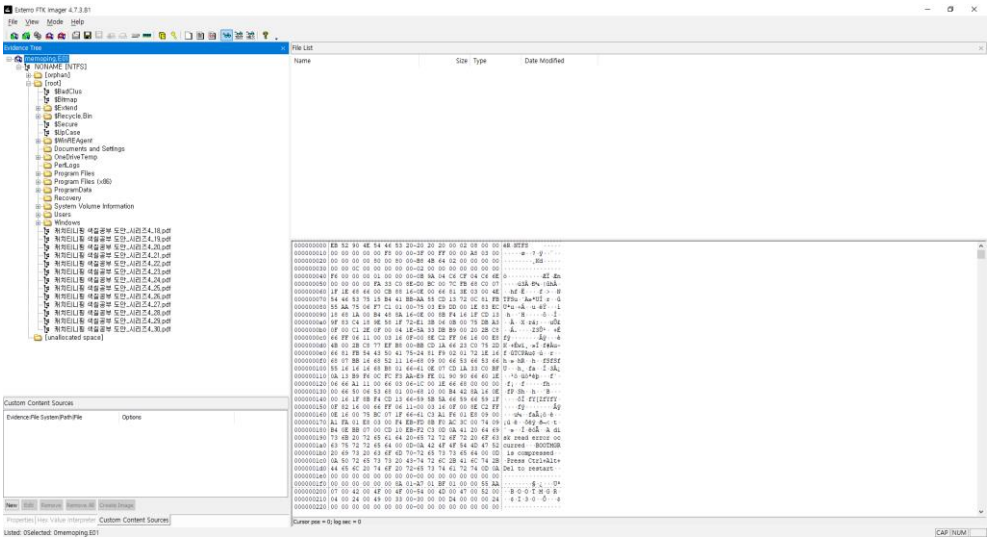
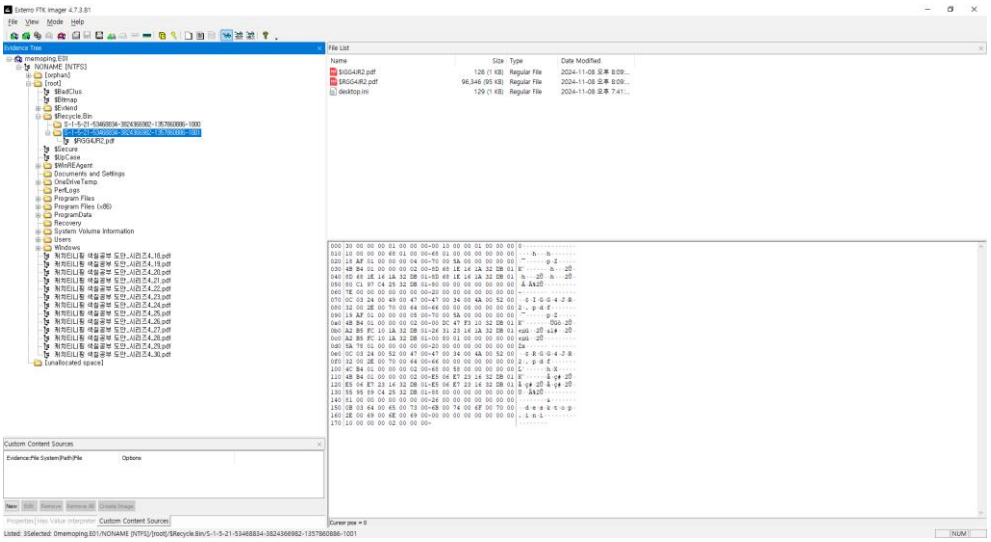
2024 JFS Writeup	
문제명	Zzoccomping
문제	겁이 많은 쪼꼼핑이 숨어버렸다. 쪼꼼핑한테 flag를 물어보자 (문제 파일은 Memoping과 동일)

문제 풀이

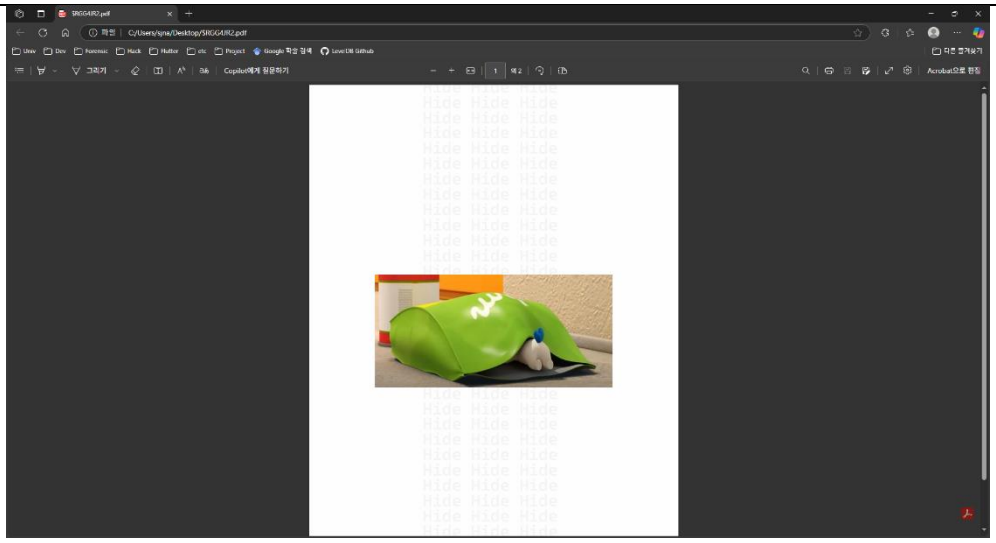
주어진 E01(Encase file format) 파일 분석을 위해 모든 문제 파일(E01-E06)을 같은 경로에 두고, FTK Imager를 사용하여 문제 파일을 마운트한다.
마운트된 정보를 아래와 같이 확인할 수 있다.



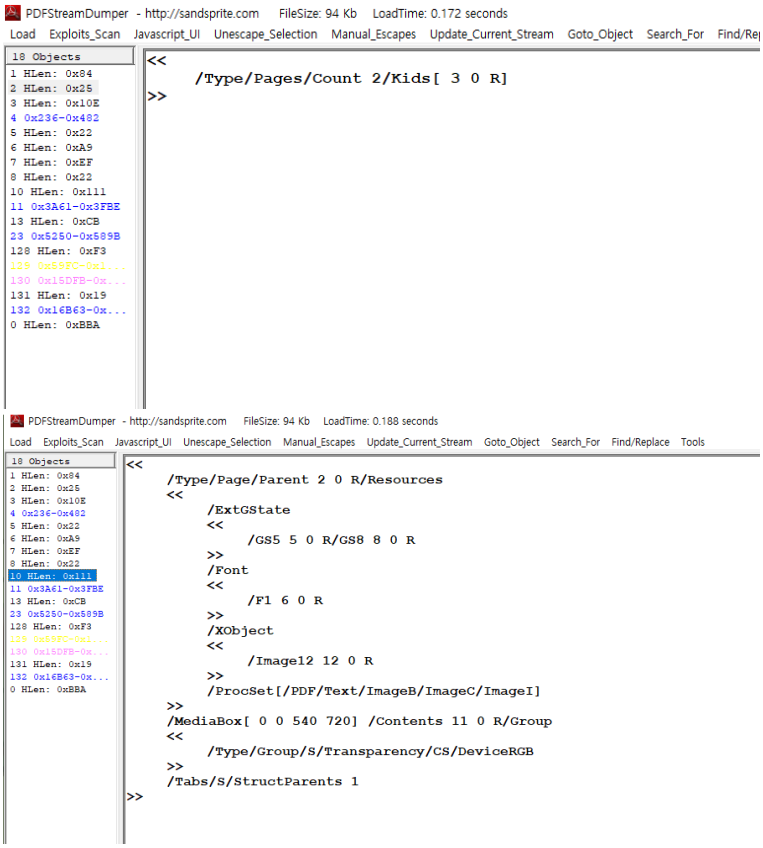
휴지통으로 삭제된 파일의 데이터가 있는 $Recycle.Bin에서 삭제된 pdf 파일을 확인할 수 있다.

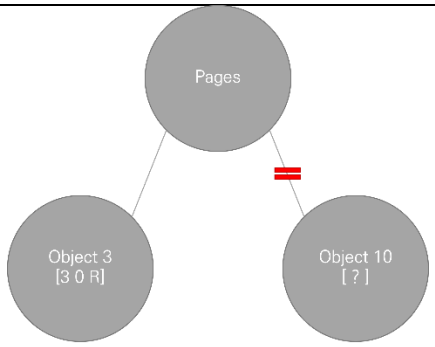


해당 경로에서 획득한 파일을 Export하여 확인하면 아래 같은 파일을 확인할 수 있다.



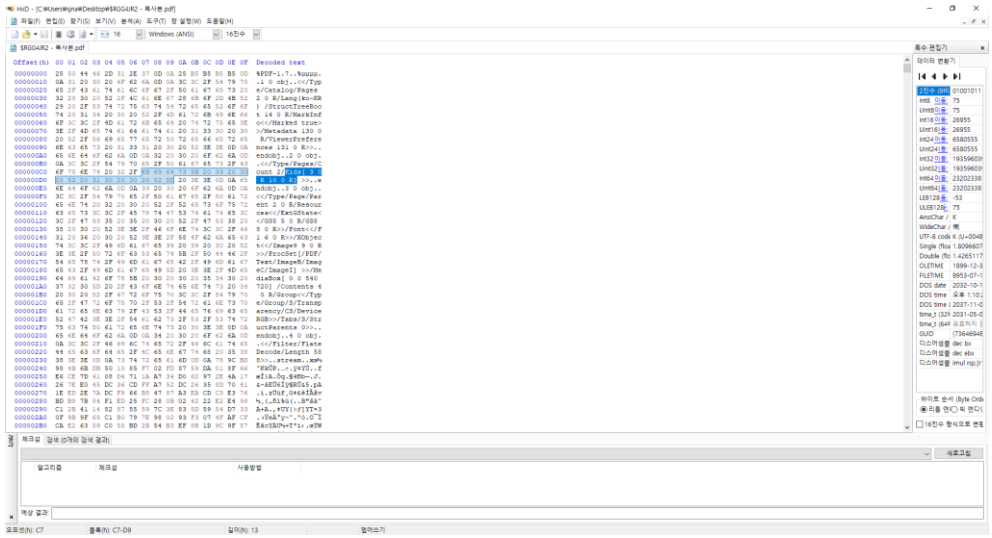
HxD 같은 HexViewer 혹은 PDFStreamDumper 같은 프로그램을 사용하여 파일을 분석하면 Object의 연결에 문제가 있는 것을 확인할 수 있다.
Page Count가 2로 총 2장의 문서가 포함되어 있는 것을 확인할 수 있는데 Kids는 [3 0 R]로 하나의 페이지(Object 3)만 가르키고 있고, 다른 페이지(Object 10)이 연결되지 않은 것을 알 수 있다.





[페이지 구조를 Tree로 표현]

해당 부분의 연결되지 않은 Object 10을 추가하고자, Hex Editor인 HxD를 사용하여 [10 0 R] 부분을 삽입한다.



수정된 파일을 통해 flag를 획득할 수 있다.