Digital Forensics

SRN : PES1UG20CS825	NAME : PREM SAGAR J S	SEC : 'H'

Lab Assignment - 3

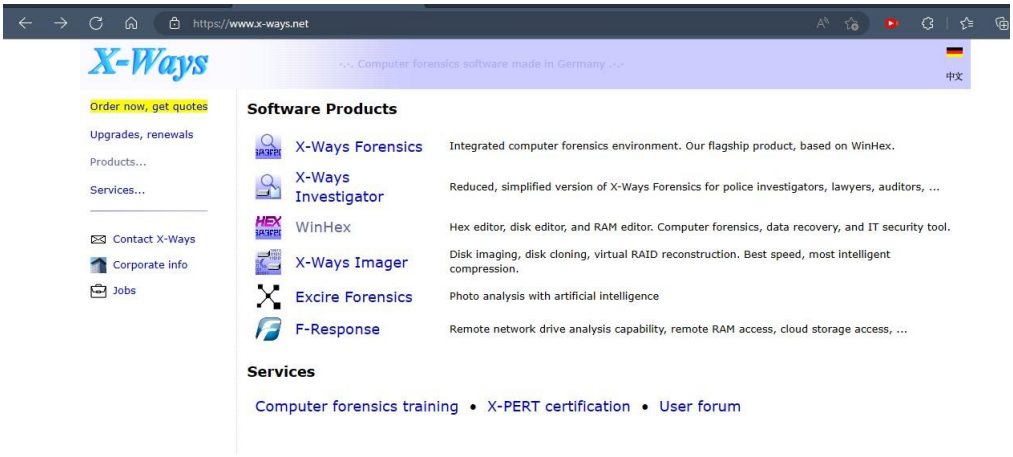
Lab 3 : Identifying the File systems

Task 1:

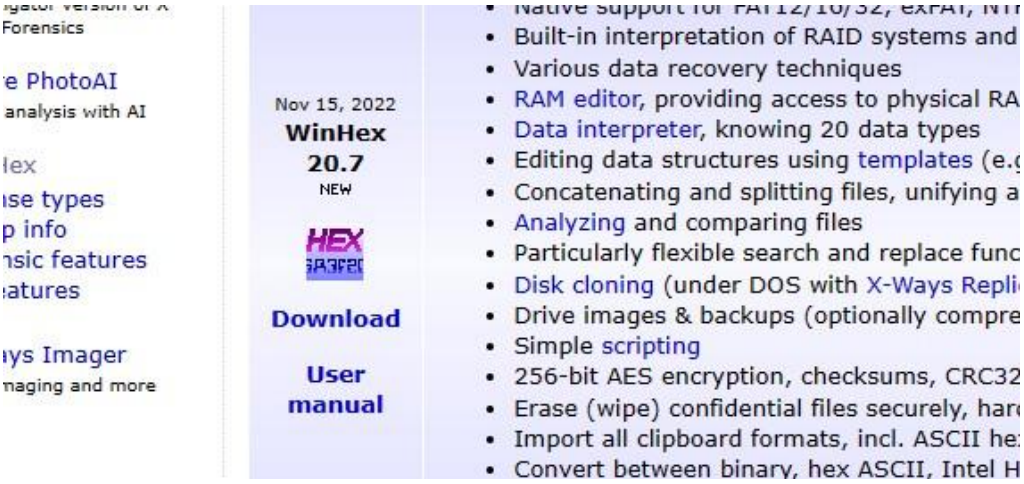
To identify the OS on an unknown disk. You can use WinHex or another hexadecimal editor, such as Hex Workshop, for this task. The following steps show you how to determine a disk's OS by using WinHex.

1. Start a Web browser, and go to http://x-ways.net. Under the Software Products heading,click WinHex. Download and install this program, after checking about where to install it on your computer.

➢ Downloading WinHex Software from the website.

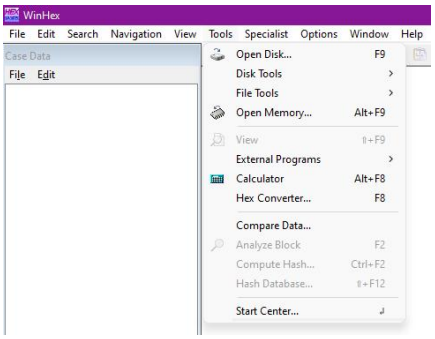


➢ Version and download Option on the website.

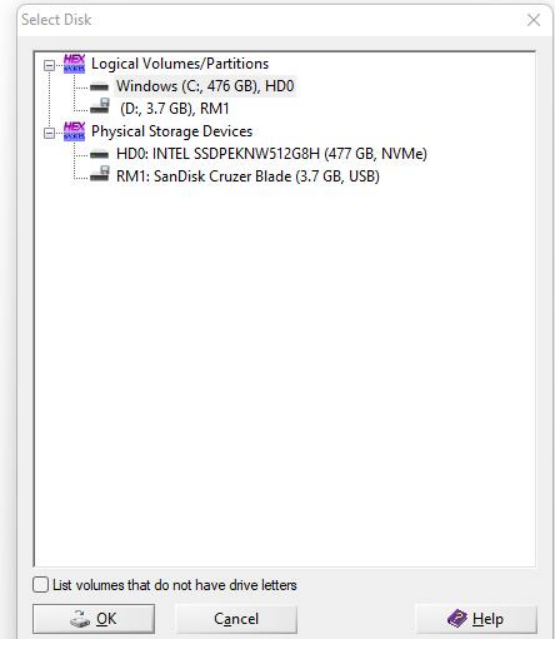


- Software downloaded successfully.

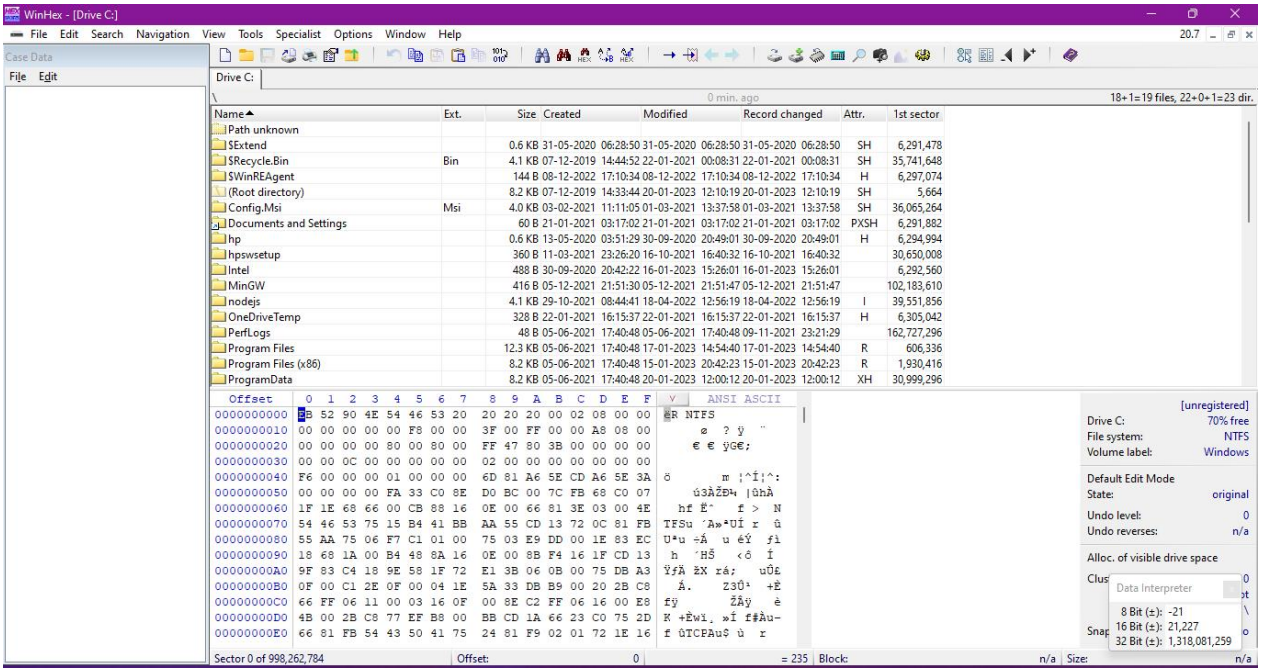
- Clicking on Tools, selecting Open Disk from the menu to get the list of logical drives.



- Selecting C drive (Partition which contains OS files.



- Showing the typical hard disk in the WinHex window.

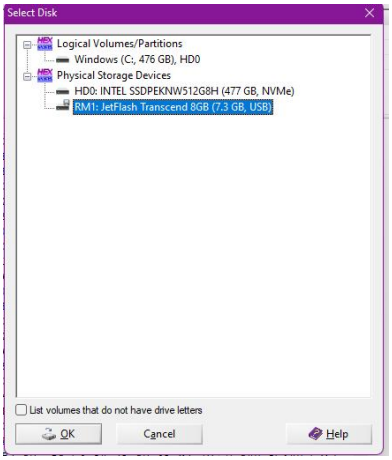


- As you can see the file system is **NTFS** type of Drive C:/.

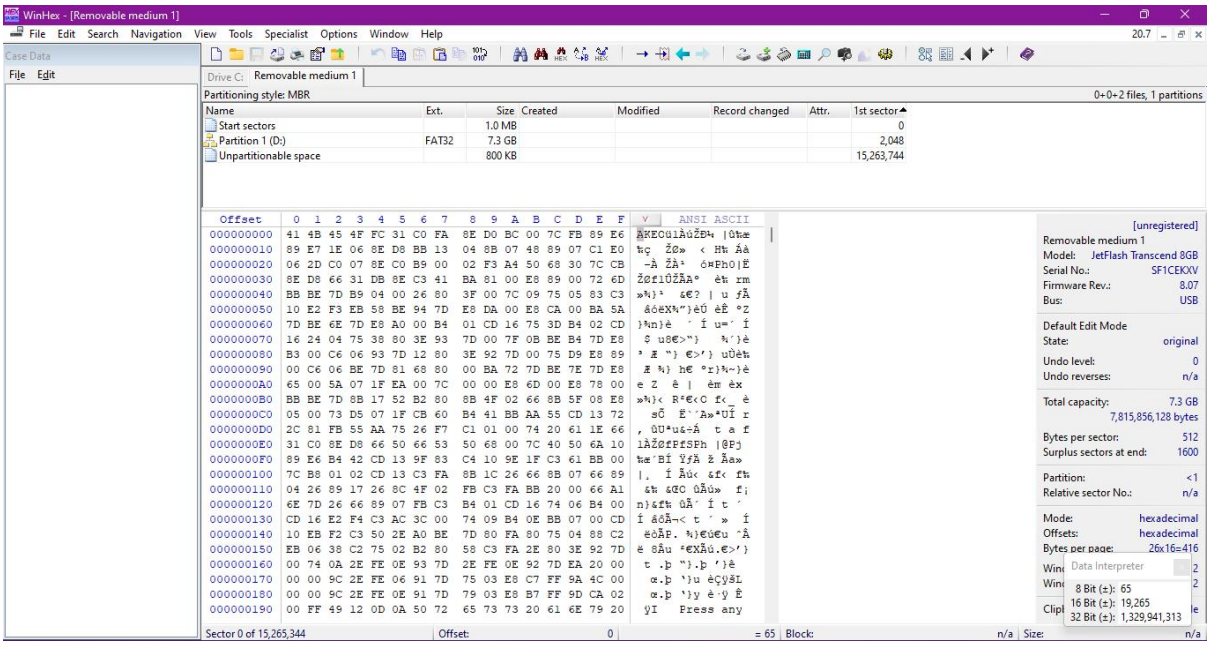
NTFS:

- New Technology File System.
- NTFS also stands for other terms, but none of them have anything to do with what's talked about on this page. These include not trusted for servers, never tested file system, new tools for storage, and no time for social.
- NTFS, an acronym that stands for New Technology File System, is a file system first introduced by Microsoft in 1993 with the release of Windows NT 3.1.
- It's the primary file system used in Microsoft's Windows 11, Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows NT operating systems.
- The Windows Server line of operating systems also primarily use NTFS. It's supported in other OSes, too, like Linux and BSD. macOS offers read-only support for NTFS.

- Opening Disk again, but this time,selecting my USB drive in the Edit Disk list.



- Displaying the information about the pendrive.



- As you can see the pendrive file ssytem type is **FAT32.**

FAT32:

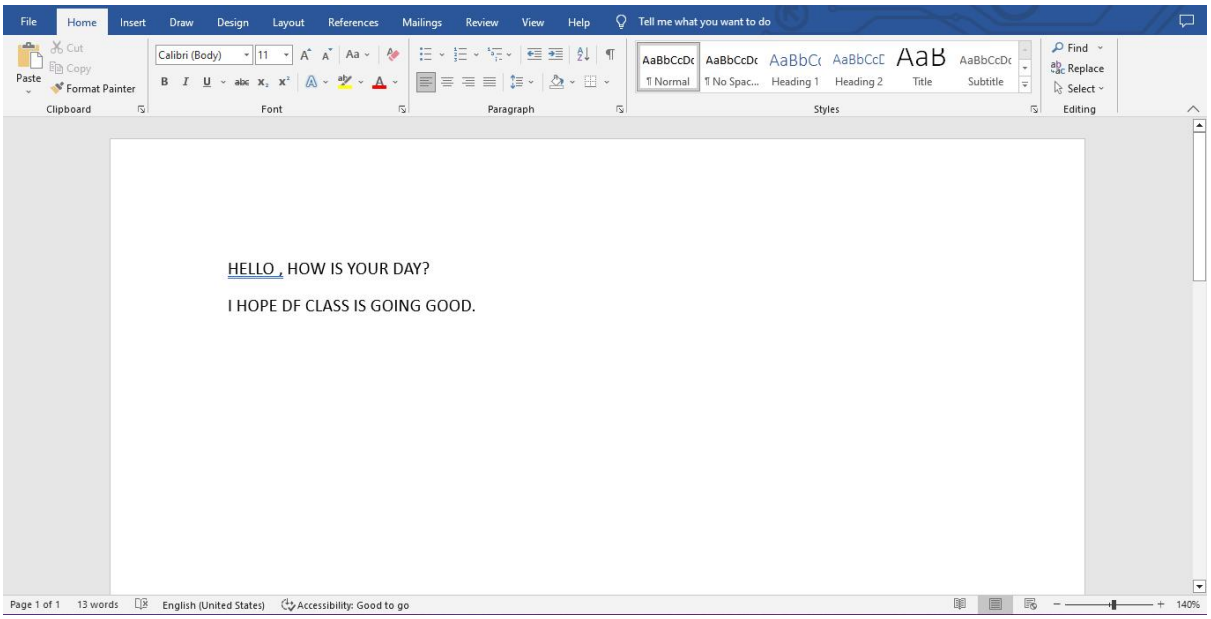
- FAT stands for **File Allocation Table**, which is the simplistic file system supported by Windows Operating System.

- It is commonly used with floppy disks, flash drives, and embedded devices. However, it is no longer the default file system for Microsoft Windows computers.

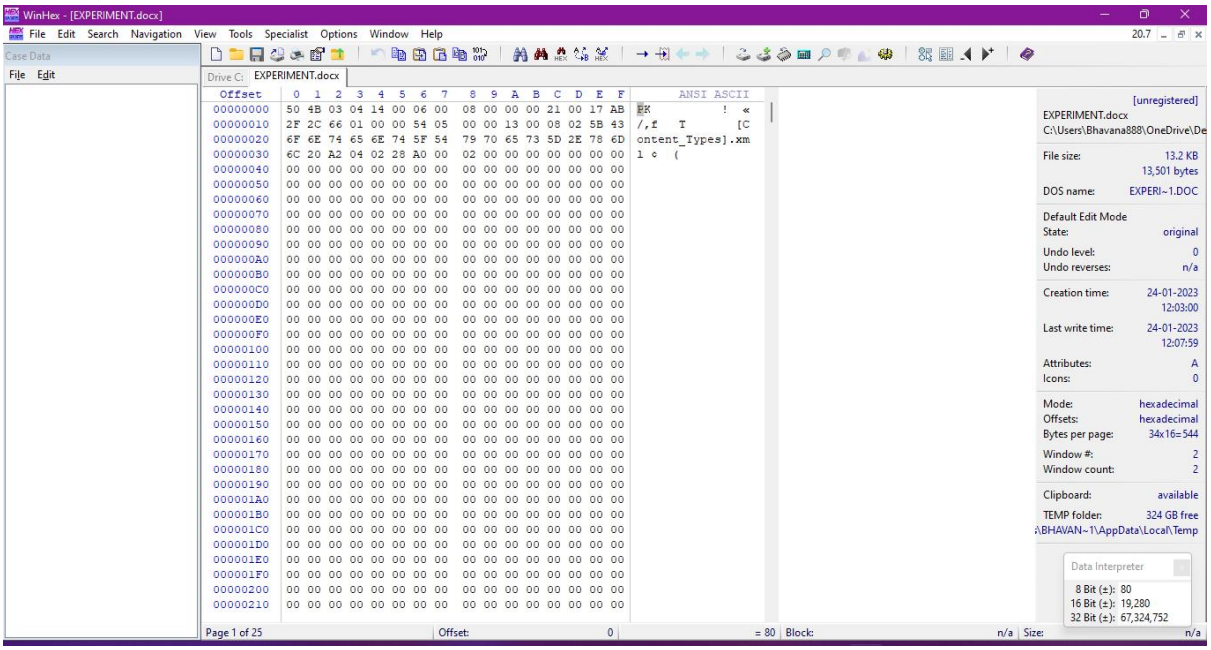
- The FAT file system has different variants that vary as per increase in disk drive capacity, and these variants are **FAT12, FAT16, and FAT32.**

Task 2:

Identify file headers to determine the file types, with or without an extension. Before performing the following steps in WinHex, use File Explorer to find a a Word document (.docx).



- Opening a Word document, clicking on File,and selecting the document .docx file.



- File Type is displayed as **PK.**

PK:

- Compressed font file created by GF to PK, a program included with some TeX software distributions; contains the compressed copy of a .GF METAFONT bitmap font file and is used for maintaining smaller font sizes.