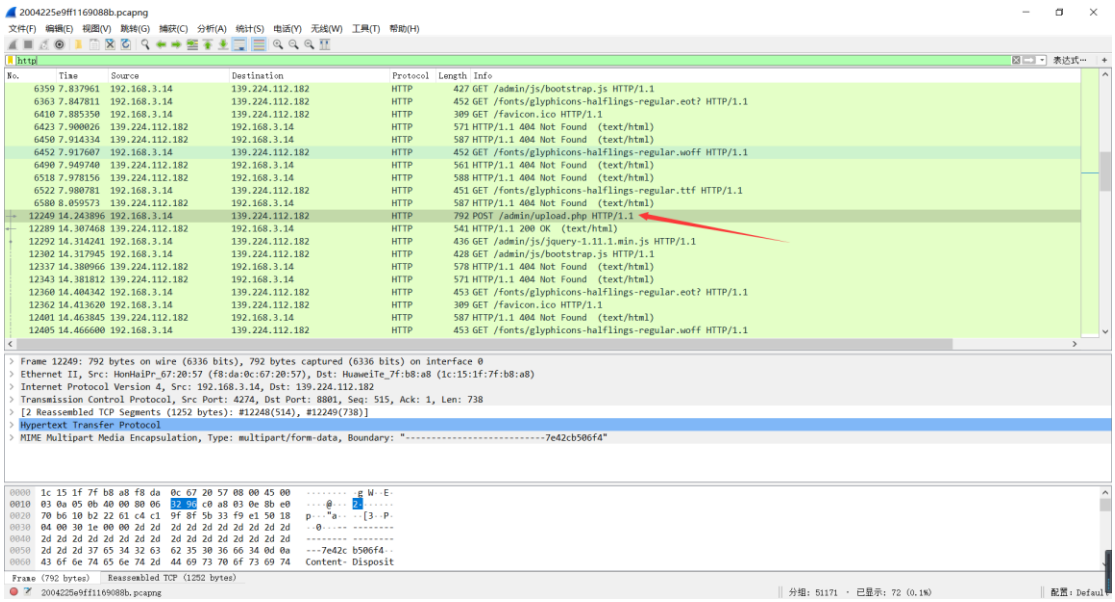
AWDshell Writeup

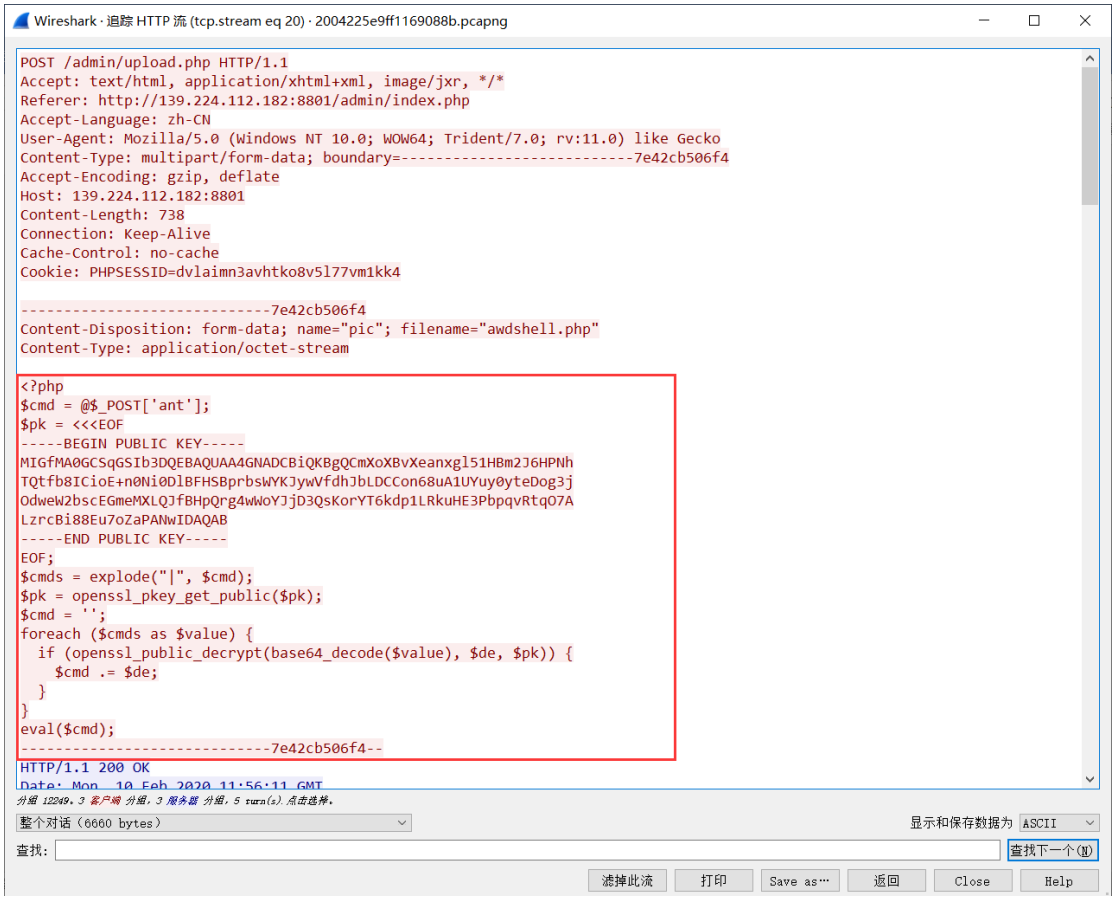
Nepnep@1cePeak

根据题目描述是一个 shell🐂，之后在大量的 udp 混淆流量中追踪 HTTP，发现 upload.php



追踪 HTTP 流

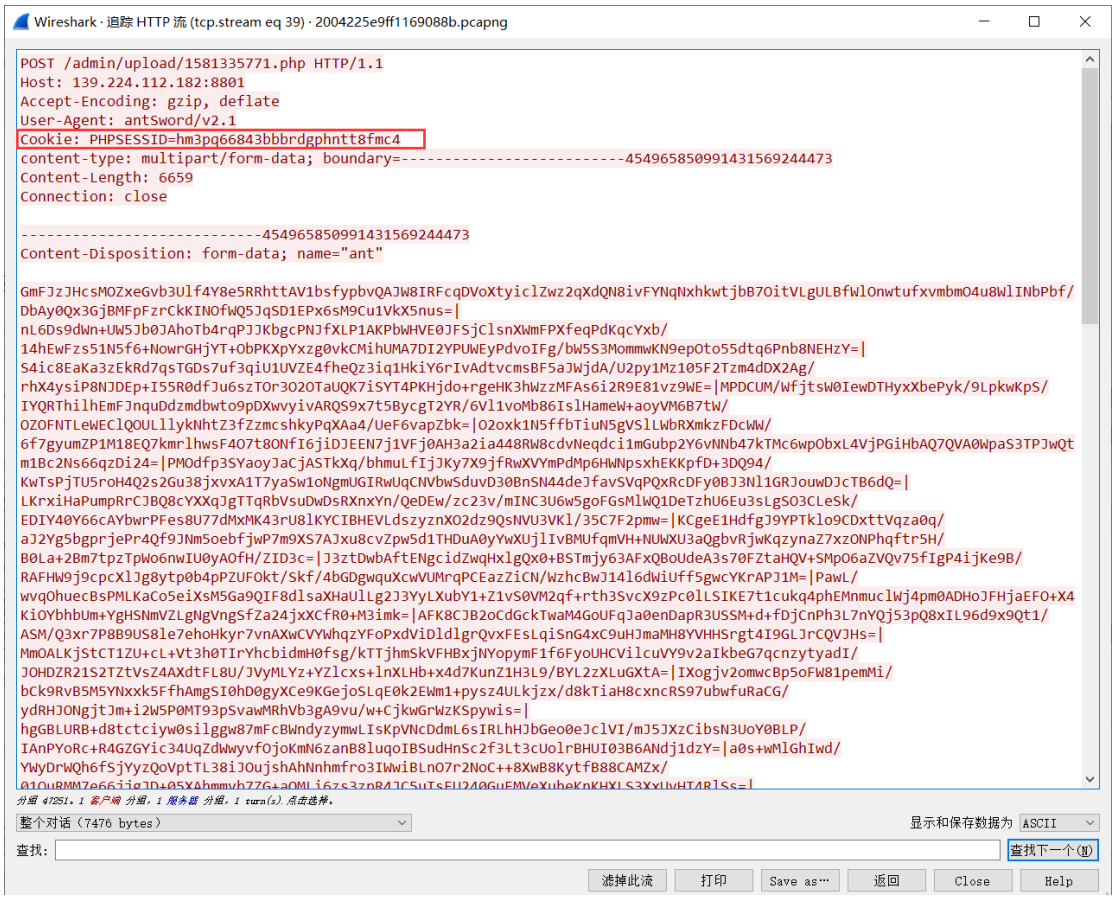
一个用蚁剑来连接的 RSA🐂



追踪其中一个木马传输的流量

拿到 session

hm3pq66843bbbrdgphntt8fmc4



分组 47251。1 客户端 分组，1 服务器 分组，1 turn(s)。点击选择。

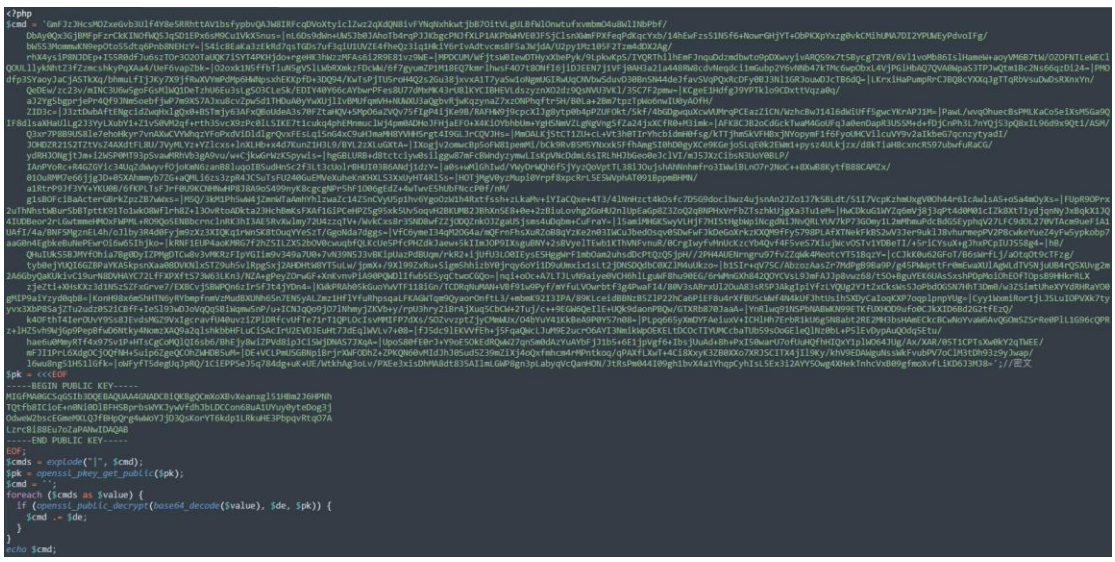
整个对话（7476 bytes）　显示和保存数据为 ASCII

查找：　查找下一个(N)

滤掉此流　打印　Save as…　返回　Close　Help

破解密文

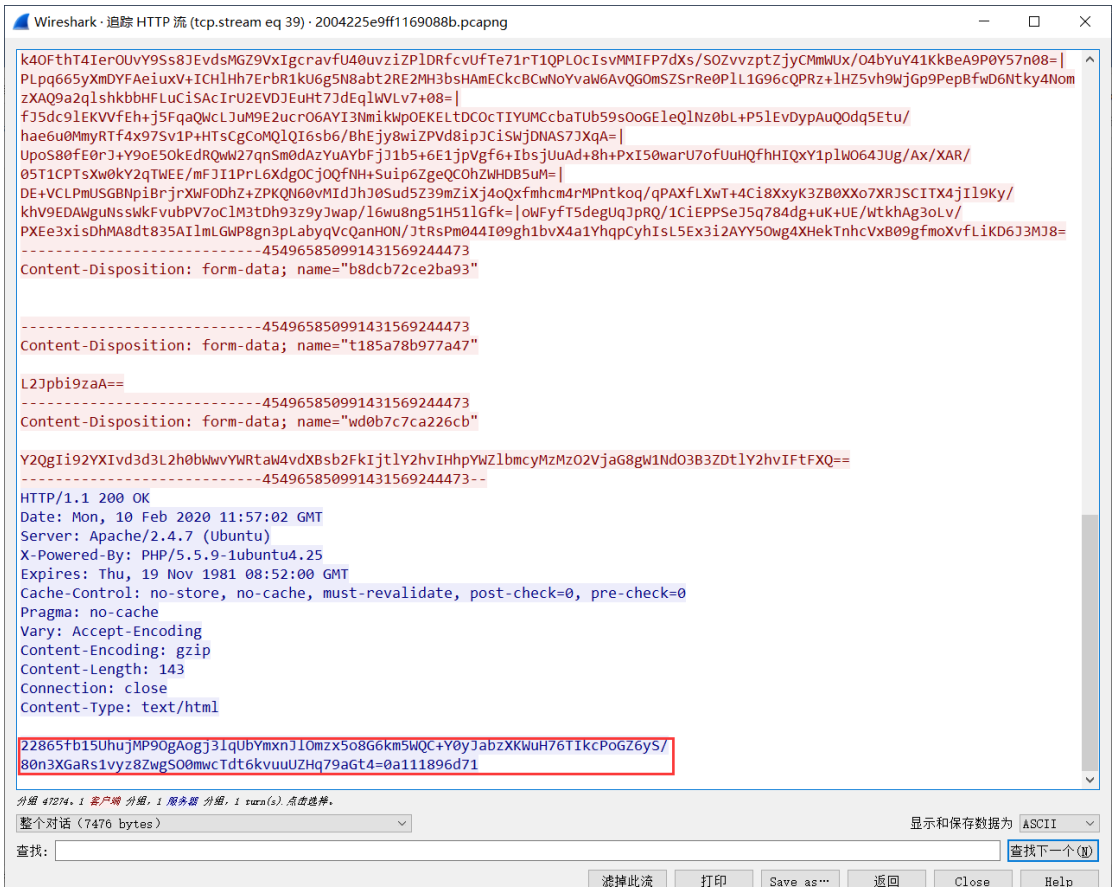
我们可以利用上传的 rsa 木马的公钥进行解密



解密后返回一串 php 代码

```
@ini_set("display_errors", "0");
@set_time_limit(0);
function asenc($out){
    @session_start();
    $key=@substr(str_pad(session_id(),16,'a'),0,16);
    return @base64_encode(openssl_encrypt(base64_encode($out), 'AES-128-ECB', $key, OPENSSL_RAW_DATA));
    };
function asoutput(){
    $output=ob_get_contents();
    ob_end_clean();
    echo "22865fb15";
    echo @asenc($output);
    echo "0a111896d71";}
    ob_start();
    try{$p=base64_decode($_POST["t185a78b977a47"]);
    $s=base64_decode($_POST["wd0b7c7ca226cb"]);
    $envstr=@base64_decode($_POST["b8dcb72ce2ba93"]);
    $d=dirname($_SERVER["SCRIPT_FILENAME"]);
```

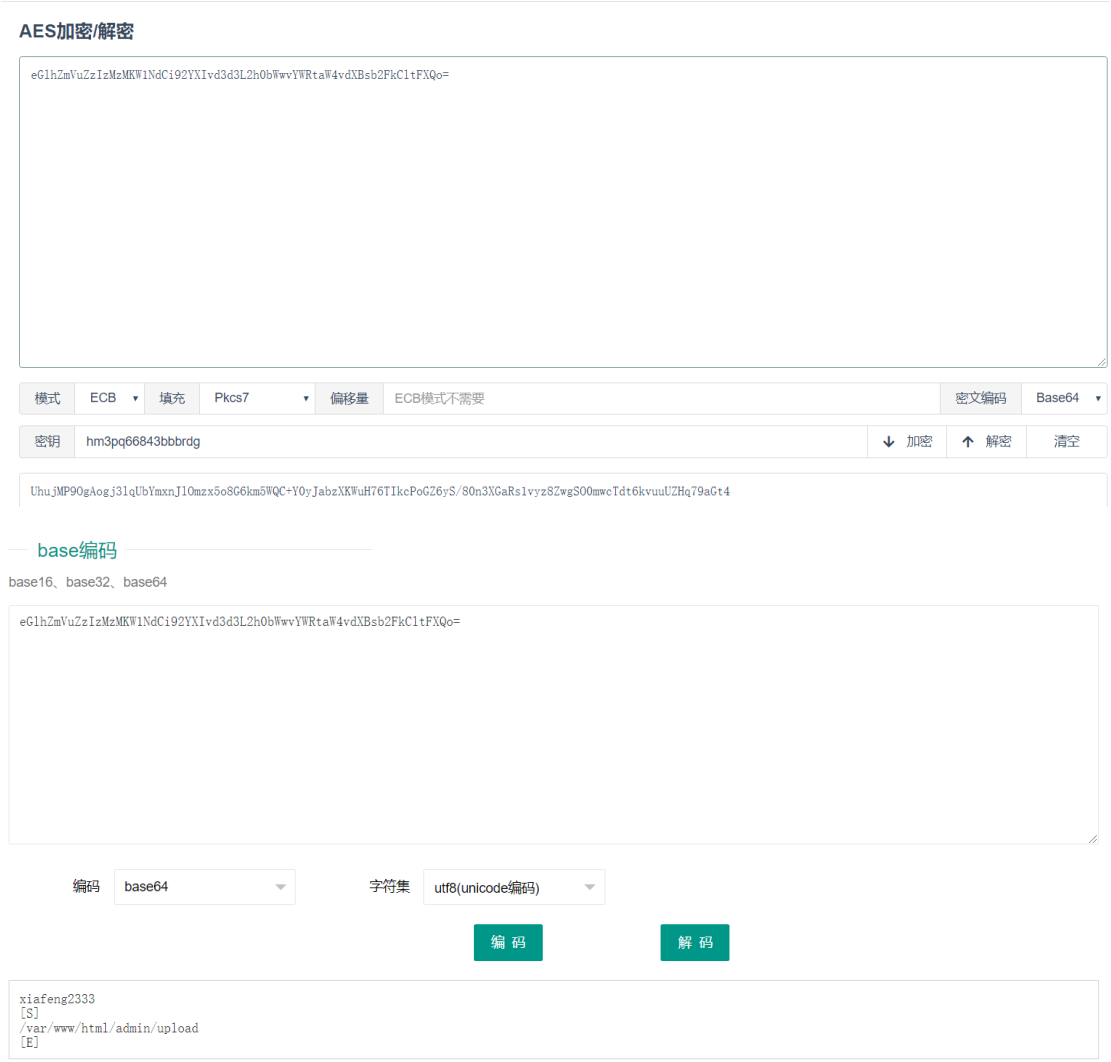
观察发现流量采用 AES-128-ECB 加密，key 取 session 的前 16 位，同时继续读代码发现流量前后都有垃圾字符（坏



AES 解密+base64 解密

AES 解密网站 https://oktools.net/aes

22865fb15UhujMP9OgAogj3lqUbYmxnJlOmzx5o8G6km5WQC+Y0yJabzXKWuH76TIkcPoGZ6yS/80n3XGaRs1vyz8ZwgSO0mwcTdt6kvuuUZHq79aGt4=0a111896d71



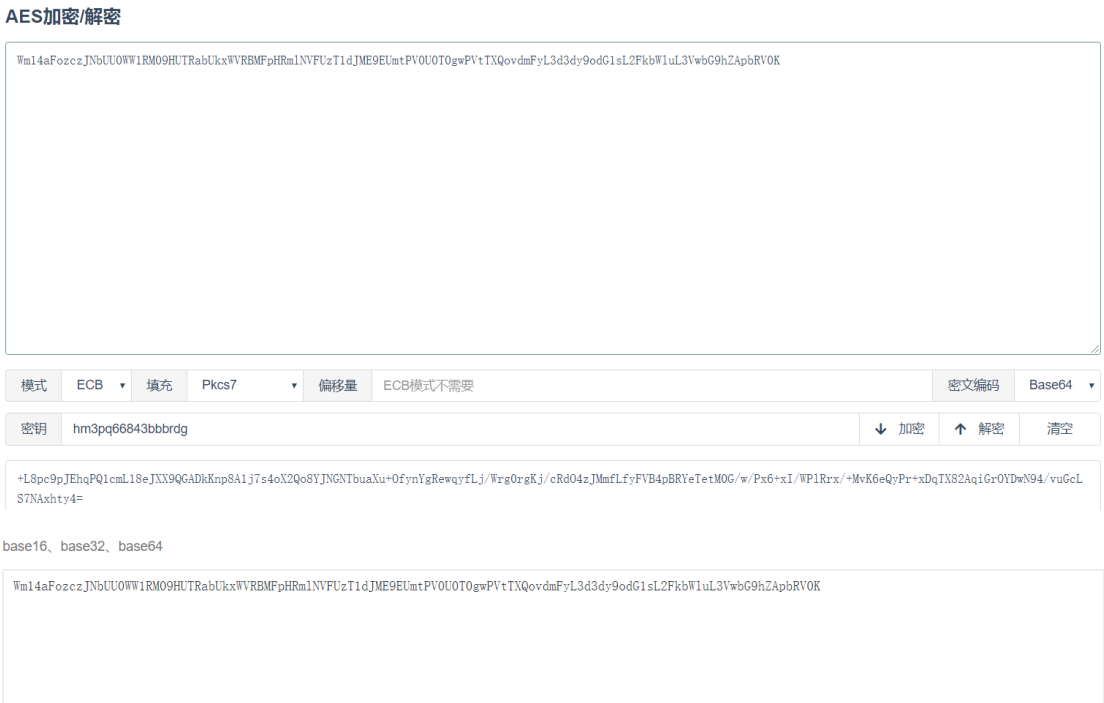
夏风师傅 tql（happymisc

芜湖~刚才追踪的最后一个流量没有发现 flag，按照以上方法逐个查找，倒数第二个有 flag

```
@ini_set("display_errors", "0");
@set_time_limit(0);
function asenc($out){
    @session_start();
    $key=@substr(str_pad(session_id(),16,'a'),0,16);
    return @base64_encode(openssl_encrypt(base64_encode($out), 'AES-128-ECB', $key, OPENSSL_RAW_DATA));
    };;
    function asoutput(){
    $output=ob_get_contents();ob_end_clean();
    echo "f3c7239848e0";
    echo @asenc($output);
    echo "05fda2646c";
    }
    ob_start();
    try{$p=base64_decode($_POST["t185a78b977a47"]);
    $s=base64_decode($_POST["wd0b7c7ca226cb"]);
```

f3c7239848e0+L8pc9pJEhqPQ1cmL18eJXX9QGADkKnp8A1j7s4oX2Qo8YJNGNTbuaXu+OfynYgRewqyfLj/Wrg0rgKj/cRdO4zJMmfLfyFVB4pBRYeTetM0G/w/Px6+xl/WPlRrx/+MvK6eQyPr+xDqTX82AqiGrOYDwN94/vuGcLS7NAxhty4=05fda2646c

AES 解密

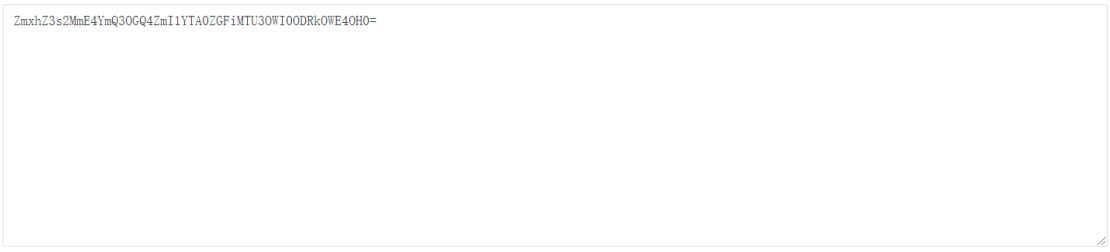


base16、base32、base64

ZmxhZ3s2MmE4YmQ3OGQ4ZmI1YTA0ZGFiMTU3OWIOODRkOWE4OHO=

再次进行 base64 解密

base16、base32、base64



成功拿到 flag

flag{62a8bd78d8fb5a04dab1579b484d9a88}