

**PES1UG20CS581**

**ROHITH H**

**J SEC**

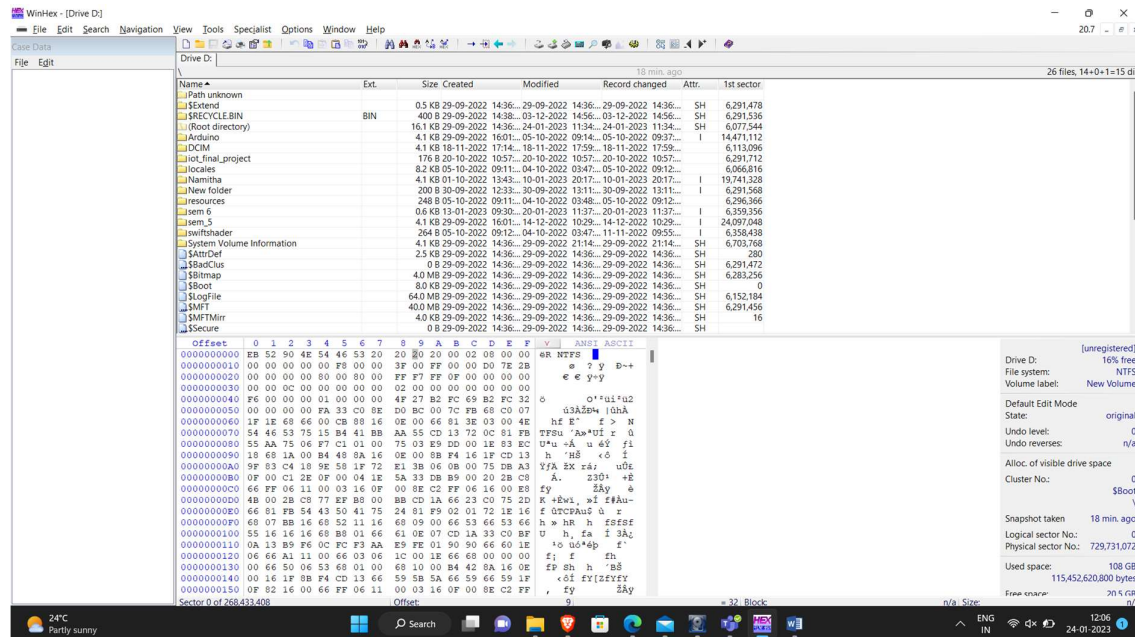
## **DIGITAL FORENSICS ASSIGNMENT -03**

### **TASK -01**

*To identify the OS on an unknown disk.*

*Local Disk screenshot on the WinHex Tool*

*For the local disk the OS is NTFS as u can see in the screenshot below*



*USB Screenshot on the WinHex Tool*

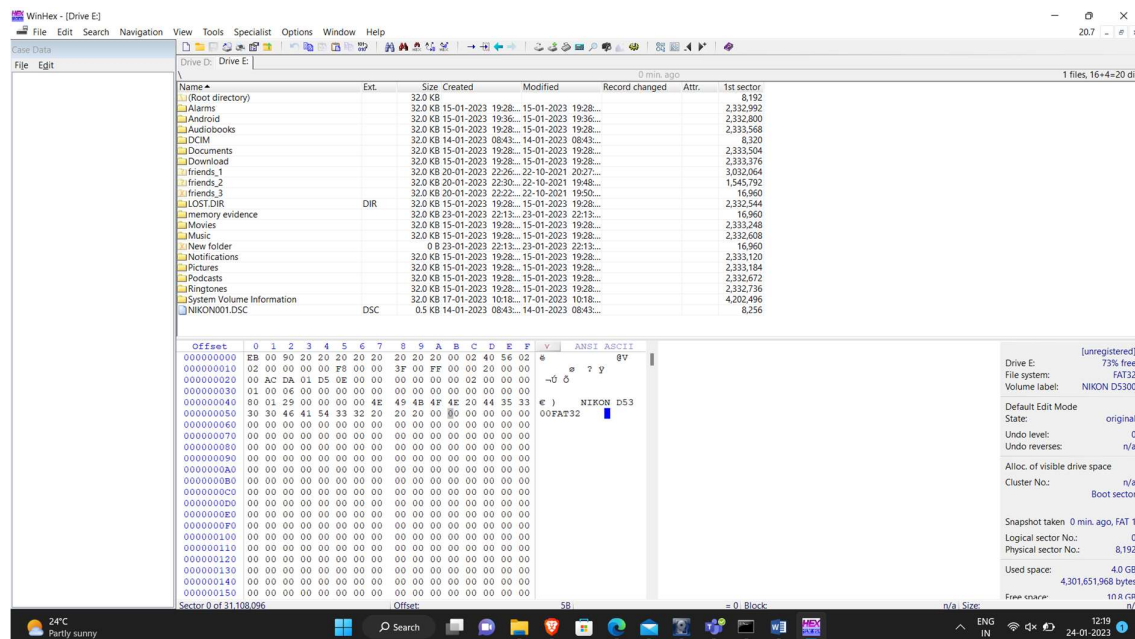
*For the USB the FAT32 is been printed on the WinHex as show in the screenshot below the File Allocation Table the disk formatting tool version 32.*

**PES1UG20CS581**

**ROHITH H**

**J SEC**

## **DIGITAL FORENSICS ASSIGNMENT -03**



### **TASK -02**

*Identify file headers to determine the file types, with or without an extension.*

*When we open the word document in the WinHex tool it shows the hexadecimal code for the documents that is “50 4B 03 04 14 00 06 00,”*

*And this is used to identify the type of document without knowing the extensions of the file and the above given hexadecimal code is displayed only for the Microsoft word documents which are above the Microsoft 2010.*

# PES1UG20CS581

## ROHITH H

### J SEC

## DIGITAL FORENSICS ASSIGNMENT -03

The screenshot displays the WinHex application interface. The top menu bar includes File, Edit, Search, Navigation, View, Tools, Specialist, Options, Window, and Help. The main window is divided into three panes. The left pane shows the 'Drive D:' directory structure, including a folder named 'sem 6' and a file named 'PES1UG20CS581\_ROHITH\_H\_DF\_01.docx'. The middle pane displays a list of files and folders with columns for Name, Ext., Size, Created, Modified, Record changed, Attr., and Test sector. The right pane shows the hex data view of the selected file, with columns for Offset, Hex, ASCII, and Comment. The hex data view shows a sequence of bytes starting with '4B 03 04 14 00 06 00'. The right sidebar contains a 'Properties' panel with details about the file, including its size (108 GB), logical sector number (138,855,440), and physical sector number (868,586,512).

Name	Ext.	Size	Created	Modified	Record changed	Attr.	Test sector
sem 6		0.0 KB	13-01-2023 09:30...	20-01-2023 11:37...	20-01-2023 11:37...	I	6,359,356
digital forensics		8.2 KB	19-01-2023 14:31...	24-01-2023 11:31...	24-01-2023 11:31...	I	79,687,680
capture memory		384 B	24-01-2023 11:12...	24-01-2023 11:20...	24-01-2023 11:20...	I	6,359,476
AccessData_FTK_Imager_4.7.1.exe	exe	510 MB	19-01-2023 14:31...	19-01-2023 14:31...	19-01-2023 14:31...	A	139,080,9...
Evidence.raw001	001	1.5 GB	24-01-2023 11:00...	24-01-2023 11:01...	24-01-2023 11:01...	A	257,117,0...
Evidence.raw001.txt	txt	1.7 KB	24-01-2023 11:09...	24-01-2023 11:10...	24-01-2023 11:11...	IA	79,702,248
Evidence.raw002	002	1.5 GB	24-01-2023 11:01...	24-01-2023 11:01...	24-01-2023 11:30...	IA	222,374,3...
Evidence.raw003	003	1.5 GB	24-01-2023 11:01...	24-01-2023 11:02...	24-01-2023 11:30...	IA	222,371,6...
Evidence.raw004	004	1.5 GB	24-01-2023 11:02...	24-01-2023 11:03...	24-01-2023 11:30...	IA	90,228,280
Evidence.raw005	005	1.5 GB	24-01-2023 11:03...	24-01-2023 11:04...	24-01-2023 11:30...	IA	97,535,240
Evidence.raw006	006	1.5 GB	24-01-2023 11:04...	24-01-2023 11:05...	24-01-2023 11:30...	IA	155,828,6...
Evidence.raw007	007	1.5 GB	24-01-2023 11:05...	24-01-2023 11:06...	24-01-2023 11:30...	IA	265,247,7...
Evidence.raw008	008	1.5 GB	24-01-2023 11:06...	24-01-2023 11:07...	24-01-2023 11:30...	IA	268,319,9...
Evidence.raw009	009	1.5 GB	24-01-2023 11:07...	24-01-2023 11:08...	24-01-2023 11:30...	IA	161,650,9...
Evidence.raw010	010	1.5 GB	24-01-2023 11:08...	24-01-2023 11:09...	24-01-2023 11:30...	IA	168,618,5...
PES1UG20CS581_ROHITH_H_DF_01.docx	docx	22.2 KB	23-01-2023 18:29...	23-01-2023 18:29...	23-01-2023 18:29...	IA	138,855,440
PES1UG20CS581_ROHITH_H_DF_01.pdf	pdf	702 KB	23-01-2023 19:24...	23-01-2023 19:24...	23-01-2023 19:24...	IA	79,731,232
winhex.zip	zip	3.6 MB	24-01-2023 11:29...	24-01-2023 11:29...	24-01-2023 11:40...	IA	145,054,3...

Offset: 0 1 2 3 4 5 6 7 8 9 A B C D E F V | ANST ASCII

108D82000 4B 03 04 14 00 06 00 08 00 00 00 21 00 91 44 PK I TO

108D82010 82 90 84 01 00 00 2D 07 00 00 13 00 08 02 5B 43 \*a - IC

108D82020 6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D content\_types].xm

108D82030 6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00 1 e (

108D82040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D820A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D820B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D820C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D820D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D820E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D820F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

108D82150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Sector 138,855,440 of 268,433,408 Offset: 108D82000 - 108D82007 Size: 8

24°C Partly sunny Search 12:19 24-01-2023