

大实验

Peter 泄密案鉴定意见书

目录

4.1 案情说明1

4.2 鉴定要求1

4.3 实验环境1

4.4 报告格式1

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： U202112146

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 20 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

编号	类型	品牌	型号	容量	备注/标注
1	笔记本计算机	联想	拯救者 R7000P	16GB/2T	无

检材照片



四、鉴定过程

（一）取证设备

- | | |
|--------------|-----|
| 1. 天宇宁达取证工作站 | 1 台 |
|--------------|-----|

（二）环境与系统

- | | | |
|---------------------|-----------|-----|
| 1. 裂痕鉴证大师 | V5.12 | 1 套 |
| 2. X-ways Forensics | V19.8.0.0 | 1 套 |

（三）鉴定过程执行的标准和规范

1. GB/T 29362-2012 电子物证数据搜索检验规程
2. GB/T 29360-2012 电子物证数据恢复检验规程
3. GA/T 976-2012 电子数据法庭科学鉴定通用方法
4. SF/Z JD0400001-2014 电子数据司法鉴定通用实施规范
5. GA/T 828-2009 电子物证软件功能检验技术规范

五、分析说明

（一）检材 1 哈希校验

编号 1 检材为笔记本电脑硬盘镜像。使用猎痕鉴证大师对 5-A 01-Peter.e01 镜像进行哈希校验，得到 MD5 值为“9887EED2F3002E72B27E32391E20CE0C”，SHA-1 值为“5E710B2D1505859639A2142773981FC5EA0E3A5D”，如图 1 所示。

备注:

内部名称: C:\CDF\实训案例\5-Windows取证\5-A01-Peter.e01

创建时间: 2024/05/10 02:15:37

注释:

描述:

胡宇

总容量: 55.9 GB
字节数: 60022480896
扇区数: 117231408
扇区大小: 512
磁盘签名: 33CD33CD

哈希: MD5: 9887EED2F3002E72B27E32391E20CE0C
SHA1: 5E710B2D1505859639A2142773981FC5EA0E3A5D

计算哈希值

确定

取消

图 1

(二) 检材 1 技术资料访问痕迹检验分析

1、对编号 1 检材中快捷方式进行分析，发现 Peter 在 2016 年 4 月 28 日 14:15:30 左右访问服务器机密数据（JMXM）的痕迹，其访问了 JMXM005、JMXM010、JMXM021 多个文件，部分信息见图 2，详细信息见附件“Peter 泄密案件附件.zip”。

Case20240512-225736\常用文件夹\所有文件\系统文件							288 文件, 2439 过滤
文件名	标签	类型	类型描述	签名状态	文件分类	路径	
112		iSCSI Initiator.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
113		JMXM005.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
114		JMXM010.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
115		JMXM010-技术资料-配方.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
116		JMXM010-技术资料-文档.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
117		JMXM021.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
118		JMXM021-技术资料-客户名单.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
119		JMXM021-技术资料-项目概况.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
120		JMXM021-技术资料-项目汇报.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
121		Launch Internet Explorer Brow...	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
122		Magnify.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]
123		Magnify.lnk	.lnk	快捷方式	匹配	系统文件	5-A01-Peter.e01\分区1 [C:]

图 2

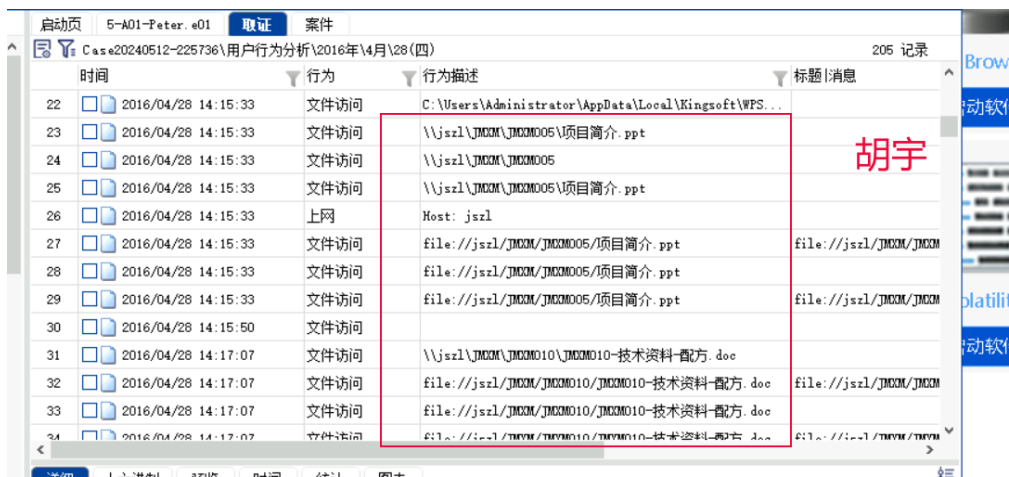
2、对编号 1 检材中跳转列表进行分析，发现 Peter 在 2016 年 4 月 28 日在 D 盘、E 盘、F 盘访问机密数据的痕迹，部分信息见图 3，详细信息见附件“Peter-快捷方式原始文件.zip”。



文件名	扩展名	路径	案件内路径	记录时间	创建
Pictures.library.ms	.libra...	D:\Users\Administrator\AppData...		28431/8/4 5:48:04	2010
Videos.library.ms	.libra...	D:\Users\Administrator\AppData...			2010
JMCOM10-技术资料-文档.docx	.docx	D:\JMCOM10\JMCOM10-技术资料-...		2016/04/28 14:37:19	2016
JMCOM21-技术资料-项目概况.doc	.doc	E:\JMCOM21\JMCOM21-技术资料-...		2016/04/28 14:42:44	2016
JMCOM21-技术资料-项目概况.doc	.doc	F:\JMCOM21\JMCOM21-技术资料-...		2016/04/28 15:38:09	2016
JMCOM21-技术资料-项目汇报.pdf	.pdf	\\jszl\JMCOM\JMCOM21\JMCOM21-...		2016/04/28 14:30:32	2016
项目简介.ppt	.ppt	\\jszl\JMCOM\JMCOM05\项目简介.ppt		2016/04/28 14:15:33	2016
				28431/8/4 5:48:04	
				28431/8/4 5:48:04	
				28431/8/4 5:48:04	
JMCOM21-技术资料-客户名单.xls	.xls	D:\JMCOM21\JMCOM21-技术资料-...		2016/04/28 14:36:37	2016
Documents.library.ms	.libra...	D:\Users\Administrator\AppData...		2016/12/14 22:11:11	2016

图 3

3、对编号 1 检材直接进行行为分析，发现 Peter 在 2016 年 4 月 28 日大量访问机密数据的痕迹，部分信息见图 4、5，详细信息见附件“Peter-快捷方式原始文件.zip”。



时间	行为	行为描述	标题/消息
2016/04/28 14:15:33	文件访问	C:\Users\Administrator\AppData\Local\Kingsoft\WFS...	
2016/04/28 14:15:33	文件访问	\\jszl\JMCOM\JMCOM05\项目简介.ppt	
2016/04/28 14:15:33	文件访问	\\jszl\JMCOM\JMCOM05	
2016/04/28 14:15:33	文件访问	\\jszl\JMCOM\JMCOM05\项目简介.ppt	
2016/04/28 14:15:33	上网	Host: jszl	
2016/04/28 14:15:33	文件访问	file://jszl/JMCOM/JMCOM05/项目简介.ppt	file://jszl/JMCOM/JMCOM
2016/04/28 14:15:33	文件访问	file://jszl/JMCOM/JMCOM05/项目简介.ppt	file://jszl/JMCOM/JMCOM
2016/04/28 14:15:33	文件访问	file://jszl/JMCOM/JMCOM05/项目简介.ppt	file://jszl/JMCOM/JMCOM
2016/04/28 14:15:50	文件访问		
2016/04/28 14:17:07	文件访问	\\jszl\JMCOM\JMCOM10\JMCOM10-技术资料-配方.doc	
2016/04/28 14:17:07	文件访问	file://jszl/JMCOM/JMCOM10\JMCOM10-技术资料-配方.doc	file://jszl/JMCOM/JMCOM
2016/04/28 14:17:07	文件访问	file://jszl/JMCOM/JMCOM10\JMCOM10-技术资料-配方.doc	file://jszl/JMCOM/JMCOM
2016/04/28 14:17:07	文件访问	file://jszl/JMCOM/JMCOM10\JMCOM10-技术资料-配方.doc	file://jszl/JMCOM/JMCOM

图 4

启动页	5-A01-Peter.e01	取证	案件
Case20240512-225736\用户行为分析\2016年\4月\28(四)			205 记录
时间	行为	行为描述	标题 消息
52	2016/04/28 14:36:37	文件访问	D:\JMXM021\JMXM021-技术资料-客户名单.xls
53	2016/04/28 14:36:37	文件访问	D:\JMXM021\JMXM021-技术资料-客户名单.xls
54	2016/04/28 14:36:37	上网	Host: 搜\$ 随便?
55	2016/04/28 14:36:37	文件访问	D:\JMXM021\JMXM021-技术资料-客户名单.xls
56	2016/04/28 14:36:37	文件访问	D:\JMXM021\JMXM021-技术资料-客户名单.xls
57	2016/04/28 14:36:37	文件访问	D:\JMXM021\JMXM021-技术资料-客户名单.xls
58	2016/04/28 14:37:14	文件访问	D:\JMXM010
59	2016/04/28 14:37:14	文件访问	D:\JMXM010
60	2016/04/28 14:37:19	文件访问	D:\JMXM010\JMXM010-技术资料-文档.docx
61	2016/04/28 14:37:19	文件访问	D:\JMXM010
62	2016/04/28 14:37:19	文件访问	D:\JMXM010\JMXM010-技术资料-文档.docx
63	2016/04/28 14:37:19	文件访问	D:\JMXM010\JMXM010-技术资料-文档.docx
64	2016/04/28 14:37:19	文件访问	D:\JMXM010\JMXM010-技术资料-文档.docx

图 5

(三) 检材 1 技术资料复制痕迹检验分析

1、对编号 1 检材中快捷方式和文件创建信息进行分析，发现 Peter 在 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 6、图 7，详细信息见附件“Peter 泄密案附件.zip”。

名称	类型	大小	路径	目标路径	案件内路径
106 JMXM010-技术资料-配.doc		24.5 KB	5-A01-Peter.e01\分区1...	\\jsz1\JMXM\JMXM010\J...	
107 JMXM010-技术资料-文.docx		15.4 KB	5-A01-Peter.e01\分区1...	D:\JMXM010\JMXM010-技...	
108 JMXM021.lnk	文件夹		5-A01-Peter.e01\分区1...	F:\JMXM021	
109 JMXM021-技术资料-客.xls		23 KB	5-A01-Peter.e01\分区1...	D:\JMXM021\JMXM021-技...	
110 JMXM021-技术资料-项.doc		153.5 KB	5-A01-Peter.e01\分区1...	F:\JMXM021\JMXM021-技...	
111 JMXM021-技术资料-项.pdf		83.5 KB	5-A01-Peter.e01\分区1...	\\jsz1\JMXM\JMXM021\J...	
112 Windows Update.lnk			5-A01-Peter.e01\分区1...		

胡宇

名称	JMXM010-技术资料-文档.lnk
类型	.docx
大小	15.4 KB
路径	5-A01-Peter.e01\分区1 [C]\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\JMXM010-技术资料-文档.lnk
目标路径	D:\JMXM010\JMXM010-技术资料-文档.docx
案件内路径	
创建时间	2016/04/28 14:33:38

图 6

Case20240512-225736\Windows取证\5-A01-Peter. e01\文件信息\快捷方式文件							284 记录
名称	类型	大小	路径	目标路径	案件内路径		
106	JMXM010-技术资料-配. .doc	24.5 KB	5-A01-Peter. e01\分区1...	\\jszl\JMXM\JMXM010\J...			
107	JMXM010-技术资料-文. .docx	15.4 KB	5-A01-Peter. e01\分区1...	D:\JMXM010\JMXM010-技...			
108	JMXM021. lnk	文件夹	5-A01-Peter. e01\分区1...	F:\JMXM021			
109	JMXM021-技术资料-客. .xls	23 KB	5-A01-Peter. e01\分区1...	D:\JMXM021\JMXM021-技...			
110	JMXM021-技术资料-项. .doc	153.5 KB	5-A01-Peter. e01\分区1...	F:\JMXM021\JMXM021-技...			
111	JMXM021-技术资料-项. .pdf	83.5 KB	5-A01-Peter. e01\分区1...	\\jszl\JMXM\JMXM021\J...			
112	Windows Update. lnk		5-A01-Peter. e01\分区1...				

名称	JMXM021-技术资料-客户名单. lnk
类型	.xls
大小	23 KB
路径	5-A01-Peter. e01\分区1 [C]\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\JMXM021-技术资料-客户名单. lnk
目标路径	D:\JMXM021\JMXM021-技术资料-客户名单. xls
案件内路径	
创建时间	2016/04/28 14:33:38

图 7

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 Peter 在 2016 年 4 月 28 日 15:35:26 机密项目文件由服务器拷贝到 F 盘，F 盘类型为 CD-ROM，即光盘，JMXM010 和 JMXM021 文件中的痕迹部分信息见图 8、图 9，详细信息见附件“Peter 泄密案附件.zip”。

启动页 5-A01-Peter. e01 取证 案件							284 记录
名称	类型	大小	路径	目标路径	案件内路径		
106	JMXM010-技术资料-配. .doc	24.5 KB	5-A01-Peter. e01\分区1...	\\jszl\JMXM\JMXM010\J...			
107	JMXM010-技术资料-文. .docx	15.4 KB	5-A01-Peter. e01\分区1...	D:\JMXM010\JMXM010-技...			
108	JMXM021. lnk	文件夹	5-A01-Peter. e01\分区1...	F:\JMXM021			
109	JMXM021-技术资料-客. .xls	23 KB	5-A01-Peter. e01\分区1...	D:\JMXM021\JMXM021-技...			
110	JMXM021-技术资料-项. .doc	153.5 KB	5-A01-Peter. e01\分区1...	F:\JMXM021\JMXM021-技...			
111	JMXM021-技术资料-项. .pdf	83.5 KB	5-A01-Peter. e01\分区1...	\\jszl\JMXM\JMXM021\J...			
112	Windows Update. lnk		5-A01-Peter. e01\分区1...				

名称	JMXM021. lnk
类型	文件夹
大小	
路径	5-A01-Peter. e01\分区1 [C]\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\JMXM021. lnk
目标路径	F:\JMXM021
案件内路径	
创建时间	2016/04/28 15:35:26
修改时间	2016/04/28 15:35:28
访问时间	2016/04/28 15:35:28

图 8

Case20240512-225736\Windows取证\5-A01-Peter.e01\文件信息\快捷方式文件						284 记录
名称	类型	大小	路径	目标路径	案件内路径	
JMXM010-技术资料-配...	.doc	24.5 KB	5-A01-Peter.e01\分区1...	\\jszl\JMXM\JMXM010\J...		
JMXM010-技术资料-文...	.docx	15.4 KB	5-A01-Peter.e01\分区1...	D:\JMXM010\JMXM010-技...		
JMXM021.lnk	文件夹		5-A01-Peter.e01\分区1...	F:\JMXM021		胡宇
JMXM021-技术资料-客...	.xls	23 KB	5-A01-Peter.e01\分区1...	D:\JMXM021\JMXM021-技...		
JMXM021-技术资料-项...	.doc	153.5 KB	5-A01-Peter.e01\分区1...	F:\JMXM021\JMXM021-技...		
JMXM021-技术资料-项...	.pdf	83.5 KB	5-A01-Peter.e01\分区1...	\\jszl\JMXM\JMXM021\J...		
Windows Update.lnk			5-A01-Peter.e01\分区1...			

名称	JMXM021-技术资料-项目概况.lnk
类型	.doc
大小	153.5 KB
路径	5-A01-Peter.e01\分区1 [C]\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\JMXM021-技术资料-项目概况.lnk
目标路径	F:\JMXM021\JMXM021-技术资料-项目概况.doc
案件内路径	
创建时间	2016/04/28 15:35:26

图 9

3、对编号 1 检材中 usb 的使用情况进行分析,发现 Peter 在 2016 年 4 月 28 日 14:35:36, 有插入一个型号为 Kingston DataTraveler 3.0 的 USB Device, 其挂载盘符为 E 盘, 部分信息如图 10, 详细信息见附件“Peter 泄密案件附件.zip”。

Case20240512-225736\Windows取证\5-A01-Peter.e01\系统痕迹\USB设备使用记录

16 记录

序列号	型号	第一次使用时间	最后一次使用时间	挂载盘符	注册表
8	1.0	Port_#0003. Hub_#0002	2016/04/28 14:49:25	2016/04/28 14:49:41	Control
9	W22021305271613460	Port_#0001. Hub_#0002	2016/04/27 20:09:15	2016/04/28 14:10:16	Control
10	08606E6D4080BF10370DEC83	Kingston DataTraveler 3.0 ...	2016/04/28 14:35:36	2016/04/28 14:35:36	E: Control
11	6a2d9edb8da0a2	Port_#0002. Hub_#0001	2016/04/19 16:23:55	2016/04/28 14:10:16	Control
12	6a2d9edb8da0a1	Port_#0001. Hub_#0001	2016/04/19 16:24:00	2016/04/28 14:10:16	Control
13	7a2f9d147f0a0000	0002.0000.0000.001.000.000...	2016/04/19 16:24:02	2016/04/28 14:10:16	Control
14	7a2f9d147f0a0001	0002.0000.0000.001.000.000...	2016/04/19 16:24:02	2016/04/28 14:10:16	Control

详细

十六进制

预览

时间

统计

已选择: 1 记录

序列号	08606E6D4080BF10370DEC83
型号	Kingston DataTraveler 3.0 USB Device
第一次使用时间	2016/04/28 14:35:36
最后一次使用时间	2016/04/28 14:35:36
挂载盘符	E:
注册表路径	ControlSet001\Enum\USB\VID_0951&PID_1666
源文件	5-A01-Peter.e01\分区1 [C]\格式化恢复\Windows\System32\config\SYSTEM
未读	已读
标签	

胡宇

图 10

4、对编号 1 检材中用户行为进行分析,发现 Peter 在 2016 年 4 月 28 日有过对 E 盘机密文件进行访问的操作, 而根据上述信息可知 E 盘是用户插入的 USB Device, 则可证明 Peter 将绝密信息复制到了

自己的U盘中，部分信息如图11，详细信息见附件“Peter泄密案件附件.zip”。

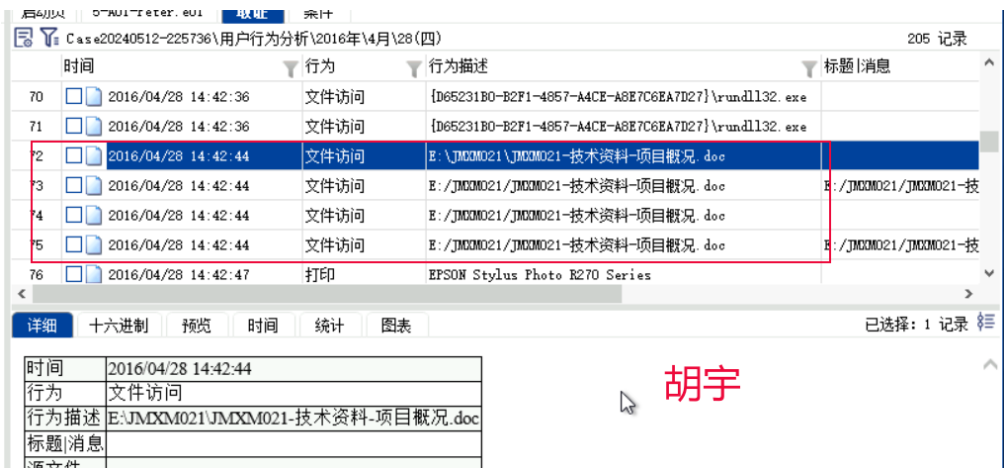


图 11

5、对编号 1 检材中打印文件进行分析，发现 Peter 在 2016 年 4 月 28 日 14:42:47 打印了源文件 FP00001.SHD，查看该源文件发现就是 E:\JMXM021\JMXM021_项目概况.doc 文件，部分信息如图 12、13，详细信息见附件“Peter泄密案件附件.zip”。



图 12

文件名称	扩展名	文件类型	描述	文件属性	文件大小	路径	创建时间	修改时间
FP00001.SHD	SHD	shd	存在的, 已查看	A	1.8 KB	Windows\Sy...	2016/04/28 14:42:47	2016/04/28 14:42:47
FP00001.SPL	SPL	spl	存在的, 已查看	A#	1.6 MB	Windows\Sy...	2016/04/28 14:42:46	2016/04/28 14:42:47

胡宇

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	00	00	01	00	54	00	00	00	10	00	00	00	00	00	00	00
00000016	45	00	3A	00	5C	00	4A	00	4D	00	58	00	4D	00	30	00
00000032	32	00	31	00	5C	00	4A	00	4D	00	58	00	4D	00	30	00
00000048	32	00	31	00	2D	00	80	62	2F	67	44	8D	99	65	2D	00
00000064	79	98	EE	76	82	69	B5	51	2E	00	64	00	6F	00	63	00
00000080	00	00	30	00	0C	00	00	00	BC	05	12	00	01	00	00	00

图 13

(四) 检材 1 技术资料外传痕迹检验分析

1、对编号 1 检材中打印文件进行分析，发现 Peter 在 2016 年 4 月 28 日 14:42:47 打印了源文件 FP00001.SHD，查看该源文件发现就是 E:\JMXM021\JMXM021_项目概况.doc 文件，部分信息如图 12、13，详细信息见附件“Peter 泄密案件附件.zip”。

2、对编号 1 检材中注册表 NTUSER.DAT 进行分析，发现 Peter 在 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 14、图 15、图 16，详细信息见附件“Peter 泄密案附件.zip”。

49	2016/04/28 14:47:30	文件访问	F:\Autorun.exe	胡宇
50	2016/04/28 14:49:25	连入usb设备	Port_#0003.Hub_#0002: 1.0	
51	2016/04/28 14:49:41	连入usb设备	Port_#0003.Hub_#0002: 1.0	

图 14

Networks 胡宇

Profile	Description	Created	Last Connected	Type	GUID
P.ZHAO	P.ZHAO	2016/04/28 14:55:19	2016/04/28 14:55:19	Wireless	{711D7270-CC6A-4678-87FF-562A13B5864E}

图 15



图 16

3、对编号 1 检材中电子邮件进行分析，发现在已删除邮件中有两条记录，Peter 于 4 月 28 日 15:31:26，将技术资料以邮件附件的形式发送给 bylwlqm1@163.com，部分信息见图 17，详细信息见附件“Peter 泄密案附件.zip”。

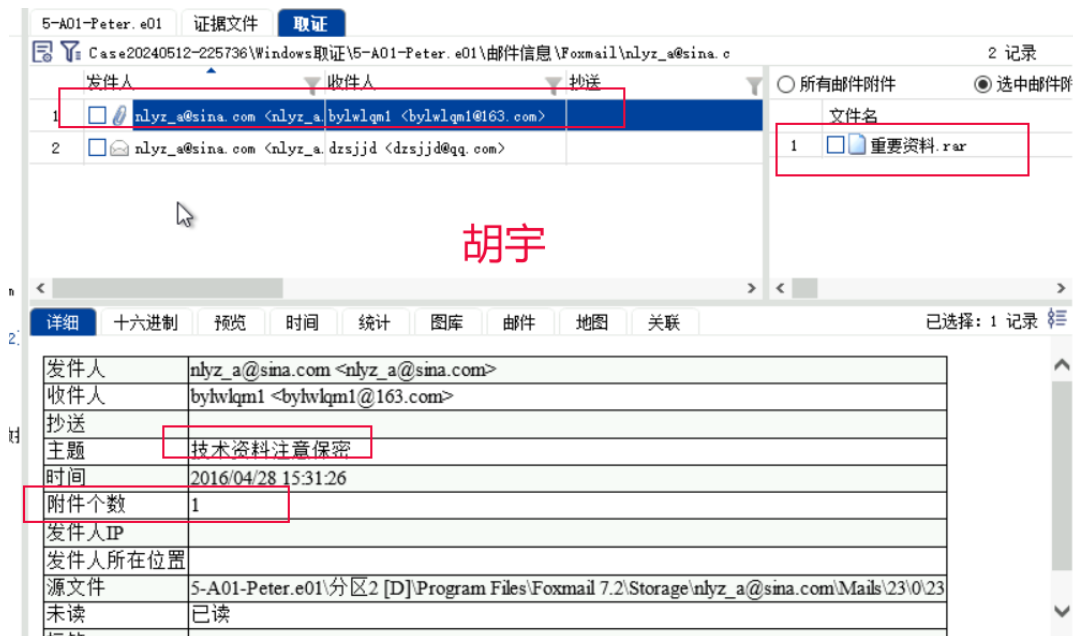


图 17

4、编号 1 检材中电子邮件进行分析，发现在已删除邮件中有两条

记录，Peter 于 4 月 28 日 15:33:07，发送了一条主题为保密资料的邮件给 dzsjjd@qq.com，邮件内容是一个百度网盘链接和提取密码 09h2，有理由推断是以百度网盘的形式将机密文件泄露，部分信息见图 18，详细信息见附件“Peter 泄密案附件.zip”。

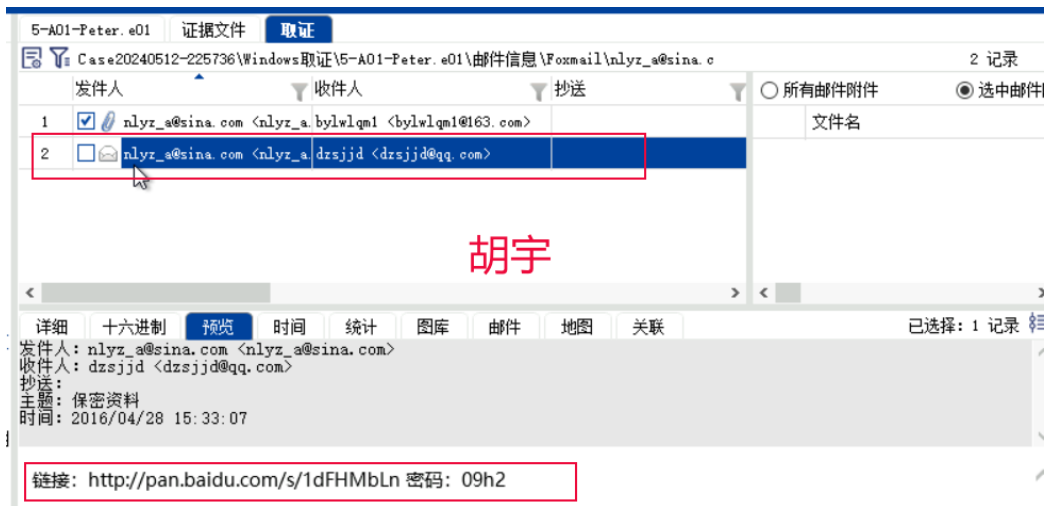


图 18

5、对编号 1 检材中网页访问痕迹进行分析，可以发现 Peter 访问了国际互联网的痕迹，不仅访问了必应、foxmail 等多个相关网站，还访问了百度云客户端下载网页，结合 4 中邮件内容，有理由推断，Peter 从互联网下载了百度云网盘客户端，然后将机密邮件上传到网盘，最后以邮件的形式将网盘信息传递出去，完成机密信息泄露。部分信息见图 19、图 20，详细信息见附件“Peter 泄密案附件.zip”。

网址	标题	日期	访问次数	原始URL
4	http://cn.msn.com/?ocid=ieh	2016/04/28 14:59:05	6	
5	http://cn.msn.com/cnmsn201	2016/04/28 14:55:39	1	
6	http://www.bing.com/search Bin	2016/04/28 14:58:07	3	
7	http://cn.bing.com/search? foxmail - 必应	2016/04/28 15:11:50	9	
8	http://pan.baidu.com/download 百度云 客户端下载	2016/04/28 15:11:48	18	
9	http://img4.mini.cache.wps	2016/04/28 15:38:39	1	
10	http://boscdn.baidu.com/ne	2016/04/28 15:08:03	2	

网址	http://pan.baidu.com/download
标题	百度云 客户端下载
日期	2016/04/28 15:11:48
访问次数	18
原始URL	
源文件	5-A01-Peter.e01\分区1 [C]\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

图 19

5-A01-Peter. e01 证据文件 取证

Case20240512-225736\Windows取证\5-A01-Peter. e01\上网记录\IE\上网记录 78 记录

网址	标题	日期	访问次数	原始URL
about:blank		2016/04/28 15:38:33	8	
http://yun.baidu.com/	百度云——云上的日子 你我共享	2016/04/28 15:11:49	11	
http://yun.baidu.com/	百度云——云上的日子 你我共享	2016/04/28 14:58:16	6	
http://pan.baidu.com/downlo	百度云 客户端下载	2016/04/28 14:59:05	4	
http://www.bing.com/search	Bin	2016/04/28 14:58:07	1	
https://ieonline.microsoft	建议网站	2016/04/28 14:58:07	2	
http://www.bing.com/search	Bin	2016/04/28 14:58:07	2	

详细 十六进制 预览 时间 统计 已选择: 1 记录

胡宇

网址	http://yun.baidu.com/
标题	百度云——云上的日子 你我共享
日期	2016/04/28 15:11:49
访问次数	11
原始URL	

图 20

6、对编号 1 检材中软件安装以及邮件信息进行分析，可以发现 Peter 下载了 foxmail，并自己拥有一个用户名为 nlyz_a@sina.com，密码为 2012nlyz! 的 foxmail 账号，其通过此账号达到机密信息泄露的目的。部分信息见图 21、图 22，详细信息见附件“Peter 泄密案附件.zip”

5-A01-Peter. e01 证据文件 取证

Case20240512-225736\Windows取证\5-A01-Peter. e01\系统信息\安装软件\办公软件 6 记录

软件名称	版本信息	安装时间	发行人	安装源程序路径	卸载命令
Foxmail	7.2	2016/04/28 15:07:32	腾讯公司		
Microsoft Office 2.12.0.6425.1000		2016/04/19 16:33:09	Microsoft Corporation	C:\Program Files\Micr...	
Foxmail	7.2	2016/04/28 15:07:32	腾讯公司		
Microsoft Office 2.12.0.6425.1000		2016/04/19 16:33:09	Microsoft Corporation	C:\Program Files\Micr...	
WPS Office (10.1.0.10.1.0.5603		2016/04/27 20:39:07	Kingsoft Corp.		
WPS Office (10.1.0.10.1.0.5603		2016/04/27 20:39:07	Kingsoft Corp.		

详细 十六进制 预览 时间 统计 已选择: 1 记录

胡宇

软件名称	Foxmail
版本信息	7.2
安装时间	2016/04/28 15:07:32
发行人	腾讯公司
安装源程序路径	
卸载命令	

图 21

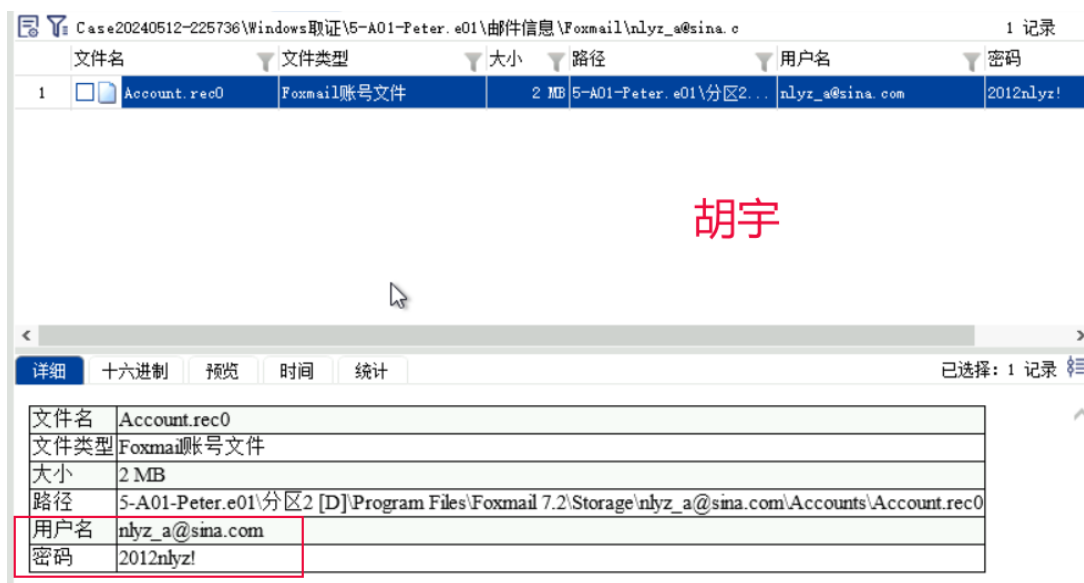


图 22

(五) 检材 1 技术资料窃密反取证痕迹检验分析

1、对编号 1 检材邮件删除记录进行分析，发现 Peter 在 2016 年 4 月 28 日删除了发送的两条机密泄露相关邮件，部分信息见图 23，详细信息见附件“Peter 泄密案附件.zip”。

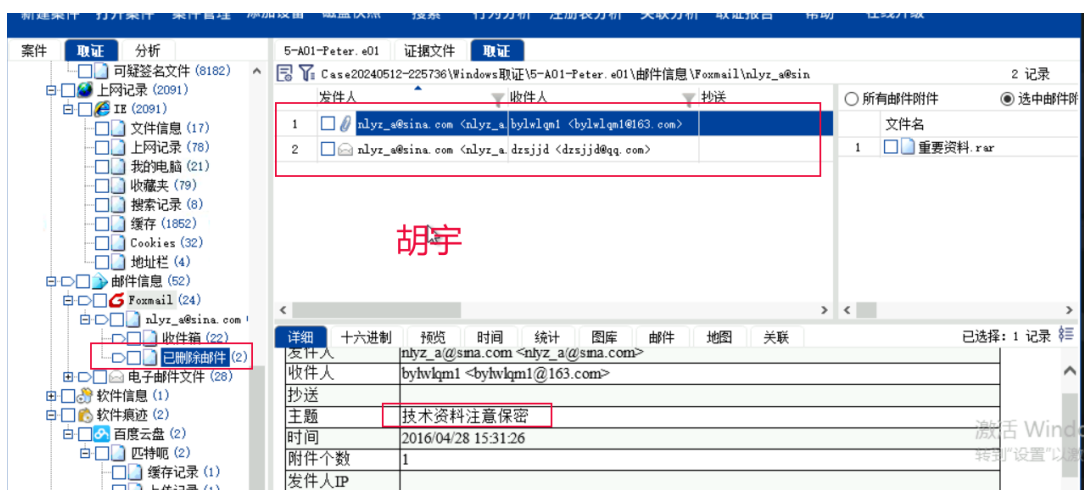


图 23

2、对编号 1 检材用户行为进行分析，发现 Peter 在 2016 年 4 月 28 日 15:42:39 删除 Foxmail 和百度云管家并关机，企图掩盖自己对

秘密信息的泄露行为，部分信息见图 24，详细信息见附件“Peter 泄密案附件.zip”。

取证					205 记录
Case20240512-225736\用户行为分析\2016年\4月\28(四)					
时间	行为	行为描述	标题 消息		
201	2016/04/28 15:42:11	文件访问	D:\BaiduYunDownload		
202	2016/04/28 15:42:39	删除文件	C:\Users\Public\Desktop\Foxmail.lnk		
203	2016/04/28 15:42:39	删除文件	C:\Users\Administrator\Desktop\百度云管家.lnk		
204	2016/04/28 15:43:06	关机			
205	2016/04/28 15:43:06	关机			

胡宇

详细	十六进制	预览	时间	统计	图表	已选择: 1 记录
时间	2016/04/28 15:42:39					
行为	删除文件					
行为描述	C:\Users\Public\Desktop\Foxmail.lnk					
标题 消息						
源文件	5-A01-Peter.e01\分区1 [C:]\$Recycle.Bin\S-1-5-21-1624523196-595389801-647913451-500\SR8GY2CF.lnk					

图 24

3、对编号 1 检材中回收站进行分析，发现 Peter 在 2016 年 4 月 28 日 15:42:39，将 Foxmail、百度网盘的快捷方式删除的痕迹，部分信息见图 25、图 26，详细信息见附件“Peter 泄密案附件.zip”。

.. = \$Recycle.Bin (5)	2.9 KB	2016/04/19 16:26:45	2016/04/19 16:26:45	+8	SH	6,3...	1-24
= S-1-5-21-16245...	2.9 KB	2016/04/28 15:42:39	2016/04/28 15:42:39	+8	SH	16...	1-14369
\$I8GY2CF.lnk	0.5 KB	2016/04/28 15:42:39	2016/04/28 15:42:39	+8	A	6,3...	1-66891
\$IFB4RTS.lnk	0.5 KB	2016/04/28 15:42:39	2016/04/28 15:42:39	+8	A	6,3...	1-67319
\$R8GY2CF.lnk (Foxmail.l)	0.7 KB	2016/04/28 15:07:32	2016/04/28 15:42:39	+8	A	6,3...	1-66045
\$RFB4RTS.lnk (百度云管)	1.0 KB	2016/04/28 15:10:30	2016/04/28 15:42:39	+8	A	17...	1-66886
desktop.ini	129 B	2016/04/19 16:26:45	2016/04/19 16:26:45	+8	SHA	6,3...	1-14370

胡宇

图 25

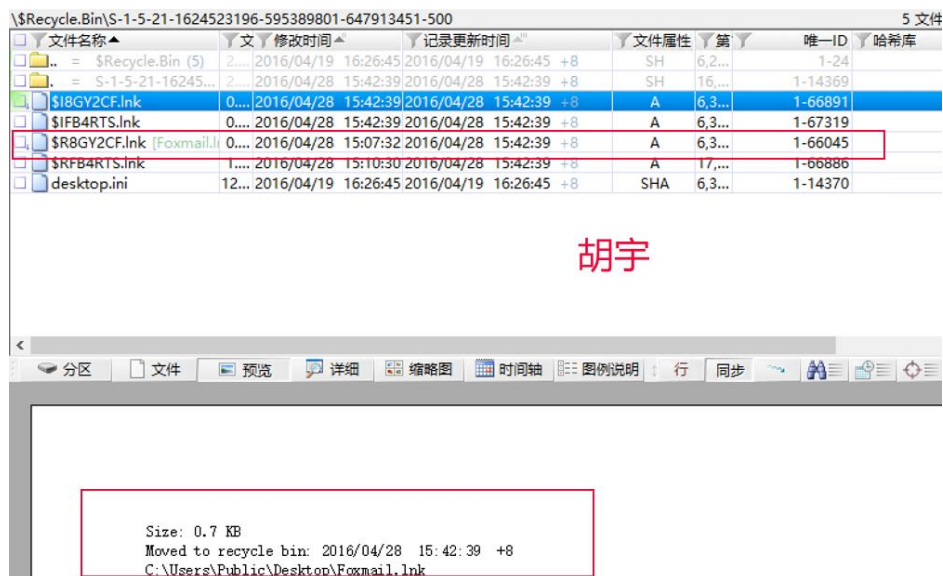


图 26

4、对编号 1 检材使用软件信息分析，发现编号 1 检材中有数据擦除软件 FileSmasher.exe，Peter 有可能利用该软件擦除数据，企图隐藏自己泄露机密数据的犯罪事实，部分信息如图 27，详细信息见附件“Peter 泄密案件附件.zip”。

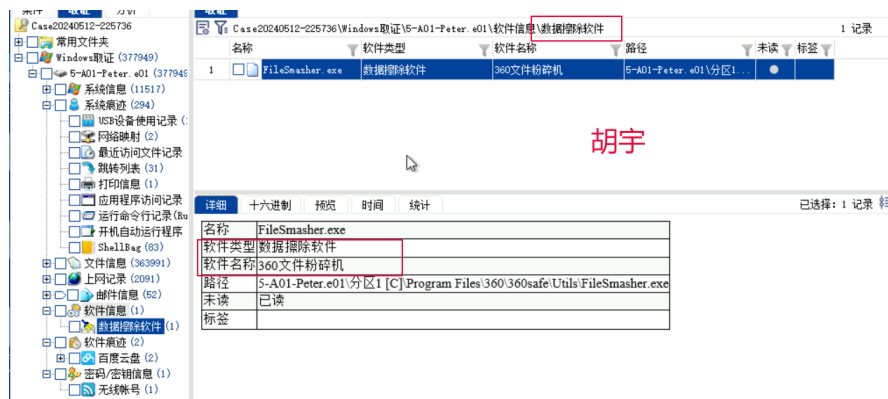


图 27

六、鉴定意见

(一) 送检材料密封和保护完整。

(二) 数据分析：

1、分析编号 1 检材中快捷方式，发现 Peter 曾访问服务器上的机密文件，包括：JMXM010-技术资料-文档.docx、JMXM021-技术资料-项目概况.doc、JMXM021-技术资料-项目汇报.pdf、JMXM005/项目介绍.ppt、JMXM010-技术资料-配方.doc、JMXM021-技术资料-客户名单.xls，并将文件拷贝到本地 D 盘的痕迹。

2、分析编号 1 检材快捷方式和跳转列表中，发现 Peter 将服务器上机密文件拷贝至本地 D 盘，于 2016 年 4 月 28 日 14:35:36 使用品牌型号为 Kingston DataTraveler 3.0 的 USB Device，挂载盘符是 E 盘，并将文件拷贝到 E 盘中；于 2016 年 4 月 28 日 14:39:14 将机密文件拷贝到类型为 CD-ROM 的 F 盘中。

3、分析编号 1 检材的打印文件和注册表中，发现 Peter 在 2016 年 4 月 28 日 14:42:47 打印 E 盘机密文件的痕迹。

4、分析编号 1 检材的网页浏览痕迹和注册表，发现 Peter 在 2016 年 4 月 28 日 14:47:30 接入无线网卡，并在 14:55:19 接入名为“P.ZHAO”的无线网络，通过网络下载 Foxmail 和百度云网盘管家软件的痕迹。

5、分析编号 1 检材的电子邮件记录、网盘使用记录以及用户行为，发现 Peter 不仅直接将机密文件拷贝到 2 中所说的移动存储设备中，还曾在 2016 年 4 月 28 日 15:30 左右将机密文件传输到百度云网盘中，并通过文件附件和网盘链接的方式发送两封 Foxmail 电子邮件，来达到泄露机密信息的目的。

6、分析编号 1 检材的回收站、删除邮件记录、软件信息，发现 Peter 曾下载数据擦除软件，在 2016 年 4 月 28 日 15:42:39，将 Fox mail、百度云的快速方式删除的痕迹，删除了涉嫌机密信息泄露的两条邮件的痕迹。

七、附件

附件一：

文件：Peter 泄密案附件.zip

大小：3,815,825 字节

MD5：D68A76CA443380CB49D2B8S2JV9SB280

SHA1：DFFE21E880D5C1EC5S8JX91BF01N478NS028SBR2S

司法鉴定人签名 胡宇

《司法鉴定执业证》证号：U202112146

司法鉴定人签名 肖凌

《司法鉴定执业证》证号：11111111111

二〇二四年五月十三日