

# Russian Tea Room

## Introduction

This report describes the followed process to resolve 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. The purpose is to use the disk as learning material and practice the maximum.

## 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 tool interface with the following components:

- Evidence Tree:** Shows the disk structure, including 'CFReDS001.E01', 'Partition 1 [62MB]', 'CFReDS001 [FAT16]', and 'Unpartitioned Space [basic disk]'.
- File List:** A table with columns: Name, Size, Type, Date Modified.
- Hex Value Interpreter:** A table showing the interpretation of hex values for various data types.
- Hex Dump:** A table showing the raw hex data of the MBR sector, with the signature 55 AA highlighted at the end.

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	

Address	Hex	ASCII
00000050	96 8A 46 04 B4 06 3C 0E-74 11 B4 0B 3C 0C 74 05	..F..<.t..<.t..
00000060	3A C4 75 2B 40 C6 46 25-06 75 24 BB AA 55 50 B4	:Au+@EF%u\$*UP'
00000070	41 CD 13 58 72 16 81 FB-55 AA 75 10 F6 C1 01 74	Ai Xr ..du*u-bA-t
00000080	0B 8A E0 88 56 24 C7 06-A1 06 EB 1E 88 66 04 BF	..A.V6c ,.e..f.c
00000090	0A 00 B8 01 02 8B DC 33-C9 83 FF 05 7F 03 8B 4E	...-U3E.y...N
000000a0	25 03 4E 02 CD 13 72 29-BE 46 07 81 3E FE 7D 55	%W-i.p)Wf..>p)U
000000b0	AA 74 5A 83 EF 05 7F DA-85 F6 75 83 BE 27 07 EB	*tZ-i.-U-du-M'-e
000000c0	6A 98 91 52 99 03 46 08-13 56 0A E8 12 00 5A EB	...R.F.V-e..Ze
000000d0	D5 4F 74 E4 33 C0 CD 13-EB B8 00 00 00 00 00 00	00ca3Ai-e,.....
000000e0	56 33 F6 56 56 52 50 06-53 51 BE 10 00 56 8B F4	V38VVRP.SQX.-V-6
000000f0	50 52 B8 00 42 8A 56 24-CD 13 5A 58 8D 64 10 72	FR,.B-V6i-2X-d-r
00000100	0A 40 75 01 42 80 C7 02-E2 F7 F8 SE C3 EB 74 49	..eu.B.C.A-a*Acti
00000110	6E 76 61 6C 69 64 20 70-61 72 74 69 74 69 6F 6E	invalid partition
00000120	20 74 61 62 6C 69 00 45-72 72 6F 72 20 6C 6F 61	table>Error loa
00000130	64 69 6E 67 20 6F 70 65-72 61 74 69 6E 67 20 73	ding operating s
00000140	79 73 74 65 6D 00 4D 69-73 73 69 6E 67 20 6F 70	ystem-Missing op
00000150	65 72 61 74 69 6E 67 20-73 79 73 74 65 6D 00 00	erating system..
00000160	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	.....
00000170	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	.....
00000180	00 00 00 00 8B FC 1E 57 8B-F5 CB 00 00 00 00 00	...u-W-8E.....
00000190	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	.....
000001a0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	.....
000001b0	00 00 00 00 00 00 00 00-00 75 BE 90 CC 00 00 00 01	...u% i....
000001c0	01 01 06 FE 3F 08 00 3F-00 00 C9 F5 01 00 00 00	..p?..?..Ed....
000001d0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	.....
000001e0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	.....
000001f0	00 00 00 00 00 00 00 00-00 00 00 00 55 AA	.....U*
00000200	30 30 30 30 30 2F 30 30-30 2F 30 32 20 30 30 30	00000/000/02 000
00000210	30 30 30 30 30 30 30 30-30 31 00 B9 B9 B9 B9 B9	000000001..*****

Byte order: ☒ Little endian ☐ Big endian

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

Selected: 0 CFReDS001.E01

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 shows the FTK Imager interface. The Evidence Tree on the left lists the disk structure. The main window displays the Hex Value Interpreter for the selected partition. The hex data shows the boot sector, and the byte 0x06 at offset 0x1c2 is highlighted, indicating the file system is FAT16. The Hex Value Interpreter also shows the file system type as FAT16 and the volume label as CFRedS001.

We can get the following information:

- OEM ID:
- Sector size: 512b
- N° of sectors per cluster: 2
- Volume label: CFRedS001
- File system: FAT16

## 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).

The screenshot displays a forensic tool interface with several components:

- Evidence Tree:** Shows a hierarchy starting with 'CFReDS001.E01', followed by 'Partition 1 [62MB]', 'CFReDS001 [FAT16]', and 'Unpartitioned Space [basic disk]'. A sub-entry 'CfReDS-utf-8.E01' is also visible.
- File List:** A table with columns 'Name', 'Size', 'Type', and 'Date Modified'. It contains a large number of entries, mostly with names starting with '0042' followed by hex values.
- Hex Value Interpreter:** A table with columns 'Type', 'Size', and 'Value'. It lists various data types like 'signed integer', 'unsigned integer', 'FILETIME (UTC)', 'DOS date', 'DOS time', 'time\_t (UTC)', and 'time\_t (local)'.
- Find Dialog:** A modal window titled 'Find' with a 'Find What' field containing 'Beverages'. It has radio buttons for 'Binary (hex)' and 'Text', and checkboxes for 'ANSI', 'Unicode', 'Match Case', and 'Regular Expression'. There are also 'Find' and 'Cancel' buttons.
- Footer:** At the bottom, it says 'Sel start = 274453, len = 18; log sec = 536; phy sec = 16664'.

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.





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.

## Recovered menu

### ***Appetizers - ЗАКУСКИ:***

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

### ***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 со сладом
- 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