填空题10个 简单题 方案设计题

电子数据证据的特点：客观性、关联性和合法性

(1) 客观性。客观性即考察电子数据证据在生成、存储、 传输过程中有无剪接、删改、替换的情况，其内容是否前后 一致、符合逻辑。

(2) 关联性。关联性即分析电子数据证据与案件事实是 否有关联，关联程度如何，是否实质性关联，其中附属信息 与系统环境往往要相互结合，并排除相互之间的矛盾，才能 与案件事实发生实质性关联。

(3) 合法性。合法性即电子数据证据应合法，违反法定

程序取得的电子数据证据应予排除。我国《刑事诉讼法》规 定：“审判人员、检察人员、侦查人员必须依照法定程序， 收集能够证实犯罪嫌疑人、被告人有罪或者无罪、犯罪情节 轻重的各种证据。严禁刑讯逼供和以威胁、引诱、欺骗以及 其他非法的方法收集证据。”

电子数据证据的特殊性：

(1) 技术依赖性。与其他证据不同，电子数据证据的形 成与存在必须依赖现代电子设备和技术实现，电子数据证据 的提取与展现也必须借助电子设备并通过一定的技术手段来 实现。因此，电子数据证据本质上是以电子形式存储或传输 的数据，具有技术依赖性。

(2) 隐蔽性。与其他传统证据相比较，电子数据证据是

以虚拟形态保存的。传统证据的内容和形态可以被直接感知， 而电子数据证据则是将信息以电磁等形式存储在介质中。例 如硬盘存储信息时，通过磁性材料而形成的电磁场将电子信 息记录下来；而在向光盘中记录信息时，则是利用激光将信 息以凹凸点的形式记录在光盘上的。这些数字信息以0和1表 示，通过排列组合来表示特定数值的数据，其内容无法被人 们直接感知。所以，记录方式的隐蔽性是电子数据证据与传 统证据最本质的区别，也是电子数据最根本的特点。

(3) 易破坏性。电子数据证据以电子信息的形式存储在

电磁介质中，较传统证据而言，电子数据证据更易被篡改， 且可不留痕迹。环境的影响如供电故障、硬件故障、病毒、 人为操作等，都会导致电子数据改变和灭失，从而影响电子 数据的真实性和完整性。因此，电子数据证据的记录方式及 介质的特殊性和网络空间的特性决定了它自身具有一定的易 破坏性。

(4) 稳定性。在电子数据内容之外也包含一些重要信息，

如隐藏在原数据中的信息、储存和运行环境中的痕迹信息等， 这些都是电子数据证据的信息。电子数据证据的这一特点，

可以使大量不为人知的电子数据得以保存，使电子数据可以 作为证据使用的效力大大增加，这是因为要对磁盘上的数据 信息、网络环境中的实时信息、计算机运行状态的系统信息 等进行修改而又不留下修改的操作痕迹是很难做到的。通过 数据恢复、数据挖掘等技术手段可以发现对数据信息修改的 蛛丝马迹，并有可能恢复原始数据信息。因此，电子数据证 据较传统证据更具有安全性和稳定性。

(4) 稳定性。在电子数据内容之外也包含一些重要信息，

如隐藏在原数据中的信息、储存和运行环境中的痕迹信息等， 这些都是电子数据证据的信息。电子数据证据的这一特点，

可以使大量不为人知的电子数据得以保存，使电子数据可以 作为证据使用的效力大大增加，这是因为要对磁盘上的数据 信息、网络环境中的实时信息、计算机运行状态的系统信息 等进行修改而又不留下修改的操作痕迹是很难做到的。通过 数据恢复、数据挖掘等技术手段可以发现对数据信息修改的 蛛丝马迹，并有可能恢复原始数据信息。因此，电子数据证 据较传统证据更具有安全性和稳定性。

(5) 开放性。从司法实践来看，电子数据证据越来越多 地与互联网联系在一起，而网络的一个重要特点是可以不受 时空限制获取电子数据，这是电子数据的开放性的表现，也 是对该类证据的收集亟须加以规范的地方。

1. 表现形式的多样性。电子数据证据的表现形式是多 种多样的，可以是文本、图像、音频、视频等，将多种表现 形式融为一体是电子数据证据独有的特点。这要求电子数据 取证工具具有识别多种形式的电子数据证据的能力。

1.2 电子数据取证

电子数据取证 技术涉及从计算机和网络设备中获取、保存、分析、出示相 关电子数据证据的法律、程序、技术等问题。

1.依法取证原则

任何证据的有效性和可采用性都取决于证据的客观性、 与案件事实的关联性和取证活动的合法性。

2.保护证据完整性原则

《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》第五条规定：“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；

(一) 扣押、封存电子数据原始存储介质；

(二) 计算电子数据完整性校验值；

(三) 制作、封存电子数据备份；

(四) 冻结电子数据；

(五) 对收集、提取电子数据的相关活动进行录像；

1. 其他保护电子数据完整性的方法。”

3.及时取证原则

电子数据证据的获取具有实效性，一旦确定对象后，应 尽快提取证据，防止证据变更和丢失。

4.证据连续性原则

2.2.4电子数据分析与检验阶段

分析证据是电子数据取证的核心和关键，通过分析已获

取的数据来确定证据的类型，包括检查文件和目录内容以及 恢复已删除的内容，分析计算机的类型，分析采用的操作系 统是否为多操作系统或有无隐藏的分区、有无可疑外设、有 无远程控制、有无木马程序及当前计算机系统的网络环境等， 并用科学的方法结合已发现的证据推出结论。鉴于要求不同， 所使用的计算机科学技术和具体程序方法不尽相同。常见的方法有数据搜索技术、数据恢复技术、加密解密技术、文件 系统分析技术、日志分析技术、静态分析技术、动态分析技 术、实时监控技术、追踪技术、数据挖掘技术等。

2.4.2 取证方法分类

1. 数据获取的方法和思路

在获取数据时，需要考虑电子数据的来源，根据来源不 同，数据获取常分为数据包获取、内存数据获取、存储介质 获取。数据包获取是一种实时获取通信流量的方法，以供后 续的分析；内存数据获取是指获取案件发生时计算机及相关 设备的状态，从而可对这些易失性数据进行进一步分析；存 储介质获取是指获取除易失性数据外的静态数据，包括硬盘 数据、Flash存储介质中的数据等。

数据搜索的方法和思路

数据搜索是指从大量电子数据中搜索特定数据的方法。 根据搜索采用方法不同，数据搜索技术常分为基于数据内容 的搜索技术、基于数字指纹的搜索技术和基于痕迹信息的搜 索技术。

2) 基于数字指纹的搜索技术

基于数字指纹的搜索技术不直接比较文件的内容，而是 通过比较能够代表文件内容的指纹来判断搜索出的文件是否 为需要获取的电子数据。表示文件指纹的方法非常多，但大 多使用二进制字符串表示，大体分为两种不同的形式：数字 指纹和模糊指纹(一种特殊的数字指纹)。

数字指纹指采用Hash函数处理后的字符串。2) 基于数字指纹的搜索技术

基于数字指纹的搜索技术不直接比较文件的内容，而是 通过比较能够代表文件内容的指纹来判断搜索出的文件是否 为需要获取的电子数据。表示文件指纹的方法非常多，但大 多使用二进制字符串表示，大体分为两种不同的形式：数字 指纹和模糊指纹(一种特殊的数字指纹)。

数字指纹指采用Hash函数处理后的字符串。

3) 基于痕迹信息的搜索技术

基于痕迹信息的搜索技术与上述搜索技术不同，它通过 发现目标数据对应的位置或者属性，间接搜索出电子数据证 据，如通过注册表中相关自启动选项去搜索木马程序等。

检验分析的方法和思路

对于不同来源的电子数据、不同案件中的电子数据，其 检验分析的方法千差万别，通常有两种方法：静态分析方法 和仿真分析方法。静态分析方法是指通过专用取证计算机或 者专用取证软件直接分析涉案电子数据镜像或者备份设备的 方法。仿真分析方法是指通过仿真软件还原用户使用设备时 的状态，或者搭建运行环境动态分析涉案电子数据的方法。

NTFS文件系统记录了以下内容：

(1) 对象(文件/文件夹)的基本属性，包括名称、日期时 间信息、大小、属性等。

(2) 对象的起始位置，即起始簇。

(3) 对象的数据片段(不连续的簇)。

(4) 逻辑卷上所有簇的状态。

恶意代码取证特点如下：

(1) 高度的加密性和隐蔽性。

(2) 证据的可靠性，封闭结构使证据效力大为提高。

基于行为分析安全系统的实现方式主要有3种，分别为

基于阈值探测、统计分析和智能学习。这3种方式中以基于智能学习的行为分析系统功能最为强大，该系统综合采用神 经网络(主要是遗传算法)、模糊技术等经典方法识别入侵特 征，自学能力极强，还能更新与扩展自身系统知识库。

病毒的植入/安装通常有以下几个步骤。

1) 隐藏程序

一般情况下，解压缩后的病毒会把程序主体部分复制到 系统目录中，正是因为系统目录中存放了许多重要系统文件， 这就导致系统用户不能轻易发现病毒程序，再加上病毒复制 程序的文件命名与系统中文件命名十分相似，对病毒程序复 制文件的定位也就变得更加困难。此外，即便计算机用户对 这些复制文件心存怀疑，也会出于担心对系统文件造成破坏 的顾虑，而不会轻易修改或删除这些文件。

2) 自启动设置

为了使病毒能够在特定条件下自动运行，病毒本身会进 行自启动设置。自启动设置的实现方法很多，常用方法如下：

(1) 病毒会修改注册表项的内容，篡改信息。

(2) 修改文件关联。文件关联其实就是打开某类型文件 的系统默认方式。

3) 修改系统的配置文件

有些系统配置文件(包括WIN.INI 、SYSTEM.INI、

AUTOEXEC.BAT等)可能会被病毒修改，在Windows 7和

Windows 8操作系统中通过注册服务和添加计划任务等方式 来实现随机启动目的。值得注意的是，为了避免被防火墙等 系统安全软件发现，许多病毒会选择在安装阶段关闭系统中 的杀毒软件和防火墙进程，从而入侵计算机。

如果仅仅把这些API调用作为恶意行为的标准，

并用这些标准来区别病毒与合法程序，结果并不是很准确， 原因主要有以下两点：

(1) API函数自身并不具备恶意性质，它们仅仅是微软 公司提供给广大用户的应用程序开发接口。也就是说，正常 程序合法调用的API，病毒程序也会频繁调用，这就很难对 API函数进行有效的区分。

(2) 表3-9中列举的API 其实并不是通过大量实际样本的 验证得到的，而只是在初步研究阶段结合反病毒工程师的经 验所得，因此只能判断API 调用为疑似恶意的，不能肯定它 们就是恶意行为的特征。

因此，若要以研究危害用户操作系统的API函数为基础

重新总结病毒的恶意行为特征，就要遵循下面几点原则：

(1) 恶意代码可能会发生的所有动作行为都应被记录下

来，暂不考虑合法程序是否出现此行为。检测模型得到的判 断结果决定了该行为究竟是不是恶意代码，因此没有必要急 于在搜集动作行为阶段做出判断。

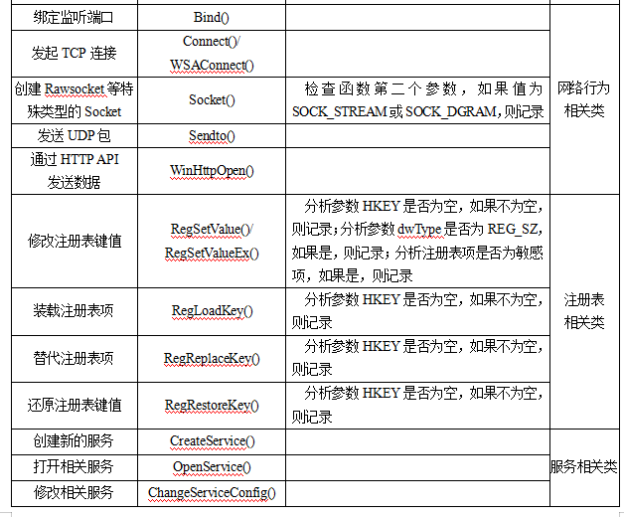
1. 行为特征分析不只是分析API，描述行为的语言也要简洁明了，示例如下：
2. 修改注册表启动项。

② 写文件。

(3) 病毒一旦在机器上运行，就会采用Rootkit隐藏踪迹

或是寄生在合法程序中，追踪其行为很困难，因此需重点强 调病毒在安装过程中的系列行为。





Windows事件日志通常可以为取证人员提 供以下信息：

(1) 发生什么：Windows内部的事件日志记录了丰富的 历史事件信息。

(2) 发生时间：事件日志中记录了丰富的时间信息，也 常称为时间戳，它记录了各种事件发生的具体时间。

(3) 涉及的用户：在Windows操作系统中，几乎每一个 事件都与相关的系统账号或用户账号有关。

(4) 涉及的系统：在联网环境中，单纯记录主机名对于 取证人员来说比较难以进一步追踪回溯访问请求的来源信息。

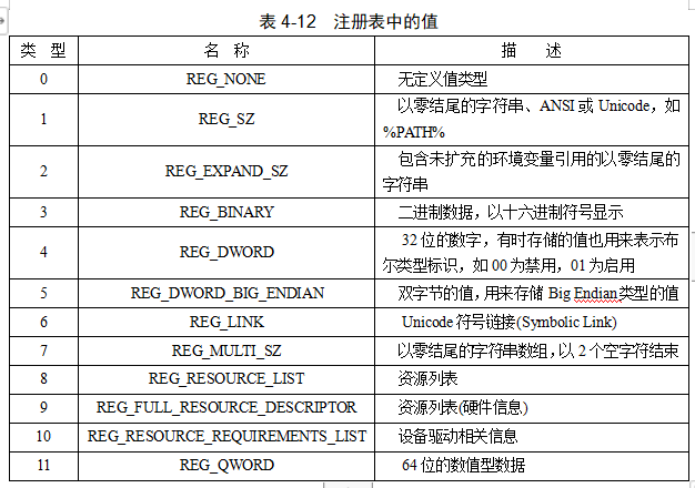
(5) 资源访问：事件日志服务可以记录细致的事件信息。

常见的Windows事件日志的分析方法。

Windows事件日志中记录的信息中，关键要素包含事件级别、记录时间、事件来源、事件ID、事件描述、涉及的用户、计算机、操作代码及任务类别等。常见Windows账户及相关事件对照表如表4-2所示，其中事件ID与操作系统版本有关，同类事件在不同操作系统中的事件ID不完全相同，最大的差异主要体现在第一版和第二版的事件日志中。因此， 在取证过程中需特别注意，当使用事件ID进行过滤搜索时，需要考虑操作系统版本的差异。

注册表的层级结构及数据类型

注册表的顶级目录一般称为键(Key)、主键或项，子目录称为子键(Subkey)或子项，存储的数据项一般称为值(Value)。注册表中的值可以存储多种不同类型的数据，如表4-12所示。



常见的注册表取证内容

1. 时区信息

注意：当被调查人 员使用的时区与取证人员计算机使用的时区不同时，切记一 定要提取注册表中的时区信息(Time Zone)，然后手工修改 取证软件对磁盘设备的时区设置，只有这样才能正确解析出 文件相关时间戳。

1. 最近使用的文件（MRU）

国内的多数计算机取证分析软件可以对常见的MRU信息进行提取和解析。

常见MRU对照表，能够列举出几个常见的来

3) 应用程序访问痕迹(UserAssist)

Windows操作系统在运行过程中对使用频率高的应用程 序进行了记录，包括应用程序名称、路径、运行次数、最后 一次执行时间等信息。记录的信息存在于注册表中的UserAssist子键中。

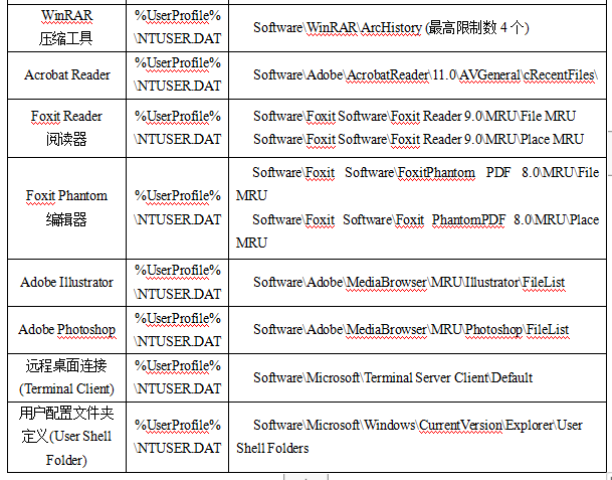
4) USB设备使用记录

USB设备(如加密狗、U盘、移动硬盘、

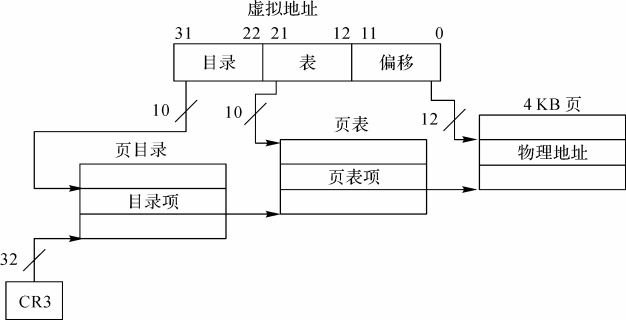
智能手机等)在与计算机连接时，系统将会识别出USB设备， 并在注册表中生成相关的键信息。







分页技术 （重点）



内存中有大量的结构化数据和非结构化数据。通过对物理内存镜像，可以提取有价值的数据。常见有价值的数据包 含以下内容：

(1) 进程列表(包括恶意程序进程、Rootkit隐藏进程等)。

(2) 动态链接库(当前系统或程序加载的动态链接库)。

(3) 打开文件列表(当前系统打开的文件列表)。

(4) 网络连接(当前活动的网络连接)。

(5) $MFT记录(常驻文件均可以直接提取恢复)。

(6) 注册表(部分注册表信息，包括系统注册表和用户注 册表文件)。

(7) 加密密钥或密码(如Windows账户密码Hash、

BitLocker 、SafeBoot 、PGP 、TrueCrypt 、 VeraCrypt等全盘 加密或加密容器的恢复密钥等)。

(8) 聊天记录(如QQ聊天记录片段)。

(9) 互联网访问(上网记录URL地址、网页缓存及InPrivate隐私模式访问数据等)。

(10) 电子邮件(如网页邮件缓存页面)。

(11) 图片及文档(尚未保存到磁盘中的图片、文档等文 件)等。

ESE数据库中的数据表及关系

通过利用Nirsoft网站提供的ESEDatabaseView工具可以 查看ESE类型的数据库内容。通过实验可以发现，在新一代 浏览器IE 10.0和IE 11.0中，上网记录、缓存文件及Cookies的记录信息都保存在WebCacheV01.dat数据库中。

Cookies可以让调查人员了解浏览器使用者访问过哪些

网址，并且在该网站进行的一些相关操作，有时甚至可以提 取到Cookies中保存的用户名、密码明文及密文(如经过散列 算法保护MD5)等用户信息。通常Cookies需要设定其有效期， 它包含一系列记录，每条记录包括以下相关信息：

(1) 变量(Key)：存储的变量名。

(2) 值(Value)：关键字的值。

(3) 主机(Host)：写入该记录的主机名称。

(4) 安全性：通常有True和False两个值(如果是SSL站点， 则通常为True)。

(5) 修改时间：最后一次修改记录的时间。

(6) 有效期：过期后该Cookies信息将失效。

打印脱机(Spooling)文件是一种为完成打印任务而生成 的临时文件，包含了要打印的数据以及完成打印任务所需的 详细信息。打印脱机池由多个动态链接库组成，用于接收、 处理、计划及分发打印请求或任务。

跳转列表文件分为以下两种类型：

(1) Automatic(自动)：系统会自动弹出此类跳转列表，

该跳转列表记录了文件使用的相关信息，并将该信息存储于 目标文件，与用于打开该文件的程序进行关联。

(2) Custom(自定义)：该跳转列表由各应用程序维护， 可提供与程序菜单或自定义分类相关的任务列表。

快捷方式文件包含一些与目标文件相关的有价值的信息，

具体如下：

(1) 文件的时间戳(网卡地址(MAC) 3个时间)。

(2) 文件大小。

(3) 卷详细信息——系列号、卷标。

(4) 原始文件路径。

Lunix操作系统下的目录

/dev：在Linux操作系统下任何设备及接口设备都是以文件形式存在于设备文件存储目录中的。

/etc：系统的主要配置文件都放在该目录下，为了避免 发生系统执行错误，在此目录下不放其他外部可执行文件。

/mnt：临时文件系统的挂载点目录。

/proc：虚拟文件系统目录，放置内存中的数据，当有

一个进程启动时，就自动创建一个文件夹。比较重要的有 /proc/meminfo和/proc/cpuinfo，可以通过这两个文件查看内 存和CPU的情况；另外还有 /proc/dma 、/proc/interrupts、

/proc/ioports 、/proc/net/\* 等文件。

inode结构信息。

inode信息中主要记录了文件模式、UID 、GID、文件大小、实际使用扇区数、访问时间、文件修改时间、inode修 改时间、文件删除时间、直间接块寻址数组或extent树、文 件ACL信息等。

（注意哪些变化，哪些没变化）

当文件被删除后，Ext中inode中的文件大小、实际使用

扇区数、extent信息均清零，而inode修改时间、文件修改时 间、文件删除时间、硬连接数均进行了更新，但文件的创建 时间未发生变化。

被删除文件的特点和恢复方法

Ext3/4文件系统中的文件被删除以后，文件内容对应的 block中的信息并未被删除，目录中block中的文件名与inode 的关联也未变化，而仅仅删除了inode位图、block块位图中 对应位的信息，以及更新了目录中相邻项长度和超级块、组 描述符表中的有关信息，但inode表中的数据块指针或者

extent信息则清零，因而给被删除文件的恢复带来了较大困 难，但可利用日志中备份inode信息或者文件头部特征等信 息进行数据恢复。通常可采用两种不同方法进行数据恢复。

方法1：利用文件系统遗留痕迹进行数据恢复。在

journal日志文件中找到残留的inode信息，根据inode信息定 位到相关目录(或先确定目录项，再在日志中确定inode备份 信息)，恢复残留inode对应的block，从而恢复被删除的文件。

方法2：利用文件自身的特殊结构进行恢复。对于具有文件头特征或者具有特殊结构和格式的文件，可根据文件自身特点进行数据恢复。这种数据恢复因不考虑文件系统本身 的特征，故可用支持该方法的通用数据恢复软件进行恢复。但在数据恢复之前需要考虑文件系统物理空间是否连续，如 果使用了LVM 、RAID等存储方式，则首先要通过重组或者仿真方法提取出整个分区的镜像，然后进行恢复，否则有可 能因数据恢复软件不能准确解析上述结构而使恢复效果变差。

完整的syslog日志中包含产生日志的程序模块(Facility)、

严重性(Severity或Level)、时间、主机名或IP、进程名、进程ID和正文。

下面介绍表5-4所列日志中的几个重要日志。

(1)  **secure 。**/var/log/secure日志文件中的每一条记录通 常包含日期与时间信息、主机名称、服务名称与ID号以及 其他显示信息。在Linux新发行版本中，secure 日志已经被 auth.log和authpriv代替。

(2) **auth** 。/var/log/auth是Linux新发行版本的安全登录日志，记录包含时间、主机名称、服务名称、ID以及登录信息。

1. **message** 。/var/log/message日志文件通常包含时间、 主机名、程序名、PID和相应消息，但由于登录信息过多， 外部接入信息有可能被掩盖，因此可以进行消息定制。

(4) **maillog** 。/var/log/maillog日志文件记录包含时间、主机名、进程、ID以及相关信息。

(5) **cron** 。/var/log/cron日志文件主要记录crontab的守护进程crond派生的子进程的信息，包含时间、用户进程、ID以及相关信息。

(6) lastlog 。/var/log/lastlog日志文件记录用户最近成功登录和最后一次未成功登录事件。每条记录包含用户名、端 口号、上次登录时间等信息。

(7) .bash\_history。“~/.bash\_history ”(“~/”表示用户目录)文件能够保存相关用户最近使用过的命令。

Linux网络信息分析的基本思路

Linux网络信息分析通常从获取用户权限和访问信息开始，分析程序管理模块，查看登录日志中是否存在可疑记录。 常见可疑记录或操作有：管理员账户登录时间是否异常，是否登录频次异常（暴力破解）、登录多次尝试失败，是否加载过跨session等异常脚本等。

网络数据源有以下内容：

1. 主机网络配置。
2. 防火墙。
3. 入侵检测系统。
4. 远程访问连接。

(5) ISP(Internet Service Provider，网络服务提供商)记录。

收集网络信息

在Linux操作系统运行过程中，网络数据可能会存在于 系统各处，具体可能分布在检测软件、日志文件、远程服务 器存储数据中等。下面着重介绍Linux操作系统里的网络日志信息部分。网络日志信息主要分为3大类：Linux系统日志、网络设 备日志(如路由器、交换机)和应用程序日志(如检测软件、VPN 、SSH等Web应用)。

Linux系统日志。

5.2.3节中已对Linux日志做了较为详细的介绍，这里主要介绍与网络信息分析有关的日志。涉 及网络信息的Linux系统日志系统主要有以下3类：

① 登录时间日志系统。

② 进程统计日志系统。

③ 错误日志系统，由进程syslogd(Linux新发行版本采 用rsyslogd进程服务)进行管理。

通常在分析网络信息时需要注意以下要点：

① 排除“良性”事件。存在一些类攻击事件是由于系 统本身运行出错导致的，需要排除这些“良性”事件。

② 创建具有时间线的证据链。

③ 完整记录分析时的操作过程。分析过程需要在取证 之后得以验证，因此完整的记录是校验操作的合理性和科学 性的有效证据。

2. 内存镜像文件分析

1) 内存镜像文件的获取

获取内存镜像文件是实验室分析内存的前提，内存镜像 可以基于硬件方式获取，也可以基于软件方式获取。基于软 件方式获取内存镜像比较灵活，目前很多取证产品均通过此 方式实现。下面仅基于软件方式介绍内存镜像文件的获取方式。

按照原理不同，基于软件获取镜像文件的方式可分为两类：第一类是利用对象或设备直接读取物理内存，第二类是利用驱动或内核扩展读取物理内存。

利用备份恢复数据库数据

在电子数据取证实务过程中，数据库恢复对电子数据取 证有至关重要的作用。常用的数据库恢复技术有以下两种：

(1) 通过binlog日志进行恢复。

(2) 通过导入备份的SQL进行恢复。

另外，数据库转储技术、数据库镜像恢复技术等都可进 行数据库恢复。

Android功能特点

1. 应用程序权限机制

2. 应用程序沙盒机制

3. 全盘加密

4. 文件级加密

图案密码的加密原理(Android 2.2～Android 5.x)

图案密码的加密方式主要分为图案输入、明文转换、计 算散列3个步骤。

(1) 用户设置图案密码“Z”字母图形，如图8-24所示。

(2) 系统按照点位排列将上述图案依序转换为00-01-02- 04-06-07-08。

(3) 对该顺序字符串00010204060708进行SHA1散列计算， 得到散列值6a062b9b34 52e366407181a1bf92ea73e 9ed4c48。

(4) 将该散列值存储为gesture.key文件。

清除key文件实现密码绕过

了解了3种密码的加密原理后，便可以通过删除对应加 密方式的密码文件实现对系统密码的绕过操作。如果该设备 已经通过不同方式获取了root权限，则可以直接使用adb命

令对gesture.key 、password.key等文件进行重命名或删除来实现清除设备锁密码。

例如，使用如下命令删除图案密码的key文件：

adb shell

cd /data/system rm gesture.key

删除后可以直接绕过图案密码进入系统。

网络取证的内容主要涉及两个方面：

一是来源取证，指取证目的主要是确定犯罪嫌疑人及其 所在位置，取证内容主要包括IP地址、MAC地址、电子邮件信箱、软件账号等；

二是事实取证，指取证目的不是查明犯罪嫌疑人是谁， 而是要确定犯罪实施的过程和具体内容，取证内容主要包括文件内容调查、使用痕迹调查、日志文件分析、网络状态和数据包分析等。

网络电子证据的特点

网络电子证据是通过网络进行传输的网络数据，其存在 形式是电磁或电子脉冲。与传统证据一样，网络电子证据必 须是可信的、准确的、完整的、符合法律法规的证据。但由于网络电子证据的存在形式依赖于网络传输协议，缺乏可见 的实体，采用不同的传输协议，其格式及传输方式就会不同。 因此，网络电子证据必须通过专门工具和技术来进行正确的提取和分析，使之具备证明案件事实的能力。

网络电子证据具有以下特点：

(1) 表现形式的多样性。

(2) 存储介质的电子性。

(3) 准确性。

(4) 脆弱性。

(5) 海量性。

(6) 广域性。

数据包获取方法和途径

1. ARP协议的抓包

ARP工作流程分为两个阶段，一个是ARP请求过程，另一个是ARP响应过程。在了解ARP协议的基础上，可以利用 Wireshark等抓包工具中的ARP捕获器直接捕获ARP协议包。 需要捕获ARP包时，可以在主机上执行ping命令，即可产生 ARP包进行获取。

针对远程节点的取证思路

获取服务器的IP、账号和密码后，应当在有录音录像以 及见证人的条件下对远程服务器进行勘验。远程节点的取证 思路主要是从登录日志、配置文件、Shadowsocks日志等内容固定本地节点的访问IP、访问记录等证据。除了常规的取证分析外，还可从以下几点进行取证分析：

(1) 通过last命令固定登录日志。

(2) 通过history命令查看历史命令，分析固定开启Shadowsocks服务的证据。

(3) 通过find命令查找Shadowsocks服务的配置文件，该文件为.json格式，一般命名为shadowsocks.json/shadow.json， 将配置文件的内容固定证据用来与本地节点的配置文件相互 印证。

(4) 通过find命令查找Shadowsocks的日志文件，该日志 文件默认存在/var/log/ shadowsocks.log，从中可以获取连接时间、连接IP、访问的URL等。

最后通过对本地节点和远程节点的综合分析比对，形成相互印证的证据链。在做好上述取证工作后，若条件许可，则可以通过远程做镜像来固定服务器内容。

基于BT种子的网络犯罪

主要从以下几点进行取证分析：

(1) 在种子发布的网站获取种子样本。

(2) 使用种子编辑器或文本编辑器打开种子文件，获取 Tracer服务器的地址。

(3) 通过分析发布网站的日志信息以及Tracer服务器的日 志信息溯源发布的IP地址。

(4) 根据种子生成的时间进行分析，分析出种子的作者。

P2P技术的视频直播软件在数据传输过程中是共享周边 的资源而不是从服务中获得的，因此它具有即时性、不可恢 复性的特点。对于该类应用，主要 从以下几方面进行取证分析：

(1) 截屏。可以借助模拟器或取证专用机安装相应的直 播应用，当发现有违法犯罪行为时及时截取屏幕或拍照，以 此固定证据。同时，通过对该用户的信息进行截屏收集，从 而获得昵称、账号、犯罪嫌疑人照片等证据。

(2) 录播。在犯罪嫌疑人直播违法犯罪时使用摄像机或 屏幕录像工具进行全程录拍。

(3) 根据固定应用账号、账号昵称、房间号、直播时间 等信息从应用公司获取相应的账号注册信息、登录日志。

(4) 通过分析将犯罪嫌疑人的手机直播应用与前面取得的证据形成证据链。在分析手机时除了基础分析以外，还应 当对存在手机本地的各个应用的日志、数据库和配置文件进 行重点分析。

伪基站

GSM(Global System for MobileCommunications，全球移动通信系统)的鉴权、加密流程主要有以下几步：

(1) 当用户开启手机时，手机向基站发送IMSI。

(2) 基站收到IMSI后，将IMSI转发给HLR来启动鉴权流程。

(3) HLR收到IMSI后，先查找该IMSI是否在其IMSI库中， 如果该IMSI属于该运营商，则将IMSI继续转发至鉴权中心。

(4) AuC随后会根据IMSI查找与之绑定的鉴权密钥，鉴权密钥是运营商在生产SIM卡时生成的一个128位的数字，与IMSI一起存储于SIM卡中。

(5) MSC/VLR接收到加密密钥、SRES 、RAND后，仅将RAND发送至手机。

(6) 手机会根据RAND 、SIM卡中存储的鉴权密钥及A3算法计算出SRES，发给MSC/VLR。

(7) MSC/VLR收到SRES后，对比HLR发送给它的SRES， 如果二者一致，则允许手机接入网络。

(8) 手机使用RAND、鉴权密钥及A8算法计算出加密密钥。

(9) 手机和网络之间的通信内容使用加密密钥和加密算法A5进行加密/解密。

伪基站的危害有以下几种：

(1) 中断通信信号。

(2) 获取用户信息。

(3) 发送垃圾广告短信。

(4) 发送诈骗短信。

(5) 截取短信、通话内容。

(6) 篡改短信、通话内容。

对比Python脚本/框架，网镜脚本有诸多优点，具体如下：

(1) 直接使用浏览器的Cookies，无须处理登录问题，只要打开另一个标签页登录后再执行即可。

(2) 可以利用jQuery通过标准CSS选择器选择元素，比通 过XPATH方式更简单直观。

(3) 自动解析json 、XML 、HTML等请求类型，编写脚 本时可直接使用结果。

(4) 提供了时间解析等函数，如将“1天前”“昨天10:11”等解析为标准时间格式。

(5) 开发方便，直接在网镜中开发，无须安装Python环境。

(6) 从弘连技术支持论坛中可以找到100多个针对不同案 件网站的脚本案例、脚本教程、技术交流帖子，更方便调查 人员快速学习和掌握脚本使用方法，使用合适的脚本样例固定同类型的新案件网站。

（问区块链是什么东西要答得出来）

区块链的核心概念

按照维基百科给出的定义，区块链是借由密码学串接并 保护内容的串连交易记录，又称区块。每一个区块包含前一 个区块的加密散列、相应时间戳记以及交易数据，这样的设 计使得区块内容具有难以被篡改的特性。用区块链串接的分 布式账本能让双方有效记录交易，且可永久查验此交易。

区块链的技术特点和应用

使用以上机制构建的区块链应用具有一些与众不同的特点，包括不可篡改性、分布式存储、匿名性、价值传递、网络共识、可编程合约等。

区块链取证要点

1. 钱包的取证分析

2. 交易的取证分析

比特币是伪匿名或非匿名的，它不会凭空消失，相反 每笔交易都是公开的，对使用比特币网络的每个人都是可见的。比特币的交易是按照时间顺序组织的公开记录。

3. 交易所的落地取证

可以通过平台注册信息、交易IP等对交易双方的真实身 份信息进行落地查证。

4. 其他取证

针对不同的应用，还可以结合其他取证方式进行取证分 析。例如，在进行比特币交易时，可以通过嗅探技术监听交 易中继，还可以通过区块链浏览器的痕迹信息或Cookies发 现蛛丝马迹。

云计算取证要点

云取证是一种飞速发展的、涉及多维度的技术。云取证主要包含3个层面：一是技术层面，其中包含收集数据的流程、云取证相关工具的研发、在线取证、对获取镜像的仿真、 取证前期准备、分析等多个方面。二是管理层面，管理层面 主要涉及多个责任方，如云计算服务提供方、云计算使用者、 云安全管理协会、执法部门、第三方鉴定机构/安全审计机构等。

云取证技术

根据云计算的定义，其服务类型可以分为IaaS 、PaaS 、 SaaS 3种。对这3种服务形式，都可以在3个层面进行证据的 获取，具体如下：

(1) 应用层面：以应用账号登录，获取应用/服务内的数据。

(2) 服务层面：以云服务账号登录，对云用户租用的各 种资源和使用情况进行固定。

(3) 管理层面：以云服务提供商的账号登录，对提供的资源、数据、日志等进行固定。

从服务层面来看，IaaS 、PaaS和SaaS可以提取的数据可

能会有所不同。

针对IaaS类的主机服务，可以获取如下数据：

(1) 实例信息、运行历史信息。

(2) 网络资源、配置信息、历史信息。

(3) 存储/块设备镜像。

(4) 存储/磁盘/数据快照，如果是私有格式，则需要提供 解析方法。

(5) 存储磁盘/数据历史备份。

针对PaaS类的服务，可以获取如下数据：

(1) 实例信息、历史运行信息。

(2) 程序、数据、配置和日志。

(3) 程序、数据历史备份。

针对SaaS类的服务，可以获取如下数据：

(1) 服务类型、服务配置和历史变动。

(2) 当前服务数据。

(3) 服务历史数据备份。

智能系统取证内容

1.智能车辆取证

现时车载应用程序可以让手机通过物理或蓝牙连接至车 载娱乐系统，实现同步联系人信息、拨打/接听电话，接管了在驾车时想用手机所做的事情。为此，对已经连接到该车辆的手机进行取证及分析成为较为快速的车辆取证主要提取方法之一。利用手动拍照或手动记录的方式对车载系统内的 数据进行文档记录的方式有很多：

(1) 逻辑获取：提取车载系统存储器内的部分数据。

(2) 文件系统获取：提取车载系统的文件系统。

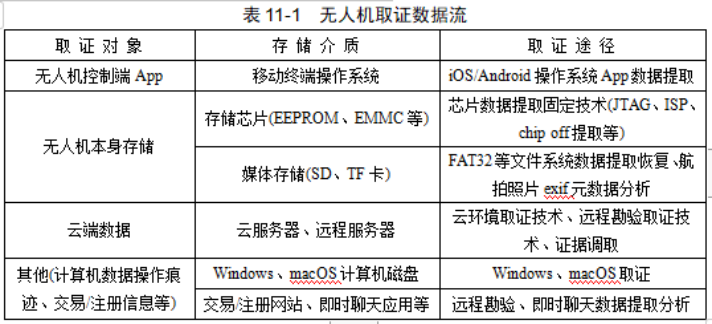
(3) 物理获取(非入侵式)：在不需要拆卸的情况下，对车载系统存储器内容进行获取。

(4) 物理获取(入侵式)：在需要拆卸的情况下，对车载系统存储器内容进行物理获取(JTAG)。

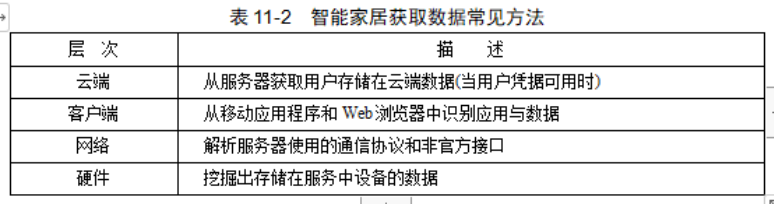
(5) 芯片获取：对车载系统存储器芯片进行移除和读取。

(6) 微读获取（意义不大）：使用高功率显微镜对车载系统存储器芯片进行物理视图。

2. 无人机取证



3. 智能家居取证



案例分析

篡改系统调用表 VFS虚拟文件系统