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.