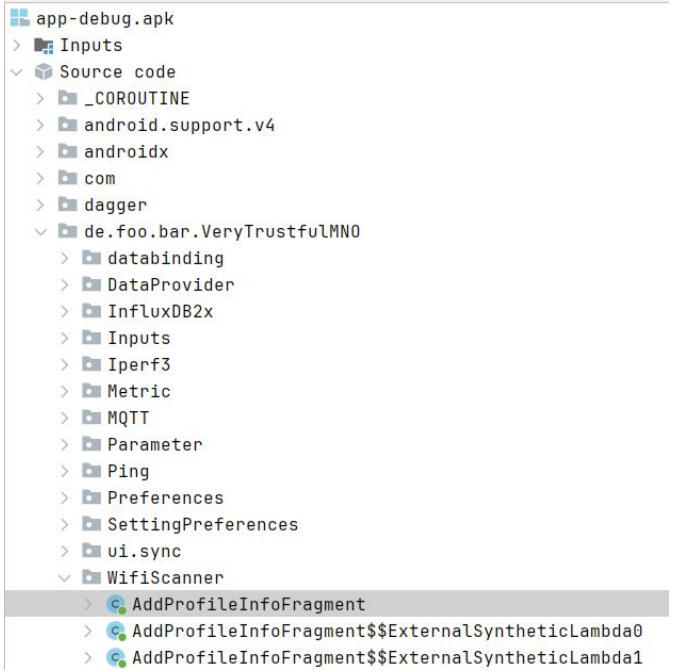
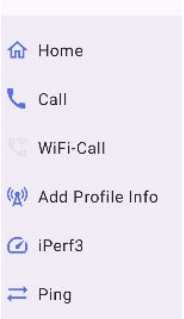
Jadix Decompiler

- using jadx-gui to analyse the apk
- wifiscanner, AddProfileInfoFragment is the suspect view.
- matches the “Add Profile Info” page we need to analyse





Function we have to check found in AddProfileInfoFragment

```
private void uploadImage(final File imageFile, final String firstName, final String lastName, final UploadCallback callback) {
    new Thread(new Runnable() { // from class: de.foo.bar.VeryTrustfulMNO.WifiScanner.AddProfileInfoFragment$$ExternalSyntheticLambda2
        @Override // java.lang.Runnable
        public final void run() {
            AddProfileInfoFragment.lambda$uploadImage$5(imageFile, firstName, lastName, callback);
        }
    }).start();
}
```

Setting hooks via Frida

Hooking the uploadImage function to find out which parameters get send over

setting hooks via frida onto the general http library to find any suspect traffic going though

```
frida -U -f de.foo.bar.VeryTrustfulMNO -l hook_upload_function.js
```

Results

hook on uploadImages found out where image is stored locally.

hook on the http library shows that the image was uploaded on supabase which is suspicious when comparing with others

```
[Android Emulator 5554::de.foo.bar.VeryTrustfulMNO ]-> [*] uploadImage called
firstName =
lastName  =
file      = /data/user/0/de.foo.bar.VeryTrustfulMNO/cache/upload1884563533717237 40.jpg

[!] IMAGE UPLOAD REQUEST DETECTED
    -> URL: https://vwhosnragmnkhkgjogoq.supabase.co/functions/v1/upload-image
    -> Host: vwhosnragmnkhkgjogoq.supabase.co
```