Alexander Rhone

COMP 597 – Computer Forensics

Assignment #3

The first image was run through fsstat with the command fsstat Q1.E01. This gave a lot of information. The pertinent information found was the file system was a FAT16, the volume label was NONAME, the cluster size was 32768, the size of the sectors was 512, and there was no backup for the boot sector. The backup was determined because fsstat gave no information for the boot sector, so it was assumed that no back up was present.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Boot Sector (Sector 0) | Sector 1 | FAT 0 (Sectors 2-240) | FAT 1 (Sectors 241-479) | Root Directory (Sectors 480-511) | Cluster Area (Sectors 512 – 3913343) |

Reserved (Sectors 0-1)

Data Area (Sectors 480 – 3913343)

The largest file in the image was determined using fsstat with the command fsstat Q1.E01. The files were searched for the largest cluster/most number of sectors. The starting sector was found to be 50048 with size of 22464 sectors. This sector was run through ifind to determine the inode number of the sector. The command was ifind -d 50048 Q1.E01 and the inode was found to be 751135. This inode was run through istat using istat Q1.E01 751135 and the file name was determine to be boulfrt.bmp and its size was 11493054 bytes.

The 2nd largest file in the image was determined using fsstat with the command fsstat Q1.E01. The files were searched for the 2nd largest cluster/most number of sectors. The starting sector was found to be 216768 with size of 7232 sectors. This sector was run through ifind to determine the inode number of the sector. The command was ifind -d 216768 Q1.E01 and the inode was found to be 3310092. This inode was run through istat using istat Q1.E01 3310092 and the file name was determine to be start.pdf and its size was 3698892 bytes.

Hidden information was present on the image. Some hidden information is sometimes in the deleted files. The deleted files was found by using the command fls -rdF Q1.E01. The deleted files contents were recovered using the command icat -r Q1.E01 inode. The deleted files and their contents are in the table below.

|  |  |  |
| --- | --- | --- |
| File Name | Sector Number | Contents |
| CompArch 2011/forms/index\_files/\_/\_.txt | 3876357 | eA |
| CompArch 2011/forms/index\_files/\_/\_.txt | 3876358 | bB |
| CompArch 2011/forms/index\_files/\_/\_.txt | 3876359 | C |
| CompArch 2011/wcop/\_h.txt | 1878544 | delete:  - cache  - temp files  - bookmarks  - history |
| WICSA 2011/index/\_d.txt | 3226119 | Things to do:  - get money from qwt@543  - go to bank  - use wireshark on:  \* |
| \_aswd.txt | 7 | htmail: sdh\_56#rt  g: theLink21  edu: 345ThreeFourFive |
| \_wd24.txt | 8 | mc: 4326443200232230  ed:0821  2222 |
| \_crt.txt | 9 | contact:71771771777 |

The \_aswd.txt file could contain passwords and an email address. The \_wd24.txt file looks like it contains some sort of pin and a credit card number. The \_crt.txt file specifically says contact followed by a phone number like string of numbers. The WICSA 2011/index/\_d.txt file specifically has directions to do. The CompArch 2011/wcop/\_h.txt file contains information to delete from the device.

Some other files were found by searching the slack space. The slack space was found using the command blkls -s Q1.E01 > slack.data. Some file extensions were searched for in the slack space for some deleted files/files that were saved over. The file extensions searched for were html, pdf, and txt. While searching for html, css file extensions, an index file was found, and 6 html documents were found. When searching for txt, a README file and 2 txt documents were found. One pdf document was found when searching for pdf extensions.

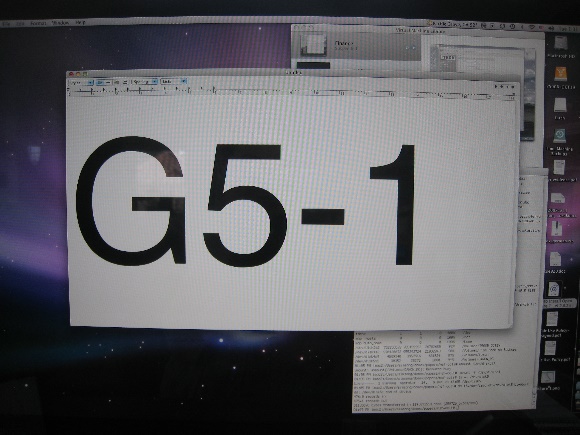
The unallocated space of the image was extracted and routed to the file unalloc.data using the command blkls -A Q1.E01 > unalloc.data.

The slack space of the image was extracted and routed to the file slack.data using the command Blkls -s Q1.E01 > slack.data.

The second image was run through fsstat with the command fsstat -o51 Q2.E01. The -o51 means with an offset of 51 sectors. This gave a lot of information. The pertinent information found was the file system was a FAT16, the volume label was CANON\_DC, the cluster size was 16384, and the size of the sectors was 512.

All of the files names, sizes, start sector, end sector, whether they were fragmented, and if they were the fragments that are after them. The following table shows the information that was found. The information was found from using the commands fsstat -o51 Q2.E01, ifind -d sectornumber Q2.E01, and then istat -o51 Q2.E01 inode.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| File Name | File Size | Starting Sector | Ending Sector | Fragmented? |
| DCIM | 16384 | 45 | 76 |  |
| 100CANON | 16384 | 77 | 108 |  |
| IMG\_0042.JPG | 1361807 | 237 | 2924 |  |
| M0100.CTG | 164 | 2957 | 2988 |  |
| IMG\_0043.JPG | 2834018 | 2989 | 3532 | Y - 5197 |
| IMG\_0003.JPG | 840101 | 3533 | 5196 |  |
| IMG\_0043.JPG | 2834018 | 5197 | 8076 | Y - 8557 |
| IMG\_0038.JPG | 1296150 | 8077 | 8556 | Y - 14925 |
| IMG\_0043.JPG | 2831018 | 8557 | 10092 | Y - 11789 |
| IMG\_0007.JPG | 865313 | 10093 | 11788 |  |
| IMG\_0043.JPG | 2831018 | 11789 | 12364 |  |
| IMG\_0009.JPG | 840692 | 13261 | 14924 |  |
| IMG\_0038.JPG | 1296150 | 14925 | 16620 | Y - 23149 |
| IMG\_0011.JPG | 771052 | 16621 | 18156 |  |
| IMG\_0013.JPG | 842160 | 19757 | 21420 |  |
| IMG\_0038.JPG | 1296150 | 23149 | 23532 |  |
| IMG\_0016.JPG | 853839 | 24781 | 26476 |  |
| IMG\_0017.JPG | 795574 | 26477 | 28044 |  |
| IMG\_0018.JPG | 784455 | 28045 | 29580 |  |
| IMG\_0019.JPG | 864257 | 29581 | 31276 |  |
| IMG\_0021.JPG | 819599 | 33005 | 34636 |  |
| IMG\_0022.JPG | 728696 | 34637 | 36076 |  |
| IMG\_0023.JPG | 858798 | 36077 | 37772 |  |
| IMG\_0024.JPG | 838434 | 37773 | 39436 |  |
| IMG\_0026.JPG | 768385 | 41005 | 42508 |  |
| IMG\_0027.JPG | 840253 | 42509 | 44172 |  |
| IMG\_0028.JPG | 815636 | 44173 | 45772 |  |
| IMG\_0029.JPG | 861552 | 45773 | 47468 |  |
| IMG\_0041.JPG | 1315993 | 48685 | 49164 | Y - 55629 |
| IMG\_0031.JPG | 749202 | 49165 | 50636 |  |
| IMG\_0032.JPG | 879834 | 50637 | 52364 |  |
| IMG\_0033.JPG | 845375 | 52365 | 54028 |  |
| IMG\_0034.JPG | 812465 | 54029 | 55628 |  |
| IMG\_0041.JPG | 1315993 | 55629 | 57260 | Y – 59021 |
| IMG\_0036.JPG | 882337 | 57261 | 58988 |  |
| CANONMSC | 16384 | 58989 | 59020 |  |
| IMG\_0041.JPG | 1315993 | 59021 | 59500 |  |

The file starting at sector 2989 was extracted using the commands blkcat -o51 Q2.E01 2989 544 > a.data, blkcat -o51 Q2.E01 5197 2880 > b.data, blkcat -o51 Q2.E01 8557 1536 > c.data, and blkcat -o51 Q2.E01 11789 576 > d.data. The data files were concatenated together using the UNIX command cat. The full command was cat a.data b.data c.data d.data > answer.JPG. The file discovered was: 

All of the deleted files were found using the command fls -rd -o51 Q2.E01. The r stands for recursively, which goes through all the directories. The d means deleted so fls finds all the deleted files.

The deleted files are DCIM/100CANON/\_MG\_0037.JPG, DCIM/100CANON/\_MG\_0006.JPG, DCIM/100CANON/\_MG\_0008.JPG, DCIM/100CANON/\_MG\_0012.JPG, DCIM/100CANON/\_MG\_0014.JPG, DCIM/100CANON/\_MG\_0039.JPG, DCIM/100CANON/\_MG\_0040.JPG, DCIM/100CANON/\_MG\_0025.JPG, DCIM/100CANON/\_MG\_0030.JPG, and DCIM/100CANON/\_MG\_0035.JPG.

4 of the deleted files were able to be recovered using icat -o51 Q2.E01 inode#. The four able to be recovered were DCIM/100CANON/\_MG\_0012.JPG, DCIM/100CANON/\_MG\_0014.JPG, DCIM/100CANON/\_MG\_0039.JPG, and DCIM/100CANON/\_MG\_0040.JPG. The rest of the files were not able to be recovered because their contents were overwritten with another file.

The four recovered files are:

