

DIGITAL FORENSICS LAB

Exercise 8

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

AIM

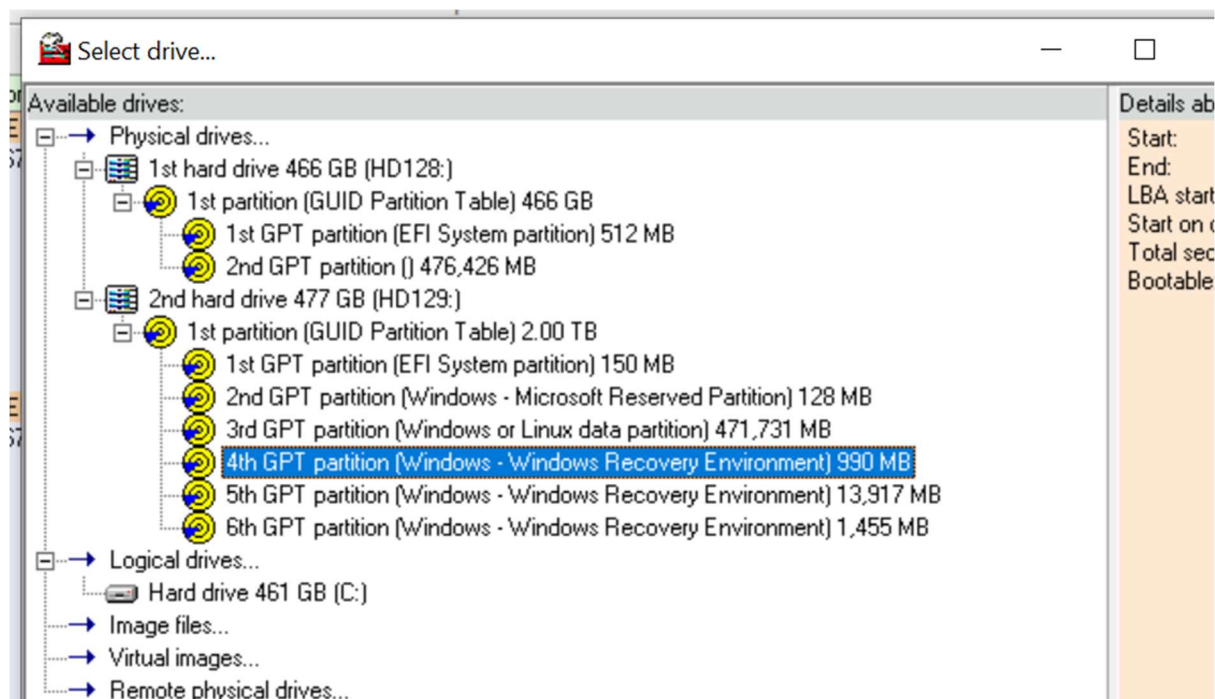
Working with DiskExplorer exploring disks and their file entries, partition table etc.

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:

Runtime's DiskExplorer for NTFS

File Goto Link Edit View Tools Help

Sector Partition table

x399E5000 Valid Partition Table

966,676,480

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

Boot Record:

Runtime's DiskExplorer for NTFS

File Goto Link Edit View Tools Help

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

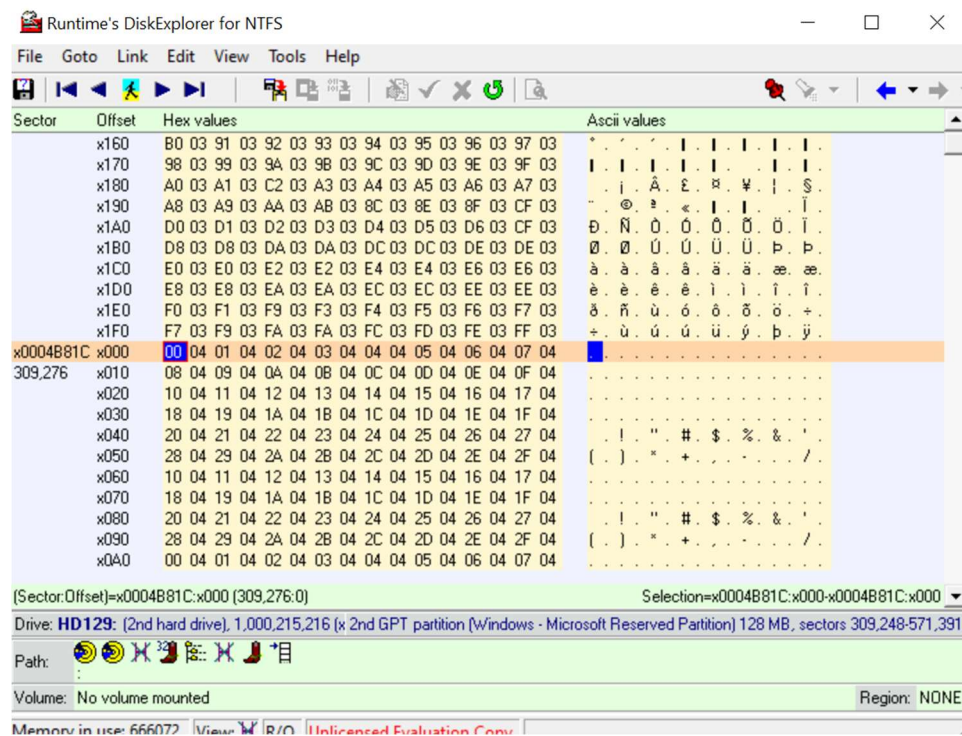
| | | | | |
|----------------------|-------------------------|-------------------------|---------------|---|
| NTFS Signature: | 0 0 T M | Physical drive #: | x00 | 0 |
| Bytes per sector: | x4700 18176 | Sectors in volume: | x000000000000 | 0 |
| Sectors per cluster: | x00 0 | 1st MFT cluster: | x00000000 | 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: | x0400 54272 | Volume serial number: | x00000000 | 0 |
| Hidden sectors: | x700724000000 603979776 | | | |

Q2

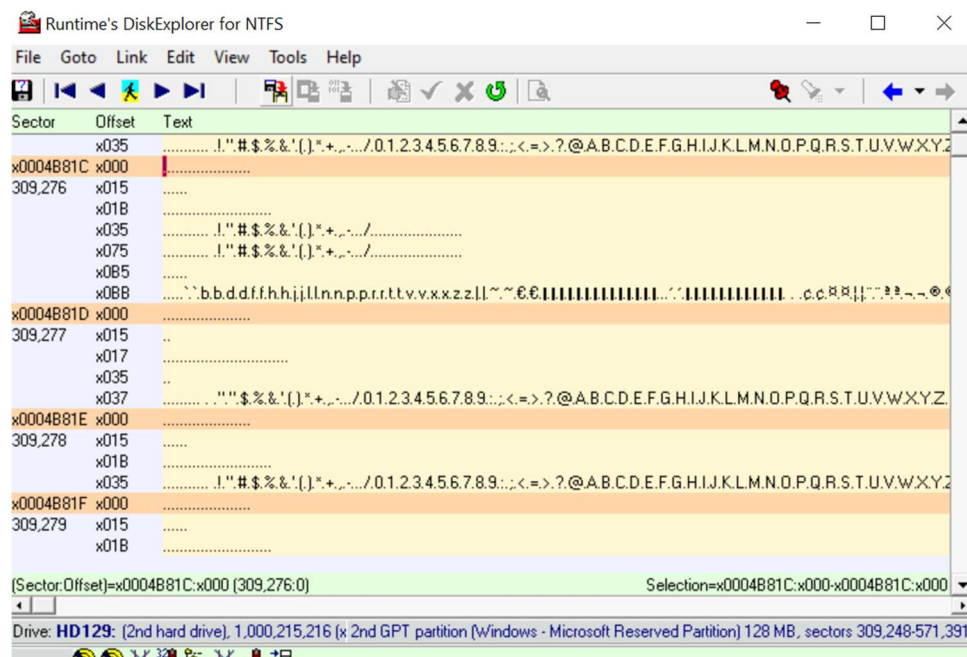
Choose between views such as hex, text, index allocation, MFT, boot record, partition table.

A

Hex View:



Text View:



MFT:

Runtime's DiskExplorer for NTFS

| Sector | Name | Type | Attributes | Size | Date | 1st cluster | NT Attributes |
|-----------|--|------|------------|---------|----------------------|-------------|----------------|
| x0004B80E | Invalid MFT entry | | | | | | |
| 309,262 | | | | | | | |
| x0004B810 | \$MFT | FILE | __sh__ | 262144 | 25-Jul-20 7:13:35 AM | x040000 | 10 30 80 B0 |
| 309,264 | No: ???[x1] (x0), Parent directory: x5[x5], Run: 31:40 00 00 04 | | | | | | |
| x0004B812 | \$MFTMirr | FILE | __sh__ | 4096 | 25-Jul-20 7:13:35 AM | x000002 | 10 30 80 |
| 309,266 | No: ???[x1] (x1), Parent directory: x5[x5], Run: 11:01 02 | | | | | | |
| x0004B814 | \$LogFile | FILE | __sh__ | 6356992 | 25-Jul-20 7:13:35 AM | x03F9DF | 10 30 80 |
| 309,268 | No: ???[x2] (x2), Parent directory: x5[x5], Run: 32:10 06 DF F9 03 | | | | | | |
| x0004B816 | \$Volume | FILE | __sh__ | 0 | 25-Jul-20 7:13:35 AM | Resident | 10 30 60 70 80 |
| 309,270 | No: ???[x3] (x3), Parent directory: x5[x5], Run: Resident | | | | | | |
| x0004B818 | Invalid MFT entry | | | | | | |

Boot record:

Runtime's DiskExplorer for NTFS

| Sector | Boot sector (NTFS) | |
|-----------|-------------------------------------|---|
| x0004B810 | Invalid Boot Sector | |
| 309,264 | NTFS Signature: E0 00 00 00 | Physical drive #: x00 0 |
| | Bytes per sector: x0000 0 | Sectors in volume: x000000000007 7 |
| | Sectors per cluster: x00 0 | 1st MFT cluster: x00000002 2 |
| | Media descriptor: x00 0 | 1st MFT mirror cluster: x00000010 16 |
| | Sectors per FAT: x0001 1 | Clusters/file record: x00180000 1572864 |
| | Sectors per track: x01A0 416 | Clusters/index block: x00000000 0 |
| | Heads: x0000 0 | Volume serial number: x00000048 72 |
| | Hidden sectors: x7067000030400 1024 | |
| x0004B811 | Invalid Boot Sector | |
| 309,265 | NTFS Signature: 00 00 00 00 | Physical drive #: x00 0 |
| | Bytes per sector: x0000 0 | 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: x0000 0 | Clusters/file record: x00000000 0 |
| | Sectors per track: x0000 0 | Clusters/index block: x00000000 0 |

Partition table:

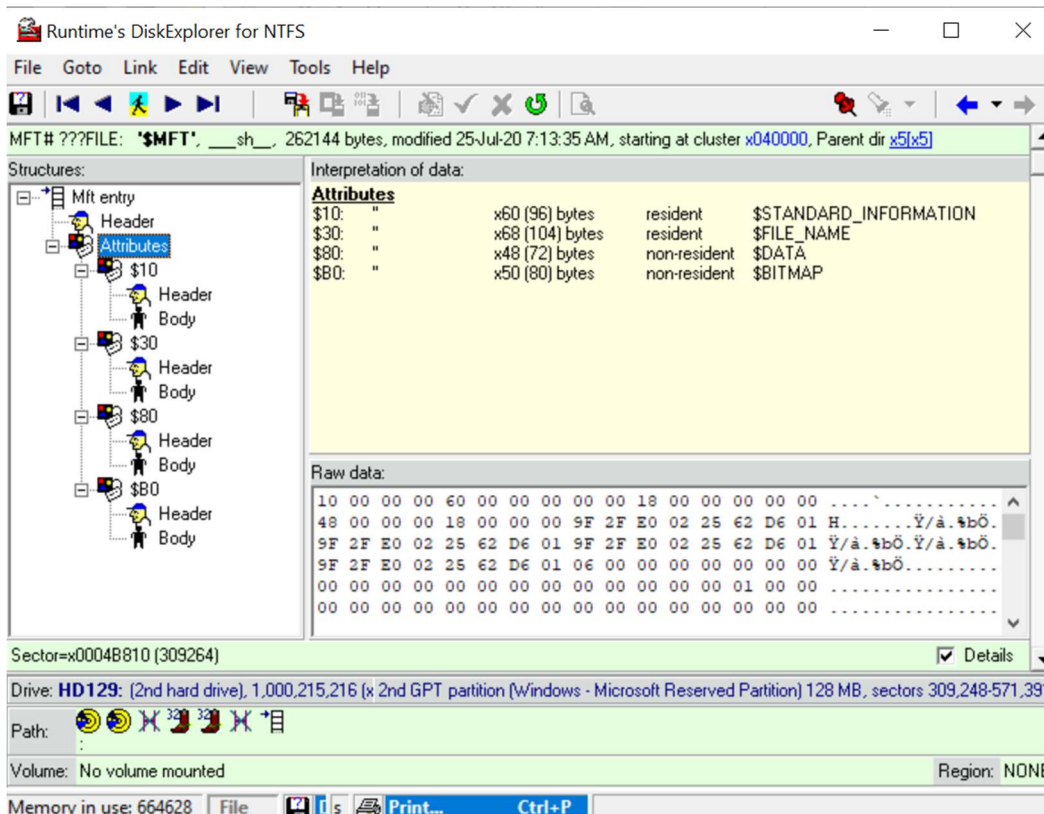
Runtime's DiskExplorer for NTFS

| Sector | Partition table | | | | | | | | | | |
|-----------|-------------------------|-----------------------|------|----------|-------|--------|----------|---------|--------|-----------------------|---------------|
| x0004B810 | Invalid Partition Table | | | | | | | | | | |
| 309,264 | Entry No | System | Boot | Cylinder | Head | Sector | Cylinder | Head | Sector | Relative Start Sector | Total Sectors |
| | 1 | Free | ??? | x000 0 | x00 0 | x00 0 | x000 0 | x00 0 | x00 0 | x00010000 65536 | x00000000 0 |
| | 2 | Free | No | x100 0 | x00 0 | x00 0 | x000 0 | x00 0 | x00 0 | x20000000 536870912 | x00000000 0 |
| | 3 | Free | No | x010 16 | x00 0 | x08 8 | x000 0 | x00 0 | x00 0 | x10080000 268959744 | x00000000 0 |
| | 4 | Xenix Bad Block Table | No | x001 1 | x00 0 | x31 49 | x031 49 | xFF 255 | x03 3 | x00C80101 13107457 | x00000000 0 |

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, we 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.