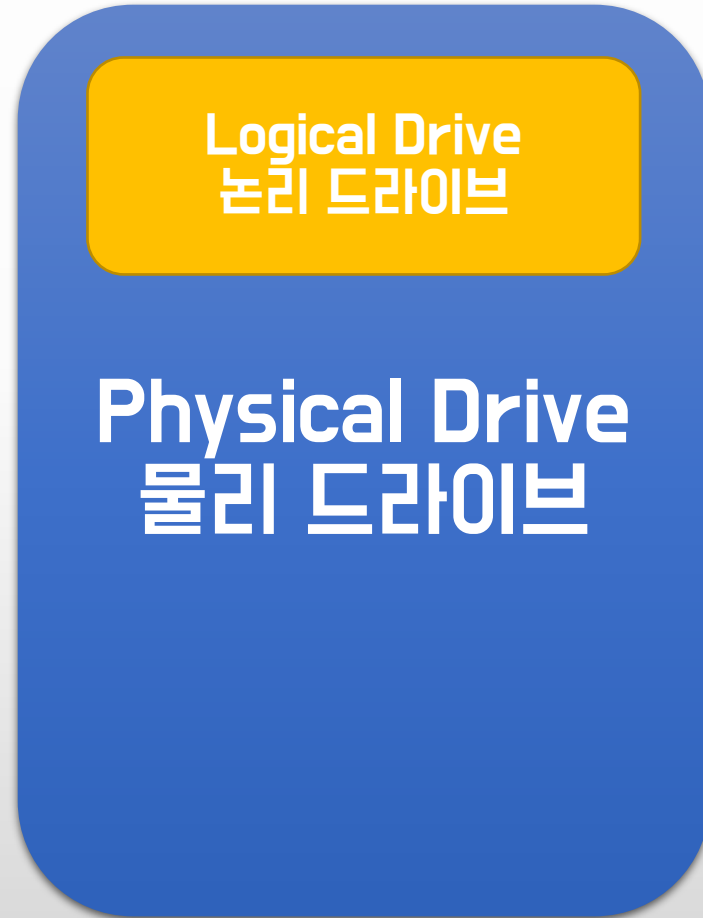


File Signature

charsyam@naver.com

Physical Drive, Logical Drive

여러분들 PC에
달려있는 SSD, HDD 가
Physical Drive

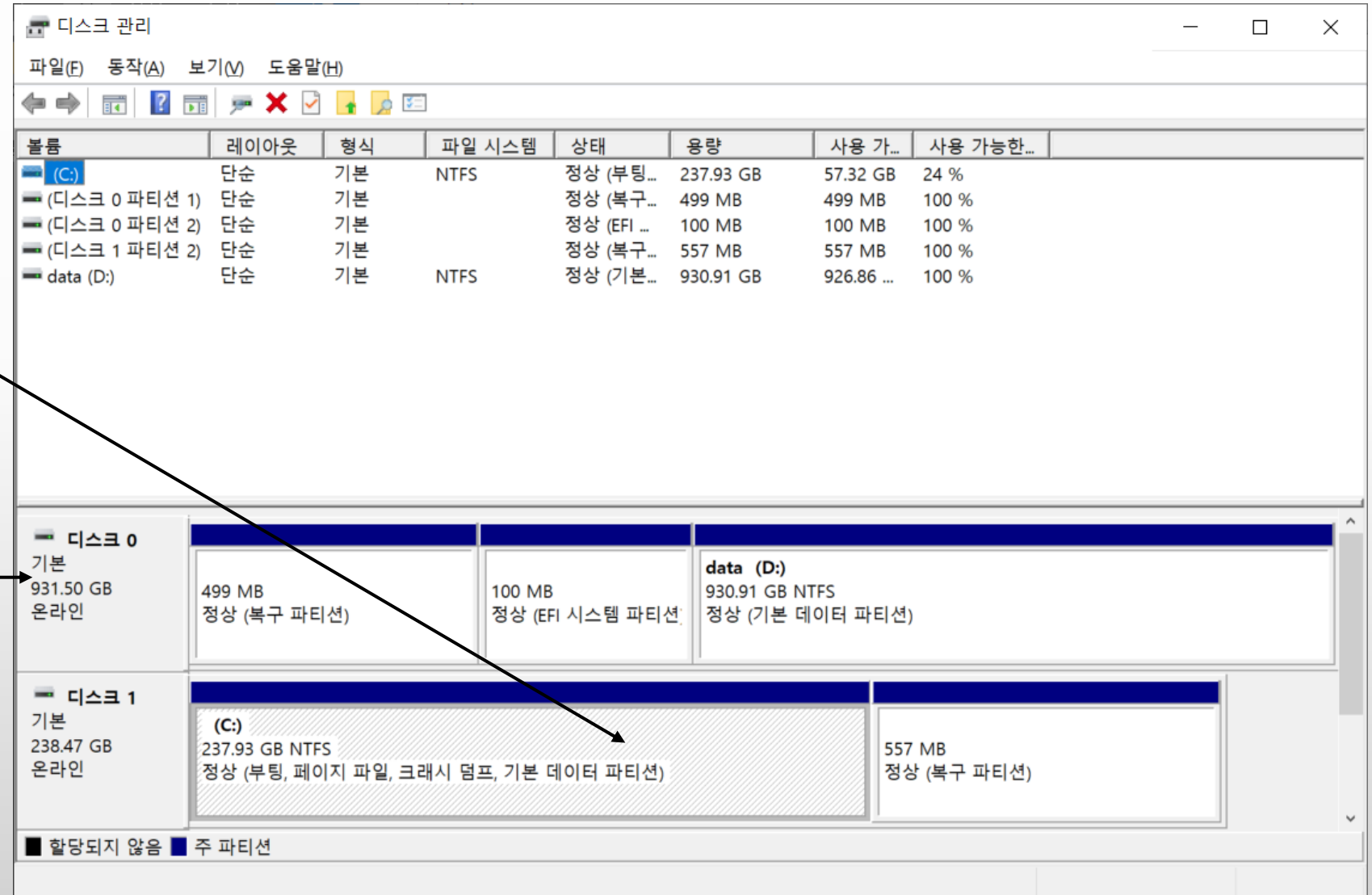


파티션을 나누게 되면 그 파티션이
하나의 논리 드라이브가 되게 된다.

Physical Drive, Logical Drive

파티션은
논리 드라이브

디스크는
물리 드라이브



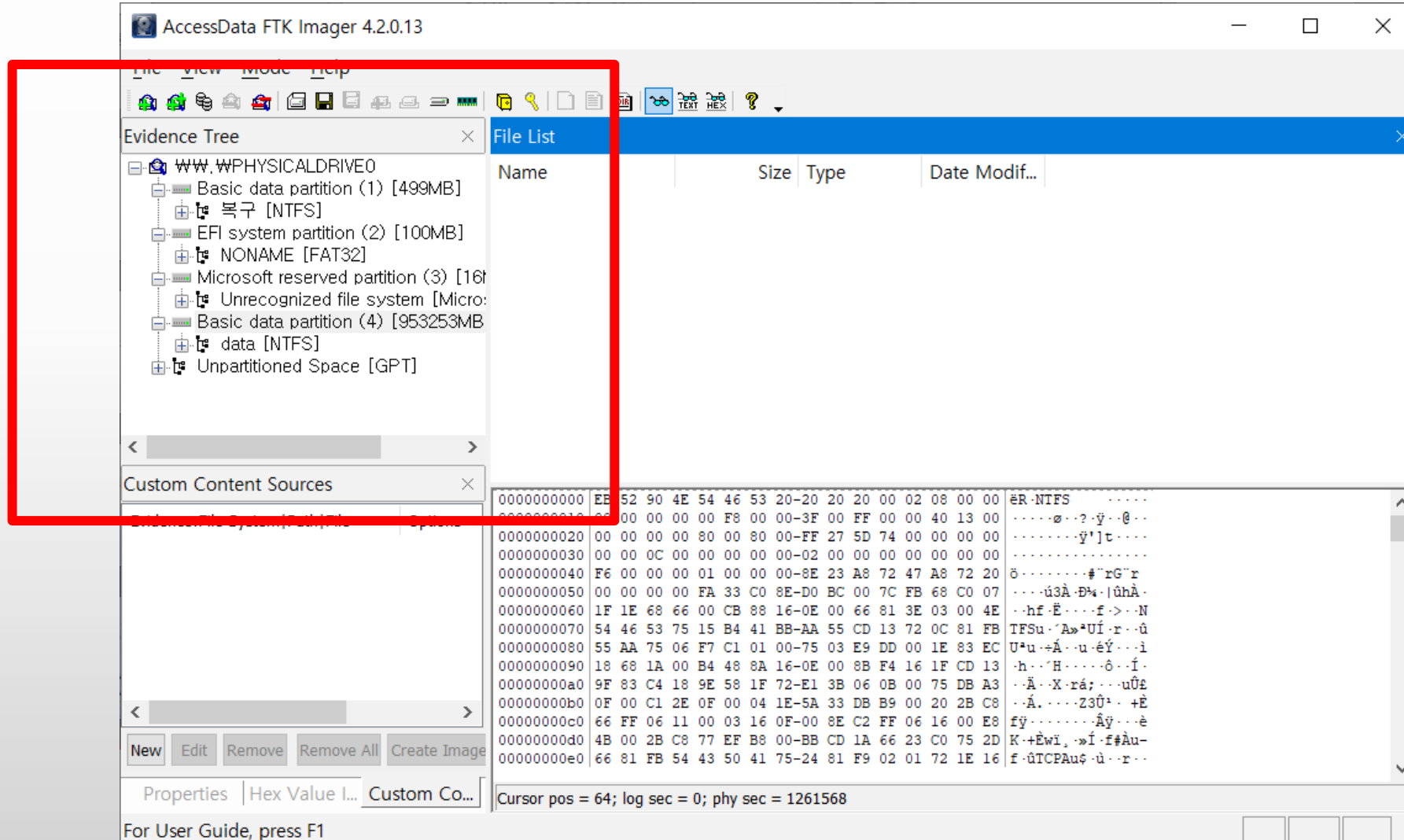
The screenshot shows the Windows Disk Management console. At the top, a table lists the volumes and their properties. Below this, the physical disks are shown with their partitions. An arrow points from the text '파티션은 논리 드라이브' to the (C:) partition on Disk 1. Another arrow points from the text '디스크는 물리 드라이브' to the Disk 0 entry in the lower section.

볼륨	레이아웃	형식	파일 시스템	상태	용량	사용 가...	사용 가능한...
(C:)	단순	기본	NTFS	정상 (부팅...	237.93 GB	57.32 GB	24 %
(디스크 0 파티션 1)	단순	기본		정상 (복구...	499 MB	499 MB	100 %
(디스크 0 파티션 2)	단순	기본		정상 (EFI ...	100 MB	100 MB	100 %
(디스크 1 파티션 2)	단순	기본		정상 (복구...	557 MB	557 MB	100 %
data (D:)	단순	기본	NTFS	정상 (기본...	930.91 GB	926.86 ...	100 %

디스크	형식	용량	온라인	파티션
디스크 0	기본	931.50 GB	온라인	<div><div>499 MB 정상 (복구 파티션)</div><div>100 MB 정상 (EFI 시스템 파티션)</div><div>data (D:) 930.91 GB NTFS 정상 (기본 데이터 파티션)</div></div>
디스크 1	기본	238.47 GB	온라인	<div><div>(C:) 237.93 GB NTFS 정상 (부팅, 페이지 파일, 크래시 덤프, 기본 데이터 파티션)</div><div>557 MB 정상 (복구 파티션)</div></div>

■ 할당되지 않음 ■ 주 파티션

Physical Drive, Logical Drive



File System

- 하나의 파티션에서 파일(데이터)를 어떻게 관리할 것인가에 대한 것이 File System
 - FAT32, NTFS, EXT4, AUFS, HFS+, XFS, ZFS 등 굉장히 여러가지 파일 시스템이 존재한다.
 - 파일을 효율적으로 저장하고 찾기 위한 방법
- 파일시스템 마다 정보를 저장하고 찾기 위한 고유한 방법이 존재한다.
 - 파일 시스템을 분석하면, 파일의 생성/접근/수정 시간등을 알아낼 수 있다.

File Signature 란?

- 우리는 굉장히 많은 파일 포맷을 사용하고 있다.
 - DOCX, HWP, ZIP, PPTX, JPG, PNG, ...
- 이런 파일들을 구분하기 위해서 고유의 값을 저장하고 있는 방법
- 보통의 경우 파일의 가장 앞쪽에 파일 시그니처가 존재하는 경우가 많다.

File Signature 예

PDF

• %PDF- 형태로 시작

00000	25	50	44	46	2D	31	2E	37-0D	0A	25	B5	B5	B5	B5	0D	%PDF-1.7 ··%µµµµ ·
00010	0A	31	20	30	20	6F	62	6A-0D	0A	3C	3C	2F	54	79	70	·1 0 obj ··<</Typ
00020	65	2F	43	61	74	61	6C	6F-67	2F	50	61	67	65	73	20	e/Catalog/Pages
00030	32	20	30	20	52	2F	4C	61-6E	67	28	6B	6F	2D	4B	52	2 0 R/Lang(ko-KR
00040	29	20	2F	53	74	72	75	63-74	54	72	65	65	52	6F	6F) /StructTreeRoo
00050	74	20	36	35	30	20	30	20-52	2F	4D	61	72	6B	49	6E	t 650 0 R/MarkIn
00060	66	6F	3C	3C	2F	4D	61	72-6B	65	64	20	74	72	75	65	fo<</Marked true
00070	3E	3E	2F	4D	65	74	61	64-61	74	61	20	31	35	31	35	>>/Metadata 1515
00080	20	30	20	52	2F	56	69	65-77	65	72	50	72	65	66	65	0 R/ViewerPrefe
00090	72	65	6E	63	65	73	20	31-35	31	36	20	30	20	52	3E	rences 1516 0 R>
000a0	3E	0D	0A	65	6E	64	6F	62-6A	0D	0A	32	20	30	20	6F	>··endobj ··2 0 o
000b0	62	6A	0D	0A	3C	3C	2F	54-79	70	65	2F	50	61	67	65	bj ··<</Type/Page
000c0	73	2F	43	6F	75	6E	74	20-37	37	2F	4B	69	64	73	5B	s/Count 77/Kids[

EXE, DLL

- MZ 로 시작 - 이것은 예전 DOS 헤더이고 실제 PE 형식으로 내부
를 좀더 확인해야 한다.

0000	4D	5A	90	00	03	00	00	00-04	00	00	00	FF	FF	00	00	MZ	ÿÿ
0010	B8	00	00	00	00	00	00	00-40	00	00	00	00	00	00	00	,	@
0020	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00
0030	00	00	00	00	00	00	00	00-00	00	00	00	80	00	00	00
0040	0E	1F	BA	0E	00	B4	09	CD-21	B8	01	4C	CD	21	54	68	. . ° . . ' . í! , . Lí!Th
0050	69	73	20	70	72	6F	67	72-61	6D	20	63	61	6E	6E	6F	is program canno
0060	74	20	62	65	20	72	75	6E-20	69	6E	20	44	4F	53	20	t be run in DOS
0070	6D	6F	64	65	2E	0D	0D	0A-24	00	00	00	00	00	00	00	mode . . . \$
0080	50	45	00	00	4C	01	03	00-52	87	AB	D6	00	00	00	00	PE . . I . . . R «Ö
0090	00	00	00	00	E0	00	22	00-0B	01	30	00	00	08	00	00 a . " . . . 0
00a0	00	08	00	00	00	00	00	00-6A	26	00	00	00	20	00	00 j&
00b0	00	40	00	00	00	00	40	00-00	20	00	00	00	02	00	00	. @ @
00c0	04	00	00	00	00	00	00	00-04	00	00	00	00	00	00	00

Registry File

- regf로 시작

00000	72	65	67	66	AD	02	00	00-AC	02	00	00	00	00	00	00 regf -
00010	00	00	00	00	01	00	00	00-05	00	00	00	00	00	00
00020	01	00	00	00	20	00	00	00-00	30	0A	00	01	00	00 0
00030	74	00	65	00	6D	00	52	00-6F	00	6F	00	74	00	5C	00 t·e·m·R·o·o·t·\·
00040	53	00	79	00	73	00	74	00-65	00	6D	00	33	00	32	00 S·y·s·t·e·m·3·2·
00050	5C	00	43	00	6F	00	6E	00-66	00	69	00	67	00	5C	00 \·C·o·n·f·i·g·\·
00060	44	00	45	00	46	00	41	00-55	00	4C	00	54	00	00	00 D·E·F·A·U·L·T·...·
00070	41	EB	C6	AB	14	6C	EA	11-A8	10	00	0D	3A	92	93	29 AëÆ«·lê·~·...·:·..)
00080	41	EB	C6	AB	14	6C	EA	11-A8	10	00	0D	3A	92	93	29 AëÆ«·lê·~·...·:·..)
00090	00	00	00	00	42	EB	C6	AB-14	6C	EA	11	A8	10	00	0D ...·BëÆ«·lê·~·...·
000a0	3A	92	93	29	72	6D	74	6D-EA	08	EB	AF	28	00	D6	01 :·..) rmtmê·ë¯(·Ö·
000b0	4F	66	52	67	01	00	00	00-00	00	00	00	00	00	00	00 OfRg·...·

File Signature 분석 로직

- 시작 512 byte 정도를 읽어와서 시그니처를 비교한다.
- 일치하는 시그니처가 있다면, 좀 더 자세히 분석한다.
 - 이유는?

