

# xctf攻防世界 MISC高手进阶区 flag\_universe

原创

18947943 于 2022-01-17 20:26:10 发布 5579 收藏 1

分类专栏: [攻防世界misc之路](#) 文章标签: [misc](#)

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/18947943/article/details/122547543>

版权



[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

## 1. 进入环境, 下载附件

下载后, 给的是pcapng文件, 果断使用wireshark打开, 在其中搜索关键词flag, 发现如下:

The screenshot shows the Wireshark interface with a search filter 'flag' applied to the 'tcp.stream eq 16' filter. The search results table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
733	71.143255571	172.17.0.1	172.17.0.2	TCP	74	53670 → 21109 [SYN] Seq=0 Win=29
735	71.143282651	172.17.0.2	172.17.0.1	TCP	74	21109 → 53670 [SYN, ACK] Seq=0 A
737	71.143307471	172.17.0.1	172.17.0.2	TCP	66	53670 → 21109 [ACK] Seq=1 Ack=1
744	71.144071889	172.17.0.2	172.17.0.1	FTP-DA...	395	FTP Data: 329 bytes (PASV) (LIST
745	71.144094629	172.17.0.1	172.17.0.2	TCP	66	53670 → 21109 [ACK] Seq=1 Ack=33
746	71.144129589	172.17.0.2	172.17.0.1	TCP	66	21109 → 53670 [FIN, ACK] Seq=330

The packet details pane shows the following text:

```
[Command: LIST -a]
[Command frame: 739]
[Current working directory: /]
Line-based text data (5 lines)
drwxrwxrwx 1 ftp ftp 384 Sep 19 07:55 .\r\n
drwxrwxrwx 1 ftp ftp 384 Sep 19 07:55 ..\r\n
-rwxrwxrwx 1 ftp ftp 41 Sep 19 07:52 flag.txt\r\n
-rwxrwxrwx 1 ftp ftp 1178630 Sep 19 07:55 new_universe.png\r\n
```

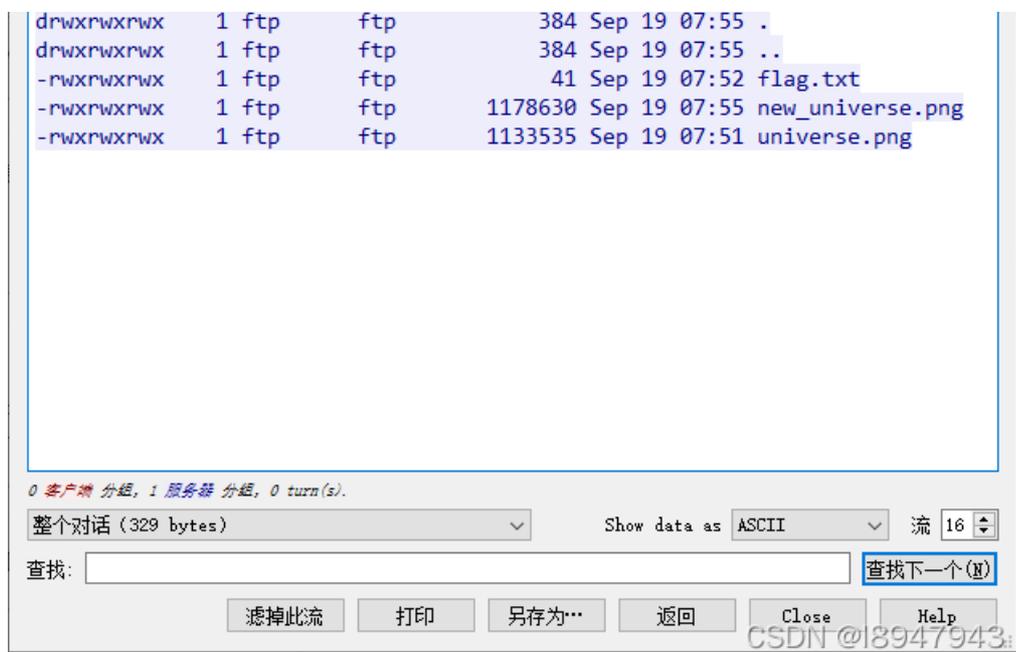
The packet bytes pane shows the following hex and ASCII data:

```
00b0 37 3a 35 35 20 2e 2e 0d 0a 2d 72 77 78 72 77 78 7:55 ... -rwxrwx
00c0 72 77 78 20 20 20 20 31 20 66 74 70 20 20 20 20 rwx 1 ftp
00d0 20 20 66 74 70 20 20 20 20 20 20 20 20 20 20 20 ftp
00e0 20 34 31 20 53 65 70 20 31 39 20 30 37 3a 35 32 41 Sep 19 07:52
00f0 20 66 6c 61 67 2e 74 78 74 0d 0a 2d 72 77 78 72 flag.txt -rwxr
0100 77 78 72 77 78 20 20 20 20 20 31 20 66 74 70 20 20 wxrwx 1 ftp
0110 20 20 20 20 66 74 70 20 20 20 20 20 20 20 20 20 ftp 11
0120 37 38 36 33 30 20 53 65 70 20 31 39 20 30 37 3a 78630 Se p 19 07:
0130 35 35 20 6e 65 77 5f 75 6e 69 76 65 72 73 65 2e 55 new_u niverse.
0140 70 6e 67 0d 0a 2d 72 77 78 72 77 78 72 77 78 20 png: -rw xrwxrwx
0150 20 20 20 31 20 66 74 70 20 20 20 20 20 20 66 74 1 ftp ft
0160 70 20 20 20 20 20 20 20 31 31 33 33 35 33 35 20 p 1133535
```

## 2. 问题分析

追踪流

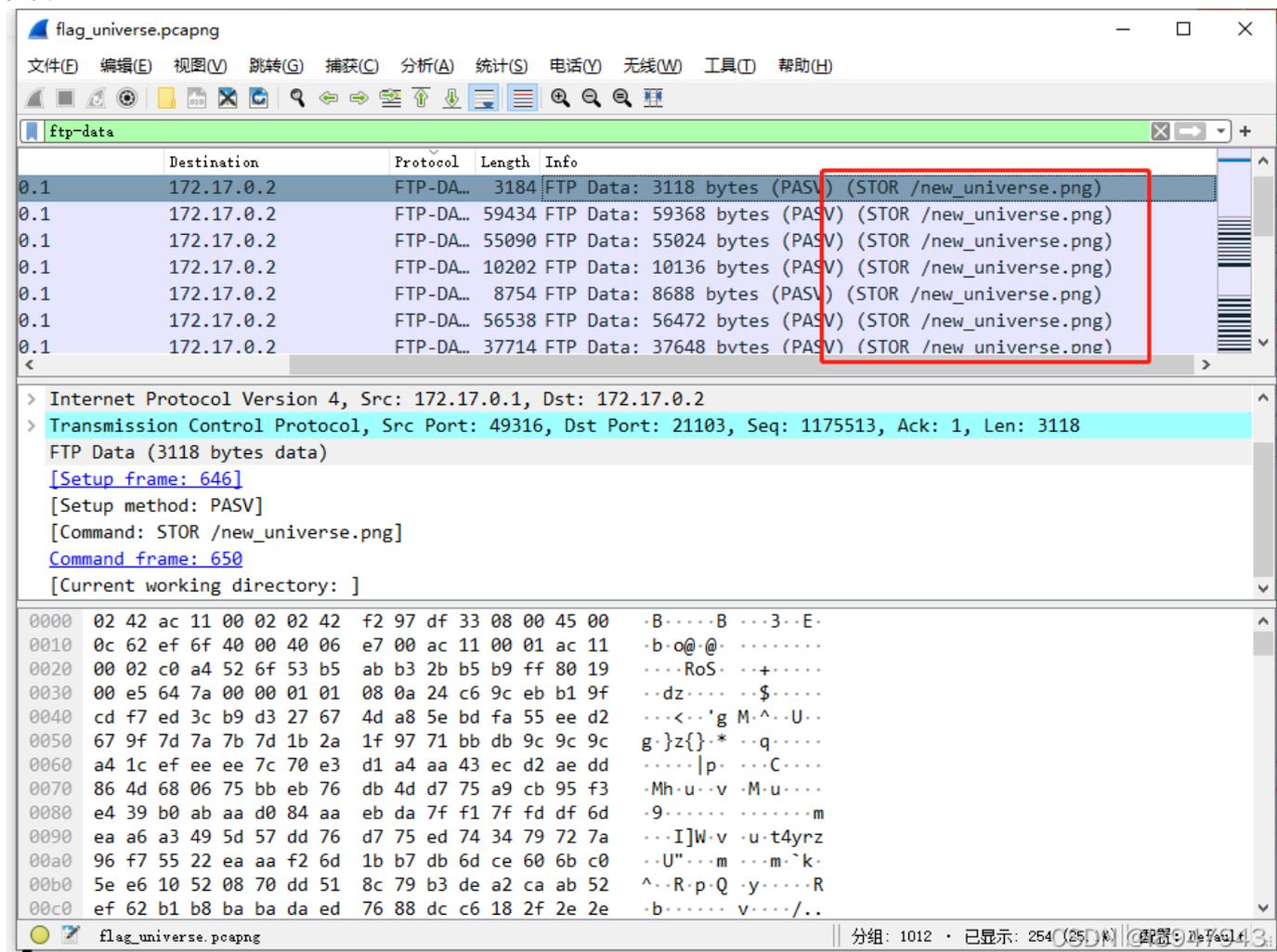




可以看到，采用的ftp协议，对文件flag.txt、new\_uniberse.png和universe.png文件进行了上传，因此，解题关键是把上传的图片给还原出来。

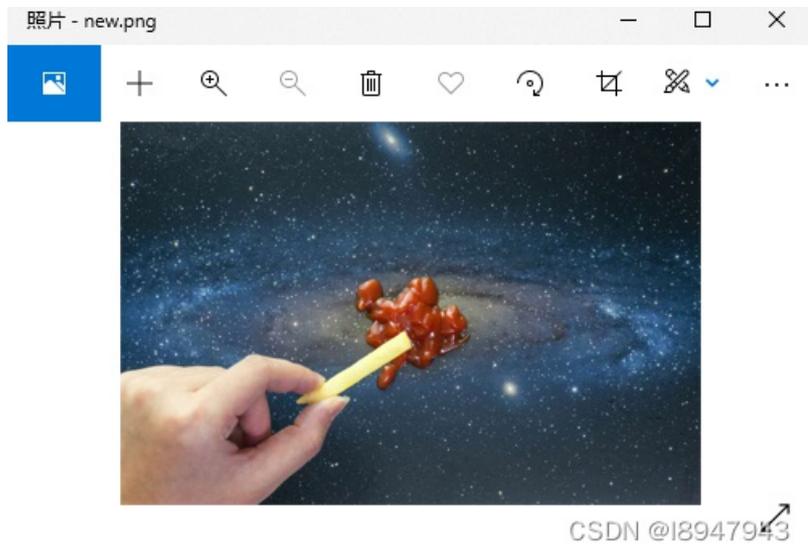
### 找到new\_uniberse.png

如图：



把找到的上传图片追踪流导出来，在这里推荐使用工具用NetworkMiner打开流量包，他妈的电脑安装后缺少什么dll文件，人麻了，手工导出吧。

追踪流，复制原始数据，到winhex中建立10MB的文件并粘贴进去，最终以为png文件命名。如图：



### 使用zstag隐写发现

先安装工具，参考博客：<https://www.cnblogs.com/lzkalisw/p/12831430.html>

使用命令进行分离，如图：

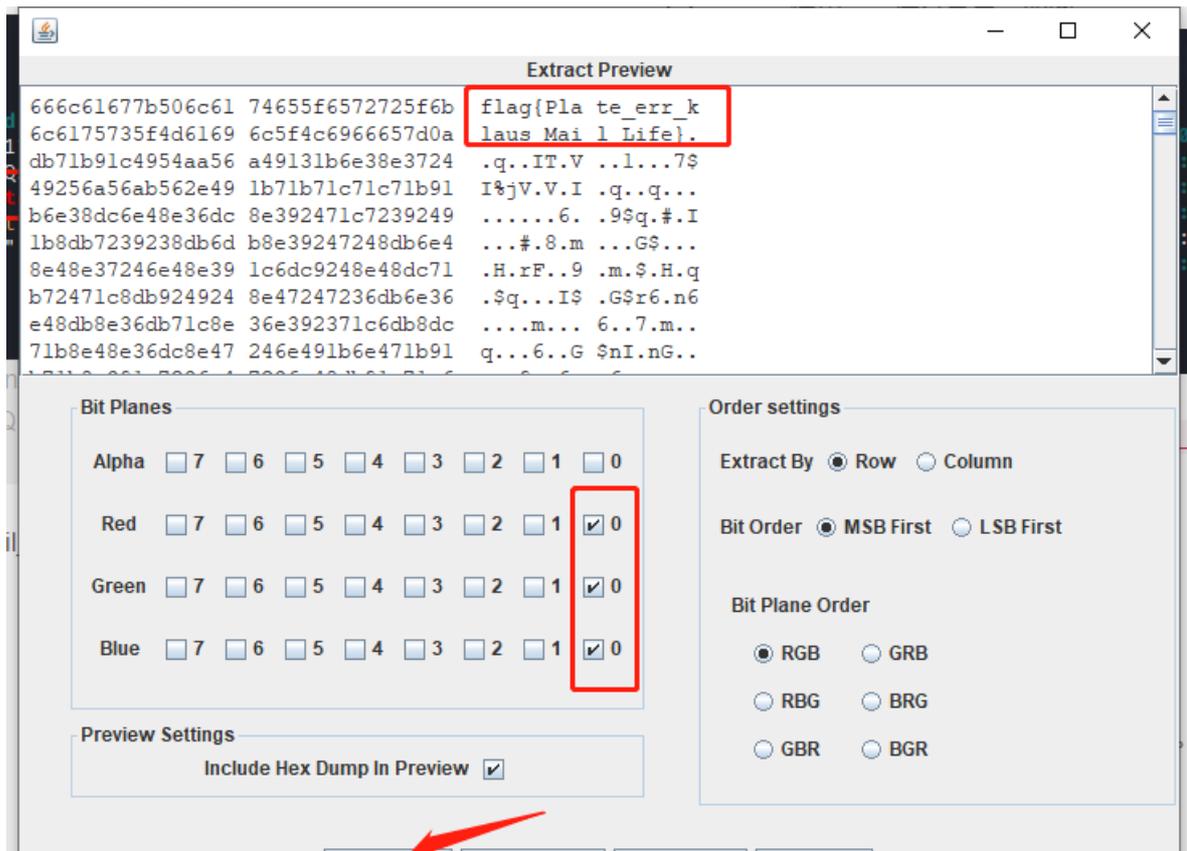
```
(zhangfa@kali)-[~/下载]
└─$ zsteg new.png
[?] 10485760 bytes of extra data after image end (IEND), offset = 0x11fc06
extradata:0 .. ["\x00" repeated 10485760 times]
imagedata .. text: "\n\n\n111???"
b1,r,lsb,xy .. text: "F28xrg.9Qz"
b1,rgb,lsb,xy .. text: "flag{Plate_err_klaus_Mail_Life}\n"
b3,g,msb,xy .. file: PGP Secret Sub-key -
b3,b,msb,xy .. text: "zC`)XUWS"

(zhangfa@kali)-[~/下载]
└─$
```

得到最终的答案：`flag{Plate_err_klaus_Mail_Life}`

### StegSolve发现隐写

如图，该工具也可以找到隐写：



### 3. 总结

- 隐写工具使用（第一次接触zstag。。。）
- 追踪流并得到传输文件

这个题学到东西了，欢迎交流~~~