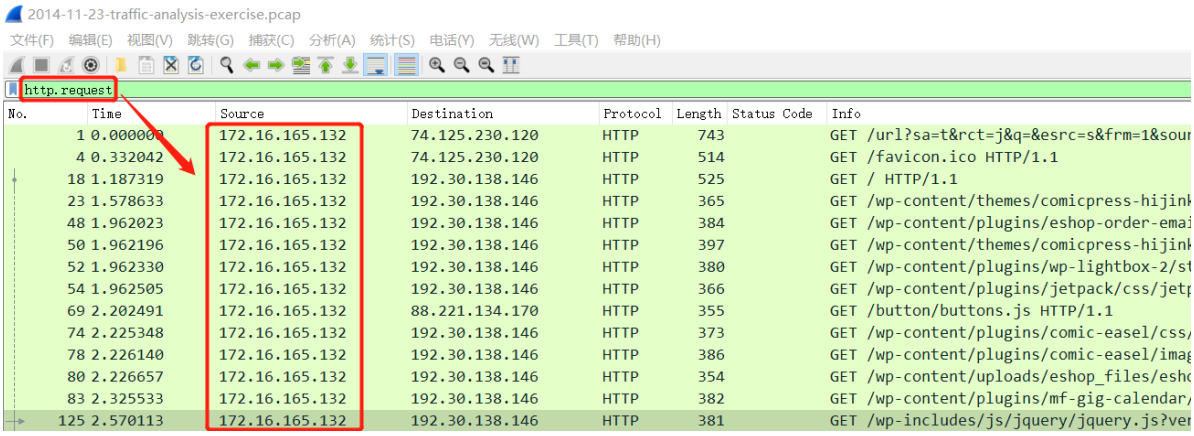
一、基本问题

1、被感染的Windows虚拟机的IP

```
# 答案
    172.16.165.132
```

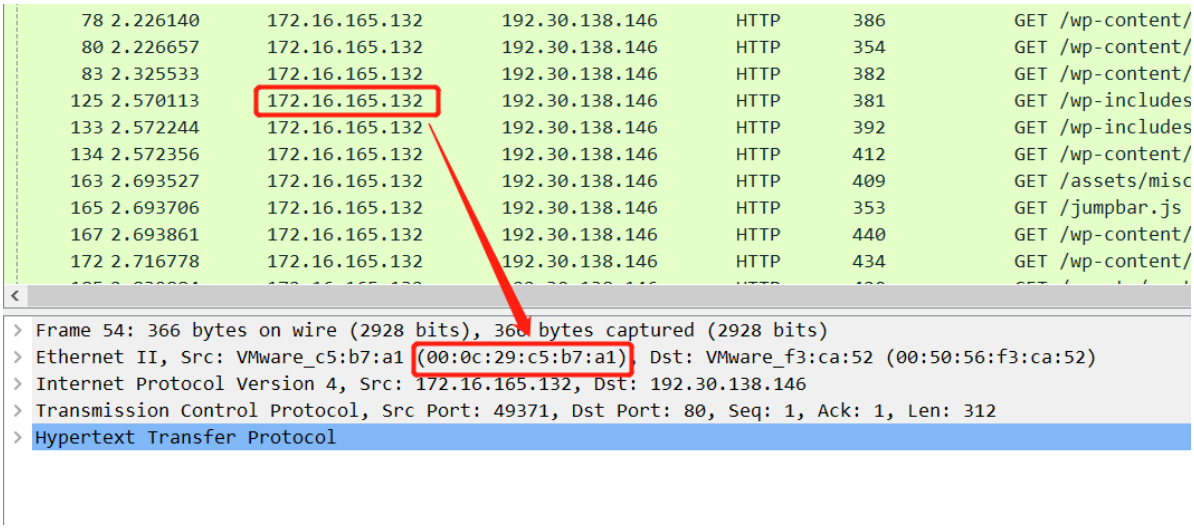
```
# 分析思路
    通过过滤"http.request"，找到所有发起http请求的主机，发现只有172这台主机
```



2、受感染虚拟机的MAC地址

```
# 答案
    00:50:56:f3:ca:52
```

```
# 分析思路
    查看关于IP172.16.165.132数据包中数据链路层的MMAC地址
```

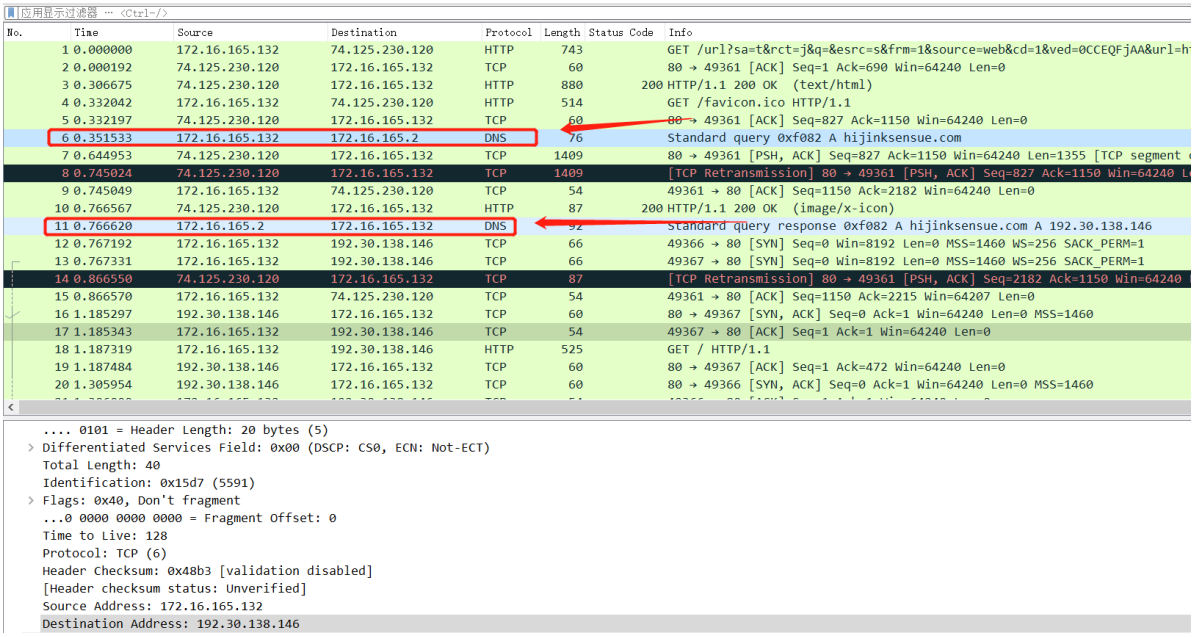


3、受感染网站的IP地址

```
# 答案
    192.30.138.146
```

分析过程

前面的分析均为跳包模式，现在从头开始追包，可以看到序号1-5包一直与IP 74.125.230.120进行交互，在序号6包、序号11包时出现了一条192.30.138.146的DNS解析记录，之后频繁与该IP进行交互，初步确认为受感染的IP



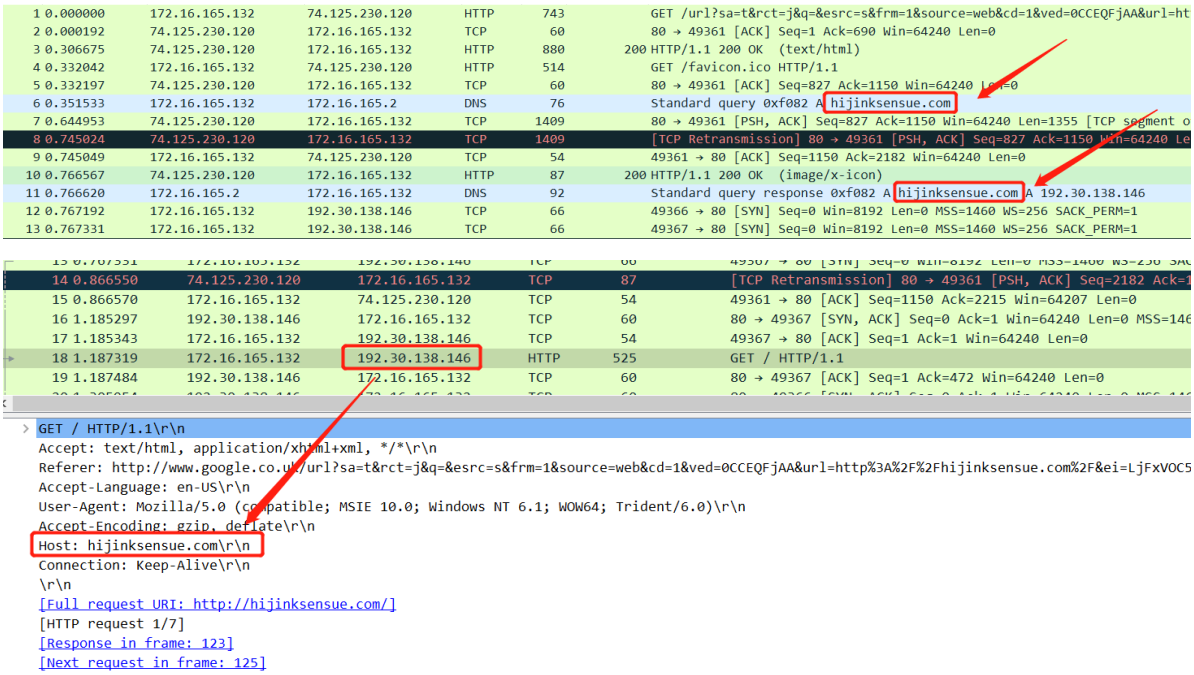
4、被入侵网站的域名

答案

hijinksensue.com

分析过程

查看关于上面IP的DNS记录或HTTP数据包中的Host值，可以看到域名为hijinksensue.com



5、提供恶意软件的IP地址和域名

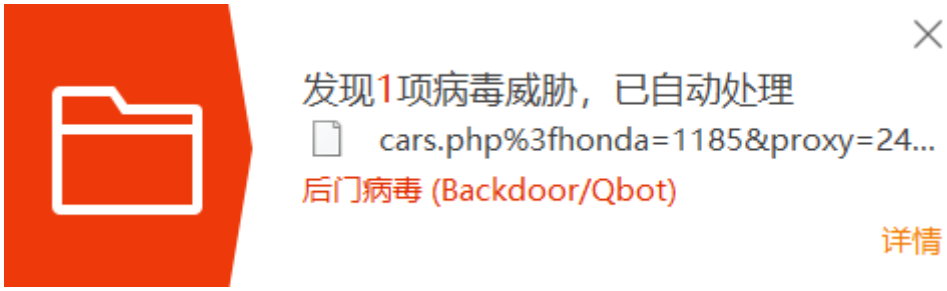
答案

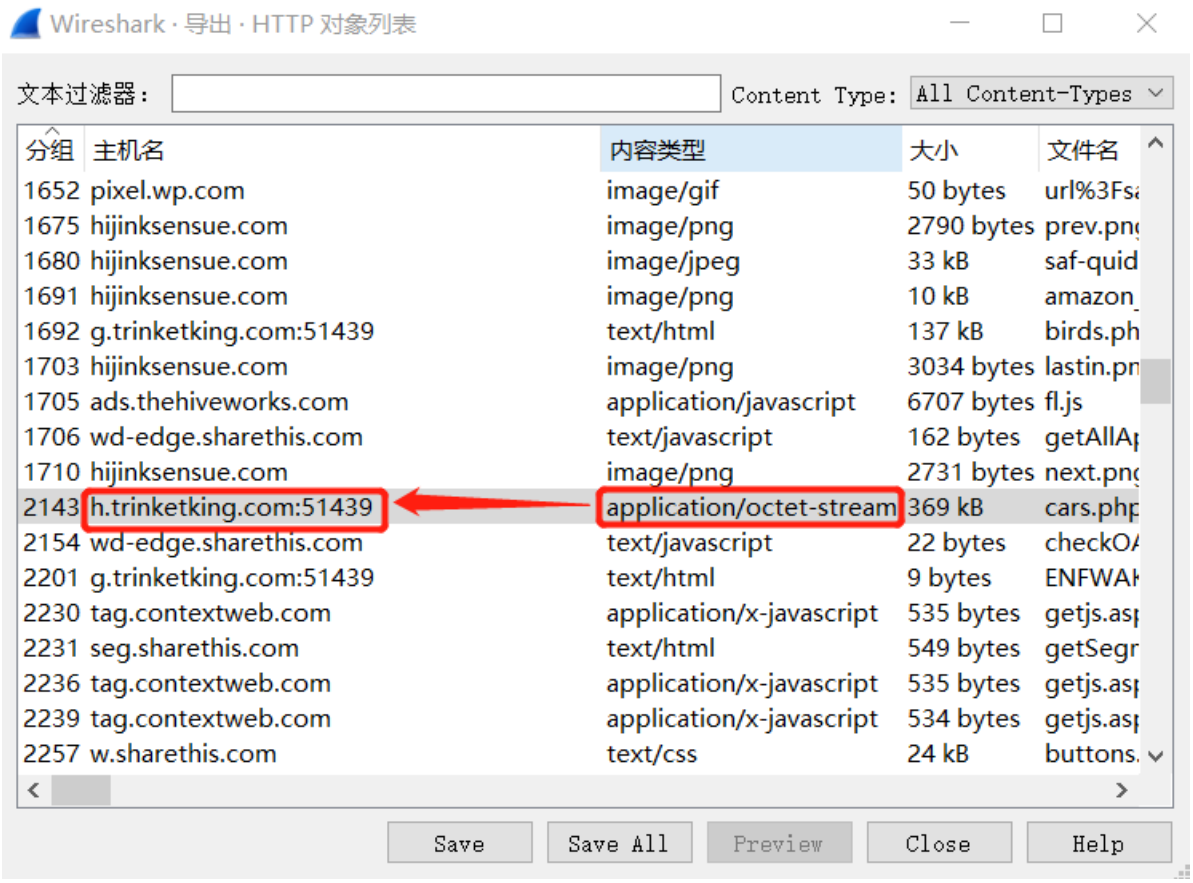
37.143.15.180

g.trinketking.com:51439

分析过程1

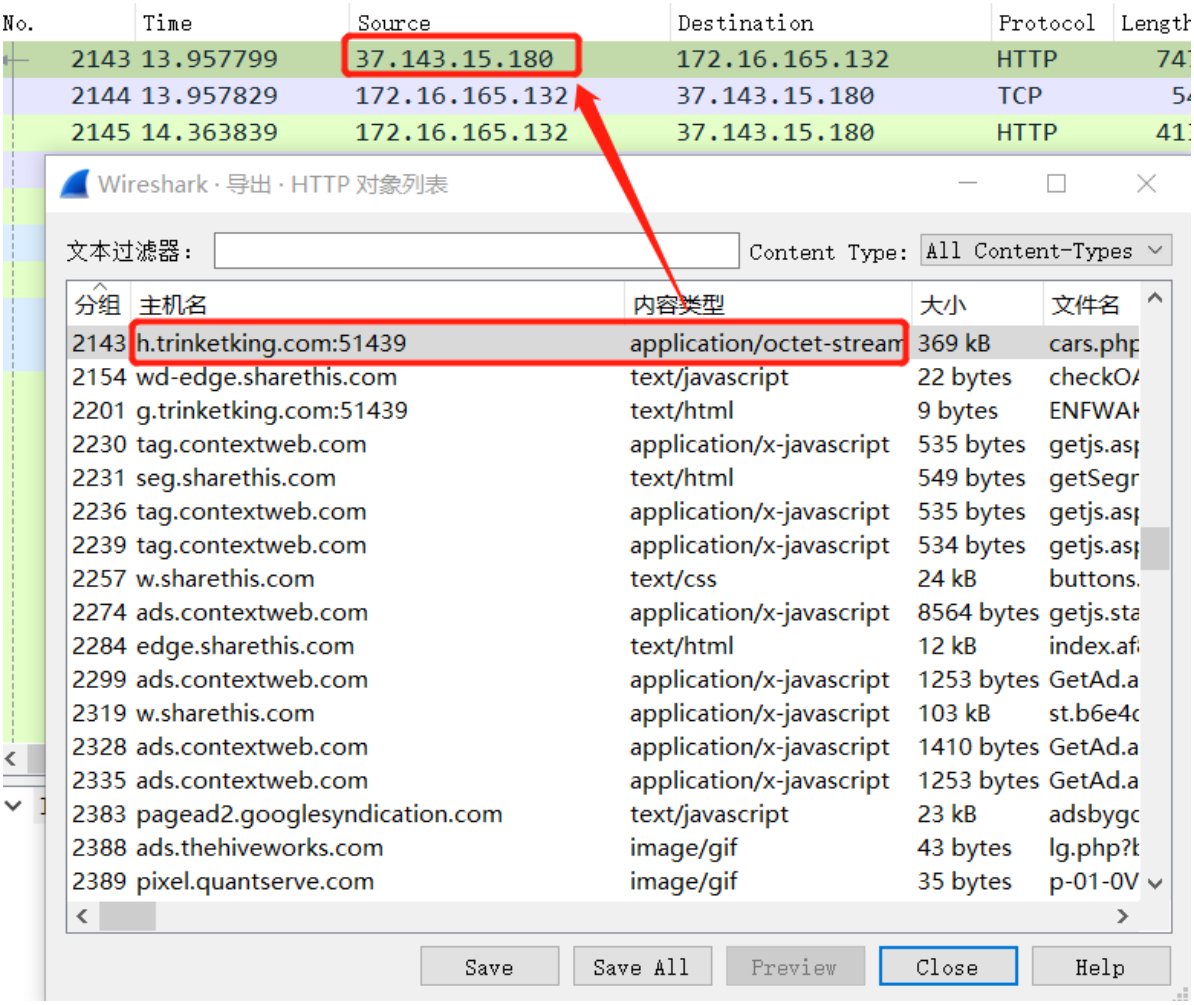
导出值 -> http，可以看到一个文件类型为"application/octet-stream"的文件，导出时直接被安全软件查杀了，其他文件均为正常的图片/文档。可以看到该恶意软件提供的主机名为"h.trinketking.com:51439"





分析过程2

定位该数据包，可以看到该恶意软件提供的IP



二、高级问题

1、传递恶意软件的EK

```
# 答案
    1.exe
```

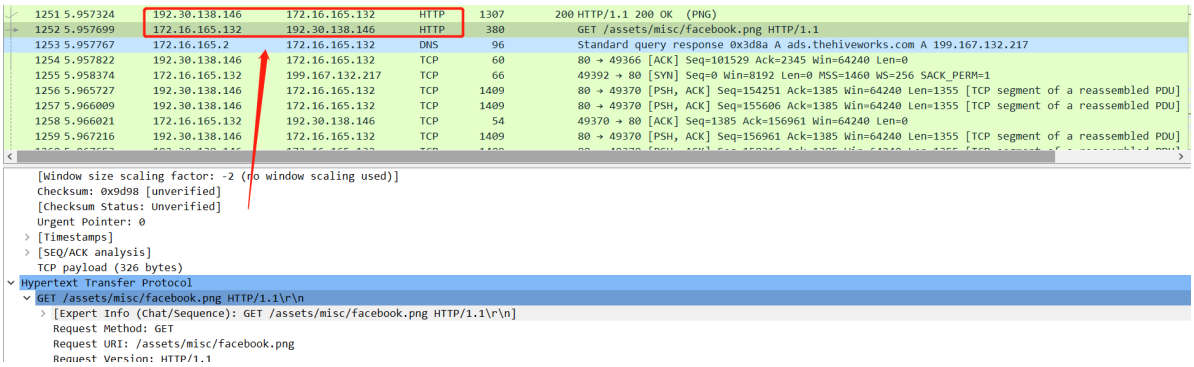
```
# 分析过程
    下载刚刚上面那个文件，传入病毒检测网站，发现为木马文件
```

2、指向EK登陆页面的重定向URL

```
# 答案
    hijinksensue.com/assets/misc/facebook.png
```

分析过程

通过查看恶意软件IP出现的第一个HTTP数据包（没有发现Referer头），在其之上虚拟机做了一次DNS解析与该IP进行连接，在该DNS解析前向192.30.138.146发出了请求，初步判断是从该位置跳转过来的



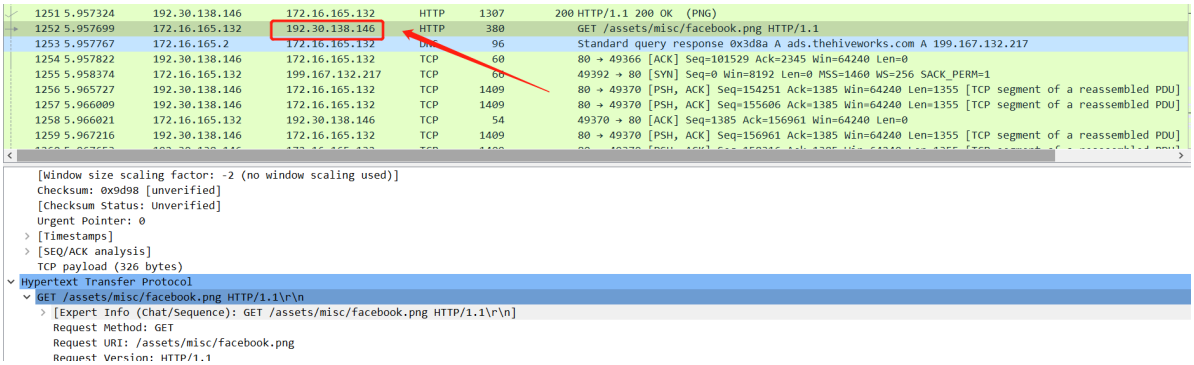
3、指向EK登录页面的重定向URL的IP

答案

192.30.138.146

分析过程

取上一个答案的IP



4、pcap提交Virus Total并触发的snort警报

Snort Alerts

- Senstive Data
  - (spp_sdf) SDF Combination Alert [1]
- Potentially Bad Traffic
  - (http_inspect) LONG HEADER [19]
  - PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority [254]
- Attempted Administrator Privilege Gain
  - SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt [2381]
  - SERVER-APACHE Apache Struts wildcard matching OGNL remote code execution attempt [29639]
- Attempted User Privilege Gain
  - BROWSER-PLUGINS AcroPDF.PDF ActiveX clsid access attempt [13913]
  - BROWSER-IE Microsoft Internet Explorer XHTML element memory corruption attempt [13974]
  - BROWSER-IE Microsoft Internet Explorer HTML DOM invalid DHTML textnode creation attempt [16301]
  - PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt [19187]
  - INDICATOR-OBFUSCATION Multiple character encodings detected [29509]
  - POLICY-OTHER PDF ActiveX CLSID access detected [38038]
  - FILE-IMAGE Apple PICT Quickdraw image converter packType 4 buffer overflow attempt [44455]
  - SERVER-OTHER Beetel Connection Manager username buffer overflow attempt [44679]
- Potential Corporate Privacy Violation
- A Network Trojan was detected
- Detection of a Denial of Service Attack

5、提取恶意软件的Payload，MD5或SHA256哈希是什么

```
# 答案
    MD5:1408275c2e2c8fe5e83227ba371ac6b3
    SHA256:cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d
```

```
# 分析过程
    提交该恶意软件到病毒分析平台，可直接查看到分析出的MD5值和SHA256值等
```