# 抓包

抓包根据抓取对象的不同分为两类：一类是通过Android智能移动终端所接入的上层网络设备或线路获取数据流，另一类则是直接在Android移动终端上监听数据流。

Tcpdump抓包属于第二类。

# Android使用tcpdump抓包的大致流程

1. Root权限解锁，本文是直接使用夜神模拟器
2. 相关工具：tcpdump和adb。

tcpdump是Linux系统中普遍使用的一款开源网络协议分析工具，使用方法详参：https://www.cnblogs.com/yc\_sunniwell/archive/2010/07/05/1771563.html

adb是谷歌提供的安卓远程调试工具，应该使用方法详参：https://www.cnblogs.com/xitang/archive/2011/09/03/2165332.html。

1. adb devices 查看当前连接的设备，连接到电脑的android设备或者模拟器将被显示
2. adb shell进入android环境shell
3. 提升要操作文件夹的权限（以/data/local为例），输入chmod 777 /data/local
4. 将本地的Tcpdump复制到android上，adb push d:/tcpdump /data/local
5. 在shell中使用chmod修改tcpdump的权限。Chmod 6755 /data/local/tcpdump
6. 在当前Shell中使用 su 命令获取管理员权限；
7. 在当前Shell中输入命令： /data/local/tcpdump -p -s 0 -w /sdcard/001.pcap；

上述过程中，tcpdump命令的参数含义如下：  
　　# "-p": disable promiscuous mode (不使用混杂模式)  
　　# "-s 0": capture the entire packet（-s参数用以指定数据包捕获长度，此处指定为0，意为抓取完整的数据包）  
　　# "-w \*.pcap": write packets to a file (将结果写入一个pcap文件，而不在终端上直接显示)

1. 在Android手机上进行相关操作，产生通信数据包，通信行为完成后在命令提示符窗口中使用 Ctrl + C 组合键退出当前Shell，以停止抓包。
2. 将抓包结果下载到本地PC上。在命令提示符窗口中使用命令：adb pull /sdcard/001.pcap <LocalPath of PcapFile >，例如：adb pull /sdcard/001.pcap E:\trafficPacket
3. 使用Wireshark等协议分析工具查看抓包结果。

# Adb常用命令介绍

1. 查看设备

    adb devices 这个命令是查看当前连接的设备，连接到电脑的android设备或者模拟器将被显示

2. 安装软件

    adb install <apk文件路径> 这个命令将指定的apk文件安装到设备上。

3. 卸载软件

    adb uninstall <软件名> 或者 adb uninstall –k <软件名> 如果加参数-k参数，为卸载软件但是保留配置和缓存文件。

4. 登录设备shell

   adb shell 或者 adb shell <command命令> 这个命令将登陆设备的shell。 后面加<command命令>将是直接运行设备命令，相当于执行远程命令。

5. 从电脑上发生文件到设备

   adb push <本地路径> <远程路径> 用push命令可以把本机电脑上的文件或者文件夹复制到设备上。

6. 从设备上下载文件到电脑

    adb pull <远程路径> <本地路径> 用pull命令可以把设备上的文件或者文件夹复制到本机电脑。

# Tcpdump详细介绍

**[tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html)采用命令行方式，它的命令格式为：  
    　　[tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html) [ -adeflnNOpqStvx ] [ -c 数量 ] [ -F 文件名 ]  
　　　　　　　　　　[ -i 网络接口 ] [ -r 文件名] [ -s snaplen ]  
　　　　　　　　　　[ -T 类型 ] [ -w 文件名 ] [表达式 ]**

(1)[tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html)的选项介绍

     -a 　　　将网络地址和广播地址转变成名字；  
　　　-d 　　　将匹配信息包的代码以人们能够理解的汇编格式给出；  
　　　-dd 　　 将匹配信息包的代码以c语言程序段的格式给出；  
　　　-ddd 　　将匹配信息包的代码以十进制的形式给出；  
　　　-e 　　　在输出行打印出数据链路层的头部信息；  
　　　-f 　　　将外部的Internet地址以数字的形式打印出来；  
　　　-l 　　　使标准输出变为缓冲行形式；  
　　　-n 　　　不把网络地址转换成名字；  
　　　-t 　　　在输出的每一行不打印时间戳；  
　　　-v 　　　输出一个稍微详细的信息，例如在ip包中可以包括ttl和服务类型的信息；  
　　　-vv 　　 输出详细的报文信息；  
　　　-c 　　　在收到指定的包的数目后，[tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html)就会停止；  
　　　-F 　　　从指定的文件中读取表达式,忽略其它的表达式；  
　　　-i 　　　指定监听的网络接口；  
　　　-r 　　　从指定的文件中读取包(这些包一般通过-w选项产生)；  
　　　-w 　　　直接将包写入文件中，并不分析和打印出来；  
　　　-T 　　　将监听到的包直接解释为指定的类型的报文，常见的类型有rpc （远程过程调用）和snmp（简单网络管理协议；）

(2). [tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html)的表达式介绍

<http://anheng.com.cn/news/24/586.html>    表达式是一个正则表达式，[tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html)利用它作为过滤报文的条件，如果一个报文满足表达式的条件，则这个报文将会被捕获。如果没有给出任何条件，则网络上所有的信息包将会被截获。在表达式中一般如下几种类型的关键字。

    第一种是**关于类型的关键字**，主要包括host，net，port, 例如 host 210.27.48.2，指明210.27.48.2是一台主机，net 202.0.0.0 指明 202.0.0.0是一个网络地址，port 23指明端口号是23。如果没有指定类型，缺省的类型是host.<http://anheng.com.cn/news/24/586.html>

    第二种是**确定传输方向的关键字**，主要包括src , dst ,dst or src, dst and src,这些关键字指明了传输的方向。举例说明，src 210.27.48.2 ,指明ip包中源地址是210.27.48.2 , dst net202.0.0.0 指明目的网络地址是202.0.0.0 。如果没有指明方向关键字，则缺省是src or dst关键字。

<http://anheng.com.cn/news/24/586.html>    第三种是**协议的关键字**，主要包括fddi,ip,arp,rarp,tcp,udp等类型。Fddi指明是在FDDI(分布式光纤数据接口网络)上的特定的网络协议，实际上它是"ether"的别名，fddi和ether具有类似的源地址和目的地址，所以可以将fddi协议包当作ether的包进行处理和分析。其他的几个关键字就是指明了监听的包的协议内容。如果没有指定任何协议，则[tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html)将会监听所有协议的信息包。

     除了这三种类型的关键字之外，其他重要的关键字如下：gateway,broadcast,less,greater,还有三种逻辑运算，取非运算是 'not ' '! ',与运算是'and','&&';或运算 是'or','││'；这些关键字可以组合起来构成强大的组合条件来满足人们的需要，下面举几个例子来说明。

      A想要截获所有210.27.48.1 的主机收到的和发出的所有的数据包：

　　#tcpdump host 210.27.48.1

　　B想要截获主机210.27.48.1 和主机210.27.48.2 或210.27.48.3的通信，使用命令：(在命令行中使用括号时，一定要添加'\')

　　#tcpdump host 210.27.48.1 and \ (210.27.48.2 or 210.27.48.3 \)

　　C如果想要获取主机210.27.48.1除了和主机210.27.48.2之外所有主机通信的ip包，使用命令：

　　#tcpdump ip host 210.27.48.1 and ! 210.27.48.2

　　D如果想要获取主机210.27.48.1接收或发出的telnet包，使用如下命令：

　　#tcpdump tcp port 23 host 210.27.48.1

　　E 对本机的udp 123 端口进行监视 123 为ntp的服务端口

　　# tcpdump udp port 123

　　F 系统将只对名为hostname的主机的通信数据包进行监视。主机名可以是本地主机，也可以是网络上的任何一台计算机。下面的命令可以读取主机hostname发送的所有数据：

　　#tcpdump -i eth0 src host hostname

　　G 下面的命令可以监视所有送到主机hostname的数据包：

　　#tcpdump -i eth0 dst host hostname

　　H 我们还可以监视通过指定网关的数据包：

　　#tcpdump -i eth0 gateway Gatewayname

　　I 如果你还想监视编址到指定端口的TCP或UDP数据包，那么执行以下命令：

　　#tcpdump -i eth0 host hostname and port 80

　　J 如果想要获取主机210.27.48.1除了和主机210.27.48.2之外所有主机通信的ip包，使用命令：

　　#tcpdump ip host 210.27.48.1 and ! 210.27.48.2

　　K 想要截获主机210.27.48.1 和主机210.27.48.2 或210.27.48.3的通信，使用命令：

　　#tcpdump host 210.27.48.1 and \ (210.27.48.2 or 210.27.48.3 \)

　　L 如果想要获取主机210.27.48.1除了和主机210.27.48.2之外所有主机通信的ip包，使用命令：

　　#tcpdump ip host 210.27.48.1 and ! 210.27.48.2

　　M 如果想要获取主机210.27.48.1接收或发出的telnet包，使用如下命令：

　　#tcpdump tcp port 23 host 210.27.48.1

(3). [tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html)的输出结果介绍

<http://anheng.com.cn/news/24/586.html>    下面我们介绍几种典型的[tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html)命令的输出信息

A,**数据链路层头信息**  
使用命令: #[tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html) --e host ice  
     ice 是一台装有[linux](http://linux.anheng.com.cn/news/24/586.html)的主机，她的MAC地址是0：90：27：58：AF：1A  
     H219是一台装有SOLARIC的SUN工作站，它的MAC地址是8：0：20：79：5B：46；上一条命令的输出结果如下所示：  
21:50:12.847509 eth0 < 8:0:20:79:5b:46 0:90:27:58:af:1a ip 60: h219.33357 > ice.telne  
t 0:0(0) ack 22535 win 8760 (DF)

    分析：21：50：12是显示的时间， 847509是ID号，eth0 <表示从网络接口eth0 接受该数据包，eth0>表示从网络接口设备发送数据包, 8:0:20:79:5b:46是主机H219的MAC地址,它表明是从源地址H219发来的数据包.0:90:27:58:af:1a是主机ICE的MAC地址,表示该数据包的目的地址是ICE . ip 是表明该数据包是IP数据包,60是数据包的长度, h219.33357 > ice.telnet表明该数据包是从主机H219的33357端口发往主机ICE的TELNET(23)端口. ack 22535表明对序列号是222535的包进行响应. win 8760表明发送窗口的大小是8760.

B,**ARP包的TCPDUMP输出信息**

使用命令:#[tcpdump](http://tcpdump.anheng.com.cn/news/24/586.html) arp

得到的输出结果是：  
22:32:42.802509 eth0 > arp who-has route tell ice (0:90:27:58:af:1a)  
22:32:42.802902 eth0 < arp reply route is-at 0:90:27:12:10:66 (0:90:27:58:af:1a)  
分析: 22:32:42是时间戳, 802509是ID号, eth0 >表明从主机发出该数据包, arp表明是ARP请求包,who-has route tell ice表明是主机ICE请求主机ROUTE的MAC地址。0:90:27:58:af:1a是主机ICE的MAC地址。

C,**TCP包的输出信息**

用TCPDUMP捕获的TCP包的一般输出信息是：

src > dst: flags data-seqno ack window urgent options  
src> dst:表明从源地址到目的地址, flags是TCP包中的标志信息,S 是SYN标志, F (FIN), P (PUSH) , R(RST) "." (没有标记); data-seqno是数据包中的数据的顺序号, ack是下次期望的顺序号,window是接收缓存的窗口大小, urgent表明数据包中是否有紧急指针. Options是选项.

D,**UDP包的输出信息**

    用TCPDUMP捕获的UDP包的一般输出信息是：

route.port1 > ice.port2: udp lenth  
UDP十分简单，上面的输出行表明从主机ROUTE的port1端口发出的一个UDP数据包到主机ICE的port2端口，类型是UDP， 包的长度是lenth

3. 辅助工具

(1) 想查看TCP或者UDP端口使用情况，使用 netstat -anp  
     如果有些进程看不见，如只显示”-”，可以尝试  
sudo netstat -anp  
     如果想看某个端口的信息，使用lsof命令，如：  
sudo lsof -i :631

-bash-3.00# netstat -tln

     netstat -tln 命令是用来查看linux的端口使用情况

/etc/init.d/vsftp start 是用来启动ftp端口~！

    看文件/etc/services

netstat

    查看已经连接的服务端口（ESTABLISHED）

netstat -a

    查看所有的服务端口（LISTEN，ESTABLISHED）

sudo netstat -ap

    查看所有 的服务端口并显示对应的服务程序名

nmap ＜扫描类型＞＜扫描参数＞

例如：

nmap localhost

nmap -p 1024-65535 localhost

nmap -PT 192.168.1.127-245

     当我们使用　netstat -apn　查看网络连接的时候，会发现很多类似下面的内容：

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 52 218.104.81.152：7710 211.100.39.250：29488 ESTABLISHED 6111/1

     显示这台服务器开放了7710端口，那么 这个端口属于哪个程序呢？我们可以使用　lsof -i ：7710　命令来查询：

COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME

sshd 1990 root 3u IPv4 4836 TCP \*：7710 （LISTEN）

     这样，我们就知道了7710端口是属于sshd程序的。

(2) 运行tcpdump命令出现错误信息排除

tcpdump: no suitable device found  
tcpdump: no devices found /dev/bpf4: A file or directory in the path name does not exist.  
解决方案 2种原因：  
1.权限不够，一般不经过处理，只用root用户能使用tcpdump  
2.缺省只能同时使用4个tcpdump，如用完，则报此类错。需要停掉多余的tcpdump

参考资料：<https://www.cnblogs.com/yc_sunniwell/archive/2010/07/05/1771563.html>