**Bonus Assignment: Russian Tea Room**

The goal of this assignment is to sharpen your skills in locating and identifying data in a forensic image.

* These skills are important for tasks related to locating and decoding data, such as executable code or malicious documents embedded in images or network logs.

**Scenario: The Case of the Little Russian Tea Room**

* There was a fire at the Little Russian Tea Room restaurant last week, and the only thing recovered was a hard drive. To start rebuilding the business, the restaurant hired you as a forensics investigator to look at the disk image and reconstruct the menu.
* You'll be working with an EnCase image of the hard drive.
* Luckily, the English and Russian menu are both in the hard drive image. However, only the English menu and two sections of the Russian menu are readable. Your must decode several sections of the Russian menu.

**Resources:**

The strings in the EnCase image are hex and represent the UTF-16 format. You'll need to be familiar with hex and UTF-16 encoding and decoding for this activity.

* Review this [Unicode Tutorial](/the-university-of-western-australia/waus-perth-cyber-pt-10-2020-u-c/-/blob/master/2-Homework/21-Digital-Forensics/Instructions/Resources/Unicode-Tutorial.md) and the practice exercises. This review will help you locate the menus on the hard drive image.

Below are the files required to complete the assignment:

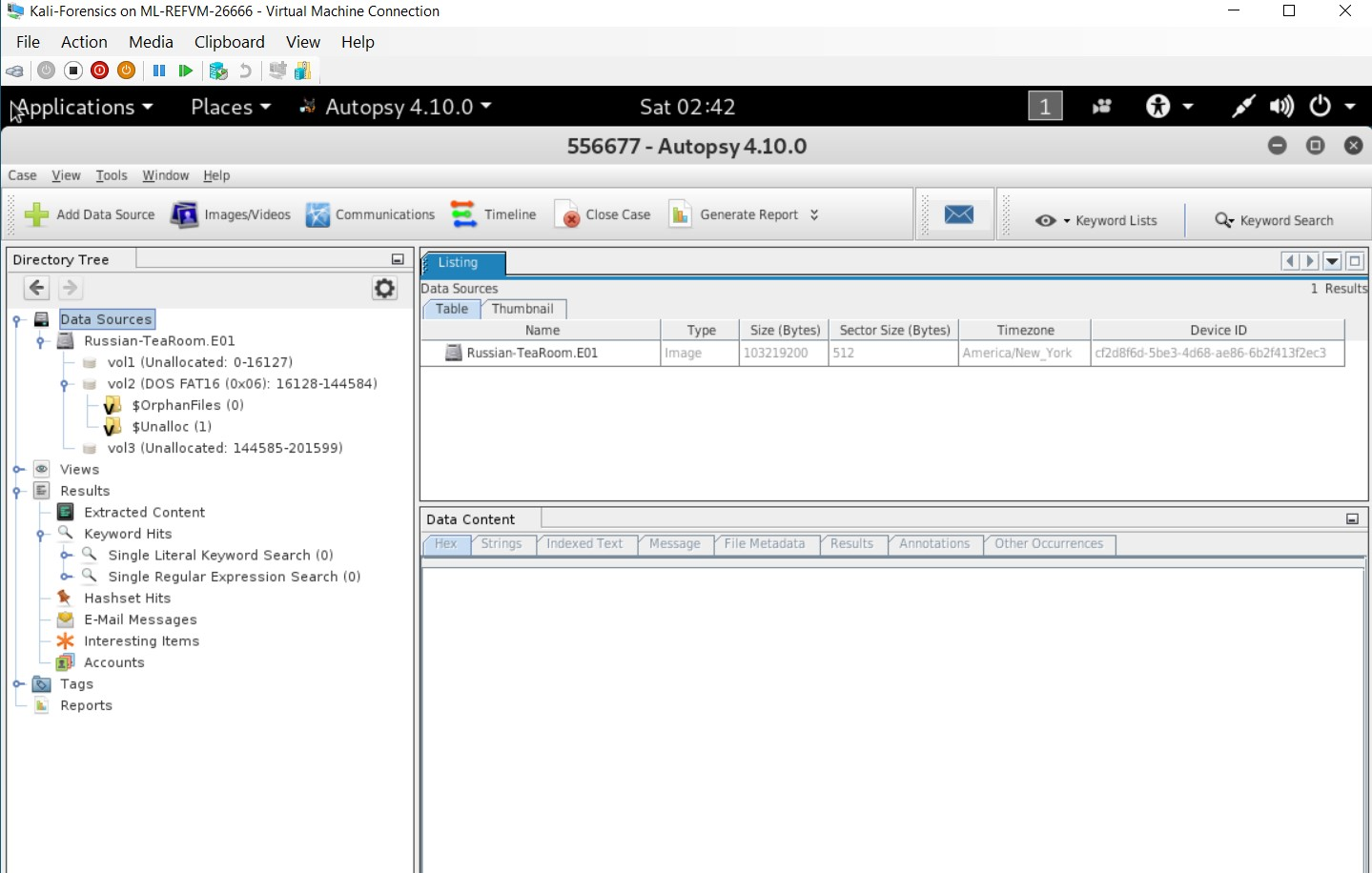
* [RussianTeaRoom.zip](/the-university-of-western-australia/waus-perth-cyber-pt-10-2020-u-c/-/blob/master/2-Homework/21-Digital-Forensics/Instructions/Resources/RussianTeaRoom.zip) (560 KB): The Autopsy case file and Encase image file.
* [menu.pdf](/the-university-of-western-australia/waus-perth-cyber-pt-10-2020-u-c/-/blob/master/2-Homework/21-Digital-Forensics/Instructions/Resources/menu.pdf) (56.0 KB): The Little Russian Tea Room menu.
* [Google Sheets: Russian Team Room](https://docs.google.com/spreadsheets/d/1GeibalvCi0jnUKay82dSne9V9kdEuUNyOxpaAEBABiU/edit#gid=0)
* [Unicode-Tutorial.md](/the-university-of-western-australia/waus-perth-cyber-pt-10-2020-u-c/-/blob/master/2-Homework/21-Digital-Forensics/Instructions/Resources/Unicode-Tutorial.md): Short Unicode tutorial.

The files can also be found in the /root/autopsy-files/homework directory in Autopsy.

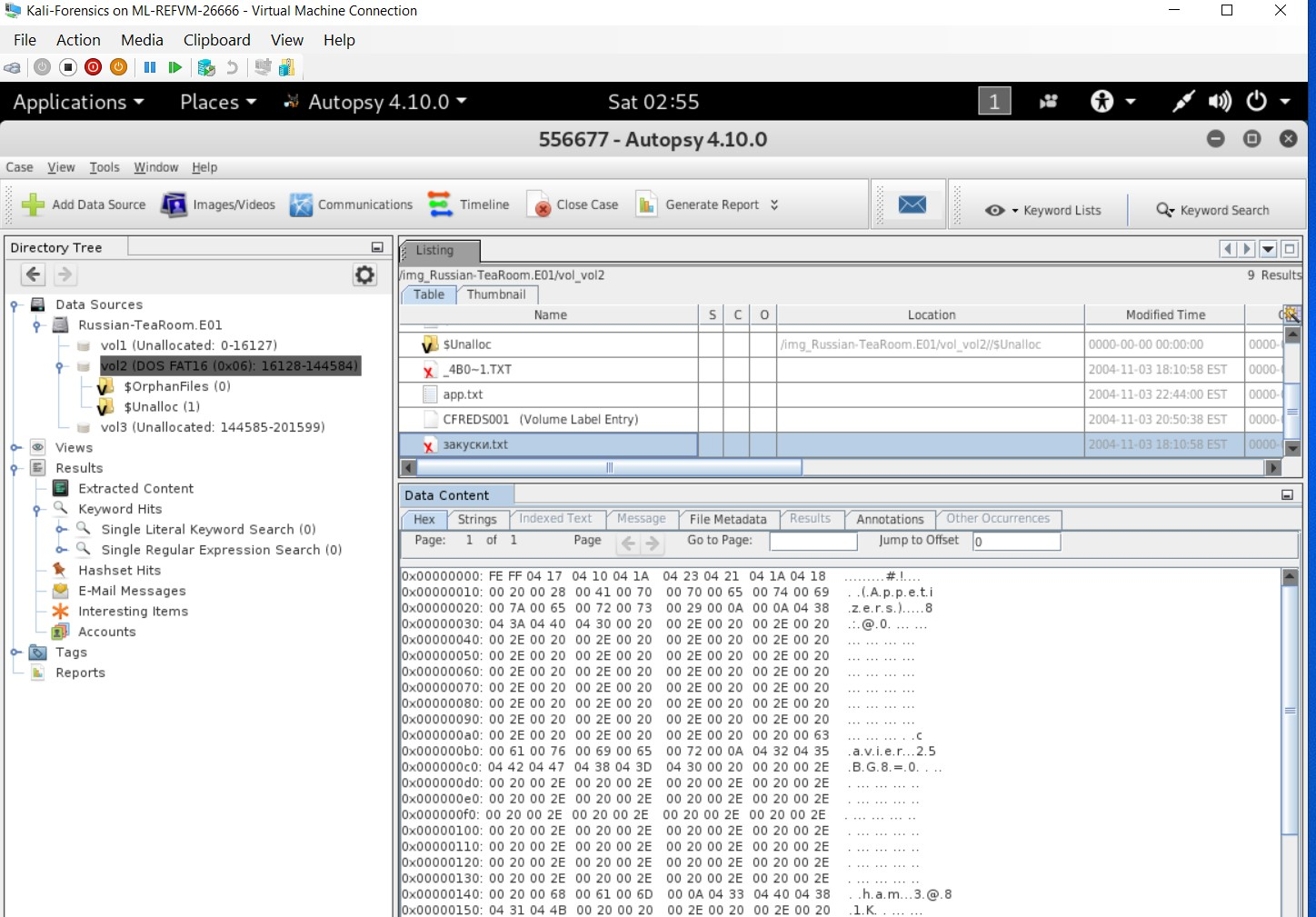
**Instructions**

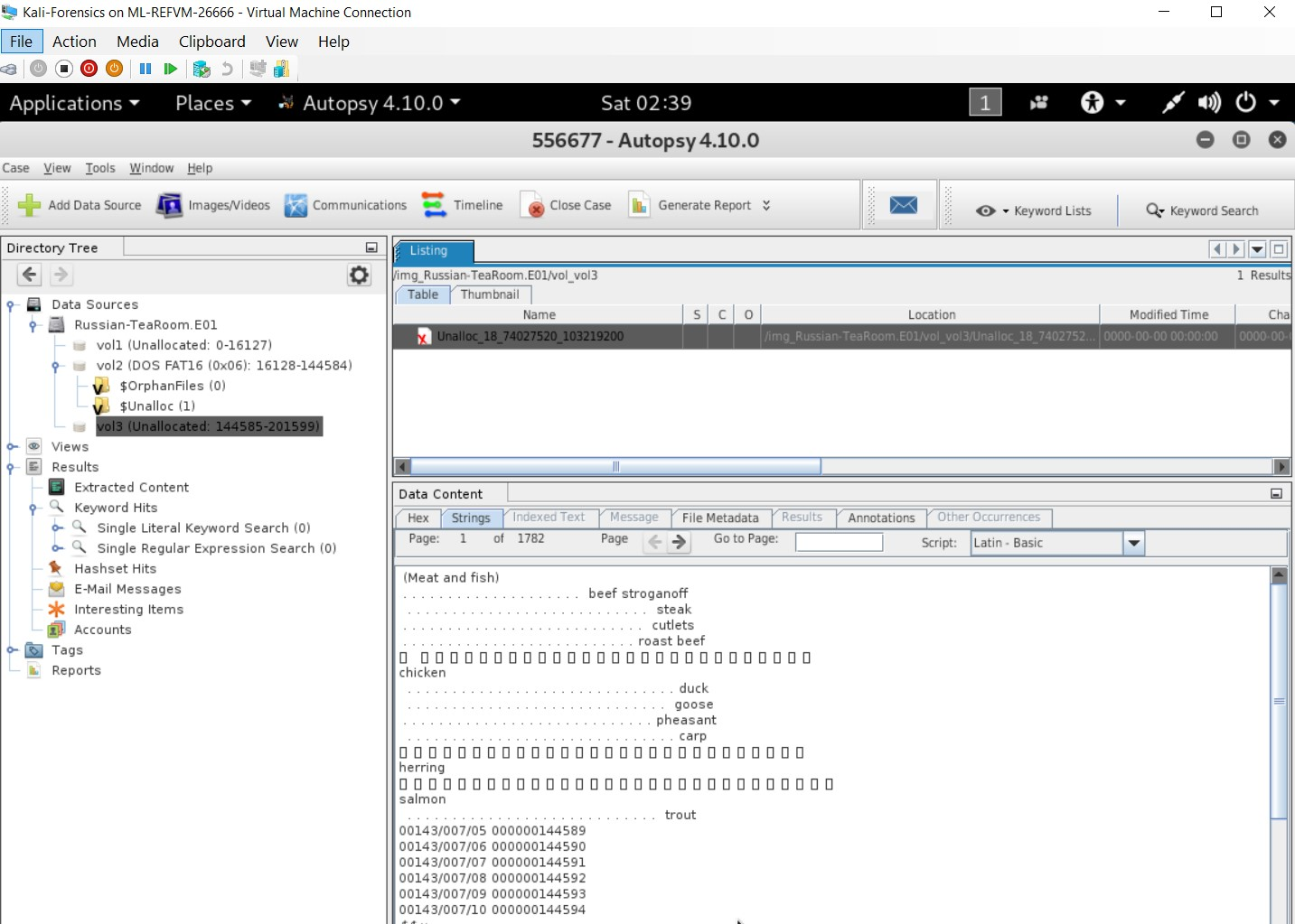
Your task is to find, decode, and document six of the menus from the hard drive image using the Unicode Cyrillic and Latin character (cipher) set.

1. 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.
   * This is a sample of the hex data in the Autopsy RussianTeaRoom case file:



1. Use [Google Sheets: Russian Team Room](https://docs.google.com/spreadsheets/d/1GeibalvCi0jnUKay82dSne9V9kdEuUNyOxpaAEBABiU/edit#gid=0) to document the remaining information from the EnCase image for the investigation.
2. Find and document the complete file locations for the six menu sections in the image.
   * **Hint:** There may be multiple locations for the same file.
3. Document the menu items in Cyrillic (e.g., бифштеке) and English (e.g., steak) for the two following menu sections:
   * Pancakes (Menu #3)
   * Meat and Fish (Menu #5)
     + **Hint:** Use the **Hex** and **String** tabs in **Data Content** window in Autopsy to view the data.





1. Include in your documentation:
   * Starting location in the hex dump.
     + For example: 0x00000010
   * Hex string for menu name or menu item.
     + For example: 00 42 00 65 00 76 00 65 00 72 00 61 00 67 00 65 00 73
   * UTF-16 escape sequence for a menu name or menu item.
     + For example: \u0042\u0065\u0076\u0065\u0072\u0061\u0067\u0065\u0073

**Submission Guidelines**

* Submit the completed [Google Sheets: Russian Team Room](https://docs.google.com/spreadsheets/d/1GeibalvCi0jnUKay82dSne9V9kdEuUNyOxpaAEBABiU/edit#gid=0) file.

**Important Note for Certification Prep Week**

* In Certification Prep Week, Day 1 you will be using CertMaster Practice in class.
* Make sure you have access to the tool and should be ready to use it during this unit.

**Important Note for Career Prep Week**

* After Certification Prep Week, we will move on to Career Prep. You will take a closer look at the cyber career landscape and will learn practical tips on how to prepare for the job hunt, hone their resume, craft their LinkedIn profile, and ace the behavioral and technical interviews.
* Please come to class with a digital copy of your resume which you will be working on and sharing with your fellow peers.
* You must also have a LinkedIn profile set up as well. If you did not set up a LinkedIn account during pre-work, please make sure you do so prior to Career Prep week.