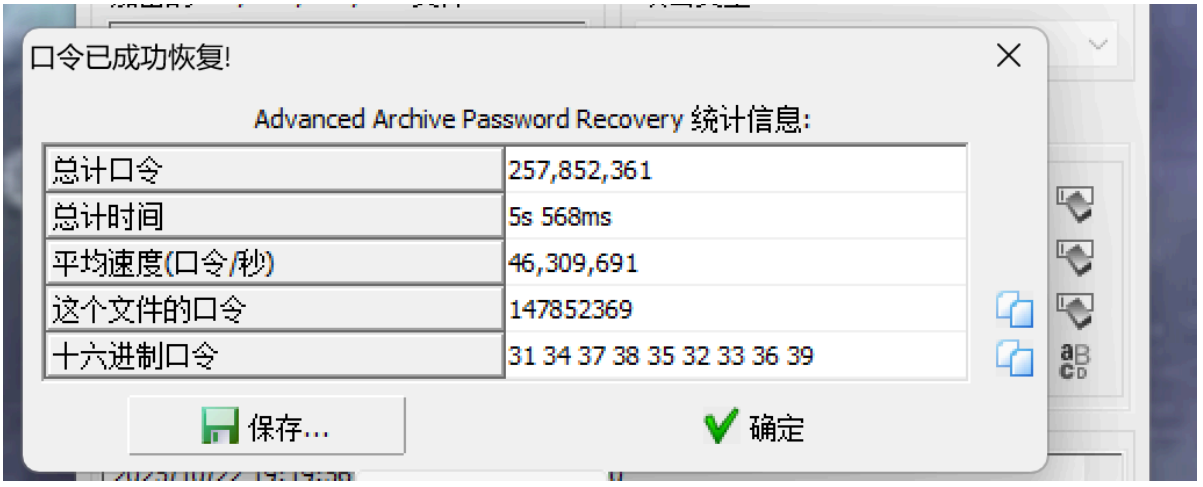
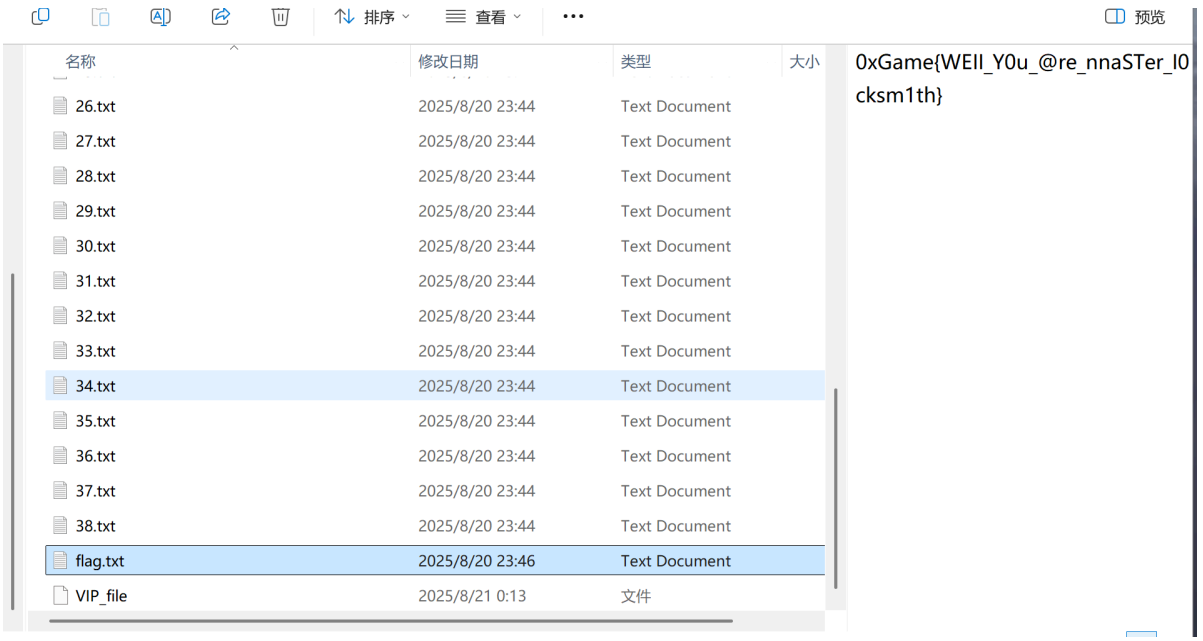
Week4_萱__B25041708_wp

Misc

1.开锁师傅2.0

当做了好久之后发现……居然能爆喵，居然能爆喵，居然能爆喵！！！





Flag：0xGame{WEll_Y0u_@re_nnaSTer_l0cksm1th}

2.开锁师傅2.0_reverge

查看不仅是真加密，而且里面有三字节的字符。CRC爆破的话，纯英文爆不了，疑似是中文

C:\Windows\System32\cmd.e

```
26 ZipCrypto  Store       900e06fe          3          15 attachment/026.txt
27 ZipCrypto  Store       d3d6edcb          3          15 attachment/027.txt
28 ZipCrypto  Store       a0abbd09          3          15 attachment/028.txt
29 ZipCrypto  Store       f175bd33          3          15 attachment/029.txt
30 ZipCrypto  Store       b037393f          3          15 attachment/030.txt
31 ZipCrypto  Store       951e15f3          3          15 attachment/031.txt
32 ZipCrypto  Store       49c8183c          3          15 attachment/032.txt
33 ZipCrypto  Store       9ca859d8          3          15 attachment/033.txt
34 ZipCrypto  Store       273a178a          3          15 attachment/034.txt
35 ZipCrypto  Store       6cd0cdac          3          15 attachment/035.txt
36 ZipCrypto  Store       267cc491          3          15 attachment/036.txt
37 ZipCrypto  Store       09003a80          3          15 attachment/037.txt
38 ZipCrypto  Store       55912595          3          15 attachment/038.txt
39 ZipCrypto  Store       b8431f23          3          15 attachment/039.txt
40 ZipCrypto  Store       43cf32bc          3          15 attachment/040.txt
41 ZipCrypto  Store       62623336          3          15 attachment/041.txt
42 ZipCrypto  Store       d2b184ff          3          15 attachment/042.txt
43 ZipCrypto  Store       32973a9e          3          15 attachment/043.txt
44 ZipCrypto  Store       1f183aa6          3          15 attachment/044.txt
45 ZipCrypto  Store       6c0fdd29          3          15 attachment/045.txt
46 ZipCrypto  Store       9e9909d2          3          15 attachment/046.txt
47 ZipCrypto  Store       01d239c2          3          15 attachment/047.txt
48 ZipCrypto  Store       7b216a3b          3          15 attachment/048.txt
49 ZipCrypto  Store       07dcdf76          3          15 attachment/049.txt
50 ZipCrypto  Store       dc21e617          3          15 attachment/050.txt
51 ZipCrypto  Store       d617d273          3          15 attachment/051.txt
52 ZipCrypto  Store       2400d931         62          74 attachment/flag.txt
53 ZipCrypto  Store       c377a0ed        792         804 attachment/huiliyidehua.txt
```

来个可以爆中文的脚本

crc6.py

D: > 0x > week4 > attachment2 > crc6.py > ...

```python
import zipfile
import zlib
from itertools import product
import os

# ========== 中日韩范围 ==========
GB2312_HANZI = ''.join(
    chr(i) for i in range(0x2000, 0xefff + 1)
)

#GB2312_HANZI = """的一是在不了有和人这中大为上个国我以要他时来用们生到作地于出就分对成会可主发年动同
#工也能下过子说产种面而方后多定行学法所民得经十三之进着等部度家电力里如水化高自二
#理起小物现实加量都两体制机当使点从业本去把性好应开它合还因由其些然前外天政四日那
#社义事平形相全表间样与关各重新线内数正心反你明看原又么利比或但质气第向道命此变条
#只没结解问意建月公无系军很情者最立代想已通并提直题党程展五果料象员革位入常文总次
#品式活设及管特件长求老头基资边流路级少图山统接知较将组见计别她手角期根论运农指几九
#区强放决西被干做必战先回则任取据处队南给色光门即保治北造百规热领七海口东导器压志世
#金增争济阶油思术极交受联什认六共权收证改清己美再采转更单风切打白教速花带安场身车例
#真务具万每目至达走积示议声报斗完类八离华名确才科张信马节话米整空元况今集温传土许步
#群广石记需段研界拉林律叫且究观越织装影算低持音众书布复容儿须际商非验连断深难近矿
#千周委素技备半办青省列习响约支般史感劳便团往酸历市克何除消构府称太准精值号率族维划
#选标写存候毛亲快效斯院查江型眼王按格养易置派层片始却专状育厂京识适属圆包火住调满县
#局照参红细引听该铁价严龙飞言尔棵密码钥匙邮棠树请输首，；。《》？？、“”：；【】、"""

def load_dict_from_file(filepath):
    """从文件加载字典，每行一个词"""
    if not os.path.exists(filepath):
```

```python
def load_dict_from_file(filepath):
    """从文件加载字典，每行一个词"""
    if not os.path.exists(filepath):
        return []
    words = []
    with open(filepath, 'r', encoding='utf-8') as f:
        for line in f:
            word = line.strip()
            if word:
                words.append(word)
    return words

def calc_crc32(data):
    return zlib.crc32(data) & 0xFFFFFFFF

def generate_candidates(target_size, custom_dict=None):
    candidates = set()
    encodings = ['utf-8', 'gbk']

    # 基础字符集
    base_chars = GB2312_HANZI + 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890 `[];,./\~!@
    common_words = ['密', '钥', '密码', '解', '锁', 'flag', 'key', 'secret', '中', '文', '好', 'OK', '是', '的
```

```python
    if custom_dict:
        common_words.extend(custom_dict)

    # 1. 单字符
    for c in base_chars:
        for enc in encodings:
            try:
                b = c.encode(enc)
                if len(b) == target_size:
                    candidates.add((c, b, enc))
            except:
                continue

    # 2. 双字符（仅当 target_size <= 6 时尝试，避免爆炸）
    if target_size <= 6:
        for c1 in GB2312_HANZI[:500]:  # 限制前500高频字
            for c2 in '0123456789' + GB2312_HANZI[:200]:
                for s in [c1 + c2, c2 + c1]:
                    for enc in encodings:
                        try:
                            b = s.encode(enc)
                            if len(b) == target_size:
                                candidates.add((s, b, enc))
                        except:
                            continue

    # 3. 常见词
    for word in common_words:
```

```python
def generate_candidates(target_size, custom_dict=None):
    # 3. 常见词
    for word in common_words:
        for enc in encodings:
            try:
                b = word.encode(enc)
                if len(b) == target_size:
                    candidates.add((word, b, enc))
            except:
                continue

    return list(candidates)

def main():
    zip_path = 'D:/0x/week4/attachment2/attachment (1).zip'#input("请输入 ZIP 压缩包路径: ").strip()
    dict_path = input("请输入自定义字典路径（留空则不用）: ").strip()

    custom_dict = load_dict_from_file(dict_path) if dict_path else None

    try:
        with zipfile.ZipFile(zip_path, 'r') as zf:
            all_info = zf.infolist()
            small_files = [info for info in all_info if 0 < info.file_size <= 3]
            if not small_files:
                small_files = [info for info in all_info if 0 < info.file_size <= 9]
```

```python
            if not small_files:
                print(": 未找到大小在 1~9 字节之间的文件。")
                return

            results = {}
            failed_files = []

            for info in small_files:
                target_size = info.file_size
                target_crc = info.CRC
                found = False

                candidates = generate_candidates(target_size, custom_dict)
                for text, data, enc in candidates:
                    if calc_crc32(data) == target_crc:
                        results[info.filename] = text
                        found = True
                        break

                # 纯数字兜底
                if not found:
                    for length in range(1, min(4, target_size + 1)):
                        for num_tuple in product('0123456789', repeat=length):
                            s = ''.join(num_tuple)
                            try:
```

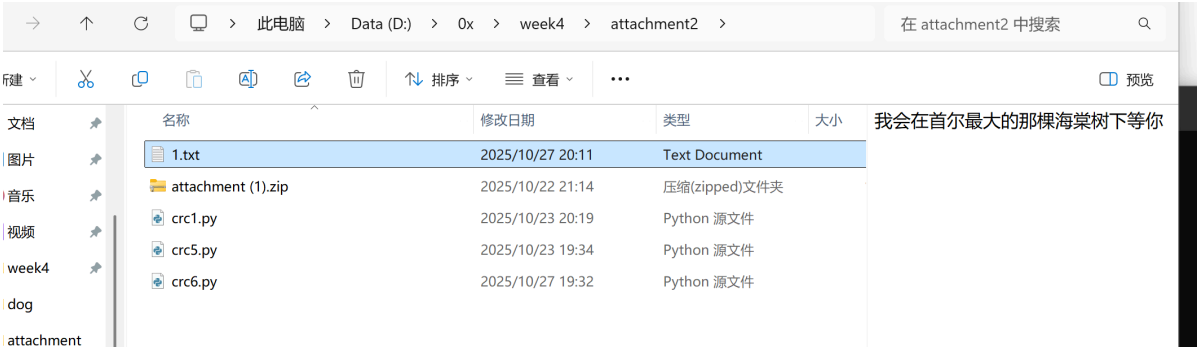
```
                    try:
                        b = s.encode('ascii')
                        if len(b) == target_size and calc_crc32(b) == target_crc:
                            results[info.filename] = s
                            found = True
                            break
                    except:
                        continue

        if not found:
            failed_files.append(info.filename)

    # ===== 输出结果 =====
    print("\n" + "="*60)
    print(":: ZIP 小文件 CRC32 爆破结果")
    print("="*60)

    if results:
        print("\n  成功:")
        for f in sorted(results):
            print(f"  {f} → '{results[f]}'")
    if failed_files:
        print("\n  失败:")
        for f in sorted(failed_files):
            info = next(i for i in zf.infolist() if i.filename == f)
            print(f"  {f} (size={info.file_size}, CRC=0x{info.CRC:08X})")
```

```
            if results:
                print("\n  成功:")
                for f in sorted(results):
                    print(f"  {f} → '{results[f]}'")
            if failed_files:
                print("\n  失败:")
                for f in sorted(failed_files):
                    info = next(i for i in zf.infolist() if i.filename == f)
                    print(f"  {f} (size={info.file_size}, CRC=0x{info.CRC:08X})")

            if len(results) == 1:
                print(f"\n  内容: {list(results.values())[0]}")
            elif len(results) > 1:
                concat = ''.join(results[f] for f in sorted(results))
                print(f"\n  结果拼接: {concat}")

            print("="*60)

    except Exception as e:
        print(f"  错误: {e}")

if __name__ == "__main__":
    main()
```

爆出来了喵：She talked a lot,但我只记得这一句话。我会在首尔最大的那棵海棠树下等你

```
attachment/027.txt → '言'
attachment/028.txt → 'だ'
attachment/029.txt → 'け'
attachment/030.txt → '覚'
attachment/031.txt → 'え'
attachment/032.txt → 'て'
attachment/033.txt → 'い'
attachment/034.txt → 'る'
attachment/035.txt → '。'
attachment/036.txt → '我'
attachment/037.txt → '会'
attachment/038.txt → '在'
attachment/039.txt → '首'
attachment/040.txt → '尔'
attachment/041.txt → '最'
attachment/042.txt → '大'
attachment/043.txt → '的'
attachment/044.txt → '那'
attachment/045.txt → '棵'
attachment/046.txt → '海'
attachment/047.txt → '棠'
attachment/048.txt → '树'
attachment/049.txt → '下'
attachment/050.txt → '等'
attachment/051.txt → '你'

结果拼接：She talked a lot,しかし、私はこの一言だけ覚えている。我会在首尔最大的那棵海棠树下等你
============================================================
```

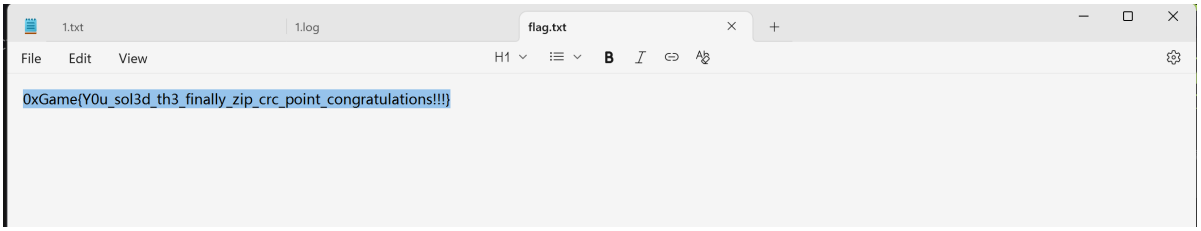
我们得记住她的话（bushi)建一个相同头的txt文件，明文攻击一下。




```
D:\bkcrack-1.8.0-win64>bkcrack -C "D:\0x\week4\attachment2\attachment (1).zip" -c "attachment/huiliyidehua.txt" -p "D:\0
x\week4\attachment2\1.txt"
bkcrack 1.8.0 - 2025-08-18
[20:34:51] Z reduction using 41 bytes of known plaintext
100.0 % (41 / 41)
[20:34:51] Attack on 188442 Z values at index 6
Keys: 9b483ffb 551530ef f195db46
3.6 % (6790 / 188442)
Found a solution. Stopping.
You may resume the attack with the option: --continue-attack 6790
[20:34:55] Keys
9b483ffb 551530ef f195db46
```

修改成简单密码

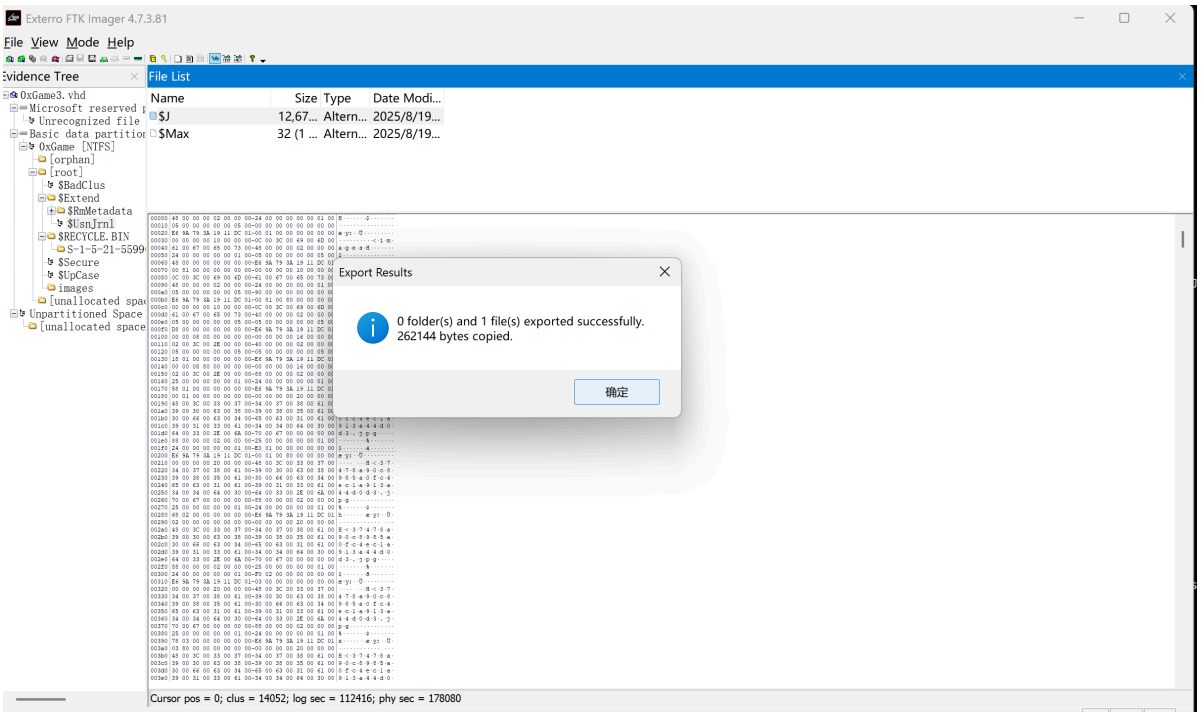
```
D:\bkcrack-1.8.0-win64>bkcrack -C "D:\0x\week4\attachment2\attachment (1).zip" -k 9b483ffb 551530ef f195db46
-U "D:\0x\week4\new.zip" abc
bkcrack 1.8.0 - 2025-08-18
[20:38:23] Writing unlocked archive D:\0x\week4\new.zip with password "abc"
100.0 % (53 / 53)
Wrote unlocked archive.
```



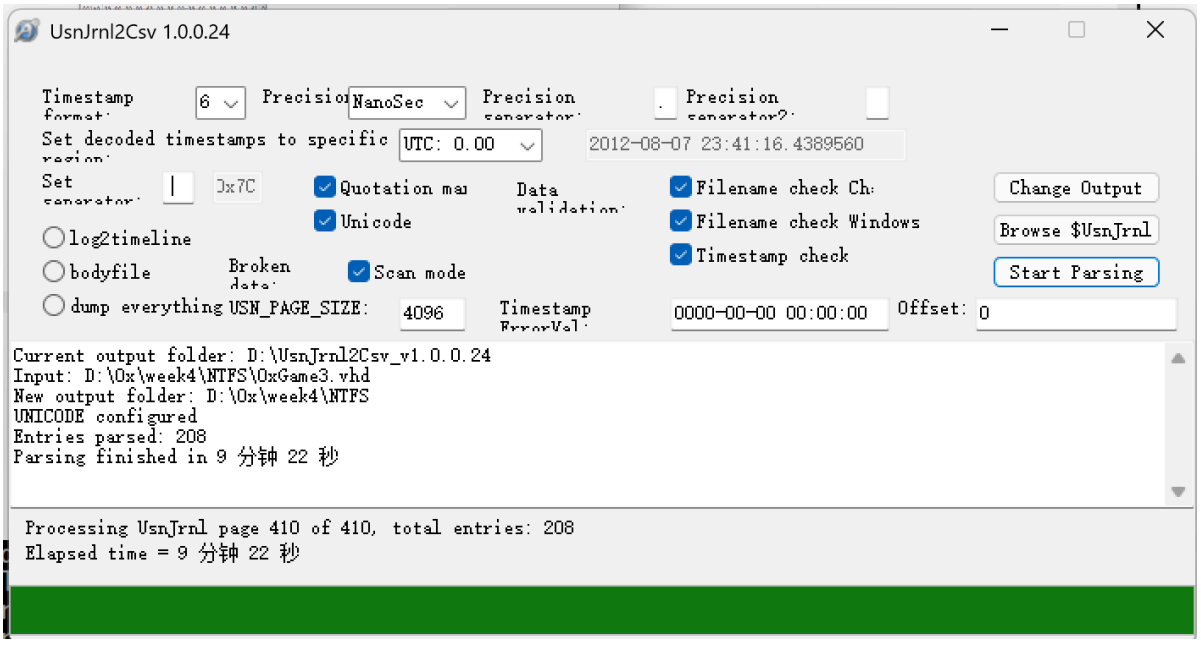
0xGame{Y0u_sol3d_th3_finally_zip_crc_point_congratulations!!!}

3.NTFS很ez啦

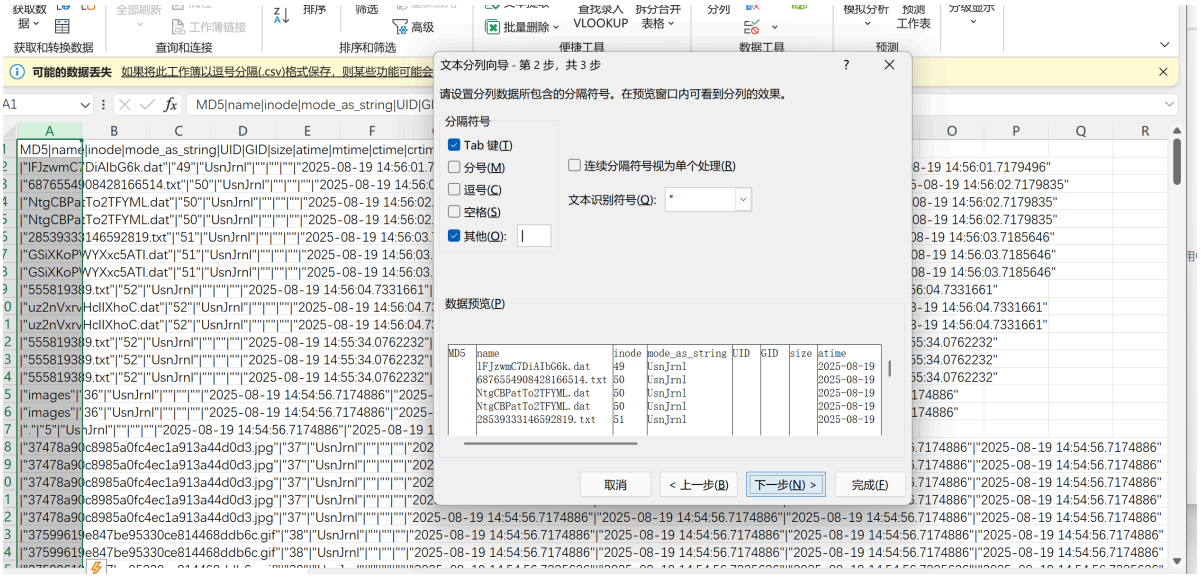
用FTK 打开，找到**$UsnJrnl** 里的**$J**，里面有数据变更的记录。



提取出来



找到csv文件，打开分列一下，获得比较直观的表格



找到一个被大量修改过名字的txt文件，提取一下数字，似乎是编码过的flag拆分

1364304685468197 9.txt
1364304685468197 9.txt
1364304685468197 9.txt
6426765720352224837.txt
6426765720352224837.txt
6426765720352224837.txt
6876554908428166514.txt
6876554908428166514.txt
6876554908428166514.txt
28539333146592819.txt
28539333146592819.txt
28539333146592819.txt
555819389.txt
555819389.txt
555819389.txt

一段一段转成十六进制再解码似乎有点问题...?

Input

307847616d657c5930755f484078005f6e6e417354640065645f4e5446342121217d

68 1 29 Raw Bytes LF

Output

0xGame|Y0u_H@x_nnAsTded_NTF4!!!}

脚本倒是没什么问题（好怪...?

```python
nums = [
    13643046854681979,
    6426765720352224837,
    6876554908428166514,
    2853933314659281 9,
    555819389
]

flag_bytes = b""
for n in nums:
    # 计算所需字节数（向上取整）
    byte_len = (n.bit_length() + 7) // 8
    # 转为大端序字节
    b = n.to_bytes(byte_len, 'big')
    flag_bytes += b

print("Raw bytes:", flag_bytes)
print("As ASCII (with escapes):", flag_bytes.decode('latin1'))

# 尝试提取 flag{...} 模式
import re
match = re.search(rb'flag\{.*?\}|CTF\{.*?\}|\{.*?\}', flag_bytes)
if match:
    print("FOUND FLAG:", match.group().decode())
else:
    # 打印所有可打印部分
    clean = ''.join(c for c in flag_bytes.decode('latin1') if 32 <= ord(c) <= 126)
    print("Cleaned:", clean)
```

```
Raw bytes: b'0xGame{Y0u_H@vE_nnAsTered_NTF3!!!}'
As ASCII (with escapes): 0xGame{Y0u_H@vE_nnAsTered_NTF3!!!}
FOUND FLAG: {Y0u_H@vE_nnAsTered_NTF3!!!}
```

```
Raw bytes: b'0xGame{_nnAsTered_NTF3!!!}'
As ASCII (with escapes): 0xGame{_nnAsTered_NTF3!!!}
FOUND FLAG: {_nnAsTered_NTF3!!!}
```

FLAG: 0xGame{Y0u_H@vE_nnAsTered_NTF3!!!}

4.问卷大调查

没啥好说的，开盒即食

(由于没有归档所以忘记flag是什么了，和一位唉唉

OK历史记录翻到了，没开无痕浏览是这样的（?

flag：0xGame{see_you_next_time}

Osint

1. 一直放坡一直爽

如视频，视频里出现了敌楼湾公交站台

OSINT3.mp4

根据视频里，一开始蹬腿用力，后面开始滑行，判定最高点。地图上附近只有一个有名字的地点。不过不是这个充电站，是这个驿站（属于是巧克力里藏史，而我是条狗orz

星星充电汽车充电站(香山公路驿站充电站)

刚刚浏览

星星充电汽车充电站 > 香山公路驿站 充电站 >

营业时间 周一至周日 00:00-24:00 详情 >

驾车173.6公里 2小时8分 香山公路驿站 浙江省湖州市长兴县夹浦镇香山公路驿站(旅游驿站)

电话

百度上搜环太湖骑行线路图也能发现这个地方。


08:54
北疆旅游
北疆旅游
文件夹
颜色
创建人
更多
十八湾湿地公园
无锡
常州太湖天远桥湿地公园
雪浪山
贡湖湾湿地公园
太湖...
行程路线
拈花湾·禅意小镇停车场
虎丘区
西京湾花田停车场
苏州
太湖
太湖渔洋山
苏州宝岛
山岛花园酒店...
香山公路驿站(旅游...
西山风景区
夕阳观
林屋洞
碧玉榭
陆巷古村
东山景区-紫金庵
长圻码头
太湖观景台
博物馆
湖畔杉隐
渔人码头3号停车场(...
太湖婆港文化展示馆
湖州
吴兴区
南浔区
高德地图
20公里
列表
显示
全览
标记好地
制作路线
结伴出行
攻略分享
更多
标记景点
标记美食
标记酒店
机场火车站
水印拍照
变清晰
去水印
涂抹消除
智能抠图

Flag:0xGame{香山公路驿站}