BUUCTF [ACTF新生赛2020]swp

原创

F10NAF11pp3d 于 2020-09-24 19:18:27 发布 437 收藏

分类专栏： BUUCTF

本文链接：https://blog.csdn.net/m0_46481239/article/details/108765830

BUUCTF 专栏收录该内容

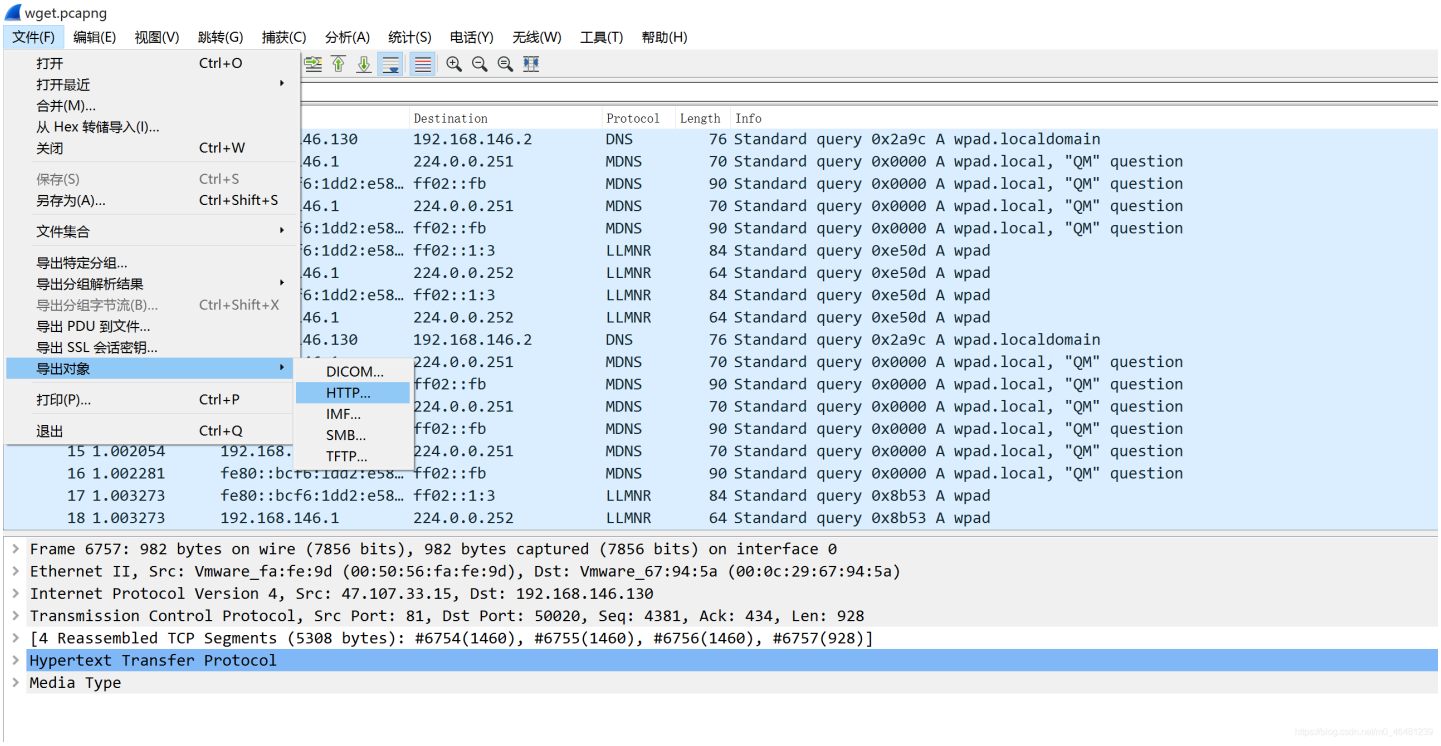
24 篇文章 1 订阅

订阅专栏

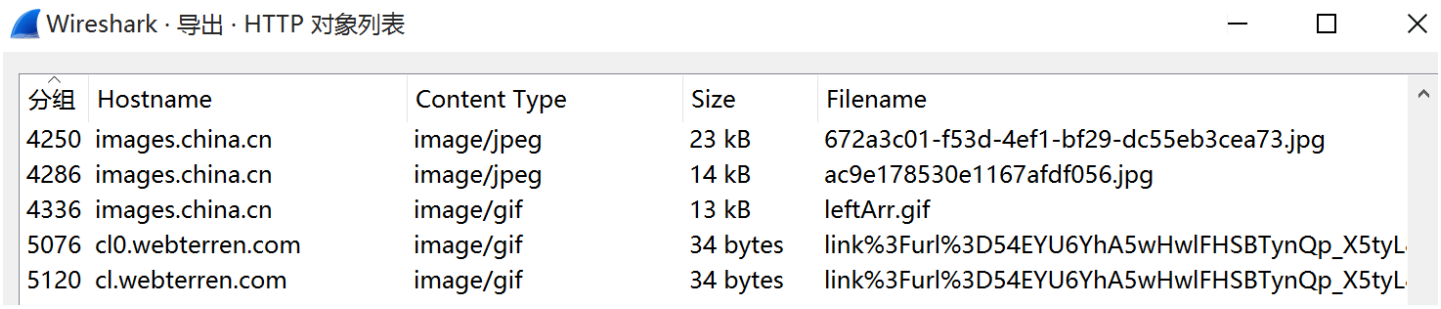
下载后解压得到一个wget.zip,再解压得到wget.pcapng

把数据包放入Wireshark里分析一下

猜测http数据传输，导入http对象



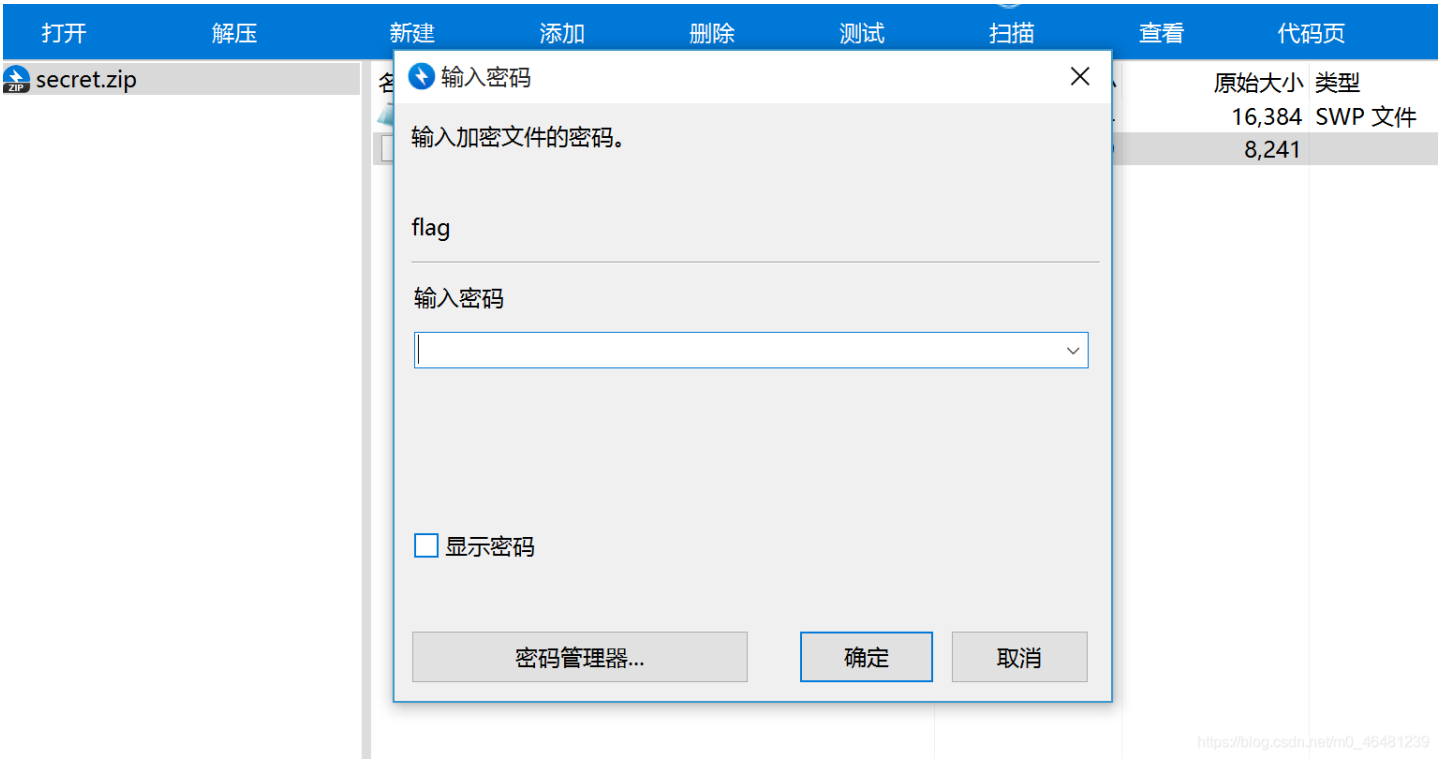
可以发现在导出的文件中发现secret.zip,保存下来



5126	images.china.cn	image/png	1152 kB	cbbebf0d-4317-4f81-a157-4947d838ce59.png
5153	tv.cctv.com	text/html	2762 bytes	index.shtml
5182	push.zhanzhang.baidu.com	text/javascript	281 bytes	push.js
5226	js.t.sinajs.cn	application/x-javascript	4312 bytes	bundle.js?version=20150130.02
5236	js.t.sinajs.cn	application/x-javascript	15 kB	client.js?version=20150130.02
5276	js.t.sinajs.cn	application/x-javascript	88 kB	iframeWidget.js?version=20140327
5290	timg.sjs.sinajs.cn	image/gif	796 bytes	loading1.gif
5340	www.cctv.com	application/javascript	7382 bytes	a2.js
5383	p5.img.cctvpic.com	image/jpeg	7292 bytes	35f51c0c428a4b19834084f8e29e0e22-79.jpg
5385	r.img.cctvpic.com	text/css	1316 bytes	style.css?93534174d3cb01f2509dddbd55f5d495
5464	p4.img.cctvpic.com	image/jpeg	7193 bytes	cf0219df98aa4ac699c2b520bb0992f1-40.jpg
5556	api.share.baidu.com	image/gif	0 bytes	content_683139.htm
5690	widget.weibo.com	text/html	0 bytes	aj_relationship.php?fuid=1791805181&callback=STK
5803	js.data.cctv.com	application/javascript	126 kB	__aplus_plugin_cctv.js,aplus_plugin_aplus_u.js
5919	p.data.cctv.com	image/gif	43 bytes	v.gif?logtype=0&title=%E6%8E%A8%E5%B9%BF1_%
6757	47.107.33.15:81	application/zip	5015 bytes	secret.zip
7792	47.107.33.15:81	text/html	320 bytes	hint.html
7796	47.107.33.15:81	text/html	287 bytes	favicon.ico

Save | Save All | Close | Help

发现需要密码才能打开



猜测是zip伪加密，利用工具ZipCenOp.jar进行修复

ZipCenOp.jar下载地址：

> https://github.com/fox-huyu/ZipCenOp.jar

打开输入：

```
java -jar .\ZipCenOp.jar r .\secret.zip
```

```
PS C:\Tools\Misc\ZipCenOp.jar> java -jar .\ZipCenOp.jar r .\secret.zip
>>>
java.lang.NullPointerException
        at zip.CenOp$1.run(CenOp.java:97)
        at java.security.AccessController.doPrivileged(Native Method)
        at zip.CenOp.clean(CenOp.java:89)
        at zip.CenOp.operate(CenOp.java:80)
        at zip.CenOp.main(CenOp.java:32)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
        at java.lang.reflect.Method.invoke(Unknown Source)
        at org.eclipse.jdt.internal.jarinjarloader.JarRsrcLoader.main(JarRsrcLoader.java:58)
success 0 flag(s) foundPS C:\Tools\Misc\ZipCenOp.jar> java -jar .\ZipCenOp.jar r .\secret.zip
>>>
success 2 flag(s) foundPS C:\Tools\Misc\ZipCenOp.jar>
```


secret.zip修复成功

打开看见flag