Digital Forensics Homework Assignment

Your task is to *find*, *decode* and *document* **six of the menus** from the hard drive image using the Unicode Cyrillic and Latin character (cipher) set.

- Launch **Autopsy** and select `Open Case`.
- Open the `RussianTeaRoom` folder and select `RussianTeaRoom.aut`
- Add the `Russian-TeamRoom.E01` Encase image file to the case.

```
student:~$ sudo apt-get install autopsy
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libafflib0v5 libbfio1 libewf2 libtsk13 sleuthkit
Suggested packages:
  mac-robber
The following NEW packages will be installed:
  autopsy libafflib0v5 libbfio1 libewf2 libtsk13 sleuthkit
0 upgraded, 6 newly installed, 0 to remove and 80 not upgraded.
Need to get 1,877 kB of archives.
After this operation, 6,049 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libafflib0v5 amd64
3.7.16-2build2 [201 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libbfio1 amd64 2017
0123-4 [306 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libewf2 amd64 20140
608-6.1build1 [469 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu bionic/universe amd64 libtsk13 amd64 4.4.
2-3 [326 kB]
```

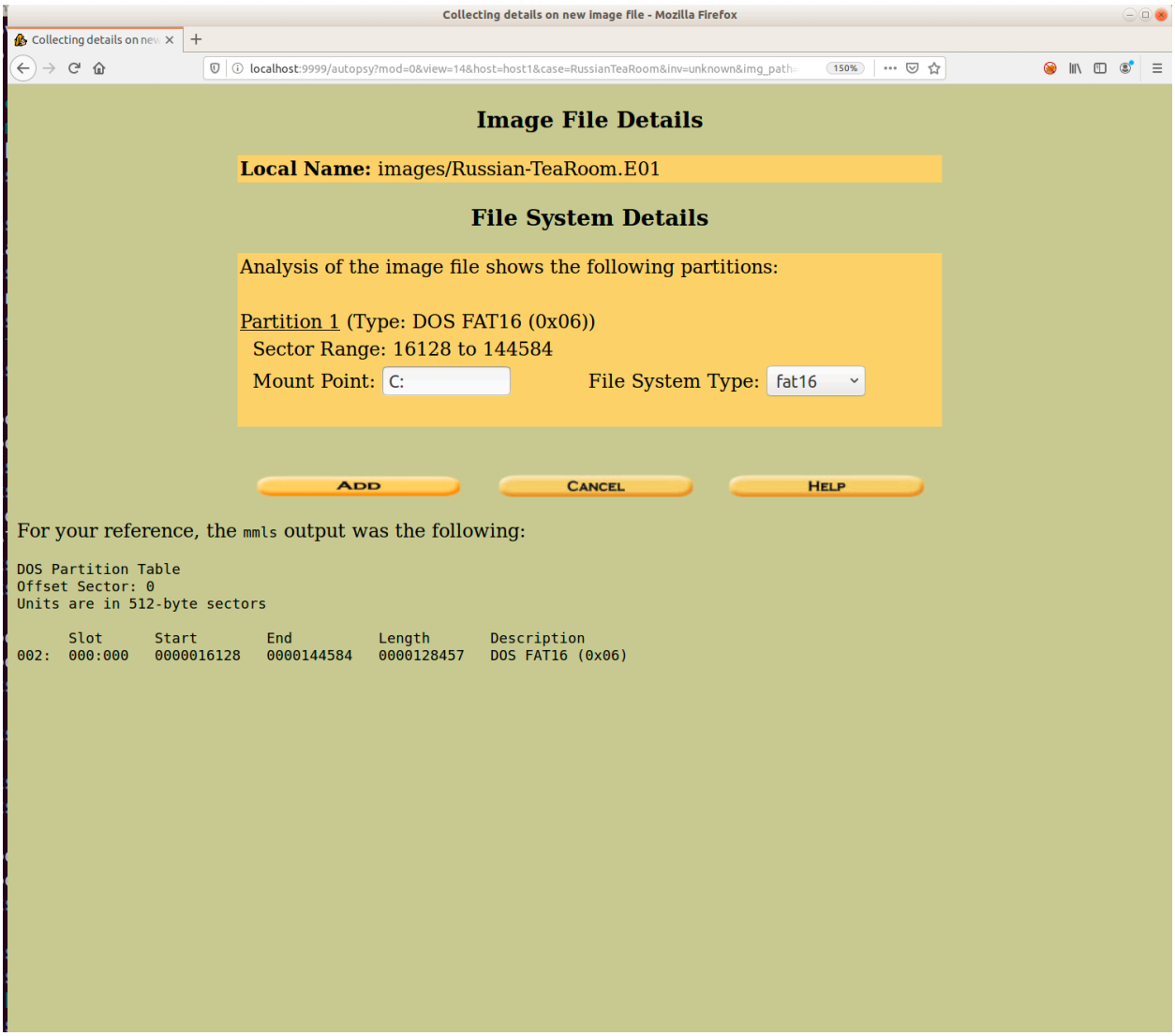
```
student:/media$ sudo bash
root:/media# cd sf_RTR
root:/media/sf_RTR# ls
root:/media/sf_RTR# ls
RussianTeaRoom-UTF16.xlsx  RussianTeaRoom.zip
root:/media/sf_RTR# unzip RussianTeaRoom.zip
Archive:  RussianTeaRoom.zip
   creating: RussianTeaRoom/
  inflating: RussianTeaRoom/autopsy.db
   creating: RussianTeaRoom/Cache/
   creating: RussianTeaRoom/Config/
 extracting: RussianTeaRoom/Config/CasePreferences.properties
   creating: RussianTeaRoom/Export/
   creating: RussianTeaRoom/Log/
  inflating: RussianTeaRoom/Log/autopsy.log.0
  inflating: RussianTeaRoom/Log/autopsy.log.1
  inflating: RussianTeaRoom/Log/autopsy.log.2
  inflating: RussianTeaRoom/Log/autopsy.log.3
  inflating: RussianTeaRoom/Log/autopsy.log.4
  inflating: RussianTeaRoom/Log/autopsy.log.5
```

```
root:/media/sf_RTR# ls
RussianTeaRoom  RussianTeaRoom-UTF16.xlsx  RussianTeaRoom.zip
root:/media/sf_RTR# mv RussianTeaRoom.zip /home/student
root:/media/sf_RTR# mv RussianTeaRoom-UTF16.xlsx  /home/student
root:/media/sf_RTR# mv RussianTeaRoom  /home/student
root:/media/sf_RTR#  cd /home/student
root:~# exit
exit
student:/media$ cd /home/student
student:~$ pwd
/home/stude
```

```
student:~$ ls
 2018-08-12-traffic-analysis-exercise.pcap.zip            'access_30DAY(1).log'   Desktop     forensicshw   Pictures   Templates
 2019-01-28-alerts-for-traffic-analysis-exercise.txt.zip   access_30DAY.log       Documents   LinuxDay3     Projects   testfi
 2019-01-28-traffic-analysis-exercise.pcap                 alert2.txt             Downloads   Music         Public     Videos
 2019-01-28-traffic-analysis-exercise.pcap.zip             anyname                error.txt   notes         sh
 2019-04-15-traffic-analysis-exercise-alerts.zip           BurpSuiteCommunity     file.txt    passwd.txt    snap
student:~$ cd forensicshw
student:~/forensicshw$ ls
RussianTeaRoom  RussianTeaRoom-UTF16.xlsx
student:~/forensicshw$ ls /forensicshw
/forensicshw
student:~/forensicshw$ ls /forensicshw/
ls: cannot access '/forensicshw/': Not a directory
student:~/forensicshw$ cat /forensicshw
cat: /forensicshw: Permission denied
student:~/forensicshw$ ls
RussianTeaRoom  RussianTeaRoom-UTF16.xlsx
student:~/forensicshw$ cd /
student:/$ ls
bin    dev          home            lib              lost+found  opt   run   srv       tmp  vmlinuz
boot   etc          initrd.img      lib64            media       proc  sbin  swapfile  usr  vmlinuz.old
cdrom  forensicshw  initrd.img.old  lock_screen.jpg  mnt         root  snap  sys       var
student:/$ cd forensicshw
bash: cd: forensicshw: Not a directory
student:/$ ls forensicshw
forensicshw
student:/$ sudo mv forensicshw RussianTeaRoom.zip
student:/$ ls
bin    dev   initrd.img      lib64            media  proc  RussianTeaRoom.zip  srv       tmp  vmlinuz
boot   etc   initrd.img.old  lock_screen.jpg  mnt    root  sbin                swapfile  usr  vmlinuz.old
cdrom  home  lib             lost+found       opt    run   snap                sys       var
student:/$ rm RussianTeaRoom.zip
rm: remove write-protected regular file 'RussianTeaRoom.zip'? yes
rm: cannot remove 'RussianTeaRoom.zip': Permission denied
student:/$ sudo rm RussianTeaRoom.zip
```

```
root:~/forensicshw# ls -l
total 16
drwxrwxrwx 9 root vboxsf  4096 Mar 25  2019 RussianTeaRoom
-rwxrwx--- 1 root vboxsf 12266 Mar 25 20:45 RussianTeaRoom-UTF16.xlsx
root:~/forensicshw# sudo chmod 777 RussianTeaRoom
RussianTeaRoom/            RussianTeaRoom-UTF16.xlsx
root:~/forensicshw# sudo chmod 777 RussianTeaRoom
RussianTeaRoom/            RussianTeaRoom-UTF16.xlsx
root:~/forensicshw# sudo chmod 777 RussianTeaRoom-UTF16.xlsx
root:~/forensicshw# ls -l
total 16
drwxrwxrwx 9 root vboxsf  4096 Mar 25  2019 RussianTeaRoom
-rwxrwxrwx 1 root vboxsf 12266 Mar 25 20:45 RussianTeaRoom-UTF16.xlsx
root:~/forensicshw# exit
exit
student:~/forensicshw$ cd RussianTeaRoom
student:~/forensicshw/RussianTeaRoom$ ls
autopsy.db  Cache  Config  Export  Log  ModuleOutput  Reports  RussianTeaRoom.aut  Russian-TeaRoom.E01  SolrCore.properties  Temp
student:~/forensicshw/RussianTeaRoom$
```

Russian-TeaRoom.E01



- After downloading the autopsy system to ubuntu
- I created a shared file: sf_RFR file within downloads on the ubuntu machine and downloaded the assignment contents to file
    - Used the file path to share Russian-TeaRoom.E01

```
student:~/forensicshw$ cd RussianTeaRoom UTF-16.xlsx
bash: cd: too many arguments
student:~/forensicshw$ cd RussianTeaRoom-UTF-16.xlsx
bash: cd: RussianTeaRoom-UTF-16.xlsx: No such file or directory
student:~/forensicshw$ sudo bash
root:~/forensicshw# cd RussianTeaRoom
root:~/forensicshw/RussianTeaRoom# ls
autopsy.db  Cache  Config  Export  Log  ModuleOutput  Reports  RussianTeaRoom.aut  Russian-TeaRoom.E01  SolrCore.properties  Temp
root:~/forensicshw/RussianTeaRoom# exit
exit
student:~/forensicshw$ cd ModuleOutput
bash: cd: ModuleOutput: No such file or directory
student:~/forensicshw$ sudo bash
root:~/forensicshw# cd ModuleOutput
bash: cd: ModuleOutput: No such file or directory
root:~/forensicshw# cd RussianTeaRoom/ModuleOutput
root:~/forensicshw/RussianTeaRoom/ModuleOutput# ls
'Embedded File Extractor'  'Image Gallery'  keywordsearch  'PhotoRec Carver'  RecentActivity  'Virtual Machine Extractor'
root:~/forensicshw/RussianTeaRoom/ModuleOutput# cd ..
root:~/forensicshw/RussianTeaRoom# cd RussianTeaRoom.aut
bash: cd: RussianTeaRoom.aut: Not a directory
root:~/forensicshw/RussianTeaRoom# cat RussianTeaRoom.aut
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<AutopsyCase>
  <SchemaVersion>4.0</SchemaVersion>
  <CreatedDate>2019/03/23 16:11:43 (EDT)</CreatedDate>
  <ModifiedDate>2019/03/23 16:11:44 (EDT)</ModifiedDate>
  <CreatedByAutopsyVersion>4.10.0</CreatedByAutopsyVersion>
  <SavedByAutopsyVersion>4.10.0</SavedByAutopsyVersion>
  <Case>
    <Name>556677_20190323_161143</Name>
    <DisplayName>556677</DisplayName>
    <Number>33456</Number>
    <Examiner>Rocky Squirrel</Examiner>
    <ExaminerPhone>703-777-9800</ExaminerPhone>
    <ExaminerEmail>rsquirell@frostbite.com</ExaminerEmail>
    <CaseNotes/>
    <CaseType>Single-user case</CaseType>
    <Database/>
    <CaseDatabase>autopsy.db</CaseDatabase>
    <TextIndex/>
  </Case>
</AutopsyCase>
root:~/forensicshw/RussianTeaRoom#
```

G	H	I	J
Russian Menu	**Start Location in Encase Image**	**Hex String for Menu Name**	**CYRILLIC UTF-16 (Unicode Escaped) for Menu Name**
ЗАКУСКИ	*img_Russian-TeaRoom.E01vol_vol2/app.txt*	04 17 04 10 04 1A 04 23 04 21 04 1A 04 18 00 20	\u0417\u0410\u041a\u0423\u0421\u041a\u0418\u0020
Russian Menu	**Start Location in Encase Image**	**Hex String for Menu Name**	**CYRILLIC UTF-16 (Unicode Escaped) for Menu Name**
БЛИНЫ	*img_Russian-TeaRoom.E01vol_vol2/app.txt*	04 11 04 1B 04 18 04 1D 04 2B	\u0411\u041b\u0418\u041d\u042b
блины с икрой	*img_Russian-TeaRoom.E01vol_vol2/app.txt*	04 31 04 3B 04 38 04 3D 04 4B 00 20 04 41 00 20 04 38 04 3A 04 40 04 3E 04 39	\u0431\u043b\u0438\u043d\u044b\u0020\u0441\u0020\u0438\u043a\u0440\u043e\u0439
блины с селёдкой, икрой, сметаной и сёмгой	*img_Russian-TeaRoom.E01vol_vol2/app.txt*	04 31 04 3B 04 38 04 3D 04 4B 00 20 04 41 00 20 04 41 04 35 04 3B 04 51 04 34 04 3A 04 3E 04 39 00 2C 00 20 04 38 04 3A 04 40 04 3E 04 39 00 2C 00 20 04 41 04 3C	\u0431\u043b\u0438\u043d\u044b\u0020\u0441\u0020\u0441\u0435\u043b\u0451\u0434\u043a\u043e\u0439\u002c\u0020\u0438\u043a\u0440\u043e\u0439\u002c\u0020\u0441\u043c\u0435\u0442\u0430\u043d\u043e\u0439\u0020\u0438\u002c
Russian Menu	**Start Location in Encase Image**	**Hex String for Menu Name**	**CYRILLIC UTF-16 (Unicode Escaped) for Menu Name**
ПИРОЖКИ И ПЕЛЬМЕНИ	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	04 1F 04 18 04 20 04 1E 04 16 04 1A 04 18 00 20 04 18 00 20 04 1F 04 15 04 1B 04 1C 04 15 04 1D 04 18	\u041f\u0418\u0420\u041e\u0416\u041a\u0418\u0020\u0418\u0020\u041f\u0415\u041b\u041c\u0415\u041d\u0418
Russian Menu	**Start Location in Encase Image**	**Hex String for Menu Name**	**CYRILLIC UTF-16 (Unicode Escaped) for Menu Name**
МЯСО И РЫБА	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28*	04 1C 04 2F 04 21 04 1E 00 20 04 18 00 20 04 20 04 2B 04 11 04 10 00 0D 00 0A	\u041c\u042f\u0421\u041e\u0020\u0418\u0020\u0420\u042b\u0411\u0410\u000d\u000a
беф-строганов	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	04 31 04 35 04 44 00 2D 04 41 04 42 04 40 04 3E 04 33 04 30 04 3D 04 3E 04 32 00 0D 00 0A	\u0431\u0435\u0444\u002d\u0441\u0442\u0440\u043e\u0433\u0430\u043d\u043e\u0432\u000d\u000a
бифштекс	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	04 31 04 38 04 44 04 48 04 42 04 35 04 3A 04 35 00 0D 00 0A	\u0431\u0438\u0444\u0448\u0442\u0435\u043a\u0435\u000d\u000a
котлеты	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	04 3A 04 3E 04 42 04 3B 04 35 04 42 04 4B 00 0D 00 0A	\u043a\u043e\u0442\u043b\u0435\u0442\u044b\u000d\u000a
ростбиф	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	04 40 04 3E 04 41 04 42 04 31 04 38 04 44 00 0D 00 0A 00 0D 00 0A	\u0440\u043e\u0441\u0442\u0431\u0438\u0444\u000d\u000a\u000d\u000a
курица	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	04 3A 04 43 04 40 04 38 04 46 04 30 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A	\u043a\u0443\u0440\u0438\u0446\u0430\u000d\u000a\u000d\u000a\u000d\u000a
утат	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	04 43 04 42 04 30 04 42 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A	\u0443\u0442\u0430\u0442\u000d\u000a\u000d\u000a\u000d\u000a\u000d\u000a
Russian Menu	**Start Location in Encase Image**	**Hex String for Menu Name**	**CYRILLIC UTF-16 (Unicode Escaped) for Menu Name**
СЫР И МОЛОЧНЫЕ	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	04 21 04 2B 04 20 00 20 04 18 00 20 04 1C 04 1E 04 1B 04 1E 04 27 04 1D 04 2B 04 15 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A	\u0421\u042b\u0420\u0020\u0418\u0020\u041c\u041e\u041b\u041e\u0427\u041d\u042b\u0415\u000d\u000a\u000d\u000a\u000d\u000a\u000d\u000a\u000d\u000a\u000d\u000a
Russian Menu	**Start Location in Encase Image**	**Hex String for Menu Name**	**CYRILLIC UTF-16 (Unicode Escaped) for Menu Name**
НАПИТКИ	*img_Russian-TeaRoom.E01/vol_vol2/_4B0~1.txt*	04 1D 04 10 04 1F 04 18 04 22 04 1A 04 18 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A 00 0D 00 0A 00 0D	\u041d\u0410\u041f\u0418\u0422\u041a\u0418\u000d\u000a\u000d\u000a\u000d\u000a\u000d\u000a\u000d\u000a\u000d\u000a

A	B	C	D	E	F
Menu 1	**File Location(s) / Name(s)**	**English Menu**	**Start Location in Encase Image**	**Hex String for Menu Name**	**Latin UTF-16 (Unicode Escaped) for Menu Name**
	Russian-TeaRoom.E01	**Appetizers**	*img_Russian-TeaRoom.E01vol_vol2/app.txt*	00 41 00 70 00 70 00 65 00 74 00 69 00 7A 00 65 00 72 00 73	\u0041\u0070\u0070\u0065\u0074\u0069\u007a\u0065\u0072\u0073
Menu 3	**File Location(s) / Name(s)**	**English Menu**	**Start Location in Encase Image File**	**Hex String for Menu Name**	**Latin UTF-16 (Unicode Escaped) for Menu Name**
	Russian-TeaRoom.E01	**Pancakes**	*img_Russian-TeaRoom.E01vol_vol2/app.txt*	00 50 00 61 00 6E 00 63 00 61 00 6B 00 65 00 73	\u0050\u0061\u006e\u0063\u0061\u006b\u0065\u0073
		pancakes with caviar	*img_Russian-TeaRoom.E01vol_vol2/app.txt*	00 70 00 61 00 6E 00 63 00 61 00 6B 00 65 00 73 00 20 00 77 00 69 00 74 00 68 00 20 00 63 00 61 00 76 00 69 00 61 00 72 00 0D 00 0A	\u0070\u0061\u006e\u0063\u0061\u006b\u0065\u0073\u0020\u0077\u0069\u0074\u0068\u0020\u0063\u0061\u0076\u0069\u0061\u0072\u000d\u000a
		pancakes with everything	*img_Russian-TeaRoom.E01vol_vol2/app.txt*	00 70 00 61 00 6E 00 63 00 61 00 6B 00 65 00 73 00 20 00 77 00 69 00 74 00 68 00 20 00 65 00 76 00 65 00 72 00 79 00 74 00 68 00 69 00 6E 00 67	\u0070\u0061\u006e\u0063\u0061\u006b\u0065\u0073\u0020\u0077\u0069\u0074\u0068\u0020\u0065\u0076\u0065\u0072\u0079\u0074\u0068\u0069\u006e\u0067
Menu 4	**File Location(s) / Name(s)**	**English Menu**	**Start Location in Encase Image File**	**Hex String for Menu Name**	**Latin UTF-16 (Unicode Escaped) for Menu Name**
	Russian-TeaRoom.E01	Meat pies and dumplings	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	00 4D 00 65 00 61 00 74 00 20 00 70 00 69 00 65 00 73 00 20 00 61 00 6E 00 64 00 20 00 64 00 75 00 6D 00 70 00 6C 00 69 00 6E 00 67 00 73	\u004d\u0065\u0061\u0074\u0020\u0070\u0069\u0065\u0073\u0020\u0061\u006e\u0064\u0020\u0064\u0075\u006d\u0070\u006c\u0069\u006e\u0067\u0073
Menu 5	**File Location(s) / Name(s)**	**English Menu**	**Start Location in Encase Image File**	**Hex String for Menu Name**	**Latin UTF-16 (Unicode Escaped) for Menu Name**
	Russian-TeaRoom.E01	Meat and fish	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	00 4D 00 65 00 61 00 74 00 20 00 61 00 6E 00 64 00 20 00 66 00 69 00 73 00 68	\u004d\u0065\u0061\u0074\u0020\u0061\u006e\u0064\u0020\u0066\u0069\u0073\u0068
		beef stroganoff	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	00 62 00 65 00 65 00 66 00 20 00 73 00 74 00 72 00 6F 00 67 00 61 00 6E 00 6F 00 66 00 66	\u0062\u0065\u0065\u0066\u0020\u0073\u0074\u0072\u006f\u0067\u0061\u006e\u006f\u0066\u0066
		steak	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	00 73 00 74 00 65 00 61 00 6B	\u0073\u0074\u0065\u0061\u006b
		cutlets	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	00 63 00 75 00 74 00 6C 00 65 00 74 00 73	\u0063\u0075\u0074\u006c\u0065\u0074\u0073
		roast beef	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	00 72 00 6F 00 61 00 73 00 74 00 20 00 62 00 65 00 65 00 66	\u0072\u006f\u0061\u0073\u0074\u0020\u0062\u0065\u0065\u0066
		chicken	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	00 63 00 68 00 69 00 63 00 6B 00 65 00 6E	\u0063\u0068\u0069\u0063\u006b\u0065\u006e
		duck	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	00 64 00 75 00 63 00 6B	\u0064\u0075\u0063\u006b
Menu 6	**File Location(s) / Name(s)**	**English Menu**	**Start Location in Encase Image File**	**Hex String for Menu Name**	**Latin UTF-16 (Unicode Escaped)**
	Russian-TeaRoom.E01	Cheese and milk products	*img_Russian-TeaRoom.E01/vol_vol3/Unalloc_28_74027520_103219200*	00 43 00 68 00 65 00 65 00 73 00 65 00 20 00 61 00 6E 00 64 00 20 00 6D 00 69 00 6C 00 6B 00 20 00 70 00 72 00 6F 00 64 00 75 00 63 00 74 00 73	\u0043\u0068\u0065\u0065\u0073\u0065\u0020\u0061\u006e\u0064\u0020\u006d\u0069\u006c\u006b\u0020\u0070\u0072\u006f\u0064\u0075\u0063\u0074\u0073
Menu 7	**File Location(s) / Name(s)**	**English Menu**	**Start Location in Encase Image File**	**Hex String for Menu Name**	**Latin UTF-16 (Unicode Escaped) for Menu Name**
	Russian-TeaRoom.E01	Beverages	*img_Russian-TeaRoom.E01/vol_vol2/_4B0~1.txt*	00 42 00 65 00 76 00 65 00 72 00 61 00 67 00 65 00 73	\u0042\u0065\u0076\u0065\u0072\u0061\u0067\u0065\u0073