CTF流量分析题

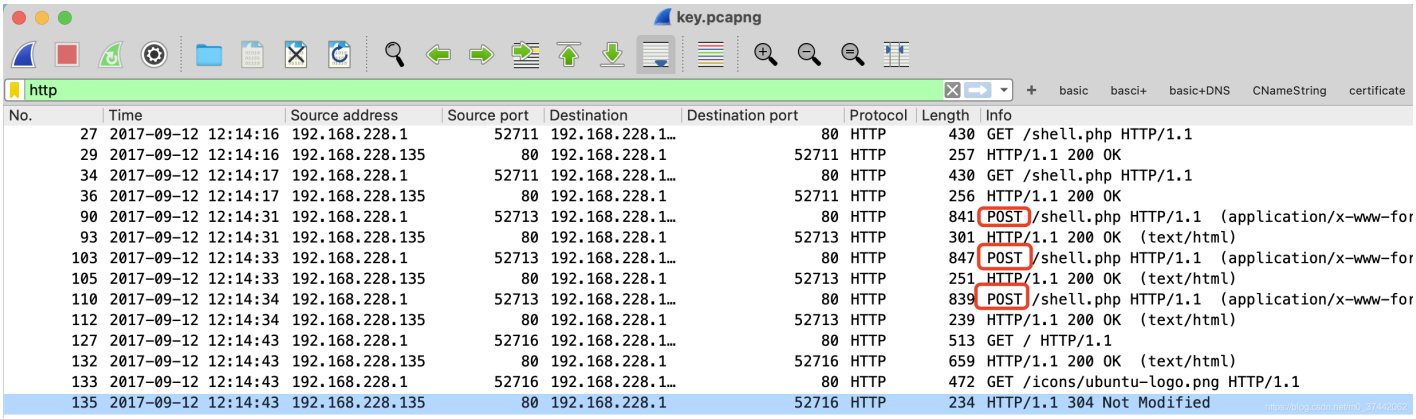
原创

进一寸有一寸的欢喜077 于 2021-05-03 21:47:57 发布 941 收藏 7
分类专栏： ctf

本文链接：https://blog.csdn.net/m0_37442062/article/details/116378287

1.flag被盗了，pcap（gnnl）

尝试http过滤，get或者post追踪tcp流即可，这里是post，



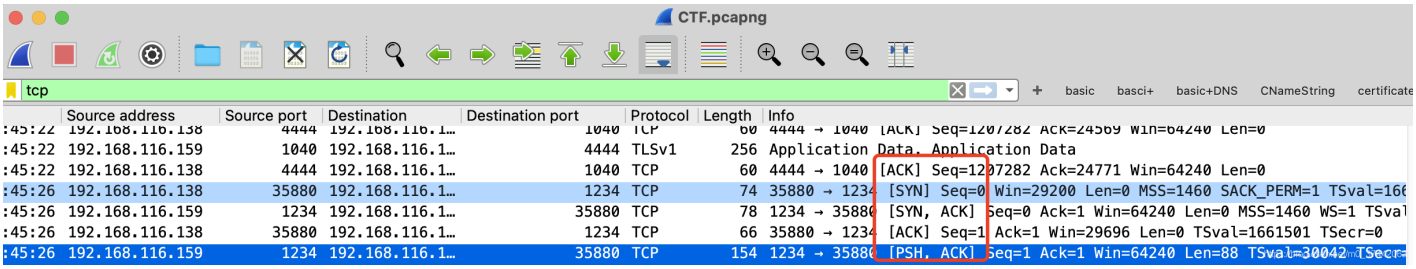
No.	Time	Source address	Source port	Destination	Destination port	Protocol	Length	Info
27	2017-09-12 12:14:16	192.168.228.1	52711	192.168.228.1…	80	HTTP	430	GET /shell.php HTTP/1.1
29	2017-09-12 12:14:16	192.168.228.135	80	192.168.228.1	52711	HTTP	257	HTTP/1.1 200 OK
34	2017-09-12 12:14:17	192.168.228.1	52711	192.168.228.1…	80	HTTP	430	GET /shell.php HTTP/1.1
36	2017-09-12 12:14:17	192.168.228.135	80	192.168.228.1	52711	HTTP	256	HTTP/1.1 200 OK
90	2017-09-12 12:14:31	192.168.228.1	52713	192.168.228.1…	80	HTTP	841	POST /shell.php HTTP/1.1 (application/x-www-for
93	2017-09-12 12:14:31	192.168.228.135	80	192.168.228.1	52713	HTTP	301	HTTP/1.1 200 OK (text/html)
103	2017-09-12 12:14:33	192.168.228.1	52713	192.168.228.1…	80	HTTP	847	POST /shell.php HTTP/1.1 (application/x-www-for
105	2017-09-12 12:14:33	192.168.228.135	80	192.168.228.1	52713	HTTP	251	HTTP/1.1 200 OK (text/html)
110	2017-09-12 12:14:34	192.168.228.1	52713	192.168.228.1…	80	HTTP	839	POST /shell.php HTTP/1.1 (application/x-www-for
112	2017-09-12 12:14:34	192.168.228.135	80	192.168.228.1	52713	HTTP	239	HTTP/1.1 200 OK (text/html)
127	2017-09-12 12:14:43	192.168.228.1	52716	192.168.228.1…	80	HTTP	513	GET / HTTP/1.1
132	2017-09-12 12:14:43	192.168.228.135	80	192.168.228.1	52716	HTTP	659	HTTP/1.1 200 OK (text/html)
133	2017-09-12 12:14:43	192.168.228.1	52716	192.168.228.1…	80	HTTP	472	GET /icons/ubuntu-logo.png HTTP/1.1
135	2017-09-12 12:14:43	192.168.228.135	80	192.168.228.1	52716	HTTP	234	HTTP/1.1 304 Not Modified

```
X@Yflag{This_is_a_f10g}
[S]
/var/www/html
[E]
X@YPOST /shell.php HTTP/1.1
X-Forwarded-For: 44.146.238.198
Referer: http://192.168.228.135/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http
```

flag{This_is_a_f10g}

2.这么多数据包找找吧，先找到getshell的流pcap（vn78）

过滤tcp



TCP流通常是命令行操作

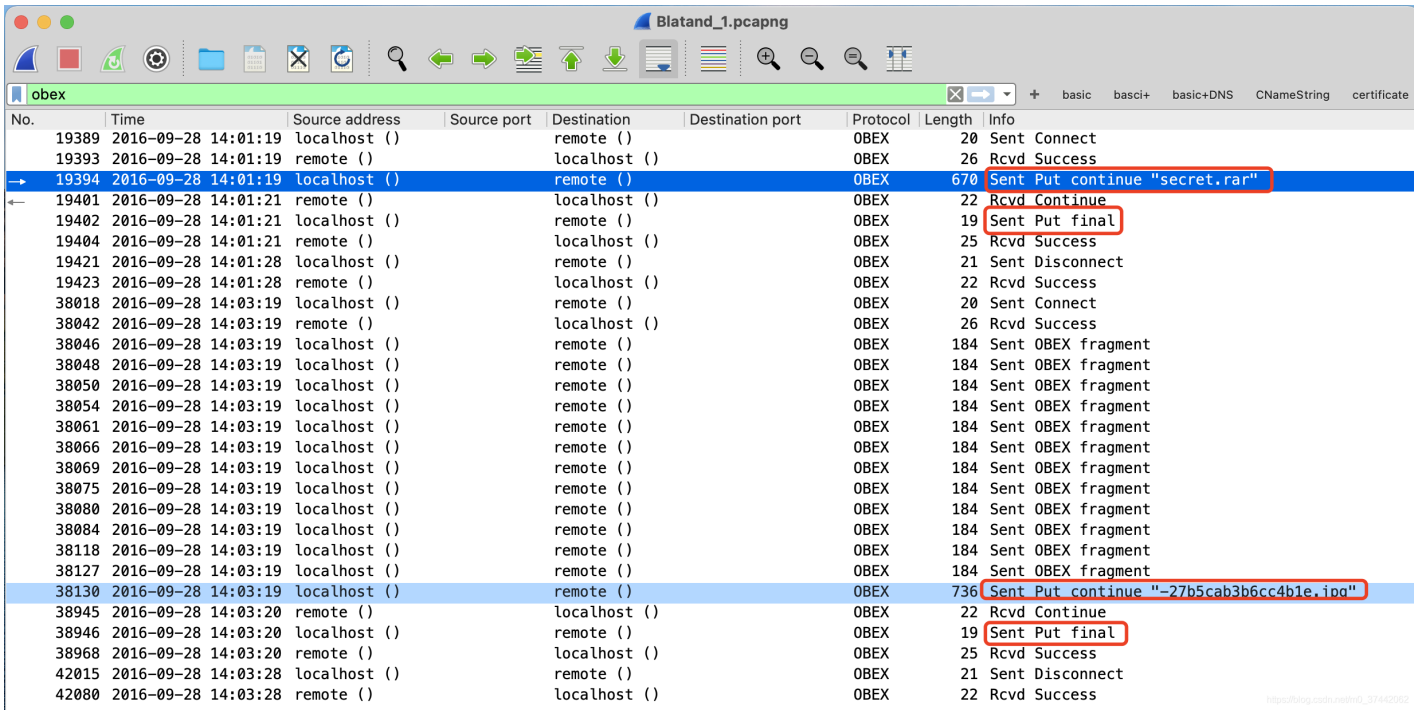
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B03C-791A

 Directory of C:\

04/14/2016  08:50 PM                 0 AUTOEXEC.BAT
04/14/2016  08:50 PM                 0 CONFIG.SYS

04/14/2016  08:52 PM    <DIR>          Documents and Settings
03/12/2012  10:24 PM            61,454 nc.exe
04/14/2016  08:54 PM    <DIR>          Program Files
04/14/2016  09:22 PM                36 s4cr4t.txt
04/14/2016  08:59 PM    <DIR>          WINDOWS
               4 File(s)         61,490 bytes
               3 Dir(s)  17,719,083,008 bytes free

C:\>type s4cr4t.txt
type s4cr4t.txt
Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==
C:\>shutdown -r -t 100 -m "Stupid Manager!"
shutdown -r -t 100 -m "Stupid Manager!"
```


Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==

解码：CCTF{do_you_like_sniffer}

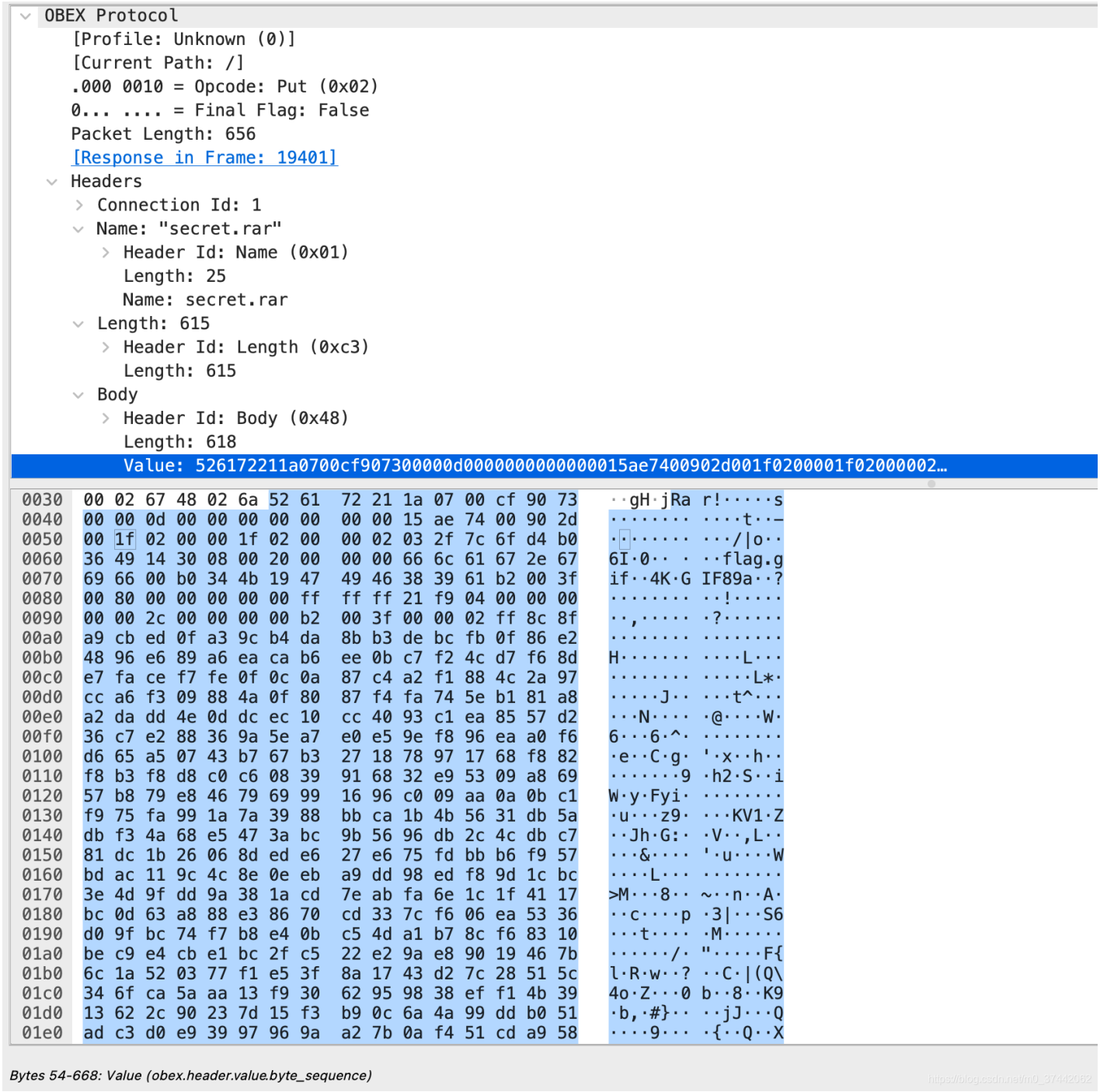
3.有一天皓宝宝没了流量只好手机来共享，顺便又从手机发了点小秘密到电脑，你能找到它吗？pcap（kbeg）

过滤obex



No.	Time	Source address	Source port	Destination	Destination port	Protocol	Length	Info
19389	2016-09-28 14:01:19	localhost ()		remote ()		OBEX	20	Sent Connect
19393	2016-09-28 14:01:19	remote ()		localhost ()		OBEX	26	Rcvd Success
19394	2016-09-28 14:01:19	localhost ()		remote ()		OBEX	670	Sent Put continue "secret.rar"
19401	2016-09-28 14:01:21	remote ()		localhost ()		OBEX	22	Rcvd Continue
19402	2016-09-28 14:01:21	localhost ()		remote ()		OBEX	19	Sent Put final
19404	2016-09-28 14:01:21	remote ()		localhost ()		OBEX	25	Rcvd Success
19421	2016-09-28 14:01:28	localhost ()		remote ()		OBEX	21	Sent Disconnect
19423	2016-09-28 14:01:28	remote ()		localhost ()		OBEX	22	Rcvd Success
38018	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	20	Sent Connect
38042	2016-09-28 14:03:19	remote ()		localhost ()		OBEX	26	Rcvd Success
38046	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38048	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38050	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38054	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38061	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38066	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38069	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38075	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38080	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38084	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38118	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38127	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38130	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	736	Sent Put continue "-27b5cab3b6cc4b1e.jpg"
38945	2016-09-28 14:03:20	remote ()		localhost ()		OBEX	22	Rcvd Continue
38946	2016-09-28 14:03:20	localhost ()		remote ()		OBEX	19	Sent Put final
38968	2016-09-28 14:03:20	remote ()		localhost ()		OBEX	25	Rcvd Success
42015	2016-09-28 14:03:28	localhost ()		remote ()		OBEX	21	Sent Disconnect
42080	2016-09-28 14:03:28	remote ()		localhost ()		OBEX	22	Rcvd Success

尝试导出分组字节流，无效

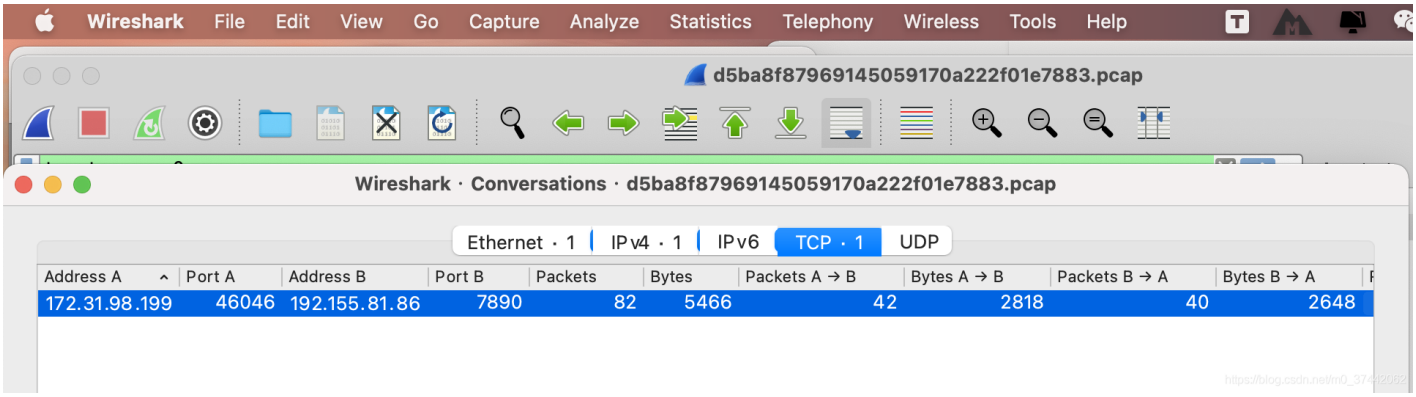


可以看到右侧有一个flag.gif

把选中部分粘贴到二进制编辑器中，保存为secret.rar，解压得到flag.gif。如下图

4.你能从截取的数据包中得到flag吗？

统计，发现tcp只有一条

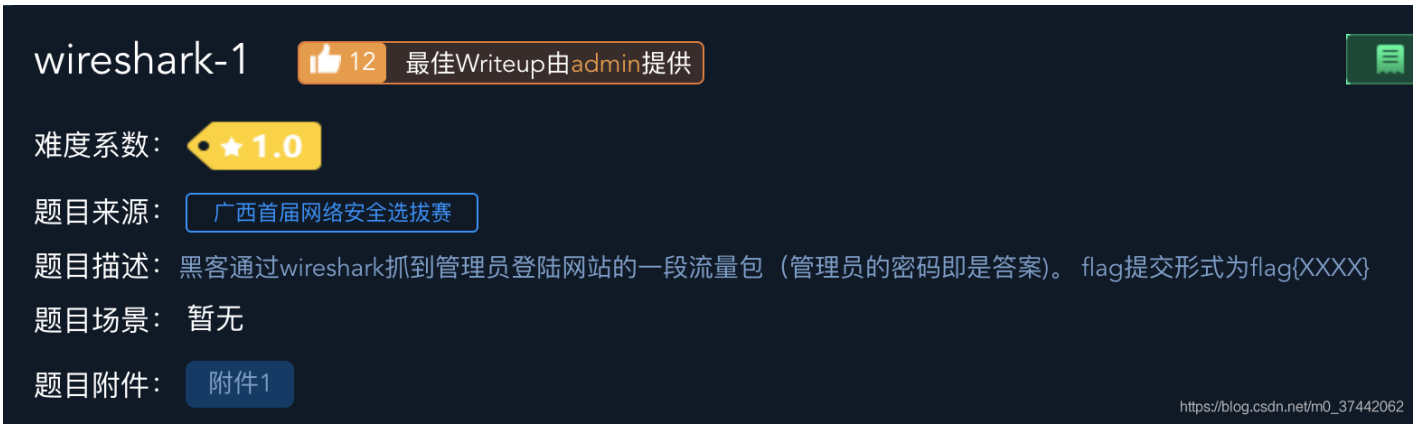


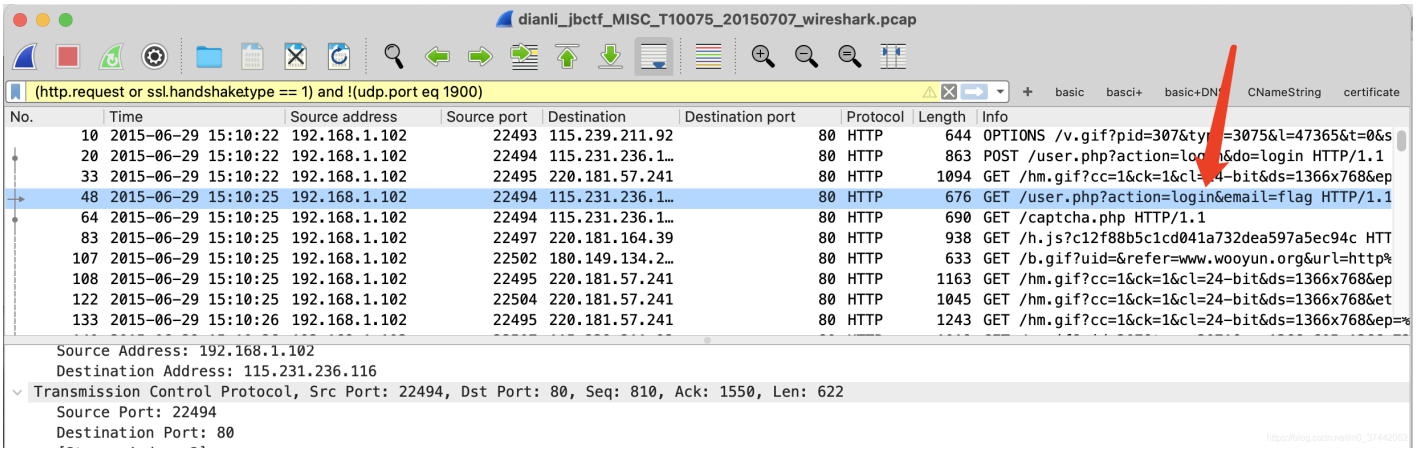
follow stream

```
FLAG:385b87afc8671dee07550290d16a8071
```

FLAG:385b87afc8671dee07550290d16a8071

5.黑客通过wireshark抓到管理员登陆网站的一段流量包（管理员的密码即是答案)。 flag提交形式为flag{XXXX}






```
POST /user.php?action=login&do=login HTTP/1.1
Host: www.wooyun.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.wooyun.org/user.php?action=login
Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400; Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1434891316,143528
bdshare_firstime=1433775454650; wy_uid=-1; PHPSESSID=h8i10mi6rdc8l9coc708otq661; Hm_lpvt_c12f88b5c1cd041a732dea597a5ec9
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

email=flag&password=ffb7567a1d4f4abdffdb54e022f8facd&captcha=BYUGHTTP/1.1 200 OK
Date: Mon, 29 Jun 2015 15:09:10 GMT
```

flag{ffb7567a1d4f4abdffdb54e022f8facd}

6.

神奇的Modbus

23 最佳Writeup由0xfafu-1 • giun提供

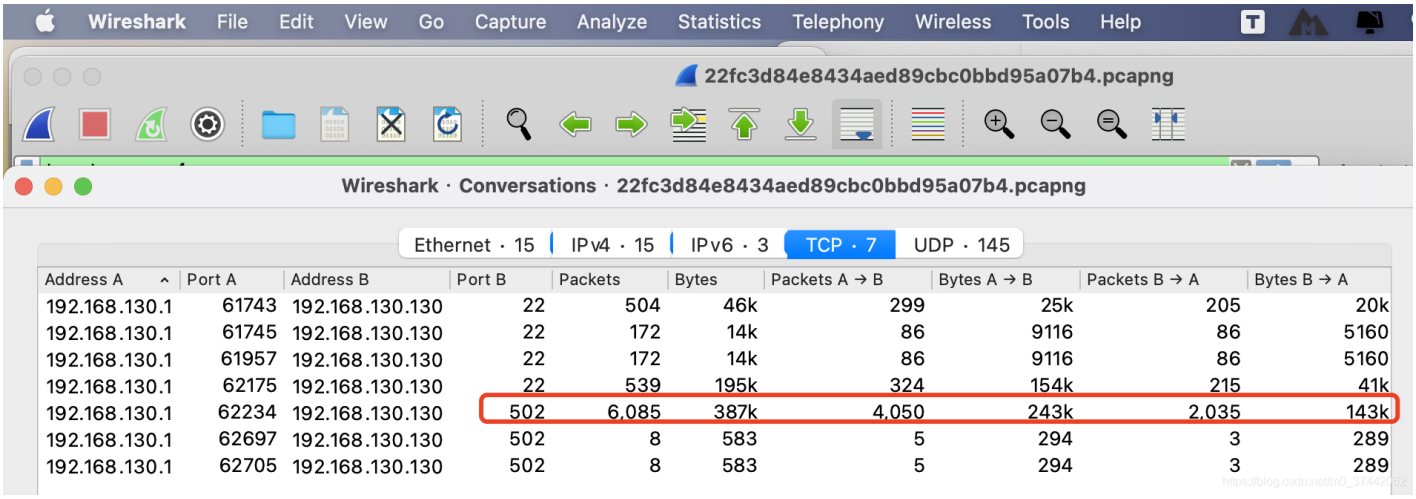
难度系数：★★2.0

题目来源：XCTF 4th-SCTF-2018

题目描述：寻找flag,提交格式为sctf{xxx}

题目场景：暂无

题目附件：附件1



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.130.1	61743	192.168.130.130	22	504	46k	299	25k	205	20k
192.168.130.1	61745	192.168.130.130	22	172	14k	86	9116	86	5160
192.168.130.1	61957	192.168.130.130	22	172	14k	86	9116	86	5160
192.168.130.1	62175	192.168.130.130	22	539	195k	324	154k	215	41k
192.168.130.1	62234	192.168.130.130	502	6,085	387k	4,050	243k	2,035	143k
192.168.130.1	62697	192.168.130.130	502	8	583	5	294	3	289
192.168.130.1	62705	192.168.130.130	502	8	583	5	294	3	289

比较大，跟踪流，发现

去除点，得到**sctf{Easy_Mdbus}**，发现提交并不对，再结合题目提交**sctf{Easy_Modbus}**即可。

7.

流量分析

3 最佳Writeup由admin提供

难度系数：★★★★★★★7.0

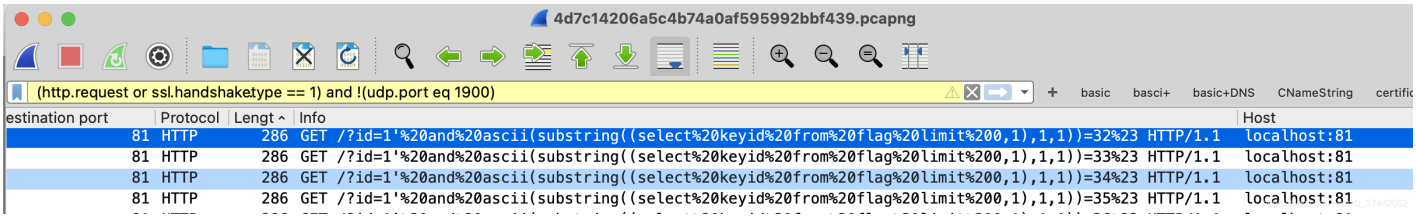
题目来源：暂无

题目描述：sql注入

题目场景：暂无

题目附件：附件1

先找到了get语句

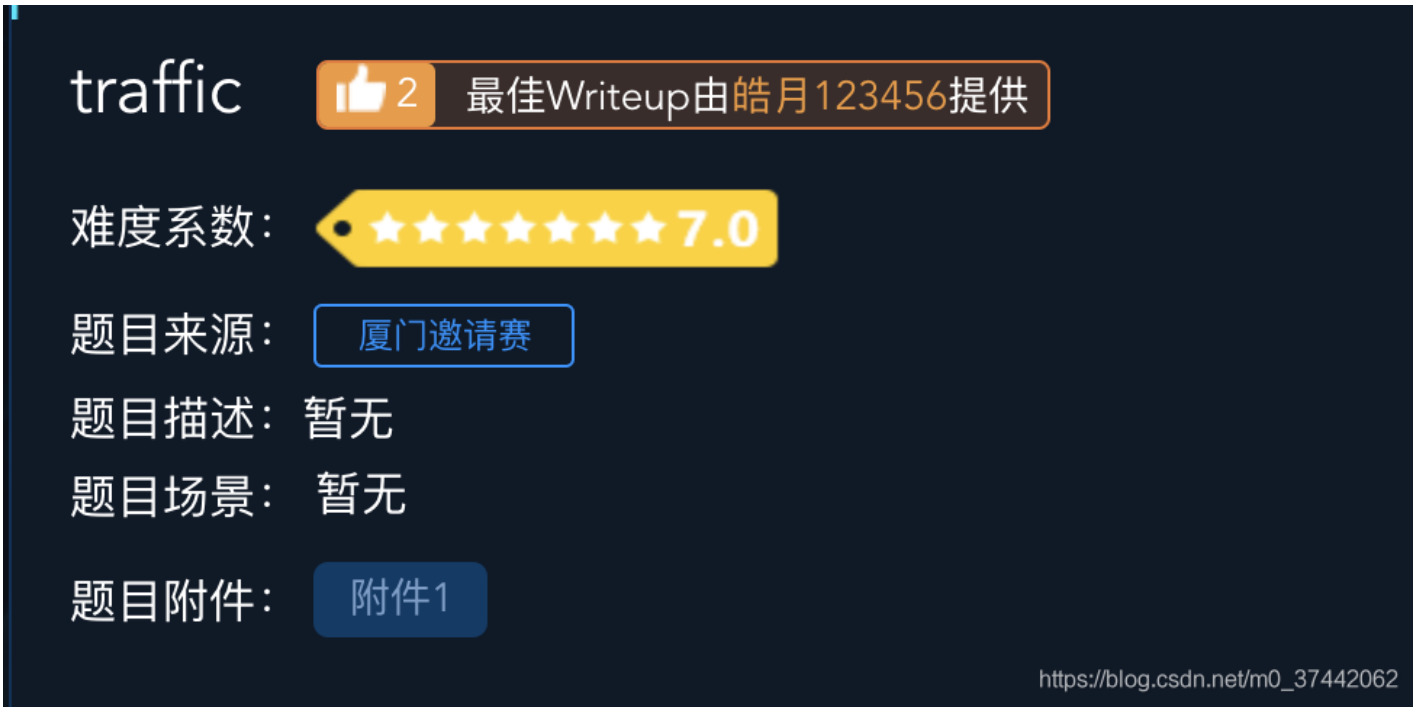


substring函数是取字符串的特定位置，此处参考攻防世界 Misc高手进阶区 7分题 流量分析

```
import re

with open("/Users/yueting/下载/4d7c14206a5c4b74a0af595992bbf439.pcapng", "rb") as f:
    contents = f.read()
    res = re.compile(r'0,1\),(\d+),1\)\)=(\d+)%23').findall(str(contents))
    dic = {}
    #取a对应b的最大值
    for a, b in res:
        if a in dic:
            if int(b) > dic[a]:
                dic[a] = int(b)
        else:
            dic[a] = int(b)
    flag = ""
    for i in range(1,39):
        flag += chr(dic[str(i)])
    print(flag)
```

flag{c2bbf9cecdaf656cf524d014c5bf046c}

8.



明天再来吧