Web Browser Forensics : Part2

blueangel

blueangel1275@gmail.com

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

개요

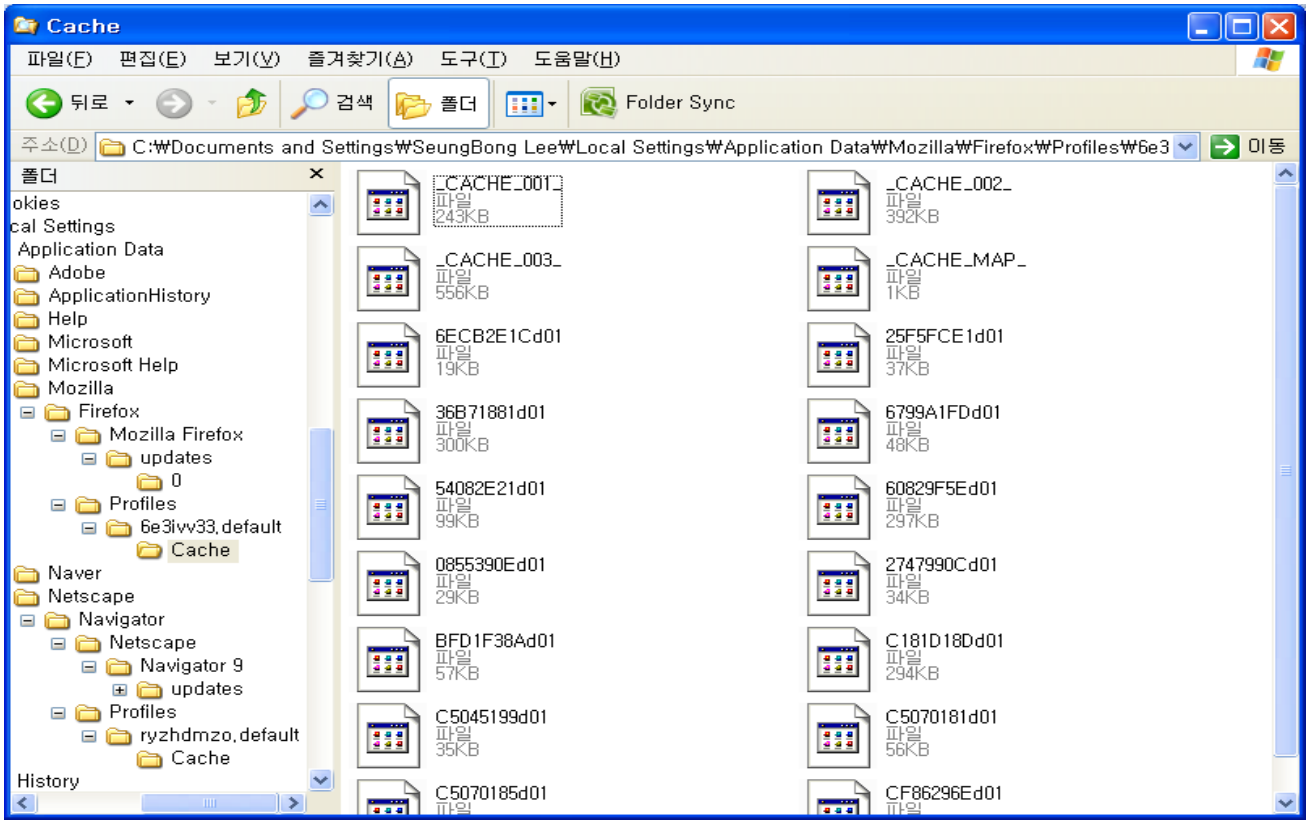
1. Firefox 로그 분석
2. Chrome 로그 분석
3. Safari 로그 분석
4. Opera 로그 분석
5. 분석 도구

Firefox 로그 분석

- **Cache 정보 분석**
- History 정보 분석
- Cookie 정보 분석
- Download 정보 분석

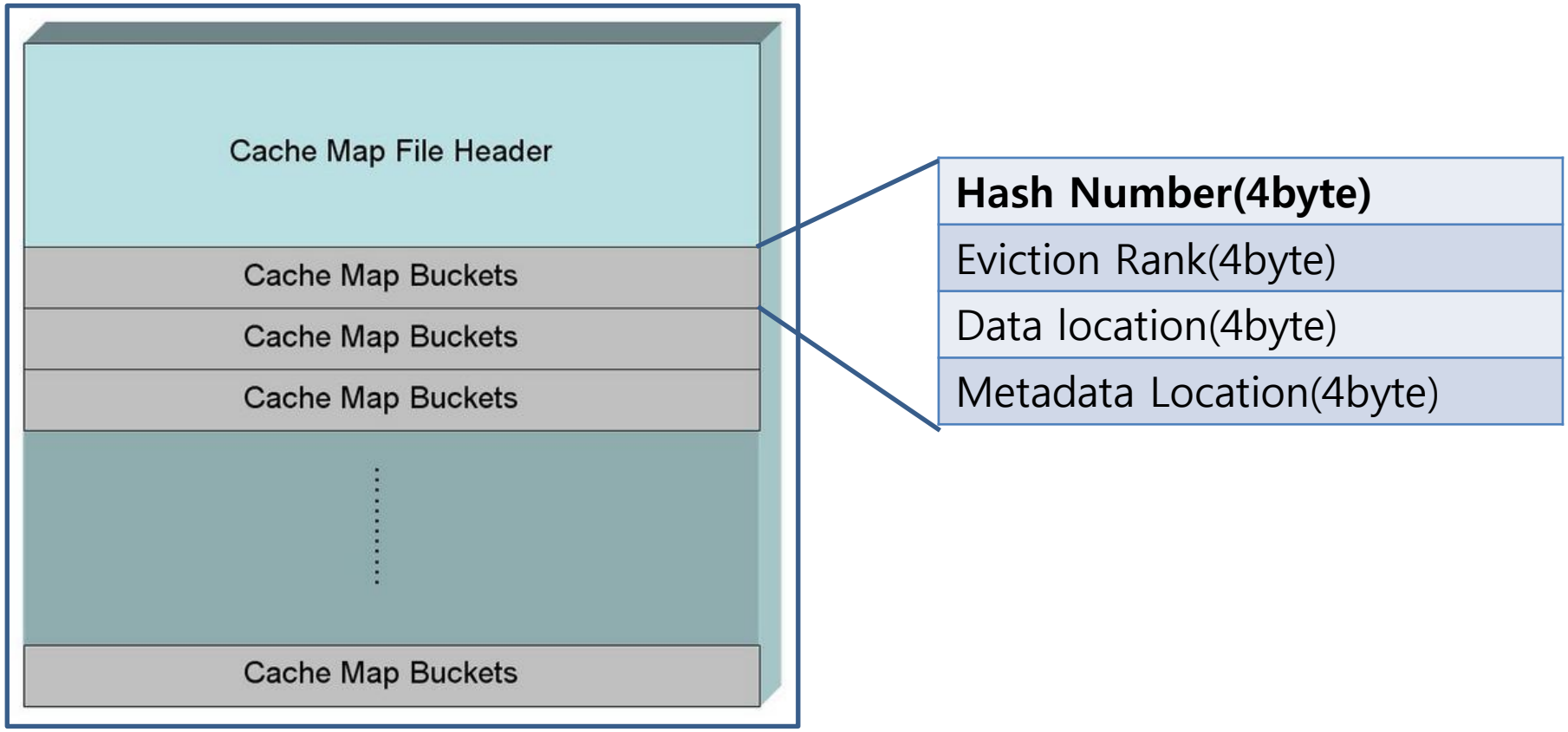
Cache 정보 분석

- **파일 구성**
  - Cache Map File : _CACHE_MAP_
  - Cache Block Files : _CACHE_00X_
  - Separate Cache Data files



Cache 정보 분석

- **Cache Map File 구조**
  - 32개의 Bucket로 이루어짐
  - 한 개의 Bucket은 256개의 Record를 포함 ➔ 총 8,192개의 Record 저장 가능
  - 하나의 Record(16byte)는 Cache 데이터의 맵핑 정보를 담고 있음



Cache 정보 분석

- **Cache Map File Record 구조**
  - Hash Number
    - ✓ Cache 파일의 이름으로 사용
  - Data location, Metadata Location
    - ✓ 최상위 바이트의 하위 3비트 값이 0이면 Separate Cache 파일에 저장 1,2,3이면 Cache Block 파일에 저장
  - Eviction Rank
    - ✓ Unkwon

Cache 정보 분석

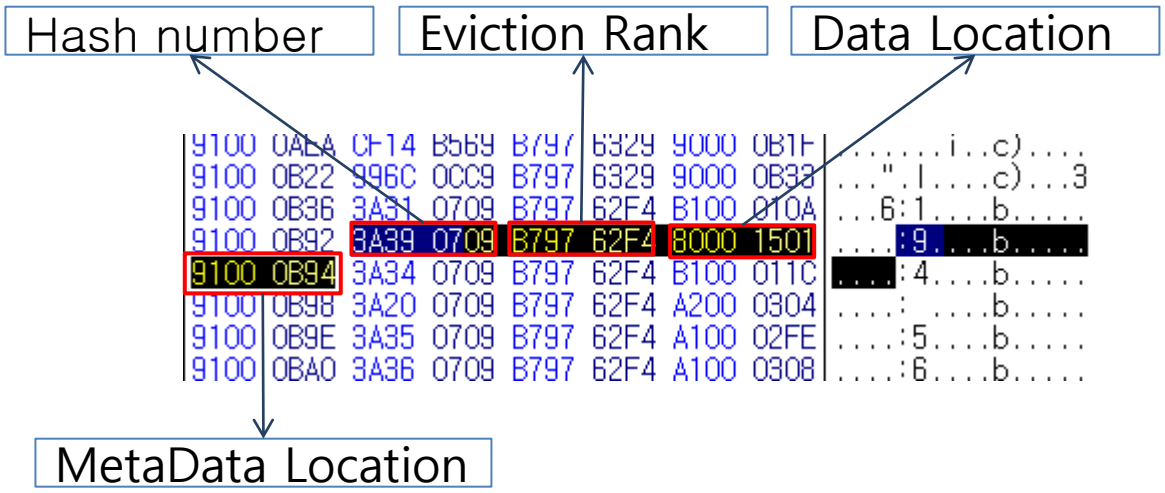
- **Separate Cache Data Files**
  - Cache Content과 Matadata의 크기가 큰 경우 사용
  - Cache Data Files의 이름
    - ✓ <HASH NUMBER><TYPE><GENERATION NUMBER>
    - ✓ HASH NUMBER
      - Cache Map file의 Hash Number
    - ✓ TYPE
      - d: Cache Content
      - m: Cache metadata
    - ✓ GENERATION NUMBER
      - Data location, Metadata Location 최하위 1바이트 값
  - Ex) F1FD0B04d01

Cache 정보 분석

- **Three Cache Block Files**
  - ✓ 데이터의 시작
    - ✓ Data location, Metadata Location의 하위 3바이트 값
  - ✓ 데이터 할당 크기(블록 단위)
    - ✓ ((Data location, Metadata Location) & 0x03000000) >> 24) + 1
  - ✓ 블록 사이즈
    - ✓ Cache Block Files의 파일 이름에 따라 다름
    - ✓ "_CACHE_001_"->256 byte (0x100)
    - ✓ "_CACHE_002_"->512 byte (0x400)
    - ✓ "_CACHE_003"_->1024 byte (0x1000)

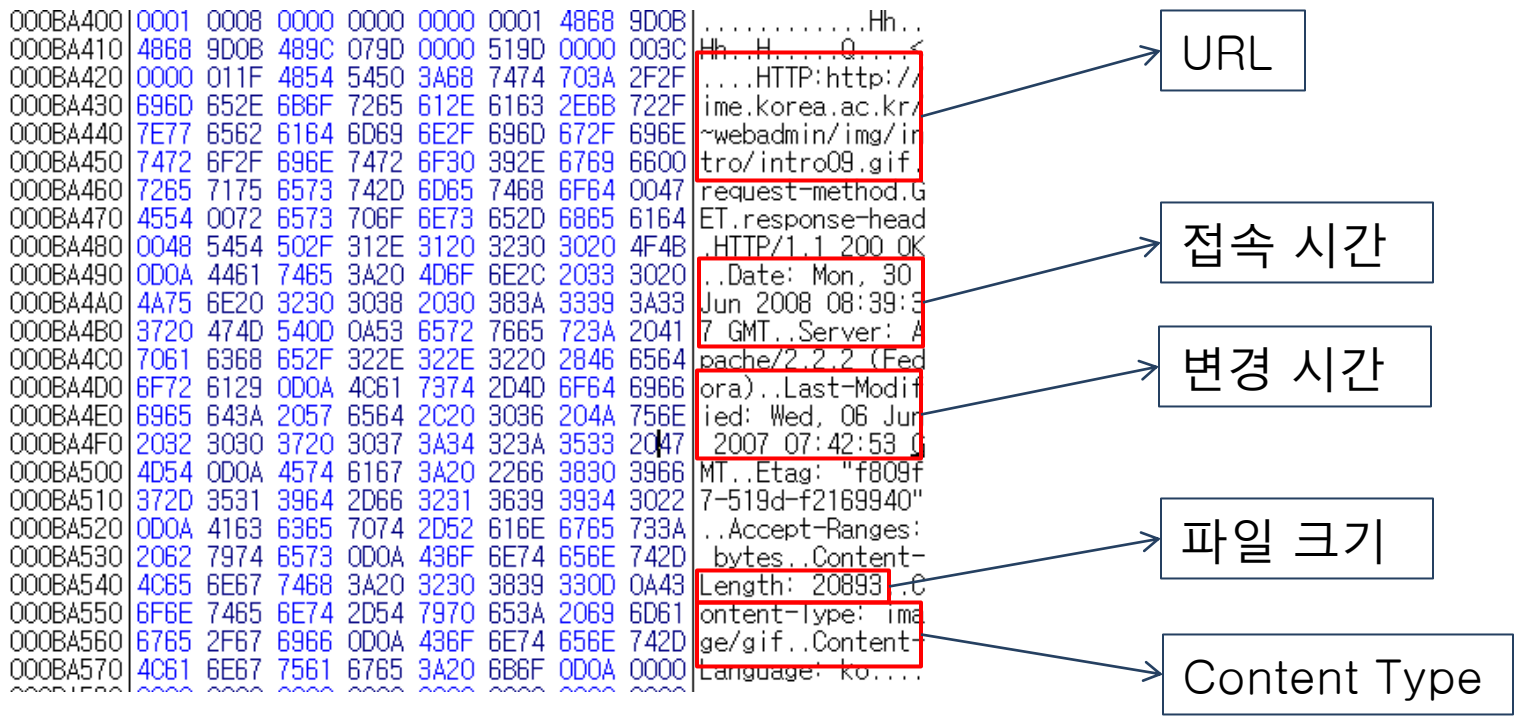
Cache 정보 분석

- **Separate Cache Data Files 내용 확인**
  - Data Location
    - ✓ 8(1000): 하위 2비트의 값이 0이므로 Separate Cache Data File에 저장
    - ✓ 파일 이름: 3A390709d01
  - MetaData Location
    - ✓ 9(1001): 하위 2비트의 값이 1 이므로 _CACHE_001_ 에 저장
    - ✓ offset: 0x000B94*0x100+0x1000 = 0x000BA400



Cache 정보 분석

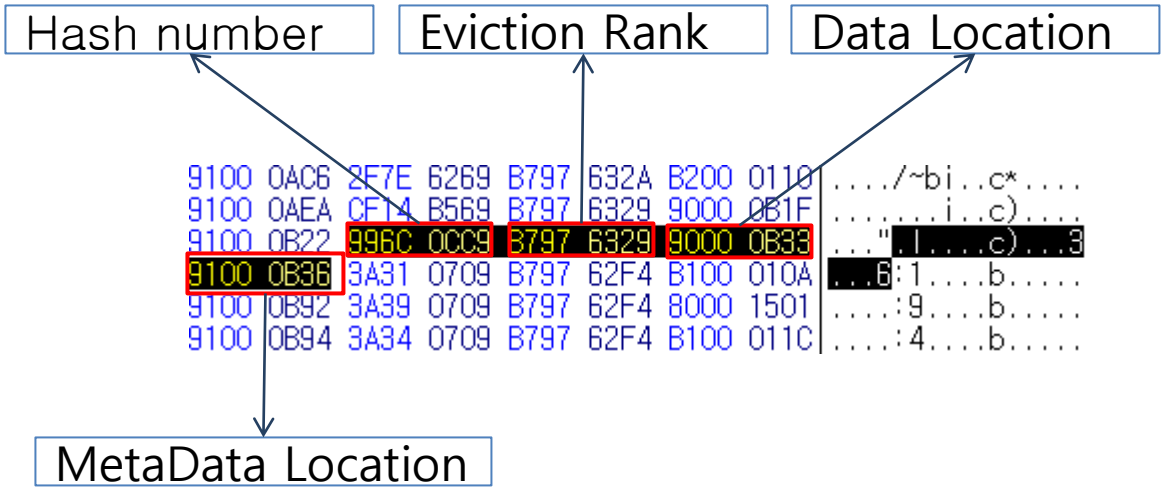
- **Separate Cache Data Files 내용 확인**
  - _CACHE_001_ 파일의 offset 0x000BA400



  - Cache 폴더의 3A390709d01파일의 확장자를 gif 로 변경하면 내용 확인 가능

Cache 정보 분석

- **Three Cache Block File 내용 확인**
  - Data Location
    - ✓ 9(1001): 하위 2비트의 값이 1이므로 _CACHE_001_ 에 저장
    - ✓ offset: 0x000B33*0x100+0x1000 = 0x000B4300
  - MetaData Location
    - ✓ 9(1001): 하위 2비트의 값이 1 이므로 _CACHE_001_ 에 저장
    - ✓ offset: 0x000B36*0x100+0x1000 = 0x000B4600



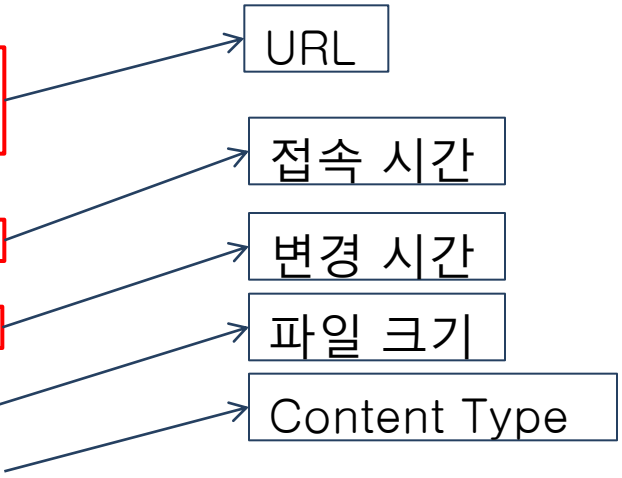
Cache 정보 분석

- **Three Cache Block File 내용 확인**
  - Content Data

```
000B4300|4749 4638 3961 2100 0A00 8001 009F 9F9F|GIF89a!.........
000B4310|FFFF FF21 F904 0100 0001 002C 0000 0000|...!.........,....
000B4320|2100 0A00 0002 2C8C 8FA9 CBED 6FC0 9132|!.....,.....o..2
000B4330|5040 A3C5 B122 0E6A 5637 7A95 A765 DB99|P@...".jV7z..e..
000B4340|5E2A 3A8A 225B 4EB2 7CE6 6F4C 42FE 0F0C|^*:."[N.|.oLB...
000B4350|0A81 0500 3B22 2073 7479 6C65 3D63 7572|....;" style=cur
000B4360|736F 723A 6861 6E64 3EBC D5BC B1BF B53C|sor:hand>......<
000B4370|2F73 7061 6E3E 3C2F 6469 763E 3C2F 7464|/span></div></td
000B4380|3E0A 2020 3C74 6420 7769 6474 683D 3730|>.  <td width=70
000B4390|2063 6C61 7373 3D72 5F73 5F66 6F6E 743E| class=r_s_font>
000B43A0|3C73 7061 6E20 7469 746C 653D 2732 3030|<span title='200
000B43B0|38B3 E220 3036 BFF9 2030 39C0 CF20 3133|8.. 06.. 09.. 13
000B43C0|BDC3 2033 33BA D020 3234 C3CA 273E 3230|.. 33.. 24..'>20
000B43D0|3038 2F30 362F 3039 3C2F 7370 616E 3E3C|08/06/09</span><
000B43E0|2F74 643E 0A20 203C 7464 2077 6964 7468|/td>.  <td width
000B43F0|3D34 3020 636C 6173 733D 725F 735F 666F|=40 class=r_s_fo
000B4400|0001 0008 0000 0000 0000 0001 4868 9CD5|............Hh..
000B4410|4868 9CD6 0000 0000 0000 A8D5 0000 003D|Hh.............=
```

  - Content Metadata

```
000B4600|0001 0008 0000 0000 0000 0001 4868 9CD5|............Hh..
000B4610|4868 9CD6 48A0 04D0 0000 0055 0000 004B|Hh..H......U...K
000B4620|0000 00F4 4854 5450 3A68 7474 703A 2F2F|....HTTP:http://
000B4630|6369 7374 2E6B 6F72 6561 2E61 632E 6B72|cist.korea.ac.kr
000B4640|2F7A 626F 6172 642F 736B 696E 2F50 726F|/zboard/skin/Pro
000B4650|5F62 5F76 3035 2F69 6D61 6765 732F 7365|_b_v05/images/se
000B4660|7475 705F 6D79 696E 666F 2E67 6966 0072|tup_myinfo.gif.r
000B4670|6571 7565 7374 2D6D 6574 686F 6400 4745|equest-method.GE
000B4680|5400 7265 7370 6F6E 7365 2D68 6561 6400|T.response-head.
000B4690|4854 5450 2F31 2E31 2032 3030 204F 4B0D|HTTP/1.1 200 OK.
000B46A0|0A44 6174 653A 204D 6F6E 2C20 3330 204A|.Date: Mon, 30 J
000B46B0|756E 2032 3030 3820 3038 3A34 343A 3038|un 2008 08:44:08
000B46C0|2047 4D54 0D0A 5365 7276 6572 3A20 4170| GMT..Server: Ap
000B46D0|6163 6865 0D0A 4C61 7374 2D4D 6F64 6966|ache..Last-Modif
000B46E0|6965 643A 204D 6F6E 2C20 3037 204D 6179|ied: Mon, 07 May
000B46F0|2032 3030 3720 3032 3A32 303A 3530 2047| 2007 02:20:50 G
000B4700|4D54 0D0A 4574 6167 3A20 2232 3335 6562|MT..Etag: "235eb
000B4710|2D35 352D 6633 3162 6334 3830 220D 0A41|-55-f31bc480"..A
000B4720|6363 6570 742D 5261 6E67 6573 3A20 6279|ccept-Ranges: by
000B4730|7465 730D 0A43 6F6E 7465 6E74 2D4C 656E|tes..Content-Len
000B4740|6774 683A 2038 350D 0A43 6F6E 7465 6E74|gth: 85..Content
000B4750|2D54 7970 653A 2069 6D61 6765 2F67 6966|-Type: image/gif
```



Cache 정보 분석

- **데이터 크기**
  - Data의 크기가 85 바이트 ➔ Content Data의 85 바이트를 setup_myinfo.gif로 저장

```
4749 4638 3961 2100 0A00 8001 009F 9F9F | GIF89a!.........
FFFF FF21 F904 0100 0001 002C 0000 0000 | ...!.........,....
2100 0A00 0002 2C8C 8FA9 CBED 6FC0 9132 | !.....,.....o..2
5040 A3C5 B122 0E6A 5637 7A95 A765 DB99 | P@...".jV7z..e..
5E2A 3A8A 225B 4EB2 7CE6 6F4C 42FE 0F0C | ^*:."[N.|.oLB...
0A81 0500 3B22 2073 7479 6C65 3D63 7572 | ....;" style=cur
736F 723A 6861 6E64 3EBC D5BC B1BF B53C | sor:hand>......<
2F73 7061 6E3E 3C2F 6469 763E 3C2F 7464 | /span></div></td
3E0A 2020 3C74 6420 7769 6474 683D 3730 | >.  <td width=70
2063 6C61 7373 3D72 5F73 5F66 6F6E 743E |  class=r_s_font>
3C73 7061 6E20 7469 746C 653D 2732 3030 | <span title='200
3833 E220 3036 BFF9 2030 39C0 CF20 3133 | 8.. 06.. 09.. 13
BDC3 2033 33BA D020 3234 C3CA 273E 3230 | .. 33.. 24..'>20
3038 2F30 362F 3039 3C2F 7370 616E 3E3C | 08/06/09</span><
2F74 643E 0A20 203C 7464 2077 6964 7468 | /td>.  <td width
3D34 3020 636C 6173 733D 725F 735F 666F | =40 class=r_s_fo
```

Firefox 로그 분석

- Cache 정보 분석
- **History 정보 분석**
- Cookie 정보 분석
- Download 정보 분석

History 정보 분석

- **로그 파일명 : places.sqlite**

- **파일 형식**
  - SQLite 데이터베이스 파일 형식

- **주요 테이블**
  - moz_places : 방문한 URL 정보 저장
  - moz_historyvisits : 실제 방문 기록 저장, place_id 값을 통해 moz_place의 url 참조

- **저장 정보**
  - URL
  - Title
  - 방문 횟수
  - 방문 타입(1 : URL 타이핑 접속, 0 : 링크 접속)
  - 방문 시간(1970년 1월 1일 00:00:00 기준 경과된 마이크로초)

History 정보 분석

- **moz_places, moz_historyvisits 테이블 구조**

Table: moz_places

	id	url	title	rev_host	visit_count	hidden	typed	favicon_id	frecency	last_visit_date
1	36	http://www.nave	네이버 :: 나의 경	moc.revan.www.	1	0	1	11	2023	1287064165281000
2	63	http://portal.kore	고려대학교 지식기	rk.ca.aerok.latrop	0	0	0		140	
3	84	http://163.152.165	Home - Phaser E	031.561.251.361.	1	0	0		140	1284014112000000
4	137	http://www.goog	Google	rk.oc.elgoog.ww	1	0	1	6	2023	1287064152875000
5	145	http://banking.sh	::::: 신한간편서비	moc.nahnihs.gni	1	0	0		140	1284346760000000
6	176	http://www.wedi	▒ 컨텐츠와 함께	rk.oc.ksidew.ww	0	0	0		140	
7	237	http://www.andr	http://www.andr	moc.bupdiordna.	1	0	0		140	1284109722000000
8	305	http://devian.tist	Devian's Life Sto	moc.yrotsit.naive	1	0	0		140	1284126640000000

Table: moz_historyvisits

	id	from_visit	place_id	visit_date	visit_type	session
1	1	0	1774	1287454082265000	1	2
2	2	1	1775	1287454078812000	5	2
3	3	2	1776	1287454078937000	6	2
4	4	3	2011	1287454086765000	1	2
5	5	4	2012	1287454086765000	1	2
6	6	0	36	1287454090859000	3	3
7	13	6	2013	1287454095921000	1	3
8	16	6	2015	1287454112500000	1	3
9	18	6	2017	1287454121234000	1	3
10	19	18	2018	1287454117656000	6	3

Firefox 로그 분석

- Cache 정보 분석
- History 정보 분석
- **Cookie 정보 분석**
- Download 정보 분석

Cookie 정보 분석

- **로그 파일명 : cookies.sqlite**

- **파일 형식**
  - SQLite 데이터베이스 파일 형식

- **주요 테이블**
  - moz_cookies : 쿠키 데이터 저장

- **저장 정보**
  - 호스트, 경로
  - 변수, 값
  - 방문 횟수
  - 마지막 접근 시간(1970년 1월 1일 00:00:00 기준 경과된 마이크로초)
  - 쿠키 만료 시간(1970년 1월 1일 00:00:00 기준 경과된 마이크로초)
  - isSecure, isHttpOnly

Cookie 정보 분석

- **moz_cookies 테이블 구조**

RecNo	id	host	path	name	value	lastAccessed	expiry	isSecure	isHttpOnly
					Click here to define a filter				
1	3	.babylon.com	/	mntrID	8000013d000000000000002215 3fcd50	1309770611406000	1325000668	0	0
2	4	.babylon.com	/	visitorID	1309448665-4070731090	1309770611406000	1325000668	0	0
3	6	.babylon.com	/	firstsearchweek	26	1309770611406000	1609372803	0	0
4	7	widgets.montiera.com	/widgets/	gck	{"cy":"KR","ct":"Seoul","cn":" Korea, Republic of","lt":"37.6","lng":"127.0"}	1309448668812000	1309621469	0	0
5	10	.yahoo.com	/	B	02gmtpp70p6eq&b=3&s=6c	1309770612046000	1372622403	0	0
6	17	.babylon.com	/	__utmz	1.1309448670.1.1.utmcsr=(dir ect)|utmccn=(direct)|utmcm d=(none)	1309770611406000	1325216670	0	0
7	26	.google.co.kr	/	PREF	ID=8f753354b4def038:U=dd7f1 3bab4b17655:FF=0:NW=1:TM =1309448676:LM=1309448688: S=XCkRVPunyVcYuM73	1309770618703000	1372520692	0	0
8	27	.mozilla.com	/	SSID	AwCeDikAAAQA8pkMTvLpA gHymQxOAQAAAAAAAAAA AAAAAADymQxOAAAM_v__ AAAAAABhAAAA	1309770617187000	1340984695	0	0
9	28	.mozilla.com	/	SSRT	8pkMTgE	1309770617187000	1340984695	0	0
10	30	.mozilla.com	/	wtspl	972133	1309770617187000	1312040697	0	0
11	32	.google.co.kr	/verify	SNID	48=op98kZzGOf4GWzyoO7bj Ysto-Ncw7MuKwEthRHuM2 w=jn3N4CS6orDrOGDL	1309448817796000	1325259898	0	1

Firefox 로그 분석

- Cache 정보 분석
- History 정보 분석
- Cookie 정보 분석
- **Download 정보 분석**

Download 정보 분석

- **로그 파일명 : downloads.sqlite**
- **파일 형식**
  - SQLite 데이터베이스 파일 형식
- **주요 테이블**
  - moz_downloads : 쿠키 데이터 저장
- **저장 정보**
  - 소스 URL
  - 다운받은 Local 경로
  - 다운로드 시간(1970년 1월 1일 00:00:00 기준 경과된 마이크로초) : 시작/ 종료시간
  - 다운로드 받은 크기, 총 다운로드 크기

Download 정보 분석

- **moz_downloads 테이블 구조**

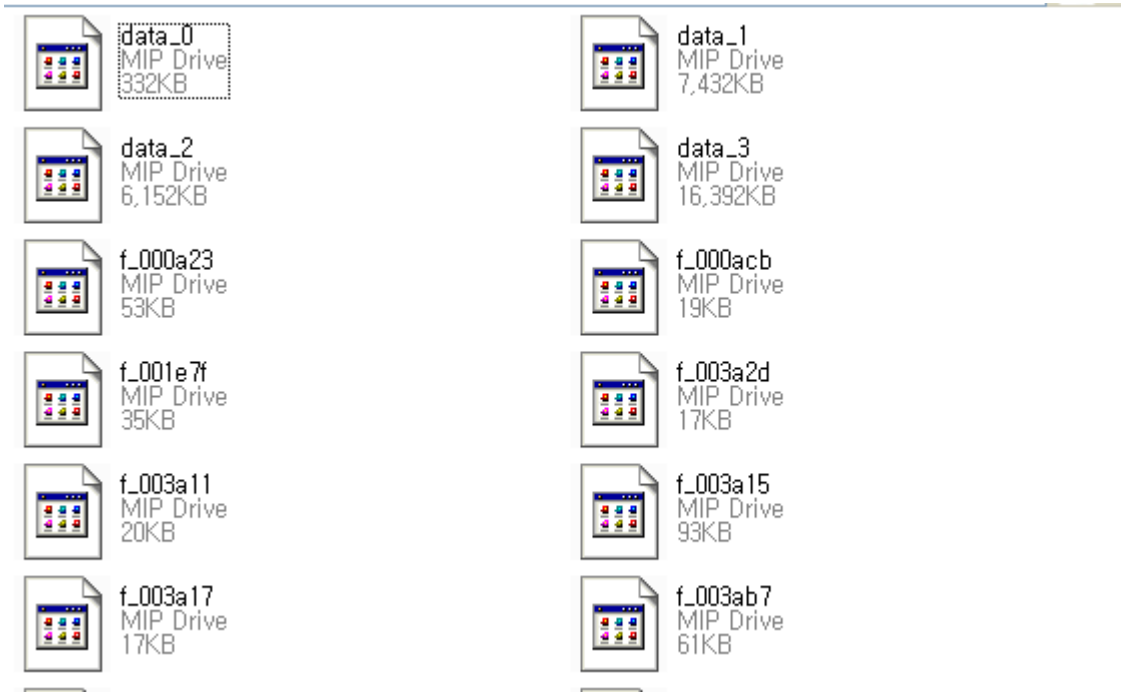
RecNo	id	name	source	target	startTime	endTime	currBytes	maxBy...
Click here to define a filter								
1	1	url.htm	http://www.google.co.kr/url?sa=t&source=web&cd=3&ved=0CEgQFjAC&url=http%3A%2F%2Fdigitalforensicssolutions.com%2Fpapers%2Fandroid-memory-analysis.pdf&rct=j&q=android%20memory%20forensic&ei=a5oMTtWmJeSfmQWEqvWZDg&usg=AFQjCNEMFr37Ej_GYQzehrNZt7naZFTLRQ&cad=rjt	file:///C:/Documents%20and%20Settings/ojh/%EB%B0%94%ED%83%95%20%ED%99%94%EB%A9%B4/url.htm	1309448866796000	1309448869796000	435	435
2	2	DigitalSignage_WizRED.pptx	http://www.wizsolution.net/support/document/DigitalSignage_WizRED.pptx	file:///C:/Documents%20and%20Settings/ojh/My%20Documents/Downloads/DigitalSignage_WizRED.pptx	1309798100062000	1309798107578000	5819896	5819896
3	3	8.pptx	http://www.intermass.com/ptx/8.pptx	file:///C:/Documents%20and%20Settings/ojh/My%20Documents/Downloads/8.pptx	1309798108250000	1309798110171000	758297	758297
4	4	Digital Citizenship Presentation .pptx	http://educationaljargonschs.wikispaces.com/file/view/Digital+Citizenship+Presentation+.pptx	file:///C:/Documents%20and%20Settings/ojh/My%20Documents/Downloads/Digital%20Citizenship%20Presentation%20.pptx	1309798109828000	1309798132765000	6826006	6826006
5	5	Digital Graphics II Year at a Glance.pptx	http://bhs.bisdtx.org/Documents/Olson/Handouts/Digital%20Graphics%20II%20Year%20at%20a%20Glance.pptx	file:///C:/Documents%20and%20Settings/ojh/My%20Documents/Downloads/Digital%20Graphics%20II%20Year%20at%20a%20Glance.pptx	1309798180578000	1309798184390000	96522	96522
6	6	0_0_7388046_1255916966662.pptx	http://www.krta.or.kr/~knrta/package/multiboard/data/mbdata/0_0_7388046_1255916966662.pptx	file:///C:/Documents%20and%20Settings/ojh/My%20Documents/Downloads/0_0_7388046_1255916966662.pptx	1309798216640000	1309798219750000	7388046	7388046

Chrome 로그 분석

- **Cache 정보 분석**
- History 정보 분석
- Cookie 정보 분석
- Download 정보 분석

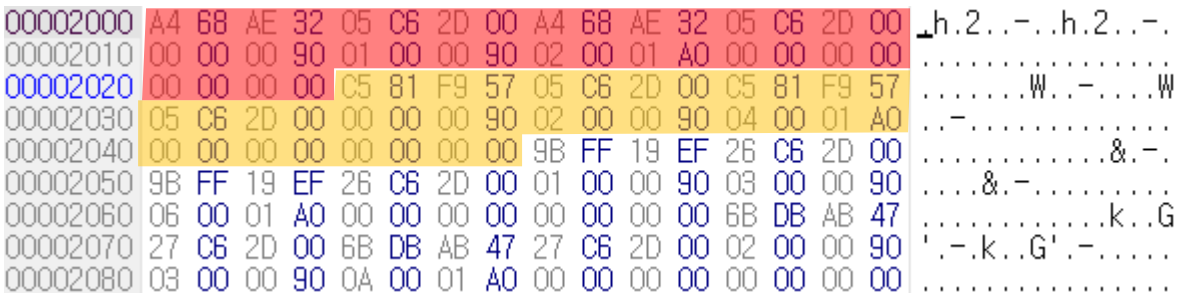
Cache 정보 분석

- **전체 파일 구성**
  - data_0, data_1, data_2, data_3, 데이터 파일



Cache 정보 분석

- **파일 구성**
  - data_0
    - ✓ 인덱스 레코드가 저장됨(URL 레코드의 위치 정보 저장)
    - ✓ 오프셋 0x2000 부터 0x24 바이트 단위로 저장



  - data_1, data_2, data_3
    - ✓ URL(URL 레코드에 저장됨), 메타데이터, Cache 데이터 저장
    - ✓ 오프셋 0x2000 부터 블록 단위로 저장
    - ✓ 블록 단위
      - data_1: 0x100
      - data_2: 0x400
      - data_3: 0x1000

Cache 정보 분석

- **data_0 에서의 인덱스 레코드 구조**

HEX	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00																
10									URL 레코드 위치 정보							
20																

  - 최초 2 바이트
    - ✓ 블록의 인덱스
    - ✓ 0x0001이면 두 번째 블록에 URL레코드가 저장 되어 있음
  - 3번째 바이트
    - ✓ 파일의 인덱스
    - ✓ 0x01이면 data_1 파일에 URL 레코드가 저장 되어 있음
  - URL 레코드 위치
    - ✓ 블록 인덱스 * 블록의 단위 + 0x2000

Cache 정보 분석

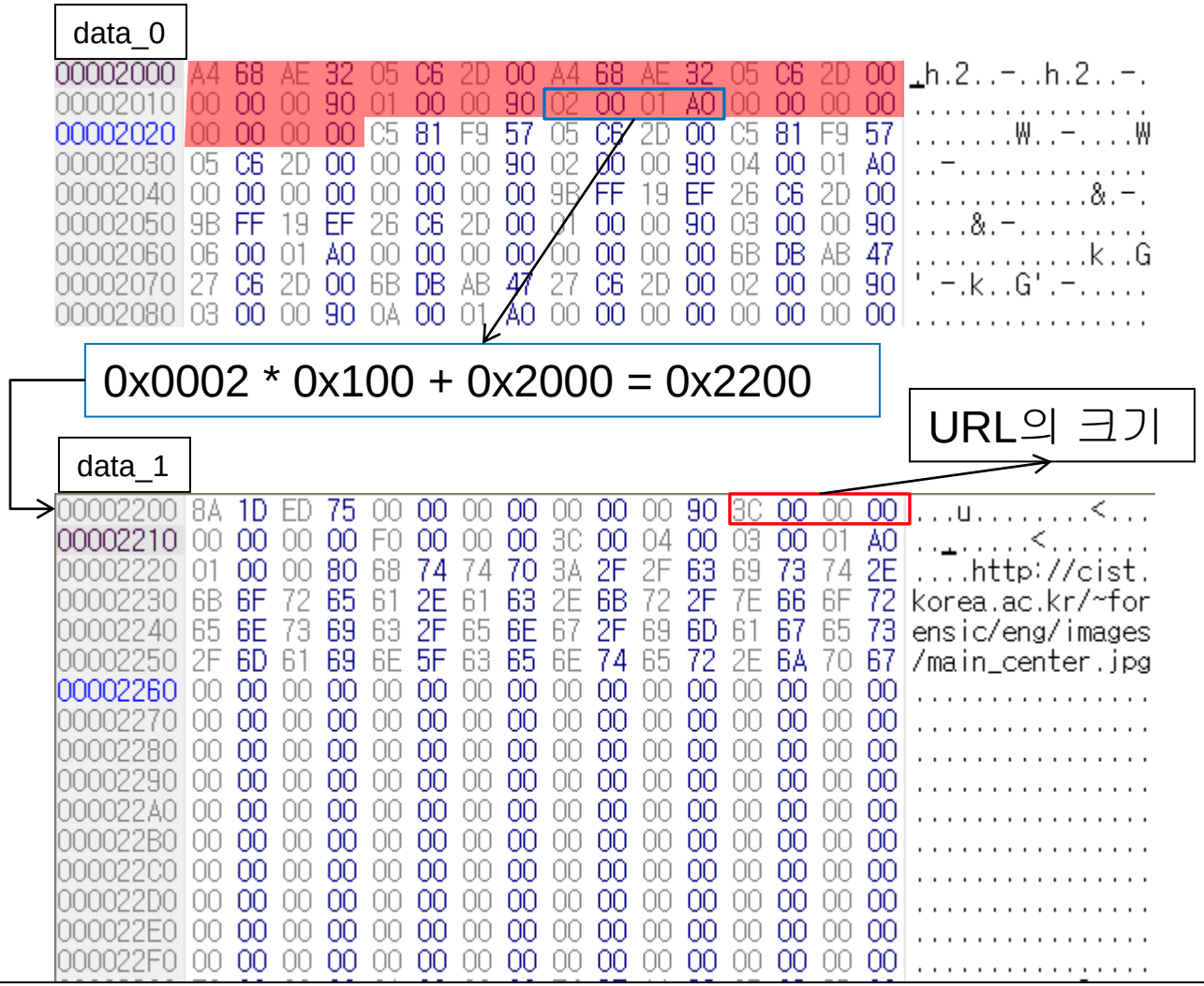
- **data_n(n=1, 2, 3) 에서의 URL 레코드 구조**

<table>
<tr><td>HEX</td><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>0A</td><td>0B</td><td>0C</td><td>0D</td><td>0E</td><td>0F</td></tr>
<tr><td>00</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4">URL의 크기</td></tr>
<tr><td>10</td><td></td><td></td><td></td><td></td><td colspan="4">메타데이터의 크기</td><td colspan="4">데이터의 크기</td><td colspan="4">메타데이터의 위치 및 이름</td></tr>
<tr><td>20</td><td colspan="4">데이터의 위치 및 이름</td><td>URL의 시작 위치</td></tr>
</table>

- (메타)데이터의 위치 및 이름
  - ✓ 4번째 바이트에 따라 저장 위치 결정
    - 0x80이면 별도의 파일로 저장 나머지 3바이트가 파일의 이름
    - 0x80이 아니면 "URL 레코드 위치"와 같은 방식으로 계산

Cache 정보 분석

- **Cache 피일 내용 확인 1 : data_0의 인덱스 레코드에서 URL 레코드 위치를 참조**



Cache 정보 분석

- **Cache 피일 내용 확인 2 : data_1의 URL 레코드에서 메타데이터의 위치를 참조**

메타데이터의 위치:data_1
0x0003 * 0x 100 + 0x2000 = 0x2300

메타데이터의 크기

data_1

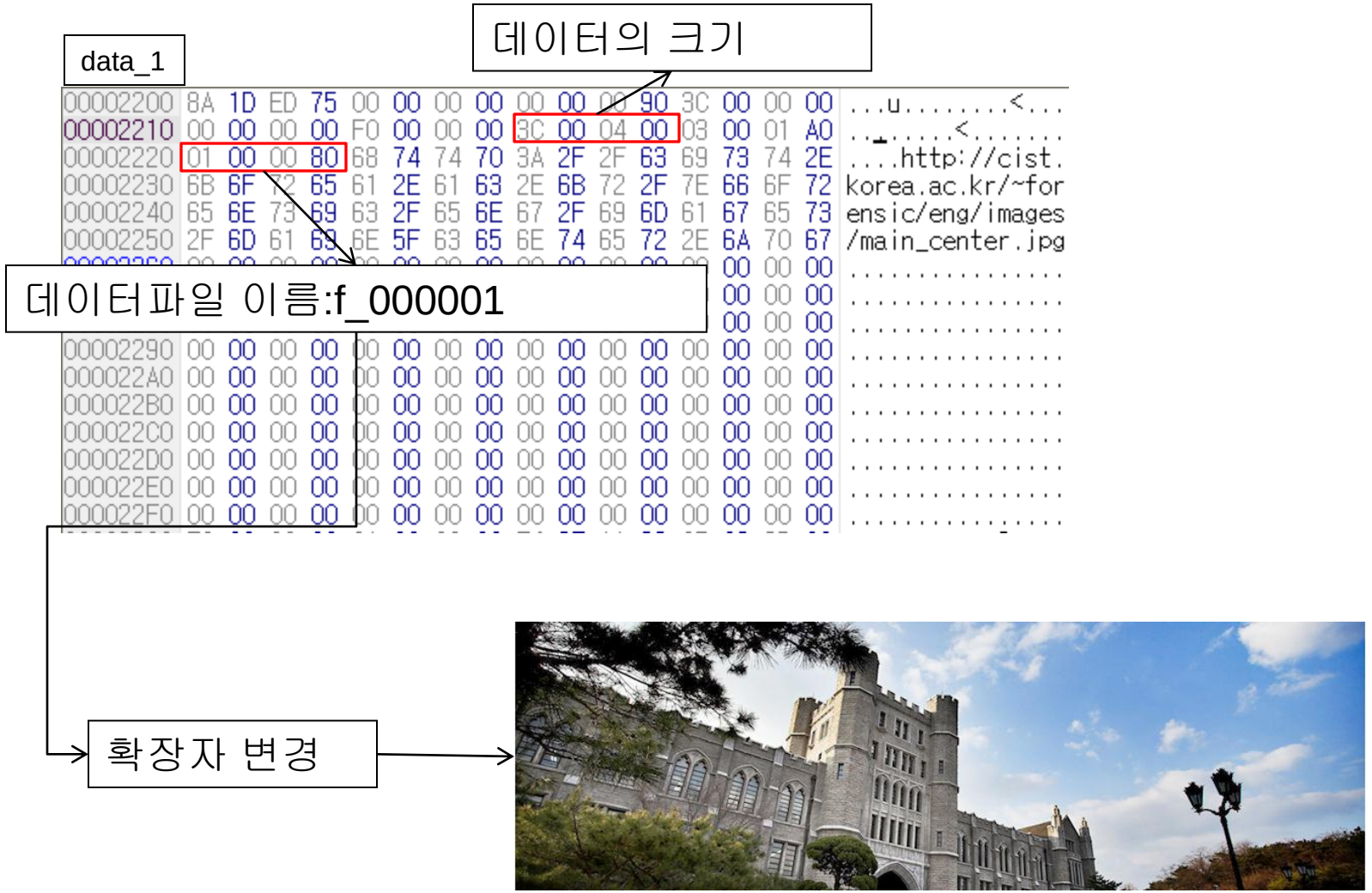
```
00002200 8A 1D ED 75 00 00 00 00 00 00 00 90 3C 00 00 00 ...u........<...
00002210 00 00 00 00 F0 00 00 00 3C 00 04 00 03 00 01 A0 ........<.......
00002220 01 00 00 80 68 74 74 70 3A 2F 2F 63 69 73 74 2E ....http://cist.
00002230 6B 6F 72 65 61 2E 61 63 2E 6B 72 2F 7E 66 6F 72 korea.ac.kr/~for
00002240 65 6E 73 69 63 2F 65 6E 67 2F 69 6D 61 67 65 73 ensic/eng/images
00002250 2F 6D 61 69 6E 5F 63 65 6E 74 65 72 2E 6A 70 67 /main_center.jpg
00002260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00002270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00002280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00002290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000022A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000022B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000022C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000022D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000022E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000022F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

data_1

```
00002300 EC 00 00 00 01 00 00 00 E4 9F AA 32 05 C6 2D 00 ...........2..-.
00002310 1C EA AA 32 05 C6 2D 00 D4 00 00 00 48 54 54 50 ...2..-.....HTTP
00002320 2F 31 2E 31 20 32 30 30 20 4F 4B 00 44 61 74 65 /1.1 200 OK.Date
00002330 3A 20 4D 6F 6E 2C 20 31 33 20 41 70 72 20 32 30 : Mon, 13 Apr 20
00002340 30 39 20 31 32 3A 33 32 3A 35 37 20 47 4D 54 00 09 12:32:57 GMT.
00002350 53 65 72 76 65 72 3A 20 41 70 61 63 68 65 00 4C Server: Apache.L
00002360 61 73 74 2D 4D 6F 64 69 66 69 65 64 3A 20 54 68 ast-Modified: Th
00002370 75 2C 20 30 35 20 4A 75 6E 20 32 30 30 38 20 30 u, 05 Jun 2008 0
00002380 38 3A 35 35 3A 32 31 20 47 4D 54 00 45 54 61 67 8:55:21 GMT.ETag
00002390 3A 20 22 37 33 34 61 36 65 2D 34 30 30 33 63 2D : "734a6e-4003c-
000023A0 38 31 35 33 62 30 34 30 22 00 41 63 63 65 70 74 8153b040".Accept
000023B0 2D 52 61 6E 67 65 73 3A 20 62 79 74 65 73 00 43 -Ranges: bytes.C
000023C0 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 32 ontent-Length: 2
000023D0 36 32 32 30 34 00 43 6F 6E 74 65 6E 74 2D 54 79 62204.Content-Ty
000023E0 70 65 3A 20 69 6D 61 67 65 2F 6A 70 65 67 00 00 pe: image/jpeg..
```

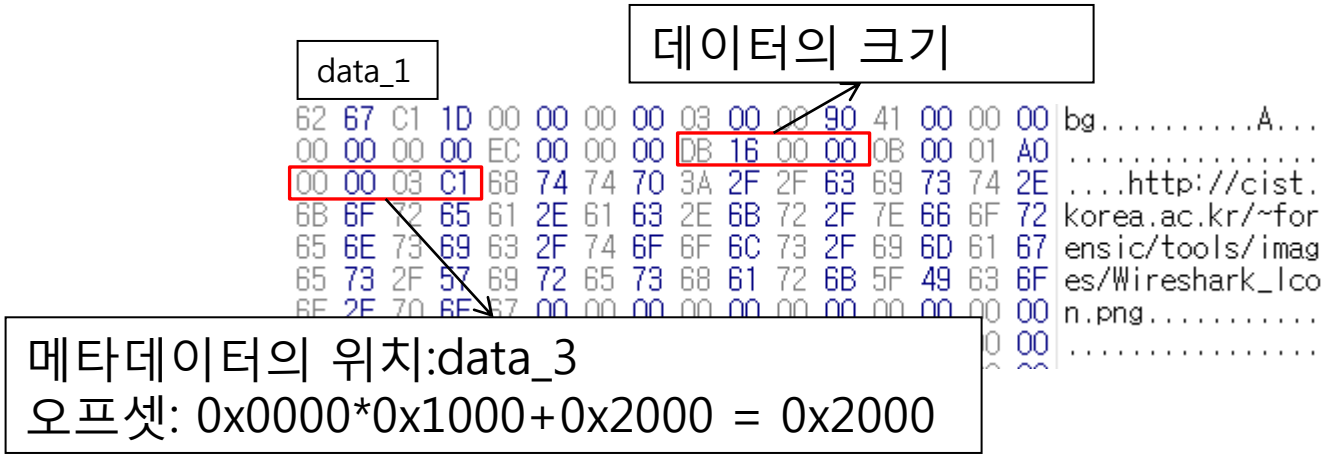
Cache 정보 분석

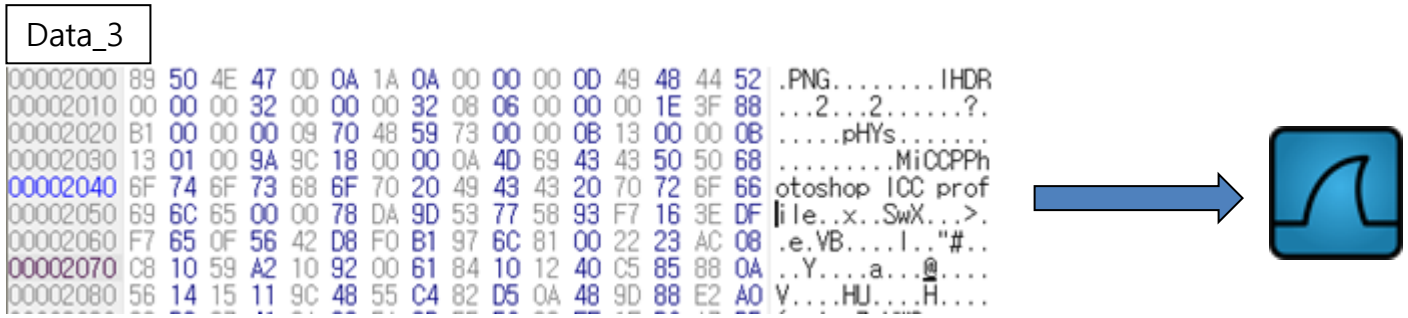
- **Cache 피일 내용 확인 3 : data_1의 URL 레코드에서 데이터의 위치를 참조**



Cache 정보 분석

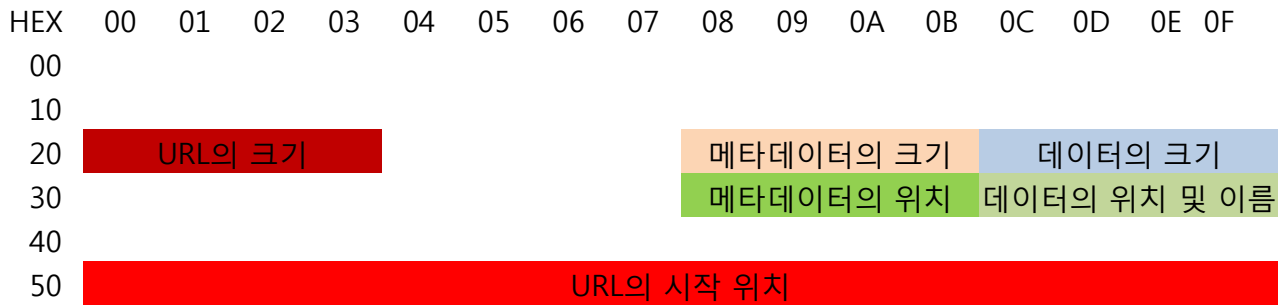
- **Cache 데이터가 Cache 파일(data_n) 안에 있는 경우**





Cache 정보 분석

- **최신 버전의 URL 레코드 구조**



- (메타)데이터의 위치 및 이름 계산 방식은 기존과 동일

Chrome 로그 분석

- Cache 정보 분석
- **History 정보 분석**
- Cookie 정보 분석
- Download 정보 분석

History 정보 분석

- **로그 파일명 : History**
- **파일 형식 : SQLite 데이터베이스 파일 형식**
- **주요 테이블**
  - urls 테이블
    - ✓ 방문한 url 정보 저장, 같은 url은 중복 저장 안 됨, 중복 방문 시 마지막 접속 시간 저장
  - visits 테이블
    - ✓ 실제 방문 정보 저장, 실제 방문 시 저장되는 url정보는 urls 테이블에서 참조
- **저장 정보**
  - URL
  - Title
  - 방문 횟수
  - 방문 타입(1 : URL 타이핑 접속, 0 : 링크 접속)
  - 방문 시간(1601년 1월 1일 00:00:00 기준 경과된 마이크로초)

History 정보 분석

- urls, visits 테이블 구조

Table: urls

	id	url	title	visit_count	typed_count	last_visit_time	hidden	favicon_id
1	1	http://www.google.com/	Google	5	0	12931895744090375	0	1
2	2	http://www.google.co.kr/	Google	5	0	12931895744090375	0	1
3	3	http://www.google.co.kr/blank.htm		5	0	12931895744159375	1	0
4	4	http://www.fomos.co.kr/	::::: Enjoy e-sports 포모스 :	1	1	12931895538815500	0	0
5	5	http://www.fomos.co.kr/main/mai		1	0	12931895538966500	1	0

Table: visits

	id	url	visit_time	from_visit	transition	segment_id	is_indexed
1	1	1	12931206565455500	0	268435462	0	0
2	2	2	12931206565455500	1	2684354566	0	0
3	3	3	12931206565523500	0	805306371	0	0
4	4	1	12931207255470625	0	268435462	0	0
5	5	2	12931207255470625	4	2684354566	0	0

Chrome 로그 분석

- Cache 정보 분석
- History 정보 분석
- **Cookie 정보 분석**
- Download 정보 분석

Cookie 정보 분석

- **로그 파일명 : Cookies**
- **파일 형식 : SQLite 데이터베이스 파일 형식**
- **주요 테이블 : cookies 테이블**
- **저장 정보**
  - 호스트, 경로
  - 변수, 값
  - 방문 횟수
  - 마지막 접근 시간(1601년 1월 1일 00:00:00 기준 경과된 마이크로초)
  - 쿠키 만료 시간(1601년 1월 1일 00:00:00 기준 경과된 마이크로초)
  - isSecure, isHttpOnly

Cookie 정보 분석

- cookies 테이블 구조

RecNo	host_key	path	name	value	last_access_utc	expires_utc	secure	httponly	creation_utc
Click here to define a filter									
1	.google.co.kr	/	PREF	ID=14641acd53608662:U=d07e3e034083a9e1:FF=0:NW=1:TM=1309447993:LM=1309448348:S=n_jiDALwE-GQFIFj	12954223509168000	13016993948000000	0	0	12953921950596500
2	.softonic.com	/	blang	en_US	12953922221420001	12985458218000000	0	0	12953922221420001
3	.softonic.com	/	country	KR	12953922221420002	12985458218000000	0	0	12953922221420002
4	.softonic.com	/	ucountry	AS	12953922221420003	12985458218000000	0	0	12953922221420003
5	.softonic.com	/	sads_country	KR	12953922221420004	12985458218000000	0	0	12953922221420004
6	.softonic.com	/	entry	http%3A%2F%2Fwww.google.co.kr%2Furl%3Fsa%3Dt%26amp%3Bsource%3Dweb%26amp%3Bcd%3D1%26amp%3Bved%3D0CDgQFjAA%26amp%3Burl%3Dhttp%253A%252F%252Fen.softonic.com%252Fs%252Finternet-explorer-10%26amp%3Brct%3Dj%26amp%3Bq%3Dinternet%2520explorer%252010%26amp%3Bei%3DoZkMTsaSNMfymAXr1LC1Dg%26amp%3Busg%3DAFQjCNF_IF3P9eHzkKiyG3dZa01anNcI	12953922221420005	12985458218000000	0	0	12953922221420005
7	.softonic.com	/	__qca	P0-2118391335-1309448624193	12953922224189000	13791859200000000	0	0	12953922224189000
8	.quantserve.com	/	mc	4e0c99ad-d4370-4abde-653d1	12953998890453500	13111775021000000	0	0	12953922224344000
9	.imrworldwide.com	/cgi-bin	V5	AStfNg4NEh0WMQsMLwAjIyhADC0PL1InHIKVVA__	12953922224818000	13016994222000000	0	0	12953922224818000

Chrome 로그 분석

- Cache 정보 분석
- History 정보 분석
- Cookie 정보 분석
- **Download 정보 분석**

Download 정보 분석

- **로그 파일명 : History**
- **파일 형식 : SQLite 데이터베이스 파일 형식**
- **주요 테이블 : downloads 테이블**
- **저장 정보**
  - 소스 URL
  - 다운받은 Local 경로
  - 다운로드 시간(1601년 1월 1일 00:00:00 기준 경과된 마이크로초) : 시작/ 종료시간
  - 총 다운로드 크기
  - 다운로드 상태 : 성공(1), 실패(0)

Download 정보 분석

- downloads 테이블

RecNo	id	full_path	url	start_time	received_bytes	total_bytes	state
Click here to define a filter							
1	1	C:\Documents and Settings\ojh\바탕 화면\android-memory-analysis.pdf	http://digitalforensicssolutions.com/papers/android-memory-analysis.pdf	1309449054	732624	732624	1
2	2	C:\Documents and Settings\ojh\My Documents\Downloads\20101228_이경식_Linux Memory Forensics.pdf	http://forensic.korea.ac.kr/~webmaster/xe/?module=file&act=procFileDownload&file_srl=7853&sid=593c8083b03c602cdb0ee49d921a361d	1309449155	1301126	1301126	1
3	3	C:\Documents and Settings\ojh\My Documents\Downloads\OWASP_T10_-_2010_Korean.pdf	http://www.securityplus.or.kr/xe/?module=file&act=procFileDownload&file_srl=25999&sid=00866c962d596769cb97cd9fadb81947	1309506668	3192897	3192897	1
4	4	C:\Documents and Settings\ojh\My Documents\Downloads\CSRF-v.0.5.docx	http://cfile1.uf.tistory.com/attach/1424E61049C4CBE05FABFE	1309525249	854678	854678	1
5	5	C:\Documents and Settings\ojh\My Documents\Downloads\web2.0-csrf.pdf	http://x82.inetcop.org/h0me/papers/web2.0-csrf.pdf	1309527433	344206	344206	1
6	6	C:\Documents and Settings\ojh\My Documents\Downloads\CSRF_Basic_by_Certlab%5B1%5D.pdf	http://cfile21.uf.tistory.com/attach/150A730F49ED6C43F9B6C0	1309537737	842578	842578	1

Safari 로그 분석

- **Cache 정보 분석**
- History 정보 분석
- Cookie 정보 분석
- Download 정보 분석

Cache 정보 분석

- **로그 파일명 : Cache.db**

- **파일 형식**
  - SQLite 데이터베이스 파일 형식

- **주요 테이블**
  - cfurl_cache_response : 캐시 인덱스 정보 저장
  - cfurl_cache_blob_data : 캐시 데이터 저장

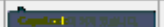
- 저장 정보
  - URL
  - 다운로드 시간(2001년 1월 1일 00:00:00 기준 경과된 초)
  - 캐시 데이터

Cache 정보 분석

- **테이블 구조**
  - cfurl_cache_response 테이블

RecNo	entry_ID	version	hash_value	storage_policy	request_key	time_stamp
Click here to define a filter						
1	1	0	932015557	0	http://www.apple.com/kr/startpage/	2011-02-22 16:44:20
2	2	0	-1219102704	0	http://www.apple.com/favicon.ico	2011-02-22 16:44:20
3	3	0	-446729224	0	http://www.apple.com/kr/hotnews/	2011-02-22 16:44:20
4	4	0	1874641984	0	http://images.apple.com/global/scripts/browserdetect.js	2011-02-22 16:44:20
5	5	0	-612172417	0	http://images.apple.com/kr/global/nav/styles/navigation.css	2011-02-22 16:44:20
6	6	0	1263151578	0	http://images.apple.com/global/scripts/apple_core.js	2011-02-22 16:44:20

  - cfurl_cache_blob_data 테이블

RecNo	entry_ID	response_object	request_object	receiver_data	proto_props	user_info
Click here to define a filter						
165	165				(null)	(null)
166	166			도니키	(null)	(null)
167	167				(null)	(null)
168	168				(null)	(null)
169	169				(null)	(null)
170	170				(null)	(null)
171	171				(null)	(null)
172	172				(null)	(null)
173	173				(null)	(null)
174	174				(null)	(null)

Safari 로그 분석

- Cache 정보 분석
- **History 정보 분석**
- Cookie 정보 분석
- Download 정보 분석

History 정보 분석

- **로그 파일명 : History.plist**

- **파일 형식**
  - Binary Plist

- **저장 정보**
  - URL
  - Title
  - 방문 횟수
  - 방문 시간(2001년 1월 1일 00:00:00 기준 경과된 초

History 정보 분석

- **History.plist 구조 (plistEditor Pro 2.0 사용)**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>WebHistoryDates</key>
   <array>
      <dict>
         <key></key>
         <string>http://www.fomos.kr/gnuboard4/bbs/board.php?bo_table=talk_gossip&amp;amp;wr_id=232764&amp;amp;page=3</string>
         <key>D</key>
         <array>
            <integer>1</integer>
         </array>
         <key>lastVisitedDate</key>
         <string>331198835.4</string>
         <key>title</key>
         <string>포모스::토크 &gt; 가십 &gt; 세계는 지금! -현재 북경의 상황입니다.</string>
         <key>visitCount</key>
         <integer>1</integer>
      </dict>
      <dict>
         <key></key>
         <string>http://www.fomos.kr/gnuboard4/bbs/board.php?bo_table=talk_gossip&amp;amp;wr_id=232913&amp;amp;page=3</string>
         <key>D</key>
         <array>
            <integer>1</integer>
         </array>
         <key>lastVisitedDate</key>
         <string>331198821.2</string>
         <key>title</key>
         <string>포모스::토크 &gt; 가십 &gt; 차시현상 동결</string>
         <key>visitCount</key>
         <integer>1</integer>
      </dict>
```

Safari 로그 분석

- Cache 정보 분석
- History 정보 분석
- **Cookie 정보 분석**
- Download 정보 분석

Cookie 정보 분석

- **로그 파일명 : Cookies.plist**

- **파일 형식**
  - Text Plist

- **저장 정보**
  - 도메인, 경로
  - 이름, 값
  - 생성 시간(2001년 1월 1일 00:00:00 기준 경과된 초)
  - 만료 시간 텍스트 형식
  - HttpOnly 옵션

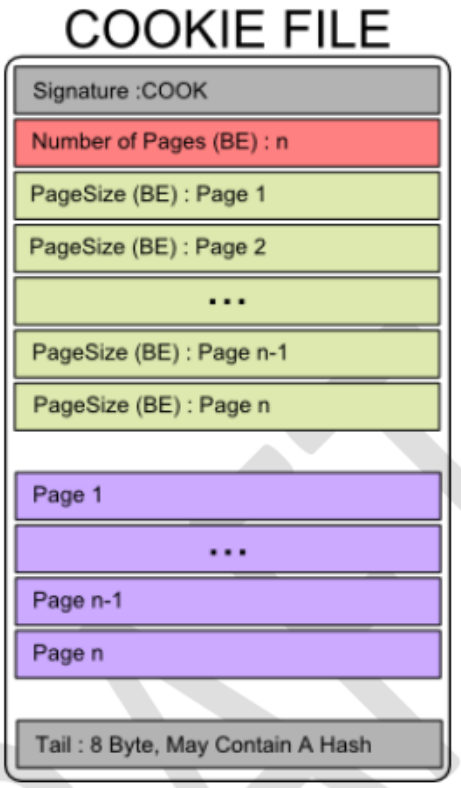
Cookie 정보 분석

- **Cookies.plist 구조**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
    <dict>
        <key>Created</key>
        <real>320087596.484375</real>
        <key>Domain</key>
        <string>.tiara.daum.net</string>
        <key>Expires</key>
        <date>2021-02-19T17:09:28Z</date>
        <key>HttpOnly</key>
        <string>TRUE</string>
        <key>Name</key>
        <string>UUID</string>
        <key>Path</key>
        <string>/</string>
        <key>Value</key>
        <string>C62Of16KsvjE.Fn3dxx6gRZKX5pVHh7i</string>
    </dict>
    <dict>
        <key>Created</key>
        <real>331198652.484375</real>
        <key>Domain</key>
        <string>.apple.com</string>
        <key>Expires</key>
        <date>2011-07-01T08:07:32Z</date>
        <key>Name</key>
        <string>dfa_cookie</string>
        <key>Path</key>
        <string>/</string>
        <key>Value</key>
        <string>applekrglobal</string>
    </dict>
```

Cookie 정보 분석 : 5.1 버전부터 새로운 파일 포멧 사용 (Cookie.binarycookie)

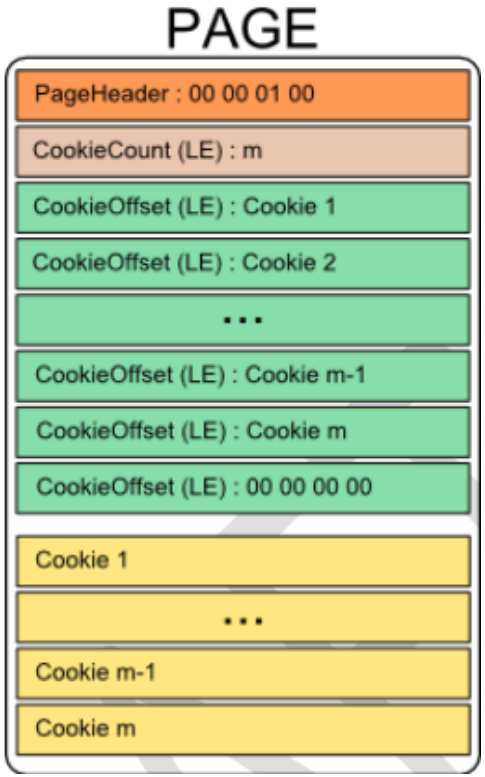
- **Cookie.binarycookie** 파일 전체 구조
  - Signature : "COOK"
  - Page 단위로 구성됨
    - ✓ Page 는 가변 길이
    - ✓ Page 사이즈를 배열 형식으로 따로 저장
    - ✓ Page 사이즈 배열이 끝나면 실제 Page 들이 위치



Field Name	Size	Description
Signature	4 bytes	"COOK" file header signature.
Number of Pages	4 bytes	Little Endian Integer
Page Size	4 bytes	Little Endian Integer. Offset from start of page to start of cookie. There are CookieCount+1 entries.
Page	X bytes	Variable size cookie data. There are CookieCount cookie entries.
Tail	8 bytes	

Cookie 정보 분석 : 5.1 버전부터 새로운 파일 포멧 사용 (Cookie.binarycookie)

- **Page 구조**
  - 각 쿠키 정보는 쿠키 레코드에 저장됨
  - 쿠키 레코드 크기는 가변
  - 각 쿠키 레코드의 위치는 배열 형식으로 저장됨

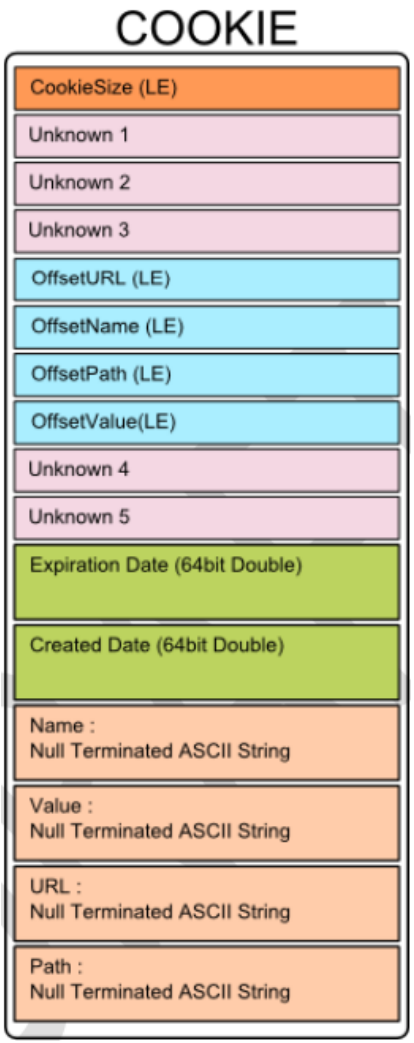


Field Name	Size	Description
Page Header	4 bytes	
CookieCount	4 bytes	Little Endian Integer
CookieOffset	4 bytes	Little Endian Integer. Offset from start of page to start of cookie. There are CookieCount+1 entries.
Cookie	X bytes	Variable size cookie data. There are CookieCount cookie entries.

Cookie 정보 분석 : 5.1 버전부터 새로운 파일 포멧 사용 (Cookie.binarycookie)

- **Cookie 레코드 구조**
  - URL, Path, Name, Value 값은 아스키 값 형태로 저장됨
  - Create Date, Expiration Date
    - ✓ 64 bit Double Mac Absolute Time(GMT) ???
    - ➔ 이 포멧에 대해 아시는 분은 메일로 알려주시면 감사하겠습니다. ㅠㅠ

Field Name	Size	Description
CookieSize	4 bytes	Size of the cookie in bytes. LE
Unknown 1	4 bytes	
Unknown 2	4 bytes	
Unknown 3	4 bytes	
OffsetURL	4 bytes	Offset from start of cookie to URL string. LE
OffsetName	4 bytes	Offset from start of cookie to Name string. LE
OffsetPath	4 bytes	Offset from start of cookie to Path string. LE
OffsetValue	4 bytes	Offset from start of cookie to Value string. LE
Unknown 4	4 bytes	
Unknown 5	4 bytes	
Expiration Date	8 bytes	64bit Double Mac Absolute Time. GMT
Created Date	8 bytes	64 Bit Double Mac Absolute Time. GMT
Name	X bytes	Cookie name. A Null (0x00) terminated ASCII string.
Value	X bytes	Cookie value. A Null (0x00) terminated ASCII string.
URL	X bytes	Cookie URL. A Null (0x00) terminated ASCII string.
Path	X bytes	Cookie path. A Null (0x00) terminated ASCII string.



Safari 로그 분석

- Cache 정보 분석
- History 정보 분석
- Cookie 정보 분석
- **Download 정보 분석**

Download 정보 분석

- **로그 파일명 : Downloads.plist**

- **파일 형식**
  - Binary Plist

- **저장 정보**
  - 소스 URL
  - 다운로드 경로
  - 다운로드 파일 크기

Download 정보 분석

- **Downloads.plist 구조**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>DownloadHistory</key>
   <array>
      <dict>
         <key>DownloadEntryIdentifier</key>
         <string>6588E5E2-8558-F04C-96B1-047A3D45A20A</string>
         <key>DownloadEntryPath</key>
         <string>C:\Documents and Settings\ojh\My Documents\url.html</string>
         <key>DownloadEntryProgressBytesSoFar</key>
         <integer>732</integer>
         <key>DownloadEntryProgressTotalToLoad</key>
         <integer>732</integer>
         <key>DownloadEntryURL</key>
         <string>http://www.google.co.kr/url?sa=t&amp;source=web&amp;cd=1&amp;ved=0CDAQhgIwAA&amp;url=http%3A%2F%2Fall.net%2FForensicsPapers%2FHandbookOfCIS.pdf
      </dict>
      <dict>
         <key>DownloadEntryIdentifier</key>
         <string>627E501B-FF12-CB48-92AE-25B8369D6ACD</string>
         <key>DownloadEntryPath</key>
         <string>C:\Documents and Settings\ojh\My Documents\forensics_module11.ppt</string>
         <key>DownloadEntryProgressBytesSoFar</key>
         <integer>3076608</integer>
         <key>DownloadEntryProgressTotalToLoad</key>
         <integer>3076608</integer>
         <key>DownloadEntryURL</key>
         <string>http://isis.poly.edu/courses/cs996-forensics/Lectures/forensics_module11.ppt</string>
      </dict>
   </array>
</dict>
</plist>
```

Opera 로그 분석

- **Generic Binary Format**
- Cache 정보 분석
- Download 정보 분석
- Cookie 정보분석
- History 정보 분석

Generic Binary Format(조금 복잡하니까 졸지 마세요...ㅠㅠ)

- **Opera 버전 5.0 부터 사용**
- **버전 3.x 와는 호환 안 됨, 버전 4.x 와는 호환 가능**
- **일련의 길이 정보를 가진 레코드들의 집합**
- **대상 파일**
  - dcache4.url : 캐시 파일
  - cookies4.dat : 쿠키 파일
  - download.dat : 다운로드 목록 파일

Generic Binary Format

- **데이터 타입**
  - 정수 정보
    - ✓ 빅 엔디안 타입으로 저장 ➔ 파싱 시, 리틀 엔디안으로 변환 필요
    - ✓ EX) 레코드 길이 정보, 시간 정보, 사이즈 정보 …
  - 시간 정보
    - ✓ time_t 타입 사용
    - ✓ 1970년 1월 1일 00:00:00 기준으로 현재까지 경과된 초
    - ✓ 빅 엔디안 타입으로 저장
  - 문자 정보
    - ✓ 기본적으로 영어는 아스키 타입으로 저장
    - ✓ 그 외 다국어 일 경우 UTF-8 로 인코딩

Generic Binary Format

- **파일 구성**
  - 헤더 + 레코드 집합
  - 헤더 구성
    - ✓ 파일 버전(4byte) : 어플리케이션 보다 파일 버전이 높으면 못 읽음
      - 하위 12bit : minor 버전
      - 상위 30bit : major 버전
    - ✓ 애플리케이션 버전(4byte)
      - 0x00002000 : 쿠키 파일
      - 0x00020000 : 캐시, 다운로드 목록 파일
    - ✓ 레코드의 Tag_ID 크기 (2byte)
    - ✓ 레코드의 데이터 크기 필드의 크기 (2byte)

Offset	0	1	2	3	4	5	6	7	8	9	10	11
00000000	00	00	10	00	00	02	00	00	00	01	00	02

Generic Binary Format

- **파일 구성 (계속)**
  - 레코드 구성
    - ✓ Tag_ID(Default : 1byte)
      - 레코드에 저장되는 데이터의 타입 정보 저장
      - Tag_ID 종류
        - » 일반 레코드 Tag_ID
          - Tag_ID+길이정보+데이터 구성
        - » Boolean 플래그 Tag_ID
          - 최상위 비트가(MSB)의 1과 0으로 참, 거짓 구분
          - Tag_ID만 존재
    - ✓ Data 길이(Default : 2byte)
    - ✓ Data

Tag_ID(1byte)	Data 길이 (2byte)	Data

Generic Binary Format

- 파일 구성 (계속)
  - 레코드 종류
    - ✓ Entry 레코드
      - 해당 파일의 정보 단위
      - 데이터 레코드들을 포함
      - Tag_ID+길이정보+데이터레코드 집합
    - ✓ Data 레코드
      - 일반적으로 Entry 레코드의 하위 레코드, 단독으로도 존재 할 수 있음
      - 실제 데이터 저장
      - 서브 데이터 레코드를 포함하는 레코드도 있음(ex: HTTP 레코드)
    - ✓ Sub_Data 레코드
      - 데이터 레코드의 하위 레코드

Generic Binary Format

- Tag_ID 정보
  - Entry Tag_ID

File	Tag id
Cache	0x01
Cookies	0x01
Download List	0x41

  - 일반 데이터 Tag_ID

Tag ID	Contents	Meaning
0x03	string	URL
0x04	time_t	마지막 방문시간
(0x0b | MSB_VALUE)	flag	The URL is a result of a form query
0x22	record	Contains the name and last visited time of relative link in the document. May repeat

Generic Binary Format

- Tag_ID 정보(계속)
  - 캐시, 다운로드 혼용 데이터 Tag_ID

Tag ID	Contents	Meaning
0x05	time_t	Localtime, when the file was last loaded, not GMT
0x07	uint8	Status of load: 2 Loaded 4 Loading aborted 5 Loading failed
0x08	uint32	Content size
0x09	string	MIME type of content
0x0A	string	Character set of content
(0x0C | MSB_VALUE)	flag	File is downloaded and stored locally on user's disk, and is not part of the disk cache directory
0x0D	string	Name of file (cache files: only local to cache directory)
(0x0F| MSB_VALUE)	flag	Always check if modified
0x10	record	Contains the HTTP protocol specific information

  - 다운로드 데이터 Tag_ID

Tag ID	Contents	Meaning
0x28	time_t	Identifies the time when the loading of the last/previous segment of the downloaded file started.
0x29	time_t	Identifies the time when the loading of the last/previous segment of the downloaded file was stopped.
0x2A	uint32	How many bytes were in the previous segement of the file being downloaded. If the time the loading ended is not known, this value will be assumed to be zero (0) and the download speed set to zero(unknown).

Generic Binary Format

- Tag_ID 정보(계속)
  - HTTP 레코드 서브 Tag_ID

Tag ID	Contents	Meaning
0x15	string	HTTP date header
0x16	time_t	Expiry date
0x17	string	Last modified date
0x18	string	MIME type of document
0x19	string	Entity tag
0x1A	string	Moved to URL (Location header)
0x1B	string	Response line text
0x1C	uint32	Response code
0x1D	string	Refresh URL
0x1E	uint32	Refresh delta time
0x1F	string	Suggested file name
0x20	string	Content Encodings
0x21	string	Content Location
0x25	uint32	Together with tag 0x0026 (both must be present) this identifies the User Agent string last used to load the resource. This value identifies the User Agent string. This value is used internally, and should not be modified.
0x26	uint32	Together with tag 0x0025 (both must be present) this identifies the User Agent string last used to load the resource. This value identifies the User Agent sub version. This value is used internally, and should not be modified.
(0x30 | MSB_VALUE)	flag	Reserved for future use
(0x31 | MSB_VALUE)	Flag	Reserved for future use

Generic Binary Format

- **기본 구성**
  - Entry 레코드들의 연속적인 집합
  - Entry 레코드 안에 Data 레코드들이 연속적으로 구성되어 있음
  - 특정 Data 레코드(EX: HTTP Data 레코드) 들은 Sub Data 레코드들을 포함함

Opera 로그 분석

- Generic Binary Format
- **Cache 정보 분석**
- Download 정보 분석
- Cookie 정보 분석
- History 정보 분석

Opera 로그 분석

Cache 정보 분석(외부 저장)

dcache4.url

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	00	00	10	00	00	02	00	00	00	01	00	02	40	00	05	30
00000016	30	31	4B	45	01	01	59	03	00	B3	68	74	74	70	3A	2F
00000032	2F	76	69	64	65	6F	2E	67	6F	6F	67	6C	65	2E	63	6F
00000048	6D	2F	54	68	75	6D	62	6E	61	69	6C	53	65	72	76	65
00000064	72	32	3F	61	70	70	3D	73	6D	68	26	63	6F	6E	74	65
00000080	6E	74	69	64	3D	32	31	35	35	36	39	66	61	35	62	33
00000096	62	65	32	39	30	26	6F	66	66	73	65	74	6D	73	3D	34
00000112	36	35	36	30	26	69	74	61	67	3D	77	31	36	30	26	73
00000128	69	67	68	3D	75	59	30	54	35	68	42	53	71	36	73	76
00000144	37	41	74	65	58	47	46	45	44	76	79	58	4A	38	63	26
00000160	68	3D	36	30	26	77	3D	38	30	26	73	69	67	68	3D	5F
00000176	5F	67	6E	73	54	33	76	77	56	52	73	76	56	52	34	36
00000192	4B	68	6D	4F	50	69	63	48	79	56	79	34	3D	04	00	04
00000208	00	00	00	00	07	00	04	00	00	00	02	09	00	0A	69	6D
00000224	61	67	65	2F	6A	70	65	67	08	00	08	00	00	00	00	00
00000240	00	0A	4A	51	00	01	01	05	00	08	00	00	00	00	4C	B5
00000256	E2	16	16	00	08	00	00	00	00	4C	B6	36	76	10	00	4A
00000272	25	00	04	00	00	00	01	26	00	04	00	00	00	00	1C	00
00000288	04	00	00	00	C8	3A	00	04	00	00	00	00	25	00	04	00
00000304	00	00	01	26	00	04	00	00	00	00	15	00	1D	57	65	64
00000320	2C	20	31	33	20	4F	63	74	20	32	30	31	30	20	31	36
00000336	3A	34	34	3A	32	39	20	47	4D	54	0D	00	13	67	5F	30
00000352	30	30	46	5C	6F	70	72	30	30	31	4B	32	2E	74	6D	70
00000368	01	00	F7	03	00	3D	68	74	74	70	3A	2F	2F	69	64	2E

```
                @  0
01KE  Y  ³http:/
/video.google.co
m/ThumbnailServe
r2?app=smh&conte
ntid=215569fa5b3
be290&offsetms=4
6560&itag=w160&s
igh=uY0T5hBSq6sv
7AteXGFEDvyXJ8c&
h=60&w=80&sigh=_
_gnsT3vwVRsvVR46
KhmOPicHyVy4=
      im
age/jpeg
  JQ      Lµ
â      L¶6v  J
%      &
  È:      %
    &      Wed
, 13 Oct 2010 16
:44:29 GMT  g_0
00F\opr001K2.tmp
  ÷  =http://id.
```

헤더

Entry 레코드

Data 레코드

Sub_Data 레코드

Entry Tag_ID

Entry 길이

Data Tag_ID

Data 길이

Sub_Data Tag_ID

Sub_Data 길이

Boolean Flag

Data

Cache 정보 분석 (내부 저장)

dcache4.url

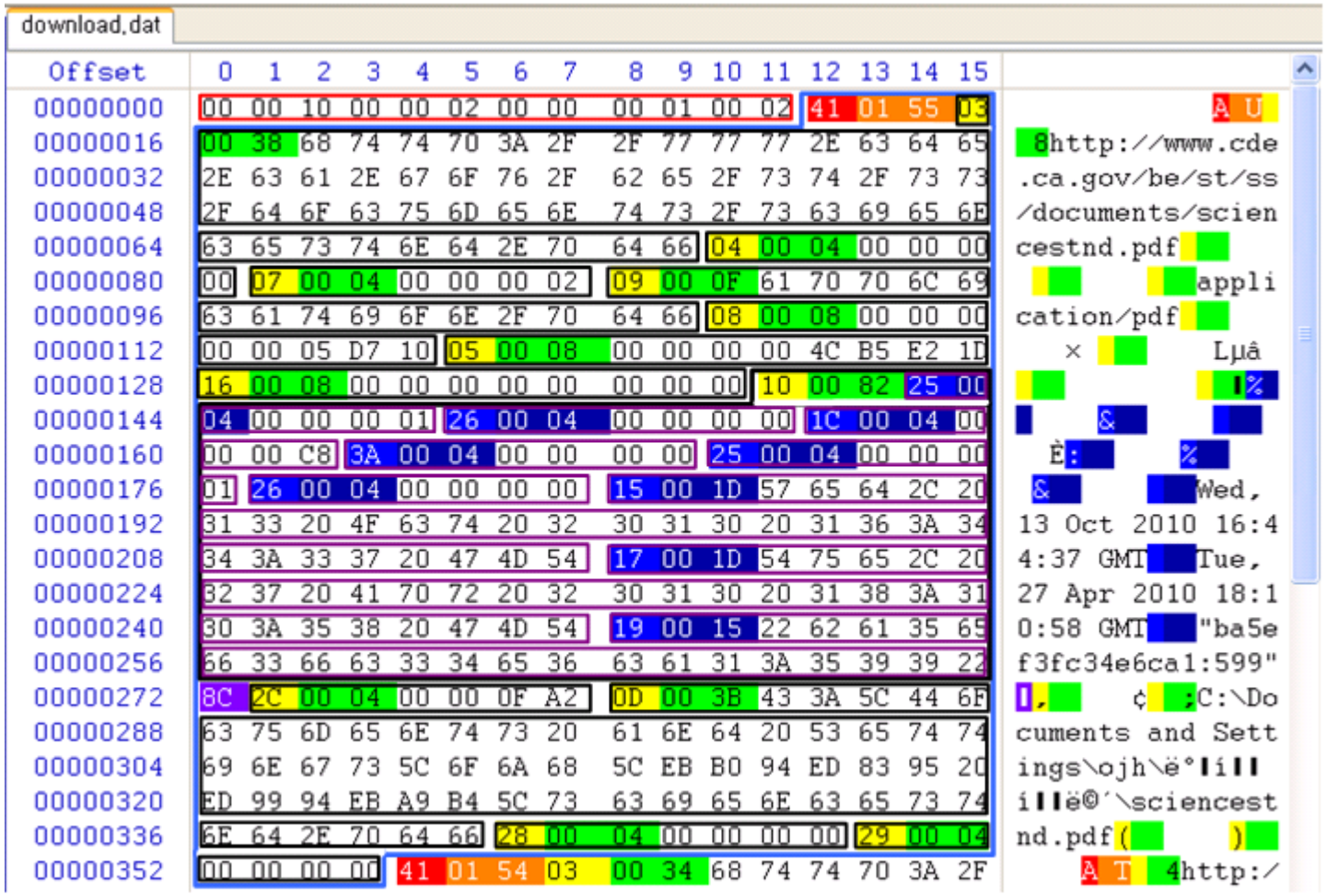
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00001264	7D	5D	29	01	01	64	03	00	91	68	74	74	70	3A	2F	2F	}]) d 'http://
00001280	63	6C	69	65	6E	74	73	31	2E	67	6F	6F	67	6C	65	2E	clients1.google.
00001296	63	6F	2E	6B	72	2F	63	6F	6D	70	6C	65	74	65	2F	73	co.kr/complete/s
00001312	65	61	72	63	68	3F	68	6C	3D	6B	6F	26	63	6C	69	65	earch?hl=ko&clie
00001328	6E	74	3D	73	65	72	70	26	65	78	70	49	64	73	3D	31	nt=serp&expIds=1
00001344	37	32	35	39	2C	32	36	34	32	35	2C	32	36	36	33	37	7259,26425,26637
00001360	2C	32	36	37	37	34	26	70	71	3D	25	45	41	25	42	39	,26774&pq=%EA%B9
00001376	25	38	30	25	45	43	25	39	37	25	42	30	25	45	43	25	%80%EC%97%B0%EC%
00001392	39	35	25	38	34	26	71	3D	66	69	6C	65	74	79	70	65	95%84&q=filetype
00001408	25	33	41	70	26	63	70	3D	31	30	04	00	04	00	00	00	%3Ap&cp=10
00001424	00	07	00	04	00	00	00	02	09	00	0F	74	65	78	74	2F	text/
00001440	6A	61	76	61	73	63	72	69	70	74	0A	00	05	75	74	66	javascript utf
00001456	2D	38	08	00	08	00	00	00	00	00	00	00	00	05	00	08	-8
00001472	00	00	00	00	4C	B5	E2	0E	16	00	08	00	00	00	00	4C	Lµâ L
00001488	B5	F0	1E	10	00	4A	25	00	04	00	00	00	01	26	00	04	µð J% &
00001504	00	00	00	00	1C	00	04	00	00	00	C8	3A	00	04	00	00	È:
00001520	00	00	25	00	04	00	00	00	01	26	00	04	00	00	00	00	% &
00001536	15	00	1D	57	65	64	2C	20	31	33	20	4F	63	74	20	32	Wed, 13 Oct 2
00001552	30	31	30	20	31	36	3A	34	34	3A	32	30	20	47	4D	54	010 16:44:20 GMT
00001568	50	00	37	77	69	6E	64	6F	77	2E	67	6F	6F	67	6C	65	P 7window.google
00001584	2E	61	63	2E	68	28	5B	22	66	69	6C	65	74	79	70	65	.ac.h(["filetype
00001600	3A	70	22	2C	5B	5D	2C	22	22	2C	22	22	2C	22	22	2C	:p",[],"","","",
00001616	22	22	2C	22	22	2C	7B	7D	5D	29	01	01	68	03	00	93	"","",{}]) h ▮

- 데이터 **Tag_ID**가 0x50인 레코드는 데이터로 실제 캐시 데이터를 저장함
- 데이터 **Tag_ID**가 0X0D인 레코드는 데이터로 '캐시 데이터가 저장 된 파일 경로명' 을 저장함
- 두 레코드 중 하나만 Entry 레코드에 존재

Opera 로그 분석

- Generic Binary Format
- Cache 정보 분석
- **Download 정보 분석**
- Cookie 정보 분석
- History 정보 분석

Download 정보 분석(



헤더

Entry 레코드

Data 레코드

Sub_Data 레코드

Entry Tag_ID

Entry 길이

Data Tag_ID

Data 길이

Sub_Data Tag_ID

Sub_Data 길이

Boolean Flag

Data

Opera 로그 분석

- Generic Binary Format
- Cache 정보 분석
- Download 정보 분석
- **Cookie 정보 분석**
- History 정보 분석

Cookie 정보 분석

- 기본 구성
  - Entry 레코드들의 연속적인 집합
    - ✓ Entry 레코드 분류
      - Domain Component : Tag ID 0x01
        - » 1/2/3단계로 분류됨(ex: www.opera.com ➔ com:1단계, opera:2단계, www:1단계)
        - » IP로만 이루어진 Domian일 경우 1단계 Domain으로만 구성됨(ex: 211.239.167.20)
        - » 그 외 도메인들은 1~2단계 혹은 1~3단계로 구성됨
      - Path Component : Tag ID 0x02, 존재 하지 않는 경우도 있음
      - Cookie Component : Tag ID 0x03

    - ✓ 구성 예 : www.opera.com/verify

```
["com" Domain component]                  // 1 단계 Domain component
  ["opera" Domain component]              // 2 단계 Domain component
    ["www" Domain component]              // 3 단계 Domain component
      [“verify”  Path component]
        [Cookie component]
      [Path component terminator]
    [end of domain flag ("www")]
  [end of domain flag ("opera")]
[end of domain flag ("com")]
```

Cookie 정보 분석

- **기본 구성(계속)**
  - Cookie Component 안에 Data 레코드들이 연속적으로 구성되어 있음
  - 1단계 Domain Component 아래 여러 개의 2단계 Domain Component 가 올 수 있음
  - 2단계 Domain Component 아래 여러 개의 3단계 Domain Component 가 올 수 있음
  - Path Component 는 1/2/3단계 Domain Component 중 어느 Component 아래에도 올 수 있음
  - 1/2/3단계 Domain Component 와 Path Component 가 결합되어 host 이름 정보를 이루며 그 아래에 있는 Cookie 정보들은 동일한 host 이름을 가짐

Cookie 정보 분석

- **Tag_ID 정보**
  - Entry Tag_ID

Tag id	Component
0x01	Domain Component
0x02	Path Component
0x03	Cookie Component

  - 데이터 Tag_ID

Tag ID	Contents	Meaning
0x1E	string	Domain 정보
0x1D	string	Path 정보
0x10	string	쿠키 이름
0x11	string	쿠키 값
0x12	time_t	만료 시간
0x13	time_t	마지막 접근 시간
0x28	?	?

Cookie 정보 분석

- **Tag_ID 정보(계속)**
  - Component Terminator

Tag id	Terminator
0x84	Domain Component Terminator
0x85	Path Component Terminator

Cookie 정보 분석(cookies4.dat 파일 분석)

cookies4.dat

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	00	00	10	00	00	00	20	01	00	01	00	02	01	00	11	1E
00000016	00	0E	32	31	31	2E	32	33	39	2E	31	36	37	2E	32	30
00000032	03	00	58	10	00	0C	57	45	42	54	52	45	4E	44	53	5F
00000048	49	44	11	00	23	31	36	33	2E	31	35	32	2E	31	36	35
00000064	2E	31	31	38	2D	31	35	38	38	39	33	38	31	39	32	2E
00000080	33	30	31	30	32	37	37	33	12	00	08	00	00	00	00	5F
00000096	5C	FB	1A	13	00	08	00	00	00	00	4C	92	02	FD	28	00
00000112	08	00	00	00	00	00	00	00	9B	A9	85	84	01	00	10	
00000128	1E	00	0D	32	32	32	2E	31	32	32	2E	34	32	2E	31	34
00000144	03	00	4D	10	00	04	4F	41	49	44	11	00	20	65	31	64
00000160	34	39	30	63	62	63	31	36	31	39	36	65	36	38	33	63
00000176	32	36	65	36	37	36	32	65	65	39	36	33	63	12	00	08
00000192	00	00	00	00	4E	72	26	50	13	00	08	00	00	00	00	00
00000208	00	00	00	28	00	08	00	00	00	00	00	00	00	00	9B	A9
00000224	85	84	01	00	10	1E	00	0D	32	32	32	2E	31	32	32	2E
00000240	34	32	2E	32	34	03	00	4D	10	00	04	4F	41	49	44	11
00000256	00	20	61	64	30	65	30	33	61	65	35	34	66	37	64	32
00000272	66	33	31	31	37	65	38	61	32	31	65	62	39	63	36	34
00000288	36	63	12	00	08	00	00	00	00	4E	72	26	64	13	00	08
00000304	00	00	00	00	00	00	00	00	28	00	08	00	00	00	00	00
00000320	00	00	00	9B	A9	85	84	01	00	06	1E	00	03	63	6F	6D
00000336	85	01	00	0A	1E	00	07	61	64	64	74	68	69	73	03	00
00000352	3B	10	00	03	75	69	64	11	00	10	34	63	39	31	66	39
00000368	64	64	66	31	63	66	64	63	36	66	12	00	08	00	00	00
00000384	00	6E	85	7E	59	13	00	08	00	00	00	00	4C	A0	A4	9F
00000400	28	00	08	00	00	00	00	00	00	00	00	A9	03	00	2C	10
00000416	00	03	70	73	63	11	00	01	33	12	00	08	00	00	00	00
00000432	6E	85	7E	59	13	00	08	00	00	00	00	00	00	00	00	28
00000448	00	08	00	00	00	00	00	00	00	00	A9	85	84	01	00	09
00000464	1E	00	06	61	64	6D	65	6C	64	85	01	00	06	1E	00	03
00000480	74	61	67	03	00	55	10	00	09	6D	65	6C	64	5F	73	65
00000496	73	73	11	00	24	65	63	34	34	63	65	34	39	2D	33	61
00000512	32	33	2D	34	63	35	64	2D	38	32	33	36	2D	39	65	36
00000528	64	37	32	35	32	38	39	65	63	12	00	08	00	00	00	00
00000544	4E	73	2D	63	13	00	08	00	00	00	00	00	00	00	00	28
00000560	00	08	00	00	00	00	00	00	00	00	A9	85	84	84	01	00

- 01 Domain Component
- 02 Path Component
- 03 Cookie Component
- Component 길이
- Data Tag_ID
- Data 길이
- 85 Path Component Terminator
- 84 Domain Component Terminator
- Boolean Flag
- Data

Opera 로그 분석

- Generic Binary Format
- Cache 정보 분석
- Download 정보 분석
- Cookie 정보 분석
- **History 정보 분석**

History 정보 분석

- **기본구성**
  - 헤더 파일 없음
  - 레코드로만 구성
  - 레코드 구성
    - ✓ Title : UTF-8 인코딩
    - ✓ URL : ASCII
    - ✓ 방문시간 : 1970년 1월 1일 00:00:00 부터 지금까지의 경과된 초(time_t)
    - ✓ 레코드 end signature : -1(2D 31)
    - ✓ 구분자 : 0x0A

History 정보 분석(global_history.dat 파일 분석)

cookies4.dat | global_history.dat | vlink4.dat | dcache4.url | download.dat

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	68	74	74	70	3A	2F	2F	72	65	64	69	72	2E	6F	70	65	http://redir.ope
00000010	72	61	2E	63	6F	6D	2F	77	77	77	2E	6F	70	65	72	61	ra.com/www.opera
00000020	2E	63	6F	6D	2F	66	69	72	73	74	72	75	6E	2F	0A	68	.com/firstrun/ h
00000030	74	74	70	3A	2F	2F	72	65	64	69	72	2E	6F	70	65	72	ttp://redir.oper
00000040	61	2E	63	6F	6D	2F	77	77	77	2E	6F	70	65	72	61	2E	a.com/www.opera.
00000050	63	6F	6D	2F	66	69	72	73	74	72	75	6E	2F	0A	31	32	com/firstrun/ 12
00000060	36	39	37	39	39	31	39	33	0A	2D	31	0A	57	65	6C	63	69799193 -1 Welc
00000070	6F	6D	65	20	74	6F	20	4F	70	65	72	61	0A	68	74	74	ome to Opera htt
00000080	70	3A	2F	2F	77	77	77	2E	6F	70	65	72	61	2E	63	6F	p://www.opera.co
00000090	6D	2F	70	6F	72	74	61	6C	2F	73	74	61	72	74	75	70	m/portal/startup
000000A0	2F	0A	31	32	36	39	37	39	39	31	39	33	0A	2D	31	0A	/ 1269799193 -1
000000B0	68	74	74	70	3A	2F	2F	72	65	64	69	72	2E	6F	70	65	http://redir.ope
000000C0	72	61	2E	63	6F	6D	2F	70	6C	75	67	69	6E	73	2F	3F	ra.com/plugins/?
000000D0	61	70	70	6C	69	63	61	74	69	6F	6E	2F	78	2D	73	68	application/x-sh
000000E0	6F	63	6B	77	61	76	65	2D	66	6C	61	73	68	0A	68	74	ockwave-flash ht
000000F0	74	70	3A	2F	2F	72	65	64	69	72	2E	6F	70	65	72	61	tp://redir.opera
00000100	2E	63	6F	6D	2F	70	6C	75	67	69	6E	73	2F	3F	61	70	.com/plugins/?ap
00000110	70	6C	69	63	61	74	69	6F	6E	2F	78	2D	73	68	6F	63	plication/x-shoc
00000120	6B	77	61	76	65	2D	66	6C	61	73	68	0A	31	32	36	39	kwave-flash 1269
00000130	37	39	39	32	35	33	0A	2D	31	0A	41	64	6F	62	65	20	799253 -1 Adobe

- Title
- URL
- 방문시간
- End Signature
- 구분자

분석 도구

- Firefox 로그 분석 도구
- Chrome 로그 분석 도구
- Safari 로그 분석 도구
- Opera 로그 분석 도구
- WEFA

Firefox 로그 분석 도구

- Nirsoft : http://www.nirsoft.net/web_browser_tools.html
  - MozillaCacheView : Cache 분석
  - MozillaHistoryView : History 분석
  - MozillaCookieView : Cookie 분석
  - FirefoxDownloadsView : Download List 분석

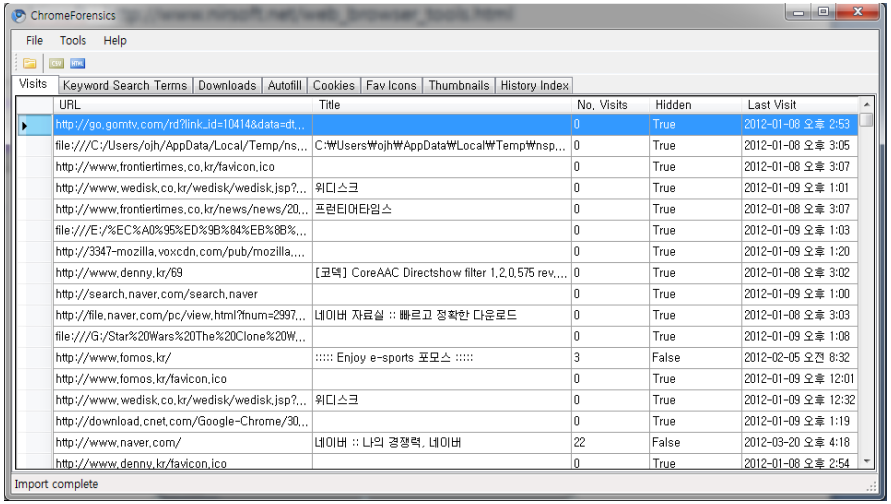
MozillaCookiesView	MozillaCookiesView is an alternative to the standard 'Cookie Manager' provided by Netscape and Mozilla browsers. It displays the details of all c allows you to save the cookies list into text, HTML or XML file, delete unwanted cookies, and backup/restore the cookies file.
MozillaHistoryView	MozillaHistoryView is a small utility that reads the history data file (history.dat) of Firefox/Mozilla/Netscape Web browsers, and displays the list c the following information is displayed: URL, First visit date, Last visit date, Visit counter, Referrer, Title, and Host name. You can also easily export the history data to text/HTML/Xml file.
MozillaCacheView	MozillaCacheView is a small utility that reads the cache folder of Firefox/Mozilla/Netscape Web browsers, and displays the list of all files current is displayed: URL, Content type, File size, Last modified time, Last fetched time, Expiration time, Fetch count, Server name, and more. You can easily select one or more items from the cache list, and then extract the files to another folder, or copy the URLs list to the clipboard.
FirefoxDownloadsView	This utility displays the list of the latest files that you downloaded with Firefox. For every download record, the following information is displayed: Do Type, File Size, Start/End Time, Download Duration, and Average Download Speed. You can easily select one or more downloads, and then save th to the clipboard and paste it into Excel or other spreadsheet application.

Chrome 로그 분석 도구

- Nirsoft : http://www.nirsoft.net/web_browser_tools.html
  - ChromeCacheView : Cache 분석
  - ChromeHistoryView : History 분석

ChromeCacheView	ChromeCacheView is a small utility that reads the cache folder of Google Chrome Web browser, and displays the list of all files currently sto displayed: URL, Content type, File size, Last accessed time, Expiration time, Server name, Server response, and more. You can easily sele another folder, or copy the URLs list to the clipboard.
ChromeHistoryView	ChromeHistoryView is a small utility that reads the history data file of Google Chrome Web browser, and displays the list of all visited Web p is displayed: URL, Title, Visit Date/Time, Number of visits, number of times that the user typed this address (Typed Count), Referrer, and Vi into html/xml/csv/text file, or copy the information to the clipboard and paste it into Excel.

- ChromeForensics : http://www.woanware.co.uk/?page_id=70
  - History, Cookie, Download List 분석 (추가적으로 자동완성, Favicons, Thumbnails)



Safari 로그 분석 도구

- Nirsoft : http://www.nirsoft.net/web_browser_tools.html
  - SafariCacheView : Cache 분석
  - SafariHistoryView : History 분석

SafariHistoryView	SafariHistoryView is a simple utility for Windows that reads and parses the history file of Safari Web browser (history.plist) and displa following information: URL, Web Page Title, Last Visit Time, Visit Count, Redirected To URL, and Record Index. SafariHistoryView allo copy the data to the clipboard and then paste it into Excel.
SafariCacheView	SafariCacheView is a simple utility for Windows that reads and parses the cache file of Safari Web browser (cache.db) and displays the following information: Filename, Content Type, URL, Content Length, Server Name, Server Time, Expiration Time, Last Modified one or more cache items and then extract them into the desired folder or save the cache list into html/text/xml/csv file.

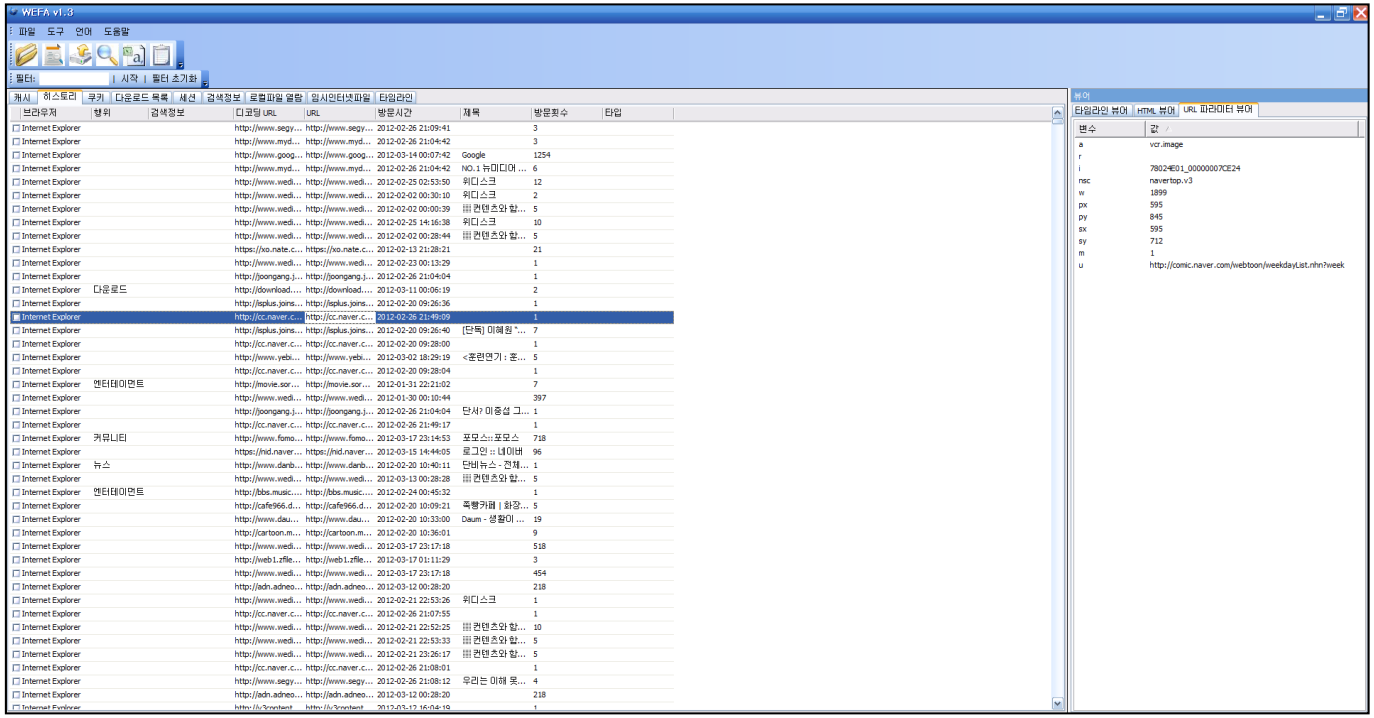
Opera 분석 도구

- Nirsoft : http://www.nirsoft.net/web_browser_tools.html
  - OperaCacheView : Cache 분석

OperaCacheView	OperaCacheView is a small utility that reads the cache folder of Opera Web browser, and displays the list of all files cu Content type, File size, Last accessed time, and last modified time in the server. You can easily select one or more items from the cache list, and then extract the files to another folder, or copy the U

WEFA(Web Browser Forensic Analyzer

- 지원 브라우저 : Internet Explorer, Firefox, Chrome, Safari, Opera
- 분석 대상 정보
  - Cache
  - History
  - Cookie(Safari 5.1 Cookie 제외)
  - Download List
- Freeware Download ➔ http://www.4n6tech.com/skin_kr/images/WEFA_v1.2_-_Freeware.zip



결 론

- 웹 브라우저 로그 파일 구조 분석의 필요성?
  - 웹 브라우저 로그 정보 분석의 기본 배경 지식 ➔ 경우에 따라 직접 수동 분석이 가능
  - 남이 만든 분석 도구는 못 믿겠다!!! or 해당 로그를 분석해 주는 도구가 없을 때
    ➔ 로그 파일 지식을 통해 직접 파싱 도구 개발
  - 기존 도구가 잘 파싱하지 못한다면?
    ➔ 웹 브라우저 로그 포멧은 버전업을 하면서 조금씩 바뀌는 경우가 많음
    ➔ 구글링을 통해 새로운 버전의 포멧 정보를 검색 or 기존 포멧을 토대로 직접 분석해 볼 필요성이 있음

- 로그 파일 분석할 때, 유의 사항~!!
  - 각 브라우저 별 서로 다른 시간 포멧을 가짐
    - ✓ 각 시간 포멧에 맞추어서 계산할 필요성이 있음
    - ✓ 해당 시간 정보가 GMT 인지 로컬 타임인지 구분 필요
  - 인코딩된 정보
    - ✓ 다국어의 경우, URL 인코딩되어 그대로 저장되는 경우가 많음 ➔ 인코딩 방식에 따른 디코딩
    - ✓ 보통은 거의 대부분 UTF-8 인코딩, 경우에 따라 유니코드 인코딩 혹은 코드페이지 인코딩

질문 및 답변