|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 6 |
| Tutorial 5 |
| **Windows File System** | |

**OBJECTIVES**

After completing this topic, you should be able to:

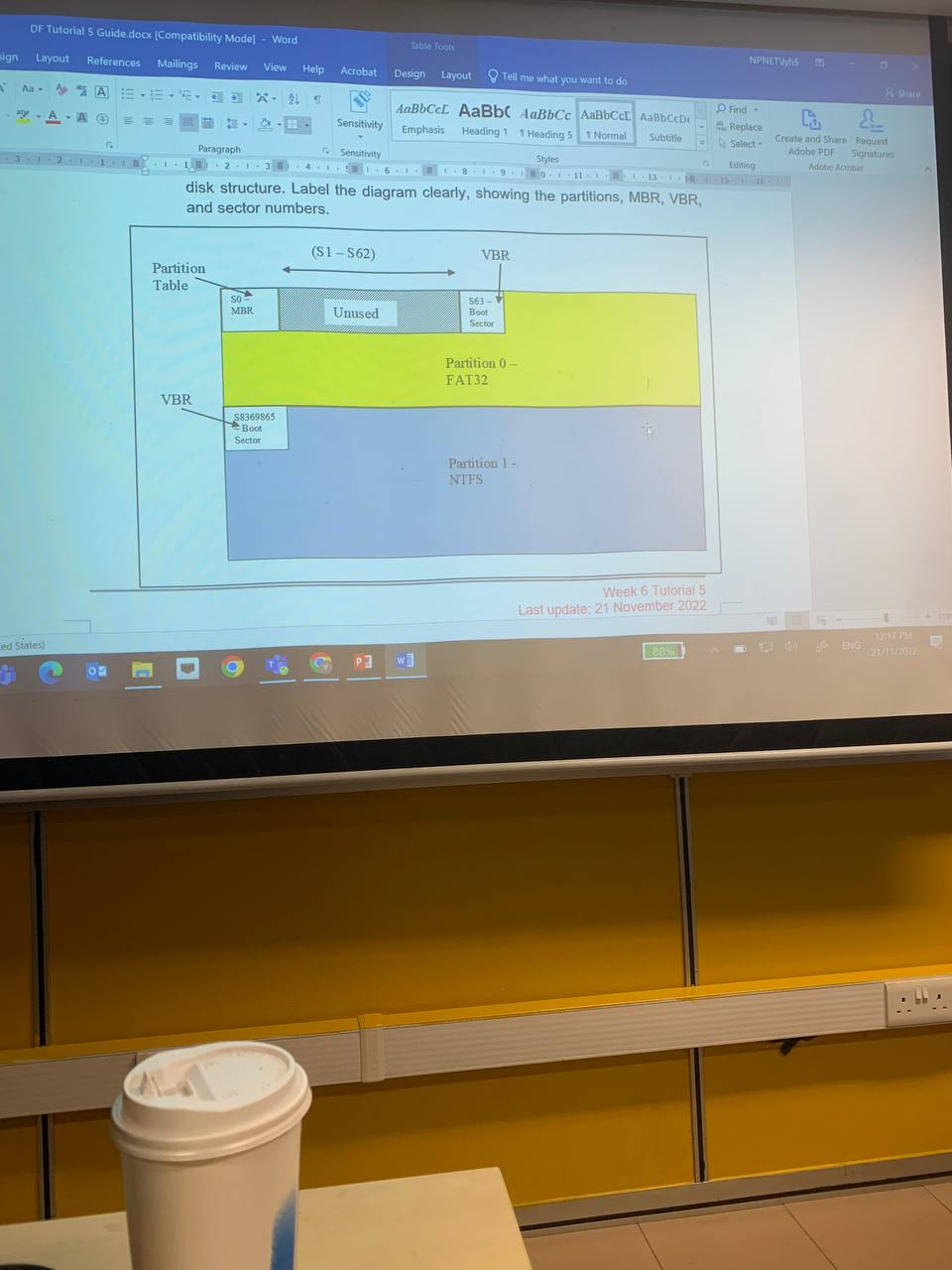
* Sketch the hard disk structure based on a partition table.
* Explain the function of master boot code.

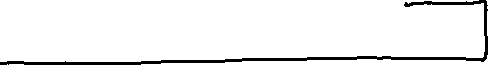
Q1. Peter is performing an examination on the image copy of a suspect’s computer. The suspect’s computer is a dual boot system and Figure 1 shows the Partition Table from the Master Boot Record of this computer. Assume that the first partition is installed with Windows XP and second partition is installed with Windows 7 operating system.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Type** | **Name** | **Status** | **Start** | **Stop** | **Relative** | **Size** |
| 0b | FAT32 | 00 | 0:1:1 | 520:254:63 | 63 | 8369802 |
| 07 | NTFS | 80 | 521:0:1 | 1023:254:63 | 8369865 | 66958920 |
| 00 | None | 00 | 0:0:0 | 0:0:0 | 0 | 0 |
| 00 | None | 00 | 0:0:0 | 0:0:0 | 0 | 0 |

Figure 1: Partition Table of Suspect’s Computer

* 1. Based on the partition table in Figure 1, sketch a diagram to show the hard disk structure. Label the diagram clearly, showing the partitions, MBR, VBR, and sector numbers.





* 1. Explain how the Master Boot Code makes use of the partition table to look for the active partition and boot the computer. Identify the active partition.

The master boot code performs the following:

* Scans the partition table for active partition, in the case the 2nd partition.
* Finds the starting sector of the active partition (sector 8369863)
* Loads a copy of the boot sector (in VBR) from the active partition into memory (RAM)
* Transfer control to te executable code in the boot sector.

- End -