윈도우 이벤트 로그 기반 PC 비정상 종료 분석 및 활용방안

김하영[1], 박현민[2], 김기범[3]
성균관대학교 일반대학원 과학수사학과 [1](석사과정), [2](박사과정), [3](교수)
hayoung1004@skku.edu, hmhm@skku.edu, freekgb02@gmail.com

Analysis of Unexpected Shutdown Based on Windows Event Log(EVTX) and its Applications in forensic

Ha-Young Kim[1], Hyeon-Min Park[2], Gi-Bum Kim[3]
Dept. of Forensic Science, SungKyunKwan University

요 약

이벤트 로그(Event Log)는 윈도우 운영체제에서 시스템 로그를 기록하는 형식으로 시스템 운영에 대한 정보를 체계적으로 관리한다. 이벤트는 시스템 자체 또는 사용자의 특정 행위로 인해 발생할 수 있고, 그러한 이벤트 로그는 시스템의 시작과 종료뿐만 아니라 기업 보안 감사, 악성코드 탐지 등 행위의 근거로 사용될 수 있다. 본 논문에서는 PC 종료 관련 실험을 통해 이벤트 로그와 ID를 분석하였다. 분석 결과를 통해 PC의 정상 및 비정상 종료 여부를 판단하여, 현장 압수·수색 시 해당 저장매체에 대해 선별압수·매체압수의 해당 여부 식별이 가능하다. 본 연구는 현장수사관이 디지털증거 압수·수색 시 절차적 적법성과 증거능력 확보의 근거 활용에 기여할 수 있다.

1. 서론

디지털증거의 압수 시, 형사소송법 제106조 제3항에 따라 원칙적으로 선별된 전자정보만 출력·복제가 가능하지만, 불가능하거나 곤란한 경우로 인정되면 정보저장매체 등을 압수할 수 있다.

최근 대법원 판결 사건 중 압수·수색 과정에서 PC를 구동하여 전자정보를 탐색하던 중 해당 PC에서 '퍽'소리가 나면서 전원이 꺼지는 사태가 발생하여, 검찰 측이 임의제출을 요청한 바 있다. 이는 PC의 '비정상 종료'를 근거로 선별압수가 곤란하여 임의제출을 요청하였다고 볼 수 있다.[1] 디지털증거 압수·수색 과정에서 PC의 비정상 종료가 발생하였을 때, 선별된 전자정보만을 출력·복제하여 압수가 곤란한 예외적인 경우로 보아 매체압수 허용여부에 대한 판단 기준 마련이 필요하다. 따라서, 디지털증거의 압수원칙을 살펴보고, 선별압수와 매체압수를 구분할 수 있는 적법한 근거를 위해 Windows 10 운영체제에서 비정상 종료 관련 이벤트 로그를 분석하여 현장수사 시 활용할 수 있는 방안을 제안한다.

2. 디지털증거의 압수원칙과 PC 비정상 종료

2.1. 선별적 압수원칙과 예외

디지털증거의 압수·수색과 관련하여 형사소송법 제106조 제3항에서 규정하고 있는 선별적 압수의 원칙에 대해 대법원 2015.7.16. 자 2011모 1893 판결에서는 「압수할 정보의 범위를 정하여 출력·복제하여 제출받아야 하고, 이러한 방법이 불가능하거나 현저히 곤란하다고 인정되는 때에 예외로 저장매체 등을 압수할 수 있다.」고 판시하고 있다. 예외적인 경우에는 정보저장매체 자체를 압수하는 것이 가능하다는 의미이다.

대검찰청의 '디지털 증거 수집 및 분석 규정' 에서는 예외적으로 「기기 또는 디지털 자료가 손상, 훼손될 우려가 있을 때에는 정보처리시스템 전부를 압수할 수 있다.」고 명시되어 있다.(제2장 제9조 1항) 디지털기기를 압수·수색·검증하거나 디지털 자료를 수집할 경우 대상 정보처리시스템으로부터 사용자를 격리하여 시스템 강제종료 등 임의적인 조작행위를 방지하여야 한다.(제10조 1항)

이처럼 안티포렌식의 일환으로 PC를 강제종료하는 행위를 방지하기 위해 김용호[2] 등은 전자정보 및 정보저장매체를 수집하는 현장에서 사용자의 대상 정보시스템 및 운영 장치에 대한 전원 차단 등 임의적 조작행위 방지를 위한 통제가 필요하며, 네트워크

에 연결된 정보처리시스템은 연결 케이블 차단을 통해 임의로 삭제하는 것을 방지해야 한다고 하였다.

최근 디지털매체 압수 및 반출을 위해 검찰 측에서 임의적 행위를 했다는 의혹과 함께 PC 압수절차에 대한 논의[3]가 PC 정상·비정상 종료의 여부로 이루어졌다. 검찰은 PC의 비정상 종료를 사유로 임의제출을 요청하였으며, 이벤트 로그를 기반으로 증빙하였다.[4] 해당 포렌식 결과에 대해 검찰과 변호인단, 양측 주장이 나뉘게 되면서 위법수집증거 여부에 대한 포렌식 관점에서의 검증이 필요할 것으로 보인다.

2.2. 이벤트 로그와 PC 종료 유형

2.2.1. 윈도우 이벤트 로그(EVTX)

윈도우 이벤트 로그(Windows Event Log)는 윈도우 운영체제의 시스템 로그 저장 방식으로, 시스템과 애플리케이션의 작동 상태 및 사용자의 행위에 따라 발생하는 모든 동작에 대한 기록을 'EVTX(Windows XML Event Log)' 파일 형식으로 관리하는 기능이다.[5] 시스템 관리자는 에러 발생 시 이러한 로그를 확인하여 원인을 찾거나 주기적인 확인을 통해 디스크 손상과 같은 문제를 미리 대비할 수 있다.[6] 각 로그에서는 메타데이터인 로그 이름, 원본, 키워드, 로그된 날짜, 이벤트 ID, 작업 범주, 수준 등과 이벤트 메시지로 구성되어 있다.[5]

Windows 10 운영체제에서 이벤트 로그(Event Log)는 이벤트 뷰어(Event Viewer)를 통해 로컬 컴퓨터에서 확인할 수 있다. 이벤트 뷰어를 통해 이벤트 ID를 확인하여 PC의 종료 유형 구분이 가능하다. 이벤트 로그는 'Windows 로그'와 '응용 프로그램 및 서비스 로그'로 구성되어 있으며, 하위 구조에는 각 로그 파일의 종류가 트리 구조로 구성되어 있다.

PC의 종료 관련 로그는 이벤트 뷰어를 통해서 확인할 경우 Windows 로그 내 System 로그에서 확인 가능하며, 이벤트 파일인 System.evtx를 통해서도 확인할 수 있다.[5] PC의 종료 관련 로그 중 이벤트 ID를 통해 정상 및 비정상 종료를 구분할 수 있다.

<표 1> PC 종료 관련 Event Log·ID

EventLog	Event ID	Contents
System	41	시스템의 비정상적 종료 후 다시 시작
	42	시스템이 절전 모드로 전환
	1001	PC 오류 검사 후 다시 시작
	1074	PC 전원 종료/다시 시작을 수행
	6008	시스템의 예기치 못한 종료

2.2.2. PC 종료(Shutdown) 유형

마이크로소프트의 공식 기술 문서[7]에 따르면 윈도우 PC에서 종료(Shutdown)는 크게 두 가지로 구분할 수 있으며 ①정상 종료(Clean/Expected Shutdown)와 ②비정상 종료(Dirty/Unexpected Shutdown)가 있다. 종료와 관련된 이벤트 로그는 다양하게 존재하며, 종료가 진행되는 동안 기록되는 이벤트들도 종료 관련 이벤트 로그로 구분할 수 있다.

전형적인 '정상 종료'의 경우라면 이벤트 ID 1074를 확인할 수 있다. 이벤트 ID 1074는 사용자가 시작메뉴에서 시스템 종료 혹은 다시 시작을 선택, Ctrl+Alt+Delete를 누른 다음 종료를 선택하여 재시작·종료를 진행한 경우에 기록된다.[8] '절전 모드' 또한 정상 종료의 유형으로 볼 수 있으며, 이벤트 ID 42가 기록된다. 절전 모드 전환 이유에 따라, 임의전환·자동전환 여부 확인이 가능하다.[5]

시스템이 예기치 않게 종료된 경우를 '비정상 종료'로 정의할 수 있는데, 이때 로깅되는 이벤트 로그의 ID 값은 6008이다. 비정상적으로 종료된 후 다시 시작할 때 이벤트 ID 41이 기록된다. 이벤트 ID 6008의 경우 레지스트리 값에 의해서도 기록이 된다. 정상 종료가 되면 레지스트리의 LastAliveStamp 값이 삭제되는데, 비정상 종료의 경우 해당 레지스트리 값이 존재하게 되어 이를 통해 비정상 종료가 되었음을 판단하여 이벤트 ID 6008이 기록된다.

비정상 종료를 유발하는 유형을 ①전력차단, ②시스템 오류 생성, ③강제종료 명령, ④기타 파손 유도 총 4가지로 분류된다.

<표 2> PC 비정상 종료 유발 유형

no	분류	세부유형	
1	전력 차단	전원 코드 뽑기	
		하드디스크 제거	
2	시스템 오류 생성	블루 스크린 오류 유도	
		바이러스	
3	강제종료 명령	전원 버튼 짧게 누르기	
		전원 버튼 길게 누르기	
		원격 조정 종료	
4	기타 파손 유도	물리적 기기 파손	손상 경도
		액체에 의한 파손	물
			음료
			소금물
		자기장 활용 파손	세기 변화
			디가우징

세부 유형 중 하드디스크 제거의 행위는 부트로더가 있는 하드디스크 제거 시 비정상 종료가 가능하나, 부트로더가 없는 하드디스크의 경우 PC 전원이 정상적으로 유지된다. 또한, 바이러스 감염 및 액체·자기장에 의한 파손 등 하드디스크 복구가 불가능할 경우 이벤트 로그 확인이 불가능하다.

3. PC 비정상 종료 실험

3.1. 실험 설계

본 연구에서는 Windows 10이 설치된 로컬 PC 2대에서 실험환경을 구성하였다. 비정상 종료 이벤트 로그 중 이벤트 ID 6008, 41을 얻기 위해 결과 확인이 불가능한 비정상 종료 유형을 제외한 ①전력차단, ②시스템 오류 생성, ③강제종료 명령 총 3가지 유형으로 실험을 진행하였다.

PC가 실행되고 있는 환경에서 전원 코드 뽑기, 전원 버튼 누르기, 시스템 오류 생성 등 강제종료 행위를 진행하였으며, 종료 후 재실행된 환경에 남겨진 이벤트 로그를 이벤트 뷰어(Event Viewer)를 통해 확인하였다.

블루 스크린을 유도하기 위해 Bang.exe 실행파일을 사용하였고, 원격 조정 종료 시 TeamViewer 프로그램을 사용하였다. 실험 종료 후 전형적인 비정상 종료 이벤트 ID 6008, 41 기록을 확인하였다. 이벤트 ID 41을 통해 '비정상 종료'의 유형을 이벤트 뷰어에서 'PowerButtonTimestamp'와 'BugCheckCode'의 값을 확인하여 세부적으로 구분할 수 있다.

<표 3> PC 비정상 종료 실험 설계

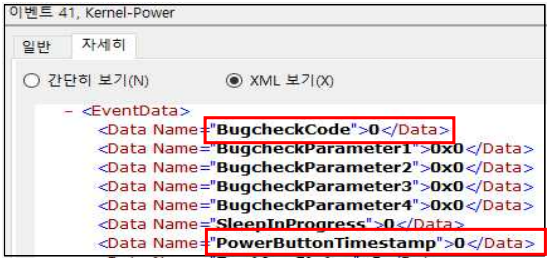
no	분류	세부유형
1	전력 차단	전원 코드 뽑기
		하드디스크 제거
2	시스템 오류 생성	블루 스크린 오류 유도
3	강제종료 명령	전원 버튼 짧게 누르기
		전원 버튼 길게(5초) 누르기
		원격 조정 종료

3.2. 실험 결과 및 분석

3.2.1. 전력 차단

PC의 비정상 종료와 관련된 이벤트 로그 분석을 위해 사용자가 임의로 조작이 가능한 유형을 가정하여 실험을 진행하였다. 전력 차단을 유발하는 유형에서는 전원 코드를 뽑는 실험과 하드디스크를 제거해보는 실험을 진행하였다.

전원 코드를 뽑는 경우, 비정상 종료가 진행되며 이벤트 ID 6008, 41이 기록되었다. 특히 이벤트 ID 41을 자세히 살펴본 결과, PowerButtonTimestamp 값과 BugCheckCode 값 모두 0인 것을 확인하였다.



(그림 1) 이벤트 41, 전원 코드 뽑기

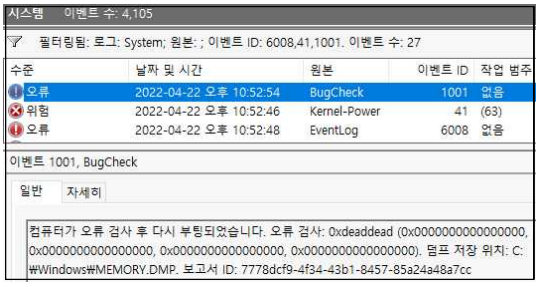
<표 4> 전력 차단 실험 결과

no \ 분류	전력 차단			
	세부유형	실험 PC	실험 회차	Event ID
1	전원 코드 뽑기	PC1	5	6008 / 41
		PC2	5	6008 / 41
2	하드디스크 제거	PC1	3	6008 / 41
		PC2	3	6008 / 41

3.2.2. 시스템 오류 생성

블루 스크린 오류를 유도하기 위해 VMware 16을 통해 가상환경에서 강제적으로 크래시를 발생시키는 'Bang.exe' 프로그램을 사용하였다.

해당 프로그램을 실행시키면, 블루 스크린이 발생하며 비정상 종료가 되어 이벤트 ID 6008, 41가 기록되었다. 다만, 추가적으로 블루 스크린으로 인한 종료 관련 이벤트 ID 1001이 기록된 것을 확인하였다. 특히 이벤트 뷰어를 통해 확인한 버그 검사의 값은 '0xdeaddead'로, 마이크로소프트 기술 문서에 의하면 해당 값은 수동으로 크래시가 발생했음을 나타내는 값인 것을 확인하였다.[9]



(그림 2) 이벤트 1001, 블루 스크린 오류

이벤트 ID 41에서는 블루 스크린 오류로 인해 종료된 경우, PowerButtonTimestamp 값은 0, BugCheckCode 값은 0이 아닌 것을 확인할 수 있다.

<표 5> 시스템 오류 생성 실험 결과

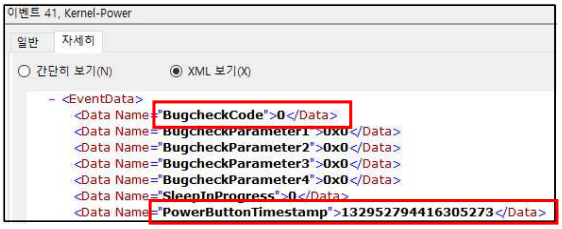
no \ 분류	시스템 오류 생성			
	세부유형	실험 PC	실험 회차	Event ID
1	블루 스크린 오류 유도	PC1	5	6008 / 41
				1001
		PC2	5	6008 / 41
				1001

3.2.3. 강제종료 명령

전원 버튼을 짧게 눌러서 종료한 후 다시 시작한 경우에는 이벤트 ID 1074가 기록되었다. 반면 전원 버튼을 길게(5초 이상) 눌러서 종료한 경우 BugCheckCode 값은 0으로 기록되었지만, PowerButton Timestamp 값이 0이 아닌 것으로 기록되었다.

사용자 환경에서 종료하는 과정과 같은 원격을 이용한 종료의 경우 이벤트 ID 1074 혹은 42가 기록

되어 '정상 종료'와 같이 기록된 것이 확인되었다.



(그림 3) 이벤트 41, 전원 버튼 길게 누르기

<표 6> 강제종료 명령 실험 결과

분류 / no	강제종료 명령			
	세부유형	실험 PC	실험 회차	Event ID
1	전원 버튼 짧게 누르기	PC1	1	1074
			4	42
		PC2	2	1074
			2	42
			1	6008 / 41
2	전원 버튼 길게(4초) 누르기	PC1	5	6008 / 41
		PC2	5	6008 / 41
3	원격 조정 종료	PC1	2	1074
			3	42
		PC2	5	42

3.3. 요약 및 한계

실험 설계 시 이벤트 ID 6008, 41은 비정상 종료로, 이벤트 ID 1074는 정상 종료로 구분하였다. 비정상 종료 유형 중 시스템 오류 생성 행위로 구분한 전원버튼을 짧게 누르는 행위와 원격 조정 종료는 정상 종료를 나타내는 행위는 이벤트 ID 1074가 기록되었다.

이 결과로, 전원 버튼을 눌러 강제적으로 종료를 할 경우 비정상 종료로 구분이 가능한지 추가 연구가 필요하다. 이벤트 ID가 1074가 기록된 유형의 경우가 비정상 종료와 정상종료의 구분이 불가능하다면 선별압수의 예외에 해당하지 않는 정상 종료로 판단해야 한다는 한계가 존재한다.

<표 7> PC 비정상 종료 실험 결과

no	분류	세부유형	Event ID
1	전력 차단	전원 코드 뽑기	6008 / 41
		하드디스크 제거	6008 / 41
2	시스템 오류 생성	블루 스크린 오류 유도	6008 / 41
			1001
3	강제종료 명령	전원 버튼 짧게 누르기	1074
			42
		전원 버튼 길게(4초) 누르기	6008 / 41
		원격 조정 종료	1074
			42

4. 결론

본 논문은 이벤트 ID를 통해 비정상 종료의 유형을 사용자의 행위를 기준으로 구분하여 실험을 설계하고 분석하여, 디지털증거 압수·수색 시 선별압수 및 매체압수의 구분기준, 증거능력 확보 등에 활용할 수 있는 근거를 제시하였다.

본 연구의 결과로 ①전원 코드 뽑기, ② 블루 스크린 오류 유도, ③전원 버튼 길게 누르기는 시스템 비정상 종료로 구분되었다. 그러나, 전원 버튼 짧게 누르기, 원격 조정 종료는 정상 종료로 구분되었고 하드디스크 제거, 물 뿌리기는 변수가 존재 해 환경마다 이벤트 값이 다르며, 바이러스 물리적 파손 등은 실험 결과를 확인할 수 없다. 이는 현장 수사 시 고려하여 활용 전략을 수립할 필요가 있다.

향후 본 연구를 토대로 바이러스 감염, 기타 파손 유도 세부 행위 등을 세분화하여 추가 연구해야 할 필요가 있으며, 현장수사 시 디지털증거 압수 과정에서 비정상 종료뿐만 아니라, 강제종료 행위를 구분할 수 있는 활용 방안의 근거가 되기를 기대한다.

참고문헌

[1] Supreme Court, "Decision 2021도11170", Jan 27, 2022

[2] YH Kim et. al "The problem point and improvement program of the scene search and seizure of digital evidence at practical affairs', Journal of the Korea Institute of Information and Communication Engineering", Vol.17, No.11, pp.2595-2601, 2013

[3] Il-Seok Go, thebriefing, "'1호 PC 비정상종료'?... 상상을 뛰어넘는 검찰의 기만행위', 2021

[4] Il-Seok Go, Jihoon-Park, "대한민국을 뒤흔든 정치검찰의 사기극 표창장", 책비, 2021

[5] SR Kang et. al, "Study on Windows Event Log-Based Corporate Security Audit and Malware Detection",Journal of The Korea Institute of Information Security & Cryptology 28(3), pp.591-603, 2018

[6] Microsoft Developer Network, [Internet] https://msdn.microsoft.com/ko-kr/library/windows/desktop/aa363632(v=vs.85).aspx

[7] Microsoft, "Dirty Shutdown and Event log, 6008", 2008

[8] MangeEngine ADAudid Plus, "Windows Server Event: 1074", [Internet] https://www.manageengine.com/products/active-directory-audit/kb/system-events/event-id-1074.html?event-log-library

[9] Microsoft, "Bug Check 0xDEADDEAD: MANUALLY_INITIATED_CRASH1", [Internet] https://docs.microsoft.com/ko-kr/windows-hardware/drivers/debugger/bug-check-0xdeaddead--manually-initiated-crash1