|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2020/21) Semester 4/6 | Week 7 |
| Practical 7 |
| **MBR and VBR** | |

**OBJECTIVES**

To be able to:

1. Examine partition information in Master Boot Record (MBR).
2. Examine Volume Boot Record (VBR).

**Part A: Partition Information**

* The first Physical Sector of a hard drive, sector 0 (PS 0), is where the Master Boot Record (MBR) resides.
* The MBR is 512 bytes in length.
* It consists of executable code, which locates and loads the Volume Boot Record from the active partition, the master partition table, error messages, and signature bytes of 55h AAh.
* There is only one MBR, but a drive can have one or more Volume Boot Records (VBR).

Steps:

1. Open Laura.Case that you have created in the previous practical activities.

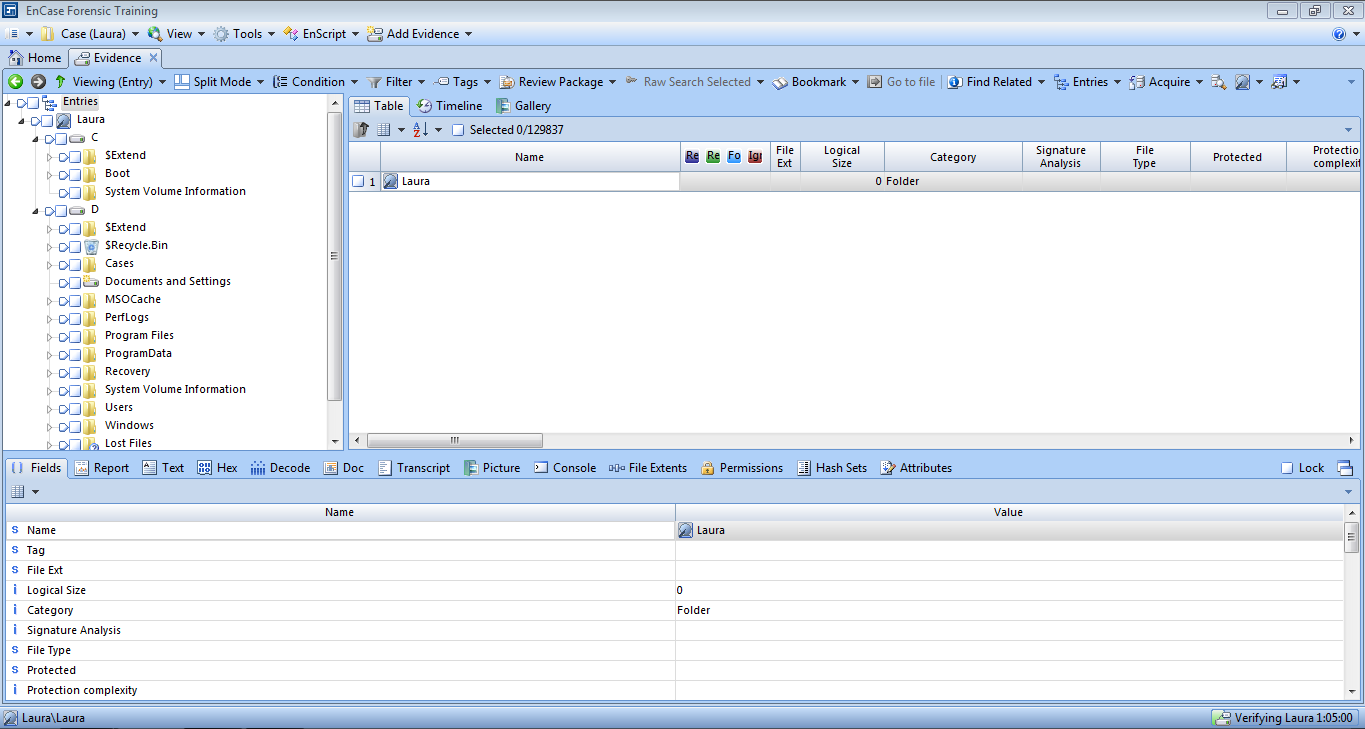


Figure A-1: Laura Case File

1. To view the MBR in the Encase program, switch the Table Pane to Disk Pane by clicking Disk View.

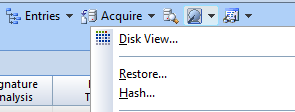


Figure A-2: Switching to Disk Pane

1. Click on the first physical sector (PS 0).

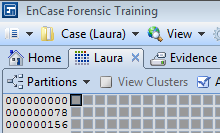


Figure A-3: PS 0

1. In the View Pane, click on Hex to view the raw data in hexadecimal presentation. The partition table begins at sector offset 446 (SO 446). Highlight the entire partition table (LE 66) from the starting point (offset 446). Immediately following the partition table is the MBR 2 byte signature (Hex 55 AA).

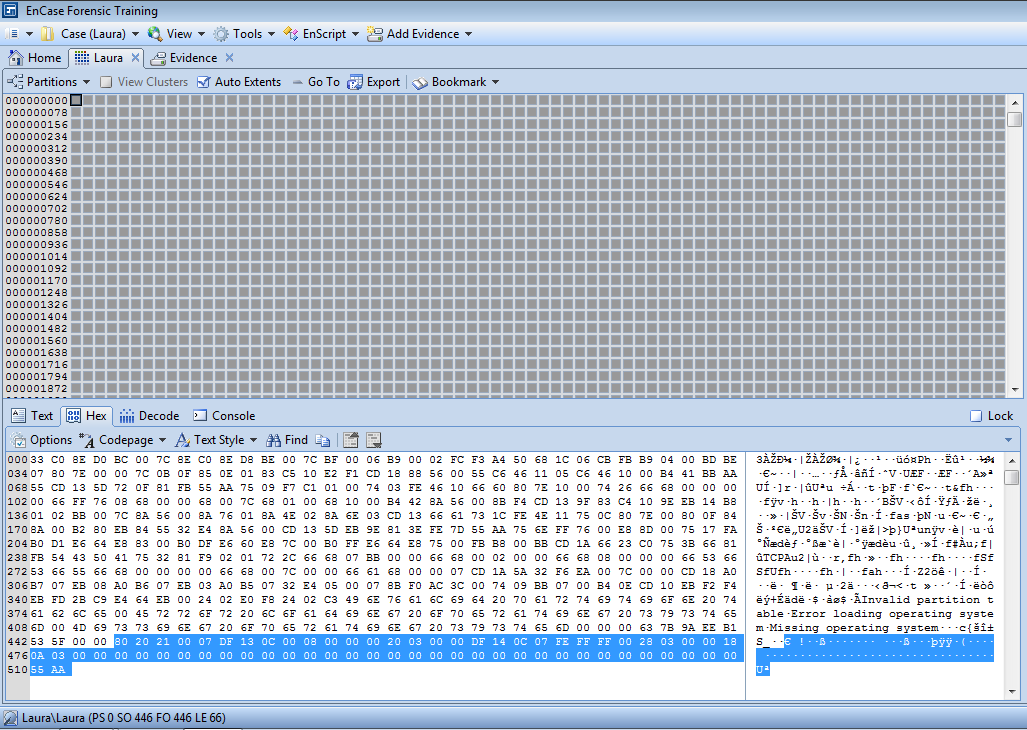
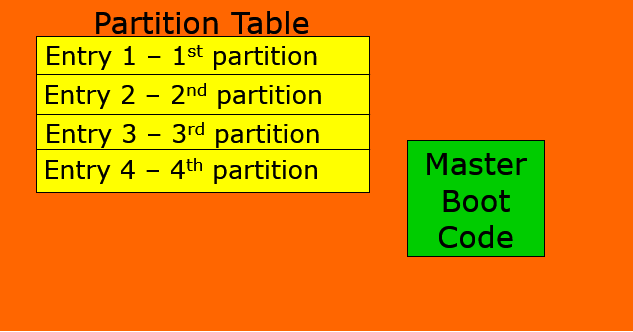


Figure A-4: MBR and the Partition Table

Q1 Sketch a diagram to show the structure of the MBR.



1. Click Decode and select Windows 🡪 Partition Entry as View Types.

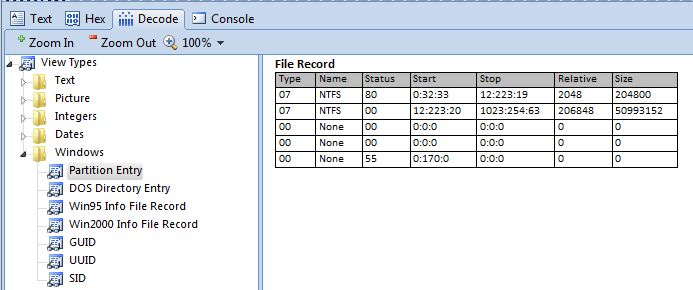


Figure A-5: Decoding Raw Data as Partition Entry

1. Right click on the Partition Entry (File Record), select Bookmark 🡪 Data Structure. In the Properties field, type “Partition Table” as Comment. Save the structure under Other Findings folder.

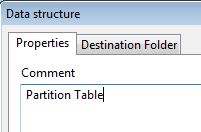


Figure A-6: Bookmarking Partition Table

A partition record consists of the following information:

1. Active (1 byte, 80=Yes, 00=No)
2. Starting sector on CHS format (3 bytes) (C-Cylinder, H-Head, S-Sector)
3. Partition Type (1 byte)
4. Ending Sector
5. Relative Sector offset (4 bytes)
6. Total Sectors of partition (4 bytes)

From the above example, the master partition table indicates that the existing partition begins at sector 2048 and has a size of 204800 sectors.

Q2 How many partitions are formatted on Laura’s hard disk? Which file system is used for each partition?

2 partition is format and both is NTFS

Q3 Which is the bootable partition?

Partition 0

Q4 Calculate the size of each partition in bytes.

Partition 0: 204800

Partition 1: 50993152

Q5 Indicate the starting and ending sector in CHS format for all partitions.

Partition 0: 0:32:33 – 12:223:19

Partition 1: 12:223:20 – 1023:254:63

**Part B: Volume/Partition Boot Record**

Using the partition information as a guide, go to the relative start point, which is physical sector 2048 (PS 2048).

1. Right click anywhere on Disk view, select Go To and enter 2048 under Other.

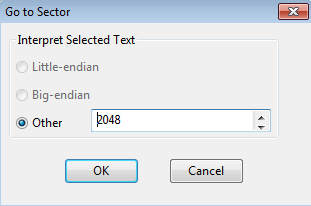
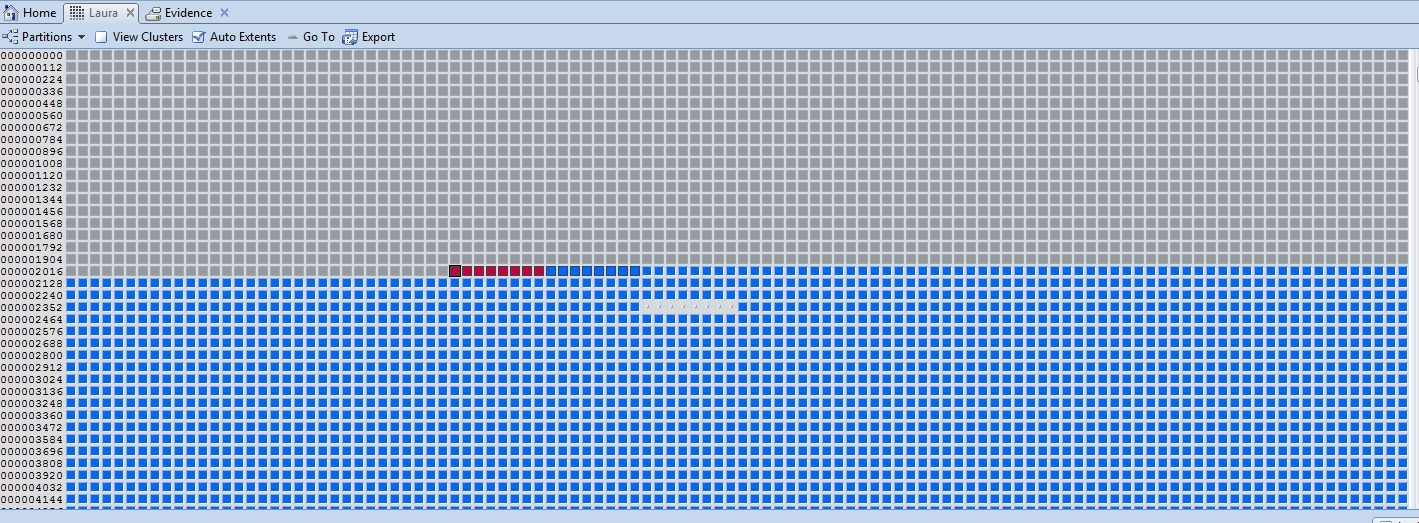


Figure B-1: Go To PS 2048

Q6 This is the volume/partition boot record (VBR). Copy the screenshot of the VBR and paste in in the box below.



You can find the File System at sector offset 3 (SO 3). Try to highlight 4 bytes from SO 3 to identify the file system.

Q7 What is the file system for this partition?

NTFS

Contained within an NTFS volume boot record (VBR) is the size of the partition, in sectors, located in the VBR at sector offset 40 (SO 40). This value is 8 bytes in length. Highlight those 8 bytes (FF 1F 03 00 00 00 00 00) right-click and decode it (Select Go To), then select Little Endian.

Q8 What is the partition size (in sectors)?

204799

Reflection: What have you learnt through this practical exercise?

How disk sector work and how storage of file work.

Decoding of data to read partition information like type and size

Reference

* Guidance Software, Inc, *EnCaseComputer Forensics I* – v6.14psvi (12.03.2009).

Reference

* Guidance Software, Inc, *EnCaseComputer Forensics II* – v6.15psvi (02.11.2010).

- The End -