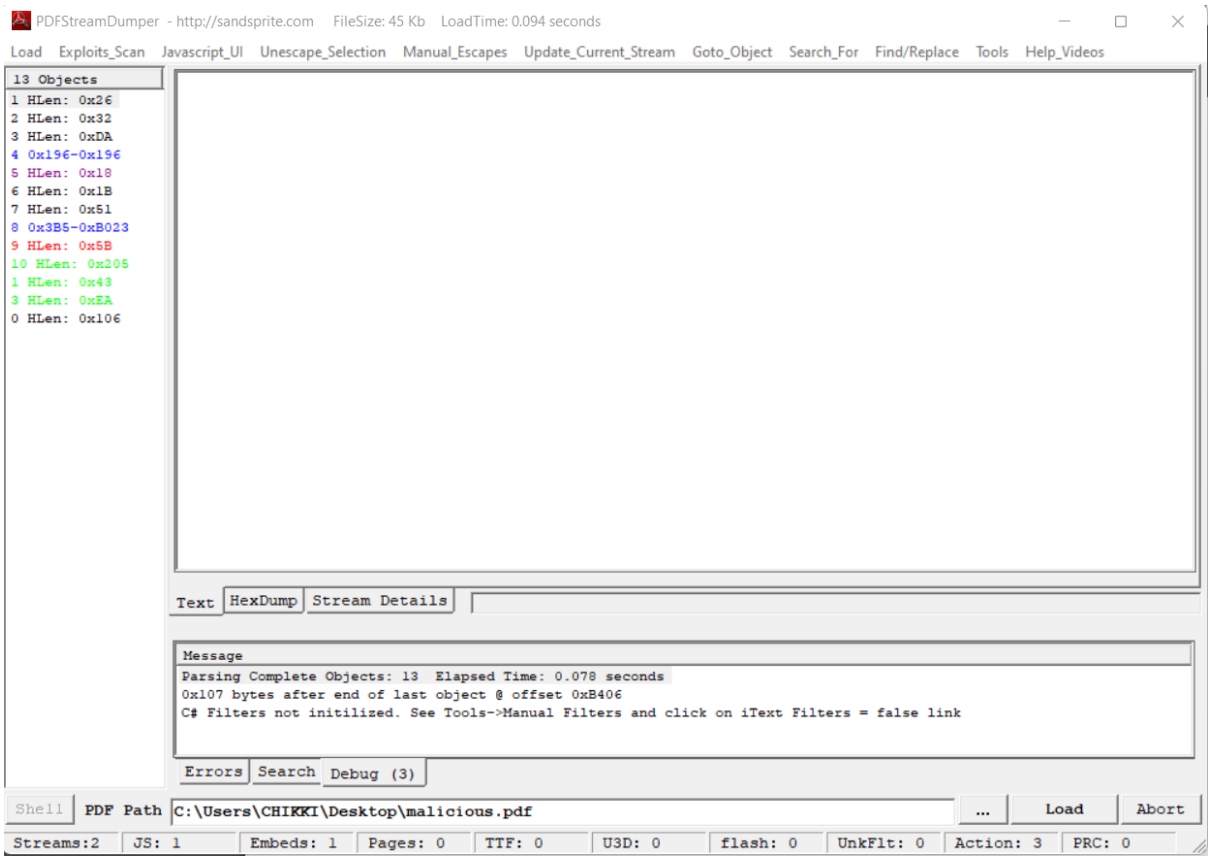
Malicious PDF File Analysis - No. 16

Stage 2: Your job is to investigate the content of a given malicious pdf file. Using the PDF analysing tools offered by the REMnux tool, spider monkey, sctest, or PDF Stream Dumper, address the following questions/activities.

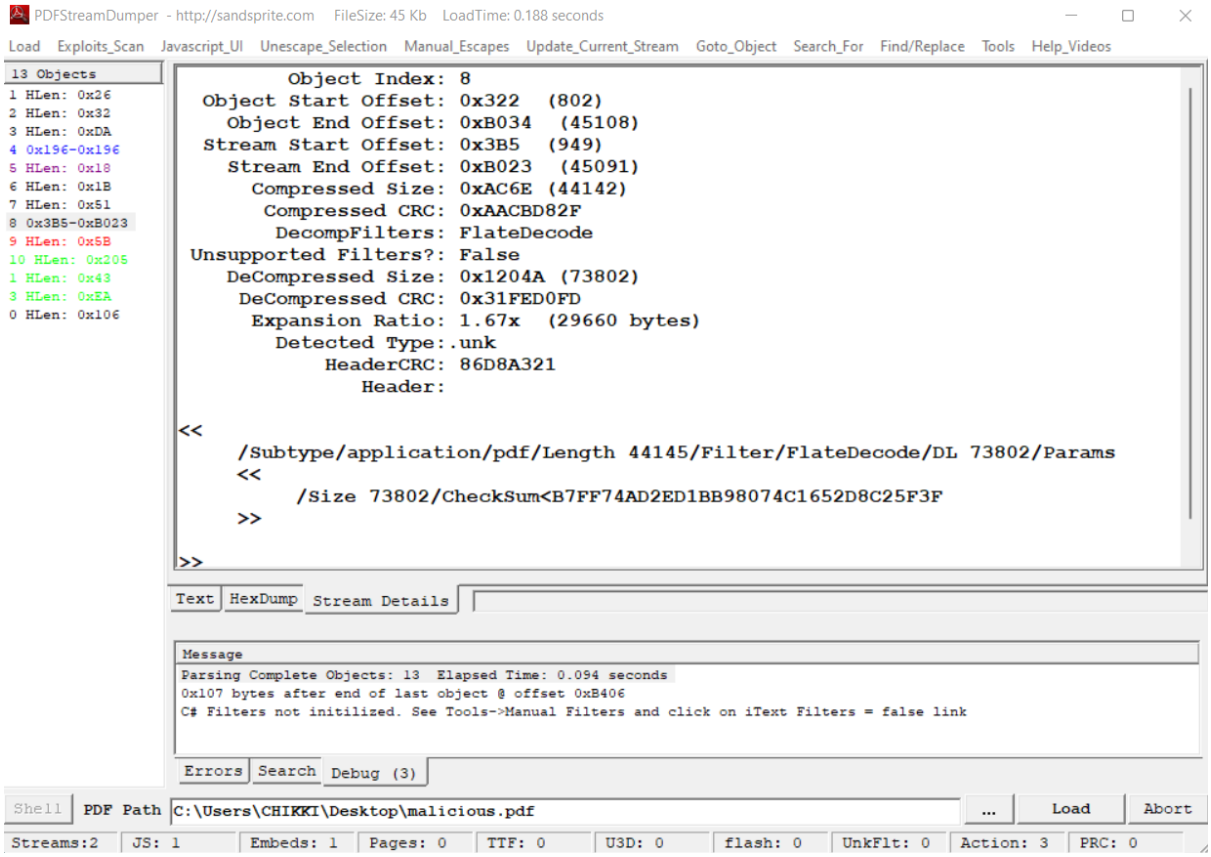
1-Report the number of objects in the file.

There are 13 objects in the given file.



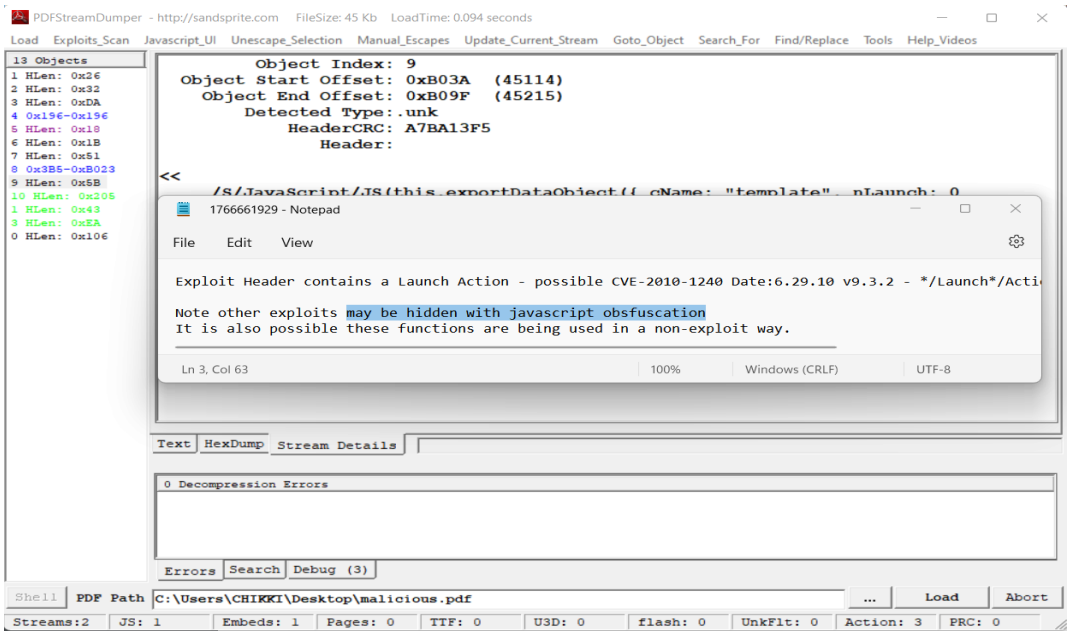
2-Determine whether the file is compressed or not.

Yes, the file is compressed.

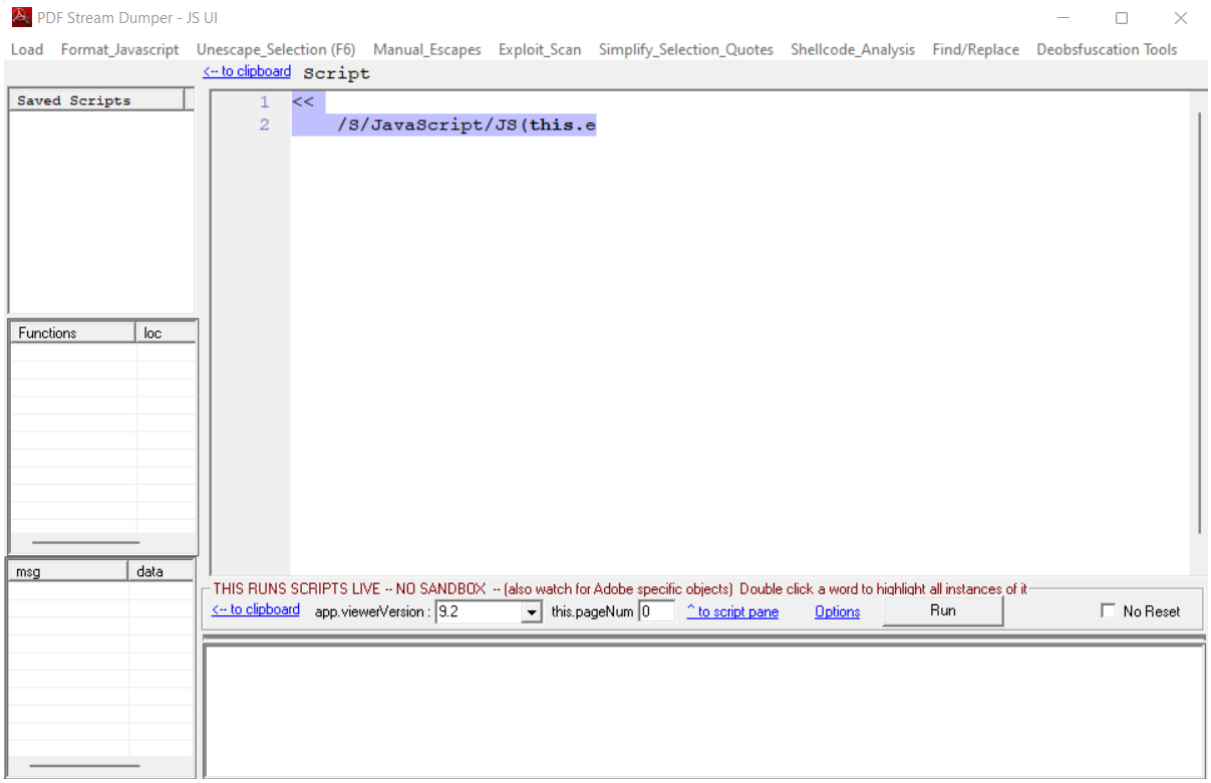


3. Determine whether the file is obfuscated or not.

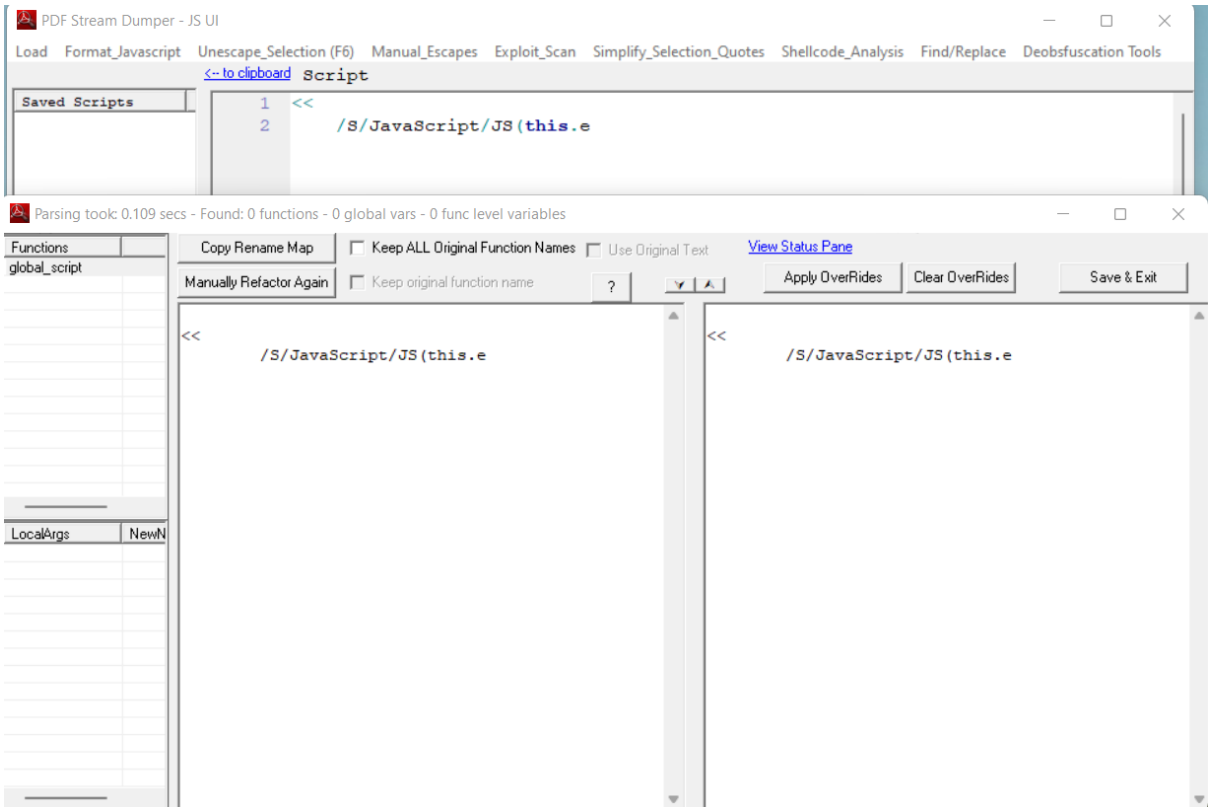
Yes, the file is obfuscated.



4. Find and Extract JavaScript.



5. De-obfuscate JavaScript.



6. Extract the shell code.

No shell code found.

7. Create a shell code executable

As there is no shell code found, unable to create shell code executable.

8. Analyse shell code and determine what is does or even execute it using sctest or spider monkey

Unable to analyse as there is no shell code.

9. What is the secret code?

No secret code found.