Цель задания

Изучить и использовать утилиту Autopsy для анализа локального жесткого диска и извлечения цифровых доказательств.

**Шаг 1:**

Autopsy это программа с открытым исходным кодом, которая используется для выполнения криминалистических операций с жесткими дисками и смартфонами. Этот инструмент применяется: правоохранительными органами местной полицией корпоративными отделами безопасности.

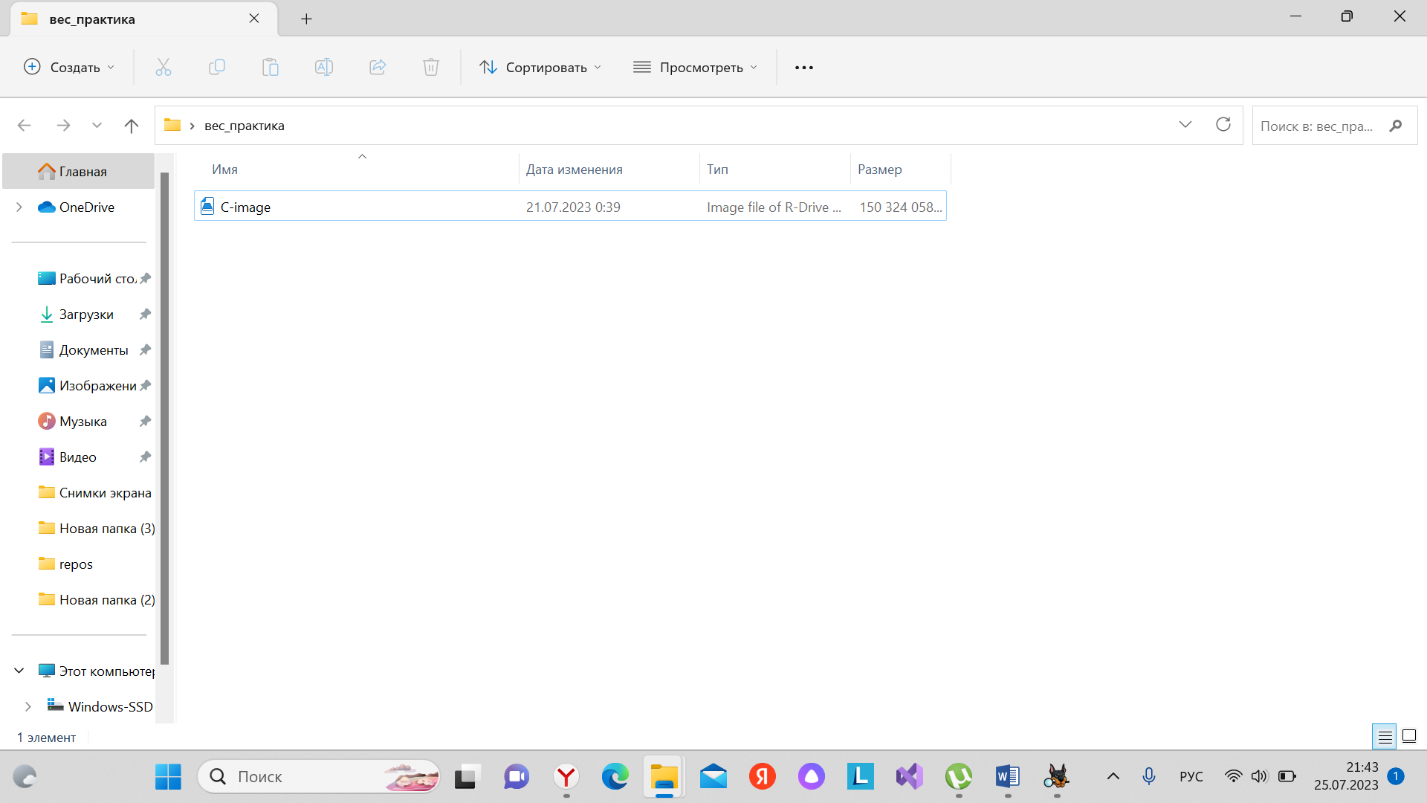
Основное предназначение программы – расследование улик киберпреступлений, но также Autopsy может использоваться для восстановления удаленной информации.

Ее можно скачать на официальном сайте.

**Шаг 2:**

**Задача:**

Создать образ (image) локального жесткого диска, который будет использоваться для анализа в Autopsy.

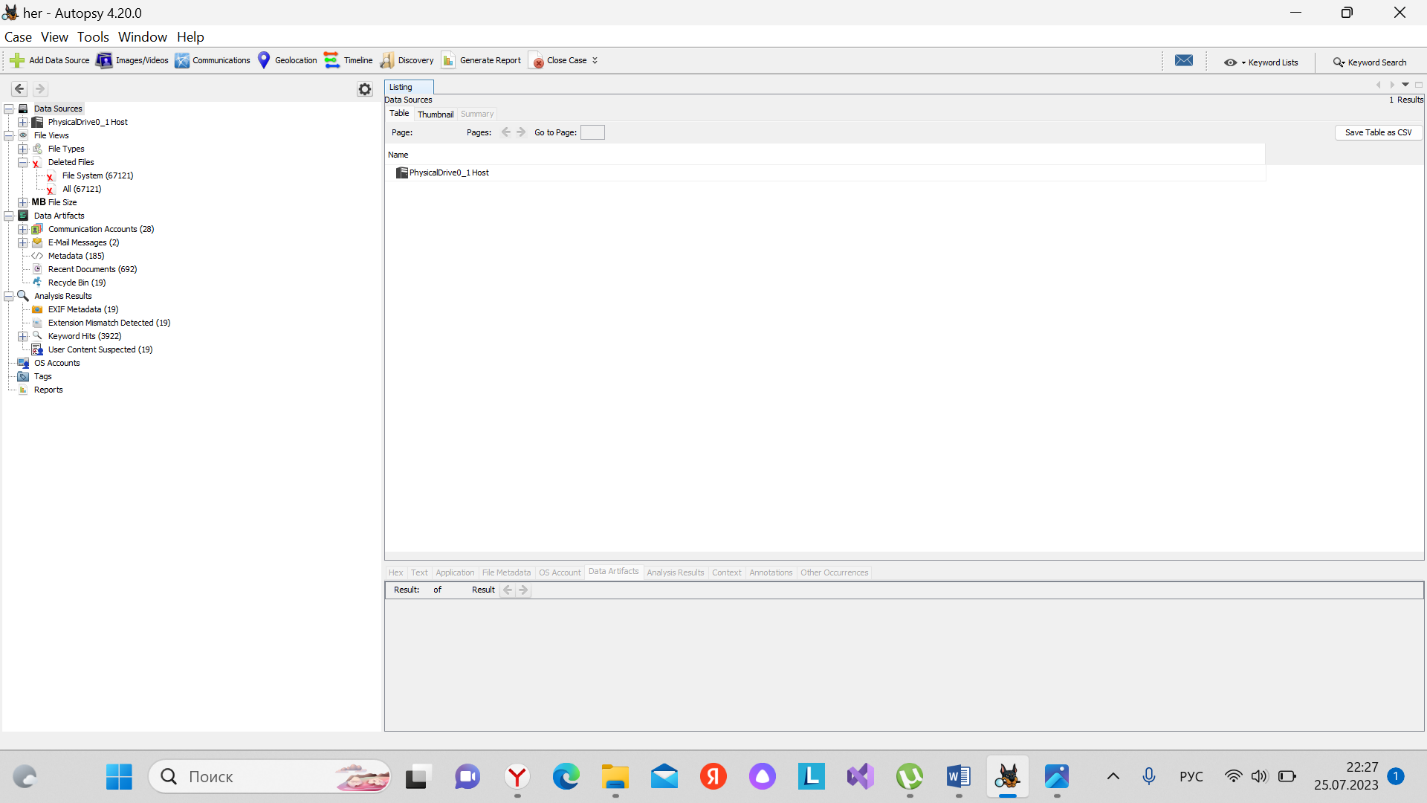
**Реализация:** Для создания образа диска была использована программа R Drive Image*.* Образ создавался для локального диска С, из которого занятый объем: 150 гб. 

**Шаг 3:**

**Задача:**

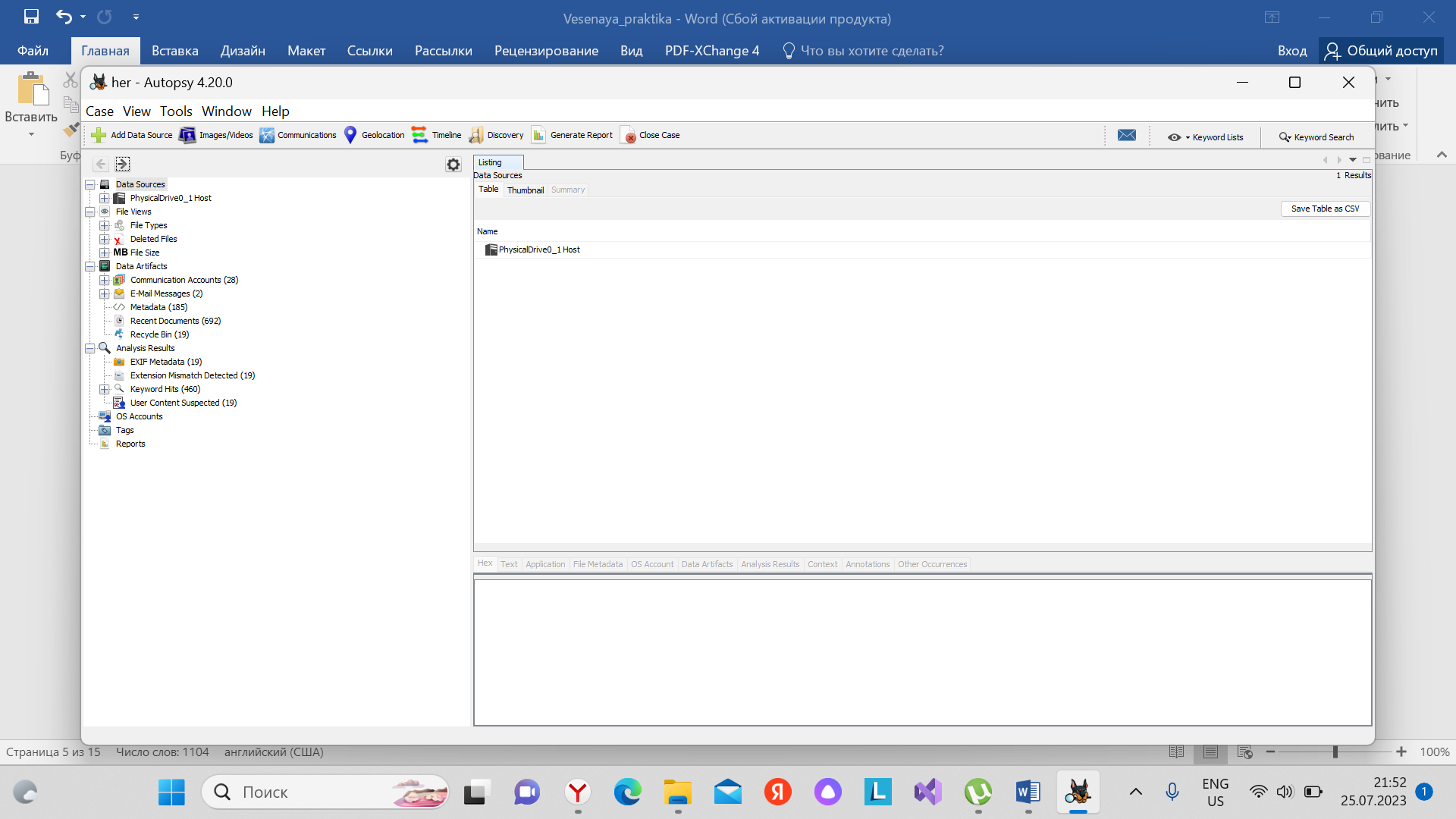
Запустите Autopsy и импортируйте созданный образ локального жесткого диска размером.

**Реализация:**

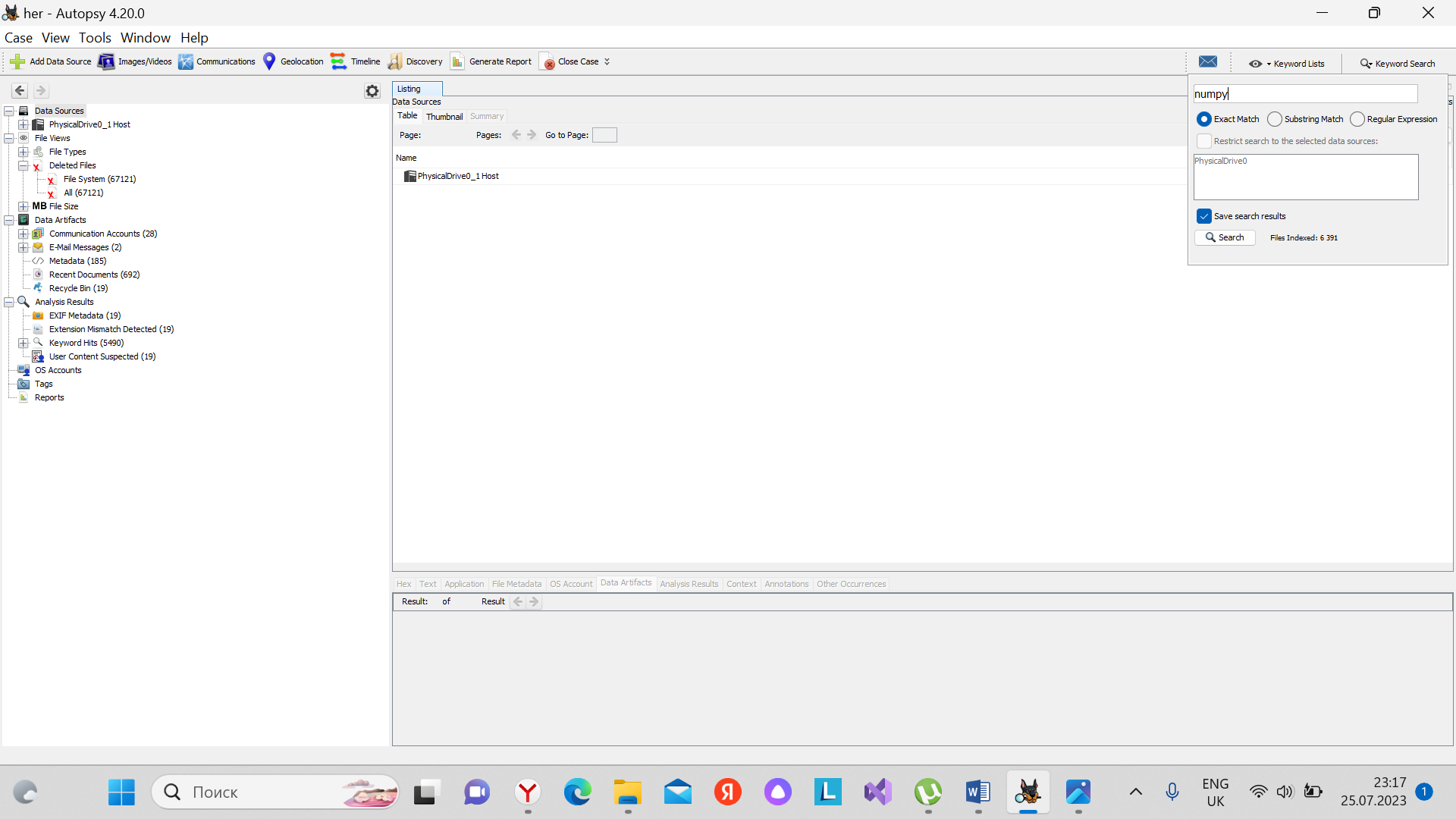
Образ диска не читался программой, выводилась ошибка. Поэтому пришлось использовать оригинал.

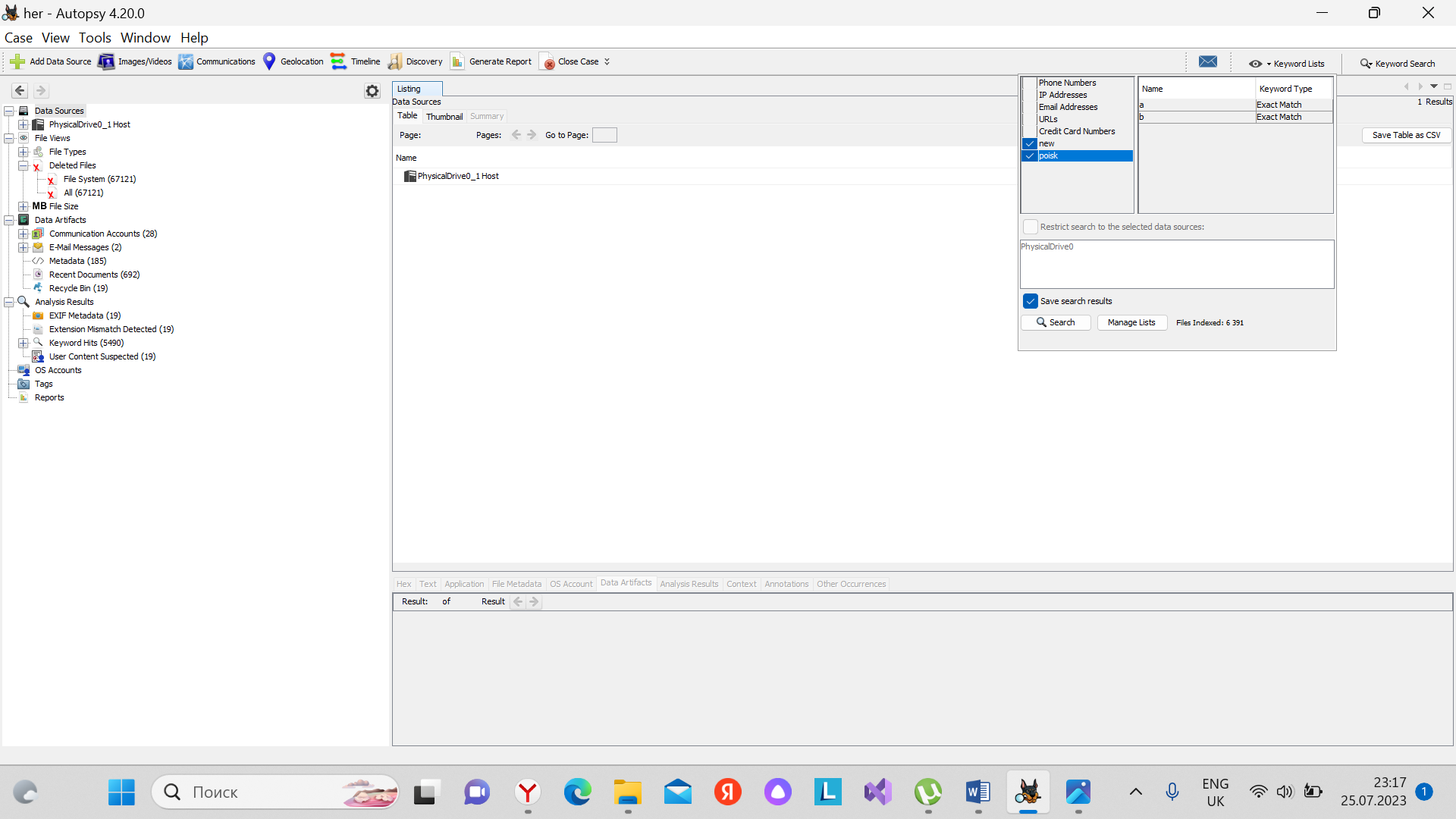
**Шаг 4:**

Просмотр файловой системы и структуры образа

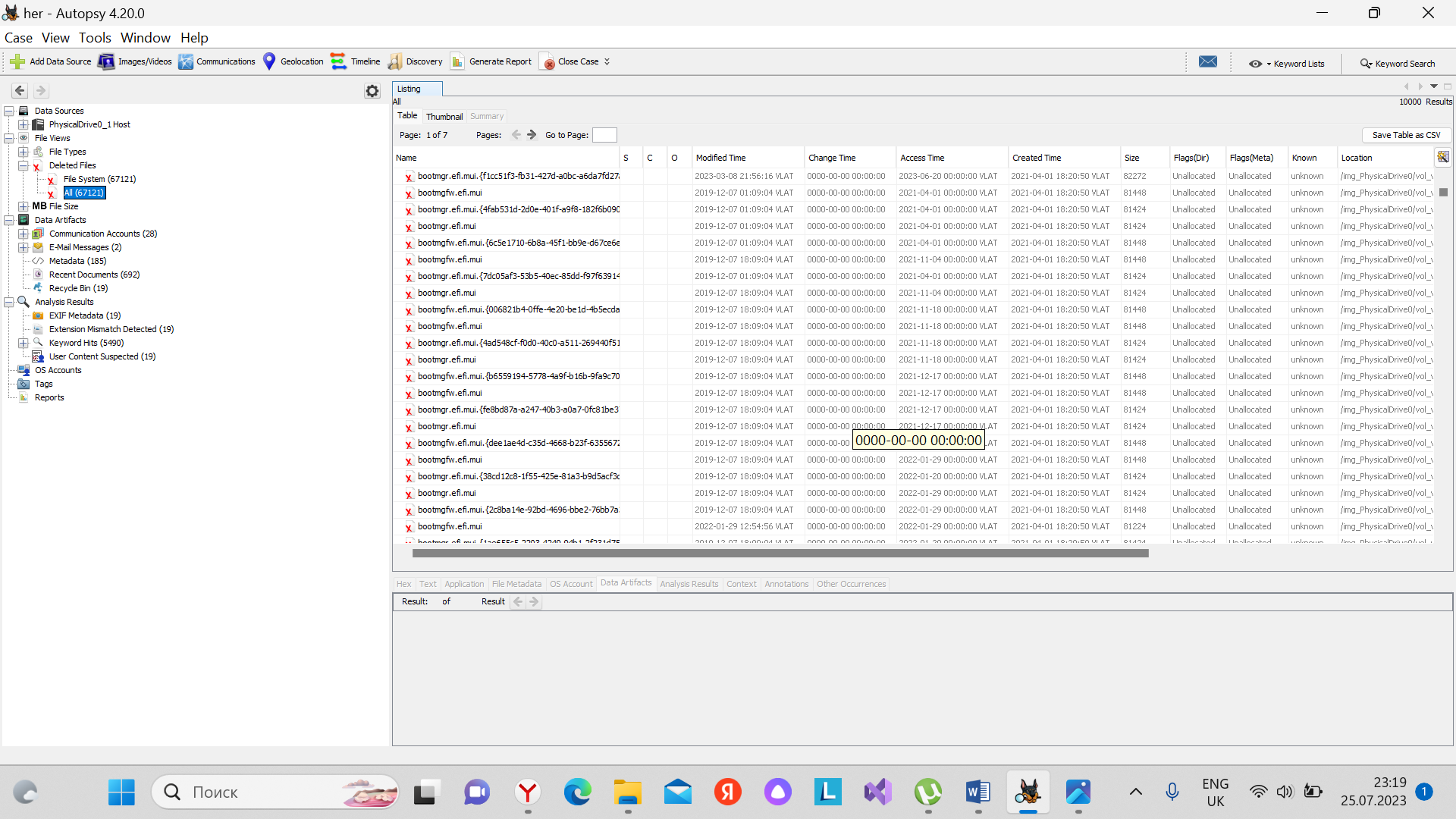
****

Поиск и фильтрация файлов и метаданных

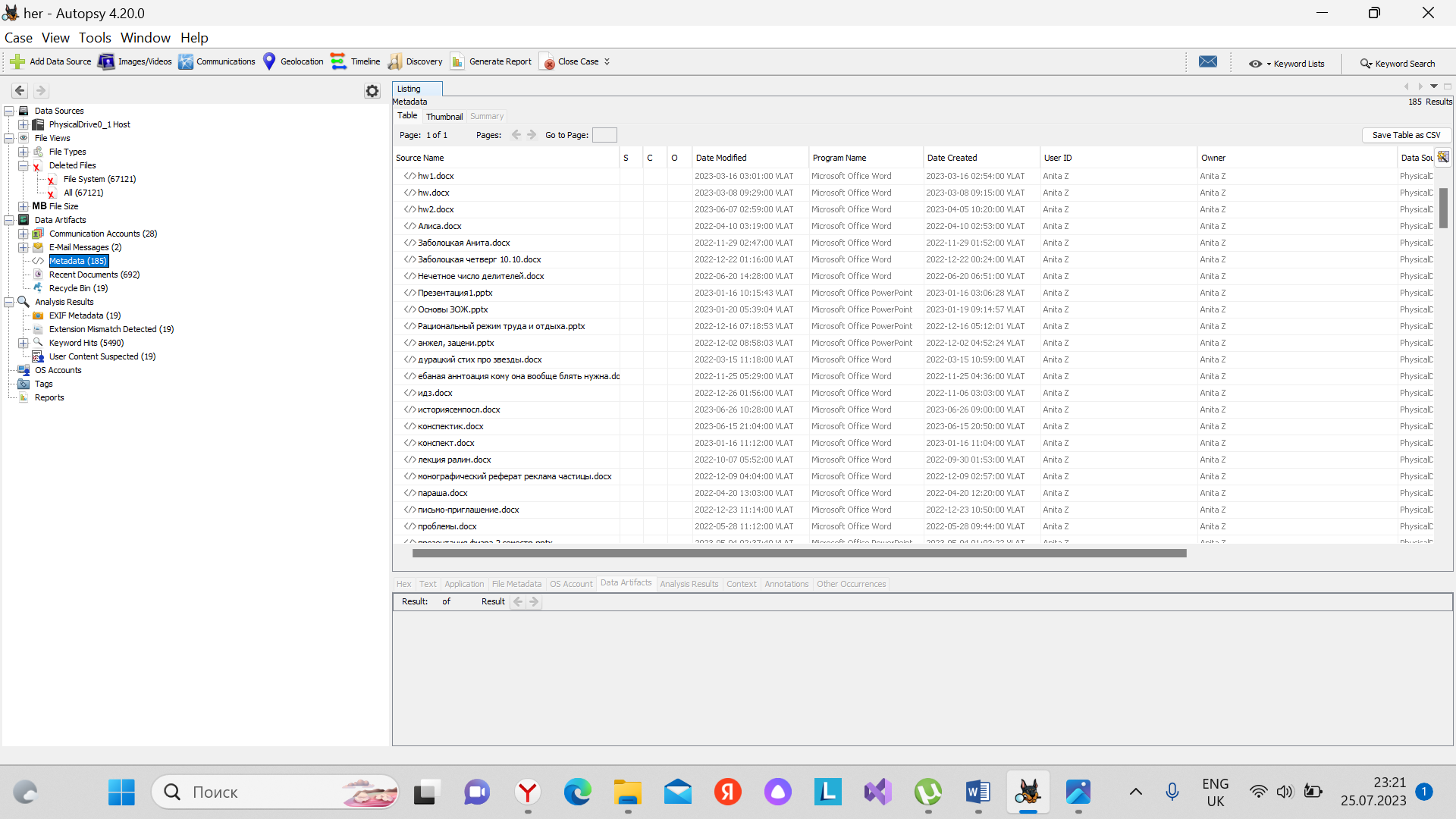
****

****

Анализ и восстановление удаленных файлов.

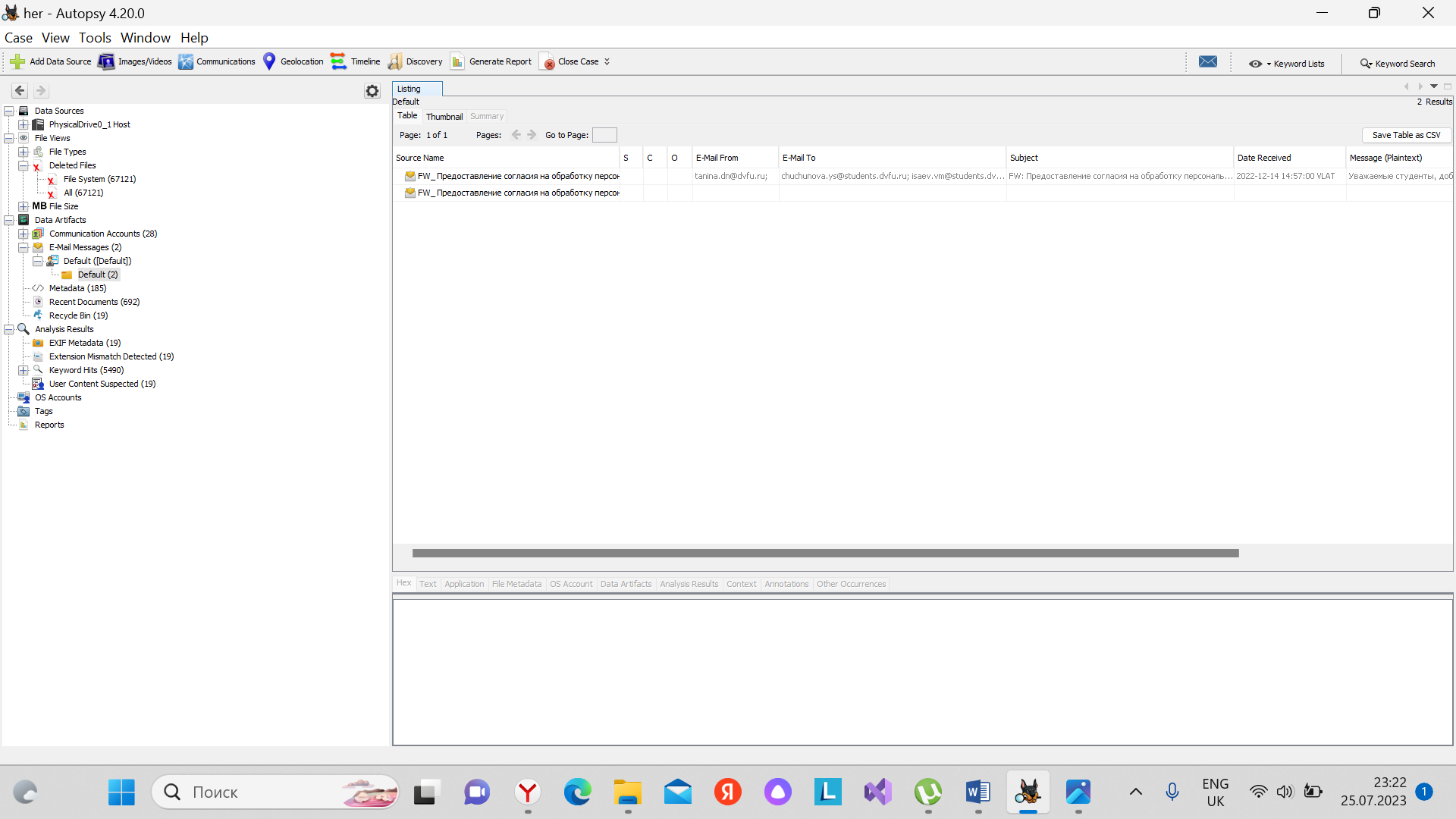


Извлечение и анализ метаданных файлов.

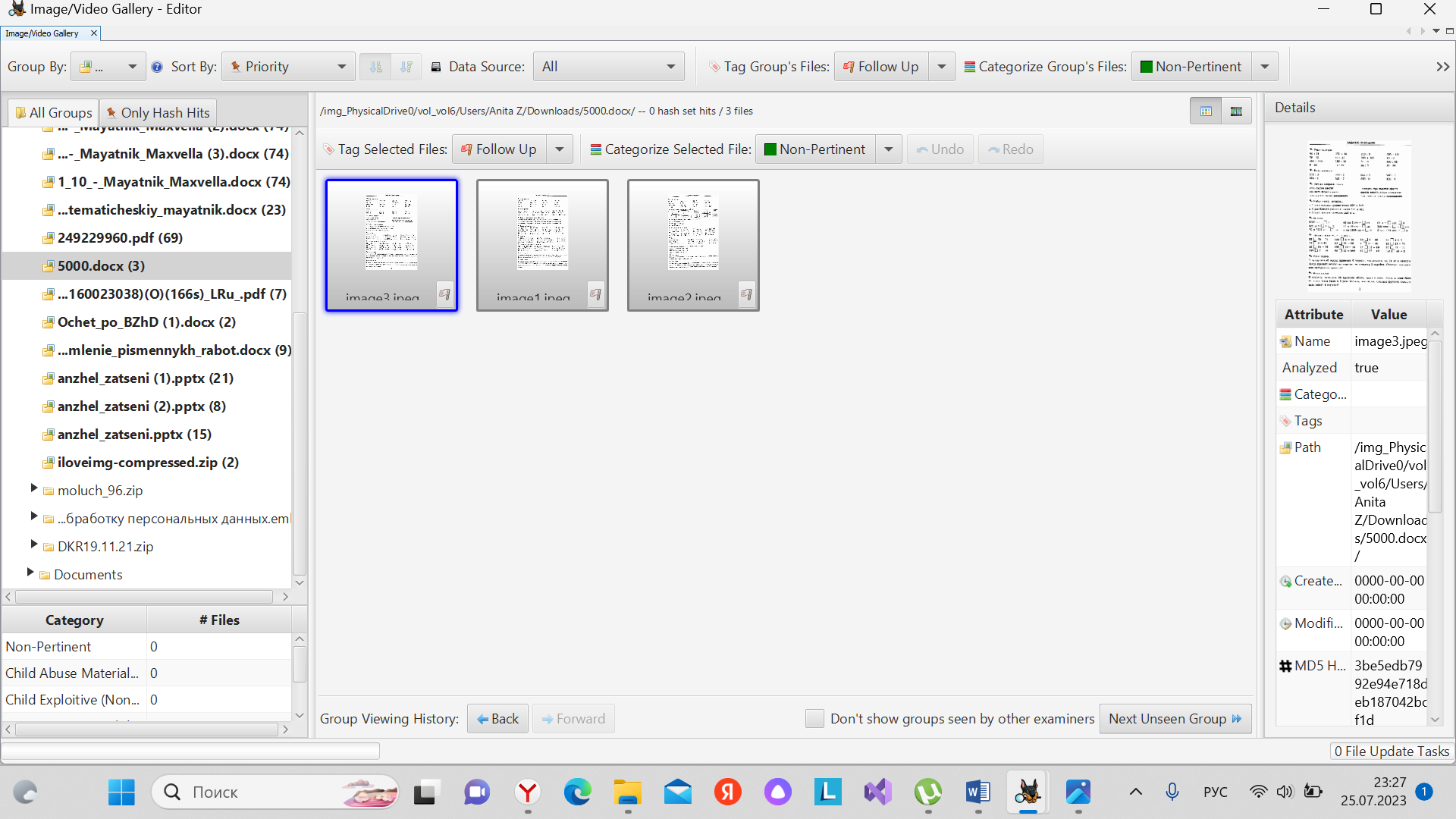


Просмотр и анализ истории веб-браузеров, электронной почты и других

Приложений. К сожалению, историю браузеров на этом ноутбуке сразу после покупки поставила «не сохранять».



Поиск и анализ медиафайлов (изображения, видео)



**Шаг 5:**

**Задача:**

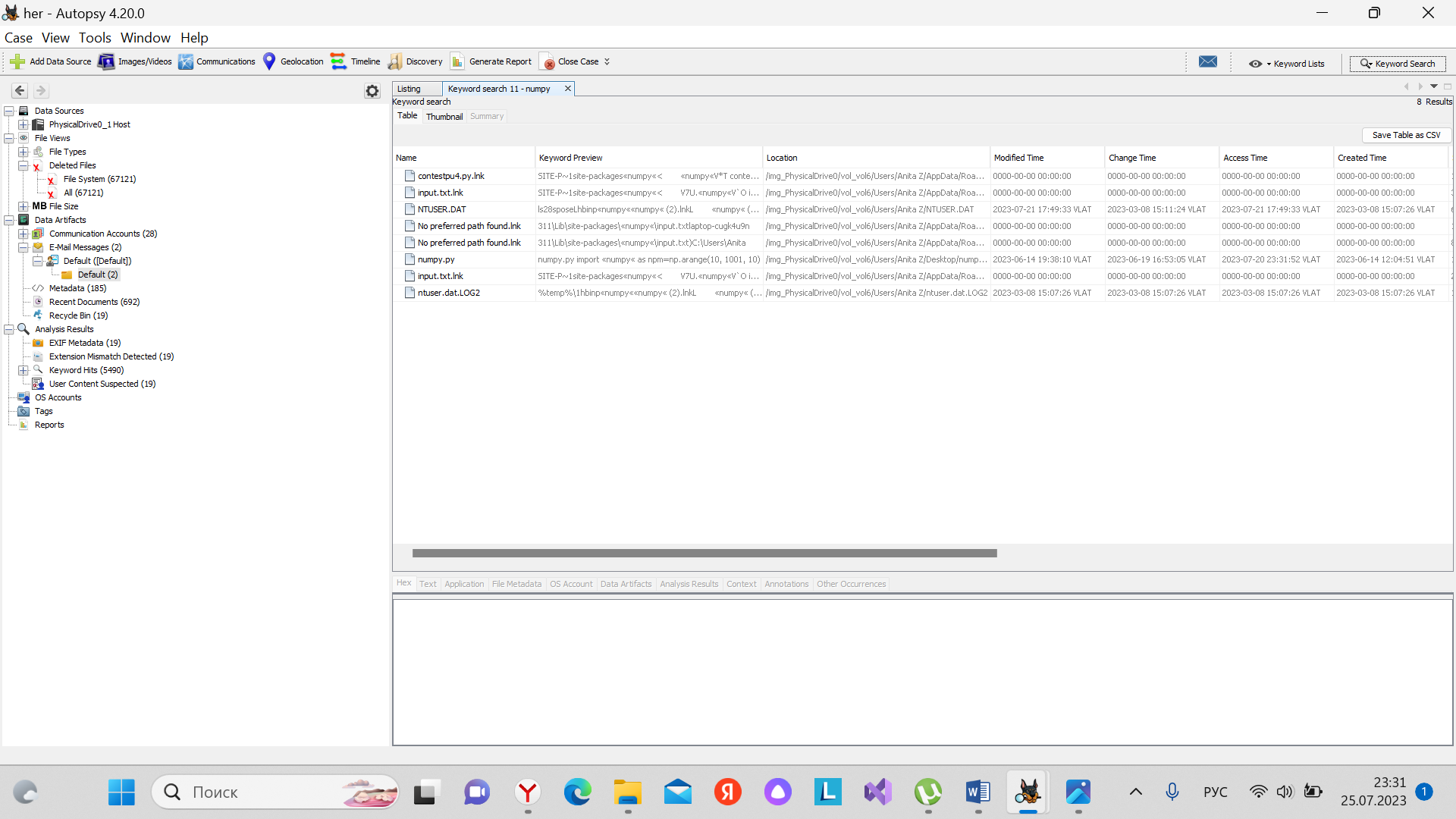
Проанализируйте образ жесткого диска, используя различные функции и возможности утилиты Autopsy.

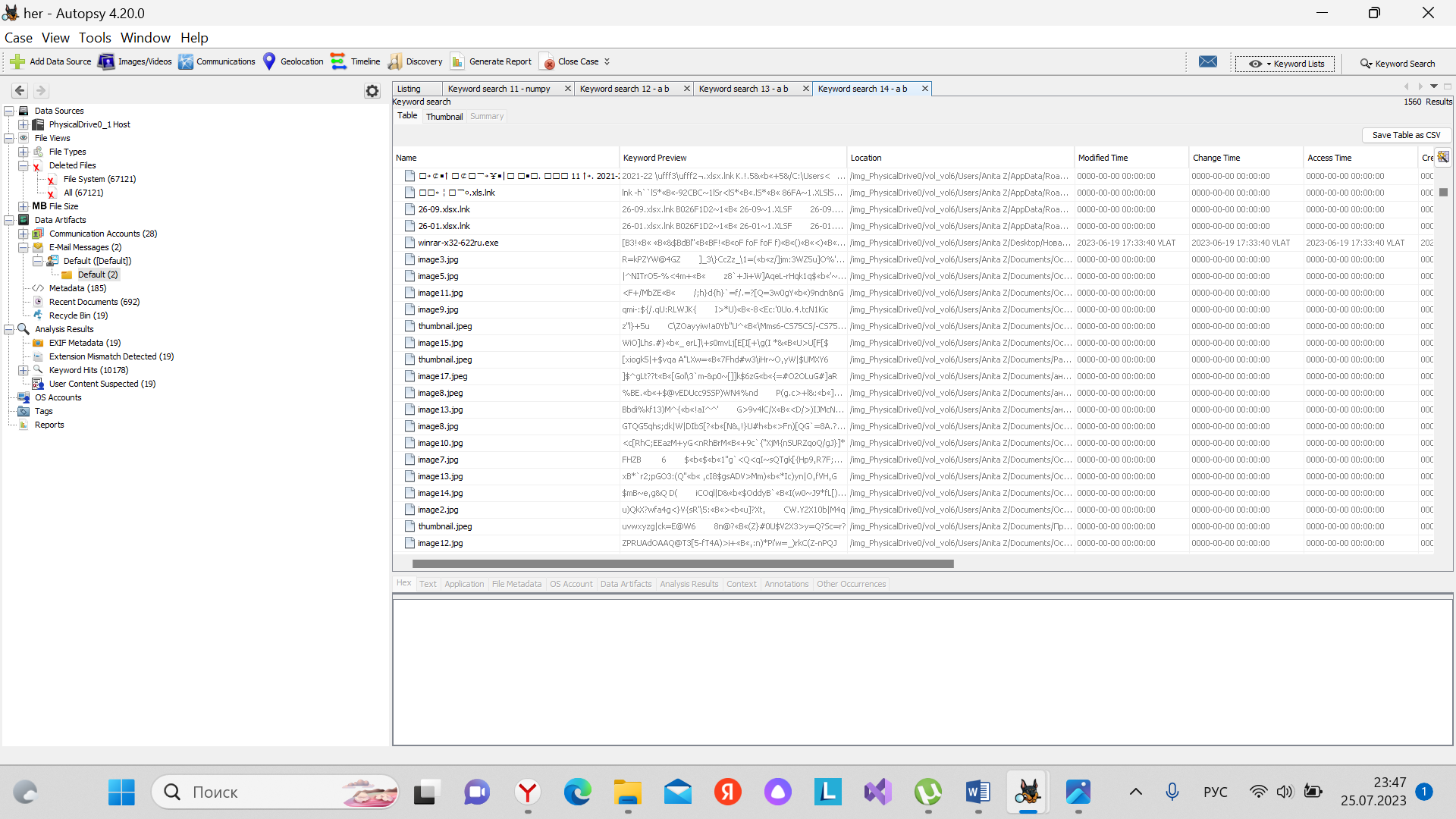
**Реализация:**

a) Выполните основные операции анализа, включая поиск, фильтрацию и восстановление файлов.

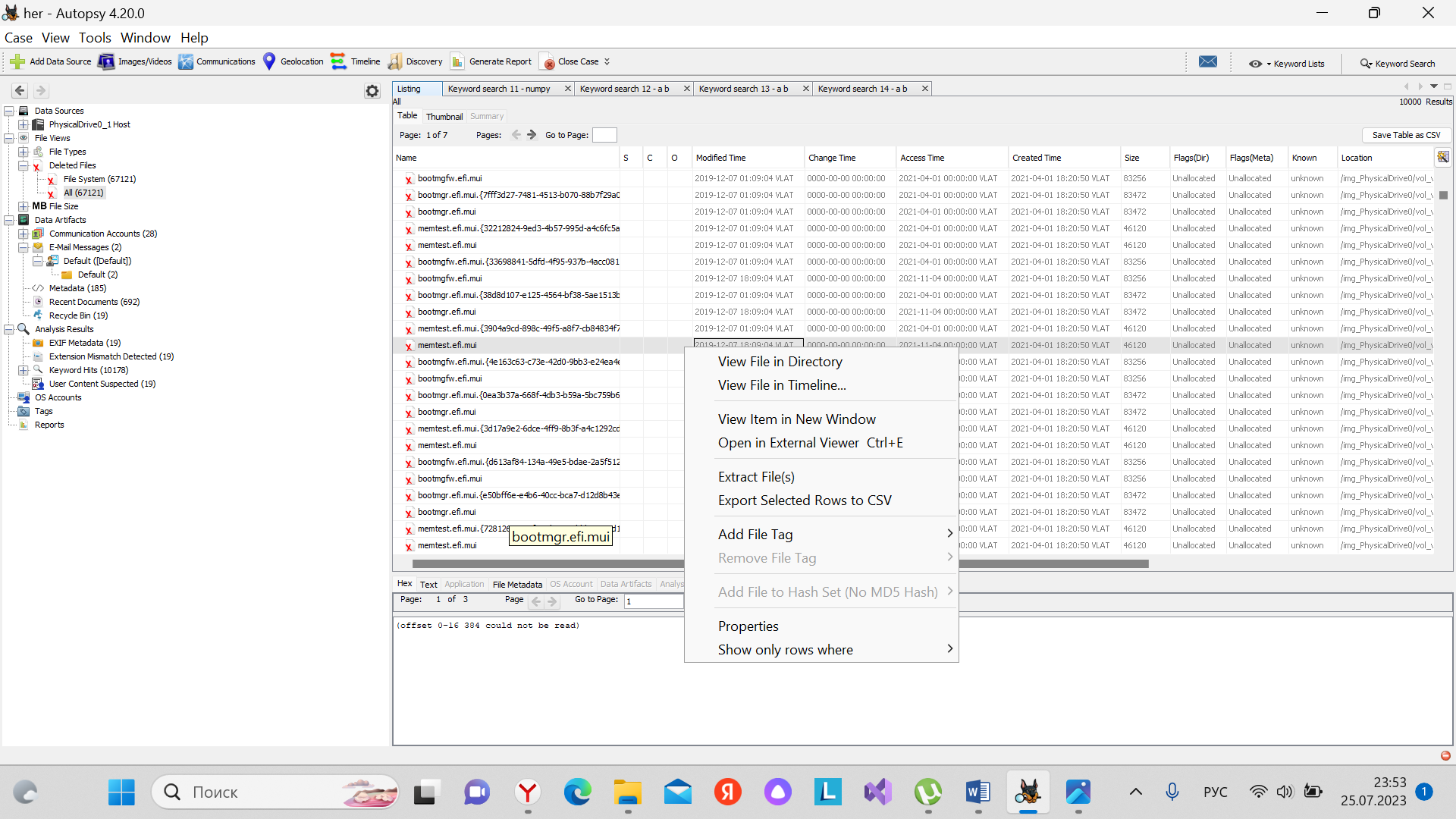
Поиск выполняется по поиску ключевых слов или создания листа с ключевыми словами, может осуществляться по точному совпадению, по электронной почте или по регулярным выражениям.

В *Keyword search* введено слово numpy и программа нашла 9 совпадений.



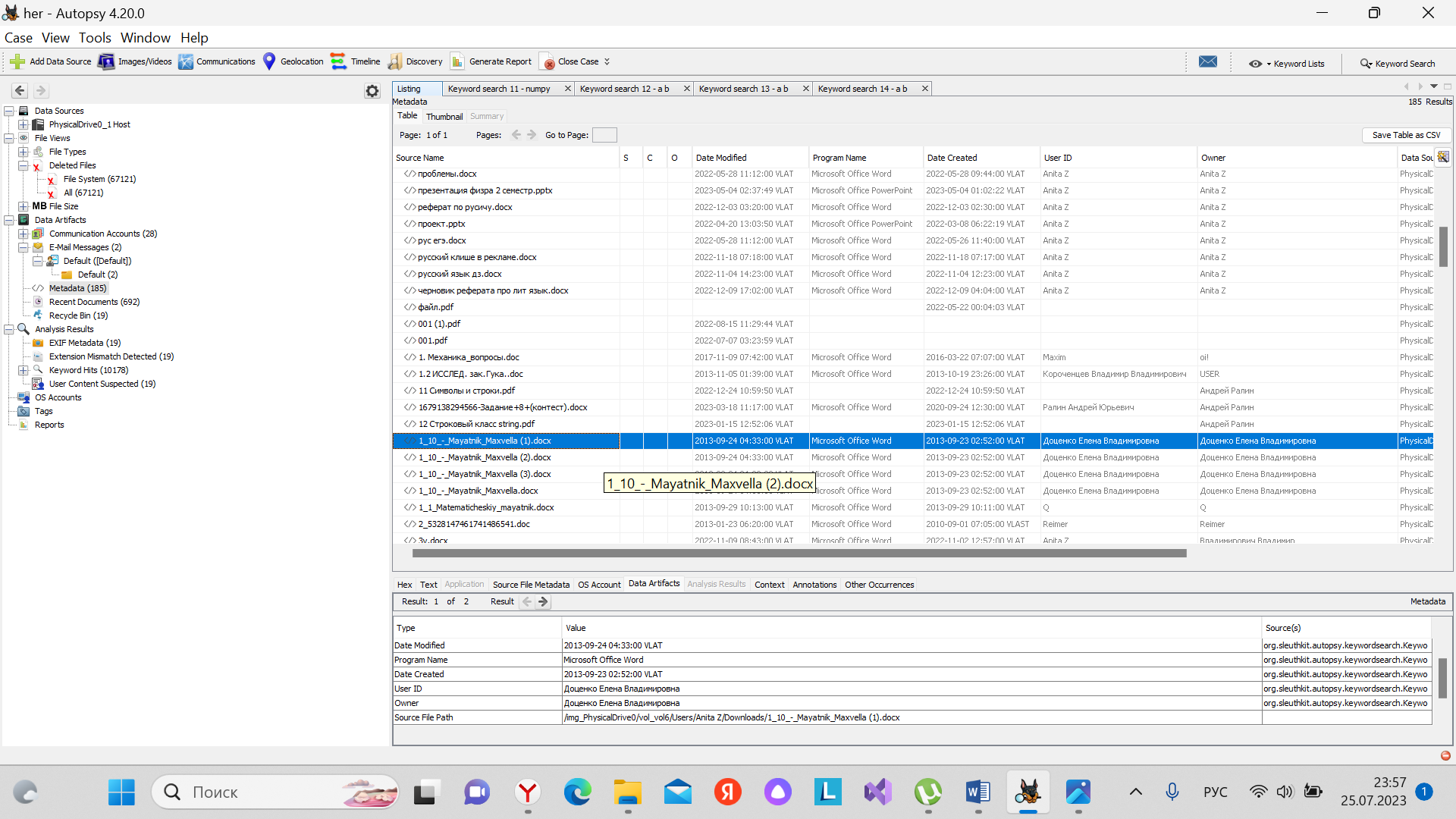
Я попыталась провести фильтрацию по ноиерам телефонов, но приложение зависло на несколько часов, а потом показало это… К сожалению и после следующих попыток показывало то же самое(

В разделе *Deleted files* можно найти информацию о файлах, которые были удалены. Для восстановления нужно извлечь файл и сохраните в соответствующем месте назначения.



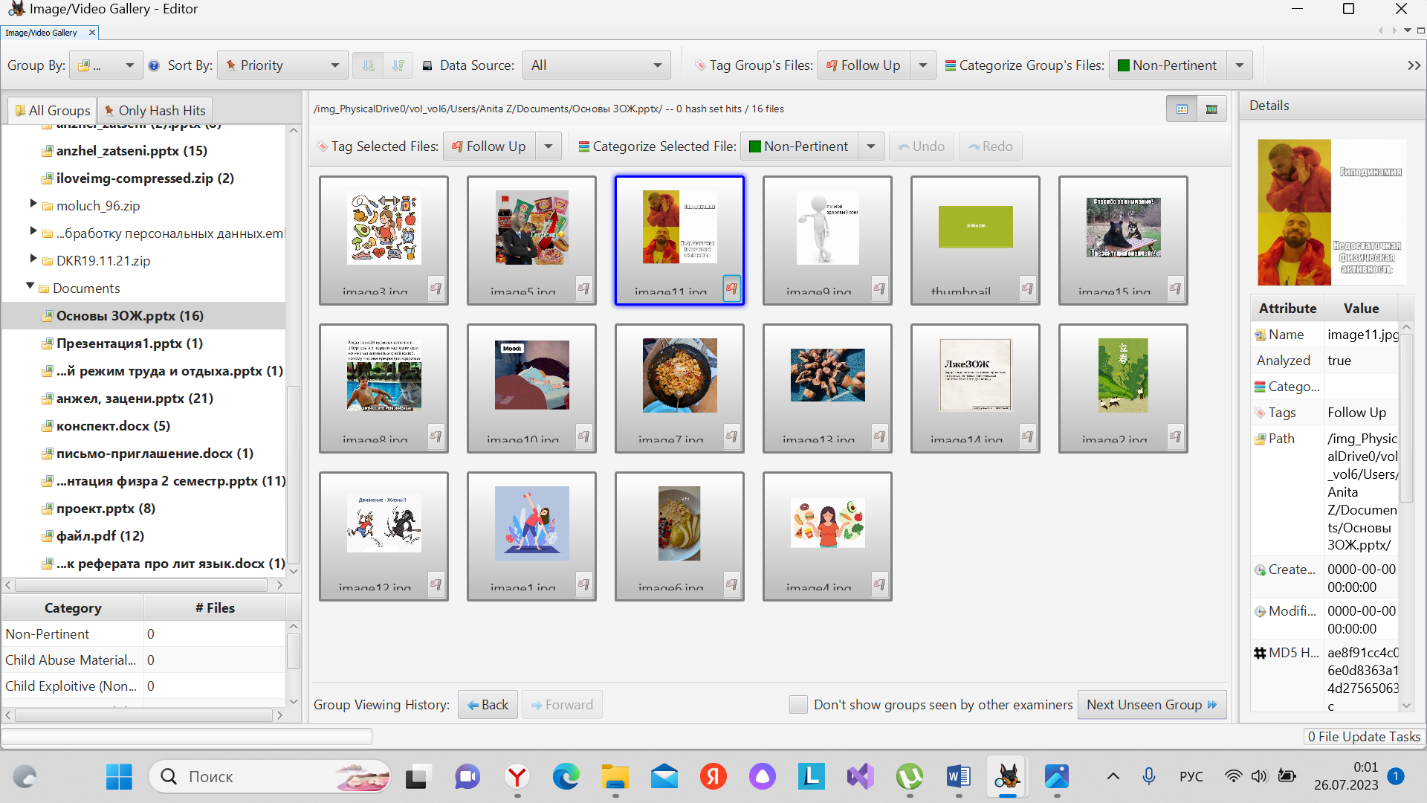
Изучите метаданные файлов и проведите анализ на основе найденных данных.

Примером анализа метаданных, может стать данный word файл. В графе “Owner” (Владелец/Создатель) мы видим имя Доценко Елена Владимировна и дату создания этой лабораторной работы по физике.



Поиск и анализ медиафайлов (изображения, видео)

Таким образом, можно просматривать изображения со всех презентаций и других документов.



**Заключение**

В ходе научно-исследовательской работы была достигнута цель: изучить и использовать утилиту Autopsy для анализа локального жесткого диска и извлечения цифровых доказательств.

Для достижения цели мы исследовали следующие свойтва утилиты:

a. Просмотр файловой системы и структуры диска.

b. Поиск и фильтрация файлов и метаданных.

c. Анализ и восстановление удаленных файлов.

d. Извлечение и анализ метаданных файлов.

e. Просмотр и анализ истории веб-браузеров, электронной почты.

f. Поиск и анализ медиафайлов (изображения, видео).

— Проанализирован жесткий диск, применены различные функции и возможности утилиты Autopsy.

a. Выполнены основные операции анализа, включая поиск, фильтрацию и восстановление файлов.

b. Изучены метаданные файлов и проведите анализ на основе найденных данных.

c. Использованы функции анализа веб-браузеров, электронной почты и других приложений для извлечения соответствующей информации.

d. Проведен анализ медиафайлов для обнаружения и изучения связанных данных.