

# Forensics Analysis Report

Case: *Russian Tea Room*

Forensics analyst: *Ramy Chemak*

Date: *October 31<sup>st</sup>, 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 screenshot displays a forensic analysis tool interface. On the left, the 'Evidence Tree' shows a hierarchy: CFReDS001.E01 > Partition 1 [62MB] > CFReDS001 [FAT16] > [root] > [unallocated space] > Unpartitioned Space [basic disk] > Creds-ut-8.E01. The 'File List' pane on the right shows a table with columns: Name, Size, Type, Date Modified. The 'Hex Value Interpreter' pane at the bottom shows a hex dump of the MBR sector (0x00000000 to 0x0000000F). The hex dump shows the signature 55 AA at the end of the sector (0x0000000F). The 'Properties' pane on the left shows the 'Hex Value Interpreter' selected. The 'Byte order' is set to 'Little endian'. The 'Sel start = 271, len = 49; phy sec = 0' is displayed at the bottom.

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Byte order: ☒ Little endian ☐ Big endian

Properties: Hex Value Inter... Custom Conte...

Sel start = 271, len = 49; phy sec = 0

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.

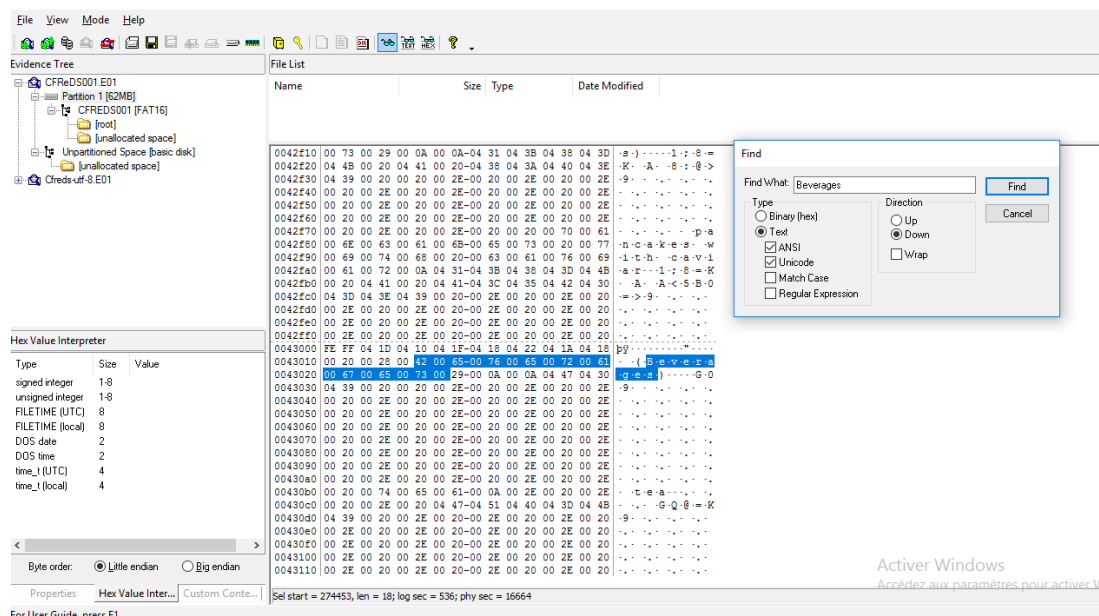
The screenshot displays the FTK Imager interface. On the left, the 'Evidence Tree' shows the loaded image 'CFReDS001.E01' and its partitions. 'Partition 1 [62MB]' is selected, showing its FAT16 file system and root directory. The 'File List' pane on the right shows the contents of the root directory, including files like 'MSWIN4.0', 'D:\ACFRED', 'S001 - FAT16', and 'Unpartitioned Space [basic disk]'. The 'Hex Value Interpreter' is open at the bottom, showing the raw data of the selected partition. The 'OEM ID' field is highlighted, showing the value 'MSWIN4.0'. The 'Sector size' is 512B, and the 'Volume label' is 'CFReDS001'. The 'File system' is 'FAT16'.

We can get the following information:

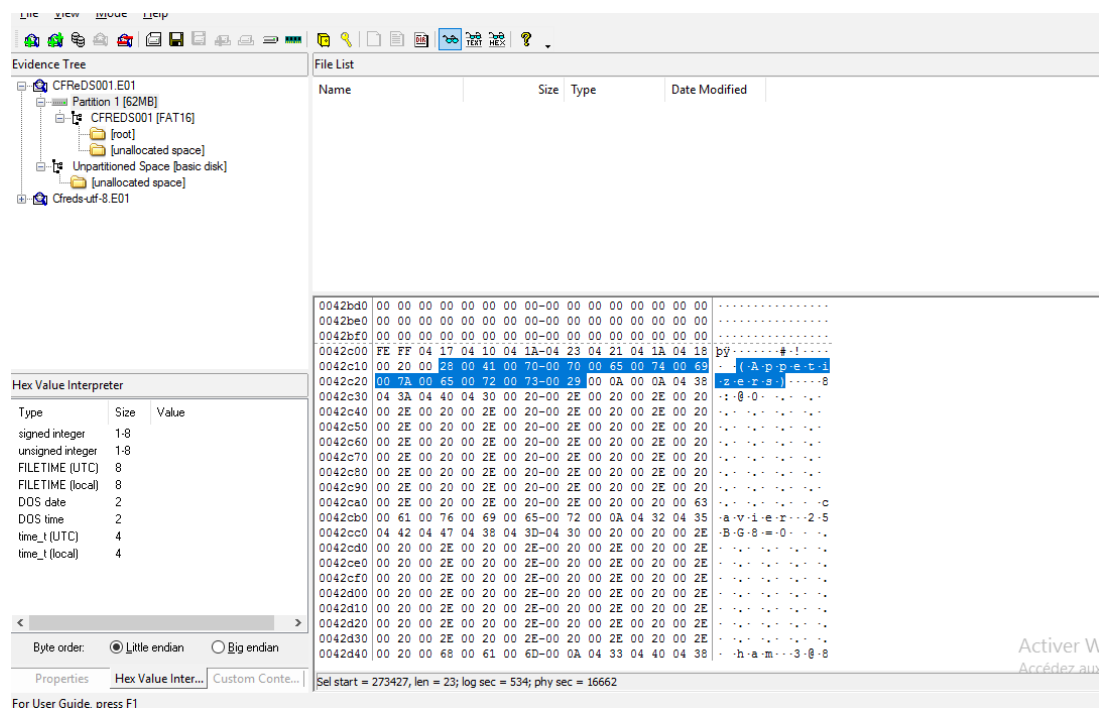
- OEM ID:
- Sector size: 512b
- N° of sectors per cluster: 2
- Volume label: CFReDS001
- File system: FAT16

## 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 (12<sup>th</sup> 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.

The screenshot shows the FTK Imager interface with the Evidence Tree on the left, listing CFReDS001.E01, Partition 1 [62MB], CFReDS001 [FAT16], [root], [unallocated space], and Unpartitioned Space [basic disk]. The File List on the right shows files: 1480-1.TXT (2 Regular File, 03/11/2004 18:00), 1480-1.TXT.FileSlack (1 File Slack), 1A47-1.TXT (1 Regular File, 03/11/2004 18:00), app.txt (2 Regular File, 03/11/2004 22:00), and app.txt.FileSlack (1 File Slack). The Hex Value Interpreter window is open, showing a hex view of the file data. The hex view shows a file entry for 1480-1.TXT, which is a deleted file (first byte 0xE5). The hex view also shows the file entry for app.txt, which is an undeleted file (first byte 0x00).

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.

The screenshot shows the FTK Imager interface with the Evidence Tree on the left, listing CFReDS001.E01, Partition 1 [62MB], CFReDS001 [FAT16], [root], [unallocated space], and Unpartitioned Space [basic disk]. The File List on the right shows files: [root] (17 Directory), [unallocated space] (0 Unallocated Space), FAT1 (125 Filesystem Metadata), FAT2 (125 Filesystem Metadata), file system slack (1 Filesystem Slack), and VBR (1 Filesystem Metadata). The Hex Value Interpreter window is open, showing a hex view of the file data. The hex view shows a file entry for 1480-1.TXT, which is a deleted file (first byte 0xE5). The hex view also shows the file entry for app.txt, which is an undeleted file (first byte 0x00).

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 -

#### **Conclusion**

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