

SAVONIA

Linux as a Cybersecurity Tool

Cybersecurity Fundamentals

Markku Kellomäki



Genal information about Linux

- Linux is a family of free and open-source operating systems based on the Linux kernel.
 - Under active development since 1991, led by [Linus Torvalds](#).
 - Today 90% of all cloud infrastructure and 74% of the world's smartphones are powered by Linux.
- Operating systems based on Linux are known as Linux distributions or distros.
 - Examples include Debian, Ubuntu, Fedora, Raspbian OS (Raspberry Pi), Kali linux, Parrot and many others.
- Differences to Windows and Mac OS
 - File systems are different
 - Command-line operation is very important in using Linux
 - Linux is free and open source

Linux distributions with cybersecurity tools

- Some Linux distributions come default with a suite of cybersecurity tools, here are some of the most popular:
 1. [Kali Linux](#) (the distribution we use in this course)
 - Most popular for pentesting
 2. [Parrot OS](#)
 - Focus on user privacy, still very good for pentesting
 3. [Black Arch](#)
 - Minimum amount of default tools but a large library for customization
 4. [CAINE Linux](#)
 - Digital forensics
 5. [NodeZero](#)
 - SaaS platform
- [Comparison of Linux distributions for cybersecurity students](#)

SAVONIA

Installation of Kali linux



Options for running Kali Linux

- There are various options for running Kali Linux depending on your host operating system.
- Windows:
 1. Bootable USB drive
 2. Dual-boot system (needs disk partitioning etc)
 3. Virtual machine: VirtualBox, VMware Workstation
- Mac
 1. Bootable USB drive (only for Intel Macs, not M-series Macs)
 2. Virtual machine: UTM, VirtualBox, VMware Fusion

Install VirtualBox

- Download Virtualbox: <https://www.virtualbox.org/wiki/Downloads>
 - Check the proper package for your computer! M1, M2, Mac = Apple Silicon
 - Accept and download also the extension pack

Download VirtualBox

The VirtualBox Extension Pack is available for personal and educational use on this page under the PUEL license. The VirtualBox Extension Pack is also available under commercial or enterprise terms. By downloading, you agree to the terms and conditions of the respective license.

VirtualBox Platform Packages

VirtualBox 7.1.6 platform packages

- [Windows hosts](#)
- [macOS / Intel hosts](#)
- [macOS / Apple Silicon hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)
- [Solaris 11 IPS hosts](#)

Platform packages are released under the terms of the [GPL version 3](#)

VirtualBox Extension Pack

VirtualBox 7.1.6 Extension Pack

This VirtualBox Extension Pack Personal Use and Educational License governs your access to and use of the VirtualBox Extension Pack. It does not apply to the VirtualBox base package and/or its source code, which are licensed under version 3 of the GNU General Public License "GPL").

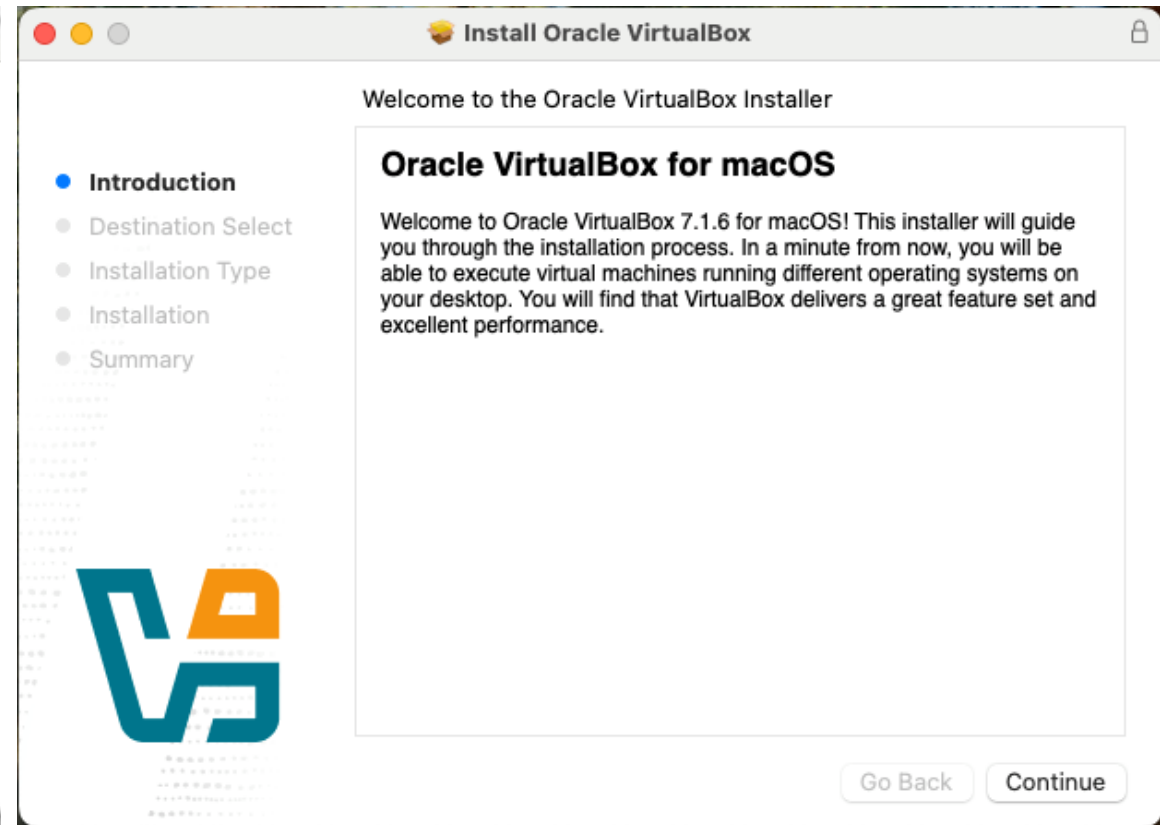
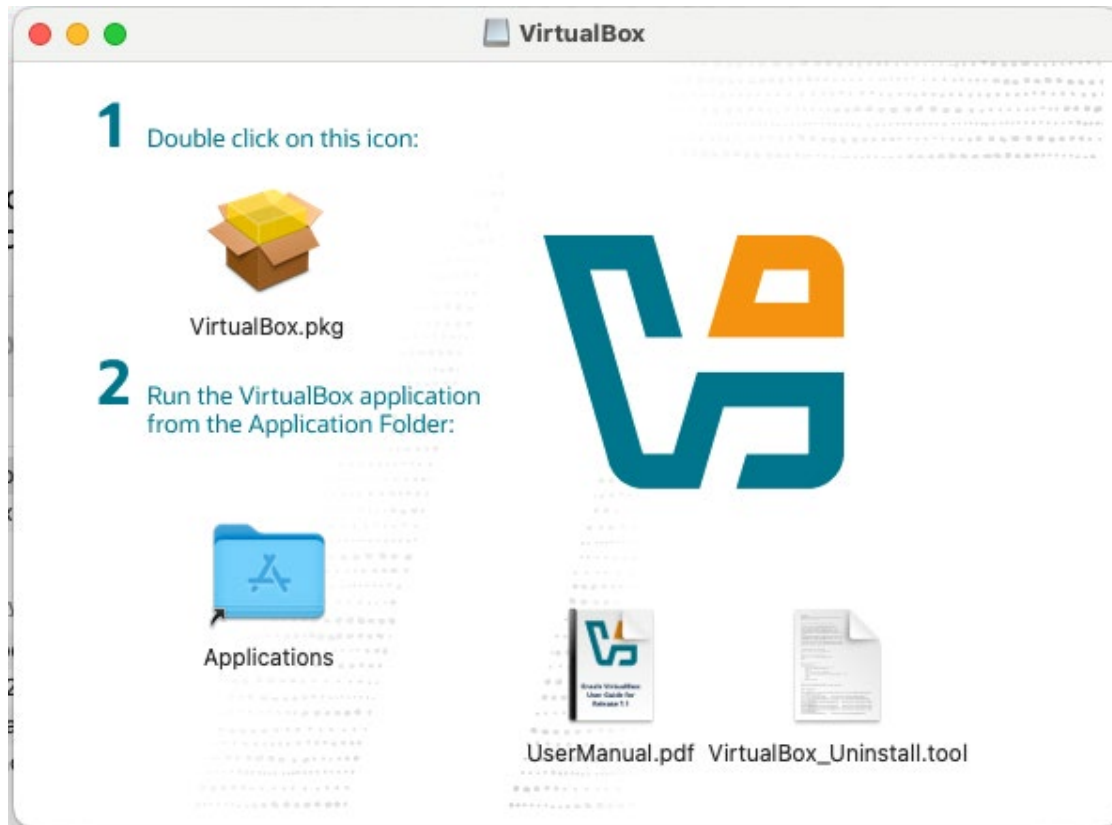
See our [FAQ](#) for answers to common questions.

VirtualBox Extension Pack Personal Use and Educational License (PUEL)

[PUEL License FAQ](#) [PUEL License Text](#) [Accept and download](#)

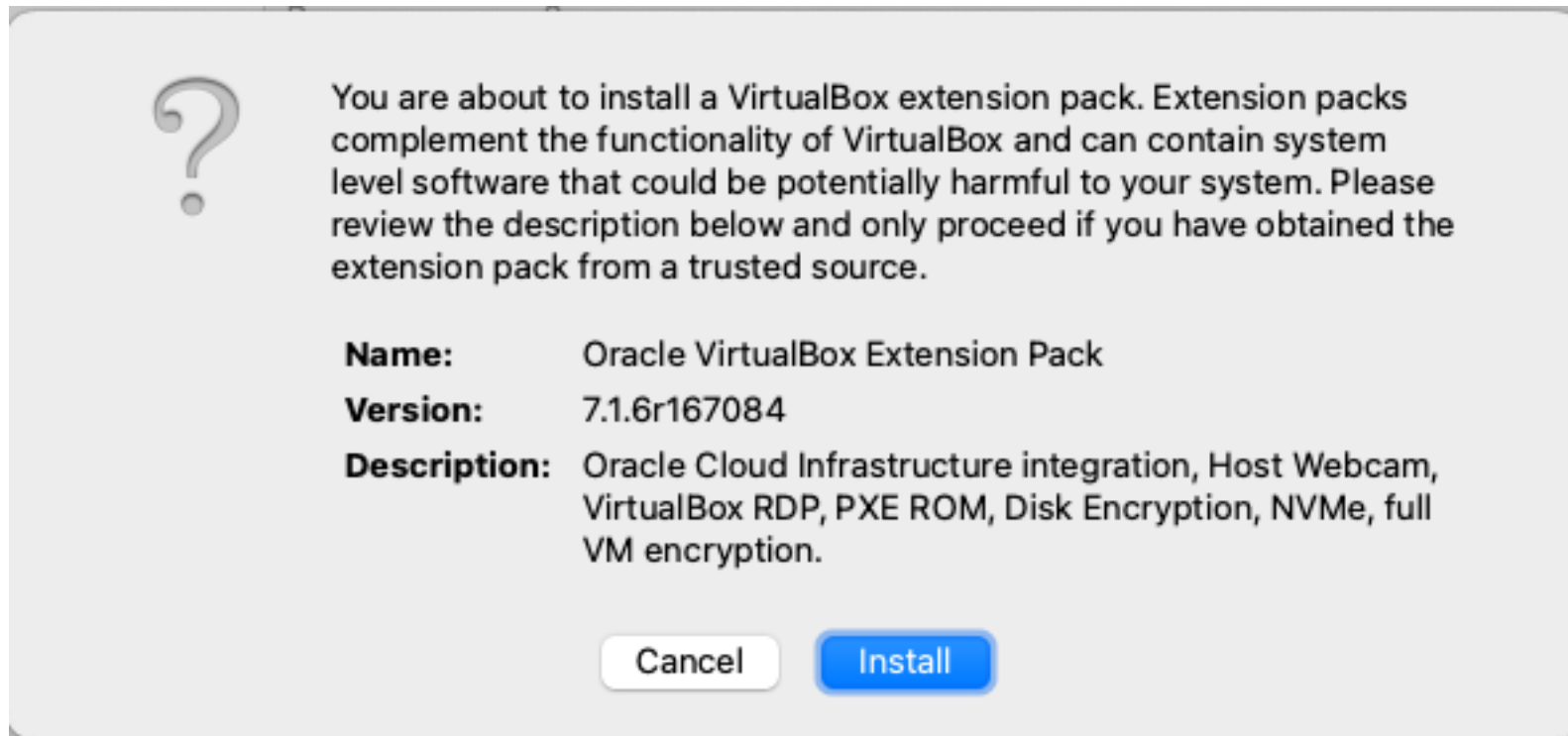
Start installer

- On Intel Mac it looks like this:



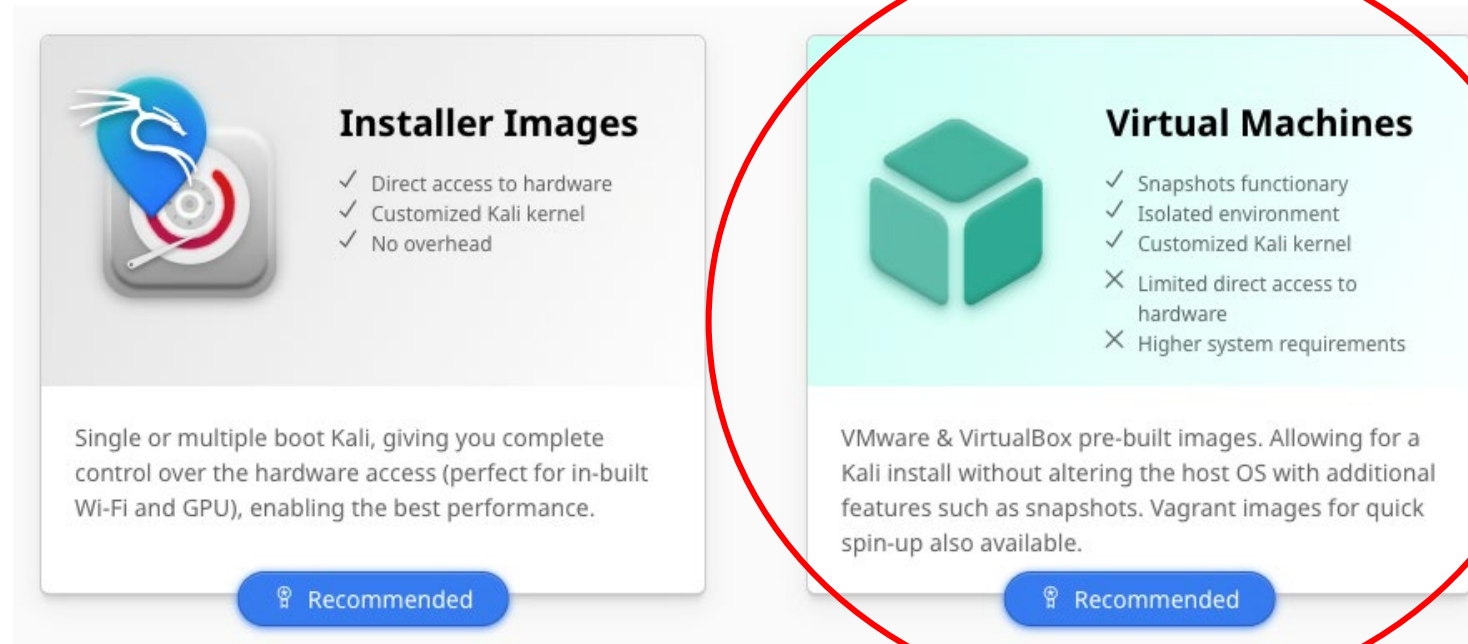
Extension pack

- Remember to download and install



Option 1: Download ready-made virtual machine

- This is not available for Apple Silicon Macs. You have to download installer instead.
- Download virtual machine from here: <https://www.kali.org/get-kali/#kali-platforms>



The screenshot displays two options for downloading Kali Linux. The 'Virtual Machines' option is highlighted with a red circle.

Option	Pros	Cons
Installer Images	<ul style="list-style-type: none">✓ Direct access to hardware✓ Customized Kali kernel✓ No overhead	
Virtual Machines	<ul style="list-style-type: none">✓ Snapshots functionality✓ Isolated environment✓ Customized Kali kernel	<ul style="list-style-type: none">✗ Limited direct access to hardware✗ Higher system requirements

Installer Images

Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

Recommended

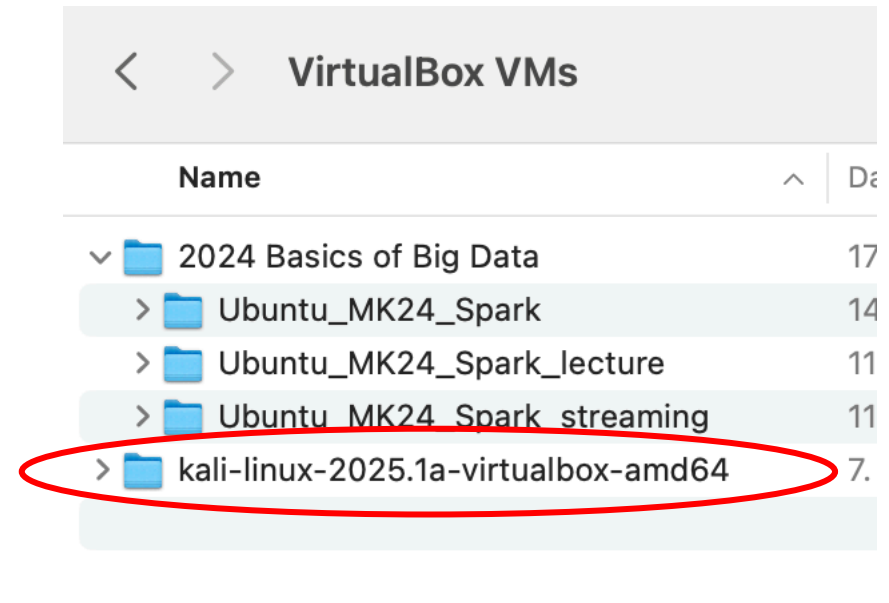
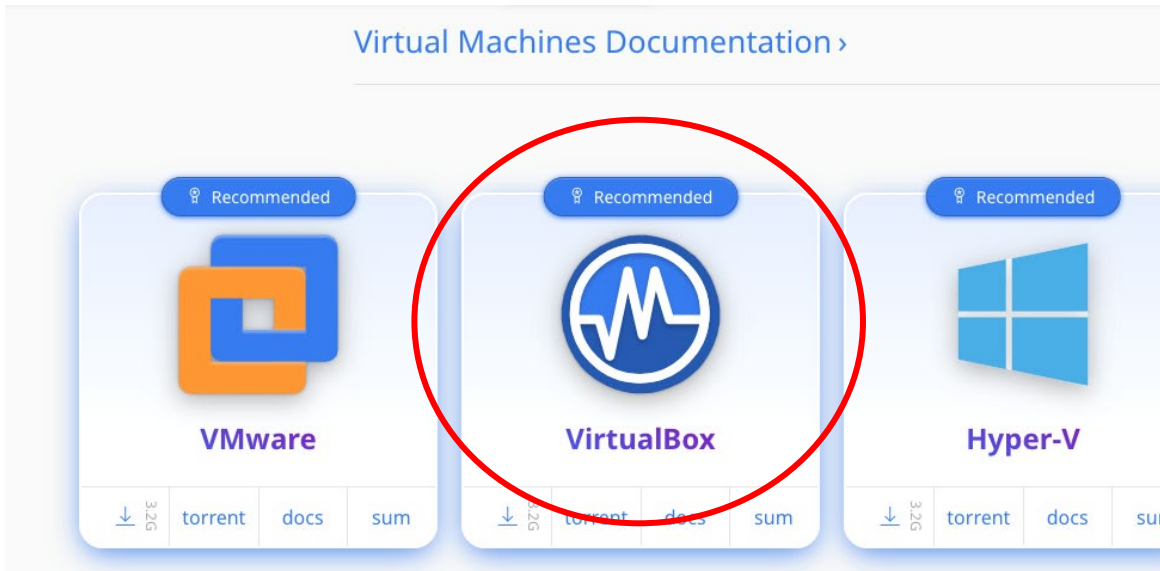
Virtual Machines

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

Recommended

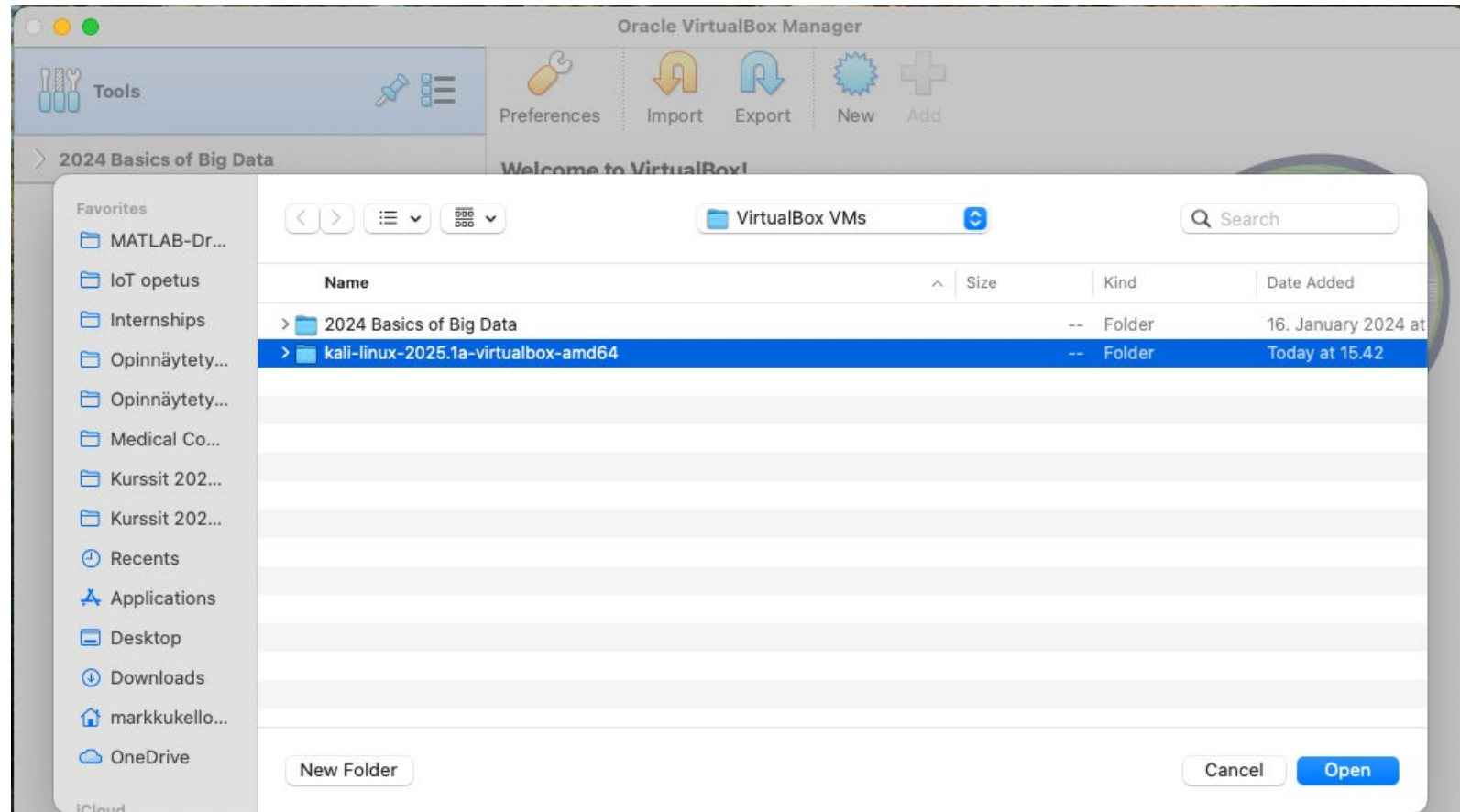
Download VirtualBox Virtual Machine (VM)

- This works for Windows and Intel Macs
- Save and unzip this VM to a directory in which you want to keep your VMs



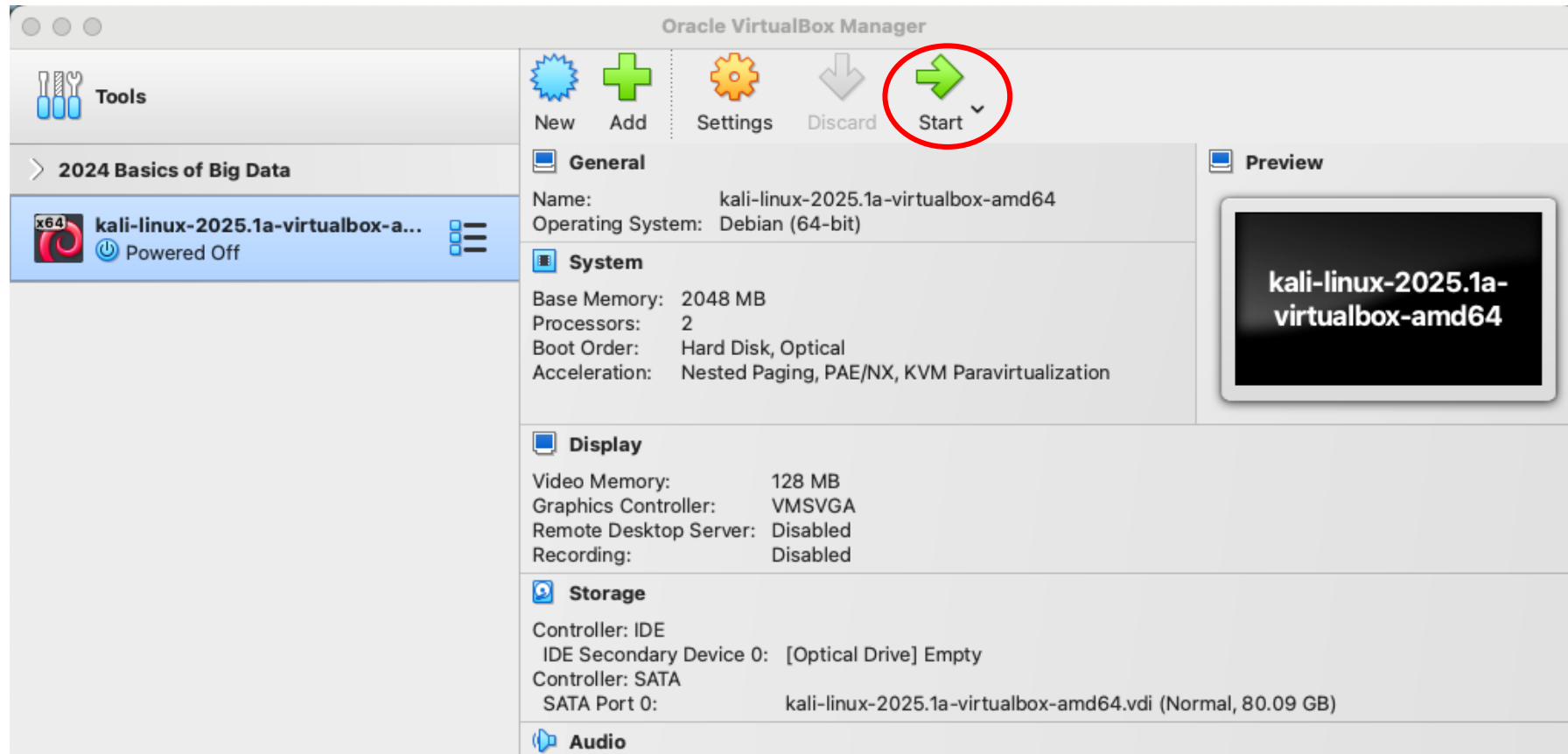
Open the VM

- Launch VirtualBox, click Add (+) and navigate to the VM directory, select and open the .vbox file



Now start the VM from start button

- This course lays the foundation for cybersecurity. After completing the course



Credentials

- The VirtualBox pre-built VMs have default credentials



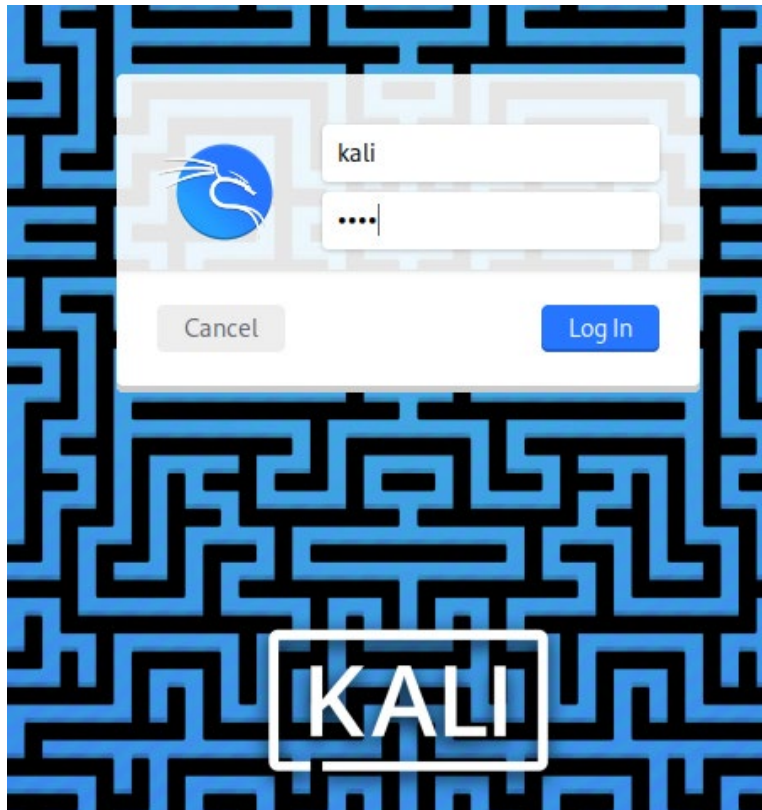
Pre-built Virtual Machines

Kali Linux [VMware](#) & [VirtualBox](#) images are available for users who prefer, or whose specific needs require a virtual machine installation.

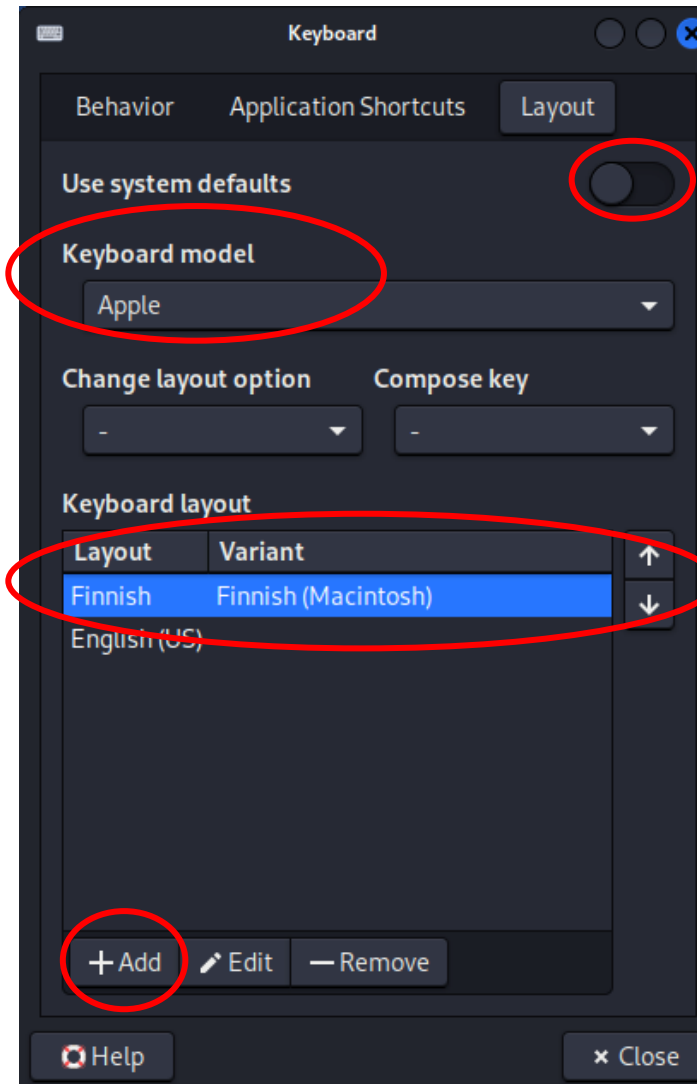
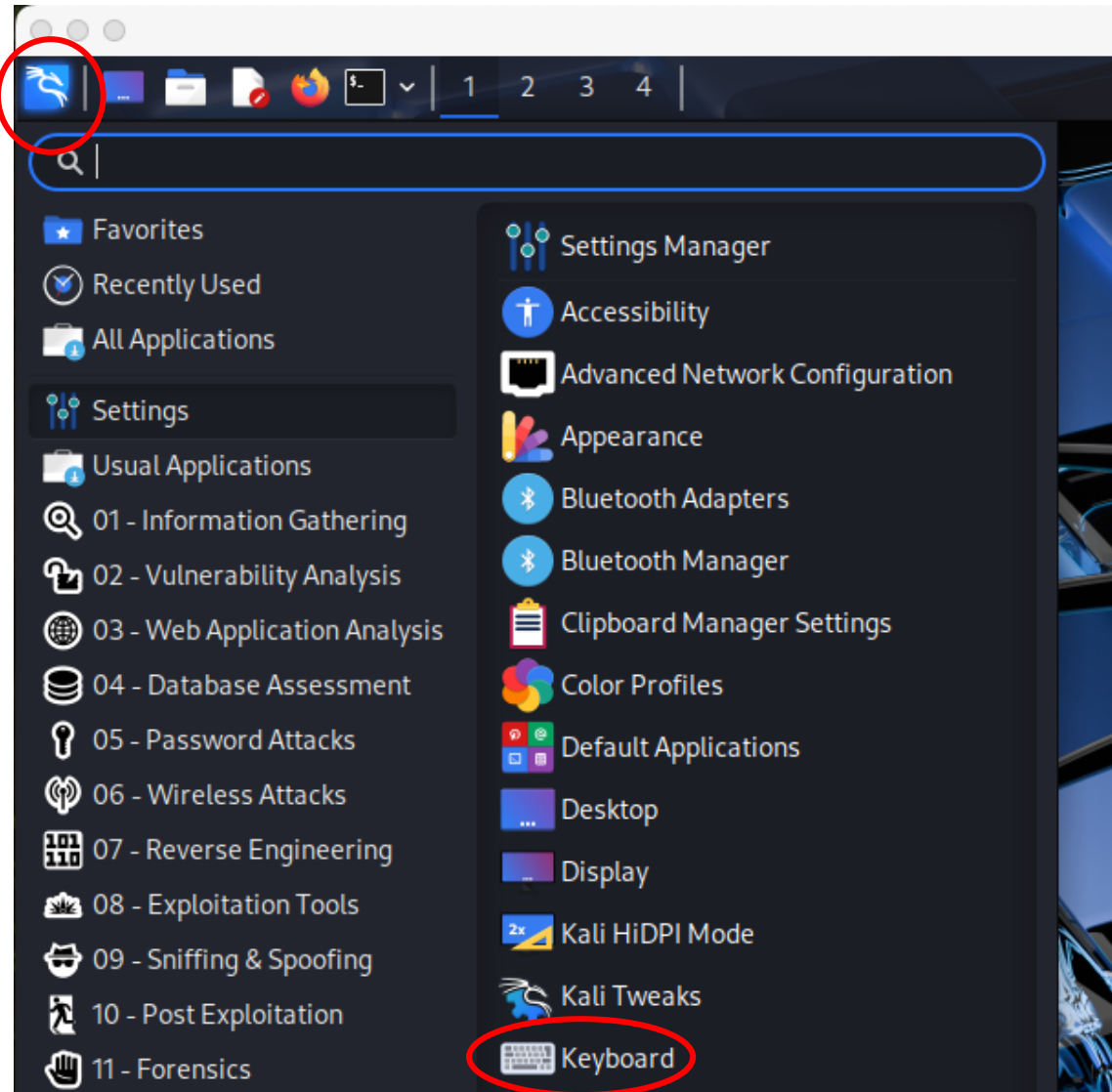
These images have the [default credentials](#) "kali/kali".

Starting up

- Go with the default option (automatically proceeds) and enter credentials



Setting up keyboard settings (language and type of keyboard)

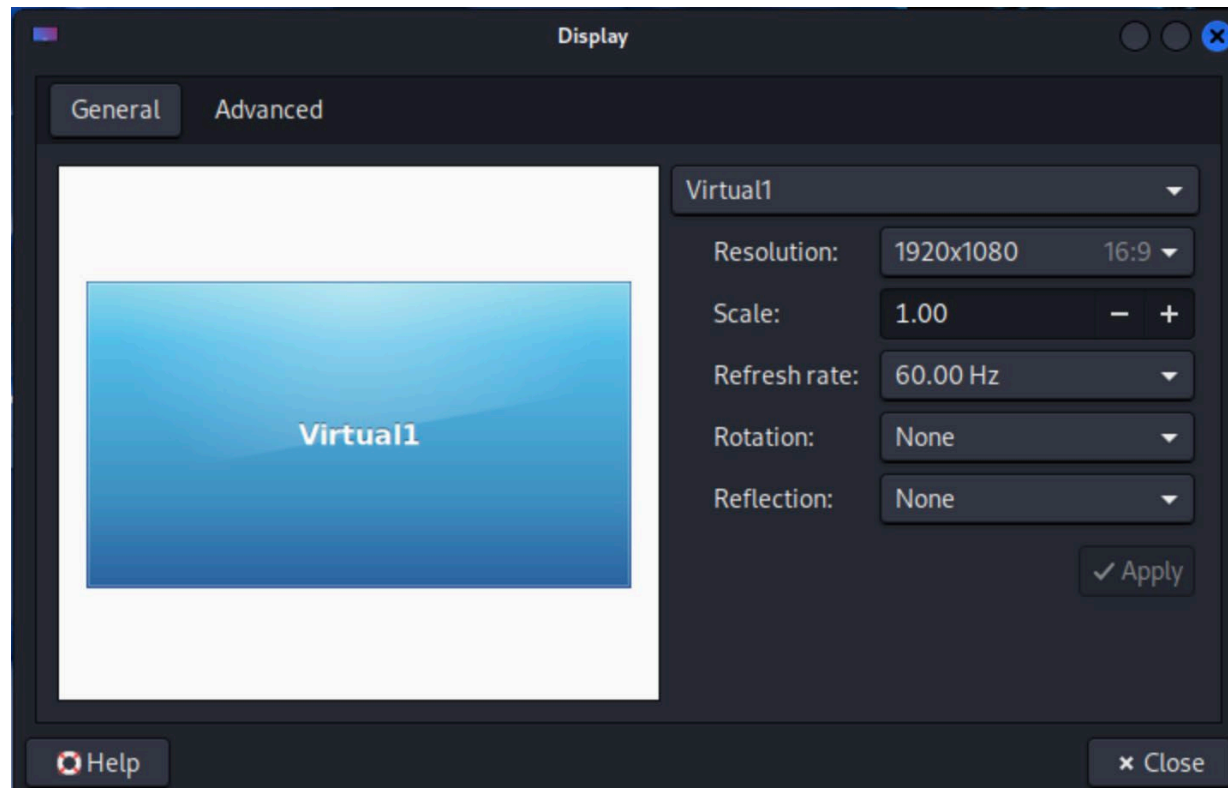


These settings are for a Macbook with Finnish keyboard.

1. Disable system defaults.
2. Add correct keyboard language
3. Select keyboard model
4. Move the correct keyboard to the top of the list

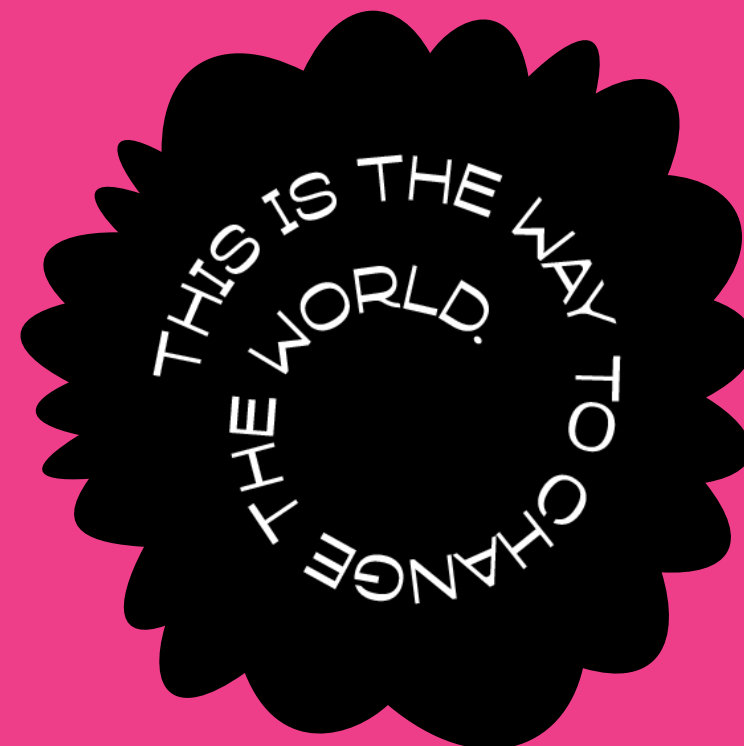
Set resolution (if necessary)

- Go to Settings / Display → set Resolution & Apply



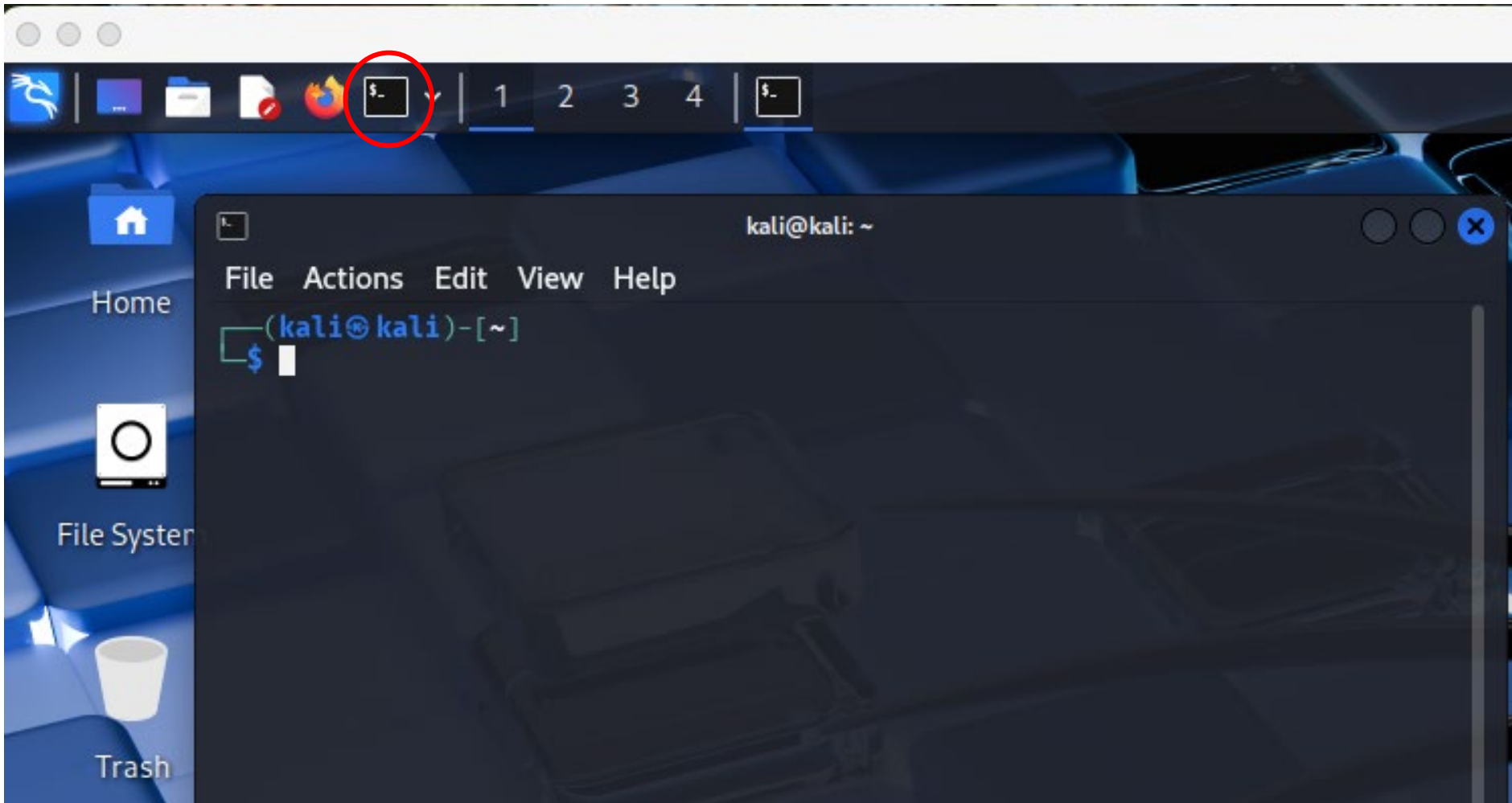
SAVONIA

Basic linux commands and usage



Start terminal by clicking the icon below

- Linux is used mostly through command line in terminal window.

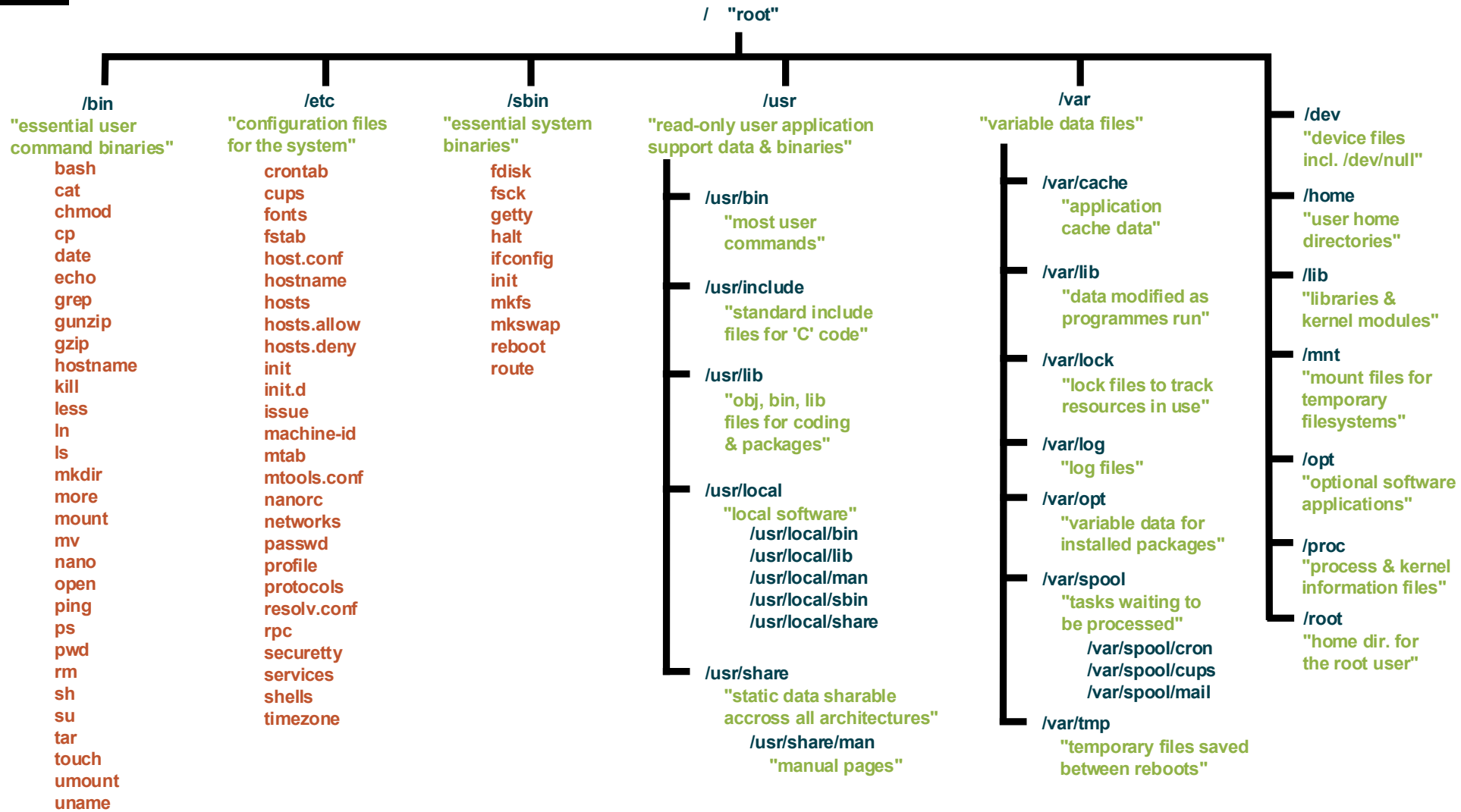


Tutorial on Linux

- Let us go through this Kali Linux tutorial:
<https://www.geeksforgeeks.org/introduction-to-kali-linux/>
 - Go through examples and try different commands
- Another useful tutorial on Linux: <https://ubuntu.com/tutorials/command-line-for-beginners#1-overview>

Linux file system hierarchy

- Check this map: <https://www.blackmoreops.com/2015/02/14/linux-file-system-hierarchy/>
- Kali Linux file management: <https://www.geeksforgeeks.org/kali-linux-file-management/>



By Ppgardne - Own work, CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=49654565>