Journal of Convergence for Information Technology
Vol. 10. No. 5, pp. 23-29, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.05.023

삭제된 $UsnJrnl 파일 복구를 통한 과거 사용자 행위 확인

김동건[1], 박석현[2], 조오현[3*]
[1]충북대학교 전자정보공학과 학생, [2]충북대학교 소프트웨어학과 학생, [3]충북대학교 소프트웨어학과 교수

Analyzing Past User History through Recovering Deleted $UsnJrnl file

Dong-Geon Kim[1], Seok-Hyeon Park[2], Ohyun Jo[3*]
[1]Student, Department of Electrical and Semiconductor Engineering, Chungbuk National University
[2]Student, Department of Computer Science, Chungbuk National University
[3]Professor, Department of Computer Science, Chungbuk National University

요 약 최근 디지털 범죄 수사는 많은 범죄 현장에서 사용되고 있다. 범죄 현장에서는 다양한 전자 장치가 존재하며, 이러한 장치의 디지털포렌식(Digital Forensics) 결과는 중요한 증거로 사용된다. 특히, 디지털포렌식에서 사용자의 행동과 해당 행동이 발생한 시간은 매우 중요한 정보이다. 하지만 사용자의 행동이 기록되는 주기가 짧은 한계점을 가지고 있다. 이러한 특징은 실제 디지털포렌식의 제한 요소로 작용한다. 본 논문에서는 삭제된 사용자 행동 레코드를 복구하고 이를 디지털포렌식에 적용하였으며, 이전 조사 방법과 차이점을 비교하였다. 스토리지에 따라 복구 결과에는 차이가 존재하지만 복구 된 사용자의 동작이 디지털포렌식에 활용 될 때, 사용자 행위 기록이 최소 6%에서 최대 539%로 증가하는 결과를 보여준다.

주제어 : 디지털포렌식, $STANDARD_INFORMATION, NTFS FileSystem, $LogFile, $UsnJrnl, 파일복구

Abstract These days, digital forensic technologies are being used frequently at crime scenes. There are various electronic devices at the scene of the crime, and digital forensic results of these devices are used as important evidence. In particular, the user's action and the time when the action took place are critical. But there are many limitations for use in real forensics analyses because of the short cycle in which user actions are recorded. This paper proposed an efficient method for recovering deleted user behavior records and applying them to forensics investigations, then the proposed method is compared with previous methods. Although there are difference in recovery result depending on the storage, the results have been identified that the amount of user history data is increased from a minimum of 6% to a maximum of 539% when recovered user behavior was utilized to forensics investigation.

Key Words : Digital Forensic, $STANDARD_INFORMATION, NTFS FileSystem, $LogFile, $UsnJrnl, File Recovery

1. 서론

1.1 연구배경

사건의 유형이나 사용자의 행위, 또는 사건의 쟁점에 따라 압수 대상물이 달라지고 분석 방향이 결정된다. 예를 들어, 기술 또는 정보 유출에 대한 범죄의 경우 해당 정보, 파일, 문건이 어떠한 종류의 장비에 존재 했는지 여부, 인터넷이나 클라우드를 통한 데이터의 복사 및 이동 여부, 외부 저장장치 연결을 통한 데이터 복사

*This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2018R1C1B5045013) And this work was supported by the research grant of the Chungbuk National University in 2018
*Corresponding Author : Ohyun Jo(ohyunjo@chungbuk.ac.kr)
Received April 22, 2020
Revised May 5, 2020
Accepted May 20, 2020
Published May 28, 2020

및 이동이 있었는지에 대한 기록은 결정적인 증거로 활용된다. 즉, 어떤 행위나 적업에 의해 관련된 문건이 유출되었는지를 판단해 분석 작업을 해야 한다[1].

개인 컴퓨터, 모바일 기기의 보급률 증가, 업무 전산화 등 생활 속의 많은 정보들이 전산화, 디지털화 되면서 보안성이 중요해졌고, 이러한 디지털 정보는 특정 사건의 증거로서의 의미가 증대되었다[2]. 반면 이러한 기술이 고도화 되고 새로운 기술 지식에 대한 접근이 용이해짐에 따라 개인들의 디지털 정보에 대한 지식이 지능화 되어 수사기관의 디지털 정보에 대한 접근은 어려워지고 있다.

최근 범죄 수사에 디지털포렌식 활용도가 높아지면서 사건이나 행위가 발생한 시간에 대한 정보가 중요한 핵심으로 자리 잡고 있다[3, 4]. 모든 범죄 사건에서 시간 정보는 굉장히 중요하다. 사건에서의 시간 정보는 해당 범죄를 규명하는데 아주 중요한 역할을 하며, 디지털 범죄에서 또한 중요한 증거로 사용될 수 있다. 디지털 범죄에서 이러한 시간 정보를 확인할 수 있는 요소는 다양하다.

본 논문은 위에서 언급한 다양한 요소 중 $UsnJrnl 파일을 활용한다. 해당 파일은 시간정보 및 사용자, 시스템의 행위를 저장하고 있다. 하지만, $UsnJrnl파일이 기록하고 있는 사용자 및 시스템 행위 저장 주기가 짧아 과거의 사용자 행위에 대한 확인에 어려움이 있다.

본 논문에서는 삭제된 $UsnJrnl 복구를 통해 기존의 $UsnJrnl파일을 확인하여 더 많은 사용자 행위 기록 정보를 확인한다. 이는 $UsnJrnl 복구를 통해 더욱 자세하고 다양한 사용자 행위를 확인하여 디지털포렌식에 활용할 수 있다.

1.2 논문 개요

본 논문은 삭제된 $UsnJrnl 파일을 분석하고 복구하는 방법을 소개한다. $UsnJrnl 파일은 Windows2000의 NTFS 5.0 버전부터 포함되었으며, 메타데이터를 구성하는 파일이다. $UsnJrnl 파일은 일종의 로그 파일로 NTFS(New Technology File System)에서 관리되는 파일들이 수정되는 경우 변경 사항을 기록한다.

$UsnJrnl 파일 분석을 통해 사용자 행위가 저장되는 방식을 확인할 수 있고 이는 실제 일어난 행위에 대한 기록을 확인할 수 있음을 의미한다.

실험에서는 각각의 다른 환경에서 사용한 PC를 이용하여 기존의 $UsnJrnl 파일 분석을 통해 사용자 행위기록을 확인한다. 그리고 제안된 방법인 삭제된 $UsnJrnl 파일 복구를 통한 사용자 행위기록을 확인한다. 마지막으로 실험 결과를 비교하여 기존의 방법과 제안된 방법을 통한 사용자 행위 기록의 차이를 분석한다.

2. 본론

2.1 NTFS 파일 시스템

NTFS는 Fig. 1와 같이 구성되며 Windows NT 계열 운영체제의 파일 시스템이다[5]. 이 파일 시스템은 모든 파일과 디렉터리를 MFT(Master File Table)에서 관리한다.

이 MFT는 Fig. 2와 같이 구성된다. MFT는 MFT Entry 들로 구성되어 있고 MFT Entry는 개별 파일들의 정보를 저장하는 레코드이다. MFT Entry의 크기는 $Boot에서 정의된다[1,6]. 시스템 내 모든 파일 혹은 디렉터리에는 하나 이상의 MFT Entry가 존재하는데 이 MFT Entry는 해당 파일의 다양한 메타데이터를 저장한다[7].

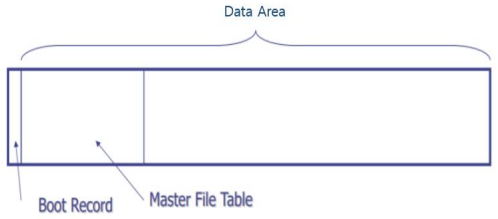

Fig. 1. NTFS Structure

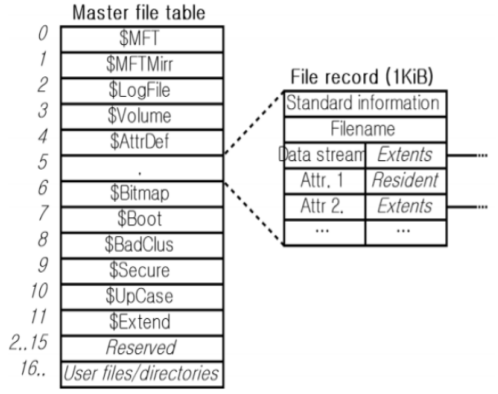

Fig. 2. MFT(Master File Table) Structure

2.2 MFT Entry

MFT Entry는 두 가지 영역으로 구분된다. 첫 번째는 헤더 영역으로, LSN($LogFile Sequence Number)과 Sequence Value를 포함시킨다. LSN은 헤더 영역에서 메타데이터가 업데이트 되는 경우 생성되는 로그 레코드의 번호이다. Sequence Value의 경우 MFT Entry의 사용 횟수를 나타낸다. MFT Entry는 보편적으로 $STANDARD_INFORMATION과 $FILE_NAME 속성을 지니고 있다[8]. [8]에서는 $Usnjrnl 파일을 이용하여 사용자 행위를 확인하는 방법에 대한 소개를 보여주나 삭제된 사용자의 기록을 확인하기 위한 방법은 제시하지 못하였다. Fig. 3은 MFT Entry의 구조를 보여준다.

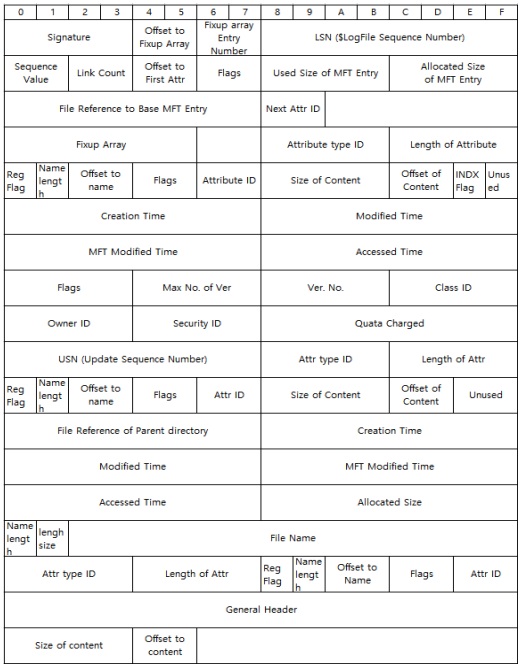

Fig. 3. MFT Entry Structure with properties $STANDARD_INFORMATION, $FILE_NAME, $DATA(Resident)

2.3 $LogFile

$LogFile은 NTFS 파일 시스템의 트랜잭션 로그파일로 작업 중이던 파일의 복구를 위해 사용된다. 모든 트랜잭션 작업을 레코드 단위로 기록하는 특징을 가지며 기록되는 레코드에는 새로운 파일/디렉터리 생성, 파일/디렉터리 삭제, 파일/디렉터리 내용변경, MFT 엔트리 내용변경 등의 내용이 기록된다.

작업 레코드에는 실제 트랜잭션 작업의 내용이 기록되며, 작업 레코드는 레코드 헤더(Header)와 레코드 데이터(Data)로 구성된다.

레코드 헤더는 레코드의 메타데이터가 저장되며, 레코드 데이터에는 작업 전 내용(Undo) 작업 후 내용(Redo)가 기록된다.

Fig. 4은 LogFile 작업 레코드 헤더의 포맷을 나타낸다[9]. 작업레코드 헤더에는 다양한 메타데이터 정보가 존재한다.

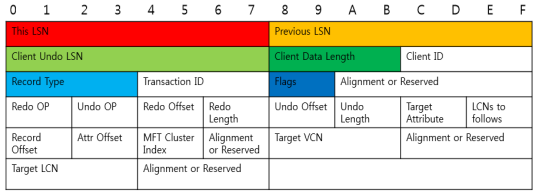

Fig. 4. $LogFile Operation Record Header Format

2.4 $UsnJrnl

$UsnJrnl은 NTFS의 메타데이터를 구성하는 파일이다. $UsnJrnl의 경우 파일 시스템에서의 파일 및 디렉터리가 변경되는 경우 해당 변경 사항을 기록하는 로그이다. $UsnJrnl 파일은 최초에 빈 파일로 생성되는데 이후 NTFS 볼륨에 변경이 생길 때 마다 정의 된 레코드 형식으로 변경을 기록하여 저널파일에 추가한다.

2.5 파일 시스템을 이용한 복구 기법

현재의 파일 복구는 파일 시스템 정보를 이용한 복구와 데이터 카빙 기법을 이용한다. Table 1은 파일 카빙 기법의 특징을 나타낸다. 또한 널리 알려진 상용 파일 복구 도구로는 Recover My Files, R-Studio가 있다.

Table 1. Characteristic of File Carving Technique [10]

Variety of File Carving technique	Characteristic of Carving technique
Header / Footer	Carving by Header of File and Footer Value
Header / File Size	Specific location file is Calculate based on Header of File
Header / Ram Slack	Carving by Header of File and Ram Slack
Carving through file structure	File extraction through Unique characteristic of File and Technique (ASCII, MIME ...)

3. 사용자 행위 분석을 위한 레코드 단위 데이터 복구기법

3.1 레코드 단위 파일 카빙 기법

본 논문에서는 레코드 단위 파일 카빙 기법을 제안한다. 파일은 여러 개의 레코드단위로 구성되어 있는데, 레코드 단위의 카빙 기법은 파일을 구성하는 레코드의 일부를 획득하기 위한 기법이다. 레코드 파일은 정해진 위치에 고유값을 가지고 있는데, 파일마다 레코드가 가지고 있는 고유값의 정보는 다르며 이 레코드 파일의 고유값을 통해 레코드 단위의 파일 카빙이 가능하다.

레코드는 집합의 개념으로 파일 내용이 저장되는 단위나 블록을 의미한다. 따라서 해당 기법을 통한 데이터 복구 시, 파일시스템 구조가 손상되어 확인할 수 없는 파일에 대한 부분적 복구가 가능한 장점이 있다.

3.2 $UsnJrnl파일 $J속성 파일레코드 복구

$J 속성의 파일레코드는 고유의 레코드구조를 가지고 구성되어 있다. 따라서 $J속성의 고유레코드 값 분석을 통해 삭제된 $J속성 레코드를 복구할 수 있다.

$UsnJrnl:$J 속성레코드를 복구하기 위해서는 레코드구조 검증을 통해 진행되며 각 레코드의 첫 4byte는 레코드 사이즈가 기록되며, 다음 4byte에는 파일 시그니쳐가 기록된다. Fig 5.를 살펴보면, $UsnJrnl:$J속성 레코드의 사이즈는 0x00000050의 Hex값을 가지며 이는 80Byte 인 것을 확인 할 수 있고, $UsnJrnl:$J속성 레코드는 0x00000020의 File Signature를 가진 것을 확인할 수 있다. 이렇듯 레코드파일이 가지고 있는 고유의 Hex값 확인을 통해 비할당 영역에 존재하는 $J속성레코드를 복구할 수 있다.

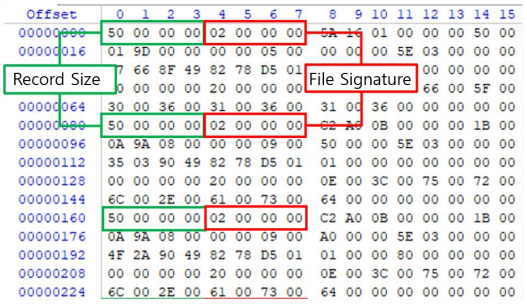

Fig. 5. $UsnJrnl : $J Attribute (Record Information)

4. 실험

본 실험에서는 삭제된 $UsnJrnl:$J속성 레코드파일 복구를 진행하고, 복구된 파일 분석을 통해 사용자 행위를 분석했을 때, 기존의 사용자행위 분석 방식과 비교하여 어떤 차이가 있는지 비교한다. 기존의 사용자 행위 분석 방식은 기존에 알려진 방법인 라이브영역에서 획득 가능한 $UsnJrnl:$J 파일을 획득 후 확인하였다.

4.1 실험 방법

기존의 NTFS 저널파일 획득 방법을 통해 현재 존재하고 있는 $UsnJrnl파일을 획득하고, 비할당 영역에서 삭제된 $UsnJrnl파일에 대한 복구를 진행한다. 복구한 $UsnJrnl 파일에서 사용자 행위 분석을 통해 기존의 방식과 복구한 파일을 추가한 경우의 차이에 대해 확인한다.

4.2 실험 도구

실험 대상물에서 $UsnJrnl파일을 획득 및 분석하기 위해 Hex Editor를 사용하며, 본 실험에서는 X-Ways사에서 개발한 WinHex를 이용하여 획득 및 분석을 진행하였다. 획득한 $UsnJrnl 파일을 분석해 사용자 행위를 확인하기 위해 Guidance Software사에서 개발한 대표적인 디지털포렌식 분석도구 Encase V7을 사용했다. 해당 도구는 보다 간편하게 획득한 증거파일에서 사용자 행위, 파일 행위, 발생 시간 등 다양한 정보를 간편하게 확인할 수 있도록 설계된 도구이다.

4.3 실험 시편

실제 업무에 사용되는 시스템을 상대로 실험을 진행하였으며, 실험에 사용된 시스템의 정보는 Fig. 6과 같다. 각각 다른 환경에서 다른 조건으로 사용한 5개의 시스템을 사용해 실험을 실시했다.

Test PC	OS	File System	Windows Usage Period	Storage Size	Non-allocated Area Size
Personal Computer_1	Windows 10 EnterPrise	NTFS	3Year 2Month	256 GB	114 GB
Personal Computer_1	Windows 7 Ultimate K	NTFS	5Year 4Month	120 GB	31.5 GB
Working Computer_1	Windows 7 Ultimate K	NTFS	2Month	750 GB	651.22 GB
Working Computer_2	Windows 7 EnterPrise K	NTFS	1Year 6Month	256 GB	181.23 GB
Public Computer_1	Windows 10 Education	NTFS	5Month	320 GB	195 GB

Fig. 6. Test System Information

4.4 기존의 방식으로 확인 가능한 사용자 행위 기록

기존의 방식대로 라이브영역에서 $UsnJrnl을 획득 후 사용자 행위에 대한 분석을 진행하였고, Fig. 7.와 같은 결과를 얻을 수 있다. 총 386,373 건의 사용자행위가 확인되었고 행위가 저장된 기간은 2019-10-06 05:30:18 ~ 2019-10-07 15:49:22 약 2일의 기간에 발생했던 사용자 행위가 확인된다.

Test PC	OS	File System	Windows Usage Period	Storage Size	Non-allocated Area Size
Personal Computer_1	Windows 10 EnterPrise	NTFS	3Year 2Month	256 GB	114 GB
$UsnJrnl:$J File Size			14,903,801,264 (13.8 GB)		
$UsnJrnl Record Count			386,373		
$UsnJrnl Record Period			2019-10-06 05:30:18 ~ 2019-10-07 15:49:22		

Fig. 7. Logging of $USnJrnl Files Acquired in Conventional Way

4.5 삭제된 $UsnJrnl 파일 복구를 통한 과거사용자 행위 확인

삭제된 $UsnJrnl:$J 파일은 비할당영역에 그 정보가 저장되게 되는데 해당영역에서 $UsnJrnl:$J 파일레코드 복구를 통해 삭제된 파일을 복구 할 수 있다.

Fig. 8은 $UsnJrnl:$J속성 레코드를 통해 확인 가능한 정보를 정리한 것으로 정해진 위치에 기록된 Hex값을 바탕으로 해당 항목에 대한 정보를 획득할 수 있다.

Fig. 9는 확인된 레코드 정보를 통해 실제 샘플을 바탕으로 복구작업을 진행한 결과이며, 3년2개월 동안 사용한 Window10운영체제에서 총 75개의 삭제된 레코드 파일을 복구할 수 있음을 보여준다.

Fig. 10은 비할당영역에 존재하고 있는$UsnJrnl:$J 속성 파일레코드를 표시한 것으로, 각각의 레코드파일은 정해진 위치에 고유값을 가지고 있는 것을 확인할 수 있다. File Signature값과 Record Size, Size of Filename의 값을 토대로 삭제된 속성 레코드파일을 찾을 수 있으며, 이를 바탕으로 사용자 행위에 대해 분석한 결과 기존의 방식보다 83,222건의 사용자 행위를 추가로 확인할 수 있었고, 확인되는 기간 또한 12일 더 이전의 기록까지 확인되었다.

	Hex value	Conversion value
Size of Record	0x00000060	96
Major Version	0x0002	2
Minor Version	0x0000	0
MFT Reference Number	0x000000007952 / 0x0006	31058, Sequence Num 6
Parent MFT Reference Number	0x00000000A722 / 0x0001	42786, Sequence Num 1
USN	0x0000000002400000	37,478,736
TimeStamp(FileTime)	0x01CAFACC90D5B665	2010-05-24 8:06
reason Flag	0x80000002	Add the data to $Data attribute
Source Informaion	00 00 00 00	0
Security ID	00 00 00 00	0
File Attributes	0x00002020	File
Size of Filename	0x0022	34
Offset to Filename	0x003C	60
File Name	53 00 43 00 6C 00 69 00 65 00 6E 00 74 00 41 00 70 00 70 00 73 00 2E 00 6C 00 6F 00 67	SBSClientApps.log

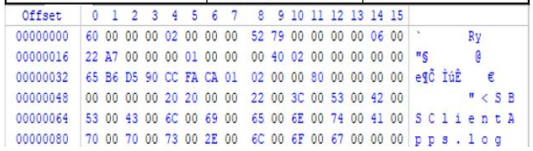

Fig. 8 Non-allocated $UsnJrnl:$J Attribute (Record Information)

Test PC	OS	File System	Windows Usage Period	Storage Size	Non-allocated Area Size
Personal Computer_1	Windows 10 EnterPrise	NTFS	3Year 2Month	256 GB	114 GB
Recovery Record File			75		
Last $UsnJrnl Record			2019-09-25 15:34:56		
Current $UsnJrnl Record			2019-10-07 16:04:45		

Fig. 9. Recovered $USnJrnl:$J FileRecord Information

Fig. 10. $USnJrnl:$J File Record Checked in Non-allocated Area

5. 실험 결과

라이브영역에서 획득 가능한 $UsnJrnl:$J속성 파일을 통해 사용자 행위를 확인하고, 비할당영역에서 삭제된 $UsnJrnl:$J속성 파일을 복구하여 사용자 행위로그를 확인을 통해, 기존의 방법과 제안한 방법의 결과물을 비교 하였다.

5.1 추가로 확인 된 사용자 행위 기록

비할당영역에 존재하는 삭제된 $UsnJrnl:$J속성 레코드 파일을 복구한 결과 Fig. 11과 같이 삭제된 레코드파일이 최소 75개에서 최대 39,912개 까지 복구 되었다. 비할당영역에서 복구가 가능한 파일의 개수는 사용한 저장장치의 종류, 사용자의 사용패턴, 데이터 저장 패턴 등을 통해 달라질 수 있다.

Test PC	Windows Usage Period	Storage Size	Non-allocated Area Size	Recovery Record File
Personal Computer_1	3Year 2Month	256 GB	114 GB	75
Personal Computer_1	5Year 4Month	120 GB	31.5 GB	115
Working Computer_1	2Month	750 GB	651.22 GB	39,912
Working Computer_2	1Year 6Month	256 GB	181.23 GB	682
Public Computer_1	5Month	320 GB	195 GB	4,312

Fig. 11. File Carving Results in Record Units

Fig. 12는 실험 시편을 대상으로 결과를 나타낸 표이다. 기존의 방식보다 최소 6%에서 최대 539%까지 확인되는 사용자 행위 기록이 증가한 것을 볼 수 있다. 제안한 방법을 통해 삭제된 $UsnJrnl:$J 레코드파일을 복구한 후 사용자 행위에 대한 조사를 하였을 경우 기존의 방법으로 사용자 행위에 기록 보다 적게는 23,222개 많게는 678,691 건의 사용자 행위가 추가발견 되었다.

Test PC	User Log		Last $UsnJrnl Record		Recovery Record File
	conventional method	Suggested method	conventional method	Suggested method	
Personal Computer_1	386,373	409,595	2019-10-06 5:30	2019-09-25 15:23	75
Personal Computer_1	328,749	391,248	2019-10-14 8:31	2019-10-01 12:27	115
Working Computer_1	154,566	833,257	2019-10-11 15:12	2019-08-07 12:03	39,912
Working Computer_2	337,707	738,710	2019-10-11 9:44	2019-09-03 16:52	682
Public Computer_1	362,089	785,753	2019-10-09 10:02	2019-04-09 17:05	4,312

Fig. 12. Conventional Method and Result

복구된 레코드 파일의 개수 또한 적게는 75개에서 많게는 39,912개 까지 복구가 된 것이 확인되며, SSD 저장장치의 경우 사용하지 않는 비할당영역에 대한 Trim기능이 설계되어 있기 때문에 실험대상 시스템이 사용하는 저장장치의 종류에 따라 복구가 되는 레코드 파일의 차이는 발생할 수 있다.

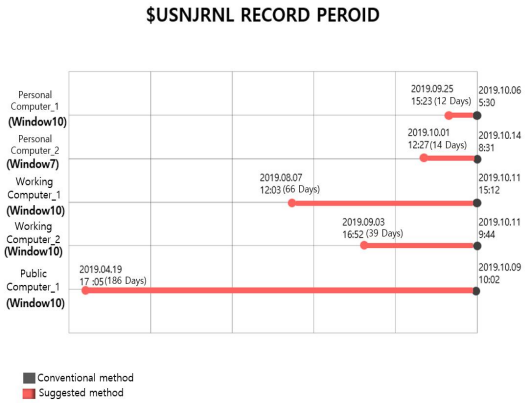

Fig. 13. Comparing the Period During which Historical User Actions Identified

Fig. 13은 실험 결과 중 과거 사용자 행위가 확인되는 기간을 비교한 그래프이다. 그래프를 비교해 보면 기존의 사용자 행위 확인 방식보다 확인되는 사용자 행위의 기간이 최소 12일에서 최대 186일 까지 증가한 것을 확인할 수 있다.

이와 같이 본 논문에서 제안한 삭제된 $UsnJrnl:$J 파일을 복구하여 사용자 행위에 대한 포렌식 조사 시, 기존의 방법에서는 삭제되어 확인할 수 없었던 과거의 사용자 행위기록과 시간을 확인할 수 있다.

6. 결론

개인 컴퓨터, 모바일 기기, IoT장비 등 수많은 디지털 장비가 보급되면서 범죄에 사용되거나, 증거자료로 활용되는 경우가 많아지고 있다. 그 결과 디지털 증거의 중요성이 점점 증가하고 있다. 특히, 사용자가 한 행위에 대한 기록과 시각은 더욱더 중요한 증거로 활용된다. 하지만, 기존의 분석대상인 $UsnJrnl 파일을 통한 사용자 행위기록은 저장되는 주기가 짧은 한계점을 가지고 있다. 이를 해결하고 보다 정확하고 자세한 정보를 획득하기 위한 방안으로 삭제된 $UsnJrnl 파일 복구방법과 이를 통한 과거의 사용자행위 분석방법을 제시하였다.

첫째, $UsnJrnl파일에 대한 분석을 통해 파일의 구조와 이를 통해 확인할 수 있는 사용자 행위에 대해 소개하였고 둘째, 비할당영역에서 삭제된 저널파일의 복구하는 방법과 이를 통한 과거사용자행위 분석방법을 제시하였다. 본 논문에서 제안한 방법을 이용하여 사용

자 행위에 대한 포렌식을 진행하면 기존의 방법에서는 획득할 수 없었던 많은 과거 기록과 정보를 획득할 수 있으며 보다 정확하고 효율적인 디지털 포렌식 조사가 가능하다.

앞으로 더 많은 정보의 복구 및 획득을 위해서는 새로운 파일에 대한 개발 및 연구가 필요하다. 또한 새로운 복구기법 개발을 통해 기존의 방법으로 복구가 불가능한 데이터를 획득할 수 있는 방법이 필요하다.

REFERENCES

[1] H. Carvey. (2013). *HowTo: Determine User Access To Files.* http://windowsir.blogspot.kr/2013/07/howto-determine-user-access-to-files.html

[2] D. Y. Won. (2015). A Study on Digital Evidence Collection Procedures Improvement. *Journal of Digital Forensics, 9(2),* 27-41.

[3] G. Palmer. (2001). *A Road Map for Digital Forensic Research.* technical report DTR-T001-0, Utica, New York

[4] C. Boyd & P. Forster. (2004). Time and Date issues in forensic computing - a case study. *Digital Investigation, 1(1),* 18-23.

[5] B. Carrier. (2005). *File System Forensic Analysis.* Addison-Wesley, 340-341.

[6] R. Russon & Y. Fledel. (2004). *NTFS Documentation,* Chapter 3. NTFS files:$LogFile, pp. 38-42. http://dubeyko.com/development/FileSystems/NTFS/ntfsdoc.pdf

[7] S. Neuner et al. (2016). Time is on my side: Stegan graphy in filesystem metadata. *Digital Investigation, 18(2016),* S76 - S86.

[8] H. J Yoon. (2018). *A study on user behavior trackingusing $UsnJrnl.* Doctoral dissertation, Graduate School of Seoul National University.

[9] J. H. Oh. (2013). *NTFS Log Tracker.* Forensic Insight ; Digitalforensic community in korea.

[10] M. S. Park. (2012). *Record File Carving Technique for Efficient File Recovery in Digital Forensic Investigation.* Graduate School of Information Security Korea University.

김 동 건(Dong-Geon Kim) [학생회원]

· 2014년 2월 : 청주대학교 전자정보공학과 (학사)
· 2020년 2월 : 충북대학교 전자정보공학부 (석사)
· 관심분야 : 디지털 포렌식, 데이터 복구/관리
· E-Mail : dgkim@myung.co.kr

박 석 현(Seok-Hyeon Park) [학생회원]

· 2019년 2월 : 세명대학교 컴퓨터학과 (학사)
· 2019년 2월 ~ 현재 : 충북대학교 컴퓨터과학과 석사과정
· 관심분야 : 수중 통신, 인공지능
· E-Mail : seokhyeon@chungbuk.ac.kr

조 오 현(Ohyun Jo) [정회원]

· 2005년 2월 : 한국과학기술원 전기및전자공학(학사)
· 2007년 8월 : 한국과학기술원 전기및전자공학(석사)
· 2011년 2월 : 한국과학기술원 전기및전자공학(박사)
· 2011년 4월 ~ 2016년 2월 : 삼성전자 DMC 연구소
· 2016년 3월 ~ 2017년 7월 : 한국전자통신연구원
· 2017년 8월 ~ 2018년 2월 : 육군사관학교 전자공학과 조교수
· 2018년 3월 ~ 현재 : 충북대학교 소프트웨어학과 조교수
· 관심분야 : IoT 융합, 정보통신 및 네트워크, 기계학습
· E-Mail : ohyunjo@chungbuk.ac.kr