File Hash Verification using VirusTotal API

This project demonstrates how to verify the integrity and safety of a file using Python and the VirusTotal public API. A file's SHA-256 hash is computed and checked for known threats.

Methodology

1. **Hash Calculation**:
   - Used certutil to compute the SHA-256 hash of textfile.txt:

     Text

API: 090e9320092486fc3dab48b85ee61feeb111FFf6de15d54F6d1535a88998cc526

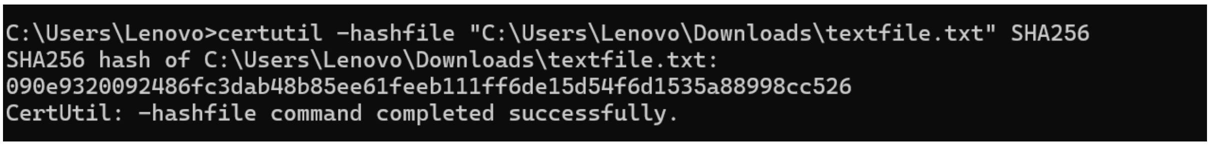
2. **Python Script**:
   - Developed a script to query VirusTotal's API with the file hash.
   - Libraries: requests (installed via pip install requests).
   - API Key used

Findings & Conclusions

The script successfully detects known files by querying VirusTotal's database. This process is useful for verifying file integrity or pre-checking suspicious files before use.

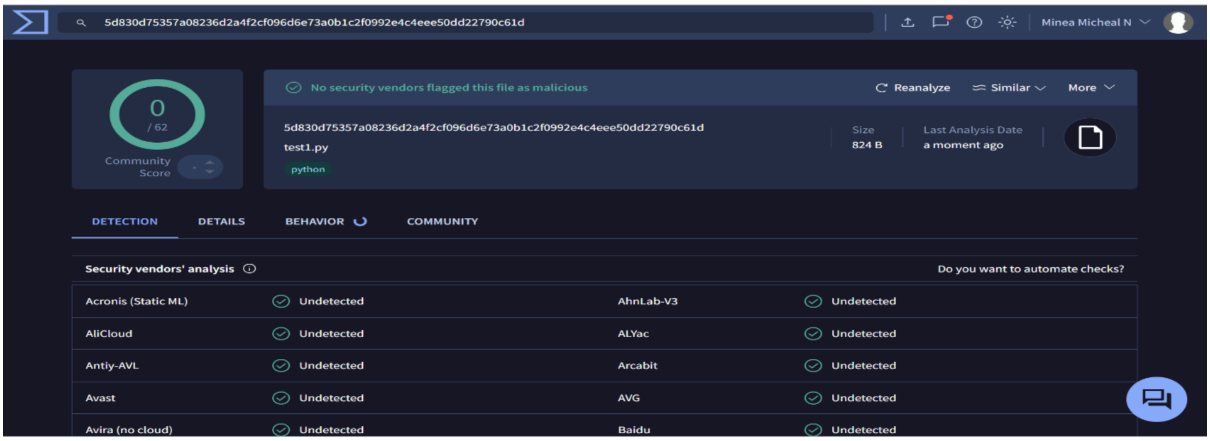
Screenshots

1. Hash Calculation:



```
C:\Users\Lenovo>certutil -hashfile "C:\Users\Lenovo\Downloads\textfile.txt" SHA256
SHA256 hash of C:\Users\Lenovo\Downloads\textfile.txt:
090e9320092486fc3dab48b85ee61feeb111ff6de15d54f6d1535a88998cc526
CertUtil: -hashfile command completed successfully.
```

2. VirusTotal:



5d830d75357a08236d2a4f2cf096d6e73a0b1c2f0992e4c4eee50dd22790c61d
Minea Micheal N
0
/ 62
Community Score
Reanalyze
Similar
More
DETECTION
DETAILS
BEHAVIOR
COMMUNITY
Do you want to automate checks?

No security vendors flagged this file as malicious

5d830d75357a08236d2a4f2cf096d6e73a0b1c2f0992e4c4eee50dd22790c61d
test1.py
python

Size 824 B

Last Analysis Date a moment ago

Security vendors' analysis

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected

CODE:

```
import requests

API_KEY = 'YOUR_API_KEY'  # Replace with actual key

file_hash = 'FILE_HASH'   # Replace with target hash

url = f'https://www.virustotal.com/api/v3/files/{file_hash}'

headers = {"x-apikey": API_KEY}

response = requests.get(url, headers=headers)

if response.status_code == 200:

   data = response.json()

   stats = data['data']['attributes']['last_analysis_stats']

   print(f"Malicious: {stats['malicious']}, Harmless: {stats['harmless']}")

else:

   print(f"Error: {response.status_code}")
```

SUBMITTED BY:

MINEA MICHEAL N