《电子证据分析》课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 实验名称 |  | 姓名 |  |
| 班级 |  | 学号 |  |
| 实验日期 |  | 指导老师 |  |
| 实验环境  (实验软硬件要求) |  | | |
| 实验目的 | （给出本次实验所涉及并要求掌握的知识点）  *使用Android Studio的虚拟机服务，并且使用安卓调试桥进行调试。*  *掌握相关的安卓系统的相关知识* | | |

|  |  |
| --- | --- |
| 实验内容 | 1. adb 的基本命令使用   利用Android Studio自带的adb命令：adb.exe devieces    可以看到设备，然后直接用 adb.exe shell -s <设备名字>即可选择对应的设备    里面进入了shell之后支持大部分的linux命令，例如，使用ls命令可以看到对应目录的文件。    如果需要知道这些文件的属性则可以使用ls -l这样显示的文件都是会显示它是不是文件（或者是目录）还有对应的权限。    另外，安卓也是和我们常用的windows不一样的，没有C盘、D盘等等。使用mount命令可以看到硬件挂载的对应的位置以及权限。    这里可以看到vda是只读的（它是系统的分区），而vdc（它是用户数据的所在的分区）   1. 破解安卓的手势和PIN锁屏密码   首先设置好了命令之后。虚拟手机显示如下：    可见已经需要使用密码才能解锁了。  然后使用adb调试软件。  首先需要确定这个密码文件在哪里。  根据老师的提示，在/data/system/内找到了gesture.key。  确定是不是这个文件，直接删除并且重启之后，发现屏幕的密码就没了。    所以就确定是这个文件，接下来重新设置个密码。    密码就是在调试桥的shell里面输入exit退出shell。  然后使用命令  adb pull /data/system/gesture.key D:\desktop  这样就会将它虚拟机里面的文件弄出来了，接下来使用软件    选定好文件的位置，点击开始破解就可以了。    接下来，破解pin密码了。  一样的，首先设置好PIN码。我设置为1234  然后就是连接adb shell，已经知道了PIN码明文哈希以后的密码是在/data/system/password.key这个文件里面，所以，查看这个文件的内容，cat /data/system/password.key  得到的内容就是  ：  这个是加了salt之后哈希的，那么salt这个随机数还在locksettings.db里面可以查看。  安卓的db都是使用的是sqlite3的，所以，使用sqlite3 locksettings.db  然后 .table可以看到里面有几个表，salt应该是在locksettings这个表里面的，所以.dump locksettings 就能得到salt了，这样两样需要的东西都有了    接下来，使用工具即可。    分别输入salt和password.key就行了。得到的结果如下： |
| 实验总结 | （对本次实验涉及到的知识点的重难点归纳、实验心得、思考与建议） |
| 评分 |  |