Data Recovery Analysis

August 2024

Version 2

(Done for Hashemite Univ. students Zinc 2)

Eng.Ali Bani Bakar

File System Forensics

- File systems are a crucial element of computer forensics
- Provide Forensics examiners the ability to retrieve a wealth of information
- How a user interacts with the files folders and running programs in the operating system environment
- A File System is responsible for managing all the activities involved with file creation and deletion ,relationships between objects , tracking times and dates as well as any available metadata for files and folders

NTFS FORENSICS

Sector = 512 Bytes (Smallest physical Unit) - Cluster = 1, 2, 4 or 8 …. Sectors

NTFS File system => Clusters (Logical Storage Unit)

Cluster = 2 Sectors	Cluster	Cluster	Cluster
Cluster	Cluster	Cluster	Cluster
Cluster	Cluster	Cluster	Cluster
Cluster	Cluster	Cluster	Cluster
Cluster	Cluster	Cluster	Cluster
Cluster	Cluster	Cluster	Cluster

Sector 512 Bytes	Sector	Sector	Sector	Sector	Sector	Sector	Sector
Sector	Sector	Sector	Sector	Sector	Sector	Sector	Sector
Sector	Sector	Sector	Sector	Sector	Sector	Sector	Sector
Sector	Sector	Sector	Sector	Sector	Sector	Sector	Sector
Sector	Sector	Sector	Sector	Sector	Sector	Sector	Sector
Sector	Sector	Sector	Sector	Sector	Sector	Sector	Sector

- Where does cluster size store?
- What does happen if a file was deleted ?
- What does happen if a file meta data was amended ?
- What does happen if a file data was amended ?

GUID PARTITION TABLE

BY: JARED ATKINSON
TEMPLATE BY: ANGE ALBERTINI

PROTECTIVE MBR

FIRST SECTOR OF DRIVE
FOR BREAKDOWN SEE MBR POSTER

```
000 33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00
010 06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00
020 BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10
030 E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00
040 B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09
050 F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74
060 26 66 68 00 00 00 00 66 FF 76 08 68 00 00 68 00
070 7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4 CD 13
080 9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00
090 8A 76 01 8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE
0A0 4E 11 75 0C 80 7E 00 80 0F 84 8A 00 B2 80 EB 84
0B0 55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E FE 7D 55
0C0 AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64
0D0 E8 83 00 B0 DF E6 60 E8 7C 00 B0 FF E6 64 E8 75
0E0 00 FB B8 00 BB CD 1A 66 23 C0 75 3B 66 81 FB 54
0F0 43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00
100 00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66
110 53 66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66
120 61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD
130 18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E4
140 05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD
150 10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8
160 24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69
170 74 69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72
180 20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69
190 6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E
1A0 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74
1B0 65 6D 00 00 00 63 7B 9A 00 00 00 00 00 00 00 00
1C0 02 00 EE FF FF FF 01 00 00 00 FF FF FF FF 00 00
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
```

IMPORTANT PROTECTIVE MBR VALUES

system id	EE - EFI GPT partition
GPT header sector offset	1

GPT HEADER

```
200 45 46 49 20 50 41 52 54 00 00 01 00 5C 00 00 00
210 F3 73 9F 97             01 00 00 00 00 00 00 00
220 FF FF 3F 01 00 00 00 00 22 00 00 00 00 00 00 00
230 DE FF 3F 01 00 00 00 00 10 E1 13 F9 35 08 F1 4C
240 96 C7 38 0B 5D B4 A4 2D 02 00 00 00 00 00 00 00
250 80 00 00 00 80 00 00 00 3B 04 A4 F8
```

signature	EFI PART
revision	1.0
header size	92
header CRC32	979F73F3
my LBA	1
alternate LBA	20971519
first usable LBA	34
last usable LBA	20971486
disk guid	f913e110-0835-4cf1-96c7-380b5db4a42d
partition entry LBA	2 (sector containing of partition table)
# of partition entries	128
size of partition entry	128
partition entry array CRC32	F8A4043B

PARITION ARRAY

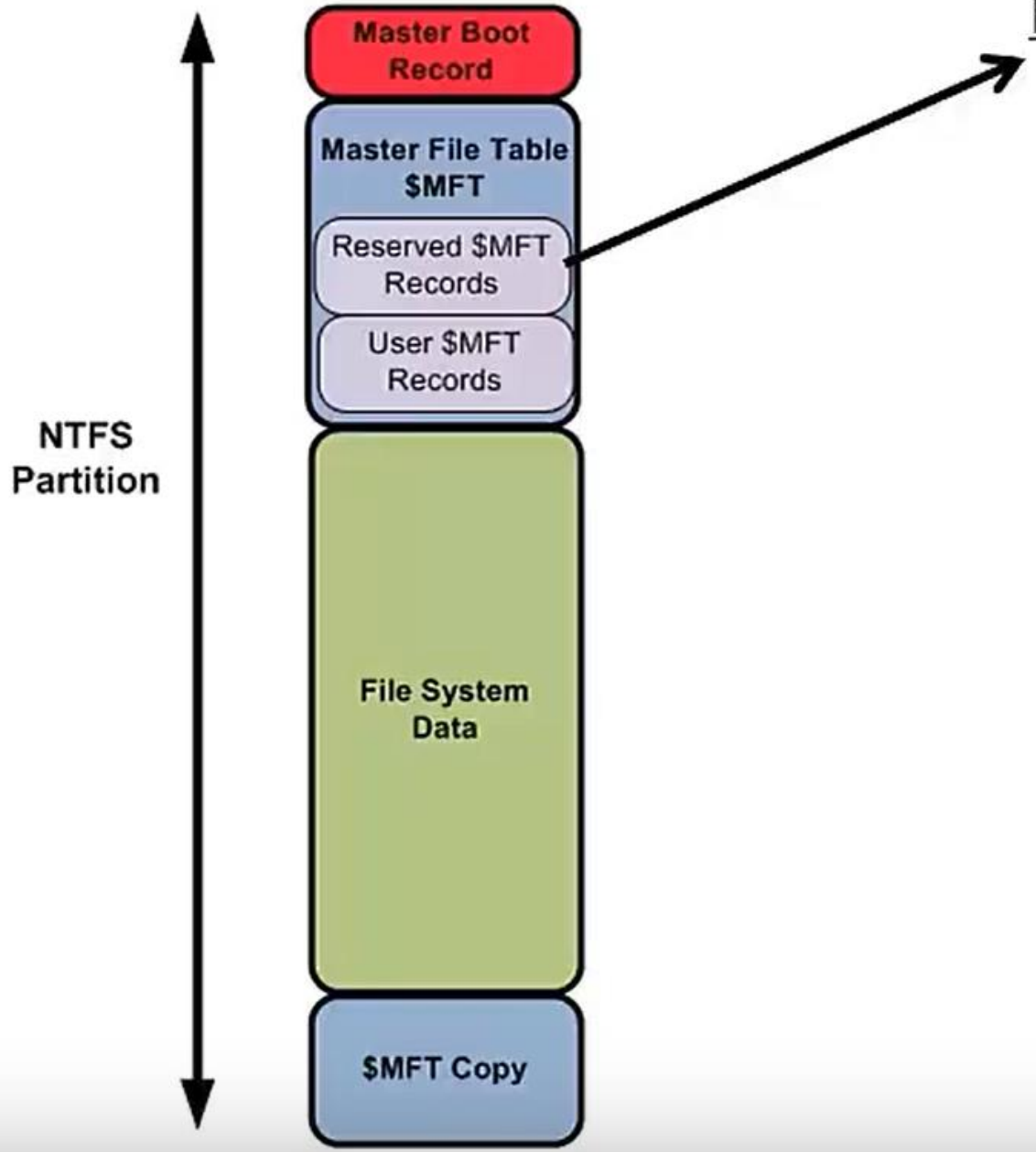
```
400 16 E3 C9 E3 5C 0B B8 4D 81 7D F9 2D F0 02 15 AE
410 47 8A 1A FF F8 08 AB 43 B4 10 53 69 7F 0B 23 23
420 22 00 00 00 00 00 00 00 21 00 01 00 00 00 00 00
430 00 00 00 00 00 00 00 00 4D 00 69 00 63 00 72 00
440 6F 00 73 00 6F 00 66 00 74 00 20 00 72 00 65 00
450 73 00 65 00 72 00 76 00 65 00 64 00 20 00 70 00
460 61 00 72 00 74 00 69 00 74 00 69 00 6F 00 6E 00
470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

480 A2 A0 D0 EB E5 B9 33 44 87 C0 68 B6 B7 26 99 C7
490 42 AE 76 6D C1 B6 BE 4F 8D 42 20 CD 36 60 26 B4
4A0 00 08 01 00 00 00 00 00 FF 07 00 00 00 00 00 00
4B0 00 00 00 00 00 00 00 00 42 00 61 00 73 00 69 00
4C0 63 00 20 00 64 00 61 00 74 00 61 00 20 00 70 00
4D0 61 00 72 00 74 00 69 00 74 00 69 00 6F 00 6E 00
4E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
4F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

500 A2 A0 D0 EB E5 B9 33 44 87 C0 68 B6 B7 26 99 C7
510 3A 5C 79 D6 4D 8A B4 4F 91 A0 48 88 12 CC E0 27
520 00 08 00 00 00 00 00 00 FF 07 41 00 00 00 00 00
530 00 00 00 00 00 00 00 00 42 00 61 00 73 00 69 00
540 63 00 20 00 64 00 61 00 74 00 61 00 20 00 70 00
550 61 00 72 00 74 00 69 00 74 00 69 00 6F 00 6E 00
560 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
570 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

partition type guid	e3c9e316-0b5c-4db8-817d-f92df00215ae
unique partition guid	ff1a8a47-08f8-43ab-b410-53697f0b2323
starting LBA	34
ending LBA	65569
attributes	0
partition name	Microsoft reserved partition

partition type guid	ebd0a0a2-b9e5-4433-87c0-68b6b72699c7
unique partition guid	6d76ae42-b6c1-4fbe-8d42-20cd366026b4
starting LBA	67584
ending LBA	2164735
attributes	0
partition name	Basic data partition

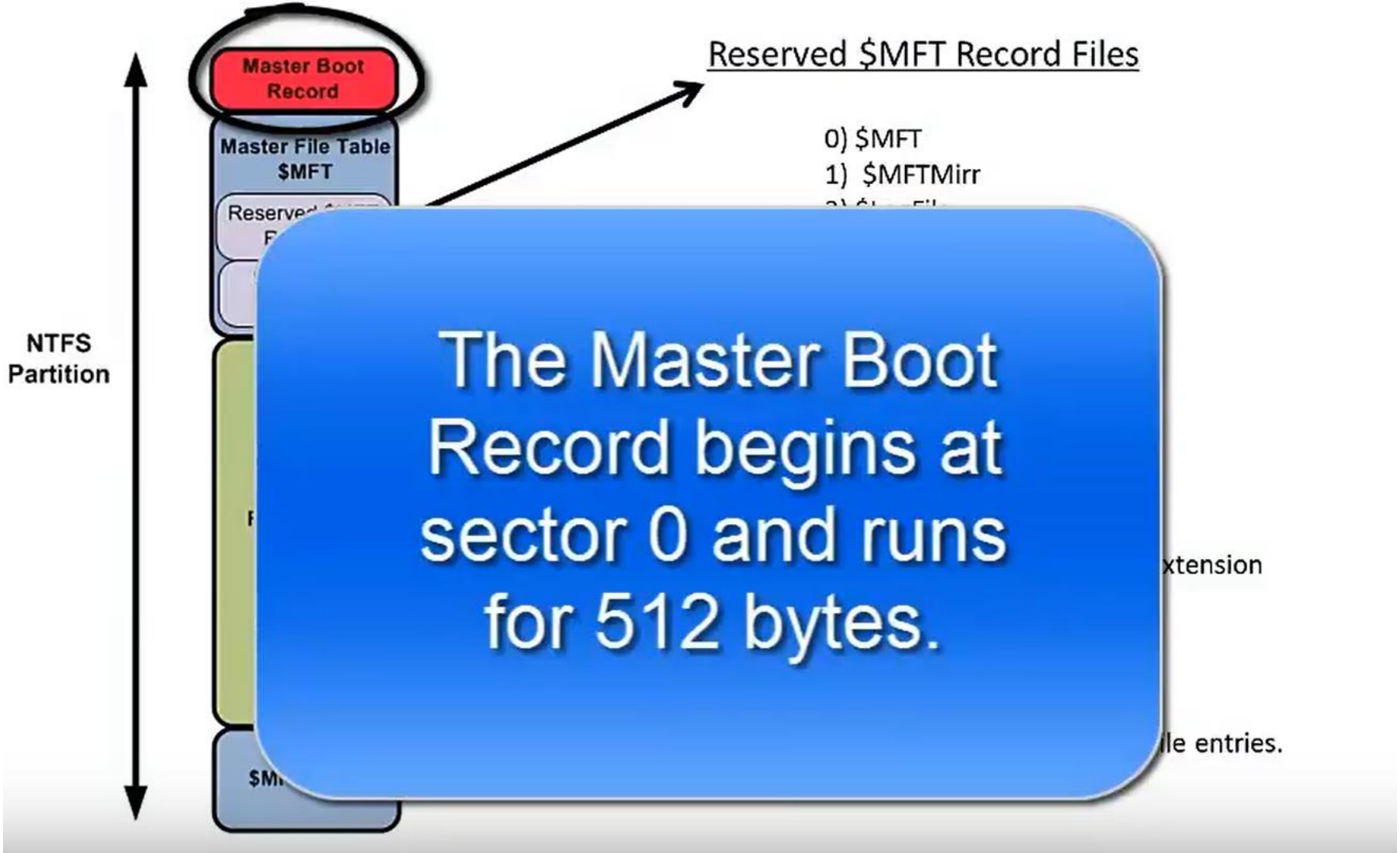
partition type guid	ebd0a0a2-b9e5-4433-87c0-68b6b72699c7
unique partition guid	d6795c3a-8a4d-4fb4-91a0-488812cce027
starting LBA	2164736
ending LBA	4261887
attributes	0
partition name	Basic data partition

ENG ALI BANI BAKAR 0778642376

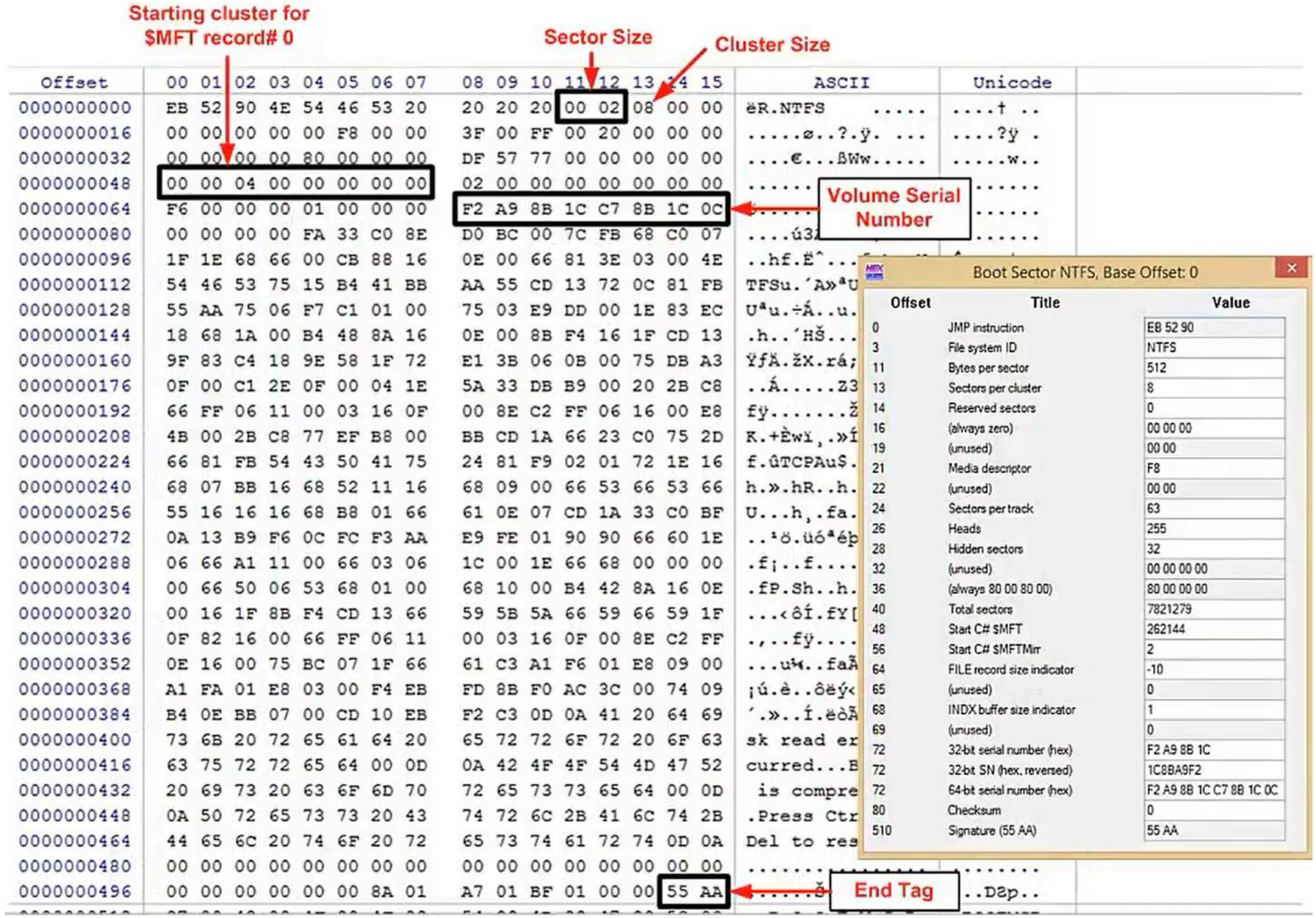


Reserved $MFT Record Files

0) $MFT
1) $MFTMirr
2) $LogFile
3) $Volume
4) $AttrDef
5) Root directory.
6) $Bitmap
7) $Boot
8) $BadClus
9) $Secure
10) $UpCase
11) $Extend
12–23) Reserved for $MFT extension entries
24) $Extend\$Quota
25) $Extend\$ObjId
26) $Extend\$Reparse
27— Beginning of regular file entries.


Master Boot Record
Master File Table $MFT
NTFS Partition
Reserved $MFT Record Files
0) $MFT
1) $MFTMirr
The Master Boot Record begins at sector 0 and runs for 512 bytes.
xtension
le entries.

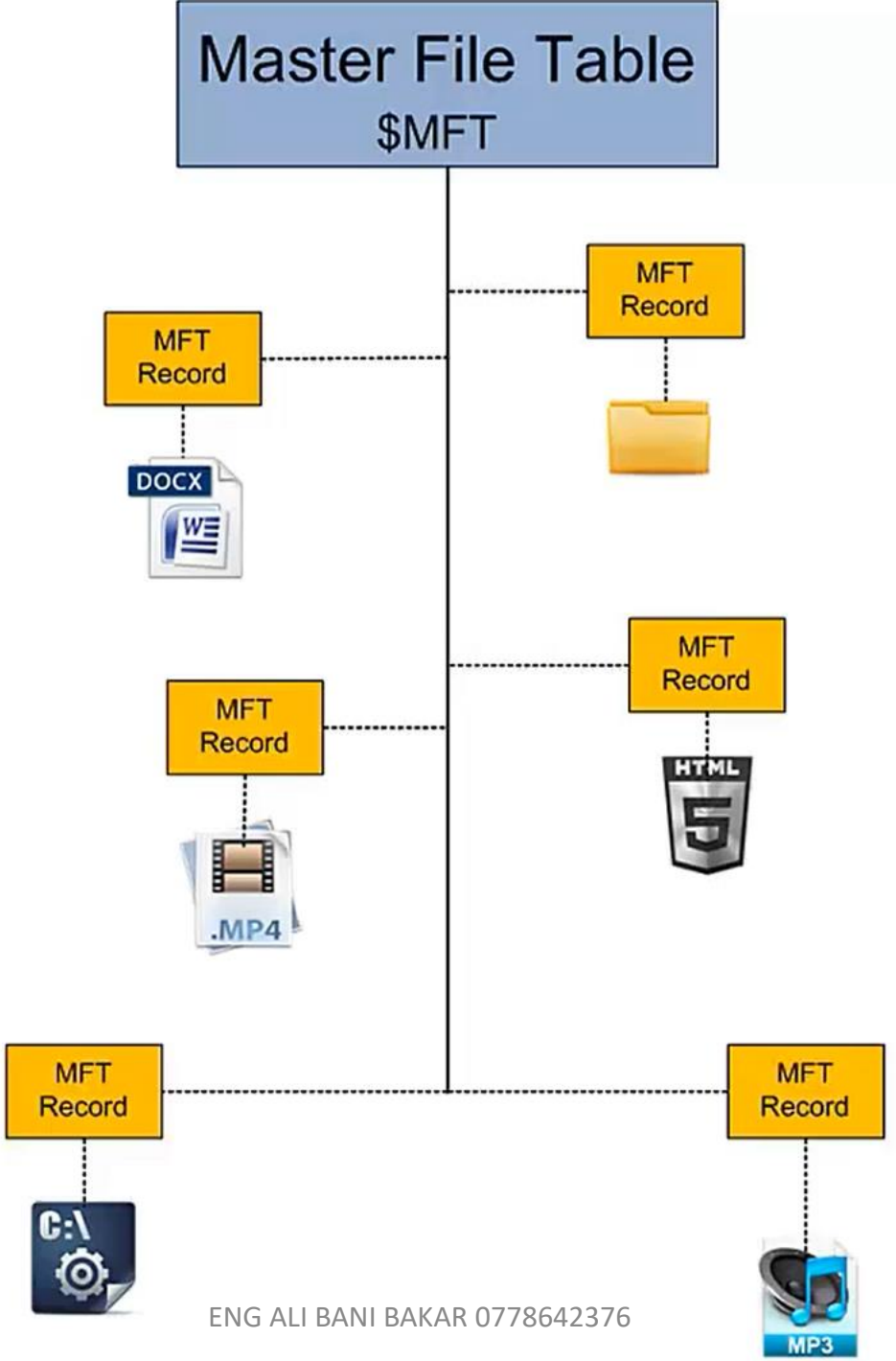
Master Boot Record



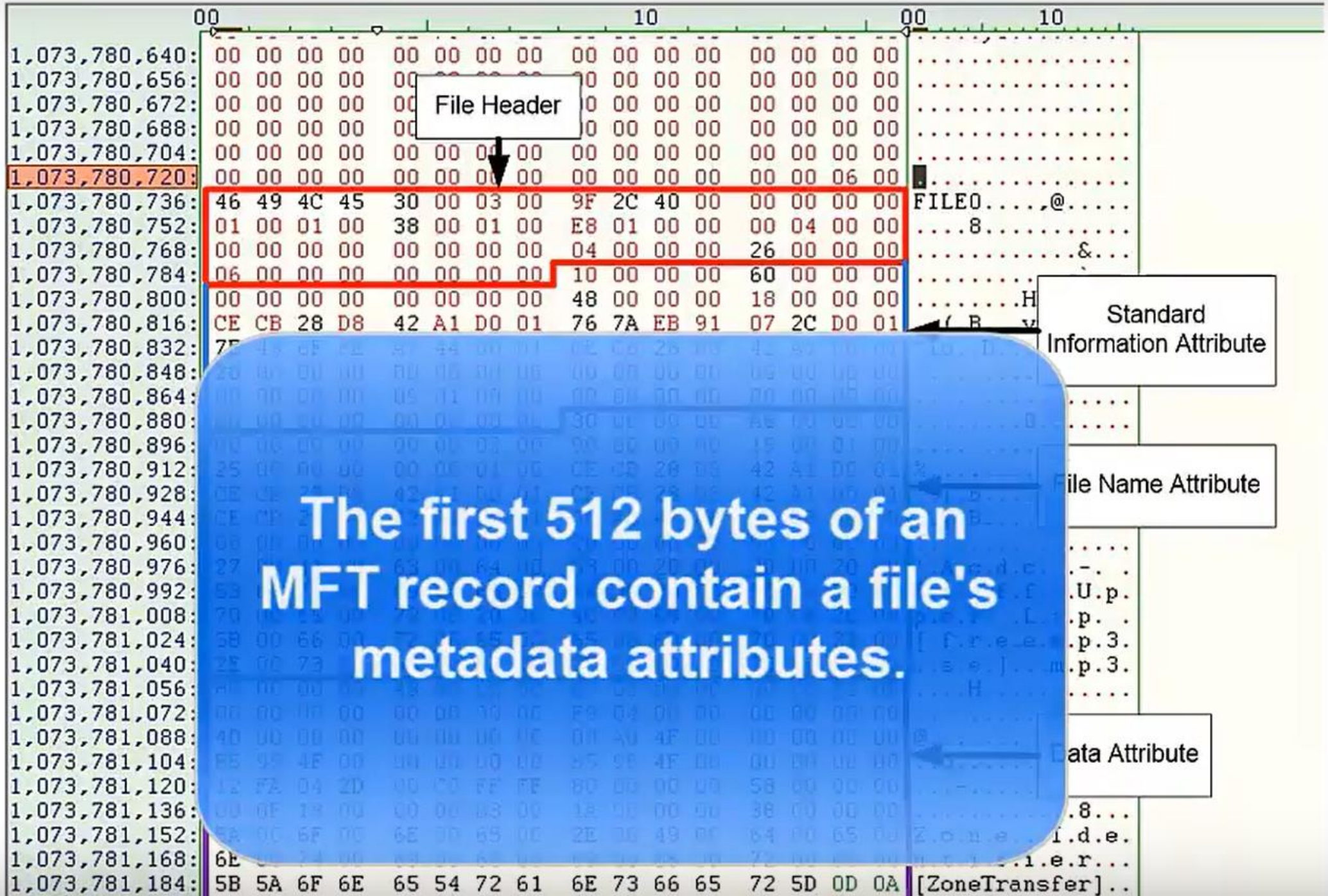
Master File Table (MFT)

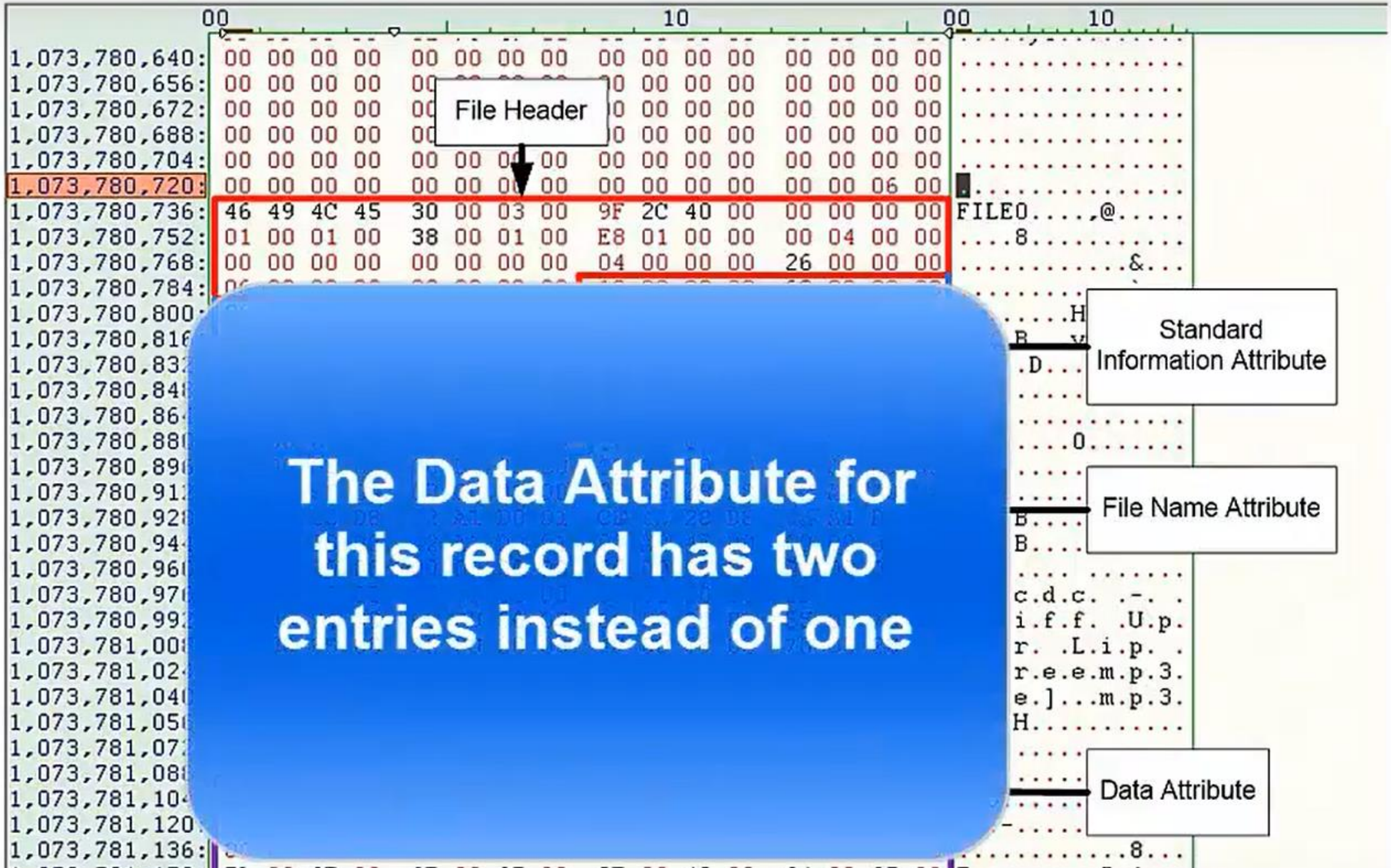
- MFT or $MFT keeps records of all files in a volume, the files' location in the directory, the physical location of the files on the drive, and file metadata.
- The metadata includes file and folder create dates, entry modified dates, access dates, last written dates, physical and logical file size, and ACLs of the files.
- The file and directory metadata is stored as an MFT entry that is 1024 bytes in size. The first 16 entries in the MFT belong to system files, such as the MFT itself.
- From a forensics investigator's perspective, entries are very interesting because when a file is deleted an entry gets marked as unallocated while the file content on the drive remains intact. The file name in the MFT entry can be overwritten due to MFT tree structure reorganization, so most of the time file names are not maintained. File data eventually is overwritten as the unallocated drive space gets used.

- MFT ia an ntfs data structure which contains records for all files created loaded updated and deleted in the volume

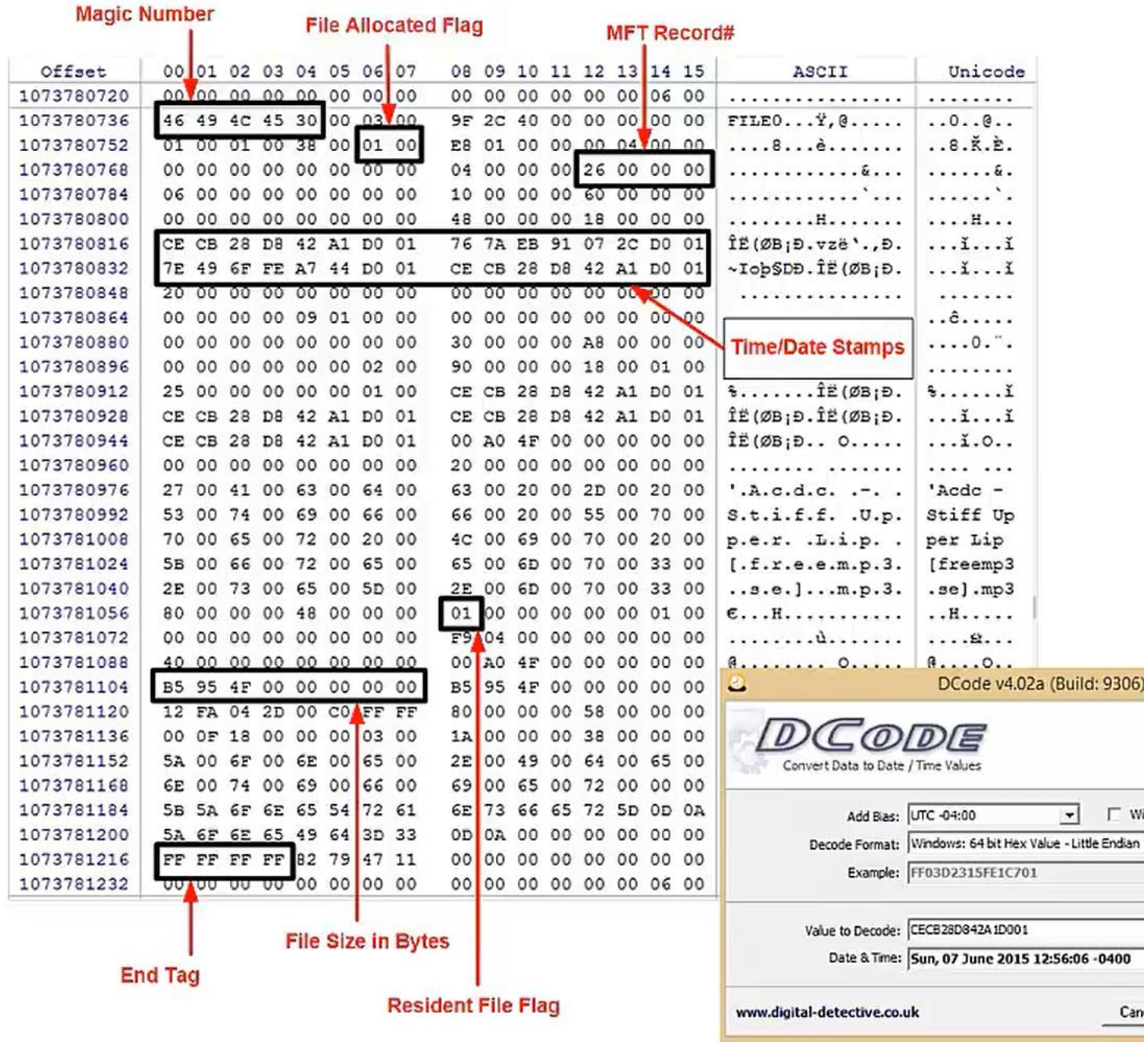


ENG ALI BANI BAKAR 0778642376


File Header
Standard Information Attribute
ile Name Attribute
ata Attribute
The first 512 bytes of an MFT record contain a file's metadata attributes.

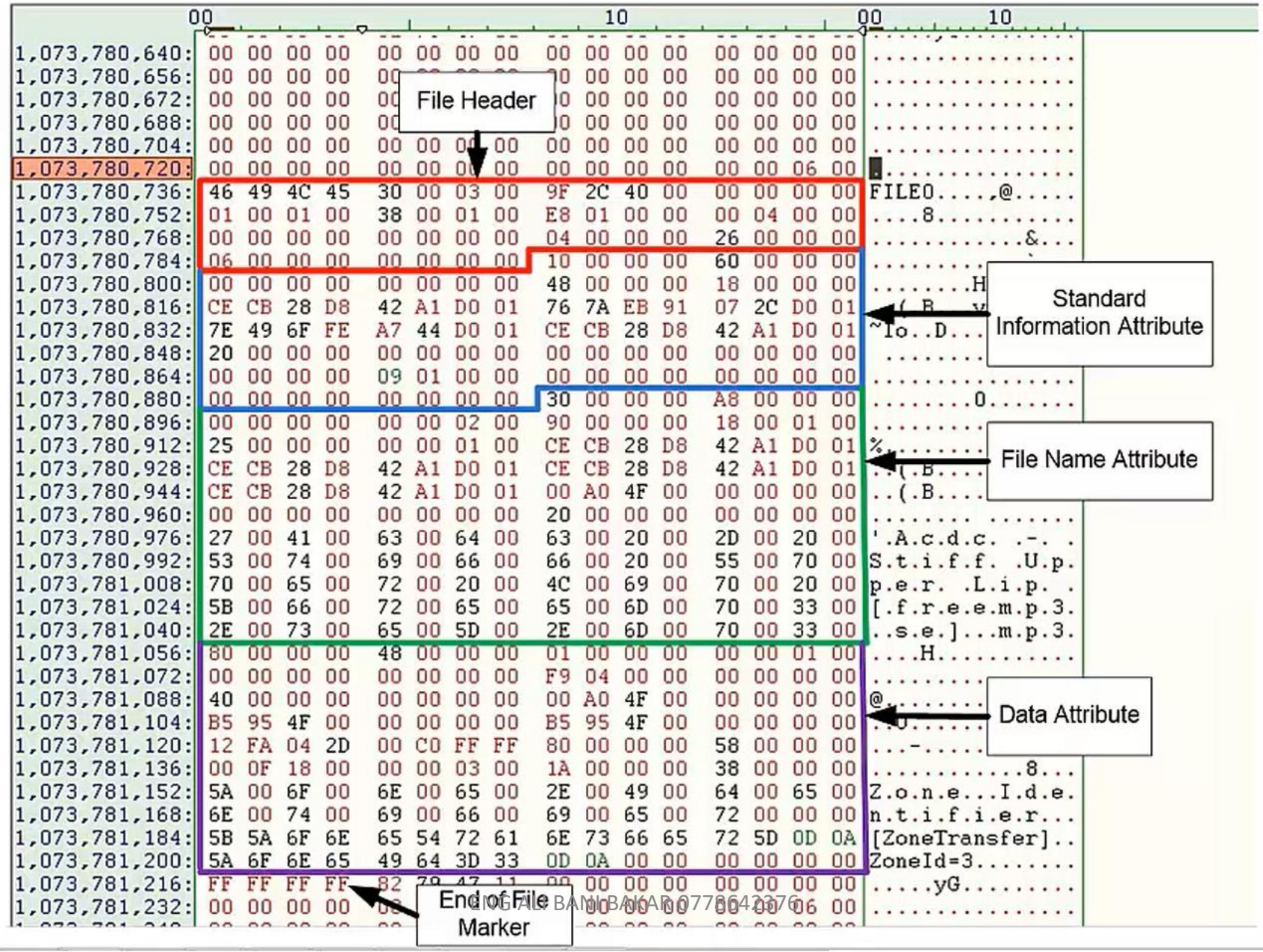

00
10
00
10
1,073,780,640: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1,073,780,656: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1,073,780,672: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1,073,780,688: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1,073,780,704: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1,073,780,720: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00
1,073,780,736: 46 49 4C 45 30 00 03 00 9F 2C 40 00 00 00 00 00 FILE0....,@.....
1,073,780,752: 01 00 01 00 38 00 01 00 E8 01 00 00 00 04 00 00 ....8...........
1,073,780,768: 00 00 00 00 00 00 00 00 04 00 00 00 26 00 00 00 ....&...
File Header
Standard Information Attribute
File Name Attribute
Data Attribute
The Data Attribute for this record has two entries instead of one

$MFT Record File



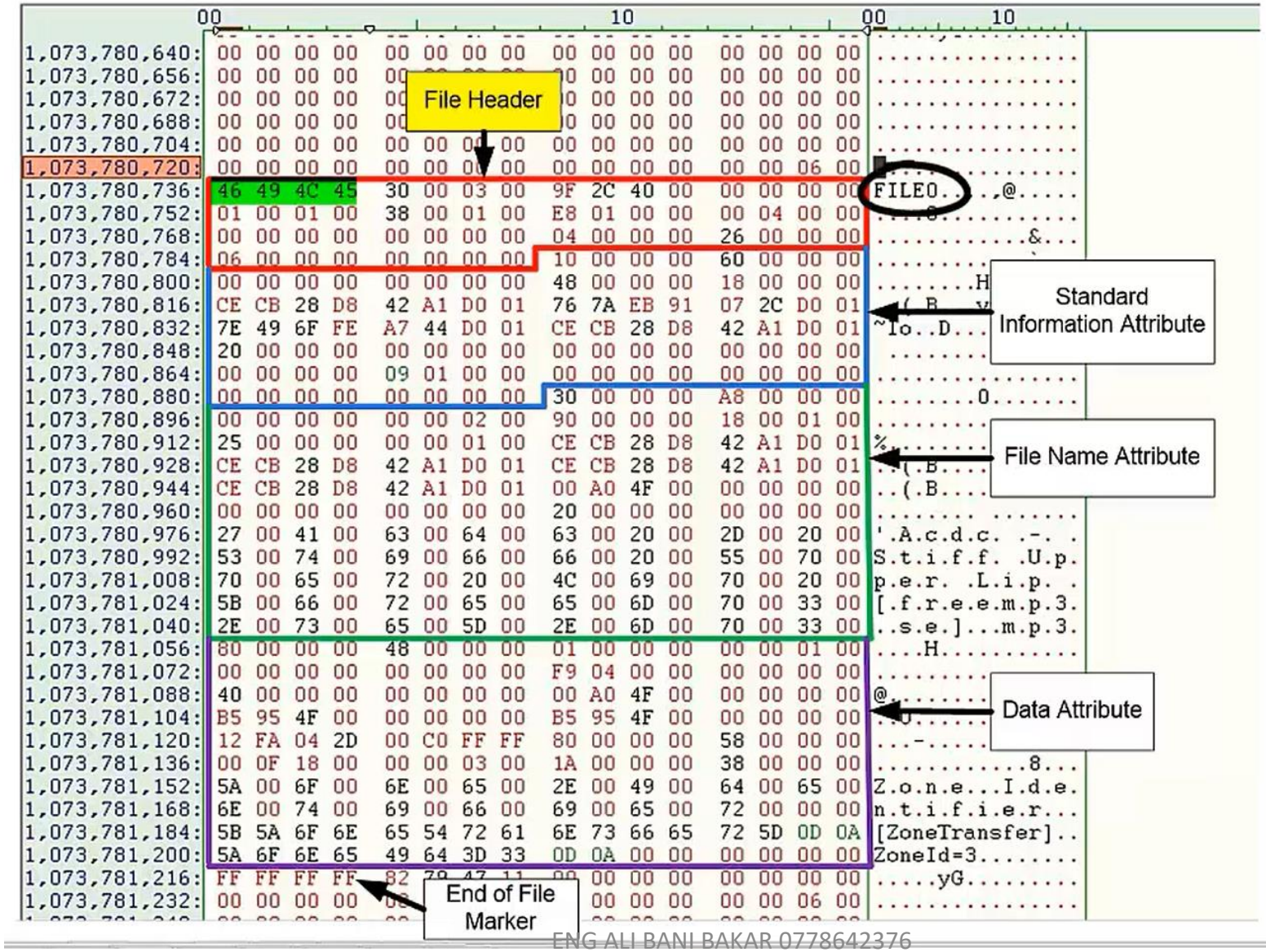
Offset	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII	Unicode
1073780720	00 00 00 00 00 00 00 00	00 00 00 00 00 00 06 00	.....	.....
1073780736	46 49 4C 45 30 00 03 00	9F 2C 40 00 00 00 00 00	FILE0...Ÿ,@.....	..0..@..
1073780752	01 00 01 00 38 00 01 00	E8 01 00 00 00 04 00 00	....8...è.....	..8.Ř.È.
1073780768	00 00 00 00 00 00 00 00	04 00 00 00 26 00 00 00	....&...	....&.
1073780784	06 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	....`...	....`.
1073780800	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	....H...	....H...
1073780816	CE CB 28 D8 42 A1 D0 01	76 7A EB 91 07 2C D0 01	ÎË(ØB¡Ð.vzë'.,Ð.	...ĭ...ĭ
1073780832	7E 49 6F FE A7 44 D0 01	CE CB 28 D8 42 A1 D0 01	~Ioþ§DÐ.ÎË(ØB¡Ð.	...ĭ...ĭ
1073780848	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....	.....
1073780864	00 00 00 00 09 01 00 00	00 00 00 00 00 00 00 00	..ê.....	
1073780880	00 00 00 00 00 00 00 00	30 00 00 00 A8 00 00 00	....0.¨.	
1073780896	00 00 00 00 00 00 02 00	90 00 00 00 18 00 01 00	.....	
1073780912	25 00 00 00 00 00 01 00	CE CB 28 D8 42 A1 D0 01	%.....ÎË(ØB¡Ð.	%.....ĭ
1073780928	CE CB 28 D8 42 A1 D0 01	CE CB 28 D8 42 A1 D0 01	ÎË(ØB¡Ð.ÎË(ØB¡Ð.	...ĭ...ĭ
1073780944	CE CB 28 D8 42 A1 D0 01	00 A0 4F 00 00 00 00 00	ÎË(ØB¡Ð.. O.....	...ĭ.O..
1073780960	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	....	....
1073780976	27 00 41 00 63 00 64 00	63 00 20 00 2D 00 20 00	'.A.c.d.c. .-. .	'Acdc -
1073780992	53 00 74 00 69 00 66 00	66 00 20 00 55 00 70 00	S.t.i.f.f. .U.p.	Stiff Up
1073781008	70 00 65 00 72 00 20 00	4C 00 69 00 70 00 20 00	p.e.r. .L.i.p. .	per Lip
1073781024	5B 00 66 00 72 00 65 00	65 00 6D 00 70 00 33 00	[.f.r.e.e.m.p.3.	[freemp3
1073781040	2E 00 73 00 65 00 5D 00	2E 00 6D 00 70 00 33 00	..s.e.]...m.p.3.	.se].mp3
1073781056	80 00 00 00 48 00 00 00	01 00 00 00 00 00 01 00	€...H.....	..H.....
1073781072	00 00 00 00 00 00 00 00	F9 04 00 00 00 00 00 00	.....ù.....	....ù...
1073781088	40 00 00 00 00 00 00 00	00 A0 4F 00 00 00 00 00	@..... O.....	@....O..
1073781104	B5 95 4F 00 00 00 00 00	B5 95 4F 00 00 00 00 00	µ.O.....µ.O.....	µ.O.....µ.O.....
1073781120	12 FA 04 2D 00 C0 FF FF	80 00 00 00 58 00 00 00	.ú.-.ÀÿÿX...	
1073781136	00 0F 18 00 00 00 03 00	1A 00 00 00 38 00 00 00	....8...	
1073781152	5A 00 6F 00 6E 00 65 00	2E 00 49 00 64 00 65 00	Z.o.n.e...I.d.e.	
1073781168	6E 00 74 00 69 00 66 00	69 00 65 00 72 00 00 00	n.t.i.f.i.e.r...	
1073781184	5B 5A 6F 6E 65 54 72 61	6E 73 66 65 72 5D 0D 0A	[ZoneTransfer]...	
1073781200	5A 6F 6E 65 49 64 3D 33	0D 0A 00 00 00 00 00 00	ZoneId=3.....	
1073781216	FF FF FF FF 82 79 47 11	00 00 00 00 00 00 00 00	ÿÿÿÿ‚yG.....	
1073781232	00 00 00 00 00 00 00 00	00 00 00 00 00 00 06 00	.....	

Structure of an $MFT Record

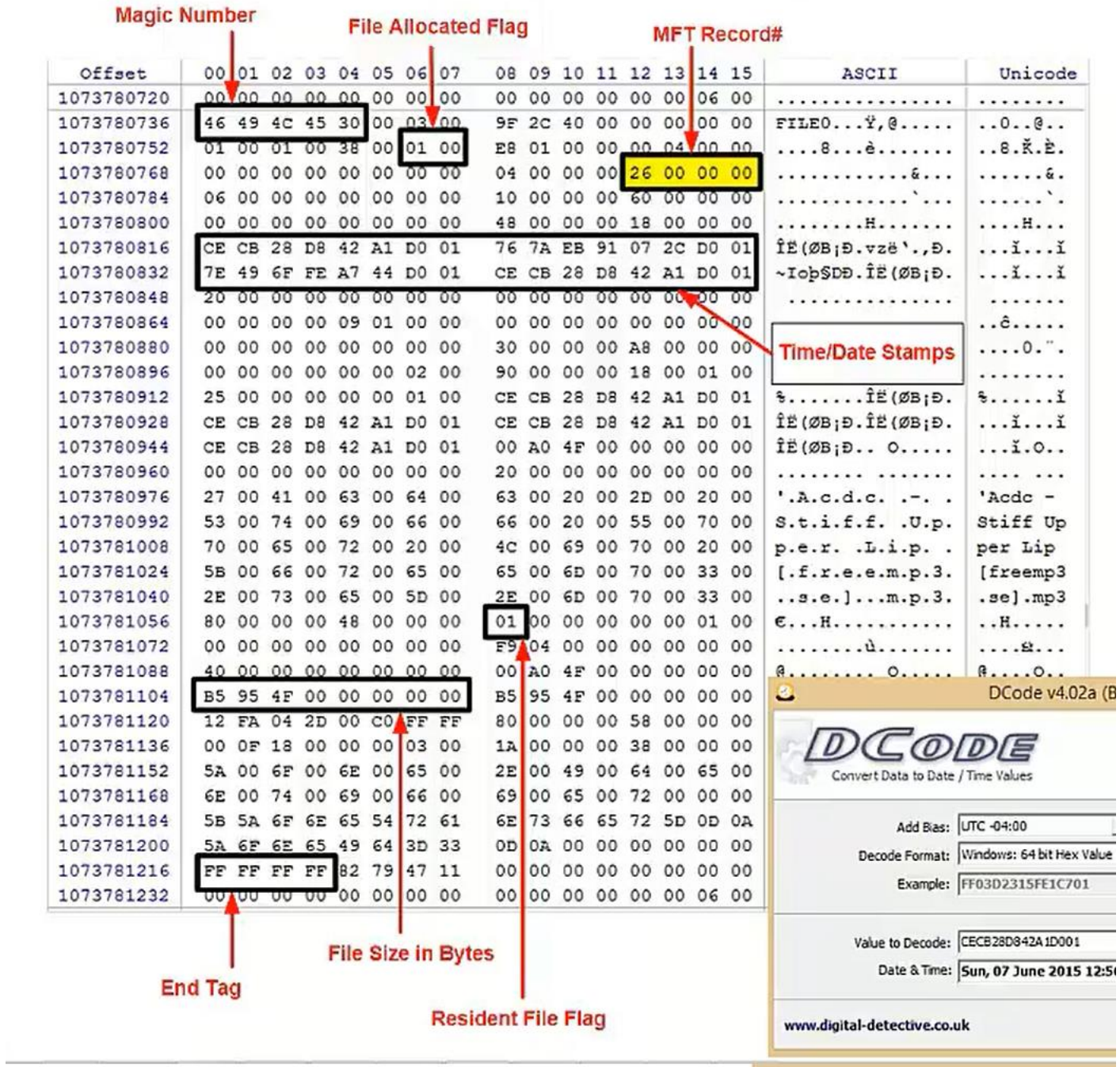


DIGITAL BANI BAKAR 0778643376

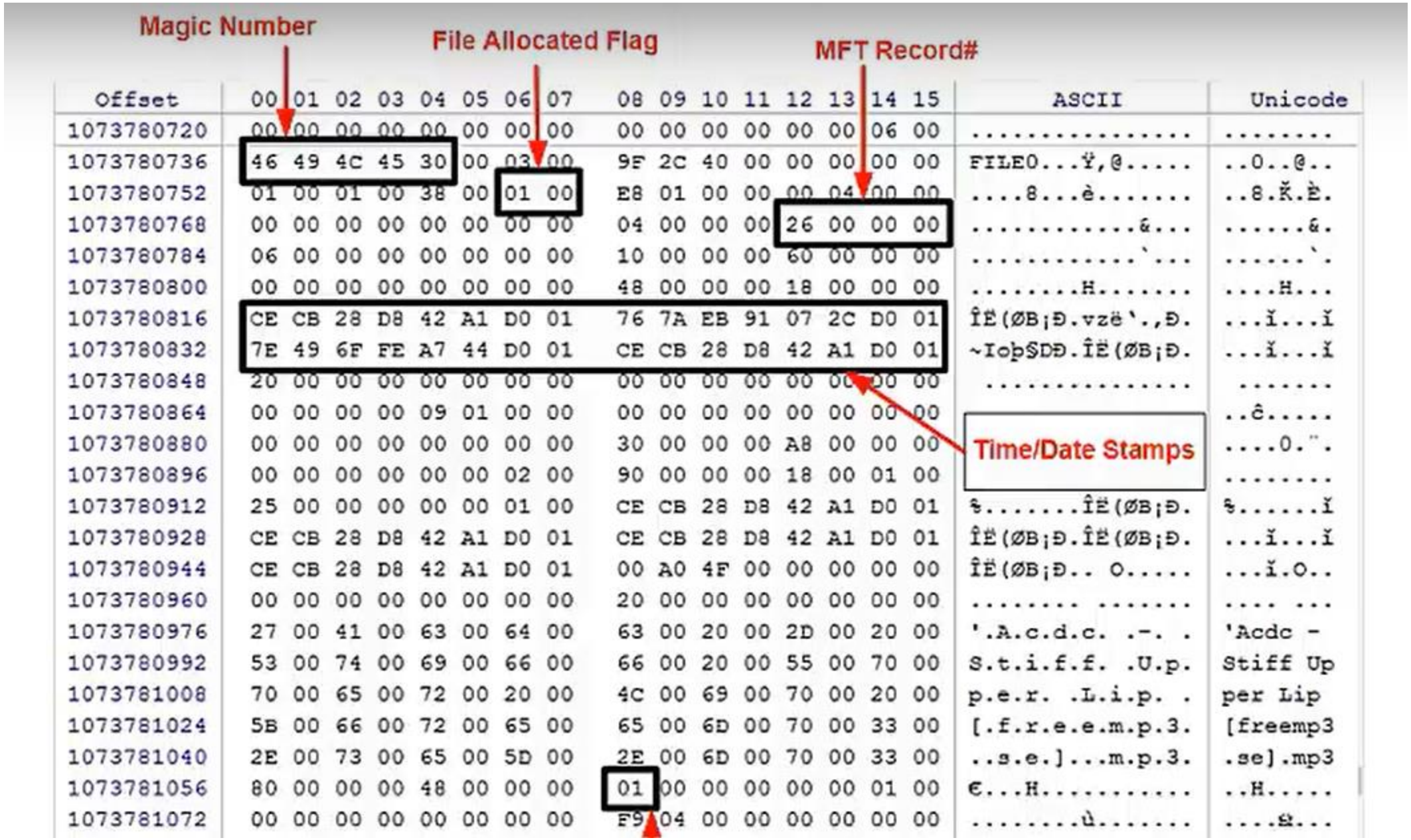
Structure of an $MFT Record



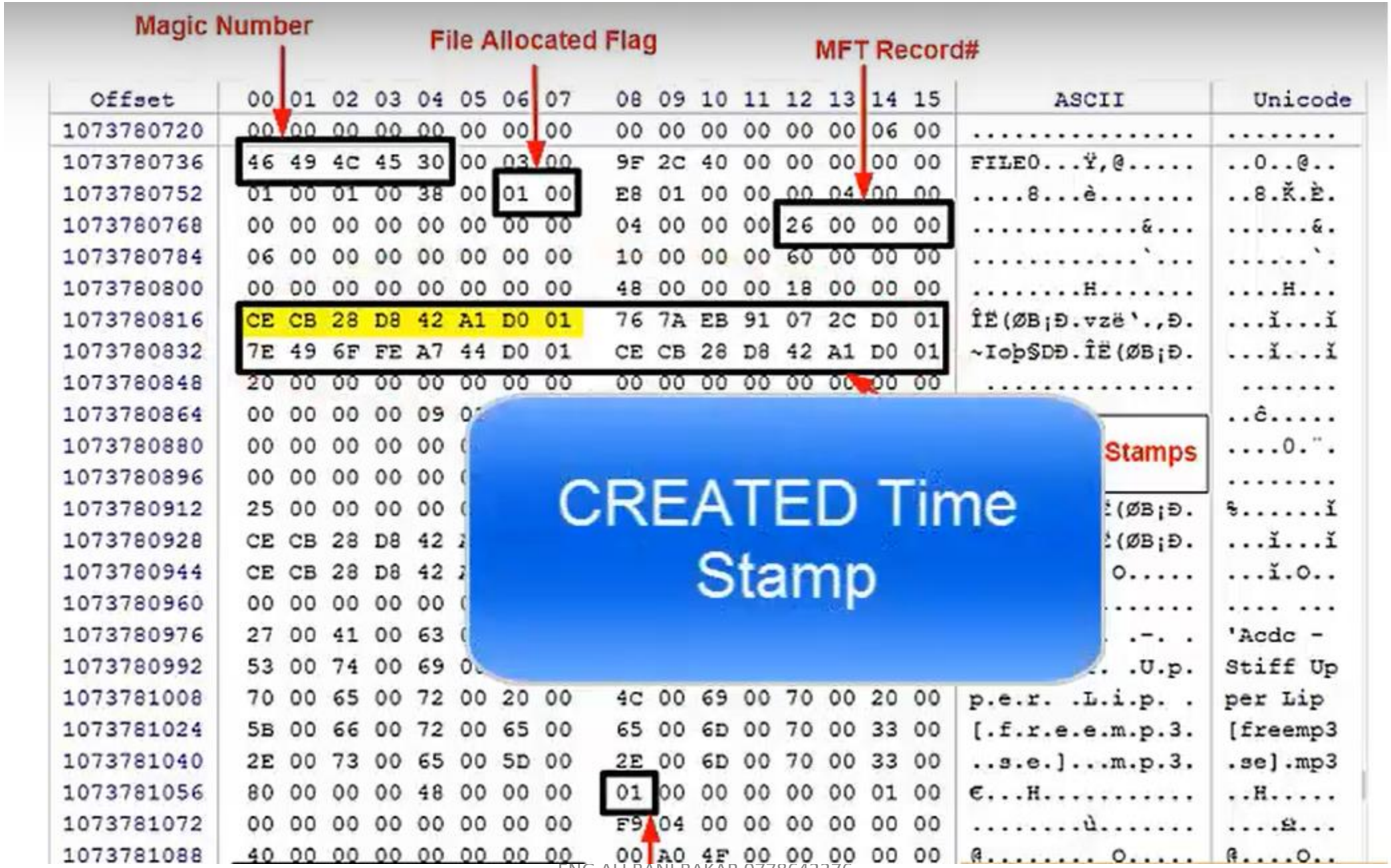
$MFT Record File



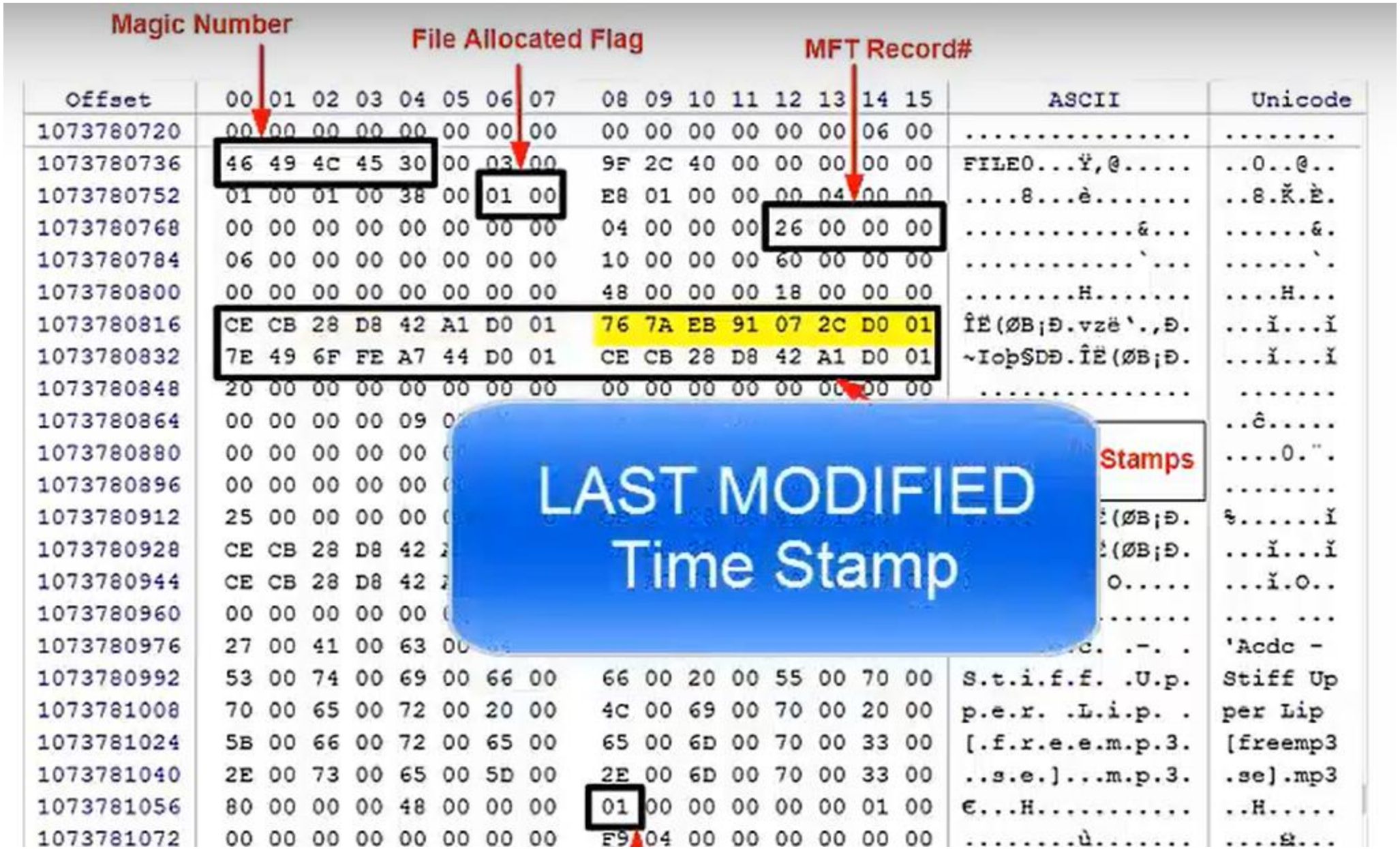
Offset	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII	Unicode
1073780720	00 00 00 00 00 00 00 00	00 00 00 00 00 00 06 00	.....	.....
1073780736	46 49 4C 45 30 00 03 00	9F 2C 40 00 00 00 00 00	FILE0...Ÿ,@.....	..0..@..
1073780752	01 00 01 00 38 00 01 00	E8 01 00 00 00 04 00 00	....8...è.....	..8.Ǩ.È.
1073780768	00 00 00 00 00 00 00 00	04 00 00 00 26 00 00 00	............&	......&.
1073780784	06 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	............`...	......`.
1073780800	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	........H.....	....H...
1073780816	CE CB 28 D8 42 A1 D0 01	76 7A EB 91 07 2C D0 01	ÎË(ØB¡Ð.vzë'.,Ð.	...ǐ...ǐ
1073780832	7E 49 6F FE A7 44 D0 01	CE CB 28 D8 42 A1 D0 01	~Ioþ§DÐ.ÎË(ØB¡Ð.	...ǐ...ǐ
1073780848	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....	.....
1073780864	00 00 00 00 09 01 00 00	00 00 00 00 00 00 00 00	..ĉ.....	
1073780880	00 00 00 00 00 00 00 00	30 00 00 00 A8 00 00 00	....0.¨.	
1073780896	00 00 00 00 00 00 02 00	90 00 00 00 18 00 01 00	.....	
1073780912	25 00 00 00 00 00 01 00	CE CB 28 D8 42 A1 D0 01	%.....ÎË(ØB¡Ð.	%.....ǐ
1073780928	CE CB 28 D8 42 A1 D0 01	CE CB 28 D8 42 A1 D0 01	ÎË(ØB¡Ð.ÎË(ØB¡Ð.	...ǐ...ǐ
1073780944	CE CB 28 D8 42 A1 D0 01	00 A0 4F 00 00 00 00 00	ÎË(ØB¡Ð.. O.....	...ǐ.O..
1073780960	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	....	....
1073780976	27 00 41 00 63 00 64 00	63 00 20 00 2D 00 20 00	'.A.c.d.c. .-. .	'Acdc -
1073780992	53 00 74 00 69 00 66 00	66 00 20 00 55 00 70 00	S.t.i.f.f. .U.p.	Stiff Up
1073781008	70 00 65 00 72 00 20 00	4C 00 69 00 70 00 20 00	p.e.r. .L.i.p. .	per Lip
1073781024	5B 00 66 00 72 00 65 00	65 00 6D 00 70 00 33 00	[.f.r.e.e.m.p.3.	[freemp3
1073781040	2E 00 73 00 65 00 5D 00	2E 00 6D 00 70 00 33 00	..s.e.]...m.p.3.	.se].mp3
1073781056	80 00 00 00 48 00 00 00	01 00 00 00 00 00 01 00	€...H.....	..H.....
1073781072	00 00 00 00 00 00 00 00	F9 04 00 00 00 00 00 00	.....ù.....	....ù...
1073781088	40 00 00 00 00 00 00 00	00 A0 4F 00 00 00 00 00	@..... O.....	@....O..
1073781104	B5 95 4F 00 00 00 00 00	B5 95 4F 00 00 00 00 00	µ•O.....µ•O.....	µ•O.....µ•O..
1073781120	12 FA 04 2D 00 C0 FF FF	80 00 00 00 58 00 00 00	.ú.-.ÀÿÿX...	
1073781136	00 0F 18 00 00 00 03 00	1A 00 00 00 38 00 00 00	.....	
1073781152	5A 00 6F 00 6E 00 65 00	2E 00 49 00 64 00 65 00	Z.o.n.e. .I.d.e.	
1073781168	6E 00 74 00 69 00 66 00	69 00 65 00 72 00 00 00	n.t.i.f.i.e.r...	
1073781184	5B 5A 6F 6E 65 54 72 61	6E 73 66 65 72 5D 0D 0A	[ZoneTransfer]..	
1073781200	5A 6F 6E 65 49 64 3D 33	0D 0A 00 00 00 00 00 00	ZoneId=3.....	
1073781216	FF FF FF FF 82 79 47 11	00 00 00 00 00 00 00 00	ÿÿÿÿ‚yG.....	
1073781232	00 00 00 00 00 00 00 00	00 00 00 00 00 00 06 00	.....	

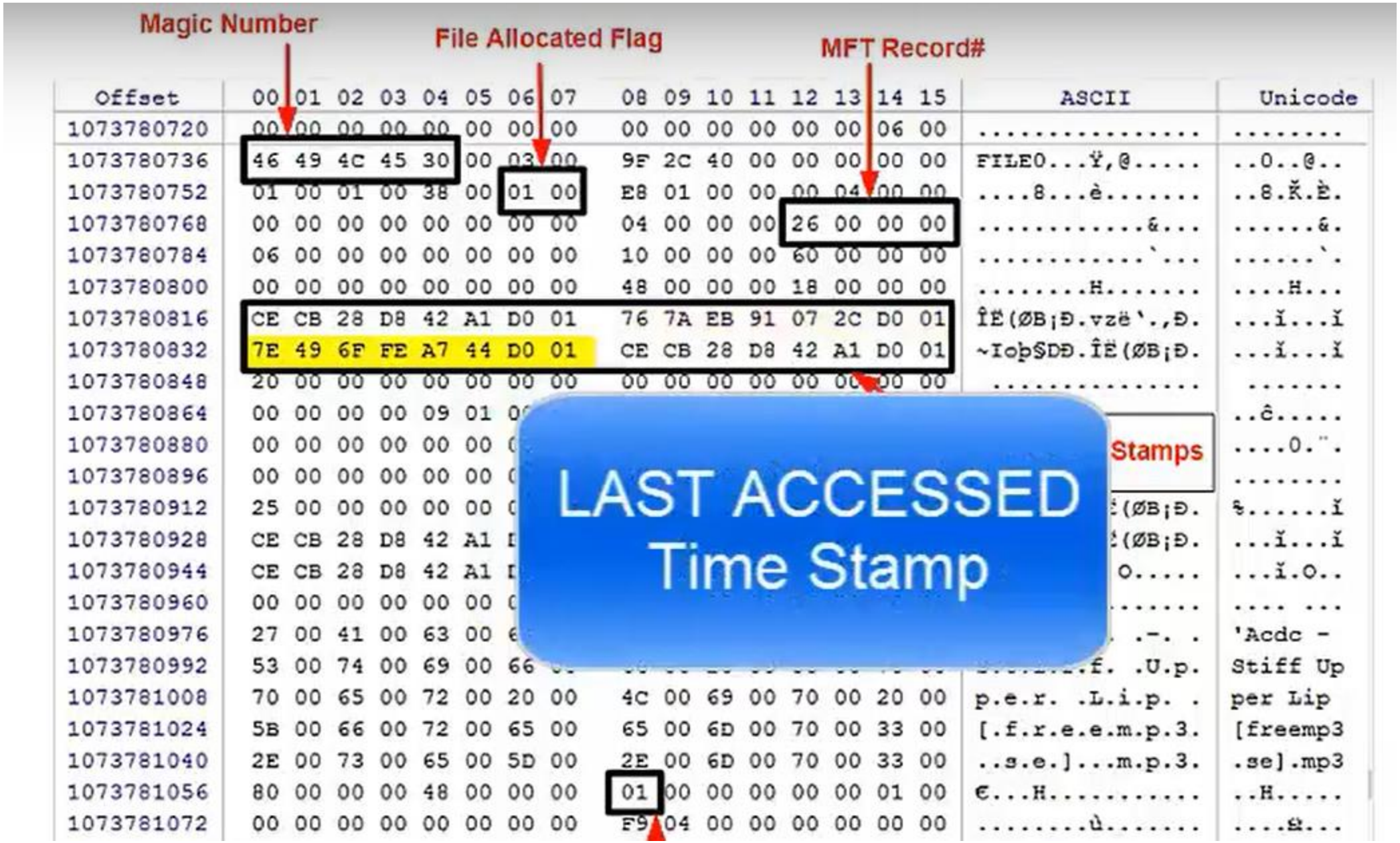


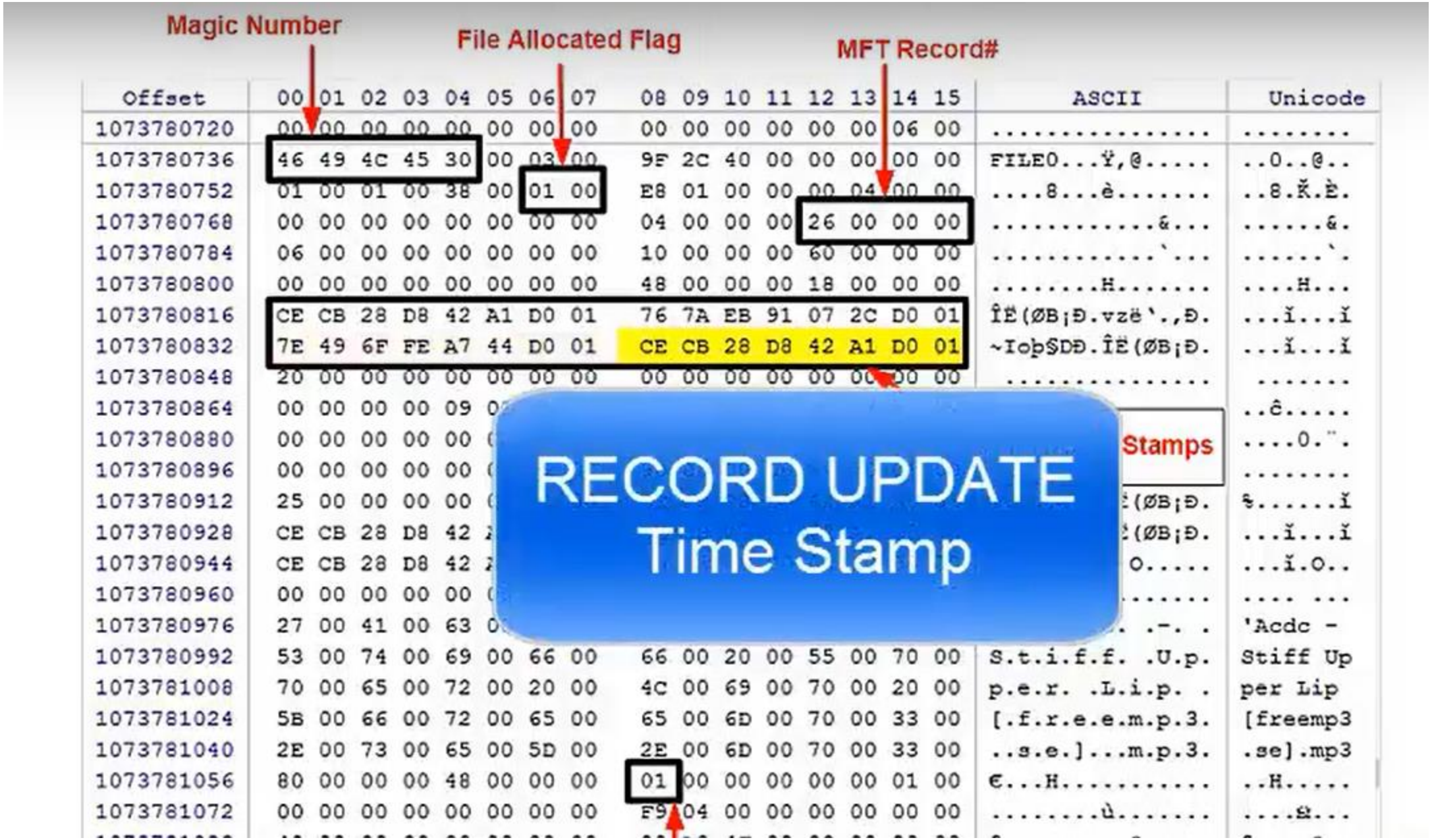
Offset	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII	Unicode
1073780720	00 00 00 00 00 00 00 00	00 00 00 00 00 00 06 00	.....	.....
1073780736	46 49 4C 45 30 00 03 00	9F 2C 40 00 00 00 00 00	FILE0...Ÿ,@.....	..0..@..
1073780752	01 00 01 00 38 00 01 00	E8 01 00 00 00 04 00 00	....8...è.....	..8.Ř.È.
1073780768	00 00 00 00 00 00 00 00	04 00 00 00 26 00 00 00	............&...	......&.
1073780784	06 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	............`...	......`.
1073780800	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	........H.....	....H...
1073780816	CE CB 28 D8 42 A1 D0 01	76 7A EB 91 07 2C D0 01	ÎË(ØB¡Ð.vzë'.,Ð.	...ĭ...ĭ
1073780832	7E 49 6F FE A7 44 D0 01	CE CB 28 D8 42 A1 D0 01	~Ioþ§DÐ.ÎË(ØB¡Ð.	...ĭ...ĭ
1073780848	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....	.....
1073780864	00 00 00 00 09 01 00 00	00 00 00 00 00 00 00 00	..ĉ.....	
1073780880	00 00 00 00 00 00 00 00	30 00 00 00 A8 00 00 00	....0.¨.	
1073780896	00 00 00 00 00 00 02 00	90 00 00 00 18 00 01 00	.....	
1073780912	25 00 00 00 00 00 01 00	CE CB 28 D8 42 A1 D0 01	%.....ÎË(ØB¡Ð.	%.....ĭ
1073780928	CE CB 28 D8 42 A1 D0 01	CE CB 28 D8 42 A1 D0 01	ÎË(ØB¡Ð.ÎË(ØB¡Ð.	...ĭ...ĭ
1073780944	CE CB 28 D8 42 A1 D0 01	00 A0 4F 00 00 00 00 00	ÎË(ØB¡Ð.. O.....	...ĭ.O..
1073780960	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	....	....
1073780976	27 00 41 00 63 00 64 00	63 00 20 00 2D 00 20 00	'.A.c.d.c. .-. .	'Acdc -
1073780992	53 00 74 00 69 00 66 00	66 00 20 00 55 00 70 00	S.t.i.f.f. .U.p.	Stiff Up
1073781008	70 00 65 00 72 00 20 00	4C 00 69 00 70 00 20 00	p.e.r. .L.i.p. .	per Lip
1073781024	5B 00 66 00 72 00 65 00	65 00 6D 00 70 00 33 00	[.f.r.e.e.m.p.3.	[freemp3
1073781040	2E 00 73 00 65 00 5D 00	2E 00 6D 00 70 00 33 00	..s.e.]...m.p.3.	.se].mp3
1073781056	80 00 00 00 48 00 00 00	01 00 00 00 00 00 01 00	€...H.....	..H.....
1073781072	00 00 00 00 00 00 00 00	F9 04 00 00 00 00 00 00	.....ù.....	....ù...



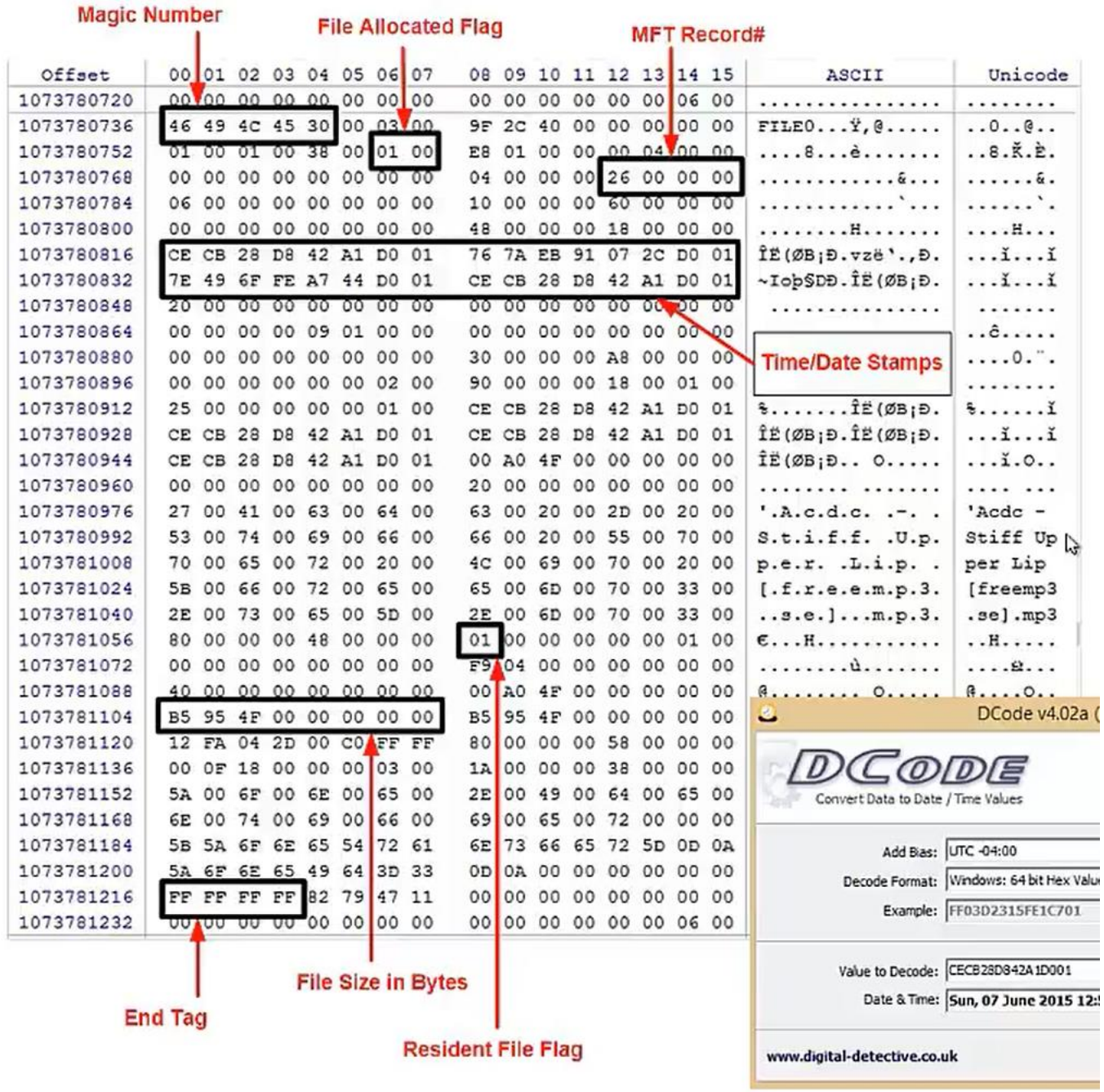
ENG ALI BANI BAKAR 0778642376


Magic Number
File Allocated Flag
MFT Record#
Offset 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 ASCII Unicode
1073780720 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 ....
1073780736 46 49 4C 45 30 00 03 00 9F 2C 40 00 00 00 00 00 FILE0...Ÿ,@..... ..0..@..
1073780752 01 00 01 00 38 00 01 00 E8 01 00 00 00 04 00 00 ....8...è..... ..8.Ǩ.È.
1073780768 00 00 00 00 00 00 00 00 04 00 00 00 26 00 00 00 ....&.
1073780784 06 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00 ....`.
1073780800 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00 ....H...
1073780816 CE CB 28 D8 42 A1 D0 01 76 7A EB 91 07 2C D0 01 ÎË(ØB¡Ð.vzë'.,Ð. ...ǐ...ǐ
1073780832 7E 49 6F FE A7 44 D0 01 CE CB 28 D8 42 A1 D0 01 ~Ioþ§DÐ.ÎË(ØB¡Ð. ...ǐ...ǐ
1073780848 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
1073780864 00 00 00 00 09 0 ..ĉ.....
1073780880 00 00 00 00 00 0 ....0.¨.
1073780896 00 00 00 00 00 0 .....
1073780912 25 00 00 00 00 0 %.....ǐ
1073780928 CE CB 28 D8 42 A ...ǐ...ǐ
1073780944 CE CB 28 D8 42 A ...ǐ.O..
1073780960 00 00 00 00 00 0 ....
1073780976 27 00 41 00 63 00 'Acdc -
1073780992 53 00 74 00 69 00 66 00 66 00 20 00 55 00 70 00 S.t.i.f.f. .U.p. Stiff Up
1073781008 70 00 65 00 72 00 20 00 4C 00 69 00 70 00 20 00 p.e.r. .L.i.p. . per Lip
1073781024 5B 00 66 00 72 00 65 00 65 00 6D 00 70 00 33 00 [.f.r.e.e.m.p.3. [freemp3
1073781040 2E 00 73 00 65 00 5D 00 2E 00 6D 00 70 00 33 00 ..s.e.]...m.p.3. .se].mp3
1073781056 80 00 00 00 48 00 00 00 01 00 00 00 00 00 01 00 €...H..... ..H.....
1073781072 00 00 00 00 00 00 00 00 F9 04 00 00 00 00 00 00 .....ù..... ....ø...
Stamps
LAST MODIFIED
Time Stamp


Magic Number
File Allocated Flag
MFT Record#
Offset
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
ASCII
Unicode
1073780720 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 ....
1073780736 46 49 4C 45 30 00 03 00 9F 2C 40 00 00 00 00 00 FILE0...Ÿ,@..... ..0..@..
1073780752 01 00 01 00 38 00 01 00 E8 01 00 00 00 04 00 00 ....8...è..... ..8.Ř.È.
1073780768 00 00 00 00 00 00 00 00 04 00 00 00 26 00 00 00 ....&... ......&.
1073780784 06 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00 ....`... ......`.
1073780800 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00 ....H....... ....H...
1073780816 CE CB 28 D8 42 A1 D0 01 76 7A EB 91 07 2C D0 01 ÎË(ØB¡Ð.vzë'.,Ð. ...ĭ...ĭ
1073780832 7E 49 6F FE A7 44 D0 01 CE CB 28 D8 42 A1 D0 01 ~Ioþ§DÐ.ÎË(ØB¡Ð. ...ĭ...ĭ
1073780848 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
1073780864 00 00 00 00 09 01 0 ..ĉ.....
1073780880 00 00 00 00 00 00 0 ....0.¨.
1073780896 00 00 00 00 00 00 0 ....
1073780912 25 00 00 00 00 00 0 %.....ĭ
1073780928 CE CB 28 D8 42 A1 D (ØB¡Ð. ...ĭ...ĭ
1073780944 CE CB 28 D8 42 A1 D O..... ...ĭ.O..
1073780960 00 00 00 00 00 00 0 ....
1073780976 27 00 41 00 63 00 6 .-. . 'Acdc -
1073780992 53 00 74 00 69 00 66 S.t.i.f. .U.p. Stiff Up
1073781008 70 00 65 00 72 00 20 00 4C 00 69 00 70 00 20 00 p.e.r. .L.i.p. . per Lip
1073781024 5B 00 66 00 72 00 65 00 65 00 6D 00 70 00 33 00 [.f.r.e.e.m.p.3. [freemp3
1073781040 2E 00 73 00 65 00 5D 00 2E 00 6D 00 70 00 33 00 ..s.e.]...m.p.3. .se].mp3
1073781056 80 00 00 00 48 00 00 00 01 00 00 00 00 00 01 00 €...H.......... ..H.....
1073781072 00 00 00 00 00 00 00 00 F9 04 00 00 00 00 00 00 ....ù....... ....ą...
Stamps
LAST ACCESSED
Time Stamp

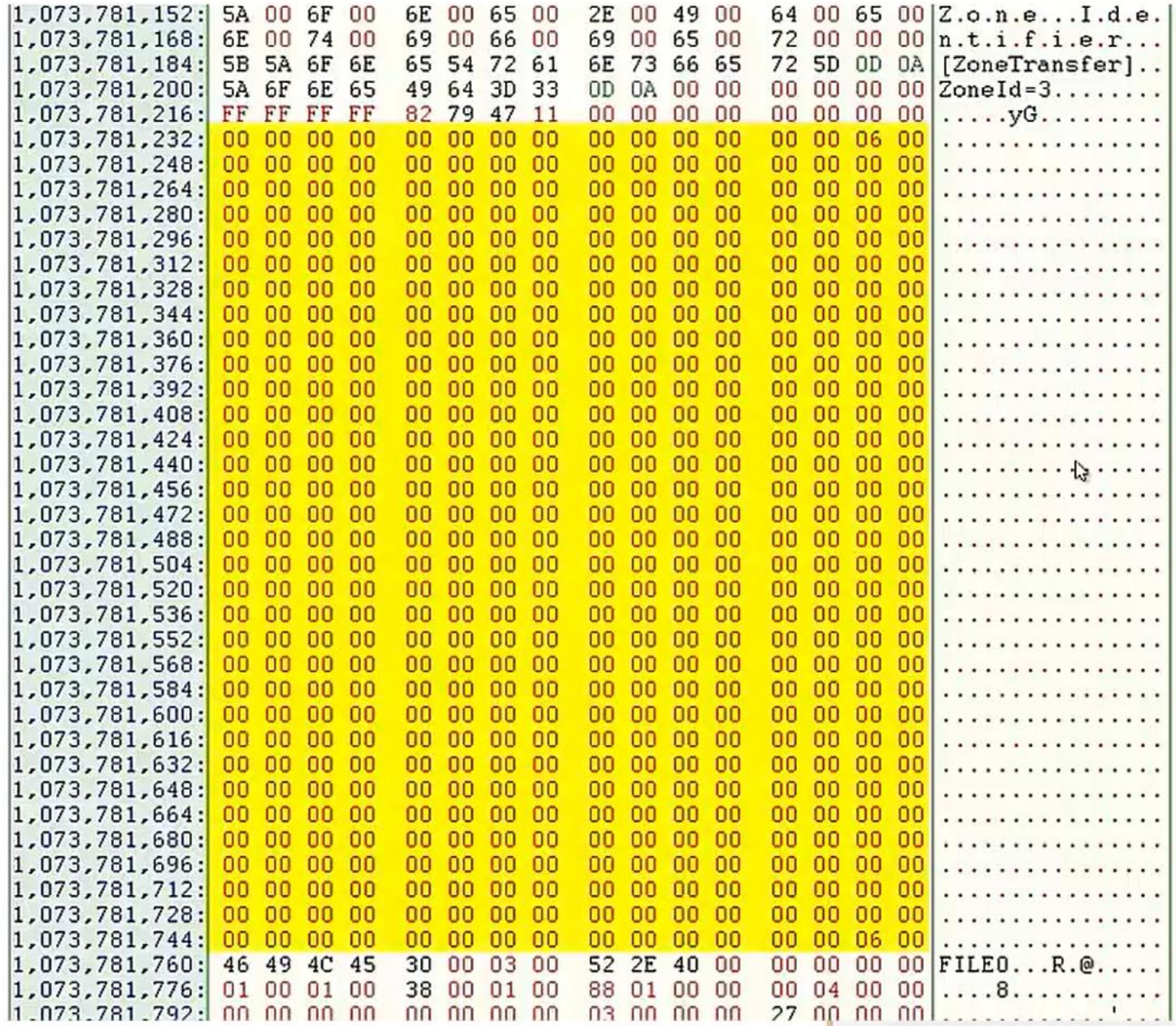

Magic Number
File Allocated Flag
MFT Record#
Offset 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 ASCII Unicode
1073780720 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 ....
1073780736 46 49 4C 45 30 00 03 00 9F 2C 40 00 00 00 00 00 FILE0...Ÿ,@..... ..0..@..
1073780752 01 00 01 00 38 00 01 00 E8 01 00 00 00 04 00 00 ....8...è..... ..8.Ř.È.
1073780768 00 00 00 00 00 00 00 00 04 00 00 00 26 00 00 00 ....&.
1073780784 06 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00 ....`.
1073780800 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00 ....H...
1073780816 CE CB 28 D8 42 A1 D0 01 76 7A EB 91 07 2C D0 01 ÎË(ØB¡Ð.vzë'.,Ð. ...ĭ...ĭ
1073780832 7E 49 6F FE A7 44 D0 01 CE CB 28 D8 42 A1 D0 01 ~Ioþ§DÐ.ÎË(ØB¡Ð. ...ĭ...ĭ
1073780848 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
1073780864 00 00 00 00 09 0 ..ĉ.....
1073780880 00 00 00 00 00 ....0.¨.
1073780896 00 00 00 00 00 .....
1073780912 25 00 00 00 00 %.....ĭ
1073780928 CE CB 28 D8 42 ...ĭ...ĭ
1073780944 CE CB 28 D8 42 ...ĭ.O..
1073780960 00 00 00 00 00 ....
1073780976 27 00 41 00 63 0 'Acdc -
1073780992 53 00 74 00 69 00 66 00 66 00 20 00 55 00 70 00 S.t.i.f.f. .U.p. Stiff Up
1073781008 70 00 65 00 72 00 20 00 4C 00 69 00 70 00 20 00 p.e.r. .L.i.p. . per Lip
1073781024 5B 00 66 00 72 00 65 00 65 00 6D 00 70 00 33 00 [.f.r.e.e.m.p.3. [freemp3
1073781040 2E 00 73 00 65 00 5D 00 2E 00 6D 00 70 00 33 00 ..s.e.]...m.p.3. .se].mp3
1073781056 80 00 00 00 48 00 00 00 01 00 00 00 00 00 01 00 €...H..... ..H.....
1073781072 00 00 00 00 00 00 00 00 F9 04 00 00 00 00 00 00 .....ù..... ....ø...
Stamps
RECORD UPDATE
Time Stamp

$MFT Record File

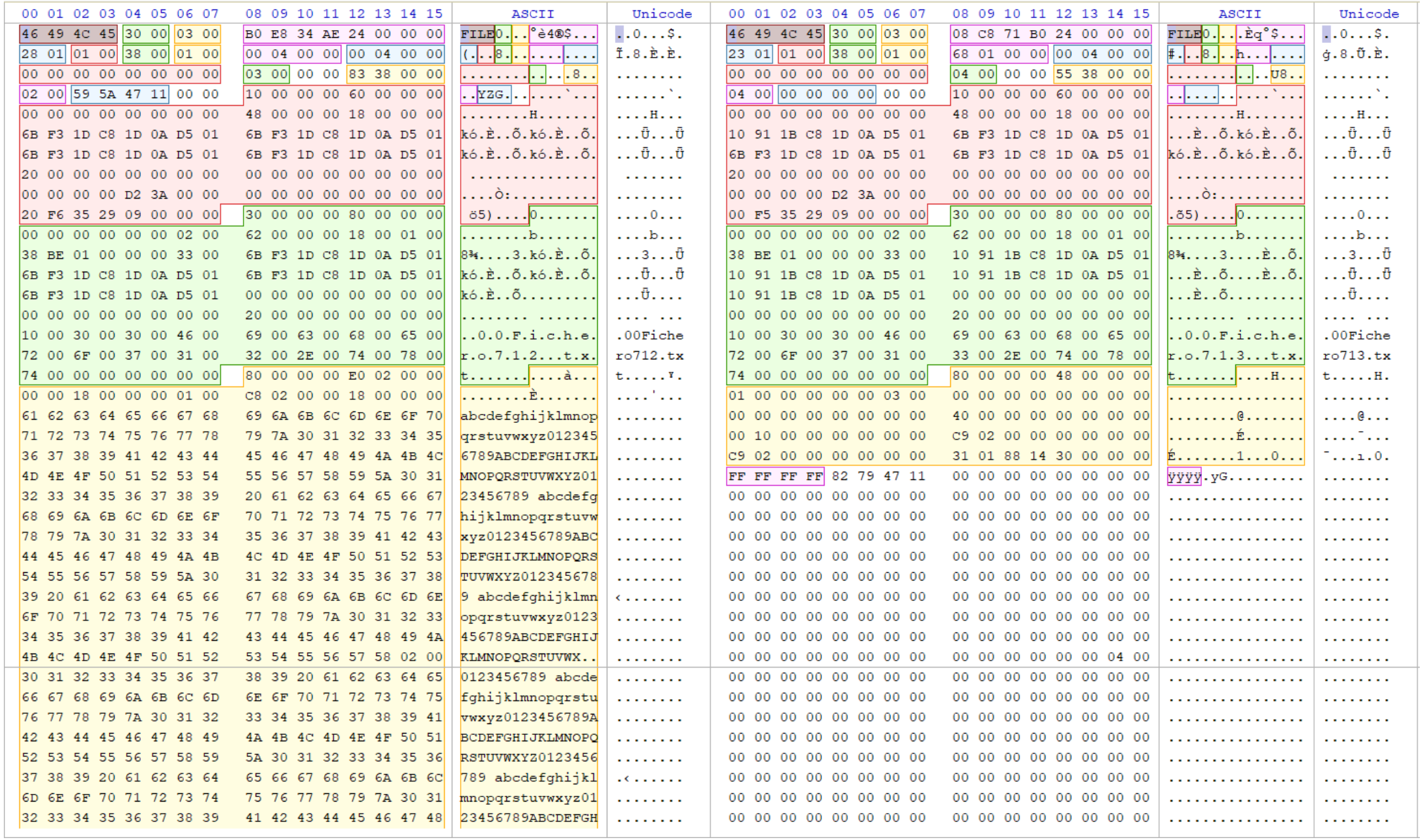


Offset	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII	Unicode
1073780720	00 00 00 00 00 00 00 00	00 00 00 00 00 00 06 00	.....	.....
1073780736	46 49 4C 45 30 00 03 00	9F 2C 40 00 00 00 00 00	FILE0...Ÿ,@.....	..0..@..
1073780752	01 00 01 00 38 00 01 00	E8 01 00 00 00 04 00 00	....8...è.....	..8.Ǩ.È.
1073780768	00 00 00 00 00 00 00 00	04 00 00 00 26 00 00 00	............&...	......&.
1073780784	06 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	............`...	......`.
1073780800	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	........H.....	....H...
1073780816	CE CB 28 D8 42 A1 D0 01	76 7A EB 91 07 2C D0 01	ÎË(ØB¡Ð.vzë'.,Ð.	...ĭ...ĭ
1073780832	7E 49 6F FE A7 44 D0 01	CE CB 28 D8 42 A1 D0 01	~Ioþ§DÐ.ÎË(ØB¡Ð.	...ĭ...ĭ
1073780848	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....	.....
1073780864	00 00 00 00 09 01 00 00	00 00 00 00 00 00 00 00	..ĉ.....	
1073780880	00 00 00 00 00 00 00 00	30 00 00 00 A8 00 00 00	....0.¨.	
1073780896	00 00 00 00 00 00 02 00	90 00 00 00 18 00 01 00	.....	
1073780912	25 00 00 00 00 00 01 00	CE CB 28 D8 42 A1 D0 01	%.....ÎË(ØB¡Ð.	%.....ĭ
1073780928	CE CB 28 D8 42 A1 D0 01	CE CB 28 D8 42 A1 D0 01	ÎË(ØB¡Ð.ÎË(ØB¡Ð.	...ĭ...ĭ
1073780944	CE CB 28 D8 42 A1 D0 01	00 A0 4F 00 00 00 00 00	ÎË(ØB¡Ð.. O.....	...ĭ.O..
1073780960	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	....	....
1073780976	27 00 41 00 63 00 64 00	63 00 20 00 2D 00 20 00	'.A.c.d.c. .-. .	'Acdc -
1073780992	53 00 74 00 69 00 66 00	66 00 20 00 55 00 70 00	S.t.i.f.f. .U.p.	Stiff Up
1073781008	70 00 65 00 72 00 20 00	4C 00 69 00 70 00 20 00	p.e.r. .L.i.p. .	per Lip
1073781024	5B 00 66 00 72 00 65 00	65 00 6D 00 70 00 33 00	[.f.r.e.e.m.p.3.	[freemp3
1073781040	2E 00 73 00 65 00 5D 00	2E 00 6D 00 70 00 33 00	..s.e.]...m.p.3.	.se].mp3
1073781056	80 00 00 00 48 00 00 00	01 00 00 00 00 00 01 00	€...H.....	..H.....
1073781072	00 00 00 00 00 00 00 00	F9 04 00 00 00 00 00 00	........ù.....	....ù...
1073781088	40 00 00 00 00 00 00 00	00 A0 4F 00 00 00 00 00	@..... O.....	@....O..
1073781104	B5 95 4F 00 00 00 00 00	B5 95 4F 00 00 00 00 00	µ•O.....µ•O.....	µ•O.....µ•O.....
1073781120	12 FA 04 2D 00 C0 FF FF	80 00 00 00 58 00 00 00	.ú.-.ÀÿÿX...	
1073781136	00 0F 18 00 00 00 03 00	1A 00 00 00 38 00 00 00	.....	
1073781152	5A 00 6F 00 6E 00 65 00	2E 00 49 00 64 00 65 00	Z.o.n.e...I.d.e.	
1073781168	6E 00 74 00 69 00 66 00	69 00 65 00 72 00 00 00	n.t.i.f.i.e.r...	
1073781184	5B 5A 6F 6E 65 54 72 61	6E 73 66 65 72 5D 0D 0A	[ZoneTransfer]...	
1073781200	5A 6F 6E 65 49 64 3D 33	0D 0A 00 00 00 00 00 00	ZoneId=3.....	
1073781216	FF FF FF FF 82 79 47 11	00 00 00 00 00 00 00 00	....‚yG.....	
1073781232	00 00 00 00 00 00 00 00	00 00 00 00 00 00 06 00	.....	

Lower 512 Bytes of $MFT Record



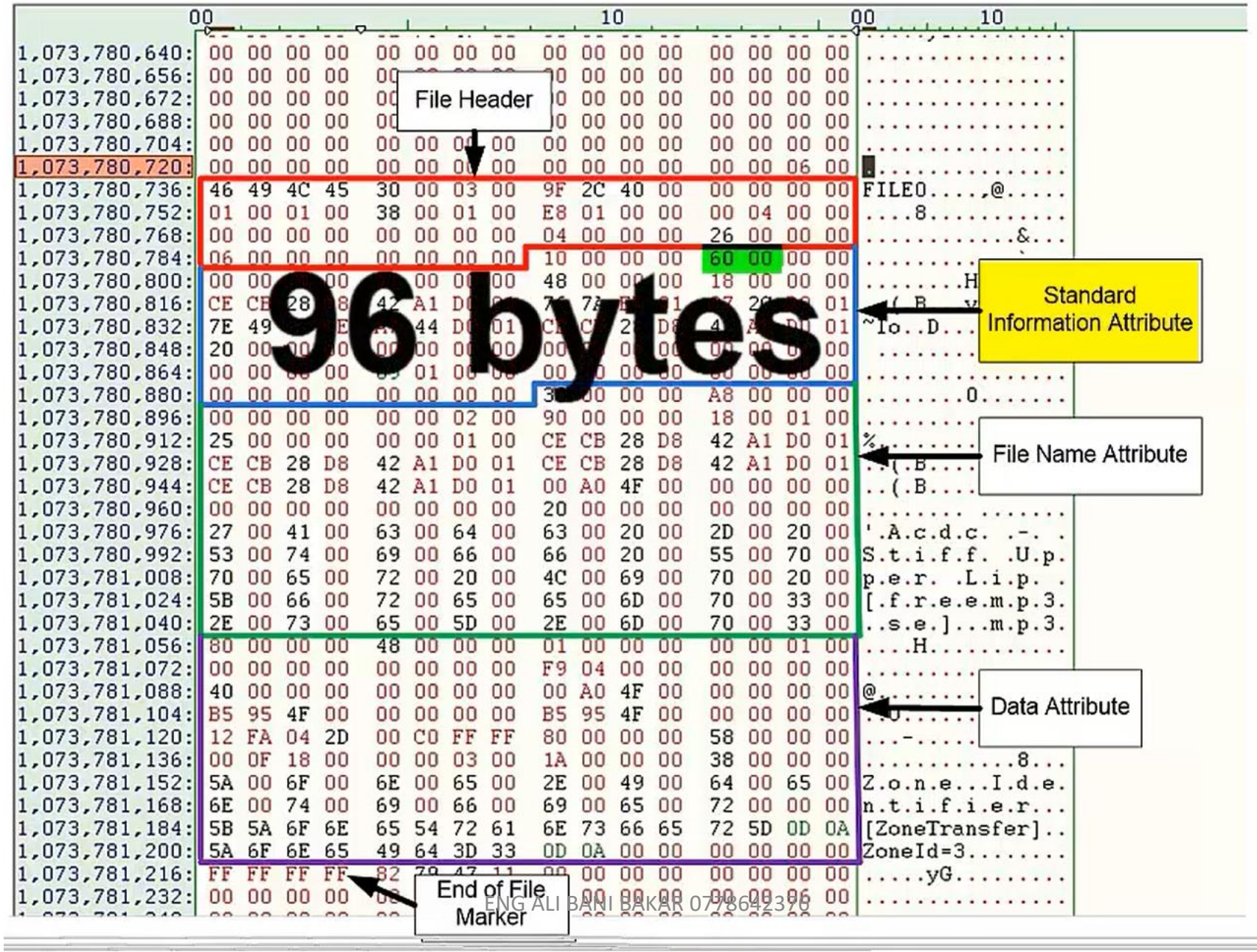
```
1,073,781,152: 5A 00 6F 00  6E 00 65 00  2E 00 49 00  64 00 65 00 Z.o.n.e...I.d.e.
1,073,781,168: 6E 00 74 00  69 00 66 00  69 00 65 00  72 00 00 00 n.t.i.f.i.e.r...
1,073,781,184: 5B 5A 6F 6E  65 54 72 61  6E 73 66 65  72 5D 0D 0A [ZoneTransfer]..
1,073,781,200: 5A 6F 6E 65  49 64 3D 33  0D 0A 00 00  00 00 00 00 ZoneId=3........
1,073,781,216: FF FF FF FF  82 79 47 11  00 00 00 00  00 00 00 00 .....yG.........
1,073,781,232: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 06 00 ................
1,073,781,248: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,264: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,280: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,296: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,312: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,328: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,344: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,360: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,376: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,392: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,408: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,424: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,440: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,456: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,472: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,488: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,504: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,520: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,536: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,552: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,568: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,584: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,600: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,616: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,632: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,648: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,664: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,680: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,696: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,712: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,728: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 ................
1,073,781,744: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 06 00 ................
1,073,781,760: 46 49 4C 45  30 00 03 00  52 2E 40 00  00 00 00 00 FILE0...R.@.....
1,073,781,776: 01 00 01 00  38 00 01 00  88 01 00 00  00 04 00 00 ....8...........
1,073,781,792: 00 00 00 00  00 00 00 00  03 00 00 00  27 00 00 00 ............'...
```



00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII	Unicode	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII	Unicode
46 49 4C 45 30 00 03 00	B0 E8 34 AE 24 00 00 00	FILE0...°è4®$...	.0...$.	46 49 4C 45 30 00 03 00	08 C8 71 B0 24 00 00 00	FILE0...Èq°$...	.0...$.
28 01 01 00 38 00 01 00	00 04 00 00 00 04 00 00	(...8..........	Ï.8.È.È.	23 01 01 00 38 00 01 00	68 01 00 00 00 04 00 00	#...8...h.....	ģ.8.Ũ.È.
00 00 00 00 00 00 00 00	03 00 00 00 83 38 00 00	..............8..	....	00 00 00 00 00 00 00 00	04 00 00 00 55 38 00 00	............U8..	....
02 00 59 5A 47 11 00 00	10 00 00 00 60 00 00 00	..YZG.......`...	......`.	04 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	..........`...	......`.
00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	........H.......	....H...	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	........H.......	....H...
6B F3 1D C8 1D 0A D5 01	6B F3 1D C8 1D 0A D5 01	kó.È..Õ.kó.È..Õ.	...Ũ...Ũ	10 91 1B C8 1D 0A D5 01	6B F3 1D C8 1D 0A D5 01	...È..Õ.kó.È..Õ.	...Ũ...Ũ
6B F3 1D C8 1D 0A D5 01	6B F3 1D C8 1D 0A D5 01	kó.È..Õ.kó.È..Õ.	...Ũ...Ũ	6B F3 1D C8 1D 0A D5 01	6B F3 1D C8 1D 0A D5 01	kó.È..Õ.kó.È..Õ.	...Ũ...Ũ
20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
00 00 00 00 D2 3A 00 00	00 00 00 00 00 00 00 00	....Ò:..........	....	00 00 00 00 D2 3A 00 00	00 00 00 00 00 00 00 00	....Ò:..........	....
20 F6 35 29 09 00 00 00	30 00 00 00 80 00 00 00	ö5).....0.......	....0...	00 F5 35 29 09 00 00 00	30 00 00 00 80 00 00 00	.õ5).....0.......	....0...
00 00 00 00 00 00 02 00	62 00 00 00 18 00 01 00	........b.......	....b...	00 00 00 00 00 00 02 00	62 00 00 00 18 00 01 00	........b.......	....b...
38 BE 01 00 00 00 33 00	6B F3 1D C8 1D 0A D5 01	8¾....3.kó.È..Õ.	...3...Ũ	38 BE 01 00 00 00 33 00	10 91 1B C8 1D 0A D5 01	8¾....3....È..Õ.	...3...Ũ
6B F3 1D C8 1D 0A D5 01	6B F3 1D C8 1D 0A D5 01	kó.È..Õ.kó.È..Õ.	...Ũ...Ũ	10 91 1B C8 1D 0A D5 01	10 91 1B C8 1D 0A D5 01	...È..Õ....È..Õ.	...Ũ...Ũ
6B F3 1D C8 1D 0A D5 01	00 00 00 00 00 00 00 00	kó.È..Õ.........	...Ũ....	10 91 1B C8 1D 0A D5 01	00 00 00 00 00 00 00 00	...È..Õ.........	...Ũ....
00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	....	....	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	....	....
10 00 30 00 30 00 46 00	69 00 63 00 68 00 65 00	..0.0.F.i.c.h.e.	.00Fiche	10 00 30 00 30 00 46 00	69 00 63 00 68 00 65 00	..0.0.F.i.c.h.e.	.00Fiche
72 00 6F 00 37 00 31 00	32 00 2E 00 74 00 78 00	r.o.7.1.2...t.x.	ro712.tx	72 00 6F 00 37 00 31 00	33 00 2E 00 74 00 78 00	r.o.7.1.3...t.x.	ro713.tx
74 00 00 00 00 00 00 00	80 00 00 00 E0 02 00 00	t...........à...	t.....ɣ.	74 00 00 00 00 00 00 00	80 00 00 00 48 00 00 00	t...........H...	t.....H.
00 00 18 00 00 00 01 00	C8 02 00 00 18 00 00 00	........È.......	....'...	01 00 00 00 00 00 03 00	00 00 00 00 00 00 00 00	....	....
61 62 63 64 65 66 67 68	69 6A 6B 6C 6D 6E 6F 70	abcdefghijklmnop	....	00 00 00 00 00 00 00 00	40 00 00 00 00 00 00 00	........@.......	....@...
71 72 73 74 75 76 77 78	79 7A 30 31 32 33 34 35	qrstuvwxyz012345	....	00 10 00 00 00 00 00 00	C9 02 00 00 00 00 00 00	........É.......	....¯...
36 37 38 39 41 42 43 44	45 46 47 48 49 4A 4B 4C	6789ABCDEFGHIJKL	....	C9 02 00 00 00 00 00 00	31 01 88 14 30 00 00 00	É.......1...0...	¯...ı.0.
4D 4E 4F 50 51 52 53 54	55 56 57 58 59 5A 30 31	MNOPQRSTUVWXYZ01	....	FF FF FF FF 82 79 47 11	00 00 00 00 00 00 00 00	ÿÿÿÿ.yG.........	....
32 33 34 35 36 37 38 39	20 61 62 63 64 65 66 67	23456789 abcdefg	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
68 69 6A 6B 6C 6D 6E 6F	70 71 72 73 74 75 76 77	hijklmnopqrstuvw	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
78 79 7A 30 31 32 33 34	35 36 37 38 39 41 42 43	xyz0123456789ABC	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
44 45 46 47 48 49 4A 4B	4C 4D 4E 4F 50 51 52 53	DEFGHIJKLMNOPQRS	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
54 55 56 57 58 59 5A 30	31 32 33 34 35 36 37 38	TUVWXYZ012345678	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
39 20 61 62 63 64 65 66	67 68 69 6A 6B 6C 6D 6E	9 abcdefghijklmn	‹.......	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
6F 70 71 72 73 74 75 76	77 78 79 7A 30 31 32 33	opqrstuvwxyz0123	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
34 35 36 37 38 39 41 42	43 44 45 46 47 48 49 4A	456789ABCDEFGHIJ	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
4B 4C 4D 4E 4F 50 51 52	53 54 55 56 57 58 02 00	KLMNOPQRSTUVWX..	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 04 00	....	....
30 31 32 33 34 35 36 37	38 39 20 61 62 63 64 65	0123456789 abcde	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
66 67 68 69 6A 6B 6C 6D	6E 6F 70 71 72 73 74 75	fghijklmnopqrstu	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
76 77 78 79 7A 30 31 32	33 34 35 36 37 38 39 41	vwxyz0123456789A	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
42 43 44 45 46 47 48 49	4A 4B 4C 4D 4E 4F 50 51	BCDEFGHIJKLMNOPQ	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
52 53 54 55 56 57 58 59	5A 30 31 32 33 34 35 36	RSTUVWXYZ0123456	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
37 38 39 20 61 62 63 64	65 66 67 68 69 6A 6B 6C	789 abcdefghijkl	.‹......	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
6D 6E 6F 70 71 72 73 74	75 76 77 78 79 7A 30 31	mnopqrstuvwxyz01	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
32 33 34 35 36 37 38 39	41 42 43 44 45 46 47 48	23456789ABCDEFGH	....	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....

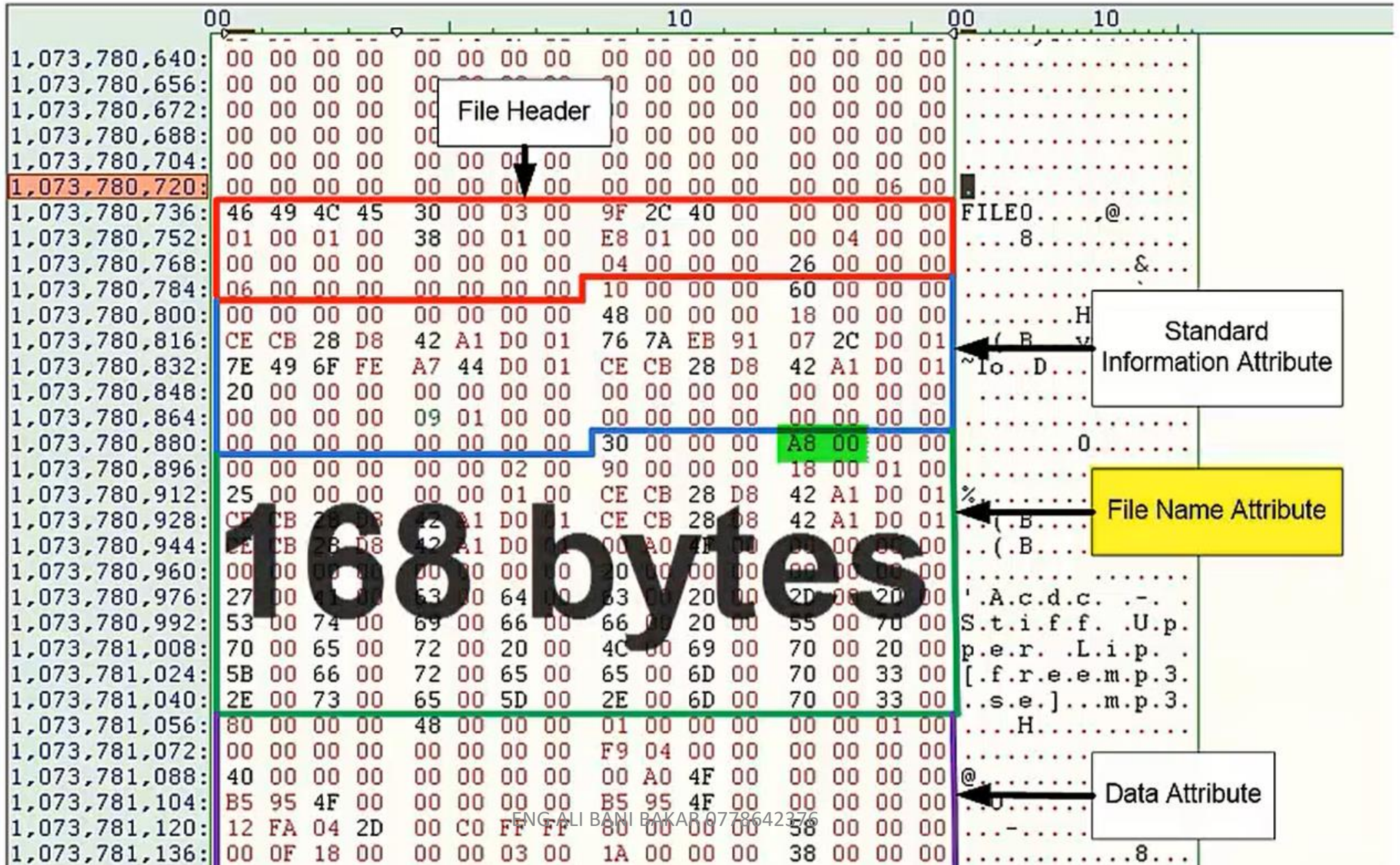
ENG ALI BANI BAKAR 0778642376

Structure of an $MFT Record



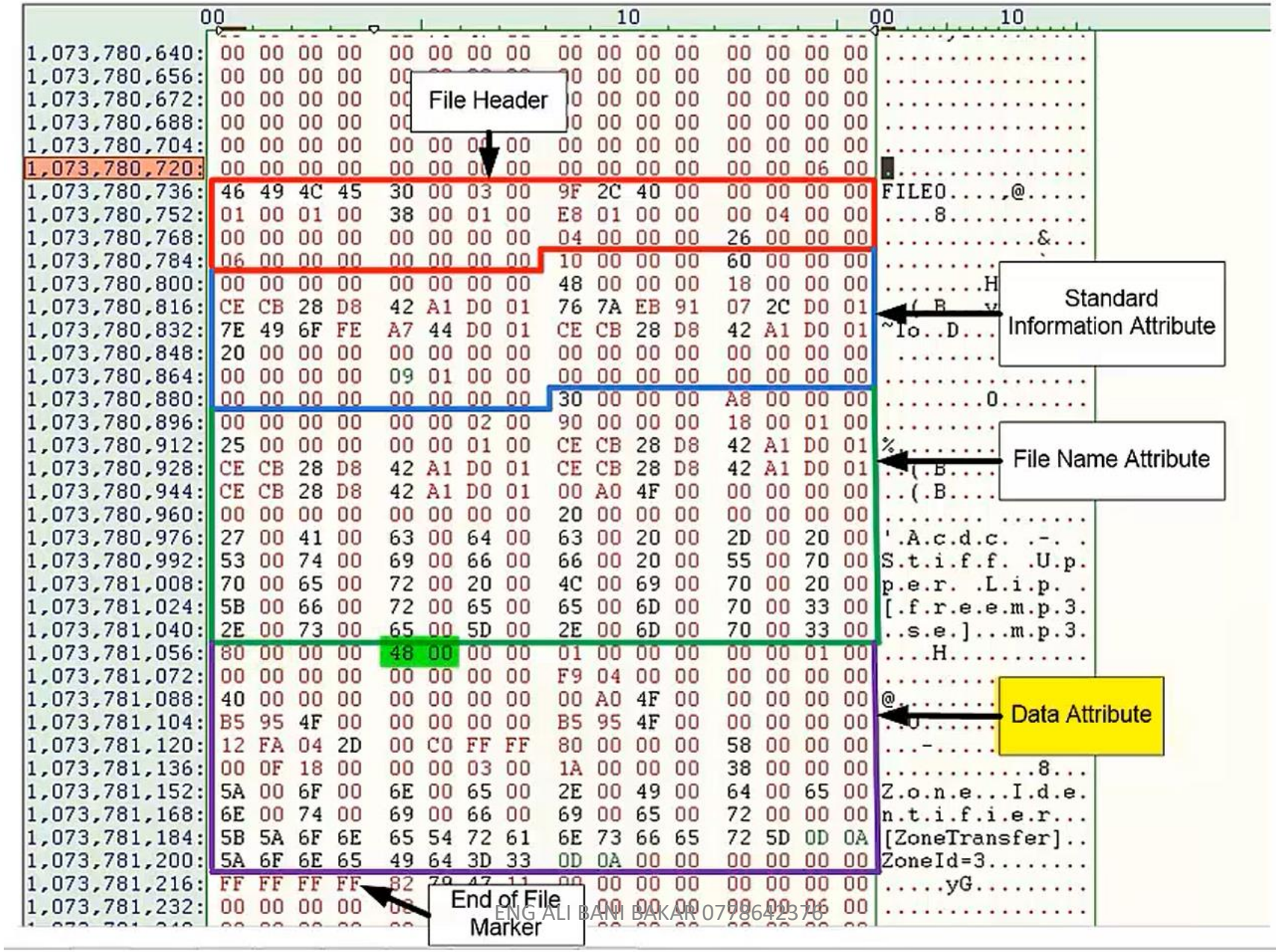
ENG ALI BANI BAKAR 07786423

Structure of an $MFT Record

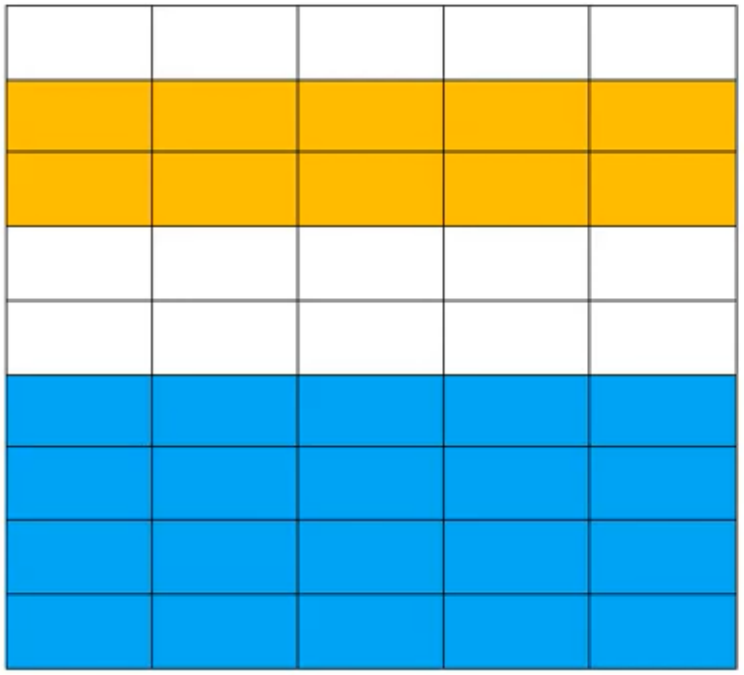


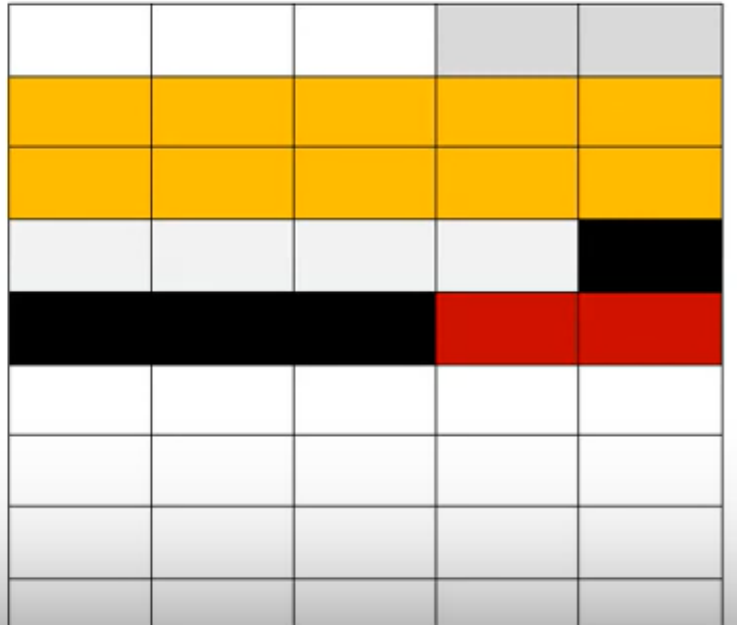
ENG ALI BANI BAKAR 0778642376

Structure of an $MFT Record



ENG ALI BANI BAKAR 07786423



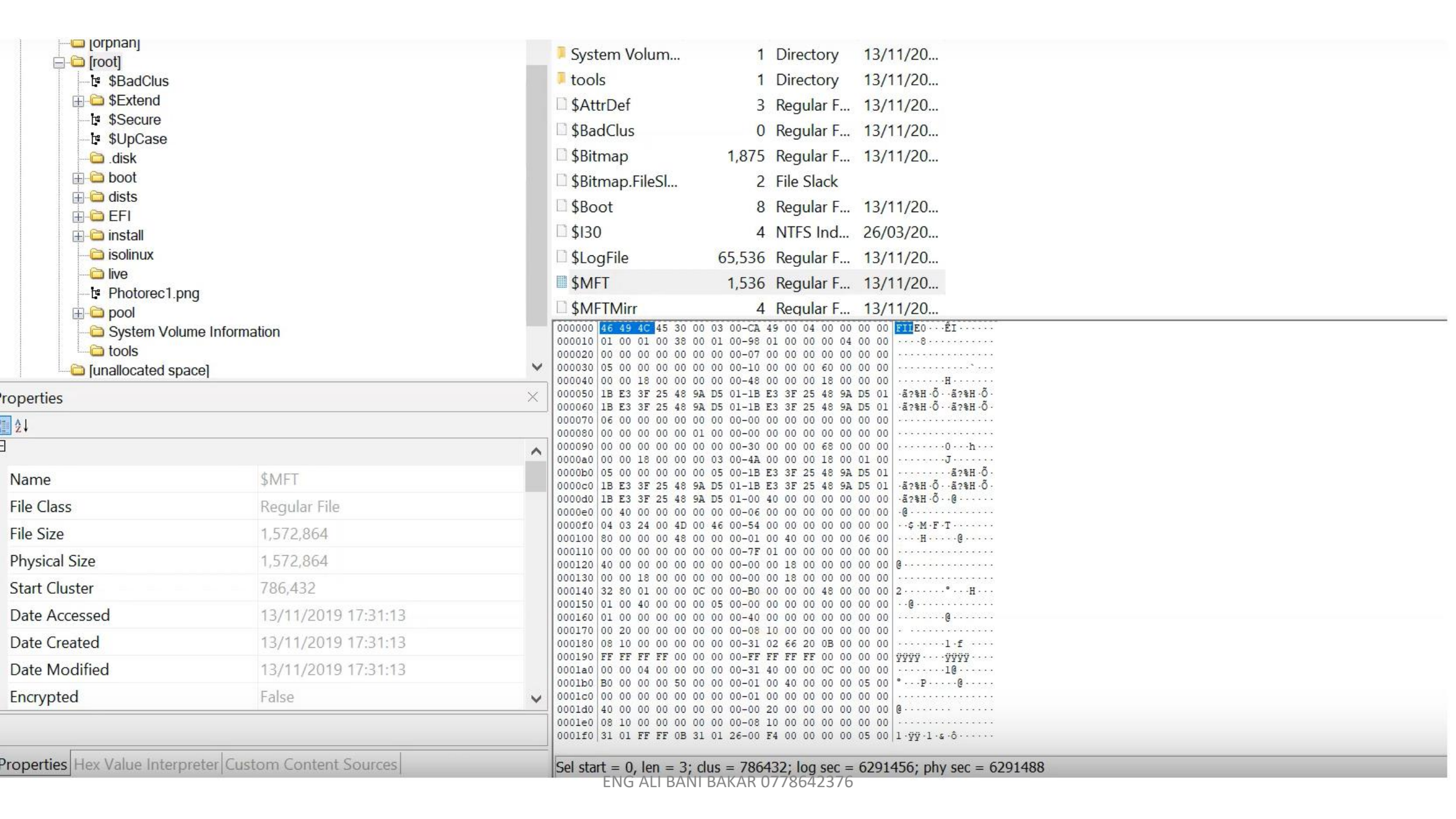


ENG ALI BANI BAKAR 0778642376

ملف ($MFT)

- حاوية تحتوي على سجلات (Records) متتالية
- لكل ملف ومجلد داخل القسم (NTFS Partition) سجل خاص به
- كل سجل عبارة عن ١٠٢٤ بايت
- السجل يحتوي على بيانات هامة جدا للمحقق الرقمي (اسم الملف، حجم الملف، تاريخ ووقت إنشاء الملف والتعديل والوصول (MAC ....)
- كل سجل يبدأ (FILE)

Record #	Record size
0	1024 Bytes
1	1024 Bytes
2	1024 Bytes
3	1024 Bytes
4	1024 Bytes
5	1024 Bytes



ENG ALI BANI BAKAR 0778642376

Offset	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII	Unicode
027129422848	46 49 4C 45 30 00 03 00	04 5D 41 A3 00 00 00 00	FILE0...]A£....	..0.....
027129422864	06 00 01 00 38 00 01 00	F0 03 00 00 00 04 00 00	....8...ð.....	..8.ж.È.
027129422880	00 00 00 00 00 00 00 00	06 00 00 00 FD 5B 03 00	............ý[..	....
027129422896	54 00 0A 53 00 00 00 00	10 00 00 00 60 00 00 00	T..S.....`...	T.....`.
027129422912	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	........H.....	....H...
027129422928	86 D5 69 DA D9 9B D5 01	6A 2C 3D 10 DA 9B D5 01	.ÕiÚÙ.Õ.j,=.Ú.Õ.	...Ūķ..Ū
027129422944	6A 2C 3D 10 DA 9B D5 01	6A 2C 3D 10 DA 9B D5 01	j,=.Ú.Õ.j,=.Ú.Õ.	ķ..Ūķ..Ū
027129422960	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	....
027129422976	00 00 00 00 8E 07 00 00	00 00 00 00 00 00 00 00	....	....
027129422992	90 F5 3D 21 00 00 00 00	30 00 00 00 70 00 00 00	.õ=!....0...p...	....0.p.
027129423008	00 00 00 00 00 00 04 00	58 00 00 00 18 00 01 00	........X.....	....X...
027129423024	20 DF 01 00 00 00 03 00	86 D5 69 DA D9 9B D5 01	ß.....ÕiÚÙ.Õ.	.....Ū
027129423040	86 D5 69 DA D9 9B D5 01	86 D5 69 DA D9 9B D5 01	.ÕiÚÙ.Õ..ÕiÚÙ.Õ.	...Ū...Ū
027129423056	86 D5 69 DA D9 9B D5 01	00 00 00 00 00 00 00 00	.ÕiÚÙ.Õ.....	...Ū....
027129423072	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	....	....
027129423088	0B 03 41 00 54 00 41 00	54 00 4F 00 4F 00 4C 00	..A.T.A.T.O.O.L.	ĂTATOOL
027129423104	2E 00 74 00 78 00 74 00	40 00 00 00 28 00 00 00	..t.x.t.@...(...	.txt@.(.
027129423120	00 00 00 00 00 00 05 00	10 00 00 00 18 00 00 00	....	.....
027129423136	7F A0 40 66 C9 07 EA 11	B9 8C A0 A4 C5 7C 80 45	. @fÉ.ê.¹. ¤Å|.E	.....
027129423152	80 00 00 00 B8 02 00 00	00 00 18 00 00 00 01 00	....¸.....	..¥.....
027129423168	9B 02 00 00 18 00 00 00	68 64 70 61 72 6D 20 66	........hdparm f	ɢ.....
027129423184	6F 72 20 6C 69 6E 75 78	0D 0A 0D 0A 0D 0A 68 74	or linux......ht	.....
027129423200	74 70 73 3A 2F 2F 65 6E	2E 77 69 6B 69 70 65 64	tps://en.wikiped	.....
027129423216	69 61 2E 6F 72 67 2F 77	69 6B 69 2F 41 54 41 54	ia.org/wiki/ATAT	.....

ENG ALI BANI BAKAR 0778642376

أنواع سمات الملف (Attribute Types)

اسم سمة الملف Attribute Name	الرمز التعريفي لسمة الملف Attribute_ID
$STANDARD_INFOMATION	0x10 00 00 00
$ATTRIBUTE_LIST	0x20 00 00 00
$FILE_NAME	0x30 00 00 00
$OBJECT_ID	0x40 00 00 00
$SECURITY_DESCRIPTOR	0x50 00 00 00
$VOLUME_NAME	0x60 00 00 00
$VOLUME_INFORMATION	0x70 00 00 00
$DATA	0x80 00 00 00
$INDEX_ROOT	0x90 00 00 00
$INDEX_ALLOCATION	0xA0 00 00 00
$BITMAP	0xB0 00 00 00
$REPARSE_POINT	0xC0 00 00 00
$EA_INFORMATION	0xD0 00 00 00
$EA	0xE0 00 00 00
$LOGGED_UTILITY_STREAM	0x00 01 00 00

(Data RunList) in DATA Attribute

نفترض أن لدينا عدد (٤) ملفات على القرص الصلب كما في الشكل:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	26	25	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	56	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80

ملف الأحمر	بداية الجزء (رقم الكتلة) Cluster Number	عدد الكتل Clusters
	١	٣
	١٠	١
	١٤	٢
	٢٢	٦
	٦٥	٢
	٧٧	٣

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	26	25	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	56	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80

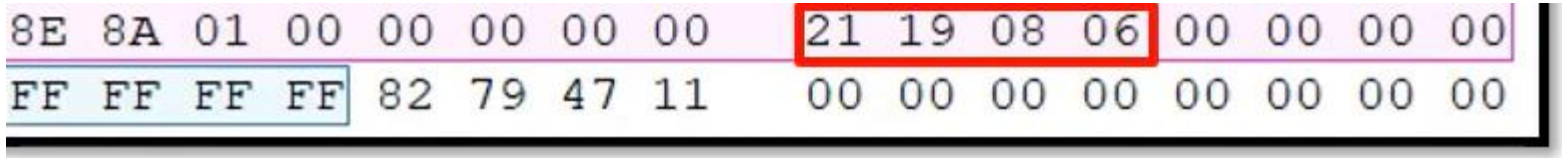
عدد الكتل Clusters	بداية الجزء (رقم الكتلة) Cluster Number	ملف الأخضر
٦	٤	
٣	١١	
٨	٣٧	
٦	٥٦	
٤	٧٣	

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	26	25	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	56	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80

عدد الكتل Clusters	بداية الجزء (رقم الكتلة) Cluster Number	الملف الأزرق
٦	١٦	
٤	٣٣	
١٠	٤٥	
١	٨٠	

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	26	25	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	56	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80

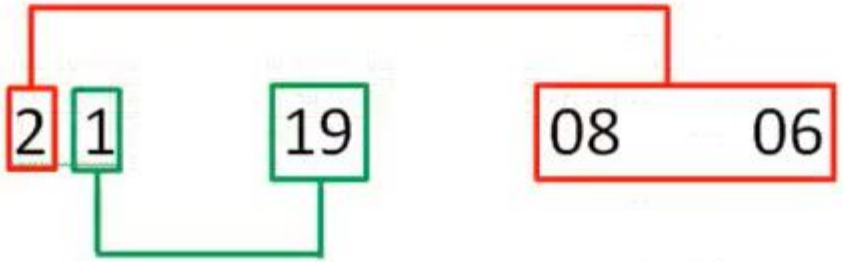
عدد الكتل Clusters	بداية الجزء (رقم الكتلة) Cluster Number	ملف الأصفر
٥	٢٨	
٤	٦١	
٦	٦٧	



البايت الأول يشر إلى عدد البايتات التي ستمثل موقع أول كتلة لمحتوى الملف

هنا نشاهد بأن البايت الثاني قيمته ٢ وعليه فإن قيمة البايت (0x0806) وبما أنها مكتوب بطريقة (Littile Endia) فإن القيمة الحقيقية هي (0x0608=1544) وسابقا قلنا بأن عدد القطاعات في الكتلة الواحدة هو ٨ قطاعات.

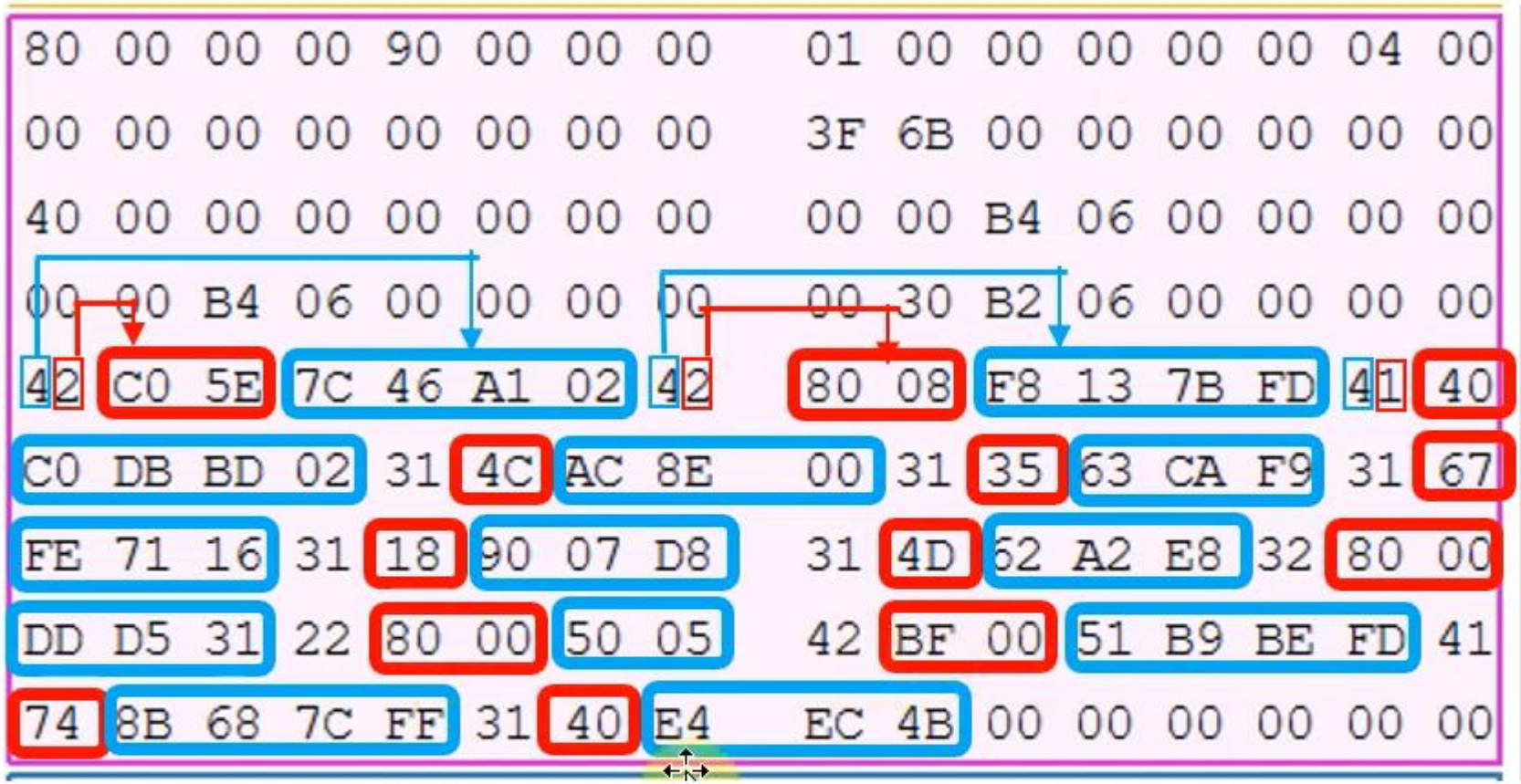
سدأ الملف فى القطاع رقم = ١٥٤٤ * ٨= ١٢٣٥٢



البايت الثاني يشر إلى عدد البايتات التي ستمثل عدد الكتل لمحتوى الملف

هنا نشاهد بأن البايت الثاني قيمته ١ وعليه نأخذ أول بايت يليه وهو يعتبر عدد الكتل للملف (0x19=25) إذا عدد ١٥ كتلة تمثل هذا الملف

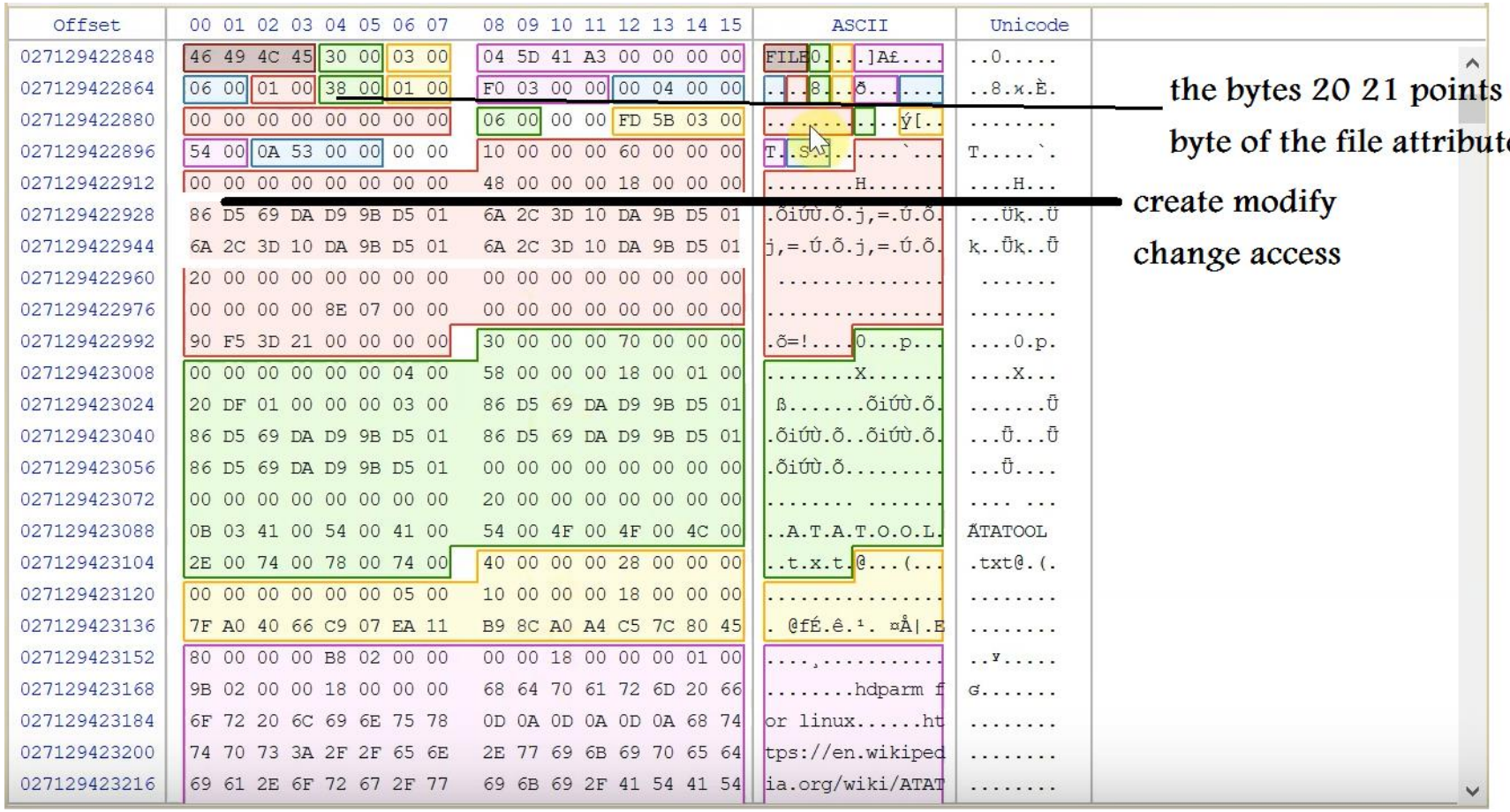
ENG ALI BANI BAKAR 0778642376



5E C0 + **08 80** + **40** + **4C** + **35** + **67** + **18** + **4D** + **00 80** +**00 80** + **00 BF** + **74** + **40** = **27456** Clusters

1 Cluster = 4096 Bytes => 27456*4096 = 112,459,776 Bytes = 107 MB

Dates



Offset	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII	Unicode
027129422848	46 49 4C 45 30 00 03 00	04 5D 41 A3 00 00 00 00	FILE0...]A£....	..0.....
027129422864	06 00 01 00 38 00 01 00	F0 03 00 00 00 04 00 00	....8...ð.....	..8.¤.È.
027129422880	00 00 00 00 00 00 00 00	06 00 00 00 FD 5B 03 00	........ý[..	....
027129422896	54 00 0A 53 00 00 00 00	10 00 00 00 60 00 00 00	T..S....`...	T.....`.
027129422912	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	........H.....	....H...
027129422928	86 D5 69 DA D9 9B D5 01	6A 2C 3D 10 DA 9B D5 01	.ÕiÚÙ.Õ.j,=.Ú.Õ.	...Ük..Ü
027129422944	6A 2C 3D 10 DA 9B D5 01	6A 2C 3D 10 DA 9B D5 01	j,=.Ú.Õ.j,=.Ú.Õ.	k..Ük..Ü
027129422960	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....	.....
027129422976	00 00 00 00 8E 07 00 00	00 00 00 00 00 00 00 00	....	.....
027129422992	90 F5 3D 21 00 00 00 00	30 00 00 00 70 00 00 00	.õ=!....0...p...	....0.p.
027129423008	00 00 00 00 00 00 04 00	58 00 00 00 18 00 01 00	........X.....	....X...
027129423024	20 DF 01 00 00 00 03 00	86 D5 69 DA D9 9B D5 01	ß.....ÕiÚÙ.Õ.	.....Ü
027129423040	86 D5 69 DA D9 9B D5 01	86 D5 69 DA D9 9B D5 01	.ÕiÚÙ.Õ..ÕiÚÙ.Õ.	...Ü...Ü
027129423056	86 D5 69 DA D9 9B D5 01	00 00 00 00 00 00 00 00	.ÕiÚÙ.Õ.....	...Ü....
027129423072	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	....	....
027129423088	0B 03 41 00 54 00 41 00	54 00 4F 00 4F 00 4C 00	..A.T.A.T.O.O.L.	ÄTATOOL
027129423104	2E 00 74 00 78 00 74 00	40 00 00 00 28 00 00 00	..t.x.t.@...(...	.txt@.(.
027129423120	00 00 00 00 00 00 05 00	10 00 00 00 18 00 00 00	.....	.....
027129423136	7F A0 40 66 C9 07 EA 11	B9 8C A0 A4 C5 7C 80 45	. @fÉ.ê.¹. ¤Å|.E	.....
027129423152	80 00 00 00 B8 02 00 00	00 00 18 00 00 00 01 00	....¸.....	..¥.....
027129423168	9B 02 00 00 18 00 00 00	68 64 70 61 72 6D 20 66	....hdparm f	¢.....
027129423184	6F 72 20 6C 69 6E 75 78	0D 0A 0D 0A 0D 0A 68 74	or linux....ht	.....
027129423200	74 70 73 3A 2F 2F 65 6E	2E 77 69 6B 69 70 65 64	tps://en.wikiped	.....
027129423216	69 61 2E 6F 72 67 2F 77	69 6B 69 2F 41 54 41 54	ia.org/wiki/ATAT	.....

the bytes 20 21 points to the first byte of the file attribute (56)

create modify

change access