

웹 아티팩트 포렌식



JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

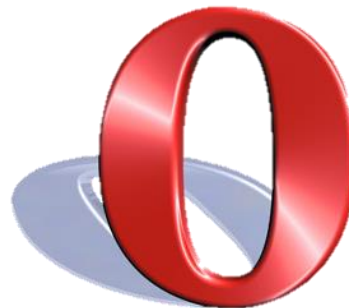
1. 웹 아티팩트 소개
2. 웹 아티팩트 수집
3. 웹 아티팩트 분석

웹 아티팩트 소개

웹 아티팩트 소개

웹 아티팩트란?

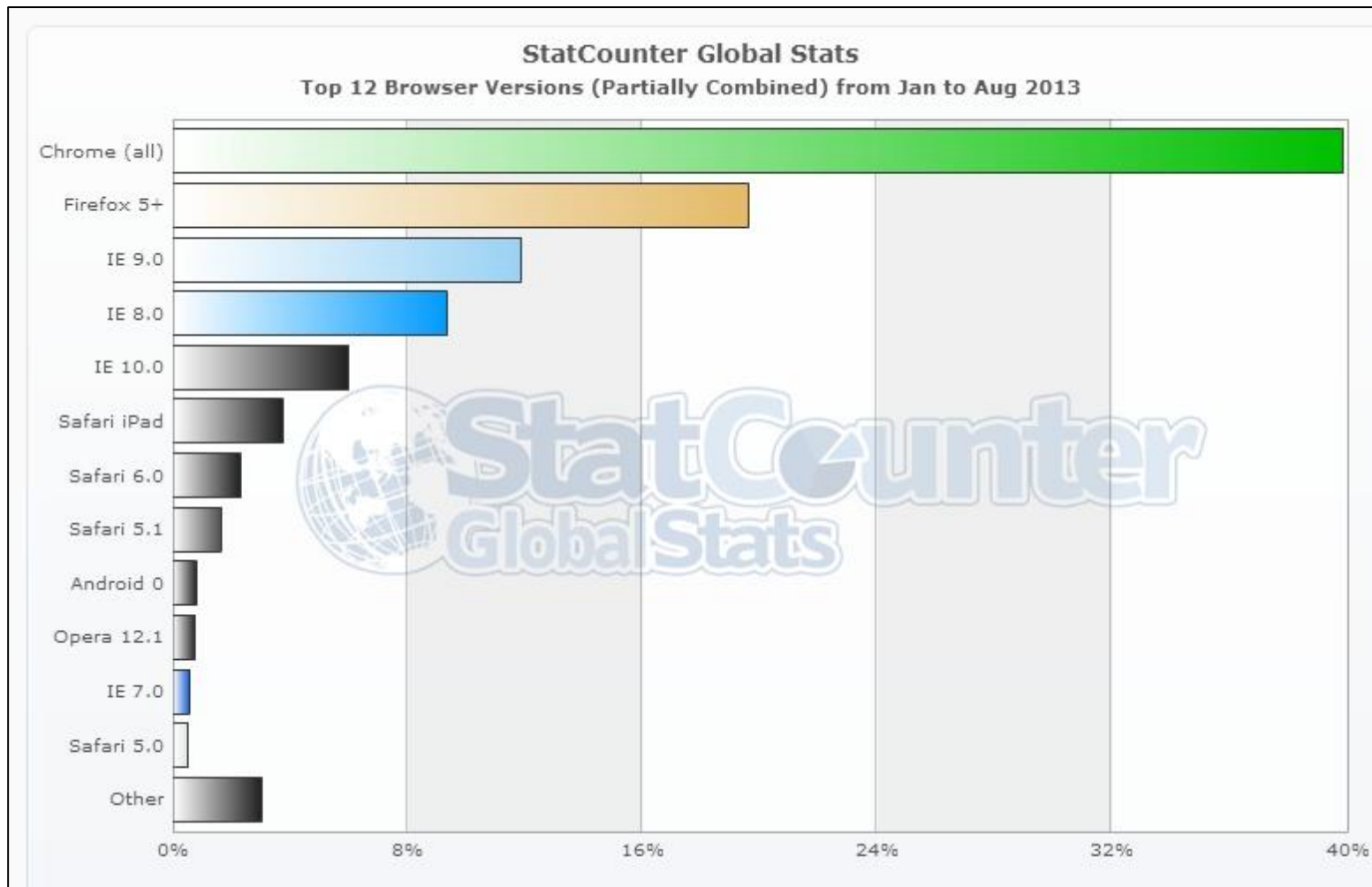
- 웹 서버와 쌍방향 통신을 하면서 생성되는 흔적
- 대부분의 웹 아티팩트는 웹 브라우저 로그



웹 아티팩트 소개

웹 브라우저 점유율

- StatCounter, 2013년 1월 ~ 8월까지 통계



웹 아티팩트 소개

웹 아티팩트 포렌식

▪ 정의

- 웹 브라우저 사용 흔적을 디지털 포렌식 분석에 활용하는 방법

▪ 필요성

- 현대인의 생활에서 웹 브라우저는 뗄래야 뗄 수 없는 필수 아이템 ➔ PC, 스마트폰 등
- 웹과 관련된 사건이라면 웹 브라우저 흔적이 분석에 매우 중요
- 사안에 따라 사건의 **동기, 목적, 수단, 방법, 사후 처리** 등 많은 정보 획득 가능

▪ 직접 증거보다는 정황증거로 활용

- “사실의 인정은 증거에 의한다” – 증거재판주의
- 직접 증거 – 증명의 대상이 되는 사실의 증명에 직접 이용되는 증거
- 정황 또는 간접 증거 – 간접 사실을 증명하는 증거

웹 아티팩트 소개

웹 아티팩트 종류

■ 웹 브라우저 캐시

- 웹 사이트 방문 시, 사이트로부터 자동으로 다운받은 콘텐츠
- 콘텐츠 캐시를 통해 재 방문 시 로딩 속도 향상

• 캐시 데이터

✓ 다운받은 데이터 : 이미지 파일, 텍스트 파일, 아이콘, HTML 파일, XML 파일, 스크립트 등

• 캐시 인덱스 정보

✓ 캐시 데이터 위치, 다운로드 URL, 다운로드 시간, 다운로드 데이터 크기 등

이름	인터넷 주소	유형	크기	만료 날짜	마지막으로 액세스한 날짜	마지막으로 수정한 날짜
 loading-large_V192238965_gif	http://g-ecx.images-amazon.com/ima...	GIF 이미지	7KB	2033-03-03 오후 12:06	2013-07-19 오후 7:08	2010-06-03 오전 10:06
 sprite-site-wide-3_V375430972_png	http://g-ecx.images-amazon.com/ima...	PNG 이미지	17KB	2033-03-04 오전 4:57	2013-07-19 오후 5:10	2013-02-07 오전 6:25
 517akZvN1QL_SL500_PIsitb-sticker-arrow-...	http://ecx.images-amazon.com/image...	JPEG 이미지	5KB	2033-03-04 오전 5:28	2013-07-19 오후 5:10	2013-01-19 오전 5:29
 sprite-cbox_V388671922_png	http://g-ecx.images-amazon.com/ima...	PNG 이미지	3KB	2033-03-04 오전 6:25	2013-07-19 오후 5:10	2012-09-19 오전 8:01
 viewcartcheckoutmedium_V195191215_gif	http://g-ecx.images-amazon.com/ima...	GIF 이미지	3KB	2033-03-04 오전 11:20	2013-07-19 오후 5:10	2010-11-03 오전 12:58
 nav-pop-v-v2_V137157005_png	http://g-ecx.images-amazon.com/ima...	PNG 이미지	2KB	2033-03-04 오후 7:27	2013-07-19 오후 7:08	2012-03-13 오전 8:57
 61b-kle1AsL_SL135_png	http://ecx.images-amazon.com/image...	JPEG 이미지	9KB	2033-03-04 오후 11:01	2013-07-19 오후 7:08	2012-07-25 오후 1:47
 navAmazonLogoFooter_V169459313_gif	http://g-ecx.images-amazon.com/ima...	GIF 이미지	2KB	2033-03-05 오전 1:03	2013-07-19 오후 7:08	2011-03-01 오전 3:36
 amznlike_sprite_02_V196113939_gif	http://g-ecx.images-amazon.com/ima...	GIF 이미지	3KB	2033-03-05 오전 1:49	2013-07-19 오후 5:10	2010-10-23 오전 8:53
 51-9l4%2BsIVL_SL500_PIsitb-sticker-arrow-...	http://ecx.images-amazon.com/image...	JPEG 이미지	5KB	2033-03-05 오전 8:56	2013-07-19 오후 5:10	2012-08-11 오후 9:03
 41AcZPYZ68L_SL135_jpg	http://ecx.images-amazon.com/image...	JPEG 이미지	4KB	2033-03-07 오전 2:43	2013-07-19 오후 7:08	2013-03-08 오후 11:13

웹 아티팩트 소개

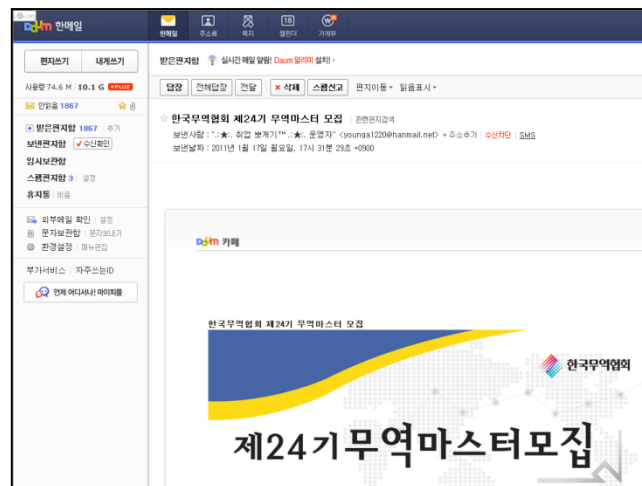
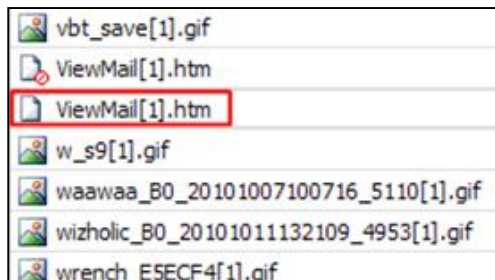
웹 아티팩트 종류

■ 웹 브라우저 캐시 분석 방법

- 다운로드 URL + 다운로드 시간 → 특정 시간에 해당 사이트 이력
- 다운로드 URL + 키워드 검색 → 중요 사이트 방문 이력 확인

 mail_view_write.js?t=20130626104800 http://mail3.nate.com/js/mail_view_write.js?t=20130626104800

- HTML 캐시 파일 - 웹 메일 내용 확인



웹 아티팩트 소개

웹 아티팩트 종류

■ 웹 브라우저 캐시 분석 방법

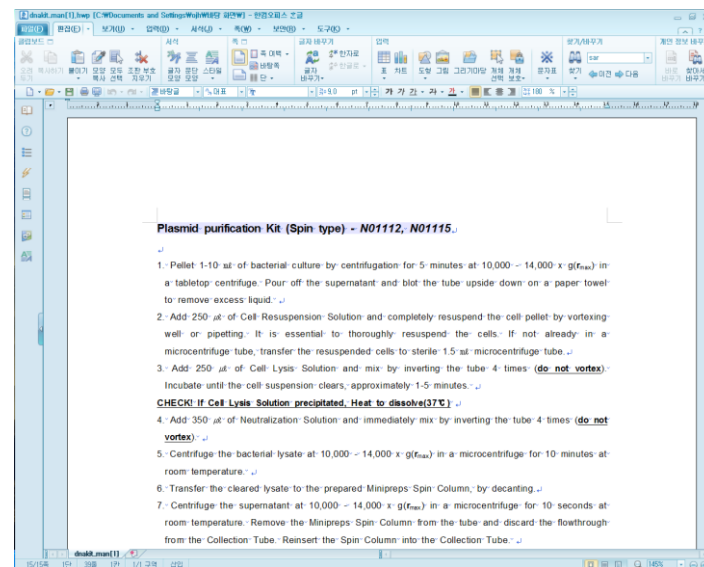
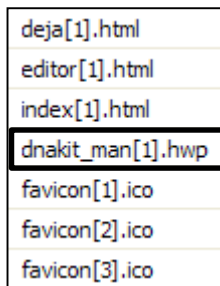
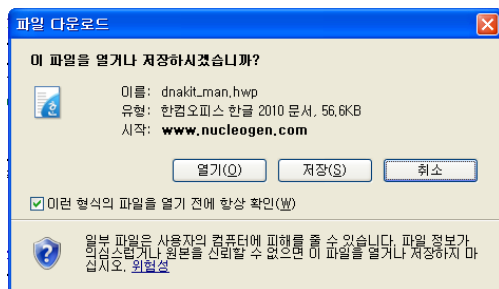
- 웹 브라우저에서 문서 열람 시 열람 파일 그대로 저장 – PDF, HWP 등

[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

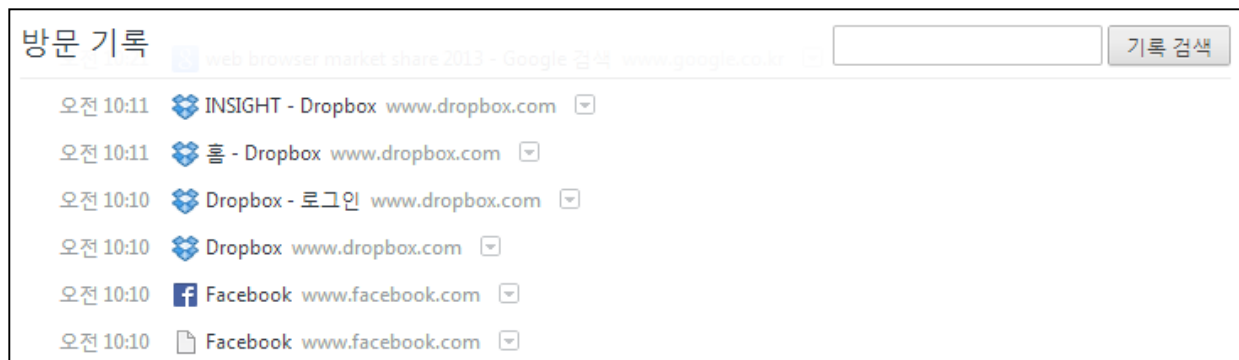
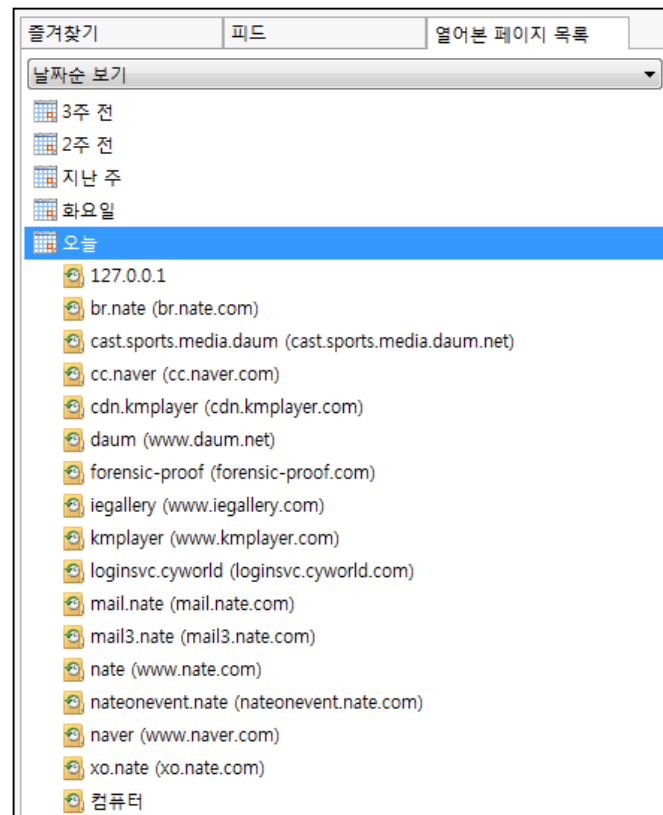


웹 아티팩트 소개

웹 아티팩트 종류

■ 웹 브라우저 히스토리

- 사용자가 방문한 웹 사이트 접속 정보 저장
- 월별, 일별 방문 기록을 분류해서 저장
- 히스토리 정보
 - ✓ 방문 사이트 URL, 방문 시간, 방문 횟수, 사이트 제목 등
- 저장 형식
 - ✓ 직접 접근 – URL 입력창에 직접 주소 입력
 - ✓ 간접 접근 – URL 링크를 통해서 접근



웹 아티팩트 소개

웹 아티팩트 종류

▪ 웹 브라우저 히스토리 분석 방법







- 방문 사이트 URL + 방문 시간 ➔ 해당 사이트 방문 이력
- 방문 사이트 URL + 방문 횟수 + 키워드 검색 ➔ 사용자 행위 분석
- 방문 URL 중 GET 방식으로 전달된 인자값 분석
 - ✓ 검색어 추출 `https://www.google.co.kr/search?q=forensic-proof`
 - ✓ 아이디, 패스워드 추출

웹 아티팩트 소개

웹 아티팩트 종류

■ 웹 브라우저 쿠키

- 웹 사이트 방문 시 자동으로 사용자 저장장치에 저장되는 텍스트 데이터
- 사용자 기반 서비스 제공
 - ✓ 자동 로그인 기능
 - ✓ 쇼핑몰 열람한 물건, 장바구니 물건
 - ✓ 웹 하드 찜 해놓은 자료, 다운받은 자료
- 쿠키 정보
 - ✓ 호스트 사이트, 경로, 수정 시간, 만료 시간, 이름, 값 등

이름	인터넷 주소	유형	크기	만료 날짜
 cookie:forensic32@plus.google.com/	Cookie:forensic32@plus.google.com/	텍스트 문서	1KB	2013-07-14 오후 2:23
 cookie:forensic32@pubmatic.com/	Cookie:forensic32@pubmatic.com/	텍스트 문서	1KB	2015-07-19 오후 5:10
 cookie:forensic32@q828.tistory.com/	Cookie:forensic32@q828.tistory.com/	텍스트 문서	1KB	2015-03-20 오후 7:58
 cookie:forensic32@realmedia.co.kr/	Cookie:forensic32@realmedia.co.kr/	텍스트 문서	1KB	2021-01-01 오전 9:00
 cookie:forensic32@rubiconproject.com/	Cookie:forensic32@rubiconproject.com/	텍스트 문서	1KB	2021-07-17 오후 5:10
 cookie:forensic32@sanddroid.xjtu.edu....	Cookie:forensic32@sanddroid.xjtu.edu.cn/	텍스트 문서	1KB	2015-07-04 오후 5:27

웹 아티팩트 소개

웹 아티팩트 종류

▪ 웹 브라우저 쿠키 분석 방법

- 호스트 ➔ 접속한 사이트
- 경로 ➔ 사용한 서비스
- 수정 시간 ➔ 마지막 접속 시간
- 이름, 값
 - ✓ 로그인 아이디 저장 옵션 활성화 시 ➔ 로그인 아이디 획득 가능
 - ✓ 구글 애널리틱스 정보

웹 아티팩트 소개

웹 아티팩트 종류

■ 다운로드 목록

- 사용자가 선택하여 시스템으로 내려 받은 파일 정보 ➔ 사용자 편의를 위해 저장
- 사용자 의도와 관련 없이 다운로드되는 캐시 데이터와는 구분

• 다운로드 목록 정보

✓ 다운로드 파일 저장 경로, 소스 URL, 파일 크기, 다운로드 시간, 다운로드 성공 여부

다운로드			
오늘 2013. 8. 14.		불후의 명곡 - 전설을 노래하다.E112.여름가요의 절대강자%21 클 특집.130803.HDTV.H264.720p-HANrel.avi.torrent http://www.torrentby.com/bbs/download.php?bo_table=torrent_variety&wr_id=32961&no=1 폴더 열기 목록에서 삭제	
2013. 8. 10.		BETA_ANJP_CLI_AUGUST (1).exe 삭제됨 https://doc-08-5s-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5... 목록에서 삭제	
		BETA_ANJP_CLI_AUGUST.exe 삭제됨 https://doc-08-5s-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5... 목록에서 삭제	
		adroit pf 31d install dm.exe http://digital-assembly.com/products/adroit-photo-forensics/downloads/get_apf/26b16614... 폴더 열기 목록에서 삭제	
2013. 8. 9.		id32.v.0.58.win.zip https://tzworks.net/prototypes/index_dat/id32.v.0.58.win.zip 폴더 열기 목록에서 삭제	

웹 아티팩트 소개

웹 아티팩트 종류

▪ 다운로드 목록 분석 방법

- 다운로드 URL → 접속 사이트
- 다운로드 시간 → 해당 파일의 다운로드 시간
- 다운로드 파일의 경로 → 파일 내용 확인
 - ✓ 다운로드 받은 파일이 없을 경우, 저장된 URL로 재다운

웹 아티팩트 수집

로그 파일 저장 경로

▪ 사용자 프로필 경로

- 사용자마다 웹 아티팩트를 구분하여 관리
- 윈도우 2K/XP
 - ✓ %SystemDrive%\Documents and Settings\<username%\
- 윈도우 Vista/7/8
 - ✓ %SystemDrive%\Users\<username%\
- 사용자 프로필 경로 환경 변수 – %UserProfile%

인터넷 익스플로러 (Internet Explorer)

■ 웹 아티팩트 경로

운영체제	구분	경로
Windows 2000, XP	Cache	%UserProfile%\Local Settings\Temporary Internet Files\Content.IE5\index.dat %UserProfile%\Local Settings\Temporary Internet Files\Content.IE5\<Random>\<All Files>
	History	%UserProfile%\Local Settings\History\History.IE5\index.dat %UserProfile%\Local Settings\History\History.IE5\<Period>\index.dat
	Cookie	%UserProfile%\Cookies\index.dat %UserProfile%\Cookies\<All Text Files>
	Download	-
Windows Vista, 7	Cache	%UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat %UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\<Random>\<All Files>
	History	%UserProfile%\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat %UserProfile%\AppData\Local\Microsoft\Windows\History\History.IE5\<Period>\index.dat
	Cookie	%UserProfile%\AppData\Roaming\Microsoft\Windows\Cookies\index.dat %UserProfile%\AppData\Roaming\Microsoft\Windows\Cookies\<All Text Files>
	Download	%UserProfile%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat (Since IE9)

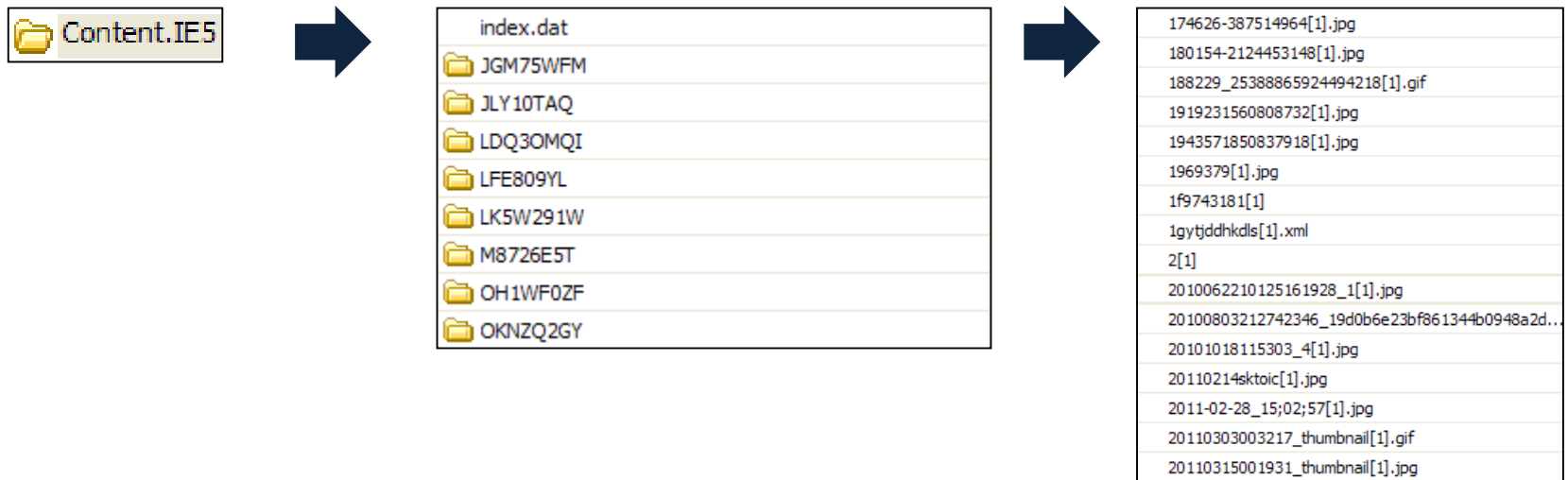
인터넷 익스플로러 (Internet Explorer)

■ 캐시 정보

- 다운로드된 캐시 데이터는 "임시 인터넷 파일" 폴더에 파일 형태로 저장
- 파일의 캐시 인덱스 정보는 동일 폴더의 "index.dat" 파일로 관리

• 수집 방법

- ✓ "[Low₩]Content.IE5" 폴더 하위의 모든 "index.dat" 파일 수집
- ✓ "[Low₩]Content.IE5" 폴더 하위의 모든 파일 수집 (수집 시간 고려)



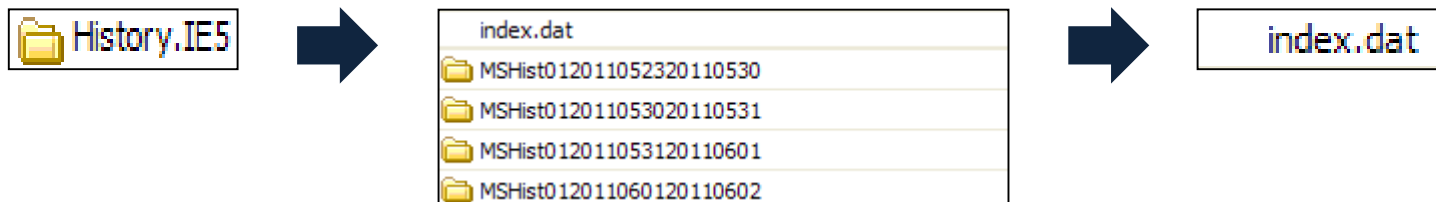
인터넷 익스플로러 (Internet Explorer)

■ 히스토리 정보

- 각 요일, 주, 월 별로 별도의 폴더로 관리
- 인덱스 정보는 "index.dat" 파일로 관리

• 수집 방법

- ✓ "[LowW]History.IE5" 폴더 하위의 모든 "index.dat" 파일 수집
- ✓ "[LowW]History.IE5" 폴더 하위의 모든 파일 수집



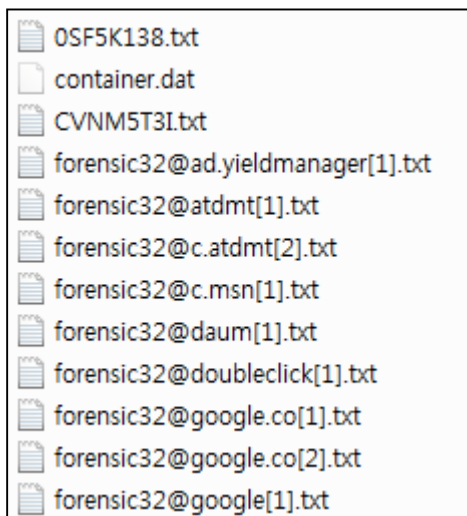
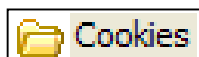
인터넷 익스플로러 (Internet Explorer)

■ 쿠키 정보

- 쿠키 폴더에 "계정명@호스트명.txt" 형식으로 저장
- 인덱스 정보는 "index.dat" 파일로 관리

• 수집 방법

- ✓ "Cookies" 폴더 하위의 모든 "index.dat" 파일 수집
- ✓ "Cookies" 폴더 하위의 모든 텍스트 파일 수집



인터넷 익스플로러 (Internet Explorer)

- 다운로드 목록 정보

- IE9 버전부터 존재
- 인덱스 정보는 "index.dat" 파일로 관리

- 수집 방법

- ✓ "IEDownloadHistory" 폴더 하위의 "index.dat" 파일 수집



웹 아티팩트 수집

크롬 (Chrome)

- 웹 아티팩트 경로

운영체제	구분	경로
Windows 2000, XP	Cache	%UserProfile%\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache\<All Files>
	History	%UserProfile%\Local Settings\Application Data\Google\Chrome\User Data\Default\History %UserProfile%\Local Settings\Application Data\Google\Chrome\User Data\Default\History Index<Year-Month>
	Cookie	%UserProfile%\Local Settings\Application Data\Google\Chrome\User Data\Default\Cookies
	Download	%UserProfile%\Local Settings\Application Data\Google\Chrome\User Data\Default\History
Windows Vista, 7	Cache	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Cache\
	History	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\History %UserProfile%\AppData\Local\Google\Chrome\User Data\Default\History\History Index<Year-Month>
	Cookie	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Cookies
	Download	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\History

크롬 (Chrome)

▪ 캐시 정보

- "data_0" 파일에 인덱스 정보를 저장
- "data_1", "data_2", "data_3"를 비롯해 나머지 파일에 캐시 데이터 저장

• 수집 방법

- ✓ "Cache" 폴더 하위의 모든 파일 수집



data_0
data_1
data_2
data_3
f_000001
f_000002
f_000003
f_000004
f_000005
f_000006

크롬 (Chrome)

▪ 히스토리, 쿠키, 다운로드 목록 정보

- SQLite 데이터베이스 파일로 저장됨

- ✓ 히스토리 : History

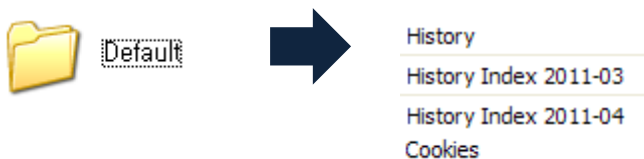
- 히스토리의 월별 정보는 "History Index <Year-Month>" SQLite 파일에 저장

- ✓ 쿠키 정보 : Cookies

- ✓ 다운로드 목록 정보 : History

- 수집 방법

- ✓ "Default" 폴더 하위의 "History", "History Index <Year-Month>", "Cookie" 파일 수집



파이어폭스 (Firefox)

■ 웹 아티팩트 경로

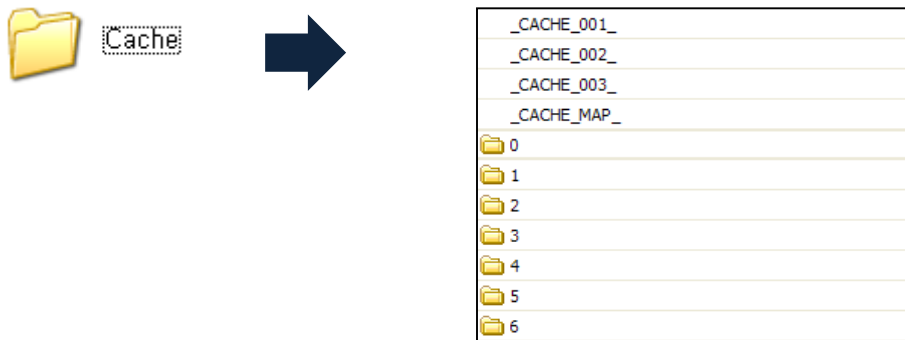
운영체제	구분	경로
Windows 2000, XP	Cache	%UserProfile%\Local Settings\Application Data\Mozilla\Firefox\Profiles\<Random>.default\Cache*. * %UserProfile%\Local Settings\Application Data\Mozilla\Firefox\Profiles\<Random>.default\Cache\<All Folder>
	History	%UserProfile%\Application Data\Mozilla\Firefox\Profiles\<Random>.default\places.sqlite
	Cookie	%UserProfile%\Application Data\Mozilla\Firefox\Profiles\<Random>.default\cookies.sqlite
	Download	%UserProfile%\Application Data\Mozilla\Firefox\Profiles\<Random>.default\downloads.sqlite
Windows Vista, 7	Cache	%UserProfile%\AppData\Local\Mozilla\Firefox\Profiles\<Random>\Cache*. *
	History	%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\places.sqlite
	Cookie	%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\cookies.sqlit
	Download	%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default\download.sqlite

- <Random> 정보는 히스토리 경로의 "Firefox" 폴더 아래, "Profiles.ini" 파일에서 확인

파이어폭스 (Firefox)

■ 캐시 정보

- 캐시 맵 파일, 분리된 캐시 데이터 파일, 캐시 블록 파일로 구성
- 캐시 맵 파일(_CACHE_[MAP, 001, 002, 003]_) 파일에 인덱스 정보 저장
- 수집 방법
 - ✓ "Cache" 폴더 하위의 "_CACHE_MAP_", "_CACHE_001_", "_CACHE_002_", "_CACHE_003_" 파일 수집
 - ✓ "Cache" 폴더 하위의 모든 폴더 수집



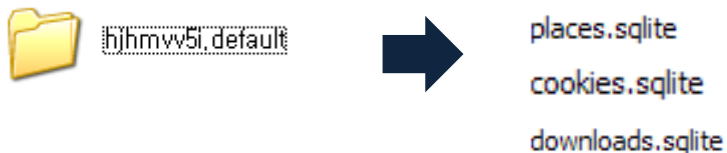
파이어폭스 (Firefox)

▪ 히스토리, 쿠키, 다운로드 목록 정보

- SQLite 데이터베이스 파일로 저장됨
 - ✓ 히스토리 정보 : places.sqlite
 - ✓ 쿠키 정보 : cookies.sqlite
 - ✓ 다운로드 목록 정보 : downloads.sqlite

• 수집 방법

- ✓ <Random>.default 폴더 하위의 SQLite 파일 수집



웹 아티팩트 수집

사파리 (Safari)

- 웹 아티팩트 경로

운영체제	구분	경로
Windows 2000, XP	Cache	%UserProfile%\Local Settings\Application Data\Apple Computer\Safari\Cache.db
	History	%UserProfile%\Application Data\Apple Computer\Safari\History.plist
	Cookie	%UserProfile%\Application Data\Apple Computer\Safari\Cookies\Cookies.plist
	Download	%UserProfile%\Application Data\Apple Computer\Safari\Downloads.plist
Windows Vista, 7	Cache	%UserProfile%\AppData\Local\Apple Computer\Safari\Cache.db
	History	%UserProfile%\AppData\Roaming\Apple Computer\Safari\History.plist
	Cookie	%UserProfile%\AppData\Roaming\Apple Computer\Safari\Cookies\Cookies.plist
	Download	%UserProfile%\AppData\Roaming\Apple Computer\Safari\Downloads.plist

사파리 (Safari)

▪ 캐시, 히스토리, 쿠키, 다운로드 목록 정보

- 캐시 인덱스 정보, 캐시 데이터 모두 SQLite 데이터베이스로 저장 → Cache.db
- 히스토리, 쿠키, 다운로드 목록은 각각 PLIST 형태로 저장
 - ✓ 히스토리 정보 : History.plist
 - ✓ 쿠키 정보 : Cookies.plist
 - ✓ 다운로드 목록 정보 : Downloads.plist
- 수집 방법
 - ✓ "Safari" 폴더 하위의 "Cache.db" 파일 수집
 - ✓ "Cookies" 폴더 하위의 "Cookies.plist" 파일 수집
 - ✓ "Safari" 폴더 하위의 "History.plist", "Downloads.plist" 파일 수집

웹 아티팩트 수집

오페라 (Opera)

- 웹 아티팩트 경로

운영체제	구분	경로
Windows 2000, XP	Cache	%UserProfile%\Local Settings\Application Data\Opera\Opera\cache\dcache4.url
	History	%UserProfile%\Application Data\Opera\Opera\global_history.dat
	Cookie	%UserProfile%\Application Data\Opera\Opera\cookies4.dat
	Download	%UserProfile%\Application Data\Opera\Opera\download.dat
Windows Vista, 7	Cache	%UserProfile%\AppData\Local\Opera\Opera\cache\dcache4.url
	History	%UserProfile%\AppData\Roaming\Opera\Opera\global_history.dat
	Cookie	%UserProfile%\AppData\Roaming\Opera\Opera\cookies4.dat
	Download	%UserProfile%\AppData\Roaming\Opera\Opera\download.dat

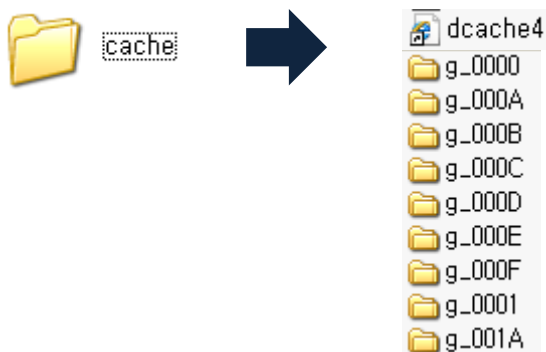
오페라 (Opera)

▪ 캐시 정보

- 캐시 인덱스 정보는 dcache4.url 파일에 저장됨
- 캐시 데이터 정보는 "cache" 폴더 하위의 서브 폴더에 저장됨

• 수집 방법

- ✓ "cache" 폴더 하위의 "dcache4.url" 파일 수집
- ✓ "cache" 폴더 하위의 모든 서브 폴더 수집



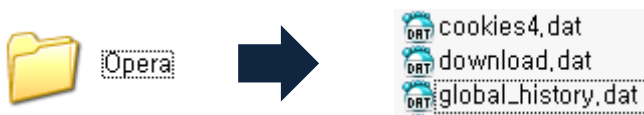
오페라 (Opera)

■ 히스토리, 쿠키, 다운로드 목록 정보

- 자체적인 포맷을 이용해 저장
 - ✓ 히스토리 정보 : global_history.dat
 - ✓ 쿠키 정보 : cookies4.dat
 - ✓ 다운로드 목록 정보 : download.dat

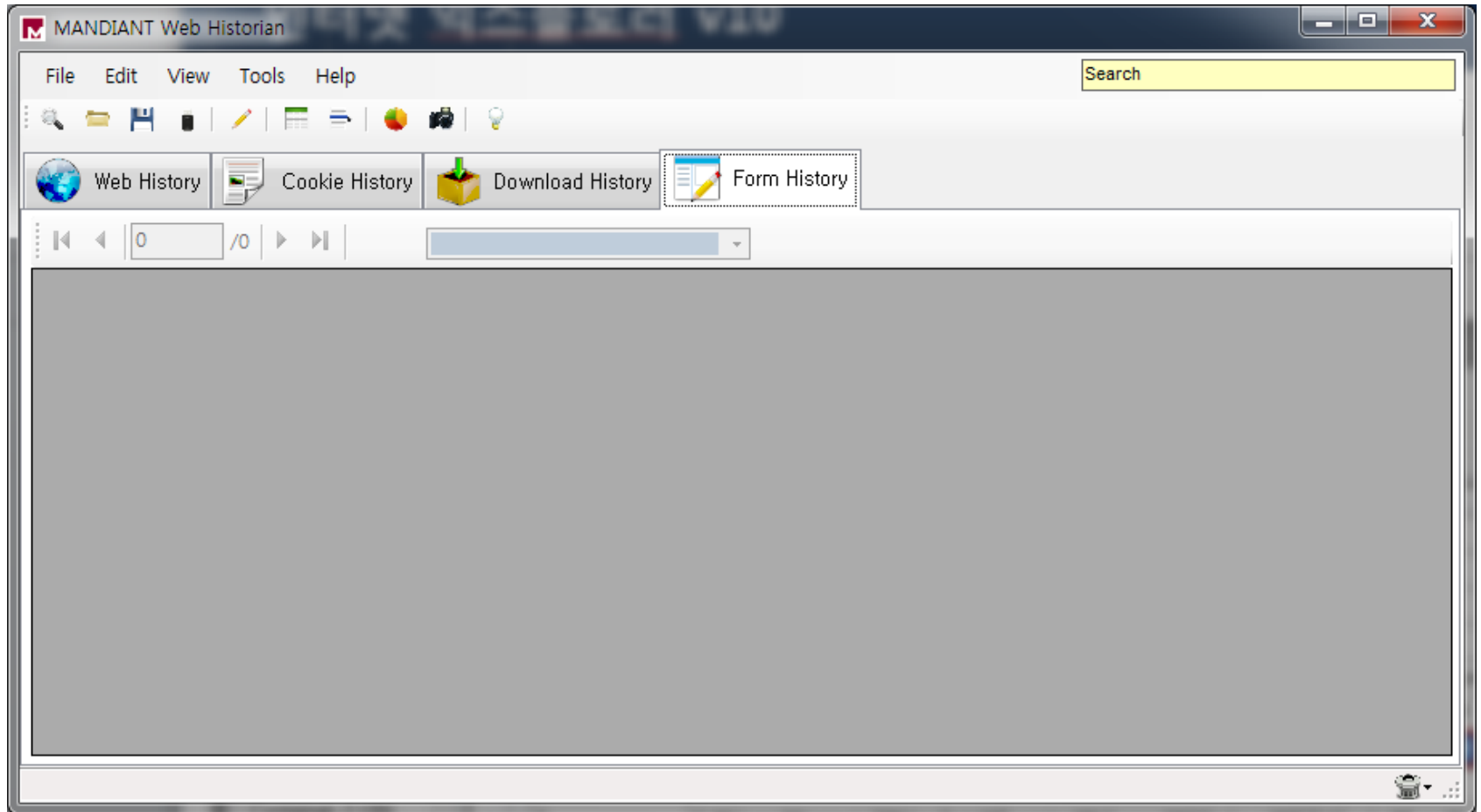
• 수집 방법

- ✓ "Opera" 폴더 하위의 각 파일 수집

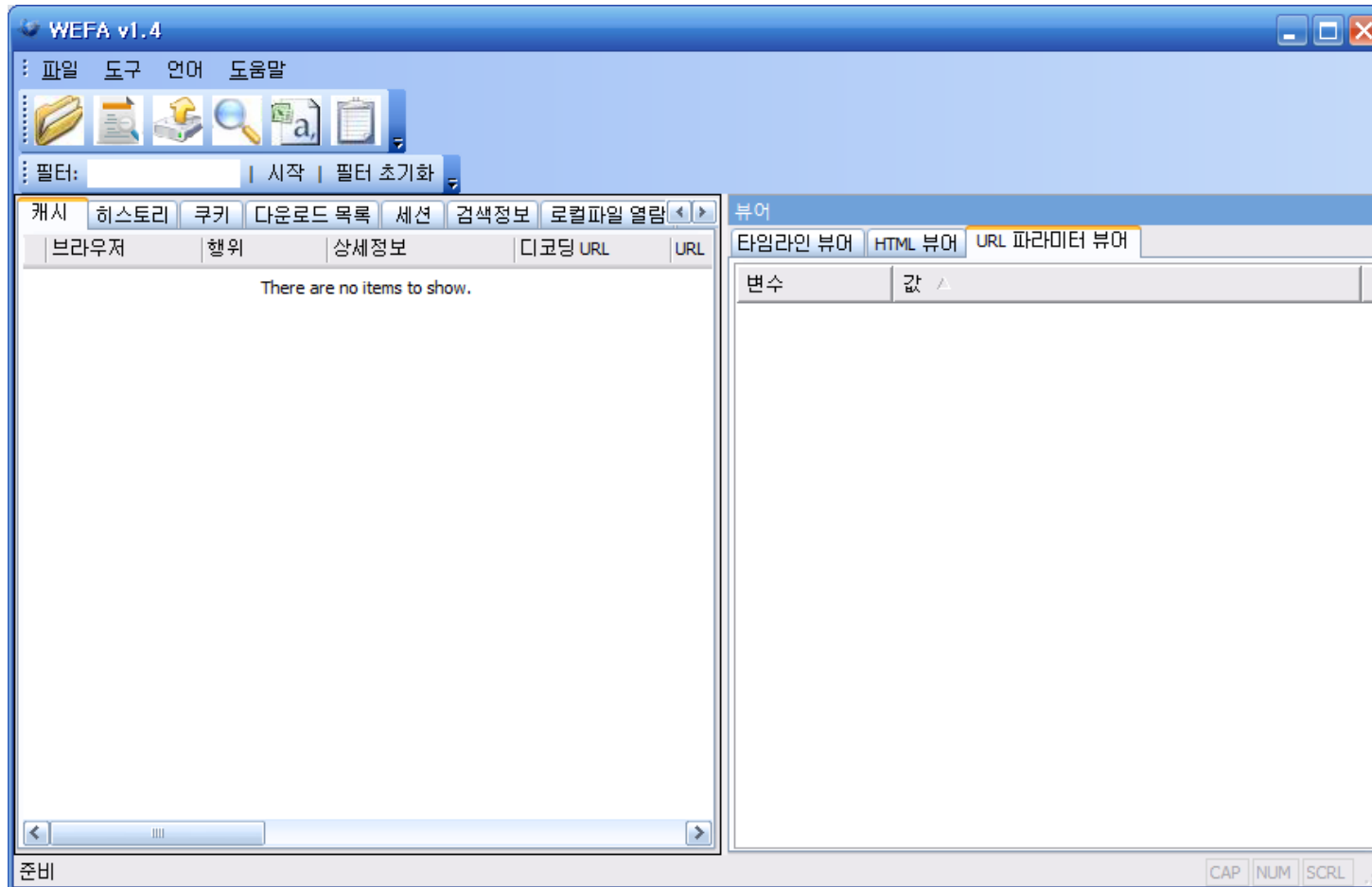


웹 아티팩트 분석

Web Historian



WEFA



실습 #1

- 로컬에서 수집한 모든 index.dat 분석하기

인터넷 익스플로러 v10

IE v10 웹 아티팩트

■ IE v10 소개

- 윈도우 8은 기본으로 IE v10을 사용
- 최근 윈도우 업데이트 수행 시 자동으로 IE v10으로 업데이트
- 캐시, 히스토리, 쿠키, 다운로드 목록 등의 웹 아티팩트를 하나의 파일로 관리함

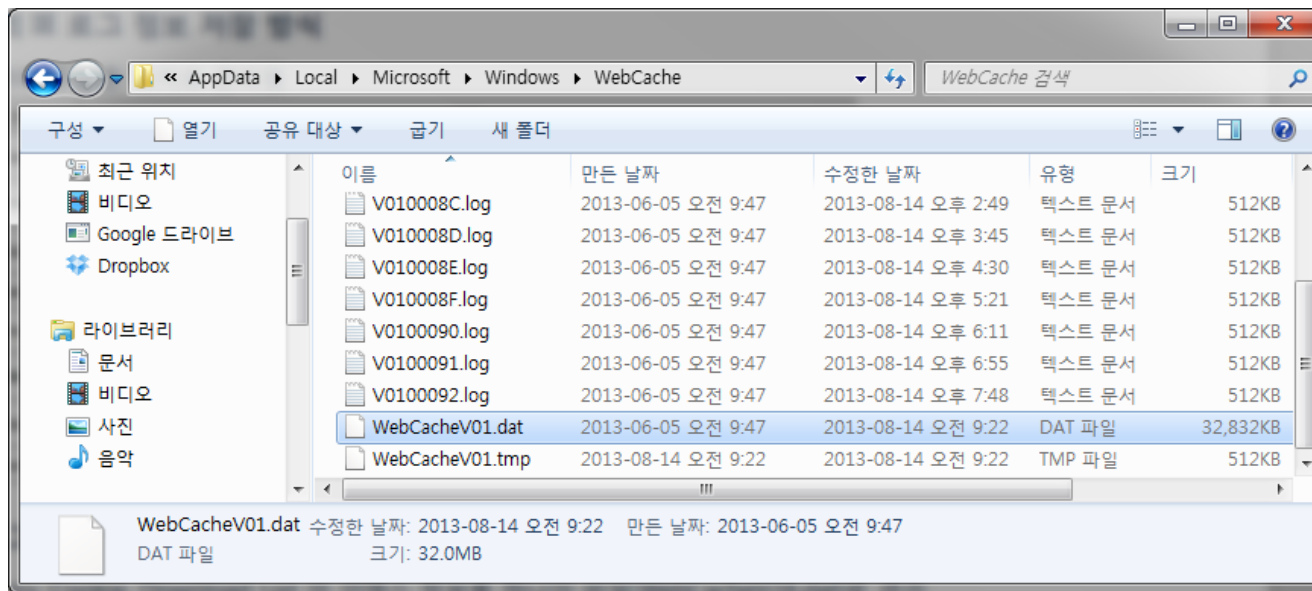


인터넷 익스플로러 v10

IE v10 웹 아티팩트

■ 웹 캐시 파일

- IE v10에서 웹 아티팩트가 통합되어 있는 파일
- 경로
 - ✓ %UserProfile%\AppData\Local\Microsoft\Windows\WebCache\
- 파일명
 - ✓ WebCacheV01.dat 또는 WebCacheV24.dat



IE v10 웹 아티팩트

▪ 웹 캐시 파일 포맷

• ESE(Extensible Storage Engine) 데이터베이스 포맷

- ✓ MS에서 개발한 ISAM(Indexed Sequential Access Method) 데이터 저장 기술
- ✓ JET Blue Storage Engine이라고도 부름 (JET Red : MS Access Database Engine)

✓ 사용 애플리케이션

- Active Directory (NTDS)
- Windows Internet Name Service (WINS)
- Certificate Server
- Catalog Database
- MS Exchange Folder (SRS, DXA)
- Instant Messaging
- Windows Mail
- Windows Search
-

IE v10 웹 아티팩트

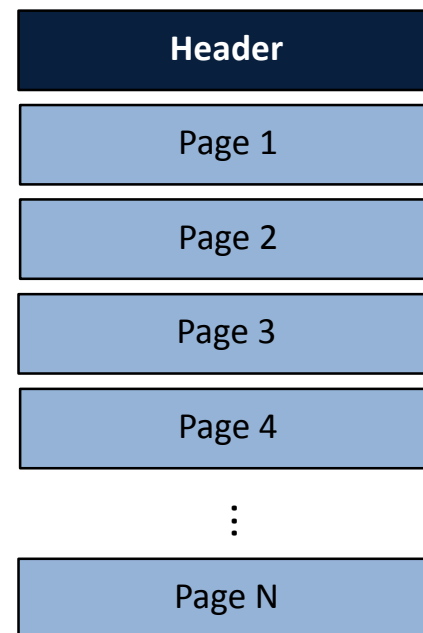
■ 웹 캐시 파일 기본 구조

• Header (최소 668 바이트)

- ✓ 시그니처 : /xEF/xCD/xAB/x89
- ✓ ESE 버전
- ✓ 페이지 크기

• Page

- ✓ 페이지 헤더는 40 또는 80바이트의 고정된 크기
- ✓ 각 응용프로그램마다 고정된 크기(2KB~32KB)의 페이지 사용
- ✓ 일정한 크기의 페이지 단위로 데이터 입출력



IE v10 웹 아티팩트

▪ 웹 캐시 파일 수집

- 라이브 상태에서 웹 캐시 파일은 TaskHost 프로세스가 열고 있음 → 일반 복사로 수집 불가
- 파일의 물리적인 위치를 알아내면 접근 가능
- 다만, 열려 있는 파일을 강제 수집할 경우 파일의 상태는 **"Dirty Shutdown"**
- 많은 ESE 데이터베이스 뷰어가 **"Dirty Shutdown"** 상태를 해석하지 못함
- ESE 유틸을 사용해 **"Dirty Shutdown"** → **"Clean Shutdown"** 상태로 변경한 후 분석
- 상태 변경 시 일부 데이터 손실됨

▪ **"Clean Shutdown"** 상태로 웹 캐시 파일 수집하기

- 윈도우를 정상 종료한 후 파일 수집

IE v10 웹 아티팩트

■ 웹 캐시 파일 상태 변경

- 라이브 상태에서 웹 캐시 파일 수집

```
C:\> forecopy -f %UserProfile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat .
```

- 웹 캐시 파일 상태 확인

```
C:\> esentutl /mh WebCacheV01.dat
```

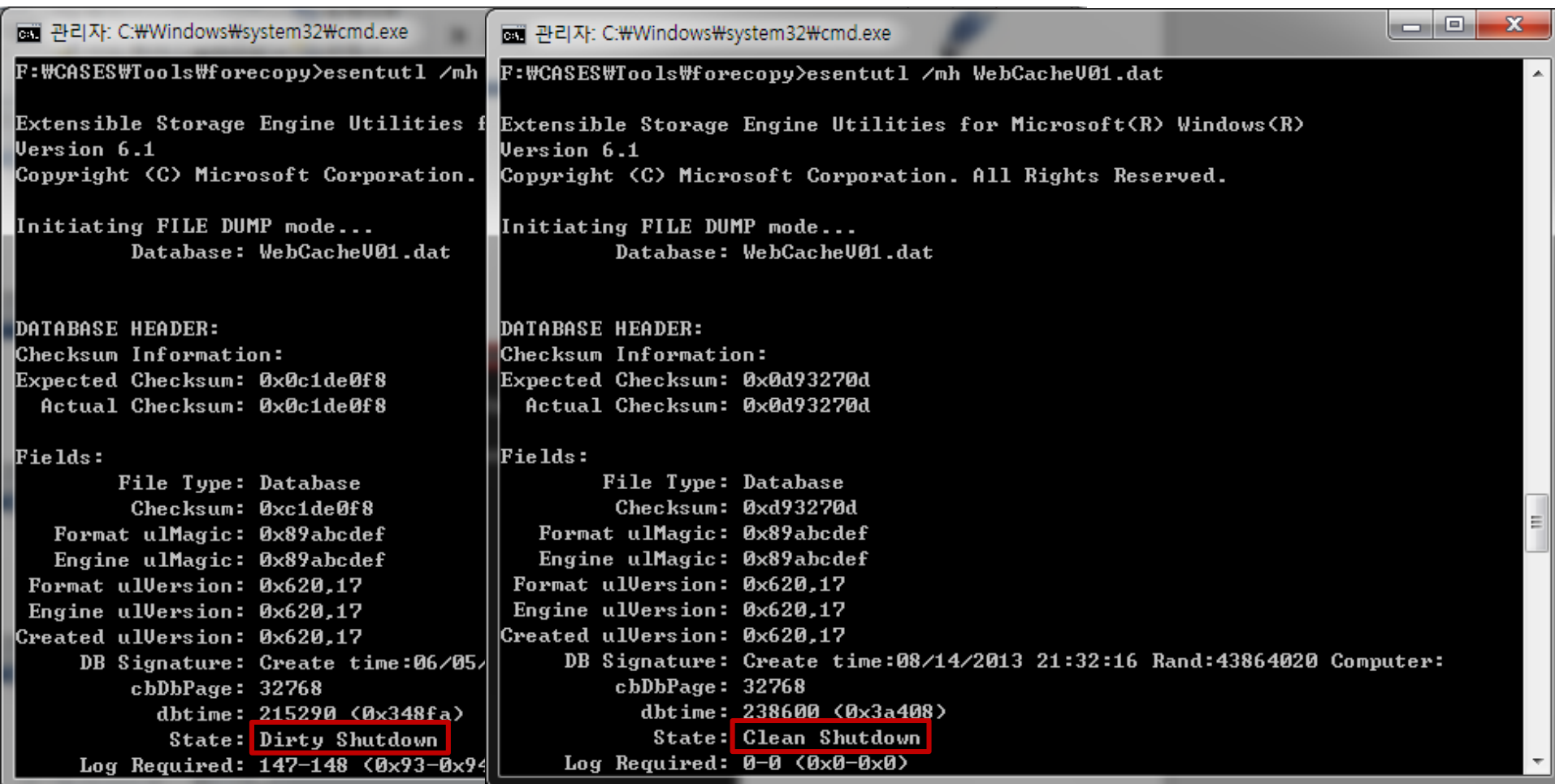
- 웹 캐시 파일 복구 (Repair)

```
C:\> esentutl /p WebCacheV01.dat
```

인터넷 익스플로러 v10

IE v10 웹 아티팩트

■ 웹 캐시 파일 상태 변경



```
관리자: C:\Windows\system32\cmd.exe
F:\WCASESWTools\forecopy>esentutl /mh
Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 6.1
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating FILE DUMP mode...
Database: WebCacheV01.dat

DATABASE HEADER:
Checksum Information:
Expected Checksum: 0x0c1de0f8
Actual Checksum: 0x0c1de0f8

Fields:
File Type: Database
Checksum: 0xc1de0f8
Format ulMagic: 0x89abcdef
Engine ulMagic: 0x89abcdef
Format ulVersion: 0x620,17
Engine ulVersion: 0x620,17
Created ulVersion: 0x620,17
DB Signature: Create time:06/05/
cbDbPage: 32768
dbtime: 215290 (0x348fa)
State: Dirty Shutdown
Log Required: 147-148 (0x93-0x94)

관리자: C:\Windows\system32\cmd.exe
F:\WCASESWTools\forecopy>esentutl /mh WebCacheV01.dat
Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 6.1
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating FILE DUMP mode...
Database: WebCacheV01.dat

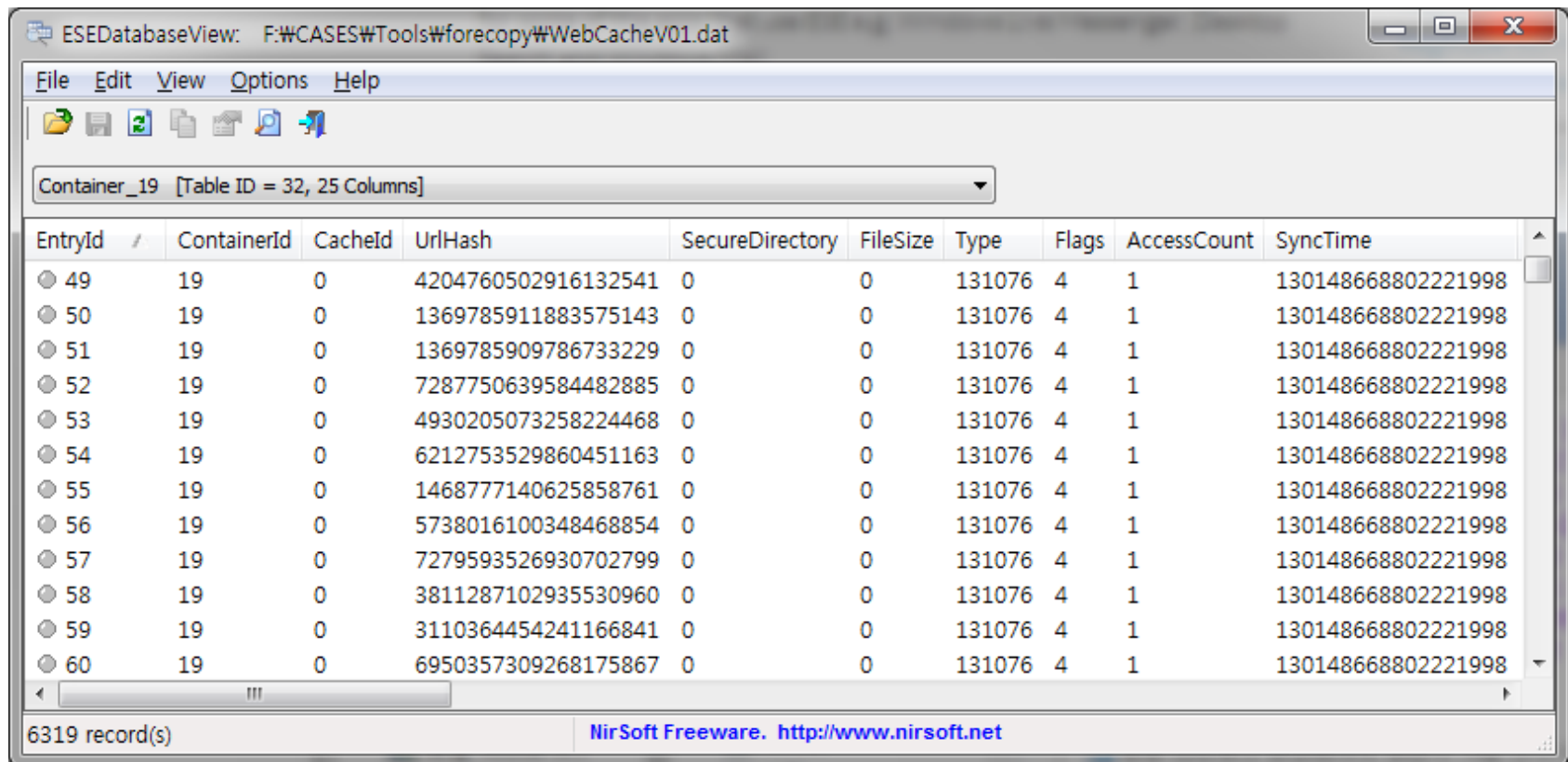
DATABASE HEADER:
Checksum Information:
Expected Checksum: 0x0d93270d
Actual Checksum: 0x0d93270d

Fields:
File Type: Database
Checksum: 0xd93270d
Format ulMagic: 0x89abcdef
Engine ulMagic: 0x89abcdef
Format ulVersion: 0x620,17
Engine ulVersion: 0x620,17
Created ulVersion: 0x620,17
DB Signature: Create time:08/14/2013 21:32:16 Rand:43864020 Computer:
cbDbPage: 32768
dbtime: 238600 (0x3a408)
State: Clean Shutdown
Log Required: 0-0 (0x0-0x0)
```

인터넷 익스플로러 v10

웹 캐시 파일 분석

- ESEDatabaseView – NirSoft

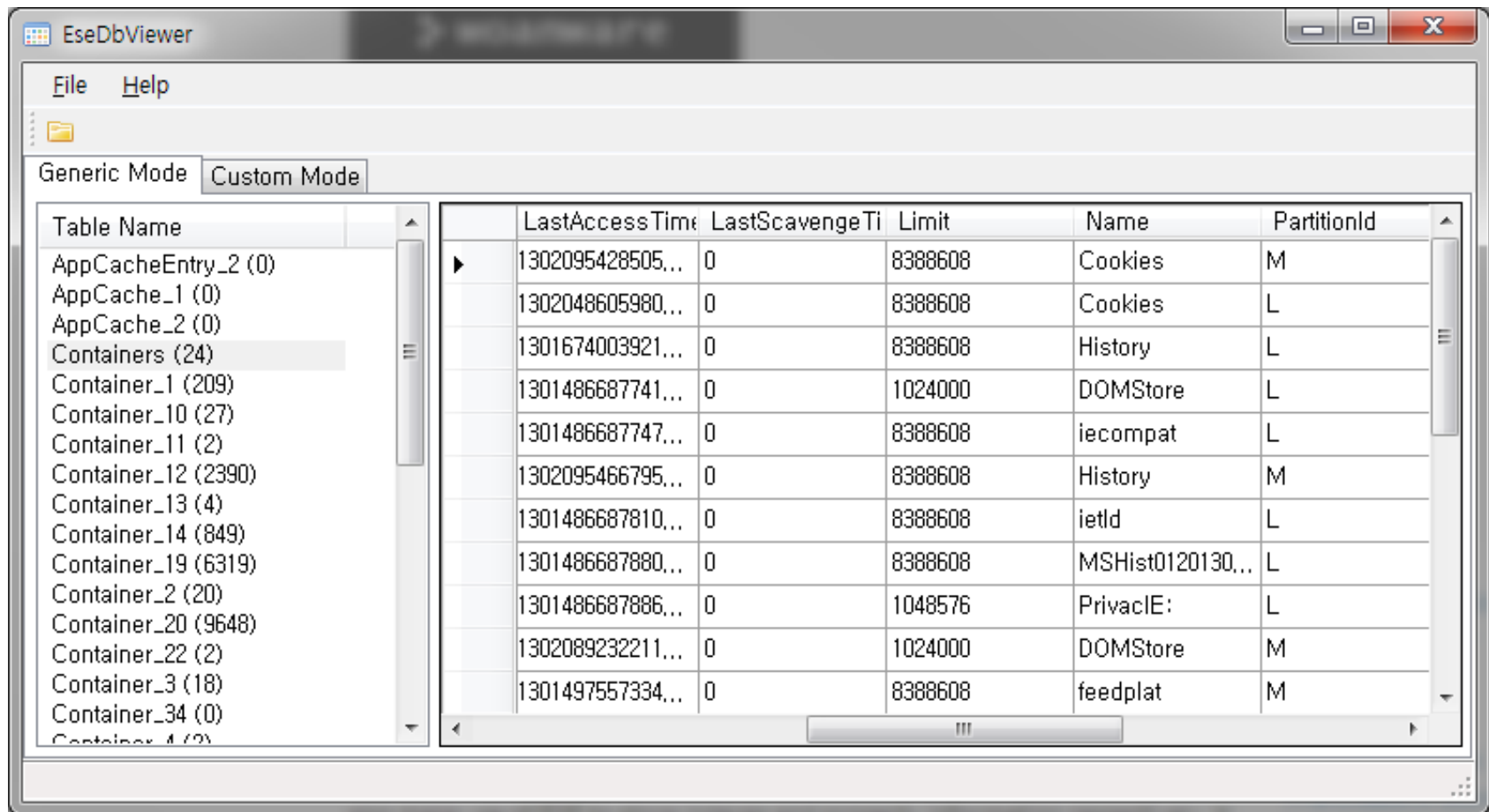


The screenshot shows the ESEDatabaseView application window. The title bar reads 'ESEDatabaseView: F:\CASES\Tools\forecopy\WebCacheV01.dat'. The menu bar includes File, Edit, View, Options, and Help. Below the menu is a toolbar with icons for file operations. A dropdown menu shows 'Container_19 [Table ID = 32, 25 Columns]'. The main area displays a table with the following columns: EntryId, ContainerId, CacheId, UrlHash, SecureDirectory, FileSize, Type, Flags, AccessCount, and SyncTime. The table contains 11 visible rows of data, all with ContainerId 19 and SyncTime 130148668802221998. The status bar at the bottom indicates '6319 record(s)' and provides the NirSoft Freeware website URL.

EntryId	ContainerId	CacheId	UrlHash	SecureDirectory	FileSize	Type	Flags	AccessCount	SyncTime
49	19	0	4204760502916132541	0	0	131076	4	1	130148668802221998
50	19	0	1369785911883575143	0	0	131076	4	1	130148668802221998
51	19	0	1369785909786733229	0	0	131076	4	1	130148668802221998
52	19	0	7287750639584482885	0	0	131076	4	1	130148668802221998
53	19	0	4930205073258224468	0	0	131076	4	1	130148668802221998
54	19	0	6212753529860451163	0	0	131076	4	1	130148668802221998
55	19	0	1468777140625858761	0	0	131076	4	1	130148668802221998
56	19	0	5738016100348468854	0	0	131076	4	1	130148668802221998
57	19	0	7279593526930702799	0	0	131076	4	1	130148668802221998
58	19	0	3811287102935530960	0	0	131076	4	1	130148668802221998
59	19	0	3110364454241166841	0	0	131076	4	1	130148668802221998
60	19	0	6950357309268175867	0	0	131076	4	1	130148668802221998

웹 캐시 파일 분석

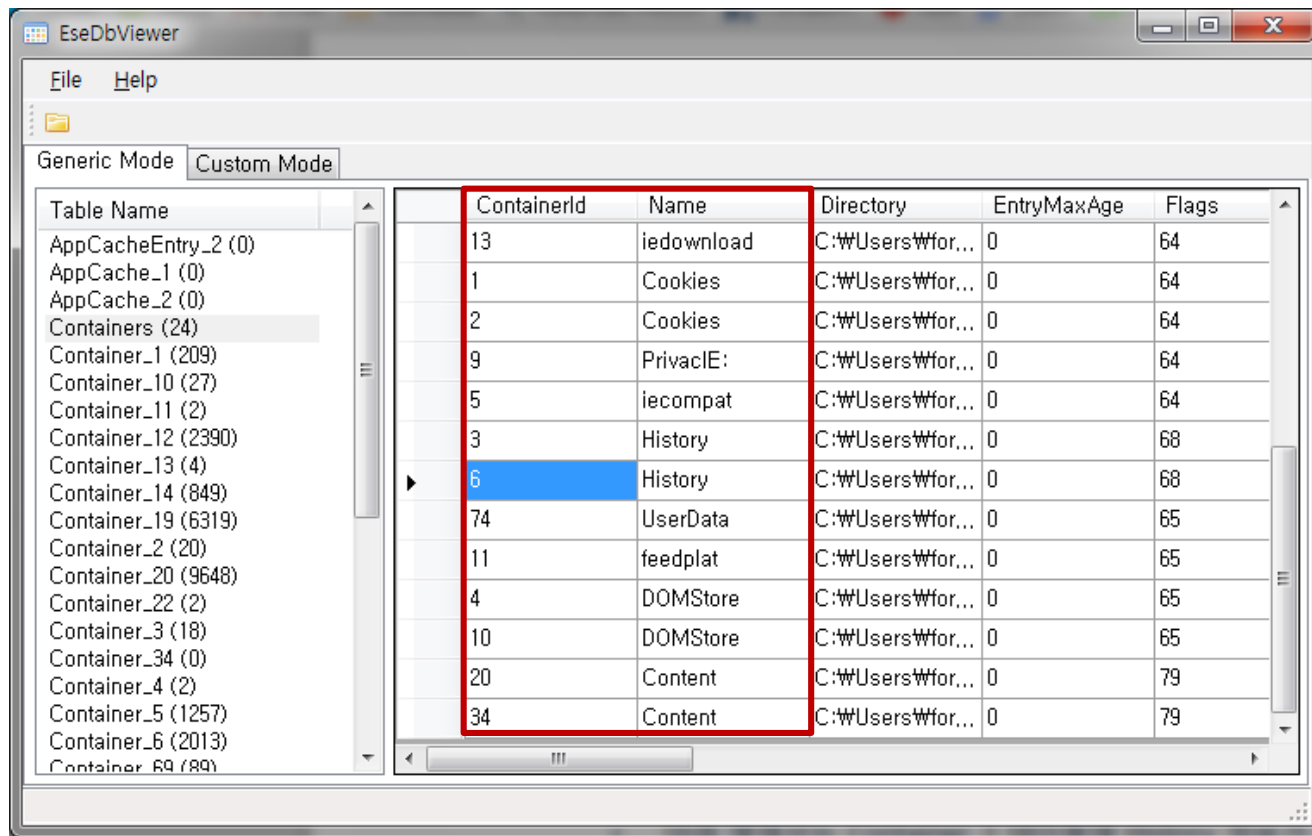
- **EseDbViewer** – woanware



웹 캐시 파일 분석

■ 웹 캐시 파일 테이블 구성

- "Containers" 테이블을 이용해 나머지 테이블의 용도 확인



EseDbViewer

File Help

Generic Mode Custom Mode

Table Name	ContainerId	Name	Directory	EntryMaxAge	Flags
AppCacheEntry_2 (0)	13	iedownload	C:\Users\Wfor...	0	64
AppCache_1 (0)	1	Cookies	C:\Users\Wfor...	0	64
AppCache_2 (0)	2	Cookies	C:\Users\Wfor...	0	64
Containers (24)	9	PrivacIE:	C:\Users\Wfor...	0	64
Container_1 (209)	5	iecompat	C:\Users\Wfor...	0	64
Container_10 (27)	3	History	C:\Users\Wfor...	0	68
Container_11 (2)	6	History	C:\Users\Wfor...	0	68
Container_12 (2390)	74	UserData	C:\Users\Wfor...	0	65
Container_13 (4)	11	feedplat	C:\Users\Wfor...	0	65
Container_14 (849)	4	DOMStore	C:\Users\Wfor...	0	65
Container_19 (6319)	10	DOMStore	C:\Users\Wfor...	0	65
Container_2 (20)	20	Content	C:\Users\Wfor...	0	79
Container_20 (9648)	34	Content	C:\Users\Wfor...	0	79
Container_22 (2)					
Container_3 (18)					
Container_34 (0)					
Container_4 (2)					
Container_5 (1257)					
Container_6 (2013)					
Container_69 (89)					

웹 캐시 파일 분석

■ 캐시 정보

- 디렉터리 경로가 "Content.IE5"로 끝나는 컨테이너

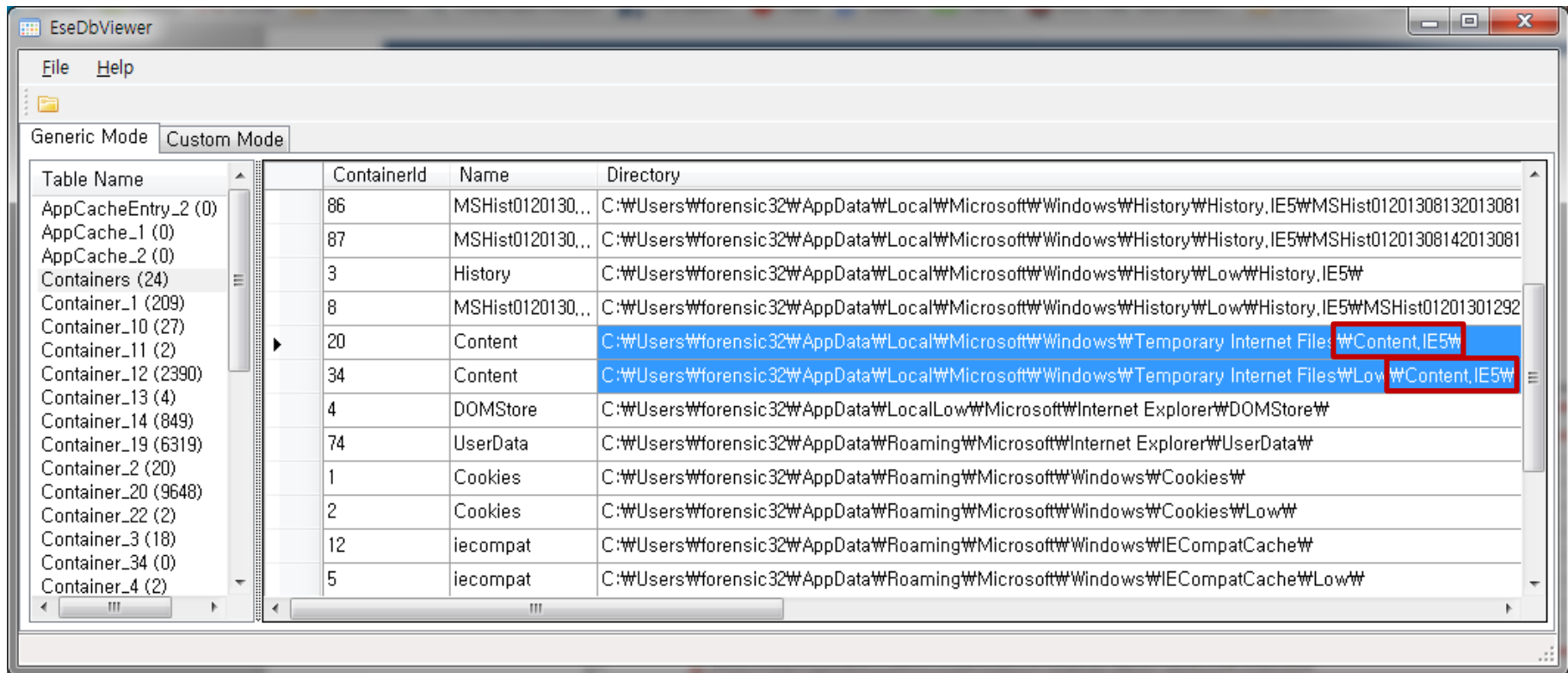


Table Name	ContainerId	Name	Directory
AppCacheEntry_2 (0)	86	MSHist0120130...	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist01201308132013081
AppCache_1 (0)	87	MSHist0120130...	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist01201308142013081
AppCache_2 (0)			
Containers (24)	3	History	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\Low\History.IE5\
Container_1 (209)	8	MSHist0120130...	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist01201301292
Container_10 (27)	20	Content	C:\Users\forensic32\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
Container_11 (2)	34	Content	C:\Users\forensic32\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\
Container_12 (2390)			
Container_13 (4)	4	DOMStore	C:\Users\forensic32\AppData\Local\Low\Microsoft\Internet Explorer\DOMStore\
Container_14 (849)	74	UserData	C:\Users\forensic32\AppData\Roaming\Microsoft\Internet Explorer\UserData\
Container_19 (6319)			
Container_2 (20)	1	Cookies	C:\Users\forensic32\AppData\Roaming\Microsoft\Windows\Cookies\
Container_20 (9648)	2	Cookies	C:\Users\forensic32\AppData\Roaming\Microsoft\Windows\Cookies\Low\
Container_22 (2)			
Container_3 (18)	12	iecompat	C:\Users\forensic32\AppData\Roaming\Microsoft\Windows\IECompatCache\
Container_34 (0)			
Container_4 (2)	5	iecompat	C:\Users\forensic32\AppData\Roaming\Microsoft\Windows\IECompatCache\Low\

웹 캐시 파일 분석

▪ 캐시 정보

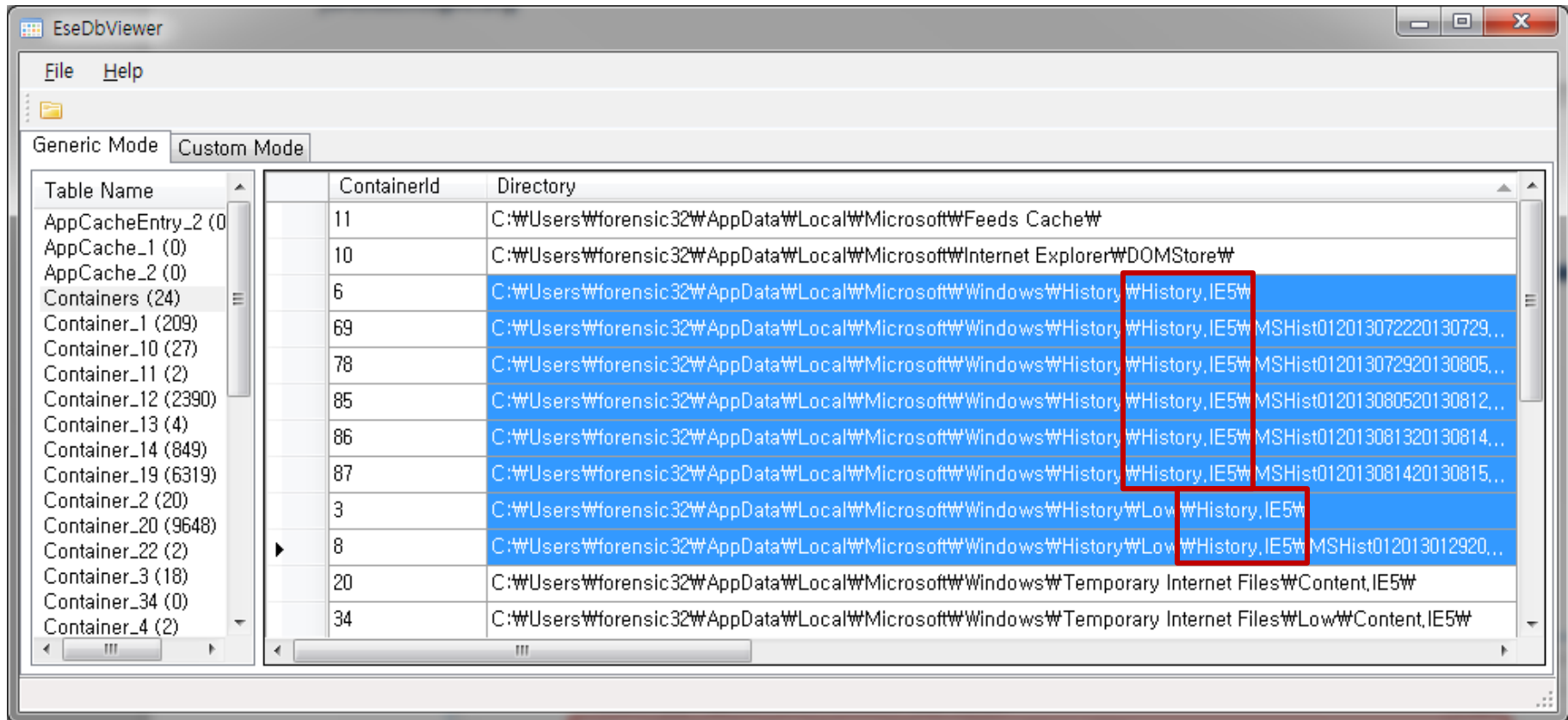
• 주요 필드 별 의미

- ✓ **URL** : 캐시 데이터를 다운로드한 사이트 주소
- ✓ **Access Time** : 캐시 데이터 다운로드(접근) 시간
- ✓ **Creation Time** : 캐시 데이터 파일 생성 시간
- ✓ **Modified Time** : 캐시 데이터 원본의 마지막 수정 시간
- ✓ **Expiry Time** : 캐시 데이터의 만료 시간, 이 값이 0이라면 웹 브라우저 종료 혹은 다른 페이지로 이동할 때 자동으로 캐시 데이터가 삭제됨
- ✓ **Sync Time** : Access Time과 동일
- ✓ **Filename** : 캐시 데이터 파일명
- ✓ **Filesize** : 캐시 데이터 크기
- ✓ **ResponseHeader** : HTTP 응답 헤더

웹 캐시 파일 분석

■ 히스토리 정보

- 경로에 "History.IE5"를 포함하는 컨테이너



EseDbViewer

File Help

Generic Mode Custom Mode

Table Name	ContainerId	Directory
AppCacheEntry_2 (0)	11	C:\Users\forensic32\AppData\Local\Microsoft\Feeds Cache\
AppCache_1 (0)	10	C:\Users\forensic32\AppData\Local\Microsoft\Internet Explorer\DOMStore\
AppCache_2 (0)	6	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\History.IE5\
Containers (24)	69	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013072220130729...
Container_1 (209)	78	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013072920130805...
Container_10 (27)	85	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013080520130812...
Container_11 (2)	86	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013081320130814...
Container_12 (2390)	87	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012013081420130815...
Container_13 (4)	3	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\Low\History.IE5\
Container_14 (849)	8	C:\Users\forensic32\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012013012920...
Container_19 (6319)	20	C:\Users\forensic32\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
Container_2 (20)	34	C:\Users\forensic32\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\
Container_20 (9648)		
Container_22 (2)		
Container_3 (18)		
Container_34 (0)		
Container_4 (2)		

웹 캐시 파일 분석

▪ 히스토리 정보

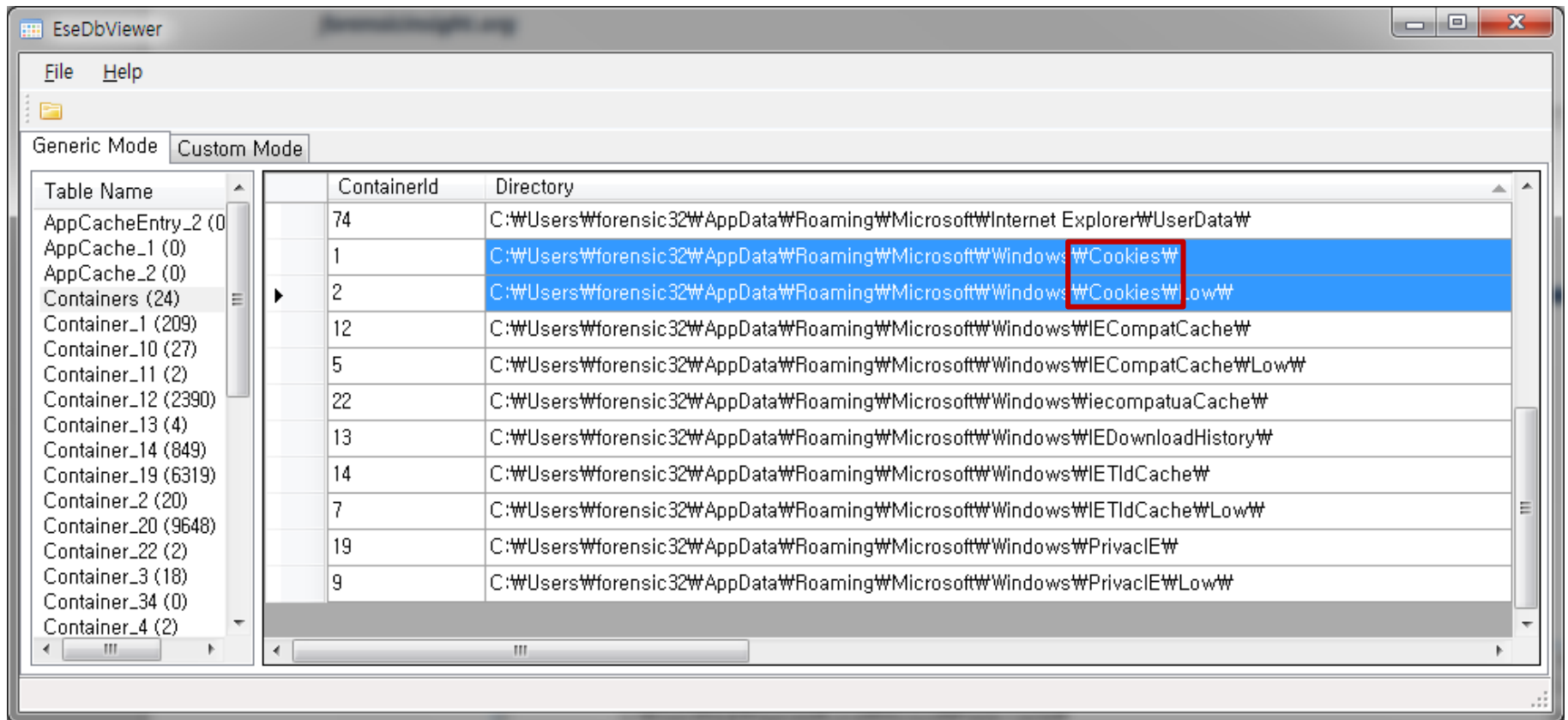
• 주요 필드 별 의미

- ✓ **URL** : 방문한 사이트(http://, https://), 열람한 파일(file://)
- ✓ **Access Time** : 사이트 접근 시간 또는 파일 열람 시간
- ✓ **Creation Time** : 항상 0
- ✓ **Modified Time** : Access Time과 유사
- ✓ **Expiry Time** : 히스토리 만료 시간, 해당 기간이 만료되면 테이블에서 레코드가 삭제됨(기본 20일)
- ✓ **Sync Time** : Access Time과 동일
- ✓ **ResponseHeader** : 웹 페이지 제목

웹 캐시 파일 분석

■ 쿠키 정보

- 경로에 "Cookies"를 포함하는 컨테이너



웹 캐시 파일 분석

▪ 쿠키 정보

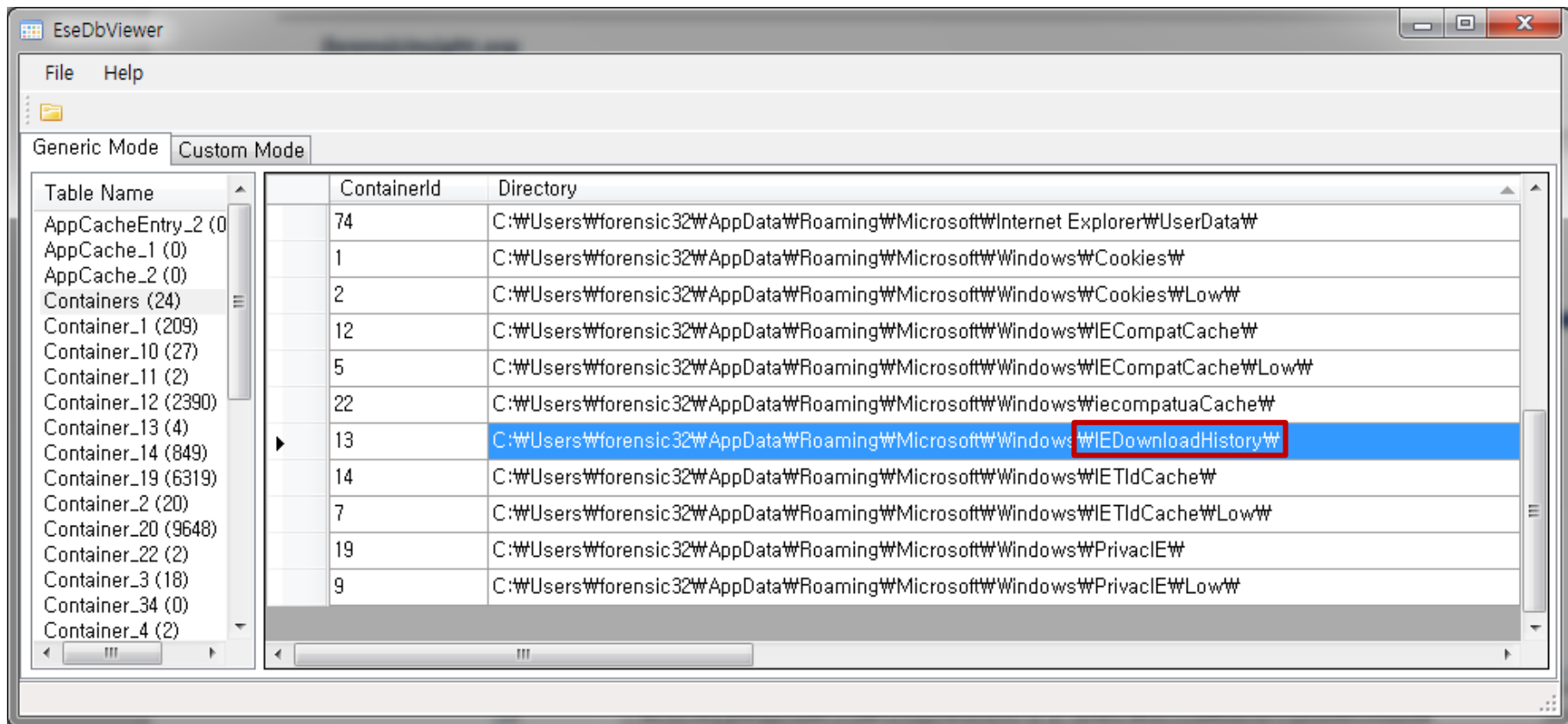
• 주요 필드 별 의미

- ✓ **URL** : 쿠키 호스트 정보
- ✓ **Access Time** : 사이트 마지막 접근 시간
- ✓ **Creation Time** : 쿠키 파일 생성 시간
- ✓ **Modified Time** : Access Time과 유사
- ✓ **Expiry Time** : 쿠키 데이터 만료 시간, 만료 시간이 지나면 테이블에서 레코드가 삭제됨(기본 20일)
- ✓ **Sync Time** : Access Time과 동일
- ✓ **Filename** : 쿠키 파일 이름

웹 캐시 파일 분석

다운로드 목록 정보

- 경로에 "IEDownloadHistory"를 포함하는 컨테이너



웹 캐시 파일 분석

▪ 다운로드 목록 정보

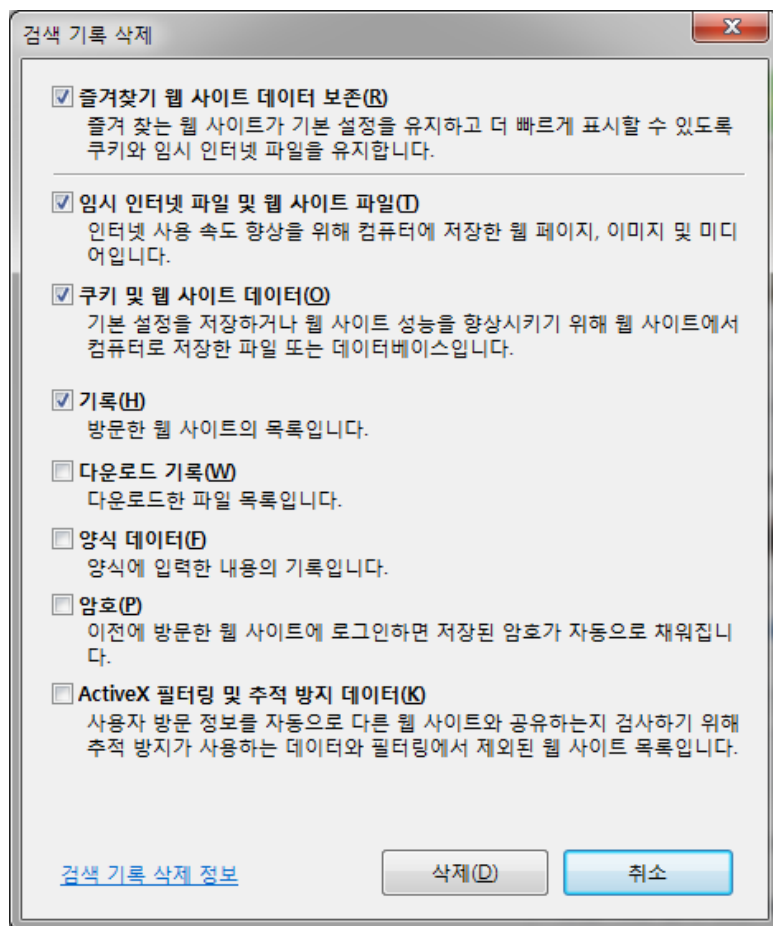
• 주요 필드 별 의미

- ✓ **URL** : 다운로드 GUID 값 저장
- ✓ **Access Time** : 다운로드 시간
- ✓ **Creation Time** : 항상 0
- ✓ **Modified Time** : 항상 0
- ✓ **Expiry Time** : 항상 0
- ✓ **Sync Time** : Access Time과 동일
- ✓ **ResponseHeader** : 소스 URL, 저장 경로 정보

삭제된 데이터 복구

■ 웹 브라우저 로그 삭제

- 기존과 동일한 방식으로 로그 삭제 가능



삭제된 데이터 복구

▪ 웹 브라우저 로그 삭제

- 로그 삭제 후 라이브에서 수집한 "Dirty Shutdown" 상태의 웹 캐시 파일
- "Clean Shutdown" 상태로 변경한 이후에도 많은 데이터가 잔존
- 일반적으로 "Dirty Shutdown" → "Clean Shutdown" 상태 변경 시 데이터 손실 발생
- "Dirty Shutdown" 상태에서 파싱이 가능한 도구 개발

실습 #2

- 웹 캐시 데이터 분석하기

