Joe and Jimmy Jungle Forensic

From the image file

0x03 OME: MSDOS5.0

0x0b byte/sector: 512

0x0d sectors/cluster: 1

0x0e reserve area size in sector: 1

0x10 number of FAT: 2

0x11 max number of files in root directory: 224 (probably FAT12 cause FAT16 is 512)

Size of root directory = 224 \* 32 / 512 = 14 sectors

So cluster 2 starts at 1 + 9 + 9 + 14 = 33 sector

0x13 number of sectors in file system: 2880 = 1.4 MB

0x15 media type 0xf0: removable

0x16 FAT size in sectors: 9

0x27 volume serial number: 0xcfcdb1c4

0x2b volume label: NO NAME

0x36 file system type: FAT12

Since this is FAT12, the root directory should be after the 2 FAT tables. And since reserve area is 1 sector, FAT 9 sector, I’ll need to jump to 19 sectors to get to the root directory.

dd if=./image bs=512 skip=19 | xxd | more

After investigating the root directory, I found total 9 entries.

First 3 is for file jimmy jungle.doc (deleted)

Cluster: 2

Size: 20480 bytes

Next 3 is coverpage.jpg in cluster

Cluster: 420

Size: 15585 bytes

Last 3 is scheduled visit.exe

Cluster: 73

Size: 1000 bytes

Jimmy jungle.doc

Since jimmy jungle.doc was deleted, and the FAT entry for cluster 2 was cleared, one of the methods of recovering the file in (Carrier, 2005) was to calculate the starting sector of the cluster and pull out that cluster and its immediates that will fit the size of the file.

Since cluster 2 is really the first cluster in data area, I’ll need to add the reserve area, 2 FAT, and the root directory inorder to reach it. According to the file system data; reserve area is 1 sector and each FAT is 9. Since the max root directory entry is 224, each entry is 32 bytes; the size of the root directory is 224 \* 32 / 512 = 14 sectors. So cluster 2 must be 1 + 9 + 9 + 14 = 33 sectors away. And since the cluster size is 512 bytes, and the jimmy jungle.doc file is 20480 bytes, I’ll need to pull out 20480 / 512 = 40 sectors. To recover the file I’ll use the following dd command.

dd if=./image bs=512 skip=33 count=40 > jungle.doc

The content was from Joe to Jimmy Jungle at 626 Jungle Ave Apt 2 Jungle, NY 11111.

Saying Jimmy’s weed made high times magazine, and he is a grower. I ran the .doc file through exiftool, and found that the file was created with MS Word 10.0. According to Wyatt (2008), that is a Microsoft Word 2002. He also emailed Jimmy his selling schedule for comments, and the file is encrypted with the same password

Scheduled visit.exe

Since this file is not deleted, I’ll traverse the FAT table by looking for cluster 73. With the help of CIS-24, I was able to build the FAT12 chain with the following equation FAT Entry \* 1.5 = offset into table. And swap the 12 bit little-endian bytes i.e. 0x123456 = 0x412 0x562

FAT entry 73 -> 0x04a = 74

FAT entry 74 -> 0x04b = 75

FAT entry 75 -> 0x04c = 76

FAT entry 76 -> 0x04d = 77

FAT entry 77 -> 0xfff = EOF

Since this file is allocated contiguously, all I have to do is find the starting sector and pull out the 5 sectors. Before extracting the file, I looked at the file signature and found that it matched Zip file signature from Kessler (2016), and the name of file is really Scheduled Visits.xls.

dd if=./image bs=512 skip=104 count=5 > schedule.zip

After trying to unzip the file, I get a prompt for a password, however currently I have no idea what it is. I tried some easy random password, but no luck. However, after re-read the .doc file, I assume there might be some old files or trace I can look for some password. So, I ran Strings on the image file, and close to the end, I found a strange string of “pw=goodtimes”, which was really the correct password

The xls file had a schedule for Apr, May and Jun 2002, including what day and which school Joe will be selling the weed. After looking closer, there is a pattern in his visits. He’ll be selling weed from Mon to Fri, and rotating those days starting from Smith, key, Leetch, Birard, Richter, Hull High School, and revisit the schools in the same order.

I ran the .xls file through exiftool, and found that the file still had the original modify time of May 23, 2002 11:20:48 and inode change time 11:20:49

Cover page.jpg

Since cover page.jpg is not marked deleted, I should be able to find the cluster chain and retrieve the image. Offset in FAT = 420 \*1.5 = 630 = 0x276. However, that offset is mark as unallocated. I decided to do signature search for a jpg using the signatures from Kessler (2016).

xxd ./image | egrep 'ffd8 ffe0'

The result was a hit at offset 0x0009200, which is the beginning of sector 73. If I convert that back to cluster I get cluster 42 = 73 + 2 – 33. I followed the cluster chain and pulled out the image with

dd if=./image bs=512 skip=73 count=31 > ./cover.jpg

The result is a complete image



I did upload the image to an online metadata viewer, but didn’t find any useful information. I ran the .jpg file through exiftool, and still didn’t find useful information other than JFIF version 1.01. I opened up the disk image in FTK and Autopsy, but still didn’t find any useful information. However, since I have found all the necessary items, and found no other entries in the FAT, I decide to wrap it up and answer the questions.

1. Joe’s supplier is at Jimmy Jungle at 626 Jungle Ave Apt 2 Jungle, NY 11111
2. The coverpage.jpg has the password to unzip the .xls file (I discover this later after the running strings on the file)
3. Joe sells pot to Smith, key, Leetch, Birard, Richter, and Hull High School in this order from Monday to Friday.
4. The .doc file was just deleted, the .xls file was compressed with password protected, password was hidden in slack space of the .jpg file, and the .jpg file entry was modified (starting cluster number)
5. Since this was a really small image, I manually traversed and extracted the files for practice.
6. This one I really have no idea of which tool was used to create it other than MS word. He probably pasted a picture in a word document then select all and save as ,jpg. However, I have no solid proof on that.

References

Wyatt (2008), Determining Word Versions of Documents

http://word.tips.net/T000601\_Determining\_Word\_Versions\_of\_Documents.html

Kessler (2016), FILE SIGNATURES TABLE

http://www.garykessler.net/library/file\_sigs.html

CIS-24, The FAT File System

http://www.c-jump.com/CIS24/Slides/FAT/lecture.html