Android 平台内存取证软件(AMF)

使用说明书

注意：本软件适用于 Windows 系统计算机与 Android 平台手机，Android 手机需获取 root 权限，使用本软件前请确认您需要取证的 Android 手机已经获得 root 权限。

1. 预配置

1.1. 首先，请确认电脑已安装 Microsoft .Net Framework 4.0 或以上版本，Python2.7。

1.2. 请确认计算机中已安装 adb(Android Debug Bridge)或 AndroidSDK(包含 adb).

检测 adb 是否已安装的方法:

运行 cmd.exe,执行命令：

adb

若输出为：

Android Debug Bridge version …

……

…….

则说明 adb 已安装。

1.3. 获得本软件所有文件后，在对 Android 设备进行内存取证之前，请先将 mem_heap 文件导入 Android 设备。具体步骤如下：

运行 cmd.exe 用 cd 命令打开 mem_heap 所在文件路径：

cd 文件路径

将 mem_heap 文件导入 Android 设备：

adb push mem_heap /data/mem_heap

2. 软件使用

2.1. 双击如图 1 中的图标标打开软件

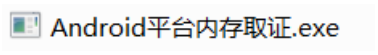

图 1

2.2. 打开软件后，界面如图 2 所示。

2.3. 连接需取证的 Android 设备，单击界面右上方“手机状态”按钮检查设备状态，如图 3 所示。

如果软件提示“无法检测到你的手机！请检查手机状态！”则表明手机未连接，或手机驱动未安装，计算机无法检测到连接的手机。

如果在 root 权限信息中提示：“未获取，您无法使用本软件的其他功能”，则说明该 Android 设备未获取 root 权限，无法正常使用本软件其他功能。

如果在 root 权限信息中提示：“已获取”，则说明本软件已获取 root 权限，其他功能可以正常使用。

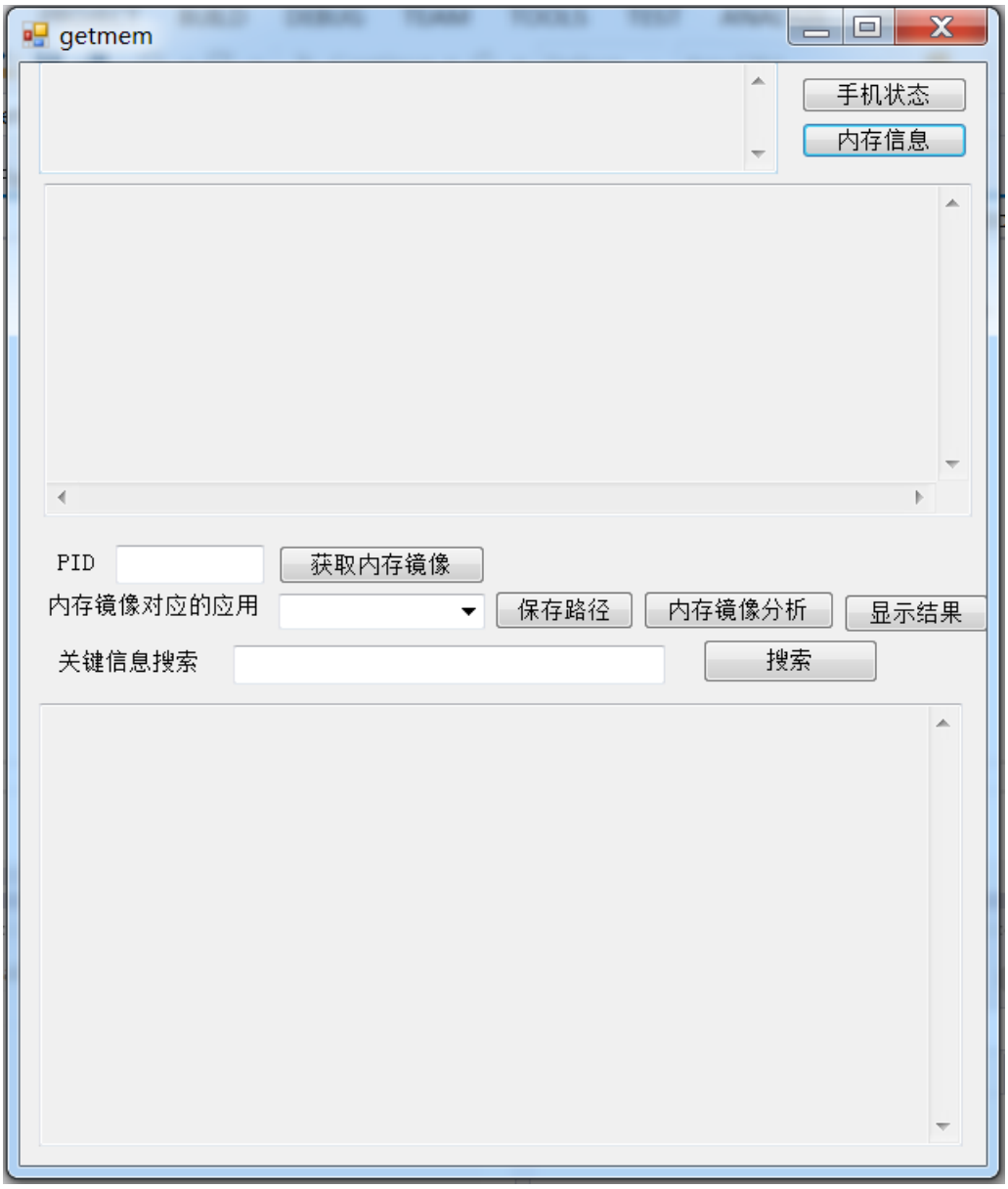

图 2

图 3

除了如下两种决定本软件能否正常使用的关键信息：

- 连接状态

- 手机 root 权限获取状态，

之外，本软件还会显示如下信息：

- 手机型号
- 制造商
- 序列号（在获取 root 权限的情况下可读取）
- Android 系统版本号
- Dalvik VM 可使用堆内存

2.4. 确认已连接手机，且手机获取 root 权限之后，单击界面右上角“手机状态”下的“内存信息”按钮，获取内存中正在运行的进程信息，显示在按钮下方的文本框中，如图 4：

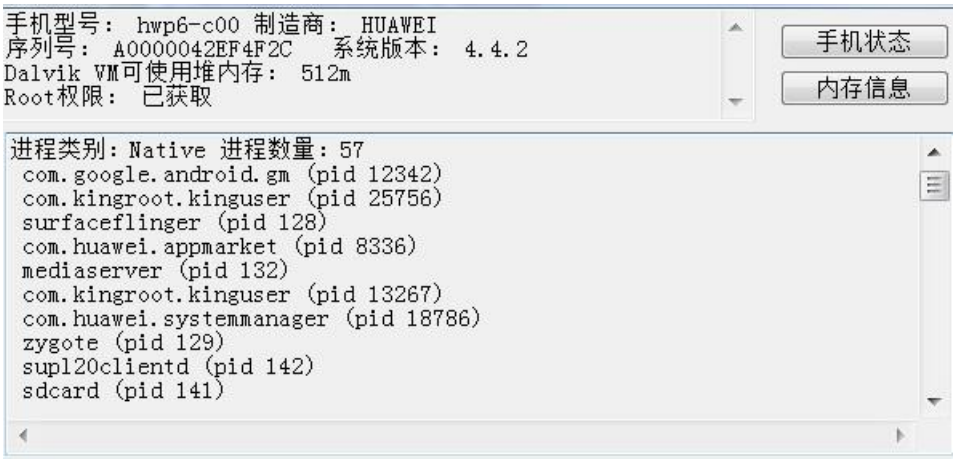

图 4

在内存信息中，我们会将内存中运行的进程按在内存中的优先级分成如下几类，以使用者方便查找：

- Native
- System
- Persistent
- Foreground
- Visible
- Perceptible
- A Services
- Home
- BServices
- Cached

同时，我们对每一类进程都统计了其数量。

对于每一个进程，我们都显示其进程名和 pid，形式为：

进程名（pid 进程的 pid 号）

注意：进程的 pid 不是固定分配的，可能会随着进程的结束和重新启动而变化。

2.5. 在界面中部的文本框中，找到需要获取内存镜像的进程的 pid。在 PID 标签旁的文本框输入该 pid，然后单击“获取内存镜像”按钮，内存镜像即会被保存至当前程序运行路径，文件名为“进程 pid.mem”。

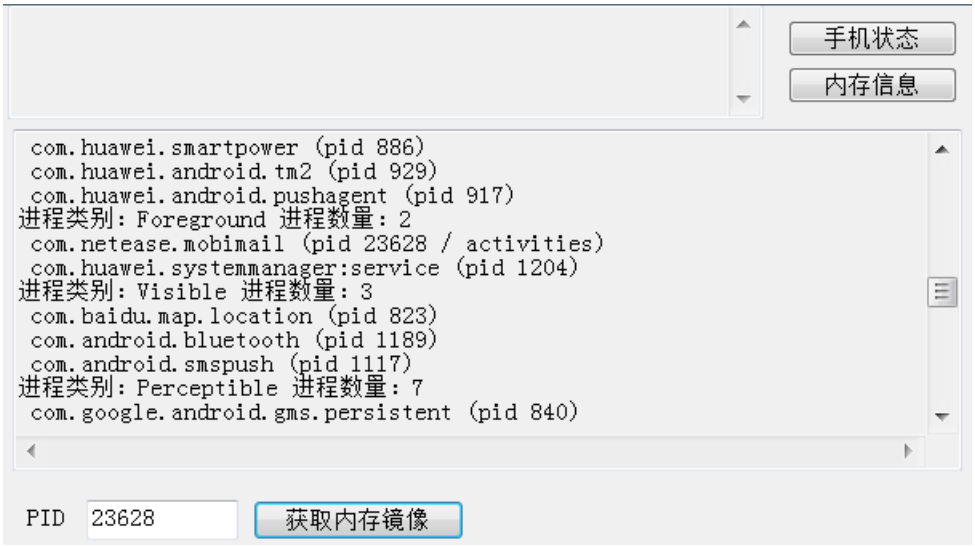

图 5

如图 5，此时我们已连接了一部获取的 root 权限的 Android 手机，并读取了其内存中运行的进程信息。在 PID 标签旁的文本框中输入 PID 号码 23628，并单击“获取内存镜像”按钮，则内存镜像会以“23628.mem”为文件名保存至本软件所在路径，如图 6 所示。

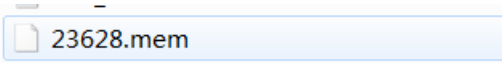

图 6

整个过程大约需要 20 秒左右的时间，请耐心等待，不要随意点击界面,以免导致界面卡死。

2.6. 本软件按照进程获取内存镜像，同样需要根据进程进行内存镜像分析。本软件当前版本支持的分析内存镜像的应用及其对应的进程有：

- 网易邮箱（进程名 com.netease.mobimail）
- 陌陌（进程名 com.immomo.momo）
- 微信（进程名 com.tencent.mm）

在需要分析内存镜像时，必须先单击界面中部的“内存镜像对应的应用”标签旁的下拉菜单，选择获取的镜像所对应的应用。

随后单击下拉菜单旁的“保存路径”按钮选择，在弹出的对话框中，选择分析结果的保存路径，并输入文件名，并单击“保存”，如图 7 所示。

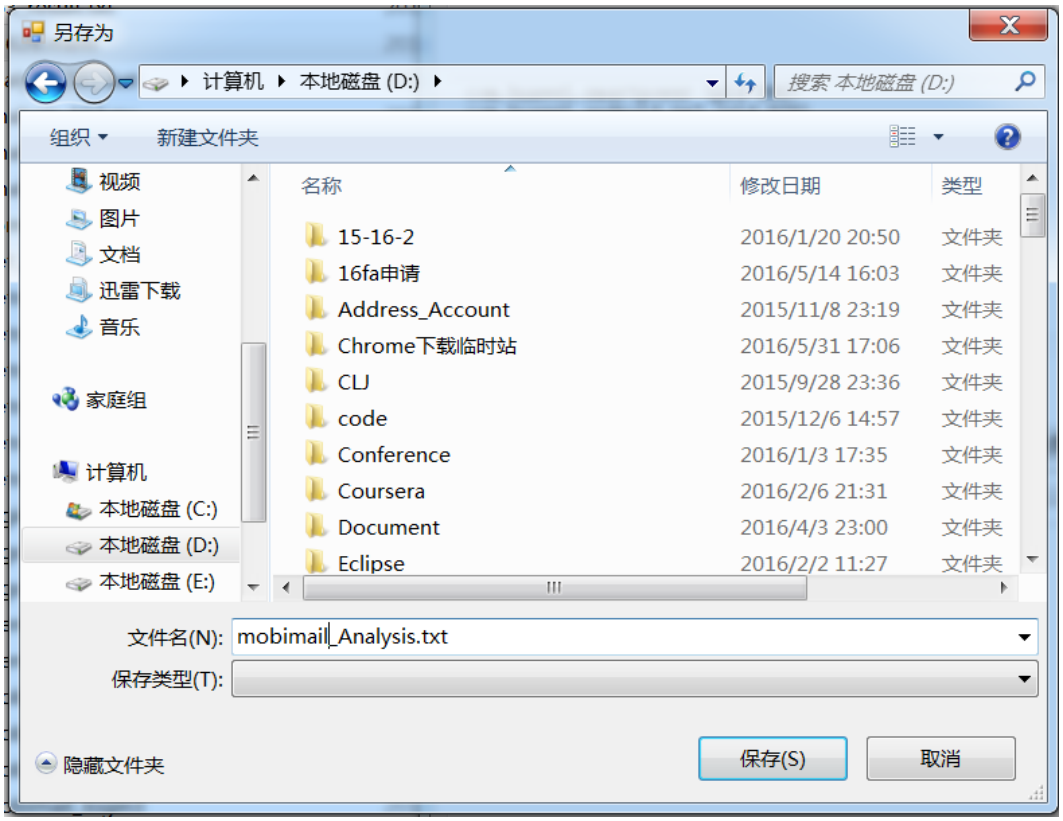
另存为
计算机 ▸ 本地磁盘 (D:) ▸
搜索 本地磁盘 (D:)
组织
新建文件夹
视频
图片
文档
迅雷下载
音乐
家庭组
计算机
本地磁盘 (C:)
本地磁盘 (D:)
本地磁盘 (E:)
名称
修改日期
类型
15-16-2 2016/1/20 20:50 文件夹
16fa申请 2016/5/14 16:03 文件夹
Address_Account 2015/11/8 23:19 文件夹
Chrome下载临时站 2016/5/31 17:06 文件夹
CLJ 2015/9/28 23:36 文件夹
code 2015/12/6 14:57 文件夹
Conference 2016/1/3 17:35 文件夹
Coursera 2016/2/6 21:31 文件夹
Document 2016/4/3 23:00 文件夹
Eclipse 2016/2/2 11:27 文件夹
文件名(N): mobimail_Analysis.txt
保存类型(T):
隐藏文件夹
保存(S)
取消

图 7

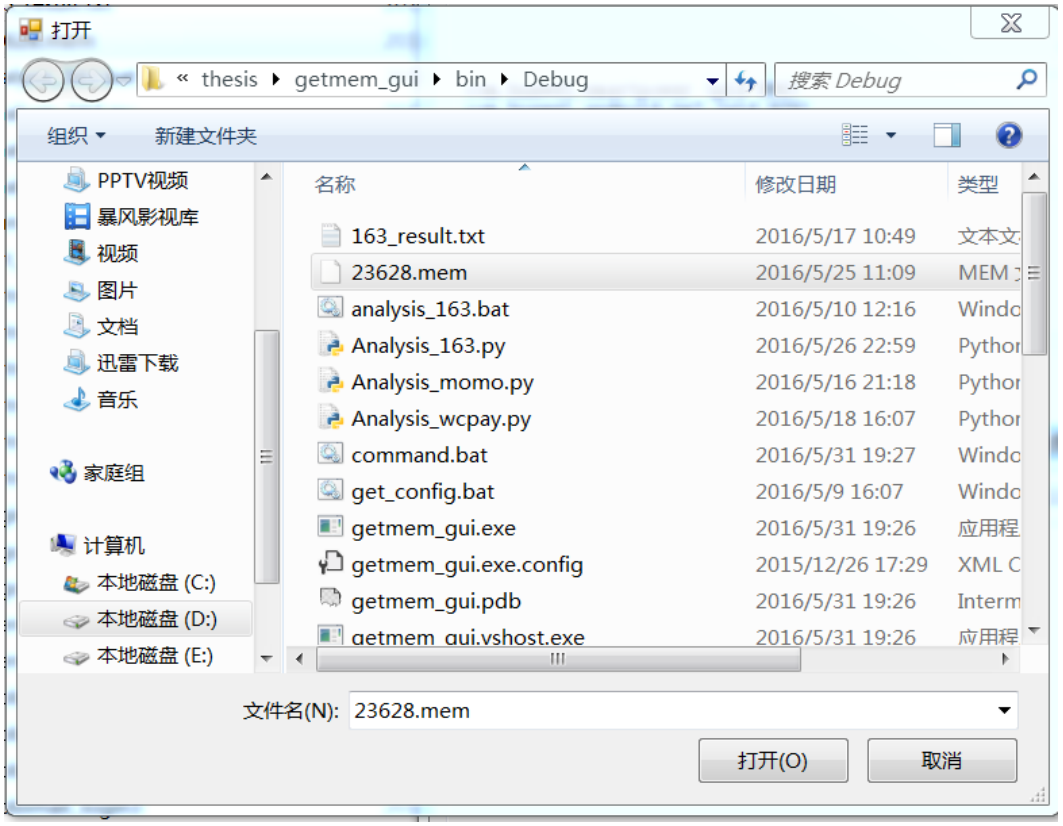
打开
« thesis ▸ getmem_gui ▸ bin ▸ Debug
搜索 Debug
组织
新建文件夹
PPTV视频
暴风影视库
视频
图片
文档
迅雷下载
音乐
家庭组
计算机
本地磁盘 (C:)
本地磁盘 (D:)
本地磁盘 (E:)
名称
修改日期
类型
163_result.txt 2016/5/17 10:49
23628.mem 2016/5/25 11:09
analysis_163.bat 2016/5/10 12:16
Analysis_163.py 2016/5/26 22:59
Analysis_momo.py 2016/5/16 21:18
Analysis_wcpay.py 2016/5/18 16:07
command.bat 2016/5/31 19:27
get_config.bat 2016/5/9 16:07
getmem_gui.exe 2016/5/31 19:26
getmem_gui.exe.config 2015/12/26 17:29
getmem_gui.pdb 2016/5/31 19:26
文件名(N): 23628.mem
打开(O)
取消

图 8

再单击“内存镜像分析”按钮选择需要分析的内存镜像文件（.mem 文件），并单击“打开”按钮，如图 8 所示。

分析完毕后，界面下方文本框会提示：

“分析完成，分析文档已保存至……(保存路径)，点击‘查看结果’按钮查看结果。”

如图 9 所示。

图 9

2.7. 随后，单击“显示结果”按钮，显示内存镜像分析结果，如图 10。

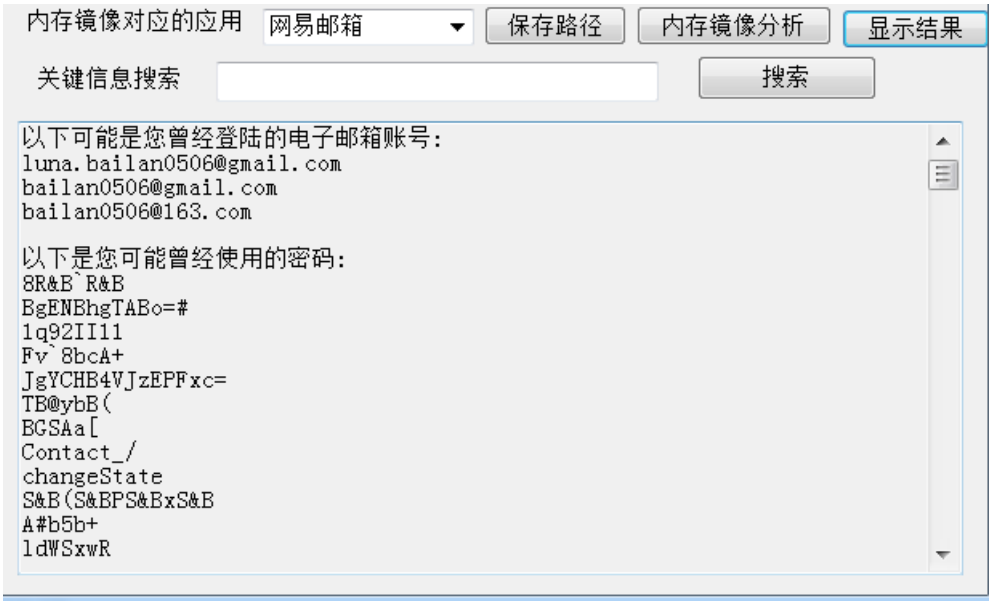

图 10

2.8. 如果发觉分析结果过长，或希望查看与某个关键词相关的信息，可以在关键信息搜索的标识旁的文本框内输入需要的关键信息，并单击搜索按钮，即可检索得到需求的信息。

如图 11 之中，我们需要搜索关于 JSM 的取证信息。那么，就在关键信息搜索旁的文本框中输入 JSM，并单击“搜索”按钮，则界面下方的文本框会显示 JSM 相关的取证数据。

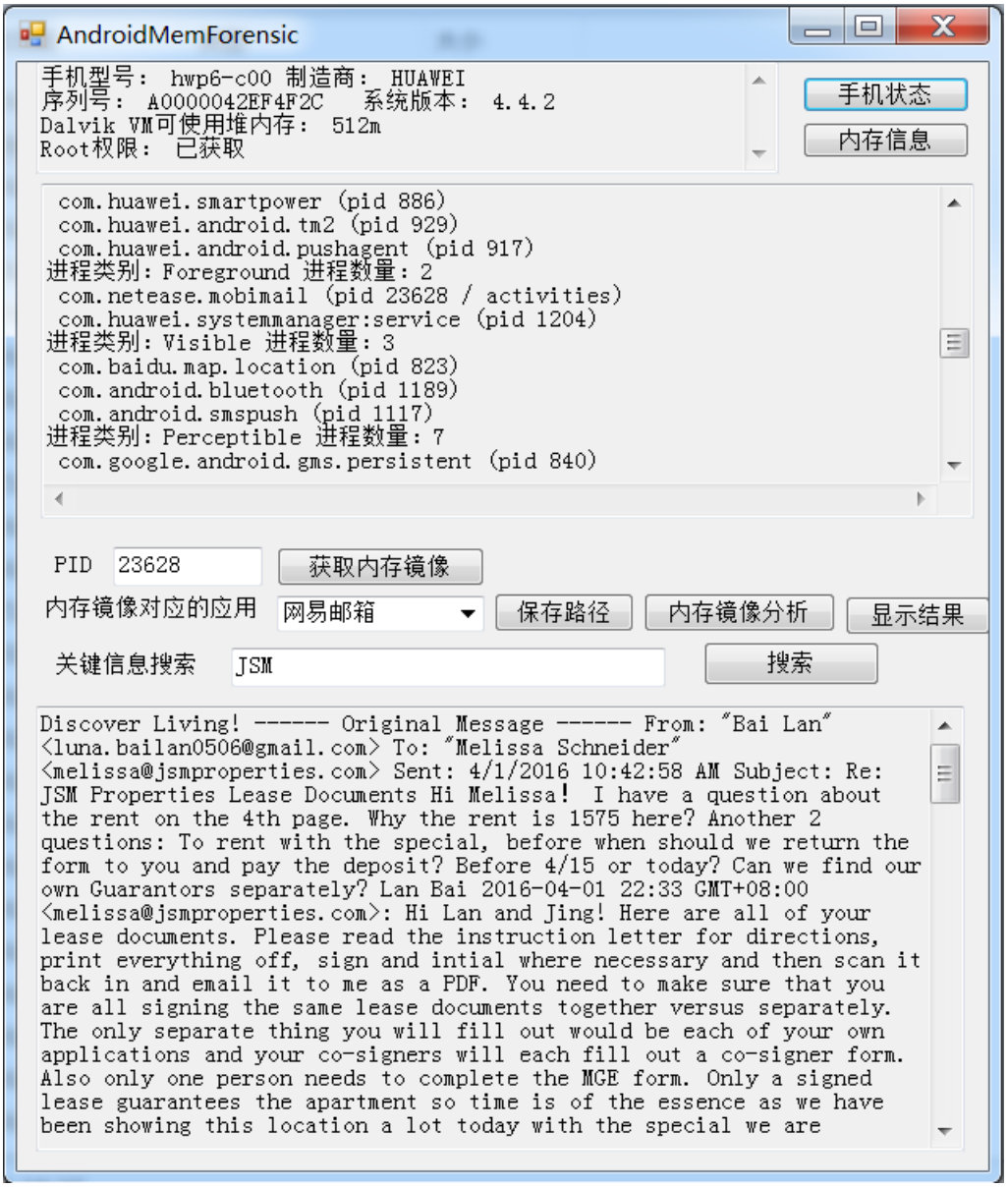

图 11