Mobile App Security Testing

1 Agenda

This document is a guide to set-up Mobile App security testing environment and help performing Static and Dynamic security testing. All the information provided in this document is for educational purpose only. The author is not responsible for any misuse of the information or your bricked devices.

Contents

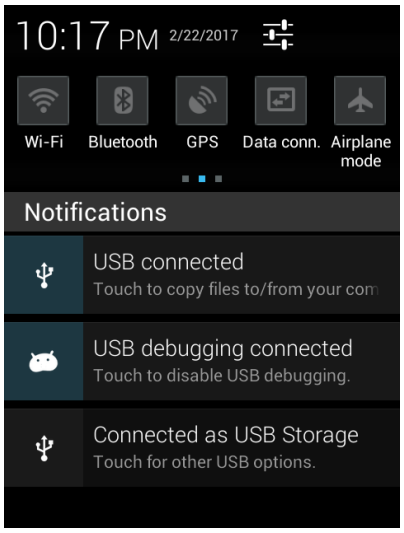
2 Android App Testing

2.1 Static analysis with Device

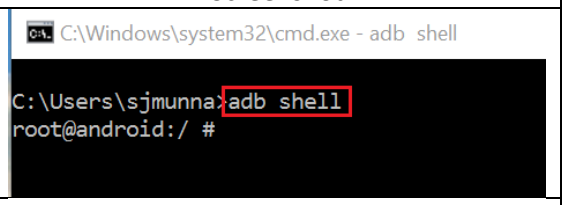
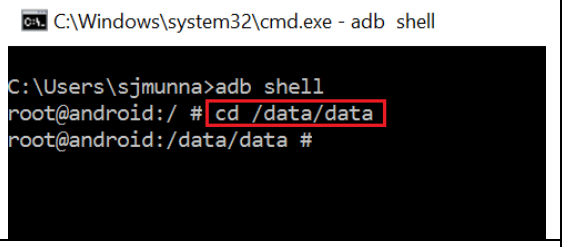
- Pre-requisites:
  - Android Device with root access & USB debugging enabled (How to Root the Device)
  - Android Studio installed in system and path variable (Environment Variable) set to adb (e.g. *C:\Users\SARWAR\AppData\Local\Android\sdk\platform-tools*)

2.1.1 Connecting to adb shell and access App Data

- Enable USB debugging in the Android device
- Connect the device to the system in "USB Storage" mode



- Open Command prompt in the system and type the following commands in sequence:

Command	Description	Screenshot
adb shell	Get shell access to the connected Device	
cd /data/data	Traverse to the Device App data folder	
ls	Displays all installed packages	
cd <target_app_ packageName >	Traverse to the target app Data folder	

ls	Displays all app data folders of the target app	cache databases files lib no_backup shared_prefs

- Traverse to the folders and open the files and search for sensitive data like Credentials, Tokens etc. (image here)

2.1.2 Pull app data from device to the system

- Create a folder in your system where the pulled data has to be saved. (e,g, *D:\N*)
- Enable USB debugging in the Android device
- Connect the device to the system in "USB Storage" mode
- Open Command prompt in the system and type the following command

  adb pull /data/data/<target_app_packageName>/ D:\N\
- Now the app data files can be browsed in system from the above folder (D:\N\).
  - Check all XML files for sensitive data
- Use sqlite browser to read/write/modify the data stored in App's local *databases*.

2.1.3 Push modified data back to Device

- Open Command prompt in the system and type the following command

  adb push D:\N\<packageName>\ /data/data/<target_app_packageName>/

2.2 Static analysis with Emulator

- Pre-requisites:
  - Android Studio installed in system and path variable (Environment Variable) set to adb (e.g. *C:\Users\SARWAR\AppData\Local\Android\sdk\platform-tools*)

2.2.1 Analyze with emulator

- Run the Android Emulator and open the target app
- Open Command prompt in the system and execute all the commands as mentioned in 2.1 section.

2.3 Dynamic analysis - Device and System both are connected to same network

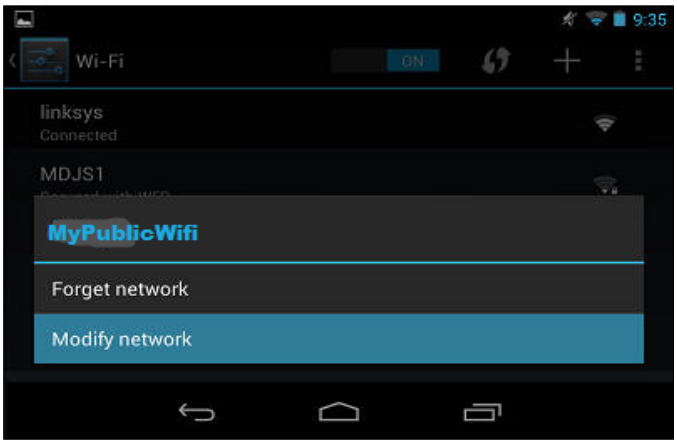
- Pre-requisites:
  - Fiddler
  - Burp Suite

2.3.1 Configure Fiddler and Burp Suite to intercept the traffic (Configure Fiddler)

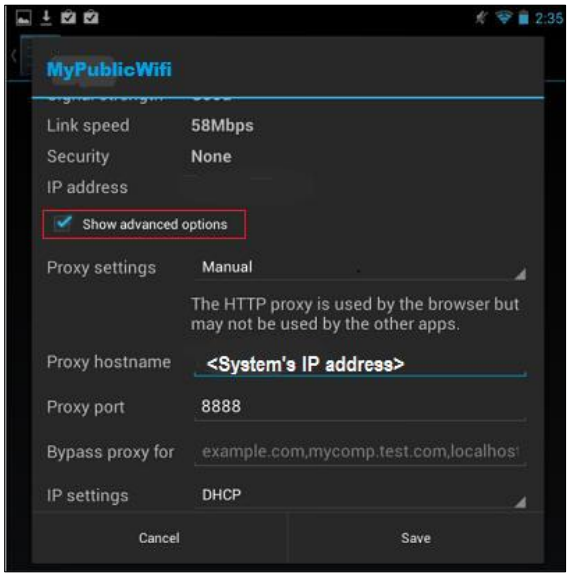
2.3.2 Install Fiddler Root Certificate in Mobile Device (Install Fiddler Root Cert & Burp Cert)

2.3.3 Configure Mobile Device:

- Long tap on the access point under device wifi settings, Tap **Modify network**



- Check ***Show advanced options,*** Select Proxy settings as **Manual.**



- As shown in above image, set proxy hostname as your system's IP address (ipconfig) and Proxy port as 8888 (Fiddler port).

2.4 Dynamic analysis – Device connected to Wi-Fi hotspot hosted in the system

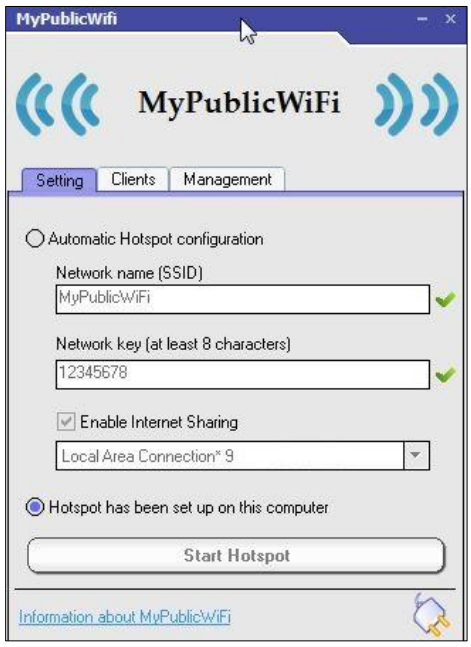
- Pre-requisites:
  - My Public Wifi
  - Fiddler
  - Burp Suite

2.4.1 Configure Fiddler and Burp Suite to intercept the traffic (Configure Fiddler)

2.4.2 Install Fiddler Root Certificate in Mobile Device (Install Fiddler Root Cert & Burp Cert)

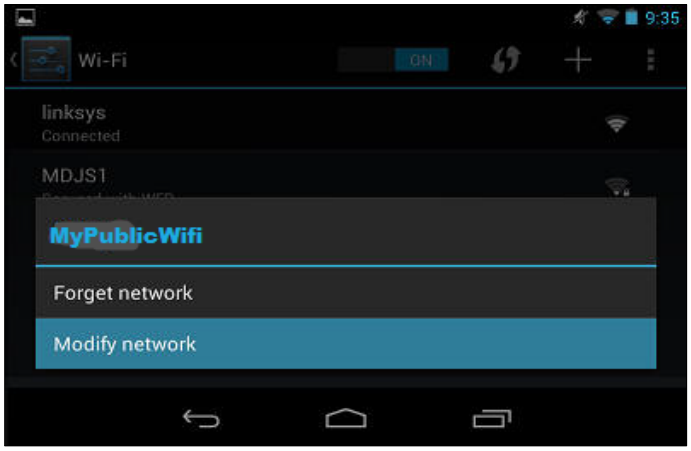
2.4.3 Creating Hotspot:

- Install **MyPublicWifi** software and Start Hotspot.

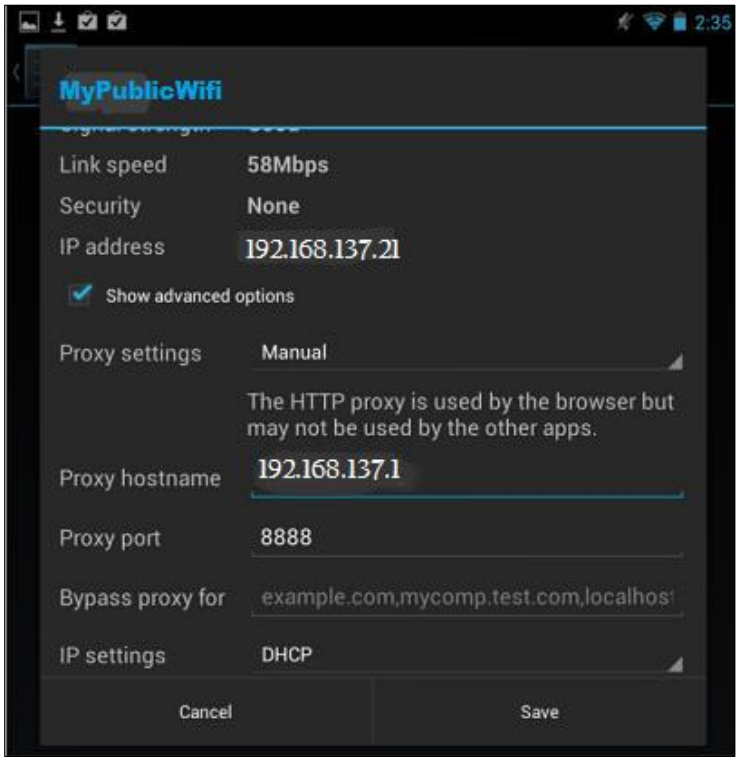


2.4.4 Configure Mobile Device:

- Connect to MyPublicWifi Hotspot
- Long tap on the access point under device wifi settings, Tap **Modify network**



- Check ***Show advanced options***



- As shown in above snapshot, IP address will be automatically assigned. Select Proxy settings as **Manual.**
- Proxy hostname: **first three octets same as IP address & last octet value as 1**
- Proxy port: **Fiddler listening port (by default 8888)**

3 iOS App Testing

3.1 Device Set-up

- Jailbreak the iOS device and install Cydia.
- Connect the device and system both in same network.
- Open Winscp in system and type the device IP.
- Enter root password of device.
    - Transfer files between the device and system.
- Use ipainstaller app in device to install ipa files.
- Use ifile app in device to explore app data.

3.2 Dynamic analysis

- Same as Android Devices

4 Miscellaneous

4.1 How to Root the Device

Rooting the device:

1. Install **KingoRoot**.apk
2. Connect the device to a wifi network
3. Run KingoRoot and root the Device

Install CWM Recovery (Optional):

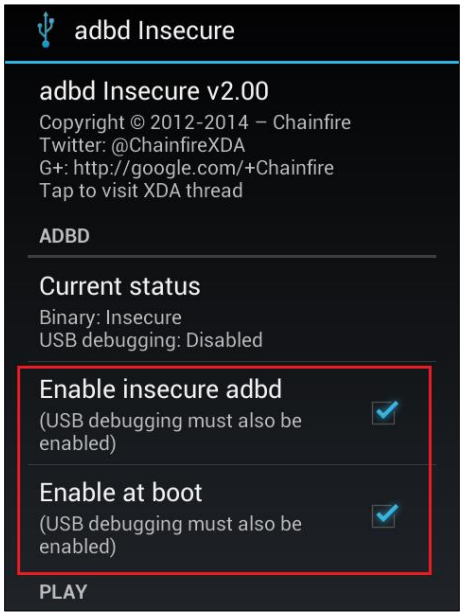
1. Copy the **recovery.img** to root folder of device storage.
2. Install **MobileUncle** in device.
3. Open the MTK tools app and select the Recovery Update option and then select the recovery.img file you copied to device root storage and click OK. Wait for a while till the app flash CWM recovery on the device.
4. Reboot your device in CWM recovery and install Custom ROMS.

Install any Custom ROM (Optional):

1. Turn on the device by pressing **Volume UP/DOWN + Power button**
2. Wipe Data/Factory Reset
3. **Format System** inside **Mount And Storage**
4. Wipe Cache
5. Install the Rom zip file (browse from SD card)
6. When Installation completed, Reboot System

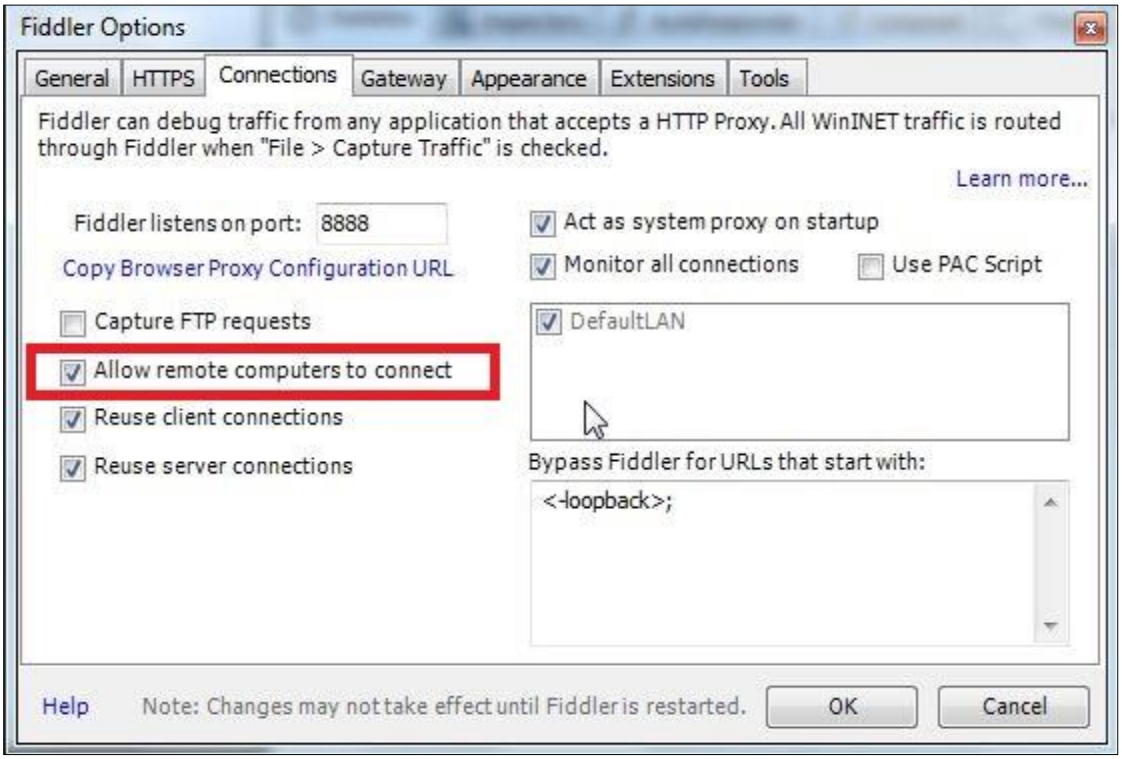
ADB Shell Access:

1. Install **adbd-Insecure-v2.00.apk** for adb shell access from system
2. Run the app in Device and make the following settings:

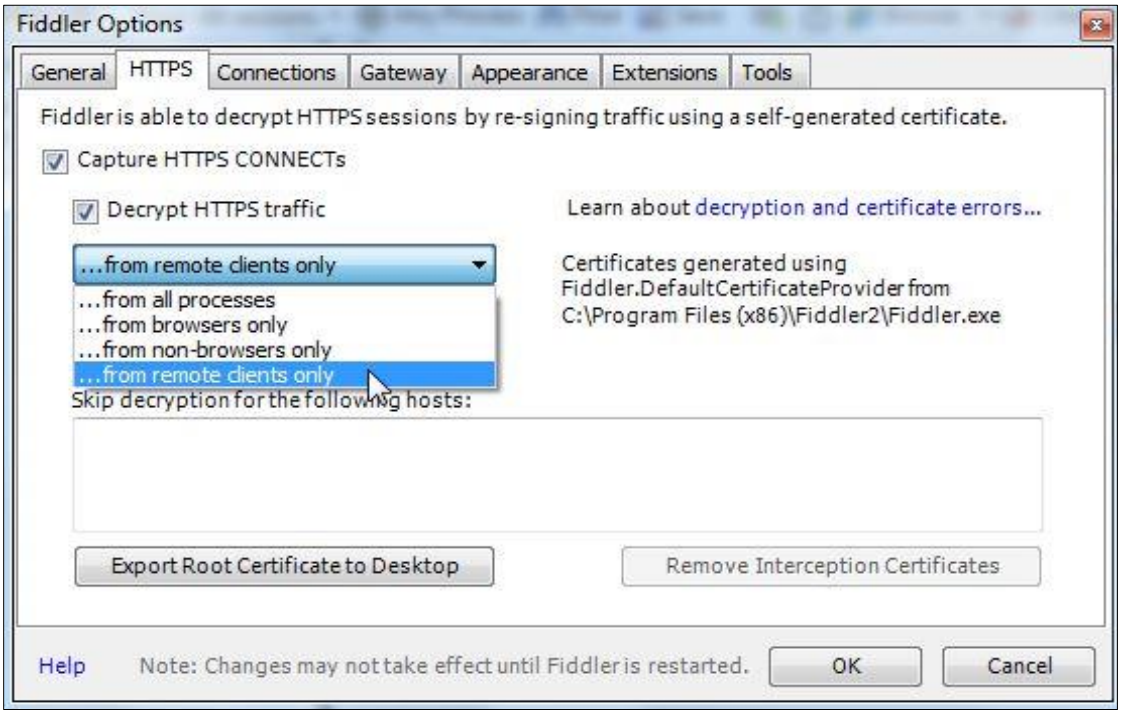


4.2 Configuring Fiddler: (Pre-requisite: install fiddlercertmaker in the system)

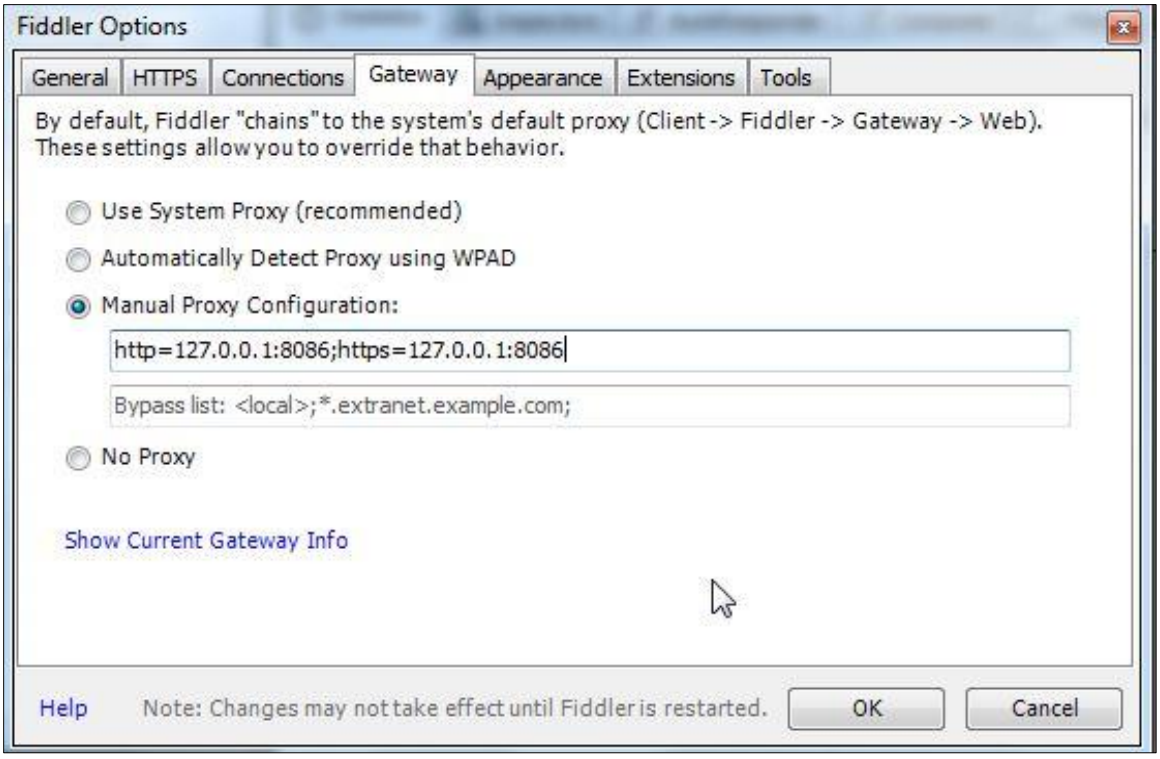
1. Allow Mobile Device traffic capture: ***Tools->Fiddler Options->Connections***



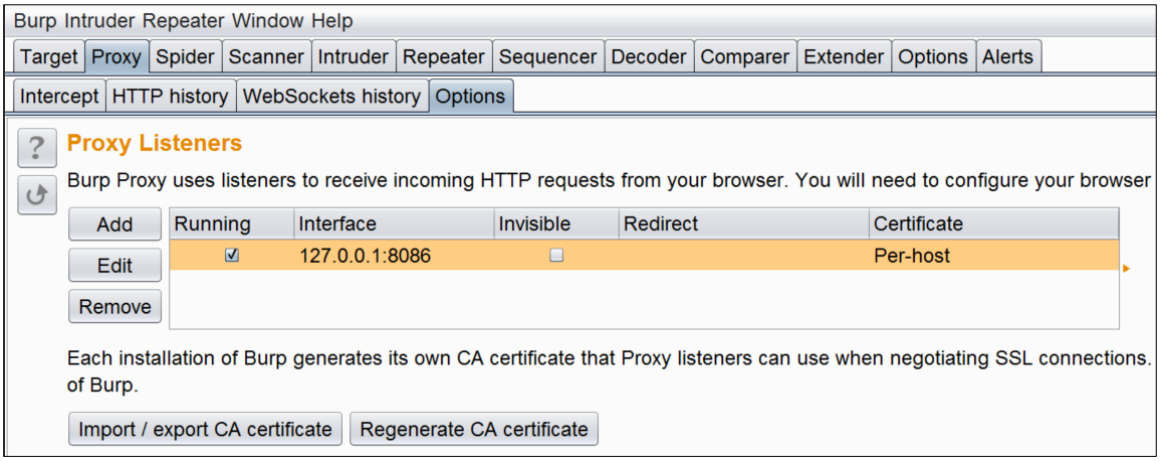
2. HTTPS traffic capture ***Tools->Fiddler Options->HTTPS***



3. Integrate with Burp Suite: ***Tools->Fiddler Options->Gateway***



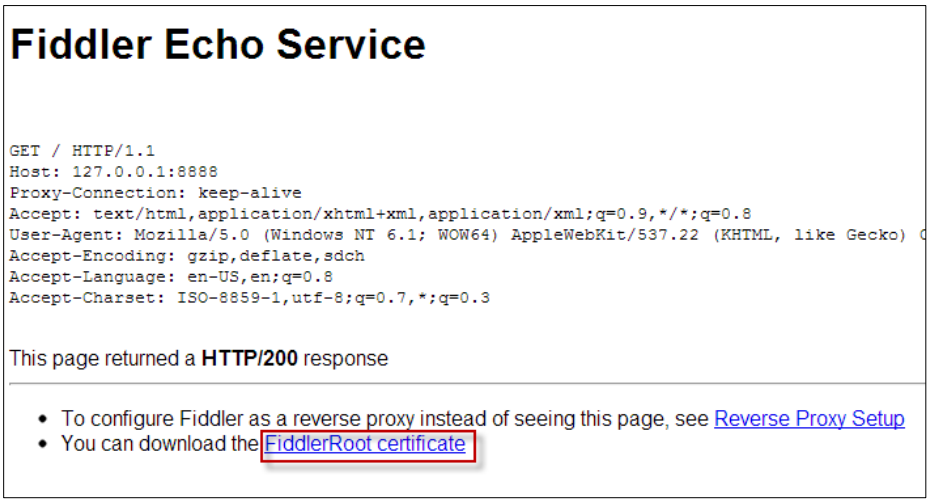
4. Burp Proxy listener



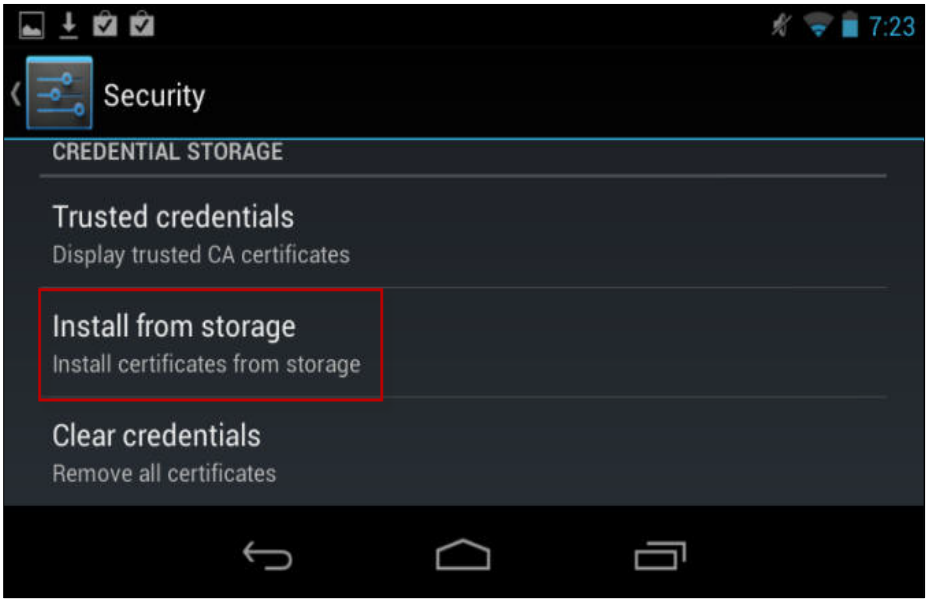
4.3 Installing Fiddler root certificate on Mobile Device:

- **Method 1: Install using Device's browser**

1. Open Firefox or Chrome browser App in Device
2. Go to **http://<Proxy hostname>.fiddler:8888/**
   (e.g. **http://192.168.137.1.fiddler:8888/**) [older fiddler versions]
   Go to **http://(hostPC):(port)/FiddlerRoot.cer**
   (e.g. **http://192.168.137.1:8888/FiddlerRoot.cer**) [latest fiddler versions]
3. Following page will get opened, Download the certificate.

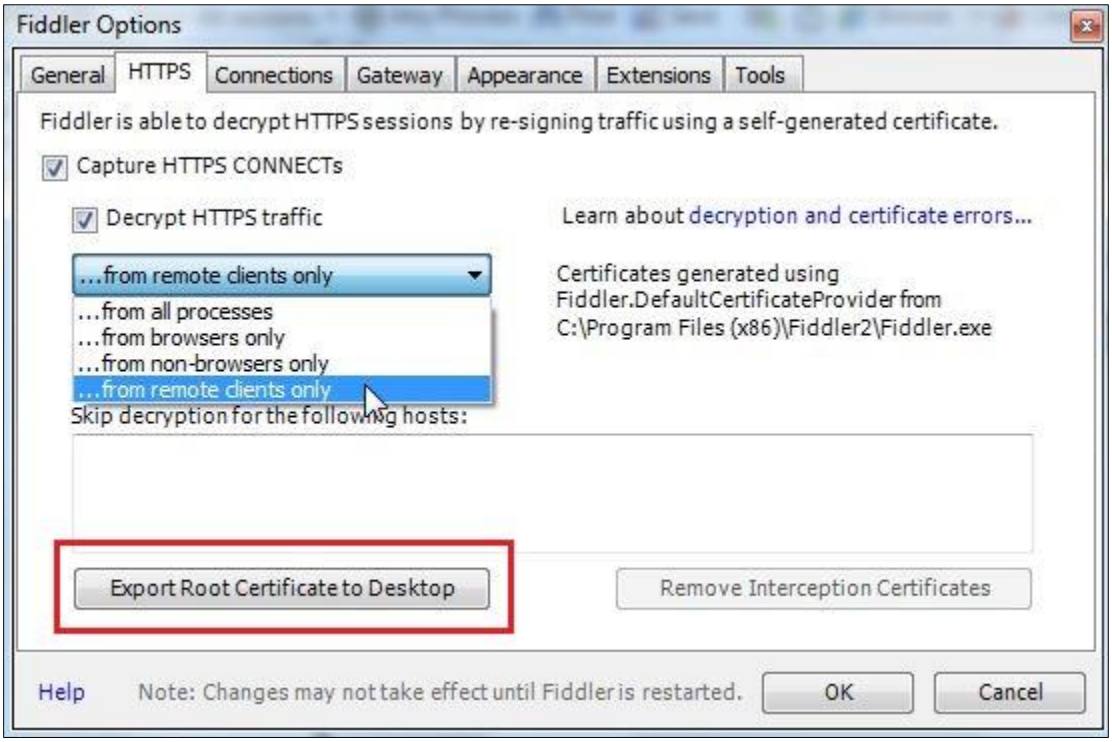


4. From the Device's *Settings->Security*, install the certificate,

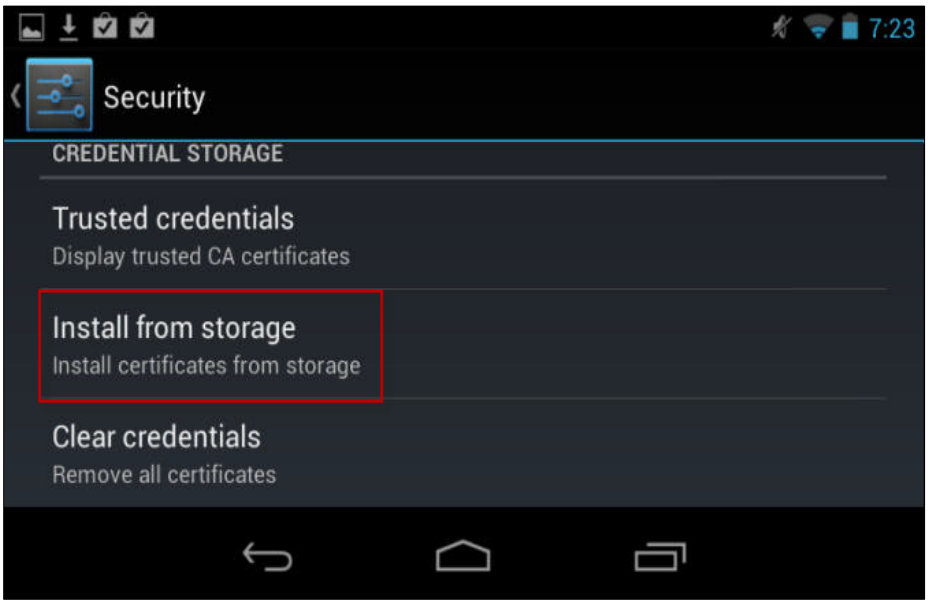


- **Method 2: Export root certificate from Fiddler tool**

1. In Fiddler, navigate to ***Tools->Fiddler Options->HTTPS*** and export the Root Certificate

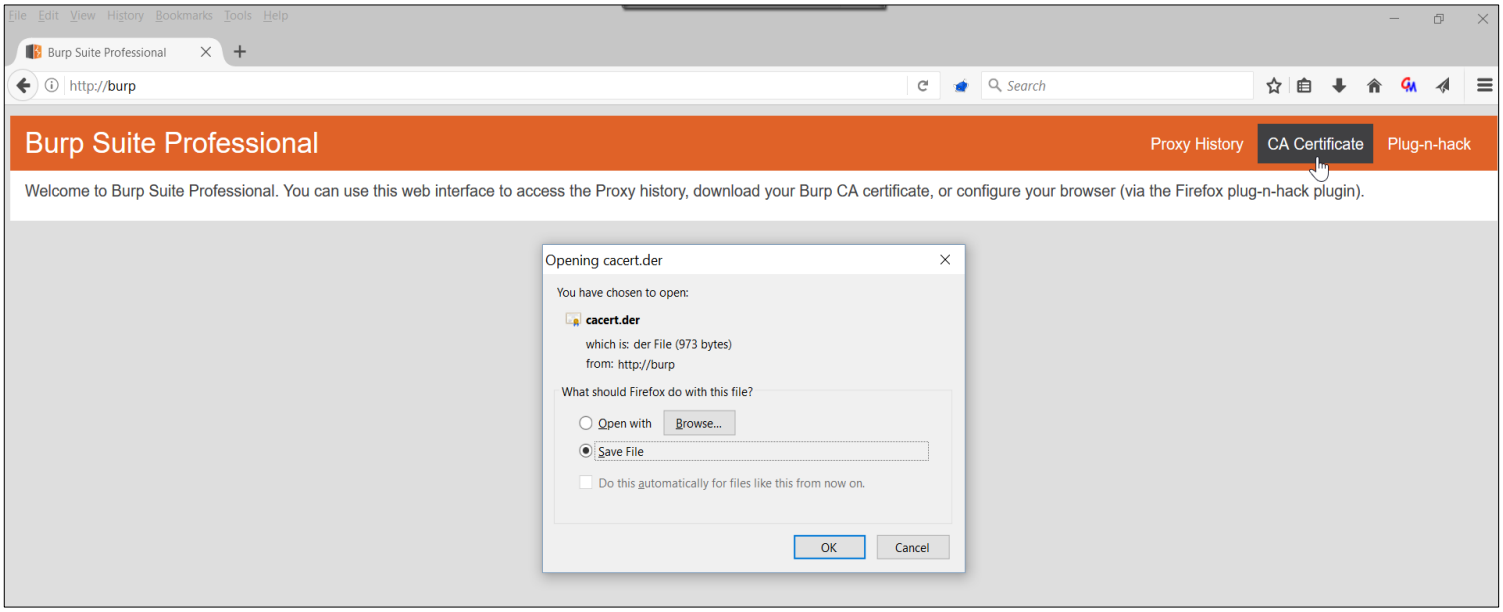


2. Copy the Certificate to mobile device.
3. From the Device's Settings->Security, install the certificate as shown below:



4.4 Installing Burp certificate on Mobile Device:

- Open Burp Suite.
- Open a browser which is configured with Burp Suite and type *http://burp*



- Download the CA Certificate
- Change the extension from .der to .cer
- Copy the Certificate to mobile device.
- From the Device's Settings->Security, install the certificate as shown below: