boot_time

Description

[함께실습] boot_time에서 실습하는 문제입니다.

당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.

주어진 이미지의 이벤트 로그를 분석하여, 해당 PC가 마지막으로 부팅된 시간을 구해주세요.

Info

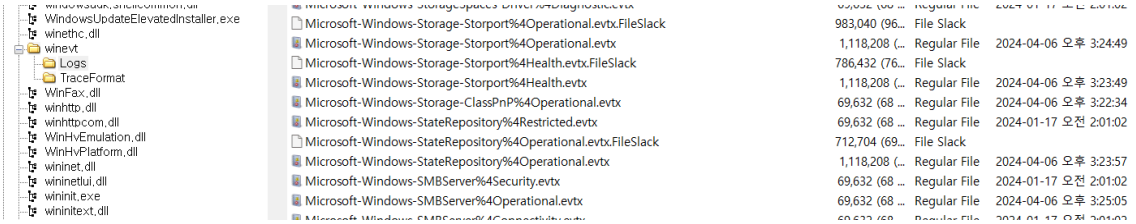
FLAG = `DH{yyyy_MM_dd_hh_mm_ss}yy` , `MM` , `dd` , `hh` , `mm` , `ss` 는 시간을 표현하는 방식으로 각각 연, 월, 일, 시, 분, 초를 나타냅니다. 예를 들어 시간이 `2024-01-02 03:04:05` 라면, FLAG는 `DH{2024_01_02_03_04_05}` 입니다.시간은 UTC+9를 기준으로 합니다.

- FLAG = `DH{yyyy_MM_dd_hh_mm_ss}`
- `yy` , `MM` , `dd` , `hh` , `mm` , `ss` 는 시간을 표현하는 방식으로 각각 연, 월, 일, 시, 분, 초를 나타냅니다. 예를 들어 시간이 `2024-01-02 03:04:05` 라면, FLAG는 `DH{2024_01_02_03_04_05}` 입니다.
- 시간은 UTC+9를 기준으로 합니다.

1. 구글에 위도운 이벤트 로그 찾기

윈도우 이벤트 로그는 기본적으로 `%SystemRoot%₩System32₩winevt₩Logs` 경로에 저장됩니다. 이벤트 로그는 시스템, 애플리케이션, 보안, 설정 등 다양한 종류로 나뉘며, 이벤트 뷰어에서 확인하거나 직접 파일 경로로 접근하여 확인할 수 있습니다.

2. FTK Imager에서 해당 e01파일 열고 경로 찾기



3. 윈도우 부팅 시스템 이벤트 ID가 4608이라는 것 확인

AI 개요

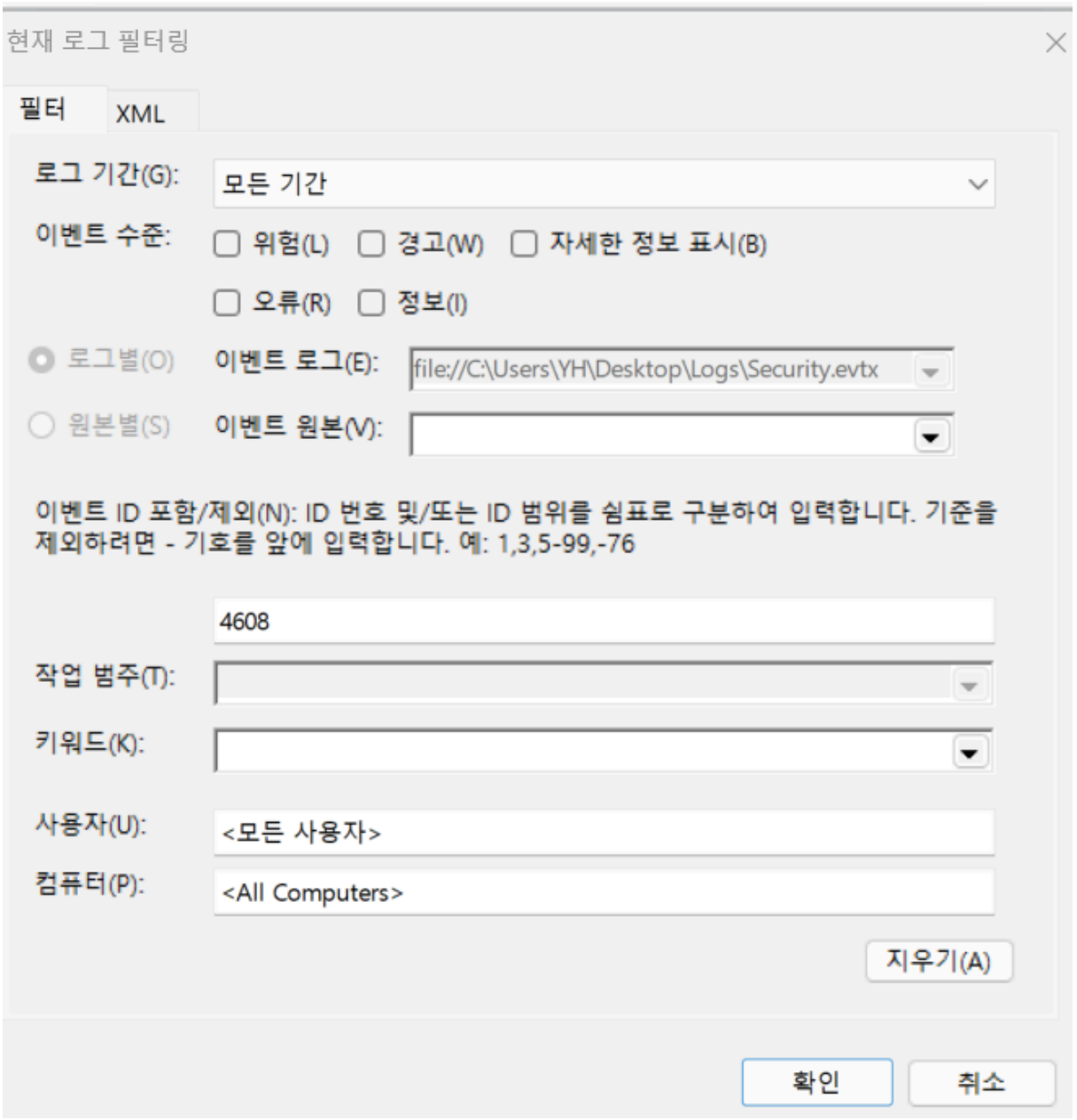
이벤트 ID 4608은 **윈도우 시스템이 시작되었음을 나타내는 이벤트**입니다. 이 이벤트는 시스템이 부팅 과정을 시작하고 LSASS.EXE 프로세스가 실행되며 감사가 초기화될 때 기록됩니다. ManageEngine 또는 Ultimate Windows Security 와 같은 사이트에서 자세한 정보를 찾을 수 있습니다.

자세한 내용:

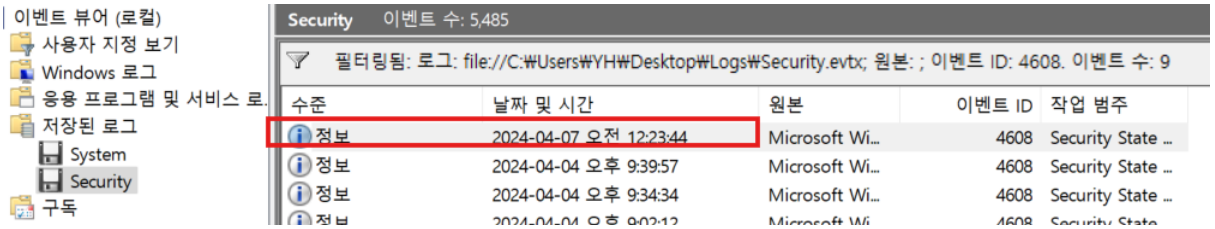
이벤트 ID 4608:

이 이벤트는 윈도우 운영 체제 자체가 부팅을 시작했음을 나타냅니다.

4. 로그 필터링 4608 확인


현재 로그 필터링
필터
XML
로그 기간(G):
모든 기간
이벤트 수준:
위험(L)
경고(W)
자세한 정보 표시(B)
오류(R)
정보(I)
로그별(O)
이벤트 로그(E):
file://C:\Users\YH\Desktop\Logs\Security.evtx
원본별(S)
이벤트 원본(V):
이벤트 ID 포함/제외(N): ID 번호 및/또는 ID 범위를 쉼표로 구분하여 입력합니다. 기준을 제외하려면 - 기호를 앞에 입력합니다. 예: 1,3,5-99,-76
4608
작업 범주(T):
키워드(K):
사용자(U):
<모든 사용자>
컴퓨터(P):
<All Computers>
지우기(A)
확인
취소

5. 날짜 및 시간 확인


이벤트 뷰어 (로컬)
사용자 지정 보기
Windows 로그
응용 프로그램 및 서비스 로...
저장된 로그
System
Security
구독
Security 이벤트 수: 5,485
필터링됨: 로그: file://C:₩Users₩YH₩Desktop₩Logs₩Security.evtx; 원본: ; 이벤트 ID: 4608. 이벤트 수: 9
수준 날짜 및 시간 원본 이벤트 ID 작업 범주
정보 2024-04-07 오전 12:23:44 Microsoft Wi... 4608 Security State ...
정보 2024-04-04 오후 9:39:57 Microsoft Wi... 4608 Security State ...
정보 2024-04-04 오후 9:34:34 Microsoft Wi... 4608 Security State ...