

# Lab - Install Ghidra on CSI Linux

## Overview

In this lab, you will learn how to install Ghidra for reverse engineering software and performing malware analysis. Ghidra is a software reverse engineering (SRE) suite of tools developed by NSA's Research Directorate to support the Cybersecurity mission. Also, Ghidra is open source.

## Lab Requirements

- On installation of VirtualBox with the extension pack.
- One virtual install of the latest version of Ubuntu, Kali Linux, or CSI Linux.
- Ensure your virtual install has been updated and upgraded.
- VirtualBox network adapter set to NAT network.

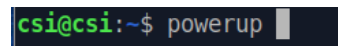
## Begin the lab!

For this lab, I will be using CSI Linux as my virtual machine.

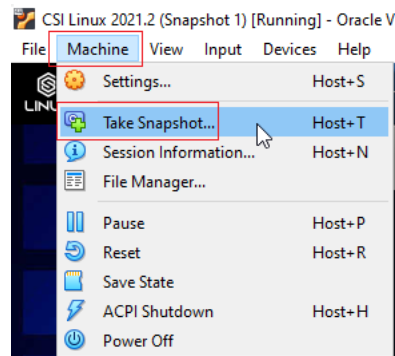
Ghidra is present in CSI Linux but needs Java installed to run. Since CSI Linux is built using Ubuntu and Ubuntu does not come with Java, we will need to install it.

Ghidra is dependent on Java. To install Java, run the following commands one at a time at your terminal prompt.

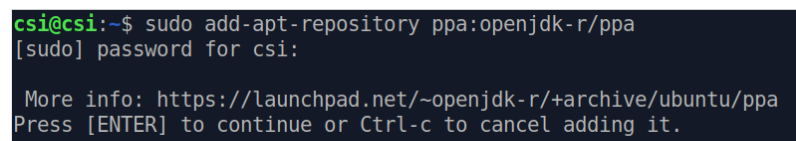
```
powerup
```



Once CSI Linux has completed updating and upgrading, create a snapshot of the system if you need to roll back to this point in time.



```
sudo add-apt-repository ppa:openjdk-r/ppa
```



```
sudo apt install openjdk-11-jdk
```

```
csi@csi:~$ sudo apt install openjdk-11-jdk
```

```
sudo apt install openjdk-11-jre-headless
```

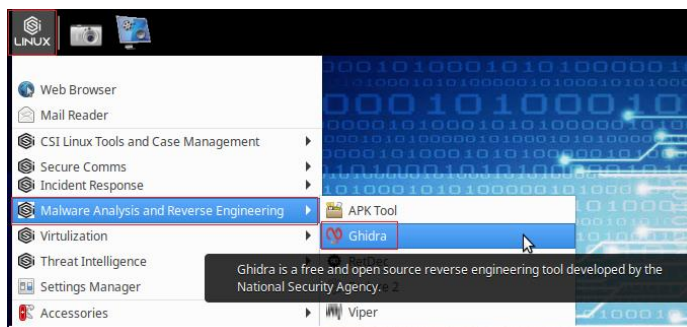
```
csi@csi:~$ sudo apt install openjdk-11-jre-headless
```

## Launch Ghidra

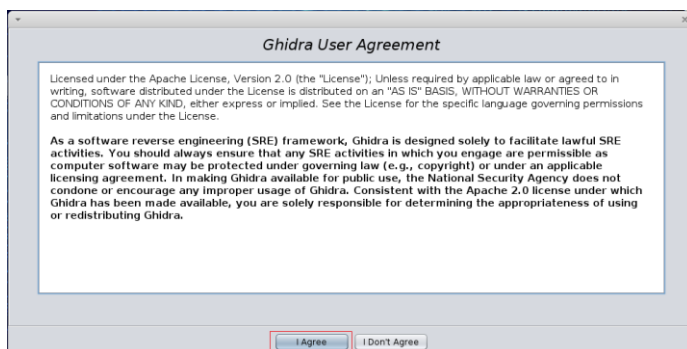
You can launch Ghidra using the Ghidra icon located in the bottom taskbar



Your other option is to use the Application launcher. Scroll down to **Malware Analysis and Reverse Engineering** and launch **Ghidra** from the content menu.



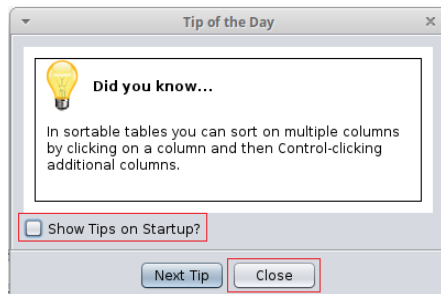
Accept the license agreement.



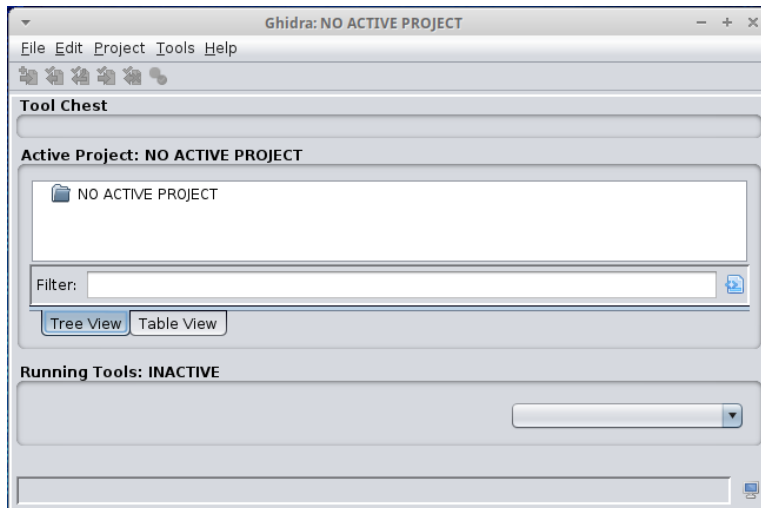
After a short pause, the help menu opens. You can close this.



The next screen is the Tip of the Day. Uncheck the box if you do not want to see the Tip of the day the next time you open Ghidra.



This brings us to the main screen.



Summary –

In this short lab, you learned how to install Java onto Ubuntu, or in this case, a derivative of Ubuntu known as CSI Linux. There are several tools in CSI Linux that are present but will not open for the lack of one or more dependencies.