|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2020/21) Semester 4/6 | Week 8 |
| Practical 8 |
| **NTFS Analysis** | |

**OBJECTIVES**

To be able to:

1. Navigate to the $MFT entry from the PBR in an NTFS partition.
2. Interpret the $MFT structure.

Steps: (You may follow the detailed steps in Practical 7)

1. Start a new case in EnCase and name it as NTFS Analysis.
2. Add Laura’s evidence file to the case.
3. Switch to Disk view.
4. Go to Physical Sector 2048, or the first logical sector of the first NTFS partition.

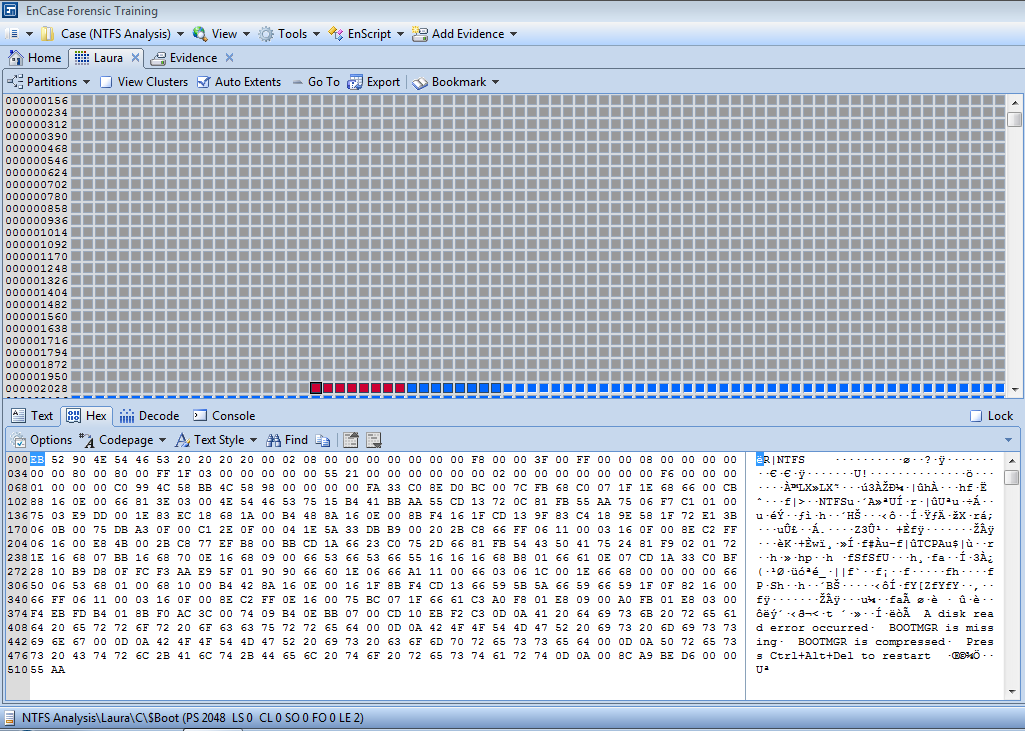


Figure 1: Physical Sector (PS) 2048

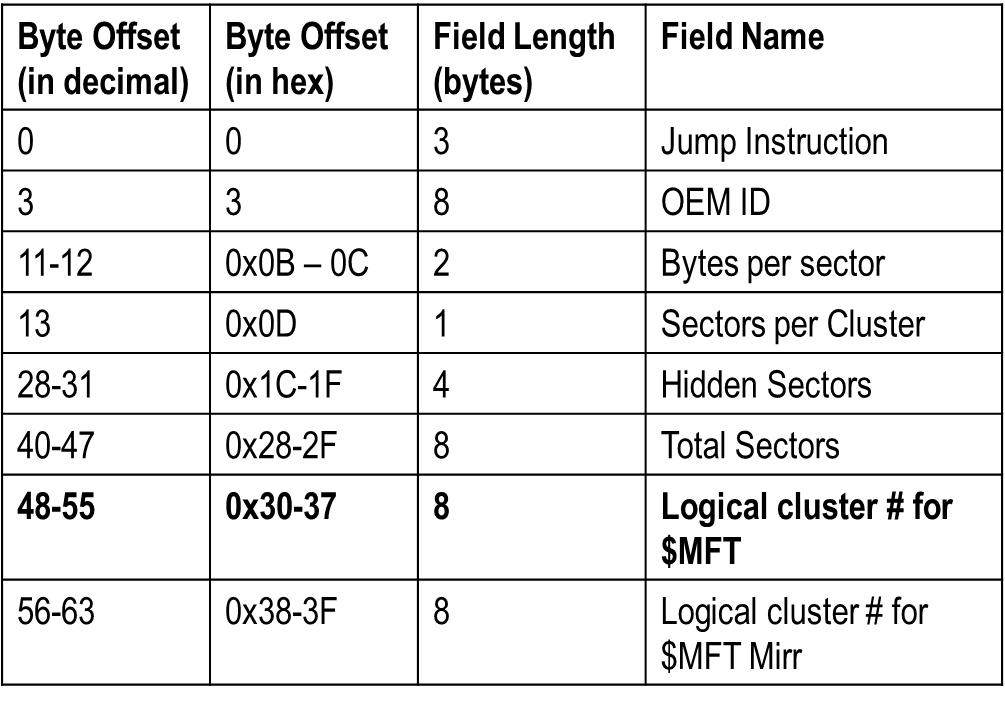


Table 1: Partition Boot Record (PBR)

With reference to Table 1 above, answer the following:

Q1: What is Original Equipment Manufacturer Identifier (OEM ID)? How many Bytes per Sector? How many Sectors per Cluster? What is the Logical cluster number for $MFT?

OEM ID is an identifier number use to identify the vender that sold this device. Byte per sector is 512 byte

Sector per cluster is 8 byte

Logical cluster number for $MFT is 8533.

1. Now, from Disk view, select View Clusters.

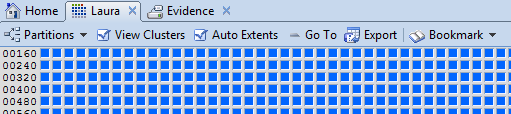


Figure 2: View Clusters

1. Right-click, select Go To and enter 8533 to view $MFT table.

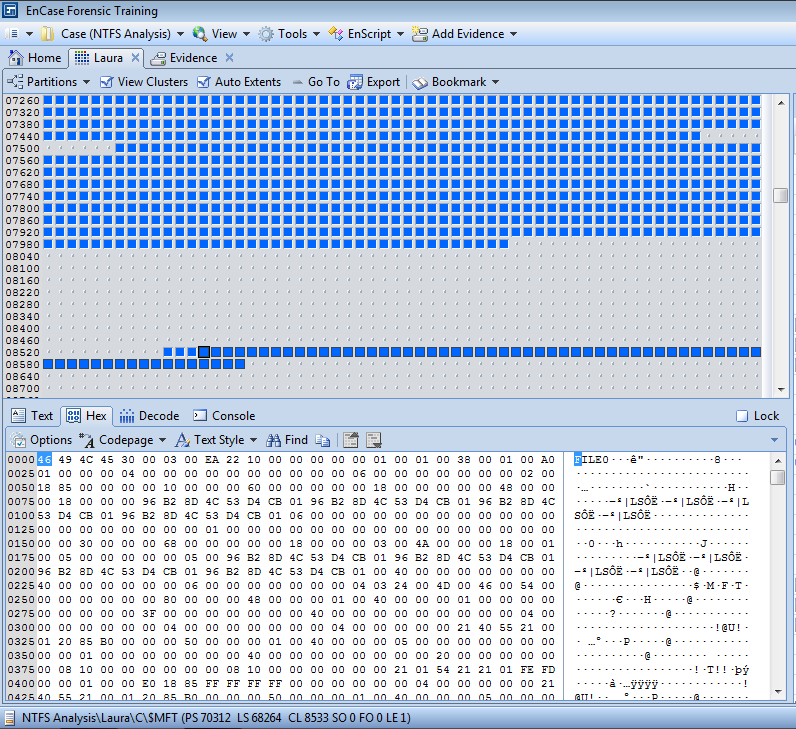


Figure 3: $MFT Entry

All MFT records follow the same structure. They are 1024 bytes in size, and start with a 48-byte header section and an 8-byte Fixup array. At offset 0x38 (48+8=56 (or 38 in hex)) is the start of a string of attributes. The header describes the properties of the record, and the attributes describe all aspects of the file from its name to its data.

1. Go to sector offset 56 (0x38) in the View pane, which is the start of first attribute. The first MFT record is $MFT table.

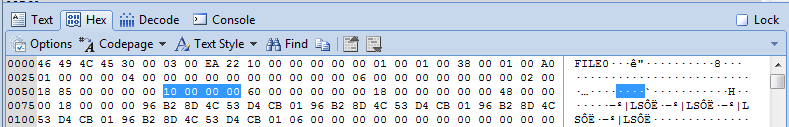


Figure 4: First Attribute

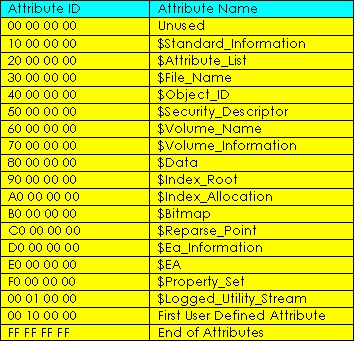


Table 2: NTFS Attributes

Q2: Complete the following for the first attribute of $MFT record.

Attribute name: $Standard\_information

Length: 96

Non-resident flag: false

Q3: How would you go to the 2nd attribute? Use Appendix A for hex to decimal conversion if necessary.

Offset of 2nd attribute is 56+96=152

Q4: Complete the following for the 2nd attribute of $MFT record.

Attribute name: $File\_Name

Length: 104

Non-resident flag: False

File name (Unicode name: offset 42 of content): $MFT

Q5: Go to 3rd attribute. Complete the following for 3rd attribute.

(To go to 3rd attribute: 0x98+0x68 = 0x100 (or 256 decimal))

Attribute name: $Data

Length: 72

Non-resident flag: True

Q6: Consolidate your findings above and complete the following diagram to show the composite of $MFT entry:

Length:

$ MFT

$ File\_Name

$ Data

$ Standard\_information

- The End -

Appendix A – Hexadecimal-to-Decimal Conversion Table

