可信时间戳互联网电子数据取证及固化保全

操作指引

(V1.0)

二0一七年七月

发布单位：联合信任时间戳服务中心（北京联合信任技术服务有限公司）

目录

摘　　要

由于数据电文（电子证据）具有易被无痕篡改、原始性认定困难的特点，在司法实践中往往给双方当事人和裁判 过程带来困扰,为了有效解决这一问题，联合信任时间戳服务中心结合可信时间戳的特点和司法实践特制定本指引。

本指引对利用可信时间戳完成基于互联网的电子数据取证及固化保全，进行了较为全面的说明，包括技术术语的 解释、时间戳服务机构的介绍、适用范围、操作过程、参考判例等。

重要提示：

本指引旨在对基于互联网的电子数据取证方法进行明，按本方法取证可较大程度避免伪造、篡改证据的可能。使用者应根据取证的实际场景设计取证环节和步骤，亦可添加取证内容用以证明取证过程和还原事实真相。

司法机构具有独立的裁决权，本指引不构成对使 用者的任何承诺！

第一章　总则

第 1 条　制定指引的目的和依据

1. 目的

本指引旨在使互联网中的电子证据的采集、固化符合有关证据原始性的要求，指导司法机关、行政机构、执法人员、律师、当事人利用可信时间戳对互联网电子数据进行客观、真实的取证和固化，用以还原事实真相、减少事实争议、降低取证费用。

2. 依据

根据《中华人民共和国电子签名法》、《中华人民共和国刑事诉讼法》、《中华人民共和国民事诉讼法》、《中华人民共和国行政诉讼法》及《中华人民共和国律师法》等法律法规的有关规定，结合互联网电子证据的特点，制定本指引。

第 2 条 缩略语与名词解释

时间戳服务机构(以下简称"TSA[1]")：是指由国家授时中心进行授时与守时保障的联合信任时间戳服务中心。该中心由北京联合信任技术服务有限公司(以下简称"联合信任")负责运营和技术支持，官方网址为 www.tsa.cn。

可信时间戳(TTS[2]):是指由联合信任时间戳服务中心签发的时间戳。用于证明电子数据（文件）申请 TSA 认证的时间和内容完整性。

可信时间戳互联网电子数据取证及固化保全（以下简称"TSA 取证"或"可信时间戳取证"）：是指采用 TSA 的可信时间戳为主要技术保障手段，结合互联网电子证据的特点而开展的电子数据取证及固化保全活动。通过该方法可以还原事实真相、防止证据灭失和篡改，以实现客观真实的反应互联网电子数据的存在性且符合电子证据完整性的要求。按照要求完成的取证过程及固化后形成的电子文件，通常用于庭审过程中的举证环节，且具有较强的去抗辩性。

第 3 条　可信时间戳取证的适用范围及场景

本方法适用于等各类涉及互联网络的电子证据取证，如网页、电子邮件、网络图片、音频、视频影像、软件代码、文字、微信、微博等需要固定电子证据、防止证据灭失的场景。

1 TSA 是 Time Stamp Authority 的缩写·

2 TTS 是 Trusted Time Stamp 的缩写·

第 4 条 可信时间戳网页证据固化的原则

基于可信时间戳的网页电子数据固化的设计原理是以联合信任时间戳服务中心作为第三方，以可信时间戳作为保障电子数据原始性的技术手段，按照规范的操作流程对取证计算机及网络环境进行安全性和清洁性检查后，对整个取证过程全程录像记 录，并对录像文件申请可信时间戳认证。采用该方法取证后，可在事后追溯取证过 程、方法及内容，形成完整的证据链。该取证方法不依赖于取证人员， 避免了取证过程可能产生的伪造、篡改等证据瑕疵。

第二章 可信时间戳取证固化业务操作指南

第 5 条 事前准备:

取证计算机需要使用 window 操作系统，版本号不限。

1. 获取可信时间戳使用权限，并测试可以正常申请时间戳。 在联合信

   任时间戳服务中心官方网站（www.tsa.cn）注册并缴费。

   提示: 首次对超大文件（1G 以上）申请时间戳认证时，需要下载安装控件后方可正常使用。随着时间戳系统升级，建议使用前先对大文件申请时间戳进行测试。

2. 下载安装屏幕录像软件

   建议使用 KK 屏幕录像机软件（也可以使用其他录屏软件，KK 录像机下载地址：http://www.kklxj.com/），安装完成后需要对软件的录屏清晰度、录音功、录像文件存放地址能等进行设置和熟悉。

3. 安装 PDF 文档阅读器

   建议安装福昕阅读器或 Adobe Reader PDF 阅读器。用于查看时间戳认证证书（pdf 格式）。

4. 安装公安部认可的杀毒软件及系统更新 事先对取证计算机进

   行更新病毒库、杀病毒木马及系统更新。

5. 连接互联网 测试计算机可正常访问互联网，并保

   障网络畅通。

6. 制定取证预案

根据取证场景事先进行取证预案设计，防止取证过程中证据不能正确获取。如是否能够正常访问并查看到 被取证的内容、是否需要下载、是否需要用户名密码登陆等。制定预案的目的是能在正式取证时流畅操作，避免重复。

第 6 条 固化取证操作步骤

说明：以下步骤的目的是能在事后举证所固定电子证据的真实来源和内容，主要步骤包括取证计算机的安全性、清洁性检查；互联网连接的真实性检查；电子证据内 容的 TSA 固化；取证过程录像的 TSA 固化等。取证人员可根据案件需要增加必要的取证内容，如 ICP 备案查询等证明电子证据来源的必要信息。

第一步：打开屏幕录像软件开始录屏 录像内容应保证能够清晰展现每个操作步

骤及所获内容，重要的操作步骤可对其
进行语音形式的描述。

第二步：计算机安全性及清洁性检查

- 打开杀毒软件对计算机查杀病毒和木马。

  注：正常状态为没有任何木马病毒。

- 清理上网记录：

  用于采集和固化网页证据的浏览器应进行上网记录清除，清除操作可以使用浏览器自带功能或者第三方软件。清除记录包括：临时文件、cookie、历史记录、下载历史记录、表单数据、自动填充保存的密码、ActiveX 筛选和跟踪保护数据以及其他形式的可用于保留历史上网记录的数据。

  注：正常状态为清理干净。

- 打开任务管理器（单击右键打开），查看程序与进程。 注：需要

  查看所有现实的进程，以备事后证明没有非法进程。

- 检查 hosts 文件，在 C:Windows\System32\drivers\etc 路径下用记事本打开 host 文件，查看文件内容。以保证取证计算机未经人为篡改系统、未被连接到虚拟网站，确定当前计算机访问的网站或获得的电子证据均来源于互联网，确保电子证据来源的唯一性，是保证相关电子证据有效性与证明力的前提。

注：hosts 文件内容一般正常为空，如果有内容需要查看是否作了影响取证的虚拟链接指向。

第三步：互联网连接真实性检查

- 在 IE 浏览器的 Internet 选项下的"连接"中点击"局域网"设置，以保证没有连接代理。

  注：代理设置需要为"关"或空状态。

- 在命令窗口（开始菜单搜索框中输入"cmd"调出命令窗口）输入"ipconfig/all"命令，显示所有网络适配器（网卡、拨号连接等）的完整 TCP/IP 配置信息。

- 在命令窗口输入"ping 目标页面域名"（如 ping www.xxx.com），利用"ping"命令可以检查网络是否连通及显示目标网站的 IP 地址。应用格式：Ping 空格 IP 地址。注意有些网站设置禁止 ping 命令，可能无法显示 ping 的结果，但是不影响取证的真实性。

- 在命令窗口输入"tracert 目标网页域名"，以确认连接到目标页面网络服务器的路径，保证接入网站的真实性。Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径。

- 登陆门户网站的方式核实网络连接正常，最好访问带有日期标示的网页（例如，国家授时中心 www.ntsc.ac.cn 和联合信任时间戳服务中心 www.tsa.cn ）。

第四步 取证与固化

- 在取证计算机桌面创建一个存放证据的空文件夹。

- 打开需要取证的网页，查找需要固化的证据。将证据另存为图片、网页或其他格式文件。针对电子邮件取证可以将邮件另存为*.eml 格式文件。

- 打开时间戳服务中心官方网站 www.tsa.cn ，进入时间戳申请系统，在存放证据的文件夹中找到需要认证的文件，对证据文件申请可信时间戳认证，申请成功后下载时间戳证书（*.tsa）和时间戳认证证书（pdf），打开时间戳认证证书（pdf）查看证书内容。

  注：1、时间戳证书 *.tsa 是一个加密格式的电子证书，用于和对应的证据文件匹配，在时间戳中心的验证平台进行验证。该电子证书不能用一般程序打开。

2、时间戳认证证书（*.pdf）主要记载电子证据的认证时间、对应证据文件的 HASH 值、时间戳签发机构信息等内容。在此处打开的目的是显示证据的取证时间，防止事后编辑篡改取证过程录像。该时间应该与取证录像结束后申请时间戳的时间形成合理的证据链。

- 取证结束后把录屏视频文件申请时间戳认证，并下载对应的时间戳证书和时 间戳认证证书。

注：录像结束后应在尽可能短的时间内对该取证过程录像申请可信时间戳认证。避免事后举证时被质疑取证过程录像文件有编辑、修改内容的可能。

第 7 条 固化后电子证据整理

完整的电子证据取证及固化包应包括：

1. 电子证据文件 、对应的时间戳认证证书（pdf 格式）及时间戳文件（后缀名为.tsa 的文件）。
2. 屏幕录像文件、对应的时间戳认证证书（pdf 格式）及时间戳文件（后缀名为.tsa 的文件）。
3. 可以根据需要对证据文件重新命名，但不可以修改证据内容，否则无法通过验证。
4. 在时间戳中心（www.tsa.cn）网站的验证平台验证所有证据，查看是否能通过验证。
5. 根据取证实际情况书写《可信时间戳电子证据取证及固化说明》，简述取证过程及需要证明的事项。（格式参见附件《可信时间戳电子证据取证及固化说明》样例）

第 8 条 证据提交与使用

1. 证据包内容刻录光盘或使用 U 盘等介质存储。
2. 提交给司法机构的证据包括：

电子证据：取证过程录像（屏幕录像、摄像机录像）、TSA 固化的电子证据及其对应的时间戳证书和时间戳认证证书；《可信时间戳电子证据取证及固化说明》、《可信时间戳互联网电子数据取证及固化保全操作指引》（可选，用以说明取证过程）。

纸质证据：时间戳认证证书打印件、证据说明文件打印件。

3. 证据使用： 所提交电子证据在证据交换、质证据环节需要进行验证，以勘验证据来源、
证据原始性、完整性、关联性等。

证据验证：登陆 www.tsa.cn 时间戳官方网站验证平台进行验证，验证时须使用证据文件和时间戳文件（*.tsa），可验证所取电子证据是否被篡改以及取证时间、取证内容、取证过程等证据要素。