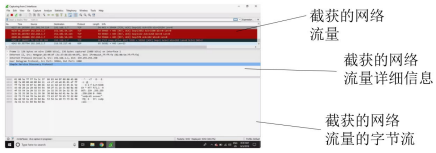


数字取证技术(Digital Forensics Technology)笔记II

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

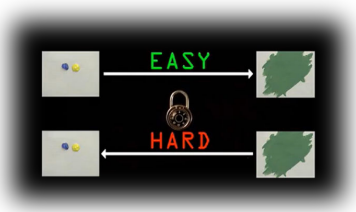
对于一个计算困难问题F,若设他的解为x^*,那么我们称x^*满足F;F的所有可能的解组成的空间称作解空间$\mathcal{X}$;计算困难问题F的求解过程即在解空间$\mathcal{X}$里面搜索x^*满足F,这一过程中要尽可能利用问题的特性来加速搜索;下面列举几个**例子**:

- 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;