ICS 35.240.01
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1172—2014

电子邮件检验技术方法

Technical methods for E-mail examination

2014-07-09 发布　　2014-07-09 实施

中华人民共和国公安部　　发布

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部第三研究所提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部第三研究所、黑龙江省公安厅刑事技术总队。

本标准主要起草人：张颖、王洪庆、郭弘、金波、黄道丽、徐克鑫。

电子邮件检验技术方法

1 范围

本标准规定了对电子邮件进行检验的技术方法。

本标准适用于在电子数据检验鉴定工作中，对电子邮件的真实性进行检验。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GA/T 756—2008 数字化设备证据数据发现提取固定方法

RFC 821 Simple Mail Transfer Protocol

RFC 1939 Post Office Protocol-Version 3

RFC 3501 Internet Massage Access Protocl-Version 4rev1

RFC 4409 Message Submission for Mail

3 术语和定义

GA/T 756—2008、RFC 821、RFC 1939、RFC 3501 和 RFC 4409 界定的以及下列术语和定义适用于本文件。

3.1

电子邮件 electronic mail(E-mail)

通过数据通讯网络进行传输的信件。

3.2

邮件应用程序接口 messaging application programming interface(MAPI)

微软公司提供的用于创建邮件撰写和工作组应用程序的开放和全面的邮件撰写接口。

3.3

电子邮件客户端 electronic mail client(E-mail Client)

使用 POP3、SMTP 等协议收发电子邮件的软件。

3.4

邮件信息号 message-ID

邮件系统创建邮件时的唯一标志，是发件方邮件服务器赋给这封邮件的编号，由唯一编号、@符号和域名组成。

3.5

邮件头 electronic mail header(E-mail header)

电子邮件消息中正文前面的部分，由字段名及值组成，能够描述出邮件在网络中的传输情况，同时表明消息的接收者、发送者、发送时间和时区、邮件主题、邮件信息号、邮件传送代理等信息。

4 检验步骤

4.1 检材编号

当送检检材为数字化设备时，对其进行唯一性编号。

4.2 检材拍照

当送检检材为数字化设备时，对其进行拍照。

4.3 检材的获取和保全备份

4.3.1 检材为数字化设备

检材为数字化设备时，对具备保全条件的检材进行保全备份，参见 GA/T 756—2008。

4.3.2 检材为独立于数字化设备的文件

分析检材，根据检材的内容选择以下的一项或多项进行检验：

a) 检材为电子邮件时，将电子邮件导出到检验环境中；

b) 检材为电子邮箱地址时，在检验环境中连接到互联网(或局域网络)后，通过电子邮件客户端或者网页登录电子信箱，查找与检验要求有关的电子邮件，并下载有关电子邮件到检验环境中，参见 GA/T 756－2008。如果通过电子邮件客户端收取电子邮件，应确认电子邮件客户端被设置为在服务器上保留邮件的副本；

c) 检材为第三方邮件服务器日志时，将服务器日志导出到检验环境中。

4.4 分析电子邮件的真伪

4.4.1 直接判定邮件真实性

检验电子邮件的发送是否使用数字签名，对于使用数字签名的电子邮件可以直接判断其真实性。

4.4.2 电子邮件服务器的邮件相关信息分析

根据从邮件服务器日志、服务器备份数据等处查找到的邮件相关信息，判断电子邮件是否经过删除、修改。

4.4.3 接收电子邮件的协议分析

对接受电子邮件的协议进行分析，判断电子邮件的真实性。

a) 检验电子邮件是否使用 IMAP 接收协议，该协议使得客户端能够与服务器端实现同步，因此使用了该协议的电子邮件需结合检材中使用的客户端软件版本、邮件头信息以及其他相关信息来判断其真实性；

b) 检验电子邮件是否使用 POP3 接收协议，使用了该协议的电子邮件应通过分析电子邮件的邮件头信息以及其他相关信息来判断其真实性；

c) 检验电子邮件是否使用 MAPI 接收协议，使用了该协议的电子邮件应通过分析电子邮件的邮件头信息以及其他相关信息来判断其真实性。

4.4.4 电子邮件头分析

查看电子邮件的邮件头，通过分析邮件头中电子邮件的发送时间、接收时间、邮件传送代理

(MTA)、邮件用户代理(MUA)、服务器 IP 地址以及邮件信息号(Message-ID)等信息来判断邮件的真伪。

4.4.5 电子邮件之间的关系分析

对接受电子邮件之间的关系进行整理分析,判断电子邮件的真实性。

a) 由于电子邮件不是孤立的,需要鉴定的电子邮件往往和其他电子邮件的内容有所关联,因此需要结合这些相关联的电子邮件,依照发送与接收的时间顺序,对需鉴定的电子邮件进行梳理,并结合邮件头信息检验电子邮件的真实性;

b) 对于发送方将电子邮件转发给第三方的情况,可根据第三方所接收到的电子邮件来判断其真实性。

4.5 检验记录

4.5.1 对于检材为数字化设备的,应记录检材的:

a) 类别;

b) 型号;

c) 出厂时唯一性编号(如果适用);

d) 照片。

4.5.2 对于检材为独立于数字化设备的文件时,应记录文件的:

a) 名称;

b) 哈希值。

4.5.3 应对检验分析的过程进行记录。

5 检验结论和意见

邮件的真实性检验结论是以下四种结论之一:

a) 发现修改/伪造;

b) 没有发现修改/伪造;

c) 没有修改/伪造;

d) 不能判定。

中华人民共和国公共安全
行业标准
电子邮件检验技术方法
GA/T 1172—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.5 字数 8 千字
2014年9月第一版 2014年9月第一次印刷
*
书号:155066·2-27342 定价 14.00 元

GA/T 1172-2014

打印日期:2014年11月11日 F009A