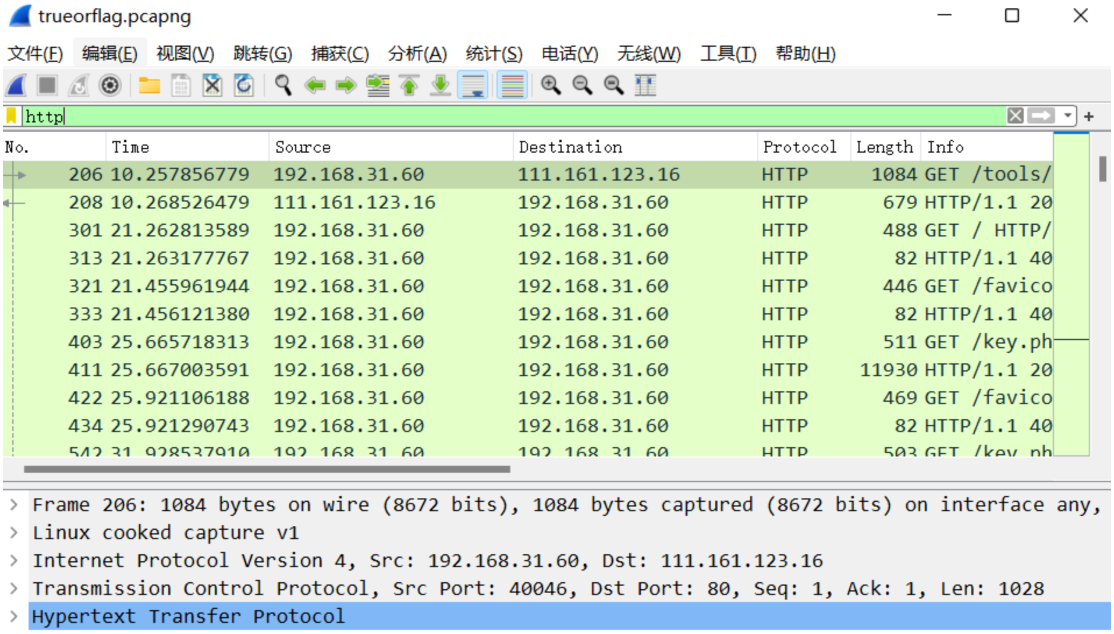
把 Protocol 包放入 wireshark 中，筛选 http 包

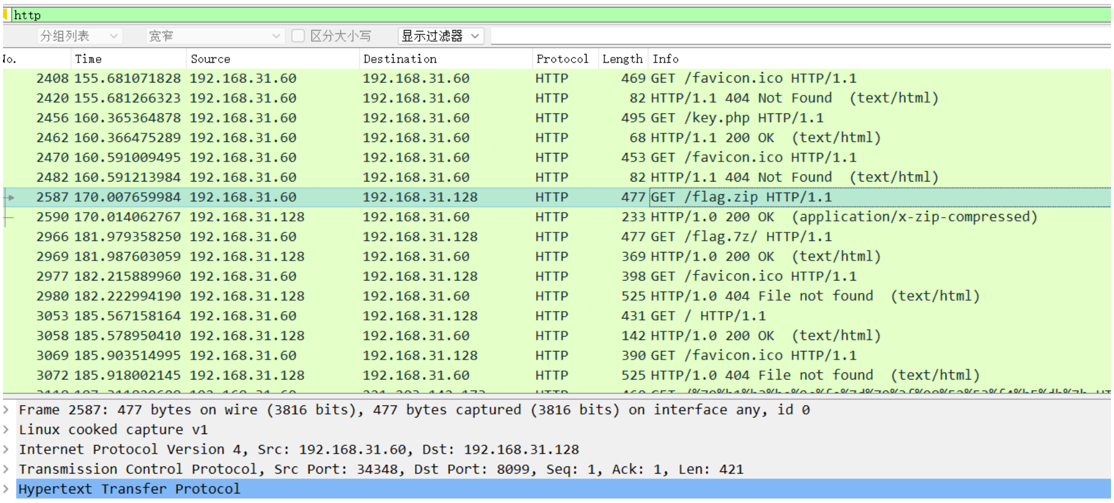

trueorflag.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http

No.	Time	Source	Destination	Protocol	Length	Info
206	10.257856779	192.168.31.60	111.161.123.16	HTTP	1084	GET /tools/
208	10.268526479	111.161.123.16	192.168.31.60	HTTP	679	HTTP/1.1 20
301	21.262813589	192.168.31.60	192.168.31.60	HTTP	488	GET / HTTP/
313	21.263177767	192.168.31.60	192.168.31.60	HTTP	82	HTTP/1.1 40
321	21.455961944	192.168.31.60	192.168.31.60	HTTP	446	GET /favico
333	21.456121380	192.168.31.60	192.168.31.60	HTTP	82	HTTP/1.1 40
403	25.665718313	192.168.31.60	192.168.31.60	HTTP	511	GET /key.ph
411	25.667003591	192.168.31.60	192.168.31.60	HTTP	11930	HTTP/1.1 20
422	25.921106188	192.168.31.60	192.168.31.60	HTTP	469	GET /favico
434	25.921290743	192.168.31.60	192.168.31.60	HTTP	82	HTTP/1.1 40
542	31.928537910	192.168.31.60	192.168.31.60	HTTP	503	GET /key.ph

```
> Frame 206: 1084 bytes on wire (8672 bits), 1084 bytes captured (8672 bits) on interface any,
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.31.60, Dst: 111.161.123.16
> Transmission Control Protocol, Src Port: 40046, Dst Port: 80, Seq: 1, Ack: 1, Len: 1028
> Hypertext Transfer Protocol
```

发现访问 flag.zip 右键追踪流

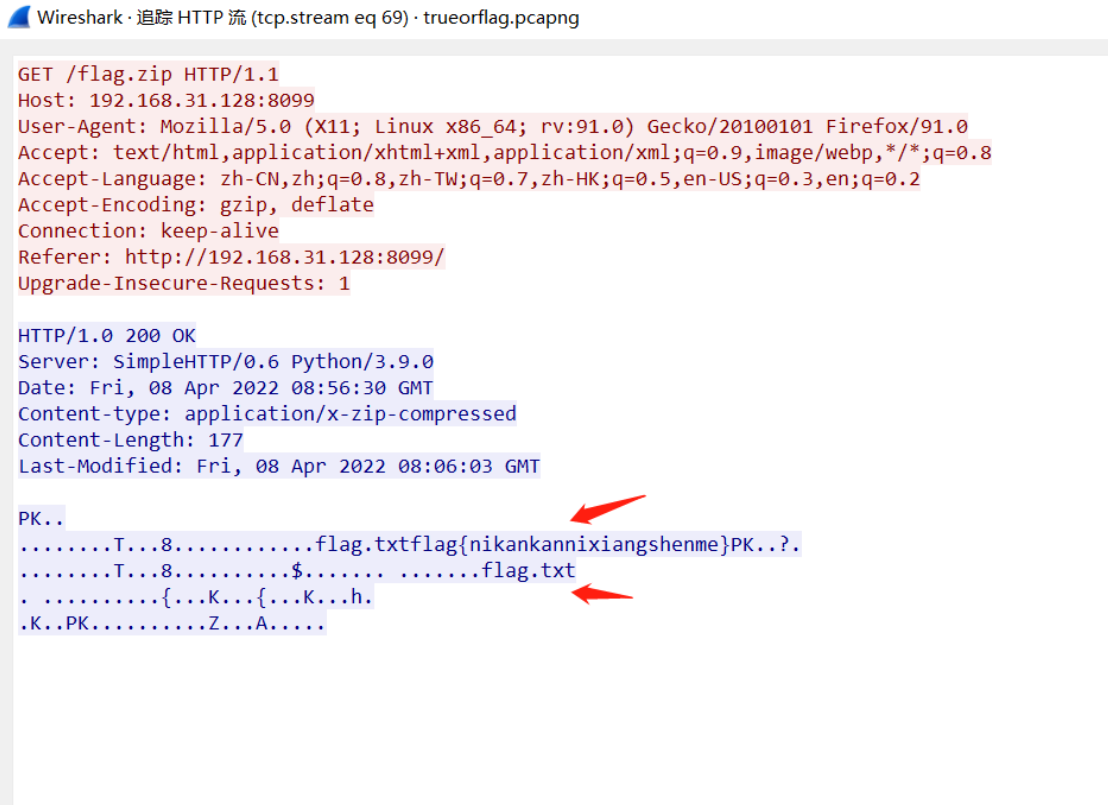


http

No.	Time	Source	Destination	Protocol	Length	Info
2408	155.681071828	192.168.31.60	192.168.31.60	HTTP	469	GET /favicon.ico HTTP/1.1
2420	155.681266323	192.168.31.60	192.168.31.60	HTTP	82	HTTP/1.1 404 Not Found (text/html)
2456	160.365364878	192.168.31.60	192.168.31.60	HTTP	495	GET /key.php HTTP/1.1
2462	160.366475289	192.168.31.60	192.168.31.60	HTTP	68	HTTP/1.1 200 OK (text/html)
2470	160.591009495	192.168.31.60	192.168.31.60	HTTP	453	GET /favicon.ico HTTP/1.1
2482	160.591213984	192.168.31.60	192.168.31.60	HTTP	82	HTTP/1.1 404 Not Found (text/html)
2587	170.007659984	192.168.31.60	192.168.31.128	HTTP	477	GET /flag.zip HTTP/1.1
2590	170.014062767	192.168.31.128	192.168.31.60	HTTP	233	HTTP/1.0 200 OK (application/x-zip-compressed)
2966	181.979358250	192.168.31.60	192.168.31.128	HTTP	477	GET /flag.7z/ HTTP/1.1
2969	181.987603059	192.168.31.128	192.168.31.60	HTTP	369	HTTP/1.0 200 OK (text/html)
2977	182.215889960	192.168.31.60	192.168.31.128	HTTP	398	GET /favicon.ico HTTP/1.1
2980	182.222994190	192.168.31.128	192.168.31.60	HTTP	525	HTTP/1.0 404 File not found (text/html)
3053	185.567158164	192.168.31.60	192.168.31.128	HTTP	431	GET / HTTP/1.1
3058	185.578950410	192.168.31.128	192.168.31.60	HTTP	142	HTTP/1.0 200 OK (text/html)
3069	185.903514995	192.168.31.60	192.168.31.128	HTTP	390	GET /favicon.ico HTTP/1.1
3072	185.918002145	192.168.31.128	192.168.31.60	HTTP	525	HTTP/1.0 404 File not found (text/html)

```
> Frame 2587: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.31.60, Dst: 192.168.31.128
> Transmission Control Protocol, Src Port: 34348, Dst Port: 8099, Seq: 1, Ack: 1, Len: 421
> Hypertext Transfer Protocol
```

发现还存在 flag.txt



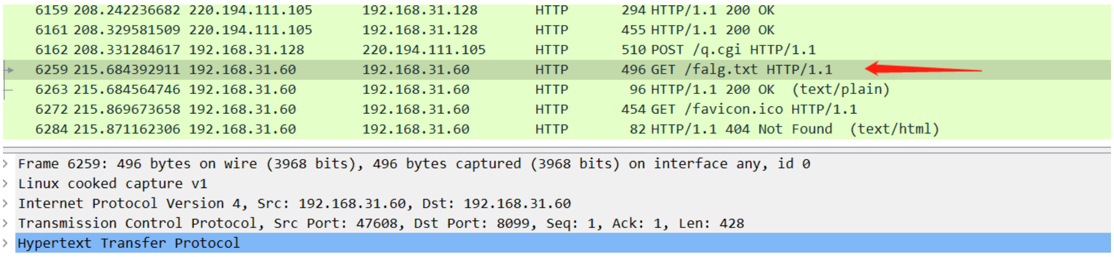
Wireshark · 追踪 HTTP 流 (tcp.stream eq 69) · trueorflag.pcapng

```
GET /flag.zip HTTP/1.1
Host: 192.168.31.128:8099
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.31.128:8099/
Upgrade-Insecure-Requests: 1

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.9.0
Date: Fri, 08 Apr 2022 08:56:30 GMT
Content-type: application/x-zip-compressed
Content-Length: 177
Last-Modified: Fri, 08 Apr 2022 08:06:03 GMT

PK..
........T...8...........flag.txtflag{nikankannixiangshenme}PK..?.
........T...8..........$.......  .......flag.txt
.  ..........{...K...{...K...h.
.K..PK..........Z...A.....
```

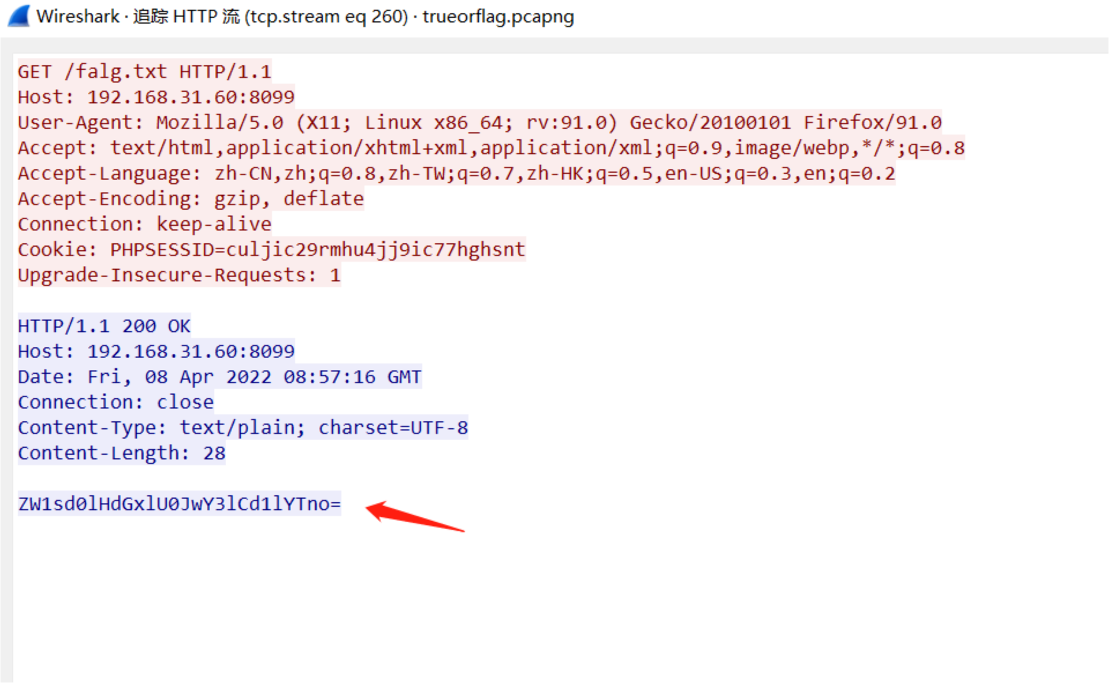
在日志底部



```
   6159 208.242236682 220.194.111.105      192.168.31.128       HTTP       294 HTTP/1.1 200 OK
   6161 208.329581509 220.194.111.105      192.168.31.128       HTTP       455 HTTP/1.1 200 OK
   6162 208.331284617 192.168.31.128       220.194.111.105      HTTP       510 POST /q.cgi HTTP/1.1
   6259 215.684392911 192.168.31.60        192.168.31.60        HTTP       496 GET /falg.txt HTTP/1.1
   6263 215.684564746 192.168.31.60        192.168.31.60        HTTP        96 HTTP/1.1 200 OK  (text/plain)
   6272 215.869673658 192.168.31.60        192.168.31.60        HTTP       454 GET /favicon.ico HTTP/1.1
   6284 215.871162306 192.168.31.60        192.168.31.60        HTTP        82 HTTP/1.1 404 Not Found  (text/html)

> Frame 6259: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.31.60, Dst: 192.168.31.60
> Transmission Control Protocol, Src Port: 47608, Dst Port: 8099, Seq: 1, Ack: 1, Len: 428
> Hypertext Transfer Protocol
```

追踪流



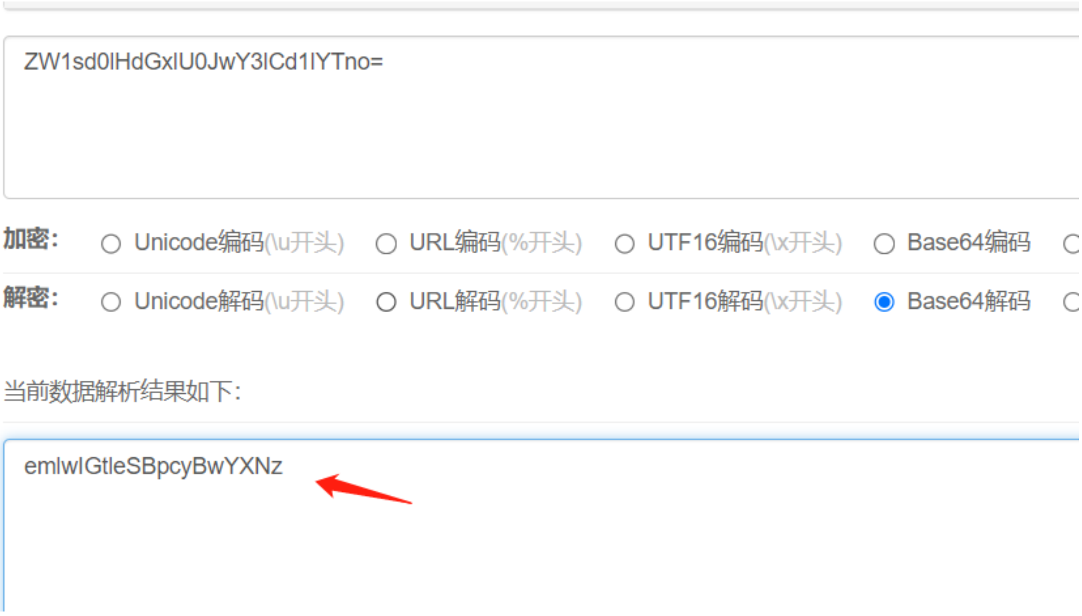
Wireshark · 追踪 HTTP 流 (tcp.stream eq 260) · trueorflag.pcapng

```
GET /falg.txt HTTP/1.1
Host: 192.168.31.60:8099
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=culjic29rmhu4jj9ic77hghsnt
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Host: 192.168.31.60:8099
Date: Fri, 08 Apr 2022 08:57:16 GMT
Connection: close
Content-Type: text/plain; charset=UTF-8
Content-Length: 28

ZW1sd0lHdGxlU0JwY3lCd1lYTno=
```

Base64 解密



```
ZW1sd0lHdGxlU0JwY3lCd1lYTno=
```

加密： ○ Unicode编码(\u开头) ○ URL编码(%开头) ○ UTF16编码(\x开头) ○ Base64编码 ○

解密： ○ Unicode解码(\u开头) ○ URL解码(%开头) ○ UTF16解码(\x开头) ● Base64解码 ○

当前数据解析结果如下：

```
emlwIGtleSBpcyBwYXNz
```

得到 flag

flag{emlwIGtleSBpcyBwYXNz}