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:

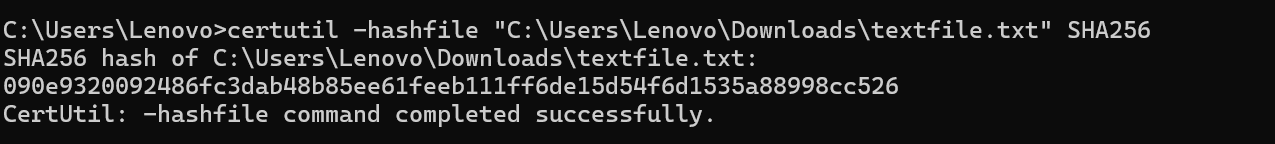
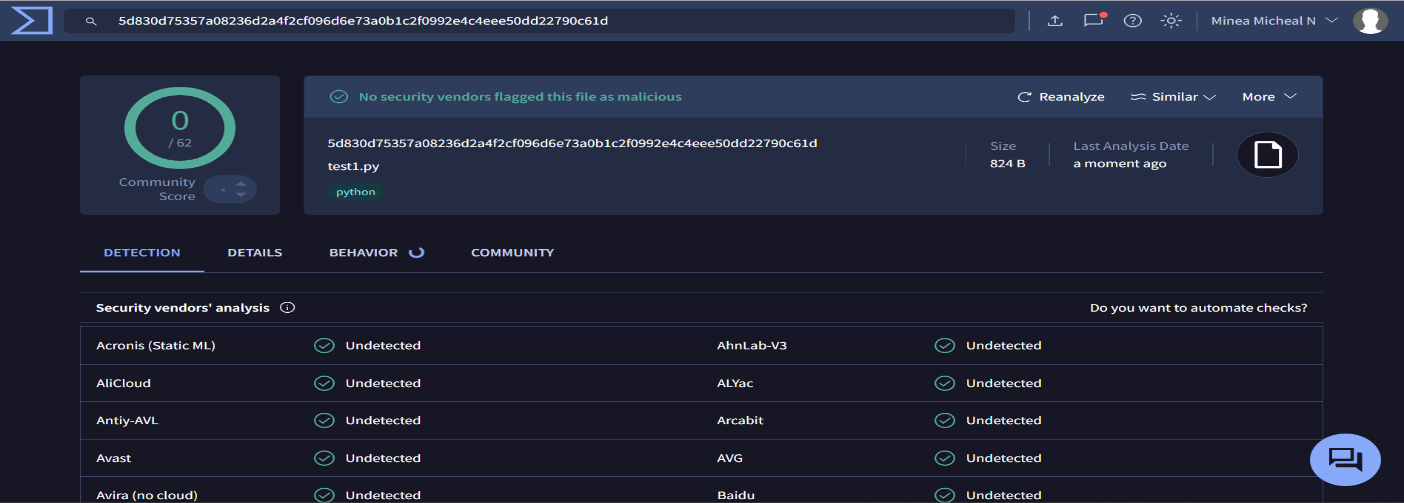
text

1. **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:  
   
2. VirusTotal:

**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**

**BTIT (2461017)**