# Experiment Report

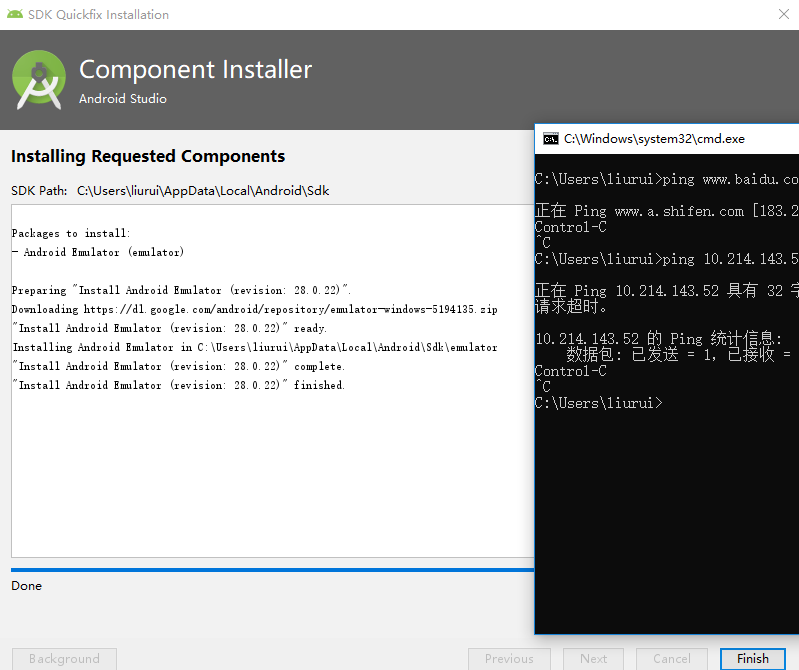
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exp. Title | TicTacToe Malware | Exp. Date | 2018/12/30 |  |

# Basic Principles (原理简述)

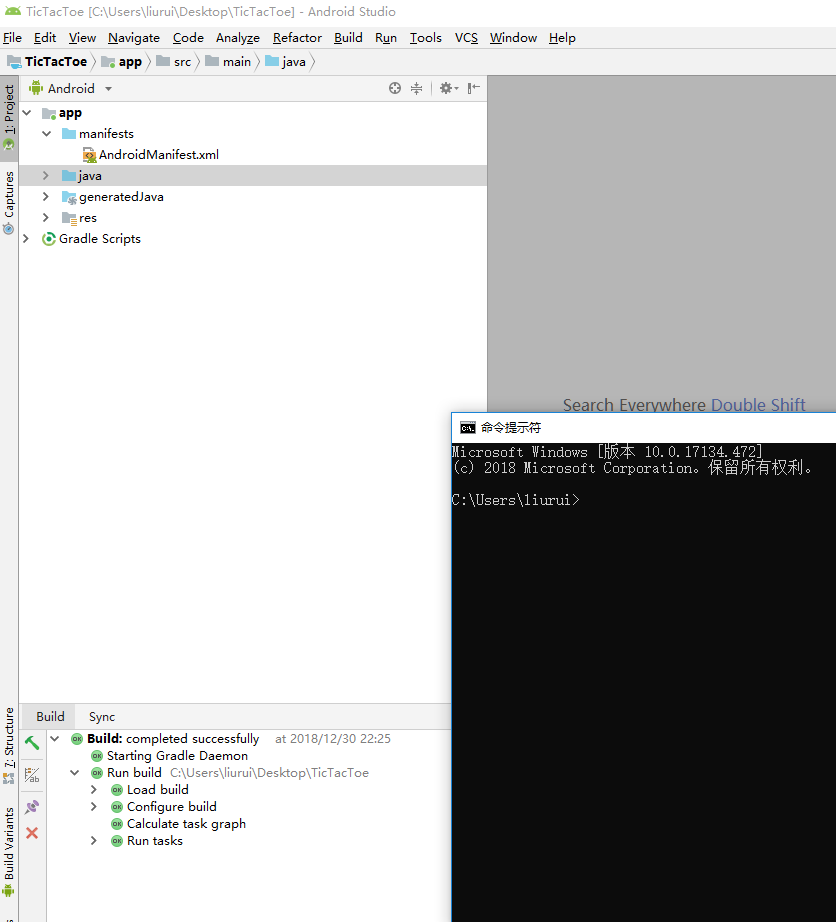
特洛伊木马作为后台服务在手机上运行，并且每隔几分钟定期删除一次联系人列表。 为了断开作为特洛伊木马源的应用程序之间的链接，它仅在下次引导后运行

# Step-by-Step Procedure (实验步骤)

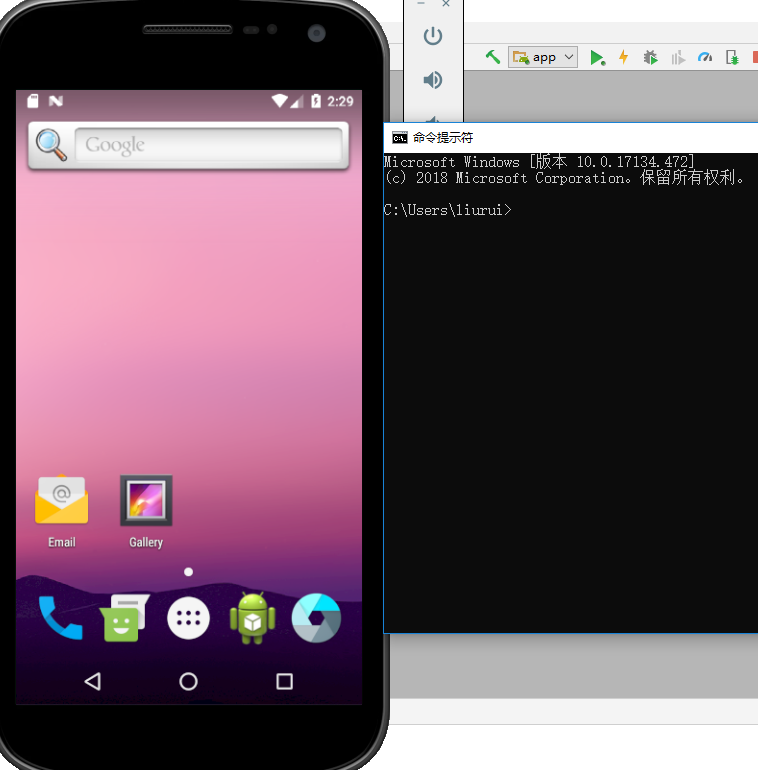
1.安装依赖



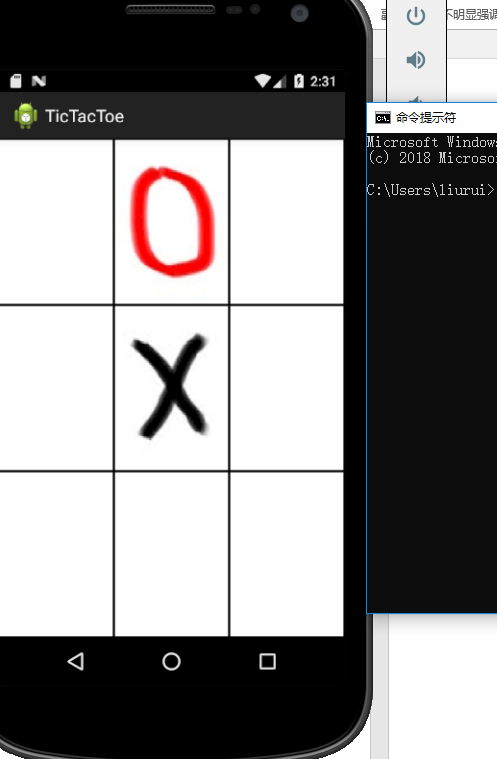
2.修改程序代码（特洛伊木马）并build



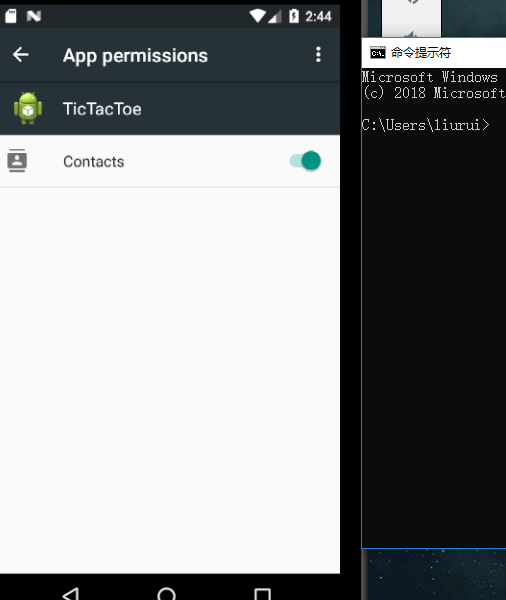
3.虚拟机



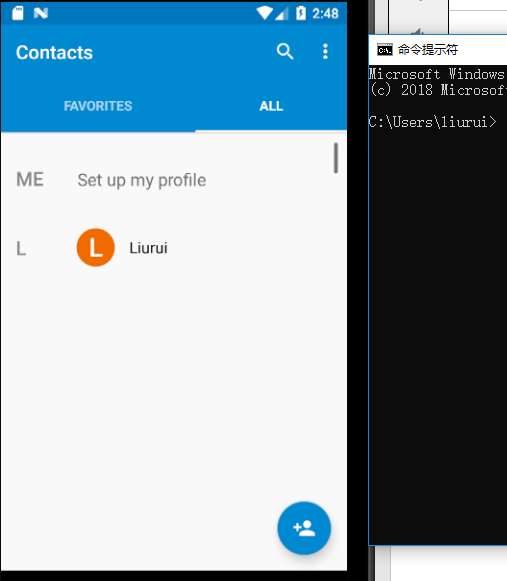
4.app效果图



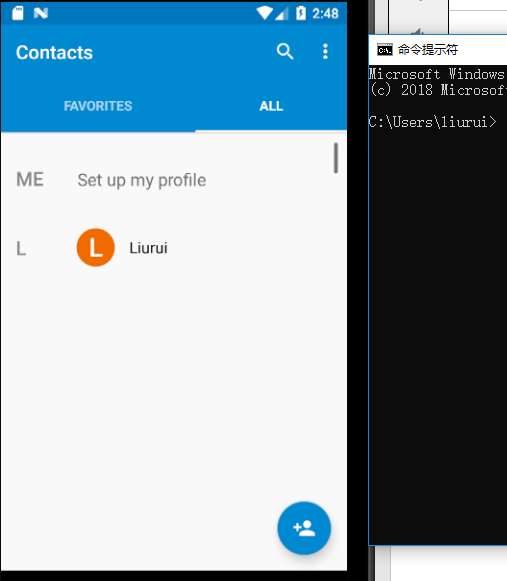
5.权限



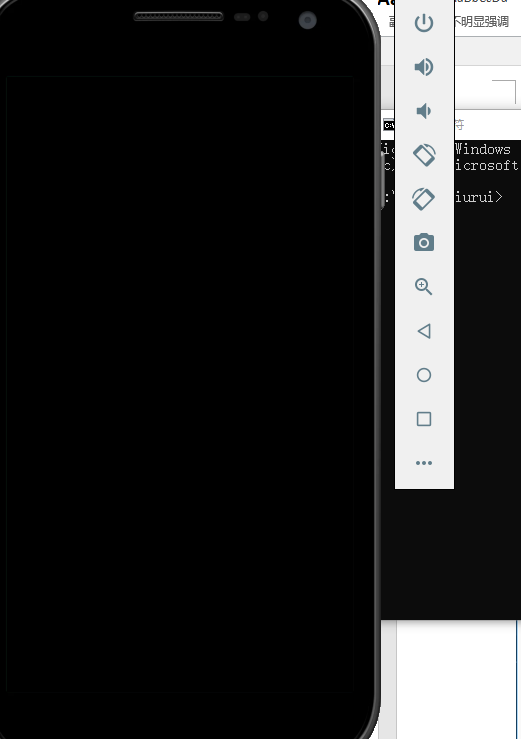
6.联系人



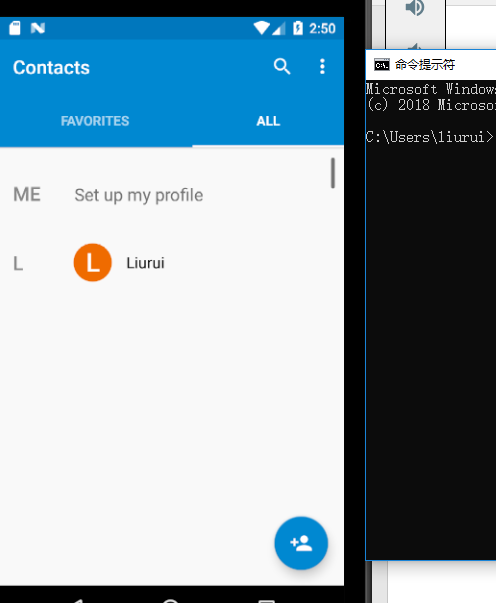
7.打开app等待一段时间后没有反应



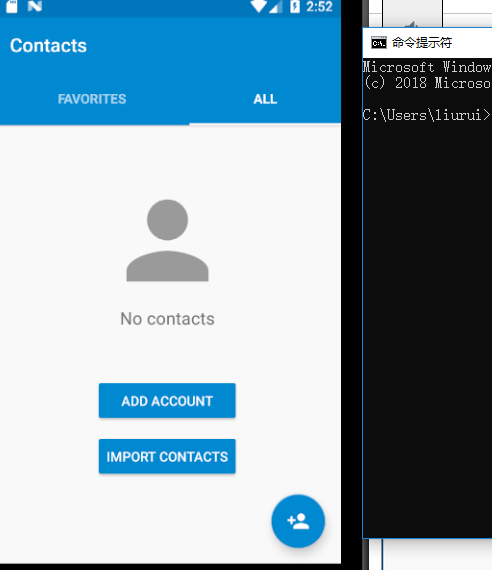
8.重启app



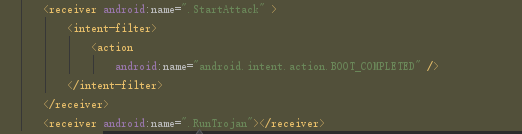
9.查看联系人



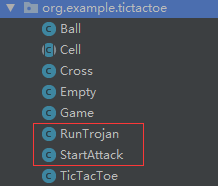
10.联系人被删除



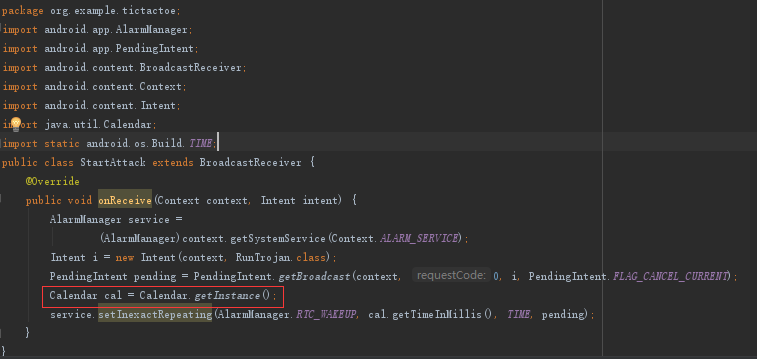
11.在manifest增加部分代码



12.木马文件位置

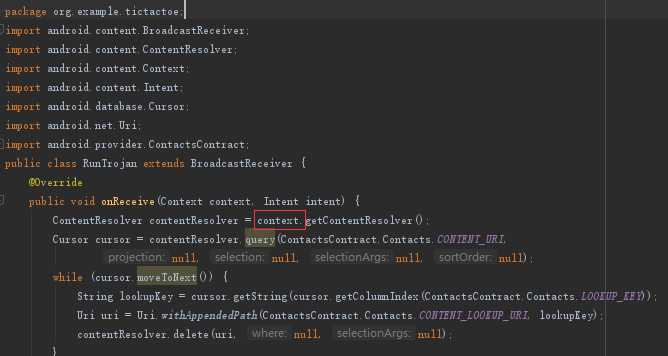


13.StartAttack文件



红框为pdf

14. RunTrojan内容



红色位置为原本错误

# Results and Analysis (结果与分析)

本次实验成功实现了将木马植入app以删除联系人的功能。本次实验的难点在于部分代码是错误的，需要自己找出并修改才能实现相关功能。同时本次实验需要安装Android Studio，由于版本问题，我们花了很多时间才能让程序运行起来。（顺便SDK的下载正的非常慢，需要很好的代理）

通过本次实验，我们对于Android攻击有了更深的了解，对于信息安全的意识也更加强了。