

基于协议逆向的移动终端通信数据解析

张明远¹, 祁欣妤², 宋宇波², 顾荣荣², 胡爱群², 朱珍超²

(1. 国家无线电监测中心检测中心, 北京 100041;

2. 东南大学网络空间安全学院, 江苏 南京 211189)

摘要: 针对移动终端通信协议及通信数据的解析, 其难点在于大部分移动终端应用程序并无相关公开的技术文档, 难以获知其采取的通信协议类型。指令执行序列分析技术通过分析程序执行的指令序列逆向推断出消息格式和状态机。但有时序列信息采集不全, 导致状态机推断不完备, 从而无法获取全部协议信息。针对上述问题, 提出了一个新型的基于状态机对比推断分析的移动终端通信协议解析方案, 可用于取证场景提高数据取证的准确性和完备性。该方案首先利用 PIN 动态二进制插桩, 识别污点源并跟踪污点轨迹分析出协议消息格式; 然后根据格式信息对提取的协议消息进行聚类分析推断出原始状态机; 最后利用最长公共子序列 (LCS, longest common subsequence) 算法与已知的协议状态机进行对比, 相似度最高者即为推断出的通信协议类型。在 Android 平台上基于两类应用程序设计实验对该方案进行测试和评估, 实验结果表明可准确提取应用程序的通信内容, 实用价值强。

关键词: 移动终端; 数据取证; 动态污点分析; 协议逆向分析; 相似性对比

中图分类号: TN915.08

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018099

Analysis of communication data of mobile terminal based on protocol reversal

ZHANG Mingyuan¹, QI Xinyu², SONG Yubo², GU Rongrong², HU Aiqun², ZHU Zhenchao²

1. The State Radio Monitoring Center Testing Center, Beijing 100041, China

2. School of Cyber Science and Engineering South East University, Nanjing 211189, China

Abstract: The most problem in analysis of communication protocols and communication data for mobile terminals is that many mobile applications do not have the relevant public technical documents, and it is difficult to know the type of communication protocol it adopts. The instruction execution sequence analysis technique takes the instruction sequence executed by the program as a research object, and inversely infers the message format and the state machine to obtain the communication protocol. However, due to the incomplete collection of sequence information, the state machine infers that the inference is incomplete and cannot be effective. A novel protocol reverse scheme based on state machine comparison is proposed, which can be used for the forensics of mobile terminal communication data. The scheme first uses PIN for dynamical identification of the taint, and track it and analyzes the trajectory to obtain the message format. Secondly, the message clustering is performed on the basis of the message format to infer the protocol state machine. Finally, the LCS algorithm is used to compare the state machines to get a complete protocol state machine. This article tests and evaluates the scheme based on two types of application design experiments on the Android platform. The experimental results show that the results are both complete and real-time, and have practical value.

Key words: mobile terminal, data forensics, dynamic stain analysis, protocol reverse analysis, similarity comparison

收稿日期: 2018-11-01; 修回日期: 2018-11-28

通信作者: 祁欣妤, 220184390@seu.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61601113); 中央高校基本科研业务费专项基金资助项目 (No.2242017K40013)

Foundation Items: The National Natural Science Foundation of China (No.61601113), The Fundamental Research Funds for the Central Universities of China (No.2242017K40013)

1 引言

移动终端已成为违法诈骗案件中最常利用的犯罪媒介之一，犯罪分子通过应用程序等方式窃取个人信息或制造恶意攻击，达到犯罪目的。存储在智能终端、智能终端附属设备以及移动运营商数据库中的联系人、短信息、通话记录、各种应用程序的数据信息等数据都可作为有效的证据信息，但对运营商数据库的调用涉及复杂的权限级别等问题，所需时间长，无法及时取证，因此如何快速有效地针对智能终端进行通信数据取证，有极为重要的意义。

随着应用程序的爆发式增长，针对应用程序执行产生的数据信息取证逐渐成为研究热点。然而，在应用程序执行过程中，程序以及用户的初始化数据极易被覆盖或抹去，或者被第三方加密，因此无法获得完整的通信数据。为了证据采集的完整性，还应对应用程序执行过程中产生的网络通信数据进行取证。网络协议规定了网络实体之间进行数据交换的通信机制和内容，对网络通信数据的分析和理解有着至关重要的作用。因此，在智能终端取证前，要先对目标应用程序所采用的网络协议进行逆向分析和推断。网络协议主要包括消息格式以及状态机，因此想要逆向分析出采用的网络协议，要推断出消息格式以及状态机。当前市场上的应用程序大多采用自定义的私有协议，并无公开范本，这给协议的推断造成了难点。现有的协议逆向分析的方法，依据分析对象的不同大致分为 3 类：人工逆向分析、报文序列逆向分析和指令执行序列逆向分析。

文献[1]对软件实现逆向分析工程的各类方法和工具进行了总结，主要有 2 类实现方法：分析观察到的信息交换和反汇编方法。第一种方法是最常用的协议逆向方法，还需使用总线分析器和数据包嗅探器，具体方法是：首先成功接入计算机总线或当前的网络连接，然后截取通信数据，最后分析观察到的总线或者网络行为。Pan 等^[2]基于这种方法，通过安装系统模拟器和嗅探器工具，提出了基于网络协议反向分析的远程控制木马漏洞挖掘方案，为移动终端的远程安全防御做出了贡献。第二种反汇编方法使用反汇编器，将

程序执行文件编译成整数（往往为十六进制），从而找到突破口实现逆向工程，文献[3-5]基于这种方法，提出运用二进制编辑器实现逆向的方案，从而完成协议漏洞检测功能。就网络协议逆向的一般方法而言，Blumbergs 等^[6]给出了大体框架结构，给相关研究工作者提供了清晰的思路：Sija 等^[7]提出了一种无记录以太网和无线协议的协议逆向工程方法，Goo 等^[8]在此基础上进一步针对精确协议给出了逆向协议分析工程的一般性框架。

遗憾的是，现有的协议逆向研究集中在协议消息格式的逆向分析上，忽略了状态机推断结果是否完整的问题，一个协议的状态机有多种状态和状态转化方式，在进行移动终端应用程序通信消息取证时提取的仅是协议消息的一个子集。因此，在此基础上推导得出的仅是一个不完备状态机，无法准确推断其所采用的通信协议类型。针对上述问题，本文提出一种新型可用于智能终端通信数据取证的协议解析方案。该方案首先利用 PIN 动态二进制插桩，识别污点源并跟踪污点轨迹，通过轨迹信息分析出协议消息格式；然后根据格式信息对提取的协议消息进行聚类分析推断出原始状态机；最后利用 LCS 算法与公开通信协议状态机进行相似性对比，从而推断出移动终端应用程序使用的通信协议类型，提高数据取证的准确性和完备性。

2 相关工作

基于协议逆向的移动终端通信数据解析的核心思想是：利用协议逆向分析技术的指令执行序列分析方法，对移动终端中应用程序的通信协议进行完整推断，从而基于协议内容实现对移动终端通信数据的主动获取分析，找到关键“证据”数据。本文的主要研究工作集中在移动终端取证系统的建立上。根据取证的自发性与否，手机取证可以分为静态取证和动态取证。

静态取证又名事后取证，是指在犯罪行为发生后，关闭目标终端并获取其存储介质中的内容，如短信、通话、网页记录等，运用各种取证手段对获得的数据进行分析，从而筛选出有效的电子证据，是一种被动的取证方式。静态取证领域的研究成果已较为成熟：对于数据获取的方法，

Barmatsalon 等^[9]归纳出手动获取、物理取证技术和逻辑取证技术这3种方法。针对操作系统权限问题, Du^[10]提出在取证前进行ADB操作的方法, 使安卓手机权限提升至root级别, 能更便捷地获取信息。之后, 文献[11-12]提出了反对意见: 权限的提升可能会导致获得的信息证据效力降低的问题, 指出了root的非必要性, 并分别利用三星的Galaxy S2的应用程序Orwe和flasher box技术成功印证了观点。针对删除数据恢复的问题, 文献[13-14]提出了一种依据Android系统SQLite存储格式和删除存储机制的恢复方法。

基于静态取证实时性不强、缺乏周期性完整证据链的弊端, 以及智能手机具有存储量小和易于擦写的特点, Grobler^[15]指出应采用动态取证弥补静态取证的缺陷, 用对事件实时控制的方式取代对既定事件的处理。动态取证是在目标手机运行的过程中对数据进行采集和分析来获得电子证据。针对智能终端存储器数据易失性、难恢复性问题, Thing 等^[16]提出了一种数据动态获取方法, 调用Kernel内核的PTRACE功能实时追踪进程, 但只能获得特定内存区域的轨迹数据。目前对手机动态取证的实验研究较少, 缺乏完整的知识架构。

3 移动终端通信数据主动取证方案

3.1 主动取证方案概述

图1描述了主动取证系统的整体架构, 它由

3部分构成: 1) 取证代理模块集成了污点源识别与轨迹跟踪记录功能, 利用动态污点分析技术, 将动态识别到的网络数据标记为污点源, 追踪污点源进入程序后的轨迹, 并将这些轨迹信息存储下来发送给下一个模块; 2) 证据分析模块以收到的轨迹信息为基础进行污点传播分析, 得到应用程序处理网络数据的过程等相关信息, 解析出应用程序的消息格式以及状态机, 在此模块本文创造性地用字符串相似度算法对比推断出的状态机和已有的状态机, 从而获得完整的协议状态机; 3) 证据存储模块将得到的结果进行存储。3个部分顺次进行、协调分工, 形成一个动态的周期性证据链。

3.2 取证代理模块

取证代理模块包含3个部分: 污点源动态识别子模块、轨迹跟踪子模块以及轨迹存储子模块。作为整个主动取证系统的核心, 取证代理模块集成了污点源识别和轨迹跟踪记录功能, 为之后的数据分析模块提供了数据基础。

3.3 证据分析模块

证据分析模块由4个部分组成: 污点传播分析子模块、消息格式解析子模块、状态机推断子模块和状态机对比子模块。其中, 消息格式解析子模块是核心环节, 实现了分隔符和关键词提取、长度域和目标域确定等功能。消息格式解析完成后, 将消息聚类并输出给状态机推断子模块。状态机推断子模块包括增广前缀树(APTA)构造、

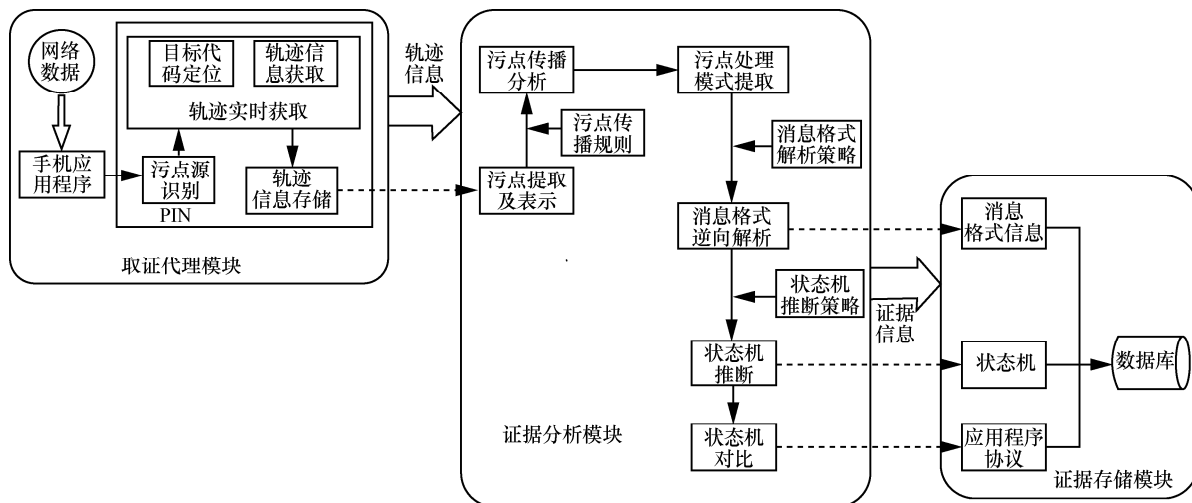


图1 主动取证系统的整体架构

状态机标记、状态机的化简。作为主动取证系统的中间环节，证据分析模块对整个系统的运行起到了承上启下的作用。

3.4 证据存储模块

证据存储模块是整个主动取证系统的最终环节，以 MySQL 数据库系统为平台，主要负责获得的电子证据的存储功能，配合时间戳、数字签名、数字摘要等技术保证了电子证据的可靠性和有效性。

MySQL 是一种开源的数据库管理系统，可用于分类存储电子证据。MySQL 具有操作简便的优点，只需登录用户界面即可查看电子证据。存储的证据类型较齐全，包括指令轨迹信息、消息格式、状态机以及推断出的网络协议。消息格式存储结构如表 1 所示，状态机中各个状态存储结构如表 2 所示。

表 1 消息格式存储结构

字段名称	字段类型	字段说明
ID	长整型	自动编号
Time	长整型	消息发生时间
Msg_Type	长整型	消息类型（接收/发送）
Protocol	长整型	消息所属协议
Msg_Content	长整型	消息内容

表 2 状态机中状态存储结构

字段名称	字段类型	字段说明
Status_ID	长整型	状态标号
Pre_Status	长整型	前一个状态
Next_Status	长整型	后一个状态
Pre_Trans	长整型	前一个状态转换规则
Next_Trans	长整型	后一个状态转换规则
First_Status	长整型	状态机第一个状态
Last_Status	长整型	状态机最后一个状态

4 基于 PIN 的污点源动态识别及轨迹追踪

PIN 是 Intel 开发的一款动态二进制插桩工具，在不同的操作系统上支持不同的 CPU 架构。PIN 的内外部程序是分开的，其固有框架的开发

和升级维护由企业内部相关人员负责，但面向外部用户，它提供了一个很大的服务中心——API 函数群供用户使用，可以完成性能分析、内存分配、资源管理、计算等工作。基于此，PIN 除了计算机架构分析之外，被广泛地应用于环境模拟、计算机安全以及计算。此外，Intel 向用户提供了一系列简易的开发插件，这些插件统称为 Pintool。在取证代理模块，本文提出了一种基于 PIN 的污点源动态识别技术和一种基于 PIN 的轨迹跟踪存储技术。

4.1 基于 PIN 的污点源动态识别

为了降低污点分析开销，本文选择在操作系统层面引入污点，应用程序获取网络报文需要调用相应的 API 函数，通过分析 API 函数的执行情况，可以得到目标应用程序接收到的消息序列的字节数和存储位置。最后将这些报文所处的内存标记成污点源。具体流程如图 2 所示。

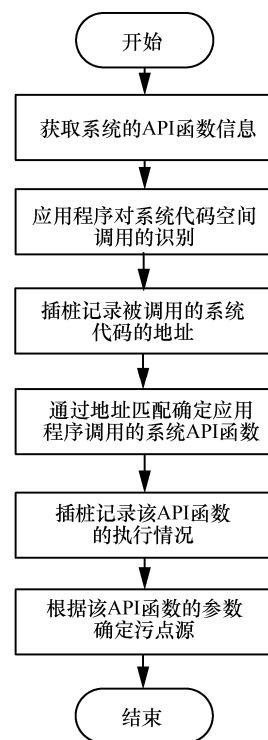


图 2 污点源识别流程

4.2 基于 PIN 的轨迹跟踪与存储

轨迹信息是指指令的执行流程和指令的操作数、操作码和地址。其中，指令的操作数在指令执行的过程中动态改变，因此需要借助额外代码及时更新新的轨迹信息。具体做法为：

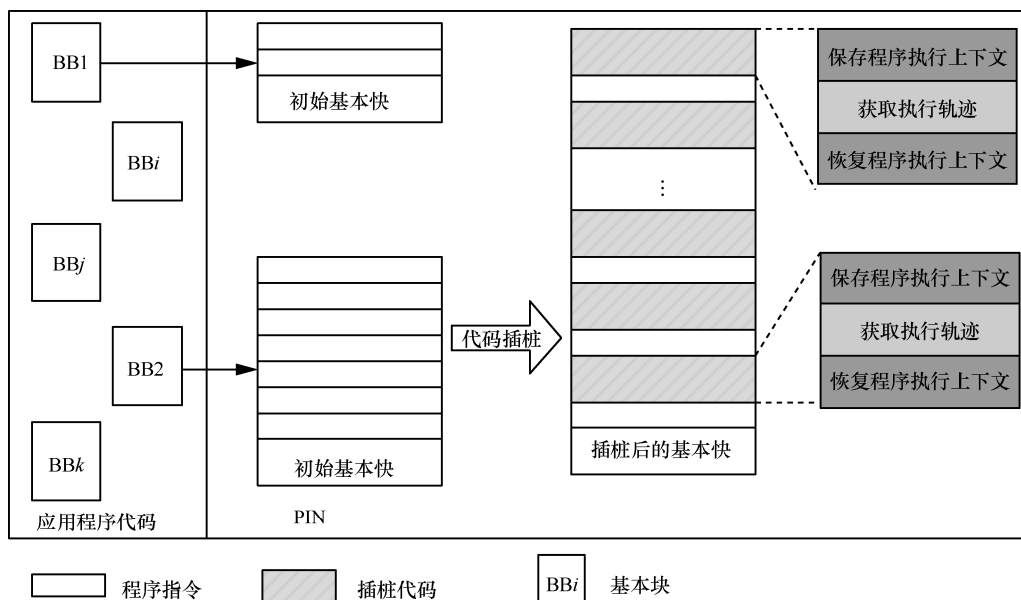


图 3 程序动态插桩示意

PIN 虚拟机载入应用程序,动态地插入分析代码,同时将分析代码缓存,及时编译、执行插桩后的代码以获得程序运行时的数据,记录轨迹信息。图 3 为程序动态插桩示意。此次实验调用了 `INS_AddInstrumentFunction` 函数,用以判断指令操作数的类型并获得操作数的内容。

5 基于 LCS 算法的状态机比对

在证据分析模块,本文提出改进的协议逆向分析技术,与现有的协议逆向技术相比,增加了基于 LCS 算法的状态机对比部分,以获得应用程序通信协议的完整消息格式和状态机文件。改进的好处是:可获得通信协议的完整消息格式和状态机,通过查看协议文档存储的关键词具体含义,理解通信双方的行为,判断捕获的数据信息能否作为证据信息。

LCS 算法是一种字符串相似度算法,除此之外的字符串相似度算法有编辑距离算法和贪婪字符串对比算法,与后两者相比,LCS 算法时间复杂度较低,故本文选用 LCS 算法进行状态机的对比。LCS 算法的具体步骤如下。

1) 计算 2 个字符串的长度记为 $Len1(str1)$ 和 $Len2(str2)$,如果其中任一个字符串的长度为 0,则最长公共子序列长度为 0。

2) 构造一个大小为 $(Len1+1) \times (Len2+1)$ 的矩阵 A ,将矩阵 A 的第一行与第一列均置零,即 $a_{0,j}=0, a_{i,0}=0$,其中, $0 \leq i \leq Len1, 0 \leq j \leq Len2$ 。

3) 计算矩阵 A 的每一个元素 a_{ij} ,则矩阵中最大元素的值为最大公共序列的长度,记为 LCS。

$$a_{i,j} = \begin{cases} a_{i-1,j-1} + 1, & Str1[i] = Str2[j] \\ \max \{a_{i,j-1}, a_{i-1,j}\}, & Str1[i] \neq Str2[j] \end{cases} \quad (1)$$

$$4) \text{ 计算相似度 } \delta = \frac{2 \times LCS}{Len1 + Len2}。$$

如表 3 所示,依次列出协议以及现有协议 1、协议 2 的转换序列,根据 LCS 算法,计算出的相似度结果为:与序列 AabBc 相似度最大的为协议 1 的 AabBFc,相似度为 91%;序列 Cac 与协议 2 的 Cac 相似度为 100%,序列 DdEc 与协议 1 的 DdEc 相似度为 100%。故协议 p 中 $\frac{2}{3}$ 状态转换与协议 1 相似,即协议 1 是逆向分析的原始协议。

表 3 状态序列示例

协议 p	协议 1	协议 2
AabBc	AabBFc	GmHnc
Cac	Cabc	DmEc
DdEc	DdEc	Cac

6 实验与评估

本文选择智能移动终端操作系统 Android 作为系统测试平台，针对目前关注度较高的 2 种应用程序类型：网页浏览类和即时通信类，选择相应的应用程序作为测试对象，实现了完整的主动取证分析系统。

6.1 网页浏览类应用程序下的主动取证分析

针对网页浏览类应用程序，本文选用 ES 文件浏览器为代表测试对象。首先打开 ES 文件浏览器的 FTP 功能，新建一个 FTP 服务器，建立后对其访问进行如下操作：在目录下新建一个 txt 文件，并将手机上的文件 001.pcap 复制至该目录，最后删除新建的 txt 文件。在进行上述操作的同时，对本文设计的主动取证系统按运行步骤相继进行测试。

根据解析出的消息格式，利用状态机推断策略，推断出 ES 文件浏览器的协议状态转换结果，如图 4 所示。根据状态机对比策略，将得到的 13 条状态转换信息与 FTP 和 SMTP 的状态转换信息进行对比，对比结果如表 4 所示。

状态转换信息
State_Trans1=<none, 220, USER, 331>
State_Trans2=<USER, 331, PASS, 230>
State_Trans3=<PASS, 230, CWD, 250>
State_Trans4=<CWD, 250, PORT, 200>
State_Trans5=<PORT, 200, LIST, 226>
State_Trans6=<PORT, 200, RETR, 226>
State_Trans7=<PORT, 200, STOR, 226>
State_Trans8=<PORT, 200, CWD, 250>
State_Trans9=<CWD, 250, PORT, 200>
State_Trans10=<LIST, 226, DELE, 250>
State_Trans11=<LIST, 226, QUIT, 221>
State_Trans12=<DELE, 250, QUIT, 221>
State_Trans13=<CWD, 250, QUIT, 221>

图 4 状态转换信息解析结果

通过状态对比可以确定 ES 文件浏览器使用了 FTP 处理上述通信数据，并将主动取证系统解析得到的 ES 文件浏览器通信数据存储在数据库中，如图 5 所示。其中，1 中的用户名、3 中的密码和其余的操作信息等都可以作为证据信息的数据。按时间顺序排列存储得到消息格式信息，可以直观地看到目标手机应用程序所执行的所有操作和操作相互之间的时序关系。

表 4 状态比对结果

状态转换信息	FTP	SMTP
State_Tr1	100%	64.28%
State_Tr2	100%	55.14%
State_Tr3	100%	28.57%
State_Tr4	100%	0
State_Tr5	100%	0
State_Tr6	100%	0
State_Tr7	100%	0
State_Tr8	100%	0
State_Tr9	100%	0
State_Tr10	100%	0
State_Tr11	100%	49.06%
State_Tr12	100%	50%
State_Tr13	100%	22.35%

msg_id	msg_time	msg_type	protocol	msg_content
Click here to define a filter				
1	2015-04-23 15:37:50	SEND	FTP	USER graduate
2	2015-04-23 15:37:50	RECV	FTP	331 User name okay, need password.
3	2015-04-23 15:37:50	SEND	FTP	PASS graduate
4	2015-04-23 15:37:50	RECV	FTP	230 User logged in, proceed.
5	2015-04-23 15:37:50	SEND	FTP	TYPE I
6	2015-04-23 15:37:50	RECV	FTP	200 Type set to I.
7	2015-04-23 15:37:50	SEND	FTP	CWD /
8	2015-04-23 15:37:50	RECV	FTP	250 Directory changed to /
9	2015-04-23 15:37:50	SEND	FTP	SYST
10	2015-04-23 15:37:50	RECV	FTP	215 UNIX Type: L8
11	2015-04-23 15:37:50	SEND	FTP	PORT 121,248,50,229,172,47
12	2015-04-23 15:37:50	RECV	FTP	200 PORT Command successful.

图 5 ES 文件浏览器解析结果展示

6.2 即时通信类应用程序下的主动取证分析

针对即时通信类应用程序，本文将手机自带的邮箱作为代表测试对象。过程如下：打开邮箱并添加账号；在成功添加账号后该应用程序会自动收取邮件；使用该账号发送一封电子邮件。

在邮件收取阶段，以通信数据消息格式的解析结果为基础，结合状态机推断策略，得到状态转换结果，如图 6 所示。根据状态机对比策略，将所得的 6 条状态转换信息与 POP3 协议和 IMAP 进行对比，与 POP3 协议的相似度高达 100%，由此可以确定该应用程序是使用 POP3 协议收取邮件的。

状态转换信息
State_Trans1=<none, q0, USER, q1>
State_Trans2=<USER, q1, PASS, q2>
State_Trans3=<PASS, q2, STAT, q3>
State_Trans4=<STAT, q3, LIST, q3>
State_Trans5=<LIST, q3, UIDL, q3>
State_Trans6=<UIDL, q3, QUIT, q4>

图 6 邮件收取阶段状态转换信息解析结果

同样地, 在邮件发送阶段, 得到状态转换结果如图 7 所示。将得到的 9 条状态转换信息与 SMTP 和 FTP 进行对比, 与 SMTP 的相似度高达 100%, 由此可以确定该应用程序是使用 SMTP 发送邮件的。

```

状态转换信息
State_Trans1=<none,220,EHLO,250>
State_Trans2=<EHLO,250,AUTH,334>
State_Trans3=<AUTH,334,user,334>
State_Trans4=<user,334,pass,235>
State_Trans5=<pass,235,MAIL,250>
State_Trans6=<MAIL,250,RCPT,250>
State_Trans7=<RCPT,250,DATA,354>
State_Trans8=<DATA,354,CONTENT,250>
State_Trans9=<CONTENT,250,QUIT,221>

```

图 7 邮件发送阶段状态转换信息解析结果

将主动取证系统解析得到的邮件应用程序通信数据存储在数据库中, 如图 8 所示。可以看出, 主动取证系统在邮件的收取阶段和发送阶段成功地获取了邮箱用户的用户名、密码、邮箱中邮件的数目和大小、邮件发送方和接收方、邮件主题等有效的证据信息。

7 结束语

本文提出了一种基于协议逆向分析的移动终端通信数据主动取证方案, 由取证代理模块、证据分析模块和证据存储模块 3 个部分组成。与现有的基于协议逆向分析的移动终端通信数据取证技术相比, 做了两方面的改进: 第一, 在取证代理模块, 利用二进制插桩工具 PIN 实现了对污染源的动态识别和轨迹动态追踪, 保证了证据采集的及时; 第二,

在证据分析模块, 增加了基于 LCS 算法的状态机对比部分, 保证了证据追溯的完整。实验结果表明, 该取证系统兼具实时性和完整性, 实用价值强。

参考文献:

- [1] SIJA B D, GOO Y H, KYU S S, et al. Survey on network protocol reverse engineering approaches, methods and tools[C]// IEEE Network Operations and Management Symposium. 2017:271-274.
- [2] PAN D, WANG Y, XUE Z. Remote control trojan vulnerability mining based on reverse analysis of network protocol[J]. Computer Engineering, 2016:124-140.
- [3] WEN S, MENG Q, FENG C, et al. Protocol vulnerability detection based on network traffic analysis and binary reverse engineering[J]. Plos One, 2017, 12(10): 186-188.
- [4] LI W, AI M, JIN B. A network protocol reverse engineering method based on dynamic taint propagation similarity[M]. Intelligent Computing Theories and Application. Springer International Publishing, 2016:580-592.
- [5] WEI X, LIU R, XU F. Reverse analysis of industrial control protocol based on static binary analysis[J]. Application of Electronic Technique, 2018: 366-372.
- [6] BLUMBERGS B, VAARANDI R. BBUZZ: a bit-aware fuzzing framework for network protocol systematic reverse engineering and analysis[C]//IEEE Military Communications Conference. 2017: 707-712.
- [7] SIJA B D, GOO Y H, SHIM K S, et al. Protocol reverse engineering methods for undocumented ethernet and wireless protocols; survey[C]//Symposium of the Korean Institute of Communications and Information Sciences. 2017:281-312.
- [8] GOO Y H, SHIM K S, CHAE B M, et al. Framework for precise protocol reverse engineering based on network traces[C]// IEEE/IFIP Network Operations and Management Symposium. 2018: 1-4.
- [9] BARMPATSAKON K, DAMOPOULOS D, KAMBOURAKIS G, et al. A critical review of 7 years of mobile device forensics[J]. Digital Investigation, 2015, (10): 323-349.
- [10] DU J. Android mobile forensics privilege promotion[J]. Silicon Valley. 2016, 14: 563-578.

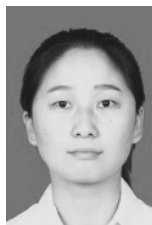
msg_id	msg_time	msg_type	protocol	msg_content
Click here to define a filter				
1	2015-04-24 14:04:26	SEND	POP3	USER shinestudy@163.com
2	2015-04-24 14:04:26	RECV	POP3	+OK core mail
3	2015-04-24 14:04:26	SEND	POP3	PASS mss331437
4	2015-04-24 14:04:26	RECV	POP3	+OK 75 message(s) [930389 byte(s)]
5	2015-04-24 14:04:26	SEND	POP3	STAT
6	2015-04-24 14:04:26	RECV	POP3	+OK 75 930389
7	2015-04-24 14:04:26	SEND	POP3	LIST
8	2015-04-24 14:04:26	RECV	POP3	+OK 75 930389
9	2015-04-24 14:04:26	SEND	POP3	UIDL
10	2015-04-24 14:04:26	RECV	POP3	+OK 75 930389
11	2015-04-24 14:04:26	SEND	POP3	QUIT
12	2015-04-24 14:04:26	RECV	POP3	+OK core mail
13	2015-04-24 14:09:56	SEND	SMTP	EHLO [172.22.226.3]
14	2015-04-24 14:09:56	RECV	SMTP	250-mail
15	2015-04-24 14:09:56	SEND	SMTP	AUTH LOGIN
16	2015-04-24 14:09:56	RECV	SMTP	334 vxnlcm5hbwU6 21e4d9ed-4980-8d97-44f775c22cf3
17	2015-04-24 14:09:56	SEND	SMTP	user: bwVuz3NoYw42LjEyM0AxNjMuY29t
18	2015-04-24 14:09:56	RECV	SMTP	334 UGFzc3dvcmQ6 21e4d9ed-4980-8d97-44f775c22cf3

图 8 邮件应用程序解析结果展示

- [11] AL BARGHOOTHY N, MARRINGTON A. A comparison of forensic acquisition techniques for android devices: a case study investigation of or Web browsing sessions[C]//2014 6th International Conference on New Technologies Mobility and Security (NTMS). 2014: 1-4.
- [12] JONKERS K. The forensic use of mobile phone flasher boxes[J]. Digital Investigation, 2015, (6): 168-178.
- [13] JEON S, BANG J, BYUN K, et al. A recovery method of deleted record for SQLite database[J]. Personal and Ubiquitous Computing, 2017, 16(6): 707-715.
- [14] YANG Y T, ZU Z Y, SUN G Z. Historical data recovery from android devices[M]//Future Information Technology. Berlin Heidelberg: Springer, 2016: 251-257.
- [15] GROBLER C, LOUWRENS C, VON SOLMS S. A multi-component view of digital forensics: fifth international conference on availability, reliability, and security[C]//IEEE Piscataway. 2011: 647-652.
- [16] THING V L L, NG K Y, CHANG E C. Live memory forensics of mobile phones[J]. Digital Investigation, 2015:74-82.



宋宇波（1977-），男，江苏无锡人，博士，东南大学副教授，主要研究方向为通信网络安全及协议安全性分析。



顾荣荣（1990-），女，江苏盐城人，东南大学硕士生，主要研究方向为智能移动终端。

[作者简介]



张明远（1982-），男，内蒙古人，硕士，国家无线电监测中心检测中心工程师，主要研究方向为新型无线电检测技术。



胡爱群（1952-），男，江苏南通人，博士，东南大学教授、博士生导师，主要研究方向为通信网络安全。



祁欣妤（1995-），女，江苏南京人，东南大学硕士生，主要研究方向为通信网络安全。



朱珍超（1982-），男，安徽霍邱人，博士，东南大学讲师，主要研究方向为密码学与网络安全。