1

计算机取证准备和现场处理

学习目标

- 理解计算机取证的概念和计算机取证的原则
- 了解计算机取证的法律程序
- 了解企业内部取证和司法取证的异同
- 掌握计算机取证前的程序准备和文档准备的方法
- 掌握计算机取证前的取证启动盘和取证工具箱的准备方法
- 掌握计算机取证现场的处理方法

项目说明

某公司一名部门经理 Adam 和一名技术骨干 Bob，在工作四年以后突然离职，并开办了另一家公司，新成立公司的业务范围与原公司几乎完全相同，从而导致原公司产品的销售量急剧减少。在发现这样的情况后，原公司的主管 Alice 怀疑这两名雇员在原公司工作期间就利用上班时间发展自己的私人业务，并窃取公司机密资料为新创办公司做准备，因此授权企业 IT 部门的调查人员 Tom 来调查这两名雇员的办公电脑和所有公司给予他们的存储介质，以便找到相关证据。

项目任务

Tom 接受这个取证任务后，应当首先完成三个任务：

1．在进入计算机取证现场之前分析案例性质，并根据案例性质进行计算机取证的程序和文档准备；

2．进行进入取证现场前的外围调查，并根据案例特点进行计算机取证的设备和工具准备；

3．在进入取证现场的时候对原始证据进行妥善处理。

基础知识

1.1 计算机取证调查和鉴定的概念

1.1.1 计算机取证和司法鉴定

计算机取证的权威性定义目前尚未完全统一，许多专业机构和学者均从不同的角度给出了计算机取证的定义。根据http://whatis.com的定义，“计算机取证是一种调查和分析技术，这种技术是用来从特定计算机设备中收集和保存证据，并向法庭出示该证据。计算机取证的目的是进行结构性调查并保存证据链，从而确切地找出在特定计算机设备上发生了什么，谁应为此负责。”；著名计算机取证专家 Judd Robbins 则认为“计算机取证不过是将计算机调查和分析技术应用于对潜在的、有法律效力的证据的确定与获取”；另一位专家 R C Mark 认为计算机取证是“从计算机中收集和发现证据的技术和工具”。

国内著名计算机取证专家麦永浩教授则根据计算机取证的发展状况给出了较为全面的定义：计算机取证（Computer Forensics）是研究如何对计算机犯罪的证据进行获取、保存、分析和出示的法律规范和科学技术。

司法鉴定是指在诉讼活动中，鉴定人运用科学技术或者专门知识对诉讼涉及的专门性问题进行鉴别和判断，并提供鉴定意见的活动。或者说，司法鉴定是指在诉讼过程中，对案件中的专门性问题，由司法机关或当事人委托法定鉴定单位，运用专业知识和技术，依照法定程序做出鉴别和判断的一种活动。

2005 年 2 月，全国人民代表大会常务委员会通过的《全国人民代表大会常务委员会关于司法鉴定管理问题的决定》规定，国家对从事下列司法鉴定业务的鉴定人和鉴定机构实行登记管理制度：

- 法医类鉴定；
- 物证类鉴定；
- 声像资料鉴定；
- 根据诉讼需要由国务院司法行政部门、最高人民法院、最高人民检察院确定的其他应当对鉴定人和鉴定机构实行登记管理的鉴定事项。

1.1.2 计算机取证调查和鉴定的业务范围

目前与计算机取证（Computer Forensics）相关的提法还有数字取证（Digital Forensics）以及电子取证（Electronic Forensics），严格地说，这两种提法和计算机取证是有一定区别的。

这种区别主要表现在取证调查针对的主体对象不同，计算机取证的主体对象是计算机系统内与案件有关的数据信息，数字取证的主体对象则是存在于各种电子设备中与案件有关的数字信息，电子取证的主体对象是所有与案件有关的电子信息。因此，严格地说，计算机取证包含于数字取证，数字取证包含于电子取证。但是由于目前计算机系统已经通过嵌入式系统的方式，在许多电子设备当中运行，因此在实际的技术运用中，通常我们所说的计算机取证涵盖了一定的数字取证和电子取证的内容。

计算机取证通常包含单机取证、网络取证、手机取证和多媒体取证等诸多方面。所谓单机取证主要指通过对单台或多台独立的计算机进行调查，从而获取、保存、分析和出示与案件相关的证据。而网络取证则不同，其主要针对的是计算机网络，调查的重点在于各种网络设备（服务器、路由器、防火墙、入侵检测系统等），也即主要是通过对各种网络行为的调查和分析，从而获取与案件相关的证据。手机取证的对象不仅包含各种手机，也包含各种智能数据终端（如 PDA、PAD 等），通过对各种数据终端的分析和调查，从而获取与案件相关的证据。多媒体取证包含的内容较广，其主要对象是各种多媒体文件（如文档、图像、音频、视频等），其主要业务范围包含多媒体版权鉴定、多媒体内容真假认证、多媒体中隐藏和嵌入隐秘信息的可能性和对隐藏的内容进行取证等。

司法鉴定通常包括：法医鉴定，即对与案件有关的尸体、人身、分泌物、排泄物、胃内物、毛发等进行鉴别和判断的活动；司法精神病鉴定，即对人是否患有精神病、有没有刑事责任能力进行鉴别和判断的活动；刑事技术鉴定，即对指纹、脚印、笔迹、弹痕等进行鉴别和判断的活动；会计鉴定，即对账目、表册、单据、发票、支票等书面材料进行鉴别和判断的活动；技术问题鉴定，即对涉及工业、交通、建筑等方面的科学技术进行鉴别和判断的活动等。

2007 年颁布实施的《司法鉴定程序通则》（中华人民共和国司法部令第 107 号）对我国司法鉴定的实施程序进行了详细规定。把司法鉴定的业务范围较为详细地划分为法医病理鉴定、法医临床鉴定、法医精神病鉴定、法医物证鉴定、法医毒物鉴定、文书鉴定、痕迹鉴定、微量鉴定、声像资料鉴定、计算机司法鉴定、环境监测司法鉴定、工程造价司法鉴定、产品质量司法鉴定、司法会计鉴定、知识产权司法鉴定、税务司法鉴定、农业司法鉴定、资产评估司法鉴定、建筑工程司法鉴定和枪弹痕迹司法鉴定。

其中“计算机司法鉴定”是指依法取得有关计算机司法鉴定资格的鉴定机构和鉴定人受司法机关或当事人委托，运用计算机理论和技术，对通过非法手段使计算机系统内数据的安全性、完整性或系统正常运行造成的危害行为及其程度等进行鉴定并提供鉴定结论的活动。而“声像资料鉴定”，是指运用物理学和计算机学的原理和技术，对录音带、录像带、磁盘、光盘、

图片等载体上记录的声音、图像信息的真实性、完整性及其所反映的情况过程进行鉴定，并对记录的声音、图像中的语言、人体、物体做出种类或同一认定。

因此本书中所讲的司法鉴定，在涉及计算机文档、资料、信息等与计算机取证相关的司法鉴定时，应属于上述的计算机司法鉴定；在涉及多媒体内容认证等问题时，应属于声像资料鉴定。

通常计算机取证与司法鉴定的业务类型主要分为以下六类：

（1）存在性认定：认定在特定的存储媒介中存储有特定的信息。

（2）信息量认定：认定在特定媒介中存在的信息量的大小，例如对于制作或传播淫秽信息案件，通常需要认定淫秽信息的数量以及点击数量等。

（3）同一性认定：同一性认定或相似性认定分为两个方面，一方面是通过信息比对和统计分析，认定两个信息是否具有同一性或它们相似的程度，另一方面是通过对特定程序的对比分析，认定两个程序在功能上是否具有同一性或它们相似的程度，同一性分析常常在知识产权侵权案件中运用。

（4）来源认定：通过分析时间信息、生成方式、传播渠道等认定特定信息的最初来源，例如某张照片是否是某台特定的数码相机拍摄的，某个程序的源代码的作者是谁，网上某个谣言传播的源头等。

（5）功能认定：通过对特定程序的静态和动态分析，对该程序是否具有某种特定的功能进行认定，例如对程序代码是否具有盗窃信息、远程控制、自我复制、逻辑炸弹等恶意功能的认定。

（6）事件重构：通常包含四个方面：

- 对犯罪主体进行认定，例如通过对特定事件的分析，描绘嫌疑人的技术水平、行为习惯等；
- 对犯罪主观方面进行认定，也即嫌疑人的特定行为是主观故意的还是过失性的；
- 对犯罪客观方面进行认定，主要是分析认定何人在何时实施了何种行为等；
- 对犯罪客体进行认定，例如对于恶意网络攻击，通常需要对攻击的范围、规模进行认定，从而认定攻击造成的破坏程度。

1.1.3 计算机取证的发展状况

当前计算机技术的应用已经深入社会生活的方方面面，计算机技术成为一种犯罪手段，计算机信息成为犯罪目标人们也已经司空见惯，但是就计算机的根本性质而言，其仅仅是存储和处理证据的场所。

20 世纪 70 年代以来，计算机犯罪的数量一直在增长。最初由于计算机以大型机为主，因此计算机犯罪通常针对大型机，且常常发生在金融领域。最出名的案例就是发生在美国的“半分钱犯罪”，即计算机程序员修改了银行利息计息的程序，将所有不足一分钱的利息自动转入自己开设的账户中，从而在普通账户不易察觉的情况下获得巨额经济利益。

随着 20 世纪 80 年代个人计算机开始普及并逐渐进入社会经济的各个领域，众多操作系统也开始出现，如 Apple 公司的 Macintosh、PC-DOS、IBM-DOS 和 MS-DOS 等。针对各种操作系统的计算机取证的初期工具开始出现，但当时的工具大多采用 C 语言或汇编语言编写，只提供给特定的执法机构使用。

到 20 世纪 90 年代初期，出现了计算机取证的专业工具，IACIS（国际计算机调查专家协会）提供了对当时取证调查软件的培训，IRS（美国国税局）则制定了针对计算机取证搜查的方案。

随后，ASR Data 公司为 Macintosh 操作系统开发出第一款商用的计算机取证工具——Expert Witness，从而将计算机取证工具从执法机构的专用工具推向商用领域，使得计算机取证不仅仅用于调查计算机犯罪，也用于公司内部违规方面的调查。ASR Data 公司的合伙人之一后来离开该公司，开发了 EnCase 软件，该软件也成为目前最为流行的计算机取证工具之一。

随着计算机技术的持续发展，人们开发出越来越多的计算机取证软件，计算机取证领域也正在快速走向成熟。来自 SANS 研究院和 Guidance 等公司的资格认证计划专门培训计算机取证分析师。一些功能完全的取证软件包为计算机取证分析人员提供了技术支持和得到法庭证明的解决方案，如由 IRS 刑事调查局维护并仅限于执法部门使用的 iLook 软件、AccessData 公司的 FTK（Forensics Toolkit）软件、EnCase、NTI 套装、Coroners Toolkit（TCT）、针对苹果 MacOS 的 Mac Forensics Lab 取证分析软件等。

在这个领域共享知识和实践经验的计算机安全专家组成了一些组织机构，如由企业界和 FBI 建立的关键设施保护组织（www.infraGard.org），高科技犯罪调查协会（HTCIA）（http://htcia.asia/），计算机应急响应组织（CERT）（http://www.cert.org.cn）等。一些大学也正在从事计算机取证的研究和教学，在国际上较为知名的有美国卡内基-梅隆（Carnegie-Mellon）大学、加利福尼亚大学伯克利分校、宾夕法尼亚州立大学等。

当前计算机取证领域的新工具和新技术正不断涌现，在可预见的未来，由于数字信息的指数级增长，计算机取证领域将充满活力和引人注目。

1.1.4 计算机取证调查与个人隐私和公司秘密的保障

一般认为，计算机空间也是一个私密空间，当事人使用计算机等设备必然有一定的隐私，所以在美国等国家如果需要实施司法计算机搜查是需要申领搜查令的。在我国，进行司法计算机搜查是否需要申请令状，本质上需要在国家机关顺利开展侦查与公民生活不受打扰两方面进行利益权衡。

隐私权已然成为我国公民日常生活的一项基本人权。因此除法律特别规定的情形外，计算机搜查原则上必须以申请令状为前提。需要申请搜查令的计算机搜查应当至少满足三项基本条件。

（1）建立在正当理由的基础上，即申请令状的计算机取证调查人员必须有相当的证据表

明，将能够从计算机硬盘等介质中寻找到涉案证据。

（2）由合格的司法人员签发，目前我国的搜查证是由侦查机关的负责人进行审查签发。

（3）详细描述搜查的地点和扣押的项目，这些都直接关系到搜查范围的确定。

另外，计算机搜查的措施不仅影响被调查者的权益，而且常常会妨碍网络服务商和其他公众的合法权益。例如，若被搜查的计算机系统是多人本地共享或远程共享的，那么其中常常除了存储被调查者的信息，也存储有其他无关人员的信息，这些信息往往关系到他人的隐私或商业秘密。因此如何在有效开展计算机搜查与避免侵犯他人合法权益之间达到平衡也是需要认真考虑的问题。

对于这一问题通常在实践中采用“必要性标准”进行判断，即取证调查人员根据取证时的具体情况判断计算机搜查过程中有无扣押他人电子信息的必要性。如果有必要则可以将他人的电子信息数据作为扣押的对象（例如扣押整个计算机系统和相关的存储介质等）；如果无必要性则通过复制方式仅仅对有关案情的电子信息进行扣押。而对于必要性的判断通常结合以下要素：

- 被调查者涉及案件的性质；
- 该电子数据作为证据的证明价值；
- 该电子数据受到篡改、删除的可能性；
- 该电子数据所有人的隐私和商业秘密的保护性质。

对于计算机信息司法鉴定的隐私保护问题，司法部 2007 年公布的《司法鉴定程序通则》第五条规定：“司法鉴定机构和司法鉴定人应当保守在执业活动中知悉的国家秘密、商业秘密，不得泄露个人隐私。未经委托人的同意，不得向其他人或组织提供与鉴定事项有关的信息，但法律、法规另有规定的除外”。这一条款，明确确定了我国司法鉴定的保密原则。在计算机证据、电子证据的鉴定过程中，除了需要提交鉴定书和有关附件数据，同时必须将鉴定过程中产生的其他中间数据进行销毁，从而更为安全地保护秘密和隐私。

1.1.5 计算机取证和司法鉴定的原则

计算机取证的主要目的就是获得可以证明案件事实或者可以证明案件事实的某些方面的电子信息，从而形成电子证据，进而在诉讼中运用于司法实践，或者在企业内部作为违规惩处的依据。计算机取证与司法鉴定是一门法学与计算机信息科学紧密结合的交叉学科，也是一门新兴的学科。

计算机取证与鉴定必须依托于科学原理及经过科学实践检验的方法。要求我们使用的工具、分析原理应当经过科学实践的检验，使用的技术原理应符合科学原理和相关法律要求。

计算机取证与鉴定包含发现、收集、固定、提取、分析、解释、证实、记录和描述电子信息和电子证据等多个步骤。计算机取证与鉴定过程是由多个环节构成的统一的技术体系。

证据是案件的核心和诉讼的关键，取证与司法鉴定是必经的司法过程，获取具有可采性的证据是取证与司法鉴定的主要目的，通过调查取证与鉴定人员进行具体的取证与司法鉴定行

为来实现这一目的。以原则规范计算机取证与鉴定，是保证电子证据可采性的关键。由加拿大、法国、德国、英国、意大利、日本、俄罗斯、美国的计算机取证与鉴定研究人员组成的 G8 小组提出了六条关于计算机取证与鉴定的原则：

- 必须应用标准的取证与司法鉴定过程；
- 获取证据时所采用的任何方法都不能改变原始证据；
- 取证与司法鉴定人员必须经过专门培训；
- 完整地记录证据的获取、访问、存储或传输的过程，并妥善保存这些记录以备随时查阅；
- 每位保管电子证据的人员必须对其在该证据上的任何行为负责；
- 任何负责获取、访问、存储或传输电子证据的机构有责任遵循以上原则。

由于不同国家在法律、道德和意识形态上存在差异，取证与司法鉴定原则取决于不同的证据使用原则。不同的国家、组织根据自身的出发点，制定的取证与鉴定原则虽然不完全相同，但大体均为保证所获证据与案件事实的关联性、证据获取过程中各要素的合法性以及证据本身的客观性，这三个性质也是保证电子信息作为证据的三个核心性质。

为充分保证计算机取证所获得的电子证据满足关联性、合法性和客观性，计算机取证和鉴定的原则应包括以下四个方面。

（1）合法原则

计算机取证与司法鉴定不仅要保证取证与司法鉴定实体合法，还要保证取证与鉴定的程序合法。取证与鉴定活动的要件是指贯穿取证与鉴定活动全过程的四个要素，即主体、对象、手段和过程，只有保证这四个要素同时合法，才能保证获取的证据的合法性。

1）主体合法。

计算机取证与鉴定的主体指的是案件证据的提交者，随着在案件中承担举证责任的地位不同，计算机取证与鉴定的主体也会有所不同。我国《民事诉讼法》和《行政诉讼法》对取证主体没有严格的规定，加之电子证据的取证与司法鉴定方法的特殊性，因此取证与司法鉴定主体必须具有相应的资格，才能依法完成电子证据的发现、收集、保全等取证与鉴定活动。

电子证据的取证与司法鉴定的主体首先应当具备法定的取证与司法鉴定的资格，只有具备合法的调查取证与鉴定身份，才能执行相应的取证与鉴定活动。鉴于计算机取证与鉴定是一门技术性非常强的交叉科学，因而调查中聘请具有法定资格的计算机取证与鉴定专家协助调查是弥补此缺陷的有效方法。计算机取证与司法鉴定的主体应当包括合法的调查人员和具有法定资格的计算机取证与鉴定专家。

2）对象合法。

为保证所有人、权利人的隐私不被侵犯，计算机取证与鉴定的对象必须是已经受到攻击、被入侵的计算机系统，或者被利用来实施犯罪行为的计算机系统（如僵尸计算机系统、僵尸网络系统等），或者其他涉案的电子设备，只有那些被怀疑与案件事实有关联的信息（通常也是搜查证中所规定合法调查范围中的对象）才能作为被取证调查的对象。在企业计算机取证调查

中，为了保证调查的对象合法，不涉及隐私权问题，往往需要在企业规章制度中做出对公司配备给职员使用的电子设备，在需要时可以进行调查取证的声明。在调查取证时，为保护与案件无关人员的权利，还需确定电子信息存储的位置、状态、方法等作为取证与鉴定的对象范围。电子证据通常存储在硬盘、光盘等大容量的存储介质中，必须在海量的数据中区分哪些是与证明案件事实有关联的信息，哪些是无关数据，哪些是犯罪者留下的记录和“痕迹”。对于与案件事实无关的数据，不能进行任意地取证，以免侵犯所有人或权利人的隐私权、商业秘密等合法的权益。

3）手段合法。

计算机取证与司法鉴定的手段主要包括物理取证和工具取证两种方式。物理取证是指取证与鉴定人员通过手工直接取证，而工具取证则是指通过特制的信息系统处理软硬件的工具进行取证。传统的物理取证要求取证人员符合技术操作规范，工具取证是针对电子证据的技术特性对物理取证的补充，不仅要符合物理取证的上述条件，取证所使用的工具和程序等必须通过国家有关主管部门的评测。

如果取证与司法鉴定的手段非法，势必导致所采集的电子证据可信度大为降低，因此在计算机取证与鉴定过程中不得采取窃录、非法定位、非法监听、非法搜查、非法扣押等措施和方法，不得使用未经审核验证合格的软硬件工具获取和验证电子证据。取证与司法鉴定活动的每个环节都应该遵循标准程序，采取的手段应该符合法律要求。

4）过程合法。

取证与司法鉴定过程中，应遵守以下规范：

- 在不对原有证物进行任何改动或损害的前提下获取证据，证明所获得的证据和原有的数据是相同的；
- 在不改变数据的前提下进行分析；
- 采用人证、书证和音像资料等传统证据形式验证电子证据的合法性，要坚持及时将可以转化的电子信息转换为书证；
- 要利用传统的音视频采集工具对取证与鉴定过程进行全程记录；
- 取证时应当至少两个合法取证人员同时在场取证；
- 整个取证与鉴定过程必须受到监督，以保证过程的合法性。

（2）无损原则

证据材料必须能够客观、真实地反映案件事实，才能成为有效的诉讼证据。我国诉讼法规定，在提交物证、书证时若提交原件确有困难，可提交复制品或副本。对于存储介质中的电子信息，基本上不存在直观可视的传统意义的“原件”，因此在当前的司法实践中使用的均是原始存储介质中电子信息的“克隆”形式。由于电子信息的复制技术不会造成信息内容的损失，同时可以保证信息在存储介质中的保存位置不变，因此只要复制的内容与原始存储介质中的内容完全相同，就应当将其视为与原件具有同等的法律效力。

但是，正因为电子证据对其存储、运行或操作环境具有较强的依赖性，对存储介质、系

统环境的任何操作均可能改变电子信息的属性，例如打开嫌疑计算机或电子设备这样的操作，都会改变设备的系统日志信息，所以对于电子证据的计算机取证和鉴定需要特别注意“无损原则”。为防止由于对涉案的设备和系统的操作损毁潜在的电子证据，计算机取证和鉴定的整个过程均不能对取证和鉴定对象进行任何修改，以维护全部信息的完整状态，这也是保证所获取的电子证据具有客观性的基础。

通常，为了遵循“无损原则”，在实施计算机取证的初期阶段，收集存储介质中的原始电子证据时，就应当采用对位拷贝或镜像制作的硬软件工具（如各种硬盘对位拷贝机、FTK imager、En.exe 等）以字符流镜像的方式对存储介质中的所有数据信息进行备份（通常至少制作两份以上的备份），并且采用数字 Hash 签名等认证技术进行原始证据的固定，而在后续的分析、鉴定等环节中只对备份数据进行操作，从而有效地保证电子证据的客观性。

另外，在证据的保存环节，由于电子证据是以电、磁、光方式存储在存储介质中的，而在电磁介质中的电磁信息受外界磁场影响可能被消磁，DVD 和 CD 等光盘介质也有损坏的可能性，因此在保存收集到的电子证据时，应当采取远离高磁场、高温环境，避免静电、潮湿、灰尘和挤压等措施，以保证电子证据的客观完整状态。

（3）全面原则

全面取证与司法鉴定原则，是指调查人员在取证与鉴定过程中应尽可能全面地调查取证与鉴定，使得所获证据能够相互印证，从而形成完整的证据链。“全面取证原则”是保证电子证据客观性的一个重要方面，调查人员必须对案件形成并保持公正无偏的观点，避免对片面的调查结果轻易下结论，并且在整个调查取证和分析鉴定过程中排除一切自身和外界的偏见，对取证与鉴定的对象进行全面的取证调查和分析鉴定，用尽所有合理的线索，并考虑所有可用的事实，才能做出客观的结论。

另外，在诉讼案例中，通常利用单个电子证据诉讼定案的情况很少，案件往往包含多个用以诉讼的证据，每一个证据从不同的侧面与案件事实进行关联，例如在利用电子邮件进行诈骗的案例中，用户的账户和密码有助于确定嫌疑人；E-mail 邮件有助于认定诈骗信息；嫌疑人使用的计算机系统和邮件服务器系统的运行日志则有助于认定作案时间，而一系列不同层面的电子证据就组成了一条完整的证据链以证明案件的全部事实。

现代信息技术环境下，往往取证和鉴定对象存在着海量的信息，如果在调查取证和分析鉴定的过程中，调查人员忽视了一些细微的数据信息，就可能导致证据链的逻辑性不严密，从而影响最终诉讼过程，甚至可能导致错误的分析判断结论。因而在进行计算机取证与鉴定时，一定要认真分析电子证据的来源并进行全方位、多角度的取证与鉴定，在确保证据与案件事实关联的基础上，将所获取的一切电子证据和其他类型证据，进行相互印证和分析，排除逻辑矛盾，最终组成严密和完整的证据链。

（4）及时原则

由于电子证据的实时性和自动性，在电子证据的类别中，有相当大一部分电子证据是在信息系统运行过程中自动和实时生成的，而系统在经过一段时间的运行以后，很可能会造成信

息系统的变化（诸如网络审计记录、系统日志、进程通信信息等潜在的电子证据就会随之而发生变化），导致这些数据信息不能再如实反映案件的事实。因而电子证据的获取具有一定的时效性，当调查人员确定取证对象后，应尽早搜集证据，保证其没有受到任何破坏和损失。从电子数据的形成到原始电子证据的获取，相隔的时间越久，越容易引起电子数据的变化。例如，IP 地址经常被用来确定涉案计算机设备的方位，但这种“网络号码”却不会像身份证号一样与所有者存在固定的标识关系，在网络攻击的案件取证中，当某一计算机连接网络后被分配了一个 IP 地址，该计算机退出网络后，此 IP 地址极有可能被分配给新连接网络的其他计算机。因此，及时取证与司法鉴定可以保证电子数据作为证据的客观性，维持电子数据与案件事实的关联性。

1.1.6 计算机取证的实施过程

作为计算机取证人员的任务就是从取证对象（通常是嫌疑人的计算机）中搜集证据，并确定是否犯罪或违反公司制度。若搜集的证据显示其已涉及犯罪或已违反公司制度，那么就有必要开始准备对案件进行调查，也即开始收集一些可以在法庭上或公司的听证会上提供的证据。为了在一起计算机取证案例中收集证据，调查人员需要对被怀疑的计算机和电子设备进行调查，并将所收集的证据进行固定保存和归档，以便需要时进行证据显示和接受质证。在开始进行调查前，必须遵守被认可的程序过程来为案件做准备并实施取证，以便保障所获得证据的关联性、合法性和客观性。通过系统和规范的过程来处理每一起案件，就能够彻底评估证据并记录取证过程或证据监管过程，即从受理案件开始，到找到这些电子证据，并最终结案或者向法庭提供证据的整个取证过程。

通常可以将计算机取证的实施过程分为案件受理、取证准备、处理现场、搜集和固定证据、证据保存、证据分析、报告生成、证据归档和证据显示与质证。

（1）案件受理

受理案件是调查人员了解案件基本情况和发现证据的重要途径，是调查的起点，也是依法开展工作的前提和基础。因此受理案件可以算是展开计算机取证与鉴定工作的最初阶段。

调查人员在受理案件时，要详细记录案情，全面地了解与案件事实相关的潜在电子证据的情况，如涉案的计算机系统、打印机等电子设备的情况，尤其是 IP 地址、域名、网络运行状况、设备的运维管理情况、当事人的信息技术水平和虚拟现场。在受理案件时，不一定以上种种情况都能够全部了解地一清二楚，但是这样的了解应当尽可能得详细，从而使调查人员可以进行有针对性的取证准备工作。

在本章的案例中，当主管 Alice 将调查 Adam 和 Bob 的案件委托给调查人员后，调查人员至少应当在受理这个案件时了解以下情况或做以下工作：

1）制作一式两份（或两份以上）书面的计算机取证调查委托书，明确委托人（公司主管 Alice）和调查责任人、调查取证的范围和对象、根据公司何种规章制度进行调查等情况，并且委托人和受托的调查人员均应当签章，作为取证调查的依据，这样既明确了取证调查的范围，

同时也使得调查人员避免了诸如隐私权侵犯等方面的纠纷。

2）从委托人 Alice 或者设备管理人员处了解本次调查取证的对象情况，如 Adam 和 Bob 分别使用何种计算机，是什么样的操作系统，他们所处的网段是什么，有没有固定的 IP 地址，他们的计算机硬盘是什么型号，容量多大，他们分别使用何种打印机，公司有没有保存配备给他们的 USB 盘、存储卡，容量多大，他们是否具有公司配给的其他电子设备等。

3）从被调查人 Adam 和 Bob 曾经的同事处了解两个人的技术水平如何，有什么样的工作习惯，技术偏向于什么方面等。

（2）取证准备

当调查人员受理了一起案件，了解了案件的基本情况后，就进入了取证调查的准备阶段。当为一个案件做准备时，通常应当考虑进行如下工作。

1）对案件类型进行初步估计：通过在案件受理阶段调查人员从委托人和其他相关人员处了解到的情况，初步估计案件调查的性质和范围，如案件是网络取证还是主机取证，是否已经扣押了取证对象（计算机、各种存储设备以及其他电子设备），取证的现场是局限在一处还是分散在多处，是否需要查看其他现场。

2）确定案件调查取证的初步方案：根据在受理阶段了解的信息，制定出调查该案件的行动纲要。例如在企业委托调查中，如果被调查人员是一名在职的雇员，并且委托人希望不公开调查，那么就要考虑是否可以在工作时间搜查取证该雇员的计算机，或者应当等到下班后或周末进行。思考，如果在引导案例中 Bob 的计算机采用的是 Linux 系统，而 Adam 的计算机采用的是 Win7 系统，那么是否需要制定不同的方案并准备不同的设备和工具。

3）制定详细的方案：通过列出需要采取的步骤的详细清单来细化行动纲要，并估计每一步需要的时间，这样的方案可以帮助调查人员在调查取证过程中不会偏离主要目的。

4）确定风险并在方案中使得风险最小化：列举出在类似案件中通常会遇到的问题，例如如果 Adam 具备丰富的计算机知识，他就很有可能已经设定了某种登录策略，当有人试图修改登录密码时，该登录策略就会关闭计算机或覆盖硬盘中的某些数据。这类问题的清单通常也叫标准风险评估；思考并验证标准风险评估中的问题，如何才能将风险最小化，并补充完善方案，在开始恢复数据前，应当对原始介质多做几个备份，以保证从硬盘进行数据恢复过程中，尽量减少原始证据数据改变的风险。

5）准备调查取证工具：根据所确定的方案，有针对性地准备调查取证的硬件设备和软件工具，特别是现场取证的工具，如数码相机或摄像机、现场勘验录音设备、硬盘拷贝机、数据终端取证设备、取证启动 USB 盘或光盘、镜像制作原件等。如果遇见不熟悉的情况，调查人员应当对方案进行预先的测试（例如在虚拟机上安装取证对象计算机上的操作系统，并熟悉其相关系统设置等）。

（3）处理现场

对于调查现场的处理，通常我们分为现场确认、现场保护、现场记录、证据搜集和远程调查等部分。

1）现场确认：计算机取证调查人员要涉足到比传统调查员更广泛的取证现场。确认犯罪现场并不容易，需要详细调查才可能了解到该从何处入手。计算的远程性和证据的分散性给调查员带来了诸多的挑战，包括：现场可能是分散的、现场可能难以进入，甚至可能不存在一个确切的物理犯罪现场。

2）现场保护：要求调查人员保证当前确认的现场中各部件的物理和逻辑安全性。在保存证据、减少潜在的证据损毁且保护案件所需数据的工作中，物理安全是最基本的，但是对于计算机取证人员，保证所有电子设备的物理安全还仅仅是整个任务的一部分，取证调查人员必须同时保证设备中数据的逻辑安全。保证数据逻辑安全的最佳方法就是及时地进行取证副本的制作。

3）现场记录：现场记录是整个计算机取证过程中一个重要的方面，在处理现场前必须记录下整个现场的情况。通常现场记录需要两个调查人员完成，一个执行现场的所有处理，另一个专门负责现场记录。在采取现场处理行动前，需要对现场所有情况进行记录，可以采用现场录像、照相、录音描述、图形绘制等多种记录方式。对于计算机取证调查，通常需要记录计算机屏幕内容、网络连接情况、外围设备连接情况等。

4）证据搜集：通常在现场获得的未加分析（或仅进行初步分析）的证据称为原始证据，在现场进行原始证据搜集时，通常分为原始的物理证据和原始的数字证据两类。现场物理证据的处理工作最好分配给那些受过专门训练的人员来做。一般都应先处理物理证据，然后再处理数字证据，除非有理由认为数字证据的延后处理会造成证据破坏或者丢失。各类电子设备除了保存着数字证据外，也是物理证据的载体。处理犯罪现场的数字证据是计算机调查员的职责所在。在对所有 IT 设备进行了物理处理后，计算机调查人员就着手负责打包和处理所有电子器件，通常在断开任何连接前，要给连接计算机的所有电缆和电子设备贴上标签。然后，在日志本中也应记录电缆的连接情况，以便为以后的重组工作提供参考。在所有电缆都被贴上标签后，就可以拔掉电源插头来关闭计算机了（通常不要使用计算机的关机按钮）。对便携式计算机而言，应拆掉电池，然后拔电源插头。断电后，从计算机上移除每一根电缆，并依次收纳到证据包里。在电缆收完之后，所有包含数字逻辑内容或者对静电敏感的物品都放置在防静电包中。防静电包也要放到证据包里，然后密封。外围设备、存储介质和其他电子产品，同样也要在放入证据包之前，先放入防静电包里。

5）远程调查：当数字证据的搜集难以进入，甚至没有一个确信的物理犯罪现场时，计算机调查员可以在法律许可的范围内执行远程调查，从而搜集原始证据。远程调查对调查员而言非常重要，它由无需直接了解嫌疑人就能进行的各种信息收集和分析行动组成。所采取的行动取决于潜在嫌疑人的谨慎度和技能。远程调查可能涉及探查指定系统，也可能需要收集其他信息进行现场取证的准备。只要不会引起警惕，应该收集任何可能减少现场处理和获取次数的信息。远程调查的典型方法是获取任何嫌疑人不会意识到，或者不会事先访问和分析的日志文件。同样，对嫌疑人系统进行物理监视或轻量级的网络探查（如执行 traceroute、ping 等）可以了解嫌疑系统的位置、配置和类型情况。

（4）搜集和固定证据

对于计算机犯罪，通常需要收集的证据资料主要来自涉案计算机系统、网络管理者与 ISP 商（网络服务提供商）。系统、网络管理者与 ISP 商的配合，是计算机犯罪调查成功的重要因素。在此期间，主要注意收集计算机审核记录（使用者账号、IP 地址、起止及使用时间等）、登录资料（申请账号时填写的姓名、联络电话、地址等）、犯罪事实资料，即证明该犯罪事实存在的数据资料（文本、屏幕界面、原始程序等）。

搜集的各种信息可以进行深入的研究，分析案件是属于何种犯罪类型，了解犯罪嫌疑人的职业身份、动机目的和犯罪手法等。例如计算机系统日志文件能产生审计痕迹，记录下重要的网络活动，包括使用者进入计算机的时间，所取用的资料、档案、程序，进行过哪些操作，何时离开系统以及哪些行为被拒绝等操作。依据这些“电子痕迹”，就可以找出何人在何时做了何事，使用者来自系统内部还是外部。

通常较为专业的计算机犯罪，嫌疑人在作案后可能会彻底删除或者混淆和隐藏证据以掩盖犯罪行为，且计算机系统中的某些事件（如正在进行的文件修改、已经发生的进程中断、内部进程通信和内存的使用情况等）或许不会在被攻击的系统中留下事后线索。因而需要实时取证分析，或对现场获取的原始证据进行深入分析，以获取全面充分的证据，支持调查人员得出具有较强确定性的结论。在证据收集过程中，收集与案件事实直接相关的数据信息的同时，不能忽视诸如数码相片的数字信息证据、网络环境参数、各硬件之间的连接情况等细节信息的搜集。

由于电子证据的相对易删改性，根据无损取证与鉴定原则，调查人员应对原始存储介质进行备份，以保证电子证据的客观真实性。同时分析过程中获取的证据信息也应当进行及时的备份，以免日后对证据的可采性滋生争议。对于证据信息的固定，通常采用数字签名（Hash 认证）和时间戳等方式来保证所获取的电子证据的客观性。

（5）证据保存

由于通常多数案例可能调查和定案时间较长，而电子证据受环境影响较大，因此应用适当的储存介质进行原始的镜像备份，且放置保存环境应当慎重选择。证据从最初收集，到其可能成为呈堂证供，以及在后续的保存归档过程中，对每一份证据的位置和经手人都应进行全程的记录，形成保管链，并维护和妥善保存该保管链。

电子证据内容实质是电磁信号，极为脆弱，如经消磁即无法恢复，因此搬运、保管电子证据时不应靠近磁性物品，防止被磁化，提取的磁性存储介质必须妥善地保存在纸袋或纸盒内，置于防碰撞的位置，不可只进行简单的塑料袋封存；对于计算机和磁性存储介质，不应放置在安有无线电收发设备的汽车内，不能放置于温度过高或过低的环境中；另外如磁带或磁盘等存储介质如果发霉或潮湿，就会难以读取其存储的记录内容，因而应将电子证据放置在防潮、干燥的地方；对获取的电子证据采用严格的安全措施进行保护，任何调取情况均进行记录，尽量利用原始证据的备份进行分析，除非必要原始证据本身不要离开保存环境，非相关人员不准操作存放电子证据的设备；不可轻易删除或修改与证据无关的文件，以免引起有价值的证据文件

永久丢失。

（6）证据分析

在进行电子证据的分析以前，必须先将证据资料备份以完整保存证据，尤其是应将硬盘、USB 盘、闪存、数字终端的内存、数码相机的存储卡等存储介质进行镜像备份，即“克隆”，在分析过程中，必要时还应重新制作备份证据材料。分析电子证据时应对备份资料进行非破坏性分析，即通过一定的数据恢复方法将嫌疑人删除、修改、隐藏的证据尽可能地恢复，在恢复出来的文件资料中分析查找线索或证据。

（7）报告生成

计算机取证和鉴定的调查者在取证调查的最后，需要通过书写报告来传达计算机取证鉴定或取证调查的结果。报告需在法庭或一个行政预审会上提出证据作为证词，除了陈述事实之外，报告也可表明专家的意见。目前，不少专业的计算机取证软件具有报告生成的功能，能够自动地记录和整理取证调查分析过程中的操作、时间、证据来源（原始证据）、证据来源验证信息、证据信息、证据信息的 Hash 码、案件调查者等，但是使用这些自动生成的报告时，应当根据具体需要呈堂和提交的要求，人工进行仔细整理和认真检查。

对于涉及计算机取证的调查案件，通常法院要求专家证人呈递书面报告，尽管报告的要求在具体细节上不尽相同，但是报告内容必须明确而没有歧义。因此，计算机取证调查的人员，必须通过报告解释他的调查和发现。此报告必须包括所有的意见、根据和达成意见所需考虑的所有信息。报告也必须包括相应的展示，例如照片或者图表等。

同时，调查和鉴定人员应该为任一笔录证词的通知或传票保留一份复件以备查阅，并且建立一个计算机取证和鉴定的档案，其中至少包含案件的类型、判决权、时间日期、案件的数量（法庭案件文件的数量）等，并且应当总结自己证词的关键点作为参考，当然如果能得到证词的抄本也应当保留一份复件。

（8）证据归档

在取证调查和分析的最后，调查人员应当整理计算机取证与鉴定的结果并进行分类归档保存，以供法庭作为诉讼证据，主要包括对涉案电子设备的检查结果；涉及计算机犯罪的日期和时间、硬盘的分区情况、操作系统和版本；使用取证与司法监定技术时，数据信息和操作系统的完整性、计算机病毒评估情况、文件种类、软件许可证以及对电子证据的分析结果和评估报告等所有相关信息。

尤其值得注意的是，在计算机取证与司法鉴定的过程中，为保证证据的可信度，必须对计算机取证和鉴定各个步骤的情况进行完全的记录、归档，包括搜集证据的时间、地点、人员、方法以及理由等，以使证据经得起法庭的质询。

（9）证据显示与质证

质证是指在法庭审判过程中由案件的当事人及其代理人，就法庭上所出示的证据采取辨认、质疑、说明、辩论等形式进行对质核实，以确认其证明力的诉讼活动。

无论是企业内部的计算机取证调查，还是涉及司法诉讼的计算机取证和鉴定，调查中获

得的任何证据都必须按照在法庭进行出示的标准进行准备。毕竟企业内部案件的调查人员也不能预料案件是否最终会走向司法诉讼，而这样的例子并不鲜见。因此调查人员所获得的证据应当接受法官、当事人及其代理人的质询，直至无异议才能成为判定案件事实的证据。

计算机证据也必须在法庭上显示，但是由于计算机证据的特殊性，使得计算机证据在法庭上进行显示及质询与传统证据有很大的不同。计算机证据有很大一部分是以电磁或光的形式记载的，因此这些证据的显示通常需要借助特定的设备，并且在显示过程中需要设定特定的环境。

1.2 计算机取证调查人员

1.2.1 计算机取证和鉴定人员的要求

计算机取证和司法鉴定包含针对各种计算机主机的取证与鉴定、针对手机与个人数据终端及其他电子设备的取证与鉴定、针对各种网络设备以及网络行为的取证与鉴定、针对多媒体资源的取证与鉴定等诸多方面。

一个想要具有计算机取证资质的机构，其首要因素是人，然后是过程和工具。许多想在计算机取证领域取得资质的公司却颠倒了先后次序，先在企业级软件和实验室硬件上花费了大量资金。当硬件条件完备后，现有职员再开始围绕新买的工具开发各种程序。最后，为了更好地发挥它们的性能，公司开始寻找拥有资质或经验的人。这一切其实是本末倒置的！

获得取证资质的更有效方法是从人员开始。应该聘用一位有经验的主考官来指导现有职员，引进补充人员，然后建立符合取证要求的取证程序。要找到一位有资质的人才，必须按以下步骤行事：

（1）要求可信的信息安全人力资源部门推荐优秀人才。

（2）关注著名机构中知识渊博的人才群体，如关键设施保护组织（InfraGard）和高科技犯罪调查协会（HTCIA）等，因为这些组织已经确认了其成员的背景或情况证明。

（3）聘用有直接调查经验的人员。

（4）仔细评估人员所获得的各种资质证书，如 CISSP、CISA、SANS 和 EnCase 等。

（5）假定候选人站在法庭证人席上，他们是否能作为专家应对司法审查。

当一个成功的候选人被授权运作计算机安全事件响应组后，首要任务是制定调查制度以及相关的程序。最起码该制度要包括以下内容：

（1）在什么情况下，谁将被授权进行调查？

（2）批准调查需要什么样的监督？

（3）怎样职能交叉地进行调查？

（4）哪些情节和事实是本次调查的凭证？

（5）如何处理调查结果？如何执行惩罚程序？

该制度规定了小组的运作结构、角色、责任以及调查范围。接下来制定调查中各方面的程序，规定谁执行特定的调查行动，常规程序必须包含哪些步骤，以及如何确认这些步骤。常规程序包含证据处理和保管链、获得取证或制作副本、应急事件通信、常规分析活动（邮件文件、文件系统、日志文件等）、引入第三方的交接条款、证据保存程序等内容。

司法鉴定人，是指由司法机关、仲裁机构或当事人聘请，运用专门知识或技能，对案件中某些专业性较强的问题进行鉴别或者判定的人员。我国实行司法鉴定人执业资格证书制度。

鉴定人的职业资格证书是鉴定人员从事司法鉴定活动的法律凭证。鉴定人的准入需要满足司法鉴定执业资格证书所必备的基本条件。

（1）具备下列条件之一的人员，可以申请登记从事司法鉴定业务：

- 具有与所申请从事的司法鉴定业务相关的高级专业技术职称；
- 具有与所申请从事的司法鉴定业务相关的专业执业资格或者高等院校相关专业本科以上学历，从事相关工作五年以上；
- 具有与所申请从事的司法鉴定业务相关工作十年以上经历，具有较强的专业技能。

因故意犯罪或者职务过失犯罪受过刑事处罚的，受过开除公职处分的以及被撤销鉴定人登记的人员，不得从事司法鉴定业务。

（2）鉴定人应当隶属于一个鉴定机构，从而从事司法鉴定业务。鉴定人从事司法鉴定业务，由所在鉴定机构统一接受委托。根据法律规定，如果鉴定人是案件的当事人或者当事人的近亲属，或者鉴定人担任过这一案件的证人、辩护人、诉讼代理人，以及鉴定人本人或近亲属与案件有利害关系，可能影响鉴定的公正性时，鉴定人应当主动回避，当事人也可以提出回避申请。

（3）司法鉴定实行鉴定人负责制度。鉴定人是中立的第三者，不受机关职能和行政主管的约束制约，也不应受权、钱、情的干扰。鉴定人应当独立进行鉴定，对鉴定意见负责并在鉴定书上签名或者盖章。鉴定意见虽是一种重要证据，对于证明案件事实有重大作用，但由于鉴定人的鉴定活动总是受到主观和客观多种因素的影响，这些因素必将或多或少地影响鉴定意见的准确性。鉴定意见所反映的案件事实与实际发生过的案件事实可能有出入甚至相互冲突，鉴定人对客体的认识虽然是建立在对客体科学分析基础上的并具有客观性，但是其对客体的解读是凭借自身对科学技术法则的认识和自身的经验，又带有一定的主观性，因此不同鉴定人，对同一鉴材鉴定时可能产生不同意见。正是由于这样的原因，法律规定多人参加的鉴定，对鉴定结果有不同意见时，应当一一注明。司法鉴定属于一种个人行为，而不是集体行为；某一专家一旦经法定程序被确定为案件的鉴定人，就应当亲自实施具体的鉴定活动，亲自在鉴定意见上签字，并亲自接受法庭的传唤或者控辩双方的申请，在法庭上出庭作证。

（4）司法鉴定人是一种诉讼参与人，享有下列权利：

- 了解、查阅与鉴定事项有关的情况和资料，询问与鉴定事项有关的当事人、证人等；
- 要求鉴定委托人无偿提供鉴定所需要的鉴材、样本；
- 进行鉴定所必需的检验、检查和模拟实验；

- 拒绝接受不合法、不具备鉴定条件或者超出登记的执业类别的鉴定委托。

（5）司法鉴定人作为诉讼参与人，也享有下列义务：

- 受所在司法鉴定机构指派按照规定时限独立完成鉴定工作，并出具鉴定意见；
- 对鉴定意见负责；
- 依法回避；
- 妥善保管送鉴的鉴材、样本和资料；
- 保守在执业活动中知悉的国家秘密、商业秘密和个人隐私；
- 依法出庭作证，回答与鉴定有关的询问；
- 自觉接受司法行政机关的管理和监督、检查；
- 参加司法鉴定岗前培训和继续教育；
- 法律、法规规定的其他义务。

（6）作为一个司法鉴定人的法律责任。

司法鉴定人若违反法定或约定的义务，应受到相应的法律制裁。司法鉴定人的法律责任同律师、会计师、医师等的法律责任相同，属于专家责任。其责任事件的产生，可能是主动积极的作为，也可能是消极的不作为。法定义务通常是由民法、刑法、行政法、诉讼法、证据法分别加以规定的。约定义务通常是司法鉴定人与委托人之间在法定义务之外依法协商补充确定的，符合法律规定的约束。

1）刑事责任，是由于司法鉴定人违反刑法规定、构成犯罪所应承担的刑事法律责任。主要表现为：主观上故意弄虚作假、隐匿事实真相，客观上作出虚假鉴定意见；故意泄露应当保守的国家秘密；故意索贿、受贿，以及其他违反法律法规构成犯罪的行为。在我国，司法鉴定人刑事犯罪的主要表现形式为伪证罪、受贿罪，国外还存在藐视法庭罪。

2）民事责任，是司法鉴定人违反司法鉴定委托协议内容或不履行鉴定义务而侵害了当事人民事权利所应承担的民事法律后果。违约或侵权主要表现为：没有按期、按委托要求完成鉴定任务，给当事人造成直接经济损失或给诉讼活动造成影响；没有依法接受监督、申请回避，从而带来严重后果；没有保守商业秘密或个人隐私，给当事人带来经济损失或造成精神伤害；没有认真接收、退还和妥善保管鉴材导致鉴材遗失、变质、毁损；没有充分理由而拒绝或延期鉴定的；没有适当理由拒绝合法传唤或不按期出庭作证。对于民事责任的处罚通常是，司法鉴定人违法执业或因过错给委托人造成的损失，首先由其所隶属的司法鉴定机构承担赔偿责任，再由司法鉴定机构对责任人进行追偿。

3）行政责任，是因司法鉴定人违反行政法规所应承担的行政法律责任。主要表现为：故意拖延鉴定时限，给诉讼活动造成了不良影响和损失；过失造成鉴定资料遗失、毁坏、污染、变质、变形、内容失真等内容与形式方面的变化，从而影响资料的完整性、真实性，使鉴材丧失鉴定条件；泄露案内秘密，造成不良后果，以及其他违反法律法规的行为。通常出现行政责任时的处罚为警告、责令改正、没收违法所得、罚款、责令停业、暂扣或者吊销执业证等。

1.2.2 企业内部调查取证人员与司法取证和鉴定人员的异同

计算机取证调查可以分为两个大类，一类是企业内部调查，即企业雇佣个人或公司对其内部违规行为和事件进行调查；另一类则是司法取证和鉴定，也即政府部门中涉及到负责犯罪调查和起诉的政府机构，对犯罪行为和事件进行调查取证和鉴定，通常司法取证和鉴定的结果是进行是否起诉和呈堂质证的选择，而企业内部调查则往往不一定非要进行司法诉讼的选择。但是，无论是企业内部调查取证人员还是司法取证和鉴定人员，他们在工作时都同样需要遵循严格的司法取证的合法程序。即使是进行企业内部调查取证，在调查之初，取证人员是无法预料案件最终是否会引起一场司法诉讼的，并且就算调查结束后仅仅进行企业内部惩罚，并没有引起司法诉讼，但是也不能保证几年后，是否会重新进入司法诉讼（这样的例子并不鲜见，特别是在因为侵权而导致员工离职的案件中），所以调查所获得的证据也必须按照司法流程进行归档和管理。

司法取证和鉴定人员与企业内部调查取证人员的相异之处在于，司法取证和鉴定人员进行计算机取证调查的主要目的是对嫌疑人进行是否有罪的判定，也即证明案件事实是否进行司法起诉。但是，企业内部调查取证人员为私营企业展开计算机调查时，调查人员应当务必使企业因调查而受到的影响减为最小。因为企业通常将重点放在正常运作和盈利上，所以在私营企业环境下，多数时候应把阻止非法行为以及将企业的损失和破坏降到最小这样的目的放在第一位，把调查与对嫌疑人的拘捕放在第二位。当然，如果在调查过程中发现涉及刑事犯罪等行为，就应当申请进入司法调查活动了。

在企业内部调查中，管理人员通常希望尽量减少或消除诉讼，因为处理民事、行政等诉讼的费用常常较为昂贵。如果在调查中发现使用被调查计算机设备的任何人可能从事严重违法行为，调查人员必须报请司法取证的介入，但是在这个时候，由于所调查计算机往往含有企业的一些商业机密，因此企业内部调查人员应当考虑如何把企业因司法取证介入而带来的商业机密信息的损失降到最低。

1.2.3 计算机取证人员的职业道德

作为一名计算机调查与取证分析员，职业道德是非常重要的，因为它决定着调查人员的诚信度。职业道德包括道德、品行和行为准则。作为一名专业人士，必须时刻展现出高水平的道德行为。为了达到这一点，在调查过程中，调查人员必须做到客观保密，还必须丰富自身的技术知识以及不断完善自己。我们在观看一些现代犯罪诉讼的影视剧时，常常可以看到律师是如何提问证人的。调查人员自身的品行往往是对方律师关注的问题，因此应保证这些方面不应当受到别人的谴责。

保持客观性也就意味着调查人员必须对案件形成并保持公正无偏见的观点。要避免对调查结果轻易下结论，应直到用尽所有合理线索并考虑所有可用的事实后再做出对结论的判断。调查人员的最终职责是找到支持诉讼的证据或为被告洗清罪行。在所有调查中，都必须排除外

界偏见，保持实情调查的完整性。例如，如果你受雇于一名律师，那么就不要让该律师的观点左右你的调查结果。调查人员的名誉和长期的职业生涯都取决于客观地对待所有事物。

调查人员必须对案件保密以保持调查的诚信度，保证只与有必要了解案件的人讨论案件。如果需要其他专业人士的建议，就只与他们讨论与案件相关的术语和犯罪行为，但不要涉及案件细节。在被指定为证人，或在律师和法院的指导下要求发布报告之前，调查人员必须对所展开的调查保密。

在企业环境中，保密是尤为重要的，特别是在处理因在上班时间利用公司计算机开办家庭企业而被停职的雇员这样的案件时。公司和雇员先前签订的协约很可能有这样的规定：公司在不提供救济金或失业补助的条件下解雇职员时，也不应提供不利于职员的介绍信。如果向其他人透露案件的细节以及该名雇员的姓名，那调查人员受雇的公司就可能因为违反协约而被起诉。

在有些情况下，公司内部调查的案件会演变成严重的刑事案件。由于法律体系的原因，也许要经过很多年该案件才会得到审判。如果有调查人员向别人谈论了该案件的数字证据，那么该案件可能因为在审判前受到公众注意而受到干扰。在调查人员协助律师调查时，调查人员只能与律师或与律师合作队伍中的其他成员讨论案件，与除此之外的其他人讨论案件都应该征得律师的同意。

除了保持客观保密的态度外，计算机取证调查人员还应通过不断的训练提高自己的职业素质。计算机调查与取证领域在不断地变化，调查人员应时刻与发生在计算机硬件与软件、网络及取证工具领域内的最新技术变化保持同步，积极学习能运用在案件中的最新调查技术。为扩展职业能力，调查人员应参加一些研讨会、协会以及由软件生产商为其产品开设的课程。

除了接受教育和培训外，成为专业组织机构的会员也可以丰富调查人员的资历。此类组织经常提供培训的机会及交流计算机调查领域内最新的技术发展与趋势。同时，还应该密切关注计算机取证领域新的书籍和论文的出版情况，尽可能多地阅读关于计算机调查与取证方面的书籍。

作为一名计算机调查取证专家，周围的人期望你能在政府部门及私有企业调查领域都达到较高水平，并希望调查人员能永远诚实、正直。因此，调查人员必须在生活的方方面面都做到高度自律，任何轻率的行为都可能让调查人员在今后的工作中陷入困境，在法庭上作证时给对方律师留下质疑调查人员工作结果的可乘之机。

1.3 电子取证相关工作基本程序

1.3.1 电子取证的基本程序

我国的电子取证程序的构建同样应遵循传统证据调查提取的原则、步骤，但由于电子证据自身的物理特性和技术特征，又决定了电子取证与传统的调查取证必定有所区别。我国的电

子取证程序可以概括为四个环节：

电子取证准备阶段：主要任务包括对电子取证的技术和设备的研发、取证人员的培训和选择、取证前信息收集、取证设备和器材选择、取证计划制定等。

电子证据收集保全阶段：主要任务是为实验室分析做准备，包括对物理空间中电子证据的收集与保全，也包括对虚拟空间中电子证据的收集与保全，既包括对计算机主机与其他电子设备的临场取证，也包括网络下载等远程取证。

电子证据检验分析阶段：电子取证的主要实施活动集中在证据分析实验室，对收集保全阶段的所得进行深入细致的分析和检验。

电子证据提交阶段：对取证结果进行汇总提交，主要任务是根据检验分析结果制作电子证据鉴定书、勘察检验笔录及其他书面报告。

1.3.2 计算机调查的程序

司法实践中，传统搜查已经形成了基本的程序：侦查人员通常要手持搜查证，强行进入某一个空间，搜索到有关的犯罪物品，妥善扣押之后离开。而对于计算机搜查应该怎么做，目前尚未有统一的规范。美国司法部联邦调查局将之总结为四种可供选择的方案，用作参考：

（1）在现场直接搜查计算机，查找到具体电子文件后打印成复制件予以保存；

（2）在现场直接搜查计算机，查找到具体电子文件后进行电子复制予以保存；

（3）在现场对计算机硬盘等存储介质进行完全复制，而后进行现场外检验；

（4）在现场扣押计算机硬盘等存储介质，完全取走进行现场外检验。

相比而言，以上方案各有优劣。第一种方案最为快捷和简便，任何略懂计算机基本知识的警察都能做到，同时，它对网络空间所造成的负面影响也最小，如从电子商务网络中打印电子文件不会影响商务活动的进行；不过，这一方案会损失大量有证据意义的电子信息，包括电子文件的日期、时间戳、路径、历史、添注等元数据。第二种方案比较简单和便捷，也获取到了元数据，不过受限于现场搜查的时间，要做到不遗漏任何电子文件是不可能的，再者，现场开机分析与复制容易改变电子文件的时间属性等信息。第三种方案克服了前两者的局限性，一方面完全复制涵盖对存储介质中元数据、系统文件与被删除文件等所有数据的复制，能保证原始数据的完整性，另一方面复制的方法采用比特级的镜像复制，能确保原始数据的每个比特都被精确地复制下来。不过，由于第三种方案耗时较长，而且将原始介质和电子数据留在了现场，只是在复制件上进行了检验，所以，也不为实务人员所认同。第四种方案既扣押了原始介质，又建立了精确的镜像复制，事后只在复制件上离线分析，并以原件加以验证，因而最能为司法人员和技术专家所接受，被称为“最佳选择”。目前在司法实践中，普遍采用第四种方案作为计算机搜查的基本程序。

1.3.3 计算机现场勘验的程序

在实施具体的勘验之前，需要明确三大原则：

- 固定和收集电子证据的措施应当确保这些证据的完整性；
- 实施勘验的人员必须经过专门的培训；
- 与电子证据的扣押、检验、贮存和运输相关的活动都应当进行记录、保存，以便接受后续审查。

计算机现场勘验的基本程序可概括如下：

（1）现场保护

任何现场勘验都离不开有效的现场保护，现场保护是现场勘验的第一步，其一般任务是，封存目标计算机系统并避免发生任何数据破坏或病毒感染，绘制计算机犯罪现场图、网络拓扑图等，在移动或拆卸任何设备之前都要拍照存档，为今后模拟和还原犯罪现场提供直接依据。保护人员赶赴现场后，通常应进行两方面工作：

1）封锁现场，进行人、机、物品之间的隔离。将现场所有人员迅速带离现场，并立即检查他们随身携带的物品，重点是书面记录、通讯工具、磁卡类可以读写的卡片、磁介质（软盘、光盘等）。有关人员在滞留检查期间，不能与外界进行联系。

2）加强现场保护。迅速看管配电室，避免发生突然断电导致系统运行中的各种数据丢失；看管现场以及现场周围的各种电信终端设施（例如传真机、调制解调器等），检查现场及周围有没有强磁场和可以产生强磁场的物品，妥善保管各种磁介质，避免被各种磁场消磁。

（2）现场勘验

现场勘验分为单机勘验和网络勘验两种。单机勘验是对单一计算机及相关设备的现场勘验，其勘验现场是封闭的计算机系统，有关证据主要分散于计算机的存储介质中，不涉及网络。单机勘验需要注意以下原则：

1）初步巡视物理现场后，确定中心现场和勘验范围，确定物理空间的勘验顺序。确定中心现场的方法是，以发观问题的计算机为中心，根据计算机系统日志或审计记录以及现场发现的其他相关信息，充分考虑犯罪嫌疑人等当事人的动机、手段以及计算机知识水平，对整个案件进行综合、全面的分析；勘验顺序可选择从中心到外围或者从外围到中心的顺序，根据已掌握的案件事实，将计算机所在的场所确定为勘验重点。

2）勘验单机的存储介质前，先用照相、录像、绘图、笔录方式对原始现场情况进行记录，对显示器屏幕上的图像、文字也应用照相、录像等方式来记录。特别是对于计算机本身及其相对于其他物品的位置、每根线的连接方式和方向，应尽可能准确地标明，贴上标号。

3）扣押数据存储介质或者通过镜像复制电子数据。对于需要扣押的存储介质，必须在关闭后方能进行位置移动，否则便可能破坏电子证据。在扣押电子证据后应将其妥善地保管在纸袋、纸盆中以防静电，而在运输过程中则应防止其接近强磁物体，特别注意不要靠近汽车上的无线电设备，注意温度、湿度、防尘。如果扣押存储介质不方便，可以在现场进行妥当的数据

复制。要用自备的、无毒的操作系统开机，记录被检查机器的时间设置，记下与实际时间的差别；因要保证在拷贝过程中数据保持一致，应采用镜像复制的方式，使磁盘里的隐藏信息、坏簇信息得以完全复制；若发现数据已经遭到破坏或删改，则可以使用专门设备读取磁盘中残留的数据；对复制件进行数字签名，保持它的完整性和真实性；将复制过程中使用的软件、复制过程、时间、地点、操作人记录下来，形成技术报告，以备庭审对质；最后，对硬盘、软盘、光盘等写保护，防止不当修改。

4）勘验中注意技术手段与普通现场勘验手段相结合，以发现与犯罪有关的传统痕迹物证，如指纹、足迹、工具痕迹、DNA 生物证据等。注意了解电脑的机种、型号、操作系统的版本与性能等，发现计算机设备有无不正确的损失等情况，检查计算机系统通信线路是否正常等；注意寻找电脑附近的纸张，垃圾桶里的物品，如其中的纸条可能写有电话号码、密码口令等；注意查看电脑的外围设备，如数码相机、扫描仪，若发现与犯罪有关应当予以扣押。

5）勘验中注意取得系统管理员的配合，邀请两名与案件无关、为人公正的人做见证人，侦查人员应制作现场勘验笔录，记录计算机犯罪案件现场勘验的情况，为诉讼提供证据。

网络勘验与单机勘验不同，网络的互联性和开放性使网上犯罪更难被侦破。在世界的任何地方，从网络上的任何一个节点进入网络，都可对网络上其他任何一个节点上的计算机系统实施犯罪。在这些案件中现场勘验的对象是虚拟的网络现场。网络现场导致电子证据分布广泛，从而给侦查造成障碍，同时电子证据分布的这种分散性恰恰也给侦查带来了一定优势。正是由于这种分散性，被调查者很难完全破坏掉所有的电子证据。保留在其他不同位置的电子证据仍有可能相互印证，构成一个完整的证据链。

（3）提取电子证据

无论是在单机勘验还是网络勘验中，调查人员都要有效地提取各种电子证据，以便用于实验室分析。一般来说，提取电子证据时可以采用以下步骤和方法：

1）记录和封存。记录和封存的对象主要是：各种数据、计算机软硬件、各种输入和输出设备、调制解调器、各种操作手册、各种连接线，同时还要注意提取计算机附近遗留的可能写有计算机指令的纸片等。记录时应注意：

- 必须提交有关提取电子证据过程的文字说明材料，并注意提取证据涉及到的硬盘等存储介质上具体文件的存储位置、文件名、文件后缀等细节；
- 所提取的电子证据来源必须与原始计算机和备份硬、软盘的编号一致；
- 要确定作案时间，注意计算机信息网络的主机时间和以北京时间表示的实际作案时间之间的差异。

2）初步分析。分析计算机的类型、采用的操作系统是否为多操作系统、有无隐藏的分区；有无可疑外设；有无远程控制、特洛伊木马及当前计算机系统的环境。特别注意开机、关机环节，避免正在运行的进程数据丢失或存在不可逆转的删除程序。

3）备份。利用同规格的软盘、硬盘、光盘、MO 盘等介质对系统中的相关数据、系统日志文件等进行复制备份。备份数目原则上应为两份。备份当中应注意的问题是：对于磁介质中

所有的数据按照其物理存放格式进行全盘复制，而不是简单地拷贝文件。

4）辨析数据。通过比较的方法，并运用数据分析技术对存储于系统中的大量数据进行分析，从中分辨出与犯罪有关的、反映案件客观事实的数据证据。在查找到相应证据后，应先确定其在计算机中存放的位置并摄像拍照。此后，将证据显示在计算机显示器上再进行摄像拍照。

（4）实验室分析

实验室分析是计算机勘验的核心和关键，其内容包括：分析计算机的类型、采用的操作系统是否为多操作系统、有无隐藏的分区；有无可疑外设；有无远程控制、木马程序及当前计算机系统的网络环境；分析在磁盘的特殊区域中发现的所有相关数据；利用磁盘存储空闲空间的数据分析技术进行数据恢复，获得文件被增、删、改、复制前的痕迹；通过将收集的程序、数据和备份与当前运行的程序数据进行对比，从中发现篡改痕迹等。

需要注意的是，分析过程的开关机阶段，应尽可能避免正在运行的进程数据丢失或存在不可逆转的删除过程。

（5）报告提交

计算机现场勘验和取证分析的所得和过程情况，最后均应作为报告提交，并给出必需的证明。对能够证明犯罪的电子证据，要转化为直观的证据，如鉴定结论。同时，在许多情况下，对已作为物证的物品也要进行鉴定。例如涉案的一些信息存储介质（如 USB 盘、存储卡、光盘和磁盘等）由于存储的信息内容不能直接呈现，也要通过鉴定来证明其与犯罪事实有关，才能发挥有效的证明作用。

1.4 企业内部取证调查和司法取证调查

1.4.1 针对私营企业内部取证现场的取证调查

私人或企业调查一般涉及私营企业和律师，这些律师主要处理违反公司制度和诸如不当解聘的诉讼争端。为私营企业展开计算机调查时，调查人员务必使企业因调查而受到的影响减为最小。因为企业通常将重点放在正常运作和盈利上，所以在私营企业环境下，多数时候应把阻止非法行为以及将企业的损失和破坏降到最小这样的目的放在第一位，把调查与对嫌疑人的拘捕放在第二位。当然，如果在调查过程中，发现涉及刑事犯罪等行为，就应当申请进入司法调查活动了。

（1）制定企业制度

公司尽量避免诉讼的方法之一就是建立和维护好员工能够轻易理解并遵守的规章制度，最重要的就是要建立员工合理使用公司计算机及网络的规章制度。企业制度为公司展开内部调查提供授权原则，该授权原则声明了谁有权展开调查，谁能够拥有证据和接触证据。

完善的企业制度规定计算机调查和取证审查员有权展开调查。同时企业制度也说明了公司对待雇员们的态度是公平客观的，所有调查都遵循相应的步骤。如果没有明确的企业制度，

公司就会处于被现有或以前员工起诉的危险之中。

（2）设置警示标语

私营企业和组织避免诉讼的另一个方法就是，在该企业组织的计算机上明确显示警示标语。当有计算机连接到企业网络、虚拟专用网络时，就会出现警示标语，它告知终端用户（终端用户就是使用计算机工作站执行日常任务而非系统管理员）本企业有权随意检查计算机系统及网络流量。如果不明确声明该项权利，当雇员访问公司计算机系统和网络时就存在虚拟隐私权的可能。有了这个虚拟隐私权，雇员们会认为他们在工作时传送消息的行为是受到保护的，就好像通过邮政机构发送信件是受到保护的一样。

警示标语为展开调查提供了便利。通过显示强有力、措辞严谨的警示标语，企业组织就有了在必要时对公司内部进行计算机取证调查的权利。

计算机系统的用户包括雇员与访客，雇员可以访问企业内部网络，而访客一般只能访问主网络。企业可以采用两种警示标语：一种针对内部雇员的访问（企业内部网访问），另一种针对外部访客的访问（互联网访问）。下面的列表推荐了应该在两种警示标语中出现的条款。在采用这些警示标语之前，应与公司的法律部门探讨是否需要进一步为工作区域或部门另外添加一些必要的合法警示标语。

根据企业机构的类型，可以在企业内部网中采用包含以下内容的警示标语：

- 访问本系统和网络是受限的；
- 使用本系统和网络仅限于公务往来；
- 雇主在任何时候都可对系统和网络进行监控；
- 使用本系统意味着同意雇主的监控；
- 未授权用户或非法用户访问本系统或网络将会受到惩罚和起诉。

当一个访问者通过互联网尝试登录公司系统时，可以显示包含以下内容的警示标语：

- 本系统属于 XX 公司；
- 本系统仅限于授权用户使用，未经许可访问本系统属违法行为，违法者将被起诉；
- 所有活动、软件、网络流量和通信将受到监控。

作为一名企业内部取证调查的计算机调查人员，应确保所显示的是完善的警示标语。如果没有警示标语，调查人员的调查权利可能会与被调查者以及其他用户的隐私权发生冲突，同时法院也可能做出不利于公司利益的判罚。

在实际的诉讼案件中，警示标语一直至关重要，因为这些标语决定了该系统用户对于存储在系统中的信息是没有隐私权的。警示标语还有一个好处就是，在诉讼时它是一个比制度手册更易提交的证据。

企业在计算机取证调查时应当建立授权条例。除了用警示标语向用户声明公司所有者的权利外，还应指定有权展开调查的授权调查员。

获得授权的调查人员在私营企业中展开计算机调查与在政府部门展开司法调查没有太大区别。在司法调查过程中，调查人员搜寻证据以支持刑事诉讼。在私营企业调查过程中，调查

人员搜查证据是为了支持对滥用公司财产行为的诉讼，但有些案件可能会涉及刑事诉讼。在企业环境中有三种情况较为普遍，即滥用或误用公司财产、滥用 E-mail、滥用 Internet。

私营企业内部的计算机调查大多涉及对计算机财产的滥用。一般来说，这种滥用是指雇员违反公司制度。对滥用计算机的投诉主要集中在雇员滥用 E-mail 和 Internet，也可能包括其他计算机资源，比如为谋取个人利益而使用公司软件制造产品。

E-mail 调查范围包括某人出于个人目的过分使用公司邮件系统，或者使用 E-mail 威胁攻击他人。一些最为普遍的 E-mail 滥用涉及发送攻击性信息和色情信息。

除了 E-mail 和一般的滥用外，计算机调查员还要调查 Internet 滥用。雇员对 Internet 资源的滥用包括雇员过分使用 Internet，如整天上网，还有在工作时浏览色情图片等。

Internet 滥用的一种极端行为是在网上浏览非法黄色图片，在大多数的审判中，浏览色情图片属于非法行为，计算机调查员必须运用高水平的专业知识来处理这种行为。在后面的章节中，你将会学习到对此类问题展开调查的步骤和过程。通过执行相应的企业制度，公司可以将它的责任过失降到最小。计算机调查人员的职责是帮助行政部门证实并纠正企业内部的计算机滥用问题。确保能够区别出公司内的滥用问题与潜在的犯罪问题。滥用问题违反了企业制度，而犯罪问题涉及商业间谍、挪用公款和其他行为，一些内部滥用行为也要负刑事或民事责任。正因为任何一起民事调查都可能会转化为刑事调查，所以调查人员必须以高度安全和负责的态度对待所有收集到的证据。

同样表面上对私营企业的调查可能只涉及民事而非刑事案件，但随着分析的进展，调查人员也可能会发现刑事案件的存在。出于这个可能，调查人员必须谨记在详尽研究民法或刑法体系后再展开工作。

在民间调查代理人或企业调查代理人将证据提交给执法机构时，企业通常要遵守银盘原则，即警官是执法部门的代理人，而企业调查人员的职责是将公司的风险降到最低。由于诉讼费用通常很昂贵，所以在收集到证据以后，一般以最低调的方式惩罚犯罪的雇员或者干脆就不追究了。然而，当调查人员发现了一起涉及第三方受害人的刑事案件时，无论从法律还是道德的角度，调查人员都有义务将这些证据交给执法部门。

许多公司制度都对个人财产和公司财产进行了区分，其中比较难区分的是 PDA 与个人笔记本电脑。假定有位雇员购买了一台 iPad 并将它连接到公司计算机上，当她用从邮件系统中拷贝下来的信息同步 iPad 上的信息时，又将 iPad 上的信息拷贝到公司网络上。因为这些数据存在于公司网络上，那么 iPad 中的这些信息是属于公司还是属于该雇员呢？

或者假定公司将 iPad 作为年终奖金的一部分发给雇员，那么公司拥有此 iPad 的所有权吗？当雇员将个人笔记本电脑带入公司并连接到公司的网络上时，同样的问题出现了。应该采取什么样的制度呢？随着计算机越来越深入人们的日常生活，这些问题是调查人员将经常碰到的。如何看待这些问题目前仍然存在争议，而公司也应建立明确的制度以解决这些问题。当然最安全的做法是不允许任何私人装置连到公司的资源上，从而限制了混淆个人信息与公司信息的可能性。

在企业内部调查中，调查员常需要在没有实验室和计算机保持不间断工作的条件下，在现场展开数字调查。例如需要调查某公司内部涉及侵害公司权利的雇员，该雇员利用公司服务器向外提供某些有利于个人的收费服务，然后将这些钱存入自己的账户。网络服务器和一些关键的网络设备中很可能记录下了某些重要的数字证据，但是如果针对网络服务器和关键网络设备进行中断服务的离线调查，即使在非常短的时间内使网络系统离线，都可能导致对公司利益造成更大的损失，调查员当然不能使用这种方法来获取证据；取而代之的是，他们获得磁盘镜像和其他信息时，始终使网络系统尽可能地保持在线状态。

1.4.2 针对执法犯罪现场的取证调查

在展开司法计算机取证调查时，调查人员必须熟悉与计算机犯罪相关的市、县、自治州、省以及国家法律，包括标准的法律程序和如何对刑事立案。在刑事案件中，嫌疑人通常是由于诸如盗窃、谋杀或强奸等犯罪行为而被审判。为了确定是否存在计算机犯罪，调查员可以提出诸如犯罪的工具是什么，仅仅是非法入侵吗，这是一起偷盗、入室盗窃还是故意破坏行为，罪犯是通过网络跟踪或电子邮件攻击侵犯他人权利的吗等问题。

目前，许多严重的罪行中大都涉及计算机，最为臭名昭著的是那些猥亵未成年人的案件。将数字图像存储在硬盘、USB 盘、各种存储卡及其他存储介质中，并流传到 Internet 上。毒品走私犯也常常会将交易信息记录在他们的计算机或平板电脑上。在各种经济犯罪的调查中，往往能够在嫌疑人的计算机或电子设备中搜索到有价值的信息。这些电子信息是非常有用的，因为它能帮助执法部门证明嫌疑人的罪行，帮助找到毒品供应者、其他同犯等。在追踪案件中，存储在计算机上被删除的电子邮件、数字图片和其他数字证据都可以帮助处理案件。

在对可能违法的罪行展开调查时，调查者应遵守的法律程序取决于当地法律标准、取证法则以及当地的习俗。但是总的来说，刑事案件需遵循三个步骤：投诉、调查和起诉。某人投诉，专家对投诉进行调查，在原告的帮助下收集证据并立案。如果犯罪已经发生，则在法庭上审判案件。

一起刑事案件开始于有人找到非法行为的证据或亲眼目睹了非法行为。目击者或受害者向执法部门投诉。基于事件或犯罪行为，原告做出控告罪行或推测罪行的控诉。由警官或警员询问原告，并书写一份关于犯罪的报告。执法机构对报告进行处理，并决定是否开始调查。

在展开调查时，执法部门要考虑保护公众的利益。但不是每一个优秀的警官都是一名计算机专家，通常根据对计算机取证调查知识的了解，可以将调查人员分为三个级别。

一级：在现场获取和查封数字证据，该工作通常由经过简单培训的第一响应的现场调查人员或警官执行。

二级：负责管理高科技调查，指导调查员搜索目标，熟悉计算机专业术语以及熟悉能够从数字证据中恢复什么，不能恢复什么。该工作通常由指派的专职计算机调查人员来处理。

三级：接受过数字证据恢复培训的专业人士，通常由数据恢复专家或计算机取证专家执行。

负责某案件的调查员，要清楚参与本案的所有警官和其他调查人员的专业特长级别。一

开始要估计好案件的范围，包括操作系统环境、硬件和辅助设备，然后确定哪些资源可以用来处理证据。例如，确定是否有合适的工具收集分析证据，是否需要召集其他专家协助收集处理证据。在收集到所需的资源后，调查人员的任务就是委派、收集和处理与控诉相关的信息。

当所调查的案件立案后，应将以上搜集的信息交给控诉人。当使用了所有已知可用的方法从被封查的证据中提取信息时，调查人员的工作就进入报告撰写阶段，接下来必须将收集到的证据写成报告交给控诉人。

项目分析

在本章的案例中，某公司的前部门经理 Adam 和技术骨干 Bob，被主管 Alice 怀疑对公司有侵权行为，因此委托计算机取证调查人员 Tom 进行调查。那么 Tom 在接受 Alice 的委托进行调查之初，应当确认这样的计算机取证调查是否合法，是否侵犯了被调查者以及相关人员的隐私权等问题。

从项目说明中可以了解到这样的取证调查应当是针对企业内部的调查。企业内部的计算机取证调查与司法取证鉴定不同，调查者首先必须确保获得进行计算机取证调查的授权。在本章引导案例中，如果 Tom 被公司主管 Alice 委托进行针对 Adam 和 Bob 的关于公司侵权案件的调查，那么 Tom 必须得到书面的委托授权书，从而明确界定调查性质、调查范围等要素。

当 Alice 决定对 Adam 和 Bob 的侵权嫌疑进行调查时，必须首先明确这样的调查是否合法，是否会侵犯 Adam 和 Bob 的隐私权。企业通常需要通过制定和发布合适的制度，提醒雇员注意并遵守这些制度以防止和处理犯罪行为。在 1.4.1 节“针对私营企业内部取证现场的取证调查”中，对于这一方面进行了有益的建议，即公司尽量避免诉讼的方法之一就是建立和维护好员工能够轻易理解并遵守的规章制度，其中最重要的就是要建立员工合理使用公司计算机及网络的规章制度。已建立好的企业制度为公司展开内部调查提供授权原则，该授权原则声明了谁有权展开调查，谁能够拥有证据和接触证据。

当 Alice 主管的公司具有这样的规章制度和明确的警示标语，同时经过咨询公司法务部门确定可以在必要的时候行使这样的权利，即确定对于 Adam 和 Bob 的侵权嫌疑进行调查是合法的时，可以采用两种方式进行调查，一种是委托专业的第三方计算机取证调查机构或公司进行调查，另一种是委托公司内部的计算机安全人员进行调查取证。无论采用哪种方式，都必须对调查者进行授权。

当然，由于本章案例中公司本身的安全人员就具有计算机取证调查的能力，因此我们从项目说明中可以了解到，Alice 是委托 IT 部门的调查人员 Tom 来调查这两名雇员的办公电脑和所有公司给予他们的存储介质，以便找到相关证据。并且这个案例的性质实质上是调查 Adam 和 Bob 是否侵犯了公司的权益，也即这是一个公司内部的侵权调查案例。