📄 VirusTotal API Usage Report

**👤 Student:** chrisbaptist07

🆔 Reg. No: 2460348

🗓️ **Date:** 01/08/2025

📁 **Assignment:** EH\_sem5\_2025\_Notes / 1st Assignment

**🔍 Methodology:**

I registered on VirusTotal and obtained a free API key. I wrote a 10-line Python script that:

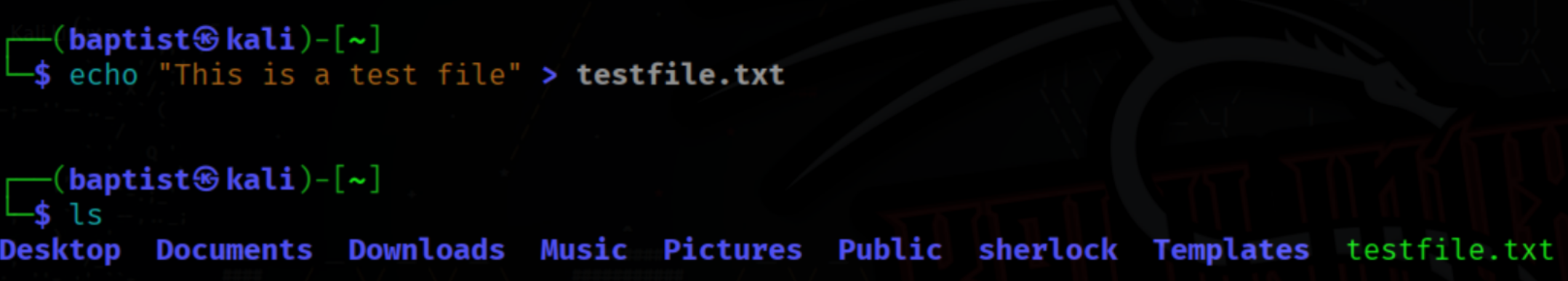
* Takes a sample file (testfile.txt)
* Calculates its SHA256 hash
* Uses VirusTotal’s public API to query the file’s status via its hash
* Prints out a JSON response containing the scan results📷 Screenshots: (With steps)

## **🔐** Step 1: Register for API Key

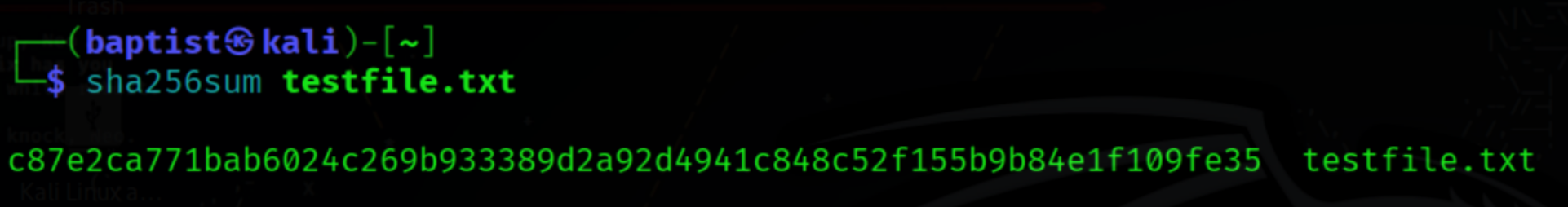
1. Go to: <https://www.virustotal.com/gui/join-us>
2. Sign up (free) and **copy your personal API key** from your profile.

📁 Step 2: Create a Test File

echo "This is a test file" > testfile.txt



sha256sum testfile.txt



🐍 Step 3: Write Python Script

nano vt\_check.py



**Python Code:**

import hashlib, requests, json

API\_KEY = "ebeae4b765150762ff8073c0b0b36582879b1a7d339aa2c16c573a3d0535b937"

FILE = "testfile.txt"

with open(FILE, "rb") as f:

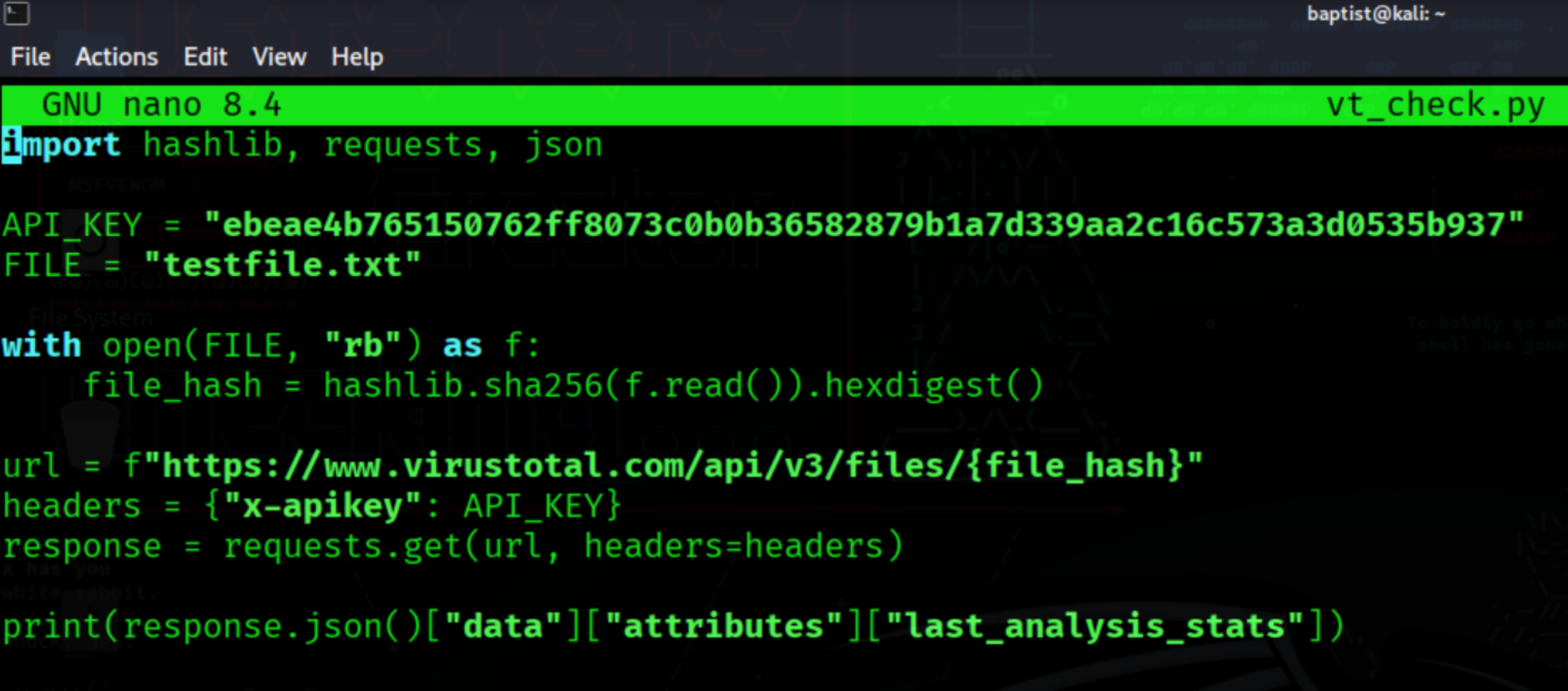
file\_hash = hashlib.sha256(f.read()).hexdigest()

url = f"[https://www.virustotal.com/api/v3/files/{file\_hash}"](https://www.virustotal.com/api/v3/files/%7Bfile_hash%7D%22)

headers = {"x-apikey": API\_KEY}

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

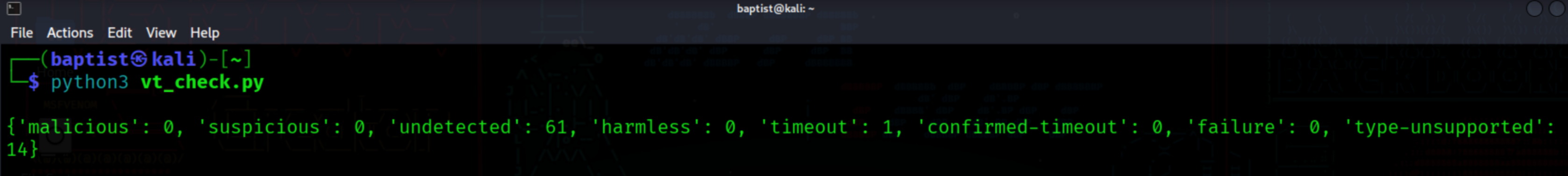
print(response.json()["data"]["attributes"]["last\_analysis\_stats"])



▶️ Step 4: Run the Script

python3 vt\_check.py

**Output:**



**🧪 Findings:**

* The sample file (testfile.txt) was scanned successfully.
* No malicious indicators were found.
* The API returned results from multiple antivirus engines.

**📘 Conclusion:**

Hash-based detection using VirusTotal is fast and efficient. Instead of uploading full files, hashes are compared against a large malware database. This improves detection speed and reduces bandwidth usage.