计算机取证概述

随着信息技术的不断发展，计算机越来越多地参与到人们的工作与生活中，与计算机相关的法庭案例（如电子商务纠纷，计算机犯罪等）也不断出现。一种新的证据形式——存在于计算机及相关外围设备（包括网络介质）中的电子证据逐渐成为新的诉讼证据之一。大量的计算机犯罪——如商业机密信息的窃取和破坏，计算机欺诈，对政府、军事网站的破坏——案例的取证工作需要提取存在于计算机系统中的数据，甚至需要从已删除、加密或破坏的文件中重获信息。电子证据本身和取证过程的许多有别于传统物证和获取的特点，对司法和计算机科学领域都提出了新的挑战。作为计算机领域和法学领域的一门交叉科学：计算机取证正逐渐成为人们研究与关注的焦点。

1、计算机取证概念

指运用计算机辨析技术，对计算机犯罪行为进行分析以确认罪犯及计算机证据，并据此提起诉讼。也就是针对计算机入侵与犯罪，进行证据获取、保存、分析和出示。

2、计算机取证理念

1、应该从一开始就把计算机作为物证对待，在不对原有物证进行任何改动或损坏的前提下获取证据；

2、证明你所获取的证据和原有的数据是相同的；

3、在不改动数据的前提下对其进行分析；

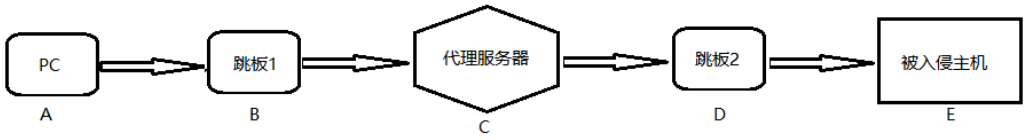
4、务必确认你已经完整地记录下你采取的每一个步骤以及采取该步骤的原因。

3、计算机取证原理

3.1 诺卡德交换原理

诺卡德交换原理：当两个对象接触时，物质会在这两个对象之间产生交换或传送。例如，两台计算机通过网络通信时，信息会在两者之间交换，一台计算机中的信息会出现在另外一台计算机的内存、日志中。一个可移动的存储设备连接到 Windows 计算机时，设备信息会保存到这台计算机上。调查人员和运行的系统进行交互时，运行程序并复制数据会导致系统的改变。这些改变可能是临时的（进程内存、网络连接），也可能是永久的（日志文件、注册表项）。

3.2 入侵取证原理



上图是一个利用多层跳板和代理攻击服务器的示意图。A 到 B 会在 B 上留下 A 的 IP，B 到 C 会在 C 上留下 B 的 IP，C 到 D 会在 D 上留下 C 的 IP，D 到 E 会在 E 上留下 D 的 IP。入侵时从 A 至 E，取证的方向恰好相反，如果中间的节点日志都没有清理，理论上可以根据日志 IP 溯源到 A，这就是入侵取证追捕罪犯的原理。

4、计算机取证步骤

1、保护目标计算机系统；

2、搜索目标系统中的所有文件；

3、全部（或尽可能）恢复发现的已删除文件；

4、最大程度地显示操作系统或应用程序使用的隐藏文件、临时文件和交换文件的内容；

5、如果可能并且如果法律允许，访问被保护或加密文件的内容；

6、分析在磁盘的特殊区域中发现的所有相关数据；

7、打印对目标计算机系统的全面分析结果，然后给出分析结论；

8、给出必需的专家证明。

5、数据收集原则

调查取证遵循一个原则：优先收集易变信息，其次收集不易变信息。易变信息存在于运行系统的内存中，其中特定类型的易变信息变化更加频繁。例如，网络连接过期不用时会存在数分钟。系统时间随时变化，剪贴板中的数据在内容改变或者关机之前保持不变。系统服务类的特殊进程会长时间的运行。那些具有更快易变特性的数据，如网络连接状态要首先收集，具有较慢易变特性的信息，如系统物理配置等可以随后收集。

6、开机取证方法

6.1 本地取证方法

本地取证意味着坐在系统的控制台前，使用键盘来输入命令，信息也保存在本地硬盘、移动介质（闪存、USB 硬盘）或映射到本地的网络共享驱动器中。这种情况非常普遍，取证人员能立即到达现场，使用光盘或闪存中的工具对系统进行直接物理访问。从数个本地系统中收集数据要比通过网络连接或者无线网络要快。使用正确数量的外部存储设备和访问权限，现场响应人员可以快速高效地收集必须的信息。为使现场工作更高效，响应人员可以将工具保存在移动硬盘上，编写具有弹性的批处理文件和脚本。

6.2 远程取证方法

远程取证方法通常包括一系列的命令，通过网络获取远程系统的信息。这种

方法对很多系统都比较实用，因为登录和运行命令的过程都可以自动执行。在安全圈内部，我们称之为可扩展性。首先调查员需要有远程登录权限，每次登录，运行命令并输出信息，安全事件日志中会添加记录，所以远程取证的第一件事就是收集安全事件日志的数据内容。