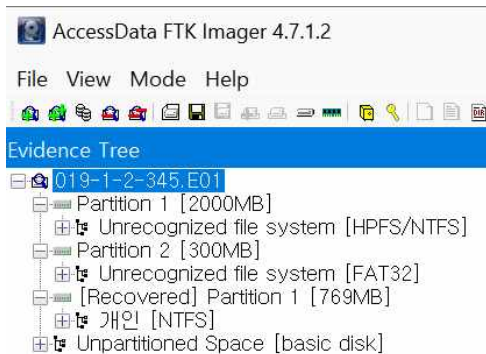


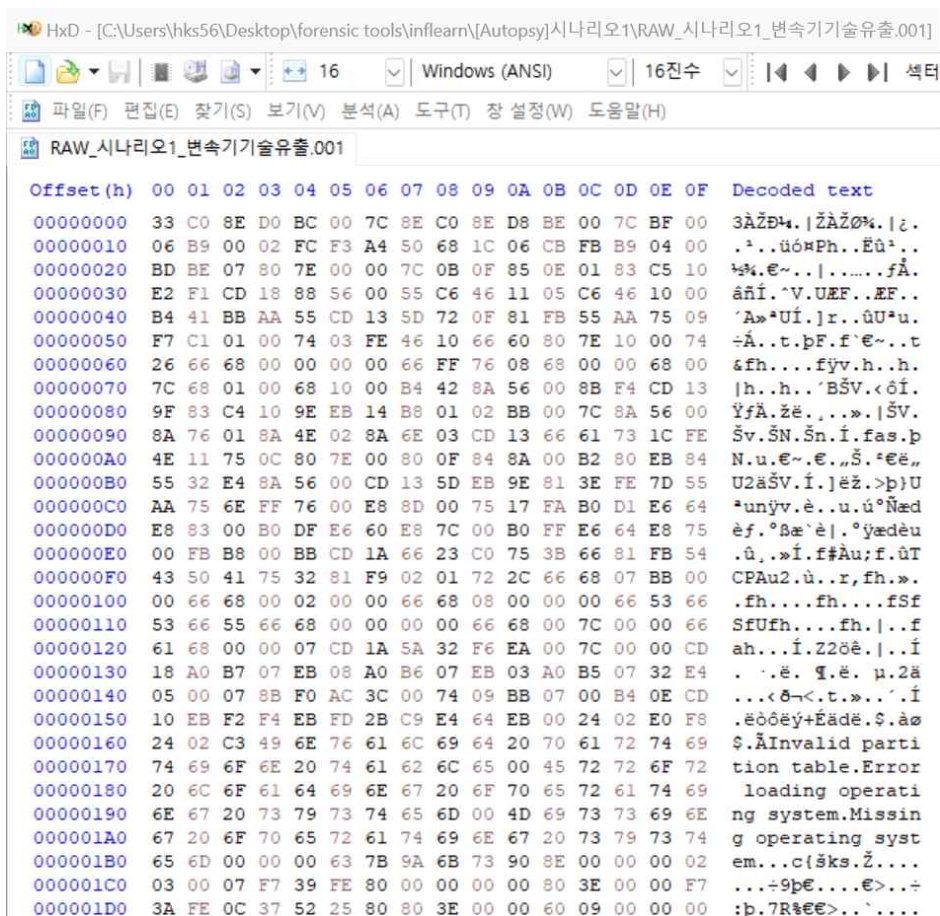
문제 4.

4. 수집한 증거 USB를 복구하고, 복구방법에 대해서 상세히 기술하시오.

1) 무결성을 유지하며 증거 USB를 FTK Imager를 이용하여 이미징 한 후, 해당 이미지 파일인 'C:\Users\hks56\Desktop\forensic tools\inflearn\[Autopsy]시나리오1\019-1-2-345.E01'을 FTK Imager에서 확인한 결과, 총 3개 파티션이 다음과 같이 확인되었음.



2) 위와 같이 3개의 파티션 중 2개의 파티션이 'Unrecognized File System'으로 내부 확인 불가, 1개의 파티션이 'Recovered'으로 내부구조 확인하여 MBR의 Partition Table이 훼손된 것으로 추정하여 해당 이미지 파일에 대한 RAW(dd)파일로 재이미징 실시하여 HxD로 불러옴.



- 0번 섹터가 mbr인지 pbr인지 확인하기 위해 마지막 내용을 다음과 같이 확인함.

000001B0	65 6D 00 00 00 63 7B 9A 6B 73 90 8E 00 00 00 02	em...c{šks.ž...
000001C0	03 00 07 F7 39 FE 80 00 00 00 00 80 3E 00 00 F7	...-9p€....€>...
000001D0	3A FE 0C 37 52 25 80 80 3E 00 00 60 09 00 00 00	:p.7Rš€€>... ..
000001E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AAU*

- 첫 번째 파티션 파일시스템 : NTFS / 시작섹터: 128 / 섹터 수: 4,096,000
- 두 번째 파티션 파일시스템 : FAT32 / 시작섹터: 4,096,128 / 섹터 수 : 614,400
- 3번째 파티션 정보는 FTK Imager에 'Recovered'라고 표시되어' 훼손된 것으로 추정

3) 훼손된 파티션 복구

가. 1번 파티션 복구

- 1번 파티션 복구를 위해 시작섹터 128로 이동 결과 모든 값이 00으로 표시/훼손됨이 확인되어 NTFS의 PBR 백업이 저장되어 있는 해당 파티션 마지막 섹터인 4,096,127로 이동하여 해당 섹터 내용 복사 후 훼손된 시작 섹터 128에 다음과 같이 붙여넣기함.

변속기기술유출.001

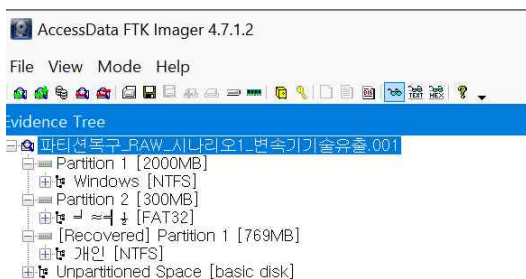
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
00010000	EB	52	90	4E	54	46	53	20	20	20	00	02	08	00	00	00	ëR.NTFS	섹터 128
00010010	00	00	00	00	00	F8	00	00	3F	00	FF	00	80	00	00	00ø..?.ÿ.€...	
00010020	00	00	00	00	80	00	80	00	FF	7F	3E	00	00	00	00	00€.€.ÿ.>.....	
00010030	AA	9A	02	00	00	00	00	00	02	00	00	00	00	00	00	00	*š.....>.....	
00010040	F6	00	00	00	01	00	00	00	62	17	11	B6	47	11	B6	68	ö.....b...qG.qh	
00010050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	...ú3ÀŽĐ*. ûhÀ.	
00010060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ë^...f.>..N	
00010070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.'A»*Uí.r..û	
00010080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	U*u.÷Á..u.éÿ...fi	
00010090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..'HŠ...<ö...í.	
000100A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ÿfÄ.žX.rá;...uŮ&	
000100B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z3Ů*. +È	
000100C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ.....ŽÄÿ...è	
000100D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K.+Ëwí...»í.f#Au-	
000100E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.ûTCPAu\$.ù..r..	
000100F0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66	h.»..hR..h...fSfSf	
00010100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF	U...h...fa...í.3Ä¿	
00010110	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E	..²ö.úó*ép...f`.	
00010120	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00	.f;...f.....fh...	
00010130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E	.fP.Sh..h..'BŠ..	
00010140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F	...<ôí.fÿ[Zfÿfÿ.	
00010150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	...fÿ.....ŽÄÿ	
00010160	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00	...u*.faÄ¿ö.è...	
00010170	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09	jú.è..ôëÿ<ö-<.t.	
00010180	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69	'.»...í.ëöÄ..A di	
00010190	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63	sk read error oc	
000101A0	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52	curréd...BOOTMGR	
000101B0	20	69	73	20	63	6F	6D	70	72	65	73	73	65	64	00	0D	is compressed..	
000101C0	0A	50	72	65	73	73	20	43	74	72	6C	2B	41	6C	74	2B	.Press Ctrl+Alt+	
000101D0	44	65	6C	20	74	6F	20	72	65	73	74	61	72	74	0D	0A	Del to restart..	
000101E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000101F0	00	00	00	00	00	00	8A	01	A7	01	BF	01	00	00	55	AAŠ\$.¿...U*	

나. 2번 파티션 복구

- 2번 파티션 복구를 위해 시작섹터 4,096,128로 이동 결과 모든 값이 00으로 표시/훼손됨이 확인되어 FAT32의 PBR 백업이 저장되어 있는 '시작섹터+6' 섹터로 이동하여 해당 섹터 내용 복사 후 훼손된 시작 섹터 4,096,128에 다음과 같이 붙여넣기함.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
7D010000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	5E	1B	EX.MSDOS5.0...^.	섹터 4,096,128
7D010010	02	00	00	00	00	F8	00	00	3F	00	FF	00	80	80	3E	00ø...?.ý.€€>.	
7D010020	00	60	09	00	51	02	00	00	00	00	00	00	02	00	00	00	...'Q.....	
7D010030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	
7D010040	00	00	29	E9	A3	1C	C6	4E	4F	20	4E	41	4D	45	20	20	€..)é£.ÆNO NAME	
7D010050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4	FAT32 3ÉŽÑ*ó	
7D010060	7B	8E	C1	8E	D9	BD	00	7C	88	56	40	88	4E	02	8A	56	{ŽĂŽŮ% . ^V@^N.ŠV	
7D010070	40	B4	41	BB	AA	55	CD	13	72	10	81	FB	55	AA	75	0A	@'A»^UÍ.r..ôU^u.	
7D010080	F6	C1	01	74	05	FE	46	02	EB	2D	8A	56	40	B4	08	CD	óÁ.t.þF.ë-ŠV@'.í	
7D010090	13	73	05	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F	B6	.s.^ÿŸŠñf.ŸÆ@f.Ÿ	
7D0100A0	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7	C9	Ñeá?÷á+íÁi.Af.·É	
7D0100B0	66	F7	E1	66	89	46	F8	83	7E	16	00	75	39	83	7E	2A	f÷áfñFøf~...u9f~*	
7D0100C0	00	77	33	66	8B	46	1C	66	83	C0	0C	BB	00	80	B9	01	.w3f<F.ffÄ.»..€^.	
7D0100D0	00	E8	2C	00	E9	A8	03	A1	F8	7D	80	C4	7C	8B	F0	AC	.è,.é".;ø)€Ä <ð~	
7D0100E0	84	C0	74	17	3C	FF	74	09	B4	0E	BB	07	00	CD	10	EB	„Ät.<ÿt.'.»..í.ë	
7D0100F0	EE	A1	FA	7D	EB	E4	A1	7D	80	EB	DF	98	CD	16	CD	19	î;ú)ëä;)}ëë\$^í.í.	
7D010100	66	60	80	7E	02	00	0F	84	20	00	66	6A	00	66	50	06	f`€~....„ .fj.fP.	
7D010110	53	66	68	10	00	01	00	B4	42	8A	56	40	8B	F4	CD	13	Sfh....'BŠV@<óí.	
7D010120	66	58	66	58	66	58	66	58	EB	33	66	3B	46	F8	72	03	fXfXfXfXfXfXf;Før.	
7D010130	F9	EB	2A	66	33	D2	66	0F	B7	4E	18	66	F7	F1	FE	C2	ùè*f3òf.·N.f÷ñþÄ	
7D010140	8A	CA	66	8B	D0	66	C1	EA	10	F7	76	1A	86	D6	8A	56	ŠËf<ðfÄè.÷v.+òŠV	
7D010150	40	8A	E8	C0	E4	06	0A	CC	B8	01	02	CD	13	66	61	0F	@ŠèÄä...ì,...í.fa.	
7D010160	82	74	FF	81	C3	00	02	66	40	49	75	94	C3	42	4F	4F	,ty.Ä..f@Iu"ÄBOO	
7D010170	54	4D	47	52	20	20	20	20	00	00	00	00	00	00	00	00	TMGR	
7D010180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
7D010190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
7D0101A0	00	00	00	00	00	00	00	00	00	00	00	00	00	0D	0A	44Di	
7D0101B0	73	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	sk errorý..Press	
7D0101C0	20	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	any key to rest	
7D0101D0	61	72	74	0D	0A	00	00	00	00	00	00	00	00	00	00	00	art.....	
7D0101E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
7D0101F0	00	00	00	00	00	00	00	00	AC	01	B9	01	00	00	55	AA¿.^...U^	

다. 파티션 복구 확인







- 첫 번째와 두 번째 파티션을 복구하여 FTK Imager로 해당 RAW파일을 열어본 결과, MBR의 Partition Table이 훼손된 세 번째 파티션을 제외한 두 파티션이 정상적 접근 확인함.
- 이후, Autopsy에서 분석을 시도한 결과 Partition Table이 훼손된 세 번째 파티션은 볼륨에 접근이 가능함을 확인하여 이후 분석 진행함.

Listing

File Search Results 4 x

/img_파티션복구_RAW_시나리오1_변속기기술유출.001

Table Thumbnail Summary

Name	ID	Starting Sector	Length in Sectors	Description	Flags
 vol1 (Unallocated: 0-127)	1	0	128	Unallocated	Unallocated
 vol2 (NTFS / exFAT (0x07): 128-4096127)	2	128	4096000	NTFS / exFAT (0x07)	Allocated
 vol3 (Win95 FAT32 (0x0c): 4096128-4710527)	3	4096128	614400	Win95 FAT32 (0x0c)	Allocated
 vol4 (Unallocated: 4710528-6291455)	4	4710528	1580928	Unallocated	Unallocated