攻防世界MISC进阶区wireshark

原创

just a leaf 于 2021-12-02 08:48:20 发布 350 收藏 1
分类专栏： ctf 文章标签： vm 网络 wireshark

前言：则是一道流量分析题使用到Wireshark等一系列工具

wireshark：

https://www.wireshark.org/

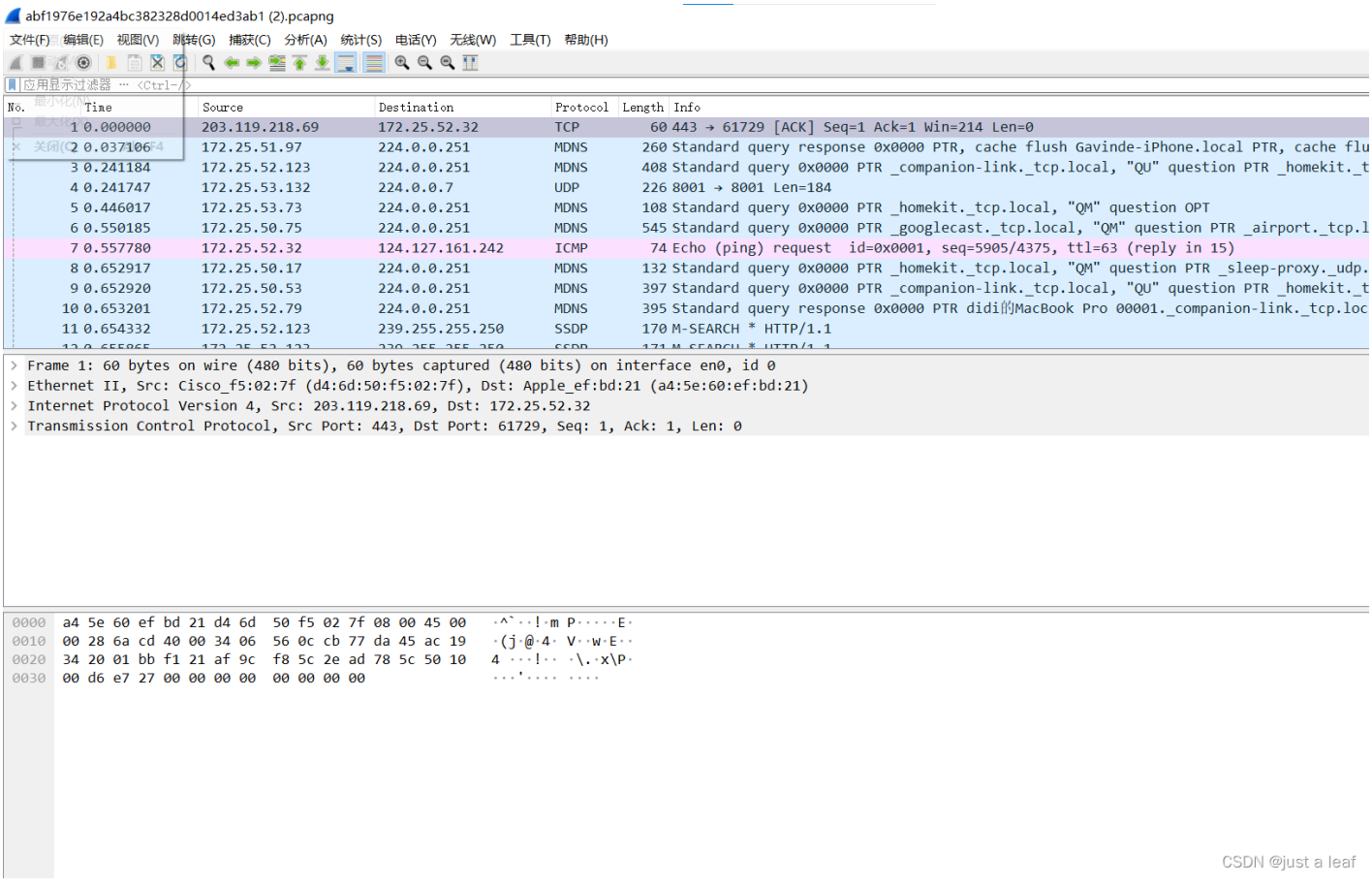
hex-editor

Free Hex Editor: Fastest Binary File Editing Software. Freeware. Windows (hhdsoftware.com)

wp：

1.打开wireshark

下载附件打开

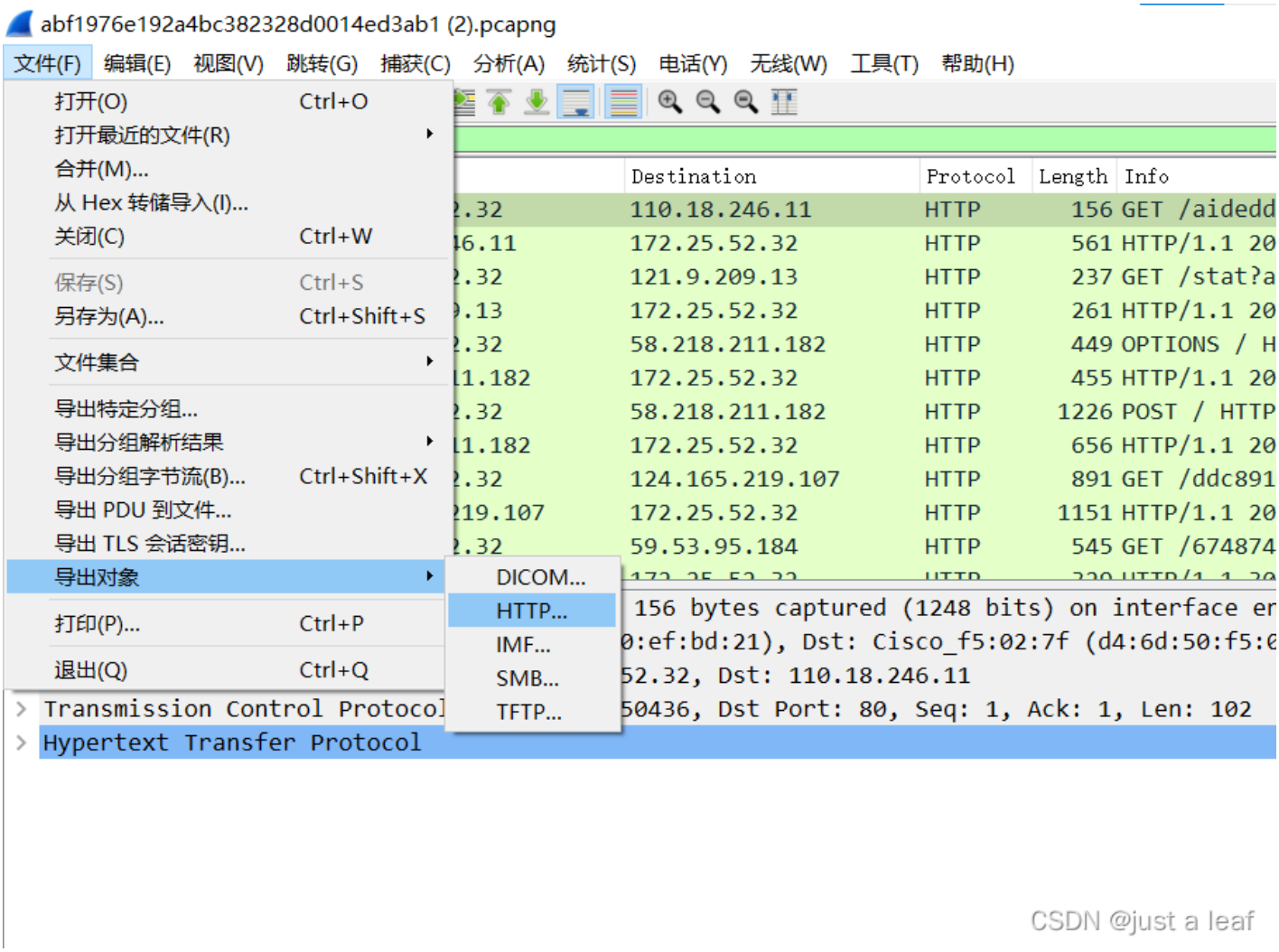


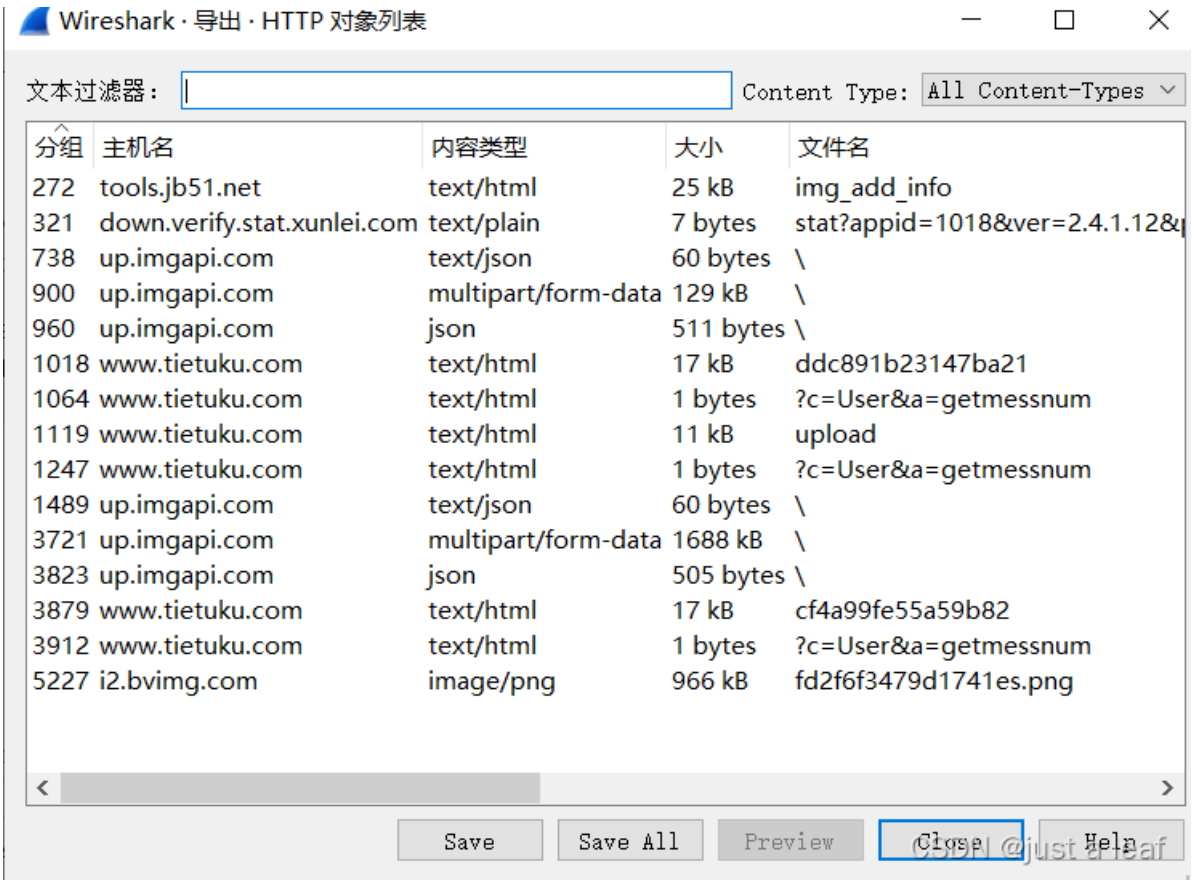
导出HTTP

2.一般信息大多是藏在url，html，图片当中的

对http进行追踪在第一条的请求中存在网页的请求：http://tools.jb51.net/aideddesign/img_add_info

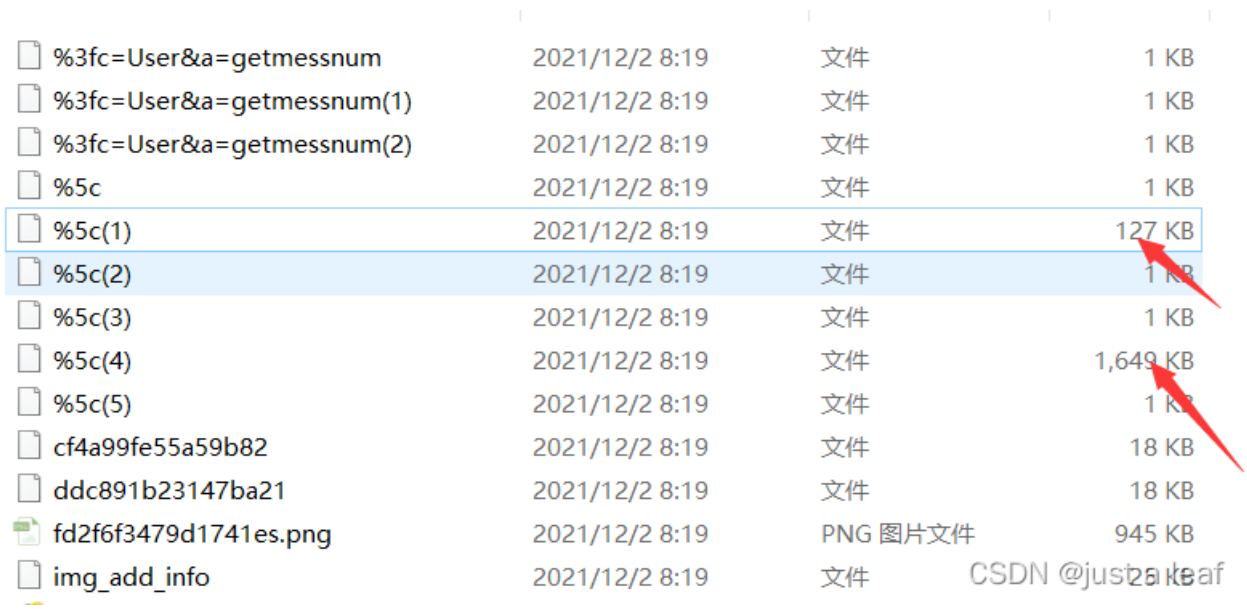
3.





一般这种题型的解题方向都在html，png,url中

省去选择的步骤直接全部恢复



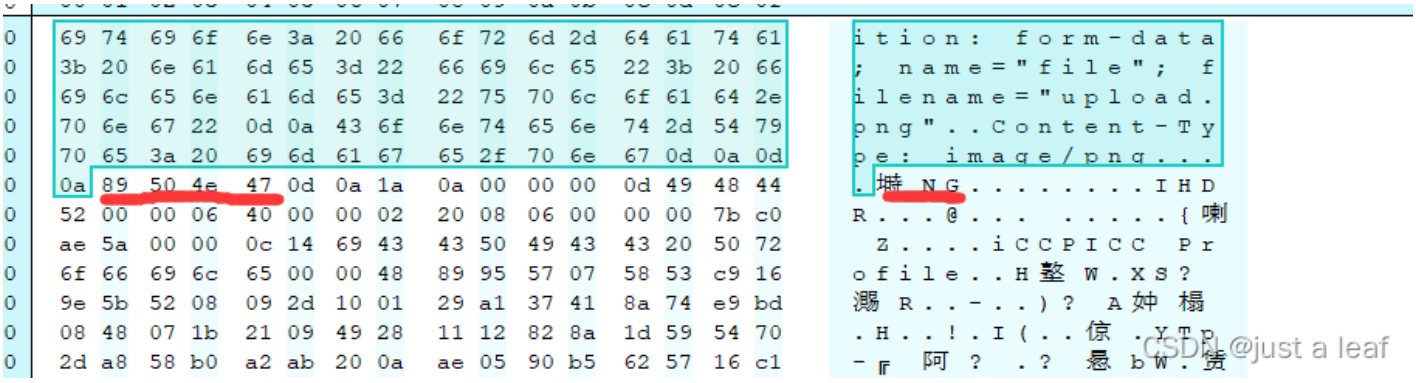
发现有一个风景照的png 和俩个较大的文件

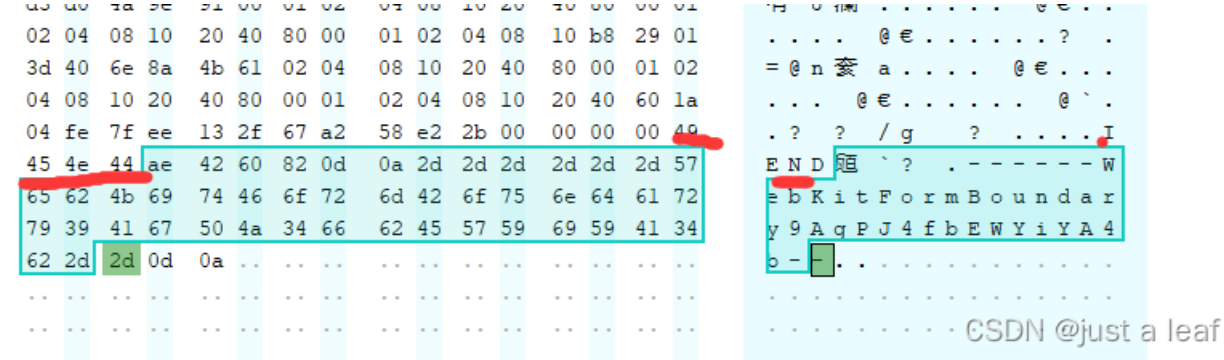
结合上述个给出的一个图像解密网址，将俩个较大文件尝试放入hex editor中删除多余的数据尝试将其也变为图片

（这时就需要了解一个知识

PNG图片固定以 89 50 4E 47 0D 0A 1A 0A（4个字节）开头

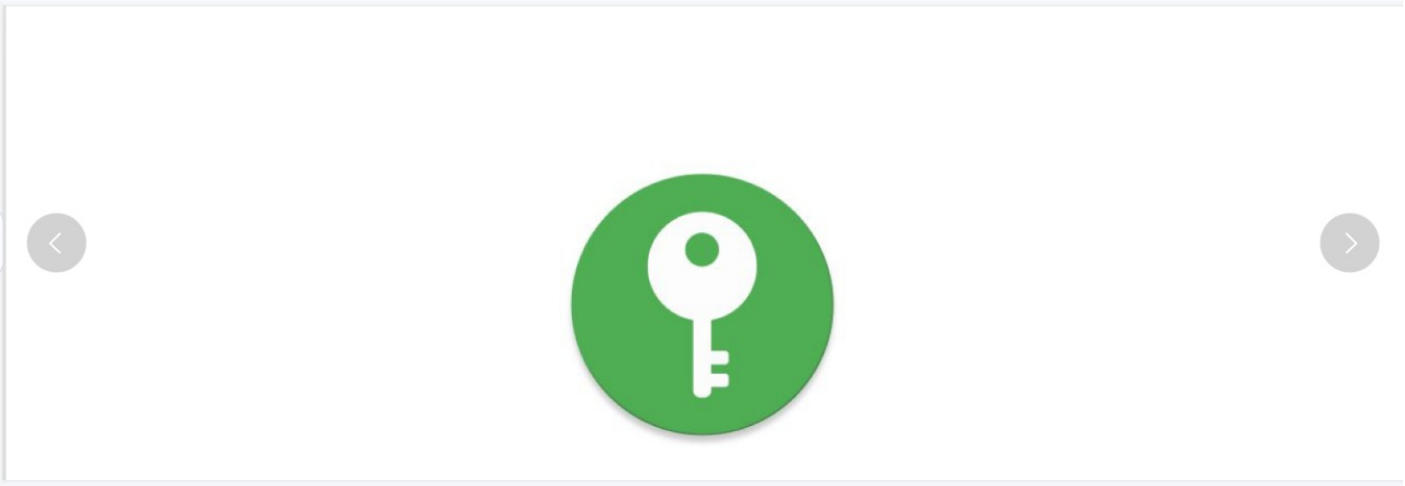
49 45 4E 44--IEND结尾）





4.删除多余数据后

改其后缀名为.png查看图片内容俩个较大数据包就会得到下面俩张图片



查看给出的解密网站发现解密时还会需要一个密码所以考虑从带key的照片入手再把其拖入hex editor

```
0 00 02 20  08 06 00 00  00 7b c0
4 69 43 43  50 49 43 43  20 50 72
0 00 48 89  95 57 07 58  53 c9 16
d 10 01 29  a1 37 41 8a  74 e9 bc
```

发现高度偏低对其进行更改

```
0d 0a 1a 0a   00 00 00 0
00 00 04 20   08 06 00 0
14 69 43 43   50 49 43 4
00 00 48 89   95 57 07 5
```

保存再次查看图片

key:57pmYyWt

出现了key

这是就返回所给出的解密网站将风景照作为解密图片上传，密码为所给出的key进行解密

1. 从电脑中选择一张带有隐藏信息的图片： 选择文件 %5c(4).png

2. 输入需要解开信息的密码（如果没有密码可以不填）： ••••••••

解密出隐藏的信息

图片中隐藏的信息为：flag+AHs-
44444354467B5145576F6B63704865556F32574F6642494E37706F6749577346303469526A747D+AH0-

看到所给出的信息包含0、1、2、3、4、5、6、7、8、9、A、B、C、D、E、F所以判断可能是base16，上网寻找在线翻译工具进行解密

44444354467B5145576F6B63704865556F32574F6642494E37706F6749577346303469526A747D

编码 解码 清空

DDCTF{QEWokcpHeUo2WOfBIN7pogIWsF04iRjt}

进而就得到了flag