

大实验

**Peter泄密案鉴定意见书**

**目录**

**[4.1 案情说明 1](#_Toc23167)**

**[4.2 鉴定要求 1](#_Toc29770)**

**[4.3 实验环境 1](#_Toc17428)**

**[4.4 报告格式 1](#_Toc12901)**

**4 电子数据取证综合分析****和报告**

**4.1 案情说明**

这是在一起涉嫌侵犯商业秘密的案件。2016年4月27日，武汉天宇宁达科技有限公司员工Peter提出辞职。2016年4月29日，Peter交回自己使用的公司电脑。公司内审部门发现公司管控系统中记录了Peter在离职前期访问过公司涉密数据服务器怀疑Peter有窃取公司公司涉密数据资料的嫌疑。2016年5月，公司法务委托CFlab公司协助调查，查找Peter窃取机密资料的相关证据，以决定后期是否报案、诉讼。公司的绝密技术资料保存于内网文件服务器中，文件服务器地址\\JSZL。不同的项目有不同的命名规则。绝密项目以“JMXM+三位数字+中文命名”，普通项目以“JSZL+三位数字+中文命名”。

公司保密部门为防止数据泄露，制定有严格的保密制度。包括：1、内外网分离，涉密计算机禁止连接国际互联网；2、禁止使用个人移动存储介质；3、禁止使用私人邮箱。

**4.2 委托鉴定要求**

1、Peter是否在离职前访问过公司涉密文件服务器？如果有，访问过哪些数据？

2、Peter连接使用过移动存储设备？分析品牌型号、分配的盘符、连接时间

3、Peter是否通过打印方式窃取了数据？请提供时间线和相关证据。

4、Peter是如何连接国际互联网？请提供时间线和相关证据。

5、Peter将公司的绝密数据都拷贝到了哪些地方？请提供时间线和相关证据

6、Peter如何将数据通过互联网外传？请提供时间线和相关证据。

7、Peter进行了哪些反取证操作？请提供时间线和相关证据。

**4.3 实验环境**

工具：CDF电子数据取证实训环境下的所有可用工具

案例：CDF\实训案例\5-Windows\5-A01-Peter.e01

**4.4 报告格式**

请参考以下报告格式形成最终司法鉴定意见书。红色部分请注意阅读或替换为实际文字。本练习不强调文书的严谨程度，重点考核分析思路、方法和报告的基本格式。

**XX司法鉴定所**

**司法鉴定意见书**

编号： 学生学号

一、基本情况

委托人：武汉天宇宁达科技有限公司

送鉴人：郭永健 肖凌

委托鉴定事项：对Peter使用其工作电脑访问、复制、外传了公司机密项目的技术资料行为进行分析。

委托日期：2023年4月27日。

鉴定材料：送检材料为笔记本本电脑镜像文件。

鉴定日期：2024年4月27日- 2024年5月x日。

鉴定地点：华中科技大学网络空间安全学院。

二、基本案情

Peter窃密案（把委托信息摘选）

三、资料摘要（请随意填写个人计算机信息，满足形式即可）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 编号 | 类型 | 品牌 | 型号 | 容量 | 备注/标注 |
| 1 | 笔记本计算机 | Xx | xx | xx | xx |

检材照片

|  |  |
| --- | --- |
| 检材1正面  贴入你的计算机图片 | 检材1反面  贴入你的计算机图片 |

四、鉴定过程

1. 取证设备
2. 天宇宁达取证工作站 1台
3. 环境与系统
4. 你使用的取证分析工具和版本-1 1套
5. 你使用的取证分析工具和版本-2 1套
6. 鉴定过程执行的标准和规范（请删除与本次鉴定无关标准，保留应使用的标准）
7. GB/T 29362-2012 电子物证数据搜索检验规程
8. GB/T 29361-2012 电子物证文件一致性检验规程
9. GB/T 29360-2012 电子物证数据恢复检验规程
10. GA/T 976-2012 电子数据法庭科学鉴定通用方法
11. SF/Z JD0401002-2015 手机电子数据提取操作规范
12. SF/Z JD0402002-2015 数据库数据真实性鉴定规范
13. SF/Z JD0400001-2014 电子数据司法鉴定通用实施规范
14. GA/T 828-2009 电子物证软件功能检验技术规范

五、分析说明

1. 检材1哈希校验

编号1检材为笔记本计算机硬盘镜像。使用X-WAYS Forensics软件对5-A01-Peter.e01镜像进行哈希校验，得到MD5值为“11111111111111111111111111417”，SHA-1值为“242f44497a1e5862111111111111628763c7179c”，如图1所示。

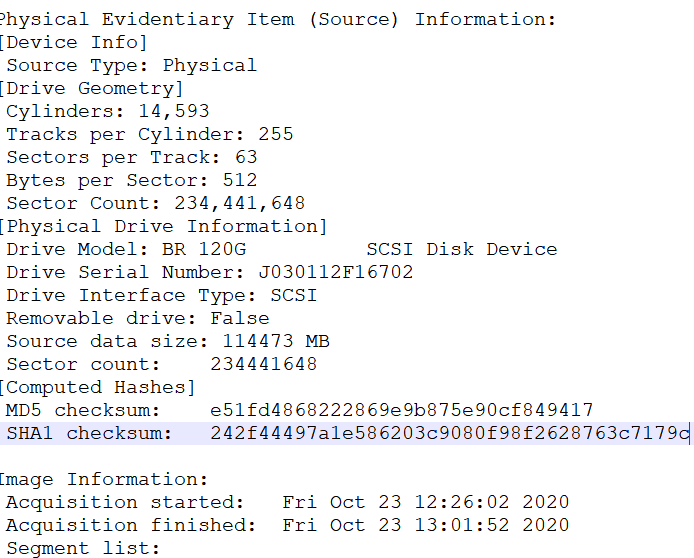


图1

1. 检材1 XXX痕迹检验分析（对分析过程中发现的各种痕迹，进行描述，配合图片进行证明。做到图文并茂，条理清楚，证据清晰。相关证据导出并压缩为“Peter泄密案附件.zip”，随鉴定意见书一起提交）
2. 对编号1检材中快捷方式进行分析，发现存在于2016年XX日访问机密数据的痕迹，部分信息见图2，详细信息见附件“Peter-快捷方式原始文件.zip”。

图2

1. 对编号1检材中跳转列表进行分析，发现存在于2016年XX日访问机密数据的痕迹，部分信息见图3，详细信息见附件“Peter-快捷方式原始文件.zip”。

图3

1. 检材1 XXX痕迹检验分析（对分析过程中发现的各种痕迹，进行描述，配合图片进行证明。做到图文并茂，条理清楚，证据清晰。相关证据导出并压缩为“Peter泄密案附件.zip”，随鉴定意见书一起提交）
2. 对编号1检材中电子邮件进行分析，发现存在于2016年XX日发送xxx邮件的痕迹，部分信息见图4，详细信息见附件“Peter-快捷方式原始文件.zip”。

图4

4、继续撰写分析过程，配合截图

六、鉴定意见

1. 送检材料密封和保护完整。
2. 数据分析：（对第五部分数据分析检验的提炼汇总，法官主要看以下意见，应描述清晰，结论明确）
3. 分析编号1检材中快捷方式，发现...。
4. 分析编号1检材跳转列表中，发现......

3、

4、

5、

七、附件

附件一：

文件：Peter泄密案附件.zip

大小：770640246 字节

MD5: 9750D162A2785aaaaaaB8D5C32708BF8

SHA1: 10EF803C15CD7aaaaaa13B0C78114B65E0AE1

（以下无正文）

司法鉴定人签名 你的名字

《司法鉴定执业证》证号：你的学号

司法鉴定人签名 肖凌

《司法鉴定执业证》证号：11111111111

二O二三年五月x日