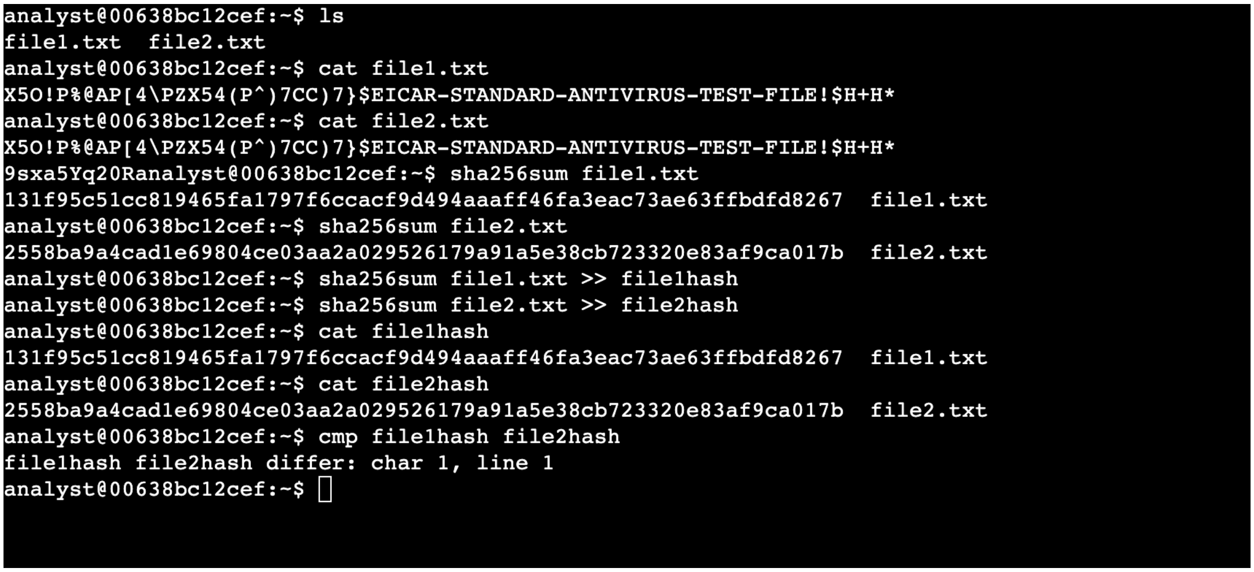
FILE INTEGRITY CHECK USING HASH FUNCTIONS

Project Description

The objective of this task was to verify the integrity of two text files and determine if they were identical or had been altered. I used Linux hashing commands and file comparison tools to generate and analyze SHA-256 checksums for each file.

Steps Performed



```
analyst@00638bc12cef:~$ ls
file1.txt  file2.txt
analyst@00638bc12cef:~$ cat file1.txt
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
analyst@00638bc12cef:~$ cat file2.txt
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
9sxa5Yq20Ranalyst@00638bc12cef:~$ sha256sum file1.txt
131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267  file1.txt
analyst@00638bc12cef:~$ sha256sum file2.txt
2558ba9a4cad1e69804ce03aa2a029526179a91a5e38cb723320e83af9ca017b  file2.txt
analyst@00638bc12cef:~$ sha256sum file1.txt >> file1hash
analyst@00638bc12cef:~$ sha256sum file2.txt >> file2hash
analyst@00638bc12cef:~$ cat file1hash
131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267  file1.txt
analyst@00638bc12cef:~$ cat file2hash
2558ba9a4cad1e69804ce03aa2a029526179a91a5e38cb723320e83af9ca017b  file2.txt
analyst@00638bc12cef:~$ cmp file1hash file2hash
file1hash file2hash differ: char 1, line 1
analyst@00638bc12cef:~$ 
```

I began by listing the directory contents, which contained two files: `file1.txt` and `file2.txt`. Inspecting their contents with the `cat` command showed that both contained the EICAR test string, although `file2.txt` included additional characters at the end.

To check integrity, I generated SHA-256 hashes for each file using the `sha256sum` command. The output produced two different hash values, confirming that the files were not identical. I then redirected each hash output into separate files, `file1hash` and `file2hash`, and displayed their contents to confirm the values.

Finally, I used the `cmp` command to compare the two hash files directly. The command reported that the files differed at the first character, which verified that `file1.txt` and `file2.txt` had different hash values and therefore were not exact duplicates.

Summary

In this project, I used Linux tools to check file integrity. By applying `sha256sum` and `cmp`, I demonstrated how hashing can detect even small differences between files. This approach is critical for verifying data integrity, detecting file tampering, and ensuring secure file management.