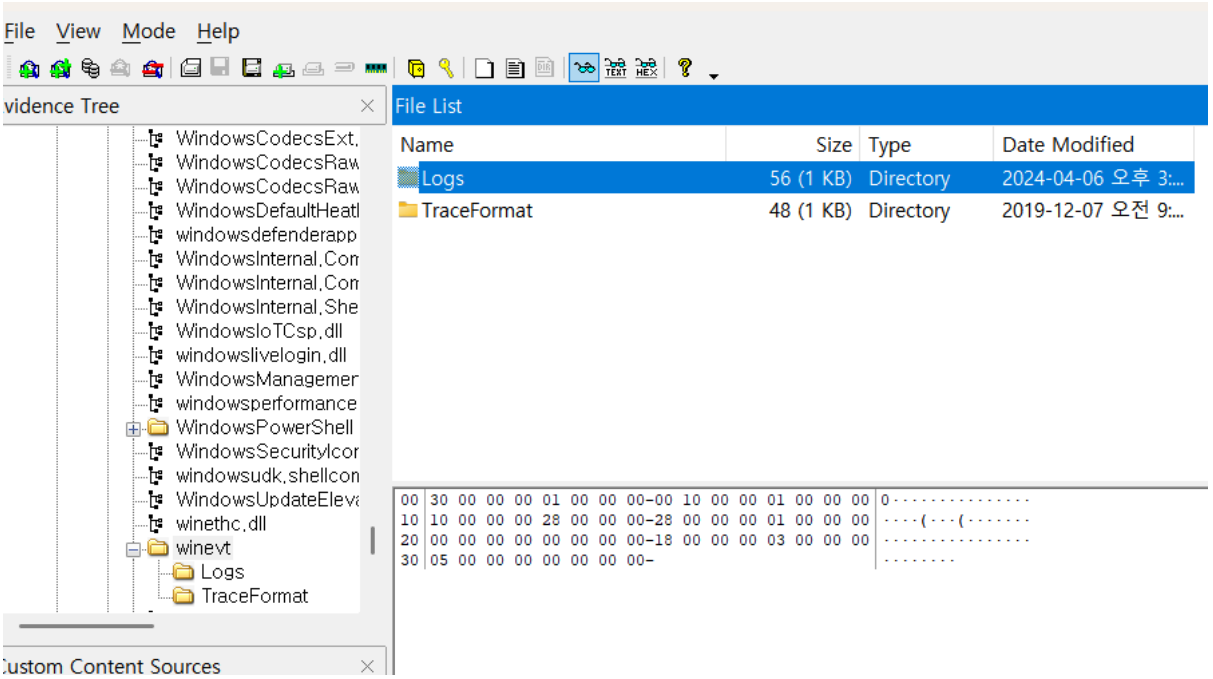
Dreamhack-boot_time

4608를 찾기!(4608: windows 시스템의 보안 로그 초기화를 알리는 이벤트)

ftk로 파일 열어주고

C:\Windows\System32\winevt\Logs\ 경로로 가면 된다.



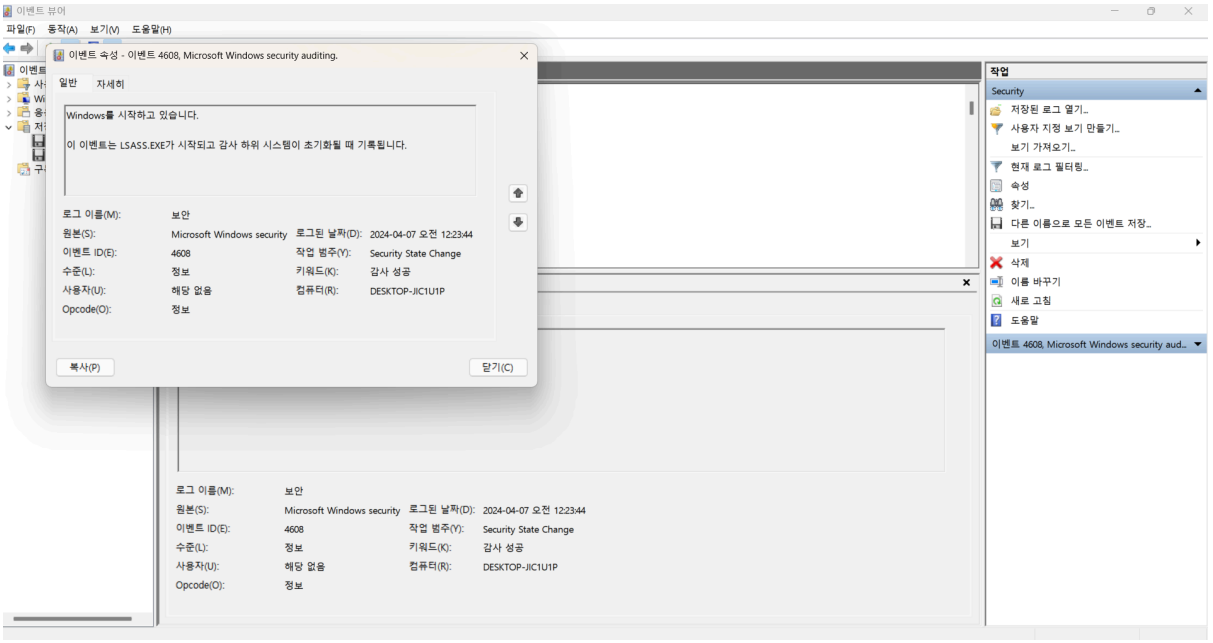
여기서 로그 파일 전체를 추출해야한다.

근데 우리는 시스템의 보안 로그 초기화를 살펴봐야하니까 시큐리티 로그에 들어가서 이벤트 로그를 검색해야 한다

추출한 로그 파일에서 시큐리티에 들어가서

현재 로그 필터링을 누르고 찾기를 통해서

4608을 검색한다 그럼 시간을 볼 수가 있다.



FLAG: DH{2024_04_07_00_23_44}