敏感电子数据痕迹保密擦除技术

严小飞 黄志炜

（厦门市美亚柏科信息安全研究所有限公司 福建 厦门 361000）

[摘 要] 本文从电子数据保密机制的反方向电子数据取证原理出发，分析了会产生敏感电子数据的终端操作、以及非取证专业人士所不知道的电子数据失泄密的风险，最后有针对性地给出解决方案和策略。

[关键词] 电子数据；敏感电子数据痕迹；保密擦除；数据恢复

0 引言

伴随着无纸化办公与电子政务的产生与发展，计算机与手机等数据终端在人们的工作与生活中成为了不可缺少的必要工具。越来越多的具有社会属性或相关性的电子数据不断地被从无到有产生出来，被集中或离散地存储在网络服务器、计算机、手机的存储介质中。所生成的电子数据中不乏涉及国家机密敏感、企业商业机密敏感、个人隐私敏感。这些电子数据所携带的信息在安全知悉范围之外传播必将带来灾难性的后果。因此，如何保证这些敏感的电子数据被安全地使用、有效防护与严密处理，是所有单位、机构、企业、个人都必须谨慎面对的问题。

1 敏感电子数据痕迹分类与关联的泄密推演

1.1已删除或格式化后的文件数据残留痕迹

计算机/手机终端在使用过程中不可避免要生成、更新、或删除文件。绝大多数没有电子数据特性相关知识经验的普通用户会理所当然地认为：文件删除或格式化存储后，文件数据就销毁了。事实并不是这样，那些被删除的或被格式化存储处理过后文件会被完整地保留在存储介质里，普通用户使用通常方式无法直接使用，但只要使用一些特殊的工具软件就可以恢复出来。出于抢救数据目的的恢复不存在问题，如果带着不良目的地恢复这些文件，就直接意味着敏感文件内容的泄密了。下图就是一个实验文件删除并经过格式化后从存储介质上直接分析读取出来的的完整内容。（示例：如图1所示 左边是存储介质偏移，中间是计算机数据视图，右边是文本解释视图）。

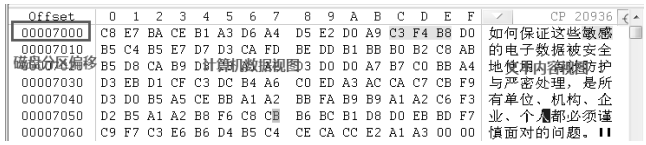


图1 被删除或格式化后残留在存储介质上的文件内容痕迹

文件是数据的载体，数据的涉密性质与隐私性质决定了作为载体的文件的涉密性质与隐私性质。文件数据是信息量最大的、最丰富、最易传播扩散、关联涉密或隐私最直接的数据。例如：涉密文件、商业计划、工程图纸、视频、图片等等。文件数据的保护是涉密保护或隐私保护的核心，目前有多种多样的保护方法，例如：文件加密、加密容器、硬件加密芯片等。同样文件数据痕迹的处理也是电子数据痕迹处理的最重要一环。电子数据各种终端的使用者数据保护意识强弱各有不同，电子数据安全专业素质高低也各不相同。所以很需要一种方法可以自动地帮助专业与意识良莠不齐的用户安全地使用数据。

1.2系统使用历史痕迹

系统使用历史痕迹包括：应用程序运行痕迹、shell命令记录（Unix/linux/MAC OS/Window/Android）、文档文件打开历史记录、系统搜索记录、打印历史记灵、远程桌面记录、开关机时间等等。这些都是计算机/手机等终端操作系统平台上用户的使用痕迹。根据这些痕迹可以推理失泄密事主职业、工作内容、作习时间、工作方式、思维方式、文档存储。如果对Linux的shell命令进行深入的分析还有可能可以得到网站拓朴、服务器架构、数据库结构、技术框架体系、必要配置文件分布等重要信息。（示例：如图2与图 3所示）

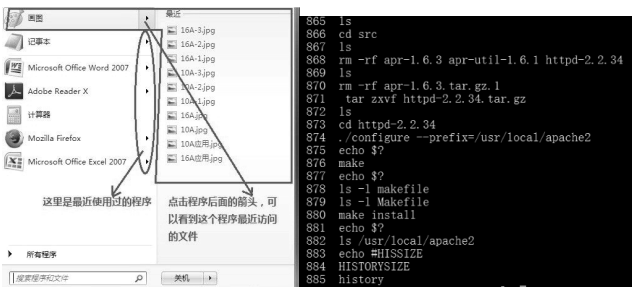


图2 windows应用与文档痕迹图3inux shell命令历史

1.3硬件设备使用历史痕迹

硬件设备使用历史痕迹包括：蓝牙设备接入记录、USB接口U盘/硬盘设备接入记录、Wifi与热点联接记录、路由器设备接入记录、开关机时间、通话记录等等。（示例：如图4与图 5所示）

通过对硬件设备使用历史痕迹的分析，可以推演出失泄密事主的工作生活地理轨迹、电话社交圈子、数据存储习惯与目标对像。

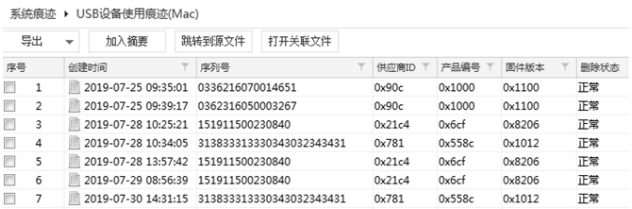


图4 从实验MacBoor Pro笔记本分析得到的USB设备使用痕迹

图5 从实验MacBoor Pro笔记本分析得到的Wifi设备接入痕迹

1.4邮件痕迹、即时通信聊天信息、上网痕迹、账户与密码

随着计算机技术的发展和普及、以及在其基础上形成的计算机网络的飞速发展，“电子化生存”的风暴席卷了社会生活的各个领域。[1]另外随着移动通信技术所提供服务水平和服务种类的不断提高和扩充，手机已日益成为人们工作生活中不可或缺的联系工具。[2]逐渐地，在互联网上检索资料替代了图书馆查阅，电子邮件替代了普通信件，即时通讯替代了传统电话，移动支付替代传统支付…，每一项技术替代的背后都有一个新的电子数据组织方式产生。每次新计算机/手机应用被使用都意味着大量的数据被临时或永久地制造出来并被存储在存储介质中，这些数据在业务生命周期结束后通常不会被自动处理，或用户有意要保留。有意或无意的保留下来的数据形成了有可能被恶意滥用的电子数据痕迹。

失泄密情况比较严重的是邮件痕迹、即时通信聊天信息、上网痕迹、账户与密码。（如图6、7）

图6 从实验计算机中分析出的邮件数据

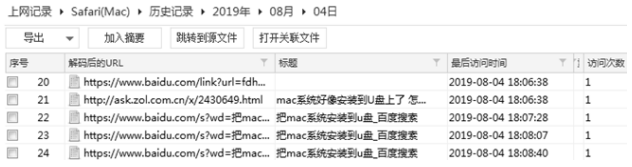


图7 从实验计算机中分析出的上网记录数据

2 敏感电子数据痕迹擦除技术

上文所述的各种敏感电子数据痕迹：文件相关操作残留痕迹、系统使用历史痕迹、硬件设备使用历史痕迹、邮件痕迹、即时通信聊天信息、上网痕迹、账户与密码等等。因为各种电子数据痕迹产生的驱动需求不同、处理时的终端宿主使用状态不同，所以针对性的敏感痕迹擦除技术也有很大的区别。根据实验与实践结果，我们把有效的敏感电子数据痕迹擦除技术分两类：在线系统处理与离线存储处理。在线系统处理是指：数据痕迹的宿主终端仍会被运行使用，仅擦除目标敏感电子数据痕迹。离线存储处理是指：出于保密要求，对存储介质中的所有数据进行无差别擦除。

●在线系统处理

1.基于驱动层监控的即时文件痕迹保密擦除

2.应用层处理的系统与APP计时周期痕迹保密擦除

●离线存储处理

1.基于离线存储介质的保密擦除

2.1基于驱动层监控的即时文件痕迹保密擦除

Windows操作系统：以NTFS文件系统为例，卷中每一个文件都至少包有一个文件记录。文件记录由文件头和一系列属性列表组成，每一个属性完成一个单独的工作，不同的属性的结合体构成了不同种类的文件记录（如图8）。

图8 windows文件记录结构示意图

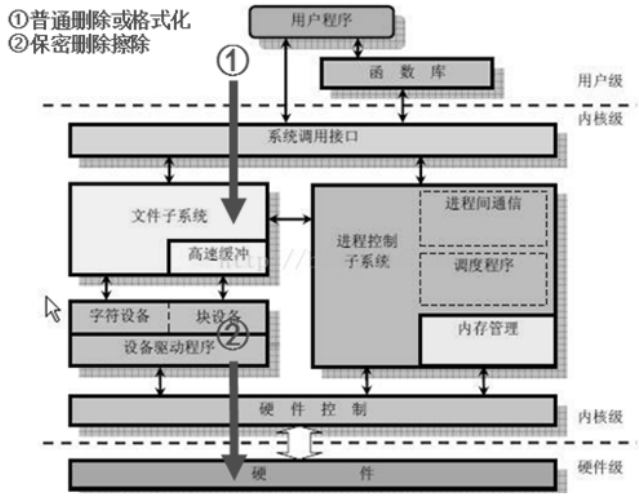
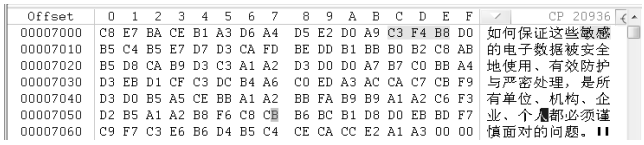


图9 驱动层监控回调保密擦除示意图

Unix/Linux/MacOS操作系统：每个文件都有以下这三层结构：dentry、inode和data。dentry含有文件名并关联inode，innode含有文件元数据并指向数据区（data）[3]。

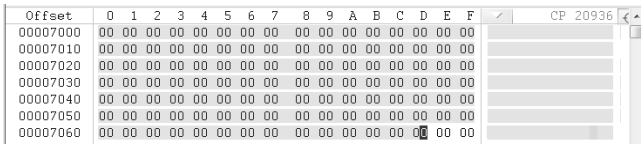
实验结果发现Windows、Unix、Linux、Mac OS等系统在完成删除文件或格式化磁盘操作时，实质都是把目标文件关联的文件记录或属性节点（inode）从操作系统的文件系统中清除，存储内容的数据在被其它数据覆盖之前并没有任何变化。

通过实践，我们发现在操作系的内核层中的驱动层增加特殊驱动程序进行监控。当监控发现文件删除或格式化等系统动作时，可以用回调处理的方式实现对存储介质上文件真实数据的进行数据覆盖写入完成即时保密擦除。（如图9）。保密擦除前后数据对比（如图10、11）。



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	CP 20936
00007000	C8	E7	BA	CE	B1	A3	D6	A4	D5	E2	D0	A9	C3	F4	B8	D0	如何保证这些敏感
00007010	B5	C4	B5	E7	D7	D3	CA	FD	BE	DD	B1	BB	B0	B2	C8	AB	的电子数据被安全
00007020	B5	D8	CA	B9	D3	C3	A1	A2	D3	D0	D0	A7	B7	C0	BB	A4	地使用、有效防护
00007030	D3	EB	D1	CF	C3	DC	B4	A6	C0	ED	A3	AC	CA	C7	CB	F9	与严密处理，是所
00007040	D3	D0	B5	A5	CE	BB	A1	A2	BB	FA	B9	B9	A1	A2	C6	F3	有单位、机构、企
00007050	D2	B5	A1	A2	B8	F6	C8	CB	B6	BC	B1	D8	D0	EB	BD	F7	业、个人都必须谨
00007060	C9	F7	C3	E6	B6	D4	B5	C4	CE	CA	CC	E2	A1	A3	00	00	慎面对的问题。

图10 保密擦除前的数据



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	CP 20936
00007000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00007010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00007020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00007030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00007040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00007050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00007060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

图11 保密擦除后的数据

2.2系统与APP用户痕迹定时周期保密擦除

在操作系统与应用APP方面，因为厂商的不同、不同时期版本不同等多方面原因，在线系统与应用APP的用户痕迹保密擦除遵循不同系统与应用使用不同方法的原则进行处理。在线系统因为一直在使用，所以系统与APP用户痕迹的保密擦除需要自动定时周期性进行。通常的步骤是：

1）找出该系统或应用的用户痕迹的记录方式（注册表、文件、数据库…）。

2）删除对应记录、初始化文件、清空数据记录。

2.3离线存储介质的保密擦除

对于离线存储介质的保密擦除，已有多个很成熟的标准可以参考。如：

●BMB21-2007 国家保密局标准：第一次使用0x00擦除，第二次使用0xFF擦除，第三、四、五次随机字符（0x00-0xFF）擦除指定扇区内的每一个字节，第六次使用0x00擦除。

●DoD5220.22-M 美国国防部标准：按DoD 5220.22要求第一次为某个字符擦除，第二次擦除为第一次使用字符的补码，第三次对指定扇区范围内的每个字节使用随机字符擦除。

●快速擦除标准：对磁介质存储器的最大数据存储扇区范围使用0x00擦除一次。

3 结束语

计算机技术、移动通迅技术、互联网技术的发展推动社会生产与生活发生变化，方便快捷的同时，敏感电子数据失泄密的风险也是必须面对的。只有提高防范意识不断做好各种有效保密措施才能避免事故的发生。

参考文献

[1]高云飞 王永全电子数据勘查取证与鉴定（电子证据保全）P1.

[2]孙奕 杨璞电子数据勘查取证与鉴定（手机取证技术）P1.

[3]红帽软件（北京）有限公司 Red Hat Linux用户基础

（下转第92页）

提高小学语文阅读教学有效性的研究策略

董华兰

（江西省抚州市临川区嵩湖乡中心小学 江西 抚州 344125）

[摘 要] 随着时代的不断发展，科技的不断进步，教育的不断改革，人们越来越重视学生的语文课程，特别是小学语文阅读能力，我们都知道，良好的开端是成功的一半，小学语文阅读教学对学生未来的语文学习以及以后的发展有非常重要的影响。

[关键词] 小学语文；阅读教学；方法探讨

在小学语文教学中，阅读教学占着举足轻重的地位。它不仅是小学语文教学的核心内容，更为重要的是它是使得学生语文素养得到有效培养的重要途径，由此可见，能否科学合理的实施小学语文教学在促使学生得到全面发展上发挥着极其重要的作用，特别是在这样一个打基础的启蒙阶段，让学生对阅读产生浓厚的学习兴趣，以及让学生体验和感受到阅读的趣味性，对学生未来的发展以及以后的学习有着非常重要的影响，同时也能使得学生的综合能力以及学生的文学素养得到有效培养。本文就小学语文教学中如何有效开展阅读教学的探讨。

一、阅读兴趣的培养是关键

提高阅读教学效果首先应该激发学生的阅读兴趣。这是培养学生阅读习惯、阅读技巧的一个最基础的环节，只有这样才能够更好地去培养小学生拥有一个良好的阅读习惯，养成一个高效的阅读方法。这是培养学生阅读能力的基础，同时也是能够让学生爱上阅读的一个方法。教师可以通过各种方法去鼓励学生进行阅读，鼓励学生在阅读的过程当中去发现更多的有趣的有价值的事物，这样学生就能够从阅读的过程当中去感受更多不同的东西，感受到阅读带给我们的喜悦和快乐，这样才能够让阅读发挥在语文教学和学习当中的作用，让阅读教学变得更加有效率，更加高效。

二、提高阅读教学效率是根本

在开展阅读教学的时候应该注重提高课堂阅读教学的效率，这样才能够更好地开展阅读教学。在课堂上，教师应该充分地引导学生能够自主地进行阅读，这样才能够让学生在语文阅读当中养成更加积极主动的学习习惯。其次，教师还应该引导学生拥有一个正确的阅读习惯，掌握必要的阅读技巧，这样才能够更加有效率地提高阅读教学，提高阅读教学的核心在于掌握阅读教学的精髓。让小学的语文教学能够更好地引导学生的思想教育成长和进步。阅读教学的教学效率提高在于坚持阅读习惯的养成。在阅读的过程当中，学生会在这阅读过程当中学习到更多的有用的知识，同时在这个过程当中也能够学会掌握更多的学习方法，积累更多的词汇，提高自身的语文水平，这才是阅读教学的目标和任务。

三、科学的方法激发学生自主阅读兴趣

教师应该引导学生养成一个独立自主的阅读习惯，用科学的方法去教学生进行阅读，引导学生有一个技巧性的方法在阅读的过程当中，这样能够让学生在独立自主的过程当中学习到更多的知识核心思想，阅读兴趣对于学生来说也是十分重要的，阅读兴趣会给学生提供更多的阅读和学习的动力，这样才能够让学生掌握更多的和阅读相关的能力和技巧，让学生在阅读当中提升自我，提高自己的語文知识能力和素质，让学生能够在阅读过程当中更好地提高自己的综合能力素质，培养学生的语文核心素养。另外，科学的阅读方法应该高效率地帮助学生进行阅读，能够缩短学生的阅读时间，节省学生的时间，能够更好地引导学生进行高效率的阅读，能够让学生在阅读当中提高自己的学习能力，这对于小学生的语文学习来说尤为重要。

四、注重培养学生养成一个良好的阅读习惯

一个良好的阅读习惯是决定小学生的阅读能力和阅读效率的关键核心，因为阅读能力的高低和学生平时的阅读学习的状态有关，如果学生能够高效率地进行阅读，那么学生就会提高自己的阅读能力，阅读习惯的养成对于学生学习语文来说也是十分重要的，因为语文的学习过程其实就是一个慢慢积累的过程，一个循序渐进的过程，只有在一点一滴的积累过程当中，才能够得到提高，才能够让小学生的语文水平得到提升，对于阅读教学来说也是同样重要的，阅读习惯对于学生的阅读能力也是一步步地得到提高的，因为阅读的过程，其实就是一种学习积累的过程，在这个过程当中，能够学习到更多的知识，能够通过自己的学习获取更多的信息，能够通过阅读体会作者的思想感情，学习作者的文字表达方式，这样也能够加强小学生的写作能力。

结束语

综上所述，阅读教学与学生质疑精神的重建、知识储备量的增加、演说形式的推进密不可分的，不能单一或花样解读，更不能进行“灌输式”的强制教育，压制学生的兴趣。教师要以促进学生的自我理解力为己任，注重培养学生的质疑能力，引领他们走进书的世界，畅游其中，最终提升自我修养。

参考文献

[1]林梅珠.浅谈如何有效开展小学语文的阅读教学[J].考试周刊，2018，（A2）：53.

[2]杨洪顺.如何在语文教学中有效开展课外阅读[J].考试周刊，2018，（A3）：52.

[3]王苏霞.浅谈小学语文教学中的有效阅读教学[J].学周刊，2018，（32）：129-130

（上接第90页）

P136.

作者简介:

严小飞（1978年5月）男，汉，福建莆田人，研究生，厦门市美亚柏科信息安全研究所有限公司，研究方向：计算机电子数据证据固定、取证分析

黄志炜（1980年8月）男，汉，福建莆田人，研究生，高级工程师，厦门市美亚柏科信息安全研究所有限公司，研究方向：电子数据证据固定、取证分析