

Web Browser Forensics : Part 1



blueangel

blueangel1275@gmail.com

<http://blueangel-forensic-note.tistory.com>



1. Web Browser Forensics
2. Web Browser 로그 파일 수집
3. Internet Explorer 로그 분석

Web Browser Forensics

- **Web Browser**
- Web Browser Forensics?
- 분석 대상 정보



Web Browser

- 웹 서버와 쌍방향 통신을 통해 HTML문서나 파일을 연동하고 출력하는 응용소프트웨어





Internet Explorer

- Microsoft사에서 개발
- Windows 운영체제에 기본 포함되어 있음
- 최신 버전 : v9.0
 - GPU 가속 기능
 - 다운로드 매니저 추가
- 점유율
 - 2012.03 기준 , 전 세계 1위 (52.84%)
 - 대한민국 점유율 1위 (98%)
 - ✓ 인터넷 뱅킹 시, ActiveX 사용
 - ✓ 대부분의 웹 사이트 제작자들이 Internet Explorer에 최적화되게 제작





Firefox

- Mozilla 재단에서 개발
- 넷스케이프 브라우저의 공개 소스형 버전
- 최신 버전 : v10.0
- 점유율 : 2012.03 기준, 전 세계 2위 (20.92%)
- 다양한 부가 기능 지원
 - Add-On 기능을 통해 손쉽게 플러그인 설치 및 제거 가능
- 기본적으로 ActiveX 지원하지 않음 (플러그인 으로 설치 가능)





Chrome

- Google사에서 개발
- 안정성과 효율적인 인터페이스에 중점
- 가장 빠른 속도와 가장 적은 CPU 점유율
- 최신버전 : v17.0
- 점유율 : 2012.03 기준, 전 세계 3위 (18.90%)
- 기본적으로 ActiveX 지원하지 않음 (별도의 설치 후 사용 가능)
- 자동 업데이트 기능





Safari

- Apple사에서 개발
- Mac에 최적화되어 있음
- iPhone, iPad의 기본 웹 브라우저
- 최신 버전 : v5.0
- 점유율 : 2012.03 기준, 전 세계 4위 (5.24 %)





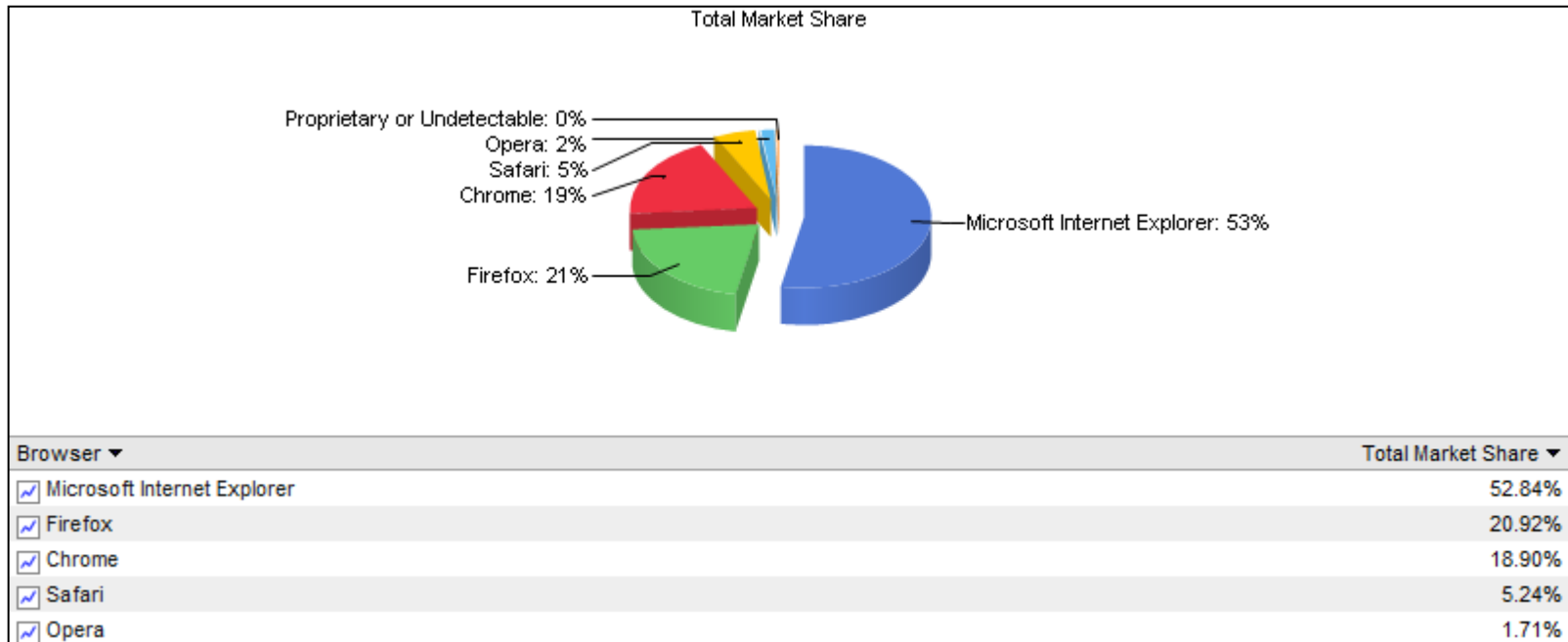
Opera

- Opera Software사에서 개발
- 5대 웹 브라우저 중 HTML 표준을 가장 정확이 따름
- 최신 버전 : v11.0
- 점유율 : 2012.03 기준, 전 세계 5위 (1.71 %)
- 모바일/스마트폰 시장에서 강세(전세계 120만)





전 세계 웹 브라우저 점유율(2012년 3월 기준)



- 출처 : NetMarketShare
(<http://netmarketshare.com/browser-market-share.aspx?qprid=0&qpcustommd=0>)

Web Browser Forensics

- Web Browser
- **Web Browser Forensics?**
- 분석 대상 정보



Web Browser Forensics ?

▪ 정의

- 용의자의 컴퓨터에 저장되는 웹 브라우저 사용 흔적을 디지털 포렌식적인 방법을 이용하여 조사하는 것
- 웹 브라우저가 남기는 **로그파일을 분석**

▪ 필요성

- 아무리 사소한 정보라도 인터넷을 이용해서 획득
- 사건과 관련된 내용이 웹 브라우저 로그 파일에 남을 가능성
- 상황에 따라 **범행동기, 목적, 수단, 방법, 사후처리** 등의 많은 정보를 획득 할 수 있음

➔ 실제로 Web Browser Forensic에서 획득한 증거는 직접증거보다는 **정황증거**로서 사용될 가능성이 많음

Web Browser Forensics











- Web Browser
- Web Browser Forensics?
- 분석 대상 정보



분석 대상 정보

Cache 정보

- 웹 사이트 접속 시, 방문사이트로부터 데이터를 자동으로 다운받는 것
- 재접속 시, 다시 다운 받지 않고 다운 받은 데이터 사용 ➔ 빠른 웹 페이지 로딩이 목적
- 분류
 - ✓ Cache 데이터 : 다운로드 받은 데이터
 - ➔ 이미지파일, 텍스트파일, 아이콘, HTML파일, XML 파일, 스크립트 ...
 - ✓ Cache 인덱스 정보 : 캐시데이터 위치, 다운로드 URL, 다운로드 시간, 데이터 크기...

이름	인터넷 주소
 52564936947113319.png	http://icon.daumcdn.net/w/c/11/05/52564936947113319.png
 main_mov_110406.js	http://s1.daumcdn.net/amsimg/www4/js/main_mov_110406.js
 52720405798420319.jpg	http://icon.daumcdn.net/w/c/11/06/52720405798420319.jpg
 52721102701825319.png	http://icon.daumcdn.net/w/c/11/06/52721102701825319.png
 52721828817661319.png	http://icon.daumcdn.net/w/c/11/06/52721828817661319.png
 52740160198587319.png	http://icon.daumcdn.net/w/c/11/06/52740160198587319.png
 51575850459082839.png	http://icon.daumcdn.net/w/c/11/06/51575850459082839.png
 51597055748193839.jpg	http://icon.daumcdn.net/w/c/11/06/51597055748193839.jpg
 51600585835954839.jpg	http://icon.daumcdn.net/w/c/11/06/51600585835954839.jpg
 52750810828532319.jpg	http://icon.daumcdn.net/w/c/11/06/52750810828532319.jpg



분석 대상 정보

▪ Cache 정보 분석 방법론(1/3)

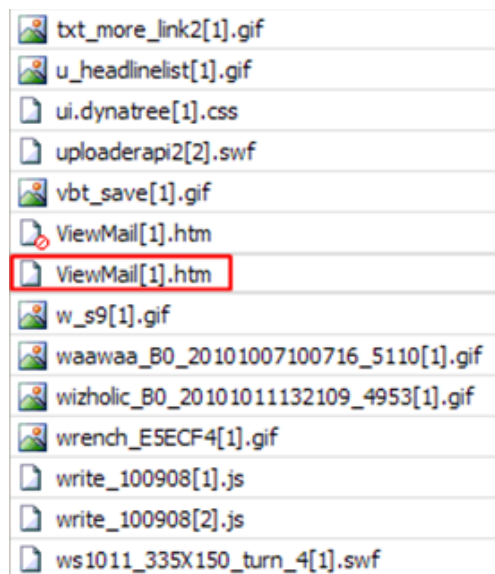
- Cache 인덱스 정보 분석
 - ✓ Cache 인덱스 정보 분류
 - 다운로드 URL
 - 다운로드 시간
 - Cache 데이터 파일명
 - Cache 데이터 크기
 - Cache 데이터 위치
- 다운로드 URL, 다운로드 시간 ➔ 사용자가 특정 시간에 해당 사이트를 방문함을 입증
- 다운로드 URL 내의 특정 키워드를 통해 사용자의 특정 행위를 유추
 - ✓ 'mail' 키워드 ➔ 웹 메일 사용 http://img-section.hanmail.net/blognews/widget/bt_recom.gif
 - ✓ '.doc, .ppt, .pdf'와 같은 문서 확장자 ➔ 웹 사이트에서의 문서 열람
http://oem.microsoft.com/public/sblicense/2008_sb_licenses/fy08_sb_license_korean.pdf



분석 대상 정보

Cache 정보 분석 방법론(2/3)

- Cache 데이터 분석
 - ✓ HTML 파일이 Cache 데이터로 저장된 경우
 - Daum 웹 메일에서 메일 본문을 확인한 경우, 본문 내용은 Temporary Internet 파일 형태로 저장됨
 - ViewMail[n].htm 파일을 열어서, 메일 본문 내용 확인 가능





분석 대상 정보

Cache 정보 분석 방법론(3/3)

Cache 데이터 분석

✓ HTML 파일이 Cache 데이터로 저장된 경우

- 한글 파일의 경우, 웹 브라우저 상에서 바로 열기를 수행할 경우, hwp 파일 형태로 그대로 저장됨

[HWP] Plasmid purification Kit (Spin type) - N01112, N01115

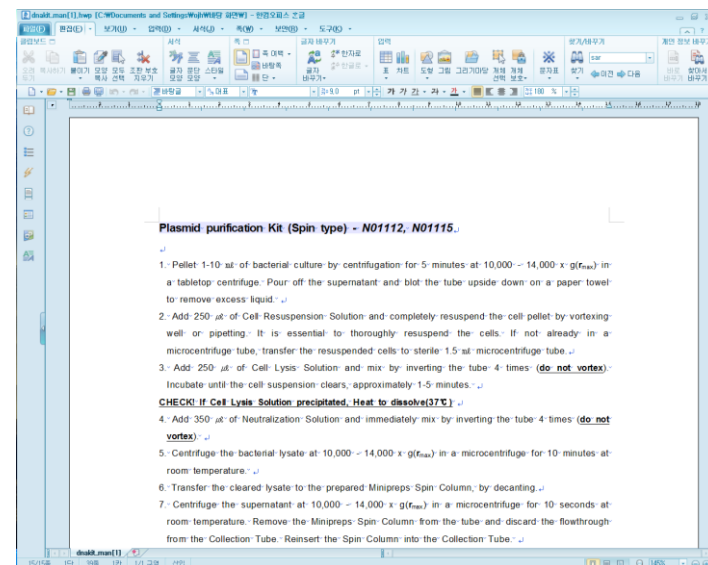
파일 형식: HWP/Hancom Hanword - [HTML 버전](#)

Plasmid purification Kit (Spin type) - N01112, N01115. 1. Pellet 1-10 mL of bacterial culture by centrifugation for 5 minutes at 10000 - 14000 x g(rmax) in ...

www.nucleogen.com/misc/dnakit_man.hwp



deja[1].html
editor[1].html
index[1].html
dnakit_man[1].hwp
favicon[1].ico
favicon[2].ico
favicon[3].ico





분석 대상 정보

■ History 정보

- 사용자가 방문한 웹사이트의 접속 정보
- 사용자의 편의를 위해 저장됨
 - ✓ 예전에 방문한 사이트를 다시 방문하고 싶을 때
 - ✓ 월별, 일별 방문 기록을 분류해서 제공
- 저장 형식 분류
 - ✓ 직접 접근 : URL 입력창에 직접 주소 입력
 - ✓ 간접 접근 : 링크를 통해서 접근

History

Today - Friday, June 3, 2011

1:26 AM Google

1:26 AM [How to Clear Google Web History | eHow.com](#)

1:25 AM Google 이미지 검색결과: <http://img.ehowcdn.com/article-page-main/ehow/images/a05/ep/04/clear...>

1:24 AM Google Search History

1:24 AM Google 이미지 검색결과: <http://blogging.seocompany.ca/wp-content/uploads/2008/12/google-hist...>

1:24 AM [Web Eraser-Web History Eraser-#1 Web Eraser software on the Web](#)

1:24 AM Google 이미지 검색결과: <http://www.internet-history-eraser.com/images/historyerase.gif>

1:24 AM Web history - Google 검색

1:23 AM Photo: Download Icon © JAVA #11251687

1:23 AM Google 이미지 검색결과: http://t1.ftcdn.net/jpg/00/11/25/16/400_F_11251687_qfD9laqqERnGxXw...

1:22 AM download - Google 검색

1:22 AM download - Google 검색

1:20 AM web history - Google 검색



분석 대상 정보

▪ History 정보 분석 방법론

- History 정보 분류
 - ✓ 방문사이트 URL
 - ✓ 방문 시간
 - ✓ 방문 횟수
 - ✓ 웹 페이지 제목(Title)
- 방문사이트 URL과 방문 시간 ➔ 해당 사이트의 방문시간 정보
- 방문 URL 내에 GET 방식으로 포함된 인자값 분석
 - ✓ 검색어 정보 추출
 - ✓ 아이디, 패스워드 추출
- URL 내의 특정 키워드를 통한 사용자 행위 분류



분석 대상 정보

■ Cookie 정보

- 웹사이트에서 사용자의 하드디스크에 저장시켜놓는 사용자에 관한 데이터
- 웹 사이트에서 사용자 별, 개인화된 서비스 제공을 위해 사용
 - ✓ 자동 로그인 기능
 - ✓ 웹 쇼핑몰 사이트 : 열람한 물건 리스트, 저장한 물건 리스트
 - ✓ 웹 하드 사이트 : 찜 해놓은 자료, 다운 받은 자료

이름	인터넷 주소
cookie:ojh@...	Cookie:ojh@sunjinsu,tistory.com/
cookie:ojh@...	Cookie:ojh@etnews.co.kr/
cookie:ojh@...	Cookie:ojh@wordpress.bladeforensics.com/
cookie:ojh@...	Cookie:ojh@krdic.naver.com/
js/	Cookie:ojh@krdic.naver.com/js/
cookie:ojh@...	Cookie:ojh@ezinearticles.com/
cookie:ojh@...	Cookie:ojh@msdn.microsoft.com/
cookie:ojh@...	Cookie:ojh@manage.rackspacecloud.com/
cookie:ojh@...	Cookie:ojh@adfront.auction.co.kr/
cookie:ojh@...	Cookie:ojh@stackoverflow.com/
cookie:ojh@...	Cookie:ojh@support.digital-detective.co.uk/
cookie:ojh@...	Cookie:ojh@store.digital-detective.co.uk/



분석 대상 정보

▪ Cookie 정보 분석 방법론

- Cookie 정보 분류
 - ✓ 호스트
 - ✓ 경로
 - ✓ 쿠키 수정 시간
 - ✓ 쿠키 만료 시간
 - ✓ 이름
 - ✓ 값
- 호스트 → 접속한 사이트
- 경로 → 사용한 서비스 유추
- 쿠키 수정 시간 → 해당 사이트의 마지막 접속 시간
- 이름, 값
 - ✓ 로그인 아이디 저장 옵션 활성화 시 → 로그인 아이디 정보 획득 가능
 - ✓ 사용자 Unique ID (ex : Facebook User ID)
 - ✓ Google Analytics 정보



분석 대상 정보

▪ Download List 정보

- 사용자가 의도적으로 선택해서 자신의 컴퓨터로 내려 받은 파일에 대한 정보
- 사용자의 의도와 관계없이 다운받아지는 캐시 데이터와는 구분 필요
- 사용자의 편의를 위해 저장됨
 - ✓ 다운 받은 자료들을 다시 다운 받고 싶을 때

Downloads

Jun 1, 2011



[mtd-utils-1.4.4.tar.bz2](#)

<ftp://ftp.infradead.org/pub/mtd-utils/mtd-utils-1.4.4.tar.bz2>

[Show in folder](#) [Remove from list](#)



[nand-dump.bin](#)

<http://www.filedropper.com/processing/filedownload.php?id=nand-dump>

[Show in folder](#) [Remove from list](#)



[nand-dump.rar](#)

<http://www676.megaupload.com/files/e0c658843d54c027199fb47d3f0d2579/nand-du...>

[Show in folder](#) [Remove from list](#)



[iLividSetupV1.exe](#)

<http://download.cdn.ilivid.com/cdn/r/101/iLividSetupV1.exe>

[Show in folder](#) [Remove from list](#)



분석 대상 정보

▪ Download List 정보 분석 방법론

- Download List 정보 분류
 - ✓ 다운로드 파일의 로컬 저장 경로
 - ✓ 다운로드 소스 URL
 - ✓ 파일크기
 - ✓ 다운로드 시간
 - ✓ 다운로드 성공여부
- 다운로드 소스 URL → 접속한 사이트 확인
- 다운로드 시간 → 해당 파일의 다운로드 시간
- 다운로드 파일의 로컬 경로 → 파일 내용 확인
 - ✓ 파일이 없을 시 → 다운로드 URL을 통해 다운로드 가능

Web Browser 로그 파일 수집

- Web Browser 로그 파일 저장 방식
- 로그 파일 수집
 - Internet Explorer
 - Firefox
 - Chrome
 - Safari
 - Opera



Web Browser 로그 파일 저장 방식

- Windows Profile 경로에 각 사용자 계정 폴더 아래 저장됨
- 여러 명이 사용할 경우, 각 계정 별로 저장됨
- Windows Profile 경로
 - Windows 2000, XP
 - ✓ <시스템 설치 드라이브>\Documents and Settings\<계정명>
 - ✓ Ex) C:\Documents and Settings\wojh
 - Windows Vista, 7
 - ✓ <시스템 설치 드라이브>\Users\<계정명>
 - ✓ Ex) C:\Users\wojh

Web Browser 로그 파일 수집

- Web Browser 로그 파일 저장 방식
- 로그 파일 수집
 - Internet Explorer
 - Firefox
 - Chrome
 - Safari
 - Opera



Internet Explorer 로그 파일 경로

- %Profile% : Profile 경로를 의미

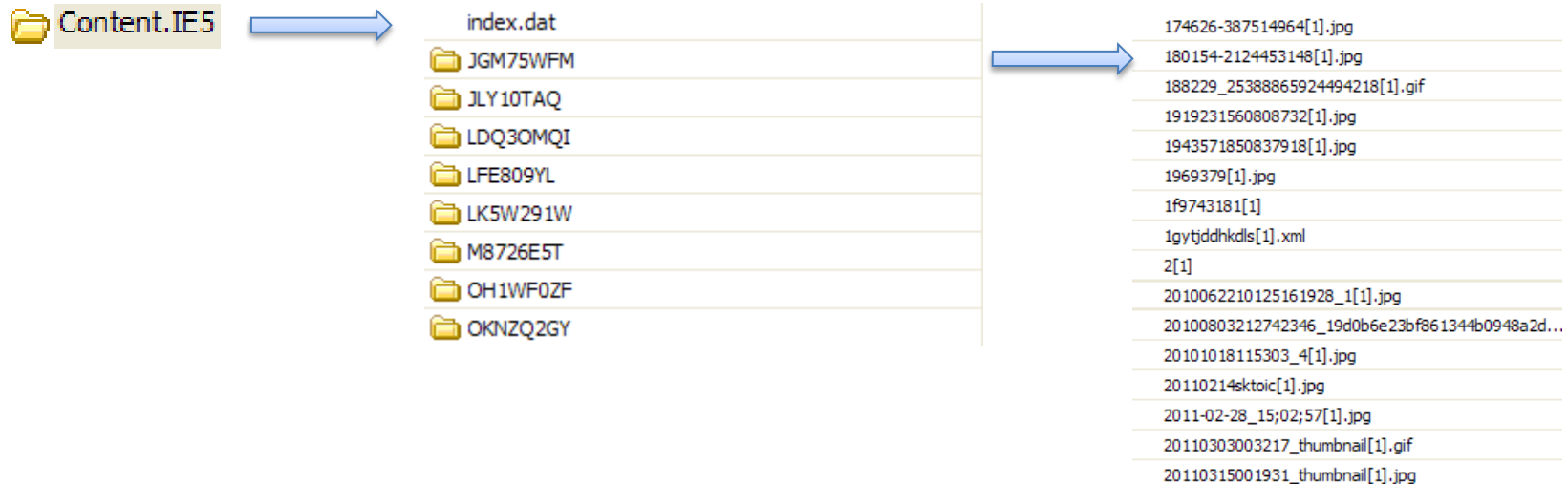
OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%\Local Settings\Temporary Internet Files\Content.IE5\Index.dat %Profile%\Local Settings\Temporary Internet Files\Content.IE5\<Random>\<모든 파일>
	History	%Profile%\Local Settings\History\History.IE5\Index.dat %Profile%\Local Settings\History\History.IE5\<기간>\Index.dat
	Cookie	%Profile%\Cookies\Index.dat %Profile%\Cookies\<모든 텍스트 파일>
	download	없음
Windows Vista, 7	Cache	%Profile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Index.dat %Profile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\<Random>\<모든 파일>
	History	%Profile%\AppData\Local\Microsoft\Windows\History\History.IE5\Index.dat %Profile%\AppData\Local\Microsoft\Windows\History\History.IE5\<기간>\Index.dat
	Cookie	%Profile%\AppData\Roaming\Microsoft\Windows\Cookies\Index.dat %Profile%\AppData\Roaming\Microsoft\Windows\Cookies\<모든 텍스트 파일>
	download	%Profile%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\Index.dat (IE 9 부터 존재)



Internet Explorer 로그 파일 수집 방법(1/4)

Cache 정보

- 다운로드된 캐시 데이터는 Temporary Internet 파일 형태로 저장됨
- index.dat 파일은 Temporary Internet 파일들의 Cache 인덱스 정보를 저장
- 수집 방법
 - ✓ Content.IE5 폴더 아래, index.dat 수집
 - ✓ Content.IE5 폴더 아래, 서브 폴더들 모두 수집 → 폴더 안에 Temporary Internet 파일들이 저장됨

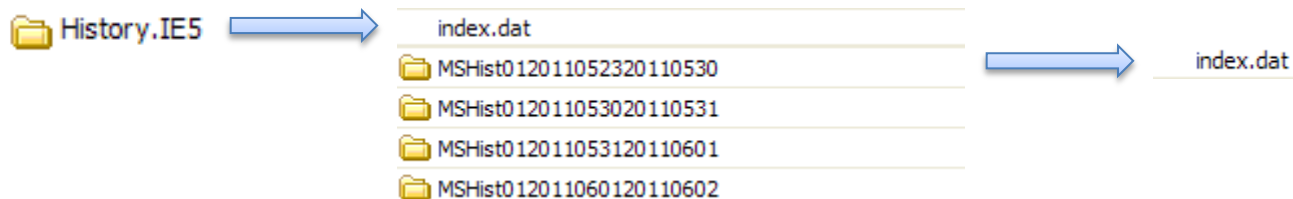




Internet Explorer 로그 파일 수집 방법(2/4)

▪ History 정보

- Hisoty.IE5 폴더 아래, index.dat 파일
 - ✓ 모든 History 정보 저장됨
- Hisoty.IE5 폴더 아래, 기간을 나타내는 서브 폴더가 있음
 - ✓ 해당 기간에 해당하는 일간/주간 History 정보가 저장됨
- 수집 방법
 - ✓ History.IE5 폴더 아래, index.dat 수집
 - ✓ History.IE5 폴더 아래, 모든 서브 폴더 수집 → 폴더 안에 일간/주간 index.dat 파일이 저장됨

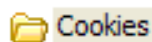




Internet Explorer 로그 파일 수집 방법(3/4)

■ Cookie 정보

- 실제 쿠키 정보는 "계정명@호스트명.txt"형식의 쿠키 파일 안에 저장됨
- index.dat 파일은 쿠키 파일들의 인덱스 정보를 저장함
- 수집 방법
 - ✓ Cookies 폴더 아래, 'index.dat' 파일 수집
 - ✓ Cookies 폴더 아래, 모든 텍스트 파일 수집



index.dat

ojh@100.naver[2].txt

ojh@100.naver[3].txt

ojh@118.107.160[2].txt

ojh@1275875737.sublog.co[1].txt

ojh@163.152.65[2].txt

ojh@211.63.158[2].txt

ojh@4shared[1].txt

ojh@abmr[2].txt



Internet Explorer 로그 파일 수집 방법(4/4)

▪ Download List 정보

- IE 9 버전 이후 부터 존재
- 수집 방법
 - ✓ IEDownloadHistory 폴더 아래, 'index.dat' 파일 수집

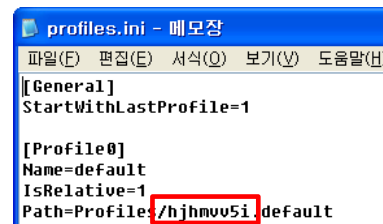
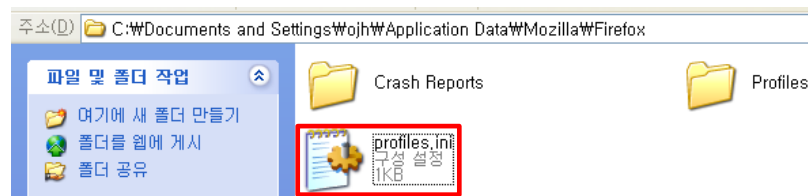




Firefox 로그 파일 경로

- %Profile% : Profile 경로를 의미
- <Random> 정보는 히스토리 경로의 'Firefox' 폴더 아래, 'profiles.ini' 파일 안에 저장됨

OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%\Local Settings\Application Data\Mozilla\Firefox\Profiles\<Random>.default\Cache\CACHE_MAP_ 외 3개 파일 %Profile%\Local Settings\Application Data\Mozilla\Firefox\Profiles\<Random>.default\Cache<모든 폴더>
	History	%Profile%\Application Data\Mozilla\Firefox\Profiles\<Random>.default\places.sqlite
	Cookie	%Profile%\Application Data\Mozilla\Firefox\Profiles\<Random>.default\cookies.sqlite
	download	%Profile%\Application Data\Mozilla\Firefox\Profiles\<Random>.default\downloads.sqlite
Windows Vista, 7	Cache	%Profile%\AppData\Local\Mozilla\Firefox\Profiles\<Random>\Cache\CACHE_MAP_(같은 폴더 안의 모든 파일 필요)
	History	%Profile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\places.sqlite
	Cookie	%Profile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\cookies.sqlite
	download	%Profile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\download.sqlite

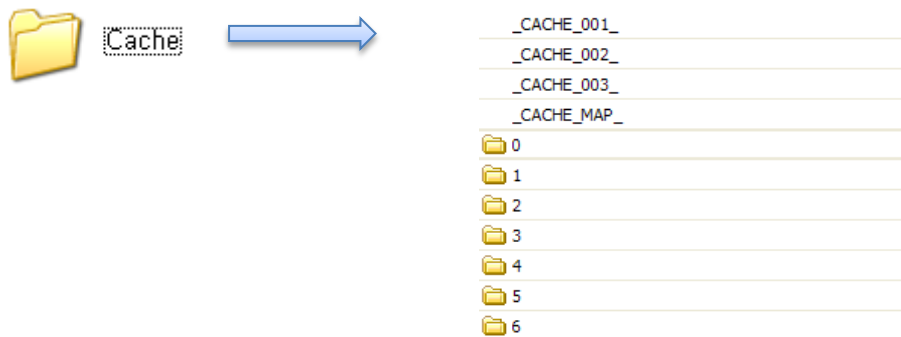




Firefox 로그 파일 수집 방법(1/2)

▪ Cache 정보

- Cache Map File, Separate Cache Data Files, Three Cache Block Files 구조로 이루어짐
- Cache Map File(_CACHE_<MAP~003>_) : 각 Cache 인덱스 정보가 저장됨
- 인덱스 정보를 바탕으로 Meta 데이터와 Content 데이터가 Separate Cache Data Files와 Three Cache Block Files에 저장됨
- 수집 방법
 - ✓ Cache 폴더 아래, _CACHE_MAP_, _CACHE_001_, _CACHE_002_, _CACHE_003_ 파일 수집
 - ✓ Cache 폴더 아래, 모든 폴더 수집





Firefox 로그 파일 수집 방법(2/2)

▪ History, Cookie, Download List 정보

- SQLite Database 파일 형태로 각각 저장됨
 - ✓ History 정보 : places.sqlite
 - ✓ Cookie 정보 : cookies.sqlite
 - ✓ Download 정보 : downloads.sqlite
- 수집 방법
 - ✓ <Random>.default 폴더 아래, places.sqlite, cookies.sqlite, downloads.sqlite 파일 수집





Chrome 로그 파일 경로

- %Profile% : Profile 경로를 의미
- Download List 정보는 History 정보와 함께 'History' 파일안에 저장됨

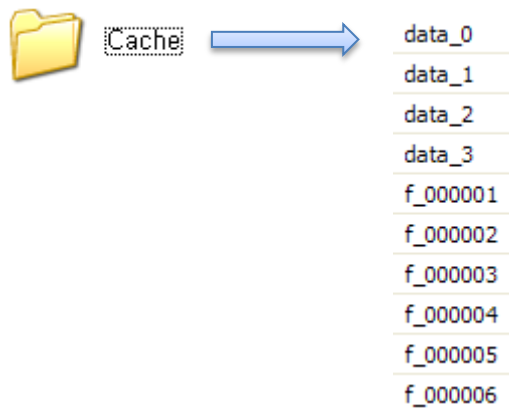
OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache< 모든 파일 >
	History	%Profile%\Local Settings\Application Data\Google\Chrome\User Data\Default\History %Profile%\Local Settings\Application Data\Google\Chrome\User Data\Default\History Index <년-월>
	Cookie	%Profile%\Local Settings\Application Data\Google\Chrome\User Data\Default\Cookies
	download	%Profile%\Local Settings\Application Data\Google\Chrome\User Data\Default\History
Windows Vista, 7	Cache	%Profile%\AppData\Local\Google\Chrome\User Data\Default\Cache\
	History	%Profile%\AppData\Local\Google\Chrome\User Data\Default\History %Profile%\AppData\Local\Google\Chrome\User Data\Default\History\History Index <년-월>
	Cookie	%Profile%\AppData\Local\Google\Chrome\User Data\Default\Cookies
	download	%Profile%\AppData\Local\Google\Chrome\User Data\Default\History



Chrome 로그 파일 수집 방법(1/2)

▪ Cache 정보

- 'data_0' 파일에 데이터 인덱스 정보를, data_1, data_2, data_3 파일과 나머지 파일에 캐시 데이터가 저장됨
- 수집 방법
 - ✓ Cache 폴더 아래, 모든 파일 수집

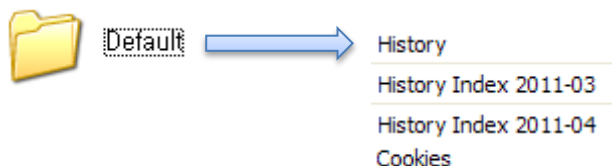




Chrome 로그 파일 수집 방법(2/2)

▪ History, Cookie, Download List 정보

- SQLite Database 파일 형태로 각각 저장됨
 - ✓ History 정보 : History
 - ✓ Cookie 정보 : Cookies
 - ✓ Download 정보 : History
- History 정보의 경우, 월별 정보가 'History Index <년-월>' SQLite 파일로 저장됨
- Download List 정보는 History 정보와 함께 'History' SQLite 파일 안에 저장됨
- 수집 방법
 - ✓ Default 폴더 아래, History, History Index <년-월>, Cookie 파일 수집





Safari 로그 파일 경로


- %Profile% : Profile 경로를 의미

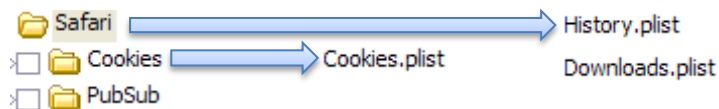
OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%\Local Settings\Application Data\Apple Computer\Safari\Cache.db
	History	%Profile%\Application Data\Apple Computer\Safari\History.plist
	Cookie	%Profile%\Application Data\Apple Computer\Safari\Cookies\Cookies.plist
	download	%Profile%\Application Data\Apple Computer\Safari\Downloads.plist
Windows Vista, 7	Cache	%Profile%\AppData\Local\Apple Computer\Safari\Cache.db
	History	%Profile%\AppData\Roaming\Apple Computer\Safari\History.plist
	Cookie	%Profile%\AppData\Roaming\Apple Computer\Safari\Cookies\Cookies.plist
	download	%Profile%\AppData\Roaming\Apple Computer\Safari\Downloads.plist



Safari 로그 파일 수집 방법

▪ Cache, History, Cookie, Download List 정보

- Cache 데이터, 인덱스 정보 모두 SQLite Database 인 Cache.db 파일에 저장됨
- History, Cookie, Download List 정보는 각각 Plist 파일 형태로 저장됨
 - ✓ History 정보 : History.plist
 - ✓ Cookie 정보 : Cookies.plist
 - ✓ Download List 정보 : Downloads.plist
- 수집 방법
 - ✓ Safari 폴더 아래, Cache.db 파일 수집  Safari → Cache.db
 - ✓ Cookies 폴더 아래, Cookies.plist 파일 수집
 - ✓ Safari 폴더 아래, History.plist, Downloads.plist 파일 수집





Opera 로그 파일 경로

- %Profile% : Profile 경로를 의미

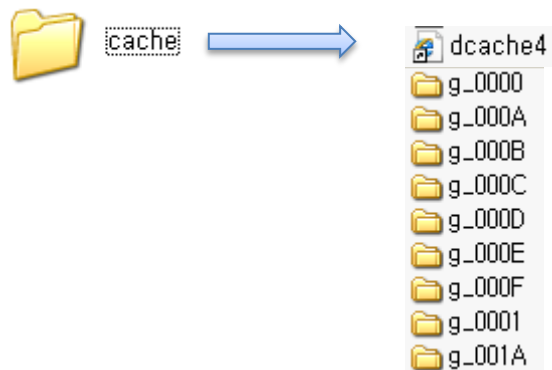
OS 버전	정보	경로
Windows 2000, XP	Cache	%Profile%\Local Settings\Application Data\Opera\Opera\cache\dcache4.url
	History	%Profile%\Application Data\Opera\Opera\global_history.dat
	Cookie	%Profile%\Application Data\Opera\Opera\cookies4.dat
	download	%Profile%\Application Data\Opera\Opera\download.dat
Windows Vista, 7	Cache	%Profile%\AppData\Local\Opera\Opera\cache\dcache4.url
	History	%Profile%\AppData\Roaming\Opera\Opera\global_history.dat
	Cookie	%Profile%\AppData\Roaming\Opera\Opera\cookies4.dat
	download	%Profile%\AppData\Roaming\Opera\Opera\download.dat



Opera 로그 파일 수집 방법(1/2)

▪ Cache 정보

- Cache 인덱스 정보는 dcache4.url 파일에 저장됨
- Cache 데이터 정보는 cache 폴더 아래, 각 서브 폴더에 파일 형태로 저장됨
- 수집 방법
 - ✓ cache 폴더 아래, dcache4.url 파일 수집
 - ✓ cache 폴더 아래, 모든 서브 폴더 수집





Opera 로그 파일 수집 방법(2/2)

▪ History, Cookie, Download List 정보

- History 정보 : global_history.dat
- Cookie 정보 : cookies4.dat
- Download List 정보 : download.dat
- 수집 방법
 - ✓ Opera 폴더 아래, 각 파일들 수집



Internet Explorer 로그 분석

- **Index.dat 로그 파일 분석**
- Cache 정보 분석
- History 정보 분석
- Cookie 정보 분석
- Download List 정보 분석
- 분석 도구



index.dat 로그 파일 분석

- Internet Explorer 에서 사용하는 로그 파일 구조
- Cache , History, Cookie, Download List 정보를 담고 있음
- 저장 정보
 - URL
 - 마지막 수정 시간(FILETIME) => GMT 시간
 - 마지막 접속 시간(FILETIME) => GMT 시간
 - 캐시 폴더 이름
 - Item-파일명
 - HTTP Header

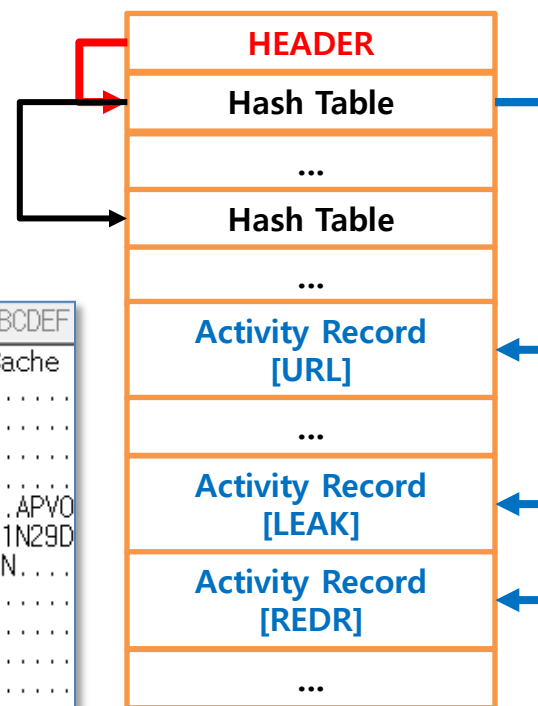


index.dat 로그 파일 분석

■ 전체 구조

- Header
- Hash Tables
- Activity Record Type
 - ✓ URL
 - ✓ REDR
 - ✓ LEAK

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	43	6C	69	65	6E	74	20	55	72	6C	43	61	63	68	65	20	Client UrlCache
00000010	4D	4D	46	20	56	65	72	20	35	2E	32	00	00	C0	93	00	MMF Ver 5.2.....
00000020	00	40	00	00	00	27	01	00	AB	26	00	00	00	00	00	00	.@...'.&.....
00000030	00	00	20	03	00	00	00	00	9E	A8	3A	02	00	00	00	00:.....
00000040	7E	04	00	00	00	00	00	00	04	00	00	00	F9	02	00	00	~.....
00000050	41	36	45	45	39	55	50	38	F7	02	00	00	41	50	56	4F	A8EE9UP8...APVO
00000060	53	56	5A	51	F7	02	00	00	4E	52	37	31	4E	32	39	44	SVZQ...NR71N29D
00000070	F6	02	00	00	39	4D	4E	46	4D	45	31	4E	00	00	00	009MNFME1N....
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00





index.dat 로그 파일 분석

Header

파일 크기

버전 정보

폴더 개수

Cache 폴더 이름

Hash Table 시작 위치

0000	436C	6965	6E74	2055	726C	4361	6368	6520	Client UrlCache
0010	4D4D	4620	5665	7220	352E	3200	0080	8400	MMF Ver 5.2.....
0020	0050	0000	8008	0100	CF52	0000	0000	0000	.P.R.....
0030	0034	4096	0000	0000	0080	B207	0000	0000	.4@.
0040	0000	0000	0000	0000	1800	0000	2001	0000
0050	4731	4D42	3058	594E	1E01	0000	3435	455A	G1MBOXYN...45EZ
0060	4739	415A	1E01	0000	4B35	494E	4F48	454E	G9AZ...K51NOHEN
0070	1E01	0000	4B35	5542	4F44	4D33	1E01	0000	...K5UBODM3...
0080	3431	3246	3054	5142	1E01	0000	3444	495A	412FOTQB...4DIZ

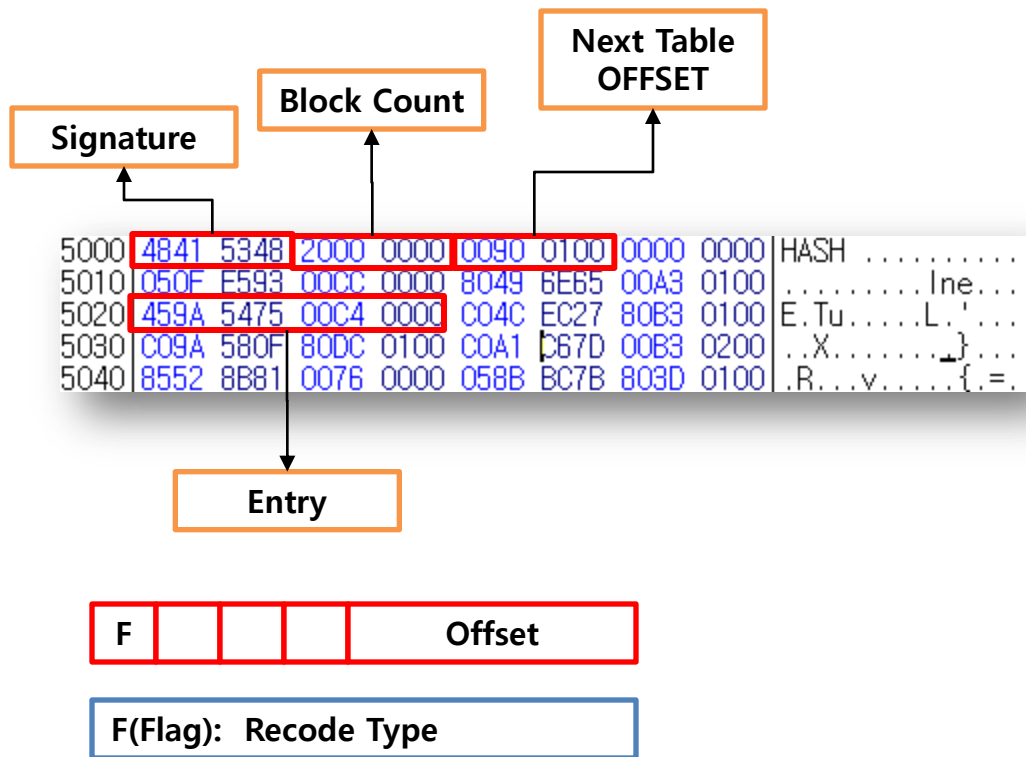
0: G1MBOXYN
1: 45EZG9AZ
...
...
23: 00000000

The screenshot shows the 'Content.IE5' folder in Windows Explorer. The address bar shows the path: C:\Documents and Settings\Wyedong\Local Settings\Temporary Internet Files\Content.IE5. The folder contains several subfolders with names like 2EGVISBK, 9MNFME1N, A6EE9UP8, APVOSVZQ, IGPEZAMJ, JXZFP246, NR71N29D, RJ7R9156, and SNAPSWSB. The 'index.dat' file is also visible at the bottom of the list.



index.dat 로그 파일 분석

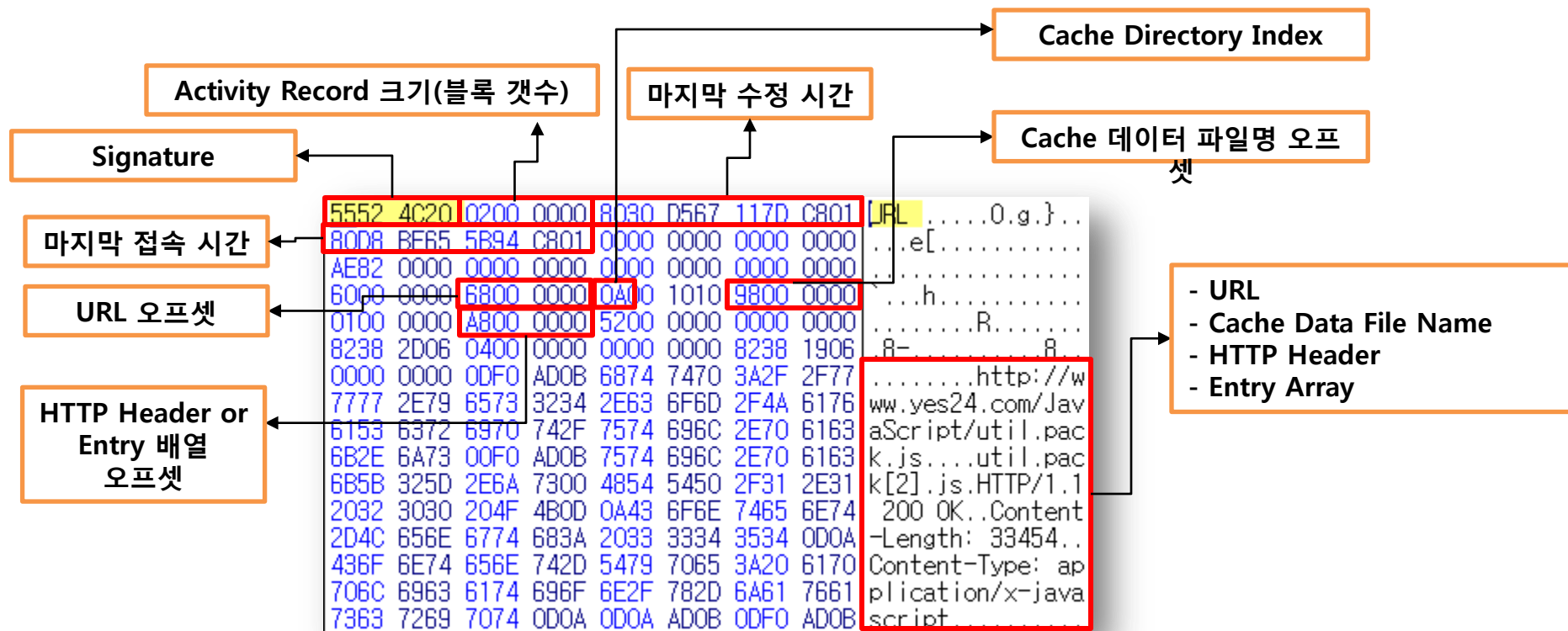
- Hash Table





index.dat 로그 파일 분석

Activity Record





index.dat 로그 파일 분석

▪ 삭제된 Activity Record 복구

- 기한이 지나 삭제된 Activity Record 들은 실제로 삭제되지는 것이 아님
 - ➔ Hash Table 에서 해당 엔트리의 Flag 값이 0x01 or 0x03으로 변경됨
 - ➔ 즉 해당 Record를 Flag 변경을 통해 비 활성화 시킴
- 모든 Activity Record 파싱 : 활성화/비활성 상관없이 모두 읽기
 - ✓ Activity Record는 블록단위로 저장됨. (1개 이상)
 - ✓ 블록의 128byte 임
 - ✓ 전체 파일을 128byte 단위로 스캔하면서 Activity Record의 시그니처인 "URL" 이 나오면 해당 Activity Record 크기 만큼 읽어들이 파싱 작업 수행

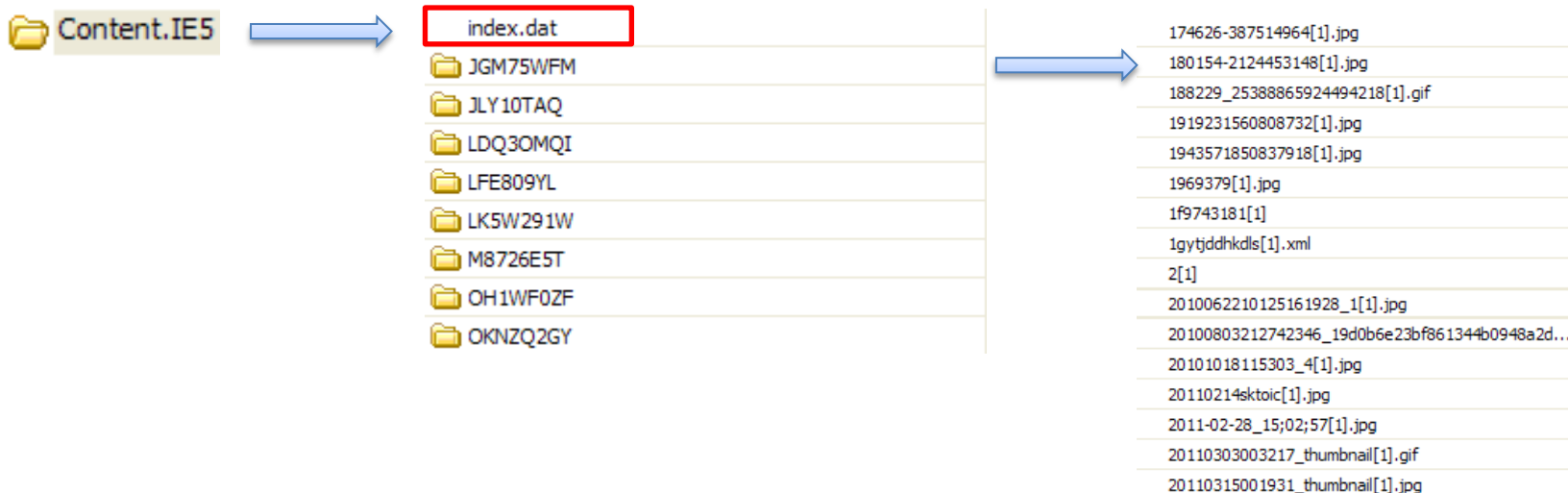
Internet Explorer 로그 분석

- Index.dat 로그 파일 분석
- **Cache 정보 분석**
- History 정보 분석
- Cookie 정보 분석
- Download List 정보 분석
- 분석 도구



Cache 정보 분석

- Cache index.dat 파일은 Cache 인덱스 정보를 가지고 있음
 - 캐시 데이터의 소스 URL
 - 캐시 데이터를 다운 받은 시간 → 접속 시간
 - 캐시 데이터 파일명
 - 캐시 데이터가 저장된 디렉토리 인덱스
- 실제 캐시 데이터는 Content.IE5 폴더 밑에 랜덤한 폴더 아래에 파일 형태로 저장됨
- 다른 index.dat 과 구별 방법 : URL 문자열이 "http://"로 바로 시작함





Cache 정보 분석

Cache index.dat Activity Record 구조

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
004A5900	55	52	4C	20	03	00	00	00	00	6E	2A	39	B8	FE	CA	01
004A5910	80	D1	81	B9	DE	37	CC	01	DD	40	32	3D	00	00	00	00
004A5920	CD	09	00	00	00	00	00	00	00	00	00	00	00	00	00	00
004A5930	60	00	00	00	68	00	00	00	08	00	10	10	94	00	00	00
004A5940	41	00	00	00	A0	00	00	00	8D	00	00	00	00	00	00	00
004A5950	DE	3E	32	3D	02	00	00	00	00	00	00	00	DE	3E	32	3D
004A5960	00	00	00	00	EF	BE	AD	DE	68	74	74	70	3A	2F	2F	77
004A5970	77	77	2E	67	6F	6F	67	6C	65	2E	63	6F	6D	2F	69	6D
004A5980	61	67	65	73	2F	6C	6F	67	6F	73	2F	6C	6F	67	6F	2E
004A5990	67	69	66	00	6C	6F	67	6F	5B	31	5D	2E	67	69	66	00
004A59A0	48	54	54	50	2F	31	2E	31	20	32	30	30	20	4F	4B	0D
004A59B0	0A	43	6F	6E	74	65	6E	74	2D	54	79	70	65	3A	20	69
004A59C0	6D	61	67	65	2F	67	69	66	0D	0A	58	2D	43	6F	6E	74
004A59D0	65	6E	74	2D	54	79	70	65	2D	4F	70	74	69	6F	6E	73
004A59E0	3A	20	6E	6F	73	6E	69	66	66	0D	0A	43	6F	6E	74	65
004A59F0	6E	74	2D	4C	65	6E	67	74	68	3A	20	32	35	30	39	0D
004A5A00	0A	58	2D	58	53	53	2D	50	72	6F	74	65	63	74	69	6F
004A5A10	6E	3A	20	31	3B	20	6D	6F	64	65	3D	62	6C	6F	63	6B
004A5A20	0D	0A	0D	0A	7E	55	3A	6F	6A	68	0D	0A	00	BE	AD	DE
004A5A30	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
004A5A40	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
004A5A50	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
004A5A60	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
004A5A70	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE

URL n*9, bÊ
 INI·07i Y@2=
 í
 , h I
 A I
 b>2= b>2=
 i%-bhttp://w
 www.google.com/im
 ages/logos/logo.
 gif logo[1].gif
 HTTP/1.1 200 OK
 Content-Type: i
 mage/gif X-Cont
 ent-Type-Options
 : nosniff Conte
 nt-Length: 2509
 X-XSS-Protection
 n: 1; mode=block
 ~U:ojh %-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b

- 4 Signature
- 4 Record 크기(128byte x 값)
- 8 마지막 수정 시간(FILETIME)
- 8 마지막 접속 시간 (FILETIME)
- 4 URL 문자열 Offset
- 1 Cache Directory 인덱스
- 4 Cache Date 파일명 Offset
- 4 HTTP 헤더 문자열 Offset
- URL
- Cache Data 파일명
- HTTP 헤더

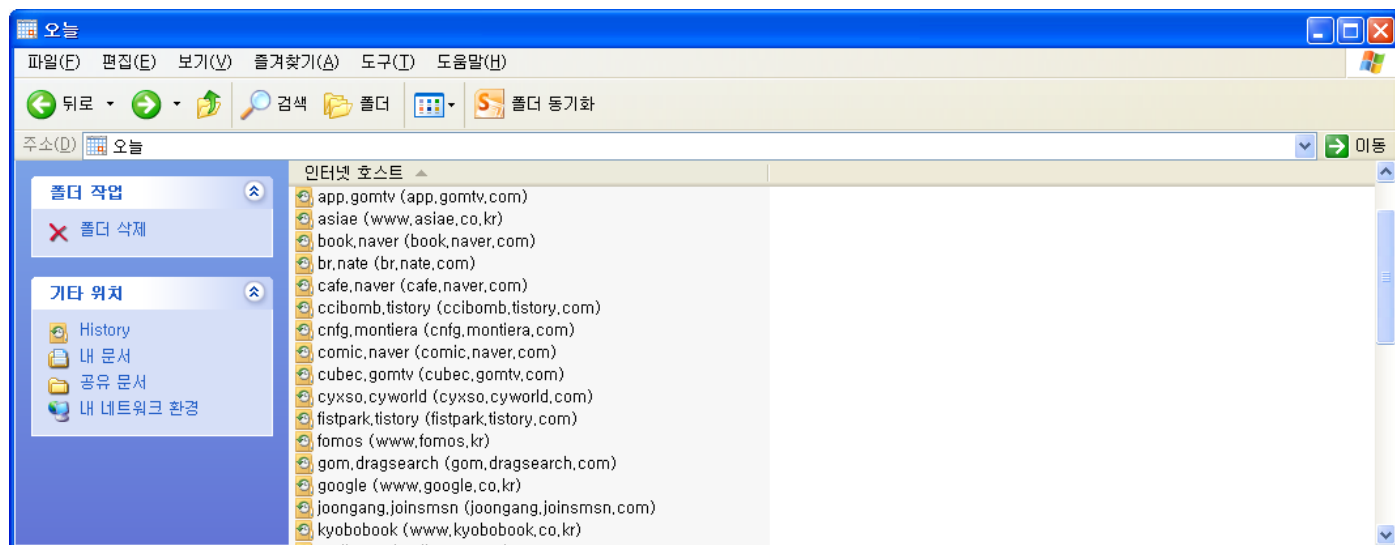
Internet Explorer 로그 분석

- Index.dat 로그 파일 분석
- Cache 정보 분석
- **History 정보 분석**
- Cookie 정보 분석
- Download List 정보 분석
- 분석 도구



History 정보 분석

- History 정보의 경우, History index.dat 파일 안에 모든 정보가 저장되어 있음
- 추가적인 정보를 저장하기 위해 Entry 배열을 사용
- 저장 정보
 - 접속 URL
 - 접속 시간
 - 방문 횟수
 - 웹 페이지 제목
 - 로컬 파일 열람 정보





History 정보 분석

History Index Entry 구조

- 데이터 길이(2바이트) + Entry Type(1바이트) + Value Type(1바이트) + 데이터

Entry type	Value type	Identifier	Description
0x02	0x00		Unknown
0x0e	0x1e		Unknown A GUID formatted as a string {000000-0000-0000-0000-00000000} with NUL character (5 trailing empty bytes)
0x10	0x1f		Page title with NUL characters (4 trailing empty bytes)
0x11	0x01		Filenames Special characters are URL encoded (4 trailing empty bytes)
0x14	0x03		Unknown (4 trailing empty bytes)
0x15	0x1e		HTTP URI of favicon with NUL character (4 trailing empty bytes)
0x16	0x1f		File URI with NUL characters Special characters are URL encoded (4 trailing empty bytes)
0x17	0x13		Unknown (4 trailing empty bytes)
0x18	0x40		Unknown Contains a filetime (4 trailing empty bytes)
0x1c	0x03		Unknown (4 trailing empty bytes)
0x1e	0x40		Unknown Contains a filetime (4 trailing empty bytes)
0x20	0x03		Unknown (4 trailing empty bytes)



History 정보 분석

History index.dat Activity Record 구조

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00028500	55	52	4C	20	03	00	00	00	F0	7C	A9	0A	31	3A	CC	01
00028510	F0	7C	A9	0A	31	3A	CC	01	FE	3E	6A	4F	00	00	00	00
00028520	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00028530	60	00	00	00	68	00	00	00	FE	00	10	10	00	00	00	00
00028540	01	00	20	00	CC	00	00	00	90	00	00	00	00	00	00	00
00028550	E4	3E	6A	4F	05	00	00	00	00	00	00	00	00	00	00	00
00028560	00	00	00	00	EF	BE	AD	DE	56	69	73	69	74	65	64	3A
00028570	20	6F	6A	68	40	68	74	74	70	3A	2F	2F	73	65	61	72
00028580	63	68	2E	6E	61	76	65	72	2E	63	6F	6D	2F	73	65	61
00028590	72	63	68	2E	6E	61	76	65	72	3F	73	6D	3D	74	61	62
000285A0	5F	68	74	79	26	77	68	65	72	65	3D	6E	65	78	65	61
000285B0	72	63	68	26	71	75	65	72	79	3D	64	69	67	69	74	61
000285C0	6C	2B	66	6F	72	65	6E	73	69	63	73	00	10	00	02	00
000285D0	00	00	00	10	00	00	00	00	01	00	00	00	2C	00	15	1E
000285E0	68	74	74	70	3A	2F	2F	73	65	61	72	63	68	2E	6E	61
000285F0	76	65	72	2E	63	6F	6D	2F	66	61	76	69	63	6F	6E	2E
00028600	69	63	6F	00	00	00	00	00	0C	00	14	03	01	00	00	00
00028610	00	00	00	00	44	00	10	1F	64	00	69	00	67	00	69	00
00028620	74	00	61	00	6C	00	20	00	66	00	6F	00	72	00	65	00
00028630	6E	00	73	00	69	00	63	00	73	00	20	00	3A	00	3A	00
00028640	20	00	24	B1	74	C7	84	BC	20	00	B5	D1	69	D5	80	AC
00028650	C9	C0	00	00	00	00	00	00	00	00	00	00	EF	BE	AD	DE
00028660	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
00028670	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE

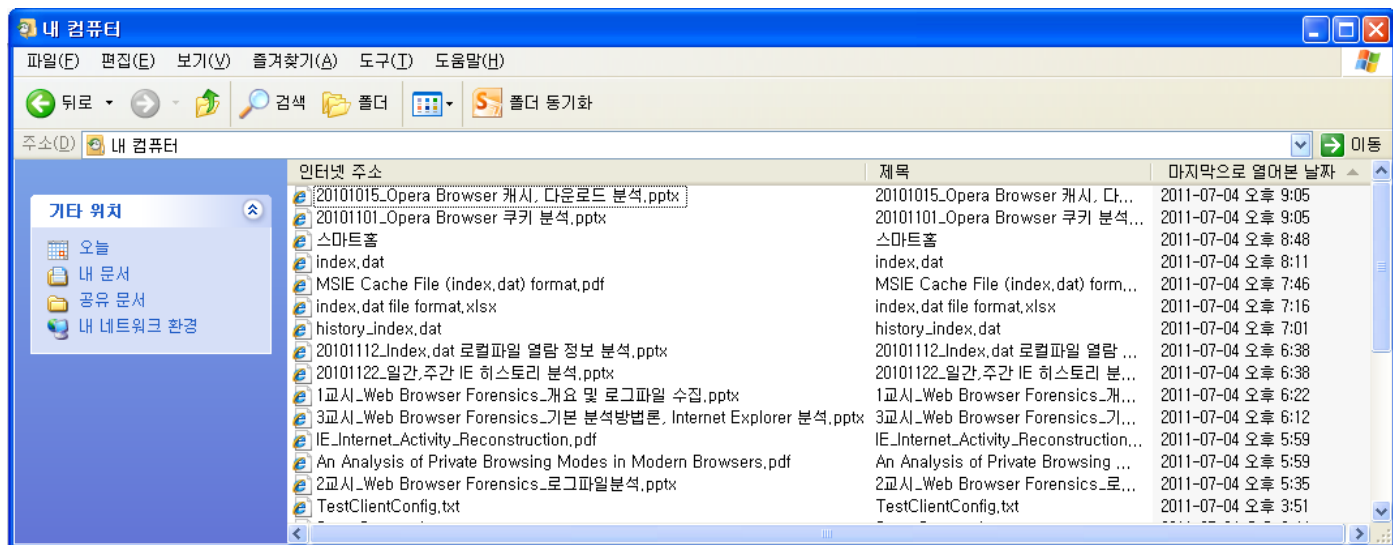
URL 8|@ 1:İ
8|@ 1:İ p>j0
h p
İ I
ä>j0
i%~p Visited:
ojh@http://search.naver.com/search.naver?sm=tab_hfty&where=nexearch&query=digital+forensics
http://search.naver.com/favicon.ico
D d i g i
t a l f o r e
n s i c s : :
\$t+C I 4 µN i O I -
EÄ i%~p
i%~p i%~p i%~p i%~p
i%~p i%~p i%~p i%~p

- Signature
- Record 크기(128byte x 값)
- 마지막 수정 시간(FILETIME)
- 마지막 접속 시간 (FILETIME)
- URL 문자열 Offset
- Entry 배열 Offset
- 방문 횟수
- URL
- 웹 페이지 제목 ENTRY HEADER
- 웹 페이지 제목



History index.dat 로컬 파일 열람 정보

- History Index.dat 파일 안에 인터넷 방문 정보와 함께 저장됨
- URL 이 “file:///” 로 시작됨
- **파일 열기 동작을 기록**(파일 실행은 기록하지 않음)
 - 대상 파일 경로
 - 열기 작업 수행 시간
- 브라우저 사용정보 삭제 기능 작동 시, 같이 삭제됨



인터넷 주소	제목	마지막으로 열려본 날짜
20101015_Opera Browser 캐시, 다운로드 분석.pptx	20101015_Opera Browser 캐시, 다...	2011-07-04 오후 9:05
20101101_Opera Browser 쿠키 분석.pptx	20101101_Opera Browser 쿠키 분석...	2011-07-04 오후 9:05
스마트홈	스마트홈	2011-07-04 오후 8:48
index.dat	index.dat	2011-07-04 오후 8:11
MSIE Cache File (index.dat) format.pdf	MSIE Cache File (index.dat) form...	2011-07-04 오후 7:46
index.dat file format.xlsx	index.dat file format.xlsx	2011-07-04 오후 7:16
history_index.dat	history_index.dat	2011-07-04 오후 7:01
20101112_Index.dat 로컬파일 열람 정보 분석.pptx	20101112_Index.dat 로컬파일 열람 ...	2011-07-04 오후 6:38
20101122_일간,주간 IE 히스토리 분석.pptx	20101122_일간,주간 IE 히스토리 분...	2011-07-04 오후 6:38
1교시_Web Browser Forensics_개요 및 로그파일 수집.pptx	1교시_Web Browser Forensics_개...	2011-07-04 오후 6:22
3교시_Web Browser Forensics_기본 분석방법론, Internet Explorer 분석.pptx	3교시_Web Browser Forensics_기...	2011-07-04 오후 6:12
IE_Internet_Activity_Reconstruction.pdf	IE_Internet_Activity_Reconstruction...	2011-07-04 오후 5:59
An Analysis of Private Browsing Modes in Modern Browsers.pdf	An Analysis of Private Browsing ...	2011-07-04 오후 5:59
2교시_Web Browser Forensics_로그파일분석.pptx	2교시_Web Browser Forensics_로...	2011-07-04 오후 5:35
TestClientConfig.txt	TestClientConfig.txt	2011-07-04 오후 3:51



History index.dat 로컬 파일 열람 정보

- URL 정보에는 열람한 파일의 Full Path를 저장(다국어인 경우 UTF-8로 URL 인코딩)
- Entry 배열의 웹 페이지 제목 Entry에 유니코드로 인코딩한 Full Path

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00020480	55	52	4C	20	03	00	00	00	10	85	DE	1F	73	81	CB	01	URL
00020496	10	85	DE	1F	73	81	CB	01	87	3D	89	3C	00	00	00	00	IP sIE
00020512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	IP sIE I-I<
00020528	60	00	00	00	68	00	00	00	FE	00	10	10	00	00	00	00	h p
00020544	01	00	20	00	D8	00	00	00	9C	00	00	00	00	00	00	00	0 I
00020560	6B	3D	89	3C	01	00	00	00	00	00	00	00	00	00	00	00	k-I<
00020576	00	00	00	00	EF	BE	AD	DE	56	69	73	69	74	65	64	3A	i%-bVisited:
00020592	20	6F	6A	68	40	66	69	6C	65	3A	2F	2F	2F	43	3A	2F	ojh@file:///C:/
00020608	44	6F	63	75	6D	65	6E	74	73	25	32	30	61	6E	64	25	Documents%20and%
00020624	32	30	53	65	74	74	69	6E	67	73	2F	6F	6A	68	2F	25	20Settings/ojh/%
00020640	45	42	25	42	30	25	39	34	25	45	44	25	38	33	25	39	EB%B0%94%ED%83%9
00020656	35	25	32	30	25	45	44	25	39	39	25	39	34	25	45	42	5%20%ED%99%94%EB
00020672	25	41	39	25	42	34	2F	54	45	53	54	2F	54	45	53	54	%A9%B4/TEST/TEST
00020688	2E	70	64	66	00	BE	AD	DE	10	00	02	00	00	00	00	10	.pdf %-b
00020704	00	00	00	00	01	00	00	00	88	00	16	1F	66	00	69	00	I f i
00020720	6C	00	65	00	3A	00	2F	00	2F	00	2F	00	43	00	3A	00	l e : / / / C :
00020736	2F	00	44	00	6F	00	63	00	75	00	6D	00	65	00	6E	00	/ D o c u m e n
00020752	74	00	73	00	25	00	32	00	30	00	61	00	6E	00	64	00	t s % 2 0 a n d
00020768	25	00	32	00	30	00	53	00	65	00	74	00	74	00	69	00	% 2 0 S e t t i
00020784	6E	00	67	00	73	00	2F	00	6F	00	6A	00	68	00	2F	00	n g s / o j h /
00020800	14	BC	D5	D0	25	00	32	00	30	00	54	D6	74	BA	2F	00	% 2 0 T 0 t 2 /
00020816	54	00	45	00	53	00	54	00	2F	00	54	00	45	00	53	00	T E S T / T E S
00020832	54	00	2E	00	70	00	64	00	66	00	00	00	00	00	00	00	T . p d f
00020848	00	00	00	00	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	i%-b i%-b i%-b



History index.dat 로컬 파일 열람 정보

▪ 기록된 파일 종류

- 텍스트 파일 : txt
- 한글 파일: hwp
- 오피스 파일 : doc, docx, ppt, pptx, xls, xlsx, one ...
- PDF 파일: pdf
- 이미지 파일 : bmp, gif, jpg, png ...
- HTML 파일 : html
- 압축 파일 : rar, egg, alz ...
- 이미지 파일 : iso, E01(인케이스 이미지) ...
- 기타 파일: sln, Enpack(인스크립트) ...

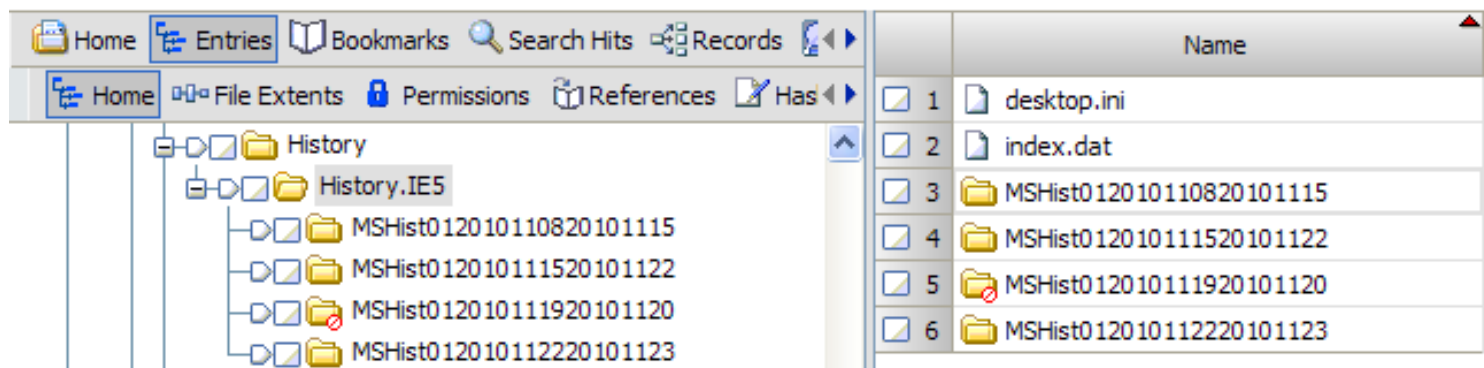
▪ 기록되는 경우

- 파일 더블 클릭으로 열 때 기록됨
- 어플리케이션에서 불러오기 기능으로 열 때 기록됨
- 드래그로 불러올 때 기록됨



Daily/Weekly History index.dat 분석

- **일간 index.dat**
 - 해당 날짜의 인터넷 방문 기록 포함
- **주간 index.dat**
 - 해당 주간의 인터넷 방문 기록 포함
 - 일간 index.dat가 일주일 동안 모이면 주간 index.dat로 병합됨
 - ➔ 기존에 있는 일간 index.dat 파일은 삭제됨
 - ➔ 비 할당 영역 카빙 작업시, 일간 index.dat 가 많이 남음





Daily/Weekly History index.dat 분석

- 시간 기록 방식
 - 해당 기간 내 동일 URL일 경우, 최근 방문 시간으로 갱신됨
 - ➔ 기록된 방문 시간은 처음 방문 시간 or 마지막 방문 시간
- 기록된 시간 내용
 - index.dat
 - ✓ 0x08 : 마지막 수정시간
 - ✓ 0x10 : 마지막 방문 시간
 - Daily index.dat
 - ✓ 0x08 : 마지막 접근 LOCAL 시간
 - ✓ 0x10 : 마지막 접근 UTC 시간
 - Weekly index.dat
 - ✓ 0x08 : 마지막 접근 LOCAL 시간
 - ✓ 0x10 : 파일 생성 UTC 시간
 - ➔ 주간 index.dat 파일 생성시간을 UTC 시간으로 기록



Daily History index.dat의 Activity Record 구조

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00009E80	55	52	4C	20	02	00	00	00	00	80	20	A1	CB	38	CC	01
00009E90	B0	64	49	12	92	39	CC	01	FC	3E	9A	32	00	00	00	00
00009EA0	00	00	00	00	00	00	00	00	00	00	00	00	80	51	01	00
00009EB0	60	00	00	00	68	00	00	00	FE	00	10	10	00	00	00	00
00009EC0	04	00	20	00	00	00	00	00	00	00	00	00	00	00	00	00
00009ED0	E3	3E	2C	78	01	00	00	00	00	00	00	00	00	00	00	00
00009EE0	00	00	00	00	EF	BE	AD	DE	3A	32	30	31	31	30	36	32
00009EF0	37	32	30	31	31	30	37	30	34	3A	20	6F	6A	68	40	68
00009F00	74	74	70	3A	2F	2F	77	77	77	2E	66	6F	6D	6F	73	2E
00009F10	6B	72	2F	67	6E	75	62	6F	61	72	64	34	2F	62	62	73
00009F20	2F	62	6F	61	72	64	2E	70	68	70	3F	62	6F	5F	74	61
00009F30	62	6C	65	3D	74	61	6C	6B	5F	74	76	26	77	72	5F	69
00009F40	64	3D	32	33	31	31	34	38	26	70	61	67	65	3D	35	00
00009F50	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
00009F60	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
00009F70	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE

URL | iE8I
 °dI °9I ü>I2
 IQ
 h b
 ä>,x
 i%-b:2011062
 720110704: ojh@h
 ttp://www.fomos.
 kr/gnuboard4/bbs
 /board.php?bo_ta
 ble=talk_tv&wr_i
 d=231148&page=5
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b

- 4** Signature
- 4** Record 크기(128byte x 값)
- 8** 마지막 접속시간 (FILETIME, LOCAL)
- 8** 마지막 접속시간 (FILETIME, UTC)
- 4** URL 문자열 Offset
- URL**



Weekly History index.dat의 Activity Record 구조

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00007900	55	52	4C	20	02	00	00	00	B0	23	C1	33	87	37	CC	01
00007910	70	A3	63	12	92	39	CC	01	FA	3E	EC	7B	00	00	00	00
00007920	00	00	00	00	00	00	00	00	00	00	00	00	80	51	01	00
00007930	60	00	00	00	68	00	00	00	FE	00	10	10	00	00	00	00
00007940	04	00	20	00	00	00	00	00	00	00	00	00	00	00	00	00
00007950	E3	3E	2C	78	01	00	00	00	00	00	00	00	00	00	00	00
00007960	00	00	00	00	EF	BE	AD	DE	3A	32	30	31	31	30	36	32
00007970	37	32	30	31	31	30	37	30	34	3A	20	6F	6A	68	40	68
00007980	74	74	70	3A	2F	2F	66	6F	72	65	6E	73	69	63	2E	6B
00007990	6F	72	65	61	2E	61	63	2E	6B	72	2F	64	66	72	63	2F
000079A0	73	75	62	5F	70	72	6F	6A	65	63	74	2F	5F	70	72	6F
000079B0	6A	65	63	74	5F	36	2E	70	68	70	00	DE	EF	BE	AD	DE
000079C0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
000079D0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
000079E0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
000079F0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE

URL °#Å3!7İ
pfc '9İ ú>i{
IQ
h p
ä>,x
i%-b:2011062
720110704: ojh@h
ttp://forensic.k
orea.ac.kr/dfrc/
sub_project/_pro
ject_6.php i%-b
i%-b i%-b i%-b i%-b
i%-b i%-b i%-b i%-b
i%-b i%-b i%-b i%-b
i%-b i%-b i%-b i%-b

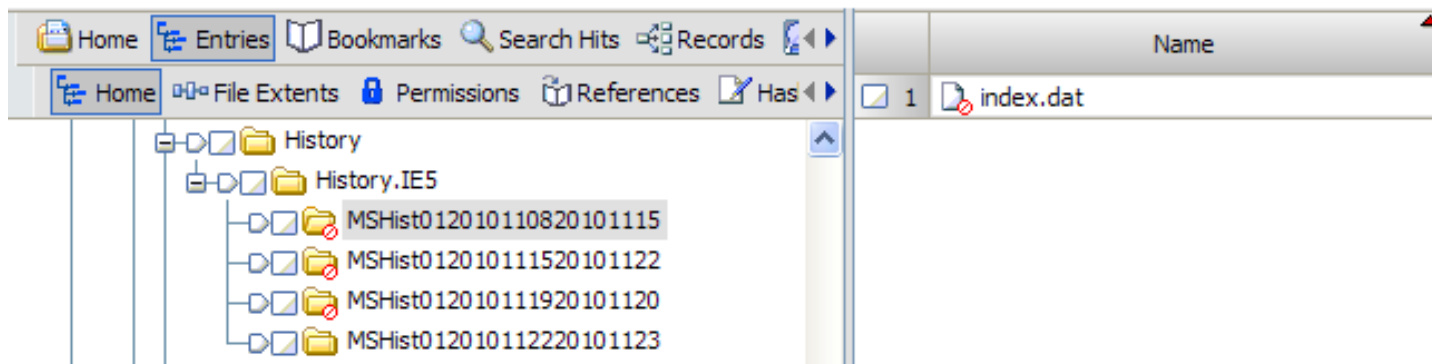
- 4 Signature
- 4 Record 크기(128byte x 값)
- 8 마지막 접속시간 (FILETIME, LOCAL)
- 8 파일 생성시간 (FILETIME, UTC)
- 4 URL 문자열 Offset
- URL



Daily/Weekly History index.dat 분석의 필요성

■ 삭제된 사용 정보 복구 관점

- 일반 index.dat 파일은 사용 정보 삭제 시, 0으로 초기화됨
 - ➔ 복구 불가능
- 일간/주간 index.dat 파일은 사용 정보 삭제 시, 폴더와 파일이 삭제됨
 - ➔ 삭제 파일 복구 가능
 - ➔ 빠른 시간 안에 복구 시, IE 히스토리 정보 추출 가능



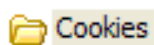
Internet Explorer 로그 분석

- Index.dat 로그 파일 분석
- Cache 정보 분석
- History 정보 분석
- **Cookie 정보 분석**
- Download List 정보 분석
- 분석 도구



Cookie 정보 분석

- Cookie index.dat 파일에는 Cookie 파일에 대한 인덱스 정보만 저장됨
- 실제 쿠키 정보는 “계정명@호스트명.txt”형식의 쿠키 파일 안에 저장됨
 - ➔ 추가적인 텍스트 쿠키 파일 파싱 필요



index.dat

ojh@100.naver[2].txt

ojh@100.naver[3].txt

ojh@118.107.160[2].txt

ojh@1275875737.sublog.co[1].txt

ojh@163.152.65[2].txt

ojh@211.63.158[2].txt

ojh@4shared[1].txt

ojh@abmr[2].txt



Cookie 정보 분석

Cookie index.dat 의 Activity Record 구조

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000DD00	55	52	4C	20	02	00	00	00	20	8D	28	87	4A	21	CC	01
0000DD10	20	8D	28	87	4A	21	CC	01	E2	3E	99	8B	00	00	00	00
0000DD20	95	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DD30	60	00	00	00	68	00	00	00	FE	00	10	10	84	00	00	00
0000DD40	01	00	10	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DD50	C2	3E	98	8B	08	00	00	00	00	00	00	00	C2	3E	98	8B
0000DD60	00	00	00	00	EF	BE	AD	DE	43	6F	6F	6B	69	65	3A	6F
0000DD70	6A	68	40	77	77	77	2E	64	61	75	6D	2E	6E	65	74	2F
0000DD80	00	BE	AD	DE	6F	6A	68	40	77	77	77	2E	64	61	75	6D
0000DD90	5B	31	5D	2E	74	78	74	00	EF	BE	AD	DE	EF	BE	AD	DE
0000DDA0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
0000ddb0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
0000DDC0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
0000DDD0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
0000DDE0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE
0000DDF0	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE

URL (IJ!)
 (IJ!) Å>||
 h p |
 Å>|| Å>||
 i%-bCookie:o
 jh@www.daum.net/
 %-poj@www.daum
 [1].txt i%-b i%-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b
 i%-b i%-b i%-b i%-b

- 4 Signature
- 4 Record 크기(128byte x 값)
- 8 마지막 수정 시간(FILETIME)
- 8 마지막 접속 시간 (FILETIME)
- 4 Cookie 파일명 Offset
- 1 Cookie 파일명



Cookie 정보 분석

■ 텍스트 파일 형식

- 라인 단위로 데이터 저장
- 별표(*)로 각 Cookie 데이터 구분

■ 저장 데이터

- 변수/값
- 호스트/패스
- 쿠키 만료 시간
- 쿠키 생성시간

```
sffocus  
home  
securityfocus.com/  
0  
1238799232  
29570658  
1484443312  
29552553  
*
```

Line	Summary
1	The Variable Name
2	The Value for the Variable
3	The Website of the Cookie's Owner
4	Optional Flags
5	The Most Significant Integer for Expired Time, in FILETIME Format
6	The Least Significant Integer for Expired Time, in FILETIME Format
7	The Most Significant Integer for Creation Time, in FILETIME Format
8	The Least Significant Integer for Creation Time, in FILETIME Format
9	The Cookie Record Delimiter (a * character)

Internet Explorer 로그 분석

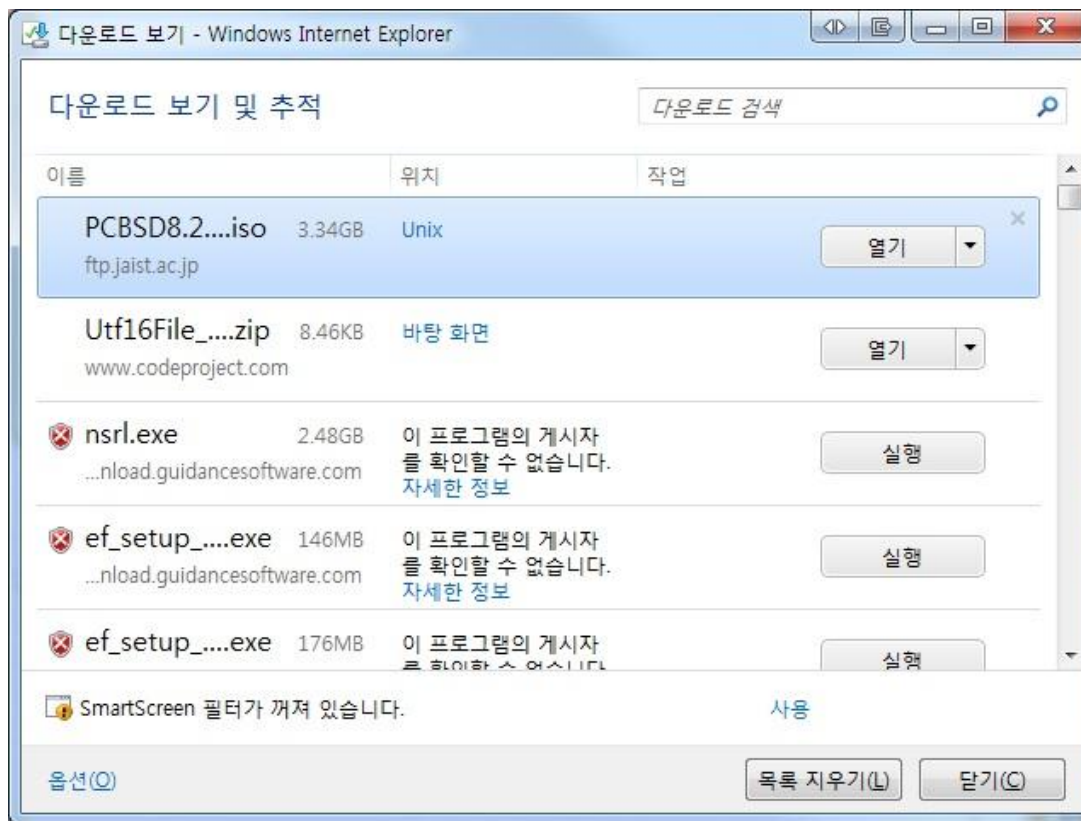
- Index.dat 로그 파일 분석
- Cache 정보 분석
- History 정보 분석
- Cookie 정보 분석
- **Download List 정보 분석**
- 분석 도구



Download List 정보 분석

Download index.dat ?

- IE 9 부터 지원되는 Download Manager의 로그파일
- IE9는 WIN 7 이상에만 동작되므로 WIN7 이상에서만 존재





Download List 정보 분석

▪ Download index.dat 분석

- 기본 구조는 기존 index.dat 동일(Activity Record 구조가 다름)
- URL 저장 위치에 GUID 값 저장
- HTTP 헤더 or 엔트리 배열 위치에 다운로드 데이터 버퍼가 위치
- 버퍼 시작 위치 부터 0x48 위치에는 8바이트 크기의 다운로드 데이트 정보 위치
- 버퍼 시작 위치 부터 0x138위치부터 문자열 배열 시작
- 문자열 배열의 마지막 문자열은 다운로드 데이터 저장 경로
- 마지막 문자열 바로 전 문자열은 다운로드 소스 URL



Download List 정보 분석

Download index.dat Active Record 구조

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00008D80	55	52	4C	20	05	00	00	00	00	00	00	00	00	00	00	00
00008D90	71	86	FF	EA	9F	17	CC	01	00	00	00	00	00	00	00	00
00008DA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008DB0	00	00	00	00	68	00	00	00	FE	00	10	10	00	00	00	00
00008DC0	09	00	00	00	9C	00	00	00	DA	01	00	00	00	00	00	00
00008DD0	B5	3E	D9	51	02	00	00	00	00	00	00	00	00	00	00	00
00008DE0	00	00	00	00	EF	BE	AD	DE	69	65	64	6F	77	6E	6C	6F
00008DF0	61	64	3A	7B	31	42	38	39	33	34	35	44	2D	38	33	39
00008E00	33	2D	31	31	45	30	2D	38	34	37	45	2D	30	30	35	30
00008E10	35	36	43	30	30	30	38	7D	00	AD	DE	85	00	00	00	00
00008E20	08	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008E30	2D	CB	3F	C4	8F	83	E0	11	84	7E	00	50	56	C0	00	08
00008E40	71	86	FF	EA	9F	17	CC	01	00	00	00	00	95	01	00	00
00008E50	00	00	00	00	01	00	00	00	00	00	00	00	01	00	00	00
00008E60	01	00	00	00	92	3E	00	00	00	00	00	00	B4	05	00	00
00008E70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008E80	00	00	00	00	00	00	00	00	00	00	00	00	06	00	00	00
00008E90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008EA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008EB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008EC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008ED0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008EE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008EF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008F00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008F10	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008F20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008F30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008F40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00008F50	00	00	00	00	66	00	74	00	70	00	3A	00	2F	00	2F	00
00008F60	66	00	74	00	70	00	2E	00	63	00	69	00	73	00	63	00
00008F70	6F	00	2E	00	63	00	6F	00	6D	00	2F	00	70	00	75	00
00008F80	62	00	2F	00	6D	00	69	00	62	00	73	00	2F	00	76	00
00008F90	32	00	2F	00	43	00	49	00	53	00	43	00	4F	00	2D	00
00008FA0	53	00	4D	00	49	00	2E	00	6D	00	79	00	00	00	43	00
00008FB0	3A	00	5C	00	75	00	73	00	72	00	5C	00	73	00	68	00
00008FC0	61	00	72	00	65	00	5C	00	73	00	6E	00	6D	00	70	00
00008FD0	5C	00	6D	00	69	00	62	00	73	00	5C	00	43	00	49	00
00008FE0	53	00	43	00	4F	00	2D	00	53	00	4D	00	49	00	2E	00
00008FF0	6D	00	79	00	00	00	AD	DE	EF	BE	AD	DE	EF	BE	AD	DE

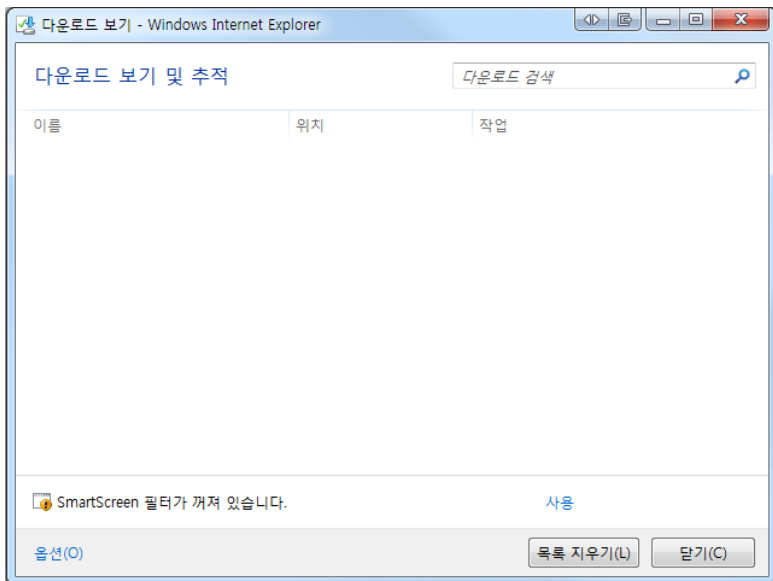
- 마지막 접속 시간 (FILETIME)
- 다운로드 데이터 버퍼 Offset
- 다운로드 데이터 버퍼 크기
- 다운로드 데이터 크기
- 다운로드 소스 URL
- 다운로드 데이터 저장 경로
- 다운로드 데이터 버퍼



Download List 정보 분석

■ 사용자 정보 삭제시 동작

- 다른 index.dat 파일과는 다르게 index.dat 파일을 초기화하지 **않음**
- 레코드만 비활성화
 - ✓ 파일 내에서 지워지지 **않음**
 - ✓ WEFA의 파싱 방식으로 모두 복구 가능



개시	히스토리	쿠키	검색어	다운로드 목록	로컬파일 열람	타임라인
브라우저	파일명	URL	저장위치	저장시간	파일크기(Byte)	다운로드 결과
<input type="checkbox"/> Internet Explorer	1_2장-hwp	http://bigmail.net...	C:\Users\Wson...	2011-05-12 23:52:36	13180928	
<input type="checkbox"/> Internet Explorer	DejaVu-Sans-Mono.zip	tp://www.font...	C:\Users\Wson...	2011-05-13 00:50:30	0	
<input type="checkbox"/> Internet Explorer	1_2장-hwp	http://bigmail.net...	C:\Users\Wson...	2011-05-13 01:37:47	12246016	
<input type="checkbox"/> Internet Explorer	익스트림스위치...	http://www.daso...	C:\Users\Wson...	2011-05-13 16:20:05	165376	
<input type="checkbox"/> Internet Explorer	VS10sp1-KB9835...	http://download...	E:\Win7\Visual S...	2011-05-12 20:36:37	813920	
<input type="checkbox"/> Internet Explorer	NanumGothicCod...	http://dev.naver...	C:\Users\Wson...	2011-05-13 00:48:11	2176424	
<input type="checkbox"/> Internet Explorer	net-snmp-5.5.1.zip	http://cdnetwor...	C:\Users\Wson...	2011-05-13 17:10:39	6636927	
<input type="checkbox"/> Internet Explorer	양식_8(사용서)...	http://cst.korea...	C:\Users\Wson...	2011-05-13 14:24:40	16384	
<input type="checkbox"/> Internet Explorer	양식_8(사용서)...	http://cst.korea...	C:\Users\Wson...	2011-05-13 14:24:39	16384	
<input type="checkbox"/> Internet Explorer	spm1993.zip	http://www.nets...	C:\Users\Wson...	2011-05-15 22:24:03	6515225	
<input type="checkbox"/> Internet Explorer	UFED Commercial...	https://mail.goog...	E:\WCIST\W00.Pr...	2011-05-16 04:36:42	302439	
<input type="checkbox"/> Internet Explorer	bpak-9.exe	http://www.oidvi...	C:\Users\Wson...	2011-05-16 12:01:29	5858280	
<input type="checkbox"/> Internet Explorer	bpak-0.exe	http://www.oidvi...	C:\Users\Wson...	2011-05-16 11:54:48	1975542	
<input type="checkbox"/> Internet Explorer	CISCO-SMT.my	ftp://ftp.disco...	C:\Users\Wshare...	2011-05-21 19:14:49	16002	
<input type="checkbox"/> Internet Explorer	OV_R45_Win7.exe	http://www.oidvi...	C:\Users\Wson...	2011-05-16 00:47:32	17027896	
<input type="checkbox"/> Internet Explorer	CISCO-SMT.my	ftp://ftp.disco...	C:\Users\Wshare...	2011-05-21 19:14:49	16002	
<input type="checkbox"/> Internet Explorer	WebPageToImag...	http://www.code...	C:\Users\Wson...	2011-05-17 01:44:23	1649218	
<input type="checkbox"/> Internet Explorer	WebPageToImag...	http://www.code...	C:\Users\Wson...	2011-05-17 01:44:50	12230	
<input type="checkbox"/> Internet Explorer	wirelesskeyview.zip	http://nirsoft.net...	C:\Users\Wson...	2011-05-21 18:12:24	54305	
<input type="checkbox"/> Internet Explorer	Thomas Cook - J...	http://bigmail-ile...	C:\Users\Wson...	2011-05-21 18:27:44	28371246	
<input type="checkbox"/> Internet Explorer	Urban Zakapa - 0...	http://bigmail-ile...	C:\Users\Wson...	2011-05-21 18:44:37	51966946	
<input type="checkbox"/> Internet Explorer	CISCO-RHINO-M...	ftp://ftp.disco...	C:\Users\Wson...	2011-05-21 19:05:27	65860	
<input type="checkbox"/> Internet Explorer	BRIDGE-MIB.my	ftp://ftp.disco...	C:\Users\Wson...	2011-05-21 21:10:09	47013	
<input type="checkbox"/> Internet Explorer	3Com-alert	http://www.mbs...	C:\Users\Wson...	2011-05-21 22:03:38	0	
<input type="checkbox"/> Internet Explorer	ubuntu-11.04-de...	http://mirror.khu...	E:\WOS\Linux\W...	2011-05-23 00:04:12	718583808	
<input type="checkbox"/> Internet Explorer	110520 사실확...	https://mail.goog...	C:\Users\Wson...	2011-05-23 12:28:13	34304	
<input type="checkbox"/> Internet Explorer	libeay32.dll	http://files.nav...	E:\WCIST\W00.Pr...	2011-05-25 01:54:03	900978	

Internet Explorer 로그 분석

- Index.dat 로그 파일 분석
- Cache 정보 분석
- History 정보 분석
- Cookie 정보 분석
- Download List 정보 분석
- **분석 도구**



분석 도구

- WEFA(Web Browser Forensic Analyzer)
- Encase
- Index.dat Analyzer
- Index.dat Viewer
- Nirsoft
 - IECacheView
 - IEHistoryView
 - IECookieView



분석 도구

WEFA(Web Browser Forensic Analyzer)

- Freeware Download → http://www.4n6tech.com/skin_kr/images/WEFA_v1.2_-_Freeware.zip

The screenshot displays the WEFA v1.3 application window. The main pane shows a list of Internet Explorer history entries with columns for browser name, status, inspection status, download URL, URL, visit time, title, visit count, and type. The entry for 'http://cc.naver.c...' is selected.

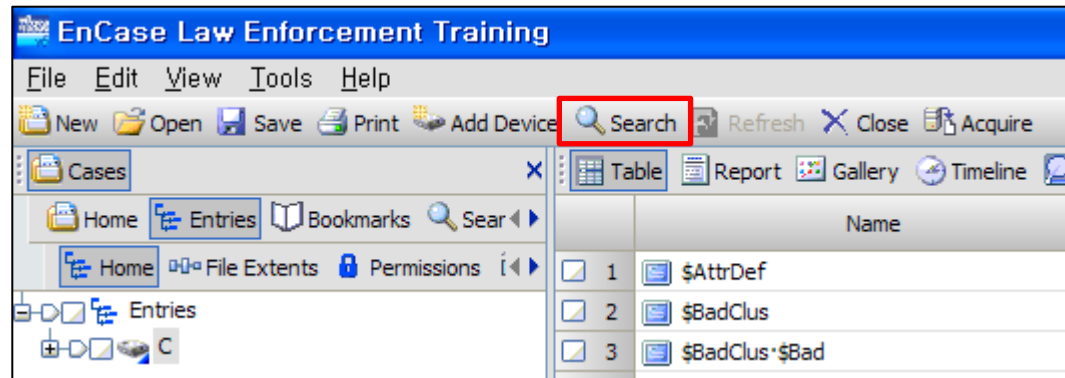
브라우저	상태	검사정보	다운로드 URL	URL	방문시간	제목	방문횟수	타입
Internet Explorer				http://www.segy...	2012-02-26 21:09:41		3	
Internet Explorer				http://www.myd...	2012-02-26 21:04:42		3	
Internet Explorer				http://www.goog...	2012-03-14 00:07:42	Google	1254	
Internet Explorer				http://www.myd...	2012-02-26 21:04:42	NO.1 뉴미디어 ...	6	
Internet Explorer				http://www.wed...	2012-02-25 02:53:50	위디스크	12	
Internet Explorer				http://www.wed...	2012-02-02 00:30:10	위디스크	2	
Internet Explorer				http://www.wed...	2012-02-02 00:00:39	컨텐츠와 합...	5	
Internet Explorer				http://www.wed...	2012-02-25 14:16:38	위디스크	10	
Internet Explorer				http://www.wed...	2012-02-02 00:28:44	컨텐츠와 합...	5	
Internet Explorer				https://xo.nate.c...	2012-02-13 21:28:21		21	
Internet Explorer				http://www.wed...	2012-02-23 00:13:29		1	
Internet Explorer				http://joongang.j...	2012-02-26 21:04:04		1	
Internet Explorer	다운로드			http://download...	2012-03-11 00:06:19		2	
Internet Explorer				http://splus.joins...	2012-02-20 09:26:36		1	
Internet Explorer				http://cc.naver.c...	2012-02-26 21:49:09		1	
Internet Explorer				http://splus.joins...	2012-02-20 09:26:40	[단독] 이해원 "...	7	
Internet Explorer				http://cc.naver.c...	2012-02-20 09:28:00		1	
Internet Explorer				http://www.yebi...	2012-03-02 18:29:19	<혼란연기> 혼...	5	
Internet Explorer				http://cc.naver.c...	2012-02-20 09:28:04		1	
Internet Explorer	엔터테인먼트			http://movie.sor...	2012-01-31 22:21:02		7	
Internet Explorer				http://www.wed...	2012-01-30 00:10:44		397	
Internet Explorer				http://joongang.j...	2012-02-26 21:04:04	단서? 미종설 그...	1	
Internet Explorer				http://cc.naver.c...	2012-02-26 21:49:17		1	
Internet Explorer	커뮤니티			http://www.fomo...	2012-03-17 23:14:53	포모스::포모스	718	
Internet Explorer				https://hid.naver...	2012-03-15 14:44:05	로그인 :: 네이비	96	
Internet Explorer	뉴스			http://www.danb...	2012-02-20 10:40:11	단배뉴스 - 견제...	1	
Internet Explorer				http://www.wed...	2012-03-13 00:28:28	컨텐츠와 합...	5	
Internet Explorer	엔터테인먼트			http://bbs.music...	2012-02-24 00:45:32		1	
Internet Explorer				http://cafe966.d...	2012-02-20 10:09:21	독행카뎀 화장...	5	
Internet Explorer				http://www.dau...	2012-02-20 10:33:00	Daum - 생활이 ...	19	
Internet Explorer				http://cartoon.m...	2012-02-20 10:36:01		9	
Internet Explorer				http://www.wed...	2012-03-17 23:17:18		518	
Internet Explorer				http://web1.zfile...	2012-03-17 01:11:29		3	
Internet Explorer				http://www.wed...	2012-03-17 23:17:18		454	
Internet Explorer				http://adn.adneo...	2012-03-12 00:28:20		218	
Internet Explorer				http://www.wed...	2012-02-21 22:53:26	위디스크	1	
Internet Explorer				http://cc.naver.c...	2012-02-26 21:07:55		1	
Internet Explorer				http://www.wed...	2012-02-21 22:52:25	컨텐츠와 합...	10	
Internet Explorer				http://www.wed...	2012-02-21 22:53:33	컨텐츠와 합...	5	
Internet Explorer				http://www.wed...	2012-02-21 23:26:17	컨텐츠와 합...	5	
Internet Explorer				http://cc.naver.c...	2012-02-26 21:08:01		1	
Internet Explorer				http://www.segy...	2012-02-26 21:08:12	우리는 이해 못...	4	
Internet Explorer				http://adn.adneo...	2012-03-12 00:28:20		218	
Internet Explorer				http://content...	2012-03-12 16:14:19		1	

The right pane shows the details for the selected entry, including the URL 'http://cc.naver.c...' and the title '[단독] 이해원 "...'. The bottom pane shows the HTML content, which includes a list of variables and their values, such as 'a: vcr.image', 'r: 78024ED1_00000007CE24', 'nsc: navetop.v3', 'w: 1899', 'px: 595', 'py: 845', 'sx: 595', 'sy: 712', 'm: 1', and 'u: http://comic.naver.com/webtoon/weekdayList.nhn?week'.



분석 도구

- Encase v6.18 : 웹 브라우저 사용 정보 탐색 Step 1.

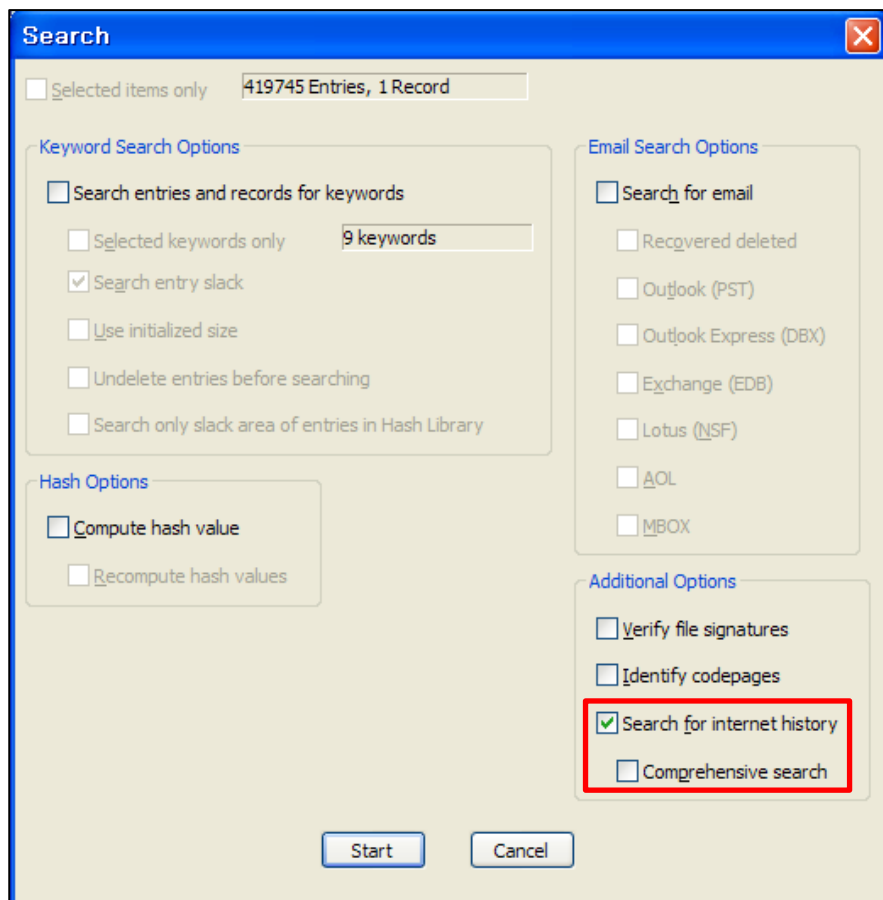




분석 도구

▪ Encase v6.18 : 웹 브라우저 사용 정보 탐색 Step 2.

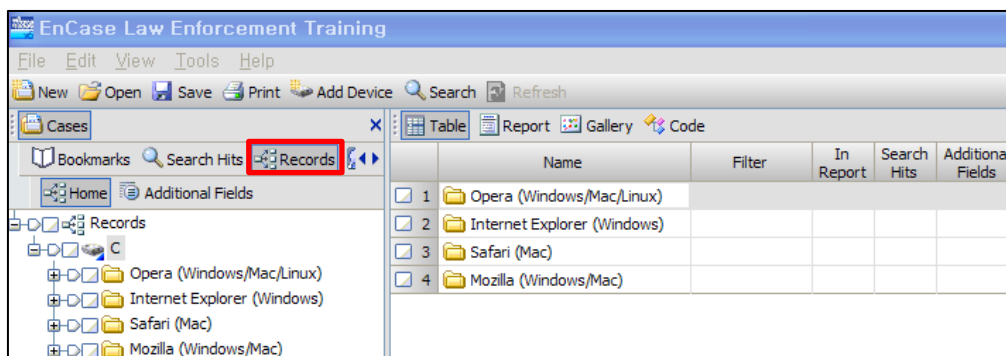
- Search Window에서 옵션 선택
 - ✓ 다른 모든 옵션 해제
 - ✓ Search for internet history 옵션 체크
 - Comprehensive search
 - ➔ 비 할당 영역도 체크, 장시간 소요





분석 도구

- **Encase v6.18 : 웹 브라우저 사용 정보 탐색 Step 3.**
 - 탐색 결과 : Records 에서 확인
 - ✓ Opera : Cache, Download List, Bookmark
 - ✓ Internet Explorer : Cache, History, Cookie, Bookmark
 - ✓ Safari : Cookie, Download List, Bookmark (Download List 의 경우, 거의 동작 안함)
 - ✓ Mozilla(Firefox) : Cache

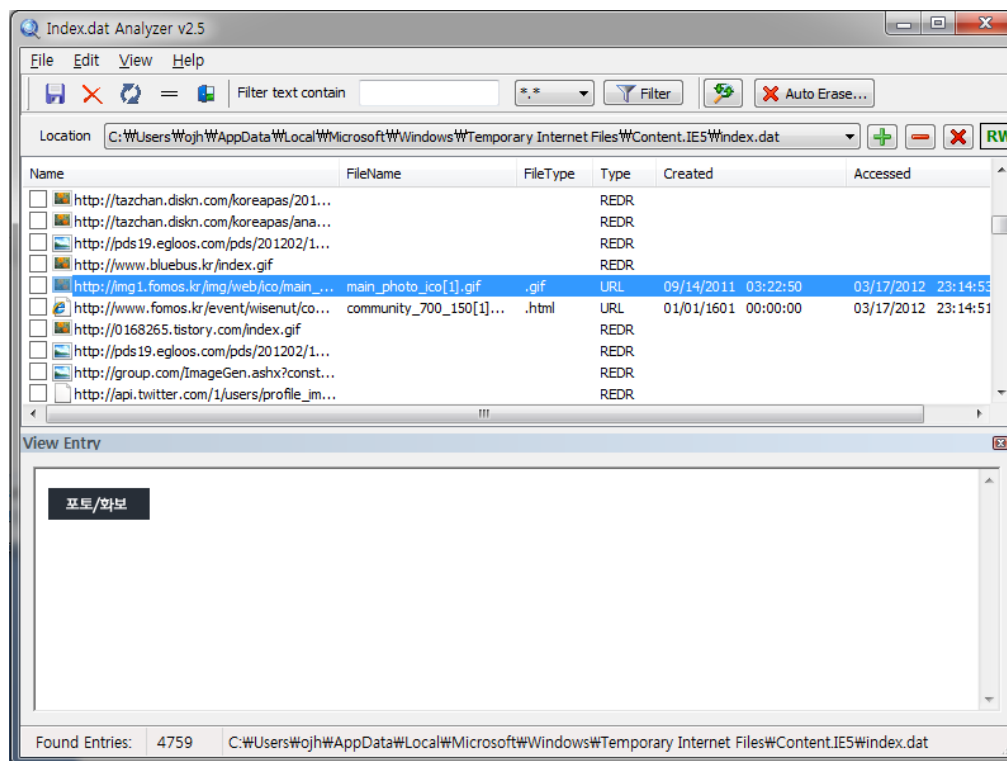




분석 도구

▪ Index.dat Analyzer

- <http://www.systemance.com/download/indexdat-setup.exe>

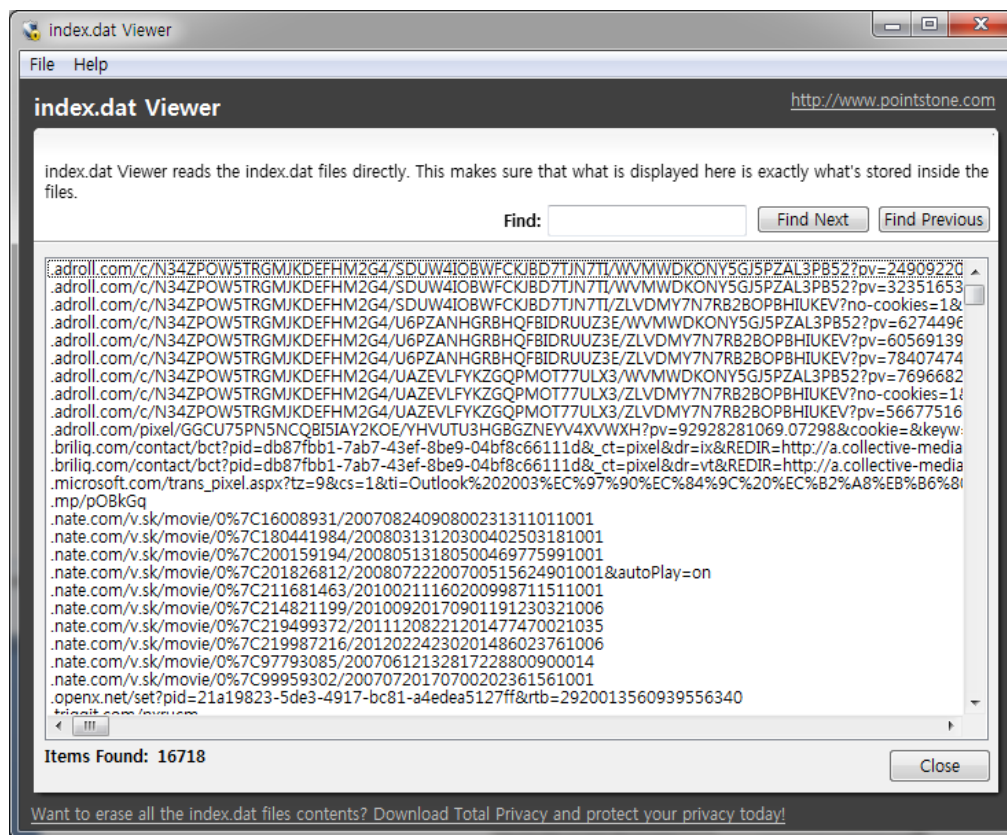




분석 도구

■ Index.dat Viewer

- <http://dl1.pointstone.com/download/freeware/index.dat-Viewer/indexdatViewer.zip>





분석 도구

■ Nirsoft : Browser Tools

- http://www.nirsoft.net/web_browser_tools.html

