Setting up the CSI Linux 2021.1 Bootable Image

This version has updated to an Ubuntu 20.04 LTS version for long term support. There have been many upgrades in the applications and additional applications. It has also been optimized to take up less space and boots faster than the 2020 versions. The original CSI Gateway has been retired and the project integrated into this system (runs like Tails) and has been renamed to CSI TorVPN. This will encapsulate all your traffic through a Tor "VPN" adapter when it is turned on.

This is a forensic bit stream copy of CSI Linux and was created as a RAW dd copy. This means that you can take imaging software and copy the dd file to a disk and should boot just like it did before it was imaged. The Raw copy is 32GB and has been compressed to 5GB for download speed.

You must be able to

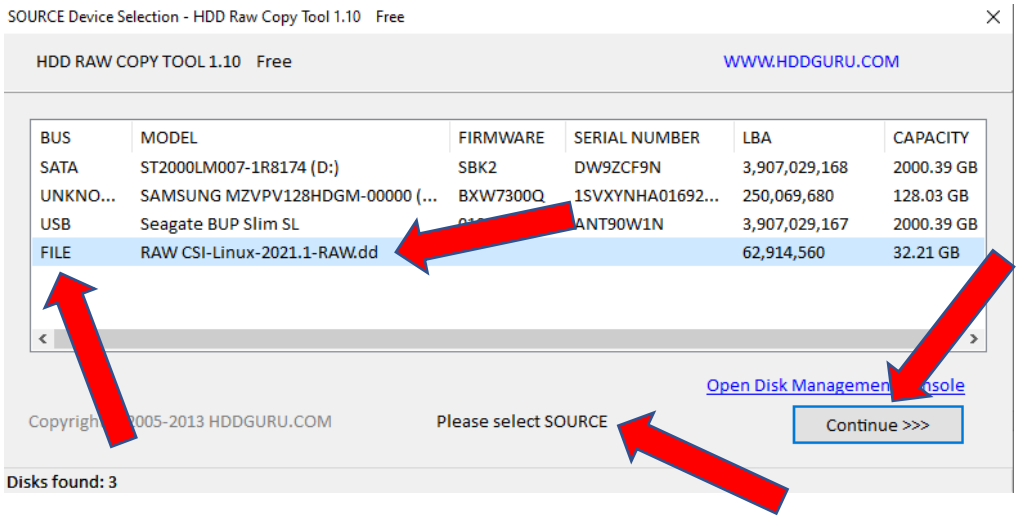
- Edit your computer BIOS.
- Allow for legacy booting.
- If booting off an external drive, change your boot device or order of your boot device.

Requirements

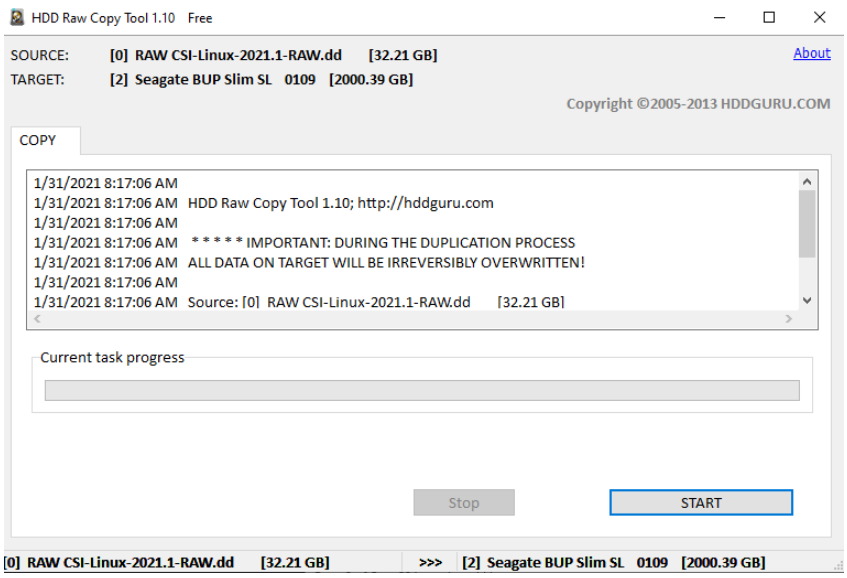
- 64 GB free space minimum
    - This is for the file download and extraction of the 32GB image.
- 64+GB hard drive or usb up to a 2 TB drive. This will be the boot device.
- 6GB Ram minimum
- Imaging tool that can copy a RAW (DD) forensic image to a disk.
    - HDDRawCopy is included in the download if you would like to use it.
- Internet for the internet related tools and updates

Installing the system

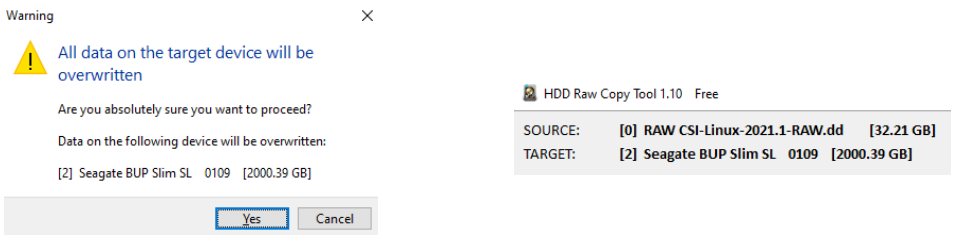
1. Download the CSI Linux 2021.1 Bootable file from the download section.
    a. If you are using the Torrent file or Magnetlink, you will need to use a BitTorrent software to open those. The BitTorrent file downloads the files needed.
    b. After it is downloaded, please consider leaving it in your torrent application to help "seed" the torrent to help others download it.
2. Verify that the .7z file has completed downloading.
3. Once the .7z file has downloaded, extract the files.
4. Make sure you chose a location that has enough disk space. For example, some systems have limited space on the C: drive, so you can install the virtual appliance on your D: drive or external.
5. Open HDDRawCopy1.10Portable.exe.
    a. The first page is for the source disk/image to copy. Verify it says "**SOURCE**". If not, close the application and restart. If it does, double-click on "**File : Double-click to open file**".
    b. Pick the **CSI-Linux-2021.1-RAW.dd** file you extracted from the **CSI-Linux-2021.1-RAW.dd.7z** file. This will be 32GB is size. If it is only 5GB, it is not the right file. The 32GB file is inside the 5GB file. Extract it and point this file to the bigger file.



c. Left click on "**Continue**".
d. The next window should say "**TARGET**". If it does, double click the drive you want to install CSI Linux onto. This can not be the drive you are currently booted off of. In this example, it is the **USB : Seagate BUP Slim SL**.
e. Left click "**Continue**".



f. Left click "**Start**".
g. Verify that this is the right source and destination. If you don't, you can destroy data you don't want to destroy, and you will have a bad day. Left click "**Yes**" if you are sure.



h. Now, wait until done. Then close HDDRawCopy.

Booting the drive

1. Enter the BIOS of your computer and allow for legacy boot. Many times, this is done by pressing the "**F2**", "**Del**", "**F12**", or other keys when you first start the computer. Each computer is different, so you may need to research how to get into your BIOS. Some systems allow you to press "**F8**" to pick a drive to boot from on a one-time basis.
2. Boot off the drive.
3. When it gets to the log in prompt, enter the username and password.
    a. User: csi
    b. Pass: csi
4. Press or click "Log In".
5. You should now be in CSI Linux.

Optional

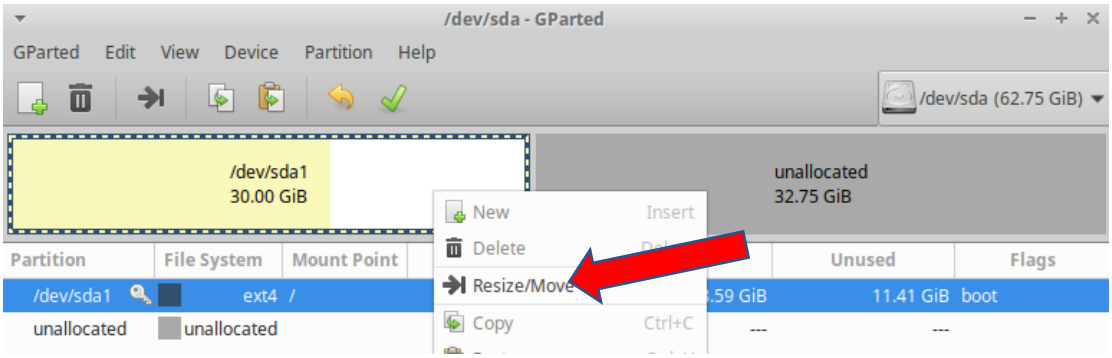
If you would like more space within CSI Linux, you can increase it to meet your needs up to 2 TB.

Step 1

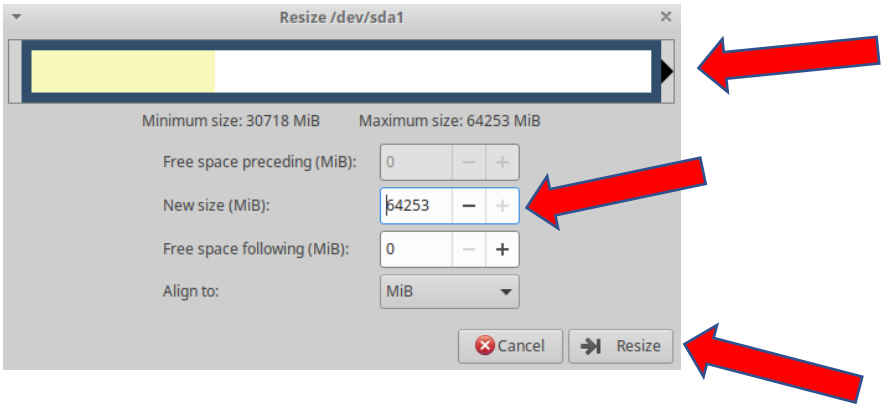
1.) Log into CSI Linux
2.) Open a terminal window by left clicking on terminal icon.
3.) Type in the following and press enter.

    sudo gparted

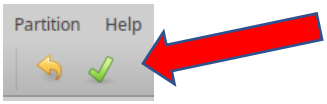
4.) Use the password "csi".
5.) Right click on the CSI Linux drive (example: 30.00 GB). Then left click on "Resize/Move".



6.) Slide the slider bar to the far right or type in "0" for the "Free space following (MiB)" and press enter. This should now fit the new size you created in step 1.



7.) Left click "Resize" and then left click the check icon.



8.) Left click "Apply". When it is done, left click "Ok", then close Gparted.

You can now start using your investigation environment with more disk space.

Optional

If you want to use CSI Linux as an Incident response triage drive, allocate most of the disk for a second partition with NTFS. This will allow you to plug the triage drive into a live running Windows computer and run Widows incident response or forensics tools. Tools like FTK Imager, NirLauncher, and Portable apps are commonly used in this way. We have a download on the CSI Linux download page with useful tools as an example or that you can use.

If you would like to be involved in the future development of CSI Linux, please contact us at dev@csilinux.com