计 算 机 取 证

（Computer Forensics）

信息安全现状

我国从首例计算机犯罪(１９８６年利用计算机贪污案)被发现至今，涉及计算机网络的犯罪无论从犯罪类型还是发案率来看都在逐年大幅度上升。而国外有的犯罪学家也曾预言，“未来信息化社会犯罪的形式将主要是计算机网络犯罪”。

2000-2004年
计算机犯罪趋势图

应急响应&计算机司法鉴定

当发生计算机违法犯罪的时候我们就需要进行应急响应或是计算机司法鉴定

什么是应急响应？

答：应急响应是指对发生在网络或者计算机上任何未经授权的、非法的、或无法接受的行为采取的措施。

什么是计算机司法鉴定？

答：计算机司法鉴定是指从计算及媒介中发掘证据来支持某项法律诉讼。（计算机取证）

计算机取证的定义

- 计算机取证（Computer Forensics）是指运用计算机辨析技术，对计算机犯罪行为进行分析以确认罪犯及计算机证据，并据此提起诉讼。也就是针对计算机入侵与犯罪，进行证据获取、保存、分析和出示。计算机证据指在计算机系统运行过程中产生的以其记录的内容来证明案件事实的电磁记录物。从技术上而言，计算机取证是一个对受侵计算机系统进行扫描和破解，以对入侵事件进行重建的过程。可理解为“从计算机上提取证据”即： 获取、保存 分析 出示 提供的证据必须可信。计算机取证(Computer Forensics)在打击计算机和网络犯罪中作用十分关键，它的目的是要将犯罪者留在计算机中的“痕迹”作为有效的诉讼证据提供给法庭，以便将犯罪嫌疑人绳之以法。因此，计算机取证是计算机领域和法学领域的一门交叉科学，被用来解决大量的计算机犯罪和事故，包括网络入侵、盗用知识产权和网络欺骗等。

计算机取证的发展

一、与电子证据相关的硬件产品发展速度减慢

美 国、英国，是开展电子证据研究最早的国家，国际目前广泛应用的计算机法证硬件产品约有80%产自美国、英国。2003-2006年间，是国际电子证据相关 硬件产品发展最为鼎盛的时期，各种硬盘复制机速度从1.8GB到3GB不断攀升，写保护接口从单一的IDE硬盘接口，到SCSI、SATA、USB 种类层出不穷，PC、MAC、Linux平台下的取证设备越来越多。取证分析计算机各式各样，出现了皮箱型、工控型，服务器型等。这些产品的大量出现，对 国际计算机法证技术的发展起到了极大的推动作用

计算机取证的发展

1.硬盘复制设备：Logicube公司推出了SuperSonix，一个应有于IT界的硬盘克隆工具，速度可达6GB。这个设备对于调查行业来说可以算个福音，对法证界还无法使用。但是Logicube在民间应用之后，应该很快就推出法证版的型号了。

计算机取证的发展

2.写保护设备：ICS 公司推出了Super DriveLock写保护设备，具有全面的接口，外观设计和实际功能都很不错。特别是最新的eSATA接口可以明显提高速度。

3.2008年,DataExpert推出的硬盘修复诊断破解设备、效率源推出的DC指南针都比较有特色，对计算机取证人员所遇到的故障硬盘有很大的帮助作用。

4. 俄罗斯Elcomsoft推出的GPU解密加速产品也是对冷清的解密市场一剂强心针。北京天宇宁公司将俄罗斯Elcomsoft推荐的个人超级计算引入国 内，将密码破解水平提升到一个全新的水平。设想一下：拥有960个核心的强大的并行处理能力，计算性能可达PC的250倍。

计算机取证的发展

二、法证分析软件层出不穷

国际电子证据分析软件产品却如雨后春笋一般，涌现了很多优秀的产品。老牌法证工具的代表是Encase和FTK，这两个软件已经发展 了若干年，基本成了计算机法证的代名词。美国Guidance公司的Encase软件这两年发展劲头不错，从4.0、5.0到6.0版，差不多每年推出一 个版本。相比之下，美国AccessData公司的FTK的进展可就相对慢了许多。最近几年，国际上先 后推出了一系列的计算机法证分析工具，如德国X-ways公司的X-Ways Forensics，韩国FINALData公司推出的FINALForensics，澳大利亚的NuixForensicDestop。从欧洲、美国、 澳大利亚这些计算机法证技术的先进国家来说，这些软件的出现可以说明显推动了冷清的市场。国内用户可能很多人都知道Winhex这个数据恢复和十六进制编辑器。由于电子证据研究离不开二进制、十六进制，也离不开数据恢复，因此Winhex的作 者Stefan将这个产品进一步开发成计算机法证工具。由于其强大的数据恢复功能、灵活的数据编辑能力，快速的升级服务，X-ways Forensics立刻在世界各地受到热烈欢迎。

计算机取证的发展

三、在线取证工具成为热门话题

所谓在线取证，就是在计算机处于开机状态下的取证方法。一般这种状态下，为了 保证证据的完整性，应该尽量避免去运行额外的程序，以免使操作系统下注册表、内存、临时文件中的数据发生更改。但近年来，由于在线取证日趋重要，很多时候 无法向早年国外专家所讲的一样，拔掉计算机电源，然后实施硬盘完整镜像。一旦关机往往会失去很多重要的内存数据、加密分区数据。因此，现在很多人都在重点 研究在线取证工具。目前常见的在线取证工具，都是在嫌疑人的计算机中直接运行取证软件，并自动获取内存、注册表中的数据。同时也可以通过 取证软件，实现对硬盘的完整镜像。但此种方法缺点在于可能造成内存中、硬盘中过多的信息被覆盖，影响取证效果。通过，在运行的系统下获取镜像，将有可能造 成系统死机，破坏证据的完整性。

计算机取证的发展

- 取证的工具和过程标准化。由于计算机取证倍受关注，很多组织和机构都投入了人力对这个领域进行研究，并且已经开发出大量的取证工具。目前除TCT和En Case以外，还有很多其它的工具。因为没有统一的标准和规范，软件的使用者很难对这些工具的有效性和可靠性进行比较。另外，到现在为止，还没有任何机构对计算机取证机构和工作人员的资质进行认证，使得取证结果的权威性受到质疑。为了能让计算机取证工作进一步向纵深方向发展，制定取证工具的评价标准、取证机构和从业人员的资质审核办法，以及取证工作的操作规范是非常必要的。

电子证据

电子证据，也被称为计算机证据，是指在计算机或计算机系统运行过程中产生的以其记录的内容来证明案件事实的电磁记录物

特点：

- 表现形式多样性
- 储存介质电子性
- 准确性
- 脆弱性
- 数据的挥发性（易失性）

电子证据的特点

1.表现形式多样性

证据不仅可以是文字、图像、声音等多种方式存储，还可以是多媒体形式。

2.存储介质电子性

数据存放在电子介质上，它的产生或者重现必须依赖其他介质

电子证据的特点

3.准确性

如果没有人恶意破坏证据，电子证据能准确反应整个事件的完整过程和经过

4.脆弱性

电子证据能被轻易的盗用，修改甚至摧毁而不留下任何证据

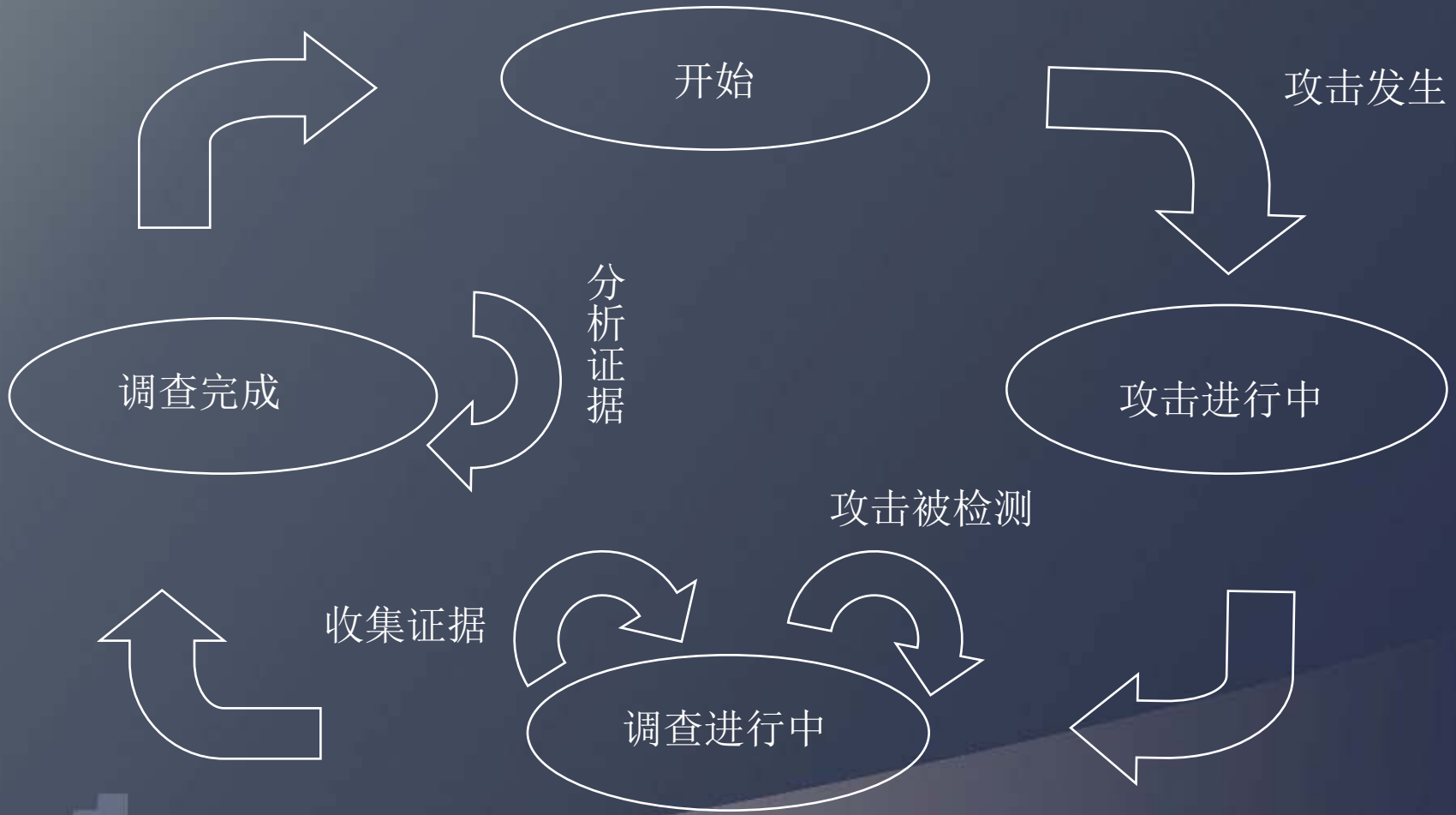
电子证据的特点

5.数据的挥发性（易失性）

经过一段时间，数据可能就无法得到或者是失效

数据	硬件或位置	存活时间
CPU	高速缓存、管道	整个时钟周期
系统	RAM	直至系统关闭
内核表	进程中	直至系统关闭
固定介质	swap、tmp	直到被覆盖或者抹去
可移动介质	floopy、hdd、flashdisk	直到被覆盖或者抹去

计算机取证模型



计算机取证的原则

1. 尽早搜集证据，并保证其没有受到任何破坏
2. 必须保证“证据连续性”（有时也被称为“chain of custody”），即在证据被正式提交给法庭时，必须能够说明在证据从最初的获取状态到在法庭上出现状态之间的任何变化，当然最好是没有任何变化
3. 整个检查、取证过程必须是受到监督的，也就是说，由原告委派的专家所作的所有调查取证工作，都应该受到由其它方委派的专家的监督。

计算机取证的要求

- 在不对原有物证进行任何改动或者损坏的情况下进行取证
- 证明所获取的证据和原有的数据是相同的
- 在不改动数据的前提下进行数据分析

常用常用取证工具

- 证据收集类：EasyRecovery、DiskScrub、SafeBack、NetMonitor
- 证据分析类：DtSearch、i2、Ipfilter、Netxray、WinHex、EnCase
- 证据呈堂（陈述）类：NTIDOC

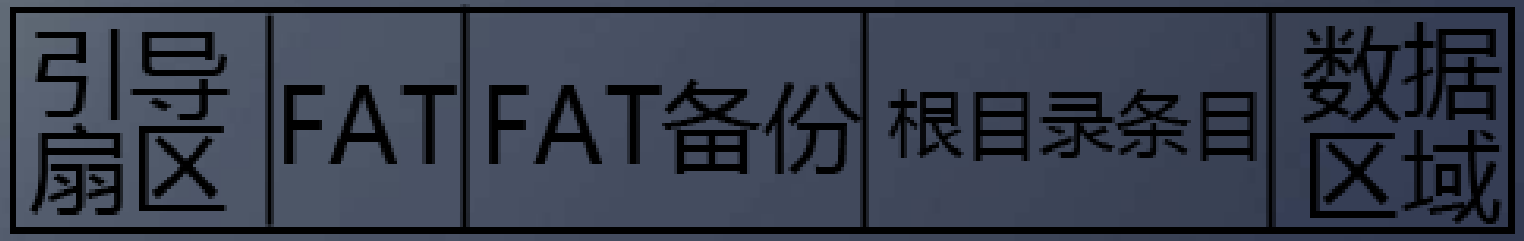
数据恢复技术

通常我们所获得的计算机硬盘中所包含的证据文件都被犯罪分子擦除或者摧毁，所以数据恢复是计算机取证的很重要的一部分

- 硬件恢复方式：①硬件替代、②伺服软件修复、③盘片读取（深层信号还原技术）
- 软件恢复方式：①基于文件目录的数据恢复、②基于文件数据特征的数据恢复、③残缺数据的数据恢复

FAT&NTFS分区结构

FAT分区结构示意图



NTFS分区结构示意图

证据收集

- windows系统调查取证

- linux系统调查取证

- unix系统调查取证

Windows系统调查取证

目前我国绝大多数计算机上都安装windows操作系统，因此windows操作系统是取证人员最有可能遇到的系统。

取证调查：

(1)、windows系统联机取证调查

(2)、windows系统静态取证分析

在计算机取证的时候为了避免被调查计算机的系统被破坏，一般采取的措施是断开网线、关闭计算机电源，妥善保管计算机，准备进行离线取证，但是这会造成案件中涉及的易失数据的丢失。

Windows系统调查取证

我们应该怎样选择较好的取证方式？

联机取证和静态取证都会使我们失去一部分证据，一般我们都根据以往的经验判断目标系统上易失性数据的价值。如果判断易失性数据的价值非常高，我们应该毫不犹豫的进行windows联机取证。

Windows系统调查取证

windows系统中证据存放位置：易失性数据(寄存，缓存)、松弛空间（slack区），未分配空间、系统日志、注册表、应用程序日志、交换文件、应用程序生成的临时文件、回收站、打印机的脱机打印序列

证据文件易失性排行：寄存器或缓存器中的数据、路由表，ARP缓存，内存中的数据、硬盘中的数据

取证演示

windows系统取证调查

- 操作系统：windows xp
- 使用工具：EnCase、hash、pslist、psloglist、winhex、IceSword等
- 目的：获取被调查计算机的有关信息

pagefile.sys(分页文件)

电脑中所运行的程序均需经由内存执行，若执行的程序很大或很多，则会导致内存消耗殆尽。为解决该问题，Windows中运用了虚拟内存技术，即匀出一部分硬盘空间来充当内存使用。当内存耗尽时，电脑就会自动调用硬盘来充当内存，以缓解内存的紧张。是计算机系统内存管理的一种技术。它使得应用程序认为它拥有连续的可用的内存（一个连续完整的地址空间），而实际上，它常是被分隔成多个物理内存碎片，还有部分暂存储于外部磁盘存储器上，在需要时进行数据交换。若计算机缺乏运行程序或操作所需的随机存储器 (RAM)，则 Windows 会用之进行补偿。它将计算机的RAM和硬盘上的临时空间组合。当RAM运行速度缓慢时，它便将数据从RAM移动到称为“分页文件”的空间中。将数据移入与移出分页文件可释放RAM，以便完成工作。

XP_CmdShell

- shell是指用户与操作系统对话的一个接口，我们发出一个命令，通过shell告诉系统让系统执行我们的指令。而SHELL前面加个前缀"CMD"则表示这个shell的类型为"CMD"，类似于我们平常所说的"WEBSHELL"，就是通过WEB向服务器发送命令。
- XP表示本存储过程是扩展的存储过程，即extend procedure

SQL注入

- 所谓SQL（“Structured Query Language”结构化查询语言）注入，就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令，比如先前的很多影视网站泄露VIP会员密码大多就是通过WEB表单递交查询字符暴出的，这类表单特别容易受到SQL注入式攻击.

SA权限

- SA权限（即 SYSTEM 和ADMIN的缩写）是msSQL数据库的默认系统帐户，具有最高权限。 可以利用扩展存储过程执行系统命令. 比如添加系统的管理员，打开远程桌面的功能，黑客就可以在自己的电脑上控制整台服务器，所以是极其危险的
注入时也有很大机率碰到ＳＡ帐号启动数据库，基本上就可以拿到系统权限．所以，现在许多网站都不用ＳＡ帐号连接数据库，保证服务器安全。

NetBIOS

- NETBIOS协议是由IBM公司开发，主要用于数十台计算机的小型局域网。该协议是一种在局域网上的程序可以使用的应用程序编程接口（API），为程序提供了请求低级服务的统一的命令集，作用是为了给局域网提供网络以及其他特殊功能，系统可以利用WINS服务、广播及Lmhost文件等多种模式将NetBIOS名解析为相应IP地址，实现信息通讯，所以在局域网内部使用NetBIOS协议可以方便地实现消息通信及资源的共享。因为它占用系统资源少、传输效率高，所以几乎所有的局域网都是在NetBIOS协议的基础上工作的。

SSDT

- SSDT(System Services Descriptor Table)，系统服务描述符表。这个表就是一个把ring3的Win32 API和ring0的内核API联系起来。SSDT并不仅仅只包含一个庞大的地址索引表，它还包含着一些其它有用的信息，诸如地址索引的基地址、服务函数个数等。　　通过修改此表的函数地址可以对常用windows函数及API进行hook，从而实现对一些关心的系统动作进行过滤、监控的目的。一些HIPS、防毒软件、系统监控、注册表监控软件往往会采用此接口来实现自己的监控模块，　　目前极个别病毒确实会采用这种方法来保护自己或者破坏防毒软件，但在这种病毒进入系统前如果防毒软件能够识别并清除它将没有机会发作.

偏移量

- 存储单元的实际地址与其所在段的段地址之间的距离称为段内偏移，也称为“有效地址或偏移量”。
- 更通俗一点讲，内存中存储数据的方式是：一个存储数据的“实际地址”=段首地址+偏移量

常用反取证工具

- 加密工具：BestCrypt、PGP、PrivateDisk
- 数据擦除工具：Zero Tracks、Tracks Eraser Pro
- 数据隐藏工具：ImageHide、MP3Stego

反取证工具演示

- 操作系统：windows 7
- 利用工具：ImageHide、MP3Stego
- 目的：将数据隐藏到流媒体、图片中，起到阻碍取证效果

相关法律法规

- 非法侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统，处3年以下有期徒刑或拘役。(刑法第285条)
- 非法对计算机信息系统功能进行删除、修改、增加、干扰，后果严重的，处5年以下有期徒刑。(刑法第286条第一款)
- 非法对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加操作，处3年以下有期徒刑或拘役。(刑法第286条第二款)
- 故意制作、传播计算机病毒等破坏性程序后果严重的，处5年以下有期徒刑。(刑法第286条第三款)
- 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪后果严重的，处5年以下有期徒刑。(刑法第287条)

总结

- 计算机取证是一个涉及法学、刑事侦查学、计算机科学等学科的交叉学科，在进行计算机取证的相关司法实践过程中，也常常需要对相关问题从相关法律、侦查方法、取证规范、取证技术等多个角度进行思考

谢谢