웹 브라우저 별 일반모드 및 시크릿모드 아티팩트 분석

김성연, 김수빈, 안예린, 조수경

서울여자대학교 정보보호학과 (학부생)

General and Secret Mode Artifact Analysis by Web Browser

SungYeon Kim, SuBin Kim, YeRin An, SuKyung Cho

Seoul Women's University (Undergraduate students)

요 약

웹 브라우저 포렌식은 용의자의 컴퓨터에 저장되는 웹 브라우저 사용 흔적을 디지털 포렌식 적인 방법을 이용하여 조사하는 것을 의미한다. 대부분의 웹 브라우저에서 제공하는 시크릿모드는 일반모드에 비해 적은 아티팩트를 남기는데, 다양한 분석 툴을 사용해 사용자 PC 안의 기록을 살펴보면 시크릿모드의 기록도 확인할 수 있다. 본 논문에서는 주요 웹 브라우저인 Chrome, Internet Explorer, Firefox와 국내 인터넷 회사 Naver가 만든 Whale까지 총 4개의 웹 브라우저 아티팩트에 대해, 사용자의 상황별 PC 상태를 기반으로 일반모드와 시크릿모드의 아티팩트에 대해 분석한 결과를 제시한다.

Ⅰ. 서론

웹 브라우저 포렌식에서의 아티팩트(artifact)란 운영체제나 애플리케이션을 사용하면서 생성되는 흔적을 의미한다. 사용자의 웹 사용 흔적과 검색기록, 자주 사용하는 페이지 등을 분석함으로써 사용자의 성향, 관심사를 파악하고 웹을 통한 정보 유출 가능성을 확인할 수 있는 정보라고 할 수 있다.

인터넷 익스플로러(Internet Explorer)는 마이크로소프트사(Microsoft)에서 개발한 웹 브라우저로, 윈도우 운영체제를 설치할 때 자동으로 설치되는 브라우저이다. 10버전부터 index.dat가 아닌 WebCacheV01.dat에 사용기록을 저장한다.

구글 크롬(Google Chrome)은 구글이 개발한 프리웨어 웹 브라우저이다. 버전 28 이후는 웹킷트의 포크인 블랑크를 사용한다. 구글 크롬은 간단하고 효율적인 인터페이스를 제공하며, 안정성과 속도, 그리고 보안성을 갖는 것을 목표로 하고 있다.

모질라 파이어폭스(Mozilla Firefox) 모질라 재단과 모질라 코퍼레이션이 개발하는 자유 소프트웨어 웹 브라우저다. 주요 특징으로써 개인정보 보호 및 보안을 내걸고 있을 만큼 보안에 각별히 신경 쓰고 있는 것으로 보인다.

네이버 웨일(Naver Whale)은 네이버(Naver)에서 5년 동안 자체적으로 개발해 2017년 09월에 런칭한 브라우저이다. 낡은 환경, 무분별한 보안위험, 불친절한 사용성 등의 문제들을 해결하고자 하는 목적을 지니고 있다. 네이버 웨일은 크로미엄(Chromium) 오픈소스를 기반으로 만들어졌기 때문에, 구글 크롬과 AppData 구조가 굉장히 유사하다.

Web Browser	Application Version	Privacy Product Service	Search Engine
Chrome	84.0.4147.89	Incognito mode	Google
Firefox	79.0	private mode	Google
Internet Explorer	10.0.9200.16384	Inprivate mode	Bing
Whale	2.8.105.22	Secret mode	Naver

표 1. 실험 대상 웹 브라우저

Ⅱ. 분석의 정의

웹 아티팩트는 크게 History, Cache, Cookie, 다운로드 기록으로 나뉜다.

분석을 위해 사용한 툴은 총 다섯 가지이다. 먼저, Volatility를 이용하여 메모리 덤프 파일을 생성할 수 있다. HxD는 AppData를 분석할 때 사용한다. WinHex로는 Pagefile.sys파일과 $MFT파일에 기록된 내용을 확인할 수 있다. IE10 Analyzer는 WebCacheV01.dat 레코드 구문 분석 및 삭제 레코드 복구 툴이다. 여기서 WebCacheV01.dat는 Internet Explorer 10, 11 및 Edge 브라우저에서 사용되는 History, Cache, Cookie 등의 로그를 관리하는 파일이다. DB Browser for SQLite는 SQLite 데이터베이스를 GUI 기반으로 조회할 수 있도록 해주는 툴이다.

해당 툴을 사용해서 찾은 파일들을 통해 검색기록, 방문 웹사이트, 다운로드 기록을 확인할 수 있다.

Ⅲ. 분석예제

상황별 기록된 아티팩트를 파악하기 위해, 다음의 3가지 상황을 만들어 실험을 진행하였다. <상황 1> 환경 조사의 경우, 웹 브라우저 창을 닫고 그 후 30분을 기다리는 과정을 거쳤다. <상황 2> 환경 조사의 경우, 전원을 종료한 다음 브라우저 창을 켰다 끈 후 분석하였다. HxD와 Winhex는 프로세스를 종료하여도 사용이 가능하지만, Volatility는 컴퓨터를 껐다 켠 직후에 프로세스가 실행 중이어야 메모리 덤프 파일을 생성할 수 있기에, 위와 같은 과정을 거쳤다. <상황 3> 환경 조사의 경우, <상황 2>의 환경에서 웹 브라우저 창을 켠 상태로 분석을 진행하였다.

Ⅳ. 연구내용

Internet Explorer 10의 아티팩트 분석 결과를 보면 다음과 같다. 일반모드에서의 검색기록은 모든 상황에서 발견된다. 그 외의 다운로드 기록, 방문 웹사이트 기록도 분석 방법별로 발견된다. 시크릿모드에서 <상황 1>과 <상황 3>의 검색기록은 어디에서도 발견되지 않았다. <상황 1>에서는 메모리 덤프 파일 분석을 통해서만 방문 웹사이트 기록과 다운로드 기록을 확인할 수 있다. <상황 2>에서 가장 많은 흔적이 나타났는데, 모든 검색기록이 나타나진 않았지만 특정한 검색기록은 나타난다. 다운로드 기록과 방문 웹사이트 기록도 나타난다. <상황 3>은 <상황 2>와 비슷하지만, 검색기록이 나타나지 않고 방문 웹사이트 기록을 추측이 가능할 정도로만 나온다는 차이점이 있다. 결론적으로 일반모드는 모든 흔적을 확인할 수 있고, 시크릿모드에서는 특정 상황의 검색기록을 제외한 흔적을 확인할 수 있다.

사진 1. IE10Analyzer를 이용한 Internet Explorer 시크릿모드 <상황 3> 방문기록 탐색 예시

Google Chrome 브라우저의 아티팩트 분석 결과를 보면 다음과 같다. 일반모드의 경우, <상황 1>, <상황 2> 경우가 <상황 3> 경우보다 검색기록이 더 잘 확인된다. <상황 3>의 경우, 메모리 덤프 파일과 History 파일에서만 검색기록을 확인할 수 있었다. 다운로드 기록의 경우, <상황 2>와 <상황 3>의 일반모드에서와 같은 결과를 확인할 수 있었다. <상황 3>에서는 Cache 파일에서도 다운로드 기록이 보이지 않는 것을 알 수 있었다. 시크릿모드의 경우 일반적인 환경에서는 검색기록, 방문 웹사이트 기록이 나오지 않는 것으로 보인다. 검색 결과와 방문 웹사이트 기록을 확인하고 싶다면 <상황 1>에서 메모리 덤프 파일을 뜨는 것을 추천한다. 다운로드 기록의 경우, 세 가지 상황 모두 메모리 덤프 파일에서 기록을 확인할 수 있었다.

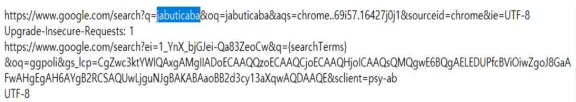

사진 2. 사진 2. Volatility 메모리 덤프 파일을 이용한 Chrome 시크릿모드 <상황 1> 검색기록 탐색 예시

Mozilla Firefox 브라우저의 아티팩트 분석 결과를 보면 다음과 같다. 일반모드에서는 대부분의 파일에서 검색기록, 방문 웹사이트 기록, 다운로드 기록이 모두 보이는 것을 확인했다. 그러나 <상황 1>의 경우 메모리 덤프 파일에서 어떠한 기록도 찾을 수 없었다. 시크릿모드에선 <상황 1>의 경우 메모리 덤프 파일에서 방문 웹사이트 기록, 다운로드 기록을 찾을 수 있었다. <상황 2>에선 어떠한 기록도 남지 않는 것을 확인했다. <상황 3>의 경우 다운로드 기록이 메모리 덤프 파일과 Pagefile.sys에 남아있는 것을 확인했다. 이때 메모리 덤프 파일에선 파일이 저장된 경로가 기록되어 있었고 Pagefile.sys에선 저장된 파일의 이름이 기록되어 있었다. 결론적으로 일반모드에선 모든 기록을 찾을 수 있었으나 시크릿모드에선 검색기록을 제외한 기록들만 찾을 수 있었다.

사진3. WinHex를 이용한 Firefox 시크릿모드 <상황 3> 다운로드 기록 탐색 예시

Naver Whale 브라우저의 일반모드의 경우, 전반적으로 검색기록, 다운로드, 방문 웹사이트 기록이 모든 파일에서 발견된다. 시크릿모드의 경우, <상황 1>에서 검색기록은 어디에서도 발견되지 않는다. 메모리 덤프 파일에서는 방문 웹사이트 기록과 다운로드 기록이 발견된다. <상황 1>에서는 방문 웹사이트 기록과 다운로드 기록이 발견되었지만, <상황 2>에서는 다운로드 기록만 메모리 덤프 파일에 남아있다. <상황 3>은 <상황 2>와 같은 결과를 도출하였다. <상황 3>의 시크릿모드에서의 다운로드 기록은 파일명과 확장자명만 확인할 수 있었다. 하지만 별개의 다른 다운로드 파일들의 경로와 함께 기록되어 있다는 사실을 통해, 해당 파일을 다운로드했다는 추측까지는 할 수 있을 것으로 보인다.

사진 4. Volatility 메모리 덤프 파일을 이용한 Whale <상황 3> 다운로드 기록 탐색 예시

Ⅴ. 결론

웹브라우저별로, 툴마다 확인할 수 있는 내용이 상이했다. Internet Explorer10, Google Chrome, Mozilla Firefox, Naver Whale의 시크릿모드 기록을 가장 많이 볼 수 있는 방법은, 해당 PC를 suspend한 상황에서 메모리 덤프 파일을 뜨는 방법이 비교적 우수했다.

브라우저	기록	상황1	상황2	상황3
Internet Explorer	검색	X	O	X
	다운로드	O	O	O
	웹사이트	O	O	O
Chrome	검색	O	X	X
	다운로드	O	X	X
	웹사이트	O	O	O
Firefox	검색	X	X	X
	다운로드	O	X	O
	웹사이트	O	X	X
Whale	검색	X	X	X
	다운로드	O	O	O
	웹사이트	O	X	X

표 2. 브라우저 별 상황에 따른 시크릿모드 기록 결과

[참고문헌]

[1] Seo Mi-Na 2018-02 “A Comparative Study on the Forensics Analysis of Web Browsers”

[2] Austen Wells “Private Browsing Forensics An Investigation into Private Browsing”

[3] Kim Myung-Hwan 2016-08 “A study on the necessity of digital forensic experts and the way to foster them”