

153 – Partition Finder

Team Information

Team Name : ForensicGPT

Team Member : Eungchang Lee, Donghyun HA, Hyunwoo Shin, Jinhyeok Son

Email Address : forensicgpt@googlegroups.com

Instructions

Description Analyze the RAW disk image file to answer the question. (The filesystem for Windows was formatted in Windows 10.)

Target	Hash (MD5)
PartitionFinder.7z	C8FAEAF9C286CB90FF5B9D671E74E7E8

Questions

- 1) Find all deleted partitions, and analyze the following information for each partition. (100 points)
 - Partition type, volume serial number, formatted date/time, capacity, 1st sector(physical)
- 2) Which volumes are connected to more than one system? Analyze the following information for those volumes. (50 points)
 - Partition type, 1st sector(physical)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	https://www.mh-nexus.de		

Name:	HashTab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com		

Name:	Dcode	Publisher:	Digital Detective
Version:	5.5		
URL:	https://www.digital-detective.net/dcode/		

Name:	FTK Imager	Publisher:	AccessData
Version:	4.7.1.2		
URL:	https://www.exterro.com/ftk-product-downloads/ftk-imager-version-4-7-1		

Step-by-step methodology:



[그림 1] 해시 값 확인

분석에 앞서, 주어진 파일에 대한 해시 값을 산출하여 MD5 해시 값이 일치함을 확인하였습니다.

1) Find all deleted partitions, and analyze the following information for each partition. (100 points)

- Partition type, volume serial number, formatted date/time, capacity, 1st sector(physical)

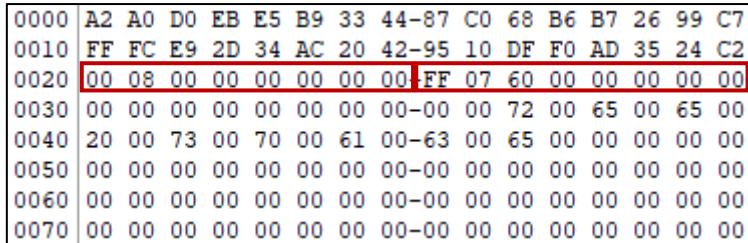


The screenshot shows a file tree for 'PartitionFinder.001' containing '파티션 1 [3072MB]' (FAT16), 'Unpartitioned Space [GPT]', and '[할당되지 않은 공간]'. To the right is a list of sectors from 000000034 to 008341504, each with its size (1,007 to 102,400 bytes) and type ('비 할당 공간' - unallocated space).

	이름	크기	유형
	000000034	1,007[Missing string: ...]	비 할당 공간
	0006293504	102,400[Missing string: ...]	비 할당 공간
	0006498304	102,400[Missing string: ...]	비 할당 공간
	0006703104	102,400[Missing string: ...]	비 할당 공간
	0006907904	102,400[Missing string: ...]	비 할당 공간
	0007112704	102,400[Missing string: ...]	비 할당 공간
	0007317504	102,400[Missing string: ...]	비 할당 공간
	0007522304	102,400[Missing string: ...]	비 할당 공간
	0007727104	102,400[Missing string: ...]	비 할당 공간
	0007931904	102,400[Missing string: ...]	비 할당 공간
	0008136704	102,400[Missing string: ...]	비 할당 공간
	0008341504	102,400[Missing string: ...]	비 할당 공간

[그림 2] 이미지 확인

먼저 주어진 파일을 압축해제 후 분할된 이미지 중 PartitionFinder.001을 FTK imager에 로드 하였을 때 위 그림과 같이 나타나는 것을 볼 수 있습니다. FAT16 파일 시스템을 가진 파티션 1만 인식이 되고, 나머지 분할된 이미지의 데이터들은 할당되지 않은 공간에 위치하는 것을 확인하였습니다. 또한, 001과 015 파일에서 GPT 헤더가 발견된 것을 보아 GPT 구조를 가지고 있음을 확인할 수 있습니다.



The screenshot shows a hex dump of the first sector (0000) of a partition. The bytes are: A2 A0 D0 EB E5 B9 33 44-87 C0 68 B6 B7 26 99 C7. The byte at address 0020 (00 08 00 00 00 00 00 FF) is highlighted in red, indicating it's the GPT header.

0000	A2	A0	D0	EB	E5	B9	33	44-87	C0	68	B6	B7	26	99	C7
0010	FF	FC	E9	2D	34	AC	20	42-95	10	DF	F0	AD	35	24	C2
0020	00	08	00	00	00	00	00	FF	07	60	00	00	00	00	00
0030	00	00	00	00	00	00	00	00-00	00	72	00	65	00	65	00
0040	20	00	73	00	70	00	61	00-63	00	65	00	00	00	00	00
0050	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
0060	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
0070	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00

[그림 3] 주요 파티션 항목 배열

GPT에서 주요 파티션 항목 배열을 살펴보면, 파티션마다 128 bytes의 크기를 나타내며 해당 GPT 파티션 엔트리에 기록되어야 하지만 한 개의 파티션만 기록되어 있습니다. 기록되어 있는 파티션의 starting LBA는 0x800으로 2048 섹터, end LBA는 0x6007FF로 6,293,503 섹터임을 알 수 있습니다. 이는 [그림 2]에서 확인 가능한 FAT16 파일 시스템을 가진 파티션 1이 시작 섹터가 2048 섹터이기 때문에 해당 파티션임을 알 수 있었습니다. 또한, 고유 GUID 정보 "2DE9FCFF-AC34-4220-9510-DFF0AD3524C2"로 같음을 확인하였습니다.

따라서, GPT 파티션 엔트리에 기록된 파티션을 제외하고 기록되지 않은 파티션들이 나머지 분할 파일 데이터에 남아 있다면 삭제된 파티션으로 간주하기 위해 HxD를 이용하여 로우 레벨로 분석을 진행하였습니다. 그리고 마지막에 GPT 파티션 테이블 엔트리를 복구하고 FTK 도구 상에서 이미지를 load 하여 파티션이 정상적으로 인식되는지 교차 검증을 진행하였습니다.

● PartitionFinder.001 – FAT16

080100000	EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 80 01 00	¶<.MSDOS5.0..€..
080100010	02 00 02 00 00 F8 00 01 3F 00 FF 00 00 00 00 00ø..?..ý.....
080100020	00 F8 7F 00 80 00 29 79 28 FB 1D 4E 4F 20 4E 41	.ø..€.)y(û.NO NA
080100030	4D 45 20 20 20 20 46 41 54 31 36 20 20 20 33 C9	ME FAT16 3É
080100040	8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C	ŽÑ4ð{ŽÙ.. žÀùë..
080100050	38 4E 24 7D 24 8B C1 99 E8 3C 01 72 1C 83 EB 3A	8NS)S<Ámè<.r.fë:
080100060	66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA	f;. &f;.&ŠWüu.€È
080100070	02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10 98 F7	.^V.€Ä.së3ÉŠF.^+
080100080	66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11	f..F..V..F..Ñ<v.
080100090	60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03	‘%Fü%Vp,. .÷æ<^..
0801000A0	C3 48 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6	ÄH÷ó.Fü.Npaž..èæ
0801000B0	00 72 39 26 38 2D 74 17 60 B1 0B BE A1 7D F3 A6	.r9&8-t.`±.%}ó!
0801000C0	61 74 32 4E 74 09 83 C7 20 3B FB 72 E6 EB DC A0	at2Nt.fÇ ;ûræëÜ
0801000D0	FB 7D B4 7D 8B F0 AC 98 40 74 0C 48 74 13 B4 0E	û}’}«ö~@t.Ht.’.
0801000E0	BB 07 00 CD 10 EB EF A0 FD 7D EB E6 A0 FC 7D EB	»..í.ëi ý}ëæ ü}ë
0801000F0	E1 CD 16 CD 19 26 8B 55 1A 52 B0 01 BB 00 00 E8	áí.í.ë<U.R°.»..è
080100100	3B 00 72 E8 5B 8A 56 24 BE 0B 7C 8B FC C7 46 F0	; .rè[ŠV\$%. <üÇFØ
080100110	3D 7D C7 46 F4 29 7D 8C D9 89 4E F2 89 4E F6 C6	=)ÇFØ))ŒÙ%Nò%NÖÈ
080100120	06 96 7D CB EA 03 00 00 20 0F B6 C8 66 8B 46 F8	.-)Èè... .¶Èf<Fø
080100130	66 03 46 1C 66 8B D0 66 C1 EA 10 EB 5E 0F B6 C8	f.F.f<ĐfÁè.ë^.¶È
080100140	4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB	JJŠF.2ä÷â.Fü.Vpë
080100150	4A 52 50 06 53 6A 01 6A 10 91 8B 46 18 96 92 33	JRP.Sj.j. ‘F.-’ 3
080100160	D2 F7 F6 91 F7 F6 42 87 CA F7 76 1A 8A F2 8A E8	Ò÷ö'÷öB#È÷v.ŠòŠè
080100170	C0 CC 02 0A CC B8 01 02 80 7E 02 0E 75 04 B4 42	Àì..ì..€~..u.‘B
080100180	8B F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03	<öŠV\$í.aar.Û.u.B.
080100190	5E 0B 49 75 06 F8 C3 41 BB 00 00 60 66 6A 00 EB	^.Iu.øÃA».. ‘fj.ë
0801001A0	B0 4E 54 4C 44 52 20 20 20 20 20 0D 0A 52 65	°NTLDR ..Re
0801001B0	6D 6F 76 65 20 64 69 73 6B 73 20 6F 72 20 6F 74	move disks or ot
0801001C0	68 65 72 20 6D 65 64 69 61 2E FF 0D 0A 44 69 73	her media.ý..Dis
0801001D0	6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73 20	k errorý..Press
0801001E0	61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74 61	any key to resta
0801001F0	72 74 0D 0A 00 00 00 00 00 00 00 AC CB D8 55 AA	rt.....-ÉØU^

[그림 4] PartitionFinder.001에 존재하는 FAT16 파티션 VBR

기존에 인식되던 파티션 1 외에 삭제된 FAT 16 파티션을 확인하고 다음과 같이 파티션 정보를 정리하였습니다. Formatted Date/Time은 해당 정보¹를 참고하였습니다.

[표 1] FAT 16 파티션 정보

속성	값
Partition Type	FAT16
Volume Serial Number	1DFB-2879
Formatted Date/Time	2023-07-30 22:04:32.0000000 (90B0FE56)
Capacity	4,293,918,720 bytes (0x7FF800 sectors) 4,293,918,720 bytes (0x3FFC00 clusters)
1 st sector	4,196,352 sector (0x400800)

¹ <http://forensic-proof.com/archives/633>

● PartitionFinder.001 – NTFS

1800000000	EB 52 90 4E 54 46 53 20 20 20 20 20 00 02 08 00 00	ER.NTFS
1800000010	00 00 00 00 00 F8 00 00 3F 00 FF 00 00 00 00 00 00ø..?..ÿ.....
1800000020	00 00 00 00 80 00 80 00 FF FF FF 04 00 00 00 00 00€.€.ÿÿ.....
1800000030	03 00 00 00 00 00 00 00 FF FF 4F 00 00 00 00 00 00ÿO.....
1800000040	F6 00 00 00 01 00 00 00 C0 0E EB 1D 34 C3 D9 01	ö.....À.ë.4ÄÙ.
1800000050	00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07ú3ÀŽÐ4.. ûhÀ.
1800000060	1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E	..hf.È^...f.>..N
1800000070	54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB	TFSu.'A»*UÍ.r..û
1800000080	55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC	U^u..Á..u.éÝ..fi
1800000090	18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13	.h..‘HŠ...<ô..í.
18000000A0	9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3	ÝfÄ..žX.rá;...uÛ£
18000000B0	0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8	..Á.....Z3Û¹. +È
18000000C0	66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8	fÿ.....žÄÿ...è
18000000D0	4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D	K.+Èwi..»í.f#Äu-
18000000E0	66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16	f.ûTCPAu\$.ù..r..
18000000F0	68 07 BB 16 68 70 0E 16 68 09 00 66 53 66 53 66	h..»hp..h..fSfSf
1800000100	55 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF	U...h..fa..í.3Àë
1800000110	28 10 B9 D8 0F FC F3 AA E9 5F 01 90 90 66 60 1E	(..Ø.üó*é...f`.
1800000120	06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00	.fi..f.....fh...
1800000130	00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E	.fP.Sh..h..‘BŠ..
1800000140	00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F	...<öí.fY[ZfYfY.
1800000150	0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF	,,..fÿ.....žÄÿ
1800000160	0E 16 00 75 BC 07 1F 66 61 C3 A0 F8 01 E8 09 00	...u4..faÃ ø.è..
1800000170	A0 FB 01 E8 03 00 F4 EB FD B4 01 8B F0 AC 3C 00	û.è..öëý`.<ð~<.
1800000180	74 09 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20	t..’..»..í.ëöÄ..A
1800000190	64 69 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20	disk read error
18000001A0	6F 63 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D	occurred...BOOTM
18000001B0	47 52 20 69 73 20 6D 69 73 73 69 6E 67 00 0D 0A	GR is missing...
18000001C0	42 4F 4F 54 4D 47 52 20 69 73 20 63 6F 6D 70 72	BOOTMGR is compr
18000001D0	65 73 73 65 64 00 0D 0A 50 72 65 73 73 20 43 74	essed...Press Ct
18000001E0	72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F 20 72 65	r1+Alt+Del to re
18000001F0	73 74 61 72 74 0D 0A 00 8C A9 BE D6 00 00 55 AA	start...ŒŒ%Ö..U²

[그림 5] PartitionFinder.001에 존재하는 NTFS 파티션 VBR

PartitionFinder.001에는 FAT16외에도 NTFS 파티션이 존재하였습니다. Formatted Date/Time은 MFT 영역의 메타데이터 파일의 시간을 참고하였습니다. 또한, VSN는 formatted date/time을 나타내는 hex값임을 확인하였습니다.

[표 2] NTFS 파티션 정보

속성	값
Partition Type	NTFS
Volume Serial Number	01D9C3341DEB0EC0 (Full Serial Number)
Formatted Date/Time	2023-07-30 22:20:59.1800000 Z
Capacity	42,949,672,448 bytes (0x04FFFFFF sectors) 42,949,668,864 bytes (0x9FFFFFF clusters)
1 st sector	12,582,912 sector (0xC00000)

● PartitionFinder.003 - NTFS

1000000000	EB 52 90 4E 54 46 53 20 20 20 20 20 00 02 08 00 00	ëR.NTFS
1000000010	00 00 00 00 00 F8 00 00 3F 00 FF 00 00 00 00 80 02ø...?..ÿ...€.
1000000020	00 00 00 00 80 00 80 00 F8 FF 5F 04 00 00 00 00 00€.€.øÿ
1000000030	16 04 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00
1000000040	F6 00 00 00 01 00 00 00 90 E6 54 94 ED C2 D9 01	ö.....æT"íÀÙ.
1000000050	00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB B8 C0 07ú3ÀŽÐ4. ù.À.
1000000060	8E D8 E8 16 00 B8 00 0D 8E C0 33 DB C6 06 0E 00	žØè...žÀ3ÚÆ...
1000000070	10 E8 53 00 68 00 0D 68 6A 02 CB 8A 16 24 00 B4	.èS.h..hj.ÉŠ.Ş..
1000000080	08 CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66	.Í.s.^ÿyŠñf.¶E@f
1000000090	0F B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F	.¶Ñ€â?÷åtÍÀi.Af.
10000000A0	B7 C9 66 F7 E1 66 A3 20 00 C3 B4 41 BB AA 55 8A	·Éf÷áff .Ã'Àx^UŠ
10000000B0	16 24 00 CD 13 72 0F 81 FB 55 AA 75 09 F6 C1 01	.\$.í.r..ûU^u.öÁ.
10000000C0	74 04 FE 06 14 00 C3 66 60 1E 06 66 A1 10 00 66	t.p...Äf`..f;..f
10000000D0	03 06 1C 00 66 3B 06 20 00 0F 82 3A 00 1E 66 6Af;.. ,:..fj
10000000E0	00 66 50 06 53 66 68 10 00 01 00 80 3E 14 00 00	.fP.Sfh....€>...
10000000F0	0F 85 0C 00 E8 B3 FF 80 3E 14 00 00 0F 84 61 00è^ÿ€>....,a.
1000000100	B4 42 8A 16 24 00 16 1F 8B F4 CD 13 66 58 5B 07	'BŠ.Ş...<öí.fX[.
1000000110	66 58 66 58 1F EB 2D 66 33 D2 66 0F B7 0E 18 00	fXfX.ë-f3Òf.
1000000120	66 F7 F1 FE C2 8A CA 66 8B D0 66 C1 EA 10 F7 36	f÷ñþÅŠÈf<ÐfÁé..÷6
1000000130	1A 00 86 D6 8A 16 24 00 8A E8 C0 E4 06 0A CC B8	..tÖŠ.Ş.ŠèÀä..Ì,
1000000140	01 02 CD 13 0F 82 19 00 8C C0 05 20 00 8E C0 66	..í...,.GÀ. .žAf
1000000150	FF 06 10 00 FF 0E 0E 00 0F 85 6F FF 07 1F 66 61	ÿ...ÿ.....oÿ..fa
1000000160	C3 A0 F8 01 E8 09 00 A0 FB 01 E8 03 00 FB EB FE	Ã ø.è.. û.è..üëp
1000000170	B4 01 8B F0 AC 3C 00 74 09 B4 0E BB 07 00 CD 10	'.<ð~<.t.'..»..í.
1000000180	EB F2 C3 0D 0A 41 20 64 69 73 6B 20 72 65 61 64	ëòÃ..A disk read
1000000190	20 65 72 72 6F 72 20 6F 63 63 75 72 72 65 64 00	error occurred.
10000001A0	0D 0A 4E 54 4C 44 52 20 69 73 20 6D 69 73 73 69	..NTLDR is missi
10000001B0	6E 67 00 0D 0A 4E 54 4C 44 52 20 69 73 20 63 6F	ng...NTLDR is co
10000001C0	6D 70 72 65 73 73 65 64 00 0D 0A 50 72 65 73 73	mpressed...Press
10000001D0	20 43 74 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F	Ctrl+Alt+Del to
10000001E0	20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00	restart.....
10000001F0	00 00 00 00 00 00 00 00 83 A0 B3 C9 00 00 55 AAf 'É..U^

[그림 6] PartitionFinder.003에 존재하는 NTFS 파티션 VBR

해당 NTFS는 VSN에 적힌 hex값에 대해 변환한 formatted time과 다른 time을 가지고 있음을 확인할 수 있습니다.

[표 3] NTFS 파티션 정보

속성	값
Partition Type	NTFS
Volume Serial Number	01D9C2ED9454E690 (Full Serial Number)
Formatted Date/Time	2010-05-04 03:24:57.1790000 Z
Capacity	37,580,959,744 bytes (0x045FFFF8 sectors) 37,580,959,744 bytes (0x8BFFFF clusters)
1 st sector	41,943,040 sector (0x2800000)

● PartitionFinder.007 – FAT16

1C00000000	EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 80 02 00	ë<.MSDOS5.0..€..
1C00000010	02 00 02 00 00 F8 00 01 3F 00 FF 00 00 00 E0 06ø...?..ÿ...à.
1C00000020	00 F8 7F 00 80 00 29 B0 ED 13 C7 4E 4F 20 4E 41	.ø..€..)°i.ÇNO NA
1C00000030	4D 45 20 20 20 20 46 41 54 31 36 20 20 20 33 C9	ME FAT16 3É
1C00000040	8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C	ŽÑ¾8{ŽÙ,. ŽÀüñ..
1C00000050	38 4E 24 7D 24 8B C1 99 E8 3C 01 72 1C 83 EB 3A	8NS}S<Á™è<.r.fë:
1C00000060	66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA	f;. &f; .&ŠWüu.€È
1C00000070	02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10 98 F7	.^V.€Ä.së3ÉŠF.^÷
1C00000080	66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11	f...F..V..F..Ñ«v.
1C00000090	60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03	`‰Fü‰Vp. .÷æ<^..
1C000000A0	C3 48 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6	ÃH÷ó.Fü.Nþaç..èæ
1C000000B0	00 72 39 26 38 2D 74 17 60 B1 0B BE A1 7D F3 A6	.r9&8-t. `±.%i)ö!
1C000000C0	61 74 32 4E 74 09 83 C7 20 3B FB 72 E6 EB DC A0	at2Nt.fÇ ;ûræeÜ
1C000000D0	FB 7D B4 7D 8B F0 AC 98 40 74 0C 48 74 13 B4 0E	û} ')<ð~@t.Ht.'..
1C000000E0	BB 07 00 CD 10 EB EF A0 FD 7D EB E6 A0 FC 7D EB	»..í.ëi ý}ëæ ü}ë
1C000000F0	E1 CD 16 CD 19 26 8B 55 1A 52 B0 01 BB 00 00 E8	áÍ.í.ë<U.R°..»..è
1C0000100	3B 00 72 E8 5B 8A 56 24 BE 0B 7C 8B FC C7 46 F0	;:rè[ŠV\$%. <üÇFö
1C0000110	3D 7D C7 46 F4 29 7D 8C D9 89 4E F2 89 4E F6 C6	=}ÇFö)}ŒÙhNòhNöE
1C0000120	06 96 7D CB EA 03 00 00 20 0F B6 C8 66 8B 46 F8	.-)Ëè.... .¶Èf< Fø
1C0000130	66 03 46 1C 66 8B D0 66 C1 EA 10 EB 5E 0F B6 C8	f.F.f<ĐfÁè..ë^.¶È
1C0000140	4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB	JJŠF.2ä÷å.Fü.Vpë
1C0000150	4A 52 50 06 53 6A 01 6A 10 91 8B 46 18 96 92 33	JRP.Sj.j. 'F.-'3
1C0000160	D2 F7 F6 91 F7 F6 42 87 CA F7 76 1A 8A F2 8A E8	Ø÷ö'÷öB‡È÷v.ŠòŠè
1C0000170	C0 CC 02 0A CC B8 01 02 80 7E 02 0E 75 04 B4 42	Àì..ì..€~..u. 'B
1C0000180	8B F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03	<ðŠV\$Í.aar.øu.B.
1C0000190	5E 0B 49 75 06 F8 C3 41 BB 00 00 60 66 6A 00 EB	^.Iu.øÅA»..`fj.ë
1C00001A0	B0 4E 54 4C 44 52 20 20 20 20 20 0D 0A 52 65	°NTLDR ..Re
1C00001B0	6D 6F 76 65 20 64 69 73 6B 73 20 6F 72 20 6F 74	move disks or ot
1C00001C0	68 65 72 20 6D 65 64 69 61 2E FF 0D 0A 44 69 73	her media.ÿ..Dis
1C00001D0	6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73 20	k errorÿ..Press
1C00001E0	61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74 61	any key to resta
1C00001F0	72 74 0D 0A 00 00 00 00 00 00 00 00 AC CB D8 55 AA	rt.....-ÉØU*

[그림 7] PartitionFinder.007에 존재하는 FAT16 파티션 VBR

[표 4] FAT16 파티션 정보

속성	값
Partition Type	FAT16
Volume Serial Number	C713-EDB0
Formatted Date/Time	2023-07-30 22:57:30.0000000 (2FB7FE56)
Capacity	4,293,918,720 bytes (0x7FF800 sectors) 4,293,918,720 bytes (0x3FFC00 clusters)
1 st sector	115,343,360 sector (0x6E00000)

● PartitionFinder.008 - NTFS

OBFF00000	EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00	ëR.NTFS
OBFF00010	00 00 00 00 00 F8 00 00 3F 00 FF 00 00 00 00 00ø..?..ý.....
OBFF00020	00 00 00 00 80 00 80 00 FF FF 87 07 00 00 00 00€.€.ýy#.....
OBFF00030	03 00 00 00 00 00 00 00 FF 7F 78 00 00 00 00 00ý.x.....
OBFF00040	F6 00 00 00 01 00 00 00 10 E2 4B 05 41 C3 D9 01	ö.....åK.AÄÙ.
OBFF00050	00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07ú3ÀŽÐ4 . uhÀ.
OBFF00060	1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E	..hf.È^...f.>..N
OBFF00070	54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB	TFSu.'A»"UÍ.r..û
OBFF00080	55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC	U"u.-Á..u.éÝ..fi
OBFF00090	18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13	.h..'HŠ...<ð..í.
OBFF000A0	9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3	ÝfÄ.žX.rá;...uÛ£
OBFF000B0	0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8	..Á.....Z3Û¹. +È
OBFF000C0	66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8	fý.....žÄý...è
OBFF000D0	4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D	K.+Èwi..»í.f#Àu-
OBFF000E0	66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16	f.ÛTCPAu\$.ù...r..
OBFF000F0	68 07 BB 16 68 70 0E 16 68 09 00 66 53 66 53 66	h..»hp..h..fsfSf
OBFF00100	55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF	U...h..fa..í.3Àç
OBFF00110	28 10 B9 D8 0F FC F3 AA E9 5F 01 90 90 66 60 1E	(..³Ø.üó"é_...f`.
OBFF00120	06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00	.f;.f.....fh...
OBFF00130	00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E	.fp.Sh..h..'BŠ..
OBFF00140	00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F	...<ðí.fY[ZfYfY.
OBFF00150	0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF	,...fý.....žÄý
OBFF00160	0E 16 00 75 BC 07 1F 66 61 C3 A0 F8 01 E8 09 00	...u¹4..faÃ ø.è..
OBFF00170	A0 FB 01 E8 03 00 F4 EB FD B4 01 8B F0 AC 3C 00	û.è..ðëý'.<ð<.
OBFF00180	74 09 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20	t.'..»..í.ëðÃ..A
OBFF00190	64 69 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20	disk read error
OBFF001A0	6F 63 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D	occurred...BOOTM
OBFF001B0	47 52 20 69 73 20 6D 69 73 73 69 6E 67 00 0D 0A	GR is missing...
OBFF001C0	42 4F 54 4D 47 52 20 69 73 20 63 6F 6D 70 72	BOOTMGR is compr
OBFF001D0	65 73 73 65 64 00 0D 0A 50 72 65 73 73 20 43 74	essed...Press Ct
OBFF001E0	72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F 20 72 65	r1+Alt+Del to re
OBFF001F0	73 74 61 72 74 0D 0A 00 8C A9 BE D6 00 00 55 AA	start...œõÖ..U"

[그림 8] PartitionFinder.008에 존재하는 NTFS 파티션 VBR

속성	값
Partition Type	NTFS
Volume Serial Number	01D9C341054BE210 (Full Serial Number)
Formatted Date/Time	2023-07-30 23:53:21.3290000 Z
Capacity	64,692,944,384 bytes (0x0787FFFF sectors) 64,692,940,800 bytes(0xF0FFFF clusters)
1 st sector	123,729,920 sector (0x75FF800)

● PartitionFinder.010 - exFAT

1000000000	EB 76 90 45 58 46 41 54 20 20 20 20 00 00 00 00 00 00	Ev.EXFAT
1000000010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1000000020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1000000030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1000000040	00 00 80 09 00 00 00 00 00 00 80 01 00 00 00 00 00 00	..€.....€..
1000000050	80 00 00 00 E8 5F 00 00 68 60 00 00 F3 F3 2F 00	€...è...h`..óó/.
1000000060	64 00 00 00 4D 20 01 1E 00 01 00 00 09 03 01 80	d...M€
1000000070	00 00 00 00 00 00 00 00 33 C9 8E D1 BC F0 7B 8E3ÉŽÑ4ç{Ž
1000000080	D9 A0 FB 7D B4 7D 8B F0 AC 98 40 74 OC 48 74 OE	Ù û)'}<ð~@t.Ht.
1000000090	B4 0E BB 07 00 CD 10 EB EF A0 FD 7D EB E6 CD 16	'..»..í.ëi ý}ëæí.
10000000A0	CD 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	í.....
10000000B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10000000C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10000000D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10000000E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10000000F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1000000100	0D 0A 52 65 6D 6F 76 65 20 64 69 73 6B 73 20 6F	..Remove disks o
1000000110	72 20 6F 74 68 65 72 20 6D 65 64 69 61 2E FF 0D	r other media.ý.
1000000120	0A 44 69 73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72	.Disk errorý..Pr
1000000130	65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 72	ess any key to r
1000000140	65 73 74 61 72 74 0D 0A 00 00 00 00 00 00 00 00 00 00	estart.....
1000000150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1000000160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1000000170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1000000180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1000000190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10000001A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10000001B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FFÿÿ
10000001C0	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
10000001D0	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
10000001E0	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
10000001F0	FF FF FF FF FF FF FF FF 00 1F 2C 55 AA	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ..,U*

[그림 9] PartitionFinder.010에 존재하는 exFAT 파티션 VBR(boot sector)

exFAT에서는 위에서 참고한 각주와 동일하게 참고하여 formatted time을 System Volume Information 폴더 생성 시간과 근접하게 추정하였습니다. 또한, 해당 파티션은 0x48~0x4F에 위치한 블록에 할당된 총 섹터 수를 기반으로 카빙을 진행해야 이미지 인식이 올바르게 되는 것을 확인하였습니다.

[표 5] exFAT 파티션 정보

속성	값
Partition Type	exFAT
Volume Serial Number	1E01-204D
Formatted Date/Time	2023-07-30 22:26:22.0000000 (4BB3FE56)
Capacity	12,884,901,888 bytes (0x01800000 sectors) 12,884,901,888 bytes(0x300000 clusters)
1 st sector	159,383,552 sector (0x9800000)

● PartitionFinder.012 – FAT16

0000000000	EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 80 01 00	ë<.MSDOS5.0..€..
0000000010	02 00 02 00 00 F8 80 00 3F 00 FF 00 00 00 00 00ø€.?.ÿ.....
0000000020	00 00 40 00 80 00 29 A5 3A 01 1E 4E 4F 20 4E 41	..@.€.)ÿ:..NO NA
0000000030	4D 45 20 20 20 20 46 41 54 31 36 20 20 20 33 C9	ME FAT16 3É
0000000040	8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C	ŽÑ4ð(ZÙ,. ŽÀùž.
0000000050	38 4E 24 7D 24 8B C1 99 E8 3C 01 72 1C 83 EB 3A	8N\$)\$. <a>è<.r.fë:
0000000060	66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA	f;. &f;.&ŠWüu.€È
0000000070	02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10 98 F7	.~V.€Ä.së3ÉŠF."÷
0000000080	66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11	f..F..V..F..Ñ<v.
0000000090	60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03	`%Fü%Vp, .÷æ<^..
00000000A0	C3 48 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6	ÄH÷ö.Fü.Nþaž..èæ
00000000B0	00 72 39 26 38 2D 74 17 60 B1 0B BE A1 7D F3 A6	.r9&8-t.`±.%i}ö!
00000000C0	61 74 32 4E 74 09 83 C7 20 3B FB 72 E6 EB DC A0	at2Nt.fÇ ;úraéÜ
00000000D0	FB 7D B4 7D 8B F0 AC 98 40 74 0C 48 74 13 B4 0E	û} `)<ð~"@t.Ht.'. .
00000000E0	BB 07 00 CD 10 EB EF A0 FD 7D EB E6 A0 FC 7D EB	»..í.ëi ý}ëæ ü)ë
00000000F0	E1 CD 16 CD 19 26 8B 55 1A 52 B0 01 BB 00 00 E8	áí.í.ë<U.R°.»..è
000000100	3B 00 72 E8 5B 8A 56 24 BE 0B 7C 8B FC C7 46 F0	;.:rè[ŠVS¾. <üÇFØ
000000110	3D 7D C7 46 F4 29 7D 8C D9 89 4E F2 89 4E F6 C6	=}ÇFØ) }ŒÙ%Nò%NòÈ
000000120	06 96 7D CB EA 03 00 00 20 0F B6 C8 66 8B 46 F8	.-)Èë... .¶Èf< Fø
000000130	66 03 46 1C 66 8B D0 66 C1 EA 10 EB 5E 0F B6 C8	f.F.f<ĐfÁê.ë^.¶È
000000140	4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB	JJŠF.2ä÷â.Fü.Vpë
000000150	4A 52 50 06 53 6A 01 6A 10 91 8B 46 18 96 92 33	JRP.Sj.j.'<F.-'3
000000160	D2 F7 F6 91 F7 F6 42 87 CA F7 76 1A 8A F2 8A E8	Ø÷ö'÷öB÷È÷v.ŠòSè
000000170	C0 CC 02 0A CC B8 01 02 80 7E 02 0E 75 04 B4 42	Àì..ì..€~..u.'B
000000180	8B F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03	<ðŠVšÍ.aar.øu.B.
000000190	5E 0B 49 75 06 F8 C3 41 BB 00 00 60 66 6A 00 EB	^.Iu.øÃA»..`fj.ë
0000001A0	B0 4E 54 4C 44 52 20 20 20 20 20 0D 0A 52 65	°NTLDR ..Re
0000001B0	6D 6F 76 65 20 64 69 73 6B 73 20 6F 72 20 6F 74	move disks or ot
0000001C0	68 65 72 20 6D 65 64 69 61 2E FF 0D 0A 44 69 73	her media.ÿ..Dis
0000001D0	6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73 20	k errorÿ..Press
0000001E0	61 6E 79 20 6B 65 79 20 74 6F 20 72 65 73 74 61	any key to resta
0000001F0	72 74 0D 0A 00 00 00 00 00 00 00 00 AC CB D8 55 AA	rt.....-ÈØU*

[그림 10] PartitionFinder.012에 존재하는 FAT16 파티션 VBR

[표 6] FAT16 파티션 정보

속성	값
Partition Type	FAT16
Volume Serial Number	1E01-3AA5
Formatted Date/Time	2023-07-30 22:10:50.0000000 (59B1FE56)
Capacity	2,147,483,648 bytes (0x400000 sectors) 2,147,483,648 bytes(0x200000 clusters)
1 st sector	184,549,376 sector (0xB0000000)

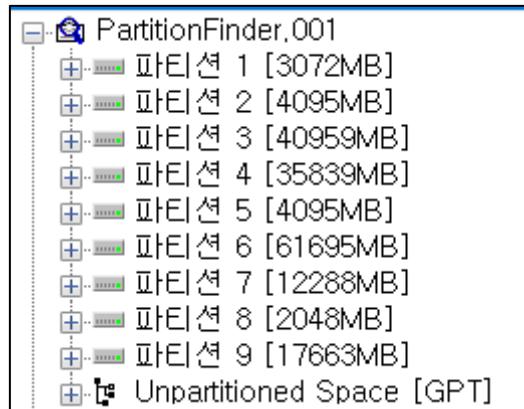
● PartitionFinder.013 - NTFS

1800000000	EB 52 90 4E 54 46 53 20 20 20 20 20 00 02 08 00 00	ER.NTFSø..?..ý.....	
1800000010	00 00 00 00 00 F8 00 00 3F 00 FF 00 00 00 00 00 00€.€.ý÷'.....	
1800000020	00 00 00 00 80 00 80 00 FF F7 27 02 00 00 00 00 00".....	
1800000030	03 00 00 00 00 00 00 00 7F 7F 22 00 00 00 00 00 00€.\$.;5ÄÜ.	
1800000040	F6 00 00 00 01 00 00 00 80 06 24 3B 35 C3 D9 01	ö.....ú3ÀŽÐ4. ûhÀ.	
1800000050	00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07hF.È^...f.>..N	
1800000060	1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E	TFSu.'A»*UÍ.r..ù	
1800000070	54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB	U*u.÷Á..u.éÝ..fi	
1800000080	55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC	18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13	.h.. 'HŠ...<ô..í.
1800000090	9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3	ÿfÄ.žX.rá;...uÛf	
18000000A0	0F 00 C1 2E OF 00 04 1E 5A 33 DB B9 00 20 2B C8	..Á.....Z3Û¹. +È	
18000000B0	66 FF 06 11 00 03 16 OF 00 8E C2 FF 06 16 00 E8	fÙ.....žÄy...è	
18000000C0	4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D	K.+Èwi.,»í.f#Äu-	
18000000D0	66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16	f.ÛTCPAu\$.ù...r..	
18000000E0	68 07 BB 16 68 70 0E 16 68 09 00 66 53 66 53 66	h.»..hp..h..fSfSf	
18000000F0	55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF	U...h..fa..í.3Àì	
1800000100	28 10 B9 D8 0F FC F3 AA E9 5F 01 90 90 66 60 1E	(..Ø.úó*é...f`.	
1800000110	06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00	.f;..f.....fh...	
1800000120	00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E	.fP.Sh..h..'BŠ..	
1800000130	00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F	...<óí.fY[ZfYfY.	
1800000140	0F 82 16 00 66 FF 06 11 00 03 16 OF 00 8E C2 FF	,...fÙ.....žÄy	
1800000150	0E 16 00 75 BC 07 1F 66 61 C3 A0 F8 01 E8 09 00	...uÛ..faÄ ø..è..	
1800000160	A0 FB 01 E8 03 00 F4 EB FD B4 01 8B F0 AC 3C 00	û.è..öëý'.<ð~<.	
1800000170	74 09 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20	t.~.»..í.ëòÄ..A	
1800000180	64 69 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20	disk read error	
1800000190	6F 63 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D	occurred...BOOTM	
18000001A0	47 52 20 69 73 20 6D 69 73 73 69 6E 67 00 0D 0A	GR is missing...	
18000001B0	42 4F 4F 54 4D 47 52 20 69 73 20 63 6F 6D 70 72	BOOTMGR is compr	
18000001C0	65 73 73 65 64 00 0D 0A 50 72 65 73 73 20 43 74	essed...Press Ct	
18000001D0	72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F 20 72 65	r1+Alt+Del to re	
18000001E0	73 74 61 72 74 0D 0A 00 8C A9 BE D6 00 00 55 AA	start...©®Ö..U*	
18000001F0			

[그림 11] PartitionFinder.013에 존재하는 NTFS 파티션 VBR

[표 7] NTFS 파티션 정보

속성	값
Partition Type	NTFS
Volume Serial Number	01D9C3353B240680 (Full Serial Number)
Formatted Date/Time	2023-07-30 22:28:57.7040000 Z
Capacity	18,520,997,376 bytes (0x227F7FF sectors) 18,520,993,792 bytes(0x44FEFF clusters)
1 st sector	213,909,504 sector (0x0CC00000)



[그림 12] GPT 파티션 엔트리 수정 후 모습

최종적으로 각 파티션의 1st sector 를 GPT 파티션 엔트리의 start LBA 영역에 대입하고, 1st sector와 capacity 를 더한 값에 -1 을 해서 end LBA 영역에 대입한 뒤 FTK imager로 열어보면 인식되지 않았던 파티션들이 모두 정상적으로 인식됨을 확인할 수 있습니다.

2) Which volumes are connected to more than one system? Analyze the following information for those volumes. (50 points)

- Partition type, 1st sector(physical)

	이름	크기	유형	수정한 날짜
	\$130	4[Missing s...]	NTFS 색인 할당	2023-07-30 오후 2:56:04
	Dyn. Disk Set A, Disk 1.e01	9,749[Missi...]	일반 파일	2010-04-08 오후 9:09:00
	Dyn. Disk Set A, Disk 2.e01	9,691[Missi...]	일반 파일	2010-04-08 오후 9:11:00
	Dyn. Disk Set A, Disk 3.e01	9,867[Missi...]	일반 파일	2010-04-08 오후 9:13:00
	Dyn. Disk Set B, Disk 1.e01	10,795[Missi...]	일반 파일	2010-04-08 오후 9:14:00
	RAID0 1.e01	861[Missin...]	일반 파일	2010-06-10 오전 8:24:40
	RAID0 2.e01	823[Missin...]	일반 파일	2010-06-10 오전 8:24:48
	RAID0 3.e01	853[Missin...]	일반 파일	2010-06-10 오전 8:24:54

[그림 13] 파티션 6(NTFS) 내 존재하는 동적 디스크 이미지와 RAID0 디스크 이미지

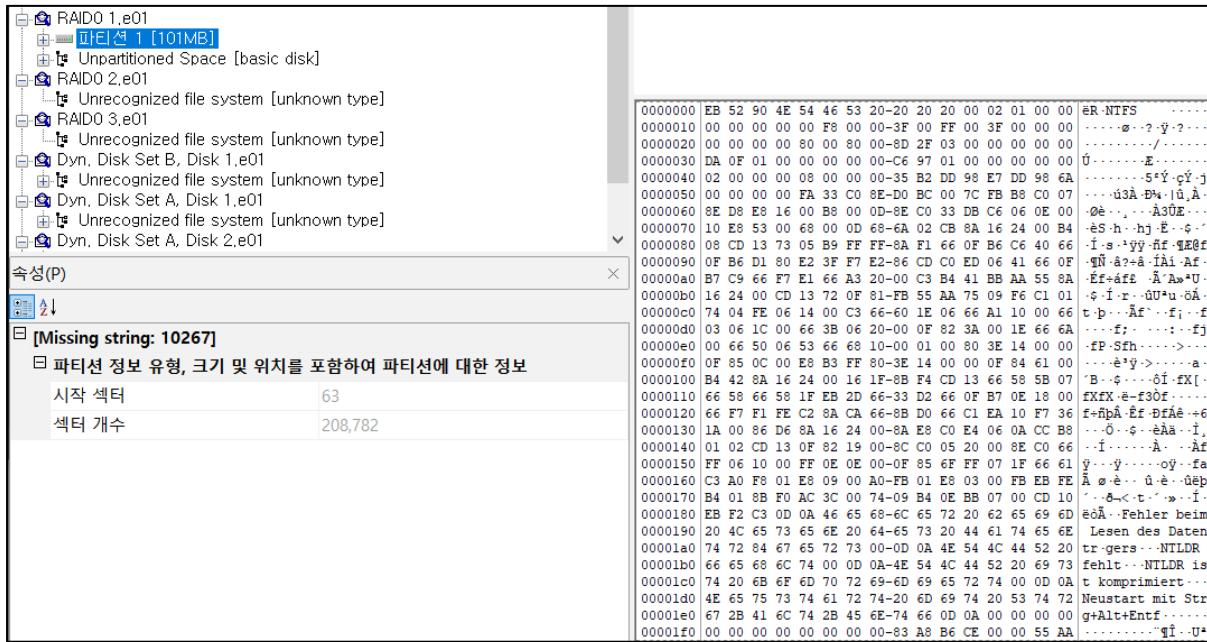
PartitionFinder.008 내에 있던 NTFS 파티션 6에서는 동적 디스크와 RAID0가 존재하는 것을 알 수 있습니다. 동적 디스크는 생성 시 저장 장치를 볼륨으로 인식하기 때문에 문제에서 요구하는 둘 이상의 시스템에 연결된 볼륨들은 위 그림에서 발견된 볼륨들로 볼 수 있습니다.

● RAID 0 1~3.e01 – NTFS

00000000	33 C0 8E D0 BC 00 7C FB-50 07 50 1F FC BE 1B 7C	3Ã·Ð¾· ûP·P·ü¾·
00000010	BF 1B 06 50 57 B9 E5 01-F3 A4 CB BD BE 07 B1 04	ç··PW¹å·ÓñÈ¾·±·
00000020	38 6E 00 7C 09 75 13 83-C5 10 E2 F4 CD 18 8B F5	8n· ·u··À·âôí··ô
00000030	83 C6 10 49 74 19 38 2C-74 F6 A0 B5 07 B4 07 8B	·È·It·8,tö u····
00000040	F0 AC 3C 00 74 FC BB 07-00 B4 0E CD 10 EB F2 88	ð-<·tü»···Í·ëo·
00000050	4E 10 E8 46 00 73 2A FE-46 10 80 7E 04 0B 74 0B	N·èF·s*pF····t·
00000060	80 7E 04 0C 74 05 A0 B6-07 75 D2 80 46 02 06 83	·~··t· ¼·uÒ·F···
00000070	46 08 06 83 56 0A 00 E8-21 00 73 05 A0 B6 07 EB	F···V··è!·s· ¼·ë
00000080	BC 81 3E FE 7D 55 AA 74-0B 80 7E 10 00 74 C8 A0	%->p}U^t····tÈ
00000090	B7 07 EB A9 8B FC 1E 57-8B F5 CB BF 05 00 8A 56	··ë@·ü·W·ôÈç···V
000000a0	00 B4 08 CD 13 72 23 8A-C1 24 3F 98 8A DE 8A FC	···Í·r#·Á\$?···p·ü
000000b0	43 F7 E3 8B D1 86 D6 B1-06 D2 EE 42 F7 E2 39 56	C=ä·Ñ·Ö±·ÖiB+â9V
000000c0	0A 77 23 72 05 39 46 08-73 1C B8 01 02 BB 00 7C	·w#r·9F·s···»··l
000000d0	8B 4E 02 8B 56 00 CD 13-73 51 4F 74 4E 32 E4 8A	·N··V·í·sQOtN2ä·
000000e0	56 00 CD 13 EB E4 8A 56-00 60 BB AA 55 B4 41 CD	V·Í·ëä·V··»·U'AÍ
000000f0	13 72 36 81 FB 55 AA 75-30 F6 C1 01 74 2B 61 60	·r6·ûU^u0öÀ·t+a`

[그림 14] RAID 0 1.e01에서 인식되는 MBR

RAID 0 1~3.e01을 각각 FTK Imager로 열어보면, RAID 0 1.e01파일에서만 MBR이 발견되는 것을 확인하였습니다.



[그림 15] NTFS 파티션 존재 확인

또한, RAID0 1.e01 파일에서 NTFS VBR이 존재하고 파티션 인식이 되는 것을 확인하였습니다. 나머지 RAID0 2.e01와 RAID0 3.e01파일은 NTFS FILE 시그니처가 발견되고 RAID0 3.e01에는 NTFS VBR 백업본이 존재하는 것으로 보아 연속된 데이터가 3개의 e01으로 저장된 것으로 판단하였습니다.

1st sector는 PartitionFinder 이미지 기준으로 RAID 0 1.e01 이미지 데이터가 처음으로 위치하는 섹터로 살펴보면 124,295,920 sector입니다. 하지만, 따로 RAID 볼륨이 존재한다면 RAID0 1~3.e01을 raw로 변환하여 데이터를 모두 접합한 후 NTFS 파티션에 대한 기준으로 계산하게 되면 1st sector는 63 섹터로 확인할 수 있습니다.

[표 8] RAID 볼륨 내 파티션 정보

속성	값
Partition Type	NTFS
1 st sector	63 sector

● Dyn. Disk Set A, Disk 1~3.e01

동적 디스크 Set A의 Disk에는 Disk 1, 2, 3 모두 MBR이 존재합니다. 또한, 해당 디스크 볼륨에는 4개의 파티션이 존재합니다.

■ 첫번째 파티션 - NTFS

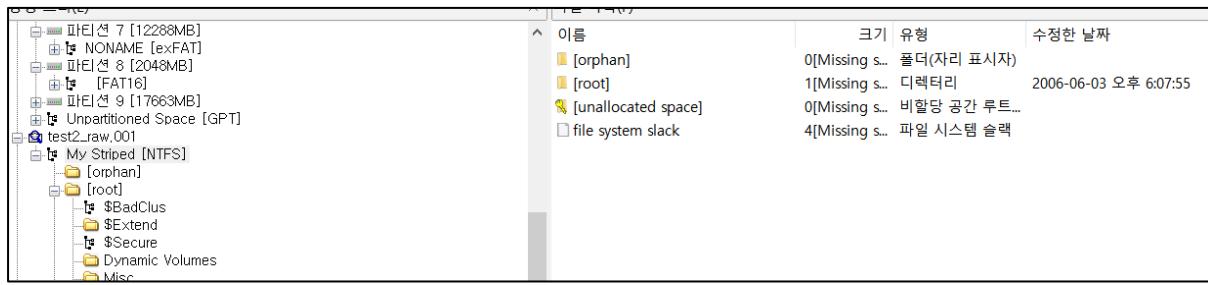
				섹터 63
00007E00	EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00	ER.NTFS	
00007E10	00 00 00 00 00 F8 00 00 01 00 01 00 1D 00 00 00ø.....		
00007E20	00 00 00 00 80 00 80 00 FF FF 17 00 00 00 00 00€.€.yy.....		
00007E30	04 00 00 00 00 00 00 00 FF 7F 01 00 00 00 00 00y.....		
00007E40	F6 00 00 00 01 00 00 B8 AA 4B 48 CF 4B 48 98	ö.....,"KHÍKH"		
00007E50	00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB B8 C0 07ú3ÀŽÐ¶. ù,À.		
00007E60	8E D8 E8 16 00 B8 00 0D 8E C0 33 DB C6 06 0E 00	žØè...žÀ3ÚÈ...		
00007E70	10 E8 53 00 68 00 0D 68 6A 02 CB 8A 16 24 00 B4	.èS.h..hj.ÈŠ.Ş..		
00007E80	08 CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66	.í.s.^yyŠñf.QEØf		
00007E90	0F B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F	.qÑeå?-å+íÀi.Af.		
00007EA0	B7 C9 66 F7 E1 66 A3 20 00 C3 B4 41 BB AA 55 8A	.Éf-áff .Ã'À»*UŠ		
00007EB0	16 24 00 CD 13 72 0F 81 FB 55 AA 75 09 F6 C1 01	.\$.í.r..úU*u.óÁ.		
00007EC0	74 04 FE 06 14 00 C3 66 60 1E 06 66 A1 10 00 66	t.p...Äf`..f;..f		
00007ED0	03 06 1C 00 66 3B 06 20 00 0F 82 3A 00 1E 66 6Af;..,;...fj		
00007EE0	00 66 50 06 53 66 68 10 00 01 00 80 3E 14 00 00	.fP.Sfh....€>...		
00007EF0	0F 85 0C 00 E8 B3 FF 80 3E 14 00 00 0F 84 61 00è^y€>....,a.		
00007F00	B4 42 8A 16 24 00 16 1F 8B F4 CD 13 66 58 5B 07	'BŠ.Ş...<óí.fX[.		
00007F10	66 58 66 58 1F EB 2D 66 33 D2 66 0F B7 0E 18 00	fXfx.é-f3Øf.		
00007F20	66 F7 F1 FE C2 8A CA 66 8B D0 66 C1 EA 10 F7 36	f-ñpÅŠEf<ØfAé..÷6		
00007F30	1A 00 86 D6 8A 16 24 00 8A E8 C0 E4 06 0A CC B8	..tÖŠ.Ş.ŞèÀä..í.		
00007F40	01 02 CD 13 0F 82 19 00 8C C0 05 20 00 8E C0 66	..í,...,çÀ. .žÄf		
00007F50	FF 06 10 00 FF 0E 0E 00 0F 85 6F FF 07 1F 66 61	ÿ...ÿ....oÿ..fa		
00007F60	C3 A0 F8 01 E8 09 00 A0 FB 01 E8 03 00 FB EB FE	Ã ø.è.. ú.è..úëp		
00007F70	B4 01 8B F0 AC 3C 00 74 09 B4 0E BB 07 00 CD 10	'.<ð-<.t.'..í.		
00007F80	EB F2 C3 0D 0A 41 20 64 69 73 6B 20 72 65 61 64	ëòÃ..A disk read		
00007F90	20 65 72 72 6F 72 20 6F 63 63 75 72 72 65 64 00	error occurred.		
00007FA0	0D 0A 4E 54 4C 44 52 20 69 73 20 6D 69 73 73 69	..NTLDR is missi		
00007FB0	6E 67 00 0D 0A 4E 54 4C 44 52 20 69 73 20 63 6F	ng...NTLDR is co		
00007FC0	6D 70 72 65 73 73 65 64 00 0D 0A 50 72 65 73 73	mpressed...Press		
00007FD0	20 43 74 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F	Ctrl+Alt+Del to		
00007FE0	20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00	restart.....		
00007FF0	00 00 00 00 00 00 00 00 83 A0 B3 C9 00 00 55 AAf ^É..U^		

[그림 16] 첫번째 파티션 NTFS의 VBR

해당 NTFS 파티션 역시 동적 디스크 볼륨 내 1st sector는 63 번째 섹터에 위치하게 됩니다.

[표 9] 동적 디스크 A 볼륨 내 첫번째 파티션 정보

속성	값
Partition Type	NTFS
1 st sector	63 sector



[그림 17] Striped 디스크 이미지 인식

해당 NTFS 파티션은 카빙 시 My Striped라는 파티션 이름과 함께 스트라이프 볼륨임을 확인하였습니다.

■ 두번째 파티션 – FAT32

10007E00	EB 58 90 4D 53 44 4F 53 35 2E 30 00 02 04 20 00	ëX.MSDOS5.0.... .	섹터 524,351
10007E10	02 00 00 00 00 F8 00 00 01 00 01 00 1D 00 00 00ø.....	
10007E20	00 00 08 00 FC 03 00 00 00 00 00 00 02 00 00 00ü.....	
10007E30	01 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00	
10007E40	80 00 29 8E D9 64 90 4E 4F 20 4E 41 4D 45 20 20	€.)ŽÙd.NO NAME	
10007E50	20 20 46 41 54 33 32 20 20 33 C9 8E D1 BC F4	FAT32 3EŽÑµö	
10007E60	7B 8E C1 8E D9 BD 00 7C 88 4E 02 8A 56 40 B4 08	{ŽÄŽÙí. ~N.ŠV@`.	
10007E70	CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66 0F	í.s.^yyŠñf.QE@f.	
10007E80	B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F B7	¶Ñeâ?~åtiÀi.Af.~	
10007E90	C9 66 F7 E1 66 89 46 F8 83 7E 16 00 75 38 83 7E	Éf~áft;Føf~..u8f~	
10007EA0	2A 00 77 32 66 8B 46 1C 66 83 C0 OC BB 00 80 B9	*.w2f< F. ffÀ.»..€`	
10007EB0	01 00 E8 2B 00 E9 48 03 A0 FA 7D B4 7D 8B F0 AC	..è+.éH. ú`'}<ð-	
10007EC0	84 C0 74 17 3C FF 74 09 B4 0E BB 07 00 CD 10 EB	„Àt.<ýt.'..»..í.ë	
10007ED0	EE A0 FB 7D EB E5 A0 F9 7D EB E0 98 CD 16 CD 19	i ú}ëå ú)ëå~í.i.	
10007EE0	66 60 66 3B 46 F8 0F 82 4A 00 66 6A 00 66 50 06	f`f;Fø.,J.fj.fP.	
10007EF0	53 66 68 10 00 01 00 80 7E 02 00 0F 85 20 00 B4	Sfh....€~.....	
10007F00	41 BB AA 55 8A 56 40 CD 13 0F 82 1C 00 81 FB 55	»*UŠV@í.....úU	
10007F10	AA 0F 85 14 00 F6 C1 01 0F 84 0D 00 FE 46 02 B4	*.....öÁ.....þF.'	
10007F20	42 8A 56 40 8B F4 CD 13 B0 F9 66 58 66 58 66 58	BŠV@ <i>öí.</i> °ùfXfXfX	
10007F30	66 58 EB 2A 66 33 D2 66 0F B7 4E 18 66 F7 F1 FE	fXë*f3Öf.·N.f~ñp	
10007F40	C2 8A CA 66 8B D0 66 C1 EA 10 F7 76 1A 86 D6 8A	ÂšÈf<ĐfÀè.÷v.+tÖš	
10007F50	56 40 8A E8 C0 E4 06 0A CC B8 01 02 CD 13 66 61	V@ŠèÀa..í...í.fa	
10007F60	0F 82 54 FF 81 C3 00 02 66 40 49 0F 85 71 FF C3	,,Tý.Ã..f@I...qýÃ	
10007F70	4E 54 4C 44 52 20 20 20 20 20 00 00 00 00 00 00 00	NTLDR	
10007F80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
10007F90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
10007FA0	00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 4E 54NT	
10007FB0	4C 44 52 20 69 73 20 6D 69 73 73 69 6E 67 FF 0D	LDR is missingý.	
10007FC0	0A 44 69 73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72	.Disk errorý..Pr	
10007FD0	65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 72	ess any key to r	
10007FE0	65 73 74 61 72 74 0D 0A 00 00 00 00 00 00 00 00	estart.....	
10007FF0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA~í..U*	

[그림 18] 두번째 파티션 FAT32의 VBR

[표 10] 동적 디스크 A 볼륨 내 두번째 파티션 정보

속성	값
Partition Type	FAT32
1 st sector	524,351 sector

■ 세번째 파티션 – FAT32

201B9A00	EB 58 90 4D 53 44 4F 53 35 2E 30 00 02 04 20 00	eX.MSDOS5.0.... .	섹터 1,052,109
201B9A10	02 00 00 00 00 F8 00 00 01 00 01 00 1D 00 00 00Ø.....	
201B9A20	00 00 08 00 FC 03 00 00 00 00 00 00 02 00 00 00ü.....	
201B9A30	01 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00	
201B9A40	80 00 29 8E D9 64 90 4E 4F 20 4E 41 4D 45 20 20	€.) Žd.NO NAME	
201B9A50	20 20 46 41 54 33 32 20 20 20 33 C9 8E D1 BC F4	FAT32 3EŽN46	
201B9A60	7B 8E C1 8E D9 BD 00 7C 88 4E 02 8A 56 40 B4 08	{ŽÄŽÜš. ^N.ŠV@.	
201B9A70	CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66 0F	í.s. ^yyŠnf. QE@f.	
201B9A80	B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F B7	qÑeå?åtíAi.Af..	
201B9A90	C9 66 F7 E1 66 89 46 F8 83 7E 16 00 75 38 83 7E	Éf-åf%Føf~..u8f~	
201B9AA0	2A 00 77 32 66 8B 46 1C 66 83 C0 0C BB 00 80 B9	*.w2f<F.fffÀ..».	
201B9AB0	01 00 E8 2B 00 E9 48 03 A0 FA 7D B4 7D 8B F0 AC	..è+.ÉH. ú} »	
201B9AC0	84 C0 74 17 3C FF 74 09 B4 0E BB 07 00 CD 10 EB	.Àt.<yt. '»..í.é	
201B9AD0	EE A0 FB 7D EB E5 A0 F9 7D EB E0 98 CD 16 CD 19	i ú)éå ù)éå"í.í.	
201B9AE0	66 60 66 3B 46 F8 0F 82 4A 00 66 6A 00 66 50 06	f`f;Fø.,J.fj.fp.	
201B9AF0	53 66 68 10 00 01 00 80 7E 02 00 0F 85 20 00 B4	Sfh....€~.....	
201B9B00	41 BB AA 55 8A 56 40 CD 13 0F 82 1C 00 81 FB 55	A»*UŠV@í...,...úU	
201B9B10	AA 0F 85 14 00 F6 C1 01 0F 84 0D 00 FE 46 02 B4	*....öÅ....pF.	
201B9B20	42 8A 56 40 8B F4 CD 13 B0 F9 66 58 66 58 66 58	BŠVø<ðí. "ùfxfxfx	
201B9B30	66 58 EB 2A 66 33 D2 66 0F B7 4E 18 66 F7 F1 FE	fxé*x3òf. -N.f-ñp	
201B9B40	C2 8A CA 66 8B D0 66 C1 EA 10 F7 76 1A 86 D6 8A	ÁšEf<ĐfÁé..÷v.+Öš	
201B9B50	56 40 8A E8 C0 E4 06 0A CC B8 01 02 CD 13 66 61	V@šèÀä..ì...í.fa	
201B9B60	0F 82 54 FF 81 C3 00 02 66 40 49 0F 85 71 FF C3	,,Ty.Å..f@I...qyÅ	
201B9B70	4E 54 4C 44 52 20 20 20 20 20 00 00 00 00 00 00	NTLDR	
201B9B80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
201B9B90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
201B9BA0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 0D OA 4E 54NT	
201B9BB0	4C 44 52 20 69 73 20 6D 69 73 73 69 6E 67 FF OD	LDR is missingy.	
201B9BC0	0A 44 69 73 6B 20 65 72 6F 72 FF OD OA 50 72	.Disk errory..Pr	
201B9BD0	65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 72	ess any key to r	
201B9BE0	65 73 74 61 72 74 0D OA 00 00 00 00 00 00 00 00	estart.....	
201B9BF0	00 00 00 00 00 00 00 00 00 AC BF CC 00 00 55 AA-í..U*	

[그림 19] 세번째 파티션 FAT32의 VBR

└─ FAT32test.001	00000000 4D 59 20 4D 49 52 52 4F-52 45 44 08 00 00 00 00 MY MIRRORED.....
└─ MY MIRRORED [FAT32]	00000010 00 00 00 00 00 00 61 9F-C3 34 00 00 00 00 00 00a.À.....
└─ [root]	00000020 42 65 00 73 00 00 00 FF-FF FF FF 0F 00 43 FF FF Be-s...yyý...CYý
└─ Dynamic Volumes	00000030 FF yyyyyyyyyy...ÿÿÿ
└─ Misc	00000040 01 44 00 79 00 6E 00 61-00 6D 00 0F 00 43 69 00 .D-y-n-a-m-..C1.
└─ Pictures	00000050 63 00 20 00 56 00 6F 00-6C 00 00 75 00 6D 00 c..V-o-l..u-m.
└─ [unallocated space]	00000060 44 59 4E 41 4D 49 7E 31-20 20 20 10 00 70 ED A0 DYNAMIC-1..pi.
└─ FAT32test.001	00000070 C3 34 C3 34 00 00 EE A0-C3 34 03 00 00 00 00 00 À4À4..i.À4.....
└─ [fat:fj-ÀéR p [FAT32]	00000080 41 50 00 69 00 63 00 74-00 75 00 0F 00 59 72 00 AP-i-c-t-u..Yr.
└─ [root]	00000090 65 00 73 00 00 00 FF-FF FF FF 00 0F 00 FF FF FF e-s...yyý...ÿÿý
└─ Dynamic Volumes	000000a0 50 49 43 54 55 52 45 53-20 20 10 00 49 F2 A0 PICTURES..Íó.
└─ Misc	000000b0 C3 34 C3 34 00 00 F3 A0-C3 34 19 00 00 00 00 00 À4À4..6 À4.....
└─ Pictures	000000c0 41 4D 00 69 00 73 00 63-00 00 0F 00 90 FF FF AM-i-s-c..ÿý
└─ [unallocated space]	000000d0 FF yyyyyyyyyy...ÿÿÿ
└─ FAT32test.001	000000e0 4D 49 53 43 20 20 20 20 20 10 00 60 FC A0 MISC ..ü
└─ FAT32test.001	000000f0 C3 34 C3 34 00 00 FD A0-C3 34 4E 09 00 00 00 00 À4À4..ý À4N.....
└─ FAT32test.001	00000100 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 ..

[그림 20] 미러 디스크 확인

세번째 파티션 FAT32는 두번째에서 살펴본 FAT32와 VSN도 같고 섹터 사이즈도 같으며, 두번째 파티션에서 파티션 이름이 MY MIRRORED인 것으로 보아 미러 디스크 쌍임을 알 수 있습니다.

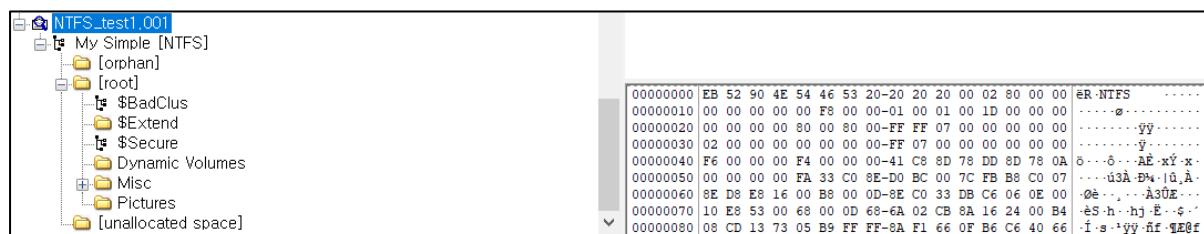
[표 11] 동적 디스크 A 볼륨 내 세번째 파티션 정보

속성	값
Partition Type	FAT32
1 st sector	1,052,109 sector

■ 네번째 파티션 - NTFS

5036B600	EB 52 90 4E 54 46 53 20 20 20 20 00 02 80 00 00	ëR.NTFS ..€..	섹터 2,628,443
5036B610	00 00 00 00 00 F8 00 00 01 00 01 00 1D 00 00 00ø.....	
5036B620	00 00 00 00 80 00 80 00 FF FF 07 00 00 00 00 00€.€.ÿÿ.....	
5036B630	02 00 00 00 00 00 00 00 FF 07 00 00 00 00 00 00ÿ.....	
5036B640	F6 00 00 00 F4 00 00 00 41 C8 8D 78 DD 8D 78 0A	ö...ö...AE.xÝ.x.	
5036B650	00 00 00 00 FA 33 C0 8E DO BC 00 7C FB B8 C0 07	...ú3ÀŽÐ4. û,À.	
5036B660	8E D8 E8 16 00 B8 00 0D 8E C0 33 DB C6 06 0E 00	žøè...,žÀ3ÛÈ...	
5036B670	10 E8 53 00 68 00 0D 68 6A 02 CB 8A 16 24 00 B4	.èS.h..hj.ÉŠ.Ş..	
5036B680	08 CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66	.í.s.ÿÿšñf.ÿEëf	
5036B690	0F B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F	.ÿNéá?åtíÀi.Af.	
5036B6A0	B7 C9 66 F7 E1 66 A3 20 00 C3 B4 41 BB AA 55 8A	·éF-áf£.Ã'À»*UŠ	
5036B6B0	16 24 00 CD 13 72 0F 81 FB 55 AA 75 09 F6 C1 01	\$.í.r..ûU*u.öA.	
5036B6C0	74 04 FE 06 14 00 C3 66 60 1E 06 66 A1 10 00 66	t.p...Ãf`..f...f	
5036B6D0	03 06 1C 00 66 3B 06 20 00 0F 82 3A 00 1E 66 6Af;.. ,.,:..fj	
5036B6E0	00 66 50 06 53 66 68 10 00 01 00 80 3E 14 00 00	.fP.Sfh....€>...	
5036B6F0	0F 85 0C 00 E8 B3 FF 80 3E 14 00 00 0F 84 61 00è'ÿ€>....,a.	
5036B700	B4 42 8A 16 24 00 16 1F 8B F4 CD 13 66 58 5B 07	'BŠ.Ş...<óí.FX[.	
5036B710	66 58 66 58 1F EB 2D 66 33 D2 66 0F B7 0E 18 00	fXfX.ë-f3òf....	
5036B720	66 F7 F1 FE C2 8A CA 66 8B D0 66 C1 EA 10 F7 36	f-ñpÅŠéf<ðrÁæ.-é	
5036B730	1A 00 86 D6 8A 16 24 00 8A E8 C0 E4 06 0A CC B8	..tÖŠ.Ş..šèÀä..í.	
5036B740	01 02 CD 13 0F 82 19 00 8C C0 05 20 00 8E CO 66	..í...,.çÀ..žÄf	
5036B750	FF 06 10 00 FF 0E 0E 00 0F 85 6F FF 07 1F 66 61	ÿ...ÿ.....oÿ..fa	
5036B760	C3 A0 F8 01 E8 09 00 A0 FB 01 E8 03 00 FB EB FE	À ø.è.. û.è..üép	
5036B770	B4 01 8B F0 AC 3C 00 74 09 B4 0E BB 07 00 CD 10	'.<ë- <t>.'.»..í.</t>	
5036B780	EB F2 C3 0D 0A 41 20 64 69 73 6B 20 72 65 61 64	ëðÀ..A disk read	
5036B790	20 65 72 72 6F 72 20 6F 63 63 75 72 72 65 64 00	error occurred.	
5036B7A0	0D 0A 4E 54 4C 44 52 20 69 73 20 6D 69 73 73 69	..NTLDR is missi	
5036B7B0	6E 67 00 0D 0A 4E 54 4C 44 52 20 69 73 20 63 6F	ng...NTLDR is co	
5036B7C0	6D 70 72 65 73 73 65 64 00 0D 0A 50 72 65 73 73	mpressed...Press	
5036B7D0	20 43 74 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F	Ctrl+Alt+Del to	
5036B7E0	20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00	restart.....	
5036B7F0	00 00 00 00 00 00 00 00 83 A0 B3 C9 00 00 55 AAf 'É..U*	

[그림 21] 네번째 파티션 NTFS의 VBR



[그림 22] 네번째 파티션 정보

해당 파티션은 카빙 시 My Simple 이란 파티션 이름으로 인식되어 단순 볼륨임을 확인하였습니다.

[표 12] 동적 디스크 A 볼륨 내 네번째 파티션 정보

속성	값
Partition Type	NTFS
1 st sector	2,628,443 sector

● Dyn. Disk Set B, Disk 1.e01

■ 첫번째 파티션 - NTFS

00007E00	EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00	éR.NTFS	섹터 63
00007E10	00 00 00 00 00 F8 00 00 01 00 01 00 1D 00 00 00ø.....	
00007E20	00 00 00 00 80 00 80 00 FF FF 0F 00 00 00 00 00 00é.é.ÿ.....	
00007E30	04 00 00 00 00 00 00 00 00 00 FF FF 00 00 00 00 00 00ÿ.....	
00007E40	F6 00 00 00 01 00 00 00 9C AC 81 F0 D4 81 F0 24	ö.....œ-øö.ø\$	
00007E50	00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB B8 C0 07ú3ÀžD4. ù,À.	
00007E60	8E D8 E8 16 00 B8 00 0D 8E C0 33 DB C6 06 0E 00	Žøè.....žA3ÚÈ...	
00007E70	10 E8 53 00 68 00 0D 68 6A 02 CB 8A 16 24 00 B4	.éS.h..hj.ÉS.S.	
00007E80	08 CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66	.í.s.ÿyšñf.¶E@f	
00007E90	0F B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F	.TÑ€á?åtÍÁi.Af.	
00007EA0	B7 C9 66 F7 E1 66 A3 20 00 C3 B4 41 BB AA 55 8A	·Éf-áff .Á`A»*Uš	
00007EB0	16 24 00 CD 13 72 0F 81 FB 55 AA 75 09 F6 C1 01	.\$.í.r..üU*u.øÁ.	
00007EC0	74 04 FE 06 14 00 C3 66 60 1E 06 66 A1 10 00 66	t.p...Åf`..fj..f	
00007ED0	03 06 1C 00 66 3B 06 20 00 0F 82 3A 00 1E 66 6Af;.. ,:..fj	
00007EE0	00 66 50 06 53 66 68 10 00 01 00 80 3E 14 00 00	.fP.Sfh....€>....	
00007EF0	0F 85 0C 00 E8 B3 FF 80 3E 14 00 00 0F 84 61 00è³ÿ€>....,a.	
00007F00	B4 42 8A 16 24 00 16 1F 8B F4 CD 13 66 58 5B 07	'BŠ.\$...<ðí.fX[.	
00007F10	66 58 66 58 1F EB 2D 66 33 D2 66 0F B7 0E 18 00	fXfX.ë-f3òf.	
00007F20	66 F7 F1 FE C2 8A CA 66 8B DO 66 C1 EA 10 F7 36	f-ñpÅŠEf<ĐfÁè..÷6	
00007F30	1A 00 86 D6 8A 16 24 00 8A E8 C0 E4 06 0A CC B8	..+ÖŠ.\$..ŠèÀä..ì.	
00007F40	01 02 CD 13 0F 82 19 00 8C C0 05 20 00 8E C0 66	..í,...,GÀ. .žÀf	
00007F50	FF 06 10 00 FF 0E 0E 00 0F 85 6F FF 07 1F 66 61	ÿ...ÿ.....oÿ..fa	
00007F60	C3 A0 F8 01 E8 09 00 A0 FB 01 E8 03 00 FB EB FE	Ã ø.è.. ü.è..üëþ	
00007F70	B4 01 8B F0 AC 3C 00 74 09 B4 0E BB 07 00 CD 10	'.<ð- <t.>..í.</t.>	
00007F80	EB F2 C3 0D 0A 41 20 64 69 73 6B 20 72 65 61 64	ëòÃ..A disk read	
00007F90	20 65 72 72 6F 72 20 6F 63 63 75 72 72 65 64 00	error occurred.	
00007FA0	0D 0A 4E 54 4C 44 52 20 69 73 20 6D 69 73 73 69	..NTLDR is missi	
00007FB0	6E 67 00 0D 0A 4E 54 4C 44 52 20 69 73 20 63 6F	ng...NTLDR is co	
00007FC0	6D 70 72 65 73 73 65 64 00 0D 0A 50 72 65 73 73	mpressed...Press	
00007FD0	20 43 74 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F	Ctrl+Alt+Del to	
00007FE0	20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00	restart.....	
00007FF0	00 00 00 00 00 00 00 00 83 A0 B3 C9 00 00 55 AAf 'É..U*	

[그림 23] 동적 디스크 B 내 NTFS 파티션 VBR

NTFS_test2.001	My RAID 5 [NTFS]	éR.NTFS
	[orphan]ø.....
	[root]ÿ.....
	[unallocated space]é.é.ÿ.....
속성(P)		
Missing string: 10267		
파일 시스템 정보		
클러스터 크기	4,096	éR.NTFS
클러스터 개수	131,071ø.....
사용 중이 아닌 클러스터 개수	62,815ÿ.....
더티 플래그	FALSEé.é.ÿ.....
볼륨 레이블	My RAID 5é.é.ÿ.....
볼륨 일련 번호	F081-AC9Cé.é.ÿ.....
파일 시스템 버전	Windows 2000 (NTFS 3.0)é.é.ÿ.....

[그림 24] 카빙 후 확인한 파티션 정보

동적 디스크 B 볼륨 내에는 My RAID 5 라는 이름으로 NTFS 파티션이 첫번째로 존재함을 확인하였습니다.

[표 13] 동적 디스크 B 볼륨 내 첫번째 파티션 정보

속성	값
Partition Type	NTFS
1 st sector	63 sector

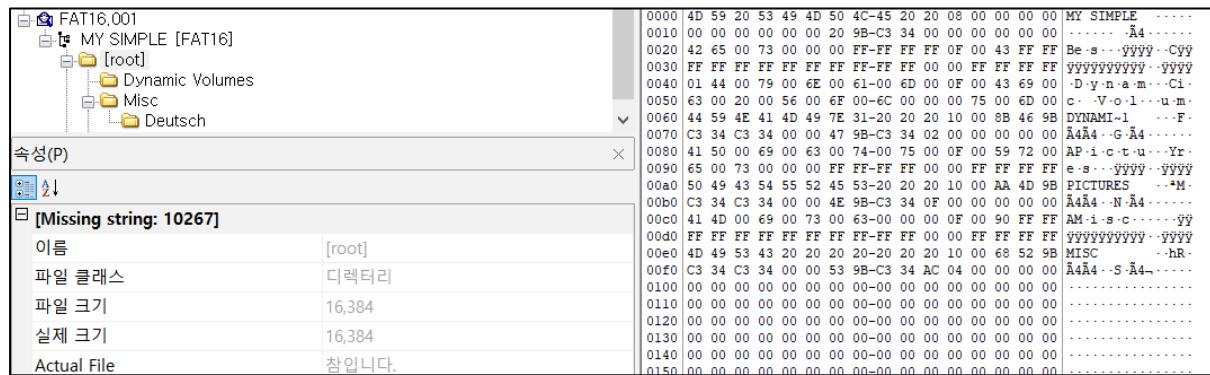
■ 두번째 파티션 – FAT16

```

10007E00 EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 08 01 00 <..MSDOS5.0.... 석터 524,351
10007E10 02 00 02 00 00 F8 00 01 01 00 01 00 1D 00 00 00 .....Ø.....
10007E20 00 00 08 00 80 00 29 3D 16 A4 FC 4E 4F 20 4E 41 ....€.)=¤ÜNO NA
10007E30 4D 45 20 20 20 46 41 54 31 36 20 20 20 33 C9 ME FAT16 3É
10007E40 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C ŽÑ¤g(ŽÙ.. ŽÄÜ¤.|
10007E50 38 4E 24 7D 24 8B C1 99 E8 3C 01 72 1C 83 EB 3A 8NS}S<Á¤e<.r.fë:
10007E60 66 A1 1C 7C 26 66 3B 07 26 8A 57 FC 75 06 80 CA f;.|&f;..&SWüu.€È
10007E70 02 88 56 02 80 C3 10 73 EB 33 C9 8A 46 10 98 F7 .~V.€Ã.së3ÉŠF.~+
10007E80 66 16 03 46 1C 13 56 1E 03 46 0E 13 D1 8B 76 11 f..F..V..F..Ñ<v.
10007E90 60 89 46 FC 89 56 FE B8 20 00 F7 E6 8B 5E 0B 03 `%FükVp, .~æ<^..
10007EA0 C3 48 F7 F3 01 46 FC 11 4E FE 61 BF 00 00 E8 E6 ÄH¤ó.Fü.Npaç..èæ
10007EB0 00 72 39 26 38 2D 74 17 60 B1 0B BE A1 7D F3 A6 .r9&8-t.`±.%}ó;
10007EC0 61 74 32 4E 74 09 83 C7 20 3B FB 72 E6 EB DC A0 at2Nt.fç ;üræéÜ
10007ED0 FB 7D B4 7D 8B F0 AC 98 40 74 OC 48 74 13 B4 0E Ù} `}ç{~@t.Ht.`.
10007EE0 BB 07 00 CD 10 EB EF A0 FD 7D EB E6 A0 FC 7D EB »..í.ëí ý}ëæ ü}ë
10007EF0 E1 CD 16 CD 19 26 8B 55 1A 52 B0 01 BB 00 00 E8 áí.í.&<U.R°.»..ë
10007F00 3B 00 72 E8 5B 8A 56 24 BE 0B 7C 8B FC C7 46 F0 ;.rè[ŠVS%4.|<üÇFð
10007F10 3D 7D C7 46 F4 29 7D 8C D9 89 4E F2 89 4E F6 C6 =>ÇFð) }ŒÙ¤Nò¤Nö¤
10007F20 06 96 7D CB EA 03 00 00 20 0F B6 C8 66 8B 46 F8 .->Èë... .¶Èf< Fø
10007F30 66 03 46 1C 66 8B D0 66 C1 EA 10 EB 5E 0F B6 C8 f.F.f<ÐfÁê.ë^..¶È
10007F40 4A 4A 8A 46 0D 32 E4 F7 E2 03 46 FC 13 56 FE EB JJŠF.2ä+â.Fü.Vpë
10007F50 4A 52 50 06 53 6A 01 6A 10 91 8B 46 18 96 92 33 JRP.Sj.j.'<F.-'3
10007F60 D2 F7 F6 91 F7 F6 42 87 CA F7 76 1A 8A F2 8A E8 Ö¤ö'÷ÖB‡È+~v.ŠòŠè
10007F70 C0 CC 02 0A CC B8 01 02 80 7E 02 0E 75 04 B4 42 Äì..í...ë~..u. B
10007F80 8B F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03 <öŠVSí.aar.@u.B.
10007F90 5E 0B 49 75 06 F8 C3 41 BB 00 00 60 66 6A 00 EB ^..Iu.øÅA»...`fj.ë
10007FA0 B0 4E 54 4C 44 52 20 20 20 20 20 0D 0A 4E 54 °NTLDR ..NT
10007FB0 4C 44 52 20 69 73 20 6D 69 73 69 6E 67 FF 0D LDR is missing.
10007FC0 0A 44 69 73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72 .Disk error..Pr
10007FD0 65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 72 ess any key to r
10007FE0 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00 00 00 estart.....
10007FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....-çIU^

```

[그림 25] 동적 디스크 B 내 FAT 16 파티션 VBR



[그림 26] 카빙 후 확인한 파티션 정보

동적 디스크 B 볼륨 내에는 MY SIMPLE이라는 이름으로 FAT16 파티션이 두번째로 존재함을 확인하였습니다.

[표 14] 동적 디스크 B 볼륨 내 두번째 파티션 정보

속성	값
Partition Type	FAT16
1 st sector	524,351 sector