



Краткая памятка использования и
основного функционала.

mac

linux

win

VM

iOS

Android

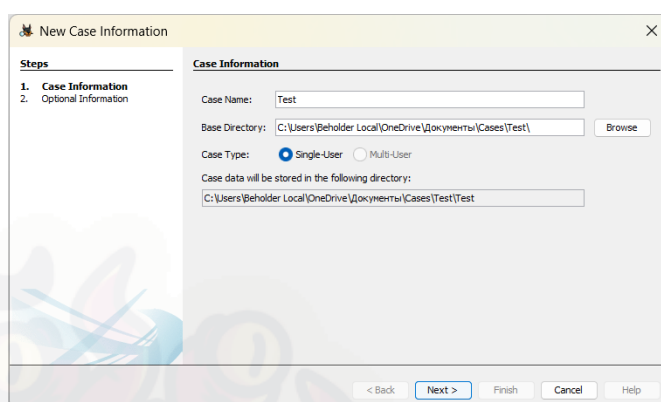
www.autopsy.com

Начало работы:

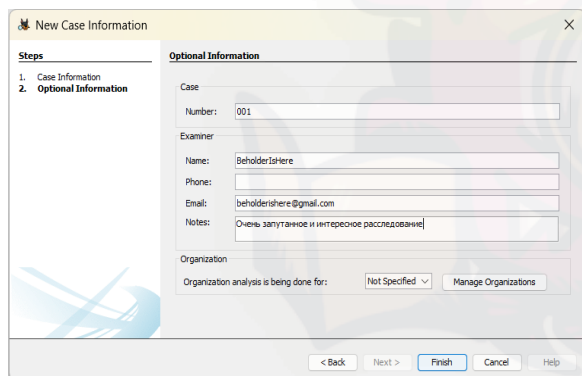
1. Запускаем Autopsy и нажимаем "New Case".



2. Вводим название дела, а также выбираем базовый каталог, для сбора данных в одном месте.



3. При необходимости можно добавить дополнительную информацию.



Примечания:

- Поскольку в рамках одного дела вы будете иметь дела с различными источниками данных, этот этап необходим для того, чтобы вся информация находилась в одном месте, а также сохранить целостность структуры исследуемой информации при переносе дела на другой компьютер.
- Физически все данные и вся информация по делу будет находиться по тому пути который вы укажете в пункте 2.



Краткая памятка использования и
основного функционала.

mac

linux

win

VM

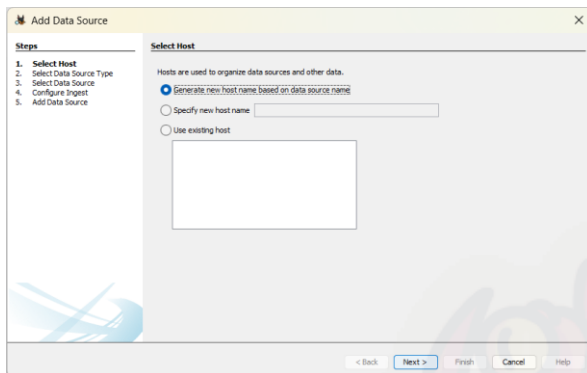
iOS

Android

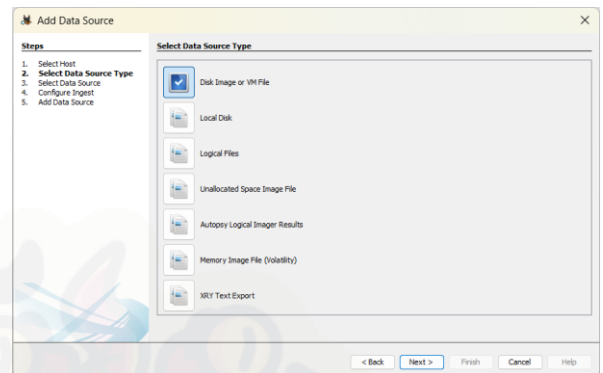
www.autopsy.com

Начало работы:

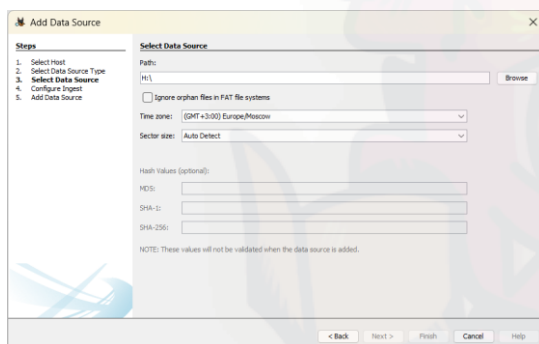
4. Сгенерируйте новое имя хоста



5. Выберите тип данных который вы добавите как источник .



6. Выберите место где находится источник данных



o Disk Image or VM file:

сюда входит файл образа, который может быть точной копией:

- жесткого диска
- карты памяти
- виртуальной машины

o Local Disk:

этот параметр включает такие устройства, как:

- жесткий диск
- USB накопители
- карты памяти и т. д.

o Logical Files:

образы любых локальных каталогов или файлов.

o Unallocated Space Image File:

файлы, запускаемые с помощью модуля Ingest.

o Autopsy Logical Imager Results:

источник данных от сканера логических разделов дисков.

o XRY Text Export:

источник данных из экспорта текстовых файлов из XRY.



Краткая памятка использования и
основного функционала.

mac

linux

win

VM

iOS

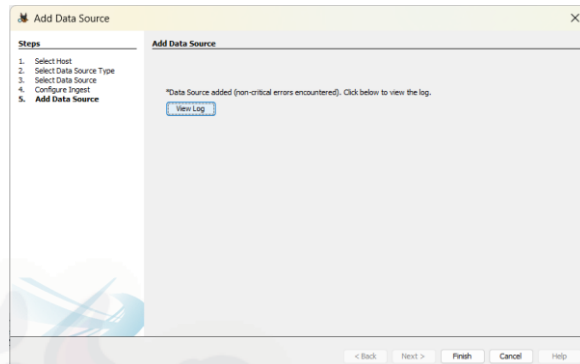
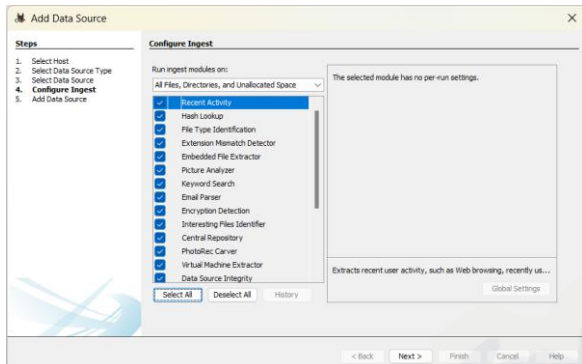
Android

www.autopsy.com

Начало работы:

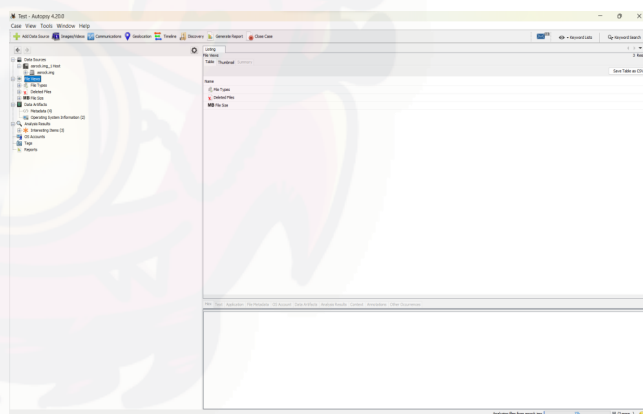
7. Выберите ingest модули которые вы будете использовать для анализа данных.

8. На шаге **Add Data Source** источник будет добавлен и проиндексирован. Это может занять некоторое время.



- **Недавняя активность.**
Обнаружение операций с файлами, дисками и системой
- **Детектор несоответствий расширений.**
Используется для идентификации файлов расширения которых могли быть подделаны
- **Поиск по хешу.**
Идентификация конкретного файла по его хеш-сумме
- **Идентификация типов файлов.**
Используется для определения типов файлов исходя из внутренних сигнатур
- **Экстрактор файлов.**
Предназначен для извлечения файлов из архивов для анализа
- **Поиск по ключевым словам.**
Поиск по ключевому слову или шаблону
- **Парсер электронной почты.**
Извлечение информации из баз данных почтовых клиентов
- **Обнаружение шифрования.**
Обнаружение зашифрованных или закрытых паролем файлов
- **Экстрактор виртуальных машин.**
Находит и помогает проанализировать виртуальные машины
- **Идентификация «интересных» файлов.**
Уведомления о наличие файлов по определенному заданному правилу
- **Анализ изображений.**
Распознавание текста на фото

9. После нажатия кнопки **Finish** вы будете готовы к исследованию данных, попав в главное окно Autopsy





Краткая памятка использования и
основного функционала.

mac

linux

win

VM

iOS

Android

www.autopsy.com

Работа с Autopsy:

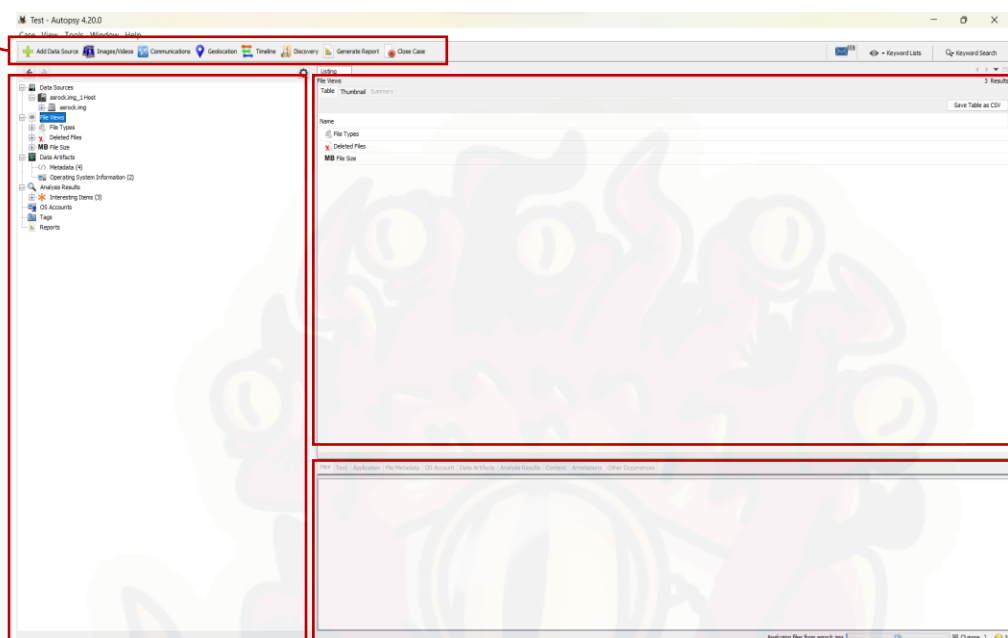
Основное рабочее пространство:

○ ФУНКЦИОНАЛЬНАЯ ПАНЕЛЬ

Содержит иконки запуска работы с данными.

○ ОКНО ИНФОРМАЦИИ

Место отображения подробной информации о объектах собранных ingest модулей.



○ ДРЕВО ДАННЫХ

Содержит консолидированную информацию собранную в процессе анализа, отсортированное по результатам работы ingest модулей

○ ОКНО СОДЕРЖИМОГО

Окно отображения найденной информации в исследуемых объектах



Краткая памятка использования и основного функционала.

Autopsy

mac

linux

win

VM

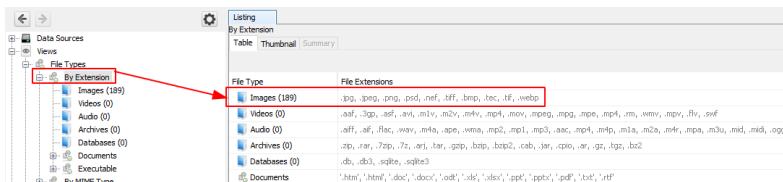
iOS

Android

www.autopsy.com

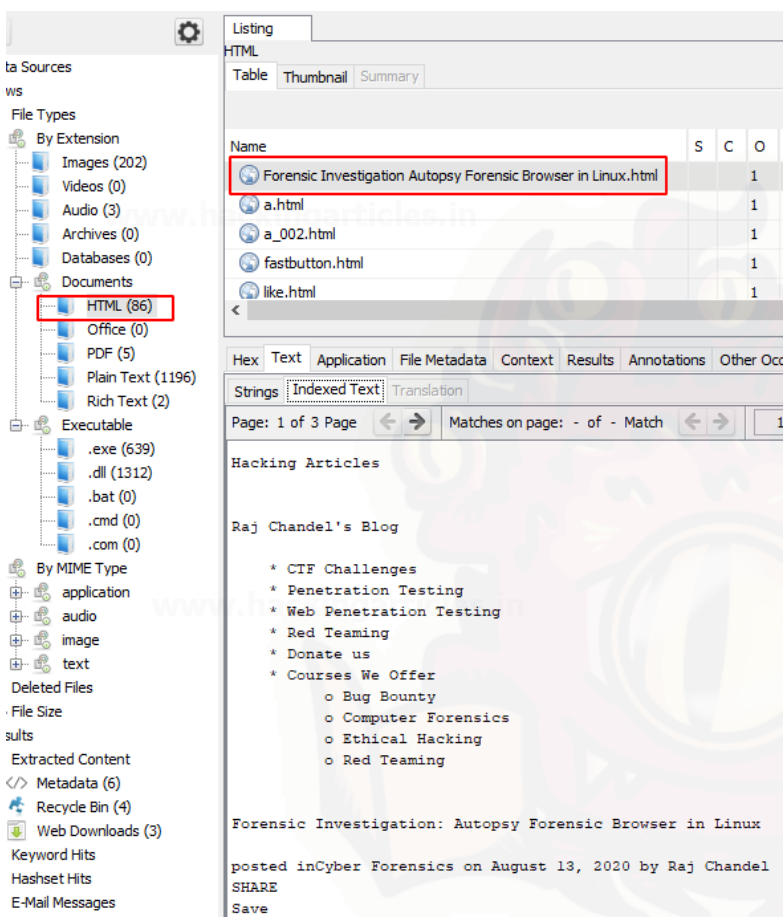
Работа с Autopsy:

ДРЕВО ДАННЫХ. FILE TYPES



КАТЕГОРИИ ФАЙЛОВ - ПО РАСШИРЕНИЮ

- Изображения
- Видео
- Аудио
- Архивы
- Базы данных и т. д.



КАТЕГОРИИ ФАЙЛОВ - ДОКУМЕНТЫ

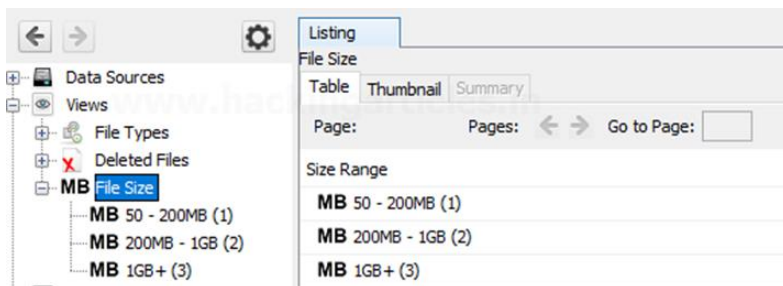
- HTML
- Office
- PDF
- обычный текст
- форматированный текст

КАТЕГОРИИ ФАЙЛОВ - РАСШИРЕНИЯ

- .exe
- .dll
- .bat
- .cmd
- .com

КАТЕГОРИИ ФАЙЛОВ – ПО МИМЕ типам

- application
- audio
- example
- image
- message
- model
- multipart
- text
- video



КАТЕГОРИИ ФАЙЛОВ – УДАЛЕННЫЕ

- Найденные части удаленных файлов

КАТЕГОРИИ ФАЙЛОВ – ПО РАЗМЕРУ

- файлы классифицируются в зависимости от их размера, начиная с 50 МБ.



Краткая памятка использования и
основного функционала.

Autopsy

mac

linux

win

VM

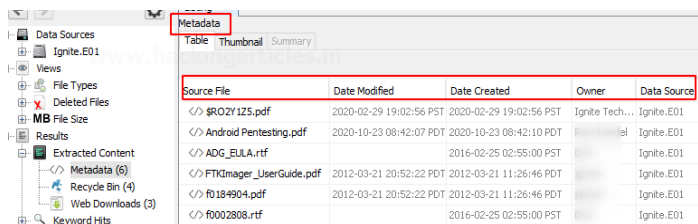
iOS

Android

www.autopsy.com

Работа с Autopsy:

ДРЕВО ДАННЫХ. RESULTS



EXTRACTED CONTENT –

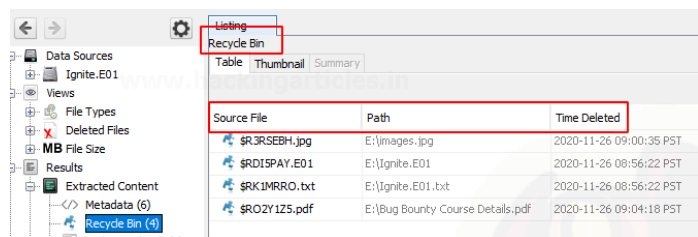
весь извлеченный контент дополнительно
детализируется.

ПРИМЕР:

Metadata

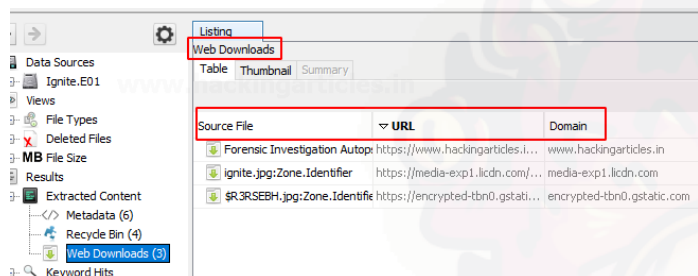
информация о найденных файлах, такие как:

- дату создания
- дату изменения
- владельца файла и т. д.



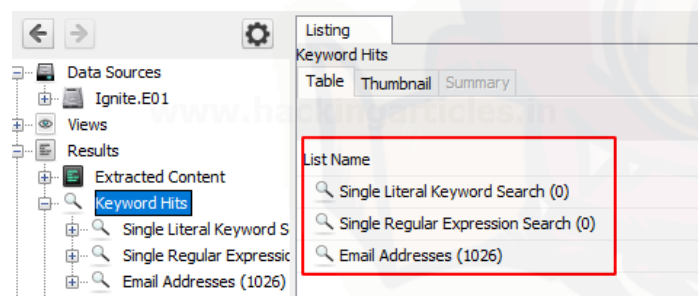
Recycle Bin

в этой категории находятся файлы,
помещенные в корзину.



Web Downloads

Файлы которые были загружены из Интернета.

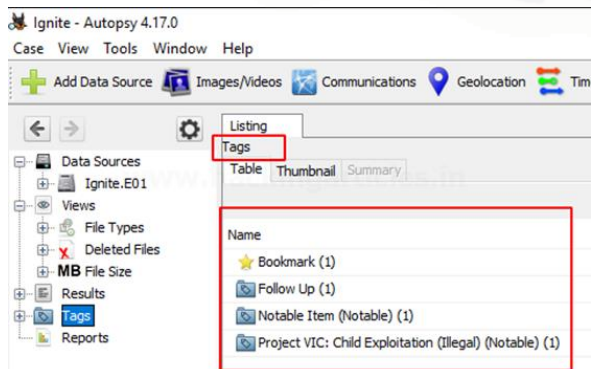


KEYWORD HITS --

Поиск по ключевым словам и маскам.

Может осуществляться по:

- точному совпадению
- электронным письмам
- регулярным выражениям и т. д.



TAGS --

Система меток используемая для:

- создания закладок
- отслеживания
- пометки любого примечательного элемента и т. д.



Краткая памятка использования и
основного функционала.

mac

linux

win

VM

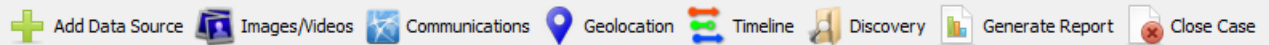
iOS

Android

www.autopsy.com

Работа с Autopsy:

ФУНКЦИОНАЛЬНАЯ ПАНЕЛЬ.



ДОБАВИТЬ ИСТОЧНИК ДАННЫХ:

Добавление дополнительного источника данных к делу

ИЗОБРАЖЕНИЕ/ВИДЕО:

Поиск изображений и видео с помощью различных параметров и нескольких категорий.

КОММУНИКАЦИИ

Визуализация встречающихся связей в сообщениях, электронной почте и т.п.

ГЕОЛОКАЦИЯ

Визуализация найденных гео координат в источниках данных в виде отметок на карте.

ТАЙМ ЛАЙН

Визуализация временных интервалов событий зафиксированных в исследуемой системе

DISCOVERY

Поиск информации по различным дополнительным параметрам

ГЕНЕРАЦИЯ ОТЧЕТА

Создание отчета по делу в различных форматах