浙江千麦司法鉴定中心

司法鉴定意见书

千麦司法鉴定
Chain Forensic Science

声　明

一、司法鉴定机构和司法鉴定人按照法律、法规和规章的规定，按照鉴定的科学规律和技术操作规范，依法独立、客观、公正进行鉴定，并出具鉴定意见，不受任何个人或者组织的非法干预。

二、委托人应向本机构提供真实、完整、充分、符合鉴定要求的鉴定材料，提供虚假鉴定材料导致鉴定意见错误的，本机构不承担任何责任。

三、本鉴定意见仅对本次委托人提供的鉴定材料负责。

四、司法鉴定意见书是否作为定案或者认定事实的根据，取决于办案机关的审查判断，司法鉴定机构和司法鉴定人无权干涉。

五、如对本鉴定书内容有任何异议或者疑问请尽早与本机构取得联系。根据司法部《司法鉴定程序通则》四十一条之规定，本机构在必要时，可以对鉴定文书进行补正或出具补正书。

六、使用司法鉴定意见书，应当保持其完整性和严肃性。未经本鉴定机构的书面同意，任何单位或个人不得部分复印本鉴定意见书（全部复印除外）。

七、鉴定意见属于鉴定人的专业意见，当事人对鉴定意见有异议，应当通过庭审质证或者申请重新鉴定、补充鉴定等方式解决。

网址：www.zjcfs.com电话：0571-85852181 传真：0571-85852191
投诉电话：0571-85256592（杭州市司法局）
地址：杭州市余杭区余杭街道华一路2号4号楼

浙江千麦司法鉴定中心
司法鉴定意见书

浙千司鉴中心[2019]电鉴字第332号

一、基本情况

委 托 人：浙江省杭州市国立公证处

委托事项：对送检的笔记本电脑日志记录进行分析

委托日期：2019年9月29日

受理日期：2019年9月29日

鉴定材料：ThinkPad笔记本电脑1台（P/N: SL10M60885，以下称检材）

鉴定日期：2019年9月29日至2019年10月11日

鉴定地点：浙江千麦司法鉴定中心电子数据鉴定实验室

二、基本案情

据委托书记载：浙江省杭州市国立公证处因在2019年9月28日下午五点的摇号结果中发现大量连号的情况，为查明事实，现委托本中心对送检的ThinkPad笔记本电脑日志记录进行分析。

三、资料摘要

无。

四、鉴定过程

依据GA/T 976-2012《电子数据法庭科学鉴定通用办法》、GB/T 29362-2012《电子物证数据搜索检验规程》和GB/T 29360-2012《电子物证数据恢复检验规程》、GA/T 1477-2018《法庭科学计算机系统接入外部设备使用痕迹检验技术规范》、GA/T 1474-2018《法庭科学计算机系统用户

操作行为检验技术规范》，使用电子物证工作站、取证大师专业版V6.1.65366、AccessData FTK Imager 3.1.2.0对检材进行检验。

1.检材检验

送检检材为笔记本电脑，品牌为“ThinkPad”、“P/N: SL10M60885”，检查设备外观完好，对检材进行唯一性标识“DZ190929JC03”并拍照固定。取出检材内的硬盘，硬盘品牌为“Intel”，“P/N: SSS0L25041”，标称容量“256 GB”，在硬盘外部贴上唯一性标识“DZ190929JC03-1”并拍照固定见附图1-3所示。

启动杀毒软件对电子物证工作站系统进行杀毒，确保工作站系统安全。将硬盘通过只读接口连接至电子物证工作站。

使用“AccessData FTK Imager”软件对检材制作镜像，镜像文件保存为“DZ190929JC03-1.dd4.001”，并计算其SHA256值为“51f683d7c22d4f800210d4cc5d8a3f3f1b19c3e721ded26e2d9837b9254efd8f”，见附图4-6所示。

2.镜像分析及数据导出

打开“取证大师专业版”软件对检材镜像文件进行检验。将检索恢复出的数据生成取证报告，并导出至路径“D:\2019年9月29日浙江省杭州市国立公证处\DZ190929JC03-1\取证报告”下，见附图7-8所示。

根据委托人要求，对时间显示为“2019年9月28日”前后的日志记录进行分析，查看发现“2019年9月27日”、“2019年9月28日”、“2019年9月29日”三天均显示有开关机记录，故将上述三天的所有日志记录分别生成对应的取证报告，并导出至路径“D:\2019年9月29日浙江省杭州市国立公证处\DZ190929JC03-1”下，见附图10所示。

五、分析说明

日志记录是记录计算机系统运行中硬件、软件和系统的各类事件信息。

通过查看Windows日志可以检查事件的类型、日期和时间、ID、来源、及详细信息，进而分析事件的情况及影响。Windows日志包括系统日志、应用程序日志和安全日志。故对提取的“2019年9月27日”、“2019年9月28日”、“2019年9月29日”的日志分别进行分析:

1.2019年9月27日相关日志分析

检索查看时间显示为“2019年9月27日”的相关痕迹记录及“Windows日志”，发现名为“glgz-9”帐号在时间“2019年9月27日13:50:29”登录系统的痕迹，并且于时间“2019年9月27日13:50:59”注销系统的痕迹，见附图11所示；未发现有连接网络及使用USB接口的痕迹记录；在Windows日志中未发现有异常日志。详细数据见取证报告“SearchReport_20190930134920（2019.9.27取证报告）”，见附图12所示。

2.2019年9月28日相关日志分析

检索查看时间显示为“2019年9月28日”的相关痕迹及“Windows日志”，发现名为“glgz-9”账号在时间“2019年9月28日17:11:43”登录系统的痕迹，并且于时间“2019年9月28日17: 20:04”注销系统的痕迹，见附图13所示。

发现1条时间为“2019年9月28日17:16:09”的错误报告日志，日志事件ID为“1001”，事件的描述记录显示这条错误日志与“javaw.exe”程序有关，见附图14所示。

发现日期为“2019年9月28日”的3条应用程序访问记录，对应名称及时间见下表所示，详细记录见附图15所示。

名称	时间
C:\Users\glgz-9\Desktop\摇号程序文件\脚本.bat	2019-09-28 17:14:17
{6D809377-6AF0-444B-8957-A3773F02200E}\Java\jre6\bin\javaw.exe	2019-09-28 17:14:19
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Root\Office16\EXCEL.EXE	2019-09-28 17:16:33

打开“脚本.bat”文件查看其内容为“@echo off

rmdir /q /s "C:\CS"

echo d | xcopy "CS" "C:\CS" /E

pause”；分析此文件用于在运行摇号软件前生成或更新存放摇号数据结果的文件夹“CS”。

发现日期为“2019年9月28日”的32条应用程序运行痕迹，逐一分析未发现异常程序运行痕迹，见附图16所示。

发现最后插拔时间为“2019-09-28 17:16:46”的1条USB设备使用痕迹，USB设备名称为“DVD RW USB Device”，见附图17所示。

未发现有连接网络的痕迹记录。

详细数据见取证报告“SearchReport_20190930135107（2019.9.28取证报告）”，见附图18所示。

3.2019年9月29日相关日志分析

检索查看时间显示为“2019年9月29日”相关痕迹及“Windows日志”，发现名为“glgz-9”账号在时间“2019年9月29日 08:20:36”登录系统的痕迹，见附图19所示；未发现有连接网络及使用USB接口的痕迹记录；在Windows日志中未发现有异常日志。详细数据见取证报告“SearchReport_20190930135240（2019.9.29取证报告）”，见附图20所示。

4.数据固定

将上述导出的取证分析报告打包压缩为文件“DZ190332.rar”，并封

盘刻录至专用的载体光盘中，载体编号为“浙千司鉴中心[2019]电鉴字第332号-ZT”。文件SHA256值为“119023dbc67158919a557d1ffc2c98543a704a4024d77109214c0972189370ef”。

六、鉴定意见

通过对送检笔记本电脑日志记录进行分析，结果如下:

1.在显示时间“2019年9月28日”内的系统运行过程中，发现有1条USB设备使用痕迹，USB设备名称为“DVD RW USB Device”；发现有3条程序访问记录，程序名称分别为“脚本.bat”（生成或更新存放摇号数据结果的文件夹）、“javaw.exe”、“EXCEL.EXE”；发现1条显示时间为“2019年9月28日 17:16:09”、描述与“javaw.exe”程序相关的错误日志记录。

2.在显示时间“2019年9月27日”至“2019年9月29日”内的系统运行过程中，未发现有连接网络的痕迹，未发现异常程序的运行和访问痕迹。

七、附件

1.附件图片共6页，内含20张图;

2.编号为“浙千司鉴中心[2019]电鉴字第332号-ZT”数据载体1份，内含“DZ190332.rar”文件。

司法鉴定人：李佳斌

执业证号：330114070049

司法鉴定人：胡斌

执业证号：330114070008

二〇一九年十月十一日

附件图片

图 1 检材正面

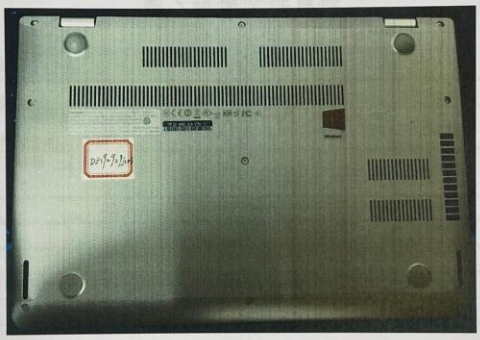


图 2 检材背面

图 3 检材硬盘

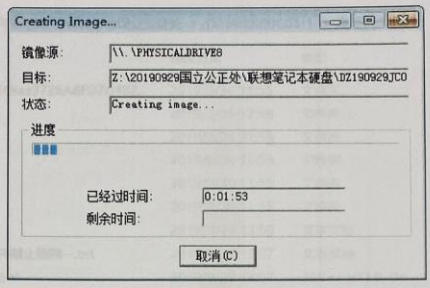


图 4 制作硬盘镜像

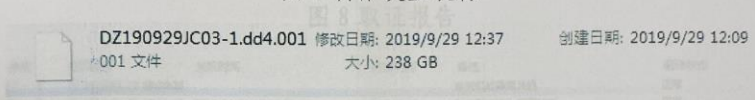


图 5 镜像文件属性

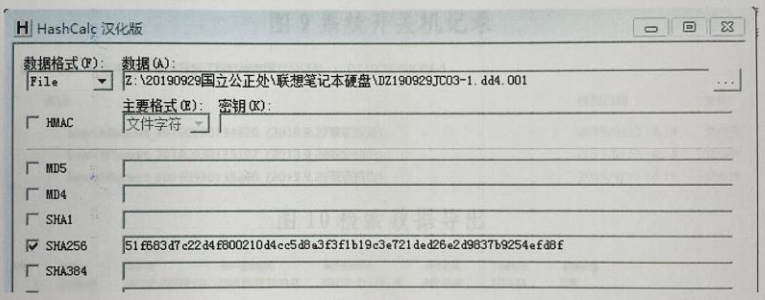


图 6 镜像文件哈希值

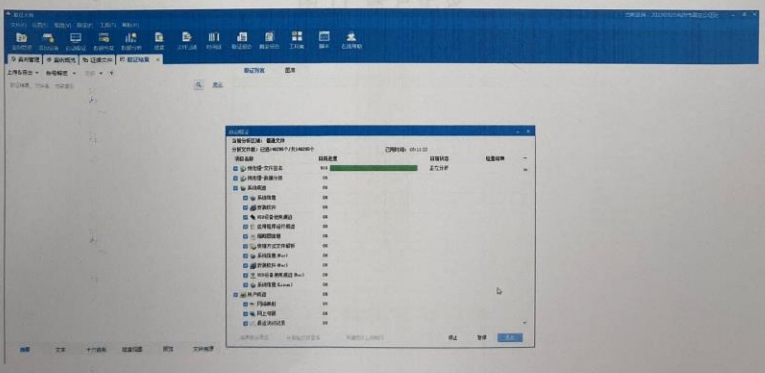


图 7 取证大师检验

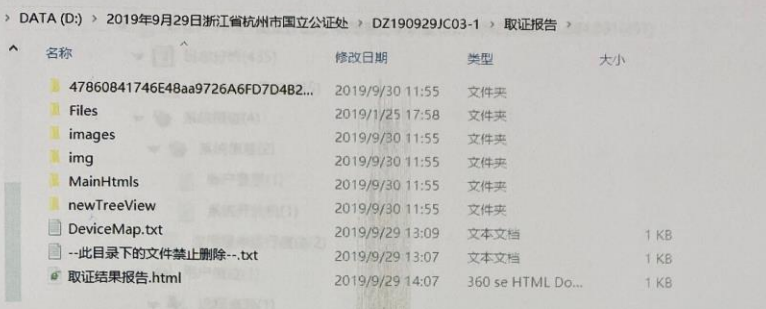


图8 取证报告

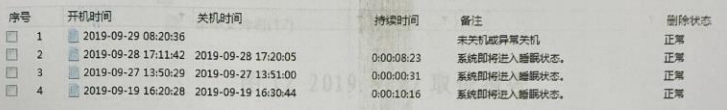


图9 系统开关机记录

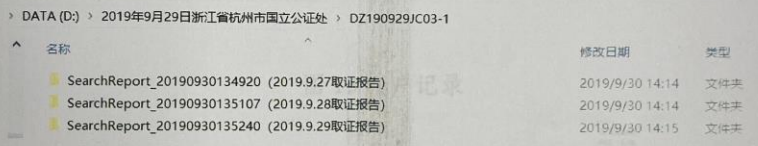


图10 检索数据导出

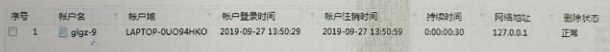


图11 帐户记录

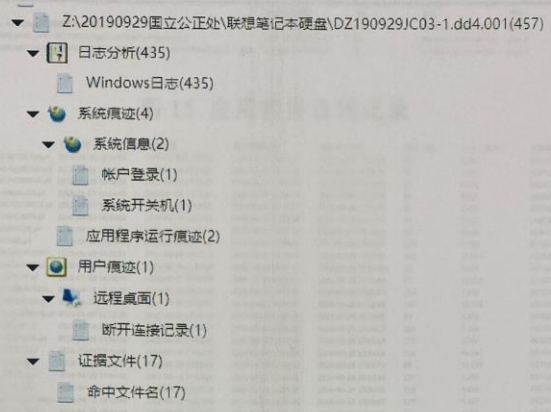


图 12 2019.9.27 取证报告

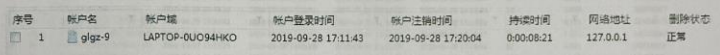


图 13 帐户记录

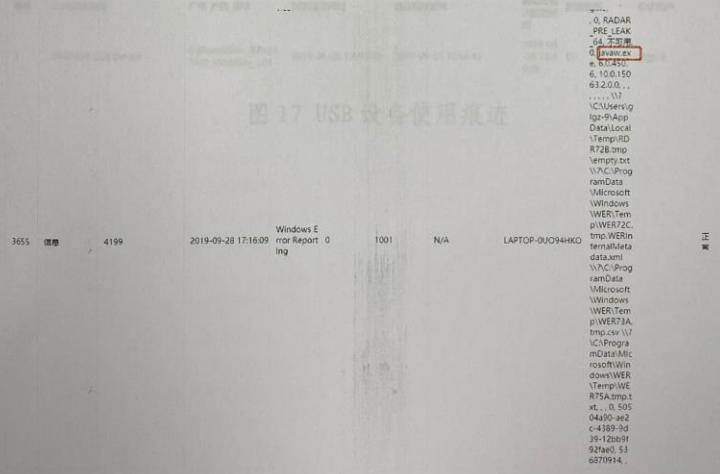


图 14 错误日志记录

序号		名称	最后运行时间	次数	系统	用户	删除状态
☑	1	C:\Users\glgz-9\Desktop\指导程序文件\版本.bat	2019-09-28 17:14:17	106	Windows 10 Home Ch...	glgz-9	正常
☑	2	{6D809377-6AF0-444B-8957-A3773F02200E}\Java\jre8\bin\javaw.exe	2019-09-28 17:14:19	113	Windows 10 Home Ch...	glgz-9	正常
☑	3	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft Office\Root\Office16\EXCEL.EXE	2019-09-28 17:16:33	75	Windows 10 Home Ch...	glgz-9	正常

图 15 应用程序访问记录

序号		名称	创建时间	修改时间	最后访问时间	最后运行时间	运行次数	大小（字节）	文件路径缺...	文件路径
☑	1	RUNDLL32.EXE-BF72C764.pf	2018-04-20 16:34:02	2019-09-28 17:20:04	2018-04-20 16:34:02	2019-09-28 17:20:04	55	6.992	BF72C764	
☑	2	MOFCOMP.EXE-5225C32D.pf	2018-04-20 16:35:44	2019-09-28 17:16:50	2018-04-20 16:35:44	2019-09-28 17:16:50	56	4.995	5225C32D	
☑	3	HP1100SM.EXE-F4DB2D4F.pf	2018-04-20 16:38:34	2019-09-28 17:16:50	2018-04-20 16:38:34	2019-09-28 17:16:40	52	6.033	F4DB2D4F	
☑	4	DLLHOST.EXE-236A1088.pf	2018-05-07 11:14:49	2019-09-28 17:16:44	2018-05-07 11:14:49	2019-09-28 17:16:38	54	7.011	236A1088	
☑	5	SPLWOW64.EXE-57576C25.pf	2018-05-07 11:14:51	2019-09-28 17:16:49	2018-05-07 11:14:51	2019-09-28 17:16:38	54	8.230	57576C25	
☑	6	DLLHOST.EXE-C60C3853.pf	2018-04-18 14:34:34	2019-09-28 17:12:03	2018-04-18 14:34:34	2019-09-28 17:11:53	39	5.117	C60C3853	
☑	7	CHSIME.EXE-450F47D5.pf	2018-04-20 16:33:54	2019-09-28 17:11:45	2018-04-20 16:33:54	2019-09-28 17:11:43	94	5.434	450F47D5	
☑	8	CMD.EXE-0BD30981.pf	2018-04-20 16:39:44	2019-09-28 17:14:18	2018-04-20 16:39:44	2019-09-28 17:14:17	172	2.755	0D30981	
☑	9	LENOVO.MODERNIMCONT...	2018-04-20 16:35:51	2019-09-28 17:15:21	2018-04-20 16:35:51	2019-09-28 17:15:11	140	37.674	73215688	
☑	10	SVCHOST.EXE-6E1A6101.pf	2018-04-20 16:34:12	2019-09-28 17:16:19	2018-04-20 16:34:12	2019-09-28 17:16:09	12	5.029	6E1A6101	
☑	11	SIHOST.EXE-1158507F.pf	2018-05-10 14:18:44	2019-09-28 17:11:54	2018-05-10 14:18:44	2019-09-28 17:11:44	47	13.023	1158507F	
☑	12	FONTDRVHOST.EXE-815230...	2018-04-18 14:35:49	2019-09-26 08:20:38	2018-04-18 14:35:49	2019-09-28 17:20:02	114	3.448	815230A4	
☑	13	SVCHOST.EXE-AE1E0CAD.pf	2018-04-20 16:34:07	2019-09-28 17:16:58	2018-04-20 16:34:07	2019-09-28 17:16:48	137	15.073	AE1E0CAD	
☑	14	WUDFHOST.EXE-DEBBE5F1.pf	2018-05-07 11:15:25	2019-09-28 17:19:18	2018-05-07 11:15:25	2019-09-28 17:19:08	63	6.292	DEBBE5F1	
☑	15	XCOPY.EXE-F5C59A8C.pf	2018-05-04 13:55:20	2019-09-28 17:14:17	2018-05-04 13:55:20	2019-09-28 17:14:17	105	2.820	F5C59A8C	
☑	16	DLLHOST.EXE-4B6CB38A.pf	2018-04-18 14:34:34	2019-09-28 17:12:23	2018-04-18 14:34:34	2019-09-28 17:12:18	172	3.967	4B6CB38A	
☑	17	JAVAW.EXE-5E8618 5A.pf	2018-05-04 13:54:23	2019-09-28 17:14:29	2018-05-04 13:54:23	2019-09-28 17:14:19	106	40.937	5E86185A	
☑	18	EXCEL.EXE-B2758640.pf	2018-04-20 16:33:13	2019-09-28 17:16:44	2018-04-20 16:33:13	2019-09-28 17:16:33	66	52.289	B2758640	
☑	19	SPHSVC.EXE-96070FE0.pf	2018-04-20 16:34:01	2019-09-28 17:16:44	2018-04-20 16:34:01	2019-09-28 17:16:34	127	7.286	96070FE0	
☑	20	CSRSS.EXE-F3C168CB.pf	2018-04-18 14:35:49	2019-09-29 08:20:38	2018-04-18 14:35:49	2019-09-28 17:20:02	119	4.416	F3C168CB	
☑	21	WINLOGON.EXE-DEODC9B6...	2018-04-18 14:35:49	2019-09-29 08:20:38	2018-04-18 14:35:49	2019-09-28 17:20:02	122	6.247	DE0DC9B6	
☑	22	ICACLS.EXE-CCAC2A58.pf	2018-04-20 16:35:44	2019-09-28 17:16:49	2018-04-20 16:35:44	2019-09-28 17:16:49	76	2.515	CCAC2A58	
☑	23	LENOVO.MODERNJMCONT...	2018-04-20 16:35:51	2019-09-28 17:16:57	2018-04-20 16:35:51	2019-09-28 17:16:47	55	17.294	DEF05A2C	
☑	24	WMIPRVSE.EXE-E8B8DD29.pf	2018-05-04 13:50:43	2019-09-28 17:17:00	2018-05-04 13:50:43	2019-09-28 17:16:50	180	6.443	E8B8DD29	
☑	25	TPNUMLKD.EXE-AB713895.pf	2018-05-04 13:48:16	2019-09-28 17:11:44	2018-05-04 13:48:16	2019-09-28 17:11:44	74	4.408	AB713895	
☑	26	DLLHOST.EXE-6389524F.pf	2018-04-18 14:35:07	2019-09-28 17:11:49	2018-04-18 14:35:07	2019-09-28 17:11:43	70	3.643	6389524F	
☑	27	SVCHOST.EXE-6CAD538D.pf	2018-04-20 16:31:50	2019-09-28 17:13:54	2018-04-20 16:31:50	2019-09-28 17:13:44	67	5.532	6CAD538D	
☑	28	TPOSD.EXE-B8FF9DC7.pf	2018-05-09 08:34:10	2019-09-28 17:11:54	2018-05-09 08:34:10	2019-09-28 17:11:44	13	9.876	B8FF9DC7	
☑	29	TASKHOSTW.EXE-2E5D4B75...	2018-04-20 16:33:51	2019-09-28 17:16:19	2018-04-20 16:33:51	2019-09-28 17:16:09	140	8.774	2E5D4B75	
☑	30	AUDIODG.EXE-AB22E9A6.pf	2018-05-04 13:52:46	2019-09-28 17:17:07	2018-05-04 13:52:46	2019-09-28 17:16:57	71	7.231	AB22E9A6	
☑	31	SVCHOST.EXE-D0F686CF.pf	2018-05-07 11:15:25	2019-09-28 17:19:18	2018-05-07 11:15:25	2019-09-28 17:19:08	62	4.611	D0F686CF	
☑	32	DWM.EXE-314E93C5.pf	2018-04-18 14:35:49	2019-09-29 08:20:38	2018-04-18 14:35:49	2019-09-28 17:20:02	109	14.832	314E93C5	

图 16 应用程序运行记录

序号	USB设备名称	厂商_产品_版本	首次插拔时间	最后插拔时间	最后一次启动的首次插拔时间	挂载盘符	系统用户
1	DVD RW USB Device	CdRom&Ven_&Prod_DVD_RW&Rev_1.01	2019-06-28 13:40:00	2019-09-28 17:16:46	2019-06-28 13:40:00	D:	glgz-9

图 17 USB 设备使用痕迹

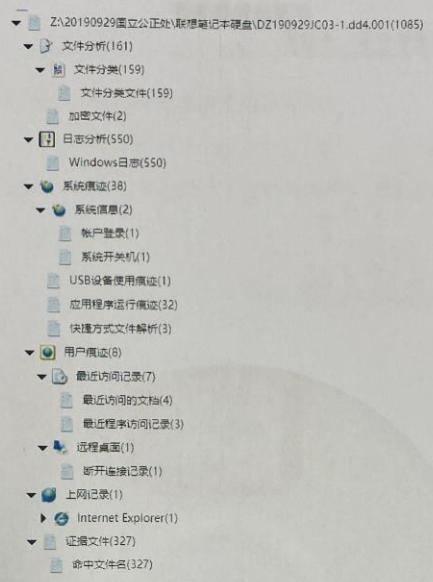


图 18 2019.9.28 取证报告

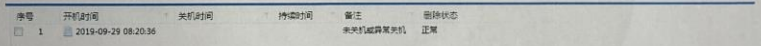


图 19 系统开关机记录

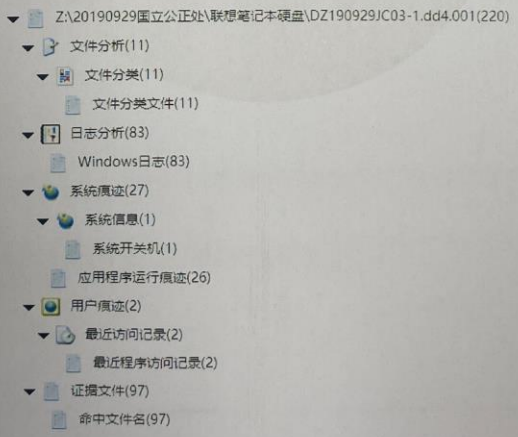


图 20 2019.9.29 取证报告

数据载体粘贴单

案件号：浙千司鉴中心[2019]电鉴字第332号

载体编号：浙千司鉴中心[2019]电鉴字第332号-ZT

载体内文件：“DZ190332.rar”文件，文件SHA256值为“119023dbc67158919a557d1ffc2c98543a704a4024d77109214c0972189370ef”。

备注：切勿剪切载体内的文件，请复制后校验哈希值再解压。

执业机构：浙江千麦司法鉴定中心

专业技术职称：

行业执业资格：

执业范围：声像资料鉴定（电子数据鉴定）

姓　　名：李佳斌

性　　别：男

执业证号：330114070049

身份证号码：330324199201122819

有效期：2019 年 07 月 18 日至 2024 年 07 月 17 日

首次获准登记日期：2019 年 07 月 18 日

颁证机关：浙江省司法厅

颁证日期：2019 年 07 月 18 日

执业机构：浙江千麦司法鉴定中心

专业技术职称：高级工程师

行业执业资格：

执业范围：痕迹鉴定

声像资料鉴定

（电子数据鉴定）

姓　　名：胡斌

性　　别：男

执业证号：330114070008

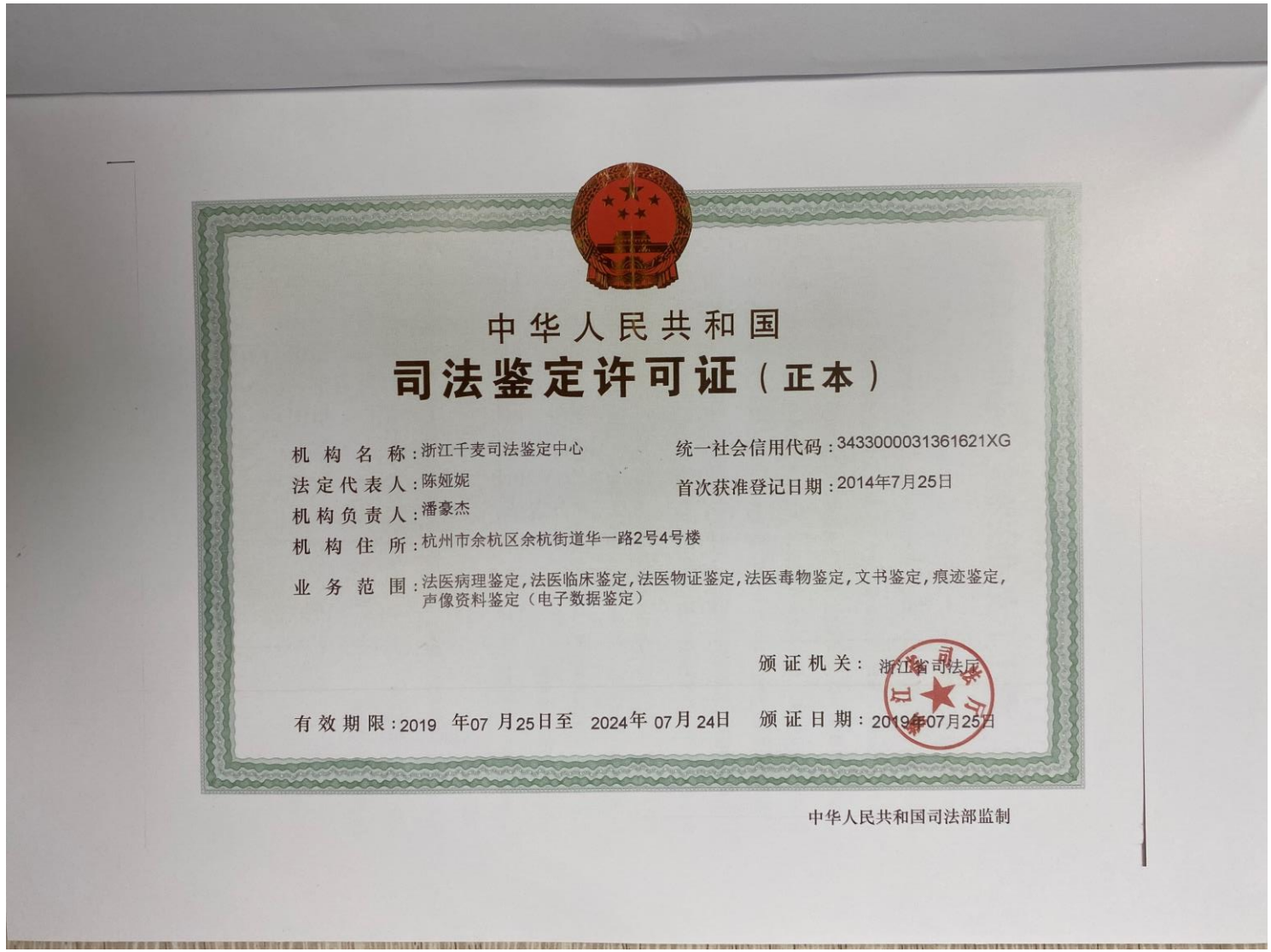
身份证号码：330802196206074030

有效期：2019 年 07 月 25 日至 2024 年 07 月 24 日

首次获准登记日期：2014 年 07 月 25 日

颁证机关：浙江省司法厅

颁证日期：2019 年 07 月 25 日



中华人民共和国

司法鉴定许可证（正本）

机 构 名 称：浙江千麦司法鉴定中心　　统一社会信用代码：34330000313616 21XG

法 定 代 表 人：陈娅妮　　首次获准登记日期：2014年7月25日

机 构 负 责 人：潘豪杰

机 构 住 所：杭州市余杭区余杭街道华一路2号4号楼

业 务 范 围：法医病理鉴定，法医临床鉴定，法医物证鉴定，法医毒物鉴定，文书鉴定，痕迹鉴定，声像资料鉴定（电子数据鉴定）

颁 证 机 关：浙江省司法厅

有 效 期 限：2019 年07 月25日至 2024年 07月 24日　　颁 证 日 期：2019年07月25日

中华人民共和国司法部监制

浙江千麦司法鉴定中心服务项目

1、**法医临床鉴定**：伤残等级评定、伤病关系鉴定、损伤程度鉴定（轻、重伤鉴定）、致伤物和致伤方式推断、三期评估（误工、护理、营养时限评定）、活体年龄鉴定 、护理依赖程度评定、工伤鉴定、男子性功能鉴定、视觉功能鉴定、听觉功能鉴定、医疗损害鉴定、医疗费合理性评定；

2、**法医病理鉴定**：死亡原因鉴定、死亡方式鉴定、死亡时间鉴定、生前伤与死后伤鉴定、硅藻检验、病理组织学诊断、伤病关系参与度鉴定、医疗纠纷尸体检验、致伤（死）物推断；

3、**法医物证鉴定**：亲权鉴定、个体识别、种属认定、有无人血迹、有无人精斑；

4、**法医毒物鉴定**：乙醇定性定量分析、生物检材中常见毒品定性分析、体外疑似毒品定性定量分析、常见毒（药）物筛选定性分析、碳氧血红蛋白饱和度测定（一氧化碳中毒）、氰化物定性定量分析；

5、**文书鉴定**：笔迹鉴定，印章印文鉴定，朱墨时序鉴定，打印、传真、复印等印刷文件鉴定，变造文件鉴定，污损文件的显现、整复、辨读等，书写工具及其他工具形成的文字压痕及其它压印痕迹的显现、辨读、鉴别等；

6、**痕迹鉴定**：车辆痕迹鉴定、车速鉴定、指印检验鉴定、足迹检验鉴定、工具痕迹鉴定、整体分离痕迹鉴定；

7、**声像资料（电子数据）鉴定**：手机、硬盘等存储介质数据恢复、提取、固定，数据库等电子数据分析，网络数据获取、固定，软件功能鉴定，软件相似性鉴定，电子邮件分析，密码破解，电子数据真实性（完整性）鉴定等。