Обзор утилиты Autopsy

Содержание

Введение

Autopsy - это простая в использовании программа на основе графического интерфейса, которая позволяет эффективно анализировать жесткие диски и смартфоны. Он имеет подключаемую архитектуру, которая позволяет находить дополнительные модули или разрабатывать пользовательские модули на Java или Python.

Ссылка на официальный сайт Autopsy: **https://www.autopsy.com/**

The Sleuth Kit - это набор инструментов командной строки и библиотека C, которая позволяет анализировать образы дисков и восстанавливать из них файлы. Он используется за кулисами в аутопсии и многих других инструментах с открытым исходным кодом и коммерческой криминалистики.

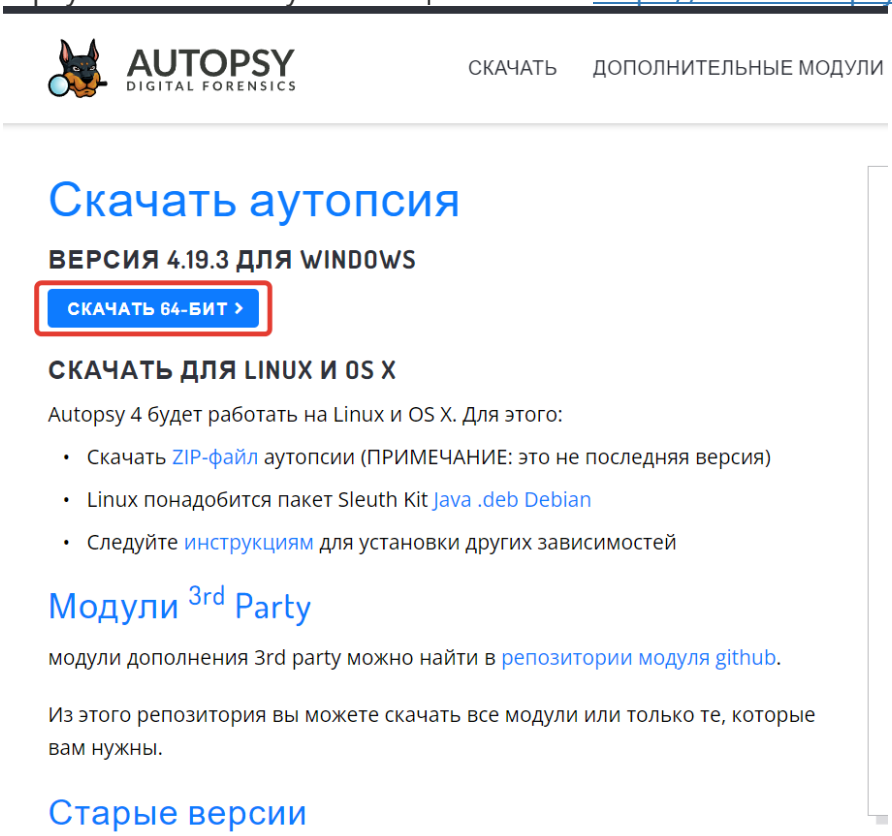
Список всех доступных инструментов с их кратким описанием можно прочитать по следующей ссылке: **https://kali.tools/?p=1811**

Установка, активация, подготовка к работе

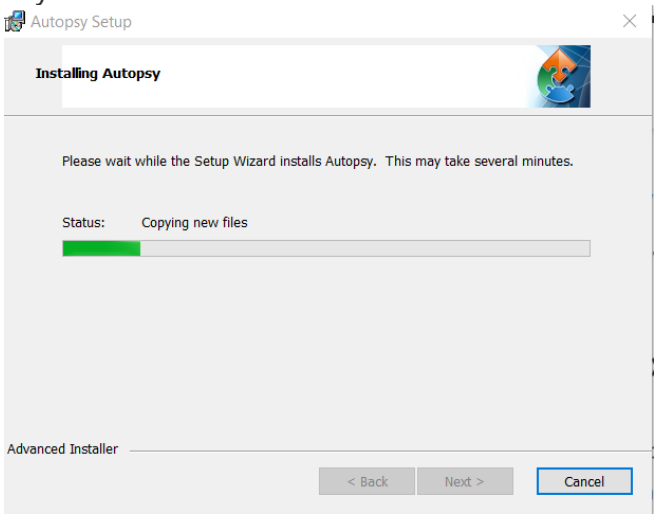
Скачать данные программы для операционных систем Windows и Linux можно с сайта: **https://sleuthkit.org/index.php**

Для Windows

При установке Autopsy скачивается установщик с сайта https://www.autopsy.com/download/

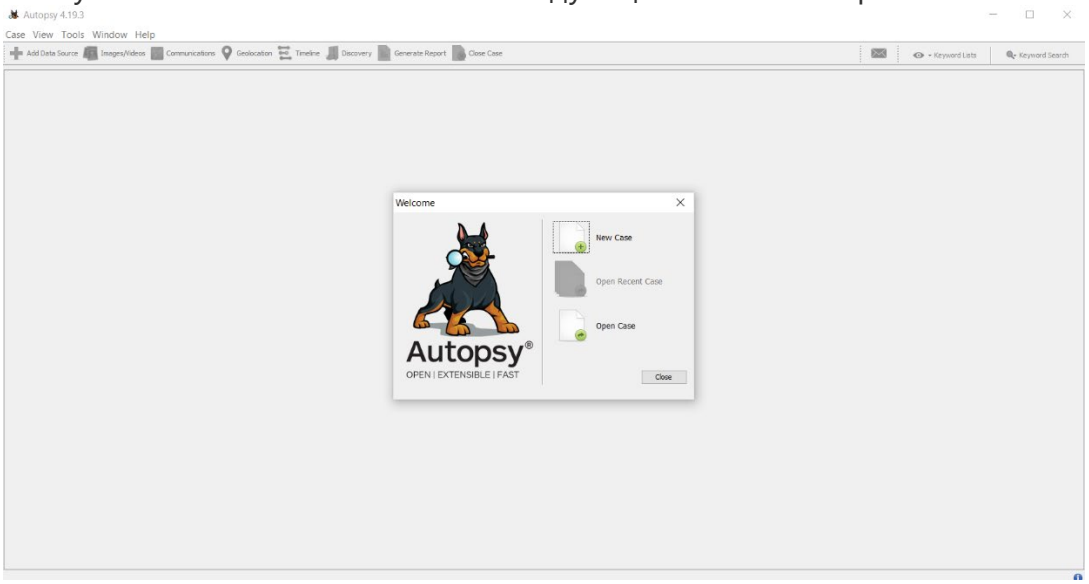


Далее запускаем скаченый файл **autopsy-X.X.X-64bit**
И устанавливаем программу.

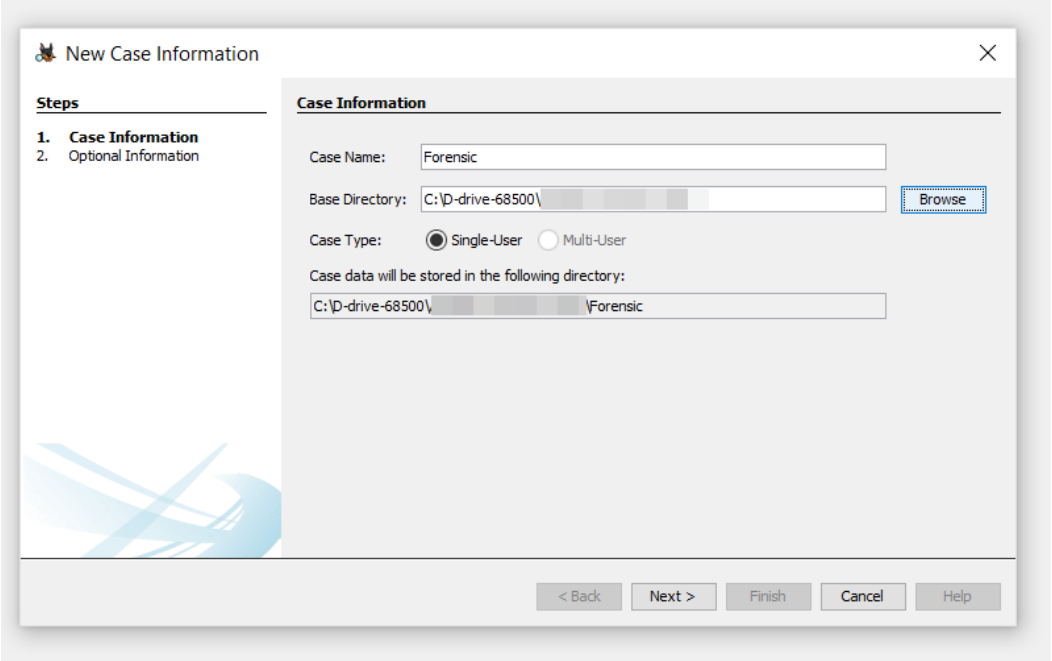


Работа с утилитой

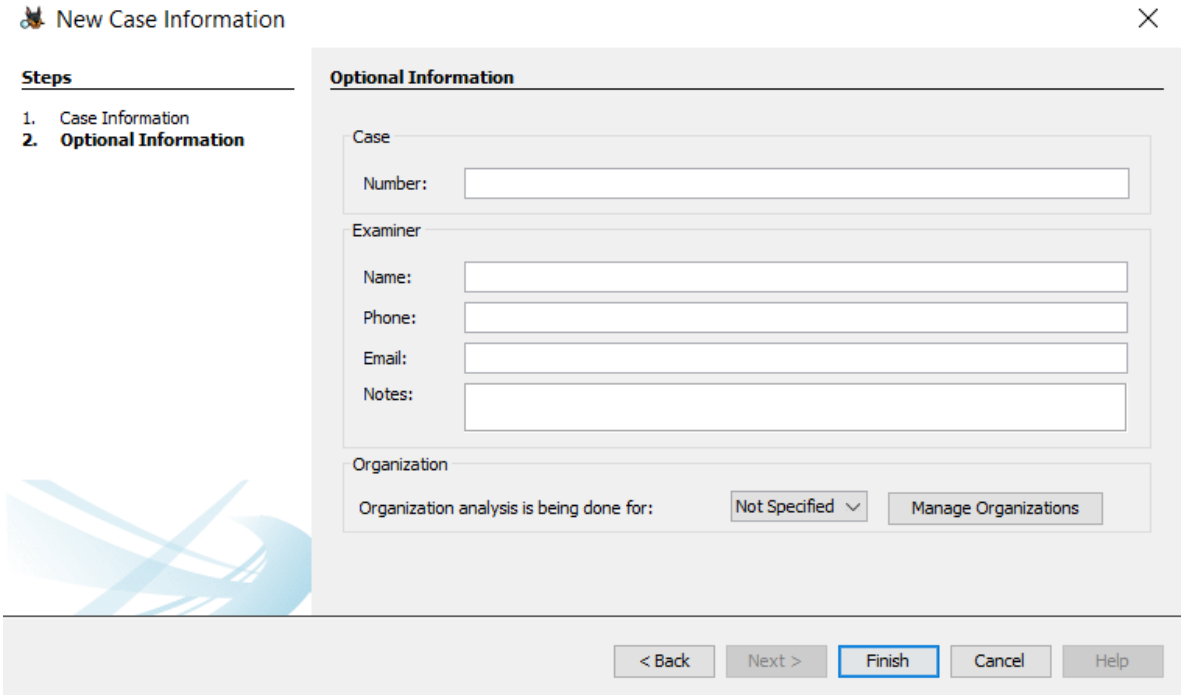
Использование Autopsy в Windows
При первом запуске в Windows появляется следующие окно. Выбираем New Case.



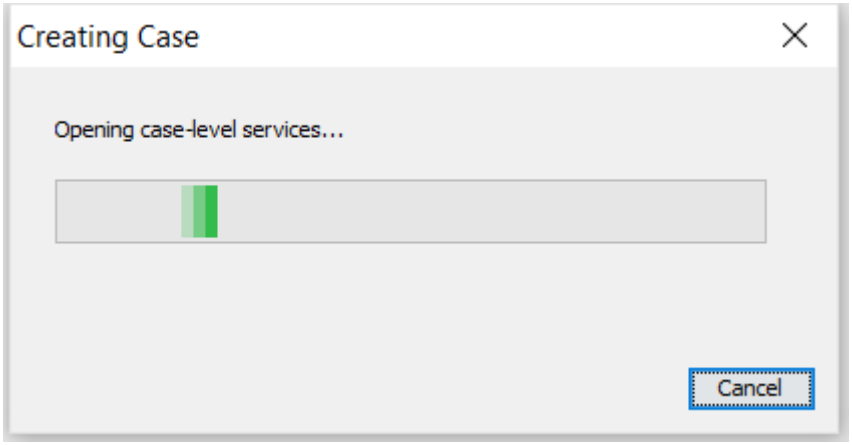
Далее выбираем название проекта и директорию, в которой будет находиться данный проект.



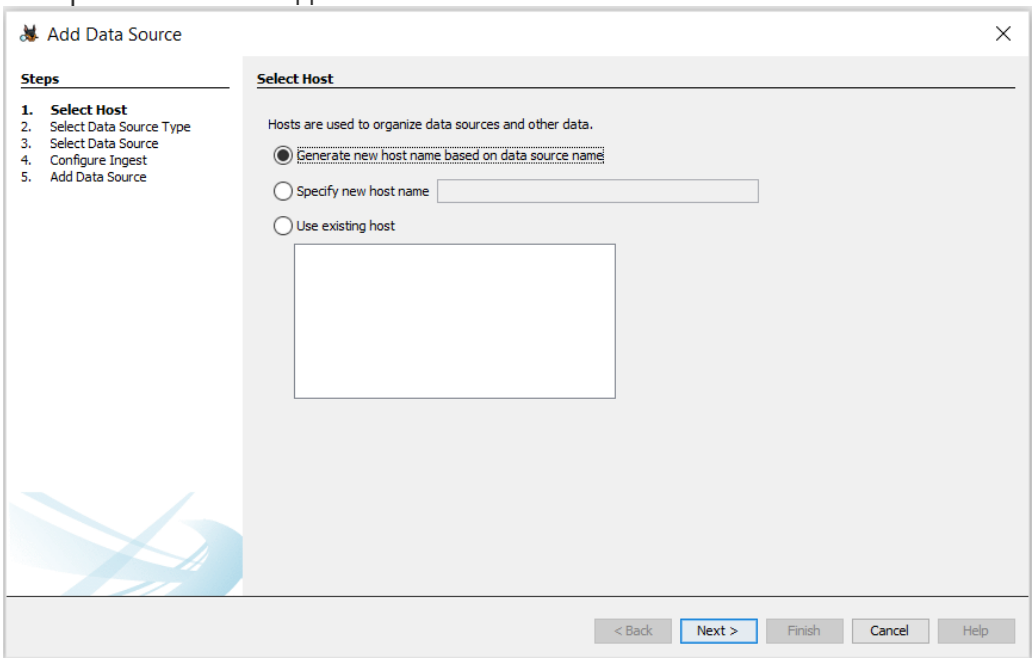
Если хотите то можно добавить дополнительные настройки.



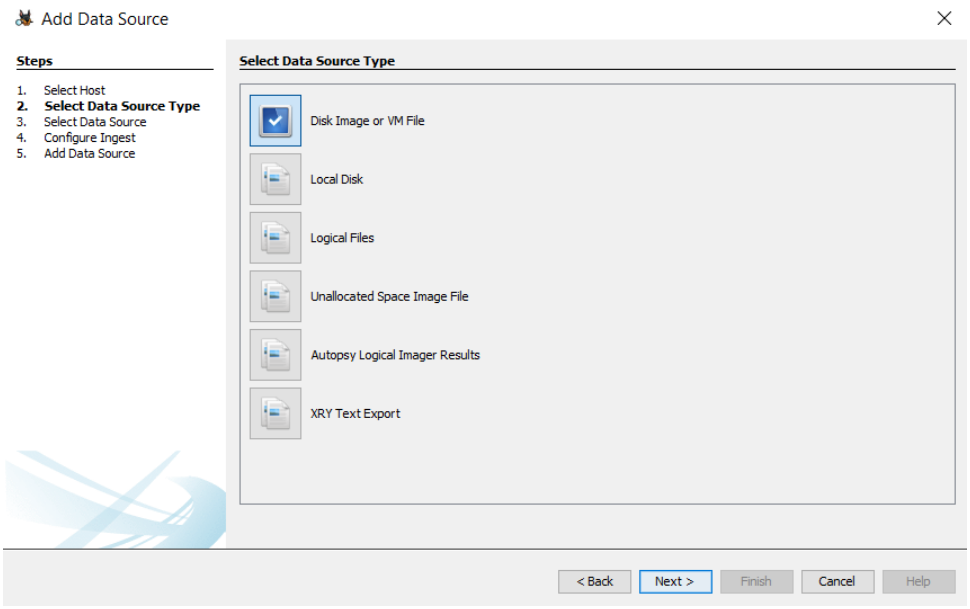
И создаём проект:



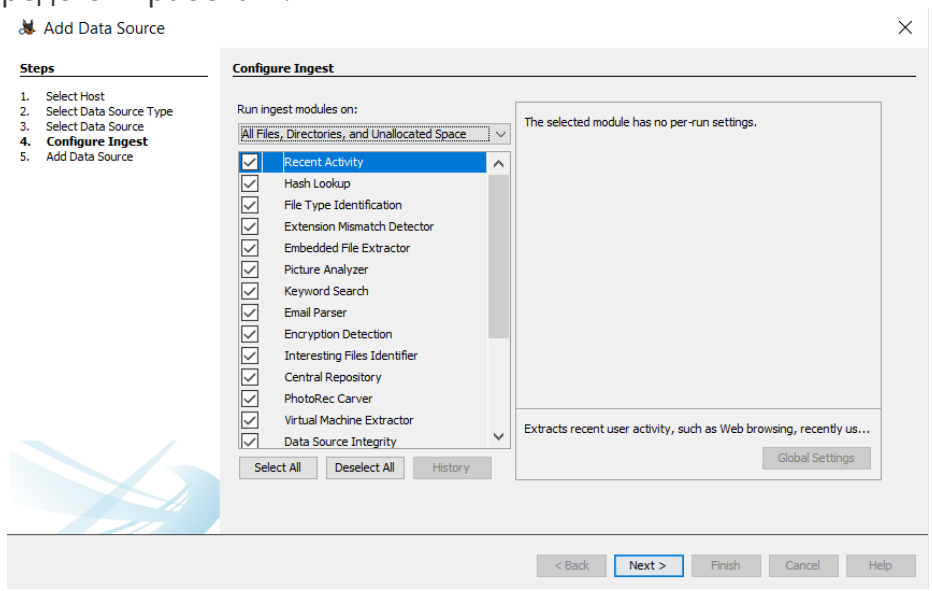
Далее нужно выбрать источник данных



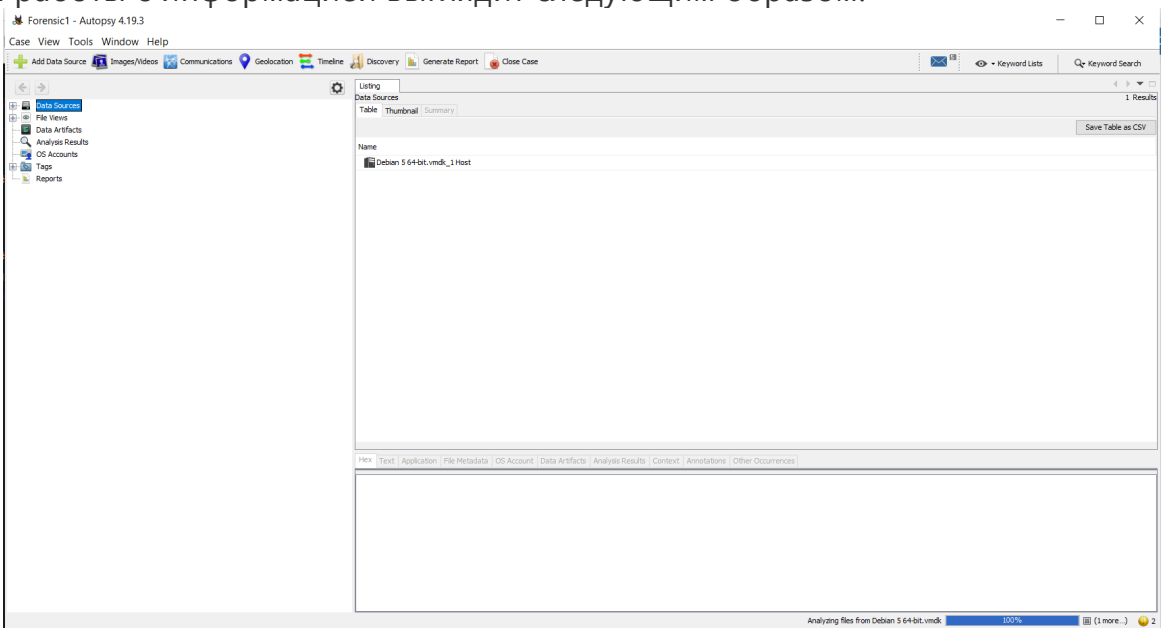
Затем выбираем тип источника файла, который будем анализировать.



Далее идет раздел **Configure Ingest** здесь можно выбрать типы файлов и каталоги с которыми нам предстоит работать.

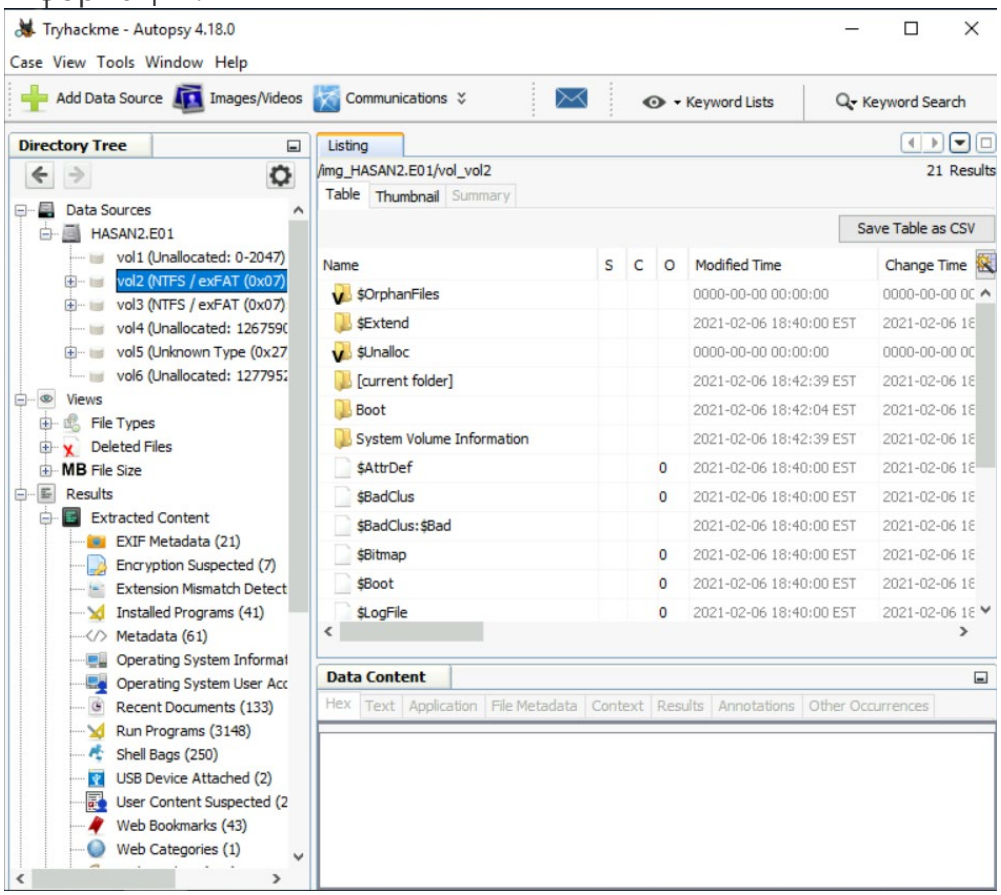


Окно для работы с информацией выглядит следующим образом.

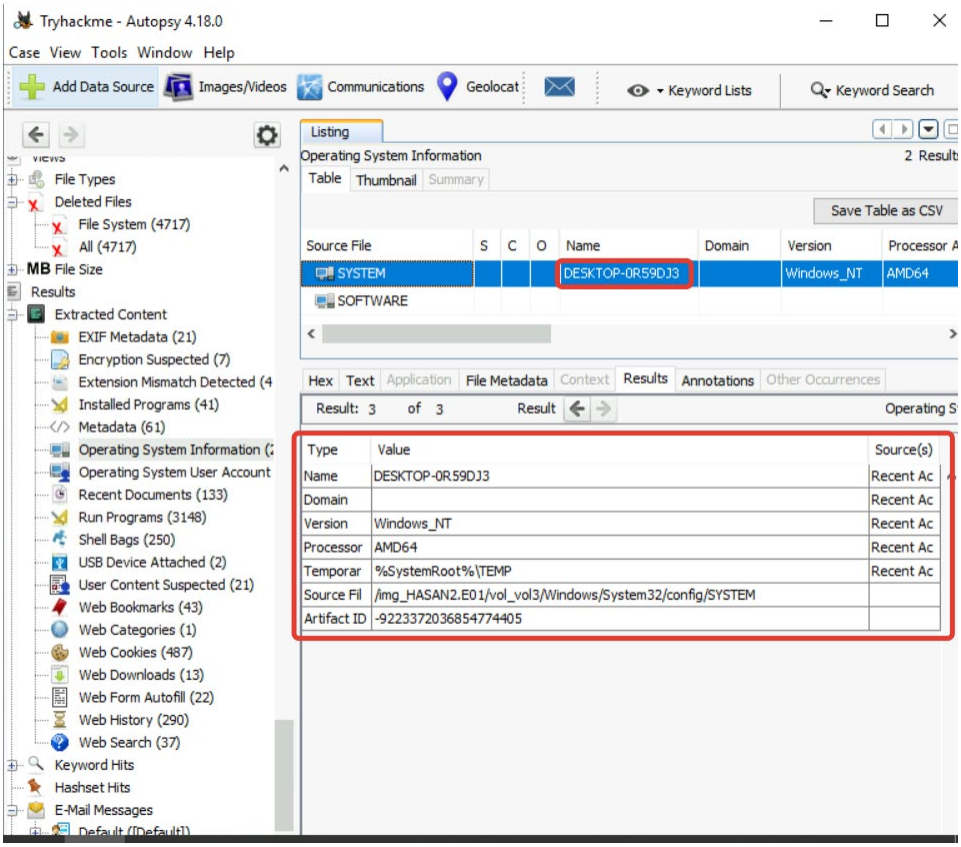


Так как на моем виртуальном диске нет информации, при помощи которой можно было бы описать все инструменты анализа данной программы, то дальше я буду показывать принцип её работы через AttackBox на сайте TryHackMe.

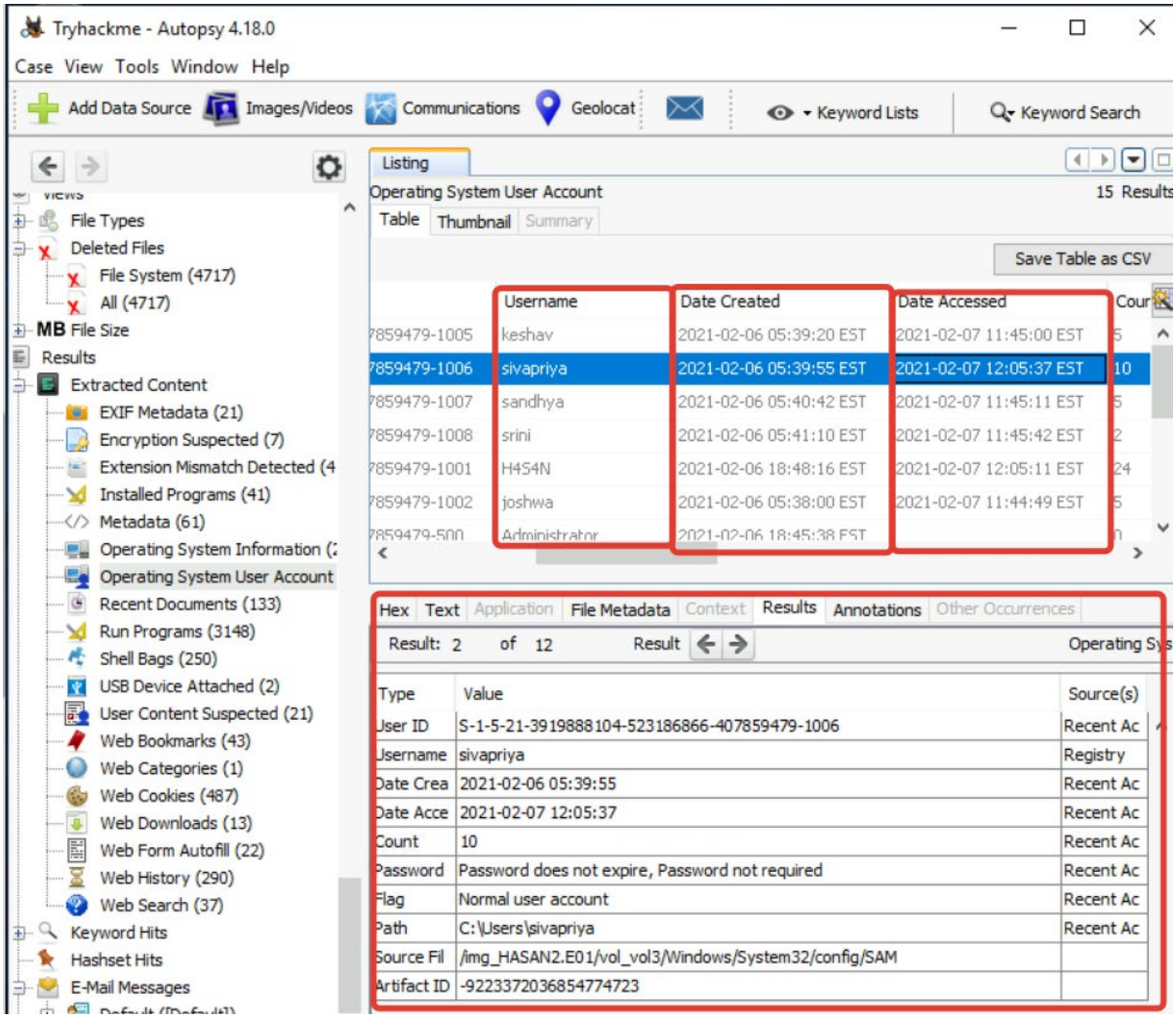
Итак, вот так выглдит программа при анализе образа диска. Далее будет рассмотрено, то какую информацию можно получить и какие инструметы The Sleuth Kit предоставляют доступ к этой информации.



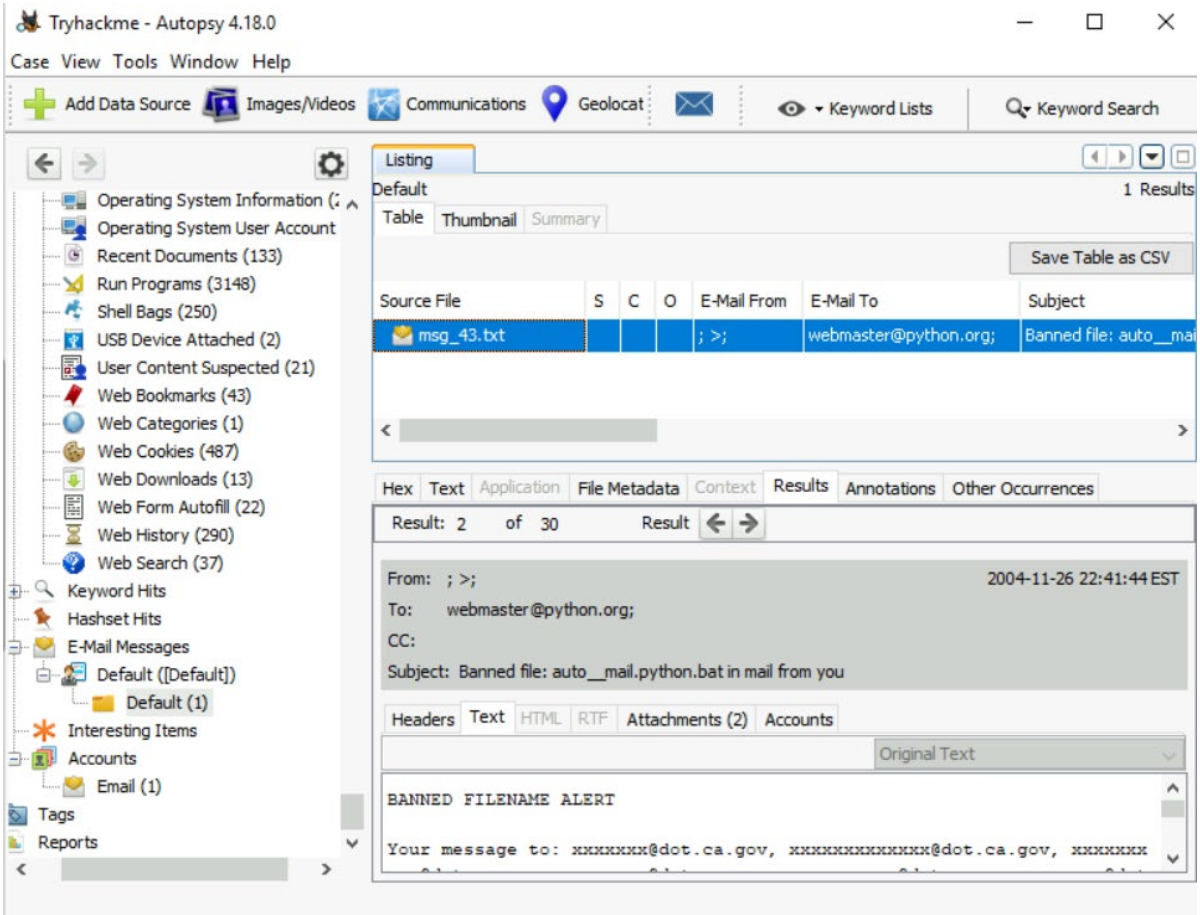
Итак, можно узнать информацию о системе: processor, version os, computer account name и тд.

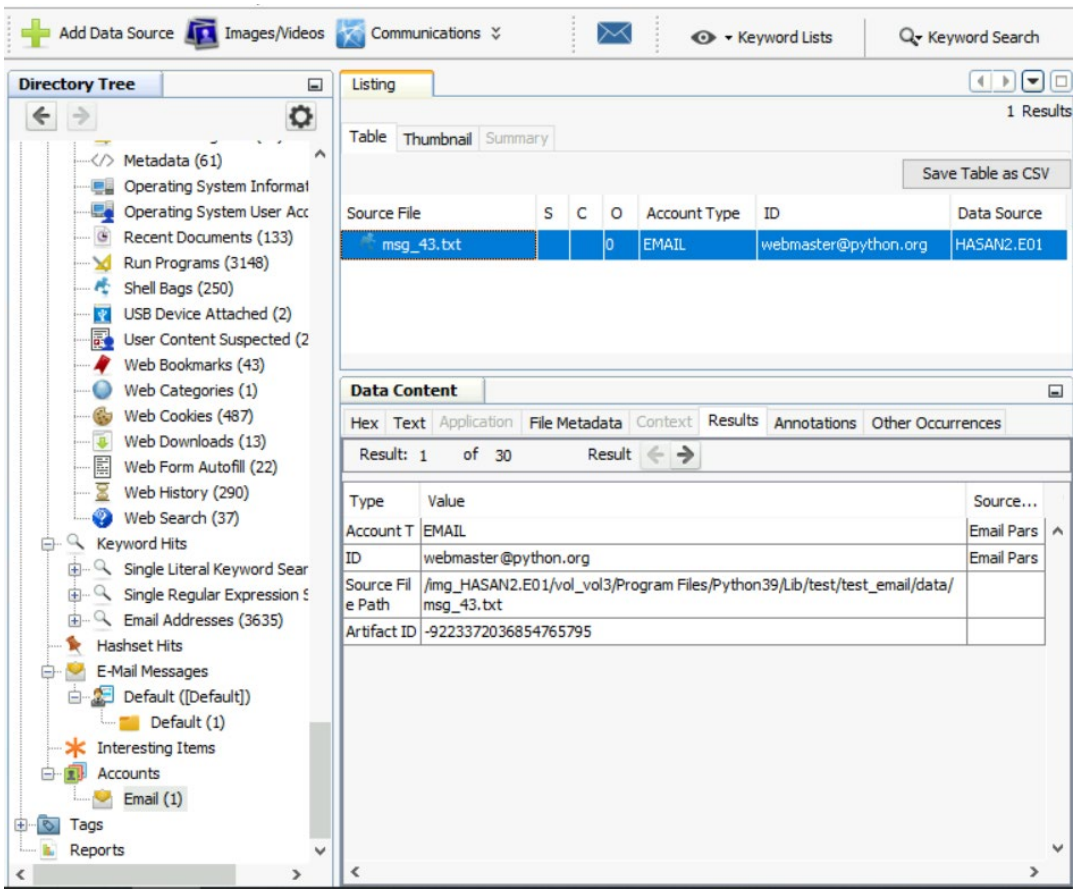


Мы также можем узнать сколько пользователей системы было на компьюторе, а также их наименование, дату создания каждого из этих пользователей, время их последней активности и тд.

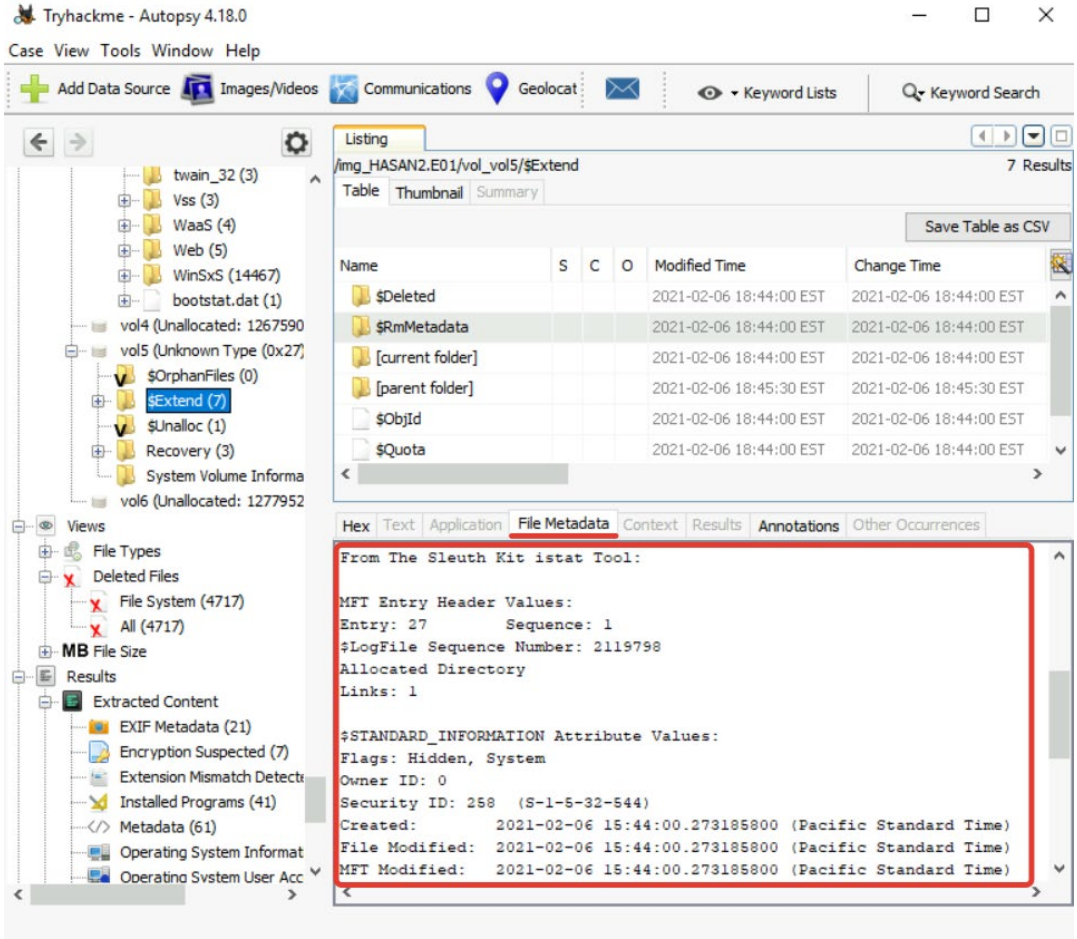


Просмотр почты и сообщений, а так же информации о том кому отправлено письмо, что написанно в письме.

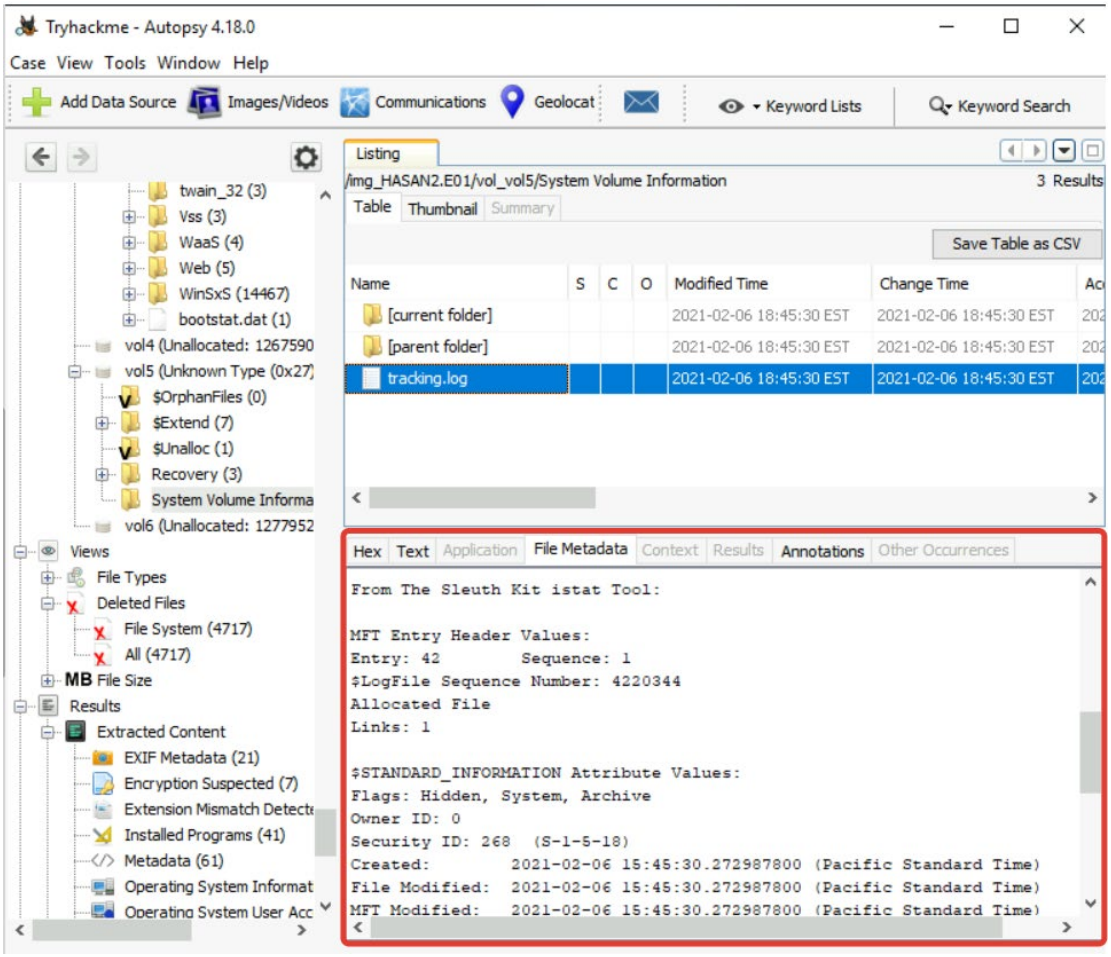




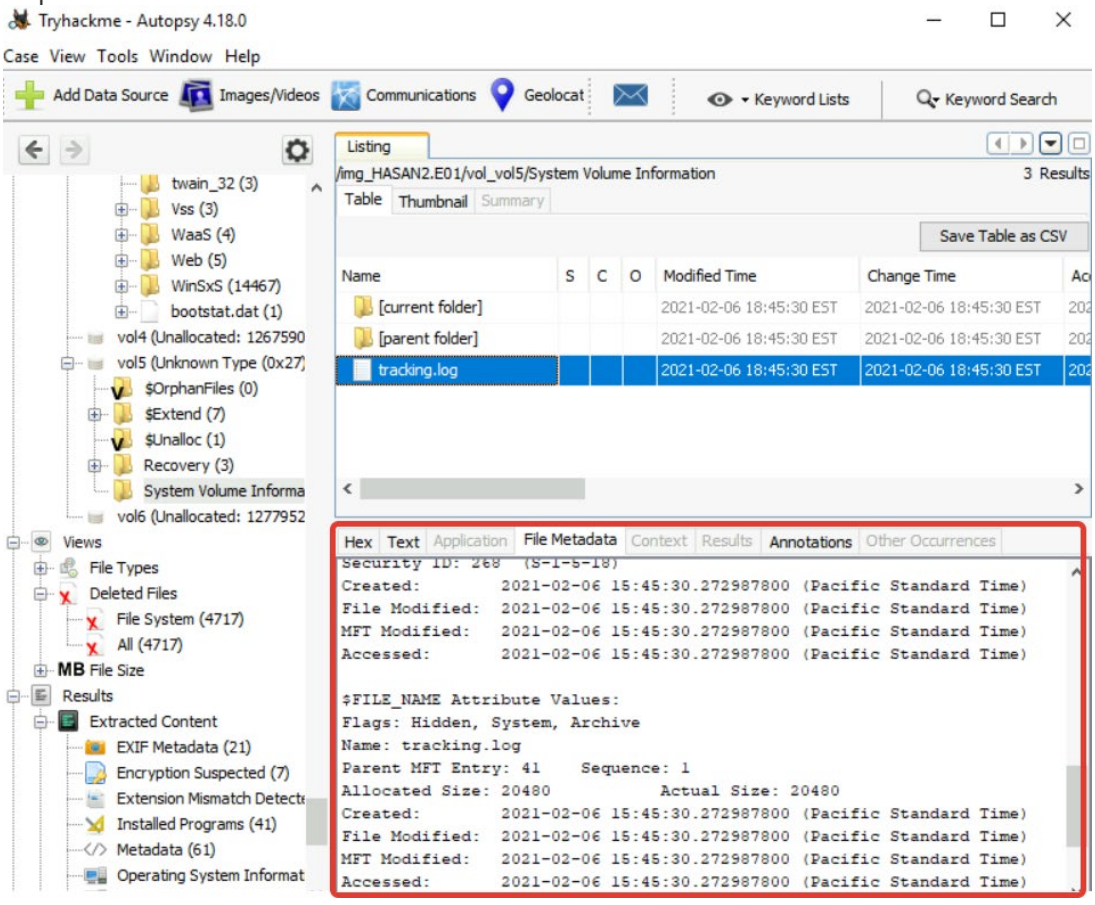
Просмотр метаданных при помощи интструментов The Sleuth Kit. Показывает значение атрибутов стандартной информации: дата создания, дата изменения, индентификатор безопасности и тд.



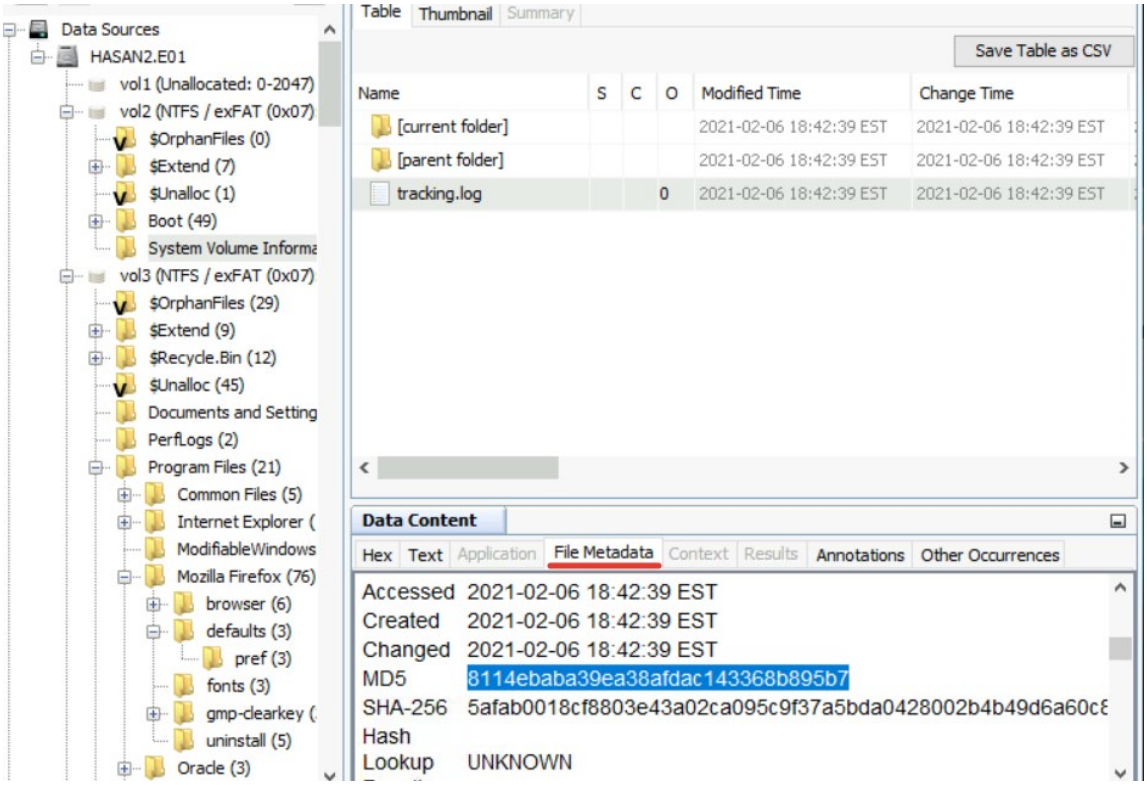
Метаданные папки.



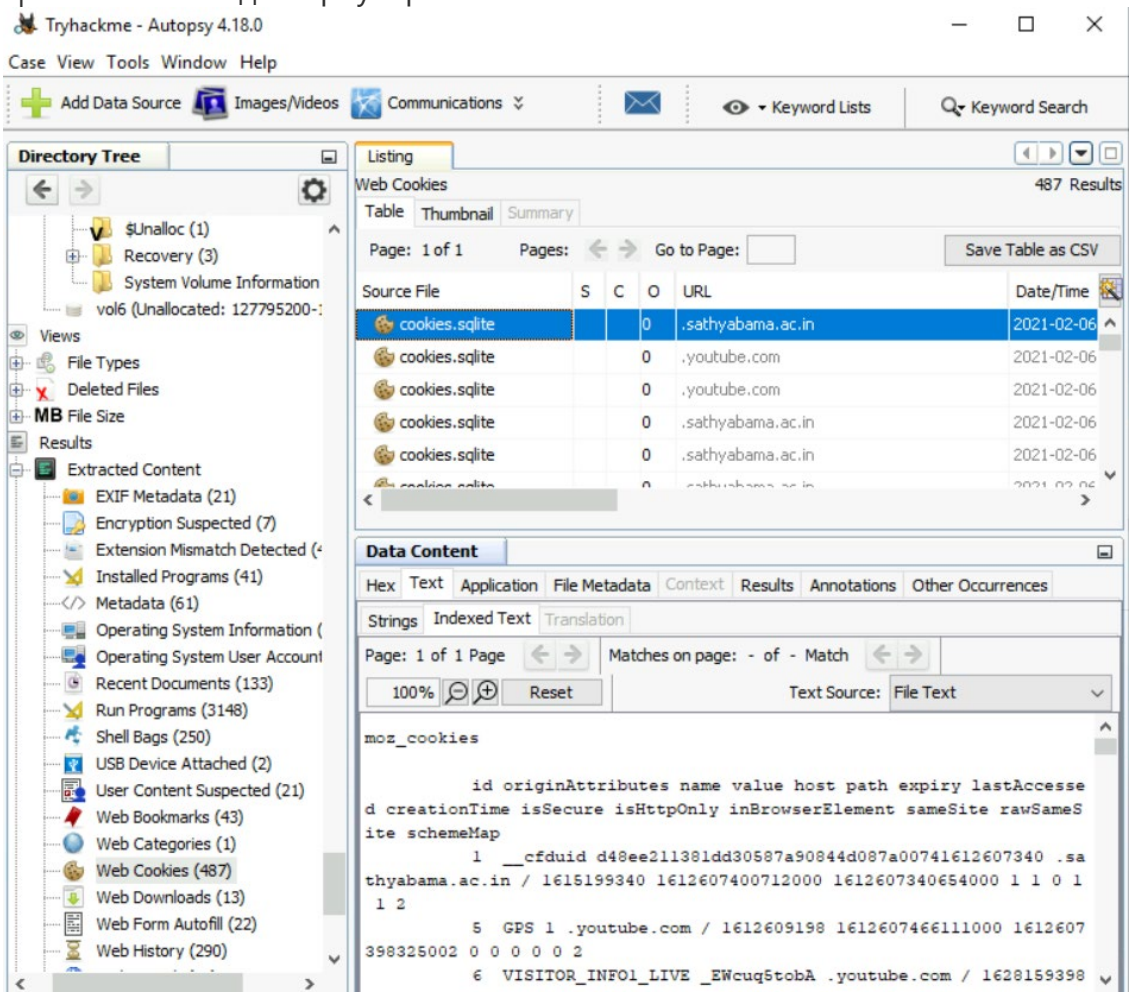
Метаданные файла.



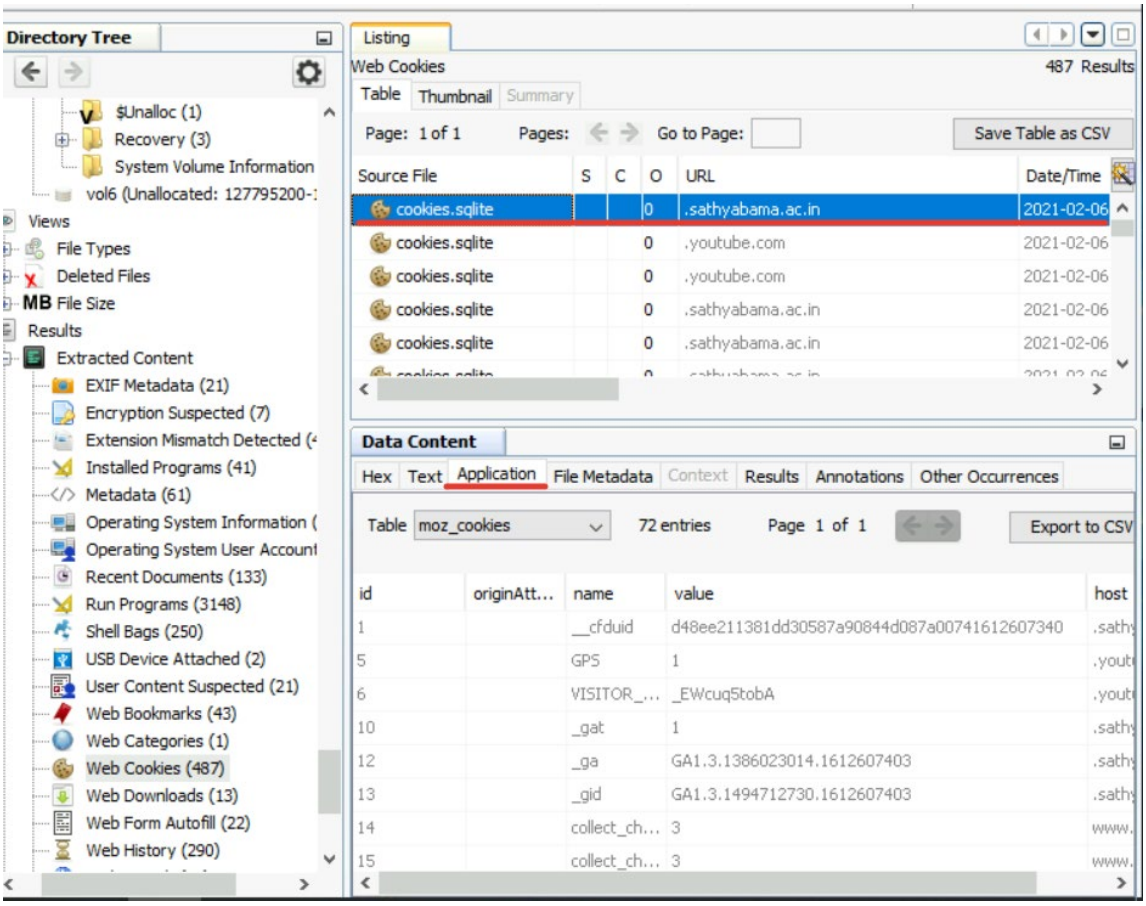
Здесь можно просмотреть дату создания файла, дату обращения, дату изменения, а также два алгоритма хештрования для этого файла - SHA-256 и MD5.



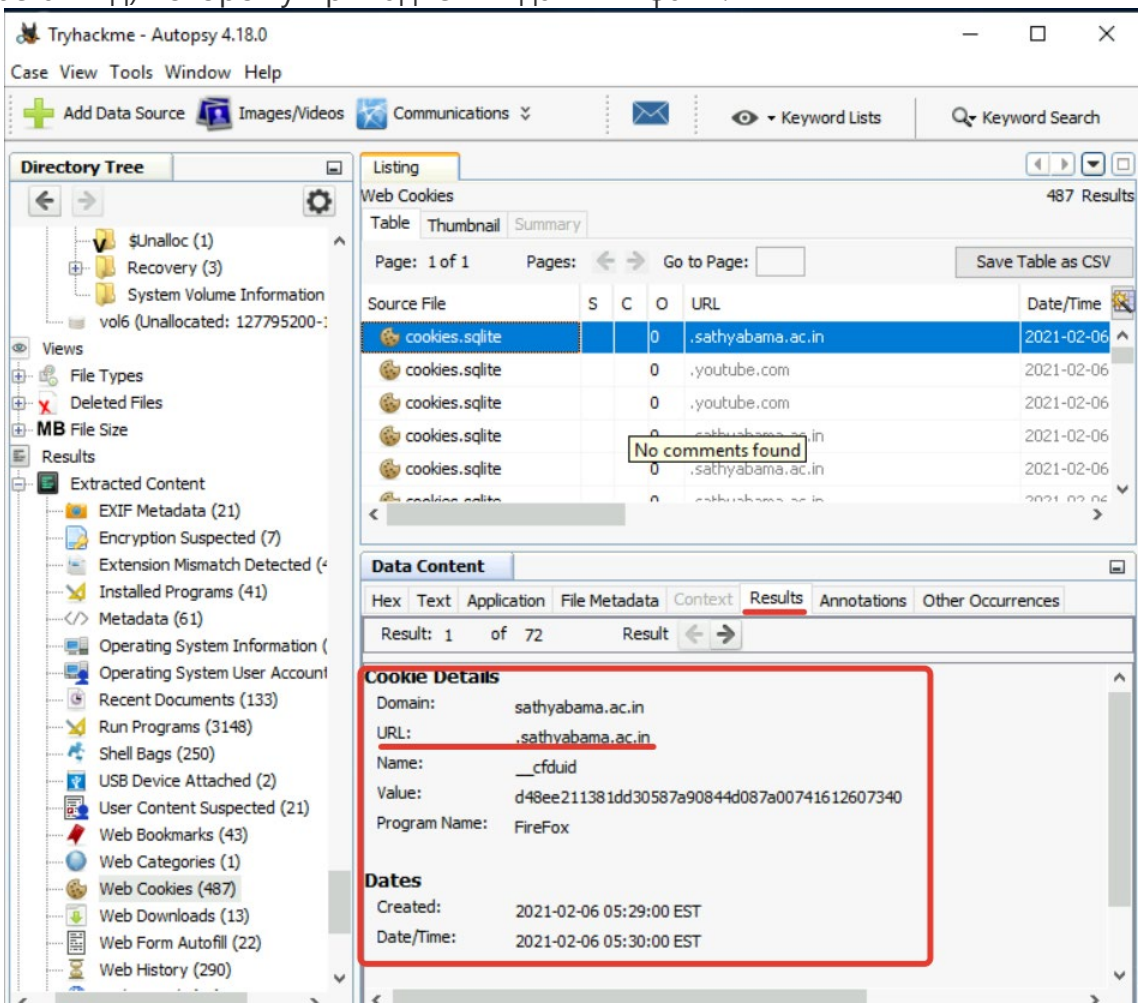
Просмотр файлов cookie для браузера.

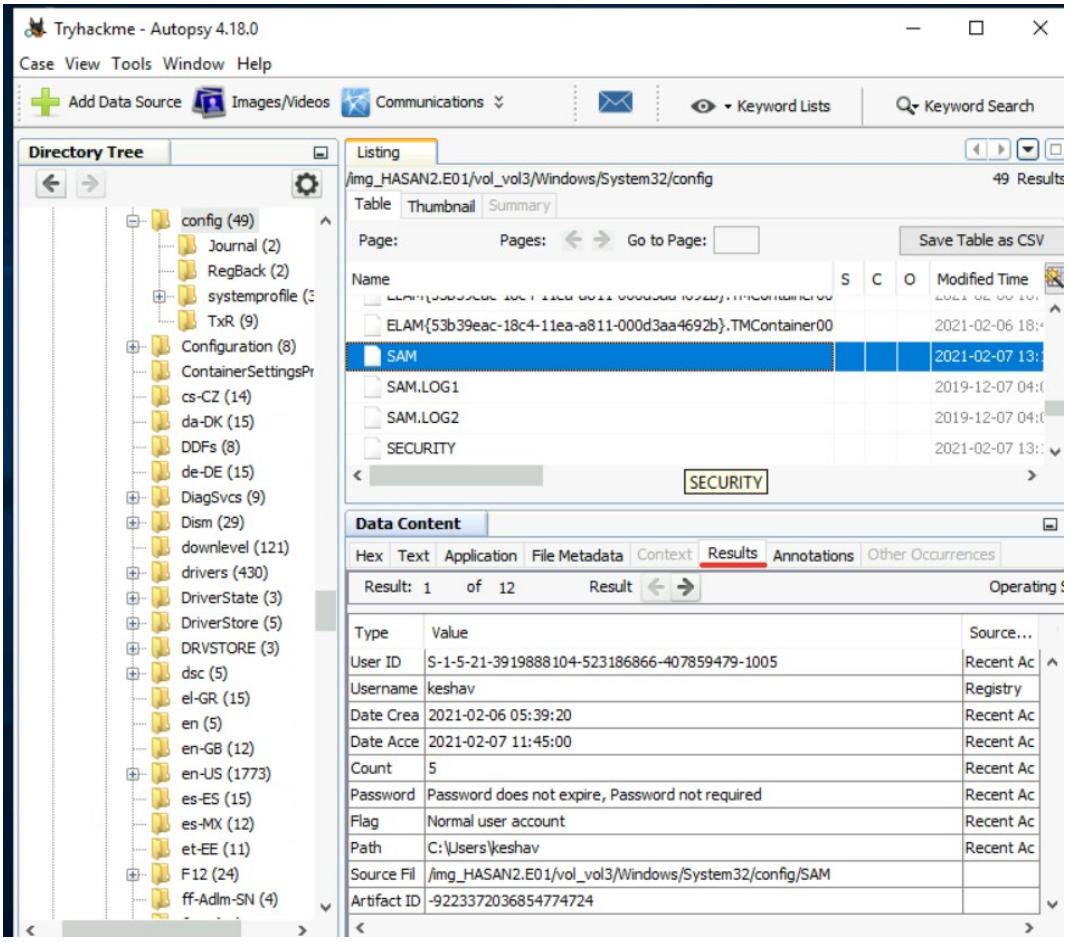


В разделе application представлена таблица со следующими атрибутами: id, name, value, host. Name устанавливает имя cookie-файла. Value сохраняет значение cookie, которое будет идентифицировать пользователя или содержать служебную информацию. Host показывает к какому сайту относится cookie файл.

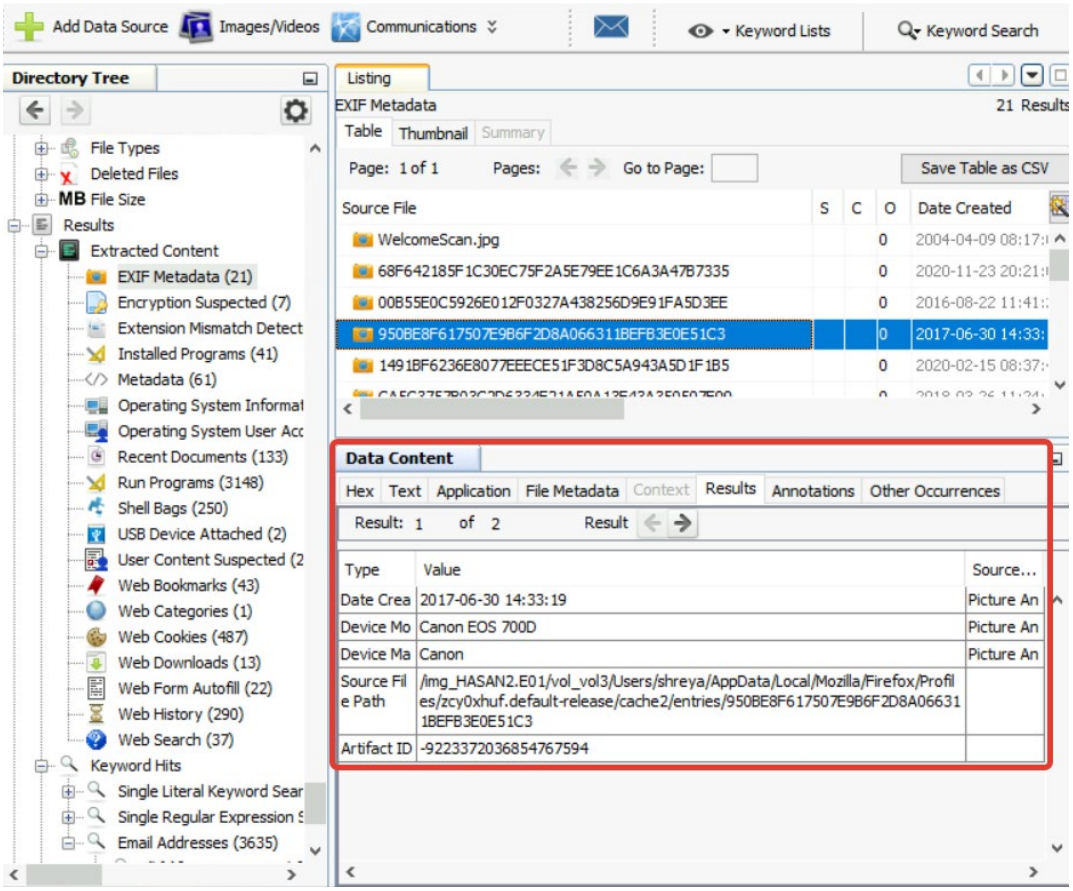


Во вкладке Results так же как и фо вкладке application представлены сведения о файлах cookie. В данном случае представлены сведения о URL и Domain сайта, названия и значения cookie файла, даты создания файла, названия программы, а именно браузера (Yandex, Google, Firefox, Opera и тд) которому принадлежит данный файл.

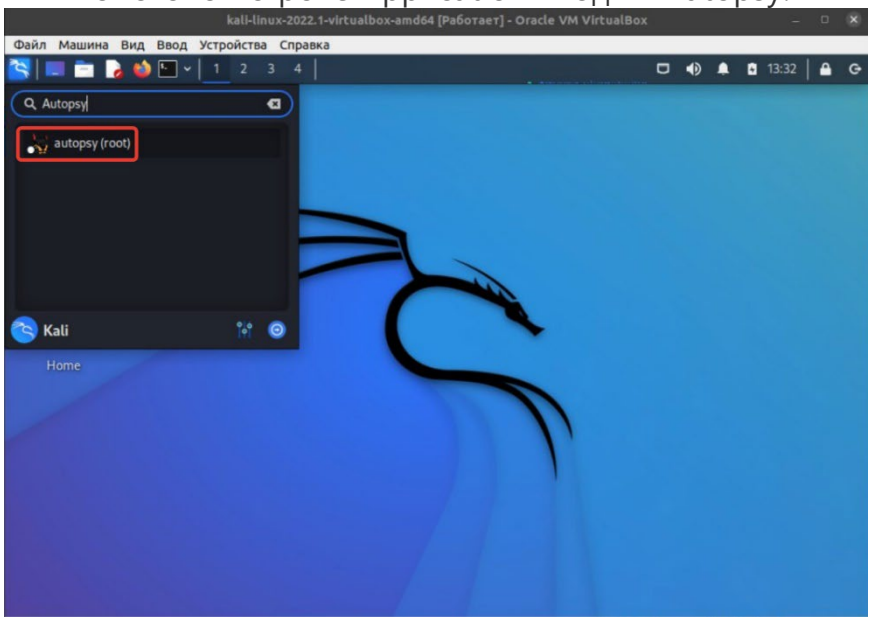




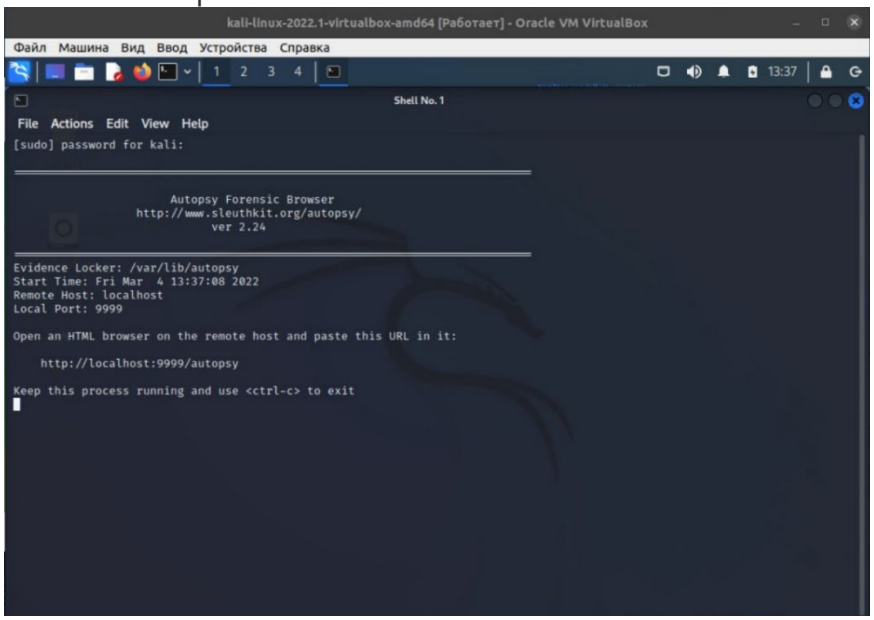
При анализе изображений можно получить следующую информацию: дату и время создания фотографии(изображения), устройство при помощи которого была сделана фотография, место хранения на диске и соответственно путь, где находится этот файл, можно узнать какой пользователь в системе загружал это изображение и через что оно было загруженно.



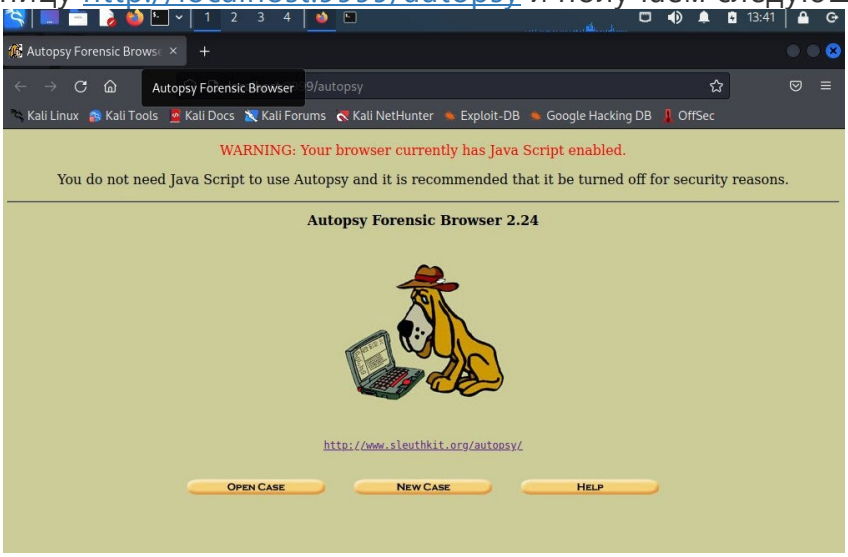
Использование Autopsy в Linux
Работа с программой Autopsy в дистрибутиве Kali Linux.
Входим в Kali Linux и в поисковой строке Application вводим Autopsy.



При открытии приложения открывается консоль.



Переходим на страницу http://localhost:9999/autopsy и получаем следующее око в браузере.



В разделе Help представлена справка по использованию Autopsy, а также некоторая информация о The Sleuth Kit.

Разделы Open case и New case по функциональности такие же как были представленны для Windows только в браузере и с другим дизайном.

Заключение

Была описана некоторая информация, которую можно получить используя Autopsy и The Sleuth Kit, а именно это информация о конфигурации системы, метаданные файлов(т.е. дату создания, дату изменения и прочее) их местоположение на диске, содержание и прочие атрибуты. Данная программа также позволяет анализировать активность браузеров, файлы cookie.

Из наиболее полезных инструментов в программе The Sleuth Kit (TSK) стоит отметить такие как: mmstat, которая отображает сведения о системе; mmls, которая отображает структуру диска; sigfind, инструмент поиска двоичного значения по заданному смещению, применяется для восстановления потерянных структур данных; tsk_loaddb - инструмент, который заполняет базу данных SQLite метаданными из образа диска; img_stat инструмент, который покажет подробную информацию о формате образа; fsstat - показывает общие сведения о файловой системе и т.д. Также многие из этих инструментов также доступны в дистрибутиве Kali Linux, и используются напрямую через терминал.