Useful commands

Network commands

- `ip route show` shows networks configuration
- `ip neigh show` shows neighbours devices (like those connected to the hotspot)

MiTMProxy

1. Enable IP forwarding:
   - `sysctl -w net.ipv4.ip_forward=1`
   - `sysctl -w net.ipv6.conf.all.forwarding=1`
2. Disable ICMP Redirects:
   - `sysctl -w net.ipv4.conf.all.send_redirects=0`
3. Create iptable rules:
   - `iptables -t nat -A PREROUTING -i wlp7s0 -p tcp --dport 80 -j REDIRECT --to-port 8080`
   - `iptables -t nat -A PREROUTING -i wlp7s0 -p tcp --dport 443 -j REDIRECT --to-port 8080`
4. Exec mitmproxy:
   - `mitmproxy --mode transparent --showhost -p 8080`

Mosquitto

- Install with `dnf install mosquitto` (fedora)
- `mosquitto_sub` receives messages of the specified topic
  - `#` can be used to sub to all topics
- `mosquitto_pub` publish simple messages

USB device

- `sudo chmod 666 /dev/ttyUSB0` set permissions to usb device
- `screen /dev/ttyUSB0 115200` receives serial data

ESPTool

- `esptool.py chip_id` get chip info
- `esptool.py --baud 115200 read_flash 0x0 0x400000 firmware.bin` dump flash memory, starting at address and for the given size in the file

Firmware analysis

- `strings`