Using Tor with CSI Linux

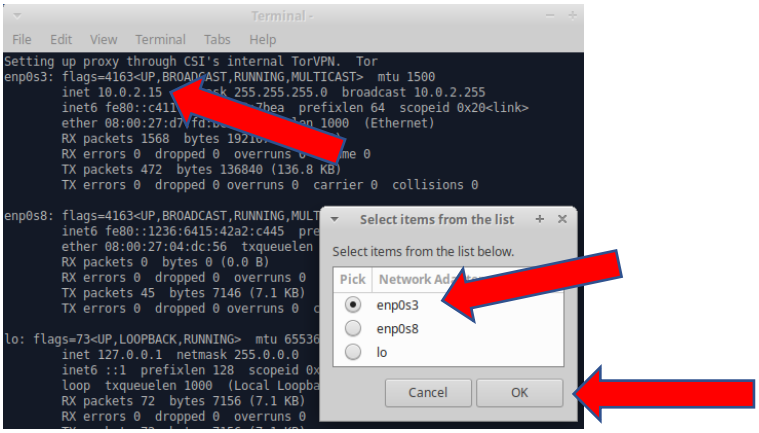
CSI Linux was built for cyber investigations starting from OSINT to computer/mobile/network forensics. When focusing on the OSINT, CSI Linux has taken special care to give investigators a secure option to help them protect their identity. You do not have to use Tor, but there have been two options we have designed to ensure if you do that you will be safe along with allowing your tools to still be able to connect to Tor .onion sites. This is critical for Dark Web investigations.

Both of these options are preventing your internet facing IP address from being identified by those under investigation while allowing all of your tools to naturally go through Tor.

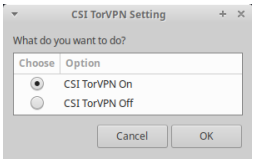
Option 1: CSI_TorVPN

This option allows for your system to encapsulate ALL of your network traffic through built in Tor entry node similar to Tails (https://tails.boum.org/). The difference is this is not a burnable temporary system that destroys your data after use (very useful in certain situations).

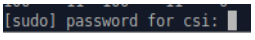
1. Run the **CSI_TorVPN** application.
2. Choose the network adapter that has an internet connection.



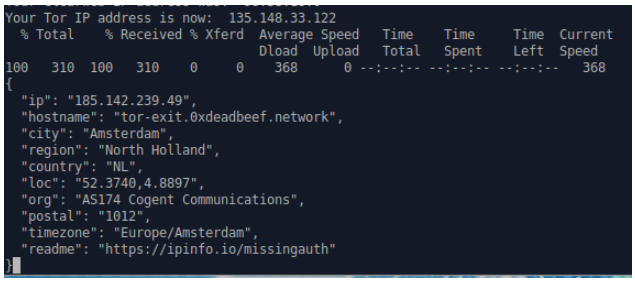
3. Turn the **CSI_TorVPN** "**On**" or "**Off**"



4. Enter the CSI password (default **csi**)



5. When you connect to Tor, you should see a different address pop up.
6. To turn the **CSI_TorVPN** off, follow same steps and change **step 3** to "**Off**".

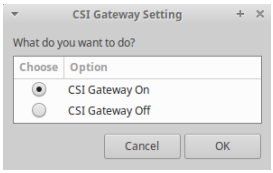


Option 2: CSI_Gateway

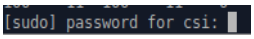
This option is only available in the Virtual Appliance and uses the Whonix gateway (https://www.whonix.org/) to tunnel ALL of your traffic through Tor. Once you download, install, and run the Whonix gateway, if you run the CSI_Gateway application, it will reconfigure CSI Linux to work with Whonix. As long as Whonix is connected to Tor, all your traffic in CSI Linux will be routed through Tor.

1. Start Whonix Gateway
2. Start CSI Linux

3. Run the **CSI_Gateway** application.
4. Choose the network adapter that has an internet connection.
5. Turn the **CSI_Gateway** "**On**" or "**Off**".



7. Enter the CSI password (default **csi**)



8. To turn the **CSI_Gateway** off, follow same steps and change **step 5** to "**Off**".

Option 3: Network Tor Gateway

Set up a network device as a Tor relay and route your traffic through that gateway.

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