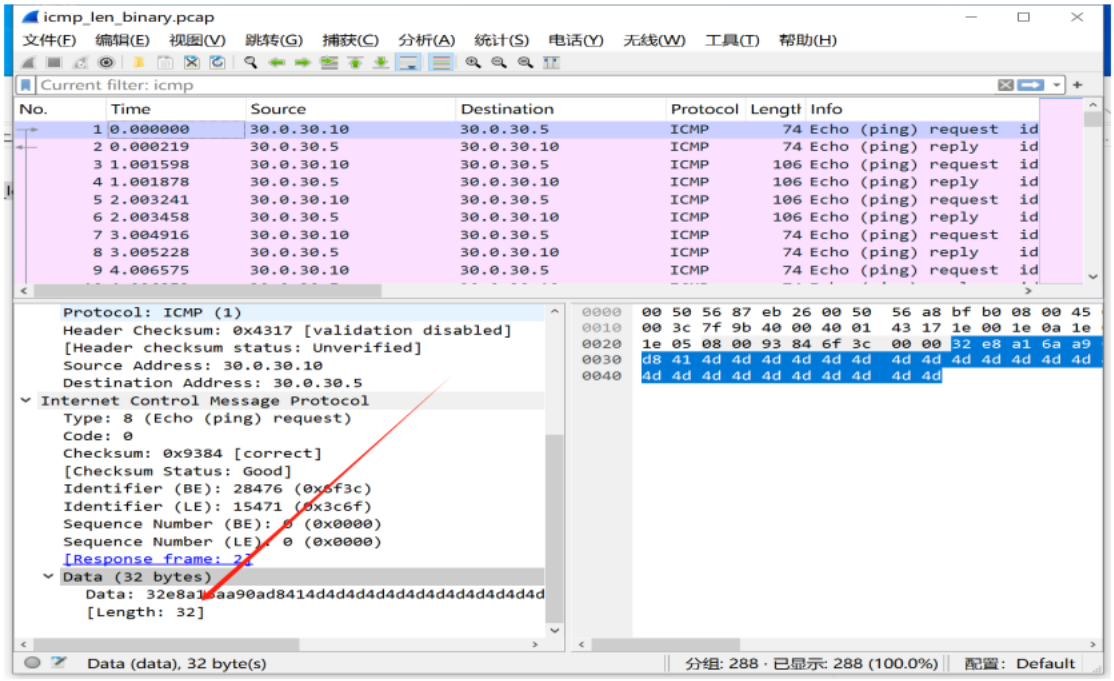
流量分析三-icmp_len_binary

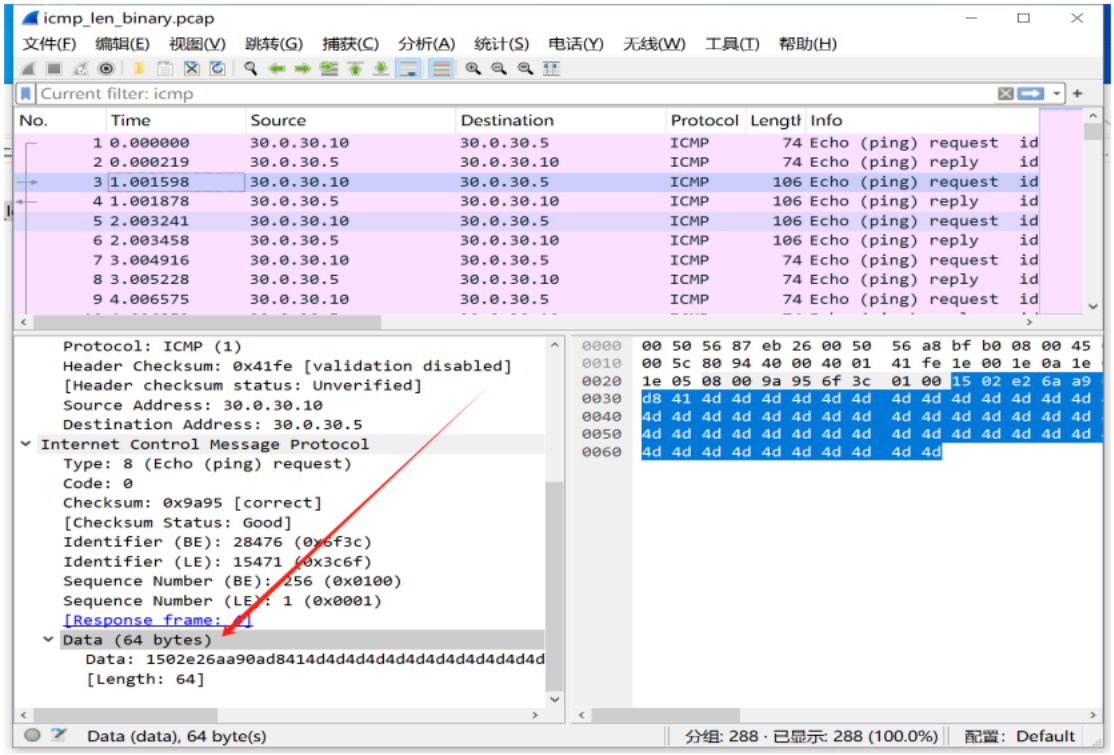
http://www.ctf8.com/index/containers/ContainerOtherCtfDetail/53

题目为 icmp_len_binary，猜测与 icmp 报文长度有关
打开数据包发现 icmp 报文只有两种长度（32bytes 和 64 bytes）

32 字节



64 字节



写脚本：（python3）用 01 来代表

```
import pyshark
import binascii
cap =
pyshark.FileCapture('icmp_len_binary.pcap',tshark_path=r'F:\2025\001-Tools\Wireshark\tshark.exe',display_filter="icmp && ip.src==30.0.30.10")
cap.load_packets()
flag = ''
con = ''
for i in range(0,len(cap)):
    if cap[i].icmp.data_len == '32':
        con += '0'
    else:
        con += '1'
print(con)
#int(con, base=2)
#这里的 con 是一个二进制的字符串（由 '0' 和 '1' 组成）。int(con, base=2) 将这个二进制字符串转换成整数。
#例如，con = '1101' 会变成 int('1101', base=2), 结果是整数 13。

#hex(...)
#hex() 函数将整数转换为十六进制字符串。返回的结果是以 '0x' 开头的十六进制数。
#例如，hex(13) 会返回 '0xd'。

#由于 hex() 返回的字符串是以 '0x' 开头的，[2:] 会去掉这个前缀，只留下十六进制部分。
```

例如，'0xd' 会变成 'd'。

# binascii.a2b_hex() 将十六进制字符串转换为字节字符串（bytes）。它的输入是一个只包含合法十六进制字符的字符串。
print(binascii.a2b_hex(hex(int(con,base=2))[2:]))
cap.close()

得 flag：
ctfhub{04efed1e05}