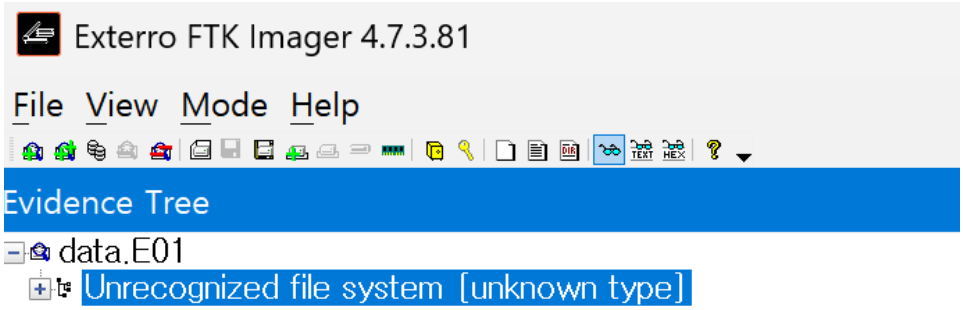
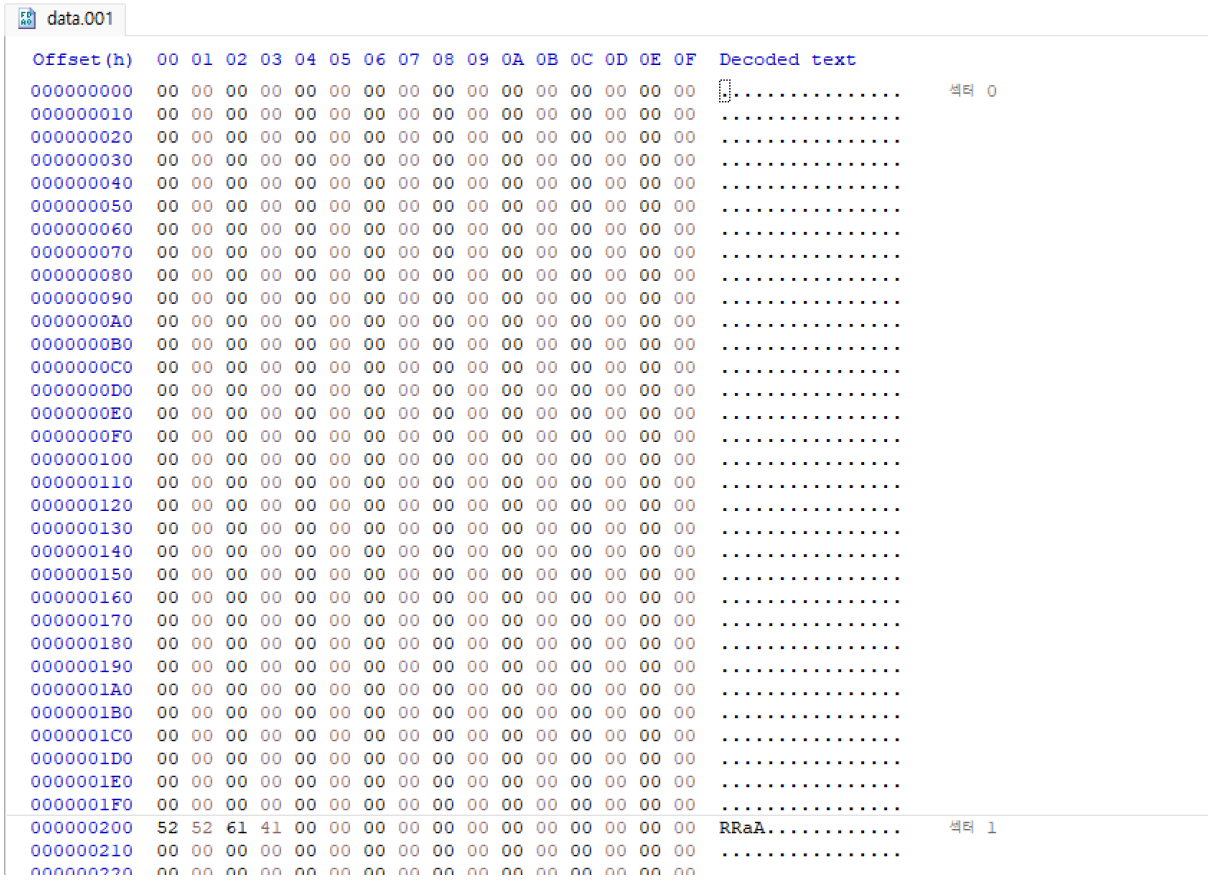


문제 이미지를 ftk imager로 열어보면 파티션이 훼손되어 있음을 확인할 수 있다.

파티션 복구를 위해 raw 파일로 export 해준다.

HxD에서 [도구]-[디스크 이미지 열기]를 통해 생성한 이미지를 열어본다.



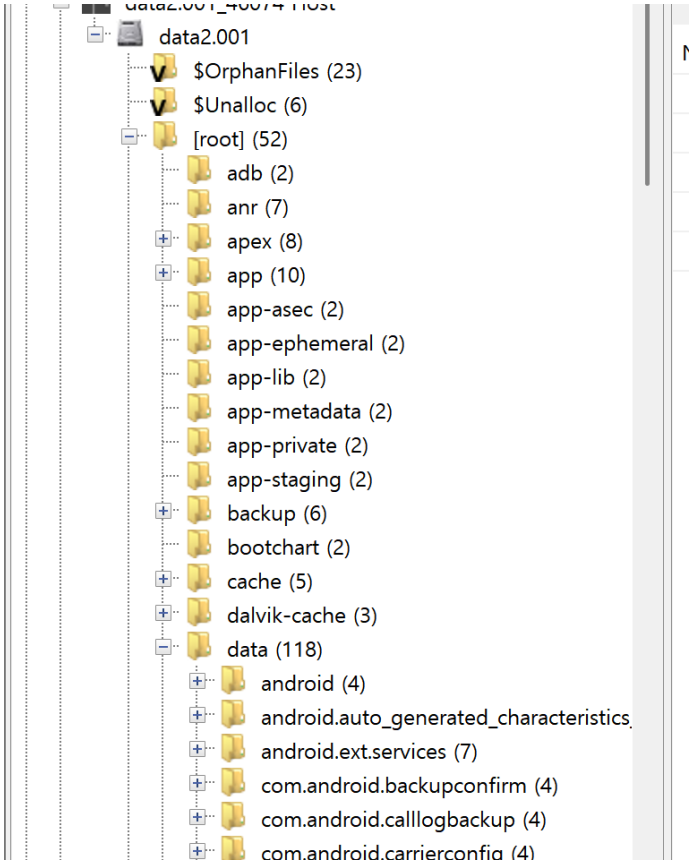
FAT32 BR 다음 섹터에 존재하는 'RRaA' 문자열이 1번 섹터에 있음을 확인할 수 있으며,

0번 섹터에 6을 더한 6번 섹터로 이동해 BR을 복사해 0번 섹터에 [붙여넣기 쓰기] 해준다.

data.001

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
000000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	4A	0B	ëX.MSDOS5.0...J.	섹터 0
000000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	20	00	00	00	.....ø..?.ÿ. ...	
000000020	E0	EB	E9	00	5B	3A	00	00	00	00	00	00	02	00	00	00	àëé.[:..........	
000000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	....	
000000040	80	00	29	95	3F	09	98	4E	4F	20	4E	41	4D	45	20	20	€.)•?.˜NO NAME	
000000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽÑ¼ô	
000000060	7B	8E	C1	8E	D9	BD	00	7C	88	56	40	88	4E	02	8A	56	{ŽÁŽÙ½.|ˆV@ˆN.ŠV	
000000070	40	B4	41	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	@´A»ªUÍ.r..ûUªu.	
000000080	F6	C1	01	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	öÁ.t.þF.ë-ŠV@´.Í	
000000090	13	73	05	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	.s.¹ÿÿŠñf.¶Æ@f.¶	
0000000A0	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	Ñ€â?÷â†ÍÀí.Af.·É	
0000000B0	66	F7	E1	66	89	46	F8	83	7E	16	00	75	39	83	7E	2A	f÷áf‰Føƒ~..u9ƒ~*	
0000000C0	00	77	33	66	8B	46	1C	66	83	C0	0C	BB	00	80	B9	01	.w3f‹F.fƒÀ.».€¹.	
0000000D0	00	E8	2C	00	E9	A8	03	A1	F8	7D	80	C4	7C	8B	F0	AC	.è,.é¨.¡ø}€Ä|‹ð¬	
0000000E0	84	C0	74	17	3C	FF	74	09	B4	0E	BB	07	00	CD	10	EB	„Àt.<ÿt.´.».Í.ë	
0000000F0	EE	A1	FA	7D	EB	E4	A1	7D	80	EB	DF	98	CD	16	CD	19	î¡ú}ëä¡}€ëß˜Í.Í.	
000000100	66	60	80	7E	02	00	0F	84	20	00	66	6A	00	66	50	06	f`€~...„ .fj.fP.	
000000110	53	66	68	10	00	01	00	B4	42	8A	56	40	8B	F4	CD	13	Sfh....´BŠV@‹ôÍ.	
000000120	66	58	66	58	66	58	66	58	EB	33	66	3B	46	F8	72	03	fXfXfXfXë3f;Før.	
000000130	F9	EB	2A	66	33	D2	66	0F	B7	4E	18	66	F7	F1	FE	C2	ùë*f3Òf.·N.f÷ñþÂ	
000000140	8A	CA	66	8B	D0	66	C1	EA	10	F7	76	1A	86	D6	8A	56	ŠÊf‹ÐfÁê.÷v.†ÖŠV	
000000150	40	8A	E8	C0	E4	06	0A	CC	B8	01	02	CD	13	66	61	0F	@ŠèÀä..Ì¸..Í.fa.	
000000160	82	74	FF	81	C3	00	02	66	40	49	75	94	C3	42	4F	4F	‚tÿ.Ã..f@Iu”ÃBOO	
000000170	54	4D	47	52	20	20	20	20	00	00	00	00	00	00	00	00	TMGR	
000000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....	
000000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....	
0000001A0	00	00	00	00	00	00	00	00	00	00	00	00	0D	0A	44	69	..............Di	
0000001B0	73	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	sk errorÿ..Press	
0000001C0	20	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	any key to rest	
0000001D0	61	72	74	0D	0A	00	00	00	00	00	00	00	00	00	00	00	art.............	
0000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....	
0000001F0	00	00	00	00	00	00	00	00	AC	01	B9	01	00	00	55	AA	........¬.¹...Uª	
000000200	52	52	61	41	00	00	00	00	00	00	00	00	00	00	00	00	RRaA............	섹터 1
000000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....	

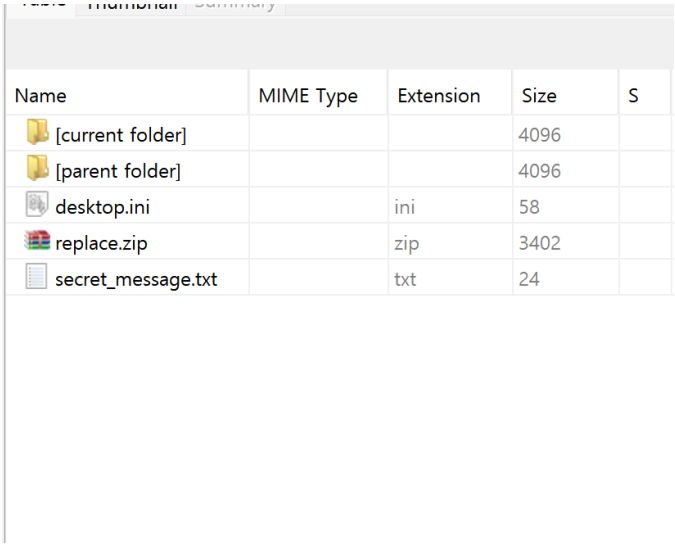
복구한 이미지를 autopsy에서 열어보면 내부 데이터를 확인할 수 있다.



문제 이름인 "Sorting list using hmm.." 에서 힌트를 줬듯, 이미지 파일 안에는 "hmm.."을 이름으로 하는 폴더가 있음을 알 수 있다.

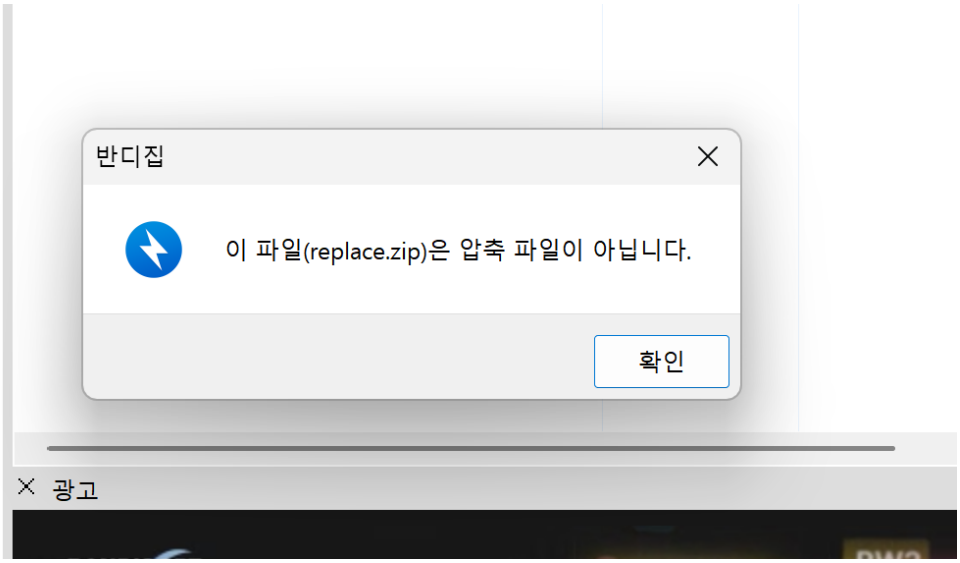
경로 : /img_data2.001/[root]/data/com.mrs.wear_file_explorer/files/hmm

해당 폴더를 들어가 확인해 보면 secret_message.txt와 replace.zip 파일을 확인할 수 있다.

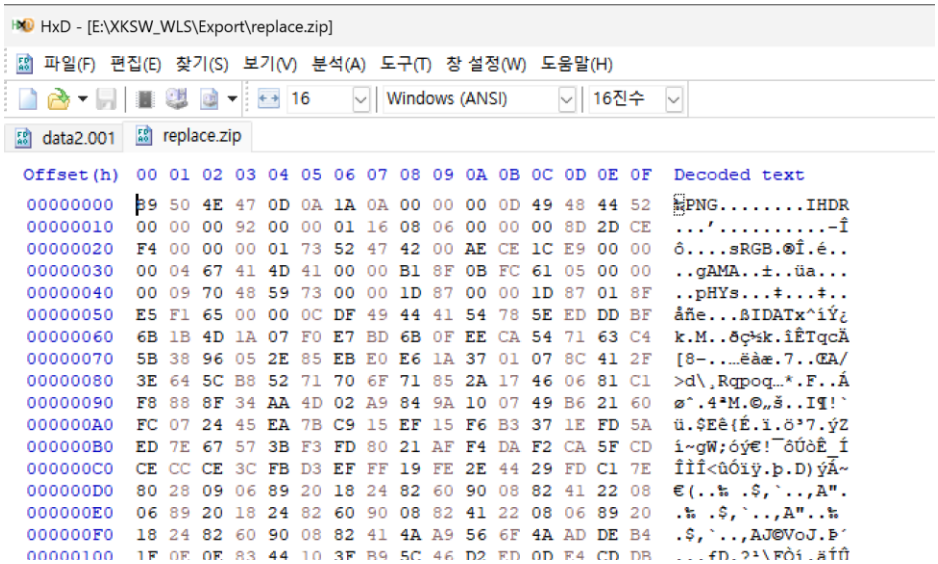


Name	MIME Type	Extension	Size	S
[current folder]			4096	
[parent folder]			4096	
desktop.ini		ini	58	
replace.zip		zip	3402	
secret_message.txt		txt	24	

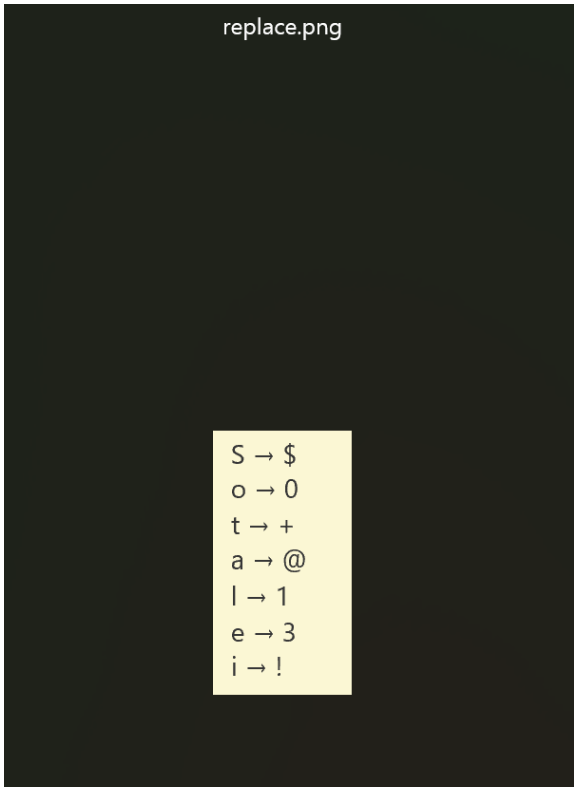
[replace.zip]



확장자가 변조된 것으로, HxD를 이용해 파일 시그니처 확인 해보면 png 시그니처임을 확인할 수 있다.

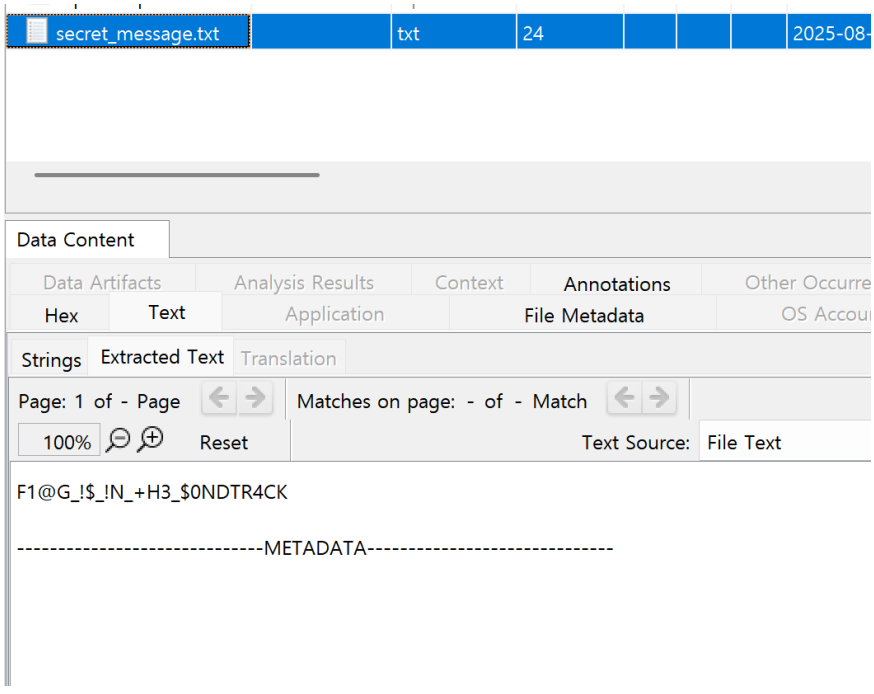


시그니처에 맞는 확장자인 png로 변경해준다.



위와 같은 사진을 확인할 수 있다.

[secret_message.txt]



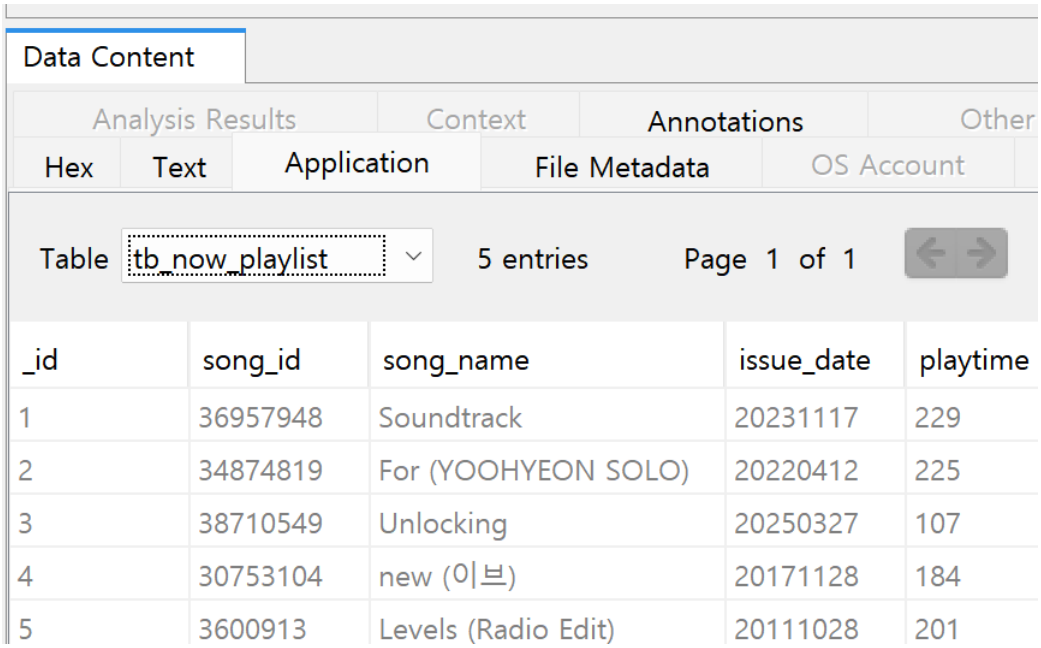
Secret_message.txt 파일 내용을 통해 사운드트랙을 만들 수 있는 앱 아티팩트를 확인해 본다.

설치된 앱 중 음악 앱은 멜론이 유일하니 멜론 경로를 확인한다.

경로 : /img_data2.001/[root]/data/com.iloen.melon

들어있는 폴더 중 /databases에 들어가 wear_db를 통해 플레이리스트를 확인할 수 있다.

테이블명 : tb_now_playlistㄴ



_id	song_id	song_name	issue_date	playtime
1	36957948	Soundtrack	20231117	229
2	34874819	For (YOOHYEON SOLO)	20220412	225
3	38710549	Unlocking	20250327	107
4	30753104	new (이브)	20171128	184
5	3600913	Levels (Radio Edit)	20111028	201

앞에서 발견한 replace.zip의 복구 사진을 참고해 플레이리스트를 나열하면 된다.

Flag : XKSW{$0und+r@ck_f0r_un10ck!ng_n3w_13v31$}