

# How to Use Kali Linux for OSINT Investigations



Practical OSINT

Follow

Published in

OSINT Team

5 min read

Nov 12, 2024

Listen

Share

More

A Comprehensive Step-by-Step Guide for Beginners.



Image source: Author's screenshot – steps for setting up Kali Linux.

## You will learn:

- How to download and install VirtualBox.
- Setting up Kali Linux.
- Researching and integrating OSINT tools from GitHub into Kali Linux.
- Troubleshooting in Kali Linux.
- Using an OSINT tool to identify websites linked to an email.

## Requirements

A desktop PC or laptop with at least 2 GB of RAM (4 GB or more is recommended for better performance).

Let's Get Started!

## 1. Setting Up VirtualBox

- Download VirtualBox by clicking here, or follow the steps outlined below.
- Run the installer and follow the on-screen instructions.



Figure 1: Steps for downloading virtualbox

- During installation, you may encounter an error stating: “Microsoft Visual C++ 2019 package missing.”

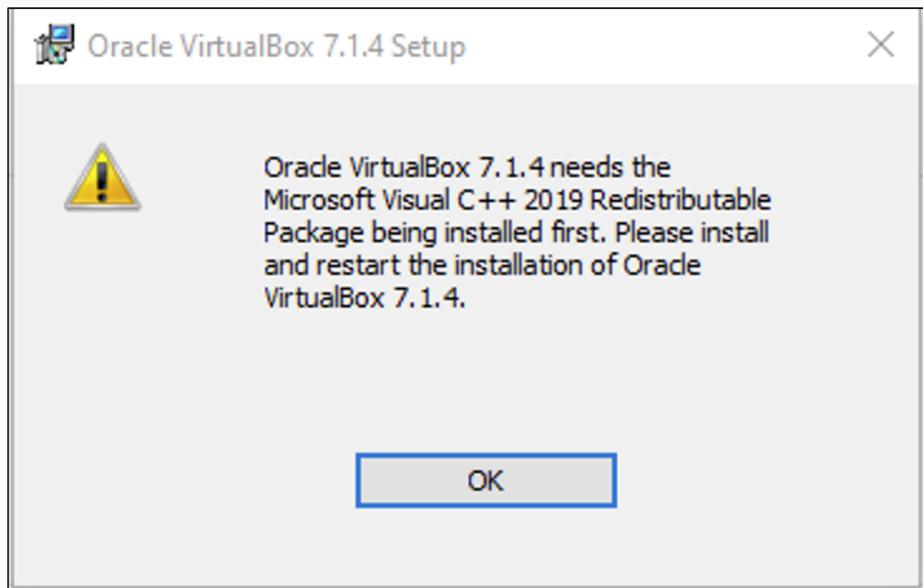


Figure 2: “Microsoft Visual C++ 2019 package missing” message

- To resolve this error, click here to download and install the Microsoft Visual C++ 2019 package or follow the following steps.



Figure 3: Steps for download and install the Microsoft Visual C++ 2019 package

- Once the package is installed, resume the installation of VirtualBox.

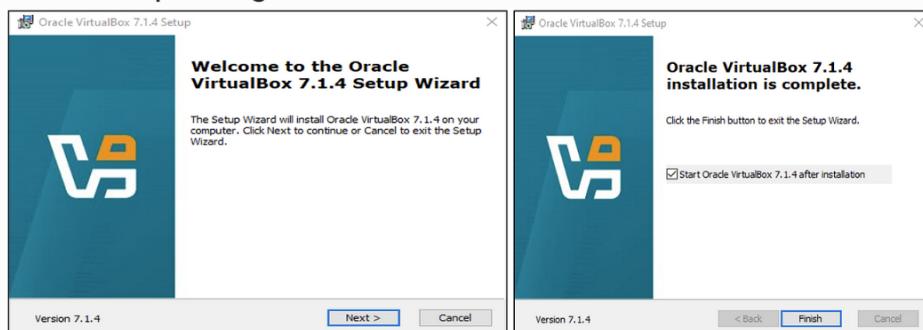


Figure 4: Resumption of VirtualBox installation

Upon successful installation, your VirtualBox interface should resemble the following:

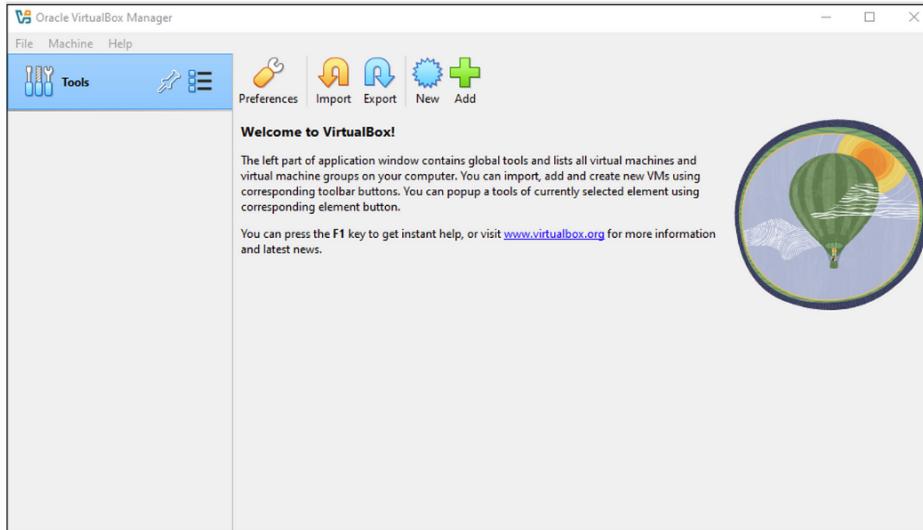


Figure 5: VirtualBox final interface

Next, install the VirtualBox Extension Pack by following the instructions or click here for a direct download.



Figure 6: Installation of VirtualBox Extension Pack

Your VirtualBox setup is complete, and you're ready to move on to Kali Linux!

## 2. Setting Up Kali Linux

- Download the pre-built Kali Linux virtual machine for VirtualBox by using the following steps, or click here for a direct download.

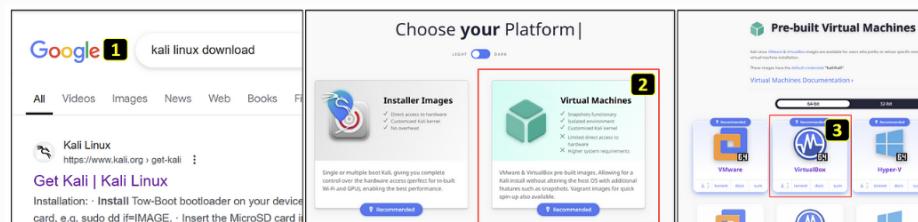


Figure 7: Steps for downloading Kali Linux

- Extract the files from the Kali Linux folder, open it, and double-click on the .vbox file, as shown below.

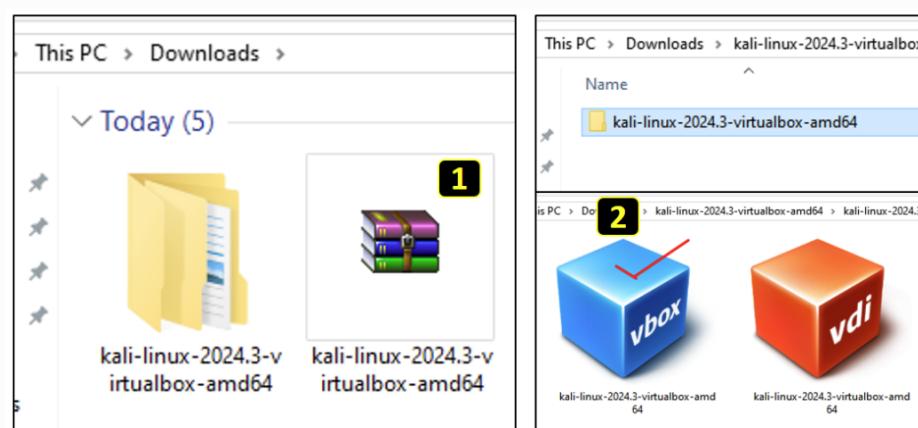


Figure 8: Extraction of Kali Linux files

After double-clicking the .vbox file, the pre-built Kali Linux virtual machine will be

automatically added to VirtualBox, as shown below.

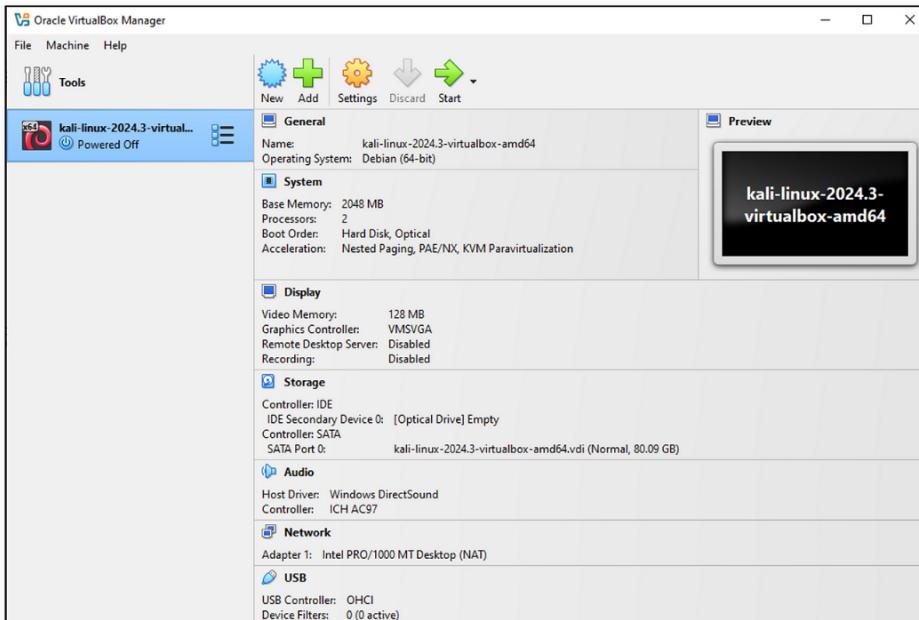


Figure 9: Adding of .vbox Kali Linux file to VirtualBox

## Configuring Memory Allocation

The default memory allocation for Kali Linux is set to 2 GB, which is suitable, but you can increase this up to your system's capability if desired.

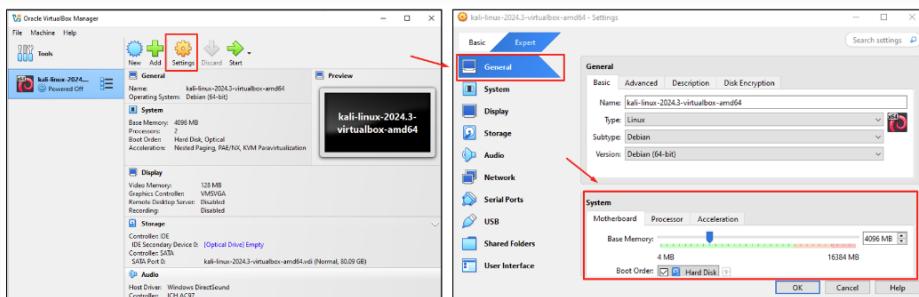


Figure 10: Configuration of memory allocation

## Starting Kali Linux

To launch Kali Linux, click the Start button and use the following credentials to log in:

- Username: kali
- Password: kali

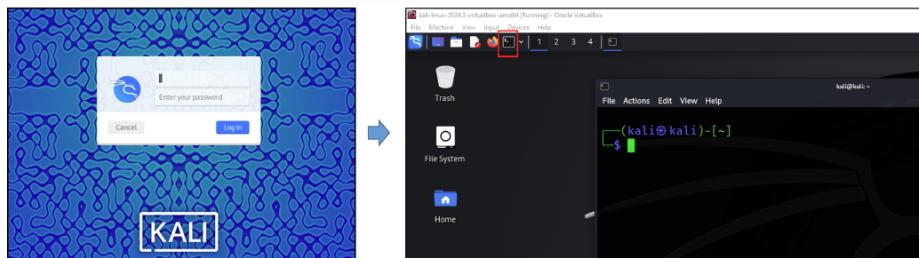


Figure 11: Starting Kali Linux

Once logged in, open the terminal and update your system with the following commands:

- sudo apt update
- sudo apt upgrade

```

Kali@Kali: ~
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.2 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.4 MB]
46% [3 Contents-amd64 3,676 kB/48.4 MB 8%] 1,125 kB/s 39s
Kali@Kali: ~
$ sudo apt upgrade

```

Figure 12: Updating and upgrading Kali Linux

Your Kali Linux system is ready for OSINT investigations!

Let's move on to the next section, where we'll learn how to find, install, and integrate OSINT tools in Kali Linux.

## 3. Integrating OSINT Tools into Kali Linux

### a. GitHub OSINT Research

Now, let's look for OSINT tools on GitHub.

To find OSINT tools, utilize Google Dorks in your searches. Here are some examples you can use:

- site:github.com “OSINT Tool”
- site:github.com “OSINT” AND “Email”
- site:github.com “OSINT” AND “Phone Number”

This will help you discover various tools specifically tailored for OSINT investigations.

You can also search directly on GitHub using terms like “Email tool” to find relevant results.

### b. Installing an OSINT Tool

Let's choose the “Email OSINT tool” for this demonstration.

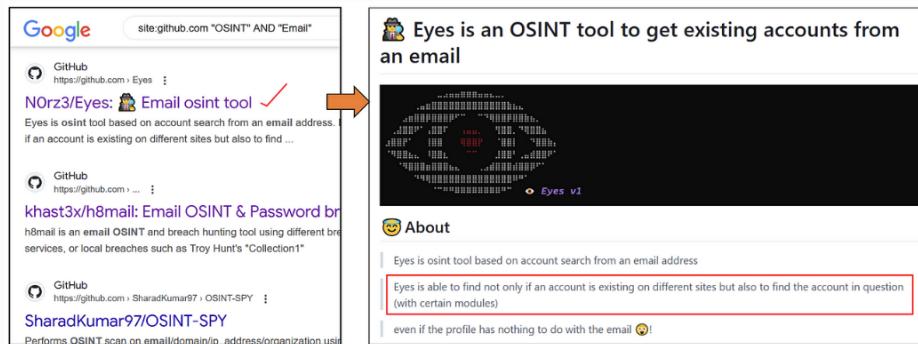


Figure 13: Researching GitHub for OSINT tools

- Open the chosen GitHub link and scroll down to the “Requirements” and “Usage” sections.
- Copy each command and paste them into the Kali Linux terminal:

```

$ git clone https://github.com/N0rz3/Eyes.git
$ cd ./Eyes
$ pip3 install -r requirements.txt

(kali㉿kali)-[~]
$ git clone https://github.com/N0rz3/Eyes.git
Cloning into 'Eyes'...
remote: Enumerating objects: 188, done.
(kali㉿kali)-[~]
$ cd Eyes
(kali㉿kali)-[~/Eyes]
$ pip3 install -r requirements.txt

  Downloading requests (from beautifulsoup4>bs4>--r requirements.txt (line 8)) (2.5)
    Downloading argparse-1.4.0-py2.py3-none-any.whl (52 kB)
      Downloading DateTime-5.5-py3-none-any.whl (23 kB)
        Downloading opencv_python-4.10.0.84-cp37abi3-manylinux2_17_x86_64.manylin
        ux2014_x86_64.whl (62.5 kB)
          52.6/52.6 kB 450.0 kB/s eta 0:00:00
          2.7/62.5 MB 389.6 kB/s eta 0:02:34

```

Figure 14: Adding GitHub tools into Kali Linux

## c. Troubleshooting Common Issues

Sometimes you may face errors during installation, such as:

```

4_x86_64.whl (4.5 MB) 4.5/4.5 MB 56.2 kB/s eta 0:00:00
Installing collected packages: scrape-search-engine, argparse, PyWavelets,
opencv-python, datetime, imagehash, bs4
ERROR: pip's dependency resolver does not currently take into account all t
he packages that are installed. This behaviour is the source of the followi
ng dependency conflicts.
netexec 1.2.0+git20240529.7ece667 requires aioconsole<0.7.0, ≥0.6.2, but yo
u have aioconsole 0.7.0 which is incompatible.
netexec 1.2.0+git20240529.7ece667 requires lsassy≥3.1.11, but you have lsa
ssy 3.1.10 which is incompatible.
netexec 1.2.0+git20240529.7ece667 requires pyasn1-modules<0.3.0, ≥0.2.8, bu
t you have pyasn1-modules 0.3.0 which is incompatible.
netexec 1.2.0+git20240529.7ece667 requires termcolor==1.1.0, but you have t
ermcolor 2.4.0 which is incompatible.
crackmapexec 5.4.0 requires aioconsole<0.4.0, ≥0.3.3, but you have aioconso
le 0.7.0 which is incompatible.
crackmapexec 5.4.0 requires masky<0.2.0, ≥0.1.1, but you have masky 0.2.0 w
hich is incompatible.

```

Figure 15: Troubleshooting errors during tools installation

Don't worry! Here are some troubleshooting steps:

- Restart your Kali Linux and re-run the command.
- Ensure your system is updated with sudo apt update and sudo apt upgrade.
- Search the first line of the error message online for potential solutions.
- Remember, the more you troubleshoot, the better you'll get at navigating Kali Linux!

For me, restarting Kali Linux and rerunning the last command \$ pip3 install -r requirements.txt helped solve installation issues.

## d. Using the Email OSINT Tool

Copy the command, paste it into the Kali Linux terminal, and press Enter, as demonstrated below.

The screenshot shows two terminal windows. The left window displays the usage information for the 'eyes' tool:

```
Usage
usage: python eyes.py [-h] [-m] [email]

positional arguments:
  email      search information on the target email with modules, se

options:
  -h, --help   show this help message and exit
  -m, --modules gives you all the email modules used by Eyes
```

An orange arrow points from the right side of the usage text to the right terminal window. The right window shows the tool's output for the email 'example@gmail.com':

```
(kali㉿kali)-[~/Eyes]
$ python eyes.py -m example@gmail.com
sh: 1: title: not found

... (A large ASCII art logo of a face with many eyes)

Eyes v1
BY norze
Tool made with * (N0rz3 on GitHub 🐫)

[*] Email modules :
  -Duolingo      # scrapable
  -GitHub         # scrapable
  -Gravatar       # scrapable
  -Imgur          #
  -Mail.ru        #
  -Pastebin       # links dump
  -Protonmail     # scrapable
  -Bitmoji        #
  -Instagram      #
  -X (Twitter)    #
```

Figure 16: Usage of GitHub tools

Now, analyze the target email to assess the tool's effectiveness. This tool reveals the profile picture and the names of social media platforms associated with the email, as shown below.

The screenshot shows the 'eyes' tool's output for the target email 'example@gmail.com'. It includes the ASCII art logo, the GitHub credit, and detailed analysis results:

```
(kali㉿kali)-[~/Eyes]
$ python eyes.py example@gmail.com
sh: 1: title: not found

... (The same ASCII art logo as in Figure 16)

Eyes v1
BY norze
Tool made with * (N0rz3 on GitHub 🐫)

#####example@gmail.com#####
[+] Email valid !
- Name : example
- Domain : gmail.com

x ProtonMail
x Mail.ru
M Duolingo
M Gravatar
x Imgur

[*] Imgur
[*] Bitmoji
M X (Twitter)

✓ GitHub
  └─ Name : my-orgainzation-example
      └─ Avatar : https://avatars.githubusercontent.com/u/8...
          └─ No default profile picture

[VENOM] ⚡ Face detected !

[+] Result save here : /home/kali/Eyes/facial_recognition-example.jpg

[~] Paste :
  https://pastebin.com/BC6YgjpQ
  https://pastebin.com/FQBFeSUg
  https://pastebin.com/sEUG6u0f
  https://pastebin.com/GYMntw9K
  https://pastebin.com/qQ3C1Rs9
  https://pastebin.com/8pM3Ebix
  https://pastebin.com/biDhzM25
  https://pastebin.com/gffdMj5X
  https://pastebin.com/vc5TchdG
```

## Wrapping Up

Congratulations! You are now equipped to explore various OSINT tools within Kali Linux. Developing expertise in Kali Linux comes down to consistent practice and troubleshooting. If you have any questions or need further assistance, don't hesitate to ask in the comments section!