**Running Apps Through Tor**

**Needs to be set up correctly to ensure all traffic is run through Tor**

e.g., with email, you may set up your client to run through Tor and all emails are sent through Tor but DNS requests may still be done normally, **ignoring the proxy settings**

The Torcc file will show your socksport and controlport

* The socksport is the one we need for routing other applications

Running a netstat when Tor isn’t running, won’t show the socksport port

* When it is running, the port should show

Any app that supports socks proxies can be configured to that port to go through that proxy

IceWeasel

* Network 🡪 advanced 🡪 settings 🡪 manual proxy config 🡪 SOCKS: 127.0.0.1, port: 9150
* Then do a tor check to see if you are connected to Tor through that proxy tunnel

To get tor to log and monitor your socks connection for drops and DNS leaks

* Put these in Torc file
  + TestSocks1
  + SafeSocks 1
* Best way to check for leaks is to use a protocol analyser on the router to look at traffic like WireShark

Can also **firewall the traffic** and set a **deny all rule** that only allows traffic to go through Tor

* Like the Whonix gateway
* This is called a trans(parent)proxy

When using a transproxy like whonix, all applications will use the same Tor circuit which can be correlated – **no stream isolation**

When using separate socks proxies, each app uses a different circuit (app will need specific option to run through socks though)

Biggest recommendation is to use Whonix on Tails

Privoxy

* An app that allows you to configure other apps to run through Tor when they don’t have a native option to configure socks proxies

Or proxyfiers