<<计算机司法鉴定>>

图书基本信息

书名：<<计算机司法鉴定>>

13位ISBN编号：9787511837196

10位ISBN编号：7511837190

出版时间：2012-7

出版时间：廖根为 法律出版社 (2012-07出版)

作者：廖根为

<<计算机司法鉴定>>

内容概要

《计算机司法鉴定:理论探索》首次从多学科交叉视角系统地对计算机司法鉴定理论进行探索，深入研究了计算机司法鉴定是什么、可以做什么、怎么做等基本问题。
全书共分两篇。
第一篇研究了计算机司法鉴定基本理论。
作者认为计算机司法鉴定包括两类不同性质的鉴定，即基于“证据发现”和基于“证据评估”的计算机司法鉴定。
第二篇和第份篇分别研究了基于“证据发现”和基于“证据评估”的计算机司法鉴定内容，并对儿种常见鉴定进行了深入分析。

作者简介

廖根为，副教授，司法鉴定人，任教于华东政法大学刑事司法学院，现从事信息安全与法律、计算机司法鉴定、声像资料司法鉴定等教学、科研和实务工作。

<<计算机司法鉴定>>

书籍目录

章节摘录

版权页： 插图： 防火墙日志主要记录进出特定计算机的连接记录。
通常一条防火墙日志记录中包括日期时间信息、活动信息、网络协议、目标地址、源地址、目标端口、源端口、状态标志等信息。
2.利用日志文件分析IP地址时应注意的事项 日志文件由许多条日志记录构成，日志记录主要记录在某个时间某一对象（包括计算机、IP地址、用户、程序或对象）采用了某种方法对某些资源进行了访问或处理以及访问处理后的结果情况。
但通过日志文件分析IP地址时，必须首先判断日志文件记录的真实性和准确性，以防止数据来源分析错误。
（1）日志文件记录是否存在伪造情况 当黑客人侵计算机系统后，常常删除或者伪造口志文件记录。
如果是对入侵或者攻击行为的来源进行分析时，还应该考虑被检索到的日志文件记录是否真实可靠。
判断日志记录中所记录IP地址的准确性与否，通常需要借鉴其他信息来确定。
（2）日志系统日期和时间的准确性 计算机日志系统在添加日志文件记录时，所记载的时间一般都以本机系统的时间进行记录。
如果本机系统时间标准与当地时间标准或者国际标准不一致，或者本机时间不准确，那么通过日期和时间来定位日志记录的方法就会出错，从而导致IP地址分析的结果可能出现错误。
因此，通过日期和时间定位日志记录时，要分析本机系统时间记录的准确性，并确定与被分析数据涉及时间标准的差异。
如果涉及多台计算机或者通信设备日志文件记录分析，更需要注意不同系统时间的差异。
（3）用户信息的准确性 有些日志文件记录了用户访问信息，这里的用户是指使用了特定系统账号的人。
记录表明可能是合法用户访问，也可能是冒充合法用户的人访问。
如果有冒充合法用户访问系统的行为，在日志文件中依然按合法用户账号进行记录，在对日志文件记录分析时，应区分这两种不同的情形。
如果日志文件记录了用户对应的IP地址信息，则可以通过IP地址信息确定用户的真实身份。
但如果没有对IP信息进行记录，则需要分析相关日志文件记录访问状态（成功登录还是失败登录）以及其他相关信息确定用户的身份，或进一步分析对应的IP地址信息。
（三）通过电子邮件分析IP地址 电子邮件中不仅包含发件人和收件人的邮件地址，在邮件首部信息中还包含所经过邮件服务器处理的相关信息。
即使电子邮件中发件人的邮箱地址信息是伪造的，通过对电子邮件首部进行分析，也可以追踪其来源。
电子邮件从发送方传输到接收方，至少要经过发送方邮件服务器和接收方邮件服务器的处理，每经过一个邮件服务器时，在电子邮件首部都会添加必要的信息。
常见的处理事项是添加“ Received域 ”到电子邮件头部。
通过检查Received域，可以检查邮件服务器名称、IP地址、接收时间、邮件协议、邮件唯一性标识等信息。
通过所经过邮件服务器的IP地址，可以重建电子邮件的转发路径，追踪其来源。
二、其他数据来源分析技术 （一）MAC地址追踪技术 在计算机网络通信的链路层，使用的是物理地址，即MAC地址。
在以太网中MAC地址为48比特大小的二进制字符串。
局域网通信时，IP地址和MAC地址有着对应的关系，其相互转化是通过ARP和RARP协议实现的。

<<计算机司法鉴定>>

编辑推荐

《计算机司法鉴定:理论探索》由廖根为著，笔者认为，以“ 证据类别 ”为核心的观点虽然揭示出司法鉴定活动的科学本质是一种对证据的真实性、相关性等进行审查判断的活动，但是司法鉴定活动中专门性问题往往比较复杂，有时候并非完全属于证据鉴别或判断活动。

<<计算机司法鉴定>>

版权说明