**ADB协议总结**

ADB（Android Debug Bridge）设计架构图

[pkiller.com](https://pkiller.com/android/android-adb%E6%9E%B6%E6%9E%84%E5%8F%8A%E5%AE%9E%E7%8E%B0%E5%88%86%E6%9E%90/)

**Android 是如何开启adb的**

Android usb的各种模式：adb、mtp、ptp

adbd的启动

adb在AOSP中的位置：system/core/adb

adb的一些端口问题

adb auth 流程

**adb 协议封装格式**

无论是通过USB线连接设备，还是通过WIFI-ADB连接设备，其遵循的协议都是一样的。

数据头24字节，小端存储



**点击图片可查看完整电子表格**

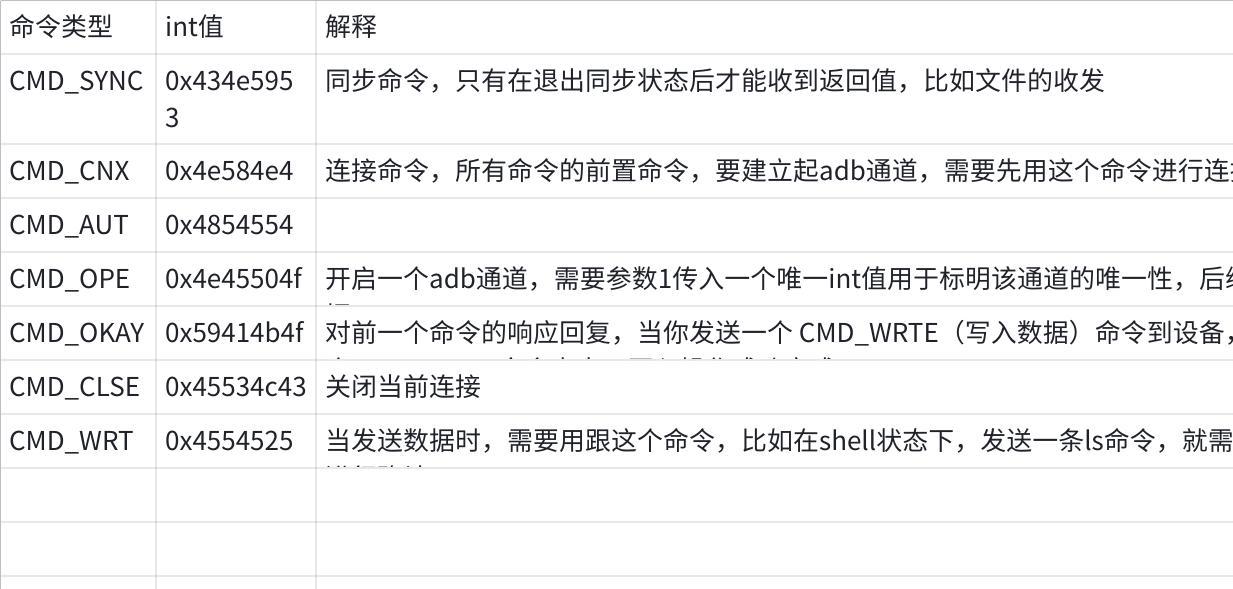
命令类型：见后续

参数1：具体命令值不一样

参数2：具体命令值不一样

数据校验和：只对数据内容进行校验

|  |
| --- |
| Java public static int checksum(byte[] payload){  int checksum = 0;  for (byte b : payload){  if (b >= 0)  checksum += b;  else  checksum += b+256;  }  return checksum;  } |



**点击图片可查看完整电子表格**

**命令举例**

**建立连接的数据包**



**点击图片可查看完整电子表格**

连接授权

所有的一次性命令都可以通过CMD\_OPEN命令来实现

**adb root**



**点击图片可查看完整电子表格**

**adb tcpip 5555**



**点击图片可查看完整电子表格**

**adb shell ifconfig**



**点击图片可查看完整电子表格**

**adb shell disable-verify 1000**

有些设备需要密码验证，不然adb shell会提示输入密码，需要关闭验证。

此时就无法发送shell:disable-verify 1000来完成了，需要使用row来指定命令。当然其它的命令也可以通过row来指定。



**点击图片可查看完整电子表格**

**adb shell**



**点击图片可查看完整电子表格**

**在shell状态下发送ls命令**



**点击图片可查看完整电子表格**

**CTRL+C关闭shell**



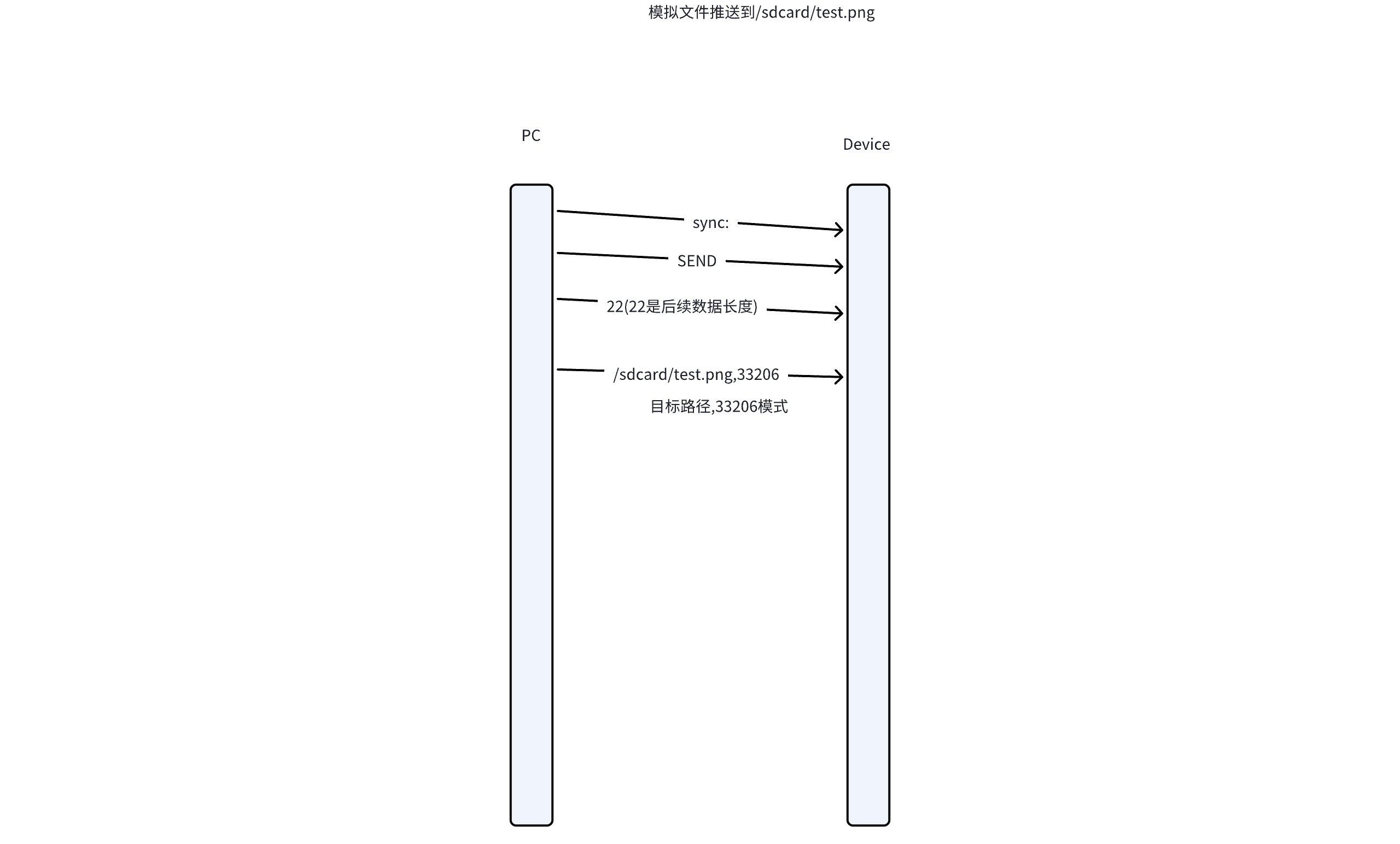
**点击图片可查看完整电子表格**

**adb push xxx xxx**

以sync:的方式打开通道



**点击图片可查看完整电子表格**



**adb pull xxx xxx**

**adb install xxx.apk**

adb install 可以拆分成两个命令：adb push xxx.apk /data/local/tmp/xxx.apk 和 adb shell pm install /data/local/tmp/xxx.apk，将apk推送到/data/local/tmp目录再安装。

**更多adb命令**

当不清楚某个adb命令需要发送什么数据时，可以通过抓包来解决。

开启设备的远程adb能力，通过远程连接到设备，远程adb使用的是tcp协议。最后使用Wireshark等抓包工具进行抓包，就能知道发送和接收的数据了。