**XX司法鉴定所**

**司法鉴定意见书**

编号： U202112131

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2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 | 联想 | ThinkBook 14 G4+ IAP | 16GB/  512GB | 无 |

检材照片

|  |  |
| --- | --- |
| 检材1正面  IMG_256 | 检材1反面  IMG_256 |

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 19.8\_SR-5 x64 1套
5. 猎痕鉴证大师综合分析系统 V5.12 1套
6. 鉴定过程执行的标准和规范
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 JD0402002-2015 数据库数据真实性鉴定规范
12. SF/Z JD0400001-2014 电子数据司法鉴定通用实施规范
13. 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“5606EA409C6370C7D3D6DFD7DA7AE487”，SHA-1值为“BECD00A12C2D4629C520B1AEF5075716E5475FF4”，如图1和图2所示。

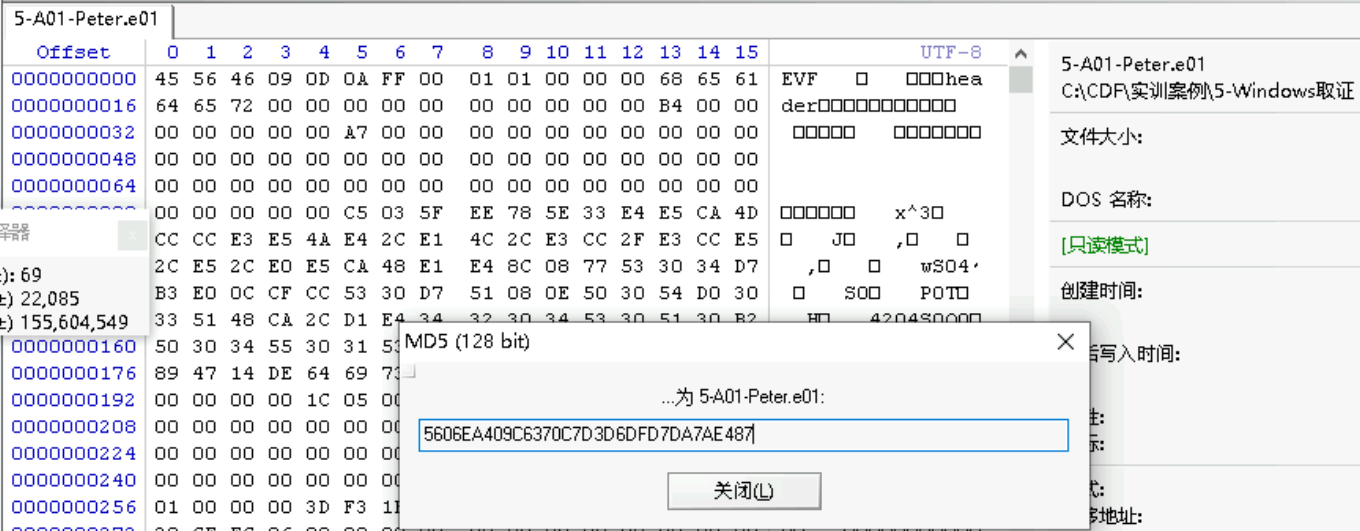


图1 MD5检验值截图

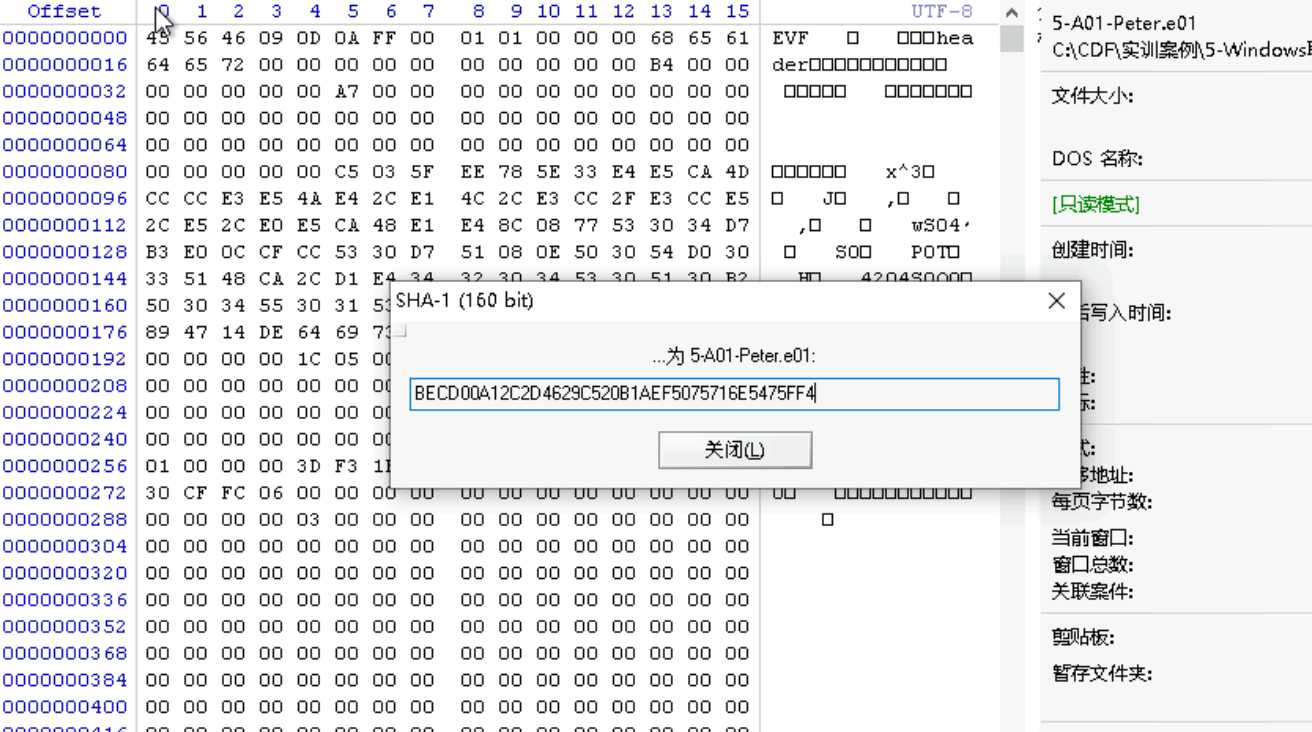


图2 SHA1检验值截图

1. 检材1 涉密文件访问痕迹检验分析
2. 对编号1检材中使用猎痕鉴证大师对快捷方式进行分析，发现存在于2016年4月28日14时到15时左右访问涉密文件服务器的痕迹，具体访问了“//jszl/JMXM/JMXM005”,“//jszl/JMXM/JMXM010”和“//jszl/JMXM/JMXM021/”目录，部分信息见图3，详细信息见附件“Peter-涉密案附件.zip”。



图3 快捷方式截图

1. 对编号1检材中跳转列表进行分析，发现存在于2016年4月28日14时到15时左右访问机密数据的痕迹，部分信息见图4，详细信息见附件“Peter-涉密案附件.zip”。



图4 跳转列表截图

1. 对编号1检材中最近访问文件记录进行分析，发现存在于2016年4月28日14时到15时左右访问机密文件的痕迹，部分信息见图5，详细信息见附件“Peter-涉密案附件.zip”。这进一步佐证了Peter曾访问涉密文件服务器并浏览机密数据。



图5 最近访问文件记录截图

1. 检材1 移动存储设备使用痕迹检验分析
2. 对编号1检材中USB设备使用记录进行分析，发现存在于2016年4月28日14:35:36连接使用移动设备的痕迹，品牌型号为Kingston DataTraveler 3.0 USBDevice，挂载盘符到E盘，如图6所示。

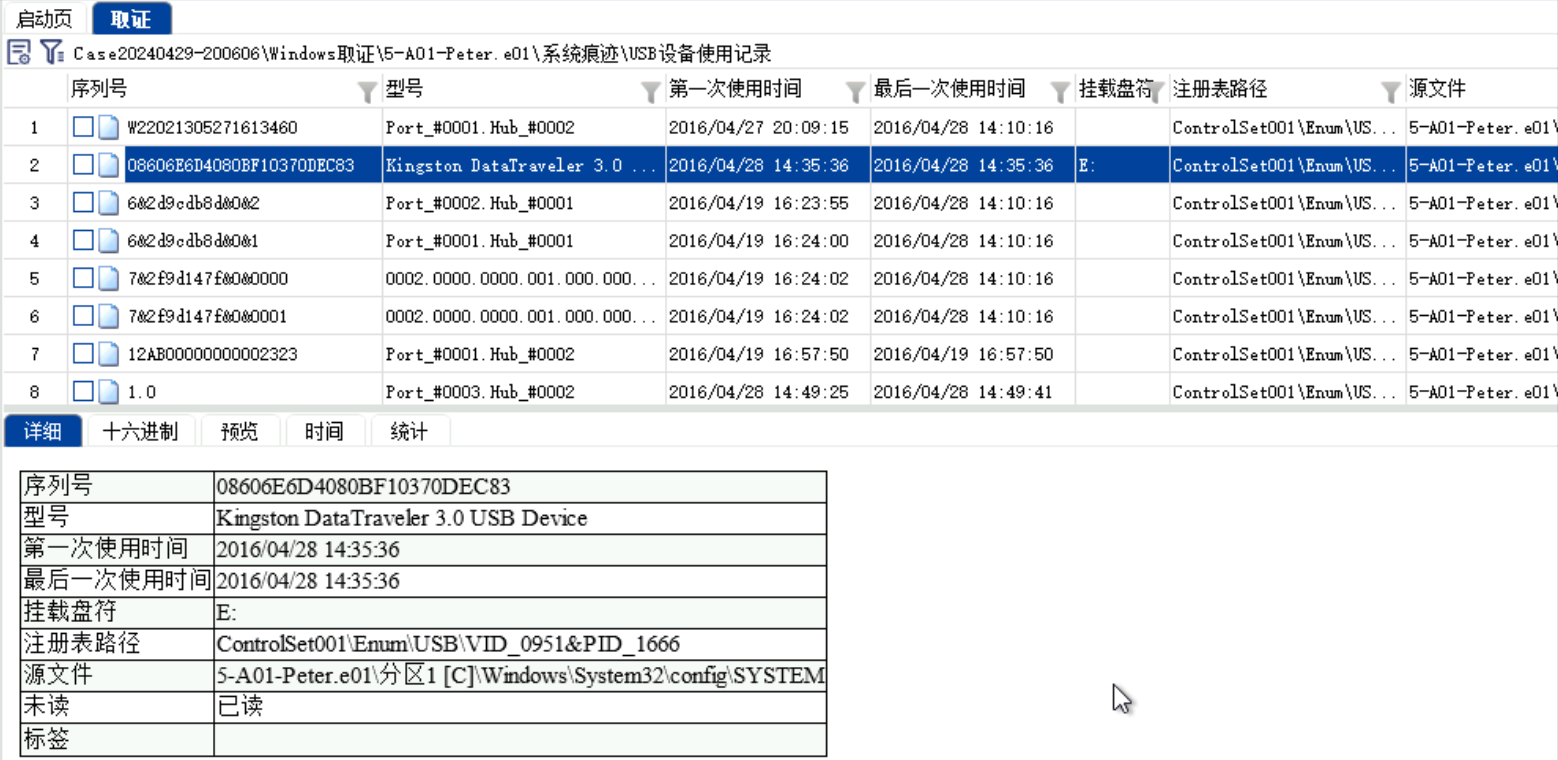


图6 USB设备使用记录截图

1. 对编号1检材中注册表信息进行分析，发现存在于2016年4月28日14:35:37使用USB设备Kingston DataTraveler的痕迹，进一步佐证Peter曾使用了移动存储设备，违反了公司禁止使用个人移动存储介质的规定，如图7所示。

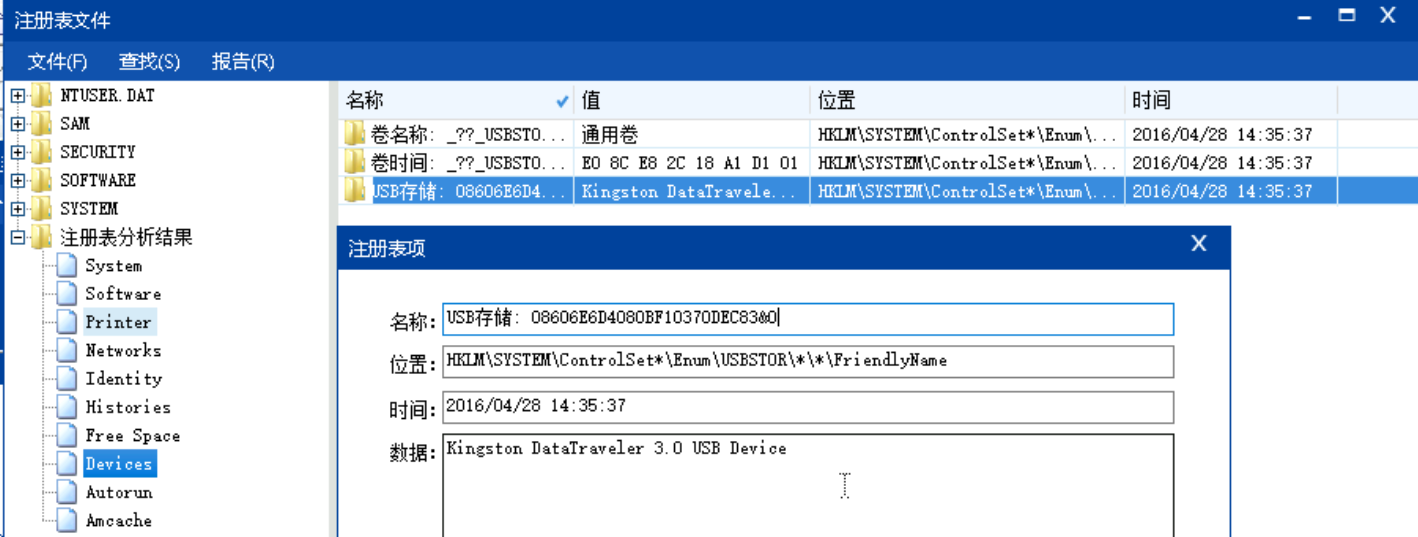


图7 注册表中USB使用记录截图

1. 检材1 打印机密数据痕迹检验分析
2. 对编号1检材中打印文件进行分析，发现存在于2016年4月28日14:42:47打印文件的痕迹，打印的文件为“JXMX021-技术资料-项目概况.doc”，使用的打印机型号为EPSON Stylus Photo R270 Series，部分信息见图8、图9和图10，详细信息见附件“Peter-涉密案附件.zip”。

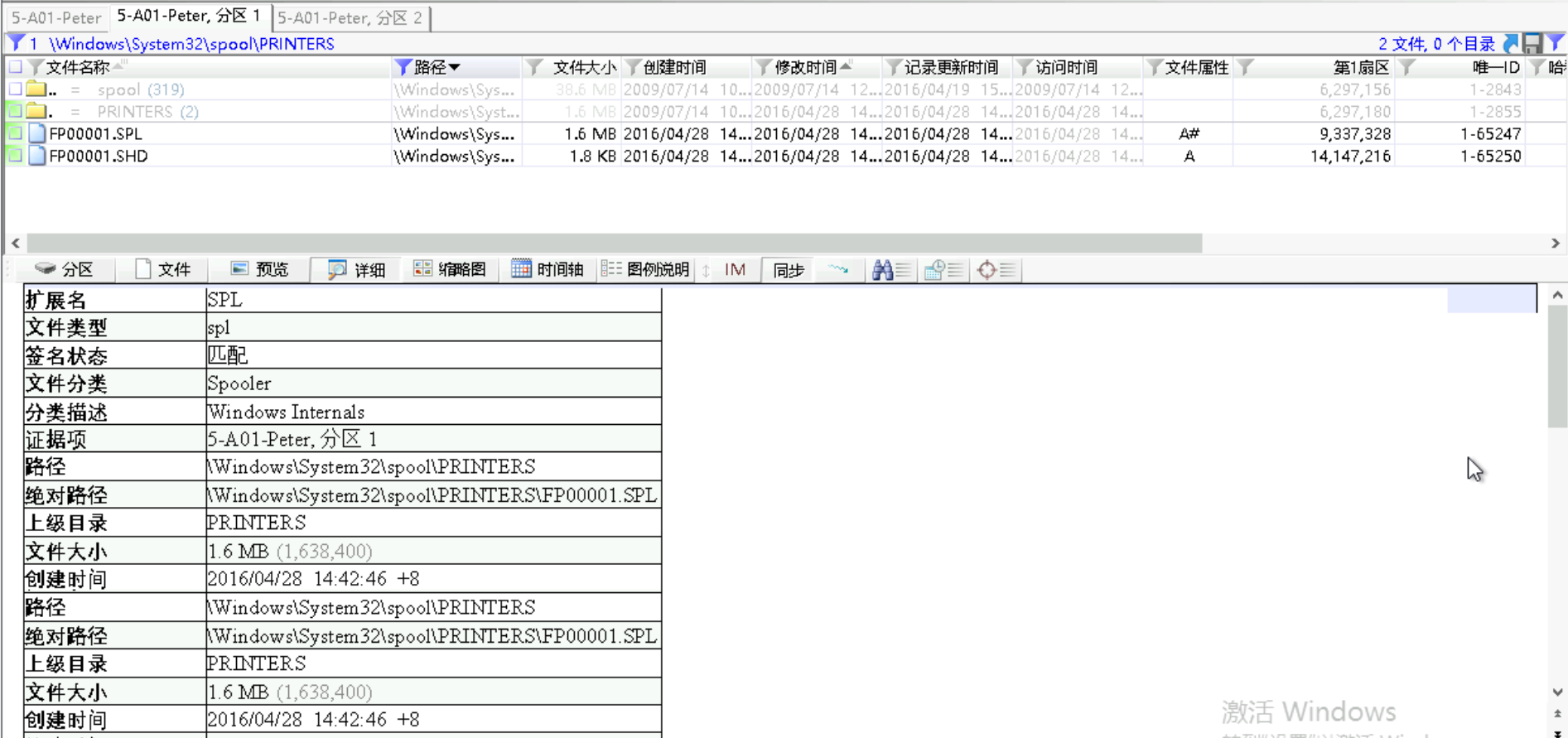


图8 打印文件信息1截图

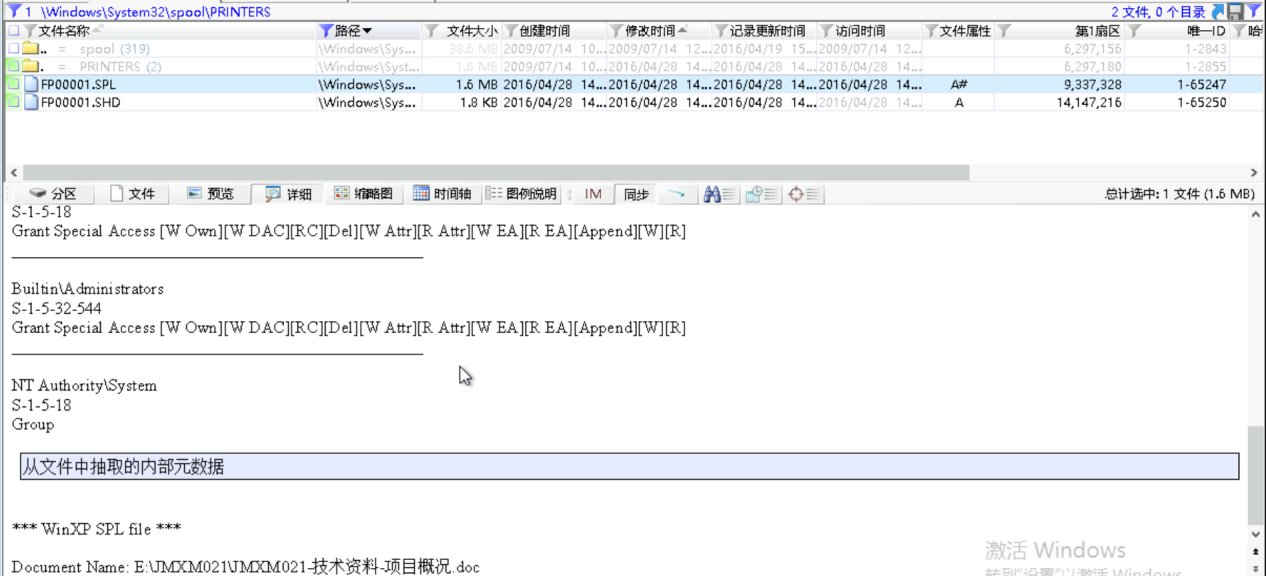
图9 打印文件信息2截图



图10 打印信息截图

1. 检材1 国际互联网连接痕迹检验分析
2. 对编号1检材中网络映射进行分析，发现存在到涉密文件服务器jszl的内网端口映射，即Peter计算机可访问涉密内网，如图11。

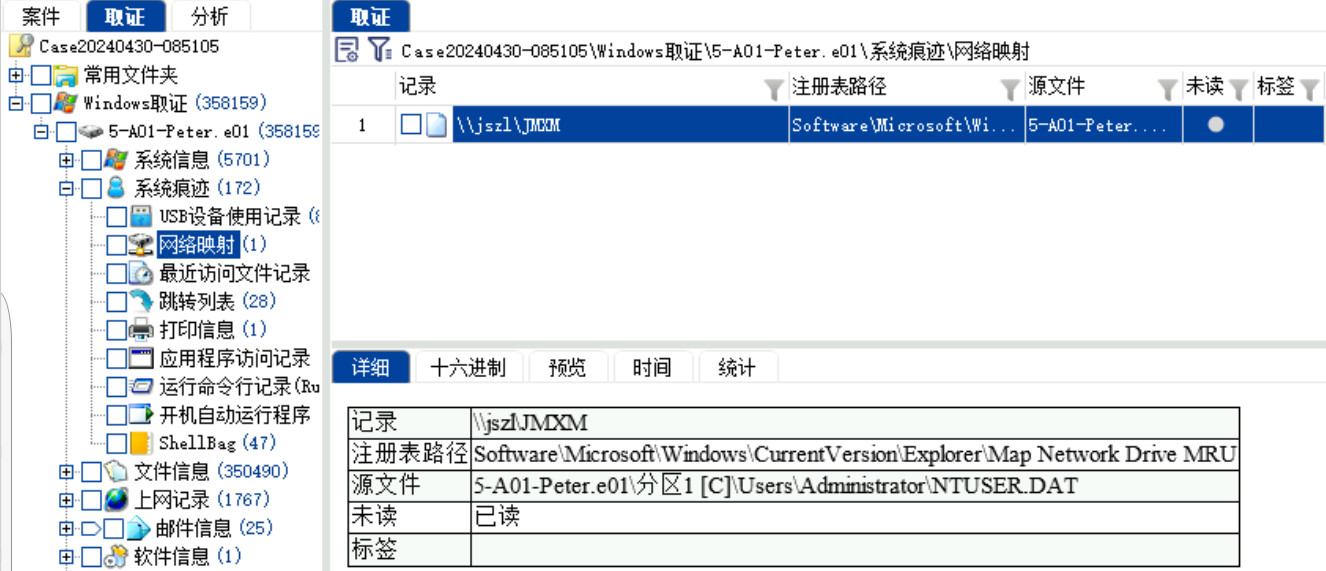


图11 网络映射信息截图

1. 对编号1检材中上网记录进行分析，发现存在于2016年4月28日14:55:19接入名为“P.ZHAO”的无线网络的痕迹，并浏览了若干网址产生cookies记录，证明Peter违反了公司的涉密计算机禁止连接国际互联网的制度。部分信息见图12和图13，详细信息见附件“Peter-涉密案附件.zip”。

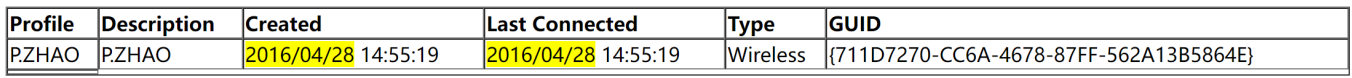


图12 网络连接信息截图

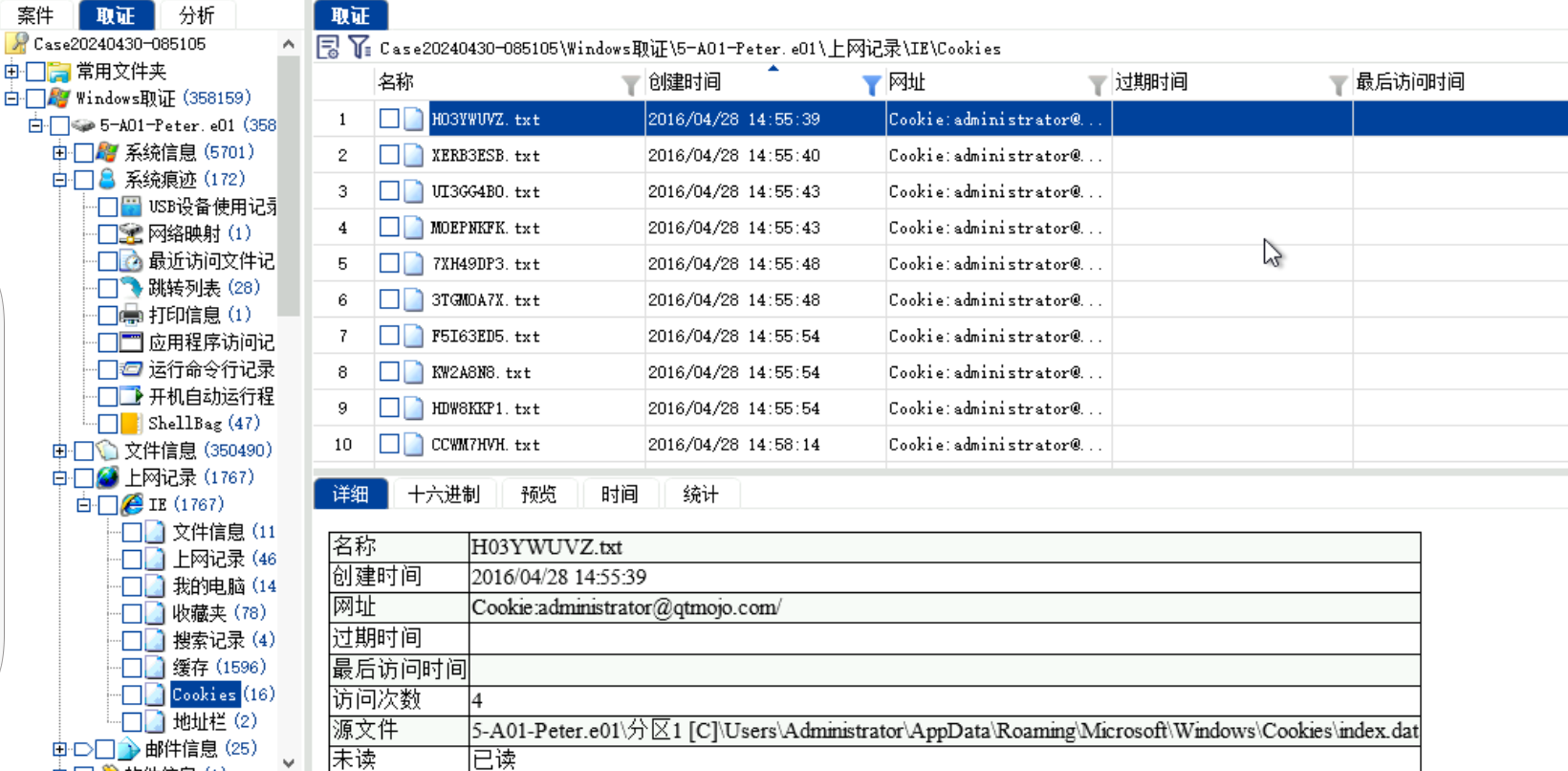


图13 cookies记录截图

1. 检材1 绝密数据拷贝痕迹检验分析
2. 对编号1检材中快捷方式和文件创建信息进行分析，发现存在于2016年4月28日14时33分创建的快捷方式JMXM010和JMXM021，目标路径为D盘和F盘，查看文件信息确定为机密文件，可见Peter将机密数据由服务器拷贝到了D盘和F盘。部分信息见图14和图15，详细信息见附件“Peter-涉密案附件.zip”。

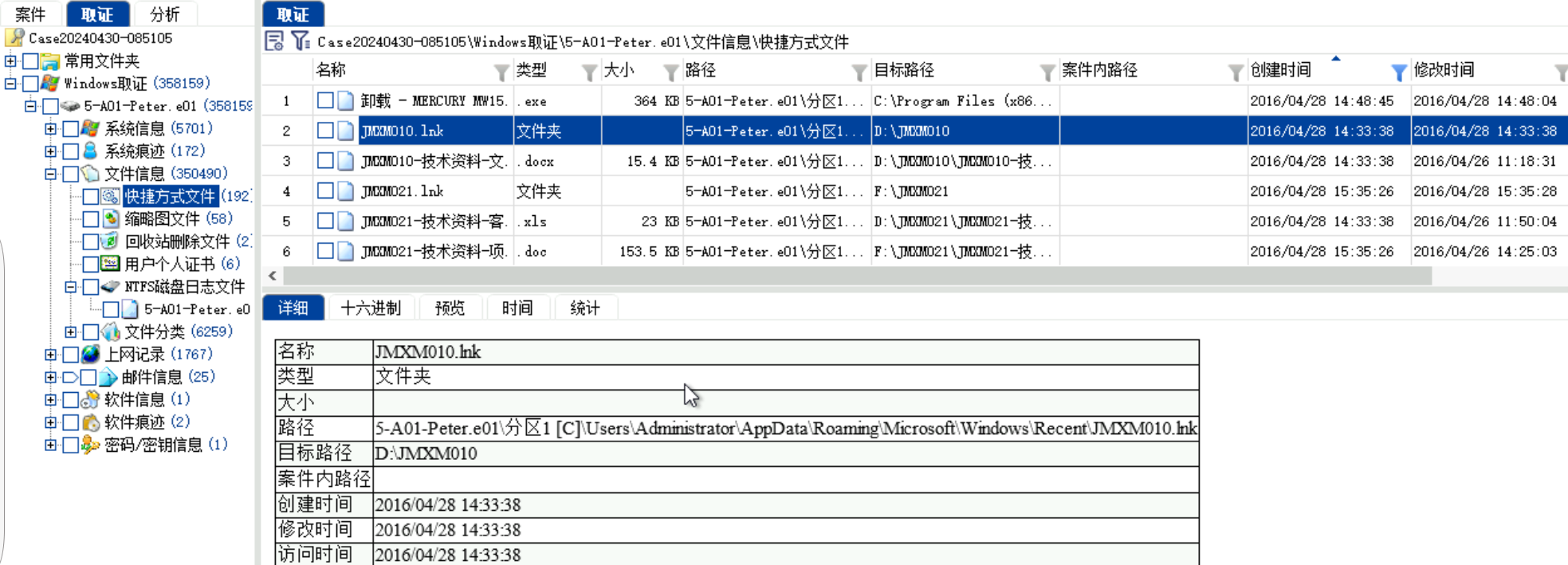


图14 机密文件快捷方式截图

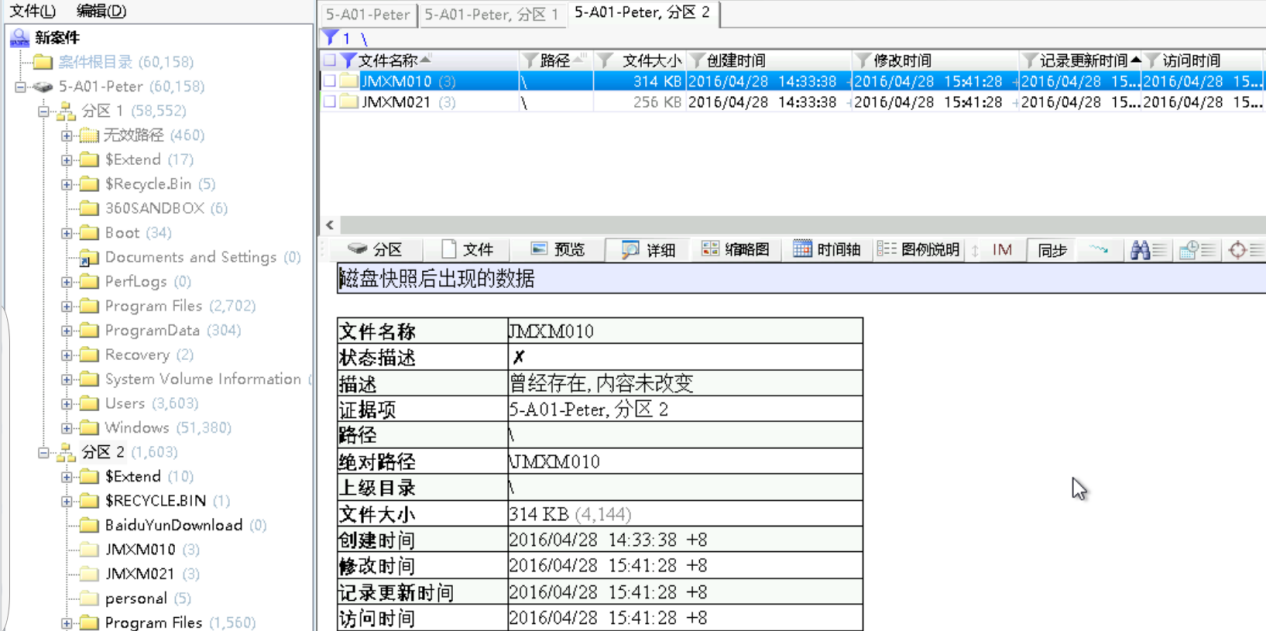


图15 文件信息截图

1. 对编号1检材中跳转列表进行分析，发现存在于2016年4月28日14时36分到E盘JMXM021文件夹的跳转，且结合前述2016年4月28日14时35分连接USB并挂载到E盘的分析，可见Peter将机密文件拷贝到了外接USB设备，部分信息见图16和图17，详细信息见附件“Peter-涉密案附件.zip”。



图16 E盘跳转列表截图

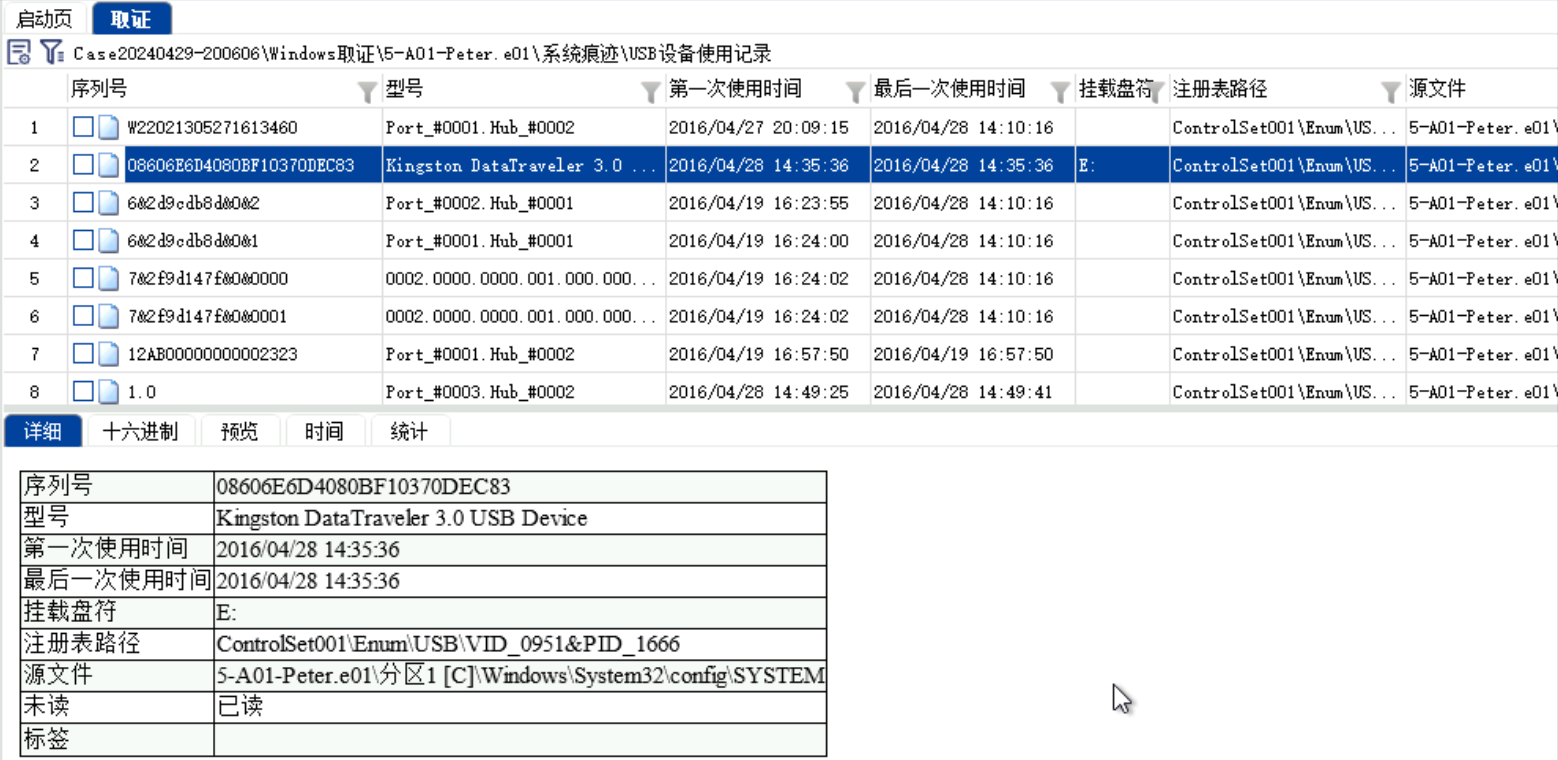


图17 连接USB并挂载E盘截图

1. 检材1 数据互联网外传痕迹检验分析
2. 对编号1检材中网页浏览记录进行分析，发现存在于2016年4月28日14时59分到15时11分上网下载百度云管家和Foxmail两个软件的痕迹，部分信息见图18，详细信息见附件“Peter-泄密案附件.zip”。

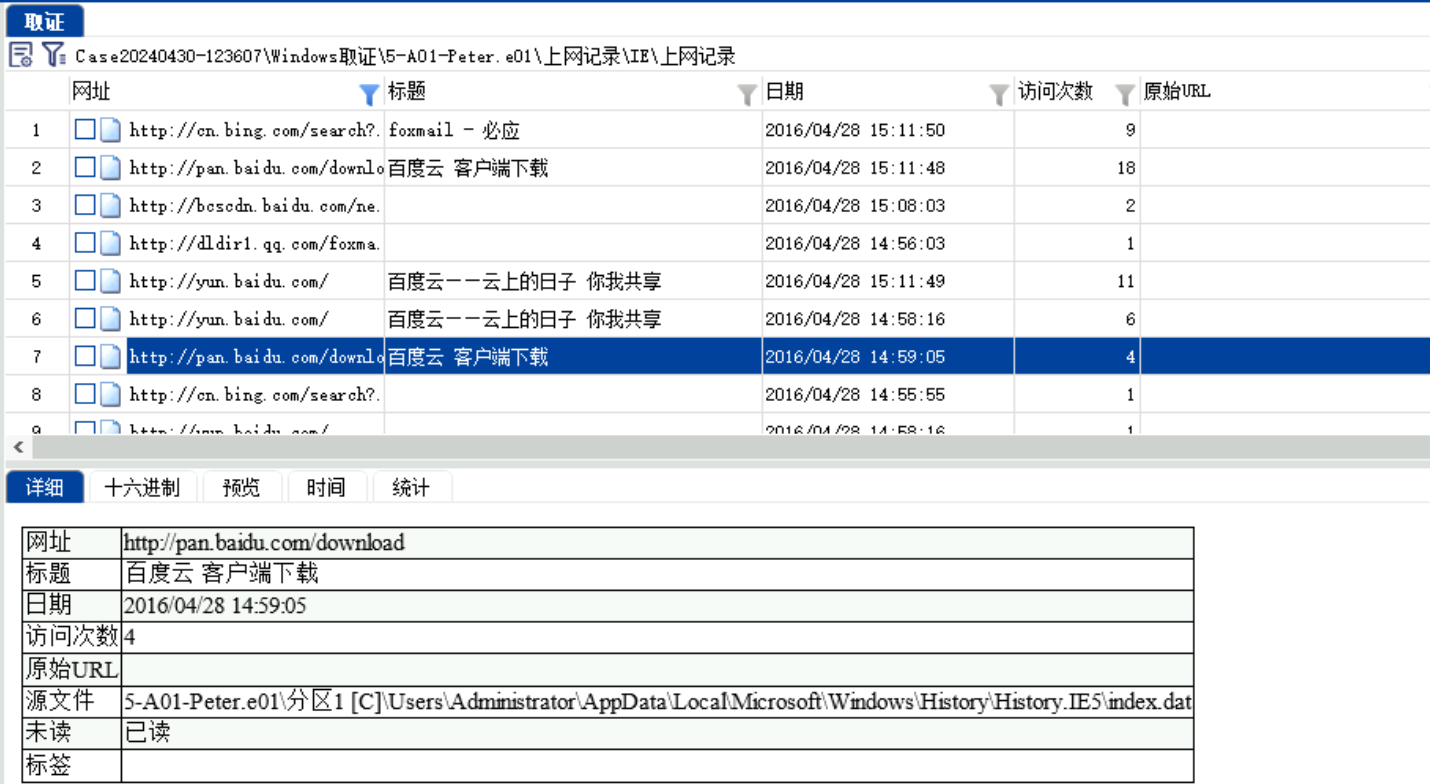


图18 上网下载软件截图

1. 对编号1检材中上网记录中我的电脑文件进行分析，发现存在于2016年4月28日对已拷贝机密数据文件的网络记录，部分信息如图19所示，详细信息见附件“Peter-泄密案附件.zip”。

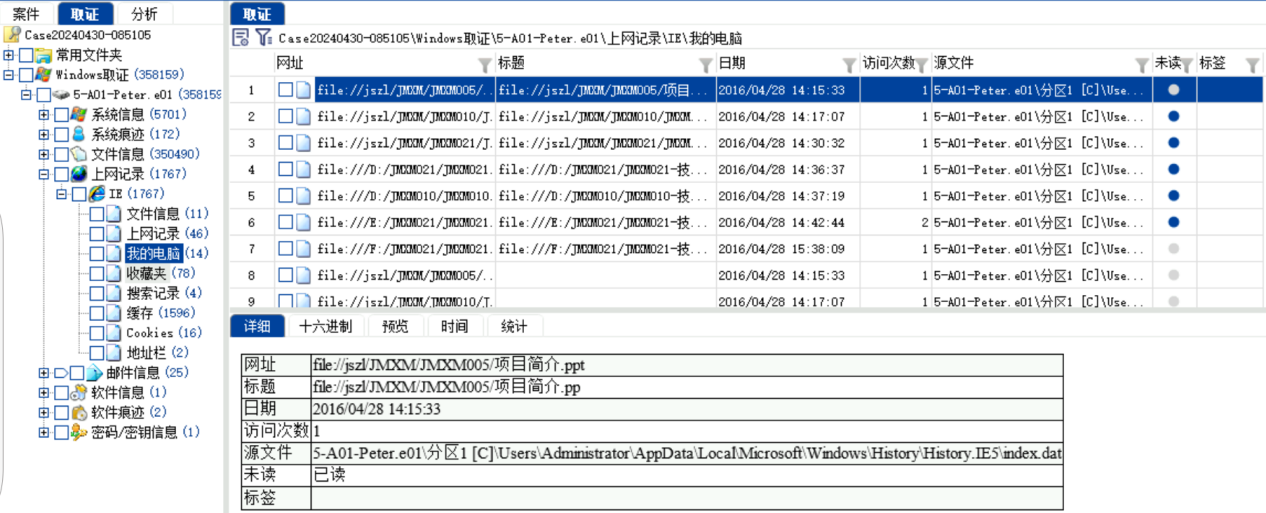


图19 我的电脑上网文件记录截图

1. 对编号1检材中软件痕迹进行分析，发现存在于2016年4月28日14时31分上传“重要资料.rar”到百度云盘账号匹特呃的痕迹，如图20所示。



图20 百度云盘上传文件记录截图

1. 对编号1检材中重要资料文件进行分析，发现该文件即拷贝后“JMXM010”文件夹机密数据的压缩包，即Peter将机密文件压缩后上传了百度云盘，如图21所示。

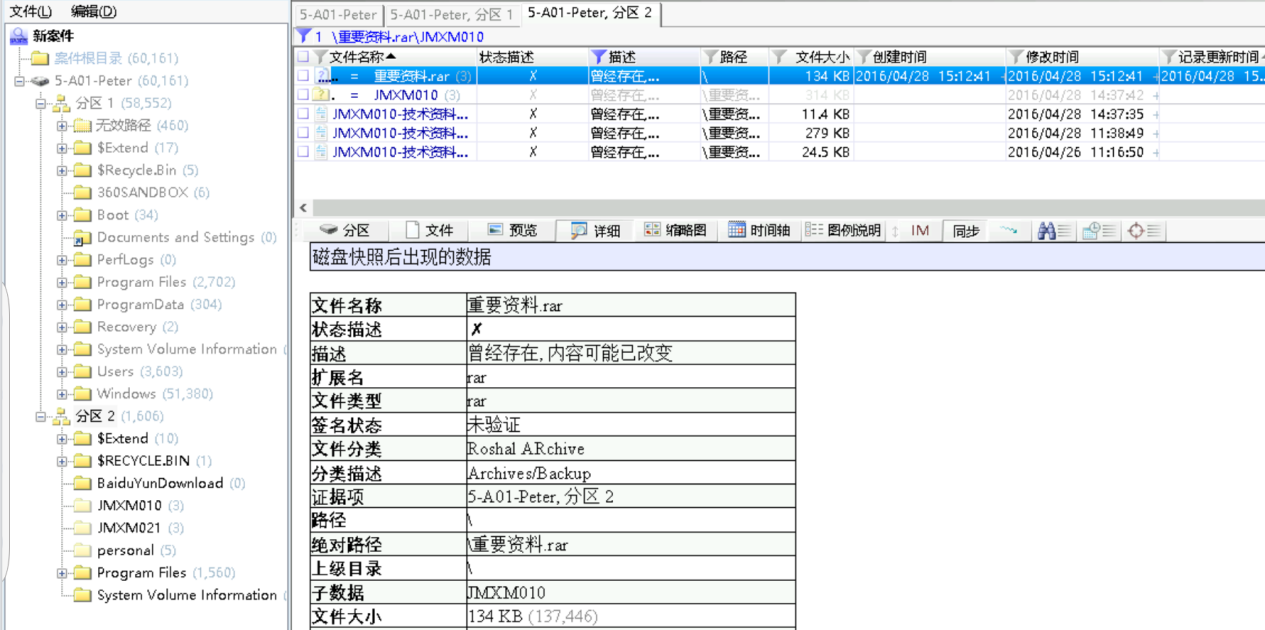


图21 重要资料压缩包内容截图

1. 对编号1检材中电子邮件进行分析，发现存在于2016年4月28日15:12:00-15:33:07的私人邮件，将机密项目文件打包传输到百度云网盘，并分别以附件和网盘链接的方式发送电子邮件外传机密文件的痕迹，违反了公司禁止使用私人邮箱的规定。发件人账号为nlyz\_a@sia.com，收件人分别为bylwlqml@163.com和dzsjjd@qq.com，部分信息见图22和图23，详细信息见附件“Peter-泄密案附件.zip”。

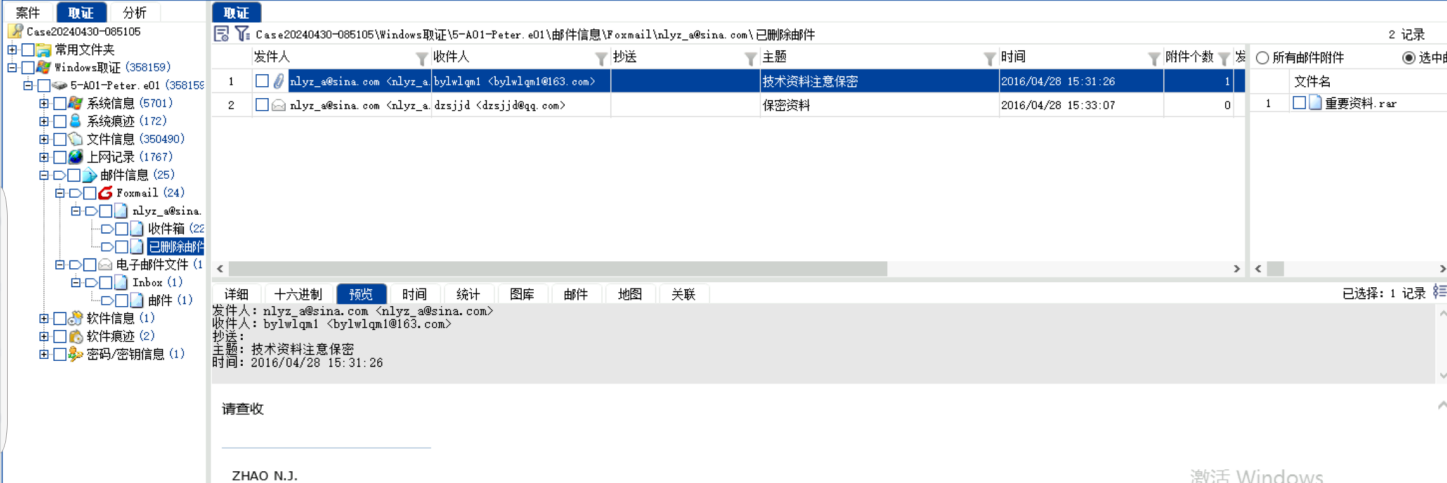


图22 邮件信息1截图



图23 邮件信息2截图

1. 检材1 反取证操作痕迹检验分析
2. 对编号1检材中文件夹状态进行分析，发现存在于2016年4月28日文件删除操作痕迹，JMXM010 、JMXM021和personal三个文件夹被删除，重要资料.rar文件被删除，部分信息见图24和图25，详细信息见附件“Peter-涉密案附件.zip”。



图24 删除文件信息截图



图25 删除文件详细信息截图

1. 对编号 1 检材回收站删除文件进行分析，发现存在于2016年4月28日15:42:39的文件删除操作。Peter于此时删除了百度云管家与Foxmail的快捷方式，如图26所示。

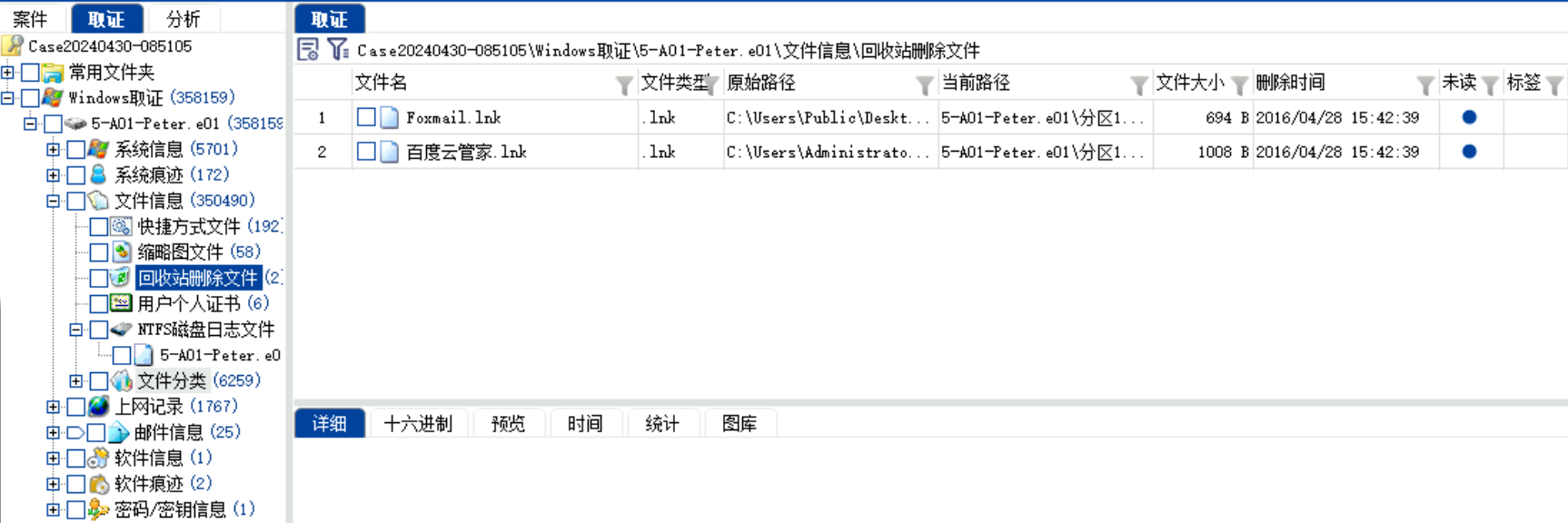


图26 回收站删除快捷方式截图

1. 对编号 1 检材已删除邮件进行分析，发现存在于2016年4月28日的删除邮件操作，删除的邮件是外送的机密数据邮件，部分信息见图27，详细信息见附件“Peter-涉密案附件.zip”。



图27 删除邮件截图

六、鉴定意见

1. 送检材料密封和保护完整。
2. 数据分析：
3. 分析编号1检材中快捷方式和跳转列表，发现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，并且把数据保存到了D盘和F盘。
4. 分析编号1检材中USB使用记录、注册表信息和跳转列表，发现连接私人移动存储设备并挂载到E盘，将机密项目文件拷贝到USB的痕迹。

3、分析编号1检材中打印文件和注册表，发现打印E盘机密文件的痕迹，具体文件为JMXM021-技术资料-项目概况。

4、分析编号1检材中上网记录，发现接入无线网卡并接入名为“P.ZHAO”的无线网络，下载Foxmail和百度云管家两款软件的痕迹。

5、分析编号1检材中快捷方式、跳转列表和文件状态信息，发现Peter将机密文件拷贝从服务器拷贝到D盘、F盘和移动存储设备挂载的E盘。

6、分析编号1检材中软件痕迹和电子邮件，发现将机密项目文件打包压缩后传输到百度云网盘，并以附件和网盘链接的方式分别发送电子邮件外传文件并进行删除邮件的痕迹。

7、分析编号1检材中文件状态、回收站删除文件、已删除邮件，发现Peter泄密后进行了若干反取证操作，具体为删除了拷贝的机密文件，删除下载的软件Foxmail和百度云盘的快捷方式，并将泄密邮件删除。

七、附件

附件一：

文件：Peter-泄密案附件.zip

大小：9491688 字节

MD5: 9E2E3117E8CDD23D2F888D05B8FC8BE7

SHA1: BF81FE8A20180C56E6A7BF17086BA410E2722DBC

司法鉴定人签名 邬雪菲

《司法鉴定执业证》证号：U202112131

司法鉴定人签名 肖凌

《司法鉴定执业证》证号：11111111111

二O二三年五月二日