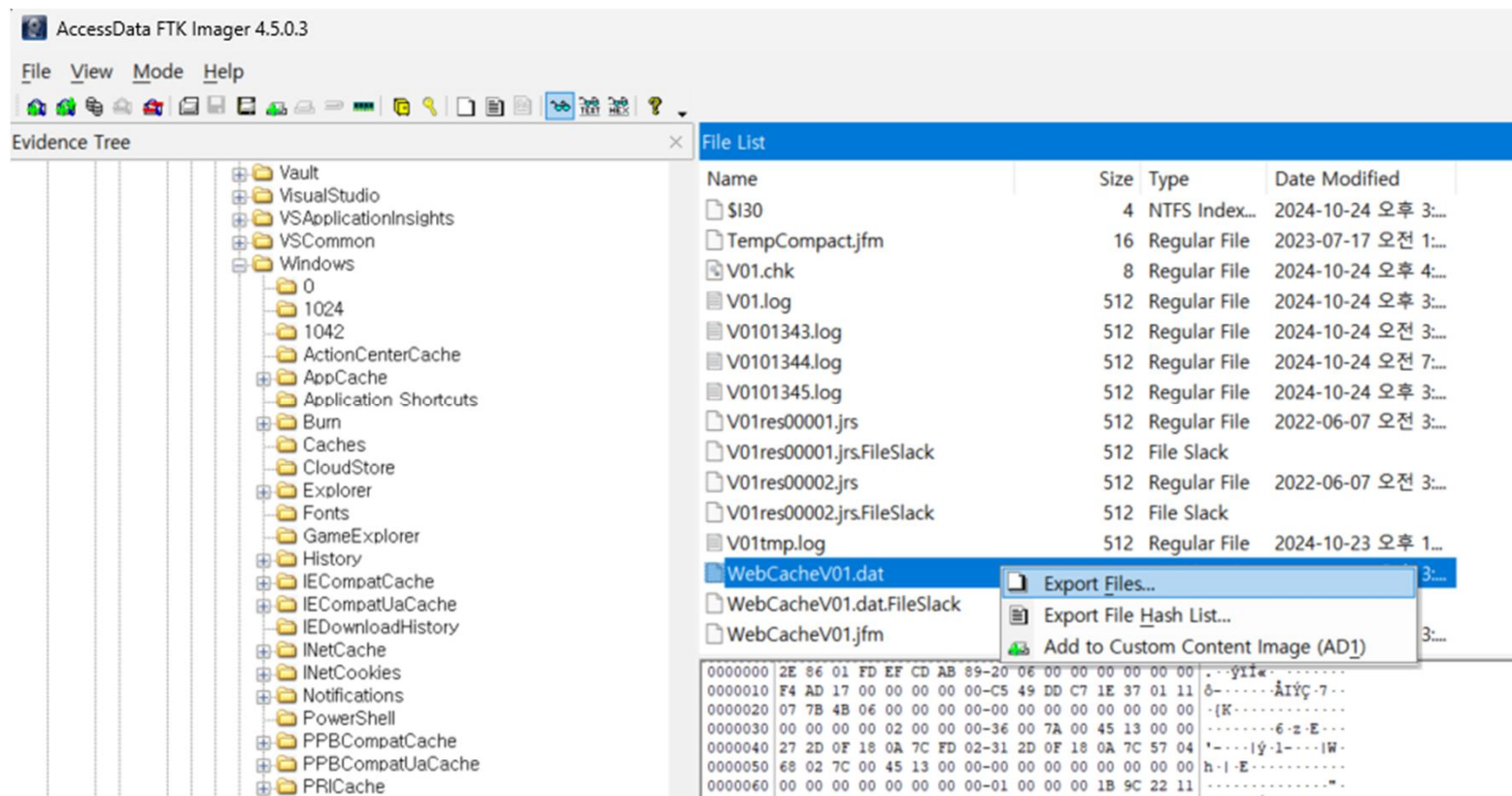


## Edge Web Artifact 수집과 분석

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

# Edge 브라우저 로그 파일 수집



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

File Edit View Options Help

Containers [Table ID = 60, 14 Columns]

| 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        |
|------------|-------------|
| Content    | 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 | Cacheld | 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<br>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<br>시간이 만료되면 삭제(기본 20일)         |
| Sync Time       | Access Time과 동일                                 |
| Response Header | 웹 페이지 제목 정보가 들어있는 데이터(Hex 형태)                   |

Properties

|                  |   |
|------------------|---|
| EntryId:         | 1   |
| ContainerId:     | 34  |
| Cacheld:         | 0   |
| UrlHash:         | 1915581085013169868   |
| SecureDirectory: | 0   |
| FileSize:        | 0   |
| Type:            | 2097153   |
| Flags:           | 0   |
| AccessCount:     | 2   |
| SyncTime:        | 132990708265079947  |
| CreationTime:    | 0   |
| ExpiryTime:      | 133013172265085177  |
| ModifiedTime:    | 132990708265079947  |
| AccessedTime:    | 132990708265079947  |
| PostCheckTime:   | 0   |
| SyncCount:       | 0   |
| ExemptionDelta:  | 0   |
| Url:             | Visited: sora@https://get.adobe.com/reader/completion/adm/?exitcode=3010&type=install&appld=50    |
| Filename:        |   |
| FileExtension:   |   |
| RequestHeaders:  |   |
| ResponseHeaders: | DE 00 00 00 DA 00 00 00 31 53 50 53 A1 14 02 00 00 00 00 C0 00 00 00 00 00 46 11 00 00 00 17 00 0 |
| RedirectUrl:     |   |
| Group:           |   |
| ExtraData:       |   |

Previous Page Next Page OK

≡ 프로그래머

132,990,708,265,079,947

HEX 1D8 7A58 3491 548B

DEC 132,990,708,265,079,947

DCode v4.02a (Build: 9306)

**D CODE**  
Convert Data to Date / Time Values

Add Bias: UTC +09:00 ☐ Window on top

Decode Format: Windows: 64 bit Hex Value - Big Endian

Example: 01C7E15F31D202FF

Value to Decode: 1D87A583491548B

Date & Time: Tue, 07 June 2022 19:20:26 +0900

www.digital-detective.co.uk

Cancel Clear Decode

[Windows:64bit Hex Value-Big Endian]

Properties

|                  |   |
|------------------|---|
| EntryId:         | 1   |
| ContainerId:     | 34  |
| Cached:          | 0   |
| UrlHash:         | 1915581085013169868   |
| SecureDirectory: | 0   |
| File Size:       | 0   |
| Type:            | 2097153   |
| Flags:           | 0   |
| AccessCount:     | 2   |
| Sync Time:       | 132990708265079947  |
| Creation Time:   | 0   |
| ExpiryTime:      | 133013172265085177  |
| Modified Time:   | 132990708265079947  |
| Accessed Time:   | 132990708265079947  |
| PostCheckTime:   | 0   |
| SyncCount:       | 0   |
| ExemptionDelta:  | 0   |
| Url:             | Visited: sora@https://get.adobe.com/reader/completion/adm/?exitcode=3010&type=install&apld=50           |
| Filename:        |   |
| FileExtension:   |   |
| RequestHeaders:  |   |
| ResponseHeaders: | DE 00 00 00 DA 00 00 00 31 53 50 53 A1 14 02 00 00 00 00 00 C0 00 00 00 00 00 00 46 11 00 00 00 17 00 0 |
| RedirectUrl:     |   |
| Group:           |   |
| ExtraData:       |   |

Previous Page Next Page OK

## 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<br>만료되면 레코드 삭제( 기본 20일)              |
| Sync Time     | Access Time과 동일                                  |
| Filename      | Cookie 파일명<br>경로는 Containers 테이블의 Directory에서 확인 |



Properties

|                    |  |
|--------------------|--|
| ContainerId:       | 20   |
| SetId:             | 0  |
| Flags:             | 192  |
| Size:              | 0  |
| Limit:             | 1024   |
| LastScavengeTime:  | 0  |
| EntryMaxAge:       | 0  |
| LastAccessTime:    | 133742102165469395   |
| Name:              | Cookies  |
| PartitionId:       | M  |
| Directory:         | C:\Users\sora\AppData\Local\Microsoft\Windows\INetCookies\ |
| SecureDirectories: |  |
| SecureUsage:       |  |
| Group:             |  |

Previous Page

|                   |                     |           |     |
|-------------------|---------------------|-----------|-----|
| DNTException      | 2022-06-07 오후 6:14  | 파일 폴더     |     |
| ESE               | 2022-06-07 오후 1:19  | 파일 폴더     |     |
| Low               | 2022-06-07 오후 6:07  | 파일 폴더     |     |
| PrivacIE          | 2022-06-07 오후 12:40 | 파일 폴더     |     |
| container.dat     | 2022-06-07 오후 1:23  | DAT 파일    | 0KB |
| deprecated.cookie | 2022-06-29 오전 8:40  | COOKIE 파일 | 1KB |

AppData > Local > Microsoft > Windows > INetCookies

[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<br>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

Cached:

0

UrlHash:

8804847493003070342

SecureDirectory:

1

File Size:

205

Type:

65

Flags:

56

AccessCount:

2

Sync Time:

133742584884100822

CreationTime:

133742584884100822

Expiry Time:

0

ModifiedTime:

0

Accessed Time:

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

| Table |  | Content(M) History(M) History(L) Content(L) |               |             |            |              |             |                |    |
|-------|--|---|---------------|-------------|------------|--------------|-------------|----------------|----|
| No.   | Table Name   | EntryId                                     | Type          | AccessCount | SyncTime   | CreationTime | ExpiryTime  | ModifiedTime   | Ac |
| 192   | Content(M)   | <input type="checkbox"/> 14365              | [Normal][Url] | 151         | 2024-10... | 0            | 2024-11-... | 2024-10-08 ... | 20 |
| 70    | History(M)   | <input checked="" type="checkbox"/> 14366   | [Normal][Url] | 100         | 2024-10... | 0            | 2024-11-... | 2024-10-08 ... | 20 |
| 91    | iecompat(M)  | <input type="checkbox"/> 15161              | [Normal][Url] | 708         | 2024-10... | 0            | 2024-11-... | 2024-10-22 ... | 20 |
| 104   | iecompatua(M)  | <input type="checkbox"/> 21843              | [Normal][Url] | 120         | 2024-10... | 0            | 2024-11-... | 2024-10-25 ... | 20 |
| 107   | BackgroundTransferApi(S-1-15-2-2551677095-2355568638-420...  | <input type="checkbox"/> 22294              | [Normal][Url] | 12          | 2024-10... | 0            | 2024-10-... | 2024-10-04 ... | 20 |
| 65    | DOMStore(S-1-15-2-2434737943-167758768-3180539153-98433E...  | <input type="checkbox"/> 22757              | [Normal][Url] | 34          | 2024-10... | 0            | 2024-11-... | 2024-10-24 ... | 20 |
| 73    | BackgroundTransferApi(S-1-15-2-350187224-1905355452-1037...  | <input type="checkbox"/> 22764              | [Normal][Url] | 7           | 2024-10... | 0            | 2024-11-... | 2024-10-19 ... | 20 |
| 77    | IEToEdgeList(M)  | <input type="checkbox"/> 22766              | [Normal][Url] | 7           | 2024-10... | 0            | 2024-11-... | 2024-10-19 ... | 20 |
| 79    | DOMStore(M)  | <input type="checkbox"/> 22774              | [Normal][Url] | 6           | 2024-10... | 0            | 2024-11-... | 2024-10-19 ... | 20 |
| 82    | History(L)   | <input type="checkbox"/> 22776              | [Normal][Url] | 5           | 2024-10... | 0            | 2024-10-... | 2024-10-04 ... | 20 |
| 83    | DOMStore(L)  | <input type="checkbox"/> 22788              | [Normal][Url] | 8           | 2024-10... | 0            | 2024-11-... | 2024-10-14 ... | 20 |
| 85    | DOMStore(S-1-15-2-1609473798-1231923017-684268153-426851...  | <input type="checkbox"/> 22795              | [Normal][Url] | 5           | 2024-10... | 0            | 2024-11-... | 2024-10-19 ... | 20 |
| 87    | DOMStore(S-1-15-2-744533573-2444454674-265863901-321546E...  | <input type="checkbox"/> 22827              | [Normal][Url] | 10          | 2024-10... | 0            | 2024-11-... | 2024-10-20 ... | 20 |
| 88    | BackgroundTransferApi(S-1-15-2-1714399563-1326177402-204i... | <input type="checkbox"/> 22956              | [Normal][Url] | 4           | 2024-10... | 0            | 2024-10-... | 2024-10-04 ... | 20 |
| 196   | Content(S-1-15-2-283421221-3183566570-1718213290-75155435... | <input type="checkbox"/> 23198              | [Normal][Url] | 5           | 2024-10... | 0            | 2024-11-... | 2024-10-10 ... | 20 |
| 208   | DOMStore(S-1-15-2-283421221-3183566570-1718213290-751554...  | <input type="checkbox"/> 23204              | [Normal][Url] | 7           | 2024-10... | 0            | 2024-11-... | 2024-10-20 ... | 20 |
| 226   | Content(S-1-15-2-1312876954-3728250218-3694470604-4188764... | <input type="checkbox"/> 23209              | [Normal][Url] | 6           | 2024-10... | 0            | 2024-11-... | 2024-10-20 ... | 20 |
| 785   | Content(S-1-15-2-2758101530-1321080646-1475665648-4066602... | <input type="checkbox"/> 23210              | [Normal][Url] | 5           | 2024-10... | 0            | 2024-11-... | 2024-10-19 ... | 20 |
| 840   | DOMStore(S-1-15-2-1910091885-1573563583-1104941280-24182...  | <input type="checkbox"/> 23211              | [Normal][Url] | 5           | 2024-10... | 0            | 2024-11-... | 2024-10-19 ... | 20 |
| 869   | Content(S-1-15-2-1327587233-2730283621-3908338074-3371811... | <input type="checkbox"/> 23212              | [Normal][Url] | 5           | 2024-10... | 0            | 2024-11-... | 2024-10-19 ... | 20 |
| 1019  | Content(L)   | <input type="checkbox"/> 23224              | [Normal][Url] | 6           | 2024-10... | 0            | 2024-11-... | 2024-10-19 ... | 20 |
| 1030  | MSHist012024093020241007(M)                                  | <input checked="" type="checkbox"/> 23335   | [Normal][Url] | 5           | 2024-10... | 0            | 2024-11-... | 2024-10-09 ... | 20 |
| 1038  | MSHist012024100720241014(M)                                  | <input type="checkbox"/> 23342              | [Normal][Url] | 4           | 2024-10... | 0            | 2024-11-... | 2024-10-14 ... | 20 |
| 1050  | MSHist012024101420241021(M)                                  | <input type="checkbox"/> 23408              | [Normal][Url] | 5           | 2024-10... | 0            | 2024-11-... | 2024-10-09 ... | 20 |