Alexander Rhone

COMP 597 – Computer Forensics

Assignment #2

**Introduction:**

Two images were received in a .dd format. The first image was provided with the goal of finding the number of partitions and the second image was provided with the goal of finding hidden data within the image. The analysis of the images was done by using the tools WxHexEditor, FTK Imager, mmls, fdisk, and Encase Imager. WxHexEditor is a hex editor with the ability to view the image bytes and the hex bytes converted to ASCII characters. FTK Imager is a volume analysis tool that can be used to convert images to different formats and also to view the partitons of the image and the files that make up the partition. Encase Imager also allows you to view the partitions of the image and the files in the partitions. mmls and fdisk are tools that show how many partitions and the number of sectors that make up each partition.

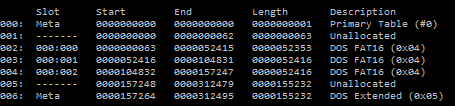
**Image One:**

**Type of Partition:**

The image file was determined to be DOS. This was determined by looking at the image in WxHexEditor. The partition table starts in the first sector which means that the image must be DOS. The first sector also ends with a 55 AA signature or how partition entries in DOS are finished.

**Sectors:**

The image was run through WxHexEditor again to determine the size of the image in sectors. This was determined by finding the last entry in the partition table (16 bits before the signature) and determining the LBA Start and the number of sectors of the last entry. Adding the LBA start (157264) and the number of sectors(155232) together, it was determined that there were 312496 sectors. This image was also run through mmls to also verify the number of sectors. The picture below was the output of mmls.



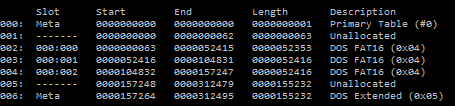
By looking at the last entry in the partition table, the number of sectors can be determined by taking the end sector and adding 1 because partition tables start at sector 0.

**Number of Partitions:**

The number of partitions were determined by using multiple programs (mmls, fdisk, FTK Imager, and Encase Imager).

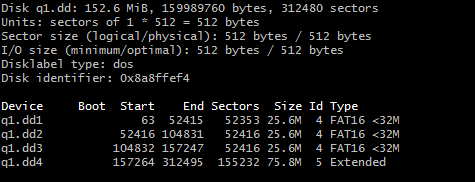
**mmls**

When the image was examined by mmls, 3 partitions and an extended partition table were found. The extended partition table seems to not have anything in it because there are no partitions that are after it. There was also some unallocated space between the 3rd partition and the extended partition table.



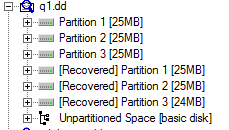
**fdisk**

When the image was examined by fdisk, 3 partitions and an extended partition table were found. The extended partition table seems to not have anything in it because there were no partitions that are after it.



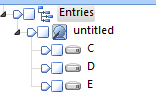
**FTK Imager**

When the image is examined by FTK Imager, 6 partitions were found. 3 of the partitions were determined to be recovered by FTK. This might mean that there were other uncovered partitions in the image.



**Encase Imager**

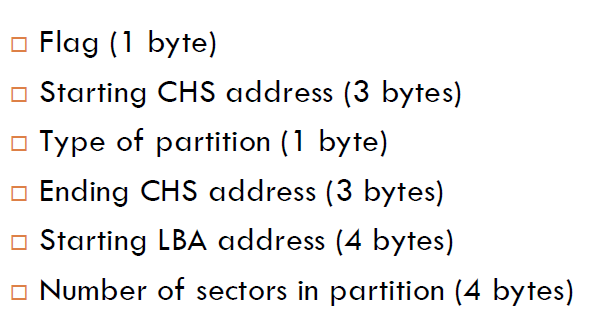
To examine the image, the image needed to be converted to a E01 file, which can be done by FTK Imager. When the image was examined by Encase Imager, 3 partitions were found.



All of the programs except for FTK Imager found 3 partitions. FTK Imager found 6 partitions and 3 of those partitions were recovered. This could mean that there are more partitions in the partition table and the partition table was changed.

**Determining partitions manually**

By using WxHexEditor, the partition table was able to be calculated manually. This was done by looking at the 4 sets of 16 bytes before the signature or 55 AA at the end of the first sector. The 16 bytes were analyzed by using the following table.

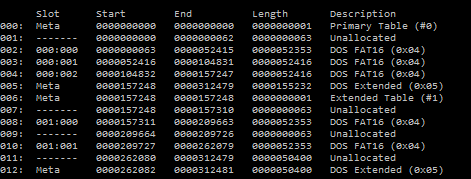


|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Partitions | Flag | Start | End | Size | Type |
| 1 | 0 | 63 |  | 52353 | 4(FAT16, 16-32 MB, CHS) |
| 2 | 0 | 52416 |  | 52416 | 4(FAT16, 16-32 MB, CHS) |
| 3 | 0 | 104832 |  | 52416 | 4(FAT16, 16-32 MB, CHS) |
| 4 | 0 | 157264 |  | 155232 | 5(Extended) |

By analyzing the partition table, it can be seen that there is an extended partition table. In the mmls image above, there are 16 bytes of unallocated space. These bytes are enough to be a partition table entry. This could be why the partition table was wrong. The hex value of the LBA address of the 4th partition entry was changed from 50 66 02 00 to 40 66 02 00 which moves the pointer to 16 bytes before. This edited image was analyzed by using the programs: mmls, fdisk, FTK Imager, Encase Imager to determine if more partitions are found.

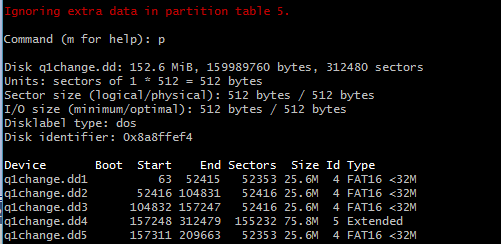
**mmls**

When the image was examined by mmls, 5 partitions and 2 extended partition tables were found. The first extended partition table is pointing to the 4th and 5th partitions found. There is another partition table that is not pointing to any other partitions.



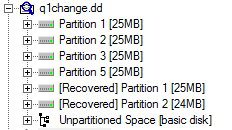
**fdisk**

When the image is examined by fdisk, 4 partitions and an extended partition table were found. The extended partition table is pointing to the 4th partition. At the top of the fdisk output, there is a line saying that the extra data in partition table 5 is ignored. This could mean that fdisk sees another partition.



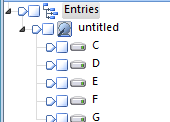
**FTK Imager**

When the image was examined by FTK Imager, 6 partitions were found. 2 of the partitions are determined to be recovered by FTK. This might mean that there are more uncovered partitions in the image.



**Encase Imager**

To examine the image, the image needed to be converted to a E01 file, which can be done by FTK Imager. When the image was examined by Encase Imager, 4 partitions were found.

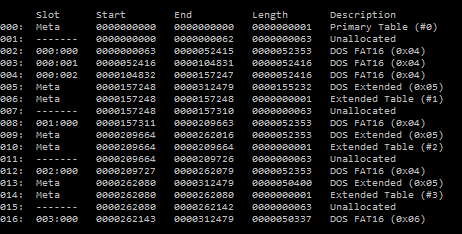


All of the programs except for FTK Imager and mmls found 4 partitions. fdisk says that it sees a 5th partition but it was not showing it in its table. FTK Imager found 6 partitions and 2 of those partitions were recovered. mmls found 5 partitions. Since there were many different amounts of partitions found, there should be atleast one more uncovered partition.

The unallocated space after the 4th non-partition table was scanned. The end of the 1st sector has a 55 AA signature. The 4 sets of 16 bytes before the signature looked like an extended partition table. If the 2nd entry of the 1st extended partition table was changed to point to the newly discovered extended partition table by changing the LBA to the number of bytes between the two extended partitions and changing the type to 05 to signify that the new entry is an extended partition table. This 2nd edited image was analyzed by using the programs: mmls, fdisk, FTK Imager, Encase Imager to determine if more partitions were found.

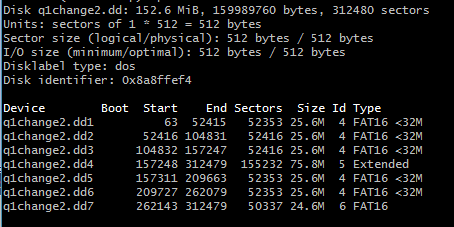
**mmls**

When the image is examined by mmls, 6 partitions and 3 extended partition tables were found. The first extended partition table is pointing to the 4th partition found, the second extended partition table is pointing to the 5th partition found, and the third extended partition table is pointing to the 6th partition found.



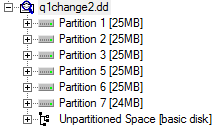
**fdisk**

When the image is examined by fdisk, 6 partitions and an extended partition table were found. The extended partition table is pointing to the last 3 partitions.



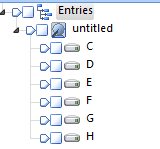
**FTK Imager**

When the image is examined by FTK Imager, 6 partitions were found.



**Encase Imager**

To examine the image, the image needs to be converted to a E01 file, which can be done by FTK Imager. When the image is examined by Encase Imager, 6 partitions were found.



All of the programs see 6 partitions, and FTK does not see any more recovered partitions. This evidence leads to the conclusion that there are no more undiscovered partitions.

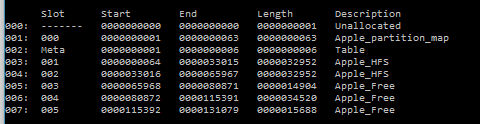
**Image Two:**

**Type of Partition:**

The image file was determined to be Apple. This was determined by looking at the image in WxHexEditor. The partition table starts in the second sector which means that the image might be GPT or Apple. The second sector begins with 50 4D which leads to the conclusion that this image is Apple. Also, when the hex is converted to ASCII, the partitions have Apple in them.

**Sectors:**

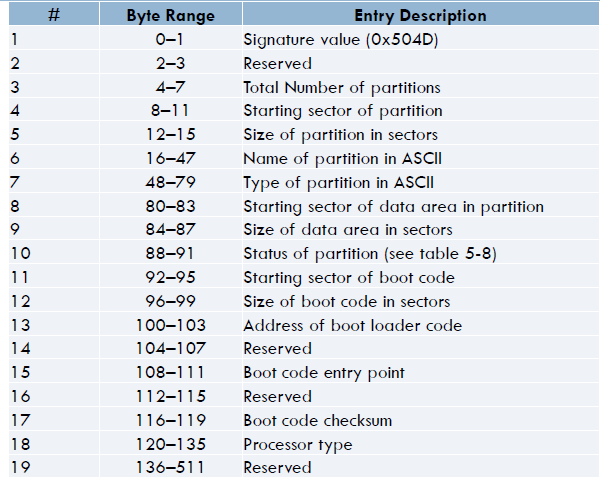
The image was run through WxHexEditor again to determine the size of the image in sectors. This was determined by looking through the first few sectors and finding the last entry in the partition table. This is possible with Apple because Apple keeps all of their partition table entries at the beginning of their hard disks while DOS has extended tables. The last partition entry starts at sector 115,392 and has a size of 15,688 sectors. This image was also run through mmls to also verify the number of sectors. The picture below is the output of mmls.



By looking at the last entry in the partition table, the number of sectors can be determined by taking the end sector and adding 1 because partition tables start at sector 0.

**Determining partitions manually**

By using WxHexEditor, the partition table is able to be calculated manually. This was done by looking at each of the sectors after the 1st sector to determine their information. The information gather was determined from the table below.



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | # of partitions | Starting sector of partition | Ending Sector of partition | Size (sectors) | Starting sector of data area | Size of data area | Type |
| 1 | 6 | 1 |  | 63 | 0 | 63 | Apple\_partition\_map |
| 2 | 6 | 64 |  | 32,952 | 0 | 32,952 | Apple\_HFS |
| 3 | 6 | 33,016 |  | 32,952 | 0 | 32,952 | Apple\_HFS |
| 4 | 6 | 65,968 |  | 14,904 | 0 | 14,904 | Apple\_Free |
| 5 | 6 | 80,872 |  | 34,520 | 0 | 34,520 | Apple\_Free |
| 6 | 6 | 115,392 |  | 15,688 | 0 | 15,688 | Apple\_Free |

By analyzing the partition table, it can be determined that there are 6 partitions including the partition map. The partitions are of type, Apple\_partition\_map, Apple\_HFS, and Apple\_Free. Apple\_Free partitions are excellent places to hid information.

**Hidden Information:**

There were 3 different types of hidden information found, 2 passwords, a story by Dr. Seuss, and one of the Apple\_Free partitions was actually a different type of partition. The Dr. Seuss book was found by scanning through the Apple\_Free partitions in WxHexEditor and in the 1st Apple\_Free partition, there was a Dr. Seuss book in the converted hex to ASCII. This lead to the conclusion that there might be more information in the ASCII. The ASCII characters were scanned using the find tool in WxHexEditor for keywords such as: email, name, password, etc. There were two passwords found this way. They were therearemore and goodbye.

The image was also scanned by using FTK Imager. The 2nd Apple\_Free partition was determined to be not an Apple\_Free partition but actually a different type of partition. This was determined because FTK knew what type of OS the partition is and Apple\_Free partitions are supposed to be free space. This partition had some image files in it. The ASCII was also able to be scanned by using FTK and the passwords and book were found as well.

The image was scanned by using Encase Imager. Encase also saw that the one Apple\_Free partition actually had an OS in it but you could not scan the ASCII to find the passwords and the book.

**Conclusion:**

In conclusion, there were two errors in the partition table of the 1st image. The first error was the main partition table did not point to the first partition table. The second error was the first partition table did not point to the second partition table. There were 4 hidden things in the 2nd image. There were two hidden passwords and a hidden book in the ASCII. There was also a mistyped partition, the partition was typed Apple\_Free when it should have been something else.