Dreamhack-Track_the_file

일단 ftk로 열어서 [root]\$LogFile 이 경로로 들어간다

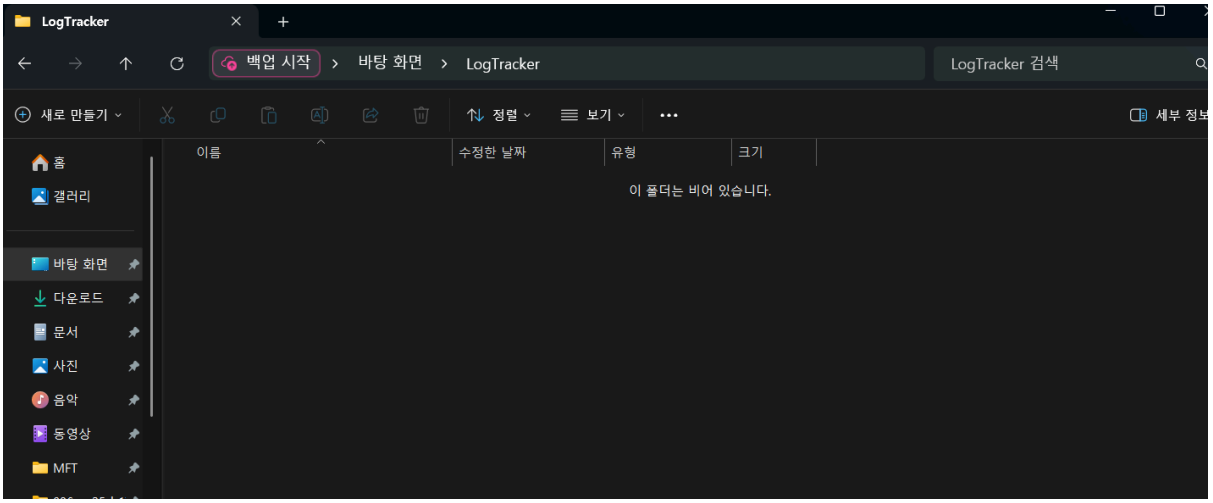
우선 우리는 logfile과 mft를 다운받아야 하는데 이 둘을 같은 경로에 다운받아야 한다.

그 다음 NTFS log tracker에 들어가서

이렇게 로그파일과 mft, db파일 경로 3가지를 적어주고 parse를 누른다.

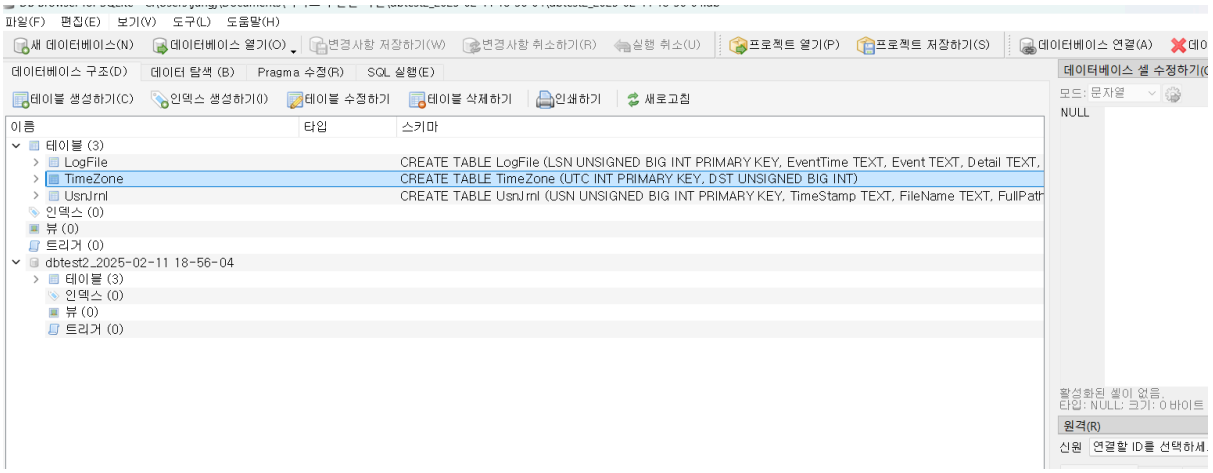
근데 이 뒤에 이제 디비 파일이 생성이 되어야 하는데...

난 계속 프로그램이 갑자기 꺼지고

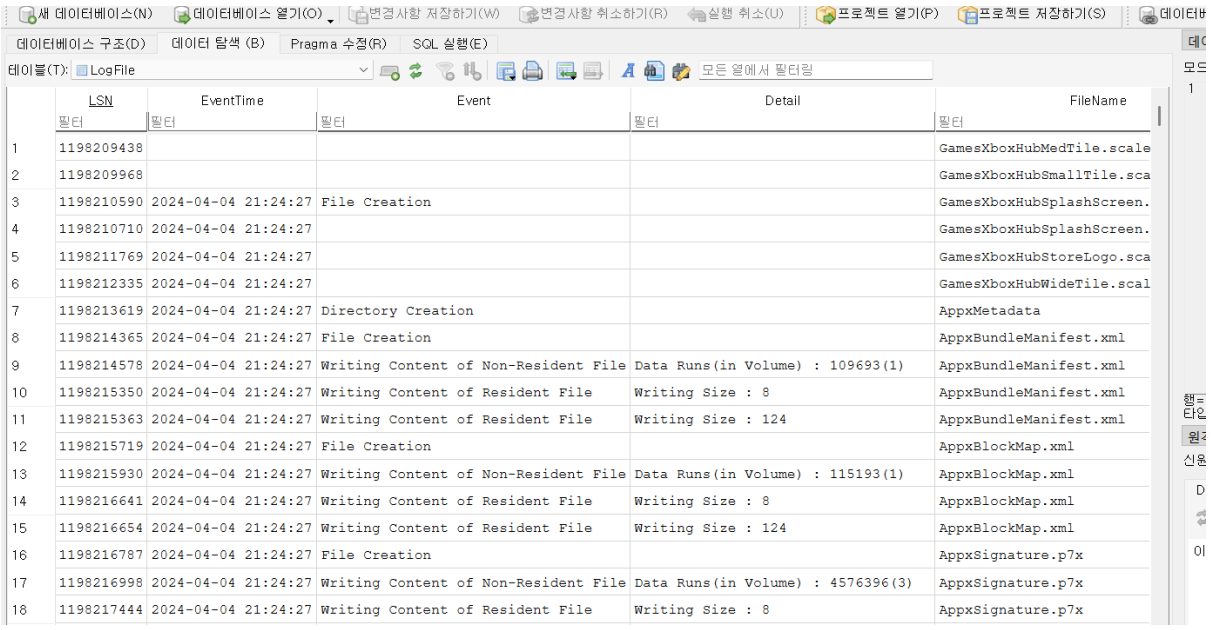


파일에 아무것도 없다...ㅠㅠ 아무래도 용량 문제 같다...

그래서!! 선호햄이 포렌식 톡방에 올린 디비 파일을 이용하기로 했다....허허 감사합니다 선호햄



sqlite로 열고 데이터베이스 연결을 누르면 다음과 같이 테이블이 뜬다.

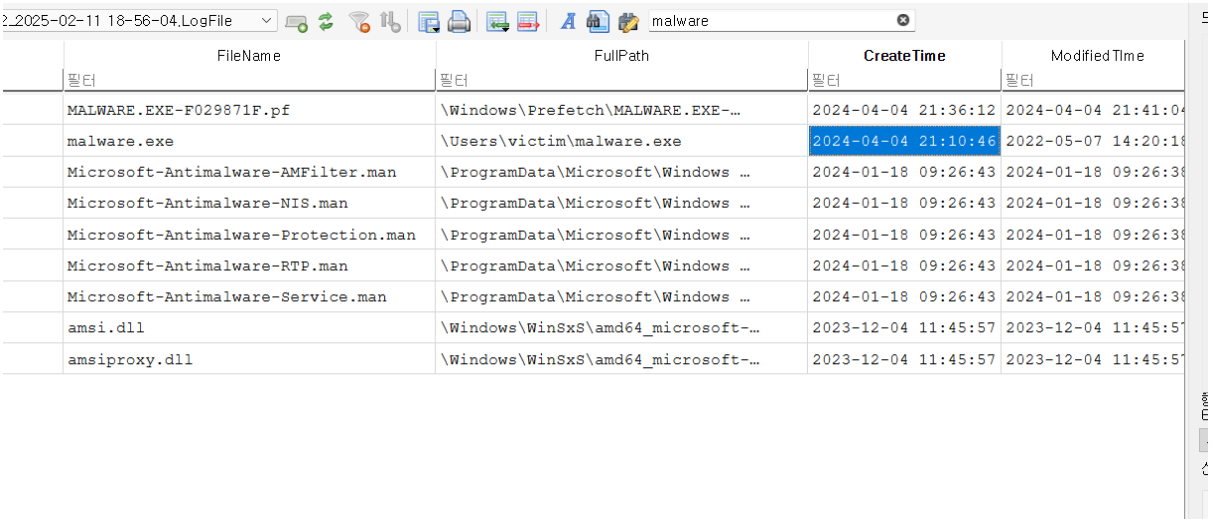


	LSN	EventTime	Event	Detail	FileName
1	1198209438				GamesXboxHubMedTile.scale
2	1198209968				GamesXboxHubSmallTile.sca
3	1198210590	2024-04-04 21:24:27	File Creation		GamesXboxHubSplashScreen.
4	1198210710	2024-04-04 21:24:27			GamesXboxHubSplashScreen.
5	1198211769	2024-04-04 21:24:27			GamesXboxHubStoreLogo.sca
6	1198212335	2024-04-04 21:24:27			GamesXboxHubWideTile.scal
7	1198213619	2024-04-04 21:24:27	Directory Creation		AppxMetadata
8	1198214365	2024-04-04 21:24:27	File Creation		AppxBundleManifest.xml
9	1198214578	2024-04-04 21:24:27	Writing Content of Non-Resident File	Data Runs(in Volume) : 109693(1)	AppxBundleManifest.xml
10	1198215350	2024-04-04 21:24:27	Writing Content of Resident File	Writing Size : 8	AppxBundleManifest.xml
11	1198215363	2024-04-04 21:24:27	Writing Content of Resident File	Writing Size : 124	AppxBundleManifest.xml
12	1198215719	2024-04-04 21:24:27	File Creation		AppxBlockMap.xml
13	1198215930	2024-04-04 21:24:27	Writing Content of Non-Resident File	Data Runs(in Volume) : 115193(1)	AppxBlockMap.xml
14	1198216641	2024-04-04 21:24:27	Writing Content of Resident File	Writing Size : 8	AppxBlockMap.xml
15	1198216654	2024-04-04 21:24:27	Writing Content of Resident File	Writing Size : 124	AppxBlockMap.xml
16	1198216787	2024-04-04 21:24:27	File Creation		AppxSignature.p7x
17	1198216998	2024-04-04 21:24:27	Writing Content of Non-Resident File	Data Runs(in Volume) : 4576396(3)	AppxSignature.p7x
18	1198217444	2024-04-04 21:24:27	Writing Content of Resident File	Writing Size : 8	AppxSignature.p7x

데이터베이스 탐색에 들어가면 다음과 같이 테이블의 데이터를 볼 수가 있다.

문제를 보면 malware.exe라는 파일이 시스템에 복사된 시간을 찾으라고 하고있다.

일단 malware가 생성되었으므로 필터링 기능을 이용해서 malware를 검색하여 준다



	FileName	FullPath	CreateTime	ModifiedTime
	MALWARE.EXE-F029871F.pf	\Windows\Prefetch\MALWARE.EXE-…	2024-04-04 21:36:12	2024-04-04 21:41:0
	malware.exe	\Users\victim\malware.exe	2024-04-04 21:10:46	2022-05-07 14:20:1
	Microsoft-Antimalware-AMFilter.man	\ProgramData\Microsoft\Windows …	2024-01-18 09:26:43	2024-01-18 09:26:3
	Microsoft-Antimalware-NIS.man	\ProgramData\Microsoft\Windows …	2024-01-18 09:26:43	2024-01-18 09:26:3
	Microsoft-Antimalware-Protection.man	\ProgramData\Microsoft\Windows …	2024-01-18 09:26:43	2024-01-18 09:26:3
	Microsoft-Antimalware-RTP.man	\ProgramData\Microsoft\Windows …	2024-01-18 09:26:43	2024-01-18 09:26:3
	Microsoft-Antimalware-Service.man	\ProgramData\Microsoft\Windows …	2024-01-18 09:26:43	2024-01-18 09:26:3
	amsi.dll	\Windows\WinSxS\amd64_microsoft-…	2023-12-04 11:45:57	2023-12-04 11:45:5
	amsiproxy.dll	\Windows\WinSxS\amd64_microsoft-…	2023-12-04 11:45:57	2023-12-04 11:45:5

그 중에서 생성된 시간을 찾으라 하였으니 malware.exe에서 생성된 저 시간을 플래그로 적어주면 된다~~

FLAG: DH{2024_04_04_21_10_46}