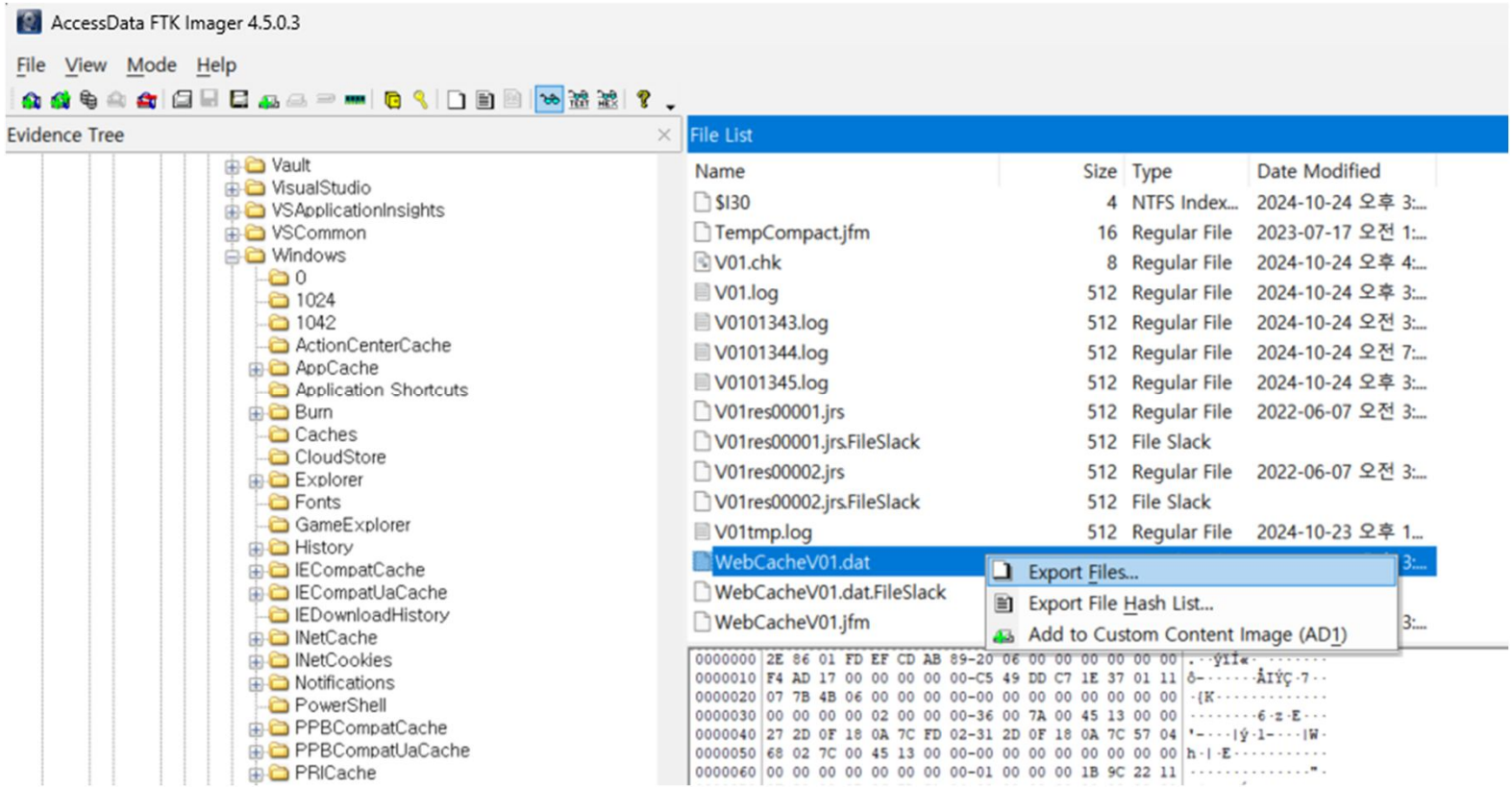
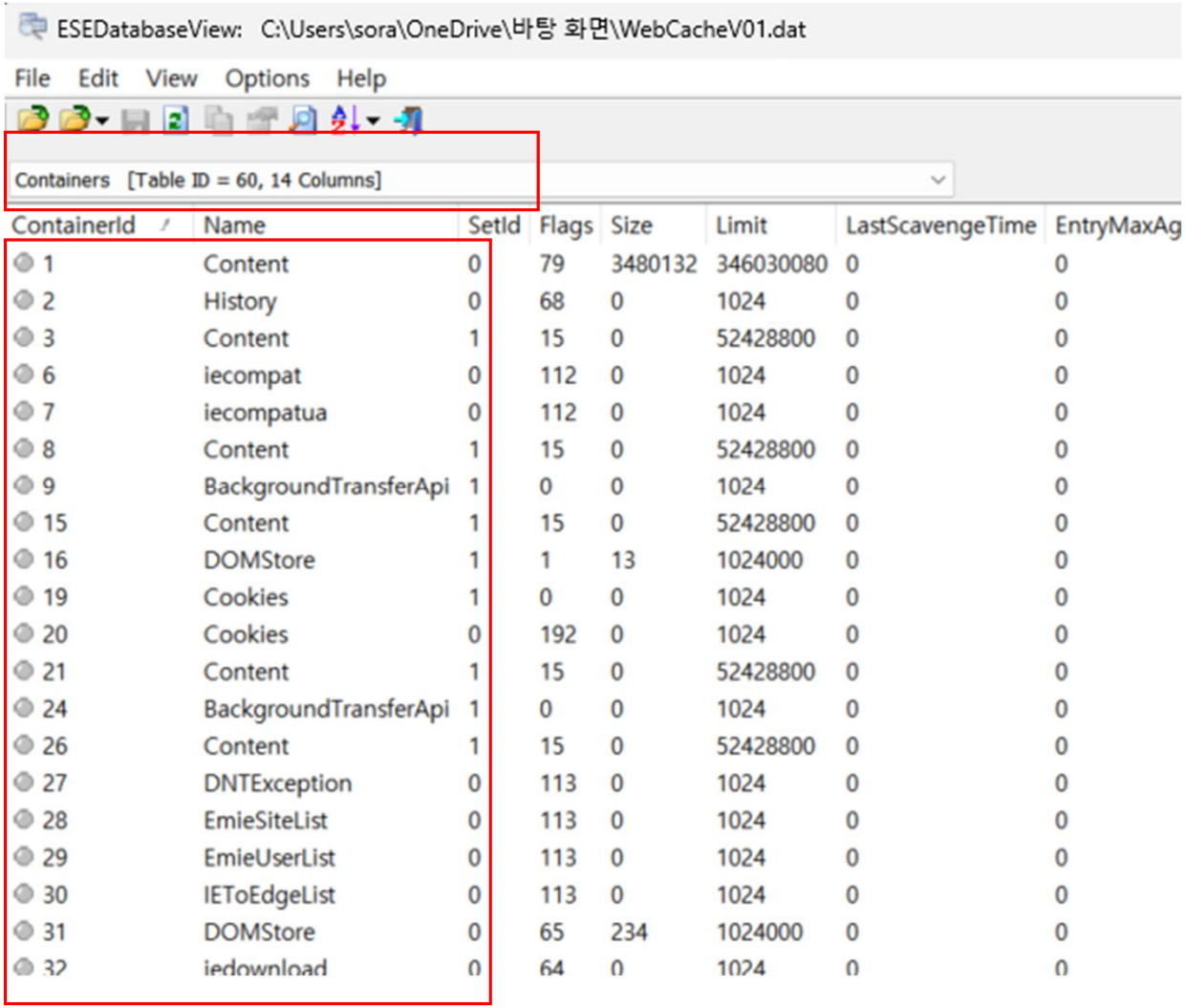
Edge Web Artifact 수집과 분석

분석 대상 OS	Windows 10
분석 대상 Browser	Microsoft Edge
Web Artifact Path (홈폴더 경로)	**%UserProfile%\AppData\Local\Packages\Microsoft.MicrosoftEdge.Stable_8wekyb3d8bbwe**
Web 정보 (데이터 경로)	Cache, History, Cookie, Download **%UserProfile%\AppData₩Local\Microsoft\Windows\WebCache\WebCacheV01.dat**
분석도구	ESEDatabaseView IE10Analyzer

Edge 브라우저 로그 파일 수집





ContainerId	Name	SetId	Flags	Size	Limit	LastScavengeTime	EntryMaxAg
1	Content	0	79	3480132	346030080	0	0
2	History	0	68	0	1024	0	0
3	Content	1	15	0	52428800	0	0
6	iecompat	0	112	0	1024	0	0
7	iecompatua	0	112	0	1024	0	0
8	Content	1	15	0	52428800	0	0
9	BackgroundTransferApi	1	0	0	1024	0	0
15	Content	1	15	0	52428800	0	0
16	DOMStore	1	1	13	1024000	0	0
19	Cookies	1	0	0	1024	0	0
20	Cookies	0	192	0	1024	0	0
21	Content	1	15	0	52428800	0	0
24	BackgroundTransferApi	1	0	0	1024	0	0
26	Content	1	15	0	52428800	0	0
27	DNTException	0	113	0	1024	0	0
28	EmieSiteList	0	113	0	1024	0	0
29	EmieUserList	0	113	0	1024	0	0
30	IEToEdgeList	0	113	0	1024	0	0
31	DOMStore	0	65	234	1024000	0	0
32	iedownload	0	64	0	1024	0	0

Name	분석내용
Centent	Cache 정보
History	History 정보
Cookie	Cookie 정보
iedownload	Download 정보

History 정보 분석

ESEDatabaseView: C:\Users\sora\OneDrive\바탕 화면\WebCacheV01.dat

File Edit View Options Help

Containers [Table ID = 60, 14 Columns]

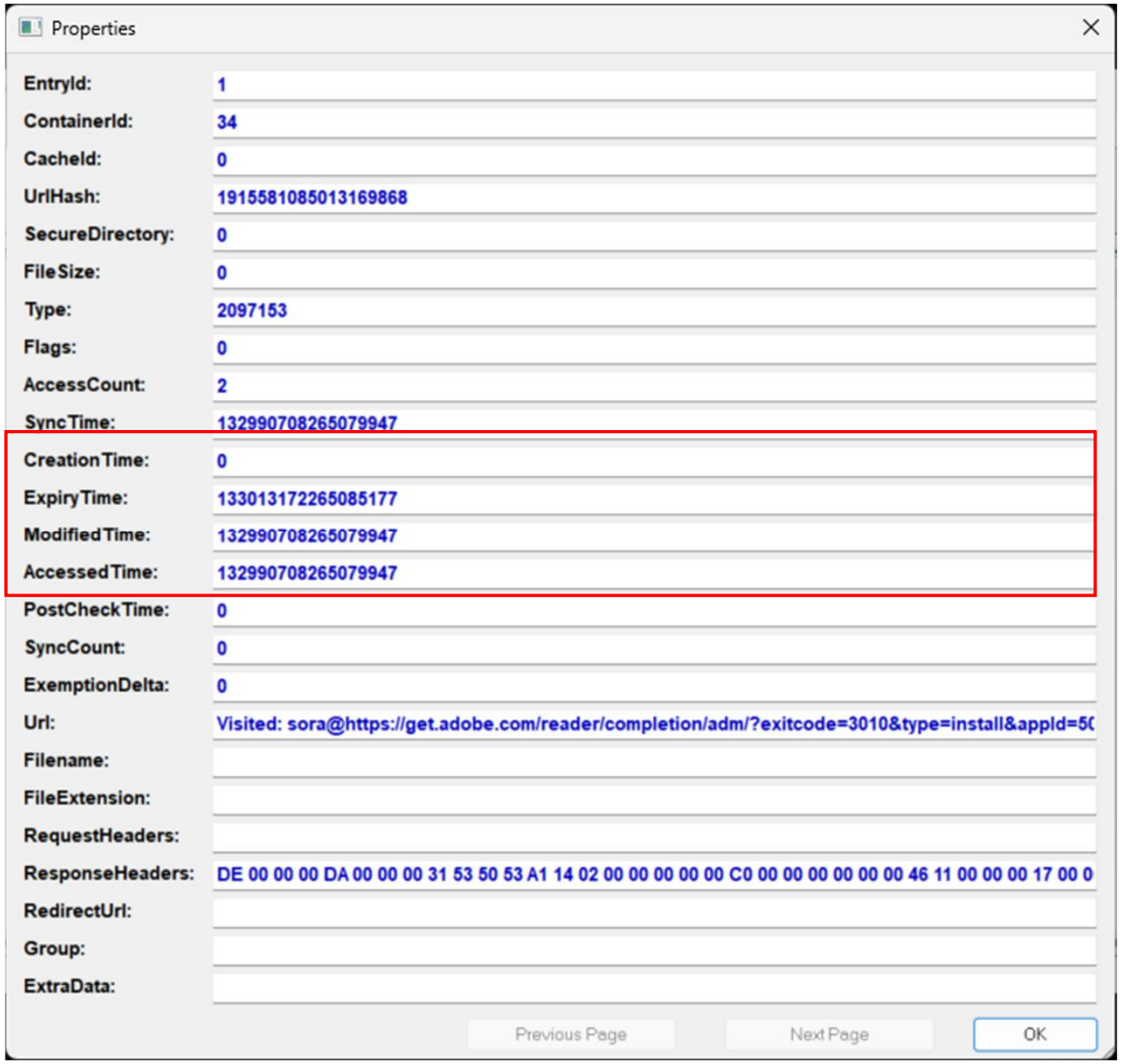
ContainerId	Name	PartitionId
28	EmieSiteList	M
29	EmieUserList	M
998	History	S-1-15-2-283421221-3183566570-1718213290-7515543
881	History	S-1-15-2-3919898394-240971480-980890888-32305582
714	History	S-1-15-2-1312876954-3728250218-3694470604-418876
2	History	M
1251	History	S-1-15-2-1327587233-2730283621-3908338074-337181
34	History	L
63	History	S-1-15-2-2434737943-167758768-3180539153-9843367
1329	History	S-1-15-2-2226957697-3030467180-2301525-424896778
6	iecompat	M
7	iecompatua	M
32	iedownload	M
30	IEToEdgeList	M

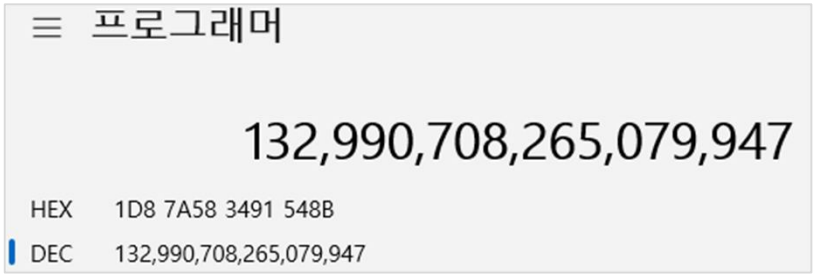
Container_34 [Table ID = 82, 25 Columns]

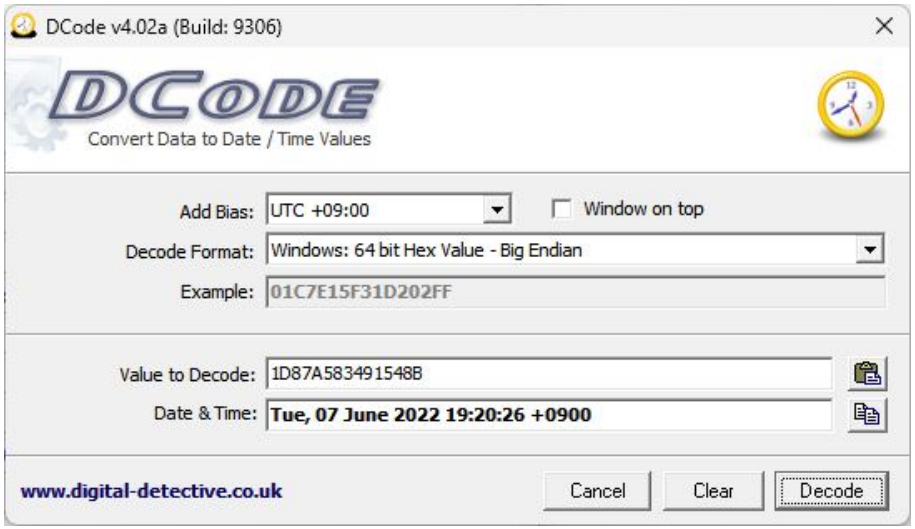
EntryId	ContainerId	CacheId	UrlHash	SecureDirectory	FileSize	Type	Flags	AccessCount	SyncTime	Cr
1	34	0	19155810850131698...	0	0	20...	0	2	132990...	0
2	34	0	55216943444333448...	0	0	20...	0	2	132997...	0
3	34	0	55216943472849306...	0	0	20...	0	2	132997...	0
4	34	0	55216943445121201...	0	0	20...	0	2	132997...	0
5	34	0	55216943447518682...	0	0	20...	0	4	132997...	0
6	34	0	81856711821150782...	0	0	20...	0	2	132997...	0
7	34	0	62457032905947165...	0	0	20...	0	10	132997...	0
15	34	0	51863428059556032...	0	0	20...	0	2	132991...	0
16	34	0	45302348959199342...	0	0	20...	0	1	132991...	0
17	34	0	51863428056192231...	0	0	20...	0	1	132991...	0
21	34	0	41721768868781334...	0	0	20...	0	1	132995...	0
22	34	0	64844837388736475...	0	0	20...	0	1	132995...	0
23	34	0	64844837362988721...	0	0	20...	0	1	132995...	0
27	34	0	36242315808229750...	0	0	20...	0	2	132997...	0
28	34	0	36242315790018138...	0	0	20...	0	2	132997...	0
29	34	0	81856711843080830...	0	0	20...	0	2	133228...	0
30	34	0	209328324727904574	0	0	20...	0	1	132997...	0
31	34	0	81856711834977758...	0	0	20...	0	1	132997...	0
32	34	0	695136691104437953	0	0	20...	0	1	132997...	0

History 정보 분석

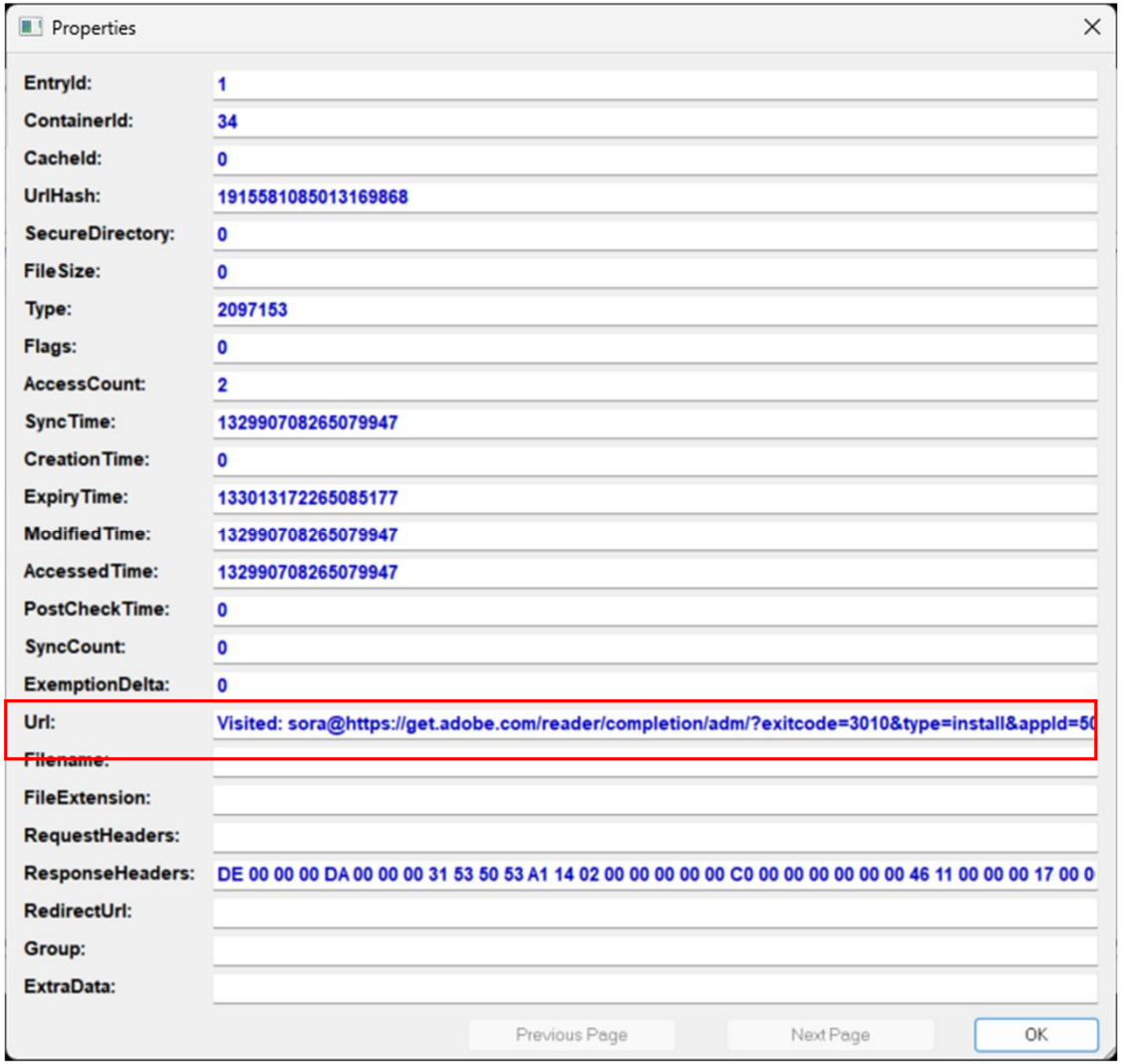
필드	설명
URL	http://~ : 방문 웹 페이지 URL File://~ : 열람한 파일 경로
Access Time	해당 웹 페이지 접근 시간 또는 파일 열람시간
Creation Time	항상 0
Modified Time	Access Time과 동일
Expiry Time	History 데이터 만료시간 시간이 만료되면 삭제(기본 20일)
Sync Time	Access Time과 동일
Response Header	웹 페이지 제목 정보가 들어있는 데이터(Hex 형태)







[Windows:64bit Hex Value-Big Endian]



Web Page 접속 정보

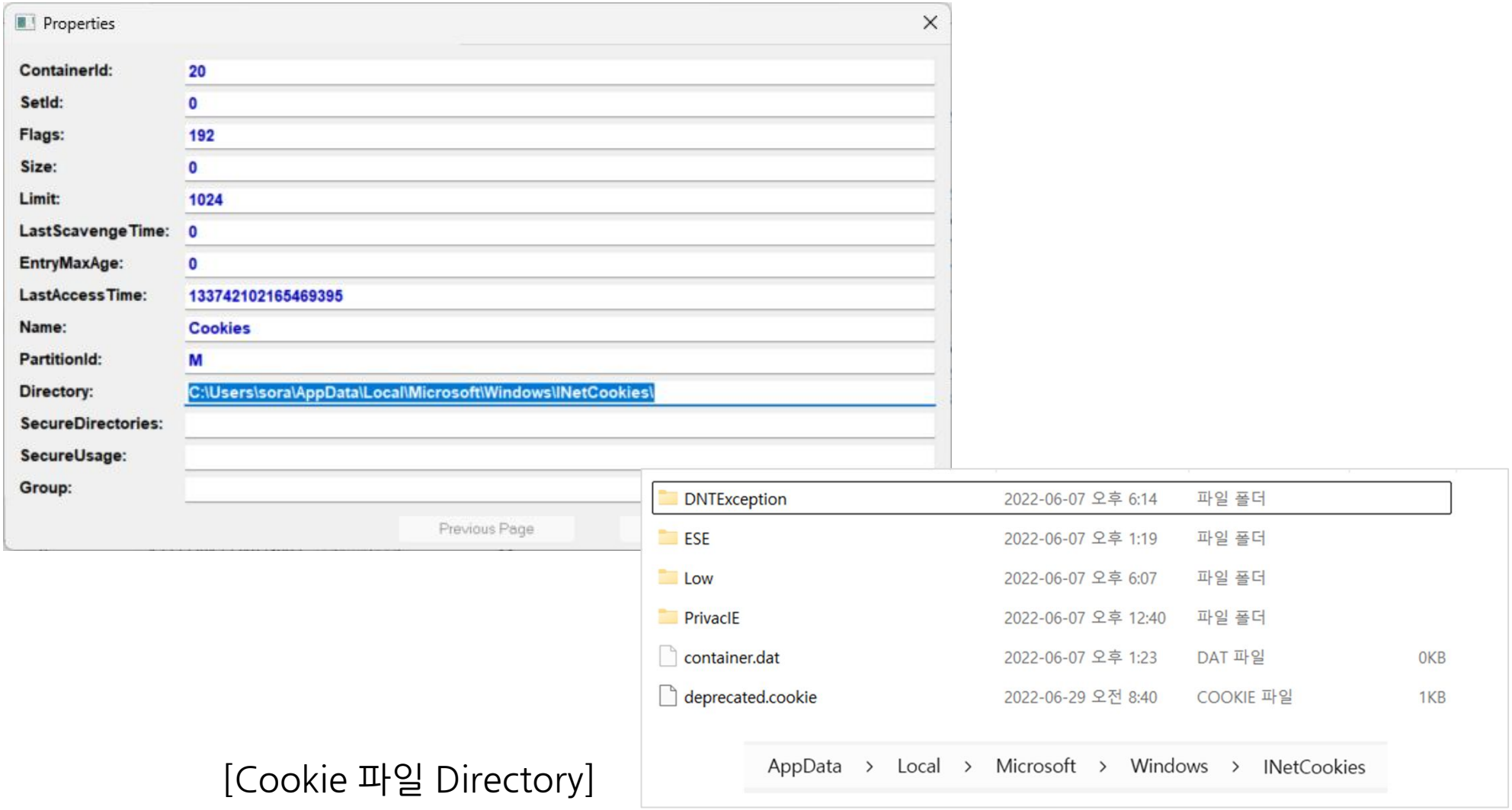
- Visited:[사용자]@http://~

파일 접속 정보

- Visited:[사용자]@file://~

Cookie 정보 분석

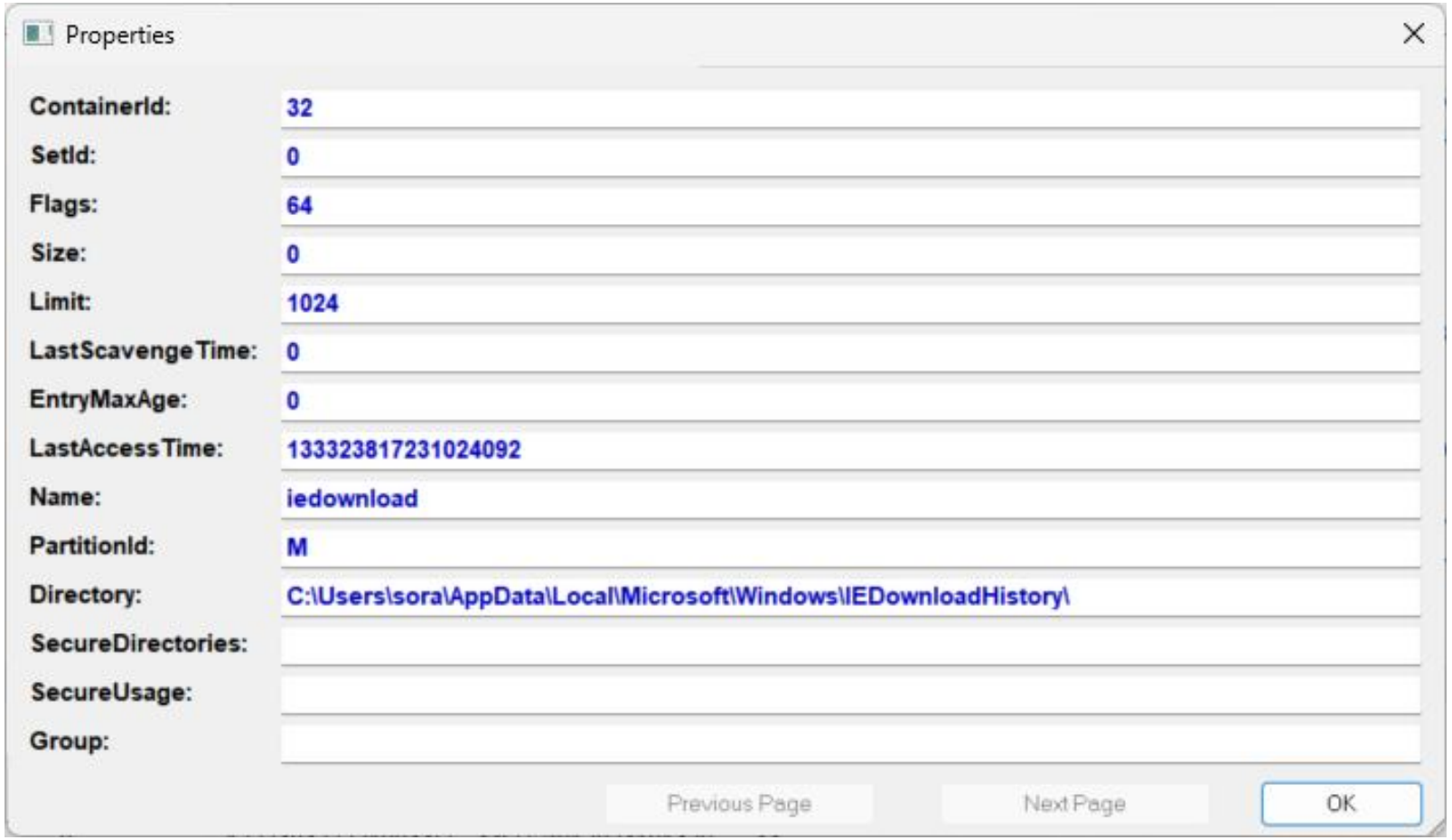
필드	설명
URL	해당 Cookie 호스트 정보
Access Time	해당 사이트 마지막 접근시간
Creation Time	해당 쿠키 파일 생성 시간
Modified Time	Access Time과 동일
Expiry Time	Cookie 만료시간 만료되면 레코드 삭제(기본 20일)
Sync Time	Access Time과 동일
Filename	Cookie 파일명 경로는 Containers 테이블의 Directory에서 확인



[Cookie 파일 Directory]

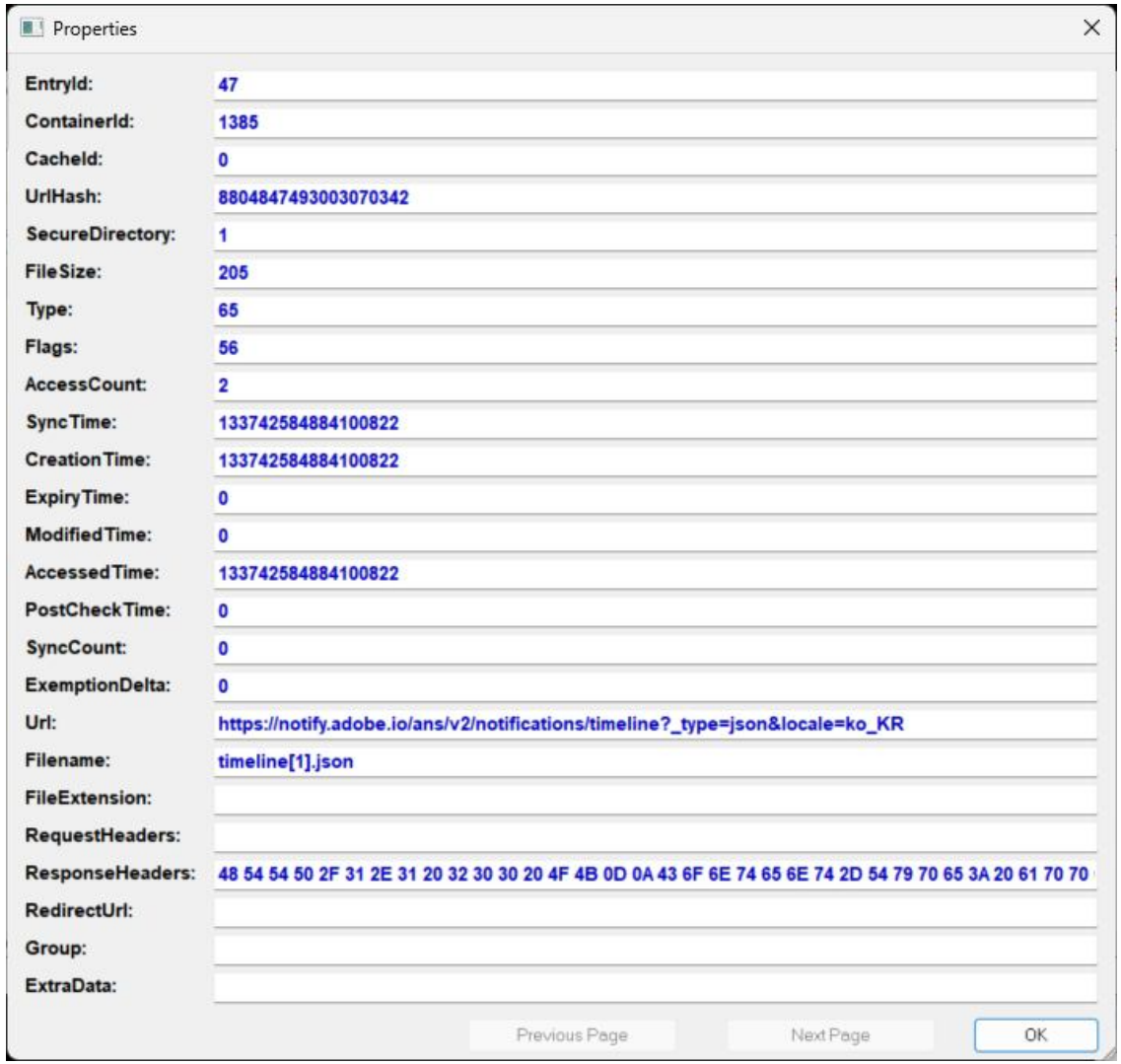
Download 정보 분석

필드	설명
URL	다운로드 GUID 값 지정
Access Time	다운로드 시간
Creation Time	항상 0
Modified Time	항상 0
Expiry Time	항상 0
Sync Time	Access Time과 동일
Response Header	URL 저장 경로 정보 데이터 저장 (Hex 값)


Properties
ContainerId: 32
SetId: 0
Flags: 64
Size: 0
Limit: 1024
LastScavengeTime: 0
EntryMaxAge: 0
LastAccessTime: 133323817231024092
Name: iedownload
PartitionId: M
Directory: C:\Users\sora\AppData\Local\Microsoft\Windows\IEDownloadHistory\
SecureDirectories:
SecureUsage:
Group:
Previous Page
Next Page
OK

Cache 정보 분석

필드	설명
URL	해당 Cache 데이터를 다운로드 한 URL
Access Time	Cache 데이터 다운로드 접근 시간
Creation Time	Cache 데이터 생성시간
Modified Time	해당 Cache 웹 서버에서 마지막 수정 시간
Expiry Time	해당 Cache 데이터 만료 시간 이 값이 0일 경우, 해당 데이터는 웹브라우저가 종료되거나 다른 페이지로 넘어갈 시 바로 삭제
Sync Time	Access Time과 동일
Filename	Cache 데이터 파일명
FileSize	Cache 데이터 크기
Response Header	URL 저장 경로 정보 데이터 저장 (Hex 값)


Properties
EntryId: 47
ContainerId: 1385
CacheId: 0
UrlHash: 8804847493003070342
SecureDirectory: 1
FileSize: 205
Type: 65
Flags: 56
AccessCount: 2
SyncTime: 133742584884100822
CreationTime: 133742584884100822
ExpiryTime: 0
ModifiedTime: 0
AccessedTime: 133742584884100822
PostCheckTime: 0
SyncCount: 0
ExemptionDelta: 0
Url: https://notify.adobe.io/ans/v2/notifications/timeline?_type=json&locale=ko_KR
Filename: timeline[1].json
FileExtension:
RequestHeaders:
ResponseHeaders: 48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70
RedirectUrl:
Group:
ExtraData:
Previous Page
Next Page
OK

IE10Analyzer를 이용한 분석