BDSec CTF 2023 —— Misc & Forensics

~~这破比赛平台还 ban 了 Vultr 的 ASN，有点离谱~~

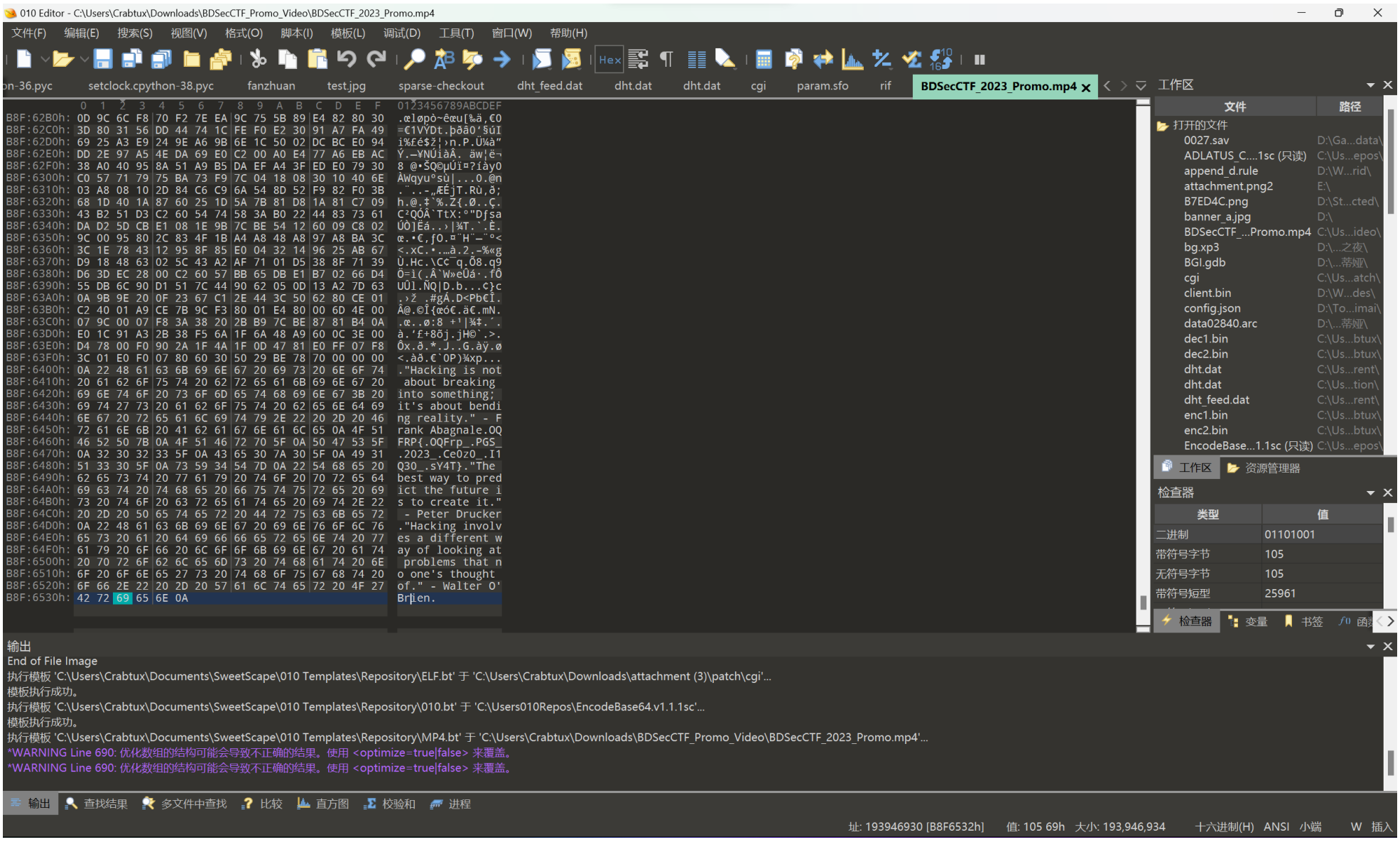
Misc

Think like a hacker

下载题给文件，解压之后得到 readme.txt 和一个 MP4 文件。readme.txt 里面写着：

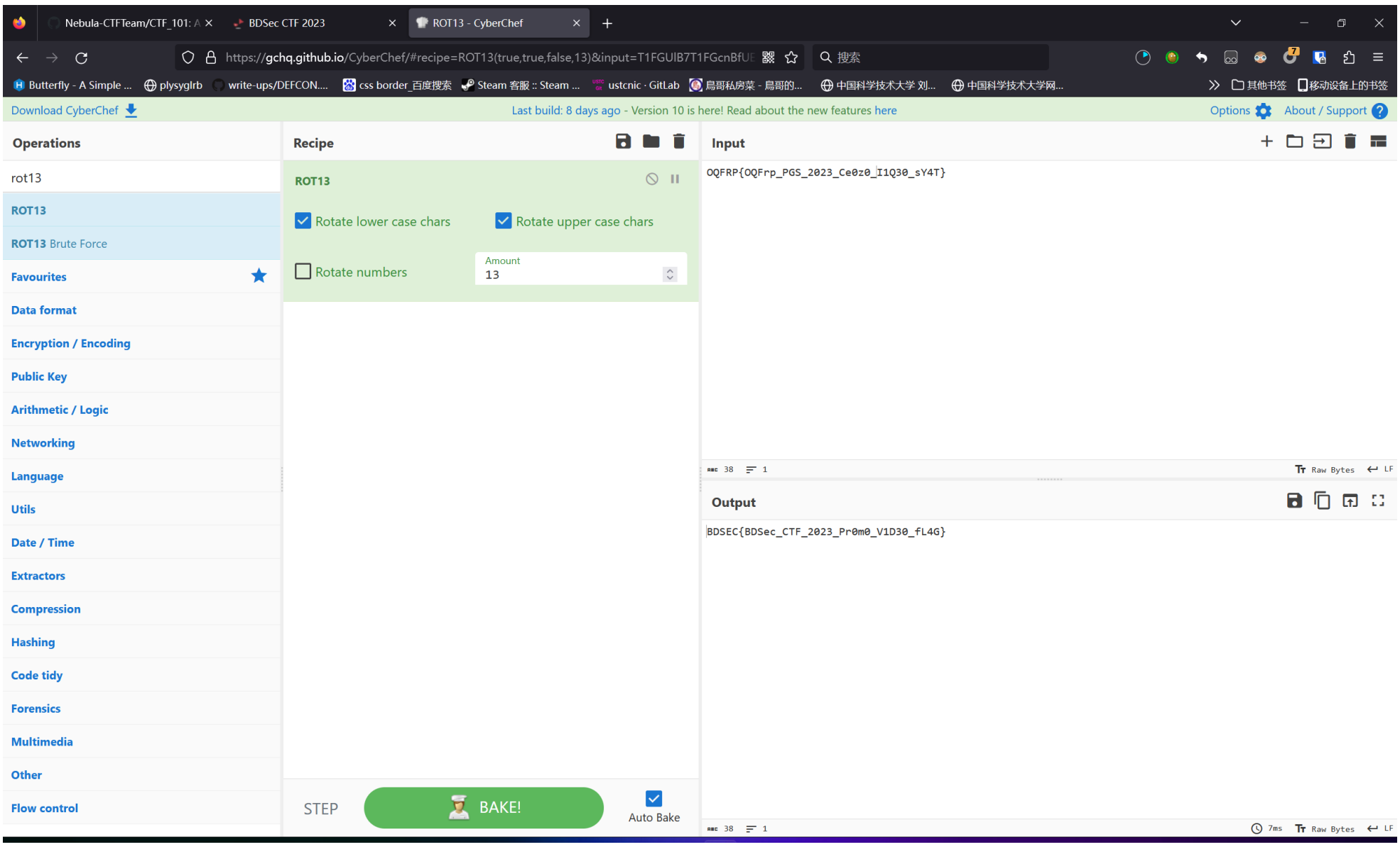
```
 "Hacking involves a different way of looking at problems that no one's thought of." - Walter O'Brien
So, do you think like a hacker ? :P
```

他让我们用 Hacker 的方式打开文件。使用 ~~记事本~~ 你最喜爱的十六进制编辑器（比如 010 Editor）打开 MP4 文件并查看文件末尾，不出意料地发现了一段 plain text：




```
"Hacking is not about breaking into something; it's about bending reality." - Frank Abagnale
OQFRP{
OQFrp_
PGS_
2023_
Ce0z0_
I1Q30_
sY4T}
"The best way to predict the future is to create it." - Peter Drucker
"Hacking involves a different way of looking at problems that no one's thought of." - Walter O'Brie
```

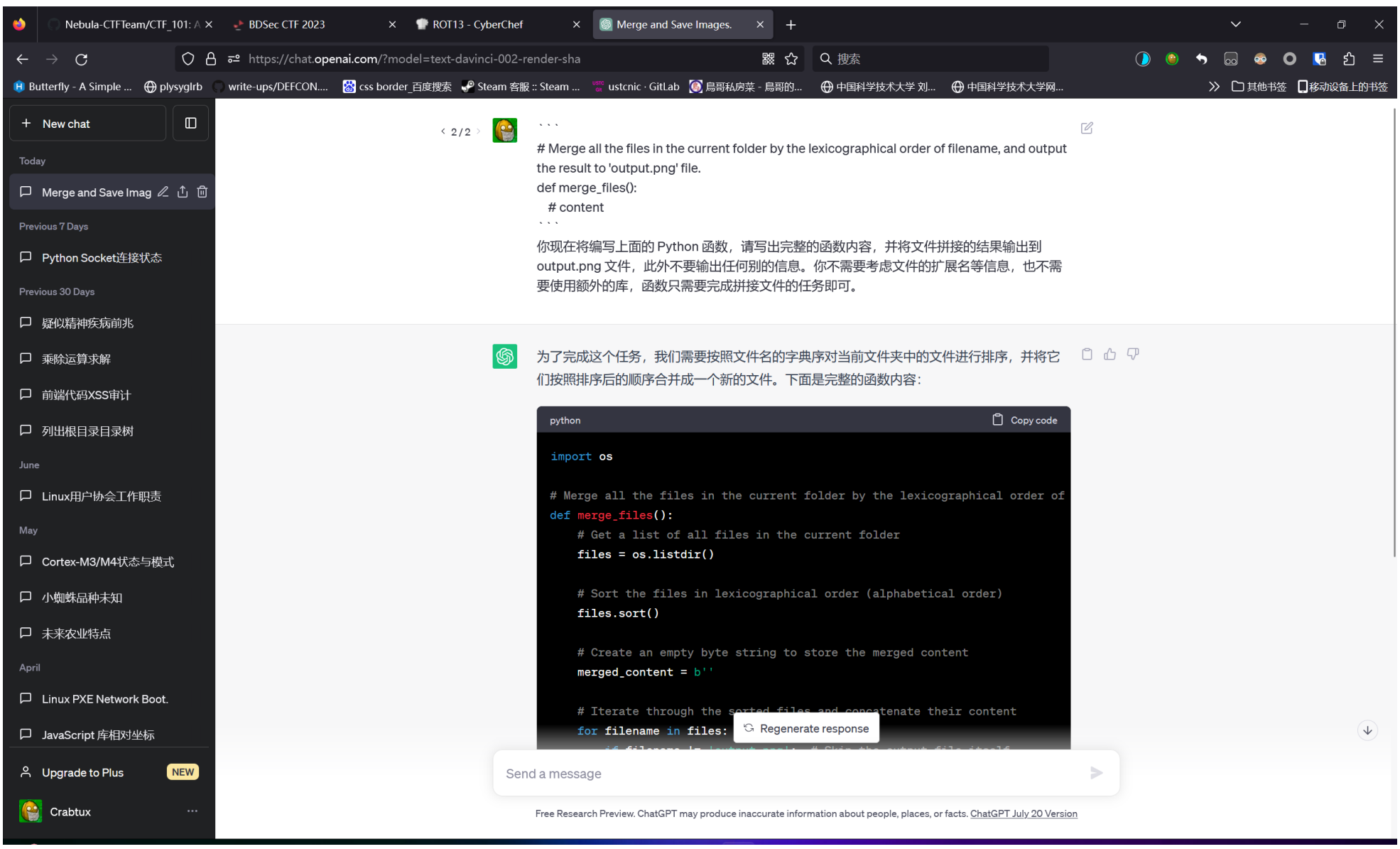
其中有一个长得很像 flag 的东西，但不符合 BDSEC{...} 的格式，根据经验猜测被 ROT13 过，使用 Cyberchef 再次 ROT13 得到 flag。



What is this?

题给文件解压，得到一堆名为 `flag_xx` 的文件。按照字典序，我们用十六进制编辑器打开 `flag_aa` 文件，发现是 PNG 文件头，根据经验猜测是要将所有文件按照文件名的字典序拼接起来，得到一张图片，图片的内容就是 flag。

下面我们演示使用 ChatGPT 书写 Python 代码来完成这一工作（x



```python
import os

# Merge all the files in the current folder by the lexicographical order of filename, and output the result to 'output.png'
file.
def merge_files():
    # Get a list of all files in the current folder
    files = os.listdir()

    # Sort the files in lexicographical order (alphabetical order)
    files.sort()

    # Create an empty byte string to store the merged content
    merged_content = b''

    # Iterate through the sorted files and concatenate their content
    for filename in files:
        if filename != 'output.png':  # Skip the output file itself
            with open(filename, 'rb') as file:
                merged_content += file.read()

    # Write the merged content to the output.png file
    with open('output.png', 'wb') as output_file:
        output_file.write(merged_content)

# Call the function to merge the files
merge_files()
```

这段代码基本正确，不过它没有考虑到 Python 脚本自身也存在于文件夹中，稍作修改即可：

```
--          if filename != 'output.png':  # Skip the output file itself
++          if filename not in ['output.png', 'exp.py']:  # Skip the output file and the exp file
```

运行这段代码，在当前文件夹下得到 output.png，打开即可得到 flag。

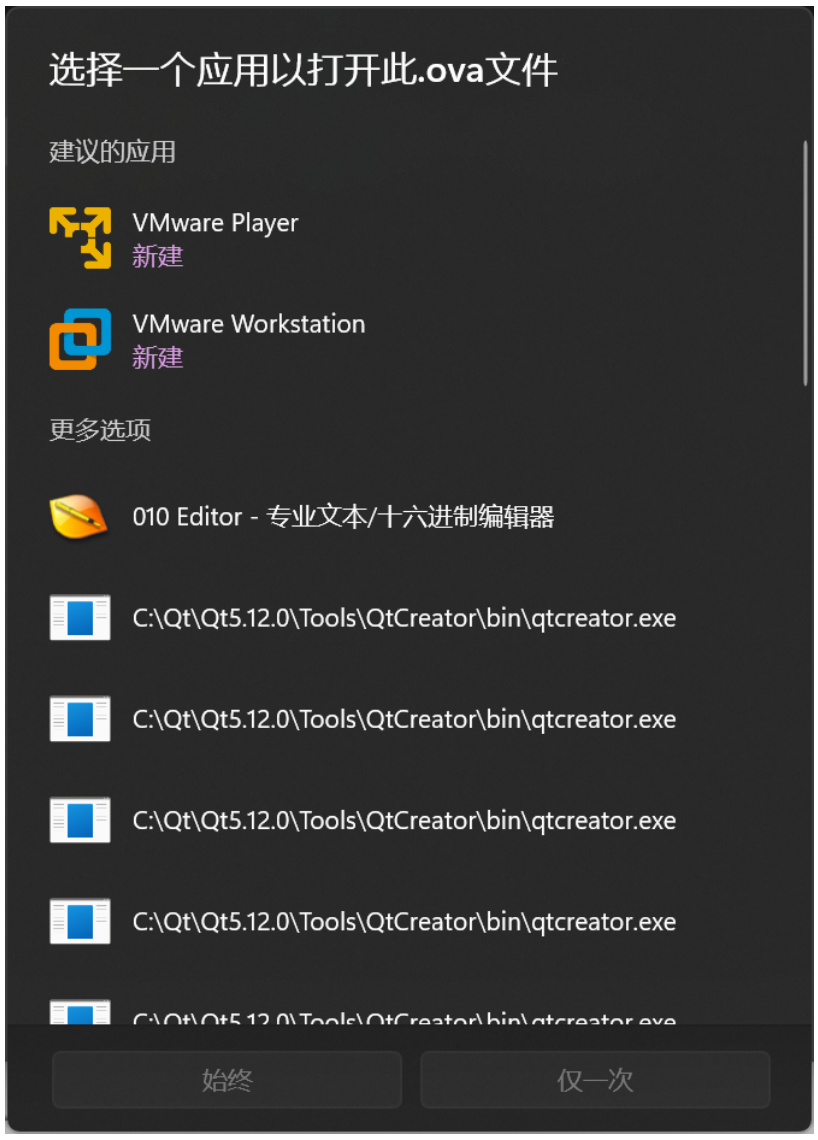
Forensics

这题给了个 Windows 7 的 ova 文件做取证， 5 题共用一个 ova 文件。

大家可能会很奇怪 ova 文件是什么呢？下面就让小编带大家一起了解吧。

~~ova 文件就是小编也不知道 ova 文件是什么，小编也感到非常惊讶（被拖走~~

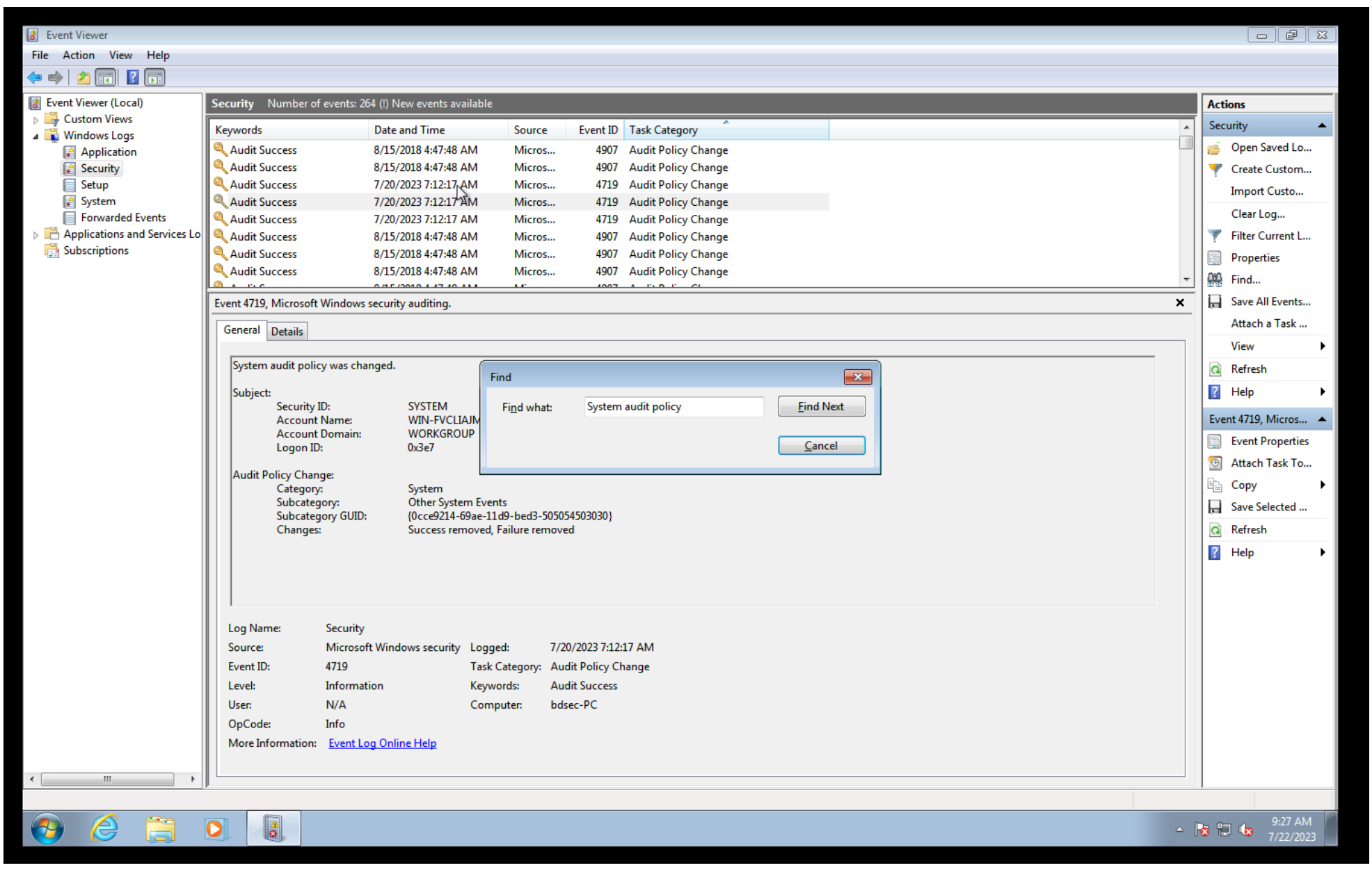
ova 文件是 VMware Workstation 导出的文件，你可以将其看作一个虚拟机模板，用 VMware 导入它并创建一台虚拟机。这属于环境配置的过程，在此省略。



System Check

```
When Last system audit policy was changed?
```

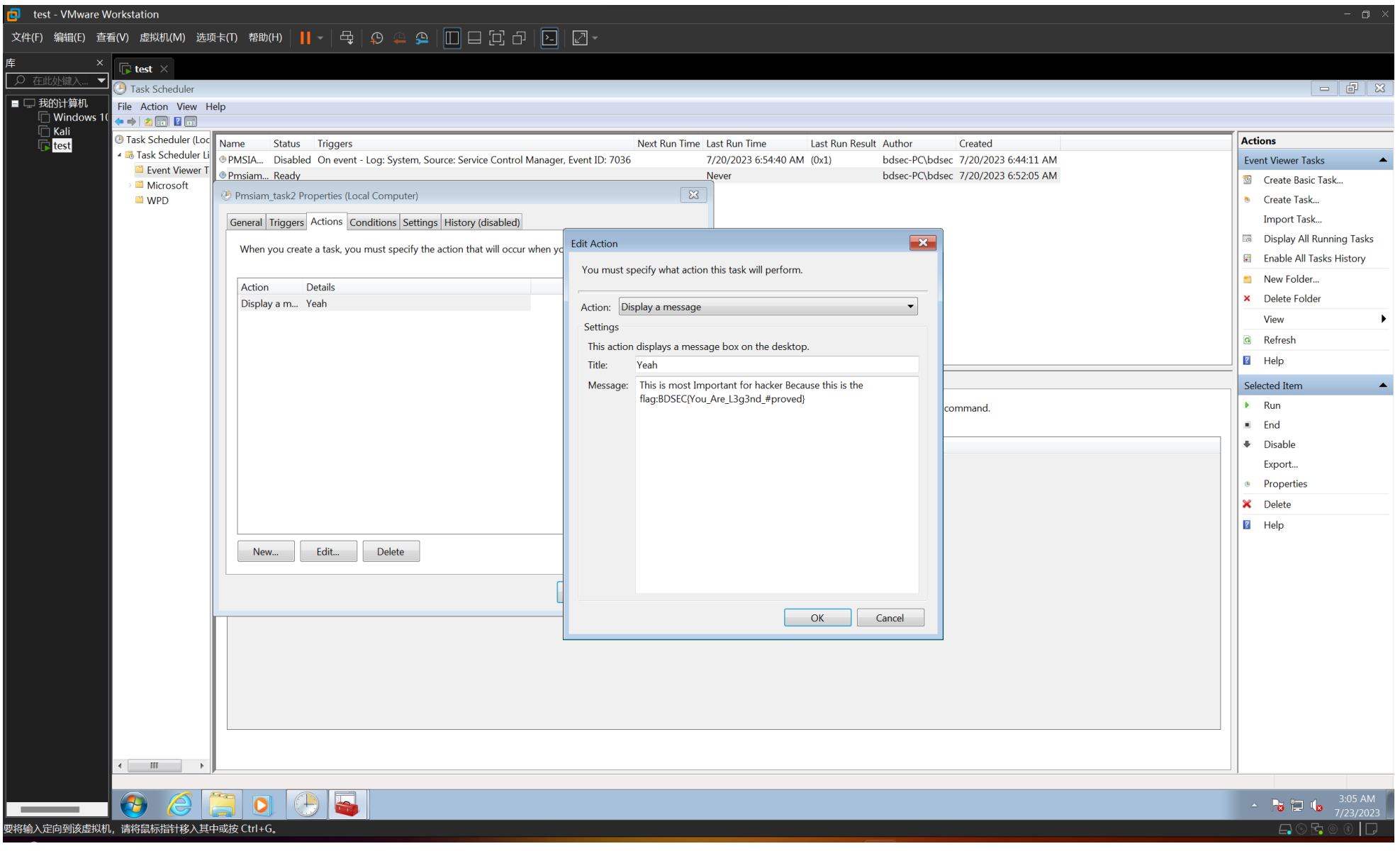
搜索发现可以在事件查看器（Event Viewer）里面查询，在 Security 分类中。



flag 是 BDSEC{07/20/2023_07:12:17_AM}。

Maintain shedule

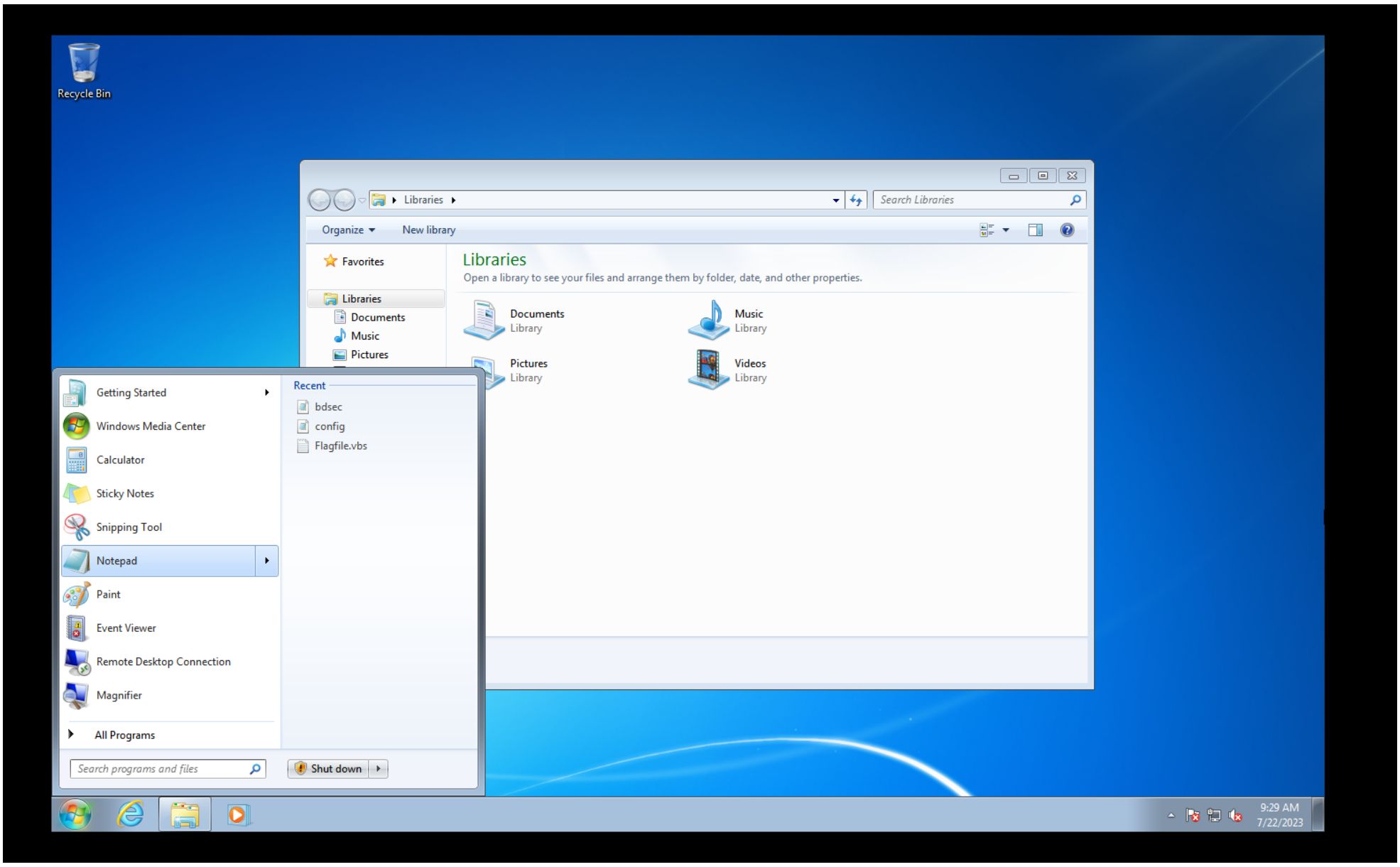
看到 schedule，第一反应是 Windows 的计划任务功能：



BDSEC{You_Are_L3g3nd_#proved}

Hacker destination file

在记事本的 Recent 里面看到奇怪的东西：



bdsec 里面的 flag 即为答案：

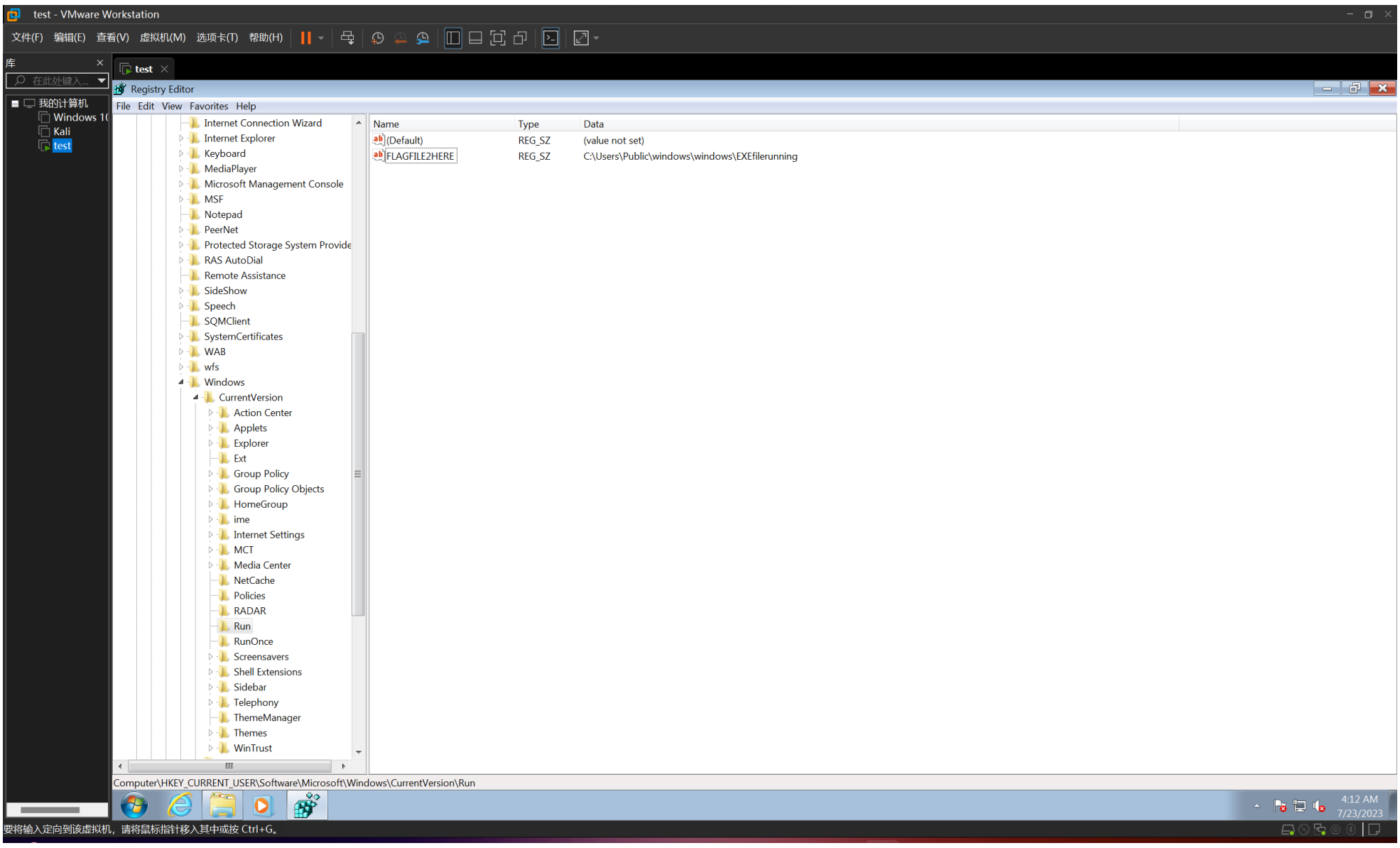
BDSEC{Y3s#_y0U#_g0T#_F14G}

意义不明（

Hackers username and email

事件查看器里面没活了，我们来看注册表。在此之前，记得把 Windows“显示隐藏文件/文件夹”的功能打开。

Win+R 输入 regedit，可以进入注册表编辑器：



跟进一下看到：

```
"user": "comando1337/blbna@mail2tor.com"
```

这就是答案了。

Find Values

ova 文件的 sha1 好获取。很容易猜到 vmdk 文件实际上包含在 ova 文件内部，网上搜一搜就能找到提取用的软件（比如 AccessData FTK Imager）。

总结

Windows 溯源中，注册表和事件查看器算是两个必须检查的东西。题目本身确实偏向新手，但感觉出得有点怪（