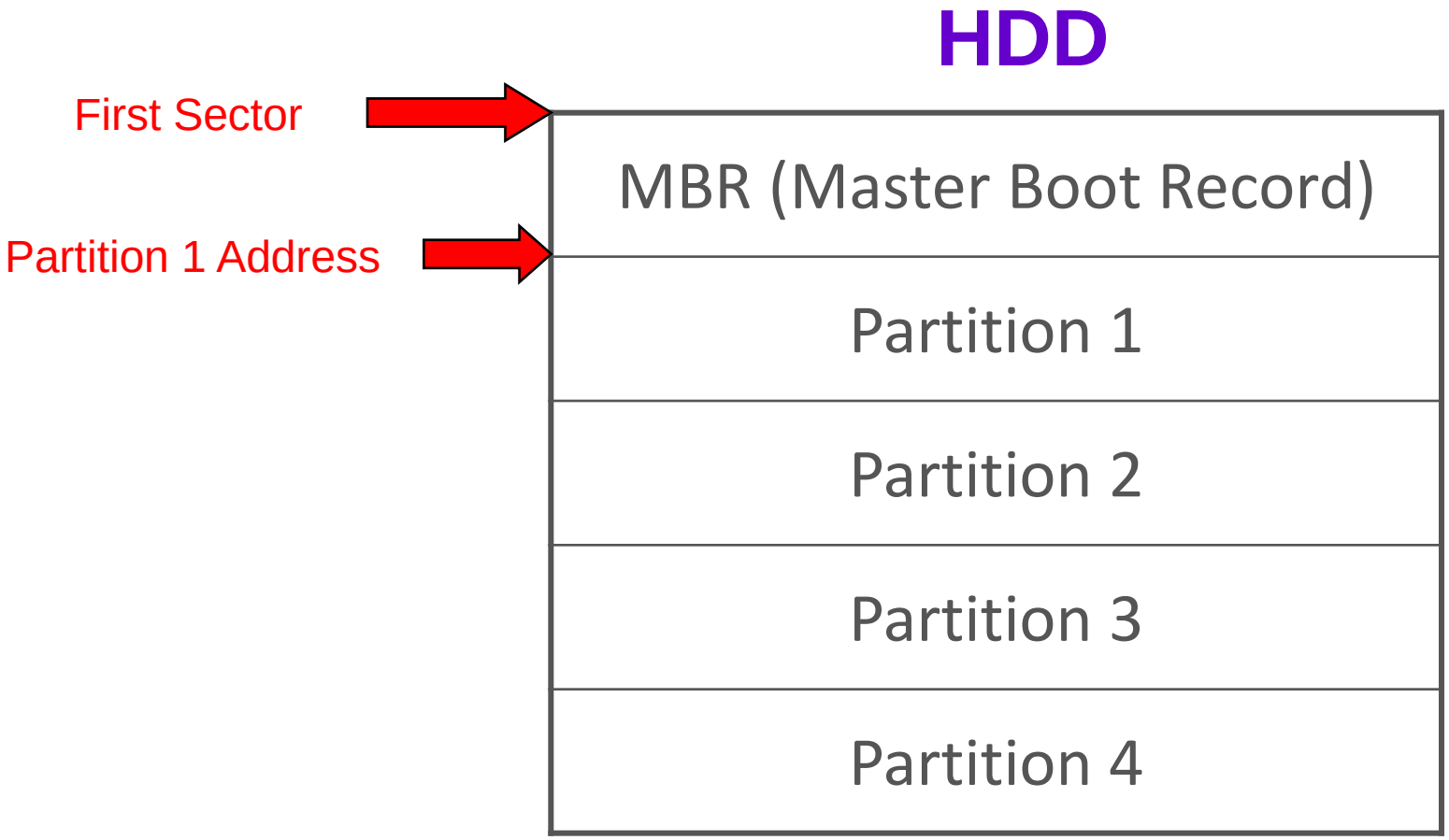
Compal NTFS Recovery User Guide

Glen Chen | AIO/SW2 | Design Manager

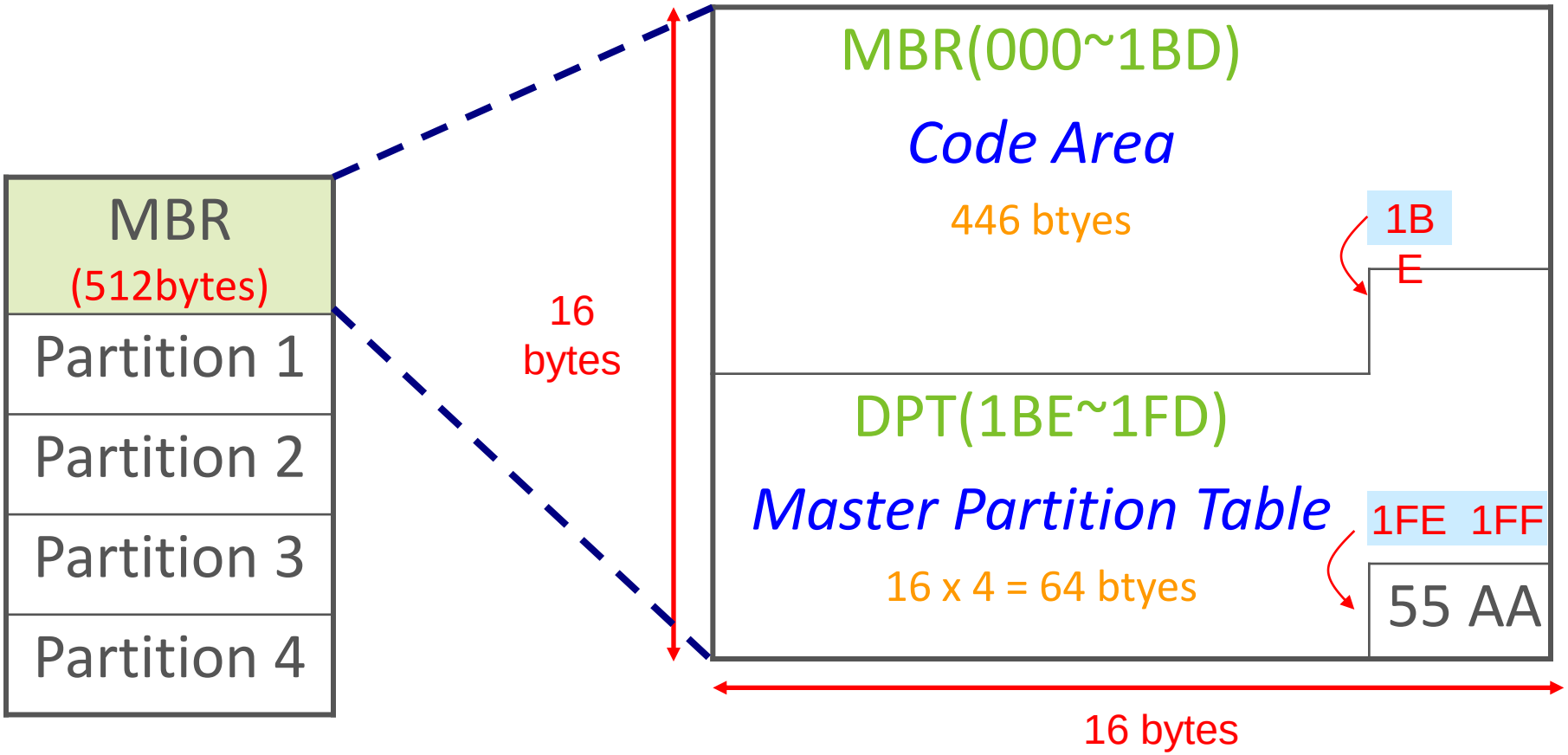
Kioster Cheng | AIO/SW2 | Design Leader

Version

September 1, 2010


HDD
First Sector
Partition 1 Address
MBR (Master Boot Record)
Partition 1
Partition 2
Partition 3
Partition 4

MBR



Partition 1	1BE~1CD
Partition 2	1CE~1DD
Partition 3	1DE~1ED
Partition 4	1EE~1FD
Signature	1FE~1FF

Partition Table

MBR sector's Partition Table

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII characters
1B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	80	01	. . . . .
1C0	01	00	07	9F	FF	57	3F	00	00	00	81	CE	A7	00	00	00	. . . . ? 3 ? . . . A . . .
1D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	. . . . .
1E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	. . . . .
1F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	. . . . . U .

Partition Table

- A Partition Table Entry

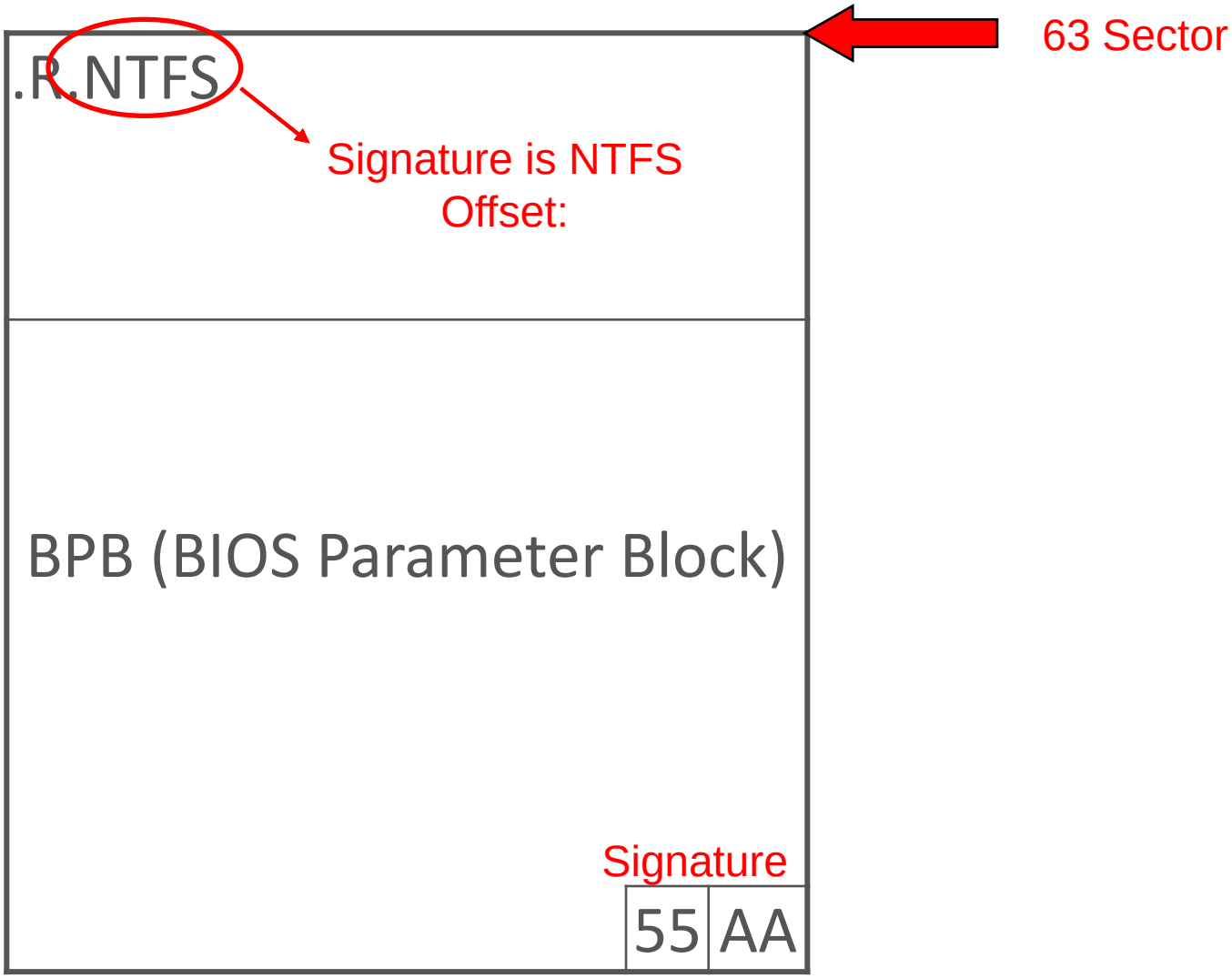
Structure of a *16-byte* Partition Table Entry		
Relative Offsets (*within entry*)	**Length (*bytes*)**	**Contents**
0	1	**Boot Indicator (80h = *active*)**
1~3	3	**Starting CHS values**
4	1	***Partition-type* Descriptor**
5~7	3	**Ending CHS values**
8~11	4	**Starting Sector LBA (Absolute Sector) value**
12~15	4	**Partition Size (in sectors)**

Partition Table

80 01 01 00 07 9F FF 57 3F 00 00 00 81 CE A7 00

The First 16-byte Entry in our Partition Table			
Relative Offsets	**Value in this Example**	**Description**	**Meaning**
1	80	Bootable? (80h = Yes; 00 = No)	YES
1~3	01 01 00	Starting Sector [First byte *always* = Head value]	00 01 01
4	07	Partition Type	NTFS
5~7	9F,FF,57	Last Sector	855 159 63
8~11	3F 00 00 00	Relative Sectors (or Offset) (0000003Fh = 63)	63
12~15	81 CE A7 00	Total Sectors (or Length) (00A7CE81h = 10,997,377 sectors = 5.2GB)	10,997,377

Partition Table



Partition Boot Sector

Byte Offset	Field Length	Field Name
0x00	3 bytes	Jump Instruction
0x03	LONGLONG	OEM ID
0x0B	25 bytes	BPB
0x24	48 bytes	Extended BPB
0x54	426 bytes	Bootstrap Code
0x01FE	WORD	End of Sector Marker

BPB Entry Item

Byte Offset	Field Length	Sample Value	Field Name
0x0B	WORD	0x0002	Bytes Per Sector
0x0D	BYTE	0x08	Sectors Per Cluster
0x0E	WORD	0x0000	Reserved Sectors
0x10	3 BYTES	0x000000	*always 0*
0x13	WORD	0x0000	*not used by NTFS*
0x15	BYTE	0xF8	Media Descriptor
0x16	WORD	0x0000	*always 0*
0x18	WORD	0x3F00	Sectors Per Track
0x1A	WORD	0xFF00	Number Of Heads
0x1C	DWORD	0x3F000000	Hidden Sectors

BPB Entry Item (Cont.)

Byte Offset	Field Length	Sample Value	Field Name
0x20	DWORD	0x00000000	*not used by NTFS*
0x24	DWORD	0x80008000	*not used by NTFS*
0x28	LONGLONG	0x4AF57F0000000000	Total Sectors
0x30	LONGLONG	0x0400000000000000	Logical Cluster Number for the file $MFT
0x38	LONGLONG	0x54FF070000000000	Logical Cluster Number for the file $MFTMirr
0x40	DWORD	0xF6000000	Clusters Per File Record Segment
0x44	DWORD	0x01000000	Clusters Per Index Block
0x48	LONGLONG	0x14A51B74C91B741C	Volume Serial Number
0x50	DWORD	0x00000000	Checksum

$MFT Table

Type	Name
0	$MFT
1	$MFT Mirror
2	$LogFile
3	$Volume
4	$AttrDef
5	$Root
6	$Bitmap
7	$Boot
8	$BadClus

Type	Name
9	$Secure
10	$UpCase
11	$Extend metadata directory
12	$Extend \ $Reparse
13	$Extend \ $UsnJrnl
14	$Extend \ $Quota
15	$Extend \ $ObjId
16~23	$
23~	$

$MFT Table

$MFT Table

Type	Name
0	$MFT
1	$MFT Mirror
2	$LogFile
3	$Volume
4	$AttrDef
5	$Root
6	$Bitmap
7	$Boot
8	$BadClus

$MFT NO.0 Address (sector) :
C0000h x 8 + Partition1 offset

2 Sectors

How to calculate the address of MFT table ?
The offset of $MFT x sector/cluster +
Partition1 offset +
MFT NO. x 2 (unit: sector)

$MFT NO.5 Address (sector) :
C0000h x 8 + 5 x 2 +
Partition1 offset

Standard NTFS Attributes (Cont.)

- **Table. Standard NTFS Attributes**

Type	Name
0x10	$STANDARD_INFORMATION
0x20	$ATTRIBUTE_LIST
0x30	$FILE_NAME
0x40	$VOLUME_VERSION / $OBJECT_ID
0x50	$SECURITY_DESCRIPTOR
0x60	$VOLUME_NAME
0x70	$VOLUME_INFORMATION
0x80	$DATA

Standard NTFS Attributes

- **Table. Standard NTFS Attributes**

Type	Name
0x90	$INDEX_ROOT
0xA0	$INDEX_ALLOCATION
0xB0	$BITMAP
0xC0	$SYMBOLIC_LINK / $REPARSE_POINT
0xD0	$EA_INFORMATION
0xE0	$EA
0xF0	$PROPERTY_SET
0x100	$LOGGED_UTILITY_STREAM

$ROOT Attributes

Type	Description	Name
0x10	$STANDARD_INFORMATION	
0x30	$FILE_NAME	. (Root Directory)
0x50	$SECURITY_DESCRIPTOR	
0x80	$DATA	$MountMgrDatabase
0x90	$INDEX_ROOT	$I30
0xA0	$INDEX_ALLOCATION	$I30
0xB0	$BITMAP	$I30

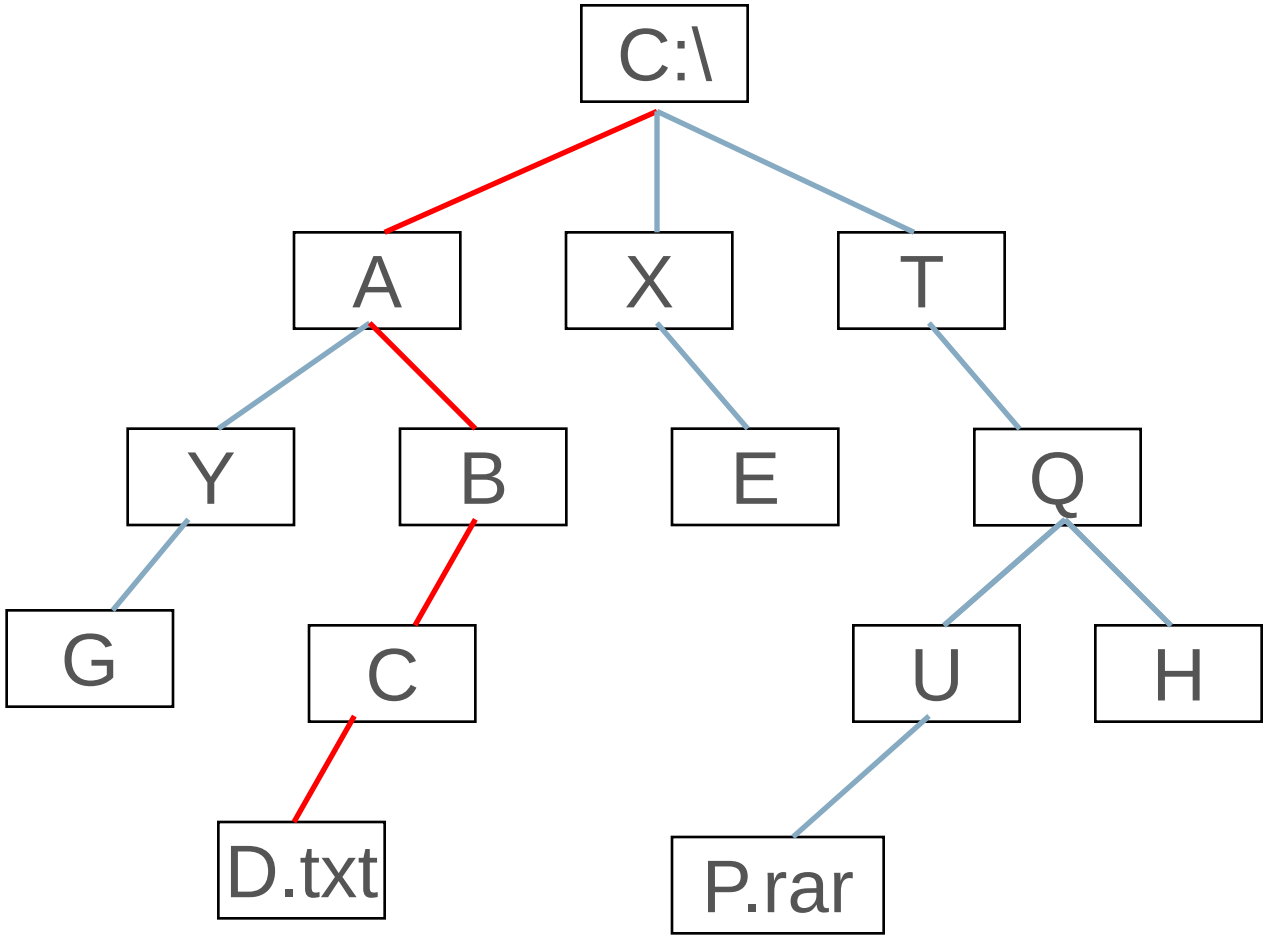
COMPAL

Index Table Header

Offset	Size	Description
0x00	4	Magic number 'INDX'
0x04	2	Offset to the Update Sequence.
0x06	2	Size in words of the Update Sequence Number &Array (S)
0x08	8	$LogFile sequence number
0x10	8	VCN of this INDX buffer in the Index Allocation
0x18	4	Offset to the Index Entries (a)
0x1C	4	Size of Index Entries (a)
0x20	4	Allocated size of the Index Entries (a)
0x24	1	if not leaf node (b)
0x25	3	Padding (always zero)
0x28	2	Update sequence
0x2A	2S-2	Update sequence array

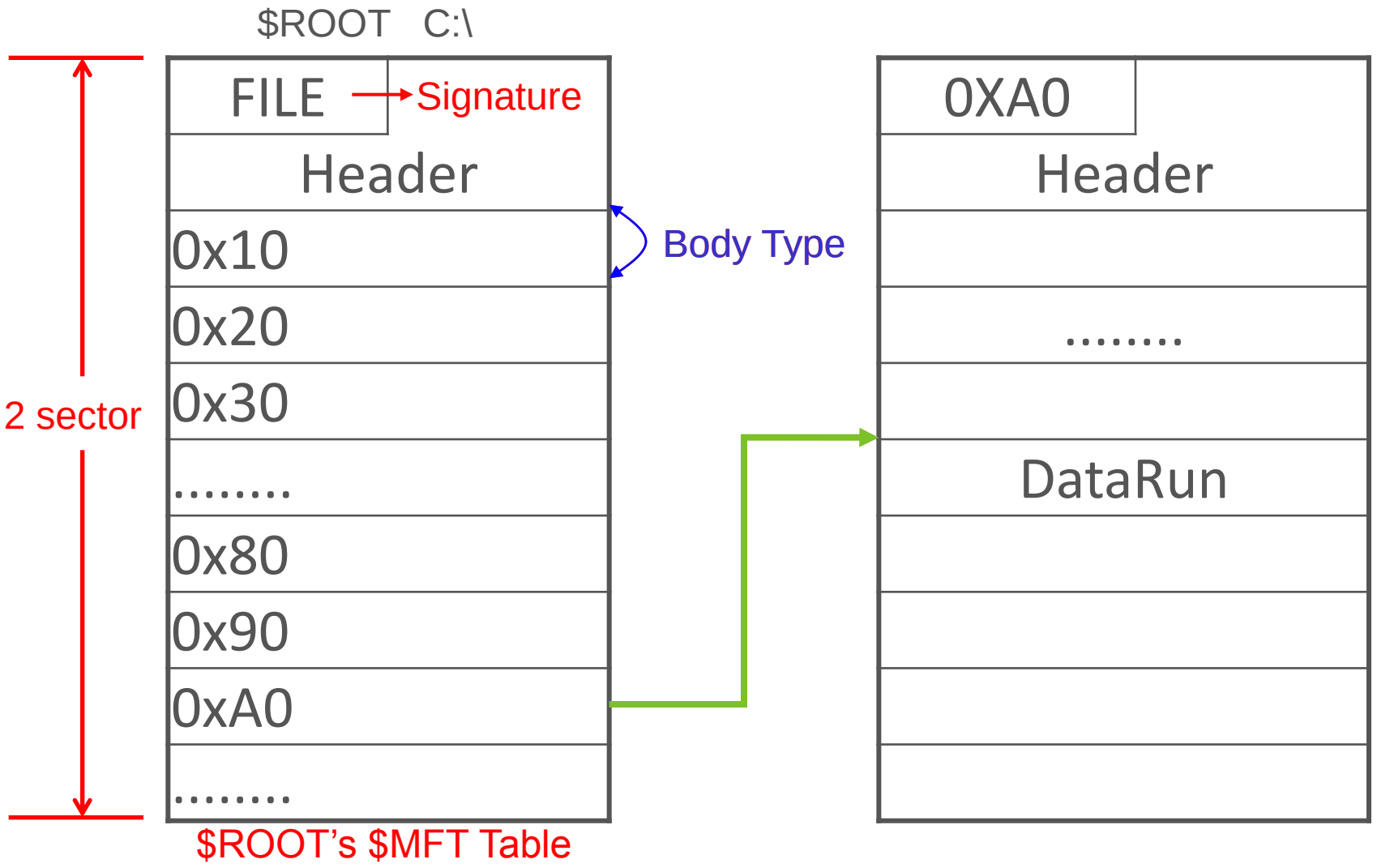
B+ Tree

C:\A\B\C\D.txt



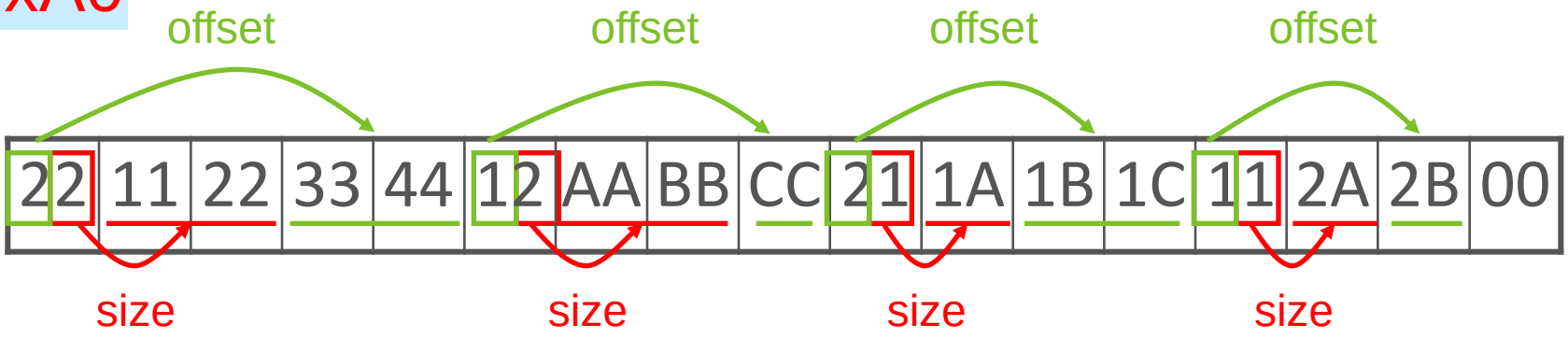
Search Film

- C:\A\B\C\D.txt



Datarun

0xA0

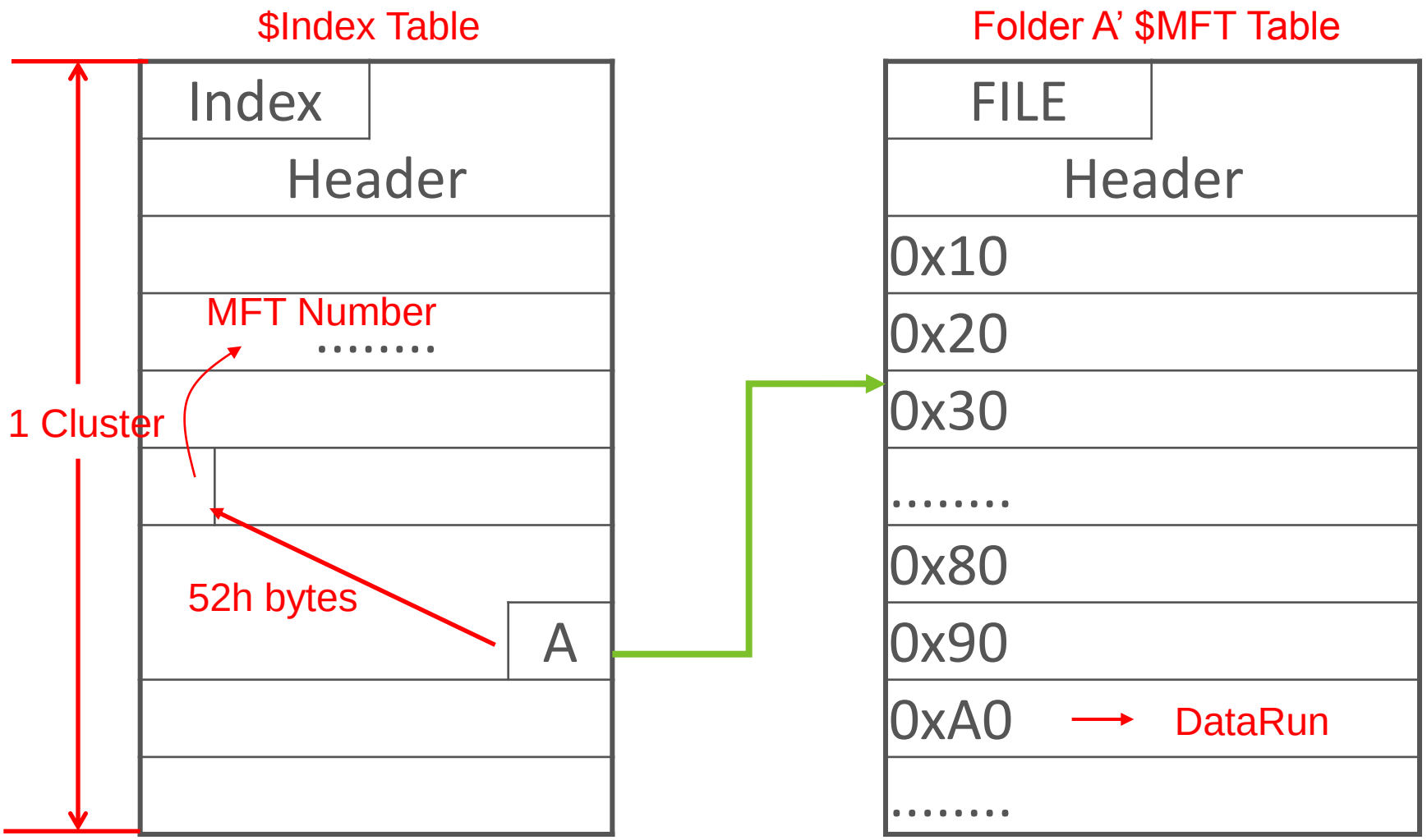


Size:	2211	BBAA	1A	2A	END
Offset:	4433	CC	1C1B	2B	

(4433+CC=44FF) (44FF+1C1B=611A) (611A+2B=6145)

0x2211 Clusters , @ LCN 4433h
0xBBAA Clusters , @ VCN CCh @LCN 44FFh
0x1A Clusters , @ VCN 1C1Bh @LCN 611Ah
0x2A Clusters , @ VCN 2Bh @LCN 6145h

C:\A\B\C\D.txt



$MFT LCN= $MFT table address+ Partition1 offset + MFT Number x 2 (sector)

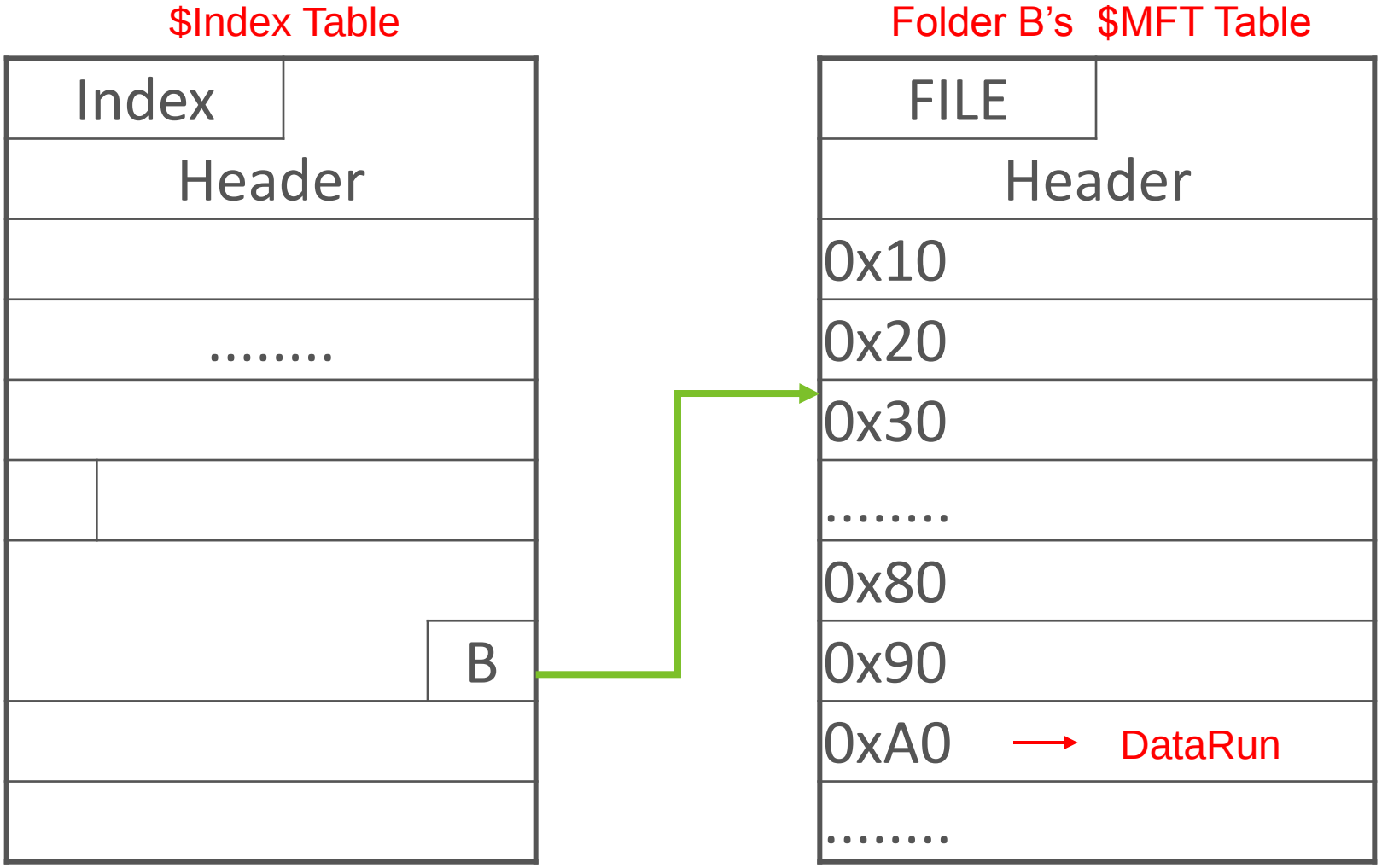
COMPAL

Index Entry Item

Offset	Size	Description
~	~	Standard Index Header
0x00	8	MFT Reference of the file
0x08	2	Size of this index entry
0x0A	2	Offset to the filename
0x0C	2	Index Flags
0x0E	2	Padding (align to 8 bytes)
0x10	8	MFT File Reference of the parent
0x18	8	File creation time
0x20	8	Last modification time
0x28	8	Last modification time for FILE record
0x30	8	Last access time
0x38	8	Allocated size of file
0x40	8	Real size of file
0x48	8	File Flags
0x50	1	Length of filename (F)
0x51	1	Filename namespace
0x52	2F	Filename
2F+0x52	P	Padding (align to 8 bytes)
P+2F+0x52	8	VCN of index buffer with sub-nodes

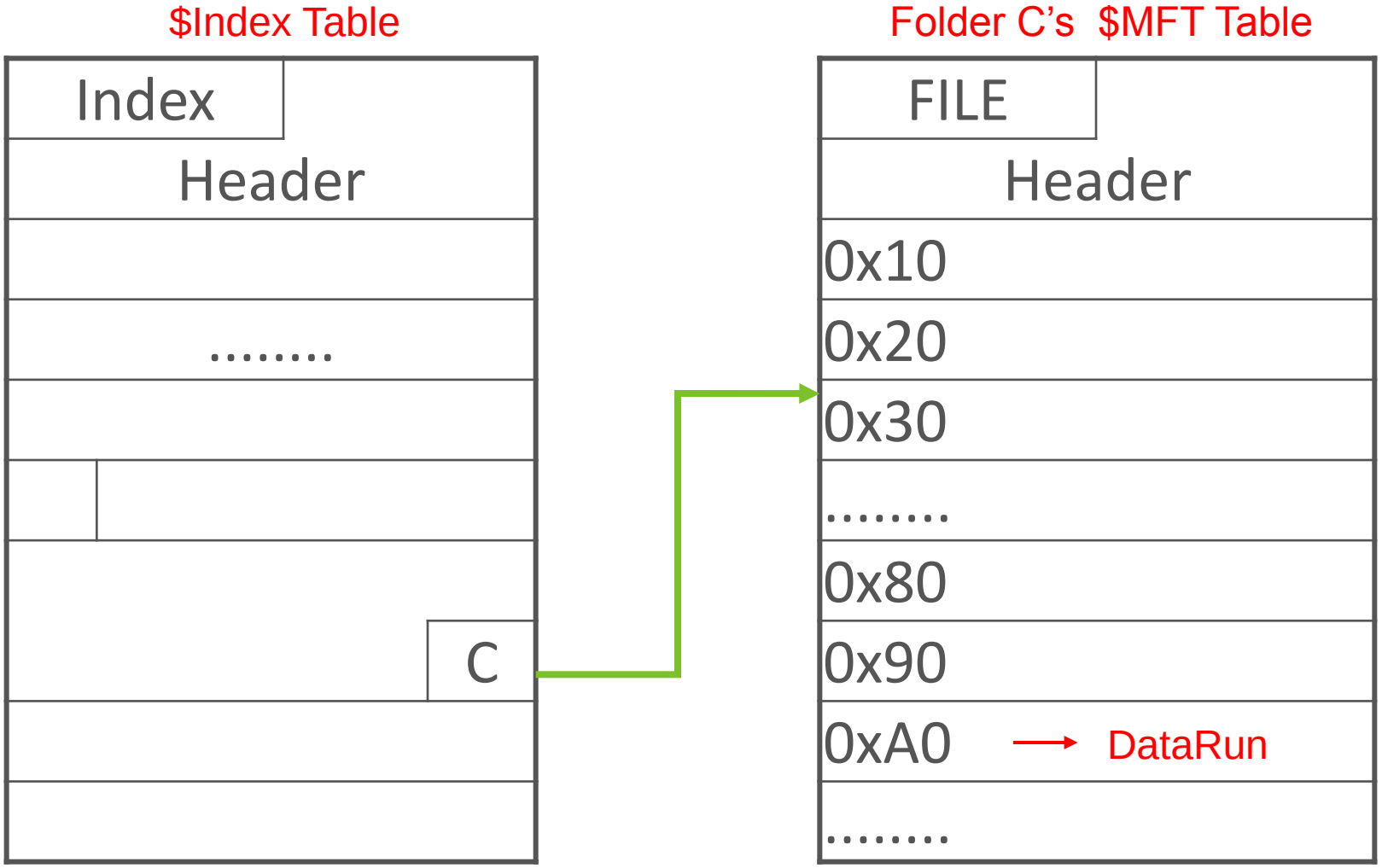
Search Film

C:\A\B\C\D.txt



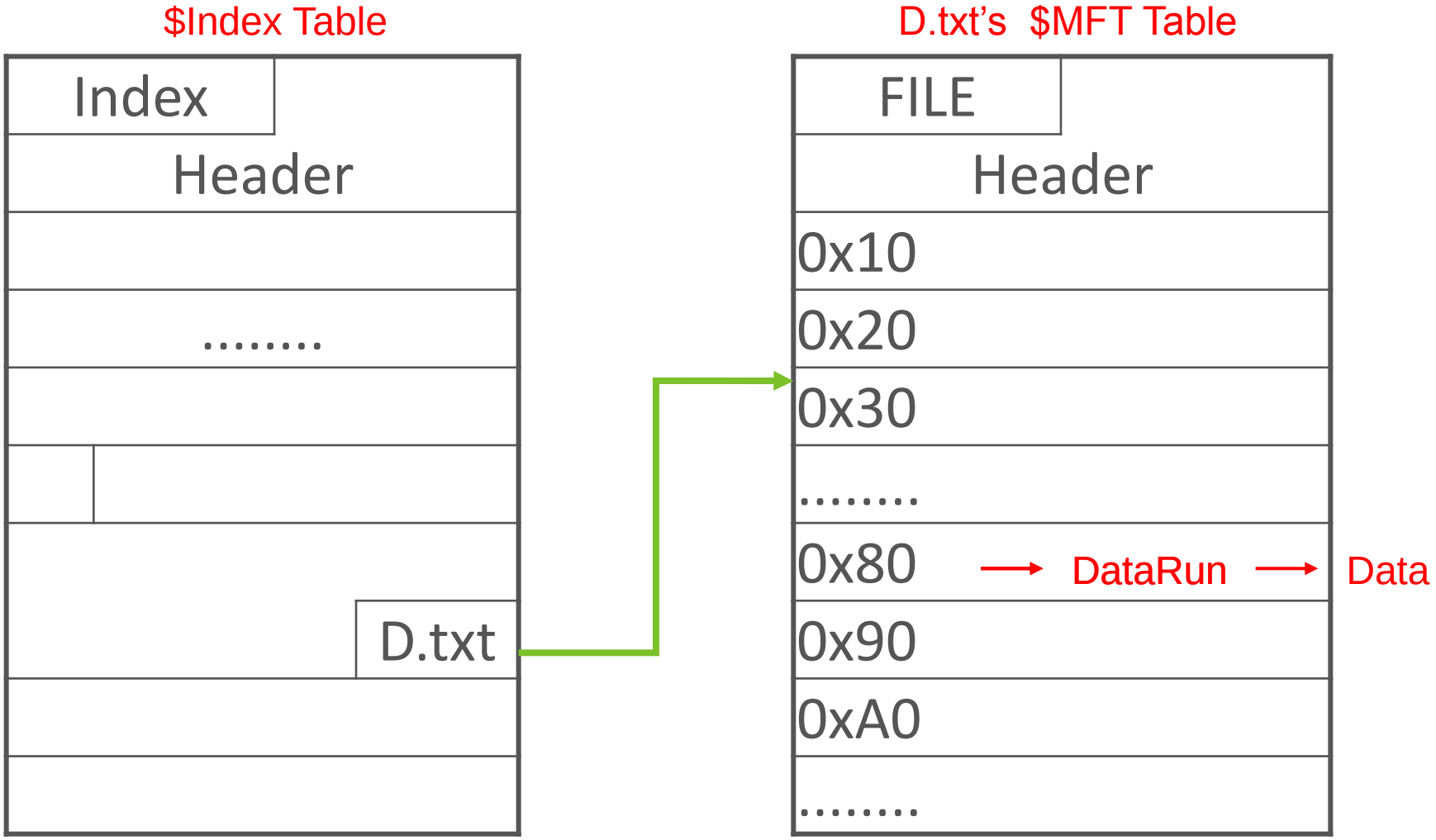
Search Film

C:\A\B\C\D.txt



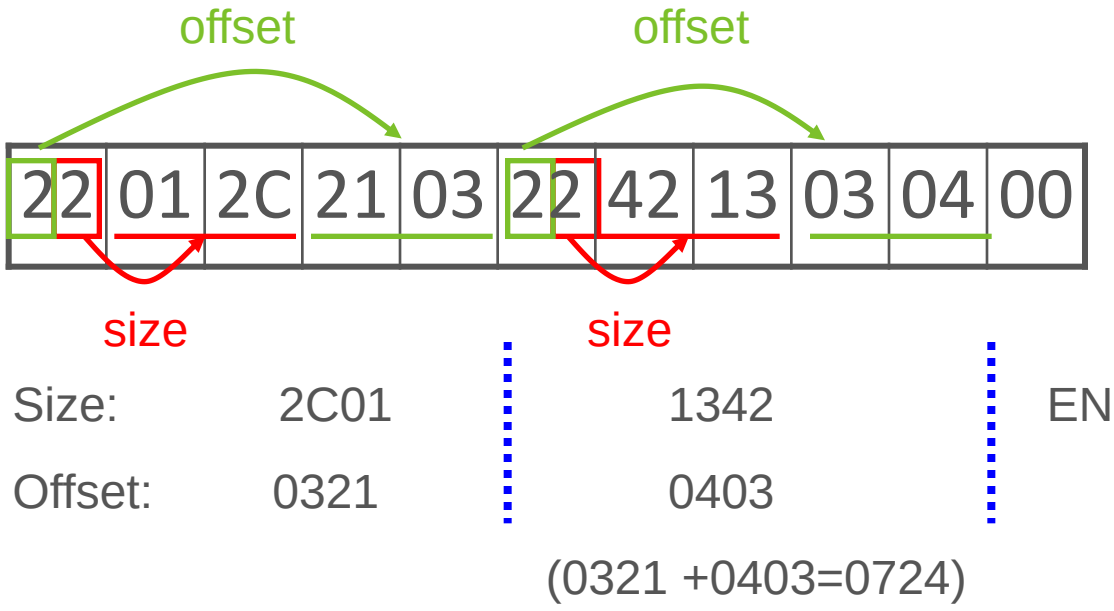
Search Film

C:\A\B\C\D.txt



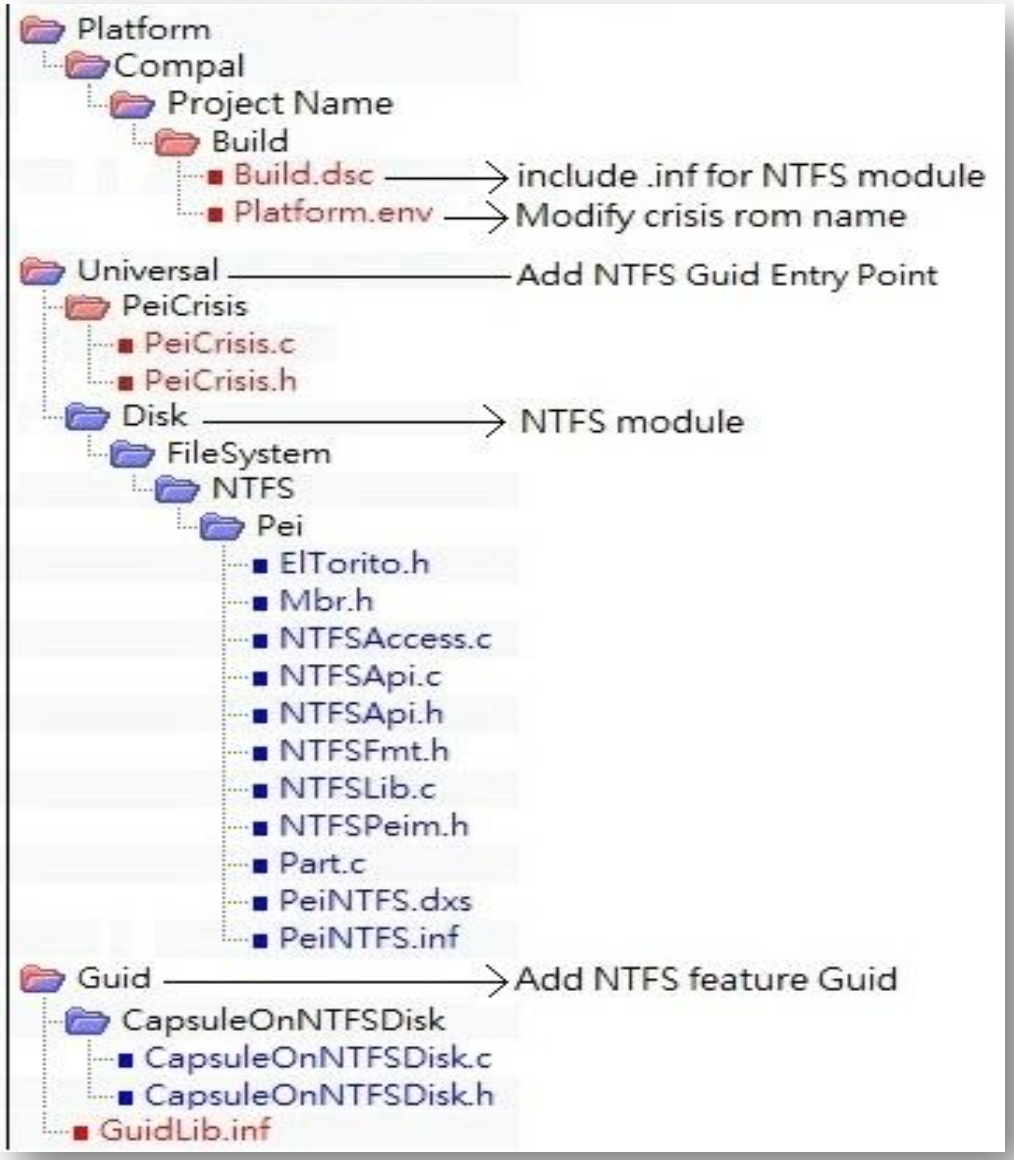
Datarun

0x80



This data (D.txt) size is 2C01+1342= 3F43(Cluster)
@ LCN 0321 and LCN 1745

File Architecture



Source Tree
New Folder

NTFS
~~NTFS5~~

File Path

- In “platform.env”

PEI_CRISIS_RECOVERY_FILE_NAME

= Layer 1\\Layer 2\\Layer3\\Layer4\\Layer5\\Layer6\\Layer7\\Layer8\\ BIOS name

Q&A