LOVELY
PROFESSIONAL
UNIVERSITY

INT 301-Open Source Technologies

CA-III

Submitted by:

Uyyuru Vamsidhar Reddy

REG NO: 11905170

ROLL NO: 12

33. Calculate MD5 and SHA1 and CRC32 (10 files) for making a comparison of files and check all the files for integrity, internet downloads and data tampering

1. Introduction:

Calculating MD5, SHA1, and CRC32 checksums can be a useful way to verify the integrity and authenticity of downloaded files and to detect any data tampering that may have occurred during transmission. These checksums are cryptographic hash functions that generate a fixed-size, unique value based on the content of a file, and can be used to compare two files and determine if they are identical or if they have been modified in any way.

By comparing the checksum values of two files, you can determine if they are identical, even if they have different names or file extensions. This can be particularly useful when downloading software, updates, or other files from the internet, where file names and extensions may be altered or obscured in some way.

When downloading files from the internet, it's important to verify the integrity of the files using checksum values to ensure that they have not been tampered with during transmission. Data tampering can occur when a file is intercepted and modified by a third-party during transmission, either to insert malware or to alter the content of the file in some other way. Verifying the checksum values of downloaded files can help to detect this kind of tampering and ensure that the downloaded files are safe and authentic.

Overall, calculating MD5, SHA1, and CRC32 checksums is a useful technique for verifying the integrity of files and detecting data tampering, and is a recommended practice for anyone who downloads files from the internet.

1.1 Objective of the project:

The objective of the project is to demonstrate how cryptographic hash functions can be used to verify the integrity and authenticity of files, especially those downloaded from the internet. The project aims to provide a practical example of how to use checksums to compare two files and determine if they are identical, even if they have different names or file extensions.

The project also aims to highlight the importance of verifying the checksums of downloaded files to detect any data tampering that may have occurred during transmission. This is particularly important in the context of internet downloads, where files may be intercepted and modified by a third-party during transmission. Overall, the project aims to show users about the benefits of using checksums to ensure the integrity and authenticity of files, and to provide a practical demonstration of how to calculate and compare MD5, SHA1, and CRC32 checksums for files.

1.2 Description of the project:

Select 10 files of different types (e.g., documents, images, videos, software installers, etc.) that you want to compare and verify for integrity. Download the 10 files from a trusted source or from the internet. Use a checksum calculation tool or utility to calculate the MD5, SHA1, and CRC32 checksums for each of the 10 files. These checksum values are unique and fixed-size values that are generated based on the content of the file. Compare the checksum values for each file to ensure that they are identical. If the

checksum values for a file are different, this indicates that the file has been modified or corrupted in some way. Verify the integrity of the downloaded files by comparing the calculated checksum values with the checksum values provided by the file creator or the source from which the file was downloaded. This ensures that the downloaded file has not been tampered with during transmission.

1.3 Scope of the project:

The scope of the project is to select the files for the project, calculate the checksums for the files and compare the checksums with original checksums provided by trusted sources which helps in the verification of integrity of the downloaded files. The scope of this project is limited to the calculation and comparison of MD5, SHA1, and CRC32 checksums for the files. However, the concepts and techniques learned can be applied to a wider range of files and can help users to develop best practices for downloading and verifying files from the internet.

2. System Description:

Window 11 operating system

8gb RAM

Intel CORE i7 8th generation processor

Hash MY Files tool to calculate checksums.

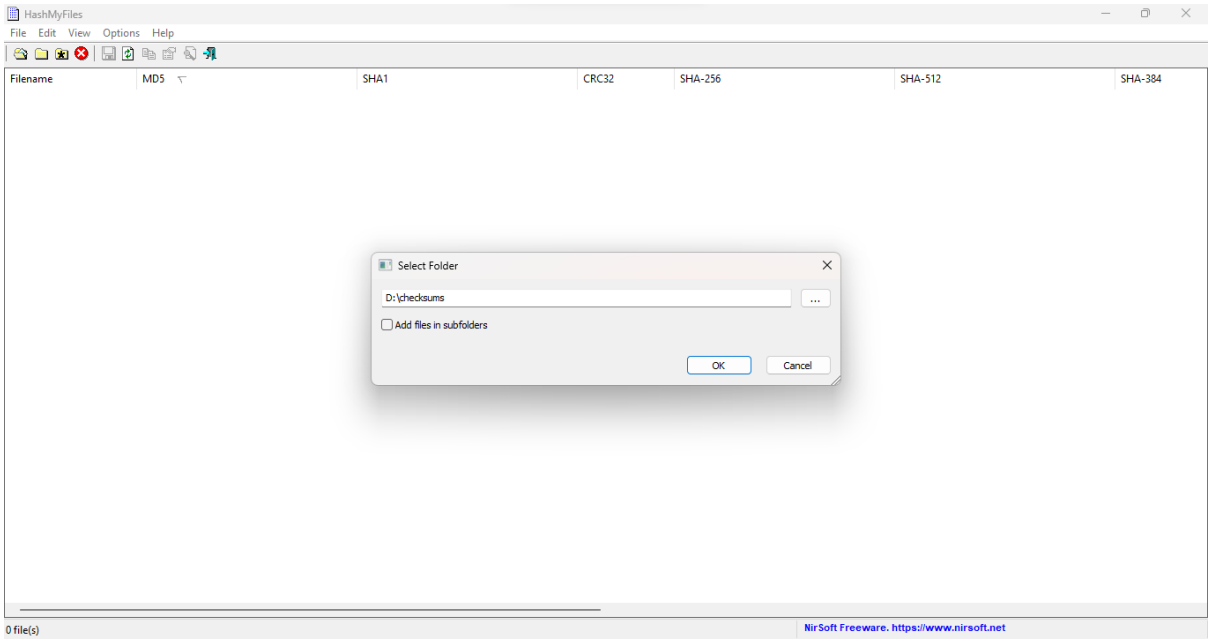
2.1 Assumptions and Dependencies:

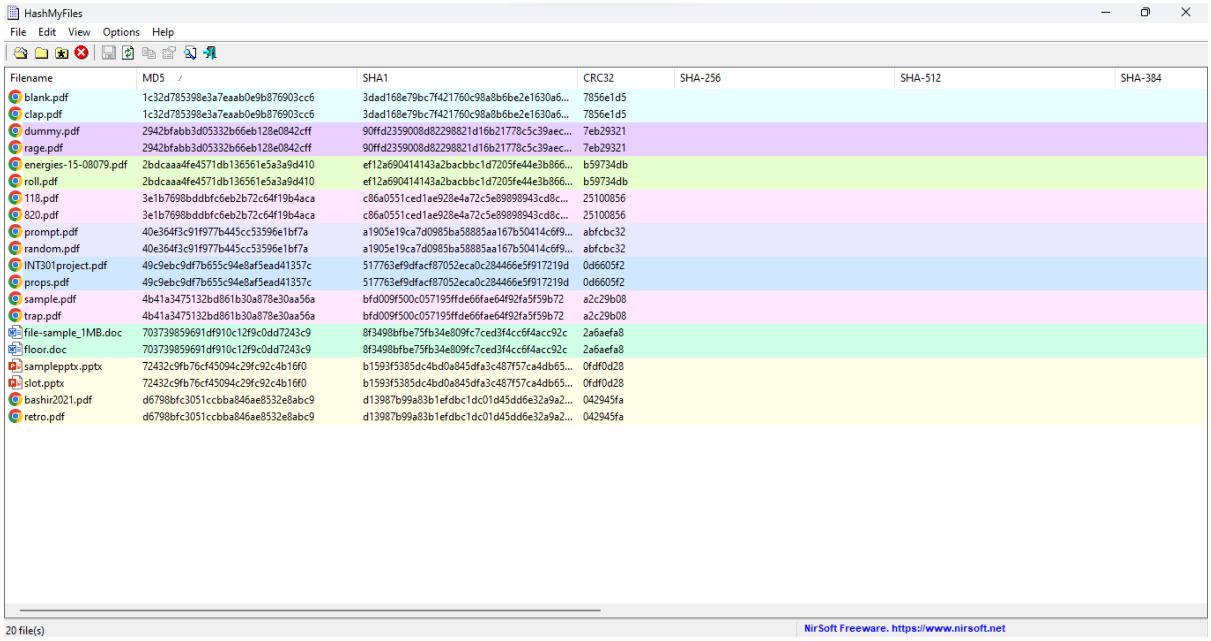
The files selected for comparison are available for download from a trusted source or the internet. The files selected for comparison have not been previously tampered with and are in their original state. The checksum calculator tool used for this project is reliable and accurate. The checksum values provided by the file creator or the source from which the file was downloaded are correct and have not been tampered with.

Overall, the assumptions and dependencies for this project are minimal and can be easily fulfilled by most users with basic computer skills. The success of the project depends on the accuracy of the checksum calculation process and the availability of the original checksum values provided by the file creator or the source from which the file was downloaded.

3. Analysis Report:

Install the HashMyFiles tool from the internet for the windows system which helps in calculating the checksum values for the files and helps us to make a comparison of files and check the integrity of the files. Firstly choose some files for which you want to calculate the checksum values and copy the chosen files and rename them to have the files with same data but different names and then add all the files in the HashMyFiles tool. After adding the files to the application it will automatically calculate the checksum values for the uploaded files.





Despite having the different names for the files uploaded in the HashMyFiles tool it shows same checksum values for the files with same data in them this helps us to identify the files with same data in them.