## Cennix write blocker

The tool is designed and developed for user to enable software write blocking on Linux (Ubuntu 16.04 & SIFT WORKSTATION) environment.

## Background

This project comes with three parts, Udev rules, device indicator and Write blocker tool.

Udev rules: We wrote a Udev script to mark all available block devices (except loop devices) as read-only. (Once the udev rules is enabled, all the devices that are plugged to the machine, will be marked as READ-ONLY).

Device indicator: The indicator detects external storage devices that are connected to the computer and present it on the menu list with some basic details of the device also send the notification bubble to Desktop

Write blocker application: The main GUI for user to enable or disable write blocking on selected devices. It also creates logs of system activities, system errors and software errors.

## Concepts

We utilize the existing facility of marking a block device as read-only and add read-only checks to a common spot in the block device driver. This allows us to block all write and discard requests originating from kernel drivers ignoring the read-only mode of a block device; this also allows us to keep the variety of physical storage device drivers untouched. Our modification is removing the need for the loop device driver, because its primary advantage, the ability to stop write and discard requests from hitting the physical drive, will be replicated in the block device driver.

In particular, we modify the *generic\_make\_request\_checks* function and insert the code used to end I/O processing when a write or discard request is issued to a read-only block device. This modification allows us to intercept write and discard requests at the lowest level possible in the block device driver.

We modified and applied the customized patch to the kernel, so it blocks write, discard, erase, flush, zone reset commands going to a read-only device. We do this because kernel drivers often lack necessary checks and send these commands to read-only block devices.

## How to install

1. Modify kernel source code and patch it.
2. Move [01-forensic-readonly.rules](https://github.com/msuhanov/Linux-write-blocker/blob/master/userspace/udev/01-forensic-readonly.rules) to /etc/udev/rules and reload rules
3. unpack and install the .deb package

## Userspace helpers

There are serval userspace helpers included to this repo:

* 01-forensic-readonly.rules
* dev\_info.py
* wb\_app.py
* wb\_indicator.py
* wrtblk

“blockdev --setro /dev/sdx” this is the command we use in the script to block devices

“blockdev –setrw / dev/sdx” this is the command we use in the script to unblock devices