# Lab - Installing CSI Linux

## Overview

In this lab, you will learn how to install CSI Linux. CSI Linux was developed by Computer Forensics, Incident Response, and Competitive Intelligence professionals to meet the current needs of their clients, government agencies, and the industry.

**Minimum Requirements:**

- 8 GB of FREE RAM (16 GB RAM Recommended)
- 70 GB free disk space (150 GB of free disk space recommended)
- 4 Core CPU
- VirtualBox
- VirtualBox Extensions
- Internet Access

## Download links

- Main download page for CSI Linux Investigator.
- Main download page for VirtualBox and extension pack.

## Caveat

Anytime you update VirtualBox, you will also need to update the VirtualBox extension pack. If VirtualBox is installed, no need to install it a second time.

We will assume you have the latest version of VirtualBox installed for this lab. Since the extension pack is available on the same page, downloading the extension pack should be a no-brainer; download and install the software.

Once you have installed the extension pack for the first time, VirtualBox will present you with the option to upgrade the extension pack each time you update VirtualBox. If you do not have the VirtualBox extension pack installed when you launch CSI Linux, you will receive an error preventing the launch of all three virtual machines.

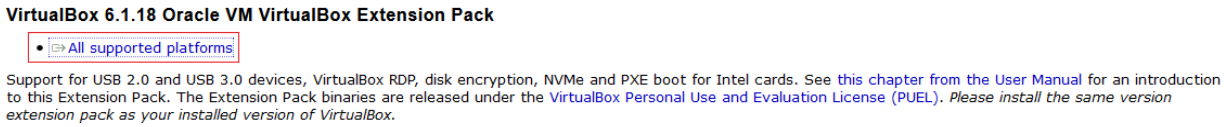
## Install the VirtualBox Extension Pack

VirtualBox Extension Pack is a binary package intended to extend the functionality of VirtualBox. The Extension pack adds the following functionality:

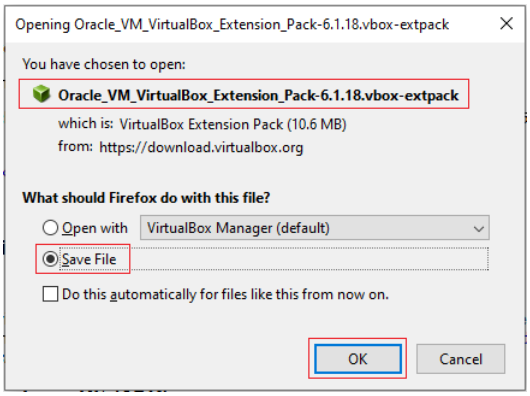
- Support for USB 2.0 and USB 3.0 devices.
- Host webcam pass-through.

- VirtualBox Remote Desktop Protocol (VRDP).
- Disk image encryption with AES algorithm.
- Intel PXE Boot ROM.

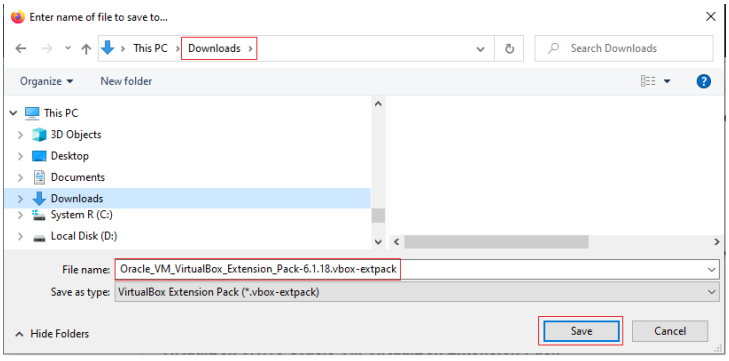
Go to the download page of VirtualBox and open the download link for the VirtualBox Extension Pack for **All supported platforms**. The name of the file used in this example is *Oracle_VM_VirtualBox_Extension_Pack-6.1.8.vbox-extpack*, and we saved the file to a specific location on our host machine. Where you save your file is up to you but do remember where you saved it to.



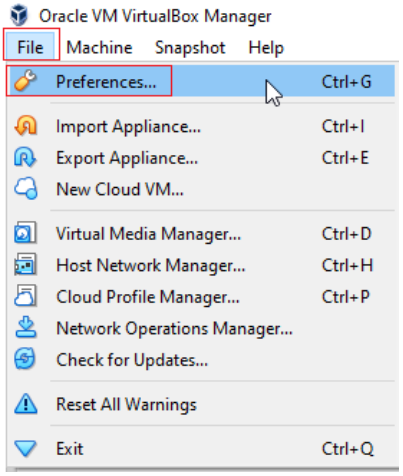

Download the extension pack.



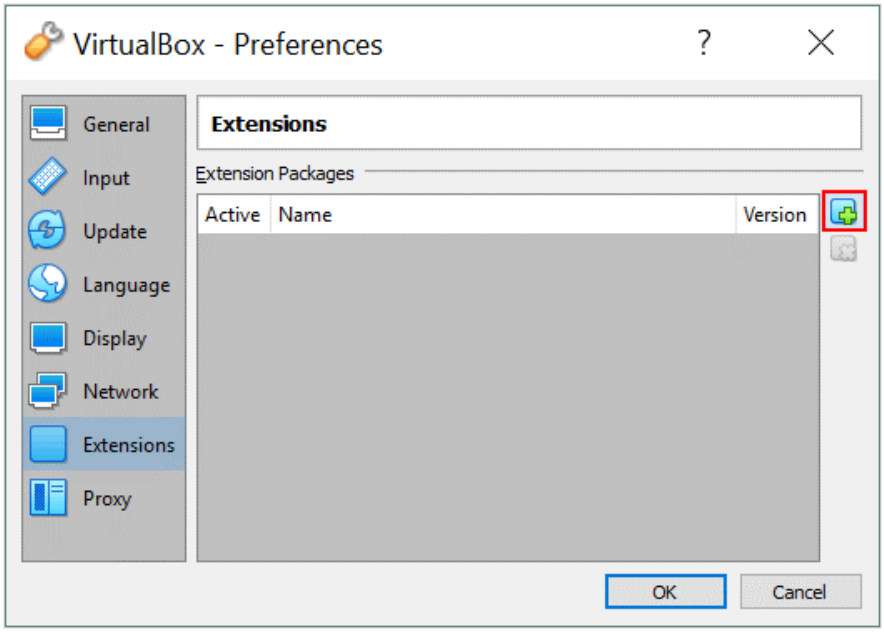

Save to your local machine.



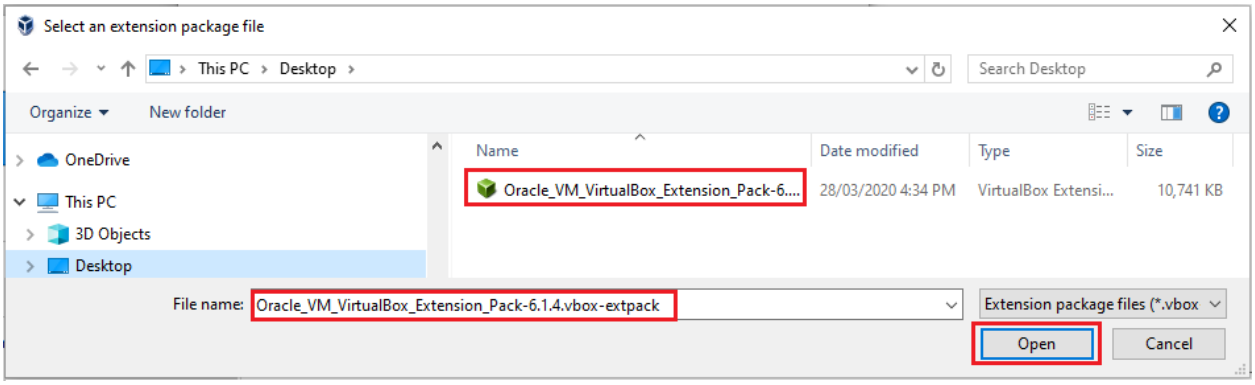

From your VirtualBox management console, click on File, and from the context menu, select preferences.



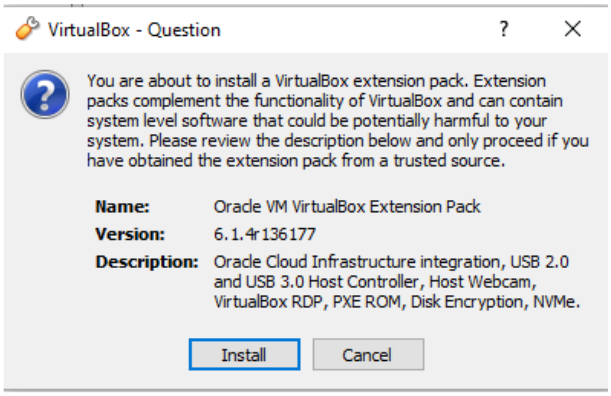

In the Preferences window, go to the Extensions section. After a fresh installation of VirtualBox, there are no extension packages installed. Click the Add a new package button (the icon with a green plus) to add the extension pack.



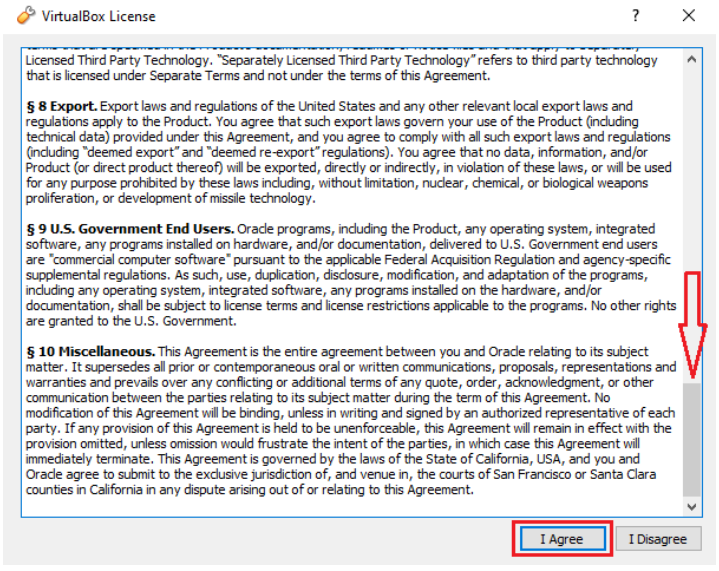

Browse to the download location where you save the previously downloaded extension pack.



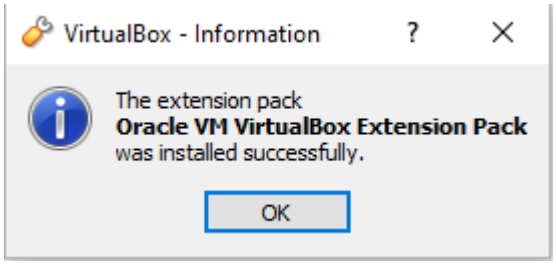

You are asked to confirm that you want to install the selected extension pack.



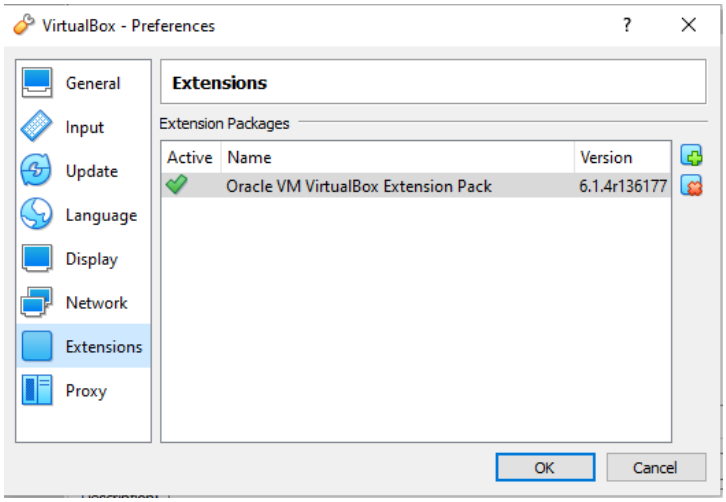

On the next screen, scroll to the bottom of the license agreement and then click the "I agree button."



Once the extension pack has been installed, you will receive the following message. Click OK.

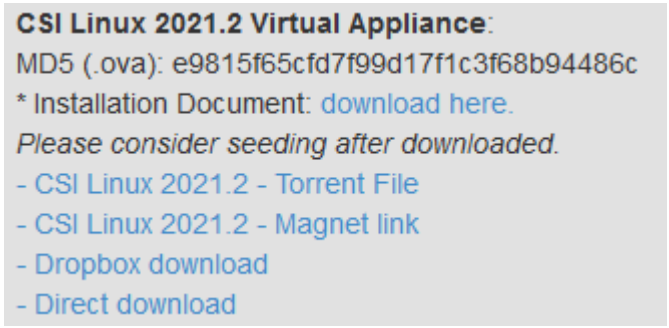



You can confirm the extension pack is installed by checking the right windows pane. Click OK to close the VirtualBox preferences.

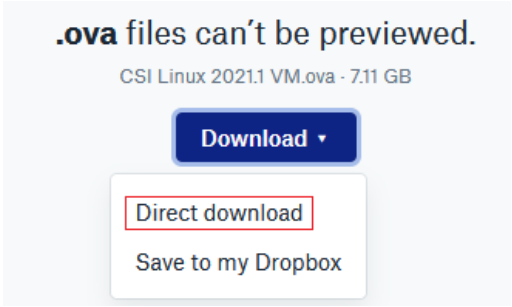


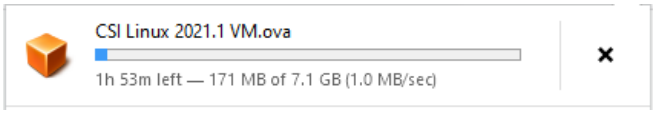

**Download and Install CSI Linux**

Point your browser to https://csilinux.com/download.html Scroll to the bottom of the page and select your download method.

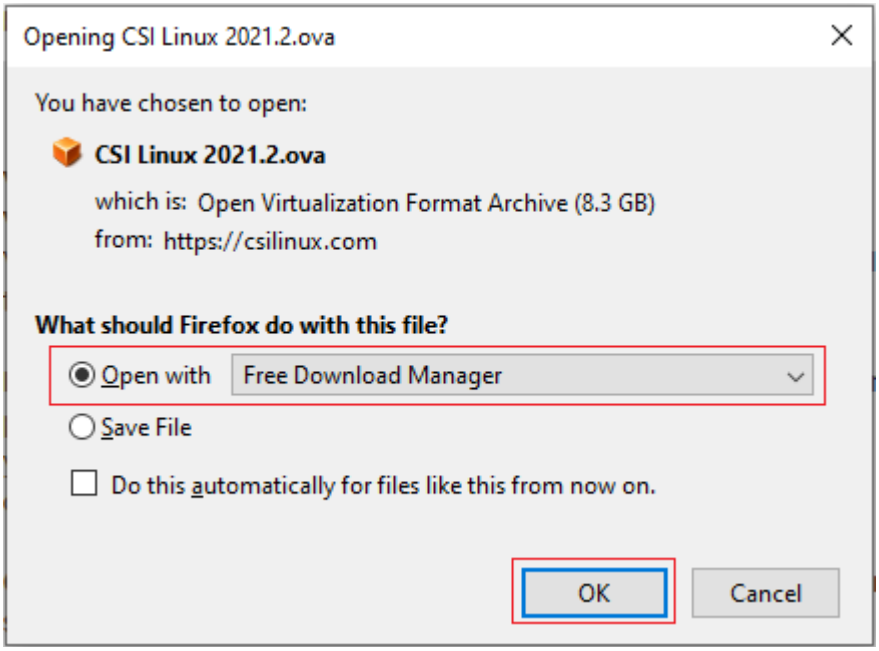


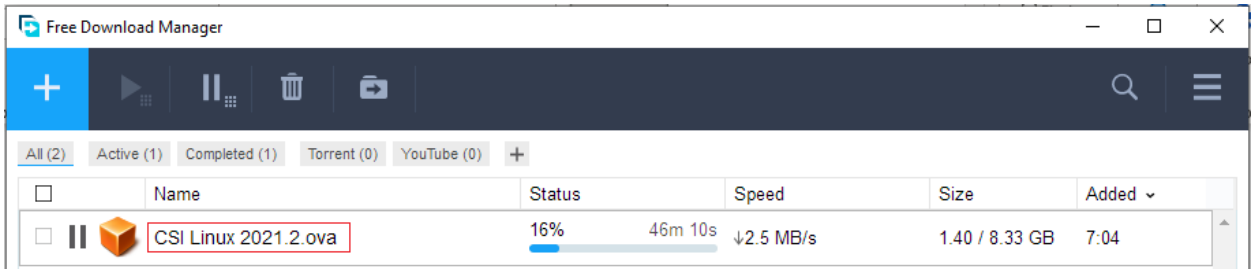
I saved a lot of time using the Dropbox download. All other methods were taking 13+ hours. Using the Dropbox download, I was able to cut the download time to less than two hours.



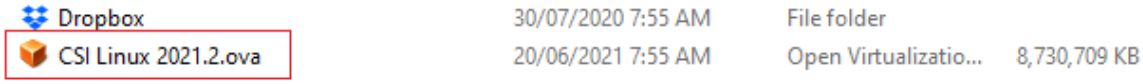




This is a large OVA file of nearly 7.11 GB. If you struggle with downloading large files, you can install the Free Download Manager and use the torrent download option.

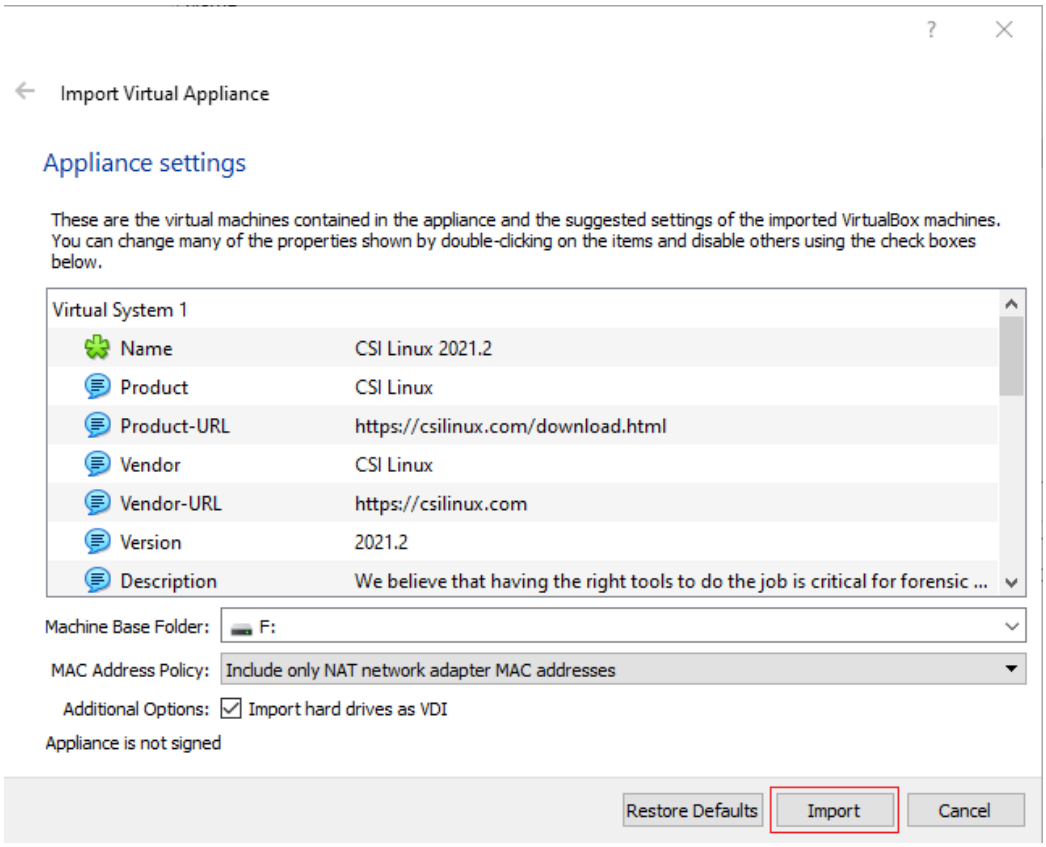




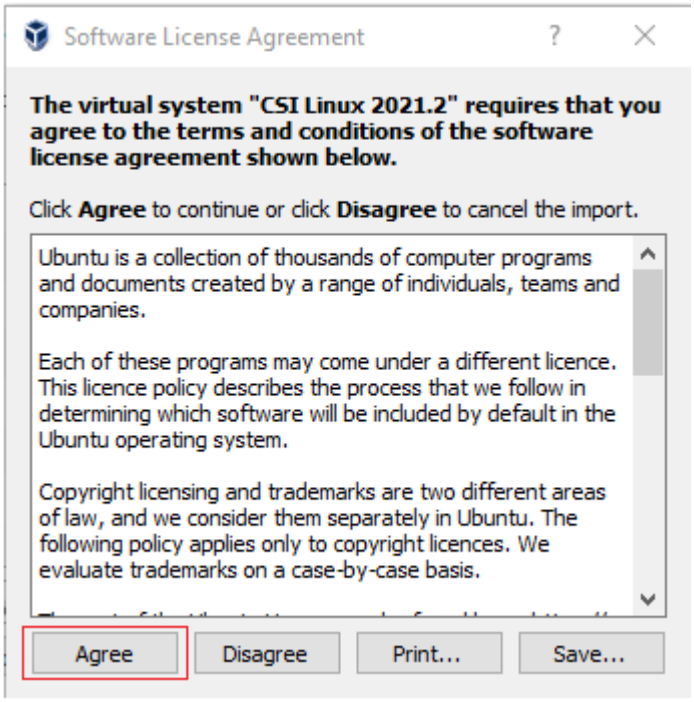

Once you have the OVA downloaded and saved, browse over to the saved location, and x2 left click on the OVA file.



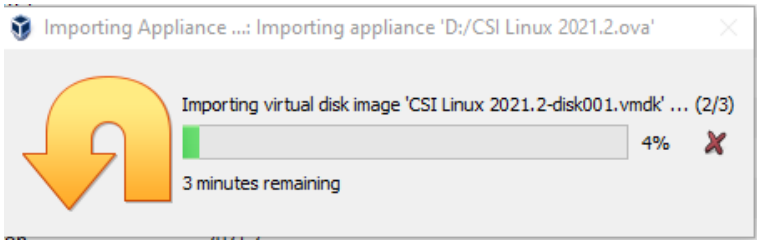

The file will immediately open inside of your VirtualBox manager. The first screen is Appliance settings. Click the Import button.



Accept the license agreement.



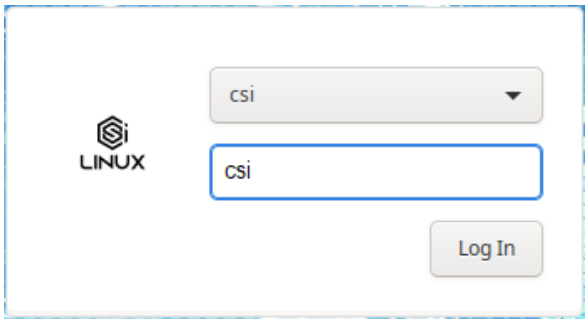

The import process begins.




Once the import process is finished, you will see three CSI Linux virtual machines in the left window pane.


Congratulations! You have completed the install portion for CSI Linux Investigator.

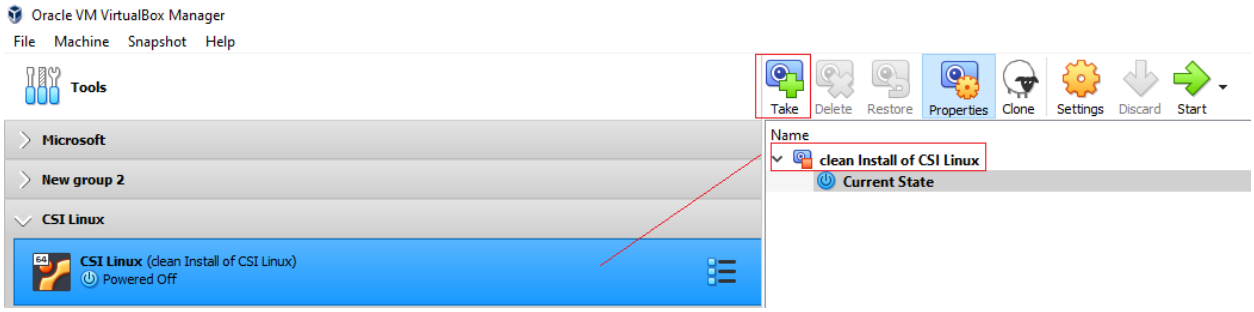
Feel free to launch the CSI Linux. The username is **csi,** and the password is **csi**, all lower case.



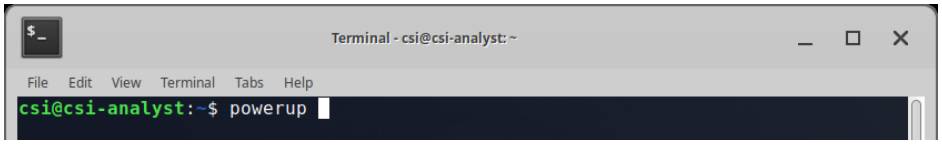

**Take a Snapshot**

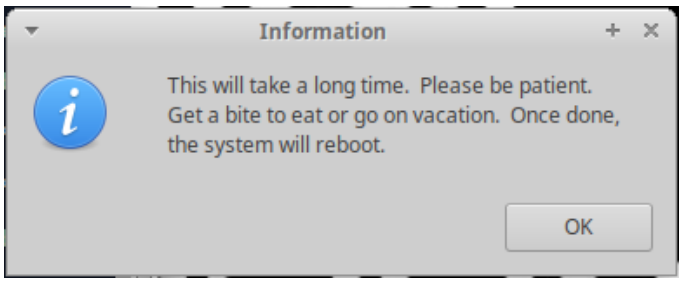
Once you have logged on, it is highly recommended that you create a snapshot of your clean configuration. Create your snapshot the same way you did for your install of Kali.

Before update.

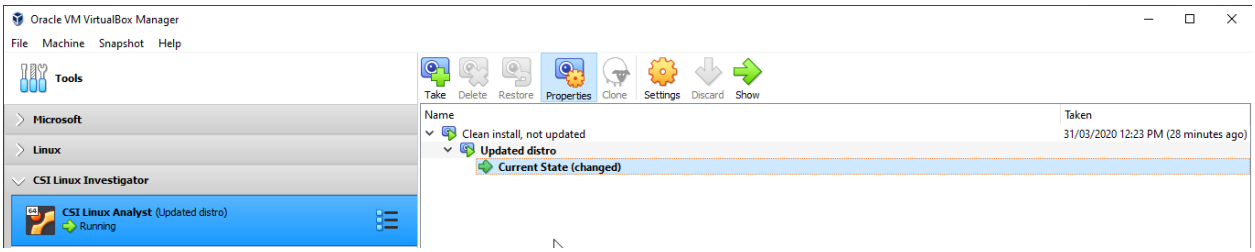



Once you have your snapshot taken, you can update by opening a terminal session and, at the prompt type, **`powerup`**.



After update




Once you have completed the update, take another snapshot to back up the changes made to the distro.

**Summary –**

The video Tutorial has more information about the changes and integration of the CSI Linux Gateway, which is now part of the single OVA downloaded for this lab.

The CSI Linux SIEM has been separated and is now separate from CSI Linux. MISP, OTX, Malcolm, Moloch, Elasticsearch, Kibana, Logstash, Zeek, and others have been combined into this growing network monitoring and forensic server environment. This will be able to be downloaded onto CSI Linux or used on another system on the network.

CSI Linux SIEM 2021.1**:**
**Follow the link and the instructions at [https://github.com/Information-Warfare-Center/CSI-SIEM/blob/master/README.md](https://github.com/Information-Warfare-Center/CSI-SIEM/blob/master/README.md)**

End of the lab!