

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：

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：2024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5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

三、资料摘要

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 编号 | 类型 | 品牌 | 型号 | 容量 | 备注/标注 |
| 1 | 笔记本计算机 | 华为 | HUAWEI 13s | 16GB/512GB | 无 |

检材照片

|  |  |
| --- | --- |
| 检材1正面 | 检材1反面 |

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. X-Ways Forensics 198\_SR-5 1套
5. 猎痕综合取证平台 V1.0.0 1套
6. 猎痕鉴证大师 1套
7. 鉴定过程执行的标准和规范
8. GB/T 29362-2012 电子物证数据搜索检验规程
9. GB/T 29361-2012 电子物证文件一致性检验规程
10. GB/T 29360-2012 电子物证数据恢复检验规程
11. GA/T 976-2012 电子数据法庭科学鉴定通用方法
12. SF/Z JD0401002-2015 手机电子数据提取操作规范
13. SF/Z JD0402002-2015 数据库数据真实性鉴定规范
14. SF/Z JD0400001-2014 电子数据司法鉴定通用实施规范
15. 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。使用鉴证大师软件对5-A01-Peter.e01镜像进行哈希校验，得到MD5值为“5606EA409C6370C7D3D6DFD7DA7AE487”，SHA-1值为“BECD00A12C2D4629C520B1AEF5075716E5475FF4”，如图1所示。





图1

1. 检材 1 Peter 在办理离职手续后曾经访问过公司服务器，并访问了服务器上的机密数据
2. 对编号1检材中快捷方式进行分析，发现存在于2016年4 月 28 日 14：15：33访问服务器上\\JSZL\JMXM 目录下的机密数据文件夹 JMXM005 的痕迹，部分信息见图2，详细信息见附件“Peter泄密案附件.zip”。



图2

1. 对编号1检材中跳转列表进行分析，访问过服务器上\\jszl\JMXM\JMXM010 目录，发现存在于2016 年 4 月 28 日 14:17:07访问机密数据的痕迹，部分信息见图3，详细信息见附件“Peter泄密案附件.zip”。

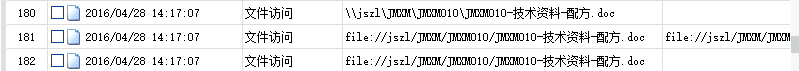


图3

3、对编号 1 检材中跳转列表进行分析，访问过服务器上\\jszl\JMXM\JMXM021 目录，其创建时间为2016 年 4 月 28 日 14：30：32，推测 Peter 于该时间访问了服务器上的该机密文件，部分信息见图 4。

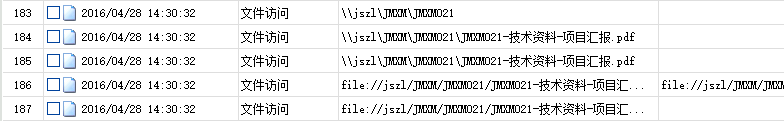


图4

1. 检材1 Peter 将服务器上的文件拷贝到本地其他存储位置
2. 对编号 1 检材中分区二下的 JMXM021 文件夹，于 2016 年 4月 28 日 14：36：37 访问 D 盘的一个 xls 文件，通过信息推测 Peter 将服务器上的机密信息文件夹拷贝到了本地 D 盘，部分信息见图 5 。



图5

1. 对编号 1 检材中分区二下的 JMXM021 和 JMXM010 文件夹进行分析，发现二者均于 2016 年 4 月 28 日 14：33：38 创建，查看这两个文件夹下的内容均与 JMXM 有关，推测被拷贝到了D 盘，部分信息见图 6 。

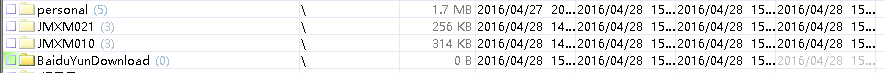


图6

1. 分析编号1检材中的快捷方式，发现其在2016年4月28日14:38:09将机密文件JMXM021-技术资料-项目概况.doc拷贝到盘符F:的光驱，留下了痕迹。相关的部分信息详见图7。

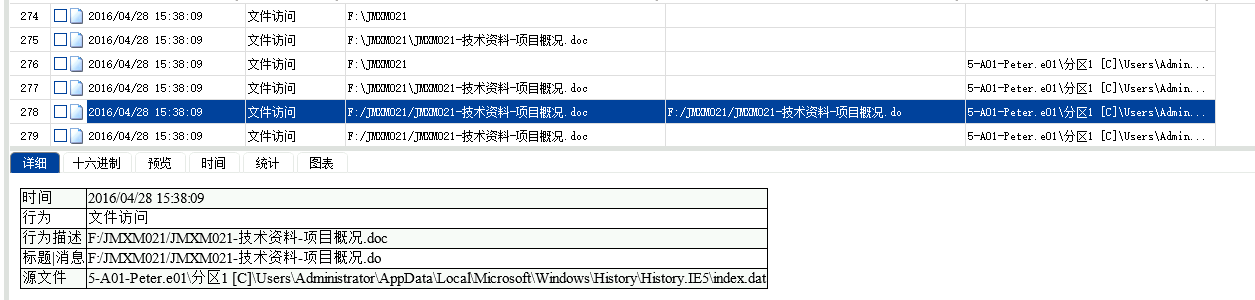


图7

1. 分析编号1检材中的分区里的JMXM010-技术资料-文档.lnk，发现其创建时间是2016年4月28日14:37:19。同时观察到Peter在同一时间在主D盘访问了JMXM010-技术资料-文档.doc文件，相关的部分信息可见于图8

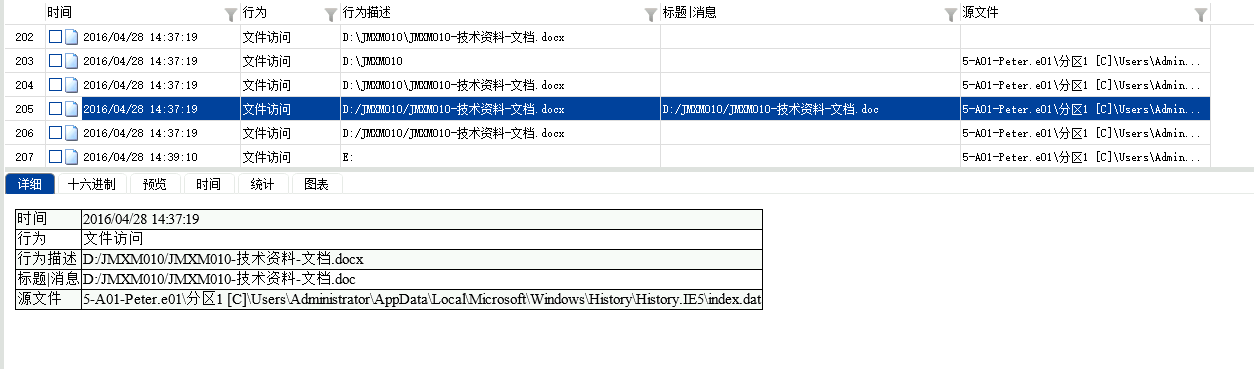


图8

1. 检材 1 Peter 将服务器上的文件拷贝到移动存储设备位置
2. 对编号1的检材分析表明，2016年4月28日14:35:36有连接USB设备的痕迹。根据时间和挂载的盘符，推断这可能是Peter的操作。相关部分信息见图9

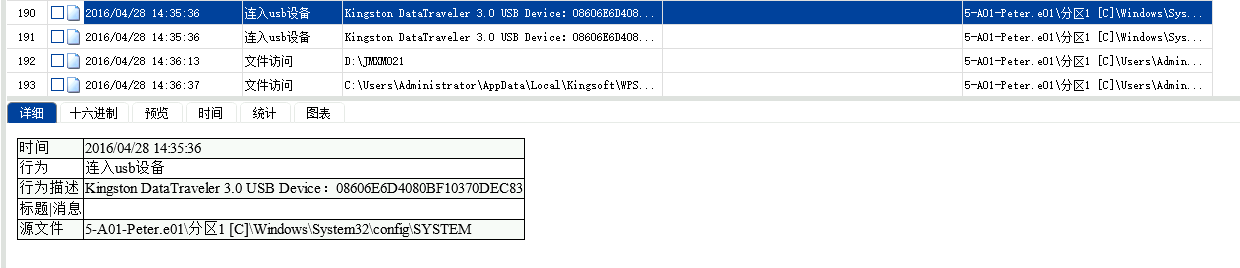


图9

1. 对编号 1 的检材的注册表进行分析，发现在 4 月 28 日 14：35：37，用户使用了 USB 设备 Kingston DataTraveler，部分信息见图 10。

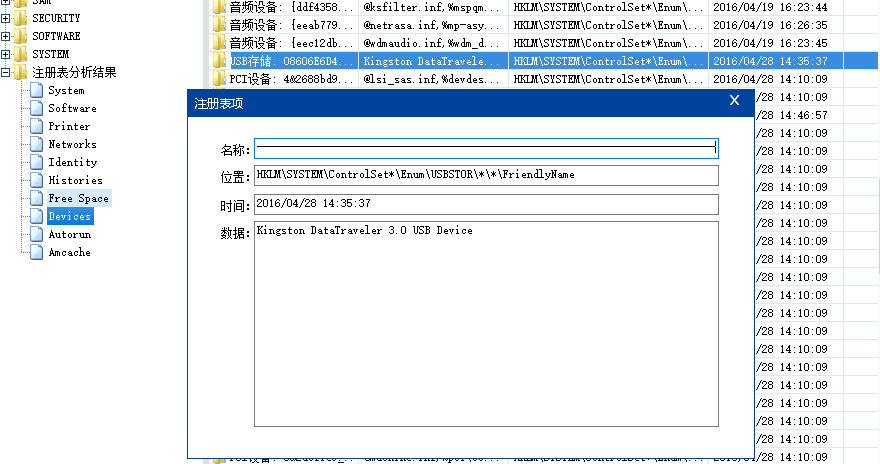


图10

1. 对编号 1 的检材的注册表进行分析，发现于2016 年 4 月28 日 14：10：14，用户使用软盘驱动器，部分信息见图11。

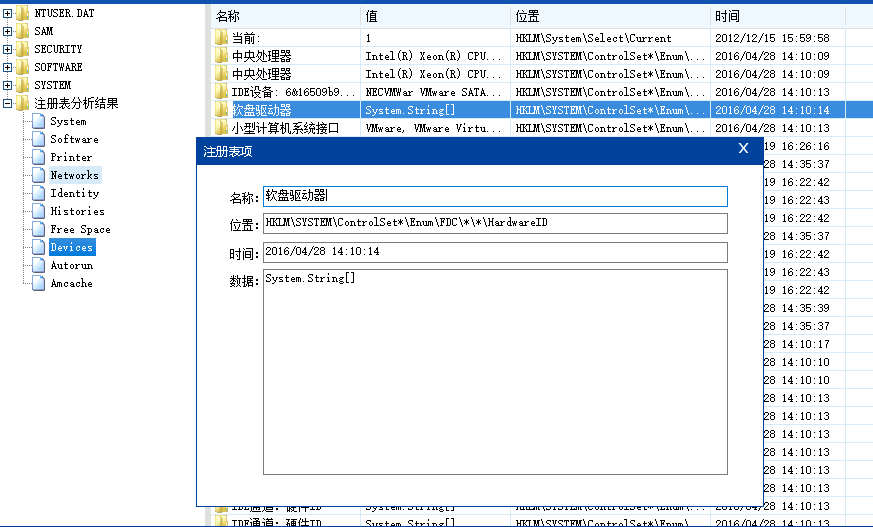


图11

1. 检材 1 Peter 离职后，使用了打印设备打印机密文件
2. 对编号 1 检材 进入\Windows\System32\spool\PRINTERS，对打印文件进行分析，其中的.SPL 文件是关于 JMXM021-技术资料-项目概况的信息，发现该文件创建于 2016 年 4 月 28 日 14：42：46。在鉴证大师调取打印信息对比时间，综合信息推测 Peter 在离职后，于该时间打印了机密文件，部分信息见图 12 和图 13

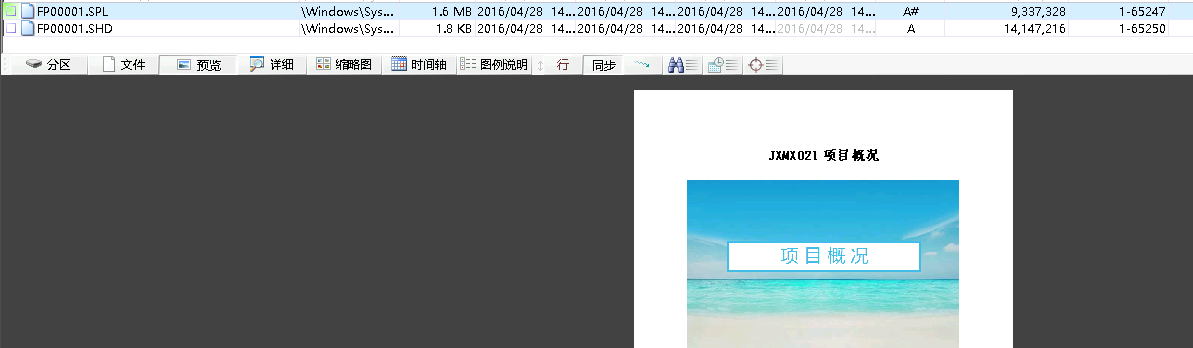


图12



图13

1. 检材 1 Peter 在泄密后删除相关机密文件
2. 对编号 1 检材中文件夹状态进行分析，发现 JMXM010 和 JMXM021 曾经存在，即已被删除，部分信息见图 14。

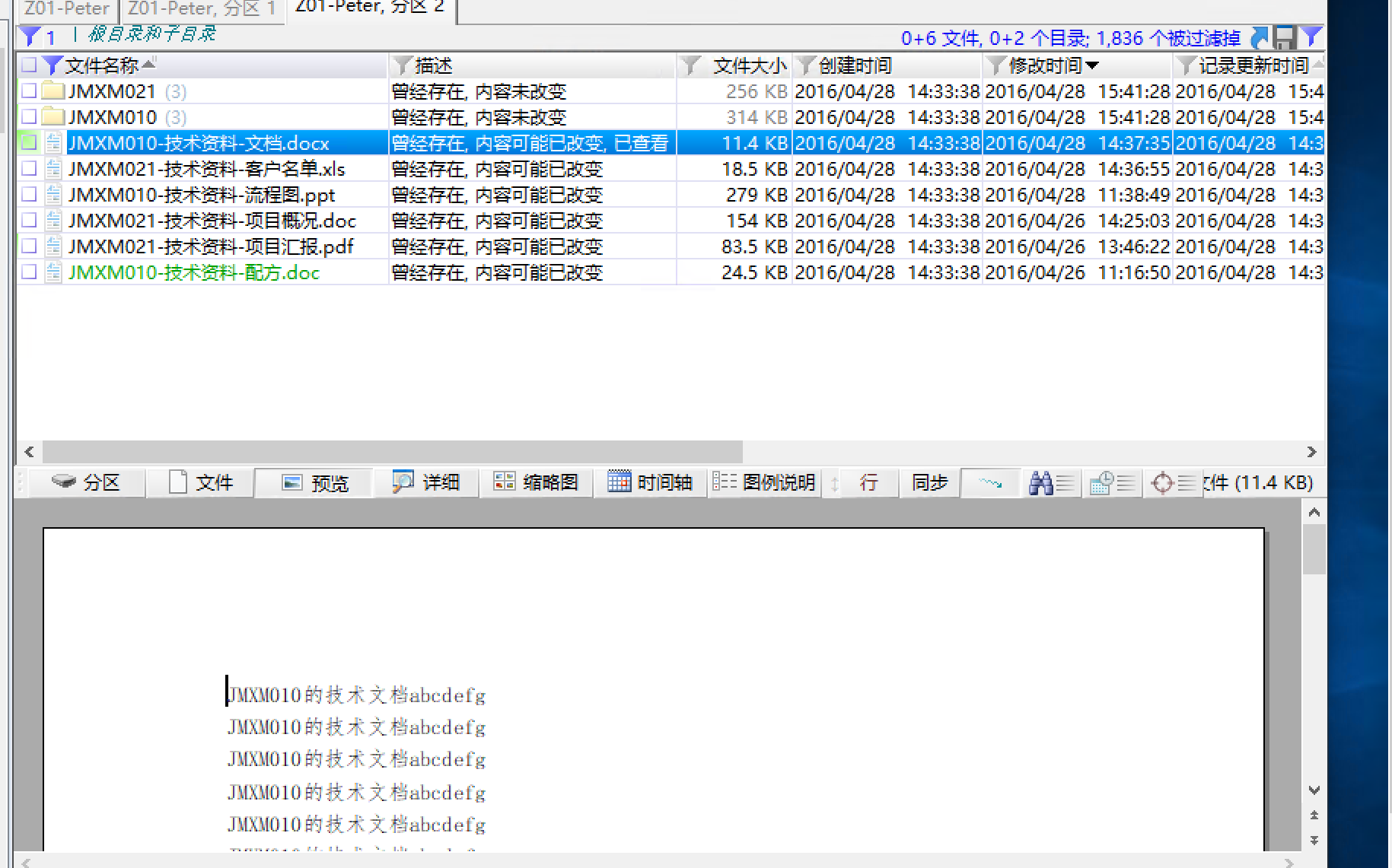


图14

1. 对编号 1 检材上述两个文件夹中的内容状态进一步分析，发现JMXM010 和 JMXM021 文件夹下的所有文件都是曾经存在，已被删除，部分信息见图 15。

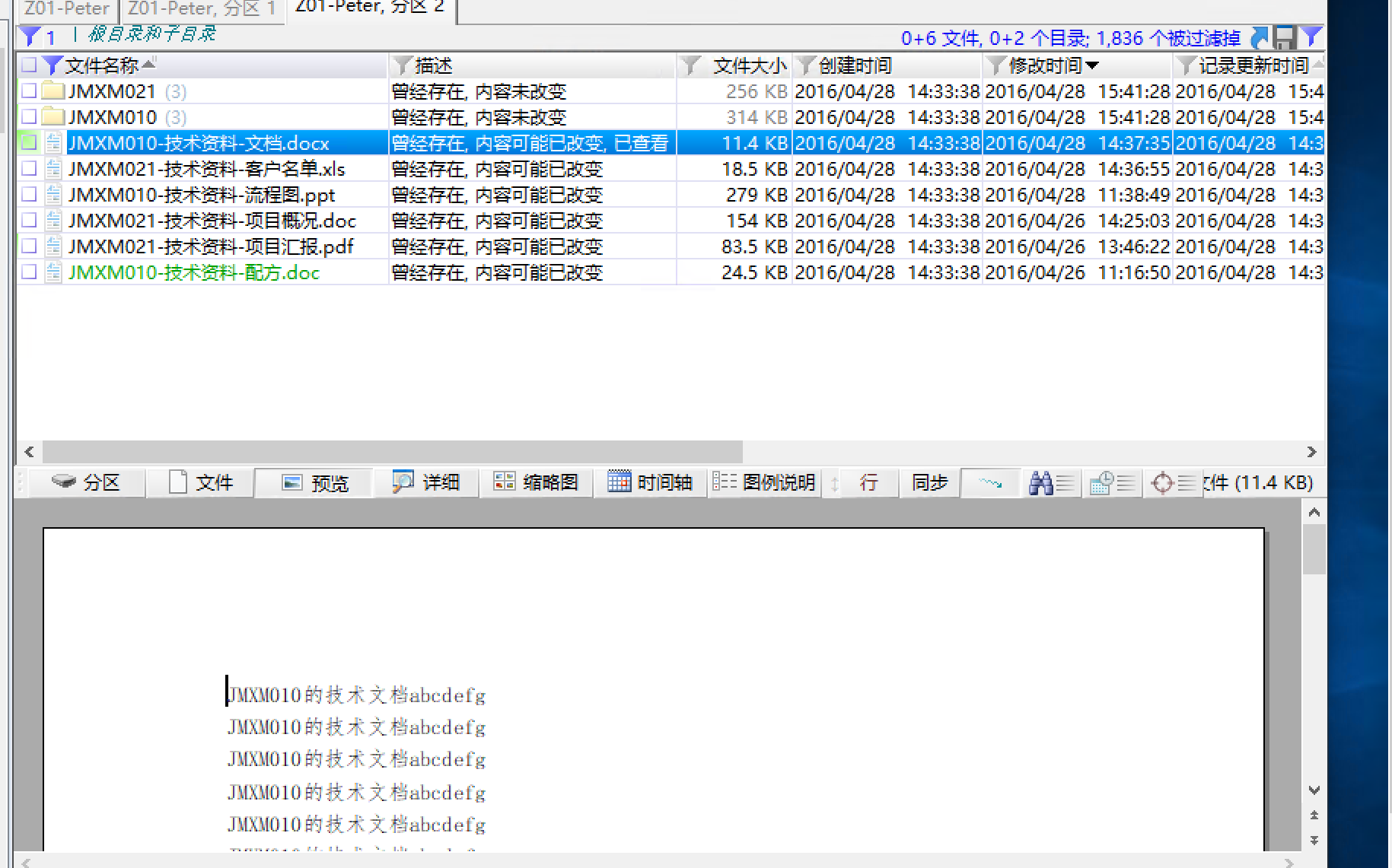


图15

1. 检材 1 Peter 离职后，使用了 Internet 传输公司机密文件
2. 对编号 1 的检材中的软件使用痕迹进行分析，找到了 2016年 4 月 28 日 15：31：35 的时候，使用百度云盘上传“重要资料.rar” 的痕迹，推断出这可能是被窃取的敏感信息，并且进行了泄露。部分信息见图 16。

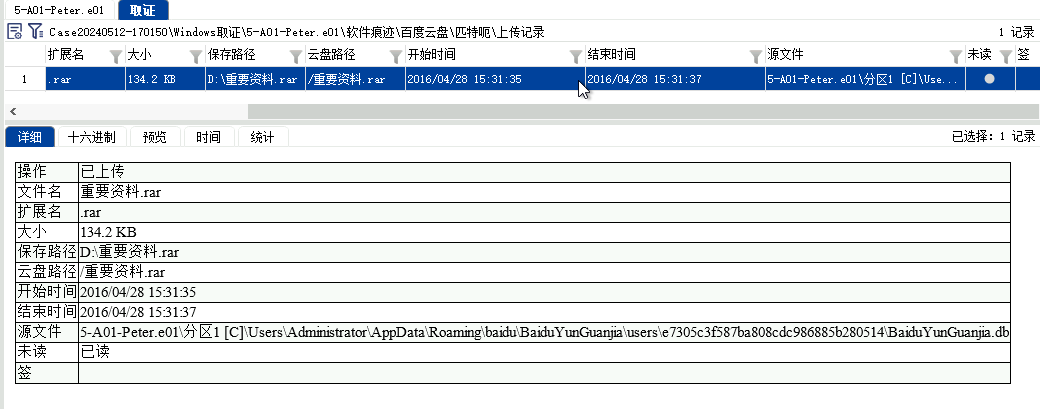


图16

1. 对编号 1 的检材进行分析，发现“重要资料.rar”曾经存在的痕迹，说明Peter将该文件上传到百度云之后将本地的文件删除。部分信息见图 17。

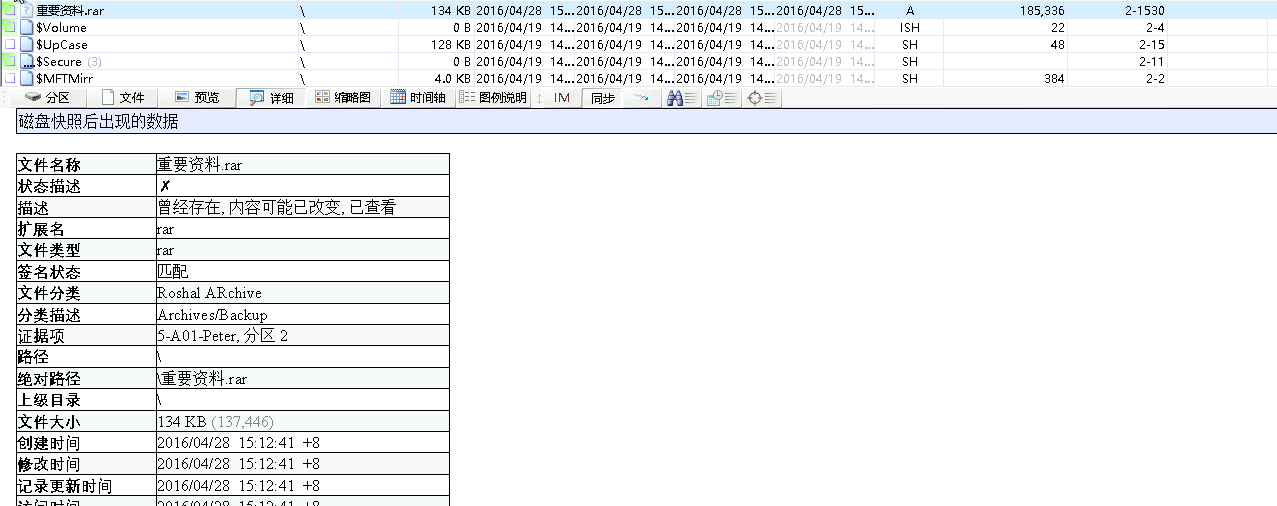


图17

1. 对编号 1 的检材进行分析，发现“重要资料.rar” 打包的就是JMXM010 文件夹内的东西，确定为机密信息。部分信息见图18。

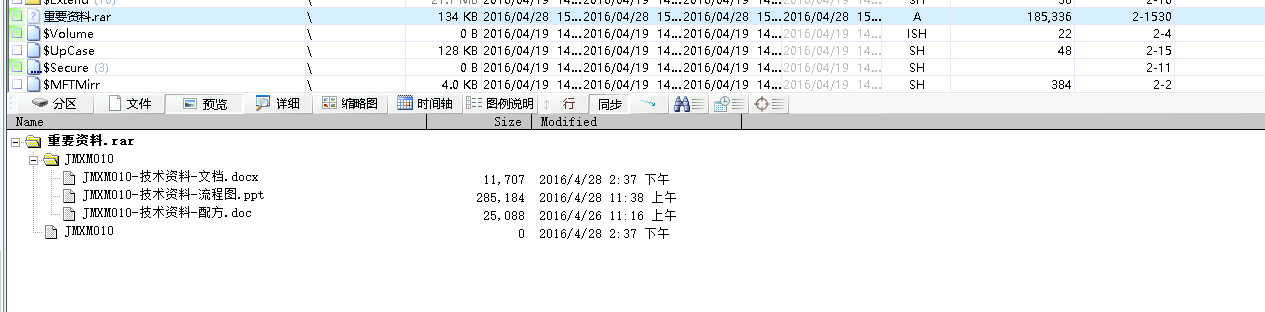
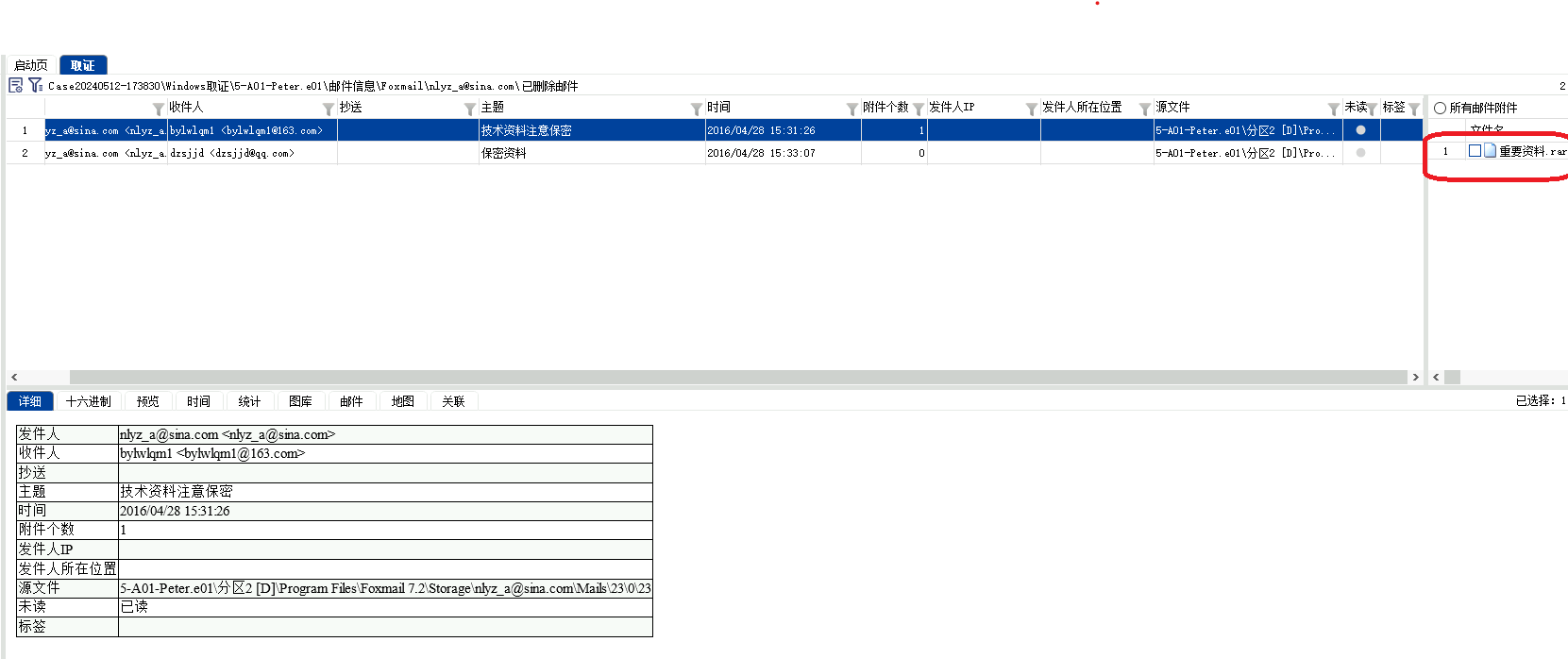


图18

1. 对编号 1 的检材进行取证，发现“重要资料.rar”被 Peter通过 Foxmail 邮箱以附件形式发送了出去，这是把机密信息外传的重要依据。部分信息见图 19。

图19

1. 对编号 1 的检材进行取证，发现“重要资料.rar” 不只通过邮件附件进行了外传，并且还被通过网盘链接的方式分享了出去，同样作为Peter泄露机密文件的有力证据。部分信息见图 20。



图20

六、鉴定意见

1. 送检材料密封和保护完整。
2. 数据分析：
3. 在编号 1 检材中快捷方式中，发现 Peter 在办理离职手续后访问过公司服务器，并访问了服务器上的机密数据，之后把数据保存到了 D 盘。
4. 在编号 1 检材中快捷方式中，发现 Peter 不仅将机密信息保存到本地，还将服务器上的文件拷贝到移动存储设备位置，具体为 Kingston DataTraveler USB 3.0 和 F 盘，软盘驱动器。

3、在编号 1 检材中快捷方式中，发现 Peter 离职后，使用了打印设备打印机密文件，具体文件为 JMXM021-技术资料-项目概况。

4、在编号 1 检材中快捷方式中，发现 Peter 在泄密后删除相关机密文件，具体表现为删除了 JMXM010 和 JMXM021 文件夹以及文件夹中的所有文件。

5、在编号 1 检材中快捷方式中，发现 Peter 离职后，使用了Foxmail和百度云外传公司机密文件。具体操作为把机密文件打包为rar，将机密文件上传到了百度云，然后以网盘链接的形式分享，并且通过 Foxmail 邮件附件的形式外传出去，完成上述操作后，Peter删除了本地的 rar 文件而且进行相关邮件信息的删除。

七、附件

附件一：

文件：Peter泄密案附件.zip

大小：348,385 字节

MD5: f66a7cf4028985255baf659b0cd0f09c

SHA1: ac11bde9c3f93086cfd1c7ac5435a14158055646

司法鉴定人签名

《司法鉴定执业证》证号：

司法鉴定人签名 肖凌

《司法鉴定执业证》证号：11111111111

二O二四年五月五日