MobileAppTesting

■http://pen-testing.sans.org/blog/pen-testing/2013/12/02/mobile-device-tips-tricks-and-resources

---------- Mobile Application Test Notes (iPhone)

Prepping Device and Application:

[+] Jailbreak iPhone/iPad - Green Poison / Absinthe 2.04
[+] Enable SSH on iPhone/iPad
[+] Install iFunbox to install the application (http://www.i-funbox.com)
[+] Connect device to lab wireless network
[+] Add web proxy settings - IP address of attacking machine port 8080
[+] Ensure connection and SSH is working

Prepping Burp Suite:

[+] Open Burp Suite and navigate to Proxy->Options,
■[-] Edit proxy listeners – enter ‘port’ as 8080, disable ‘loopback only’ and select ‘support invisible’.

[+] Download and install burp certificate (.crt) onto ipad.

Mobile Application Penetration Testing:

[+] Browse the following Directory for insecure storage
■[-] /private/var/mobile/applications/

Notes:

[+] Application file type - x.ipa

[+] Easy way:

- Place attacking machine and apple device on wireless network with app installed.
- Email burps .cer to apple device and install
- Start burp and disable firewall on listening machine.
- Change proxy settings on apple device to point to listening burp machine/port.

---------- Mobile Application Test Notes (Android)

Prepping the application
(After Android Nougat, Apps need to repackaged since they don't trust user certificates by default)
- https://android-developers.googleblog.com/2016/07/changes-to-trusted-certificate.html

[+] apktool d <path of the .apk file>
[+] Update AndroidManifest.xml
■[-] Add android:networkSecurityConfig="@xml/network_security_config" to application tag in xml
[+] Add network_security_config.xml to res/xml folder
■[-] "Trusting user-added CAs for all secure connections" section in
■■https://android-developers.googleblog.com/2016/07/changes-to-trusted-certificate.html
[+] Repackage the application
■[-] apktool b unpacked_apk_folder -o <output path to new apk file>
[+] Signing the application
■[-] Create a keystore using keytool
■[-] jarsigner -keystore <path to your keystore> -storepass <password> -keypass <password> <path to apk> android

Creating an emulator and installing the application

[+] Create a virtual device:
■[-] android avd

[+] Start the emulator:
■[-] emulator –avd testavd

[+] Install the application:
■[-] adb install <path of the .apk file>

[+] Open Burp Suite and navigate to Proxy->Options,
■[-] Edit proxy listeners – enter ‘port’ as 8080, disable ‘loopback only’ and select ‘support invisible’.

[+] Start the emulator and proxy:
■[-] emulator –avd testavd –http-proxy http://localhost:8080

[+] Download and install burp certificate (.crt) onto the emulator using the push shell command.

Notes:

[+] Application file type - x.apk

Install Certs: http://www.realmb.com/droidCert/
SQLite Database Browser: http://sourceforge.net/projects/sqlitebrowser/?source=pdlp

http://www.mcafee.com/uk/resources/white-papers/foundstone/wp-pen-testing-android-apps.pdf