流量分析之usb键盘分析

例题：https://buuoj.cn/challenges#USB

题目分析

刚打开就是一个rar和一个ftm

打开ftm可以看到一个key.pcap，用wireshark打开pcap可以看到这是一个usb流量包。

再看他的capture data，是十六位的，可以确定这大概是一个键盘的流量（鼠标是8位）

先利用tshark将流量中的capture data输出为txt

```
.\tshark.exe -r C:\Users\12558\Downloads\key.pcap -T fields -e usb.capdata
>"C:\Users\12558\Downloads\usbdata.txt"
```

使用脚本来处理一下

```
# 使用脚本删除空行
with open('usbdata.txt', 'r', encoding='utf-16') as f:
    lines = f.readlines()
lines = filter(lambda x: x.strip(), lines)
with open('usbdata.txt', 'w', encoding='utf-16') as f:
    f.writelines(lines)

# 将上面的文件用脚本分隔，加上冒号；
with open('usbdata.txt', 'r', encoding='utf-16') as f:
    with open('out.txt', 'w', encoding='utf-16') as fi:
        while True:
            a = f.readline().strip()
            if a:
                if len(a) == 16:  # 键盘流量的话len为16鼠标为8
                    out = ''
                    for i in range(0, len(a), 2):
                        if i + 2 != len(a):
                            out += a[i] + a[i + 1] + ":"
                        else:
                            out += a[i] + a[i + 1]
                    fi.write(out)
                    fi.write('\n')
            else:
                break

# 最后用脚本提取
# print((line[6:8])) # 输出6到8之间的值
# 取出6到8之间的值
mappings = {
    0x04: "A", 0x05: "B", 0x06: "C", 0x07: "D", 0x08: "E", 0x09: "F", 0x0A: "G",
0x0B: "H", 0x0C: "I", 0x0D: "J", 0x0E: "K", 0x0F: "L",
    0x10: "M", 0x11: "N", 0x12: "O", 0x13: "P", 0x14: "Q", 0x15: "R", 0x16: "S",
0x17: "T", 0x18: "U", 0x19: "V", 0x1A: "W", 0x1B: "X",
    0x1C: "Y", 0x1D: "Z", 0x1E: "1", 0x1F: "2", 0x20: "3", 0x21: "4", 0x22: "5",
0x23: "6", 0x24: "7", 0x25: "8", 0x26: "9", 0x27: "0",
    0x28: "\n", 0x2A: "[DEL]", 0x2B: "    ", 0x2C: " ", 0x2D: "-", 0x2E: "=",
0x2F: "[", 0x30: "]", 0x31: "\\", 0x32: "~", 0x33: ";",
    0x34: "'", 0x36: ",", 0x37: "."
}

nums = []
with open('out.txt', 'r', encoding='utf-16') as keys:
    for line in keys:
        if line[0] != '0' or line[1] != '0' or line[3] != '0' or line[4] != '0'
or line[9] != '0' or line[10] != '0' or \
           line[12] != '0' or line[13] != '0' or line[15] != '0' or line[16] !=
'0' or line[18] != '0' or line[19] != '0' or \
           line[21] != '0' or line[22] != '0':
            continue
        nums.append(int(line[6:8], 16))

output = ""
for n in nums:
    if n == 0:
        continue
    if n in mappings:
        output += mappings[n]
    else:
        output += '[unknown]'

print('output :\n' + output)
```

结果如图：屏幕截图 2025-05-14 130347

发现他键盘输入的是KEYXINAN

返回来处理一下rar文件，直接打开只看到了一个16b的txt，压缩包有1.54MB，事情不简单，打开010看看屏幕截图 2025-05-14 130823

原来是文件头的标识处损坏了，把7A改成74就好了屏幕截图 2025-05-14 131246

用stegsolve打开屏幕截图 2025-05-14 131410

发现在blue的0通道有一个二维码，扫描结果如下：

结合上文，我们在usb的流量分析中得到的key：xinan。

我们先猜是维吉尼亚加密屏幕截图 2025-05-14 132427

emmmmm，好像有了？只能说该有的格式都有了，那再试试栅栏吧

屏幕截图 2025-05-14 132831

最后得到了flag

```
flag{vig3ne2e_is_c00l}
```

屏幕截图 2025-05-14 132935