Lab 4

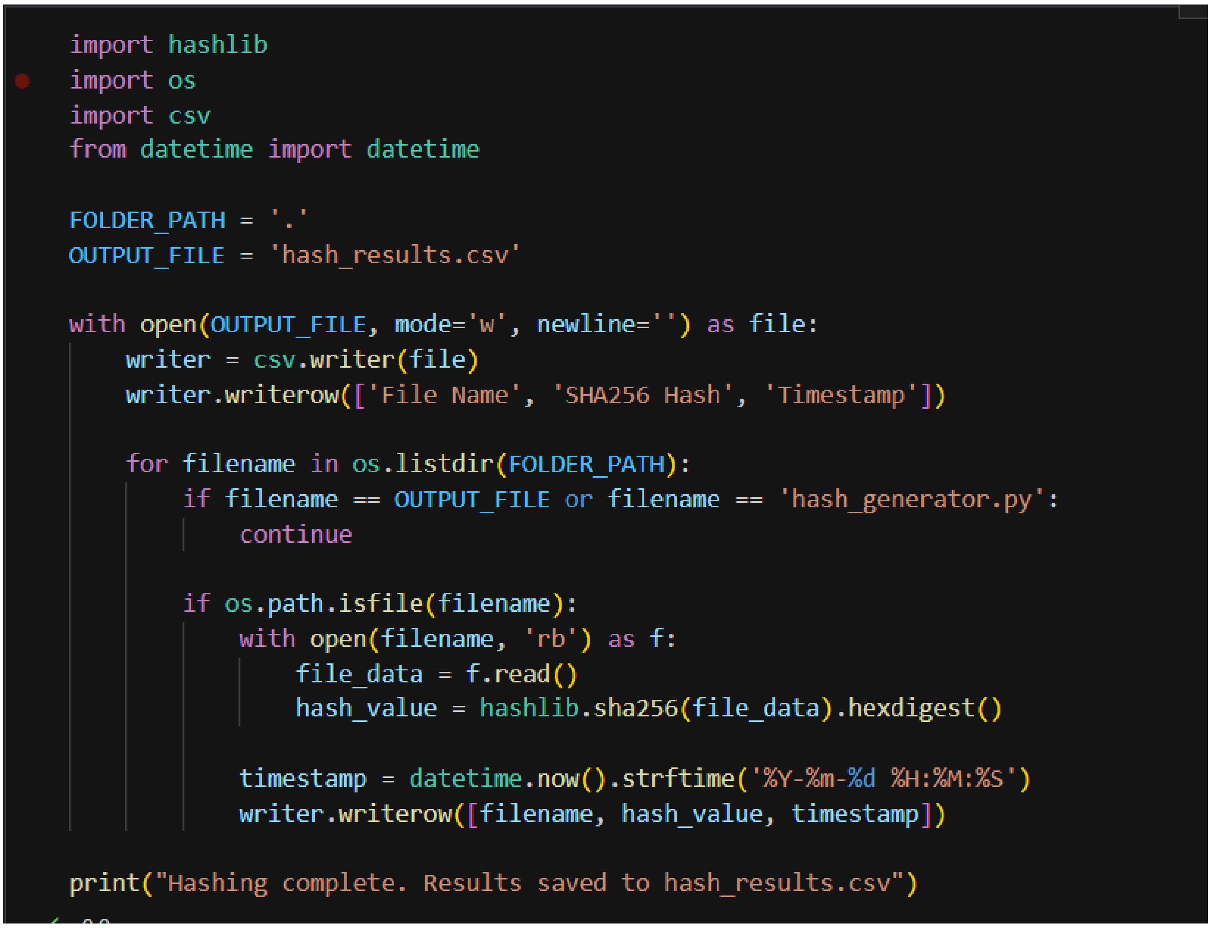
The purpose of this lab was to understand **how malware can be detected using file integrity checking and basic malware detection techniques**. Instead of working with real malware (which is dangerous), the lab **simulated how antivirus systems work** using safe Python scripts.

The main goals were to:

- Understand **how malware modifies system files**
- Learn how **hashing can detect file tampering**
- Detect **suspicious file changes**
- Scan files using **signature-based detection**
- Simulate **worm-style network spreading**
- Design **layered security countermeasures**

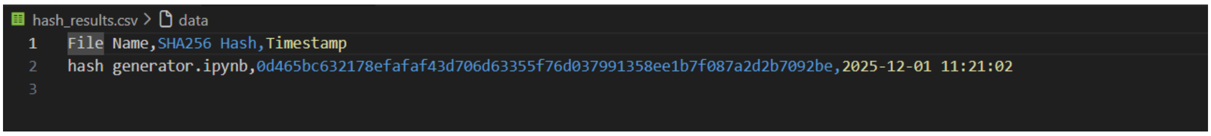
This reflects how real cybersecurity tools monitor systems for infection

Lab 4



```python
import hashlib
import os
import csv
from datetime import datetime

FOLDER_PATH = '.'
OUTPUT_FILE = 'hash_results.csv'

with open(OUTPUT_FILE, mode='w', newline='') as file:
    writer = csv.writer(file)
    writer.writerow(['File Name', 'SHA256 Hash', 'Timestamp'])

    for filename in os.listdir(FOLDER_PATH):
        if filename == OUTPUT_FILE or filename == 'hash_generator.py':
            continue

        if os.path.isfile(filename):
            with open(filename, 'rb') as f:
                file_data = f.read()
                hash_value = hashlib.sha256(file_data).hexdigest()

            timestamp = datetime.now().strftime('%Y-%m-%d %H:%M:%S')
            writer.writerow([filename, hash_value, timestamp])

print("Hashing complete. Results saved to hash_results.csv")
```

Hashing script - generating the hash and writing onto a csv



```
File Name,SHA256 Hash,Timestamp
hash generator.ipynb,0d465bc632178efafaf43d706d63355f76d037991358ee1b7f087a2d2b7092be,2025-12-01 11:21:02
```

CSV results for the hash