

# Buuctf 流量中的线索

原创

Dexret 于 2021-11-18 21:15:13 发布 1231 收藏

分类专栏: [Buuctf Misc](#) 文章标签: [安全](#) [加密解密](#) [wireshark](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Dexret/article/details/121410279>

版权



[Buuctf Misc](#) 专栏收录该内容

47 篇文章 0 订阅

订阅专栏

下载该文件, 发现该文件为一个wireshark流量包文件

用wireshark打开该文件

流量中的线索.pcapng - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
5	0.41913300	172.16.80.5	172.16.66.100	TCP	http > ecsqdmn [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 ws=9 SACK_PERM=1
6	0.41919700	172.16.66.100	172.16.80.5	TCP	ecsqdmn > http [ACK] Seq=1 Ack=1 win=65700 Len=0
7	0.42036300	172.16.66.100	172.16.80.5	HTTP	GET /sdk/vmservice?wsd HTTP/1.1
8	0.42076600	172.16.80.5	172.16.66.100	HTTP	HTTP/1.1 301 Moved Permanently (text/html)
9	0.42076600	172.16.80.5	172.16.66.100	TCP	http > ecsqdmn [FIN, ACK] Seq=243 Ack=76 win=65536 Len=0
10	0.42083800	172.16.66.100	172.16.80.5	TCP	ecsqdmn > http [ACK] Seq=76 Ack=243 win=65456 Len=0
11	0.42164200	172.16.66.100	172.16.80.5	TCP	ecsqdmn > http [RST, ACK] Seq=76 Ack=244 win=0 Len=0
12	0.66732400	172.16.66.100	108.61.161.195	HTTP	Continuation or non-HTTP traffic
13	0.70636900	172.16.66.100	192.168.199.1	DNS	Standard query PTR 100.66.16.172.in-addr.arpa
14	0.71206900	172.16.66.100	192.168.199.1	DNS	Standard query PTR 27.210.239.115.in-addr.arpa
15	0.71778900	172.16.66.100	192.168.199.1	DNS	Standard query PTR 51.93.112.114.in-addr.arpa
16	0.72374600	172.16.66.100	192.168.199.1	DNS	Standard query PTR 5.80.16.172.in-addr.arpa
17	1.12600500	172.16.66.100	192.168.199.1	DNS	Standard query PTR 195.161.61.108.in-addr.arpa
18	1.13173800	172.16.66.100	192.168.199.1	DNS	Standard query PTR 1.199.168.192.in-addr.arpa
19	2.10839300	172.16.66.100	108.61.161.195	HTTP	Continuation or non-HTTP traffic
20	2.21035100	108.61.161.195	172.16.66.100	TCP	http > canocentral10 [ACK] Seq=1 Ack=2 win=307 Len=0 SLE=1 SRE=2
21	2.29232200	172.16.66.100	114.114.114.114	DNS	Standard query A teredo.ipv6.microsoft.com
22	2.63591100	114.114.114.114	172.16.66.100	DNS	Standard query response, No such name CNAME teredo.ipv6.microsoft.com.nsatt.net
23	3.05074600	172.16.66.90	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
24	3.19282600	172.16.66.100	192.168.199.1	DNS	Standard query PTR 114.114.114.114.in-addr.arpa
25	3.25845700	115.239.210.27	172.16.66.100	TLSv1.2	Alert (Level: warning, Description: Bad Certificate Status Response)
26	3.25845700	115.239.210.27	172.16.66.100	TCP	https > swrmi [FIN, ACK] Seq=32 Ack=1 win=248 Len=0
27	3.25862800	172.16.66.100	115.239.210.27	TCP	swrmi > https [ACK] Seq=1 Ack=33 win=16341 Len=0
28	3.84152200	172.16.66.100	192.168.199.1	DNS	Standard query PTR 90.66.16.172.in-addr.arpa
29	3.84710300	172.16.66.100	192.168.199.1	DNS	Standard query PTR 250.255.255.239.in-addr.arpa
30	3.84728300	172.16.66.100	114.114.114.114	DNS	Standard query PTR 100.66.16.172.in-addr.arpa
31	3.85947700	114.114.114.114	172.16.66.100	DNS	Standard query response, No such name
32	4.27022400	172.16.66.100	114.114.114.114	DNS	Standard query PTR 195.161.61.108.in-addr.arpa
33	4.47929300	172.16.66.100	114.114.114.114	DNS	Standard query PTR 27.210.239.115.in-addr.arpa
34	4.48729700	114.114.114.114	172.16.66.100	DNS	Standard query response, No such name
35	4.65242900	115.239.211.112	172.16.66.100	TLSv1.2	Encrypted Alert
36	4.65243000	115.239.211.112	172.16.66.100	TCP	https > transact [FIN, ACK] Seq=32 Ack=1 win=221 Len=0

Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)

Ethernet II, Src: 20:89:84:32:73:c5 (20:89:84:32:73:c5), Dst: 0c:da:41:9e:cc:85 (0c:da:41:9e:cc:85)

**Internet Protocol, Src: 172.16.66.100 (172.16.66.100), Dst: 115.239.210.27 (115.239.210.27)**

Transmission Control Protocol, Src Port: Fiorano-rtrsvc (1855), Dst Port: https (443), Seq: 1, Ack: 1, Len: 1

Secure Socket Layer

```
0000 0c da 41 9e cc 85 20 89 84 32 73 c5 08 00 45 00  ..A... .2s...E.
0010 00 29 45 b9 40 00 40 06 00 00 ac 10 42 64 73 ef  .)E.@.@. ....Bds.
0020 d2 1b 07 3f 01 bb 29 8b b1 41 a1 3c 03 6c 50 10  ...?..). .A.<.TP.
0030 40 b0 34 9b 00 00 00  ..4....
```

File: "C:\Users\13631\Desktop\流量中的... Packets: 212 Displayed: 212 Marked: 0 Load time: 0:00.099 Profiler: Default CSDN @Dexret

## 发现好多tcp和http的数据包，过滤该数据包

Wireshark interface showing a list of network packets. The filter is set to 'http'. The selected packet (No. 142) is highlighted in blue. The packet details pane shows the following information:

- Frame 142: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits)
- Ethernet II, Src: Oc:da:41:9e:cc:85 (Oc:da:41:9e:cc:85), Dst: 20:89:84:32:73:c5 (20:89:84:32:73:c5)
- Internet Protocol, Src: 172.16.80.120 (172.16.80.120), Dst: 172.16.66.100 (172.16.66.100)
- Transmission Control Protocol, Src Port: http (80), Dst Port: ibm-mqisd (1883), Seq: 86141, Ack: 386, Len: 390
- [Reassembled TCP Segments (86530 bytes): #62(1460), #64(1460), #66(1460), #67(1460), #69(1460), #70(1460), #71(1460), #73(1460), #74(1460), #75(1460), #77(1460), #78(1460), #79(1460), #81
- Hypertext Transfer Protocol

Packet bytes: 0000 20 89 84 32 73 c5 0c da 41 9e cc 85 08 00 45 00 ..2s... A....E.  
0010 01 ae 9c 6f 40 00 3f 06 b2 dd ac 10 50 78 ac 10 ...o8.?. ...PX..  
0020 42 64 00 50 07 5b 21 e6 53 28 c1 88 88 08 50 19 Bd.P.[!. S(...P.

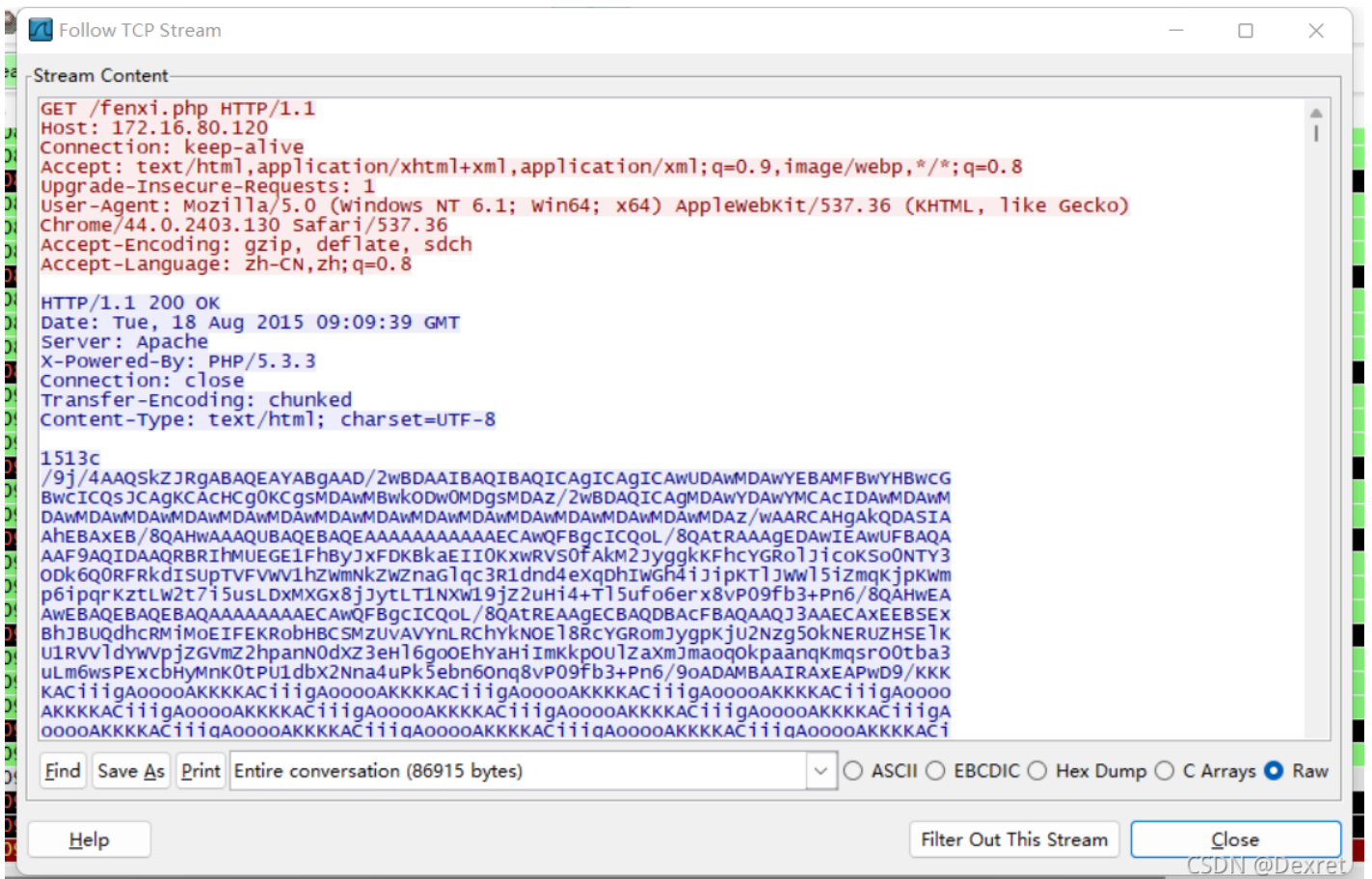
## 选择一条http的数据包，右键选择数据流追踪

Wireshark interface showing the same list of network packets. A right-click context menu is open over the selected packet (No. 142). The 'Follow TCP Stream' option is highlighted with a red box. The menu options are:

- Mark Packet (toggle)
- Ignore Packet (toggle)
- Set Time Reference (toggle)
- Manually Resolve Address
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SLIP
- Follow TCP Stream**
- Follow UDP Stream
- Follow SSL Stream
- Copy
- Decode As...
- Print...
- Show Packet in New Window

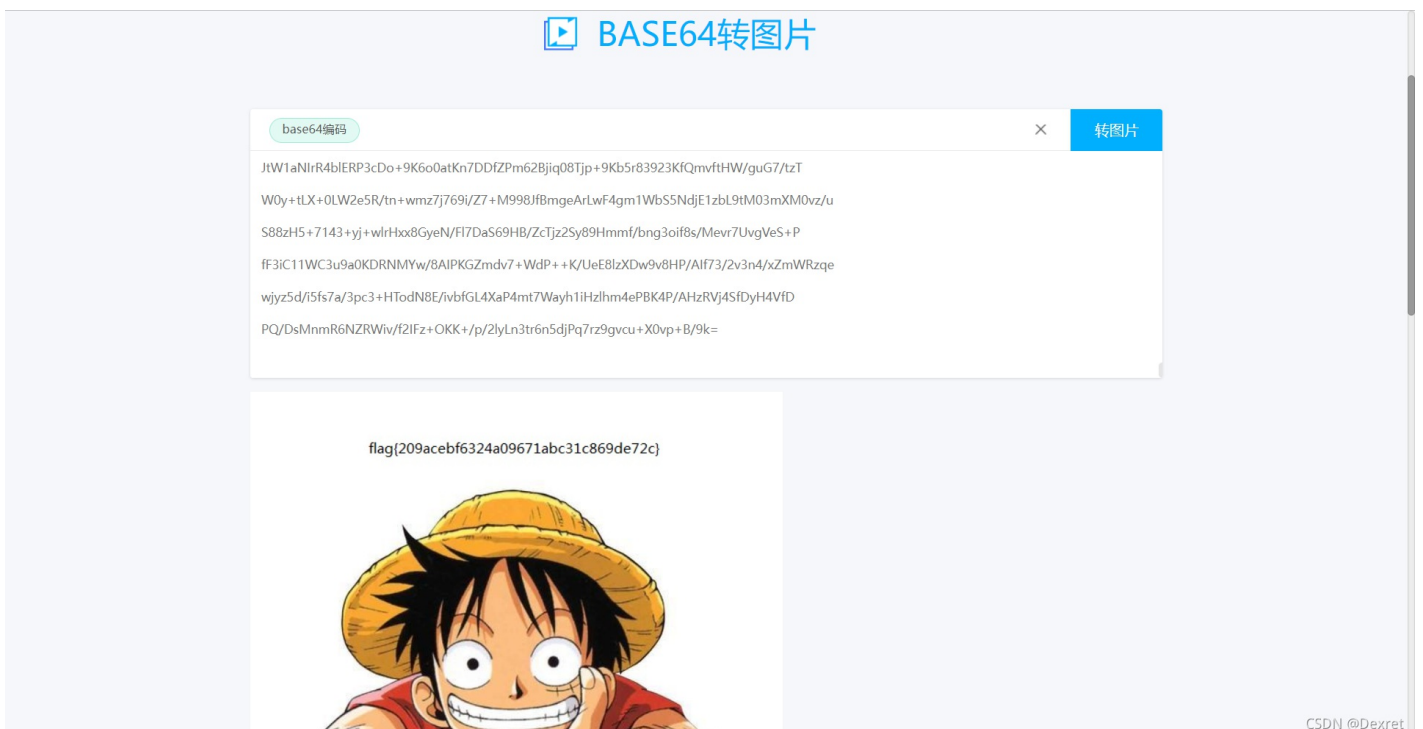
Packet bytes: 0000 20 89 84 32 73 c5 0c da 41 9e cc 85 08 00 45 00 ..2s... A....E.  
0010 01 ae 9c 6f 40 00 3f 06 b2 dd ac 10 50 78 ac 10 ...o8.?. ...PX..  
0020 42 64 00 50 07 5b 21 e6 53 28 c1 88 88 08 50 19 Bd.P.[!. S(...P.

## 发现有一段很长的代码，这段代码很像base64加密



在网上找一个base64解码工具

BASE64转图片 - 站长工具 - 极速数据 (jisuapi.com) <https://tool.jisuapi.com/base642pic.html> 解码该段代码后发现是一张图片，且该题flag就在图片上



该题的flag为

flag{209acebf6324a09671abc31c869de72c}