



Document: Setup mitmproxy with Real Device for Mobile App Traffic Inspection

◆ 1. Prerequisites

- PC/Laptop (Windows/Mac/Linux)
 - Real Android or iOS device
 - Both PC and device connected to the **same Wi-Fi network**
 - Admin rights on PC (needed for installation & firewall rules)
-

◆ 2. Install mitmproxy

On Windows

1. Download installer from: <https://mitmproxy.org>
2. Install by running the `.exe`.
3. Add installation folder to **System PATH** (if not auto-added).

On Mac (brew)

```
brew install mitmproxy
```

On Linux (Ubuntu/Debian)

```
sudo apt update  
sudo apt install mitmproxy
```

Verify

```
mitmproxy --version
```

◆ 3. Run mitmproxy

Start mitmproxy on your machine:

```
mitmproxy --listen-port 8080
```

- Default port: **8080**
 - This terminal will show all intercepted traffic.
-


◆ 4. Configure Proxy on Device

On Android (real device)

1. Open **Settings** → **Wi-Fi**.
2. Long press on your connected Wi-Fi → **Modify Network**.
3. Tap **Advanced Options**.
4. Change **Proxy** → **Manual**.
 - **Hostname** = your PC's local IP (e.g., **192.168.1.25**).
 - **Port** = **8080**.
5. Save.

On iOS

1. Go to **Settings** → **Wi-Fi**.

2. Tap the  info icon next to your network.
3. Scroll to **HTTP Proxy** → set to **Manual**.
 - **Server** = your PC's IP.
 - **Port** = **8080**.

 Use your **PC's local IP address**, not **localhost**. To find it:

- Windows: **ipconfig**
- Mac/Linux: **ifconfig**

◆ 5. Test Proxy Connection

On the phone's browser, open:

http://<your-pc-ip>:8080

- If successful → mitmproxy should respond.
- If fails → check:
 - Both devices are on same Wi-Fi network.
 - Firewall allows inbound traffic on port **8080**.
 - Mobile Data/VPN is disabled.

◆ 6. Install mitmproxy Certificate

To inspect HTTPS traffic, install the mitmproxy root certificate.

On the phone's browser, visit:

<http://mitm.it>

- 1.
 2. Choose your platform (Android/iOS).
 3. Download and install the certificate.
 4. (Android 11+ only) → Go to **Settings** → **Security** → **Install certificates** and install as **VPN & Apps** certificate.
 5. (iOS) → Install profile in **Settings** → **General** → **Profiles** and trust the certificate.
-

◆ 7. Inspect App Traffic

- Launch your mobile app.
- mitmproxy will show requests/responses in terminal UI.
- Look for **API calls that return snackbar/toast messages**.

You can filter by keyword:

```
mitmproxy -q | grep "Invalid"
```

- (or use built-in search `/keyword` inside mitmproxy UI)
-

◆ 8. Capture Toast/Snackbar Text

- Identify whether the toast/snackbar is coming from:
 - **Backend API response** (JSON payload, error message field).
 - Or **hard-coded UI** (not in network traffic).

👉 If it's in API response → you can reliably capture it using mitmproxy or by hooking API calls in your test automation.

◆ 9. Cleanup

When done testing:

- Remove proxy settings from device Wi-Fi.
- (Optional) Remove mitmproxy certificate if not needed anymore.