

# boot time

## Description

당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.  
주어진 이미지의 이벤트 로그를 분석하여, 해당 PC가 마지막으로 부팅된 시간을 구해주세요.

FLAG = DH{yyyy\_MM-dd\_hh\_mm\_ss}  
yy, MM, dd, hh, mm, ss는 시간을 표현하는 방식으로 각각 연, 월, 일, 시, 분, 초를 나타냅니다.  
시간은 UTC+9를 기준으로 합니다.

## 사용한 도구

FTK Imager, Event Viewer

## Background

### Event Log

- 윈도우에서 발생하는 HW, SW 및 시스템 문제에 대한 다양한 이벤트들이 기록
- Windows 운영체제에서 발생 된 특정 이벤트를 추적하여 파티션 삭제, USB 접근 등 다양한 증거 수집 가능
- 기본 경로: `C:\Windows\System32\winevt\Logs`

응용 프로그램 로그	윈도우에서 API를 사용하는 응용 프로그램이 중요한 이벤트를 알리고, 활동 내역을 기록
시스템 로그	윈도우의 시스템 운영과 유지에 관련된 대부분의 정보, 주로 하드웨어 장치나 드라이버 오류 정보 및 동작 여부 등이 기록
보안 로그	시스템 로그인, 파일 접근, 인증, 계정 생성, 권한 사용 등에 따른 이벤트와 보안과 관련된 항목들이 저장, 어떤 파일에 접근했는지에 대한 정보

### 주요 Eventlog 파일

Application.evtx	소프트웨어를 비롯해서 사용자의 어플리케이션의 이벤트를 기록
Security.evtx	보안 관련된 이벤트 로그, Windows 로그인, 네트워크 등 다양한 로그 기록
System.evtx	서비스 실행 여부나 파일 시스템, 디바이스 오류 등의 정보 기록

Setup.evtx	어플리케이션 설치 시 발생하는 이벤트를 기록, 프로그램이 잘 설치되었는지, 호환성 정보 기록
------------	---

- 레지스트리에 기록되는 Eventlog 경로: `HKLM\SYSTEM\CurrnetControlSet\Services\Eventlog`

## Event ID

Window 부팅 관련 이벤트 ID

- System

6005	이벤트 로그 서비스 시작, 부팅 시 기록
6006	정상적인 시스템 종료 시 기록
6008	비정상적인 시스템 종료 시 기록
6009	부팅 시 OS 버전, 빌드 번호, 서비스팩 수준 그리고 기타 시스템 관련 정보 기록
4624	계정 로그인
4647	계정 로그아웃

- Security

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx?i=j> : 여기서 Security 관련 이벤트 ID 확인 가능

4608	윈도우 시스템 부팅
4609	윈도우 shutting down

## 시스템 로그의 eid 6005와 시큐리티 로그의 eid 4608의 차이

System 로그의 Event ID 6005:

- Windows 시스템의 시작을 알리는 이벤트
- Windows 운영 체제가 부팅될 때 시스템 로그 서비스가 시작되었음을 기록
- 보통 시스템이 정상적으로 부팅되었는지 확인하기 위해 사용
- 주로 시스템의 시작 시간과 운영 상태를 파악할 때 사용

Security 로그의 Event ID 4608:

- Windows 시스템의 보안 로그 초기화를 알리는 이벤트
- 시스템 부팅 후 보안 설정이 초기화되는 시점을 기록
- 보안 관련 이벤트 로깅이 시작된다는 의미, 시스템이 부팅되거나 재시작될 때 나타납니다.

- 보안 측면에서 시스템이 재시작된 시점을 파악하는 데 유용하며, 보안 로그 모니터링의 기점으로 사용될 수 있음.

## 1. FTK Imager에서 C:\Windows\System32\winevt\Logs 파일 추출

## 2. Event Viewer를 활용하여 System.evtx, Security.evtx 확인

- Security.evtx

수준	날짜 및 시간	원본	이벤트 ...	작업 범...
정보	2024-04-07 오전 12:23:45	Micros...	4624	Logon
정보	2024-04-07 오전 12:23:45	Micros...	4648	Logon
정보	2024-04-07 오전 12:23:45	Micros...	4624	Logon
정보	2024-04-07 오전 12:23:45	Micros...	4648	Logon
정보	2024-04-07 오전 12:23:45	Micros...	4672	Special ...
정보	2024-04-07 오전 12:23:45	Micros...	4624	Logon
정보	2024-04-07 오전 12:23:45	Micros...	4902	Audit P...
정보	2024-04-07 오전 12:23:44	Micros...	4624	Logon
정보	2024-04-07 오전 12:23:44	Micros...	4608	Securit...
정보	2024-04-07 오전 12:23:44	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:44	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:44	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:43	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:43	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:43	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:43	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:42	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:39	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:39	Micros...	4688	Process...
정보	2024-04-07 오전 12:23:39	Micros...	4826	Other ...
정보	2024-04-07 오전 12:23:39	Micros...	4696	Process...

Security.evtx 에서 Event ID 가 4608이고 가장 최근에 실행된 이벤트 로그를 찾았다.



이벤트 ID 와 로그된 날짜를 확인할 수 있었다.

- System.evtx

System 이벤트 수: 1,458					
필터링됨: 로그: file://C:\Users\User\Desktop\Logs\System.evtx; 원본: ; 이벤트 ID: 6005. 이벤트 수: 9					
수준	날짜 및 시간	원본	이벤트 ID	작업 범주	
정보	2024-04-07 오전 12:23:48	EventLog	6005	없음	
정보	2024-04-04 오후 9:40:00	EventLog	6005	없음	
정보	2024-04-04 오후 9:34:36	EventLog	6005	없음	
정보	2024-04-04 오후 9:02:14	EventLog	6005	없음	
정보	2024-04-04 오후 9:00:20	EventLog	6005	없음	
정보	2024-04-04 오후 8:59:55	EventLog	6005	없음	
정보	2024-01-17 오전 11:18:36	EventLog	6005	없음	
정보	2024-01-17 오전 11:01:23	EventLog	6005	없음	
정보	2024-01-17 오전 10:59:32	EventLog	6005	없음	

이번엔 로그 필터링 기능을 활용해서 이벤트 ID가 6005인 로그를 필터링하여 확인해보았다.

일반

자세히

이벤트 로그 서비스가 시작되었습니다.

로그 이름(M): 시스템

원본(S): EventLog

이벤트 ID(E): 6005

수준(L): 정보

사용자(U): 해당 없음

Opcode(O): 정보

로그된 날짜(D): 2024-04-07 오전 12:23:48

작업 범주(V): 없음

키워드(K): 클래식

컴퓨터(R): DESKTOP-JIC1U1P

복사(P)

닫기(C)

마찬가지로 이벤트 ID 와 로그된 날짜를 확인할 수 있었다.

Security.evtx의 시간이 4초가량 더 빠른 것을 확인 가능하다

## **FLAG**

DH{2024\_04\_07\_00\_23\_44}

→ 처음엔 12로 했는데 실패해서 00으로 재시도 하였다.