

20251013-DFIR-复赛-Writeup

DFIR-rensom

请分析【检材1】，并对以下问题作答。

警方破获了一起勒索病毒案件，获取病毒开发者的电脑后，对开发者的电脑进行取证。本题涉及到文件恢复、系统数据恢复、勒索病毒、Windows 11系统新特性等实用场景，希望考察选手在灵活运用取证工具的同时，也能利用自己扎实的取证技术基本功。试题中的仿真勒索病毒文件在正常情况下不会造成数据丢失，但仍建议采用虚拟机进行调试。

1. 恢复系统数据，给出主机用户的姓名全拼（全小写，例：zhangsan）。

The screenshot displays a forensic analysis tool interface. On the left is a sidebar with navigation icons for '案件' (Case), '文件' (Files), '分析' (Analysis), '位置' (Location), '时间线' (Timeline), '搜索' (Search), '笔记' (Notes), '报告' (Reports), '研判' (Analysis), and '工具箱' (Toolbox). The main area is divided into a left pane showing a tree view of system data and a right pane showing detailed information for the selected item.

In the left pane, the tree view shows the following structure:

- 检材1-rensom... 1/23851
 - 用户痕迹 104
 - Notepad 1
 - 基本信息 1222
 - 系统信息 19
 - 默认浏览器 1
 - 用户列表 8
 - 账户操作记录 4
 - 登录信息 2
 - 开关机时间 3
 - 自启动程序 2
 - 默认打开方式 225
 - 系统服务 606
 - 安装软件 2
 - 可执行程序 103
 - USB设备信息 4
 - USB最近使用记... 13
 - 硬件信息 199
 - 网络配置 26
 - 系统补丁 2
 - 安全问题 3
 - 事件日志 18679
 - 事件日志分析 2078
 - 服务日志 5
 - ShimCache 233
 - 任务计划 237
 - win10通知 1 /3
 - 用户桌面 1

The right pane shows the '用户列表' (User List) tab. It contains a table with the following columns: 序号 (Serial Number), 名称 (Name), 用户类型 (User Type), 登录密码 (Login Password), and 描述 (Description).

序号	名称	用户类型	登录密码	描述
1	Administrator	本地账户	[空密码]	管理计算机(域)的内置帐户
2	Guest	本地账户	[空密码]	供来宾访问计算机或访问域的内置帐户
3	DefaultAccount	本地账户	[空密码]	系统管理的用户帐户。
4	WDAGUtility...	本地账户		系统为 Windows Defender 应用程序防...
5	马爱雨	本地账户		
6	Network Servi...	本地账户		
7	SYSTEM	本地账户		
8	LocalService	本地账户		

Below the table, the '详细信息' (Detailed Information) section for the selected user '马爱雨' (Ma Aiyu) is shown:

- 名称: 马爱雨
- 用户类型: 本地账户
- SID: S-1-5-21-2628726947-1163023753-3710451547-1001
- 最后登录时间: 2025-10-14 15:32:54
- 最后修改密码时间: 2025-10-13 00:50:42
- 账号过期时间: 2185-07-22 07:34:33
- 账户是否有效: 是
- 登录次数: 8
- 用户目录: C:\Users\马爱雨
- IM HASH: aad3b435f51404eeaad3b435f51404e...

flag{maaiyu}

2. 给出主机最近一次插过的U盘的厂商，全小写（例：barracuda）。

从设备最近活动取证结果得到。

刷新 详情/预览

请选择/输入持有人/检材

文件

分析

位置

时间线

搜索

笔记

报告

研判

工具箱

检材1-rensom.E01

基本信息

USB设备信息

请勾选/输入设备名称/设备描述/设备序列号/设备类型

过滤

过滤

过滤

过滤

序号	名称	设备描述	设备序列号	设备类型
1	@System32\drivers\usbxhci.sys, #10...	其他名称: @System32\drivers\usbxhci.sys, #1073807361, %...		Unknown
2	VMware Virtual USB Mouse	其他名称: USB Composite Device		Input.Mouse
3	JetFlash Transcend 64GB USB Device	盘符: F:\; 其他名称: JetFlash Transcend 64GB USB Devic...	AA000000000000489	Storage
4	Virtual Disk	实际容量: 50G		Storage

详细信息

名称: JetFlash Transcend 64GB USB Device

厂商_产品_版本: JetFlash_Mass Storage Device_1100

设备描述: 盘符: F:\; 其他名称: JetFlash Transcend 64GB USB Device, F:\; 实际容量: 56G

设备序列号: AA000000000000489

设备类型: Storage

设备实例路径: USB\VID_8564&PID_1000\031VDX9043N5171V

首次接入时间: 2025-10-14 15:00:08

最后弹出时间: 2025-10-14 15:26:43

最后弹出时间: 2025-10-14 15:26:43

服务: USBSTOR

硬件ID: USB\VID_8564&PID_1000&REV_1100 USB\VID_8564&PID_1000

设备GUID: {36fc9e60-c465-11cf-8056-444553540000}

驱动: {36fc9e60-c465-11cf-8056-444553540000}\0007

flag{jetflash}

3. 给出电脑的OEM厂商品牌名称，全小写（例：xiaomi）。

通过仿真右键计算机属性得到OEM信息是H3C H3CBook Ultra 14T

设置

查找设置

马爱雨 本地帐户

主页

系统

蓝牙和其他设备

网络和 Internet

个性化

应用

帐户

时间和语言

游戏

辅助功能

隐私和安全性

Windows 更新

rensom H3C H3CBook Ultra 14T 重命名

Ethernet0 2 无法访问 Internet

Windows 更新 最新

脱机

所有功能尽在 Microsoft 帐户

登录以将你喜爱的 Microsoft 应用连接到你的设备。

W X P S O

登录

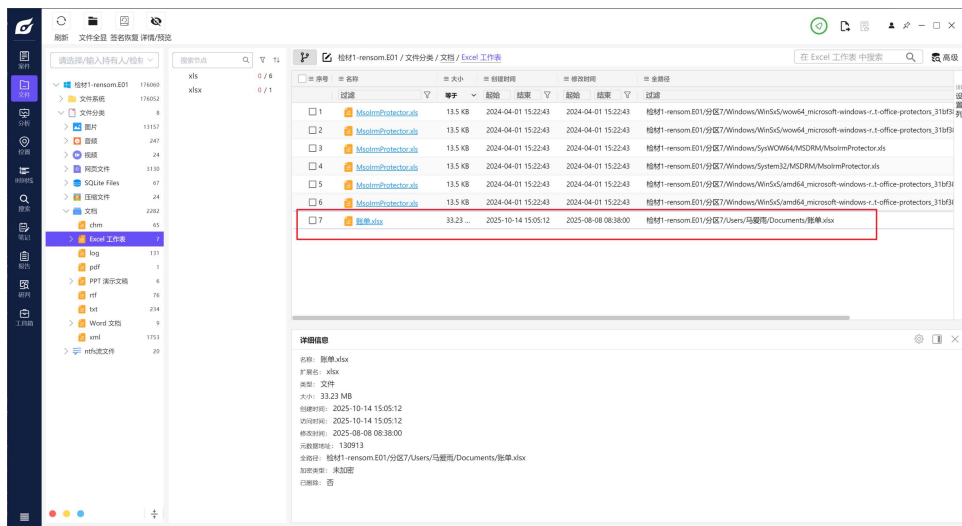
推荐设置

14:29:51 2025/11/13

flag{h3c}

4. 恢复账单文件，给出主机用户2023年全年的净支出金额，保留两位小数（例：233621.14）。

1. 从主机用户的磁盘内提取Excel表，把头部的P7改回PK，并进行简单的统计分析，过滤马爱雨在2023年的账单，用expense求和减去income，就可以获得，难度适中。
2. 考察选手对主流办公文件格式的了解，xlsx本质是一个zip压缩包，魔数一定是PK开头，二进制对比不难发现头部魔数被篡改。



```
from decimal import Decimal
```

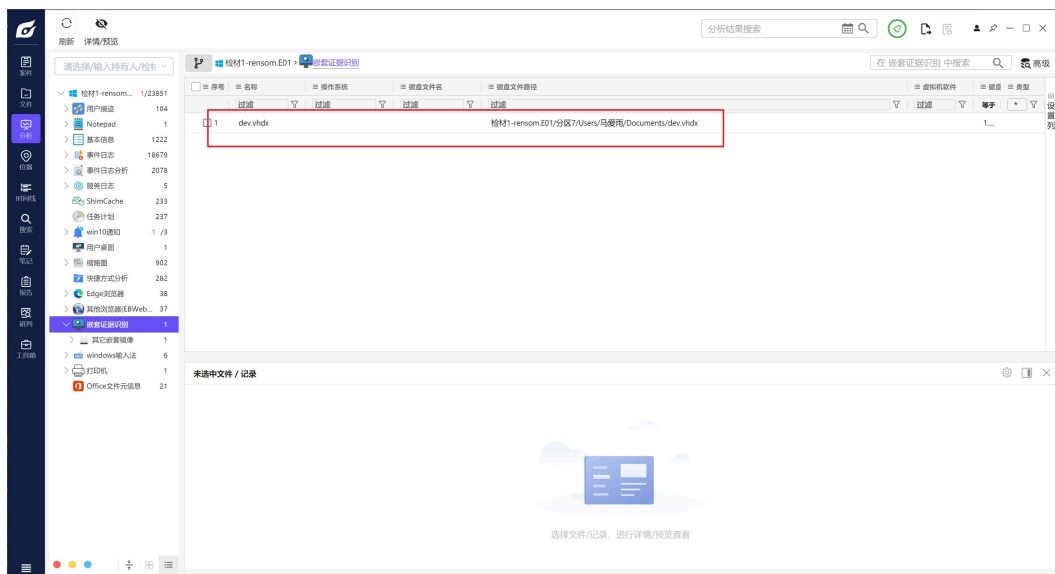
```
expe = Decimal()
inco = Decimal()
for l in open('账单.csv', 'r', encoding='utf-8-sig'):
    if '马爱雨' in l and l.startswith('2023'):
        if 'expense' in l:
            expe += Decimal(l.split(',')[1])
        if 'income' in l:
            inco += Decimal(l.split(',')[1])

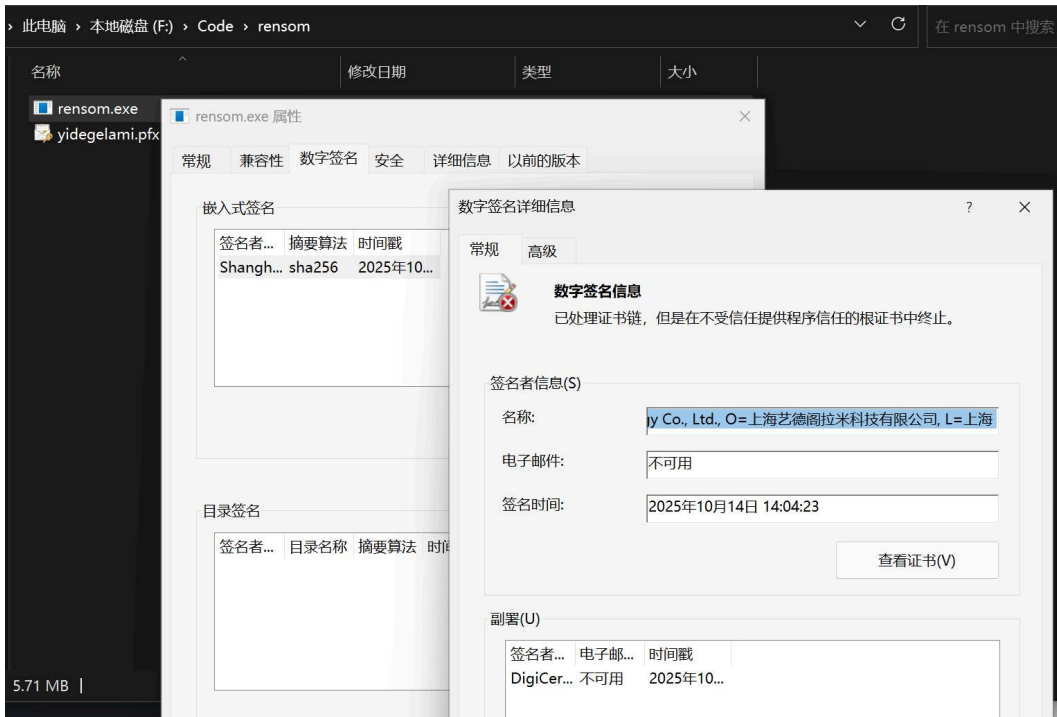
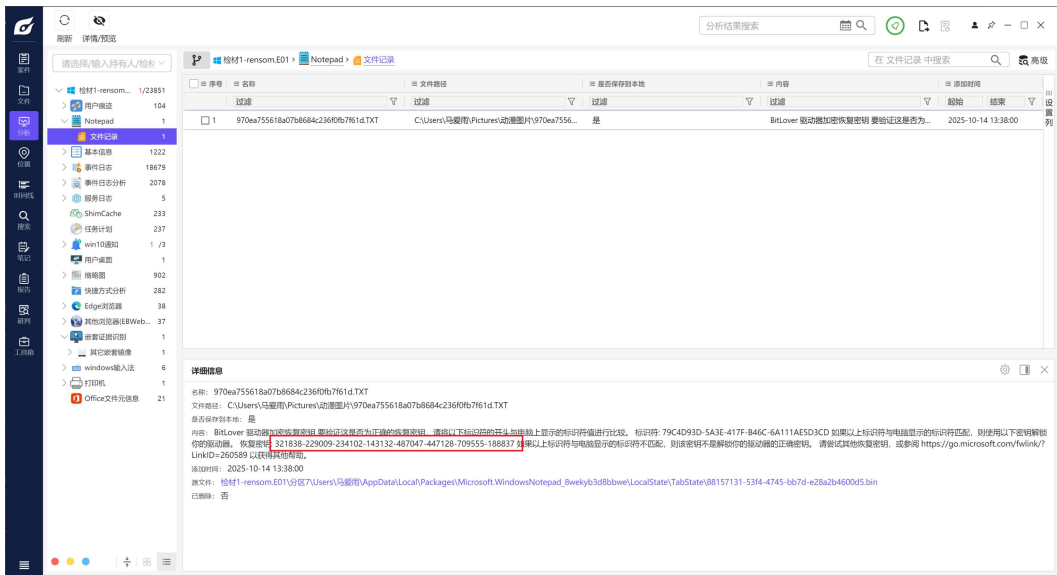
print(expe-inco)
```

```
flag{3368873.19}
```

5. 挂载虚拟磁盘，恢复勒索病毒文件，勒索病毒伪造了某单位的证书签名，给出该单位名称全拼（全小写，例：北京心脏跳动有限公司->beijingxinzangtiaodongyouxiangongsi）。

1. 图片目录下的txt文件包括了bitlocker的解锁密钥，解锁bitlocker后，可以在Code/rensom下找到勒索病毒，右键属性可以看到病毒的签名使用了某家公司的证书。难度适中。
2. 从这一题开始，选手需要对Bitlocker有基本的理解，并且有在系统中恢复加密文件密钥的能力。选手还需要对exe文件可包含的信息有所了解。

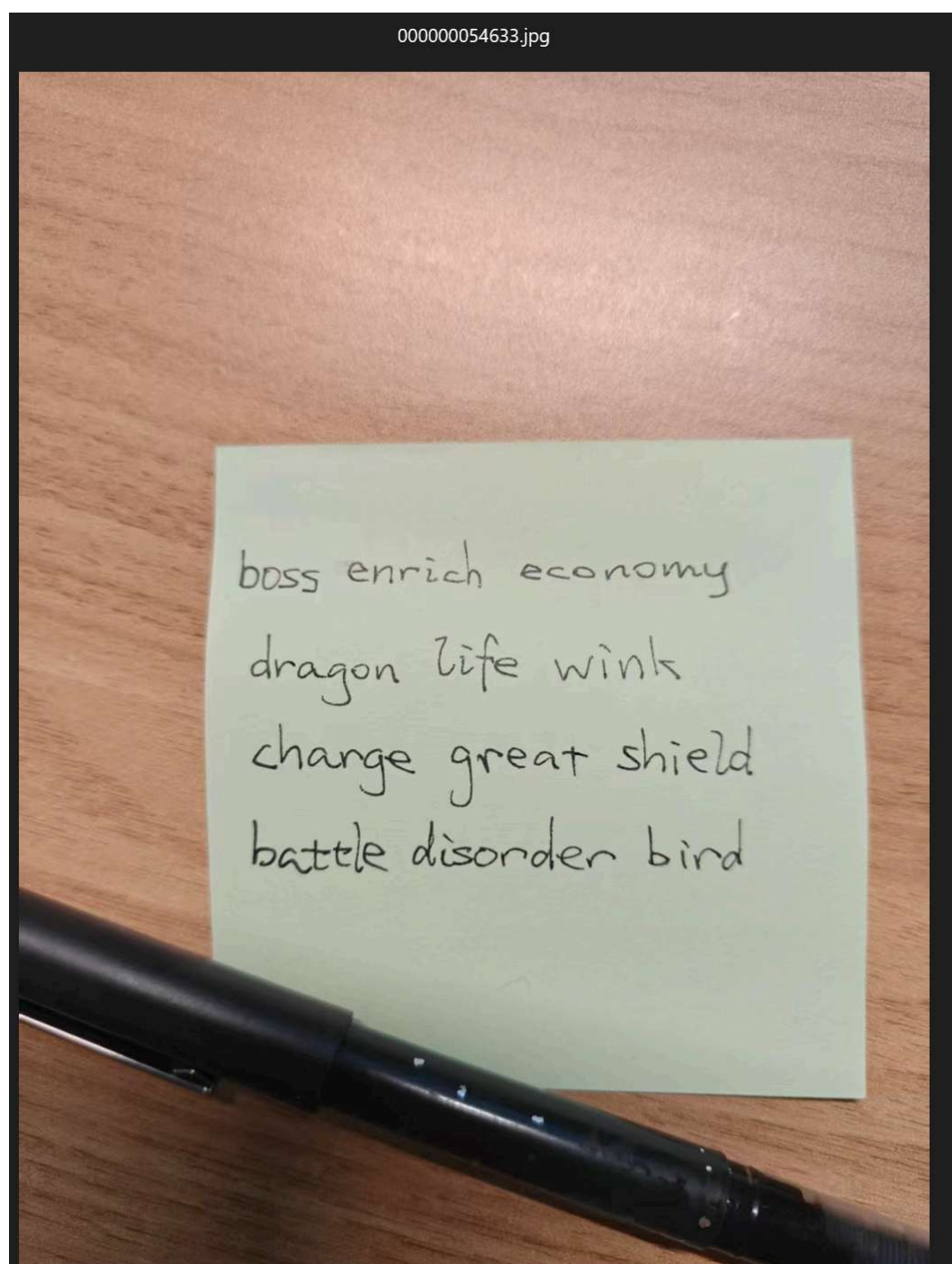
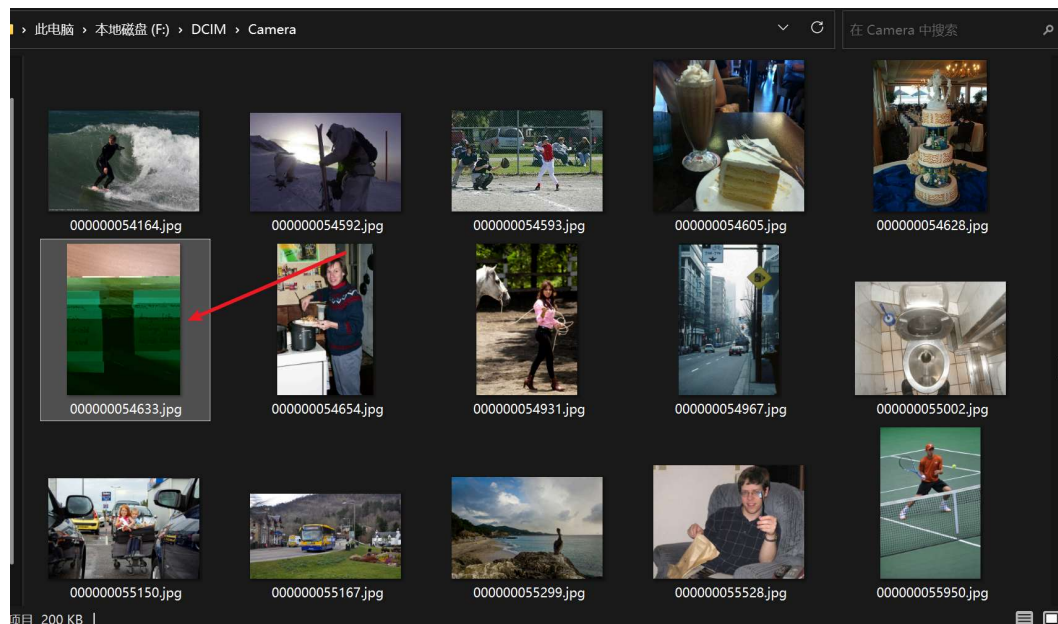




flag{shanghaiyidegelamikejiyouxiangongsi}

6. 修复损坏的图片，得到勒索收款钱包的前三个助记词（全小写，用下划线拼接，例：
play_nice_boat）。

1. 解法是在DCIM/Camera目录下找到助记词图片000000054633.jpg，发现图片错位污染。如果使用二进制编辑器，会发现JPEG尾部就存在ABAABALABUBU这个异常序列，二进制文件被该序列插入导致图片被破坏，移除这个序列即可恢复原图。难度中高。
2. 如果选手有图片处理技能，也可以通过耐心调整图片错位，拼出原图。
3. 需要选手对区块链有基本的了解，知道助记词的概念；此外，需要选手掌握主流图片文件格式的结构，知道JPG的APP0段、APP1段、0xFFD9结束标记等基本结构知识。



flag{boss_enrich_economy}

7. 分析或找到勒索病毒使用的加密密钥（例：QxRqyY!S4g^FvL）。

1. 这道题存在两个解题路径。擅长二进制分析的选手可以从Code/rensom开发目录下面找到勒索病毒的二进制程序进行逆向分析，有比较花的加密算法，没有进行混淆，动态调试也可以在传入函数插桩导出该解。
2. 擅长磁盘取证的选手不难发现嫌疑人在%APPDATA%/Roaming/下还存有一个大文件，虽然后缀名不一致，但通过魔数可以判断其是一个vhdx文件。提取出来是ReFS格式的备份，可以在仿真内找出这个备份并挂载（使用相同的bitlocker恢复密钥），里面直接可以看到本题的答案。
3. 主要考察选手对大文件、魔数、用户目录结构等取证关键信息的敏感程度，考察基本功。此外需要选手了解Windows 11 24H2版本在ReFS Dev Drive的新特性，对ReFS文件系统有所掌握。

案件: fin-22

案件信息

案件编号: 20251025015850F
创建时间: 2025-10-25 01:58:58
保存位置: E:\HL\fin-22

检材列表 (1)

检材2-archer.E01
20251025015859OX6FST | 6.97 GB | 2025-10-25 01:59:09

计算哈希 | 哈希值 | 添加文件

检材: 检材2-archer.E01

基本信息

检材编号: 20251025015859OX6FST
保存位置: D:\TMP\20251016-qz-questions\复赛\检材2-archer\检材2-archer.E01
检材时区: (UTC+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐
创建时间: 2025-10-25 01:59:09
检材大小: 6.97 GB
检材平台: Windows
磁盘大小: 40 GB
磁盘SM3: 42DDE4A368FD17641E8B56017081A5B00CAB11B89FD88495E3FE2D684A9F3DC9
预置密码:
archer |

分区信息 分区详情

flag{42DDE4A368FD17641E8B56017081A5B00CAB11B89FD88495E3FE2D684A9F3DC9}

2. 给出用户账户“archer”的创建时间。(格式: 2001-12-21 05:23:15 精确到秒)

用户操作记录

序号	操作时间	主机名称	用户名	用户SID	操作描述	操作描述
40	2022-02-05 00:21:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已更改用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
41	2022-02-05 00:21:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已更改用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
42	2022-02-05 00:21:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已更改用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
43	2022-02-05 00:21:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已更改用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
44	2022-02-05 00:21:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已更改用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
45	2022-02-05 00:25:26	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已创建用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
46	2022-02-05 00:25:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已应用用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
47	2022-02-05 00:25:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已更改用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
48	2022-02-05 00:25:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已更改用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
49	2022-02-05 00:25:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已更改用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
50	2022-02-05 00:26:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已禁用用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...
51	2022-02-05 00:26:...	WORKGROUP	WIN-47955LSEQ4F5	S-1-5-18	已更改用户帐户	目标主机名称: DESKTOP-2R4NG80, 目标...

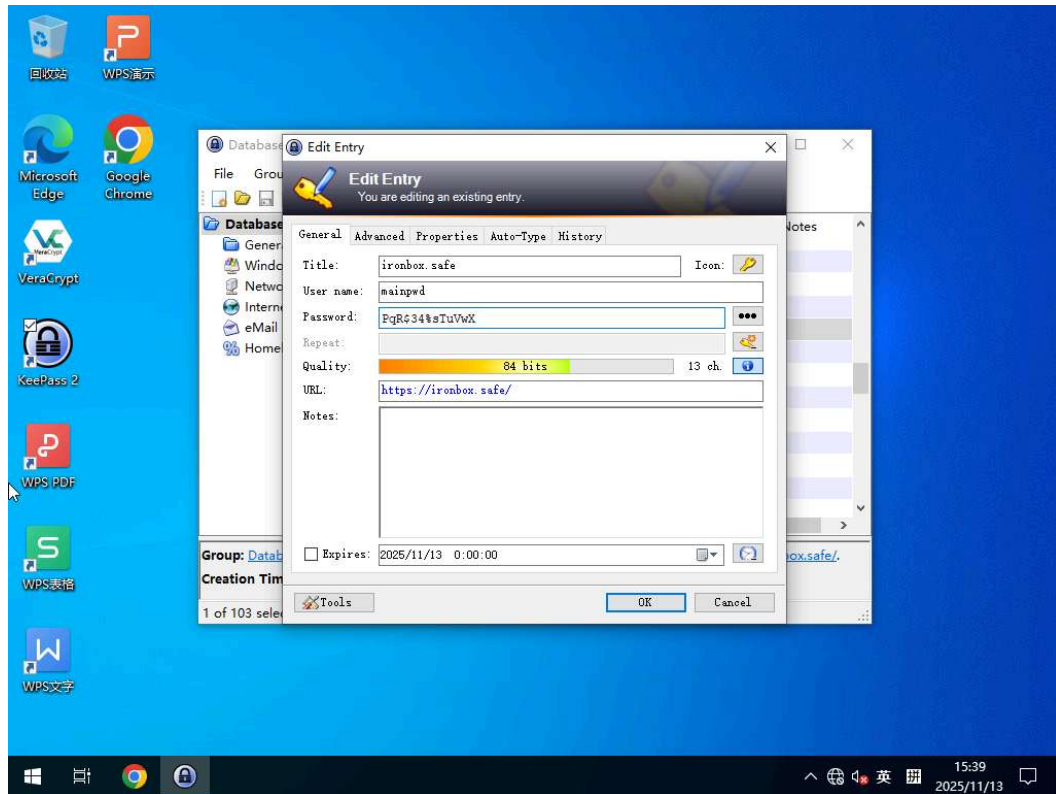
详细信息

操作时间: 2022-02-05 00:25:26
主机名称: WORKGROUP
用户名: WIN-47955LSEQ4F5
用户SID: S-1-5-18
操作描述: 已创建用户帐户
源文件: 目标主机名称: DESKTOP-2R4NG80, 目标用户名称: archer, 目标用户SID: S-1-5-21-2112860572-2941941206-3437165743-1001
源文件: 检材2-archer.E01\分区B\Windows\System32\wininit\Logs\Security.evtx
已删除: 否

flag{2022-02-05 00:25:26}


















3. 给出VeraCrypt加密卷解密的密码。

使用 *##4636#*## 解密 KeePass，获得密码。



flag{PqR\$34%\$TuVwX}

4. VeraCrypt加密卷中的最新的Excel中有一张热成像图片，计算该图片的SM3校验值（全大写）

名称	修改日期	类型	大小	最后一次保存的日期
 童缘商品介绍表.xls	2021/07/18 14:52	Microsoft Excel ...	64 KB	2021/07/18 14:52
 合同审批单.xls	2021/07/18 14:52	Microsoft Excel ...	21 KB	2019/07/03 14:13
 招商合同审批表最新版.xls	2021/07/18 14:52	Microsoft Excel ...	40 KB	2017/12/27 15:49
 合同审批表(1).xls	2021/07/18 14:52	Microsoft Excel ...	16 KB	2017/07/25 10:34
 档案使用登记表.xls	2021/07/18 14:52	Microsoft Excel ...	19 KB	2017/05/11 15:06
 合同审批表样板.xls	2021/07/18 14:52	Microsoft Excel ...	155 KB	2017/03/26 14:52
 档案借阅登记表.xls	2021/07/18 14:52	Microsoft Excel ...	28 KB	2017/02/23 14:09
 公司内部文件归档登记表.xls	2021/07/18 14:52	Microsoft Excel ...	22 KB	2016/03/18 09:21
 文件资料存档登记表.xls	2021/07/18 14:52	Microsoft Excel ...	21 KB	2015/08/12 09:27
 公司合同审批表.xls	2021/07/18 14:52	Microsoft Excel ...	34 KB	2014/11/27 17:44
 档案归档登记表 (1).xls	2021/07/18 14:52	Microsoft Excel ...	19 KB	2013/12/27 10:05
 办公用品采购记录统计表.xlsx	2021/07/18 14:52	Microsoft Excel ...	13 KB	2012/12/05 14:03
 部门经营会议表.xlsx	2021/07/18 14:52	Microsoft Excel ...	17 KB	2012/12/03 17:39
 各部门工作计划表.xlsx	2021/07/18 14:52	Microsoft Excel ...	9 KB	2012/09/11 15:57
 赔偿处理调查报告书.xlsx	2021/07/18 14:52	Microsoft Excel ...	15 KB	2012/09/06 20:26
 清洁工作安排表.xlsx	2021/07/18 14:52	Microsoft Excel ...	13 KB	2012/09/05 09:53
 车辆租借申请表.xlsx	2021/07/18 14:52	Microsoft Excel ...	11 KB	2012/09/04 17:18

D:\TMP\20251016-qz-questions\复赛\检材2-archer\v\template\童缘商品介绍表.xls\xl\media\

文件(F) 编辑(E) 查看(V) 书签(A) 工具(T) 帮助(H)

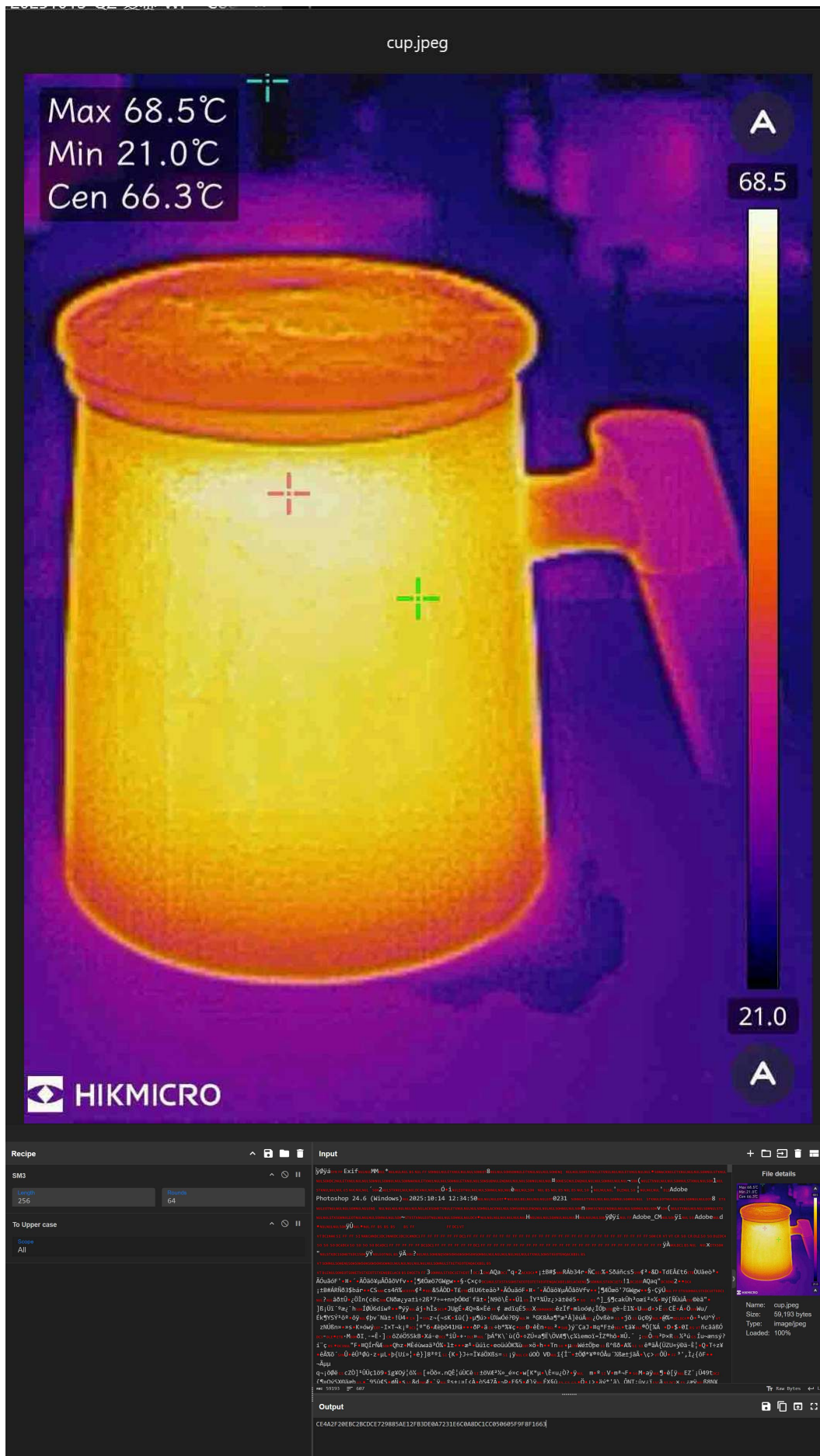
      

添加 解压 测试 复制 移动 删除 信息



v\template\童缘商品介绍表.xls\xl\media\

名称	
 cup.jpeg	59
 image1.jpeg	4



flag{CE4A2F20EBC2BCDCE729885AE12FB3DE0A7231E6C0A8DC1CC050605F9F8F1663}

5. VeraCrypt加密卷中有一个路由器备份镜像, 请给出其中的PPPoE账号

```
/检材2-archer/v/backup
$ grep -i pppoe . -R
匹配到二进制文件 ./mtd1.bin
匹配到二进制文件 ./mtd4.bin
匹配到二进制文件 ./mtd6.bin
```

mtd1.bin x

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
3DD0	65	69	6E	63	6E	5F	4C	32	3D	31	35	00	76	32	72	61	eincn_L2=15.v2ra
3DE0	79	5F	64	6F	6F	72	3D	31	30	39	39	00	61	70	70	5F	y_door=1099.app_
3DF0	31	32	39	3D	30	33	36	32	61	62	32	35	32	33	34	33	129=0362ab252343
3E00	00	6E	66	5F	61	6C	67	5F	68	33	32	33	3D	30	00	76	.nf_alg_h323=0.v
3E10	70	6E	73	5F	6F	76	5F	6D	6F	64	65	3D	31	00	66	61	pns_ov_mode=1.fa
3E20	6B	65	69	6E	63	6E	5F	4C	33	3D	35	00	61	70	70	5F	keincn_L3=5.app_
3E30	31	38	3D	30	00	77	6C	5F	77	65	70	5F	78	3D	30	00	18=0.wl_wep_x=0.
3E40	72	74	5F	6D	6F	64	65	3D	61	70	00	73	74	5F	66	74	rt_mode=ap.st_ft
3E50	70	5F	70	6D	61	78	3D	35	30	31	30	30	00	64	68	63	p_pmax=50100.dhc
3E60	70	5F	64	6E	73	33	5F	78	3D	00	76	70	6E	70	72	6F	p_dns3_x=.vpnp
3E70	78	79	5F	77	61	6E	5F	70	6F	72	74	3D	38	38	38	38	xy_wan_port=8888
3E80	00	77	61	6E	5F	70	70	70	6F	65	5F	75	73	65	72	6E	.wan_pppoe_usern
3E90	61	6D	65	3D	68	65	72	65	79	6F	75	61	72	65	00	61	ame=hereyouare.a
3EA0	70	70	35	5F	76	65	72	3D	32	30	32	32	2D	30	34	2D	pp5_ver=2022-04-
3EB0	30	34	00	73	68	65	6C	6C	69	6E	61	62	6F	78	5F	65	04.shellinbox_e
3EC0	6E	61	62	6C	65	3D	30	00	77	61	6E	5F	73	74	62	5F	nable=0.wan_stb_
3ED0	78	3D	30	00	72	74	5F	67	75	65	73	74	5F	65	6E	61	x=0.rt_guest_ena
3EE0	62	6C	65	3D	30	00	69	70	36	5F	77	61	6E	5F	70	72	ble=0.ip6_wan_pr
3EF0	69	76	3D	30	00	61	64	6D	5F	73	74	61	74	75	73	3D	iv=0.adm_status=
3F00	35	63	39	39	39	62	00	72	74	5F	4B	69	63	6B	53	74	5c999b.rt_KickSt
3F10	61	52	73	73	69	4C	6F	77	3D	30	00	73	74	5F	66	74	aRssiLow=0.st_ft
3F20	70	5F	6D	6F	64	65	3D	31	00	77	6C	5F	63	72	79	70	p_mode=1.wl_cryp

Find Results

	Address	Value
	35B3h	pppoe
	37EFh	pppoe
12	3E85h	pppoe

flag{hereyouare}

DFIR-prx

请分析【检材3】，并对以下问题作答。

1. 请给出该计算机的最后一次异常关机的开机时间（格式：2001-12-21 05:23:15 精确到秒）

刷新 详情/预览

请选择/输入持有人/检索

检材3-clash... 7/18533

- 用户痕迹 151
- 基本信息 1881
- 系统信息 23
- 默认浏览器 1
- 用户列表 8
- 账户操作记录 106
- 本地凭据 1
- 登录信息 10
- 开关机时间 6**
- 自启动程序 4
- 默认打开方式 195
- 系统服务 572
- 安装软件 67
- 软件快捷方式 52
- 可执行程序 48
- USB设备信息 8
- USB最近使用记录 10
- 硬件信息 211
- 网络配置 28
- 驱动信息 362
- 回收站记录 3
- 预执行文件 165
- 系统时间变更 1
- 服务日志 32
- 事件日志 13722

检材3-clash.aff > 基本信息 > 开关机时间

序号	开始时间	关机时间	持续时间	备注
1		2022-02-05 06:21:47		关机类型: 非正常关机。如果系统停止响应, 发生崩溃或意外断电, 则可能会导致此错误;
2	2022-02-05 06:21:36			非正常关机或未关机
3	2025-10-15 18:10:55	2025-10-15 18:11:07	00:00:12	关机类型: 非正常关机。如果系统停止响应, 发生崩溃或意外断电, 则可能会导致此错误;
4	2025-10-15 18:34:20	2025-10-15 18:34:29	00:00:09	关机类型: 非正常关机。如果系统停止响应, 发生崩溃或意外断电, 则可能会导致此错误;
5	2025-10-15 18:52:57	2025-10-15 18:53:07	00:00:10	关机类型: 非正常关机。如果系统停止响应, 发生崩溃或意外断电, 则可能会导致此错误;
6	2025-10-15 19:24:37			非正常关机或未关机

详细信息

开机时间: 2025-10-15 19:24:37

备注: 非正常关机或未关机

源文件: 检材3-clash.aff\分区6\Windows\System32\winevt\Logs\System.evtx

已删除: 否

flag{2025-10-15 19:24:37}

2. 该系统中曾经插入过一个USB设备“SMI USB DISK”，请给出他的序列号

刷新 详情/预览

请选择/输入持有人/检索

检材3-clash... 7/18533

- 用户痕迹 151
- 基本信息 1881
- 系统信息 23
- 默认浏览器 1
- 用户列表 8
- 账户操作记录 106
- 本地凭据 1
- 登录信息 10
- 开关机时间 6
- 自启动程序 4
- 默认打开方式 195
- 系统服务 572
- 安装软件 67
- 软件快捷方式 52
- 可执行程序 48
- USB设备信息 8**
- USB最近使用记录 10
- 硬件信息 211
- 网络配置 28
- 驱动信息 362
- 回收站记录 3
- 预执行文件 165
- 系统时间变更 1
- 服务日志 32
- 事件日志 13722
- 事件日志分析 1276
- ShimCache 41
- win10通知 7 / 8
- 缩略图 554
- 任务计划 191

检材3-clash.aff > 基本信息 > USB设备信息

序号	名称	设备描述	设备序列号
1	SMI USB DISK USB Device	其他名称: SMI USB DISK USB Device, E:\; 实际容量: 30G	AA00000000000489
2	Bluetooth Device (Personal Area Net...	其他名称: Bluetooth Device (Personal Area Network)	
3	@System32\drivers\usbxhci.sys,#10...	其他名称: @System32\drivers\usbxhci.sys,#1073807361;%...	
4	VMware Virtual USB Mouse	其他名称: USB Composite Device	
5	VMware Virtual USB Tablet	其他名称: USB Input Device	
6	VMware Virtual USB Hub	其他名称: Generic USB Hub	
7	VMware Virtual USB Hub	其他名称: Generic USB Hub	
8	VMware Virtual USB Hub	其他名称: Generic USB Hub	

详细信息

名称: SMI USB DISK USB Device

厂商_产品_版本: SMI_USB_DISK_1100

设备描述: 其他名称: SMI USB DISK USB Device, E:\; 实际容量: 30G

设备序列号: AA00000000000489

设备类型: Storage

设备实例路径: USB\VID_090C&PID_1100\AA000000000015053

首次接入时间: 2022-02-05 06:26:11

最后接入时间: 2025-10-15 17:57:52

最后弹出时间: 2025-10-15 17:57:52

服务: USBSTOR

硬件ID: USB\VID_090C&PID_1100&REV_1100 USB\VID_090C&PID_1100

设备Guid: {36fc9e60-c465-11cf-8056-444553540000}

驱动: {36fc9e60-c465-11cf-8056-444553540000}\0010

全路径: 检材3-clash.aff\分区6\Windows\System32\config\SYSTEM

flag{AA00000000000489}

3. 镜像中安装了代理工具“Ficlash”，请给出使用了“globaldns”作为域名服务器的代理配置文件中，使用vmess协议的代理节点对应的UUID（全大写）

选择并输入持有人/临时编号

检测3-clash.aff / 分区6 / Users / caster / AppData / Roaming / com.follow / clash / profiles

在 profiles 中搜索

序号	名称	大小	创建时间	修改时间	来源
1	1644013114514.yaml	5.56 KB	2022-02-05 06:29:00	2022-02-05 06:29:00	检测3-clash.aff/分区6/Users/caster/AppData/Roaming/com.follow/clash/profiles/1644013114514.yaml
2	1644013739086.yaml	8.97 KB	2022-02-05 06:28:59	2022-02-05 06:28:59	检测3-clash.aff/分区6/Users/caster/AppData/Roaming/com.follow/clash/profiles/1644013739086.yaml
3	1644013875545.yaml	5.31 KB	2022-02-05 06:31:15	2022-02-05 06:31:15	检测3-clash.aff/分区6/Users/caster/AppData/Roaming/com.follow/clash/profiles/1644013875545.yaml
4	1644013888767.yaml	3.81 KB	2022-02-05 06:31:28	2022-02-05 06:31:28	检测3-clash.aff/分区6/Users/caster/AppData/Roaming/com.follow/clash/profiles/1644013888767.yaml

详细信息

名称: 1644013114514.yaml
扩展名: .yaml
类型: 文件
大小: 5.56 KB
创建时间: 2022-02-05 06:29:00
更新时间: 2022-02-05 06:29:00
修改时间: 2022-02-05 06:29:00
元数据哈希: 35001
来源: 检测3-clash.aff/分区6/Users/caster/AppData/Roaming/com.follow/clash/profiles/1644013114514.yaml
加密类型: 未加密
已删除: 否

原类型视图 文本视图 十六进制视图

PAGE ZOOM HIGHLIGHT

```
allow-port: 7890
allow-lan: true
bind-address: "*"
mode: v2c
log-level: info
external-controller: "127.0.0.1:9090"
dns:
  enable: false
  ip6: false
  default-nameserver: [223.5.5.5, 119.29.29.29]
  enhanced-mode: fake-ip
  fake-ip-range: 198.18.0.1/16
  use-hosts: true
  nameserver: ["https://doh.pub/dns-query", "https://dns.cloudflare.com/dns-query"]
  fallback: ["https://doh.dns.sb/dns-query", "https://dns.cloudflare.com/dns-query", "https://dns.burx.net/dns-query", "https://7.8.4.4:837"]
  fallback-filter: { geoip: true, ipcidr: [240.0.0.0/4, 0.0.0.0/24] }
proxies:
  - { name: flag6, type: vless, server: zhu.ji.chi, port: 11451, uuid: F2BE4BD1-872F-4FB0-84BD-04514CB52B9, udp: true, tls: true, skip-cert-verify: false, flow: "", client-fingerprint: chrome, servername: ha.ji.me, reality-opts: { public-key: hAjImbOnAnBelIudUoHaJiDaAiYiDiNaLuMiAoMiAo, short-id: hAjImb0 }, network: grpc, grpc-opts: { grpc-service-name: tj } }
  - { name: flag6, type: vless, server: zhu.ji.chi, port: 11451, uuid: F2BE4BD1-872F-4FB0-84BD-04514CB52B9, udp: true, tls: true, skip-cert-verify: false, flow: "", client-fingerprint: chrome, servername: ha.ji.me, reality-opts: { public-key: hAjImbOnAnBelIudUoHaJiDaAiYiDiNaLuMiAoMiAo, short-id: hAjImb0 }, network: grpc, grpc-opts: { grpc-service-name: tj } }
  - { name: welcome, server: bala.baba.ba, port: 11451, type: vmess, uuid: AB9E6E97-A28E-4262-8584-48D7F850D531, alterId: 0, cipher: auto, tls: false, skip-cert-verify: true, udp: true, tfo: false }
  - { name: flag7, type: trojan, server: u.cc.you, port: 443, password: "niceworkkude" }
  - { name: flag8, type: trojan, server: u.cc.you, port: 443, password: "niceworkkude" }
  - { name: flag9, type: trojan, server: u.cc.you, port: 443, password: "niceworkkude" }

proxy-groups:
```

flag{AB9E6E97-A28E-4262-8584-48D7F850D531}

4. 用户在导入代理文件后，删除了复制进计算机的代理配置文件，请给出删除该文件的账户SID

Windows 10 系统信息界面。左侧是系统设置树，右侧是系统信息详情。在“用户列表”部分，显示了本地账户列表。其中，用户名为“caster”的本地账户被选中，其详细信息如下：

名称	用户类型	登录密码	SID	最后登录时间
Administrator	本地账户	[空密码]	S-1-5-21-...	
Guest	本地账户	[空密码]	S-1-5-21-...	
DefaultAccount	本地账户	[空密码]	S-1-5-21-...	
WDAGUtility...	本地账户	[空密码]	S-1-5-21-...	
caster	本地账户	[空密码]	S-1-5-21-2839104552-2639793746-125108461-1001	2025-10-15 19:24:49
SYSTEM	本地账户	[空密码]	S-1-5-18	
LocalService	本地账户	[空密码]	S-1-5-19	
NetworkServi...	本地账户	[空密码]	S-1-5-20	

详细信息：

- 名称: caster
- 用户类型: 本地账户
- 登录密码: [空密码]
- SID: S-1-5-21-2839104552-2639793746-125108461-1001
- 最后登录时间: 2025-10-15 19:24:49
- 账号过期时间: 2185-07-22 07:34:33
- 账户是否有效: 是
- 登录次数: 6
- 用户目录: C:\Users\caster
- LM HASH: aad3b435b51404eeaad3b435b51404ee
- NT HASH: 31d6cfe0d16ae931b73c59d7e0c089c0
- 已删除: 否

flag{S-1-5-21-2839104552-2639793746-125108461-1001}

5. 用户在境外网站下载了一个PDF并进行了打印，请给出打印内容中的软件序列号

Windows 10 文件资源管理器界面。左侧是文件树，右侧是文件列表。在“下载”文件夹中，选中了名为“感谢你的购买.pdf”的文件。该文件的详细信息如下：

名称	大小	创建时间	修改时间	全路径
感谢你的购买.pdf	148.52 KB	2025-10-15 17:51:34	2025-10-15 19:28:36	检材3-clashaff\分区6\无效数据\感谢你的购买.pdf

详细信息：

- 名称: 感谢你的购买.pdf
- 扩展名: pdf
- 类型: 文件
- 大小: 148.52 KB
- 创建时间: 2025-10-15 17:51:34
- 访问时间: 2025-10-15 19:28:36
- 修改时间: 2025-10-15 19:28:36
- 元数据地址: 101336
- 全路径: 检材3-clashaff\分区6\无效数据\感谢你的购买.pdf
- 加密类型: 未加密
- 已删除: 是

十六进制视图显示的内容如下：

```
[RonBox Pro] *****
*****
*** A3F8-JK22-MSQT-R4T6 ***
*****
1. [RonBox Pro] *****
2. *****
3. *****
4. *****
***** [*****]
```

flag{A3F8-JK22-MSQT-R4T6}

DFIR-RAID

请分析【检材4】，并对以下问题作答。

数码博主牛同学家里的设备坏了，需要你提取并恢复数据。

本题涉及到对fnOS、MD-RAID、LVM和btrfs的数据恢复和固定。

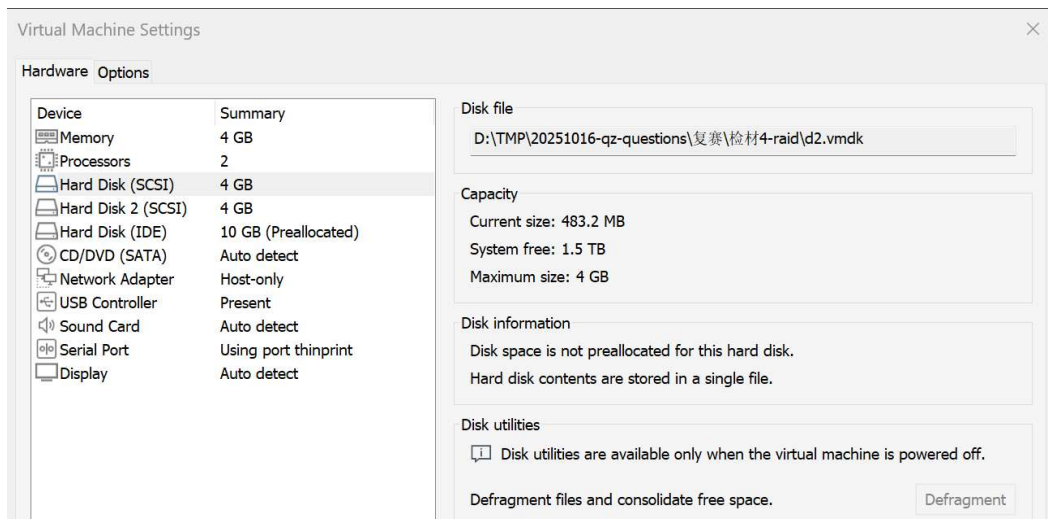
1. 给出引导分区的UUID（如：84f012d9-1880-4306-9ce3-00695f81771c）。

导出检材4-raid-1.E01 检材4-raid-2.E01文件的RAW磁盘，并转换为VMDK格式，

qemu-img.exe convert -pO vmdk r1.001 d1.vmdk

qemu-img.exe convert -pO vmdk r2.001 d2.vmdk

仿真 检材4-raid-0.E01，并将 d1.vmdk d2.vmdk 挂载进虚拟机。



```
root@kknnew:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G   0% /dev
tmpfs           394M   7.9M  386M   2% /run
/dev/sdc2       9.7G   5.5G   3.7G  60% /
tmpfs           2.0G   1.4M   2.0G   1% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
efivarfs        256K   57K   195K  23% /sys/firmware/efi/efivars
/dev/sdc1       93M   8.1M   85M   9% /boot/efi
tmpfs           394M   0    394M   0% /run/user/0
root@kknnew:~# blkid /dev/sdc1
/dev/sdc1: UUID="68F8-C0E3" BLOCK_SIZE="512" TYPE="ufat" PARTLABEL="BOOT" PARTUUID="09f8b70e-8787-4df8-9b61-f60c9d8764dd"
root@kknnew:~#
```

flag{09f8b70e-8787-4df8-9b61-f60c9d8764dd}

2. 给出系统DLNA服务端的版本号（如：1.14.514）。

```
root@kknnew:/var/log# ps aux | grep -i dlna
root      1534  0.0  0.4 219156 17404 ?        Ssl  16:34   0:00 /usr/trim/bin/minidlnad -f /usr/trim/
root      2641  0.0  0.0  6340  2164 tty1    S+   16:37   0:00 grep --color=auto -i dlna
root@kknnew:/var/log# /usr/trim/bin/minidlnad --help
Usage:
  /usr/trim/bin/minidlnad [-d] [-u] [-f config_file] [-p port]
                        [-i network_interface] [-u uid_to_run_as] [-g group_to_run_as]
                        [-t notify_interval] [-P pid_filename]
                        [-s serial] [-m model_number]
                        [-w url] [-r] [-L] [-S] [-U] [-h]

Notes:
  Notify interval is in seconds. Default is 895 seconds.
  Default pid file is /var/run/minidlna/minidlna.pid.
  With -d minidlna will run in debug mode (not daemonize).
  -w sets the presentation url. Default is http address on port 80
  -u enables verbose output
  -h displays this text
  -r forces a rescan
  -R forces a rebuild
  -L do not create playlists
  -S changes behaviour for systemd/launchd
  -U print the version number
root@kknnew:/var/log# /usr/trim/bin/minidlnad -U
Version 1.3.3
root@kknnew:/var/log#
```

flag{1.3.3}

3. 给出名为newnew的LVM卷组的UUID（大小写字母+数字，如：FmGRh3-zhok-iVi8-7qTD-S5Bl-MAEN-NYM5Sk）。

```
root@kknnew:/var/log# ugs -v
Creating directory "/etc/lvm/archive"
Archiving volume group "newnew" metadata (seqno 4).
Creating directory "/etc/lvm/backup"
Creating volume group backup "/etc/lvm/backup/newnew" (seqno 4).
UG Attr Ext #PV #LV #SN VSize UFree UG UUID UProfile
newnew wz--n- 4.00m 1 2 1 <7.99g <5.99g B85Yqn-ZGfs-GCVj-wN0U-4EBW-9Pxz-snxGtv
root@kknnew:/var/log#
```

flag{B85Yqn-ZGfs-GCVj-wN0U-4EBW-9Pxz-snxGtv}

如果这一步mdadm未能自动重建RAID，可通过 mdadm --stop /dev/md127 拆分旧的组，然后 mdadm --assemble /dev/md1 /dev/sda1 /dev/sdb1 手动重建。

4. newnew-vol1 使用的文件系统uuid为（全小写）。

```
root@knewnew:/var/log#
root@knewnew:/var/log# btrfs filesystem show
WARNING: adding device /dev/mapper/newnew-bak202510 gen 19 but found an existing device /dev
ERROR: cannot scan /dev/mapper/newnew-bak202510: File exists
Label: none      uuid: 5ab9456c-cce7-4bcd-8e8c-f81823fd059d
Total devices 1 FS bytes used 198.81MiB
devid    1 size 1.00GiB used 574.38MiB path /dev/mapper/newnew-vol1
root@knewnew:/var/log#
```

flag{5ab9456c-cce7-4bcd-8e8c-f81823fd059d}

5. 恢复数据盘的磁盘阵列，恢复逻辑卷备份，给出卷内被删除文件的文件名（如：result.txt）。

```
root@knewnew:/var/log# ls
LV      VG      Attr      LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
bak202510 newnew sui-a-s--- 1.00g      vol1    3.20
vol1     newnew ovi-a-s--- 1.00g
root@knewnew:/var/log# mkdir mount^C
root@knewnew:/var/log# ls /mnt
root@knewnew:/var/log# mkdir /mnt/vol1 /mnt/bak202510
root@knewnew:/var/log# mount /dev/mapper/
control          newnew-bak202510          newnew-bak202510-cow  newnew-vol1          newnew-vol1-real
root@knewnew:/var/log# mount /dev/mapper/newnew-vol1 /mnt/vol1
root@knewnew:/var/log# mount /dev/mapper/newnew-bak202510 /mnt/bak202510/
root@knewnew:/var/log# cd /mnt
root@knewnew:/mnt# ls
bak202510  vol1
root@knewnew:/mnt#
```

```
root@knewnew:/mnt# ls
bak202510  vol1
root@knewnew:/mnt# diff --brief bak202510/ vol1/
Common subdirectories: bak202510/Code and vol1/Code
Common subdirectories: bak202510/Music and vol1/Music
Common subdirectories: bak202510/thumb and vol1/thumb
root@knewnew:/mnt# diff -r --brief bak202510/ vol1/
Only in vol1/Code: axum: cred-0009.json
Only in bak202510/Code: dubbo-dubbo-configcenter/dubbo-configcenter-zookeeper/src/test/java/org/apache/dubbo/configcenter/support/zookeeper: ZookeeperDynamicConf
figurationTest.java
Only in vol1/thumb: Code
root@knewnew:/mnt#
```

flag{ZookeeperDynamicConfigurationTest.java}

DFIR-流量分析

请分析【教材5】，并对以下问题作答。

1. 被攻击的软件名称

Wireshark · Conversations · 教材5-pcap.cap

Conversation Settings

Address A	Address B	分组	Bytes	Stream ID	Packets A → B
192.168.122.1	192.168.122.187	648	367 kB	0	398
192.168.122.23	192.168.122.187	8 550	1 MB	1	4,277
192.168.122.75	192.168.122.187	199	621 kB	5	112
192.168.122.187	39.156.70.37	8	784 字节	4	4
192.168.122.187	101.6.15.130	67	49 kB	3	29
192.168.122.187	146.75.114.132	10	1 kB	2	6

复制

Follow Stream...

教材5-pcap.cap

文件(F) 编辑(E) 视图(V) 规格(S) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(T) 帮助(H)

ipstream eq 5

No.	Time	DT	Source	Destination	Protocol	Length	Info
3090	102.729381	2025-10-23 00:10:12.635824	192.168.122.75	192.168.122.187	TCP	74	37358 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2111224904 TSecr=0 WS=128
3091	102.729447	2025-10-23 00:10:12.635890	192.168.122.187	192.168.122.75	TCP	74	6379 → 37358 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1234189597 TSecr=2111224904
3092	102.729490	2025-10-23 00:10:12.635933	192.168.122.75	192.168.122.187	TCP	66	37358 → 6379 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2111224905 TSecr=1234189597
3093	102.729510	2025-10-23 00:10:12.635952	192.168.122.187	192.168.122.75	RESP	108	Request: AUTH default: 12345678901234567890
3094	102.729545	2025-10-23 00:10:12.635988	192.168.122.187	192.168.122.75	TCP	66	6379 → 37358 [ACK] Seq=1 Ack=40 Win=65152 Len=0 TSval=1234189597 TSecr=2111224905
3095	102.729648	2025-10-23 00:10:12.636091	192.168.122.187	192.168.122.75	RESP	130	Response: Error: WRONGPASS invalid username-password pair or user is disabled.
3096	102.729679	2025-10-23 00:10:12.636122	192.168.122.75	192.168.122.187	TCP	66	37358 → 6379 [ACK] Seq=40 Ack=65 Win=64256 Len=0 TSval=2111224905 TSecr=1234189597
3097	102.729716	2025-10-23 00:10:12.636159	192.168.122.75	192.168.122.187	RESP	93	Request: COMMAND DOCS
3098	102.729760	2025-10-23 00:10:12.636203	192.168.122.187	192.168.122.75	RESP	100	Response: Error: NOAUTH Authentication required.
3099	102.729798	2025-10-23 00:10:12.636241	192.168.122.75	192.168.122.187	RESP	92	Request: INFO SERVER
3100	102.729840	2025-10-23 00:10:12.636283	192.168.122.187	192.168.122.75	RESP	100	Response: Error: NOAUTH Authentication required.
3101	102.729881	2025-10-23 00:10:12.636324	192.168.122.75	192.168.122.187	RESP	83	Request: COMMAND
3102	102.729917	2025-10-23 00:10:12.636360	192.168.122.187	192.168.122.75	RESP	100	Response: Error: NOAUTH Authentication required.
3105	102.773471	2025-10-23 00:10:12.679914	192.168.122.75	192.168.122.187	TCP	66	37358 → 6379 [ACK] Seq=110 Ack=167 Win=64256 Len=0 TSval=2111224949 TSecr=1234189597
3110	104.525681	2025-10-23 00:10:14.432124	192.168.122.75	192.168.122.187	TCP	66	37358 → 6379 [FIN, ACK] Seq=110 Ack=167 Win=64256 Len=0 TSval=2111224949 TSecr=1234189597
3111	104.525870	2025-10-23 00:10:14.432313	192.168.122.75	192.168.122.187	TCP	66	6379 → 37358 [FIN, ACK] Seq=167 Ack=111 Win=65152 Len=0 TSval=1234111393 TSecr=2111226701
3122	113.404031	2025-10-23 00:10:13.310474	192.168.122.75	192.168.122.187	TCP	66	37358 → 6379 [ACK] Seq=111 Ack=168 Win=64256 Len=0 TSval=2111226701 TSecr=123411393
3123	113.404059	2025-10-23 00:10:13.310592	192.168.122.75	192.168.122.187	TCP	74	46688 → 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2111235578 TSecr=0 WS=128
3124	113.404111	2025-10-23 00:10:13.310554	192.168.122.187	192.168.122.75	TCP	74	6379 → 46688 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1234128271 TSecr=2111235578
3125	113.404206	2025-10-23 00:10:13.310649	192.168.122.187	192.168.122.75	RESP	66	46688 → 6379 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2111235578 TSecr=1234128271
3126	113.404230	2025-10-23 00:10:13.310673	192.168.122.75	192.168.122.187	TCP	66	46688 → 6379 [ACK] Seq=47 Ack=65 Win=64256 Len=0 TSval=2111235579 TSecr=1234128272
3127	113.404271	2025-10-23 00:10:13.310714	192.168.122.75	192.168.122.187	RESP	93	Request: COMMAND DOCS
3128	113.404344	2025-10-23 00:10:13.310787	192.168.122.187	192.168.122.75	RESP	100	Response: Error: NOAUTH Authentication required.
3129	113.404374	2025-10-23 00:10:13.310817	192.168.122.75	192.168.122.187	RESP	92	Request: INFO SERVER
3130	113.404438	2025-10-23 00:10:13.310881	192.168.122.187	192.168.122.75	RESP	100	Response: Error: NOAUTH Authentication required.
3131	113.404473	2025-10-23 00:10:13.310916	192.168.122.75	192.168.122.187	RESP	83	Request: COMMAND

Frame 3093: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on 0

Ethernet II, Src: 52:54:00:30:00:00 (52:54:00:30:00:00), Dst: 52:54:00:58:00:1f (52:54:00:58:00:1f)

Internet Protocol Version 4, Src: 192.168.122.75, Dst: 192.168.122.187

Transmission Control Protocol, Src Port: 37358, Dst Port: 6379, Seq: 1, Ack: 1, Len: 39

Redis Serialization Protocol

Array Length: 3

Length: 3

Bulk String: AUTH

Bulk String: default

Bulk String: aaaaaa

```
flag{redis}
```

2. 攻击者第二次测试的密码

```
File Edit View Window Help
文(文件) 编辑(E) 视图(V) 窗口(W) 帮助(H)
[Icons] [Search Bar] [Filter] [Columns: No., Time, DT, Source, Destination, Protocol, Length, Info] [Refresh] [Zoom In] [Zoom Out] [Reset Zoom] [Full Screen]

nmapstream eq 5

No.    Time      DT          Source                Destination            Protocol  Length  Info
-----
3090   102.729381  2025-10-23 00:10:12.635824  192.168.122.75        192.168.122.187       TCP      74      37358 -> 6379 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=211224984 TSecr=1234109557
3091   102.729447  2025-10-23 00:10:12.635898  192.168.122.187       192.168.122.75       TCP      74      6379 -> 37358 [SYN, ACK] Seq=0 Ack=1 Win=65168 Len=0 MSS=1460 SACK_PERM TSval=2112341139 TSecr=1234109557
3092   102.729490  2025-10-23 00:10:12.635933  192.168.122.75        192.168.122.187     TCP      76      37358 -> 6379 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=211224905 TSecr=1234109597
3093   102.729519  2025-10-23 00:10:12.635962  192.168.122.75        192.168.122.187     RESP     105     Request: AUTH default aaaaaa
3094   102.729545  2025-10-23 00:10:12.635988  192.168.122.187       192.168.122.75       TCP      66      6379 -> 37358 [ACK] Seq=1 Ack=1 Win=65152 Len=0 TSval=2112340957 TSecr=1211222495
3095   102.729548  2025-10-23 00:10:12.635991  192.168.122.187       192.168.122.75       RESP     138     Response: Error: WRONGPASS invalid username-password pair or user is disabled.
3096   102.729679  2025-10-23 00:10:12.636165  192.168.122.75        192.168.122.187     RESP     93      Request: COMMAND DOCS
3097   102.729716  2025-10-23 00:10:12.636159  192.168.122.75        192.168.122.187     RESP     93      Request: COMMAND DOCS
3098   102.729760  2025-10-23 00:10:12.636203  192.168.122.187       192.168.122.75       RESP     100     Response: Error: NOAUTH Authentication required.
3099   102.729788  2025-10-23 00:10:12.636241  192.168.122.187       192.168.122.187     RESP     92      Request: INFO SERVER
3100   102.729840  2025-10-23 00:10:12.636283  192.168.122.75        192.168.122.187     RESP     100     Response: Error: NOAUTH Authentication required.
3101   102.729881  2025-10-23 00:10:12.636324  192.168.122.75        192.168.122.187     RESP     83      Request: COMMAND
3102   102.729917  2025-10-23 00:10:12.636360  192.168.122.187       192.168.122.75       RESP     100     Response: Error: NOAUTH Authentication required.
3103   102.729947  2025-10-23 00:10:12.636360  192.168.122.75        192.168.122.187     RESP     83      Request: COMMAND
3104   102.729978  2025-10-23 00:10:12.636414  192.168.122.75        192.168.122.187     TCP      76      37358 -> 6379 [FIN, ACK] Seq=110 Ack=167 Min=64256 Len=0 TSval=211224949 TSecr=1234109595
3110   104.525681  2025-10-23 00:10:14.432124  192.168.122.75        192.168.122.187     TCP      66      37358 -> 6379 [FIN, ACK] Seq=110 Ack=167 Min=64256 Len=0 TSval=211226701 TSecr=12341139
3111   104.525870  2025-10-23 00:10:14.432313  192.168.122.187       192.168.122.75       TCP      66      6379 -> 37358 [FIN, ACK] Seq=110 Ack=167 Min=65152 Len=0 TSval=2112341139 TSecr=2112341139
3112   104.525946  2025-10-23 00:10:14.432389  192.168.122.75        192.168.122.75       TCP      66      37358 -> 6379 [ACK] Seq=111 Ack=168 Min=64256 Len=0 TSval=211226701 TSecr=12341139
3110   113.403869  2025-10-23 00:10:23.310312  192.168.122.75        192.168.122.187     TCP      74      46688 -> 6379 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=211235578 TSecr=1234109557
3121   113.403991  2025-10-23 00:10:23.310434  192.168.122.187       192.168.122.75       TCP      74      6379 -> 46688 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1234109557 TSecr=1234109557
3122   113.404031  2025-10-23 00:10:23.310474  192.168.122.75        192.168.122.187     TCP      66      46688 -> 6379 [ACK] Seq=1 Ack=1 Min=64256 Len=0 TSval=211235578 TSecr=1234109557
3123   113.404059  2025-10-23 00:10:23.310523  192.168.122.187       192.168.122.75       TCP      66      6379 -> 46688 [ACK] Seq=1 Ack=47 Min=65152 Len=0 TSval=211235578 TSecr=1234109557
3124   113.404111  2025-10-23 00:10:23.310554  192.168.122.187       192.168.122.75       TCP      66      6379 -> 46688 [ACK] Seq=1 Ack=47 Min=65152 Len=0 TSval=211235578 TSecr=1234109557
3125   113.404206  2025-10-23 00:10:23.310649  192.168.122.187       192.168.122.75       RESP     138     Response: Error: WRONGPASS invalid username-password pair or user is disabled.
3126   113.404320  2025-10-23 00:10:23.310673  192.168.122.75        192.168.122.187     RESP     93      Request: COMMAND DOCS
3127   113.404371  2025-10-23 00:10:23.310714  192.168.122.75        192.168.122.187     RESP     93      Request: COMMAND DOCS
3128   113.404344  2025-10-23 00:10:23.310787  192.168.122.187       192.168.122.75       RESP     100     Response: Error: NOAUTH Authentication required.
3129   113.404374  2025-10-23 00:10:23.310817  192.168.122.75        192.168.122.75       RESP     92      Request: INFO SERVER
3130   113.404418  2025-10-23 00:10:23.310881  192.168.122.75        192.168.122.75       RESP     100     Response: Error: NOAUTH Authentication required.
3131   113.404473  2025-10-23 00:10:23.310916  192.168.122.75        192.168.122.187     RESP     83      Request: COMMAND

Frame 3123: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface eth0
Ethernet II, Src: 52:54:00:3b:d8:b4 (52:54:00:3b:d8:b4), Dst: 52:54:00:58:b0:1f (52:54:00:58:b0:1f)
Internet Protocol Version 4, Src: 192.168.122.75, Dst: 192.168.122.187
Transmission Control Protocol, Src Port: 46688, Dst Port: 6379, Seq: 1, Ack: 1, Len: 46
Redis Serialization Protocol
Array: length 3
Length: 3
Bulk String: AUTH
Bulk String: default
Bulk String: 1234567qwer
```

flag{1234567qwer}

3. 攻击过程中写入的文件绝对路径

The screenshot displays the Wireshark network protocol analyzer interface. The top toolbar contains various icons for file operations, network analysis, and search. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is #16, which is a TCP Reset (RST) from 192.168.122.75 to 192.168.122.75. The reset sequence number is 37068702070687069666f2829203b3f3e.
- Packet Details:** Shows the structure of the selected packet. The top section is the Ethernet II header. The bottom section is the TCP Reset (RST) header, showing the reset sequence number and the window size.
- Packet Bytes:** Shows the raw data of the selected packet. The data is a PHPinfo() output, which is a text-based representation of the server's configuration and status. The output includes various configuration variables and their values, such as 'config', 'set', 'xxx', 'dir', 'share/caddy', 'dbfilename', and 'testinfo.php'.

Red arrows point to the 'share/caddy' and 'testinfo.php' fields in the packet bytes pane, indicating the specific paths and files being accessed or modified.

```
flag{/usr/share/caddy/testinfo.php}
```