



# NTFS bit by byte

By: Mike Wilkinson

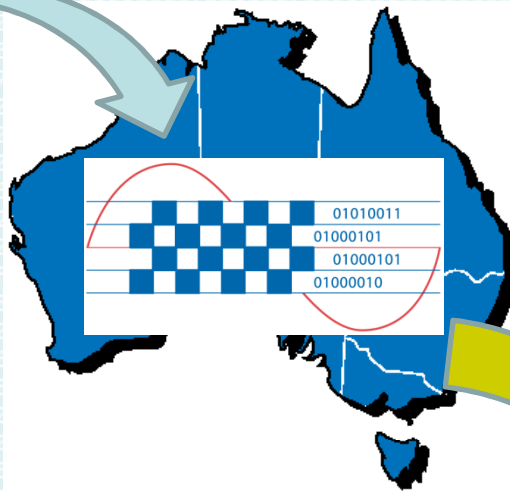


CHAMPLAIN  
COLLEGE

# About Mike



IT Contractor



CHAMPLAIN  
COLLEGE  
BURLINGTON, VERMONT

# Disclaimer

- Information from multiple sources:
  - Microsoft (authoritative?)
  - Carrier (2005) *File system Forensic Analysis*
  - Other training courses
  - Online (e.g. ntfs.com)
  - Experimentation & testing
- Problem, there are differences!
- MS terminology is used where known

# Disk layout

Partition 1  
(NTFS)

Master Boot Record

Reserved sectors

Boot sector

Files

\$MFT

More files

Boot sector backup

Boot Sector 2

includes partition table

normally 63 or 2047, count includes MBR

(points to \$MFT)

Somewhere in the middle of the partition

In the last sector of the partition





# Everything is a file

- Boot sector contain BPB
- BPB points to \$MFT & \$MFTMirr
- \$MFT points to boot sector (\$boot)....



# Boot Sector

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0	Jump Instruction			OEM ID									Bytes/ Sector		Sect/ clust	res	
10	0x000000			unused		Media desc	0x0000		Sect / track		Number heads		Hidden Sectors				
20	unused								Total Sectors								
30	Logical Cluster of \$MFT								Logical Cluster of \$MFTMirr								
40	Clust / File record segment				Clusters / Index Block				Volume Serial Number								
50	Checksum				Boot Code												
60	Boot Code																
70	Boot Code																
80	Boot Code																
90	Boot Code																
100	Boot Code																
110	Boot Code																
120	Boot Code																
130	Boot Code																
140	Boot Code																
150	Boot Code																
160	Boot Code																
170	Boot Code																
180	Boot Code																
190	Boot Code																
200	Boot Code																
210	Boot Code																
220	Boot Code																
230	Boot Code																
240	Boot Code																
250	Boot Code																
260	Boot Code																
270	Boot Code																
280	Boot Code																
290	Boot Code																
300	Boot Code																
310	Boot Code																
320	Boot Code																
330	Boot Code																
340	Boot Code																
350	Boot Code																
360	Boot Code																
370	Boot Code																
380	Boot Code																
390	Boot Code																
400	Boot Code																
410	Boot Code																
420	Boot Code																
430	Boot Code																
440	Boot Code																
450	Boot Code																
460	Boot Code																
470	Boot Code																
480	Boot Code																
490	Boot Code																
500	Boot Code																
510	Boot Code																
520	Boot Code																
530	Boot Code																
540	Boot Code																
550	Boot Code																
560	Boot Code																
570	Boot Code																
580	Boot Code																
590	Boot Code																
600	Boot Code																
610	Boot Code																
620	Boot Code																
630	Boot Code																
640	Boot Code																
650	Boot Code																
660	Boot Code																
670	Boot Code																
680	Boot Code																
690	Boot Code																
700	Boot Code																
710	Boot Code																
720	Boot Code																
730	Boot Code																
740	Boot Code																
750	Boot Code																
760	Boot Code																
770	Boot Code																
780	Boot Code																
790	Boot Code																
800	Boot Code																
810	Boot Code																
820	Boot Code																
830	Boot Code																
840	Boot Code																
850	Boot Code																
860	Boot Code																
870	Boot Code																
880	Boot Code																
890	Boot Code																
900	Boot Code																
910	Boot Code																
920	Boot Code																
930	Boot Code																
940	Boot Code																
950	Boot Code																
960	Boot Code																
970	Boot Code																
980	Boot Code																
990	Boot Code																
1000	Boot Code																
1010	Boot Code																
1020	Boot Code																
1030	Boot Code																
1040	Boot Code																
1050	Boot Code																
1060	Boot Code																
1070	Boot Code																
1080	Boot Code																
1090	Boot Code																
1100	Boot Code																
1110	Boot Code																
1120	Boot Code																
1130	Boot Code																
1140	Boot Code																
1150	Boot Code																
1160	Boot Code																
1170	Boot Code																
1180	Boot Code																
1190	Boot Code																
1200	Boot Code																
1210	Boot Code																
1220	Boot Code																
1230	Boot Code																
1240	Boot Code																
1250	Boot Code																
1260	Boot Code																
1270	Boot Code																
1280	Boot Code																
1290	Boot Code																
1300	Boot Code																
1310	Boot Code																
1320	Boot Code																
1330	Boot Code																
1340	Boot Code																
1350	Boot Code																
1360	Boot Code																
1370	Boot Code																
1380	Boot Code																
1390	Boot Code																
1400	Boot Code																
1410	Boot Code																
1420	Boot Code																
1430	Boot Code																
1440	Boot Code																
1450	Boot Code																
1460	Boot Code																
1470	Boot Code																
1480	Boot Code																
1490	Boot Code																
1500	Boot Code																
1510	Boot Code																
1520	Boot Code																
1530	Boot Code																
1540	Boot Code																
1550	Boot Code																
1560	Boot Code																
1570	Boot Code																
1580	Boot Code																
1590	Boot Code																
1600	Boot Code																
1610	Boot Code																
1620	Boot Code																
1630	Boot Code																
1640	Boot Code																
1650	Boot Code																
1660	Boot Code																
1670	Boot Code																
1680	Boot Code																
1690	Boot Code																
1700	Boot Code																
1710	Boot Code																
1720	Boot Code																
1730	Boot Code																
1740	Boot Code																
1750	Boot Code																
1760	Boot Code																
1770	Boot Code																
1780	Boot Code																
1790	Boot Code																
1800	Boot Code																
1810	Boot Code																
1820	Boot Code																
1830	Boot Code																
1840	Boot Code																
1850	Boot Code																
1860	Boot Code																
1870	Boot Code																
1880	Boot Code																
1890	Boot Code																
1900	Boot Code																
1910	Boot Code																
1920	Boot Code																
1930	Boot Code																
1940	Boot Code																
1950	Boot Code																
1960	Boot Code																
1970	Boot Code																
1980	Boot Code																
1990	Boot Code																
2000	Boot Code																
2010	Boot Code																
2020	Boot Code																
2030	Boot Code																
2040	Boot Code																
2050	Boot Code																
2060	Boot Code																
2070	Boot Code																
2080	Boot Code																
2090	Boot Code																
2100	Boot Code																
2110	Boot Code																
2120	Boot Code																
2130	Boot Code																
2140	Boot Code																
2150	Boot Code																
2160	Boot Code																
2170	Boot Code																
2180	Boot Code																
2190	Boot Code																
2200	Boot Code																
2210	Boot Code																
2220	Boot Code																
2230	Boot Code																
2240	Boot Code																
2250	Boot Code																
2260	Boot Code																
2270	Boot Code																
2280	Boot Code																
2290	Boot Code																
2300	Boot Code																
2310	Boot Code																
2320	Boot Code																
2330	Boot Code																
2340	Boot Code																
2350	Boot Code																
2360	Boot Code																
2370	Boot Code																
2380	Boot Code																
2390	Boot Code																
2400	Boot Code																
2410	Boot Code																
2420	Boot Code																
2430	Boot Code																
2440	Boot Code																
2450	Boot Code																
2460	Boot Code																
2470	Boot Code																
2480	Boot Code																
2490	Boot Code																
2500	Boot Code																
2510	Boot Code																
2520	Boot Code																
2530	Boot Code																
2540	Boot Code																
2550	Boot Code																
2560	Boot Code																
2570	Boot Code																
2580	Boot Code																
2590	Boot Code																
2600	Boot Code																
2610	Boot Code																
2620	Boot Code																
2630	Boot Code																
2640	Boot Code																
2650	Boot Code																
2660	Boot Code																
2670	Boot Code																
2680	Boot Code																
2690	Boot Code																
2700	Boot Code																
2710	Boot Code																
2720	Boot Code																
2730	Boot Code																
2740	Boot Code																
2750	Boot Code																
2760	Boot Code																
2770	Boot Code																
2780	Boot Code																
2790	Boot Code																
2800	Boot Code																
2810	Boot Code																
2820	Boot Code																
2830	Boot Code																
2840	Boot Code																
2850	Boot Code																
2860	Boot Code																
2870	Boot Code																
2880	Boot Code																
2890	Boot Code																
2900	Boot Code																
2910	Boot Code																
2920	Boot Code																
2930	Boot Code																
2940	Boot Code																
2950	Boot Code																
2960	Boot Code																
2970	Boot Code																
2980	Boot Code																
2990	Boot Code																
3000	Boot Code																
3010	Boot Code																
3020	Boot Code																
3030	Boot Code																
3040	Boot Code																
3050	Boot Code																
3060	Boot Code																
3070	Boot Code																
3080	Boot Code																
3090	Boot Code																
3100	Boot Code																
3110	Boot Code																
3120	Boot Code																
3130	Boot Code																
3140	Boot Code																
3150	Boot Code																
3160	Boot Code																
3170	Boot Code																
3180	Boot Code																
3190	Boot Code																
3200	Boot Code																
3210	Boot Code																
3220	Boot Code																
3230	Boot Code																
3240	Boot Code																
3250	Boot Code																
3260	Boot Code																
3270	Boot Code																
3280	Boot Code																
3290	Boot Code																
3300	Boot Code																
3310	Boot Code																
3320	Boot Code																
3330	Boot Code																
3340	Boot Code																
3350	Boot Code																
3360	Boot Code																
3370	Boot Code																
3380	Boot Code																
3390	Boot Code																
3400	Boot Code																
3410	Boot Code																
3420	Boot Code																
3430	Boot Code																
3440	Boot Code																
3450	Boot Code																
3460	Boot Code																
3470	Boot Code																
3480	Boot Code																
3490	Boot Code																
3500	Boot Code																
3510	Boot Code																
3520	Boot Code																
3530	Boot Code																
3540	Boot Code																
3550	Boot Code																
3560	Boot Code																
3570	Boot Code																
3580	Boot Code																
3590	Boot Code																
3600	Boot Code																
3610	Boot Code																
3620	Boot Code																
3630	Boot Code																
3640	Boot Code																
3650	Boot Code																
3660	Boot Code																
3670	Boot Code																
3680	Boot Code																
3690	Boot Code																
3700	Boot Code																
3710	Boot Code																
3720	Boot Code																
3730	Boot Code																
3740	Boot Code																
3750	Boot Code																
3760	Boot Code																
3770	Boot Code																
3780	Boot Code																
3790	Boot Code																
3800	Boot Code																
3810	Boot Code																
3820	Boot Code																
3830	Boot Code																
3840	Boot Code																
3850	Boot Code																
3860	Boot Code																
3870	Boot Code																
3880	Boot Code																
3890	Boot Code																
3900	Boot Code																
3910	Boot Code																
3920	Boot Code																
3930	Boot Code																
3940	Boot Code																
3950	Boot Code																
3960	Boot Code																
3970	Boot Code																
3980	Boot Code																
3990	Boot Code																
4000	Boot Code																
4010	Boot Code																
4020	Boot Code																
4030	Boot Code																
4040	Boot Code																
4050	Boot Code																
4060	Boot Code																
4070	Boot Code																
4080	Boot Code																
4090	Boot Code																
4100	Boot Code																
4110	Boot Code																
4120	Boot Code																
4130	Boot Code																
4140	Boot Code																
4150	Boot Code																
4160	Boot Code																
4170	Boot Code																
4180	Boot Code																
4190	Boot Code																
4200	Boot Code																
4210	Boot Code																
4220	Boot Code																
4230	Boot Code																
4240	Boot Code																
4250	Boot Code																
4260	Boot Code																
4270	Boot Code																
4280	Boot Code																
4290	Boot Code																
4300	Boot Code																
4310	Boot Code																
4320	Boot Code																
4330	Boot Code																
4340	Boot Code																
4350	Boot Code																
4360	Boot Code																
4370	Boot Code																
4380	Boot Code																
4390	Boot Code																
4400	Boot Code																
4410	Boot Code																
4420	Boot Code																
4430	Boot Code																
4440	Boot Code																
4450	Boot Code																
4460	Boot Code																
4470	Boot Code																
4480	Boot Code																
4490	Boot Code																
4500	Boot Code																
4510	Boot Code																
4520	Boot Code																
4530	Boot Code																
4540	Boot Code																
4550	Boot Code																
4560	Boot Code																
4570	Boot Code																
4580	Boot Code																
4590	Boot Code																
4600	Boot Code																
4610	Boot Code																
4620	Boot Code																
4630	Boot Code																
4640	Boot Code																
4650	Boot Code																
4660	Boot Code																
4670	Boot Code																
4680	Boot Code																
4690	Boot Code																
4700	Boot Code																
4710	Boot Code																
4720	Boot Code																
4730	Boot Code																
4740	Boot Code																
4750	Boot Code																
4760	Boot Code																
4770	Boot Code																
4780	Boot Code																
4790	Boot Code																
4800	Boot Code																
4810	Boot Code																
4820	Boot Code																
4830	Boot Code																
4840	Boot Code																
4850	Boot Code																
4860	Boot Code																
4870	Boot Code																
4880	Boot Code																
4890	Boot Code																
4900	Boot Code																
4910	Boot Code																
4920	Boot Code																
4930	Boot Code																
4940	Boot Code																
4950	Boot Code																
4960	Boot Code																
4970	Boot Code																
4980	Boot Code																
4990	Boot Code																
5000	Boot Code																
5010	Boot Code																
5020	Boot Code																
5030	Boot Code																
5040	Boot Code																
5050	Boot Code																
5060	Boot Code																
5070	Boot Code																
5080	Boot																

# Practice

Jump Instruction

OEM ID

Bytes per Sector

Sectors per Cluster

Hidden Sectors

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000000000	EB	52	90	4E	54	46	53	20	20	20	20	02	08	00	00	00
000000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	28	03	00
000000020	00	00	00	00	80	00	80	00	FF	D7	31	0C	00	00	00	00
000000030	00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00
000000040	F6	00	00	00	01	00	00	00	C6	6E	97	6A	85	97	6A	C8
000000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07
000000060	1F	1E	68	66	00	00	00	00	B1	3E	03	00	4E	00	00	00

\$MFT cluster

Total Sectors

Clusters per File  
record segment

\$MFTMirr cluster

# BUT

- Intel processor reads number right to left



- 0000 0200 = 0x0200 = 512

- Boot sector is at cluster 0



# Practice...

Jump Instruction

OEM ID

Bytes per Sector  
0x0200  
512

Sectors per  
Cluster  
8

Hidden Sectors  
0x032800  
206,848

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00
000000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	28	03	00
000000020	00	00	00	00	80	00	80	00	FF	D7	31	0C	00	00	00	00
000000030	00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00
000000040	F6	00	00	00	01	00	00	00	C6	6E	97	6A	85	97	6A	C8
000000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07
000000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	00

Clusters per File  
record segment  
0xF6 = 246

\$MFT cluster  
0x0C0000 = 786432

\$MFTMirr cluster  
0x02

Total Sectors  
0x0C31D7FF =  
204,593,151  
  
97GiB

# Your turn PFIC\_01

Sectors per Cluster

Bytes per Sector

Hidden Sectors

Jump Instruction

OEM ID

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00
00000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	3E	00	00	00
00000020	00	00	00	00	80	00	00	00	8D	FD	02	00	00	00	00	00
00000030	E5	1F	00	00	00	00	00	00	02	00	00	00	00	00	00	00
00000040	F6	00	00	00	01	00	00	00	61	5E	BA	66	76	BA	66	0E
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07
00000060	1F	1E	68	66	00	00	00	00	81	3E	03	00	4E	00	00	00
00000070	54	46	53	75	15	00	00	00	13	72	0C	81	FB	00	00	00
00000080	55	AA	75	06	F7	C1	01	00	75	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000B0	00	00	00	00	00	00	00	00	33	DB	B9	00	20	2B	C8	00
000000C0	00	00	00	00	00	00	00	00	8E	C2	FF	06	16	00	E8	00

\$MFT cluster

Total Sectors

Clusters per File  
record segment

\$MFTMirr cluster

# Your turn...

Jump Instruction

OEM ID

Bytes per Sector  
0x0200  
512

Sectors per  
Cluster  
8

Hidden Sectors  
0x0000003E  
62

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00
00000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	3E	00	00	00
00000020	00	00	00	00	80	00	00	00	8D	FD	02	00	00	00	00	00
00000030	E5	1F	00	00	00	00	00	00	02	00	00	00	00	00	00	00
00000040	F6	00	00	00	01	00	00	00	61	5E	BA	66	76	BA	66	0E
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07
00000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	
00000070	54	46	53	75	1											

Clusters per File  
record segment  
0xF6 = 246

\$MFT cluster  
0x1FE5 = 8165

\$MFTMirr cluster  
0x02

Total Sectors  
0x02FD8D =  
195,981  
  
95MiB

# Where is the \$MFT?

- Cluster 786,432
- 1 sector = 512 bytes
- 1 cluster = 8 sectors

• \$MFT starts at byte  $786,432 \times 512 \times 8$   
 $= 3,221,225,472$   
 $= 0xC0000000$



# Your turn 2 – Find the \$MFT on PFIC\_01

- \$MFT start cluster =
- 1 sector = ??? bytes
- 1 cluster = ? sectors
- \$MFT starts at byte  $x \times x$

# Where is the \$MFT on PFIC\_01?

\$MFT start cluster =  $0x1FE5 = 8165$

1 sector = 512 bytes

1 cluster = 8 sectors

\$MFT starts at byte  $8165 \times 512 \times 8$   
 $= 33,443,840$   
 $= 0x1FE5000$

# NTFS files...

## Everything is a file

File	Name	record #
\$MFT	Master File Table	0
\$MFTMirr	MFT mirror	1
\$LogFile	Log file	2
\$Volume	Volume	3
\$AttrDef	Attribute definitions	4
.	Root file name index	5
\$Bitmap	Cluster bitmap	6
\$Boot	Boot sector	7
\$BadClus	Bad cluster file	8
\$Secure	Security File	9
\$Upcase	Upcase table	10
\$Extend	NTFS extension file	11
	reserved	12-15

# \$MFT

- Contains a record for every file
- Each record is a chain of attributes
- Default record size 1024 bytes
- May contain empty records
- Default size determined by partition size



# \$MFT entry structure

ATTRIBUTE\_RECORD\_HEADER

FILE\_RECORD  
\_SEGMENT\_  
HEADER

Attribute Data

Attribute data may be located  
outside the \$MFT



# FILE\_RECORD\_SEGMENT\_HEADER

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F	I	L	E	Update Seq array offset		Update Seq array size		\$LogFile Sequence Number							
1	Seq no		Hard Link Count		1 <sup>st</sup> attrib offset		Flags		Used size of file record				Allocated size of file record			
2	File reference to base file record								Next attrib ID				MFT Record No			
3	default location of update seq array (size determined by seq size)						Reserved for update sequence array?									
	Reserved for sequence array?								Common location of 1 <sup>st</sup> attrib							

## FILE\_RECORD\_SEGMENT\_HEADER

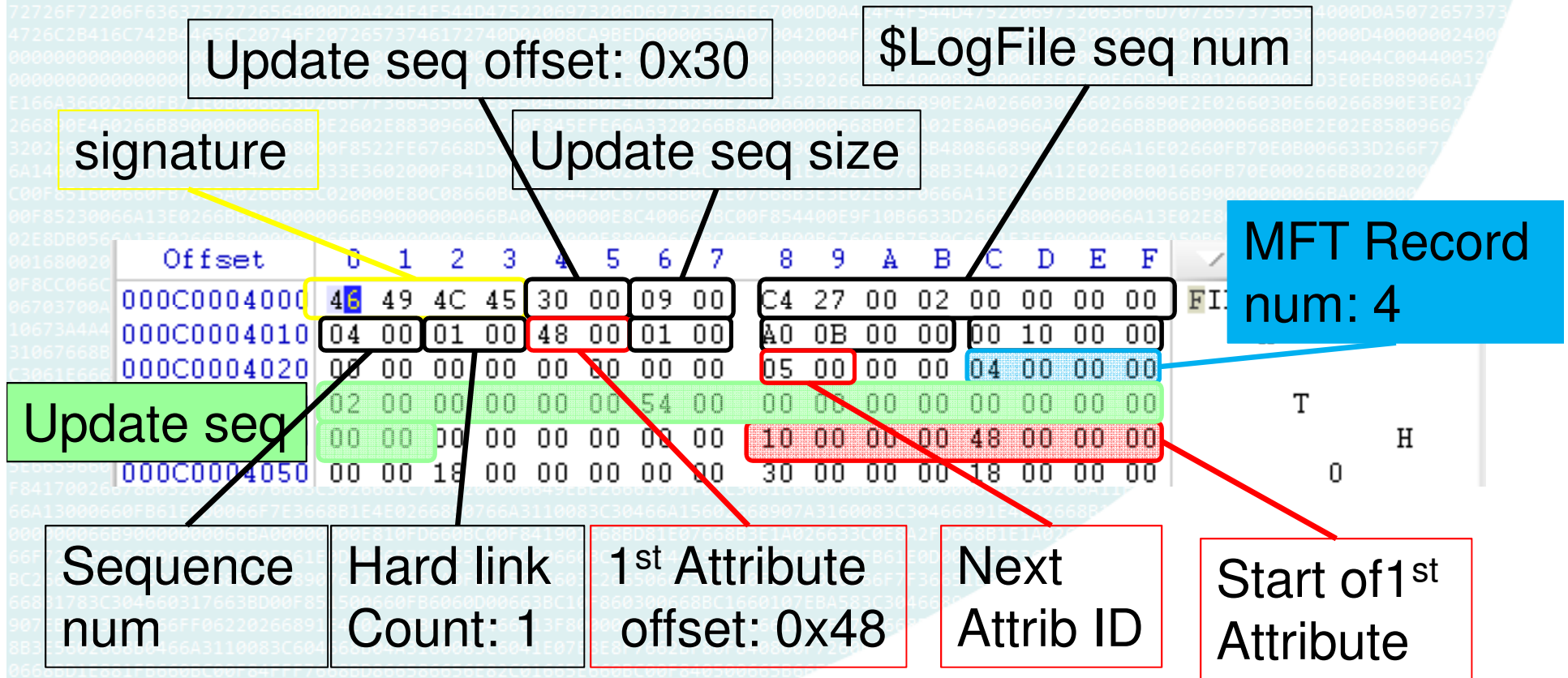
- Update sequence – integrity checking if record during move or copy
- \$LogFile seq num – Reference to entry in \$LogFile (journal)
- Sequence num – number of times record has been updated
- Flags – 0x0001 = in use  
0x0002 = directory

# FILE\_RECORD\_SEGMENT\_HEADER

- Next attrib ID – next ID to be allocated, tells us how many attributes to look for.



# FILE\_RECORD\_SEGMENT\_HEADER



# Resident Attribute Header

Standard for all resident attributes

Name refers to attribute name, which is optional

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Type ID				Attribute Length				Form code	name len	Name offset	flags		Attrib ID		
1	Content length				Content offset		unused									

Source: <http://msdn.microsoft.com/en-us/library/bb470039%28v=VS.85%29.aspx>

Form code

0x00 = Resident

0x01 = Non resident

Flags

0x00FF = Compressed

0x8000 = Sparse

0x4000 = Encrypted

# MFT Attributes - \$AttrDef

ID	Attribute Type	Description
0x10	Standard Information	Includes information such as time stamp and link count.
0x20	Attribute List	Lists the location of all the attribute records that do not fit in the MFT record.
0x30	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 MS-DOS-readable, 8.3, case-insensitive name for the file. Additional names, or hard links, required by POSIX can be included as additional file name attributes.
0x40	Object ID	A volume-unique file identifier. Used by the link tracking service. Not all files have object identifiers.
0x50	Security Descriptor	Shows information about who owns the file and who can access the file.
0x60	Volume Name	Used only in the \$Volume system file. Contains the volume label.
0x70	Volume Information	Used only in the \$Volume system file. Contains the volume version.
0x80	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.
0x90	Index Root	Used to implement folders and other indexes.
0xA0	Index Allocation	Used to implement folders and other indexes.
0xB0	Bitmap	Used to implement folders and other indexes.
0xC0	Reparse Point	Used for directory junction points and volume mount points. They are also used by file system filter drivers to mark certain files as special to that driver.
0x100	Logged Tool Stream	Similar to a data stream, but operations on a logged tool stream are logged to the NTFS log file just like NTFS metadata changes. Used by EFS.

Source: <http://technet.microsoft.com/en-us/library/cc976808.aspx>

# \$Standard\_Information

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Date Created*								Date Modified							
10	Date MFT record modified								Date Accessed							
20	Flags				Max Versions				Version Num				Class ID			
30	Owner ID				Security ID				Quota Charged							
40	Update Sequence Number															

\*Time values are in 100 nanoseconds since January 1, 1601 UTC



# \$Standard\_Information flags

Bit	Meaning
0	Read only
1	Hidden
2	System
3	
4	
5	Archive
6	Device
7	Normal
8	Temporary
9	Sparse File
A	Reparse Point
B	Compressed
C	Offline
D	Not Indexed
E	Encrypted
F	

More information:

[http://msdn.microsoft.com/en-us/library/aa365535\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa365535(v=VS.85).aspx)

# Standard Information Times

- Read by the NTFS driver
- Read by forensic tools
- Changed by timestomp
- Changed by MS SetFileTime function

[http://msdn.microsoft.com/en-us/library/ms724933\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724933(v=VS.85).aspx)

# Practice \$Standard\_Information

Diagram illustrating the structure of a file's \$Standard\_Information attribute, showing various fields and their corresponding values in hexadecimal.

**Fields and Values:**

- Form code:** resident
- Flags:** 0x06 or 0110 = hidden & system
- Content len:** 0x10 = Std\_info
- Type ID:** 0x10 = Std\_info
- Attrib len:** 0x60
- Content offset:** 0x18
- Date Created:** 0x00000207
- MFT record modified:** 0x00000208
- Date Modified:** 0x00000209
- Date Accessed:** 0x0000020A
- Start of 2<sup>nd</sup> Attribute:** 0x30000000

**Hexadecimal Data (hex dump):**

```

00 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00
00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00
86 71 34 47 47 C6 CB 01 86 71 34 47 47 C6 CB 01
86 71 34 47 47 C6 CB 01 86 71 34 47 47 C6 CB 01
06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 30 00 00 00 70 00 00 00
  
```

**Annotations:**

- Red boxes highlight the Type ID (0x10), Content len (0x10), and the start of the 2<sup>nd</sup> attribute (0x30000000).
- Black boxes highlight the Content offset (0x18) and the Date Modified (0x00000209).
- Arrows point from the labels to the corresponding fields in the hex dump.

# Your turn 3

Decode first record entry on the \$MFT on PFIC\_01

01FE5000	46 49 4C 45 30 00 03 00	F4 22 10 00 00 00 00 00	FILE0	␣"
01FE5010	01 00 01 00 38 00 01 00	A0 01 00 00 00 04 00 00	8	
01FE5020	00 00 00 00 00 00 00 00	06 00 00 00 00 00 00 00		
01FE5030	03 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00		
01FE5040	00 00 18 00 00 00 00 00	48 00 00 00 18 00 00 00	H	
01FE5050	05 AE CD B9 FB 8C CC 01	05 AE CD B9 FB 8C CC 01	⓪í'û	⓪í'û
01FE5060	05 AE CD B9 FB 8C CC 01	05 AE CD B9 FB 8C CC 01	⓪í'û	⓪í'û
01FE5070	06 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
01FE5080	00 00 00 00 00 01 00 00	00 00 00 00 00 00 00 00		
01FE5090	00 00 00 00 00 00 00 00	30 00 00 00 68 00 00 00	0	h

Use the data interpreter for the dates.



# Your turn 3, solution

1<sup>st</sup> Attribute  
offset: 0x38

Flags: 0x01  
In use

Size of MFT  
record: 0x01A0

MFT Record  
num: 0 (\$MFT)

Next  
Attrib num

Attrib ID  
0x10

Resident

Flags 0x06 = 0110  
= hidden & system

Date Created  
Oct 17, 2011

Next attribute type  
0x30 = FileName

Attrib  
Length  
0x60

Content Offset

Content length

# \$File\_Name

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Parent Directory								Date Created							
10	Date Modified								Date MFT Modified							
20	Date Accessed								Logical file size							
30	Size on disk								Flags*				Reparse value			
40	Name len	Name type	Name (variable length)													

## Name types

Value	Description
0	POSIX (unicode, case sensitive)
1	Win32 (unicode, case insensitive)
2	DOS (8.3 ASCII, case insensitive)
3	Win32 7 DOS (when Win32 fits in DOS space)

\* Same meaning as \$Standard\_Information

Attrib ID  
0x30

Attrib Length  
0x78

## Content Offset

## Content length

# Parent Directory

# Size of name

Name type  
0x02 = Dos

Start of file  
name

Date Created  
Oct 17, 2011

# Non Resident Attribute Header

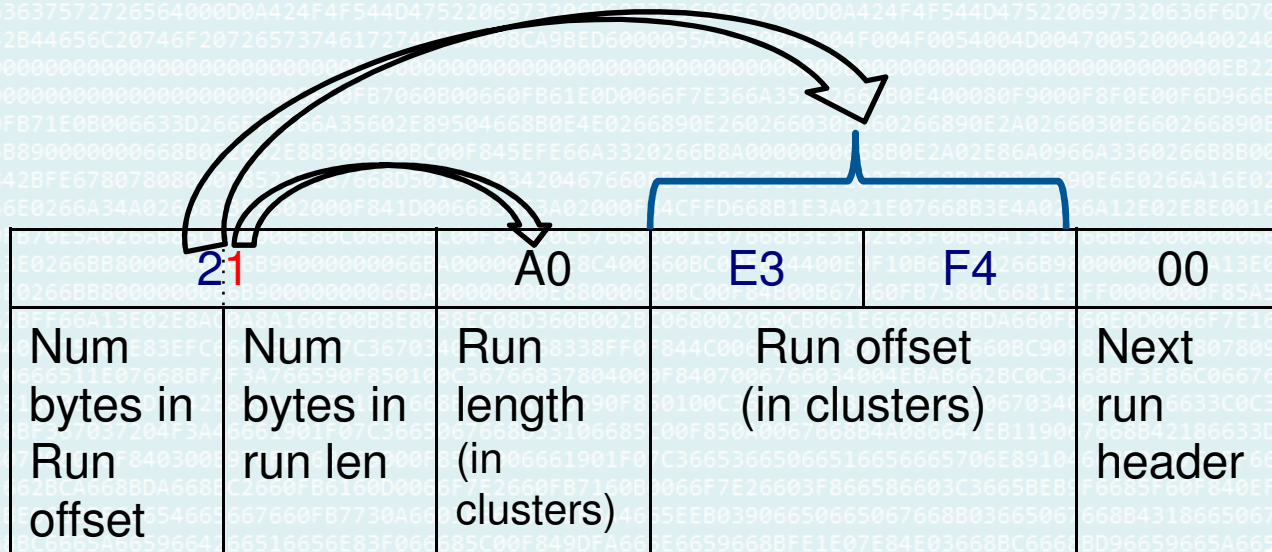
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Type ID				Attribute Length				Form code	name len	Name offset		flags		Atrib ID	
10	Start virtual cluster number								Ending virtual cluster number							
20	Runlist offset		Compres sion unit size		0x0000				Size of attribute content							
30	size on disk of attribute content								Initialized size of attribute content							
40	Data runlists															

Attrib ID starts from zero

Virtual cluster numbers are used when a MFT record is fragmented



# Data runlists



Run header

# Data runs, take 2

32 18 01 60 34 56 00

Run 1

Header = 0x32 = 2 byte len, 3 byte offset

Length = 0x0118

Offset = 0x563460

Start cluster = 0x563460, length of data =  
0x118 clusters

# \$Data

Standard header, with data run (if non resident)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Type ID 0x80				Attribute Length				Form code	name len	Name offset		flags		Atrib ID	
10	Start virtual cluster number								Ending virtual cluster number							
20	Runlist offset		Compres sion unit size		0x0000				Size of attribute content							
30	size on disk of attribute content								Initialized size of attribute content							
40	Data runlists															

# Practice

Non  
Resident

Type ID  
0x80, Data

Attrib Length  
0x48

VCN end

VCN start

Run list offset

Size: 0x1000  
= 4096 bytes  
= 1KiB

Run list  
Header = 11  
Run length = 0x01 (1 cluster)  
Run offset = 0x02 (cluster 2)





# Your turn 4

Find the contents of the file named  
“small\_file.txt” in PFIC\_02.001

Hint: it is MFT record number 0x23

# Resident Data

Resident

Data size

Type ID  
0x80, Data

Attrib Length  
0x48

Content offset

01FEDD70	6C 00 6C 00 5F 00 66 00 69 00 6C 00 65 00 2E 00	1 1 - f
01FEDD80	74 00 78 00 74 00 00 00 80 00 00 00 28 00 00 00	t x t
01FEDD90	00 00 18 00 00 00 01 00 0F 00 00 00 18 00 00 00	
01FEDDA0	73 6F 6D 65 20 73 68 6F 72 74 20 74 65 78 74 00	some short text
01FEDDB0	FF FF FF FF 82 79 47 11 00 00 00 00 00 00 00 00	yyyylyG
01FEDDC0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

16 bytes of content



# Your turn 5

Find the file named “big\_file.txt” in  
PFIC\_02.001

Hint: it is MFT record number 0x24

# Non Resident data

Type ID  
0x80, Data

Attrib Length  
0x48

Non  
Resident

```

01FEE110 80 00 00 00 48 00 00 00 01 00 00 00 00 00 01 00
01FEE120 00 00 00 00 00 00 00 00 0C 00 00 00 00 00 00 00
01FEE130 40 00 00 00 00 00 00 00 00 D0 00 00 00 00 00 00
01FEE140 58 C0 00 00 00 00 00 00 58 C0 00 00 00 00 00 00
01FEE150 21 0D 36 1F 00 00 00 00 FF FF FF FF 82 79 47 11
01FEE160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  
```

Run list offset

Size: 0xC058  
= 49,240 bytes  
= 48KiB

Run list

Header = 21

Run length = 0x0D (14 clusters, 53,248 bytes)

Run offset = 0x1F36

(= 1F36 x 200 x 8 = 0x1F36000)



# Additional Challenges

- PFIC\_03.001
- Find:
  - Compressed directory and file
  - Directory with permissions set
  - Hidden directory
  - A directory that has been renamed



# Thank you

- Todays exercises are at:

<http://www.writeblocked.org>