SOGETI

YOLO (F:)
Tap to choose what happens with removable drives.

# NTFS: Forensics, malwares and vulnerabilities

*Who said that recoding the wheel is useless ?*

Stéfan Le Berre (Heurs)

# Why speaking about NTFS ?

**A little story**

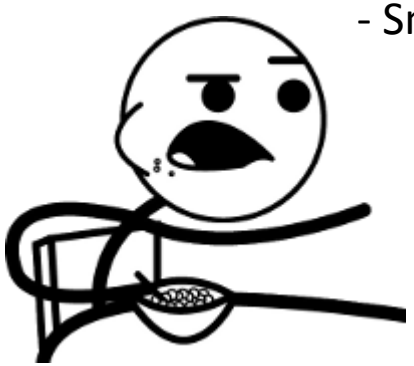
- Hey bro ! For the malware hunting we can't trust the kernel when we ask him to list a directory?

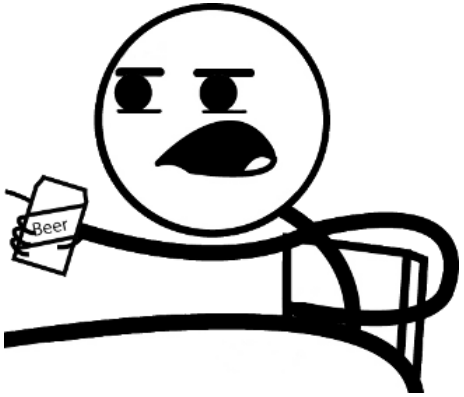
- No of course... But we can have a raw access to the FileSystem right?

- Yes, but we will not dump the MFT, it's too large!

- Yes, I agree... We should to recode a MFT parser to diff a standard list result with a raw list result...

- Smell like a bad idea...





# Why to speak about NTFS ?

A little story

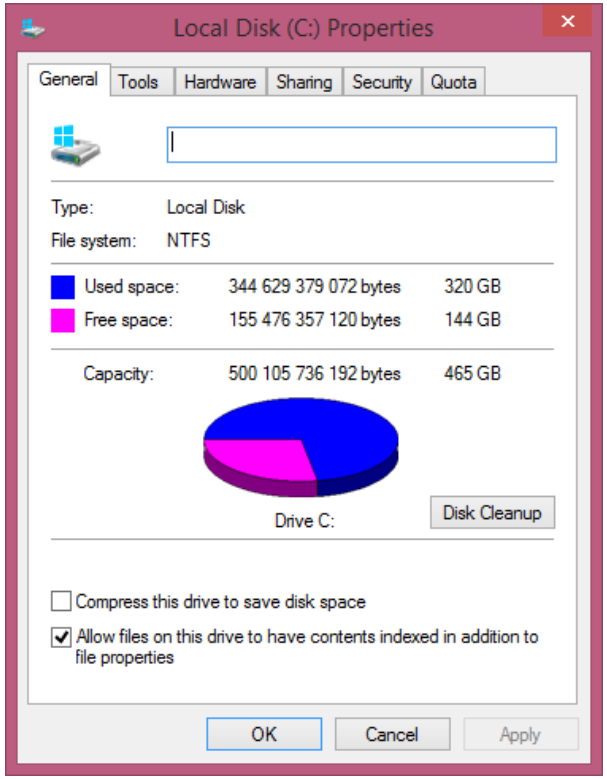
WORST IDEA EVER!


*At this moment it's gone to shit*

# What is NTFS ?

- FileSystem introduced with Windows NT 3.1, 1993
- Never stop to evolve

Everybody use it, do you understand how it works?



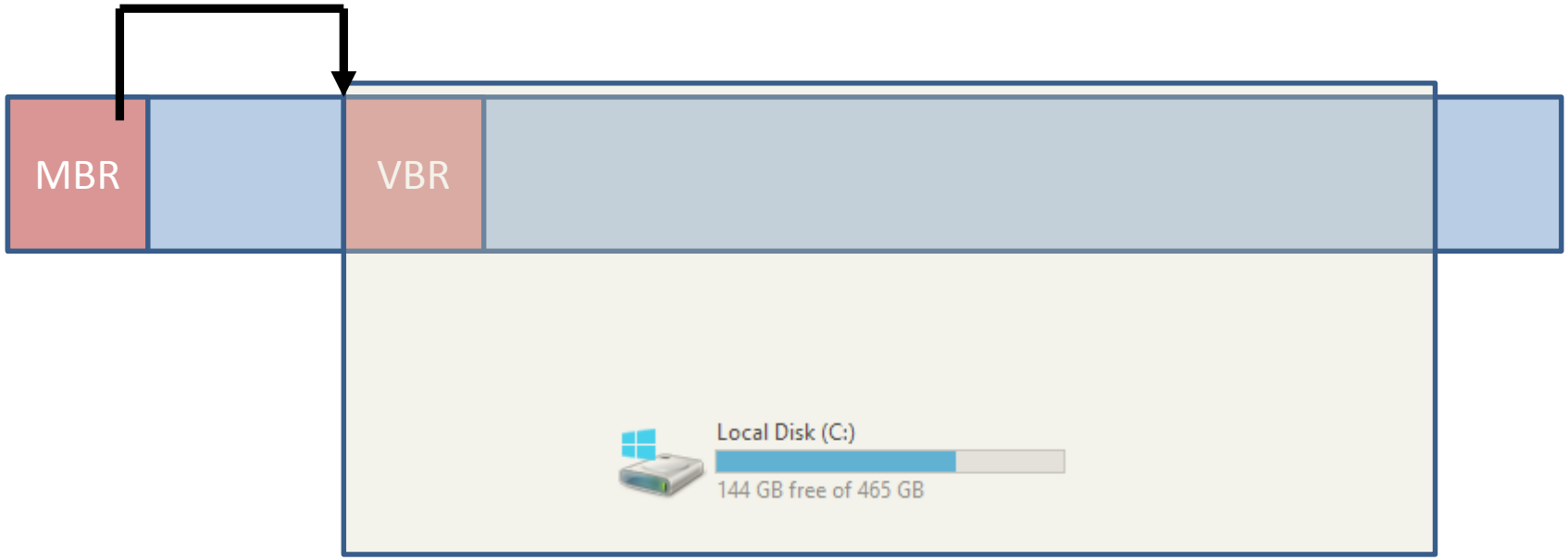
# What is NTFS ?

- No official documentation (thanks MS)
- ~130p of unofficial documentation

And what do I have to debug and read a NTFS volume ?

A hexa editor (woot \o/ )

# NTFS – MBR -> VBR



# NTFS - VBR

Ok cool, we start by opening "c:"

```
EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00   ëR.NTFS    .....
00 00 00 00 00 F8 00 00 3F 00 FF 00 00 08 00 00   .....ø..?.ÿ.....
00 00 00 00 80 00 80 00 FF 4F 38 3A 00 00 00 00   ....€.€.ÿO8:....
00 00 0C 00 00 00 00 00 02 00 00 00 00 00 00 00   ................
F6 00 00 00 01 00 00 00 70 E7 E9 62 10 EA 62 E4   ö.......pçéb.êbä
00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07   ....ú3ÀŽÐ¼.|ûhÀ.
1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E   ..hf.Ëˆ...f.>..N
54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB   TFSu.´A»ªUÍ.r..û
55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC   Uªu.÷Á..u.éÝ..ƒì
18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13   .h..´HŠ...‹ô..Í.
9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3   ŸƒÄ.žX.rá;...uÛ£
0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8   ..Á.....Z3Û¹. +È
66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8   fÿ.......ŽÂÿ...è
4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D   K.+Èwï¸.»Í.f#Àu-
66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16   f.ûTCPAu$.ù..r..
68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66   h.».hR..h..fSfSf
55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF   U...h¸.fa..Í.3À¿
0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E   ..¹ö.üóªéþ...f`.
06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00   .f¡..f.....fh...
00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E   .fP.Sh..h..´BŠ..
00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F   ...‹ôÍ.fY[ZfYfY.
0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF   .‚..fÿ.......ŽÂÿ
0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00   ...u¼..faÃ¡ö.è..
A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09   ¡ú.è..ôëý‹ð¬<.t.
B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69   ´.»..Í.ëòÃ..A di
73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63   sk read error oc
63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52   curred...BOOTMGR
20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D    is compressed..
0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B   .Press Ctrl+Alt+
44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A   Del to restart..
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 8A 01 A7 01 BF 01 00 00 55 AA   ......Š.§.¿...Uª
```

# NTFS - VBR

MFT entry

sector size

sectors per cluster

Executable code

total sectors

Signature

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 000h: | EB | 52 | 90 | 4E | 54 | 46 | 53 | 20 | 20 | 20 | 20 | 00 | 02 | 08 | 00 | 00 | ëR.NTFS ....  |
| 010h: | 00 | 00 | 00 | 00 | 00 | F8 | 00 | 00 | 3F | 00 | FF | 00 | 00 | 08 | 00 | 00 | .....ø..?.ÿ..... |
| 020h: | 00 | 00 | 00 | 00 | 80 | 00 | 80 | 00 | FF | 4F | 38 | 3A | 00 | 00 | 00 | 00 | ....€.€.ÿO8:.... |
| 030h: | 00 | 00 | 0C | 00 | 00 | 00 | 00 | 00 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 040h: | F6 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 70 | E7 | E9 | 62 | 10 | EA | 62 | E4 | ö.....pçéb.êbä |
| 050h: | 00 | 00 | 00 | 00 | FA | 33 | C0 | 8E | D0 | BC | 00 | 7C | FB | 68 | C0 | 07 | ....ú3ÀŽÐ¼.\|ûhÀ. |
| 060h: | 1F | 1E | 68 | 66 | 00 | CB | 88 | 16 | 0E | 00 | 66 | 81 | 3E | 03 | 00 | 4E | ..hf.Ëˆ...f.>..N |
| 070h: | 54 | 46 | 53 | 75 | 15 | B4 | 41 | BB | AA | 55 | CD | 13 | 72 | 0C | 81 | FB | TFSu.´A»ªUÍ.r..û |
| 080h: | 55 | AA | 75 | 06 | F7 | C1 | 01 | 00 | 75 | 03 | E9 | DD | 00 | 1E | 83 | EC | Uªu.÷Á..u.éÝ..ƒì |
| 090h: | 18 | 68 | 1A | 00 | B4 | 48 | 8A | 16 | 0E | 00 | 8B | F4 | 16 | 1F | CD | 13 | .h..´HŠ...‹ô..Í. |
| 0A0h: | 9F | 83 | C4 | 18 | 9E | 58 | 1F | 72 | E1 | 3B | 06 | 0B | 00 | 75 | DB | A3 | ŸƒÄ.žX.rá;...uÛ£ |
| 0B0h: | 0F | 00 | C1 | 2E | 0F | 00 | 04 | 1E | 5A | 33 | DB | B9 | 00 | 20 | 2B | C8 | ..Á.....Z3Û¹. +È |
| 0C0h: | 66 | FF | 06 | 11 | 00 | 03 | 16 | 0F | 00 | 8E | C2 | FF | 06 | 16 | 00 | E8 | fÿ.....ŽÂÿ...è |
| 0D0h: | 4B | 00 | 2B | C8 | 77 | EF | B8 | 00 | BB | CD | 1A | 66 | 23 | C0 | 75 | 2D | K.+Èwï¸.»Í.f#Àu- |
| 0E0h: | 66 | 81 | FB | 54 | 43 | 50 | 41 | 75 | 24 | 81 | F9 | 02 | 01 | 72 | 1E | 16 | f.ûTCPAu$.ù..r.. |
| 0F0h: | 68 | 07 | BB | 16 | 68 | 52 | 11 | 16 | 68 | 09 | 00 | 66 | 53 | 66 | 53 | 66 | h.».hR..h..fSfSf |
| 100h: | 55 | 16 | 16 | 16 | 68 | B8 | 01 | 66 | 61 | 0E | 07 | CD | 1A | 33 | C0 | BF | U...h¸.fa..Í.3À¿ |
| 110h: | 0A | 13 | B9 | F6 | 0C | FC | F3 | AA | E9 | FE | 01 | 90 | 90 | 66 | 60 | 1E | ..¹ö.üóªéþ...f`. |
| 120h: | 06 | 66 | A1 | 11 | 00 | 66 | 03 | 06 | 1C | 00 | 1E | 66 | 68 | 00 | 00 | 00 | .f¡..f.....fh... |
| 130h: | 00 | 66 | 50 | 06 | 53 | 68 | 01 | 00 | 68 | 10 | 00 | B4 | 42 | 8A | 16 | 0E | .fP.Sh..h..´BŠ.. |
| 140h: | 00 | 16 | 1F | 8B | F4 | CD | 13 | 66 | 59 | 5B | 5A | 66 | 59 | 66 | 59 | 1F | ...‹ôÍ.fY[ZfYfY. |
| 150h: | 0F | 82 | 16 | 00 | 66 | FF | 06 | 11 | 00 | 03 | 16 | 0F | 00 | 8E | C2 | FF | .‚..fÿ.....ŽÂÿ |
| 160h: | 0E | 16 | 00 | 75 | BC | 07 | 1F | 66 | 61 | C3 | A1 | F6 | 01 | E8 | 09 | 00 | ...u¼..faÃ¡ö.è.. |
| 170h: | A1 | FA | 01 | E8 | 03 | 00 | F4 | EB | FD | 8B | F0 | AC | 3C | 00 | 74 | 09 | ¡ú.è..ôëý‹ð¬<.t. |
| 180h: | B4 | 0E | BB | 07 | 00 | CD | 10 | EB | F2 | C3 | 0D | 0A | 41 | 20 | 64 | 69 | ´.»..Í.ëòÃ..A di |
| 190h: | 73 | 6B | 20 | 72 | 65 | 61 | 64 | 20 | 65 | 72 | 72 | 6F | 72 | 20 | 6F | 63 | sk read error oc |
| 1A0h: | 63 | 75 | 72 | 72 | 65 | 64 | 00 | 0D | 0A | 42 | 4F | 4F | 54 | 4D | 47 | 52 | curred...BOOTMGR |
| 1B0h: | 20 | 69 | 73 | 20 | 63 | 6F | 6D | 70 | 72 | 65 | 73 | 73 | 65 | 64 | 00 | 0D | is compressed.. |
| 1C0h: | 0A | 50 | 72 | 65 | 73 | 73 | 20 | 43 | 74 | 72 | 6C | 2B | 41 | 6C | 74 | 2B | .Press Ctrl+Alt+ |
| 1D0h: | 44 | 65 | 6C | 20 | 74 | 6F | 20 | 72 | 65 | 73 | 74 | 61 | 72 | 74 | 0D | 0A | Del to restart.. |
| 1E0h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 1F0h: | 00 | 00 | 00 | 00 | 00 | 00 | 8A | 01 | A7 | 01 | BF | 01 | 00 | 00 | 55 | AA | .....Š.§.¿...Uª |

(0x3a384fff * 512)/1024/1024/1024 = 465 (total size)

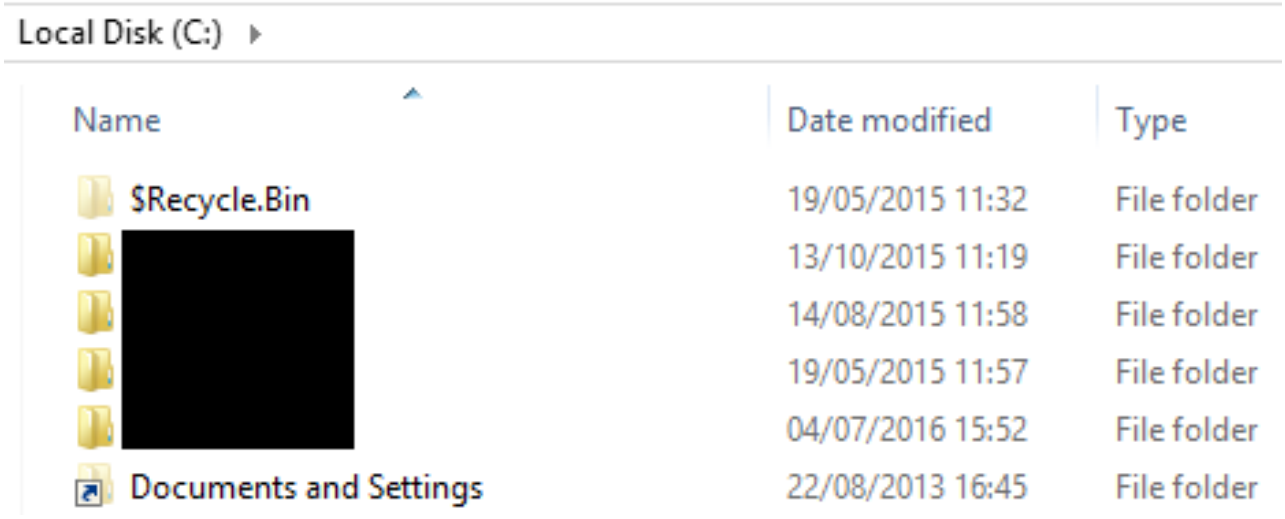
0xc0000*(0x200 * 8) = 0xc0000000 (MFT entry) (l'entry is after 3Go)

# NTFS – MFT basics

- Each MFT node's size is 1024 bytes
- Each node is a file
- Node 96 = MFT Entry + 96*1024 (but not always)
- If a file can be stored inside a node, it's done
- All nodes from 0 to 31 are reserved for NTFS internals management

# NTFS – Organisation

- How we see a NTFS volume with explorer.



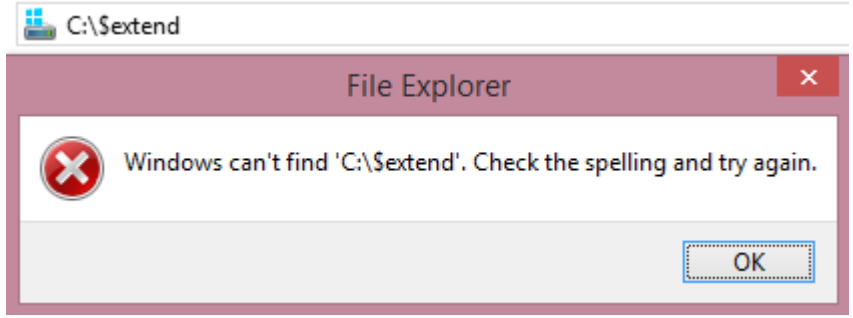
# NTFS – Organisation

- When we see with a raw NTFS crawler:

```
parseNTFS.py -ls C:\
      0000-00-00 00:00:00              0 $attrdef (4)
      0000-00-00 00:00:00              0 $badclus (8)
      0000-00-00 00:00:00              0 $bitmap (6)
      0000-00-00 00:00:00              0 $boot (7)
<DIR> 2015-05-04 18:55:38              0 $extend (11)
      0000-00-00 00:00:00              0 $logfile (2)
      2015-05-04 18:55:38          16384 $mft (0)
      0000-00-00 00:00:00              0 $mftmirr (1)
<DIR> 2015-05-19 09:32:01              0 $recycle.bin (57)
      2015-05-04 18:55:38              0 $secure (9)
      0000-00-00 00:00:00              0 $upcase (10)
      0000-00-00 00:00:00              0 $volume (3)
<DIR> 2016-07-01 14:32:39              0 . (5)
```

Not a NTFS internal directory

# NTFS – Organisation




```
parseNTFS.py -ls C:\$extend
      2015-05-04 18:55:39                0 $objid (25)
      2015-05-04 18:55:39                0 $quota (24)
      2015-05-04 18:55:39                0 $reparse (26)
<DIR> 2015-05-04 18:55:39                0 $rmmetadata (27)
      2015-05-04 09:01:15                0 $usnjrnl (75483)
```

Special case, not use for internal management but internal logs

# NTFS – Node

Each file have an uniq ID.

Here we see the node ID 0.

```
:0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
:0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
:0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
:0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Û¢ÿÿ........`...
:0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
:0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
:0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
:0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
:0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
:0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
:00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
:00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  .........….é›†Ð.
:00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
:00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  .….é›†Ð..@......
:00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
:00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
:0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
:0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
:0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
:0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
:0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
:0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
:0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
:0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @........à......
:0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
:0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
:01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
:01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
:01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
:01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @........ ......
:01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
:01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛ¢
:0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
:0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
:0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

[0:4] = Magic (FILE)

[4:6] = UPD Offset

[6:8] = UPD Size

[0x14:0x16] : Offset First Attrib

[0x20:0x28] : ID (File Ref)

[0x16:0x18] : Flags (Used/Dir)

```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00   FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00   ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00   ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00   Ûcÿÿ........`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00   ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01   .….é›†Ð.….é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01   .….é›†Ð.….é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00   ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00   ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00   ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01   .........….é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01   .….é›†Ð.….é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00   .….é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00   .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00   ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00   €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00   ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00   @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00   ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF   2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00   °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00   ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00   @........à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00   .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00   1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00   ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00   ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00   ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00   @........ ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00   ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2   1.ÿÿ...ÿ.½ˆ..àÛc
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00   ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

# NTFS – Node

Each node have an integrity check system.

If:

[0x30:0x32] == [0x1FE:0x200]

[0x30:0x32] == [0x3FE:0x400]

```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Ûcÿÿ....    ....`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  ..........….é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  .….é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @.......à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @.......  ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛc
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

# NTFS – Node

Each node have an integrity check system.

If:

[0x30:0x32] == [0x1FE:0x200]

[0x30:0x32] == [0x3FE:0x400]

Store:

[0x32:0x34] -> [0x1FE:0x200]

[0x34:0x36] -> [0x3FE:0x400]

```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Ûcÿÿ....    ....`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  .........….é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  .….é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @.......à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @.......  ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛc
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

# NTFS – Node

[4:8] = Size

[0:4] = Type

[8] = 0:Resident/1:Non-Resid

[9] = Name Len

[0xa:0xc] = Name Offset

```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Ûcÿÿ........`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð.….é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð.….é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  .........….é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð.….é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  .….é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @........à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @........ ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛc
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

# NTFS – Node

Resident header (0)

[0x10:0x14] = Datas Size

[0x14:0x16] = Offset

```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Ûcÿÿ....    ....`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  .........….é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..….é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  .….é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @........à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @.......  ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛc
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

# NTFS – Node

[0x18:0x20] End VCN

Non-Resident header (1)

[0xc:0xa] Flags (compress, crypt, ...)

[0x10:0x18] Start VCN

[0x20:0x22] **DataRuns** Offset

```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Ûcÿÿ....    ....`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð.….é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð.….é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  .........….é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð.….é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  .….é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @........à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @.......  ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛc
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

# NTFS – Node


## DataRuns :

(from now we won't count with bytes but with nibbles, 1 byte = 2 nibbles)

[0](F) = Size of the Offset field

[1](L) = Size of the Length field

[2] = Length of the run (L * 2)

[2+2*L] = Offset to the starting LCN of the previous element (F * 2)

LCNs (dynamic size) have a relative address...

# NTFS – Node


## DataRuns :

Runlist:

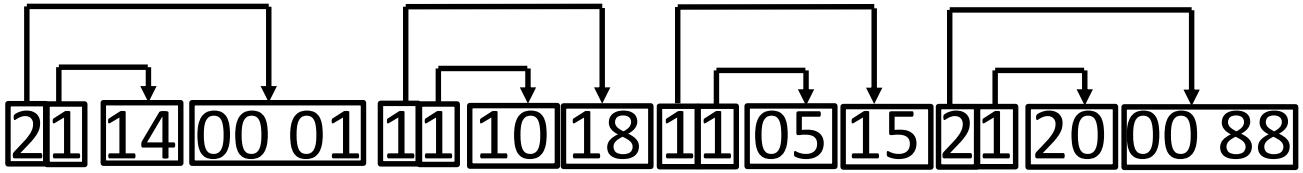
21 14 00 01 11 10 18 11 05 15 21 20 00 88

# NTFS – Node


## DataRuns :

Runlist:

21 14 00 01 11 10 18 11 05 15 21 20 00 88




Decode

read 0x14 bytes at 0x100 21 0x100, 0x14

read 0x10 bytes at + 0x18 11 0x18, 0x10

read 0x05 bytes at + 0x15 11 0x15, 0x05

read 0x20 bytes at - 30720 21 0x8800, 0x20

# NTFS – Node

Types :

**$STANDARD_INFORMATION (0x10)**

$ATTRIBUTE_LIST (0x20)

**$FILE_NAME (0x30)**

$OBJECT_ID (0x40)

$SECURITY_DESCRIPTOR (0x50)

$VOLUME_NAME (0x60)

$VOLUME_INFORMATION (0x70)

**$DATA (0x80)**

**$INDEX_ROOT (0x90)**

**$INDEX_ALLOCATION (0xA0)**

$BITMAP (0xB0)

**$REPARSE_POINT (0xC0)**

$EA_INFORMATION (0xD0)

$EA (0xE0)

$LOGGED_UTILITY_STREAM (0x100)

```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Û¢ÿÿ....    ....`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..…é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..…é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  ..........…é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  .….é›†Ð..…é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  .….é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @........à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @........ ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛ¢
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

# NTFS – Node

**$STANDARD_INFORMATION (0x10)**

[8:0x10] = Altered Time

[0:8] = Create Time

[0x10:0x18] = MFT Change

[0x18:0x20] = Read Time

[0x20:0x24] = DOS File Permissions

```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Û¢ÿÿ....`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  ....é›†Ð.....é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  ....é›†Ð.....é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  ..........….é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  ....é›†Ð.....é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  ....é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @........à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @........ ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛ¢
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

**$FILE_NAME (0x30)**

[0:8] = Parent Ref (6 + 2)

[8:0x10] = Create Time

[0x10:0x18] = Altered Time

[0x18:0x20] = Modif Time

[0x20:0x28] = Read Time

[0x28:0x30] = Alloc size of the file

[0x30:0x38] = Real size of the file

[0x38:0x3c] = Flags (Dir, compress, ...)

[0x40] (L) = File name length

[0x42:0x42+L*2] = File Name

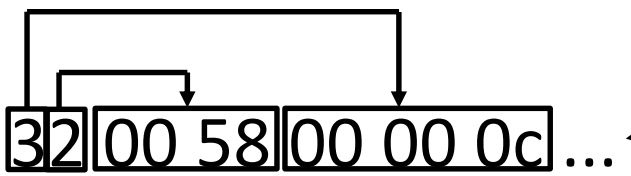
```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Û¢ÿÿ....`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  ....é›†Ð.....é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  ....é›†Ð.....é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  ..........é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  ....é›†Ð.....é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  ....é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @........à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @........ ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛ¢
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

# NTFS – Node

**$DATA (0x80)**

Non Resident Flag !

Datas of the file, are described with **Dataruns**.




```
0000h: 46 49 4C 45 30 00 03 00 99 71 10 5F 0F 00 00 00  FILE0...™q._....
0010h: 01 00 01 00 38 00 01 00 A0 01 00 00 00 04 00 00  ....8... .......
0020h: 00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00  ................
0030h: DB A2 FF FF 00 00 00 00 10 00 00 00 60 00 00 00  Û¢ÿÿ....`...
0040h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00  ........H.......
0050h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  ....é›†Ð.....é›†Ð.
0060h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  ....é›†Ð.....é›†Ð.
0070h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ................
0090h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00  ........0...h...
00A0h: 00 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00  ........J.......
00B0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01  ..........….é›†Ð.
00C0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01  ....é›†Ð.....é›†Ð.
00D0h: 0F 85 07 E9 9B 86 D0 01 00 40 00 00 00 00 00 00  ....é›†Ð..@......
00E0h: 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 00  .@..............
00F0h: 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00  ..$.M.F.T.......
0100h: 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00  €...P.....@.....
0110h: 00 00 00 00 00 00 00 00 FF 98 03 00 00 00 00 00  ........ÿ˜......
0120h: 40 00 00 00 00 00 00 00 00 00 90 39 00 00 00 00  @..........9....
0130h: 00 00 90 39 00 00 00 00 00 00 90 39 00 00 00 00  ...9.......9....
0140h: 32 00 58 00 00 0C 43 00 41 03 94 85 57 02 00 FF  2.X...C.A.”…W..ÿ
0150h: B0 00 00 00 48 00 00 00 01 00 40 00 00 00 05 00  °...H.....@.....
0160h: 00 00 00 00 00 00 00 00 1D 00 00 00 00 00 00 00  ................
0170h: 40 00 00 00 00 00 00 00 00 E0 01 00 00 00 00 00  @........à......
0180h: 08 D0 01 00 00 00 00 00 08 D0 01 00 00 00 00 00  .Ð.......Ð......
0190h: 31 1E A7 22 11 00 00 00 FF FF FF FF 00 00 00 00  1.§"....ÿÿÿÿ....
01A0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01B0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01C0h: FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00  ÿÿÿÿ....ÿÿÿÿ....
01D0h: 40 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00  @........ ......
01E0h: 08 10 00 00 00 00 00 00 08 10 00 00 00 00 00 00  ................
01F0h: 31 01 FF FF 0B 11 01 FF 00 BD 88 03 00 E0 DB A2  1.ÿÿ...ÿ.½ˆ..àÛ¢
0200h: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ÿÿÿÿ............
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

# NTFS – Node

**$INDEX_ROOT (0x90)**

[8:0xc] = Size of Index Allocation Entry

[0x10:0x14] = Offset to first Index Entry

[0x18:0x1c] = Allocated size of the Index Entries

[0x1c] = Flags (Small Index / Large Index)

"$I30" <- Indicate a directory

Succession of INDEX_ENTRY

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
2C00h: 46 49 4C 45 30 00 03 00 BD 04 3C 08 00 00 00 00   FILE0...¼.<.....
2C10h: 0B 00 01 00 38 00 03 00 50 03 00 00 00 04 00 00   ....8...P.......
2C20h: 00 00 00 00 00 00 00 00 05 00 00 00 0B 00 00 00   ................
2C30h: 0B 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00   ............`...
2C40h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00   ........H.......
2C50h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01   .….é›†Ð..….é›†Ð.
2C60h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01   .….é›†Ð..….é›†Ð.
2C70h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2C80h: 00 00 00 00 01 01 00 00 00 00 00 00 00 00 00 00   ................
2C90h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00   ........0...h...
2CA0h: 00 00 00 00 00 00 03 00 50 00 00 00 18 00 01 00   ........P.......
2CB0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01   ..........….é›†Ð.
2CC0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01   .….é›†Ð..….é›†Ð.
2CD0h: 0F 85 07 E9 9B 86 D0 01 00 00 00 00 00 00 00 00   .….é›†Ð.........
2CE0h: 00 00 00 00 00 00 00 00 06 00 00 10 00 00 00 00   ................
2CF0h: 07 03 24 00 45 00 78 00 74 00 65 00 6E 00 64 00   ..$.E.x.t.e.n.d.
2D00h: 90 00 00 00 48 02 00 00 00 04 18 00 00 00 04 00   ....H...........
2D10h: 28 02 00 00 28 00 00 00 24 00 49 00 33 00 30 00   (... . .$.I.3.0.
2D20h: 30 00 00 00 01 00 00 00 00 10 00 00 01 00 00 00   0...............
2D30h: 10 00 00 00 18 02 00 00 18 02 00 00 00 00 00 00   ................
2D40h: 19 00 00 00 00 00 01 00 60 00 4E 00 00 00 00 00   ........`.N.....
2D50h: 0B 00 00 00 00 00 0B 00 07 F8 16 EA 9B 86 D0 01   .........ø.ê›†Ð.
2D60h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2D70h: 07 F8 16 EA 9B 86 D0 01 00 00 00 00 00 00 00 00   .ø.ê›†Ð.........
2D80h: 00 00 00 00 00 00 00 00 26 00 00 20 00 00 00 00   ........&.. ....
2D90h: 06 00 24 00 4F 00 62 00 6A 00 49 00 64 00 00 00   ..$.O.b.j.I.d...
2DA0h: 18 00 00 00 00 00 01 00 60 00 4E 00 00 00 00 00   ........`.N.....
2DB0h: 0B 00 00 00 00 00 0B 00 07 F8 16 EA 9B 86 D0 01   .........ø.ê›†Ð.
2DC0h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2DD0h: 07 F8 16 EA 9B 86 D0 01 00 00 00 00 00 00 00 00   .ø.ê›†Ð.........
2DE0h: 00 00 00 00 00 00 00 00 26 00 00 20 00 00 00 00   ........&.. ....
2DF0h: 06 00 24 00 51 00 75 00 6F 00 74 00 61 00 0B 00   ..$.Q.u.o.t.a...
2E00h: 1A 00 00 00 00 00 01 00 68 00 52 00 00 00 00 00   ........h.R.....
2E10h: 0B 00 00 00 00 00 0B 00 07 F8 16 EA 9B 86 D0 01   .........ø.ê›†Ð.
2E20h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2E30h: 07 F8 16 EA 9B 86 D0 01 00 00 00 00 00 00 00 00   .ø.ê›†Ð.........
2E40h: 00 00 00 00 00 00 00 00 26 00 00 20 00 00 00 00   ........&.. ....
2E50h: 08 00 24 00 52 00 65 00 70 00 61 00 72 00 73 00   ..$.R.e.p.a.r.s.
2E60h: 65 00 00 00 00 00 00 00 1B 00 00 00 00 00 01 00   e...............
2E70h: 68 00 58 00 00 00 00 00 0B 00 00 00 00 00 0B 00   h.X.............
2E80h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2E90h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2EA0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2EB0h: 06 00 00 10 00 00 00 00 0B 00 24 00 52 00 6D 00   ..........$.R.m.
2EC0h: 4D 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00   M.e.t.a.d.a.t.a.
2ED0h: DB 26 01 00 00 00 02 00 68 00 52 00 00 00 00 00   Û&......h.R.....
2EE0h: 0B 00 00 00 00 00 0B 00 9A CF 49 E0 48 86 D0 01   ........šÏIàH†Ð.
2EF0h: 9A CF 49 E0 48 86 D0 01 9A CF 49 E0 48 86 D0 01   šÏIàH†Ð.šÏIàH†Ð.
2F00h: 9A CF 49 E0 48 86 D0 01 00 00 00 00 00 00 00 00   šÏIàH†Ð.........
2F10h: 00 00 00 00 00 00 00 00 26 02 00 00 00 00 00 00   ........&.......
2F20h: 08 00 24 00 55 00 73 00 6E 00 4A 00 72 00 6E 00   ..$.U.s.n.J.r.n.
2F30h: 6C 00 61 00 74 00 61 00 00 00 00 00 00 00 00 00   l.a.t.a.........
2F40h: 10 00 00 00 02 00 00 00 FF FF FF FF 00 00 00 00   ........ÿÿÿÿ....
```

[8:0xa] = Size of the entry

[0x0:0x8] = Ref, inode (6 + 2)

**$INDEX_ROOT (0x90)**

INDEX_ENTRY

[0x10:0x18] = Parent ref, inode (6 + 2)

[0x18:0x20] = Create Time

[0x20:0x28] = Modif Time

[0x28:0x30] = FILE record modif

[0x30:0x38] = Access Time

[0x40:0x48] = Real file size

[0x38:0x40] = Allocated file size

[0x50] = File name length

[0x52:0x52+L*2] = File Name

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
2C00h: 46 49 4C 45 30 00 03 00 BD 04 3C 08 00 00 00 00   FILE0...¼.<.....
2C10h: 0B 00 01 00 38 00 03 00 50 03 00 00 00 04 00 00   ....8...P.......
2C20h: 00 00 00 00 00 00 00 00 05 00 00 00 0B 00 00 00   ................
2C30h: 0B 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00   ............`...
2C40h: 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00   ........H.......
2C50h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01   .….é›†Ð..….é›†Ð.
2C60h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01   .….é›†Ð..….é›†Ð.
2C70h: 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2C80h: 00 00 00 00 01 01 00 00 00 00 00 00 00 00 00 00   ................
2C90h: 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00   ........0...h...
2CA0h: 00 00 00 00 00 00 03 00 50 00 00 00 18 00 01 00   ........P.......
2CB0h: 05 00 00 00 00 00 05 00 0F 85 07 E9 9B 86 D0 01   ........….é›†Ð.
2CC0h: 0F 85 07 E9 9B 86 D0 01 0F 85 07 E9 9B 86 D0 01   .….é›†Ð..….é›†Ð.
2CD0h: 0F 85 07 E9 9B 86 D0 01 00 00 00 00 00 00 00 00   .….é›†Ð.........
2CE0h: 00 00 00 00 00 00 00 00 06 00 00 10 00 00 00 00   ................
2CF0h: 07 03 24 00 45 00 78 00 74 00 65 00 6E 00 64 00   ..$.E.x.t.e.n.d.
2D00h: 90 00 00 00 48 02 00 00 00 04 18 00 00 00 04 00   ....H...........
2D10h: 28 02 00 00 20 00 00 00 24 00 49 00 33 00 30 00   (... ...$.I.3.0.
2D20h: 30 00 00 00 01 00 00 00 00 10 00 00 01 00 00 00   0...............
2D30h: 10 00 00 00 18 02 00 00 18 02 00 00 00 00 00 00   ................
2D40h: 19 00 00 00 00 00 01 00 60 00 4E 00 00 00 00 00   ........`.N.....
2D50h: 0B 00 00 00 00 00 0B 00 07 F8 16 EA 9B 86 D0 01   .........ø.ê›†Ð.
2D60h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2D70h: 07 F8 16 EA 9B 86 D0 01 00 00 00 00 00 00 00 00   .ø.ê›†Ð.........
2D80h: 00 00 00 00 00 00 00 00 26 00 00 20 00 00 00 00   ........&.. ....
2D90h: 06 00 24 00 4F 00 62 00 6A 00 49 00 64 00 00 00   ..$.O.b.j.I.d...
2DA0h: 28 00 00 00 00 00 01 00 60 00 4E 00 00 00 00 00   ........`.N.....
2DB0h: 0B 00 00 00 00 00 0B 00 07 F8 16 EA 9B 86 D0 01   .........ø.ê›†Ð.
2DC0h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2DD0h: 07 F8 16 EA 9B 86 D0 01 00 00 00 00 00 00 00 00   .ø.ê›†Ð.........
2DE0h: 00 00 00 00 00 00 00 00 26 00 00 20 00 00 00 00   ........&.. ....
2DF0h: 06 00 24 00 51 00 75 00 6F 00 74 00 61 00 0B 00   ..$.Q.u.o.t.a...
2E00h: 1A 00 00 00 00 00 01 00 68 00 52 00 00 00 00 00   ........h.R.....
2E10h: 0B 00 00 00 00 00 0B 00 07 F8 16 EA 9B 86 D0 01   .........ø.ê›†Ð.
2E20h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2E30h: 07 F8 16 EA 9B 86 D0 01 00 00 00 00 00 00 00 00   .ø.ê›†Ð.........
2E40h: 00 00 00 00 00 00 00 00 26 00 00 20 00 00 00 00   ........&.. ....
2E50h: 08 00 24 00 52 00 65 00 70 00 61 00 72 00 73 00   ..$.R.e.p.a.r.s.
2E60h: 65 00 00 00 00 00 00 00 1B 00 00 00 00 00 01 00   e...............
2E70h: 68 00 58 00 00 00 00 00 0B 00 00 00 00 00 0B 00   h.X.............
2E80h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2E90h: 07 F8 16 EA 9B 86 D0 01 07 F8 16 EA 9B 86 D0 01   .ø.ê›†Ð..ø.ê›†Ð.
2EA0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2EB0h: 06 00 00 10 00 00 00 00 0B 00 24 00 52 00 6D 00   ..........$.R.m.
2EC0h: 4D 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00   M.e.t.a.d.a.t.a.
2ED0h: DB 26 01 00 00 00 02 00 68 00 52 00 00 00 00 00   Û&......h.R.....
2EE0h: 0B 00 00 00 00 00 0B 00 9A CF 49 E0 48 86 D0 01   ........šÏIàH†Ð.
2EF0h: 9A CF 49 E0 48 86 D0 01 9A CF 49 E0 48 86 D0 01   šÏIàH†Ð.šÏIàH†Ð.
2F00h: 9A CF 49 E0 48 86 D0 01 00 00 00 00 00 00 00 00   šÏIàH†Ð.........
2F10h: 00 00 00 00 00 00 00 00 26 02 00 00 00 00 00 00   ........&.......
2F20h: 08 00 24 00 55 00 73 00 6E 00 4A 00 72 00 6E 00   ..$.U.s.n.J.r.n.
2F30h: 6C 00 61 00 74 00 61 00 00 00 00 00 00 00 00 00   l.a.t.a.........
2F40h: 10 00 00 00 02 00 00 00 FF FF FF FF 00 00 00 00   ........ÿÿÿÿ....
```

[0:4] = Magic (INDX)

[4:6] = Offset to the Update Sequence

[6:8] = Size in words of the Update Sequence (in WORD)

**$INDEX_ALLOCATION (0xA0)**

Non Resident Flag !

There are **DataRuns**, goto INDX !

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2000h: | 49 | 4E | 44 | 58 | 28 | 00 | 09 | 00 | 4F | FF | 66 | 4C | 0E | 00 | 00 | 00 | INDX(...OÿfL.... |
| 2010h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 00 | 50 | 07 | 00 | 00 | .....@...P... |
| 2020h: | E8 | 0F | 00 | 00 | 00 | 00 | 00 | 00 | 9F | 03 | 05 | 00 | 05 | 00 | 00 | 00 | è.....Ÿ..... |
| 2030h: | 00 | 00 | D0 | 01 | 00 | 00 | D1 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..Ð...Ñ..... |
| 2040h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 2050h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 04 | 00 | 00 | 00 | 00 | 00 | 04 | 00 | ..... |
| 2060h: | 68 | 00 | 52 | 00 | 00 | 00 | 00 | 00 | 05 | 00 | 00 | 00 | 00 | 00 | 05 | 00 | h.R..... |
| 2070h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 2080h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 2090h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 20A0h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 08 | 03 | 24 | 00 | 41 | 00 | 74 | 00 | .....$.A.t. |
| 20B0h: | 74 | 00 | 72 | 00 | 44 | 00 | 65 | 00 | 66 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | t.r.D.e.f..... |
| 20C0h: | 08 | 00 | 00 | 00 | 00 | 00 | 08 | 00 | 68 | 00 | 52 | 00 | 00 | 00 | 00 | 00 | .....h.R..... |

[0x20:0x24] = Allocated size of the Index Entries

[0x1c:0x20] = Size of Index Entries

[0x18:0x1c] = Offset to the Index Entries + 0x18

After: List of INDEX_ENTRY

# NTFS – Node

**$REPARSE_POINT (0xC0)**

Symbolic links!

[0xe:0x10] = Path Size

[0xc:0xe] = Full path Size

Here:

File name: C:\Users\All Users

Redirection: C:\ProgramData

```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
:F800h: 46 49 4C 45 30 00 03 00 55 71 71 03 00 00 00 00   FILE0...Uqq.....
:F810h: 01 00 02 00 38 00 03 00 48 02 00 00 00 04 00 00   ....8...H.......
:F820h: 00 00 00 00 00 00 00 00 06 00 00 00 3E 73 00 00   ............>s..
:F830h: 3F 00 3A 00 00 00 00 00 10 00 00 00 60 00 00 00   ?.:.......`...
:F840h: 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00   ........H.......
:F850h: 41 CC BF 4C 46 9F CE 01 41 CC BF 4C 46 9F CE 01   AÌ¿LFŸÎ.AÌ¿LFŸÎ.
:F860h: B1 5F 3B FA 9B 86 D0 01 41 CC BF 4C 46 9F CE 01   ±_;ú›†Ð.AÌ¿LFŸÎ.
:F870h: 06 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .$..............
:F880h: 00 00 00 00 3A 02 00 00 00 00 00 00 00 00 00 00   ....:...........
:F890h: 00 00 00 00 00 00 00 00 30 00 00 00 70 00 00 00   ........0...p...
:F8A0h: 00 00 00 00 00 00 05 00 52 00 00 00 18 00 01 00   ........R.......
:F8B0h: F1 07 00 00 00 00 01 00 41 CC BF 4C 46 9F CE 01   ñ.......AÌ¿LFŸÎ.
:F8C0h: 41 CC BF 4C 46 9F CE 01 0B A4 3A FA 9B 86 D0 01   AÌ¿LFŸÎ..¤:ú›†Ð.
:F8D0h: 41 CC BF 4C 46 9F CE 01 00 00 00 00 00 00 00 00   AÌ¿LFŸÎ.........
:F8E0h: 00 00 00 00 00 00 00 00 06 24 00 10 0C 00 00 A0   .........$.....
:F8F0h: 08 02 41 00 4C 00 4C 00 55 00 53 00 45 00 7E 00   ..A.L.L.U.S.E.~.
:F900h: 31 00 73 00 00 00 00 00 30 00 00 00 70 00 00 00   1.s.....0...p...
:F910h: 00 00 00 00 00 00 02 00 54 00 00 00 18 00 01 00   ........T.......
:F920h: F1 07 00 00 00 00 01 00 9E 41 38 FA 9B 86 D0 01   ñ.......žA8ú›†Ð.
:F930h: 9E 41 38 FA 9B 86 D0 01 9E 41 38 FA 9B 86 D0 01   žA8ú›†Ð.žA8ú›†Ð.
:F940h: 9E 41 38 FA 9B 86 D0 01 00 00 00 00 00 00 00 00   žA8ú›†Ð.........
:F950h: 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00   ................
:F960h: 09 01 41 00 6C 00 6C 00 20 00 55 00 73 00 65 00   ..A.l.l. .U.s.e.
:F970h: 72 00 73 00 00 00 00 00 90 00 00 00 50 00 00 00   r.s.....P...
:F980h: 00 04 18 00 00 00 01 00 30 00 00 00 20 00 00 00   ........0... ...
:F990h: 24 00 49 00 33 00 30 00 30 00 00 00 01 00 00 00   $.I.3.0.0.......
:F9A0h: 00 10 00 00 01 00 00 00 10 00 00 00 20 00 00 00   ............ ...
:F9B0h: 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ...............
:F9C0h: 10 00 00 00 02 00 00 00 60 00 00 00 78 00 00 00   ........`...x...
:F9D0h: 00 00 00 00 00 00 04 00 5A 00 00 00 18 00 00 00   ........Z.......
:F9E0h: 0C 00 00 A0 52 00 00 00 00 00 24 00 26 00 1C 00   ... R.....$.&...
:F9F0h: 00 00 00 00 5C 00 3F 00 3F 00 5C 00 43 00 3F 00   ....\.?.?.\.C.?.
:FA00h: 5C 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00   \.P.r.o.g.r.a.m.
:FA10h: 44 00 61 00 74 00 61 00 00 00 43 00 3A 00 5C 00   D.a.t.a...C.:.\.
:FA20h: 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00 44 00   P.r.o.g.r.a.m.D.
:FA30h: 61 00 74 00 61 00 00 00 00 00 FF FF 82 79 47 11   a.t.a.....ÿÿ,yG.
:FA40h: FF FF FF FF 82 79 47 11 00 00 00 00 00 00 00 00   ÿÿÿÿ,yG.........
```

# NTFS – Forensics

## Unused nodes:

When a file is removed, its node is set to FREE, but all information remains accessible.

Because a node contains its parent node id you can reconstruct a FileSystem with only the MFT.

# NTFS – Forensics

## Timestamps:

There are stored in multiple locations

- $STANDARD_INFORMATION
- $FILE_NAME (not modified)

But also in "INDX" datas (directory enumerations)

# NTFS – Forensics

## INDX sign:

Directory header starts with "INDX" tag. When you carve raw datas on a disk you can find old "INDX". They can be useful to find overwritten nodes information.

# NTFS – Forensics

## Paddings:

A file is stored in a node of 1024 bytes. When the used space of a node shrinks, datas previously written stay in the used space.

# NTFS – Malwares

## ADS (Alternate Data Streams) case:

What is an ADS ?

# NTFS – Malwares

## ADS (Alternate Data Streams) case:

What is an ADS ?

We access by opening a file like "c:\toto:titi"

"titi" is the ADS.

An ADS is just a second $DATA chunk added and named.

# NTFS – Malwares

## ADS (Alternate Data Streams) case:

```
parseNTFS.py -ls c:\users\Heurs
[…]
 2017-06-19 13:48:47          4096 toto (134614)
<ADS>                                  toto:titi

parseNTFS.py -indexOffset c:134614
MFT node offset : 0x2060d11800
 00000000 46 49 4C 45 30 00 03 00  64 90 54 0F 58 00 00 00  FILE0.♥.d.T☼X...
 00000010 FE 01 01 00 38 00 01 00  90 01 00 00 00 04 00 00  .☺☺.8.☺..☺...♦..
[…]
 00000140 41 01 08 57 65 01 00 FF  80 00 00 00 40 00 00 00  A☺.We☺.■....@...
 00000150 00 04 18 00 00 00 05 00  1A 00 00 00 20 00 00 00  .♦↑...♣.→... ...
 00000160 74 00 69 00 74 00 69 00  49 20 77 61 73 20 68 69  t.i.t.i.I was hi
 00000170 64 64 65 6E 2C 20 79 6F  75 20 63 68 65 61 74 21  dden, you cheat!
 00000180 0D 0A 74 00 78 00 74 00  FF FF FF FF 82 79 47 11  ..t.x.t.■■■■.yG◄
```

# NTFS – Malwares

## Regin/ZeroAccess (EA) case:

Those malwares use a legacy trick to store datas, the Extended Attributes.

In MFT tags are:

- $EA_INFORMATION (0xD0)
- $EA (0xE0)

# NTFS – Malwares

## Regin/ZeroAccess (EA) case:

```
parseNTFS.py -ls c:\users\Heurs
[…]
 2017-06-19 13:48:47          4096 toto (134614)
```

```
MFT node offset : 0x2025e6d800
 00000000 46 49 4C 45 30 00 03 00  93 44 16 12 58 00 00 00  FILE0.♥..D—↨X...
 00000010 00 02 01 00 38 00 01 00  70 01 00 00 00 04 00 00  .☻☺.8.☺.p☺...♦..
 00000020 00 00 00 00 00 00 00 00  05 00 00 00 D6 0D 02 00  ........♣.....☻.
[...]
 00000130 10 00 00 00 14 00 00 00  E0 00 00 00 30 00 00 00  ►...¶.......0...
 00000140 00 00 00 00 00 00 04 00  14 00 00 00 18 00 00 00  ......♦.¶...↑...
 00000150 14 00 00 00 00 02 09 00  45 41 00 45 61 20 44 61  ¶....☻..EA.Ea Da
 00000160 74 61 73 00 00 00 00 00  FF FF FF FF 82 79 47 11  tas.....■■■■.yG◄
```

# NTFS – Malwares

## Flame case:

To spread to disconnected computers Flame used a FileSystem trick to discuss with a compromised host by USB key.

Any idea how to make a file invisible for the user and the Anti-virus ?

# NTFS – Malwares

## Flame case:

Create a file and rename it "."!

"." is the directory base of root. So when Explorer see "." in the root it doesn’t display it. And if you try to read "." Windows will confuse it with the real root directory :-)

# NTFS – Malwares

## Another idea:

Indexes 0 to 31 are reserved for NTFS internals files. But there are not all allocated. You can reallocate a file to one of those indexes to protect it from user access.

See more on: https://github.com/jschicht

# NTFS – Malwares

## Another idea:

New Volume (E:)

| Name | Date modified | Type |
|---|---|---|
| $RECYCLE.BIN | 07/07/2016 14:10 | File folder |
| System Volume Information | 07/07/2016 14:09 | File folder |

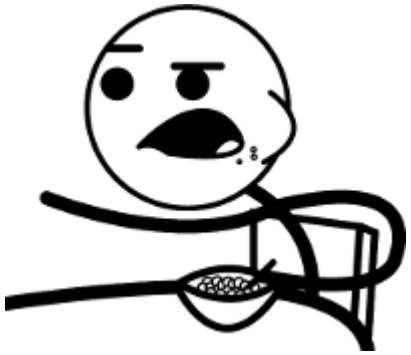
```
parseNTFS.py -ls e:\
      0000-00-00 00:00:00              0 $attrdef (4)
      0000-00-00 00:00:00              0 $badclus (8)
<ADS>                                    $badclus:$Bad
      0000-00-00 00:00:00              0 $bitmap (6)
      0000-00-00 00:00:00              0 $boot (7)
<DIR> 2016-07-07 12:09:04              0 $extend (11)
      0000-00-00 00:00:00              0 $logfile (2)
      2016-07-07 12:09:04          16384 $mft (0)
      0000-00-00 00:00:00              0 $mftmirr (1)
<DIR> 2016-07-07 12:10:00              0 $recycle.bin (38)
      2016-07-07 12:09:04              0 $secure (9)
<ADS>                                    $secure:$SDS
      2016-07-07 12:39:04             16 $malware (13)
      0000-00-00 00:00:00              0 $upcase (10)
<ADS>                                    $upcase:$Info
      0000-00-00 00:00:00              0 $volume (3)
<DIR> 2016-07-07 12:39:16              0 . (5)
<DIR> 2016-07-07 12:09:08              0 system volume information (35)
```

# NTFS – Vulnerabilities

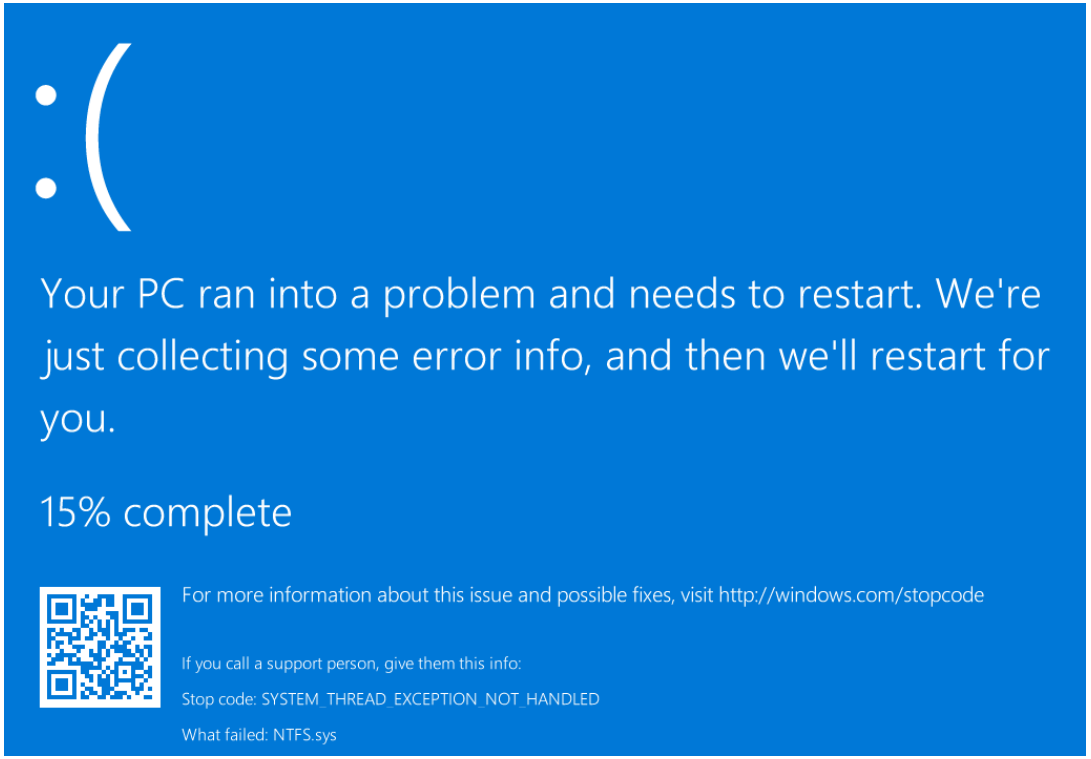
- Hey bro ! I'll craft corrupted NTFS volumes to see if Windows NTFS driver is safe. It should be fun to find a vuln!

- NTFS have already seen really a lot of fucked FS, you can't do worst than some softwares.

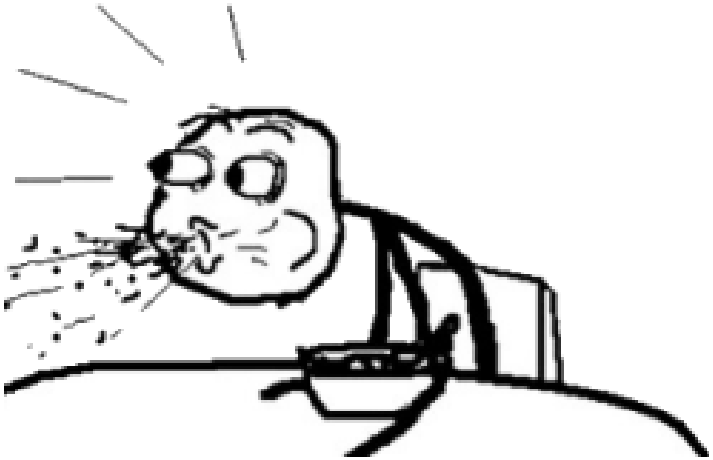
- Yes, I agree... It's just to test, NTFS is really a robust driver and tested since 25 years.



# NTFS – Vulnerabilities




(up to date: 19/06/2017)



Your PC ran into a problem and needs to
just collecting some error info, and then
you.

15% complete

For more information about this issue and possible fixes, visit http://w

If you call a support person, give them this info:

Stop code: SYSTEM_THREAD_EXCEPTION_NOT_HANDLED

What failed: NTFS.sys

# NTFS – Vulnerabilities

## NTFS.SYS crash, ok, so...

```
EXCEPTION_RECORD:  87b2998c -- (.exr 0xffffffff87b2998c)
ExceptionAddress: 854bf3f4 (Ntfs!NtfsIncrementCloseCounts+0x00000008)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 00000000
   Parameter[1]: 00000054
Attempt to read from address 00000054

CONTEXT:  87b293f0 -- (.cxr 0xffffffff87b293f0;r)
eax=00000000 ebx=00000000 ecx=854a9595 edx=00000002 esi=a8934ee0 edi=a6134c18
eip=854bf3f4 esp=87b29a54 ebp=87b29a54 iopl=0         nv up ei pl zr na pe nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00010246
Ntfs!NtfsIncrementCloseCounts+0x8:
854bf3f4 8b4854          mov     ecx,dword ptr [eax+54h] ds:0023:00000054=????????
```

# NTFS – Vulnerabilities

## NTFS.SYS crash, ok, so...

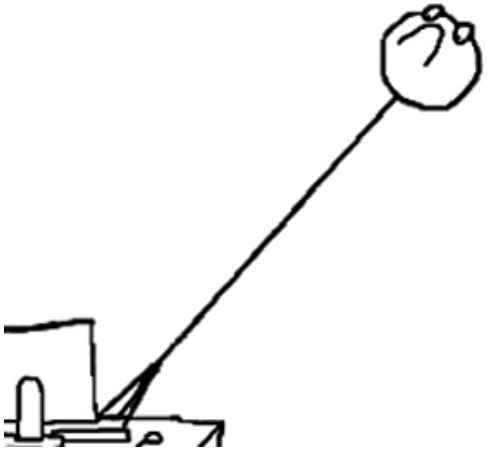
When a volume is too fucked up to be used, but base files are present, Windows try to rebuild some NTFS internal files.

```
NtfsInitializeDirectory((int)Entry, v8, 0, 1, (int *)&v24);
NtfsIncrementCloseCounts(v24, 0, 0);
```

Here it try to read "c:\$extend\$rmmetadata\$txf" directory, but the tag "$I30" is overwritten. So it can’t get a handle on it and don’t check if the handle is valid before using it.

# NTFS – Vulnerabilities (CVE-2017-0244)

A second crash surprised me a little bit more:



```
Arg1: 89f16854, Virtual address for the attempted execute.
Arg2: 279df963, PTE contents.
Arg3: 89f16720, (reserved)
Arg4: 00000002, (reserved)
[...]
TRAP_FRAME:  89f16720 -- (.trap 0xffffffff89f16720)
ErrCode = 00000011
eax=c000025f ebx=00010000 ecx=0000000c edx=84fc4d48 esi=949fc0f8 edi=871f80d8
eip=89f16854 esp=89f16794 ebp=89f16a90 iopl=0         nv up ei pl zr na pe nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00010246
89f16854 0030            add     byte ptr [eax],dh          ds:0023:c000025f=00
```

# NTFS – Vulnerabilities (CVE-2017-0244)

In NTFS you can to compress a file. To do it you can select the chunk MFT->Node->Data (0x80), offset 0xc (Flags).

Theoretically it’s set to 1 if the file is compressed. But technically it call "RtlGetCompressionWorkSpaceSize".

# NTFS – Vulnerabilities (CVE-2017-0244)

## Pseudo-code (windows 7) :

```
int __stdcall RtlGetCompressionWorkSpaceSize(__int16 a1, int a2, int a3)
{
  int result; // eax@4

  if ( (_BYTE)a1 && (unsigned __int8)a1 != 1 )
  {
    if ( a1 & 0xF0 )
      result = 0xC000025F;
    else
      result = ((int (__stdcall *)(int, int, int))RtlWorkSpaceProcs[(unsigned
__int8)a1])(a1 & 0xFF00, a2, a3);
  }
  else
  {
    result = 0xC000000D;
  }
  return result;
}
```

# NTFS – Vulnerabilities (CVE-2017-0244)

The jump table struct is compiled for a 64b computer, but if you are on a 32b this is the same.

So you can call "0 " address or a "RtlCompressBuffer", but arguments size is different. And at the "return " instruction you will execute a stack address!

```
PAGELK:0071FE34 _RtlWorkSpaceProcs dd 0                  ; DATA XREF: RtlGetCompressionWorkSpaceSize(x,x,x)+31
PAGELK:0071FE38                    dd 0
PAGELK:0071FE3C                    dd offset _RtlCompressWorkSpaceSizeLZNT1@12 ; RtlCompressWorkSpaceSizeLZNT1(x,x,x)
PAGELK:0071FE40                    dd offset _RtlCompressWorkSpaceSizeNS@12 ; RtlCompressWorkSpaceSizeNS(x,x,x)
PAGELK:0071FE44                    dd offset _RtlCompressWorkSpaceSizeNS@12 ; RtlCompressWorkSpaceSizeNS(x,x,x)
PAGELK:0071FE48                    dd offset _RtlCompressWorkSpaceSizeNS@12 ; RtlCompressWorkSpaceSizeNS(x,x,x)
PAGELK:0071FE4C                    dd offset _RtlCompressWorkSpaceSizeNS@12 ; RtlCompressWorkSpaceSizeNS(x,x,x)
PAGELK:0071FE50                    dd offset _RtlCompressWorkSpaceSizeNS@12 ; RtlCompressWorkSpaceSizeNS(x,x,x)
PAGELK:0071FE54 _RtlCompressBufferProcs dd 0             ; DATA XREF: RtlCompressBuffer(x,x,x,x,x,x,x,x)+40
PAGELK:0071FE58                    dd 0
PAGELK:0071FE5C                    dd offset _RtlCompressBufferLZNT1@32 ; RtlCompressBufferLZNT1(x,x,x,x,x,x,x,x)
PAGELK:0071FE60                    dd offset _RtlCompressBufferNS@32 ; RtlCompressBufferNS(x,x,x,x,x,x,x,x)
PAGELK:0071FE64                    dd offset _RtlCompressBufferNS@32 ; RtlCompressBufferNS(x,x,x,x,x,x,x,x)
PAGELK:0071FE68                    dd offset _RtlCompressBufferNS@32 ; RtlCompressBufferNS(x,x,x,x,x,x,x,x)
PAGELK:0071FE6C                    dd offset _RtlCompressBufferNS@32 ; RtlCompressBufferNS(x,x,x,x,x,x,x,x)
PAGELK:0071FE70                    dd offset _RtlCompressBufferNS@32 ; RtlCompressBufferNS(x,x,x,x,x,x,x,x)
```

# NTFS – Conclusion

NTFS is fun, but coding a parser is painful :-(

You can find interesting things when you look at the lower level of a FS.

Malwares coders know that and advanced threat use it to hide themselves.

NTFS is an old format that have surely seen some really strange FS, but as you can see some bugs survived.


Refences:

- Joakim Schit codes: https://github.com/jschicht
- http://ftp.kolibrios.org/users/Asper/docs/NTFS/ntfsdoc.html