# 电子邮件取证中的关键问题

江 璜[1],陈海凌[2]

(1.汕头职业技术学院 计算机系,广东 汕头 515041;
2.汕头市龙湖区人民法院,广东 汕头 515000)

**摘 要**:首先分析了电子邮件证据的特点,然后针对涉及电子邮件的案件中争议较多的焦点,提出解决电子邮件取证中的几个关键问题的方法,即如何确定邮件的发送者、邮件到达时间以及确认收到邮件。

**关键词**:电子证据;数字取证;电子邮件取证;邮件头

**中图分类号**:TP393.098 **文献标识码**:A **文章编号**:1674-7720(2013)01-0042-03

## Key problems in email forensics

Jiang Huang[1], Chen Hailing[2]

(1.Department of Computer, Shantou Polytechnic, Shantou 515041, China;
2.People's Court of Shantou City Longhu District, Shantou 515000, China)

**Abstract**: This paper firstly analyzes the characteristics of email evidence. Then, according to the focus in some email cases, it puts forward the methods to solve key problems in email forensics, such as how to identify the sender of the email and email arrival time, how to confirm the receipt of email.

**Key words**: electronic evidence; digital forensics; email forensics; email header

2011年,十一届全国人大常委会第二十三次会议初次审议了《中华人民共和国民事诉讼法修正案(草案)》。新修正的草案规定,将在第六十三条证据种类中新增"电子数据"。这意味着电子邮件、QQ聊天记录、微博等电子数据都将作为一种独立证据正式成为呈堂证供。其实随着信息技术的发展,在近年出现的不少继承纠纷、名誉权纠纷、合同纠纷等民事案件中,已经有很多客观事实正是通过电子证据反映出来的,其中,电子邮件证据尤为常见。因此,作为数字取证的一个重要分支,电子邮件取证的技术应用及相关法律法规问题成为当前研究和讨论的热点。

我国司法实践中广泛地使用电子证据这一概念,其涵盖的范畴包括任何以电子形式存储、处理、传输的证据。电子邮件作为一种重要的电子证据,具有如下不同于普通证据的两个重要特点。

(1)技术性。电子邮件的产生、存储、传输及其采集、分析和判断都必须借助计算机技术与网络通信技术。

电子邮件证据的技术性要求取证人员应当了解或通晓计算机技术,以便于及时采取相应的技术方法收集证据,排查案情。电子邮件证据的技术性,还要求在涉及相关软件的使用等问题时,应指派或聘请技术专家进行协助或鉴定。

(2)脆弱性。由于电子邮件数据可以被修改、伪造、删除,这使电子邮件证据具有脆弱性,因此使用电子邮件证据的同时通常还需要结合其他证据才能进行裁定。

电子邮件是以电子元件和磁性材料为物质载体的二进制数字,存储在计算机等电子设备上。行为人可以通过技术手段对电子邮件数据进行修改、伪造或者删除。日益普及的网络环境和快速的数据通信传输又为操纵计算机提供了更为便利的机会,使得变更、毁灭电子邮件证据也更加方便。这一特点给电子邮件证据的审查判断带来不少技术上的困难。

在不少涉及电子邮件的案件中,争议较多的往往不是针对邮件内容本身,而是否认自己是邮件的发送者;在时效性要求比较高的场合,质疑电子邮件的发送接收时间;或者无法确认是否收到邮件。由于非专业人士要

篡改电子邮件并不容易，只要取证过程合法可行，比如通过申请法院保全或者通过公证，就可以认定取得的电子邮件证据真实可靠，也就是能证明邮件由A发送给B，并且邮件内容真实。但如何把网络中的ID（A或B）和现实中的行为人联系起来呢？在电子邮件取证中，要解决的关键问题就是如何确定邮件的发送者、邮件到达时间以及确认对方已收到邮件。

## 1 确定邮件发送者

要确定发送者，根据发送者使用的邮箱地址，分以下3种情况。

### 1.1 实名认证邮箱

如果邮件使用的是实名认证的邮箱，那该邮箱的真实用户资料在邮件服务器端有备案。只要核对邮件服务器上的真实用户名、邮箱账号和密码等资料就可以确定邮件的发送者了。如果用户否认，根据“谁主张谁举证”的原则，则必须提供邮箱被盗用的相关证据，否则就可以认定其为该邮箱的拥有者，应为以该信箱收发电子邮件的行为负责。

### 1.2 免费邮箱或公共邮箱

现在很多人都使用免费的电子邮箱，虽然这些电子邮箱在申请时要求输入基本的信息，并对其进行记录，但由于不是实名认证，邮箱的提供者很少对提供的信息的真实性进行确认，因此记录的很多信息往往是虚假的。如果获取到的电子邮件使用一个免费的电子邮箱，那仅依据其在邮件服务器登记的用户信息并不能确定收发者。对于使用公共邮箱的用户，或者开放自己的电子邮箱者，更加难以认定其使用者。

这时，应该分析邮件头。一般情况下，电子邮件常用信头字段内容如表1所示。

表1 电子邮件常用信头字段

| 字段名称 | 描 述 | 字段名称 | 描 述 |
|---|---|---|---|
| From | 信件发信人 | Date | 信件创建日期 |
| Sender | 信件发信人 | Received | 信件MTA轨迹 |
| Reply-to | 发信回复地址 | Return-path | 发信人地址 |
| To | 信件主收信人 | Subject | 信件主题 |
| Cc | 信件辅收信人（抄送） | Comments | 关于信件的其他说明 |
| Bcc | 信件的密件抄送收信人 | Keywords | 信件主题关键字 |
| Message-id | 信件唯一标识符 | Encrypted | 加密信息 |
| Status | 由MUA插入标识是否信件状态（是否新信件、已阅读、回复等） | X-* | 信件扩展字段，由开发者创建的非标准字段 |

从邮件头中可以查看邮件收发者及邮件服务器的IP地址、发送及接收时间，然后根据邮件服务器和ISP上的日志记录，查看在相应时间使用此地址发送邮件的机器的物理位置。再结合以往与该邮箱的邮件往来历史记录，最终确定发送者。

### 1.3 匿名或伪造的邮箱地址

如果发送者使用Open Relay、Open Proxy以及匿名E-mail等技术来隐藏其真实的邮箱地址，那就需要更专业的技术来查找发送者。

开放Open Relay功能的邮件服务器不理会邮件发送者或邮件接收者是否为系统所设定的用户，而对所有的入站邮件一律进行转发（Relay）。发信者在发送电子邮件的时候，就会选择这种开放功能的邮件服务器作为中转服务器，从而隐藏发送者的个人信息。

Open Proxy是网络信息传递的中间代理，当Proxy没有对使用者及TCP端口作相应的限制时，很容易被利用作为跳板来连接另外一台邮件服务器的25端口，并通过发送特定的SMTP指令就可以实现使用Open Proxy发送邮件并隐藏自己。这种方式经常被利用来发送大量的垃圾邮件。

使用Advanced Direct Remailer、ghostmail等软件或登录到一些提供匿名发送邮件的网站上，可以发送匿名邮件或伪造一个虚假的发送人邮箱地址。这时接收方收到的邮件上没有任何发件人信息或者只能看到一个伪造的地址。

对于以上这些使用匿名或伪造邮件地址手段来发送的邮件，仍然可以从邮件头入手。通过Open Relay服务器或采用匿名Email软件发送的电子邮件中仍包含真正发送者的IP地址信息，可以结合邮件服务器和ISP的记录定位其物理位置和使用时间。对于使用Proxy而不能直接得到发送者IP地址的，可以逐级回溯到代理服务器上，在其日志文件中查找线索。

## 2 确定邮件到达时间

时间因素是取证分析和案件审理过程中判定事件、犯罪行为发生情况的重要依据。一般在电子邮件头中就有邮件创建和接收的时间，邮件接收时间即为到达时间。邮件从发送到接收一般以秒为单位，但是还需要考虑当时网络线路等因素。当邮件到达时间成为区分当事人双方权利义务的界限时，到达时间的确认就特别重要。收发者可能会故意改动时间以期维护自己的经济利益。发生争议时，比较可行的方法是不以接收人计算机内储存的电子邮件时间为准，而以邮件服务器所显示的时间为准，因为邮件服务供应商通常是独立的第三方，由其出具证明更为公平和真实。所以，将来关于电子签名的立法应当指明，凡邮件收发方要求邮件服务供应商对接收时间出具证明的，邮件服务供应商应当予以配合。

另外，还应注意邮件服务器本身的时间误差。服务器的时间应当定期调校，力求准确。建议在立法上，应当将定期调校服务器时间列为邮件服务商的法定义务之一。如果邮件服务器是在国外的，到达时间实际为国外时间，这时则要注意进行时差换算，以换算后的时间为到达时间。如果中间经过很多邮件中继的，应根据邮件头部的信息逐个追踪邮件所经过的中间节点，确定到达

时间。

3 确定已收到邮件

“收到”这一概念，在电子商务贸易过程中，具有相当重要的法律意义。国际货物销售公约和大陆法规定，不论是发盘还是接收，均以抵达接收人或发盘人作为生效的条件之一。而英美法则规定，信件或电报一经发出，立即生效，生效的时间以投递邮件收据上邮局所盖邮戳为准，而不管对方是否收到。在电子商务环境中，为避免贸易纠纷，确定了“收到生效”的原则，也就是说，不论什么传递，只有对方收到才具有法律意义。如果采用电子邮件传输，那电子邮件只有被对方收悉才有意义。

电子邮件的传输速度很快，如果遇到线路故障或其他因素的干扰，就可能造成延迟或发送失败。在这种情况下，发件人以为收件人已经收到该电文，而收件人却并不知道发件人给自己发了邮件以及所发邮件的内容。为了解决这个问题，《示范法》第 14 条建立了“确认收讫”概念，类似于邮政系统的“回执制度”。确认收讫可通过系统设计自动回复以确认邮件确实到达了目标信箱，也可以要求由收件人直接回复邮件或发送阅读回执，以确认邮件已被收到并阅读。按照我国《电子签名法》第 10 条的规定，是否需要特定的程序和以何种程序对数据电文的传递予以确认收讫，完全取决于双方当事人的协商。即使法律、行政法规特别规定应该确认收讫的，双方当事人也可以通过约定的方式予以改变。但一旦约定需要确认收讫，或者在法律、行政法规规定需要确认收讫的情况下，收件人应该在一定的期限内按照规定的或者约定的程序向发送人发出确认，否则，发送人将认为数据电文未被收到，并有权否定该项电文的效力。

目前，虽然我国尚无完整规范电子证据、数字取证方面的法规，司法机关的设备也尚无法满足审理此类案件的物质需要，但是，电子邮件等电子证据所带来的法律问题却已实实在在地摆在了我们的面前。与其他法规相比，电子证据的法规需要结合计算机科学、法学、刑侦学等各学科的专业知识，这就给立法、司法提出了更高的要求。借鉴国外相关法律法规制定并完善适合国情的电子证据法律势在必行，任重道远。

参考文献

[1] 杨泽明，刘宝旭，许榕生.电子邮件取证技术[J].信息网络安全，2002(6)：33-34.

[2] 电子证据的固定采集与展示业务操作指引[EB/OL].http://www.sdlawyer.org.cn/doc/201202/9a2937b2-603a-4372-bbb1-1237363341 98.htm，2009-08-15.

[3] 孙国梓，耿伟明，陈丹伟，等.电子数据取证的可信固定方法[J].北京工业大学学报，2010，36(5)：621-626.

[4] 电子合同中电子邮件应用的法律问题研究[EB/OL].http://www.topoint.com.cn/html/article/2005/06/174378_5.html，2005-06-17.

[5] 程伟杰.关于电子邮件证据问题的探讨[J].档案，2007(5)：5-7.

（收稿日期：2012-07-11）

作者简介：

江璜，女，1979 年生，硕士，主要研究方向：计算机网络应用。