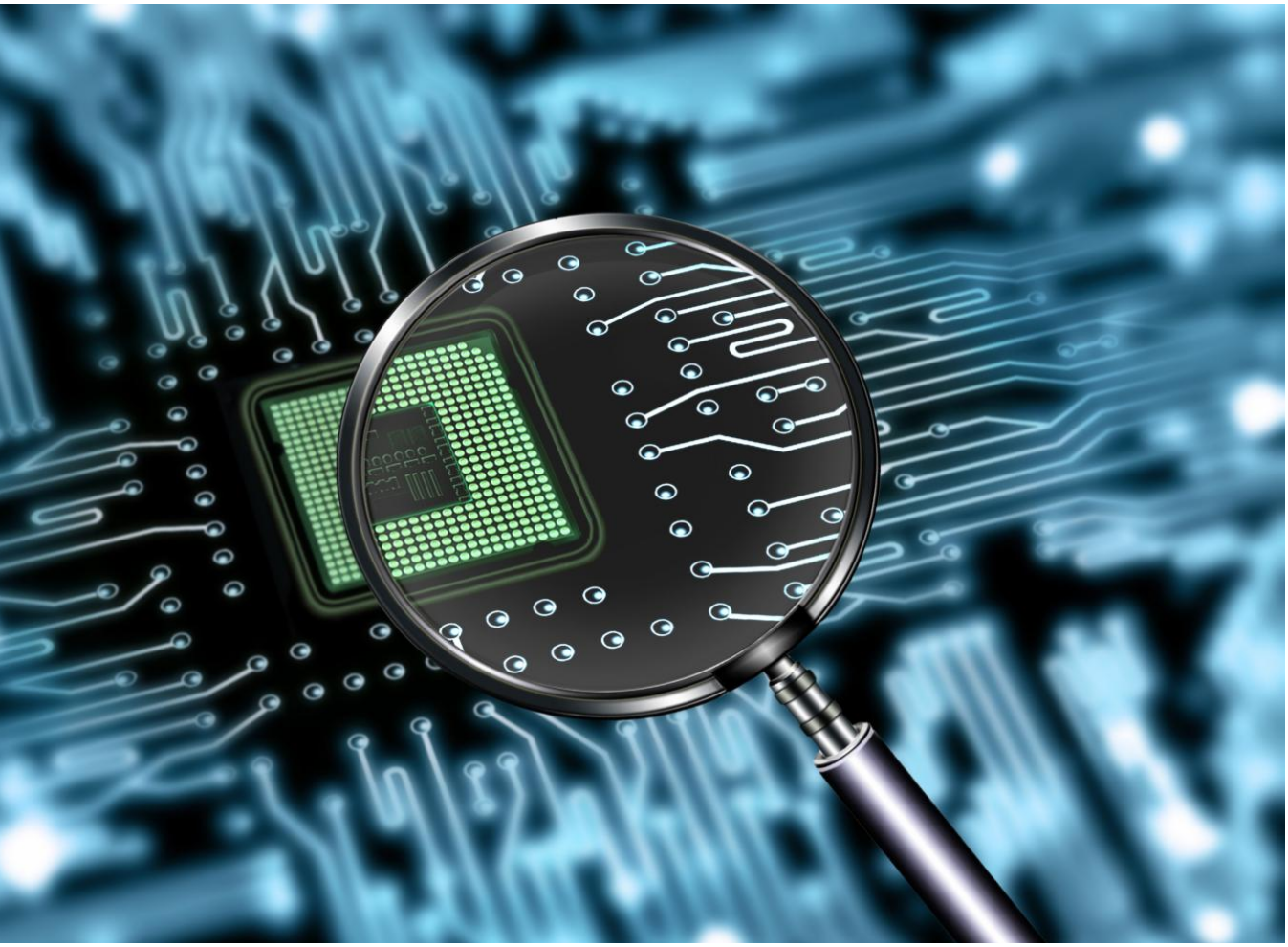


# 反舞弊调查中的电子数据

随着近年互联网和电子设备应用的飞速普及，电子数据取证也已逐渐成为侦办各类案件的重要手段和支撑。

我们结合星瀚内控和反舞弊中心的典型案例，对电子数据取证相关内容进行了梳理和汇编，以期和相关人士一起，共同提高防范意识和调查能力，筑牢企业运营安全的围墙。

# 反舞弊调查和电子数据取证

**（汇编）**

2020.07

舞弊是企业员工利用自身权力，通过非法手段，谋取个人不正当利益的行为，它无孔不入，存在于不同的经济体和各个行业之中，呈现出手段多样、行为隐蔽等特点。

舞弊人员大部分是企业高管，在企业制度并不完善的前提下，其行为从表面上看，往往具有一定的“合规性和合理性”，如何开展调查、调查的重点是什么、通过法律途径如何处理等已成为企业管理者面前的棘手问题。

星瀚内控和反舞弊法律中心长期以来深耕内控和反舞弊专业领域，围绕企业核心利益，致力于解决调查难、办案难、追偿难等问题，形成了自身独有的体系，能够为企业提供从调查立案、审查起诉、审判到经济追偿等不同阶段的完整服务。

随着互联网和电子设备应用的飞速普及，电子数据取证也已成为侦办各类案件的重要手段和支撑，在星瀚反舞弊体系中，发挥出巨大的作用和能力。但在实践中，我们感受到企业管理者、内控和监察人员、甚至是律师，对于电子数据取证是什么，如何开展电子数据取证，电子数据取证与法律服务如何有机协作等问题仍较为模糊，甚至茫然。为此，我们结合星瀚内控和反舞弊中心的部分典型案例，专门对相关内容进行了梳理和汇编，把电子数据取证这个技术专业性较强的工作，以平白的表述进行普及，以期和相关人士一起，共同提高防范意识和调查能力，筑牢企业运营安全的围墙。

# 目录

# 电子数据应用概述

电子数据作为一种新的证据形式，在司法实践中已被广泛应用，电子数据取证作为一门对技术性、专业性要求极高的工作，对法律工作者无疑提出了更高的要求，传统的调查工作在遇到电子数据时，往往陷入无从下手的困境。在我们的实践中，大量有价值的线索或证据材料便隐匿在看不见的 0 和 1 之中。今天，我们就从基础开始，对电子数据做一个简要的概述。

## 一、基本定义

### （一）电子数据

电子数据是案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。概括起来，主要包含了以下几种类型：

1、计算机文件，如：文档、图片、音视频、数字证书、计算机程序等电子文件。

2、用户日志和记录，如：用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息。

3、通信信息，如：手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息。

4、互联网信息，如：网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息。

### （二）电子数据取证

电子数据取证是一门借助计算机技术对电子数据进行获取、分析及鉴定的学科。主要包含了以下几块的内容：

1、数据恢复：对存储介质上被删除的文档、数据碎片进行恢复

2、数据获取：从存储介质上提取文档、图片、日志等各类数据

3、密码恢复：对开机密码、加密文件、用户登录密码等进行破解恢复

4、数据分析：紧密结合案情，对用户行为轨迹、关键信息进行综合分析，追查涉案线索，固定重要证据

## 二、身边的线索宝库

### （一）电子数据适用于“触物留痕”的刑事科学技术原则

奠定刑事科学技术的三大基本原理是：**物质交换和信息转移原理、同一认定原理、种类认定原理。**三大原理中的第一条“物质交换和信息转移原理”指的是：物质经过交换和转移，但物质成分和结构等特征一般不会发生变化，仍能客观真实的反映其原所在客体的本质，因而为刑事技术的检验认定不同时间、地点出现过的客体是否同一类客体或同一客体。

用通俗的话讲就是四个字——“触物留痕”。

触物留痕这一事实，能否在所有的场合都能被证实，这是与显示这种痕迹的手段和方法紧密相关的。因为留下疲迹的力有轻有重，其形成物质有多有少，遗留的时间有长有短，承受客体的条件有所不同，以及科技手段有齐有缺，操作水平有高有低，即使有了痕迹亦未必

均能被发现，有些痕迹，极其轻徽，以目前的科技水平尚无办法把它且示出来。可见，触物留痕是事实，能否把它发现出来又是另一回事。

手一经接触物体即留下了痕迹，这是唯物的、客观的，电子数据取证作为新兴的刑事科学技术，可以说同样也遵循“触物留痕”的原则，也就是说，一旦电子数据被访问，必然会留下相应的痕迹，而能否发现这些痕迹，则技术手段的齐缺和操作水平的高低来决定的。

**（二）常见的电子痕迹**

1、各类文件

最常见的有 office 文档、图片（相机、手机拍摄，各类程序生成）、音视频、PDF（合同、证照多以此种格式保存）、压缩文件等。

2、浏览器历史记录

主流浏览器有 IE、Chrome、火狐，360 等，这些浏览器会记录用户访问的网站、时间、用户名等信息，通过这些记录可以还原用户行为，刻画行为动机，佐证案情或直接证明。

3、电子邮件

常见的有网页版、客户端两种访问方式，企业用户多偏向客户端方式，比如 outlook、foxmail 等。邮件服务搭建常见有：自建服务器、租用腾讯、网易的企业邮箱。

4、即时通信

常见的是 QQ、微信和阿里旺旺等聊天记录。

【案例分享】中介飞单案件

通过微信图片解密恢复，结合案情圈定特定时间范围内特定图片，筛选出部分资金流水清单的截图，以此为基础进行扩展侦查和谈话，固定了案件关键证据。

**（三）易被忽略的电子痕迹**

1、系统日志

例如：通过计算机开关机日志记录，可以得知当事人是否有在非工作时间开关机的行为，结合具体案情可以推断用户行为动机。

2、应用程序日志

系统中安装的应用程序，启动、操作、关闭，都可能产生对应的日志文件，我们经常可以用到的就是 word 软件中的撤销恢复功能，这个功能就是通过记录用户每一步的操作来实现的。

3、系统临时文件

临时文件包含相当多的重要信息，包含了文档、数据库等，该类文件常以“$”开头，或以一串无规律的字符作为文件名，且没有后缀名，在正常情况下，系统不会自动识别，需要通过数据底层分析的方法实现。

4、网盘历史记录

通过对下载工具软件或网盘的日志分析，可以在存储介质上直接找到涉案证据，比如知识产权案件中的涉案文档、图片等，更重要的是，当原始数据被删除后，只要日志信息能够保留，就可以作为用户曾经操作过涉案文档的明确证据。

5、快捷方式

在特定条件下，快捷方式就是用户行为习惯的一个指针，结合案情可以从侧面反映用户的使用习惯。

6、网络链接

网络连接记录可以侧面反映使用人的上网地点，配合对网络交换设备的取证，可以推导用户的行为轨迹。

【案例分享】某案件中，用户使用百度网盘将涉案文件从公司转移至其个人电脑，通过对相关计算机和网络设备的取证分析，从底层代码中搜索到相关文件的片段信息，从而结合谈话突破案件。

## 三、电子取证与案情分析相结合的重要性

### （一）电子数据分析必须结合案情

电子取证从技术角度讲，就是从相关介质中回复、提取数据，所有的数字、文字、图片等信息，从技术角度上讲，仅仅是 0 和 1，但当这些数据与具体案情结合，就成为了有针对性、指向性的线索或证据。

一般来讲，数据分析可以结合以下几个方面的关键信息来进行：

1、当事人和关联人的基本情况，相互关系；

2、合同、票据等实物物证；

3、人物关系图、时间时间线等。

### （二）电子数据取证必须多次往复，逐层深入

电子数据取证是分步逐层深入的，其流程是：

1、电子数据固定

接洽案件初期，为客户定制相应的数据采集方案，防止在办案过程中出现数据损毁、丢失，对原始介质和数据进行保存，为侦查起诉阶段提供原始证据保障。

2、数据分析和恢复

采取“对位复制”方式对原始介质中的数据无损复制后做全盘数据扫描和分析，并利用文件特征恢复被删除清理的文件、字节碎片。

3、外围排查+案情分析

数据分析结果与具体案情想结合，同步重点人、物和时间的外围调查，从而梳理出人物关系、案件轨迹和时间线，进一步从中发现涉案线索。

4、数据深挖

通过时间、关键字信息，往复深入地挖掘数据，最终确定关键性涉案证据信息。

（本文首发于 2018 年 4 月 26 日）

# 案情主导型电子取证介绍

笔者常常在不同场合被问到一些电子取证方面的问题，其中有个比较典型的问题是——星瀚的电子取证和司法鉴定机构的电子取证一样么？

其实，星瀚电子取证在多年的实践中已经逐步形成了一套自身独有的工作体系和方法，归纳起来的核心就是案情主导型电子取证。

## 一、什么是案情主导型电子取证？

这个提法并不是拍脑袋想出来的，而是在星瀚长期的反舞弊实践工作中，逐渐形成、逐渐清晰的一个概念。

传统的司法鉴定电子取证，侧重点是“证据”，是在有明确的违法行为指向的前提下，从电子介质检材中恢复、查找可以证明犯罪事实的证据，为完善案件证据链提供有力的支撑。

案情主导型电子取证的侧重点则是“线索”，是把电子数据取证纳入到整体性的案件调查中，结合外围排查，开展综合性、全方位、多维度和递进式的数据分析，从无到有，从 0 到 1，至始至终围绕案情，对互有关联的人、事、地、物、时等信息，从深度和广度上进行拓展。如果脱离了对于案情的分析和研判，单纯利用技术手段提取、还原数据，那这样的电子取证只能称之为“电子取证技术”而不是“电子取证”。

## 二、如何开展案情主导型电子取证

在反舞弊实务领域，常见的刑法罪名往往就是职务侵占罪、非国家工作人员受贿罪等寥寥几个，刑法上定义的犯罪构成在原则上是通用的，因此案件调查必然有通用和原则性的方法。但从另一个方面来说，在案件调查初期，虽然可以套用某种格式化的调查流程，但随着调查的深入，单一个案就会显现出各不相同特点，例如行业背景、职务岗位、涉案个体或群体、关联人关系结构、实施犯罪的具体行为、侵占、收受、挪用的财物和资金金额等等，甚至某个涉案人的性格和行为模式，都决定了每起调查的唯一性，这就需要我们结合实情来分析，从而判断和调整调查的方向。

### （一）证据固定

“案情主导”始终贯穿在电子数据取证的全过程中，拿取证流程中的第一步“证据固定”来说，由于涉案电子数据介质（如个人电脑、移动存储、服务器、网络设备等）的所有权、使用权、所在地实际环境等不同，就要结合委托人反映的具体情况，有针对性地为客户定制相应的数据采集方案，防止在办案过程中出现数据损毁、丢失，在尚未公开的情况下，避免调查行动惊动涉案人员，还要灵活地采取适宜的方法对原始介质和数据进行保存，以便为侦查起诉阶段提供原始证据保障。

### （二）外围排查+案情分析

在进行数据分析之前，就应该先一步开展外围排查，收集主要的基础信息、涉案情节、重点人员、票据凭证和重要时间节点等信息，并从中进一步梳理人物关系、案件轨迹和时间线，为电子数据分析做好线索准备。

### （三）数据恢复和基础分析

基础的数据恢复和分析仍旧是围绕“案情”展开，以数据恢复为例：该恢复哪些文件？该

从哪些地方查找某种类型文件丢失的数据碎片？残缺的文件如何修补？这些都需要和案情结合，才更精准的发现目标,而且从取证技术的角度来说，确定目标后开展的数据恢复和分析，其效率可能是整盘数据机械性遍历的数倍乃至数十倍，在面对同一案件却有大批量检材的情况时，这也往往是案件调查是否成功的关键要素。

**（四）往复滚动地进行数据深挖**

在进行了第一轮初步外围调查和电子数据分析后，很大程度上可能已获取了原先并不掌握的新线索，尽管从表面上看可能尚无法利用这些新线索判断案件调查的结果。为此，就要通过人、时、地、物、事等维度，开展往复深入的数据挖掘，并且同步跟进外围排查，使两者能够有机结合、优势互补，形成良性互动，通过综合的手段，发现从电子数据或者外围调查中发现关键线索和证据，进而完成调查。

在此过程中，尤其要善于利用外围调查的手段，了解涉案人员行为特征和时间轨迹，结合其涉案介质中的电子数据痕迹如系统日志等进行时间轴分析，从数据中还原“作案现场”，给案件带来意想不到的突破。

（本文首发于 2019 年 2 月 14 日）

# 电子数据取证技术与律师调查工作的结合

星瀚内控和反舞弊团队一直致力于案件主导型的电子取证，结合外围综合调查，灵活运用技术手段，服务于核心调查工作。此外，还面向律师、公司法务等人员，经常性地通过沙龙、论坛等形式，开展电子数据取证知识普及的活动，拉近法律和技术两个行业的距离，探索一条技术派法律人的电子取证新路。

很多法律从业人员限于自身的专业领域，往往缺乏对于技术的必要了解，以至于在工作中容易忽视技术的力量，不懂得借助技术的手段提高工作效率、突破疑难案件。为此，我们汇总梳理了一些常见的问题，集中做个解答。

**Q：电子数据取证在律师办案中用得到么？**

A：早期的电子数据取证通常针对计算机和网络犯罪，目标是发现黑客入侵、病毒传播等行为痕迹。随着信息化的发展，当前的电子数据取证目的已经扩展到了日常社会经济民生活动的各个领域，因为人的活动借助计算机、智能设备和网络，所以人的活动就会在这些载体上留下痕迹。因此，律师办理的民商事、刑事等各类案件，只要有电子设备，只要存在有电子化的数据，就可以进行电子取证，包括但不限于：各类计算机和周边设备、网络设备、智能手机、智能穿戴设备、GPS 导航仪等等。在日常工作中有意识地增强电子取证方面的实践，往往会给律师调查带来意想不到的效果。

**Q：电子数据取证和第三方机构的司法鉴定有什么不同？**

A：很多律师在咨询电子数据取证业务时都会问到电子数据取证与第三方鉴定机构的不同。在我看来，第三方机构的数据鉴定重点在于鉴别、固定数据，使之成为具有法律效力的证据，主要侧重于证据的固定转化，解决证据的对错真假问题。而电子数据取证更多的是根据案情排查线索，挖掘数据，为突破案件和闭合证据链服务，解决证据或线索的有无问题。在此提醒：在案件调查初期，一定要在合法的规则前提下进行电子数据取证，以防证据失效。

**Q: 网页、聊天等截图或者拍照能作为证据吗？**

A：截图或者聊天记录，提交人必须要证实有效，否则不能作为电子证据。比较稳妥的办法是通过公证处进行公证，或者请第三方鉴定机构出具鉴定报告。如事出紧急，可以采取全程摄录像等方式进行固定。

**Q：手机取证中，安卓系统和苹果 IOS 系统哪个更难？**

A：安卓属于开源系统，IOS 内核保密，理论上是苹果 IOS 设备的取证更难一点。但也同时因为安卓是开源的，不同品牌、不同型号的手机，定制的安卓系统五花八门，反而给取证人员带来了各种潜在不明的障碍，我就在工作中就碰到过委托人需要导出保存手机的微信聊天记录情况，当时利用 itunes 备份 IOS 系统中的微信记录非常顺利，而在备份某不常见型号的安卓手机时，却遇到了诸如不能 ROOT 等的各种问题，反而非常不便。

**Q：如何保证电子数据的真实性和完整性，避免证据失效？**

A：保证电子数据完整性和真实性，需要进行数据保全，比如冻结、保护计算机等设备的软硬件不受改变，常规的方法是硬盘对位镜像拷贝。合规的方式可以参考最高人民法院、最高人民检察院、公安部 2016 年联合印发的《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》中电子数据完整性的保护方法来进行电子数据固定。比如，对作为证据使用的电子数据，应当采取以下一种或者几种方法保护电子数据的完整性：

（1）扣押、封存电子数据原始存储介质。

（2）计算电子数据完整性校验值。

（3）制作、封存电子数据备份。

（4）冻结电子数据。

（5）对收集、提取电子数据的相关活动进行录像。

（6）其他保护电子数据完整性的方法。

对于企业内部调查人员来说，可以自行进行证据固定，但如果对电子数据有证据上的要求，仍建议与第三方鉴定机构事先商定取证方案，同步固定证据，确保万无一失。

**Q：电子数据取证是不是从计算机中找到有用的文件？**

A：文件检索仅仅是电子数据取证的一个组成部分，要做好线索和证据的深挖，还需要配合其他方法，其中系统日志分析就是一个重要的取证手段。服务器上的日志记录了用户的登录时间、登录账号、来源 IP 和端口、操作的某些具体行为等等。个人计算机日志记录了开关机时间、USB 设备连接、网络使用、各类软件使用等等的各类信息，在具体办案实践中如果能灵活运用，将会大大拓展调查思路、增加线索发现的可能性。

**Q：文件加密有没有办法破解？**

A：有锁就有钥匙，没钥匙就要锁匠来解锁。文件被加密就要有密码，不掌握密码就要用破解手段。锁越来越牢固，解锁的手段也不断的跟进。加密文件的破解，只能说有可能实现，而不能保证一定成功，在破解过程中，往往还要结合外围调查的信息进行辅助的密码范围设定，才能提高密码破解的效率和成功率。

（本文首发于 2018 年 12 月 12 日）

# 三类典型舞弊犯罪的电子取证要点及案例分享

电子取证是个广义的概念，只要是信息化、数字化的电子设备都可以进行电子取证，但不同的案件类别、不对的对象介质、不同的涉案行为，都要根据实际情况有针对性的开展取证工作，比较典型如：网络攻击入侵案件、利用互联网犯罪案件等等，都有自身取证的重点方向和方法。同样，舞弊类犯罪案件的电子取证也因其自身的犯罪特点而有别于其他的案件。

企业舞弊行为按刑法罪名区分，在现实中常见的主要有三大类：

**（一）职务侵占和挪用资金类舞弊**

**（二）商业贿赂类舞弊**

**（三）侵犯商业秘密类舞弊**

这三类舞弊行为从实质上讲都严重侵害了企业利益，使企业在有形资产或者隐形价值上都遭受损失，但从手法上来讲却各有不同，所体现的特征与其所处的行业、职务和涉案项目往往会形成一定的对应关系，进而开展电子数据取证，也必须相应的调整方向，运用不同手段。

在长期的反舞弊案件调查过程中，我们逐渐形成了一套对于舞弊案件开展快速、有效、针对性的电子取证方法，切实有效地提高了案件调查的效率和发现重要线索的概率。

## 一、职务侵占和挪用资金类舞弊

### （一）人员行为分析

这两类舞弊行为属于资产侵犯型舞弊，涉案人员的一个明显特征是利用职务上的便利，目的是窃取、骗取、侵占本单位财物以或将单位财物占为己有。犯罪手法主要有：虚设中间环节，赚取差额费用；虚报业务，签订虚假合同；虚构或虚高应付合同款项或业务支出；利用商业活动中惯例的小额好处费这一明目，进行虚高或者虚构；夸大、虚构报销费用；利用单位系统内部漏洞，篡改数据，侵占挪用单位资金，制作假账进行掩饰。

### （二）电子取证要点

1、电子邮件：记录业务往来情况；

2、PDF、word、excel 文档：记录合同、预算、流水等重要涉案线索；

3、图片：在对外业务交流，同案人交流中，可能留存相应的资金流水、统计表格等重要信息的截图。

### （三）案例分享

在一起货运公司员工职务侵占案件中，涉案人员通过在正常业务流程中插入一个中间公司（虚设），按照每单 10-20%的比例抬高价格，获取非法利益。在电子取证过程中，调查人员重点分析了涉案员工电脑上的电子邮件和文档类文件，从中发现了主要的涉案线索和证据：

1、通过邮件客户端和 webmail 的历史记录，分析出涉案人员曾经使用虚设关联公司的域名邮箱，由此可以证实该员工与中间公司存在密切关联。

2、涉案人曾在电脑上留存部分合同、银行对账单等票据的 PDF 文档和图片，经电子数据恢复，找到关键证据。

3、对合同、发票、流水、到账、运费等涉案关键字进行全盘遍历检索，发现部分被删

除的文件碎片，结合外围排查，锁定涉案的时间、人员、金额、转账银行账号等重要线索。

## 二、商业贿赂类舞弊

### （一）人员行为分析

商业贿赂多发生于商品采购、服务外包、项目招投标等经营活动中，涉案人员身居要职，具有审批、签字等高级权限，利用职务便利，通过给予相关公司业务优先权、商业机密等好处，换取对方贿赂。在不同行业中，表现形式还有所区别，如：采购中抬高合同支付金额，销售中给予折扣，招投标中提供竞标机密等。

收受、索取贿赂的常见手段有现金、银行、支付宝、微信转账等，当下还出现了利用有价证券、境外地产、境外保险等方式进行收受贿赂的新趋势。

### （二）电子取证要点

1、电子邮件：重点查找涉案项目往来信息和附件文档。

2、文档：重点检索涉案项目、产品关键信息、涉案人近亲属关键字，尤其是关注修改过的同名文件副本，通过比对工具查看文本修改痕迹，结合文本修改者信息，发现修改价格等线索。

3、图片：重点检索查找银行流水或对账单等的截图，还要关注通过外围调查得到的重点关联人与涉案员工的个人相机拍摄的照片等图片，锁定人员关联性。

### （三）案例分享

在一起跨国公司员工舞弊案的过程中，调查人员通过多种手段结合，还原了人员关系和基本案情，并在与涉案人员询问过程中，以这些关键信息突破对方心里防线，使案件成功告破：

1、利用新型行贿手段关键字全盘遍历筛查，由此发现含有关键信息的文件碎片，同步结合外围排查，发现行为人现实轨迹与电子数据完全吻合。

2、对所有图片进行技术性排除，随后人工检查，发现涉案人员、近亲属和行贿人员密切往来的照片，并通过照片上 GPS 记录信息倒推出某时间共同前往欧洲旅游的行为轨迹，在涉案人员询问过程中，发挥重要作用。

## 三、侵犯商业秘密类舞弊

### （一）人员行为分析

针对电子数据的侵犯商业秘密行为，涉案人员通常会利用到即时通信、电子邮件、网盘、移动介质，甚至屏幕拍照等方式来窃取、传输涉案秘密信息，而事后为了掩盖作案痕迹，往往会卸载相关软件，并利用文件粉碎机等工具破坏原始数据，毁灭证据。

### （二）电子取证要点

结合被窃取的电子数据，以传输渠道和时间轴为重点，还原行为轨迹：

1、电子邮件分析；

2、网盘、文件粉碎机等软件分析；

3、移动存储介质插拔记录；

4、涉案秘密信息关键字筛查。

### （三）案例分享

在一起侵犯商业秘密案中，某公司技术员通过盗取其他员工账户的方式，侵入数据库窃取技术资料，并通过百度网盘转移至家里的个人电脑。

1、通过电子邮件排查向外发送涉密信息的线索，未果。

2、通过软件分析，发现曾经安装百度云盘但已被删除，通过数据恢复发现该软件留存在电脑中的痕迹信息和部分日志；

3、对涉案秘密文件的文件名和重点关键字进行二进制筛查，发现被删除后存留的文件碎片和时间，结合百度云盘的分析结果和 usb 口设备插拔记录，列出时间轴，还原涉案行为。

以上所列是对于一个案件概括性的调查方向，比如舞弊行为必然会关联到的资金、票据、合同、关联公司、关联人等。除此之外，还必须结合涉案人员个人工作、生活的其他痕迹，加以利用分析，才能抽丝剥茧，层层深入的揭开案件的真相。就笔者几年电子数据调查的不完全统计，尚未出现过一个完全同类型的案件，每个案件都有自身的具体情况，取证分析也必须结合具体的情况区别对待。

（本文首发于 2019 年 1 月 30 日）

# 取证的“套路”和“蹊径”——还原一个电子取证案例的全过程

电子数据取证过程必须严格遵从国家法律，按照法定程序进行，用流行的词来讲就是——“套路”，但在案件调查和司法实践中，我们往往要打破这个“套路”，以案情为核心，以破案为导向，积极转变思路，不拘一格地扩展、深挖线索，这也给取证人员的能力提出了更高的要求，优秀的取证人员往往同时具备技术、法律、侦查等多方面专业知识。

下面就以一个电子数据取证案例的完整过程，简要介绍取证人员从常规手段入手，通过合理分析推断，最终利用独特手段获取关键性证据的经过。

## 一、基本案情

某大型企业监察部门接到员工举报称，该公司某下属业务部门负责的一个大型项目中，有员工“吃回扣”、“收好处费”、虚假报销，致使公司利益受损，但举报人对涉案人员的人数、情况并不知情。

## 二、内部调查

针对这样“风闻”式的举报，公司监察部门仍给予了高度重视，为避免公开调查可能带来的不利影响，调查人员遵循保密原则，从外围开展了隐蔽式的前期调查，并将焦点逐步集中到业务部门负责人王某和经理张某身上，怀疑该两名员工涉嫌利用职务便利虚构业务项目，侵占公司巨额财产。

经查验业务档案发现，涉案业务的合同和票据存在伪造的嫌疑，合同为激光打印机打印，票据为针式打印机打印，此类文件必须通过计算机进行编辑。

调查人员随即以秘密取证的方式，获取了涉案人员日常工作使用的两台计算机硬盘镜像，经过电子数据分析，系统日志显示该两台计算机长期闲置，并未发现任何涉案线索。

在一方面，通过对伪造合同和票据的比对发现，伪造的数据、金额与真实的业务存在一定的对应关系，涉案人员伪造文书应是同步对照真实业务数据进行的，而公司业务数据集中保存在加密的文件服务器上，必须通过公司内部网络访问，且公司配发的个人计算机安装有限制外来移动存储设备的软件，较难通过 U 盘等设备拷贝外带。为此，调查人员将仍旧将重点定位在公司内部，经过排查发现该部门的一台计算机为多人公共使用，于是以 IT 部门硬件更新升级为名回收该计算机，进行后续电子取证。

## 三、常规电子取证

获得该计算机后，调查人员按照常规取证流程开展了电子数据取证，主要方面如下：

### 1、电子数据介质证据固定

取出计算机硬盘，连接取证设备，对硬盘数据作无损对位镜像拷贝，计算 HASH 值，然后封存原始硬盘以备司法诉讼阶段调取质证。

### 2、基本信息分析

分析镜像，系统基础信息显示，该公用计算机建有多个登录账户，其中一个登录账户名即为涉案业务经理张某姓名的全拼，进一步通过检查发现保存在该账户个人文档和桌面的个

人文档资料，由此确认以张某姓名全拼为用户名的计算机账户为张某使用。提取该计算机账户开关机和登录时间，为后续比对涉案伪造文件提供时间佐证。

**3、文件分析**

通过文件基础分析和恢复，从镜像中按常用文件后缀名如：DOCX、XLSX、PDF、RAR等各类文件约2000余个，导出后按文件类型分别存放，备查。

**4、最近打开的文档**

提取用户目录下 Recent 文件夹，发现涉案人员曾经下载、查看、创建、编辑的多个文件快捷方式，文件名明确显示与涉案的伪造文件有关，但快捷方式指向的路径和文件均以被删除，无法直接证明伪造文件的行为。

**5、输入法用户词库**

提取该用户账户使用的输入法用户自造词库，与伪造文件的部分特征关键字进行比对分析，显示涉案人员在操作计算机时曾输入若干非输入法自带的项目、设备、人员名称，可以推断涉案人员曾输入与项目有关内容，但仍无法直接证明其伪造文件的行为。

## 四、非“套路”的扩展侦查

结合基础分析，调查人员重新研究案情，勾勒和还原了部分涉案行为轨迹，决定从以下几个容易被忽视的方面进一步深入开展电子数据取证：

**1、临时文件和文件碎片关键字检索**

由于最近打开文档中快捷方式指向的涉案文件和文件夹均已被删除，因此调查人员对临时文件夹、未分配簇和文件残留区进行了关键字底层排查，从中发现部分与伪造文档相关的数据碎片，没有找到完整文档。

**2、数据清理软件**

结合用户 Recent 目录下大量的快捷方式和较少的文件数据碎片，调查人员提取了系统日志，从中发现“360 文件粉碎机”软件的使用痕迹，根据经验判断，该计算机硬盘中数据已基本无法完整恢复。

**3、USB 设备使用记录**

在之前对Recent目录的检查中发现，部分快捷方式指向的一个盘符并未在硬盘中出现，怀疑为涉案人员插入USB移动存储介质进行文件操作。

由于公司计算机预设限制移动存储介质连接，因此提取 USB 设备连接记录，将序列号与公司移动介质领用登记表进行比对后查明，该两名涉案人员曾领用的 U 盘曾连接该计算机。由此推断，涉案伪造文档极有可能存于相关 U 盘上。在确保涉案人员未做准备的情况下，突击检查办公场所，获取涉案U盘。

**4、加密文件破解**

检查涉案U盘发现空无一物，但庆幸的是，涉案人员仅仅是对U盘做了格式化，而并未使用文件粉碎机一类的软件做数据清理。通过数据恢复，获取多个带有密码的 DOCX、XLSX 和 RAR 文件。

随后，调查人员结合涉案人员及主要亲属关联人的基础信息，对身份证号码、生日、家庭住住、固话、手机等进行组合排列，利用字典软件生成专用密码字典，使用技术手段成功破解上述文档，最终完整获取关键证据文档，使得案件顺利告破。

## 五、经验总结

从上述案例可以看出，电子数据取证有一定的“套路”可循，比如常规的数据固定、基础信息分析、文件分类检索、系统日志勘察、关键字检索等等，部分案件仅仅用到这些常规流程就能顺利获取关键证据。

而具备一定的反侦查意识和手段的涉案人员，会利用硬盘格式化、系统重装、文件清理等方式来销毁电子数据，逃避检查。在这种情况下，我们就要拓展思路，紧紧围绕案情，利用临时文件和碎片字节检索、硬盘未分配区检索、USB 设备记录倒查、加密破解等等非常规技术手段对涉案线索进行深挖，尽最大可能为突破案件提供有力的支撑。

（本文首发于 2018 年 10 月 24 日）

# 反舞弊调查之保障电子数据原始态

在调查实践中，经常会出现企业内部调查人员不注意涉案信息保密，给涉案员工提供了处理电子数据的空间和时间，从而导致数据损失。为此，需要调查人员多采用“秘密”和“突击”的检查手段，确保在第一时间掌握涉案员工电子数据介质，使所获取的电子数据符合法律证据要求，避免出现因人为因素导致的数据“污染”。

## 一、辛普森案中的证据失效

说到美国的辛普森杀妻案，几乎是人尽皆知。1994 年，前美式橄榄球明星 O.J.Simpson 杀妻一案成为当时美国最为轰动的事件。此案当时的审理一波三折，Simpson 在用刀杀前妻及餐馆侍应生郎·高曼两项一级谋杀罪的指控中，由于警方的几个重大失误导致有力证据失效，以无罪获释，仅被民事判定为对两人的死亡负有责任。该案也成为美国历史上疑罪从无的最大案件。

血样、毛发、手套、作案工具，以及散落在现场的其他间接物证，原本都是“铁证”，然后由于警方在证据采集、固定过程中是因为“不严谨”或是“故意”，这些证据反而成了辩方为 Simpson 脱罪的合法理由，由此可见证据采集过程合法合规的重要性。

“**证据失效**”不仅是传统证据所面临的挑战，在电子数据已经被列为正式法定证据的今天，同样也是一个不容忽视的大课题。

## 二、电子数据原始态和 HASH

电子数据从本质上讲就是存储介质上的 0 和 1，具有易失、易改的特性，在数据保存、迁移、提取、分析过程中，任何一个操作都有可能改变数据原始的状态，取证人员的行为痕迹如果混杂于原始数据中，就等同于原始数据受到了污染，不再是原始状态。这就好比 Simpson 案中辩方专家在检验袜子上的血迹时发现其中含有浓度很高的螯合剂（EDTA），并非原始血样，而警方在抽取辛普森血样时也添加了同样的螯合剂。在证据污染、存在瑕疵甚至不合理的情况下，证据的证明效力就大大削弱了。

在电子数据取证中，要获知一个存储介质是否是原始态，就要说到一个技术上的概念——HASH 值。

Hash，专业翻译叫做“散列”，通常的叫法就是直接音译“哈希”，它是把任意长度的输入（又叫做预映射 pre-image）通过算法变换成固定长度的输出，输出值就是哈希值，简单说就是一种将任意长度的信息压缩到某一固定长度的信息摘要的函数，只要输入的信息发生一个字节的改变，则输出的哈希值就完全不同。

这种算法的转换是一种压缩映射，哈希值的空间通常远小于输入的空间，不同的输入可能会有相同的输出，所以不可能从哈希值来确定唯一的输入值，这个过程是单向不可逆的。

HASH 算法应用非常广泛，我们不做展开，在电子数据取证中，HASH 算法就是鉴别数据“原始态”的重要工具。

当取证人员获得一个数据集合（比如说一块硬盘）时，我们可以认为该数据集合是一个原始态，通过对这个原始态的数据集进行 HASH 算法校验，可以得到一个哈希值，将该哈

希值作为证据进行固定。此后，若原始数据发生任何改动，那么再次校验的哈希值将发生改变。因此只要校验 HASH 值不变，就可以充分证明数据仍旧保持原始状态，未做任何一个字节的变动。

**三、保证电子数据原始态的重要性**

取证分析过程中，保证电子数据的原始态至关重要，这种原始态从理论上来说，就是电子数据存储介质从脱离涉案人员掌控的时间开始，数据的任何一个字节都没有发生变动，从而证明电子数据与涉案人员的唯一性关联。

然而在现实的反舞弊实务中，无视电子数据原始态的现象比比皆是，星瀚受委托的所有案件中，在没有事前明确告知的情况下，几乎没有一起案件的委托人真正了解如何保障电子数据原始态。企业内部调查涉案人员的电子设备往往是由 IT 部们负责，尽管 IT 人员具备较高的计算机技术水平，但在未受过电子数据取证专业培训的情况下，常会习惯性地忽略电子数据的易失易改特性，第一时间进行直接开机查验，而其相应操作行为则被系统日志记录下来，使原始数据状态遭到破坏。在后期数据取证分析过程中，取证人员获取的数据就可能掺杂了前期开机查验留下的痕迹。

比如在某起员工舞弊案中，取证人员在时间轴上发现了大量文件操作、网盘下载、邮件检索日志等信息，而细看操作时间，竟然是涉案员工离职交还电脑的两个月后，这显然是企业内部其他人员而不是涉案员工所为。

更有甚者，有些企业调查人员还擅自在涉案电脑中安装数据恢复、电子取证类软件，在原始数据介质上进行数据恢复和分析，这些未按电子数据取证规范操作的行为，严重影响了电子数据的原始态，给后期电子取证带来了不可挽回的影响。

**四、相关建议**

（一）电子证据非常脆弱，很容易遭到破坏，调查人员应牢固树立原始证据意识，做好信息记录（必要时最好同步摄录像）。妥善保管电子设备、存储介质和其他数据，避免被强磁、高温、灰尘、潮湿等环境因素的破坏，不擅自在涉案设备上进行开机、登录、文件拷贝、网络连接、安装软件等操作。

（二）在调查开展前，咨询电子取证鉴定机构或专业取证人员，制定详细周全的取证方案，尽最大可能保证电子设备储存的内容不被破坏。

（三）很多数据只有在开机状态下才可以提取，如系统、桌面、进程、网络连接等信息，一旦关机则会彻底清除消失，因此，当电子设备若处于开机状态，还需要进一步考虑是否需要联系电子取证鉴定机构或取证专业人员在第一时间获取。必要时对操作系统桌面和当前时间等可以通过拍照方式先期进行固定。

（本文首发于 2018 年 10 月 18 日）

# 反舞弊调查之特征关键字排查

电子数据取证是一个严谨的过程，从取证准备到结案的整个过程都要按照符合法律诉讼要求的流程开展，为确保取证过程的效率和合法性，相关国家和组织提出了多种合理取证的模型，基础组成均为 3 个阶段：一是证据获取，即固定证据，如制作硬盘无损镜像，截屏保存等；二是证据分析，即数据分析与案情关联；三是证据表现，即对电子证据与案件关联性进行总结陈述。其中，证据获取和证据表现这两个阶段，相对而言更强调流程的合理性、合法性和操作的规范性，而证据分析阶段则是电子数据取证的核心和关键，涵盖了所有的取证技术，是最体现取证人员能力的环节。

分析的内容包括系统信息、文件信息等多种信息，黑客入侵案件还要进行功能分析，例如远程控制和木马程序功能和危害程度等。分析的过程主要包括：获取目标基本信息、文件过滤、文件分析、关键词检索、数据恢复、密码破解、证据标签管理、证据链梳理等。

不同类型的案件需要不同的分析方法，舞弊行为在电子数据上通常表现为**文档、邮件和图片**等形式，对于文档、邮件的数据排查，主要是以关键字检索来替代效率较低的人工检查，以保证关键信息完整筛查，此外，部分数据无法以常规直观方式读取，还需要借助专业软件进行代码层的检索，比如以二进制形式在介质中进行遍历，搜索已删除文件、文件松弛区（Slack Space）和未分配空间（Unallocated Space），从而达到找到数据的目的。

根据我们的反舞弊调查实践，舞弊行为所体现的特征与其所处的行业、职务和涉案项目常常能形成一定的对应共性关系，比如共性的有：转账、汇款、现金等，个案相关的有：人名、设备名、个人生活轨迹、习惯等。

如何快速、有效地设定关键字来进行第一次数据筛查？如何在初步排查基础上，进一步结合案情和排查结果进行反复深入的滚动筛查？涉案关键字一般隐藏在哪些文件里？哪些文件是容易被忽视而错过的？下面就结合部分案例，就如何利用好特征关键字开展电子数据取证做一点探讨。

## 一、舞弊行为共性关键字

舞弊行为最典型的三类罪名：一是职务侵占和挪（盗）用资金；二是商业贿赂；三是侵犯商业秘密、著作权或其他知识产权。这些行为在其动机、手段、方式上都具共性，而在涉案人员电子介质中，这些行为又同时表现出一定的关键词特征。

### （一）职务侵占和挪用资金类舞弊

资产侵犯型舞弊涉及职务侵占罪与挪用资金罪两个罪名，其特征是“利用职务上的便利”，窃取、骗取、侵占本单位财物以或将单位财物占为己有。主要行为特征包括：

1、虚报业务，签订虚假合同骗取单位财产；

2、虚报应付款，虚构或虚高应付合同款项或业务支出；

3、虚报“好处费”，按照商业惯例赠送小额“好处费”为法律所认可，业务人员据此虚高或者虚构“好处费”；

4、虚假报销，弄虚作假，夸大、虚假报销费用；

5、虚设中间环节，赚取差额费用；

6、篡改票据，盗窃、伪造支票或偷盗签发空白支票，转移资金；

7、篡改数据，业务人员、技术人员利用单位系统内部漏洞，篡改数据，侵占挪用单位资金，同时制作假账，填平账进行掩饰。

伴随以上行为，在涉案人员电子介质中，往往会出现以下特征关键字：***合同、采购、销售、发票、打款、到账、价格、收款、微信、支付宝、现金、转（帐）账、银行、账（帐）目、帐（账）号、帐（账）户、报销、签字等。***

**（二）商业贿赂类舞弊**

公司企业中的行贿受贿型舞弊一般属于商业贿赂的范畴，多发生于商品采购、服务外包、项目招投标等经营活动中，涉案人员往往身居要职，具有审批、签字等高级权限，如在采购过程中，利用签订合同的权力，抬高合同支付金额，在帐外以现金、转账等方式从供应商提取回扣；在销售过程中，以折扣明示、如实入帐的方式给予对方的价格优惠，接受对方“好处费”；在招投标中，向某特定投标人提供竞标机密，接受各类“好处”的回报。

收受、索取贿赂的常见手段有**现金、银行、支付宝、微信**转账等，但随着企业逐步重视内审监察，涉案人员的行为也呈现出两个趋势：

**1、形式多样化**

舞弊人员不再通过简单的资金转移方式行贿受贿，转而更多地利用有价证券、境外地产、境外保险等方式。例如：在星瀚 2018 年承办的一起大型跨国化妆品公司员工舞弊案的过程中，调查人员通过“香港”、“保险”、“受益人”等关键词对涉案人员计算机进行遍历筛查，对应找到其计算机上即时聊天内容备份的文件碎片，在此基础上结合外围排查，从而发现行贿人以为舞弊人员儿女购买境外保险的方式进行行贿的犯罪线索。

**2、行为隐蔽性**

舞弊人员往往会通过第三方人员、企业来进行财物的转移，以规避风险、逃避审查。因而，与舞弊人员相关联的第三方公司、主要近亲属的信息就成为了关键字排查的重要方面。比如，在我们经办的一起互联网金融信息服务公司员工舞弊案中，该员工利用其发放贷款项目的职务便利，以渠道费名义收受借款人及资金中介好处费，我方数据鉴定人员通过周边调查了解到其父母、配偶和子女的基本信息，通过对这些**近亲属姓名、身份证号码**的关键字排查，查到了相应的银行转账记录，从而掌握关键线索，顺利推进案件侦办。

**（三）侵犯商业秘密类舞弊**

在信息化高度普及的背景下，我们所遇到的绝大多数侵犯商业秘密行为，都是针对电子数据而进行的。涉案人员侵犯的行为通常会利用工作便利，通过网络传输、移动介质拷贝，甚至是显示屏拍照等方式，窃取机密信息和重要数据，出卖商业秘密给竞争对手，以此获取回报。

在电子取证中，关键字的设定往往是围绕被侵犯的电子数据展开，比如：**文件名、属性、关键内容信息**，比如在一起侵犯商业秘密案中，某公司技术员通过盗取其他员工账户的方式，侵入数据库窃取技术资料，并通过 QQ 软件的文件暂存功能转移至其个人电脑。我们从委托人处获得了被窃取的电子数据，将被窃取的技术资料文件中某些信息转化成特定的关键字列表，在涉案人员电脑上进行了数据恢复和筛查，成功发现了被删除后的文件碎片数据，同时

结合行为分析等综合调查手段，最终查清了数据转移的整个行为路径。在无法辩驳的证据面前，涉案人最终完整交代了作案过程，使案件顺利告破。

## 二、关联信息二次滚动筛查

舞弊行为具有的明显的交互性特征，其必然会与资金、票据、合同等往来紧密关联，在互联网成为人们工作、生活必需品的大环境下，涉案人员的舞弊行为与其个人工作、生活的其他痕迹往往是交叠共存，混杂相生，电子数据分析要善于利用这些信息，同时结合外围调查、公开信息排查等手段，才能抽丝剥茧，层层深入地揭示隐藏于普通信息中的涉案线索和证据。

在星瀚多年的反舞弊工作实践中，关键性线索和证据往往是通过多次反复排查而得到的。一般来说，经过共性关键字的第一轮排查后，往往会得到与具体案情相关的多个文档、邮件，从中我们可以发现、梳理出一部分个性化的个案关键字。将个案关键字与外围调查信息相结合，就能汇总整理出第二轮排查的关键字列表……以此往复深入，同时结合其他分析手段，往往就能够找到涉案的关键线索和证据。

在一起公司业务人员飞单案件中，我们通过对涉案人外围调查，获取了相关亲属姓名和关系，在第一次关键字排查中，把相关亲属的姓名作为关键字进行了筛查，排查出含有这些关键字的部分 xls 文件，而在这些文件中，同时记录了与人员对应的身份证号、银行卡号等其他个人信息，从而进一步在第二次关键字筛查中，利用了这些信息，最终查到了涉案人员记录有银行卡号对应的收付款账目明细，为办案提供了重要线索和证据。

## 三、关键字排查范围

### 1、基础排查文件类型

**（1）office、wps 文档**

office 和 wps 作为日常办公不可或缺的软件，利用其生成、阅读相关文档，是绝大多数公司员工必备的工作手段，也是舞弊线索最有可能隐藏的文件类别。比如：涉案人员通常会利用 office 软件制作虚假合同，记录财务收款信息等；

**（2）邮件**

outlook 和 foxmail 作为最常用的邮件客户端程序，其本地文件夹内保存和记录了大量往来邮件、通讯录信息，除了当前在用的邮箱，还会保存相关邮件的备份，生成备份文件，在取证中也是容易被忽视的一个重要数据源。

**（3）压缩文件**

在信息交换往来过程中，为了提高传输效率，往往会对文件集合进行打包，也就是压缩，用户压缩、解压、拷贝、传输等一系列操作后，常常是对相关文档进行删除、移动等操作而忽略压缩文件本身。因此，电脑中大量的压缩文件（zip、rar、7z 等）也应列为排查的主要范围。

### 2、容易被忽略的程序和文件

在电子数据关键字筛查中，系统临时文件、程序数据库文件比较容易被忽视。举例来说，百度网盘传下载记录会保存在相应的一个数据库文件中，其中可能包含了重要的用户行为痕迹，在我们曾经办过的一个侵犯知识产权的案件，就是用百度网盘的文件传输记录中，发现

涉案文件名信息，补足了证据链上重要的环节。

**3、已删除文件和数据碎片的搜索排查**

在特定条件下，用户刻意删除的文件，往往是突破案件的线索所在，因此，要尤其留心和注意对已删除文件的恢复和排查（数据恢复方面另行撰文介绍）。此外，数据碎片同样是很容易被忽略的数据源，特别是在数据恢复过程中，恢复的文件有很多都是不完整的，表面上看似一个文件，实际上是不同来源的数据字节拼凑而成的，需要通过非常规的技术手段来检索和排查。

（本文首发于 2018 年 9 月 5 日）

# 反舞弊调查之电子数据恢复（上）

在电子数据取证中，数据恢复是一项重要工作，被删除的数据常常是涉案人员最不希望被别人发现的数据，也意味着可能隐藏着最为重要的信息。

在一般人眼中，电子数据恢复技术高深莫测，然而在真实的电子数据取证中，数据恢复却是相对比较客观单一的步骤，恢复概率的大小与介质本身密切相关，除了硬件故障需要专业设备进行开盘等操作，一般的数据恢复都通过软件层面来解决。

## 一、什么是电子数据恢复？

电子数据恢复就是把遭受破坏导致丢失的数据还原成正常数据的过程。

数据丢失有很多原因，其中包括硬件故障（如硬盘故障无法读取）、软件问题（程序异常致数据丢失）、黑客入侵、病毒破坏（如某种病毒会导致 U 盘文件异常丢失）、异常断电（如处理到一半的文档遭遇断电）、人为操作（包括误操作和故意破坏）等。

以上这些都可能需要数据恢复，甚至从某种程度讲，用户由于各种原因忘记自己把文件保存在哪里了，由技术人员通过专业的检索方法帮用户找到目标文件，也算是一种数据恢复。

## 二、数据恢复的可行性

数据恢复是一个逆向进程，从恢复到完整的原始状态，到仅仅只是恢复部分数据碎片甚至毫无所获，这两个极端结果之间的任何情况都有可能发生。恢复的概率和介质的实际情况紧密相关，以下列举几个判断数据能否恢复的必要不充分条件；

1、原始数据存储在哪里？

2、数据是怎么删除的？

3、数据删除后存储介质是否仍在使用过？

4、数据删除后是否有新数据写入？

……

所以，要想搞清楚数据能否恢复，就要先了解一下数据是如何存储的。

## 三、数据存储

数据存储从原理上讲很简单，以机械硬盘为例，在硬盘的磁片上整齐排列着大量磁性单元，就像一个个永磁铁，这些磁性单元 S 极和 N 极的朝向分别代表电子数据最基本的单位 0 和 1。当硬盘写入数据时，盘片高速旋转，磁头准确定位在需要修改数据的一个个磁性单元上，通过施加电压，磁性单元的磁极被逆转，实现从 0 到 1 的改变。

可是这么多的 0 和 1，操作系统是如何知道具体是哪个数据存在硬盘的什么位置呢？这就引入了现代硬盘上一个重要的概念：分区表。

如果把整个硬盘比作一个图书馆，不同的分区就像不同的图书室，文件夹就好像一个个书架，具体数据则是一本本书。分区表就像图书馆的检索卡片，它包含了所有图书室（分区）、书架（文件夹目录）、书籍（数据）的信息，操作系统通过读取分区表，就可以将文件所处的逻辑位置（某某分区某某文件夹）和硬盘上的物理位置对应起来。系统查找数据的模式，

就好比人去图书馆检索图书一样。

**四、数据删除**

了解了数据的写入，再来看一个有趣的现象，平时在使用电脑时一定会注意到：写入文件的时间和文件大小成比例变化，大文件时间长，小文件时间短；但删除文件的时候，无论文件大小，几乎都是一瞬间就完成了，时间上没有明显的差别。

这种是由系统删除文件的机理决定的，写入过程与时间成比例是因为数据中的每个 0 和 1 都要在磁盘上进行校验，一致的就“放行”，相反的就“逆转”，每个磁性单元都如此地遍历一次，其表象就是写入时间与文件大小成比例。

而删除的过程，系统只是在分区表里将文件标注成了“不存在”，却根本不清除数据本身，也就好比在图书馆中把图书检索卡片拿走，却没有真正在对应书架上拿走那本书！这样做大大提高了删除文件的速度，改善了用户体验，而且由于硬盘上的磁极只有 SN 之分，当下次有别的文件要写入的时候，实际上未必需要修改所有的磁极指向——这也变相延长了硬盘的寿命。

**五、数据恢复**

因为机械硬盘特殊的删除机制，给数据恢复提供了机会。通过专用软件将所有没被新数据覆盖的部分进行扫描，对分区表进行重建，好比图书馆的索引卡片都遗失了，只要重新清点一遍库存，就能找到尚存的所有书籍，并且建立起新的索引，数据就是这么简单就被恢复了。

绝大多数民用级别的数据恢复软件在恢复刚刚删除的文件时都能应对自如，就是基于这个原理。

**六、硬盘格式化的数据恢复**

硬盘格式化与删除文件的机理是相同的，区别仅仅在于，删除文件时系统只是删除分区表中对应文件信息，而格式化则是把整个分区表重建成空白磁盘的状态，所以原始的数据没有受到影响，通过扫描磁盘，几乎可以完整重建原来的分区表，恢复所有数据。但如果格式化后大量写入新文件，或者长期频繁使用电脑，那就无法保证原始数据不被破坏，恢复相应文件的概率也就逐步降低了。

**七、数据恢复的技术含量**

数据恢复基础原理很简单，但实际情况千差万别，要想尽可能的恢复目标数据，远远不止上述情形这么容易。

比如，原始文件被删除后，硬盘又重新写入大量新数据，如果新数据就写在原始数据存储的磁盘位置上，覆盖了原始数据，使原始数据本身遭到破坏，那就只能对文件未被覆盖的数据残留部分进行还原恢复。

这样恢复后的文件一定是一种受损残缺的状态，可能丢失了文件头，也可能丢失了内容数据，所以正常的打开操作是无法完成的，要读取原始文件恢复出的部分数据，就必须借助其他工具进行数据读取、转换和拼接，这就需要技术人员具备较高的电子数据恢复知识水平，

熟悉各类文件底层代码，如果是针对案件调查的电子数据恢复取证，甚至还需要调查人员有足够的案情敏感度和丰富的办案经验才能完成。

【说明】结合目前技术和产业发展的现状，最广泛使用的电子数据存储介质主要是磁盘（如机械硬盘）和闪存（如固态硬盘、U 盘等）两种，以上表述均以机械硬盘为例加以说明，特此说明。

（本文首发于 2018 年 10 月 31 日）

# 反舞弊调查之电子数据恢复（下）

前文中我们对电子数据恢复这门技术的原理进行了介绍，分别对传统的机械硬盘和现下更流行的固态硬盘在数据存储、删除原理上的不同做了一些对比。本文我们将结合日常工作实际，分享几款常见常用的数据恢复软件和使用注意事项。

对于专业的电子数据恢复人员来说，只要数据没有被覆盖，数据就有可能恢复，因为实际情况千差万别，整个恢复过程会用到多种专业的设备和软件，并使用特殊和方法，才能尽可能的恢复目标数据。

但在一般的办公日常中，绝大多数情况可以通过使用一些简易的数据恢复软件进行有效的恢复，而不必动用例如 Winhex 这样需要专业技术的软件，下面简要做些介绍。

## 一、常见简易数据恢复软件

### 1、Easyrecovery

EasyRecovery 由世界著名数据恢复公司 Ontrack 公司出品的数据恢复软件，它威力非常强大，能够恢复丢失的数据，重建文件系统。它支持恢复不同存储介质数据，包括：硬盘、光盘、U 盘/移动硬盘、数码相机、手机、Raid 文件恢复等，能恢复的文件类型包括：文档、表格、图片、音视频等。无论文件是被命令行方式删除，还是被应用程序或者文件系统删除，都能实现恢复，甚至能重建丢失的 RAID。


此外，EasyRecovery 操作简便易学，一般的数据恢复只需要按提示一步一步操作，就能完成整个恢复过程，即使电脑小白也能很快地上手。同时，它价格便宜，操作安全，用户自主操作时不会在源驱动器上写入任何东西，也不会对源驱做任何改变。

### 2、Finaldata

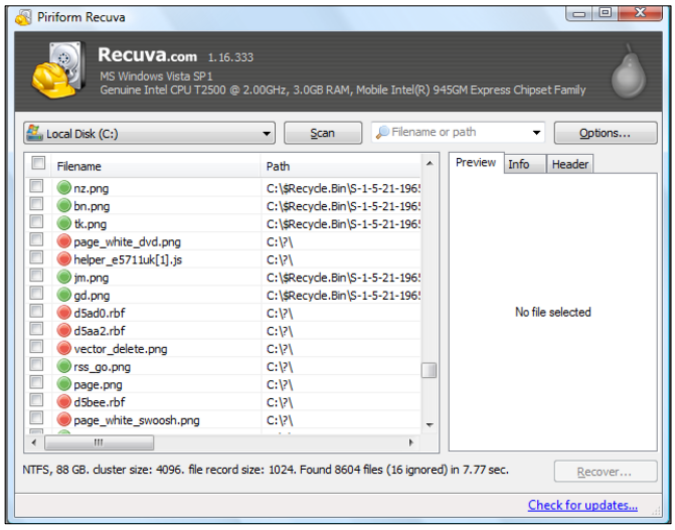
Finaldata 作为数据恢复软件的最大特点就是——恢复速度快，大大缩短了搜索丢失数据的等待时间，速度快不仅表现在硬盘扫描上，也表现在已找到文件的恢复保存上，基本比其他同类型软件快一倍以上。


在数据恢复功能上，Finaldata 也很强大，不仅可以按照物理硬盘或者逻辑分区来进行扫描，还可以通过对硬盘的绝对扇区来扫描分区表，找到丢失的分区。

Finaldata 同样以其简单易用而受到喜爱，从安装到使用，只要按照软件提示一步一步进行即可，一般的数据恢复，只要选定逻辑驱动器或整个物理磁盘，FinalData 就会自动的搜索和分析哪些是正常的目录和文件，哪些是已被删除的文件，在完成所有检查后，目标任务驱动器所有文件会自动分类，以表格形式罗列出来，包括正常的目录、已删除的目录和删除的文件等大类，以及文件名、大小、状态（是否破损）和创建时间等具体信息，连文件所在的物理簇位置也会显示，大大方便了数据的恢复。

**3、Recuva File Recovery**

Recuva File Recovery 由 Piriform 公司开发，是一款免费 的 Windows 平台文件恢复工具，它可以用来恢复硬盘、闪盘、存储卡中被误删除的文件，只要没有新数据覆盖写入，无论格式化还是删除均可直接恢复。

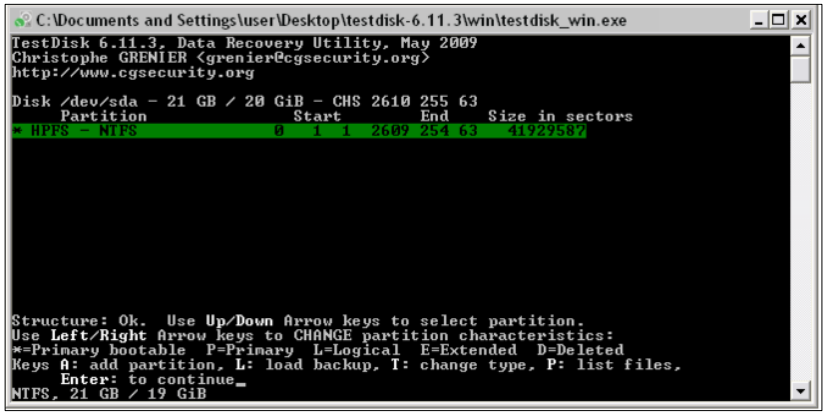



软件的操作也非常简单，只要选择要扫描的驱动器后点击扫描按钮即可，搜索被删除文件的速度极快。新版本在向导中还添加了对 iPod 的支持，优化了深度扫描和对可移动存储驱动器的支持。

除此之外，Recuva File Recovery 的“预览已删除文件”功能，可以在恢复文件前预览文件内容，以确认要还原的数据就是目标数据，从而节省了时间。

**4、TestDisk**

TestDisk 是一款命令行形式的磁盘修复工具，可以修复由于软件缺陷或某些病毒导致的分区丢失或分区表丢失导致磁盘无法启动的问题。它通过 BIOS 或操作系统查询硬盘特性(LBA 大小和 CHS 参数)，快速检查磁盘数据结构并恢复、重建分区表，从而恢复相关数据。




虽然该软件也属于简易型数据恢复软件，但由于是命令行界面，对于普通电脑用户来说，就显得不如图形界面软件那么友好了。

**5、Restoration**

Restoration 是一款免安装且大小仅为 229 Kb 的免费软件，它支持被删除文件的找回，还能支持输入关键字或扩展名对特定文件的恢复。

此外，该软件还有一个“Delete Completely”功能，可以让用户对被删除文件进行扫描检索，对检索出的可恢复文件进行彻底的删除。

小巧、绿色、非常易用是该软件最大的特色。

上述这些软件都是笔者日常使用的，除了这些以外，在互联上上还可以找到很多优秀的数据恢复软件，免费和收费软件都有，即使是收费软件，价格也非常平易近人，可以下载一些试用版本，根据自己的使用习惯来进行挑选。

**二、数据恢复软件使用原则和注意事项**

为了避免数据的“二次破坏”，在数据恢复过程中，必须要相应地遵循一些规则，操作上也尽量按照规定的流程来进行。

1、在发现数据丢失（比如误删除）后，必须马上停止一切操作，最好是直接强制关机（长按电源按钮或直接断电），因为哪怕是保存一个正在修改的 WORD 文件，都有可能导致目标数据无法恢复。

2、禁止对需要作数据恢复的源盘做数据写入操作，包括在源盘上安装数据恢复软件，把需要恢复的文件直接写回到源盘上等等，而应采取只读方式制作全盘镜像，在镜像文件中进行恢复操作，以防恢复过程中的意外情况而导致更大的数据损失。

3、不要做 DskChk 磁盘检查。文件系统出现错误后，系统开机进入启动画面时会自动提示是否需要做磁盘检查，默认 10 秒后开始进行 DskChk 磁盘检查操作，这个操作有时候可以修复一些小损坏的目录文件，但很多时候会破坏数据。因为复杂的目录结构它是无法修复的，所以修复失败后，会在根目录下形成 FOUND.000 这样的目录，里面有大量的以.CHK 为扩展名的文件，从而影响正常的数据恢复。

4、硬盘在出现故障异常而无法读取时，不要尝试没有把握的方法（比如重新格式化、重建分区表等等）。这样的操作，只会让让原本可能很简单的恢复工作变得异常复杂，同时，错误的操作也会大大降低数据成功恢复的可能性。

5、建议在日常使用的计算机中安装一到两款数据恢复软件作为常备，以便应对一些简单的数据丢失，也可以避免在遇到问题后临时安装数据恢复软件对源盘的数据写入和原始数据破坏。

最后老生常谈一句

——“硬盘有价，数据无价！”

强烈建议，一定要养成备份数据的习惯，通过本地磁盘、刻盘、移动存储、网络硬盘等多重备份的方式，以确保重要数据的绝对安全。

（本文首发于 2018 年 11 月 14 日）

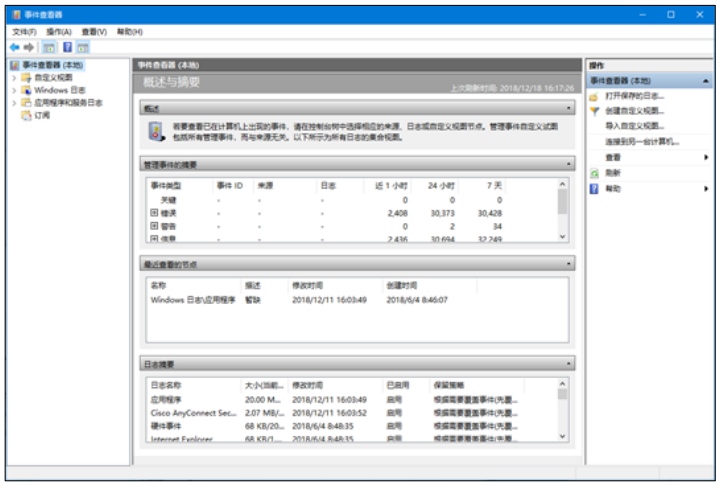
# 反舞弊调查之 Windows 日志中隐藏的线索

Windows 系统在使用中会记录大量日志信息，主要分为两大类：一是 Windows 事件日志；二是应用程序和服务日志。

对于调查人员来说，日志是非常有价值的电子数据，通过细节分析，可以倒推追查特定用户在系统中做了什么，或者系统自动做了什么，还可以显示远程活动曾经尝试或成功执行的操作。

在案件调查的日常中，可以有机地结合外围排查，对涉案人员的行为做出更为全面的侧写，能够发现隐藏的线索，还能成为应对涉案人员抗辩的有力支撑，成为破案的关键环节。

## 一、Windows 事件日志



事件日志留存了 Windows 系统中关键日志事件的详细资料，事件日志文件（evt 文件）以特定数据结构方式存储内容，每条记录事件中包含 9 个组成部分，分别是：日期和时间、事件类型、用户、计算机、事件 ID、来源、类别、描述、数据。

**事件日志分为 3 大类：**

**1、系统日志**，记录系统进程、设备磁盘活动等系统事件的详细资料，包括设备驱动无法正常启动或停止、硬件失败、IP 地址重复、系统进程启动、停止及暂停等；

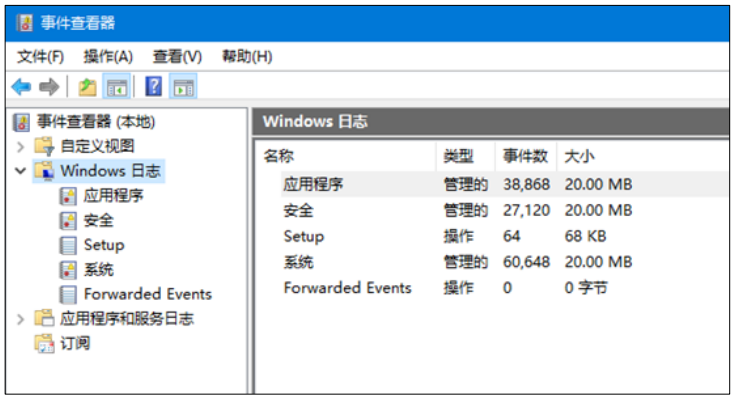
**2、安全日志**，记录登录、退出和其他安全活动信息，包括安全性相关的事件，如用户权限变更、登录和注销、文件及文件夹访问、打印等；

**3、应用程序日志，**记录应用程序、软件相关事件，包括错误、警告及任何应用程序需要报告的信息。

根据日志取证，调查人员可以追根溯源地了解到计算机上曾经发生过哪些具体事件，是非常重要的取证对象。

## 二、事件日志的查看方法

查看系统日志的标准方法是使用 Windows 系统自带的“事件查看器”（可以通过运行“eventvwr”来启动），如下图：




在事件查看器中，系统日志被分为成 Windows 日志和应用程序和服务日志两大类，其中 Windows 日志包括了应用程序、安全、Setup、系统和 forwarded events（转发事件）。

事件查看器可以将日志文件导出为 evt、evtx、xml、txt 和 csv 等格式，并导入其他系统的事件查看器进行浏览。因为日志文件格式在各个 WinNT 版本中通用，所以调查人员也可以利用本地计算机的事件查看器远程连接其他计算机，以管理员权限查看浏览日志文件。一般来说，为防止打开的文件受损，原则上都会对源数据进行全盘镜像复制后对镜像文件进行操作，以防原始证据失效。

调查人员可以利用事件查看器“筛选”功能，显示特定时间类型和时间段的相关内容。

## 三、日志核心文件

事件日志记录在系统内置的三个核心日志文件中，应用程序日志为 AppEvent.evt 或 Application.evtx，系统日志为 SysEvent.evt 或 System.evtx，安全日志为 SecEvent.evt 或 Security.evtx，该三个文件的默认大小均为 20MB，当事件数据超过 20MB 时，新的日志将优先覆盖最早的记录。应用程序及服务日志文件的默认大小为 10MB，超过该限制也会优先覆盖最早期的记录。

## 四、事件日志的类型

Windows 事件日志共有 5 种事件类型，所有事件必须且只能属于其中的一种类型。

**1、Information（信息事件）**：指应用程序、驱动程序或服务的成功操作的事件。

**2、Warning（警告事件）**：指非直接、主要的，会导致将来问题发生的事件，如磁盘空间不足或未找到打印机时，会记录一个“警告事件”。

**3、Error（错误事件）**：指用户应知道的重要问题，通常指功能和数据的丢失，如某个服务不能作为系统引导被加载，就会产生一个错误事件。

**4、Success audit（成功审核）**：记录用户登录和注销、对象访问、特权使用、账户管理、策略更改、详细跟踪、目录服务访问、账户登录等事件，如所有成功的系统登录都会记录为“成功审核事件”。

**5、Failure audit（失败审核）**：用户访问失败会被作为失败审核事件记录。

## 五、取证常用的日志事件

### （一）应用程序日志

应用程序日志由应用程序使用，Windows 允许第三方软件通过 API 记录应用程序事件，防病毒软件和安装程序通常会使用这样的功能，在调查中经常使用到的有：

**1、确认软件安装。**使用微软安装程序的情况下，通过事件 ID11707（成功）、事件 ID11708（失败）和事件 ID11724（卸载）来记录软件包的运行，查看这些 ID 可以发现特定软件的安装、试图安装和卸载的时间。

**2、确认和排除病毒感染。**大多数防病毒软件在检测到病毒时，会产生一个 ID5 事件。案件调查中，涉案人员有时会辩解称系统问题是病毒引起，通过查看这个事件，可以显示和排除其声称的时间内是否有病毒发作。

**3、启动和关闭防火墙。**记录了用户主动打开或关闭系统防火墙的行为。

**4、检查黑客攻击企图。**ID 为 1000~1004 的事件记录有错误的应用程序，可以提供应用程序漏洞被利用的线索，事件 ID4097 也有可能代表类似活动。

应用程序日志事件常依赖于特定系统中安装的具体应用程序，以及是否独立使用事件日志服务，或者利用本地私有日志对系统日志进行补充，所以调查人员在检查应用程序日志之外，通常还必须检查应用程序是否使用了本地私有日志记录。

**（二）系统日志**

系统日志可以捕获由系统自身产生的事件。任何自动执行的操作，或直接利用 OS 功能的用户驱动操作都会记入日志，包括软硬件安装、打印作业和网络层事件等。取证人员关注的系统事件常与案件的性质和被调查者的抗辩有关，常见的有：

**1、事件日志启动和停止。**事件 ID6005 和 6006 代表日志服务的启动和停止，主动关闭日志服务的行为往往值得深入追查。

**2、系统关系和重启。**事件 ID6008 表示系统的一次意外关闭，6009 则和系统重启相关。当发现 ID6006 后不久紧跟 6009 事件，通常可以认为是系统原因。事件 ID1074 显示引起系统关闭的进程，ID1076 显示系统关闭的原因。

**3、登录失败。**事件 ID100 表示一个已知账户的验证失败，调查中发现的这类事件，有可能是特定用户通过猜测密码或使用穷举等破解工具的线索。

**4、机器信息改变。**事件 ID6011 表示系统名称改变，如果发现名称与现存信息不匹配，就要重点查找这个事件 ID。

**5、打印。**ID10 显示的是打印作业和来源，以打印请求者用户名的方式显示。

**（三）安全日志**

安全日志是所有日志的基础，登录、注销、尝试连接和改变系统策略等关键事件，都会在安全日志中反映出来。企业为了支持安全事件调查和溯源，通常会在本地或组策略下的审核策略中要求计算机系统激活如审核账户登录事件、账户管理、登录、策略改变、特权使用等。其中，登录和注销对于证实什么人在什么时间执行了什么操作尤为重要，而其他安全事件则根据案件不同，会对某些特定的调查有帮助。

**1、成功登录和注销事件。交**互式的登录事件通过事件 ID528 来描述，是登录类型的一个子类，调查人员比较关注的登录类型有 ID2（本地）、ID3（网络）、ID7（Ctrl+Alt+Del 或屏幕解锁）、ID10（远程桌面）、ID11（缓存的用户凭证登录）。

另外，注销事件显示了某用户连接的时间段，以 ID551 为用户启动注销的开始，ID538 为结束。远程桌面连接中，ID683 表示断开连接，ID682 表示重新连接。

**2、登录失败事件。**登录失败是判定是否有人进行密码猜测或暴力攻击的有力证据之一，日志会记录失败尝试的不同原因：ID529（用户名或密码错误）、ID531（账户不可用）、ID532（账户到期）、ID539（账户被锁）、ID533（越权访问资源）等

**3、对象访问。**在一个特定对象属性的“安全”选项卡上点击“高级”按钮，可对待定的 NTFS 文件和文件夹进行审核。激活对象审核可以记录从试图读取对象到成功删除对象的任何操作，。如果系统开启这个级别的审核，就能显示某个特定实体在何时被访问、被谁访问、特定文件和目录的改变和删除，或者突出显示对关键对象的非法访问企图。相关事件有：ID560（打开对象，试图打开一个文件或文件夹）、ID564（删除对象，成功删除一个文件或文件夹）。

**4、日志清除。**事件 ID517 表示安全事件日志被清楚。在没有合理原因将旧文件存储到一个新文件之前，安全日志几乎是不会被清楚的，一旦有该时间发生，很有可能表明使用者或入侵者在故意掩盖痕迹。

（本文首发于 2018 年 12 月 19 日）

# 反舞弊调查之不寻常的系统安装时间

电子数据取证作为一种重要的案件查办手段，已经得到了普遍的共识，在我们接洽的大量案件中，委托人也表现出对于电子数据足够的重视。然而，进入调查实务阶段后，我们发现，由于各种原因造成的电子数据损毁、缺失等现象非常普遍，这其中有制度建设不全、设备管理混乱等基础工作方面的原因，也有证据保护和信息保密意识不强等人为方面的原因。

2017 年年底，我所接办一起大型国有企业员工涉嫌职务侵占和受贿案件，在与委托人初步沟通了解案情后，律师要求委托人提供涉案人员曾使用的计算机作进一步的电子取证。委托人企业内部调查负责人随即下达指令给 IT 部门，要求该部门收集涉案员工使用的工作电脑和移动存储设备。

我所在收到委托人提供的涉案电脑后立即开展电子数据取证，并在电脑硬盘中发现只安装有一个“纯净”的操作系统，没有任何其他软件安装、文件编辑、邮件收发等日常工作必须的操作痕迹和其他有价值的信息。为此，取证人员进一步对操作系统和硬盘残留数据作了针对性地分析，在系统日志中果然发现了不寻常的信息——**操作系统安装日期**。

为什么说这个系统安装日期不寻常呢？因为我们的电子数据取证始终是和案情紧密相连的，当发现硬盘出乎意料的“干净”时，取证人员立即敏锐的察觉到，正常使用的电脑根本不可能如此“纯洁”，于是便重点查看了系统安装时间的日志记录，将日志时间与关联人现实活动时间比对，由此发现：系统安装时间就是在 IT 部门接到收集电脑的指令后的当天夜晚至次日凌晨。通过系统安装时间点的分析可以看出，涉案人员是在接到上交电脑的通知后进行的硬盘格式化、操作系统重装等相关操作，其目的很明显是为了毁灭证据，逃避调查。

在该案中，虽然原始数据遭到破坏，取证人员只能通过数据恢复手段，有限地提取到部分数据碎片，极大影响了证据收集和案件侦办工作的顺利开展。但是，通过对这个“不寻常”的系统安装时间的分析，办案人员开展了倒查，最终发现该时间段内进行系统重装的正是企业 IT 部门的负责人，而该涉案人员原先并未被列入调查视线。

企业内部调查人员不注意涉案信息保密，处理涉案电子设备随意性大，因而给涉案员工逃避检查提供了可乘之机，这在我们反舞弊实践中是最频繁遇到的问题，最常见的做法是在电脑、移动存储设备不在控制视线的情况下，直接与涉案人员进行谈话，告知调查事项，要求其主动上交电子设备，这样做往往会使涉案人员从不知情到高度警惕，促使其抓紧一切时机毁灭证据，包括：删除电子数据、格式化硬盘、重装操作系统、以空白硬盘替换原始硬盘，甚至借口“电脑丢失”，以赔偿损失的方式避重就轻。

建议在案件调查初期，由于涉案线索和人员存在着极大的不确定性，企业内部调查人员必须保持高度的警惕，主动加强保密工作，尽量缩小知情范围，如需收集涉案人员计算机和电子设备，可以采取“秘密调查”、“突击检查”的方式，避免让涉案人员有充分的时机删除数据、毁灭证据。此外，还可以利用 IT 部门的权限，以“修补操作系统安全漏洞”、“病毒查杀”等借口，集中收取部门或企业所有员工的电脑和电子设备，是涉案员工放松警惕，避免打草惊蛇。

（本文首发于 2018 年 9 月 27 日）

# 反舞弊调查之 USB 设备连接中的奥秘

USB（通用串行总线，英文 Universal Serial Bus）是连接计算机系统与外部设备的一种串口总线标准，也是一种输入输出接口的技术规范，从 1996 年面市以来，已从 1.0 版（传输速度从 1.5Mb/s）发展到 USB 3.1（理论速度 10Gb/s），传输速率提升了 5000 多倍。

USB 被广泛地应用于个人电脑、移动设备、摄影器材、数字电视（机顶盒）、游戏机等各个领域，比如日常使用的手机、U 盘、移动硬盘、照相机，使用的都是 USB 接口，毫不夸张地说，USB 已和我们的生活、工作密不可分。

USB 作为计算机与其他存储设备连接不可或缺的外部接口，在电子数据取证工作中有着相当重要的作用，分析利用保存在计算机中的 USB 设备连接记录，也是电子数据取证中重要手段。

## 一、USB 设备连接记录哪些信息

计算机会自动记录 USB 接口设备的连接信息，这些信息主要存在于注册表和系统目录下相关的日志文件中，当 USB 设备与计算机断开连接后，这些连接信息会依然存在。

在电子数据取证分析中，USB 设备连接记录是被作为重要证据来对待的，记录中包含了 USB 的设备类型、厂商代码、产品代码、序列号、连接和断开时间等信息。

USB（Universal Serial BUS 通用串行总线）协议规定，所有的 USB 设备都有 VID（Vendor ID 供应商识别码）和 PID（Product ID 产品识别码）。VID 由供应商向 USB-IF（Implementers Forum 应用者论坛）申请，每个供应商的 VID 是唯一的；PID 由供应商自行决定。主机通过 VID 和 PID 来识别不同设备，根据它们（以及设备的版本号），可以给设备加载或安装相应的驱动程序。VID 和 PID 的长度都是两个字节，常见的各大供应商的 VID 和 PID，可以通过 http://www.linux-usb.org/usb.ids 查询。

USB 还定义了种类代码信息，它被用来识别设备功能，以便根据这些功能加载驱动，这些信息包含在基类、子类和协议 3 个字节里。设备里两个地方可以存放种类代码信息，一个是设备描述符，另一个是接口描述符。

## 二、USB 设备连接信息有什么用

电子数据取证分析从本质上讲，可以看作是传统刑事侦查手段的延伸和拓展，它同样遵循刑事侦查的基本原则，目的是通过电子数据所留下的痕迹，查找涉案线索，还原犯罪现场，固定犯罪证据，认定侵害结果。

USB 设备连接信息就是行为人使用多种外接设备的一种痕迹，它向鉴证人员提供了鼠标、键盘、打印机、手机、移动存储介质、网银身份认证设备、企业法人一证通等信息。这些信息往往需要与具体案情结合起来综合分析，相关设备的 VID、PID 和序列号等信息也可以和其他涉案电子设备进行比对，从中还原行为人在某个时间的行为轨迹，为完善证据链提供重要的信息。

【案例一】

在星瀚反舞弊中心曾经调查的一起侵犯商业秘密案件中，涉案人员利用工作便利获取了公司文件服务器高级权限后，通过公司内部网络连接服务器，下载大量设计图纸文件，随后复制到移动硬盘，并删除原始文件。案发后，电子数据取证人员对涉案电脑进行了数据恢复，锁定了涉案图纸文件，并提取了涉案电脑上操作日志和 USB 移动硬盘连接的设备序列号和连接时间，通过综合比对分析，清晰还原了涉案人员行为轨迹，完善了证据链，使案件得以顺利突破。

【案例二】

在另一起职务侵占案件中，涉案人员通过设立“白手套”公司，签订虚假合同，非法转移公司资金。案发后，涉案人员辩称，该“白手套”公司系正常经营，双方合作系正常业务往来，案件陷入僵局。电子数据取证人员提取了涉案电脑上的 USB 设备连接记录，重点筛选出设备类型为“网银 U 盾”、“企业法人一证通”的 USB 设备，通过与委托人公司相关设备进行比对，发现了多个非本公司的网银 U 盾和法人一证通设备，经与外围调查反馈信息比对，确认为涉案“白手套”公司所有，从而印证了该涉案人员同时实际控制多家公司，相关合同、转账均系其一人操作的行为，为顺利突破案件起到了关键性的作用。

**三、需要重点关注的几类 USB 设备**

**（一）移动存储介质**（U 盘、移动硬盘）：最常见的 USB 接口设备，是日常办公、转移和保存电子文件的主要载体，较多出现在涉嫌侵犯著作权、知识产权案件中。

**（二）手机**：容易被忽视的 USB 设备。手机常被视为移动通信工具和掌上信息处理终端，而在实际应用中，很多用户仍有使用 USB 线连接手机和电脑进行数据传输、文件备份的习惯，由连接信息分析，往往可以得到曾经连接电脑的手机部分信息，为进一步调查案情提供线索。

**（三）网银 U 盾**：容易被忽视的 USB 设备。网上银行转账是一种常规的资金转移手段，目前大部分网上银行的登录、确认交易等操作均需要使用“U 盾”（不同银行的验证设备可能为不同名称，但基本功能一致）来验证身份，虽然通过 USB 连接记录无法直接获取网银账号和交易信息，但可以从 VID、PID 得知银行名称，而设备序列号的唯一性也常应用于案件调查，帮助我们锁定证据物品，完善证据链。

**（四）企业法人一证通**：容易被忽视的 USB 设备。对于企业用户来说，“法人一证通”是登录工商、税务等主要办事网站、系统的“身份证”和“钥匙”，如税务系统软件 ETAX 和个税申报系统，需要插入“法人一证通”，输入密码，才可以正常访问使用，是企业日常财税工作必不可少的工具。在调查企业财务人员舞弊行为的过程中，“法人一证通”在电脑上的使用痕迹，可以在某种程度上印证涉案人员诸如超越财务权限、直接控制“白手套”公司等舞弊行为，也可以为询问涉案人员提供直接或间接的证据支撑，增强威慑力。

（本文首发于 2018 年 9 月 13 日）

# 反舞弊调查之文件的时间属性

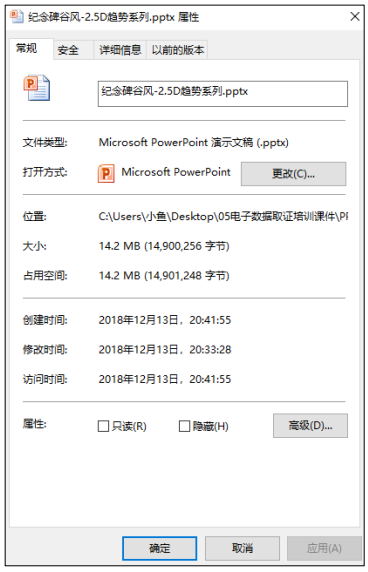
对于取证人员来说，时间点永远是一个敏感的字眼，各类取证软件在功能设计时总是要把“时间轴梳理”纳入其中，也正是因为它的重要性。

| | |
|---|---|
| 创建时间: | 2018年12月3日，15:55:35 |
| 修改时间: | 2018年12月3日，15:55:36 |
| 访问时间: | 2018年12月13日，20:19:45 |

在 windows 系统中给，通过右键点击文件，在菜单中选取“属性”命令可以打开文件的属性对话框，我们可以直接看到文件的基本属性，其中就有文件的创建时间、修改时间和访问时间这 3 个时间属性。

NFTS 文件系统除了上述 3 种时间属性外，还有隐藏的文件内容修改时间属性，这个属性需要通过特别的软件进行读取，它反映了包括文件内容、权限等所有变动的时间记录。

文件的创建时间反映的是这个文件来到当前目录下的时间，但这个时间并不一定是文件初次创建的时间，因为文件创建时间也可能是通过复制的方式来到当前目录的时间。通过复制而来的文件，创建时间是晚于修改时间的；而修改时间代表了这个文件在其他目录下最后修改的时间点，创建时间则记录下该文件被复制到当前目录的时间点。




当然，只要文件创建后对内容有过修改，那么修改时间一定是晚于创建时间的，这种情况下，就不能单一地通过时间属性来判断文件是否为本地生成的了。

虽然时间属性是每个文件都有的基本属性，但在实际的调查办案过程中，优秀的取证人员往往会有意识的结合案情，收集、梳理、排序行为人现实行为、文件创建/修改/访问、邮件发送/接收等这些关键信息的时间点，并与其它各种数据痕迹(比如前几期提到的文档元数据中的文档创建者、修改者、最后一次打印时间、GPS 信息，还有 USB 接口使用记录信息等)进行比对、归纳和分析，查找案情关联性，从而帮助发现重要线索，还原事实真相。

（本文首发于 2019 年 1 月 17 日）

# 反舞弊调查之 OFFICE 文档和图片元数据

很多企业调查人员在进行舞弊调查时，会着重查看涉案人员的各类 OFFICE 文档，如合同文档、票据、资金流水等，这类文档中往往找到的都是较直接的证据。但随着舞弊员工的警惕性和技术手段的提高，有时查遍 OFFICE 文档也难以发现有用信息。

其实很多人忽略了 OFFICE 文档的“元数据”。什么是元数据？它包含了哪些有用的信息？在舞弊案件调查时是如何具体应用的。本文将结合我们办过的案例进行介绍。

## 一、什么是元数据？

元数据（Metadata），又称中介数据、中继数据，它是关于数据的组织、数据域及其关系的信息，即被定义为描述数据的数据（data about data）。

1995 年 3 月，OCLC（Online Computer library Center，联机计算机图书馆中心）和 NCSA（National Center for Supercomputing Applications，美国国家超级计算应用中心）联合在美国俄亥俄州的都柏林镇召开了第一届元数据研讨会，会上产生了一个精简的元数据集——都柏林核心元素集（Dublin Core Element Set），简称 DC。其目的是，如何用一个简单的元数据记录来描述种类繁多的电子信息，使非图书馆专业人员也能了解和使用这种著录格式，达到有效地描述和检索网上资源的目的。

在此之后，元数据随着技术和应用的发展，根据使用场景的变化而衍生出了许多不同的定义，如有关数据的数据（data about data）、有关信息对象之结构的信息（structured information about an information object）、描述资源属性的数据 (Data describes attributes of resources)等。

## 二、元数据和用户数据的关系

我们编辑一个文档，制作一张图片，剪辑一段视频，甚至对数据库进行操作时，能够直接看到的文字、图片、影像、数据值等，都是数据的本体。

但当我们操作那些看得见的数据时，文件系统还会同步产生一些无法直接看到、与数据本体关联的数据，比如文件系统中文件检索表、路径和地址信息等，这些数据就是文档、图片、视频的元数据。比如：从网上下载的电影，其播放的内容本身是视频文件数据，而通过右键查看到的存储路径、码率、文件尺寸、艺术家、专辑名、版权方等属性信息就是视频文件的元数据。

## 三、OFFICE 文档元数据的应用

在我们对职务犯罪的调查中，OFFICE 文档是最为重要的对象，可以说，只要是办公，几乎都会用到 OFFICE 软件（为便于同 OFFICE 用户兼容，金山 WPS 同样使用 OFFICE 文档格式）。

职务侵占类案件调查中，受到重视的往往是文档内容本身，诸如合同、票据、资金流水等，这些数据可以清楚印证涉案行为，是对涉案人员行为最直接的证明。

但对于优秀的取证人员来说，仅重视文档内容是不够的，因为 OFFICE 文档的元数据中同样包含了大量有用的信息，对于扩展案件调查范围，排查可疑线索，甚至突破案件调查瓶

颈有着不可忽略的重要作用。

OFFICE 文档的元数据主要包含：Title（标题）、Word 软件版本、Creator（文档创建者）、LastModifiedBy（最后修改者）、文档创建时间、最后一次保存时间、最后一次打印时间等（如下图所示）。

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <cp:coreProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:dcmitype="http://purl.org/dc/dcmitype/" x
  xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-p
    <dc:title/>
    <dc:subject/>
    <dc:creator>汪银平</dc:creator>
    <cp:keywords/>
    <dc:description/>
    <cp:lastModifiedBy>汪银平</cp:lastModifiedBy>
    <cp:revision>1</cp:revision>
    <dcterms:created xsi:type="dcterms:W3CDTF">2017-11-13T02:41:00Z</dcterms:created>
    <dcterms:modified xsi:type="dcterms:W3CDTF">2017-11-13T10:01:00Z</dcterms:modified>
</cp:coreProperties>
```

【案例应用】

在一起职务侵占案件中，委托人提供了涉案员工工作邮箱的所有备份邮件，通过检索发现了多个可疑邮件和附件中的 OFFICE 文档，我们通过对文档正文内容中的落款名称和元数据中“文档创建者”、“最后一次修订者”进行比对，同时将邮件发送时间、文档落款时间和文档元数据中“创建时间”、“修订时间”进行比对。仔细比对后发现，文档元数据中显示的文档创建者为一台未纳入调查视线的计算机，通过后续调整方向对该计算机进行调查，我们从中发现大量涉案电子数据，从而成功深挖出隐藏的涉案人员，并全面突破整个案件。

同样，在侵犯知识产权类案件中，将文档内容比对和文档元数据比对相结合，从而印证文档原始来源，也是常见的一种调查手段。

## 四、图片元数据的应用

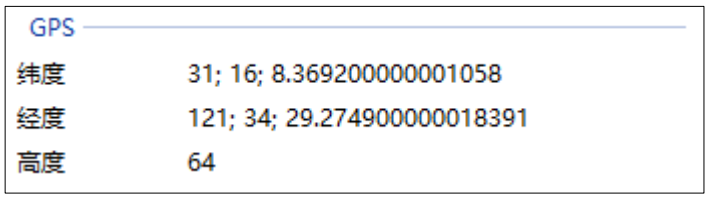
图片是另一种常见的电子数据取证对象，图片的元数据叫做 EXIF，记录了数字图像的属性信息。

EXIF 常常包括相机参数、拍摄参数、拍摄时间、GPS 经纬度信息等重要信息。从反舞弊实务的角度来看，单独的这些信息并不能够成为舞弊行为的直接证明，而如果结合案情，这些信息就变得非常重要。

照相机

| | |
|---|---|
| 照相机制造商 | HUAWEI |
| 照相机型号 | Che1-CL10 |
| 光圈值 | f/2 |
| 曝光时间 | 1/120 秒 |
| ISO 速度 | ISO-100 |
| 曝光补偿 | |
| 焦距 | 4 毫米 |
| 最大光圈 | |
| 测光模式 | |
| 目标距离 | |
| 闪光灯模式 | 无闪光，强制 |
| 闪光灯能量 | |
| 35mm 焦距 | 27 |

（注：EXIF 中的拍摄参数信息）




（注：EXIF 中的 GPS 信息）

【案例应用】

在星瀚所调查的一起公司高管侵占公司利益案件中，从举报人反映的线索中，我们获知该名高管与某外省市的关联人员频繁接触，并曾多次赶赴位北方某市的项目现场直接参与项目的进程。我方的调查目的是需要证明其到过该市项目现场的行为和时间，但限于尚未立案，甚至连其是否曾坐过高铁、飞机的记录都无法调取，因此需要调查人员能够从其使用的笔记本电脑中找到相关线索。

循着这个方向，星瀚电子取证团队对该高管的电脑进行了针对性调查，恢复了部分已被删除的图片，经确认为手机拍摄的照片备份，通过对照片本身内容和 EXIF 中包含的拍摄设备、拍摄时间以及 GPS 定位信息的分析，最终固定了该高管前往该市项目现场与关联人的接触行为和具体时间。

随后，以该时间点为焦点，缩小了外围调查和电子数据取证范围，通过深挖进一步获取了重要涉案线索和证据信息，最终使涉案人员在大量的证据面前放弃抵抗，如实供述了案情，圆满地完成了案件调查。

（本文首发于 2018 年 12 月 26 日）

# 反舞弊调查之哈希（HASH）简介和取证应用

## 一、哈希是什么?

“哈希”是一个音译词，源于英文的 hash, 其本义“切碎并搅拌”，英语里有一种食物就叫 Hash，也就是把食材切碎搅拌做成的。

计算机科学中的哈希一般指 hash 函数，也经常称作“散列”。哈希值在电子数据取证领域常用作校验数据的完整性,它的地位相当于法医的 DNA 检验、笔迹鉴定的书写动力定型、指纹鉴定的细节特征组合。

哈希并不神秘，它的实质其实就是一个算法。

在数学中，算法可以很简单，比如 b+1=a，把 b 看作是一个输入，a 看作是一个输出，经过 b+1 的运算，得到 a 这个结果，我们输入 2，经过 2+1 运算，得到 3。

就是这么简单！

哈希算法从原理上来讲和 b+1 是一样的，只不过其运算相对复杂而已。它的输入可以是字符串、数据或者任何文件，任意长度的信息经过哈希运算后，输出一个固定长度的值，这个值就是哈希值。哈希运算是一种压缩映射，在哈希计算器中无论输入什么样的数据，最后得到的结果都是一个固定长度的数字/字母混合的随机数列。

哈希运算有两个特点：

1、只要原始信息更改哪怕一个字节，哈希计算的结果都会完全不同，要找到同一哈希值的两个不同源数据，在计算上来说是基本不可能的。

2、在哈希函数中，不同的输入有可能会得到相同的哈希值，因此不可能通过哈希值来逆向确定唯一的输入值。通俗的讲就是，哈希算法不能从结果推算出输入。

## 二、哈希的分类

哈希算法有很多种,常见的如 32 位十六进制的 MD5、64 位十六进制数的 SHA-256 等，一般将这些哈希算法分为普通哈希和加密哈希两个大类。

从本质上来讲，它们并没有什么不同，加密哈希跟普通哈希的区别只是安全性。例如：MD5 算法设计初衷是做加密哈希的，但由于计算机的发展，MD5 出现碰撞的概率变大，所以就只能被当普通哈希用来做数据校验。SHA-1 曾经是加密哈希算法,从 2017 年开始,SHA-1 算法生成的加密证书也被各大浏览器拒绝。目前流行的加密算法是 SHA-2，跟 SHA-1 不同，SHA-2 不是一种算法，而是一系列算法的统称，其中就包括上面说过的 SHA-256。

原则上，只要一种哈希算法出现过碰撞，就不会被推荐当作加密哈希，只有安全度高的哈希算法才能用作加密哈希。虽然哈希算法的安全性不单跟哈希数列长度有关，但大致上还是可以按照输出哈希的长度来区分，一般来说长度越长的算法被认为越安全，安全度低的被认为是普通哈希算法，主要用来做完整性校验；安全度高的被称为加密哈希算法，被用在加密算法中。

不同的哈希算法的应用场景不同，由于越安全的哈希算法处理速度就越慢，所以并不是所有的场合都适合用加密哈希来替代普通哈希。

几种常见的哈希算法：

**1、MD5**

MD5 消息摘要算法（MD5 Message-Digest Algorithm）是一种被广泛使用的密码散列函数，可以产生一个 128 位（16 字节）的哈希值，用于确保信息传输完整一致。它由美国密码学家罗纳德·李维斯特（Ronald Linn Rivest）设计，于 1992 年公开。

**2、SHA-1**

SHA 全称叫作安全哈希算法（Secure Hash Algorithm），主要适用于数字签名标准（Digital Signature Standard DSS）里定义的数字签名算法（Digital Signature Algorithm DSA）。对于长度小于 264 位的消息，SHA-1 会产生一个 160 位的消息摘要。当接收到消息的时候，这个消息摘要可以用来验证数据的完整性。在传输的过程中，数据很可能会发生变化，那么这时候就会产生不同的消息摘要。 SHA-1 有如下特性：不可以从消息摘要中复原信息；两个不同的消息不会产生同样的消息摘要,(但会有 1×1048 分之一的机率出现相同的消息摘要,一般使用时忽略)。

**3、SHA-256**

SHA-256 是 SHA-2 下细分出的一种算法，名称来自于安全散列算法 2（Secure Hash Algorithm 2）的缩写，是一种密码散列函数算法标准，由美国国家安全局研发，属于 SHA 算法之一，是 SHA-1 的后继者。SHA-2 下又可再分为六个不同的算法标准，包括了：SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256。这些变体除了生成摘要的长度、循环运行的次数等一些微小差异外，算法的基本结构是一致的。对于任意长度的消息，SHA-256 都会产生一个 256 位长的哈希值，称作消息摘要，这个摘要相当于是个长度为 32 个字节的数组，通常用一个长度为 64 的十六进制字符串来表示。

## 三、哈希的应用

哈希有很多不同的称呼，有时候叫 Digest（摘要），有时候叫 Checksum（校验值），有时候叫 Fingerprint（指纹），其实说的意思差不多，也就是说哈希是可以用来代表数据本身的。

因为数据在存储或者传输过程中如果有丝毫改动，它的哈希就会改变，由于这个独一无二的特性，哈希函数最常见作用就是进行数据完整性校验（Integrity Check），即数据无损校验。

### （一）文件校验

常见的校验算法有奇偶校验和 CRC 校验，这两种校验在一定程度上能检测并纠正数据传输中的信道误码，却不能防止对数据的恶意破坏，没有抗数据篡改能力。

MD5 算法的“数字指纹”特性，使之成为目前应用最广泛的文件完整性校验算法，常被用在下面的 2 种情况下：

**1、文件传输校验**

将传输后的文件与源文件的 md5 哈希值进行比对，确保一致性，就可以从统计上保证

两个文件是完全相同的。一般用以检验文件在传输过程中是否出现错误，保证文件在传输过程中未被恶意篡改。很多下载工具软件中，也是利用 MD5 的特性，在用户多次断点续传后，仍能保证下载文件的正确性。

还有一种更为先进的解决方法，就是所谓的代码签名。文件接受者不仅能验证文件的完整性，还可以依据自己对证书签发者和证书拥有者的信任程度，决定是否接受文件。浏览器在下载运行插件和 java 小程序时，使用的就是这样的模式。

比方说我们从服务器下载一个软件，如果这个软件被黑客更改了，那么我们下载的就不是原来的软件，如果是银行客户端可能就会有账户被盗的风险。有了哈希运算后，可以把下载的软件经过哈希运算得到哈希值，然后把哈希值跟软件发行方公布的哈希值对比，就能知道软件是否有被篡改了。

**2、保存二进制文件系统数字指纹**

不少系统管理和安全软件都提供文件系统完整性评估的功能，在系统初始安装完毕后，建立对文件系统的基础校验和数据库，因为散列校验和的长度很小，它们可以方便的被存放在容量很小的存储介质上。以后还可以定期或根据需要，再次计算文件系统的校验值，一旦发现与原来保存的值有不匹配，就说明该文件已经被非法修改，或者是被病毒感染，或者被木马程序替代。

**（二）数字签名**

Hash 算法是现代密码体系中一个重要组成部分,由于非对称算法的运算速度较慢，所以在数字签名协议中，单向散列函数扮演了重要的角色。在这种签名协议中，双方必须事先协商好双方都支持的 Hash 函数和签名算法。

签名方先对该数据文件进行哈希值计算，然后再对很短的哈希值用非对称算法进行数字签名操作。对方在验证签名时，也是先对该数据文件进行计算其哈希值，然后再用非对称算法验证数字签名。对 Hash 值进行数字签名在统计上可以认为与对文件本身进行数字签名是等效的。首先，数据文件本身可以同它的哈希值分开保存，签名验证也可以脱离数据文件本身的存在而进行。其次，有些情况下签名密钥可能与解密密钥是同一个，也就是说，如果对一个数据文件签名，与对其进行非对称的解密操作是相同的操作，这是相当危险的，恶意的破坏者可能将一个试图骗你将其解密的文件，充当一个要求你签名的文件发送给你。因此，在对任何数据文件进行数字签名时，只有对其 Hash 值进行签名才是安全的。

**（三）鉴权协议**

有个称为“挑战-认证模式”的鉴权协议：需要鉴权的一方，向将被鉴权的一方发送随机串（“挑战”），被鉴权方将该随机串和自己的鉴权口令字一起进行 Hash 运算后，返还鉴权方，鉴权方将收到的 Hash 值与在己端用该随机串和对方的鉴权口令字进行 Hash 运算的结果相比较（“认证”），如相同，则可在统计上认为对方拥有该口令字，即通过鉴权。

**（四）网站注册**

在用户注册提交用户名密码时，用户名被直接保存到网站的数据库中，但密码却并不直接保存，而是把密码转换成哈希，再把哈希值保存到网站数据库中。因此，即使是网站管理

人员，也拿不到用户的密码，万一公司数据库泄露，用户密码依然安全。

当用户自己登录网站输入密码提交到服务器时，服务器也进行相同的哈希运算，由于输入数据没变，所以哈希也不变，登录成功。

**（五）区块链和加密货币**

在比特币系统中主要使用了两个密码学 Hash 函数，分别是 SHA-256 和 RIPEMD160。

以 SHA-256 为例，它是构造区块链所用的主要密码哈希函数。无论是区块的头部信息还是交易数据，都使用这个哈希函数去计算相关数据的哈希值，以保证数据的完整性。同时，在比特币系统中，基于寻找给定前缀的 SHA256 哈希值，设计了工作量证明的共识机制；SHA256 也被用于构造比特币地址，即用来识别不同的用户。

在比特币系统中，SHA-256 算法的一个主要用途是完成 PoW（工作量证明）计算。而区块链就可以看作一类使用哈希指针的链表，这个链表链接一系列的区块，每个区块包含数据以及指向表中前一个区块的指针。区块链中，前一个区块指针由哈希指针所替换，因此每个区块不仅仅告诉前一个区块的位置，也提供一个哈希值去验证这个区块所包含的数据是否发生改变。

利用区块链构造一个防篡改的日志系统，在这个系统中，基于区块链的日志节点链表被用来存储数据，链表节点通过哈希指针链接，新节点追加在日志链表的尾部。同时，日志链表的头哈希指针所指向的头节点内容不可改变。若日志链表中的某个节点的数据被篡改，则系统能够检测出来。

因此，若攻击者想在日志链表中的任意位置改变数据，为保持一致性，他必须向表头方向修改所有的哈希指针，最终由于不能改变链表头部而失败。因此，只需单个哈希指针，基本上就能保证整个链表的哈希值的一致性，从而达到防篡改的目的。

（本文首发于 2019 年 3 月 14 日）

# 反舞弊调查之隐藏在文件背后的蛛丝马迹

摘要：在常规电子数据取证中，一般都较为重视文档、图片的检索、恢复，因为这些内容往往直接包含了犯罪的线索和证据。但在文件的背后，计算机还同时包含了大量的日志、元数据、缩略图等用户使用的电子痕迹，这些隐含的痕迹记录了用户行为轨迹，是案件调查取证的重要内容。

## 一、电子痕迹是什么？

刑事侦查学中的刑事科学技术包含三个基本原理：

- 物质交换和信息转移原理
- 同一认定原理
- 种类认定原理

其中的“物质交换和信息转移原理”认为，物质经过交换和转移，但物质成分和结构等特征一般不会发生变化，仍能客观真实的反映其原所在客体的本质。

这个原理在传统的刑事犯罪现场调查中应用最多的就是现场痕迹取证，而最为典型的就是“指纹”。人的手上会分泌汗液，接触到物体后就会留下痕迹，也就是“指纹”，由于人类指纹的唯一性，通过指纹就能反向锁定相应的人，从而为确定案件侦破提供线索和证据。

电子设备在使用中也会留下痕迹，比如：日志、元数据、缩略图等。用户在使用电子设备时，并不会以此类信息作为直接访问对象，而是由操作系统自动按一定的数据格式进行记录，这些被系统同步记录下来的信息就是所谓的“电子痕迹”。

相较于传统的现场物证痕迹，电子痕迹同样是反映用户行为，锁定用户个体的重要线索和证据，它与用户活动息息相关，而且更加完整、全面和详细。对电子痕迹的取证，是电子数据取证中不可获取的一个重要内容。

## 二、电子痕迹的来源

电子数据主要是通过两种方式产生。

（一）使用者主动生成，比如：创建文档、收发邮件、拍摄图片、下载文件等，这些电子数据的产生遵循了用户的使用习惯，与其日常工作、生活相关。

（二）系统自动生成，比如：浏览器历史记录，文件系统日志等，这些数据是操作系统和应用系统按照规则和格式自动记录的信息，并且随着使用过程不断发生改变，用户在设备使用过程中往往不会察觉，一般也无法主动控制相关进程。

值得注意的是，在办案实践中，我们也多次发现涉案人员主动对系统自动产生的电子痕迹进行清理、删除和修改，希望借此毁灭证据、逃避调查，却不知系统仍有其他的方式记录这类操作行为，所谓“触物必留痕”，通过对电子痕迹的调查，反而给描摹用户行为轨迹、还原案件真相提供了线索和证据。

## 三、容易被忽略的几类电子痕迹

用户使用电子设备的日常行为，在系统中会产生大量电子痕迹，进行电子数据调查不应

忽视这些信息。较为常见的电子痕迹有：系统日志、应用程序日志、临时文件、元数据、快捷方式、缩略图、网络连接等。

**（一）系统和应用程序日志**

系统日志和程序日志是反映用户操作行为轨迹最直接有效的证据，可以说就是一个“行为记录表”。传统刑事犯罪现场的指纹、脚印、血迹都要人工提取、分析，其中还可能出现疏漏、错误，时间也需要进行倒推判断。而电子痕迹则是非常忠实的记录用户的行为，尤其是能够准确记录行为时间，用好日志信息，对于精确还原用户行为，有着至关重要的作用。

系统日志是一门完整的学问，要讲透的话，恐怕写一本书可不为过，这里仅作一个极其简要的介绍，不展开讨论。

在办案实践中有个利用日志信息结合外围排查的真实案例：某高新技术企业的一个技术人员，通过偷窥系统管理员的账号密码，违规访问公司核心知识产权信息库，下载大量技术文档，以百度网盘为中间媒介，转移到个人在家中的计算机，试图寻求卖家牟利。案件调查中，取证人员通过百度网盘的日志信息数据库文件，结合系统文件访问的日志信息和办公场所监控录像，完整地将其作案过程进行了还原。

浏览器日志也同样能够发挥巨大作用，在轰动一时的杭州保姆莫焕晶纵火案和复旦投毒案中，公安机关也是通过提取嫌疑人手机、电脑的浏览器历史记录，发现了印证作案动机重要证据，有力证明了犯罪嫌疑人蓄谋犯罪的主观故意，有效辩驳辩方提出的临时起意、冲动作案的辩护意见。

**（二）元数据**

系统在存储文件本身的同时，还会生成一些隐性的、与文件数据相关的数据，如文件系统中文件检索表、路径信息、地址信息等，这些信息就是元数据（Metadata），在英文名称中又叫做“数据的数据”，它隐含在文档、图片等文件中，用来描述这个文件的结构、资源和其他辅助信息。

比如，我们用手机拍摄一张照片，其本身显示出来的是我们拍摄的对象，而在图像属性中还包含了拍摄时间、拍摄设备、镜头型号、光圈、快门等辅助信息，这些辅助信息就是照片的元数据，而图片的元数据还有一个特别的名字——EXIF （Exchangeable image file 可交换图形文件）。如果在手机设置中开启了定位功能，元数据中还会记录拍摄点的 GPS 信息。

在调查一起建筑企业员工职务侵占案件的过程中，取证人员就是通过对涉案人员存留在电脑中的照片元数据分析，获取照片拍摄的时间、GPS 信息，确定涉案人员在案发时间前往位于某外省工地的证据，有力地反驳了涉案人员编造的谎言，突破其心理防线。

再比如，电子数据取证中经常用到 Office 文件的元数据，虽然元数据本身不包含用户主动输入的数据，但却记录了包括：标题、版本、创建者、修改者、创建时间、修改时间、访问时间、最近一次保存时间、最近一次打印时间等大量重要信息，在案件调查中为文件来源分析提供重要依据和扩大侦查的线索。

**（三）临时文件**

应用程序使用过程中，为了防止突发性宕机等非常规事件，会设定某种保护机制来对数据进行实时备份。

我们日常使用的很多软件都有“撤销”和“恢复”功能，尤其在 office、PS 等软件中更为常用，这种功能就是通过临时文件来完成的。当用户进行某项改动或操作时，应用软件将操作

步骤和数据改动保存在一个自动生成的临时文件中，如果用户认为这种改动不符合预期，需要“撤销”，应用程序就会从临时文件中把之前保存过的原始内容提取出来，有效地保障了用户数据的安全性。

临时文件在系统中，根据作用不同存留相应的时间，有些随着软件关闭自动清理删除，比如 office 软件临时文件，而有些则可能会在系统临时文件夹中存留相当长时间，甚至需要手动或借助软件人工清理，比如浏览器的页面缓存。无论存留的时间长短，临时文件都会在磁盘上留下相应的电子痕迹，这也给电子数据调查提供了对象。

在一起企业员工受贿案件中，调查人员对其使用的笔记本电脑做了常规的数据分析，却没有找到有效的信息。而在进一步对系统进行数据恢复和全局检索的过程中，却发现系统临时文件夹中存留了手机备份的临时文件，经技术处理，还原了手机银行、即时通信等软件的重要数据，为案件有效突破提供了关键性证据和线索。

**（四）快捷方式**

在 windows 系统下，快捷方式文件的扩展名为.lnk，用于指向其他文件，便于用户快速调用原始文件。

快捷方式可以由用户主动创建和系统自动创建 2 种方式生成，这里主要讲的是系统自动创建方式。

在使用者打开文件时，系统会在“user\用户名\AppData\Roaming\Microsoft\Windows\Recent\”目录下自动创建一个链接文件，显示在用户界面中即为“最近使用项目”。

在部分案件中，涉案人员习惯于将用户文档存放于外置的移动硬盘和 U 盘，当无法获取此类存储介质时，办案很容易陷入瓶颈。这种情况下，有经验的调查人员通常会进一步检查系统快捷方式文件，通过调查快捷方式包含的原始文件名称、路径、磁盘和网络等信息，同时结合 USB 设备信息和插拔记录，从侧面锁定用户打开、修改文件的行为轨迹证据，为扩展侦查和收集证据提供线索。

上述列举的电子痕迹仅仅是相对较为典型的几种类型，在实际应用中，电子痕迹的内容远大于这个范围，本文仅以一点浅薄的介绍做个普及，希望能够抛砖引玉，为大家拓展调查思路提供一点帮助。

（本文首发于 2019 年 7 月 24 日）

# 企业数据安全保护的基本原则

员工利用工作之便，擅自复制、传送、甚至故意删除破坏企业重要资料和文件，利用企业商业机密谋取个人私利，而给企业带来巨大风险和损失，是当下很多企业面临的突出现实问题。保障重要数据信息安全，防止员工泄密，已经成为企业管理的一项重要工作。（注：本文所指“企业数据”指的是以电子数据形式存储的各类企业信息，不含其他传统的纸质文件等数据信息存储形式。）

## 一、企业数据泄露的危害

近 20 年来，电子信息产业爆炸式发展，互联网应用已经普及到社会生活的方方面面，大多数企业的日常经营活动都通过计算机和网络进行，各类重要文件也基本都是以电子数据的形式保存，常见的如计算机源代码、客户和订单信息、自有知识产权的图纸和设计文稿等。

信息化、电子化办公在给工作带来极大便利和效率的同时，也使得员工非法占有、窃取企业重要文件资料更加得隐蔽和便捷。

据互联网非权威的调查数据统计显示，约八成的员工在离职前都曾带走过企业资料，这些员工中，有些是为了在下一个工作岗位上有可以参考和依据的资料；有些是为了仿制产品、软件，与原企业形成同业竞争；有些甚至直接拿到各类商业秘密资料倒手专卖，非法获利。

无论这种行为出于何种目的，都势必给企业经营带来巨大的风险，严重的机密外泄将直接导致企业重大经济损失，甚至使企业面临破产倒闭的危险。

## 二、易泄密的数据类型

### （一）技术类信息

主要是具有知识产权、著作权的软件产品、开发文档、设计图纸、视听资料等。在我所经办的一起知识产权侵权案中，某软件开发公司员工在工作期间大量复制保存公司核心软件源代码，在离职后开办公司，通过软件“外壳”包装等改头换面，利用源代码制作出一款功能完全一致的软件，与原公司形成市场竞争，严重损害原公司利益。

### （二）经营类商业秘密信息

主要指的是企业的客户资料、订单信息、推广营销渠道、合同协议文档、财务数据等。例如房产中介行业较为普遍的飞单案件，其核心就是一种典型的商业秘密外泄。还有企业销售人员掌握的客户资料，财务人员掌握的公司财务信息，都是企业生存发展的核心信息，此类信息的泄密将给企业带来经营和法律上的双重风险。

## 三、企业数据安全保护的基本原则

企业数据的重要性毋庸置疑，有些核心数据甚至是企业赖以生存的生命。但尽管如此，仍旧还是有侵犯商业秘密和知识产权的案件不断发生，企业仍然对员工飞单操作防不胜防，甚至在此类案发后依然找不到有效的证据抓手，无法将违法者绳之以法。

更有效保护企业数据的安全，防止核心数据和其他重要信息泄密，这个议题从宏观的企业文化、制度建设到微观具体的网络设置、计算机管理、用户操作权限设定，如果讲透，甚

至可以写出一本书来。尽管内容庞杂，但我们仍可以删繁就简，从中归纳出几项重要的原则，作为数据保护的指导性建议。

**原则一：以完善的企业制度作为前提**

企业要做好数据保护工作，首先应将制度建设作为前提来抓，从企业设立、发展到稳定运营整个阶段，根据企业自身实际情况，逐步地建立完善管理、人事、保密、培训、计算机和网络使用、以及企业信息化应用系统的各项管理制度和规定，要让企业员工从入职开始就明确自身的职责、权力，同时也要对违反制度规定的行为制定相应的处罚准则。

**原则二：以完备的技术手段作为辅助**

在信息化大背景下，企业商业机密等重要数据基本都是以电子文档的形式保存在计算机和服务器，在为提供便利的同时也使数据泄露渠道更加多样和隐蔽，常见的有移动介质拷贝、网盘、邮件、FTP 和即时聊天工具传送等方式。因此，必须在制度建设的同时，采取文件加密、权限设置、网络流量同步监控等多种技术手段来杜绝文件泄密的渠道，保护商业机密安全。技术手段也要辅助对各类数据提供存留，比如企业邮箱的备份，移动存储设备连接记录，外来计算机接入公司网络记录等。

**原则三：以必要的刑事个案作为威慑**

百密也有一疏，尽管在可能的情况下做好了预防工作，总难免会有人铤而走险，以身试法。因此，企业监察人员应当做好常规巡检，重视公司内部举报线索，对于涉嫌侵犯公司商业秘密、知识产权，破坏公司数据信息的刑事犯罪行为，要及时开展调查，必要时应向公安机关报案，配合做好刑事犯罪侦查、起诉，同时在结合公司内部日常管理，强化法制宣传，警示员工，对潜在违法犯罪行为形成有效威慑，预防犯罪发生。

注：企业在发现涉嫌刑事违法线索后，应在保密前提下开展先期调查，有条件的可以请专业律师配合介入，梳理已有的线索和证据，制作完整的报案材料，向具备管辖权的公安机关报案。

（本文首发于 2018 年 11 月 21 日）

# 企业数据安全保护之硬盘选择

本文对目前广泛使用闪存类存储介质的数据存储恢复机理作个简要介绍。

**Q1. 什么是固态硬盘？**

固态硬盘（Solid State Disk）——用固态电子存储芯片阵列而制成的硬盘，由控制单元和存储单元（FLASH 芯片、DRAM 芯片）组成，其在接口规范和定义、外形和尺寸、功能、使用方法上与普通硬盘都完全一致。被广泛应用于军事、车载、工控、视频监控、网络监控、网络终端、电力、医疗、航空、导航设备等诸多领域。

**Q2. 固态硬盘的优缺点（与机械硬盘相比）**

**（一）优点**

**1、读写速度快**

尤其在读写零碎文件时，固态硬盘速度要比机械硬盘快几十倍。最明显的感受就是开机时间，固态硬盘基本 10 多秒就能完成操作系统启动，进入系统后还不用等待，而大多数机械硬盘的启动时间要几分钟，并且进入系统后硬盘仍继续疯狂读取数据，要等上好一段时间才能正常使用系统。

**2、使用寿命长（这里一直有个误区）**

对于稍微了解一点固态硬盘知识的人来说，都会认为固态硬盘的写入次数是有限的，而这也的确是个事实。但实际上，固态硬盘寿命足以使用很长时间，举个形象的例子来说，一个目前最普遍使用的容量——128g 固态硬盘，就算每天高频大量进行写入操作，其使用寿命也大于十年。另外，固态硬盘寿命和容量成正比，容量翻倍寿命也翻倍，也就是说，要写死一个 256GB 的固态硬盘，你得从大学毕业用到孩子上大学！对比来看，机械硬盘则由于机械结构的精密性，震动和高温都会导致损坏，根据实际使用数据统计，普通的机械硬盘用了几年之后一般都会产生“坏道”（损坏的存储单元）。从这点上看，机械硬盘并没有固态硬盘耐用！

**3、防震抗摔**

固态硬盘使用闪存颗粒制作，内部不存在任何机械部件，即使在高速移动甚至伴随翻转倾斜的情况下也不会影响到正常使用，在发生碰撞和震荡时能够将数据丢失的可能性降到最小。

**4、低功耗、无噪音、发热小**

没有机械结构的固态硬盘，在功耗上明显低于传统硬盘，噪音值为 0 分贝，发热量小、散热快。

**（二）缺点**

**1、意外断电时容易损坏**

固态硬盘最主要的“敌人”不是日常频繁写入的操作，而是意外意外断电，这是由固态硬盘的内在构成所决定的（此处不作技术解释，了解即可），为了使固态硬盘的寿命延长，可以花一二百块钱买个小型的 UPS（不间断电源），防止电脑意外断电即可。

**2、贵！贵！贵！**

说多少遍缺点，最大的缺点仍旧是个“贵”字！当下主流的 128GB 或者 256GB 固态硬盘，价格从 300 到 800 不等，而同样价格，可以买到从 1T 到 3T 容量的机械硬盘。如果是存储电影、音乐、大量文档，选择机械硬盘还是适合的，因为放在固态硬盘里带来的读写速度也不会给我们带来明显的提升。

**Q3. 固态硬盘可以恢复数据吗？**

个人计算机从 CPU、内存到显卡近些年都呈现非常大的技术革新和性能提成，计算机整体性能的瓶颈早就卡在了硬盘上，固态硬盘的出现才改变了这个现状。

对于普通用户来说，固态硬盘带来的性能和速度提升是显而易见的，但对于电子数据恢复来说，固态硬盘则变得难以预测。

上期分享说过，传统的机械硬盘上如果数据被删除或者硬盘格式化，仍旧有非常大的概率能够把原始数据恢复出来。而对于固态硬盘，根据实测数据的不完全统计，在默认设置的情况下，90%的概率是无法恢复的。

固态硬盘数据恢复低成功率的关键，在于它和机械硬盘完全不同的结构和数据存储机理，接下来，我们就讲讲固态硬盘的存储方式。

**Q4. 固态硬盘数据存储方式**

大多数民用固态硬盘都是用“闪存”而不是磁盘来作为存储介质，根据容量不同，固态硬盘安装有不同数量的闪存模块，在新数据写入之前闪存必须进行擦除操作，这样的擦写操作是有次数限制（也就是寿命）的。

为了保证固态硬盘随时都有可以写入空间，平均各个闪存模块的擦写频率，就要用到一个名为 FTL 的动态链表来记录和维护这些操作的数据信息。

由于 FTL 链表的动态特性，就使得固态硬盘的数据存放位置和外部存取地址不能一一对应，除了固态硬盘控制器外，谁都不知道数据到底存放在硬盘的哪个闪存模块中，所以使用数据恢复软件按操作系统在写入时记录的地址，根本无法找到想要恢复的数据。

**Q5. 什么情况下固态硬盘数据可以被恢复？**

**（一）还是先说结论：**

**如果固态硬盘关闭 Trim 指令功能，数据有可能可以恢复。**

**反之，数据基本不可恢复。**

**（二）Trim 指令简介**

TRIM 指令是微软联合各大 SSD 厂商所开发的一项技术，它告诉闪存固态存储设备要擦除哪些数据,当相关页面的数据可以被覆盖时，操作系统会发给固态硬盘一个 TRIM 指令,因为在写入操作过程中不用花时间去擦除原本的数据，写入速度要快得多。

当我们在操作系统中删除一个文件时，系统并没有真正删掉这个文件的数据，它只是把这些数据占用的地址标记为“空”，即可以覆盖使用。但这只是在文件系统层面的操作，硬盘本身并不知道那些地址的数据已经无效，除非系统通知它要在这些地址写入新的数据。

闪存不允许覆盖，只能先擦除再写入，要得到空闲闪存空间进行写入，就必须进行数据

擦除。在没有 Trim 的情况下，SSD 无法事先知道那些被删除的数据页已经是无效的，必须到系统要求在相同的地方写入数据时才知道那些数据可以被擦除，这样就无法在最适当的时机做出最好的优化，既影响效率性能，又影响固态硬盘的寿命。

打开 Trim 指令可以提高固态硬盘性能，同时延长使用寿命，但数据恢复基本无法实现。而当硬盘上存有重要数据的情况下，关闭 Trim 功能则能提高数据恢复的概率，更大程度保障数据安全，也给电子数据取证提供更多的机会。

**结语：**

从数据保障和电子数据恢复的角度，建议还是将固态硬盘作为操作系统和程度的安装盘，而个人信息则还是存在机械硬盘中更为安全。

企业用户的计算机可以使用小容量固态硬盘+大容量机械硬盘的方式更为妥帖，既保证了计算机的性能和运行速度，又给数据恢复提供了可行的机会。

（本文首发于 2018 年 11 月 7 日）

# 企业数据安全保护之防范数据被恶意拷贝

在企业反舞弊实务中，员工侵犯知识产权、著作权的案例经常发生，侵犯的对象往往是以电子化方式存储的设计稿、软件源代码、客户资料、销售渠道等涉及核心内部资料的电子数据文件。

本文概述企业数据泄露的途径，并对一些防范利用计算机 USB 端口恶意拷贝文件的技术手段做简要介绍。

## 一、信息外泄的三大途径

电子数据外泄从途径上讲，归纳起来主要有 3 类：一是网络传输，比如即时通信工具点对点互传、网盘上传、邮件发送等；二是移动存储介质复制，常见的是通过 U 盘、移动硬盘等移动存储介质复制，而通过智能手机与电脑连接进行文件互传比较容易被忽等；三是屏幕拍照，虽然这种方式比较原始，但是对于一些数据量较小的机密数据的安全防范，比如外来人员顺手拍摄客户名单、销售表格等等，仍需要注意防范。

## 二、防范信息外泄的三大手段

防范企业数据外泄的手段，主要有 3 类：

一是网络软硬件综合监控布局，通过对网络传输数据的监管、限制，实时发现违规行为，并对网络使用作常规记录，为日后取证提供便利；

二是个人计算机软硬件监控设置，在员工使用的个人计算机、移动设备中安装监控软件，对 USB 端口设备的连接进行比较的设置，比如将 USB 端口设定为只有报备过的特定设备可以连接等，有条件的还可以对计算机硬件进行定制，记录日常软件使用情况，防范文件恶意拷贝行为等；

三是全面部署视频监控，在办公区域尽量不留死角，为可能发生的案件调查提供相应证据。

上述三种手段往往要综合利用，才能更好的起到防范效果，限于篇幅，本期先重点聊一聊如何控制个人计算机外设端口的数据传输。

## 三、限制计算机外设端口的三类方法

从限制个人计算机端口数据传输入手来防范企业数据外泄是一种比较直接的手段，在日常普通应用中，以限制 USB 端口使用最为常见，按方法分主要是 3 个大类：

### （一）物理封锁

物理封锁可细分成完全禁用、弹性禁用和贴标检查等。

#### 1、粘贴易碎贴纸

这种方法针对企业来访者临时使用计算机时较为常用，在计算机 USB 口和网络口上粘贴易碎贴纸，利用易碎贴纸的特性可以直观地确认来访者是否曾经通过这些接口联接外设设备。

**优点：简单粗暴，肉眼可辨**

**缺点：贴纸清理容易残留，影响美观；贴纸易碎，误触后容易引发误会**

**2、断开 USB 面板与主板连接线**

该方法仅针对台式计算机面板扩展 USB 端口，移除计算机面板 USB 口连接到主板的连接线，可以实现 USB 口的功能。

**优点：彻底的物理隔断，使 USB 口完全失效**

**缺点：仅隔断机箱前面板 USB 口，无法限制后面板连接，因此使用时需要其他物理手段配合，且重新启用 USB 口要打开机箱来连接跳线，做法上较为麻烦。**

**3、热熔胶封堵**

这是一种永久性破坏的封锁方式，常用于一些涉密等级较高的政府机关、企事业单位等

**优点：彻底封锁**

**缺点：破坏性方法，不可逆**

**4、配置专用适配卡（推荐）**

这是一类可以加装的计算机硬件，如 PCI 适配卡，或者 USB 控制器，其功能是通过硬件方式设定、限制计算机权限，比如限制 USB 外设连接功能。

**优点：可以通过密码控制，不影响正常操作，切换便捷**

**缺点：需要具有高管理权限的 IT 人员配合切换功能**

**5、硬件锁**

用来锁住电脑接口，课根据使用需求而取下，恢复接口功能。

**优点：不改动破坏硬件，上锁、开锁便捷**

**缺点：管理弹性较差**

**（二）修改操作系统设定**

**1、设置 BIOS**

在主板的 BIOS 设定里，我们可以将 USB 设为禁用。设定容易，做法简单，成为企业管理 USB 设备的常用手段。为了防止员工自行进入 BIOS 重新启用 USB 功能，一般在完成设定之后，需要同时设定 BIOS 管理密码，只有相关获得授权的人员才能访问、更改 BIOS 设定。如果对主板进行放电操作，BIOS 密码会恢复成默认值，而员工就能趁机进入 BIOS 更改设定。不过，对企业来说，一般都不允许员工私自拆装公司所配发的电脑，而只要非 IT 部门的人员，在进行类似的动作时，就很容易引起其他人的注意。在机密数据外泄事件发生后，此人自然会成为公司重点排查的可疑对象。

**优点：设定容易，做法简单**

**缺点：BIOS 管理密码破解较为容易，需要同时在机箱粘贴封条**

**2、删除 USB 设备驱动程序**

适用于未曾连接过任何 USB 储存设备的电脑。在 WINDOWS\inf 路径下，可以找到 usbstor.inf、usbstor.PNF 两个安装信息文档，这是 Windows 系统用来辨识 USB 储存设备的驱动程序。针对这两个文件设置存取权限、修改文件名称，或者直接删除，可以使员工无法在自己电脑上使用 USB 储存设备。相同的做法，也能用于打印机、网络摄像头等 USB 设备的管理。

**优点：可针对不同 USB 设备个别控制**

**缺点：仅能针对先前未曾连接 USB 储存设备的电脑**

**3、修改 Windows 注册表项**

工作中经常用到 U 盘，又不能完全禁止 U 盘的使用，所以该方法可以禁止电脑文件到 U 盘的复制而不影响其他外设的连接，方法是在注册表的——“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\USBSTOR”下找到 Start 项，将数值由预设的 3 修改为 4，即可实现禁止文件复制的功能。

**优点：设置简单**

**缺点：对于了解计算机设置的员工，作用有限**

**（三）外设控制整体解决方案**

企业对于 USB 的管理需求往往不只是单纯的开与关，而是希望根据实际需求来决定要开放什么样的功能，在此种情况下，就需要导入外部设备控制产品来实现。

这类产品通常会通过安装在用户电脑上的代理程序实施管理，而且能够整合 Windows AD、LDAP 等目录服务，让同一部门、相同群组的电脑套用相同的规则做管理，省去个别调整设置的麻烦。

除了设置开关之外，这类产品对于外设的插口，可以提供相当精细的管理功能，对于 USB 储存设备，可以设置成只读属性，只能阅览移动存储设备里的数据，但不可以执行写入操作，对于智能型手机，这类员工工作上经常使用到的设备，通过这类型的产品，可以只允许电脑与手机之间交换通讯簿，与行事历，但不能将电脑里的数据复制到手机上的记忆卡里。

企业可以在员工将数据写入 USB 储存设备的时，同步备份到指定储存空间，供日后稽查检查之用。

为了避免数据储存量的问题，也可以只记录文档传输动作，比如何时传送了什么样的文件作为日志进行记录，但这样做的话，对于员工以编辑修改方式外泄机密数据，无法有效地加以管理。

除了市面上的产品之外，网络上也有许多免费版本的 USB 控制软件，比如 USB Blocker，不过，也要注意某些工具有可能是广告软件或间谍软件。和付费相比，这一类控制产品的功能比较少见，采用与否，需视企业实际需求与部署规模而定。

**优点：可根据需求开放一部分的功能，具备良好的管理弹性**

**缺点：无法防止员工以编辑修改的方式将机密数据外流**

（本文首发于 2018 年 12 月 5 日）

# 企业数据安全保护之中小企业电子邮箱数据安全

自互联网兴起以来，电子邮件在社会生产、经济往来、商务办公领域的地位至今无法撼动，尤其在大型企业、跨国公司的日常工作中，电子邮件是最核心最主要的通信工具，其数据安全对企业至关重要。

也正因为电子邮件的核心地位，其在企业内控和反舞弊调查中的作用不可或缺。通过多年反舞弊调查工作的实践，我们针对企业电子邮箱管理中存在的一些共性问题做了专题调研，在此与大家做个简要的分享。

## 一、不同规模企业电子邮箱使用现状

（一）大型跨国企业在业务中使用电子邮箱使用较为普遍，基本为自建服务器和邮件系统，或使用 exchange 等企业邮箱服务，客户端功能丰富，可应对大部分业务工作需求。有些企业基本将电子邮件作为唯一的往来通讯手段，所有内部业务和对外往来均以电子邮件为准。

（二）国内大型企业基本配备电子邮件系统，自建服务器或租用阿里、腾讯、网易等商用邮件系统，员工日常工作中会使用电子邮箱收发较为正式或重要的信息，而使用 QQ、微信等即时通信工具作为日常通讯的比例较高。

（三）国内中小企业鉴于成本和管理问题，基本以腾讯企业邮箱（含免费版）和网易企业邮箱（含免费版）为员工开设企业电子邮箱，而大部分中小企业员工仅以企业电子邮箱为工作的一个附属工具，在实际工作中主要以微信、QQ 等即时聊天工具为业务往来的主要方式。

## 二、反舞弊调查中电子邮箱现状

在反舞弊调查中，我们发现不同企业对于电子邮件的重视程度差别极大，而在案件调查过程中，电子邮箱系统不同管理方式和策略的结果也显而易见。

【实例 1】某日本大型跨国企业，自建立企业电子邮箱系统起，就在服务器端设定对员工往来邮件进行实时增量备份，十几年来的所有邮件均得以保留，以便作为工作追溯的依据。在某年员工舞弊案发后，这些备份的邮件作为案件调查的重要线索和证据，极大的拓宽了调查的广度，为深度锁定犯罪行为起到了关键性作用。

【实例 2】某国内制药企业，使用腾讯企业邮箱作为员工电子邮件系统，管理员在后台的工作基本就是开设和删除员工邮箱、重置密码等简单操作，并未对邮件做任何形式备份。某年，一名员工被他人举报舞弊，公司随即开展调查，但此时并未对其使用的电脑和电子邮箱采取任何措施。在调查尚未公开之际，涉案员工闻风主动离职，先一步删除了企业邮箱中所有往来邮件，并将公司配发的工作电脑格式化删除信息，以致调查陷入僵局，结果可想而知。

凡事预则立，不预则废——上述两个实例充分证明了未雨绸缪的重要性，要想维护自身利益，就必须事前做好充足的准备，防患未然。星瀚律师事务所反舞弊中心今年改为内控和反舞弊中心，多了“内控”二字，就是看到了预防在企业反舞弊工作中的重要性和前瞻性，才将“内控”提到了甚至是高于案件调查的高度。

## 三、国内主流电子邮件系统管控初探

对内控我们不做展开，仍旧回到电子邮件的主题。

认识到电子邮件管理的重要性，接下来就要说说如何做好电子邮件管理。对于有自建服务器和邮件系统需要的，一般均为大型企业，且都有主流的系统集成供应商提供设备、软件和服务，备份、日志等基本功能均能满足需求，不作赘述。

以下针对很多中小企业常用的腾讯和网易两大邮件系统做了些粗浅的调研，与大家分享交流（不是广告）。

### （一）腾讯企业邮箱

通过腾讯企业邮箱帮助中心查询了解到：付费版邮箱的**“邮件归档”**和**“邮件备份”**两种功能可以实现备份，免费版无法实现。

**1、邮件备份**

- 备份功能从设置生效后才备份，之前的邮件不会进行备份；
- 可根据“关键字”和“成员邮箱账号”两种方式进行备份设置，备份规则总计上限 20 条；
- 备份邮箱邮件有排重规则，可以保证邮件不出现重复。比如：同一封邮件有多个收件人，并且这些收件人都是要备份到某个目标备份邮箱的，那么目标备份邮箱只会备份一封邮件，系统对相同邮件会进行排重，不会重复。
- 用于存放备份邮件的邮箱需要大小足够容纳，建议及时使用客户端工具将邮件收取到本地，否则如果来信过多，邮箱满后，将无法接受备份邮件。

**2、邮件归档功能**

可以设置归档帐号,永久保存企业邮箱往来邮件

**3、收费标准：750 元/5 账户/年，按人数递增。**


### （二）网易企业邮箱

通过网易企业邮箱帮助中心查询了解到：付费版邮箱**“邮件备份”**和**“萨班斯归档”**功能可以实现邮件备份功能。

**1、邮件备份**

- 可对重要邮箱的邮件信息进行自主备份，所有被备份邮箱的收发邮件均会同时发至主备份邮箱进行备份。
- 设置生效后的邮件才会备份，设置时间点之前的邮件不会进行备份。
- 如果来信过多，可能导致备份邮箱满。建议及时使用客户端工具将邮件收取到本地。

**2、萨班斯归档**

萨班斯归档的本质是按照美国政府出台的一部涉及会计职业监管、公司治理、证券市场监管等方面的重要法律《萨班斯法案》要求进行邮件归档的功能。

网易萨班斯归档功能可以对某些重要邮箱的**往来邮件实时记录和存储**，并且**保证归档邮件长久保存、不被篡改，归档后的邮件直接满足《萨班斯法案》对邮件存档的审计要求，可以成为法律证据。**

萨班斯归档服务需要企业进行购买，收费方式按照购买归档功能邮箱数量计。

企业还需提供已签署的《萨班斯归档服务购买协议》、《关于指定、变更萨班斯归档服务验证码接收手机号码的申请书》和一个复核的手机号码（一般为企业最高领导或法务人员），每次进入归档系统，都须验证发往复核人手机的短信验证码。

**3、收费标准：1500 元/5 用户/年，随人数递增。**

**产品主要参数及报价**

| 邮箱容量 | 普通附件 | 云附件 | 个人网盘 | 企业网盘 | 移动办公平台 |
|---|---|---|---|---|---|
| 无限容量 | 100M | 16G | 5G | 50G | 马上办 |

我想购买 5 个用户

标准价：1500元/年； 优惠价：1000元/年

**四、给中小企业的建议**

对比腾讯和网易两大企业邮箱，异同点有：

1、均可对指定的目标邮箱地址进行邮件同步备份，备份内容从设置生效。

2、用于备份的邮箱空间需足够大，且日常管理中需及时导出到本地保存，以免邮箱容量达到上限无法接受新邮件。

3、从公开宣传资料看，腾讯邮箱对备份规则和目标邮箱均有所限制，而网易邮箱并未提及。

4、备份和归档等功能均为付费版所有，免费版不具备此类功能。

5、网易邮箱独具萨班斯归档功能，对有审计、司法证据要求的企业而言，不失为一种具备性价比的选择。

腾讯和网易两大企业邮箱都有免费版，对于人数较少、邮件应用不多的企业，的确是一

个控制成本的好选择。

而中、大型企业，如业务工作和电子邮件较为紧密，可选择使用收费版企业邮箱，并对重点岗位或人员开设长期的备份归档机制，由公司内控部门做日常监控管理。

至于大型企业，由于人数的增加，商用收费版企业邮箱由于按用户数按年收费，性价比已然降低，笔者建议还是自建邮件服务的性价比更高，定制功能更贴近企业需求，日常管理也相对更具私密性和可控性。

（本文首发于 2019 年 12 月 19 日）

# 四条建议让企业远离电子取证中的“神操作”

互联网时代，企业员工的沟通交互、签呈流转、合作对接、成果展现等与工作有关的方方面面基本都于电脑端或手机端呈现，当企业发觉员工有舞弊行为的端倪时，也会有意识地希望通过“控制”员工的电脑或手机、进而“获取”有价值的线索、甚至是证据。

但是，企业的“控制”、“取证”行为稍有不慎，便可能产生极其严重的后果，导致证据毁损或丧失法律效力。

如何避免企业自查过程中的“神操作”应当是各家企业高度重视的问题。本文就将为大家提供四条建议。

## 完善企业内部制度

优秀的企业内控合规制度是开展电子取证的有力保障，其至少应当明确约定企业员工办公所用设备的所有权，并通过在制度文件上签字、开展培训课程等方式明确告知员工，企业对自有电子设备的调查权、监控权和知情权等；当然，企业在设计相关规范时应当遵守个人信息收集相关的法律规定。

不仅如此，相关制度也需要规定，如有员工被列入调查对象，调查人员应当遵循的操作流程以及与各部门配合时的注意事项。

我们曾经遇到过的案例情况有，某公司 IT 部门在预备调查一名员工的电脑前，先行予以口头告知，但并未及时将涉案人员的行为和设备纳入视线，从而为员工留下了充分的时间和空间毁灭证据。甚至是在口头告知的两天后，IT 部门才真正收回员工使用的电脑，此时，该电脑已被多次格式化，原始数据无法恢复。

制度的意义并不在于其白纸黑字的形式，而在于所载的内容能保护企业的权益、解决企业所面临的问题。我们建议企业投入时间和精力在制度建设上，让企业能够真正掌握主动权。

## 提高企业相关人员的证据意识

目前，企业对内控反舞弊的重视程度越来越高，不乏企业设置监察部、内审部以应对员工犯罪问题；但是，由于相关专业领域的建设尚在起步发展阶段，更多的企业依然选择以合规、法务、风控、或者人事岗位的人员负责相关事宜。无论是专职、专业的人员，还是兼职、新入行的人员，处在与企业内控、反舞弊有关的岗位上，证据意识无疑是相当重要的。

可以给大家说几个因为证据意识薄弱而引发的“惨案”。比如，有企业在发现员工舞弊行为后，没有使用专业的设备固定证据，而是自行安装了民间开发的免费版取证软件，导致原始数据完全损坏。又比如，有企业就涉案员工的邮件处理方式仅仅是转发后保存，随后便直接删除了涉案员工的原始邮箱账号……这类行为会对追究涉案员工的责任造成极大困难。

企业还应树立起电子数据的“原始态”意识，做好数据记录。原始数据一旦被更改，就难以恢复到“原始态”。在缺乏专业人员的现场，尽量不要对涉案设备擅自进行操作。

## 设立预案制定机制

除了日常制度的设立、内控反舞弊岗位人员的证据意识提高外，企业还有必要设立电子

数据取证的预案机制，即企业在启动调查前务必咨询专业取证人员，三思而后行，针对法律上的风险、技术上的可行性制定出周全的方案后再进行取证。

电子取证并不单纯是对电子数据做镜像如此简单。

首先，就电子取证的调查对象来看，涉案电子介质和数据不仅包含电脑和手机，还可以包括：行车记录仪、电子手表、移动硬盘等，甚至一些智能电器也可以成为电子数据的载体。

其次，就电子取证的调查内容——线索与证据而言，企业应当知道，相比于线索，法律对于证据做出了更为严格的规定。刑事证据的获取、对象和操作流程都必须由具备资质的第三方机构来完成。

此外，企业需要意识到，电子取证的调查作用包括了为案件调查提供线索和为司法流程提供证据。线索虽然无法达到证据的法定性和证明力，但线索却可以为案件办理提供重要的、甚至是关键性的指引。因此，企业需要设立预案机制，审慎地处理线索、严谨地开展电子取证，才能使线索的效用最大化。

**取证力争维持“现场性”**

所谓对取证的过程维持“现场性”，就是指，要尽量在电子数据处于开机状态时进行获取，必要的时候，可以考虑联系电子取证鉴定机构或取证人员执行相关工作。

电子取证工作离不开系统的规划、细致的落实。我们也遇到过专业素养、思想意识颇高的企业因为一点小小的错误而功亏一篑的情况，更是令人痛心。

比如，有企业将涉案员工的笔记本电脑送检并完成数据镜像固定后，就以为取证流程完全结束了，没有做好原始数据的保管工作，而是将电脑交由其他员工使用，导致原始数据灭失；此时，即便已经发现了重要线索甚至公安机关已经立案，也无力回天了。

还有企业尽管斥巨资搭建了邮件服务器，但日常监控和备份工作却没能有效开展，导致邮件信息的留存发生问题，案件处理难度颇高。

希望企业在后续开展电子取证工作时，能够不再出现本文若干案例所述的情形。一方面，在日常管理中设计完善合规内控制度，捍卫企业对自有电子设备与电子数据的所有权；另一方面，在调查取证时，尽可能地避免在无专门机构或专业人员在场的情况下自行操作，要有证据意识和预案规划，从而全面保障企业的健康发展。

（本文首发于 2020 年 6 月 22 日）

021-5109 6488-110

上海市长宁区长宁路1193号长宁来福士T3座7楼

BD@ricc.com.cn

星瀚客服小星

星瀚微法苑