

2025 HACKTHEON SEJONG

팀 이름
Team Name

문제 이름
Question

HAINT

Nothing is essential

문제 풀이과정 작성 (캡처화면 필수) / Write-up Details (The screenshot is mandatory)

The screenshot shows the AccessData FTK Imager 4.7.1.2 interface. The 'Evidence Tree' on the left displays a directory structure including 'Microsoft', 'AC', 'InetCache', 'InetCookies', 'InetHistory', 'Microsoft', 'CryptnetUrlCache', 'Content', 'MetaData', 'Temp', 'TokenBroker', 'AppData', 'LocalCache', 'LocalState', 'DiagOutputDir', 'profile', 'RoamingState', and 'Settings'. The 'File List' on the right shows a table of files with columns for Name, Size, Type, and Date Modified. The 'hex' view at the bottom displays the raw data of the selected file, 'plum.sqlite-wal', which contains JSON data for a schedule appointment.

Name	Size	Type	Date Modified
DiagOutputDir	1	Directory	2025-03-12 오전 5:55:...
profile	1	Directory	2025-03-12 오전 5:55:...
\$I30	4	NTFS Index All...	2025-03-12 오전 5:41:...
Ecs.dat	3	Regular File	2025-03-12 오전 5:41:...
plum.sqlite	4	Regular File	2025-03-12 오전 5:41:...
plum.sqlite-shm	32	Regular File	2025-03-12 오전 5:55:...
plum.sqlite-wal	242	Regular File	2025-03-12 오전 5:55:...

```

2a0c0 63 68 73 22 3a 20 5b 0d-0a 20 20 20 20 20 20 7b cks": [ .. {
2a0d0 0d 0a 20 20 20 20 20 20-20 20 22 69 64 22 3a 20 .. "id":
2a0e0 22 61 65 65 61 35 61 31-33 2d 65 35 62 34 2d 34 "acea5a13-e5b4-4
2a0f0 62 37 34 2d 61 33 61 32-2d 66 34 30 32 39 30 32 b74-a3a2-f402902
2a100 30 37 35 36 39 22 2c 0d-0a 20 20 20 20 20 20 07569", ..
2a110 20 22 74 79 70 65 22 3a-20 22 70 61 72 61 67 72 "type": "paragr
2a120 61 70 68 22 2c 0d 0a 20-20 20 20 20 20 20 22 aph", .. "
2a130 63 6f 6e 74 65 6e 74 22-3a 20 5b 0d 0a 20 20 20 content": [ ..
2a140 20 20 20 20 20 20 20 20 7b-0d 0a 20 20 20 20 20 { ..
2a150 20 20 20 20 20 20 22 74-65 78 74 22 3a 20 22 53 "text": "S
2a160 63 68 65 64 75 6c 65 20-61 70 70 6f 69 6e 74 6d chedule appointm
2a170 65 6e 74 3a 20 4d 65 65-74 20 61 74 20 4d 61 72 ent: Meet at Mar
2a180 6b e2 80 99 73 20 64 6f-6f 72 73 74 65 70 20 6f kâ--s doorstep o
2a190 6e 20 31 34 20 4d 61 72-63 68 20 32 30 32 35 20 n 14 March 2025
2a1a0 61 74 20 31 37 3a 3a 30-22 2c 0d 0a 20 20 20 20 at 17:40", ..
2a1b0 20 20 20 20 20 20 20 20 20-22 73 74 79 6c 65 73 22 "styles"
2a1c0 3a 20 5b 5d 0d 0a 20 20-20 20 20 20 20 20 20 : [ ] ..
2a1d0 7d 0d 0a 20 20 20 20 20-20 20 5d 2c 0d 0a 20 } ..
2a1e0 20 20 20 20 20 20 20 22-62 6c 6f 63 6b 53 74 79 "blockSty
2a1f0 6c 65 73 22 3a 20 7b 7d-0d 0a 20 20 20 20 20 20 les": { } ..
2a200 7d 0d 0a 20 20 20 20 5d-0d 0a 20 20 7d 2c 0d 0a } ..
2a210 20 20 22 63 72 65 61 74-65 64 41 74 22 3a 20 22 "createdAt": "
2a220 32 30 32 35 2d 30 33 2d-31 32 54 30 35 3a 34 30 2025-03-12T05:40
2a230 3a 32 35 5a 22 2c 0d 0a-20 20 22 6c 61 73 74 4d :25Z", .. "lastM
2a240 6f 64 69 66 69 65 64 22-3a 20 22 32 30 32 35 2d odified": "2025-
2a250 30 33 2d 31 32 54 30 35-3a 34 30 3a 35 34 5a 22 03-12T05:40:54Z"
2a260 2c 0d 0a 20 20 22 64 6f-63 75 6d 65 6e 74 4d 6f , .. "documentMo
2a270 64 69 66 69 65 64 41 74-22 3a 20 22 32 30 32 35 difiedAt": "2025
2a280 2d 30 33 2d 31 32 54 30-35 3a 34 30 3a 35 34 2e -03-12T05:40:54.
2a290 33 35 35 5a 22 2c 0d 0a-20 20 22 6d 65 64 69 61 355Z", .. "media
2a2a0 22 3a 20 5b 5d 2c 0d 0a-20 20 22 74 61 67 73 22 ": [ ], .. "tags"
2a2b0 3a 20 5b 5d 0d 0a 7d 05-39 35 63 36 39 31 63 34 : [ ] ..
2a2c0 2d 34 66 37 39 2d 34 62-33 37 2d 38 66 37 61 2d -4f79-4b37-8f7a-
2a2d0 35 64 39 61 66 32 39 33-30 64 63 61 64 38 31 36 5d9af2930dca816
2a2e0 39 32 31 61 2d 32 31 33-64 2d 34 37 34 35 2d 62 921a-213d-4745-b
2a2f0 65 64 31 2d 65 63 31 61-66 32 61 33 66 32 61 65 ed1-eclaf2a3f2ae
2a300 08 dd 61 28 63 5b 6a 80-08 dd 61 28 74 da a2 30 ·ÿa(c) ·ÿa(t)·e0
2a310 00 00 01 00 0d 82 21 09-08 00 19 08 00 00 00 00 .....!.....
2a320 00 08 00 55 55 06 00 06-4d 61 6e 61 67 65 64 50 ...UU...ManagedP
2a330 6f 73 69 74 69 6f 6f 7d-44 65 76 69 63 65 49 64 ception-PartiaT4
    
```

FTK에서 주어진 파일을 열고 Appdata local packages microsoftstickynotes_ localstate plum.sqlite-wal 에서 써졌던 메모를 확인하니 "text": "Schedule appointment: Meet at Mark?s doorstep on 14 March 2025 at 17:40", 를 얻을 수 있었다.