We have successfully installed Fiddler and are working on MobSF installation. Fiddler can do dynamic analysis of both Android/iOS apps and MobSF can do both static and dynamic analysis but only for Android apps.

PFB our findings -

For dynamic analysis, an app will fall in one of these 4 categories -

1. An app is validating both certificate chain (certificate is signed by Trusted Root CA) and hostname.

2. App is validating only certificate chain but not hostname.

3. App is validating only hostname but not certificate chain.

4. App is not validating either of them.

**The strategy we have decided on is as follows -**

1. Check Certificate Validation (Given correct host name) - In this part we want to check if the app is checking the chain of trust for the certificate presented to it. So, we will be giving the app a certificate with nearly valid host name (which is collected by Fiddler using CONNECT request) and Fiddler's root certificate will NOT be added as trusted in the phone. Therefore, we can check if the app is validating the chain of trust when it is given the certificate with correct hostname.

2. Check Hostname Verification (Given Trusted Certificate)  - In this part we want to check if app is matching Common Name of certificate with that of the server's name. So, we will be making Fiddler's certificate a Trusted one in the phone and provide any random hostname certificate to the app which is signed by the trusted Fiddler's CA.

Therefore, we can check if the app is checking host name also or it is just stopping all the validation after checking the chain of trusted CA's.

Real World Scenario - An adversary can give any certificate to the app, signed by a worldwide trusted authority and perform mitm.

3. If an app fails for both of above scenarios, then we will check Category -4 i.e. app is not validating either of them. So, we will give any random hostname certificate to the app signed by our own CA which is not even on the list of trusted CA in the phone and check whether the app works or not.

**How Fiddler Works :**

Similar to the mitmproxy/Packer capture app, Fiddler will decrypt HTTPS packets if Fiddler's root certificate is installed as Trusted one in the phone by providing a fake certificate to the app with a similar hostname as expected by the app(which is collected by Fiddler using CONNECT request) on the fly.

**How we are using Fiddler -**  
  
1. For Certificate Validation- Without installing Fiddler's certificate as trusted one in the phone, we will try to decrypt HTTPS messages and find out if the app is doing certificate validation correctly.  
  
2. For Hostname verification- After installing fiddler's certificate as a trusted one  on the phone, and hardcoding fiddler to send a fake certificate with a random Hostname, signed with Fiddler's root CA and then we try to decrypt HTTPS messages and find out if the app is doing Hostname verification correctly.