Introduction to Computer Forensics and Security **6G7Z1009**

Introduction to NTFS

Examining NTFS Disks

- New Technology File System
  - Introduced with Windows NT.
  - NTFS is the primary file system for Windows XP.
  - NTFS uses security features.
  - Allows for smaller cluster sizes.
  - Uses Unicode.
- Spin off of HPFS (High Performance File System)
  - Collaboration with IBM’s OS/2
  - NT was backwards compatible with HPFS

Examining NTFS Disks

- New Technology File Systems (NTFS) created to be:
  - Flexible
  - Adaptable
  - Highly secure
  - Highly reliable
- Positioned Windows as a “serious” OS for business and corporate users
  - Especially in a networked environment

Examining NTFS Disks

- Maximum capacity of an NTFS volume is:
  - ❑ 2^{64} bytes

quadrillion

18,446,744,073,709,551,616 bytes!

quintillion

trillion

- 18 billion gigabytes

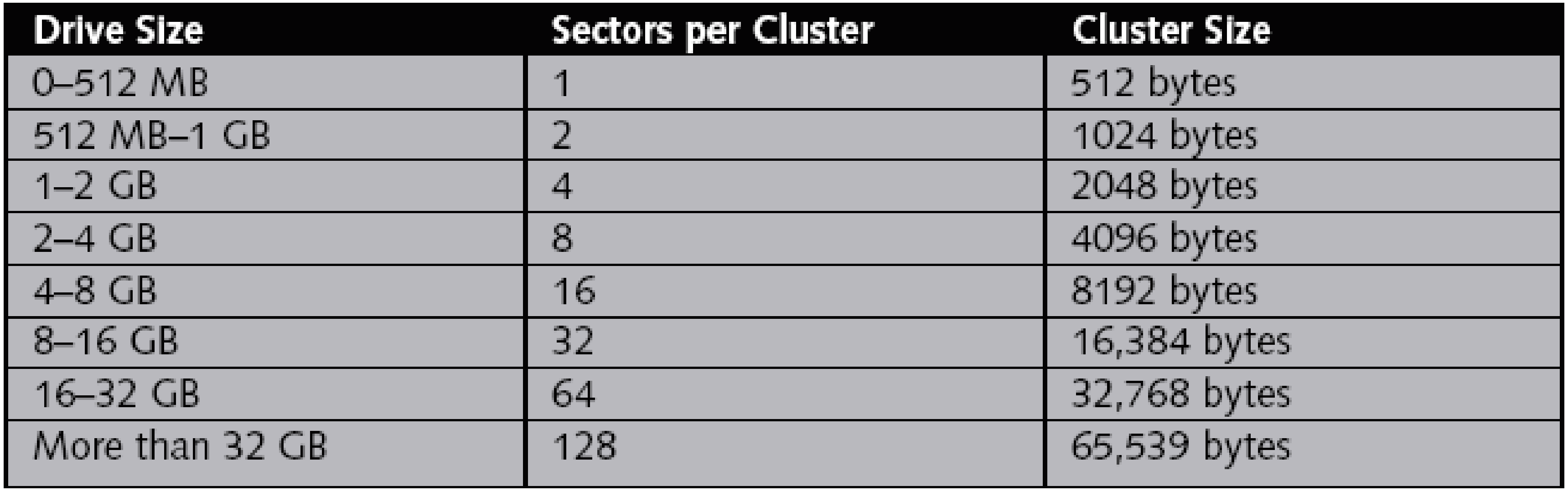
Examining NTFS Disks

- Microsoft’s move to a journaling file system
  - Keep track of transactions
    - Deletes
    - Saves
  - Records transactions before system carries it out
    - If system failure occurs
      - Transaction completion recovery is possible
      - Return to previous state also possible

Examining NTFS Disks

- Reduces slack space
  - Note smaller cluster sizes for smaller capacity disks

Table 7-3 Cluster Sizes in an NTFS Disk



Drive Size	Sectors per Cluster	Cluster Size
0–512 MB	1	512 bytes
512 MB–1 GB	2	1024 bytes
1–2 GB	4	2048 bytes
2–4 GB	8	4096 bytes
4–8 GB	16	8192 bytes
8–16 GB	32	16,384 bytes
16–32 GB	64	32,768 bytes
More than 32 GB	128	65,539 bytes

Examining NTFS Disks

Partition Boot Sector – The first data set of an NTFS disk. It starts at sector [0] of the disk drive and it can be expanded up to 16 sectors.

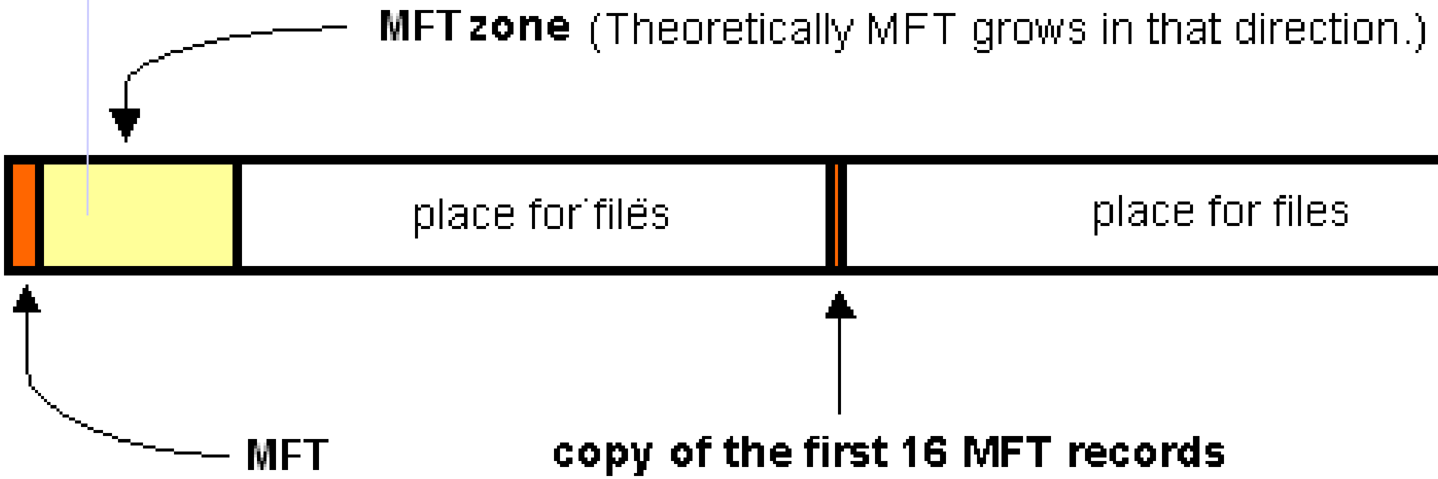
Master File Table – Used by NTFS to track files. It contains information about the access rights, date and time stamps, system attributes, and parts of the file.

Examining NTFS Disks

- Next is Master File Table (MFT)
  - Similar to FAT
  - First file on disk
  - Created when a disk partition is formatted as NTFS
  - Takes up about 12.5% of disk
    - Can expand to 50%
  - Contains information about all files on disk (meta-data)

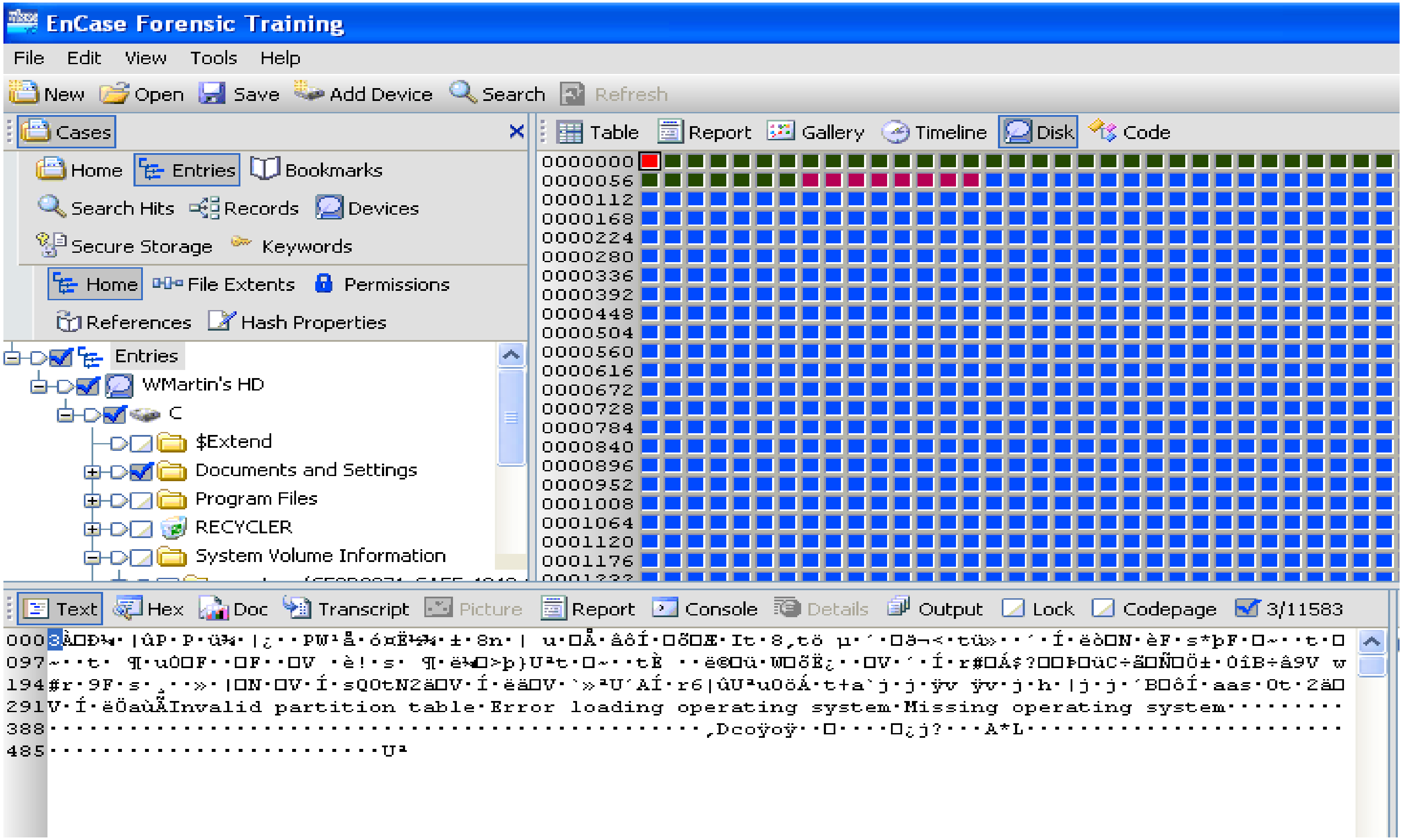
Examining NTFS Disks

(Almost) always kept empty to prevent MFT fragmentation


MFT zone (Theoretically MFT grows in that direction.)
place for files
place for files
MFT
copy of the first 16 MFT records

http://www.digit-life.com/articles/ntfs/

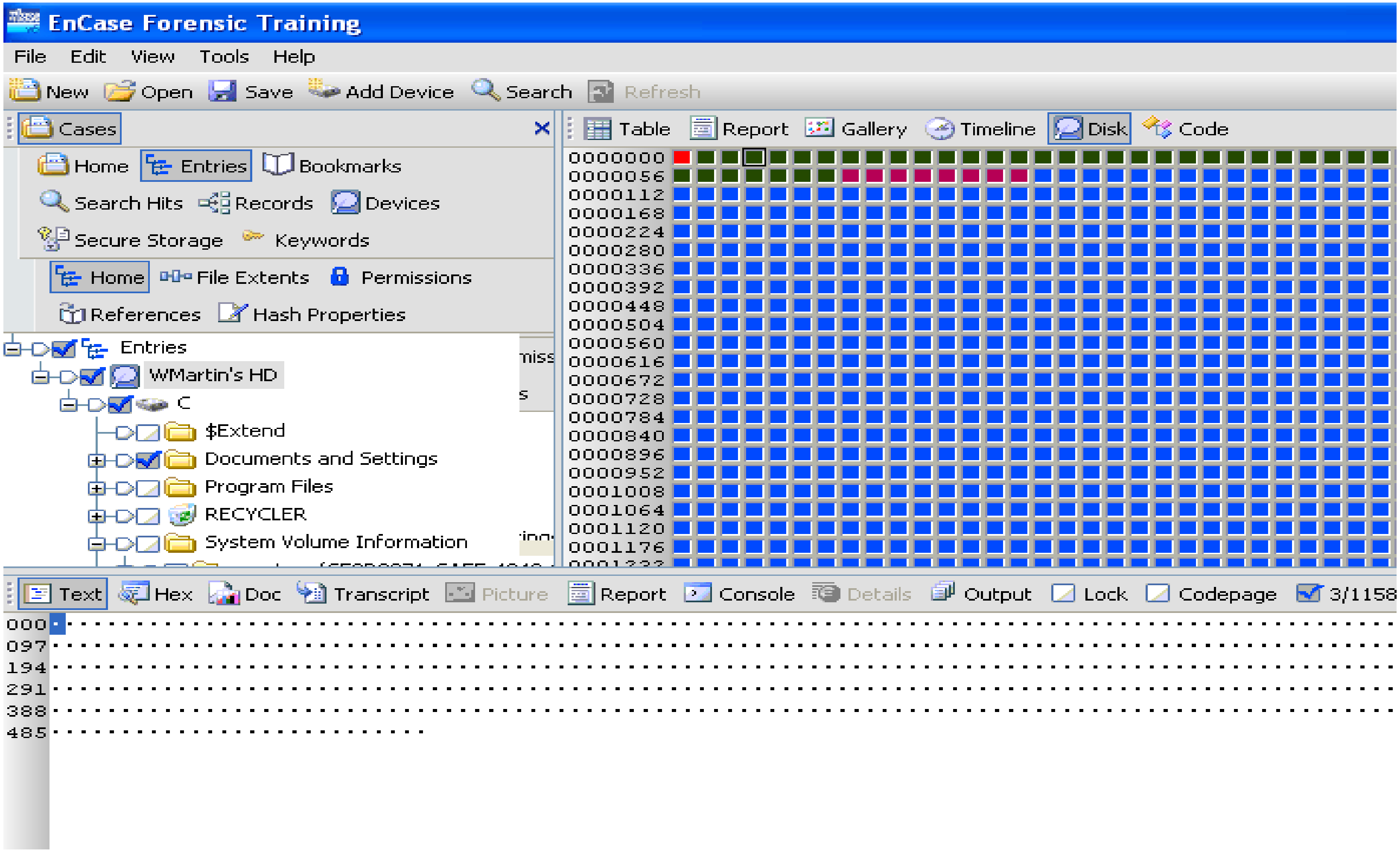
NTFS Disk Structure - MBR



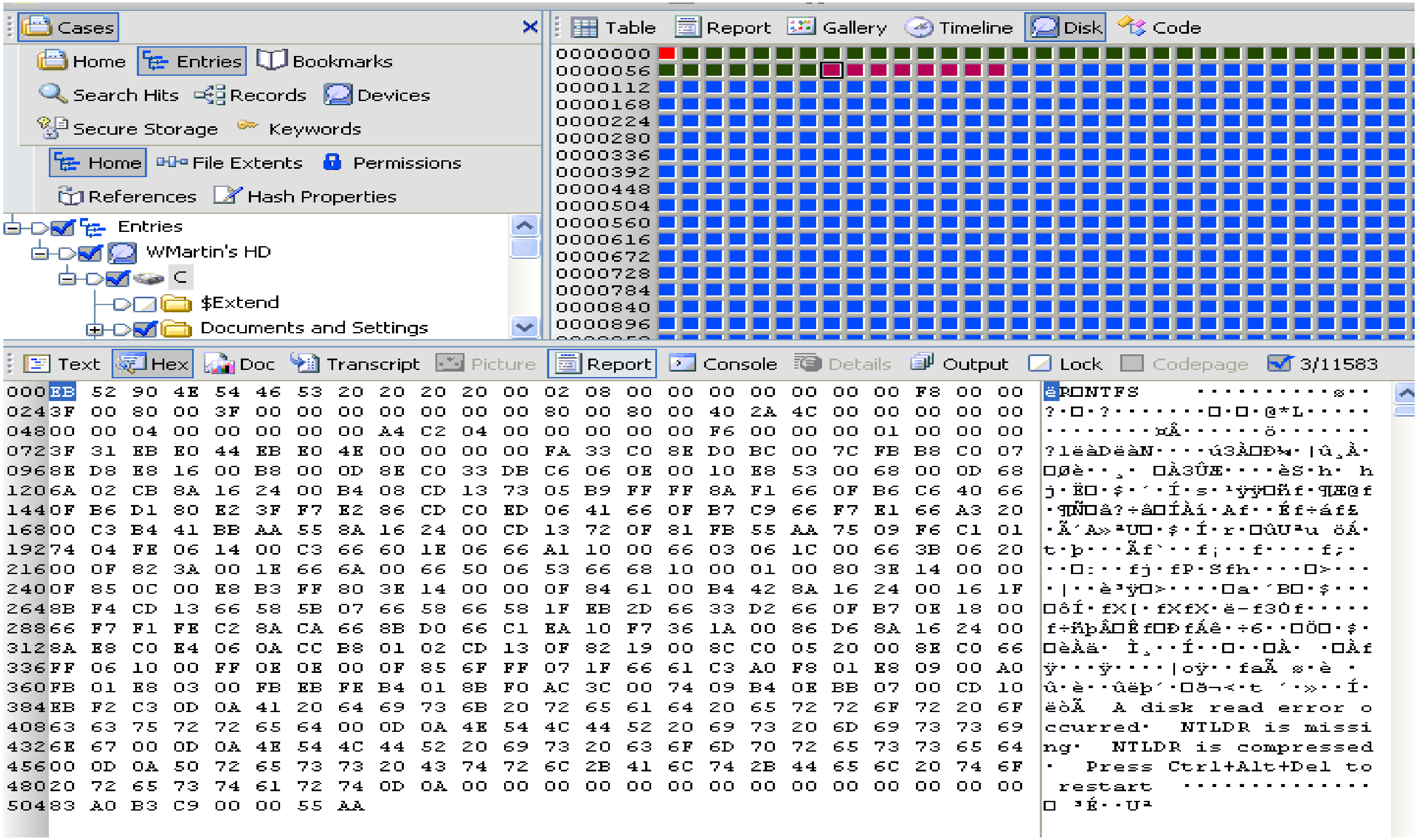
```
0000000
0000056
0000112
0000168
0000224
0000280
0000336
0000392
0000448
0000504
0000560
0000616
0000672
0000728
0000784
0000840
0000896
0000952
0001008
0001064
0001120
0001176
```

```
0003À□Ð¼·|ûP·P·ü¾·|¿··PW¹å·ó¤Ë½¾·±·8n·| u·□Å·âôÍ·□õ□Æ·It·8,tö µ·´·□ă¬<·tü»··´·Í·ëò□N·èF·s*þF·□~··t·□
097~···t·  ¶·uÔ□F··□F··□V  ·è!·s·  ¶·ë¾□>þ}Uªt·□~···tÈ  ··ë©□ü·W□õË¿··□V·´·Í·r#□Á$?□□Þ□üC÷ã□Ñ□Ö±·ÖîB÷â9V  w
194#r·9F·s·¸··»·|□N·□V·Í·sQ0tN2ä□V·Í·ëä□V·`»ªU´AÍ·r6|ûUªuÖöÁ·t+a`j·j·ÿv ÿv·j·h·|j·j·´B□ôÍ·aas·Ot·2ä□
291V·Í·ëÖaùÅInvalid partition table·Error loading operating system·Missing operating system·········
388····································································,Dcoÿoÿ··□····□¿j?···A*L·························
485··························Uª
```

NTFS Disk Structure - Reserved Area

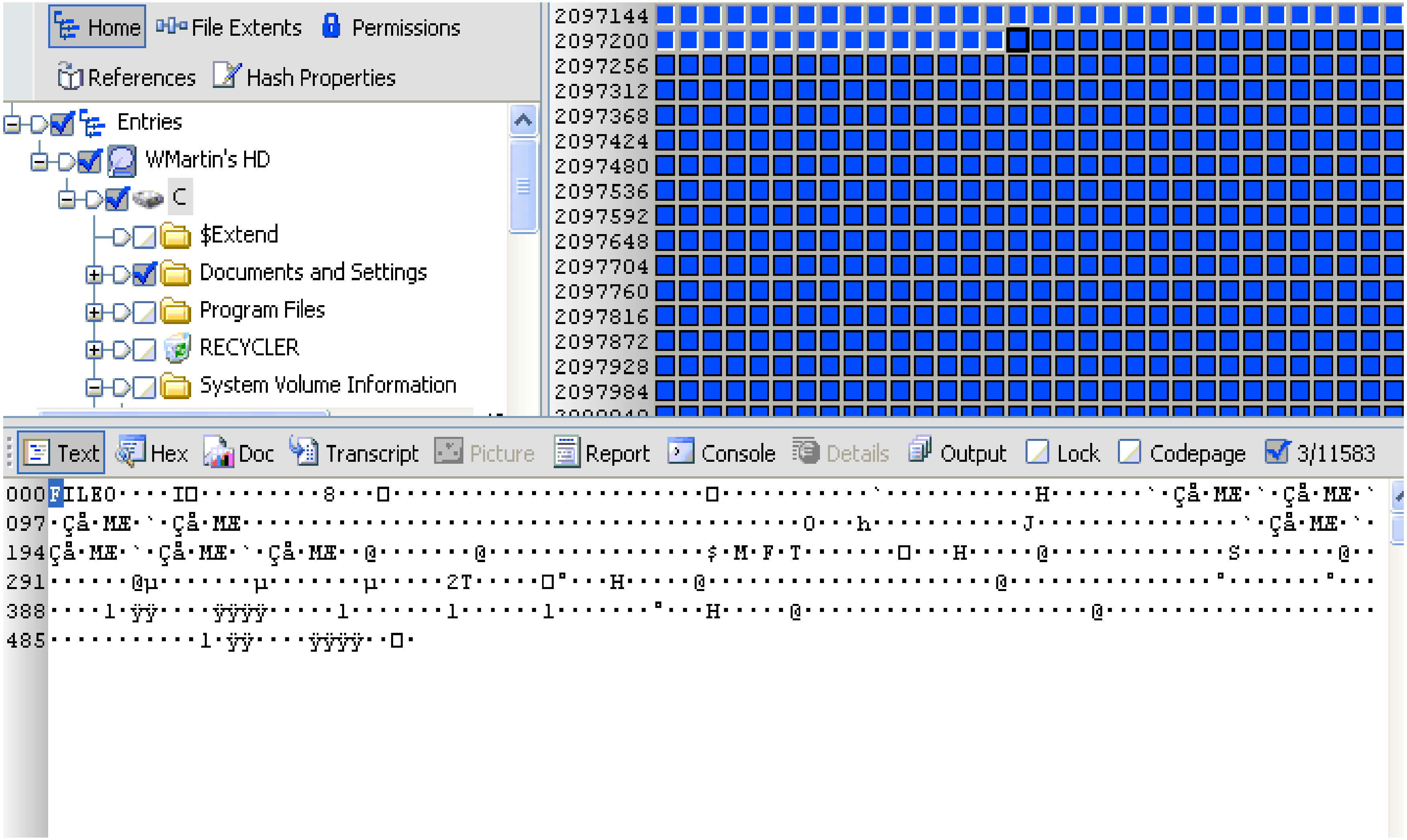


NTFS Disk Structure - Volume Boot Record



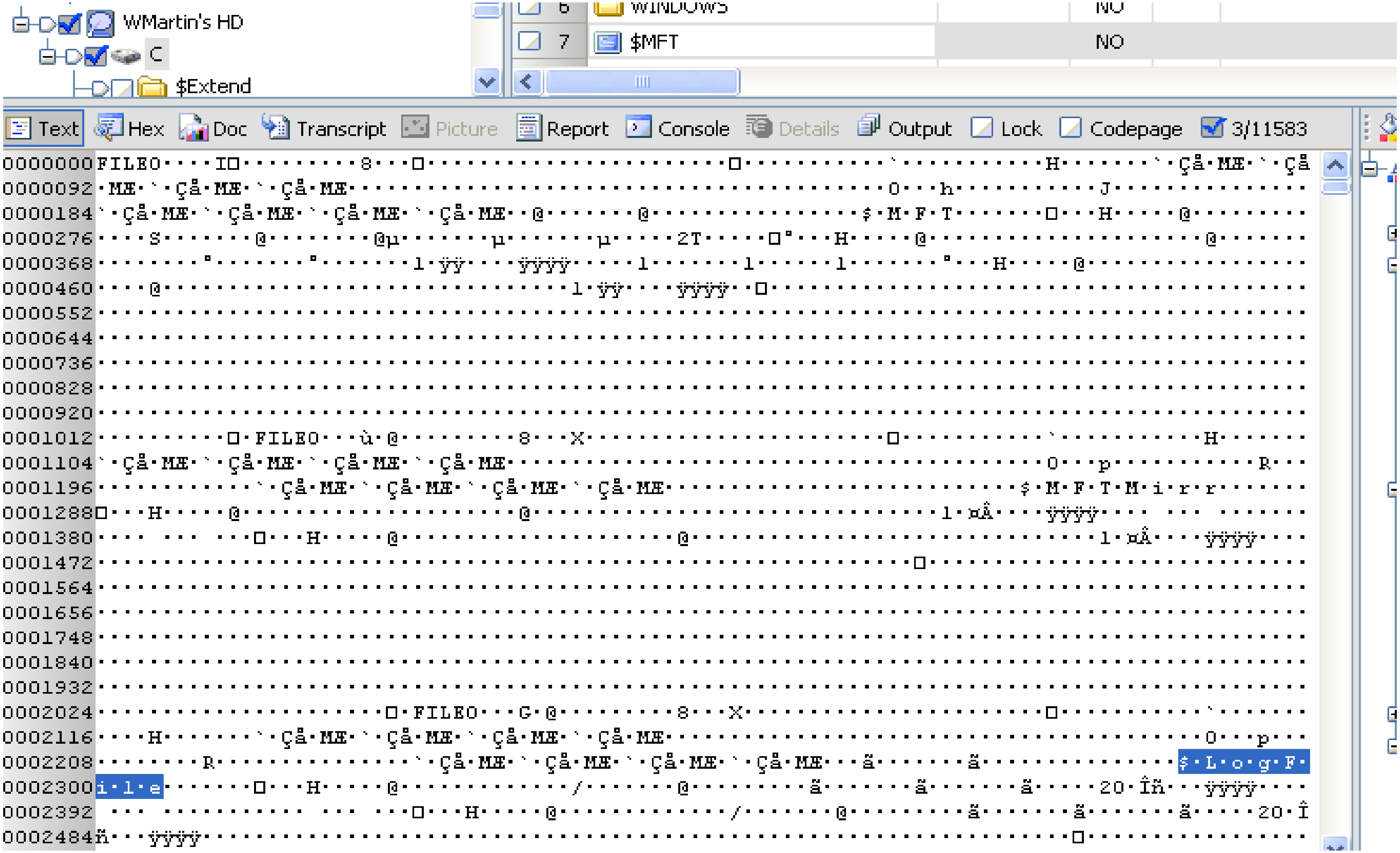
```
000EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 00 00 00 00 00 F8 00 00  ëRONTFS    ···········ø··
0243F 00 80 00 3F 00 00 00 00 00 00 00 80 00 80 00 40 2A 4C 00 00 00 00 00  ?·□·?·······□·□·@*L·····
04800 00 04 00 00 00 00 00 A4 C2 04 00 00 00 00 00 F6 00 00 00 01 00 00 00  ········¤Â······ö·······
0723F 31 EB E0 44 EB E0 4E 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB B8 C0 07  ?1ëàDëàN····ú3À□Ð¼·|û¸À·
0968E D8 E8 16 00 B8 00 0D 8E C0 33 DB C6 06 0E 00 10 E8 53 00 68 00 0D 68  □Øè··¸· □À3ÛÆ····èS·h· h
1206A 02 CB 8A 16 24 00 B4 08 CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66  j·Ë□·$·´·Í·s·¹ÿÿ□ñf·¶Æ@f
1440F B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F B7 C9 66 F7 E1 66 A3 20  ·¶Ñ□â?÷â□ÍÀí·Af··É f÷áf£
16800 C3 B4 41 BB AA 55 8A 16 24 00 CD 13 72 0F 81 FB 55 AA 75 09 F6 C1 01  ·Ã´A»ªU□·$·Í·r·□ûUªu öÁ·
19274 04 FE 06 14 00 C3 66 60 1E 06 66 A1 10 00 66 03 06 1C 00 66 3B 06 20  t·þ···Ãf`··f¡··f····f;·
21600 0F 82 3A 00 1E 66 6A 00 66 50 06 53 66 68 10 00 01 00 80 3E 14 00 00  ··□:···fj·fP·Sfh····□>···
2400F 85 0C 00 E8 B3 FF 80 3E 14 00 00 0F 84 61 00 B4 42 8A 16 24 00 16 1F  ·|···è³ÿ□>·····□a·´B□·$···
2648B F4 CD 13 66 58 5B 07 66 58 66 58 1F EB 2D 66 33 D2 66 0F B7 0E 18 00  □ôÍ·fX[·fXfX·ë-f3Òf·····
28866 F7 F1 FE C2 8A CA 66 8B D0 66 C1 EA 10 F7 36 1A 00 86 D6 8A 16 24 00  f÷ñþÂ□Êf□ÐfÁê·÷6··□Ö□·$·
3128A E8 C0 E4 06 0A CC B8 01 02 CD 13 0F 82 19 00 8C C0 05 20 00 8E C0 66  □èÀä· Ì¸··Í··□··□À· ·□Àf
336FF 06 10 00 FF 0E 0E 00 0F 85 6F FF 07 1F 66 61 C3 A0 F8 01 E8 09 00 A0  ÿ···ÿ·····|oÿ··faÃ ø·è ·
360FB 01 E8 03 00 FB EB FE B4 01 8B F0 AC 3C 00 74 09 B4 0E BB 07 00 CD 10  û·è···ûëþ´·□ð¬<·t ´·»···Í·
384EB F2 C3 0D 0A 41 20 64 69 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F  ëòÃ  A disk read error o
40863 63 75 72 72 65 64 00 0D 0A 4E 54 4C 44 52 20 69 73 20 6D 69 73 73 69  ccurred·  NTLDR is missi
4326E 67 00 0D 0A 4E 54 4C 44 52 20 69 73 20 63 6F 6D 70 72 65 73 73 65 64  ng·  NTLDR is compressed
45600 0D 0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F  ·  Press Ctrl+Alt+Del to
48020 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00   restart  ··············
50483 A0 B3 C9 00 00 55 AA                                                  □ ³É··Uª
```

NTFS Disk Structure - MFT Location



```
000FILE0····I□··········8···□·······················□···········`···········H·······`·Çå·MÆ·`·Çå·MÆ·`
097·Çå·MÆ·`·Çå·MÆ·····························0···h···········J·················`·Çå·MÆ·`·
194Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ··@·······@················$·M·F·T·······□···H·····@·············S········@··
291······@µ········µ········µ·····2T·····□°···H·····@·······················@··············°········°···
388····l·ÿÿ····ÿÿÿÿ·····l········l······l········°···H·····@·······················@·················
485············l·ÿÿ····ÿÿÿÿ··□·
```

MFT Example



```
0000000FILE0····I□·········8···□·······················□···········`···········H·······`·Çå·MÆ·`·Çå
0000092·MÆ·`·Çå·MÆ·`·Çå·MÆ·········································O···h···········J···············
0000184`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ··@·······@················$·M·F·T·······□···H·····@·········
0000276····S·······@········@µ·······µ·······µ·····2T·····□°···H·····@·····················@·······
0000368········°·······°·······1·ÿÿ····ÿÿÿÿ·····1·······1······1·······°···H·····@·················
0000460····@·······························1·ÿÿ····ÿÿÿÿ··□·········································
0000552············································································
0000644············································································
0000736············································································
0000828············································································
0000920············································································
0001012··········□·FILE0···ù·@·········8···X·······················□···········`···········H·······
0001104`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ·········································O···p···········R···
0001196············`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ··························$·M·F·T·M·i·r·r·······
0001288□···H·····@·····················@·······························1·¤Å····ÿÿÿÿ···· ··· ·······
0001380···· ··· ···□···H·····@·····················@·······························1·¤Å····ÿÿÿÿ····
0001472··············································································□·····························
0001564············································································
0001656············································································
0001748············································································
0001840············································································
0001932············································································
0002024······················□·FILE0···G·@·········8···X·······················□···········`·······
0002116····H·······`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ·········································O···p···
0002208········R···············`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ·`·Çå·MÆ···ã·······ã···············$·L·o·g·F·
0002300i·l·e·······□···H·····@·············/·······@·········ã·······ã·······ã·····20·Îñ···ÿÿÿÿ····
0002392 ··· ··········· ··· ···□···H·····@·············/·······@·········ã·······ã·······ã·····20·Î
0002484ñ···ÿÿÿÿ··································································□·················
```

NTFS System Files

- 1st 15 MFT records reserved for information about system files.

- Records in the MFT are called **metadata**

NTFS System Files

File Name	Usage	Record	Description
$MFT	MFT	0	Information about MFT itself (as a file)
$MFTmirr	MFT 2	1	Copy of the first 4 MFT records (placed in the middle of the disk). Useful for recovery
$LogFile	Log File	2	Previous transaction storage (for recovery)
$Volume	Volume	3	Housekeeping information specific to the volume: label, file system version, etc.
$AttrDef	Attribute definitions	4	Table listing descriptions of attributes used on the volume
$.	Root File name index	5	Pointer to the root directory
$Bitmap	Bit map	6	Map of the volume showing used/unused clusters
$Boot	Boot sector	7	Used to mount volume during boot process. May have additional code if this is boot volume

NTFS System Files

File Name	Usage	Record	Description
$BadClus	Bad cluster file	8	Lists all clusters marked as “bad”
$Secure	Security file	9	Contains security descriptors for the volume. Includes Access Control List (ACL) for all files and folders on the volume
$Quota	Quota Table	9	Contains quota information if disk quotas are in use
$Upcase	Upcase table	10	Used to convert filenames to Unicode
$Extend	NTFS extension file	11	Various data: quotas, object identifiers, etc.
		12-15	Reserved for future use

NTFS System Files

- In the NTFS MFT
  - All files and folders are stored in separate records of 1024 bytes each
- Each record contains file or folder information
  - This information is divided into record fields containing metadata

NTFS System Files

- A record field is referred to as an **attribute ID**
    - Name
    - Security information
    - Data itself!
    - All attributes have a unique attribute type code
- File or folder information is typically stored in one of two ways in an MFT record:
    - Resident and nonresident

NTFS File Attributes

- Resident attributes
  - Stored in the MFT itself
    - Filename and timestamp always resident
- Nonresident attributes
  - File information too large to fit in the MFT
    - Files larger than 512 bytes are stored outside the MFT, MFT record provides cluster addresses where the file is stored on the drive's partition, Referred to as **data runs**
- Each MFT record starts with a header identifying it as a resident or nonresident attribute

NTFS File Attributes

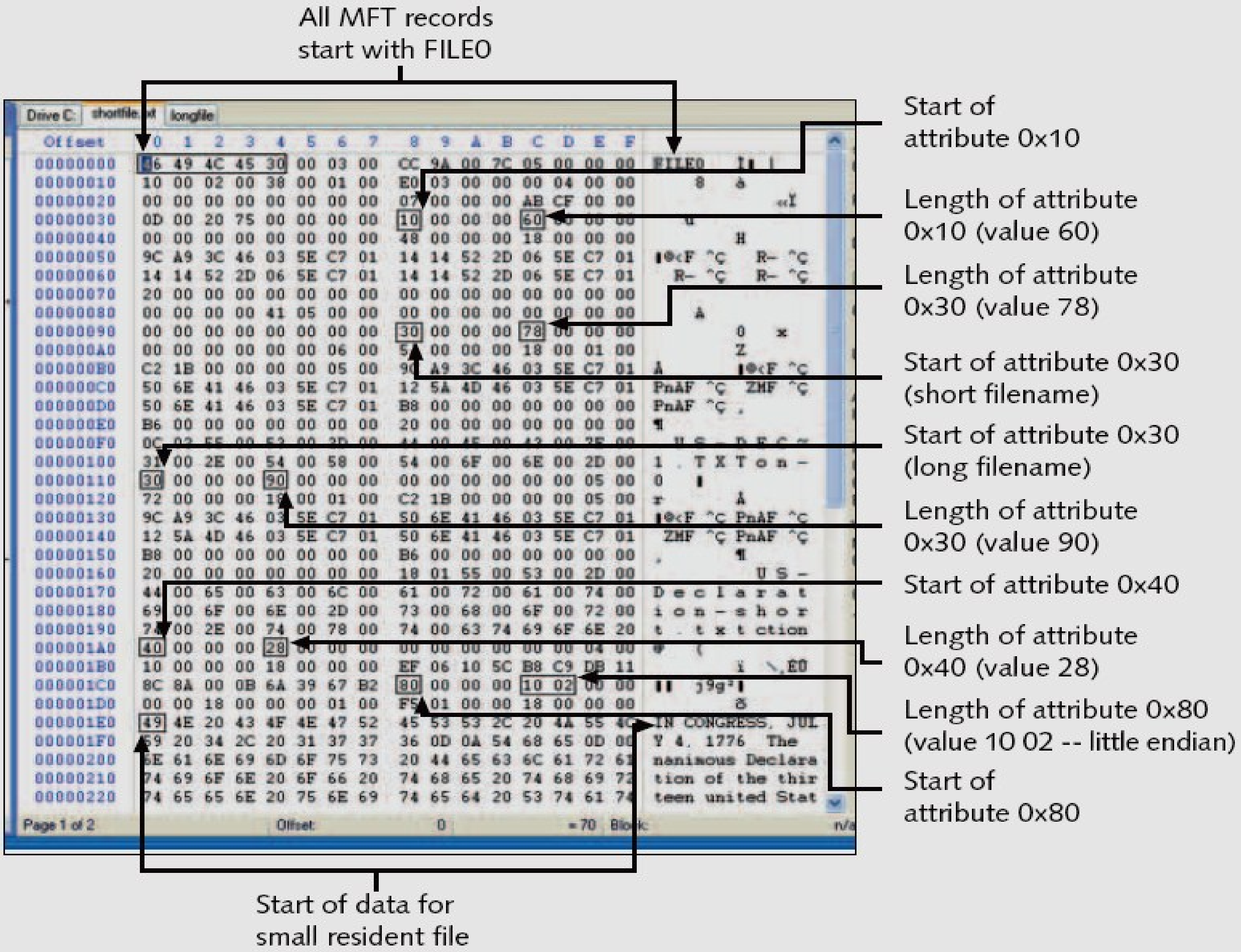
Attribute Type	**Description**
Standard Information	Includes information such as timestamp and link count.
Attribute List	Lists the location of all attribute records that do not fit in the MFT record, i.e., non-resident attributes
File Name	A repeatable attribute for both long and short file names. The long name of the file can be up to 255 Unicode characters. The short name is the case-insensitive name for the file. Additional names can be included as additional file name attributes.
Security Descriptor	Describes who owns the file and who can access it

NTFS File Attributes

Attribute Type	**Description**
Data	Contains file data. NTFS allows multiple data attributes per file. Each file typically has one unnamed data attribute. A file can also have one or more named data attributes, each using a particular syntax.
Object ID	A volume-unique file identifier. Used by the distributed link tracking service. Not all files have object identifiers.
Logged Tool Stream	Similar to a data stream, but operations are logged to the NTFS log file just like NTFS metadata changes. This is used by EFS.
Reparse Point	Used for volume mount points. They are also used by Installable File System (IFS) filter drivers to mark certain files as special to that river.

NTFS File Attributes

Attribute Type	**Description**
Index Root	Used to implement folders and other indexes
Index Allocation	Used to implement folders and other indexes
Bitmap	Used to implement folders and other indexes
Volume Information	Used only in the $Volume system file. Contains the volume version
Volume Name	Used only in the $Volume system file. Contains the volume label.



All MFT records start with FILE0
Start of attribute 0x10
Length of attribute 0x10 (value 60)
Length of attribute 0x30 (value 78)
Start of attribute 0x30 (short filename)
Start of attribute 0x30 (long filename)
Length of attribute 0x30 (value 90)
Start of attribute 0x40
Length of attribute 0x40 (value 28)
Length of attribute 0x80 (value 10 02 -- little endian)
Start of attribute 0x80
Start of data for small resident file
Drive C:
shortfile.txt
longfile

```
 Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000   46 49 4C 45 30 00 03 00  CC 9A 00 7C 05 00 00 00  FILE0    I| |
00000010   10 00 02 00 38 00 01 00  E0 03 00 00 00 04 00 00      8   à
00000020   00 00 00 00 00 00 00 00  07 00 00 00 AB CF 00 00            «Ï
00000030   0D 00 20 75 00 00 00 00  10 00 00 00 60 00 00 00     u
00000040   00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
00000050   9C A9 3C 46 03 5E C7 01  14 14 52 2D 06 5E C7 01  ▮©<F ^Ç   R- ^Ç
00000060   14 14 52 2D 06 5E C7 01  14 14 52 2D 06 5E C7 01    R- ^Ç   R- ^Ç
00000070   20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000080   00 00 00 00 41 05 00 00  00 00 00 00 00 00 00 00      A
00000090   00 00 00 00 00 00 00 00  30 00 00 00 78 00 00 00          0   x
000000A0   00 00 00 00 00 00 06 00  5A 00 00 00 18 00 01 00          Z
000000B0   C2 1B 00 00 00 00 05 00  90 A9 3C 46 03 5E C7 01  Â       ▮©<F ^Ç
000000C0   50 6E 41 46 03 5E C7 01  12 5A 4D 46 03 5E C7 01  PnAF ^Ç  ZMF ^Ç
000000D0   50 6E 41 46 03 5E C7 01  B8 00 00 00 00 00 00 00  PnAF ^Ç ¸
000000E0   B6 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00  ¶
000000F0   0C 02 55 00 53 00 2D 00  44 00 45 00 43 00 7E 00    U S - D E C ~
00000100   31 00 2E 00 54 00 58 00  54 00 6F 00 6E 00 2D 00  1 . T X T o n -
00000110   30 00 00 00 90 00 00 00  00 00 00 00 00 00 05 00  0   ▮
00000120   72 00 00 00 18 00 01 00  C2 1B 00 00 00 00 05 00  r       Â
00000130   9C A9 3C 46 03 5E C7 01  50 6E 41 46 03 5E C7 01  ▮©<F ^Ç PnAF ^Ç
00000140   12 5A 4D 46 03 5E C7 01  50 6E 41 46 03 5E C7 01   ZMF ^Ç PnAF ^Ç
00000150   B8 00 00 00 00 00 00 00  B6 00 00 00 00 00 00 00  ¸       ¶
00000160   20 00 00 00 00 00 00 00  18 01 55 00 53 00 2D 00            U S -
00000170   44 00 65 00 63 00 6C 00  61 00 72 00 61 00 74 00  D e c l a r a t
00000180   69 00 6F 00 6E 00 2D 00  73 00 68 00 6F 00 72 00  i o n - s h o r
00000190   74 00 2E 00 74 00 78 00  74 00 63 74 69 6F 6E 20  t . t x t ction
000001A0   40 00 00 00 28 00 00 00  00 00 00 00 00 00 04 00  @   (
000001B0   10 00 00 00 18 00 00 00  EF 06 10 5C B8 C9 DB 11          ï  \¸ÉÛ
000001C0   8C 8A 00 0B 6A 39 67 B2  80 00 00 00 10 02 00 00  ▮▮  j9g²▮
000001D0   00 00 18 00 00 00 01 00  F5 01 00 00 18 00 00 00          õ
000001E0   49 4E 20 43 4F 4E 47 52  45 53 53 2C 20 4A 55 4C  IN CONGRESS, JUL
000001F0   59 20 34 2C 20 31 37 37  36 0D 0A 54 68 65 0D 00  Y 4, 1776  The
00000200   6E 61 6E 69 6D 6F 75 73  20 44 65 63 6C 61 72 61  nanimous Declara
00000210   74 69 6F 6E 20 6F 66 20  74 68 65 20 74 68 69 72  tion of the thir
00000220   74 65 65 6E 20 75 6E 69  74 65 64 20 53 74 61 74  teen united Stat
Page 1 of 2          Offset:          0          = 70   Block:          n/a
```

Figure 6-9 Resident file in an MFT record

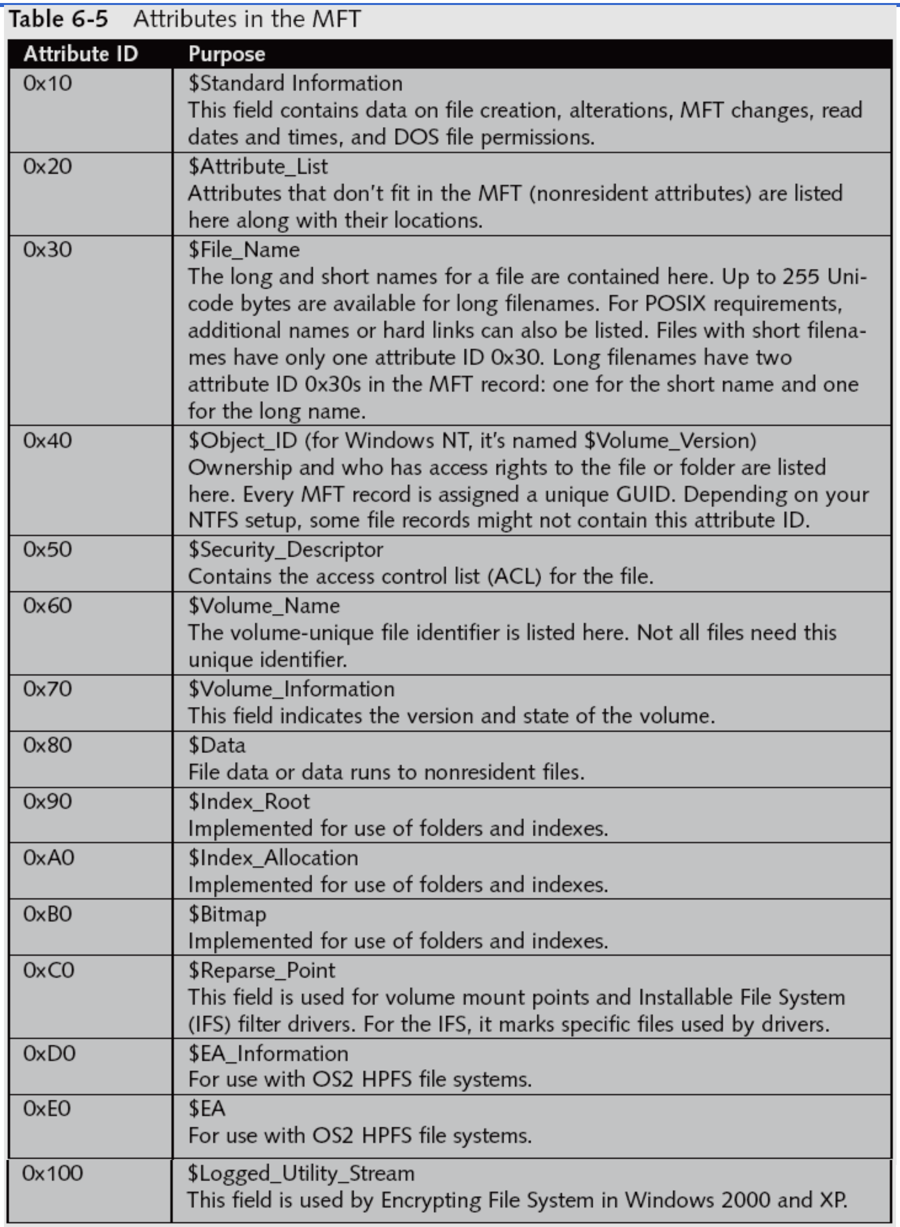
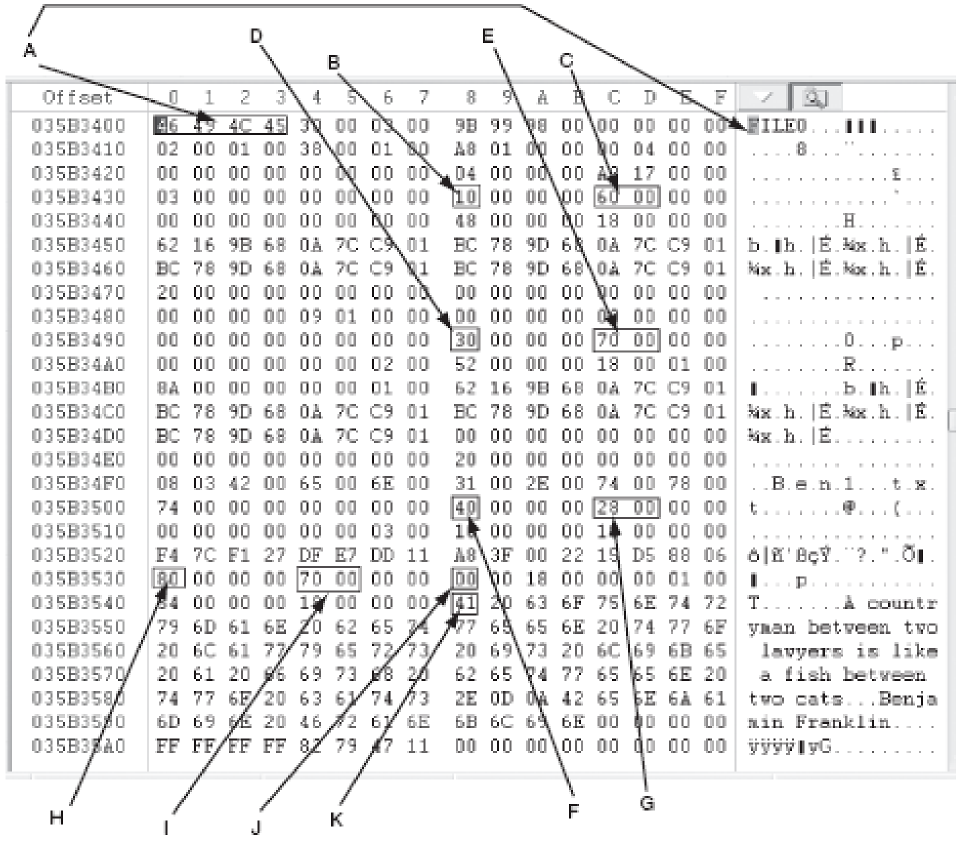


Table 6-5 Attributes in the MFT

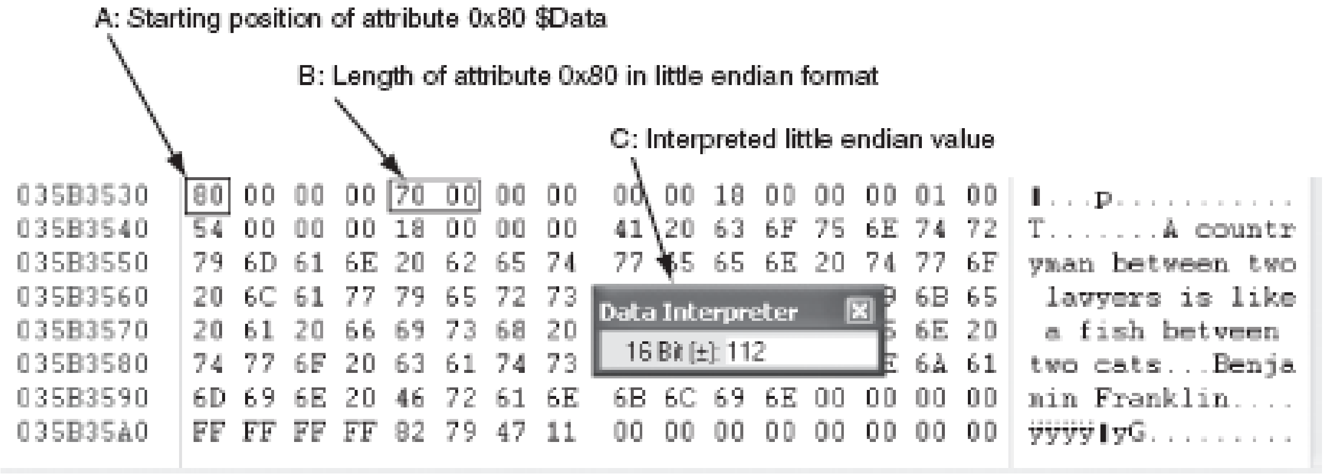
Attribute ID	Purpose
0x10	$Standard Information This field contains data on file creation, alterations, MFT changes, read dates and times, and DOS file permissions.
0x20	$Attribute_List Attributes that don't fit in the MFT (nonresident attributes) are listed here along with their locations.
0x30	$File_Name The long and short names for a file are contained here. Up to 255 Unicode bytes are available for long filenames. For POSIX requirements, additional names or hard links can also be listed. Files with short filenames have only one attribute ID 0x30. Long filenames have two attribute ID 0x30s in the MFT record: one for the short name and one for the long name.
0x40	$Object_ID (for Windows NT, it's named $Volume_Version) Ownership and who has access rights to the file or folder are listed here. Every MFT record is assigned a unique GUID. Depending on your NTFS setup, some file records might not contain this attribute ID.
0x50	$Security_Descriptor Contains the access control list (ACL) for the file.
0x60	$Volume_Name The volume-unique file identifier is listed here. Not all files need this unique identifier.
0x70	$Volume_Information This field indicates the version and state of the volume.
0x80	$Data File data or data runs to nonresident files.
0x90	$Index_Root Implemented for use of folders and indexes.
0xA0	$Index_Allocation Implemented for use of folders and indexes.
0xB0	$Bitmap Implemented for use of folders and indexes.
0xC0	$Reparse_Point This field is used for volume mount points and Installable File System (IFS) filter drivers. For the IFS, it marks specific files used by drivers.
0xD0	$EA_Information For use with OS2 HPFS file systems.
0xE0	$EA For use with OS2 HPFS file systems.
0x100	$Logged_Utility_Stream This field is used by Encrypting File System in Windows 2000 and XP.



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
035B3400  46 49 4C 45 30 00 03 00  9B 99 98 00 00 00 00 00  FILE0...▮▮▮.....
035B3410  02 00 01 00 38 00 01 00  A8 01 00 00 00 04 00 00  ....8...".......
035B3420  00 00 00 00 00 00 00 00  04 00 00 00 A8 17 00 00  ............£...
035B3430  03 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00  ............`...
035B3440  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......
035B3450  62 16 9B 68 0A 7C C9 01  BC 78 9D 68 0A 7C C9 01  b.▮h.|É.¼x.h.|É.
035B3460  BC 78 9D 68 0A 7C C9 01  BC 78 9D 68 0A 7C C9 01  ¼x.h.|É.¼x.h.|É.
035B3470  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ...............
035B3480  00 00 00 00 09 01 00 00  00 00 00 00 00 00 00 00  ................
035B3490  00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00  ........0...p...
035B34A0  00 00 00 00 00 00 02 00  52 00 00 00 18 00 01 00  ........R.......
035B34B0  8A 00 00 00 00 00 01 00  62 16 9B 68 0A 7C C9 01  ▮.......b.▮h.|É.
035B34C0  BC 78 9D 68 0A 7C C9 01  BC 78 9D 68 0A 7C C9 01  ¼x.h.|É.¼x.h.|É.
035B34D0  BC 78 9D 68 0A 7C C9 01  00 00 00 00 00 00 00 00  ¼x.h.|É.........
035B34E0  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00  ........ .......
035B34F0  08 03 42 00 65 00 6E 00  31 00 2E 00 74 00 78 00  ..B.e.n.1...t.x.
035B3500  74 00 00 00 00 00 00 00  40 00 00 00 28 00 00 00  t.......@...(...
035B3510  00 00 00 00 00 00 03 00  10 00 00 00 10 00 00 00  ................
035B3520  F4 7C F1 27 DF E7 DD 11  A8 3F 00 22 19 D5 88 06  ô|ñ'ßçÝ.¨?.".Õ▮.
035B3530  80 00 00 00 70 00 00 00  00 00 18 00 00 00 01 00  ▮...p...........
035B3540  54 00 00 00 18 00 00 00  41 20 63 6F 75 6E 74 72  T.......A countr
035B3550  79 6D 61 6E 20 62 65 74  77 65 65 6E 20 74 77 6F  yman between two
035B3560  20 6C 61 77 79 65 72 73  20 69 73 20 6C 69 6B 65   lawyers is like
035B3570  20 61 20 66 69 73 68 20  62 65 74 77 65 65 6E 20   a fish between 
035B3580  74 77 6F 20 63 61 74 73  2E 0D 0A 42 65 6E 6A 61  two cats...Benja
035B3590  6D 69 6E 20 46 72 61 6E  6B 6C 69 6E 00 00 00 00  min Franklin....
035B35A0  FF FF FF FF 82 79 47 11  00 00 00 00 00 00 00 00  ÿÿÿÿ▮yG.........
```

A: All MFT records start with FILE0
B: Start of attribute 0x10
C: Length of attribute 0x10 (value 60)
D: Start of attribute 0x30
E: Length of attribute 0x30 (value 70)
F: Start of attribute 0x40
G: Length of attribute 0x40 (value 28)
H: Start of attribute 0x80
I: Length of attribute 0x80 (value 70)
J: Attribute 0x80 resident flag
K: Starting position of resident data

Figure 6-9 Resident file in an MFT record



A: Starting position of attribute 0x80 $Data

B: Length of attribute 0x80 in little endian format

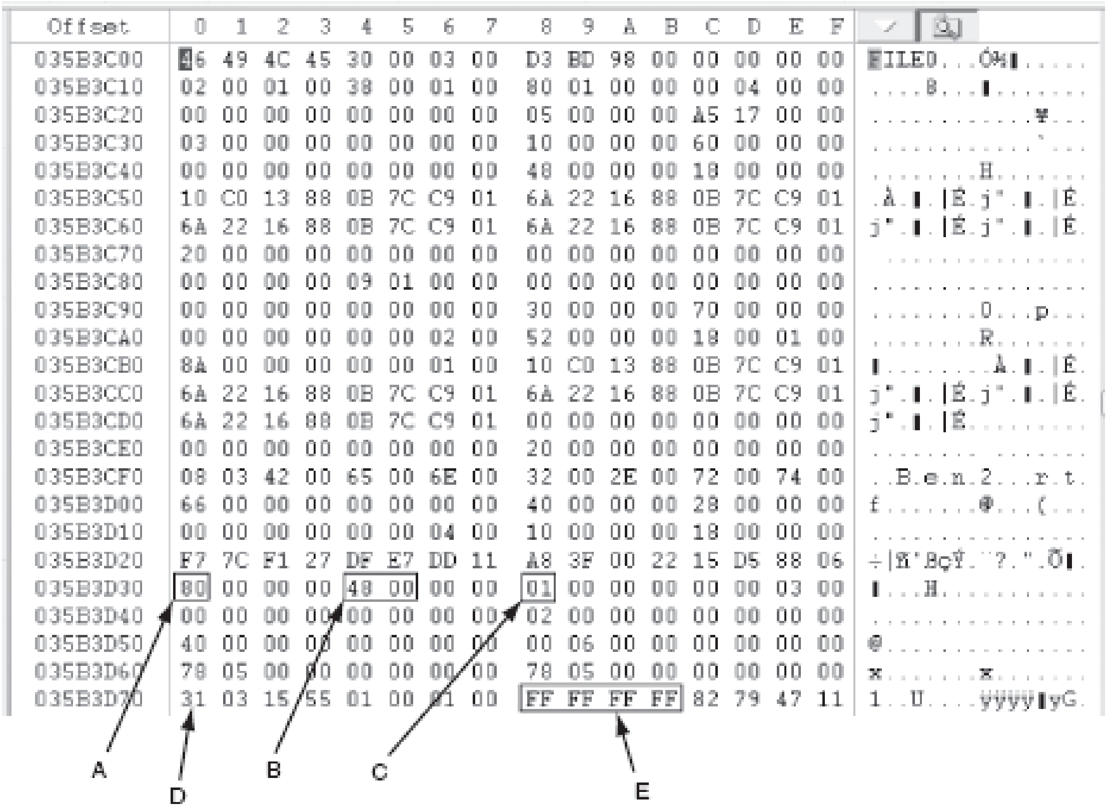
C: Interpreted little endian value

```
035B3530   80 00 00 00 70 00 00 00   00 00 18 00 00 00 01 00   ▮...p...........
035B3540   54 00 00 00 18 00 00 00   41 20 63 6F 75 6E 74 72   T.......A countr
035B3550   79 6D 61 6E 20 62 65 74   77 65 65 6E 20 74 77 6F   yman between two
035B3560   20 6C 61 77 79 65 72 73                   9 6B 65    lawyers is like
035B3570   20 61 20 66 69 73 68 20                   5 6E 20    a fish between
035B3580   74 77 6F 20 63 61 74 73                   E 6A 61   two cats...Benja
035B3590   6D 69 6E 20 46 72 61 6E   6B 6C 69 6E 00 00 00 00   min Franklin....
035B35A0   FF FF FF FF 82 79 47 11   00 00 00 00 00 00 00 00   ÿÿÿÿ▮yG.........
```

Data Interpreter

16 Bit (±): 112

Figure 6-10 File data for a resident file



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
035B3C00  46 49 4C 45 30 00 03 00  D3 BD 98 00 00 00 00 00  FILE0...Ó½▮.....
035B3C10  02 00 01 00 38 00 01 00  80 01 00 00 00 04 00 00  ....8...▮.......
035B3C20  00 00 00 00 00 00 00 00  05 00 00 00 A5 17 00 00  ............¥...
035B3C30  03 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00  ............`...
035B3C40  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......
035B3C50  10 C0 13 88 0B 7C C9 01  6A 22 16 88 0B 7C C9 01  .À.▮.|É.j".▮.|É.
035B3C60  6A 22 16 88 0B 7C C9 01  6A 22 16 88 0B 7C C9 01  j".▮.|É.j".▮.|É.
035B3C70  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ...............
035B3C80  00 00 00 00 09 01 00 00  00 00 00 00 00 00 00 00  ................
035B3C90  00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00  ........0...p...
035B3CA0  00 00 00 00 00 00 02 00  52 00 00 00 18 00 01 00  ........R.......
035B3CB0  8A 00 00 00 00 00 01 00  10 C0 13 88 0B 7C C9 01  ▮........À.▮.|É.
035B3CC0  6A 22 16 88 0B 7C C9 01  6A 22 16 88 0B 7C C9 01  j".▮.|É.j".▮.|É.
035B3CD0  6A 22 16 88 0B 7C C9 01  00 00 00 00 00 00 00 00  j".▮.|É.........
035B3CE0  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00  ........ .......
035B3CF0  08 03 42 00 65 00 6E 00  32 00 2E 00 72 00 74 00  ..B.e.n.2...r.t.
035B3D00  66 00 00 00 00 00 00 00  40 00 00 00 28 00 00 00  f.......@...(...
035B3D10  00 00 00 00 00 00 04 00  10 00 00 00 18 00 00 00  ................
035B3D20  F7 7C F1 27 DF E7 DD 11  A8 3F 00 22 15 D5 88 06  ÷|ñ'ßçÝ.¨?.".Õ▮.
035B3D30  80 00 00 00 48 00 00 00  01 00 00 00 00 00 03 00  ▮...H...........
035B3D40  00 00 00 00 00 00 00 00  02 00 00 00 00 00 00 00  ................
035B3D50  40 00 00 00 00 00 00 00  00 06 00 00 00 00 00 00  @...............
035B3D60  78 05 00 00 00 00 00 00  78 05 00 00 00 00 00 00  x.......x.......
035B3D70  31 03 15 55 01 00 01 00  FF FF FF FF 82 79 47 11  1..U....ÿÿÿÿ▮yG.
```

A: Start of nonresident attribute 0x80
B: Length of nonresident attribute 0x80
C: Attribute 0x80 nonresident flag
D: Starting point of data run
E: End-of-record marker (FF FF FF FF) for the MFT record

Figure 6-11 Nonresident file in an MFT record

Deleting NTFS Files

- When a file is deleted in Windows XP, 2000, or NT:
  - NTFS renames file
  - Moves it to Recycle Bin in a unique subfolder
  - Information on original path and file name stored in Info2 file (control file for the Recycle Bin)
    - Date/time of deletion and other info

Deleting NTFS Files

- When file is deleted via DOS:
  - Associated clusters designated as free
  - $Bitmap file marked to show new available space
  - File attribute record in MFT marked to indicate it’s available
  - Inodes and cluster numbers removed from MFT

Deleting NTFS Files

- NTFS is more efficient than FAT
  - Reclaiming deleted space
  - Deleted files are overwritten more quickly

Questions?

m.owda@mmu.ac.uk