

# Обзор утилиты Autopsy

## Содержание

1. Введение
2. Установка, активация, подготовка к работе
3. Работа с утилитой
4. Заключение

## 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/>



**AUTOPSY**  
DIGITAL FORENSICS

СКАЧАТЬ

ДОПОЛНИТЕЛЬНЫЕ МОДУЛИ

## Скачать аутопсия

**ВЕРСИЯ 4.19.3 ДЛЯ WINDOWS**

[СКАЧАТЬ 64-БИТ >](#)

**СКАЧАТЬ ДЛЯ LINUX И OS X**

Autopsy 4 будет работать на Linux и OS X. Для этого:

- Скачать [ZIP-файл](#) аутопсии (ПРИМЕЧАНИЕ: это не последняя версия)
- Linux понадобится пакет Sleuth Kit [Java](#) [.deb](#) [Debian](#)
- Следуйте [инструкциям](#) для установки других зависимостей

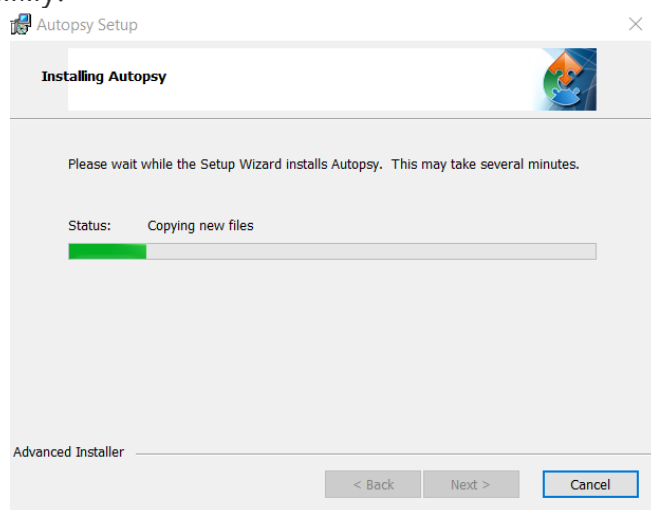
## Модули 3rd Party

модули дополнения 3rd party можно найти в [репозитории модуля github](#).

Из этого репозитория вы можете скачать все модули или только те, которые вам нужны.

## Старые версии

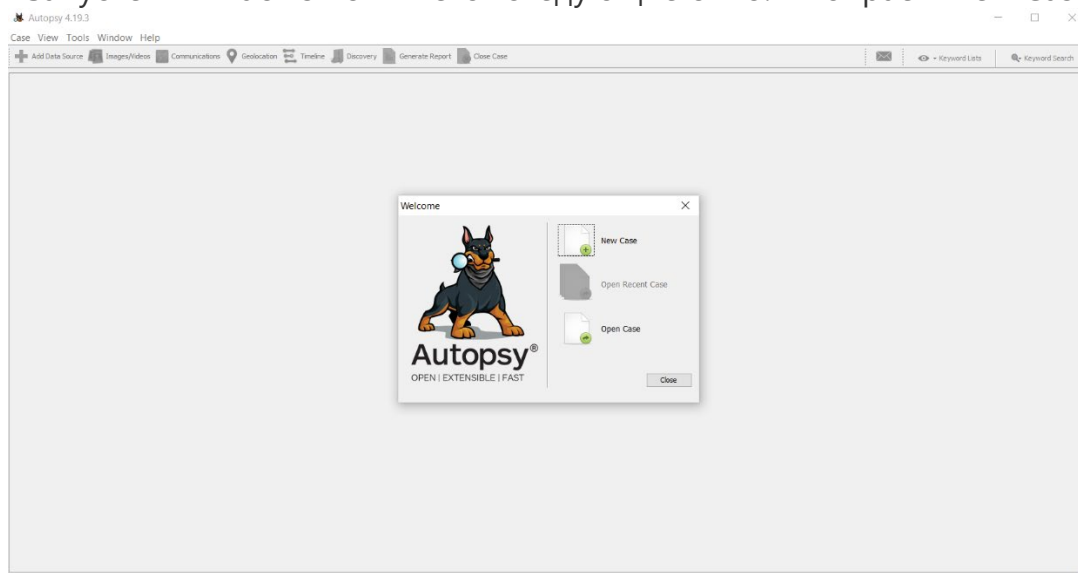
Далее запускаем скаченный файл **autopsy-X.X.X-64bit**  
И устанавливаем программу.



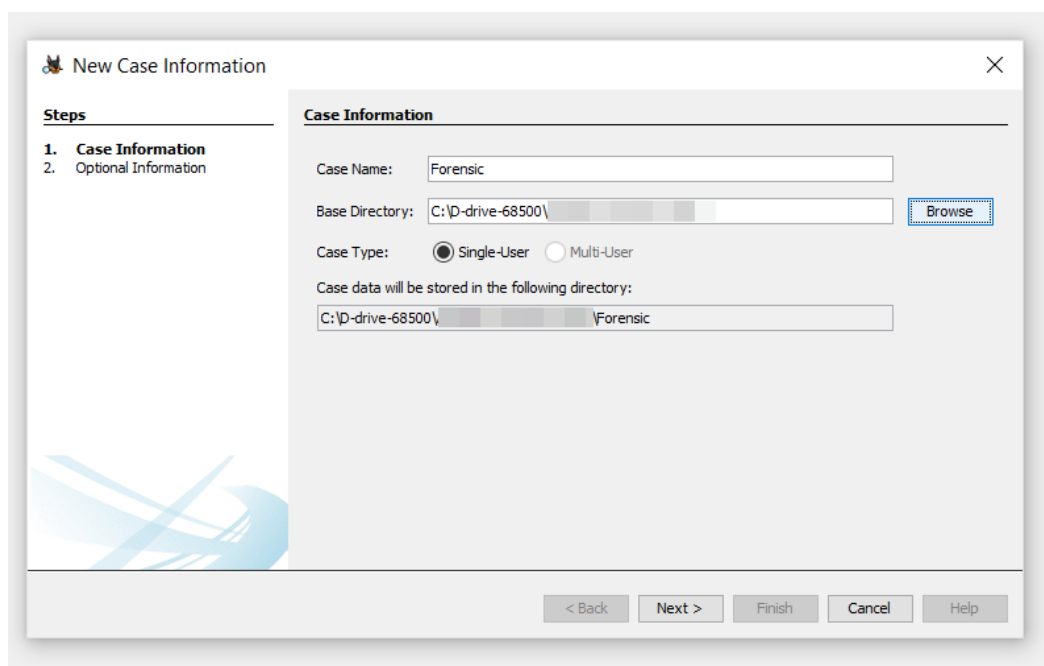
Работа с утилитой

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.

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > Finish Cancel Help

И создаём проект:

Creating Case

Opening case-level services...

Cancel

Далее нужно выбрать источник данных

Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

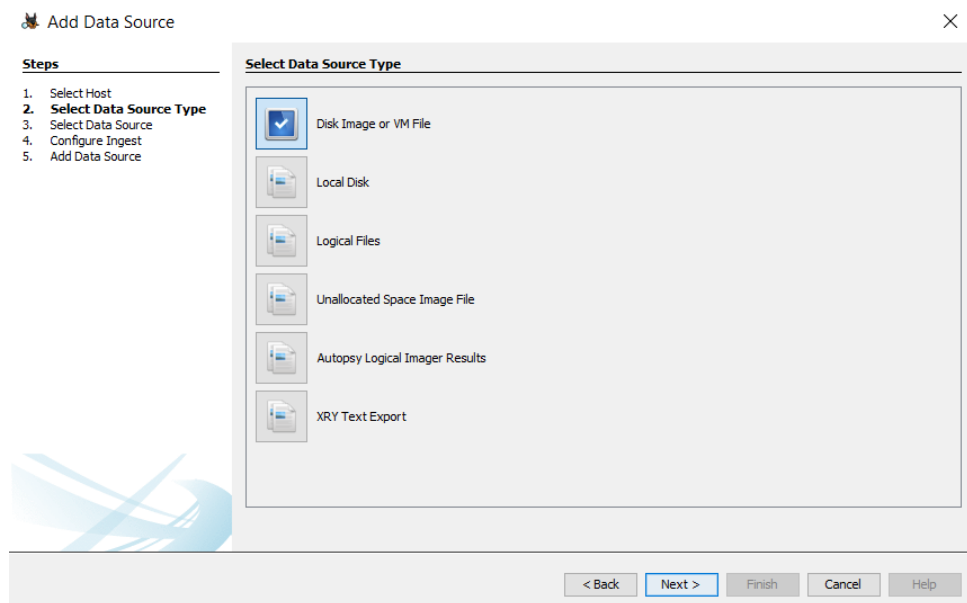
☒ Generate new host name based on data source name

☐ Specify new host name

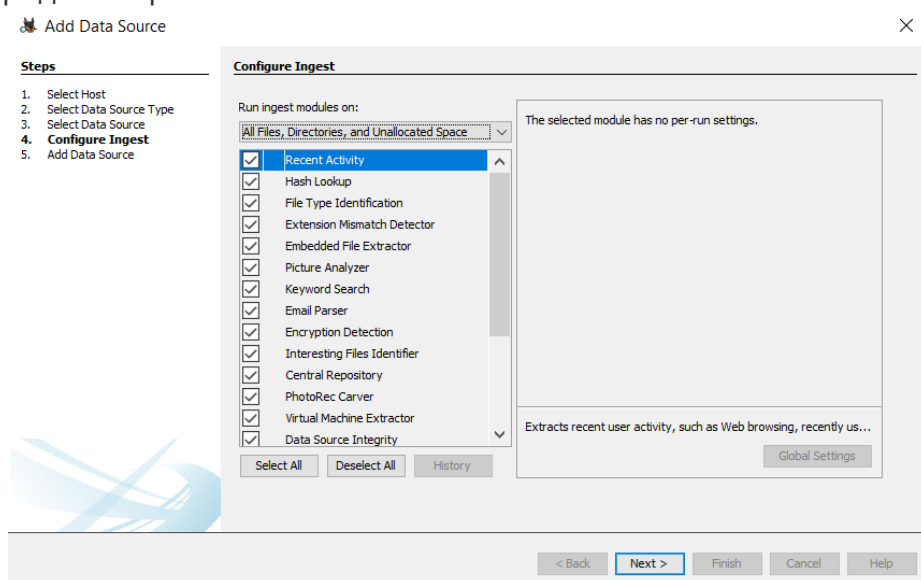
☐ Use existing host

< Back Next > Finish Cancel Help

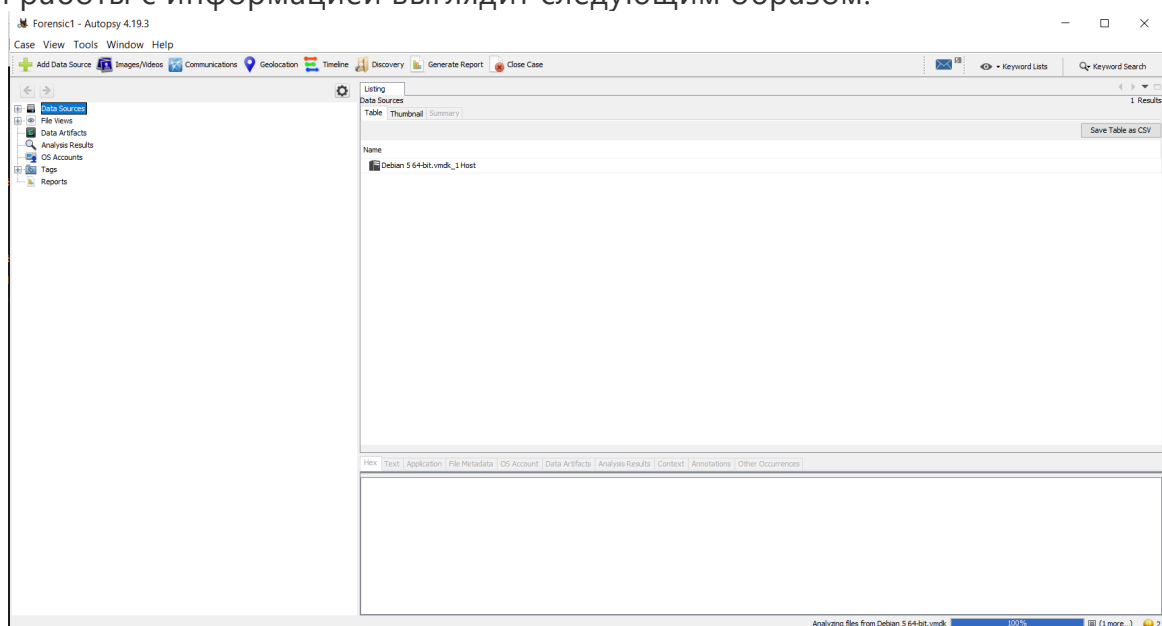
Затем выбираем тип источника файла, который будем анализировать.



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

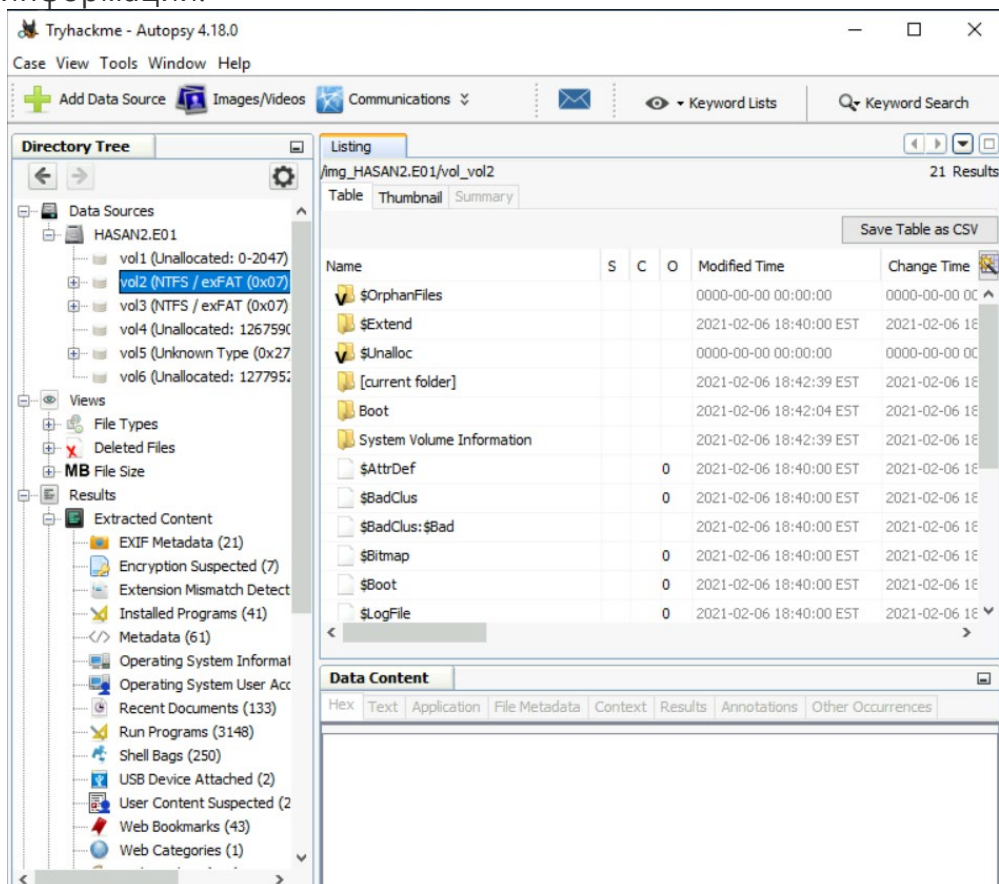


Окно для работы с информацией выглядит следующим образом.

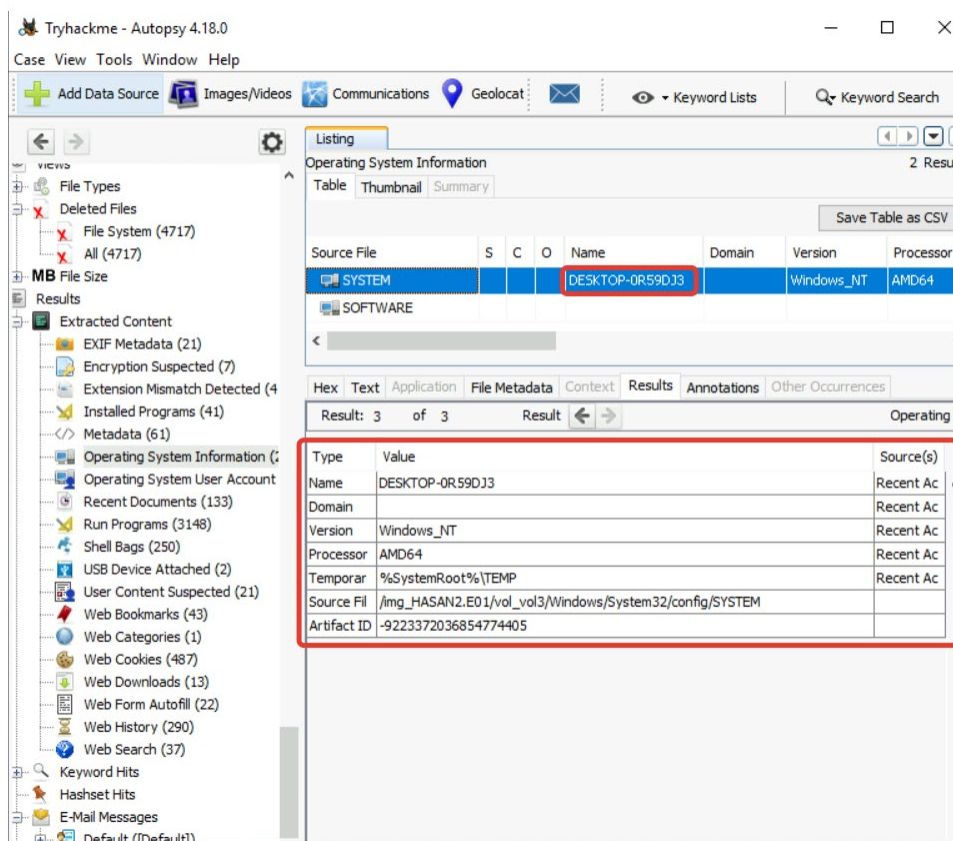


Так как на моем виртуальном диске нет информации, при помощи которой можно было бы описать все инструменты анализа данной программы, то дальше я буду показывать принцип её работы через AttackBox на сайте TryHackMe.

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



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



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



Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocat Keyword Lists Keyword Search

Views

- File Types
- Deleted Files
- File System (4717)
- All (4717)
- MB File Size
- Results
- Extracted Content
- EXIF Metadata (21)
- Encryption Suspected (7)
- Extension Mismatch Detected (4)
- Installed Programs (41)
- Metadata (61)
- Operating System Information (3)
- Operating System User Account
- Recent Documents (133)
- Run Programs (3148)
- Shell Bags (250)
- USB Device Attached (2)
- User Content Suspected (21)
- Web Bookmarks (43)
- Web Categories (1)
- Web Cookies (487)
- Web Downloads (13)
- Web Form Autofill (22)
- Web History (290)
- Web Search (37)
- Keyword Hits
- Hashset Hits
- E-Mail Messages
- Default ([Default])
- Interesting Items
- Accounts
- Email (1)
- Tags
- Reports

Listing

Operating System User Account 15 Results

Table	Thumbnail	Summary
7859479-1005	keshav	2021-02-06 05:39:20 EST
7859479-1006	sivapriya	2021-02-06 05:39:55 EST
7859479-1007	sandhya	2021-02-06 05:40:42 EST
7859479-1008	sriini	2021-02-06 05:41:10 EST
7859479-1001	H454N	2021-02-06 18:48:16 EST
7859479-1002	joshwa	2021-02-06 05:38:00 EST
7859479-500	Administrator	2021-02-06 18:45:38 EST

Save Table as CSV

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 2 of 12 Result

Type	Value	Source(s)
User ID	S-1-5-21-3919888104-523186866-407859479-1006	Recent Ac
Username	sivapriya	Registry
Date Crea	2021-02-06 05:39:55	Recent Ac
Date Acce	2021-02-07 12:05:37	Recent Ac
Count	10	Recent Ac
Password	Password does not expire, Password not required	Recent Ac
Flag	Normal user account	Recent Ac
Path	C:\Users\sivapriya	Recent Ac
Source File	/img_HASAN2.E01/vol_vol3/Windows/System32/config/SAM	
Artifact ID	-9223372036854774723	

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

Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocat Keyword Lists Keyword Search

Views

- Operating System Information (3)
- Operating System User Account
- Recent Documents (133)
- Run Programs (3148)
- Shell Bags (250)
- USB Device Attached (2)
- User Content Suspected (21)
- Web Bookmarks (43)
- Web Categories (1)
- Web Cookies (487)
- Web Downloads (13)
- Web Form Autofill (22)
- Web History (290)
- Web Search (37)
- Keyword Hits
- Hashset Hits
- E-Mail Messages
- Default ([Default])
- Interesting Items
- Accounts
- Email (1)
- Tags
- Reports

Listing

Default 1 Results

Table	Thumbnail	Summary
msg_43.txt		

Save Table as CSV

Source File S C O E-Mail From E-Mail To Subject

msg_43.txt				>	webmaster@python.org;	Banned file: auto_mail
------------	--	--	--	---	-----------------------	------------------------

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 2 of 30 Result

From: > 2004-11-26 22:41:44 EST

To: webmaster@python.org;

CC:

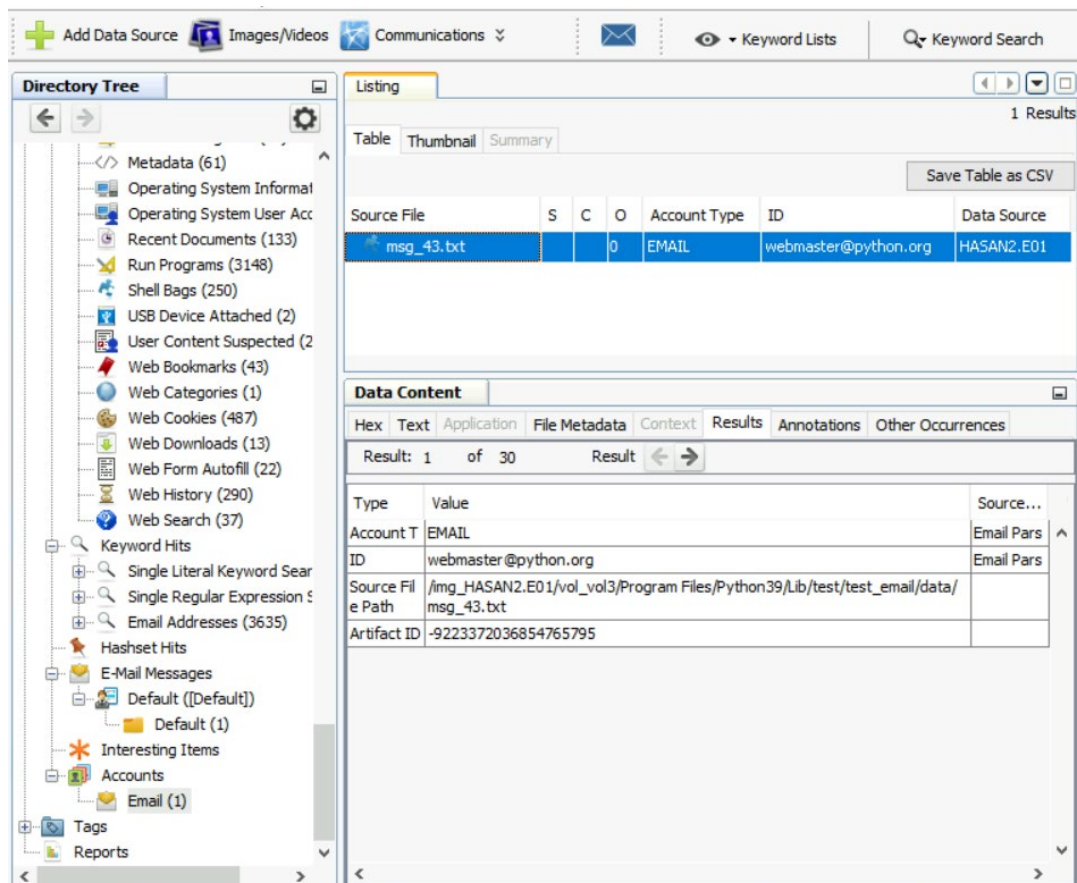
Subject: Banned file: auto\_mail.python.bat in mail from you

Headers Text HTML RTF Attachments (2) Accounts

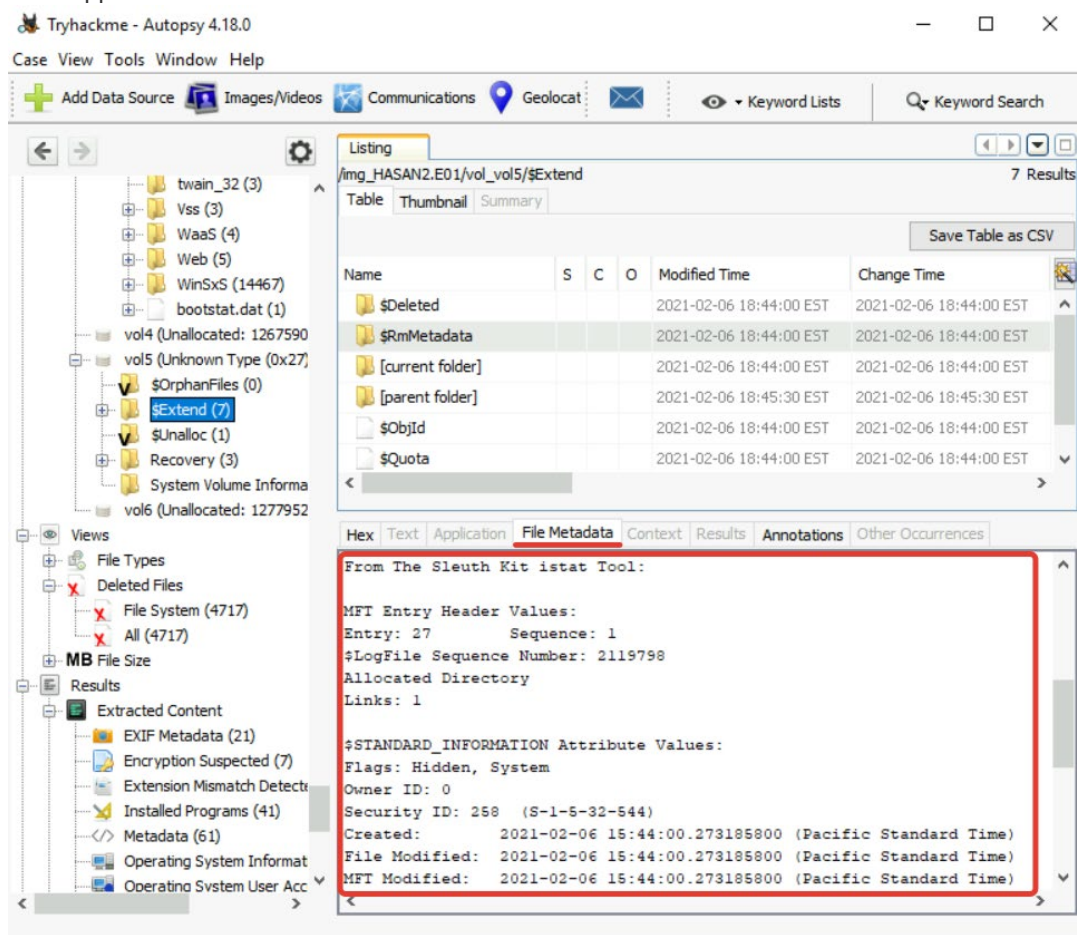
Original Text

BANNED FILENAME ALERT

Your message to: xxxxxxxx@dot.ca.gov, xxxxxxxxxxxx@dot.ca.gov, xxxxxxxx



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



Метаданные папки.



Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocat Keyword Lists Keyword Search

Listing  
/img\_HASAN2.E01/vol\_vol5/System Volume Information 3 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Ac
[current folder]				2021-02-06 18:45:30 EST	2021-02-06 18:45:30 EST	202
[parent folder]				2021-02-06 18:45:30 EST	2021-02-06 18:45:30 EST	202
tracking.log				2021-02-06 18:45:30 EST	2021-02-06 18:45:30 EST	202

Hex Text Application File Metadata Context Results Annotations Other Occurrences

From The Sleuth Kit istat Tool:

MFT Entry Header Values:  
Entry: 42 Sequence: 1  
\$LogFile Sequence Number: 4220344  
Allocated File  
Links: 1

\$STANDARD\_INFORMATION Attribute Values:  
Flags: Hidden, System, Archive  
Owner ID: 0  
Security ID: 268 (S-1-5-18)  
Created: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)  
File Modified: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)  
MFT Modified: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)

Метаданные файла.

Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocat Keyword Lists Keyword Search

Listing  
/img\_HASAN2.E01/vol\_vol5/System Volume Information 3 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Ac
[current folder]				2021-02-06 18:45:30 EST	2021-02-06 18:45:30 EST	202
[parent folder]				2021-02-06 18:45:30 EST	2021-02-06 18:45:30 EST	202
tracking.log				2021-02-06 18:45:30 EST	2021-02-06 18:45:30 EST	202

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Security ID: 268 (S-1-5-18)  
Created: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)  
File Modified: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)  
MFT Modified: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)  
Accessed: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)

\$FILE\_NAME Attribute Values:  
Flags: Hidden, System, Archive  
Name: tracking.log  
Parent MFT Entry: 41 Sequence: 1  
Allocated Size: 20480 Actual Size: 20480  
Created: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)  
File Modified: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)  
MFT Modified: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)  
Accessed: 2021-02-06 15:45:30.272987800 (Pacific Standard Time)

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



Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time
[current folder]				2021-02-06 18:42:39 EST	2021-02-06 18:42:39 EST
[parent folder]				2021-02-06 18:42:39 EST	2021-02-06 18:42:39 EST
tracking.log			0	2021-02-06 18:42:39 EST	2021-02-06 18:42:39 EST

Data Content

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Accessed 2021-02-06 18:42:39 EST  
 Created 2021-02-06 18:42:39 EST  
 Changed 2021-02-06 18:42:39 EST  
 MD5 8114ebaba39ea38afdac143368b895b7  
 SHA-256 5afab0018cf8803e43a02ca095c9f37a5bda0428002b4b49d6a60c8  
 Hash  
 Lookup UNKNOWN

Просмотр файлов cookie для браузера.

Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Keyword Lists Keyword Search

Directory Tree

Listing

Web Cookies 487 Results

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Source File	S	C	O	URL	Date/Time
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06
cookies.sqlite			0	.youtube.com	2021-02-06
cookies.sqlite			0	.youtube.com	2021-02-06
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06

Data Content

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match Text Source: File Text

```

mor_cookies

id originAttributes name value host path expiry lastAccessed
creationTime isSecure isHttpOnly inBrowserElement sameSite rawSameSite schemeMap
1 __cfduid d48ee211381dd30587a90844d087a00741612607340 .sathyabama.ac.in / 1615199340 1612607400712000 1612607340654000 1 1 0 1
1 2
5 GPS 1 .youtube.com / 1612609198 1612607466111000 1612607398325002 0 0 0 0 2
6 VISITOR_INFO1_LIVE_EWcuq5tobA .youtube.com / 1628159398
  
```

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.

The screenshot shows the Autopsy interface with the 'Web Cookies' results pane. The 'Listing' tab is active, displaying a table of cookies. The 'Data Content' pane below shows the 'moz\_cookies' table with 72 entries.

Source File	S	C	O	URL	Date/Time
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06
cookies.sqlite			0	.youtube.com	2021-02-06
cookies.sqlite			0	.youtube.com	2021-02-06
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06

id	originAtt...	name	value	host
1		__cfduid	d48ee211381dd30587a90844d087a00741612607340	.sathy
5		GPS	1	.yout
6		VISITOR_...	_EWcuq5tobA	.yout
10		__gat	1	.sathy
12		__ga	GA1.3.1386023014.1612607403	.sathy
13		__gid	GA1.3.1494712730.1612607403	.sathy
14		collect_ch...	3	www.
15		collect_ch...	3	www.

Во вкладке Results так же как и во 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.

The screenshot shows the Autopsy interface with the 'Web Cookies' results pane. The 'Listing' tab is active, displaying a table of cookies. The 'Data Content' pane below shows the 'moz\_cookies' table with 72 entries. A red box highlights the 'Cookie Details' section, which provides information about a specific cookie.

Source File	S	C	O	URL	Date/Time
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06
cookies.sqlite			0	.youtube.com	2021-02-06
cookies.sqlite			0	.youtube.com	2021-02-06
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06
cookies.sqlite			0	.sathyabama.ac.in	2021-02-06

**Cookie Details**

Domain: sathyabama.ac.in

URL: .sathyabama.ac.in

Name: \_\_cfduid

Value: d48ee211381dd30587a90844d087a00741612607340

Program Name: Firefox

**Dates**

Created: 2021-02-06 05:29:00 EST

Date/Time: 2021-02-06 05:30:00 EST



Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Keyword Lists Keyword Search

**Directory Tree**

- config (49)
  - Journal (2)
  - RegBack (2)
  - systemprofile (3)
  - TxR (9)
  - Configuration (8)
  - ContainerSettingsPr
  - cs-CZ (14)
  - da-DK (15)
  - DDFs (8)
  - de-DE (15)
  - DiagSvc (9)
  - Dism (29)
  - downlevel (121)
  - drivers (430)
  - DriverState (3)
  - DriverStore (5)
  - DRVSTORE (3)
  - dsc (5)
  - el-GR (15)
  - en (5)
  - en-GB (12)
  - en-US (1773)
  - es-ES (15)
  - es-MX (12)
  - et-EE (11)
  - F12 (24)
  - ff-Adlm-SN (4)

**Listing**

/img\_HASAN2.E01/vol\_vol3/Windows/System32/config 49 Results

Table Thumbnail Summary

Page: Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time
ELAM{53b39eac-18c4-11ea-a811-000d3aa4692b}.TMContainer00				2021-02-06 18:...
<b>SAM</b>				2021-02-07 13:...
SAM.LOG1				2019-12-07 04:...
SAM.LOG2				2019-12-07 04:...
SECURITY				2021-02-07 13:...

**SECURITY**

**Data Content**

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 1 of 12 Result Operating S

Type	Value	Source...
User ID	S-1-5-21-3919888104-523186866-407859479-1005	Recent Ac
Username	keshav	Registry
Date Crea	2021-02-06 05:39:20	Recent Ac
Date Acce	2021-02-07 11:45:00	Recent Ac
Count	5	Recent Ac
Password	Password does not expire, Password not required	Recent Ac
Flag	Normal user account	Recent Ac
Path	C:\Users\keshav	Recent Ac
Source Fil	/img_HASAN2.E01/vol_vol3/Windows/System32/config/SAM	
Artifact ID	-922337203685477424	

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 загружено.

+ Add Data Source Images/Videos Communications Keyword Lists Keyword Search

**Directory Tree**

- File Types
- Deleted Files
- MB File Size
- Results
  - Extracted Content
    - EXIF Metadata (21)**
    - Encryption Suspected (7)
    - Extension Mismatch Detect
    - Installed Programs (41)
    - Metadata (61)
    - Operating System Informal
    - Operating System User Acc
    - Recent Documents (133)
    - Run Programs (3148)
    - Shell Bags (250)
    - USB Device Attached (2)
    - User Content Suspected (2)
    - Web Bookmarks (43)
    - Web Categories (1)
    - Web Cookies (487)
    - Web Downloads (13)
    - Web Form Autofill (22)
    - Web History (290)
    - Web Search (37)
  - Keyword Hits
    - Single Literal Keyword Sear
    - Single Regular Expression S
    - Email Addresses (3635)

**Listing**

EXIF Metadata 21 Results

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Source File	S	C	O	Date Created
WelcomeScan.jpg			0	2004-04-09 08:17:...
68F642185F1C30EC75F2A5E79EE1C6A3A47B7335			0	2020-11-23 20:21:...
00B55E0C5926E012F0327A438256D9E91FA5D3EE			0	2016-08-22 11:41:...
<b>950BE8F617507E9B6F2D8A066311BEFB3E0E51C3</b>			0	2017-06-30 14:33:...
1491BF6236E8077EECE51F3D8C5A943A5D1F1B5			0	2020-02-15 08:37:...
CAEC27E7B03C7D632A5E1A50A13E42A2E057E00			0	2018-02-26 11:24:...

**Data Content**

Hex Text Application File Metadata Context Results Annotations Other Occurrences

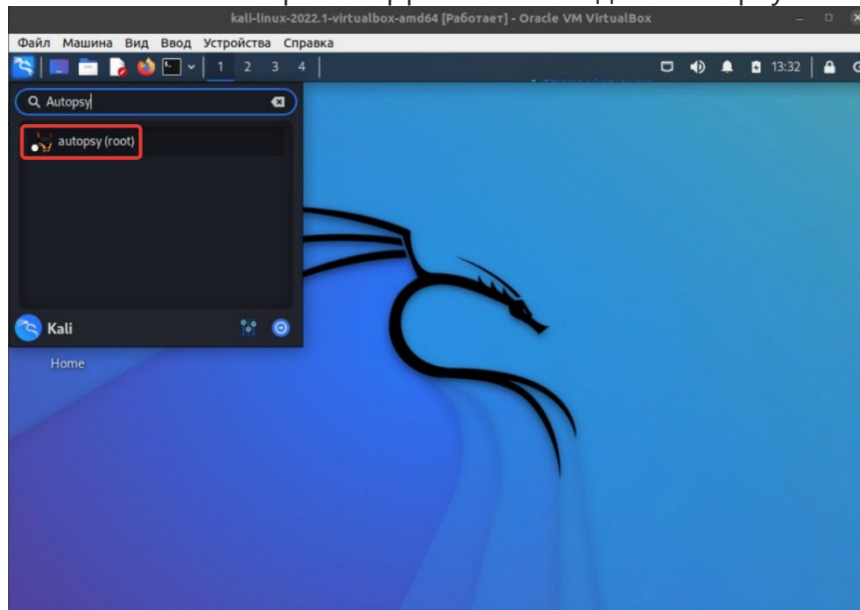
Result: 1 of 2 Result

Type	Value	Source...
Date Crea	2017-06-30 14:33:19	Picture An
Device Mo	Canon EOS 700D	Picture An
Device Ma	Canon	Picture An
Source Fil e Path	/img_HASAN2.E01/vol_vol3/Users/shreya/AppData/Local/Mozilla/Firefox/Profiles/zcy0xhuf.default-release/cache2/entries/950BE8F617507E9B6F2D8A066311BEFB3E0E51C3	
Artifact ID	-9223372036854767594	

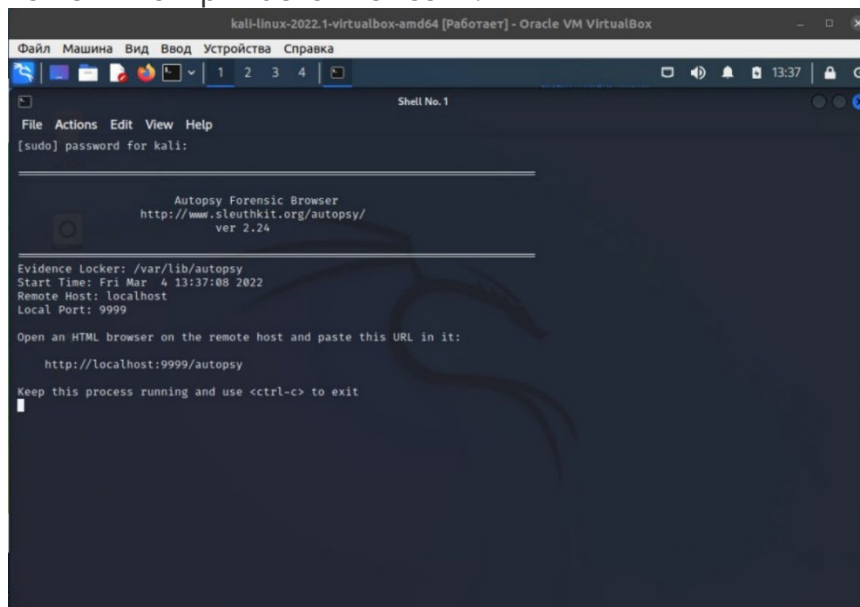
## Использование Autopsy в Linux

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 представлены 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.