# FORENSICS
# LAB SERIES

# Lab 3: Introduction to Partitions (MBR & GPT)

| Material in this Lab Aligns to the Following Certification Domains/Objectives | | |
|---|---|---|
| GIAC Certified Forensics Examiner (GCFE) Domains | Certified Cyber Forensics Professional (CCFP) Objectives | Computer Hacking Forensic Investigator (CHFI) Objectives |
| 4. File and Program Activity Analysis | 4: Digital Forensics | 8: Windows Forensics |

**Document Version: 2016-08-17**

# Contents



## Introduction

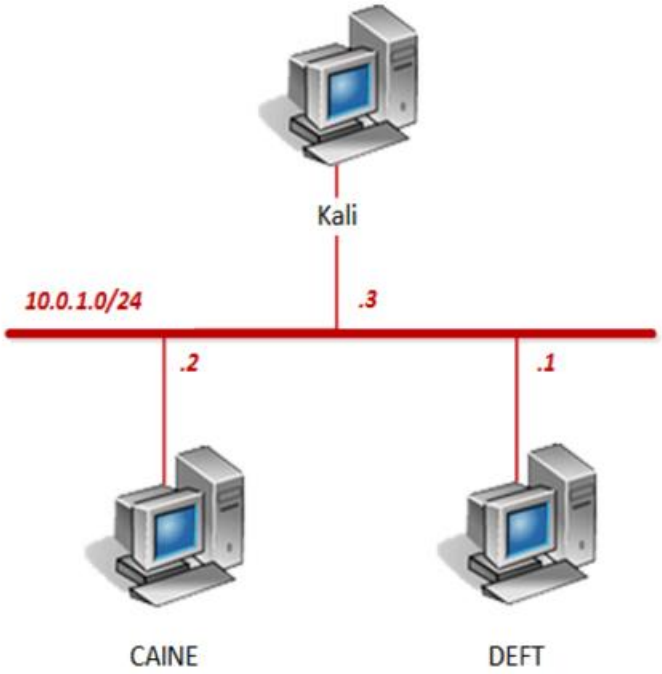
This lab focuses on exploring partitioning systems with a hex editor. This lab will help teach at a hex level how the operating system understands and interprets a Master Boot Record (MBR) versus GUID Partition Table (GPT) partitioning scheme.

## Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Exploring Linux Data Structure
2. Exploring the /dev/sda3 Partition
3. Exploring the /dev/sda2 Partition
4. Exploring the /dev/sda1 Partition
5. Exploring Windows Data Structure
6. Exploring the /dev/sdb1 Partition
7. Exploring the /dev/sdb2 Partition
8. Exploring GPT Partitions

## Pod Topology



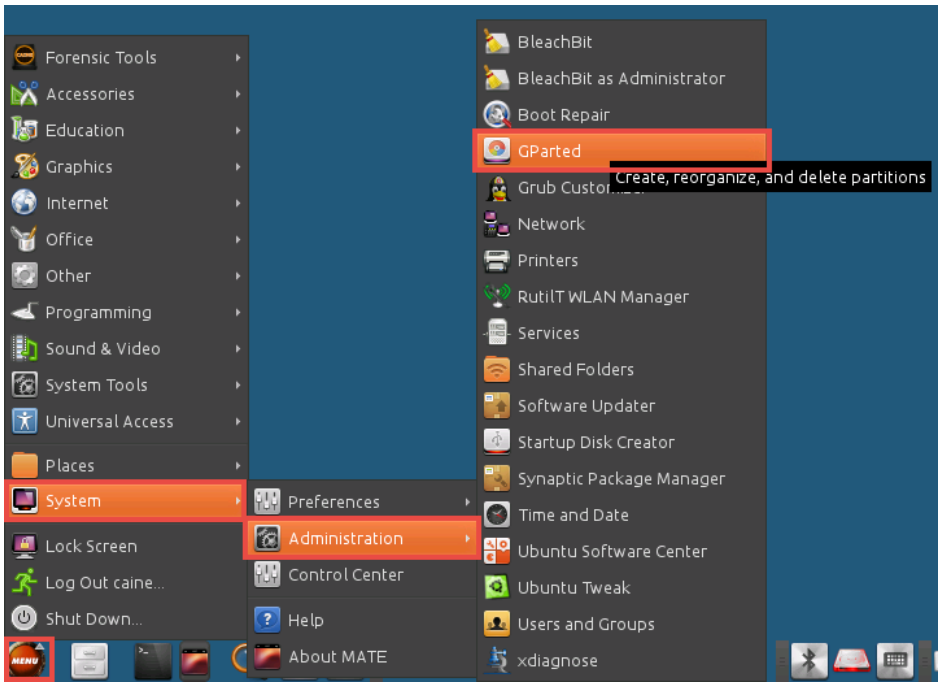
## Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

| Virtual Machine | IP Address | Account (if needed) | Password (if needed) |
|---|---|---|---|
| DEFT | 10.0.1.1 | deft | password |
| CAINE | 10.0.1.2 | caine | |
| Kali | 10.0.1.3 | root | toor |

# 1 Exploring Linux Data Structure

1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Open the *GParted* partition editor by navigating to **Menu > System > Administration > GParted**.

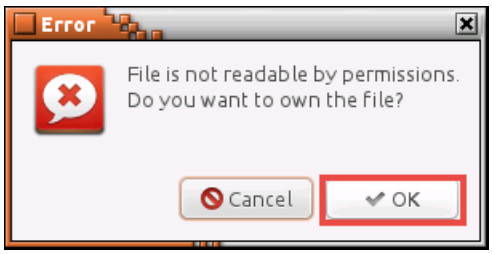



3. Once the *GParted* application window appears, minimize it and open a new terminal by clicking on the **MATE Terminal** icon from the bottom tool bar.


4. Using the terminal, enter the command below to open the **/dev/sda** disk with **wxHexEditor**.

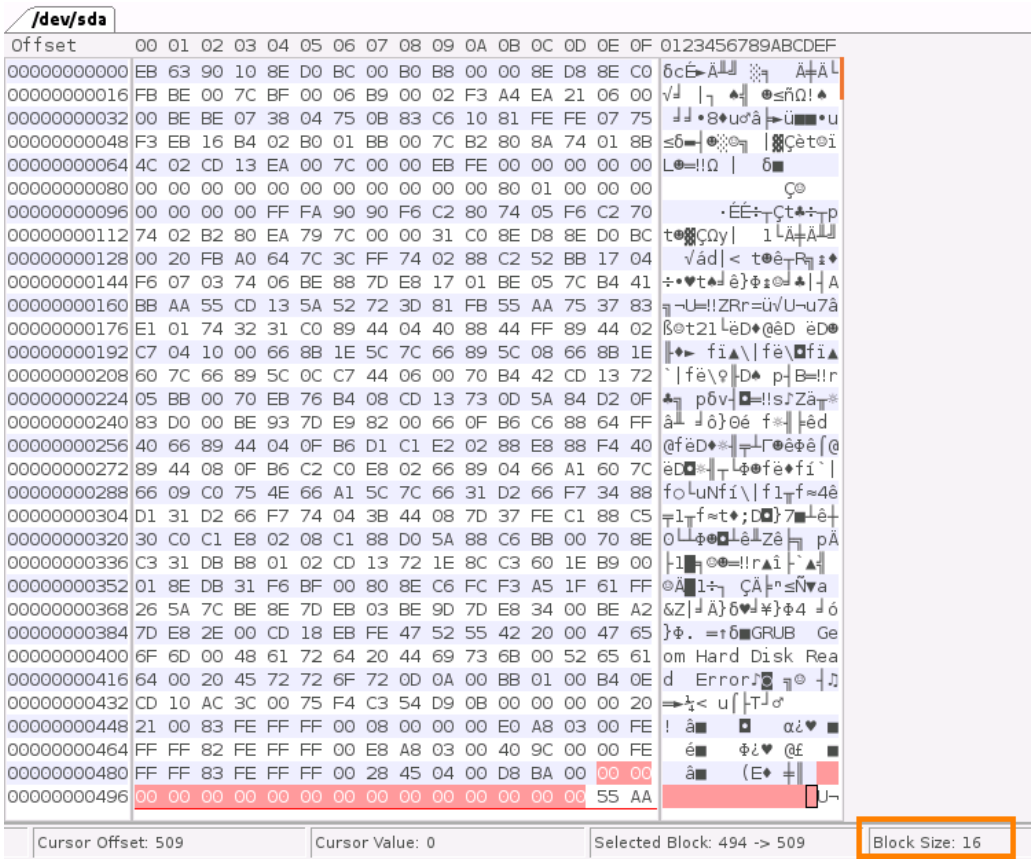
```
wxHexEditor /dev/sda
```

5. If presented with a permissions error message, click **OK** to continue.



6. Notice the hex of the boot sector appears for the 1st Linux drive, which is */dev/sda*. The boot sector ends with a signature of *55 AA*. This sda drive was setup as a PC DOS style layout with a *MBR*. Therefore, we can have up to 4 primary partitions max. Locate the 4th partition by counting back from "*55 AA*" by 16 bytes (16 bytes is the size of a partition table entry).

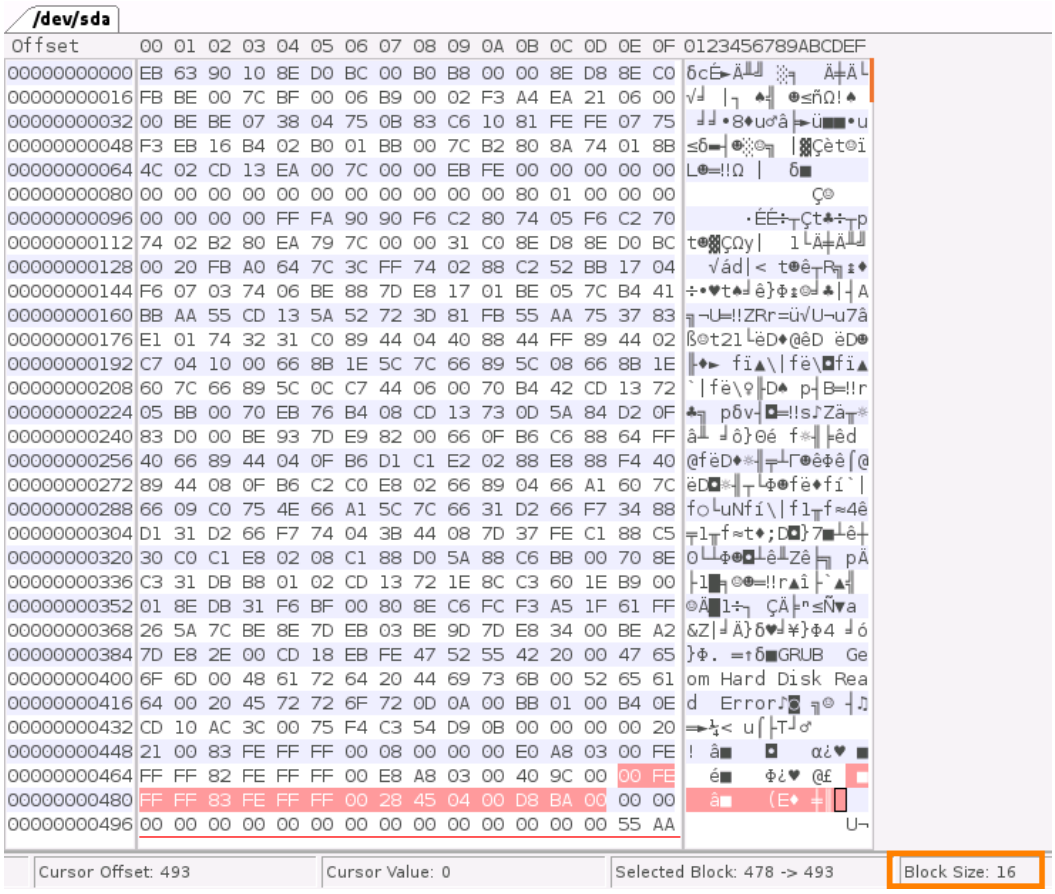



This is the 4th partition, which is empty.

## 2 Exploring the /dev/sda3 Partition

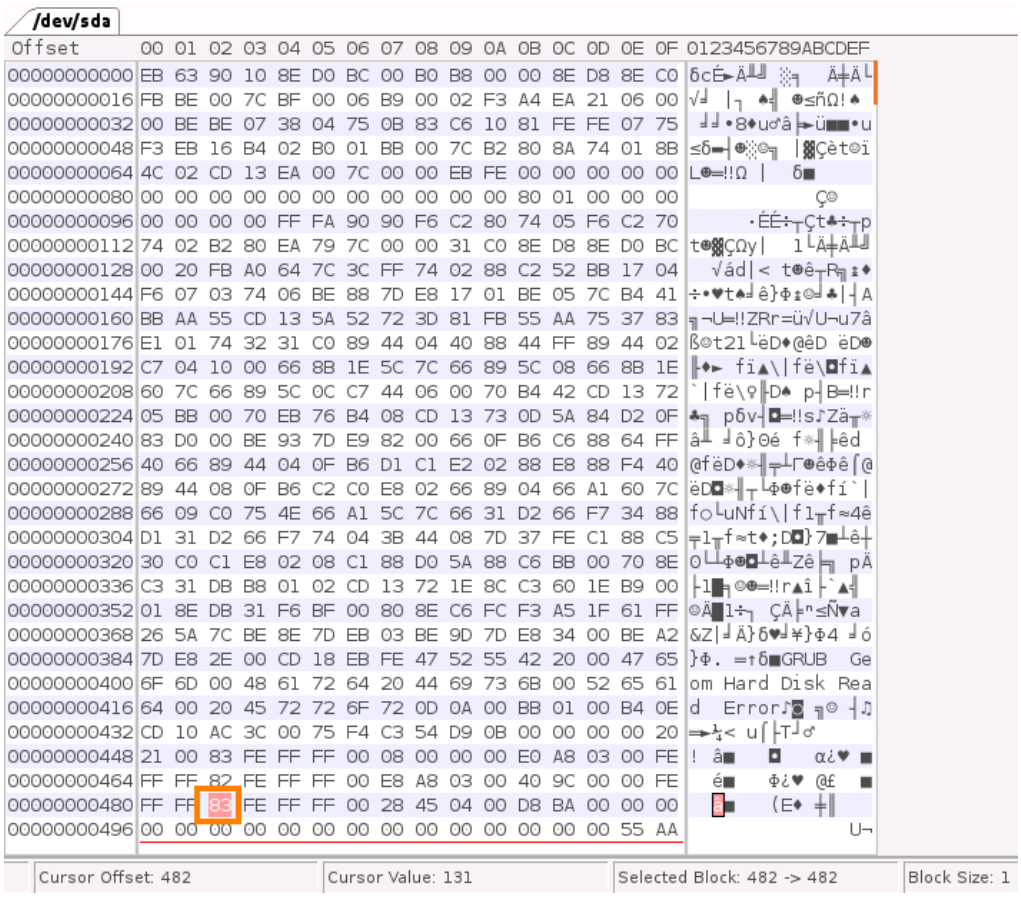
1. Count back another 16 bytes to locate the 3rd partition.




This is the 3rd partition, notice that it is populated.

2. Examine the 3rd partition. Count 4 bytes from the beginning of the partition and identify the partition ID type of **83**.



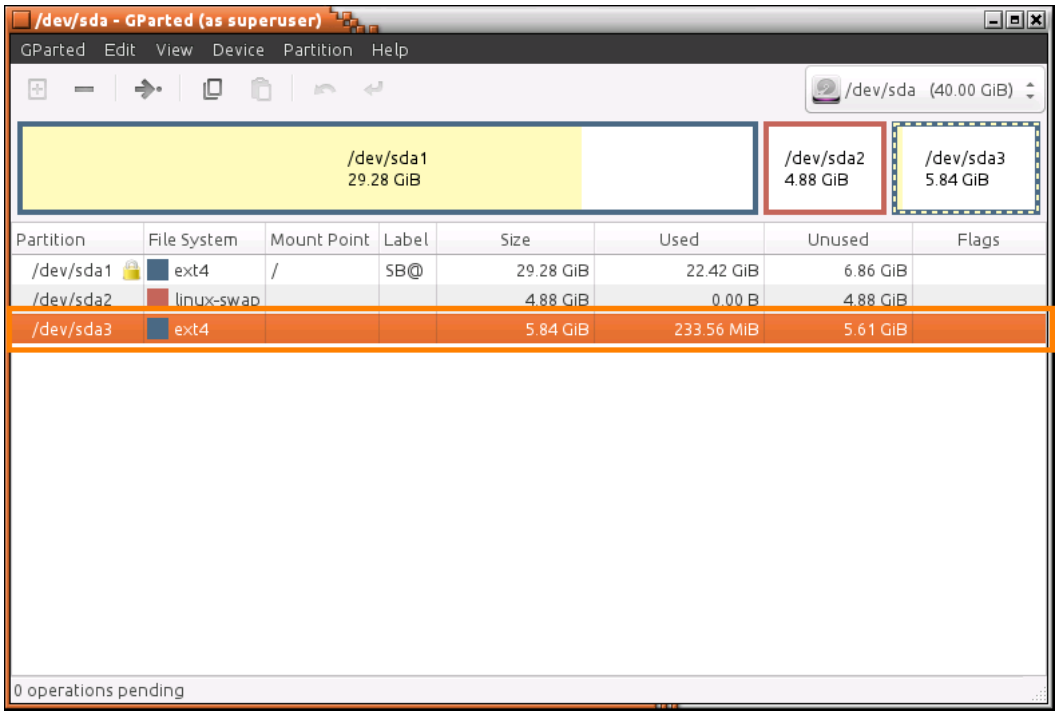
Reference the table below to identify partitions by ID. Notice *Type ID 83* is a Linux partition, therefore /dev/sda3 should be a Linux partition.

| Type ID | Partition system | Type ID | Partition system | Type ID | Partition system | Type ID | Partition system |
|---|---|---|---|---|---|---|---|
| 0x00 | Empty | 0x1e | Hidden W95 FAT1 | 0x80 | Old Minix | 0xbe | Solaris boot |
| 0x01 | FAT12 | 0x24 | NEC DOS | 0x81 | Minix/old Lin | 0xbf | Solaris |
| 0x02 | XENIX root | 0x39 | Plan 9 | 0x82 | Linux swap/ So | 0xc1 | DRDOS/sec |
| 0x03 | XENIX usr | 0x3c | PartitionMagic | 0x83 | Linux | 0xc4 | DRDOS/sec<32M |
| 0x04 | FAT16 <32M | 0x40 | Venix 80286 | 0x84 | OS/2hidden C: | 0xc6 | DRDOS/sec>32M |
| 0x05 | Extended | 0x41 | PPC PReP Boot | 0x85 | Linux extended | 0xc7 | Syrinx |
| 0x06 | FAT16 | 0x42 | SFS | 0x86 | NTFS volume set | 0xda | Non-FS data |
| 0x07 | HPFS/NTFS | 0x4d | QNX4.x | 0x87 | NTFS volume set | 0xdb | CP/M / CTOS |
| 0x08 | AIX | 0x4e | QNX4.x 2nd part | 0x88 | Linux plaintext | 0xde | Dell Utility |
| 0x09 | AIX bootable | 0x4f | QNX4.x 3rd part | 0x8e | Linux LVM | 0xdf | BootIt |
| 0x0a | OS/2 Boot | 0x50 | OnTrack DM | 0x93 | Amoeba | 0xe1 | DOS access |
| 0x0b | W95 FAT32 | 0x51 | OnTrack DM6 Aux | 0x94 | Amoeba BBT | 0xe3 | DOS R/O |
| 0x0c | W95 FAT32 (LBA) | 0x52 | CP/M | 0x9f | BSD/OS | 0xe4 | SpeedStor |
| 0x0e | W95 FAT16 (LBA) | 0x53 | OnTrack DM6 Aux | 0xa0 | IBM Thinkpad hi | 0xeb | BeOS fs |
| 0x0f | W95 Ext'd (LBA) | 0x54 | OnTrackDM6 | 0xa5 | FreeBSD | 0xee | EFI GPT |
| 0x10 | OPUS | 0x55 | EZ-Drive | 0xa6 | OpenBSD | 0xef | EFI (FAT-12/16/ |
| 0x11 | Hidden FAT12 | 0x56 | Golden Bow | 0xa7 | NeXTSTEP | 0xf0 | Linux/PA-RISC b |
| 0x12 | Compaq diagnost | 0x5c | Priam Edisk | 0xa8 | Darwin UFS | 0xf1 | SpeedStor |
| 0x14 | Hidden FAT16 <3 | 0x61 | SpeedStor | 0xa9 | NetBSD | 0xf2 | DOS secondary |

3. Change focus to the **GParted** window.

4. Using the GParted application, identify the third partition, **/dev/sda3**. Notice that the file system is setup as *ext4,* which is a Linux file system.




5. Identify the size of the partition using the **wxHexEditor** application.

6. Since the partition was created on an Intel machine, data is stored in reverse order or also called *Little Endian*. Bytes 12 to 15 read *00 D8 BA 00* in hex, which needs to be put into *Little Endian* order.

/dev/sda

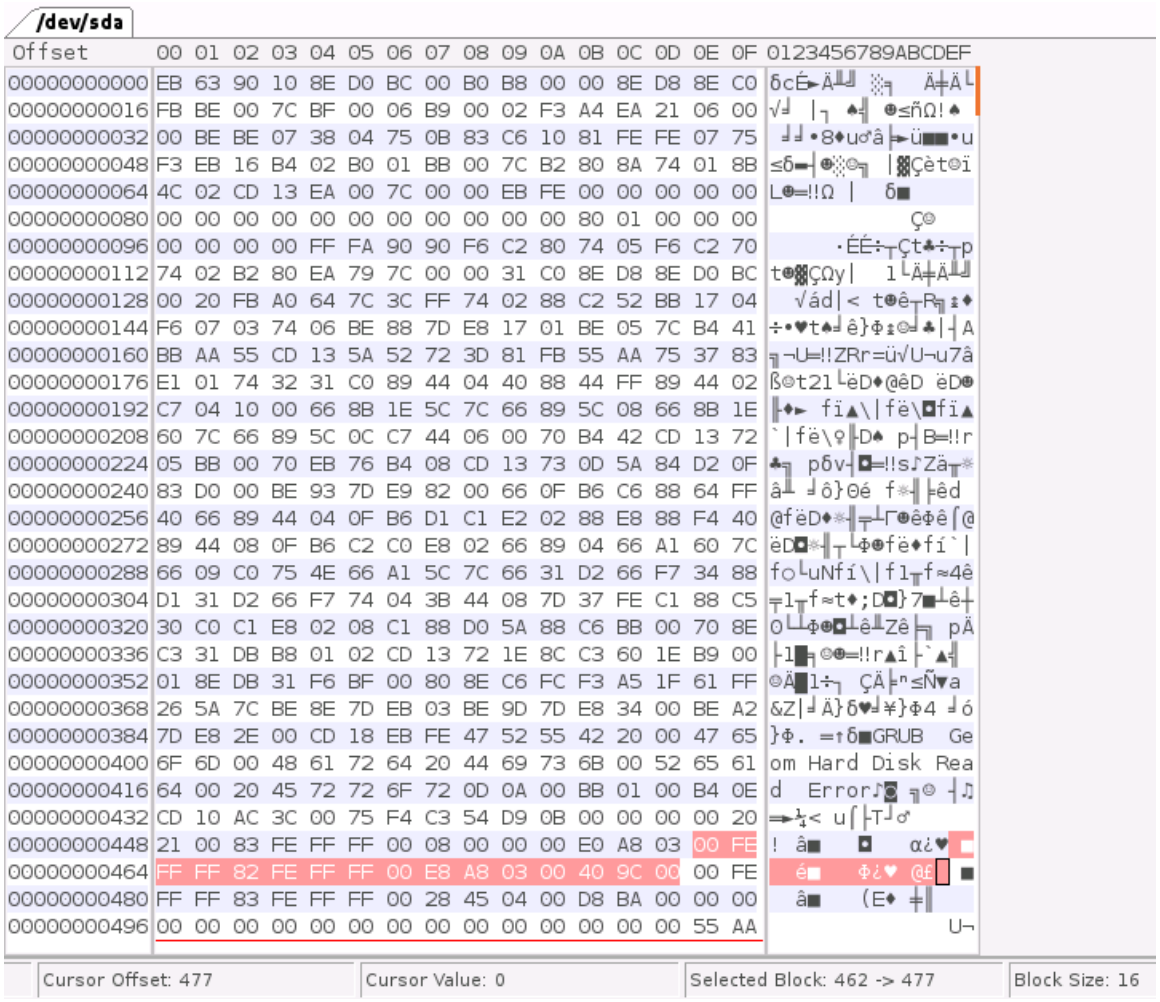
| Offset | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000000 | EB | 63 | 90 | 10 | 8E | D0 | BC | 00 | B0 | B8 | 00 | 00 | 8E | D8 | 8E | C0 | δcÉ►Ä╩╝ ▒┐ Ä╪Ä└ |
| 00000000016 | FB | BE | 00 | 7C | BF | 00 | 06 | B9 | 00 | 02 | F3 | A4 | EA | 21 | 06 | 00 | √╝ │┐ ♠╣ ☻≤ñΩ!♠ |
| 00000000032 | 00 | BE | BE | 07 | 38 | 04 | 75 | 0B | 83 | C6 | 10 | 81 | FE | FE | 07 | 75 | ╝╝•8♦u♂â╞►ü■■•u |
| 00000000048 | F3 | EB | 16 | B4 | 02 | B0 | 01 | BB | 00 | 7C | B2 | 80 | 8A | 74 | 01 | 8B | ≤δ▬┤☻▒☺┐ │▓Çèt☺ï |
| 00000000064 | 4C | 02 | CD | 13 | EA | 00 | 7C | 00 | 00 | EB | FE | 00 | 00 | 00 | 00 | 00 | L☻═!!Ω │ δ■ |
| 00000000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 80 | 01 | 00 | 00 | 00 | Ç☺ |
| 00000000096 | 00 | 00 | 00 | 00 | FF | FA | 90 | 90 | F6 | C2 | 80 | 74 | 05 | F6 | C2 | 70 | ·ÉÉ÷┬Çt♣÷┬p |
| 00000000112 | 74 | 02 | B2 | 80 | EA | 79 | 7C | 00 | 00 | 31 | C0 | 8E | D8 | 8E | D0 | BC | t☻▓ÇΩy\| 1└Ä╪Ä╨╝ |
| 00000000128 | 00 | 20 | FB | A0 | 64 | 7C | 3C | FF | 74 | 02 | 88 | C2 | 52 | BB | 17 | 04 | √ád\|< t☻ê┬R╗↨♦ |
| 00000000144 | F6 | 07 | 03 | 74 | 06 | BE | 88 | 7D | E8 | 17 | 01 | BE | 05 | 7C | B4 | 41 | ÷•♥t♣╛ê}Φ↨☺┘♣\|┤A |
| 00000000160 | BB | AA | 55 | CD | 13 | 5A | 52 | 72 | 3D | 81 | FB | 55 | AA | 75 | 37 | 83 | ╗¬U═!!ZRr=ü√U¬u7â |
| 00000000176 | E1 | 01 | 74 | 32 | 31 | C0 | 89 | 44 | 04 | 40 | 88 | 44 | FF | 89 | 44 | 02 | ß☺t21└ëD♦@êD ëD☻ |
| 00000000192 | C7 | 04 | 10 | 00 | 66 | 8B | 1E | 5C | 7C | 66 | 89 | 5C | 08 | 66 | 8B | 1E | ╟♦► fï▲\|fë\◘fï▲ |
| 00000000208 | 60 | 7C | 66 | 89 | 5C | 0C | C7 | 44 | 06 | 00 | 70 | B4 | 42 | CD | 13 | 72 | `\|fë\♀╟D♠ p┤B═!!r |
| 00000000224 | 05 | BB | 00 | 70 | EB | 76 | B4 | 08 | CD | 13 | 73 | 0D | 5A | 84 | D2 | 0F | ♣╗ pδv┤◘═!!s♪Zä╥* |
| 00000000240 | 83 | D0 | 00 | BE | 93 | 7D | E9 | 82 | 00 | 66 | 0F | B6 | C6 | 88 | 64 | FF | â╙ ╛ô}Θé f*╢╞êd |
| 00000000256 | 40 | 66 | 89 | 44 | 04 | 0F | B6 | D1 | C1 | E2 | 02 | 88 | E8 | 88 | F4 | 40 | @fëD♦*╢╤┴Γ☻êΦê⌠@ |
| 00000000272 | 89 | 44 | 08 | 0F | B6 | C2 | C0 | E8 | 02 | 66 | 89 | 04 | 66 | A1 | 60 | 7C | ëD◘*╢┬└Φ☻fë♦fí`\| |
| 00000000288 | 66 | 09 | C0 | 75 | 4E | 66 | A1 | 5C | 7C | 66 | 31 | D2 | 66 | F7 | 34 | 88 | fo└uNfí\|f1╥f≈4ê |
| 00000000304 | D1 | 31 | D2 | 66 | F7 | 74 | 04 | 3B | 44 | 08 | 7D | 37 | FE | C1 | 88 | C5 | ╤1╥f≈t♦;D◘}7■┴ê┼ |
| 00000000320 | 30 | C0 | C1 | E8 | 02 | 08 | C1 | 88 | D0 | 5A | 88 | C6 | BB | 00 | 70 | 8E | 0└┴Φ☻◘┴êZê╞╗ pÄ |
| 00000000336 | C3 | 31 | DB | B8 | 01 | 02 | CD | 13 | 72 | 1E | 8C | C3 | 60 | 1E | B9 | 00 | ├1█╕☺☻═!!r▲î├`▲╣ |
| 00000000352 | 01 | 8E | DB | 31 | F6 | BF | 00 | 80 | 8E | C6 | FC | F3 | A5 | 1F | 61 | FF | ☺Ä█1÷┐ ÇÄ╞ⁿ≤Ñ▼a |
| 00000000368 | 26 | 5A | 7C | BE | 8E | 7D | EB | 03 | BE | 9D | 7D | E8 | 34 | 00 | BE | A2 | &Z\|╛Ä}δ♥╛¥}Φ4 ╛ó |
| 00000000384 | 7D | E8 | 2E | 00 | CD | 18 | EB | FE | 47 | 52 | 55 | 42 | 20 | 00 | 47 | 65 | }Φ. =↑δ■GRUB Ge |
| 00000000400 | 6F | 6D | 00 | 48 | 61 | 72 | 64 | 20 | 44 | 69 | 73 | 6B | 00 | 52 | 65 | 61 | om Hard Disk Rea |
| 00000000416 | 64 | 00 | 20 | 45 | 72 | 72 | 6F | 72 | 0D | 0A | 00 | BB | 01 | 00 | B4 | 0E | d Error♪◙ ╗☺ ┤♫ |
| 00000000432 | CD | 10 | AC | 3C | 00 | 75 | F4 | C3 | 54 | D9 | 0B | 00 | 00 | 00 | 00 | 20 | ═►¼< u⌠├T┘♂ |
| 00000000448 | 21 | 00 | 83 | FE | FF | FF | 00 | 08 | 00 | 00 | 00 | E0 | A8 | 03 | 00 | FE | ! â■ ◘ α¿♥ ■ |
| 00000000464 | FF | FF | 82 | FE | FF | FF | 00 | E8 | A8 | 03 | 00 | 40 | 9C | 00 | 00 | FE | é■ Φ¿♥ @£ ■ |
| 00000000480 | FF | FF | 83 | FE | FF | FF | 00 | 28 | 45 | 04 | 00 | D8 | BA | 00 | 00 | 00 | â■ (E♦ ╪ |
| 00000000496 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 55 | AA | U¬ |

7. To find the number of sectors using the *Little Endian* order, take the Little Endian order *00 BA D8 00* and convert it to decimal. When converted, the output is **12,244,992** which is the number of sectors.
8. Convert the number of sectors to bytes; **12,244,992** X **512** bytes/sector = **6,269,435,904** bytes.
9. Convert the number of bytes to gigabytes; **6,269,435,904** bytes / **1,073,741,824** bytes (or $2^{30}$) = **5.838** GiB.
10. Change focus to the **GParted** application and notice that the manual computation resembles closely to the *5.84* GiB size output for */dev/sda3*.

## 3 Exploring the /dev/sda2 Partition

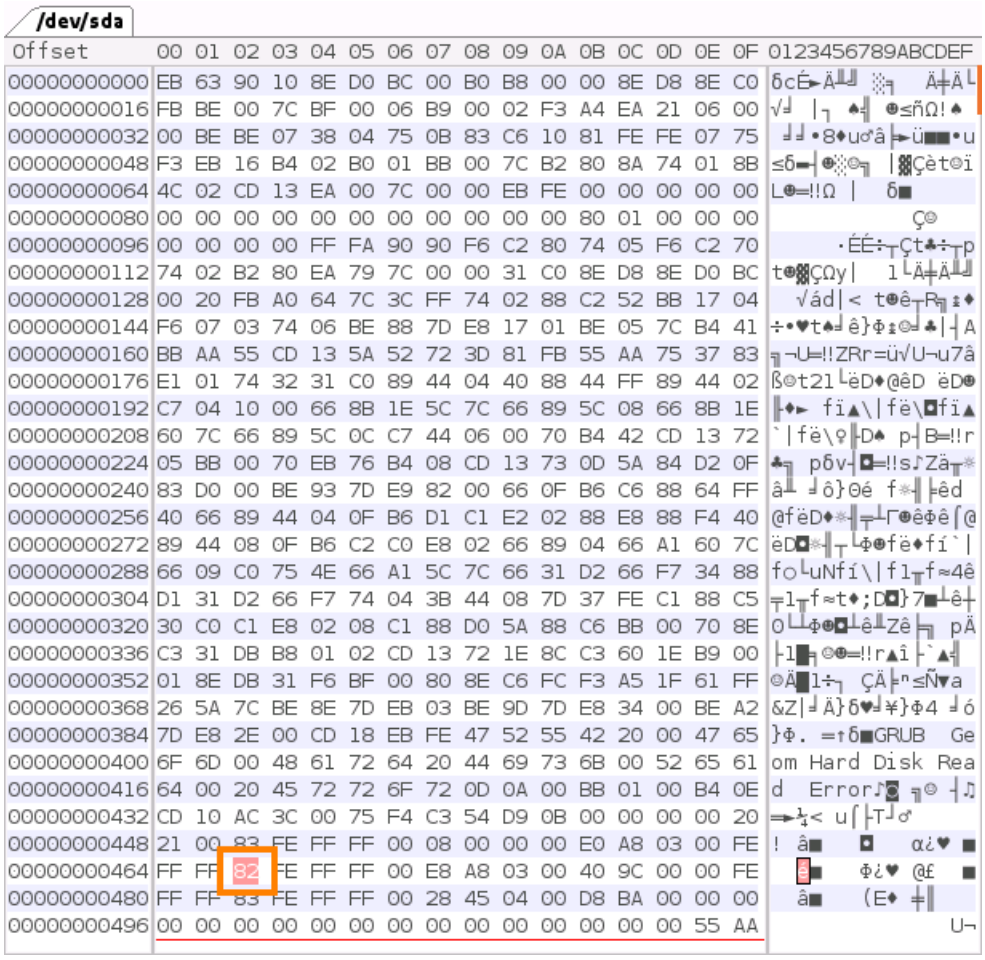
1. Change focus Identify to the **wxHedEditor** application and go another 16 bytes back.




This is the second partition, which is */dev/sda2*.

2. Count 4 bytes in and identify the partition *Type ID 82*. When referencing to the table on *page 10*, notice that this partition type is a Linux swap.

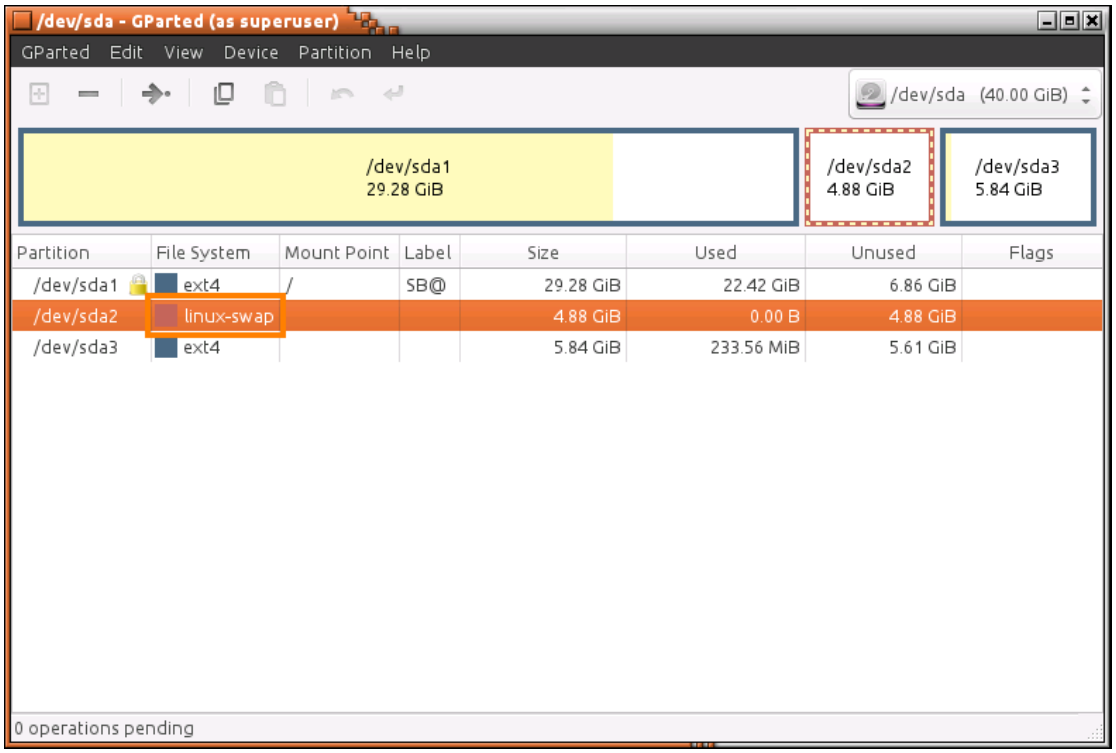


/dev/sda

| Offset | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000000 | EB | 63 | 90 | 10 | 8E | D0 | BC | 00 | B0 | B8 | 00 | 00 | 8E | D8 | 8E | C0 | δcÉ►Ä╩╝ ▒┐ Ä╪Ä└ |
| 00000000016 | FB | BE | 00 | 7C | BF | 00 | 06 | B9 | 00 | 02 | F3 | A4 | EA | 21 | 06 | 00 | √┘ \|┐ ♠╡ ☻≤ñΩ!♠ |
| 00000000032 | 00 | BE | BE | 07 | 38 | 04 | 75 | 0B | 83 | C6 | 10 | 81 | FE | FE | 07 | 75 | ┘┘•8♦u♂â╟►ü■■•u |
| 00000000048 | F3 | EB | 16 | B4 | 02 | B0 | 01 | BB | 00 | 7C | B2 | 80 | 8A | 74 | 01 | 8B | ≤δ▬┤☻▒◎┐ \|▓Çètº ï |
| 00000000064 | 4C | 02 | CD | 13 | EA | 00 | 7C | 00 | 00 | EB | FE | 00 | 00 | 00 | 00 | 00 | L☻═!!Ω \| δ■ |
| 00000000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 80 | 01 | 00 | 00 | 00 | Ç☺ |
| 00000000096 | 00 | 00 | 00 | 00 | FF | FA | 90 | 90 | F6 | C2 | 80 | 74 | 05 | F6 | C2 | 70 | ·ÉÉ÷┬Çt♣÷┬p |
| 00000000112 | 74 | 02 | B2 | 80 | EA | 79 | 7C | 00 | 00 | 31 | C0 | 8E | D8 | 8E | D0 | BC | t☻▒ÇΩy\| 1└Ä╪Ä╩╝ |
| 00000000128 | 00 | 20 | FB | A0 | 64 | 7C | 3C | FF | 74 | 02 | 88 | C2 | 52 | BB | 17 | 04 | √ád\|< t☻ê┬R╗↨♦ |
| 00000000144 | F6 | 07 | 03 | 74 | 06 | BE | 88 | 7D | E8 | 17 | 01 | BE | 05 | 7C | B4 | 41 | ÷•♥t♠┘ê}Φ↨☺┘♣\|┤A |
| 00000000160 | BB | AA | 55 | CD | 13 | 5A | 52 | 72 | 3D | 81 | FB | 55 | AA | 75 | 37 | 83 | ╗¬U═!!ZRr=ü√U¬u7â |
| 00000000176 | E1 | 01 | 74 | 32 | 31 | C0 | 89 | 44 | 04 | 40 | 88 | 44 | FF | 89 | 44 | 02 | ß☺t21└ëD♦@êD ëD☻ |
| 00000000192 | C7 | 04 | 10 | 00 | 66 | 8B | 1E | 5C | 7C | 66 | 89 | 5C | 08 | 66 | 8B | 1E | ╟♦► fï▲\|fë\◘fï▲ |
| 00000000208 | 60 | 7C | 66 | 89 | 5C | 0C | C7 | 44 | 06 | 00 | 70 | B4 | 42 | CD | 13 | 72 | `\|fë\♀╟D♠ p┤B═!!r |
| 00000000224 | 05 | BB | 00 | 70 | EB | 76 | B4 | 08 | CD | 13 | 73 | 0D | 5A | 84 | D2 | 0F | ♣╗ pδv┤◘═!!s♪Zä╥* |
| 00000000240 | 83 | D0 | 00 | BE | 93 | 7D | E9 | 82 | 00 | 66 | 0F | B6 | C6 | 88 | 64 | FF | â└ ┘ô}Θé f*╢╟êd |
| 00000000256 | 40 | 66 | 89 | 44 | 04 | 0F | B6 | D1 | C1 | E2 | 02 | 88 | E8 | 88 | F4 | 40 | @fëD♦*╢╤┴Γ☻êΦê⌠@ |
| 00000000272 | 89 | 44 | 08 | 0F | B6 | C2 | C0 | E8 | 02 | 66 | 89 | 04 | 66 | A1 | 60 | 7C | ëD◘*╢┬└Φ☻fë♦fí`\| |
| 00000000288 | 66 | 09 | C0 | 75 | 4E | 66 | A1 | 5C | 7C | 66 | 31 | D2 | 66 | F7 | 34 | 88 | f○└uNfí\|f1╥f≈4ê |
| 00000000304 | D1 | 31 | D2 | 66 | F7 | 74 | 04 | 3B | 44 | 08 | 7D | 37 | FE | C1 | 88 | C5 | ╤1╥f≈t♦;D◘}7■└ê┼ |
| 00000000320 | 30 | C0 | C1 | E8 | 02 | 08 | C1 | 88 | D0 | 5A | 88 | C6 | BB | 00 | 70 | 8E | 0└┴Φ☻◘└êZê╠╗ pÄ |
| 00000000336 | C3 | 31 | DB | B8 | 01 | 02 | CD | 13 | 72 | 1E | 8C | C3 | 60 | 1E | B9 | 00 | ├1█╕☺☻═!!r▲î├`▲╣ |
| 00000000352 | 01 | 8E | DB | 31 | F6 | BF | 00 | 80 | 8E | C6 | FC | F3 | A5 | 1F | 61 | FF | ☺Ä█1÷┐ ÇÄ╞ⁿ≤Ñ▼a |
| 00000000368 | 26 | 5A | 7C | BE | 8E | 7D | EB | 03 | BE | 9D | 7D | E8 | 34 | 00 | BE | A2 | &Z\|┘Ä}δ♥┘¥}Φ4 ┘ó |
| 00000000384 | 7D | E8 | 2E | 00 | CD | 18 | EB | FE | 47 | 52 | 55 | 42 | 20 | 00 | 47 | 65 | }Φ. ═↑δ■GRUB Ge |
| 00000000400 | 6F | 6D | 00 | 48 | 61 | 72 | 64 | 20 | 44 | 69 | 73 | 6B | 00 | 52 | 65 | 61 | om Hard Disk Rea |
| 00000000416 | 64 | 00 | 20 | 45 | 72 | 72 | 6F | 72 | 0D | 0A | 00 | BB | 01 | 00 | B4 | 0E | d Error♪◙ ╗☺ ┤♫ |
| 00000000432 | CD | 10 | AC | 3C | 00 | 75 | F4 | C3 | 54 | D9 | 0B | 00 | 00 | 00 | 00 | 20 | ═►¼< u⌠├T┘♂ |
| 00000000448 | 21 | 00 | 83 | FE | FF | FF | 00 | 08 | 00 | 00 | 00 | E0 | A8 | 03 | 00 | FE | ! â■ ◘ α¿♥ ■ |
| 00000000464 | FF | FF | 82 | FE | FF | FF | 00 | E8 | A8 | 03 | 00 | 40 | 9C | 00 | 00 | FE | ■ Φ¿♥ @£ ■ |
| 00000000480 | FF | FF | 83 | FE | FF | FF | 00 | 28 | 45 | 04 | 00 | D8 | BA | 00 | 00 | 00 | â■ (E♦ ╪ |
| 00000000496 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 55 | AA | U¬ |

3. Change focus to the **GParted** application and notice */dev/sda2* is listed as a *linux-swap* file system.



4. Change focus to the **wxHexEditor** application. Calculate the size of the partition. The bytes 12 to 15 read *00 40 9C 00* in hex, which needs to be put into *Little Endian* order.

/dev/sda

| Offset | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000000 | EB | 63 | 90 | 10 | 8E | D0 | BC | 00 | B0 | B8 | 00 | 00 | 8E | D8 | 8E | C0 | δcÉ►Ä╩╝ ▒┐ Ä╪Ä└ |
| 00000000016 | FB | BE | 00 | 7C | BF | 00 | 06 | B9 | 00 | 02 | F3 | A4 | EA | 21 | 06 | 00 | √╝ │┐ ♣╡ ☻≤ñΩ!♠ |
| 00000000032 | 00 | BE | BE | 07 | 38 | 04 | 75 | 0B | 83 | C6 | 10 | 81 | FE | FE | 07 | 75 | ╝╝•8♦u♂â╞►ü■■•u |
| 00000000048 | F3 | EB | 16 | B4 | 02 | B0 | 01 | BB | 00 | 7C | B2 | 80 | 8A | 74 | 01 | 8B | ≤δ▬┤☻▒☺┐ │▓Çèt☺ï |
| 00000000064 | 4C | 02 | CD | 13 | EA | 00 | 7C | 00 | 00 | EB | FE | 00 | 00 | 00 | 00 | 00 | L☻═!!Ω │ δ■ |
| 00000000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 80 | 01 | 00 | 00 | 00 | Ç☺ |
| 00000000096 | 00 | 00 | 00 | 00 | FF | FA | 90 | 90 | F6 | C2 | 80 | 74 | 05 | F6 | C2 | 70 | ·ÉÉ÷┬Çt♣÷┬p |
| 00000000112 | 74 | 02 | B2 | 80 | EA | 79 | 7C | 00 | 00 | 31 | C0 | 8E | D8 | 8E | D0 | BC | t☻▒ÇΩy\| 1└Ä╪Ä╩╝ |
| 00000000128 | 00 | 20 | FB | A0 | 64 | 7C | 3C | FF | 74 | 02 | 88 | C2 | 52 | BB | 17 | 04 | √ád\|< t☻ê┬R╗↨♦ |
| 00000000144 | F6 | 07 | 03 | 74 | 06 | BE | 88 | 7D | E8 | 17 | 01 | BE | 05 | 7C | B4 | 41 | ÷•♥t♣╝ê}Φ↨☺╝♣\|┤A |
| 00000000160 | BB | AA | 55 | CD | 13 | 5A | 52 | 72 | 3D | 81 | FB | 55 | AA | 75 | 37 | 83 | ╗¬U═!!ZRr=ü√U¬u7â |
| 00000000176 | E1 | 01 | 74 | 32 | 31 | C0 | 89 | 44 | 04 | 40 | 88 | 44 | FF | 89 | 44 | 02 | ß☺t21└ëD♦@êD ëD☻ |
| 00000000192 | C7 | 04 | 10 | 00 | 66 | 8B | 1E | 5C | 7C | 66 | 89 | 5C | 08 | 66 | 8B | 1E | ╟♦► fï▲\|fë\◘fï▲ |
| 00000000208 | 60 | 7C | 66 | 89 | 5C | 0C | C7 | 44 | 06 | 00 | 70 | B4 | 42 | CD | 13 | 72 | `\|fë\♀╟D♠ p┤B═!!r |
| 00000000224 | 05 | BB | 00 | 70 | EB | 76 | B4 | 08 | CD | 13 | 73 | 0D | 5A | 84 | D2 | 0F | ♣╗ pδv┤◘═!!s♪Zä╥* |
| 00000000240 | 83 | D0 | 00 | BE | 93 | 7D | E9 | 82 | 00 | 66 | 0F | B6 | C6 | 88 | 64 | FF | â╩ ╛ô}Θé f*╢╞êd |
| 00000000256 | 40 | 66 | 89 | 44 | 04 | 0F | B6 | D1 | C1 | E2 | 02 | 88 | E8 | 88 | F4 | 40 | @fëD♦*╢╤┴Γ☻êΦê⌠@ |
| 00000000272 | 89 | 44 | 08 | 0F | B6 | C2 | C0 | E8 | 02 | 66 | 89 | 04 | 66 | A1 | 60 | 7C | ëD◘*╢┬└Φ☻fë♦fí`\| |
| 00000000288 | 66 | 09 | C0 | 75 | 4E | 66 | A1 | 5C | 7C | 66 | 31 | D2 | 66 | F7 | 34 | 88 | f○└uNfí\|f1╥f≈4ê |
| 00000000304 | D1 | 31 | D2 | 66 | F7 | 74 | 04 | 3B | 44 | 08 | 7D | 37 | FE | C1 | 88 | C5 | ╤1╥f≈t♦;D◘}7■┴ê┼ |
| 00000000320 | 30 | C0 | C1 | E8 | 02 | 08 | C1 | 88 | D0 | 5A | 88 | C6 | BB | 00 | 70 | 8E | 0└┴Φ☻◘┴êΔZê╣ pÄ |
| 00000000336 | C3 | 31 | DB | B8 | 01 | 02 | CD | 13 | 72 | 1E | 8C | C3 | 60 | 1E | B9 | 00 | ├1█╕ ☺☻═!!r▲î├`▲╣ |
| 00000000352 | 01 | 8E | DB | 31 | F6 | BF | 00 | 80 | 8E | C6 | FC | F3 | A5 | 1F | 61 | FF | ☺Ä█1÷┐ ÇÄ╞ⁿ≤Ñ▼a |
| 00000000368 | 26 | 5A | 7C | BE | 8E | 7D | EB | 03 | BE | 9D | 7D | E8 | 34 | 00 | BE | A2 | &Z\|╛Ä}δ♥╝¥}Φ4 ╛ó |
| 00000000384 | 7D | E8 | 2E | 00 | CD | 18 | EB | FE | 47 | 52 | 55 | 42 | 20 | 00 | 47 | 65 | }Φ. =↑δ■GRUB Ge |
| 00000000400 | 6F | 6D | 00 | 48 | 61 | 72 | 64 | 20 | 44 | 69 | 73 | 6B | 00 | 52 | 65 | 61 | om Hard Disk Rea |
| 00000000416 | 64 | 00 | 20 | 45 | 72 | 72 | 6F | 72 | 0D | 0A | 00 | BB | 01 | 00 | B4 | 0E | d Error♪◙ ╗☺ ┤♫ |
| 00000000432 | CD | 10 | AC | 3C | 00 | 75 | F4 | C3 | 54 | D9 | 0B | 00 | 00 | 00 | 00 | 20 | ═►¼< u⌠├T┘♂ |
| 00000000448 | 21 | 00 | 83 | FE | FF | FF | 00 | 08 | 00 | 00 | 00 | E0 | A8 | 03 | 00 | FE | ! â■ ◘ α¿♥ ■ |
| 00000000464 | FF | FF | 82 | FE | FF | FF | 00 | E8 | A8 | 03 | 00 | 40 | 9C | 00 | 00 | FE | é■ Φ¿♥ @£ ■ |
| 00000000480 | FF | FF | 83 | FE | FF | FF | 00 | 28 | 45 | 04 | 00 | D8 | BA | 00 | 00 | 00 | â■ (E♦ ╪╢ |
| 00000000496 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 55 | AA | U¬ |

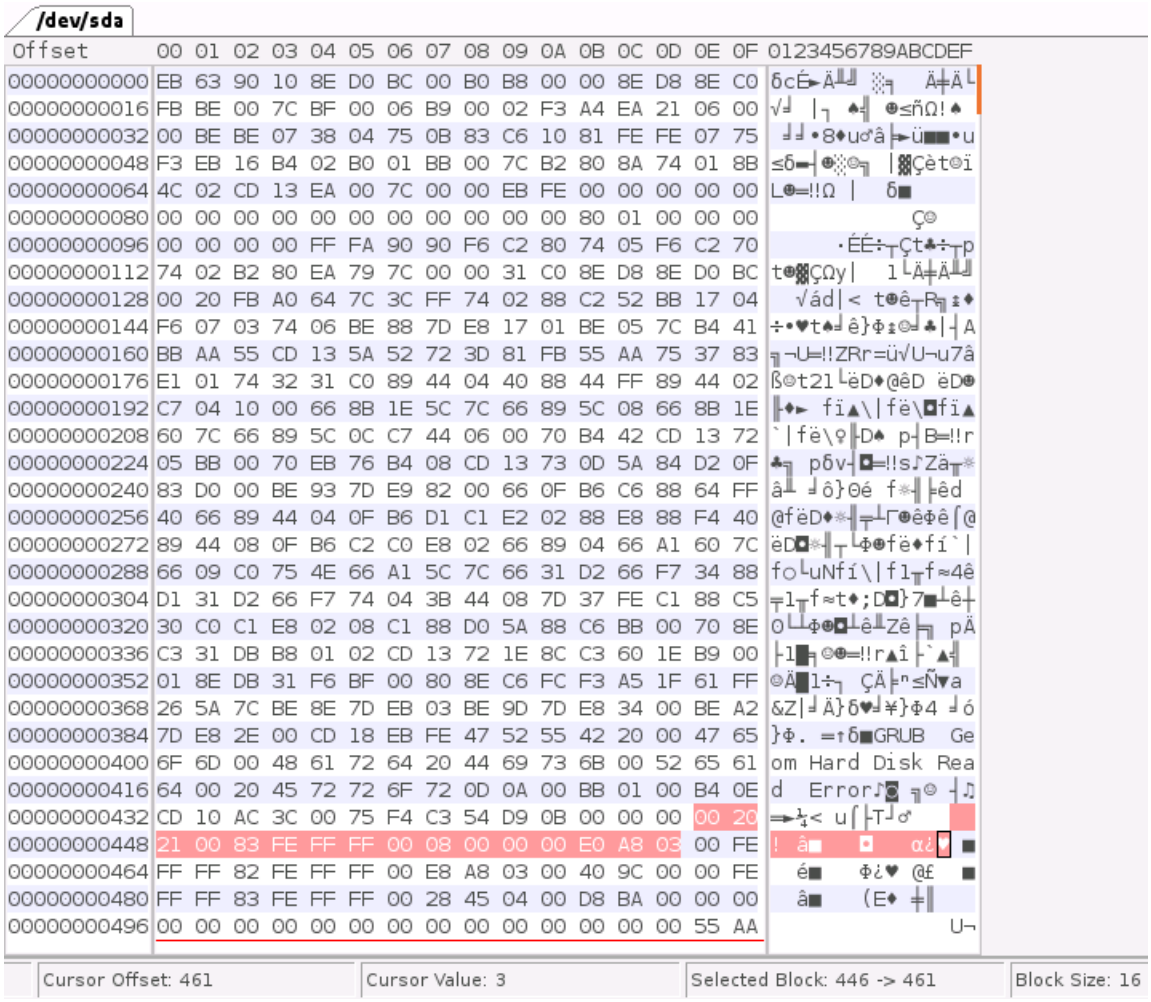
5. To find the number of sectors using the *Little Endian* order, take the Little Endian order *00 9C 40 00* and convert it to decimal. When converted, the output is **10,240,000,** which is the number of sectors.
6. Convert the number of sectors to bytes; **10,240,000** X **512** bytes/sector = **5,242,880,000** bytes.
7. Convert the number of bytes to gigabytes; **5,242,880,000** bytes / **1,073,741,824** bytes (or $2^{30}$) = **4.882** GiB.
8. Change focus to the **GParted** application and notice that the manual computation resembles closely to the *4.88* GiB size output for */dev/sda2*.


9. Change focus to the **wxHexEditor** application.

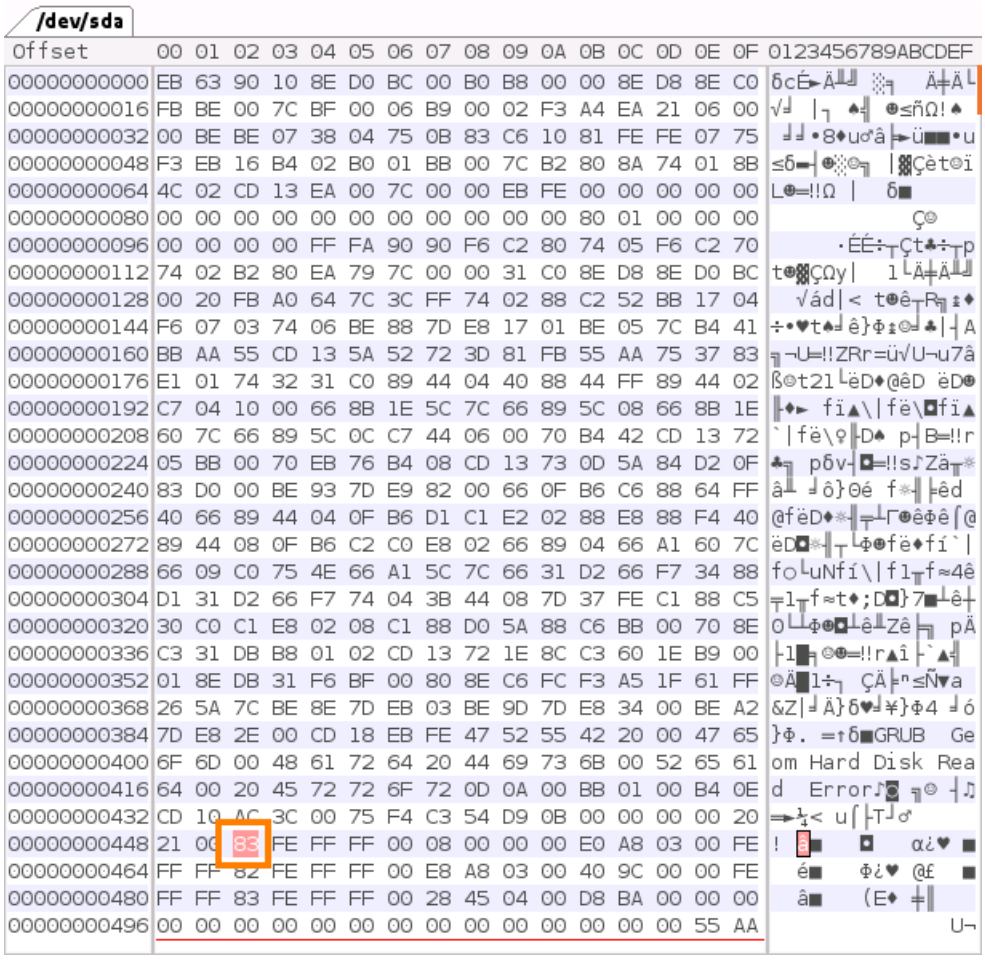
## 4 Exploring the /dev/sda1 Partition

1. Identify the first partition **/dev/sda1** by moving back 16 bytes from the last position.



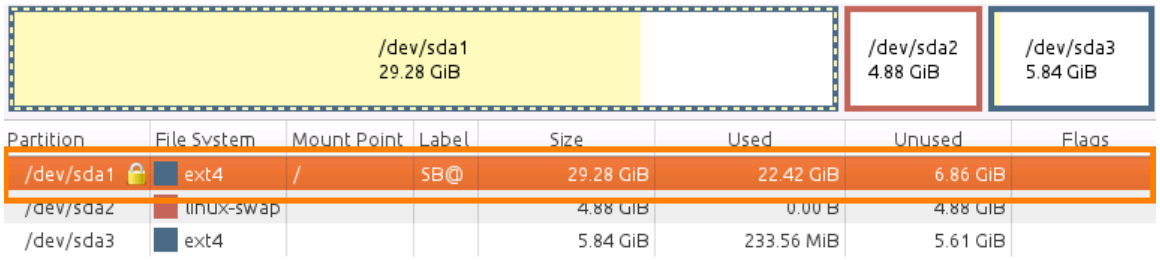
2. Notice the partition *Type ID* is *83*, which is a Linux ext4 file system when referencing back to the *Type ID* table.



/dev/sda

| Offset | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000000 | EB | 63 | 90 | 10 | 8E | D0 | BC | 00 | B0 | B8 | 00 | 00 | 8E | D8 | 8E | C0 | δcÉ►Ä╩╝ ▒╕ Ä╪Ä└ |
| 00000000016 | FB | BE | 00 | 7C | BF | 00 | 06 | B9 | 00 | 02 | F3 | A4 | EA | 21 | 06 | 00 | √╝ \|┐ ♠╡ ☻≤ñΩ!♠ |
| 00000000032 | 00 | BE | BE | 07 | 38 | 04 | 75 | 0B | 83 | C6 | 10 | 81 | FE | FE | 07 | 75 | ╜╜•8♦u♂â╞►ü■■•u |
| 00000000048 | F3 | EB | 16 | B4 | 02 | B0 | 01 | BB | 00 | 7C | B2 | 80 | 8A | 74 | 01 | 8B | ≤δ▬┤☻▒☺╕ \|▓Çèt☺ï |
| 00000000064 | 4C | 02 | CD | 13 | EA | 00 | 7C | 00 | 00 | EB | FE | 00 | 00 | 00 | 00 | 00 | L☻═!!Ω \| δ■ |
| 00000000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 80 | 01 | 00 | 00 | 00 | Ç☺ |
| 00000000096 | 00 | 00 | 00 | 00 | FF | FA | 90 | 90 | F6 | C2 | 80 | 74 | 05 | F6 | C2 | 70 | ·ÉÉ÷┬Çt♣÷┬p |
| 00000000112 | 74 | 02 | B2 | 80 | EA | 79 | 7C | 00 | 00 | 31 | C0 | 8E | D8 | 8E | D0 | BC | t☻▓ÇΩy\| 1└Ä╪Ä╩╝ |
| 00000000128 | 00 | 20 | FB | A0 | 64 | 7C | 3C | FF | 74 | 02 | 88 | C2 | 52 | BB | 17 | 04 | √ád\|< t☻ê┬R╗↨♦ |
| 00000000144 | F6 | 07 | 03 | 74 | 06 | BE | 88 | 7D | E8 | 17 | 01 | BE | 05 | 7C | B4 | 41 | ÷•♥t♣╜ê}Φ↨☺╜♣\|┤A |
| 00000000160 | BB | AA | 55 | CD | 13 | 5A | 52 | 72 | 3D | 81 | FB | 55 | AA | 75 | 37 | 83 | ╗¬U═!!ZRr=ü√U¬u7â |
| 00000000176 | E1 | 01 | 74 | 32 | 31 | C0 | 89 | 44 | 04 | 40 | 88 | 44 | FF | 89 | 44 | 02 | ß☺t21└ëD♦@êD ëD☻ |
| 00000000192 | C7 | 04 | 10 | 00 | 66 | 8B | 1E | 5C | 7C | 66 | 89 | 5C | 08 | 66 | 8B | 1E | ╟♦► fï▲\|fë\◘fï▲ |
| 00000000208 | 60 | 7C | 66 | 89 | 5C | 0C | C7 | 44 | 06 | 00 | 70 | B4 | 42 | CD | 13 | 72 | `\|fë\♀╟D♠ p┤B═!!r |
| 00000000224 | 05 | BB | 00 | 70 | EB | 76 | B4 | 08 | CD | 13 | 73 | 0D | 5A | 84 | D2 | 0F | ♣╗ pδv┤◘═!!s♪Zä╥* |
| 00000000240 | 83 | D0 | 00 | BE | 93 | 7D | E9 | 82 | 00 | 66 | 0F | B6 | C6 | 88 | 64 | FF | â╙ ╛ô}Θé f*╢ ╠êd |
| 00000000256 | 40 | 66 | 89 | 44 | 04 | 0F | B6 | D1 | C1 | E2 | 02 | 88 | E8 | 88 | F4 | 40 | @fëD♦*╢═╙Γ☻êΦê⌠@ |
| 00000000272 | 89 | 44 | 08 | 0F | B6 | C2 | C0 | E8 | 02 | 66 | 89 | 04 | 66 | A1 | 60 | 7C | ëD◘*╢┬└Φ☻fë♦fí`\| |
| 00000000288 | 66 | 09 | C0 | 75 | 4E | 66 | A1 | 5C | 7C | 66 | 31 | D2 | 66 | F7 | 34 | 88 | fo└uNfí\|f1╥f≈4ê |
| 00000000304 | D1 | 31 | D2 | 66 | F7 | 74 | 04 | 3B | 44 | 08 | 7D | 37 | FE | C1 | 88 | C5 | ═1╥f≈t♦;D◘}7■┴êâ |
| 00000000320 | 30 | C0 | C1 | E8 | 02 | 08 | C1 | 88 | D0 | 5A | 88 | C6 | BB | 00 | 70 | 8E | 0└┴Φ☻◘┴êZê╠╗ pÄ |
| 00000000336 | C3 | 31 | DB | B8 | 01 | 02 | CD | 13 | 72 | 1E | 8C | C3 | 60 | 1E | B9 | 00 | ├1█╕☺☻═!!r▲î├`▲╣ |
| 00000000352 | 01 | 8E | DB | 31 | F6 | BF | 00 | 80 | 8E | C6 | FC | F3 | A5 | 1F | 61 | FF | ☺Ä█1÷┐ ÇÄ╞ⁿ≤Ñ▼a |
| 00000000368 | 26 | 5A | 7C | BE | 8E | 7D | EB | 03 | BE | 9D | 7D | E8 | 34 | 00 | BE | A2 | &Z\|╜Ä}δ♥╜¥}Φ4 ╜ó |
| 00000000384 | 7D | E8 | 2E | 00 | CD | 18 | EB | FE | 47 | 52 | 55 | 42 | 20 | 00 | 47 | 65 | }Φ. ═↑δ■GRUB Ge |
| 00000000400 | 6F | 6D | 00 | 48 | 61 | 72 | 64 | 20 | 44 | 69 | 73 | 6B | 00 | 52 | 65 | 61 | om Hard Disk Rea |
| 00000000416 | 64 | 00 | 20 | 45 | 72 | 72 | 6F | 72 | 0D | 0A | 00 | BB | 01 | 00 | B4 | 0E | d Error♪◙ ╗☺ ┤♫ |
| 00000000432 | CD | 10 | AC | 3C | 00 | 75 | F4 | C3 | 54 | D9 | 0B | 00 | 00 | 00 | 00 | 20 | ═►¼< u⌠├T┘♂ |
| 00000000448 | 21 | 00 | 83 | FE | FF | FF | 00 | 08 | 00 | 00 | 00 | E0 | A8 | 03 | 00 | FE | ! â■ ◘ α¿♥ ■ |
| 00000000464 | FF | FF | 82 | FE | FF | FF | 00 | E8 | A8 | 03 | 00 | 40 | 9C | 00 | 00 | FE | é■ Φ¿♥ @£ ■ |
| 00000000480 | FF | FF | 83 | FE | FF | FF | 00 | 28 | 45 | 04 | 00 | D8 | BA | 00 | 00 | 00 | â■ (E♦ ╪\| |
| 00000000496 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 55 | AA | U¬ |

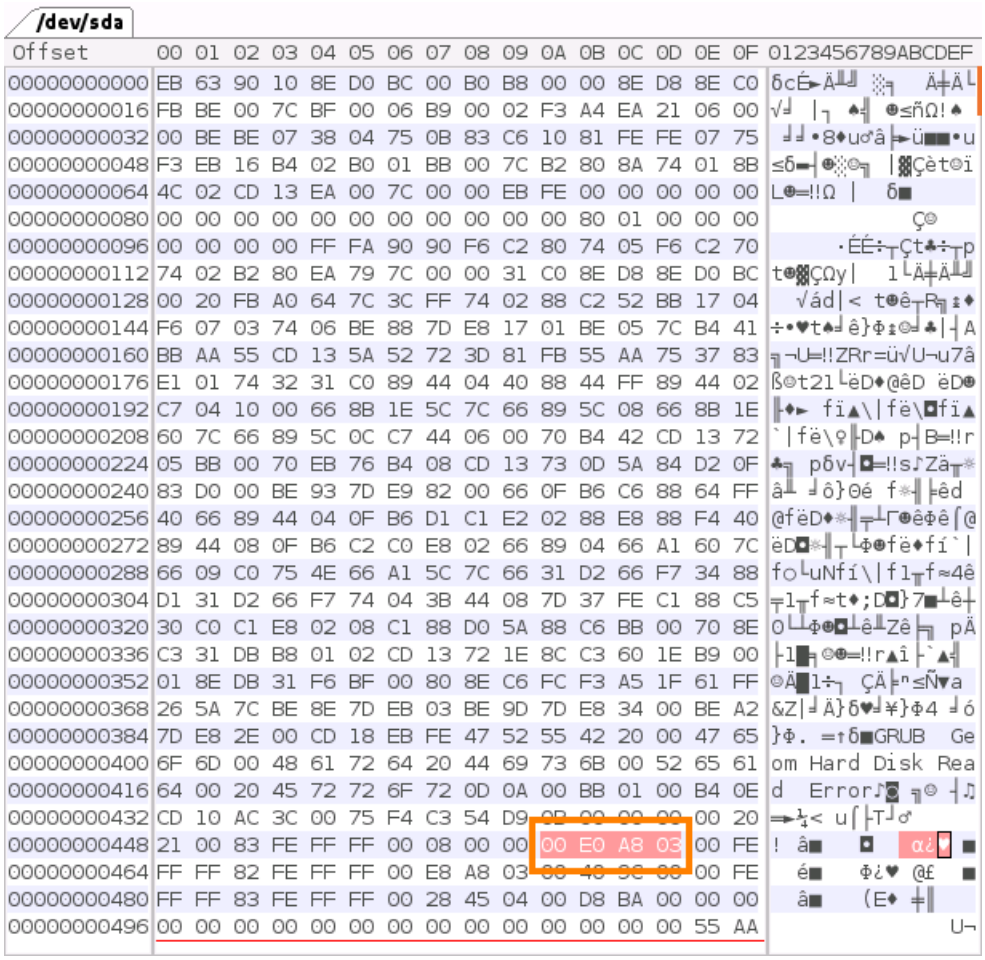
3. Change focus to the **GParted** application.
4. Notice the information is accurate, labeling the partition file system as *ext4*.




| Partition | File System | Mount Point | Label | Size | Used | Unused | Flags |
|---|---|---|---|---|---|---|---|
| /dev/sda1 | ext4 | / | SB@ | 29.28 GiB | 22.42 GiB | 6.86 GiB | |
| /dev/sda2 | linux-swap | | | 4.88 GiB | 0.00 B | 4.88 GiB | |
| /dev/sda3 | ext4 | | | 5.84 GiB | 233.56 MiB | 5.61 GiB | |

5. Change focus back to the **wxHexEditor**. Calculate the size of the partition. The bytes 12 to 15 read *00 E0 A8 03* in hex, which needs to be put into *Little Endian* order.

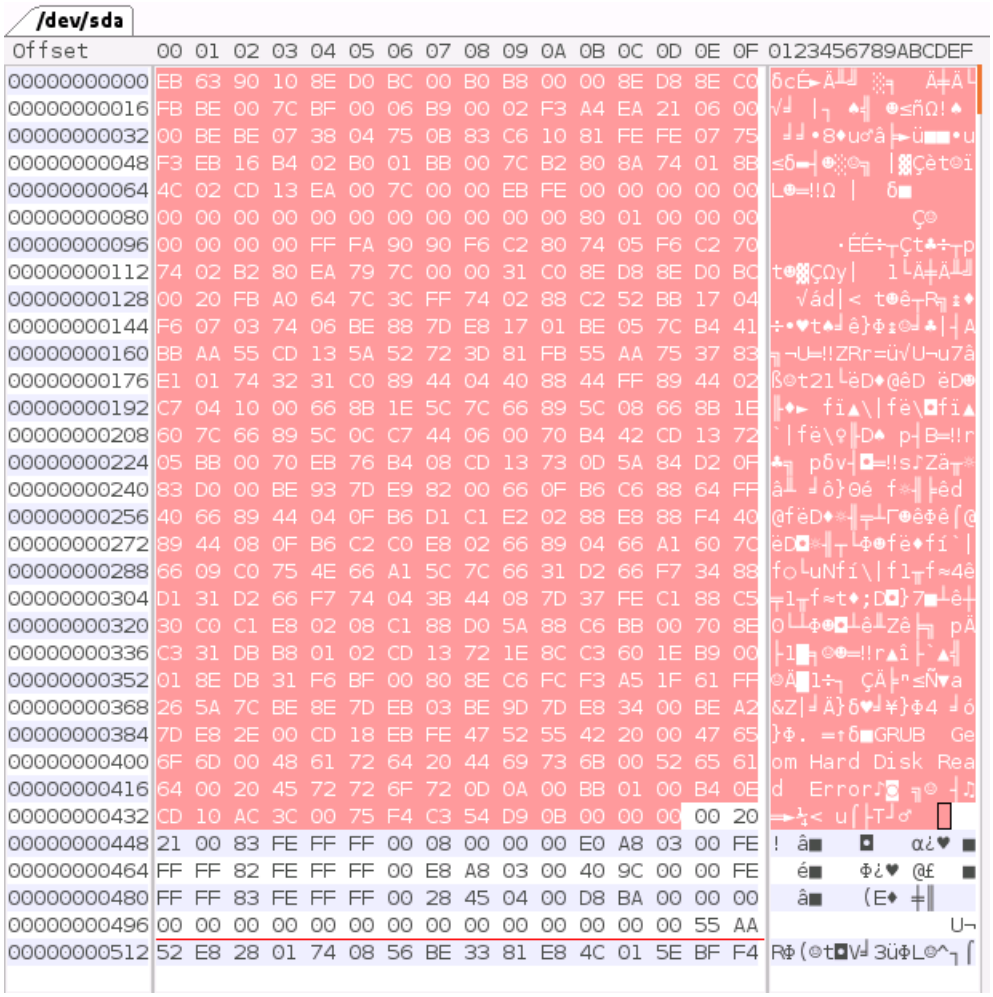



6. To find the number of sectors using the *Little Endian* order, take the Little Endian order *03 A8 E0 00* and convert it to decimal. When converted, the output is **61,399,040,** which is the number of sectors.
7. Convert the number of sectors to bytes; **61,399,040** X **512** bytes/sector = **31,436,308,480** bytes.
8. Convert the number of bytes to gigabytes; **31,436,308,480** bytes / **1,073,741,824** bytes (or $2^{30}$) = **29.277** GiB.
9. Change focus to the **GParted** application and notice that the manual computation resembles closely to the *29.28* GiB size output for */dev/sda1*.


10. Change focus to the **wxHexEditor** application.

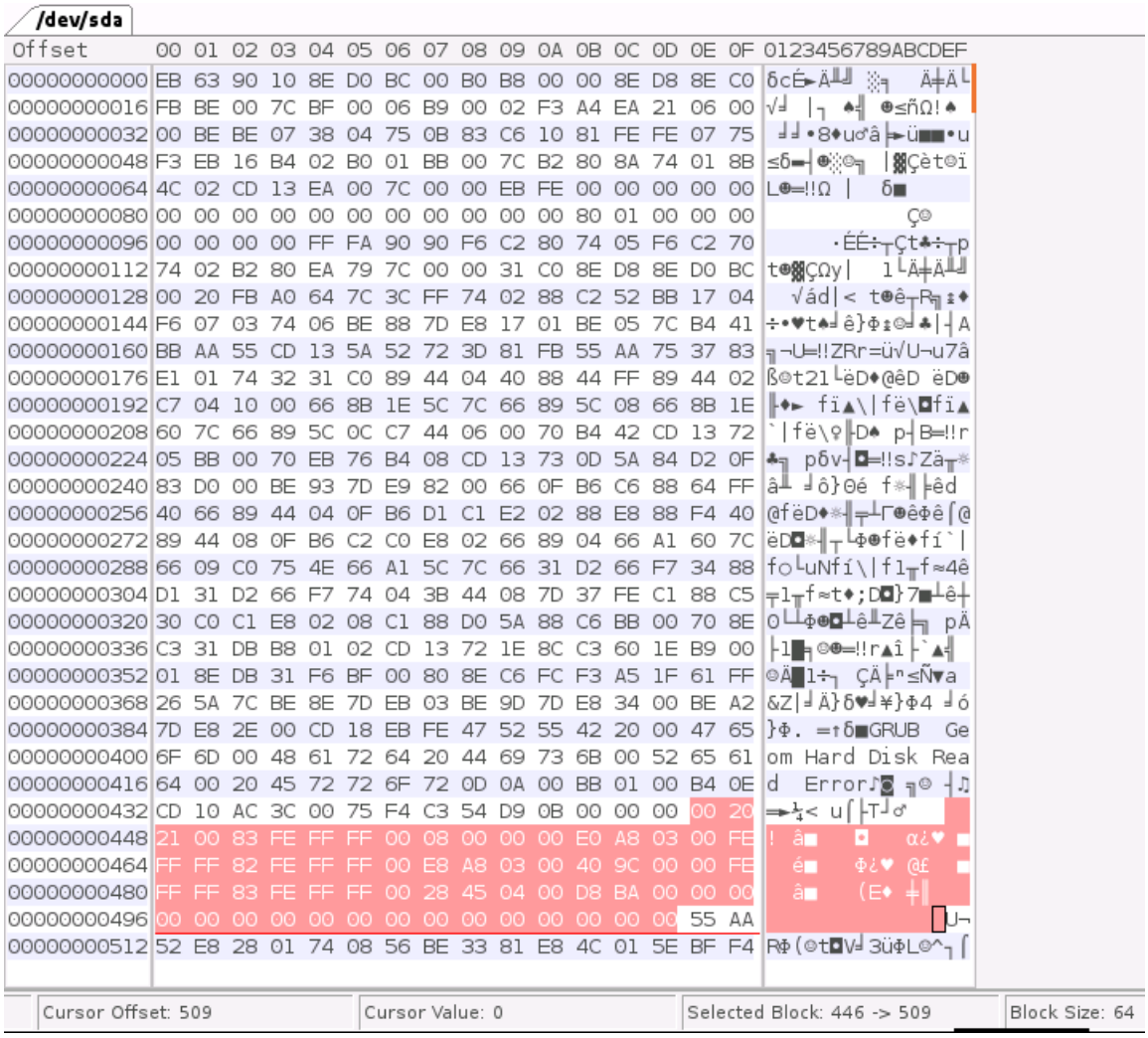
  

11. Identify the beginning of the drive. This is the boot code area of the drive.



12. Notice the entire partition table follows and it is 64 bytes. End with the boot signature of "*55 AA*".

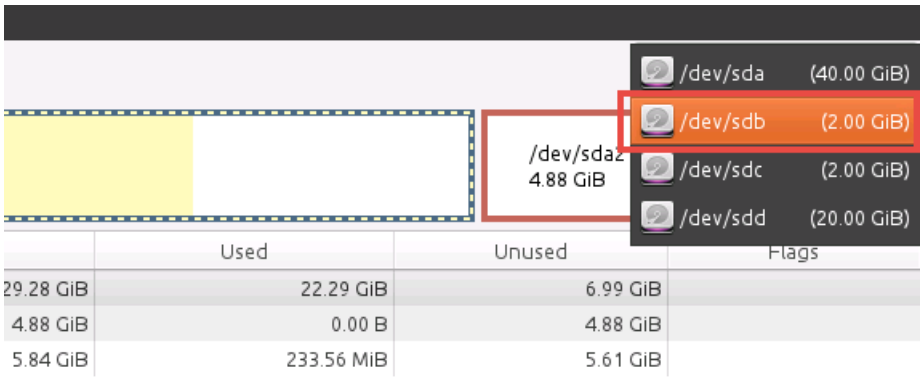



13. Close the **wxHexEditor** and **terminal** application window.

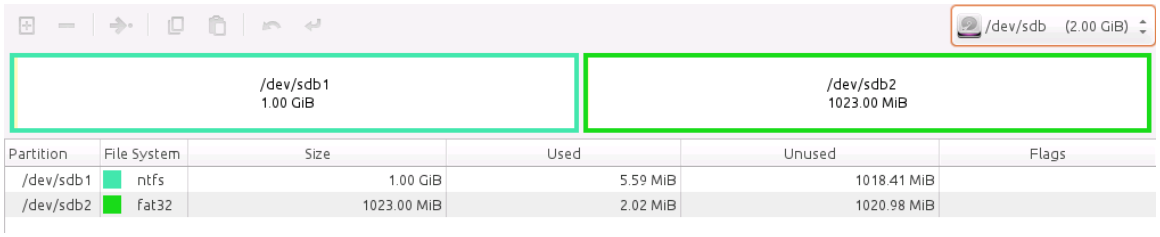
  

## 5 Exploring Windows Data Structure

1. Change focus to the **GParted** application window.
2. In the top-right corner, click on the **/dev/sda (40.00GiB)** drop-down menu and choose **/dev/sdb**.




3. Notice the different hard drive with two partitions.

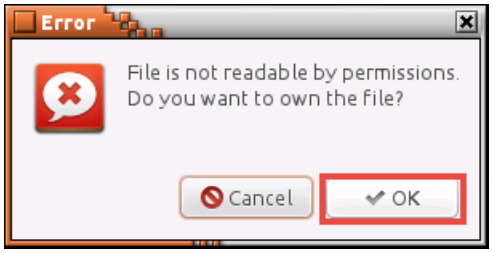



4. Open a new **terminal** window.

5. Using the terminal, enter the command below to open the **/dev/sdb** drive with **wxHexEditor**.

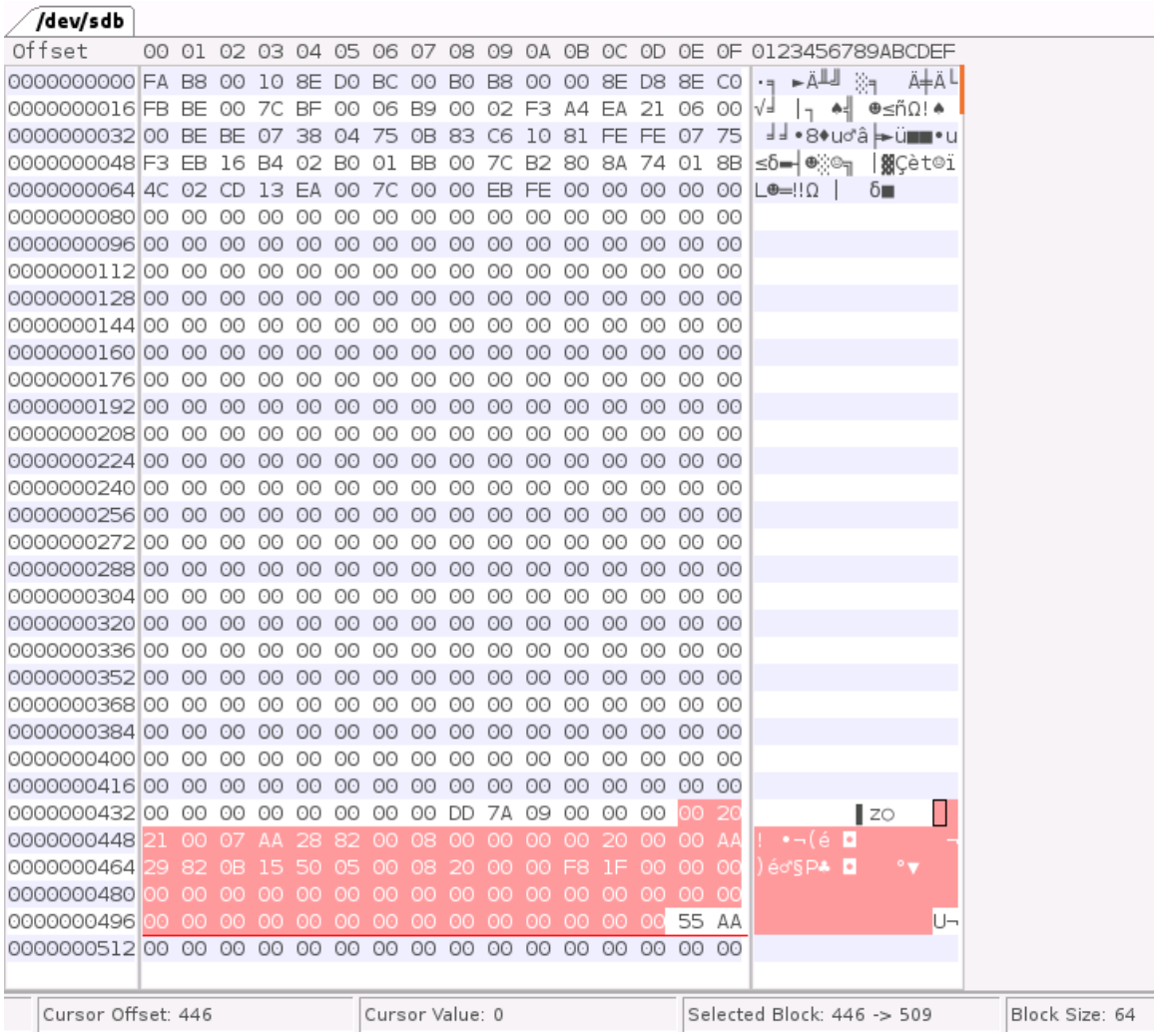
```
wxHexEditor /dev/sdb
```


6. If presented with a permissions error message, click **OK** to continue.



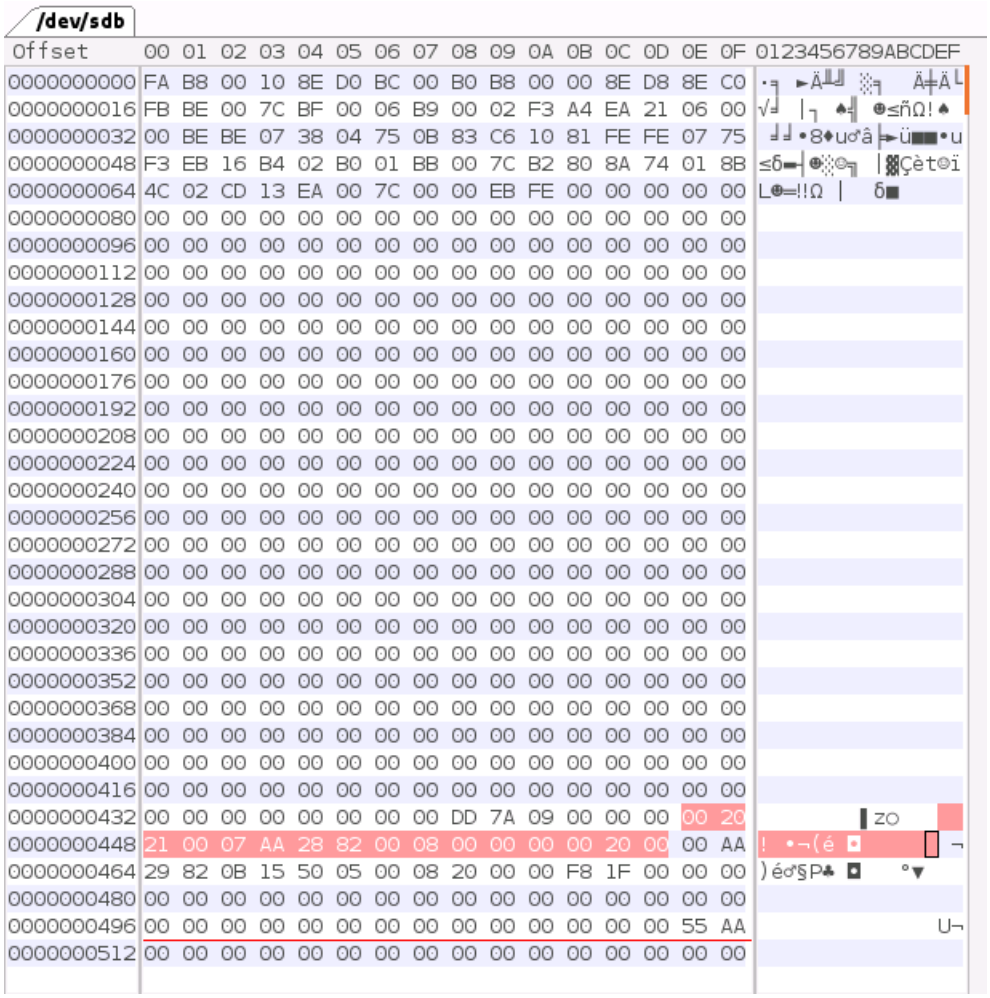
7. Using the *wxHexEditor*, identify the partition table. To do so, find the signature, **55 AA**, and count back 64 bytes.



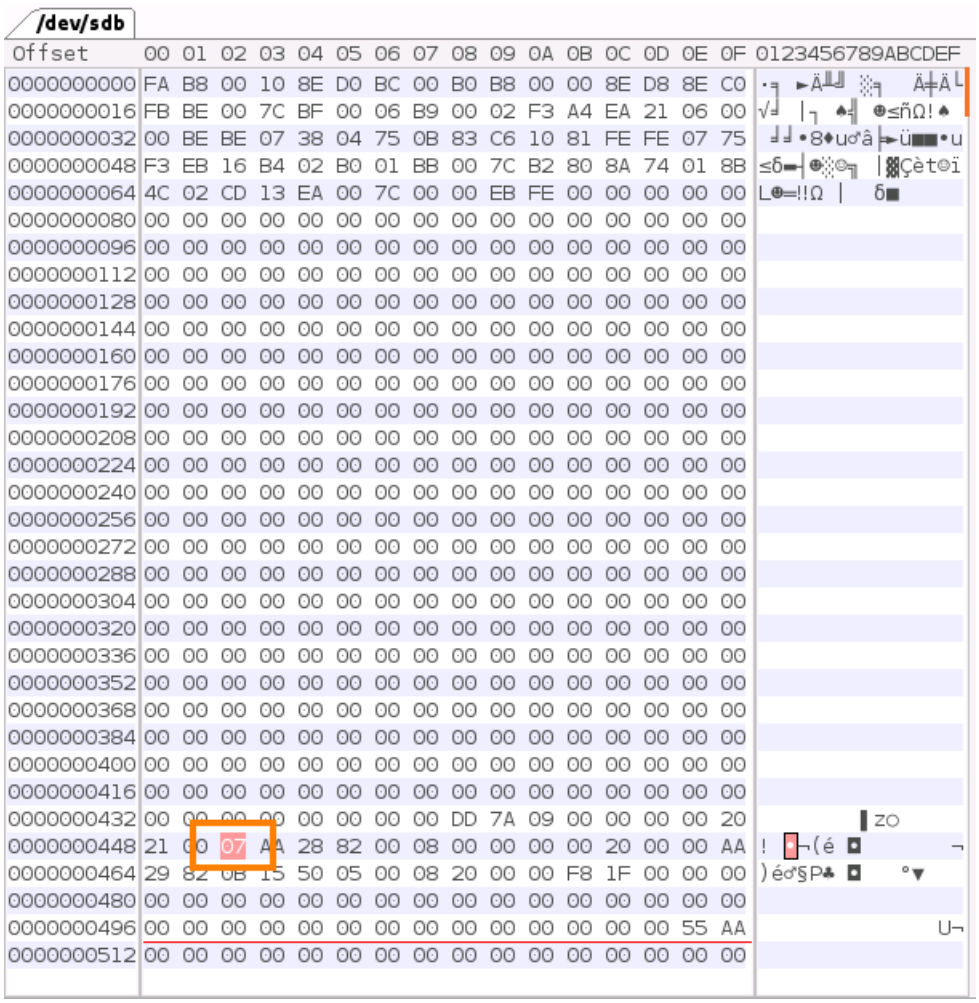
## 6 Exploring the /dev/sdb1 Partition

1. Identify the first partition, which will be **/dev/sdb1**.

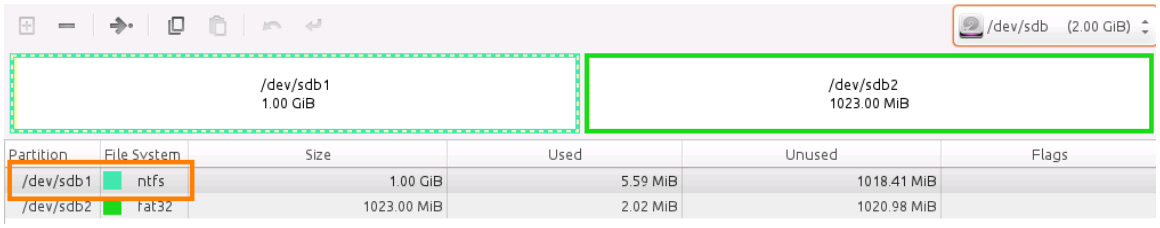


2. Identify the 4th byte of the */dev/sdb1* partition. Notice that the partition ID number is "*07*".

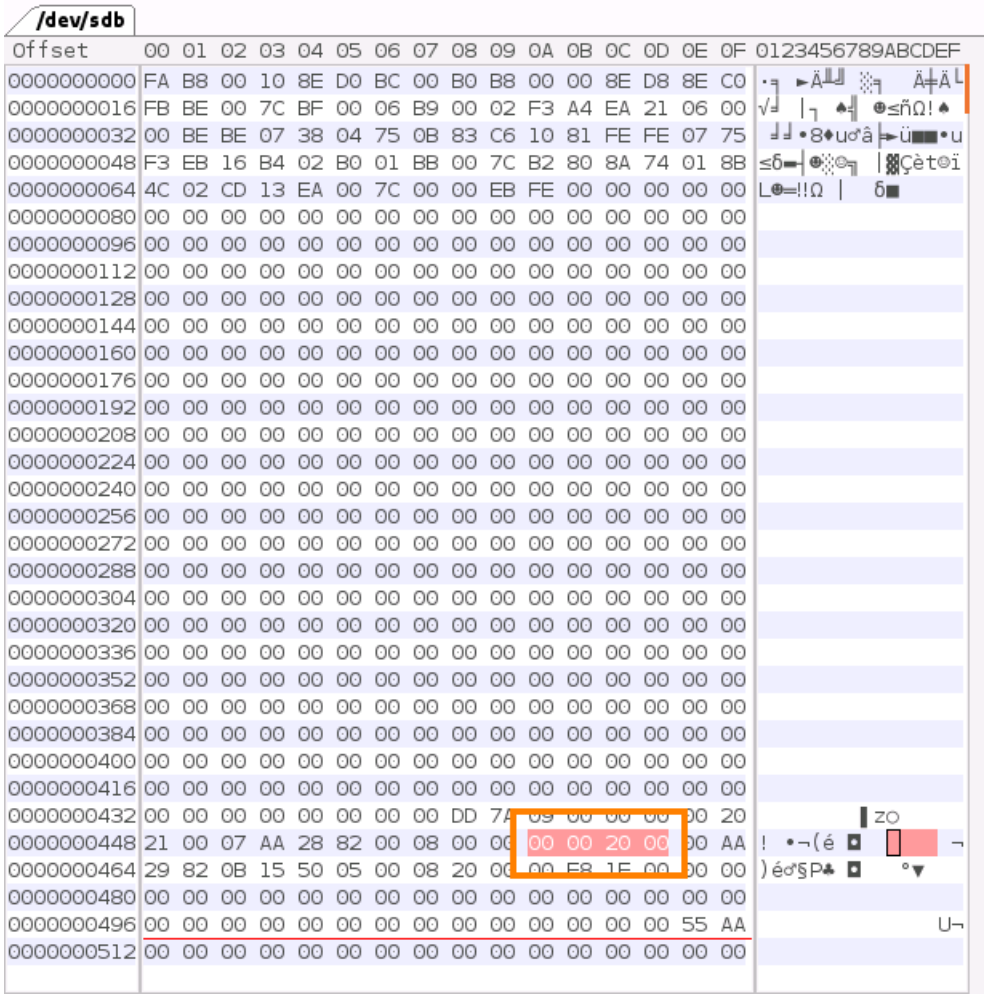



3. When referencing back to the partition ID table from *Task 2*, notice that partition ID #07 is *NTFS*. Change focus to the **GParted** application window.
4. Notice that in the *GParted* application, it labels the */dev/sdb1* partition as a *NTFS* file system as well.

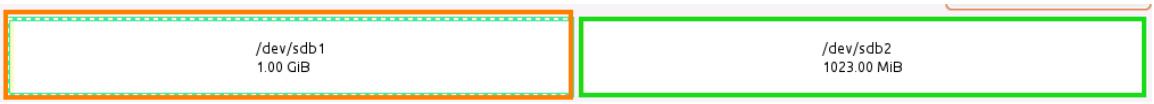


5. Change focus back to the **wxHexEditor**. Calculate the size of the partition. The bytes 12 to 15 read *00 00 20 00* in hex, which needs to be put into *Little Endian* order.



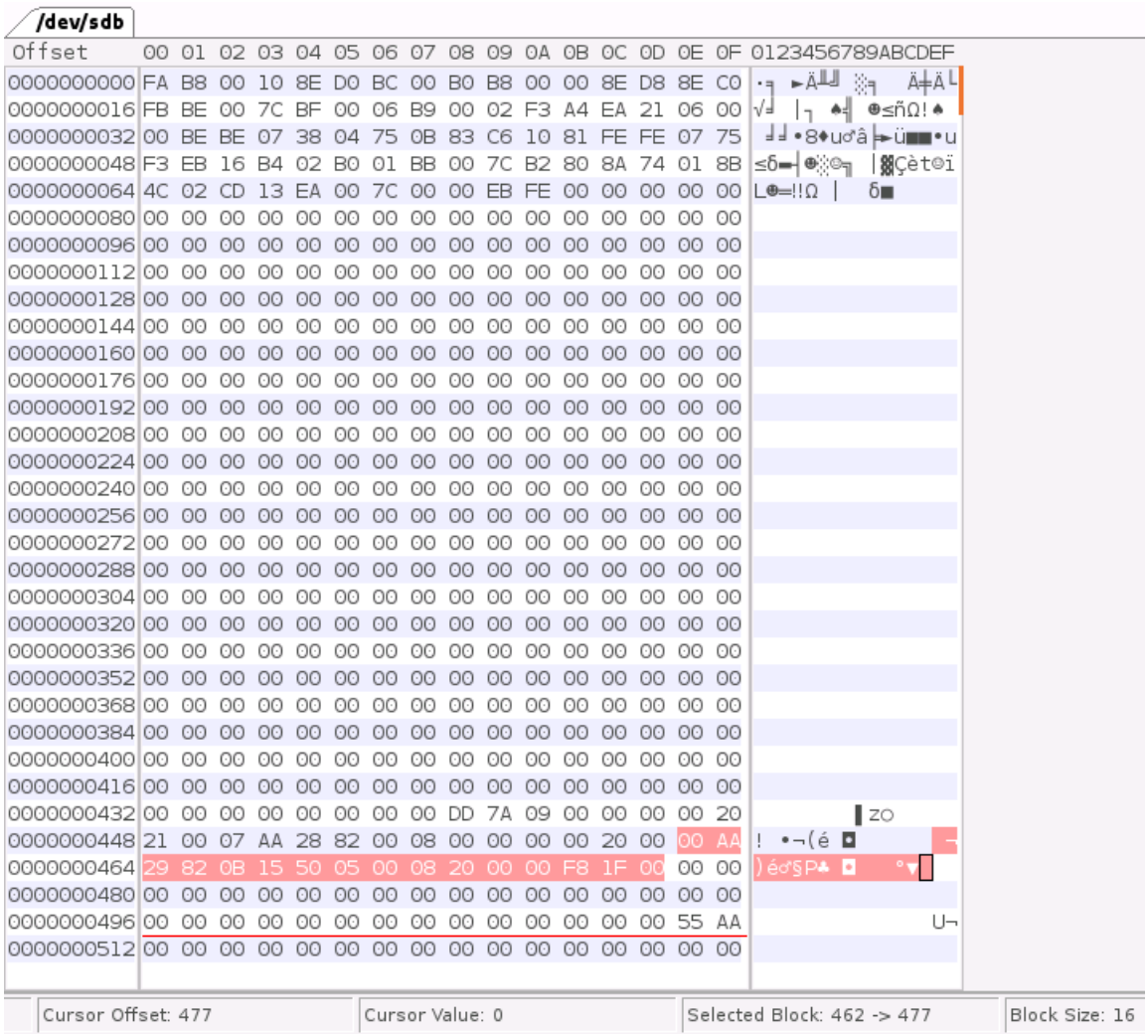

6. To find the number of sectors using the *Little Endian* order, take the Little Endian order *00 20 00 00* and convert it to decimal. When converted, the output is **2,097,152,** which is the number of sectors.
7. Convert the number of sectors to bytes; **2,097,152** X **512** bytes/sector = **1,072,741,824** bytes.
8. Convert the number of bytes to gigabytes; **1,072,741,824** bytes / **1,073,741,824** bytes (or $2^{30}$) = **0.999** GiB.
9. Change focus to the **GParted** application and notice that the manual computation resembles closely to the *1.00* GiB size output for */dev/sdb1*.



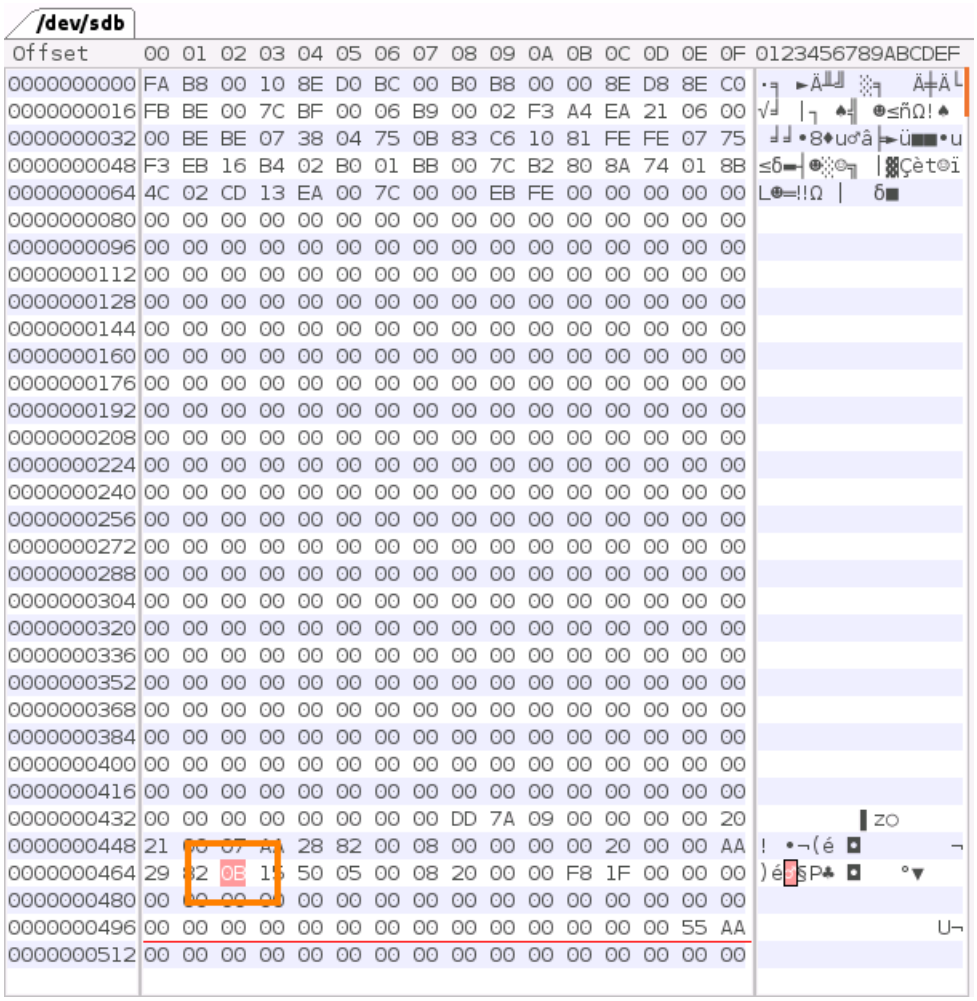
## 7 Exploring the /dev/sdb2 Partition

1. Change focus to the **wxHexEditor** application window.
2. Identify the second partition on the */dev/sdb* disk.

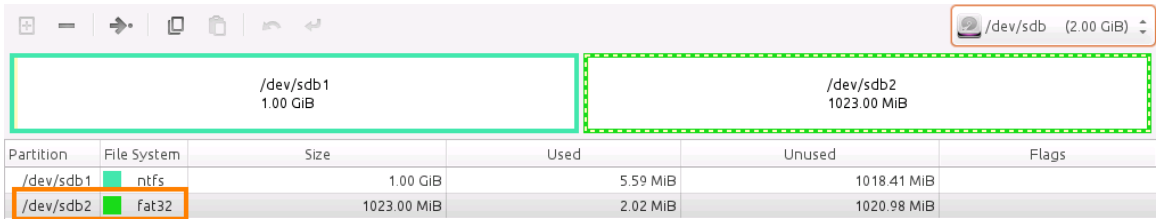


3. Identify the 4th byte of the */dev/sdb2* partition. Notice that the partition ID number is "*0B*".

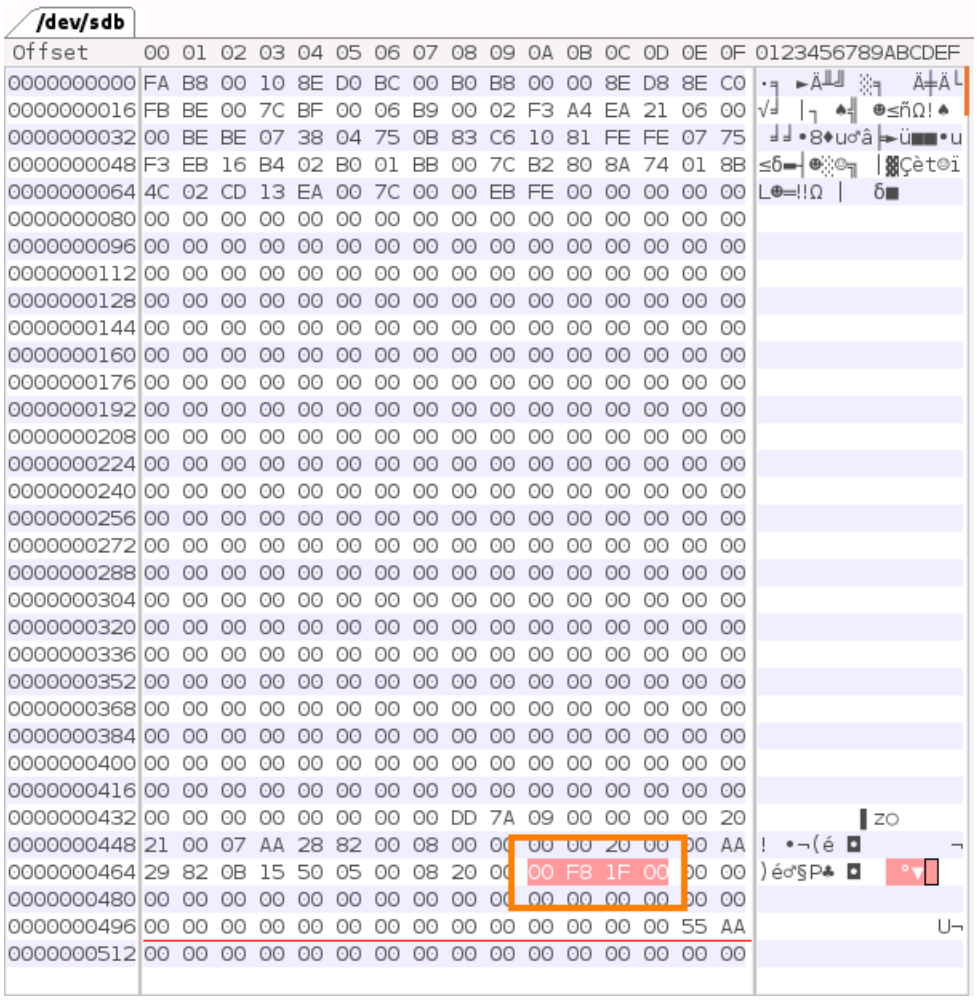



4. When referencing back to the partition ID table from *Task 2*, notice that partition ID #0B is *FAT32*. Change focus to the **GParted** application window.
5. Notice that in the *GParted* application, it labels the */dev/sdb2* partition as a *FAT32* file system.

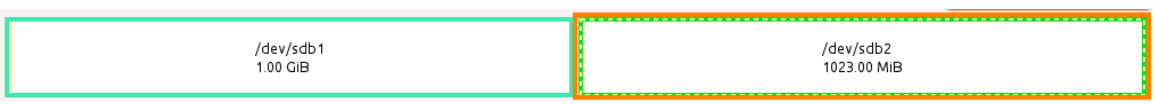


6. Change focus back to the **wxHexEditor**. Calculate the size of the partition. The bytes 12 to 15 read *00 F8 1F 00* in hex, which needs to be put into *Little Endian* order.



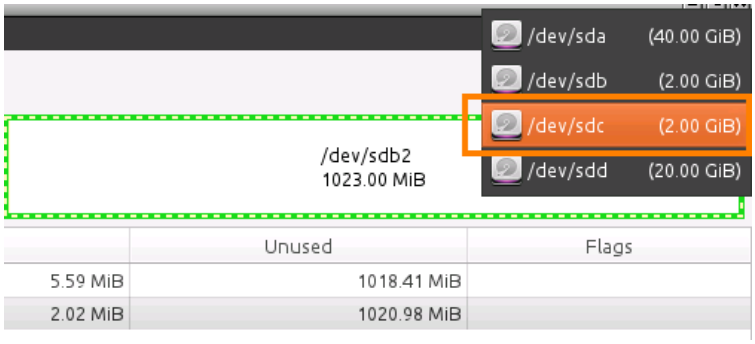

7. To find the number of sectors using the *Little Endian* order, take the Little Endian order *00 1F F8 00* and convert it to decimal. When converted, the output is **2,095,104,** which is the number of sectors.
8. Convert the number of sectors to bytes; **2,095,104** X **512** bytes/sector = **1,072,741,824** bytes.
9. Convert the number of bytes to gigabytes; **1,072,693,248** bytes / **1,073,741,824** bytes (or $2^{30}$) = **0.999** GiB.
10. Close the **wxHexEditor** and terminal application windows.
11. Change focus to the **GParted** application and notice that the manual computation resembles closely to the *1023.00* MiB size output for */dev/sdb2*.



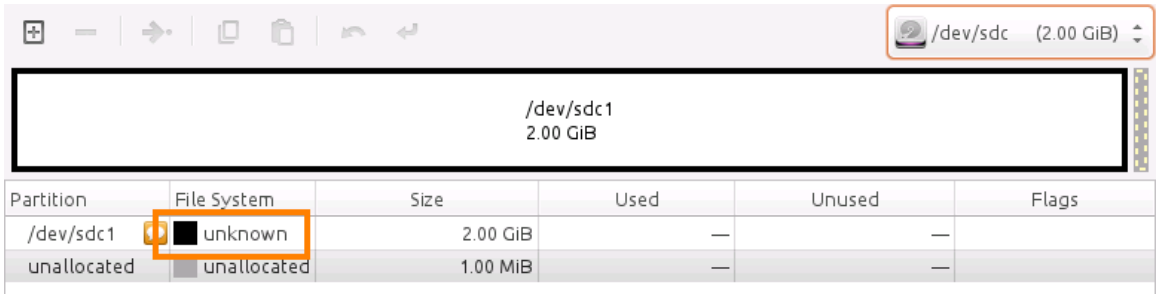

  

## 8 Exploring GPT Partitions

1. Using the *GParted* application, in the top-right corner, click on the **/dev/sdb (2.00GiB)** drop-down menu and choose **/dev/sdc**.




2. Notice the different hard drive with only one unknown partition.




3. Open a new **terminal** window.

4. Using the terminal, enter the command below as an attempt to identify the unknown partition of */dev/sdc*.

```
sudo gdisk /dev/sdc
```

```
caine@Caine01:~$ sudo gdisk /dev/sdc
GPT fdisk (gdisk) version 0.8.8

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.

Command (? for help):
```

Notice that *GPT* is present on the disk, therefore, the partition is *GPT*.

5. Enter the **P** character followed by pressing the **Enter** key.

```
Command (? for help): p
Disk /dev/sdc: 4194304 sectors, 2.0 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 129E29BB-94D0-41C9-90B5-33B481CC1739
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 4194270
Partitions will be aligned on 2048-sector boundaries
Total free space is 4029 sectors (2.0 MiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048         4192255   2.0 GiB     8300

Command (? for help):
```

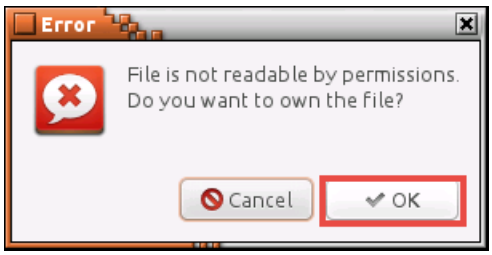
Notice the partition table can hold up to 128 entries as opposed to just 4 with an *MBR*.

6. Press the **Q** character followed by pressing the **Enter** key to quit.
7. Using the same terminal, enter the command below to open the **/dev/sdc** drive with **wxHexEditor**.

```
wxHexEditor /dev/sdc
```

```
caine@Caine01:~$ wxHexEditor /dev/sdc
```

8. If presented with a permissions error message, click **OK** to continue.



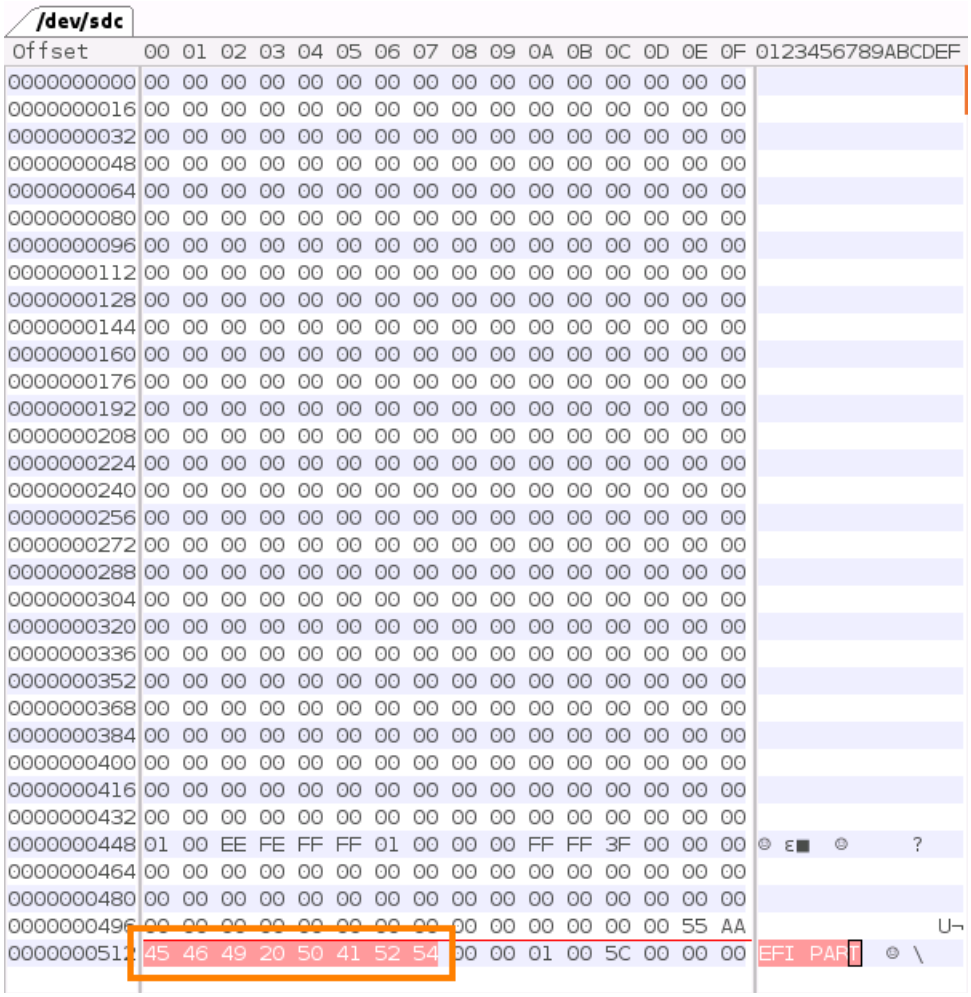

  

9. Notice in *wxHexEditor* that the */dev/sdb* disk looks different when compared to a *Master Boot Record* (*MBR*) scheme. In *MBR*, the sector starts on *0000000000*. *GUID Partition Table* (*GPT*) on the other hand, starts right after the *55 AA* signature. This is to preserve backwards compatibility with legacy MBR boot code. Moving forward with the lab, use the table below as a reference for the GPT scheme.

| Offset | Length | Contents |
|---|---|---|
| 0 | 8 bytes | Signature ("EFI PART", 45 46 49 20 50 41 52 54) |
| 8 | 4 bytes | Revision (For GPT version 1.0 (through at least UEFI version 2.3.1), the value is 00 00 01 00) |
| 12 | 4 bytes | Header size in little endian (in bytes, usually 5C 00 00 00 meaning 92 bytes) |
| 16 | 4 bytes | CRC32 of header (0 to header size), with this field zeroes during calculation |
| 20 | 4 bytes | Reserved; must be zero |
| 24 | 8 bytes | Current LBA (location of this header copy) |
| 32 | 8 bytes | Backup LBA (location of the other header copy) |
| 40 | 8 bytes | First usable LBA for partitions (primary partition table last LBA + 1) |
| 48 | 8 bytes | Last usable LBA (secondary partition table first LBA – 1) |
| 56 | 16 bytes | Disk GUID (also referred to as UUID on UNIXes) |
| 72 | 8 bytes | Partition entries starting LBA (always 2 in primary copy) |
| 80 | 4 bytes | Number of partition entries |
| 84 | 4 bytes | Size of partition entry (usually 128) |
| 88 | 4 bytes | CRC32 of partition array |
| 92 | * | Reserved; must be zeroes for the rest of the block (420 bytes for a 512-byte LBA) |
| **LBA size** | **Total** | |

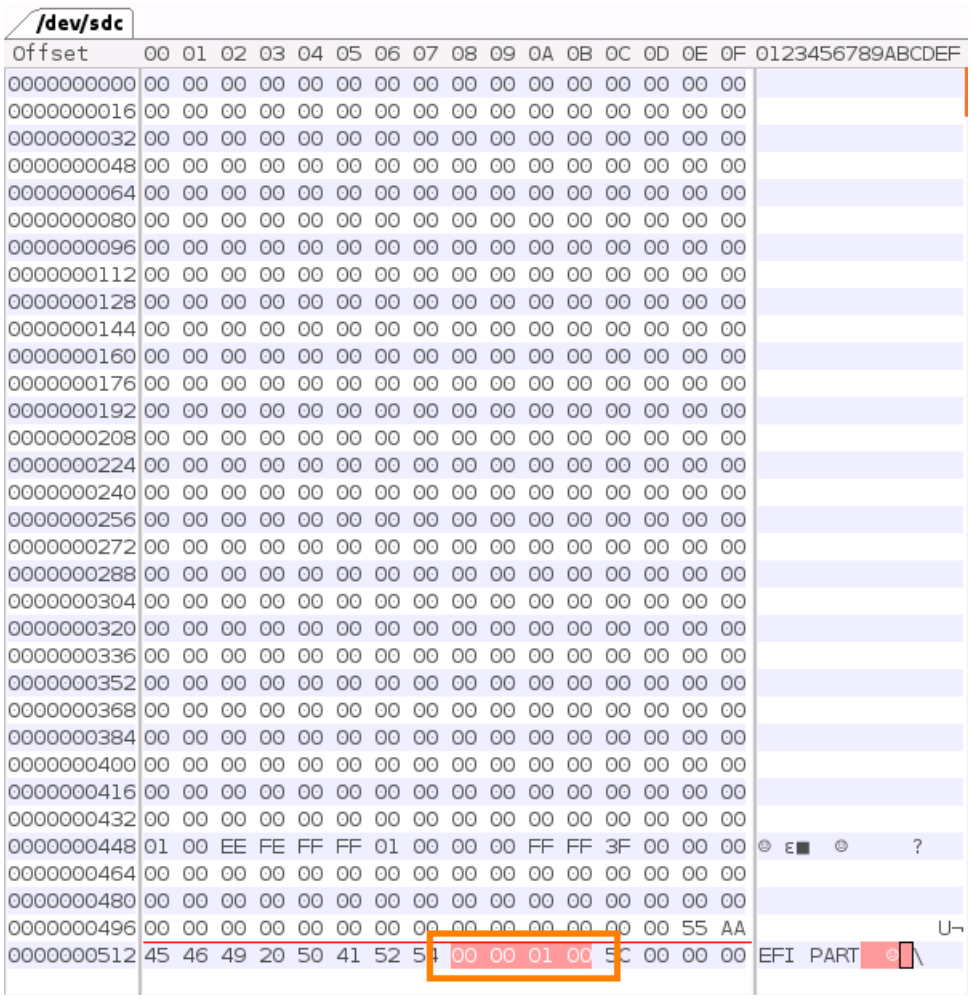
  

10. Using *wxHexEditor*, notice that from *0x00* to *0x08* identifies this disk as an *EFI* (adheres to the *Unified Firmware Interface*) partition.



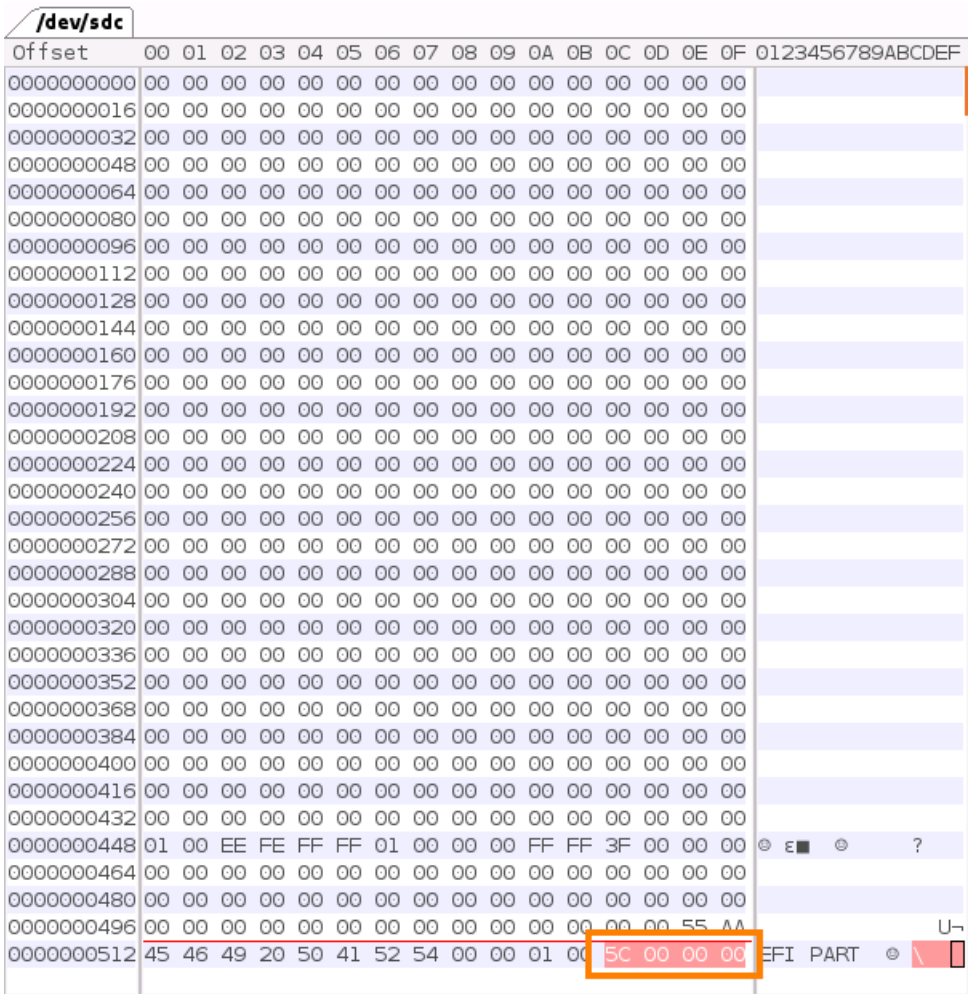

  

11. Using *wxHexEditor*, move over to the next 4 bytes to identify the revision number.



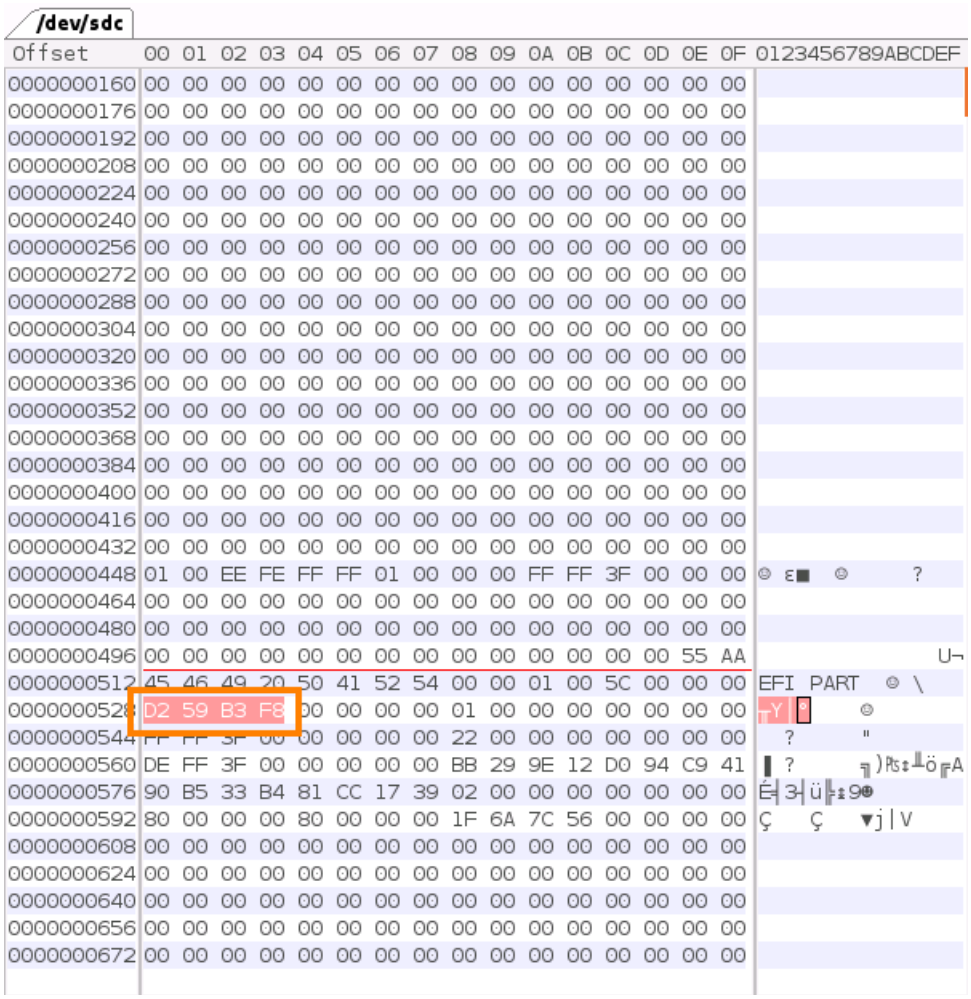
12. Move over another 4 bytes to identify the header size in *Little Endian*.




The hex identified is *5C 00 00 00* which equals *5C* in *Little Endian* format (by removing the leading zeros) to equal out 92 bytes in decimal.

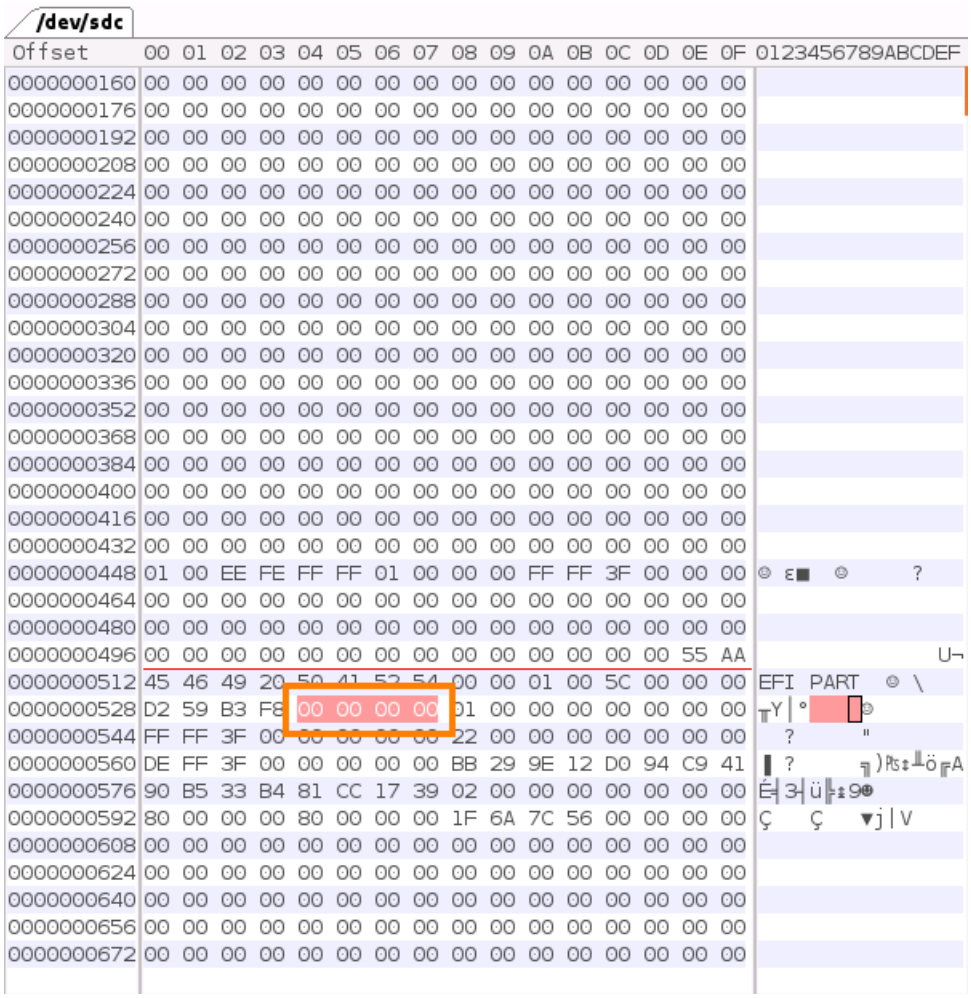
  

13. Moving to the next 4 bytes and the *Cyclic Redundancy Check* (*CRC-32*) can be identified.



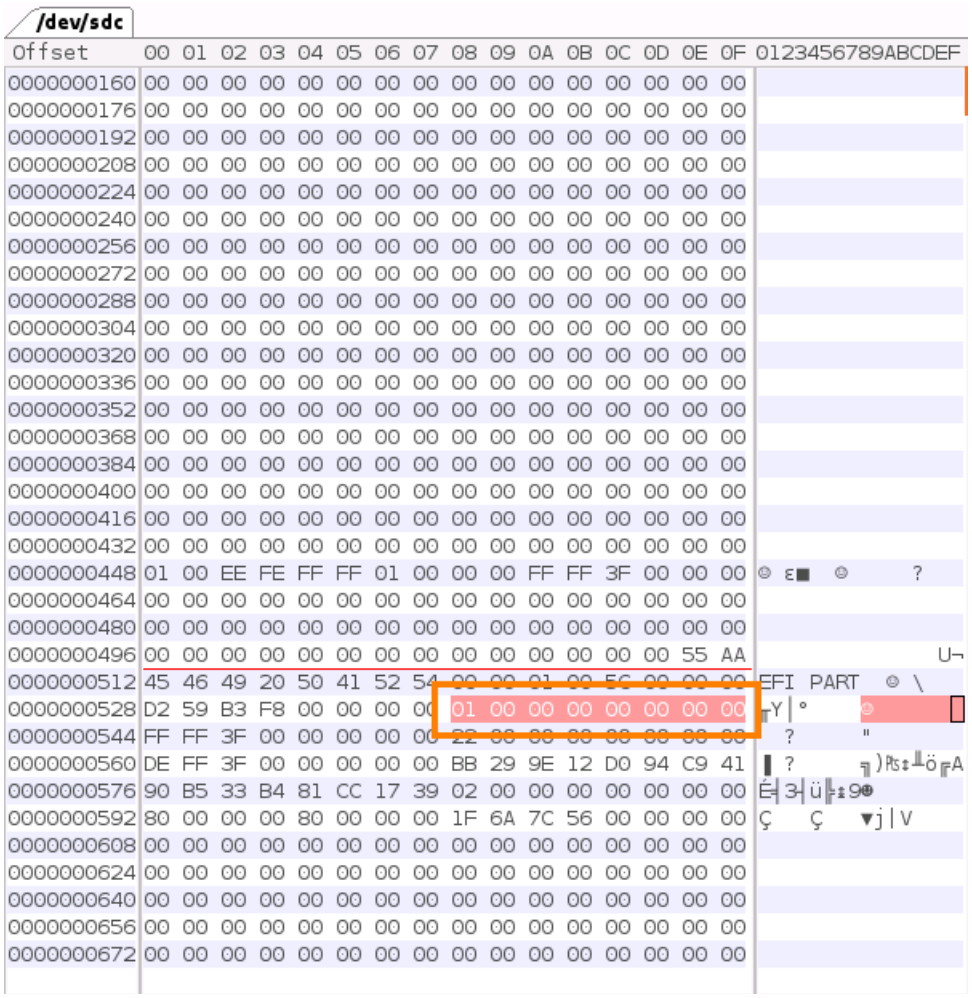

  

14. The following 4 bytes are reserves and must be zeros.



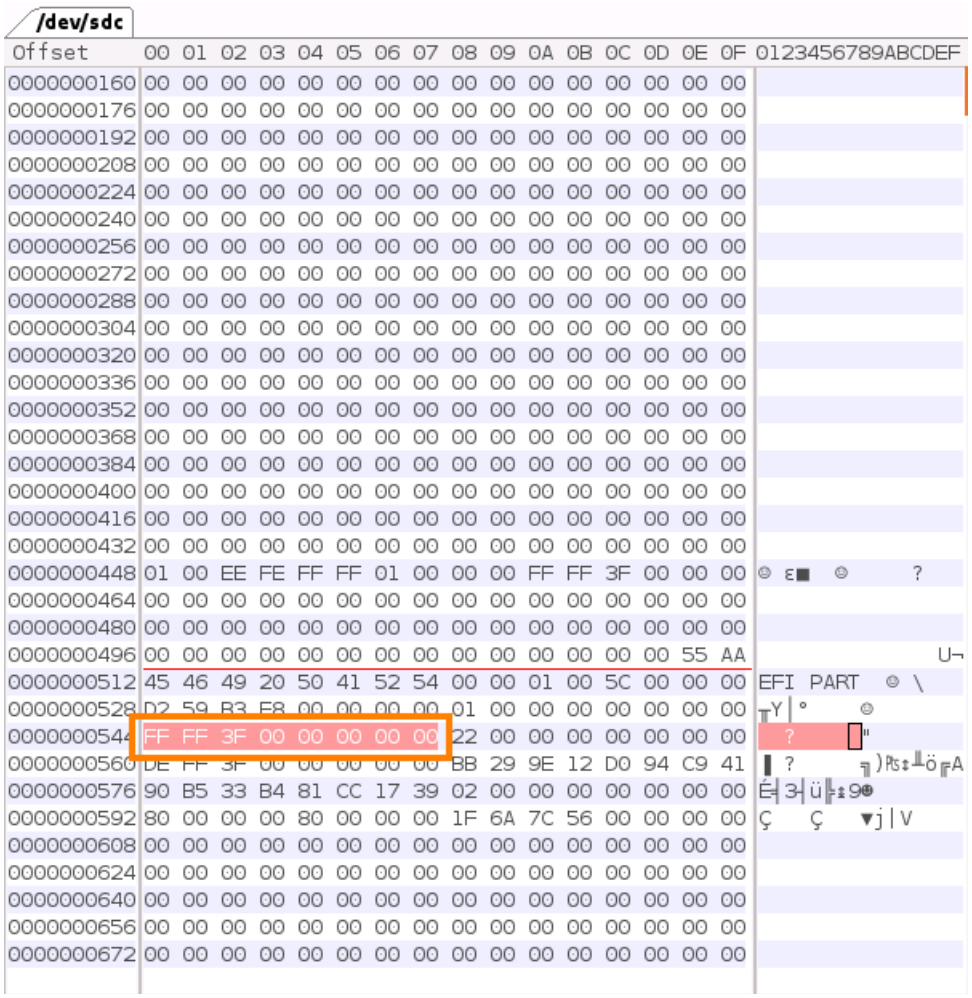
15. The next 8 bytes helps identify the location of the header block.




When converting to Little Endian; take the original hex, *01 00 00 00 00 00 00 00*, and convert to *00 00 00 00 00 00 00 01* which equals sector 1.

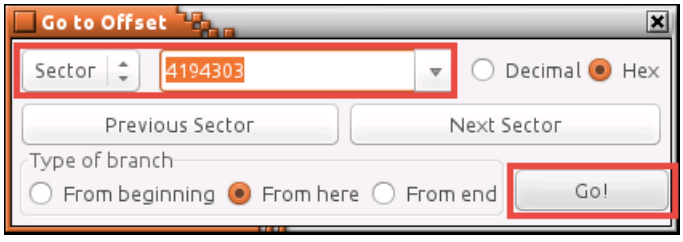
  

16. The next 8 bytes is where the backup is kept.



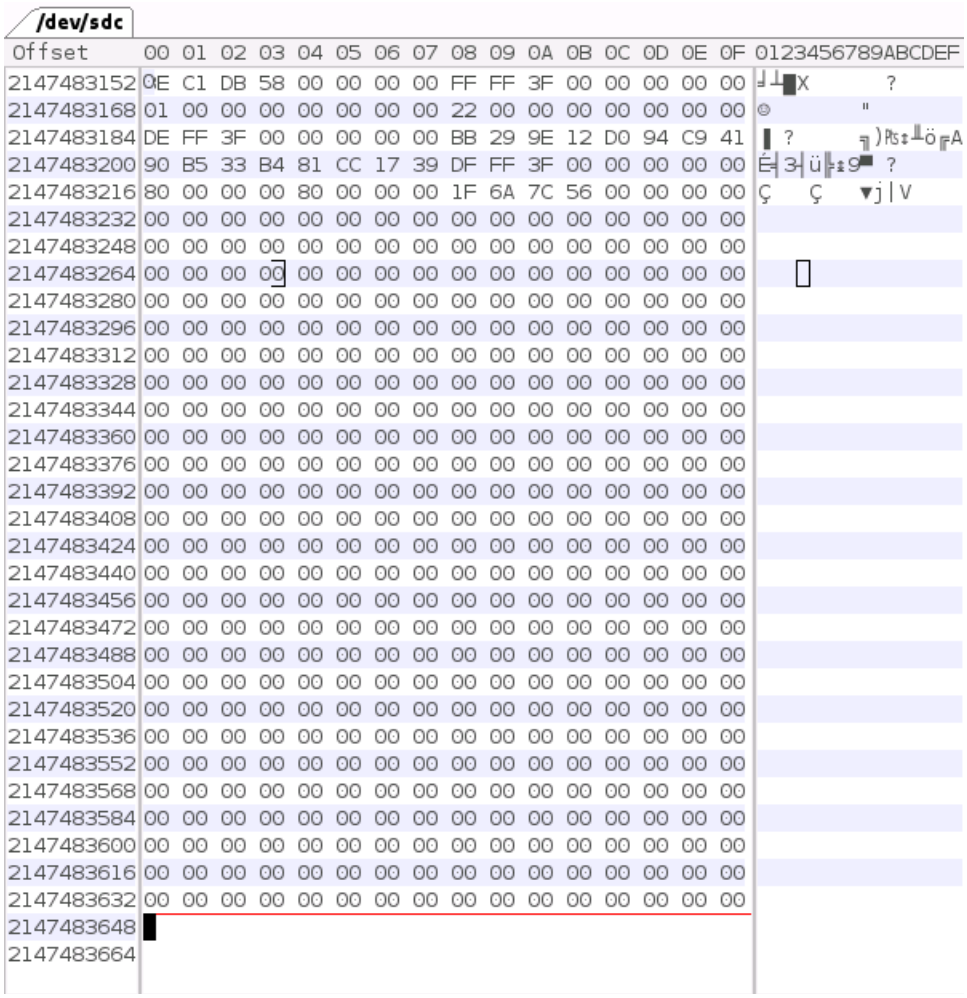

When converting to Little Endian; take the original hex, *FF FF 3F 00 00 00 00 00*, and convert to *00 00 00 00 3F FF FF* which equals sector 4194303.

17. Using *wxHexEditor*, press **CTRL+G** and type the sector number, **4194303**, in decimal and make sure **Sector** is selected. Click the **Go!** button.



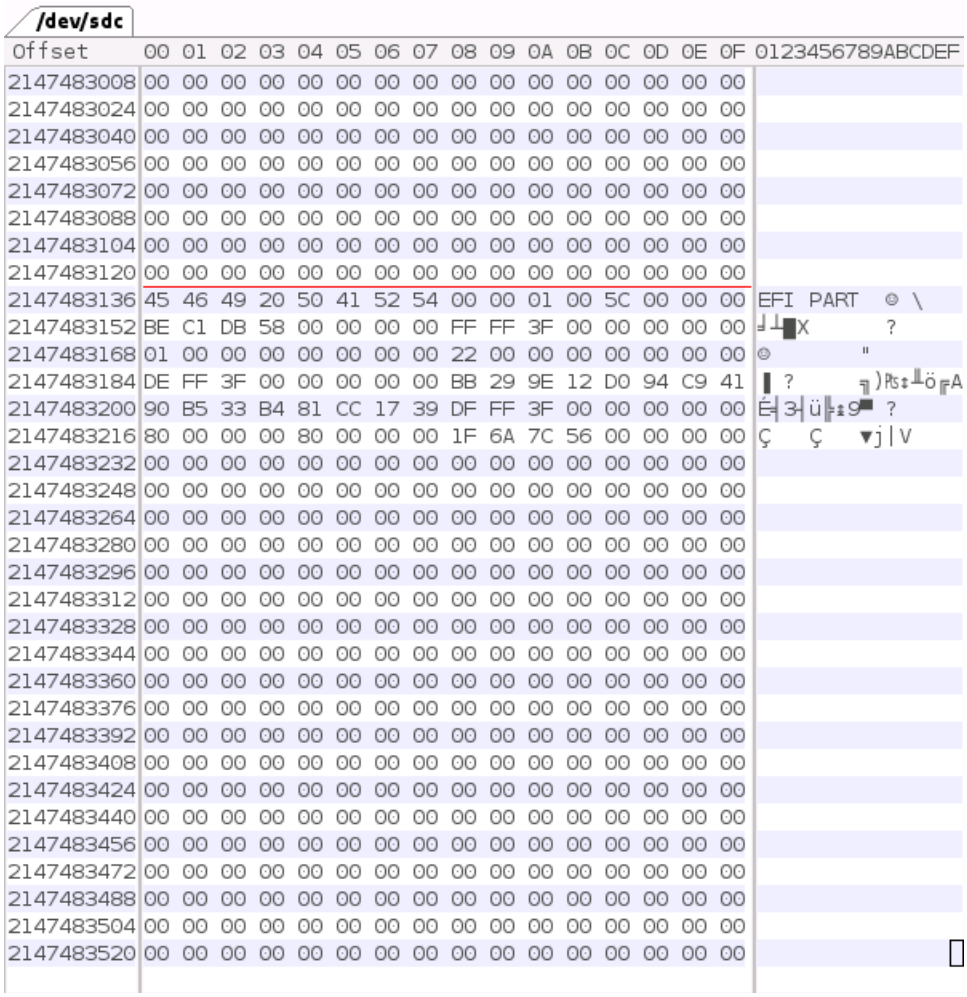

  

18. Notice that it takes you to the end of the disk.

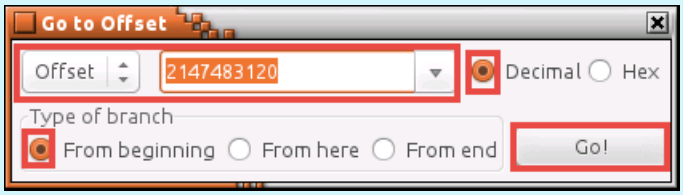


19. Scroll up a few offsets, to offset **2147483120**, and notice the backup copy. This is the backup for sector 1.

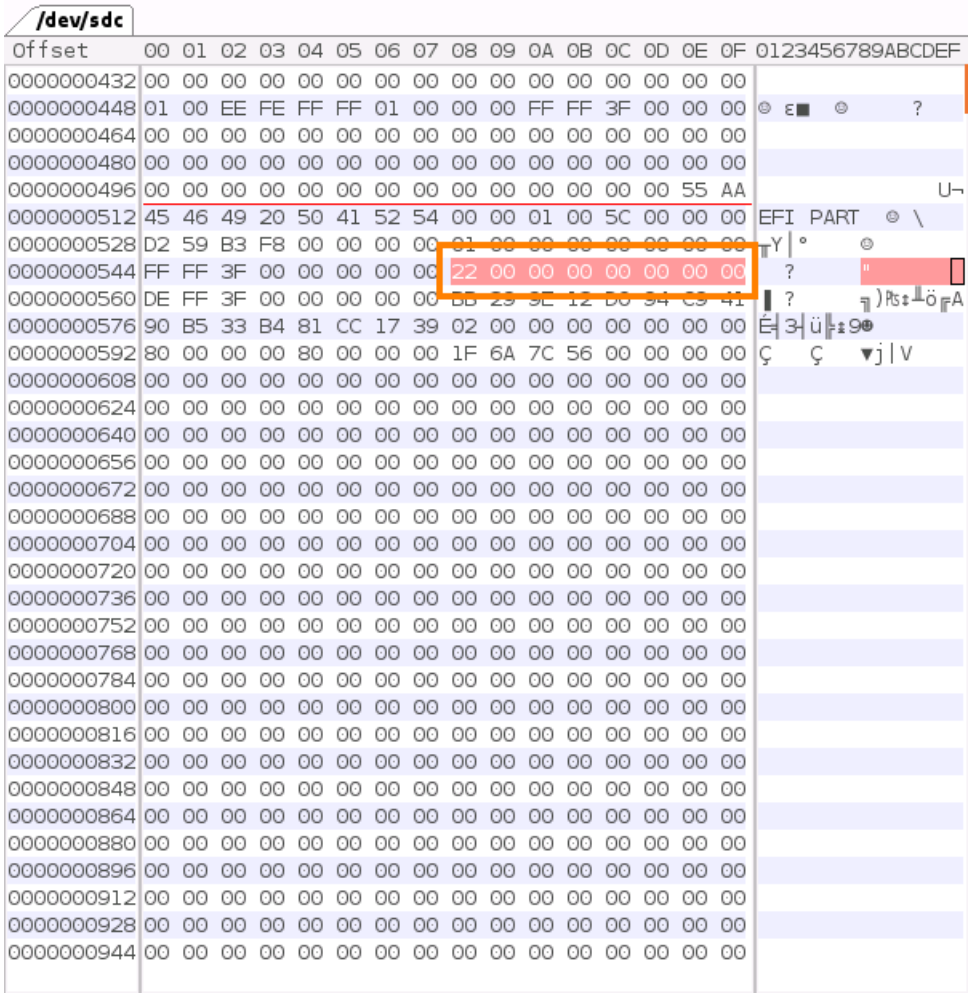



It may be easier to navigate using the available search by offset function provided by the *wxHexEditor* application. Press **CTRL+G** and search by the desired offset, in this case, **2147483136**, with **Decimal** selected.



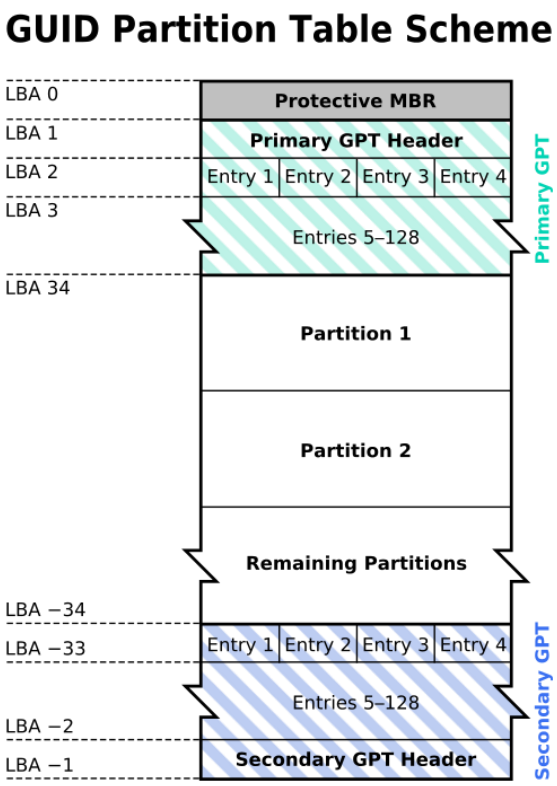

  

20. Navigate back towards the beginning, specifically to the **00000000544** offset. The 8 bytes shown below are assigned for the first usable *Logical Block Addressing* (*LBA*) for partitions (primary partition table last *LBA* 1).



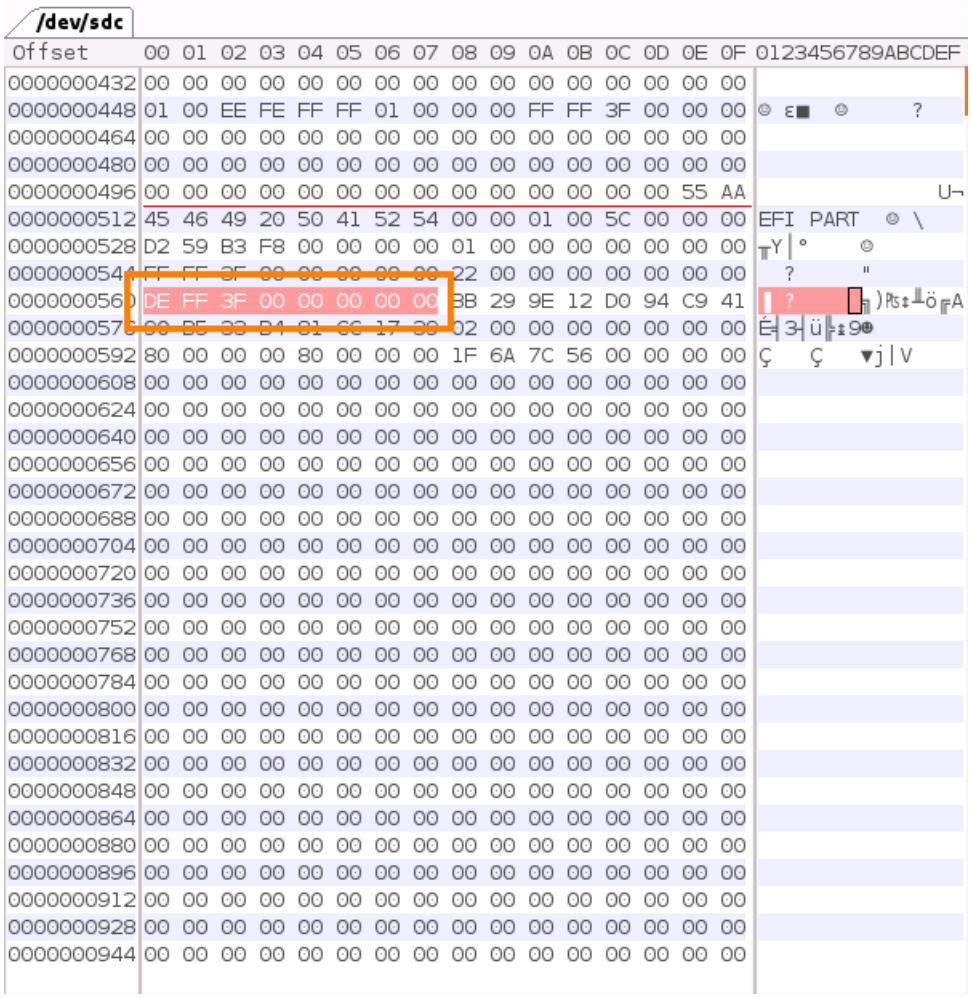

  

When converting to Little Endian; take the original hex, *22 00 00 00 00 00 00 00*, and convert to *00 00 00 00 00 00 00 22* which equals 34 bytes in decimal. See the table below for reference on *LBA 34*.



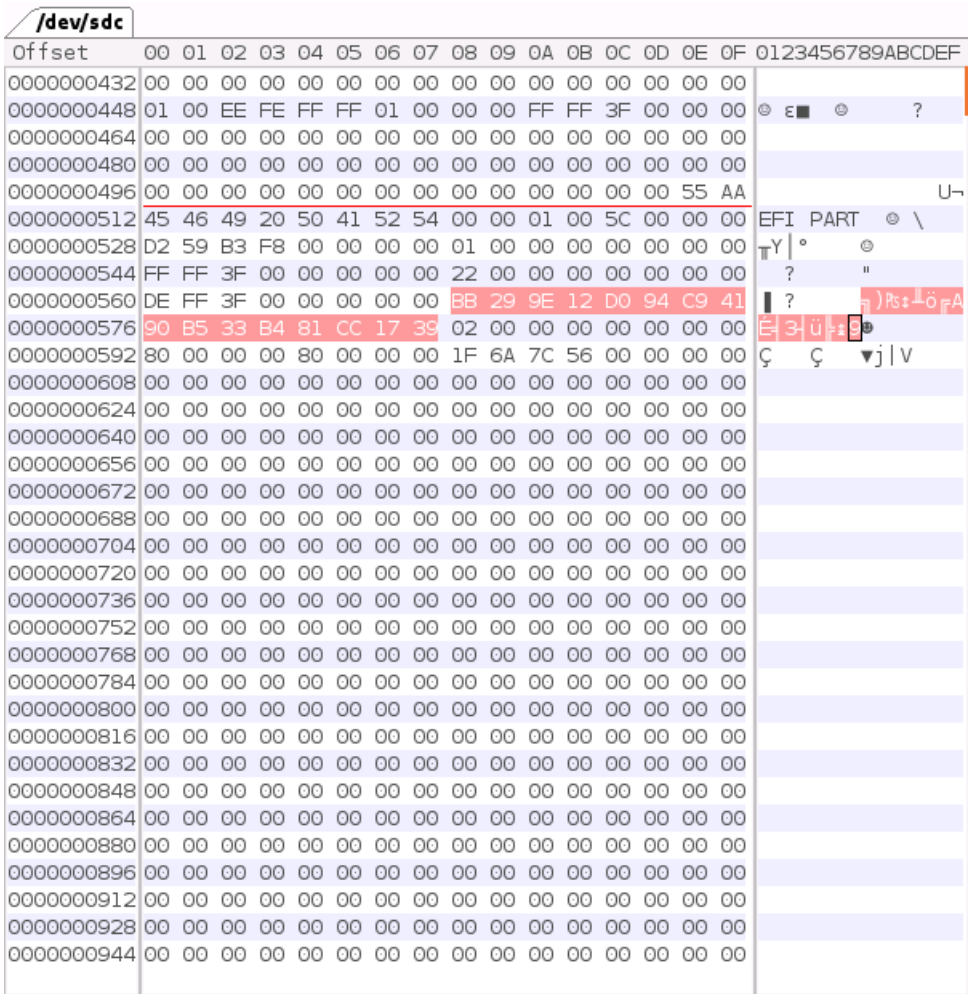
21. The next 8 bytes are the last usable *LBA* (secondary partition table first *LBA* -1).




When converting to Little Endian; take the original hex, *DE FF 3F 00 00 00 00 00*, and convert to *00 00 00 00 3F FF DE,* which equals sector 4194270.

22. The following 16 bytes are reserved for the *GUID*.



/dev/sdc

| Offset | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000000432 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000448 | 01 | 00 | EE | FE | FF | FF | 01 | 00 | 00 | 00 | FF | FF | 3F | 00 | 00 | 00 | ☺ ε■ ☺ ? |
| 0000000464 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000480 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000496 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 55 | AA | U¬ |
| 0000000512 | 45 | 46 | 49 | 20 | 50 | 41 | 52 | 54 | 00 | 00 | 01 | 00 | 5C | 00 | 00 | 00 | EFI PART ☺ \ |
| 0000000528 | D2 | 59 | B3 | F8 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ╥Y│° ☺ |
| 0000000544 | FF | FF | 3F | 00 | 00 | 00 | 00 | 00 | 22 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ? " |
| 0000000560 | DE | FF | 3F | 00 | 00 | 00 | 00 | 00 | BB | 29 | 9E | 12 | D0 | 94 | C9 | 41 | ▌? ╕)₧↕╨ö╔A |
| 0000000576 | 90 | B5 | 33 | B4 | 81 | CC | 17 | 39 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | É╡3┤ü╠↨9☻ |
| 0000000592 | 80 | 00 | 00 | 00 | 80 | 00 | 00 | 00 | 1F | 6A | 7C | 56 | 00 | 00 | 00 | 00 | Ç Ç ▼j\|V |
| 0000000608 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000624 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000640 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000656 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000672 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000688 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000704 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000720 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000736 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000752 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000768 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000784 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000800 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000816 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000832 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000848 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000864 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000880 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000896 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000912 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000928 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000944 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |

23. Reference back to *Task 8*, *Step 5*. When analyzing the */dev/sdc* disk with *gdisk*, the GUID printed is: *129E29BB-94D0-41C9-90B5-33B481CC1739*.

When converting the *GUID* value to hex, it is printed as: *BB 29 9E 12 D0 94 C9 41* ***90 B5 33 B4 81 CC 17 39***. Notice the last 8 bytes match with ***90 B5 33 B4 81 CC 17 39***.

To match the first 8 bytes of the GUID, the first 4 bytes of the 8 bytes need to be reversed and the second 4 bytes of the first 8 bytes require each 2-byte block to be reversed, as shown below:

First 8 bytes in Hex: *BB 29 9E 12 D0 94 C9 41*

*First 4 bytes (reverse the 4 bytes):*
BB 29 9E 12 = 12 9E 29 BB

Second 4 bytes (reverse each 2-byte block):
D0 94 C9 41 =

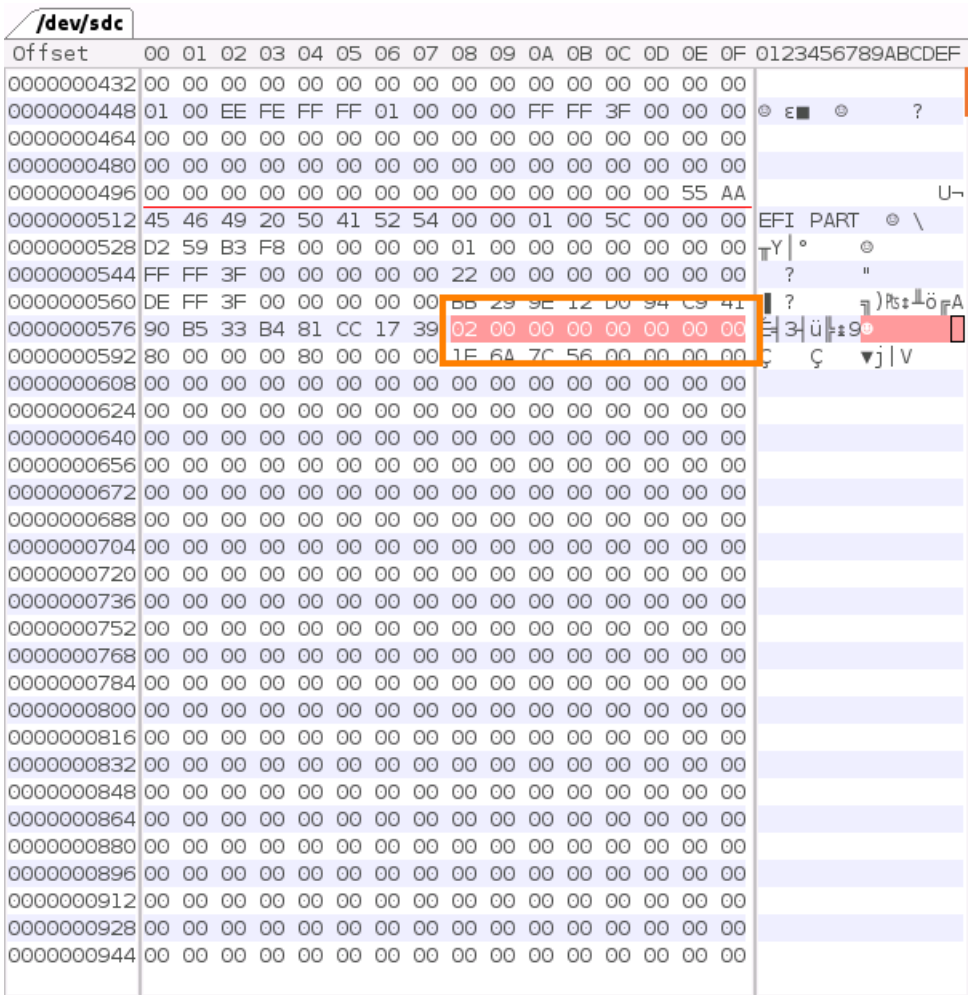
D0 94 = 94 D0
C9 41 = 41 C9

= 94 D0 41 C9

First 8 bytes in GUID: *129E29BB-94D0-41C9*

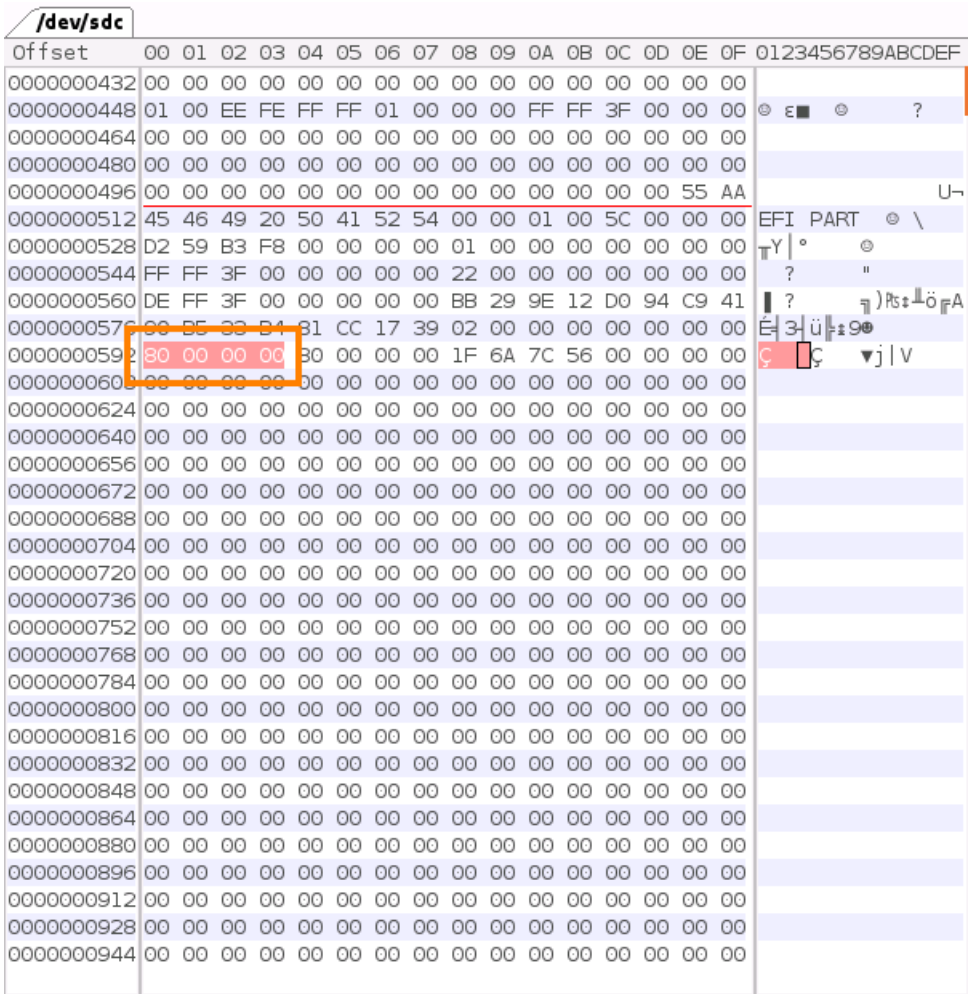
24. Focusing on *wxHexEditor*, the next 8 bytes are reserved for the partition entries starting *LBA*, which is always 2.




When converting to Little Endian; take the original hex, *02 00 00 00 00 00 00 00*, and convert to *00 00 00 00 00 00 02,* which equals 2 bytes in decimal.

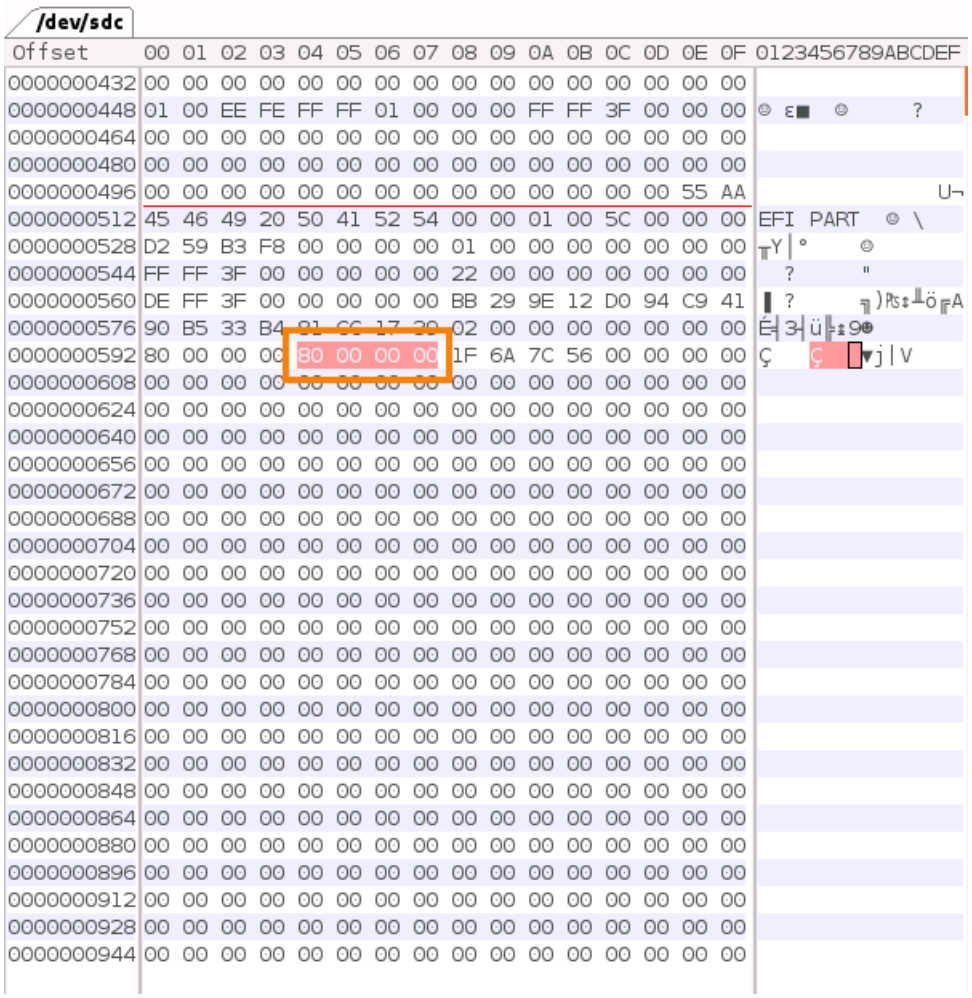
25. Notice, the next 4 bytes show the number of partition entries.




When converting to Little Endian; take the original hex, *80 00 00 00*, and convert to *00 00 00 80,* which equals 80 bytes in decimal. In return, that equals 128 partitions.

26. The next 4 bytes is the size of a partition entry.



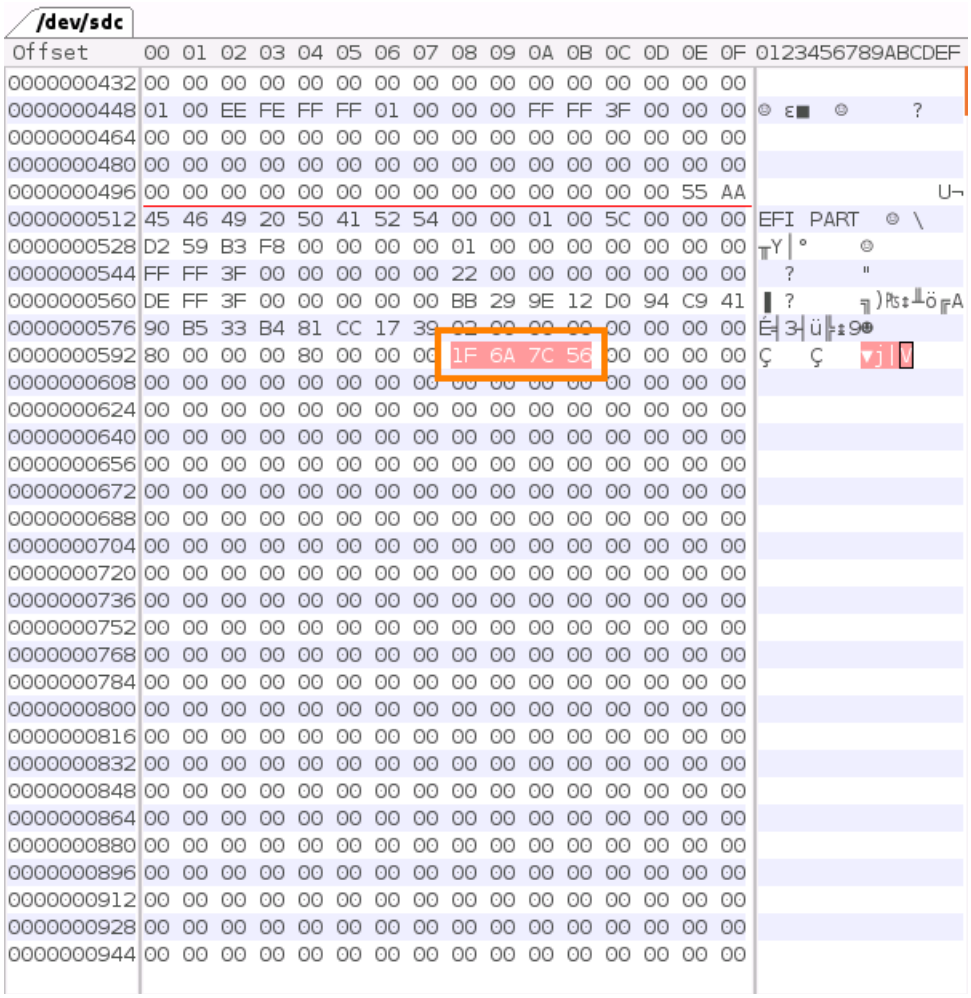
/dev/sdc

| Offset | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000000432 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000448 | 01 | 00 | EE | FE | FF | FF | 01 | 00 | 00 | 00 | FF | FF | 3F | 00 | 00 | 00 | ☺ ε■ ☺ ? |
| 0000000464 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000480 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000496 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 55 | AA | U¬ |
| 0000000512 | 45 | 46 | 49 | 20 | 50 | 41 | 52 | 54 | 00 | 00 | 01 | 00 | 5C | 00 | 00 | 00 | EFI PART ☺ \ |
| 0000000528 | D2 | 59 | B3 | F8 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ╥Y│° ☺ |
| 0000000544 | FF | FF | 3F | 00 | 00 | 00 | 00 | 00 | 22 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ? " |
| 0000000560 | DE | FF | 3F | 00 | 00 | 00 | 00 | 00 | BB | 29 | 9E | 12 | D0 | 94 | C9 | 41 | ▌? ╗)₧↕╨ö╔A |
| 0000000576 | 90 | B5 | 33 | B4 | 81 | CC | 17 | 39 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | É╡3┤ü╠↨9☻ |
| 0000000592 | 80 | 00 | 00 | 00 | 80 | 00 | 00 | 00 | 1F | 6A | 7C | 56 | 00 | 00 | 00 | 00 | Ç Ç ▼j\|V |
| 0000000608 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000624 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000640 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000656 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000672 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000688 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000704 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000720 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000736 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000752 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000768 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000784 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000800 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000816 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000832 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000848 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000864 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000880 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000896 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000912 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000928 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 0000000944 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |

When converting to Little Endian; take the original hex, *80 00 00 00*, and convert to *00 00 00 80,* which equals 80 bytes in decimal. Which again, in return, equals 128 partitions.

27. The *CRC32* of the partition array is the next 4 bytes shown.



28. The rest are reserves and must be zero.


29. Close all **PC Viewers** and end the reservation to complete the lab.