Incident Response and Forensics Analysis

Name: J.Srikanth

Date: October 17, 2025

1. Introduction

This project simulates a cybersecurity incident and demonstrates the steps taken for response, forensic analysis, and post-incident review using the Autopsy digital forensics tool.

2. Simulated Incident

A fake security incident was simulated by creating a folder named 'FakeIncident' containing suspicious files such as 'malware.exe', 'invoice.pdf.exe', 'passwords.txt', and 'system_log.txt'. These files were designed to simulate a phishing attack and data leak scenario.

3. Incident Response

Upon discovering the suspicious files, the system was assumed to be isolated to prevent further damage. The incident was documented, and forensic analysis was initiated to investigate the nature and origin of the suspicious files.

4. Forensic Analysis

Autopsy was used to examine the files within the FakeIncident folder. The analysis revealed the presence of executable files mimicking documents and a text file with fake credentials. Metadata and file contents were examined for signs of malicious behavior.

Key Findings:

- - 'malware.exe': Fake executable posing as malware.
- - 'invoice.pdf.exe': Disguised executable likely to trick users.
- - 'passwords.txt': Contained fake credentials.
- - 'system_log.txt': Log mentioning suspicious activity and fake user 'hacker123'.

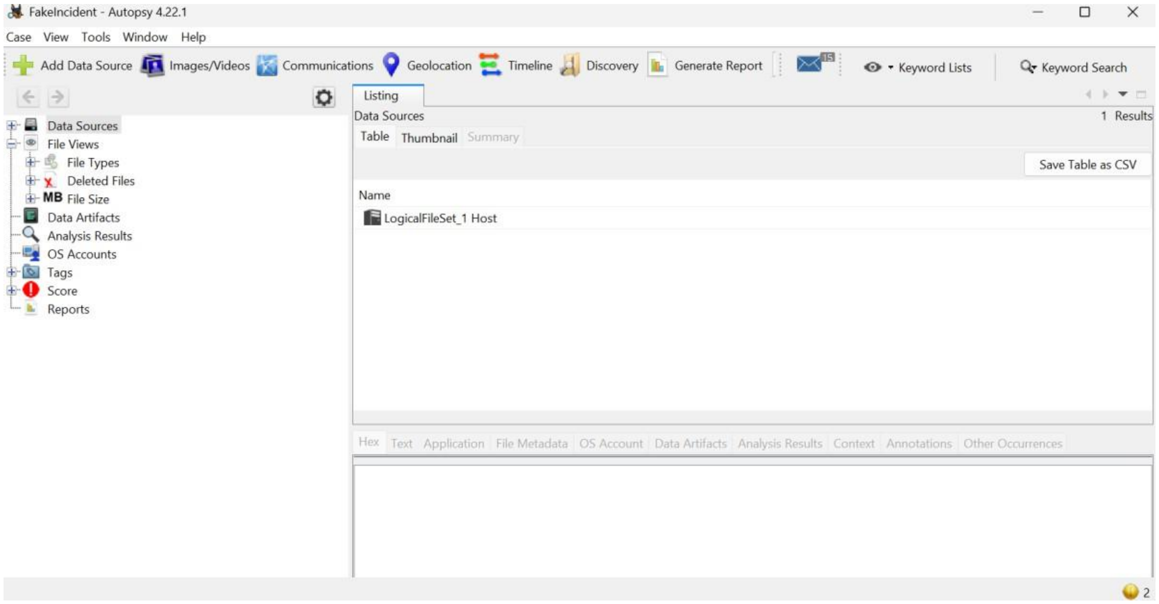
5. Post-Incident Analysis

The response to the simulated incident was effective in identifying and containing the threat. However, improvements could include real-time alerts, better user training to recognize suspicious files, and automated incident reporting tools.

6. Conclusion

This mini project provided hands-on experience in simulating, responding to, and analyzing a cybersecurity incident. Tools like Autopsy are crucial in digital forensics for identifying and understanding threats.

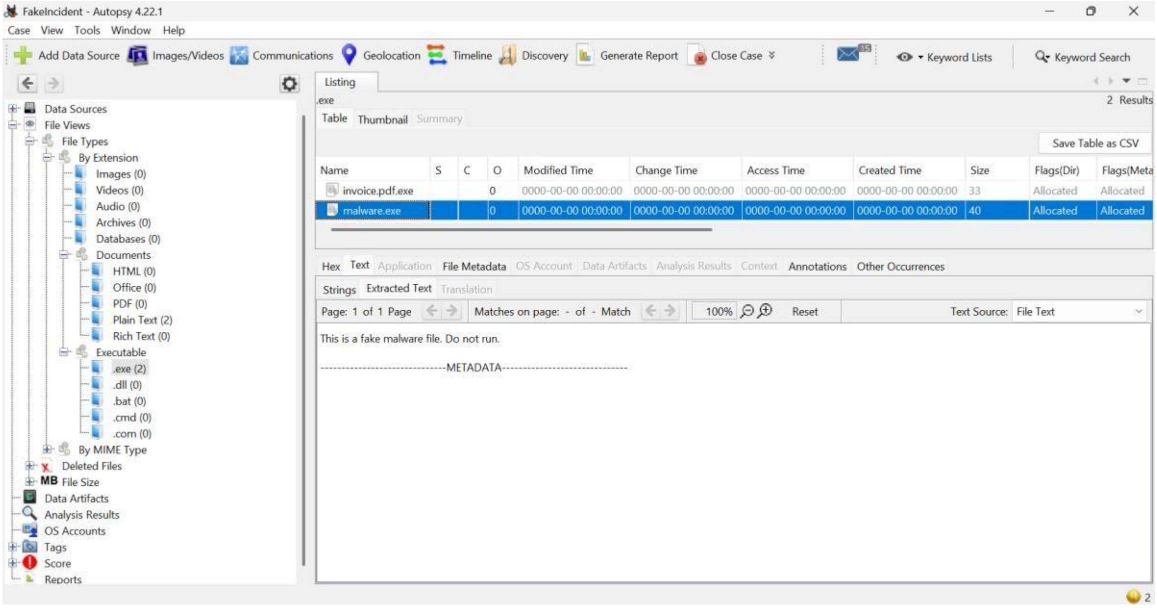
7. Appendix (Screenshots)



Data Sources

1 Results

Name
LogicalFileSet_1 Host

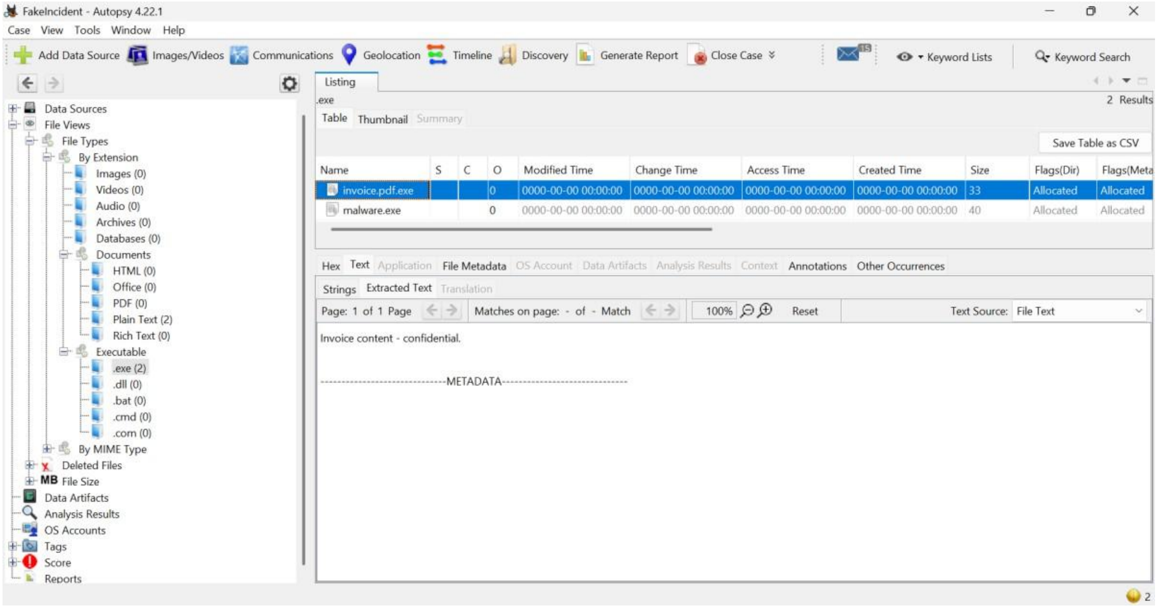


.exe

2 Results

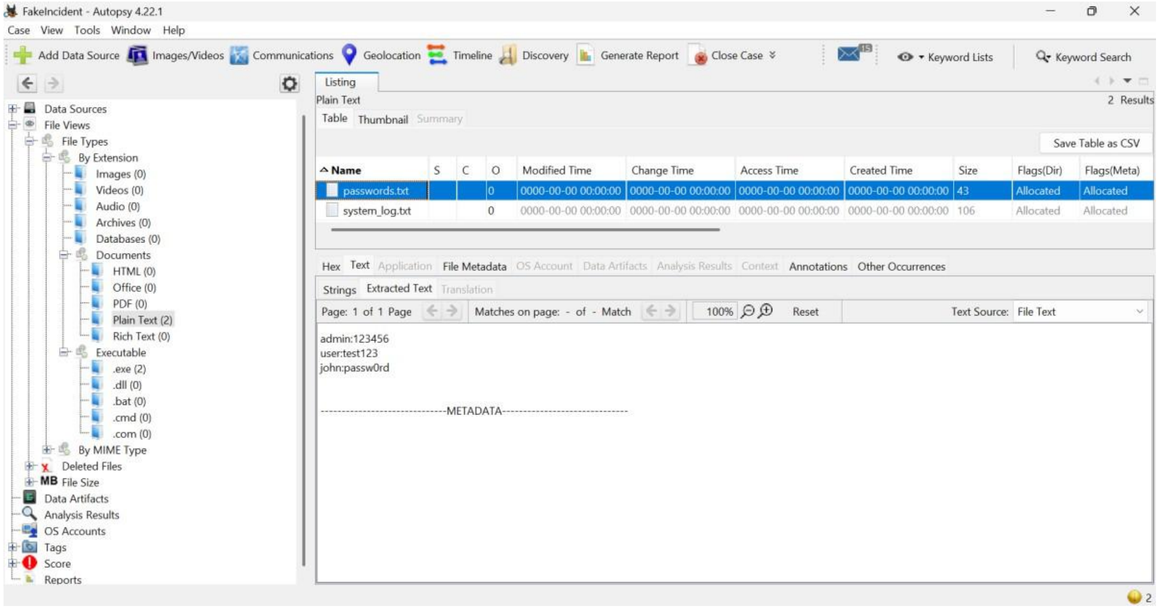
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta
invoice.pdf.exe			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	33	Allocated	Allocated
malware.exe			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	40	Allocated	Allocated

```
This is a fake malware file. Do not run.

-----------------------------METADATA-----------------------------
```



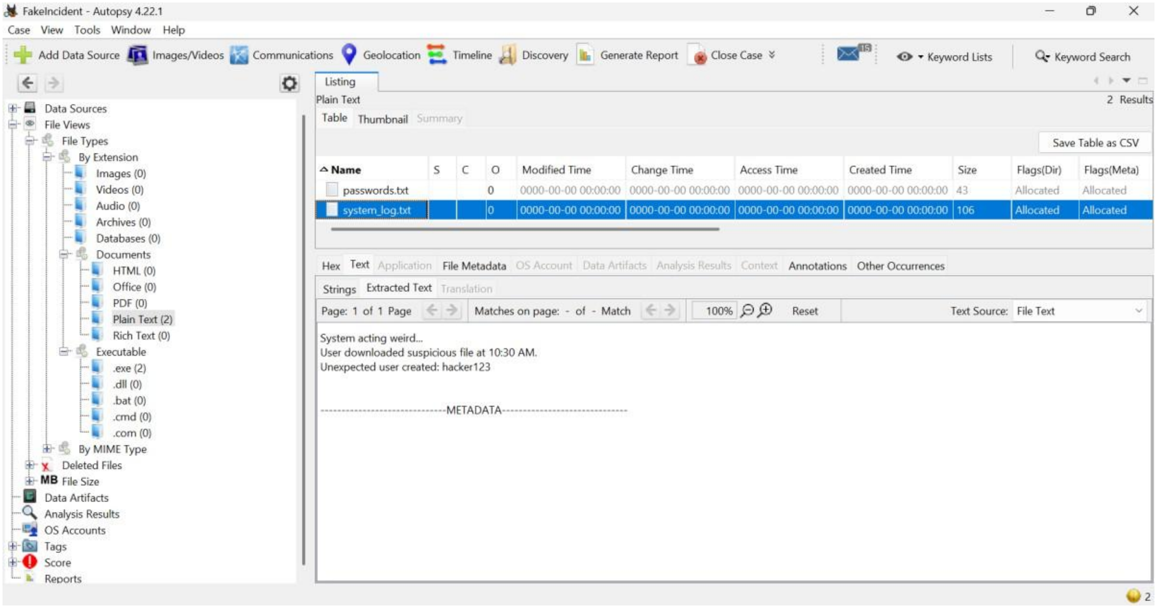
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta
invoice.pdf.exe			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	33	Allocated	Allocated
malware.exe			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	40	Allocated	Allocated

```
Invoice content - confidential.


-----------------------------METADATA------------------------------
```



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
passwords.txt			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	43	Allocated	Allocated
system_log.txt			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	106	Allocated	Allocated

```
admin:123456
user:test123
john:passw0rd


-----------------------------METADATA------------------------------
```



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
passwords.txt			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	43	Allocated	Allocated
system_log.txt			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	106	Allocated	Allocated

```
System acting weird...
User downloaded suspicious file at 10:30 AM.
Unexpected user created: hacker123


-----------------------------METADATA-----------------------------
```