BUUCTF Misc 数据包中的线索

原创

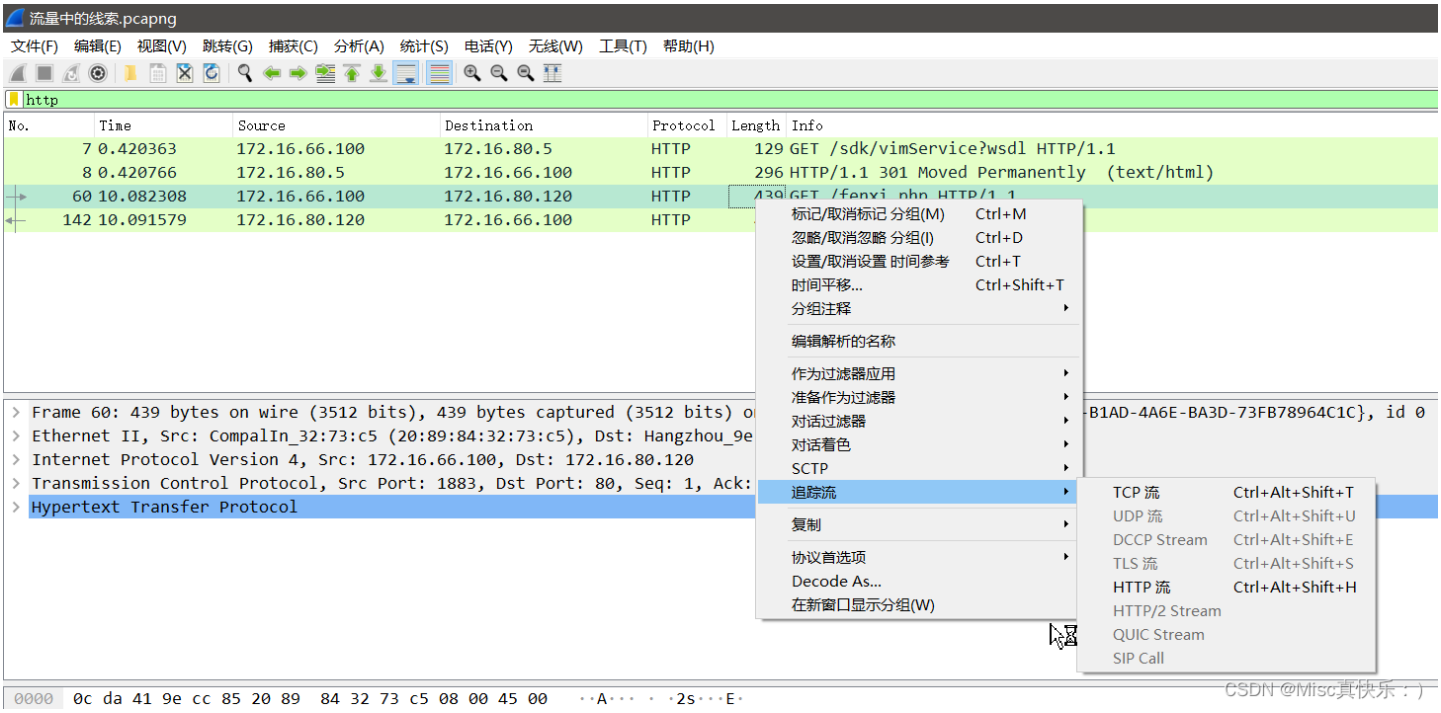
Misc真快乐：） 于 2022-02-28 16:34:56 发布 391 收藏

分类专栏： BUUCTF Misc 文章标签： 网络安全 信息安全

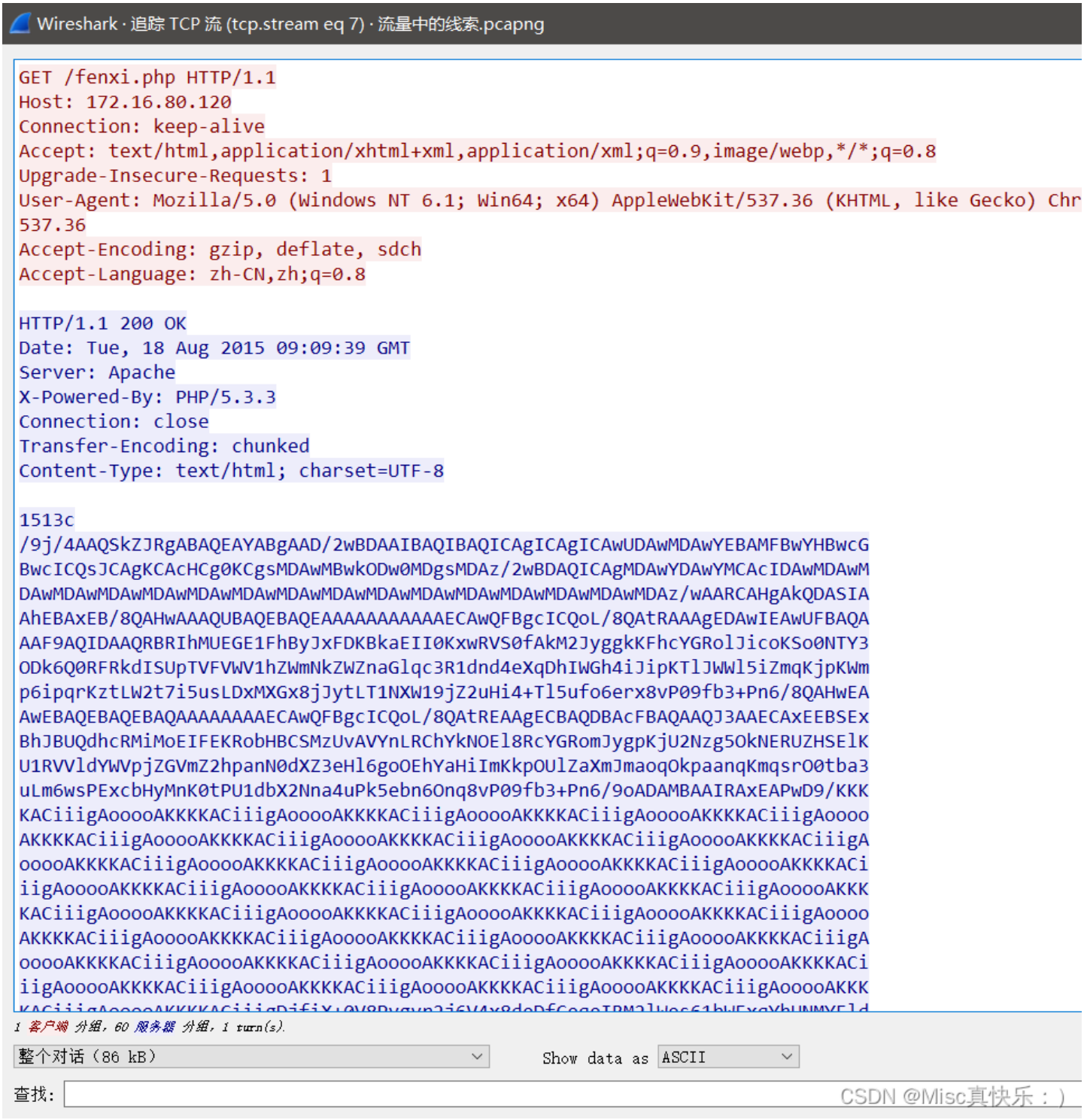
本文链接：https://blog.csdn.net/Leslie_LIL/article/details/123185158

题目如下：

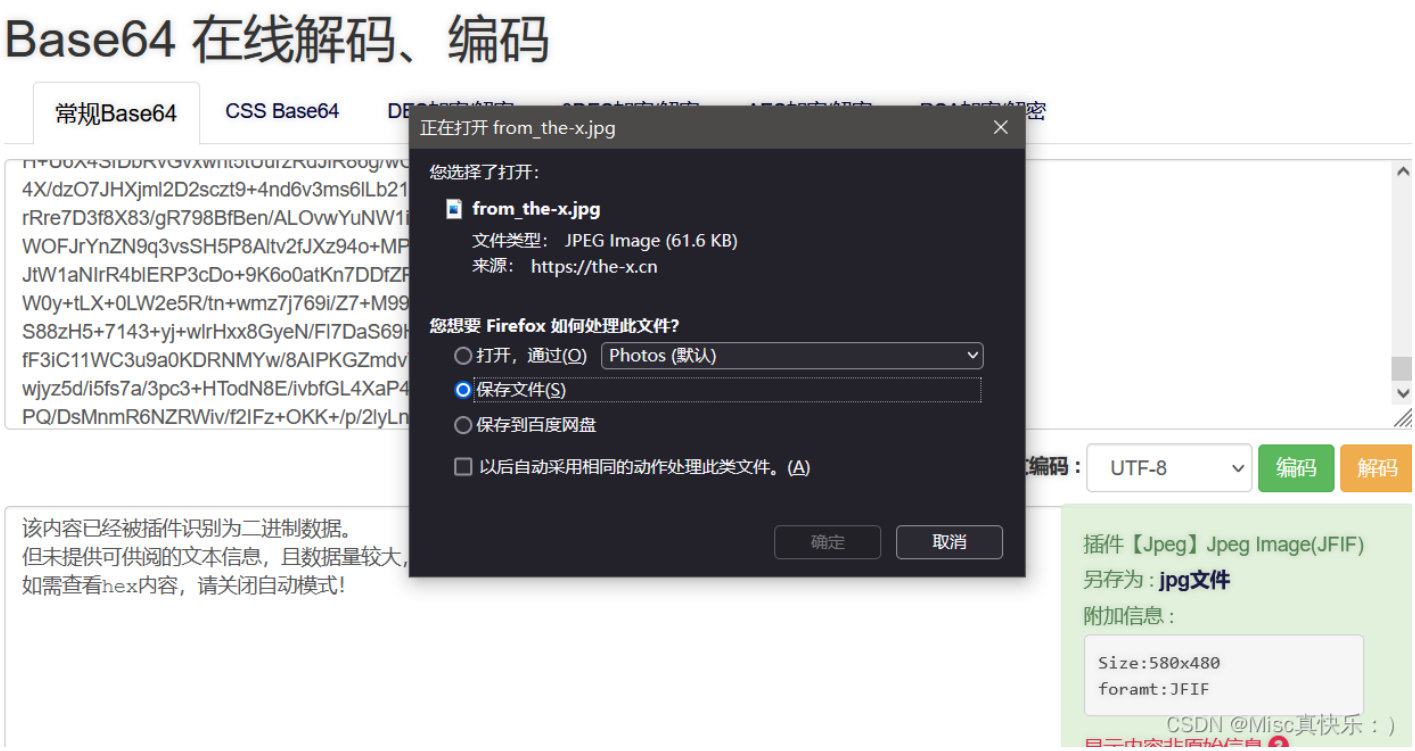
wireshark打开文件，追踪TCP流


流量中的线索.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)
http
No. Time Source Destination Protocol Length Info
7 0.420363 172.16.66.100 172.16.80.5 HTTP 129 GET /sdk/vimService?wsdl HTTP/1.1
8 0.420766 172.16.80.5 172.16.66.100 HTTP 296 HTTP/1.1 301 Moved Permanently (text/html)
60 10.082308 172.16.66.100 172.16.80.120 HTTP 439 GET /fenxi.php HTTP/1.1
142 10.091579 172.16.80.120 172.16.66.100 HTTP
Frame 60: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits) o
Ethernet II, Src: CompalIn_32:73:c5 (20:89:84:32:73:c5), Dst: Hangzhou_9e
Internet Protocol Version 4, Src: 172.16.66.100, Dst: 172.16.80.120
Transmission Control Protocol, Src Port: 1883, Dst Port: 80, Seq: 1, Ack:
Hypertext Transfer Protocol
标记/取消标记 分组(M) Ctrl+M
忽略/取消忽略 分组(I) Ctrl+D
设置/取消设置 时间参考 Ctrl+T
时间平移... Ctrl+Shift+T
分组注释
编辑解析的名称
作为过滤器应用
准备作为过滤器
对话过滤器
对话着色
SCTP
追踪流
复制
协议首选项
Decode As...
在新窗口显示分组(W)
TCP 流 Ctrl+Alt+Shift+T
UDP 流 Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS 流 Ctrl+Alt+Shift+S
HTTP 流 Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call
0000 0c da 41 9e cc 85 20 89 84 32 73 c5 08 00 45 00
CSDN @Misc真快乐：）

发现一段base64



在线base64解码，得到一个jpg文件


Base64 在线解码、编码
常规Base64
CSS Base64
正在打开 from_the-x.jpg
您选择了打开:
from_the-x.jpg
文件类型: JPEG Image (61.6 KB)
来源: https://the-x.cn
您想要 Firefox 如何处理此文件?
打开，通过(O) Photos (默认)
保存文件(S)
保存到百度网盘
以后自动采用相同的动作处理此类文件。(A)
确定
取消
编码：
UTF-8
编码
解码
该内容已经被插件识别为二进制数据。
但未提供可供阅的文本信息，且数据量较大，
如需查看hex内容，请关闭自动模式!
插件【Jpeg】Jpeg Image(JFIF)
另存为：jpg文件
附加信息：
Size:580x480
foramt:JFIF
CSDN @Misc真快乐：）

得到图片中的flag


from_the-x.jpg
010101
011010
011100
流量中的线索.
pcapng