Resident Data on NTFS File Systems

Behavior of resident data in space and time

CIRCL
Computer Incident
Response Center
Luxembourg

CIRCL *TLP:CLEAR*

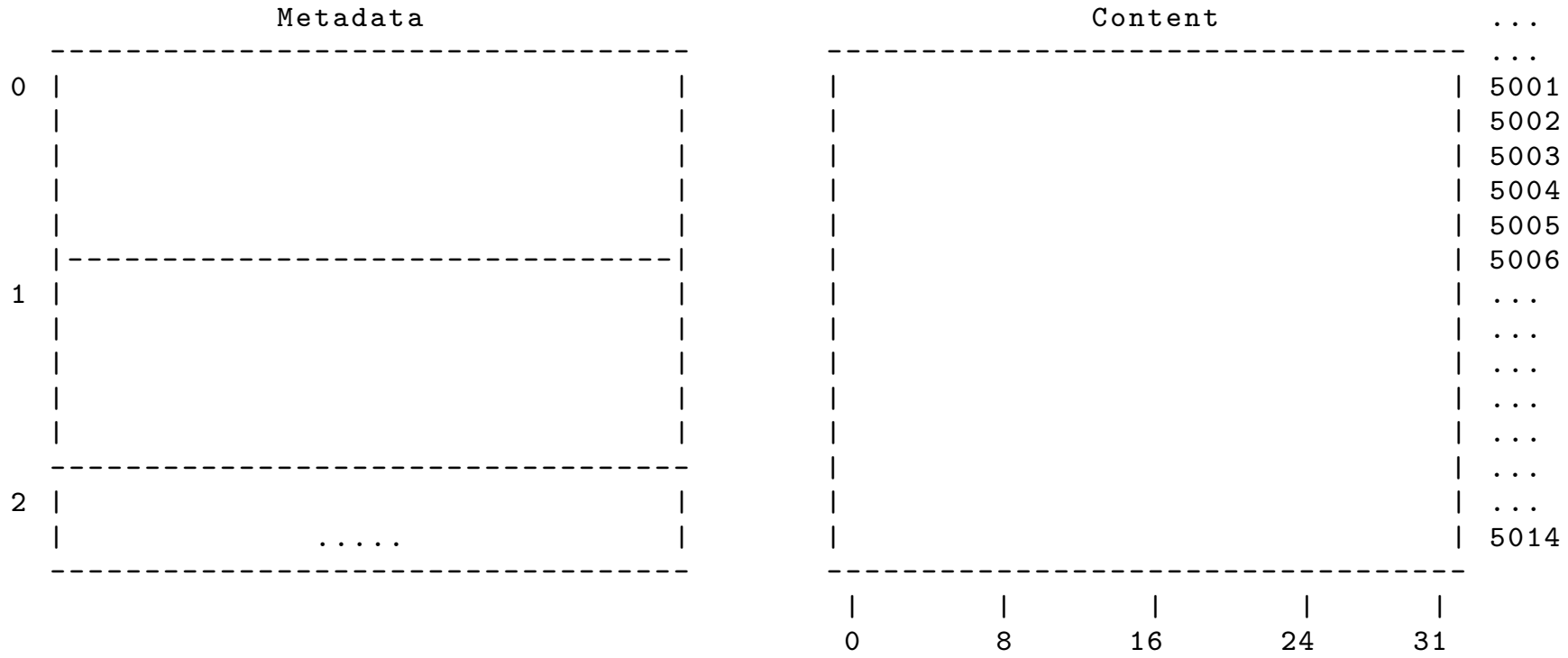
info@circl.lu

CyberDay: 2023-10-12

1. File System Analysis - Abstract

1.1 Organizing data in files

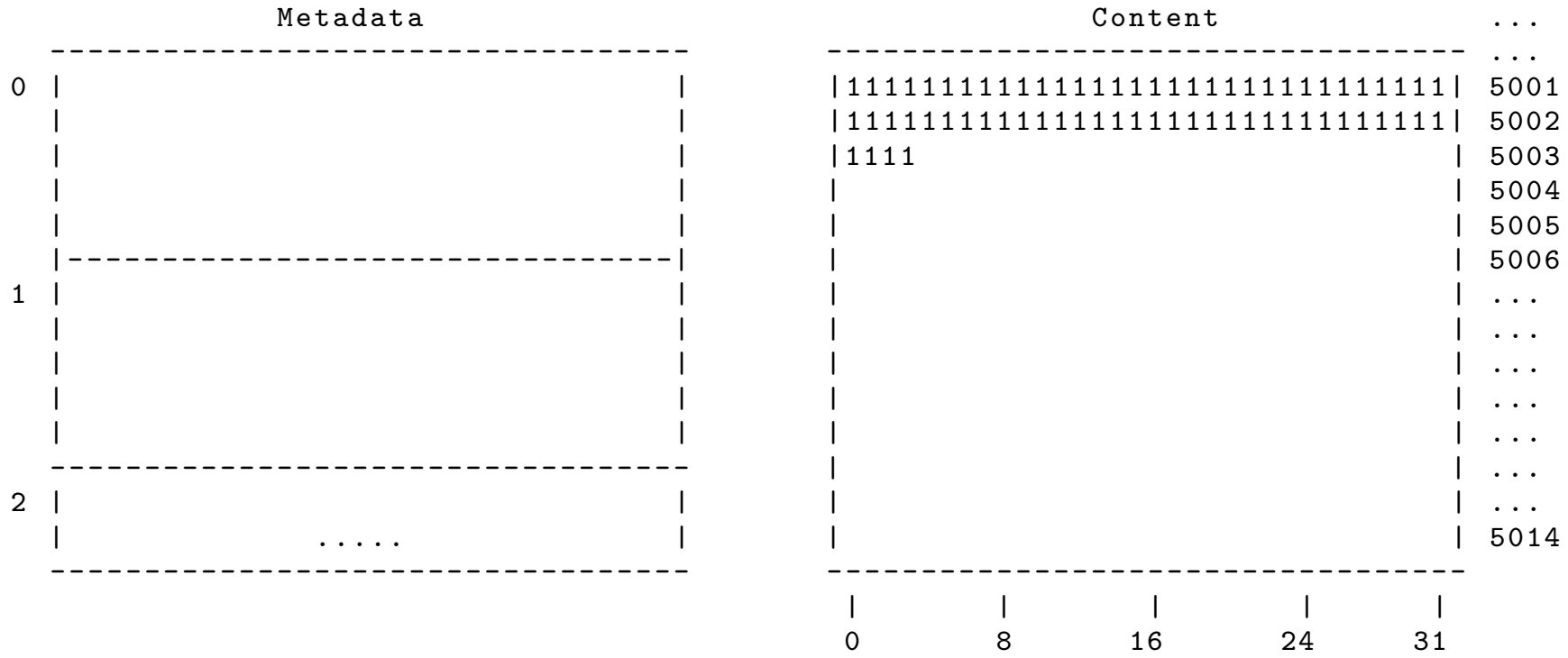
- Organizing data on a disc/partition
  - Read/write/modify raw data
  - Maintain allocation status of clusters
  - Maintain file related meta data



Allocation table:

1.1 Organizing data in files

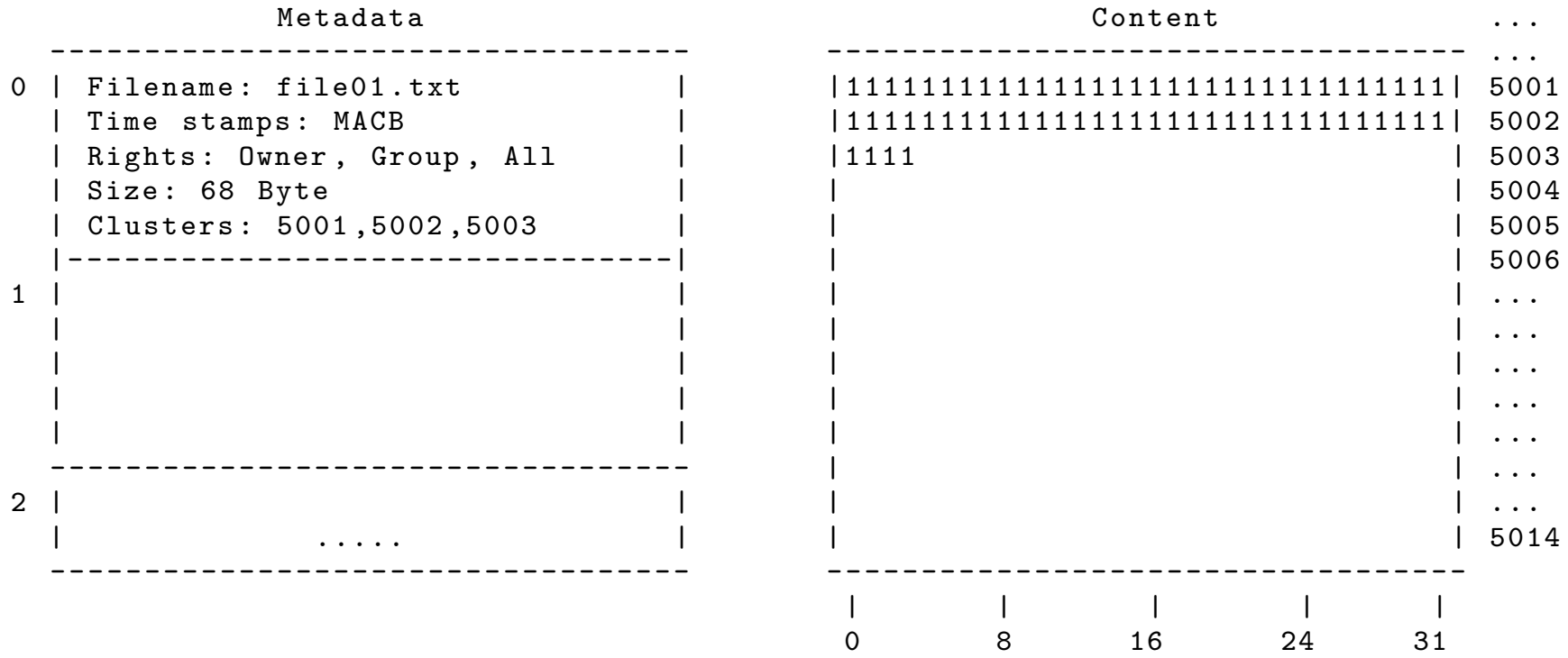
- Organizing data on a disc/partition
  - Read/write/modify raw data
  - Maintain allocation status of clusters
  - Maintain file related meta data



Allocation table:

1.1 Organizing data in files

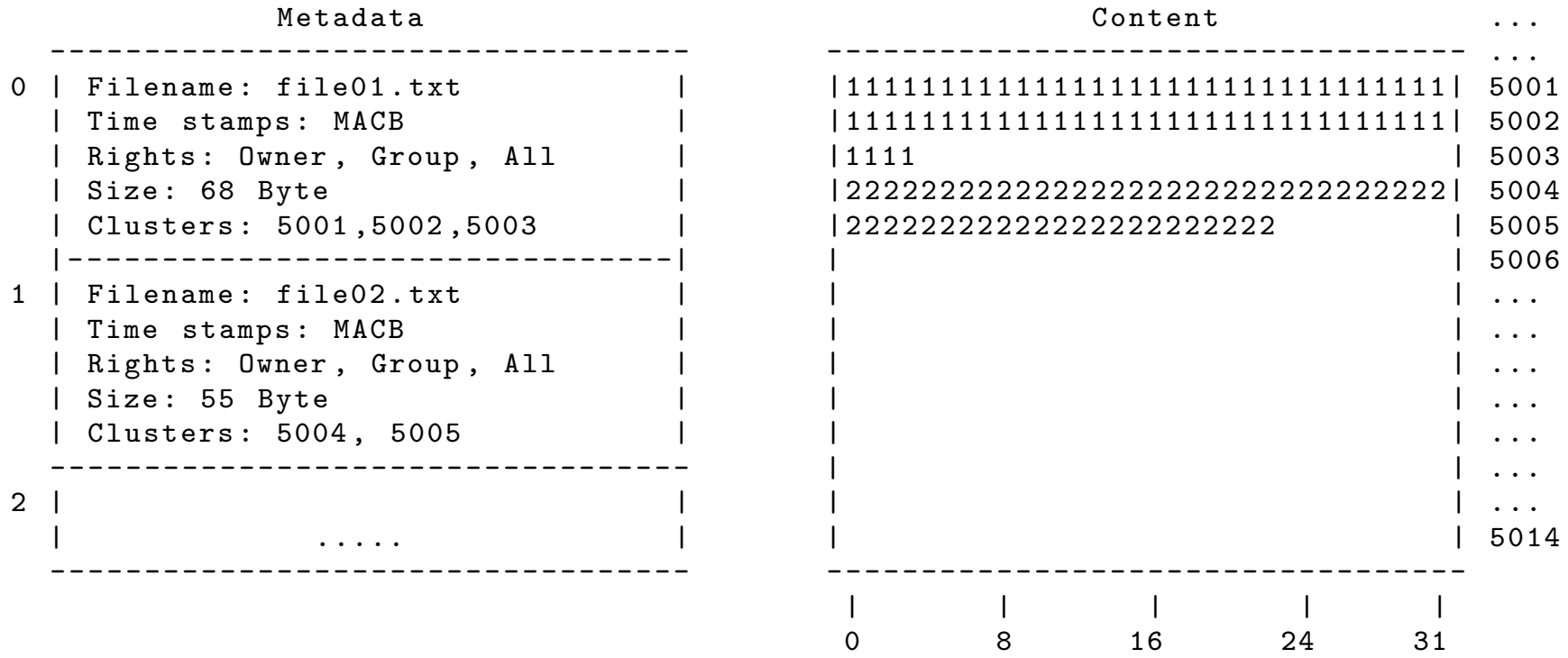
- Organizing data on a disc/partition
  - Read/write/modify raw data
  - Maintain allocation status of clusters
  - Maintain file related meta data



Allocation table: 5001, 5002, 5003

1.1 Organizing data in files

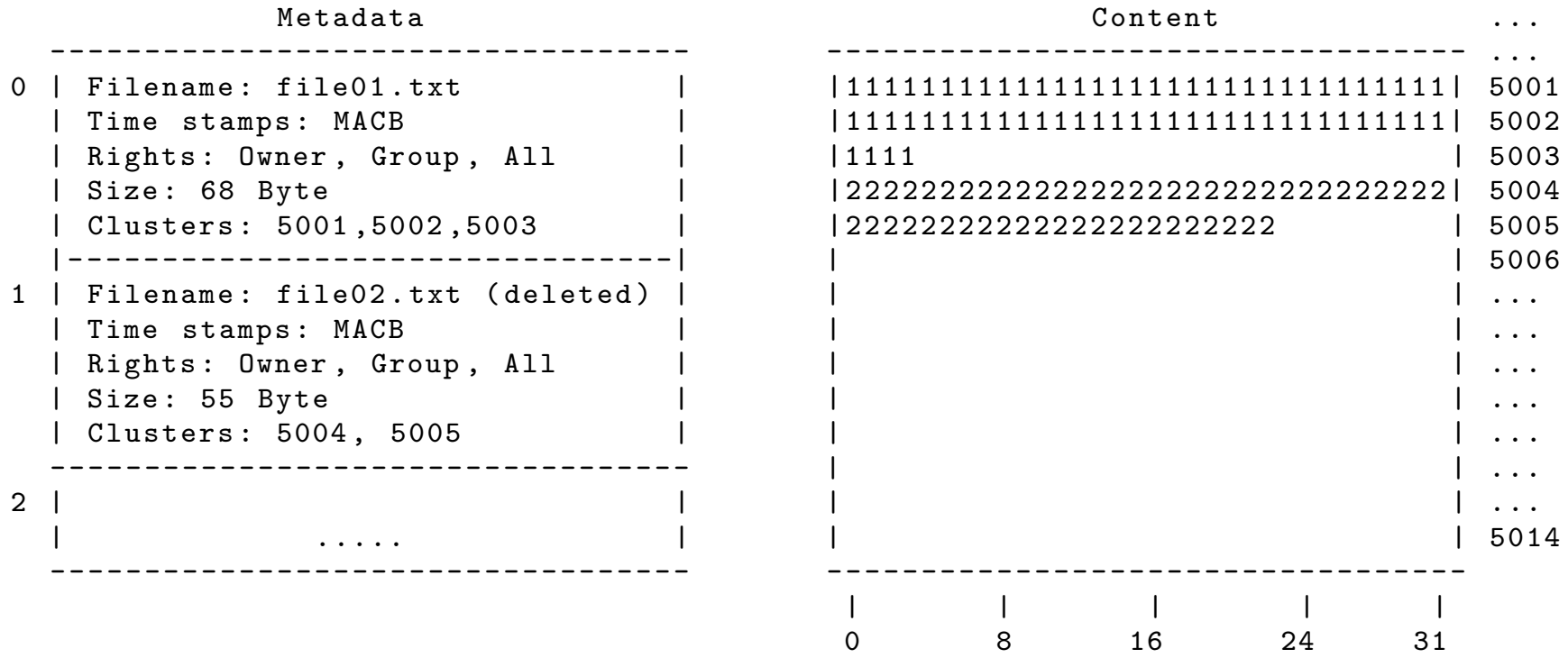
- Organizing data on a disc/partition
  - Read/write/modify raw data
  - Maintain allocation status of clusters
  - Maintain file related meta data



Allocation table: 5001, 5002, 5003, 5004, 5005

1.2 Deleting a file

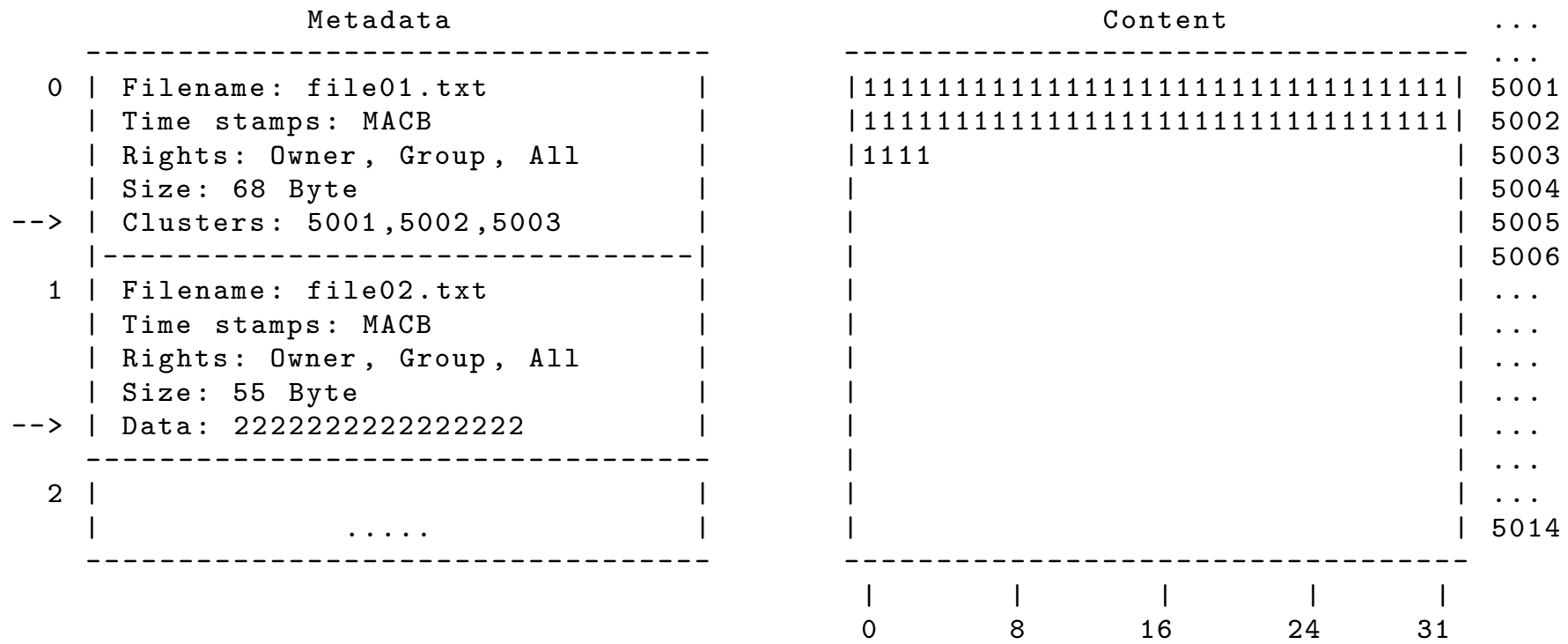
- Organizing data on a disc/partition
  - Read/write/modify raw data
  - Maintain allocation status of clusters
  - Maintain file related meta data



Allocation table: 5001, 5002, 5003

1.3 Resident & (Non)-Resident Data

- MFT - Master File Table - 1024 Byte per file
- Normal files, as is
- Very small files: Resident
- NTFS feature

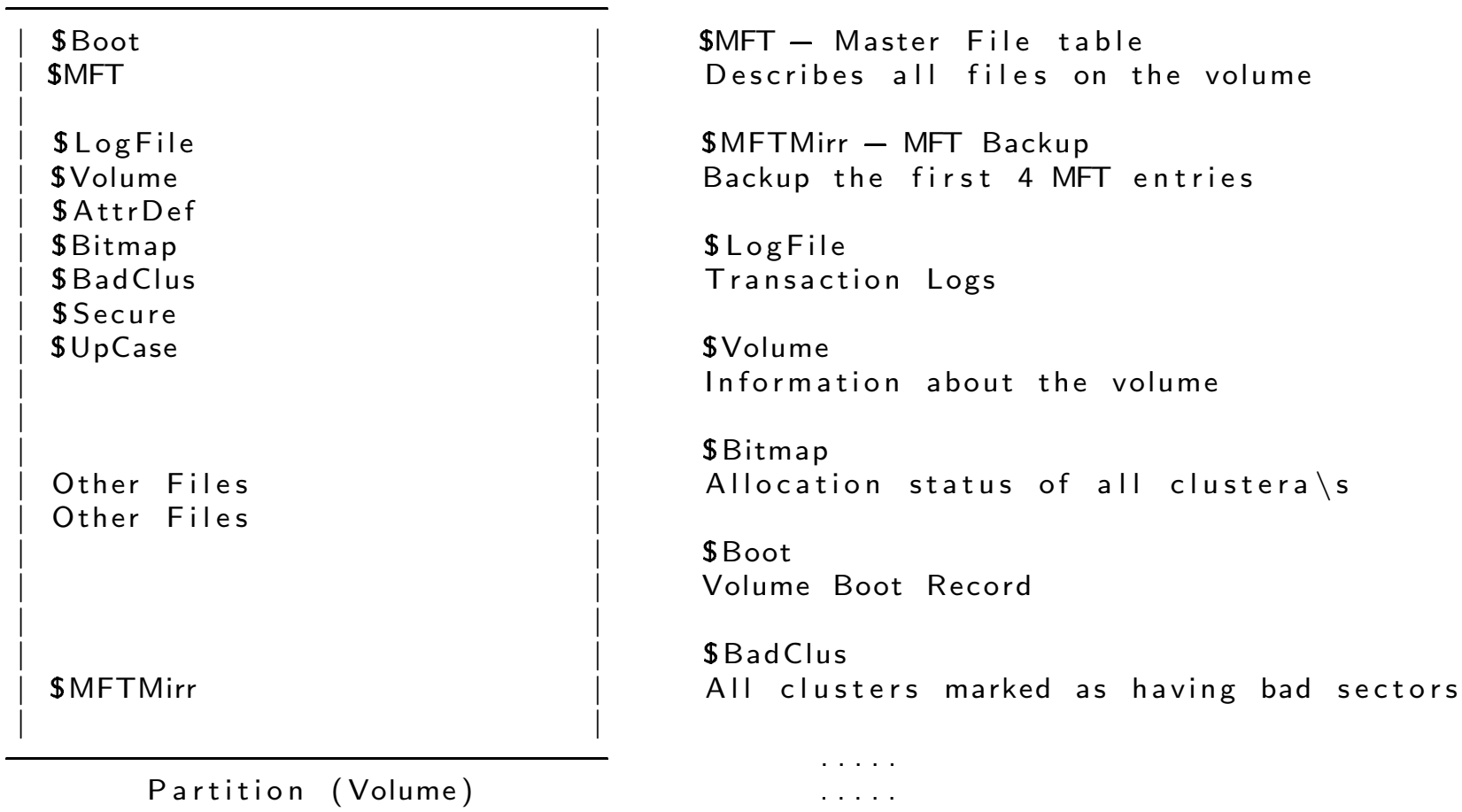


Allocation table: 5001, 5002, 5003

2. NTFS

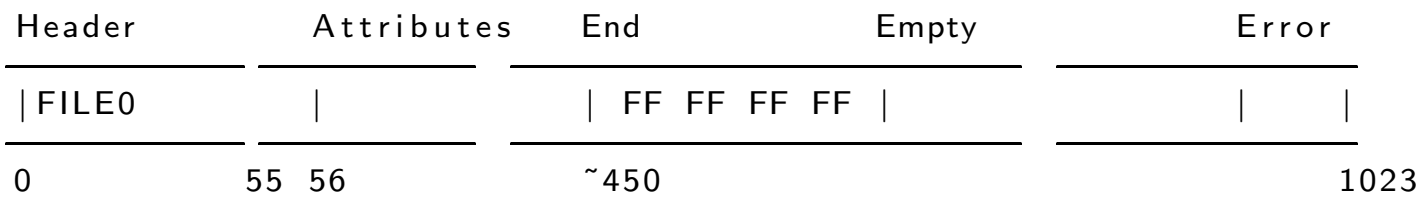
2.1 NTFS file system structure

- NTFS - New Technology File System
- Everything is a file



2.2 Master File Table

- Overview:
  - MFT maintain 1 record per file/directory
  - Size: 1024 Bytes per record
  - In NTFS everything is a file
    $\rightarrow$ Incl. meta files like $MFT
- MFT: Record Structure




```
Record Header:
      Signature: FILE
      Link Count: File is listed in x directories
      Is this a file or a directory
      Size of the file
      Deleted: Is the file already deleted
Attributes: $STANDARD_INFORMATION; $FILE_NAME; $Data
End of Recort: FF FF FF FF
Empty (Resident Data)
Error Check Sequence
```

2.3 Master File Table - Investigate - Exercise

```
$ mmls resident_data.dd
```

2.3 Master File Table - Investigate - Exercise

```
$ mmls resident_data.dd
```

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001:	———	0000000000	0000002047	0000002048	Unallocated
002:	000:000	0000002048	0002097151	0002095104	NTFS / exFAT (0x07)

2.3 Master File Table - Investigate - Exercise

```
$ mmls resident_data.dd
```

```
      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0002097151   0002095104   NTFS / exFAT (0x07)
```

```
$ fls -o 2048 resident_data.dd
```

2.3 Master File Table - Investigate - Exercise

```
$ mmls resident_data.dd

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0002097151   0002095104   NTFS / exFAT (0x07)
```

```
$ fls -o 2048 resident_data.dd

r/r 7-128-1:    $Boot
r/r 0-128-1:    $MFT
r/r 1-128-1:    $MFTMirr
```

2.3 Master File Table - Investigate - Exercise

```
$ mmls resident_data.dd

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0002097151   0002095104   NTFS / exFAT (0x07)
```

```
$ fls -o 2048 resident_data.dd

r/r 7-128-1:    $Boot
r/r 0-128-1:    $MFT
r/r 1-128-1:    $MFTMirr
```

```
$ istat -o 2048 resident_data.dd 0
```

2.3 Master File Table - Investigate - Exercise

```
$ mmls resident_data.dd

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0002097151   0002095104   NTFS / exFAT (0x07)
```

```
$ fls -o 2048 resident_data.dd

r/r 7-128-1:    $Boot
r/r 0-128-1:    $MFT
r/r 1-128-1:    $MFTMirr
```

```
$ istat -o 2048 resident_data.dd 0

.....
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 27648   init_size: 27648
4 5 6 7 8 9 10
```

2.3 Master File Table - Investigate - Exercise

```
$ mmls resident_data.dd

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0002097151   0002095104   NTFS / exFAT (0x07)
```

```
$ fls -o 2048 resident_data.dd

r/r 7-128-1:    $Boot
r/r 0-128-1:    $MFT
r/r 1-128-1:    $MFTMirr
```

```
$ istat -o 2048 resident_data.dd 0

.....
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 27648   init_size: 27648
4 5 6 7 8 9 10
```

```
$ icat -o 2048 resident_data.dd 0 | xxd | less
```

2.3 Master File Table - Investigate - Exercise

```
$ mmls resident_data.dd

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0002097151   0002095104   NTFS / exFAT (0x07)
```

```
$ fls -o 2048 resident_data.dd

r/r 7-128-1:    $Boot
r/r 0-128-1:    $MFT
r/r 1-128-1:    $MFTMirr
```

```
$ istat -o 2048 resident_data.dd 0

.....
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 27648   init_size: 27648
4 5 6 7 8 9 10
```

```
$ icat -o 2048 resident_data.dd 0 | xxd | less

00000000: 4649 4c45 3000 0300 0000 0000 0000 0000  FILE0...........
00000010: 0100 0100 3800 0100 9801 0000 0004 0000  ....8...........
.....
00000400: 4649 4c45 3000 0300 0000 0000 0000 0000  FILE0...........
00000410: 0100 0100 3800 0100 5801 0000 0004 0000  ....8...X.......
.....
```

3. Behavior: Resident & (Non)-Resident

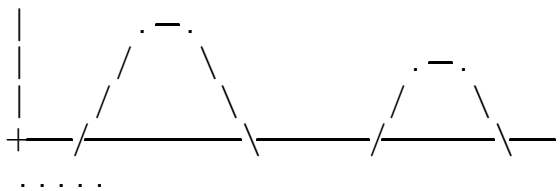
3. Behavior: Resident & (Non)-Resident

Activity	MFT	Cluster
1. Create small file:	CyberDay 2023.== ==========..Thi s is a small tex t for testing th	

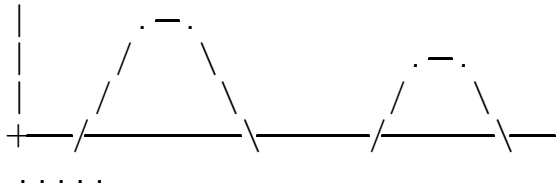
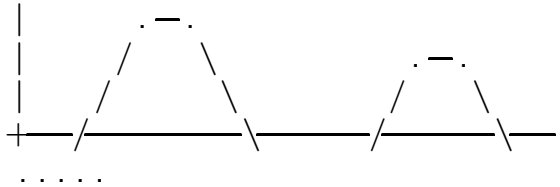
3. Behavior: Resident & (Non)-Resident

Activity	MFT	Cluster
1. Create small file:	CyberDay 2023.== ==========..Thi s is a small tex t for testing th	
2. Make file great:		CyberDay 2023.== ==========..Thi s is a small tex t for testing th .....

3. Behavior: Resident & (Non)-Resident

Activity	MFT	Cluster
1. Create small file:	CyberDay 2023.== ==========..Thi s is a small tex t for testing th	
2. Make file great:		CyberDay 2023.== ==========..Thi s is a small tex t for testing th .....
3. Modify content:		 .....

3. Behavior: Resident & (Non)-Resident

Activity	MFT	Cluster
1. Create small file:	CyberDay 2023.== ==========..Thi s is a small tex t for testing th	
2. Make file great:		CyberDay 2023.== ==========..Thi s is a small tex t for testing th .....
3. Modify content:		 .....
4. (Non) Persistent:	..... e behavior of re sident data..A f unky cool test f	 .....

4. Summary

Resident data not modified in big files

Resident data can survive for many years

Training material will be online

Do the Exercise!

5. Exercise: Resident & (Non)-Resident

5.1 Exercise: Prepare the Exercise

```
# Mount partition

  $ sudo mount -o offset=$((2048 * 512)) resident_data.dd /mnt/
```

-

5.1 Exercise: Prepare the Exercise

```
# Mount partition

  $ sudo mount -o offset=$((2048 * 512)) resident_data.dd /mnt/


# Create a small text file

  $ cat evidences_1.txt > /mnt/test123.txt

        CyberDay 2023
        ==============

        This is a small text for testing the behavior of resident data.
        A funky cool test for CyberDay 2023

        ==============
        CyberDay 2023
```

-

5.1 Exercise: Prepare the Exercise

```
# Mount partition

  $ sudo mount -o offset=$((2048 * 512)) resident_data.dd /mnt/


# Create a small text file

  $ cat evidences_1.txt > /mnt/test123.txt

        CyberDay 2023
        ==============

        This is a small text for testing the behavior of resident data.
        A funky cool test for CyberDay 2023

        ==============
        CyberDay 2023


# List the small text file

    ls -lh /mnt/test123.txt

        158 Sep 12 14:13 /mnt/test123.txt
-
```

5.2 Exercise: Analyze the small text file

```
# Identify the MFT number

  $ fls -o 2048 resident_data.dd

        r/r 64-128-2:    test123.txt
```

-

5.2 Exercise: Analyze the small text file

```
# Identify the MFT number

  $ fls -o 2048 resident_data.dd

        r/r 64-128-2:   test123.txt


# Analyze the MFT entry

  $ istat -o 2048 resident_data.dd 64

        Entry: 64        Sequence: 1
        Allocated File

        $STANDARD_INFORMATION Attribute Values:
        Created:        2023-09-12 14:13:49.139773000 (CEST)
        File Modified:  2023-09-12 14:13:49.140046300 (CEST)
        MFT Modified:   2023-09-12 14:13:49.140046300 (CEST)
        Accessed:       2023-09-12 14:13:49.139773000 (CEST)

        $FILE_NAME Attribute Values:
        Name: test123.txt

        Attributes:
        Type: $DATA (128-2)   Name: N/A   Resident   size: 158
-
```

5.3 Exercise: Analyze the corresponding MFT entry

```
# Read MFT and scroll to position 64

  icat -o 2048 resident_data.dd 0 | xxd | less

      .....
      .....
      00010000: 4649 4c45 3000 0300 0000 0000 0000 0000  FILE0...........
      00010010: 0100 0100 3800 0100 1802 0000 0004 0000  ....8...........
      .....
      .....
      000100d0: 2000 0000 0000 0000 0b00 7400 6500 7300  ..........t.e.s.
      000100e0: 7400 3100 3200 3300 2e00 7400 7800 7400  t.1.2.3...t.x.t.
      .....
      .....
      00010160: 0000 0000 0000 0200 9f00 0000 1800 0000  ................
      00010170: 4379 6265 7244 6179 2032 3032 330a 3d3d  CyberDay 2023.==
      00010180: 3d3d 3d3d 3d3d 3d3d 3d3d 3d0a 0a54 6869  ==========..Thi
      00010190: 7320 6973 2061 2073 6d61 6c6c 2074 6578  s is a small tex
      000101a0: 7420 666f 7220 7465 7374 696e 6720 7468  t for testing th
      000101b0: 6520 6265 6861 7669 6f72 206f 6620 7265  e behavior of re
      000101c0: 7369 6465 6e74 2064 6174 612e 0a41 2066  sident data..A f
      000101d0: 756e 6b79 2063 6f6f 6c20 7465 7374 2066  unky cool test f
      000101e0: 6f72 2043 7962 6572 4461 7920 3230 3233  or CyberDay 2023
      000101f0: 0a0a 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 0600  ..==========..
      00010200: 4379 6265 7244 6179 2032 3032 330a 0a00  CyberDay 2023...
      00010210: ffff ffff 0000 0000 0000 0000 0000 0000  ................
      .....
      .....
```

5.4 Exercise: Make the file great again

```
# Increase file size by 6.2 KByte

  $ cat ascii.txt >> /mnt/test123.txt
  $ ls -lh /mnt/test123.txt

        6,4K Sep 13 14:21 /mnt/test123.txt*



# Analyze the MFT entry
```

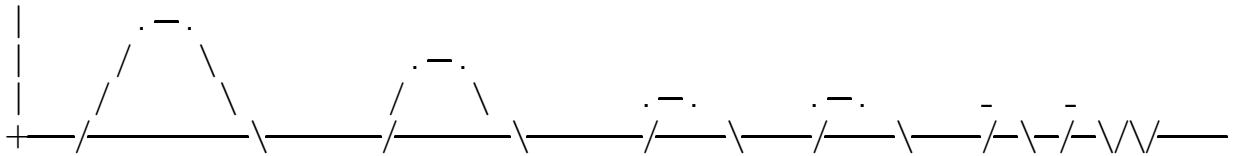
-

5.4 Exercise: Make the file great again

```
# Increase file size by 6.2 KByte

  $ cat ascii.txt >> /mnt/test123.txt
  $ ls -lh /mnt/test123.txt

        6,4K Sep 13 14:21 /mnt/test123.txt*



# Analyze the MFT entry

  $ istat -o 2048 resident_data.dd 64

        Entry: 64        Sequence: 1
        Allocated File

        $STANDARD_INFORMATION Attribute Values:
        Created:        2023-09-12 14:13:49.139773000 (CEST)
        File Modified:  2023-09-13 14:21:59.547693000 (CEST)
        MFT Modified:   2023-09-13 14:21:59.547693000 (CEST)
        Accessed:       2023-09-12 14:13:49.139773000 (CEST)

        $FILE_NAME Attribute Values:
        Name: test123.txt

        Attributes:
        Type: $DATA (128-2)   Name: N/A   Non-Resident   size: 6504   init_size: 6504
        32848 32849
```

5.4 Exercise: Make the file great again

```
# Read the data linked to the inode

  $ icat -o 2048 resident_data.dd 64 | less

        CyberDay 2023
        =============
        This is a small text for testing the behavior of resident data.
        A funky cool test for CyberDay 2023
```



5.4 Exercise: Make the file great again

```
# Read the data linked to the inode

  $ icat -o 2048 resident_data.dd 64 | less

        CyberDay 2023
        =============
        This is a small text for testing the behavior of resident data.
        A funky cool test for CyberDay 2023

        |      .-.
        |     /   \          .-.
        |    /     \        /   \       .-.     .-.     _   _
        +---/-------\------/-----\-----/---\---/---\---/-\-/-\/\/---
```

```
# Read sectors raw from the disk

  $ dd if=resident_data.dd skip=$((2048 + 32848 * 8)) count=16 | less

        CyberDay 2023
        =============
        This is a small text for testing the behavior of resident data.
        A funky cool test for CyberDay 2023

        |      .-.
        |     /   \          .-.
        |    /     \        /   \       .-.     .-.     _   _
        +---/-------\------/-----\-----/---\---/---\---/-\-/-\/\/---
```

5.5 Exercise: Modify file content

```
# Modify file content

  $ cat ascii.txt > /mnt/test123.txt
  $ ll /mnt/test123.txt

        6346 Sep 13 16:20 /mnt/test123.txt
```

-

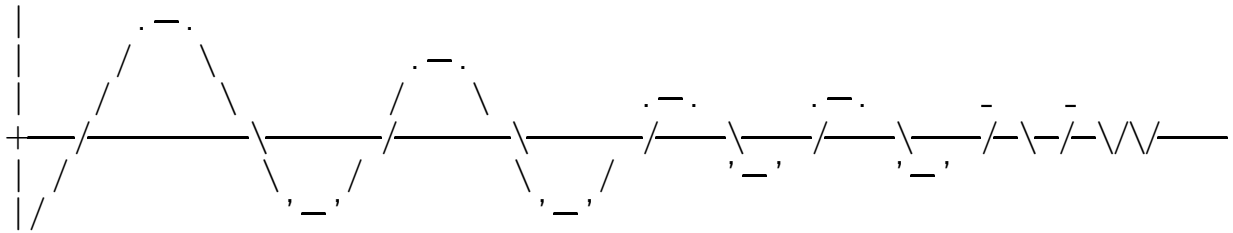
5.5 Exercise: Modify file content

```
# Modify file content

  $ cat ascii.txt > /mnt/test123.txt
  $ ll /mnt/test123.txt

        6346 Sep 13 16:20 /mnt/test123.txt



# Analyze the MFT entry

  $ istat -o 2048 resident_data.dd 64

        Type: $DATA (128-2)   Name: N/A   Non-Resident   size: 6346   init_size: 6346
        36944 36945
```

-

5.5 Exercise: Modify file content

```
# Modify file content

  $ cat ascii.txt > /mnt/test123.txt
  $ ll /mnt/test123.txt

        6346 Sep 13 16:20 /mnt/test123.txt



# Analyze the MFT entry

  $ istat -o 2048 resident_data.dd 64

        Type: $DATA (128-2)   Name: N/A   Non-Resident   size: 6346   init_size: 6346
        36944 36945



# Read the data linked to the inode

  $ icat -o 2048 resident_data.dd 64 | less
```



5.6 Exercise: What about the data inside the MFT entry

```
# Read MFT and scroll to position 64

  $ icat -o 2048 resident_data.dd 0 | xxd | less

        .....
        .....
        00010000: 4649 4c45 3000 0300 0000 0000 0000 0000  FILE0...........
        00010010: 0100 0100 3800 0100 a801 0000 0004 0000  ....8...........
        .....
        .....
        000100d0: 2000 0000 0000 0000 0b00 7400 6500 7300   .........t.e.s.
        000100e0: 7400 3100 3200 3300 2e00 7400 7800 7400  t.1.2.3...t.x.t.
        .....
        .....
        00010160: 0100 4000 0000 0200 0000 0000 0000 0000  ..@.............
        00010170: 0100 0000 0000 0000 4000 0000 0000 0000  ........@.......
        00010180: 0020 0000 0000 0000 ca18 0000 0000 0000  . ..............
        00010190: ca18 0000 0000 0000 3102 5090 0000 0000  ........1.P.....
        000101a0: ffff ffff 0000 0000 ffff ffff 0000 0000  ................
        000101b0: 6520 6265 6861 7669 6f72 206f 6620 7265  e behavior of re
        000101c0: 7369 6465 6e74 2064 6174 612e 0a41 2066  sident data..A f
        000101d0: 756e 6b79 2063 6f6f 6c20 7465 7374 2066  unky cool test f
        000101e0: 6f72 2043 7962 6572 4461 7920 3230 3233  or CyberDay 2023
        000101f0: 0a0a 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 0f00  ..==========....
        00010200: 4379 6265 7244 6179 2032 3032 330a 0a00  CyberDay 2023...
        00010210: ffff ffff 0000 0000 0000 0000 0000 0000  ................
        .....
```

A.1 What if the file becomes very small again

```
# Overwrite content

  $ echo "Hello CyberDay 2023" > /mnt/test123.txt
  $ ll /mnt/test123.txt

        20 Sep 14 14:35 /mnt/test123.txt
```

-

A.1 What if the file becomes very small again

```
# Overwrite content

  $ echo "Hello CyberDay 2023" > /mnt/test123.txt
  $ ll /mnt/test123.txt

        20 Sep 14 14:35 /mnt/test123.txt



# Analyze the MFT entry

  $ istat -o 2048 resident_data.dd 64

        Type: $SECURITY_DESCRIPTOR (80-1)   Name: N/A   Resident   size: 80
        Type: $DATA (128-2)   Name: N/A   Resident   size: 20
```

-

A.1 What if the file becomes very small again

```
# Overwrite content

  $ echo "Hello CyberDay 2023" > /mnt/test123.txt
  $ ll /mnt/test123.txt

        20 Sep 14 14:35 /mnt/test123.txt



# Analyze the MFT entry

  $ istat -o 2048 resident_data.dd 64

        Type: $SECURITY_DESCRIPTOR (80-1)   Name: N/A   Resident   size: 80
        Type: $DATA (128-2)   Name: N/A   Resident   size: 20



# Read the data linked to the inode

  $ icat -o 2048 resident_data.dd 64 | less

_       Hello CyberDay 2023
```

A.1 What if the file becomes very small again

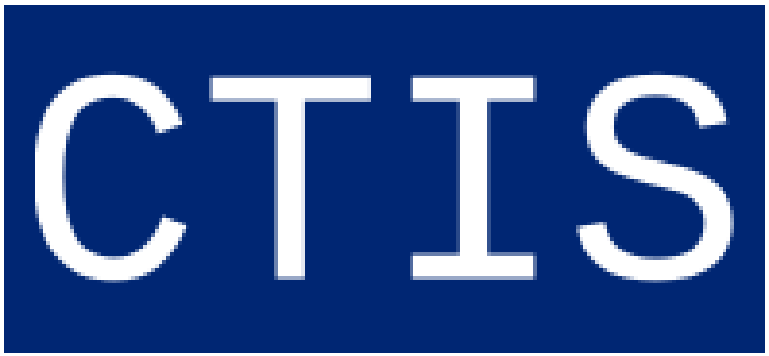
```
# Read MFT and scroll to position 64

  $ icat -o 2048 resident_data.dd 0 | xxd | less

        .....
        .....
        00010000: 4649 4c45 3000 0300 0000 0000 0000 0000  FILE0...........
        00010010: 0100 0100 3800 0100 9001 0000 0004 0000  ....8...........
        .....
        .....
        000100d0: 2000 0000 0000 0000 0b00 7400 6500 7300  ..........t.e.s.
        000100e0: 7400 3100 3200 3300 2e00 7400 7800 7400  t.1.2.3...t.x.t.
        .....
        .....
        00010160: 0000 1800 0000 0200 1400 0000 1800 0000  ................
        00010170: 4865 6c6c 6f20 4379 6265 7244 6179 2032  Hello CyberDay 2
        00010180: 3032 330a 0000 0000 ffff ffff 0000 0000  023.............
        00010190: 0000 0000 0000 0000 0002 5090 0000 0000  ..........P.....
        000101a0: ffff ffff 0000 0000 ffff ffff 0000 0000  ................
        000101b0: 6520 6265 6861 7669 6f72 206f 6620 7265  e behavior of re
        000101c0: 7369 6465 6e74 2064 6174 612e 0a41 2066  sident data..A f
        000101d0: 756e 6b79 2063 6f6f 6c20 7465 7374 2066  unky cool test f
        000101e0: 6f72 2043 7962 6572 4461 7920 3230 3233  or CyberDay 2023
        000101f0: 0a0a 3d3d 3d3d 3d3d 3d3d 3d3d 3d3d 1300  ..==========....
        00010200: 4379 6265 7244 6179 2032 3032 330a 0a00  CyberDay 2023...
        00010210: ffff ffff 0000 0000 0000 0000 0000 0000  ................
        .....
        .....
```

A.2 Safe the Date

HACK.LU & CTI Summit

Week 42 October 2023

16.10.2023 – 19.10.2023



Resident Data on NTFS File Systems

Behavior of resident data in space and time

CIRCL
Computer Incident
Response Center
Luxembourg

CIRCL *TLP:CLEAR*

info@circl.lu

CyberDay: 2023-10-12