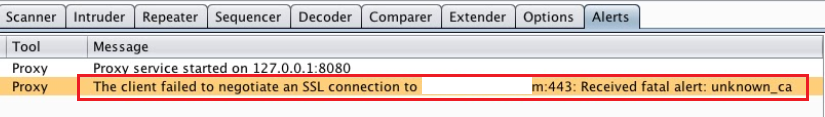
**SSL Pinning bypass using Frida**

First try to capture app traffic. If SSL Pinning is implemented then you will get certificate error.



Follow below steps to capture HTTPs traffic by bypassing SSL Pinning using Frida

1. Install Frida and Frida tools

pip install Frida

pip install frida-tools



2. Download adb platform tools if not installed on your computer.

3. Download frida injection script (pinning.js and universal-ssl-check-bypass.js) for bypass SSL pinning

<https://gist.github.com/cubehouse/56797147b5cb22768b500f25d3888a22>

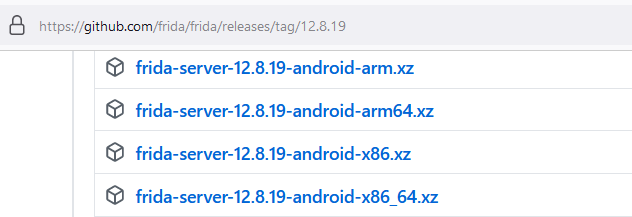
<https://techblog.mediaservice.net/2018/11/universal-android-ssl-pinning-bypass-2/>

4. Connect your device using below adb command

adb connect <ip of device:port>

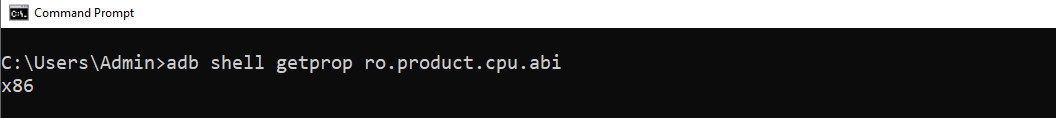
5.Download Frida’s server for supported android device’s arch version form below link

<https://github.com/frida/frida/releases/>



6. To find out arch version of device use below command

adb shell getprop ro.product.cpu.abi



7. Push Frida-server into device using below command

adb push <path of frida-server folder><space></data/local/tmp>



8. Give permissions to frida-server using below command

adb shell chmod 777 /data/local/tmp/frida-server



9. Pushing the proxy’s CA Certificate

adb push <path to cacert.der> /data/local/tmp/cert-der.crt

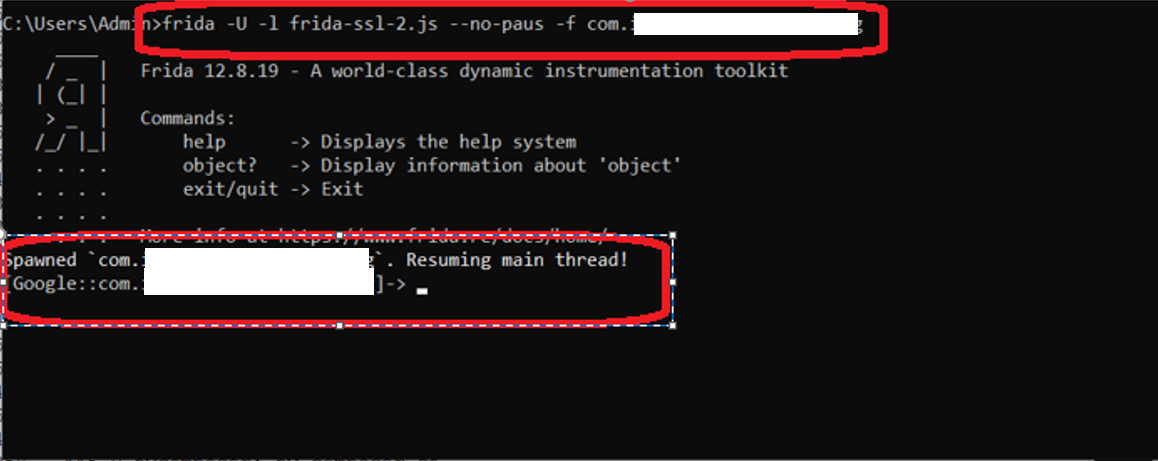
10. Check and run frida server in device

adb shell /data/local/tmp/frida-server &



11. Hook target application with script by using below command

frida -U -l <path\_to\_frida-ssl-2.js\_on\_your\_pc> --no-paus -f <your\_app\_package\_name>



12. The following screenshot shows that SSL Pinning is bypassed successfully and now we are able to capture https traffic in proxy tool

