Day 14 – Hashing & File Integrity

What is Hashing?

- A **hash** is a fixed-length string generated from input data (like a file).
- Common algorithms: **SHA-256**, **SHA-1**, **MD5**
- Even a 1-character change in a file = completely different hash!
- Used in:
  - File integrity verification
  - Password storage
  - Digital forensics

Task: Generate Hashes in PowerShell (Windows)

Step 1: Open PowerShell

Right-click and "Run as administrator"

Step 2: Generate a hash for a test file

```
Get-FileHash -Algorithm SHA256 "C:\Path\To\Your\File.txt"
```

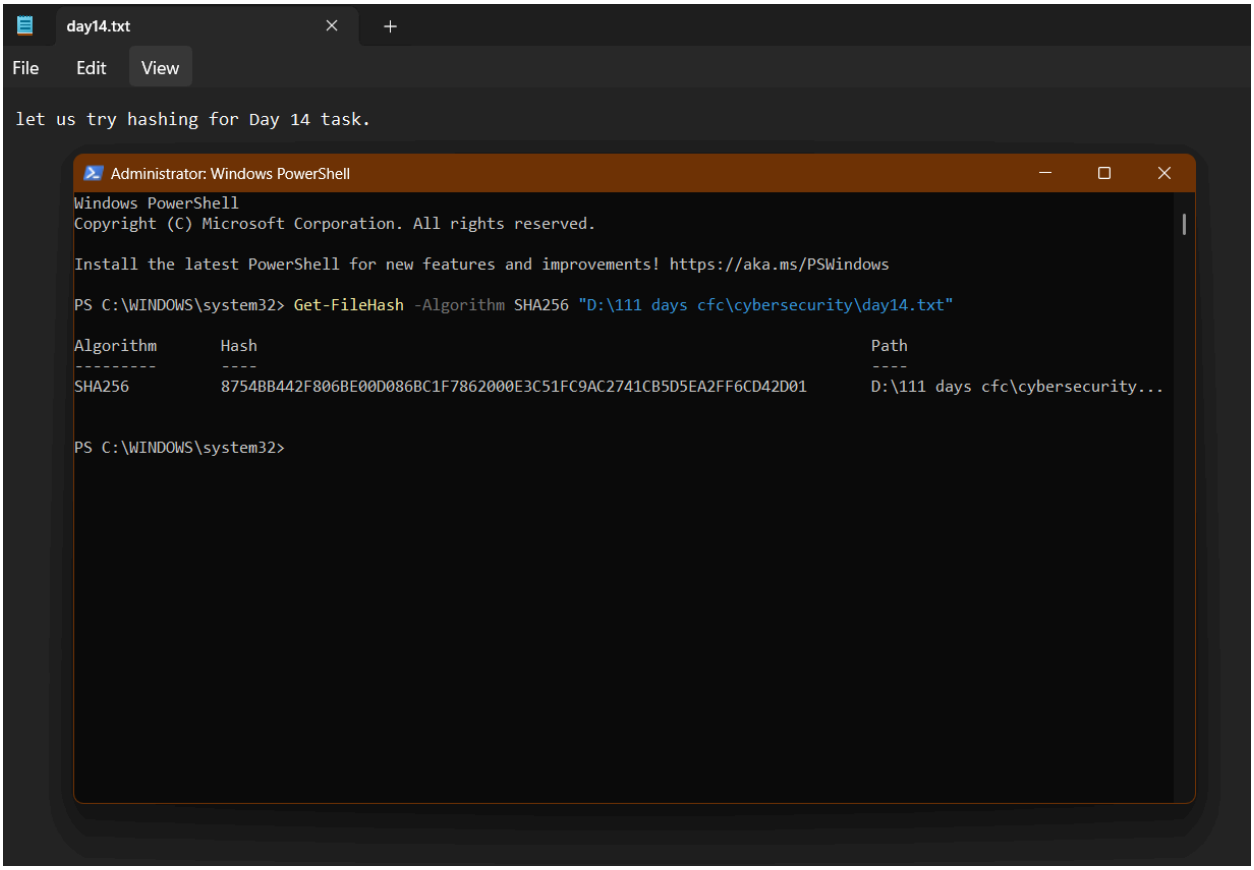
Tip: Create a test file using Notepad:

```
This is a test file for hashing.
```

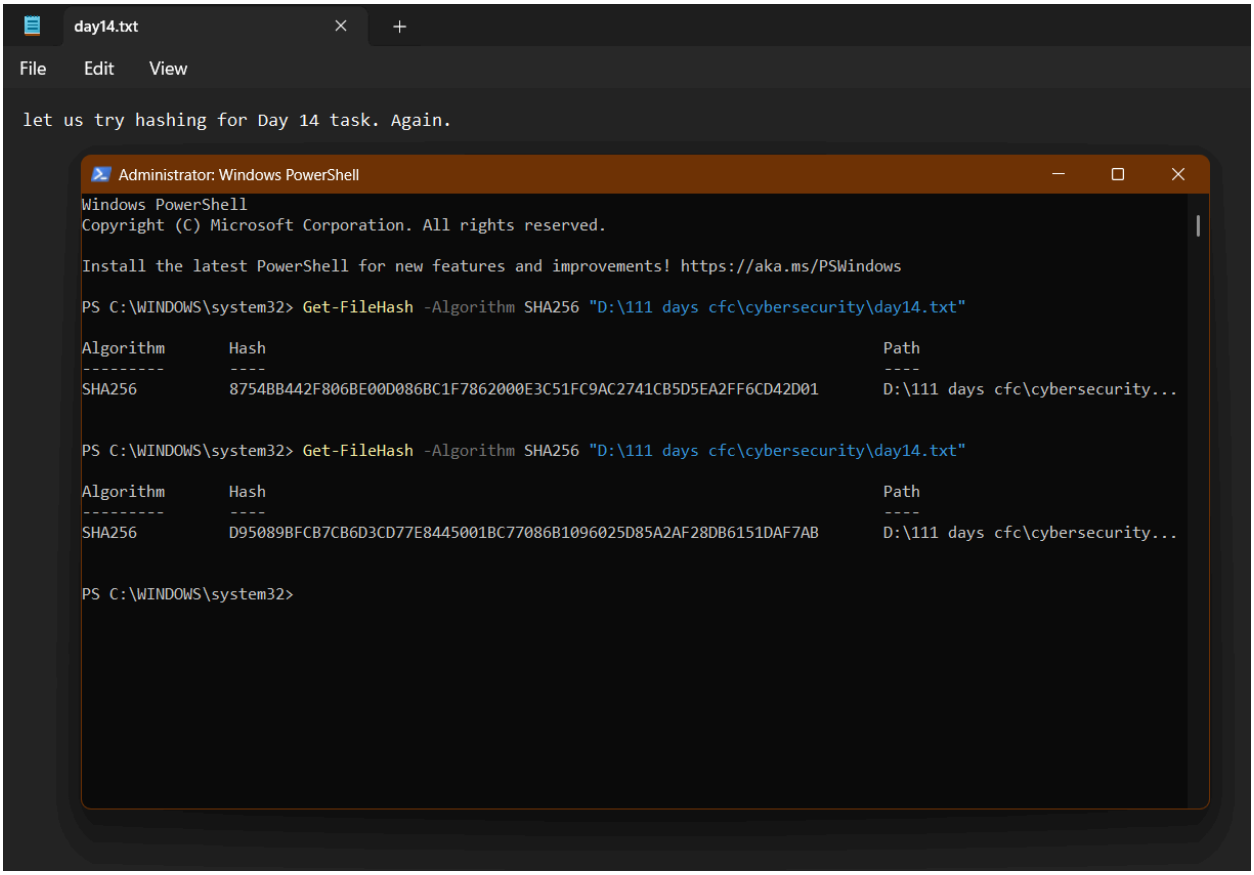
Step 3: Change the file content and re-run the hash

Notice how the hash **completely changes** with even a tiny modification.

Hash values before changing text in file



Hash values after changing text in file



What I Learned

- How to use `Get-FileHash` in PowerShell
- Why hashing is crucial for detecting file tampering
- Realized how **hashes act as digital fingerprints** for files