情報保護學會論文誌
第20卷 第5號, 2010. 10

웹 브라우저 다중 사용 환경과 비영어권 국가에서의 인터넷 사용흔적 조사 방법*

이 승 봉,† 이 상 진‡
고려대학교 정보경영공학전문대학원

A Method for Tracing Internet Usage in Multi-use Web browser Environment and Non-English Speaking Countries*

Seung-bong Lee,† Sang-jin Lee‡
Graduate School of information Management and Security, Korea University

요 약

웹 브라우저는 인터넷을 사용하기 위한 필수적인 응용 프로그램이다. 만약 용의자가 범죄 행위 시 웹 브라우저를 사용하였다면, 범죄와 관련된 흔적은 웹 브라우저 로그 파일에 저장이 된다. 따라서 용의자의 컴퓨터에 저장되어 있는 웹 브라우저 로그 파일을 조사 한다면, 사건과 관련된 유용한 정보를 얻을 수 있다. 특히 검색어는 범죄 수사 시 매우 유용한 정보를 제공한다. 그러나 영어가 아닌 언어는 인코딩되어 표현되기 때문에 국내 범죄 수사 시 어려움이 존재한다. 본 논문에서는 웹 브라우저 로그 파일 조사에 관련한 사전 연구와 도구들에 대하여 살펴보고 이러한 로그 파일을 포렌식 관점에서 분석하는 방법을 소개한다. 그리고 소개한 방법을 적용한 도구를 실제 사건에 적용한 사례에 대하여 설명한다.

ABSTRACT

Web browser is essential application for using internet. If suspect use a web browser for crime, evidence related crime is stored in log file. Therefore, we obtain the useful information related crime as investigating web browser log file. In this paper, we look at the related work and tools for web browser log file. And we introduce analysis methodology of web browser log file focus on the digital forensics. In addition, we apply to our tool at real case.

Keywords: Web Browser, Cache, History, Cookies, Keyword, URL Decoding

I. 서 론

많은 사람들이 인터넷을 사용하기 위하여 웹 브라우저를 사용한다. 이것은 용의자 또한 마찬가지일 것이다. 용의자는 범죄를 저지르기 전에 범죄와 관련된 정보를 얻기 위해 웹 브라우저를 사용할 것이며, 범죄를 저지른 후에도 범죄와 관련된 소식을 접하거나 범죄를 은폐하기 위한 방법을 얻기 위해 웹 브라우저를 사용할 것이다. 아니면 웹 브라우저 자체가 범행을 위한 도구로서 사용될 수도 있다. 따라서 디지털 포렌식에서 웹 브라우저 로그 파일을 조사하는 것은 매우 중요한 일이다.

웹 브라우저를 이용하여 인터넷을 이용할 경우, 여러 사용 흔적들이 사용자의 컴퓨터에 남게 된다. 이러한 흔적들은 조사관이 용의자의 컴퓨터를 조사할 때

접수일(2010년 5월 6일), 게재확정일(2010년 7월 11일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술 개발사업의 일환으로 수행되었음.[10035157, 실시간 분석을 위한 디지털 포렌식 기술 개발]
† 주저자, fdc629@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr

범죄와 관련된 유용한 정보를 제공한다. 일반적으로 웹 브라우저 사용 시 컴퓨터에 저장되는 사용 흔적은 히스토리, 임시 인터넷 파일, 쿠키 파일에 저장되며, 웹 브라우저에 따라 기타 몇몇 파일에 추가적인 정보를 저장하기도 한다.

따라서 웹 브라우저 로그 파일을 분석하면 용의자가 웹 브라우저를 이용한 사용 내역을 파악할 수 있다. 현재 웹 브라우저 로그 파일 분석에 대한 여러 논문과 도구가 존재한다. 그리고 이러한 논문과 도구들은 대체로 다음과 같은 특징을 지닌다.

첫째로, 특정 웹 브라우저만을 대상으로 하거나, 특정 웹 브라우저의 특정 로그 파일만을 대상으로 한다. 현재 여러 종류의 웹 브라우저가 사용되고 있고 각각의 특징도 서로 다르기 때문에 한 사용자가 여러 개의 웹 브라우저를 동시에 사용할 수 있다. 이러한 경우 웹 브라우저 별로 따로 분석하는 것은 용의자의 인터넷 사용 흔적을 조사하는데 부적합하다. 또한 인터넷 사용 흔적은 여러 로그 파일에 저장되므로 특정 로그 파일 만을 조사하는 것은 적절치 않다.

둘째로, 로그 파일을 단순히 파싱하여 보여주는 수준에 머물러 있다. 효과적인 분석을 위해서는 좀 더 추가적인 분석이 필요하다.

웹 브라우저 사용흔적 조사에 있어 좀 더 유용한 정보를 획득하기 위해서는 위에서 살펴본 기존 논문들과 도구들의 특징을 벗어나 추가적인 분석방법이 필요하다. 본 논문에서는 위에서 나열한 특징을 벗어난 추가적인 분석방법을 제시한다. 논문의 2절에서는 웹 브라우저 로그 파일 조사에 관한 사전 연구에 대하여 알아보고, 3절에서 관련 도구들에 대하여 살펴본다. 4절에서는 위에서 제시한 문제점을 해결하기 위한 방법을 제시하며 5절에서 적용한 방법을 실제 사례에 적용한 결과를 살펴보고 6절에서 결론을 맺는다.

II. 관련 연구

웹 브라우저 포렌식에 대한 선행 연구는 특정 웹 브라우저를 대상으로 이루어져 왔으며, 로그 파일의 구조 분석에 초점이 맞춰져 있다.

Keith J. Jones는 internet Explorer의 index.dat 파일의 구조와 삭제된 Activity Records를 추출하는 방법을 설명하였으며, index.dat 파일을 분석할 수 있는 도구 Pasco를 소개하였다[1]. Index.dat 파일은 크게 헤더, 해쉬 테이블, Activity Table로 구성되어 있다. 헤더에는 파일의 크기, 해쉬 테이블의 오프셋, 캐쉬 디렉토리 정보가 있으며, 해쉬 테이블에는 다음 해쉬 테이블의 위치와 Activity Record의 위치를 포함하고 있다. Activity Record에는 URL, 접속 시간, 캐쉬 파일의 이름, 캐쉬 파일이 저장된 디렉토리 정보, HTTP 헤더가 포함되어 있다. Index.dat 파일에서 삭제된 Activity Record를 찾아내는 방법은 매우 간단하다. 모든 Activity Record의 위치는 0x80의 배수로 저장되며, 각 Activity Record는 시작부분에 4바이트의 식별자를 가진다. 따라서 실제 Activity Record의 위치와 해쉬 테이블의 Activity Record의 위치 정보를 비교함으로써 삭제 여부를 파악할 수 있다. Pasco는 위에서 설명한 index.dat 파일의 구조를 자동으로 해석하여 보여주는 도구이며, 삭제된 영역까지 추출하는 기능을 지원한다. 이 논문에서 분석 대상이 되는 IE의 버전은 5이며 현재 버전 8까지 출시가 되었지만 논문의 내용은 아직도 적용 가능하다.

Keith J. Jones et al.는 실제 사건을 모방한 가상 사건을 이용하여 IE와 Firefox2 웹 브라우저 포렌식에 대하여 설명하였다[2, 3]. Part1에서는 주로 IE 포렌식에 대하여 설명하고 몇몇 도구들을 소개하였다. IE 포렌식은 위 절에서 설명한 내용과 같으며, 이용 가능한 도구는 크게 공개용 도구(Pasco, Web Historian)와 상용 도구(IE History, FTK)로 나누어 설명하였다. Part2에서는 Firefox2 포렌식을 설명하였으며 주로 캐쉬 파일에 대하여 설명하였다. Firefox2의 캐쉬 파일은 IE 처럼 캐쉬 파일을 있는 그대로 저장하지 않고 별도의 방법으로 저장하므로 캐쉬 파일을 보기 위해서는 파일 구조 분석이 필요하다. Firefox2의 캐쉬 파일은 windows xp에서 "\Documents and Settings\<user name>\Application Data\Mozilla\Firefox\Profiles\<random text>\Cache"에 저장되며, 폴더 안에는 캐쉬 맵 파일, 3가지 캐쉬 블록 파일, 분리된 캐쉬 데이터 파일이 존재한다.

Murilo tito Pereira는 firefox2에서 firefox3로 버전이 올라 가면서 바뀐 새로운 히스토리 시스템에 대하여 자세하게 설명 하였으며, 비할당 영역에서 firefox3의 삭제된 히스토리 정보를 찾는 방법을 제시하였다[4]. firefox3의 히스토리는 SQLite Database 시스템을 사용하며, 포렌식 관점에서 중요하게 조사해야 할 파일은 "Places.sqlite", "Formhistory.sqlite", Downloads.sqlite", "Cookies.sqlite"가 있다. Firefox3는 실행 중에 "Places.sqlite"의

일부 또는 전체 내용을 포함하는 rollback journal 파일을 생성하고 실행이 중지되면 rollback journal 파일을 삭제한다[4]. 따라서 비할당 영역에는 firefox3의 히스토리 정보가 남아있을 가능성이 존재한다. 저자는 논문에서 비할당 영역에서 firefox3의 히스토리 정보를 추출 하는 방법으로 sqlite database의 구조적인 접근 방법을 제시 하였다.

III. 기존 도구

현재 웹 브라우저 포렌식을 위한 도구들이 많이 존재한다. 이번 절에서는 이러한 도구들에 대하여 간략하게 살펴보겠다. [표 1]은 웹 브라우저 포렌식을 위한 도구들과 그 기능을 정리한 것이다.

[표 1]에서 소개한 도구들은 대부분이 특정 웹 브라우저만을 분석하거나, 여러 웹 브라우저를 분석 하더라도 특정 범주만을 분석한다. 앞에서 말했듯이 웹 브라우저의 종류가 다양해지고, 각각의 기능과 성능이 다양해지면서 한 사용자가 여러 개의 웹 브라우저를 동시에 사용할 수 있다. 이러한 상황에서 어느 한쪽의 웹 브라우저 또는 기능에 치우친 분석은 포렌식적으로 잘못된 분석을 초래할 수 있다. 다양한 웹 브라우저 분석과 여러 범주에서 분석하는 도구에는 Cacheback, Encase가 있다. 하지만 Encase는 여러 개의 웹 브라우저를 연관성 없이 분석한다. 포렌식적으로 웹 브라우저 로그 파일을 분석하는 것은 용의자의 인터넷 사용 내역을 추적하고, 일련의 시간 흐름 속에서 범죄와 관련된 증거를 찾는데 있다. 여러 웹 브라우저를 사용한 용의자의 컴퓨터를 조사할 때 연관성을 배제한 분석은 용의자의 인터넷 사용 내역 추적을 어렵게 만들 수 있다. Cacheback은 여러 웹 브라우저의 캐쉬와 히스토리를 서로 관련 지어서 분석할 수 있으므로 현재까지 나와있는 웹 브라우저 로그파일 분석도구로서 가장 적합하다고 볼 수 있다[5]. 하지만 포렌식 분석도구로서 가치가 있기 위해서는 좀 더 심층적인 분석이 필요하다. 본 논문의 제 4 절에서는 웹 브라우저 포렌식에서 필요한 심층 분석에 대하여 자세하게 설명한다.

IV. 심층 분석 방법

현재까지 나와 있는 도구들은 포렌식 분석도구로서 부족하다. 포렌식 조사에서 이러한 도구들이 유용하고 효과적으로 사용되기 위해서는 단순히 데이터를 파싱하고 보여주는 이상의 작업이 필요하다. 이번 절에서는 웹 브라우저 로그파일을 분석하는데 필요한 방법들에 대하여 소개한다.

4.1 통합 분석

웹 브라우저의 종류가 다양해지고 각각의 특장점이 달라지면서 한 사용자가 여러 웹 브라우저를 동시에 사용하는 경우가 늘어나고 있다. 이러한 경우 특정 웹 브라우저의 로그 파일만을 조사해서는 사용자의 사이트 방문 내역을 정확히 추적하기 어렵다. 한 시스템에 여러 웹 브라우저가 설치되었다면 조사관은 이들 모두를 조사할 필요가 있다. 그리고 각각의 웹 브라우저에서 분석한 데이터를 서로 관련시켜 분석하여야 한다. 모든 웹 브라우저의 로그에는 시간 정보를 포함하므로 조사관은 이를 이용하여 서로 다른 웹 브라우저의 로그를 관련시킬 수 있다.

4.2 타임라인 분석

디지털 포렌식 조사에서 용의자의 행위에 대한 일련의 과정을 추적하는 것은 중요하다. 이것은 타임라인 분석을 통해 이루어질 수 있다. 타임라인 분석은 시간 정보를 이용하여 각각의 로그를 시간의 흐름에 따라 나열하여 분석하는 것을 말한다. 조사관은 타임라인 분석을 이용하여 사이트 이동 경로와 각 사이트에서의 행위를 조사함으로서 용의자의 범죄 행위에 대한 전반적인 과정을 추적할 수 있다.

도메인	Path(/../../)	변수(&..=)	값	...	변수(&..=)	값

[그림 1] URL 형식

도메인	Path	변수	값	변수	값	변수	값	변수	값	변수	값	변수	값
google.com	/search	hl	en	source	hp	q	forensic	aq	f	oq		aqi	g10

[그림 2] google 검색 URL 형식

4.3 검색어 추출

웹 브라우저 포렌식에서 용의자의 사이트 방문 내역을 조사하는 것 이외에 중요한 것이 검색 키워드이다. 검색 키워드는 특정 정보를 검색하기 위해 용의자가 입력한 단어 또는 문장이다. 따라서 검색 키워드는 용의자가 범죄 행위와 관련된 정보를 얻기 위해 웹 브라우저를 사용하였다는 정황 증거로서 활용될 수 있으며, 검색 키워드에 따라 범행 동기, 수법, 목적 등의 내용을 파악할 수 있다.

검색 키워드는 URL 내에 포함되어 있다. 일반적으로 URL은 [그림 1]과 같이 구성되어 있다[6].

여기서 도메인과, path를 이용하여 해당 URL이 검색을 위한 것임을 알 수 있으며, 변수의 이름을 이용하여 키워드를 알 수 있다. 예를 들어 google 검색 엔진에서 "forensic"이란 단어를 검색 하였을 경우 다음과 같은 URL 주소가 남게 된다.

- http://www.google.com/search?hl=en&source=hp&q=forensic&aq=f&oq=&aqi=g10

위 URL에서 도메인, path, 변수, 값은 [그림 2]와 같다.

[그림 2]에서 구글의 도메인은 "google.com"이고, path는 "/search"이다. 즉 도메인과 path에서 구글의 검색과 관련된 URL임을 알 수 있으며, 검색 키워드의 값을 나타내는 변수는 'q'임을 알 수 있다. 따라서 도메인이 "google.com"이고 path가 "/search"인

[표 1] 웹 브라우저 포렌식 관련 도구들

이름	분석 웹 브라우저	분석 내용	상용 여부
Pasco	IE 5-8	Index.dat 파일 분석	X
Web Historian 1.3	IE 5-8, Firefox 2 Safari3 이하 Opera 10 이하	히스토리 분석	X
index.dat analyzer 2.5	IE 5-8	Index.dat 파일 분석	X
Firefox forensic 2.3	Firefox 2,3	쿠키, 히스토리, 다운로드, 북마크 및 firefox3의 sqlite database 파일 분석	○
Foxanalysis 1.3.2	Frefox 3	히스토리, 쿠키, 북마크, 다운로드, form History	X
Firefox3 extractor 0.8.9	Firefox 3 Chrome	sqlite database 파일 분석	X
chromeAnalysis 1.0	Chrome	히스토리, 쿠키, 북마크, 다운로드, 검색어, 로그인, archived website history, archived search terms	X
Google chrome forensic 1.3	Chrome	히스토리, 쿠키, 다운로드, 검색어, 로그인 및 기타 sqlite database 파일 분석	○
MozillaHistoryView 1.15	FireFox 2, 3	히스토리 분석	X
IECacheView 1.31	IE	임시 파일 분석	X
IEHistoryView 1.41	IE	히스토리 분석	X
IECookiesView 1.74	IE	쿠키 분석	X
MozillaCacheView 1.26	FireFox 2, 3	임시 파일 분석	X
MozillaCookiesView 1.26	FireFox 2, 3	쿠키 분석	X
MyLastSearch 1.42	Internet Explorer 5-8 Firefox 2, 3 Chrome	주요 포탈 사이트에서 검색한 내용 추출	X
Netanalysis 1.3	IE 5-8, Firefox 2 Safari 3 이하, Opera 9 이하	히스토리 분석	○
Cacheback 2.7	IE 5-8, Firefox 2, 3 Safari 3 이하, Opera 9 이하, Chrome	임시 파일, 히스토리, 쿠키 분석	○
Encase 6.0	IE 5-8, Firefox 2, Safari 3, Opera 9	임시 파일, 히스토리, 쿠키 분석	○

URL에서 변수 'q'의 값을 찾으면 구글에서 검색한 모든 키워드를 추출할 수 있다.

하지만 검색엔진마다 도메인, path, 변수 명이 서로 다르므로 많이 사용되는 검색 엔진의 URL 형태를 조사할 필요가 있다. [그림 3]은 현재 세계적으로 사용되는 검색 엔진의 점유율을 나타낸 것이다[7].

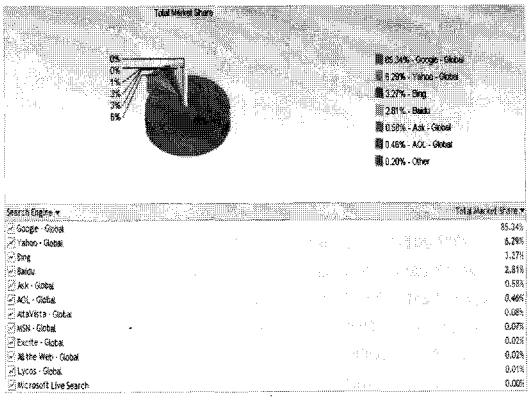
[표 2]는 상위 10위에 랭크되어 있는 검색 엔진의 도메인, path, 키워드를 저장하는 변수 명을 정리한 것이다.

[표 2]에서 알 수 있듯이 검색 엔진마다 도메인, path, 변수 명이 다르므로 한 가지 방법으로 검색어를 추출할 수 없다. 결국 각 검색 엔진의 도메인, path, 변수 명의 형태를 모두 알고 있어야 해당 검색 엔진에서 검색한 키워드를 추출할 수 있다. 하지만 모든 사이트의 URL 형식을 아는 것은 불가능하다. 즉, 알지 못하는 검색 엔진 및 기타 사이트에 대한 검색 키워드를 추출할 수 없다. 따라서 일반적이지는 않지만 상당수를 포함할 수 있는 검색 키워드 추출 방법이 필요하다.

[표 2]를 자세히 살펴보면 상당수 검색 엔진의 도메인과 path에 "search"라는 단어가 들어간 것을 알 수 있다. 또한 대다수의 변수 명이 'q', 'p'인 것을 알 수 있다. 따라서 우리는 도메인과 path에 "search"라는 단어가 포함되고 변수 명이 'q' 또는 'p'를 포함하는 URL에서 검색 키워드를 추출할 수 있다. 이것은 상위 10위에 랭크되어 있는 검색엔진의 60%에 적용할 수 있다. 또한 상위 10위에 랭크되어 있지는 않지만 한국의 검색 포털 사이트 naver, daum, nate와 일본의 검색 포털 사이트 livedoor, 중국의 검색 포털 사이트 netease에도 적용 가능하다.

[표 2] 상위 10위 검색 엔진의 검색 URL 형식

검색 엔진	도메인	path	키워드 변수
Google	googel.com	/search	q
Yahoo	search.yahoo.com	/search	p
Bing	bing.com	/search	q
Baidu	baidu.com	/s	wd
Ask	ask.com	/web	q
Aol	search.aol.com	/aol/search	q
Altavista	altavista.com	/web/results	q
MSN	bing.com	/search	q
Excite	msxml.excite.com	/excite/ws/	results
All the Web	alltheweb.com	/search	q



[그림 3] 검색 엔진 사용자 점유율

위에서 제시한 방법이 적용되지 않는 검색 포털 사이트의 경우 검색 키워드를 추출할 때 각각의 도메인과 path, 변수 명을 임의로 지정하여 검색 키워드를 추출 할 수 있다.

4.4 URL 디코딩

ASCII 이외의 다른 문자는 URL에 인코딩 되어 표현된다. 이러한 경우 조사관은 URL의 의미를 짐작하기 어렵다. 이는 특히 검색 키워드가 영어가 아닌 언어일 때 주로 나타나며, 인코딩된 검색 키워드를 디코딩 하는 것은 비영어권 나라에서 매우 중요하다. 가령 Google에서 "포렌식"("forensic"의 한국말)이라는 단어를 검색하였을 경우 URL은 다음과 같다.

- http://www.google.com/search?hl=en&source=hp&q=%ED%8F%AC%EB%A0%8C%EC%8B%9D&aq=f&oq=&aqi=g10

4.3절에서 설명 하였듯이 밑줄 친 부분이 검색 키워드임을 알 수 있다. 하지만 직관적으로 무엇을 의미하는지 알 수가 없다. URL 인코딩은 해당 언어를 특정 방법으로 인코딩 한 후 그것을 헥사 코드로 표현한 후 1바이트 단위로 '%' 문자를 앞부분에 추가한다[6]. 인코딩 방법은 사이트마다 각각 다르다. 표 3은 상위 10위에 랭크되어 있는 검색 엔진에서 사용하는 인코딩 방법을 나타낸 것이다.

[표 3]에서 알 수 있듯이 대부분의 포털 사이트가 utf-8을 사용한다. Baidu, All the Web은 각각 멀티바이트를 기본 인코딩 방식으로 사용하며, baidu는 중국어가 아닌 언어를 검색할 경우 유니코드로 검색 키워드

〔표 3〕 상위 10위 검색 엔진의 인코딩 방법

검색 엔진	인코딩 방법
Google	utf-8
Yahoo	utf-8
Bing	utf-8
Baidu	멀티바이트(중국어 간체(GB2312))
Ask	utf-8
Aol	utf-8
Altavista	utf-8
MSN	utf-8
Excite	utf-8
All the Web	멀티바이트(서유럽어(ISO))

를 인코딩한다. 표에서 조사한 사이트 외에 한국(naver, nate, daum), 중국(netease), 일본(livedoor)의 검색 사이트를 조사한 결과 모든 사이트가 utf-8, 멀티바이트, 유니코드 중 하나를 인코딩 방법으로 사용하고 있었다. 따라서 URL이 ASCII 문자 이외의 언어로 표현되어 인코딩 된 경우 위의 3가지 방법으로 디코딩을 시도하여 가독성이 있도록 만들어야 한다.

V. 사례 분석

본 절에서는 웹 브라우저 사용흔적을 조사하여 사건을 해결한 사례를 소개한다.

5.1 사건 개요

피의자는 잦은 사업의 실패로 수천만 원의 빚을 지고 신용불량자로 전락했다. 이에 피의자는 보험금을 타기위한 목적으로 가족을 살해하기로 결정한다. 먼저 피의자는 범행을 저지르기 전 보험회사 두 곳에 생명보험을 가입했다. 또한 가족을 살해하기 위한 목적으로 인터넷 자살사이트에서 알게 된 3명과 서울역에서 만난 30대 남자에게 청산가리 10g을 공동 구매 했다. 뿐만 아니라 애완용 햄스터 2마리를 사 청산가리를 먹여 죽이는 실험을 하는 등 범행의 치밀함 까지 보였다.

피의자는 가족이 아침에 일어나면 물을 마시는 습관을 이용하여 물병에 미리 청산가리를 타 아내와 첫째·둘째 아들을 살해 한 후, 물을 마시지 않은 막내아들을 목을 졸라 살해하였다. 이후 범행을 은폐하려는 목적으로 집안에 시너를 뿌리고 불을 질렀다.

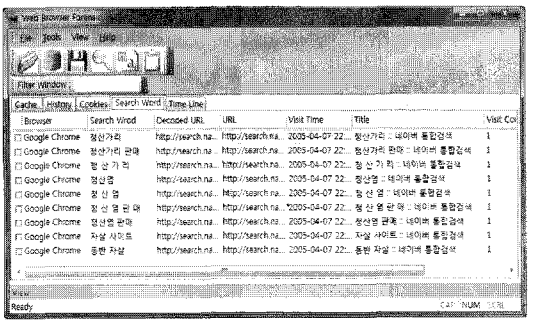
5.2 분석 사항

수사관은 유력한 용의자로 친아버지를 지목하였으나 명백한 증거가 없어 범행을 추궁하는데 어려움에 겪고 있던 중 피의자가 사용한 컴퓨터의 웹 브라우저 로그 파일에서 다음과 같은 사항을 밝혀냈다.

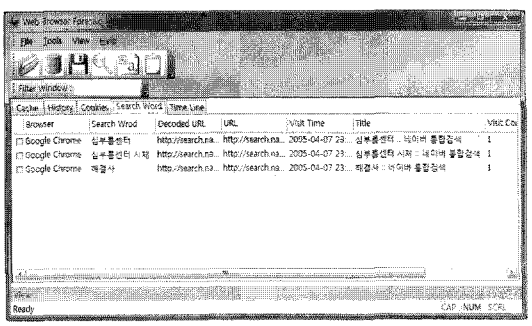
5.2.1 생명 보험 관련 사이트 접속

피의자는 보험금을 타기위한 목적으로 범행 전에 생명보험비교 사이트와 국·내외 보험사 사이트 두 곳에 접속하였다. 〔그림 4〕는 Cache File에서 피의자가 생명 보험 관련 사이트를 접속한 사실을 보여준다.

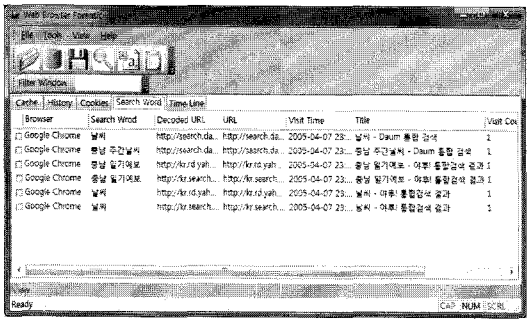
〔그림 4〕 생명 보험 관련 사이트 접속



〔그림 5〕 독극물 관련 내용 검색



〔그림 6〕 해결사 관련 내용 검색



〔그림 7〕 날씨 관련 내용 검색

5.2.2 독극물 관련 내용 검색

피의자는 일가족을 살해하기 위한 목적으로 주요 포탈 사이트에서 독극물·수면제 판매·자살 카페 관련 내용을 검색하였다. 〔그림 5〕는 history file에서 피의자가 독극물 관련 내용을 검색한 사실을 보여준다.

5.2.3 해결사 관련 내용 검색

피의자는 범행을 은폐하기 위한 목적으로 심부름·해결사 등을 검색하였다. 〔그림 6〕은 history file에서 피의자가 해결사, 심부름 관련 내용을 검색한 사실을 보여준다.

5.2.4 날씨 관련 내용 검색

피의자는 범행을 은폐하기 위한 목적으로 방화로 위장하기 위하여 비가 오지 않는 날을 범행일로 선택하고자 다음, 야후 등에서 제공하는 지역별 일기예보, 특히 피의자가 거주하고 있는 충남지역의 날씨를 확인하였다. 〔그림 7〕은 Cache file 및 history file에서 피의자가 날씨 관련 내용을 검색한 사실을 보여준다.

VI. 결론

웹 브라우저 포렌식은 디지털 포렌식에서 매우 중요하다. 웹 브라우저 포렌식을 이용하여 나온 증거는 용의자의 범죄 행위뿐만 아니라 목적, 수단, 방법과 같은 폭 넓은 정보를 제공해 줄 수 있으며 범죄 수사에 도움을 주는 단서를 제공해 줄 수 있다. 따라서 용의자의 컴퓨터를 조사할 경우 웹 브라우저 로그 파일은 필수적으로 조사되어야 한다. 본 논문에서는 웹 브라우저 포렌식에 대한 사전 연구들에 대하여 살펴보았으며, 여러 도구들의 특징들을 살펴보았다. 그리고 웹 브라우저 포렌식을 좀 더 실용적으로 수행하기 위한 방법들을 소개 하였다. 조사관은 한 시스템에 여러 웹 브라우저가 설치되었을 경우, 이를 통합적으로 분석하여야 한다. 또한 타임라인 분석을 통하여 용의자의 사이트 접속 행위에 대한 일련의 과정을 분석하여야 한다. 검색 키워드는 직관적으로 알 수 있는 정보를 제공하므로 반드시 조사해야 하며, 아스키 문자 이외의 언어를 사용하여 인코딩 된 경우에는 이를 디코딩하는 작업이 필요하다.

본 논문의 향후 과제로서 본 논문에서 다루지 않은 웹 브라우저 로그 파일의 추가적인 분석이 필요하다. 또한 논문에서 다루는 웹 브라우저 파일의 새로운 버전이 나올 때마다 로그 파일의 구조가 변경 될 수 있다. 따라서 변경된 로그 파일의 경우 꾸준한 분석을 통하여 새로운 버전의 웹 브라우저 사용흔적 분석이 가능하도록 해야 한다. 웹 브라우저 사용흔적 조사는 디지털 포렌식에서 수사에 필요한 매우 유용한 정보를 제공할 것이다.

참 고 문 헌

〔1〕 Keith J. Jones. "Forensic Analysis of Internet Explorer Activity Files," Foundstone, http://www.foundstone.com/us/pdf/wp_index_dat.pdf. 2003.

〔2〕 Keith j. Jones, Blani Rohyt. "Web browser forensic. Security focus," http://www.securityfocus.com/infocus/1827. 2005a.

〔3〕 Keith j. Jones, Blani Rohyt. "Web browser forensic. Security focus," http://www.securityfocus.com/infocus/1832. 2005b.

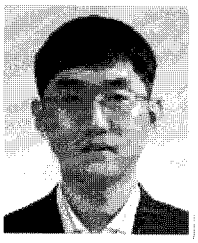
〔4〕 Murilo Tito Pereira. "Forensic analysis of the Firefox3 Internet history and recovery of deleted SQLite records," *Digital Investigation*. pp. 93-103. 2009.

〔5〕 SiQuest corporation. CacheBack, http://www.cacheback.ca/default.asp. 2009.

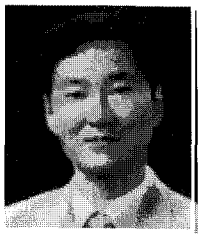
〔6〕 T. Berners-Lee, R. Fielding, L. Masinter. Uniform Resource Identifier(URI): Generic Syntax. RFC3986, 2005. 01

〔7〕 Net Application. Browser Market Share, http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=4. 2009b.

〈著者紹介〉



이 승 봉 (Seung-bong Lee) 정회원
2007년 8월: 서울시립대학교 수학과 졸업
2007년 9월~현재: 고려대학교 정보보호대학원 석사과정
2010년 3월~현재: 금융보안연구원 연구원
〈관심분야〉 디지털 포렌식, 정보보호



이 상 진 (Sang-jin Lee) 종신회원
1987년 2월: 고려대학교 학사 졸업
1989년 2월: 고려대학교 석사 졸업
1994년 8월: 고려대학교 박사 졸업
1989년 10월~1999년 2월: ETRI 연구원 역임
1999년 3월~현재: 고려대학교 정교수
〈관심분야〉 디지털 포렌식, 암호 이론, 정보 은닉, 암호 분석