

# NTFS 파일 복구

23 고은이

# INDEX

- 1. NTFS 파일 구조
- NTFS와 FAT32 비교
- 2. NTFS 삭제 파일 복구 실습

# NTFS 파일 구조



## ○ VBR

-> MBR영역과 비슷하게 부트 섹터와 부트 코드가 위치하고 있는 영역

## ○ 마스터 파일 테이블(MFT)

-> 파일 이름, 생성 날짜, 액세스 권한, 크기 등을 포함하는 메타파일 데이터를 저장하는 디렉터리

## ○ MFT엔트리

-> MFT 안에 있는 각 파일이나 디렉터리에 해당하는 레코드

(resident, non-resident)

## ○ 클러스터

-> 디스크에 데이터를 저장하는 최소 단위

## ○ 메타파일

-> 파일 시스템을 정의 및 구성하고, 중요한 파일 시스템 데이터를 백업하고, 파일 시스템 변경 사항을 버퍼링하고, 여유 공간을 할당하는 등 메타 데이터를 효율적으로 구성하는데 도움을 줌

# NTFS와 FAT32 비교

- NTFS는 FAT32보다 더 큰 볼륨 크기와 파일 크기를 지원
- NTFS는 갑작스러운 오류에 대한 내결함성이 존재
- NTFS는 파일 압축 허용
- NTFS는 FAT32와 달리 다른 운영체제와 호환이 잘 안됨

=> NTFS는 더 큰 파일과 디스크를 처리하고 안전성과 보안 측면에서 뛰어남

# 파일 복구 순서

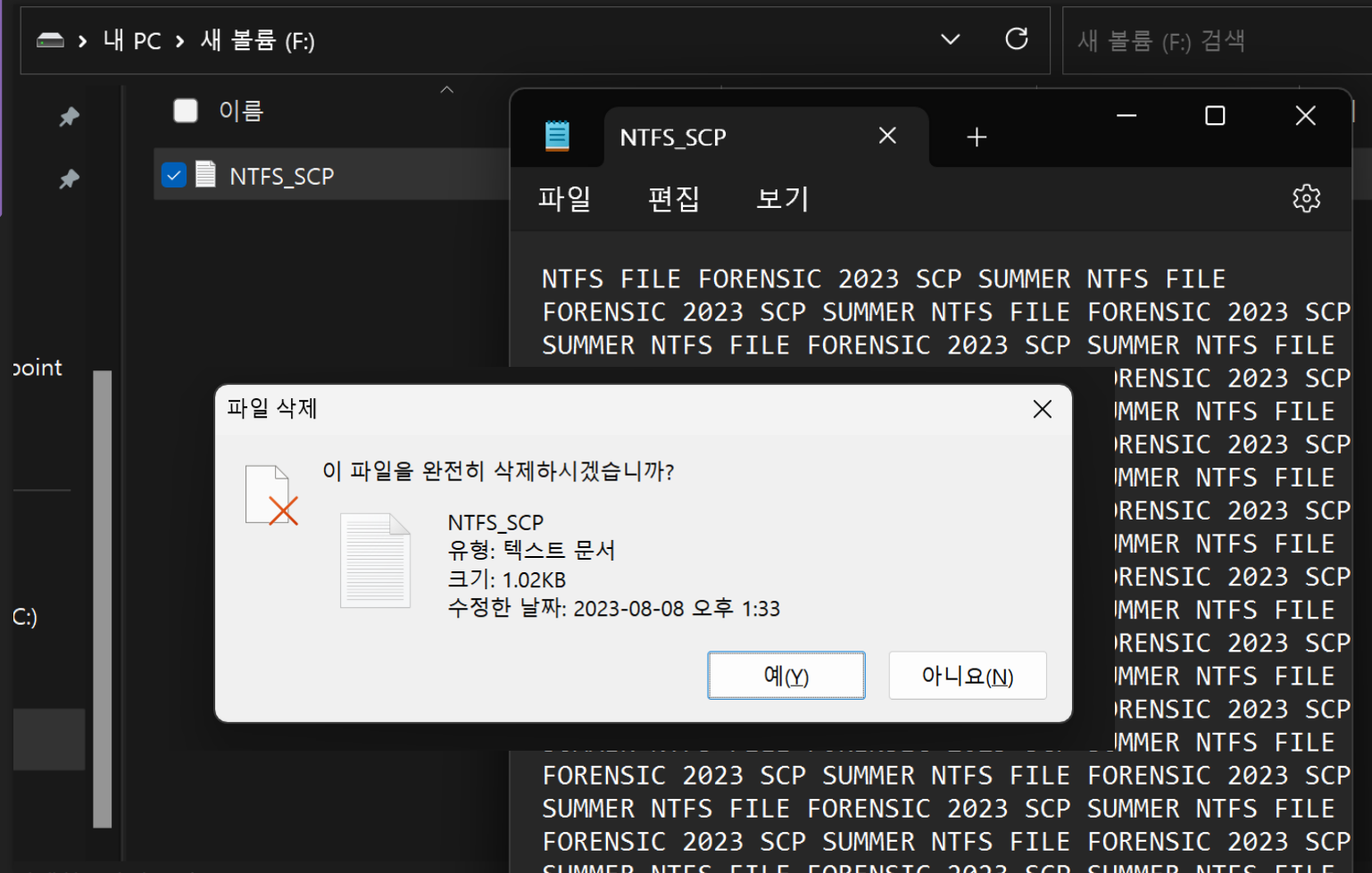
MBR에서 VBR 시작 주소  
구하고 이동

VBR에서 MFT파일 헤더 주소  
찾고 이동

MFT에서 데이터 영역 주소  
구하고 복구

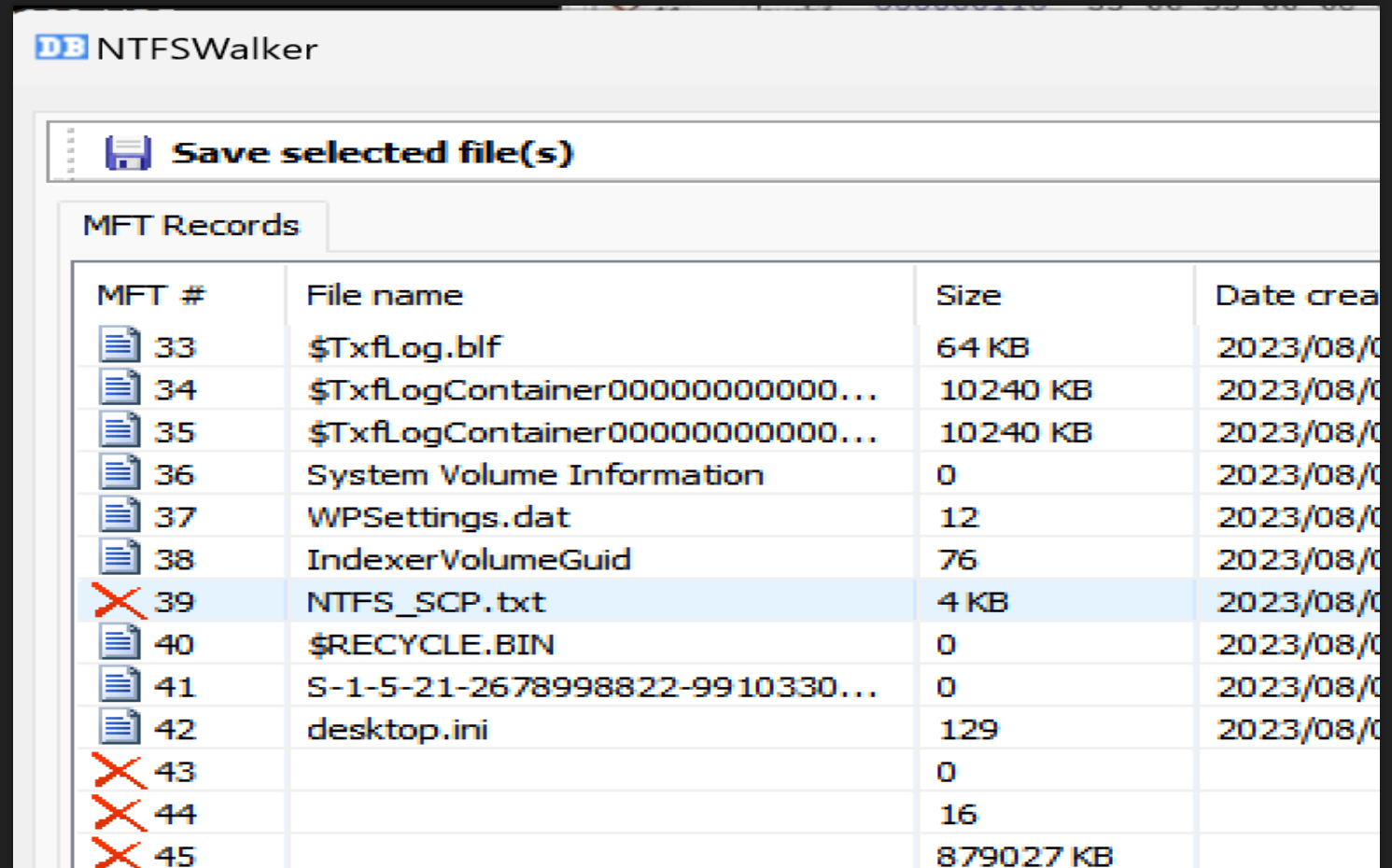
## NTFS 삭제 파일 복구 실습

NTFS로 포맷된 디스크에 텍스트 파일 생성  
후 영구 삭제



## NTFS 삭제 파일 복구 실습

NTFS Walker에서 MFT #값이 39번인 파일이 삭제되어 있는 것을 확인 할 수 있다.



DB NTFSWalker

Save selected file(s)

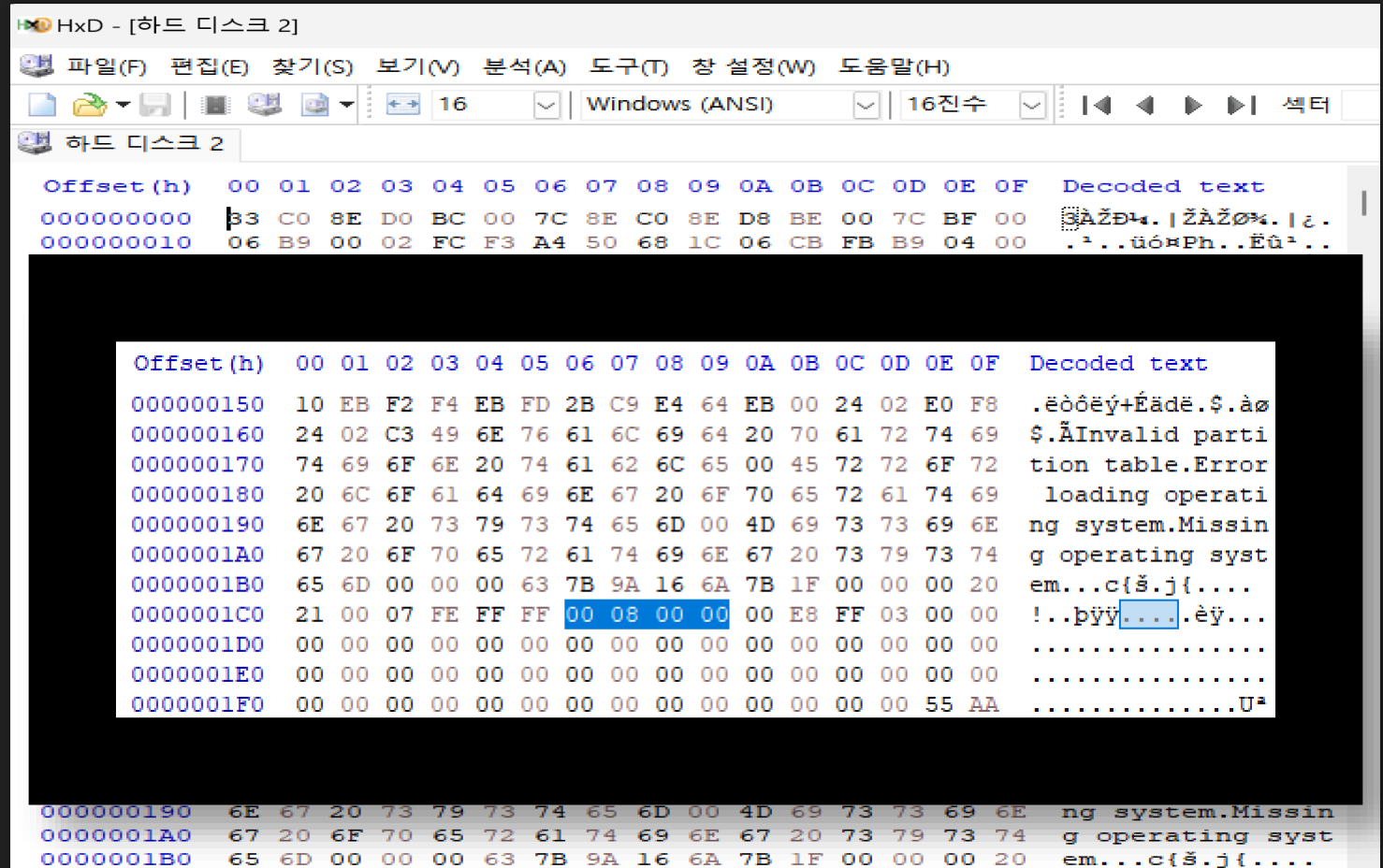
MFT Records

MFT #	File name	Size	Date crea
33	\$TxfLog.blf	64 KB	2023/08/0
34	\$TxfLogContainer000000000000...	10240 KB	2023/08/0
35	\$TxfLogContainer000000000000...	10240 KB	2023/08/0
36	System Volume Information	0	2023/08/0
37	WPSettings.dat	12	2023/08/0
38	IndexerVolumeGuid	76	2023/08/0
X 39	NTFS_SCP.txt	4 KB	2023/08/0
40	\$RECYCLE.BIN	0	2023/08/0
41	S-1-5-21-2678998822-9910330...	0	2023/08/0
42	desktop.ini	129	2023/08/0
X 43		0	
X 44		16	
X 45		879027 KB	

## NTFS 삭제 파일 복구 실습

HxD로 열고 첫번째 파티션 파란 부분이  
VBR섹터 번호다.

0x000800 = 2048 이므로  
2048섹터로 이동한다.





## NTFS 삭제 파일 복구 실습

$786432 * 8 + 2048 + 78$

⇒ 6293582 로 이동

Start of MFT(0x00000C0000)

⇒ 786432

클러스터 크기 08 / 8개 섹터

⇒ 8

VBR영역 2048섹터

⇒ 2048

삭제 파일의 MFT # 39 / 섹터 두개를 차지하기 때문에  
곱하기 2

⇒ 78

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000100000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ER.NTFS .....
000100010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	08	00	00	.....ø...?.ÿ.....
000100020	00	00	00	00	80	00	80	00	FF	E7	FF	03	00	00	00	00	.....€..ÿçÿ.....
000100030	00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00	.....
000100040	F6	00	00	00	01	00	00	00	0C	44	34	C8	59	34	C8	4C	ö.....D4ÈY4ÈL
000100050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	....ú3ÀŽĐ*. ûhÀ.
000100060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ë^...f.>..N
000100070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.'A»²UÍ.r..û
000100080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	U²u.÷Á..u.éÝ..fì
000100090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..'HŠ...<ö..í.
0001000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ÿfÄ.žX.rá;...uŮ&
0001000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Ä.....Z3Ů¹. +È
0001000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.....ŽÄÿ...è
0001000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Èwi...»Í.f#Àu-
0001000E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.ûTCPAu\$.ù..r..
0001000F0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h.»..hR..h..fSfSf
000100100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h...fa..Í.3À¿
000100110	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	...²ö.üó²ép...f`.
000100120	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f;...f.....fh...
000100130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..'BŠ..
000100140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...<óí.fÿ[Zfÿfÿ.
000100150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	...fÿ.....ŽÄÿ
000100160	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u²...faÄ;ö.è..
000100170	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	¡ú.è...öëÿ<ð-<.t.
000100180	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	'.»...Í.èöÄ..A di
000100190	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc
0001001A0	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52	curred...BOOTMGR
0001001B0	20	69	73	20	63	6F	6D	70	72	65	73	73	65	64	00	0D	is compressed..
0001001C0	0A	50	72	65	73	73	20	43	74	72	6C	2B	41	6C	74	2B	.Press Ctrl+Alt+

⇒ 51760 으로 이동

⇒ 6214

클러스터 크기 08

⇒ 8

## VBR영역 2048섹터

⇒ 2048

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0C0109C00	46	49	4C	45	30	00	03	00	CD	7A	00	01	00	00	00	00	FILE0...í z.....
0C0109C10	02	00	01	00	38	00	00	00	88	01	00	00	00	04	00	00	....8...^.....
0C0109C20	00	00	00	00	00	00	00	00	06	00	00	00	27	00	00	00	.....'...
0C0109C30	05	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	.....`...
0C0109C40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	.....H.....
0C0109C50	D4	A1	A4	41	B1	C9	D9	01	3D	D7	D7	80	B1	C9	D9	01	Ô; ¢A±ÉÜ. =××€±ÉÜ.
0C0109C60	3D	D7	D7	80	B1	C9	D9	01	3D	D7	D7	80	B1	C9	D9	01	=××€±ÉÜ. =××€±ÉÜ.
0C0109C70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0C0109C80	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00	.....
0C0109C90	00	00	00	00	00	00	00	00	30	00	00	00	78	00	00	00	.....0...x...
0C0109CA0	00	00	00	00	00	00	03	00	5A	00	00	00	18	00	01	00	.....Z.....
0C0109CB0	05	00	00	00	00	00	05	00	D4	A1	A4	41	B1	C9	D9	01	.....Ô; ¢A±ÉÜ.
0C0109CC0	D4	A1	A4	41	B1	C9	D9	01	D4	A1	A4	41	B1	C9	D9	01	Ô; ¢A±ÉÜ. Ô; ¢A±ÉÜ.
0C0109CD0	D4	A1	A4	41	B1	C9	D9	01	00	00	00	00	00	00	00	00	Ô; ¢A±ÉÜ.....
0C0109CE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	.....
0C0109CF0	0C	00	4E	00	54	00	46	00	53	00	5F	00	53	00	43	00	..N.T.F.S._.S.C.
0C0109D00	50	00	2E	00	74	00	78	00	74	00	00	00	00	00	00	00	P...t.x.t.....
0C0109D10	40	00	00	00	28	00	00	00	00	00	00	00	00	00	04	00	@... (.....
0C0109D20	10	00	00	00	18	00	00	00	6B	25	F5	67	8F	35	EE	11	.....k%ôg.5î.
0C0109D30	A6	94	00	A5	54	E0	EB	34	80	00	00	00	48	00	00	00	! ".¥Tàè4€...H...
0C0109D40	01	00	00	00	00	00	05	00	00	00	00	00	00	00	00	00	.....
0C0109D50	00	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	.....@.....
0C0109D60	00	10	00	00	00	00	00	00	19	04	00	00	00	00	00	00	.....
0C0109D70	19	04	00	00	00	00	00	00	21	01	46	18	00	00	00	00	.....!.F.....
0C0109D80	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	ÿÿÿÿ, yG.....

## NTFS 삭제 파일 복구 실습

삭제되었던 파일을 찾을 수 있다.

해당 부분을 복사해 새로 열어주고 저장하면 복구된다.

하드 디스크

Offset (h)

001946000  
001946010  
001946020  
001946030  
001946040  
001946050  
001946060  
001946070  
001946080  
001946090  
0019460A0  
0019460B0  
0019460C0  
0019460D0  
0019460E0  
0019460F0  
001946100  
001946110  
001946120  
001946130  
001946140  
001946150  
001946160  
001946170  
001946180  
001946190  
0019461A0  
0019461B0  
0019461C0

HxD - [무제1]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

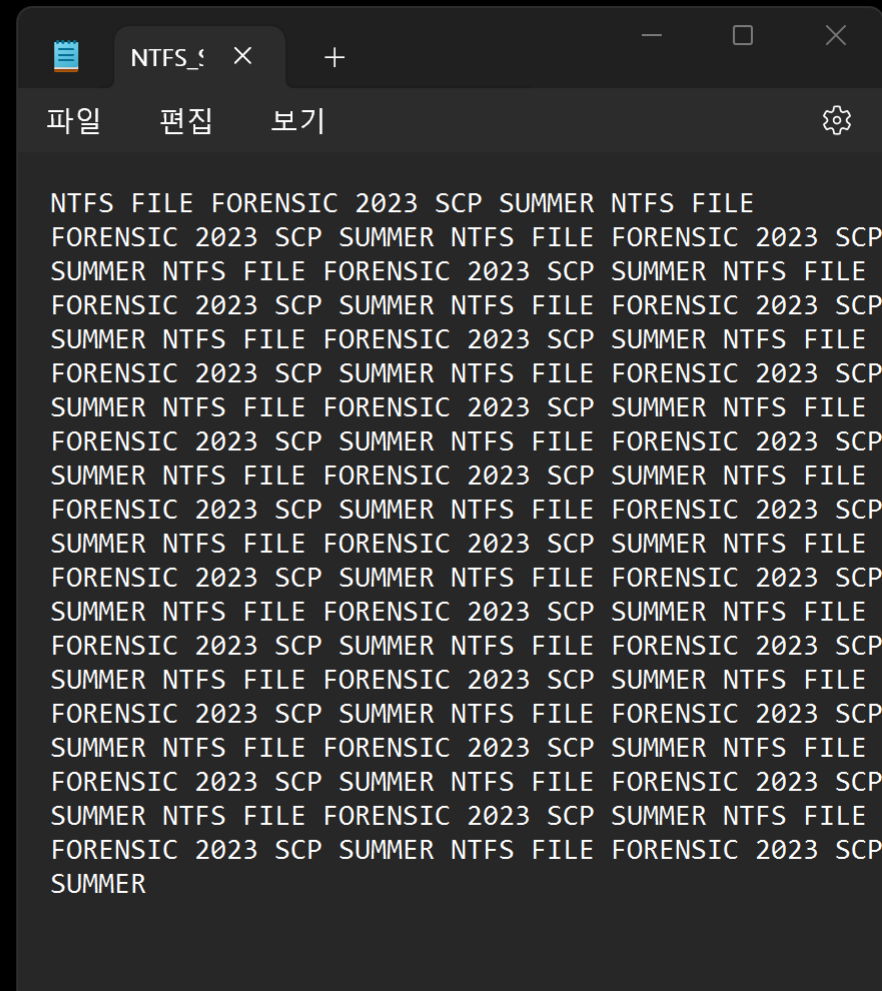
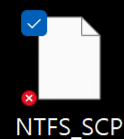
16 Windows (ANSI) 16진수

하드 디스크 2 무제1

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4E	54	46	53	20	46	49	4C	45	20	46	4F	52	45	4E	53	NTFS FILE FORENS
00000010	49	43	20	32	30	32	33	20	53	43	50	20	53	55	4D	4D	IC 2023 SCP SUMM
00000020	45	52	20	4E	54	46	53	20	46	49	4C	45	20	46	4F	52	ER NTFS FILE FOR
00000030	45	4E	53	49	43	20	32	30	32	33	20	53	43	50	20	53	ENSIC 2023 SCP S
00000040	55	4D	4D	45	52	20	4E	54	46	53	20	46	49	4C	45	20	UMMER NTFS FILE
00000050	46	4F	52	45	4E	53	49	43	20	32	30	32	33	20	53	43	FORENSIC 2023 SC
00000060	50	20	53	55	4D	4D	45	52	20	4E	54	46	53	20	46	49	P SUMMER NTFS FI
00000070	4C	45	20	46	4F	52	45	4E	53	49	43	20	32	30	32	33	LE FORENSIC 2023
00000080	20	53	43	50	20	53	55	4D	4D	45	52	20	4E	54	46	53	SCP SUMMER NTFS
00000090	20	46	49	4C	45	20	46	4F	52	45	4E	53	49	43	20	32	FILE FORENSIC 2
000000A0	30	32	33	20	53	43	50	20	53	55	4D	4D	45	52	20	4E	023 SCP SUMMER N
000000B0	54	46	53	20	46	49	4C	45	20	46	4F	52	45	4E	53	49	TFS FILE FORENSI
000000C0	43	20	32	30	32	33	20	53	43	50	20	53	55	4D	4D	45	C 2023 SCP SUMME
000000D0	52	20	4E	54	46	53	20	46	49	4C	45	20	46	4F	52	45	R NTFS FILE FORE
000000E0	4E	53	49	43	20	32	30	32	33	20	53	43	50	20	53	55	NSIC 2023 SCP SU
000000F0	4D	4D	45	52	20	4E	54	46	53	20	46	49	4C	45	20	46	MMER NTFS FILE F
00000100	4F	52	45	4E	53	49	43	20	32	30	32	33	20	53	43	50	ORENSIC 2023 SCP
00000110	20	53	55	4D	4D	45	52	20	4E	54	46	53	20	46	49	4C	SUMMER NTFS FIL
00000120	45	20	46	4F	52	45	4E	53	49	43	20	32	30	32	33	20	E FORENSIC 2023
00000130	53	43	50	20	53	55	4D	4D	45	52	20	4E	54	46	53	20	SCP SUMMER NTFS
00000140	46	49	4C	45	20	46	4F	52	45	4E	53	49	43	20	32	30	FILE FORENSIC 20
00000150	32	33	20	53	43	50	20	53	55	4D	4D	45	52	20	4E	54	23 SCP SUMMER NT
00000160	46	53	20	46	49	4C	45	20	46	4F	52	45	4E	53	49	43	FS FILE FORENSIC
00000170	20	32	30	32	33	20	53	43	50	20	53	55	4D	4D	45	52	2023 SCP SUMMER
00000180	20	4E	54	46	53	20	46	49	4C	45	20	46	4F	52	45	4E	NTFS FILE FOREN
00000190	53	49	43	20	32	30	32	33	20	53	43	50	20	53	55	4D	SIC 2023 SCP SUM
000001A0	4D	45	52	20	4E	54	46	53	20	46	49	4C	45	20	46	4F	MER NTFS FILE FO
000001B0	52	45	4E	53	49	43	20	32	30	32	33	20	53	43	50	20	RENSIC 2023 SCP
000001C0	53	55	4D	4D	45	52	20	4E	54	46	53	20	46	49	4C	45	SUMMER NTFS FILE
000001D0	20	46	4F	52	45	4E	53	49	43	20	32	30	32	33	20	53	FORENSIC 2023 S
000001E0	43	50	20	53	55	4D	4D	45	52	20	4E	54	46	53	20	46	CP SUMMER NTFS F
000001F0	49	4C	45	20	46	4F	52	45	4E	53	49	43	20	32	30	32	ILE FORENSIC 202
00000200	33	20	53	43	50	20	53	55	4D	4D	45	52	20	4E	54	46	3 SCP SUMMER NTF
00000210	53	20	46	49	4C	45	20	46	4F	52	45	4E	53	49	43	20	S FILE FORENSIC
00000220	32	30	32	33	20	53	43	50	20	53	55	4D	4D	45	52	20	2023 SCP SUMMER
00000230	4E	54	46	53	20	46	49	4C	45	20	46	4F	52	45	4E	53	NTFS FILE FORENS
00000240	49	43	20	32	30	32	33	20	53	43	50	20	53	55	4D	4D	IC 2023 SCP SUMM
00000250	45	52	20	4E	54	46	53	20	46	49	4C	45	20	46	4F	52	ER NTFS FILE FOR
00000260	45	4E	53	49	43	20	32	30	32	33	20	53	43	50	20	53	ENSIC 2023 SCP S
00000270	55	4D	4D	45	52	20	4E	54	46	53	20	46	49	4C	45	20	UMMER NTFS FILE
00000280	46	4F	52	45	4E	53	49	43	20	32	30	32	33	20	53	43	FORENSIC 2023 SC
00000290	50	20	53	55	4D	4D	45	52	20	4E	54	46	53	20	46	49	P SUMMER NTFS FI
000002A0	4C	45	20	46	4F	52	45	4E	53	49	43	20	32	30	32	33	LE FORENSIC 2023
000002B0	4E	53	49	43	20	53	55	4D	4D	45	52	20	4E	54	46	53	SCP SUMMER NTFS

## NTFS 삭제 파일 복구 실습

## 복구 성공!



**Q & A**