

计算机取证复习要点

R.G. 整理版

一段话记一下（说是结合时政。, 。必考）：

《中共中央关于全面推进依法治国若干重大问题的决定》明确提出，要“推进以审判为中心的诉讼制度改革，确保侦查、起诉的案件事实证据经得起法律的检验。全面贯彻证据裁判规则，严格依法收集、固定、保存、审查、运用证据，完善证人、鉴定人出庭制度，保证庭审在查明事实、认定证据、保护诉权、公正裁判中发挥决定性作用”。

- https://www.sohu.com/a/278351269_100284895

计算机取证复习要点

Chapter 1：取证与司法鉴定概论

1. 取证与司法鉴定概念/def:
2. 电子数字取证 vs 电子取证 vs 计算机取证与司法鉴定
3. 计算机取证的层次功能:
4. 反取证技术
5. 主动取证技术 (p5、23)
6. G8小组提出的关于取证与司法鉴定的6条原则
7. 计算机取证的4条基本原则 (通用的取证与司法鉴定原则)
8. 依法取证4要素 (要保证取证与司法鉴定的四要素同时合法才能保证证据合法)
9. 计算机取证与司法鉴定技术主要分为两类:
10. (国外) 取证与司法鉴定的过程模型 【按上一点分两类】
11. 取证与司法鉴定过程模型 (通用模型, 考试应该考这个不考上面的)
12. 取证与司法鉴定中的分析鉴定作为核心环节通常需要实施以下方案:
13. 取证与司法鉴定 计划的制定
14. 取证和司法鉴定的工作环境和证据链监督
15. 计算机取证的操作程序规则 (6条)
16. 计算机证据的显示与质证

Chapter 2: 取证与司法鉴定的相关法学问题 (这一章没有在老师的提纲里, 应该不做重点)

1. 取证与司法鉴定的主要任务:
2. 取证与司法鉴定的主要内容:
3. 取证与司法鉴定的3大技术基础
4. 取证与司法鉴定相关事项
5. 司法鉴定的8大原则
6. 司法鉴定的方法
7. 司法鉴定的程序

Chapter 3: 取证与司法鉴定基础知识

1. 仪器设备 配置原则
2. 取证的8类 必备设备
3. 取证的选配设备 (按照取证与司法鉴定的类别层次 分 3类)

4. 取证准备阶段的4个主要工作
5. 计算机证据的保全主要是解决证据的完整性
6. 计算机证据分析的主要内容(6步)【证据分析是取证的核心和关键】

Chapter 4: Windows系统取证与分析

1. Win现场取证的固定证据有哪些(3个)【感觉老师这说法不对。,。应该是需要固定的证据有哪些】
2. Win现场取证固定易丢失证据有哪些(6个)【应该是需要固定的易丢失的证据有哪些】
3. Win现场取证,现场数据收集的基本过程(4点)
4. Win两个关键的证据来源
5. Win深入获取证据的途径(4点)
6. Win电子证据的获取(7大块)
7. 常用Win取证工具
8. 现场取证和脱机取证(p113小结里)

Chapter 5: Unix/Linux取证与分析

0. Unix/Linux系统概要
1. Unix/Linux现场证据获取(Linux的现场证据有哪些?4点)
2. Unix/Linux电子证据分析
3. Unix/Linux取证与分析工具

Chapter 6: 网络取证

1. 网络取证定义、目的
2. 网络取证的特点(4点)
3. 黑客攻击的一般步骤(7步)
4. 网络取证的重点环节(5个)
5. 两类专用网络取证
6. 网络取证数据源
7. 网络通信数据的收集(2块,技术问题+法律问题)
8. 网络通信数据的检查与分析(5块:辨认相关事件、检查数据源、得出结论、攻击者确认、对检查和分析的建议)

Chapter 7: 木马取证

1. 木马简介(定义、特性、种类)
2. 木马的基本结构和原理
3. 木马的取证与分析方法
4. 书上的案例看一下:PC-Share、灰鸽子、广外男生

Chapter 8: 手机取证

1. 手机取证3大难点:
2. 手机犯罪的3中行为:
3. 手机取证概述(def、证据来源、原则、流程)
4. 手机取证基础知识(了解即可,设计一些移动通信的知识)
5. 手机取证与分析工具
6. 专业电子设备的取证与分析

Chapter 9: 取证案例

1. 熊猫烧香
2. 软件侵权

更多资料/实验代码,请关注我的GitHub、CSDN【后续我会把在HDU-网安的实验报告、复习资料,上传】:

Chapter 1：取证与司法鉴定概论

1. 取证与司法鉴定概念/def:

1. 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
2. 对计算机证据的保护、确认、提取、归档的过程
3. 从计算机中收集、发现证据
4. 运用计算机科学理论和技术，以及其他相关专门知识和经验对涉及诉讼的电子数据进行判断、鉴定
(p26)

2. 电子数字取证 vs 电子取证 vs 计算机取证与司法鉴定

1. 电子数字取证主体对象：存在于各种电子设备、计算机系统内与案件有关的数据信息
2. 电子取证主体对象：电子化存储的、能反应有关案件真实情况的数据信息
3. 取证与司法鉴定主体对象：计算机系统内与案件有关的数据信息

3. 计算机取证的层次功能：



表 1-1 计算机取证与司法鉴定的层次功能表

计算机取证与司法鉴定	证据层	溯源取证	同一取证	内容取证	刑事责任	
					行政责任	
		功能取证		复合取证		民事责任
	应用层	用户行为取证		手机数据取证		数据库取证
		计算机病毒与恶意代码取证	电子数据相似性取证		网络数据取证	电子文档与数据电文取证
	技术层	基础技术			主机证据保全、恢复和分析技术；网络数据捕获与分析、网络追踪技术；主动取证技术；密码分析与破解技术等	
		网络技术				
	工具集成运用					
	基础层	法律基础	规范标准		技术基础	案例研究

4. 反取证技术

def：反取证技术就是删除或隐藏证据使调查失效

分类：

- 数据擦除
- 数据隐藏
- 数据加密

典型工具：Runefs

5. 主动取证技术 (p5、23)

def：通过诱骗或攻击性手段获取犯罪证据

1. 典型技术---蜜罐（HoneyPot）技术--分类：
 - 产品型：用来降低网络安全风险，提供入侵监测能力

- 研究型：用来记录和研究入侵者的活动步骤、工具、方法
2. 边界进入技术以及信息获取技术（SQL注入、缓冲区溢出、自动脚本执行、弱配置和弱密码发现）
 3. 动态监听与日志保全技术（入侵取证系统，亦称“黑匣子”）
 4. 密码分析与破解技术

6. G8小组提出的关于取证与司法鉴定的6条原则

1. 必须用标准的取证与司法鉴定过程（用标准）
2. 获取证据时所采取的任何方式都不能改变原始证据（不更改）
3. 取证与司法鉴定人员必须经过专门培训（必培训）
4. 完整第记录证据的获取、访问、存储或传输的过程，并妥善保存（完整性）
5. 电子证据保管人员必须对在该证据上的任何行为负责（须负责）
6. 任何负责获取、访问、存储、传输电子证据的机构有责任遵循以上原则（循原则）

7. 计算机取证的4条基本原则（通用的取证与司法鉴定原则）

1. 依法取证
2. 无损取证
3. 全面取证
4. 及时取证（有些数据证据具有时效性）

【依法、无损、全面、及时】

8. 依法取证4要素（要保证取证与司法鉴定的四要素同时合法才能保证证据合法）

1. 主体合法（证据的提交者：合法的调查人员+合法的取证鉴定技术专家）
2. 对象合法（受攻击/被入侵的电子设备或计算机系统）
3. 手段合法（物理取证「手工直接取证」+工具取证「通过特制工具取证」）
4. 过程合法（遵循取证与司法鉴定的规范 + 2个合法取证人员取证 + 完整性保护）

9. 计算机取证与司法鉴定技术主要分为两类：

- 主机与其他电子设备取证
- 网络取证

因此，分析取证与司法鉴定的模型也可以从这两类进行

10. （国外）取证与司法鉴定的过程模型【按上一点分两类】

- 主机与其他电子设备取证与分析鉴定系统模型【5种典型的取证过程模型】
 1. 基本过程模型（领航和奠基作用；取证过程粒度粗，没有把事件发生前的取证准备作为取证的阶段）
 2. 事件响应过程模型（“攻击预防阶段”概念的提出，成为专业取证方法区别于非专业的关键步骤）
 3. 法律执行过程模型（美国司法部-DOJ提出，侧重于物理犯罪取证（非数字取证），对系统分析涉及少）
 4. 过程抽象模型（里程碑作用，分两类）：
 - AIRFORCE过程抽象模型（美国空军提出，抽象出通用取证过程共性，真正扩展到数字取证，进一步奠定基础、迈上新台阶）

- DOJ过程抽象模型（美国司法部DOJ提出，又一次发展，真正触及了数字取证的核心）

5. 其他过程模型（第一个大规模的研究数字取证理论的联盟组织——数字取证研究组Digital Forensics Research Workshop, DFRW, 规范取证理论）

● 网络取证与分析系统模型

- 网络取证主要对 **网络流量、审计迹、主机系统日志** 等实时监控和分析，目前研究更强调 **对网络的动态信息收集 和 网络安全的主动防御**
- 基于模糊专家系统的网络取证系统 流程图：

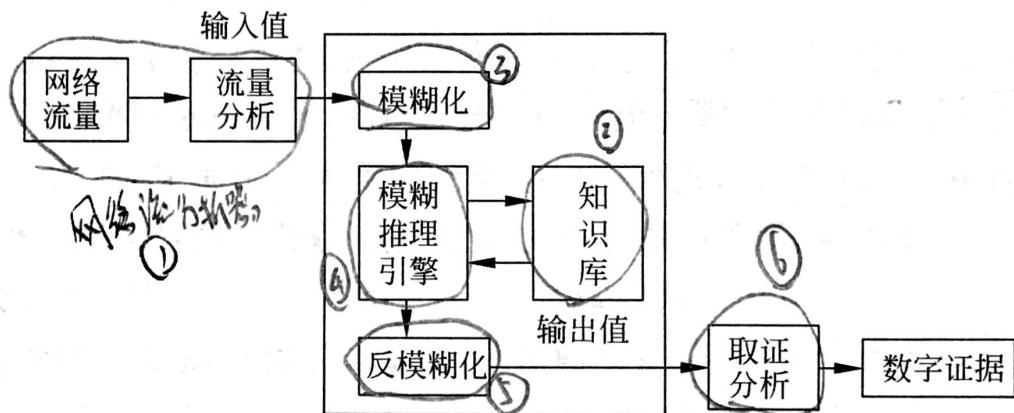


图 1-1 基于模糊专家系统的网络取证系统流程图

- 6个部分组成：网络流分析器、知识库、模糊化、模糊推理引擎、反模糊化、取证分析器

11. 取证与司法鉴定过程模型（通用模型，考试应该考这个不考上面的）

计算机取证与司法鉴定的模型包括法律方案的制订和技术方案的制订，实际进行计算机取证与司法鉴定的时候大都把两者融合在一起，制订详细的计算机取证与司法鉴定计划，它们与计算机取证与司法鉴定的法律基础、技术基础以及具体计划的开展和实施一起，形成了本书提出的计算机取证与司法鉴定的模型流程，如图 1-2 所示。

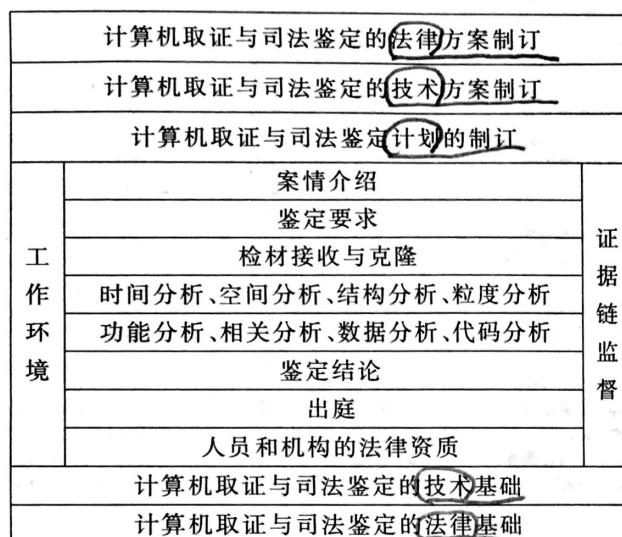


图 1-2 计算机取证与司法鉴定的模型流程

12. 取证与司法鉴定中的分析鉴定作为核心环节通常需要实施以下方案：

计算机取证与司法鉴定中的分析鉴定作为核心环节通常需要实施以下方案。

- (1) 注意弄清案件的组成和相互关系。
- (2) 注意弄清当事人的动机、手段。
- (3) 把调查区分优先次序。
- (4) 查找隐藏的电子数字证据。
- (5) 确定另外的证据。
- (6) 发现线索。
- (7) 注意法庭上提交诉讼案的需要。
- (8) 预测当事人行为并评估其行为潜力的需要等。

13. 取证与司法鉴定计划的制定

1. 空间分析

- 由于网络的特点导致证据的分布性（分散性，不仅在PC上，还在网络流量中），要将涉案的证据进行融合推理分析，推理分析的基础理论是：Locard交换原理，即当任两个物体相互接触时，就会产生交叉转移（核心原则就是，实施犯罪必有蛛丝马迹。感觉是p话）

2. 功能分析

- 理解证据的作用、了解作案意图动机，评估数字证据的可靠性和含义

3. 时间分析

- 确定某一时段事态的证据，识别时间的顺序和事件的即时性（创建、修改、最后一次访问时间——时间戳）

4. 结构分析和粒度分析

- 结构和粒度越大，分析越简单，反之则越需要技术和设备

5. 数据分析和代码分析

- 扫描文件类型，对比各类文件特征，注意隐藏和改变属性存储的文件、系统日志、注册表、上网记录、删除的数据、文件碎片

14. 取证和司法鉴定的工作环境和证据链监督

- 工作环境：远离磁场、高温、灰尘、积压、潮湿、腐蚀性化学试剂，防窃、防病毒、防消磁，用正版合法取证软件和存储软件
- 证据链监督：
 - 证据的移交、保管、开封、拆卸必须由司法人员+保管人员共同完成
 - 真实性、完整性
 - 校验技术用于证据链监督、认证
 - 时间戳技术用于对电子数据登记并提供注册后的时间信息

15. 计算机取证的操作程序规则（6条）

1. 受理案件
2. 保护涉案现场（首要之事——冻结现场计算机系统，保护当前状态）
3. 收集电子证据

4. 固定与保管电子证据
5. 分析电子证据
6. 归档电子证据

16. 计算机证据的 显示与质证

- 证据显示（展示、再现、先悉）：庭审调查前在双方当事人之间获取涉案信息、证据交换
- 质证：在庭审过程中由案件当事人就法庭上所出示的证据采取辨认、质疑、说明、辩论等心事进行对质核实，以确认证据的证明力

Chapter 2: 取证与司法鉴定的相关法学问题（这一章没有在老师的提纲里，应该不做重点）

1. 取证与司法鉴定 的主要任务：

- 通过对数据、软件、程序功能以及对电子证据进行的 提取、检查、分析、鉴定，以此对电子证据的真伪、因果、种属、完整性给出鉴定意见

2. 取证与司法鉴定 的主要内容：

- 来源取证（确定数据来源，IP、MAC、email...）
- 同一取证（确定两份电子文档是否一致）
- 内容取证（文档内容真实性、隐藏数据、加密数据...）
- 功能取证（软件功能、特征）
- 损失取证（涉案资产损失评估，有形资产、无形资产）
- 复合取证（其他的特殊取证，软件知识产权取证、计算机会计取证...）

3. 取证与司法鉴定 的3大技术基础

- 只读技术
- 克隆技术
- 校验技术

4. 取证与司法鉴定 相关事项

1. 认定信息的 存在性
2. 认定信息的 量
3. 认定信息的 同一性和相似性
4. 认定信息的 来源
5. 认定程序的 功能
6. 认定程序的 同一性和相似性
7. 重构事件

5. 司法鉴定的 8大原则

1. 合法
2. 科学
3. 客观
4. 独立
5. 监督

6. 保密
7. 时限
8. 公平、公正、公开

6. 司法鉴定的方法

1. 同一认定
2. 种属认定
3. 因果认定

7. 司法鉴定的程序

1. 司法鉴定的申请
2. 司法鉴定的决定
3. 司法鉴定的委托
4. 司法鉴定的实施
5. 鉴定意见的出具
6. 鉴定人出庭
7. 鉴定意见的质证
8. 鉴定意见的认证

Chapter 3: 取证与司法鉴定基础知识

1. 仪器设备配置原则

1. 预检工作（拍照、录像、通电测试，记录检材受理前的各种真实状态和电器属性）
2. 检材接受（正式受理后对检材进行 Hash校验并封存Hash值）
3. 检材克隆（位对位克隆、Hash值比对，确保副本和原检材的一致性）
4. 数据分析（多形式、多手段、多层次粒度分析数据）
5. 提取固定、鉴定结论、出庭质询（提取并固定有价值证据，形成鉴定结论，做好出庭质询的准备）
6. 工作环境、证据链监督、仪器设备的评测准入（是计算机取证与司法鉴定过程控制与质量管理的具体体现）

2. 取证的 8类 必备设备

1. 照相机+摄像机
2. 只读接口
3. 数据克隆工具
4. 校验码计算工具
5. 电子数据校验专用计算机
6. 综合性电子数据恢复、搜索、分析软件
7. 电子物证存储柜
8. 其他必要工具（转接口、数据线等）

3. 取证的选配设备（按照取证与司法鉴定的类别层次分3类）

1. 技术支撑设备
 - 密码破解系统
 - 专业数据恢复工具

- 磁盘阵列重组设备
- 海量数据存储系统

2. 应用支撑设备

- 即时通信 综合取证分析工具
- 病毒及恶意代码 综合分析工具
- 电子文档与数据电文 综合分析工具
- 数据比较工具
- 现场取证工具
- 在线取证工具
- 手机数据提取、恢复、分析工具
- Mac/Linux系统检验工具

3. 其他工具设备

- 数据销毁设备
- 存储介质修复工具
- 工业超净间
- 电焊台
- 磁力显微镜
- 录音笔
- 扫描仪
- 路由器
- ...

表 3-1 计算机取证与司法鉴定机构仪器设备配置标准

03 计算机取证与 司法鉴定	1 2 3 4 5 6 7 8 密码破解系统 专业数据恢复工具 磁盘阵列重组设备 海量数据存储系统 即时通信综合取证分析工具 病毒及恶意代码综合分析工具 电子文档与数据电文综合分析工具 数据比较工具 现场取证工具 在线取证工具 手机数据提取、恢复、分析工具 MAC/Linux 系统检验工具	照相机	1 台	必备	电子数据检验系统须 配备防范计算机病毒 等恶意代码及网络入 侵的措施
		摄像机	1 台	必备	
		只读接口	3 套	必备	
		数据克隆工具	1 套	必备	
		校验码计算工具	1 套	必备	
		电子数据检验专用计算机	2 台	必备	
		综合性电子数据恢复、搜索、分析软件	1 套	必备	
		电子物证存储柜	1 套	必备	
		其他必备工具	1 套	必备	
		密码破解系统	1 套	选配	
		专业数据恢复工具	1 套	选配	
		磁盘阵列重组设备	1 套	选配	
		海量数据存储系统	1 套	选配	
		即时通信综合取证分析工具	1 套	选配	
		病毒及恶意代码综合分析工具	1 套	选配	
		电子文档与数据电文综合分析工具	1 套	选配	
		数据比较工具	1 套	选配	
		现场取证工具	1 套	选配	
		在线取证工具	1 套	选配	
		手机数据提取、恢复、分析工具	1 套	选配	
		MAC/Linux 系统检验工具	1 套	选配	

4. 取证准备阶段的 4 个主要工作

1. 明确案例调查对象（企业高管、企业组织律师、企业HR、企业技术部门）
2. 尽早明确取证目标（硬件和其他证据（各种电子设备）、计算机设备内的所有数据（内存、磁盘）、计算机设备内的所需数据（email）、网络中的数据）
3. 根据实际情况准备取证工具及设备（取证的各种软件、硬件）
4. 审查响应计划中取证需遵循的程序和步骤，依据实际情况做调整

5. 计算机证据的保全主要是解决证据的完整性

- 因为计算机证据易修改、易损毁，必须确保完整性
- 时间戳也是重要技术，证明证据的时间信息和在此时间内不曾修改

6. 计算机证据分析的主要内容（6步）【证据分析是取证的核心和关键】

1. 分析硬盘的分区表
2. 浏览文件系统的目录树并打印
3. 关键词搜索
4. 用数据恢复工具找回删除文件
5. 用专门工具检查文件系统中未分配空间和闲散空间以寻找残留数据
6. 备份证据，制作可读性文件

Chapter 4: Windows系统取证与分析

1. Win 现场取证的固定证据有哪些（3个）【感觉老师这说法不对。, 。应该是需要固定的证据有哪些】

1. 固定硬盘（位对位克隆硬盘，ENCASE工具）
2. 部分文件的固定
3. 固定易丢失的证据

2. Win 现场取证固定易丢失证据有哪些（6个）【应该是需要固定的易丢失的证据有哪些】

1. 系统时间和日期
2. 最近运行的进程列表
3. 最近打开的套接字列表
4. 打开的套接字上进行监听的应用程序
5. 当前登陆的用户列表
6. 当前/最近与系统建立连接的系统列表

3. Win 现场取证，现场数据收集的基本过程（4点）

1. 打开一个可信的命令解释程序
2. 数据收集系统的准备（不能将数据写回被入侵机器的硬盘，要写到取证用的移动硬盘）
3. 收集易失性证据（用各种初始响应工具收集，cmd、pslist、fport、netcat、netstat）
4. 编写初始响应脚本（自动化运行各种初始响应工具）

补充，各种初始响应工具作用：

对 Windows 系统进行初始响应之前,首先应该创建初始响应工具包,目前在 Windows 上常用的初始响应工具有如下几种。

- (1) cmd. exe: Windows NT 和 Windows 2000 的命令行工具。
- (2) loggedon. exe: 用于显示所有本地和远程连接用户的工具。
- (3) pslist. exe: 用于列出在目标系统上正在运行的所有进程的工具。
- (4) netstat. exe: 用于列出所有监听端口和在那些端口上的所有当前连接的内置系统工具。
- (5) arp. exe: 系统内置工具用于显示最后一分钟内与目标系统进行通信的系统的 MAC 地址。
- (6) nbtstat. exe: 用于列出最近 10 分钟内的 NetBIOS 连接的内置系统工具。
- (7) fport. exe: 用于列出在 Windows 系统上打开着的任何 TCP/IP 端口的所有进程的工具。
- (8) MD5sum. exe: 用于为一个给定的文件创建 MD5 散列的工具。
- (9) doskey. exe: 为打开的 cmd. exe 命令行程序显示其命令历史的系统内置工具。
- (10) netcat. exe: 用于在两个不同的系统之间创建一个通信信道的工具。

对 Windows 系统进行深入初始响应之前,首先应该创建深入初始响应工具包,目前在 Windows 上常用的深入初始响应工具有以下几种。

- (1) auditpol: 用于确定系统的审核策略的 NT 资源工具箱(NTRK)命令行工具。
- (2) reg: 用于存储 Windows 注册表特定信息的 NTRK 命令行工具。
- (3) regdump: 用于将注册表转储为文本文件的 NTRK 命令行工具。
- (4) pwdump: 用于转储 SAM 数据库以便破解密码的工具。
- (5) ntlast: 用于监视系统中成功的和失败的登录的工具。
- (6) sfind: 用于检测 NTFS 文件流中隐藏的文件的工具。
- (7) afind: 用于搜索文件系统在确定特定时间范围内对文件的访问的工具。
- (8) dumpel: 用于转储 Windows 事件日志的 NTRK 命令行工具。

4. Win 两个关键的证据来源

1. 事件日志
2. 注册表

5. Win 深入获取证据的途径 (4点)

1. 事件日志 (Win日志文件: 系统日志、安全日志、应用程序日志) 【工具: ntlast、Win事件查看器】
2. 注册表 (存储了大量在初始响应期间的重要数据) 【reg、regdump】
3. 系统密码 (SAM文件是Win NT的用户账户数据库, 所有NT用户的登录名和口令等相关信息都存放在此, 口令会被加密) 【pwddump、findpass、LC5】
4. 转储系统RAM (保存内存数据) 【dumpit】

6. Win 电子证据的获取 (7大块)

1. 日志
 - 系统日志 (Win系统维护3个相互独立的日志文件: 系统日志、安全日志、应用程序日志)
 - 服务程序日志 (Windows Internet Information Services - IIS服务)
 - 防火墙、入侵检测系统日志 (分析数据报: 端口、协议等)

2. 文件和目录

- 启动目录（把想要自启动的程序的文件或快捷方式放在启动目录文件夹里就好了）
 - C:\documents and settings\用户名\开始菜单\程序\启动
 - C:\documents and settings\all users\开始菜单\程序\启动
- 系统目录（存放操作系统主要文件，直接影响系统能否正常工作）
 - 我的文档
 - 最近打开的文档
 - 删除文件的恢复

3. 注册表

- 启动项（检查工具AutoRuns）
- 用户信息项（用户名、用户所属组织、产品ID等）
- 系统信息项（注册表查询工具reg，自带的）

4. 进程列表

- 系统进程（包括基本系统进程（必备，一般无法强制结束）、附加进程（非必需））
- 用户进程（一般指用户安装的应用程序进程）
- 开始运行处进程（启动时自运行的进程）【用自带的 services.msc 查看服务进程】
- 进程分析（进程操作文件、注册表、访问网络的情况）【工具 pslist、fport、netstat】

5. 网络轨迹

- 网站访问下拉列表
- 网站访问的历史记录
- 网站收藏夹

6. 系统服务

- 计划任务服务（工具 at命令 可创建、安排、查看计划任务）
- 共享服务（网络共享文件夹）
- 远程控制和远程访问服务（常用远程控制软件：PCAnywhere、Radmin、TerminalService）

7. 用户分析

- 用户列表（系统中有哪些用户，默认的两个账户：Administrator、Guest）
- 用户属性（属于哪个组，权限如何）
- 用户相关的文档（所有权等）

7. 常用Win 取证工具

1. EnCase（广泛使用的取证与司法鉴定工具）
2. MD5sums（MD5校验值计算工具）
3. pslist（进程工具）
4. AutoRuns（注册表工具）
5. fport（网络查看工具，查看系统进程与端口关联）
6. netstat（网络查看工具，各种网络连接信息）
7. psservice（服务管理工具）

8. 现场取证和脱机取证（p113 小结里）

- 现场取证：除了取硬盘、文件目录，更多的是取易失性数据，此外还需取注册表、日志、系统密

码等数据

- 脱机取证：对现场取证时取下的硬盘进行进一步取证，一般对注册表、进程、服务、文件和目录、日志文件、网络轨迹等进行取证，形成文件，并固定

Chapter 5: Unix/Linux 取证与分析

0. Unix/Linux 系统概要

- Unix/Linux系统主要由3部分组成：内核（Kernel）、Shell、文件系统
- Unix/Linux 文件目录及功能：

表 5-1 UNIX 文件系统的目录及其功能

目 录 名 称	功 能
/	文件系统的根目录,超级用户的主目录
✓ /bin	存放最常用的基本用户程序
✓ /home	存放所有用户私有目录
✓ /mnt	用于安装可移动媒介
✓ /dev	硬件设备文件
/dev/dsk	磁盘设备文件
/usr	用户相关目录
/usr/bin	用户命令
/usr/etc	系统维护命令
/usr/lib	标准 UNIX 程序的支持文件
/usr/local	应用程序安装目录
/usr/local/bin	本地可执行文件目录
/usr/users	用户目录
/usr/x	X-Windows 系统支持工具
/usr/x/bin	X-Windows 系统执行文件
✓ /tmp	临时文件
/sbin	管理命令,维护程序
✓ /etc	关键的启动文件和配置文件
/opt	附加应用软件包的根目录
✓ /var	可变数据信息,如日志
/var/adm	记账文件、资源使用记录
✓ /proc	内存映射,包含系统进程

1. Unix/Linux 现场证据获取（Linux的现场证据有哪些？4点）

1. 屏幕信息

- 控制台下：setterm -dump 控制台编号；如果只想获取文字信息，直接用管道重定向保存就好
- X-Windows下：xwd、xwud截图工具，ScreenShooter、Ksnapshot等截图工具

2. 内存及硬盘信息

- 查看硬盘分区：fdisk -l、more /proc/partitions
- 挂载设备：mount 分区位置 挂载位置（mount /dev/sdb1 /mnt/usbhd1）
- 读取内存信息并转储到移动硬盘上：

- dd if=/dev/sdb1 of=/mnt/sdcard/data bs=1024(块大小, 单位是byte)
count=1024 (块数)
- 用nc将信息输出到另外一台pc, nc建立监听:
 - nc -l (启动监听) -p (指定监听端口) 10015 (指定的端口) > collect.mem.img (接受数据的文件) & (后台运行)
 - 参考[Linux 中的 &](#)、[linux - netcat网络工具-nc](#)

3. 进程信息

- who命令: 查看当前登录的用户情况。
- w命令: 该命令也用于显示登录到系统的用户情况,但是与who不同的是,w命令功能更加强大, 它不但可以显示哪些用户登录到系统,还可以显示出这些用户当前正在进行的工作,w命令是who命令的一个增强版。
- ps命令: 进程查看命令, 可以查看正在运行的进程及运行的状态、进程是否结束、进程有没有僵死、哪些进程占用了过多的资源等。ps 命令还可以监控后台进程的工作情况,因为后台进程是不和屏幕键盘这些标准输入/输出设备进行通信的,如果需要检测其情况,可以使用ps命令。
- top命令: 和ps命令的基本作用是相同的,显示系统当前的进程及其状态,但是top命令是一个动态显示过程,可以通过用户按键来不断刷新当前状态。如果在前台执行top命令, 它将独占前台, 直到用户终止该程序为止
- 参考: [w和who命令详解](#)、[ps与top命令](#)

4. 网络连接

netstat

- -a: 显示所有Socket, 包括正在监听的
- -c: 每隔1秒就重新显示一遍, 直到用户中断它
- -i: 显示所有网络接口的信息, 格式同"ipconfig -e"
- -n: 以网络IP地址代替名称, 显示出网络连接情况
- -r: 显示核心路由表。格式同"route -e""
- -t: 显示TCP协议的连接情况
- -u: 显示UDP协议的连接情况
- -v: 显示正在进行的工作

2. Unix/Linux 电子证据分析

1. 数据预处理

- 数据备份和分类, 尝试对硬盘数据进行部分恢复

2. 日志文件

- 系统日志: /etc/syslog.conf (缺乏认证模式, 易被篡改)

```

[root@localhost root]# cat /etc/syslog.conf
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
*kern.*                                     /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none      /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                    /var/log/secure

# Log all the mail messages in one place.
mail.*                                         -/var/log/maillog

# Log cron stuff
cron.*                                         /var/log/cron

# Everybody gets emergency messages
*.emerg                                         *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                  /var/log/spooler

# Save boot messages also to boot.log
local7.*                                         -/var/log/boot.log

```

图 5-6 /etc/syslog.conf 文件内容

(1) 消息类型是由“消息来源”和“关键状况”构成的，中间用点号连接。在图 5-6 中，news.crit 表示来自 news 的“关键”状况。在这里，news 是消息来源，crit 代表关键状况。通配符 * 可以代表一切消息来源。

紧急程度可以分成八大类，下面按重要性从大到下依次为紧急 emerg(emergency)、警报 alert、关键 crit(critical)、错误 err(error)、警告 warning、通知 notice、信息 info、调试 debug。消息来源分类如表 5-2 所示。

表 5-2 系统日志中的消息来源

名 称	来 源
auth	认证系统，如 login 或 su，即询问用户名和口令
cron	系统执行定时任务时发出的信息
daemon	某些系统的守护程序的 syslog
kern	内核信息
lpr	打印机信息
mail	处理邮件的守护进程发出的信息
mark	定时发送消息的时标程序
news	新闻组的守护进程的信息
user	本地用户的应用程序信息
uucp	uucp 子系统信息
*	表示所有可能的信息来源

- 子系统日志（连接时间日志、进程统计日志、错误日志）

Linux 系统一般有 3 个主要的日志子系统：连接时间日志、进程统计日志和错误日志。

(1) 连接时间日志。连接时间日志由多个程序执行，把记录写入到 /var/og/wtmp 和 /var/run/utmp。login 等程序更新 wtmp 和 utmp 文件，使系统管理员能够跟踪谁在何时登录到系统。连接时间日志也就是登录日志。

(2) 进程统计日志。进程统计日志由系统内核执行。当一个进程终止时，为每个进程往进程统计文件 (pacct 或 acct) 中写一个记录。进程统计的目的是为系统中的基本服务提供命令使用统计。

(3) 错误日志。错误日志由 syslogd 执行。各种系统守护进程、用户程序和内核通过 syslog 向文件 /var/og/messages 报告值得注意的事件。另外还有许多 UNIX 类程序创建日志，像 HTTP 和 FTP 这样提供网络服务的服务器也有详细的日志。

- 查看日志文件的命令

wtmp 和 utmp 文件都是二进制文件，它们不能被诸如 tail 之类的命令剪贴或合并（使用 cat 命令），需要使用 who、w、users、last 和 ac 等命令来使用这两个文件包含的信息。

(1) who 命令

who 命令查询 utmp 文件并报告当前登录的每个用户。who 的默认输出包括用户名、终端类型、登录日期及远程主机。

如果指明了 wtmp 文件名，则 who 命令查询所有以前的记录。命令 who/var/log/wtmp 将报告自从 wtmp 文件创建或删改以来的每一次登录。

(2) w 命令

w 命令查询 utmp 文件并显示当前系统中每个用户和它所运行的进程信息。

(3) users 命令

users 命令用单独的一行打印出当前登录的用户，每个显示的用户名对应一个登录会话。如果一个用户有不止一个登录会话，那他的用户名将显示相同的次数。

(4) last 命令

last 命令往回搜索 wtmp 来显示自从文件第一次创建以来登录过的用户。如果指明了用户，那么 last 只报告该用户的近期活动。

(5) ac 命令

ac 命令根据当前的 /var/log/wtmp 文件中的 登录进入和退出 来报告用户连接的时间（小时），如果不使用标志，则报告总的时间。该命令加参数 -d 可显示每天的总的连接时间。加参数 -p，则显示每个用户的总的连接时间。

(6) lastlog 命令

lastlog 文件在 每次有用户登录时 被查询。可以使用 lastlog 命令检查某特定用户上次登录的时间，并格式化输出上次登录日志 /var/log/lastlog 的内容。它根据 UID 排序显示登录名、端口号 (tty) 和上次登录时间。如果某用户从未登录过，lastlog 显示 ** Never logged in **。该命令需要使用 root 权限运行。

- 进程统计 (lastcomm 命令监测系统中任何时候执行的命令)
- 程序日志与其他 (su 命令日志 syslog、http 服务端 Apache 日志 access_log、error_log)

3. 其他信息源

- 账号信息 (/etc/passwd)
- 时间调度程序 (crontab 命令用于在一定时间间隔调度一些命令的执行，/etc/crontab，crontab -l 显示用户的 crontab 文件内容，注意其中的 run-parts)
- 内核转储文件 (用 file 命令显示内存转储文件来源及原因)

- /tmp (临时目录，是整个系统的缓冲区，会周期性自动清除)
- 隐藏文件和目录 (.folder 以点开头的文件是隐藏的)
- Shell (bash的历史文件 .bash_history)
- 信任关系 (/etc/hosts.equiv、rhosts文件)
- 非法文件 (目录中的可疑文件)

3. Unix/Linux取证与分析工具

- TCT
- Sleuthkit (TASK)
- Autopsy
- SMART

Chapter 6: 网络取证

1. 网络取证 定义、目的

- def: 指针对涉及民事、刑事、管理事件而进行的对网络数据流的研究
- 目的: 保护用户和资源, 防范由于持续膨胀的网络连接而产生的被非法利用、入侵以及其他犯罪行为
- 网络数据流def: 主机之间通过有线或无线方式进行的计算机网络通信
- 对于网络取证, 目前研究更强调 对网络的动态信息收集 和 网络安全的主动防御

2. 网络取证的 特点 (4点)

1. 主要研究对象与 数据报、网络数据流 有关, 不局限于计算机
2. 动态取证, 满足证据的 实时性、连续性, 可以重建入侵过程
3. 可分布式取证, 以满足证据的 完整性, 需部署多个取证点or取证代理, 且各取证点彼此相关联动
4. 需与 网络监控 相结合

3. 黑客攻击的一般步骤 (7步)

1. 信息收集
2. 践点
3. 查点
4. 探测弱点
5. 突破
6. 创建后门
7. 清除

4. 网络取证的重点环节 (5个)

1. 周界网络 (本地网的防火墙以外, 与外部公网相连的所有设备及连接)
2. 端到端 (攻击机-受害机 的连接)
3. 日志相关 (日志文件中 日期时间、来源、目的、协议)
4. 环境数据 (删除后仍然存在, 以及存在于 交换文件 和 slack空间 的数据)
5. 攻击现场 (重现攻击过程, 组织攻击逻辑顺序)

5. 两类 专用网络取证

- 与公网完全隔离的专用网络（具有物理边界，eg：公安网、军网、铁路网、特殊单位内网）【取证较为简单】
- 虚拟专用网络-VPN（在公网上建立专用的网络）【取证稍微复杂，设计隧道技术】加密技术、认证技术等】

6. 网络取证数据源

1. **防火墙和路由器**（时间日期、源+目的地IP、传输层协议（TCP、UDP、ICMP）、基本协议信息（端口号之类的）、NAT映射表）
2. **数据包嗅探器和协议分析器**（wireshark工具）
3. **入侵检测系统-IDS**（监视特定系统的现象和事件，仅监视与自身有关的网络通信）
4. **远程访问服务器**（VPN网关、调制解调服务器、SSH、Telnet等，提供了网络之间的连接）
5. **SEM软件**（Security Event Management-安全事件管理软件，自身不产生原始数据，从不同的网络通信数据源（防火墙日志、IDS日志等）导入安全事件信息并关联这些数据源的事件，然后从安全通道提取日志副本，并将其规范成标准格式，最后通过匹配ID、时间标记等特征来识别相关事件）
6. **网络取证分析工具**（Network Forensic Analysis Tools—NFAT，提供上述2、5等类似的功能，其主要功能如下）
 - 重放网络通信数据来重建事件
 - 可视化网络数据通信以及主机之间的联系
 - 建立典型入侵行为的模式及其可能的变化
 - 按关键字搜索应用层的内容
7. **其他来源**（蜜罐、DHCP服务器、网络监控软件、ISP记录、C/S程序、主机的网络配置和连接）

7. 网络通信数据的收集（2块，技术问题+法律问题）

● 技术问题

1. **关联分析技术**（用户名关联、密码关联、时间关联、关系人关联）
2. **关键字搜索技术**
3. **结构化数据搜索技术**（GREP语法，类似正则表达式匹配搜索）
4. **数据存储容量**（要准备充足的取证存储空间）
5. **加密数据通信**（IPSec、SSH、SSL、VPN或其他隧道技术，收集设备必须位于能看到解密网络活动的地方）
6. **服务运行在不明端口**（IDS、协议分析器依赖端口号来识别连接所用服务，故要能辨别不明端口）
7. **改变了进入点**（入侵者会绕开网络监控，如利用用户工作站的调制解调器/无线访问点，进入工作站，用工作站对用户主机发起攻击，故要对网络潜在的进入点加以限制，确保每个入口点都在监控之下）
8. **监控失效**（监控设备故障，故用冗余设备、多级监控来减小影响）
9. **时间问题**（要了解操作系统和文件的时间属性，构建正确事件时间线，杀毒软件自动扫描、取证软件都有可能改变原文件时间，因此需要注意；时间属性统称MAC时间）

● 法律问题

- 网络流量数据的收集会引起法律问题
- 注意隐私和安全问题
- 保护原始日志

- 保密问题

8. 网络通信数据的 检查与分析 (5块：辨认相关事件、检查数据源、得出结论、攻击者确认、对检查和分析的建议)

1. 辨认相关事件

- 识别事件的两个方法（企业内工作人员发现异常、分析人员例行安全检查）
- 常见的Web应用层攻击方式
 - 参数篡改攻击
 - 缓冲区溢出攻击
 - 篡改Cookies攻击
 - 命令植入攻击
 - 跨站脚本攻击
 - SQL注入攻击
- 查看Web服务器的记录是最直接有效的方法
- Web服务器SQL注入攻击的一般辨认步骤（3步）
 - 确定入侵时间
 - 从日志中找ASP木马
 - 确定入侵者提升权限的方式

2. 检查数据源

- 网络易失性数据的收集次序（根据其数据容易改变的程度排序）

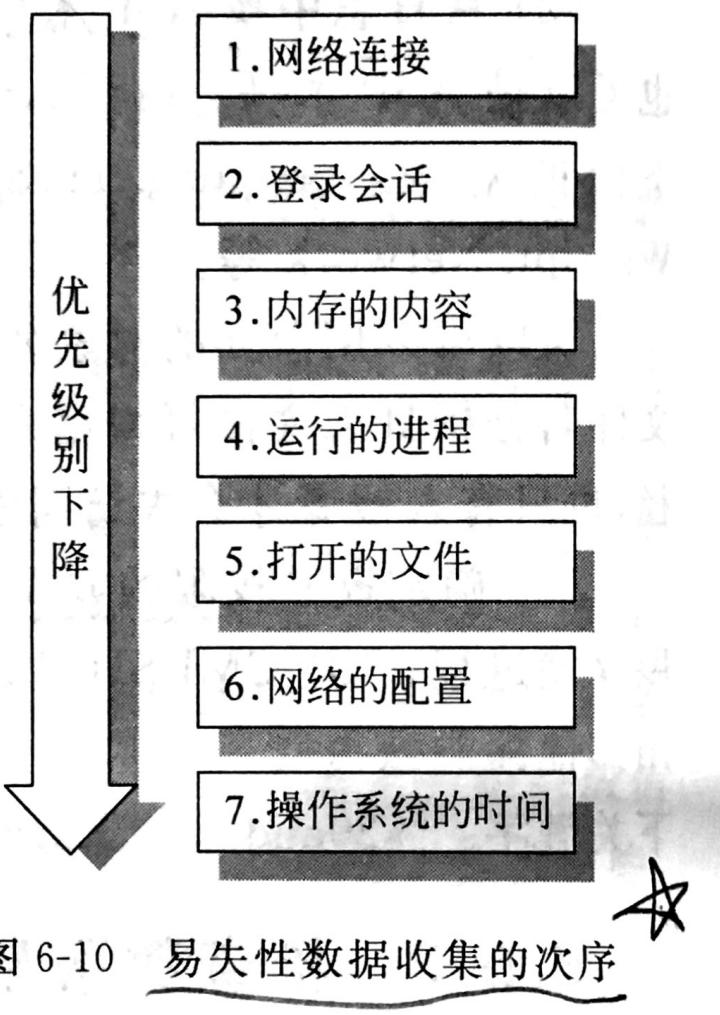


图 6-10 易失性数据收集的次序

- 除了主要的网络数据源，还要检查其他次要网络数据流的原因
 - 主要数据源可能没有数据
 - 主要数据源上的数据不充分 or 无法确认
 - 次要数据源可能有更重要的数据
- 数据源价值（不同数据源在不同情况下价值不同）
 - IDS软件（取决于IDS报警规则的有效性，误报信息价值就低）
 - SEM软件（取决于其导入的数据源的可靠性 以及 SEM的数据规范能力+事件关联能力）
 - NFAT软件（只有当其监控到相关事件时，才有价值）
 - 防火墙、路由器、代理服务器、远程访问服务器（通常这些数据源记录的事件信息少，缺少事件本质的数据，价值小；NAT映射表价值还挺大）
 - DHCP（记录了IP、MAC分配、时间戳，但可能伪造欺骗）
 - 数据包嗅探器（数据量大，作为补充数据，由协议分析器来解释数据）
 - 网络监控（当辨认与正常网络流有极大偏差的数据时 有用，如DDoS）
 - ISP记录（追踪攻击源，特别是使用了欺骗IP的攻击源，有用）
- 检测与分析工具
 - 针对不同情况选择不同工具
 - 用工具过滤数据
 - 人工审查数据不可行/能时，用工具自动化审查（如将日志载入数据库进行查询）
 - 用可视化工具，图表、网络图进行展示分析

3. 得出结论

在网络取证得出结论之前，要确保数据源符合6个条件：

- 1 规范化（相同事件可能有不同的名称or代码，要归一）
- 2 消除冲突（具有相同名称的事件可能有多个时间，因此可能会有重复判定）
- 3 排除假象（被误判成攻击事件的良性事件）
- 4 创建证据链和事件时间线（统一时间基准）
- 5 分析过程中不仅记录发现什么，更要记录如何发现的
- 6 用证据证明每一个假设

4. 攻击者确认

- 实施攻击涉及的IP问题
 - 假冒IP
 - 许多的源IP（DDoS，用大量错误IP迷惑）
 - IP的合法性（IP时动态分发的，攻击发生时的攻击IP可能之后时另外一个系统在使用；有些IP不是攻击机的，而是网络基础设施的）
- 证实可疑主机身份的5种方法
 - 1 联系IP地址所有者
 - 2 给IP地址发送网络通信（不应向一个明显正在攻击的IP发送信息，这样会被攻击者发现）
 - 寻求ISP帮助（设计法律问题，通常只有严重情况下，才找ISP）
 - 调查IP地址的历史
 - 在应用程序内容中寻找IP线索

5. 对检查和分析的建议（6点）

网络通信中数据使用的6点重要建议：

1. 有对设计隐私和敏感信息的管理策略
2. 提供充分的网络活动日志的存储容量
3. 优化配置数据源，加强信息收集能力
4. 分析人员具备综合的技术知识
5. 分析人员要考虑每个数据源的真实性和价值
6. 分析人员要关注事件的特征和影响

Chapter 7: 木马取证

1. 木马简介（定义、特性、种类）

- **def:** 指从网上下载的可以控制用户计算机的程序，其可以获取目标主机信息并取得控制权，本质上是一种远程控制工具，与一般的远控软件的区别是 **木马具有隐蔽性和非授权性**
- **特性：**
 - 隐蔽性
 - 非授权性
 - 自启动性
 - 自我保护性
 - 具有非法功能
- **种类：**

按功能分类（7类）

- 1 破坏型 (破坏系统、删文件、格式化硬盘、关闭网络连接)
- 2 密码型 (获取信息, 记录/破解密码)
- 3 键盘记录型
- 4 DoS攻击型 (依据攻击者旨意, 利用受害机对指定目标发起某种攻击)
- 5 代理型 (当作攻击的跳板)
- 6 FTP型 (为攻击者提供上传、下载功能)
- 7 自我保护型 (关闭目标主机中的查杀软件、防火墙等安全软件)

按网络连接分类 (2类)

- 主动连接型 (主动连接控制端, 流行)
- 被动连接型 (开放一个端口, 等待控制端连接, 易被发现, 不适用)

2. 木马的基本结构和原理

- 基本构成和原理:

- 一般由服务端程序 和 控制端程序 组成
- 中木马的受害PC 安装 服务端程序

- 木马的植入方式 (6种)

1. 邮件植入
2. IM植入 (Internet Messaging- 互联网即时通讯, 利用QQ等)
3. 下载植入 (网站下载木马、捆绑木马的程序)
4. 直接植入 (利用目标主机的漏洞植入)
5. 网页植入 (浏览网页的时候植入, 网页挂马)
6. 移动存储植入 (U盘)

- 木马的自启动方式 (8种)

1. 在 **Win.ini** 的 [Windows] 中添加启动命令
2. 在 **System.ini** 的 [boot] 中添加启动命令
3. 在 **注册表 RUN 项** 中添加
4. 在 **启动组** 中添加
5. 在 **文件关联** 中添加
6. 在 **其他应用程序** 中添加
7. 在 **系统服务** 中添加
8. **欺骗自启动**

- 木马的隐藏和 **Rootkit**

- 木马的隐藏分为

1. 木马文件的隐藏
2. 木马进程的隐藏 (简单的木马隐藏, 窗口隐藏)
3. 木马自启动的隐藏
4. 木马通讯的隐藏 (端口复用技术)

- 木马隐身的一般技术是 **Rootkit** (攻击者用来隐藏踪迹和保留访问权的程序)

- Rootkit通常通过改变操作系统的执行路径or直接修改操作系统维护的某些数据结构来达到隐藏目的
- 典型的 Rootkit 结构 (包括4部分) :

1. 以太网嗅探程序 (用于获取网络传输的用户名、密码)
2. 特洛伊木马程序 (提供后门)

3. 隐藏攻击者目录和进程 的程序 (改动 ps、netstat、ls、rshd等命令原始脚本)
4. 日志清理工具 (用 zap、zap2、z2等 删除 utmp、wtmp、lastlog中的日志痕迹)
5. 复杂的Rootkit 还提供 Telnet、Shell、Finger等服务
6. 其他的清理脚本 (清理 /var/log 、/var/adm)

- Rootkit分类

- 按照 **运行环境** 分2类:

1. **用户模式**Rootkit (改动操作系统二进制程序、挂钩、注入等方式)

2. **内核模式**Rootkit

- Linux下通过 可加载模块 实现, Win下通过 加载设备驱动程序 实现

- 特点: 无进程、无端口、难发现、难查杀、生存能力强

- 按照 **隐藏技术** 分2类:

1. 通过 **挂钩Hook** 来隐藏 (如 Hacker Defender)

2. 通过 **直接内核对象操作** 「Direct Kernel Object Manipulation - DKOM」 来隐藏 (如 FU Rootkit)

- 按照 **运行周期** 分2类:

1. **持续型**Rootkit (重启后自动加载执行, 留驻硬盘, 添加自启动项)

2. **基于内存的**Rootkit (不在硬盘中保留, 不自启动加载, 通过某漏洞加载, 只
 驻内存 —— 更难发现、取证)

- 木马的感染现象

通常没有明显迹象, 但也会用如下情况:

1. 浏览器自动打开某网站
2. 突然弹框
3. Win系统配置被改动
4. 硬盘繁忙、网络缓慢、鼠标屏幕异常
5. 系统速度变慢、资源占用多、任务表有未知程序运行
6. 发生死机、重启

- 木马的 检测

- 木马在计算机中的载体: 文件、启动项、网络通信
- 检测方式: 端口扫描、网络连接查看、注册表检查、文件搜索
- 工具: 手动检测、防病毒软件检测

3. 木马的 取证与分析 方法

1. 一般的 取证步骤 (如果问 win取证步骤、Linux取证步骤, 也回答这个, 可以额外配上 Chapter 1 - 15. 计算机取证的操作程序规则 (6条))

1. 发现证据 (定位主机)
2. 提取证据 (定位文件)
3. 存储证据
4. 分析证据 (功能分析、代码分析、来源分析)
5. 鉴定证据

2. 木马取证的步骤

1. 识别木马 (方法: IDS、防火墙、FTP、WWW、反病毒软件等日志异常检测, 木马发现工具
 查找识别)
2. 证据提取

3. 证据分析（动态、静态分析、网络数据分析、各种日志分析，目的->找出木马功能、作者、使用者）
3. 识别木马的方法（11点）
 1. 查看 **主机基本信息**（hostname、nbtstat -a \$(hostname)、net share）
 2. 查看 **开放端口**（netstat -an、fport、图形化工具Active Ports、IceSword、超级巡警、木马防线也可以查看端口）
 3. 查看 **系统配置**（win.ini 和 system.ini 文件，或可以使用 autoruns 和 msconfig 工具）
 4. 查看 **系统服务**（控制面板-计算机管理工具）
 5. 查看 **系统进程**（任务管理器）
 6. 查看 **进程加载的模块**（进程查看器、IceSword、ProcessExplorer）
 7. 查看 **启动程序**（注册表、启动文件夹）
 8. 查看 **注册表**
 9. 使用 **木马检测软件**（IceSword）
 10. 使用 **Rootkit检测工具**（Patchfinder、VICE、RootkitRevealer、F-Secure、Klister、SVV）

4. 木马证据的提取

- 动态提取/在线取证：进程、注册表、文件、网络端口、数据流，输出到文件并存储，MD5sum校验
- 静态提取/离线取证：FBI、EnCase、FTK（Forensic Tool Kit, 首选）、AccessData（处理加密过的压缩后的驱动器）【提供数据分析、检查能力】

5. 木马证据分析

- 分析目的：找出木马的功能、作者、使用者 + 各种时间信息
- 分析方式：
 1. 查看文件类型（PEiD、FileInfo）
 2. 查看文件结构（UltraEdit、Stud_PE）
 3. 反汇编（IDA、UltraEdit）
 4. 动态行为分析（6大分析工具）
 - 1 系统监视软件（ProcessMonitor、ProcessExplorer）
 - 2 注册表监视工具（regshot、regsnap）
 - 3 文件监视工具（Filemon）
 - 4 嗅探器（Etheal）
 - 5 系统分析工具（autoruns）
 - 6 API调用查询工具（APISpy）

4. 书上的案例看一下：PC-Share、灰鸽子、广外男生

提交报告

[案例信息]

时间：

地点：xxx

网络：IP:xxxx. xxxx. xxxx. xxxx

[文件信息]

文件及 md5

hacker. com. cn. exe

Server. exe

[系统状态信息]

隐藏进程

注册表

修改文件

启动服务

[分析结论]

综合以上分析，可以总结出该木马的性质，一个服务安装启动方式的木马程序，会使用进程注入技术（注入 iexplore. exe）穿透防火墙的网络连接控制，并带简单的 Rootkit 功能（隐藏其启动的 iexplore. exe 进程）。

Chapter 8: 手机取证

1. 手机取证3大难点：

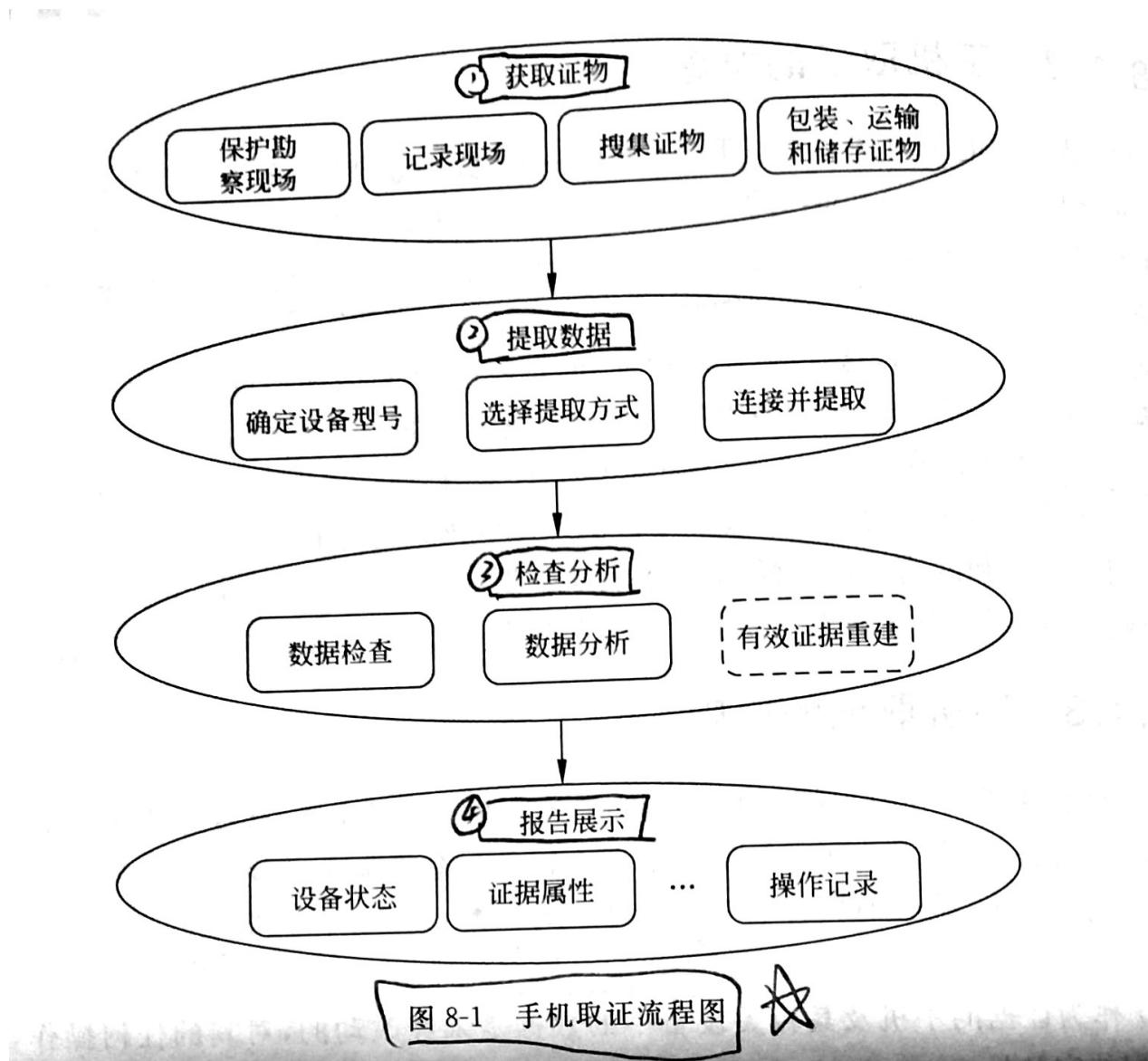
1. 犯罪用的手机、银行卡等作案工具没有实名登记
2. 取证难（手机、银行卡等易被销毁）
3. 破案成本高

2. 手机犯罪的3中行为：

1. 犯罪过程中，手机充当通讯工具
2. 手机用做犯罪证据的存储媒质
3. 手机用做短线诈骗/骚扰、病毒传播工具

3. 手机取证概述（def、证据来源、原则、流程）

- **def**: 在健全的取证环境中，用恰当手段从手机及相关设备中恢复出数据证据（取证环境健全、取证手段恰当 - 保证证据完整性和有效性）
- **证据来源**: 手机内存、SIM卡、闪存卡、移动运营商、短信提供商
- **手机取证4条原则**:
 1. 保证原始数据完整性，手机中的证据未经改动
 2. 有资格的专门取证人员进行取证操作，能解释取证行为
 3. 所有操作（证据的获得、访问、提取、存储、转换）都必须由第三方监理日志审计，并完全归档保存，以备质询
 4. 复杂操作和调查的人员/组织必须遵循上述原则并负责
- **手机取证的流程图**:



4. 手机取证基础知识（了解即可，设计一些移动通信的知识）

- 移动通信相关知识
 - 移动通信技术的发展：
 - 第一代移动通信系统- 蜂窝组网技术
 - 第二代 - GSM (Global System for Mobile Communications, 全球移动通信系统 - 全球通)
 - 第三代 数字通信系统- 3G (比前两代，多了 处理图片、视频流、音乐流)
 - GSM系统：

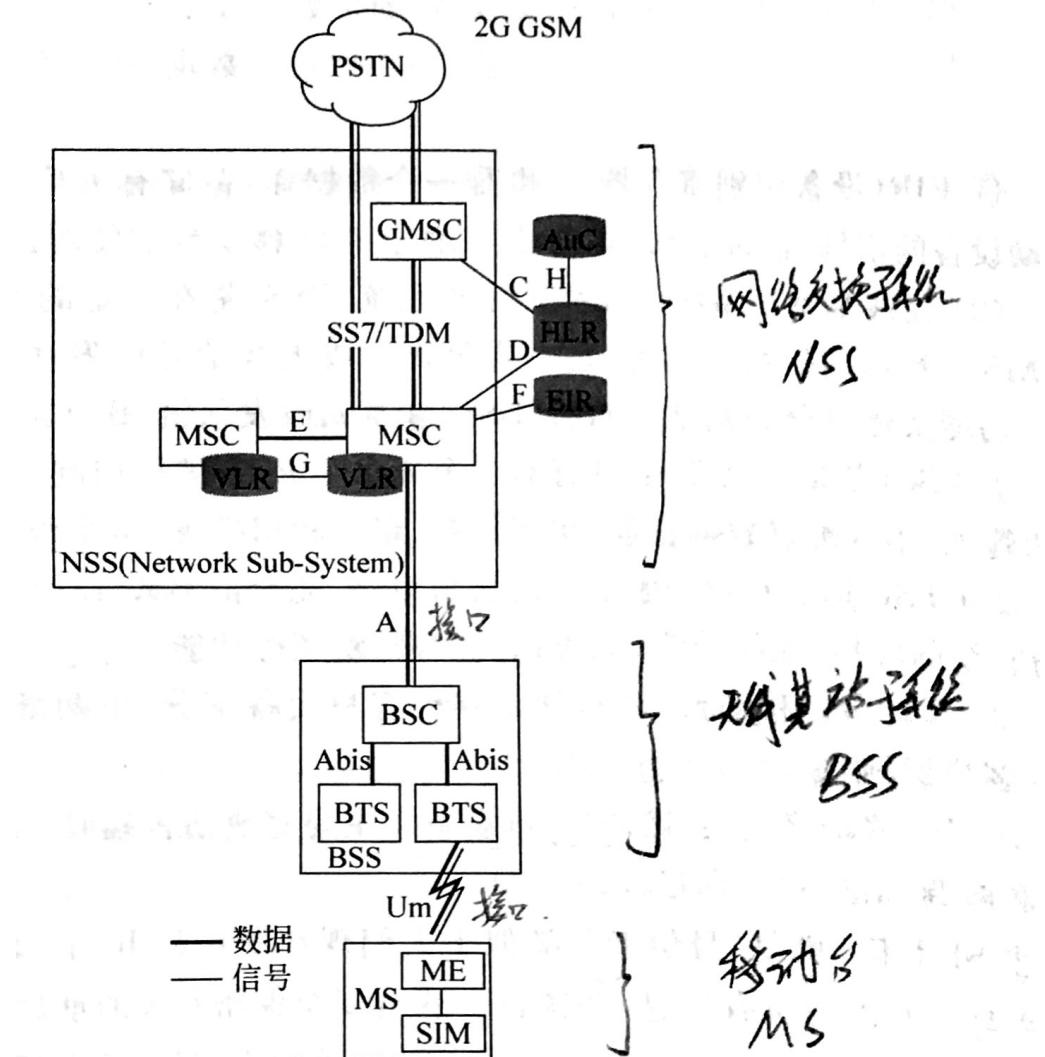


图 8-2 GSM 系统构成

- SIM卡相关知识

- SIM (Subscriber Identity Module, 客户识别模块) 卡：也称为智能卡、用户身份识别卡，存储与网络和客户有关的管理数据
- GSM网络系统下用SIM卡，CDMA网络系统用 USIM卡
- SIM密码分为 PIN码、PIN2码、PUK码、PUK2码：
 - PIN (PIN1) : SIM卡的个人识别码，4位，默认运营商提供，可以更改
 - PUK (PUK1) : 8位，运营商提供，不可更改，输错3次PIN时，SIM卡会被锁，用PUK解锁【PUK输错10次，SIM永久报废】
 - PIN2: 用于手机计费，锁了没太大影响
 - PUK2: PIN2输错3次，用PUK2解锁
- SIM卡数据：
 1. SIM卡生产厂商存入的系统原始数据（永久驻入，不可更改）
 2. 网络方面的数据（只允许网络运行部门查阅、更新）
 3. 用户数据（允许用户读写）
 4. 相关业务代码（PIN、PUK之类的）
- IMEI号

- International Mobile Equipment Identifier - 国际移动设备标识，全球唯一，移动厂商生产的手机进入市场所必备
- 拨号盘输入 *#06# 可查询、或者 手机设置里也可以找到

5. 手机取证与分析工具

1. 几种常用的手机取证工具：

表 8-1 几种常用的手机取证工具

工 具	CDMA	GSM	SIM
BITPIM	√	√	
Oxygen PM		√	
Mobiledit		√	√
✓ CellDEK	√	√	√
Device Seizure	√	√	√
GSM XRY	√	√	√
SIMTS			√
Forensic SIM			√
Forensic CR			√
SIMCon			√

2. 便携式手机取证箱 CellDEK
3. Micro Systemation 手机取证主导系统 —— XRY系统

6. 专业电子设备的取证与分析

- 专业电子设备的电子证据有哪些（10个）
 1. 自动应答设备
 2. 手持电子设备
 3. 网络设备
 4. 数码相机
 5. 打印机
 6. 扫描仪
 7. 复印机
 8. 传真机
 9. 读卡机
 10. 全球定位仪
- 专业电子设备取证的一般方法/流程（4点）：
 1. 确定取证目标，制定取证计划
 2. 发现和判别电子证据
 3. 记录现场，收集证据
 4. 分析鉴别，形成证据链

Chapter 9: 取证案例

1. 熊猫烧香

1. 鉴定要求

2. 鉴定环境
3. 检材克隆与md5校验
4. 鉴定过程
5. 鉴定结论

2. 软件侵权

1. 鉴定要求
2. 文件系统结构比对
3. 模块文件结构、数目、类型、属性对比
4. 数据库对比
5. 运行界面对比
6. MD5校验对比
7. 鉴定结论

更多资料/实验代码，请关注我的GitHub、CSDN【后续我会把在HDU-网安的实验报告、复习资料，上传】：

- <https://github.com/RGNil>
- https://blog.csdn.net/qq_41709370
- 动动小手，点个赞、关注、给个Star、fork，不要做白嫖党哦！！
- 你的鼓励，万分感激
- 如果想了解更多HDU-网安的事情，欢迎联系我（博客留言等方式）！！