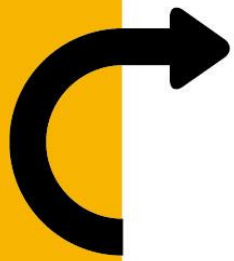
移动端安全测试工具介绍

（PDF测试岗位课程）



第一部分 移动端安全测试工具介绍

第二部分 反编译工具基本使用

第三部分 Drozer工具基本使用

第四部分 Wireshark工具基本使用

第五部分 其他调试和查看工具使用介绍

移动端安全测试工具集

移动端的安全测试工具也非常多，归纳起来可以分为下图列表的几个方面，同时也包含其比较有代表性的工具和适用系统：

类型	名称	适用系统
网络分析工具	burpsuite	Android、IOS
	Fiddler	
	wireshark	
反编译工具	apktool	Android
	dex2jar	Android
	IDA	IOS
	otool	IOS
签名工具	keytool/jarsigner	Android
	signapk	Android
权限分析工具	manitree	Android
动态分析工具	DroidBox	Android
	DDMS	Android
静态分析工具	APKInspector	Android
	otertool	Android
	ApkAnalyser	Android
安全审计集成工具	drozer	Android
	mercury	Android
	iAuditor	IOS
其他工具	SDB	Android

移动端安全测试工具集

基于移动端的在安全测试领域的现状，我们主要关注点是放在Android系统上，从安全测试的角度，选取了部分工具作为介绍，其中反编译工具Dex2jar、jd-gui、安全审计工具Drozer，网络抓包工具Wireshark（BurpSuite等通用，不做介绍），以及其他工具DDMS、SDB等 。

第一部分 移动端安全测试工具介绍

第二部分 反编译工具基本使用

第三部分 Drozer工具基本使用

第四部分 Wireshark工具基本使用

第五部分 其他调试和查看工具使用介绍

反编译

Android apk反编译即通过apk文件进行逆向工程，获取原始的数据资源。

工具主要有：
apktool ：资源文件获取，可以提取出图片文件和布局文件进行使用查看
Dex2jar：将apk反编译成Java源码（classes.dex转化成jar文件）
jd-gui：查看APK中classes.dex转化成出的jar文件，即源码文件

安全测试主要是查看源码，故我们重点讲解下Dex2jar、 jd-gui对apk文件的反编译过程。

Dex2jar

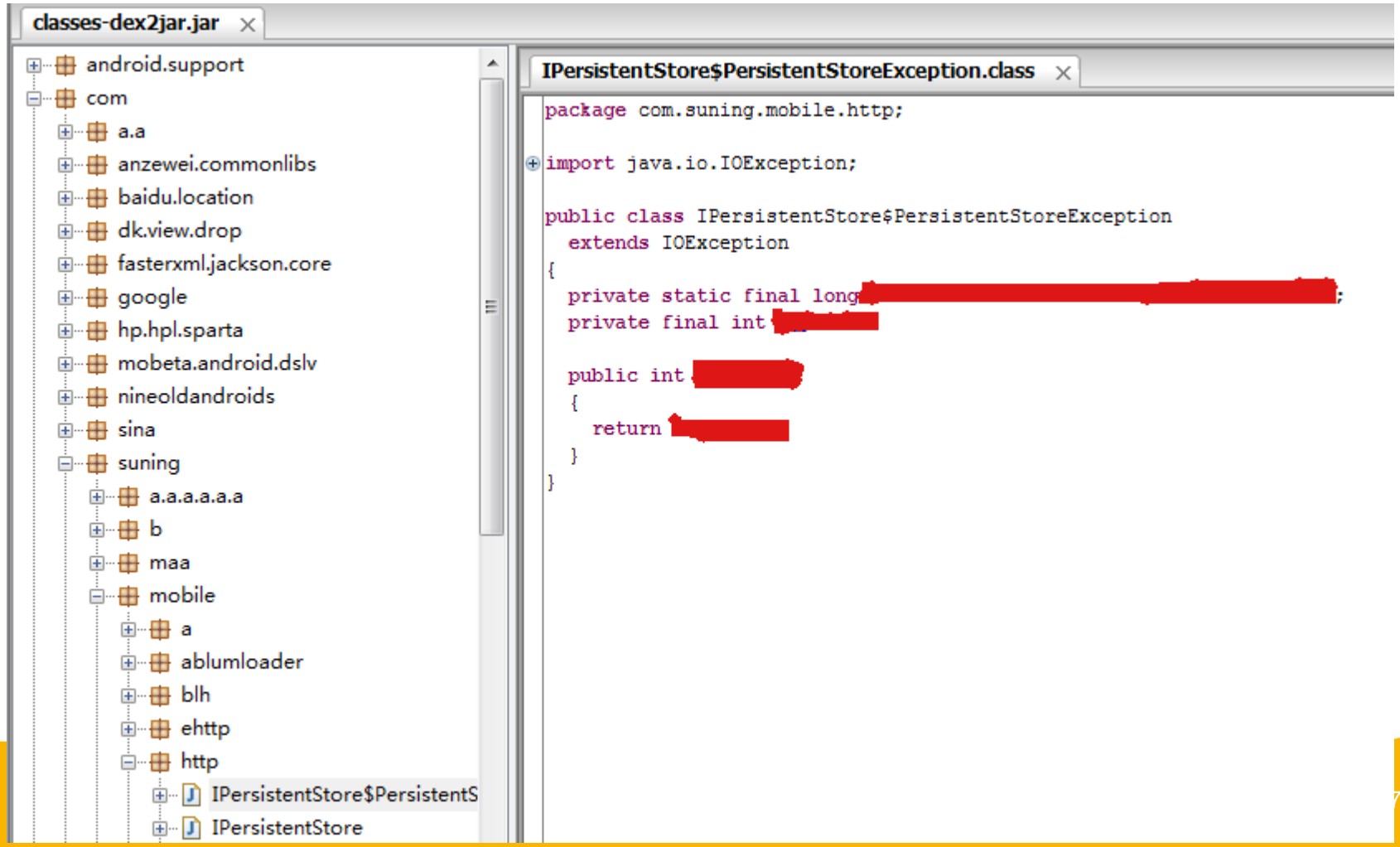
将要反编译的APK后缀名改为.rar，并解压，得到其中的classes.dex文件（它就是java文件编译再通过dx工具打包而成的），将获取到的classes.dex放到工具dex2jar目录下，在命令行下执行命令d2j-dex2jar.bat classes.dex --force，效果如下：

```
F:\Tools>cd decompilation\app tools\dex2jar-0.0.9.15

F:\Tools\decompilation\app tools\dex2jar-0.0.9.15>d2j-dex2jar.bat classes.dex --
force
dex2jar classes.dex -> classes-dex2jar.jar

F:\Tools\decompilation\app tools\dex2jar-0.0.9.15>
```

表示已反编译成功。

jd-gui

直接通过jd-gui打开反编译后的文件，即可查看到源代码：



第一部分 移动端安全测试工具介绍

第二部分 反编译工具基本使用

第三部分 Drozer工具基本使用

第四部分 Wireshark工具基本使用

第五部分 其他调试和查看工具使用介绍

Drozer工具介绍

Drozer是Android下的开源app安全审计框架。Drozer可以通过与Dalivik VM,其它应用程序的IPC端点以及底层操作系统的交互，避免正处于开发阶段，或者部署于你的组织的android应用程序和设备暴露出不可接受的安全风险。drozer提供了很多Android平台下的渗透测试exploit供测试和修复。

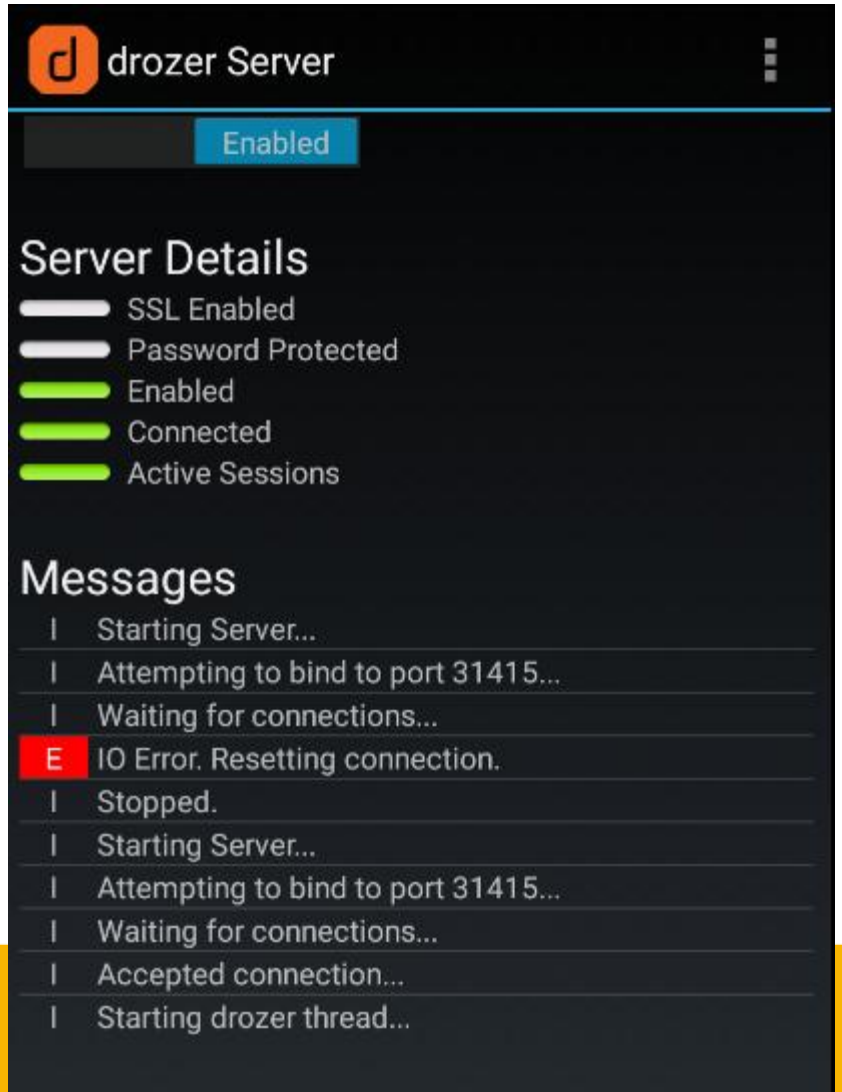
下载地址：https://labs.mwrinfosecurity.com/tools/drozer/

需同时下载drozer攻击端和drozer服务端 (即Agent .apk only)
一般drozer攻击端安装在电脑上
Drozer服务端安装在被测的app所在的安卓手机或模拟器上

Drozer使用介绍

1. 测试准备

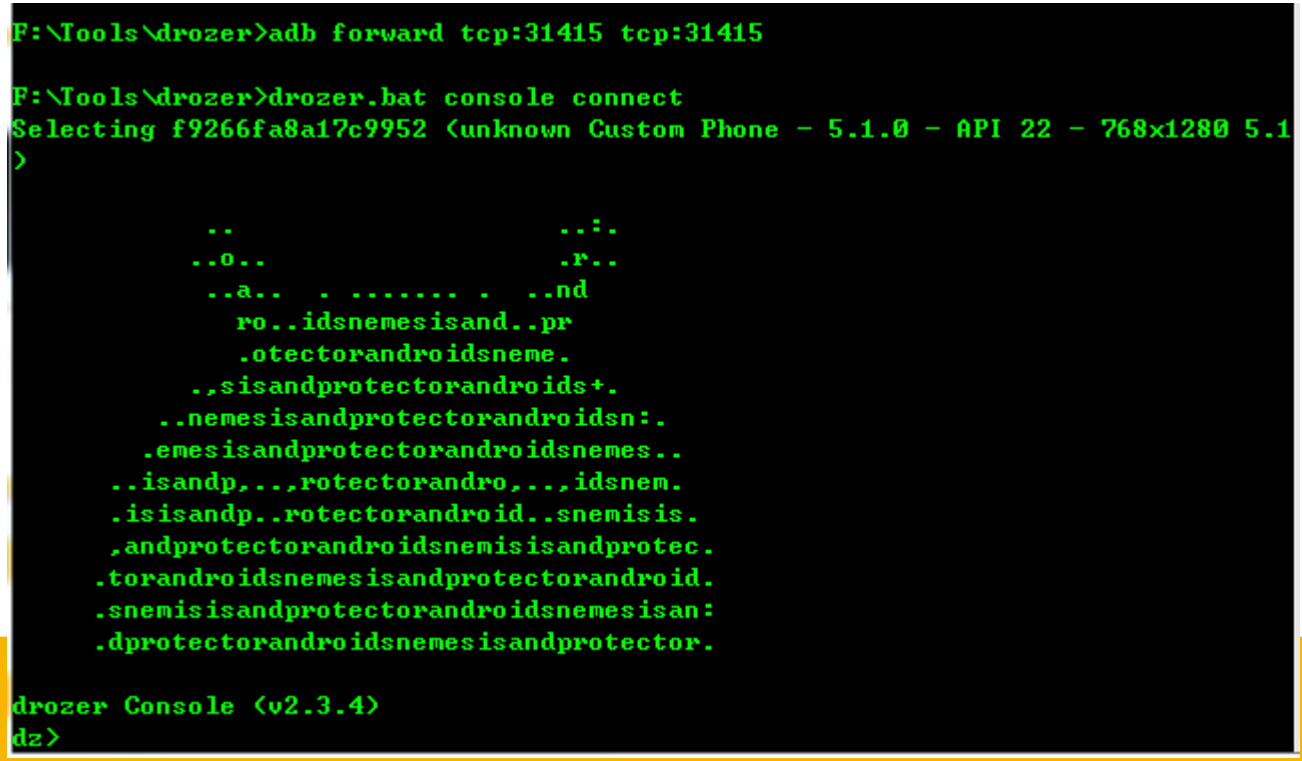
①首先在被测移动端上打开Drozer Server，并将其置于开启状态，如图所示：



Drozer使用介绍

②配置adb工具并加入环境变量，执行命令adb forward tcp:31415 tcp:31415，打开端口监听

③进入adb安装目录，执行命令drozer.bat console connect，当出现以下信息时代表drozer启动成功：



Drozer使用介绍

2. 查看可攻击的风险点

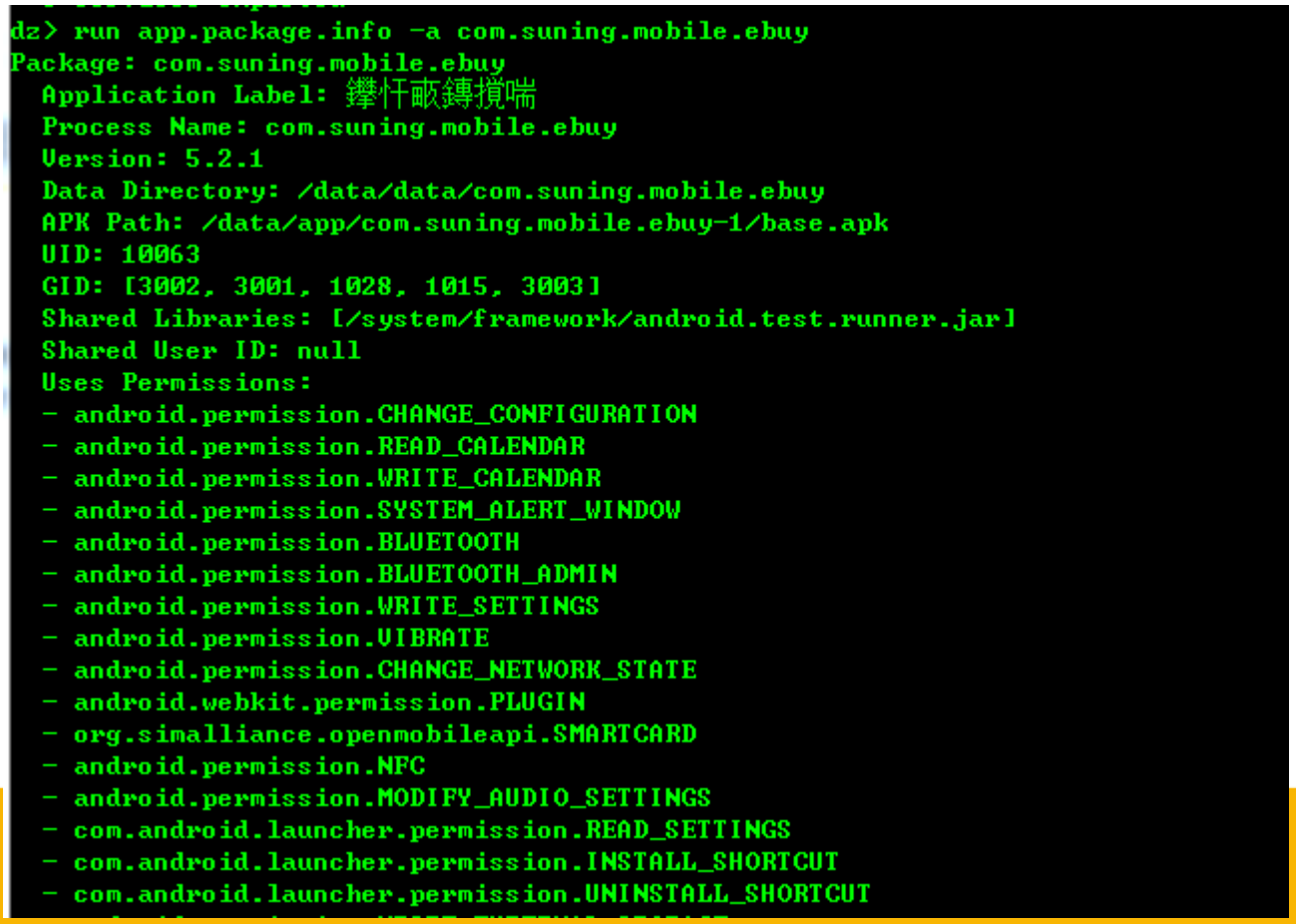
①查看Attack surfaces：
格式：run app.package.attacksurface app名
例：run app.package.attacksurface com.suning.mobile.ebuy

```
dz> run app.package.attacksurface com.suning.mobile.ebuy
Attack Surface:
  6 activities exported
  6 broadcast receivers exported
  0 content providers exported
  6 services exported
dz>
```

6 activities exported表示可能存在6个activities相关的安全风险；
6 broadcast receivers exported表示可能存在6个receivers相关的安全风险；
0 content providers exported表示不存在content相关的安全风险；
6 services exported表示可能存在6个services相关的安全风险。

Drozer使用介绍

②获取app的信息：
格式： run app.package.info -a app名
例： run app.package.info -a com.suning.mobile.ebuy



Drozer使用介绍

3. Intent组件测试

①查看暴露的广播组件信息：
格式： run app.broadcast.info -a app名
例： run app.broadcast.info -a com.suning.mobile.ebuy

```
dz> run app.broadcast.info -a com.suning.mobile.ebuy
Package: com.suning.mobile.ebuy
  com.suning.mobile.ebuy.base.host.push.ui.NetChangeReceiver
    Permission: null
  com.suning.mobile.ebuy.base.host.pushmessage.PushReceiver
    Permission: null
  com.suning.cloud.push.pushservice.MiMessageReceiver
    Permission: null
  com.xiaomi.push.service.receivers.NetworkStatusReceiver
    Permission: null
  com.taobao.accs.EventReceiver
    Permission: null
  com.taobao.agoo.AgooCommondReceiver
    Permission: null

dz>
```

Drozer使用介绍

②拒绝服务攻击测试
a，发送空action
格式：run app.broadcast.send --action app名 receiver名
例：run app.broadcast.send --action com.suning.mobile.ebuy com.suning.mobile.ebuy.base.host.pushmessage.PushReceiver
b, 发送空extras
格式：run app.broadcast.send --component app名 receiver名
例：run app.broadcast.send --component com.suning.mobile.ebuy com.suning.mobile.ebuy.base.host.pushmessage.PushReceiver

③提升权限
例： run app.service.start --action com.test.vulnerability.SEND_SMS --extra string dest 11111 --extra string text 1111 --extra string OP SEND_SMS

Drozer使用介绍

4. Provider测试

①查看provider信息：
格式： run app.provider.info –a app名
例： run app.provider.info –a com.suning.mobile.ebuy

②利用drozer查看可能的sqlite注入的uri：
格式： run scanner.provider.injection –a app名
例： run scanner.provider.injection –a com.suning.mobile.ebuy

③尝试简单的注入：
格式： run app.provider.query content:脆弱uri --projection “”
例： run app.provider.query content:
//com.suning.mobile.ebuy/favorites?notify=false --projection “”

第一部分 移动端安全测试工具介绍

第二部分 反编译工具基本使用

第三部分 Drozer工具基本使用

第四部分 Wireshark工具基本使用

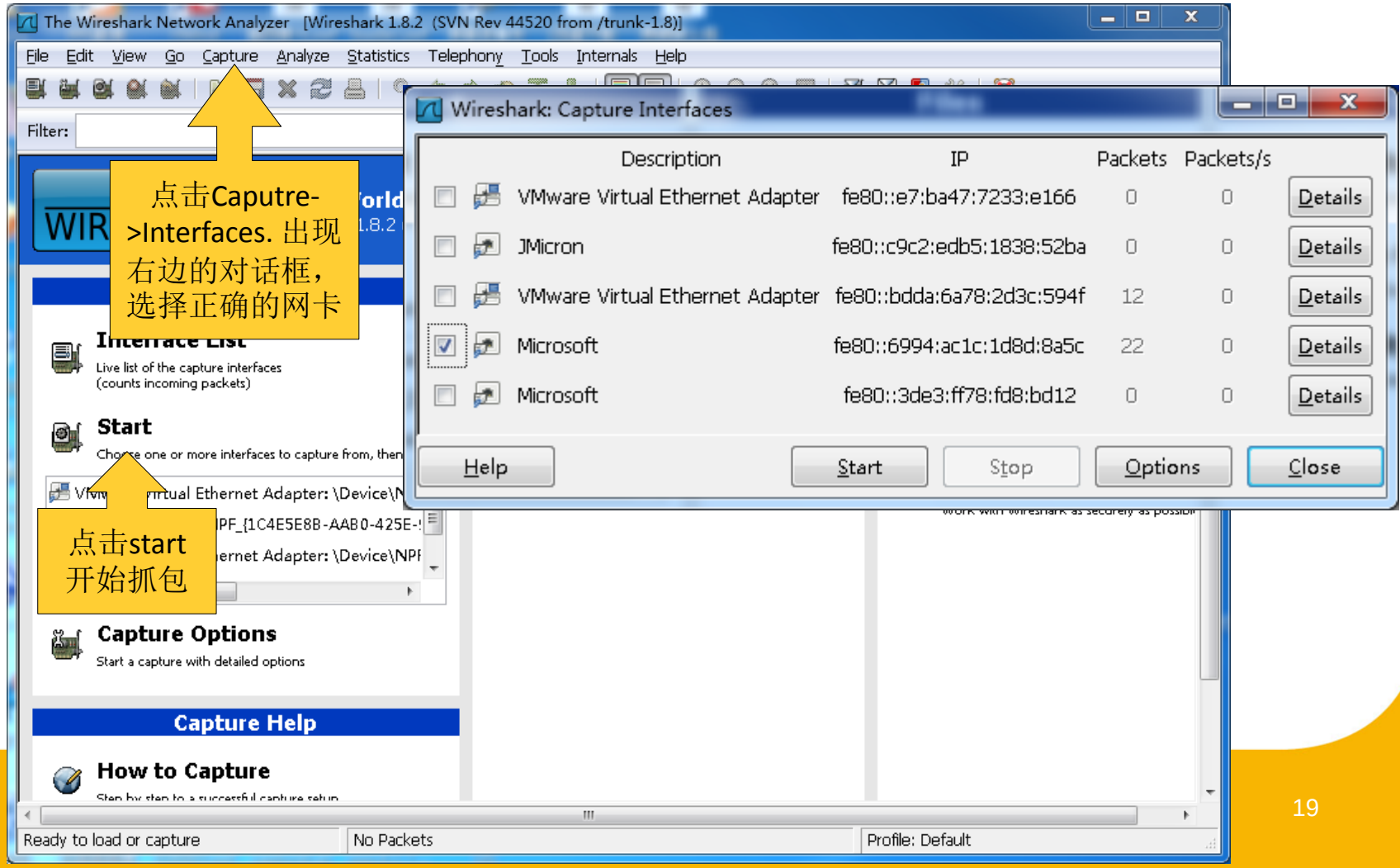
第五部分 其他调试和查看工具使用介绍

wireshark

wireshark是非常流行的网络封包分析软件，功能十分强大。可以截取各种网络封包，显示网络封包的详细信息。使用wireshark时需了解网络协议，否则看不懂wireshark。为了安全考虑，wireshark只能查看封包，而不能修改封包的内容，或者发送封包。

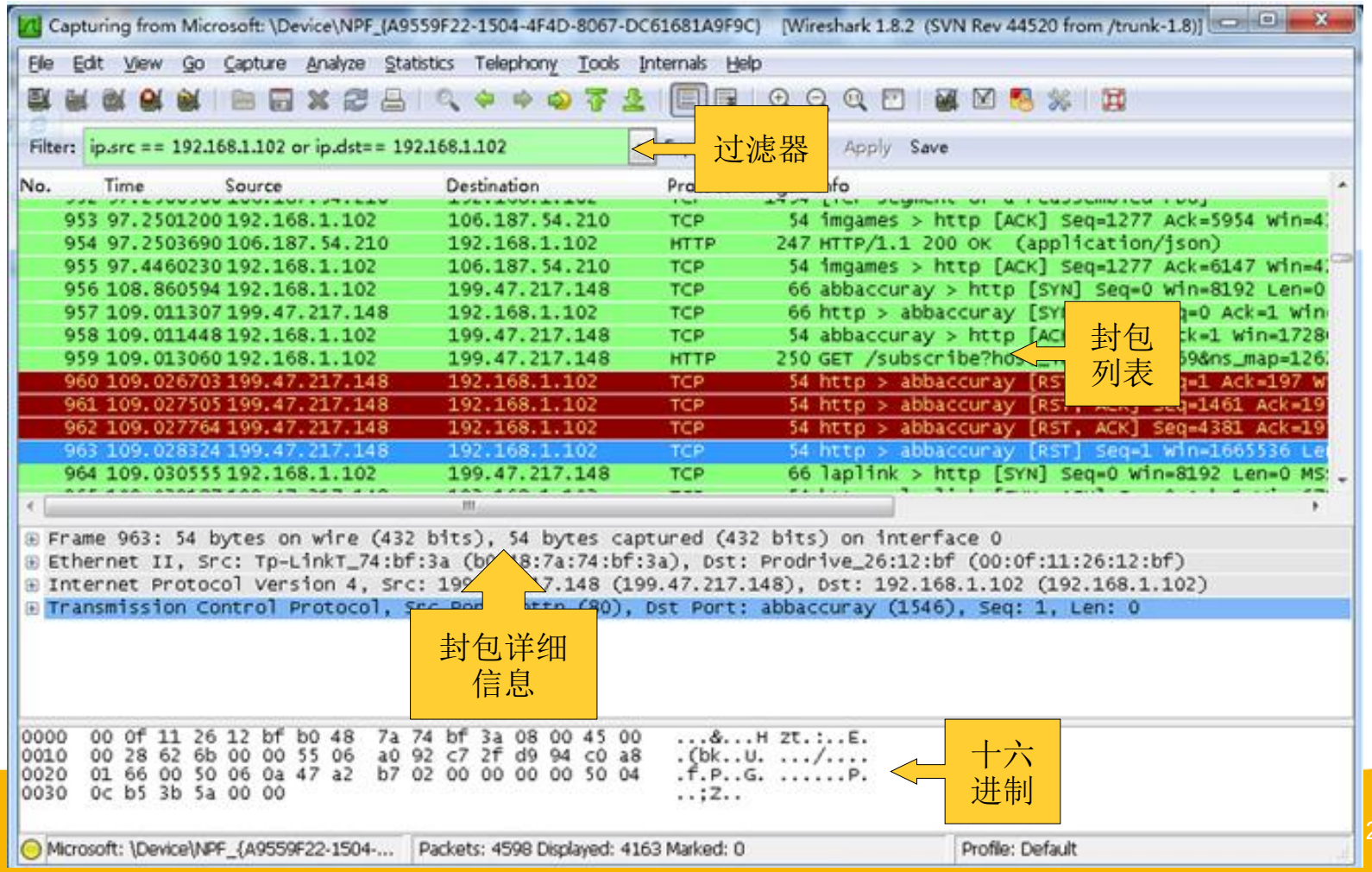
wireshark也能获取HTTP和HTTPS，但不能解密HTTPS，如果是代理或处置HTTP，HTTPS协议的数据包建议还是用Burpsuite、Fiddler等工具，而TCP，UDP协议的可用wireshark。移动端的APP很多情况与服务器进行交互时采用的是TCP/IP协议进行传输，此时wireshark就能派上用场了！

1. 抓包操作


The Wireshark Network Analyzer [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
点击Caputre->Interfaces. 出现右边的对话框，选择正确的网卡
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
点击start开始抓包
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Ready to load or capture
No Packets
Profile: Default
Wireshark: Capture Interfaces
Description
IP
Packets
Packets/s
VMware Virtual Ethernet Adapter fe80::e7:ba47:7233:e166 0 0 Details
JMicron fe80::c9c2:edb5:1838:52ba 0 0 Details
VMware Virtual Ethernet Adapter fe80::bdda:6a78:2d3c:594f 12 0 Details
Microsoft fe80::6994:ac1c:1d8d:8a5c 22 0 Details
Microsoft fe80::3de3:ff78:fd8:bd12 0 0 Details
Help
Start
Stop
Options
Close

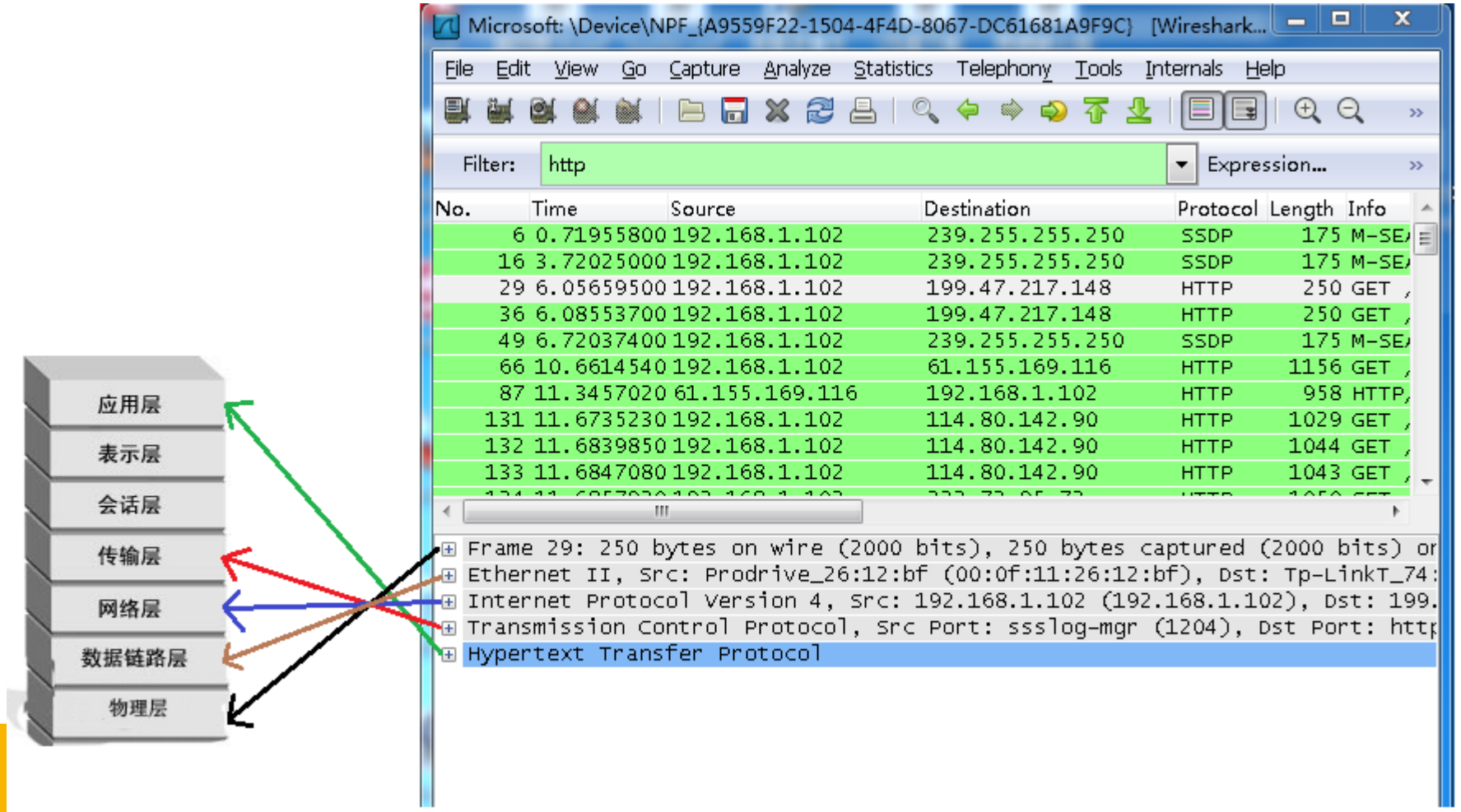
wireshark

2. 抓包窗口



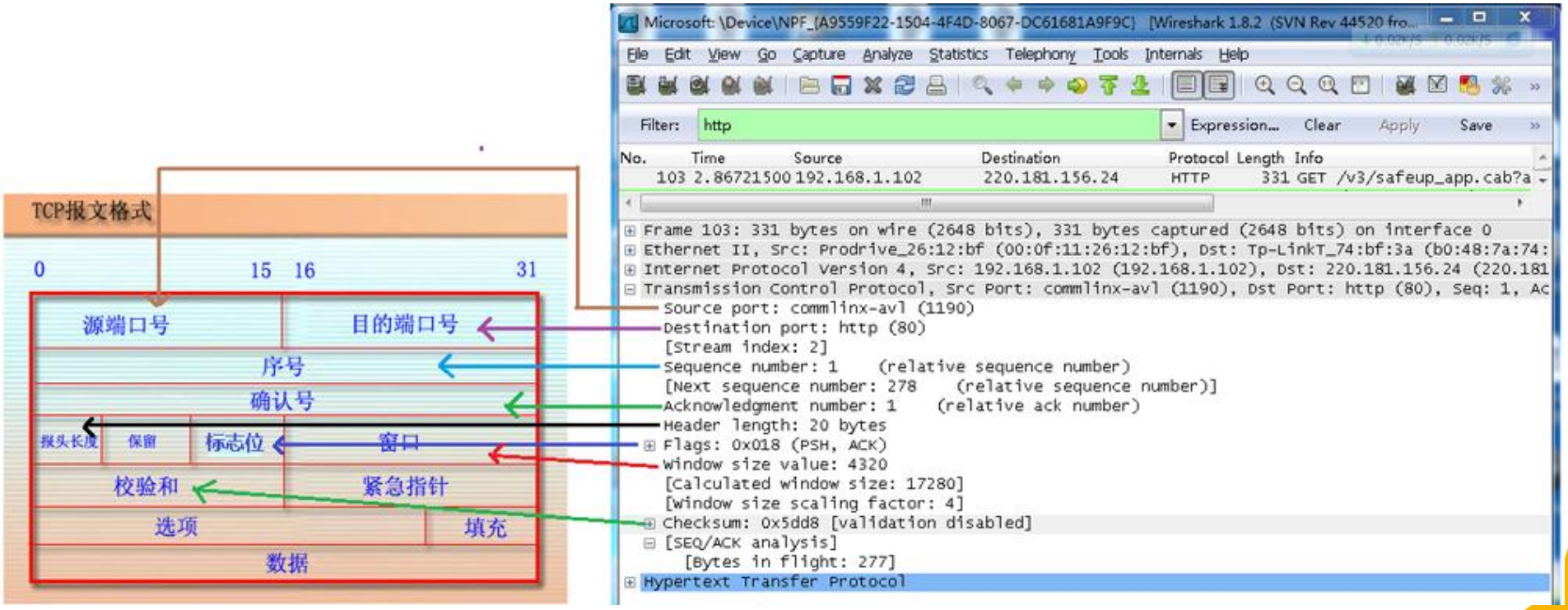
wireshark

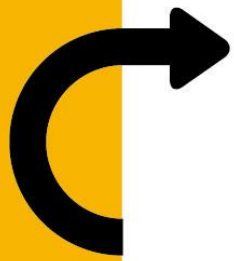
3. Wireshark与OSI七层网络模型关系：



wireshark

4. 封包中的每个字段结构：





第一部分 移动端安全测试工具介绍

第二部分 反编译工具基本使用

第三部分 Drozer工具基本使用

第四部分 Wireshark工具基本使用

第五部分 其他调试和查看工具使用介绍

其他实用工具

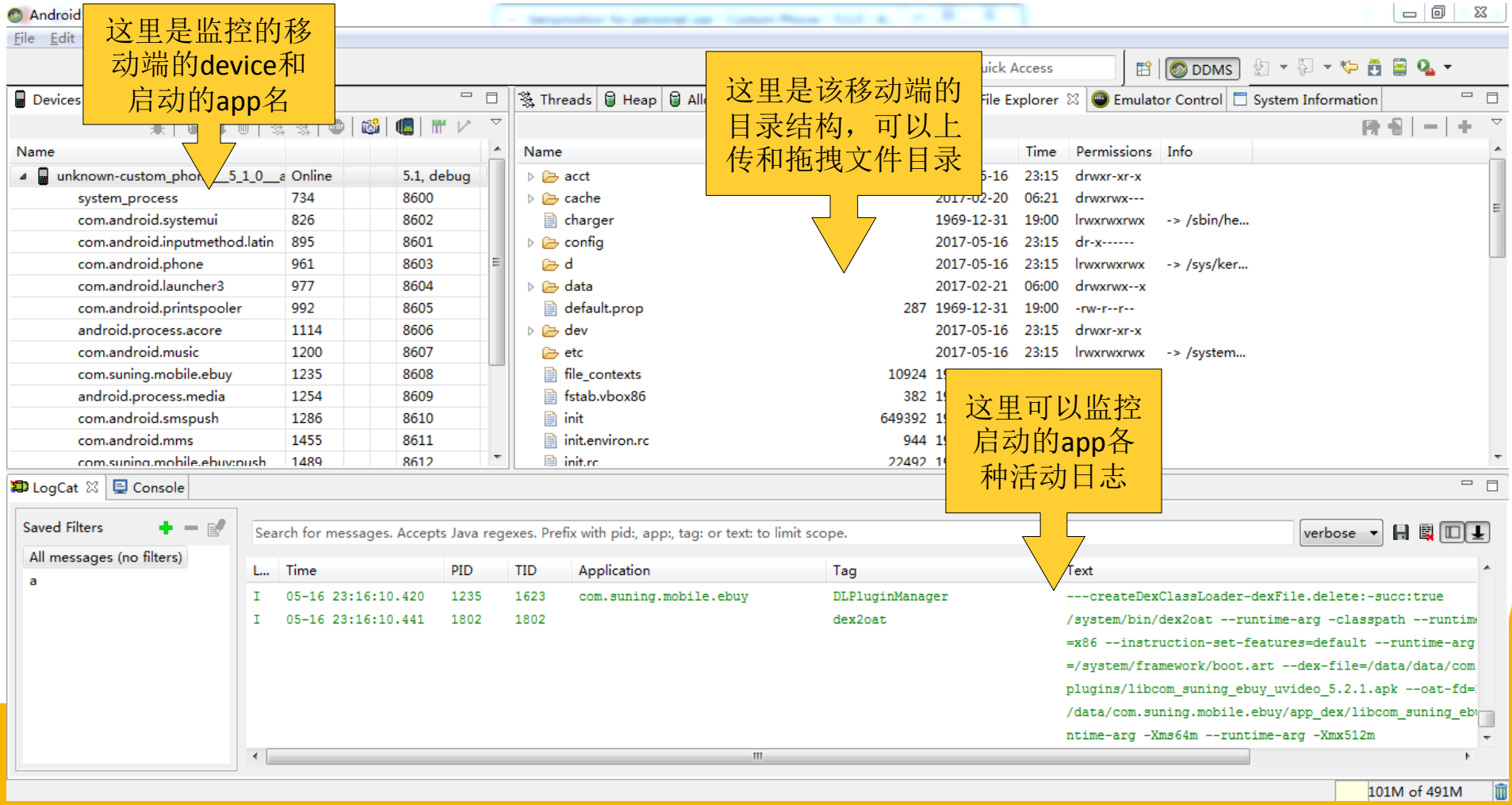
除了上诉工具外，其他比较实用的工具有：DDMS、SDB

DDMS的全称是Dalvik Debug Monitor Service，是Android开发环境中的Dalvik虚拟机调试监控服务。在ADT集成开发环境中自带的工具箱里，一般启动批处理文件monitor.bat可以打开DDMS。

SDB的全称是SQLite Database Browser，是一个手机存储数据库格式的文件查看器，可以直接下载后使用，无需安装。

DDMS

1. DDMS界面简介



DDMS

2. SDB界面简介

SQLite Database Browser - E:/box/ttt/app_webview/Cookies

File Edit View Help

Database Structure | Browse Data

选择表名

Table: cookies

New Record | Delete Record

字段内容

	creation_utc	host_key	name	value	path	expires_utc	secure	httponly	last_access_u	has_expires	persistent	priority	encrypted_va
1	3139303893665476	passportpre.cnsu	ids_r_me	NjExNDU3MDU4OV9B	/			0	3139304208570977	0	0	1	
2	3139303893665847	passportpre.cnsu	TGC	TGTCA6113F7A149B	/ids/			0	3139304208570977	0	0	1	
3	3139303893666020	.cnsuning.com	custno	6114570589	/			0	3139304163817257	0	0	1	
4	3139303893668223	passportpre.cnsu	_device_session_	"242678515020149	/ids	0	0	0	3139304208570977	0	0	1	
5	3139303894732767	.cnsuning.com	authId	si6BDAAE6570D17B	/	0	0	1	3139304163817257	0	0	1	
6	3139303894732870	.cnsuning.com	secureToken	591D96E376A60AE5	/	0	1	1	3139304165720762	0	0	1	
7	3139303900113724	shoppingpre.cnsu	_device_session_	"242678515020149	/app/cart1/gatew	0	0	0	3139303900113724	0	0	1	
8	3139303901283312	.cnsuning.com	mtisAbTest	B	/	0	0	0	3139304163817257	0	0	1	
9	3139303901397208	.cnsuning.com	mtisCartQty	0	/	0	0	0	3139304163817257	0	0	1	
10	3139303996851364	vfastpre.cnsunin	JSESSIONID	QbHF1In94MGFvvP2	/vfast-web	0	0	0	3139303996851364	0	0	1	
11	3139304002842444	.suning.com	_snmc	1	/	3139305802000000	0	0	3139304096120520	1	1	1	
12	3139304002844604	.suning.com	_snsr	direct%7Cdirect%	/	3139390402000000	0	0	3139304096120520	1	1	1	
13	3139304002845736	.suning.com	_snma	1%7C149483040283	/	3202376002000000	0	0	3139304096120520	1	1	1	
14	3139304002856048	.suning.com	_snmp	9483040283168245	/	0	0	0	3139304096120520	0	0	1	
15	3139304002856859	.suning.com	_snmb	1494830402846187	/	0	0	0	3139304096120520	0	0	1	
16	3139304002891039	.suning.com	__ssar	direct%7Cdirect%	/	3139390402000000	0	0	3139304096120520	1	1	1	
17	3139304002893393	.suning.com	__ssav	1494830402839636	/	3202376002000000	0	0	3139304096120520	1	1	1	
18	3139304002906378	.suning.com	__ssas	1494830402896314	/	3139305802000000	0	0	3139304096120520	1	1	1	
19	3139304007488718	orderpre.cnsunin	JSESSIONID	QhmpP7dRmGrr5OAJ	/mobile/v1/onlin	0	0	0	3139304203412100	0	0	1	
20	3139304007711010	mypre.cnsuning.c	JSESSIONID	cmIqgCHTmKal9bZc	/msi-web	0	0	0	3139304007711010	0	0	1	
21	3139304008053912	hqpre.cnsuning.c	JSESSIONID	1QfC7cpJaxMSY9Yr	/bof	0	0	0	3139304208992746	0	0	1	
22	3139304014410759	rxfpre.cnsuning.	JSESSIONID	WFeXek9k8BabkjCr	/epps-cpf	0	0	0	3139304014410759	0	0	1	
23	3139304015333427	.cnsuning.com	_snsr	direct%7Cdirect%	/	3139390415000000	0	0	3139304163817257	1	1	1	
24	3139304068781695	.cnsuning.com	__ssar	direct%7Cdirect%	/	3139390468000000	0	0	3139304163817257	1	1	1	

1 - 43 of 43

Go to: 0

Thanks!