计算机取证中时间戳问题的研究[1]

沈金明　　龚俭[2]

（东南大学计算机科学与工程系　江苏省计算机网络技术重点实验室　南京 210096）

摘　要：当我们调查涉及计算机或计算机网络的犯罪活动时，建立事件的时间链可以帮助我们重建犯罪场景，确认犯罪嫌疑人是否具备犯罪时机，甚至可以帮助最终确认面临指控的嫌疑人是否有罪。计算机系统在许多方面提供了时间戳功能，这有助于我们在计算机取证过程中建立正确的时间链。本文介绍了计算机取证的概念和电子证据的特征，对时间戳在计算机取证中的作用以及计算机取证中容易出现的时间戳相关的问题进行了总结，提出了利用时间戳进行计算机取证的方法。

关键词：计算机取证，电子证据，时间戳

Study on Time-Stamp Issues about Computer Forensics

Abstract: In the investigation of a criminal case involving a computer or computer network, the timeline of events may help to reconstruct the scenario of criminal, can determine whether the suspects have chance to commit a crime, even can help to ultimately determine the guilt or innocence of those who facing criminal charges. The computer system provides time-stamp functions, which can help us construct correct timeline of the event during computer forensics. This paper introduces the conception of computer forensics and characteristics of electronic evidence. We give a summary of the function of time-stamp and relative issues in computer forensics.　Finally, we provide the methods of computer forensics with time-stamp.

Key word: computer forensics, electronic evidence, time-stamp

1．引言

“计算机取证”这个名词由International Association of Computer Specialist (IACS)在1991年美国举行的年会上正式提出，是指对能够为法庭所接受、足够可靠和有说服力的、存在于计算机和相关外设中的电子证据的确认、保护、提取和归档的过程。计算机取证按照取证的对象不同可以分为计算机主机取证和计算机网络取证，计算机主机取证的对象是存放在计算机硬盘、内存、外围设备中的文件、进程等信息；计算机网络取证的对象是计算机网络中的报文信息和相应的服务的日志、审计信息。按照取证的时机不同，计算机取证又分为实时取证和事后取证，事后取证，也称为静态取证，是指计算机在已遭受入侵的情况下，运用各种技术手段对其进行分析取证工作；实时取证，也称动态取证，指利用相关的网络取证工具，

[1] 本文受江苏省网络与信息安全重点实验室（BM2003201）资助

[2]作者简介：沈金明（1974--），男，江苏南京，硕士研究生，研究领域为计算机安全，计算机取证学。龚　俭（1957--），男，博士生导师，教授，研究领域为开放系统互联理论及其应用，开放分布式处理理论及其应用，计算机互联网络工程，网络管理，网络安全。

实时获取网络数据并以此分析攻击者的身份、企图和获得攻击者的行为证据。计算机取证的基本步骤为[1][2]：保护现场和现场勘查、获取证据、保全证据、分析证据、递交结果。与传统取证技术不同，计算机取证的对象和结果是电子证据。电子证据[3]是指以电子形式存在的、用作证据使用、能够证明案件真实情况的一切材料及其派生物，所谓电子形式依照印度《1999 年信息技术法》第 2 条第 1 款第 18 项的规定，可以概括为“ 由介质、磁性物、光学设备、计算机内存或类似的设备生成、发送、接收、存储的任一信息存在形式 ”。电子证据多以二进制形式存储于计算机的存储介质之中，这些信息必须要以特殊的手段来获取，并以特定的形式输出，才可能人们理解。电子信息在存储、传输过程中易被复制、篡改、假冒，从表面上看难以区分其原件和复制件、真实件和伪造件。因此，电子证据具有脆弱性特征。电子证据虽然在形式上不同于传统证据，但是，电子证据具有和传统证据一样的证明能力，RFC3227[2]给出了计算机信息作为法律证据的标准：

- 可接受性：电子证据在递交法庭之前必须符合一定的法律准则，即证据的提取方法和收集程序以及证据的表现形式必须符合有关的法律规定，也可以叫做合法性标准；
- 可信性：电子证据要能够证明和案件事实或其他有争议的事实具有一定的关联，也叫关联性标准；
- 完全性：电子证据必须能够全面证明犯罪事件，而不是犯罪事件的一部分；
- 可靠性：在电子证据收集和处理过程中不存在真实性和准确性的方面的怀疑，即证据的内容和形式必须符合客观存在性，也叫做客观性标准；
- 有说服力：电子证据必须能够被法官理解并且能够说服法官和陪审团对案件作出正确宣判。

时间戳可以定义为计算机系统在运行和通讯过程中产生并存储在计算机媒体中的日期和时间信息。时间戳反映了计算机系统的状态和处理事件的过程信息，对于计算机取证具有重大意义，是我们在进行取证时应该注意的重要因素。

（1）时间戳本身就是电子证据。计算机系统产生的时间戳可能揭示案件开始和结束的时间，以及持续的时间。因此，一个可信的时间戳可以作为证据来指控罪犯的犯罪行为。

（2）时间戳有助于我们重构犯罪场景。建立正确的事件顺序和时间跨度是在案件调查中和法庭上重建犯罪活动的基本方法。根据计算机系统中记录的不同事件的时间戳，我们可以决定事件间的时间顺序，从而建立一条时间链，根据这条时间链我们可以对发生在现实世界的犯罪过程进行回放。

（3）可以用于事件的聚类和关联。我们可以对计算机系统中的事件按照时间戳进行统计，然后基于统计进行关联聚类，划分出正常的事件和异常事件，缩小取证的范围，我们可以通过改变时间粒度的大小来提高检查的精度。我们还可以根据事件的时间戳中记录的开始时间和结束时间来将不同的事件进行关联和合并，我们还可以根据某一事件的时间戳关联到特定的使用者，从而找到犯罪嫌疑人。利用时间戳将电子证据关联到具体事件，也是电子证据满足证据的可信性标准的要求。

（4）可以验证电子证据的完整性。我们可以通过比较文件的 MAC 时间、日志中记录的时间戳以及环境时间等，发现电子证据是否被篡改和假冒，判定电子证据是否有效，是否满

足电子证据作为证据的可靠性标准。

（5）构成保管链（chain of custody ）。保管链，又叫证据链，是判定一个证据是否具有法律效力的重要因素，我们在法庭上递交证据时必须同时向法官出示证据保管链，要能够证明证据经过严格的保管程序，在证据获取、保全、分析、递交过程中都有清晰的纪录，证明证据未发生变化，对证据的操作都能有案可查。时间戳和保管人员、保管地点等共同构成了保管链。

2．时间戳与计算机取证

2．1 计算机系统中的时间标准[4][5]

计算机系统是一个基于时间的系统，在 CPU 这一级，计算机指令是在内部时钟的驱动下在 CPU 中顺序执行，按时间片轮流使用 CPU；在数据传输和总线级，数据也是基于时间速率有序地通过总线在 CPU、存储器和外围设备之间流动，在网络应用上，网络设备根据时间戳决定报文的产生时间、报文超时重传的时间间隔、报文收发同步等等。可以说，如果没有一个时间标准，计算机和计算机网络可能瘫痪。为了规范计算机应用中的时间格式和标准，适应计算机发展的国际化的需要，国际标准化组织 ISO 给出了统一的时间标准 ISO8601。在此基础上，IETF 也给出了关于 Internet 上的时间戳的格式和标准 RFC3339。RFC3339 是 ISO8601 的子集，是其在 Internet 中的简化形式，这两个标准都是以 UTC 时间为基准的。

TAI(International atomic time)，国际原子时，1967 年，CIPM(国际度量衡标准会议)定义一秒为铯原子的衰变周期的 9,192,631,770 倍，利用此原理的时钟称为原子钟，国际原子时就是由世界上 40 多个国家 200 多个时频标准实验室的原子钟组成，由 BIPM(国际度量衡局)平均所得，并每月发布。

UTC(coordinate universal time)，又称世界协调时，从 1972 年开始，世界上超过四十个国家采用此时间为官方标准时间。这是目前世界上大多数国家采用的实际时间标准，是由 BIPM 和 IERS(国际地球自转服务组织)建立和保持的世界法定时间，与国际原子时（TAI）相差整数秒，UTC 的零时是格林威治时间（GMT）的零时，由于地球自转并不稳定，会随着季节的变化而变化，而且地球绕着太阳公转的时间也会受到宇宙中其他因素影响而发生偏移，因此，存在闰年和闰秒。闰年的设置比较固定，每隔 4 年的二月增加一天，而闰秒则不固定，是由 IERS 负责计算发布，而且存在着正闰秒和负闰秒，所以，RFC3339 在定义秒的格式时存在 00-58、00-59、00-60 三种格式，分别对应着负闰秒、正常时间、正闰秒。

为了使用方便，我们计算机系统中采用的时间通常是时区时间，就是在 UTC 时间的基础加上时区偏移量。主机上的时间一般存放在 CMOS 中，依靠内部时钟维持，可以通过 GPS 时间源进行校准，也可以通过本国时间管理机构发布的标准时间校准，或者是通过网络时间协议（NTP）进行网络时间同步。

2．2 计算机取证中应该注意的时间戳问题

时间戳作为计算机取证过程中的一个重要资源，我们必须科学分析，如果只是机械的对待时间戳，可能达不到预期效果，甚至会产生错误的结果。为了保证计算机取证的科学性，确保获得的电子证据满足证据的基本原则，我们应该在取证过程中注意以下时间戳问题。

（1）时间戳的易变性。时间戳作为计算机系统产生的附加信息，和其他电子证据一样，

容易被篡改和伪造。例如，单用户操作系统，如 DOS，以及 windows95 以前的视窗操作系统，普通用户就可通过 time 或 date 命令轻易地修改 CMOS 中的时间，从而改变系统产生的时间戳的值。多用户操作系统，如 VMS、UNIX、Windows NT 等，只要具备管理员、root 或超户权限，也可以通过上述命令修改系统时间。对于一些日志文件中记录的时间戳数据，可以简单地通过 vi、UltraEdit 等编辑软件进行修改。在 Unix 系统中，利用 touch 命令可以任意修改文件的 MAC 时间。因此，我们在利用时间戳进行分析取证时一定要先鉴别时间戳的真实性和有效性。

（2）时间戳的多样性。不同的操作系统、不同的计算机设备产生的时间戳格式会不相同，另外不同的应用程序产生时间戳的方法也不一样。

（3）时间源的精度。计算机主机中的时间存放在 CMOS 中，由内置的时钟维持，由于电源的供电的波动或电力不足、时钟电路的振荡的跳跃、数学计算的不精确等原因会导致系统时钟漂移，从而使得产生的时间戳和真实时间存在误差。

（4）网络时间同步。在计算机网络取证过程中，不同的主机的 CMOS 时间可能并不一致，信息在网络中传输还会因网络拥塞等原因产生延迟，如果我们直接依赖这些时间戳来重构事件的时间顺序，可能导致错误的结果。对于不同国家和地区还应考虑时区和夏令时问题。

3 应用时间戳进行计算机取证

3。1 计算机取证中可以利用的时间戳资源

- 文件的 MAC 时间。MAC 时间是操作系统为文件管理提供的一项功能，可以用来追踪文件创建、打开、修改行为。M 时间(modified)：是指文件最后一次被修改的时间；A 时间（access）：文件最后一次被访问的时间，当我们打开或执行一个文件时，该文件的 A 时间自动更新为打开或执行的时刻；C 时间（create）：文件夹或文件的创建时间。在 Linux/Unix 操作系统下我们可以利用著名的取证工具 TCT 中的 mactime 程序获取计算机文件系统中的 MAC 时间，在 windows 操作系统下，可以在文件夹或文件图标上单击鼠标右键选择“ 属性 ”，就可以看到该文件夹或文件的 MAC 时间，需要注意的是 atime 已经变为当前操作发生的时间，我们可以用商用的取证工具 Encase 等来获取完整的 MAC 时间。
- 电子邮件头部时间。根据 RFC2822[6]规定，电子邮件的头部包含邮件的发送时间和接收时间以及转发时间，这些时间揭示了电子邮件从创建、传输到接收的过程。但是，一个入侵者可以通过 telnet 到邮件服务器的 25 端口采取手工编写邮件头部的方法伪造邮件的发送时间，我们一定要鉴别邮件发送时间的真伪。我们还要考虑到不同的邮件服务器所在地理位置的时区差别以及网络时间同步问题，要进行时间转换和补偿。
- 系统登录和退出时间。操作系统系统日志和安全日志中提供了计算机用户登陆系统和退出系统的时间戳，记录了本地用户登录和远程用户通过 telnet、rlogin 等方式登录的时间和退出时间，ftp 服务和 SMB 服务的日志文件也记录了远程用户登陆到服务器的时间，可以和日志中的用户名或用户账号、IP 地址等信息相结合来判定

非法用户的身份、行为和时间。

- IDS、防火墙报警时间。IDS（Intrusion Detection System ）根据入侵特征匹配或网络行为特征统计来发现网络中的异常行为，发出警报，并将相关信息记录入日志中。一般的 IDS 日志中包含了入侵事件开始时间、结束时间、源宿主机 IP 地址和端口号、入侵特征简单描述等信息；防火墙则根据事先配置的规则对经过防火墙的报文流进行过滤，当发现禁止的报文试图通过防火墙时也发出报警信号，并在防火墙日志中记录下时间、IP 地址、协议类型等信息。我们可以通过 IDS 和防火墙日志中记录的时间戳来判定入侵事件或入侵企图发生的准确时间。
- Web 访问时间。Web 服务器软件在日志中对访问 web 网页的请求信息进行记录，日志中包含请求信息类型、请求发生的时间、访问者 IP 地址、请求的 URL 等。IE 浏览器的临时文件、历史文件和收藏夹中含有计算机使用者访问特定网页的时间记录，cookie 文件中包含用户最后一次访问某个站点的时间信息。
- 代理服务器日志中的时间戳。代理服务器的日志中包含每次客户通过代理服务器访问外界的时间、客户账号、源宿 IP 地址、服务类型等信息。
- 报文获取工具在抓包时记录下的时间戳。tcpdump、windump、sniffer、ethereal 等抓包工具在抓获报文时都在保存的报文文件中添加每个报文抓获时的时间信息，其他的专业的网络取证工具在实时抓包时也会记录下相应的时间戳信息。
- 其他时间戳信息。操作系统和一些应用程序在运行期间或者是异常终止时会在日志中记录时间和事件类型，例如，windows 的系统日志和应用程序日志就记录着系统错误和应用程序错误发生的时间和事件类型信息。一些网络服务也都具有详细的日志功能，如聊天室服务器端和客户端都有关于聊天过程的日志，这些日志中详细地记录了时间戳信息，其他的还有 BBS、BLOG、USENET、BT 下载等日志纪录了 IP 地址和时间等信息。

3．2 利用时间戳进行计算机取证

计算机系统中存在着大量的时间戳信息，由于不同的计算机系统的时间戳格式和处理时间戳的方法不尽相同，目前还没有统一的标准的处理程序，这里仅结合取证实践给建议如下：

1） 及时收集和保存计算机系统中的时间戳信息。鉴于时间戳的易变性特性，我们要在第一时间收集相关计算机系统中的各类时间戳信息，有些时间戳信息本身就是电子证据的一部分，可以结合电子证据的获取同时进行，例如日志文件和报文抓获等。对电子证据中那些容易发生改变的时间戳信息，我们应先收集时间戳信息，再对电子证据进行深入分析，更不能盲目的操作。例如，如果我们利用杀毒软件对计算机系统进行杀毒操作，将会使计算机文件系统中全部文件的 A 时间全部更新，利用浏览器打开文件夹也会改变文件夹的 A 时间，在文件夹间复制和移动文件或者使用 chmod、chown、chgrp 命令会改变文件的创建时间。如果是远程获取日志文件等信息，应该采用安全通道进行信息传输，如 SSH 和 SSL。我们可以通过对收集到的原始时间戳信息加密或数字签名的方法确保其完整性。进一步的取证分析应该在复制件上进行。

2） 对时间戳进行归一化处理。统一时间戳的格式，并将时间戳中的时间统一为 UTC 时间，要考虑到时区和夏令时等因素。在获取时间戳的同时，要记录下所在计算机的系统时间和当地的标准时间，要根据系统时间和标准时间的差值进行时间补偿。对于不同的网络设备上的时间戳，还要考虑网络时间同步和网络延迟问题，也要相应地进行时间补偿。要鉴定时间戳的真实性，文献[7]给出了动态时间戳分析方法，对文件的 MAC 时间采用动态关联的方法找出事件发生的真实时间。

3） 利用时间戳验证电子证据的完整性。文献[8]给出了一种将时间戳和数字签名相结合的验证电子证据的完整性的方法。我们也可以引入可信的第三方提供可靠的时间戳来验证证据的完整性，RFC3161[9]给出了基于 X.509 证书的时间戳协议，取证方向可信的第三方 TSA(Time Stamp Authority)发出时戳请求，TSA 给出包含时间戳和证书信息的应答，请求方在验证应答信息的有效性后决定是否接收时间戳，这样我们就可以通过时间戳和 X.509 证书来验证电子证据的完整性。

4） 基于时间戳进行聚类和关联。按照时间顺序对事件进行统计聚类，利用数据挖掘等技术从大量的计算机事件中发现异常事件，缩小取证范围。根据日志信息中的事件的开始时间和结束时间对事件按照时间顺序进行排序，对于开始时间和结束时间都比较接近的两个事件在它们的其他属性基本一致的前提下，可以认为是同一事件，从达到约减的目的。我们还可以根据不同事件的开始时间和结束时间以及它们的发生条件 pre-conditon 和发生的可能后果 post-result 是否有前后、因果关系来关联两个事件。

5） 利用时间戳建立证据链（chain of custody）。在 Unix 系统中我们可以使用 script 和 date 命令相结合将我们在终端上输入的命令、命令开始和结束的时间、命令执行的结果输入到日志中，实现证据链的完整；

6） 利用时间戳建立事件的时间链，按照时间顺序对事件排序，重构犯罪场景。将取证结果整理成符合法律要求的电子证据形式递交给司法机关。

4 结论

计算机取证学还是一门年轻的学科，随着计算机和计算机网络技术的普及，计算机取证技术将变得越来越重要。本文论述了计算机取证的定义、分类和步骤，介绍了电子证据的特征和作为合法证据应具备的准则。分析了时间戳在计算机取证中的作用和应该注意的事项，给出了可能有用的时间戳资源。最后，简单地论述了利用时间戳进行计算机取证的方法。这些方法还不够完善，有待我们进一步的研究，提高计算机取证的效率和准确性，确保计算机和网络的安全使用，为维护社会稳定和促进国民经济的健康发展做出贡献。

参考文献

[1]丁丽萍、王永吉，计算机取证的相关法律技术问题的研究，软件学报，2005，16（2）：0260-0275

[2] Dominique, Brezinski.，“ Guidelines for Evidence Collection and Archiving ”，RFC3227，February 2002

[3]李鹏 ，电子数据证据新论，http://www.chinacourt.org/public/detail.php?id=80

[4]International Standardization Organization，“ Data elements and interchange formats – Information interchange - Representation of dates and times ”，ISO 8601:2000

[5]Chris Newman, Graham Klyne .，“ Date and Time on the Internet: Timestamps ”，RFC3339，July 2002

[6] Peter W. Resnick .，“ Internet Message Format ”，RFC2822，April 2001

[7]Weil M.，“ Dynamic Time & Data Stamp Analysis ”，International Journal on Digital Evidence，Summer 2002 ，Volume 1，Issue 2

[8]Hosmer C.，“ Proving the Integrity of Digital Evidence ”，International Journal on Digital Evidence，Spring 2002 ，Volume 1，Issue 1

[9]Carlisle.A, Pat.C, etc，“ Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) ”，RFC3161，August 2001