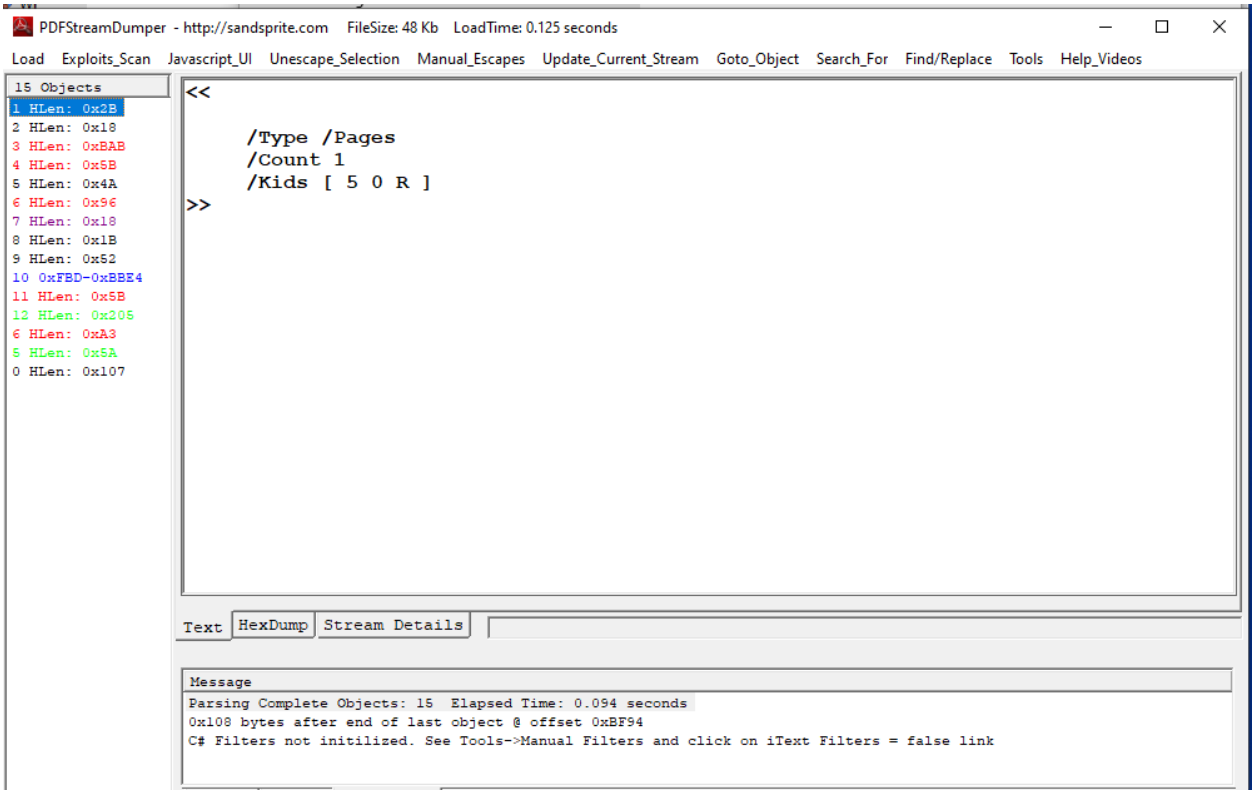
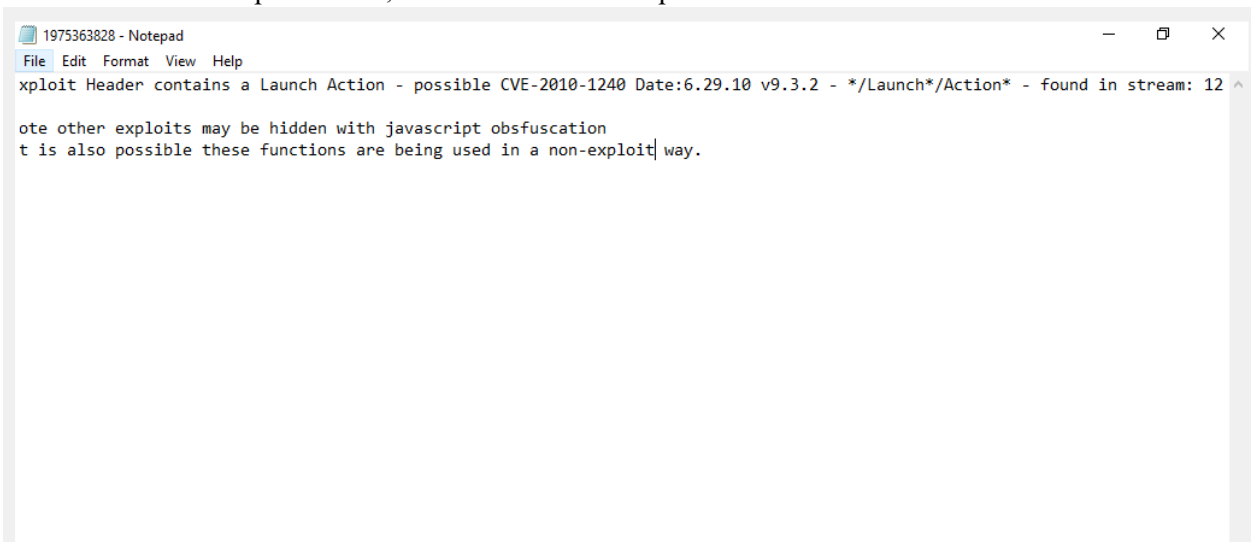
By using PDFStreamDumper on Windows 10. The outcomes of malware PDF are:

1. The PDF contains 15 objects.

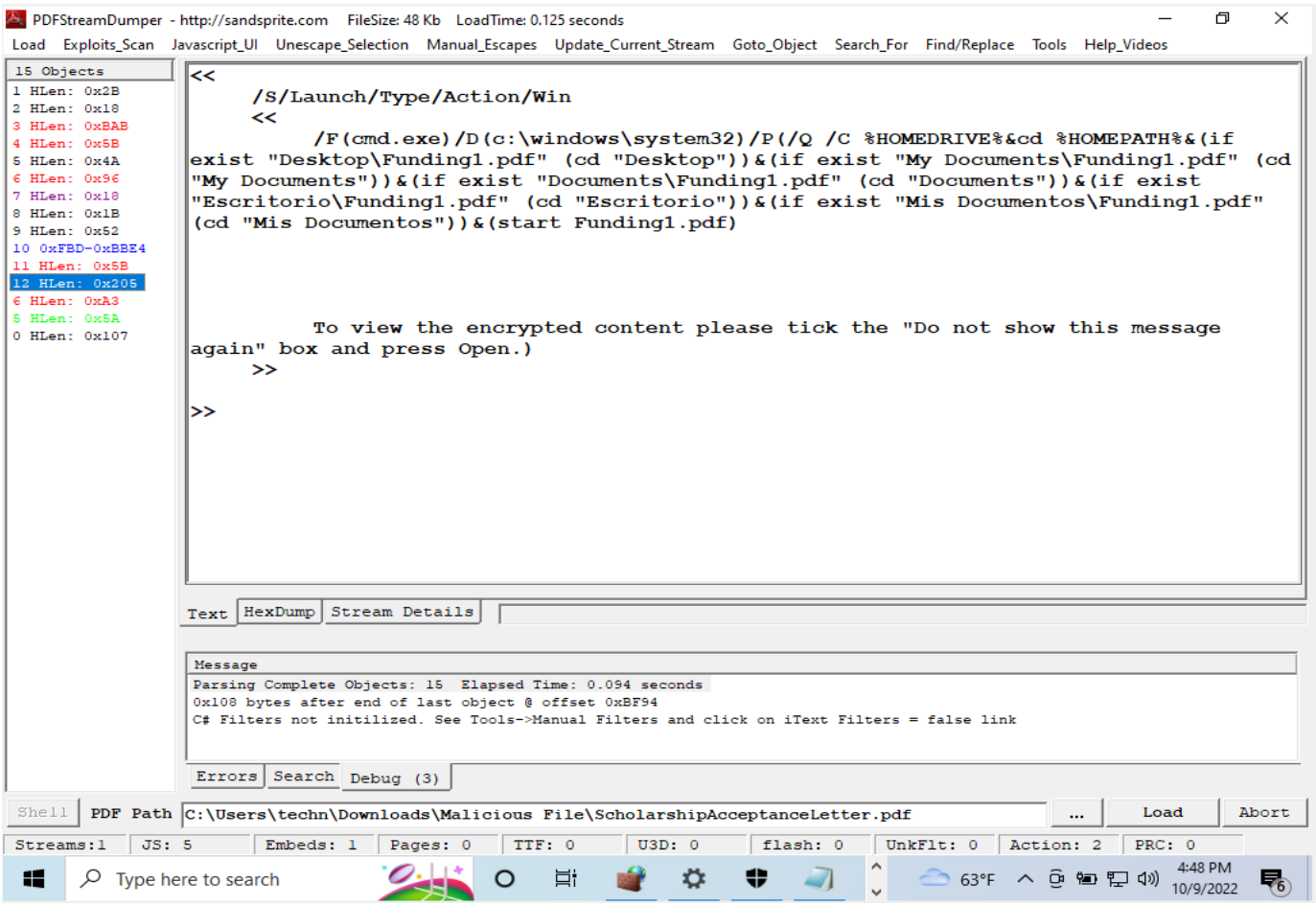


2. When clicked on “Exploit Scan”, we see that there is exploit hidden in stream 12.

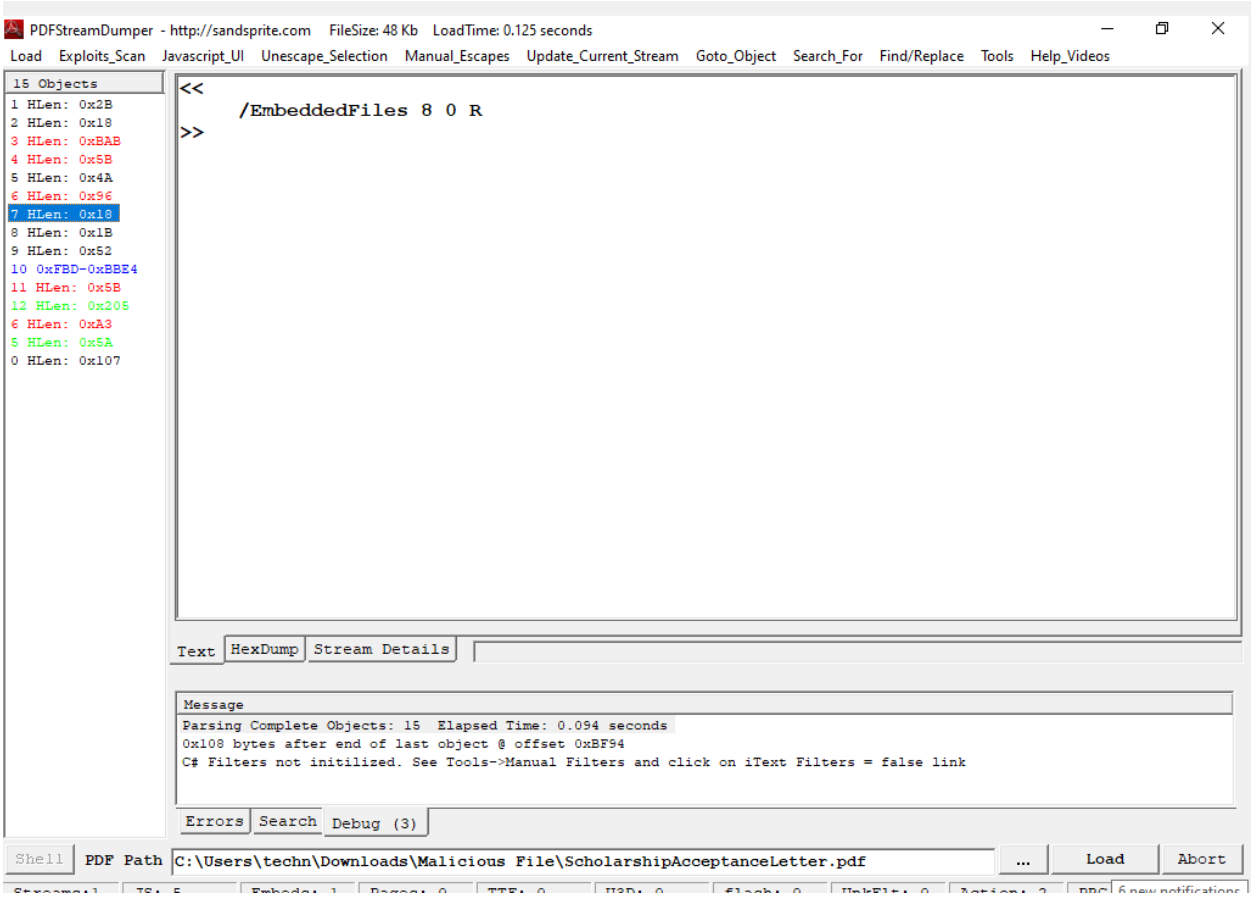


3. The javascript executes to open a CMD when the payload is ran and tries to redirect to another pdf named Funding1.pdf inside the object 12.

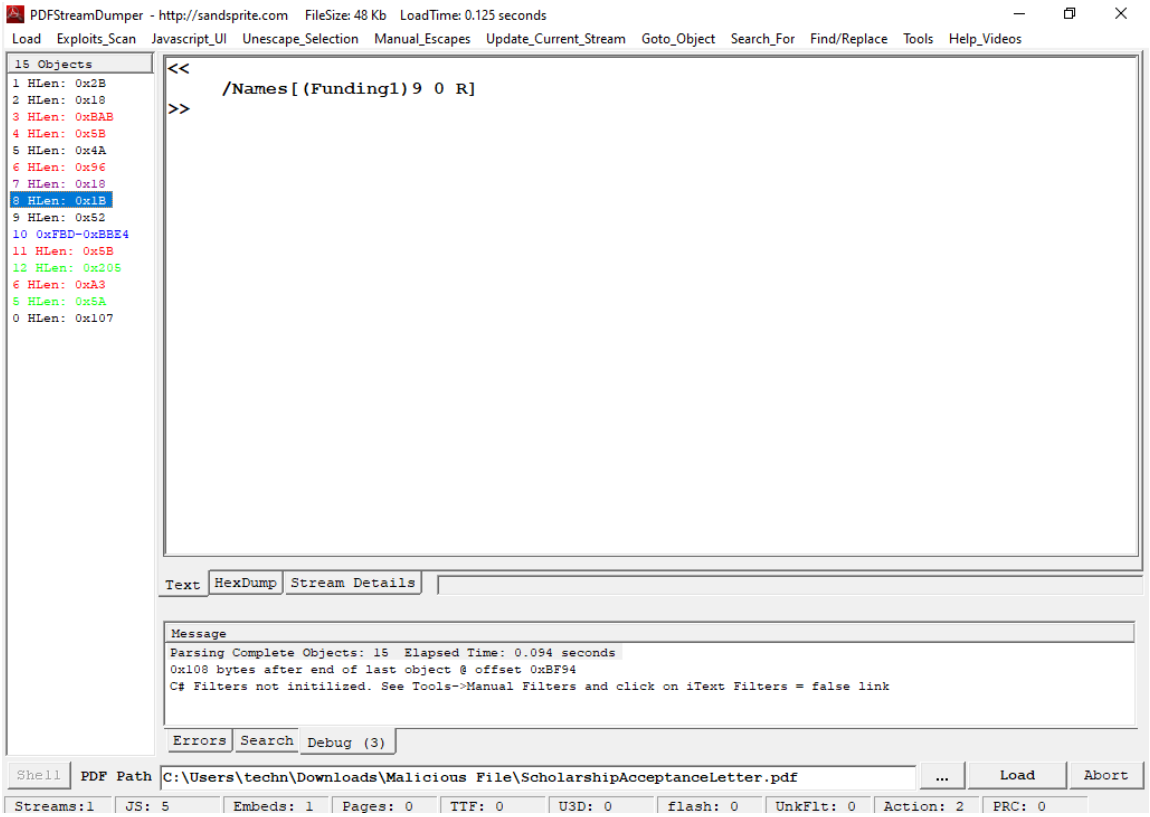
   /S/Launch represents launch message. We see there is no launch message embedded.
   To view the encrypted content please tick the “Do not show this message again” box and press open. This launch message comes automatically for every PDF by default.

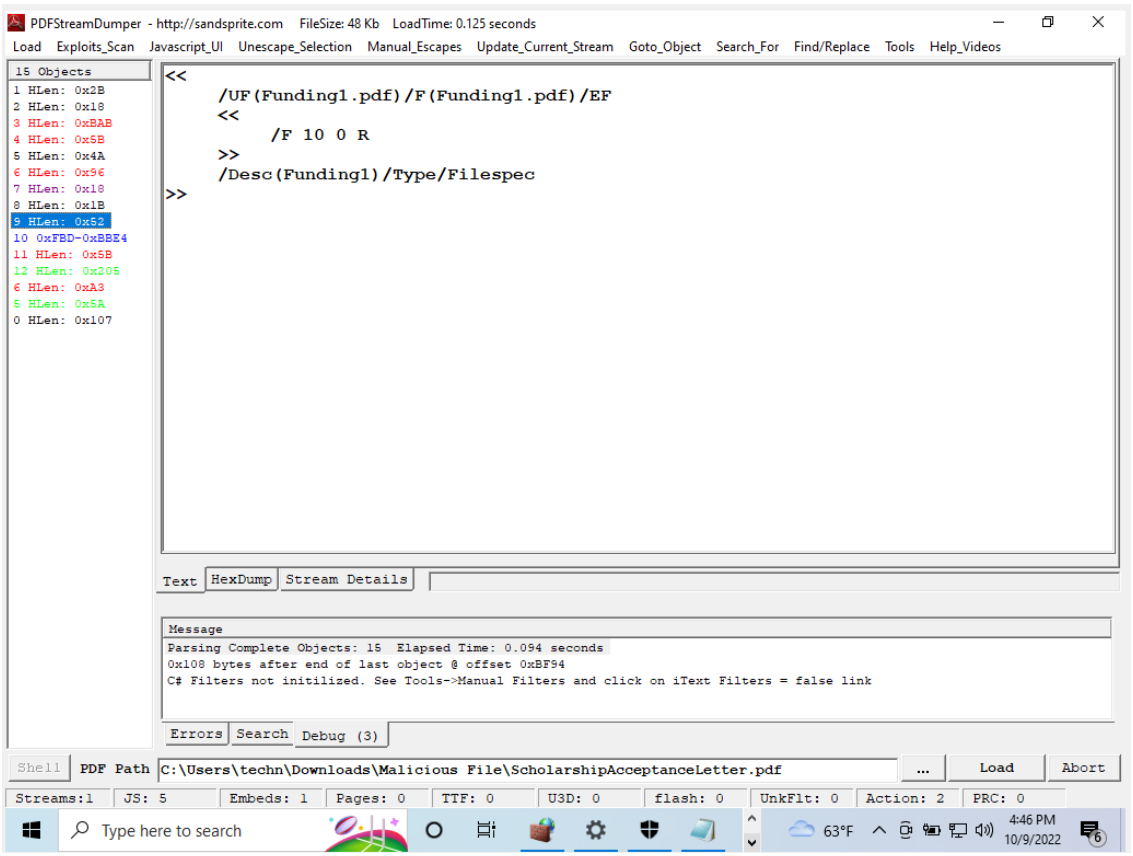
4. 

5. Here for object 7 we observe that the “exploitation type” used is **EmbeddedFiles.** There is no **Compression** or **obfuscation** found in the JS Objects.

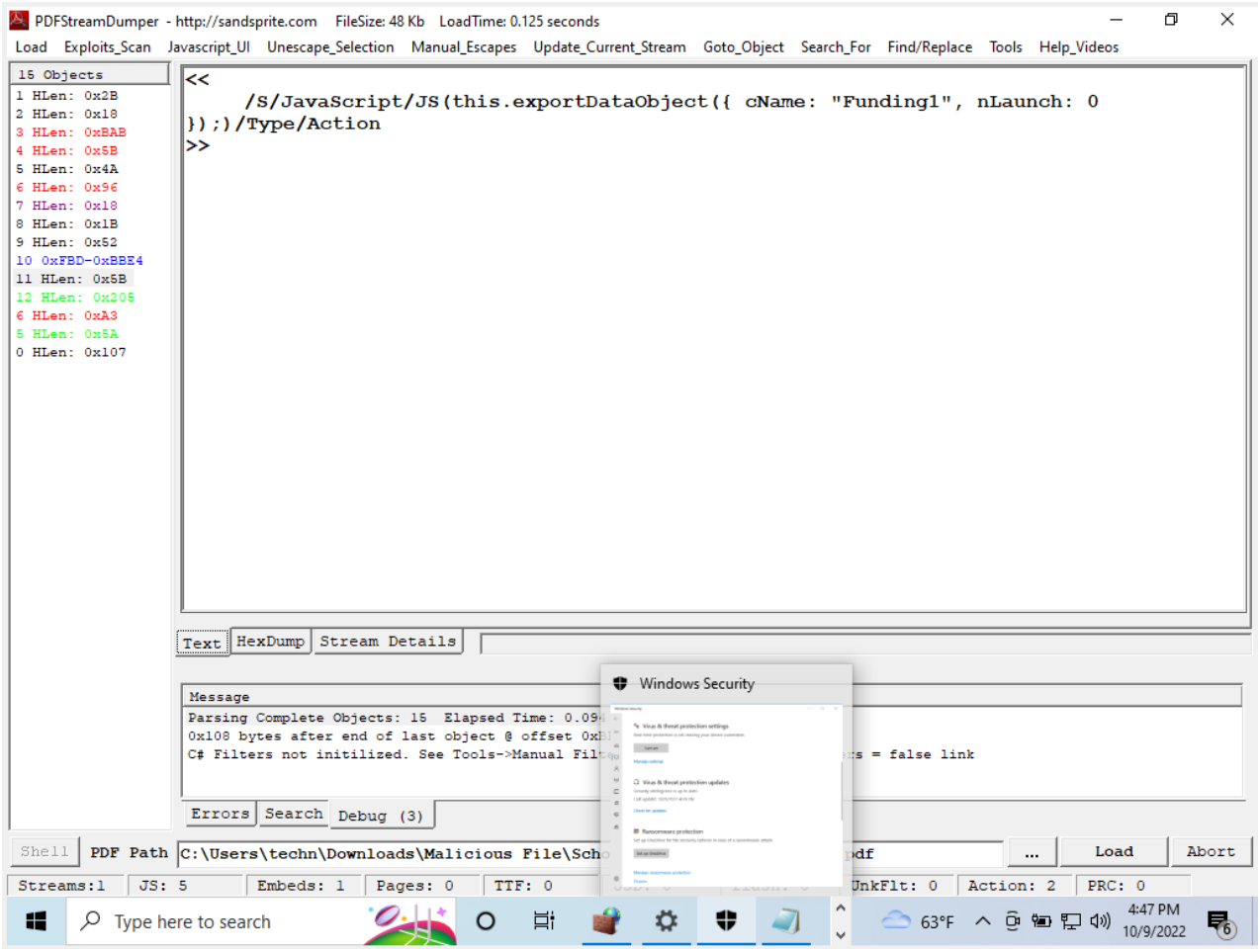


6. If clicked on object 8, we observe the /Names tag which give previous name of the file this shows that the filename is **Funding1** which is later renamed to **ScholarshipAcceptanceLetter.pdf**

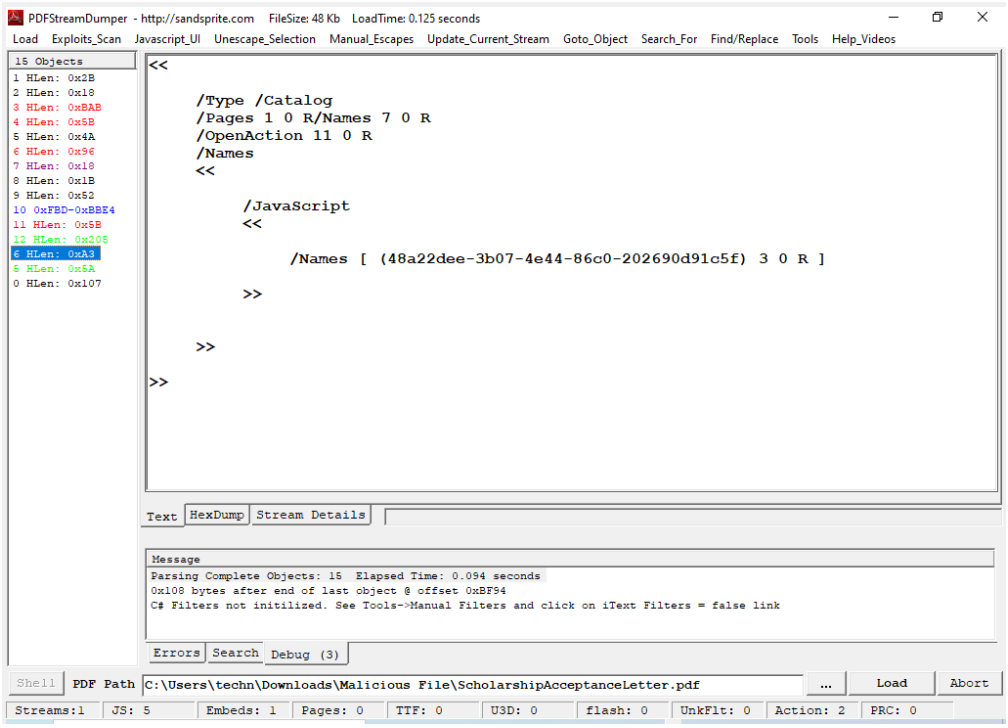


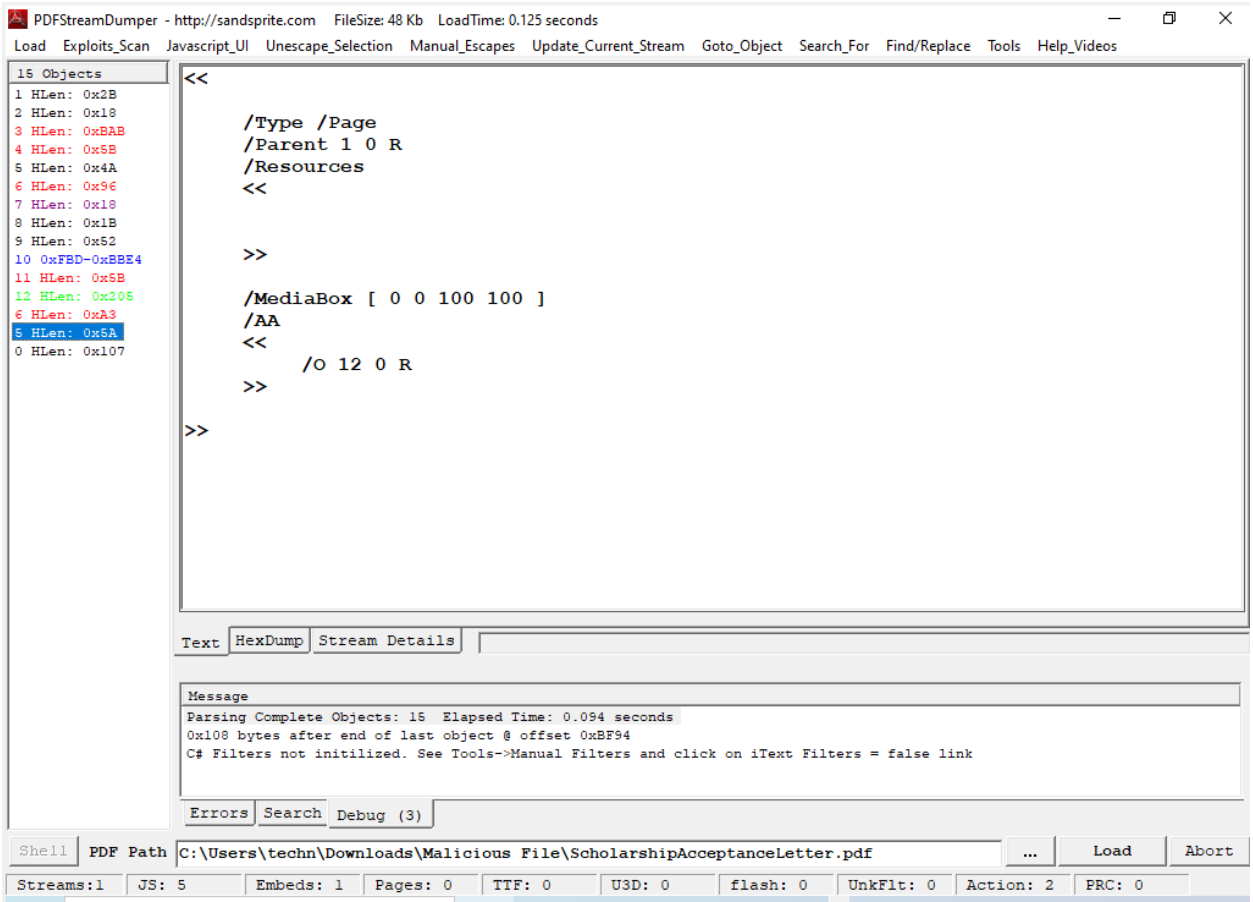


7. This shows if there is any JavaScript payload embedded, here we don't have any JS embedded with PDF.

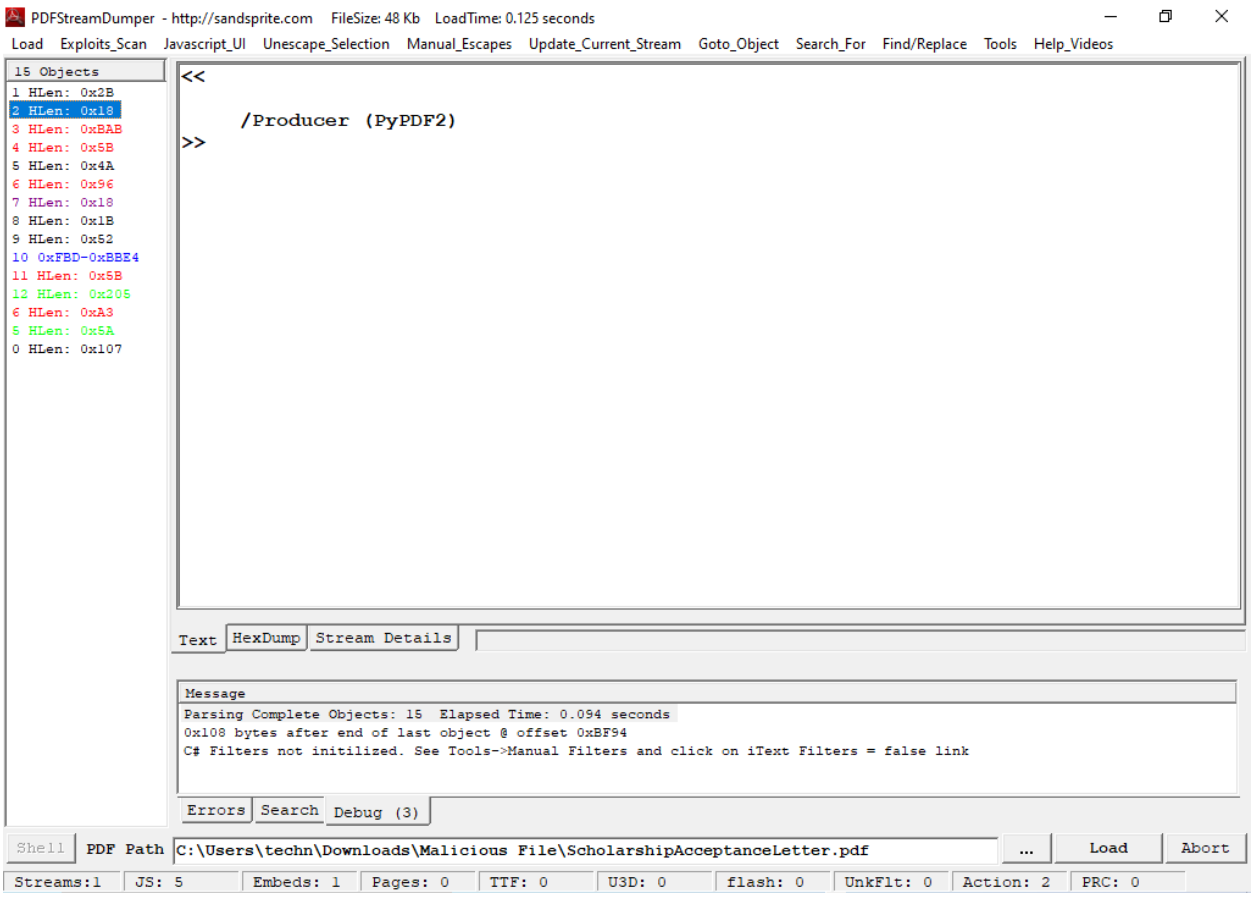


8. Represents number of pages in PDF, we analyse that number of pages are 1.





9. We see that no filters are added to PDF
   In message box, **Filters = false** is observed.



10. The JavaScript Code contains Unicode-encoded text when clicked on **Javascript_UI**, which is probably shell code. The script is not obfuscated.