**Project**

**NIST-Russian Tea Room**

**Digital Forensics**

**Submitted by:** Momenah Saif

**Roll number:** 21i-1909

**Date:** 3-5-2024

**Table of Contents**

[ **Case** 3](#_Toc165925042)

[ **Tool** 3](#_Toc165925043)

[ **Download evidence file and create case** 3](#_Toc165925044)

[ **Finding Evidence** 7](#_Toc165925045)

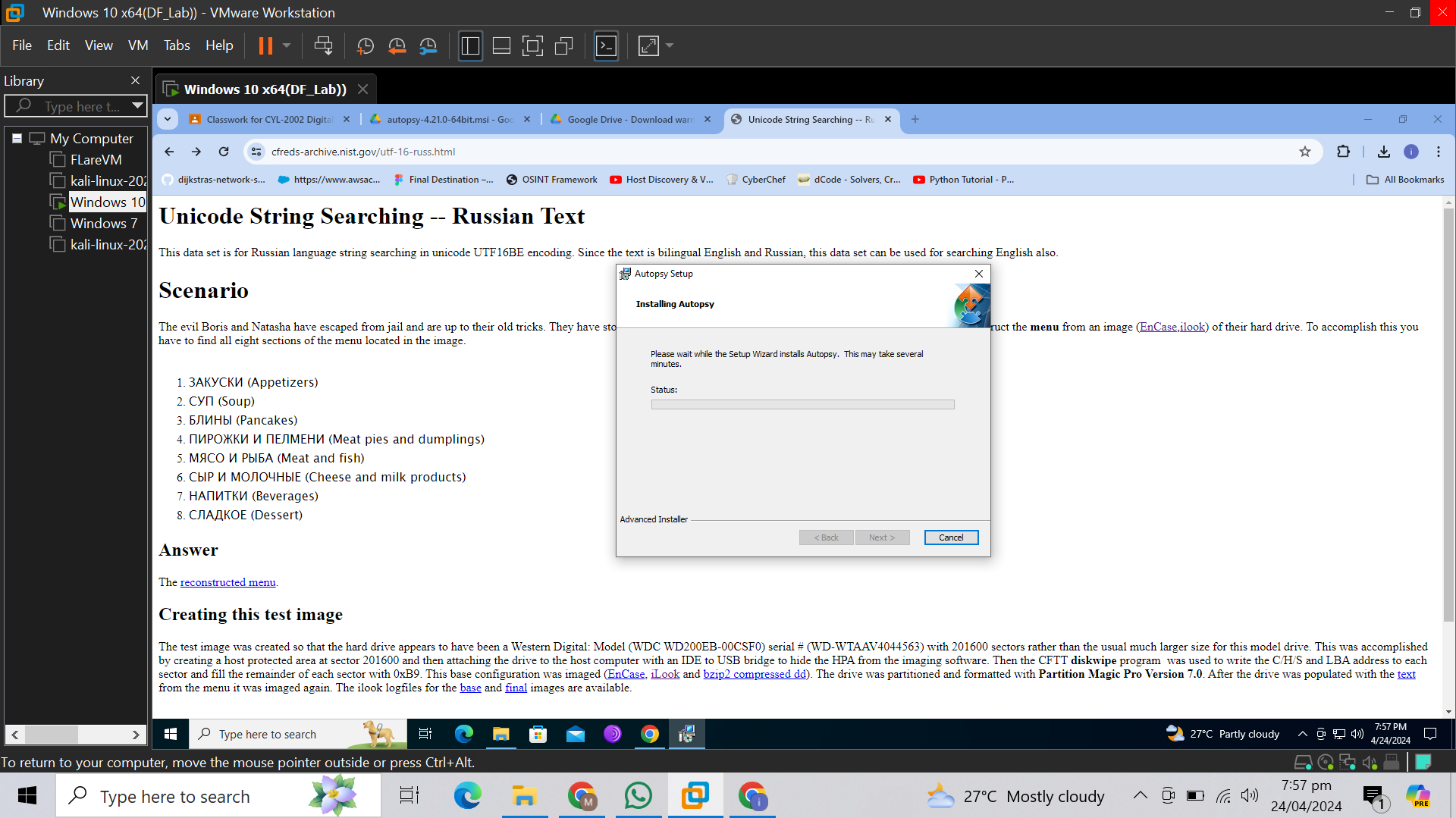
[ **Other Information found** 11](#_Toc165925046)

# **Case**

The evil Boris and Natasha have escaped from jail and are up to their old tricks. They have stolen the new menu from The Little Russian Tea Room. Your task is to reconstruct the menu from an image of their hard drive. To accomplish this, you have to find all eight sections of the menu located in the image.

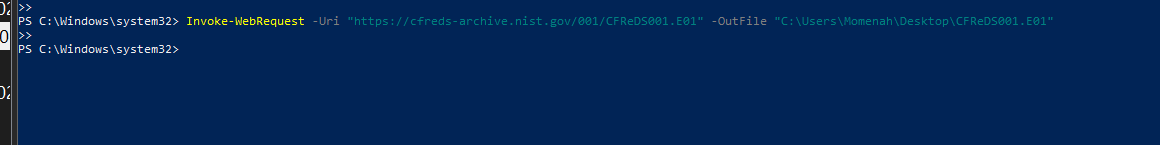
# **Tool**

Autopsy and HashCalc

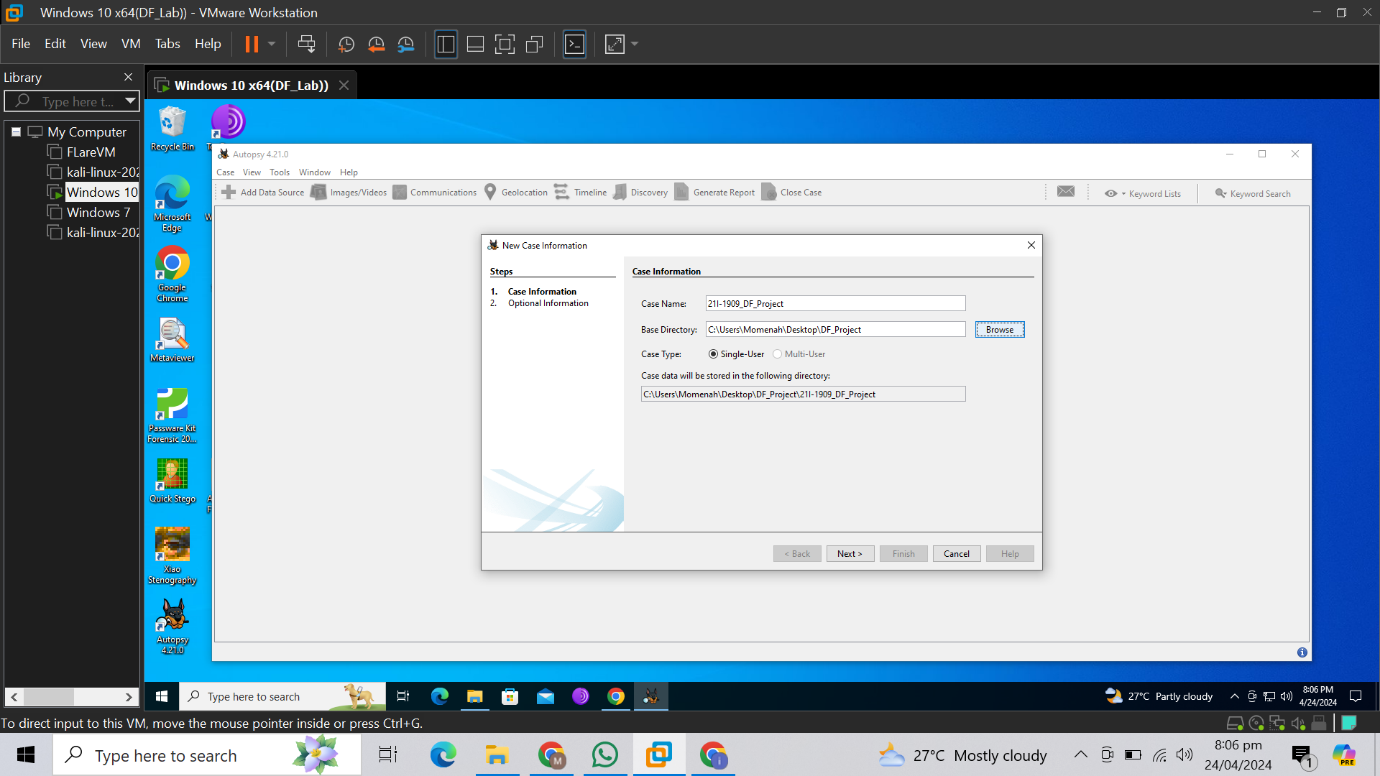


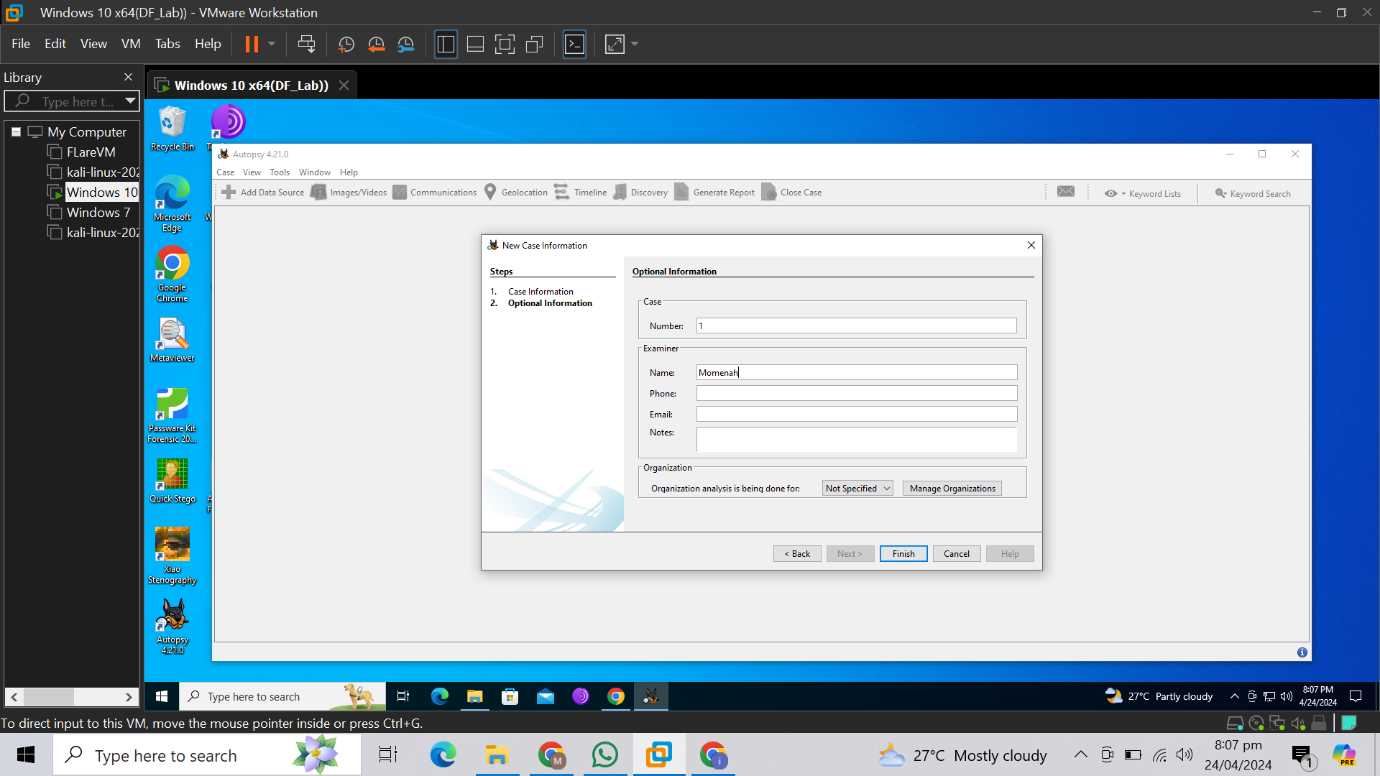
# **Download evidence file and create case**

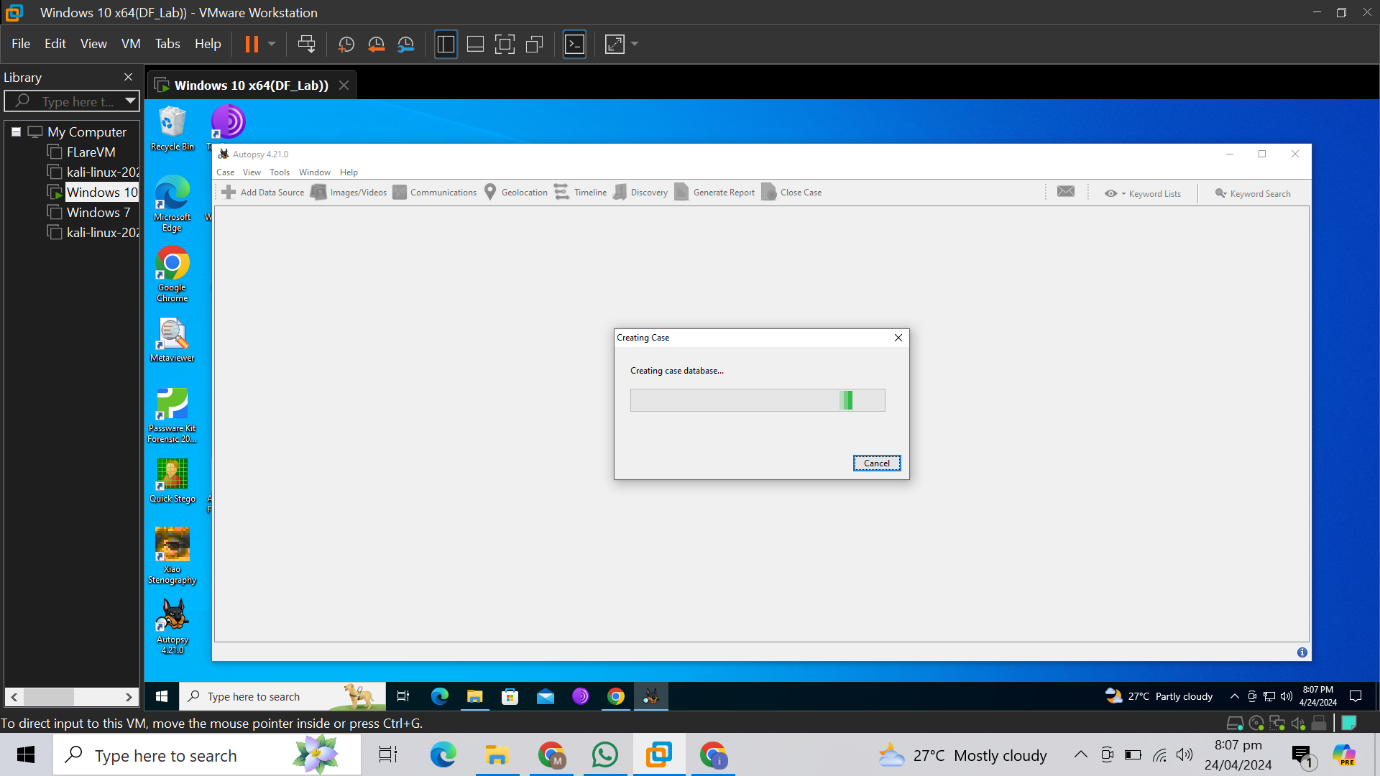
* Downloaded the evidence file from the site by running the below command in Windows PowerShell with admin privileges.



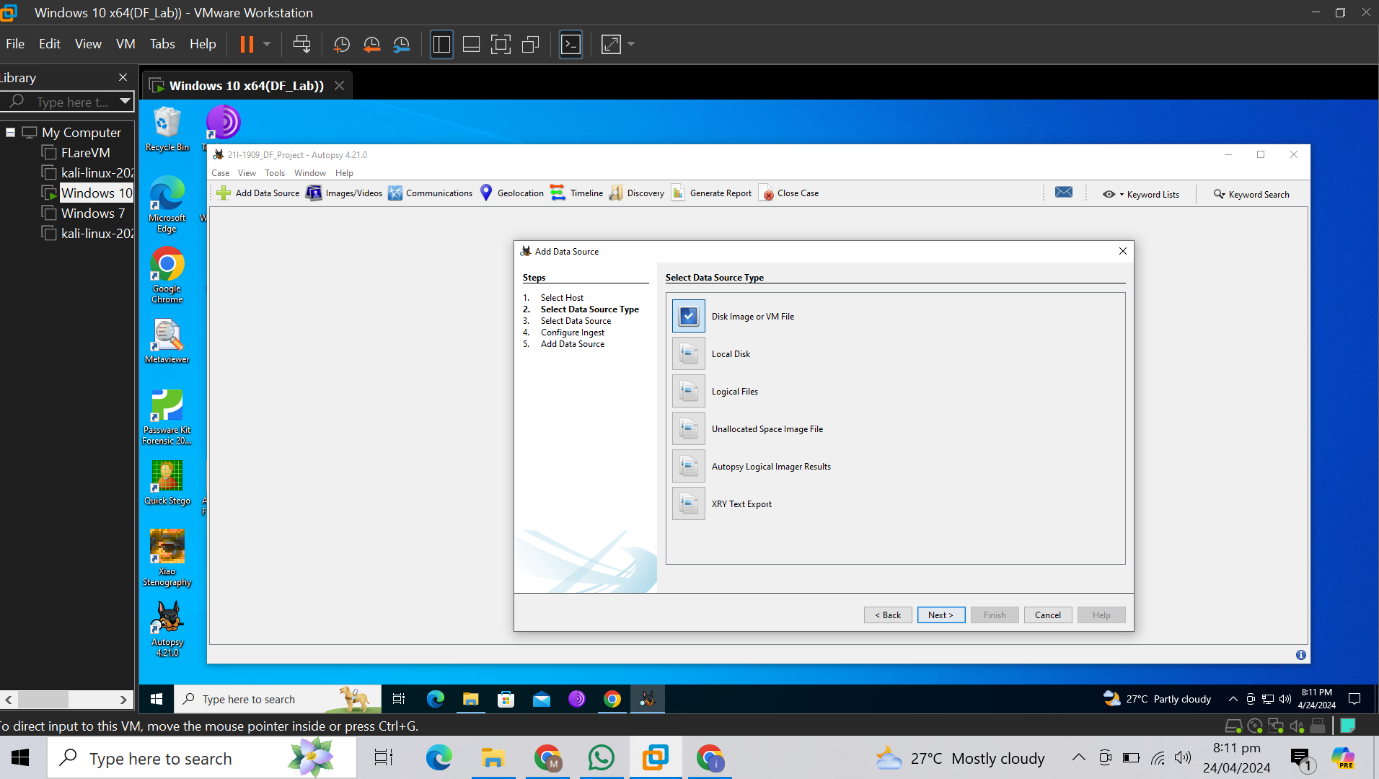
* Created a case in Autopsy



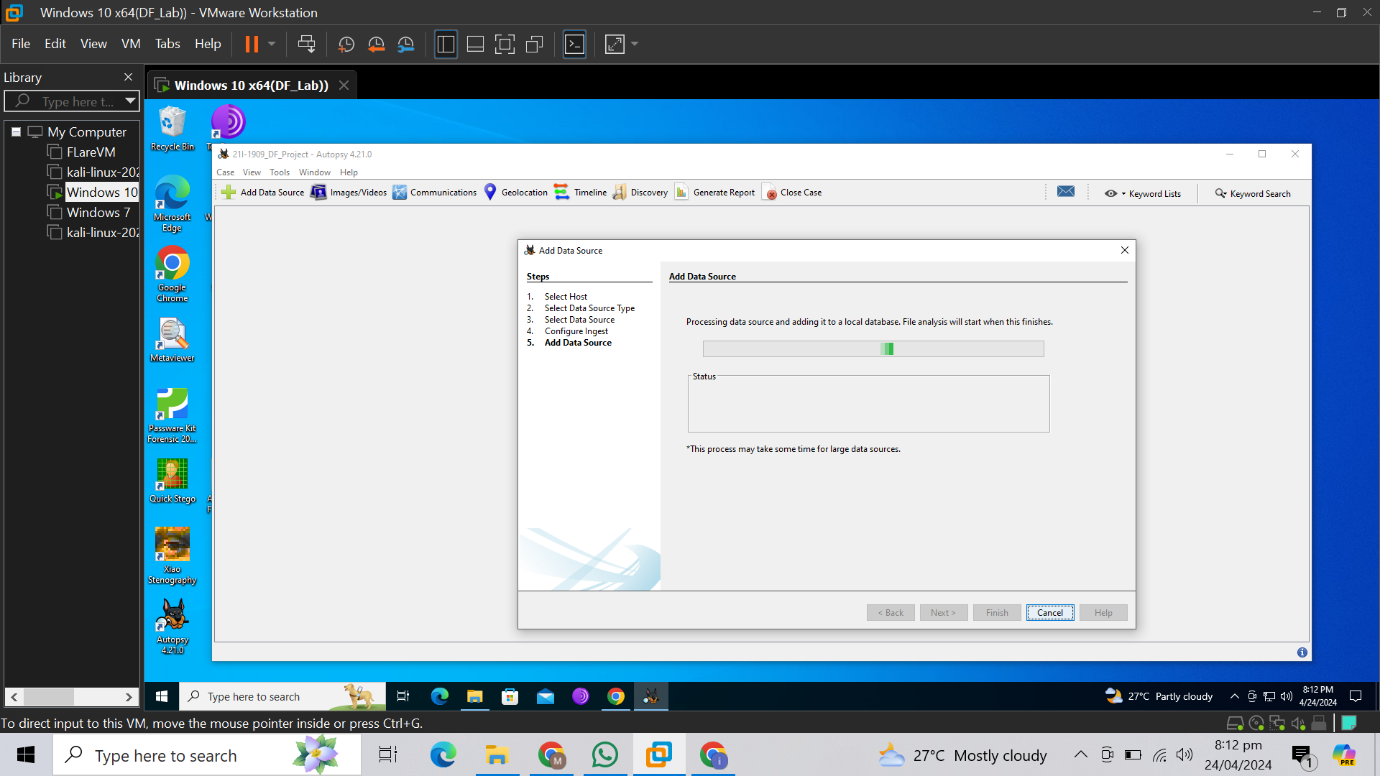
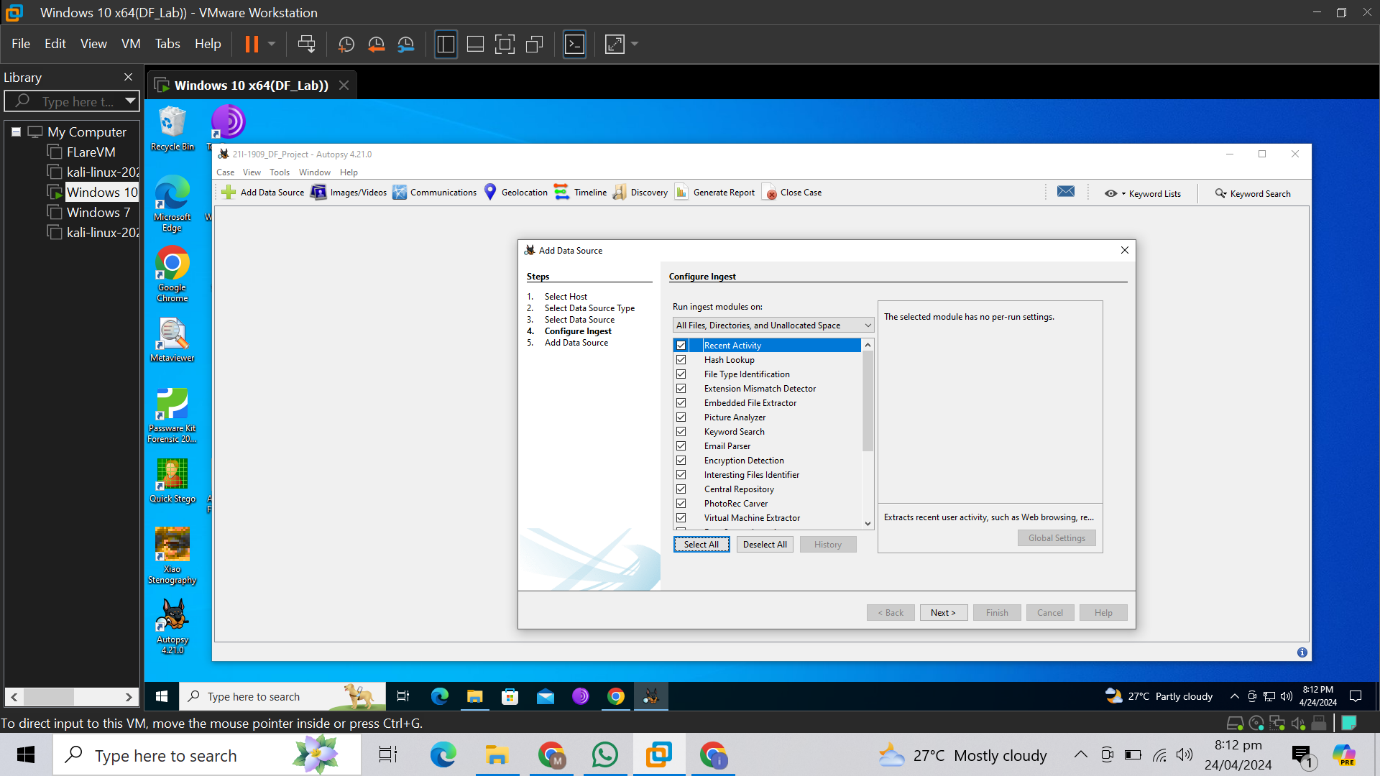




* Inserted the downloaded evidence file through selecting Disk or Image file option.



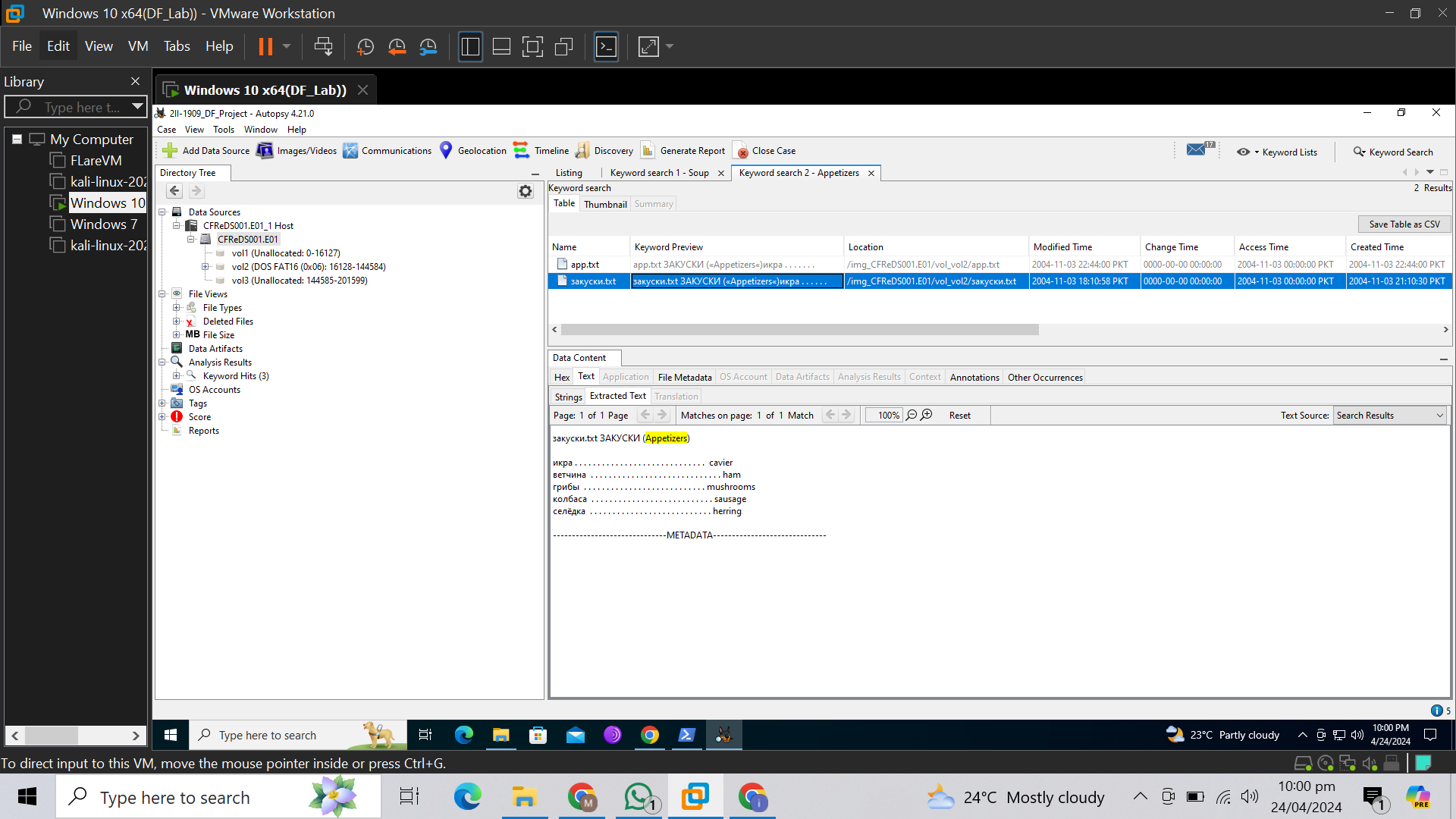
* Selected options to allow search for keywords in the case

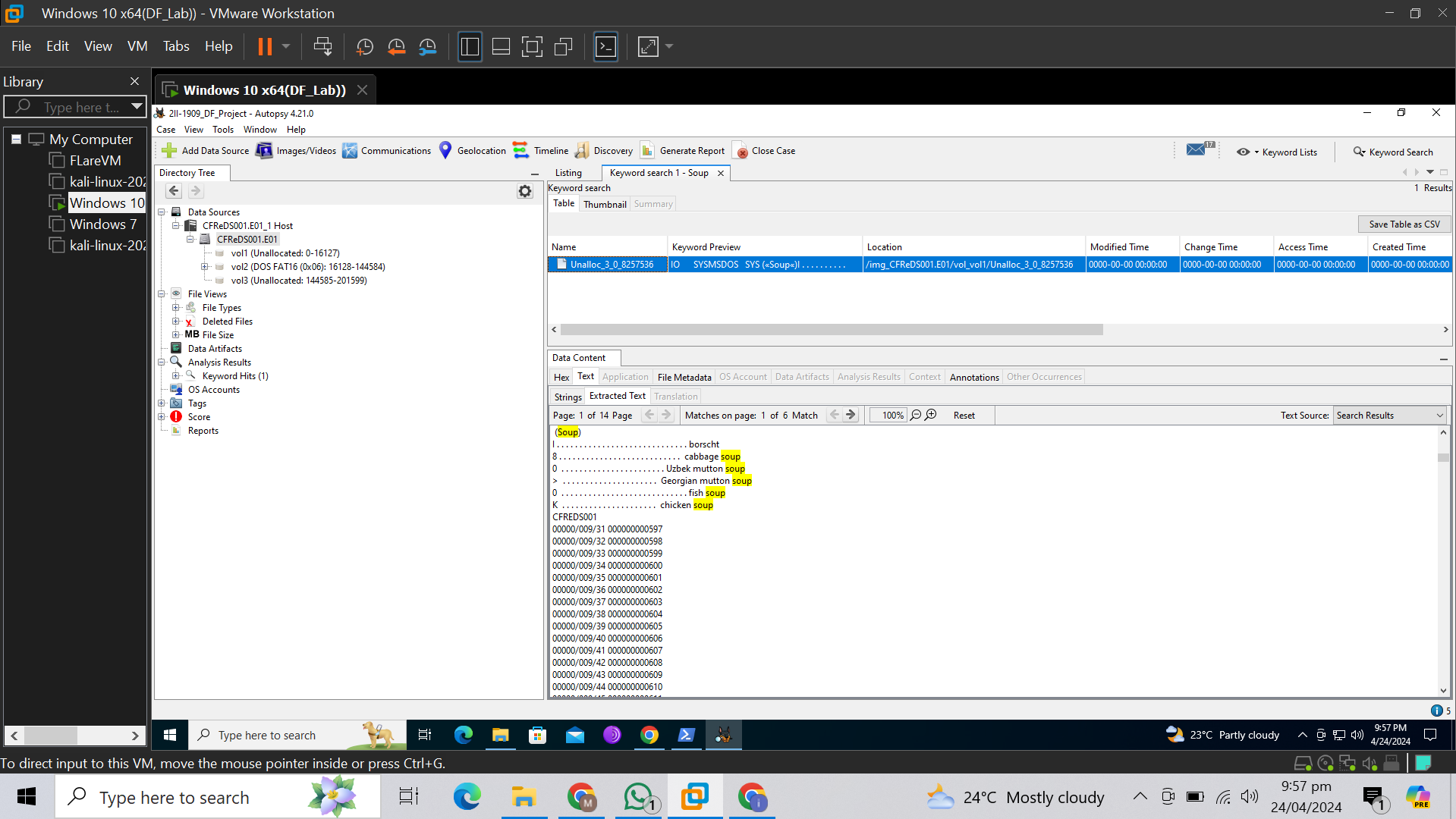


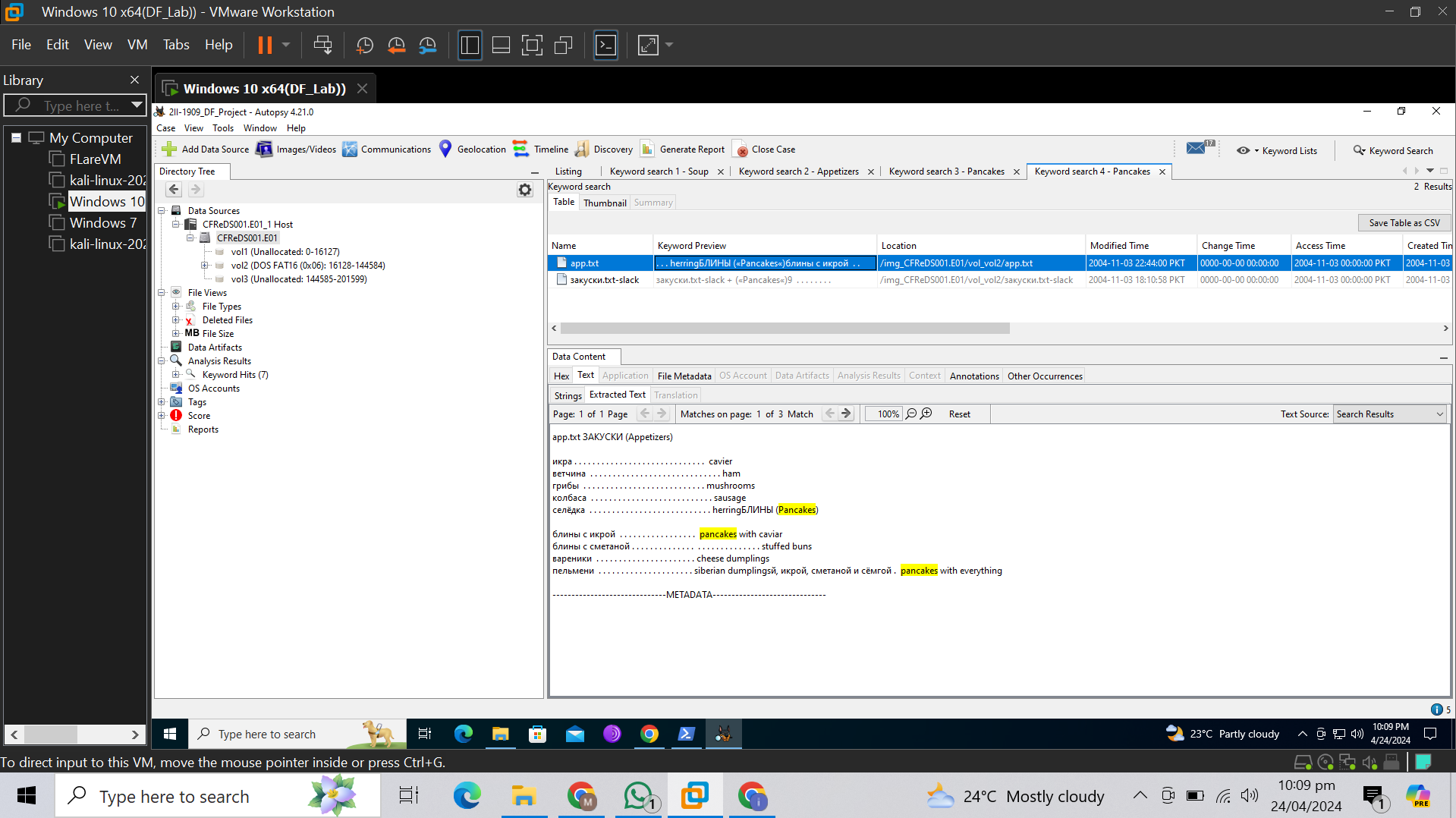
# **Finding Evidence**

* Searched the eight sections of menu in the file using keyword search

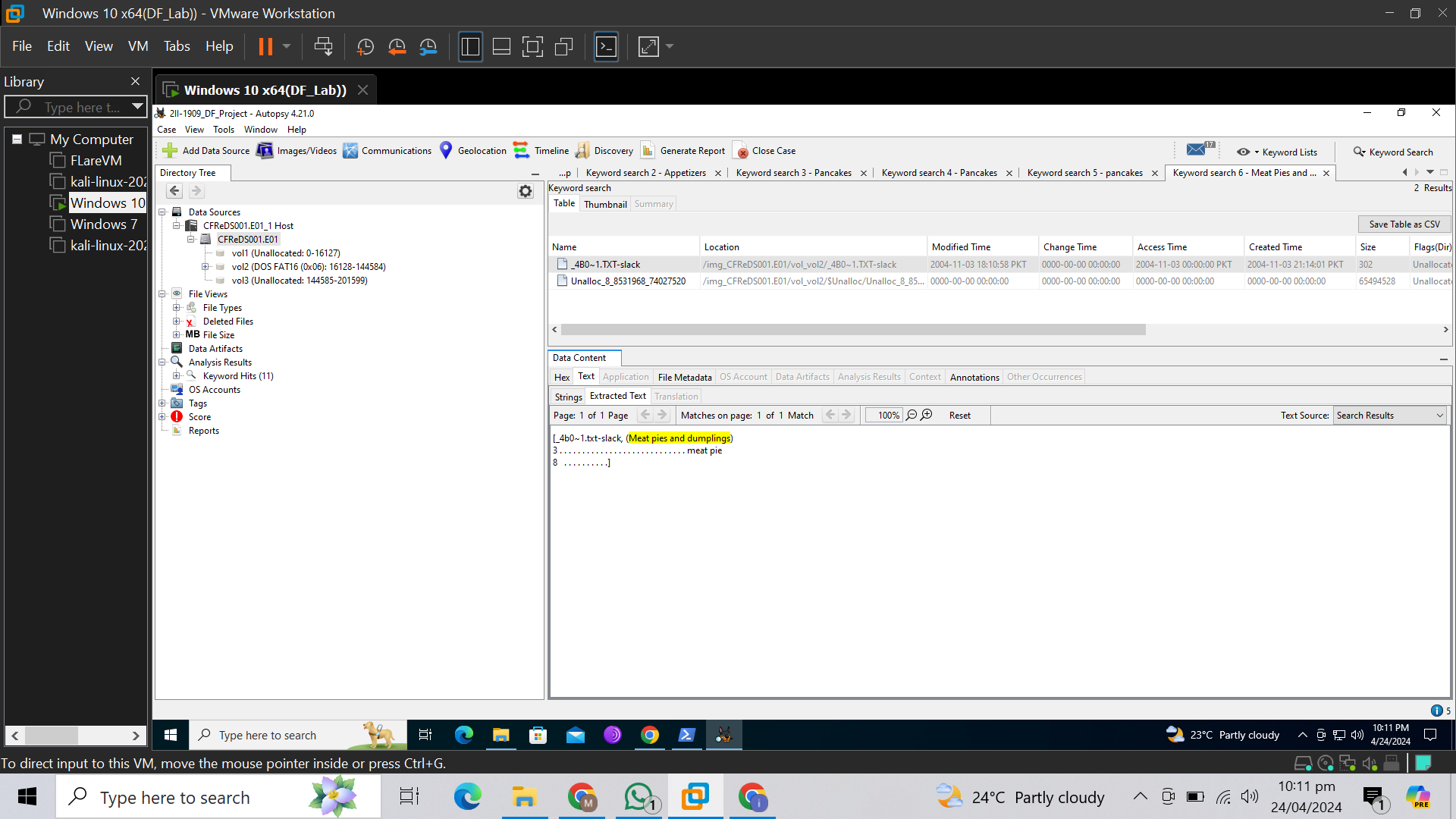
1. **ЗАКУСКИ (Appetizers)**



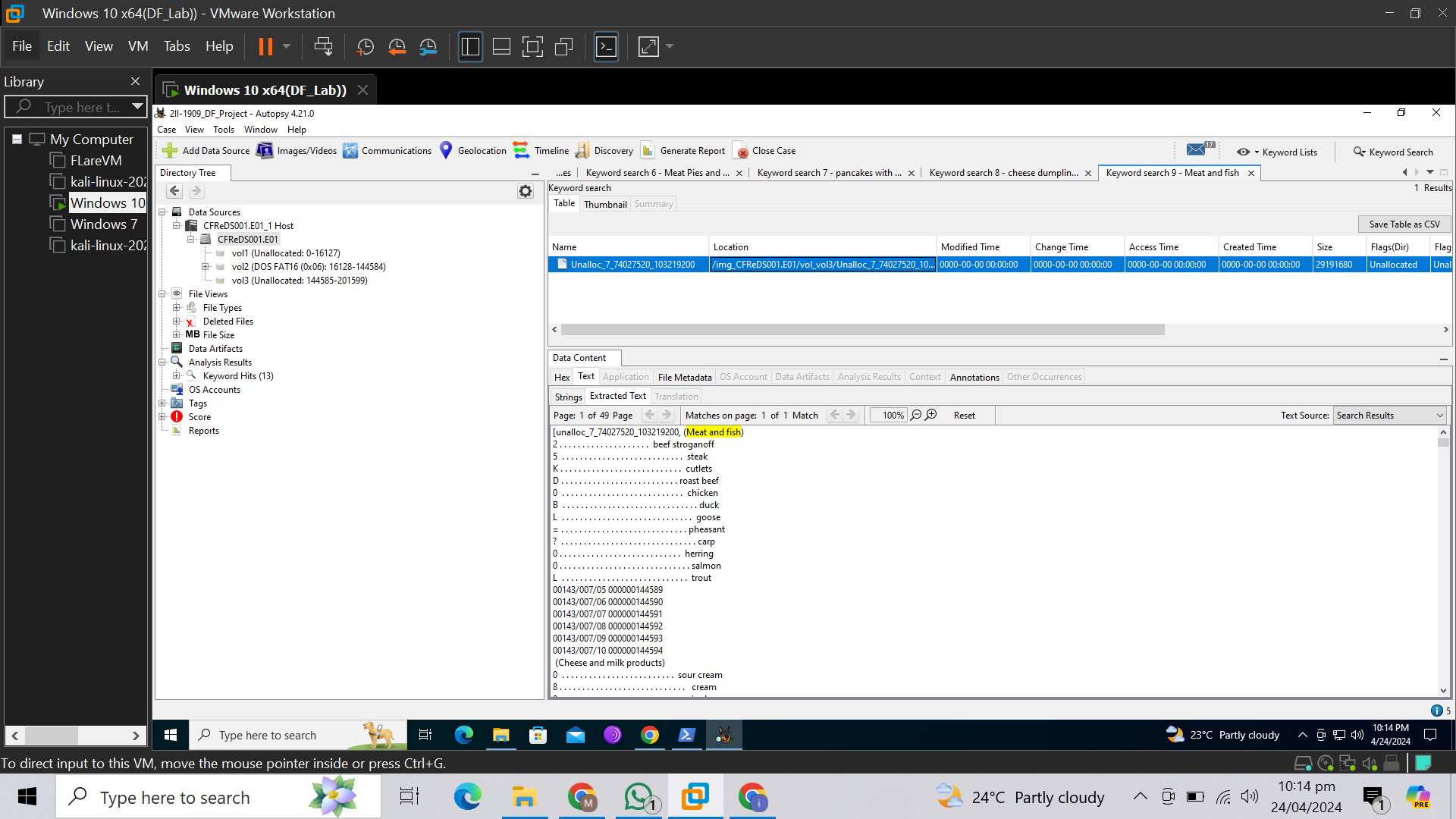
1. **СУП (Soup)**
2. **БЛИНЫ (Pancakes)**

****

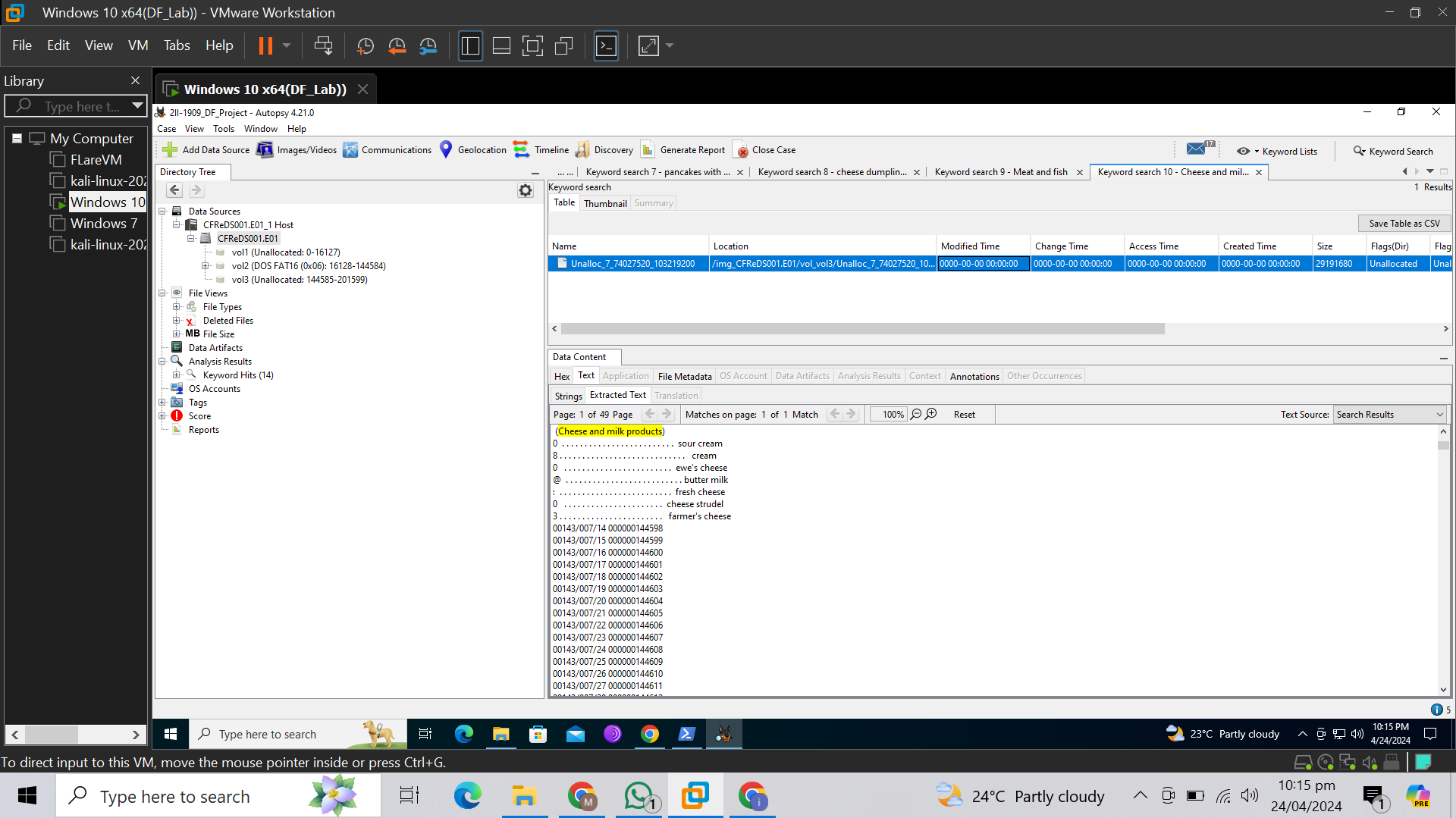
1. **ПИРОЖКИ И ПЕЛМЕНИ (Meat pies and dumplings)**

****

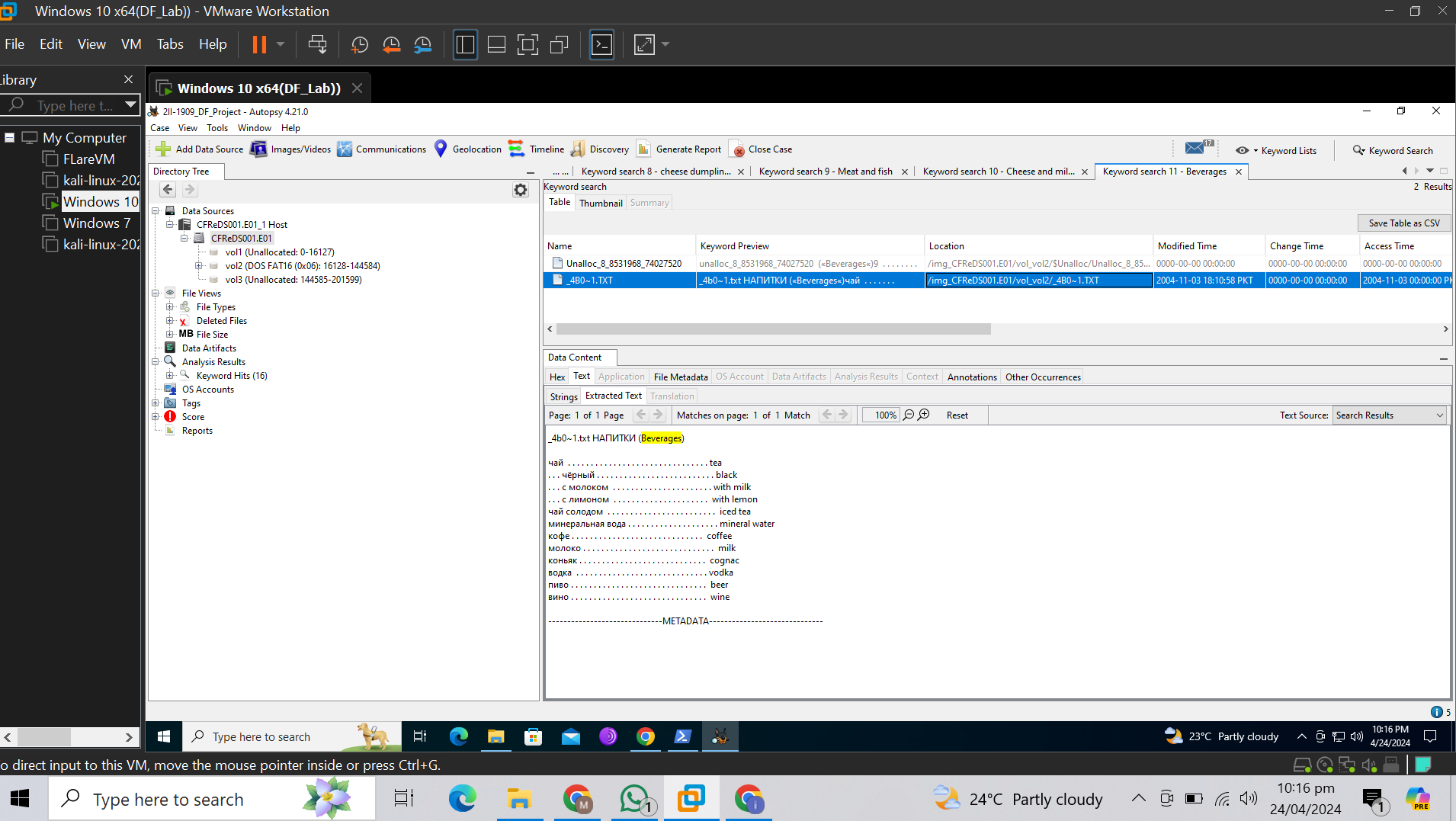
1. **МЯСО И РЫБА (Meat and fish)**

****

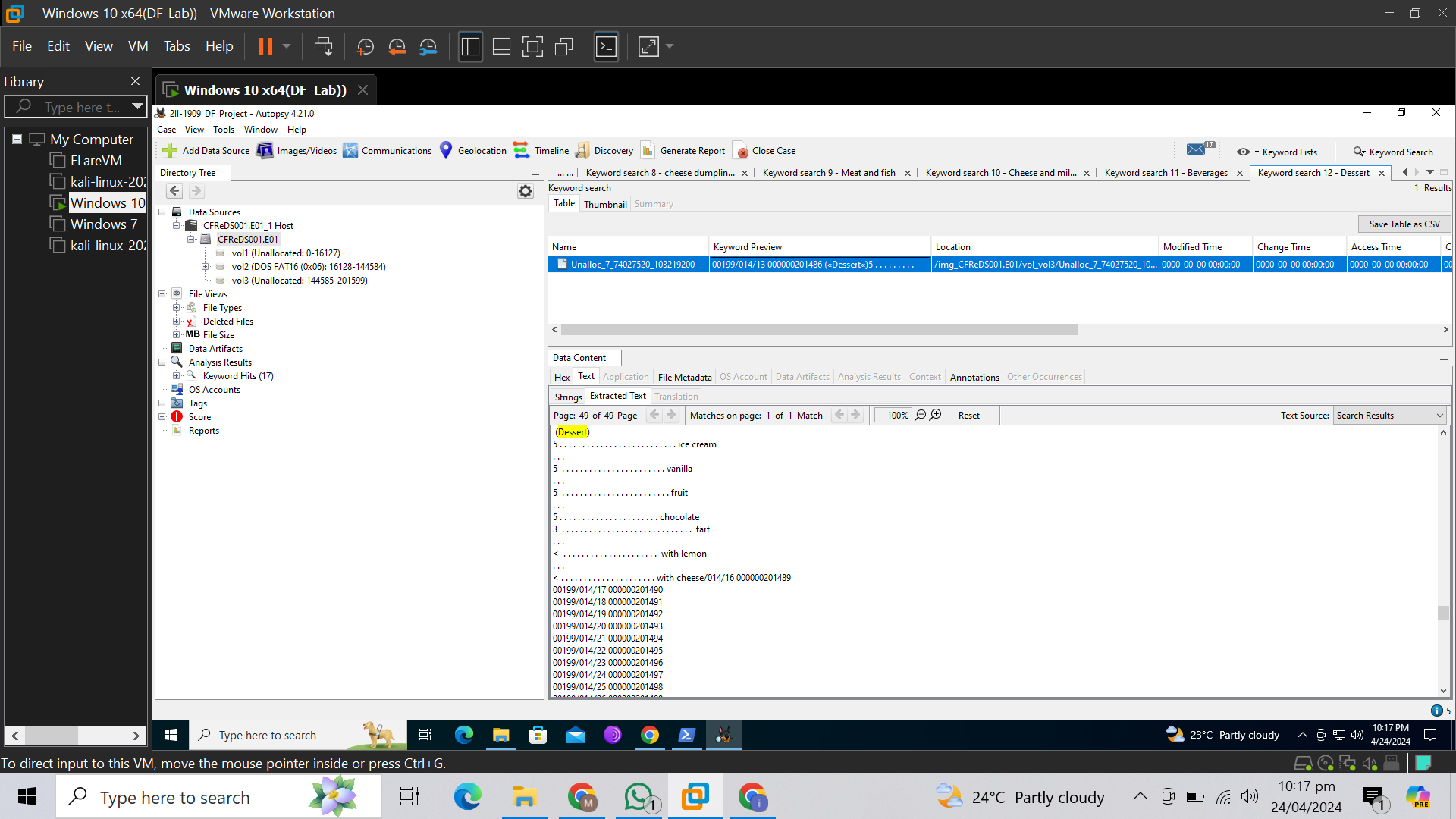
1. **СЫР И МОЛОЧНЫЕ (Cheese and milk products)**

****

1. **НАПИТКИ (Beverages)**

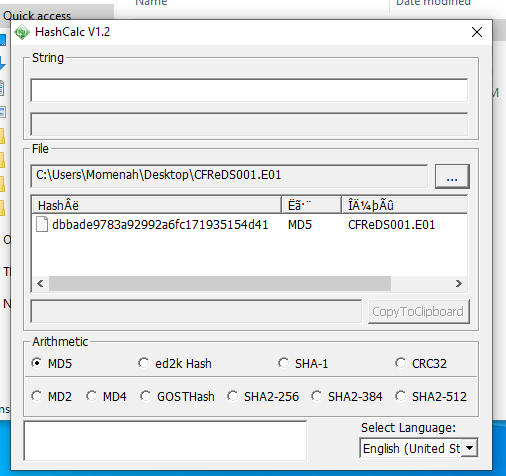
****

1. **СЛАДКОЕ (Dessert)**

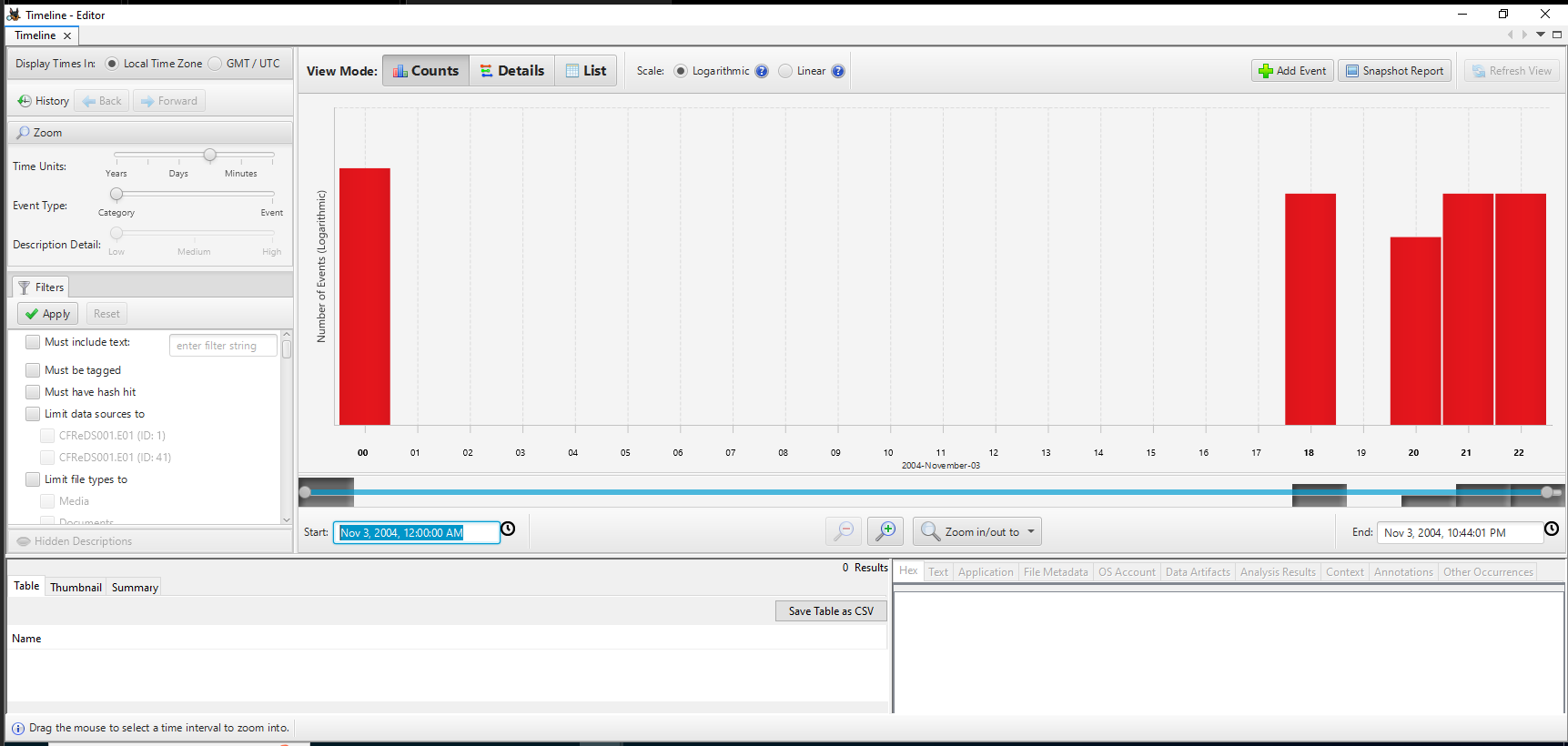
****

# **Other Information found**

* MD5 Hash



* TimeLine of the evidence file



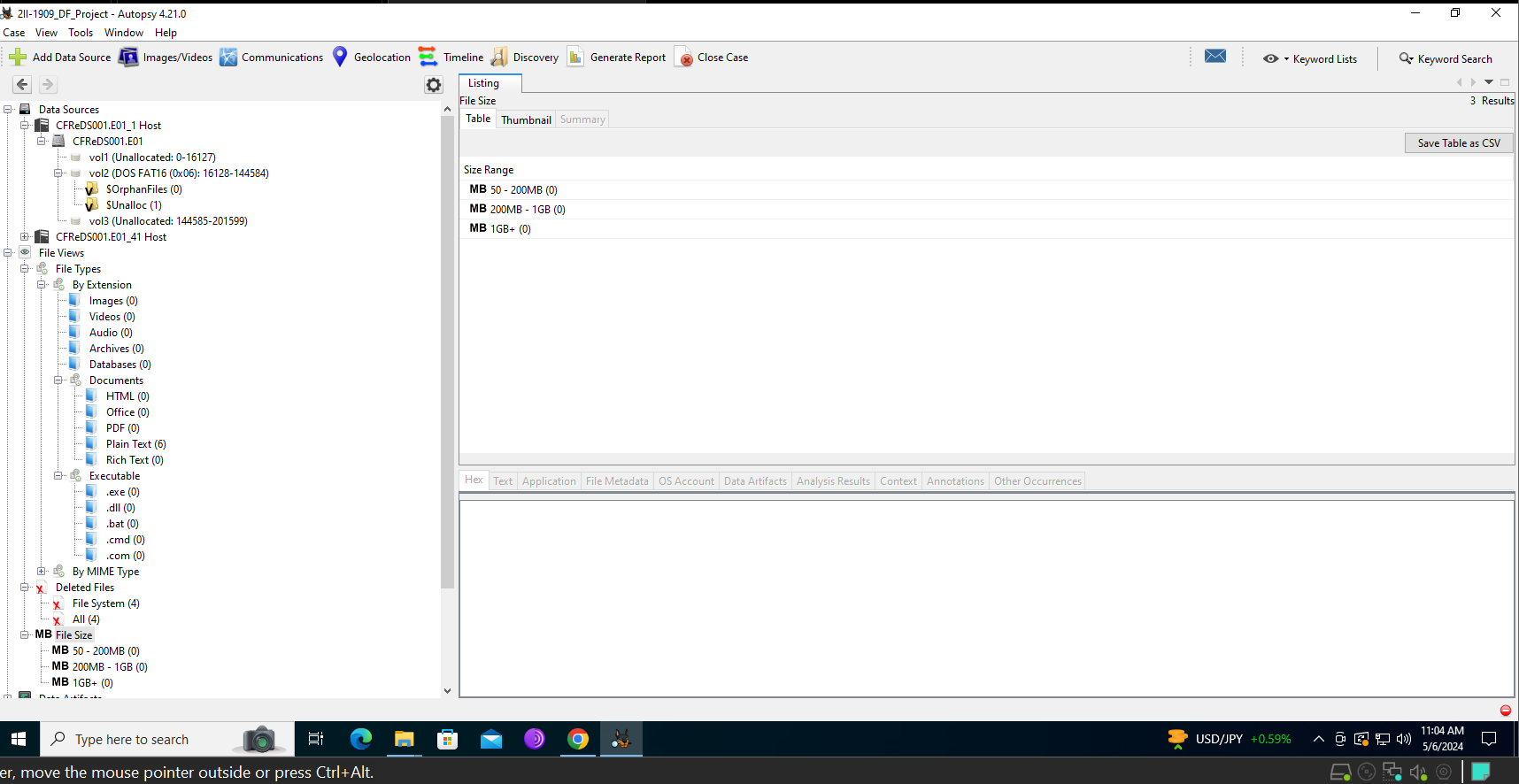
* Deleted files: They also contained the menu.



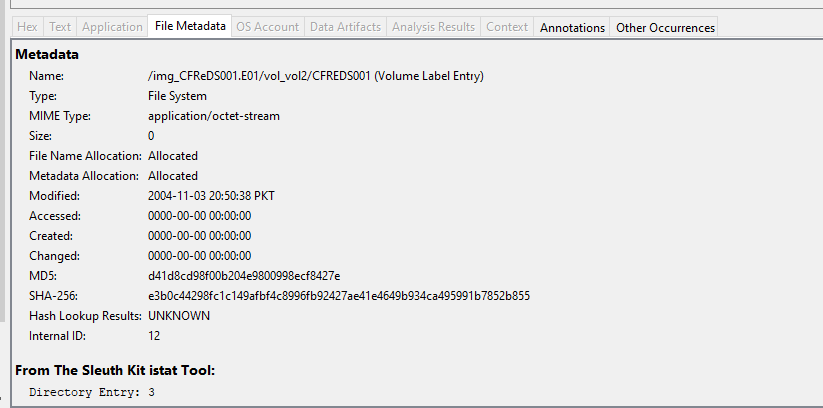
* Suspicious files: They also contained the menu



* File Size:



* Metadata



* **Name: CFREDS001:**

This is the name of the file.

* **Type: File System**

Indicates the type of the entry. In this case, it's a file system entry.

* **MIME Type: application/octet-stream**

MIME (Multipurpose Internet Mail Extensions) type specifies the format of the file's data. "application/octet-stream" is a generic binary file.

* **Size: 0**

Size of the file in bytes. Here, it's 0, meaning the file is empty or contains no data.

* **File Name Allocation: Allocated**

Indicates whether the file name is allocated (exists).

* **Metadata Allocation: Allocated**

Indicates whether metadata (data about the file) is allocated (exists).

* **Modified: 2004-11-03 20:50:38 PKT**

Timestamp indicating when the file's content was last modified, in this case, November 3, 2004, at 20:50:38 PKT (Pakistan Standard Time).

* **Accessed: 0000-00-00 00:00:00**

Timestamp indicating when the file was last accessed. In this case, it's not available (0000-00-00 00:00:00).

* **Created: 0000-00-00 00:00:00**

Timestamp indicating when the file was created. In this case, it's not available (0000-00-00 00:00:00).

* **Changed: 0000-00-00 00:00:00**

Timestamp indicating when the file was last changed. In this case, it's not available (0000-00-00 00:00:00).

* **MD5: d41d8cd98f00b204e9800998ecf8427e**

MD5 hash of the file's content. In this case, it's a well-known hash for an empty file.

* **SHA-256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855**

SHA-256 hash of the file's content. Again, for an empty file, this hash is a well-known value.

* **Hash Lookup Results: UNKNOWN**

Indicates that the hash values are not recognized or known.

* **Internal ID: 12**

An internal identifier for the file.

* **From The Sleuth Kit istat Tool: Directory Entry: 3**

Information regarding the directory entry.

* **Sectors: (not provided)**

Typically, this section would contain information about the sectors on the storage device where the file's data is stored.