DIGITAL FORENSICS LAB

Exercise 8	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	5th September, 2021

AIM

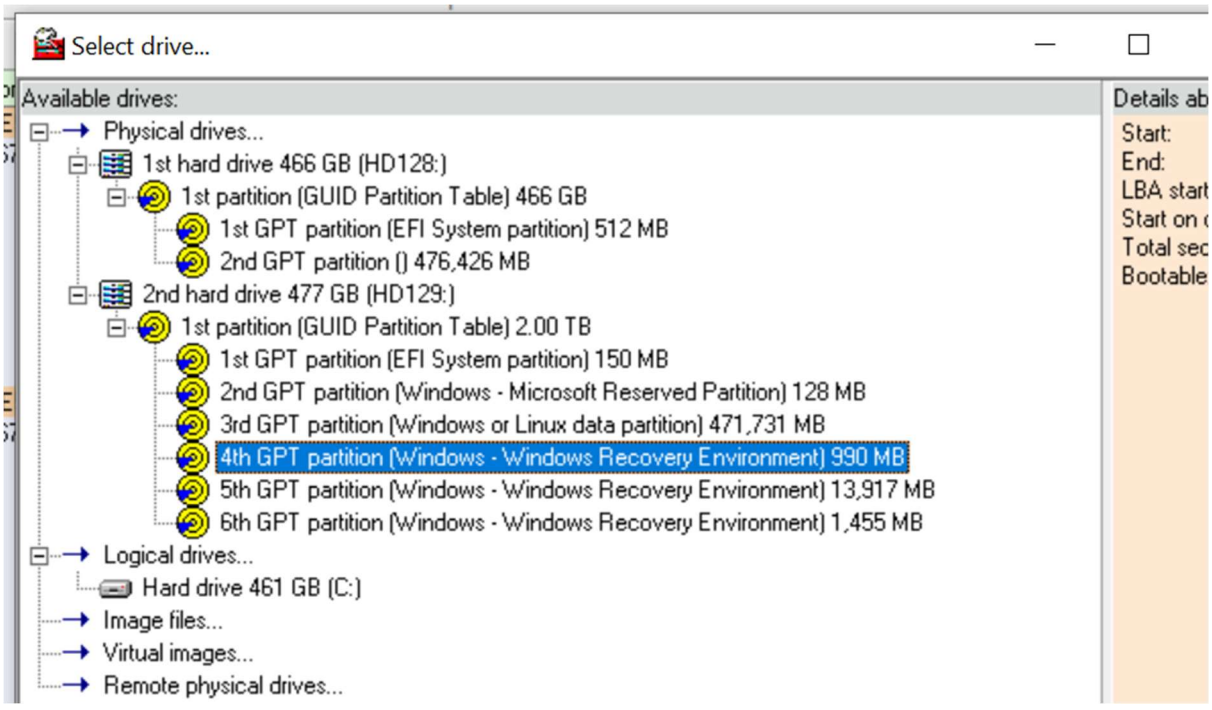
Working with DiskExplorer exploring disks and their file entries, partition table etc.

Q1

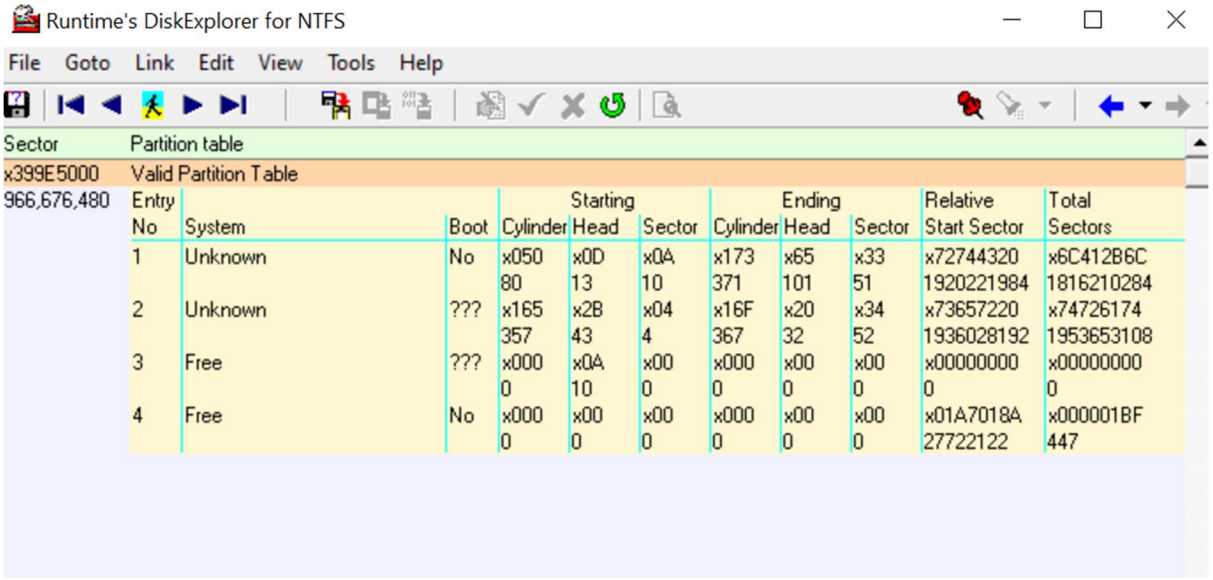
Navigate your NTFS drive by jumping to the partition table, boot record, Master file table or the root directory.

A

We select a drive first.

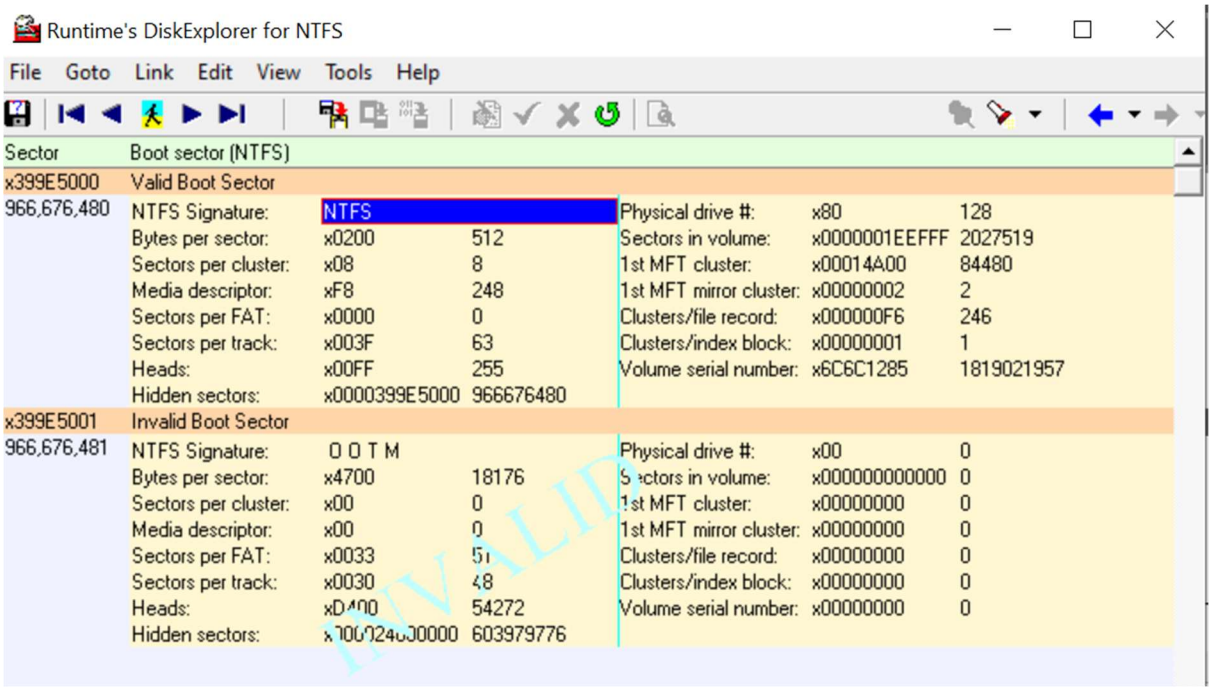


Partition table:



Sector	Partition table										
x399E5000	Valid Partition Table										
966,676,480	Entry No	System	Boot	Starting Cylinder	Starting Head	Starting Sector	Ending Cylinder	Ending Head	Ending Sector	Relative Start Sector	Total Sectors
	1	Unknown	No	x050	x0D	x0A	x173	x65	x33	x72744320	x6C412B6C
				80	13	10	371	101	51	1920221984	1816210284
	2	Unknown	???	x165	x2B	x04	x16F	x20	x34	x73657220	x74726174
				357	43	4	367	32	52	1936028192	1953653108
	3	Free	???	x000	x0A	x00	x000	x00	x00	x00000000	x00000000
				0	10	0	0	0	0	0	0
	4	Free	No	x000	x00	x00	x000	x00	x00	x01A7018A	x000001BF
				0	0	0	0	0	0	27722122	447

Boot Record:



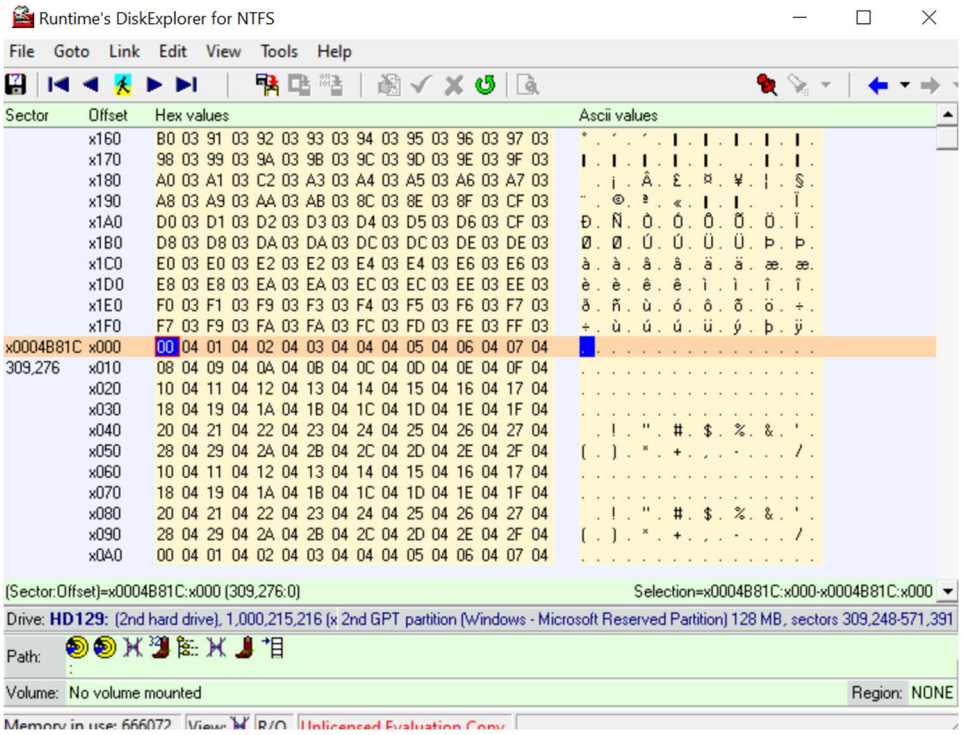
Sector	Boot sector (NTFS)					
x399E5000	Valid Boot Sector					
966,676,480	NTFS Signature:	NTFS		Physical drive #:	x80	128
	Bytes per sector:	x0200	512	Sectors in volume:	x0000001EEFFF	2027519
	Sectors per cluster:	x08	8	1st MFT cluster:	x00014A00	84480
	Media descriptor:	xF8	248	1st MFT mirror cluster:	x00000002	2
	Sectors per FAT:	x0000	0	Clusters/file record:	x000000F6	246
	Sectors per track:	x003F	63	Clusters/index block:	x00000001	1
	Heads:	x00FF	255	Volume serial number:	x6C6C1285	1819021957
	Hidden sectors:	x0000399E5000	966676480			
x399E5001	Invalid Boot Sector					
966,676,481	NTFS Signature:	0 0 T M		Physical drive #:	x00	0
	Bytes per sector:	x4700	18176	Sectors in volume:	x000000000000	0
	Sectors per cluster:	x00	0	1st MFT cluster:	x00000000	0
	Media descriptor:	x00	0	1st MFT mirror cluster:	x00000000	0
	Sectors per FAT:	x0033	51	Clusters/file record:	x00000000	0
	Sectors per track:	x0030	48	Clusters/index block:	x00000000	0
	Heads:	xD400	54272	Volume serial number:	x00000000	0
	Hidden sectors:	x[illegible]00000	603979776			

Q2

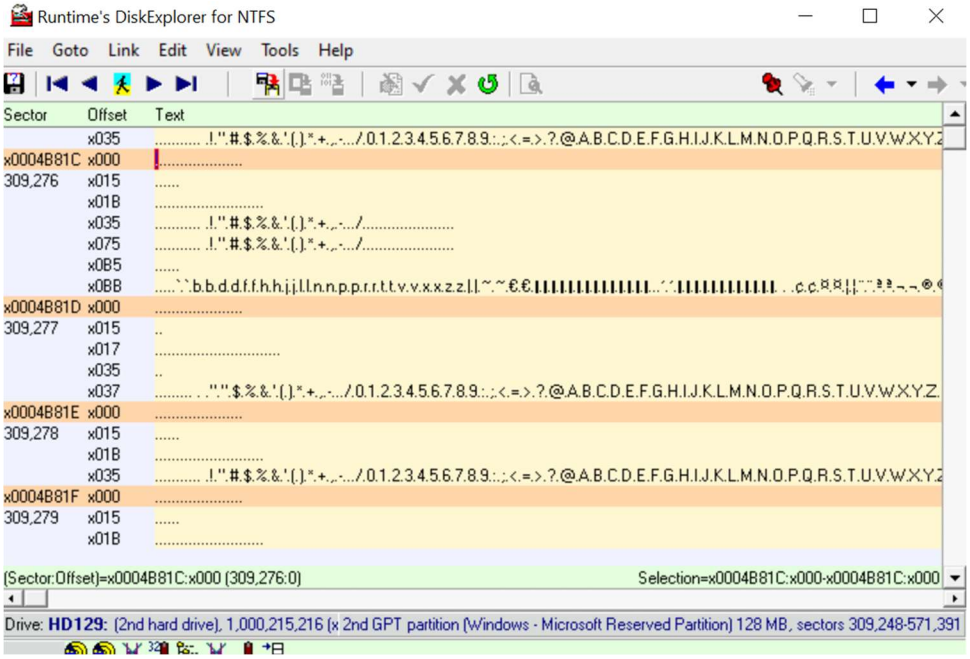
Choose between views such as hex, text, index allocation, MFT, boot record, partition table.

A

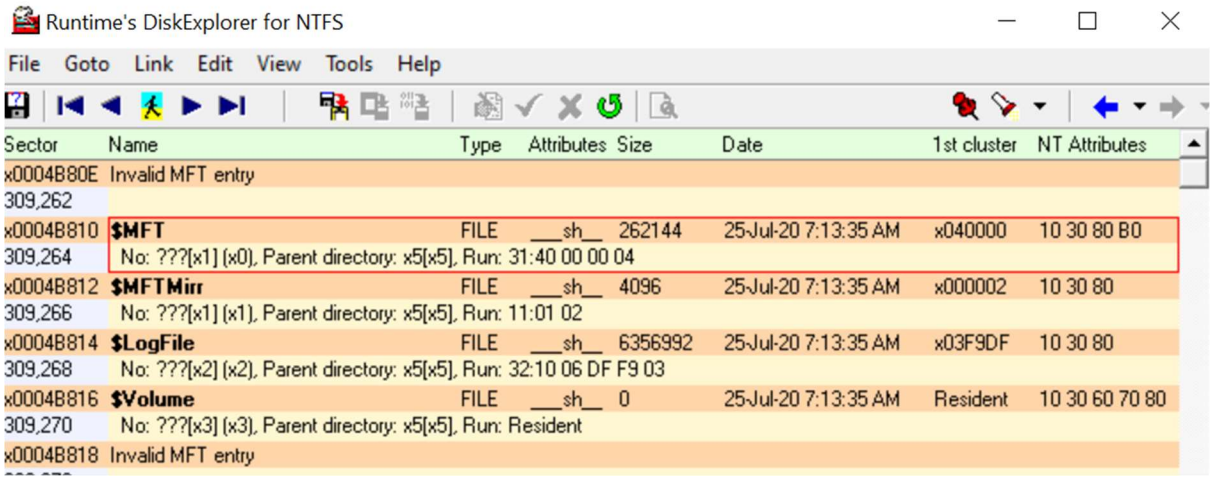
Hex View:



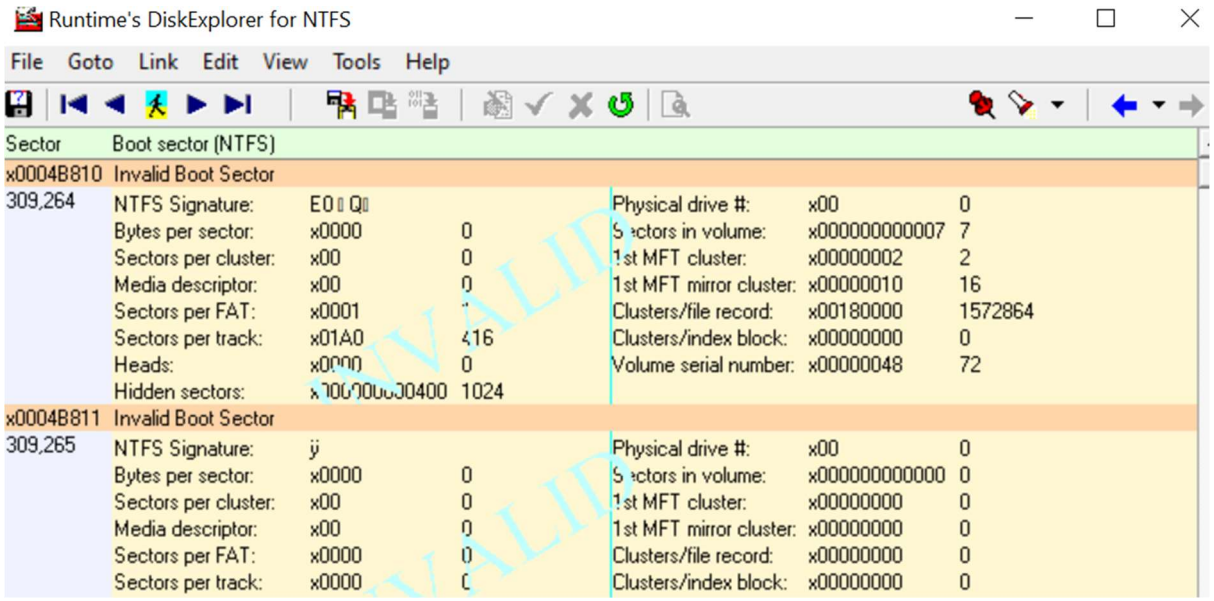
Text View:



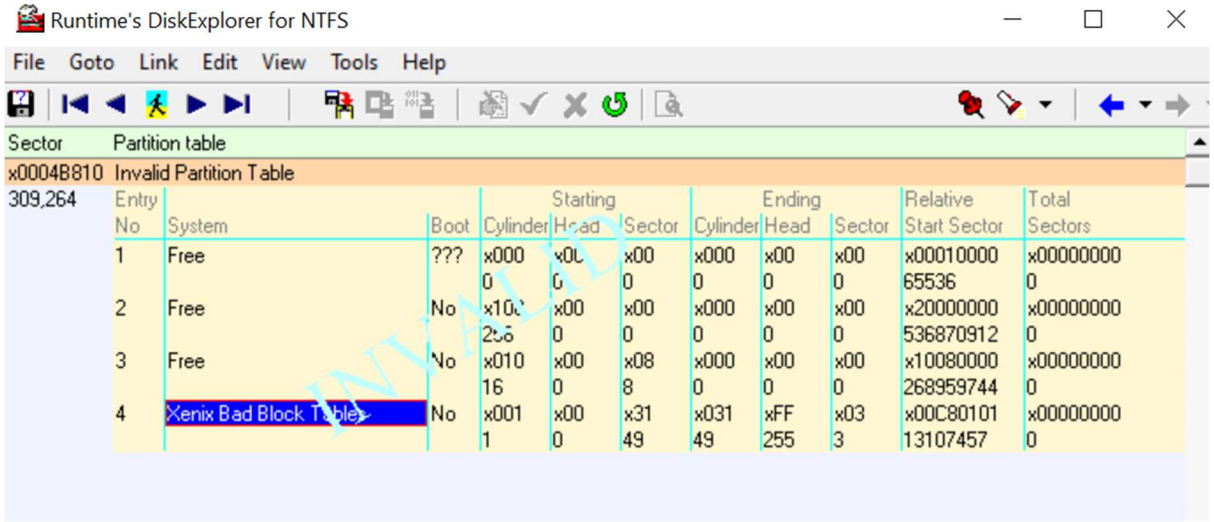
MFT:



Boot record:



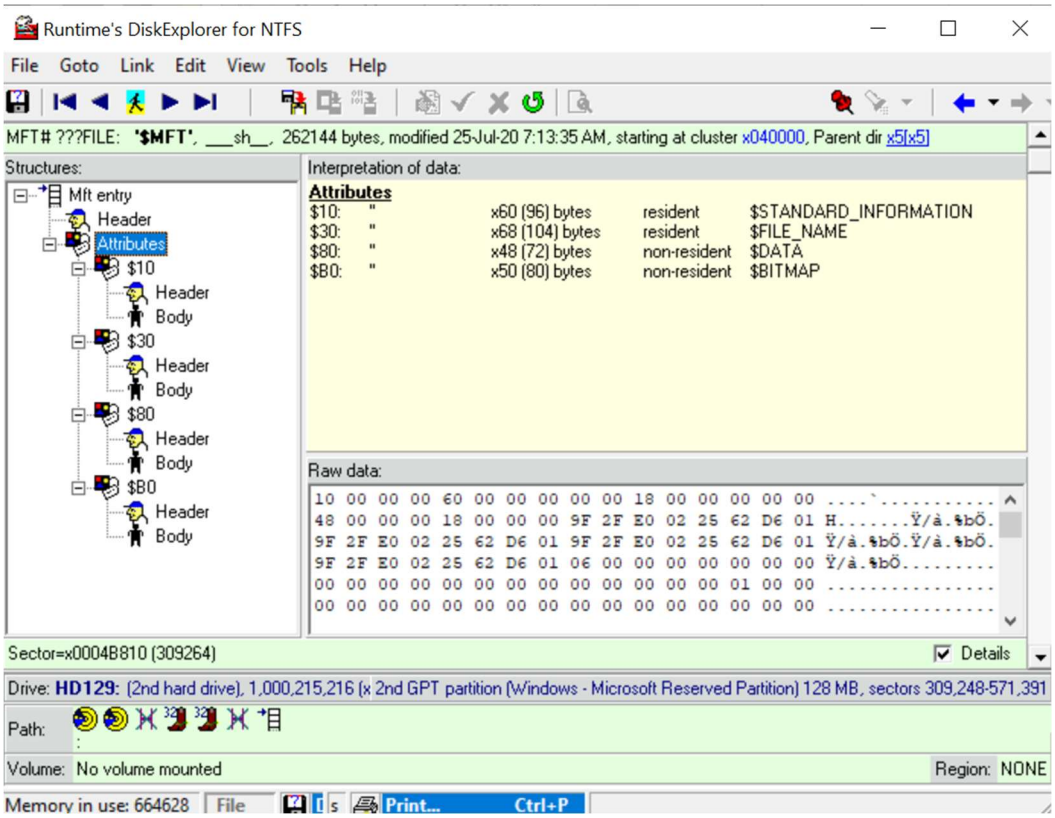
Partition table:



Q3

Inspect the file entry details, NT attributes etc.

A



OBSERVATIONS

DiskExplorer is a low-level disk editor which we use to view and manipulate information at a sector level. It is also used for data recovery from drives. As seen in screenshots above, se can see what each sector of a drive holds. This is used in Digital Forensics so as to get an idea of the suspect drive and its contents. We can see the partition table

CONCLUSION

We have worked with DiskExplorer and discovered its capability and functionalities. The tool is powerful enough to interact with the disk on a sector level and recover data.