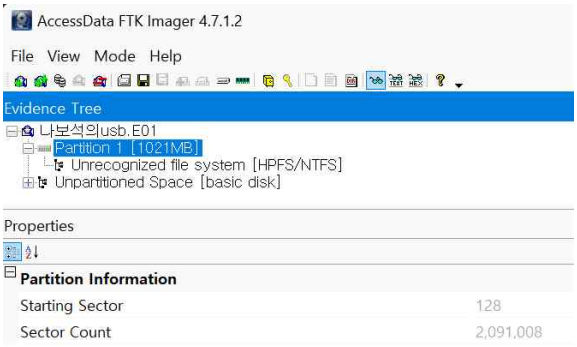
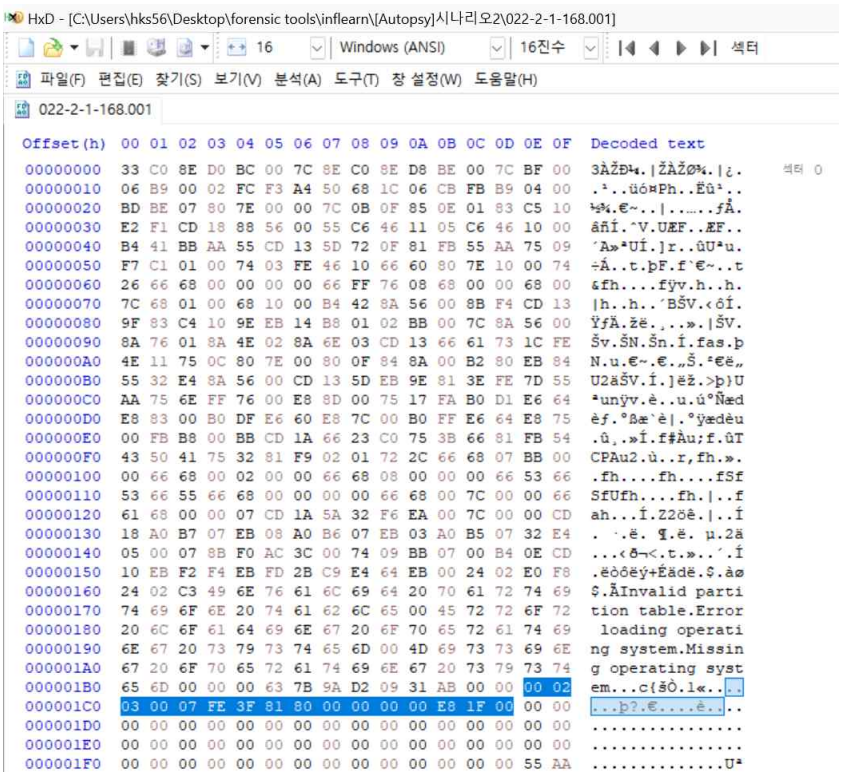
문제 2.

2. 훼손된 파티션의 복구 및 복구과정을 상세히 서술하시오

증거 USB를 .E01 파일로 이미징해 FTK Imager에서 불러온 결과, 아래와 같이 파티션 하나가 존재하였음. 해당 파티션은 128번 섹터부터 시작하여 2,091,008의 섹터 수를 가진 NTFS로 추정, Unrecognized file system으로 표시되어 내부 구조를 확인할 수 없었음. 이에 RAW 파일(.001)로 재이미징을 진행함.



HxD를 활용하여 이에 재이미징한 RAW 파일(.001)을 확인하였을 때, 첫 번째 섹터인 MBR(0번 섹터)의 Partition Table로 파티션 정보를 다음과 같이 확인할 수 있었으며,



파티션 1에 대한 파티션 테이블 정보를 확인하여 해당 파티션 시작 섹터인 128로 이동하여 확인한 결과, PBR이 훼손되었음을 확인, 이에 NTFS PBR 백업본이 저장되어 있는 해당 파티션 마지막 섹터(128+2,091,008-1=2,091,135 섹터)로 이동하여 원래 PBR 위치인 128번 섹터에 붙여넣기 쓰기해 복구하여 다른이름으로 저장함.

이후 FTK Imager에서 복구 이미지파일 확인 시 아래와 같이 해당 파티션 내부구조를 확인할 수 있었음.