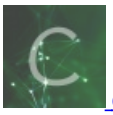
DDCTF 2019 writeup Wireshark

原创

barzar 于 2019-04-20 01:35:25 发布

分类专栏： ctf 文章标签： wireshark ddctf ctf 数据包



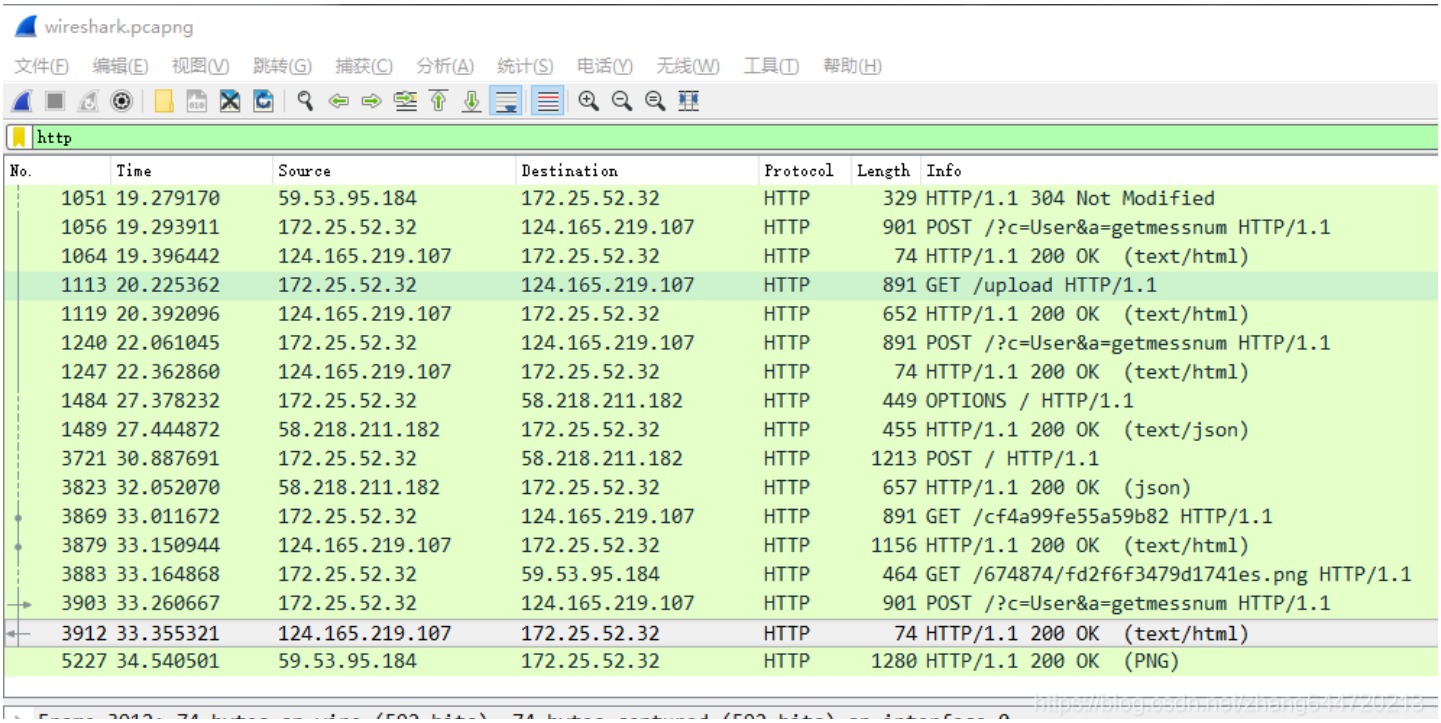
DDCTF 2019 Wireshark

写在最前

总的来说这是一道挺常规的Wireshark分析题，一般的wireshark题的信息总是隐藏在http的url，html或者图片里面，所以一般拿到Wireshark的题直接奔http就行啦 ~~要是不在http我就不承认我说过这句话~~
Wireshark数据包下载地址

分析数据包

拿到数据包先搜索http

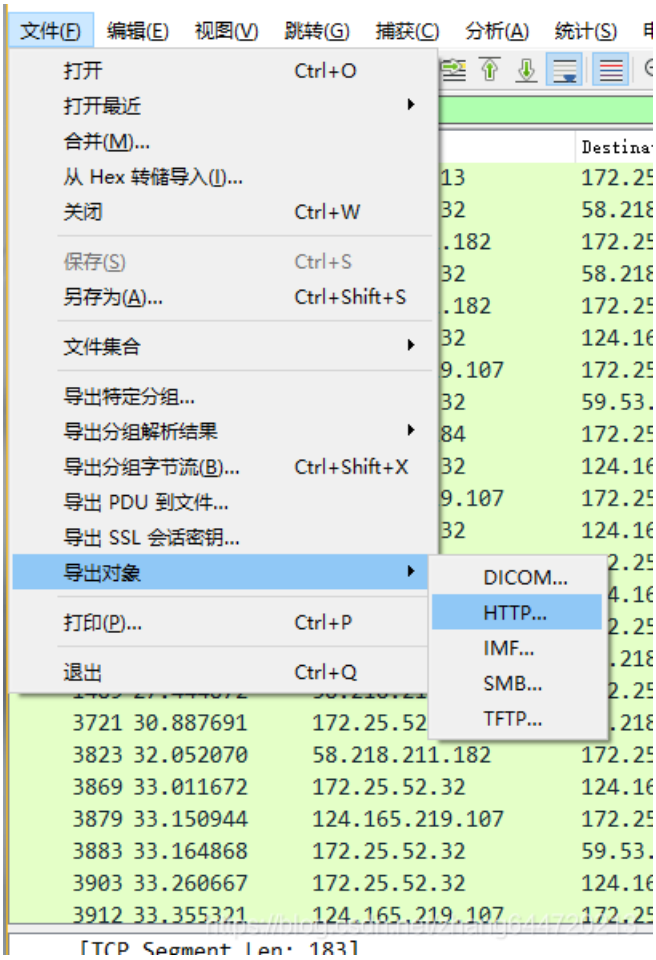


```
> Frame 3912: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
```

通过分析发现http的数据包不是很多，并且还附带了几张png
看到这我的内心毫无波动甚至有点想笑

```
tocol  Length  Info
TP       455 HTTP/1.1 200 OK  (text/json)
TP      1226 POST / HTTP/1.1  (PNG)
TP       656 HTTP/1.1 200 OK  (json)
TP       891 GET /ddc891b23147ba21 HTTP/1.1
TP      1151 HTTP/1.1 200 OK  (text/html)
TP       545 GET /674874/7782abccd820677fs.png HTTP/1.1
TP       329 HTTP/1.1 304 Not Modified
TP       901 POST /?c=User&a=getmessnum HTTP/1.1
TP        74 HTTP/1.1 200 OK  (text/html)
TP       891 GET /upload HTTP/1.1
TP       652 HTTP/1.1 200 OK  (text/html)
TP       891 POST /?c=User&a=getmessnum HTTP/1.1
TP        74 HTTP/1.1 200 OK  (text/html)
TP       449 OPTIONS / HTTP/1.1
TP       455 HTTP/1.1 200 OK  (text/json)
TP      1213 POST / HTTP/1.1
TP       657 HTTP/1.1 200 OK  (json)
TP       891 GET /cf4a99fe55a59b82 HTTP/1.1
TP      1156 HTTP/1.1 200 OK  (text/html)
TP       464 GET /674874/fd2f6f3479d1741es.png HTTP/1.1
TP       901 POST /?c=User&a=getmessnum HTTP/1.1
TP        74 HTTP/1.1 200 OK  (text/html)
TP      1280 HTTP/1.1 200 OK  (PNG)
28 bits) on interface 0
```

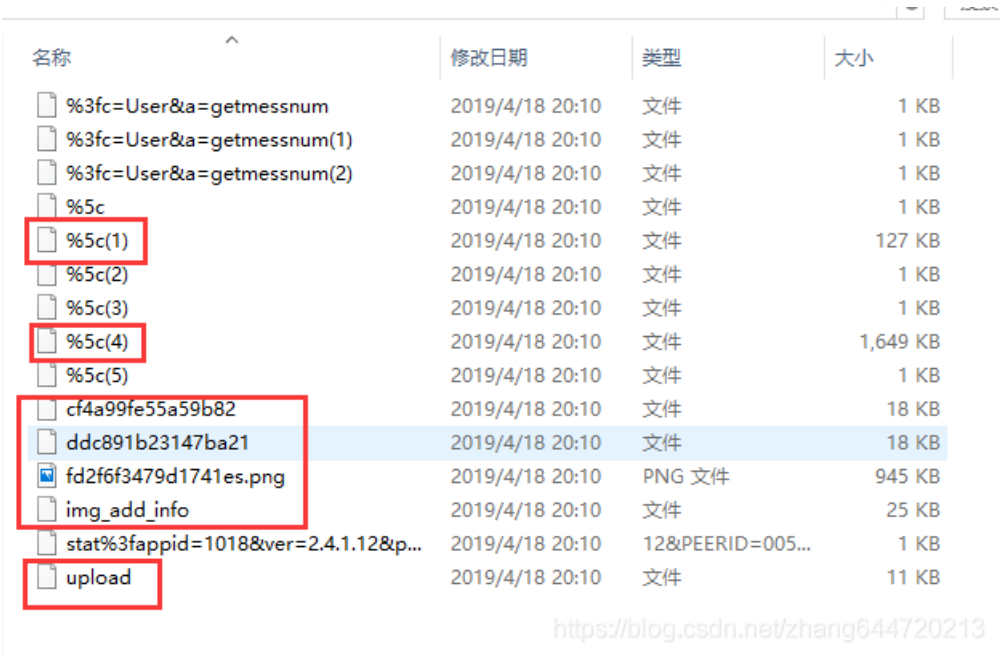
所以我们直接一键保存http的所有包再一个个分析

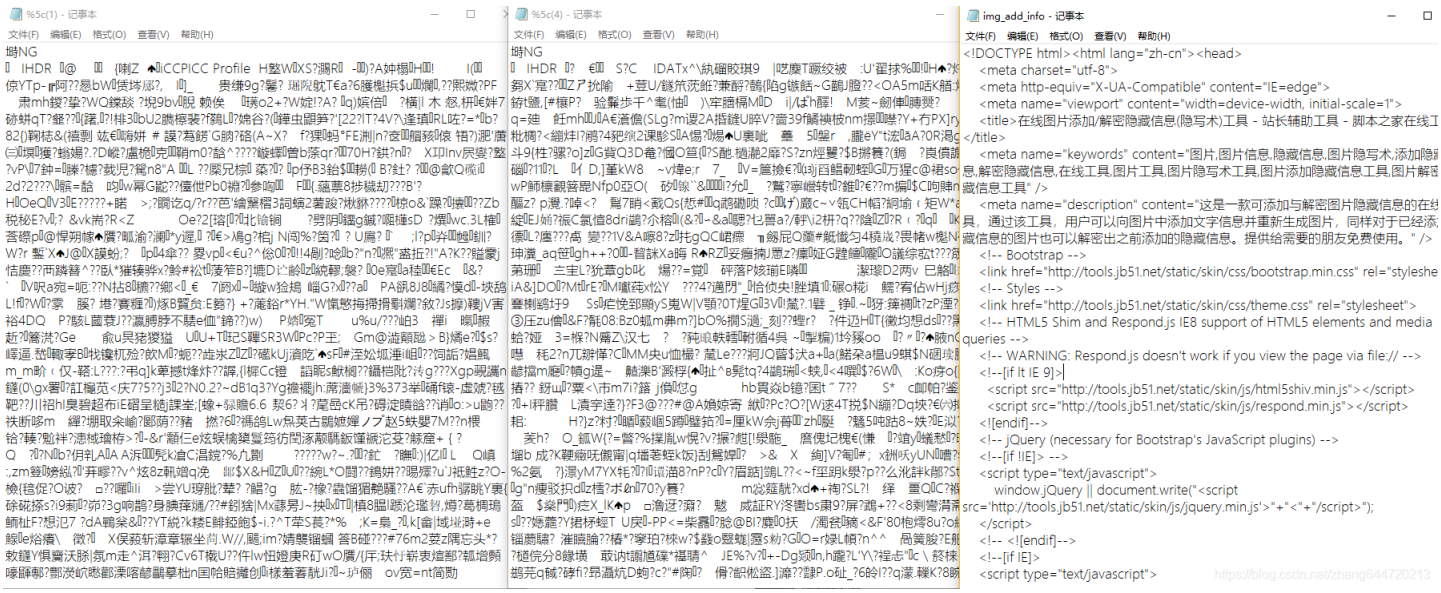


分析文件

通过查看提取出来的文件发现有那么几个可疑的文件，以及一张图片。我们把图片放一边，先查看一下那些文件，最后筛选出两个包含png的文件，以及一个html文件，提取一下html的url发现是个图片解密网站，而且需要密钥，于是猜想和文件中的两张png有关

图片解密网址

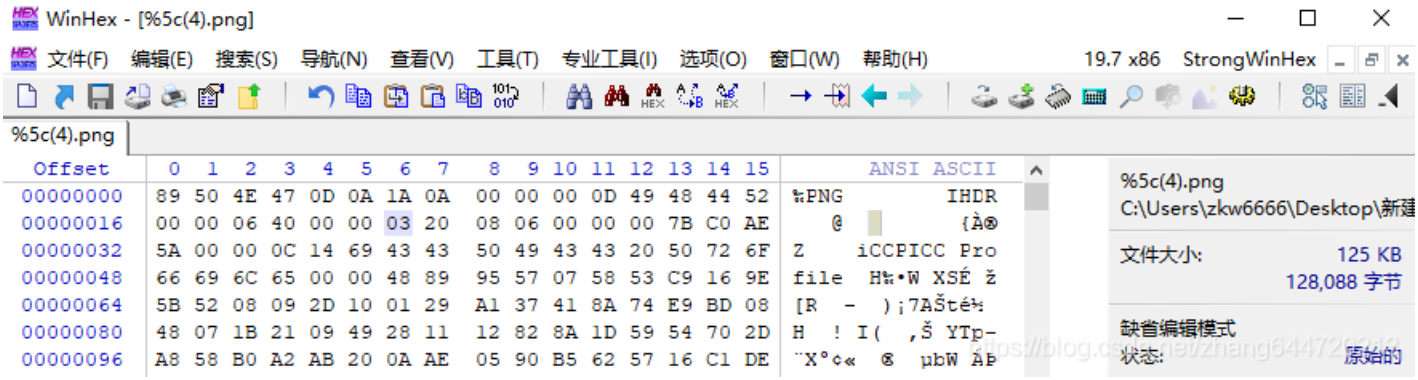




我们用winhex打开那张唯一的png图片，与另外两个文件作比较，并且用winhex提取出两张png

解码

这里可以看到有一张钥匙一样的图片，那么可以确定解密密钥肯定在这张图片里面，本来打算拖进kali里面用binwalk分析一波，结果发现连图片都打不开，emmmm...m?
我脸上洋溢着灿烂的微笑，以我做了三四道图片隐写题的经验，这是png宽高爆破啊
直接拖进winhex，修改下高度就出来了



key:57pmYyWt

然后直接去那个提取出来的网址里面解一下密

1. 从电脑中选择一张带有隐藏信息的图片： 选择文件 %5c(1).png

2. 输入需要解开信息的密码（如果没有密码可以不填）： ••••••••

解密出隐藏的信息

图片中隐藏的信息为：flag+AHs-
44444354467B5145576F6B63704865556F32574F6642494E37706F6749577346303469526A747D+AH0-

得出来的一看就是一串16进制的ascii码（因为最后一个是7D，在ascii中为'}'字符，所以很容易得出来）
直接base16一下就行了

Base16编码解码

44444354467B5145576F6B63704865556F32574F6642494E37706F6749577346303469526A747D

编码 解码

DDCTF{QEWokcpHeUo2WOfBIN7pogIWsF04iRjt}