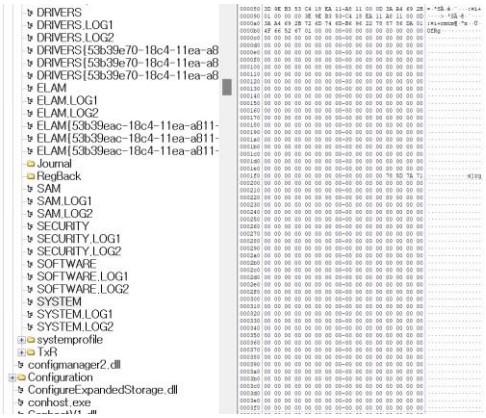
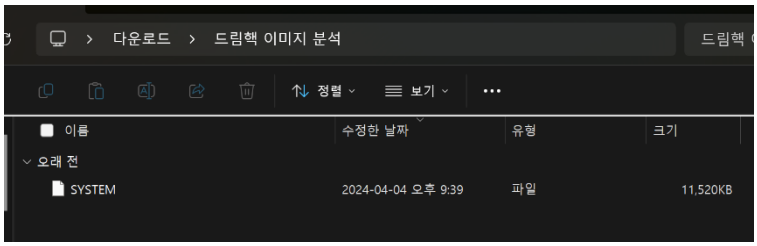
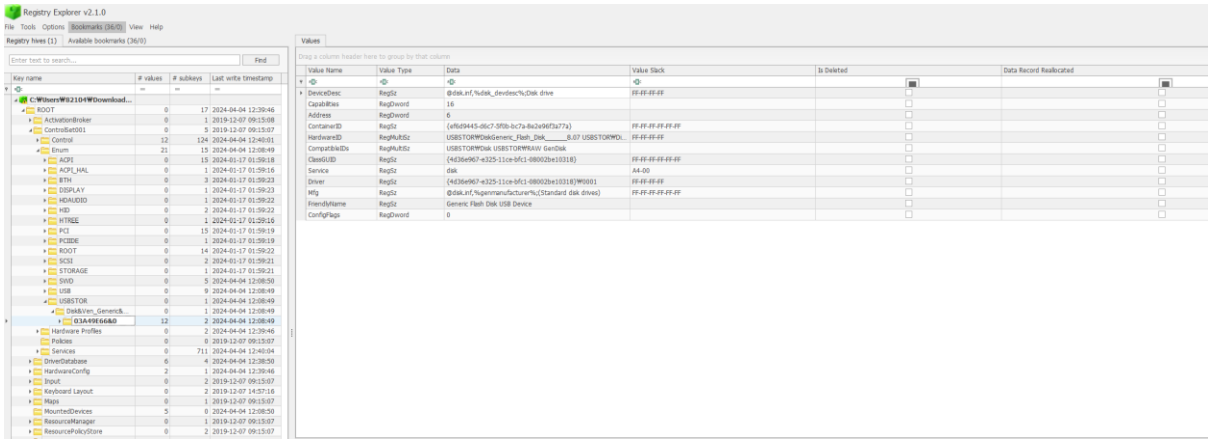
8) 관련 워게임 풀이

1. Find the USB

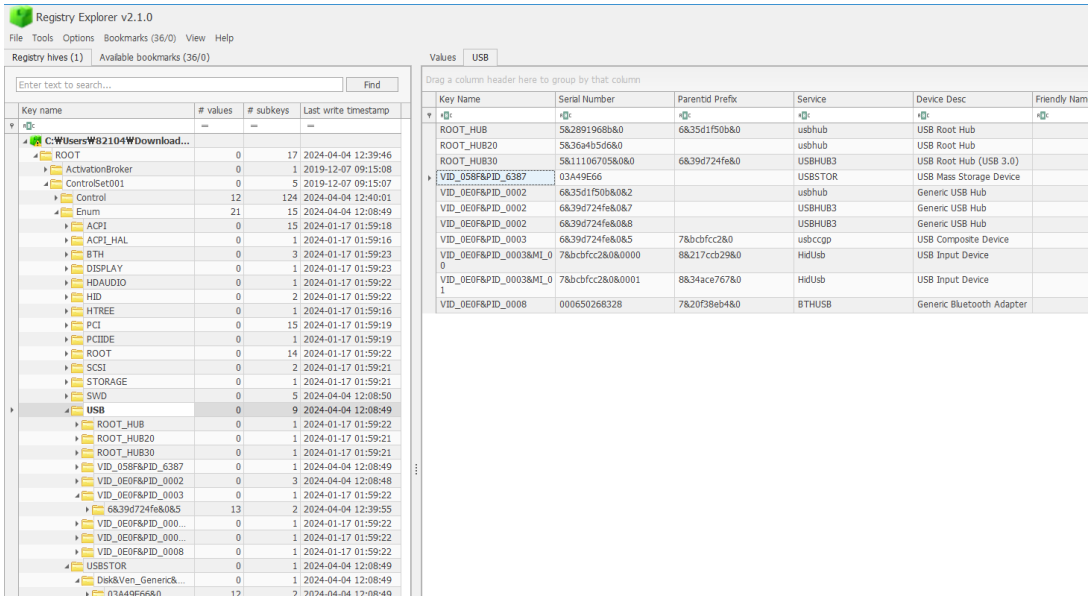




문제 디스크 이미지에서 FTK Imager을 사용해, SYSTEM 하이브만 추출해냈다.



그리고, 추출한 하이브를 Register Explorer를 활용해, ControlSet001₩Enum₩USBSTOR 해당 경로를 들어가니, 2024-04 날짜로 기록된 USB 디바이스 기록 하나를 발견할 수 있었다.



이번에는 ControlSet001₩Enum₩USB 경로로 들어가, 해당 2024년 4월 4일에 연결 및 제거된 USB 장치를 찾았다. 그리고 이의 VID, PID, Device Serial Number를 알아내 플래그 값을 얻을 수 있었다.

DH{058F_6387_03A49E66}