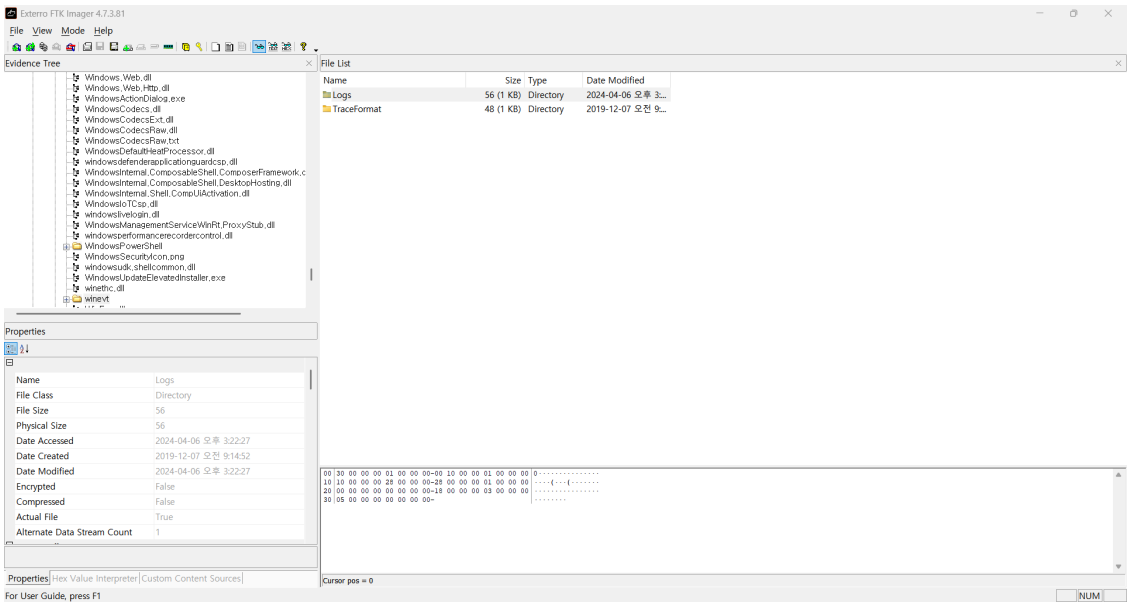
Dreamhack-boot_time (level1)

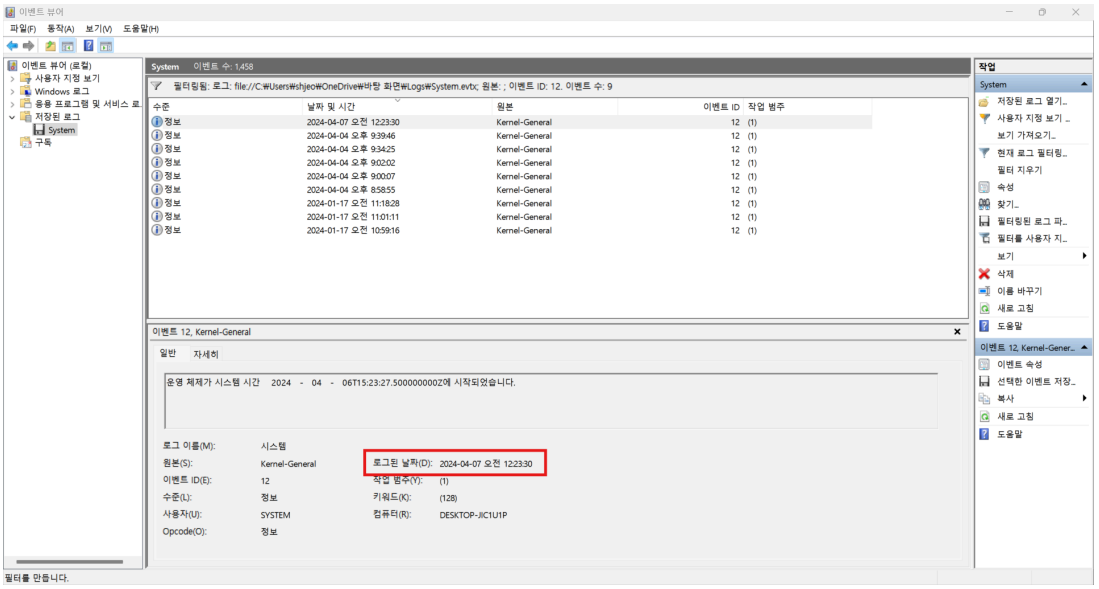
> 👉 **[함께실습] boot_time에서 실습하는 문제입니다.**
>
> **당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.**
>
> **주어진 이미지의 이벤트 로그를 분석하여, 해당 PC가 마지막으로 부팅된 시간을 구해주세요.**

사용 툴 - FTK Imager, 이벤트 뷰어

1. FTK Imager 를 통해 로그 파일 추출
    - 경로 : `C:\Windows\system32\winevt\Logs`



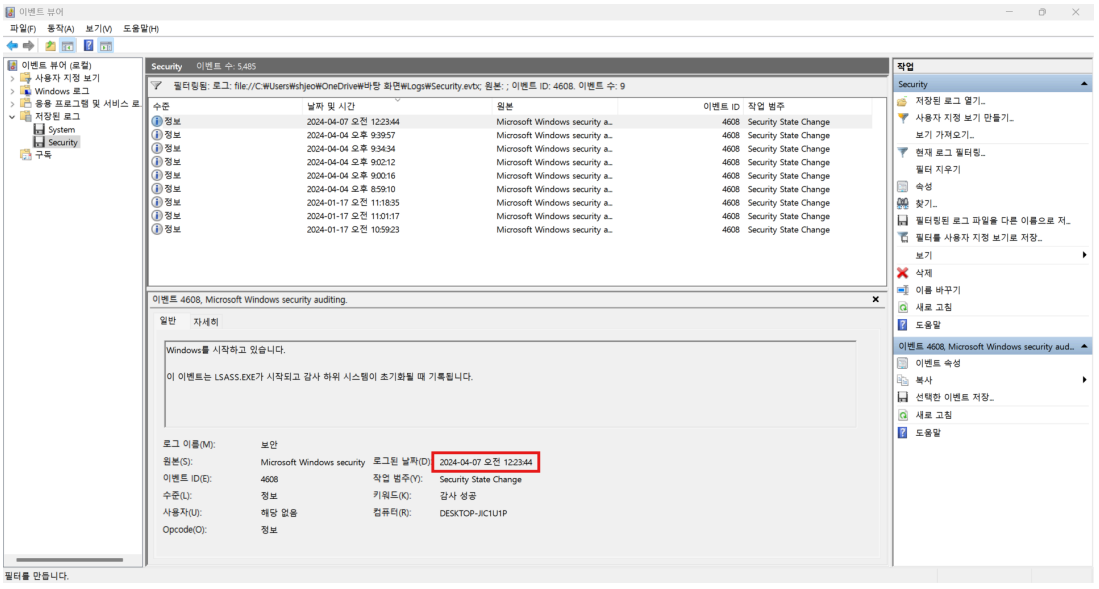
2. 이벤트 뷰어를 통해 System.evtx 확인
    - 분석 내용 : 이벤트 ID 12 = 커널이 부팅 시작했을 때 (Operating system started)



3. System.evtx 와 정답이 일치하지 않음

4. 이벤트 뷰어를 통해 Security.evtx 확인

   - 분석 내용 : 이벤트 ID 4608 = 시스템이 시작될 때 (부팅 직후)



👉 DH{2024_04_07_00_23_44}

- CF. 이벤트 ID 12 VS 4609
  - 12 : 시스템이 부팅되어 이벤트 로그 서비스를 시작했음
  - 4608 : 운영체제 자체가 부팅을 시작했음

  → 일반적으로 12를 사용함