

# 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](#)

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/xiao\\_he0123/article/details/121660357](https://blog.csdn.net/xiao_he0123/article/details/121660357)

版权



[ctf](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

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

abf1976e192a4bc382328d0014ed3ab1 (2).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)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	203.119.218.69	172.25.52.32	TCP	60	443 → 61729 [ACK] Seq=1 Ack=1 Win=214 Len=0
2	0.03710664	172.25.51.97	224.0.0.251	MDNS	260	Standard query response 0x0000 PTR, cache flush Gavinde-iPhone.local PTR, cache flu
3	0.241184	172.25.52.123	224.0.0.251	MDNS	408	Standard query 0x0000 PTR_companion-link_tcp.local, "QU" question PTR_homekit_t
4	0.241747	172.25.53.132	224.0.0.7	UDP	226	8001 → 8001 Len=184
5	0.446017	172.25.53.73	224.0.0.251	MDNS	108	Standard query 0x0000 PTR_homekit_tcp.local, "QM" question OPT
6	0.550185	172.25.50.75	224.0.0.251	MDNS	545	Standard query 0x0000 PTR_googlecast_tcp.local, "QM" question PTR_airport_tcp.l
7	0.557780	172.25.52.32	124.127.161.242	ICMP	74	Echo (ping) request id=0x0001, seq=5905/4375, ttl=63 (reply in 15)
8	0.652917	172.25.50.17	224.0.0.251	MDNS	132	Standard query 0x0000 PTR_homekit_tcp.local, "QM" question PTR_sleep-proxy_udp.
9	0.652920	172.25.50.53	224.0.0.251	MDNS	397	Standard query 0x0000 PTR_companion-link_tcp.local, "QU" question PTR_homekit_t
10	0.653201	172.25.52.79	224.0.0.251	MDNS	395	Standard query response 0x0000 PTR_didi的MacBook Pro_00001_companion-link_tcp.loc
11	0.654332	172.25.52.123	239.255.255.250	SSDP	170	M-SEARCH * HTTP/1.1
12	0.655055	172.25.52.123	239.255.255.250	SSDP	171	M-SEARCH * HTTP/1.1

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en0, id 0  
> Ethernet II, Src: Cisco\_f5:02:7f (d4:6d:50:f5:02:7f), Dst: Apple\_ef:bd:21 (a4:5e:60:ef:bd:21)  
> Internet Protocol Version 4, Src: 203.119.218.69, Dst: 172.25.52.32  
> Transmission Control Protocol, Src Port: 443, Dst Port: 61729, Seq: 1, Ack: 1, Len: 0

```
0000  a4 5e 60 ef bd 21 d4 6d 50 f5 02 7f 08 00 45 00  .^...!m P.....E.
0010  00 28 6a cd 40 00 34 06 56 0c cb 77 da 45 ac 19  .(j@.4.V.w.E...
0020  34 20 01 bb f1 21 af 9c f8 5c 2e ad 78 5c 50 10  4 ...!... \.x\P.
0030  00 d6 e7 27 00 00 00 00 00 00 00 00 00 00 00  .....

```

CSDN @just a leaf

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.

abf1976e192a4bc382328d0014ed3ab1 (2).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)

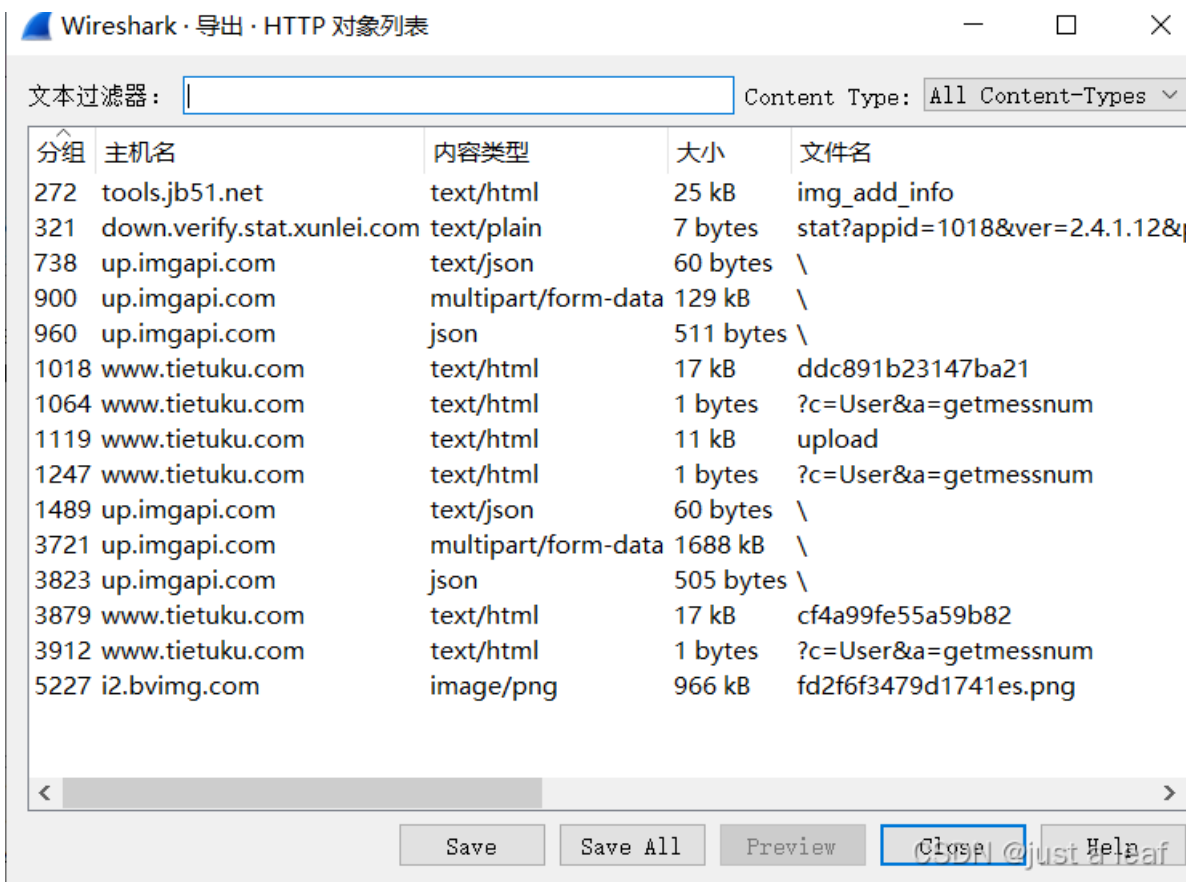
	Destination	Protocol	Length	Info
2.32	110.18.246.11	HTTP	156	GET /aidedd
16.11	172.25.52.32	HTTP	561	HTTP/1.1 20
2.32	121.9.209.13	HTTP	237	GET /stat?a
9.13	172.25.52.32	HTTP	261	HTTP/1.1 20
2.32	58.218.211.182	HTTP	449	OPTIONS / H
1.182	172.25.52.32	HTTP	455	HTTP/1.1 20
2.32	58.218.211.182	HTTP	1226	POST / HTTP
1.182	172.25.52.32	HTTP	656	HTTP/1.1 20
2.32	124.165.219.107	HTTP	891	GET /ddc891
19.107	172.25.52.32	HTTP	1151	HTTP/1.1 20
2.32	59.53.95.184	HTTP	545	GET /674874
	172.25.52.32	HTTP	220	HTTP/1.1 20

导出对象

- DICOM...
- HTTP... 156 bytes captured (1248 bits) on interface er
- IMF... 0:ef:bd:21), Dst: Cisco\_f5:02:7f (d4:6d:50:f5:c
- SMB... 52.32, Dst: 110.18.246.11
- TFTP... 50436, Dst Port: 80, Seq: 1, Ack: 1, Len: 102

> Transmission Control Protocol

> Hypertext Transfer Protocol



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

📄 %3f=User&a=getmessnum	2021/12/2 8:19	文件	1 KB
📄 %3f=User&a=getmessnum(1)	2021/12/2 8:19	文件	1 KB
📄 %3f=User&a=getmessnum(2)	2021/12/2 8:19	文件	1 KB
📄 %5c	2021/12/2 8:19	文件	1 KB
📄 %5c(1)	2021/12/2 8:19	文件	127 KB
📄 %5c(2)	2021/12/2 8:19	文件	1 KB
📄 %5c(3)	2021/12/2 8:19	文件	1 KB
📄 %5c(4)	2021/12/2 8:19	文件	1,649 KB
📄 %5c(5)	2021/12/2 8:19	文件	1 KB
📄 cf4a99fe55a59b82	2021/12/2 8:19	文件	18 KB
📄 ddc891b23147ba21	2021/12/2 8:19	文件	18 KB
📄 fd2f6f3479d1741es.png	2021/12/2 8:19	PNG 图片文件	945 KB
📄 img_add_info	2021/12/2 8:19	文件	CSDN @justleaf

发现有一个风景照的png 和两个较大的文件



CSDN @just a leaf

结合上述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)

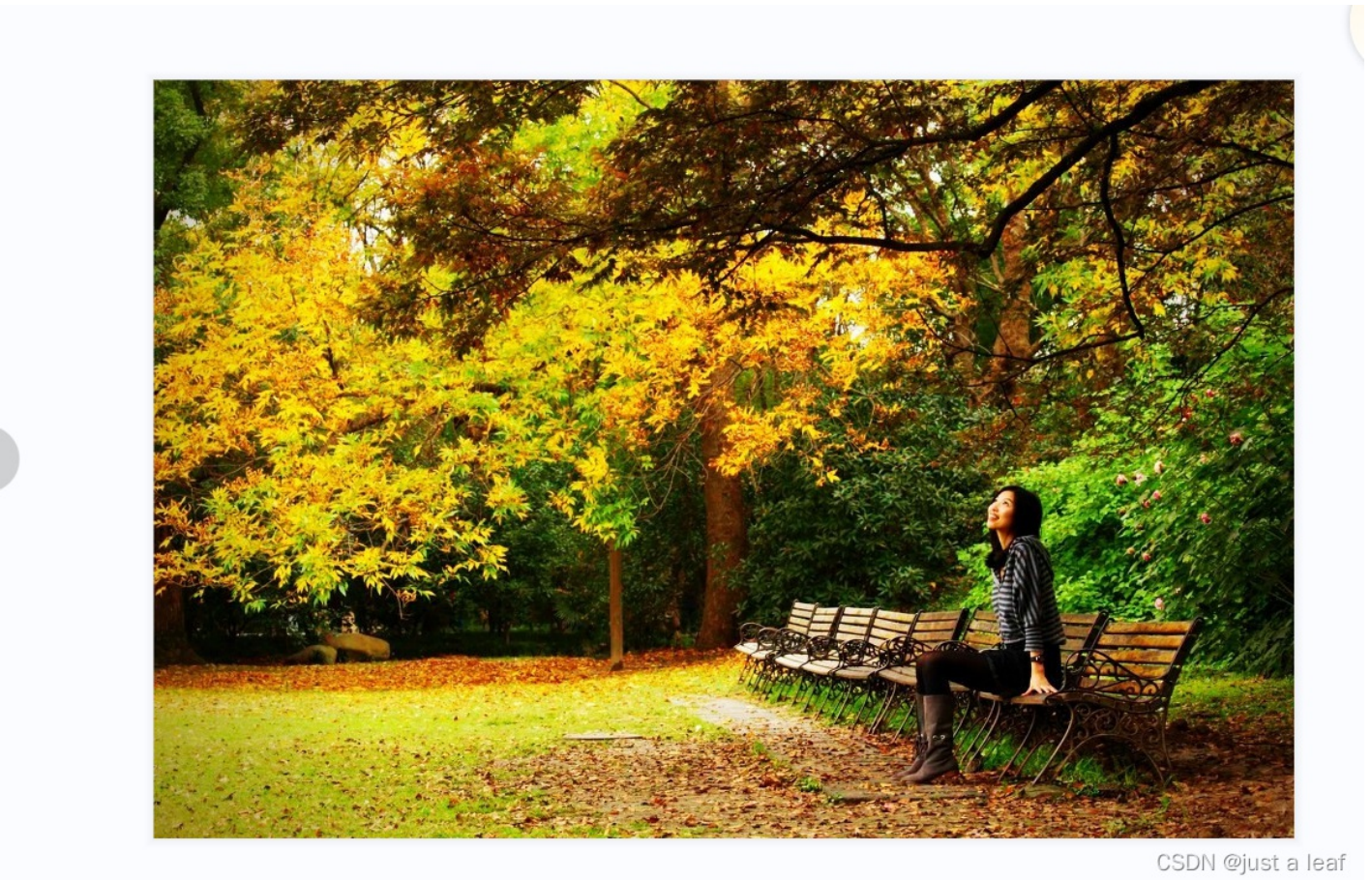
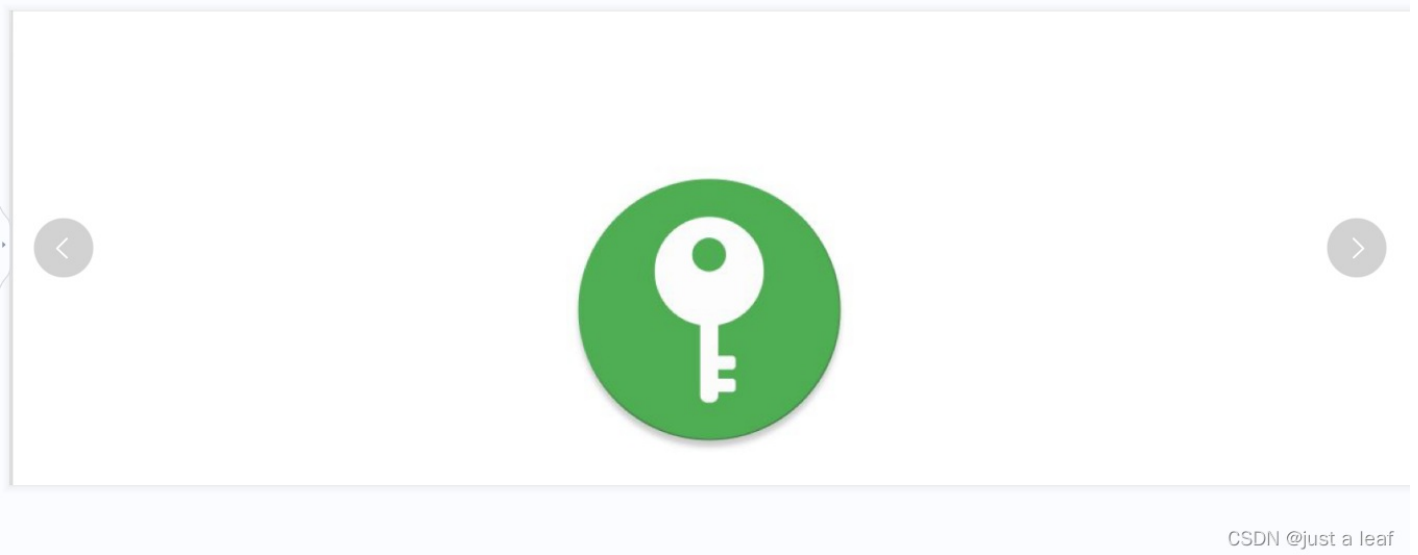
0	69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61	ition: form-data
0	3b 20 6e 61 6d 65 3d 22 66 69 6c 65 22 3b 20 66	; name="file"; f
0	69 6c 65 6e 61 6d 65 3d 22 75 70 6c 6f 61 64 2e	ilename="upload.
0	70 6e 67 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79	ong"..Content-Ty
0	70 65 3a 20 69 6d 61 67 65 2f 70 6e 67 0d 0a 0d	pe: image/png...
0	0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44	.PNG.....IHD
0	52 00 00 06 40 00 00 02 20 08 06 00 00 00 7b c0	R...@.....{喇
0	ae 5a 00 00 0c 14 69 43 43 50 49 43 43 20 50 72	Z....iCCPICC Pr
0	6f 66 69 6c 65 00 00 48 89 95 57 07 58 53 c9 16	ofile..H整 W.XS?
0	9e 5b 52 08 09 2d 10 01 29 a1 37 41 8a 74 e9 bd	溺 R..-..)? A 姊 榻
0	08 48 07 1b 21 09 49 28 11 12 82 8a 1d 59 54 70	.H...!.I(.. 惊 .YTp
0	2d a8 58 b0 a2 ab 20 0a ae 05 90 b5 62 57 16 c1	-F 阿? .? 悬 bW. 赞

02 04 08 10 20 40 80 00 01 02 04 08 10 b8 29 01	.....@e.....?
3d 40 6e 8a 4b 61 02 04 08 10 20 40 80 00 01 02	=@n 衰 a.....@e...
04 08 10 20 40 80 00 01 02 04 08 10 20 40 60 1a	.....@e.....@`
04 fe 7f ee 13 2f 67 a2 58 e2 2b 00 00 00 00 49	.? ? /g ? .....I
45 4e 44 ae 42 60 82 0d 0a 2d 2d 2d 2d 2d 57	END 随 `? .-----W
65 62 4b 69 74 46 6f 72 6d 42 6f 75 6e 64 61 72	ebKitFormBoundary
79 39 41 67 50 4a 34 66 62 45 57 59 69 59 41 34	y9AqPJ4fbEWYiYA4
62 2d 2d 0d 0a .. .. .. .. .. .. .. ..	o-.....

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的照片入手再将其拖入hex editor

```
u va 1a va 00 00 00 0a 75 70 75  
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 1e  
d 10 01 29 a1 37 41 8a 74 e9 bc  
c 10 00 11 10 00 00 11 50 51 75
```

发现高度偏低对其进行更改

```
0d 0a 1a 0a 00 00 00 c
00 00 04 20 08 06 00 c
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

CSDN @just a leaf

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:  %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-

CSDN @just a leaf

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

DDCTF{QEWokcpHeUo2WOfBIN7pogIWsf04iRjt}

CSDN @just a leaf

进而就得到了flag