Forensics Analysis Report

Case: Russian Tea Room

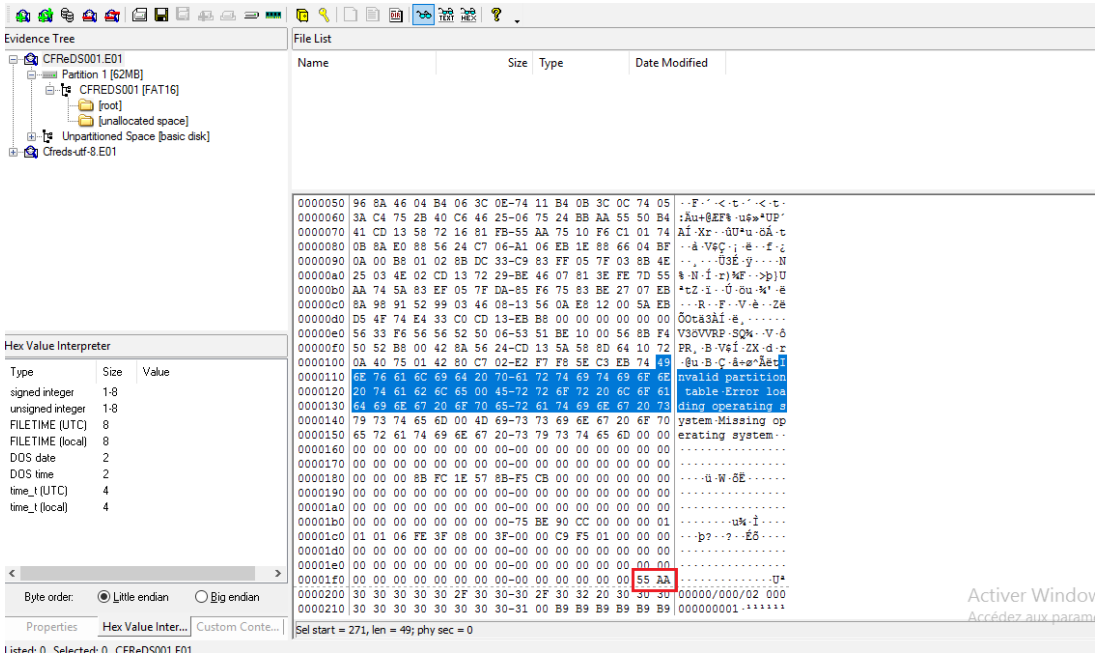
Forensics analyst: Ramy Chemak
Date: October 31st, 2020

Introduction

This report describes the followed process to solve the "Russian Tea Room" case. Not all extracted information is useful for the main task (recover the stolen menu). This is a practice, so the other forensic-related skills, such as VBR reading or MPT recovery, might be put into practice despite being pointless to the case itself. The purpose is to use the disk as learning material and practice at best possible.

1. Disk pre-analysis

I first notice that the MBR is probably broken. The data explicitly displays the error of an "Invalid partition table". The MBR sector could easily be identified as it occupies the first 512b of the disk (sector 0), ending with the signature 55 AA.



The MPT has one entry indicating the presence of only one partition. The byte 0x06 located at the offset 0x1c2 indicates that the file system we're dealing with is a FAT16

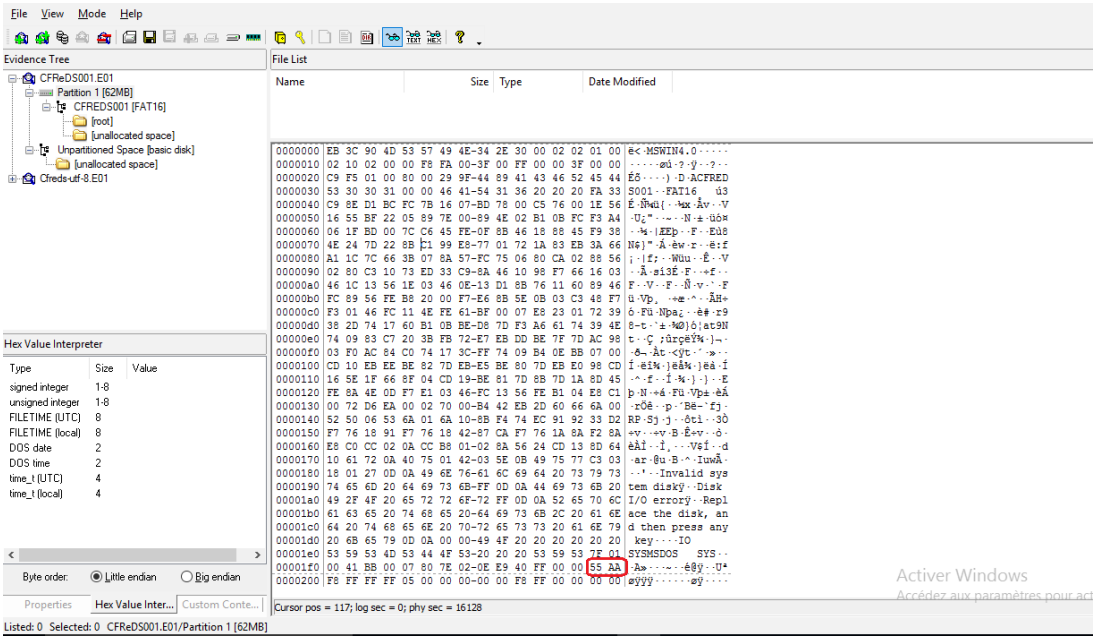
(as FTK Imager has already told). We therefore deduce the following information about the partition:

- File system: FAT16
- CHS of partition end: 540 670
- LBA of start sector: 16 128
- Partition length: 128 457 sectors

The GPT partition was overwritten with 0xB9 (like much of the disk). There isn't much to get from anyway.

While considering the main task of this case, the information we have collected about the disk should do the job. The task consists in recovering some information about a menu, probably lost somewhere in a file. The start and size of partition tells us where we should be looking, and the file system will guide us how to read, recover and carve eventual files.

We also have the volume boot record (VBR) for FAT16, from which we can extract a number of information.

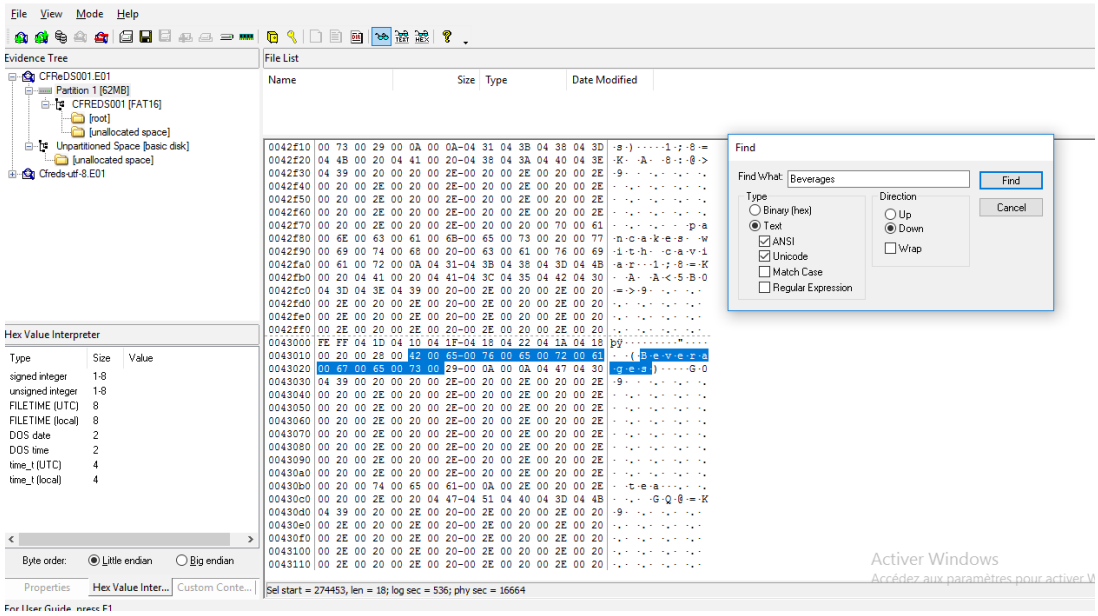


We can get the following information:

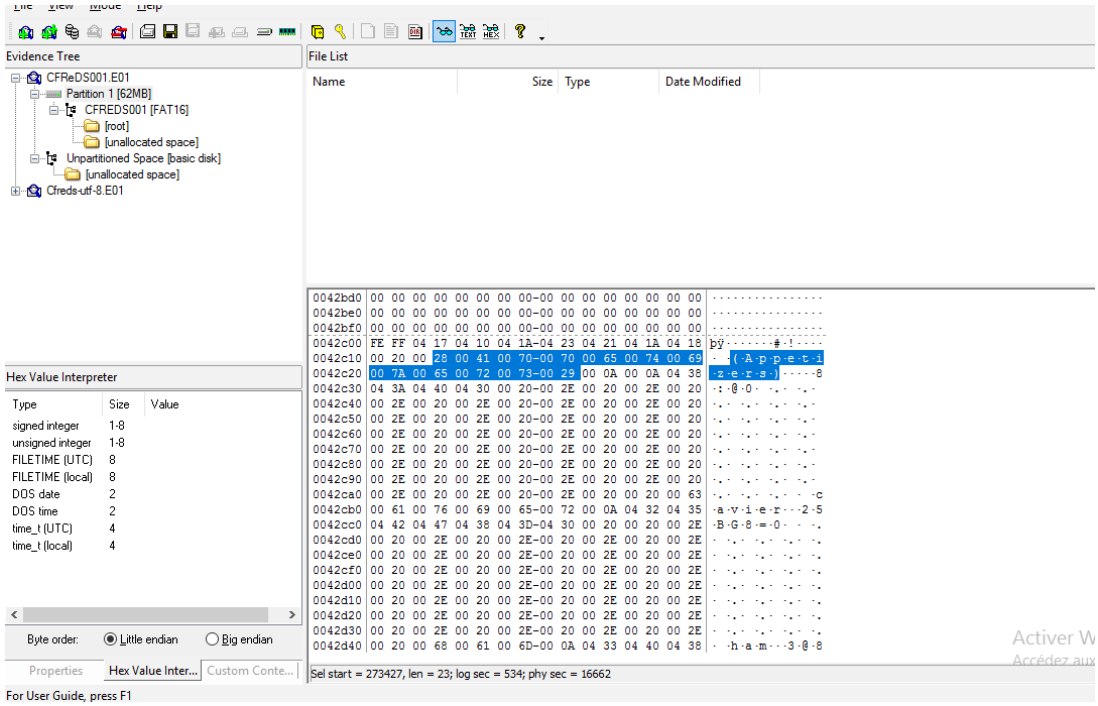
- OEM ID:
- Sector size: 512b
- N° of sectors per cluster: 2
- Volume label: CFREDS001
- File system: FAT16

2. Data recovery

I first start a simple string search. I noticed that one of the text files found the file system contains the beverages, which is one of the menu sections to recover. So I would guess that looking for the string 'Beverages' might be a good lead to find something about the rest (a corrupt file to carve for example).

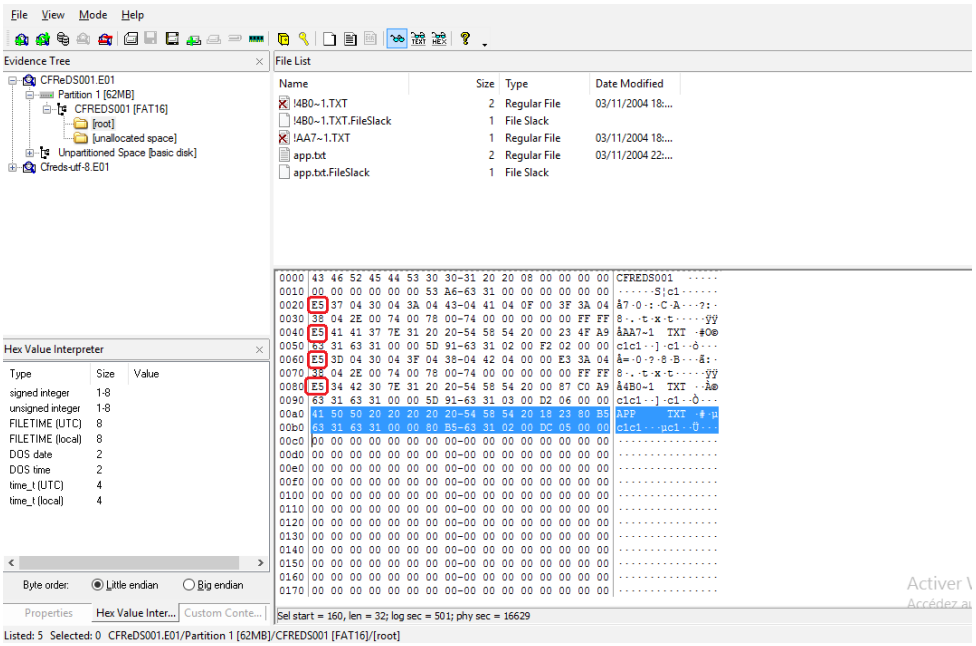


I go up until I reach the beginning of this written (cluster 16662). In short, I find what looks like the start of the 'Appetizers' section, while all (or at least a big deal) of what is preceding it is empty. According to instructions, the 'Appetizers' section is the first of menu sections to recover. So I may be looking at the right cluster.

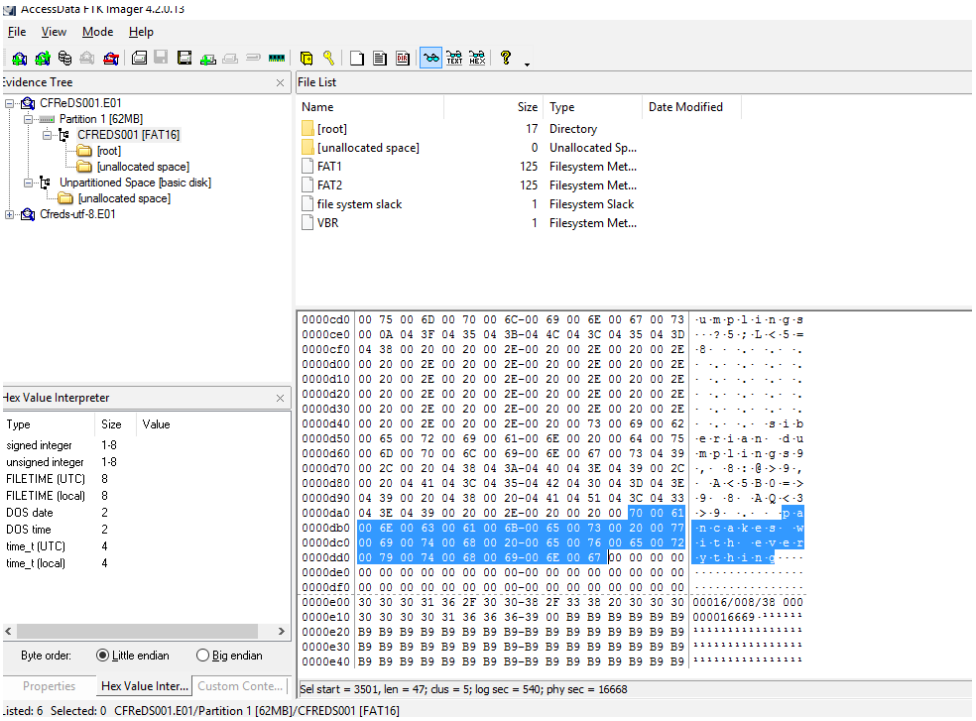


On cluster 16629, I could find several FAT16 file entries. By checking out the file attribute type (12th byte) in each record, we come to the following observations.

The first entry corresponds to the volume label, which is totally expectable. The four next entries however correspond to four deleted files, with the first byte set to 0xE5. One of them is a read-only hidden system volume and two are archive files. A last entry corresponds to an undeleted file app.txt, which has already been recovered by FTK Imager. The file contains a portion of the menu to recover.



Two of those deleted files are of size 0 while two others have some weight. So I would deduce that they might be worth looking into. Indeed, we are able to find some raw information in there, which occurs to be helpful for further data reconstruction.



I end up with some overlapping parts between sections “Pancakes” and “Meat pies and dumplings”. That’s odd and might suggest that I’ve made a mistake somewhere.

At this point, I was so far able to recover much of the stolen menu. But I still lack at least four sections, which are: “Soup”, “Meat and Fish”, “Cheese and milk products” and “Dessert”. The first partition doesn’t really provide further information. The rest of the disk is completely overwritten either by 0xB9 or just 0x00. The unpartitioned space remains so far undiscovered though. So I might be looking for a lead from there. I can’t really find anything concrete. Therefore, my last resort is the classical string search. This way, I’m able to find some lost portions of text, all over the disk, which allows me to reconstruct the rest of the stolen menu.

3. Recovered menu

Appetizers - ЗАКУСКИ

- Cavier (probably caviar) - икра
- Ham - ветчина
- Mushrooms - грибы
- Sausage - колбаса
- Herring - селёдка

Soup - СУП

- Borscht - борщ
- Cabbage soup
- Uzbek mutton soup
- Georgian mutton soup
- Fish soup
- Chicken soup

Pancakes - БЛИНЫ:

- Pancakes with caviar - блины с икрой
- Stuffed buns - блины с сметаной
- Cheese dumplings - вареники
- Siberian dumplings – пельмени
- Pancakes with everything

Meat pies and dumplings:

- Meat pie
- Stuffed buns- блины с сметаной
- Cheese dumplings- вареники
- Siberian dumplings – пельмени

Meat and fish - МЯСО И РЫБА:

- Beef stroganoff
- Steak
- Cutlets
- Roast beef
- Chicken
- Duck
- Goose
- Pheasant
- Carp
- Herring
- Salomon

Cheese and milk products - СЫР И МОЛОЧНЫЕ:

- Sour cream
- Cream
- Ewe's cheese
- Butter milk
- Fresh cheese
- Farmer's cheese

Beverages – НАПИТКИ:

- Tea – чай
  - Black - чёрный
  - With milk - с молоком
  - With lemon - с лимоном
- Iced tea - чай солодом

- Mineral water - минеральная вода
- Coffee - кофе
- Milk - молоко
- Cognac - коньяк
- Vodka - водка
- Beer - пиво
- Wine - вино

Dessert – СЛАДКОЕ:

- Ice cream
- Vanilla
- Fruit
- Chocolate
- Tart
  - With lemon - с лимоном
  - With cheese

Conclusion

This case was useful to practice, among other things, system forensics, file recoery and file carving.

Список литературы