《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) | 安卓模拟器、adb | | |
| 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   使用adb的shell  利用Android Studio自带的adb命令：  adb.exe devieces # 查看目前连接的设备  adb -s <设备名> shell # 选择连接的设备    里面进入了shell之后会支持大部分的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）则是可读可写的。  这个也可以解释为什么在进行系统升级的时候我们的手机会需要关机进行操作，因为手机的系统分区在这里被设置为只读，只可以关机以后进入另外的系统，然后再修改系统分区。  这样也就是为什么大多数的系统升级都是会保留下用户的数据的，以及恢复出厂设置系统的版本依旧停留在当前的版本的原因。  另外，之所以说是支持大部分的命令，但是有些时候不知道为什么命令会有时候生效有时候无法生效，在上课的时候我使用虚拟安卓，使用ll命令列出目录内容的时候会报错，显示没有这个命令，但是在回到家重新实验时，发现这条命令又可以正常使用了。     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：    因为老师提供的软件是仅支持4位的PIN码，所以之前在尝试最开始的6位PIN码的时候就出现了问题。   1. 详述手机文件系统中的伪文件系统dev分区和proc分区内容   不知道为什么我的dev分区和proc分区用之前的办法ls直接不显示了，很奇怪。    但是直接使用cd还是可以进入这两个“不存在的”分区的    其实这两个分区也就是伪文件系统（VFS），先说说dev，在这个目录里面使用了ls -al以后可以看到手机里所有的硬件，例如CPU、内存(mem)、字符型设备(tty)等等……    要注意的是，这些看上去都是存在的文件，但是事实上都是虚假的，只是用文件的形式来将这些硬件展示给我们看而已  如果尝试访问这些文件，他们就会将这些硬件里的信息给我们展示（以mem为例）    不过这些都是乱码，应该是需要专门的16进制查看器才能看明白。  另外，dev分区里面有一个比较重要的地方，就是下面的block这个“目录”：  进入这个目录后就会发现里面有这部手机所有的块设备    那么，如果需要制作vda分区的镜像，那么只需要使用下面的命令就能制作对应的镜像了：    这个命令就是制作vda分区的dd镜像，并且输出文件名为11.dd  上面这样就可以了。  然后就是proc分区。它以文件系统的方式为访问系统内核数据的操作提供接口。    它将所有的文件都以数字来进行命名，而且这些数字就是对应的进程的id号。  在进入了任意一个进程文件之后，就能看到这个进程里面的所有的信息  当然，这些也都是伪文件。  oom值是安卓独有的，linux里面是没有的。  这里面要注意，status表示这个进程的状态，可以用cat来查看。    在这里面state表示的是这个进程当前的状态，如果被调试了，这个state的值就会是D（表示debug）  这里的cwd表示当前的目录    这里的exe表示的是可执行性文件的全目录 |
| 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）  安卓的伪文件系统比较特别，它本身并不存在于手机的外存中，而是在手机的内存空间里，它以文件系统的方式来提供访问系统的内核数据的接口。这样的伪文件系统与我们之前学习的windows操作系统是有比较大的差异的。 |
| 评分 |  |