

## CSE 4004

### Digital Forensics

#### Lab Session 8

TOPIC: Investigating NTFS / FAT/ Linux drives

---

Name: Makesh Srinivasan  
Registration number: 19BCE1717  
Slot: L49 + L50  
Date: 30-September-2021-Monday  
Faculty: Prof. Nagaraj

---

**AIM:** Exploring and Investigating NTFS/FAT/Linux drives in Linux and Microsoft Windows 10 environments

#### **INSTRUCTIONS:**

Download an evaluation version of a tool for exploring disk drives such as DiskExplorer from <https://www.runtime.org/diskexplorer.htm>

It is available for NTFS, FAT and Linux.

Use the tool to investigate your NTFS drive and conduct your data recovery, using the following features:

- 1) Navigate your NTFS drive by jumping to the partition table, boot record, Master file table or the root directory.
- 2) Choose between views such as hex, text, index allocation, MFT, boot record, partition table.
- 3) Inspect the file entry details, NT attributes etc.
- 4) Search your drive for text, partition tables, boot records, MFT entries, and index buffers.

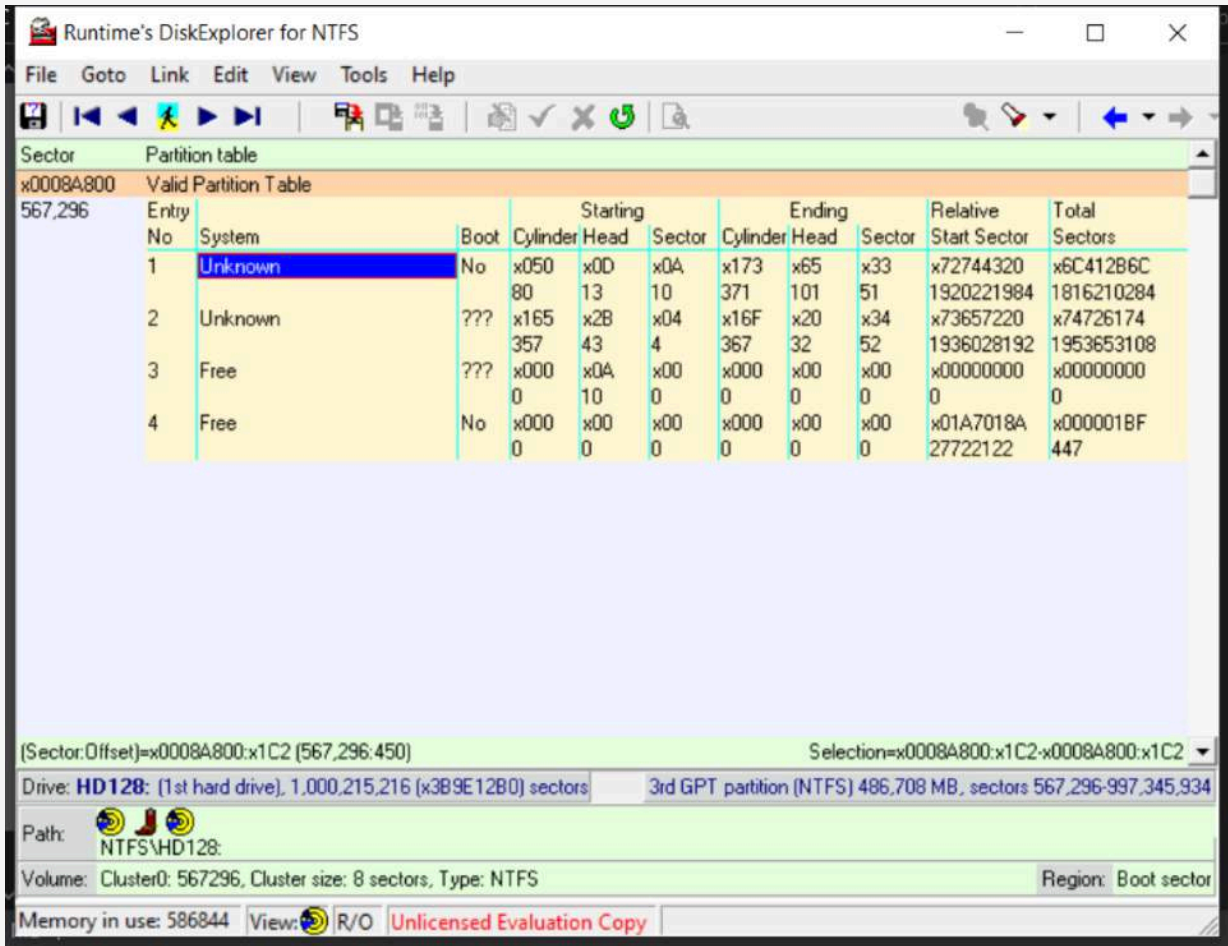
Do a similar exercise for FAT and Linux drives.

Include screenshots in your submission.

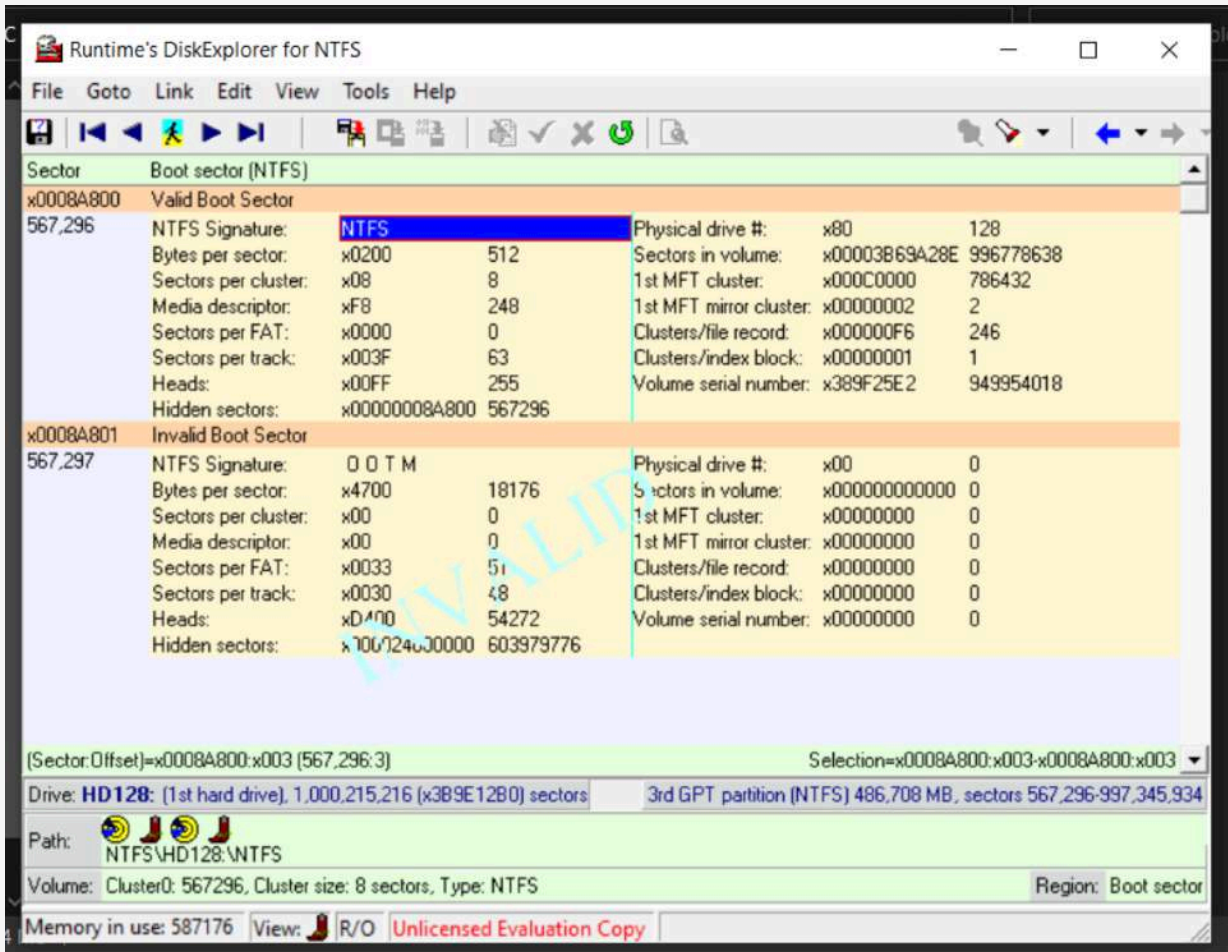
OBSERVATION:

1) NTFS

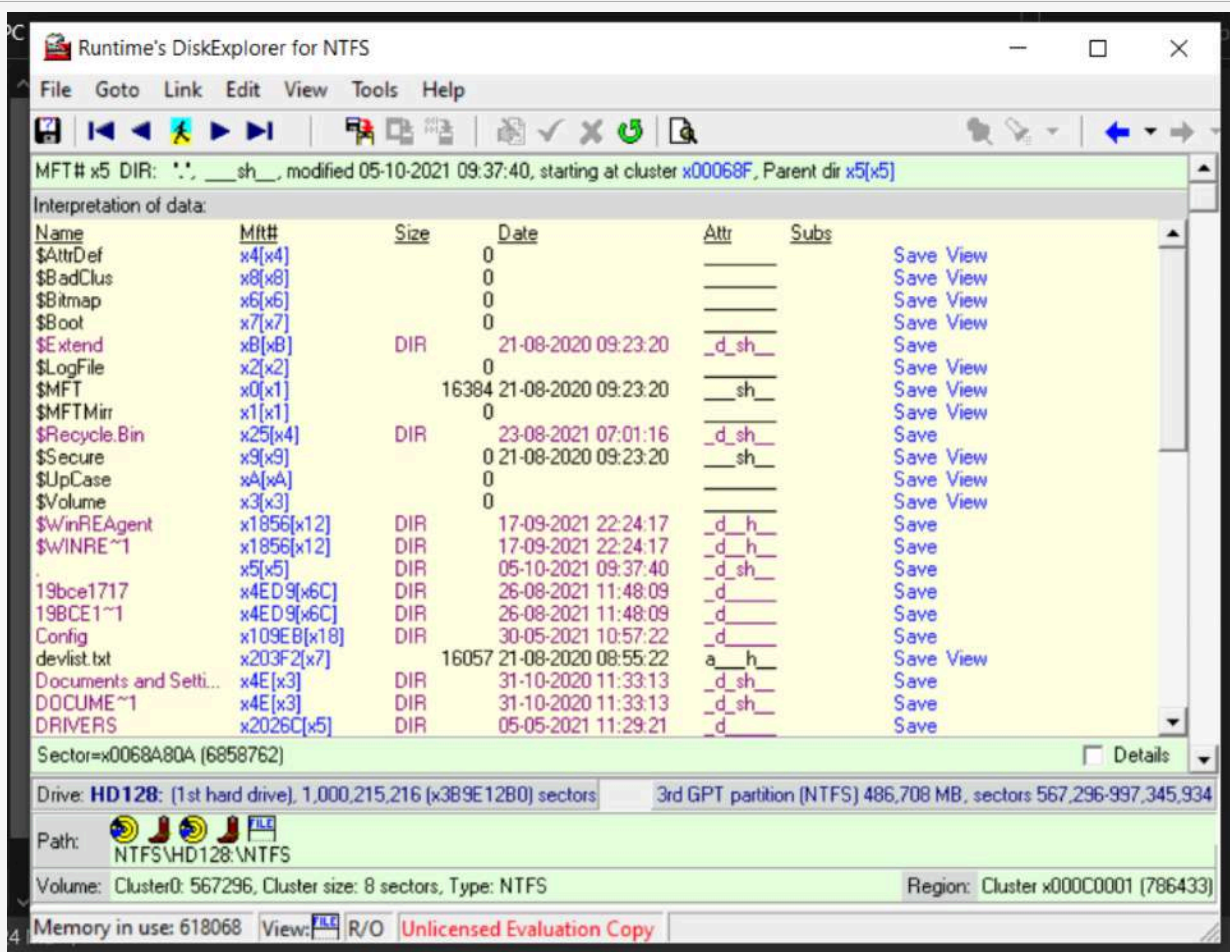
Partition table



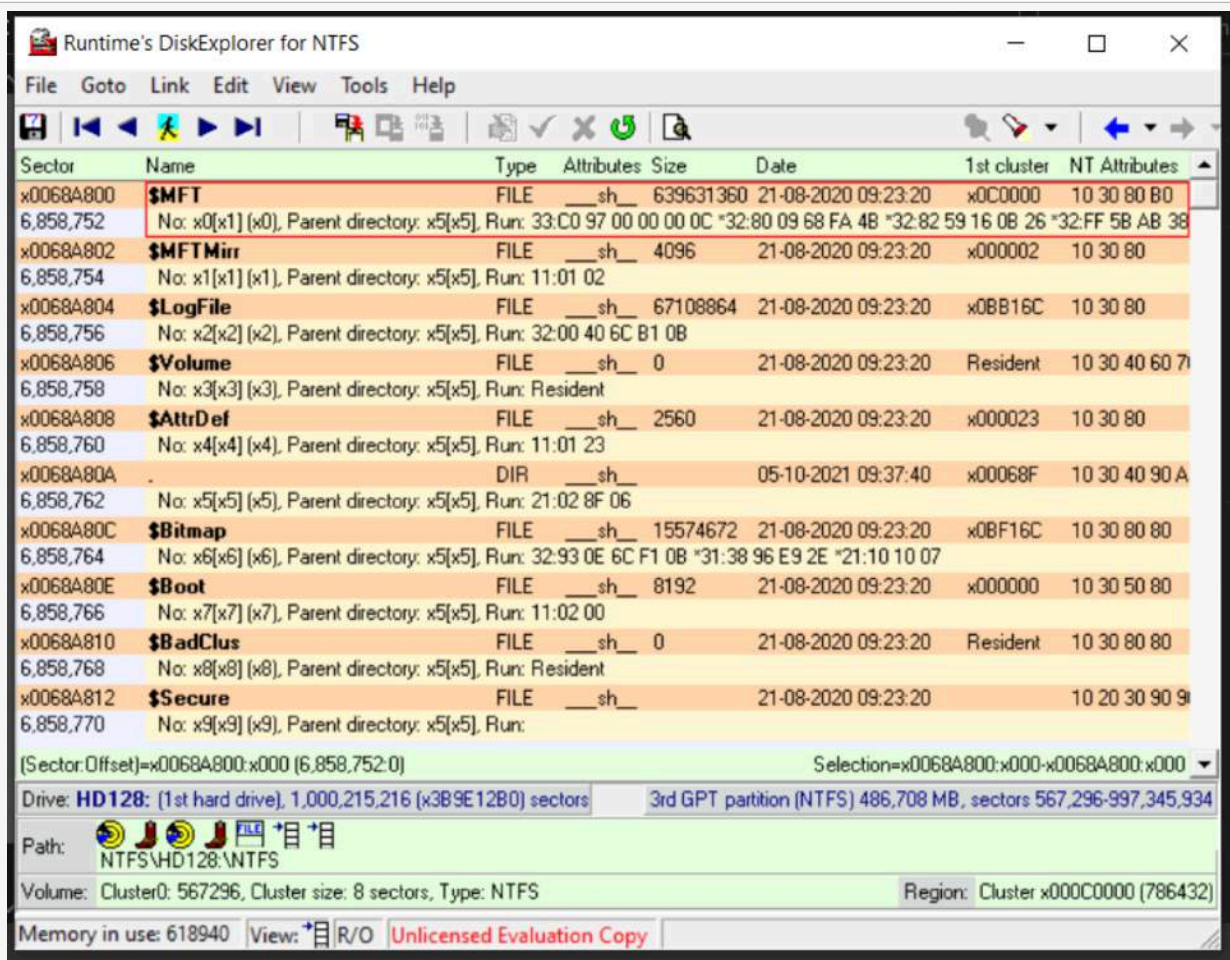
Boot sector



Root directory

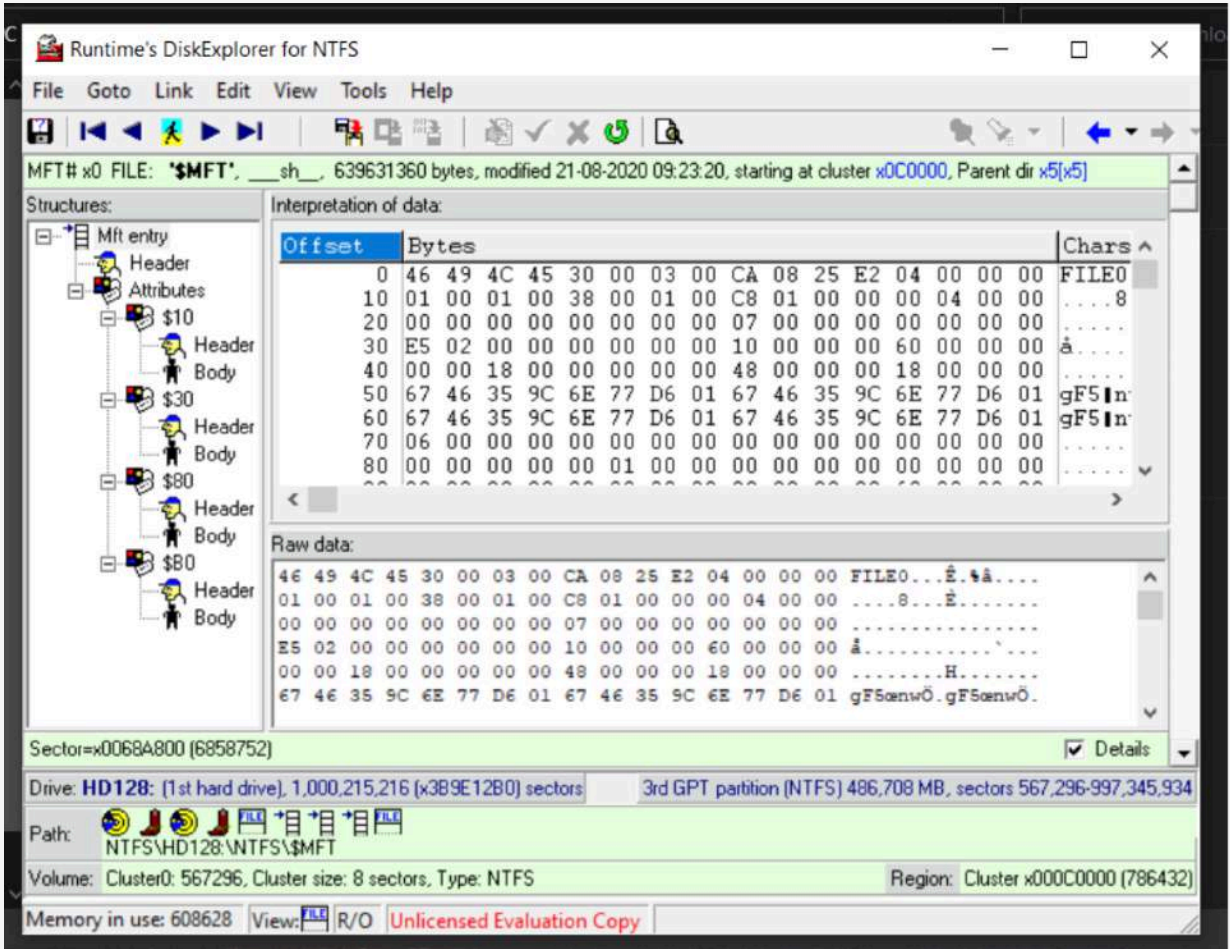


MFT (Master file table)

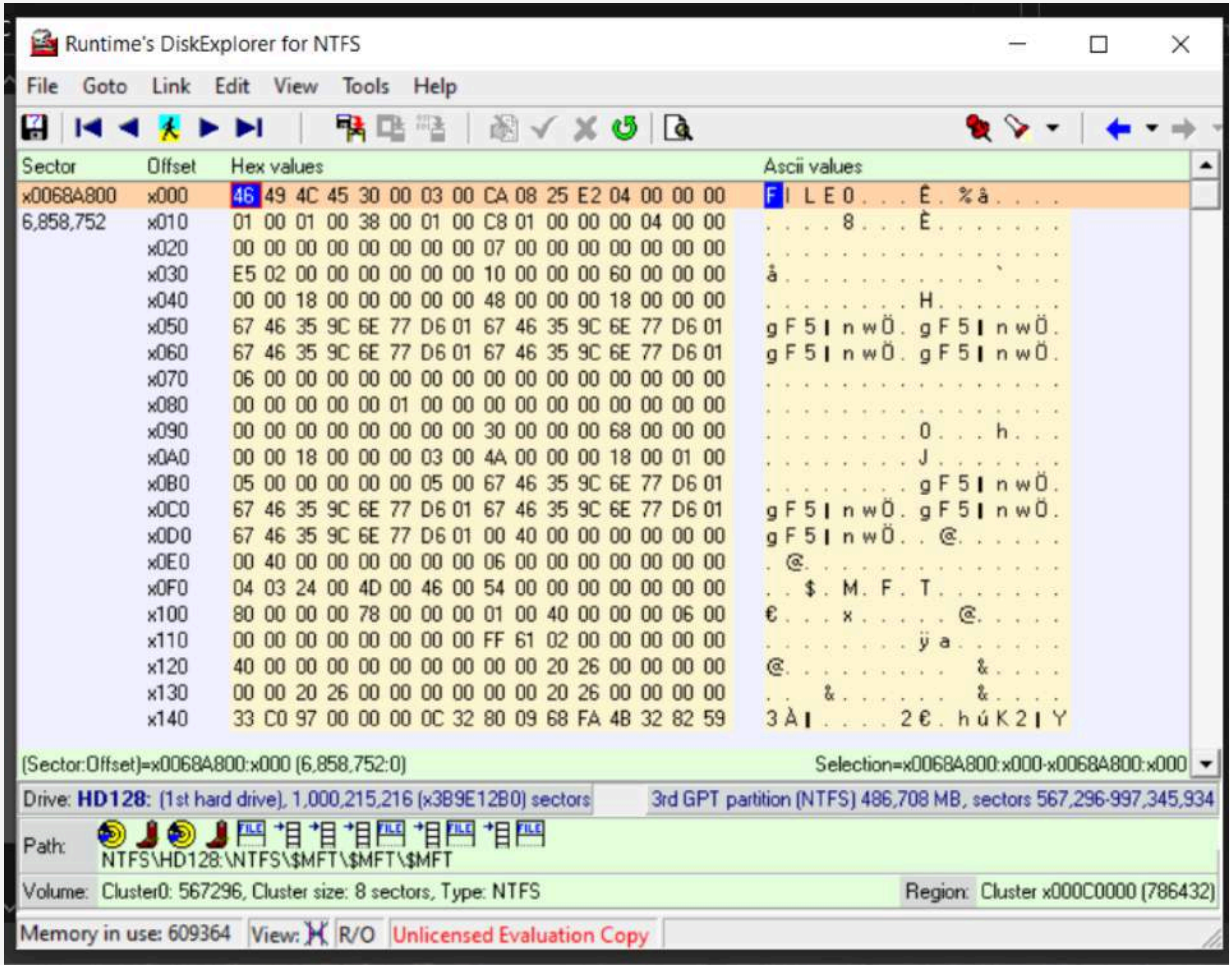




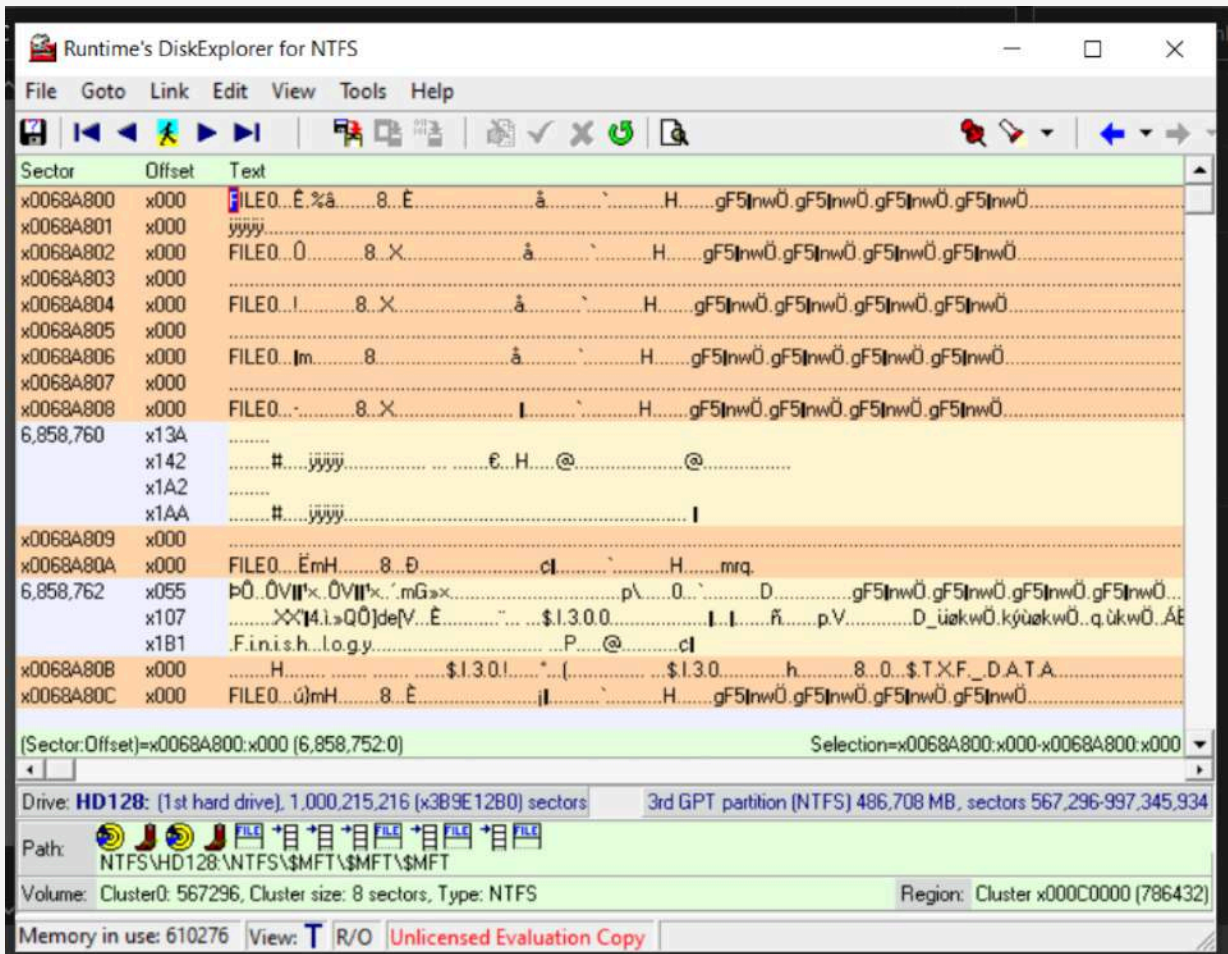
Inspect the file entry details, NT attributes etc.



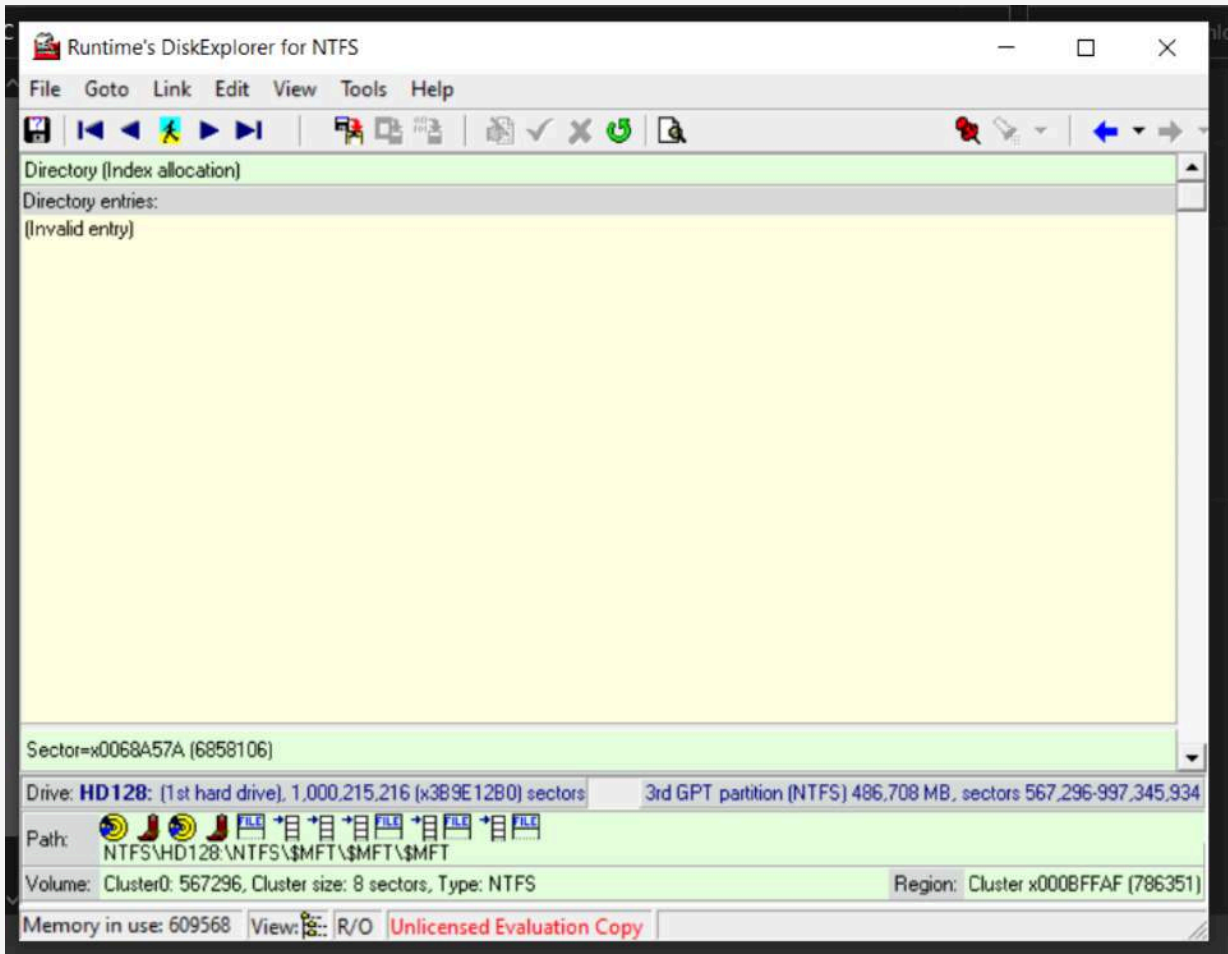
Hex



Text format view



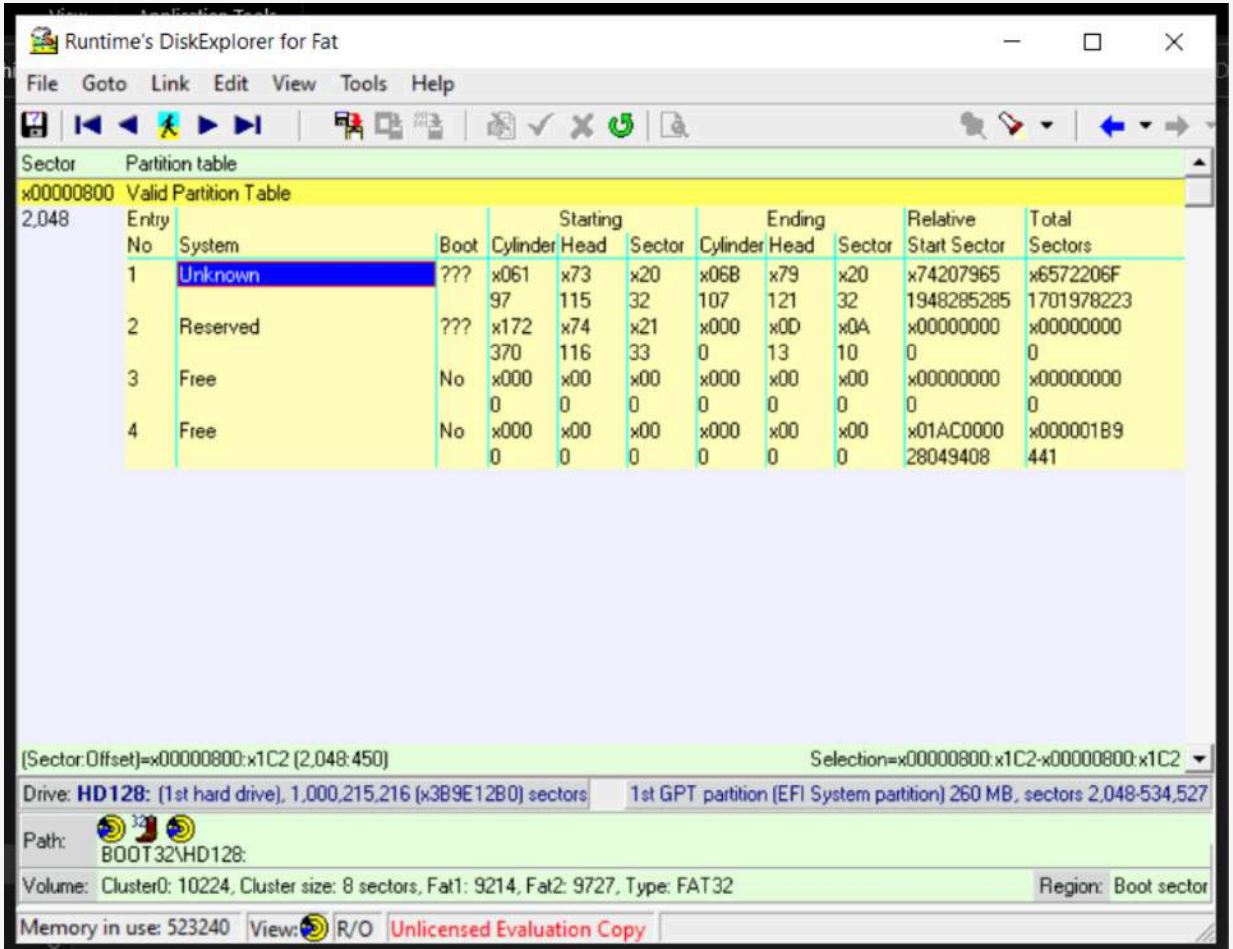
As index allocation



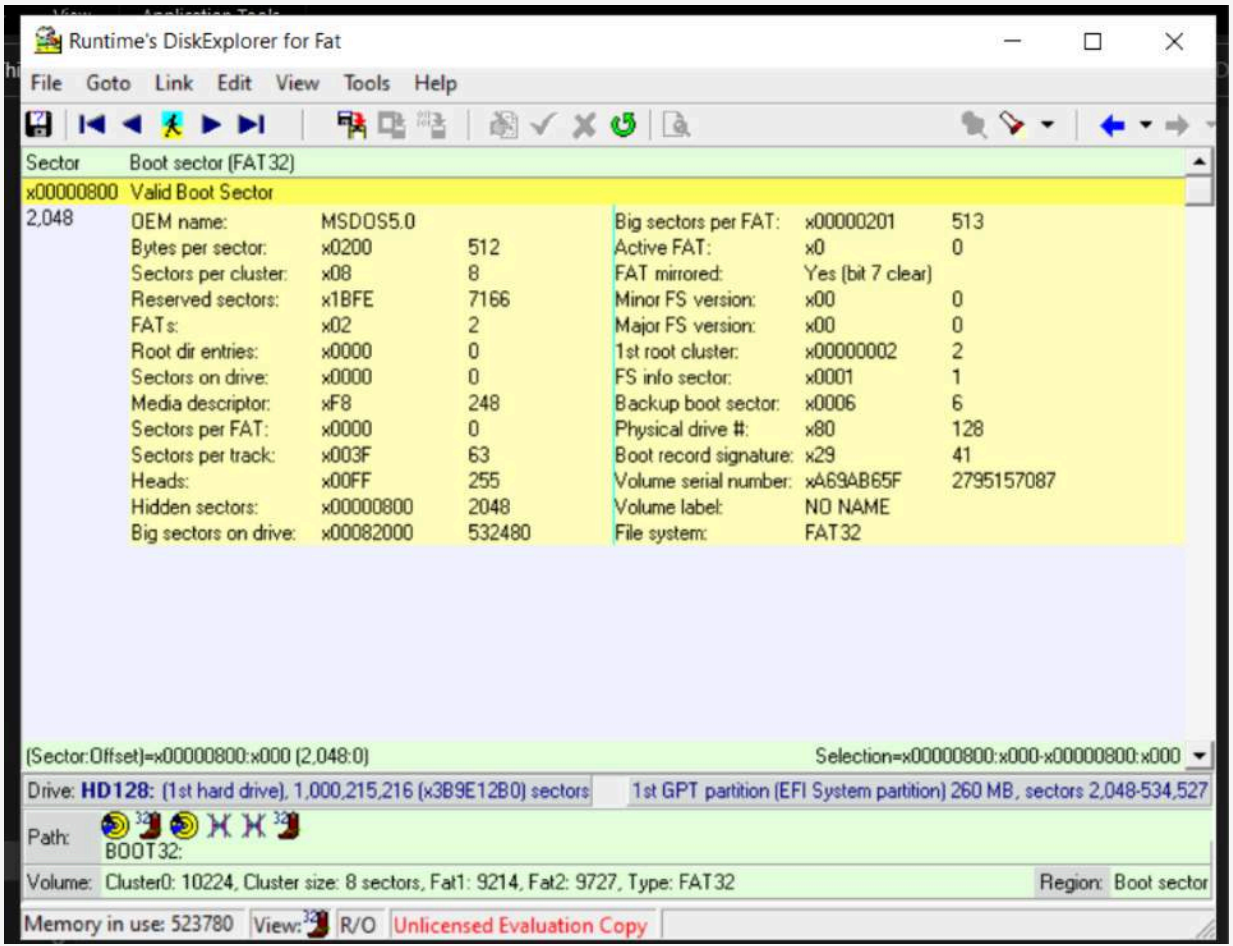


2) FAT

Partition table



Boot sector



Root directory

Runtime's DiskExplorer for Fat											
File Goto Link Edit View Tools Help											
Sector	Offset	Name	Ext	Status	Type	Attributes	Size	Date	Time	Cluster	Created
x00002800	x000	SYSTEM			DIR	_l_ 0		2020-08-20	19:53:18	x00000000	00
10,240	x020	Tools		deleted	LFN	Check Sum: xAB					
	x040	s00LS		deleted	DIR	_d_ 4096		2020-08-20	19:53:14	x00000003	2020-08-20 19
	x060	EFI			DIR	_d_ 0		2020-08-20	19:55:46	x00000009E	2020-08-20 19
	x080	Information		#2 last	LFN	Check Sum: x72					
	x0A0	System Volume		#1	LFN	Check Sum: x72					
	x0C0	SYSTEM*1			DIR	_d_sh_ 0		2020-08-20	20:02:44	x00001B26	2020-08-20 20
	x0E0			unused	FILE		0		00:00:00	x00000000	00
	x100			unused	FILE		0		00:00:00	x00000000	00
	x120			unused	FILE		0		00:00:00	x00000000	00
	x140			unused	FILE		0		00:00:00	x00000000	00
	x160			unused	FILE		0		00:00:00	x00000000	00
	x180			unused	FILE		0		00:00:00	x00000000	00
	x1A0			unused	FILE		0		00:00:00	x00000000	00
	x1C0			unused	FILE		0		00:00:00	x00000000	00
	x1E0			unused	FILE		0		00:00:00	x00000000	00
x00002801	x000			unused	FILE		0		00:00:00	x00000000	00
10,241	x020			unused	FILE		0		00:00:00	x00000000	00
	x040			unused	FILE		0		00:00:00	x00000000	00
	x060			unused	FILE		0		00:00:00	x00000000	00
(Sector:Offset)=x00002800:x000 (10,240:0) Selection=x00002800:x000-x00002800:x000											
Drive: HD128: (1st hard drive), 1,000,215,216 (x3B9E12B0) sectors 1st GPT partition (EFI System partition) 260 MB, sectors 2,048-534,527											
Path: BOOT32\BOOT32\ FAT FAT 32 32											
Volume: Cluster0: 10224, Cluster size: 8 sectors, Fat1: 9214, Fat2: 9727, Type: FAT32 Region: Cluster x00000002 (2)											
Memory in use: 525908 View: R/O Unlicensed Evaluation Copy											

FAT 1

Runtime's DiskExplorer for Fat											
File Goto Link Edit View Tools Help											
Sector	Offset	Fat32 values									
x000023FE	x000	FFFFFFFFB	FFFFFFFF	<eof>	00000004	00000005	00000006	00000007	00000008		
9,214	x020	00000009	0000000A	0000000B	0000000C	0000000D	0000000E	0000000F	00000010		
	x040	00000011	00000012	00000013	00000014	00000015	00000016	<eof>	00000018		
	x060	00000019	0000001A	0000001B	0000001C	0000001D	0000001E	0000001F	00000020		
	x080	00000021	00000022	00000023	00000024	00000025	00000026	00000027	00000028		
	x0A0	00000029	0000002A	<eof>	0000002C	0000002D	0000002E	0000002F	00000030		
	x0C0	00000031	00000032	00000033	00000034	00000035	00000036	00000037	00000038		
	x0E0	00000039	0000003A	0000003B	0000003C	0000003D	0000003E	<eof>	00000040		
	x100	00000041	00000042	00000043	00000044	00000045	00000046	00000047	00000048		
	x120	00000049	0000004A	0000004B	0000004C	0000004D	0000004E	0000004F	00000050		
	x140	00000051	00000052	<eof>	00000054	00000055	00000056	00000057	00000058		
	x160	00000059	0000005A	0000005B	0000005C	0000005D	0000005E	<eof>	00000060		
	x180	00000061	00000062	00000063	00000064	00000065	00000066	00000067	00000068		
	x1A0	00000069	0000006A	0000006B	0000006C	0000006D	0000006E	0000006F	00000070		
	x1C0	00000071	00000072	<eof>	00000074	00000075	00000076	00000077	00000078		
	x1E0	00000079	0000007A	0000007B	0000007C	0000007D	0000007E	0000007F	00000080		
x000023FF	x000	00000081	00000082	00000083	00000084	00000085	00000086	<eof>	00000088		
9,215	x020	00000089	0000008A	0000008B	0000008C	0000008D	0000008E	0000008F	00000090		
	x040	00000091	00000092	<eof>	<eof>	00000095	<eof>	00000097	00000098		
	x060	<eof>	00000000	00000000	00000000	00000000	00000000	<eof>	<eof>		
	x080	00000093	<eof>	000000A3	000000A4	000000A5	000000A6	000000A7	000000A8		
(Sector:Offset)=x000023FE:x000 (9,214:0) Selection=x000023FE:x000-x000023FE:x000											
Drive: HD128: (1st hard drive), 1,000,215,216 (x3B9E12B0) sectors 1st GPT partition (EFI System partition) 260 MB, sectors 2,048-534,527											
Path: BOOT32\BOOT32\ FAT FAT 32 32											
Volume: Cluster0: 10224, Cluster size: 8 sectors, Fat1: 9214, Fat2: 9727, Type: FAT32 Region: Fat1 x00000000 (0)											
Memory in use: 524084 View: FAT32 R/O Unlicensed Evaluation Copy											



### FAT 32

The screenshot displays the 'Runtime's DiskExplorer for Fat' application. The main window shows a list of sectors and their corresponding FAT32 values. The sectors are organized into two groups: 10,240 and 10,241. Each group contains 16 entries, each with an offset (x000 to x00F) and a series of 10 FAT32 values. The values are displayed in a grid format, with some cells highlighted in yellow. The application's status bar at the bottom provides additional information about the drive (HD128), the partition (1st GPT partition), the volume (Cluster0), and the memory in use (527652).

Sector	Offset	Fat32 values
10,240	x000	54535953 20204D45 08202020 00000000 00000000 9EA90000 00005114 00000000
	x020	6F0054E5 6C006F00 0F007300 0000A800 FFFFFFFF FFFFFFFF 0000FFFF FFFFFFFF
	x040	4C4F4FE5 20202053 10202020 9EA91C00 51145114 9EA70000 00035114 00001000
	x060	20494645 20202020 10202020 9EF63D00 51145114 9EF70000 009E5114 00000000
	x080	49002042 66006E00 0F006F00 00727200 0061006D 00690074 0000006F 0000006E
	x0A0	79005301 74007300 0F006500 006D7200 00560020 006C006F 00000075 0065006D
	x0C0	54535953 317E4D45 16202020 A0556900 51145114 A0560000 1B265114 00000000
	x0E0	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x100	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x120	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x140	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x160	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x180	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x1A0	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x1C0	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x1E0	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
10,241	x000	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x020	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x040	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x060	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
	x080	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Drive: **HD128:** (1st hard drive), 1,000,215,216 (x3B9E12B0) sectors | 1st GPT partition (EFI System partition) 260 MB, sectors 2,048-534,527

Path: **BOOT32\BOOT32:**

Volume: Cluster0: 10224, Cluster size: 8 sectors, Fat1: 9214, Fat2: 9727, Type: FAT32 | Region: Cluster x00000002 (2)

Memory in use: 527652 | View: **FAT32** | R/O | **Unlicensed Evaluation Copy**

New Notice - Olympia Sequel - Local Panchavat et

Runtime's DiskExplorer for Fat

File Goto Link Edit View Tools Help

Sector Offset Hex values Ascii values

x00002800 x000 53 59 53 54 45 4D 20 20 20 20 20 08 00 00 00 00 SYSTEM

10,240 x010 00 00 00 00 00 00 A9 9E 14 51 00 00 00 00 00 00 . . . . . Q . . . . .

x020 E5 54 00 6F 00 6F 00 6C 00 73 00 0F 00 A8 00 00 . . . . . T . . . . .

x030 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF . . . . .

x040 E5 4F 4F 4C 53 20 20 20 20 20 20 10 00 1C A9 9E . . . . .

x050 14 51 14 51 00 00 A7 9E 14 51 03 00 00 10 00 00 . . . . .

x060 45 46 49 20 20 20 20 20 20 20 20 10 00 3D F6 9E E F I . . . . .

x070 14 51 14 51 00 00 F7 9E 14 51 9E 00 00 00 00 00 . . . . .

x080 42 20 00 49 00 6E 00 66 00 6F 00 0F 00 72 72 00 B . . . . .

x090 6D 00 61 00 74 00 69 00 6F 00 00 00 6E 00 00 00 m . . . . .

x0A0 01 53 00 79 00 73 00 74 00 65 00 0F 00 72 6D 00 . . . . .

x0B0 20 00 56 00 6F 00 6C 00 75 00 00 00 6D 00 65 00 . . . . .

x0C0 53 59 53 54 45 4D 7E 31 20 20 20 16 00 69 55 A0 SYSTEM~1 . . . . .

x0D0 14 51 14 51 00 00 56 A0 14 51 26 18 00 00 00 00 . . . . .

x0E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .

x0F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .

x100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .

x110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .

x120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .

x130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .

x140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .

(Sector:Offset)=x00002800:x000 (10,240:0) Selection=x00002800:x000-x00002800:x000

Drive: HD128: (1st hard drive), 1,000,215,216 (x3B9E12B0) sectors 1st GPT partition (EFI System partition) 260 MB, sectors 2,048-534,527

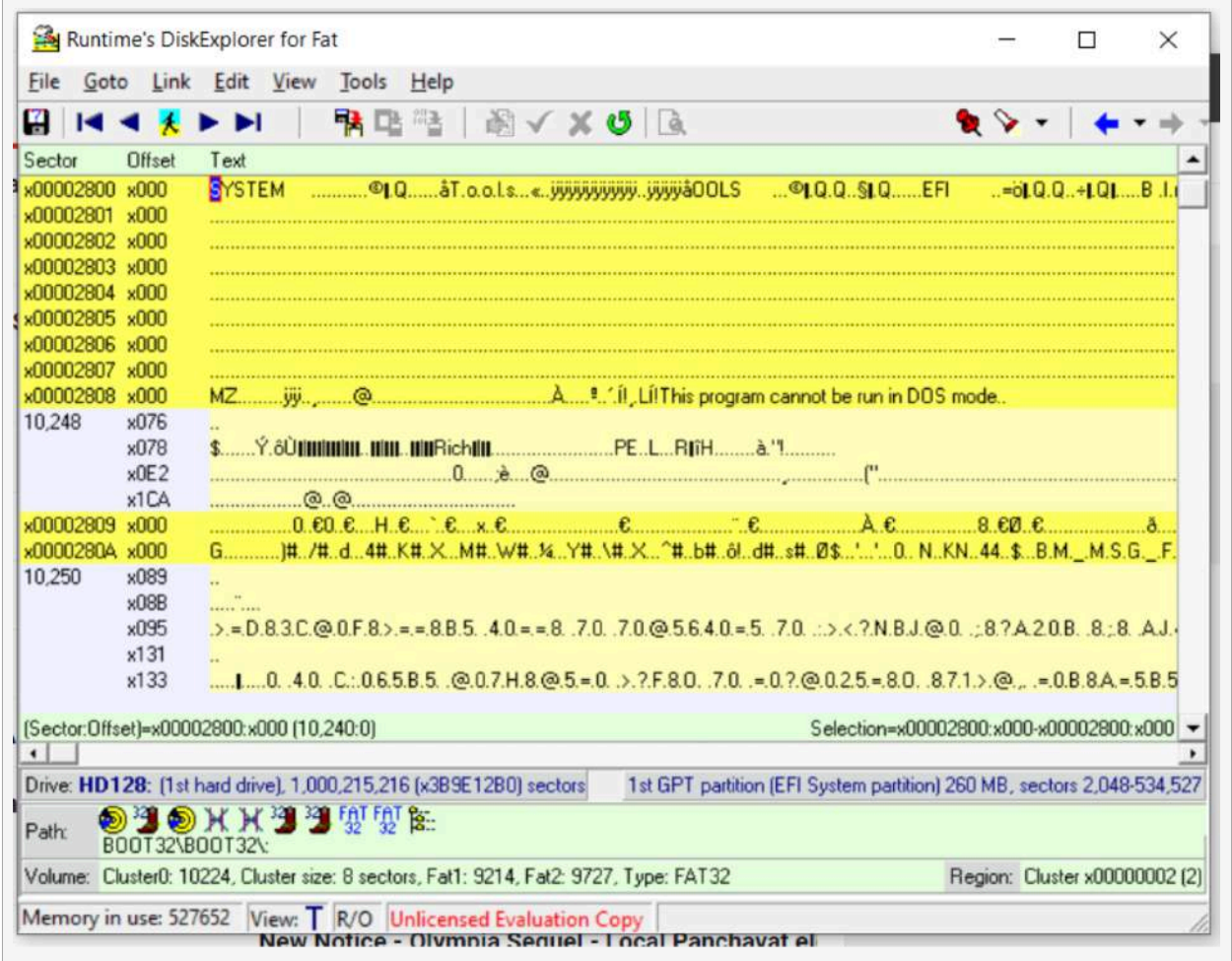
Path: BOOT32\BOOT32\

Volume: Cluster0: 10224, Cluster size: 8 sectors, Fat1: 9214, Fat2: 9727, Type: FAT32 Region: Cluster x00000002 (2)

Memory in use: 526916 View: R/O Unlicensed Evaluation Copy

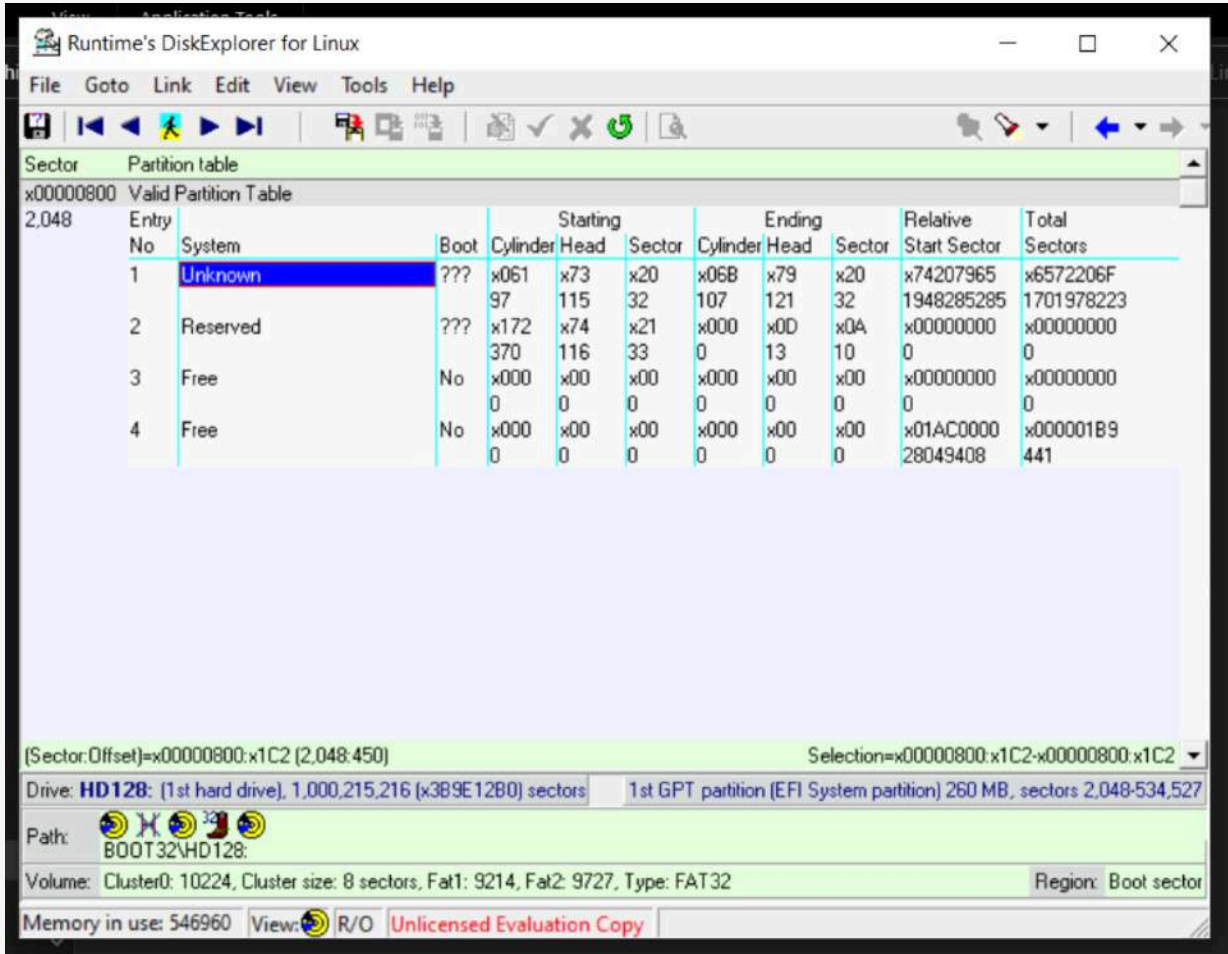


Text format view

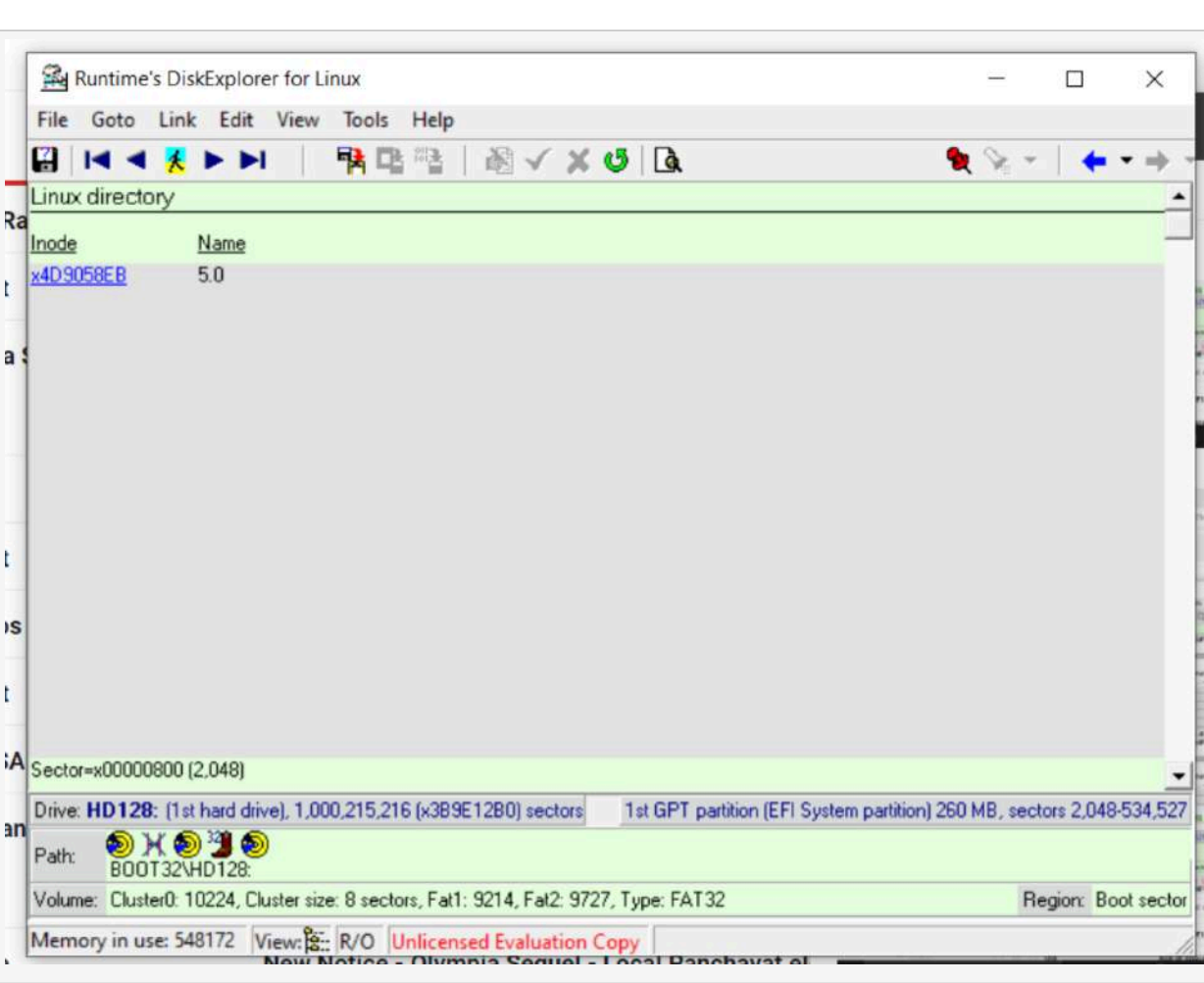


Linux

Partition table

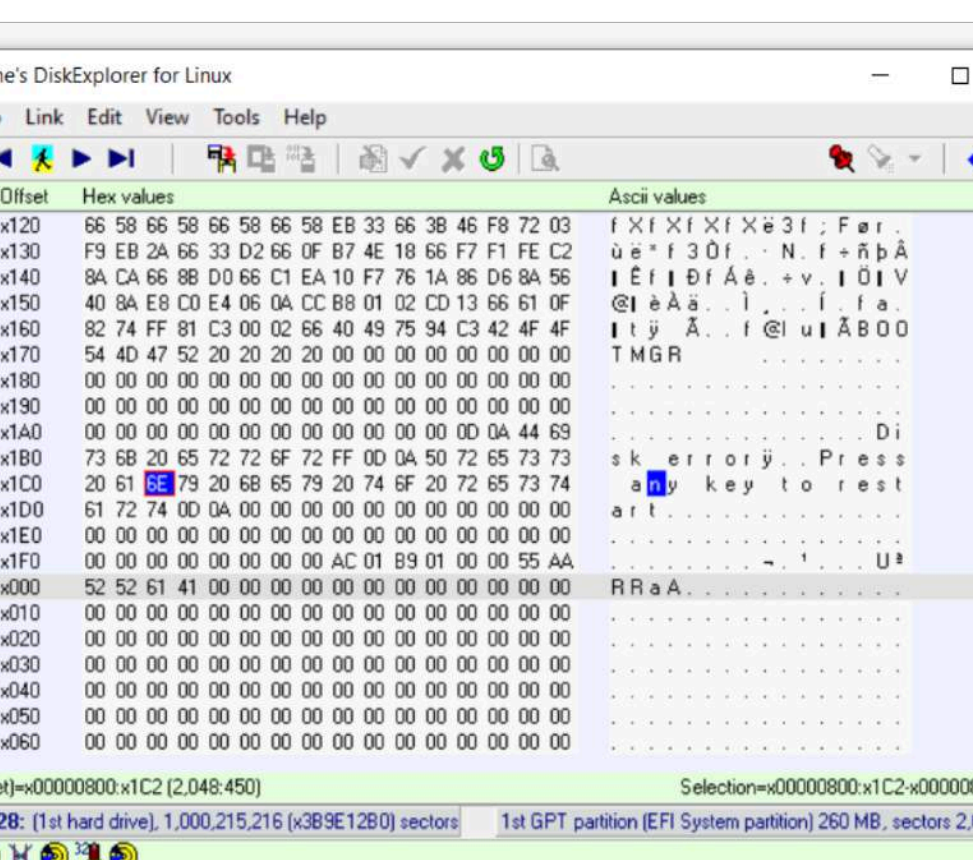


Root directory





# Hex



Runtime's DiskExplorer for Linux

File Goto Link Edit View Tools Help

Sector Offset Text

Sector	Offset	Text
2,048	x080	00000000
	x14C	00000000
	x157	00000000
	x1AE	00000000
	x1B8	00000000
	x1D5	00000000
x00000801	x000	RRaA.....
x00000802	x000	.....
x00000803	x000	.....
x00000804	x000	.....
x00000805	x000	.....
x00000806	x000	.....
2,054	x080	00000000
	x14C	00000000
	x157	00000000
	x1AE	00000000
	x1B8	00000000
	x1D5	00000000
x00000807	x000	RRaA.....
x00000808	x000	.....

(Sector:Offset)=x00000800:x1C2 (2,048:450) Selection=x00000800:x1C2-x00000800:x1C2

Drive: HD128: (1st hard drive), 1,000,215,216 (x389E12B0) sectors 1st GPT partition (EFI System partition) 260 MB, sectors 2,048-534,527

Path: BOOT32\HD128

Volume: Cluster0: 10224, Cluster size: 8 sectors, Fat1: 9214, Fat2: 9727, Type: FAT32 Region: Boot sector

Memory in use: 548004 View: T R/O Unlicensed Evaluation Copy

New Notice - Olivia Serial - Local Panchavat al