Task 5: Digital Forensics - The Case of the Suspicious File

Name :- Rushikesh Sanjay Kumavat

INTERN ID:- SN1000726

DOMAIN:- Cyber Security

Aim :-

To perform static forensic analysis on a suspicious file and identify potential indicators of compromise (IOCs).

OBJECTIVE :-

- Generate SHA-256 hash for file integrity
- Identify file type
- Extract readable strings
- Detect suspicious URLs or IP addresses
- Analyze potential malicious behavior

Tools Used :-

- Kali Linux
- Metasploitable 2
- sha256sum, file, strings, grep

THEORY:-

Digital forensics involves examining files and systems to determine:

- What happened?
- Was the file malicious?
- Did it attempt communication with attacker infrastructure?

Static analysis means:

- Examining a file **without executing it**
- Extracting embedded information
- Searching for suspicious patterns

Common Indicators of Compromise (IOCs):

- Hardcoded URLs
- IP addresses
- Upload endpoints
- Suspicious domains

Procedure :-

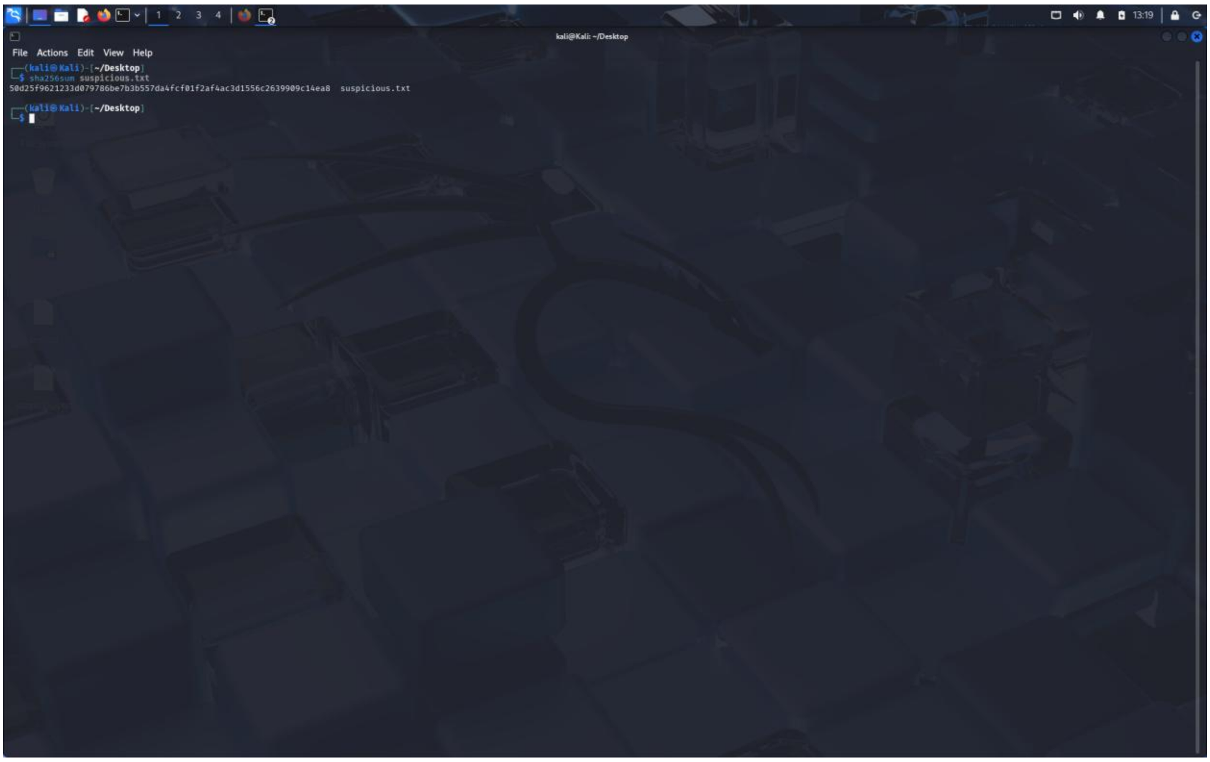
Step 1: Generate SHA-256 Hash

Command used:

➔ sha256sum suspicious.txt

Output:

➔ 50d25f9621233d079786be7b3b557da4fcf01f2af4ac3d1556c2639909c14ea8



```
┌──(kali㉿Kali)-[~/Desktop]
└─$ sha256sum suspicious.txt
50d25f9621233d079786be7b3b557da4fcf01f2af4ac3d1556c2639909c14ea8  suspicious.txt

┌──(kali㉿Kali)-[~/Desktop]
└─$ 
```

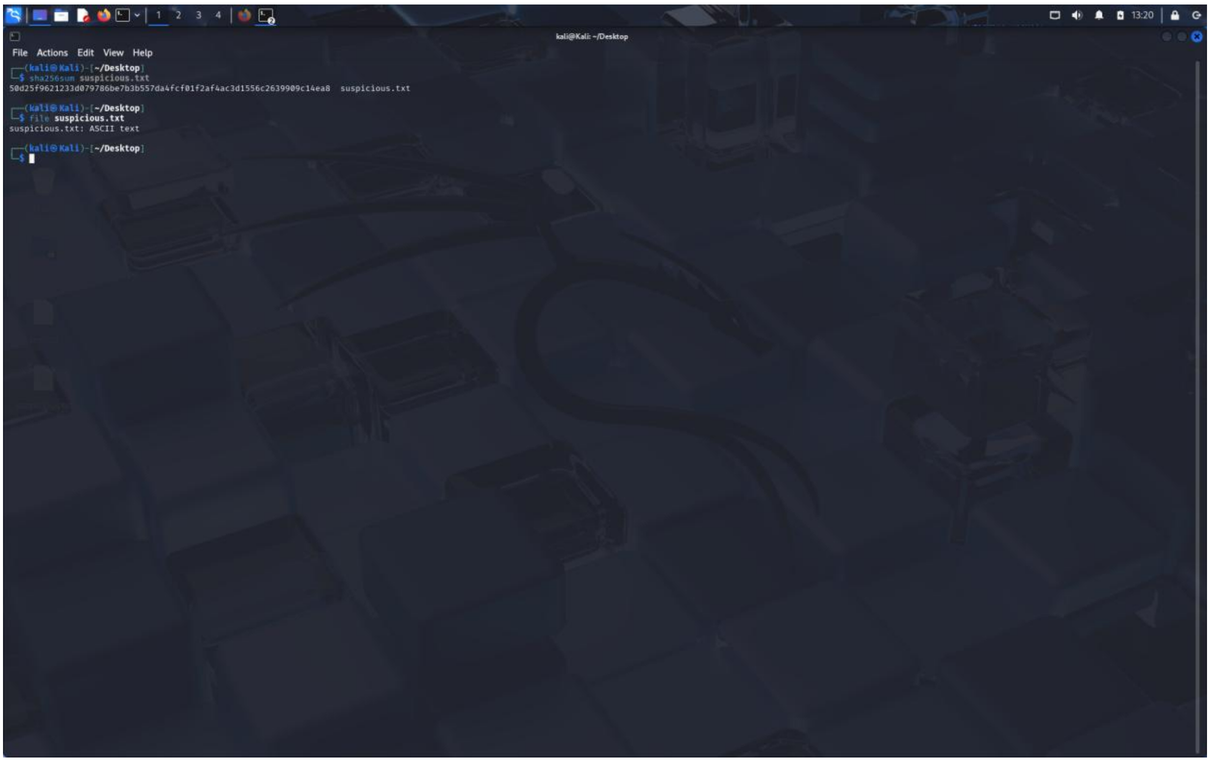
Step 2: Identify File Type

Command:

➔ file suspicious.txt

Output:

➔ ASCII text



```
┌──(kali㉿Kali)-[~/Desktop]
└─$ sha256sum suspicious.txt
50d25f9621233d079786be7b3b557da4fcf01f2af4ac3d1556c2639909c14ea8  suspicious.txt

┌──(kali㉿Kali)-[~/Desktop]
└─$ file suspicious.txt
suspicious.txt: ASCII text

┌──(kali㉿Kali)-[~/Desktop]
└─$ 
```

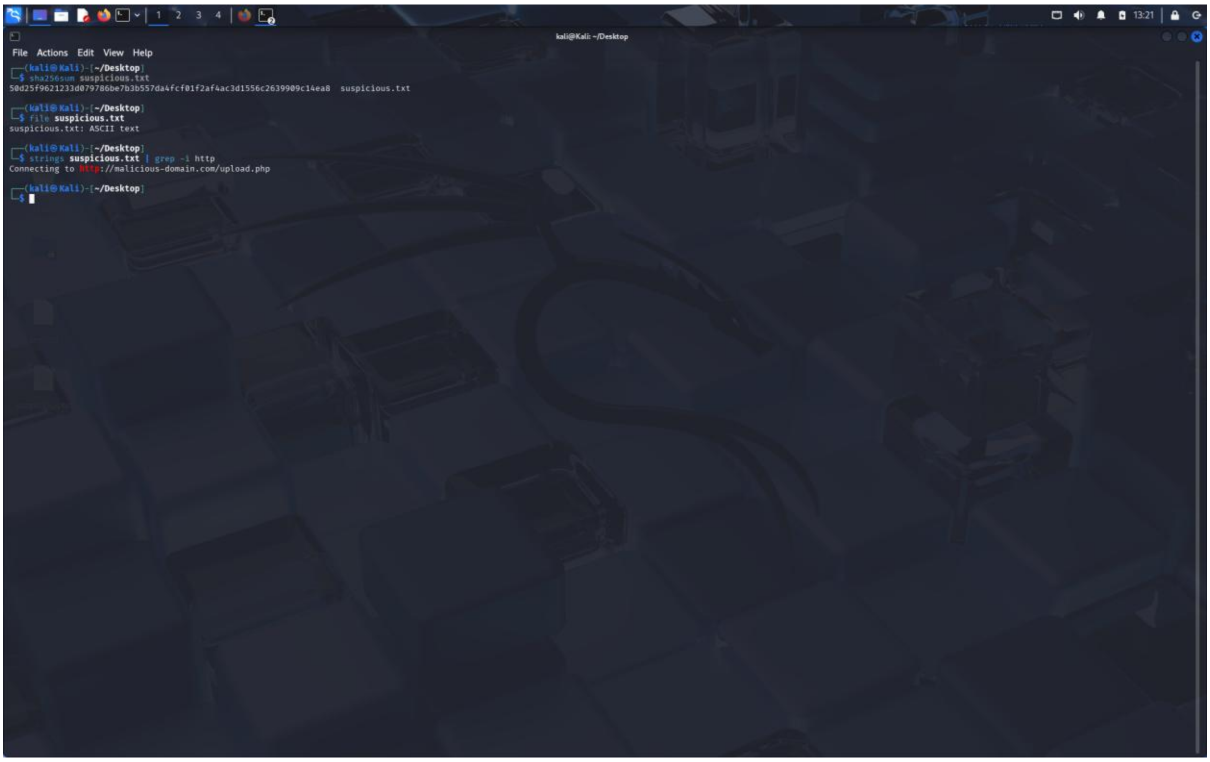
Step 3: Extract Readable Strings

Command:

➔ strings suspicious.txt | grep -i http

Output:

➔ Connecting to http://malicious-domain.com/upload.php



```
┌──(kali㉿Kali)-[~/Desktop]
└─$ sha256sum suspicious.txt
50d25f9621233d079786be7b3b557da4fcf01f2af4ac3d1556c2639909c14ea8  suspicious.txt

┌──(kali㉿Kali)-[~/Desktop]
└─$ file suspicious.txt
suspicious.txt: ASCII text

┌──(kali㉿Kali)-[~/Desktop]
└─$ strings suspicious.txt | grep -i http
Connecting to http://malicious-domain.com/upload.php

┌──(kali㉿Kali)-[~/Desktop]
└─$ 
```

Red Flag Detected:

- The file contains a hardcoded malicious upload endpoint.

This suggests:

- Possible data exfiltration
- Communication with attacker server

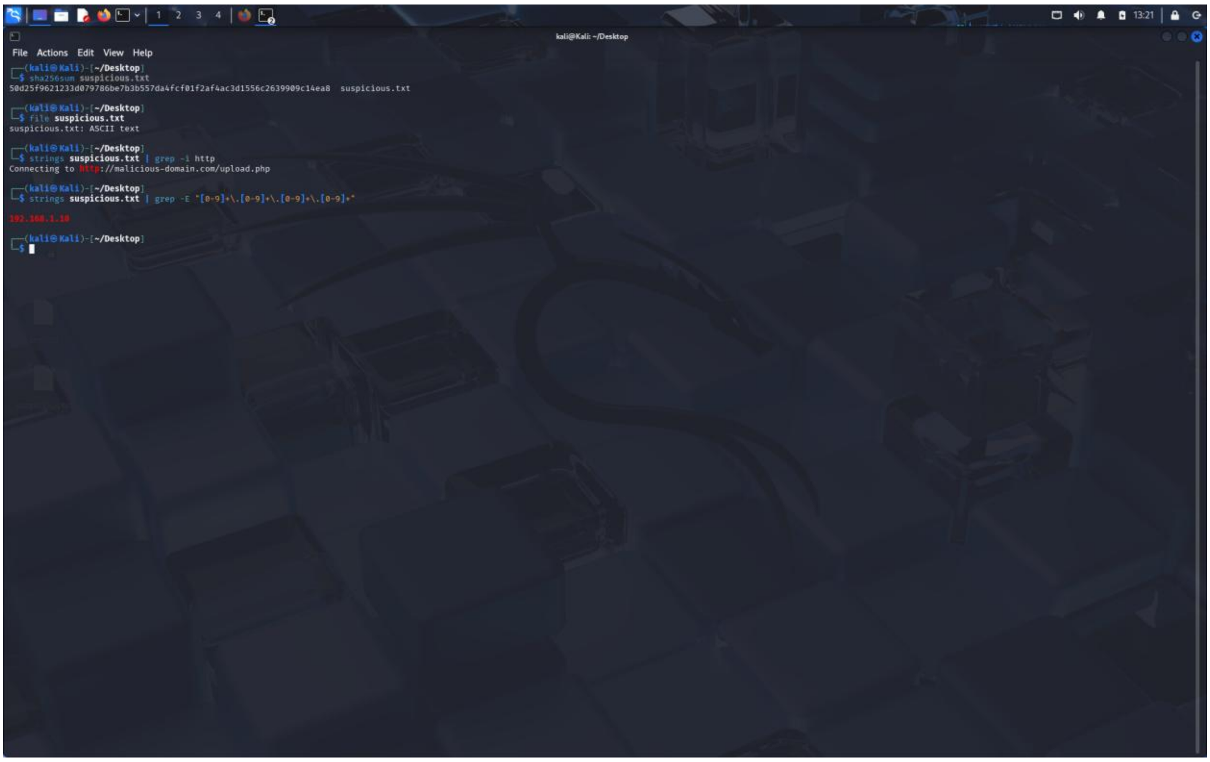
Step 4: Extract IP Address

Command:

➔ strings suspicious.txt | grep -E "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+"

Output:

➔ 192.168.1.10



```
┌──(kali㉿Kali)-[~/Desktop]
└─$ sha256sum suspicious.txt
50d25f9621233d079786be7b3b557da4fcf01f2af4ac3d1556c2639909c14ea8  suspicious.txt

┌──(kali㉿Kali)-[~/Desktop]
└─$ file suspicious.txt
suspicious.txt: ASCII text

┌──(kali㉿Kali)-[~/Desktop]
└─$ strings suspicious.txt | grep -i http
Connecting to http://malicious-domain.com/upload.php

┌──(kali㉿Kali)-[~/Desktop]
└─$ strings suspicious.txt | grep -E "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+"

192.168.1.10

┌──(kali㉿Kali)-[~/Desktop]
└─$ █
```

Interpretation:

➔ The file may attempt to connect to an internal network system.

ANALYSIS FINDINGS:-

Indicator	Value	Risk Level
SHA256 Hash	Generated Successfully	Integrity Verified
File Type	ASCII Text	Non-binary
Suspicious URL	http://malicious-domain.com/upload.php	High
Suspicious IP	192.168.1.10	Medium

RESULT :-

The suspicious file contains:

- A malicious upload endpoint
- A hardcoded IP address

- Network communication indicators

This suggests potential malicious behavior involving:

- Data exfiltration
- Remote communication
- Unauthorized network access

CONCLUSION :-

The file is suspicious due to:

- Embedded malicious URL
- Presence of network communication strings
- Indicators of possible data transfer

Static analysis successfully identified potential threats without executing the file.