CIS2390 PRACTICAL

Week 14

Questions

This week you may download an NTFS filesystem image from:

http://helios.hud.ac.uk/scomcjp/ntfs-img-kw-1.dd

This image has the MD5 hash:

389e42124eb23c5053ff6596976d6710.

Use *Winhex* to analyze this image and answer the following questions:

1. In the MFT, what is the MFT Entry at byte offset 0x1400?
2. Describe the attributes that the MFT entry at byte offset 0x1400 has? In doing this, ensure that you document:
   - the attribute type
   - the attribute name (if any)
   - the attribute residency status
   - the MFT Entry offset to the start of the attribute.
3. Where are the contents of the file *file-r-1.dat* located?
4. Where are the contents of the alternate data stream *file-n-5.dat:here* located?

NTFS Data Structures

NTFS File System Metadata Files

MFT Entry Number	File Name
0	$MFT
1	$MFTMirr
2	$LogFile
3	$Volume
4	$AttrDef

MFT Entry Number	File Name
5	.
6	$Bitmap
..-11	..

MFT Entry

Byte Range	Description
0-3	Signature (eg. “FILE”)
..	..
18-19	link count
20-21	Offset to first attribute
22-23	In use and directory flags
..	
40-41	Next attribute ID
42-1023	Attributes and fixup values

Attribute Header

Attribute Type Values

Type Identifier	Name
16	$STANDARD_INFORMATION
32	$ATTRIBUTE_LIST
48	$FILE_NAME
64	$OBJECT_ID
80	$SECURITY_DESCRIPTOR
96	$VOLUME_NAME
112	$VOLUME_INFORMATION
128	$DATA

Type Identifier	Name
144	$INDEX_ROOT
160	$INDEX_ALLOCATION
176	$BITMAP

First 16 Bytes of an Attribute

Byte Range	Description
0-3	Attribute type identifier (see previous table)
4-7	Length of attribute
8-8	Non-resident flag
9-9	Length of name
10-11	Offset to name
12-13	Flags
14-15	Attribute identifier

Notes: Attribute length allows the next attribute to be located. Last attribute is followed by the value 0xFFFFFFFF.

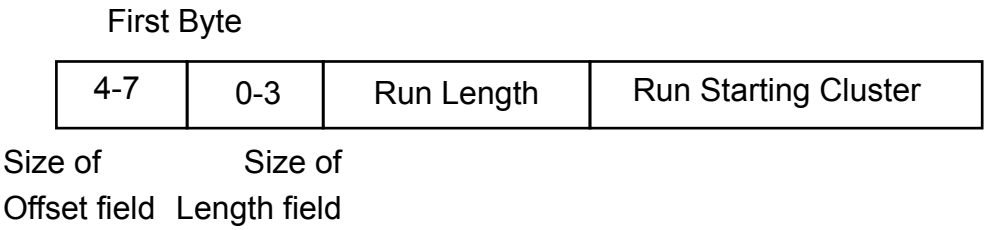
Resident Attribute

Byte Range	Description
0-15	General header (see table above)
16-19	Size of content
20-21	Offset to content

Non-Resident Attribute

Byte Range	Description
0-15	General header (see table above)
16-23	Starting VCN of the runlist
24-31	Ending VCN of the runlist
32-33	Offset to the runlist
..	..
48-55	Size of content
..-63	..

Runlist



Note: end of runlist is identified by a runlist of length 0 (ie. first byte of runlist is null).