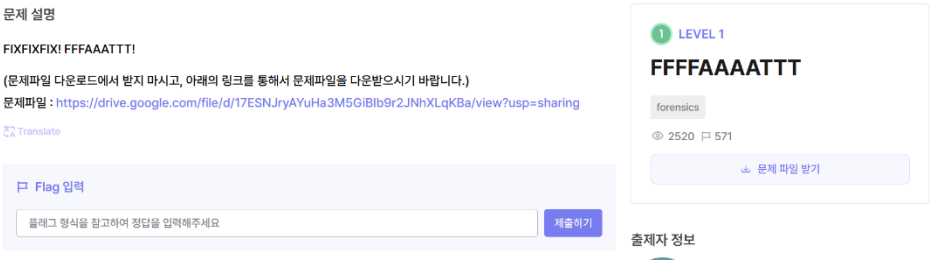
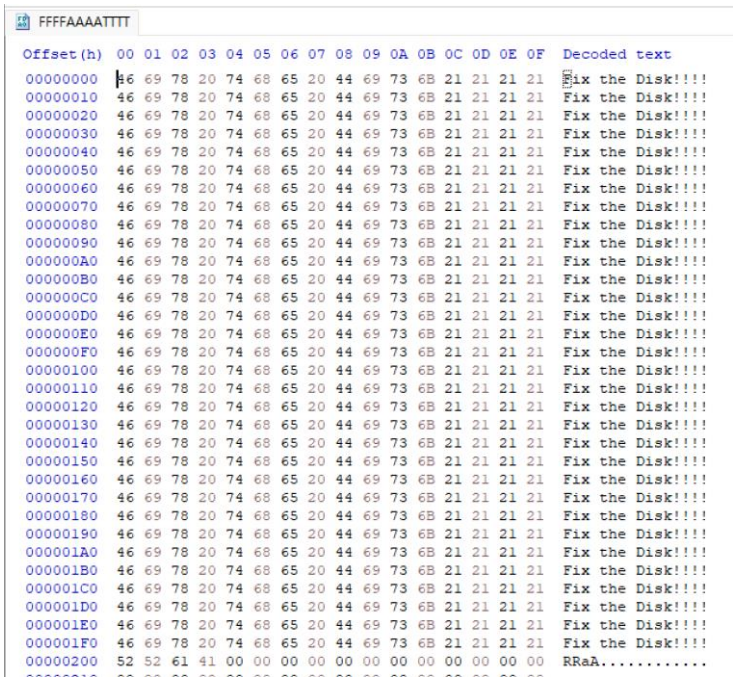
3. 관련 워게임 풀이

1) 드림핵 “FFFFAAAATTT”



드림핵의 FFFFAAAATTT를 풀이해보도록 하겠다. 문제 이름으로 보아 아마 FAT32에 대한 문제일 것으로 보인다.

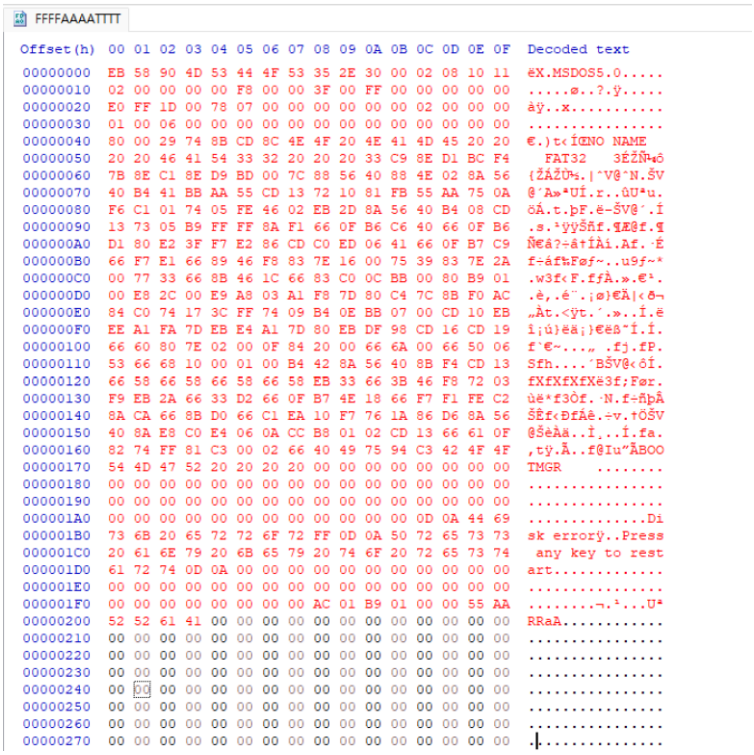

FFFFAAAATTT

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000010	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000020	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000030	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000040	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000050	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000060	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000070	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000080	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000090	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000A0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000B0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000C0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000D0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000E0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000000F0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000100	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000110	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000120	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000130	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000140	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000150	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000160	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000170	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000180	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000190	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000001A0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000001B0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000001C0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000001D0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000001E0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
000001F0	46	69	78	20	74	68	65	20	44	69	73	6B	21	21	21	21	Fix the Disk!!!!
00000200	52	52	61	41	00	00	00	00	00	00	00	00	00	00	00	00	RRaA.....

문제 파일을 다운받은 후, HxD로 살펴보니, ‘Fix the Disk!!’라는 문구가 바로 맨처음부터 나온다. 아마 디스크가 손상되어서 고치라는 것 같아 보인다. 일반적인 FAT32의 구조는 맨처음에 EB 58 90으로 시작하여 FAT32 파일 시스템을 가르키는 46 41 54 33 32 20 20 20가 포함된 Reserved Area 부분이 가장 맨처음에 나와야 한다. 따라서 컴퓨터 부팅을 시작하는 데 필요한 데이터를 유지/관리하는 데에 사용되는 하드 디스크 저장소 공간 섹션인 부트 레코드 부분이 제대로 있지 않고 손상된 것으로 보인다. FAT32는 보통 부트 레코드 뒤에 바로 백업 부트레코드를 가지고 있으므로, 백업 부트 레코드를 찾아보려고 한다.

```
00000C00  EB 58 90 4D 53 44 4F 53 35 2E 30 00 02 08 10 11  ëX.MSDOS5.0.....
00000C10  02 00 00 00 00 F8 00 00 3F 00 FF 00 00 00 00 00  .....ø..?.ÿ.....
00000C20  E0 FF 1D 00 78 07 00 00 00 00 00 00 02 00 00 00  àÿ..x...........
00000C30  01 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000C40  80 00 29 74 8B CD 8C 4E 4F 20 4E 41 4D 45 20 20  €.)t‹ÍŒNO NAME
00000C50  20 20 46 41 54 33 32 20 20 20 33 C9 8E D1 BC F4    FAT32   3ÉŽÑ¼ô
00000C60  7B 8E C1 8E D9 BD 00 7C 88 56 40 88 4E 02 8A 56  {ŽÁŽÙ½.|ˆV@ˆN.ŠV
00000C70  40 B4 41 BB AA 55 CD 13 72 10 81 FB 55 AA 75 0A  @´A»ªUÍ.r..ûUªu.
00000C80  F6 C1 01 74 05 FE 46 02 EB 2D 8A 56 40 B4 08 CD  öÁ.t.þF.ë-ŠV@´.Í
00000C90  13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66 0F B6  .s.¹ÿÿŠñf.¶Æ@f.¶
00000CA0  D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F B7 C9  Ñ€â?÷â†ÍÀí.Af.·É
00000CB0  66 F7 E1 66 89 46 F8 83 7E 16 00 75 39 83 7E 2A  f÷áf‰Føƒ~..u9ƒ~*
00000CC0  00 77 33 66 8B 46 1C 66 83 C0 0C BB 00 80 B9 01  .w3f‹F.fƒÀ.».€¹.
00000CD0  00 E8 2C 00 E9 A8 03 A1 F8 7D 80 C4 7C 8B F0 AC  .è,.é¨.¡ø}€Ä|‹ð¬
00000CE0  84 C0 74 17 3C FF 74 09 B4 0E BB 07 00 CD 10 EB  „Àt.<ÿt.´.».Í.ë
00000CF0  EE A1 FA 7D EB E4 A1 7D 80 EB DF 98 CD 16 CD 19  î¡ú}ëä¡}€ëß˜Í.Í.
00000D00  66 60 80 7E 02 00 0F 84 20 00 66 6A 00 66 50 06  f`€~...„ .fj.fP.
00000D10  53 66 68 10 00 01 00 B4 42 8A 56 40 8B F4 CD 13  Sfh....´BŠV@‹ôÍ.
00000D20  66 58 66 58 66 58 66 58 EB 33 66 3B 46 F8 72 03  fXfXfXfXë3f;Før.
00000D30  F9 EB 2A 66 33 D2 66 0F B7 4E 18 66 F7 F1 FE C2  ùë*f3Òf.·N.f÷ñþÂ
00000D40  8A CA 66 8B D0 66 C1 EA 10 F7 76 1A 86 D6 8A 56  ŠÊf‹ÐfÁê.÷v.†ÖŠV
00000D50  40 8A E8 C0 E4 06 0A CC B8 01 02 CD 13 66 61 0F  @ŠèÀä..Ì¸..Í.fa.
00000D60  82 74 FF 81 C3 00 02 66 40 49 75 94 C3 42 4F 4F  ‚tÿ.Ã..f@Iu”ÃBOO
00000D70  54 4D 47 52 20 20 20 20 00 00 00 00 00 00 00 00  TMGR    ........
00000D80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000D90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000DA0  00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 44 69  ..............Di
00000DB0  73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73  sk errorÿ..Press
00000DC0  20 61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74   any key to rest
00000DD0  61 72 74 0D 0A 00 00 00 00 00 00 00 00 00 00 00  art.............
00000DE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000DF0  00 00 00 00 00 00 00 00 AC 01 B9 01 00 00 55 AA  ........¬.¹...Uª
00000E00  52 52 61 41 00 00 00 00 00 00 00 00 00 00 00 00  RRaA............
```

뒤에 부분을 살펴보니, EB 58 90으로 시작하는 백업 부트레코드를 찾을 수 있었다! RRaA가 나오는 부분까지가 백업 레코드로 이 부분을 복사하여 맨 첫 부분에 붙여넣어 보려고 한다.

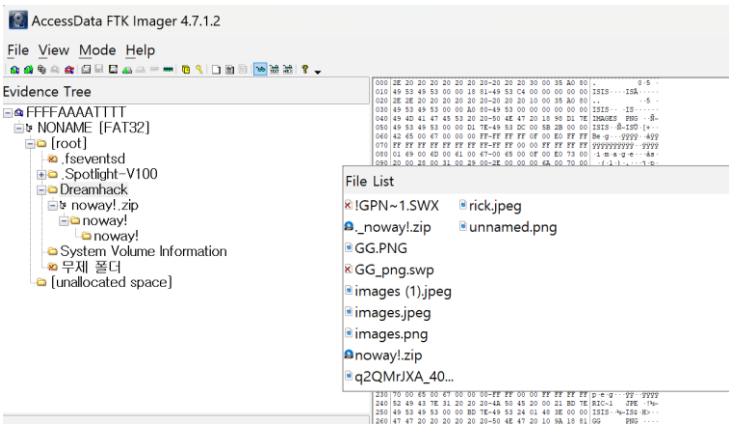


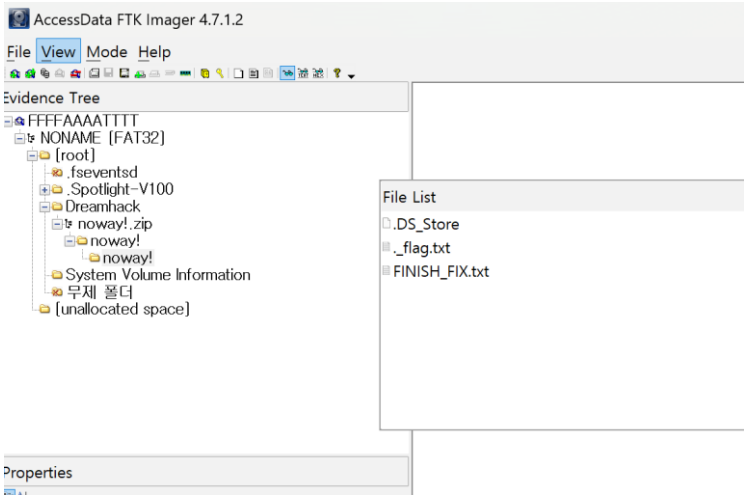
기존의 Fix the Disk!!의 RRaA 부분까지 전부 삭제하고, 아까 발견한 백업 부트레코드를 복사하여 삽입하였다.

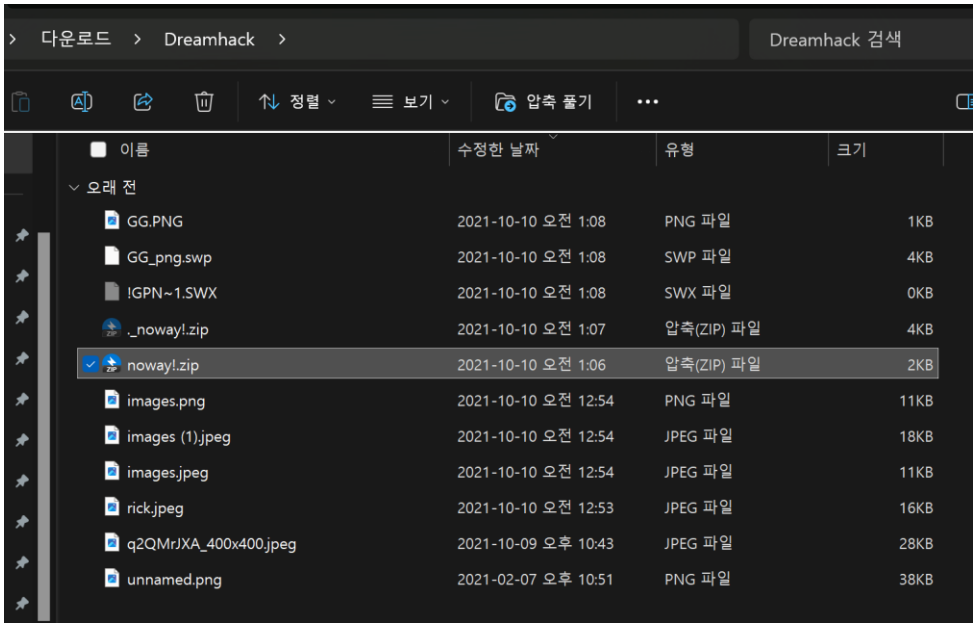
FFFFAAAATTTT

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
004D7000	50	4B	03	04	14	03	00	00	00	00	55	98	47	53	00	00	PK.....U˜GS..
004D7010	00	00	00	00	00	00	00	00	00	00	07	00	00	00	6E	6F	..............no
004D7020	77	61	79	21	2F	50	4B	03	04	14	03	01	00	08	00	71	way!/PK.......q
004D7030	7F	49	53	68	8D	56	1D	88	01	00	00	04	18	00	00	10	.ISh.V.^........
004D7040	00	00	00	6E	6F	77	61	79	21	2F	2E	44	53	5F	53	74	...noway!/.DS_St
004D7050	6F	72	65	CB	0D	72	7D	F4	F9	34	65	E6	DA	F2	9F	71	oreË.r}ôù4eæÚòŸq
004D7060	F3	20	2F	AD	A8	D7	78	DE	CA	FA	56	8B	CC	48	9F	20	ó /.¨×xÞÊúV‹ÌHŸ
004D7070	91	1B	08	96	CA	54	3F	B4	CF	E9	C9	01	72	74	3F	39	'..–ÊT?´ÏéÉ.rt?9
004D7080	98	78	59	02	2E	BF	71	DF	09	22	ED	F9	EA	BF	BF	C7	˜xY..¿qß."íùê¿¿Ç
004D7090	E9	6E	94	59	03	14	F0	63	CE	F1	1D	7B	10	31	51	74	én”Y..ðcÎñ.{.1Qt
004D70A0	3C	74	60	93	15	67	47	EC	3A	94	0C	50	1A	F3	31	FC	<t`“.gGì:”.P.ó1ü
004D70B0	E4	FD	15	C9	A4	D5	58	86	C4	04	32	69	22	E4	2D	A0	äý.É¤ÕX†Ä.2i"ä-
004D70C0	CA	4A	A2	2E	B1	19	DE	DB	F1	CA	A1	52	F4	B4	06	7F	ÊJ¢.±.ÞÛñÊ¡Rô´..
004D70D0	DE	8E	6B	37	D6	08	A2	A7	CC	47	5F	DF	2B	7F	4C	3C	ÞŽk7Ö.¢§ÌG_ß+.L<
004D70E0	EC	E9	F8	02	5D	3E	F7	50	88	6E	80	DD	DC	74	41	37	ìéø.]>÷P^n€ÝÜtA7
004D70F0	3B	2D	AE	E3	78	2B	C9	15	7E	B0	C7	FA	5A	E2	5B	56	;-®ãx+É.~°ÇúZâ[V
004D7100	13	4F	82	0A	9D	CE	8E	2D	5D	85	9D	39	16	98	29	B8	.O‚..ÎŽ-]….9.˜)¸
004D7110	94	46	B6	42	FF	1B	02	84	72	4A	9F	B2	A6	70	DC	7A	”F¶Bÿ..„rJŸ²¦pÜz
004D7120	32	BA	C8	CE	4D	8A	6F	A4	B8	C0	B1	9D	9D	1A	A5	1C	2ºÈÎMŠo¤¸À±...¥.
004D7130	44	FF	13	DA	BE	90	D0	BC	7E	69	99	56	14	70	DB	A6	Dÿ.Ú¾.Ð¼~i™V.pÛ¦
004D7140	02	F1	C4	69	9B	D9	14	10	8A	4A	62	B1	2D	48	0F	89	.ñÄi›Ù..ŠJb±-H.‰
004D7150	C9	AC	E9	49	EF	60	06	95	66	BE	A4	6D	0B	AF	4C	22	É¬éIï`.•f¾¤m.¯L"
004D7160	C0	96	8D	34	62	4F	50	44	E8	49	A6	1E	94	5A	00	3C	À–.4bOPDèI¦.”Z.<
004D7170	C0	FA	B9	90	DB	F1	F4	EA	35	A7	3A	F6	E6	DB	BA	4D	Àú¹.ÛñôÊ5§:öæÛºM
004D7180	61	0B	05	C5	C6	2D	60	40	86	C2	81	39	2E	5E	21	5C	a..ÅÆ-`@†Â.9.^!\
004D7190	D2	C9	4B	48	CE	CA	F3	A2	CB	70	11	C0	17	BF	E9	79	ÒÉKHÎÊó¢Ëp.À.¿éy
004D71A0	66	F7	78	1C	A2	11	49	AC	83	BF	A2	7D	8F	D0	C5	27	f÷x.¢.I¬ƒ¿¢}.ÐÅ'
004D71B0	84	EC	7C	0A	C0	C7	3B	F8	C1	F8	FA	1D	B8	C3	21	13	„ì|.ÀÇ;øÁøú.¸Ã!.
004D71C0	A4	72	A6	F5	D4	BA	BA	76	83	43	30	AB	FA	CC	AD	47	¤r¦õÔººvƒC0«úÌ.G
004D71D0	84	D2	D9	6E	2C	9E	90	07	BD	3B	56	50	4B	03	04	14	„ÒÙn,ž..½;VPK...
004D71E0	03	00	00	00	00	00	80	49	53	00	00	00	00	00	00	00	......€IS.......
004D71F0	00	00	00	00	00	0E	00	00	00	6E	6F	77	61	79	21	2F	.........noway!/
004D7200	6E	6F	77	61	79	21	2F	50	4B	03	04	14	03	01	00	08	noway!/PK.......
004D7210	00	00	80	49	53	9A	7B	6D	D0	DC	00	00	00	04	18	00	..€ISš{mÐÜ......
004D7220	00	17	00	00	00	6E	6F	77	61	79	21	2F	6E	6F	77	61	.....noway!/nowa
004D7230	79	21	2F	2E	44	53	5F	53	74	6F	72	65	BA	F9	DB	EF	y!/.DS_StoreºùÛï
004D7240	5F	FF	0D	BE	61	B3	3A	53	69	04	EB	53	9A	A9	9E	7D	_ÿ.¾a³:Si.ëSš©ž}
004D7250	FF	E8	7E	02	31	5B	E1	D5	21	03	6B	31	AC	F0	DD	20	ÿè~.1[áÕ!.k1¬ðÝ
004D7260	98	A1	7C	C4	2B	D2	F0	12	0A	62	52	C6	7F	12	CD	57	˜¡|Ä+Òð..bRÆ..ÍW
004D7270	63	DA	B9	98	86	A1	5F	7A	C6	E0	33	DC	61	CD	BD	60	cÚ¹˜†¡_zÆà3Üaí½`
004D7280	55	8E	08	43	6A	C0	A9	A3	55	8B	8E	F3	32	9C	80	12	UŽ.CjÀ©£U‹Žó2œ€.

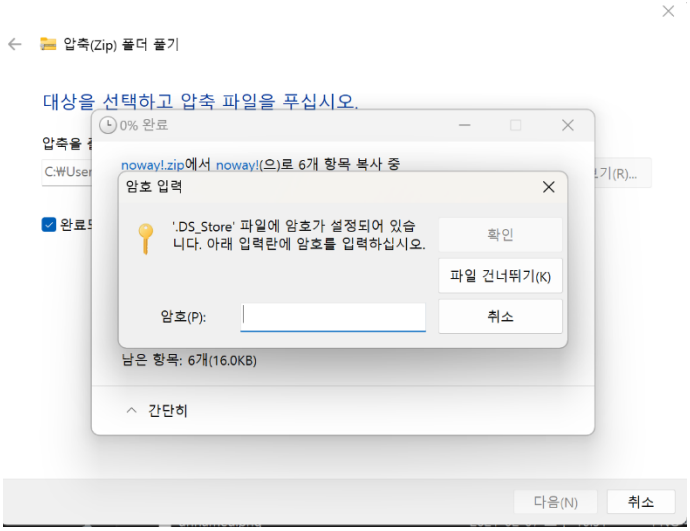
뒤에 부분을 살펴보니 50 4B 03 04 ZIP 파일 시그니처를 발견하였다. 해당 디스크에 ZIP 파일이 숨겨져 있는 것을 추정할 수 있었고, 제대로 고친 디스크를 분석해보면 저 ZIP 파일을 발견할 수 있을 것 같다고 생각이 들었다.



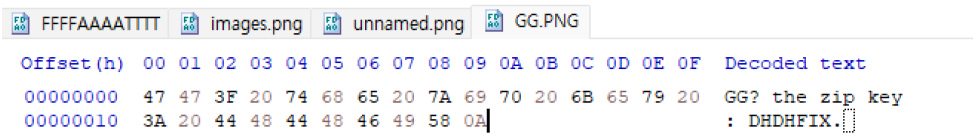




고친 디스크를 FTK Imager로 살펴보니, Dreamhack이라는 폴더가 있고, 그 폴더 안에 아까 위에서 발견한 noway! ZIP 파일이 있었다. Dreamhack에 있는 다른 파일들도 살펴보기 위해, 해당 폴더를 추출해주었다.



해당 noway! 파일을 압축 해제 하려고 하자 암호를 입력하라고 뜬다.



Dreamhack 폴더에 있는 열리지 않는 GG.PNG 파일을 혹시나 HxD로 살펴보니, zip key가 DHDHFIX라고 한다.