정 보 보 호 학 회 지
제 32 권 제6호, 2022. 12

File wiping 행위 탐지를 위한 Windows 아티팩트 흔적 분석 연구

주 다 빈*, 이 지 원**, 정 두 원***

요 약

안티 포렌식 기술은 정보보안에는 효과적이지만 해당 기술을 악용하여 증거를 은닉하거나 증거 인멸에 사용할 경우 이로 인해 수사에 걸리는 시간이 길어지거나 수사관이 중요한 증거를 찾기 힘들게 만든다는 점에서 디지털 포렌식 수사에 악영향을 주는 요인으로 작용할 수 있다. 또한 우리나라의 경우 선별압수를 원칙으로 하지만 안티 포렌식 흔적이 발견될 경우 전체압수가 가능해지기 때문에 수사관이 하드웨어 내에서 안티 포렌식 활동이 이루어졌는지 여부를 파악하는 것이 중요하다. 따라서 본 연구에서는 안티 포렌식 중 File wiping 도구의 실행이 Windows 아티팩트에 남기게 되는 흔적을 분석하고 본 연구를 확장시켜 향후 연구의 방향성과 수사관들이 File wiping 도구의 실행 흔적을 손쉽게 파악할 수 있도록 할 수 있는 방안을 모색해보고자 한다.

Ⅰ. 서 론

최근 일상생활에서 컴퓨터가 차지하는 비중이 점점 늘어남에 따라 정보보호에 대한 사회적인 인식이 높아지고 있으며 이로 인해 포렌식 기술로부터 정보를 보호할 수 있는 안티 포렌식에 대한 관심도 함께 높아지고 있다. 안티 포렌식이란 포렌식 과정의 증거 수집, 분석을 방지, 방해하는 것을 목표로 하는 행위를 말하는 것으로, 즉 디지털 포렌식 기술에 대응하여 디지털 증거를 훼손하거나 숨기려는 일련의 행위를 말한다. 안티 포렌식은 용법과 사용 목적에 따라 Artifact wiping, Data hiding, trail obfuscation, Attacks against forensic technology 4가지 종류로 나뉠 수 있으며 이 중 본 논문에서 주목하고 있는 File wiping 기술의 경우 Artifact Wiping에 속하는 기술로 일반적인 삭제 방법으로는 삭제되지 않는 데이터 영역을 완벽하게 삭제하는 기술을 말한다.

이러한 File wiping 기술은 정보를 보호하는 데에는 효과적이지만 증거의 은닉, 인멸, 조작 등 악용될 가능성이 존재한다. 그리고 이러한 행위가 증거물 하드웨어에서 이루어졌을 경우 수사관들이 증거를 발견하기 힘들어지며 이로 인해 수집에 필요한 시간이 증가하게 된다. 또 File wiping 도구를 사용하여 증거 파일이 삭제되었을 경우 수사관들이 해당 파일이 존재했다는 사실 자체를 인지하는데 어려움이 발생하기도 하므로 안티 포렌식 도구의 사용은 효율적이고 정확한 수사를 힘들게 만드는 요인이 될 수 있다. 또한 우리나라의 경우 디지털 증거의 선별압수가 원칙이지만 File wiping 행위가 발견되면 증거 하드웨어의 전체 압수가 가능해진다. 따라서 File wiping 행위를 압수 이전에 파악할 수 있다면 선별압수로 인해 놓칠 수 있는 부분까지 상세한 분석을 할 수 있게 되며 이는 보다 정확하고 효율적인 수사로 이어지게 된다. 따라서 증거물 하드웨어 내에서의 File wiping 행위 여부를 선제적으로 파악하는 것은 포렌식 수사에 있어 중요하다.

본 논문에서는 File wiping 도구가 Windows 운영체제 내 아티팩트에 남기게 되는 흔적을 분석하여 어떤 아티팩트에 흔적이 남는지를 알아보고자 하였으며 향후 연구에서 이를 어떻게 발전시키고 활용할 수 있을지를 살펴보고자 한다. 이를 위해 2장에서는 안티

본 연구는 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2022-0-00281, Development of digital evidence analysis technique using artificial intelligence technology).
* 동국대학교 일반대학원 경찰행정학과 사이버수사전공 (대학원생, wnekqls09@gmail.com)
** 동국대학교 일반대학원 경찰행정학과 사이버수사전공 (대학원생, jiwon2750@dgu.ac.kr)
*** 동국대학교 경찰사법대학 경찰행정학부 (조교수, doowon@dgu.ac.kr)

포렌식과 File wiping 기술의 이론적 배경과 관련된 선행 연구를 알아보고자 한다. 또 3장에서는 해당 논문에서 사용한 연구 방법에 관해 서술하고 4장에서는 이를 통해 도출된 연구 결과에 대해 살펴보고자 한다. 마지막으로 5장에서는 해당 논문의 결론 및 향후 연구 방향에 대해 논하고자 한다.

Ⅱ. 이론적 배경과 선행 연구

2.1. 안티 포렌식 기술

본 절에서는 선행 연구를 통해 분류된 안티 포렌식 기술의 종류에 대해 설명하고, 본 연구에서 집중적으로 다루고자 하는 File wiping 기술에 대해 자세히 설명하고자 한다. Hussein Majed 외 2명[1]의 연구에 따르면 안티 포렌식 도구는 크게 Artifact wiping, Data Hiding, Trail obfuscation, Attack against forensics tools&processes 총 4가지 종류로 나눌 수 있다.

먼저 Artifact wiping 기술은 데이터를 완전하게 삭제하거나 파괴하기 위해 고안된 것으로 Secure wiping이라고 불리기도 한다. 일반적인 삭제의 경우 삭제 대상 파일이나 폴더의 실제 데이터를 가리키는 주소에 대한 정보를 삭제하는 것이기 때문에 실제 데이터에 해당하는 부분은 다른 데이터로 덮어씌워지기 전까지 계속 남아있게 된다. 하지만 Artifact wiping 기술을 사용하여 삭제를 진행하게 되면 도구가 파일이나 폴더의 실제 데이터에 해당하는 부분을 특정 알고리즘을 사용하여 덮어씌우기 때문에 파일의 완벽한 삭제를 위해 해당 기술을 사용한다.

이러한 Artifact wiping 기술은 삭제하고자 하는 대상이 무엇인지에 따라 5가지 하위 분류로 나뉜다. 해당 하위 분류로는 먼저 특정 파일의 데이터를 다른 데이터로 덮어씌우는 File wiping, 특정 디스크나 파티션의 모든 섹터를 삭제하는 Disk/Partition Wiping, 그리고 물리적 방법을 사용하여 저장장치의 모든 내용을 지우는 Disk Degaussing이 있다. 또 레지스트리 내부에 있는 아티팩트를 삭제하는 Registry Wiping, 파일의 메타데이터를 삭제하는 Metadata Manipulation이 있다.

김연수 외 3인의 연구[3]에 따르면 Artifact wiping은 크게 하드웨어적 기술, 소프트웨어적 기술 2가지로도 나뉠 수 있다. 먼저 하드웨어적인 기술은 하드디스크 드라이브와 같은 저장장치에 자기장을 가하거나 전기적인 방식을 사용해 물리적인 손상을 주는 것으로 Disk Degaussing이 이에 해당한다. 소프트웨어적인 기술은 지우고자 하는 부분에 DoD 5220.22-M, Gutmann, Pfitzner 등 여러 알고리즘을 통해 생성된 랜덤 데이터를 사용하여 덮어씌우는 방식으로 인터넷에서 소프트웨어를 다운로드하여 사용한다. 본 연구에서 연구하고자 하는 File wiping이 해당 카테고리에 속하며 File wiping에 대한 설명은 뒤에서 자세히 다루고자 한다.

Data hiding은 저장장치에서 해당하는 데이터의 존재를 감추기 위한 기술로 Artifact wiping과 비슷하지만, Artifact wiping은 파일이나 폴더의 실제 데이터를 지우는 것에 초점을 맞추고 있는데 반해 Data hiding의 경우 데이터의 존재 자체를 지우거나 감추는 기술이라는 데에 차이가 존재한다. Data hiding은 Steganography, Encryption, Network-based Data Hiding으로 나뉘며 이 중 많이 쓰이는 것은 Steganography와 Encryption이다. 여기서 Steganography는 다른 파일 내부에 숨기고 싶은 메시지를 숨기는 기술이며 Encryption은 암호화 알고리즘들로 특정 파일, 데이터베이스, 이메일 또는 디스크를 암호화하여 해당 데이터들의 존재를 감추는 기술이다.

Trail obfuscation은 디지털 포렌식 조사 시 조사관들에게 거짓 기록을 제공하여 혼란을 주는 것을 목표로 하는 기술로 어느 부분에서 혼란을 주느냐에 따라 종류가 나뉜다. 하위 분류로는 먼저 log를 조작하는 Log Manipulation, 신분을 속이거나 공격지를 속이기 위해 IP를 속이는 IP spoofing과 Proxy Server, 중앙 서버나 호스트가 존재하지 않는 P2P Networking이 있다.

마지막으로 Attacks against forensics tools & processes는 단순히 수사관을 속이거나 증거를 감추는 것에 그치지 않고 직접 수사관들의 포렌식 과정에 공격을 가하는 것을 의미하며 Program packers, Attacks against the integrity of investigating parties, AF가 이에 해당한다.

2.2. File wiping

일반적인 삭제의 경우 실제 데이터가 지워지는 것이 아니라 데이터가 저장되어 있는 영역을 가리키고 있는 인덱스가 지워지는 것으로, 실질적으로 저장장치

에 파일의 데이터가 다른 데이터로 인해 덮어씌워지기 전까지는 지워지지 않고 남아있는 것으로 볼 수 있다.

File wiping 기술은 이러한 일반적인 삭제 방식과는 달리 실제 데이터에 여러 종류의 알고리즘을 사용해 생성된 랜덤 데이터를 덮어씌우는 방식으로 실제 데이터를 완전하게 지워 논리적, 물리적인 방법을 통한 복구가 불가능하게 하는 것을 목적으로 하는 기술이다. 파일 자체, 파일의 메타데이터 영역, 덮어 씌워진 메타데이터 영역과 실제 데이터 영역 총 세 가지 종류의 데이터가 File wiping의 타겟이 되는데 이 중 해당 연구에서 주목하는 부분은 첫 번째 타겟인 파일 자체이다. 여기서 파일 자체라는 것은 아직 삭제가 이루어지지 않은 파일의 실제 데이터 영역과 파일 시스템 메타데이터를 말한다. File wiping에는 도구에 따라 각각 다른 알고리즘이 사용되며 보편적으로 많이 사용되는 알고리즘으로는 US DoD 5220.22-M(ECE), US DoD 5220.22-M(E), Peter Gutmann, Pseudorandom Data 등이 있다.

이러한 File wiping 기술은 보안 유지 측면에서 유용하게 쓰일 수 있지만 디지털 증거의 인멸에 사용될 수 있다는 점에서 양날의 검으로 작용할 수 있다는 문제가 존재한다. 이러한 File wiping의 특성 때문에 많은 나라에서 이러한 행위를 불법으로 지정하고 있다.[8]

2.3. Related Works

File wiping에 대한 연구는 꾸준히 이루어져 왔으며 소프트웨어 도구에 집중하고 있다. 해당 절에서는 최근 File wiping 도구와 관련된 선행 연구들에 대해 설명하고자 한다.

Przemslaw외 1인의 연구[2]는 안티 포렌식 기술 중 File wiping, Data hiding, Software credibility undermining 기술에 대해 12가지 도구를 사용하여 실험을 진행하였으며 Heidi Eraser, Free Wipe Wizard 등 총 5가지 도구가 사용되었다. 해당 실험은 도구들이 삭제 대상 파일의 MFT 엔트리, 실제 파일 데이터를 제대로 삭제하는지를 확인하였으며 그 결과 R-Wipe and Clean 도구만이 제대로 모든 흔적을 삭제한 것을 확인하였다. 하지만 해당 연구의 경우 FTK를 사용하여 삭제된 파일을 복구할 수 있는지에 초점을 두고 있어 본 연구에서 다루고자 하는 내용과는 차이가 있다.

김연수 외 3인[3]의 연구에서는 DataEraser, EastTec Eraser 등 총 6개 도구를 사용하여 실험을 진행하였다. 해당 실험은 FAT, NTFS 파일 시스템에서 진행되었으며 파일 시스템에서의 메타 영역과 데이터 영역에 흔적이 남는지, 도구를 설치, 실행, 제거했을 때 생성된 Prefetch 파일의 흔적이 존재하는지, 도구 설치 시 생성된 프로그램 폴더의 흔적이 존재하는지, 레지스트리에 등록된 키값이 존재하는지에 대한 분석을 진행하였다.

Gregory 외 1인[4]의 연구도 File wiping 도구를 대상으로 하고 있으며 Eraser, Evidence Eliminator, Jetico BCWipe 등 총 5개의 도구에 대한 조사를 진행하였다. 해당 연구는 NTUSER.DAT 내의 LastVisitedPidlMRU, OpenSavePidlMRU , CIDSizeMRU 등 총 8개의 아티팩트에 남는 File wiping 도구의 흔적을 확인하고자 하였으며 이 외에도 keyword string search를 통해 다른 아티팩트에 남는 흔적을 찾고자 하였다. 해당 연구는 아티팩트에 대한 분석 외에도 MD5 hash analysis, Internet search analysis, analysis of newly created files 등의 여러 분석을 진행하였다.

Muhammad 외 2인[5]은 Windows 7 환경에서 여러 종류의 파일들을 대상으로 Eraser v6 도구의 동작을 집중적으로 분석하였다. 해당 연구에서는 $MFT에 남아있는 흔적과 메타데이터, resident data와 $LogFile에 저장된 log 등을 조사하는 등 삭제된 대상의 흔적뿐만 아니라 wiping 도구의 흔적에 대해서도 조사를 진행하였다. 또 해당 연구에서는 휴지통을 통해 파일을 삭제하는 것과 완전 삭제의 차이점에 대해서도 추가적으로 다루고 있다.

Bhupendra 외 1인의 연구[6]는 본 연구와 비슷하게 File wiping 도구가 실행되었을 때 Windows 아티팩트에 남기게 되는 흔적에 대한 연구를 진행하였다. 해당 연구는 Windows 운영체제에서 진행되었으며 CCleaner, CleanAfterMe, EasyCleaner 등 5가지 도구를 사용하였다. 각 도구를 실행한 후 Prefetch, Jumplist, lnk, UserAssist, Amcache, IconCache.db, AppCompatFlags 등 총 11개의 아티팩트 내에 남게 되는 흔적을 분석하였다. 분석 결과 Amcache, IconCache.db, AppCompatCache, SRUDB.dat 아티팩트에서 모든 도구의 실행 흔적을 발견하였으나 그 외

아티팩트에서는 도구마다 흔적이 각각 다르게 나타나는 것을 확인하였다.

Graeme[7]는 Windows 10 환경에서 Eraser, Freeraser, DP Wipe 등 총 8개의 도구를 사용해 FAT32 NTFS 파일 시스템에서 삭제를 진행하였다. 해당 연구에서는 삭제 전과 삭제 후 데이터 영역의 차이를 비교하여 각각의 도구가 바꾸는 영역과 변경 방식, 패턴을 분석하였다.

오동빈 외 2인의 연구[8]는 BCWipe, Eraser, Moo0 File Shredder 등 5개 도구를 대상으로 삭제 후 $MFT, $UsnJrnl, $LogFile에 남은 흔적을 분석하였다. 그리고 분석 결과를 토대로 머신러닝 모델을 활용한 자동화된 탐지 시스템을 고안하였으며 평가 메트릭을 사용하여 이를 평가하였다.

Rayed 외 2인[12]은 Windows 10 운영체제에서 SecureDelete, SecureEraser 등 총 4가지 File wiping 도구를 사용하여 실험을 진행하였다. 해당 실험은 FAT32, exFAT, NTFS 파일 시스템에서 진행되었으며 파일시스템마다 남게 되는 아티팩트가 다르므로 파일시스템마다 다른 아티팩트를 분석하였다. 먼저 FAT32과 exFAT의 경우 directory entry, 실제 데이터, file metadata를 살펴보았으며 NTFS의 경우 $MFT, $LogFile, $UsnJrnl, RecentApps Key 등 총 9가지 아티팩트에 대해 분석을 진행하였다. 또 추가적으로 진행된 연구에서는 Resident $DATA attribute analysis, ADS analysis에 대한 분석을 진행하였다.

Marcos 외 2인[9], Mohamad 외 3인[10]의 연구는 Linux 운영체제에서 진행되었으며 포트 스캐닝과 Linux 명령어를 사용하여 연구를 진행하였다. Emre[11]는 Ubuntu Linux와 Windows 운영체제에서 실험을 진행하였으며 메모리 분석을 추가적으로 진행하였다.

이렇듯 기존 연구들의 경우 File wiping 도구가 $MFT, $LogFile, $DATA 영역에 가하게 되는 변화에 집중하고 있는 경우가 대부분이며 아티팩트에 남는 File wiping 도구의 흔적에 대한 연구는 아직 많이 이루어지지 않은 것을 확인할 수 있다. 아티팩트를 다룬 연구들의 경우에도 흔적이 남는지만을 다루고 있거나 각 아티팩트에 대해 하나의 흔적만을 보여주고 있어 하나 이상의 흔적이 남을 경우 이를 알기 어렵고 논문마다 서로 다른 아티팩트를 조사하였기 때문에 종합적인 분석이 힘들다는 한계가 존재한다. 따라서 본 논문에서는 이전에 연구된 아티팩트들을 종합적으로 살펴봄과 더불어 2가지 아티팩트를 추가적으로 분석하고자 하였다.

Ⅲ. 연구 방법

3.1. 실험에 사용된 File wiping 도구

본 연구에서는 일반적인 범죄자들이 증거를 없애기 위한 방식으로 택하기 용이한 소프트웨어 도구를 대상으로 아티팩트에 남기게 되는 흔적에 대해 알아보고자 하였다. 도구는 선행 연구들[7], [10]에서도 활용한 CNET[1]의 정보를 기준으로 다운로드 횟수가 많은 순서대로 상위 5개를 선정하였다. [표 1]은 선정된 도구의 정보를 정리해 놓은 것이다.

〔표 1〕 선정된 File wiping 도구의 정보

File wiping tool	Downloaded file name	hash(MD5)
Glary Utilities	gu5setup.exe	cef857df1df0bb55af6608d7449fb768
Wise Care 365	WiseCare365_5.5.8.553.exe	5edeace198d080c38edfc238fb352839
Eraser	Eraser 6.2.0.2992.exe	eb3a2e8678d65259a76c11198bebcd89
Ashampoo WinOptimizer	ashampoo_winoptimizer_18_18.00.16_sm.exe	a241c19c07b713a5aa7f8c2ddab37cf8
File Shredder	file_shredder_setup.exe	38debb1ffd53d8c1c00a972d2c5e6676

3.2. 실험에 사용된 아티팩트

본 연구에서는 선행 연구에서 다룬 아티팩트와 더불어 File wiping 도구의 실행 흔적이 남을 것으로 예상되는 아티팩트들에 대해 추가적으로 분석을 진행하였다. 해당 실험에 사용된 아티팩트는 Jumplist, Prefetch, UserAssist, AmCache.hve, ShimCache, IconCache.db, IconCache, Thumbcache, CIDSizeMRU, LastVisitedPidlMRU, Open&SavePidlMRU, LNK, SRUDB.dat 총 13개이다.

아티팩트들의 분석을 위해 사용한 도구는 X-Ways Forensic 19.9 SR4 x64, REGA v1.5.3.0, Registry

1) https://download.cnet.com/windows/

Explorer v1.6.0.0, 레지스트리 편집기, Jumplister v1.1.0, JumpList Explorer 1.4.0.0, WinPrefetchView v1.36, UserAssistView v1.02, ThumbCache Viewer Version 1.0.3.6, SRUM_DUMP 2.4이다.

각 아티팩트 별로 흔적이 남는 방식이 상이하므로 각각의 아티팩트마다 프로그램의 실행 여부를 판단하는 데 사용될 시그니처를 지정하였다. 따라서 본 연구팀은 여러 컴퓨터에 프로그램을 설치한 뒤 이를 비교하여 프로그램의 고유한 흔적으로 볼 수 있는 시그니처를 아티팩트마다 지정하였다. 각 아티팩트 별로 지정한 시그니처와 시그니처를 통해 확인할 수 있는 File wiping 도구와 관련된 정보는 다음 표와 같다.

3.3. 분석 방법

3.3.1. 실험 환경

실험에는 Intel(R) Core(TM) i5-10400 CPU 프로세서, 24GB RAM 성능을 가진 하드웨어를 사용하였으며 VMware Workstation 16 Pro 프로그램의 16.2.2 build-19200509 버전으로 가상머신을 생성 및 실행하였다. 가상머신은 Windows 10 Home 64비트 운영체제의 Intel(R) Core(TM) i5-10400 CPU@ 2.90GHz CPU, 2GB RAM으로 설정하였으며 NTFS 파일시스템을 사용하였다. 각각의 가상머신에는 실험 대상 File wiping 프로그램 하나와 아티팩트들을 분석하기 위해 필요한 프로그램들을 설치하였고 txt와 png 파일을 삭제 대상으로 선정하여 실험을 진행하였다.

3.3.2. 실험 방법

실험 방법은 다음과 같다. 먼저 테스트용 가상머신 환경을 생성하고 삭제할 대상 파일들을 다운로드하여 바탕화면으로 옮기고 File wiping 도구와 분석에 필요한 도구들을 다운로드하여 설치한다. 그리고 삭제할 대상 파일들을 File wiping 도구를 사용하여 완전 삭제하고 분석 도구들을 사용하여 앞에서 서술한 방식대로 아티팩트 분석을 진행하였다.

Ⅳ. 분석 결과

분석을 진행한 결과 File wiping 프로그램 대부분이 Open&SaveMRU와 LNK에는 흔적을 거의 남기지 않은 것을 확인하였으며 그 외의 아티팩트들의 경우 대부분의 File wiping 프로그램의 흔적이 남은 것을 확인하였다. 또한 프로그램마다 흔적의 개수와 형태가 다르게 나타나는 것을 확인하였다. 이에 대해 본 연구진은 아이콘 및 썸네일의 개수, 프로그램 실행 방식, 제공하는 기능들이 프로그램마다 다르기 때문이라고

〔표 2〕 각 아티팩트별 시그니처

Artifact	Signature	도구 관련 정보
Jumplist	프로그램 실행 파일 전체 경로	File wiping 프로그램의 실행 파일 이름 및 전체 경로
Prefetch	Processed EXE file name	File wiping 프로그램의 실행 파일 이름
UserAssist	프로그램 실행 파일 경로 (ROT-13 인코딩)	File wiping 프로그램의 실행 파일 이름 및 경로
AmCache.hve - Inventory Application - Inventory Application File	ProgramID	File wiping 프로그램의 ProgramID
AmCache.hve - Inventory Application Shortcut	프로그램 shortcut 경로	File wiping 프로그램의 실행 파일 이름 및 shortcut 경로
ShimCache - AppCompat Cache	프로그램 실행 파일 경로	File wiping 프로그램의 실행 파일 이름 및 경로
ShimCache - AppCompat Flags	프로그램 실행 파일 경로	File wiping 프로그램의 실행 파일 이름 및 경로
IconCache.db	프로그램 이름, 또는 경로 (1바이트 단위로 저장)	File wiping 프로그램의 이름, 또는 경로 (1바이트 단위로 저장)
IconCache	아이콘 Data Checksum 값	File wiping 프로그램 아이콘
ThumbCache	썸네일 Data Checksum 값	File wiping 프로그램 썸네일
Open&Save MRU	프로그램 실행 파일 경로	File wiping 프로그램의 실행 파일 이름 및 경로
LastVisited PidMRU	프로그램 실행 파일 경로	File wiping 프로그램의 실행 파일 이름 및 경로
CIDSizeMRU	프로그램 실행 파일 경로	File wiping 프로그램의 실행 파일 이름 및 경로
LNK	LNK 파일 이름	File wiping 프로그램의 실행 파일 이름
SRUM	Sheet 이름, 프로그램 이름	File wiping 프로그램의 실행 파일 이름

〔표 3〕 아티팩트에 남은 File wiping 흔적

Tool / 아티팩트	Glary Utilities	Wise Care 365	Eraser	Ashampoo WinOptimizer	File Shredder
Jumplist	X	1	X	10	X
Prefetch	12	4	2	5	4
UserAssist	9	3	3	3	3
AmCache.hve - Inventory Application - Inventory Application File	3	3	3	3	3
AmCache.hve - Inventor Application Shortcut	5	5	3	5	5
ShimCache - AppCompat Cache	47	9	1	9	2
ShimCache - AppCompat Flags	3	3	2	2	2
IconCache.db	67	15	12	14	4
IconCache	49	12	9	12	1
ThumbCache	3	6	3	120	1
Open&Save MRU	X	X	X	X	1
LastVisited PidMRU	1	1	1	1	1
CIDSize MRU	1	1	1	1	1
LNK	1	X	X	X	X
SRUM	11	11	5	2	3

추정하였다. 다음 표는 각각의 아티팩트에 도구에 대한 흔적이 남았는지, 남았다면 몇 개의 흔적이 남았는지를 정리한 것이다.

Ⅴ. 결 론

정보보호의 중요성이 대두됨에 따라 자신의 정보를 남기지 않기 위한 안티 포렌식 도구의 사용이 늘어나고 있다. 하지만 이러한 안티 포렌식 도구들은 범죄에 악용되어 조사관들의 포렌식 수사를 더욱 어렵게 하므로 안티 포렌식 도구와 관련한 특정 아티팩트들을 미리 파악하고 이를 활용해 완전 삭제 행위 여부를 식별할 수 있다면 포렌식 수사 관점에서 큰 도움이 될 것으로 예상된다.

이에 따라 본 연구에서는 File wiping 도구가 남기는 아티팩트 흔적을 조사 및 분석하였으며, 아티팩트별로 File wiping 도구의 고유한 흔적이 남게 되는 시그니처를 지정해 아티팩트에 남는 흔적을 분석, 어떤 아티팩트에 흔적이 남았는지를 파악하였다는 것에 의의가 있다.

다만 여전히 신규 File wiping 도구들이 개발되고 있으며 기존의 도구들도 업데이트되는 경우가 많으므로 아티팩트 흔적 조사도 지속적, 주기적으로 수행해야 한다. 또한, 본 연구에서는 Windows 10 운영체제를 중점적으로 다루고 있기 때문에 타 운영체제에서의 File wiping 도구 사용 흔적에 대한 분석도 필요하다. 향후에는 이러한 한계점을 개선하고 File wiping 프로그램 흔적 조사를 자동화하는 방안을 모색하고자 한다.

참 고 문 헌

[1] Majed, Hussein & Noura, Hassan & Chehab, Ali. “Overview of Digital Forensics and Anti-Forensics Techniques”. *The 8th International Symposium on Digital Forensics and Security*. 2020.

[2] Pajek, Przemyslaw & Pimenidis, Elias. “Computer Anti-Forensics Methods and Their Impact on Computer Forensic Investigation”. *Communications in Computer and Information Science*. 45. 145-155. 2009.

[3] Kim, Yeon-Soo & Bang, Jewan & Kim, Jin-Kook & Lee, Sangjin. “A Study of Trace for Data Wiping Tools”. *The Kips Transactions:partc*. 17C. 159-164. 2010.

[4] Carlton, Gregory & Kessler, Gary. “Identifying Trace Evidence from Target-Specific Data Wiping Application Software”. *Journal of Digital Forensics, Security and Law*. 2012.

[5] Zareen, Muhammad & Aslam, Baber & Akhlaq, Monis. “CRITERIA FOR VALIDATING SECURE WIPING TOOLS”. *IFIP International Conference on Digital Forensics*. 321-339. 2015.

[6] Singh, Bhupendra. “Program execution analysis

in Windows: A study of data sources, their format and comparison of forensic capability". *Computers & Security*. 74. 2018.

[7] Horsman, Graeme. "Digital tool marks (DTMs): a forensic analysis of file wiping software". *Australian Journal of Forensic Sciences.* 53. 1-16. 2019.

[8] Oh, Dong & Park, Kyung & Kim, Huy Kang. "De-Wipimization: Detection of data wiping traces for investigating NTFS file system". *Computers & Security*. 99. 2020.

[9] Pereira, Marcos & José, Diógenes & Nascimento, Leonardo. *Forensics and Anti-Forensics a Case Study with Port Scan Intrusion and Data Wipe.* 16-24. 2019.

[10] Wani, Mohamad Ahtisham & Bhat, Wasim & Dehghantanha, Ali. "An analysis of Anti-Forensic capabilities of B-tree file system (Btrfs)". *Australian Journal of Forensic Sciences.* 52. 1-16. 2018.

[11] Hosgor, Emre. "Detection and Mitigation of Anti-Forensics". *International Journal of Computer Science and Information Security,* 18. 46-52. 2020.

[12] AlHarbi, Rayed & Alzahrani, Ali & Bhat, Wasim. "Forensic analysis of Anti-Forensic file-wiping tools on Windows". *Journal of forensic sciences*. 67. 2021.

[13] Park, Kyoung & Park, Jung-Min & Kim, Eun-jin & Cheon, Chang & James, Joshua I. "Anti-Forensic Trace Detection in Digital Forensic Triage Investigations". *Journal of Digital Forensics, Security and Law*. 2017.

[14] Ölvecký, Miroslav & Gabriska, Darja. "Wiping Techniques and Anti-Forensics Methods". *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY).* 2018.

[15] Singh, Bhupendra & Singh, Upasna. "A forensic insight into Windows 10 Jump Lists". *Digital Investigation.* 17. 1-13. 2016.

[16] A. Duby, T. Taylor, G. Bloom, Y. Zhuang, *Detecting and classifying self-deleting windows malware using prefetch files*, pp. 0745 - 0751, 2022.

[17] Narasimha Shashidhar & Dylan Novak. "Digital forensic analysis on prefetch files". *International Journal Of Information Security Science 4* . 39 - 49. 2016.

[18] Singh, Bhupendra & Singh, Upasna. (2016). "Leveraging the Windows Amcache.hve File in Forensic Investigations". *Journal of Digital Forensics, Security and Law.* 11. 37-54. 2016.

〈저자소개〉

주 다 빈 (Dabin Joo)

2022년 8월 : 동국대학교 경찰행정학부 졸업
2022년 9월~현재 : 동국대학교 경찰행정학과 사이버수사전공 석사과정
<관심분야> 디지털 포렌식, 정보보호, 아티팩트 등

이 지 원 (Jiwon Lee)

2022년 8월 : 동국대학교 경찰행정학부 졸업
2022년 9월~현재 : 동국대학교 경찰행정학과 사이버수사전공 석사과정
<관심분야> 디지털 포렌식, 멀티미디어 포렌식, 인공지능 등

정 두 원 (Doowon Jeong)

2019년 2월 : 고려대학교 정보보호대학원 공학박사
2020년 9월~현재 : 동국대학교 경찰사법대학 조교수
2022년 1월~현재 : 동국대학교 융합안전학술원 사이버안전연구센터 센터장
<관심분야> 디지털 포렌식, 정보보호 등