you sent him (into the ‘Hash:’ box) then click the ‘Verify’ button.

Windows: use **MD5/SHA Hash**
To download, go to:

https://download.cnet.com/MD5-SHA-Checksum-Utility/3000-2092_4-10911445.html



Linux: use GtkHash
To download:
Visit the Linux repositories and search for ‘GtkHash’



Experiment with it. Hashes can also be used for generating complex passwords, etc. which you can easily recover over and over for copy/pasting. Just be sure the file you use to create the hash is not altered in any way.