

# **WEFA 1.3**

## **Web browser Forensic Analyzer**

웹 브라우저 포렌식 조사 도구

사용자 설명서

Copyright © 2012 4&6TECH Co., Ltd. All rights reserved.

## 책임의 한계와 법적고지

각 사용자는 설명서를 숙지해야 하며 설명서에서 고지되지 않은 사항에 대한 사용 책임은 사용자에게 있습니다.

본 제품과 설명서를 사용하여 발생하는 모든 사건에 대해 (주)포앤식스테크는 어떠한 경우도 민,형사 상의 책임을 지지 않습니다.

## 목차

<b>개요</b>	<b>8</b>
실행하기	8
종료하기	10
화면구성	11
필터 톨바	13
View Window	14
Main Window	19
<b>케이스 생성</b>	<b>37</b>
새 케이스 생성하기	37

<b>수집</b>	<b>39</b>
웹 브라우저 정보 수집하기	39
<b>분석</b>	<b>46</b>
기본 분석	46
키워드 검색	52
상세 검색	55
<b>보고서</b>	<b>60</b>
CSV 파일로 내보내기	60
REPORT	63

## 시작하기 전에

### 고객 지원

---

- 전화 상담 서비스: 02-922-4677
- 이메일 서비스: [4n6tech@4n6tech.com](mailto:4n6tech@4n6tech.com)

## 개발사

---



- (주)포앤식스테크
  - 전화: (02) 922-4677
  - 팩스: (02) 6280-4753
  - Homepage: <http://www.4n6tech.com>
-

## 지원 브라우저

---

Internet Explorer v6~9(다운로드 목록은 버전 9 부터 지원합니다.)

Firefox v7 이하

Chrome v15 이하

Safari v5.0 이하(v5.1 이상일 경우 Cookie 분석을 지원하지 않습니다.)

Opera v11 이하

## 주의사항

---

모든 제품은 함께 제공된 USB 를 PC 에 연결해야 동작합니다.

## 개요

제품을 실행하고 종료하는 방법을 설명합니다.

## 실행하기

USB 하드드라이브의 ELF 볼륨 내에 있는 WEFA.exe

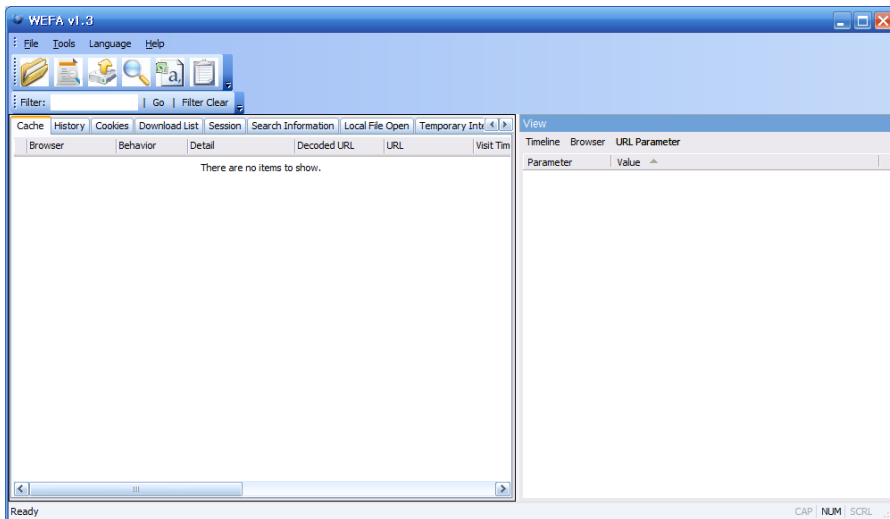


WEFA.exe  
Web browser Forensic Analyzer  
4&6TECH Co., Ltd.

을 더블 클릭합니다.



제품이 실행되고 다음과 같은 화면이 출력됩니다.

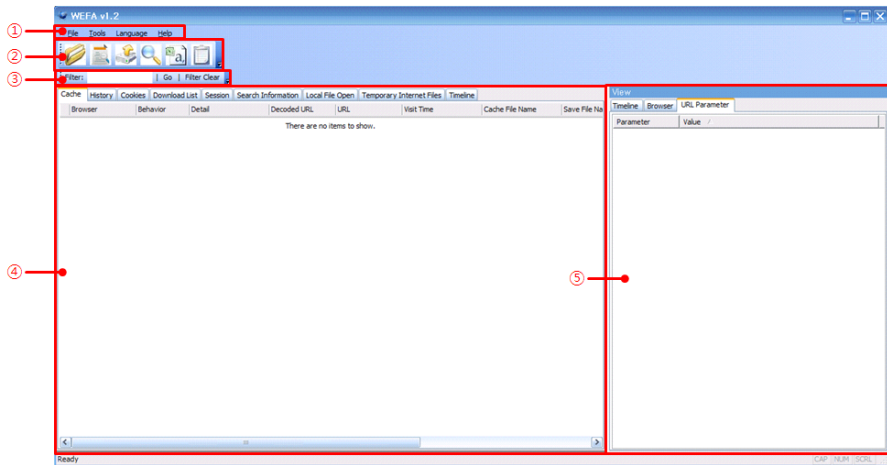


## 종료하기

메뉴의 File > Exit 를 클릭하거나 프로그램 실행 화면 우측 상단의 버튼을 클릭합니다.



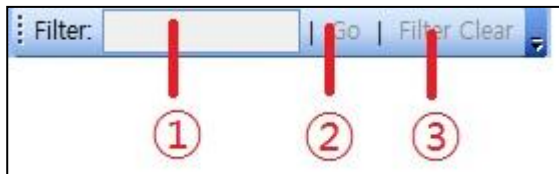
## 화면 구성



①	Menu	제품이 제공하는 기본 메뉴입니다
②	Toolbar	주요 기능을 수행하는 도구 모음입니다.
③	Filter Toolbar	키워드 검색 필터링 도구 모음입니다.
④	Main Window	분석 결과를 출력합니다.
⑤	View Window	타임라인 분석 결과 또는 웹 페이지를 출력합니다.

### 필터 툴바

- ① Filter: 필터링을 수행할 문자열을 입력하는 창입니다.
- ② Go: 필터링을 수행합니다.
- ③ Filter Clear: 초기 화면으로 되돌립니다.



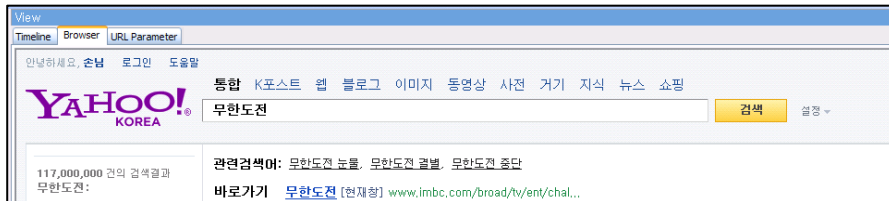
## VIEW WINDOW

## Timeline 탭:

View							
Timeline		Browser		URL Parameter			
Browser	Beha... /	Search Information	Decoded Url	URL	Visit Date	Title	visitcount
Internet Explorer	Cafe&Club		http://portal.ko...	http://portal.ko...	2011-11-10 12:09:24	고려대학교 지...	95
Internet Explorer			http://cist.kore...	http://cist.kore...	2011-11-10 12:09:30	CIST 논문관리...	13
Internet Explorer			http://ime.kore...	http://ime.kore...	2011-11-10 12:09:13	고려대학교 정...	33
Internet Explorer			http://www.du...	http://www.du...	2011-11-10 15:30:32	시티신문	1
Internet Explorer			http://dkevent...	http://dkevent...	2011-11-10 15:00:16		3
Internet Explorer			http://www.fo...	http://www.fo...	2011-11-10 12:11:13	포모스::토크 ...	2
Internet Explorer			http://filejo.co...	http://filejo.co...	2011-11-10 15:30:17		10
Internet Explorer			http://filejo.co...	http://filejo.co...	2011-11-10 15:30:16		3
Internet Explorer			http://www.file...	http://www.file...	2011-11-10 15:30:18		3
Internet Explorer			http://www.so...	http://www.so...	2011-11-10 15:22:04		1

Main Window 의 Timeline 탭에서 특정 날짜를 클릭하면 View Window 의 Timeline 탭에 해당 날짜에 방문한 모든 인터넷 접근 기록이 표시됩니다.

## Browser 탭:



Main Window 의 History 탭에서 특정 항목을 클릭하면 해당 웹 사이트가 View Window 의 Browser 탭에 출력됩니다. 이 기능은 Session 탭, Search 탭에서도 동일하게 적용됩니다.

Cache 탭에서 특정 항목을 클릭할 경우, 해당 Cache 데이터가 View Window 의 Browser 탭에 출력됩니다. 해당 기능은 Temporary Internet Files 탭에서도 동일하게 적용됩니다.

Download 탭에서 특정 항목을 클릭할 경우, 해당 정보의 URL 에 접속하여 데이터를 다운로드 합니다.



## URL Parameter 탭 :

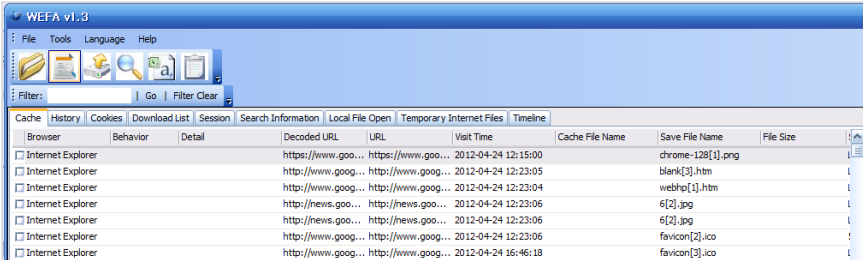
View	
Timeline	Browser
URL Parameter	
Parameter	Value ▲
hl	ko
newwindow	1
q	승인을 바다
rlz	1R2GGLT_koKR397
gs_sm	e
gs_upl	1219138281013984191212101013188150113.911310
bav	on.2,or.r_gc.r_pw.,cf.osb
biw	1672
bih	847
wrapid	tlif132015659073410
um	1
ie	UTF-8
sa	N
tab	wT

Main Windows 의 Cache 탭, History 탭에서 특정 항목을 클릭하면 해당 URL 의 변수 값들을 정렬하여 출력합니다.

URL 은 '변수=값&변수=값'의 형태로 구성되는데, WEFA 는 이를 분석하여 일목요연하게 출력합니다.

## MAIN WINDOW

Cache 탭:



The screenshot shows the WEFA v1.3 application window with the 'Cache' tab selected. The window has a menu bar (File, Tools, Language, Help) and a toolbar with icons for file operations. Below the toolbar is a 'Filter:' section with 'Go' and 'Filter Clear' buttons. The main area displays a table of cache entries with columns for Browser, Behavior, Detail, Decoded URL, URL, Visit Time, Cache File Name, Save File Name, and File Size. The table lists seven entries, all from Internet Explorer, with various URLs and file names.

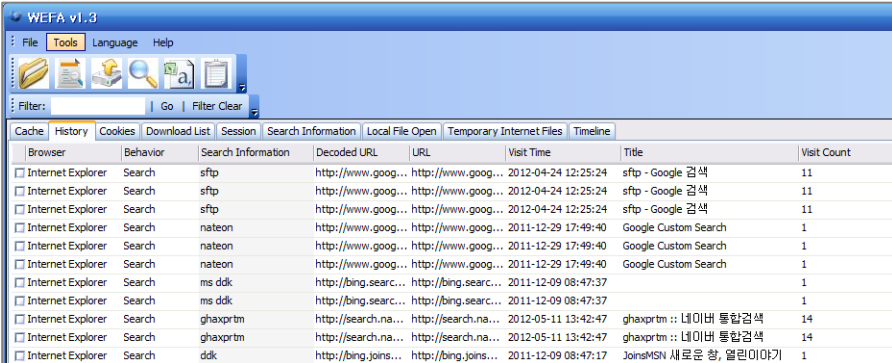
Browser	Behavior	Detail	Decoded URL	URL	Visit Time	Cache File Name	Save File Name	File Size
<input type="checkbox"/> Internet Explorer			https://www.goo...	https://www.goo...	2012-04-24 12:15:00	chrome-128[1].png		
<input type="checkbox"/> Internet Explorer			http://www.goog...	http://www.goog...	2012-04-24 12:23:05	blank[3].htm		
<input type="checkbox"/> Internet Explorer			http://www.goog...	http://www.goog...	2012-04-24 12:23:04	webhp[1].htm		
<input type="checkbox"/> Internet Explorer			http://news.goo...	http://news.goo...	2012-04-24 12:23:06	6[2].jpg		
<input type="checkbox"/> Internet Explorer			http://news.goo...	http://news.goo...	2012-04-24 12:23:06	6[2].jpg		
<input type="checkbox"/> Internet Explorer			http://www.goog...	http://www.goog...	2012-04-24 12:23:06	favicon[2].ico		
<input type="checkbox"/> Internet Explorer			http://www.goog...	http://www.goog...	2012-04-24 16:46:18	favicon[3].ico		

사용자 컴퓨터에 저장된 인터넷 Cache 데이터에 대한 분석 결과를 출력합니다.

다음의 웹 브라우저 Cache 정보를 확인할 수 있습니다.

- Browser
- Behavior
- Detail
- Decoded URL
- URL
- Visit Time
- Cache File Name
- Save File Name
- File Size
- Save Folder Name
- Local Path

## History 탭:



The screenshot shows the WEFA v1.3 application window with the 'History' tab selected. The window has a menu bar (File, Tools, Language, Help) and a toolbar with various icons. Below the toolbar is a 'Filter' section with a text input and 'Go' and 'Filter Clear' buttons. The main area displays a table of browser history entries.

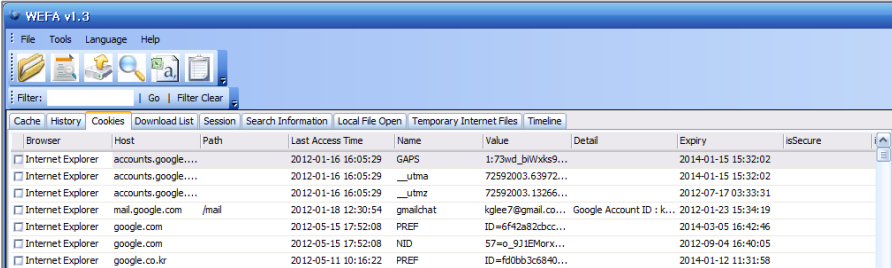
Browser	Behavior	Search Information	Decoded URL	URL	Visit Time	Title	Visit Count
<input type="checkbox"/> Internet Explorer	Search	sftp	http://www.goog...	http://www.goog...	2012-04-24 12:25:24	sftp - Google 검색	11
<input type="checkbox"/> Internet Explorer	Search	sftp	http://www.goog...	http://www.goog...	2012-04-24 12:25:24	sftp - Google 검색	11
<input type="checkbox"/> Internet Explorer	Search	sftp	http://www.goog...	http://www.goog...	2012-04-24 12:25:24	sftp - Google 검색	11
<input type="checkbox"/> Internet Explorer	Search	nateon	http://www.goog...	http://www.goog...	2011-12-29 17:49:40	Google Custom Search	1
<input type="checkbox"/> Internet Explorer	Search	nateon	http://www.goog...	http://www.goog...	2011-12-29 17:49:40	Google Custom Search	1
<input type="checkbox"/> Internet Explorer	Search	nateon	http://www.goog...	http://www.goog...	2011-12-29 17:49:40	Google Custom Search	1
<input type="checkbox"/> Internet Explorer	Search	ms ddk	http://bing.searc...	http://bing.searc...	2011-12-09 08:47:37		1
<input type="checkbox"/> Internet Explorer	Search	ms ddk	http://bing.searc...	http://bing.searc...	2011-12-09 08:47:37		1
<input type="checkbox"/> Internet Explorer	Search	ghaxprtm	http://search.na...	http://search.na...	2012-05-11 13:42:47	ghaxprtm :: 네이버 통합검색	14
<input type="checkbox"/> Internet Explorer	Search	ghaxprtm	http://search.na...	http://search.na...	2012-05-11 13:42:47	ghaxprtm :: 네이버 통합검색	14
<input type="checkbox"/> Internet Explorer	Search	ddk	http://bing.joins...	http://bing.joins...	2011-12-09 08:47:17	JoinsMSN 새로운 창, 열람이야기	1

인터넷 사용 이력에 대한 분석 결과를 출력합니다.

다음의 웹 브라우저 History 정보를 확인할 수 있습니다.

- Browser
- Behavior
- Search Information
- Decoded URL
- URL
- Visit Time
- Title
- Visit Count
- Typed

## Cookies 탭:



The screenshot shows the WEFA v1.3 interface with the 'Cookies' tab selected. The table below lists the cookies found on the system.

Browser	Host	Path	Last Access Time	Name	Value	Detail	Expiry	isSecure
<input type="checkbox"/> Internet Explorer	accounts.google....		2012-01-16 16:05:29	GAPS	1:73wd_bIWxs9...		2014-01-15 15:32:02	
<input type="checkbox"/> Internet Explorer	accounts.google....		2012-01-16 16:05:29	__utma	72592003.63972...		2014-01-15 15:32:02	
<input type="checkbox"/> Internet Explorer	accounts.google....		2012-01-16 16:05:29	__utmz	72592003.13266...		2012-07-17 03:33:31	
<input type="checkbox"/> Internet Explorer	mail.google.com	/mail	2012-01-18 12:30:54	gmailchat	kglee7@gmail.co...	Google Account ID : k...	2012-01-23 15:34:19	
<input type="checkbox"/> Internet Explorer	google.com		2012-05-15 17:52:08	PREF	ID=6f42a82cbcc...		2014-03-05 16:42:46	
<input type="checkbox"/> Internet Explorer	google.com		2012-05-15 17:52:08	NID	57=o_91IEMorx...		2012-09-04 16:40:05	
<input type="checkbox"/> Internet Explorer	google.co.kr		2012-05-11 10:16:22	PREF	ID=fd0bb3c6840...		2014-01-12 11:31:58	

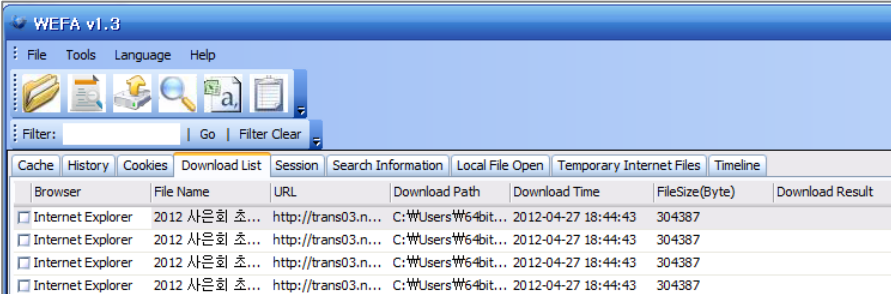
웹 사이트에서 사용자 컴퓨터에 자동 저장한 Cookie 데이터에 대한 분석 결과를 출력합니다.

다음의 웹 브라우저 Cookies 정보를 확인할 수 있습니다.

- Browser
- Host
- Last Access Time
- Name
- Value
- Detail
- Expiry
- Path
- isSecure
- isHttpOnly



## Download List 탭:



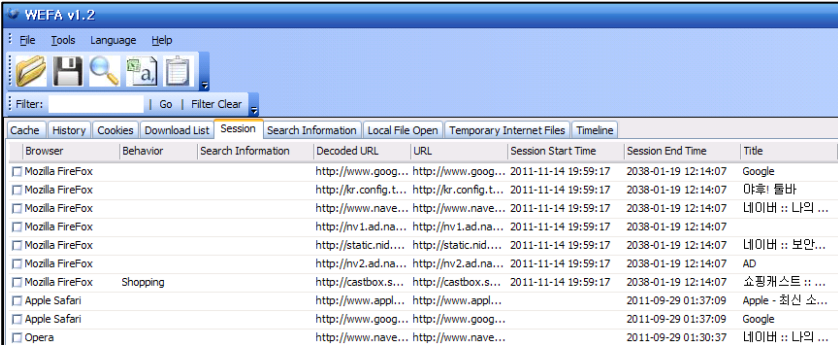
Browser	File Name	URL	Download Path	Download Time	FileSize(Byte)	Download Result
<input type="checkbox"/> Internet Explorer	2012 사은회 초...	http://trans03.n...	C:\Users\W64bit...	2012-04-27 18:44:43	304387	
<input type="checkbox"/> Internet Explorer	2012 사은회 초...	http://trans03.n...	C:\Users\W64bit...	2012-04-27 18:44:43	304387	
<input type="checkbox"/> Internet Explorer	2012 사은회 초...	http://trans03.n...	C:\Users\W64bit...	2012-04-27 18:44:43	304387	
<input type="checkbox"/> Internet Explorer	2012 사은회 초...	http://trans03.n...	C:\Users\W64bit...	2012-04-27 18:44:43	304387	

사용자가 웹 브라우저를 통해 다운로드한 파일에 대한 정보를 출력합니다.

다음의 웹 브라우저 Download 한 파일의 정보를 확인할 수 있습니다.

- Browser
- File Name
- URL
- Download Path
- Download Time
- File Size(Byte)
- Download Result

## Session 탭:



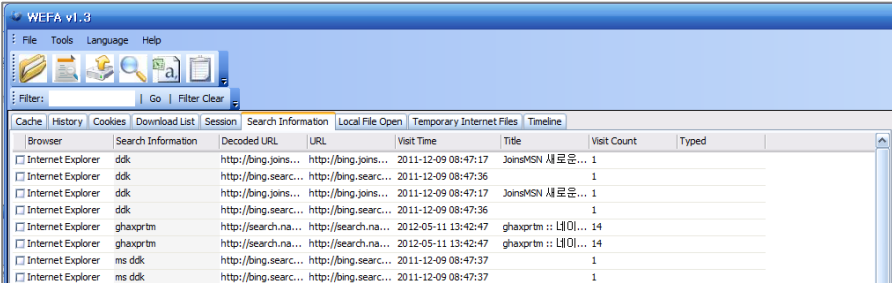
Browser	Behavior	Search Information	Decoded URL	URL	Session Start Time	Session End Time	Title
<input type="checkbox"/> Mozilla Firefox			http://www.goog...	http://www.goog...	2011-11-14 19:59:17	2038-01-19 12:14:07	Google
<input type="checkbox"/> Mozilla Firefox			http://kr.config.t...	http://kr.config.t...	2011-11-14 19:59:17	2038-01-19 12:14:07	마후! 돌바
<input type="checkbox"/> Mozilla Firefox			http://www.nave...	http://www.nave...	2011-11-14 19:59:17	2038-01-19 12:14:07	네이버 :: 나의 ...
<input type="checkbox"/> Mozilla Firefox			http://nv1.ad.na...	http://nv1.ad.na...	2011-11-14 19:59:17	2038-01-19 12:14:07	
<input type="checkbox"/> Mozilla Firefox			http://static.nid...	http://static.nid...	2011-11-14 19:59:17	2038-01-19 12:14:07	네이버 :: 보안...
<input type="checkbox"/> Mozilla Firefox			http://nv2.ad.na...	http://nv2.ad.na...	2011-11-14 19:59:17	2038-01-19 12:14:07	AD
<input type="checkbox"/> Mozilla Firefox	Shopping		http://castbox.s...	http://castbox.s...	2011-11-14 19:59:17	2038-01-19 12:14:07	쇼핑캐스트 :: ...
<input type="checkbox"/> Apple Safari			http://www.appl...	http://www.appl...		2011-09-29 01:37:09	Apple - 최신 소...
<input type="checkbox"/> Apple Safari			http://www.goog...	http://www.goog...		2011-09-29 01:37:09	Google
<input type="checkbox"/> Opera			http://www.nave...	http://www.nave...		2011-09-29 01:30:37	네이버 :: 나의 ...

사용자가 마지막으로 사용한 웹 브라우저 세션 정보에 대한 분석 결과를 출력합니다.

다음의 웹 브라우저 Session 정보를 확인할 수 있습니다.

- Browser
- Behavior
- Search Information
- Decoded URL
- URL
- Session Start Time
- Session End Time
- Title

## Search Information 탭:



WEFA v1.3.3

File Tools Language Help

Filter: | Go | Filter Clear

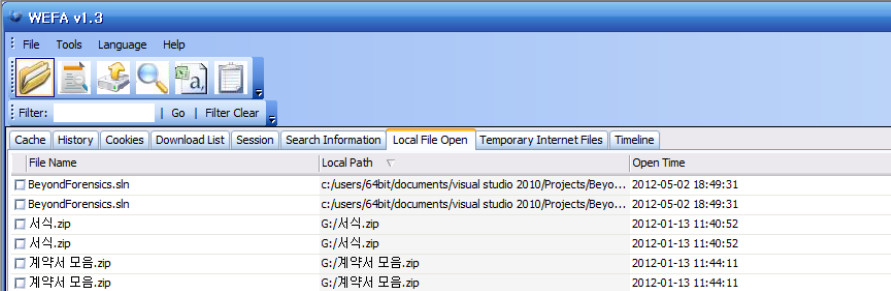
Browser	Search Information	Decoded URL	URL	Visit Time	Title	Visit Count	Typed
<input type="checkbox"/> Internet Explorer	ddk	http://bing.joins...	http://bing.joins...	2011-12-09 08:47:17	JoinsMSN 새로운...	1	
<input type="checkbox"/> Internet Explorer	ddk	http://bing.searc...	http://bing.searc...	2011-12-09 08:47:36		1	
<input type="checkbox"/> Internet Explorer	ddk	http://bing.joins...	http://bing.joins...	2011-12-09 08:47:17	JoinsMSN 새로운...	1	
<input type="checkbox"/> Internet Explorer	ddk	http://bing.searc...	http://bing.searc...	2011-12-09 08:47:36		1	
<input type="checkbox"/> Internet Explorer	ghaxprtm	http://search.na...	http://search.na...	2012-05-11 13:42:47	ghaxprtm :: 네이...	14	
<input type="checkbox"/> Internet Explorer	ghaxprtm	http://search.na...	http://search.na...	2012-05-11 13:42:47	ghaxprtm :: 네이...	14	
<input type="checkbox"/> Internet Explorer	ms ddk	http://bing.searc...	http://bing.searc...	2011-12-09 08:47:37		1	
<input type="checkbox"/> Internet Explorer	ms ddk	http://bing.searc...	http://bing.searc...	2011-12-09 08:47:37		1	

웹 브라우저 History 정보 중 검색 정보가 있는 항목만 출력합니다.

다음의 웹 브라우저 검색 정보를 확인할 수 있습니다.

- Browser
- Search Information
- Decoded URL
- URL
- Visit Time
- Title
- Visit Count
- Typed

## Local File Open 탭:



File Name	Local Path	Open Time
<input type="checkbox"/> BeyondForensics.sln	c:/users/64bit/documents/visual studio 2010/Projects/Beyo...	2012-05-02 18:49:31
<input type="checkbox"/> BeyondForensics.sln	c:/users/64bit/documents/visual studio 2010/Projects/Beyo...	2012-05-02 18:49:31
<input type="checkbox"/> 서식.zip	G:/서식.zip	2012-01-13 11:40:52
<input type="checkbox"/> 서식.zip	G:/서식.zip	2012-01-13 11:40:52
<input type="checkbox"/> 계약서 모음.zip	G:/계약서 모음.zip	2012-01-13 11:44:11
<input type="checkbox"/> 계약서 모음.zip	G:/계약서 모음.zip	2012-01-13 11:44:11

사용자가 컴퓨터에서 열어본 파일에 대한 분석 결과를 출력합니다.

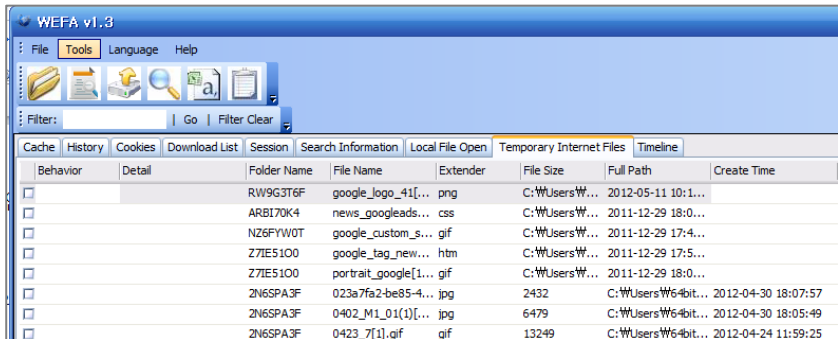
다음의 파일 열람 정보를 확인할 수 있습니다.

- File Name
- Local Path
- Open Time

사용자가 컴퓨터에서 문서 파일 등을 열람하면 해당 정보가 웹 브라우저 로그에 기록됩니다. WEFA 는 이를 분석하여 문서 열람 기록을 출력합니다.



## Temporary Internet Files(임시 인터넷 파일) 탭:



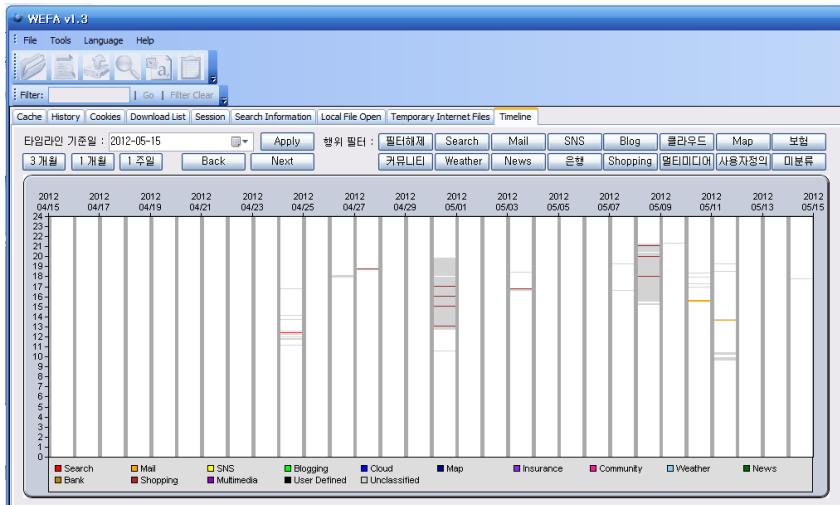
Behavior	Detail	Folder Name	File Name	Extender	File Size	Full Path	Create Time
<input type="checkbox"/>		RW9G3T6F	google_logo_41[...	png		C:\Users\W...	2012-05-11 10:1...
<input type="checkbox"/>		ARBI70K4	news_googleads...	css		C:\Users\W...	2011-12-29 18:0...
<input type="checkbox"/>		NZ6FYW0T	google_custom_s...	gif		C:\Users\W...	2011-12-29 17:4...
<input type="checkbox"/>		Z7IE5100	google_tag_new...	htm		C:\Users\W...	2011-12-29 17:5...
<input type="checkbox"/>		Z7IE5100	portrait_google[1...	gif		C:\Users\W...	2011-12-29 18:0...
<input type="checkbox"/>		ZN6SPA3F	023a7fa2-be85-4...	jpg	2432	C:\Users\W64bit...	2012-04-30 18:07:57
<input type="checkbox"/>		ZN6SPA3F	0402_M1_01(1)[...	jpg	6479	C:\Users\W64bit...	2012-04-30 18:05:49
<input type="checkbox"/>		ZN6SPA3F	0423_7[1].gif	gif	13249	C:\Users\W64bit...	2012-04-24 11:59:25

사용자 컴퓨터에 저장된 Internet Explorer의 임시 인터넷 파일에 대한 분석 결과를 출력합니다.

다음의 임시 인터넷 파일 정보를 확인할 수 있습니다.

- Behavior
- Detail
- Folder Name
- File Name
- File Size
- Full Path
- Create Time

## Timeline 탭:



인터넷 사용 시간대 분석 결과를 막대 그래프로 출력합니다.


그래프의 가로축은 날짜의 흐름을 나타내고, 세로축은 24 시간을 나타냅니다.

각 이벤트는 그래프 내에 특정 색상으로 표현됩니다.

## 케이스 생성

새 케이스 생성 방법을 설명합니다. 모든 기능은 케이스를 생성한 후에 사용할 수 있습니다.

### 새 케이스 생성하기

- 1 메뉴의 Files > Creating the New Case 또는 툴 바의  를 클릭합니다.

- 2 조사관 이름과 케이스 번호, 케이스 폴더 생성 경로를 입력합니다.  
추가적으로 Description 에 사건 설명을 입력합니다.

Creating the New Case

Case Information

Investigator  
4&6Tech

Case No.  
0001

Description  
Memo

Case Folder Path


C:\Documents and Settings\wojh\바탕 화면

OK Cancel

## 수집

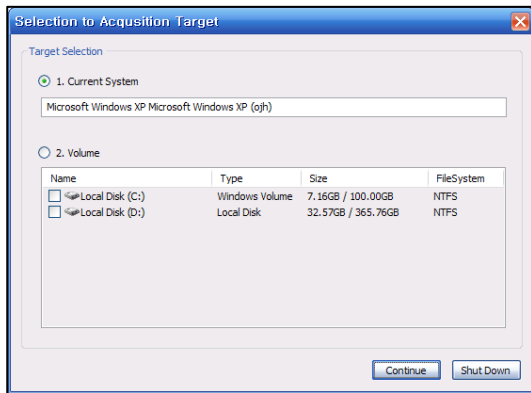
웹 브라우저 정보를 수집하는 방법을 설명합니다.

### 웹 브라우저 정보 수집하기

1 메뉴의 Files > Collection of Web Browser Log File 또는 톨 바의  를 클릭합니다.

2 수집될 파일들은 케이스 생성시 생성된 케이스 폴더의 "Collection" 폴더 아래 저장됩니다.

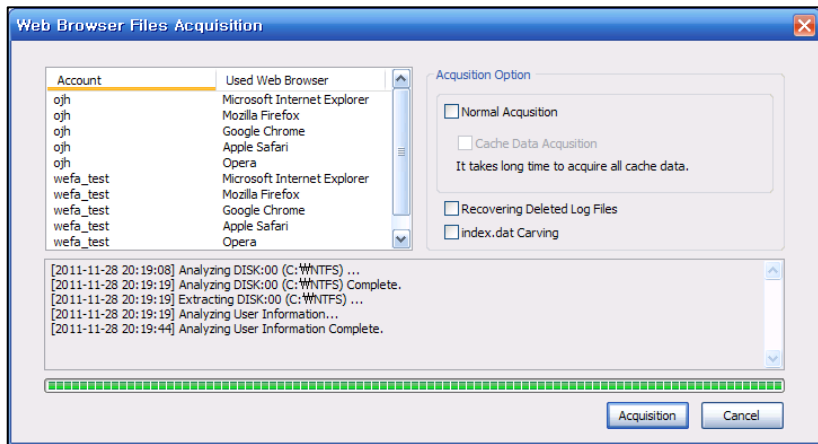
### 3 수집 대상 시스템 혹은 볼륨을 선택합니다.



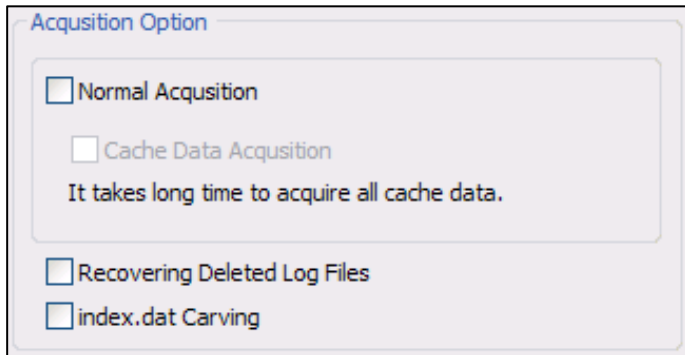
Current System 을 선택하면 현재 시스템에 대한 수집을 진행하고 Volume 을 선택하여 원하는 볼륨에 대한 수집을 진행할 수 있습니다.



4 수집 대상 볼륨에 운영체제가 설치되어 있다면 사용자 계정과 사용한 웹 브라우저 정보를 획득합니다.



5 수집 옵션을 선택하고 Acquisition 을 클릭합니다.



Normal Acquisition 은 기본적인 웹 브라우저 로그 파일들을 수집합니다.  
그리고 Cache Data Acquisition 을 선택하면 추가로 Cache 데이터를  
수집합니다. 모든 Cache 데이터를 수집하는 작업은 시간이 오래 걸립니다.  
필요에 따라서 선택합니다.

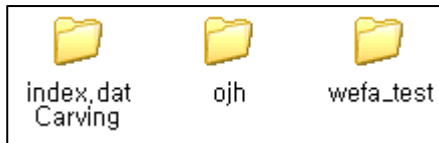
Recovering Deleted Log Files 를 선택하면 삭제된 로그 파일을 복구합니다.

index.dat Carving 을 선택하면 비 할당 영역에서 Internet Explorer 의  
index.dat 파일을 복구합니다.

6 수집 폴더는 “WebBrowserFiles\_년월일시분초” 형식으로 생성됩니다.



수집 폴더 아래에는 사용자 계정 별로 폴더가 생성되고 계정 별 수집된 로그 파일들이 저장됩니다. index.dat Carving 을 선택하였을 경우 index.dat Carving 폴더가 생성되어 복구된 index.dat 파일들이 저장됩니다.



각 계정 폴더 아래에는 사용한 웹 브라우저 폴더가 존재하며 해당 폴더 아래에 각 브라우저의 로그 파일들이 저장된다. **Recovered Files** 폴더 아래에는 파일 단위로 삭제된 로그 파일들이 복구되어 저장됩니다.




## 분석

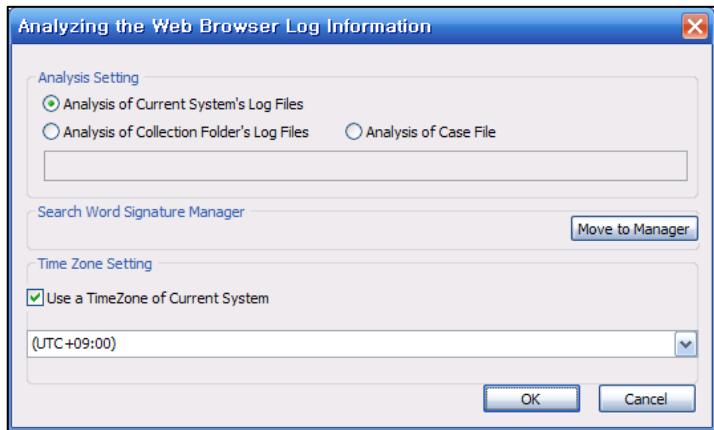
웹 브라우저 정보를 분석하는 기능을 소개합니다.

### 기본 분석

웹 브라우저 정보에 대한 기본적인 분석 방법을 소개합니다.

- 1 메뉴의 File > Analysis of Web Browser Log Information 을 클릭  
또는 툴바의  을 클릭합니다.

2 Open Setting 에서 분석 대상을 선택합니다.



다음은 분석 대상 옵션에 대한 설명입니다.

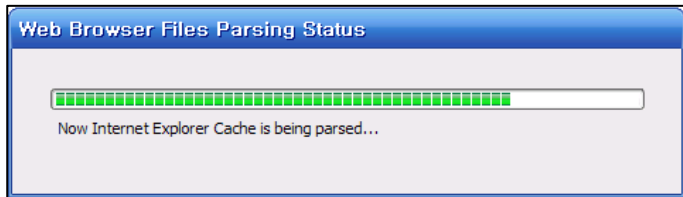
- **Analysis of Current System's Log Files** 을 선택할 경우:  
현재 시스템에 설치된 웹 브라우저의 로그파일을 자동으로 탐지하여 분석합니다.
- **Analysis of Collection Folder's Log Files** 을 선택할 경우:  
미리 수집된 웹 브라우저 로그 파일을 분석합니다. 라디오 버튼을 클릭하여 수집 폴더의 경로를 지정합니다. 정확한 분석 결과를 얻으려면 생성된 “WEFA\_Collection\_년월일시분초” 폴더를 선택합니다.
- **Analysis of Case File** 을 선택할 경우:  
로그 파일 분석 시, 생성된 케이스 파일을 다시 읽어 들입니다.



### 3 Time Zone Setting 에서 표준 시간대를 설정합니다.

- 시스템의 표준 시간대를 그대로 선택하거나 조사관이 임의로 표준 시간대를 설정할 수 있습니다.
- 여기서 설정된 UTC 시간대는 웹 브라우저 정보 분석 결과로 출력되는 모든 시간 정보에 적용됩니다.

4 OK 를 클릭합니다. 웹 브라우저 파일 분석을 시작하고 진행 상황을 표시합니다.



5 분석이 완료되면 메인 윈도우에 기본적인 분석 결과가 출력됩니다.

WEFA v1.3

File Tools Language Help

Filter: | Go | Filter Clear

Cache	History	Cookies	Download List	Session	Search Information	Local File Open	Temporary Internet Files	Timeline	
	Browser	Behavior	Search Information	Decoded URL	URL	Visit Time	Title	Visit Count	Typed
<input type="checkbox"/>	Internet Explorer			http://www.code...	http://www.code...	2012-05-10 16:57:39		1	
<input type="checkbox"/>	Internet Explorer			https://vpn.kore...	https://vpn.kore...	2012-04-24 11:10:59		3	
<input type="checkbox"/>	Internet Explorer	Mail		http://mail.4n6te...	http://mail.4n6te...	2012-05-10 15:35:18		1	
<input type="checkbox"/>	Internet Explorer			http://go.microso...	http://go.microso...	2011-12-29 17:48:54		4	
<input type="checkbox"/>	Internet Explorer			http://main.conn...	http://main.conn...	2012-04-26 18:08:20		1	
<input type="checkbox"/>	Internet Explorer			http://xdn.altool...	http://xdn.altool...	2012-04-24 11:50:41		4	
<input type="checkbox"/>	Internet Explorer			http://search.na...	http://search.na...	2012-05-10 17:19:49		1	
<input type="checkbox"/>	Internet Explorer			http://www.goog...	http://www.goog...	2012-04-24 12:14:28		2	
<input type="checkbox"/>	Internet Explorer			http://sdn.altools...	http://sdn.altools...	2012-04-24 12:16:53		2	
<input type="checkbox"/>	Internet Explorer			http://ko-kr.altoo...	http://ko-kr.altoo...	2012-04-24 12:17:35		4	
<input type="checkbox"/>	Internet Explorer			http://xo.nate.c...	http://xo.nate.c...	2012-04-27 18:44:20		33	
<input type="checkbox"/>	Internet Explorer			http://advert.est...	http://advert.est...	2012-04-24 11:46:29		1	
<input type="checkbox"/>	Internet Explorer			http://note.nate...	http://note.nate...	2012-05-11 13:41:23		6	
<input type="checkbox"/>	Internet Explorer	SNS		http://sess.cywo...	http://sess.cywo...	2012-05-11 09:39:32		161	
<input type="checkbox"/>	Internet Explorer			http://lifetop.lgn...	http://lifetop.lgn...	2012-04-24 11:59:28		7	
<input type="checkbox"/>	Internet Explorer			http://ko-kr.altoo...	http://ko-kr.altoo...	2012-04-24 11:50:48		2	
<input type="checkbox"/>	Internet Explorer			http://ko-kr.altoo...	http://ko-kr.altoo...	2012-04-24 11:50:47		2	
<input type="checkbox"/>	Internet Explorer			http://www.nave...	http://www.nave...	2012-05-14 17:48:56		18	
<input type="checkbox"/>	Internet Explorer			http://lifetop.lgn...	http://lifetop.lgn...	2012-04-24 11:59:37		3	
<input type="checkbox"/>	Internet Explorer	SNS		http://cyxso.cyw...	http://cyxso.cyw...	2012-04-30 12:45:22		1	
<input type="checkbox"/>	Internet Explorer			http://xo.nate.c...	http://xo.nate.c...	2012-04-30 12:45:22		1	
<input type="checkbox"/>	Internet Explorer	Shopping		http://www.nate...	http://www.nate...	2012-04-30 12:50:43		1	
<input type="checkbox"/>	Internet Explorer	News		http://www.goog...	http://www.goog...	2011-12-29 19:15:45		1	

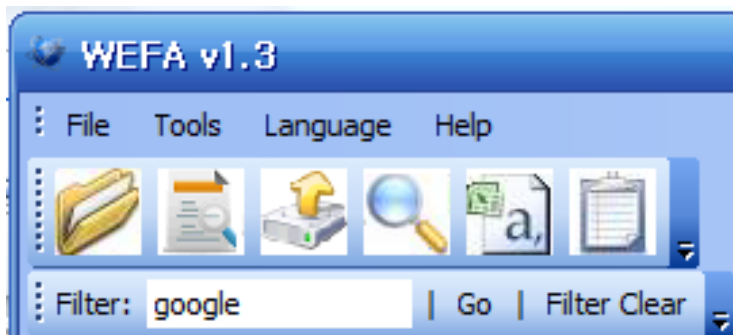
## 키워드 검색

웹 브라우저 정보에 대한 키워드 검색 방법을 설명합니다.

**1** 필터 툴바의 **Filter** 에 검색하고자 하는 키워드를 입력합니다.


**2** 엔터키를 누르거나 **Go** 를 클릭합니다.  
키워드 검색이 수행됩니다.

3 Filter Clear 를 클릭하면 현재 검색 결과분석 초기 상태로 돌아갑니다.



## 상세 검색

웹 브라우저 정보에 대한 상세 검색 방법을 설명합니다.

- 1 메뉴의 Tools > Search 또는 툴바의 을 클릭합니다. Search 대화상자가 생성됩니다.

**Search**

Keywords

Include: ☐ GREP

naver|daum|google

X to apply multiple keywords, separate the words by semicolon(;) )

**GREP Grammar**

.	Any character
*	Repeat 0+ times
+	Repeat 1+ times
?	Repeat 0 or 1
{min,max}	Repeat min~max times
[a-z]	One character in group
[abc]	One character in group
[^abc]	One character not in group
^	Beginning of the sentence
\$	End of the sentence
^^	Beginning of the file
\$\$	End of the file
\r	Form feed
\n	New line
\r	Carriage return
\t	Horizontal tab
\v	Vertical tab
\xhh	Hexadecimal
\uhhhh	Unicode
A B	A or B
()	Group

☒ Date

From: 2011-11-01

To: 2011-11-28

☒ Specific Filter

☐ Cache Tab

<input type="checkbox"/> Browser	<input type="checkbox"/> Behavior	<input type="checkbox"/> Detail	<input type="checkbox"/> Decoded URL
<input type="checkbox"/> URL	<input type="checkbox"/> Visit Time	<input type="checkbox"/> Cache File Name	<input type="checkbox"/> File Name
<input type="checkbox"/> File Size	<input type="checkbox"/> Folder Name	<input type="checkbox"/> Local Path	

☒ History Tab

<input checked="" type="checkbox"/> Browser	<input checked="" type="checkbox"/> Behavior	<input checked="" type="checkbox"/> Search Word	<input type="checkbox"/> Decoded URL
<input type="checkbox"/> URL	<input type="checkbox"/> Visit Time	<input type="checkbox"/> Title	<input type="checkbox"/> Visit Count
<input type="checkbox"/> Typed			

☐ Cookies Tab

<input type="checkbox"/> Browser	<input type="checkbox"/> Host	<input type="checkbox"/> Path	<input type="checkbox"/> Last Access Time
<input type="checkbox"/> Name	<input type="checkbox"/> Value	<input type="checkbox"/> Detail	<input type="checkbox"/> Expiry
<input type="checkbox"/> isSecure	<input type="checkbox"/> isHttpOnly		

☐ Download List Tab

<input type="checkbox"/> Browser	<input type="checkbox"/> File Name	<input type="checkbox"/> URL	<input type="checkbox"/> Download Path
<input type="checkbox"/> Download Time	<input type="checkbox"/> File Size	<input type="checkbox"/> Download Result	

☐ Session Tab

<input type="checkbox"/> Browser	<input type="checkbox"/> Behavi	<input type="checkbox"/> Search Information	<input type="checkbox"/> Decoded URL
<input type="checkbox"/> URL	<input type="checkbox"/> Session Start Time	<input type="checkbox"/> Session End Time	<input type="checkbox"/> Title

☒ Search Word Tab

<input checked="" type="checkbox"/> Browser	<input checked="" type="checkbox"/> Search Word	<input type="checkbox"/> Decoded URL	<input type="checkbox"/> URL
<input type="checkbox"/> Visit Time	<input type="checkbox"/> Title	<input checked="" type="checkbox"/> Visit Count	<input type="checkbox"/> Typed

☐ Local File Open Tab

<input type="checkbox"/> File Name	<input type="checkbox"/> Local Path	<input type="checkbox"/> Open Time
------------------------------------	-------------------------------------	------------------------------------

☐ Temporary Internet File Tab

<input type="checkbox"/> Behavior	<input type="checkbox"/> Detail	<input type="checkbox"/> Folder Nan	<input type="checkbox"/> File Name
<input type="checkbox"/> Extender	<input type="checkbox"/> File Size	<input type="checkbox"/> Full Path	<input type="checkbox"/> Create Time

OK Cancel

2 일반적인 키워드 검색을 수행하고 싶을 때는 GREP 을 선택하지 않고 검색을 수행합니다. 정규표현 검색을 하고 싶으면 GREP 을 선택하고 문법에 맞는 정규 표현식을 입력합니다. 추가적으로 기간 검색과 필드 별 검색을 수행할 수 있습니다. OK 버튼을 클릭하면 검색이 수행됩니다.



- 다음 그림은 History 탭의 browser, title, URL 필드와 Search Word 탭의 Browser, Search Word, Title 필드에서 naver, daum, google 중 적어도 하나의 문자열을 포함하고 2011 년 11 월 1 일로부터 2011 년 11 월 28 일까지 발생된 데이터를 검색하는 방법을 예시합니다.

**Keywords**

Include: ☒ GREP

naver|daum|google

※ To apply multiple keywords, separate the words by semicolon( ; )

☒ **Date**

From: 2011-11-01

To: 2011-11-28

- 특수 필터 기능은 아래 그림과 같이 특정 필드를 대상으로 검색하고자 할 때 유용합니다.
- 특히 Grep 기능, 즉 정규표현식을 이용하여 특정 형태의 문자열을 내포한 데이터를 검색할 때 매우 유용합니다.
- WEFA의 정규표현 검색은 C++ Technical Report (TR1) 문법을 따릅니다.  
( <http://msdn.microsoft.com/en-us/library/bb982727.aspx> )

☒ Specific Filter

☒ Cache Tab

<input checked="" type="checkbox"/> Browser	<input checked="" type="checkbox"/> Behavior	<input checked="" type="checkbox"/> Detail	<input type="checkbox"/> Decoded URL
<input type="checkbox"/> URL	<input type="checkbox"/> Visit Time	<input checked="" type="checkbox"/> Cache File Name	<input type="checkbox"/> File Name
<input type="checkbox"/> File Size	<input type="checkbox"/> Folder Name	<input type="checkbox"/> Local Path	

☒ History Tab


<input checked="" type="checkbox"/> Browser	<input type="checkbox"/> Behavior	<input checked="" type="checkbox"/> Search Word	<input type="checkbox"/> Decoded URL
<input type="checkbox"/> URL	<input type="checkbox"/> Visit Time	<input type="checkbox"/> Title	<input type="checkbox"/> Visit Count
<input type="checkbox"/> Typed			

## 보고서

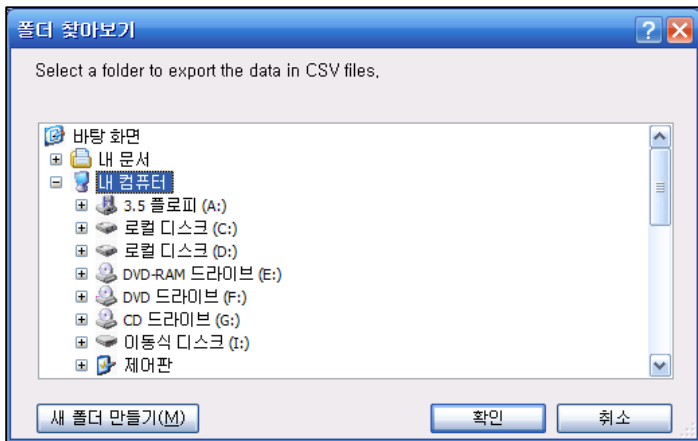
분석 결과를 문서 파일로 출력하는 기능을 소개합니다.

### CSV 파일로 내보내기

분석 결과를 CSV(Common-Separated Values) 파일로 내보내는 방법을 설명합니다.

**1** 메뉴의 Tools > Export Data in CSV files 또는 툴바의  을 클릭합니다.

2 폴더 찾아보기 대화상자에서 분석 결과를 내보낼 경로를 지정합니다.  
확인을 클릭하면 내보내기를 수행합니다.



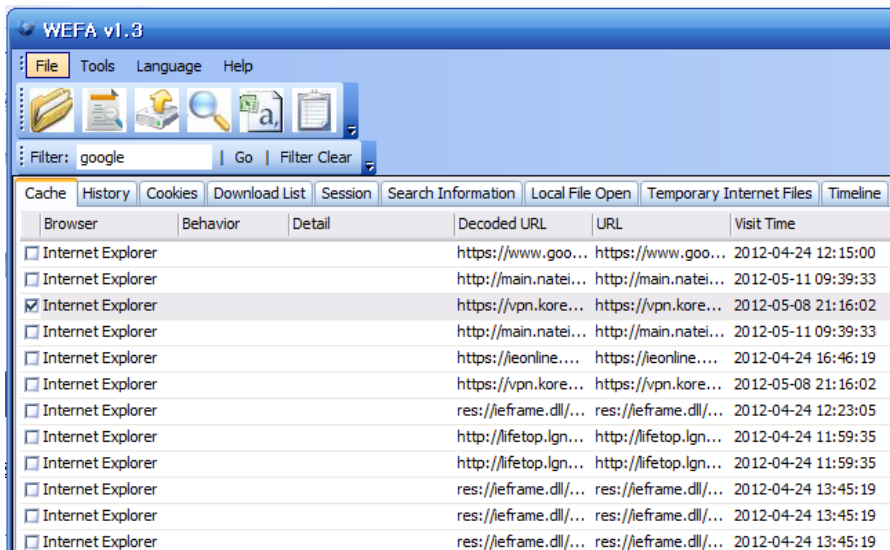
3 내보내기가 완료되면 다음과 같은 메시지가 출력됩니다.




## REPORT

분석 결과를 보고서로 출력하는 방법을 설명합니다.

- 1** 분석된 항목 중에서 보고서로 출력하고자 하는 항목의 좌측에서 첫 번째 열에 있는 체크박스를 클릭합니다.



2 메뉴의 Tools > Report 또는 툴바의  을 클릭합니다. Report 화면에 보고서가 출력됩니다. 캐쉬, 히스토리, 검색어, 쿠키 정보를 확인할 수 있습니다.



# Web History Examination Report

Case Number	00
Examiner Name	4n6Tech
Description	New
Date	2011-11-28

AccessTime	URL	SaveFileName	Behavior	Detail
2011-11-24 15:58:08	http://static.naver.net/www/u/2011/1124/nmms_12941661c.jpg	nmms_12941661c [1].jpg		
2011-11-28 11:11:30	http://ptimg.realclick.co.kr/201111/pkg20787_1712_4.jpg	pkg20787_1712_4 [1].jpg		
2011-11-24 07:12:18	http://common.nate.com/name/UI/CommonNameUI.js?ver=201111240717	CommonNameUI A58F7Mw.js		

### History Information:

OK

3 우측 하단에 Print 를 클릭하면 인쇄 미리보기 화면이 출력됩니다. 설정 확인 후 인쇄합니다.

