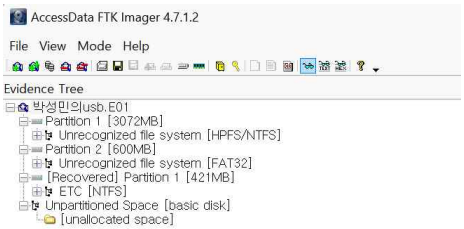
문제 2.

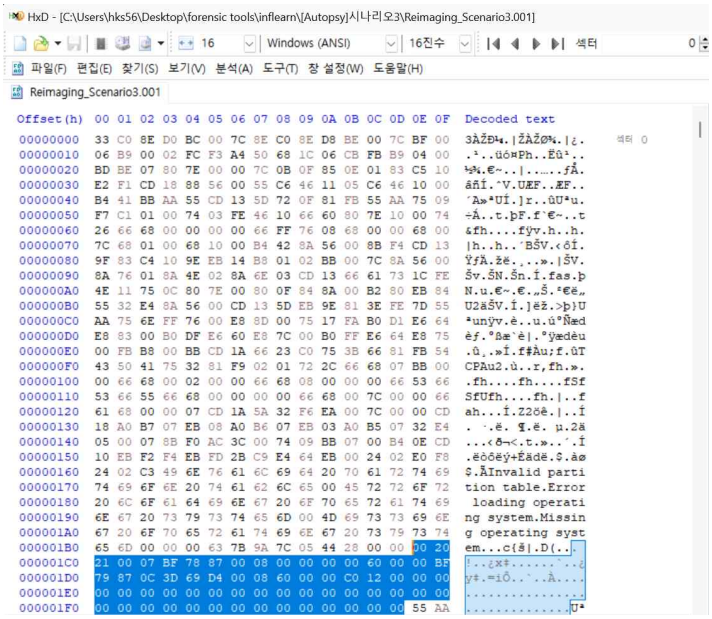
2. 훼손된 파티션을 복구하고 복구과정을 상세히 기술하시오

1) 사본 이미지 파일 확인



- 증거 원본USB를 이미징한 사본 이미지파일(.E01)을 FTK Imager를 통해 열어본 결과 총 3개의 파티션이 존재하였으며, [파티션1]과 [파티션2]는 Unrecognized file system으로 해당 파티션들의 내부를 확인할 수 없었고, [Recovered-파티션1]은 해당 파티션 내부를 확인할 수 있어 [파티션1]과 [파티션2]에 대한 파티션 복구를 다음과 같은 과정으로 실시함.

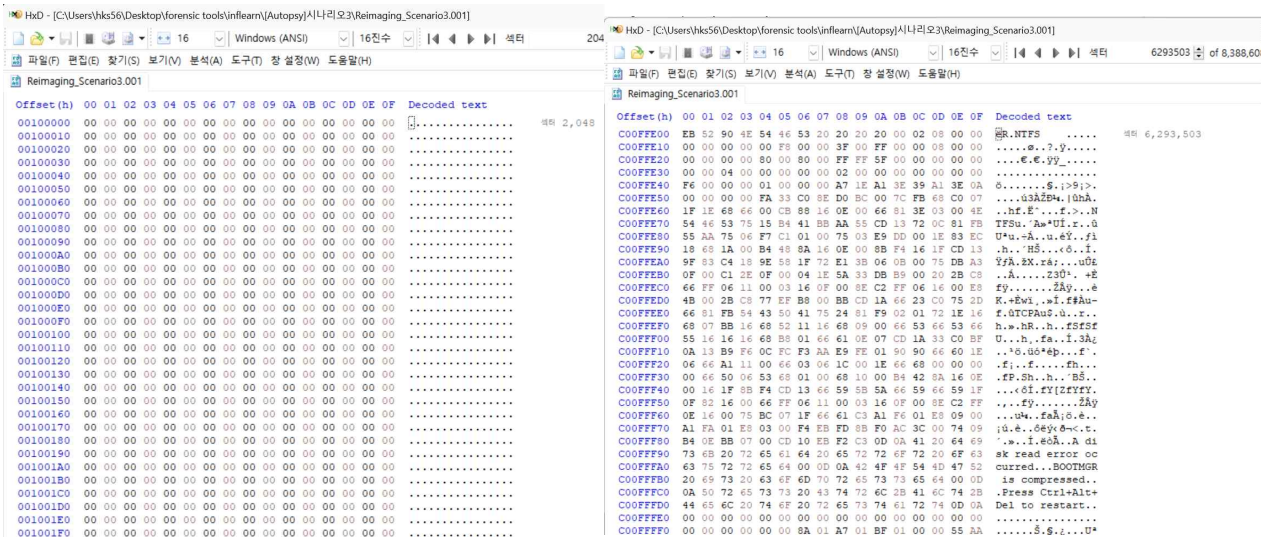
2) 파티션 복구



- HxD를 활용하여 파티션 복구하기 위해 .E01 이미지 파일을 .001 (RAW) 파일로 재이미징하여 HxD에서 해당 재이미지 파일 불러와 섹터 0(MBR) 내용 확인함. MBR 내 Partition Table/FTK Imager에서 교차확인하여(리틀엔디안->빅엔디안) 복구할 파티션 정보 획득.

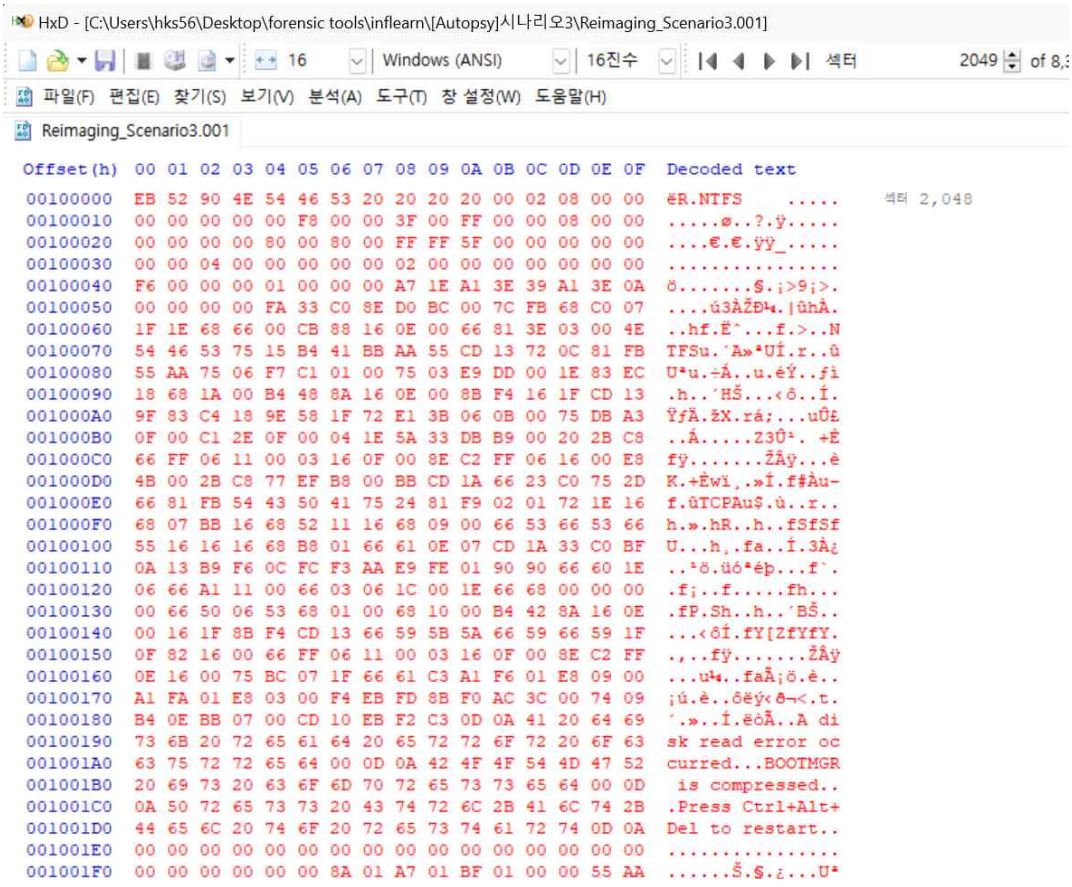
	Starting Sector	Sector Count	File System
파티션1	2,048	6,291,456	NTFS(0X07 ; PBR 백업본 : 6,293,503)
파티션2	6,293,504	1,228,800	FAT32(0X0C ; PBR 백업본 : 6,293,510)

가. [파티션1] 복구

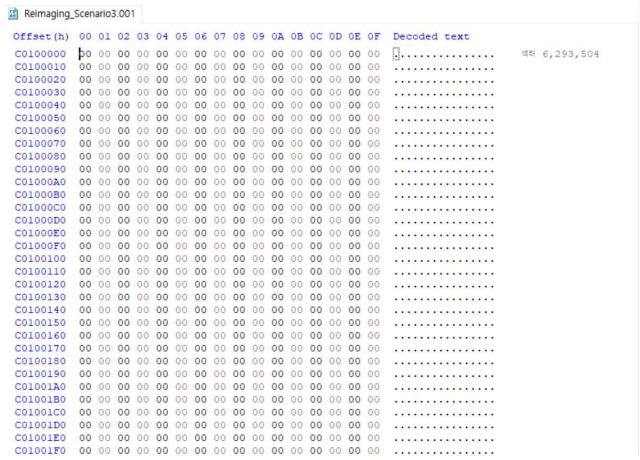


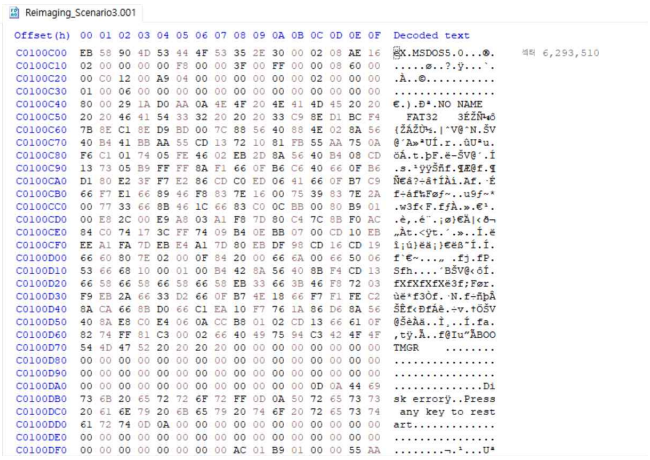
- [파티션1] 복구를 위해 해당 파티션 시작 섹터인 2,048로 이동하여 PBR확인 시 PBR 훼손되었음. 이에 따라 NTFS 파일시스템에서 PBR 백업본이 존재하는 해당 파티션(파일시스템) 마지막 섹터로 이동 (Starting Sector)2,048 + (Sector Count)6,291,456 -1 = 6,293,503

- 해당 PBR 백업본 복사 후 시작섹터 2,048에 붙여넣어 [파티션1] 복구



나. [파티션2] 복구

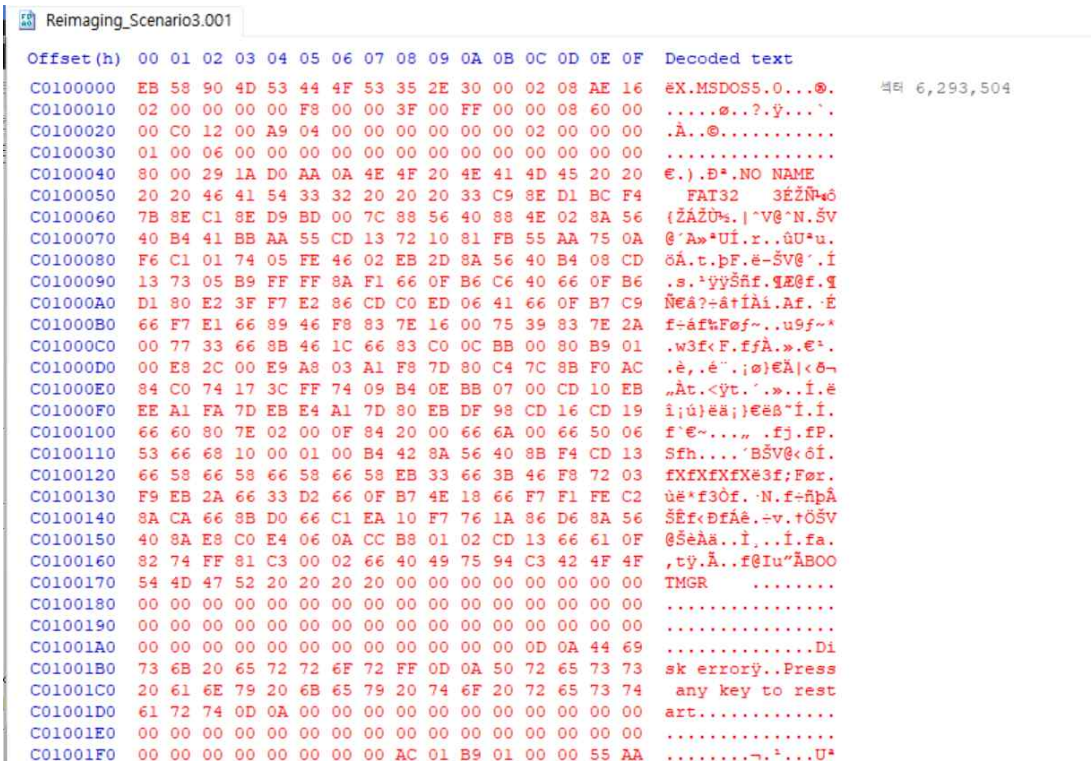




- [파티션2] 복구를 위해 해당 파티션 시작 섹터인 6,293,504로 이동하여 PBR확인 시 PBR 훼손되었음. 이에 따라 FAT32 파일시스템에서 PBR 백업본이 존재하는

(해당 파티션(파일시스템) 시작 섹터 6,293,504 + 6 =) 6,293,510 섹터로 이동

- 해당 PBR 백업본 복사 후 시작섹터 6,293,504에 붙여넣어 [파티션2] 복구하여 다른 이름으로 저장함.



- 이후 FTK Imager, Autopsy로 다음과 같이 분석을 위해 복구된 이미지 파일 열람, 파티션 복구되어 모든 파티션 내부구조 확인 가능.