정 보 보 호 학 회 지
제26권 제5호, 2016. 10

윈도우즈 시스템 포렌식

전 상 준*

요 약

디지털 포렌식은 전자 증거를 사법기관에 제출하기 위해 데이터를 수집, 분석, 보고서를 작성하는 일련의 작업을 말한다. 초기에는 "컴퓨터 포렌식"이라고도 불렸지만 사회 전반에 걸쳐 디지털 기기가 범람하고, 또 기술 적용 범위가 컴퓨터(서버나 데스크탑)에 국한되지 않기에, 점차 디지털 포렌식이라는 용어로 정립되어 왔다. 그 중에서도 윈도우즈 포렌식(Windows Forensics)는 국내에서 가장 점유율이 높은 운영체제인 윈도우즈 패밀리를 대상으로 한다는 점에 있어 효용성이 높고, 앞으로도 꾸준히 발전해야 하는 기술이다. 본 논문에서는 윈도우즈 포렌식에 대한 기본 사항에 대해 정리하며 현재 기술 수준에 대해 짚어보고, 앞으로의 발전 방향에 대하여 논하고자 한다.

Ⅰ. 서 론

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변환하고 있다.사회 전반의 전산화가 진행됨에 따라 현대의 대부분의 기록은 디지털 데이터의 형태로 이루어지고, 사회 대부분의 사건, 사고에 디지털 기기가 연관됨에 따라 디지털 데이터를 과학적으로 분석하여 범죄 사실을 규명하는 디지털 포렌식 기술이 매우 중요하게 되었다. 디지털 포렌식 기술은 디지털 데이터를 제한 없이 다룬다는 점에 있어서 그 범위가 매우 넓다. 하지만 그 중에서도 윈도우즈 운영체제를 대상으로 하는 윈도우 포렌식은 국내 전산 기술 발달의 중심에 있어왔고 여전히 높은 점유율을 가진 윈도우즈를 대상으로 한다는 점에 있어서 그 중요도가 매우 높다.

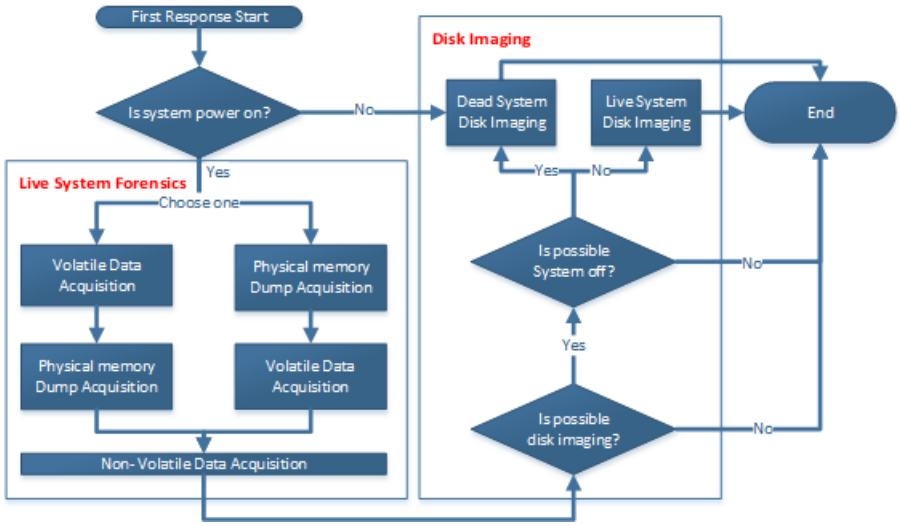
윈도우 시리즈는 지난 수십 년간 국내 PC 사용자들의 주 운영체제로 사용되어 왔다. 이러한 점 때문에 윈도우즈에서 구동되는 것을 목적으로 한 응용프로그램 또한 매우 다양하게 개발되어온 것이 사실이다. 수 많은 상업용 프로그램에서부터 규모가 작은 실험용 프로그램까지 매우 많은 응용프로그램 풀을 가진 것 또한 윈도우즈 사용자들에게는 큰 매력이라고 할 수 있다. 이렇게 다양하게 존재하는 응용프로그램은 각각이 남기는 흔적에 따라 디지털 포렌식 분석가들에게도 많은 분석의 기회를 제공하고 있다. 하지만 응용프로그램의 다양성은 일관된 분석 기술의 사용을 방해하기 때문에 그만큼 분석에 대한 부담을 가중시키는 영향도 없지 않다. 응용프로그램의 다양성 뿐 아니라 윈도우 시스템의 구동에 따른 흔적 역시 다양한 번들 프로그램으로부터 남기 때문에 다양한 흔적을 다양한 기술을 통해서 분석을 진행해야 한다. 따라서 안정적이고 깊이 있는 윈도우 포렌식 분석을 수행하기 위해서는 상대적으로 분석가들의 노력이 더욱 많이 필요한 실정이다.

본 논문에서는 윈도우 시스템 분석을 위해 다루어야 할 수집에서부터 분석 기술까지의 전반적인 디지털 포렌식 요소를 살펴보며 현재의 기술 수준에 대해 짚어보고 향후의 발전 방향에 대해 논하고자 한다.

Ⅱ. 데이터의 수집 (초기 대응)

디지털 포렌식 조사에서 초기 대응은 조사를 수행하기 위해 사건 현장에서 우선적으로 이루어지는 일련의 과정을 의미하며, 때에 따라 현장 대응이라고 불리기도 한다. 초기대응의 절차에 정답은 없지만, 보통 휘발성이 강한 순서로 데이터를 수집하는 것이 바람직하다. 포렌식 조사관이라면, 조직의 상황과 조사의 목적에 맞게 적당한 초기 대응 절차를 마련할 필요가 있다. [그림 1]은 초기 대응 절차의 예시를 나타내며, 초기 대응의 전체 과정은 활성시스템 포렌식 조사(Live System Forensics)와

* 고려대학교 정보보호대학원 (heros86@korea.ac.kr)



〔그림 1〕 초기 대응 기본 절차 순서도

디스크 이미징(Disk Imaging) 과정으로 나뉜다.

2.1. 활성시스템 포렌식

활성 시스템 (Live System)이란, 전원에 연결되어 정상적으로 가동 중인 시스템을 의미한다. 그리고 활성 시스템 포렌식 (Live System Forensics)은 말 그대로, 디지털 포렌식 조사 과정 중 활성 시스템을 마주한 경우 이루어지는 절차를 의미한다.

[그림 1]에서 좌측 네모박스는 활성 시스템 포렌식 조사 단계를 개략적으로 나타낸 것이다. 해당 절차는 초기 대응(First Response)의 한 부분이기도 하며, 그림에서 알 수 있듯이 데이터의 분석 보다는 활성 상태에서 수집 가능한 모든 데이터를 최대한 수집하는 데 초점이 맞추어져 있다. 이 때, 휘발성 데이터의 수집과 물리 메모리의 수집은 상황과 여건에 따라 순서를 바꾸어도 크게 무관하지만, 시간에 따른 데이터의 변화가 상대적으로 적은 비휘발성 데이터보다는 먼저 수집되는 것이 바람직하다.

2.1.1. 휘발성 데이터의 수집

휘발성 데이터란, RAM과 같은 휘발성 메모리에 저장되어, 전원이 꺼지면 사라지는 데이터를 의미한다. 그 특성 때문에, 활성 상태의 시스템에서만 획득 가능하며, 수집 시점에 따른 상태의 변화가 발생할 수 있으므로 신속한 수집이 매우 중요하게 여겨진다. 따라서 조사자는 사건 현장에 도착 시 시스템 전원이 켜져 있는 경우 휘발성 데이터에 대해 우선적으로 수집하는 것이 옳다.

이러한 휘발성 데이터의 수집에는, 물리 메모리 전체의 내용을 복사(덤프)하는 방법과 시스템 명령 등을 이용하여 필요한 정보를 텍스트나 파일 형태로 추출하는 방법이 있다. 각각의 방법에는 장·단점이 존재하는데, 물리 메모리 전체를 수집하는 방법은 휘발성 데이터 전체를 빠짐없이 수집하여 잔존 패스워드를 추출할 수 있도록 하는 등, 정밀한 조사를 가능하게 한다. 하지만, 수집 과정에서 시스템에 손상을 줄 수 있는 위험이 존재하고 수집 후 원하는 정보 획득을 위해서는 추가적인 분석 기술을 갖추어야 하는 부담이 동시에 존재한다.

반면, 시스템 명령어를 이용해 조사에 필요한 데이터를 각각 수집하는 방법은 손쉽고 안전하게 필요한 정보를 획득할 수 있다는 장점이 있으나, 시스템 명령 자체가 변조되었을 가능성이 있고, 추출된 결과 자체가 분석 결과이기 때문에, 물리 메모리의 비정형 데이터 분석과 같은 추가 정보를 기대할 수 없고, 조사 결과에 대한 사실관계 입증이 다소 어려울 수도 있다는 단점이 존재한다. 이와 같은 특징이 있지만 최근에는 강력한 물리메모리 수집·분석 도구가 공개됨에 따라 활성 시스템 포렌식 조사 자체가 물리 메모리 조사로 대체되어가는 면도 보인다[1].

[표 1]은 윈도우 포렌식에서 휘발성 데이터 수집 시 고려해야 하는 항목과 관련된 명령어를 개략적으로 나

〔표 1〕 활성시스템 조사 관련 명령

관련 정보	명령어
System information	systeminfo
System time	date /t, time /t
Network connection	netstat -nao
Process List	tlist -vcstm, tasklist -v
Logon users	net sessions, psloggedon
Loaded DLL List	listdlls 〈process_name|pid〉
Handles	handle -a -p 〈pid〉
Open files	net file, openfiles
Open ports	netstat -anob, fport
Command history	doskey /history
Service List	psservice
NIC information	ipconfig /all, promiscdetect
Routing table	netstat -r
Schedule	schtasks
Network drives	net use
Netbios	nbtstat -c
Process dump	userdump 〈pid〉〈filename〉

타낸 것이다. 조사관은 실제 조사에 임하기에 앞서 데이터 수집에 필요한 기본적인 명령어의 실행 결과 등을 미리 숙지하고 조사 환경에 알맞은 명령어를 준비해 둘 필요가 있다[2].

2.1.2. 비휘발성 데이터의 수집

비휘발성 데이터란 휘발성 데이터와 다르게 전원이 꺼져도 하드디스크(HDD)나 SSD와 같은 보조 기억 장치에 남아있는 데이터를 의미한다. 이와 같은 비휘발성 데이터는 디스크 사본 생성 시 획득 가능하지만, 디스크 이미징에 소요되는 시간을 활용한 효율적인 조사를 위해 일부 데이터의 선별 수집이 요구되기도 한다. 비 휘발성 데이터를 선별적으로 우선 수집을 하고자 할 때의 기준에 정답은 없으며, 숙련된 분석가의 판단에 의해 사건에 가장 관련이 깊은 정보를 가진 데이터 중 용량이 크지 않은 것들이 주 수집 대상이 된다.

예를 들면, 윈도우 시스템을 조사하고자 할 때에는 레지스트리 하이브와 이벤트 로그를 추출하여 조사 대상 시스템에 관한 전반적인 정보를 얻고자 할 때가 많다. 이와 같은 조사는 사건 전체에 대한 그림을 그리는데 도움을 준다. 결국 주요 파일에 대한 조사만으로도 올바른 조사 방향이 설정되고, 사본 생성이 완료되는 시점에는 정밀 조사로 유효 증거 획득에 집중하는 등 효율적인 조사를 가능하게 하는 효과를 가질 수 있는 것이다.

이러한 비휘발성 데이터의 수집이 이루어지기 이전에는 반드시 휘발성 데이터의 수집을 수행해야 한다. 휘발성 데이터는 말 그대로, 쉽게 증발할 수 있는 데이터로 시스템의 조사를 위한 작은 운용에도 크게 영향 받기도 하며, 네트워크 접속 상태와 같은 일부 휘발성 데이터는 전원 차단 여부와 관계없이 시간 흐름에 따라 자연스럽게 사라지기도 하기 때문이다.

윈도우 포렌식에서 비휘발성 데이터를 수집할 때 고려가 필요한 목록은 [표 2]와 같으며, 이는 디스크 이미지 분석 시 분석되는 주요 아티팩트의 목록과도 같다.

〔표 2〕 수집 대상 비휘발성 데이터 목록

구분	획득 가능 정보
FileSystem artifact	파일 시스템 구성 정보
Web artifact	웹브라우저 사용 흔적
Event log	시스템 운용 기본 정보
Prefetch and Superfetch	실행파일 사용 흔적
Shortcut	최근 접근 문서 등
Jump lists	최근 접근 문서 등
Recycle.Bin info file	휴지통 사용 정보
Windows System logs	시스템 운용 기본 정보 2
Thumnail	시스템에 존재하는(했던) 멀티미디어 부분 정보
Windows search DB	윈도우 검색 인덱스 정보

2.2. 디스크 이미징

디스크 이미징(Disk imaging)이란 디지털 포렌식 조사를 위해 조사 대상 저장매체의 사본(Image)을 생성하는 것을 의미한다. 그리고 이렇게 생성된 사본을 이미지(Image)파일이라 하며, 저장장치 이미징 절차는 윈도우 포렌식뿐 아니라 저장장치를 가진 매체를 조사할 때에 일반적으로 수행되는 절차이다.

기본적으로, 디스크 사본 생성 기술은 적법절차에 의한 디지털 포렌식 분석이 가능하도록 하기 위하여 개발되었다고 보아도 무방하다. 원본의 훼손을 막고, 반복적이고 안정적인 분석을 가능하게 하는 최선의 수단은 원

본과 동일한 사본을 생성하여 분석하는 것이기 때문이다. 전체 디지털 포렌식 분석 절차에서 디스크 이미징은 초기 대응 과정에 속한다. 초기 대응은 크게 활성 시스템 포렌식과 디스크 사본 생성 과정으로 나눌 수 있으며, 활성 시스템 포렌식을 마친 후에 사본 생성이 가능한 환경이거나, 분석을 위해 디스크를 전달받은 경우라면 반드시 디스크 이미징(사본 생성)을 가장 먼저 수행해야 한다.

2.3. 활성시스템 분석과 디스크사본 분석 비교

디지털 포렌식 조사는 기본적으로 사건에 대한 증거를 수집하기 위해 발전해 왔으므로, 디스크 사본을 획득하여 분석을 진행하는 것이 일반적이다. 포렌식 분석에서 디스크 사본의 획득은, 원본에 대한 온전한 보존 이외에도 대상에 대한 다각적 분석, 안전한 증거 보관 등을 위한 기본적인 조치로서도 필요한 것이다.

하지만, 실제 조사 과정에서는 간혹 아래와 같이 디스크 사본의 수집이 불가능한 상황이 발생하기도 한다.

- 조사 대상에 기업 비밀이나 사용자 개인 정보 등 민감함 데이터가 포함된 경우
- 이미지 획득에 대한 권한이 없는 경우(민간기관의 조사, 영장의 부재)
- 디스크 용량이 과다하여, 허락된 시간 내에 사본 생성이 불가능한 경우
- 사본 생성 과정에서의 오류로 시스템 장애가 발생할 것이 우려되는 경우
- 그밖에도 조사 의뢰자(혹은 대상자)가 사본 생성을 강력히 거부하는 모든 경우

이와 같은 경우에는 활성 시스템 포렌식의 수행만으로 조사를 진행해야 하는 경우가 있다. 반면, 활성 시스템 포렌식(Live System Forensi cs)의 수행은, 조사 대상 시스템에 전원이 들어와 있는 경우에만 가능하다. 활성 시스템에서만 획득 가능한 데이터가 존재하기 때문에, 전원이 켜져 있다면 반드시 활성 상태의 조사를 해야 하지만, 그 시도 자체가 불가능한 경우가 있는 것이다. 따라서 활성 시스템 분석 결과와 디스크 사본에 대한 분석 결과를 교차하여 최종 결과를 도출하는 방법이 항상 유효한 것은 아니다. 그리고 디스크 사본의 수집이 불가능한 경우에는 활성 시스템에서 수집 가능한 데이터만으로 조사를 수행하고, 반대의 경우에는 디스크 사본의 정보로만 모든 정황을 파악해야 한다.

결론적으로, 활성 시스템에서 수집된 데이터와 디스크 사본의 데이터는 그 분석 목적이 다르고, 모두 중요하게 다루어져야 한다고 볼 수 있다.

Ⅲ. 데이터의 분석

윈도우즈 운영체제를 포함한 시스템의 분석은 크게 파일 시스템 분석, 시스템 아티팩트 분석, 윈도우 레지스트리 분석, 메모리 분석으로 나뉠 수 있다. 윈도우 운영체제 파티션에서 주로 사용되는 NTFS 파일 시스템은 메타데이터를 파일 형태로 관리하는 특성상 시스템 아티팩트 분석 과정에서 함께 분석되기도 하지만 파일 시스템의 조사는 저장장치 전체에 대한 일련의 조사라는 점에 있어서 구분될 필요도 있다.

3.1. 파일 시스템 분석

윈도우즈 패밀리는 전통적으로 FAT (File Allocation Table) 계열의 파일시스템을 사용해 왔으며, NTFS (New Technology File System)이 개발된 이후에는 시스템 파티션에서 주로 NTFS를 사용하고 있다. 최근에는 서버용으로 ReFS(Resilient File System)가 개발되어 일부(Windows 2012) 운영체제에서 사용되고 있기는 하지만 여전히 NTFS의 사용률이 매우 높은 상황이다[6].

파일 시스템의 분석은 일반적으로 메타데이터 영역의 분석, 데이터 영역에서의 데이터 추출, 미 할당 영역에서의 데이터 복원에 초점을 맞추어 진행되며, 이는 운영체제의 종류에 상관없이 저장장치가 사용하는 파일 시스템의 특징에 따라 진행되어야 한다는 특징이 있다. Encase, FTK, X-way Forensics, Autopsy 등과 같은 주요 디지털 포렌식 분석 도구는 대부분의 파일 시스템 분석을 지원하며, 그 중에서도 FAT, NTFS 계열의 파일 시스템의 사용률이 높기에 대부분의 파일 시스템 분석 도구에서 기본적으로 지원하는 파일 시스템이기도 하다.

위와 같이 파일 시스템의 분석은 운영체제의 종류에 그 특성이 기인하지는 않는 편이지만, NTFS는 대부분

의 윈도우 시스템 파티션에서 사용되고 있고 구성 특성상 메타데이터를 파일로 관리한다는 특징으로 인해 분석 방법이 다소 구분되는 면이 있다. 메타데이터가 파일 형태로 관리된다는 것은 저장매체의 사본을 생성하기에 앞서 주요 시스템 아티팩트를 수집할 때 함께 수집할 수 있다는 것을 의미하며, 이렇게 수집된 메타데이터는 파일 시스템 구성의 전반적인 면과 기본적인 운용 상태를 알 수 있게 해주므로 분석을 매우 용이하게 진행될 수 있도록 한다. 아래는 NTFS 파일 시스템에서 분석에 주로 활용되는 파일과 그 특징을 기술한 것이다.

- **$MFT :** $MFT(Master File Table)파일은 파일 시스템 내부의 각 파일의 속성 정보를 포함하는 NTFS 파일 시스템의 핵심 메타 파일이다. 여기서 재미있는 것은 $MFT파일의 속성 정보 역시 $MFT 파일에 포함되어 있다는 것이다. 따라서 운영체제는 로딩 시 필요한 파일에 접근하기 위하여 $MFT의 해석을 최우선적으로 진행한다. 그렇다는 것은 포렌식 분석가 역시 파일 시스템의 전체 구성 및 파일의 속성 정보를 확인하기 위해서 $MFT파일을 필수적으로 수집해야 함을 의미한다.

- **$LogFile :** NTFS 트랜잭션 로그 파일이라 불리는 $LogFile은 시스템 오류나 갑작스런 전원 차단 발생 시, 작업 중이던 파일의 복구를 위해 사용한다. 모든 트랜잭션 작업을 레코드 단위로 기록하며, MFT Entry 번호, 변경된 속성, 수정된 위치, 값 등 변경 전, 후의 모든 정보를 상세하기 기록하므로 이를 분석하여 파일 시스템의 사용 이력을 비교적 정확하게 그려낼 수 있다.

- **$UsnJrnl :** $UsnJrnl 역시 보다 안정적인 파일 시스템의 사용을 위하여 Windows 7 이상에서 사용하는 파일 변경 이벤트 관리 로그 파일이다. 응용 프로그램이 특정 파일의 변경 여부를 파악하기 위해 사용하며, 레코드 단위로 순차적으로 저장하여 관리한다. 레코드에는 파일에 어떠한 변화가 일어났는지에 관한 정보가 담겨 있기에 정확하게 분석한다면 $LogFile을 통해 얻은 정보와 조합하여 데이터의 흐름 정보를 얻을 수 있게 된다.

3.2. 시스템 아티팩트 분석

시스템 아티팩트란, 시스템이 운용되면서 사용자 또는 운영체제에 의해 남게 되는 모든 흔적을 의미한다. 결국, 운영체제에 따라 아티팩트의 유형과 조사 대상이 정의되며, 그 항목을 단정 지을 수는 없다. 따라서, 특정 운영체제를 디지털 포렌식 관점에서 분석한다는 의미는 결국 운영체제에 존재하는 아티팩트를 분석한다는 것과도 같다. 이에 더해 디스크 및 주변 네트워크 환경, 저장 장치 등의 특징을 조사한다면 운영체제가 겪었던 일련의 경험을 거의 모두 파악할 수 있을 것이다[9].

[표 4]는 이러한 관점에서 조사 시 살펴볼 필요가 있는 아티팩트의 목록 및 관련 경로 등을 나타낸 것이며, 본 절에서는 윈도우 계열의 시스템을 분석할 때, 조사 대상이 되는 아티팩트의 목록과 그 특징에 관해서 기술한다[10].

- **파일 시스템 아티팩트 :** 파일 시스템과 관련된 분석 내용은 앞서 기술한 바와 같이 디스크 및 파일 시스템 분석 과정에서 통합적으로 다루는 것이 옳다. 하지만 전통적으로 윈도우에서 가장 많이 사용하는 파일 시스템인 NTFS의 경우에는 파일 시스템 메타 데이터를 또다른 파일 형태로 관리하기에, 아티팩트 분석 시 같이 추출하여 분석하기에 용이하고, 시간 흐름에 따른 파일의 상태 등과 같은 정보를 제공하여 시스템 분석에 상당한 도움을 준다는 특징이 있다[11]. 따라서 분석 대상 시스템의 파티션이 NTFS로 포멧되어 있다면 관련 아티팩트를 수집하여 분석을 진행할 필요가 있다.

- **웹 아티팩트 :** 인터넷에 접속하기 위한 목적으로 사용되는 웹 브라우저는 문서작업, 게임과 더불어 PC의 일반적인 사용 목적이기도 하며, 사용자의 성향, 관심사를 파악할 수 있는 흔적을 많이 남기게 되므로 포렌식 조사시 매우 중요한 역할을 한다. 분석가는 주로 웹 히스토리, 웹 캐시, 웹 쿠키, 다운로드 파일 등을 통해 사용자의 웹 브라우저 사용 내역을 조사하게 된다. 또한 인터넷 익스플로러, 크롬, 사파리, 파이어폭스, 오페라가 5대 웹 브라우저로서 주 분석 대상이 되는데, 익스플로러를 제외한 브라우저는 비 윈도우 계열의 시스템이나 모바일 운영체제에서도

〔표 3〕 윈도우 포렌식 조사기술의 분류 예시

Technical Group	Category	Analysis Point	Target
Windows Analysis	Artifact Analysis	FileSystem artifact	*%SystemDrive%₩$MFT %SystemDrive%₩$LogFile %SystemDrive%₩$Extend₩$UsnJrnl...*
		Event log	*%SystemRoot%₩System32₩winevt₩Logs₩security.evtx %SystemRoot%₩System32₩winevt₩Logs₩system.evtx...*
		Prefetchand Superfetch	*%SystemRoot%₩prefetch₩*.pf %SystemRoot%₩prefetch₩*.db*
		Shortcut	*%UserProfile%₩Desktop₩ %UserProfile%₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩...*
		Jump lists	*%UserProfile%₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩AutomaticDestinations₩...*
		Restore point	*%SystemDrive%₩System Volume Information₩...*
		Recycle	*%SystemDrive%₩$Recycle.bin₩<User SID>₩...*
		Windows System logs	*Setupact NetseZtup...*
		System Temp	*%SystemRoot%₩Temp₩...*
		Thumnail	*%UserProfile%₩AppData₩Local₩Microsoft₩Windows₩Explorer₩Thumbcache_##.db*
		Windows search DB	*%SystemDrive%₩Users₩AllUsers₩ApplicationData %ProgramData%₩Microsoft₩Search₩Data₩Applications₩Windows₩Windows.edb*
		etc...	*%SystemRoot%₩system32₩spool₩printers₩ %UserProfile%₩AppData₩Roaming₩Microsoft₩StickyNotes...*
	Registry Analysis	System information	*HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩InstallDate...*
		Application History or Recent	*HKU₩{USER}₩Software₩Classes₩Local Settings₩Software₩Microsoft₩Windows₩Shell...*
		User Information	*HKLM₩SAM₩SAM₩Domains₩Account₩Users₩{RID}...*
		System Recent	*HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RecentDocs₩...*
		Bundle related	*HKLM₩SECURITY₩Policy₩PolAdtEv...*
		Search List	*HKU₩{USER}₩SOFTWARE₩Microsoft₩Search Assistant₩ACMru₩####...*
		External Storage	*HKLM₩SYSTEM₩ControlSet00X₩Enum₩USBSTOR...*
		Autoruns	*HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce₩...*

비슷한 형태로 흔적을 남기기 때문에, 분석 방법을 숙지해둘 경우 분석에 큰 도움이 될 것이다.

- **이벤트 로그 :** 윈도우 이벤트 로그는 윈도우의 특정 동작(이벤트)에 관한 내용을 기록하여 보관하는 바이너리 로그 어플리케이션이다. 사용자의 행위보다는 시스템의 운용 상태를 알 수 있는 정보가 많이 포함되기 때문에, 부정 조사보다는 침해사고 대응에 조금 더 유용하다는 특징이 있지만, 운영체제 설정에 따라 사용자의 기본적인 시스템 운용까지도 파악할 수 있는 로그를 기록하기 때문에, 조사 시 꼭 살펴볼 필요가 있다[13].

- **프리패치 & 슈퍼패치 :** 프리패치는 원래 보조기억장치와 주기억장치의 I/O속도 차이에 따른 시스템 부하를 최대한 극복하고자 자주 사용되는 응용프로그램을 미리 메모리에 로드하기 위해 사용된 윈도우 시스템의 요소이다. 이러한 프리패치는 본연의 역할을 충실히 수행하기 위해 실행파일에 대한 다양한 정보를 내부에 기록해 두고 있다. 따라서 디지털 포렌식 관점에서 실행파일의 사용 흔적을 조사할 때 프리패치에 기록된 내용은 반드시 살펴볼 필요가 있다.

- **바로가기 파일 :** 윈도우 바로가기 파일은 시스템 사용자가 편의를 위해서 사용하는 경우도 많지만, 운영체제가 자동 실행이나 최근 접근한 데이터에 관한

정보를 관리할 때에 사용하기도 한다. 바로가기 파일에는 링크 대상 파일에 관한 생성·접근·수정시간 정보 및 원본 위치 등에 관한 기록을 포함하고 있으므로, 정보 유출에 관한 조사나 시스템 사용에 관한 시간 관계를 정리할 때 유용하게 사용되는 경우가 많다.

- **점프 리스트 :** 점프리스트는 Windows 7부터 추가된 기능으로 바로가기의 확장형이라고 볼 수 있기 때문에, 정보의 해석과 활용은 바로가기 링크 파일과 유사하다. 전용 포멧을 사용하는 .CustomDestinations 파일과 컴파운드 파일 포맷을 사용하는 .automaticDestination-ms파일이 각각 존재하기 때문에, 전용 도구와 컴파운드 뷰어를 활용하여 분석이 가능하다. 바로가기 파일 분석 시 점프리스트가 존재한다면 교차 분석을 진행하는 것이 옳다.

- **시스템 복원 지점 :** 시스템 복원 지점은 안정적인 운영체제의 운용을 위해 주기적으로 시스템의 상태를 기록하여, 중대한 오류가 발생한 경우나 사용자가 원하는 경우 특정 시점으로 시스템의 상태를 돌리기 위해 사용된다. 따라서 시스템 복원 지점은 해당 시점의 시스템의 상태를 기록하며, 각종 아티팩트나 주요 파일을 같이 저장해 두기 때문에, 과거 시점의 시스템 설정 상태 등을 조사할 때 매우 유용하게 사용된다. 다만, 그 크기가 크고 조사 대상의 내용이 비효율적으로 많기 때문에 최후까지 분석이 미뤄지는 경우가 많다.

- **휴지통 및 휴지통 정보파일 :** 휴지통에는 사용자가 임의로 삭제했거나 은닉을 목적으로 이동된 데이터가 존재한다. 윈도우 시스템은 휴지통 폴더 내부에 간단한 형태로 삭제된 파일에 관한 정보를 기록한다. 이에 따라 삭제된 파일의 삭제 시점과 같은 중요 정보를 파악할 수도 있으며, 정보파일에 기록되지 않은 파일은 의도적인 은닉 파일이라고 간주할 수도 있다.

- **시스템 로그 :** 윈도우 시스템도 간단하게 축적해야 할 정보는 텍스트 로그로 기록한다. 대부분, 운영체제 설치 시점부터 지속적으로 발생하는 여러 동작들을 기록하기 때문에 다른 아티팩트와 교차 분석하여 결과의 신뢰도를 높일 수 있는 여지를 주기도 하며, 추가적인 정 역시 제공하는 측면이 있다.

3.3. 윈도우 레지스트리 분석

윈도우 레지스트리는 윈도우 시스템에서 운영체제 및 어플리케이션에 관한 각종 설정 정보를 담고 있는 데이터베이스이다. 초기 윈도우에서는 INI파일을 사용하여 각 프로그램이나 운영체제 구성품 별로 설정 정보를 저장하였는데, 시스템 구성이 복잡해지고 응용프로그램이 많아짐에 따라 종합적인 관리가 어려워지는 문제가 발생하였다. 이에 따라 윈도우는 레지스트리라는 설정 정보 저장 체계를 구성한 것이다.

레지스트리는 그 자체로 하나의 파일 시스템과 같이 체계적으로 정보를 저장한다. 사용자 및 응용프로그램 별로 영역(레지스트리 키)를 나누어 사용할 수 있도록 구성되었으며, 실제 파일 시스템과 같이 계층 구조로 설정 정보를 저장할 수 있기 때문에 INI파일보다 훨씬 체계적으로 설정 정보 저장이 가능하다. 또한, 몇 개의 파일 내부에 모든 정보를 저장하기 때문에 백업, 복원, 내용 검색 등의 관리도 훨씬 용이하다. 이와 같은 레지스트리의 사용은 단지 윈도우 운영체제 뿐 아니라, 윈도우 포렌식에도 큰 영향을 미친다.

운영체제와 응용프로그램은 사용자에게 연속적인 사용성을 제공하기 위해 수많은 정보를 레지스트리에 저장한다. 결국, 시스템 최초 분석 시 레지스트리에 관한 내용만 정밀하게 분석하더라도 시스템에 관한 기본적인 상태는 대부분 파악이 가능하다. 이러한 특징은 하나의 시스템 아티팩트로도 볼 수 있는 레지스트리 분석이 윈도우 아티팩트 분석과 별도로 구분되는 원인이기도 하다.

아래는 레지스트리를 분석할 때, 관심을 두어야 할 부분과 얻을 수 있는 정보에 대해 기술한 내용이다.

- **레지스트리 하이브 파일 :** 레지스트리는 계층구조를 담는 전체 혹은 최상위 단위를 레지스트리 하이브라 칭하고 있으며, 하이브 단위로 파일을 생성하여 관리를 하고 있다. (일부 키는 하이브간의 연동도 존재) 이처럼, 하이브를 담는 파일을 레지스트리 하이브 파일이라고 하며 이와 같은 파일들은 아래와

같은 경로에 존재한다[14].

- %UserProfile%\NTUSER.DAT
- %UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat
- %WinDir%\System32\config\system
- %WinDir%\System32\config\software
- %WinDir%\System32\config\default
- %WinDir%\System32\config\sam
- %WinDir%\System32\config\security

- **시스템 정보 :** 레지스트리에는 시스템의 설치 시점부터, 운영체제 버전 정보를 비롯한 여러 가지 시스템 구성 정보가 상세하게 기록되어 있다. 활성 시스템에서 시스템 관련 정보를 획득하지 못한 경우 가장 편리하게 정보를 확인할 수 있는 방법이 레지스트리를 확인하는 것이며, 활성 시스템 조사 명령으로 확인하지 못하는 내용도 확인이 가능한 경우도 있다.

- **응용프로그램 사용 내역 :** 응용 프로그램 사용 내역은 레지스트리의 주 분석 목적이라고도 이야기 될 만큼 중요하게 다뤄지는 경우가 많다. 레지스트리에는 각각의 응용프로그램이 최근에 사용한 데이터 파일의 위치를 기록하기도 하며, 운영체제 차원에서 응용프로그램 사용 로그를 관리하기도 한다. 이와 같은 정보는 다양한 상황에서 용의자의 행위나 악성코드의 구동 흔적을 파악할 수 있는 중요한 단서가 되기도 한다.

- **사용자 정보 :** 레지스트리는 시스템 사용자에 관한 내용 역시 상세하게 기록한다. 기본적인 계정 정보를 비롯하여 사용자의 홈 경로, 마지막 로그인 시간, 로그인 실패 시간, 패스워드 해쉬 등 다양한 정보를 기록하기 때문에 사용자 계정에 관한 특이점이나 주로 사용된 계정 등에 관한 정보를 파악할 때 용이하게 사용될 수 있다.

- **최근 접근 내역 :** 각각의 응용프로그램도 자체적으로 최근 접근 파일에 관한 내용을 관리하듯이, 운영체제 역시 익스플로러를 통해 최근 접근한 목록을 관리하여 사용자에게 편의를 제공해 준다. 최근 접근 내역은 조사에 도움을 주는 경우가 많다.

- **외장 장치 정보 :** 정보 유출 탐지에 관련된 조사에서 외장 장치에 관한 정보는 굉장히 소중하게 다뤄진다. 시스템 로그인 setupapi 로그에서도 외장 장치 연결에 관한 정보를 찾을 수 있지만, 레지스트리에서 조금 더 정밀하게 내용을 관리하므로, 수집하여 내용을 교차 분석할 필요가 있다.

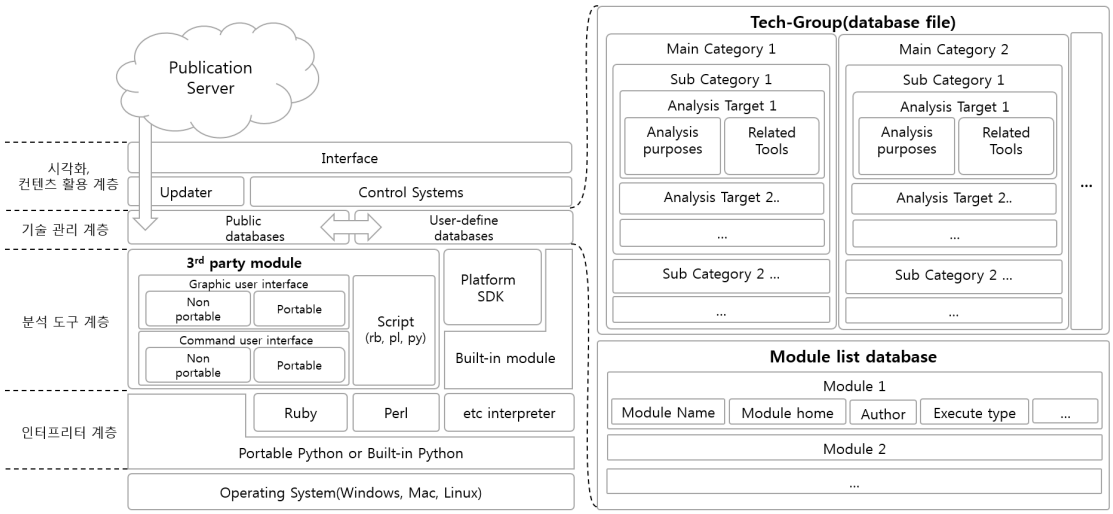
- **자동 실행** : 시스템에 등록된 자동실행 항목(부팅 시, 혹은 특정 상황 시)은 악성코드가 매우 즐겨 사용하는 행위이기 때문에, 침해사고 조사 시 굉장히 유용하게 사용된다. 레지스트리에는 여러 가지 자동실행에 관련된 키가 존재한다. 기서는 소단원에 관한 내용을 간단히 살펴보겠습니다. 게다가 소소단원에 관한 내용도 간단히 살펴보겠습니다.

Ⅳ. 분석 지원 플랫폼 (PFP)

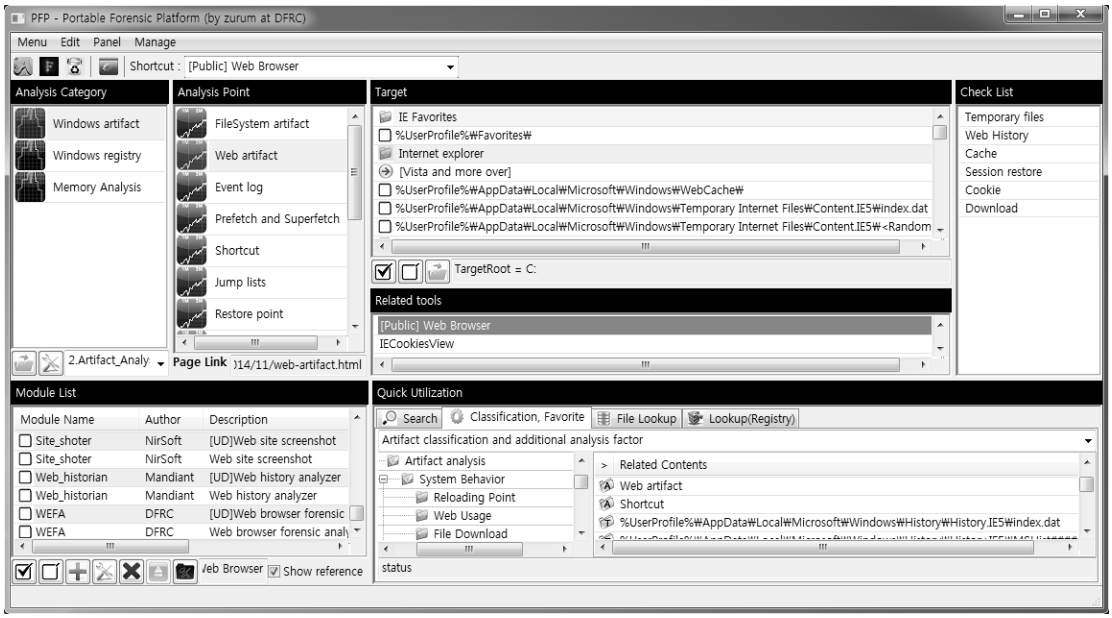
앞서 기술한 바와 같이 디지털 포렌식 분석은 매우 다양한 아티팩트를 교차로 확인하며 사건과 관련된 정보를 획득하는 과정으로 이루어진다. 디지털 포렌식 기술을 위한 아티팩트에는 제한이 없으며, 분석에 도움이 되는 정보를 포함한다면 어떠한 데이터도 아티팩트로 활용될 수 있다.

이러한 특징으로 인해 포렌식 분석을 위한 아티팩트의 종류는 지속적으로 증가될 가능성이 크다. 이로 인해 새로운 포렌식 분석가를 양성하는데 드는 비용은 지속적으로 증가하게 되며 기존의 분석가들은 더욱 어려운 상황에서 분석을 진행할 수밖에 없게 된다. 또한 프로그램은 오류를 내포할 가능성이 크기 때문에 분석 결과와 도구 사용의 신뢰성을 보장하기 위해서는 같은 기능을 하는 다양한 도구를 사용하여 결과를 교차 분석할 필요가 있다.

하지만 조사관들이 여러 가지 상황에서 매번 다양한 도구를 사용하여 분석하는 환경을 구축하기에는 현실적인 어려움이 따른다. 또한 조직 내에 통일된 가이드라인이 없을 경우 조사관의 성향에 따라 상이한 결과가 발생하기도 한다. 이와 같은 점을 고려할 때, 조사관들에게 조사 상황에 알맞는 자동화 도구의 정보와 실행환경이 제공된다면 조사 결과의 신뢰성과 조사 효율을 높이



〔그림 2〕 플랫폼 전체 구조



〔그림 3〕 PFP(Portable Forensic Platform)

는데 크게 도움이 될 것이다.

디지털 포렌식 기술 관리 플랫폼(PFP)은 위와 같은 목적을 달성하기 위해 제작된 프로젝트의 산출물이다. [그림 3]과 같은 구동 화면을 가진 PFP는 [그림 2]와 같은 구조로서 모듈(분석 프로그램) 축적 시스템과, 분석 대상(아티팩트) 축적 시스템 및 컨텐츠의 원활한 활용을 위한 지원 시스템으로 구성되어 있다. PFP는 운용에 필요한 데이터를 SQLite에 적재하며[15], Portable Python을 활용하여 구동되도록 구현되어[16] 휴대성을 대폭 높혔다. 또한, 플랫폼 설계에 따라 중앙 관리 영역에 대한 지속적인 컨텐츠 업데이트를 진행한다. 업데이트에 사용자 정의 컨텐츠는 영향을 받지 않도록 구성되어 있기 때문에, PFP 사용자는 안정적으로 기술을 축적해 나갈 수 있다. 개발된 도구는 http://thesoft.org을 통

해프로그램과 사용자 매뉴얼을 제공하며, 이후에 배포되는 모든 기능 역시 컨텐츠와 함께 자동 업데이트를 통해 전달될 수 있도록 하였다[17].

Ⅴ. 결 론

본 논문에서는 윈도우 포렌식의 현재 상황에 대해 전반적인 내용을 살펴보았다. 윈도우 포렌식은 윈도우즈 운영체제의 점유율이 높은 만큼 그 기술의 중요도가 높기 때문에 디지털 포렌식 기술의 역사와 함께 꾸준히 발전해 왔다. 현재에는 다양한 아티팩트 분석 기술이 꾸준히 소개되고 있으며, 파일 시스템과 레지스트리의 분석 기술도 매우 발전하여 윈도우 시스템에 대해서는 매우 정밀한 분석이 가능한 시점에 이르렀다.

하지만 이렇게 발전해오며 넓어져온 기술 스펙트럼을 소화해야 하는 분석가들의 고충과 이에 따라 부수적으로 발생하는 문제점에 대해서도 짚어 보았다. 이는 자동화된 기술로 해결 가능한 것들이 대부분이었으며 유연하게 설계된 플랫폼으로 문제를 극복함과 동시에 디지털 포렌식의 기술 발전이 안정적으로 이루어질 수 있기에 기술 관리 플랫폼을 소개하였다.

기술 관리 플랫폼에서는 크게 디지털 포렌식 분석 시 유용한 정보를 제공하는 분석 대상과 그에 관련된 정보를 저장, 활용할 수 있도록 하였으며, 지금까지 개발된 다양한 자동화 도구를 포용하고 활용할 수 있도록 구성되었다. 또한 이와 같은 구성 요소를 지능적이며 효율적이게 활용 가능하도록 하는 제어 시스템을 포함하고 있다.

앞으로도 윈도우 포렌식에 대한 중요도는 꾸준히 높아질 것이 예상되며 새로운 기술이 운영체제에 적용됨에 따라 새로운 분석 기술도 꾸준히 요구될 것이다. 빠르게 발전하는 윈도우 포렌식 기술은 꾸준히 안정적으로 축적될 필요가 있으며, 분석가들은 이를 적절히 활용할 수 있도록 꾸준한 노력을 기울일 필요가 있겠다.

참 고 문 헌

[1] Windows Memory Analysis, “http://www.forensicswiki.org/wiki/Windows_Memory_Analysis”

[2] Wikipedia, “COFFE(Computer Online Forensic Evidence Extractor)”, http://en.wikipedia.org/wiki/Computer_Online_Forensic_Evidence_Extractor

[3] PassMark Software, “OSF(OSForen- sics)”, http://www.osforensics.com/do wnload.html

[4] ArxSys, “DFF“, http://www.digital-for-ensic.org/en/

[5] DeftLinux, “DART2”, http://www.deft-linux.net/

[6] Wikipedia, “File System”, https://en.wikipedia.org/wiki/File_system

[7] M Kohn, MS Olivier, JHP Eloff, “Fram ework for a Digital Forensic Investigat ion”, JHP Eloff - ISSA, 2006

[8] M Reith, C Carr, G Gunsch, “An exam ination of digital forensic models”, Inte rnational Journal of Digital Evid ence, 2002

[9] SANS, “Windows Artifact Analysis: Evidence of...”, https://uk.sans.org/poster s/windows_artifact_analysis.pdf010 Editor, Binary Template, http://w ww.sweetscape.com/010editor/templates.html

[10] wikipedia, List of file formats, https:/ /en.wikipedia.org/wiki/List_of_file_formats

[11] Log2Timeline, Log2Timeline, https:// github.com/log2timeline/plaso

[12] Data Structure, https://en.wikipedia. org/wiki/Data_structure

[13] Willi Ballenthin , python-evtx module, http://www.williballenthin.com/evtx/index.html

[14] Willi Ballenthin, python-registry mod ule,http://www.williballenthin.com /registry/index.html

[15] SQLite, The SQLite Database File For mat, https://www.sqlite.org/fileformat 2.html

[16] Portable Python, “Portable Python”, http://portablepython.com/

[17] SangJun Jeon, “Portable Forensic Platf orm”, https://thesoft.org

〈저 자 소 개〉

전 상 준 (Jeon Sang Jun)
정회원

2010년 2월 : 고려대학교 산업시스템정보공학과 졸업
2013년 2월 : 고려대학교 정보보호대학원 박사수료
2013년 1월~2014년 11월 : ㈜안랩 A-FIRST, 연구원
2014년 12월~2016년 2월 : 고려대학교 정보보호대학원 디지털포렌식연구센터, 강사 및 연구원
2016년 3월~2016년 6월 : 김&장 법률사무소 LegalTech, 연구원
2016년 6월~현재 : 프리랜서
관심분야 : 정보보호, 디지털포렌식, 역분석