IE10 Forensics

blueangel

blueangel1275@gmail.com

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

목차

IE10 Forensics

- 기존 버전과의 차이점
- WebCacheV24.dat ?
- 데이터 수집
- 데이터 분석
- 삭제 데이터 복구 가능성 확인
- 결론

IE10 Forensics

- **기존 버전과의 차이점**
- WebCacheV24.dat ?
- 데이터 수집
- 데이터 분석
- 삭제 데이터 복구 가능성 확인
- 결론

기존 버전과의 차이점

▪ 기존 버전에서의 IE 로그 정보 저장 방식

- 각 정보는 아래와 같은 위치로 관리됨

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)

▪ IE 10에서의 로그 정보 저장 방식

- Cache, History, Cookie, Download List 의 인덱스 정보를 하나의 파일(WebCacheV24.dat)로 관리
- 위치 : %Profile%₩Appdata₩Local₩Microsoft₩Windows₩WebCache₩WebCacheV24.dat
- 예전 버전에서 각 정보가 위치했던 경로에는 container.dat 파일(빈 파일)이 존재, 해당 파일은 빈 파일임

IE10 Forensics

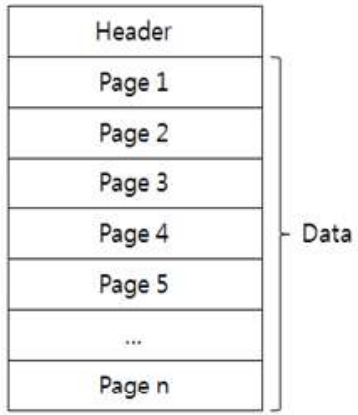
- 기존 버전과의 차이점
- **WebCacheV24.dat ?**
- 데이터 수집
- 데이터 분석
- 삭제 데이터 복구 가능성 확인
- 결론

WebCacheV24.dat ?

- ESE(Extensible Storage Engine) Database Format
  - Microsoft 사가 개발한 Indexed Sequential Access Method (ISAM) 데이터 저장 기술
  - JET Blue Storage Engine 라고도 함 (JET Red : Microsoft Access Database Engine)
  - MS Exchange (priv1.edb), Active Directory (ntds.dit), Windows Search (Windows.edb) 등에서 데이터를 저장하기 위해 사용함
  - 분류
    - ✓ ESE97 : Exchange 5.5
    - ✓ ESE98 : Exchange 2000 and later
    - ✓ ESENT : Windows NT and later, Active Directory, Windows Search

WebCacheV24.dat ?

- **기본 구조**



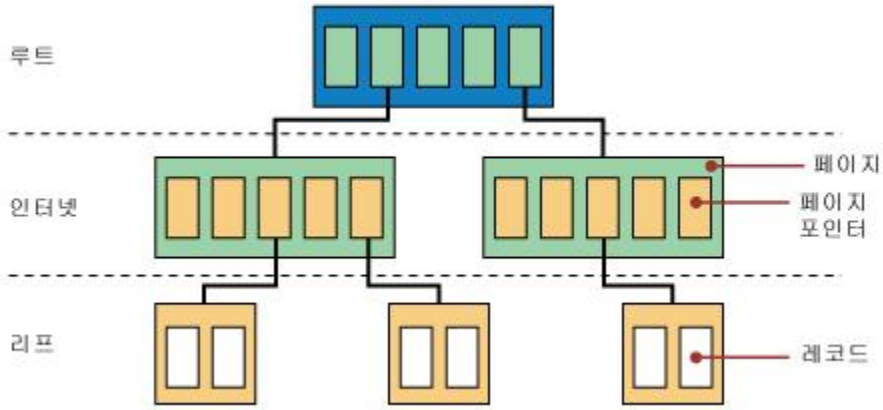
- **Header**
  - ✓ Signature : /xEF/xCD/xAB/x89
  - ✓ ESE Version
  - ✓ Page Size

E2	FC	43	13	EF	CD	AB	89	20	06	00	00	00	00	00	00
57	7F	20	00	00	00	00	00	38	FA	38	00	2B	04	0B	10
07	6E	01	00	00	00	00	00	00	00	00	00	00	00	00	00

- **Page**
  - ✓ 페이지 단위(2KB ~ 32KB)로 저장, 사용하는 응용프로그램에 따라 크기가 다름
  - ✓ 페이지는 40바이트의 페이지 헤더로 시작
  - ✓ 페이지 번호, 수정시간, 트리상에서 인접한 왼쪽/오른쪽 페이지 번호, 페이지 내 사용 가능 바이트 크기/시작위치
  - ✓ 일정한 크기의 페이지 단위로 저장하기 때문에 비할당 영역이 존재 가능

WebCacheV24.dat ?

- **B+ 트리 구조**
  - 데이터베이스 파일 내의 모든 데이터는 B+ 트리에 저장됨
  - 각 테이블은 데이터를 포함하는 하나의 B+ 트리로 구성됨
  - 테이블 및 관련 B+ 트리의 정의는 시스템 카탈로그라는 다른 B+ 트리에 저장됨



IE10 Forensics

- 기존 버전과의 차이점
- WebCacheV24.dat ?
- **데이터 수집**
- 데이터 분석
- 삭제 데이터 복구 가능성 확인
- 결론

데이터 수집

- WebCacheV24.dat 파일 수집의 주의 사항
  - WebCaheV24.dat 파일은 TaskHost 프로세스가 잡고 있음, 따라서 일반적인 복사로도 수집할 수 없음
  - 파일 시스템 분석을 통해 파일을 수집하여도 파일의 상태가 Dirty Shutdown 임

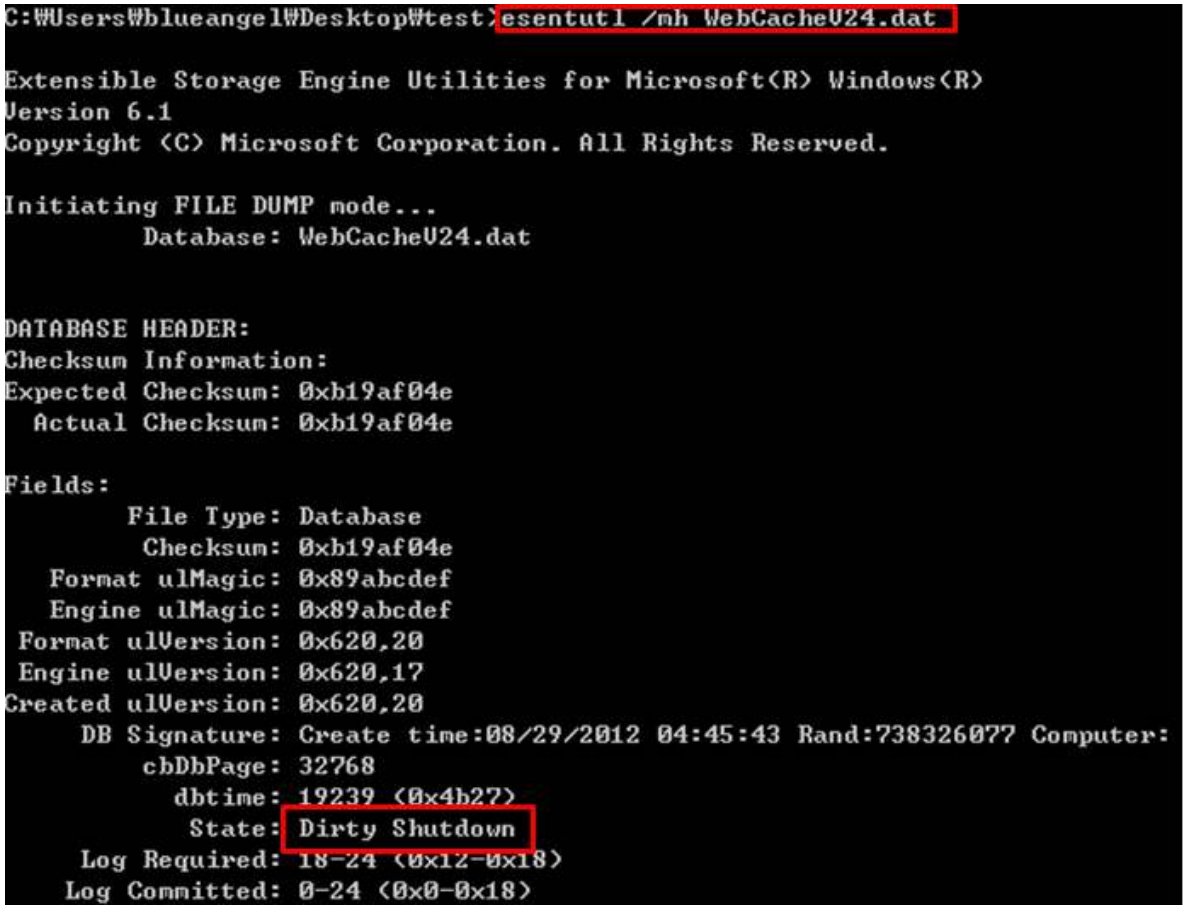
    ➔ 이 경우 일반적으로 많이 사용되는 EseDbViewer 로 분석을 수행할 수 없음

    ➔ Clean Shutdown 상태이어야 분석 가능

- Clean Shutdown 상태로 수집하기 위한 방법
  - Windows 를 정상 종료한 후, 파일 수집
  - esentutl 프로그램을 사용, 복구 작업을 수행하여 파일을 Clean Shutdown 상태로 변경

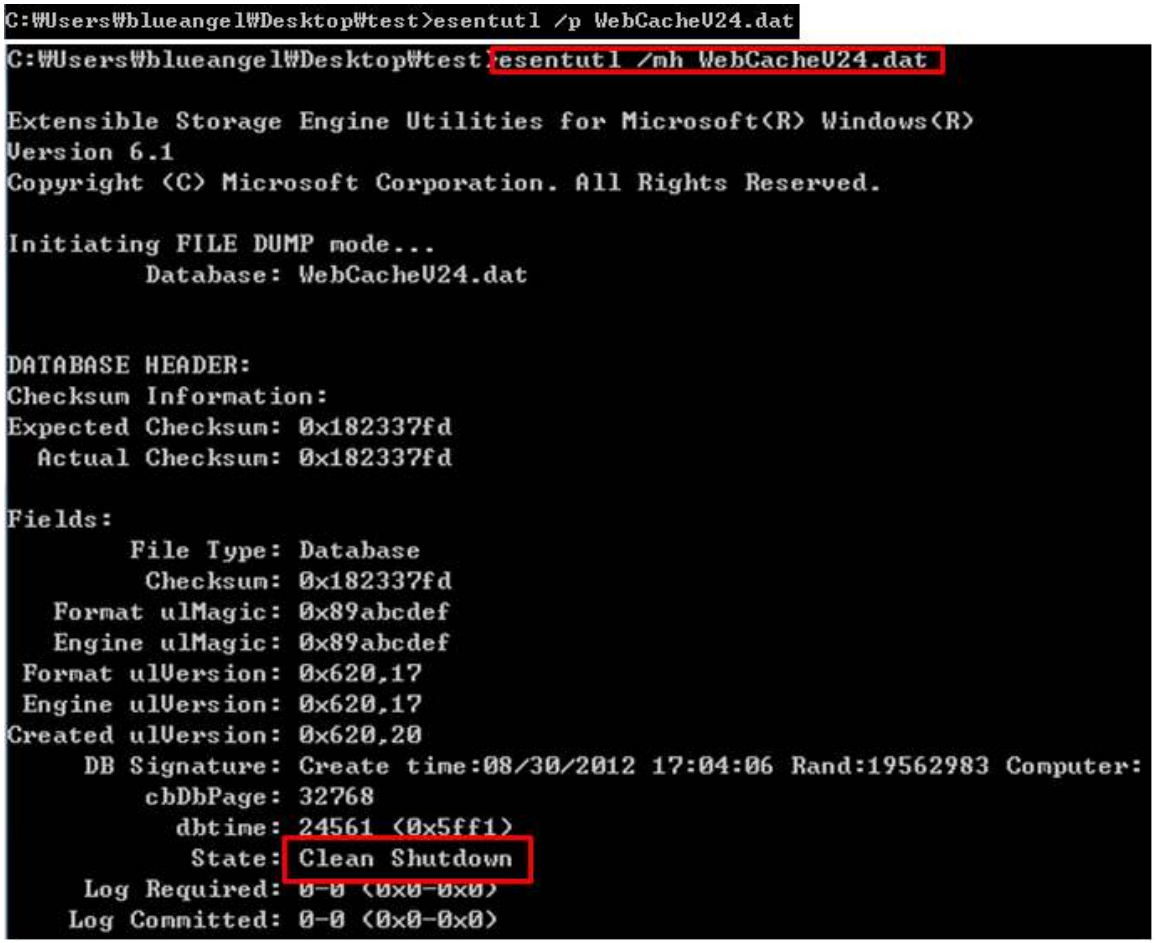
데이터 수집

- **Esentutl을 통한 WebCache24.dat 파일 수집**
  - esentutl /mh 옵션으로 분석 대상 파일의 상태 확인



데이터 수집

- **Esentutl을 통한 WebCache24.dat 파일 수집**
  - esentutl /p 옵션으로 파일 복구 후, 상태 확인



IE10 Forensics

- 기존 버전과의 차이점
- WebCacheV24.dat ?
- 데이터 수집
- **데이터 분석**
- 삭제 데이터 복구 가능성 확인
- 결론

데이터 분석

▪ 분석 도구

- EseDbViewer(http://www.woanware.co.uk/?page_id=89)
  - ✓ 관리자 권한으로 실행해야 동작함

▪ DB 전체 구성

- 각 정보들은 Container_N 형식의 이름을 가진 테이블에 저장됨
- 각 Container_N 테이블에 저장되는 정보의 종류는 Containers 테이블을 참조, 정보의 종류는 Directory 경로와 Name 값으로 구분
- 아래 예에서는 Container_3 테이블에 History 정보가 저장됨

Table Name
AppCacheEntry_1
AppCacheEntry_3
AppCacheEntry_5
AppCacheEntry_6
AppCache_1
AppCache_2
AppCache_3
AppCache_4
AppCache_5
Containers
Container_1
Container_10
Container_11

ContainerId	Directory	Name
1	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Fil...	Content
2	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Feeds Cache₩	feedplat
3	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩History₩History.IE5₩	History
4	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowsphotos_8wek...	Content
5	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowsphotos_8wek...	Cookies
6	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowscommunicati...	Cookies
7	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩IECompatCache₩	iecompat
8	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩iecompatuaCache...	iecompatua
9	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩Cookies₩Low₩	Cookies

데이터 분석

▪ Cache 정보 분석

- 저장 테이블

  ✓ Name 값이 "Content"

  ✓ Directory 경로의 끝이 "Content.IE5" 로 끝남

ContainerId	Directory	Name
1	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.IE5₩	Content
2	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Feeds Cache₩	feedplat
3	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩History₩History.IE5₩	History
4	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowsphotos_8wekyb3d8bbwe₩AC₩INetCache₩	Content
5	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowsphotos_8wekyb3d8bbwe₩AC₩INetCookies₩	Cookies
6	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowscommunicationsapps_8wekyb3d8bbwe₩AC₩INetCookies₩	Cookies
7	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩IECompatCache₩	iecompat
8	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩iecompatuaCache₩	iecompatua
9	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩Cookies₩Low₩	Cookies
10	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩History₩Low₩History.IE5₩	History
11	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Low₩Content.IE5₩	Content

데이터 분석

▪ Cache 정보 분석

- 주요 필드별 저장 정보
  - ✓ Url : 해당 Cache 데이터를 다운로드한 URL
  - ✓ Access Time : Cache 데이터 다운로드(접근) 시간 (FILETIME 을 10진수로 변환한 값)
  - ✓ Creation Time : Cache 데이터 파일 생성 시간
  - ✓ Modified Time : 해당 Cache 데이터의 웹 서버에서의 마지막 수정 시간
  - ✓ Expiry Time : 해당 Cache 데이터의 만료 시간, 이 값이 0일 경우, 해당 데이터는 웹 브라우저가 종료되거나 다른 페이지로 넘어갈 시 바로 삭제됨
  - ✓ Sync Time : Access Time 과 동일
  - ✓ Filename : Cache 데이터 파일명
  - ✓ Filesize : Cache 데이터 크기
  - ✓ SecureDirectory : 해당 Cache 데이터가 저장되어 있는 폴더의 인덱스 정보
    - 폴더 정보는 Containers 테이블의 SecureDirectories 필드의 16진수값을 사용
    - 해당 16진수값을 8자 단위로 끊어서 배열로 만듬
    - SecureDirectory 필드의 인덱스 값을 위에서 만든 배열에 적용
    - 인덱스 값을 통해 배열에서 얻어온 16진수가 해당 캐시 데이터가 저장되어 있는 폴더명임 => 이를 통해 해당 캐시 데이터가 저장되어 있는 전체 경로를 구할 수 있음

SecureDirectories
F2OE37B0OVCNLQ17UXGVEAT6PKX87JQR

데이터 분석

▪ Cache 정보 분석

• 주요 필드별 저장 정보(계속)

✓ ResponseHeader : 해당 캐시 데이터의 HTTP 헤더값(Hex 값) ➔ 실제로 보면 해당 데이터가 그대로 들어가 있음

ResponseHeaders
485454502f312e3120323030204f4b0d0a436f6e74...
485454502f312e3120323030204f4b0d0a436f6e74...
485454502f312e3120323030204f4b0d0a436f6e74...
485454502f312e3120323030204f4b0d0a436f6e74...

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
01507888	00	2E	00	68	00	74	00	6D	00	00	00	01	48	54	54	50	...h.t.m....HTTP
01507904	2F	31	2E	31	20	32	30	30	20	4F	4B	0D	0A	43	6F	6E	/1.1 200 OK..Con
01507920	74	65	6E	74	2D	4C	65	6E	67	74	68	3A	20	31	30	38	tent-Length: 108
01507936	38	38	0D	0A	43	6F	6E	74	65	6E	74	2D	54	79	70	65	88..Content-Type
01507952	3A	20	74	65	78	74	2F	68	74	6D	6C	3B	20	63	68	61	: text/html; cha
01507968	72	73	65	74	3D	75	74	66	2D	38	0D	0A	58	2D	41	73	rset=utf-8..X-As
01507984	70	4E	65	74	2D	56	65	72	73	69	6F	6E	3A	20	34	2E	pNet-Version: 4.
01508000	30	2E	33	30	33	31	39	0D	0A	58	2D	50	6F	77	65	72	0.30319..X-Power

✓ UrlHash : 무슨 hash?? => URL의 앞 부분이 비슷하면 Hash의 앞 부분도 비슷해짐

Url	UrlHash
http://ad.realmedia.co.kr/empty.html	476633729630323915
http://www.gstatic.com/inputtools/images/tia.png	538928554743058525
http://www.gstatic.com/bg/8yfWzKzwlcE2ofUqWK0LjbpyQA3mnwz_HPapssxP01I.js	538928556953535846
http://ads.realclick.co.kr/photo/fomos1_pt2.js	789735489698357665
http://ads.realclick.co.kr/ad_tpl/headcopy.rc?dsn=1&mcode=Zm9tb3My	789735490270174323
http://ads.realclick.co.kr/ad_tpl/headcopy.rc?dsn=1&mcode=Zm9tb3M2	789735490625967812
http://ads.realclick.co.kr/ad_tpl/headcopy.rc?eff=ss&dsn=1&mcode=Zm9tb3M5	789735491723898084
http://ads.realclick.co.kr/ad_photo/fomos3_pt1.js	789735492055459288
http://ads.realclick.co.kr/ad_tpl/headcopy.rc?dsn=1&mcode=Zm9tb3MxMQ==	789735492341084577
http://t3.gstatic.com/images?q=tbn:ANd9GcQR3BoFkwiOQPxnUpvo8SjNxX-QmIKqS5Xsz1S_DiMAGN0cz_IogqWp	946908635450847949
http://cdn.semanticrep.com/mov/lottesoju0731.mp4	1108317219489148053
http://cdn.semanticrep.com/mov/firstbirthday.mp4	1108317220232051507
http://cdn.semanticrep.com/mov/unicef.mp4	1108317221084784188
res://ieframe.dll/errorPageStrings.js	1108335023924497798
res://ieframe.dll/NewErrorPageTemplate.css	1108335027245762666
res://ieframe.dll/dnserror.htm	1108335027536763309
res://ieframe.dll/httpErrorPagesScripts.js	1108335028020826921

데이터 분석

▪ History 정보 분석

- 저장 테이블

  ✓ Name 값이 "History" or "MSHist01~ "

  ✓ Directory 경로의 끝이 "History.IE5" 로 끝남

ContainerId	Directory	Name
1	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.IE5₩	Content
2	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Feeds Cache₩	feedplat
3	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩History₩History.IE5₩	History
4	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowsphotos_8wekyb3d8bbwe₩AC₩INetCache₩	Content
5	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowsphotos_8wekyb3d8bbwe₩AC₩INetCookies₩	Cookies
6	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowscommunicationsapps_8wekyb3d8bbwe₩AC₩INetCooki...	Cookies
7	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩IECompatCache₩	iecompat
8	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩iecompatuaCache₩	iecompatua
9	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩Cookies₩Low₩	Cookies
10	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩History₩Low₩History.IE5₩	History
11	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Low₩Content.IE5₩	Content
12	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩History₩History.IE5₩MSHist012012082920120830₩	MSHist012012082920120830

데이터 분석

▪ History 정보 분석

- 주요 필드별 저장 정보
  - ✓ Url
    - http://~ => 방문 사이트 URL
    - file:///~ => 열람한 파일 전체 경로

```
Visited: %EC%A0%95%ED%9B%88@file:///C:/Users/i i/Desktop/test.txt.txt
Visited: %EC%A0%95%ED%9B%88@file:///C:/Users/i i/AppData/Roaming/Microsoft/Windows/Cookies/Low/C9P5TZJL.txt
Visited: %EC%A0%95%ED%9B%88@http://www.google.co.kr/url?sa=t&rct=j&q=filetype%3Apdf%20digital%20forensics&source=web&c
Visited: %EC%A0%95%ED%9B%88@http://www.google.co.kr/
Visited: %EC%A0%95%ED%9B%88@http://eyenews.hankooki.com/mm_view.php?gisa_id=123982&cate_code=0101
Visited: %EC%A0%95%ED%9B%88@http://eyenews.hankooki.com/mm_theme_view.php?gisa_id=00120038&cate_code=0402
```

  - ✓ Access Time : 해당 사이트 접근 시간 or 해당 파일 열람 시간 (FILETIME을 10진수로 변환한 값)
  - ✓ Creation Time : 항상 0
  - ✓ Modified Time : Access Time 과 동일(조금 차이 날 수 도 있지만 변환해 보면 초 시간까지 동일)
  - ✓ Expiry Time : 해당 History 데이터 만료 시간, 해당 기간이 만료되면 테이블에서 레코드가 삭제됨(기본 20일)
  - ✓ Sync Time : Access Time 과 동일
  - ✓ ResponseHeader : 웹 페이지 제목 정보가 들어있는 데이터가 저장됨 (Hex 값)
    - 저장되어 있는 Hex 데이터를 Hex 에디터에 붙여 넣으면 다음과 같음
    - 시작 위치부터 0x3A 위치에 4바이트 크기로 웹 페이지 제목 문자열 크기가 저장됨. 웹 페이지 제목은 유니코드 이므로 실제 값에 2배를 해주어야 읽을 바이트 수를 구할 수 있음
    - 문자열 크기 데이터에 바로 이어서 웹 페이지 제목 문자열이 유니코드로 저장됨

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	C6	00	00	00	C2	00	00	00	31	53	50	53	A1	14	02	00	Æ...Â...1SPSi...
00000010	00	00	00	00	C0	00	00	00	00	00	00	46	11	00	00	00	....À.....F....
00000020	17	00	00	00	00	13	00	00	00	02	00	00	00	4D	00	00	.............M..
00000030	00	10	00	00	00	00	1F	00	00	00	1D	00	00	00	44	00	..............D.
00000040	61	00	75	00	6D	00	20	00	2D	00	20	00	DD	C0	5C	D6	a.u.m. .-. .ÝÀ\Ö
00000050	74	C7	20	00	14	BC	10	B0	E4	B2	21	00	20	00	4C	00	tÇ ..¼.°ä²!. .L.
00000060	69	00	66	00	65	00	20	00	4F	00	6E	00	20	00	44	00	i.f.e. .O.n. .D.
00000070	61	00	75	00	6D	00	00	00	00	00	15	00	00	00	18	00	a.u.m...........

  - ✓ UrlHash : 무슨 hash?? => URL의 앞 부분이 비슷하면 Hash의 앞 부분도 비슷해짐

데이터 분석

▪ Cookie 정보 분석

- 저장 테이블

✓ Name 값이 "Cookies"

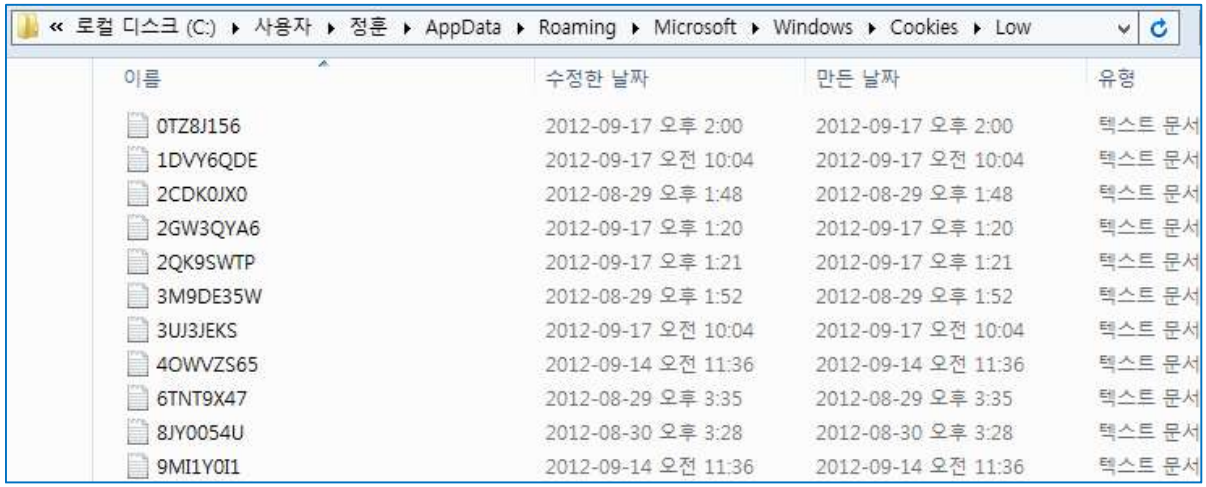
✓ Directory 경로의 끝이 "Cookies" 폴더가 있음

ContainerId	Directory	Name
1	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Content.IE5₩	Content
2	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Feeds Cache₩	feedplat
3	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩History₩History.IE5₩	History
4	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowsphotos_8wekyb3d8bbwe₩AC₩INetCache₩	Content
5	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowsphotos_8wekyb3d8bbwe₩AC₩INetCookies₩	Cookies
6	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowscommunicationsapps_8wekyb3d8bbwe₩AC₩INetCookies₩	Cookies
7	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩IECompatCache₩	iecompat
8	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩iecompatuaCache₩	iecompatua
9	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩Cookies₩Low₩	Cookies
10	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩History₩Low₩History.IE5₩	History
11	C:₩Users₩정훈₩AppData₩Local₩Microsoft₩Windows₩Temporary Internet Files₩Low₩Content.IE5₩	Content
13	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩Cookies₩	Cookies
14	C:₩Users₩정훈₩AppData₩LocalLow₩Microsoft₩Internet Explorer₩DOMStore₩	DOMStore

데이터 분석

▪ Cookie 정보 분석

- 주요 필드 별 저장 정보
  - ✓ Url : 해당 Cookie 정보의 호스트 정보
  - ✓ Access Time : 해당 사이트 마지막 접근 시간 (FILETIME을 10진수로 변환한 값)
  - ✓ Creation Time : 해당 쿠키 파일(.txt) 생성 시간
  - ✓ Modified Time : Access Time 과 동일(조금 차이 날 수 도 있지만 변환해 보면 초 시간까지 동일)
  - ✓ Expiry Time : 해당 Cookie 데이터 만료 시간, 해당 기간이 만료되면 테이블에서 레코드가 삭제됨(기본 20일)
  - ✓ Sync Time : Access Time 과 동일
  - ✓ Filename : 실제 쿠키 정보를 저장하고 있는 쿠키 파일(.txt)의 이름, 경로는 Container 테이블의 Directory에서 확인, 쿠키 파일 포멧은 이전과 동일



데이터 분석

▪ Download List 정보 분석

- 저장 테이블

  ✓ Name 값이 "History" or "MSHist01~ "

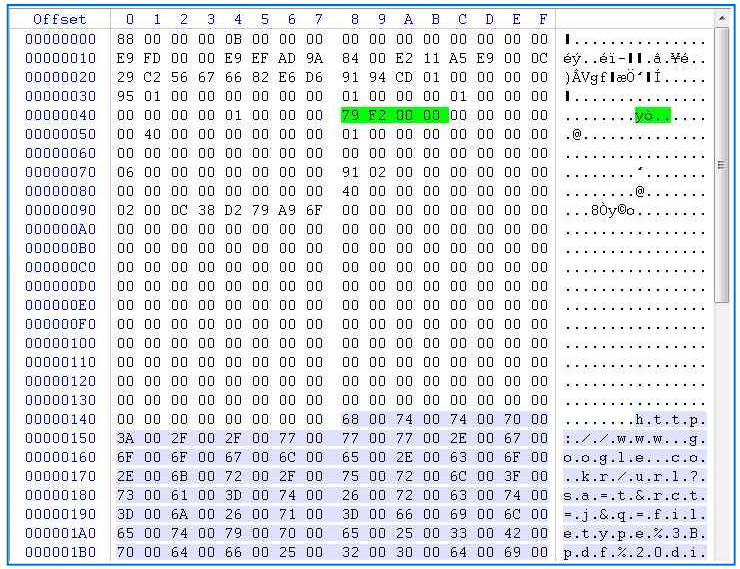
  ✓ Directory 경로의 끝이 "History.IE" 로 끝남

23	C:₩Users₩정훈₩AppData₩Local₩Packages₩windows_ie_ac_001₩AC₩INetCache₩	Content
24	C:₩Users₩정훈₩AppData₩Local₩Packages₩windows_ie_ac_001₩AC₩Microsoft₩Internet Explorer₩DOMStore₩	DOMStore
25	C:₩Users₩정훈₩AppData₩Roaming₩Microsoft₩Windows₩IEDownloadHistory₩	iedownload
26	C:₩Users₩정훈₩AppData₩Local₩Packages₩microsoft.windowscommunicationsapps_8wekyb3d8bbwe₩AC₩Microsoft₩Inter...	DOMStore

데이터 분석

▪ Download List 정보 분석

- 주요 필드 별 저장 정보
  - ✓ Url : 다운로드 GUID 값 저장
  - ✓ Access Time : 다운로드 시간 (FILETIME을 10진수로 변환한 값)
  - ✓ Creation Time : 항상 0
  - ✓ Modified Time : 항상 0
  - ✓ Expiry Time : 항상 0
  - ✓ Sync Time : Access Time 과 동일
  - ✓ ResponseHeader : 소스 URL, 저장 경로 정보가 들어 있는 데이터가 저장됨(Hex 값)
    - 시작 위치 부터 0x48 위치에 다운로드 데이터 크기 정보(8byte)
    - 시작 위치 부터 0x148(index.dat 에서는 0x138) 위치에 문자열 배열 시작



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	88	00	00	00	0B	00	00	00	00	00	00	00	00	00	00	00	▮.....
00000010	E9	FD	00	00	E9	EF	AD	9A	84	00	E2	11	A5	E9	00	0C	éý..éï-▮▮.â.¥é..
00000020	29	C2	56	67	66	82	E6	D6	91	94	CD	01	00	00	00	00	)ÂVgf▮æÖ´▮Í.....
00000030	95	01	00	00	00	00	00	00	01	00	00	00	01	00	00	00	▮.....
00000040	00	00	00	00	01	00	00	00	79	F2	00	00	00	00	00	00	........yò.....
00000050	00	40	00	00	00	00	00	00	01	00	00	00	00	00	00	00	.@.....
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000070	06	00	00	00	00	00	00	00	91	02	00	00	00	00	00	00	........´.....
00000080	00	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	........@.....
00000090	02	00	0C	38	D2	79	A9	6F	00	00	00	00	00	00	00	00	...8Òy©o.....
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	.....
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	00	00	00	00	00	00	00	00	68	00	74	00	74	00	70	00	.....h.t.t.p.
00000150	3A	00	2F	00	2F	00	77	00	77	00	77	00	2E	00	67	00	:././.w.w.w...g.
00000160	6F	00	6F	00	67	00	6C	00	65	00	2E	00	63	00	6F	00	o.o.g.l.e...c.o.
00000170	2E	00	6B	00	72	00	2F	00	75	00	72	00	6C	00	3F	00	..k.r./.u.r.l.?.
00000180	73	00	61	00	3D	00	74	00	26	00	72	00	63	00	74	00	s.a.=.t.&.r.c.t.
00000190	3D	00	6A	00	26	00	71	00	3D	00	66	00	69	00	6C	00	=.j.&.q.=.f.i.l.
000001A0	65	00	74	00	79	00	70	00	65	00	25	00	33	00	42	00	e.t.y.p.e.%.3.B.
000001B0	70	00	64	00	66	00	25	00	32	00	30	00	64	00	69	00	p.d.f.%.2.0.d.i.

데이터 분석

▪ Download List 정보 분석

- 주요 필드 별 저장 정보(계속)
  - ✓ ResponseHeader : 소스 URL, 저장 경로 정보가 들어 있는 데이터가 저장됨(Hex 값)
    - 문자열 배열의 마지막 문자열은 저장 경로, 마지막에 두 번째 문자열은 소스 URL

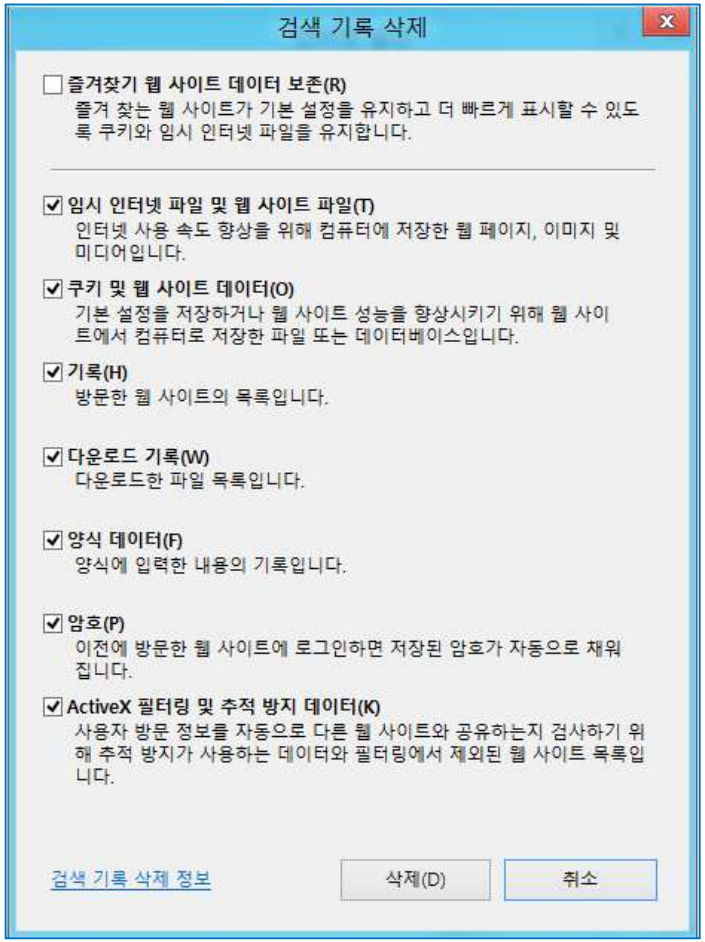
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000912	00	00	61	00	70	00	70	00	6C	00	69	00	63	00	61	00	..a.p.p.l.i.c.a.
00000928	74	00	69	00	6F	00	6E	00	2F	00	70	00	64	00	66	00	t.i.o.n./.p.d.f.
00000944	00	00	43	00	3A	00	5C	00	55	00	73	00	65	00	72	00	..C.:.\.U.s.e.r.
00000960	73	00	5C	00	15	C8	C8	D6	5C	00	41	00	70	00	70	00	s.\..ÈÈÖ\.A.p.p.
00000976	44	00	61	00	74	00	61	00	5C	00	4C	00	6F	00	63	00	D.a.t.a.\.L.o.c.
00000992	61	00	6C	00	5C	00	4D	00	69	00	63	00	72	00	6F	00	a.l.\.M.i.c.r.o.
00001008	73	00	6F	00	66	00	74	00	5C	00	57	00	69	00	6E	00	s.o.f.t.\.W.i.n.
00001024	64	00	6F	00	77	00	73	00	5C	00	54	00	65	00	6D	00	d.o.w.s.\.T.e.m.
00001040	70	00	6F	00	72	00	61	00	72	00	79	00	20	00	49	00	p.o.r.a.r.y. .I.
00001056	6E	00	74	00	65	00	72	00	6E	00	65	00	74	00	20	00	n.t.e.r.n.e.t. .
00001072	46	00	69	00	6C	00	65	00	73	00	5C	00	4C	00	6F	00	F.i.l.e.s.\.L.o.
00001088	77	00	5C	00	43	00	6F	00	6E	00	74	00	65	00	6E	00	w.\.C.o.n.t.e.n.
00001104	74	00	2E	00	49	00	45	00	35	00	5C	00	52	00	4A	00	t...I.E.5.\.R.J.
00001120	41	00	47	00	4B	00	4F	00	30	00	57	00	5C	00	63	00	A.G.K.O.0.W.\.c.
00001136	6F	00	6D	00	70	00	75	00	74	00	65	00	72	00	5F	00	o.m.p.u.t.e.r._.
00001152	66	00	6F	00	72	00	65	00	6E	00	73	00	69	00	63	00	f.o.r.e.n.s.i.c.
00001168	73	00	5F	00	70	00	72	00	69	00	6D	00	65	00	72	00	s._.p.r.i.m.e.r.
00001184	5B	00	31	00	5D	00	2E	00	70	00	64	00	66	00	00	00	[.1.]...p.d.f...
00001200	68	00	74	00	74	00	70	00	73	00	3A	00	2F	00	2F	00	h.t.t.p.s.:././.
00001216	76	00	69	00	61	00	66	00	6F	00	72	00	65	00	6E	00	v.i.a.f.o.r.e.n.
00001232	73	00	69	00	63	00	73	00	2E	00	63	00	6F	00	6D	00	s.i.c.s...c.o.m.
00001248	2F	00	77	00	70	00	69	00	6E	00	73	00	74	00	61	00	/.w.p.i.n.s.t.a.
00001264	6C	00	6C	00	2F	00	77	00	70	00	2D	00	63	00	6F	00	l.l./.w.p.-.c.o.
00001280	6E	00	74	00	65	00	6E	00	74	00	2F	00	75	00	70	00	n.t.e.n.t./.u.p.
00001296	6C	00	6F	00	61	00	64	00	73	00	2F	00	32	00	30	00	l.o.a.d.s./.2.0.
00001312	30	00	38	00	2F	00	31	00	31	00	2F	00	63	00	6F	00	0.8./.1.1./.c.o.
00001328	6D	00	70	00	75	00	74	00	65	00	72	00	5F	00	66	00	m.p.u.t.e.r._.f.
00001344	6F	00	72	00	65	00	6E	00	73	00	69	00	63	00	73	00	o.r.e.n.s.i.c.s.
00001360	5F	00	70	00	72	00	69	00	6D	00	65	00	72	00	2E	00	_.p.r.i.m.e.r..
00001376	70	00	64	00	66	00	00	00	43	00	3A	00	5C	00	55	00	p.d.f...C.:.\.U.
00001392	73	00	65	00	72	00	73	00	5C	00	15	C8	C8	D6	5C	00	s.e.r.s.\..ÈÈÖ\.
00001408	44	00	6F	00	77	00	6E	00	6C	00	6F	00	61	00	64	00	D.o.w.n.l.o.a.d.
00001424	73	00	5C	00	63	00	6F	00	6D	00	70	00	75	00	74	00	s.\.c.o.m.p.u.t.
00001440	65	00	72	00	5F	00	66	00	6F	00	72	00	65	00	6E	00	e.r._.f.o.r.e.n.
00001456	73	00	69	00	63	00	73	00	5F	00	70	00	72	00	69	00	s.i.c.s._.p.r.i.
00001472	6D	00	65	00	72	00	2E	00	70	00	64	00	66	00	00	00	m.e.r...p.d.f...

IE10 Forensics

- 기존 버전과의 차이점
- WebCacheV24.dat ?
- 데이터 수집
- 데이터 분석
- **삭제 데이터 복구 가능성 확인**
- 결론

삭제 데이터 복구 가능성 확인

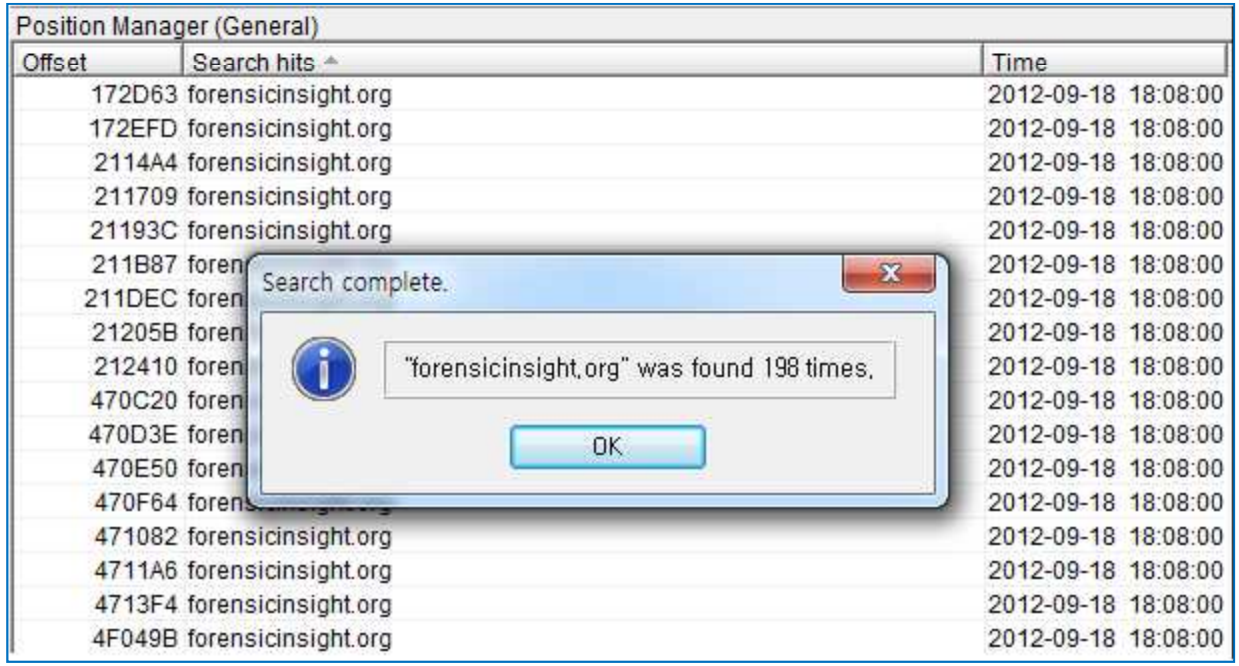
- **로그 삭제**
  - 기존 방식과 동일하게 웹 브라우저 로그 기록 삭제 가능



삭제 데이터 복구 가능성 확인

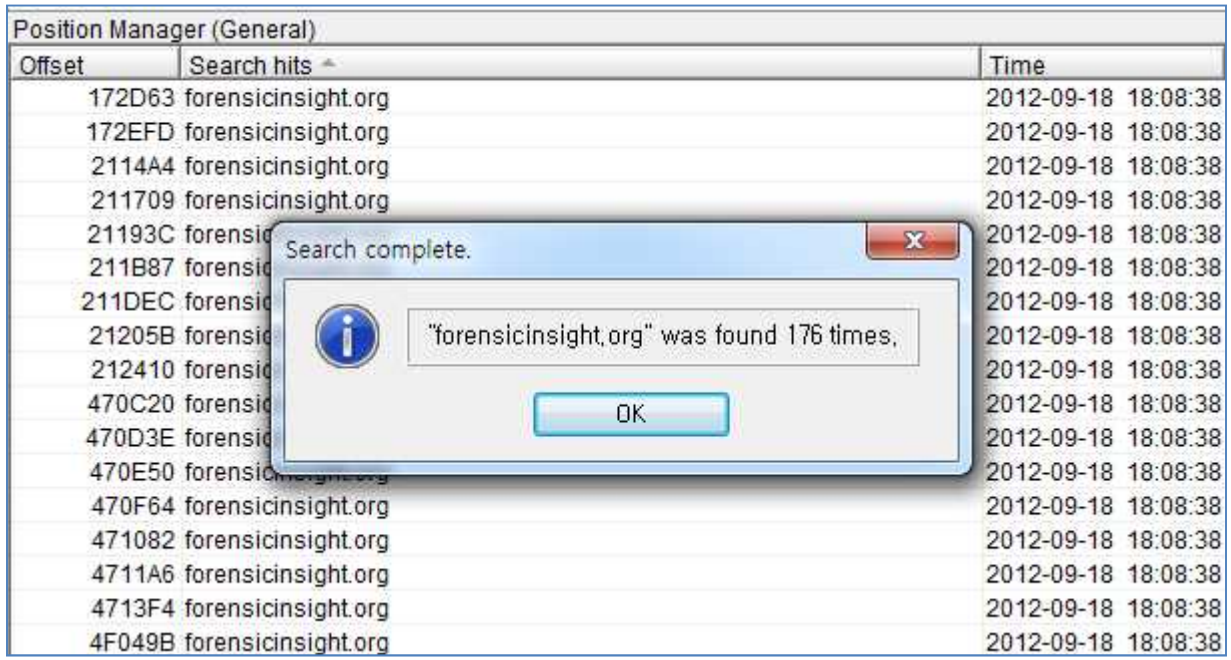
- **복구 가능성 확인**
  - 삭제 후, 바로 수집한 Dirty Shutdown 상태에서는 많은 양의 레코드가 남아 있는 것을 확인
  - Clean Shutdown 상태로 변환(esentutl or 재부팅)하면 거의 대부분의 레코드가 없어지는 것을 확인하였음

- 삭제 전



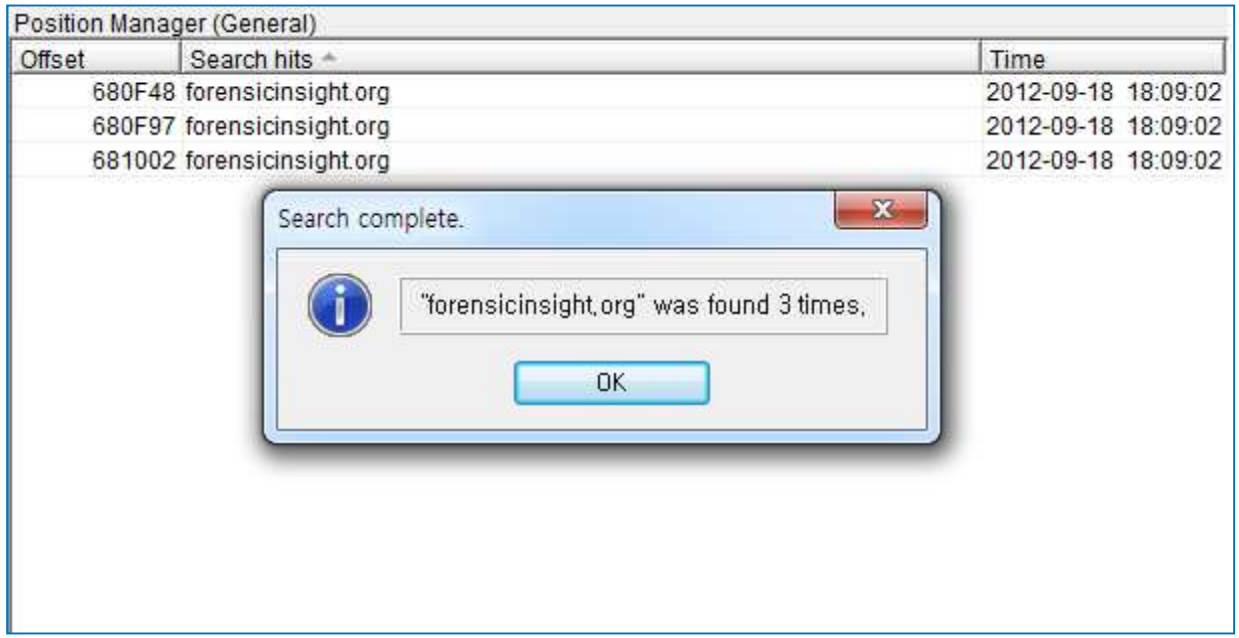
삭제 데이터 복구 가능성 확인

- **복구 가능성 확인**
  - 삭제 후(Dirty Shutdown 상태)



삭제 데이터 복구 가능성 확인

- **복구 가능성 확인**
  - 삭제 후(Clean Shutdown 상태)



  - 따라서, Dirty Shutdown 상태에서 DB 파일을 수집하여 데이터를 파싱, 삭제 레코드 복구하는 방법이 필요함 ~!!!

IE10 Forensics

- 기존 버전과의 차이점
- WebCacheV24.dat ?
- 데이터 수집
- 데이터 분석
- 삭제 데이터 복구 가능성 확인
- **결론**

결론

- IE 10으로 넘어 오면서 로그 저장 방식이 바뀌었음
- 기존 EseDbViewer을 사용한 분석은 한계가 있음
  - 단순 파싱 ➔ Data Type을 고려한 파싱 필요
  - API 사용, Dirty State 상태의 파일에 대한 분석 불가능
- 앞으로의 계획
  - ESE DB 포멧 상세 분석 후, 삭제 레코드 복구 알고리즘 개발
  - IE 10 로그 분석 모듈 개발

질문 및 답변