Dreamhack-boot time(level1)

[forensics]

Description

당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.

주어진 이미지의 이벤트 로그를 분석하여, 해당 PC가 마지막으로 부팅된 시간을 구해주세요. (2024.10.02)

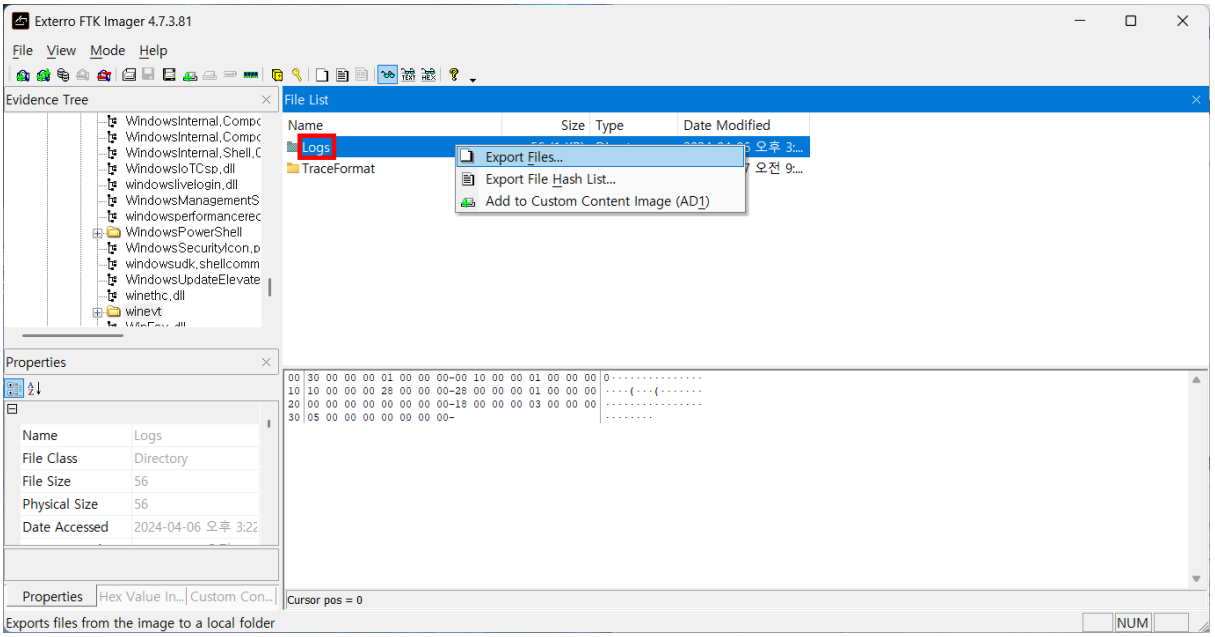
Info

- 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.

Write up

- 사용 도구: FTK Imager, 이벤트 뷰어

- FKT Imager를 통해 `C:\Windows\System32\winevt\Logs` 폴더 추출

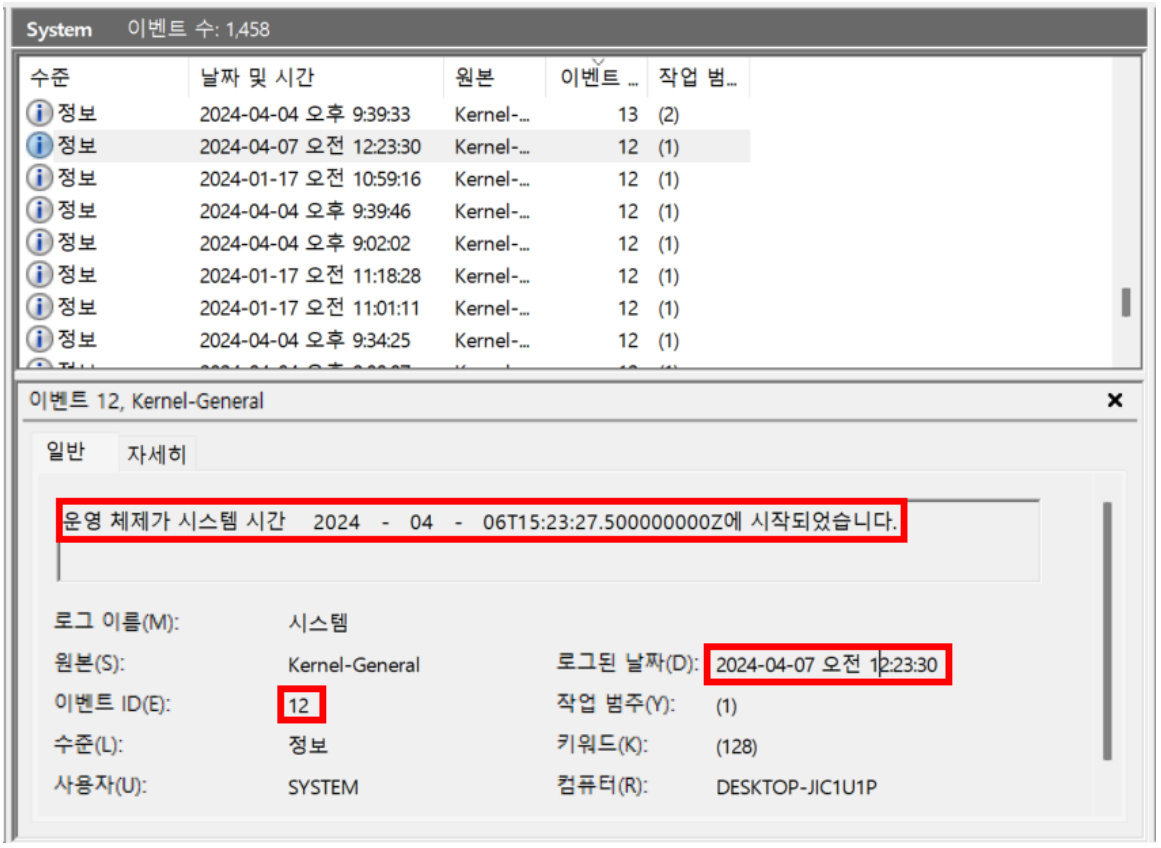


<System.evtx>

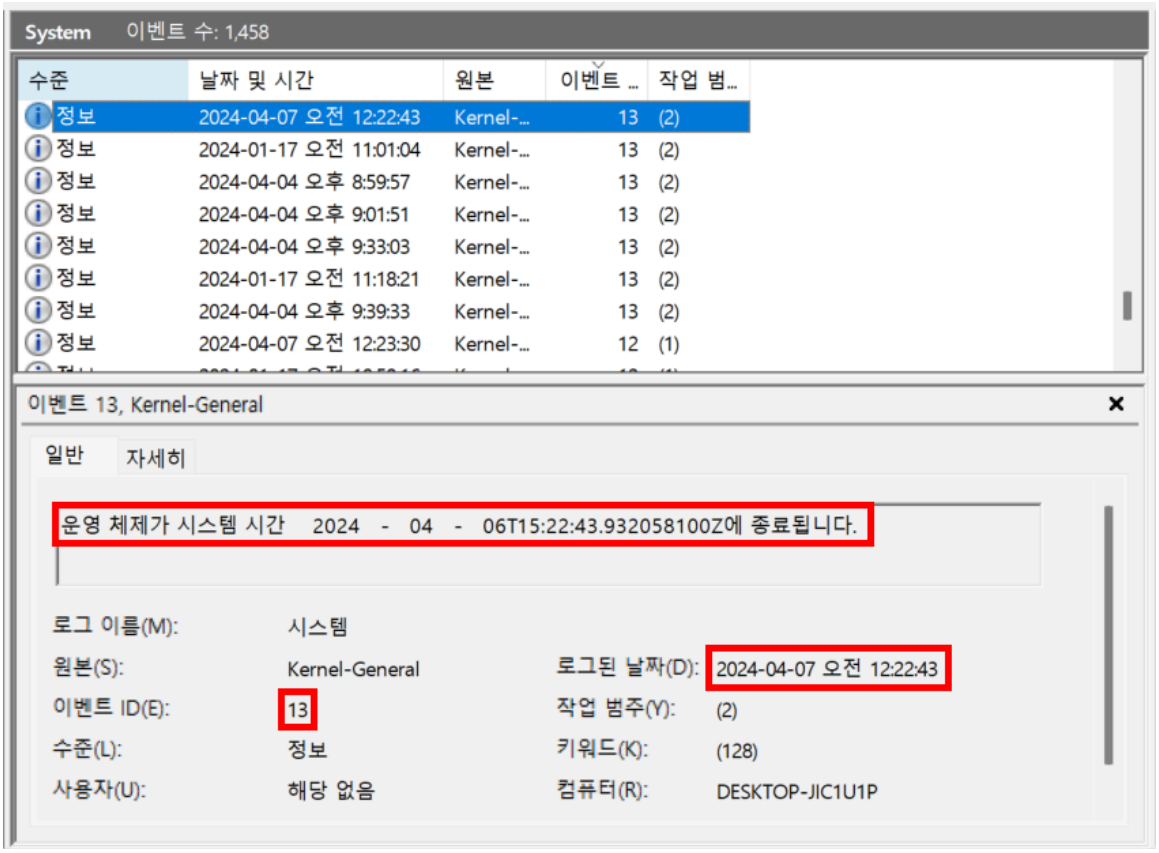
- 부팅 관련 이벤트 ID

12	Kernel-General, 운영체제 시작 기록
13	Kernel-General, 운영체제 종료 기록
18	Kernel-Boot, 부팅 초기화 작업 완료
20	Kernel-Boot, 부팅 작업 완료
6005	이벤트 로그 서비스 시작(부팅 후 서비스 시작)
6006	이벤트 로그 서비스 종료(부팅 전 서비스 종료)

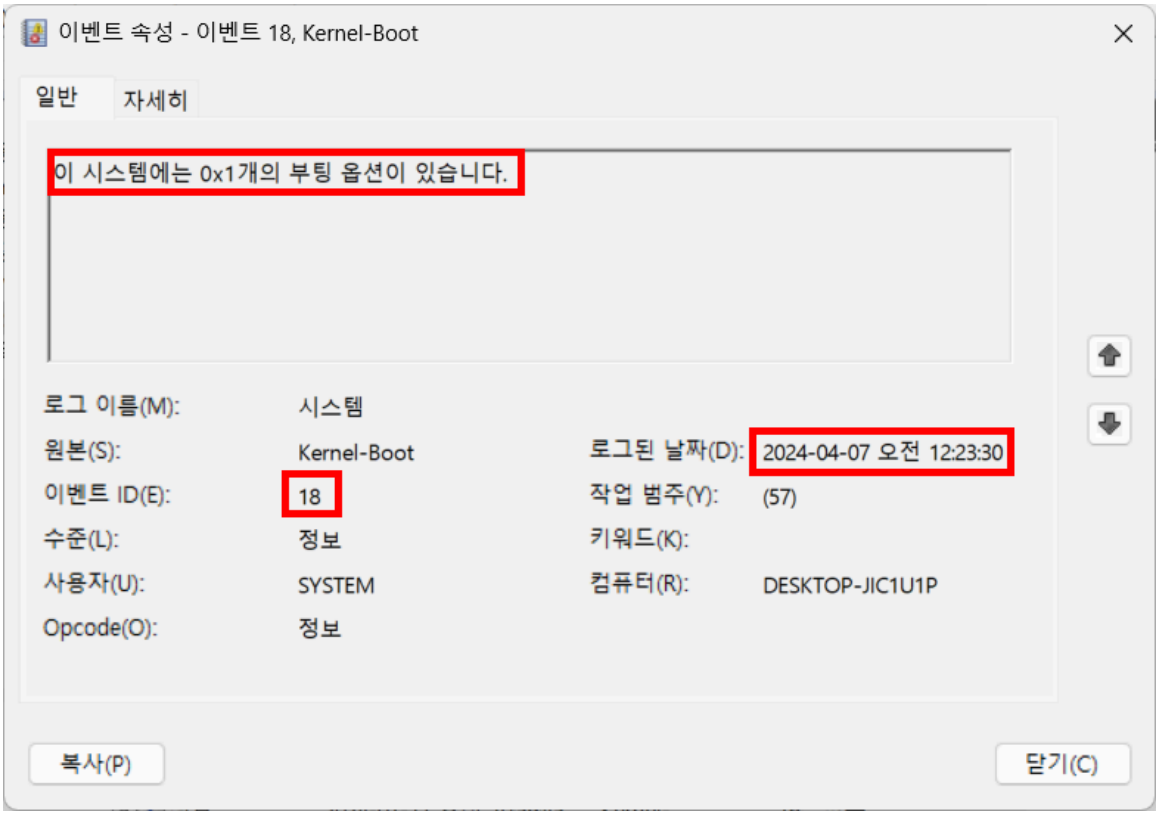
- 이벤트 로그 12, 2024-04-07 00:23:30



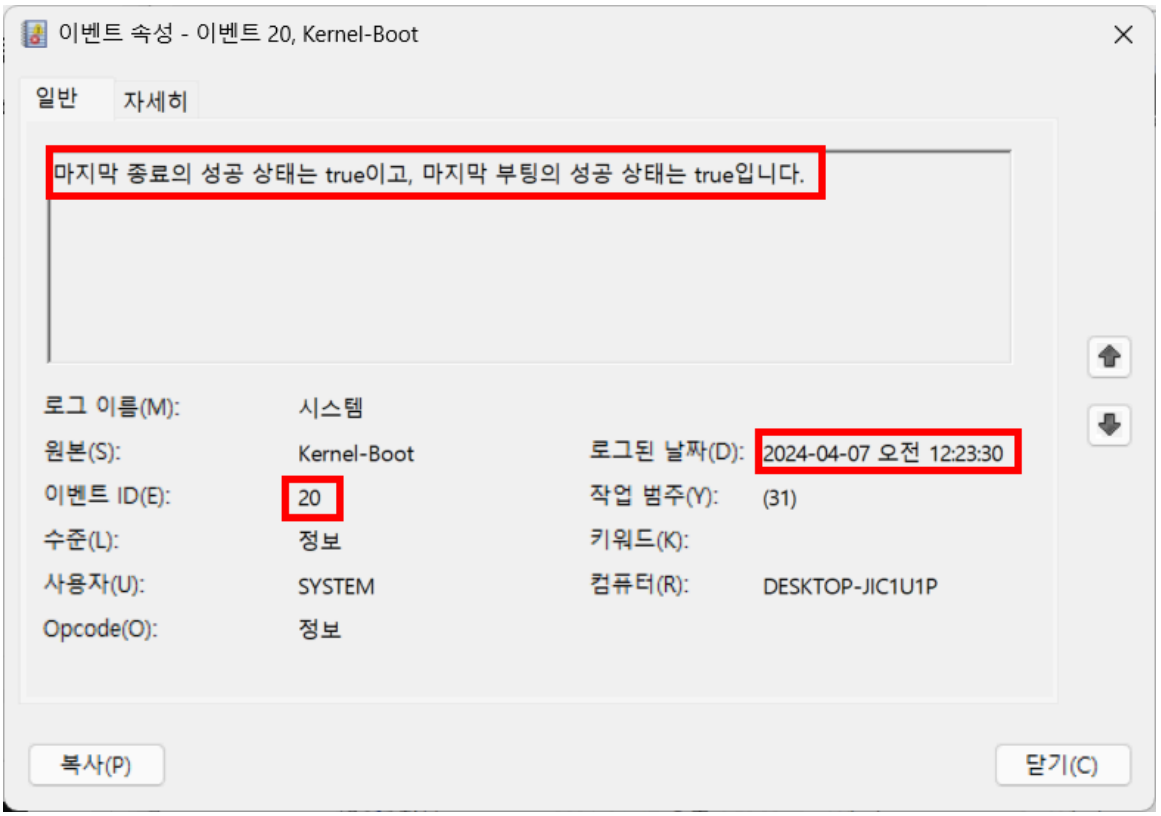
- 이벤트 로그 13, 2024-04-07 00:22:43



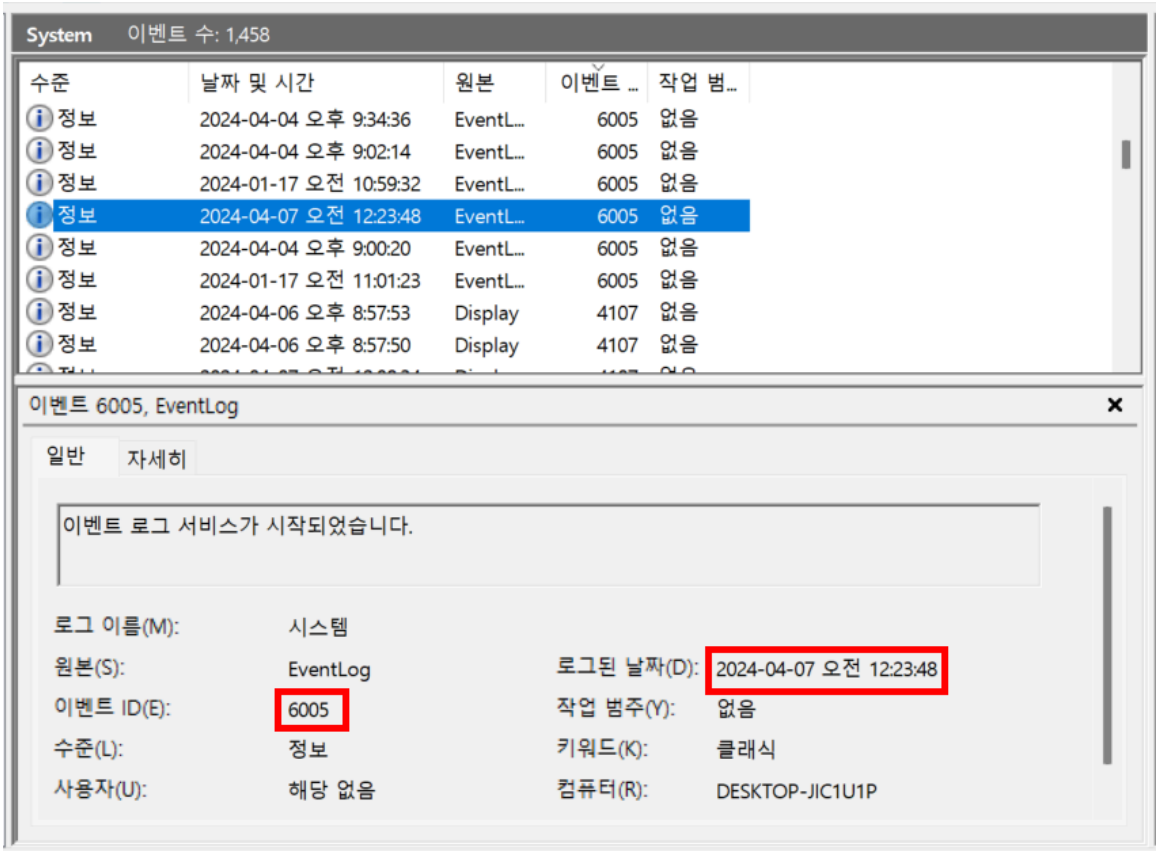
- 이벤트 로그 18 2024-04-07 00:23:30



- 이벤트 로그 20 2024-04-07 00:23:30



- 이벤트 로그 6005, 2024-04-07 00:23:48



- 이벤트 로그 6006, 2024-04-07 00:22:33

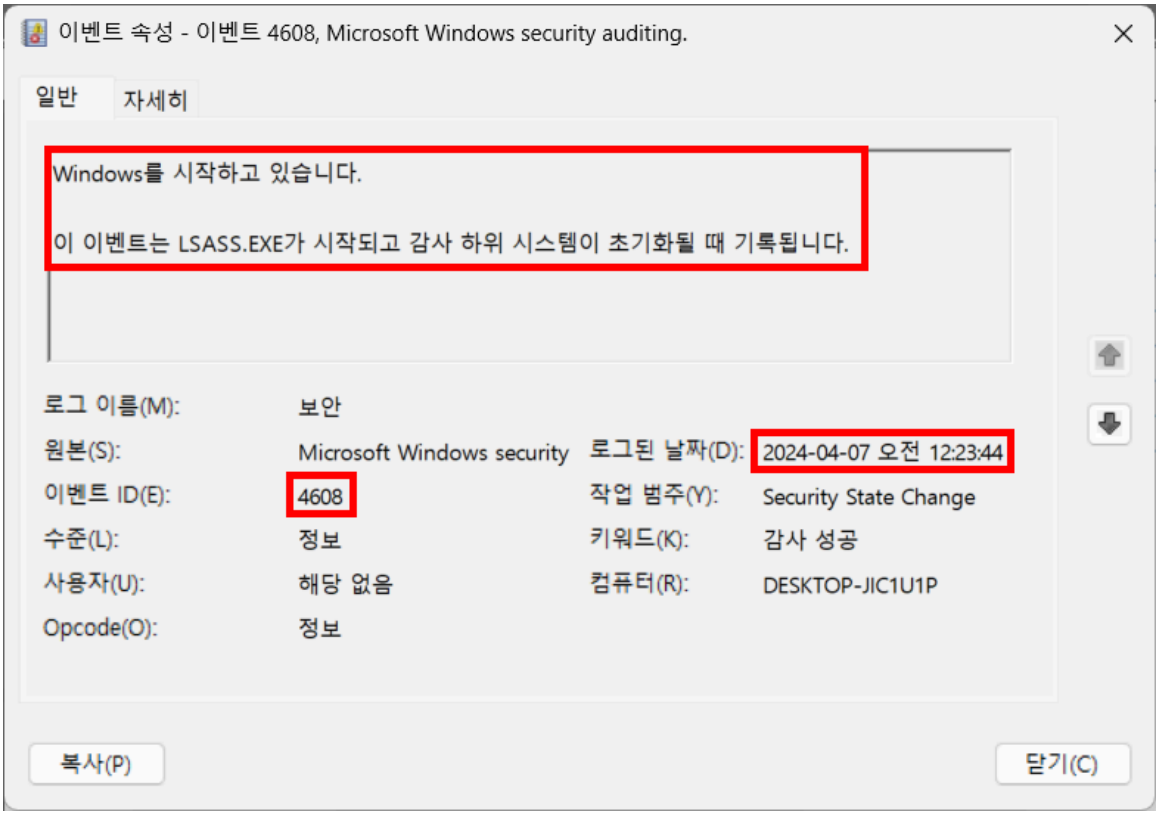
⇒ System 로그의 시간은 정답과 일치하지 않음. 이에 따라 보안 로그 분석 시도

<Security,evtx>

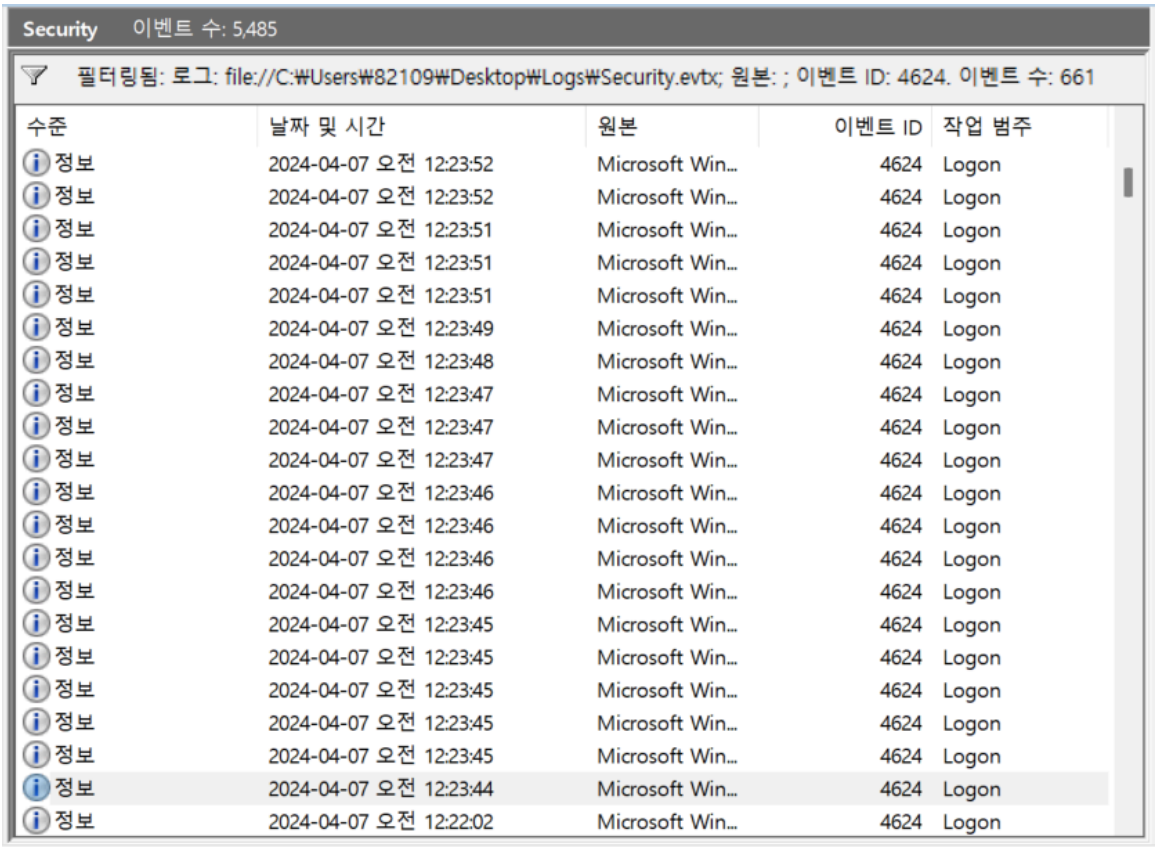
- 부팅 관련 이벤트 ID

4608	시스템 시작(부팅 후 보안 로그 활성화)
4624	계정 로그온 성공(부팅 후 최초 로그인)

- 이벤트 로그 4608, 2024-04-07 00:23:44



- 이벤트 로그 4624, 로그온 이벤트가 매우 많아 마지막 부팅 시점을 특정하기 어려워 판단 불가



Security 이벤트 수: 5,485

필터링됨: 로그: file://C:₩Users₩82109₩Desktop₩Logs₩Security.evtx; 원본: ; 이벤트 ID: 4624. 이벤트 수: 661

수준	날짜 및 시간	원본	이벤트 ID	작업 범주
정보	2024-04-07 오전 12:23:52	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:52	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:51	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:51	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:51	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:49	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:48	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:47	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:47	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:47	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:46	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:46	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:46	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:46	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:45	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:45	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:45	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:45	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:45	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:23:44	Microsoft Win...	4624	Logon
정보	2024-04-07 오전 12:22:02	Microsoft Win...	4624	Logon

- 시스템 시작 시간 중 가장 최근 시간을 마지막 부팅 시간으로 간주
- 즉, **2024-04-07 00:23:44**
- FLAG 형식으로는, DH{2024_04_07_00_23_44}

- System 로그뿐만 아니라 Security 로그 이벤트도 반드시 검토해야 함을 확인함!!

FLAG

DH{2024_04_07_00_23_44}