한국사물인터넷학회논문지 Vol. 5, No. 1, pp. 35-39, 2019 https://doi.org/10.20465/KIOTS.2019.5.1.035

사물인터넷 환경에서 삭제된 파일의 목록을 이용한 포렌식 분석 간편화

임정현[1], 이근호[2*]
[1]백석대학교 정보통신학부, [2]백석대학교 정보통신학부

Simplified Forensic Analysis Using List of Deleted Files in IoT Envrionment

Jeong-Hyeon Lim[1], Keun-Ho Lee[2*]
[1]Student, Div. of Information Communication, BaekSeok University
[2]Professor, Div. of Information Communication, BaekSeok University

요 약 급격한 정보화 사회로의 발달로 사람들은 디지털기기의 사용이 급격히 증가하면서 이를 분석하는 기술에 대한 중요성이 증가하였다. 디지털 증거는 사용자가 삭제하더라도 Prefetch, Recent, Registry, Event Log 등 여러 곳에 산재되어 저장되는 특성이 있다. 때문에 포렌식 분석관이 초기에 사용자가 이용한 파일들에 대해 완벽한 파악이 어렵다는 단점이 존재한다. 따라서 본 논문에서는 사용자가 직접 삭제한 파일에 대한 정보를 먼저 파악할 수 있도록 RemoveList 폴더가 존재하고, RemoveList에는 AES를 이용하여 삭제된 파일에 대한 정보가 암호화되어 자동 저장되는 방안을 제안하고자 한다. 이를 통하여 분석가가 초기에 사용자의 PC를 파악하는 것이 어렵다는 문제점을 완화할 수 있다는 기대를 할 수 있다.

주제어 : 디지털 포렌식, 디지털 증거, 디지털 파일 사용 흔적

Abstract With the rapid development of the information society, the use of digital devices has increased dramatically and the importance of technology for analyzing them has increased. Digital evidence is stored in many places such as Prefetch, Recent, Registry, and Event Log even if the user has deleted it. Therefore, there is a disadvantage that the forensic analyst can not grasp the files used by the user at the beginning. Therefore, in this paper, we propose a method that the RemoveList folder exists so that the user can grasp the information of the deleted file first, and the information about the deleted file is automatically saved by using AES in RemoveList. Through this, it can be expected that the analyst can alleviate the difficulty of initially grasping the user's PC.

Key Words : Digital Forensics, Digital Evidence, Trace of using digital file

본 논문은 2019년 백석대학교 학술연구에 의하여 지원되었음
*Corresponding Author : 이근호(root1004@bu.ac.kr)
접수일 2019년 4월 18일 수정일 2019년 06월 04일 심사완료일 2019년 06월 27일

1. 서론

정보화 사회로의 급격한 발달로 디지털 기기에 증거나 단서가 저장되는 경우가 증가하였다. 이를 수집하고 분석하기 위해 디지털 포렌식의 중요성이 증가하였다[1]. 디지털 포렌식이란 전자적 특성을 갖는 증거물을 수집하고 분석하며, 보고서를 작성하는 일련의 과정을 의미한다[2]. 현재 컴퓨터 포렌식 증거 분석을 도와주는 도구는 Guidance Software사의 Encase, AccessData사의 Forensic ToolKit이 많이 사용되고 있다[1]. 이들은 PC를 대상으로 분석하는 경우, 무결성 검증을 위해 디스크 이미지를 획득한 후 포렌식 분석도구를 이용하는 것이 일반적이다[2].

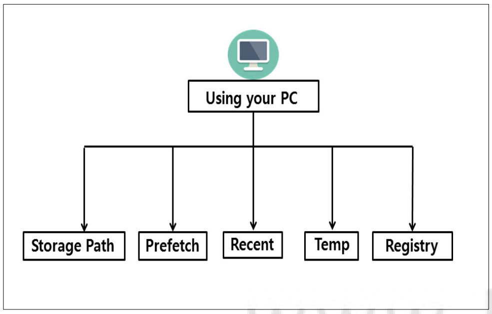
디지털 증거는 많은 양이 동시다발적으로 동일한 시스템 내의 여러 곳에 산재되어 저장된다는 특징이 있다[3]. 따라서 사용자가 다운로드 받은 파일을 삭제했더라도, 흔적이 존재한다. 포렌식 분석관은 PC의 사용자가 어떠한 프로그램을 삭제했는지 초기에 완벽한 파악이 불가능하기 때문에 사용자가 어떠한 파일을 사용했고, 삭제했는지 단시간에 파악할 수 있는 새로운 확인 방식이 필요하다.

본 논문의 구성은 다음과 같다. 2장에서는 사용자가 이용한 파일에 대한 흔적이 어떠한 형식으로 남게 되는지 알아보며, 3장에서는 사용자가 직접 삭제한 파일을 AES를 이용하여 목록화 시키는 제안방법에 대해 알아보고, 4장에서는 이를 이용한 방안의 장점과, 후에 연구해야 할 방향에 대해 논하고자한다.

2. 관련연구

2.1 디지털 파일 저장 경로

사용자가 프로그램을 사용할 경우 다양한 경로에 다양한 확장자로 사용 흔적이 저장된다. [Fig. 1]은 디지털 파일이 저장되는 간단한 경로를 나타낸 그림이다.



[Fig. 1] A list of deleted files

2.2 디지털 파일 사용 흔적

2.2.1 Prefetch

사용자가 인터넷을 사용하거나, 문서작성 프로그램 등을 사용할 경우 Prefetch 폴더에는 확장자가 '*.pf', *.db' 인 파일이 생성된다[4]. 생성된 파일을 통하여 어떠한 프로그램을 사용하였고, 프로그램이 마지막으로 실행된 시간(Last Launch Time)은 언제인지에 대한 리틀 엔디안으로 저장된 정보를 알 수 있다[5]. Prefetch 폴더의 경로는 'C:\Windows\Prefetch' 이다.

2.2.2 Recent

사용자가 최근에 이용한 문서파일, 열어본 이미지 파일, 사용한 폴더 등이 Recent 폴더에 저장된다. 이 폴더는 사용자가 최근에 이용한 파일들을 파악할 수 있다. 경로는 'C:\Users\UserName\AppData\Roaming\Microsoft\Windows\Recent'이며, 파일 확장자는 저장된 확장자다.

2.2.3 Jump Lists

Jump Lists는 Windows7 이후에 만들어졌으며, 해당 응용프로그램이나 내부 엔트리가 제거되었더라도 정보가 남아있어 포렌식 수사에 중요한 부분이다.[6] 이를 이용하여 사용자가 최근에 열어본 파일을 알려주는 최근항목, 사용자가 빈번하게 접근하는 파일을 알려주는 자주 사용하는 항목, 사용자가 사용하기 위해 직접 고정한 항목, 작업에 관한 정보를 알 수 있다[6].

Jump Lists는 크게 두 가지로 구분된다. 첫 번째는 최근항목과 사용자가 고정한 항목을 알 수 있는 '*automaticDestinations-ms' 파일, 두 번째는 자주 사용하는 항목과 작업정보를 알 수 있는 '*.customDestinations-ms' 파일이다[6, 7]. 이 파일의 저장경로는 'C:\Users\Username\AppData\Roaming\Microsoft\Windows\Recent'의 하위폴더로, 폴더명은 AutomaticDestinations, CustomDestinations이다[6].

2.2.4 Temp

Temp 폴더는 임시 폴더로, 문서, 사용자가 이용한 프로그램에 대한 임시파일 등이 Temp에 존재한다. 경로는 'C:\Users\UserName\AppData\Local\Temp'이며, 폴더

에 존재하는 파일의 일부 확장자는 '.tmp'이며, 그 외에 '.log', '.dll' 도 존재한다.

2.2.5 Registry

Registry(이하 레지스트리)는 윈도우 운영체제가 윈도우 계정 로그인, 휴지통, Prefetch, Event Log 등 시스템 운영에 필요한 정보들을 저장해놓은 데이터베이스이다[8]. 레지스트리를 분석하기 위해서는 하이브(Hive)파일의 수집이 필요하며, 레지스트리 분석은 활성 레지스트리 분석과 비활성 레지스트리 분석으로 구분되며, 대부분 비활성을 대상으로 진행된다[9]. <Table 1>은 레지스트리에 대한 정보를 간략하게 구분한 것이다.

〈Table 1〉 Registry Classification[10].

Hive	Explain	
HKEY_CLASSES_ROOT	COM object information registration	
HKEY_CURRENT_USER	Logined user profile Information	
HKEY_LOCAL_MACHINE	SYSTEM	System settings Information
	SOFTWARE	Installed Application Information
	SAM	Connection log of registered account information
HKEY_-USERS	USER_SID	User settings information

레지스트리 분석을 통하여 PC에 연결된 기기(USB 등)의 고유한 Serial Number, 사용한 인터넷 사이트의 URL 정보, 운영체제 관련 정보, 최근에 사용한 문서와 실행파일 정보 등을 알 수 있다. 또한 ShellBag 분석, 시스템 관련 정보 등을 알 수 있다[9].

2.2.6 Event Log

윈도우 이벤트 로그는 로그에 대한 기록을 EVTX(Windows XML Event Log) 파일 형식으로 관리하는 것으로, 확장자는 '*.evtx'이다[11].이벤트는 전역로그(시스템, 보안 등)와 응용 프로그램 및 서비스 로그(디렉터리 서비스 로그 등)가 존재하며, 하나의 이벤트는 원본과 로그된 날짜, 이벤트 ID등이 포함되어있는 메타데이터와 메시지로 구성되어있다[11-13]. 대표적으로 System.evtx 로그에는 서비스 실행, 종료 이력 등을 얻을 수 있고, Application.evtx 로그는 프로그램이 남긴 정보를 통해 어떠한 프로그램이 실행 중이었는지 일부 추정할 수 있다. 그리고 사용자가 PC의 시간을 조작했는지에 대한 여부도 파악할 수 있다. 그리고 OAlerts.evtx에는 Microsoft Office가 동작 중 발생하는 오류, 그 외의 이벤트 등의 Alert가 발생한 경우 기록을 남기며, 이를 통하여 파워포인트나 워드, 엑셀 등의 문서 열람과 수정시도 등 일정 부분을 파악할 수 있다[14].

2.2.7 슬랙 공간

슬랙 공간(Slack Space)이란 저장매체의 물리적 구조와 논리적인 구조의 차이로 발생하는 낭비공간으로, 물리적으로는 할당된 공간이지만 논리적으로는 사용할 수 없는 공간을 의미한다. 이러한 이유로 슬랙 공간을 정보를 은닉시키기 위한 공간, 악성코드를 숨기기 위한 목적으로 사용되기도 하며, 또한 삭제된 파일 조각들을 발견할 수 있는 공간이기도 하다. 따라서 획득한 데이터를 분석하기 전에 슬랙 영역의 존재유무를 확인하는 절차를 포함함으로써 은닉되어있는 영역을 확인해야 한다[15].

2.2.8 브라우저 관련 정보

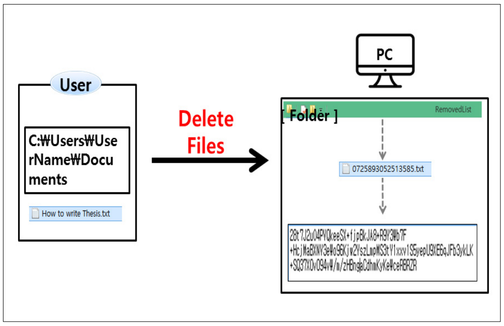
사용자가 인터넷을 사용하여 파일을 다운로드 할 경우 다운로드한 파일이 흔적으로 존재한다. 더불어 파일을 다운로드하지 않아도 사용자가 행했던 행동이 사용자의 PC에 흔적으로 존재한다. 사용자는 크롬(Chrome), 인터넷 익스플로러(Internet Explorer), 파이어폭스(FireFox)등을 사용한다. 브라우저마다, 사용자가 사용하는 운영체제의 버전마다 흔적이 저장되는 경로에 약간의 차이는 존재하지만 임시 인터넷 파일, 쿠키 정보, 방문 히스토리 정보, 플러그인등이 저장된다. 이를 통하여 사이트에 방문한 방문자, 방문 시간, 방문 사이트 등을 알 수 있다. 이와 더불어 사용자의 사이트 방문 패턴 등도 파악할 수 있다.

3. 제안기법

3.1 시스템 설계

사용자가 프로그램이나 파일을 사용할 경우 사용한 흔적이 다양한 경로에 존재하게 된다. 사용자 PC에 대해 포렌식 분석을 진행할 경우, 초기에 사용자가 사용한 파

일이나 프로그램이 무엇인지 정확히 파악하기 어렵다. 따라서 본 논문에서는 이러한 부분을 보완하기 위하여 사용자가 직접 삭제한 파일만을 목록화하여 저장하는 방안을 제안하고자 한다.



[Fig. 2] A list of deleted files

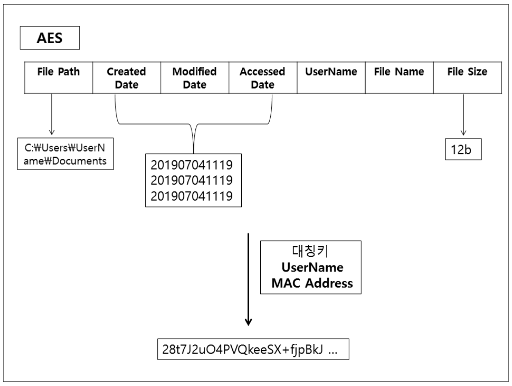
국내 대표적 메신저 어플리케이션인 카카오톡 PC 버전은 대화내용이 모두 사용자의 PC에 저장되며, 저장되는 파일에는 메시지 내용, 메시지를 받은 시간, 송신자 정보 등에 대한 데이터가 저장되어있다[16]. 이러한 방식에 착안하여 대칭키 암호화 알고리즘은 AES(Advanced Encryption Standard)를 이용하여 삭제한 파일을 '*.txt' 형식으로 목록화한다. 다음 [Fig. 2]는 사용자가 파일을 삭제할 경우 시스템 동작에 대한 그림이다.

사용자의 PC에는 'C:\Users\UserName\AppData\Local\Microsoft\Windows' 경로에 'RemoveList' 라는 폴더가 위치한다. 이 폴더는 기본 설정일 때에는 사용자에게 노출되지 않게 기본적으로 보호된 운영체제 파일로써 숨겨진 파일로 설정되어있다. 사용자가 문서 파일이나 프로그램 등을 직접 삭제할 경우 삭제한 파일에 대한 정보는 '*.txt' 파일 형태로 저장되며, 파일명은 임의의 숫자로 정해진다.

3.2 시스템 구조

사용자가 삭제한 파일을 AES를 이용하여 암호화 되는 과정은 [Fig. 3]과 같다.

사용자가 디지털 파일을 삭제하면 파일명, 파일 경로, 파일 크기, 만든 날짜, 수정한 날짜, 액세스한 날짜, 사용자 이름 전체가 AES 알고리즘을 이용하여 암호화되어 '*.txt' 파일로 저장된다. 이때 AES 알고리즘에 사용되는 키 값은 PC의 사용자 이름과 고유한 정보인 MAC(Media Access Control Address) 주소를 이용한다.



[Fig. 3] Encrypt the deleted file using AES

이렇게 하여 RemoveList에 저장된 파일들을 포렌식 분석 시 초기에 분석하여 사용자가 삭제한 파일들에 대한 정보를 가장 먼저 얻은 후, 대략적인 구조를 잡은 뒤 세부적인 포렌식 분석을 시작할 수 있다.

4. 결론

포렌식 분석관이나 일반 사용자가 본격적인 분석 전 사용자의 이름과 고유한 MAC주소를 획득한다. 그 다음 RemoveList 폴더 안의 파일들을 보고 해당 파일이 만들어진 시간을 파악할 수 있다. 대략적인 시간을 파악한 후, 사용자의 이름과 MAC 주소로 암호화 된 문장을 복호화한다. 복호화하면 사용자가 삭제한 파일과 파일이 존재했던 경로, 만들어진 시간과 수정된 시간들을 파악할 수 있다. 이를 통하여 분석하고자하는 시스템을 초기에 대략적으로 파악할 수 있기 때문에 좀 더 빠른 분석이 가능하다.

본 논문에서는 사용자가 디지털 기기를 사용할 경우 어떠한 사용 흔적이 사용자의 PC에 남는지 살펴보았으며, 좀 더 효율적인 포렌식 분석을 위하여 사용자가 직접 삭제한 파일을 중심으로 목록화하여, 지정된 폴더에 대칭키 암호 알고리즘인 AES를 사용하여 텍스트파일 형식으로 저장되는 방안을 제안하였다. 향후 삭제된 파일의 목록이 대량화 되었을 때의 대응방안과, 사용자의 이름과 MAC 주소의 유출 시 복호화가 쉽게 되는 문제에 대한 연구가 필요하다.

REFERENCES

[1] I.R.Jeong, D.W.Hong and K.I.Chung, "Technologies and Trends of Digital Forensics", Vol.22, No.1, pp.97-104, 2007.

[2] S.H.Kim, E,C, Kim, J,M, Kim, S.Y.Hwang, J.H.Song and S.J.Lee, "macOS Forensic Analysis Technique", Vol.11, No.3, pp.14-28, 2017.

[3] I.Yoon, "The Research about the User Attribution Method of Digital Files", Vol.11, No.1, pp. 73-93, 2017.

[4] J.S.Jun, "Windows System Forensic", Vol.26, No.5, pp.6-16, 2016.

[5] "[Tech Report] Analyze 'Time', Time is 'Imformation'", AhnLab, last modified Jan 8. 2013, accessed July 4. 2019, https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=20374

[6] S.R.Kang, S.R.Kim, J,Y.Cho and J.S.Kim, "Development of Integrated Jump Lists Parser and Its Utilization in Forensic", Vol.11, No.1, pp.1-15, 2017.

[7] E.J.Kim, K.B,Kim and H,N,Hwang, "How To Identify Accessed Files Based On NTFS Filesystem", Vol.11, No.2, pp.1-17, 2017.

[8] H.G.Kim, D.W.Kim and J.S.Kim, "Study on Forensic Analysis with Access Control Modification for Registry", Vol.26, No.5, pp. 1131-1139, 2016.

[9] S.J.Oh and K,H.Kim, "A Study on The Procedure Analysis Vulnerability for Security Incidents Using The Registry Parsing", 『The Institute of Electronics and Information Engineers』, pp. 287-290, 2016.

[10] "Analysis of infringement incident using Windows registry analysis", IGLOOSECURITY, last modified Apr 4. 2018, accessed July 4. 2019, http://www.igloosec.co.kr/BLOG_%EC%9C%88%EB%8F%84%EC%9A%B0%20%EB%A0%88%EC%A7%80%EC%8A%A4%ED%8A%B8%EB%A6%AC%20%EB%B6%84%EC%84%9D%EC%9D%84%20%EC%9D%B4%EC%9A%A9%ED%95%9C%20%EC%B9%A8%ED%95%B4%EC%82%AC%EA%B3%A0%20%EB%B6%84%EC%84%9D%20%EA%B8%B0%EB%B2%95?searchItem=&searchWord=&bbsCateId=17&gotoPage=1

[11] S,R.Kang, S.R.Kim, M.S.Park and J.S.Kim, "Study on Windows Event Log-Based Corporate Security Audit and Malware Detection", Vol.28, No.3, pp.591-603, 2018.

[12] Y.H.Shin, J.Y.Cheon and J.S.Kim, "Study on Recovery Techniques for the Deleted or Damaged Event Log(EVTX) Files", Vol.26, No.2, pp.387-396, 2016.

[13] "Windows log management and analysis method", AhnLab, last modified May 8. 2006, accessed July 4. 2019, https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=3&seq=7887

[14] M.S.Lee and S.J.Lee, "A Study on the Setting Method of the File System Audit Function of Windows for Enhancing Forensic Readiness", Vol.27, No.1, pp.79-90, 2017.

[15] S.H.Kim, J.H.Han and S.J.Lee, "A Study on Detecting Data Hiding Area of Removable Storage Device Based on Flash Memory", Vol.12, No.2, pp.21-29, 2018.

[16] C.U.Park and S.J.Lee, "Digital Evidence Collection Procedure for Hardware Unique Information Collection", Vol.28, No.4, pp.839-845, 2018.

임 정 현(Jeong-Hyeon Lim) [학생회원]

- 2016년 3월 ~ 현재 : 백석대학교 ICT학부

<관심분야>
디지털 포렌식, 정보보호

이 근 호(Lee, Keun Ho) [정회원]

- 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 ICT학부 부교수

<관심분야>
이동통신 보안, 융합보안, 개인정보보호