网络安全 – 取证技术

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

计算机犯罪简述

计算机取证定义

计算机取证原则与步骤

国内外计算机取证应用现状

蜜罐技术

计算机犯罪简述

计算机取证定义

计算机取证原则与步骤

国内外计算机取证应用现状

蜜罐技术

背景

随着社会信息化、网络化大潮的推进，社会生活中的计算机犯罪由最初的“小荷才露尖尖角”到目前的层出不穷，举不胜举。

因此，电子数据证据的法律效力正在成为学界关注的焦点。

社会信息化发展步伐 – 硬件方面

Moore定律：每18个月相同价格的集成电路的处理能力就会加倍。

Intel研制出“纳米”晶体管，摩尔定律将被推翻

硅芯片晶体密度提百倍，摩尔定律再用20年

英特尔即将启用远紫外技术，摩尔定律再获新发展

……

社会信息化发展步伐 – 软件方面

由最初的手动编制二进制代码到汇编语言、高级语言、面向对象的概念、软件工程到UML建模技术，软件开发日益呈现工程化、自动化趋势，软件的应用范围日益拓展，已成为社会生活重要组成部分。

社会信息化发展步伐 – 网络与通信

CNNIC的统计：我们的网民总量截至2002年7月为4580万，上网计算机数量为1613万台，CN下注册的域名数量是126146个。

WWW站点数（包括.CN、.COM、.NET、.ORG下的网站）大约293213个。

计算机犯罪概念 – 广义

Computer related crime or computer aimed crime?

广义说：计算机犯罪———通常是指所有涉及计算机的犯罪。如：

- **欧洲经济合作与发展组织的专家认为:“在自动数据处理过程中任何非法的、违反职业道德的、未经过批准的行为都是计算机犯罪。”**
- **我国刑法学者有人认为:“凡是故意或过失不当使用计算机致使他人受损失或有受损失危险的行为,都是计算机犯罪。”**

计算机犯罪概念 – 狭义

狭义说：计算机犯罪————通常是对计算机资产本身进行侵犯的犯罪。例如：

瑞典的私人保密权法规定:“未经过批准建立和保存计算机私人文件,非法窃取电子数据处理记录或非法篡改、删除记录侵犯个人隐私的行为都是计算机犯罪。”

我国有学者认为,“计算机犯罪是指利用计算机操作所实施的危害计算机信息系统(包括内存数据及程序)安全的犯罪行为” 。

计算机犯罪概念 – 折中

折衷说：计算机本身在计算机犯罪中以“犯罪工具”或“犯罪对象”的方式出现,这一概念注重的是计算机本身在犯罪中的作用。如：

德国学者施奈德认为：“计算机犯罪指的是利用电子数据处理设备作为作案工具的犯罪行为，或者把数据处理设备当作作案对象的犯罪行为。”

我国学者认为：“计算机犯罪是以计算机为工具或以计算机资产为对象的犯罪行为。”

计算机犯罪的特点 - 1

犯罪形式的隐蔽性

- **计算机犯罪一般不受时间和地点限制,可以通过网络大幅度跨地域远程实现,其罪源可来自全球的任何一个终端,随机性很强**

计算机犯罪的特点 - 2

犯罪主体和手段的智能性

- **计算机犯罪的各种手段中,无论是“特洛依木马术”,还是“逻辑炸弹”,无一不是凭借高科技手段实施的,而熟练运用这些手段并实现犯罪目的的则是具有相当丰富的计算机技术知识和娴熟的计算机操作技能的专业人员**

计算机犯罪的特点 - 3

复杂性

- **犯罪主体的复杂性**
- **犯罪对象的复杂性**

计算机犯罪的特点 - 4

跨国性

- 网络冲破了地域限制，计算机犯罪呈国际化趋势。因特网络具有“时空压缩化”的特点，当各式各样的信息通过因特网络传送时，国界和地理距离的暂时消失就是空间压缩的具体表现。这为犯罪分了跨地域、跨国界作案提供了可能。
- 犯罪分子只要拥有一台联网的终端机，就可以通过因特网到网络上任何一个站点实施犯罪活动。而且，可以甲地作案，通过中间结点，使其他联网地受害。由于这种跨国界、跨地区的作案隐蔽性强、不易侦破，危害也就更大

计算机犯罪的特点 - 5

匿名性

- 罪犯在接受网络中的文字或图像信息的过程是不需要任何登记，完全匿名，因而对其实施的犯罪行为也就很难控制。
- 罪犯可以通过反复匿名登录，几经周折，最后直奔犯罪目标，而作为对计算机犯罪的侦查，就得按部就班地调查取证，等到接近犯罪的目标时，犯罪分子早已逃之夭夭了

计算机犯罪的特点 - 6

损失大，对象广泛，发展迅速，涉及面广

- **计算机犯罪始于六十年代，七十年代迅速增长，八十年代形成威胁。美国因计算机犯罪造成的损失已在千亿美元以上，年损失达几十亿，甚至上百亿美元，英、德的年损失也达几十亿美元**
- **我国从1986年开始每年出现至少几起或几十起计算机犯罪，到1993年一年就发生了上百起，近几年利用计算机计算机犯罪的案件以每年30%的速度递增，其中金融行业发案比例占61%，平均每起金额都在几十万元以上，单起犯罪案件的最大金额高达1400余万元，每年造成的直接经济损失近亿元**

计算机犯罪的特点 - 7

持获利和探秘动机居多

- 全世界每年被计算机犯罪直接盗走的资金达20亿美
- 我国2001年发现的计算机作案的经济犯罪已达100余件，涉及金额达1700万元，在整个计算机犯罪中占有相当的比例
- 各种各样的个人隐私、商业秘密、军事秘密等等都成为计算机犯罪的攻击对象。侵害计算机信息系统的更是层出不穷

计算机犯罪的特点 - 8

低龄化和内部人员多

- 我国对某地的金融犯罪情况的调查，犯罪的年龄在35岁以下的人占整个犯罪人数的比例：1989年是69.9%，1990年是73.2%，1991年是75.8%。其中年龄最小的只有18岁
- 此外，在计算机犯罪中犯罪主体中内部人员也占有相当的比例。据有关统计，计算机犯罪的犯罪主体集中为金融、证券业的“白领阶层”，身为银行或证券公司职员而犯罪的占78%，并且绝大多数为单位内部的计算机操作管理人员；
- 从年龄和文化程度看，集中表现为具有一定专业技术知识、能独立工作的大、中专文化程度的年轻人，这类人员占83%，案发时最大年龄为34岁

计算机犯罪的特点 - 9

巨大的社会危害性

- **网络的普及程度越高，计算机犯罪的危害也就越大，而且计算机犯罪的危害性远非一般传统犯罪所能比拟，不仅会造成财产损失，而且可能危及公共安全和国家安全。**
- **据美国联邦调查局统计测算，一起刑事案件的平均损失仅为2000美元，而一起计算机犯罪案件的平均损失高达50万美元。据计算机安全专家估算，近年因计算机犯罪给总部在美国的公司带来的损失为2500亿美元**

计算机犯罪的类型举例 - 1

非法侵入计算机信息系统罪

《刑法》第285条规定,违反国家规定,侵入国有事务、国防建设、尖端科学技术领域的计算机信息系统的,处三年以下有期徒刑或者拘役。

计算机犯罪的类型举例 - 2

破坏计算机信息系统罪。

这一行为《刑法》第286条概括为破坏计算机信息系统罪。主要表现为:

- **故意对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重的行为**
- **故意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、增加的操作,后果严重的行为**
- **故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重的行为**

计算机犯罪的类型举例 - 3

《刑法》第287条规定了利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密罪。利用计算机实施盗窃的行为纳入盗窃罪定罪处罚的范围,从而使盗窃罪更具信息时代的特征

如盗窃电子资金,不法分子往往利用电子资金过户系统,例如定点销售系统(ＰＯＳ Ｓ)、自动存取款机(ＡＴＭＳ)自动化票据交换所(ＡＣＨＳ)、电子身份证系统等提供的便利,使用计算机技术通过网络修改电子资金帐目,窃取电子资金

计算机犯罪的形式 - 1

数据欺骗

- **非法篡改输入/输出数据获取个人利益,是最普通最常见的计算机犯罪活动。发生在金融系统的此种计算机犯罪多为内外勾结,串通作案,由内部人员修改数据,外部人员提取钱款**

计算机犯罪的形式 - 2

意大利香肠术

- **侵吞存款利息余额,积少成多的一种作案手段,是金融系统计算机犯罪的典型类型。**
- **这种方法很像偷吃香肠一样,每次偷吃一小片并不引起人们的注意,但是日积月累的数目也是相当可观。**
- **此类案件在国内外均有发现,因为只有修改计算机程序才能达到其犯罪目的,故多为直接接触程序的工作人员所为。**
- **目前国内多数为局域网管理银行帐目而产生此类犯罪,因此,要警惕采用此手段作案的罪犯**

计算机犯罪的形式 - 3

特洛依木马

- “特洛依木马”来源于古希腊传说,相传希腊人为了攻陷特洛依城,在城外故意抛下一个木马并假装撤退,特洛依人将木马拖回城内后,埋伏在木马内的希腊士兵就打开城门,里应外合而将特洛依城攻陷。
- 它是表面上来看是正常合适的,但在内部却隐藏秘密指令和非法程序段的程序的代名词。
- “特洛依木马”就是用来表示以软件程序为基础进行欺骗和破坏的方法

计算机犯罪的形式 - 4

冒名顶替

- 利用别人口令,窃用计算机谋取个人私利的做法。
- 在机密信息系统和金融系统中,罪犯常以此手法作案。单用户环境多为内部人员所为,网络系统则可能为非法渗透。
- 由于人们普遍存在猎奇心理,对别人加密程序,总想解密一睹,因此用户口令应注意保密和更新,且最好不用容易破译的口令密码,如电话号码、出生日期、人名缩写等

计算机犯罪的形式 - 5

清理垃圾

- **从计算机系统周围废弃物中获取信息的一种方法。**
- **由此带来损失的例子并不罕见,提醒计算机用户不要随便处理所谓废弃物,因为其中可能含有不愿泄漏的信息资料**

计算机犯罪的形式 - 6

逻辑炸弹

- **指插入用户程序中的一些异常指令编码,该代码在特定时刻或特定条件下执行破坏作用,所以称为逻辑炸弹或定时炸弹**

计算机犯罪简述

计算机取证定义

计算机取证原则与步骤

国内外计算机取证应用现状

蜜罐技术

取证的基本概念

定义

- **计算机取证（ computer forensics ）就是对计算机犯罪的证据进行获取、保存、分析和出示，实际上可以认为是一个详细扫描计算机系统以及重建入侵事件的过程**
- **可以认为，计算机取证是指对能够为法庭接受的、足够可靠和有说服性的，存在于数字犯罪场景(计算机和相关外设)中的数字证据的确认、保护、提取和归档的过程**

取证的基本概念

目的

- **计算机取证的目的是根据取证所得的证据进行分析，试图找出入侵者和/或入侵的机器，并重构或解释入侵过程**
- **who /when /where/ how/ what**

取证的基本概念

计算机取证希望解决的问题

- **攻击者是如何进入的?**
- **攻击者停留了多长时间?**
- **攻击者做了什么?**
- **攻击者得到了什么?**
- **如何确定在攻击者主机上的犯罪证据?**
- **如何赶走攻击者?**
- **如何防止事件的再次发生?**
- **如何能欺骗攻击者?**

有关电子数据证据

任何材料要成为证据，均需具备三性：

- **客观性**
- **关联性**
- **合法性**

计算机取证（电子取证）定义

综合：

- **计算机取证是指对能够为法庭接受的、足够可靠和有说服性的，存在于计算机和相关外设中的电子证据的确认、保护、提取和归档的过程。**

计算机取证（电子取证）定义

计算机取证专业资深人士Judd Robins:

- 计算机取证不过是简单地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上

一家专业计算机紧急事件响应和计算机取证咨询公司：

- 计算机取证包括了对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档

一篇综述文章给出了如下的定义：

- 计算机取证是使用软件和工具，按照一些预先定义的程序全面地检查计算机系统，以提取和保护有关计算机犯罪的证据

取证的基本概念 - 证据的特点

- 可信的
- 准确的
- 完整的
- 使法官信服的
- 符合法律法规的，即可为法庭所接受的

电子证据的特点

- 表现形式和存储格式的多样性
- 高科技性和准确性
- 脆弱性和易毁坏性
- 数据的挥发性

电子证据的优点

- 可以被精确的复制
- 用适当的软件工具和原件对比，很容易鉴别当前的电子证据是否有改变
- 在一些情况下，犯罪嫌疑人完全销毁电子证据是比较困难的

电子证据的来源 - 1

来自系统

- 硬盘、移动硬盘、U盘、MP3播放器、各类软盘、磁带和光盘等
- 系统日志文件、应用程序日志文件等
- 交换区文件，如386.swp、PageFile.sys；临时文件、数据文件等
- 硬盘未分配空间；系统缓冲区等
- 备份介质等

电子证据的来源 - 2

来自网络

- 防火墙日志、IDS日志
- 系统登录文件、应用登录文件、网络单元登录(Network Element logs)
- 磁盘驱动器、网络数据区和记数器、文件备份等

电子证据的来源 - 3

来自其他数字设备

- **便携设备中存储的数据**
- **路由器、交换机中的数据**
- **各种配置信息**
- **磁卡、IC卡等**

电子证据与传统证据的区别

- 计算机数据无时无刻不在改变；
- 计算机数据不是肉眼直接可见的，必须借助适当的工具
- 搜集计算机数据的过程，可能会对原始数据造成很严重的修改，因为打开文件、打印文件等一般都不是原子操作
- 电子证据问题是由于技术发展引起的，因为计算机和电信技术的发展非常迅猛，所以取证步骤和程序也必须不断调整以适应技术的进步

计算机犯罪简述

计算机取证定义

计算机取证原则与步骤

国内外计算机取证应用现状

蜜罐技术

取证的原则 - 1

一般原则

- 尽早搜集证据，并保证其没有受到任何破坏
- 必须保证取证过程中，计算机病毒不会被引入目标计算
- 不要在作为证据的计算机上执行无关的程序

取证的原则 - 2

一般原则

- 必须保证“证据连续性”（最好是没有变化）
- 整个检查、取证过程必须是受到监督的
- 要妥善保存得到的物证
- 详细记录所有的取证活动

取证步骤

数据获取

- 不知道哪些数据将作为证据，所以该阶段复制硬盘上所有数据

数据分析

- 不同案例对数据分析需求不一样
- 数据分析在原始数据的物理拷贝进行

证据陈述

- 给出调查所得到的的结论已经相应证据
- 法官、律师、陪审团、听众

取证步骤 - 数据获取 1

- 了解所有可能存放有电子证据的地方
- 了解主机系统以外的相关软硬件配置
- 无损地复制硬盘上所有已分配和未分配的数据
- 对不同类型的计算机采取不同的策略以收集计算机内的所有数据

取证步骤 - 数据获取 2

- 在取证检查中，保护目标计算机系统，远离磁场，避免发生任何的改变、伤害、数据破坏或病毒感染
- 对系统进行数据备份

计算机取证相关技术 – 数据获取技术

数据获取技术包括：

- 对计算机系统和文件的安全获取技术，避免对原始介质进行任何破坏和干扰
- 对数据和软件的安全搜集技术
- 对磁盘或其它存储介质的安全无损伤备份技术
- 对已删除文件的恢复、重建技术
- 对磁盘空间、未分配空间和自由空间中包含的信息的发掘技术
- 对交换文件、缓存文件、临时文件中包含的信息的复原技术
- 计算机在某一特定时刻活动内存中的数据的搜集技术
- 网络流动数据的获取技术等

取证步骤 - 数据分析

- 根据现有的（包括已经被删除的、临时的、交换区、加密的）数据，分析出对案件有价值的电子证据
- 需要分析师的经验和智慧
- 注意保护数据完整性
- 取证过程必须可以复验以供诉状结尾的举例证明

计算机取证相关技术 – 数据分析技术

数据分析技术：在已经获取的数据流或信息流中寻找、匹配关键词或关键短语是目前的主要数据分析技术，具体包括：

- 文件属性分析技术；
- 文件数字摘要分析技术；
- 日志分析技术
- 根据已经获得的文件或数据的用词、语法和写作（编程）风格，推断出其可能的作者的分析技术
- 发掘同一事件的不同证据间的联系的分析技术
- 数据解密技术
- 密码破译技术
- 对电子介质中的被保护信息的强行访问技术等

取证步骤 - 证据陈述

- 对专家和/或法官给出调查所得到的结论及相应的证据
- 陈述过程中需注意遵守国家法律、政策、企业规章制度

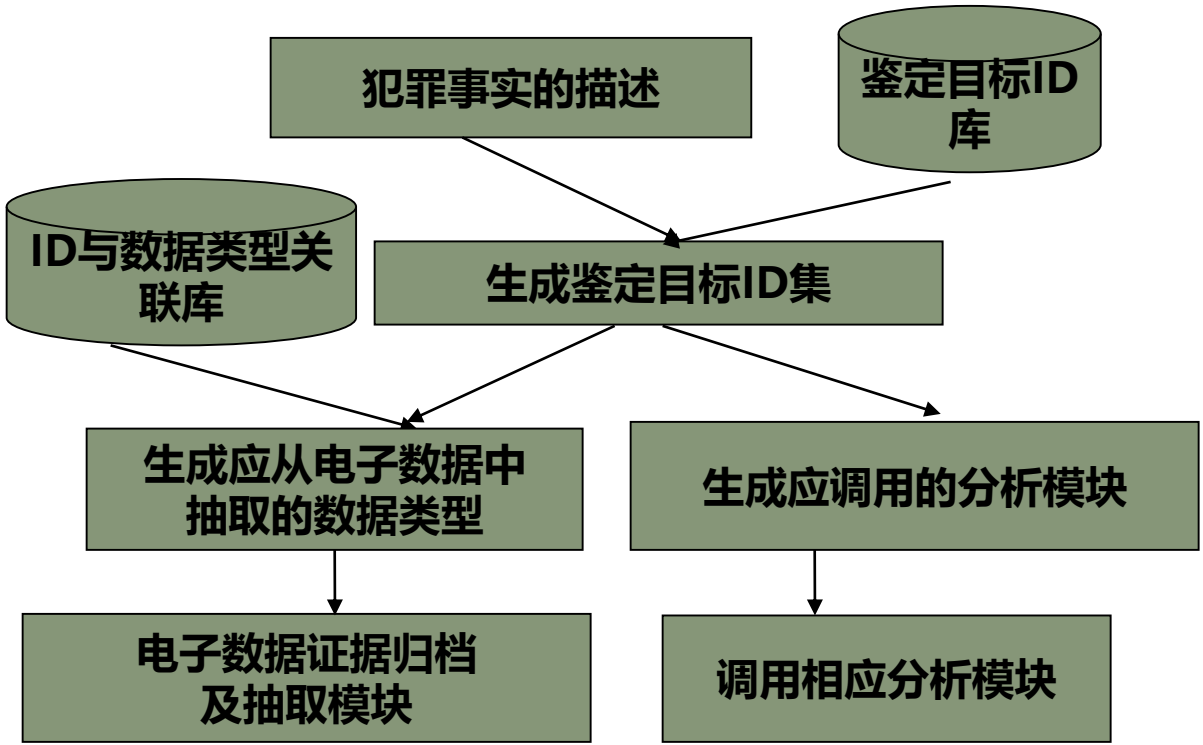
计算机取证技术发展趋势

计算机取证技术进一步与信息安全技术相结合

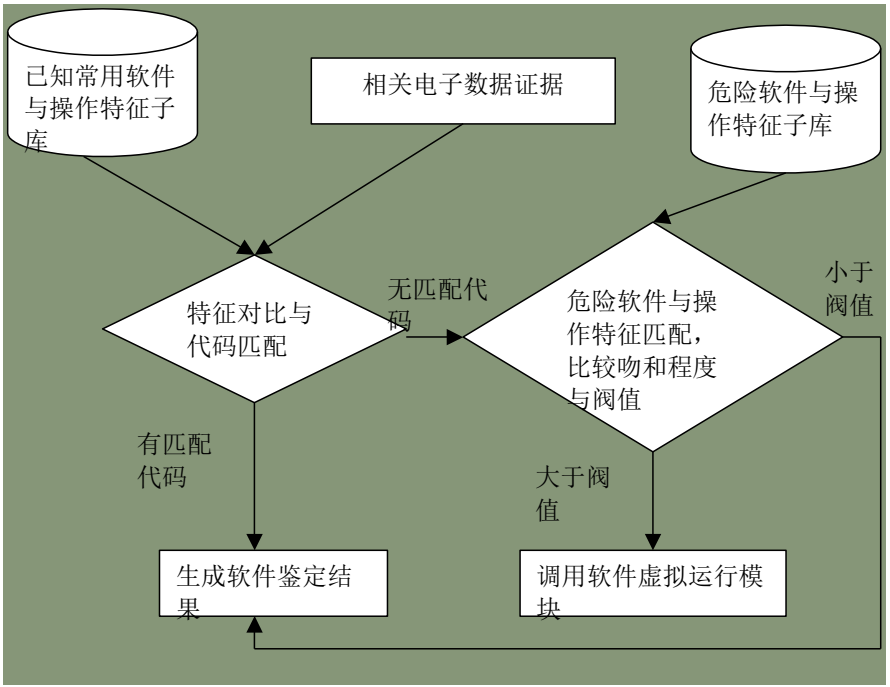
在网络协议设计过程中考虑到未来取证的需要，为潜在的取证活动保留充足信息。

取证工具的开发往往结合人工智能、机器学习、神经网络和数据挖掘技术

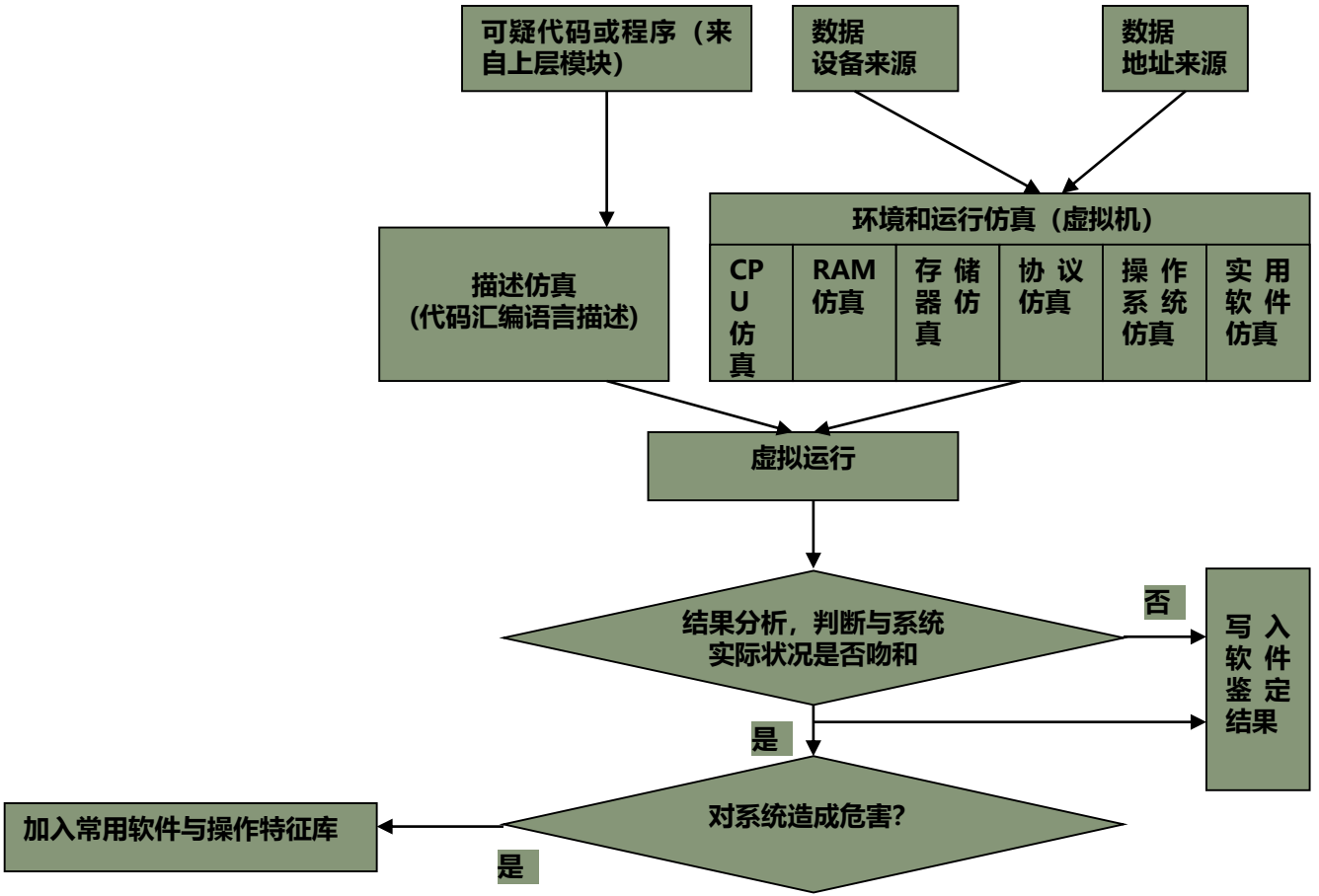
鉴定目标描述转换模块


犯罪事实的描述
鉴定目标ID库
ID与数据类型关联库
生成鉴定目标ID集
生成应从电子数据中抽取的数据类型
生成应调用的分析模块
电子数据证据归档及抽取模块
调用相应分析模块

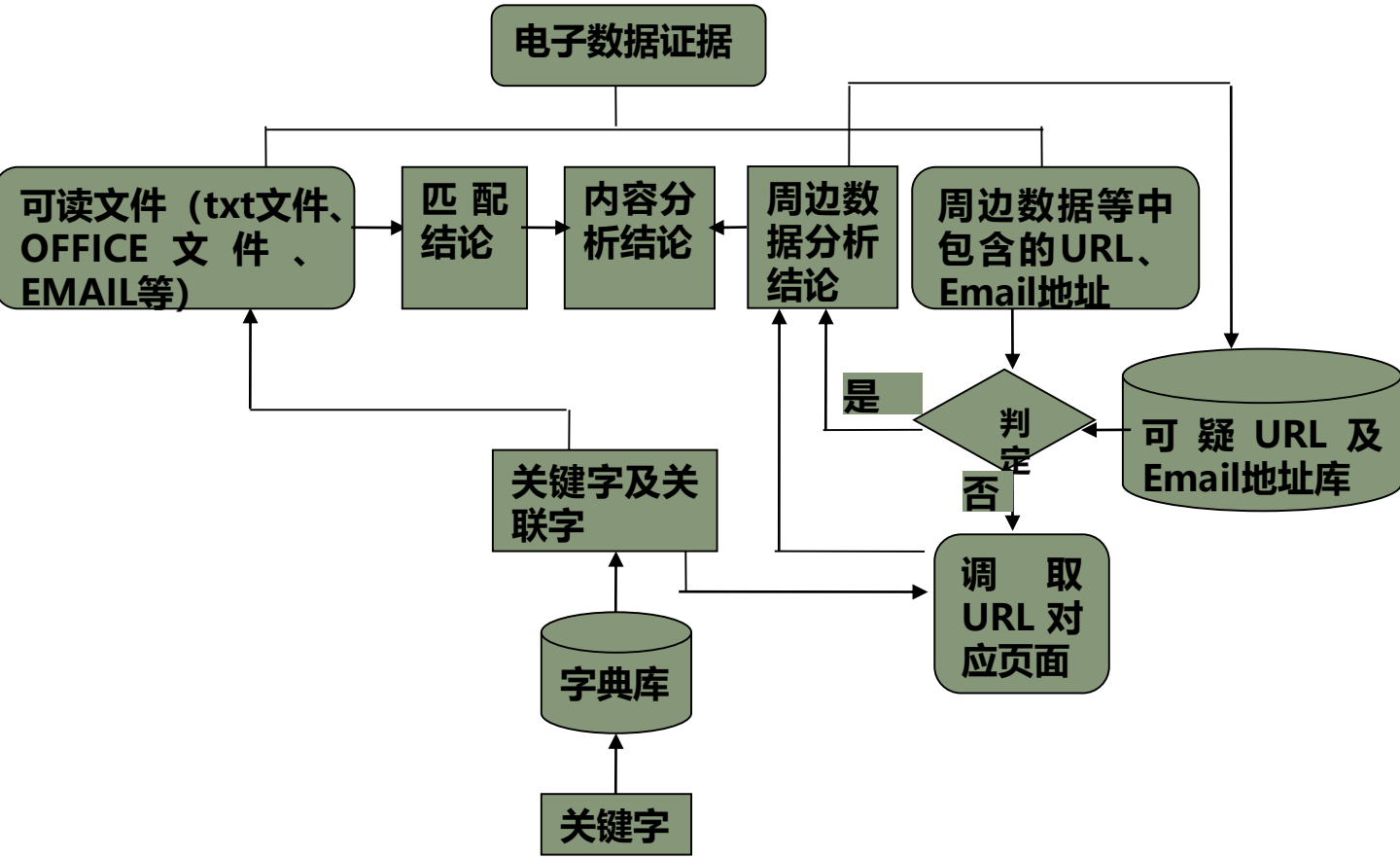
数据软件来源智能分析模块



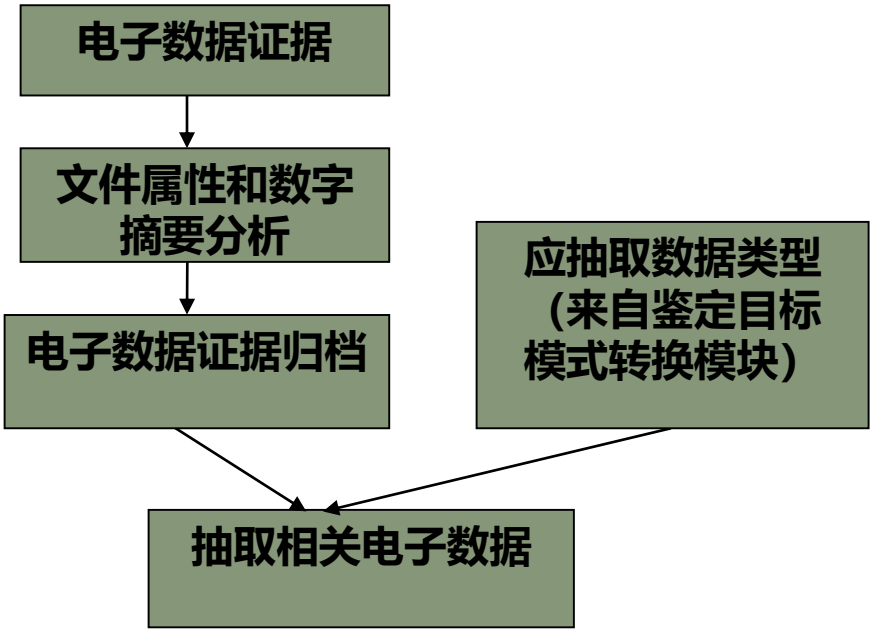
特定软件与操作虚拟运行模块



电子数据证据内容分析


电子数据证据
可读文件（txt文件、OFFICE 文 件 、EMAIL等)
匹 配结论
内容分析结论
周边数据分析结论
周边数据等中包含的URL、Email地址
是
判定
否
可 疑 URL 及 Email地址库
关键字及关联字
调 取 URL 对应页面
字典库
关键字

电子数据证据归档及抽取模块



电子数据证据的法律性搜集 - 1

主要是指电子证据收集的法律程序上的要求,主要包括收集主体的要求、收集具体程序的要求，以及其收集中和相关权利的冲突和协调。

由于电子证据的不稳定性和易更改性,为收集者作假和随意变更提供了可能,因此对于电子证据的收集的主体应当严格限定。

电子数据证据的法律性搜集 - 2

证据的收集必须遵循法定的程序

我国刑事诉讼法第43条就明确规定了收集证据应当遵循的程序,民事诉讼法也规定了收集证据的必须程序。

由于电子证据的特殊性,所以在电子证据的收集过程中既应当遵循一般证据的收集的规则,又应当遵循其特有的规则。包括:

- **全面收集原则,这主要是指在刑事诉讼中,既要收集对犯罪嫌疑人、被告人不利的证据也要收集对其有利的证据,收集过程重要注重对其人权的保护。**

电子数据证据的法律性搜集 - 3

民事诉讼中电子证据的收集的程序要求分为法院主持下的收集和当事人的收集。

在法院主持下的收集,应当有审判人员的主持,并且由两个以上的人共同进行,要对证据收集的若干情况进行详细的记载。

在当事人个人收集电子证据时,应当有特定的国家机关,主要是公证机关对其收集过程、以及所收集证据的真实程度进行见证或者公证。

无论是何种收集方式,在收集时都应当有相关的见证人在场,特别是记载该数据的计算机的操作员或者管理者的在场。

电子数据证据的法律性搜集 - 4

在电子证据的收集过程中,要注意电子证据的收集和相关人的隐私权之间的冲突问题的解决,这类问题主要发生在国家机关收集电子证据的过程中

在一般情形下,电子证据的收集和提取主要是对在计算机的数据处理系统中已经存储或者处理的数据

但是许多情形下,电子数据并不是现成的,而这种时候往往会采取对电子邮件、电子通讯等的监听和窃听的方式来取得证据。

这种方式如果运用不当就会侵犯公民的隐私权。

计算机犯罪简述

计算机取证定义

计算机取证原则与步骤

国内外计算机取证应用现状

蜜罐技术

国外计算机取证历史及现状 - 1

法律的制定：

- 自1976年的Federal Rules of Evidence起，美国出现了如下一些法律解决由电子证据带来的问题：
- The Economic Espionage Act of 1996: 处理商业机密窃取问题
- The Electronic Communications Privacy Act of 1986: 处理电子通信的窃听问题
- The Computer Security Act of 1987(Public Law 100-235): 处理政府计算机系统的安全问题

国外计算机取证历史及现状 - 2

取证技术：

- **逐渐走向自动化、智能化，政府与各专业机构均投入巨大人力、物力开发计算机取证专用工具**

国外计算机取证历史及现状 - 3

用于电子数据证据获取的工具：

- **如 Higher Ground Software Inc. 的软件 Hard Drive Mechanic 可用于从被删除、被格式化的和已被重新分区的硬盘中获取数据。**
- **NTI公司的GetFree可从活动的Windows Swap分区中恢复数据，该公司的软件GetSlack可自动搜集系统中的文件碎片并将其写入一个统一的文件**

国外计算机取证历史及现状 - 4

用于电子数据证据归档的工具：

- **如NTI公司的软件NTI-DOC可用于自动记录电子数据产生的时间、日期及文件属性。**

国外计算机取证历史及现状 - 5

结论：

- 针对计算机取证的全部活动而言，美国的各研究机构与公司所开发的工具主要覆盖了电子数据证据的获取、保全、分析和归档的过程
- 各研究机构与公司也都在进一步优化现有的各种工具，提高利用工具进行电子证据搜集、保全、鉴定、分析的可靠性和准确度，进一步提高计算机取证的自动化和智能化
- 但目前还没有能够全面鉴定电子数据证据设备来源、地址来源、软件来源的工具

国内计算机取证历史及现状 - 1

我国的计算机普及与应用起步较晚，有关计算机取证的研究与实践工作也仅有10年的历史，相关的法律法规仍很不完善，学界对计算机犯罪的研究也主要集中于计算机犯罪的特点、预防对策及其给人类带来的影响。

目前法庭案例中出现的计算机证据都比较简单，多是文档、电子邮件、程序源代码等不需特殊工具就可以取得的信息。

但随着技术的进步，计算机犯罪的水平也在不断提高，目前的计算机取证技术已不能满足打击计算机犯罪、保护网络与信息安全的要求，自主开发适合我国国情的、能够全面检查计算机与网络系统的计算机取证的工具与软件已经迫在眉睫。

计算机取证技术 – 展望

计算机取证是一门专业性与技术性很强又发展极其迅速的应用学科。随着我国信息产业的迅猛发展，计算机取证的应用日益拓展，同时也对计算机取证人员提取了巨大的挑战。

现阶段，在实践中适用的计算机取证专用工具还比较少，但我们国家也已经开始投入巨大的人力、物力从事专业工具的研发，相信在我们的共同努力下，不久的将来我们必会缔造一个更加安全、纯净的信息、网络空间！

计算机犯罪简述

计算机取证定义

计算机原则与步骤

国内外计算机取证应用现状

蜜罐技术

蜜罐技术 – 概述

蜜罐系统是一个包含漏洞的诱骗系统

- 它通过模拟一个或多个易受攻击的主机，给攻击者提供一个容易攻击的目标
- 让攻击者在蜜罐上浪费时间，延缓对真正目标的攻击
- 对入侵的取证提供重要的信息和有用的线索，并使之成为入侵的有力证据

虽然蜜罐不会直接提高计算机网络安全，但它却是其它安全策略不可替代的一种主动防御技术

蜜罐技术 – 主要功能

对系统中所有的操作和行为进行监视和记录

通过对系统进行伪装，使得攻击者在进入到蜜罐系统后并不会知晓其行为已经处于系统的监视之中

优点

- **使用简单（无计算、存储、匹配）**
- **资源占用少（仅捕获）**
- **数据价值高**

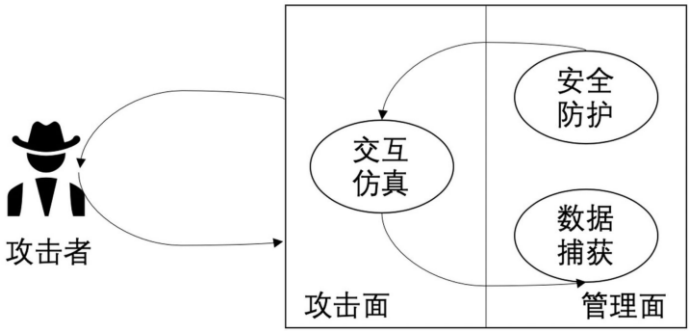
缺点

- **数据收集面狭窄，只能搜集对蜜罐的攻击数据**
- **可能给使用者带来额外的风险**

蜜罐技术 – 分类 1

根据设计目的

- **产品型**
- **研究型**



交互程度

- **低交互蜜罐、中交互蜜罐和高交互蜜罐**

技术

- **牺牲型蜜罐、外观型蜜罐和测量型蜜罐**

3类交互蜜罐对比

	低交互蜜罐	中交互蜜罐	高交互蜜罐
包含等级	低	中	高
真实操作系统	否	否	是
危险性	低	中	高
信息收集	连接	请求	所有
被攻陷期望	否	否	是
运行所需知识	低	低	高
建立所需时间	低	高	中
维护时间	低	低	很高

蜜罐技术 – 分类 2

技术

- **牺牲型蜜罐：可建立在任何设备上的真实系统，包括加载操作系统，定期检查判断是否被入侵**
- **外观型蜜罐：模拟系统**
- **测量型蜜罐：容易访问，难饶过，在用户终端配置和管理**

蜜罐技术 – 配置方式

诱骗服务

弱化系统

- **对已知攻击作用不大**

强化系统

- **管理员比攻击者更高安全知识技能**

用户模式服务器

- **一个进程模拟一个服务器**
- **防护性好**

蜜罐技术 – Honeynet

Honeynet是专门为研究设计的高交互型蜜罐

- **与蜜罐的区别?**

与其他大部分蜜罐不同在于:

- **它不进行模拟，而是对真实的系统不进行修改或改动很小**
- **不是一个单独的系统而是由多个系统和多个攻击检测应用组成的网络**
- **系统产品都是真实设备，防护改进基于真实问题**

蜜罐技术 – 发展趋势

提高仿真度

- **增加可以模拟的服务**
- **增加与攻击者交互的深度**

降低引入的风险

增加蜜罐可以运行的平台

反蜜罐技术

现有的反蜜罐措施主要针对低交互蜜罐，它本身具备一些指纹信息比如软件硬编码或网络层指纹信息。

硬编码特征是低交互蜜罐在开发的过程中，引入了一些固定字段即硬编码特征，导致在响应数据包中会暴露蜜罐系统，而蜜罐仿真系统对协议分片的处理不正确或协议仿真不完全都会导致出现网络层指纹信息。

攻击者亦可利用时间延迟也可识别蜜罐，因为低交互蜜罐作为软件运行在操作系统上层，会对资源造成消耗，增大响应时延。

也有一些反蜜罐措施是在进入蜜罐系统后，采用系统调用的方式，调用内部某些功能，依据执行的结果判断是否是蜜罐。

课后习题

1. 简述蜜罐的目的和蜜罐系统的工作原理

2. Honeynet与蜜罐有哪些相似和不同之处?

谢谢!