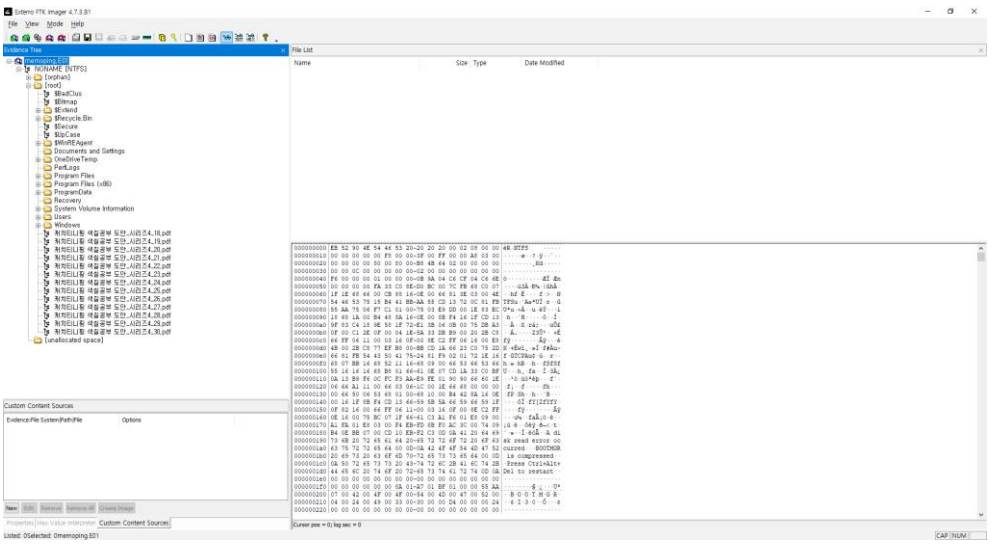
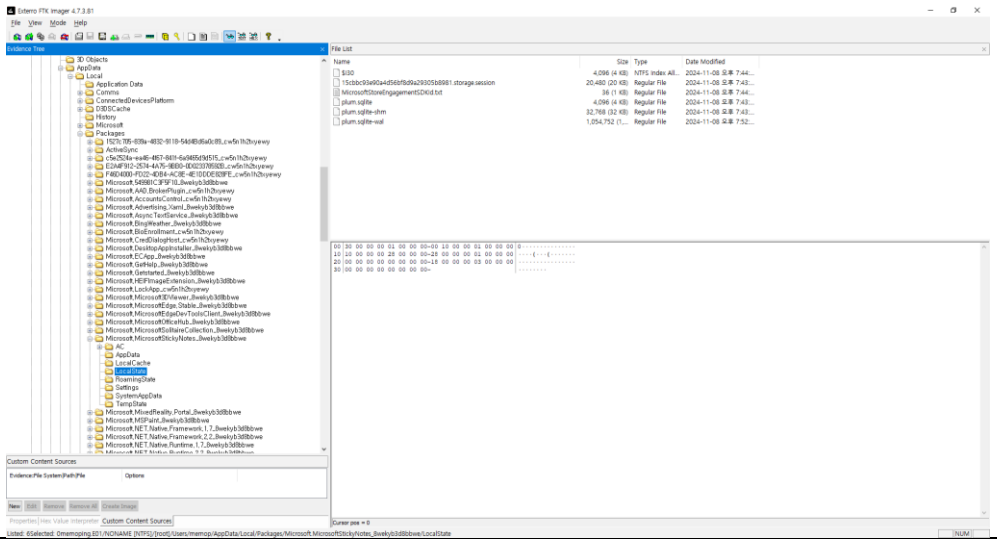
2024 JFS Writeup	
문제명	Memoping
문제	메모핑은 뭐든 까먹지 않기 위해 메모를 해둔다. 메모를 따라가보자👀
문제 풀이	

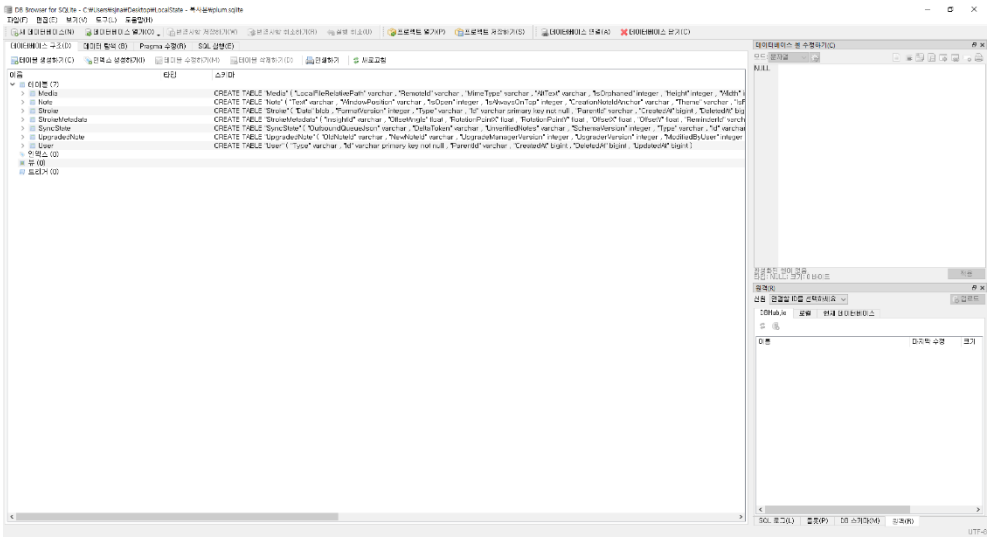
주어진 E01(Encase file format) 파일 분석을 위해 모든 문제 파일(E01-E06)을 같은 경로에 두고, FTK Imager를 사용하여 문제 파일을 마운트한다.
마운트된 정보를 아래와 같이 확인할 수 있다.



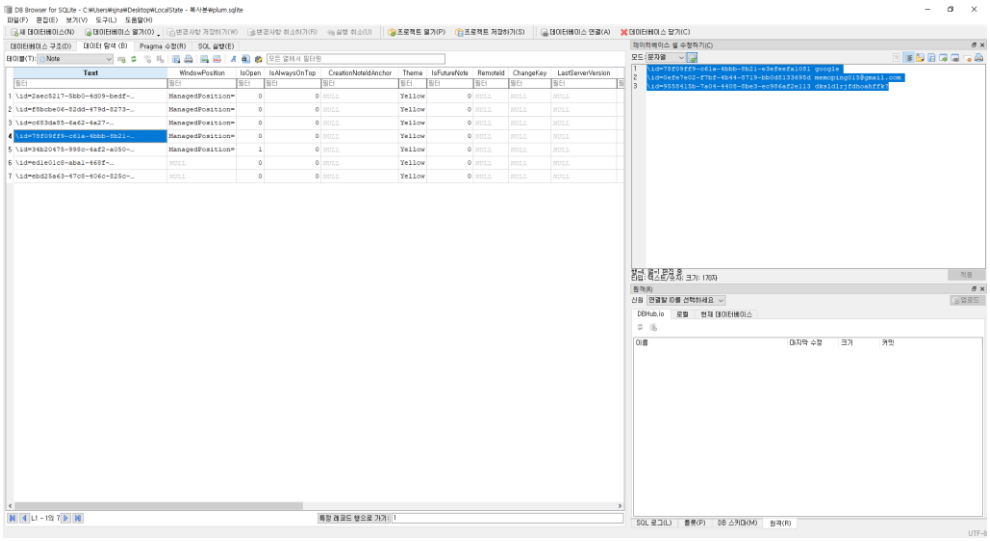
메모와 관련된 파일을 확인하기 위해서는 Windows에서 기본 패키지로 제공하는 Sticky notes에 대한 아티팩트를 분석할 수 있다.
User > AppData > Local > Packages > Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe > LocalState 하위에 아티팩트(데이터베이스)를 통해 사용자가 로컬에서 작성한 메모를 획득할 수 있다.



획득한 3개의 plum* 파일을 동일한 경로에 두고 DB Browser for SQLite를 사용하여 sqlite 파일을 확인하면 아래 같은 결과를 확인할 수 있다.



Note 테이블에서 하나의 노트를 하나의 튜플로 저장하고 있는 것을 확인할 수 있다.
이 중 Google 계정에 대해 작성된 노트를 찾을 수 있다.



계정 정보를 통해 로그인 후 Google Drive를 확인하면 FLAG 이름을 가진 docx 파일이 있다.
해당 문자열은 Base64로 인코딩되어 있어 해당 정보를 디코딩하면 최종 Flag를 획득할 수 있다.