ACCCF / 应用知识库

08

卷

保存可验证的内容和语境

西班牙语版 · 2026

电子邮件、在线出版物和社交媒体内容认证手册

EML、邮件头、URL、文件、出版物、可追溯性和呈现

在消息或发布内容消失之前保存可供复核的材料，不把截图当作数据源，也不把屏幕上的日期当作来源证明。

适用于律师、鉴定人、合规、传播和调查人员，以及需要保存电子邮件、出版物或在线对话的人。公证、司法鉴定或行政认证取决于所在地域和程序。

编辑统筹：Jocsan Laguna · 美国网络安全与计算机取证委员会

通用技术指南和开放教育材料。不构成法律意见、专家鉴定意见，也不构成未经授权访问系统的操作指导。示例和数据均为虚构；图示为编辑重构。

目录

可见页码对应 PDF 版本。Word 打开文档时可能会更新此索引；标题保留内部导航。

前言：在变化前保全 3

第1章 范围与准备 3

- **1.1 需要证明的主张** 3
- **1.2 准备捕获环境** 4

第2章 完整消息 4

- **2.1 EML：正文、邮件头和附件** 4
- **2.2 转发、下载和转换** 5
- **2.3 附件与第三方交付** 5

第3章 渠道认证 6

- **3.1 Received 邮件头与传输** 6
- **3.2 DKIM、SPF 和 DMARC** 6
- **3.3 日期、Message-ID 与内容** 7

第4章 文件、URL 和出版物 8

- **4.1 URL 的完整记录** 8
- **4.2 发布、会话线程和多媒体** 8
- **4.3 网络存档和第三方日期** 8

第5章 保全与记录在案的认证 9

- **5.1 取证获取记录** 9
- **5.2 保管和访问控制** 10
- **5.3 司法鉴定、公证或行政认证** 10

第6章 撤回、举报与媒体损害 10

- **6.1 撤回前先保全** 10
- **6.2 损害与范围** 10
- **6.3 综合案例** 11

附录A 保全格式 11

- **A.1 邮件记录** 11
- **A.2 发布记录** 11
- **A.3 对象清单文件** 12
- **A.4 撤回申请记录** 12

附录B 法律框架与最终清单 12

前言：在变化前保全

出版物可能被编辑，账户可能关闭，附件可能被替换，链接可能失效。保全旨在记录某个时刻存在什么、位于何处、如何取得，以及留下的是哪种表现形式。截图可以显示片段，但复核需要完整对象及其语境：URL、账户、日期、时区、文件、回复、元数据和获取过程。

电子邮件是一个清楚的例子。如果只保存消息图像，就会丢失邮件头、结构和附件。如果只保存附件，就会丢失解释其内容的声明，有时还会丢失可用于验证的哈希值。EML 汇集这些组件并建立关联，但不能证明其中的全部陈述真实，也不能证明某个具体的人写了正文。

这里的“认证”是指记录在案的过程，不是普遍保证。公证行为、司法鉴定、保存证明和见证截图可能具有不同功能和效力。保全人员必须说明自己做了什么、能够证明什么，不能用庄严措辞掩盖不完整的数据源。

> **黄金规则**
> 同时保存内容和语境。一张清晰但没有 URL 和日期的出版物截图只是有用的参考，不是对对象的完整重建。

第1章 范围与准备

1.1 需要证明的主张

证明出版物存在、由某账户发布、由某人撰写、曾向公众开放、含有威胁，或交付了某个具体文件，并不是同一项任务。主张决定数据源：可见出版物、导出文件、EML、平台日志、接收方、管理员或证人。如果只需证明其在某日存在，就不得把分析扩大为作者身份判断。

应界定时间段、账户、URL、关键词、参与者、内容类型和第三方数据，还应明确保全用于举报、撤回、诉讼、内部调查还是存档。保全的紧迫性并不消除授权要求和保护第三方的必要性。

目标	优先数据源	应声明的局限
出版物存在	URL、内容、页面和有记录的保全。	不能证明自然人作者身份，也不能证明账户的全部内容。
邮件内容	包含正文、邮件头和附件的 EML。	不能证明文本内容真实。
文件交付	附件、正文、哈希值、下载和清单文件。	不能证明源系统的覆盖范围。
公开范围	可见性、受众、链接和访问证据。	不等于实际读者人数。

目标	优先数据源	应声明的局限
作者身份或控制	账户、会话、设备和语境。	可见名称不能识别个人。
序列	日期、时区、回复、编辑和引用。	孤立截图无法还原完整历史。

1.2 准备捕获环境

应使用经授权的设备和账户，记录日期和时区，使用已知浏览器并控制存储。避免使用个人账户登录，以免向证据添加不必要的数据。与出版物的交互应限于必要范围：回复、举报或分享可能改变其覆盖范围并通知作者。

应分别准备原始文件、工作副本、截图、导出文件、日志和清单文件目录。潜在非法或有害内容不得分发给整个团队。应记录其存在并通过受限渠道交付。如果某人面临风险，首要任务是保障其安全并联系主管渠道，而不是追加技术证明。

> **事先决策**
> 如果出版物可能消失且已有保全授权，应先记录对象及其语境，再申请撤回或复核。先撤回后保全，可能只留下没有数据源支持的断言。

第2章 完整消息

2.1 EML：正文、邮件头和附件

RFC 5322 描述互联网消息格式，包括邮件头字段和正文。EML 可以保存包含这些组件及附件的邮件表现形式。应记录取得方式：客户端导出、服务器下载或他人交付。来源会改变解释，不能用常见扩展名掩盖。[1]

在使用可能修改文件的工具打开之前，应先保存文件。分别计算 EML 和附件的哈希值并记录在清单文件中。正文可能声明某个文件的算法和值，应进行核验，而不是把值抄到单独备注中。如果存在差异，应保留首次交付并要求澄清。

[1] RFC Editor. RFC 5322, Internet Message Format：消息结构、邮件头和正文。这是保存和理解电子邮件的技术参考，并不能自动证明人的身份。 官方在线来源

2.2 转发、下载和转换

转发邮件可能增加邮件头并改变消息与文件的关系。打印为 PDF 只能保存可视化内容，不能保存结构。通过网页邮件下载可能产生不同格式。每项操作都应记录并保存各版本，不能把转发件当然地视为原始消息。

转发的消息仍可作为某人在某日收到内容的有效证据，但先前内容应结合邮件头和其他来源分析。如果目标是证明某个文件的交付，供应商原始 EML 比转发截图更可取。如果无法取得，应声明该局限，并在其他邮箱或服务器中查找消息。

表现形式	保留的内容	需要补充的内容
原始 EML	正文、邮件头和可用附件。	来源和内容验证。
转发的 EML	新的交付和先前内容的呈现。	转发历史和先前来源。
邮件 PDF	版式和可读文本。	邮件头、附件和结构。
截图	屏幕上显示的片段。	URL、账户、日期、语境和文件。
仅附件	单个文件的数据。	消息、声明、关系和过程。

2.3 附件与第三方交付

不得为了便于阅读而在保全前编辑或转换附件。应计算哈希值，检查是否与声明值一致，并记录打开情况和覆盖范围。如果 CSV 能打开但缺少字段字典，应申请字段含义。哈希值只能证明两个比较对象一致，不能证明行完整或真实。

> **虚构案例**
>
> 供应商交付一个 CSV 和一个 PDF，并在邮件正文中分别给出哈希值。CSV 一致，PDF 不一致。应保留全部材料，要求重新交付 PDF，并记录 CSV 与声明一致，但不得声称供应商的内容完整。第二次交付使用另一个标识符，不替代第一次。



图1 EML、附件和声明：相互关联的对象。完整性分别对应不同对象。编辑重构；不构成真实证据。

第3章 渠道认证

3.1 Received 邮件头与传输

Received 字段提供一组声明的服务器、日期和传输数据。应按消息结构定义的顺序审查，不能默认所有字段都可靠，也不能把第一个可见字段当作自然人来源。有些字段可能由中间系统添加。分析应比较服务器、时间、域名和其他认证结果。

可见的 From 地址可能与经认证域名或发送服务器不一致。邮件头中的 IP 可以识别基础设施，不能识别个人。日期可能取决于不同时钟。分析不能把复杂邮件头当作神奇证据，而应说明哪些组件可验证、哪些依赖信任。

3.2 DKIM、SPF 和 DMARC

DKIM 通过密码学签名将域名与消息关联，并允许验证已签名的组件。SPF 在协议范围内公布哪些主机获域名授权；DMARC 提供域名对齐和策略。这些机制有助于评估渠道和域名，但不能证明由谁撰写文本或文本是否真实。失败也可能需要检查转发、配置或转换。[2][3]

[2]RFC Editor. RFC 6376, DomainKeys Identified Mail (DKIM) Signatures：域名责任和已签名组件的密码学验证。它本身不能证明由谁撰写文本或内容是否真实。 官方在线来源

[3]RFC Editor. RFC 8616 及 SPF RFC7208、DKIM RFC6376 和 DMARC RFC7489 技术参考：主机授权、域名签名、对齐和策略。它们有助于评估渠道，但本身不能证明自然人身份或内容真实性。 官方在线来源

报告应在可用时记录域名、选择器、已签名字段、结果、日期和查询来源。不能只写“DKIM pass”就当作个人身份识别。“SPF fail”也不能单独证明恶意伪造，必须检查传输路径和配置。技术分析应保留原始消息供他人核验。

3.3 日期、Message-ID 与内容

Message-ID 有助于关联消息和系统，但其唯一性和结构取决于生成器。日期应连同所在时区按原样保存，并与服务器日志和接收事件比较。下载日期不是发送日期，附件日期则属于另一层。

陈述	可以核验什么	不能据此推出
经认证的域名	签名、对齐和渠道配置。	自然人撰写了该消息。
发送日期	邮件头和日志一致。	文本是在同一时刻创建的。
收到消息	邮箱、EML 和服务器日志。	某人已阅读或理解。
内容真实	叙述事实的独立数据源。	DKIM 或哈希值证明事实。
账户失陷	会话、恢复和异常活动。	不同地址本身即证明被盗。

解读规则

邮件头用于分析传输和域名，不是个人供述。作者身份需要额外印证。



图2 解读邮件头，但不将其当作自然人身份识别。传输、域名和内容线索。编辑重构；不构成真实证据。

第4章 文件、URL 和出版物

4.1 URL 的完整记录

应保存完整 URL、参数、域名、日期和时区、可见账户、访问类型、角色、语言、浏览器版本和页面状态，并记录是否发生重定向、登录、地域限制或错误。URL 地址不变时内容也可能改变，因此必须同时保存对象和获取过程。

截图应包含足以识别页面的语境，但不得暴露不必要的数据。在有用且合法时，还应保存 HTML 文件、多媒体资源和原生导出文件，并说明哪些内容无法取得。动态页面可能向每位访问者显示不同内容，报告不得将其概括为所有访问者共同的视图。

4.2 发布、会话线程和多媒体

应保存文本、表面作者、出版物标识符、可见日期、URL、相关回复、引用、转发、回应和多媒体。回复顺序可能因算法或审核而变化。捕获会话线程时，应记录浏览路径和覆盖终点。脱离语境的一条回复可能歪曲整个对话。

经授权后下载图像或视频文件，并分别计算哈希值。出版物与文件应在清单文件中关联。如果研究内容真实性，应使用专门的多媒体分析卷册；保全只能证明该版本在该数据源和时点可用。

4.3 网络存档和第三方日期

第三方存档可能保存有用快照，但其日期属于存档捕获时间，不一定属于首次发布时间。应记录由谁存档、捕获哪个版本、缺少哪些资源以及如何查询。内容中的日期可能被作者编辑，也可能采用其他时区。印证应查找相近时间的出版物、通知、链接和日期记录。

要素	必要记录	局限
URL 和重定向	完整地址和访问序列。	内容会变化或个性化。
发布和会话线程	标识符、文本、回复和捕获范围。	覆盖范围有限时，不代表整个对话。
多媒体	文件、质量、哈希值和来源。	不能证明场景真实性或作者身份。
外部存档	保管人、快照、日期和缺失资源。	不能证明首次发布或内容完整。
访问	账户、角色、可见性和限制。	并非所有用户都看到相同内容。

呈现规则

不得用网络存档声称“一直如此”，也不得用截图声称“这就是全部”。应描述实际能够证明的版本、日期和覆盖范围。



图3 出版物与其环境一并保存。截图是一种表现形式，不是全部内容。编辑重构；不构成真实证据。

第5章 保全与记录在案的认证

5.1 取证获取记录

取证记录应标识案件、操作员、授权、地点、日期和时区、设备、浏览器或工具、账户和角色、获取对象、操作、格式、异常情况和哈希值。如果捕获屏幕，应记录路径和筛选条件；如果导出，应记录参数和输出；如果使用供应商，应保存答复和渠道。记录必须描述实际实施的操作，而不是未发生的理想流程。

保存证明可以补充完整性和可访问性证据。在墨西哥，NOM-151 对其范围内的数据电文保存和数字化有具体要求；它不能证明内容真实性，也不能替代完整消息的获取。时间戳或哈希值不能证明自然人作者身份或获取合法性。[4][5]

[4]NOM-151-SCFI-2016，数据电文的保存和数字化，发布于 30-03-2017。关于记录、完整性、可访问性和电子数字指纹的要求。 官方在线来源

[5]经济部。PLATIICA。NOM-151-SCFI-2016 数据电文保存和数字化条目。用于核实现行效力，并作为 DOF 文本的补充参考。 官方在线来源

5.2 保管和访问控制

数据源应与工作副本分开并限制访问。电子移交应记录接收方、权限、日期、版本、密钥交付渠道和下载验证。报告不得包含密码、令牌或 cookie。如果保存需要认证的页面，应记录角色但不得暴露会话。

工作副本用于分析、匿名化和展示。公开版本应复核，避免出现个人数据、私密图像、住址和无关第三方。不得为了制作删减版而销毁完整的保存版本；完整版本的访问和后续使用应受到限制。

5.3 司法鉴定、公证或行政认证

选择取决于法域、对象和目的。公证行为可以记录一次查看；司法鉴定可以分析来源、结构、真实性、关系和语境；行政证明可以确认其范围内的行为。这些形式都不能把片段变成完整证据。开始前就应申请适当形式，避免在可能变化的页面上重复操作。

> **质量标准**
> 最好的认证不是印章最多的认证，而是能让他人了解看到了什么、在哪里、何时、用何方法，以及哪些内容被排除的认证。

第6章 撤回、举报与媒体损害

6.1 撤回前先保全

申请撤回内容之前，应保存 URL、标识符、出版物、账户、多媒体、回复和访问日期，还应记录已经变化的版本和参考链接。如果存在直接威胁，应优先考虑安全和紧急渠道，不得为了保全而造成危险延误。

向平台提交的报告必须具体：对象、URL、理由、证据、日期和请求。不得包含超出必要的个人数据，也不得把有害文件发送到非指定渠道。应保存报告编号、内容、日期和答复。链接被删除不能证明所有副本都已消失，也不能证明损害已经停止。

6.2 损害与范围

分析应区分内容、再发布、可见范围、回应和声明的后果。平台计数器可能含义不同，不能证明具体读者或全部影响。指标应连同日期和已知含义保存。不得在没有依据的情况下用曝光量推算经济损害。

媒体损害评估可能需要证言、工作文件、合同、沟通记录和其他非数字数据源。技术保全证明内容和序列，不能证明全部损害。报告不得虚构匿名账户的所有者，也不得根据出版物语气推断其意图。

6.3 综合案例

一则虚构出版物包含一项指控和多条回复。应保存可用会话线程、文件和带日期的指标。随后，账户修改文本并删除一条回复。第一个版本连同其局限保存，新版本作为关联对象保存。分析应比较变化而不抹去历史。撤回申请也应记录，但报告不得声称内容已停止在其他账户传播。

> **启示**
>
> 媒体损害证据需要版本和语境共同构建。最终截图显示的内容可能比最初更少，但最初截图也不能证明全部过程。

附录A 保全格式

A.1 邮件记录

虚构记录

```
案件/对象：EXP-DEMO-2026-008 / EML-001-R00
来源：[邮箱、服务器、客户端或第三方]
获取：[导出、下载或交付]
表面发件人和收件人：[记录]
消息日期和时区：[原始值]
获取日期和时区：[原始值]
正文和声明：[参考、算法和哈希值]
邮件头：[完整文件]
附件：[名称、大小、格式和哈希值]
认证：[DKIM / SPF / DMARC（如已审查）]
验证：[一致和差异]
异常情况：[格式、缺失、错误或局限]
保管：[原件、工作副本和访问]
```

A.2 发布记录

字段	最低内容要求	控制
URL 和标识符	完整地址、参数和重定向。	对象可定位。
账户和可见性	表面作者、角色、访问和可见受众。	不得自动归属。
日期	可见日期、获取日期、时区和精度。	不得混淆发布和下载。
内容	文本、回复、回应、多媒体和版本。	会话线程的覆盖范围。
过程	工具、版本、筛选条件和操作。	可重复性。
文件	HTML、图像、视频、导出和哈希值。	原始材料/派生对象关系。
异常情况	错误、访问、内容缺失和局限。	不得隐瞒覆盖范围。

A.3 对象清单文件

交付清单

ID / 原始名称 / 对象类型
来源和关系：[原始文件、导出文件、派生对象]
接收日期和时区
方法和工具/版本
大小和格式
对象的算法和哈希值
父对象和关联对象
打开和验证
敏感数据和限制
保存位置和工作副本
移交和接收方
局限和待解决事项

A.4 撤回申请记录

虚构格式

平台和渠道：[官方]
URL / 出版物 / 账户：[具体对象]
理由和所附证据：[标识符]
请求：[撤回、复核、保全]
日期和时区：[发送]
报告编号：[参考]
答复：[日期、内容和行动]
其他已知副本：[URL 和状态]
与受影响者沟通：[渠道和版本]
待解决事项：[覆盖范围和后续复核]

附录B 法律框架与最终清单

墨西哥在 CCom 89–94 和 1205 中承认数据电文；CFPC/CNPCF 按过渡情况发展可靠性、归属和完整性；NOM-151 规范其范围内的保存。秘鲁区分签名、程序和档案；智利区分签名和日期；阿根廷强调可

靠性；哥伦比亚和厄瓜多尔要求保存格式、来源、目的地和日期；西班牙结合 eIDAS、LEC 和信任服务。任何规则都不会仅因消息是电子形式就使其内容成为真实。[6][7][8][9][10][11][12][13][14][15][16]

保全还受到隐私和第三方权利的限制。应限制角色、访问和传播，区分工作版本和公开版本，避免发布私密内容、未成年人数据、秘密信息或凭据。证据必须通过获授权的渠道并附清单文件交付，而不是作为公开文件集。[17][18][19]

最终核查	验收问题
对象	是否提供 EML、URL、文件和语境?
过程	是否记录由谁取得、使用何种角色、筛选条件和日期?
完整性	每个哈希值是否对应一个对象和时刻?
渠道	是否在限定范围内解释 DKIM / SPF / DMARC?
覆盖范围	会话线程、回复和缺失是否已声明?
归属	是否避免混淆账户和个人?
隐私	交付是否避免不必要的暴露?

结语

保全就是留下可验证的路径，证明某物在某个时刻曾经存在，而不是不断收集截图直到看似足够。

[6]墨西哥《商法典》第 89–94 和 1205 条：中立性、归属、书面形式、原件、完整性、可访问性和数据电文采纳。官方汇编。 官方在线来源

[7]《国家民事和家庭诉讼法典》第 348–350 条。汇编包含 15-01-2026 的修订。逐步适用，并取决于相关宣告。 官方在线来源

[8]NOM-151-SCFI-2016，数据电文的保存和数字化，发布于 30-03-2017。关于记录、完整性、可访问性和电子数字指纹的要求。 官方在线来源

[9]秘鲁。IOFE 条例，DS 052-2008-PCM，第 3 和 4 条：经数字签名的电子文件的要求与认可。 官方在线来源

[10]秘鲁。《民事诉讼法典》第 188–197 和 245.5 条：目的、合法性、证据、举证责任、评价和通过技术手段确定日期。 官方在线来源

[11]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。 官方在线来源

[12]阿根廷。《民商法典》第 318–319 条：允许以任何方式通信，并评价介质和技术程序的可靠性。 官方在线来源

[13]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。 官方在线来源

[14]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。 官方在线来源

[15]《（UE）910/2014 号 eIDAS 条例》，第 25–26 和 46 条：不得因电子签名和文件的格式而加以歧视，高级电子签名及合格电子签名的效力。 官方在线来源

[16]西班牙。《民事诉讼法》第 326 和 384 条：私人文件、质疑、用于归档、了解或复制数据的措施、检查、保管和合理审查。 官方在线来源

[17]墨西哥。《联邦私人持有个人数据保护法》，文本发布于 20-03-2025，修订于 14-11-2025。第 5–9、18–20 和 31 条：原则、安全、保密、数据泄露和权利请求受理。现行联邦主管机关为反腐败与善治部。 官方在线来源

[18]哥伦比亚。2012 年第 1581 号法律，第 4、8、12、17–18 和 26 条：原则、权利、告知、控制方和受托处理方的义务，以及向第三国传输。 官方在线来源

[19]欧盟。（UE）2016/679 号条例，第 5、25、28 和 32–34 条：原则、设计保护、受托处理方、安全及数据安全泄露的通知/告知。西班牙还要求审查适用的国家和行业法律。 官方在线来源