Partition Recovery course

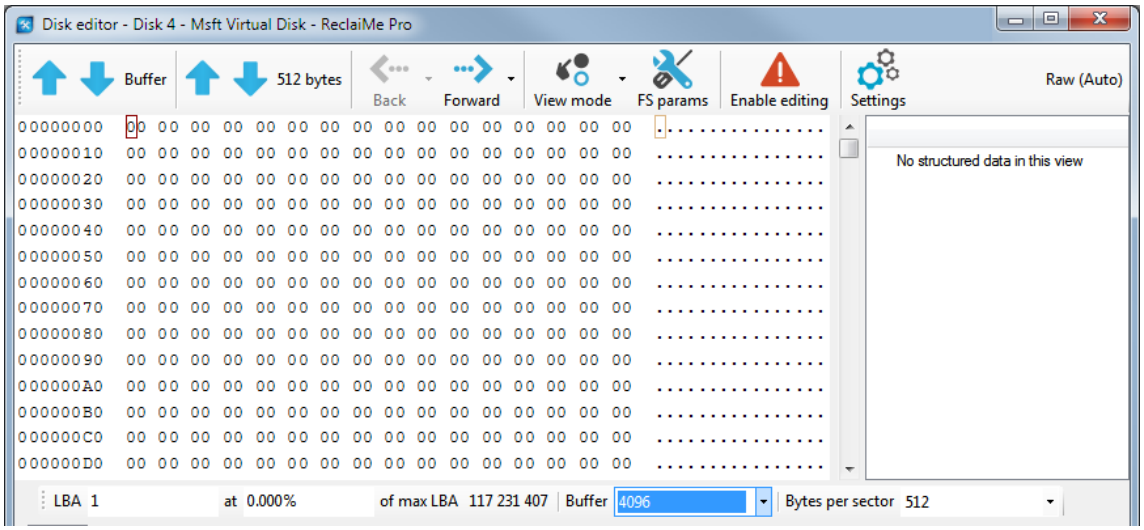
Lesson 3 - GPT partitioning scheme

Practice part

Task – GPT partition recovery

First open Disk Management and attach a VHD file (*Action -> Attach VHD*). Note that you should not set a *Read-only* flag for the VHD file because we are going to edit it. You should get the following:

We see that Disk Management does not see partitions on the disk. Launch ReclaiMe Pro, select our disk (Msft Virtual Disk) and click *Disk editor*. First, we see a protective MBR located in the sector 0. Move on to the next sector (downward arrow next to *512 bytes*) where GPT header has to be. Surprisingly, there's nothing there.



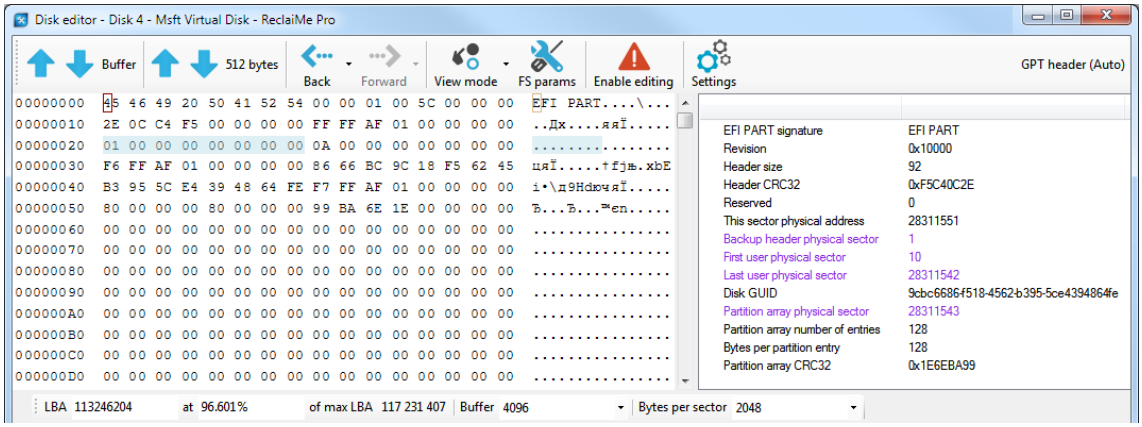
We can conclude that either GPT has been damaged to such an extent that there are no traces of it at all, or it is located somewhere else, and therefore the sector size of 512 bytes must be incorrect. There are two ways to find GPT header:

- Move through the disk to larger LBAs using the downward arrow (*512 bytes*). It is the simplest way since GPT is located in the first physical sector.
- Use the search function of ReclaiMe Pro at the bottom of the *Disk editor* window (*Object -> GPT header*). However, we should note that we do not recommend this option since it is always useful to look at the actual data during the recovery (in this case, just scrolling down the sectors).

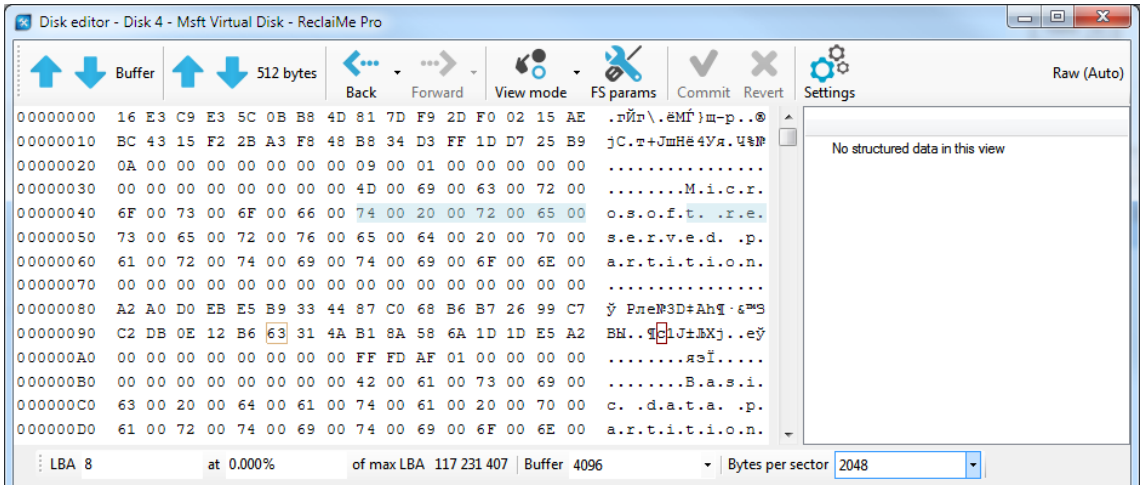
Moving through the disk, we have found GPT header at LBA 4; therefore, the size of physical sector on this disk is $4 * 512 = 2048$ bytes. Often, confusion occurs with LBA and physical sectors. It is needed always to follow through what sector size you work with. We use "sector" when we mean a physical sector size (whatever size it has) and LBA to designate a 512-byte sector (regardless of the physical sector size). Such confusion often occurs when one works with disk image files which do not store information about physical sector size.

ReclaiMe Pro disk editor uses physical sectors to move around the disk (double click on violet values), so to get the correct links you need to set the correct sector size (in our case 2048 bytes) in the *Bytes per sector* field. Otherwise, all values displayed in physical sectors should be multiplied by 4.

Then we need to check a sector with a backup header. Click *Backup header physical sector* and confirm that it looks OK.

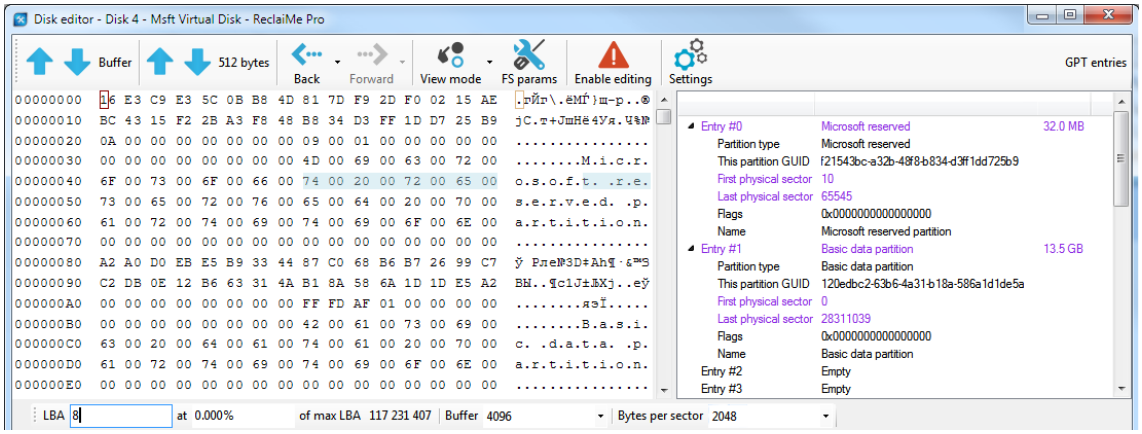


Then move on to the *Partition array physical sector*. Although we see some data on the left, it still seems that there is a problem because no data is shown on the right in structured view.



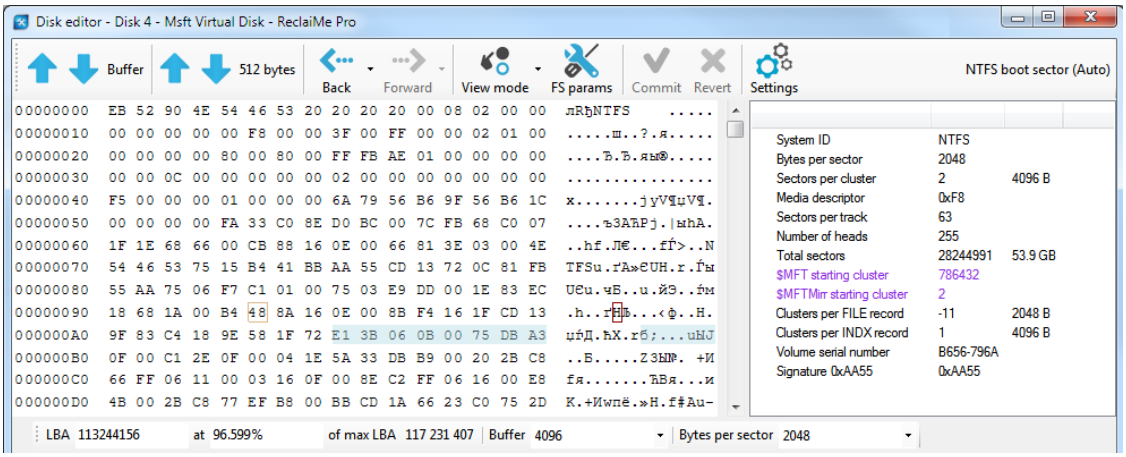
The failure of the automatic view mode recognition is often the first hint of something fishy. If the data is good enough, the automatic recognition works properly.

To understand what is wrong we need to switch from the automatic mode to manual. To do this click *View mode -> Partition tables -> GPT entries*. Partition types look correct; however, in *Basic data partition* we see that *First physical sector* is 0 meaning that the first (Microsoft reserved) partition is located inside the second (Basic data) partition.



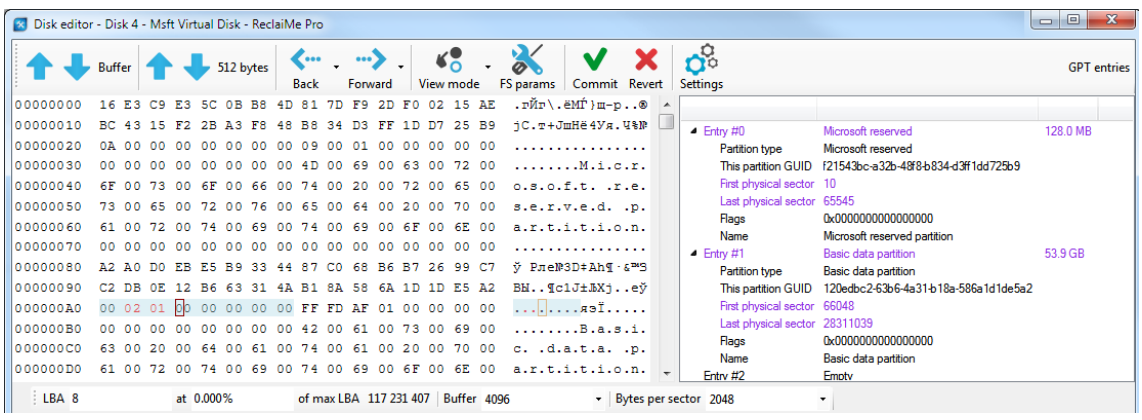
This can not be. Therefore, we should correct *First physical sector* value for the *Basic data partition.*

To determine the value we need to subtract the partition size from *Last physical sector.* To know the partition size you need to double click *Last physical sector* and then switch from the manual mode back to the automatic. This brings us to the backup NTFS boot sector where we see that number of sectors in the partition equals 28 244 991.



28 311 039 – 28 244 991 = 66 048 (our first physical sector). Now convert the calculated value to the hexadecimal value: 66 048 = 0x10200 and then return to the GPT entries (*Back -> 8 as GPT entries*), click *First physical sector*, then *Enable editing*, make the correction, and click *Commit*. Since GPT uses so called *little endian* number encoding, the value should be written starting from the rightmost byte to the left, that is 00 02 01 00.

Important: Before you start editing the value, check once again that you are going to edit *First physical sector* field rather than something else.



Now we need to make sure that we did everything right and corrected what we had to correct. The first thing that comes to mind is to go to Disk Management and hope to see the partition on the analyzed disk. However, this will not work since the sector size in this VHD file does not correspond to the actual sector size. To make sure that we have complete the task correctly we should launch ReclaiMe Pro once again and specify GPT in the *Disk and image scan options* window. Once ReclaiMe Pro scanned the devices, it has detected a partition on the analyzed disk. Select the partition and click *Start scan*. Just a couple of seconds later, click the NTFS folder and see our text file.

It should be noted that there are another ways to solve the task:

- Look for the correct value of *First physical sector* in the backup copy of GPT entries, which is located in the end of the disk just before the backup copy of GPT header.
- Instead of going to the backup NTFS boot sector, find the main NTFS boot sector using the automatic search function of ReclaiMe Pro and then do the same calculations.

Conclusion

We have determined the sector size – 2048 bytes and found the error in GPT entries: incorrect *First physical sector* value for the data partition. Then, on the fixed partition, we were able to do file recovery and see the file. As for explanation why file recovery was needed to get access to the file, this is because Windows believes that the sector size used in a VHD file is 512 bytes while in this case this is not true; that's why it is impossible to mount the partition in Windows.