司　法　鉴　定　技　术　规　范

SF/Z JD0402001—2014

电子邮件鉴定实施规范

2014－3－17 发布　　2014－3－17 实施

中华人民共和国司法部司法鉴定管理局　发布

目　　次

前　言

本技术规范按照 GB/T 1.1-2009 给出的规则起草。
本技术规范由司法部司法鉴定科学技术研究所提出。
本技术规范由司法部司法鉴定管理局归口。
本技术规范起草单位：司法部司法鉴定科学技术研究所。
本技术规范主要起草人：施少培、杨旭、卞新伟、陈晓红、李岩、卢启萌。
本技术规范为首次发布。

电子邮件鉴定实施规范

1 范围

本技术规范规定了电子邮件鉴定的术语和定义、鉴定步骤、检验记录、鉴定意见的规范性要求。
本技术规范适用于电子数据鉴定中的电子邮件鉴定。

2 术语和定义

下列术语和定义适用于本文件。

2.1

电子邮件 electronic mail（E-mail）
通过网络在用户终端之间传送的信函。由邮件头和邮件内容组成。

2.2

邮件头 E-mailheader
电子邮件的信封部分，反映了邮件的传送和投递情况，包含邮件的接收人、发送人、发送时间、主题、邮件ID、路由过程等信息。

2.3

邮件内容 E-mailbody
电子邮件的发送人要投递给接收人的信息部分，除正文外，还可添加以文件形式传送的附件。

2.4

电子邮件客户端 E-mail client
用户终端中安装的发送、接收与管理电子邮件的软件，如Outlook Express、Foxmail等。

2.5

网页电子邮件服务webmail
基于网页浏览器发送、接收与管理电子邮件的服务。

2.6

检材 material for examination
包含需要进行鉴定电子邮件的硬件设备或网络电子邮箱。

2.7

检材邮件 questioned E-mail
检材中需要进行鉴定的电子邮件，又称待检邮件、需检邮件，

3 鉴定步骤

3.1 了解相关情况

3.1.1 了解检材邮件形成过程的陈述。

3.1.2 了解检材邮件提交方的电子邮件收发情况，如接收和发送方式、使用的电子邮件客户端等。

3.1.3 当检材邮件位于网络电子邮箱中时，了解电子邮箱地址及其口令信息，并获得其使用授权。

3.1.4 如检材邮件有抄送方和密送方时，尽可能获取抄送方和密送方的相关电子邮件，拓展信息来源。

3.2 固定保全

3.2.1 计算机等硬件设备

当检材为计算机等硬件设备时：

a) 对检材进行惟一性标识；

b) 对检材进行拍照或录像，记录其特征；

c) 对具备条件的检材进行保全备份，并进行完整性校验，之后使用备份数据进行检验；

d) 搜寻、提取检材邮件及相关邮件，计算检材邮件或包含检材邮件的数据文件的哈希值。

3.2.2 网络电子邮箱

当检材为网络电子邮箱时：

a) 通过电子邮件客户端或网页方式搜寻、提取检材邮件及相关邮件；

b) 对登录网络电子邮箱及提取邮件过程进行截图或录像，并记录登录时间、地点、人员、环境等信息；

c) 计算提取的检材邮件的哈希值。

注：提取时不得删除保存在邮件服务器上的电子邮件。

3.3 搜索和恢复

按照相关技术方法，搜索、恢复保存在硬件设备上的电子邮件及其它相关文件和数据。

3.4 真实性检验和分析

3.4.1 检验和分析内容

根据检材邮件具体情况，视需要对下列全部或部分内容进行检验和分析：

a) 邮件基本信息检验：查看检材邮件及其所在电子邮箱中其它邮件的结构、格式、内容、收件人、发件人、抄送人、密送人、时间、数字签名等情况；

b) 邮件结构和格式分析：根据电子邮件服务和电子邮件客户端的特点，分析检材邮件的结构、格式、属性信息等是否存在异常；

c) 邮件头分析：分析检材邮件的邮件头信息是否存在异常。重点关注邮件头格式、时间信息、路由信息、客户端信息、邮件 ID 信息等内容；

d) 邮件正文分析：分析检材邮件的正文信息是否存在异常。重点关注正文的结构及内容的合理性和逻辑性等情况；

e) 邮件附件分析：通过附件元数据等信息，分析检材邮件的附件是否存在异常。重点关注附件的时间属性等情况；

f) 往来邮件分析：搜索相同发件人/收件人/抄送人/密送人之间对同主题邮件（检材邮件）的往来邮件，分析相互之间的逻辑关系是否存在矛盾；

g) 其它相关信息分析：在检材中搜索检材邮件及其附件中出现的关键词和文件，分析搜索到的内容与检材邮件是否存在关联，相互之间的逻辑关系是否存在矛盾；

h) 邮件服务器分析：如条件允许，对收发检材邮件的服务器进行检验，分析其中的相关信息与检材邮件是否存在矛盾。包括保存在服务器上的电子邮件、服务器日志及数据备份等。

3.4.2 综合评断

根据上述检验结果，对检材邮件的真实性进行综合分析，注意把握以下原则：

a) 检材邮件与其他邮件之间的相互印证关系对于证实其真实性具有较高的价值；
b) 检材邮件与邮件服务器中信息之间的相互印证关系对于证实其真实性具有较高的价值；
c) 对于带有数字签名、邮件客户端结构严密等类型的电子邮件，应考虑进行伪造篡改的技术可行性；
d) 有些异常现象，特别是时间异常，有可能是邮件服务器或用户终端的系统设置所致，应通过对其他邮件的比较，判断其性质；
e) 对于检验中发现的一些存疑现象，应通过实验分析，判断其性质；
f) 注意分析检验结果与检材邮件的形成过程陈述是否存在矛盾。

4 检验记录

与鉴定活动有关的情况应及时、客观、全面地记录，保证鉴定过程和结果的可追溯性。检验记录应反映出检验人、检验时间、审核人等信息。检验记录的主要内容有：

a) 有关合同评审、变更及与委托方的沟通等情况。
b) 检材固定保全情况，包括检材照片或录像、登录网络电子邮箱和提取检材邮件的截图或录像、检材及检材邮件的哈希值等；
c) 检验设备和工具情况；
d) 检验过程和发现；
e) 对检验发现的分析和说明；
f) 其他相关情况。

5 鉴定意见

5.1 电子邮件固定保全及搜索

根据委托要求，对电子邮件的存储位置、状态及接收、发送等信息进行客观描述，并附提取的电子邮件。提取的电子邮件可以为纸质或电子形式，并做好标识。

5.2 电子邮件真实性鉴定

5.2.1 确定经过伪造篡改

判断依据：发现检材邮件存在异常，并分析这些异常为伪造篡改形成。

5.2.2 排除经过伪造篡改

判断依据：未发现检材邮件存在异常，并分析不存在通过现有技术手段无法发现的伪造篡改可能性。

5.2.3 未发现经过伪造篡改

判断依据：未发现检材邮件存在异常或发现的异常能够得到合理解释，但尚不能完全排除存在根据现有技术手段难以发现的伪造篡改痕迹的可能性。

5.2.4 无法判断是否经过伪造篡改

判断依据：检材邮件存在异常，但无法准确判断其性质或形成原因；或，检材邮件信息量过少，无法形成明确性意见；或，其他经综合分析亦无法形成明确性意见。