数字取证技术(Digital Forensics Technology)笔记I

数字取证技术概述

👉**知识点(数字取证技术)** 数字取证是信息安全领域的一个重要分支,关注收集、分析、保存电子数据证据,用于法律诉讼程序.数字取证的基本步骤:

- 电子数据获取(Acquire):包括截获或解码解密数据(常用工具如Wireshark,Autopsy);
- 数据的鉴定,恢复和保护(Maintenance):包括修复损坏的数据或复制保护已有的数据(常用工具如Guymager,dd,Recuvan,PhotoRec,TestDisk,R-Studio,Runtime's GetDataBack,Ontrack EasyRecovery);
- 数据的分析(Analyze):应用数学或计算机算法更清晰地呈现数据的内涵(常用工具如c++,python,opencv,numpy,SageMath...);
- 数据的报告展示(Present):撰写报告使普通人能理解取证的客观结论(常用工具如Markdown);

▧**例子(数字取证技术的历史)** 不限于使用计算机取证的历史(Forensics Timeline):

- 1835年:Henry Goddard使用物理方法分析子弹和凶杀案的关联性(物理方法);
- 1836年:James Marsh设计了化学检测手段用于检测凶杀案中的砒霜成分(化学方法);
- 1930年:Karl Landsteiner因为血液鉴定分类方法获得了诺贝尔奖(生物方法);
- 1988年:国际计算机调查专家协会(International Association of Computer Investigative Specialists,IACIS)成立,标志着数字取证技术成为刑事调查的主流手段;

(♞**思考)** 计算机取证是否只能应对计算机领域的犯罪?请列举反例;

Linux基本知识

👉**知识点(grep)** 用于查找含有某个字段的文件(比如在文件夹"/home/doc"中迭代地查找含有"name"字段的文件):

```
$ grep -ri /home/doc "name"
```

👉**知识点(find)** 用于查找含有某个名字的文件(比如在文件夹"/home/code"中迭代地查找c++文件):

```
$ find /home/code -name *.cpp
```

👉**知识点(管道)** "管道"(pipe)是一种强大的功能,允许将一个命令的输出作为另一个命令的输入(比如在展示的进程里过滤出含"GameName"的进程):

```
$ ps -aux | grep "GameName"
```

(🐴**思考**) Linux的关机命令是什么,为什么不提倡直接关闭电源来关机;

(🐴**思考**) 作为系统管理员,需要定期检查位于/var/log/auth.log的系统认证日志文件,以识别所有失败的sudo尝试;编写一个管道命令,筛选出所有包含"sudo"和"失败"关键字的日志条目,并计算这类事件的总数;

```
$ grep "sudo" /var/log/auth.log | grep "失败" | wc -l
```

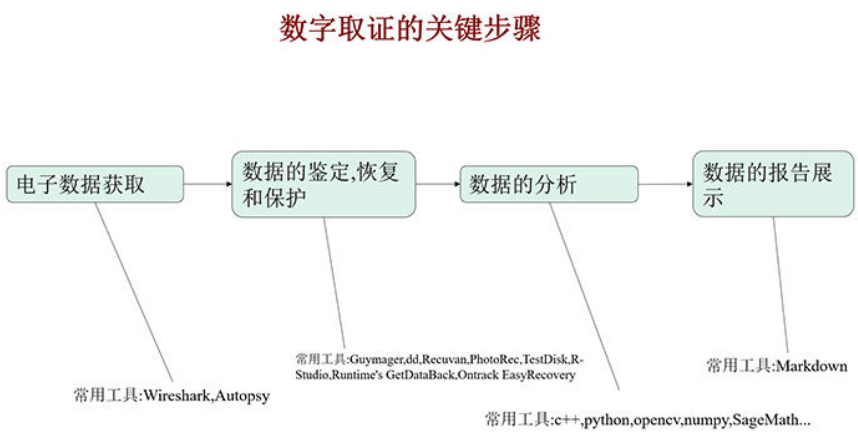
(🐴**思考**) 在一台运行Linux的服务器上,有一个位于/var/www/html目录下的大型网站,该目录包含数千个.php和.html文件;如何找出所有文件内容中包含字符串"deprecated"(表示使用了不推荐的代码)的文件,并将这些文件的完整路径和文件名输出到/home/user/deprecated-list.txt文件中;

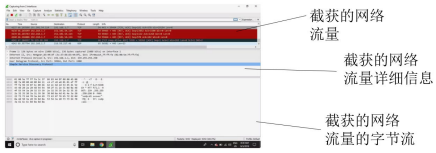
```
$ grep -rl "deprecated" /var/www/html/ --include=\*.{php,html} >
 /home/user/deprecated-list.txt
```

(🐴**思考**) 现在怀疑某个不明确的进程可能在不适当的时间进行网络连接,试图发送敏感数据;编写一个命令或脚本来监控和记录过去一小时内所有尝试通过TCP端口443(HTTPS)建立外部连接的进程名称和它们的PID,保留这些信息以供日后分析;

```
$ netstat -tunapl | awk '/:443/ {print $7}' | sort |
uniq -c | sort | tail -n +1
```

命令行使用netstat列出所有活动的连接,awk '/:443/ {print $7}'筛选出目标端口为443的连接,并打印出其进程ID和名称。然后通过排序和统计每个进程的连接数,显示了在过去一小时内尝试建立外部连接的独特进程(tail命令用于查看文件末尾内容,它通常与标准输入或文件相关联,并将其最后一部分输出到屏幕或其他设备上);





数字取证技术(Digital Forensics Technology)笔记II

数字取证技术:数据获取工具

👉**知识点(Wireshark)**:Wireshark是一种广泛使用的网络协议分析工具,它能够捕获和逐个显示经过网络接口的数据包.这使得Wireshark在排除网络问题、网络安全分析以及学习网络协议操作时成为一个极有价值的工具;

👉**知识点(Autopsy)**:Autopsy是一个开源的数字取证平台,用于进行硬盘和手机取证.它通过提供一个用户友好的图形界面,让用户能够快速有效地进行数据分析.Autopsy可以在多种操作系统上运行,包括Windows、Linux和macOS,虽然在Windows上使用得最为广泛.

👉**知识点(数据恢复原理)**:数据恢复技术的根本原理基于存储设备(如硬盘、SSD、USB驱动器、SD卡等)处理删除文件的方式.当文件被删除或存储设备被格式化时,大多数操作系统仅标记这些文件占据的空间为"可用"以供未来写入使用,并不立即物理上擦除文件数据.这意味着,直到新的数据覆盖(或部分覆盖)原有位置之前,原始数据在物理层面上仍然存在于存储介质上.数据恢复工具正是利用这一特性来恢复被删除的文件;

计算困难问题和加密方法

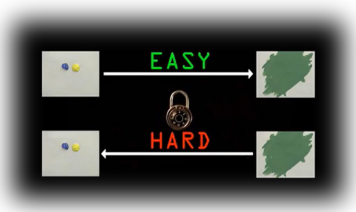
对于一个计算困难问题F,若设他的解为x^*,那么我们称x^*满足F;F的所有可能的解组成的空间称作解空间$\mathcal{X}$;计算困难问题F的求解过程即在解空间$\mathcal{X}$里面搜索x^*满足F,这一过程中要尽可能利用问题的特性来加速搜索;下面列举几个**例子**:

- 对于旅行商问题(TSP),解空间$\mathcal{X}$即为所有可行的路径组成的轨迹空间;
- 对于可满足性问题(SAT),解空间$\mathcal{X}$即为所有变元(假设数量为n)的真值空间$(T,F)^n$;
- 对于布尔方程组求解问题,解空间$\mathcal{X}$即为所有变元(假设数量为n)的布尔值空间$(0,1)^n$;

计算困难问题有个特点,验证某个可能的解$x \in \mathcal{X}$是否是计算困难问题F的解是容易的(验证是多项式级别的复杂度$\mathcal{O}(n^c)$,其中c是常数),但是找到计算困难问题F的解$x^* \in \mathcal{X}$是困难的(求解是超多项式级别的复杂度,比如指数复杂度$\mathcal{O}(c^n)$,其中c是常数);验证容易,可以用来设计加密解密算法,即加密算法的**有效性和高效性**,求解困难,则保证了**安全性**;

数字签名:RSA签名方案

👉**知识点(签名流程)**:非对称签名算法的签名和验证过程:



1. Alice用私钥d对消息M进行签名得到消息和签名(M,S);

2. Alice将消息和签名(M, S)发送给Bob;
3. Bob用公钥e对得到的消息和签名(M, S)进行验证(确认是Alice发送);

👉**知识点(RSA签名方案)**:非对称签名算法,它依赖于大整数的因数分解问题,签名和验证过程:

首先是密钥生成:

1. 随机选择两个大的质数p和q,且一般它们的位数相近,以确保安全性.
2. 计算p和q的乘积$n = p \cdot q$,n的长度(比特数)决定了密钥的长度.
3. 计算n的欧拉函数$\phi(n)$,对于质数p和q,$\phi(n) = (p-1) \cdot (q-1)$.
4. 选择一个整数e,作为公钥指数,它满足$1 < e < \phi(n)$且e与$\phi(n)$互质.常用的值有3或65537.
5. 计算e关于$\phi(n)$的模逆元d,即$d \cdot e \equiv 1 \mod \phi(n)$.
6. 生成的公钥为一个对(n, e),私钥为d.

然后是签名过程:假设明文为M,M是一个数字,且$0 \leq M < n$.使用发送方的私钥(n, d)将明文M签名为S:

$$S = M^d \mod n$$

签名后,将消息和签名(M, S)一并发送给接收方.验证过程:接收方已经得到了签名S,并拥有公钥e.使用公钥e来验证S是否对应消息明文M:

$$M = S^e \mod n$$

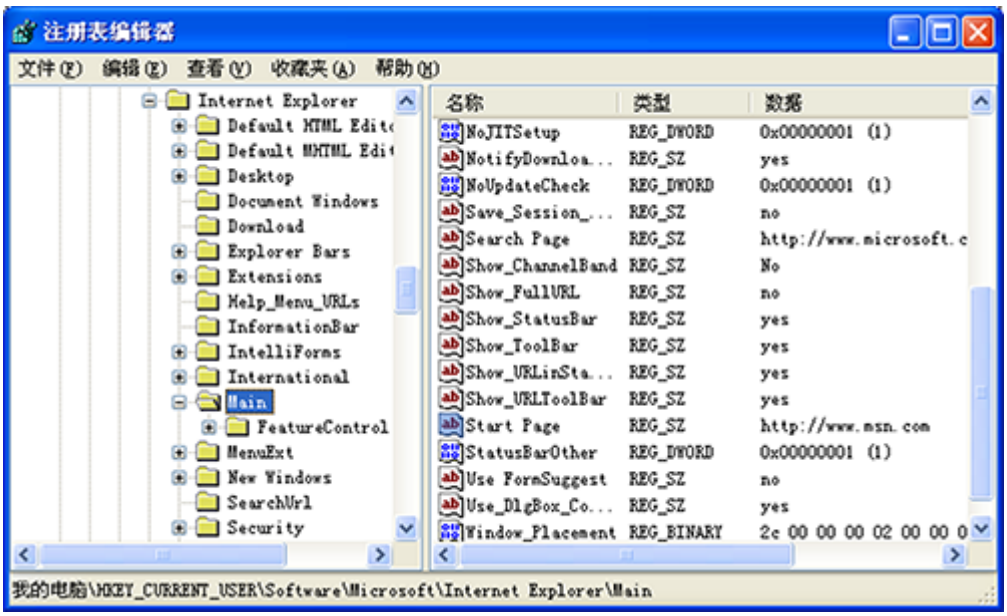
(✎**习题**):给出一个RSA签名方案的实例,里面的数字不需要很大,只需要表现RSA签名方案的工作原理即可;

(✎**习题**):列举5种以上的计算困难问题以及他们在密码学方法里的应用;

数字取证技术(Digital Forensics Technology)笔记III

Windows操作系统取证技术

👉**知识点(注册表的功能)**:Windows注册表是一个集中式分层数据库,每一个文件夹表示注册表中的项,项又包括子项和值项,项和子项的关系就像目录可以包含子目录一样.例子:查看用户的IE浏览器默认首页;

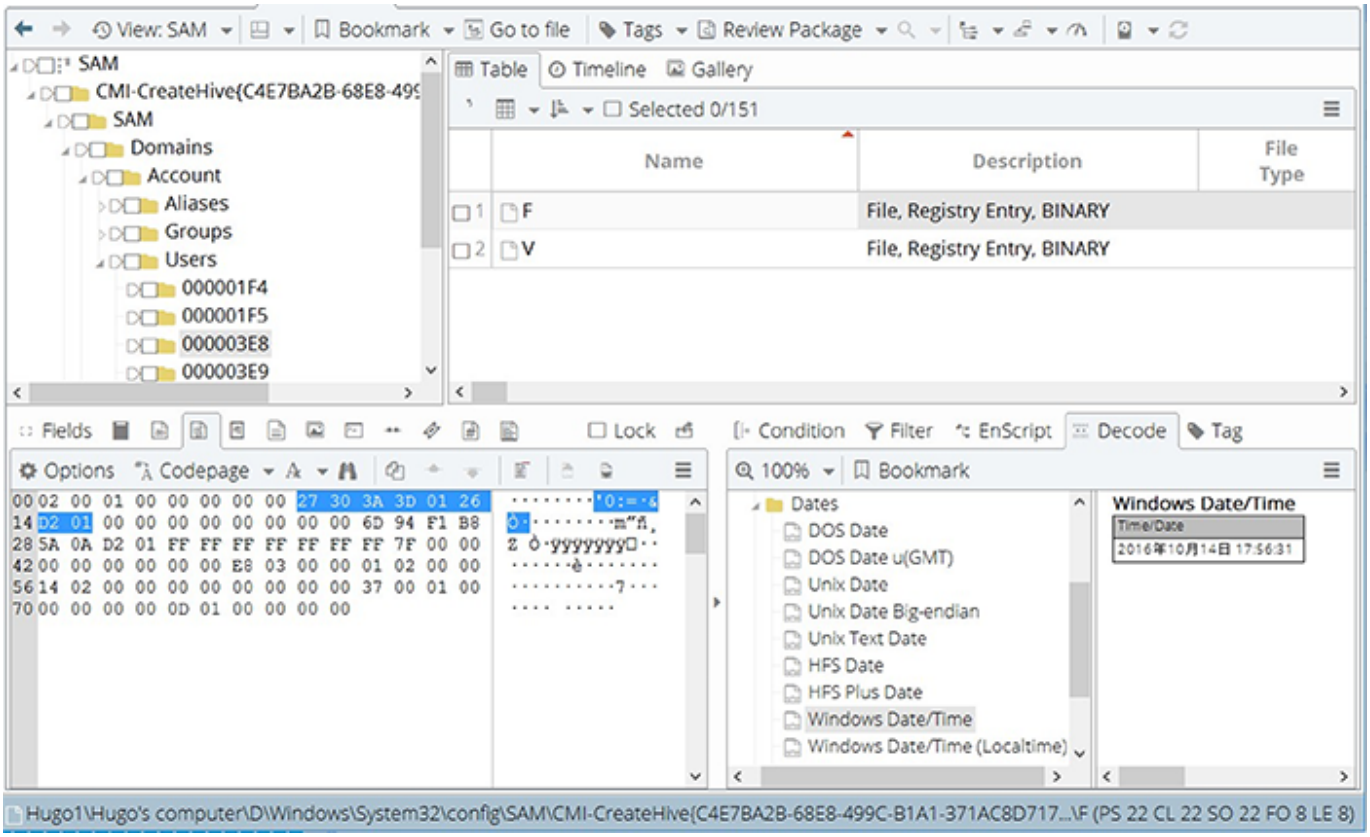


👉**知识点(Windows注册表核心文件)**:Windows注册表用于存储系统配置、用户设置和软件信息等.Windows系统中,注册表的核心由几个主要的文件组成,这些文件在系统中是隐藏的,存储在`%SystemRoot%\System32\config\`目录下.核心的注册表文件包括:

1. **SYSTEM**:存储了系统级的配置信息,如硬件设备、系统服务等.
2. **SOFTWARE**:包含了所有用户级软件和系统软件的设置.
3. **SAM**:存储了安全账户管理器信息,包括用户账户和安全描述符.
4. **SECURITY**:包含安全相关信息,例如安全策略和访问控制列表.

除了这些核心文件,还有一些其他重要的注册表文件:

- **DEFAULT**:包含了默认用户配置的注册表信息,适用于新用户的初始配置.
- **NTUSER.DAT**:位于每个用户的个人目录下(`%USERPROFILE%`),存储了特定用户的设置和配置.
- **USRCLASS.DAT**:存储了每个用户的类注册信息,也位于每个用户的个人目录下的`AppData\Local\Microsoft\Windows`目录中.



👉**知识点(Windows注册表的取证)**:主要的工具和技术:

1. **注册表编辑器(Registry Editor)**:Windows自带的注册表编辑器(regedit.exe)是最基本的工具之一.它允许用户浏览、编辑和导出注册表中的键值.虽然它主要用于系统管理和配置,但在取证工作中也可以用于快速查看注册表的内容.

2. **注册表取证工具**:如EnCase Forensic、Registry Recon、FTK Registry Viewer、X-Ways Forensics等.这些工具可以帮助分析人员以更有效的方式浏览、搜索、导出和分析注册表中的数据.提供了用户友好的界面和高级的分析功能,有助于取得更深入的证据.

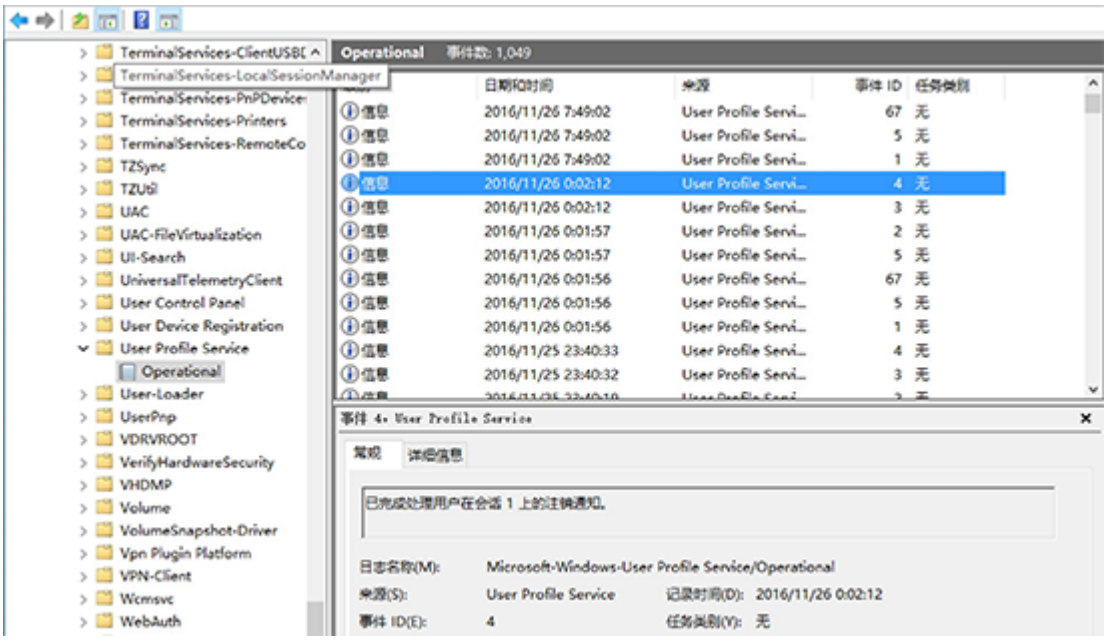
3. **取证镜像工具**:在进行注册表取证时,通常需要先获取系统的镜像.取证镜像工具如FTK Imager、EnCase、DD等可用于创建完整的磁盘镜像,包括注册表文件和其他系统文件,以确保数据的完整性和可靠性.

4. **数据恢复工具**:注册表文件可能已损坏或被删除.数据恢复工具如Recuva、R-Studio等可用于尝试恢复已删除或损坏的注册表文件,从而帮助还原重要的取证数据.

5. **静态和动态分析技术**:在进行注册表取证时,可以采用静态和动态分析技术.静态分析涉及对注册表文件的离线分析,而动态分析则涉及在运行时监视系统的注册表活动.这两种方法可以结合使用,以获取更全面的证据.

👉**知识点(Windows事件日志取证)**:Windows事件日志提供了丰富的数据,可用于取证分析,特别是在监测和记录用户行为,如登录、插拔移动设备以及修改系统时间等方面.主要工具和方法:

- **Event Viewer (事件查看器)**:Windows自带的Event Viewer是最基础的工具,允许用户查看和搜索本地计算机的事件日志.可以查看安全日志来跟踪用户登录和注销活动,系统日志和应用程序日志也可提供关于设备事件和系统时间更改的信息.
- **LogParser**:Microsoft提供的强大工具,能以SQL风格查询日志数据,非常适用于从大量日志数据中快速提取信息.可用于分析各种类型的日志文件,包括Windows事件日志.
- **Windows Sysinternals**:提供了一系列强大的工具,如Process Monitor,可以实时监控Windows进程和线程的活动,包括对事件日志的访问.
- **用户登录行为**:Windows用户登录/注销的事件日志中的事件ID 1到5;可查看登录尝试的详细信息,包括用户名、登录类型、登录时间和登录源.对这些事件进行监控和分析可以帮助识别未授权的登录尝试或其它可疑活动.
- **用户插拔移动设备行为**:事件ID 20001或20003(关于即插即用设备的事件)可用于跟踪USB设备的插拔活动.审计这些事件可以帮助识别潜在的数据泄露或非法访问尝试.
- **用户修改系统时间的行为**:事件ID 4616(系统时间被更改)记录了系统时间的更改.分析这类事件可以帮助确定是否有企图隐藏或伪造其他安全事件的行为.
- **用户无线网络接入的行为**:在WLAN-AutoConfig和NetworkProfile日志文件中有相关信息,事件ID 10001(网络接入/断开).



👉**知识点(磁盘与文件)**:磁盘存储和文件系统是计算机系统中核心的组成部分,它们负责管理和存储文件及目录的方式.不同的文件系统具有不同的特点、设计理念以及优缺点:

- FAT(File Allocation Table)

    - **特点**:FAT文件系统是最早广泛使用的文件系统之一,它简单且与多种操作系统兼容.文件存储在磁盘上时使用一个分配表来记录文件的位置.
    - **设计思维**:设计上追求简单和跨平台兼容性,易于实现和维护.适用于小容量存储设备,如早期的个人计算机和移动存储设备.
    - **优点**:兼容性好,几乎所有的操作系统都能识别和读写FAT文件系统.结构简单,易于实现,在嵌入式系统和小型设备中仍然非常流行.
    - **缺点**:不支持大文件(FAT32的单个文件最大限制为4GB)和大磁盘.没有内置的文件加密和安全控制机制.文件碎片整理比较频繁,随着使用时间的增加,性能可能下降.
- NTFS(New Technology File System):
    - **特点**:NTFS是由微软开发,用于替代FAT的更先进的文件系统,现在广泛用于Windows操作系统中.支持大文件和大容量存储,具有日志记录、文件权限和数据恢复功能.
    - **设计思维**:提供高性能和高可靠性,适合企业和专业环境.引入了元数据概念和更复杂的数据结构,以支持详细的文件安全权限和磁盘配额.
    - **优点**:支持文件压缩和加密.支持文件权限和安全设置,更适合企业级应用.系统出错时,恢复能力更强,支持事务日志处理.
    - **缺点**:相对FAT,NTFS复杂,消耗的系统资源也更多.在非Windows平台上的兼容性和支持较差.
- EFS(Encrypted File System)
    - **特点**:EFS不是一个独立的文件系统,而是构建在NTFS之上的一个功能,允许用户对文件进行加密.加密是透明的,即用户在访问文件时不需进行额外操作,系统自动加解密.
    - **设计思维**:设计上注重数据安全,目的是保护存储在硬盘上的敏感数据不被未授权访问.与NTFS紧密集成,保持文件系统的高效性和安全性.
    - **优点**:对用户透明,易于使用,提供强大的数据安全保护.结合NTFS的其他功能,如文件权限,为企业数据提供双重保障.
    - **缺点**:文件加密虽然提高了安全性,但一旦加密密钥丢失,数据将不可恢复.性能开销相对较大,特别是在大量文件加密和解密的情况下.

👉**知识点(Windows下的文件取证技术)**:Windows操作系统中的文件取证是一个重要的过程,涉及对文件系统内的数据进行详细分析,以获取法律和安全相关的证据.在Windows环境下,文档文件、图片文件、视频文件的取证尤为重要,因为这些类型的文件常常包含敏感或关键信息.下面介绍这些文件的取证技术及一些简单例子.

- **文档文件取证**:使用专门的取证工具,如FTK(Forensic Toolkit) 或 EnCase,这些工具可以帮助提取文档文件的元数据和内容,包括创建日期、修改日期、作者信息等.分析文档的内容和结构,查找隐藏信息或修改痕迹,如Word、Excel、PDF等文件中的修订记录和注释.例子:在一起骚扰起诉的调查中,取证分析人员使用FTK工具从疑犯电脑中恢复了删除的Word文档.通过分析这些文档的修订记录,确认了骚扰信件的起草和修改过程,为案件提供了关键证据.

- **图片文件取证**:图片文件的取证通常涉及分析图片的EXIF数据,这包括拍摄时间、设备信息、地理位置信息等.使用工具如PhotoRec进行恢复已删除的图片.分析图片内容,使用StegExpose等工具检测隐写术,即分析图片是否被用来隐藏其他文件或信息.例子:在一起涉密拍摄案件中,调查人员通过分析嫌疑人相机中的照片EXIF信息,确定了照片的拍摄时间和地点.与案发地点和时间的匹配加强了案件的证据链.

- **视频文件取证**:视频文件取证涉及提取视频文件的元数据,如编码信息、创建和修改时间等.使用视频分析软件,如Amped FIVE,可以进行视频内容的增强、格式转换、速度分析等,以辅助取证分析.检查视频文件是否经过编辑或篡改.例子:在一起交通事故责任争议中,通过对事故监控视频的分析,取证专家使用Amped FIVE软件调整了视频的清晰度和对比度,清晰地显示了事故发生时各车辆的位置和行驶状态,帮助法庭确定了责任方.

思考题

(♞思考) Windows事件日志取证中,用户登录事件对应"已收到用户在会话的登录通知","正常登录","完成处理用户在会话的登录通知","已收到用户在会话上的注销通知","已完成处理用户在会话上的注销通知"的 EventID 分别是几多?

答:分别是1,67,2,3,4;

(♞思考) 一家公司怀疑一个高级员工在离职前删除了重要文件.请描述如何利用Windows文件系统的日志和取证工具来确定此员工是否删除了文件,包括查找哪些日志记录.

答:使用Windows事件查看器(Event Viewer)检查安全日志,特别是关注事件ID 4663(一个对象的访问尝试)和 4656(受保护的对象的访问尝试).这些事件可以显示哪些文件被访问.查找事件ID 4660(删除对象),它记录了文件删除活动.利用文件系统日志分析工具,如 USN Journal Viewer,分析NTFS驱动器的USN日志,这可以帮助识别文件创建、修改和删除的时间线.考虑到文件可能被彻底删除,使用如Recuva或EnCase等数据恢复工具尝试恢复已删除的文件,以便进一步分析.

数字取证技术(Digital Forensics Technology)笔记IV

> 在数字取证领域,Linux操作系统被认为是强大且灵活的环境,具备许多适用于分析和应对复杂取证任务的工具.与Windows操作系统取证相比,Linux取证具有一些独特的特点和优势.Linux操作系统取证更加依赖技术知识和命令行工具的使用,而在Windows中,则更侧重用户界面的灵活性和易用性.Linux操作系统的开源特性为取证分析提供了更深入的可见性,但也意味着需要较高的技术熟练程度.两种环境上的取证均要求对系统特有的文件结构、日志机制和工具集有所了解.

Linux操作系统取证技术

👉**知识点(dd)**:用于创建磁盘或分区的位镜像.

示例:

```
dd if=/dev/sda1 of=/tmp/disk_image.iso bs=4096 conv=noerror,sync
```

- `if`:输入文件(input file),这里是指磁盘设备.
- `of`:输出文件(output file),即创建的磁盘镜像位置.
- `bs`:块大小(block size),每次读取/写入的字节数.
- `conv`:转换选项,`noerror` 继续操作发生错误的读取,`sync` 使用空字节填充块.

结果示例:

```
20480+0 records in
20480+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 10.0253 s, 10.5 MB/s
```

- 显示了读取和写入的块数量、总字节数、花费的时间及平均速率.

👉**知识点(strings)**:从二进制文件中提取可打印的字符序列.

示例:

```
strings -n 10 /bin/bash
```

- `-n`:输出长度至少为10的字符串序列.

结果示例:

```
/usr/lib/locale
LC_CTYPE
POSIX
```

- 这是从`/bin/bash`中提取出的字符串序列清单,通常更长,这里只展示了部分.

👉**知识点**(hexdump):以十六进制格式查看文件内容.

示例:

```
hexdump -C -n 100 /bin/bash
```

- `-C`:规范格式显示,展示十六进制和ASCII内容.
- `-n`:指定查看文件的前100个字节.

结果示例:

```
00000000  7f 45 4c 46 02 01 01 00  00 00 00 00 00 00 00 00  |.ELF............|
00000010  03 00 3e 00 01 00 00 00  60 09 40 00 00 00 00 00  |..>.....`.@.....|
...
```

- 每行包含了十六进制的字节表示和相应的ASCII字符.

👉**知识点**(find):搜索文件系统中的文件.

示例:

```
find / -name "*.log" -mtime -7 -print
```

- `/`:从根目录开始搜索.
- `-name`:搜索符合给定模式的文件名.
- `-mtime`:搜索在最近7天内被修改的文件.
- `-print`:打印找到的文件全路径.

结果示例:

```
/var/log/syslog
/var/log/kern.log
...
```

- 输出最近7天内被修改过的`.log`文件列表.

👉**知识点(grep)**:搜索文件内容.

示例:

```
grep "Failed password" /var/log/auth.log
```

- 搜索`/var/log/auth.log`中包含"Failed password"的行.

结果示例:

```
Feb 15 10:17:31 ubuntu sshd[2898]: Failed password for invalid user root from
192.168.1.101 port 22 ssh2
...
```

- 输出所有包含"Failed password"的日志行,显示登录失败的尝试.

👉**知识点(netstat)**:显示网络连接、路由表、接口统计等信息,有助于理解发生在系统上的网络事件.

示例:

```
netstat -antup
```

- `-a` 显示所有选项,默认情况下不显示监听的服务器套接字.
- `-n` 显示数字形式的地址(默认显示域名).
- `-t` 显示TCP连接.
- `-u` 显示UDP连接.
- `-p` 显示监听端口的程序名.

结果示例:

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1234/sshd
...
```

- 列出了系统上的所有TCP网络连接和监听状态,以及关联的进程.

👉**知识点(df)**:显示文件系统的磁盘空间使用情况,有助于发现异常的数据存储模式.

示例:

```
df -h
```

- `-h` 以易读的格式(如 MB、GB)显示信息.

结果示例:

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        20G   13G  6.0G  65% /
...
```

- 显示了每个文件系统的总大小、已使用空间、可用空间和使用百分比.

👉**知识点(lsof)**:列出当前系统打开文件的工具,用于发现正在运行的进程及其文件使用情况.

示例:

```
lsof -u username
```

- `-u` 按指定用户的进程列出文件.

结果示例:

```
COMMAND  PID   USER   FD   TYPE DEVICE SIZE/OFF     NODE NAME
sshd     1234  user   cwd  DIR  8,1    4096          2   /home/user
...
```

- 显示了用户`username`所运行进程的文件使用情况.

👉**知识点(mount/umount)**:挂载(mount)和卸载(umount)文件系统,常用于访问存储设备或磁盘镜像.

示例:

```
mount /dev/sdb1 /mnt/usb
```

- 将 `sdb1` 设备挂载到 `/mnt/usb`.

```
umount /mnt/usb
```

- 卸载 `/mnt/usb` 处的设备.

结果示例:通常不产生输出.

👉**知识点(fsck)**:检查和维护完整性和一致性的文件系统工具.

示例:

```
fsck /dev/sdb1
```

- 对设备 `sdb1` 进行文件系统检查.

结果示例:

```
fsck from util-linux 2.31.1
e2fsck 1.44.1 (24-Mar-2018)
/dev/sdb1: clean, 11/128016 files, 14221/512000 blocks
```

- 输出显示 `/dev/sdb1` 的文件系统检查结果.

👉**知识点(md5sum /sha256sum)**:计算和校验文件的 MD5 或 SHA-256 哈希值,用于验证文件的完整性.

示例:

```
md5sum example.txt
```

- 计算并显示 `example.txt` 文件的 MD5 哈希值.

```
sha256sum example.txt
```

- 计算并显示 `example.txt` 文件的 SHA-256 哈希值.

结果示例:

```
9e107d9d372bb6826bd81d3542a419d6  example.txt
```

- 显示了 `example.txt` 文件的 MD5 哈希值.

```
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855  example.txt
```

- 显示了 `example.txt` 文件的 SHA-256 哈希值.

👉**知识点(注册表的功能)**:...

思考题

(🐴**思考**):作为取证分析师,您怀疑某个犯罪分子修改了系统上的某些图片文件来隐藏信息.这些图片文件的后缀名为".png".请问如何使用Linux命令来计算特定目录下所有PNG图片文件的SHA-256哈希值,以便稍后进行检查和验证?

参考答案:

```
find /suspect/directory -name "*.png" -exec sha256sum {} + > image_hashes.txt
```

该命令使用 `find` 来搜索 `suspect/directory` 目录下所有 `.png` 文件,然后对每个找到的文件执行 `sha256sum` 命令,并将结果重定向输出到文件 `image_hashes.txt` 中.借助 `-exec` 参数, `{}` 代表当前处理的文件名, `+` 表示对找到的所有文件一起执行 `sha256sum` 命令.

(🐴**思考**):如果您需要查找最近7天内修改过的可疑脚本文件,这些脚本位于特定用户的home目录下,例如用户"bob",并且具有".sh"扩展名,您将如何使用Linux命令行来完成这项任务?

参考答案:

```
find /home/bob -name "*.sh" -mtime -7 -ls
```

- 这个 `find` 命令检查了用户"bob"的home目录(`/home/bob`)下所有 `.sh` 文件,在过去7天内修改过的文件会被列出,选项 `-ls` 会显示出每个找到文件的详细信息.

(🐴**思考**):如何使用单个Linux命令行,从系统中已经删除（但磁盘上尚未被覆盖的数据）的文件中恢复可能存在的可打印字符串?

参考答案:

```
grep --binary-files=text -a -C 200 '特定字符串' /dev/sda1 > recovered_text.txt
```

命令 `grep` 用于搜索磁盘 `/dev/sda1` 中含有'特定字符串'的数据,选项 `-a` 把二进制文件当作文本处理, `-C 200` 表示在找到的字符串周围包含200字节的内容,这有助于找到完整的字符串或文本段落,

输出重定向到了文件`recovered_text.txt`中.

(♞思考):对一次安全事件中某服务器的网络连接情况进行调查,如何使用命令行列出所有当前的TCP连接,以及每个连接的源地址和目的地址?

参考答案:

```
netstat -atn
```

`netstat`命令用于显示网络连接,选项`-a`显示所有连接和监听端口,`-t`表示仅显示TCP连接,`-n`显示数字地址,不进行主机名解析.

数字取证技术(Digital Forensics Technology)笔记V

> 这部分内容涵盖了IOS系统取证技术,移动终端取证技术和电子数据取证环境的知识点.

电子数据取证环境

☞**知识点**:台式计算机

- **硬盘种类**:通常使用机械硬盘(HDD)和固态硬盘(SSD).
- **接口类型**:SATA用于大多数HDD和SSD连接;较新的台式机可能支持NVMe接口,一般通过PCIe插槽直接连接至主板,提供更快的数据传输速度.

☞**知识点**:笔记本电脑

- **硬盘种类**:更常使用固态硬盘(SSD)因其抗震性能好;依然有使用2.5英寸的机械硬盘(HDD)的情况.
- **接口类型**:多数采用SATA接口,高性能笔记本电脑可能采用NVMe接口SSD.

☞**知识点**:苹果电脑(MacBook/iMac)

- **硬盘种类**:早期型号可能会有机械硬盘(HDD),但现代Apple设备多采用固态硬盘(SSD).
- **接口类型**:MacBook Air和MacBook Pro等新机型会使用专有的闪存存储或NVMe接口SSD,这些接口速度快.

☞**知识点**:苹果手机(iPhone)

- **硬盘种类**:iPhone使用内置非拆卸式的NAND闪存.
- **接口类型**:苹果设备通常通过Lightning或USB-C端口进行数据传输和充电,并采用专用的iOS系统存储文件.

☞**知识点**:安卓手机

- **硬盘种类**:安卓手机一般使用内置的NAND闪存,并且许多设备支持通过microSD卡扩展存储;
- **接口类型**:安卓手机多采用 microUSB 或 USB-C 端口进行数据传输和充电;文件系统更加开放,通常运行与Linux兼容的文件系统,如ext4;

IOS系统取证技术

☞**知识点**:时间戳查看:在MacOS中,文件和目录的时间戳信息包括创建时间(c时间),修改时间(m时间),元数据修改时间(md时间)和最后访问时间(a时间).可以使用终端应用程序并利用`ls -la`命令查看文件的详细信息,包括时间戳.也可以使用`stat`命令获取特定文件或目录的时间戳数据.

☞**知识点**:文件保险箱(FileVault)

- **FileVault**:MacOS提供的全盘加密功能称为FileVault,它使用XTS-AES-128加密与4096位秘钥链结合的加密技术.
- **加密解密**:FileVault加密通常在用户层有密码保护.要访问加密数据,取证专家可能需要用户的密码或恢复钥匙.在某些案件中,法律程序可能需要来获取这些信息.
- **取证注意点**:一旦有权访问,取证工具可以在启动到特殊外部驱动器或在保持系统未解锁的状态下,通过创建加密磁盘的物理镜像来提取数据.

☞**知识点**:数据提取

- **备份方法**:利用Time Machine等备份工具制作全盘备份可以作为数据提取的方式.取证专家可以分析这些备份,或直接从中恢复数据.
- **直接提取**:通常需使用专门的取证工具进行直接数据提取,如使用EnCase,FTK或MacQuisition等支持MacOS文件提取的取证工具.
- **逻辑提取**:逻辑提取常用于获取文件和文件系统数据,而不是制作完整的物理镜像.

移动终端取证技术

☞**知识点**:人工提取(Manual Extraction)

- **描述**:操作手机,手动获取信息.这可能包括浏览用户数据、短信、通话记录、应用程序数据等.
- **工具**:无需特定工具,但可能需要密码或用户锁定模式的绕过.
- **优点**:简单且不会损坏手机.
- **缺点**:提取数据的范围有限,取证人员可访问的数据量取决于用户权限和手机锁定状态.

☞**知识点**:逻辑提取(Logical Extraction)

- **描述**:使用专业软件通过USB等接口读取手机存储的逻辑信息.
- **工具**:Cellebrite UFED、Oxygen Forensics、XRY等.
- **优点**:相比人工提取可以获得更多的信息,且不需要物理改动设备.
- **缺点**:无法获取已删除或隐藏的数据,受设备保护状态影响较大.

☞**知识点**:JTAG/ISP方法

- **描述**:JTAG/ISP是直接操作手机硬件,通过测试点来获取存储在手机中的数据.
  - **JTAG**(Joint Test Action Group):通过设备上的测试接口,将手机置于特殊模式,直接读取内存数据.
  - **ISP**(In-System Programming):通过直接连接到手机主板上的内存芯片接口进行读取数据.
- **工具**:需要具有JTAG或ISP功能的设备和适当的训练.
- **优点**:能够绕开操作系统获取更深层次的数据.
- **缺点**:需要专业知识和工具,且可能破坏保修.

☞**知识点**:Chip-Off提取方法

- **描述**:物理移除手机上的内存芯片,然后使用特殊的读卡器或编程器提取数据.
- **工具**:芯片拆卸工具、电子显微镜、读卡器、热风枪等.
- **优点**:可以绕过所有软件锁定,直接读取内存数据.
- **缺点**:风险高,可能造成不可逆的损坏.

☞**知识点**:微读方法(Micro-reading / Microscopic Examination)

- **描述**:通过高级显微镜等设备进行芯片的微观结构分析,可能用于密码或加密破解(对NAND或NOR芯片存储层进行微观状态观察,并借助均衡磨损原理等固态介质存储理论进行数据还原).
- **工具**:电子显微镜、专业级实验室设备.
- **优点**:可以用于高难度的数据恢复,如焚毁、损坏的设备.
- **缺点**:需要高度专业的设备和技能,成本和时间消耗大.

数字取证技术(Digital Forensics Technology)习题课I

练习题

(♞ **思考**):在数字取证中,经常需要分析和识别大量日志数据中的模式和关联性,例如识别网络攻击过程中的事件关联或用户行为模式.假设有数万条由网络传感器生成的事件日志,需要建立一个事件关联矩阵,并用它与不同的用户行为模式矩阵相乘,以便快速地识别潜在的威胁和异常行为模式.由于数据量巨大,单线程计算矩阵乘法需要的时间会非常长,因此需要设计一种并行矩阵乘法算法来加速这一过程.

设计一个算法实现两个矩阵的并行乘法:输入为两个矩阵 A 和 B,矩阵 A 的维度为 $m \times n$,矩阵 B 的维度为 $n \times w$.输出为结果矩阵 C,其维度为 $m \times w$.

提示(Hint):思考矩阵乘法里哪些步骤是可以并行的;

(♞ **思考**):在数字取证领域,分析文本内容以发现潜在的模式和关键信息是一项常见的任务.假设你是一名取证专家,正在处理一项涉及大量电子邮件和聊天记录的案件.任务是从这些文本数据中,找出频率最高的100个单词二元组合及其频次,例如词组"客观-公平","物质-奖励"等.由于数据量非常庞大,需要设计一个高效的算法来处理这一任务,并确保能够快速准确地统计出最常见的单词二元组合.

提示(Hint):数据量非常庞大,这本质上是一个关于存储的算法问题;

复习(Review):有同学疑惑,为什么 HashTab 在不分治和分治的情形下差异很大;这主要是体现在时间复杂度方面:分治时是并行统计二元组频率,而合并其实所需的复杂度其实不大,而且也可以比较高效统计(这是因为我们还维护了一个词频的序,因此每个主机可以按这个内排序),而统计完后可以先过滤一遍,设定一个阈值τ(比如为5,那么小于5次的直接删去),这样又能减少很多空间复杂度,接下来再按照二元组频率排序(此时待排序的 HashTab 元素已经大大减少),就能快速获取前m位;

(♞ **思考**):(取证文件时间线排序)在数字取证过程中,通常需要将发现的证据(如文件、日志条目等)按照某种顺序排列以构建事件的时间线.在某次调查中,你获得了一份由不同来源(如文件系统元数据、网络传输记录等)收集到的时间戳数据.由于这些时间戳来自不同的系统,格式和精度也不同,你需要将它们按照真实的事件发生顺序进行排序,以辅助案件分析.

由于不同时间戳具有不同的格式和表示精度(如"YYYY-MM-DD HH:MM:SS","Unix时间戳","MM/DD/YYYY HH:MM"等),传统的按数字大小排序的方法不能直接适用.因此需要设计一个分治算法,该算法能够高效地处理此类复合格式的时间戳排序问题,并构建正确的事件时间线.

提示(Hint):回忆上一次课讲的分治排序方法;

复习(Review):可以先批处理一遍,比如令所有时间戳的格式都为UNIX/C格式,再进行排序;

数字取证技术(Digital Forensics Technology)习题课II

练习题

(🐴思考):(实时网页访问活动监控)在数字取证领域中,对疑似违规行为的实时监测是一个重要任务.开发一个系统来监控和检测用户的网页浏览行为,特别是对可能访问的违规网站进行检测.此监控系统需要即时评估用户的行为,当检测到用户在一定时间范围内访问违规网站数量超过阈值时,系统将报警.假设系统可以实时接收用户的网页访问事件流,并且每个网页访问事件包含有时间戳和URL.系统中应有一个违规网站的列表来判断访问的网站是否违规.如果系统检测到在给定的时间窗口(比如10分钟内)用户访问了超过N个不同的违规网站,则触发警报.

输入:

- 用户的网页访问事件流,格式为`(timestamp, URL)`.每个事件的时间戳均为Unix时间戳格式.
- 违规网站列表.

输出:警报信息,指出时间窗口和违规访问次数.

提示(Hint):使用动态规划的方法来减少重复的状态检查,以降低系统的处理时间,实时地监测网页访问事件流;

答:初始化变量:

- 定义违规网站集合`violating_sites_set`.定义时间窗口`time_window`,例如10分钟转换为秒.
- 定义访问违规网站数阈值`N`.
- 定义队列`activity_deque`,用于存储滑动时间窗口内的违规网站事件.

```
对于每个事件 event in event_stream:
    timestamp, url = event.timestamp, event.url;
    如果 url 在 violating_sites_set 中:
        # ---- 1.移除不在时间窗口内的最老事件 ----
        当 activity_deque 不为空且 timestamp - activity_deque.第一个元素.timestamp >
time_window:
            activity_deque.pop_left()
        # ---- 2.添加新的事件到 activity_deque ----
        activity_deque.append(event)
        # ---- 3.触发警报 ----
        如果 activity_deque 的大小 > N:
            触发警报("时间窗口内访问违规网站数超过阈值", activity_deque.第一个元
素.timestamp, timestamp)
```

(♞**思考**):(恢复故意删除的图片证据)当一个用户在Windows操作系统上故意删除图片文件时,系统通常只是将文件标记为可覆盖,并从文件分配表中移除文件的指向信息,而实际数据仍然在硬盘上,直到新的数据写入并覆盖原来的空间.描述了一个可行的方案用以尝试恢复这些被删除的图片文件;

答:

1.**立即停止使用磁盘**:在发现证据被删除的时刻起,立即停止使用相关的磁盘驱动器.因为当新的数据写入时,有可能会覆盖到被删除文件占用的空间,这会降低恢复数据的成功率.

2.**创建磁盘映像**:在进行任何恢复尝试之前,先使用取证级的磁盘成像工具如 FTK Imager 来创建磁盘的完整位镜像,以保持证据的原始状态和完整性.存储磁盘映像时应确保介质保护,避免任何可能的数据篡改.

3.**使用数据恢复软件**:利用专业的数据恢复软件,如 Recuva、EaseUS Data Recovery Wizard、Disk Drill 等来分析磁盘映像.这些软件能够扫描硬盘上未被分配的空间,尝试找到并恢复已删除的图片文件.

4.**分析和验证**:一旦数据恢复软件找到潜在的文件,分析工具将根据文件头(如图像的EXIF数据)或文件签名来识别图片并尝试恢复.完成恢复操作后,需要验证文件的完整性和可读性.

5.**报告和记录**:在整个过程中,应记录所有的步骤和发现,包括操作日期时间、使用的工具和版本、恢复的文件信息等.编写详细的报告以说明恢复过程和结果,为法律程序提供支持.