ICS 07.140
CCS A92

SF

中华人民共和国司法行政行业标准

SF/T 0156—2023
代替 SF/Z JD0402001—2014

电子邮件鉴定技术规范

Technical specification for e-mail forensics

2023－10－07 发布　　2023－12－01 实施

中华人民共和国司法部　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替SF/Z JD0402001—2014《电子邮件鉴定实施规范》，与SF/Z JD0402001—2014相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 文件名称更改为“电子邮件鉴定技术规范”，英文名称更改为“Technical specification for e-mail forensics”（见封面，2014 年版的封面）；
b) 增加了规范性引用文件（见第 2 章）；
c) 删除了术语“电子邮件”“邮件内容”“网页电子邮件服务”“检材”（见 2014 年版的 2.1、2.3、2.5、2.6）；
d) 增加了术语“电子邮箱文件”“电子邮件复本”“样本电子邮件”“电子邮件真实性鉴定”“电子邮件服务器”（见 3.4、3.5、3.7、3.8、3.9）；
e) 增加了第 4 章“设备和工具”（见第 4 章）；
f) 将“鉴定步骤”更改为“鉴定分析”，并更改了内容（见第 5 章，2014 年版的第 3 章）；
g) 更改了检验记录要求（见第 6 章，2014 年版的第 4 章）；
h) 将鉴定意见分类更改为按照存在性和真实性分类（见 7.1 和 7.2，2014 年版的 5.1 和 5.2），并更改了每类鉴定意见的要求。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由司法鉴定科学研究院提出。

本文件由司法部信息中心归口。

本文件起草单位：司法鉴定科学研究院、最高人民检察院检察技术信息研究中心、华东政法大学、上海市人民检察院、广西壮族自治区公安厅、广东安证计算机司法鉴定所。

本文件主要起草人：施少培、李岩、郭弘、李佳、王永全、高峰、陈兴文、魏智煌、卢启萌、耿浦洋、杨恺、李致君、田野、曾锦华、毛晓、凌嵘。

本文件及其所代替文件的历次版本发布情况为：

——2014 年首次发布为 SF/Z JD0402001—2014；
——本次为第一次修订，标准编号调整为 SF/T 0156—2023。

电子邮件鉴定技术规范

1 范围

本文件规定了电子邮件鉴定的设备和工具、鉴定分析过程、检验记录以及鉴定意见的判断依据和推荐表述等内容的要求。

本文件适用于司法鉴定领域中对电子邮件的鉴定。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 29360 法庭科学 电子数据恢复检验规程

GB/T 29362 法庭科学 电子数据搜索检验规程

GB/T 37002—2018 信息安全技术 电子邮件系统安全技术要求

SF/T 0105 存储介质数据镜像技术规程

SF/T 0157 移动终端电子数据鉴定技术规范

3 术语和定义

GB/T 37002—2018界定的以及下列术语和定义适用于本文件。

3.1

邮件客户端 e-mail client

电子邮件客户端

用户终端中安装的发送、接收与管理电子邮件的软件。

3.2

邮件头 e-mail header；message header

位于电子邮件数据的头部，反映电子邮件的基本信息和传送、投递等情况的数据。

注：通常包含电子邮件的接收人、发送人、发送时间、主题、Message-ID和路由过程等信息。

3.3

电子邮件文件 e-mail file

存储单封电子邮件的文件。

示例：RFC 2822 邮件文件（扩展名为.eml）、Microsoft Outlook 导出邮件文件（扩展名为.msg）。

3.4

电子邮箱文件 mailbox file

存储多封电子邮件及其关联关系的数据文件。

示例：Microsoft Outlook 客户端的 PST（Personal Storage Table）文件。

3.5

电子邮件复本 e-mail duplicate

同一封电子邮件客体的不同表现形式或复制件。

示例1：电子邮件在其收发关系的各方均存在至少一个复本。

示例2：备份或归档形成的多个电子邮箱文件中包含同一电子邮件的多个复本。

3.6

检材邮件 questioned e-mail

检材电子邮件

需要鉴定的电子邮件。

注：包含检材邮件的检材一般是电子设备、存储介质或特定邮件地址对应的网络电子邮箱。

3.7

样本邮件 known e-mail

样本电子邮件

用于比较和对照的电子邮件。

注：通常为自然情况下形成或通过模拟实验形成。

3.8

电子邮件真实性鉴定 genuine identification of e-mail

对电子邮件是否经过伪造/篡改进行检验和鉴别的专门技术。

3.9

邮件服务器 e-mail server

电子邮件服务器

为客户端提供邮件应用服务的计算机系统。

注：由服务器硬件、操作系统、支撑系统（Web服务，中间件和数据库）和邮件应用系统组成。

[来源：GB/T 37002—2018，3.2，有修改]

4 设备和工具

4.1 电子邮件鉴定使用的设备和工具应具备的功能包括：

a) 使用邮局协议第3版（POP3）/使用安全套接层的POP3（POP3S）/互联网邮件访问协议（IMAP）/使用安全套接层的IMAP（IMAPS）等协议从电子邮件应用系统获取电子邮件；
b) 将邮件客户端数据或电子邮箱文件解析为单封电子邮件；
c) 从电子邮件中提取和分析邮件头；
d) 存储介质镜像制作和数据提取；
e) 网页数据固定；
f) 域名和IP地址分析；
g) 解码及编码转换；
h) 元数据分析。

4.2 电子邮件鉴定使用的设备和工具宜具备的功能包括但不限于：

a) 利用邮件头中的特定字段建立电子邮件间的关联关系；
b) 时间线建立和分析；
c) 操作系统仿真；
d) 移动终端数据提取；
e) 网络数据包获取及分析；
f) 系统和应用软件日志分析。

5 鉴定分析

5.1 鉴定准备

5.1.1 了解检材邮件/样本邮件形成过程的陈述，包括收发方式、使用的邮件客户端和密送/抄送人等。

5.1.2 若检材为网络电子邮箱，了解登录网址及身份认证信息，并获得其使用授权。

5.1.3 适用时，宜从检材邮件收发关系（如发送、接收、抄送和密送等）中的其他方获取电子邮件复本。

5.1.4 为检材及检材邮件/样本邮件指定唯一性编号。

5.2 存在性鉴定

5.2.1 固定保全

5.2.1.1 对于包含检材邮件的存储介质，应按照SF/T 0105的规定制作存储介质镜像。不具备制作镜像条件的，可直接提取其中的电子邮件文件、电子邮箱文件及其他相关数据，并全程录像。

5.2.1.2 对于包含检材邮件的移动终端，应按照SF/T 0157的规定提取其中的电子邮件。

5.2.1.3 对于网络电子邮箱，应按照以下步骤固定、提取检材邮件/样本邮件及其他相关邮件：

a) 使用屏幕录像软件启动屏幕录制，或使用数字摄像机拍摄屏幕显示内容；
b) 从可信时间源获取当前时间；
c) 必要时，对电子邮件域名信息或邮箱注册信息进行固定；
d) 登录电子邮箱，查看邮箱基本信息和设置；
e) 在 Web 界面搜索、过滤找到电子邮件并下载为电子邮件文件或电子邮箱文件，或借助专用工具使用 POP3/POP3S/IMAP/IMAPS 等协议下载电子邮件；
f) 若邮件附件与电子邮件分离保存，及时下载邮件附件文件；
g) 计算下载文件的完整性校验值；
h) 再次获取当前时间后，结束屏幕录制或摄像机拍摄。

5.2.1.4 固定保全过程中不应删除、修改电子邮件，或执行其他可能影响电子邮件真实性的操作。

5.2.1.5 必要时，可对邮箱设置（如协议开启情况）、日志记录（如登录日志、收发日志和删信日志等）、邮件状态（已读/未读、标签）等内容进行固定。

5.2.1.6 必要时，可使用网络数据包捕获的方式进行固定。

5.2.1.7 若固定保全过程中修改了邮箱设置，应记录修改并在固定保全结束后还原设置。

5.2.1.8 固定保全过程形成的存储介质镜像、电子邮件文件、电子邮箱文件及录像文件应计算完整性校验值，用于后续检验和分析的数据应使用复制件。

5.2.2 数据恢复和搜索

5.2.2.1 应按照 GB/T 29360 的规定，恢复保存在存储介质中的电子邮箱文件、电子邮件文件及其他相关的文件或数据，恢复电子邮箱文件中的已删除电子邮件。

5.2.2.2 应按照 GB/T 29362 的规定，选择适当的关键字，搜索电子邮件及其他相关文件或数据。

5.2.3 数据处理和保存

5.2.3.1 必要时，可建立电子邮件之间的关联，或以适当方式分类、索引和编排，以直观展示相互关系。

5.2.3.2 必要时，可利用电子邮件中的时间信息建立时间线。

5.2.3.3 作为结果提交给委托方的电子邮件宜使用便于浏览的格式输出保存。

5.3 真实性鉴定

5.3.1 总体要求

电子邮件真实性鉴定应关注检材邮件在发送接收全路径上的相关痕迹。根据鉴定需要，应在5.3.2至5.3.10中列出检验项目中选择部分或全部内容进行检验和分析，然后按照5.3.11进行综合分析。

5.3.2 基本信息检验

应检验电子邮件的结构、格式、内容、收发方、时间和数字签名等信息及其与电子邮件服务提供者的符合性。

5.3.3 邮件客户端检验

根据电子邮件服务提供者和邮件客户端的特点，应选择以下内容中的1项或多项进行检验：

a) 检材邮件的结构、格式和属性等信息与邮件客户端的符合性；
b) 邮件客户端所在操作系统中与检材邮件相关的备份数据；
c) 邮件客户端所在操作系统中与检材邮件相关的日志和缓存等其他数据。

5.3.4 邮件头检验

提取检材邮件的邮件头进行检验，检验的内容应包括但不限于：

a) 邮件头各个域的布局和顺序；
b) 明文时间、时区信息和经过编码的时间信息；
c) Received 等域反映的电子邮件传输路由信息；

d) 邮件客户端信息；
e) 来源 IP 地址；
f) 邮件地址、域名或 IP 地址的有效性；
g) 代发和代收情况；
h) 基于域的邮件身份验证、报告和符合性（DMARC）、发件人策略框架（SPF）以及域名密钥识别邮件（DKIM）等电子邮件安全机制。

5.3.5 邮件内容检验

应检验电子邮件内容的多用途互联网邮件扩展（MIME）结构、内容布局与衔接、落款等方面的信息是否存在异常。

5.3.6 邮件附件检验

应检验检材邮件附件的元数据和结构等信息是否存在异常。宜重点关注附件的时间和作者等信息及其与其他来源相近的文件的关联性。

5.3.7 关联邮件检验

应检验5.2.3.1中的关联邮件，必要时宜按照5.2.2.2搜索更多关联邮件，分析相互之间的逻辑关系是否存在矛盾。

5.3.8 时间线检验

宜检验5.2.3.2中的时间线，分析各事件之间、事件与了解到的检材邮件形成过程之间是否存在矛盾。

5.3.9 样本收集及检验

应收集同一邮箱中其他邮件或通过实验收集相近场景下收发的电子邮件作为样本邮件，与检材邮件进行比较检验。

5.3.10 邮件服务器检验

在获得授权的情况下，应检验邮件服务器中的电子邮件数据、服务器日志、数据备份和审计记录等相关信息。

5.3.11 综合分析

5.3.11.1 宜通过设计实验模拟、与其他邮件的比较等方式，评价检材邮件特征与正常邮件特征的符合和差异情况。

5.3.11.2 应分析检验发现的印证关系，包括但不限于：
a) 检材邮件与其他电子邮件之间的相互印证；
b) 检材邮件与其电子邮件复本的相互印证；
c) 检材邮件与其他相关信息的相互印证。

5.3.11.3 应对检验发现的矛盾、异常或存疑点进行逐一分析，评判其成因。

示例1：邮件服务器和用户终端的时间不同步可能导致时序错乱，可通过与同期邮件的比较进行评判。

示例2：电子邮件系统版本更迭可能导致不同时期的邮件头结构发生变化，可通过与不同时期邮件的比较进行评判。

6 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。检验记录宜包括以下内容：

a) 检验时间、检验人员和审核人员；
b) 电子邮箱或服务器的身份认证信息及其授权和使用记录；
c) 检材邮件形成过程的关键点；
d) 固定保全过程中形成的照片、录像、数据文件及其完整性校验值；
e) 使用工具检验的检验过程和发现；

f) 对检验发现的分析；
g) 鉴定人员认为有必要记录的其他相关情况。

7 鉴定意见

7.1 存在性鉴定

应对电子邮件的存储位置、状态及委托要求所涉及的关键信息进行客观描述，并将提取的电子邮件采用便于浏览和打印的格式作为检验结果提供。若电子邮件附件独立存储，应注明电子邮件附件与电子邮件的对应关系。

7.2 真实性鉴定

7.2.1 鉴定意见分类

电子邮件真实性鉴定的鉴定意见应在以下4类中选择：
a) 确定经过伪造/篡改；
b) 排除经过伪造/篡改；
c) 未发现经过伪造/篡改；
d) 无法判断。

7.2.2 确定经过伪造/篡改

7.2.2.1 判断依据：检验发现检材邮件存在异常，并分析异常为伪造/篡改形成。
7.2.2.2 鉴定意见宜表述为“检材邮件经过伪造/篡改。”若无法确定改动的性质，可使用“修改”替代“篡改”的表述。

7.2.3 排除经过伪造/篡改

7.2.3.1 判断依据：对 5.3 中所列项目进行了全面、充分的检验和分析，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。
7.2.3.2 鉴定意见宜表述为“检材邮件排除经过伪造/篡改。”

7.2.4 未发现经过伪造/篡改

7.2.4.1 判断依据：对 5.3 中所列项目进行了全面、充分的检验和分析，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。
7.2.4.2 鉴定意见宜表述为“未发现检材邮件经过伪造/篡改。”

7.2.5 无法判断

7.2.5.1 判断依据应满足以下条件之一：
a) 综合各项检验结果，所提供的信息仍然不足；
b) 检验发现了矛盾或异常，但无法准确判断其性质或形成原因；
c) 由于客观条件所限导致检验无法进行或难以得出明确意见。
7.2.5.2 鉴定意见宜表述为“无法判断检材邮件是否经过伪造/篡改。”

参 考 文 献

[1] GB/T 37234—2018 文书鉴定通用规范
[2] GB/T 37238—2018 篡改（污损）文件鉴定技术规范
[3] GA/T 756—2021 法庭科学 电子数据收集提取技术规范
[4] GA/T 1172—2014 电子邮件检验技术方法
[5] SF/T 0123—2021 录像真实性鉴定技术规范