

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"
```

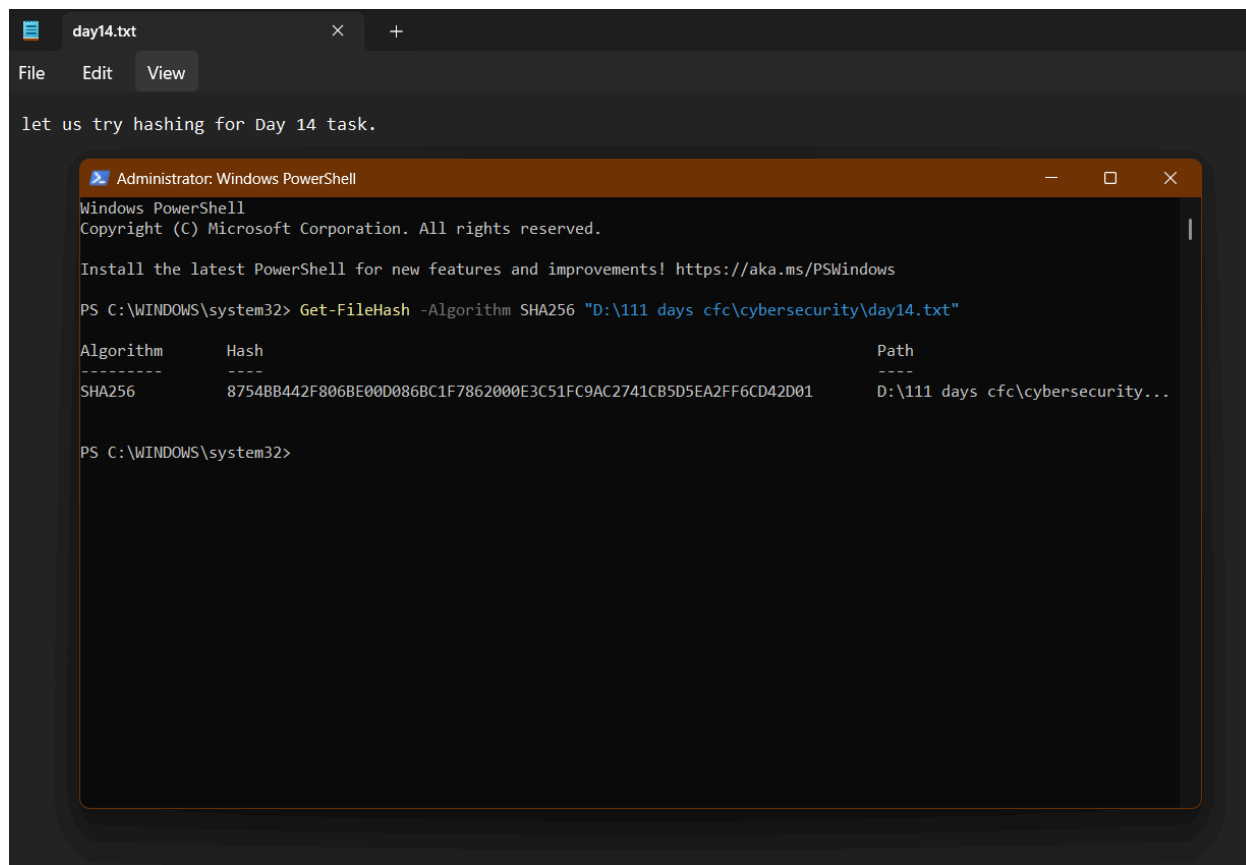
Tip: Create a test file using Notepad:

```
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



The screenshot shows a Windows file editor window titled 'day14.txt' with the text 'let us try hashing for Day 14 task.' Below it, an Administrator Windows PowerShell terminal window is open. The terminal displays the command to calculate the SHA256 hash of the file and the resulting output.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

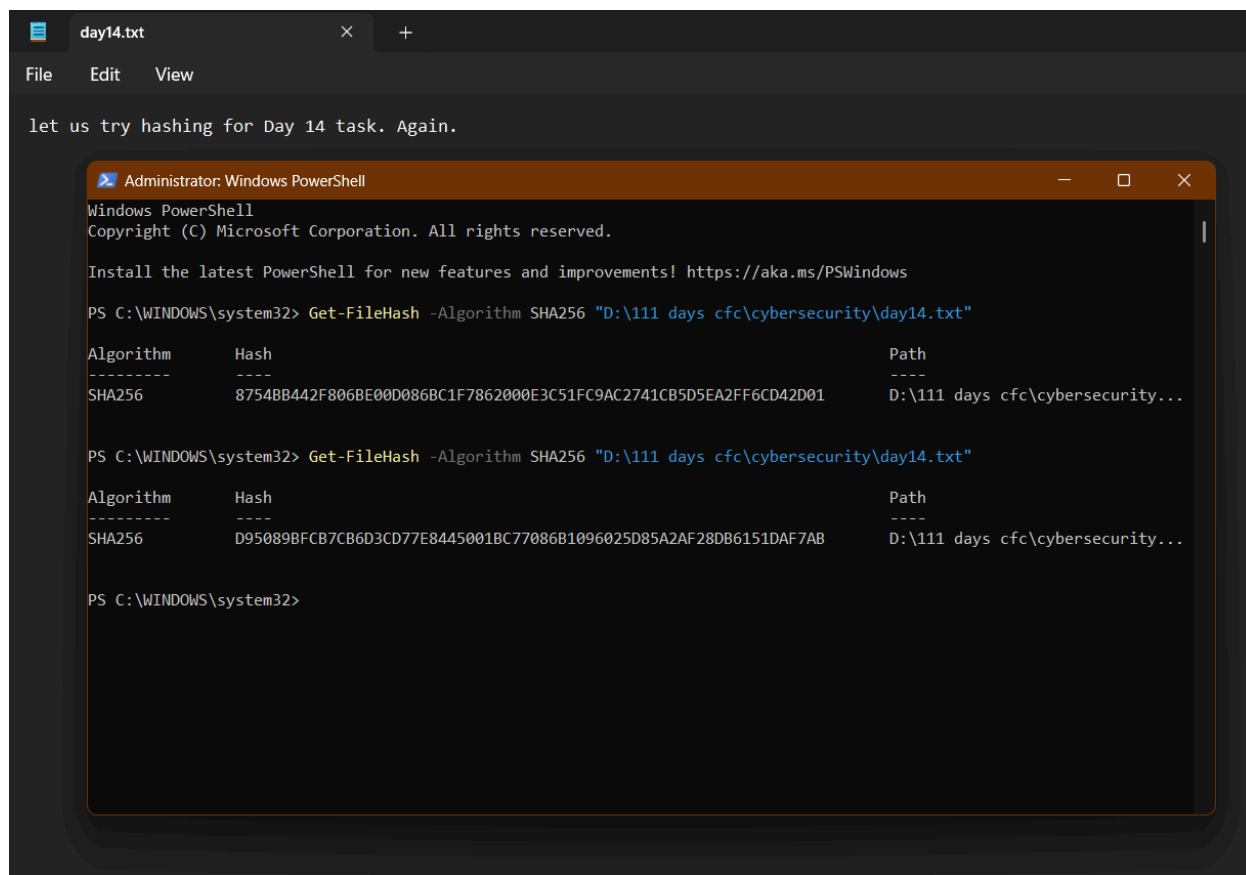
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-FileHash -Algorithm SHA256 "D:\111 days cfc\cybersecurity\day14.txt"

Algorithm      Hash
-----
SHA256         8754BB442F806BE00D086BC1F7862000E3C51FC9AC2741CB5D5EA2FF6CD42D01
Path
-----
D:\111 days cfc\cybersecurity\day14.txt

PS C:\WINDOWS\system32>
```

Hash values after changing text in file



The screenshot shows a text editor window titled 'day14.txt' with a menu bar (File, Edit, View) and a single line of text: 'let us try hashing for Day 14 task. Again.' Overlaid on this is an 'Administrator: Windows PowerShell' terminal window. The terminal displays the following content:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-FileHash -Algorithm SHA256 "D:\111 days cfc\cybersecurity\day14.txt"

Algorithm      Hash
-----
SHA256         8754BB442F806BE00D086BC1F7862000E3C51FC9AC2741CB5D5EA2FF6CD42D01
D:\111 days cfc\cybersecurity\day14.txt

PS C:\WINDOWS\system32> Get-FileHash -Algorithm SHA256 "D:\111 days cfc\cybersecurity\day14.txt"

Algorithm      Hash
-----
SHA256         D95089BFCB7CB6D3CD77E8445001BC77086B1096025D85A2AF28DB6151DAF7AB
D:\111 days cfc\cybersecurity\day14.txt

PS C:\WINDOWS\system32>
```

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