Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.1, Feb. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.1.135

Windows 7·8 IconCahe.db 파일 포맷 분석 및 활용방안*

이 찬 연,† 이 상 진‡
고려대학교 정보보호대학원

The analysis of Windows 7·8 IconCache.db and its application*

Chan-Youn Lee,† Sang-Jin Lee‡
Center for Information Security Technologies(CIST), Korea University

요 약

디지털 포렌식 조사를 회피하기 위한 안티포렌식이 발전하고 있는 가운데, 안티포렌식 행위를 찾아내기 위한 포렌식 방법들 또한 다각도로 연구되고 있다. 사용자 행위분석을 위한 여러 요소 중 응용프로그램의 아이콘 정보를 저장하고 있는 IconCache.db 파일은 디지털 포렌식 조사를 위한 의미 있는 정보들을 제공하고 있다. 본 논문은 IconCache.db 파일의 특성을 알아보고 안티포렌식에 대응할 수 있는 활용방안을 제시한다.

ABSTRACT

Since anti-forensics have been developed in order to avoid digital forensic investigation, the forensic methods for analyzing anti-forensic behaviors have been studied in various aspects. Among the factors for user activity analysis,"Iconcache.db" files, which have the icon information of applications, provides meaningful information for digital forensic investigation. This paper illustrates the features of IconCache.db files and suggests the countermeasures against anti-forensics utilizing them.

Keywords: IconCache.db, Antiforensic, Digital Forensic, User Behavior, Icon

I. 서 론

최근 디지털 증거가 법정에서 중요한 증거가 되는 사례가 많아지면서, 디지털 증거를 삭제하거나 숨기는 등의 안티포렌식 기술도 함께 발전하고 있다.

때문에 안티포렌식 행위를 적발하기 위한 연구 또한 활발히 진행되고 있다. Windows Registry[1]와 PreFetch Folder[2] 등에 대한 분석이 안티포렌식 행위를 찾아내기 위한 대표적인 방법이다. 그러나 역설적이게도 Windows Registry와 PreFetch Folder의 삭제는 안티포렌식 방법 중 가장 기초적인 것에 해당한다.

IconCache.db 파일은 사용자 컴퓨터 및 외부 저장매체에서 열람 및 실행한 응용프로그램들의 아이콘 캐시정보를 저장하고 있다. 또한 기록된 응용프로그램의 아이콘 캐시 정보는 삭제되지 않는 특성을 가지고 있다. 그럼에도 불구하고 IconCache.db 파일은 안티포렌식 행위를 찾아내기 위한 분석대상으로 주목받지 못했다.

IconCache.db 파일은 사용자가 삭제했거나 외부 저장매체 등을 통해 실행 또는 열람한 응용프로그램의 흔적을 저장하고 있으므로, 사용자의 안티포렌식 행위를 분석하는 방법으로 의미가 있다.

따라서 기존의 사용자 행위분석 방법과 함께 Icon-

접수일(2013년 10월 23일), 게재확정일(2013년 12월 8일)
* 이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구입니다.(2012M3A2A1051106)
† 주저자, liebich@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr (Corresponding author)

Cache.db 파일을 분석하면 보다 효과적으로 디지털 증거를 분석할 수 있다.

본 논문에서는 IconCache.db 파일 구조를 비롯한 실행 메커니즘과 특성을 알아보고 디지털 포렌식 측면의 활용방안에 대해 연구하였다.

II. 관련 연구

앞서 언급한 바와 같이 안티포렌식 흔적을 찾기 위해 다양한 분야에 대한 연구가 이루어지고 있지만, IconCache.db 파일에 대한 연구는 상대적으로 미미하였다.

현재까지 IconCache.db 파일에 대한 연구는 Jan Collie가 유일하다[3]. Jan Collie는 외부 저장매체 및 호스트 컴퓨터에서 응용프로그램을 복사 또는 실행, 열람 시 IconCache.db 파일에 기록되는 아이콘의 이미지와 아이콘의 저장 경로정보 값의 변화를 중심으로 IconCache.db 파일의 특성을 설명하였다.

그러나 IconCache.db 파일의 구체적인 파일구조를 비롯하여 아이콘의 이미지 정보 및 아이콘이 저장된 경로정보 값의 기록 메커니즘에 대한 구체적인 연구가 부족하다. 또한 최근 사용자가 증가하고 있는 Windows Vista를 비롯한 7과 8의 IconCache.db 파일에 대한 구체적인 구조에 대한 연구도 이루어지지 않았다.

IconCache.db 파일이 디지털 포렌식 분석 대상으로 활용되기 위해서는 Windows Vista를 비롯한 7과 8버전의 IconCache.db 파일에 대한 구체적인 추가 연구가 필요하다.

III. IconCache.db 파일 구조

IconCach.db 파일은 Windows 95 부터 사용되고 있으며, 윈도우 버전별 파일의 이름과 저장 경로는 상이하다. 세부 내용은 Table 1.과 같다.

Windows XP 버전까지는 IconCache.db 파일의 이미지와 경로정보를 분석할 수 있는 분석도구(ThumnailExpert[1])가 개발되었기 때문에 Windows 7・8의 IconCache.db을 중심으로 분석을 진행하였다.

1) http://www.thumbnailexpert.com

Table 1. The name and storage path of IconCache.db file

File name	Win Ver.	Path
ShellIcon Cache	95	%SystemDrive%\Windows\ShellIconCache
	NT 2000	%SystemDrive%\Winnt\ShellIconCache
Icon Cache.db	XP	%SystemDrive%\Documents and Settings\Username\Local Settings\Application Data\IconCache.db
	Vista 7 / 8	%UserProfile%\AppData\Local\IconCache.db

3.1 전체구조

Windows Vista・7・8의 IconCache.db 파일 구조는 Fig. 1.과 같이 서로 상이하다. Windows Vista와 7에서는 파일 헤더와 경로정보, 이미지 데이터를 저장하는 부분으로 구분되어 있다. 그러나 Windows 8에서는 이미지 데이터 없이 경로정보만을 저장하고, 이미지 데이터는 Fig. 2.와 같이 별도의 파일에 따로 저장하고 있다.

Windows Vista와 7의 IconCache.db 파일은 각 아이콘의 이미지를 해상도에 따라 분류하여 BMP 이미지로 저장하고 있으며, 각각의 이미지 데이터 영

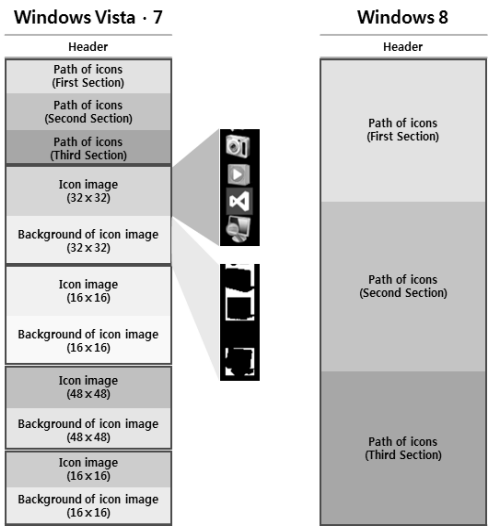


Fig.1. File structure of IconCache.db in Windows Vista, 7 and 8

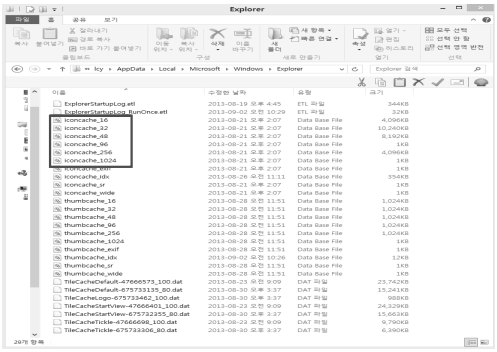


Fig.2. The stored image file of IconCache.db in Windows 8

역의 크기는 아이콘 캐시 데이터 증가와 비례하여 증가한다.

Windows 8은 Fig. 2.에서 보는 바와 같이 "%USERPROFILE%\AppData\Local\Microsoft\ Windows\Explorer" 경로에 아이콘 캐시 이미지 데이터를 해상도별로 구분하여 파일로 저장하고 있다. 또한 Windows 7보다 해상도가 높은 96, 256, 1024 크기의 아이콘 데이터를 저장하고 있다.

IconCache.db 파일의 헤더 구조는 Table 2.와 같다. 파일 헤더에는 헤더의 크기, 시그니쳐, 파일 버전정보 등 일반적인 정보가 저장되어 있다.

Table 2. IconCache.db file header structure

	0 1 2 3	4 5 6 7	8 9 A B	C D E F
0X00	Header size	Signature	File version	Windows build number
0X10	Unknown	Unknown	Unknown	Unknown
0X20	Unknown	Unknown	Unknown	Unknown
0X30	Unknown	Unknown	Unknown	Unknown

IconCache.db 파일 헤더의 크기와 파일 버전 값이 Windows XP와 이후의 것이 상이하다. 세부 내용은 Table 3.과 같다.

Table 3. Windows version-specific IconCache.db file header value

win ver.	Header size	Signature	File version	Windows build number
XP	50h	57 69 6E 34	05 05 00 00	54 0B 00 06
Vista	40h	57 69 6E 34	06 05 00 00	72 17 00 06
7	40h	57 69 6E 34	06 05 00 00	B0 1D 01 06
8	40h	57 69 6E 34	06 05 00 00	F0 23 02 06

IconCache.db 파일의 헤더 구조가 변경되었기 때문에 Jan Collie가 Windows XP의 IconCache.db 파일 분석 시 사용한 분석도구(ThumnailExpert[2])를 사용해 Windows Vista·7·8 버전의 IconCache.db 파일을 분석하는 것은 어렵다.

3.2 경로정보 구조

IconCache.db 파일의 헤더정보 다음에는 아이콘의 경로정보가 저장되어 있다. 경로정보는 Fig. 3.과 같이 세 섹션으로 구분되어 저장된다. 또한 각 섹션이 시작하는 앞부분의 4byte는 섹션별 경로정보의 개수를 의미한다.

경로정보의 첫 번째 섹션에는 윈도우 설치 시 Default로 설치되는 아이콘의 경로정보와 사용자가 열람 또는 실행하는 응용프로그램의 아이콘 정보가 순서대로 저장된다. 두 번째 섹션에는 링크 또는 단축아이콘의 경로정보가 저장된다. 마지막으로 세 번째에는 윈도우 설치 후 사용자가 실행하거나 열람·복사한 응용프로그램의 아이콘 경로정보가 순서대로 저장된다.

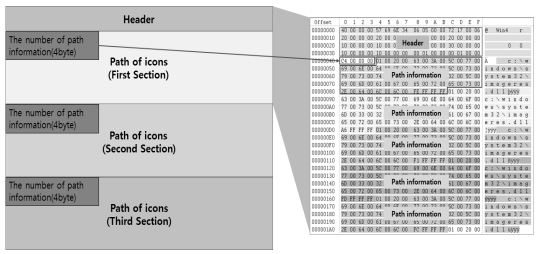


Fig. 3. The entire structure of path information of IconCache.db file

경로정보의 첫 번째 섹션 구조는 두 번째와 세 번째 섹션 구조와 상이하며, 구체적인 구조는 Fig. 4.와 같다.

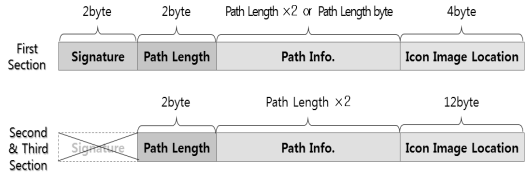


Fig.4. Structure-specific path information in each section

2) http://www.thumbnailexpert.com

앞에서 언급했듯이 각 섹션별 경로정보의 개수를 의미하는 값에 이어 아이콘의 경로정보 값이 기록된다. 경로정보 앞부분에는 시그니쳐와 경로정보의 문자열 길이 값이 있고, 경로정보 뒤에는 아이콘 이미지 데이터의 위치정보가 기록되어 있다.

시그니쳐는 윈도우 버전별로 상이하며, 파일경로의 문자열 길이 값에 대한 계산 방법은 시그니쳐에 따라 다르다. 계산 방법은 Table 4.와 같다.

Table 4. The calculation methods depending on signatures and versions of Windows.

윈도우	시그니쳐	파일 경로 문자열 길이 계산
Win7	01, 11, 41	File Path Length × 2
	02, 22, 42	File Path Length
Win8	01, 41, 81, 91, a1, c1	File Path Length × 2
	02, 22, 42	File Path Length

Fig. 5.의 첫 번째 경로정보 시그니쳐는 '01 00' 이고, 파일경로의 문자열 길이 값은 '20 00' 이다. Table 4.를 참고하여 경로정보의 문자열 길이를 계산하면 20h × 2 = 40h이 된다.

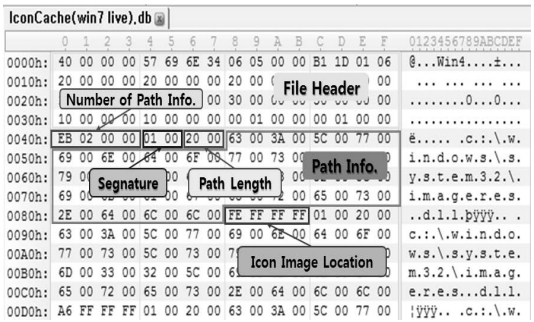


Fig.5. The hex structure of the first path information

Table 4.와 같이 시그니쳐에 의해 문자열 길이 값을 계산하는 방식이 달라지는 이유는 유니코드와 아스키코드 형식의 문자열 표기방법이 다르기 때문이다.

Fig. 4.를 보면 경로정보 뒤에 기록된 각각4byte와 12byte의 헥사값이 기록되어 있는데, 이 부분에는 아이콘 이미지가 저장된 위치정보를 저장하고 있다.

Fig. 6.을 보면 IconCache.db 파일의 두 번째와

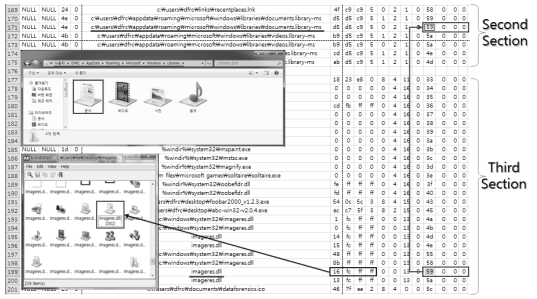


Fig.6. Calculating the location of icon image data

세 번째 경로정보 세션에서는 12byte 헥사값 중 마지막 4byte 값이 같은 쌍을 발견할 수 있다. "%USERPROFILE%\appdata\roaming\microsoft\ windows\libraries\documents.library-ms" 파일경로의 마지막 4byte와 세 번째 세션의 23번째 파일인 imageres.dll의 마지막 4byte 값(59 00 00 00)이 같다.

23번째 파일(Imageres.dll)의 경로정보 뒤 4byte 값(16 FC FF FF)을 리틀앤디안으로 변환 후 2의 보수를 취하면 "1002"라는 값을 얻을 수 있는데, "1002"는 Imageres.dll 파일에 저장된 1002번째 아이콘 이미지를 가리킨다. Fig. 6.을 보면 Imageres.dll 파일의 1002번째 아이콘 이미지와 "%USERPROFILE%\appdata\roaming\microsoft\windows\libraries\documents.library-ms" 경로의 아이콘 이미지가 같음을 확인할 수 있다.

따라서 경로정보 뒤에 있는 4byte의 헥사값은 아이콘 이미지 데이터의 위치정보를 저장하고 있으며, 두 번째와 세 번째 섹션의 12byte 헥사값 중 마지막 4byte는 같은 아이콘 이미지 데이터를 연결해주는 역할을 하고 있다.

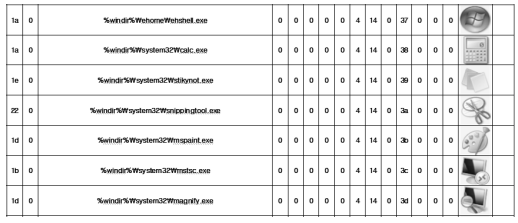


Fig.7. Icons and images of icons in third section

실험파일을 대상으로 이미지 데이터를 계산해본 결과 Fig. 7.과 같이 파일경로와 이미지 데이터를 매칭시킬 수 있다.

윈도우 "*.dll" 파일에 저장된 아이콘 이미지 데이터를 사용하는 응용프로그램의 아이콘 이미지 데이터 위치 값 계산은 위에서 설명한 방법으로 계산할 수 있다. 그러나 고유한 아이콘 이미지 데이터를 사용하는 응용프로그램의 파일경로와 아이콘 이미지 데이터의 매칭 방법은 아직 연구 중이다.

IV. IconCache.db 파일의 특성

Jan Collie의 논문에서 연구된 IconCache.db 파일의 일반적인 특성 외에 디지털 포렌식 측면에서 보다 의미 있는 특성을 찾아내기 위해 아이콘 캐시정보의 생성 및 삭제 메커니즘에 대해 추가연구를 진행하였다.

4.1 IconCache.db 파일의 데이터 생성

IconCache.db 파일의 실행 메커니즘을 알아보기 위해 MS에서 개발한 Process Monitor[3]를 사용하여 실험하였다. 실험 결과 Fig. 8.과 같이 컴퓨터 부팅 시 IconCache.db 파일에 저장된 데이터가 Explorer 프로세스에 업로드 된다.

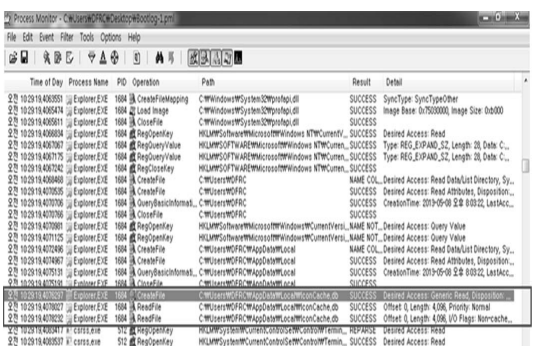


Fig.8. IconCache.db file on Explorer Process after booting

응용프로그램에 저장된 아이콘 이미지 데이터는 일반적으로 PNG 파일로 저장된다. 그러나 IconCache.db 파일은 아이콘 이미지 데이터를 BMP 파일 형태로 저장한다.

Fig. 9.에서 보는 바와 같이 MS에서 개발한 Process Explorer[4]를 사용하여 Explorer 프로세스를 모니터링 한 결과, IconCache.db 파일은 IconCodecService.dll 파일을 통해 PNG 형태의 아이콘 이미지 데이터를 BMP 파일 형태로 변환하여 저장하는 것을 알 수 있었다.

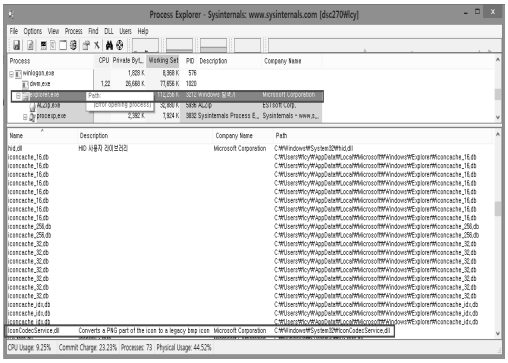


Fig.9 Explorer process real-time monitoring

IconCache.db 파일은 사용자가 컴퓨터에서 파일을 실행하지 않고 단순히 응용프로그램의 아이콘만 열람한 경우에도 Fig. 10.과 같이 해당 아이콘에 대한 정보를 기록한다[3].

Fig.10. Viewing only the icon of the application

IconCache.db 파일은 응용프로그램의 설치, 복사 또는 아이콘의 단순 열람 시에도 사용자가 응용프로그램을 사용한 순서대로 관련 정보를 기록한다.

Fig. 11.은 3개의 응용프로그램을 차례로 복사 및 설치한 그림이다. 가장 먼저 decode.exe 파일이 복

3) http://technet.microsoft.com/en-us/ sysinternals/bb896645

4) http://technet.microsoft.com/en-us/sysinternals/bb896653

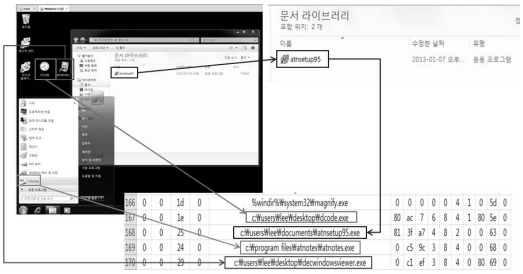


Fig.11. Copy and install the application procedure

사되고, 이어서 atnotes.exe 파일의 설치 파일인 atnsetup95 파일을 복사한 후 실행하였다. atnsetup95 파일 실행으로 atnotes.exe 파일의 경로정보가 기록된 것을 알 수 있다. 마지막으로 decwindowsviewer.exe 파일을 복사하였다.

Fig. 11.의 IconCache.db 파일을 보면 파일들이 복사되고 실행된 순서대로 기록되어 있음을 확인할 수 있다.

응용프로그램을 임의 폴더에 숨겨 컴퓨터에 복사 후 응용프로그램을 설치하거나 아이콘을 열람하지 않을 경우, IconCache.db 파일에는 어떠한 정보가 기록되는지 알아보기 위해 추가 실험을 수행하였다.

Fig. 12.와 같이 "Test1" 폴더에 각종 실행파일 및 압축파일 등을 저장 후 폴더를 실험 대상 컴퓨터에 복사하였다. 복사 이후 아이콘을 열람하거나 응용프로그램을 설치하지 않은 상태로 IconCache.db 파일을 분석하였다.

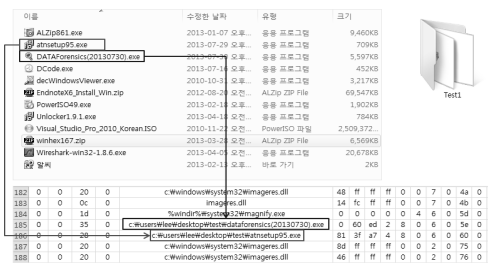


Fig.12. Copy the hidden icon files

실험 결과 폴더에 저장된 여러 종류의 파일 중 수정시간이 가장 최근인 두 개의 실행파일에 대한 아이콘 경로정보가 IconCache.db 파일에 기록되었다. Fig. 12.의 "Test1" 폴더 그림과 같이 아이콘을 크게 할 경우 보이는 2개의 미리보기 파일에 대한 정보가 IconCache.db 파일에 기록 되는 것을 알 수 있다.

따라서 사용자가 응용프로그램을 임의의 폴더에 숨긴 채 컴퓨터에 복사 하더라도 IconCache.db 파일을 통해 응용프로그램에 대한 정보를 얻을 수 있다.

IconCache.db 파일의 데이터 생성 시 특성은 아래와 같이 요약할 수 있다. IconCache.db 파일은 사용자가 실행하거나 열람했던 응용프로그램의 아이콘 정보를 순서대로 기록하며, 실행파일을 폴더에 숨긴 채 컴퓨터에 복사할지라도 수정시간이 가장 최근인 두 개의 실행파일에 대한 아이콘 캐시정보를 기록한다.

4.2 IconCache.db 파일의 데이터 삭제

앞에서 언급한 바와 같이 Explorer 프로세스에 업로드되어 있던 아이콘 캐시정보는 윈도우 종료시 IconCache.db 파일에 재 기록된다. 따라서 IconCache.db 파일을 삭제하더라도 Explorer 프로세스에 업로드 되어있던 아이콘 캐시 데이터들은 삭제되지 않기 때문에 새로운 IconCache.db 파일을 생성하여 기존의 아이콘 캐시 데이터들을 다시 저장하게 된다.

그러나 불행하게도 IconCache.db 파일을 삭제한 후, 위도우를 비정상 종료시키거나 Explorer 프로세스를 강제 종료시키게 될 경우에는 Explorer 프로세스에 업로드 되어있던 아이콘 캐시 데이터들을 다시 저장할 수 있는 시간이 없기때문에 IconCache.db 파일은 초기화가 되어버린다. 초기화된 IconCache.db 파일은 두 번의 재부팅과정을 거쳐 다시 생성된다. 재생성된 IconCache.db 파일은 오직 바탕화면에 있는 아이콘 캐시 데이터만을 저장하게 된다.

Fig. 13. Deleting the IconCache.db file and after the abnormal termination, recreated the IconCache.db file and icons on desktop

Fig. 13.을 보면 초기화된 이후 재 생성된 IconCache.db 파일에 저장된 아이콘 캐시정보와 컴퓨터 바탕화면의 아이콘이 일치함을 알 수 있다.

V. 디지털 포렌식 측면에서의 활용 방안

IconCache.db 파일은 컴퓨터 사용자가 사용한 응용프로그램의 아이콘 정보를 기록하고 있기 때문에 디지털 포렌식 관점에서 사용자 행위 분석을 위한 의미 있는 자료로 활용될 수 있다. 따라서 아이콘 캐시의 특성을 고려한 효과적인 수집 및 분석 방법을 제시하고자 한다.

5.1 삭제된 프로그램에 대한 정보 수집

컴퓨터에서 사용자가 사용한 응용프로그램의 흔적은 Windows Registry[4], PreFetch folder[2] 또는 단축아이콘[5]을 통해 확인할 수 있다.

그러나 컴퓨터 사용흔적 제거를 위해 레지스트리를 초기화 하거나, 파일을 완전 삭제함으로써 관련 범죄 행위에 대한 단서를 찾을 수 없도록 하는 등의 안티포렌식 행위는 이미 널리 알려진 방법이 되었다. 관련 도구들 또한 인터넷을 통해 쉽게 다운받아 사용할 수 있다.

그러나 응용프로그램을 삭제하더라도 IconCache.db 파일에 저장된 삭제된 응용프로그램의 아이콘 캐시정보는 삭제되지 않는 다는 사실은 많은 사람들이 모르고 있다. 실제로 아래 실험을 통해 삭제된 응용프로그램의 흔적이 IconCache.db 파일에 남아 있음을 확인 할 수 있다.

dataforensics copy.exe와 dataforensics original.exe를 삭제한 후 IconCache.db 파일을 확인한 결과 Fig. 14.에서 보듯이 삭제된 파일에 대한 정보가 남아 있다.

248	NULL	NULL	20	0	c:₩windows₩system32₩imageres.dll	ef	ff	ff	ff	0	0	0c	0	84	0	0	0
249	NULL	NULL	20	0	c:₩windows₩system32₩imageres.dll	16	fc	ff	ff	0	0	0c	0	85	0	0	0
250	NULL	NULL	1f	0	c:₩windows₩system32₩zipfldr.dll	0	0	0	0	0	0	0c	0	86	0	0	0
251	NULL	NULL	1a	0	%windir%₩system32₩wfsr.dll	0	0	0	0	0	0	0c	0	87	0	0	0
252	NULL	NULL	20	0	c:₩windows₩system32₩sendmail.dll	2f	f8	ff	ff	0	0	0c	0	88	0	0	0
253	NULL	NULL	2d	0	c:₩users₩lcy₩documents₩dataforensics copy.exe	60	2a	49	2	8	2	1	0	89	0	0	0
254	NULL	NULL	31	0	c:₩users₩lcy₩documents₩dataforensics original.exe	0	e3	cc	5	8	4	1	0	8a	0	0	0
255	NULL	NULL	32	0	c:₩users₩lcy₩documents₩dataforensics original1.exe	60	2a	49	2	8	2	1	0	8b	0	0	0
256	NULL	NULL	2d	0	c:₩users₩lcy₩documents₩dataforensics copy.exe	0	e3	cc	5	8	4	1	0	8c	0	0	0
257	NULL	NULL	31	0	c:₩users₩lcy₩documents₩dataforensics original.exe	60	2a	49	2	8	2	1	0	8d	0	0	0

Fig.14. IconCache.db files after deleting an application

Fig. 15.는 실험환경이 아닌 실제 데이터를 분석한 결과이다. Fig. 15.에 기록된 완전삭제 프로그램은 (Revo Uninstaller[5]) 레지스트리 분석 시에는 발견할 수 없었으나, IconCache.db 파일에서는 설치 흔적을 확인할 수 있었다.

494	NULL	NULL	26	0	c:₩program files₩unlocker₩unlocker.exe	0	24	20	0b	8	2	0	80	ff	ff	ff	ff
495	NULL	NULL	27	0	c:₩windows₩system32₩actioncenterps1.dll	ff	ff	ff	ff	0	0	0	80	ff	ff	ff	ff
496	NULL	NULL	43	0	c:₩program files₩vs revo group₩revo uninstaller₩revouninstaller.exe	70	ee	da	3	8	2	0	80	ff	ff	ff	ff
497	NULL	NULL	27	0	c:₩users₩王昊宇₩downloads₩revosetup130.exe	30	d5	fd	6	8	2	2e	0	6b	0	0	0
498	NULL	NULL	21	0	%systemroot%₩system32₩mrtcsync.exe	0	0	0	0	0	0	4	0	80	ff	ff	ff

Fig.15. The installation trace of deleted the wiping-tool

따라서 컴퓨터에 응용프로그램의 설치 및 사용 흔적이 삭제되었을 경우, IconCache.db 파일 분석을 통해 과거에 사용되었으나 현재에는 삭제된 응용프로그램에 대한 정보를 얻을 수 있다.

5.2 삭제된 프로그램의 상대적인 시간정보 확인

위에서 언급한 바와 같이 IconCache.db 파일을 통해 삭제된 응용프로그램에 대한 정보를 얻을 수 있다.

따라서 IconCache.db 파일에 남아있는 삭제된 응용프로그램의 정보와 레지스트리 및 프리패치에 남아 있는 다른 응용프로그램들의 시간정보를 비교 분석하면 삭제된 응용프로그램의 상대적인 설치시간을 확인 할 수 있다.

Fig. 16.을 보면 삭제된 bcwipeSetup.exe 파일이 2013년 9월 13일 19:25:45 ~ 19:41:22 사이에 설치되었었음을 추론할 수 있다.

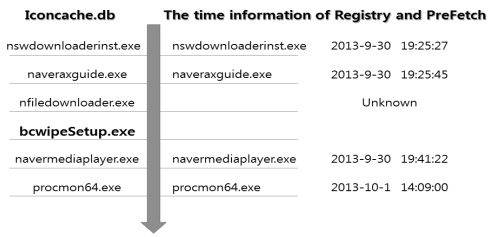


Fig.16. Inferring the relative time of deleting files

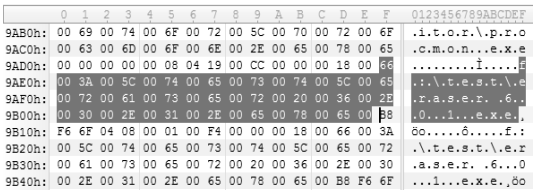
삭제된 응용프로그램과 전·후에 설치된 응용프로그램의 시간 차이가 많을 경우 구체적인 시간정보를 획득하는 것은 제한될 수 있으나, 프로그램의 실행 순서 또는 사건의 전·후 관계 등을 파악할 수 있는 단서로 활용될 수 있다.

5) http://www.revouninstaller.com

5.3 안티포렌식 행위 분석

IconCache.db 파일은 사용자가 외장형 저장매체에 있는 실행파일을 열람하거나 복사・실행 할 경우에도 관련 응용프로그램의 아이콘 캐시 정보를 기록한다.

Fig. 17.을 보면 USB에 저장된 Eraser 프로그램을 단순히 열람만 했음에도 불구하고, IconCache.db 파일에는 F드라이브에 저장된 Eraser 프로그램에 대한 정보가 기록된다.



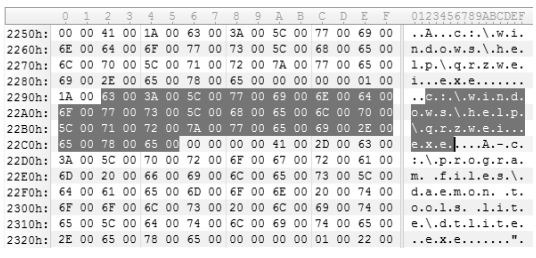
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
9AB0h:	00	69	00	74	00	6F	00	72	00	5C	00	70	00	72	00	6F	.i.t.o.r.\.p.r.o
9AC0h:	00	63	00	6D	00	6F	00	6E	00	2E	00	65	00	78	00	65	.c.m.o.n...e.x.e
9AD0h:	00	00	00	00	00	08	04	19	00	CC	00	00	00	18	00	66	.....Ì.....f
9AE0h:	00	3A	00	5C	00	74	00	65	00	73	00	74	00	5C	00	65	.:.\.t.e.s.t.\.e
9AF0h:	00	72	00	61	00	73	00	65	00	72	00	20	00	36	00	2E	.r.a.s.e.r. .6..
9B00h:	00	30	00	2E	00	31	00	2E	00	65	00	78	00	65	00	B8	.0...1...e.x.e.¸
9B10h:	F6	6F	04	08	00	01	00	F4	00	00	00	18	00	66	00	3A	öo.....ô.....f.:
9B20h:	00	5C	00	74	00	65	00	73	00	74	00	5C	00	65	00	72	.\.t.e.s.t.\.e.r
9B30h:	00	61	00	73	00	65	00	72	00	20	00	36	00	2E	00	30	.a.s.e.r. .6...0
9B40h:	00	2E	00	31	00	2E	00	65	00	78	00	65	00	B8	F6	6F	...1...e.x.e.¸öo

Fig.17. Eraser program stored in a USB

따라서 사용자가 USB에 완전삭제 프로그램을 저장하고 있거나, 그것을 활용하여 컴퓨터에 저장된 증거자료를 삭제하였을 경우, IconCache.db 파일 분석을 통해 사용자의 안티포렌식 행위에 대한 단서를 찾을 수 있다.

5.4 악성코드 침해 분석

악성코드의 경우 컴퓨터 사용자가 일반적으로 접근하지 않거나 인지하기 어려운 장소에 저장된다. 때문에 악성코드에 감염되었을 경우 감염여부 인지와 더불어 악성코드가 설치된 위치를 찾는 것이 쉽지 않다.



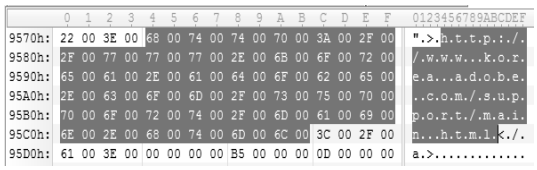
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2250h:	00	00	41	00	1A	00	63	00	3A	00	5C	00	77	00	69	00	..A...c.:.\.w.i.
2260h:	6E	00	64	00	6F	00	77	00	73	00	5C	00	68	00	65	00	n.d.o.w.s.\.h.e.
2270h:	6C	00	70	00	5C	00	71	00	72	00	7A	00	77	00	65	00	l.p.\.q.r.z.w.e.
2280h:	69	00	2E	00	65	00	78	00	65	00	00	00	00	00	01	00	i...e.x.e.....
2290h:	1A	00	63	00	3A	00	5C	00	77	00	69	00	6E	00	64	00	..c.:.\.w.i.n.d.
22A0h:	6F	00	77	00	73	00	5C	00	68	00	65	00	6C	00	70	00	o.w.s.\.h.e.l.p.
22B0h:	5C	00	71	00	72	00	7A	00	77	00	65	00	69	00	2E	00	\.q.r.z.w.e.i...
22C0h:	65	00	78	00	65	00	00	00	00	00	41	00	2D	00	63	00	e.x.e.....A.-.c.
22D0h:	3A	00	5C	00	70	00	72	00	6F	00	67	00	72	00	61	00	:.\.p.r.o.g.r.a.
22E0h:	6D	00	20	00	66	00	69	00	6C	00	65	00	73	00	5C	00	m. .f.i.l.e.s.\.
22F0h:	64	00	61	00	65	00	6D	00	6F	00	6E	00	20	00	74	00	d.a.e.m.o.n. .t.
2300h:	6F	00	6F	00	6C	00	73	00	20	00	6C	00	69	00	74	00	o.o.l.s. .l.i.t.
2310h:	65	00	5C	00	64	00	74	00	6C	00	69	00	74	00	65	00	e.\.d.t.l.i.t.e.
2320h:	2E	00	65	00	78	00	65	00	00	00	00	00	01	00	22	00	..e.x.e.......".

Fig.18. Malicious code path information

그러나 Fig. 18.과 같이 IconCache.db 파일에 저장된 악성코드 "qrzwei.exe"[6]의 아이콘 캐시정보를 통해 "c:\windows\help\qrzwei.exe" 경로에 악성코드 "qrzwei.exe"가 저장되어 있음을 확인할 수 있다.

5.5 기타 프로그램 실행 흔적

IconCache.db 파일은 외부 저장매체에 저장된 응용프로그램의 아이콘 정보뿐만 아니라 CD/DVD에 저장된 응용프로그램의 정보도 포함하고 있다. 또한 인터넷을 통해 응용프로그램을 다운로드 할 경우 응용프로그램을 다운로드 받은 인터넷 URL 주소를 Fig. 19.와 같이 저장하고 있다.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
9570h:	22	00	3E	00	68	00	74	00	74	00	70	00	3A	00	2F	00	">.h.t.t.p.:./.
9580h:	2F	00	77	00	77	00	77	00	2E	00	6B	00	6F	00	72	00	/.w.w.w...k.o.r.
9590h:	65	00	61	00	2E	00	61	00	64	00	6F	00	62	00	65	00	e.a...a.d.o.b.e.
95A0h:	2E	00	63	00	6F	00	6D	00	2F	00	73	00	75	00	70	00	..c.o.m./.s.u.p.
95B0h:	70	00	6F	00	72	00	74	00	2F	00	6D	00	61	00	69	00	p.o.r.t./.m.a.i.
95C0h:	6E	00	2E	00	68	00	74	00	6D	00	6C	00	3C	00	2F	00	n...h.t.m.l.</./.
95D0h:	61	00	3E	00	00	00	00	00	B5	00	00	00	0D	00	00	00	a.>.....µ.....

Fig.19. Stored URL address during application downloads from the Internet

그리고 네트워크를 통해 공유된 컴퓨터에 저장된 응용프로그램을 열람 및 실행할 경우에도 공유된 컴퓨터와 응용프로그램의 이름을 확인할 수 있다. 네트워크에서 공유된 컴퓨터 "sylar"에 저장된 응용프로그램 "jd-gul.exe"를 열람하자 Fig. 20.과 같이 IconCache.db 파일에 관련 기록이 저장된다.

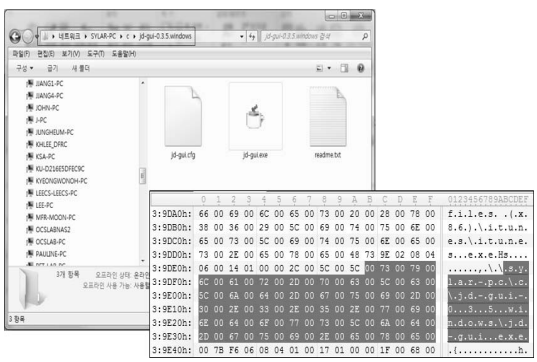


Fig.20. Viewing the shared icon on shared folder

위 실험에서 보는 바와 같이 IconCache.db 파일 분석을 통해 악성코드 탐지 및 인터넷을 비롯한 네트워크에서의 사용자 행위를 분석할 수 있다.

5.6 IconCache.db 파일 분석 도구 소개

현재까지 분석된 IconCache.db 파일 구조를 바탕으로 Windows 7·8에서 사용할 수 있는 IconCache.db 파일 분석 도구(Fig. 21.)를 개발하였다. 분석도구는 인터넷[6]에서 다운받아 사용 할 수 있다.

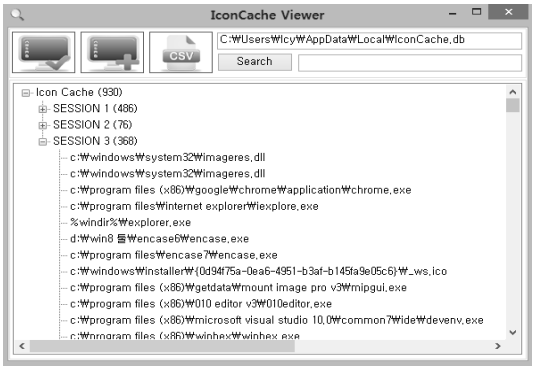


Fig.21. IconCache_Viewer for Windows Vista, 7 and 8

VI. 결론 및 향후 연구방향

IconCahe.db 파일은 사용자가 실행하거나 열람, 설치, 복사, 저장한 응용프로그램의 아이콘 이미지와 경로정보를 저장하고 있어, 안티포렌식 행위에 대한 흔적을 탐지할 수 있다. 또한 악성코드를 비롯해 인터넷 및 네트워크를 통해 다운로드 또는 열람한 파일에 대한 정보도 확인 할 수 있다. 때문에 디지털 포렌식 관점에서 사용자 행위를 분석하는데 의미 있는 자료로 활용될 수 있다.

아쉽게도 IconCache.db 파일은 아이콘 캐시정보에 대한 시간정보를 가지고 있지 않은 단점이 있다. 그러나 분석가가 기존의 디지털 포렌식 분석방법과 융합하여 활용한다면, 삭제된 파일의 상대적인 설치시간 정보와 같은 의미 있는 결과를 얻을 수 있다.

Windows Vista·7·8 버전용 IconCache.db 파일 분석도구는 아직 경로정보만을 분석할 수 있다. 때문에 향후 연구에서는 윈도우의 기본 아이콘을 사용하지 않는 응용프로그램의 아이콘 이미지 데이터에 대한 추가 연구를 통해 아이콘 이미지 데이터까지 분석할 수 있는 도구를 개발할 예정이다.

6) https://code.google.com/p/icon-cache-viewer/

References

[1] Harlan Carvey, "The Windows Registry as a forensic resource," Digital Investigation, vol. 2, issues. 3, pp. 201-205, Sep. 2005.

[2] Harlan Carvey, "Windows forensic analysis DVD toolkit, second edition," Syngress, p.296, chapter 5, May. 2009.

[3] Jan Collie, "The windows IconCache. db: A resource for forensic artifacts from USB connectable devices," Digital Investigation, vol. 9, issues 3-4, pp. 200-210, Jan. 2013.

[4] Vivienne Mee, Theodore Tryfonas and Iain Sutherland, "The Windows registry as a forensic artifact: illustrating evidence collection for Internet usage," Digital Investigation, vol. 3, issues 3, pp. 166 - 173, Jul. 2006.

[5] Eoghan Casey, "Handbook of Computer Crime Investigation: Forensic Tools and Technology," Elsevier, p. 152, Oct. 2001.

[6] KISA, "Forensic technique research in the new operating system" Research Report, pp. 101-108, Sep. 2012.

〈저자소개〉

이 찬 연 (Chan - Youn Lee) 학생회원
2003년 3월: 육군사관학교 독일어과 졸업
2013년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호, 디지털 포렌식, 안티포렌식

이 상 진 (Sang - Jin Lee) 종신회원
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 대칭키 암호, 정보은닉이론, 디지털 포렌식