**华中科技大学网络空间安全学院XX司法鉴定所**

**司法鉴定意见书**

编号： U201911658

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：2022年5月5日。

鉴定材料：送检材料为笔记本本电脑镜像文件。

鉴定日期：2022年5月20日- 2022年5月30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 | XiaoXinPro-13 | 16GB/512GB |  |

检材照片

|  |  |
| --- | --- |
| 检材1正面  IMG_1133 | 检材1反面  IMG_1134 |

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. 鉴证大师 V5.9 1套
5. X-Ways Forensics V19.8.0.0 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 29360-2012 电子物证数据恢复检验规程
9. SF/Z JD0400001-2014 电子数据司法鉴定通用实施规范
10. GA/T 828-2009 电子物证软件功能检验技术规范
11. GA/T 1172-2014 电子邮件检验技术方法

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Z01-Peter.e01镜像文件进行哈希校验，得到MD5值为“5606EA409C6370C7D3D6DFD7DA7AE487”，SHA-1值为“BECD00A12C2D4629C520B1AEF5075716E5475FF4”，如图1所示。

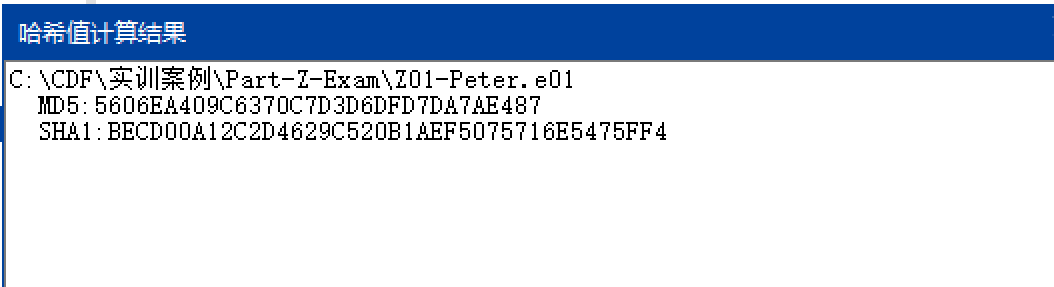


图1

1. 检材1 技术资料访问痕迹检验分析
2. 对编号1检材中注册表SYSTEM进行分析，发现存在于2016年4月28日 14:10:19开机的痕迹部分信息见图2，详细信息见附件“Peter泄密案附件.zip”中Report-sys.html。

L{9X_N[6K3REN(V]O5LBB_R

图2

1. 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14:15:33-14:30:32期间访问服务器机密数据的痕迹，路径为“//jszl/JMXM/JMXM005”和“//jszl/JMXM/JMXM010/”目录下的数个文件，部分信息见图3、图4，详细信息见附件“Peter泄密案附件.zip”。

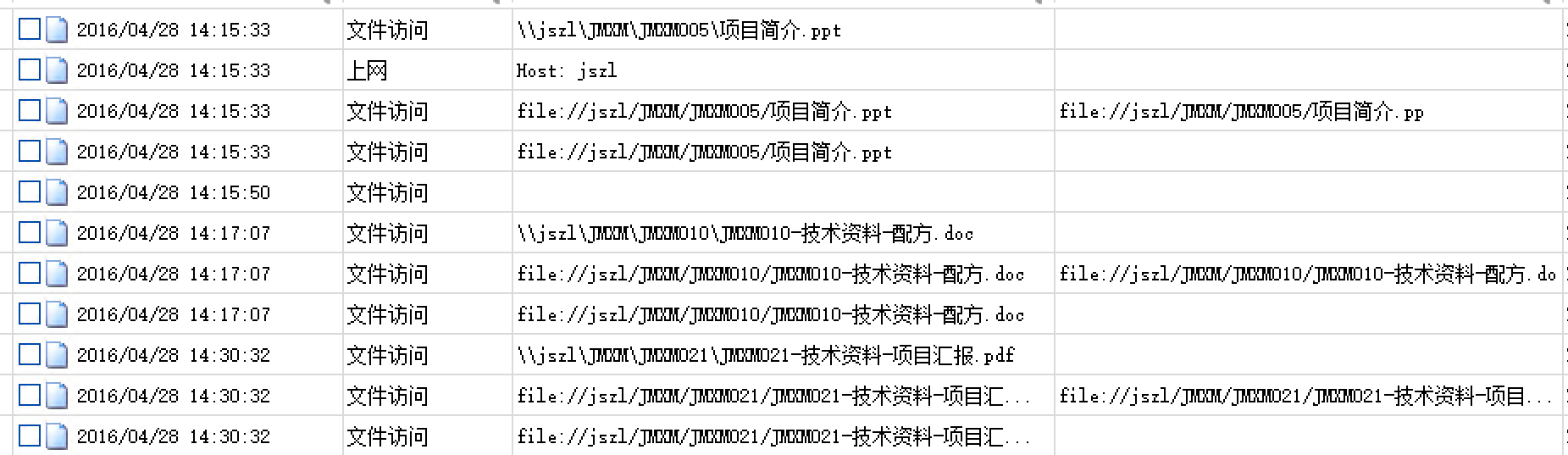


图3

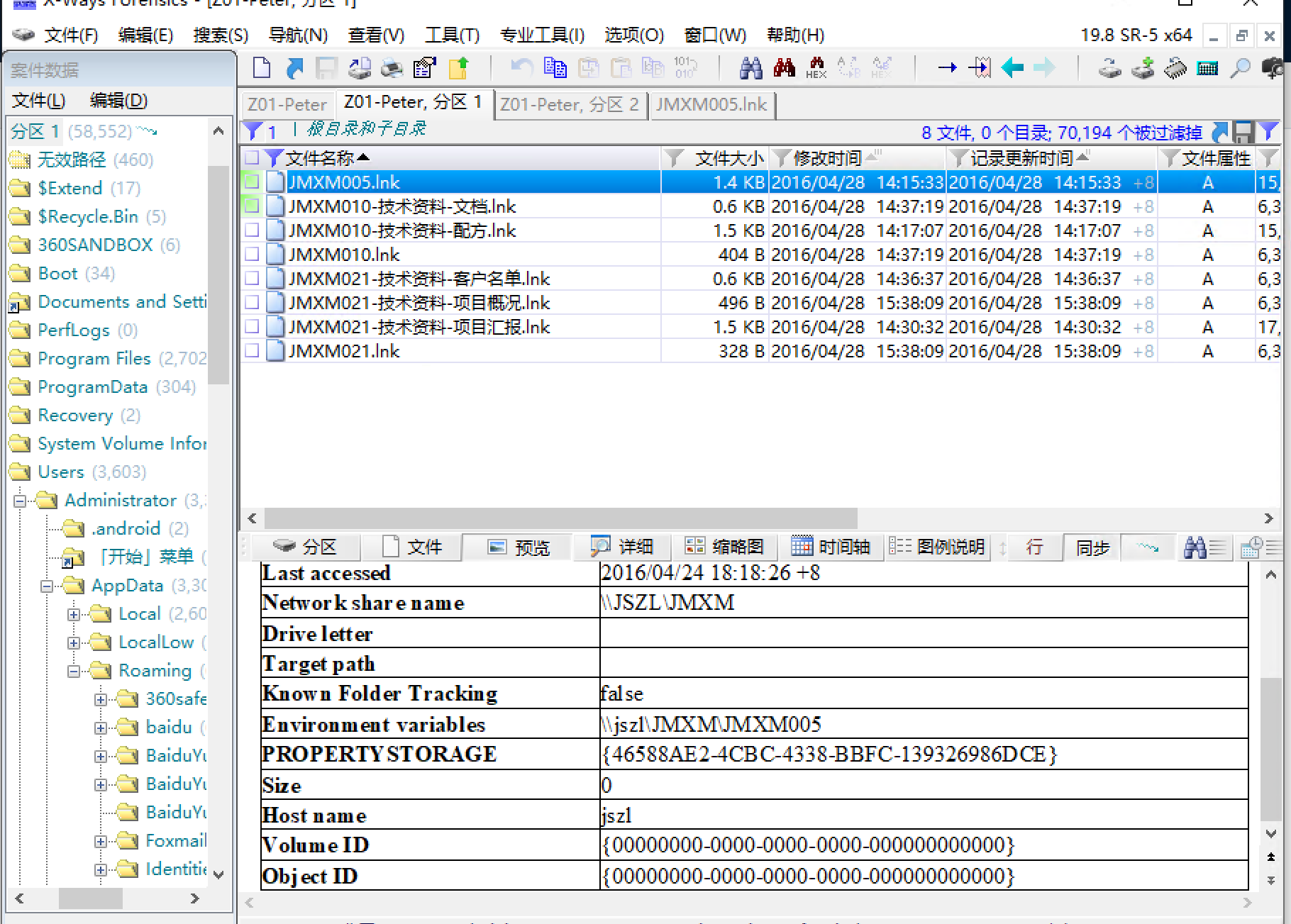


图4

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 14:15:33-14:30:32访问机密数据的痕迹，部分信息见图5、图6，详细信息见附件“Peter泄密案附件.zip”。

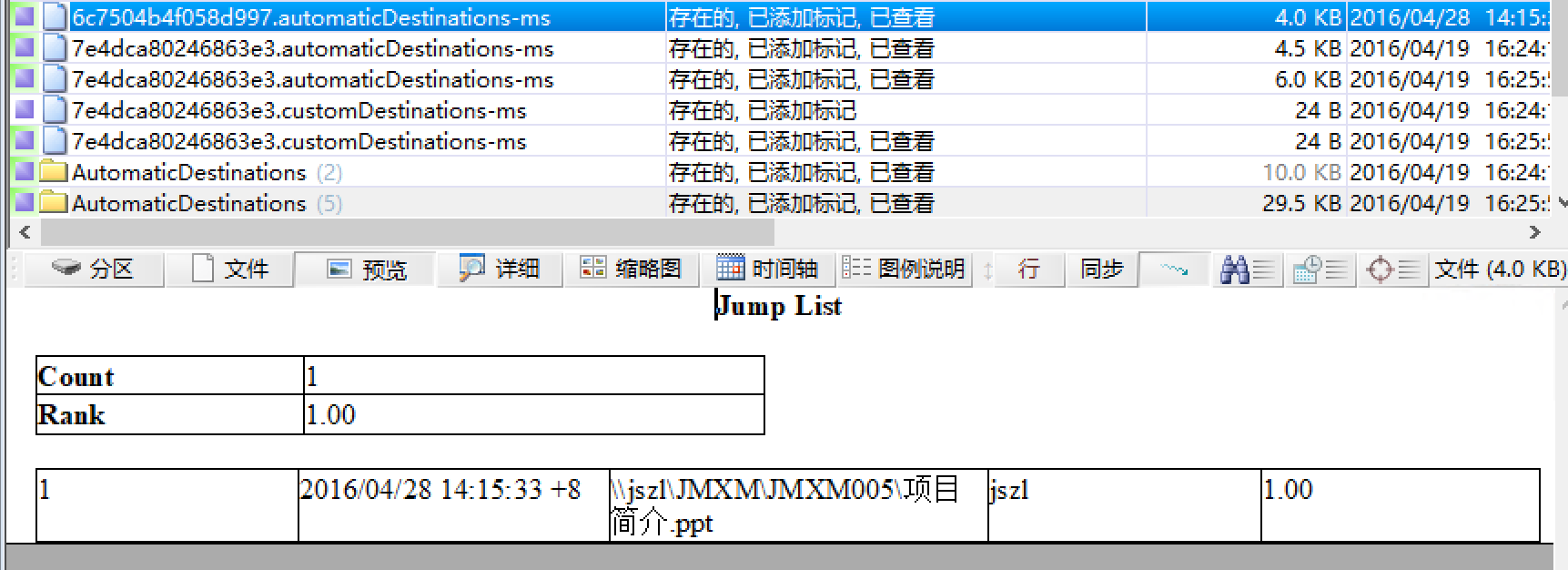


图5

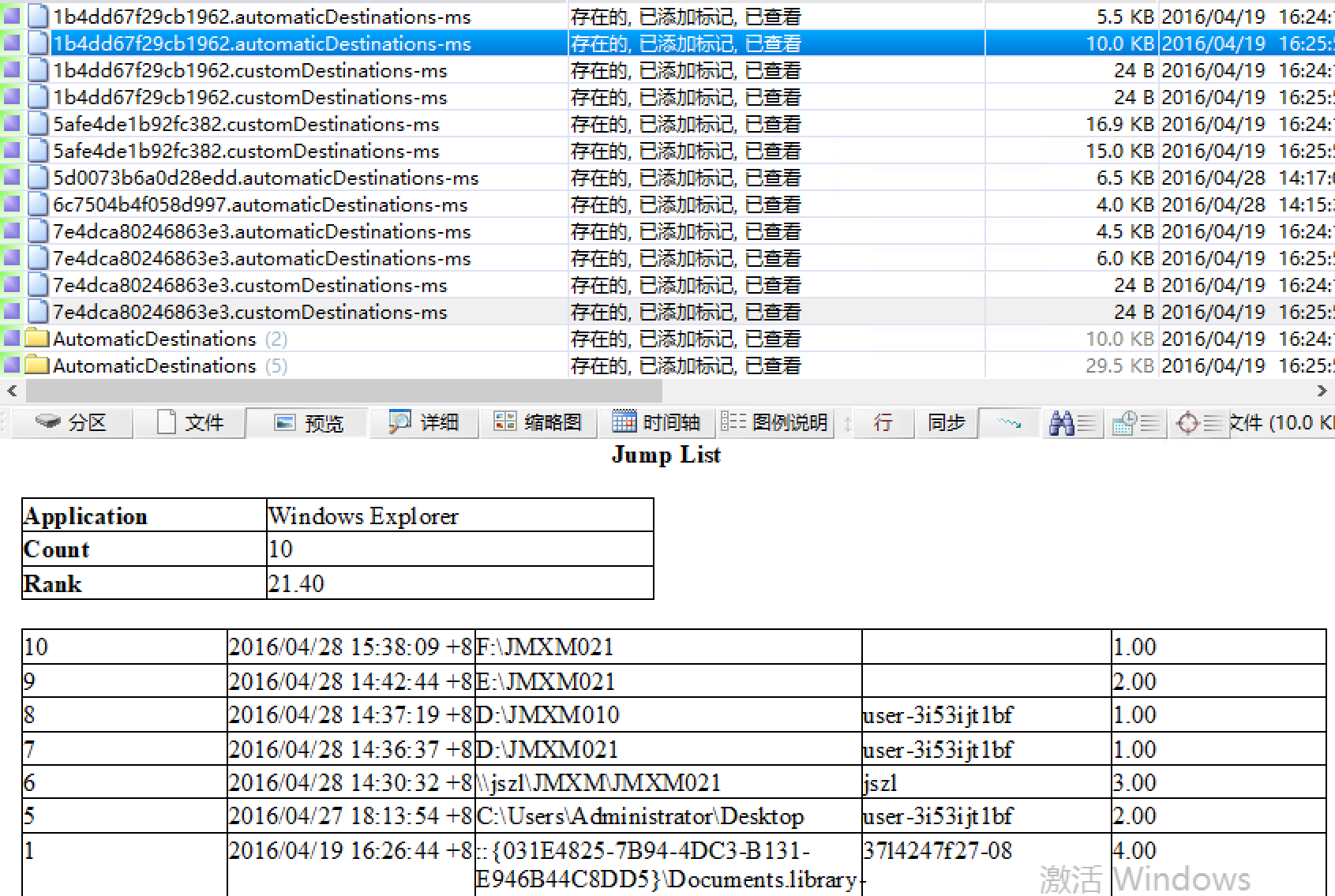


图6

1. 检材1 技术资料复制痕迹检验分析
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 14:33:38机密项目文件由服务器拷贝到D盘JMXM010和JMXM021文件中的痕迹部分信息见图7、图8，详细信息见附件“Peter泄密案附件.zip”。

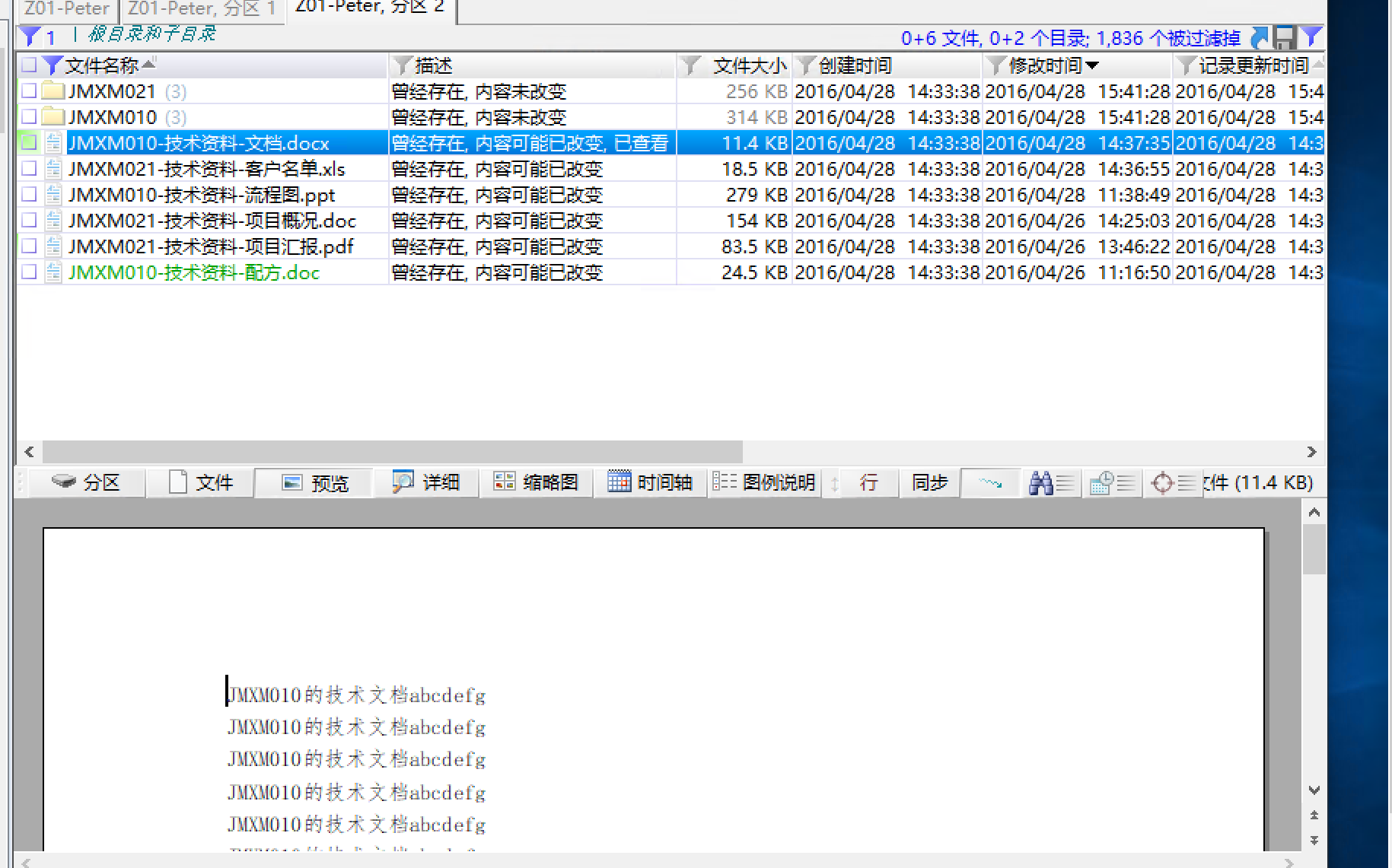


图7

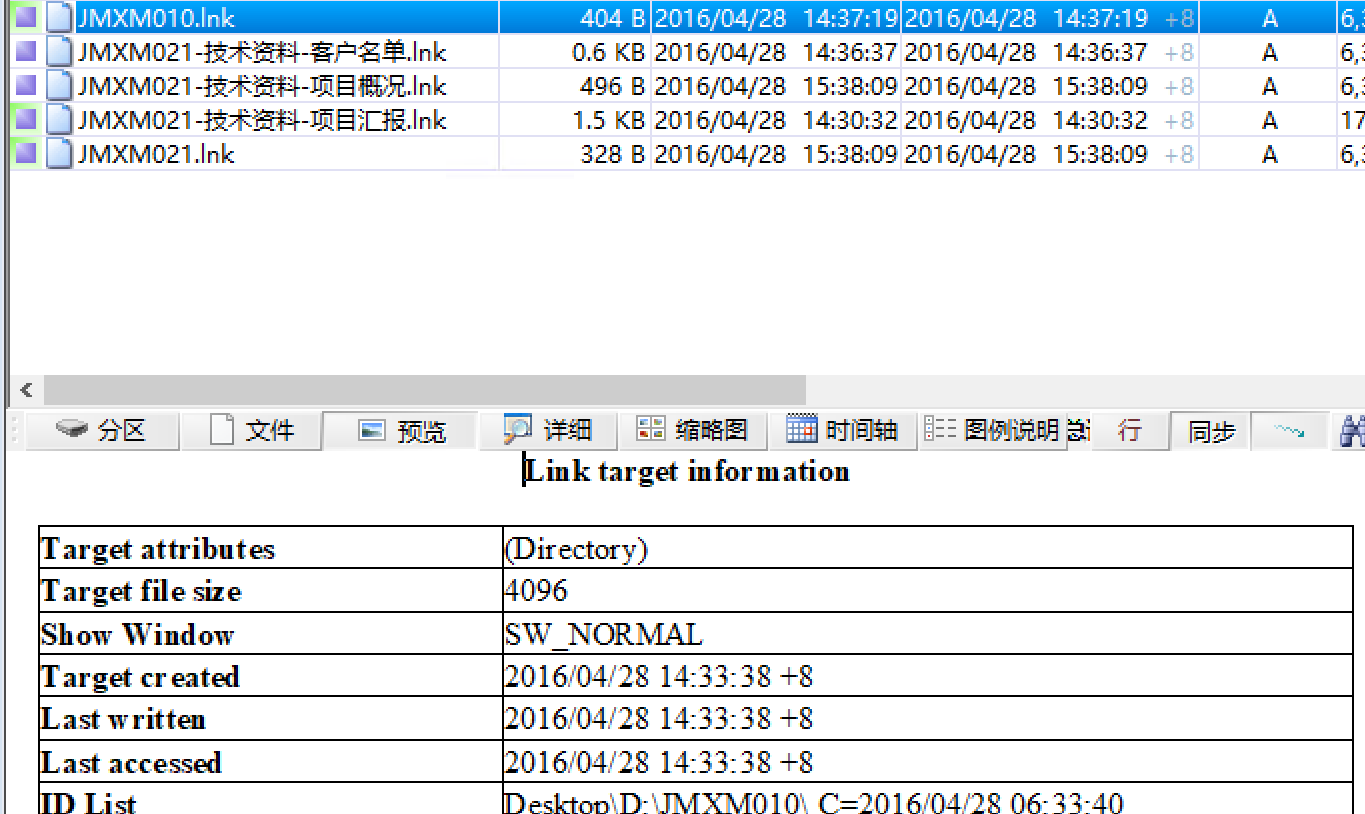


图8

1. 对编号1检材中注册表SYSTEM进行分析，发现存在于2016年4月28日 14:35:37接入U盘，盘符为E的痕迹部分信息见图9，详细信息见附件“Peter泄密案附件.zip”。

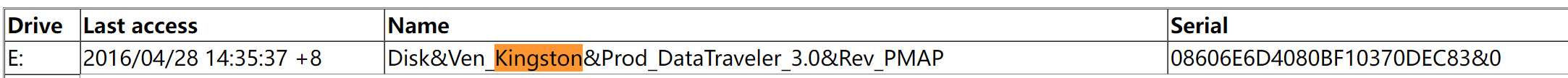


图9

1. 对编号1检材中跳转列表和快捷方式进行分析，发现存在于2016年4月28日 14:38:38拷贝机密项目文件到外接U盘E盘的痕迹部分信息见图10，详细信息见附件“Peter泄密案附件.zip”。

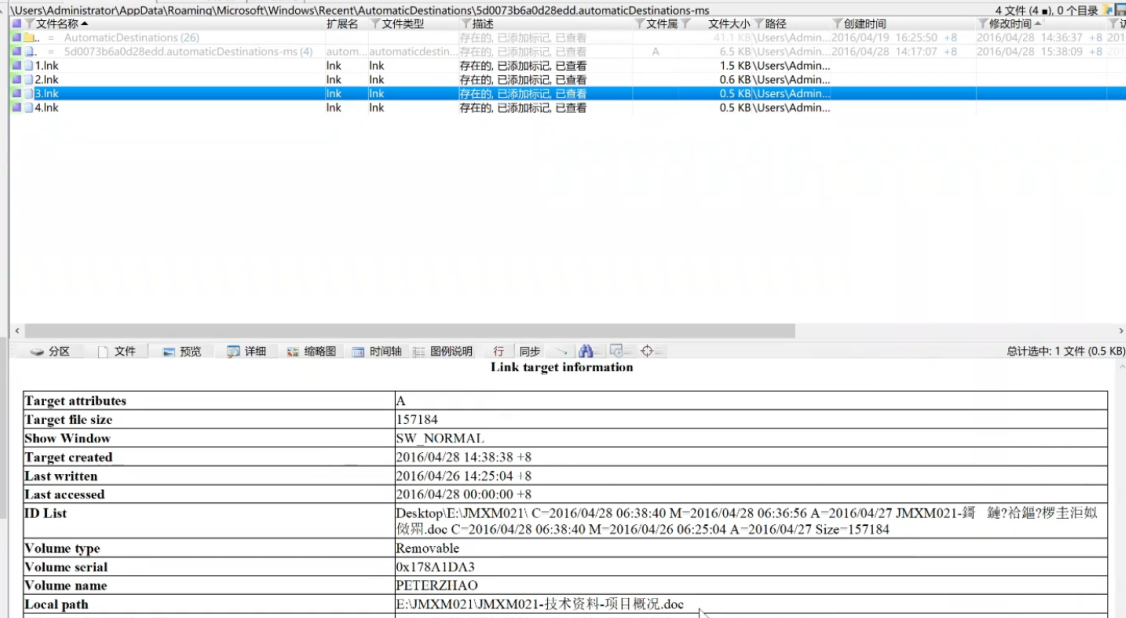


图10

1. 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 14:42:46打印E:\JMXM021\JMXM021\_项目概况.doc文件的痕迹部分信息见图11、图12，详细信息见附件“Peter泄密案附件.zip”。

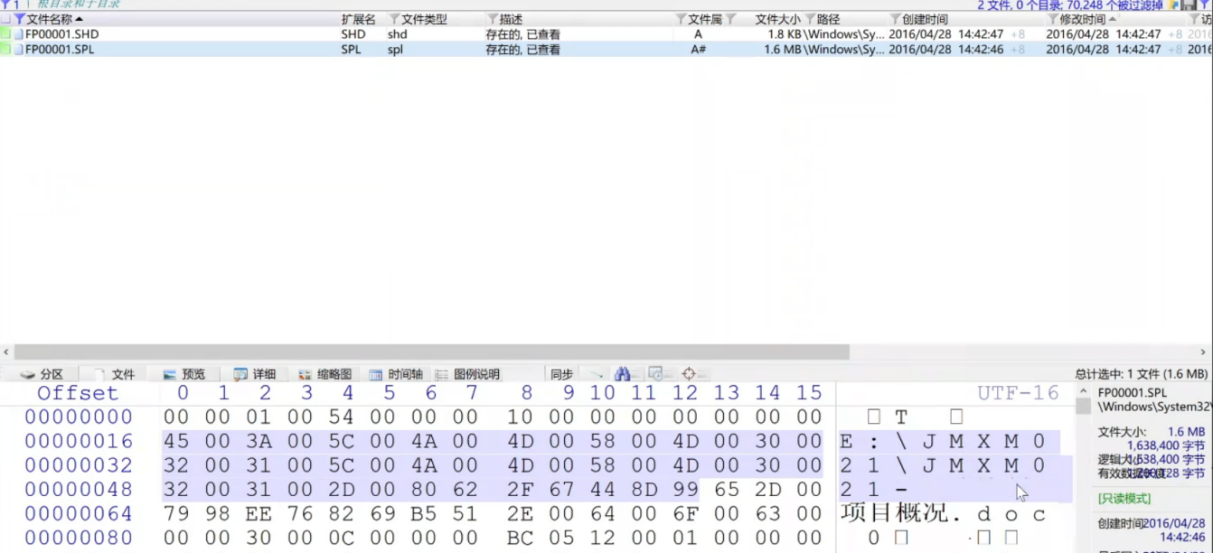


图11



图12

1. 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 15:35拷贝机密文件至盘符为F:的光驱的痕迹部分信息见图13、图14，详细信息见附件“Peter泄密案附件.zip”。



图13

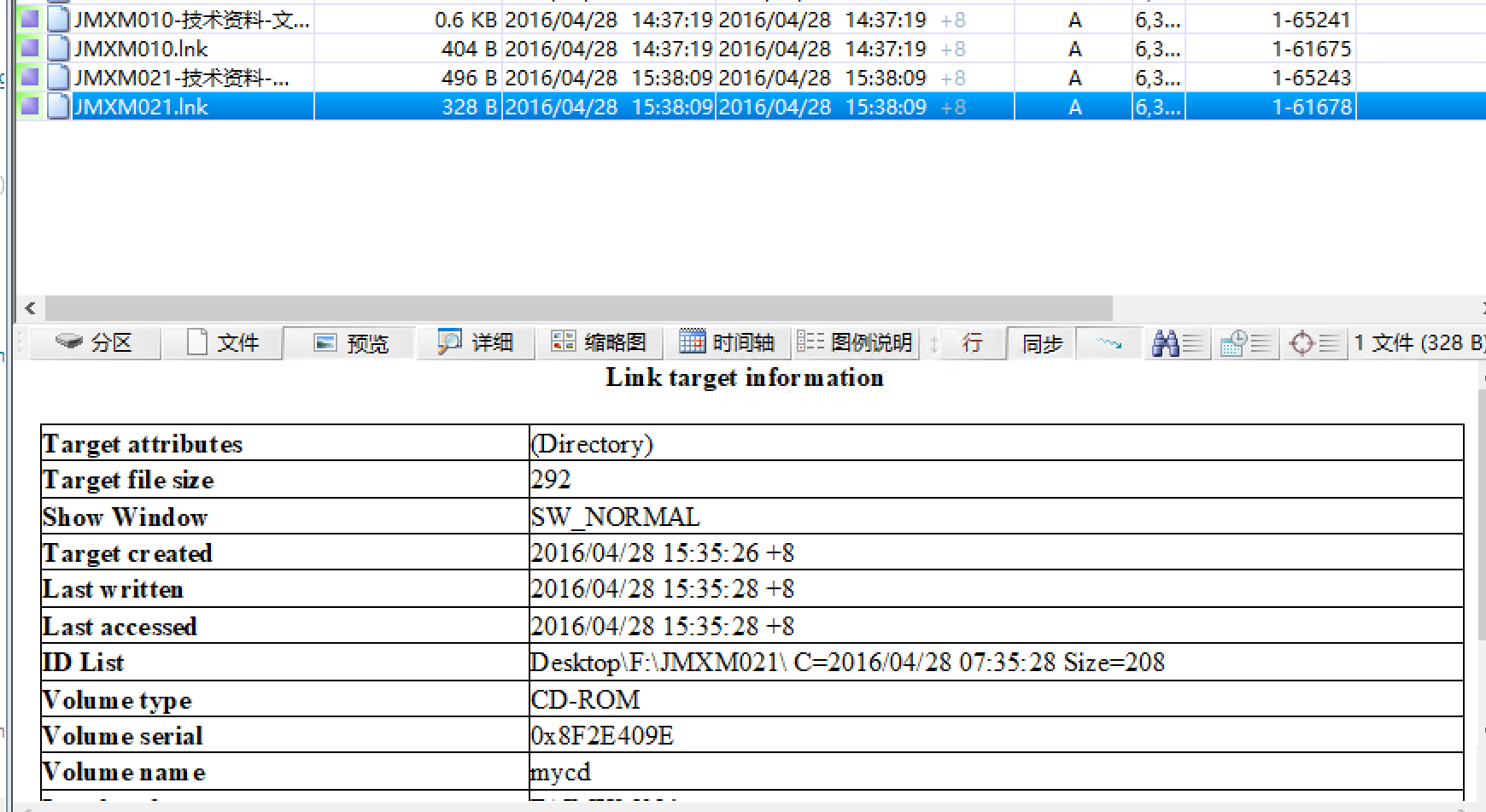


图14

1. 检材1 技术资料外传痕迹检验分析
2. 对编号1检材中注册表NTUSER.DAT 进行分析，发现存在于2016年4月28日””14:47:30接入无线网卡的痕迹，并于14：55：19接入名为“P.ZHAO ”的无线网络，部分信息见图15、图16，详细信息见附件“Peter泄密案附件.zip”。



图15

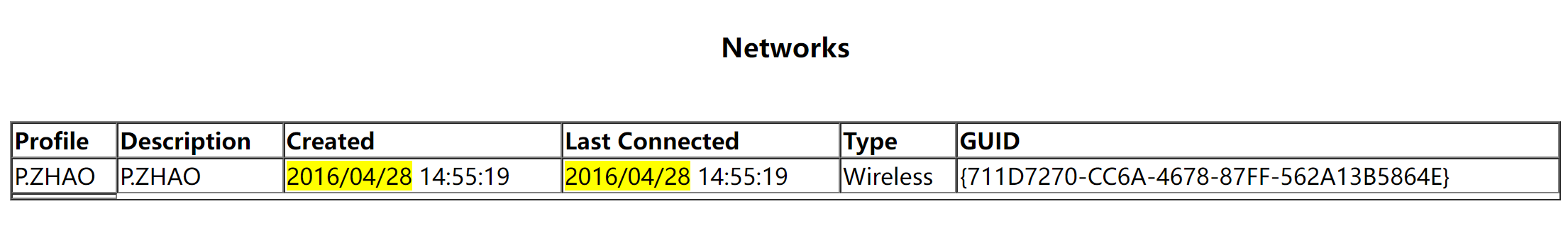


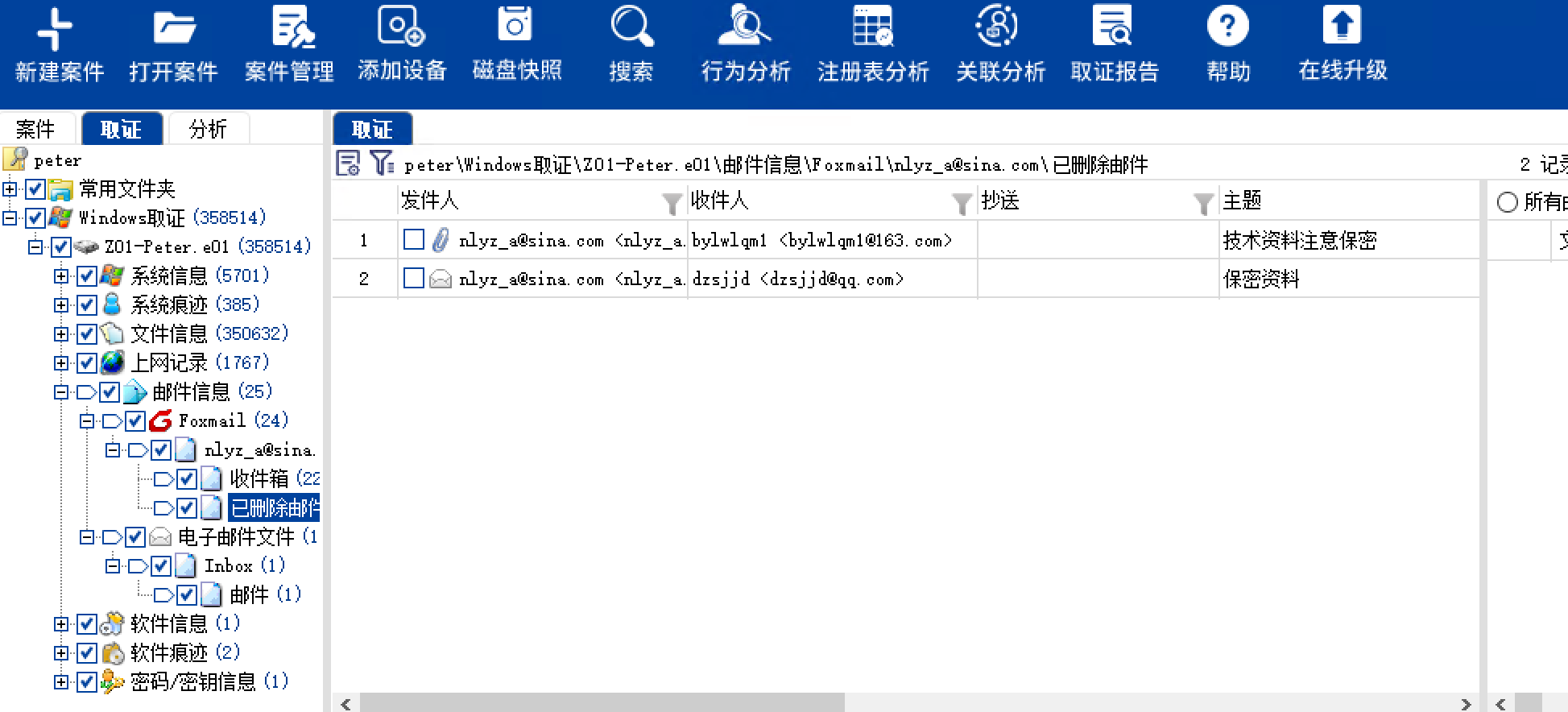
图16

1. 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14:55:37-15:11:49上网下载Foxmail和百度云管家两个软件的痕迹，部分信息见图17，详细信息见附件“Peter泄密案附件.zip”。



图17

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，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文件的痕迹，部分信息见图18、图19、图20、图21，详细信息见附件“Peter泄密案附件.zip”。

图18

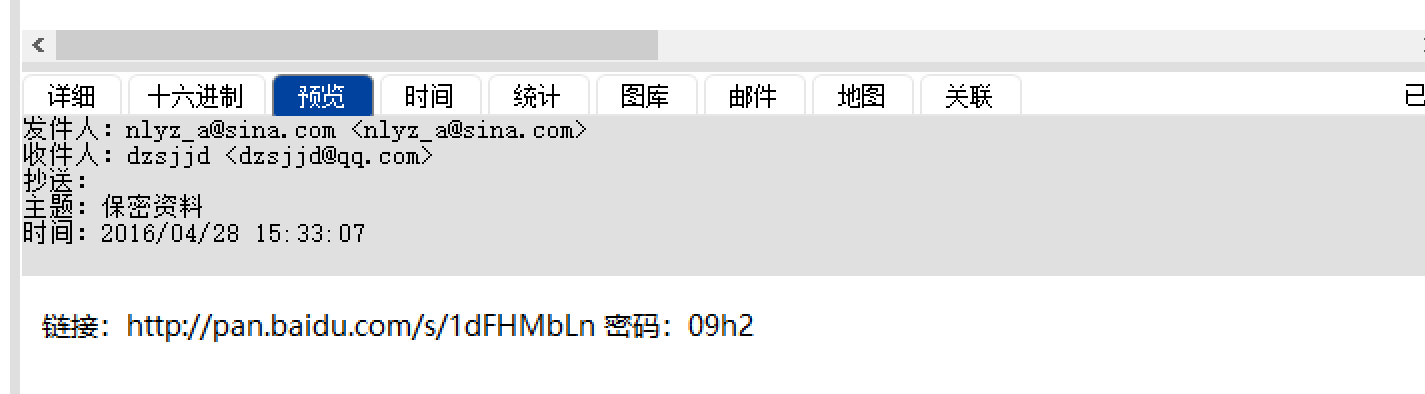


图19

图20

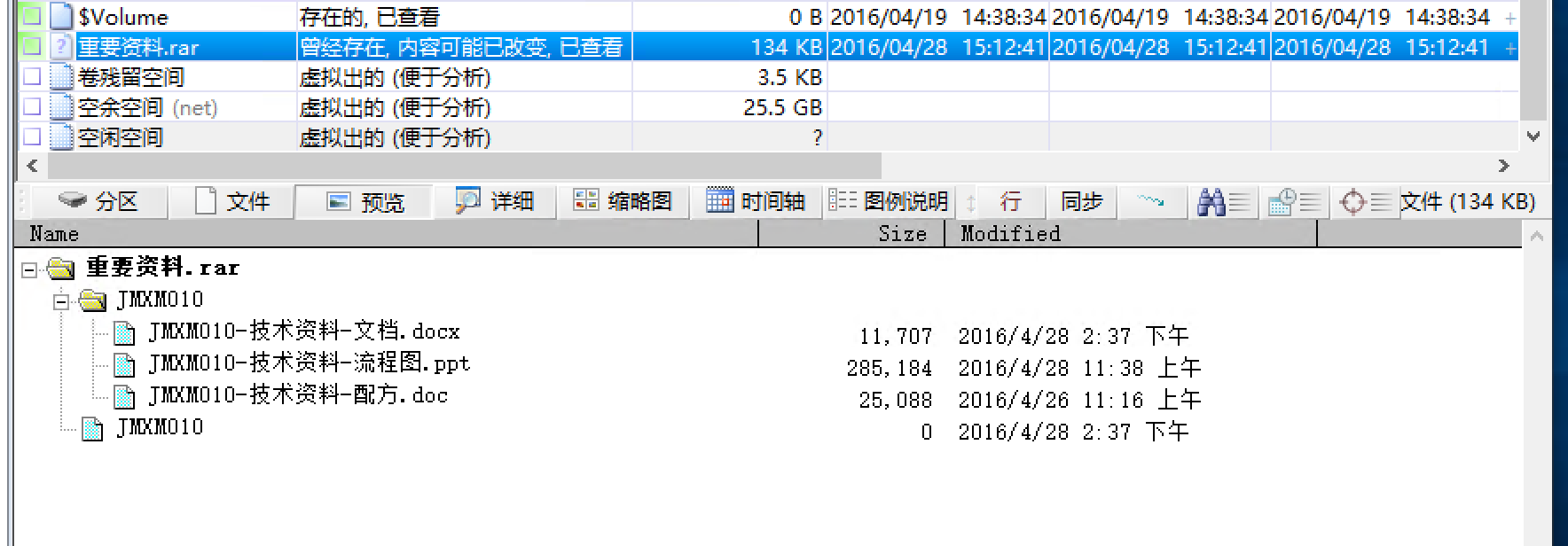


图21

1. 检材1 技术资料窃密反取证痕迹检验分析
2. 对编号1检材中回收站进行分析，发现存在于2016年4月28日15:42:39，Foxmail、百度云的快捷方式删除的痕迹，部分信息见图22、图23，详细信息见附件“Peter泄密案附件.zip”。

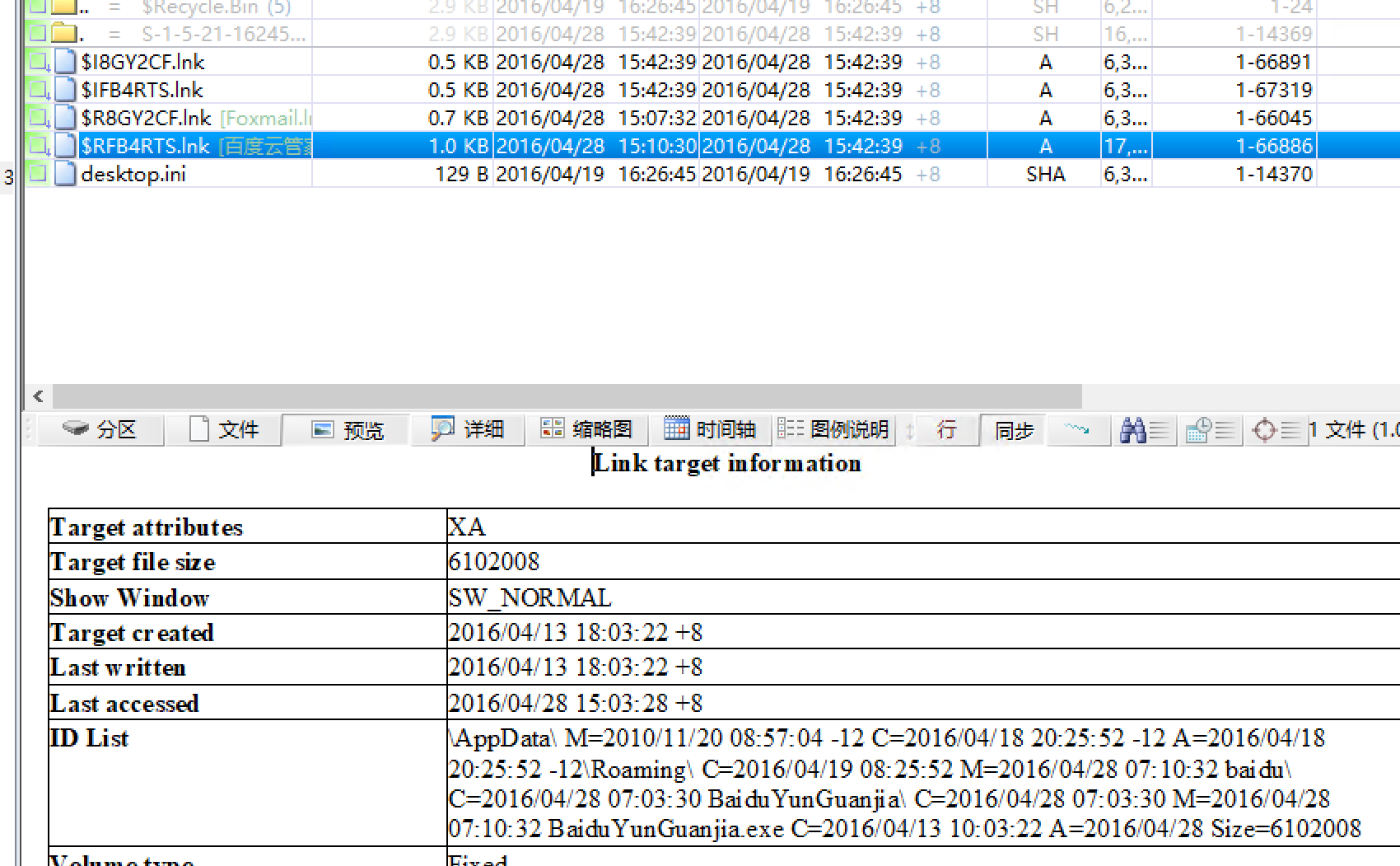


图22

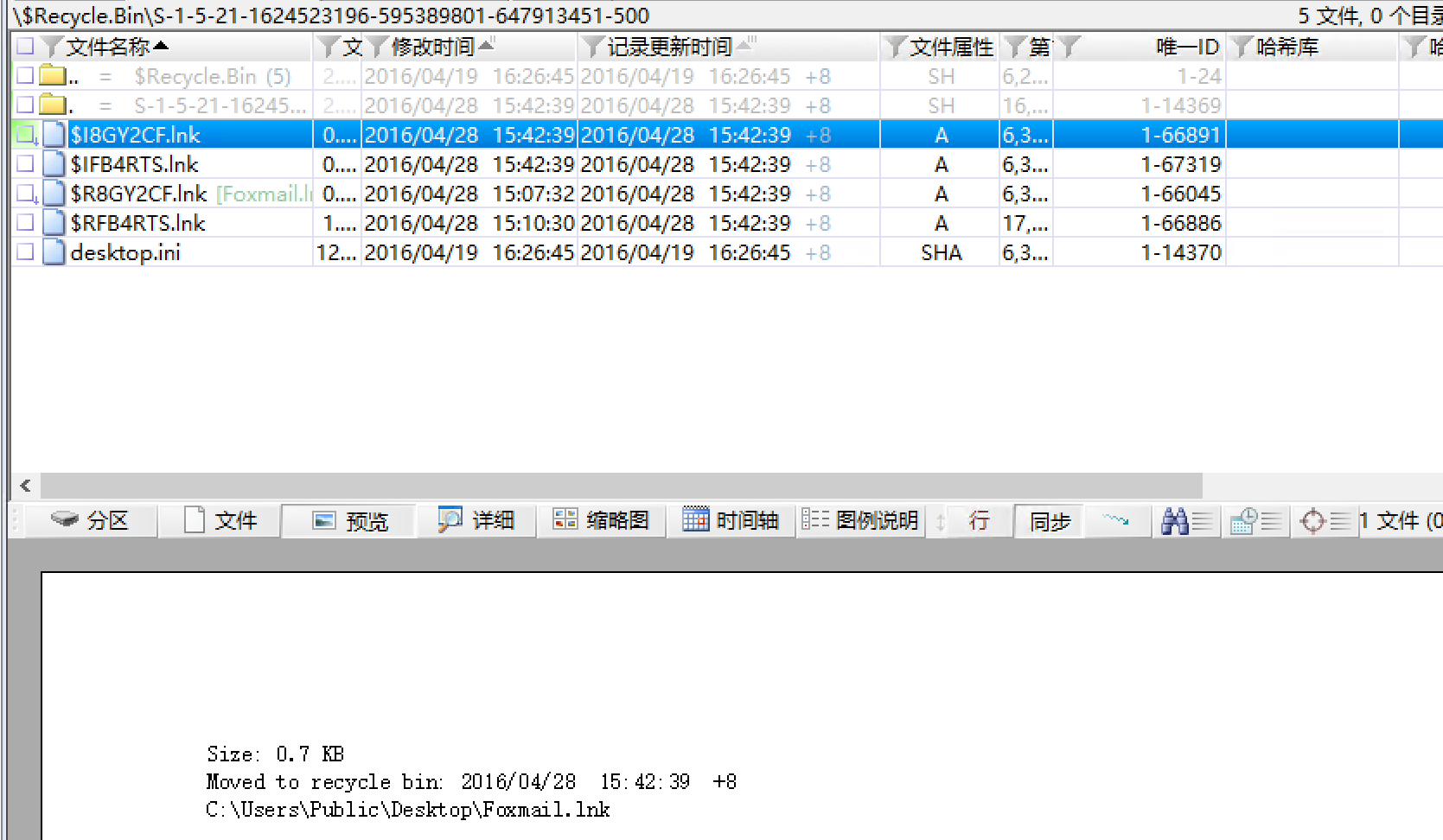


图23

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检材的快捷方式中，发现拷贝机密项目文件至D盘、E盘优盘、F盘光驱的痕迹；
4. 在编号1检材的跳转列表中，发现在D盘、E盘访问机密项目文件的痕迹；
5. 在编号1检材的打印文件和注册表中，发现打印E盘机密文件的痕迹；
6. 在编号1检材的注册表和网页浏览记录中，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；
7. 在编号1检材的电子邮件和百度网盘上传记录中，发现将机密项目文件打包传输到百度云网盘，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；
8. 在编号1检材的回收站中，发现将Foxmail和百度云管家快捷方式删除的痕迹；

七、附件

附件一：

文件：Peter泄密案附件.zip

大小：3,320,745字节

MD5: DD968AD7630CA443380CB4969D32BCD8

SHA1: D121FAFCF31F6EE2014EE8B8C0BD756CA19E3C05

司法鉴定人签名 李欣宇

《司法鉴定执业证》证号：U201911658

司法鉴定人签名 肖凌

《司法鉴定执业证》证号：11111111111

二O二二年五月三十日