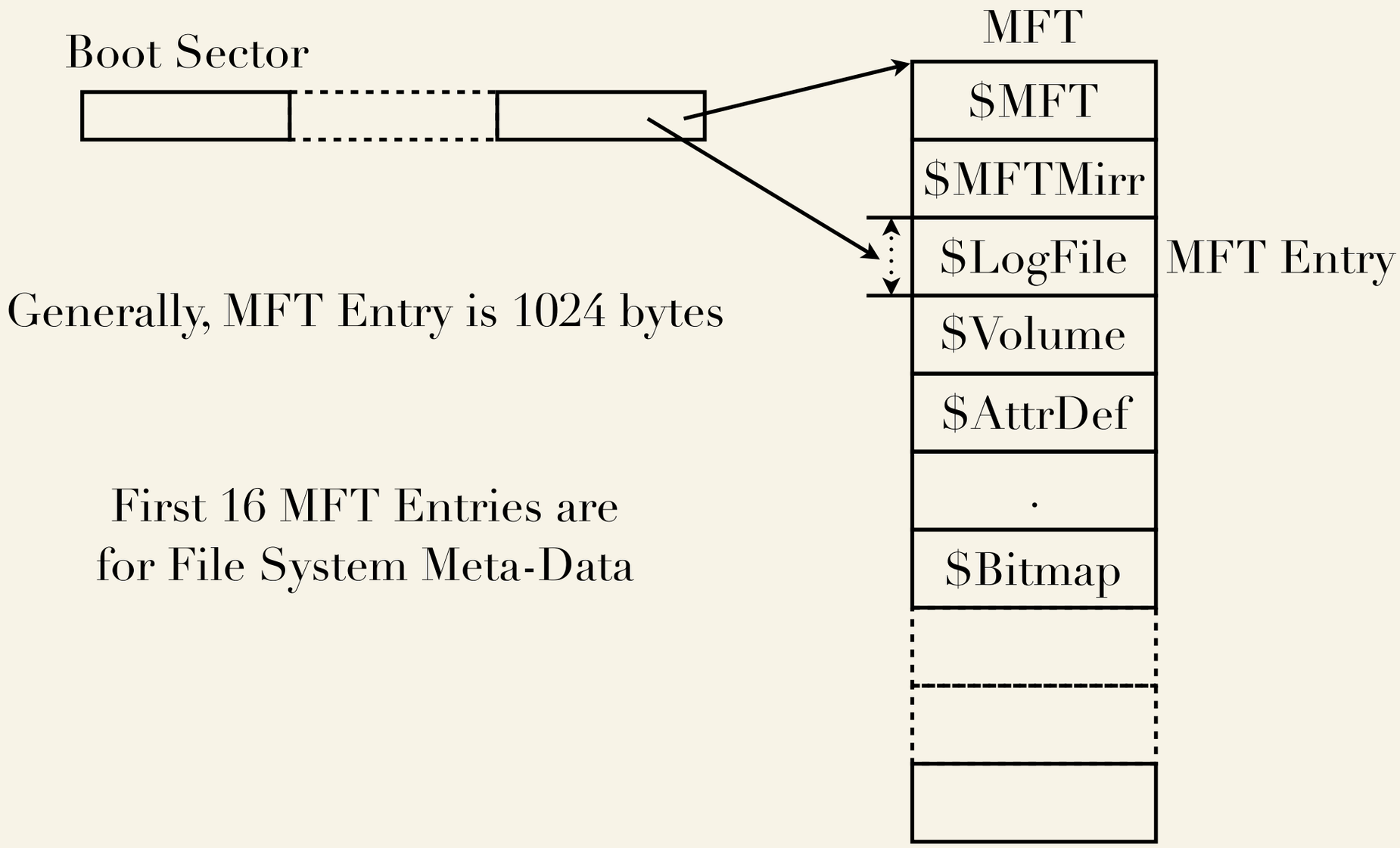
Security Workshop

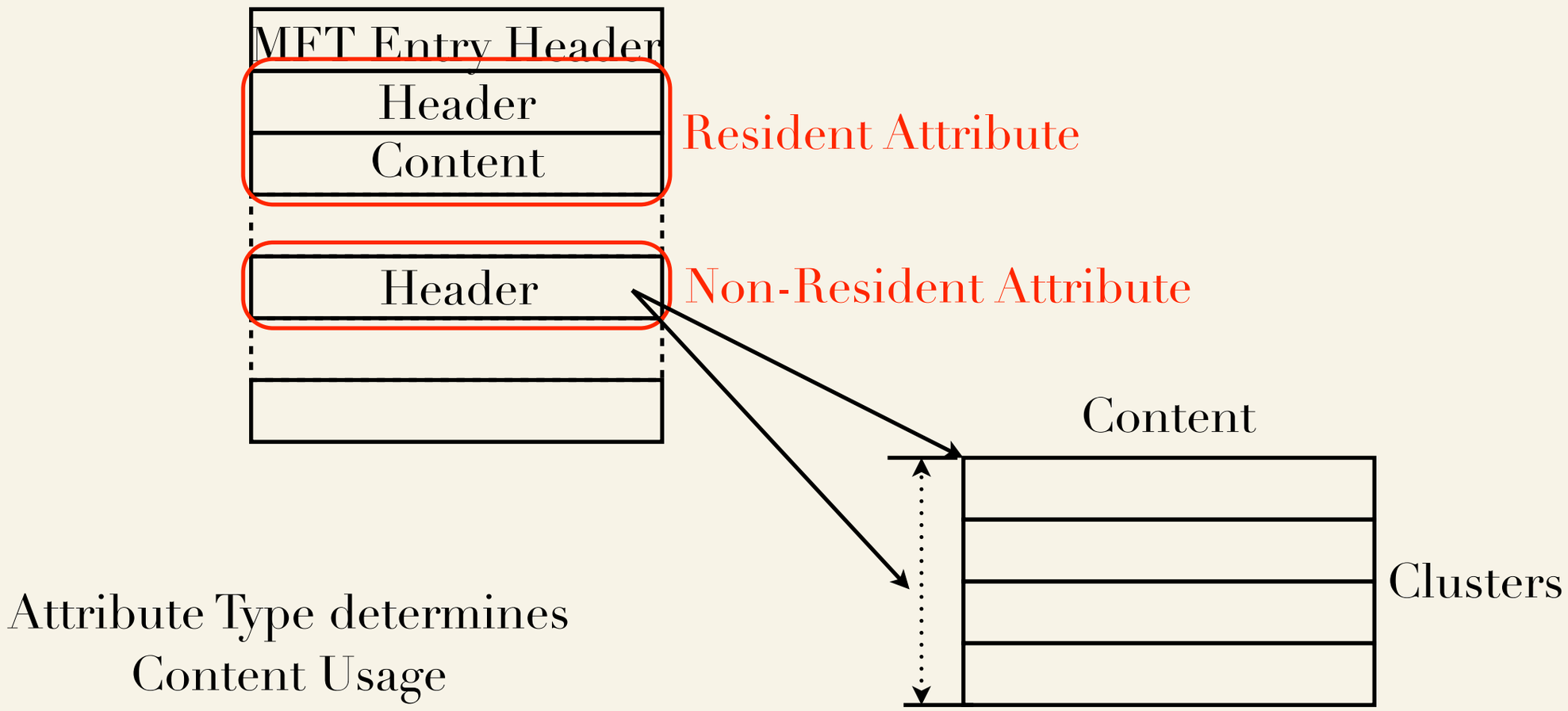
Dr. Carl Pulley
c.j.pulley@hud.ac.uk

Thursday, 14 January 2010

Master File Table



MFT Entry



Thursday, 14 January 2010

MFT Entries represent files in NTFS.
For simplicity, we ignore that multiple physical MFT entries may be used to make up a single logical MFT entry (cf. base MFT entries) - $ATTRIBUTE_LIST attribute type in base MFT entry points to associated physical MFT entries.
MFT entry header has offset to first attribute.
Attribute header has a type field and a note of the attribute record size in the MFT (thus next attribute may be calculated). Header also records the attributes resident status.
End of attribute list indicated with the value #FFFFFFFF.
Attributes may have names (as well as types) - these do not necessarily agree! Attribute header holds pointer to name start along with names length.

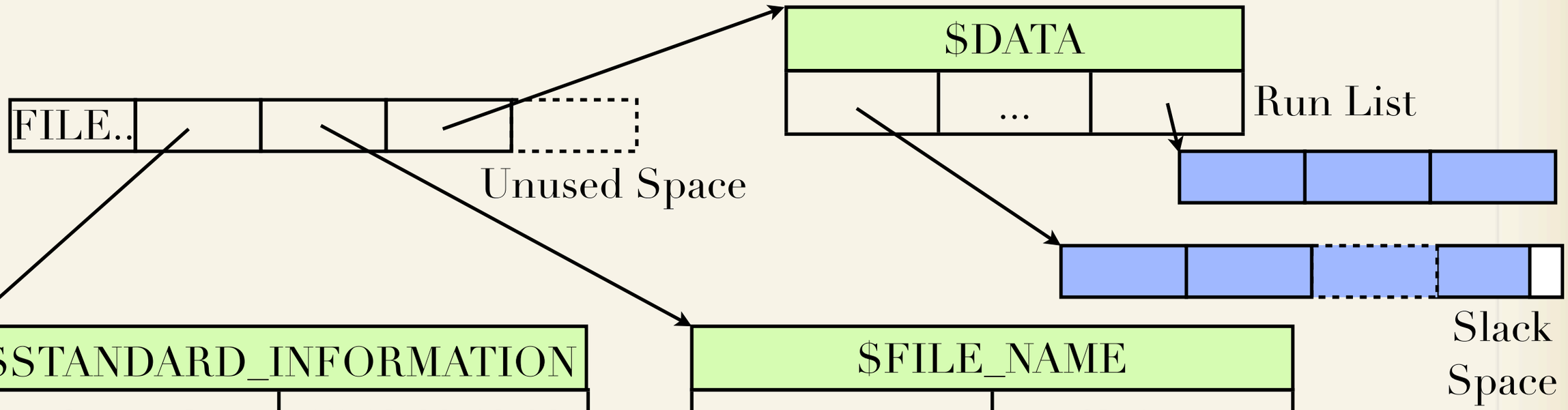
Attribute Types

- $STANDARD_INFORMATION
  - timestamps, user/group ID, etc.
- $FILE_NAME
  - timestamps and unicode file name
- $DATA
  - file contents
  - additional $DATA attributes have names associated with them
    - ie. alternate data streams

Thursday, 14 January 2010

This is a sample of the available attributes.
Every file has a $DATA attribute.

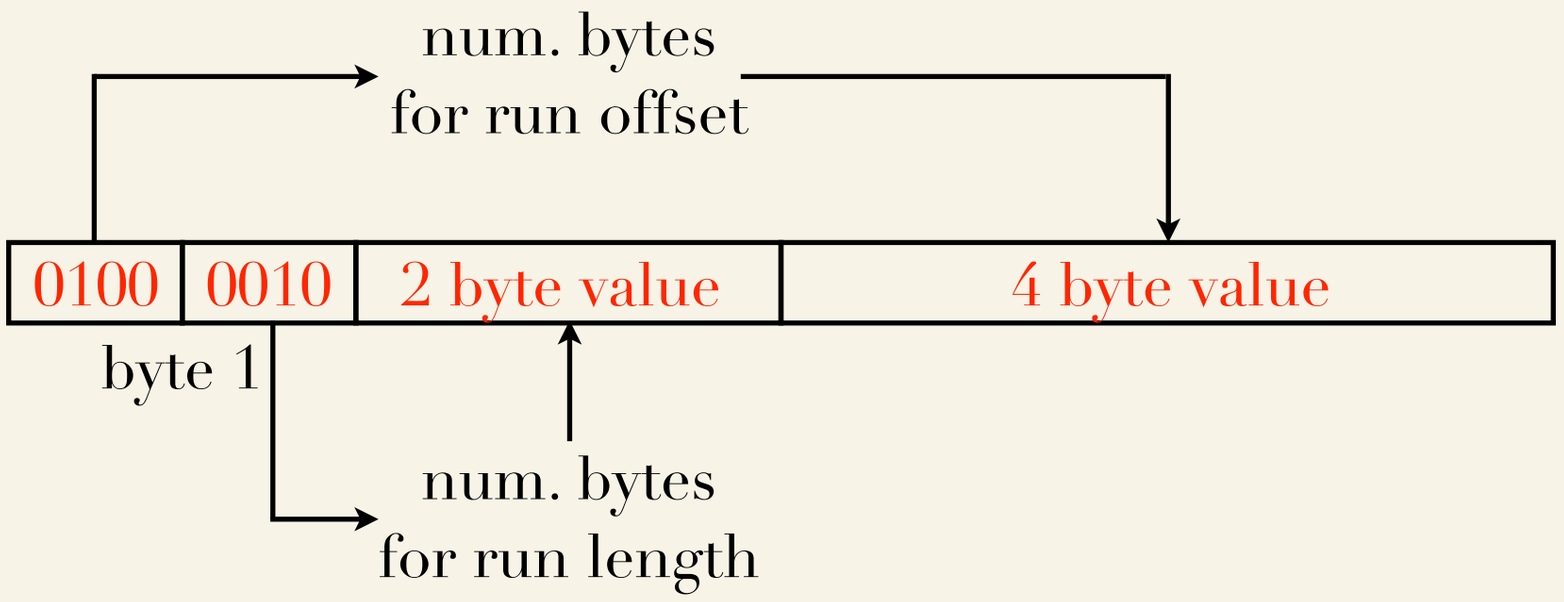
Example File



$STANDARD_INFORMATION	
Created	15/12/09 12:00
File Altered	15/12/09 12:00
MFT Altered	15/12/09 12:00
File Accessed	15/12/09 12:00
Flags	Hidden,Normal

$FILE_NAME	
Name	file1.txt
File Created	15/12/09 12:00
File Modified	15/12/09 12:00
MFT Modified	15/12/09 12:00
File Accessed	15/12/09 12:00

Runs



Values are cluster sized values

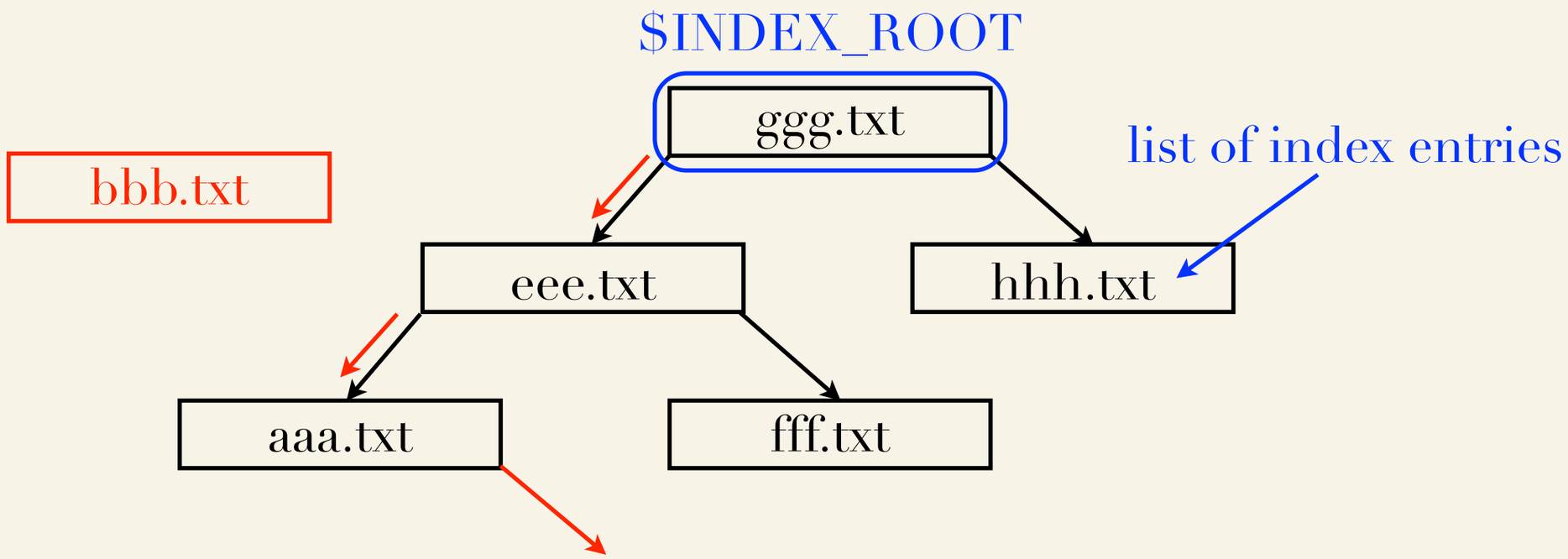
Values are signed integers

Run list offsets are relative to **last** offset!

Thursday, 14 January 2010

When we have logical MFT entries made up from multiple physical MFT entries, then virtual cluster numbers (VCNs) define the relationship between a physical MFT entries run list (ie. a collection of clusters) and the original file.
The difference between the starting VCN and ending VCN should be consistent with the total number of clusters drawn from each run (ie. total clusters in the entries run list).
Run lists end with a null byte (ie. an empty run!).

B-Trees



Thursday, 14 January 2010

With NTFS, more than two children can exist per node.
B-Trees are used to represent directory structures.
Every directory has a $INDEX_ROOT attribute (this attribute is always resident).
Nodes are implemented using index entries. Index entries are held in an index node. Index nodes are stored in either $INDEX_ROOT (this is aways the root of the B-Tree) or $INDEX_ALLOCATION attributes in the MFT.
$INDEX_ALLOCATION attributes are non-resident. Buffer of index records - each index record is a list of index entries.
End of index entry lists determined by an empty entry.