한국정보보호학회
Korea Institute of Information Security & Cryptology

2019 한국정보보호학회 하계학술대회

CISC-S'19

Conference on Information Security and Cryptography-Summer 2019

2019. 6. 20(목)~22(토)

부산 동명대학교 (제1정보통신관, 중앙도서관)

Proceedings

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 동명대학교 TONGMYONG UNIVERSITY

후원 국가정보원 National Intelligence Service Korea, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, IITP 정보통신기획평가원, AhnLab

Windows환경에서의 효율적인 침해사고 분석을 위한 포렌식 도구 커버리지 조사

원혜린*, 박기웅†

*세종대학교 시스템보안연구실, † 세종대학교 정보보호학과

A Coverage Survey of Forensic Analysis Tools for Effective Infiltration Analysis in Windows

Hye-Rin Won*, Ki-Woong Park†

*SysCore Lab., Sejong University.

† Dept. of Computer and Information Security, Sejong University

요 약

정보통신의 기술이 발달하면서 정보의 디지털화가 계속되고 있다. 이에 따라 디지털 정보 탈취 또는 파괴를 목적으로 시스템을 공격하는 사례가 갈수록 늘고 있다. 이러한 침해사고를 분석하기 위해 다양한 포렌식 도구들이 개발되고 있다. 하지만 각 포렌식 도구들은 서로 기능이 다르고 분석할 수 있는 커버리지 또한 서로 상이하기 때문에 원하는 결과를 효율적으로 얻기 위해서는 각 도구의 커버리지를 정확하게 파악하고 침해사고를 분석해야 한다. 따라서 본 논문에서는 Windows 환경에서의 효율적인 침해사고 분석을 위한 포렌식 도구의 기능을 조사하고 커버리지를 분석했다. 본 논문에서의 분석 결과를 통해 분석가가 포렌식 도구를 사용할 때 사용목적에 부합하는 포렌식 도구를 선택하여 침해사고 분석의 효율성을 높일 것을 예상한다.

I. 서론

정보통신의 기술이 발달함에 따라 디지털화된 정보의 양이 늘고 있다. 이러한 디지털 정보를 악용하기 위해 시스템을 공격하는 사고가 계속해서 발생하고 있다. 이에 따라 포렌식 연구에 대한 중요성이 커지게 되었고 침해사고 분석을 위한 다양한 포렌식 도구들이 개발되고 있다.

현재까지 국내외에서 개발된 포렌식 도구는 매우 다양하다 [1, 2, 3, 4, 5, 6]. 각 도구들은 서로 다른 특징과 커버리지를 가지고 있기 때문에 분석 대상의 시스템 상황이나 침해사고 유형에 적합한 포렌식 도구를 선택해서 사용해야 한다. 만약 사용자가 목적에 부합하지 않은 포렌식 도구를 사용하게 된다면 원하지 않은 결과를 얻게 되거나 필요이상의 시간이 소모될 수 있다. 따라서 분석가는 효율적인 침해사고 분석을 위해 포렌식 도구의 정확한 커버리지를 파악해서 사용목적에 부합하는 포렌식 도구를 사용해야 한다.

본 논문에서는 효율적인 침해사고 분석을 위해 대표적으로 사용되고 있는 포렌식 도구들의 커버리지를 조사하고 분석했다.

본 논문의 구성은 다음과 같다. 2장은 수집정보 특성에 따라 데이터를 구분하고 각 데이터의 추출 가능한 아티팩트를 분류하였다. 3장은 대중적으로 사용되는 포렌식 도구를 선정하여 특징과 각 도구의 커버리지를 조사하여 분석했다. 그 결과를 바탕으로 4장에서 결론을 낸다.

II. 수집정보 특성에 따른 아티팩트 분류

침해사고가 발생하고 나면 아티팩트라고 하

†교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원(No.2018-0-00420, No.2019-0-00273) 및 한국연구재단 연구과제(NRF-2017R1C1B2003957)의 지원을 받아 수행된 연구임.

는 증거물이 생긴다. 분석가는 아티팩트를 수집하고 분석하여 침해사고 원인 등을 알아낸다. 시스템의 상황에 따라 수집하고 분석해야할 정보는 다르며 크게 휘발성 데이터와 비휘발성 데이터로 나뉠 수 있다. 이 장에서는 휘발성 데이터와 비휘발성 데이터의 아티팩트를 조사하고 유형별로 구분한다.

2.1 휘발성 데이터

휘발성 데이터는 전원이 차단이 되면 더 이상 수집할 수 없는 데이터를 말한다 [7]. 따라서 전원이 차단이 되지 않았다면 우선적으로 수집해야한다. 휘발성 데이터는 메모리에 주로 정보가 담겨 있기 때문에 휘발성 데이터를 수집 및 분석하기 위해서는 메모리를 이미징하고 분석해야 한다. 다음은 휘발성 데이터 중에서 필수적으로 분석을 해야 하는 중요한 유형을 나열한 것이다.

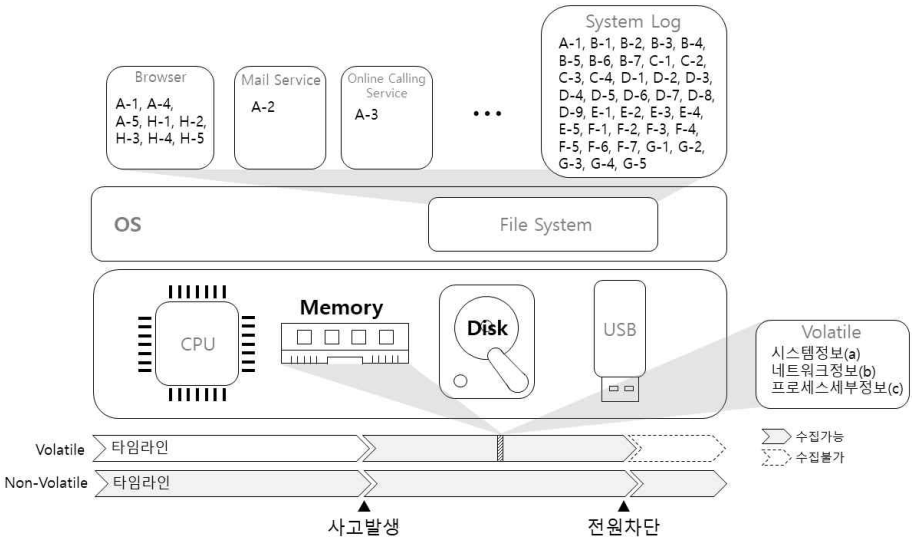
- 시스템 정보 (a) : 사건 구성의 가장 기본적인 정보이며 분석 대상의 데이터에 대한 분석 기준을 제공하기 때문에 중요한 정보이다. 시스템 정보를 통해 침해사고가 발생할 수 있는 취약점에 대한 정보를 얻을 수 있다.
- 네트워크 정보 (b) : 현재 시스템과 연결된 네트워크 정보를 말한다. 네트워크 정보를 통해 허가되지 않은 연결이나 실행중인 프로세스의 네트워크 연결 정보를 알아낸다.
- 프로세스 정보 (c) : 시스템에 악영향을 미치는 악성 프로그램, 이상 프로세스에 대한 정보를 얻기 위해 필요한 정보이다.

2.2 비휘발성 데이터

비휘발성 데이터는 전원이 차단되어도 수집할 수 있는 데이터이다 [8]. 따라서 휘발성 데이터를 수집하고 난 후 수집한다. 비휘발성 데이터는 파일시스템 분석을 위해 디스크를 이미징하고 분석한다. 하지만 분석 시에 많은 영역을 봐야하기 때문에 원하는 정보를 얻기 위해서는 많은 시간이 소모된다. 따라서 침해사고 분석 시에 분석해야 할 유형을 정리해서 목적에 맞게 데이터를 수집하고 분석을 해야 한다. 다음은 [표 1]은 SANS의 Windows Artifact를 참고하여 사용자 활동별 유형을 나열하였다 [9].

[표 1] 수집정보의 특성에 따른 아티팩트 분류

		아티팩트								
		1	2	3	4	5	6	7	8	9
비휘발성데이터	A	Open/Save MRU	E-mail Attachments	Skype History	Index.dat/ Places.sqlite	Downloads.sqlite				
	B	UserAssist	Last Visited MRU	RunMRU Start->RUN	Application Compatibility Cache	Win7 Jump Lists	Prefetch	Services Events		
	C	Open/Save MRU	Last Visited MRU	Recent Files	Office Recent Files	Shell bags	Shortcut(LNK) Files	Win7 Jump Lists	Prefetch	Index.dat file://
	D	Win7 Search-WordWheelQuery	Last Visited MRU	Thumbs.db	Win7 Thumbnails	Win7 Recycle Bin	Index.dat file://			
	E	Timezone	Win7 Network History	Cookies	Browser Search Terms					
	F	Key Identification	First/Last Times	User	Volume Serial Number	Drive Letter and Volume Name	Shortcut(LNK) Files	P&P Event Log		
	G	Last Login	Last Password Change	Success /Fail Logon	Logon Types	RDF Usage				
	H	Hisroty	Cookies	Cache	Session Restore	Flash&Super Cookies				
휘발성데이터	a	시스템 시간	열려있는 파일 정보	현재 실행중인 프로세스 리스트	현재 실행중인 서비스 리스트	현재 로그인한 사용자 계정	클립 보드 내용	명령어 콘솔 사용 정보		
	b	네트워크 카드 정보	라이팅 테이블	ARP 테이블	TCP 연결 상태	UDP 연결 상태	열린 TCP포트와 연결된 프로세스 정보	열린 UDP포트와 연결된 프로세스 정보		
	c	프로세스 실행 파일의 전체 경로	프로세스를 실행한 계정	부모/자식 프로세스	프로세스가 로드한 라이브러리	사용 중인 네트워크 연결 정보	실행시작 시간			



[그림 1] 각 아티팩트 수집 및 분석을 위해 살펴봐야할 영역

- File Download (A)

메일이나 웹을 통해 다운로드 된 파일이나 프로그램의 경로나 기록 등을 분석하는 유형이다. 다운로드를 통해 악성 코드에 감염이 되는 사례가 많기 때문에 중요한 유형에 속한다.

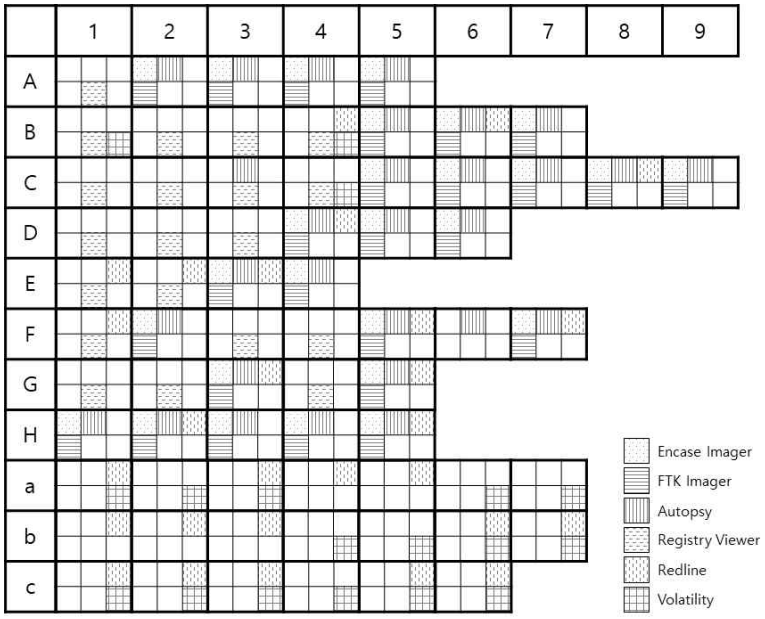
- Program Execution (B) : 악성 프로그램은 사용자 모르게 실행이 되면서 사용자의 정보를 훔치거나 해당 컴퓨터를 느리게 만든다. 프로그램 실행 분석을 통해 본인도 모르게 작동되고 있는 프로그램이나 의심되는 활동을 하는 프로그램을 찾는다.
- File Opening/Creation (C) : 파일을 열거나 생성된 시간이나 순서 등을 분석하는 유형이다. 컴퓨터 사용 중에 발생한 침해사고의 원인이 되는 파일을 찾는다.
- Deleted File or File Knowledge (D) : Thumbnail이나 휴지통 등을 분석해 삭제된 파일 중에 침해사고의 원인이 되는 파일을 찾는 유형이다.
- Physical Location (E) : 시간 정보나 네트워크, 웹 사이트 정보를 찾는 유형이다. 의심이 가는 시간대의 활동이나 외부에서의 접속 시도, 인터넷 사용 기록 등을 찾고 분석하여 침해사고의 원인을 찾는다.
- USB or Drive Usage (F) : USB나 Drive의 정보를 알아내고 연결된 시간, 사용자 등을 찾고 분석하는 유형이다.
- Account Usage (G) : 허가되지 않은 사용자가 로그인하여 침해사고를 발생시킬 수 있다. 이러한 경우 계정 사용에 대한 분석을 해야 한다. 로그인을 시도한 기록이나 유형, 시간 등을 분석해서 악의적인 계정 사용자를 찾는다.
- Browser Usage (H) : 침해사고는 웹 사이트의 방문을 통해 감염이 되는 경우가 많이 발생한다. 침해사고가 발생한 이후 방문한 웹 사이트의 기록 등을 분석해서 원인을 찾아내는 유형이다.

2.3 유형별 아티팩트 정리

[표 1]은 1절과 2절에서 조사한 휘발성과 비휘발성 데이터의 유형별 아티팩트를 정리한 표이다. 또한, 각 아티팩트를 수집하고 분석하기 위해 살펴봐야할 영역을 [그림 1]로 구성했다. [표 1]은 3장에서 포렌식 도구 커버리지 분석 시에 참고가 된다.

III. 포렌식 도구 분석 커버리지 분석

침해사고가 계속해서 발생함에 따라 이를 분석하기 위한 다양한 포렌식 도구들이 개발되고 있다. 각 포렌식 도구의 특성은 서로 다르고 분



[그림 2] 포렌식 도구 커버리지 분석

석할 수 있는 커버리지 또한 서로 상이하다. 이 장에서는 대중적으로 사용되고 있는 포렌식 도구를 선정하여 기능이나 특성을 조사하고 Window7 환경에서 각 포렌식 도구의 커버리지를 분석하였다.

3.1 포렌식 도구 조사

- Encase Imager v7 [1] : Guidance Software에서 개발한 디스크 이미징 도구이며 윈도우 운영체제 환경에서 실행 가능하다. 수집과 분석이 가능하지만 상세 분석을 위해서는 Enscript를 작성해야 하기 때문에 Enscript에 대한 전문적인 지식이 필요하다.
- FTK Imager [2] : AccessData에서 개발한 이미징 도구이다. 디스크뿐만 아니라 RAM과 같은 휘발성 데이터 수집도 가능하다. 수집 외에도 이미지 내의 내용을 확인할 수 있고 휴지통에서 복구한 파일도 확인 할 수 있다.
- Autopsy [3] : 윈도우에서 GUI형태로 이용할 수 있도록 개발된 오픈소스 기반 포렌식 도구이다. 다양한 운영체제의 파일 시스템 내용을 분석할 수 있으며, 검색 및 타임라인 분석, 해쉬 필터링 등의 기능을 제공한다.
- Registry Viewer [4]: AccessData에서 개발한 Windows 운영체제 레지스트리 분석 도구이다. 이 도구는 암호, 사용자 이름 및 기타 정보가 포함되어 있는Protected Storage에 액세스할 수 있다. 또한 중요한 레지스트리 정보를 분석할 수 있는 다양한 기능을 제공한다.
- Redline [5] : FireEye의 Mandiant에서 개발한 메모리 포렌식 도구이다. 물리적 메모리에서 동작하고 있는 프로세스 정보, 파일 시스템 메타 데이터, 레지스트리, 이벤트, 네트워크, 서비스, 웹 히스토리 정보 등을 확인할 수 있다. GUI환경으로 제작되었으면 사용자가 매우 편리하고 쉽게 사용할 수 있다.
- Volatility [6] : 메모리 분석을 위한 대표적인 포렌식 도구이다. 이 도구는 플러그인 형태로 다양한 기능을 제공하고 있는 메모리 포렌식 도구이다. 사용자는 Volatility에서 지원하는 플러그인을 활용하여 메모리부터 필요한 정보를 추출할 수 있다.

3.2 포렌식 도구 분석 커버리지 정리

Windows환경에서 대중적으로 사용되는 포렌식 도구를 선정하여 Window7에서의 각 포렌식 도구 커버리지를 분석했다. 통합 포렌식 도구인 Encase Imager, FTK Imager, Autopsy와 레지

스트리 분석 도구인 Registry Viewer, 메모리 분석 도구인 Redline, Volatility 총 6개의 포렌식 도구가 커버리지 분석에 사용되었다. [그림 2]를 참고하여 분석 결과를 살펴보면 전체를 분석할 수 있는 포렌식 도구는 없었고 파일시스템을 분석할 때 레지스트리 분석 도구를 함께 사용해야 전체를 분석할 수 있었다. 또한 메모리 분석 도구로 휘발성 정보를 분석할 수 있었고 메모리에 있는 일부 레지스트리를 분석할 수 있었다. 하지만 본 논문에 사용된 두 개의 메모리 포렌식 도구는 메모리를 분석하는 도구이지만 분석 커버리지 영역이 완전히 일치하지 않았다.

IV. 결과

본 논문에서는 Windows 환경에서의 효율적인 침해사고 분석을 위해 대중적으로 사용하는 포렌식 도구를 선정하여 각 도구의 기능과 커버리지를 조사하고 분석했다. 분석 결과 전체의 시스템을 분석할 수 있는 포렌식 도구는 없었고 파일시스템 분석 시 레지스트리 분석 도구와 함께 사용해야 했다. 또한 메모리 분석 도구는 휘발성 정보를 분석할 수 있었지만 각 도구에 따라 분석 커버리지 영역은 서로 상이했다. 본 논문의 분석 결과를 통해 분석가가 포렌식 도구를 사용할 때 사용목적에 부합하는 포렌식 도구를 사용하여 침해사고 분석의 효율성을 높일 것을 예상한다.

[참고문헌]

[1] Bunting, Steve, and William Wei. ENCASE COMP. FORENSICS CERTIFIED STUDY GUIDE (With CD). John Wiley & Sons, 2006.

[2] Schweitzer, Douglas. Incident response: computer forensics toolkit. New York: Wiley, 2003.

[3] Carrier, Brian. File system forensic analysis. Addison-Wesley Professional, 2005.

[4] Carvey, Harlan. Windows registry forensics: Advanced digital forensic analysis of the windows registry. Elsevier, 2011.

[5] Pomeranz, Hal. Detecting malware with memory forensics. at. 2015.

[6] Macht, Holger. Live memory forensics on android with volatility. Friedrich-Alexander University Erlangen-Nuremberg, 2013.

[7] Hay, Brian; NANCE, Kara. Forensics examination of volatile system data using virtual introspection. ACM SIGOPS Operating Systems Review, 2008, 42.3: 74-82.

[8] Reith, M., C. Carr, and G. Gunsch. An examination of digital forensic models International Journal of Digital Evidence. 2002.

[9] SANS, https://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf