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

GA/T 1172—2014

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

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

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。