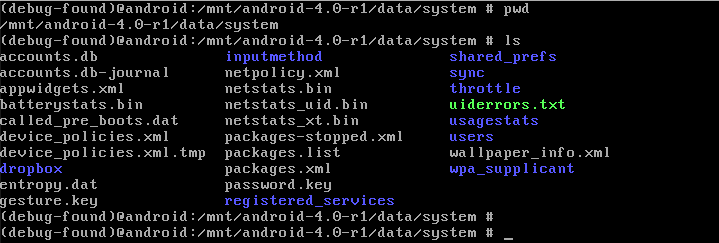
# BadDroid

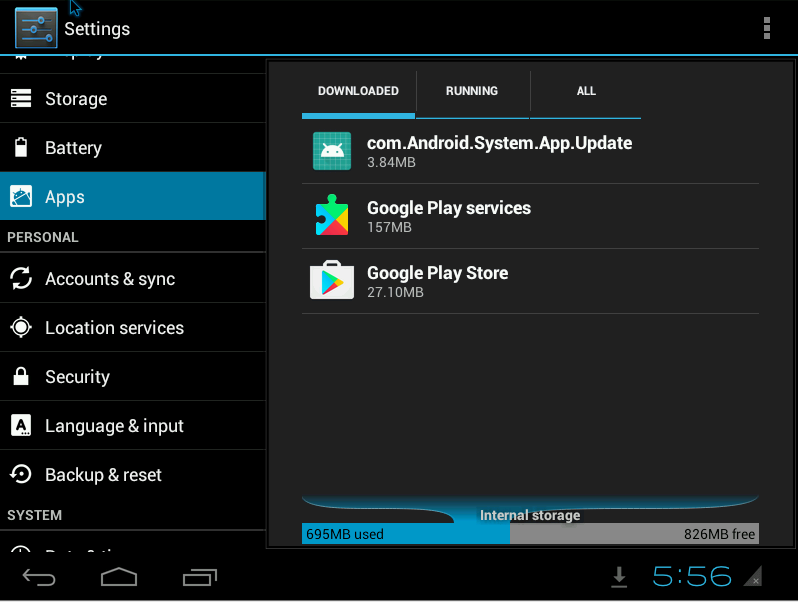
Дана виртуальная машина андроид, нужно найти артефакты.  
При первом запуске видим что она запаролена - имеем несколько вариантов обхода данной функции. Данные аккаунта мы не знаем - поэтому этот вариант не рассматриваем.

По причине некорректной работы sqlite - выбираем способ не переписывания базы данных, а удаления файла ключей

Запускаем виртуалку в debugMode и идем по пути:

Видим два файла: gesture.key и password.key. Удаляем их и ребутаем машину.

Далее можно зайти без всяких проблем.

Открываем настройки-настройки-приложения и видим следующую картину:  


Вытаскиваем любым из способов данных APK и реверсим его (связки dex2jar или просто через AndroidStudio), смотрим исходники.  
Собственно приложение не делает ничего плохого, но зачем то стучится на сервер + видно часть флага:

Заходим на сервер и забираем первую часть флага - изи сотка.

P.S. Да, можно было бы отследить трафик с виртуалки, но без реверсинга апк все равно бы не обошлось. Есть так же способ достать апк не выключая пин, но это совсем другая история.