# Initial setup

Install dependencies:

git clone <https://github.com/reynaldicheok/StegoDetectoLive.git>

Navigate into the cloned folder, then execute the command below

cd ./StegoDetectoLive && pip install -r requirements.txt

# Application Start:

To run the application:

python main.py -F

Either -F or -R <url> must be set.

Example for reverse proxy: python main.py -R <http://127.0.0.1:5000> -P 12345

Example for forward proxy: python main.py -F -P 12345

Users can also run this in transparent mode with -T to have it function like an IDS instead.

Example: python main.py -F -P 12345 -T

# Help Menu:

-F : Forward proxy mode.

-R <url> : Reverse proxy mode. Requires the target url to be set.

-M <int>: Minimum number of successful algorithms before blocking

-T : This will allow all traffic to pass through the proxy. Potential Steganography image data will still be saved to the triage folder with its respective metadata.

-P : Port number to run the proxy

# Add mitmproxy as trusted CA when in forward proxy mode

1. Connect to the running proxy
2. Access <http://mitm.it/>

# Example of using with forward proxy

1. Go to Extensions and Manage Extensions

A screenshot of a computer

Description automatically generated

1. Search for ‘foxyproxy’ in the search bar

A screenshot of a computer

Description automatically generated

1. Download Foxyproxy standard and add to Firefox.
2. Access <http://mitm.it/>

A screenshot of a computer

Description automatically generated

1. Download the certificate according to your platform and add the certificate as a trusted Certificate Authority in Firefox under “Settings”, “Privacy and Security”, “View Certificates” and “Import” to add the downloaded certificate. Configure the proxy in ‘foxyproxy’.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Enable the configured proxy and you are good to go

A screenshot of a computer

Description automatically generated