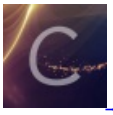
bugku-writeup-MISC-ping

原创

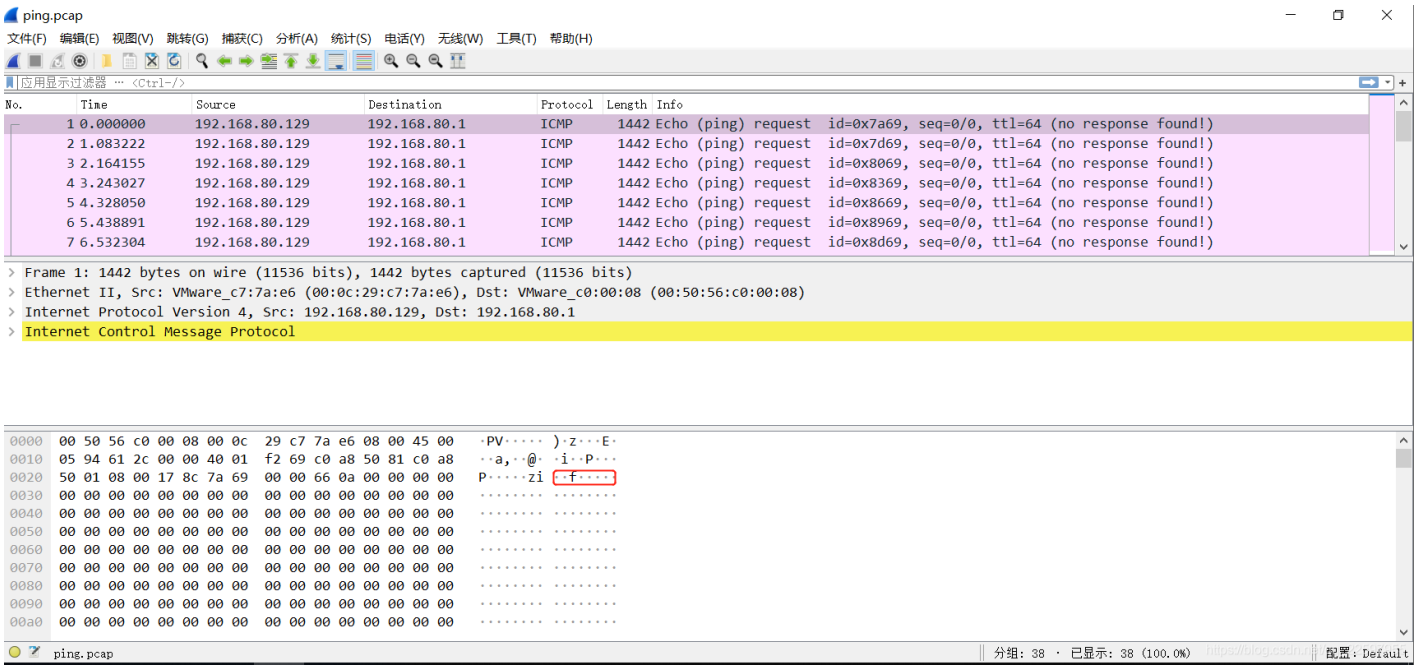
dark2019 于 2021-06-28 18:30:10 发布 431 收藏
分类专栏： 信息安全 wp 文章标签： 信息安全 wp wireshark

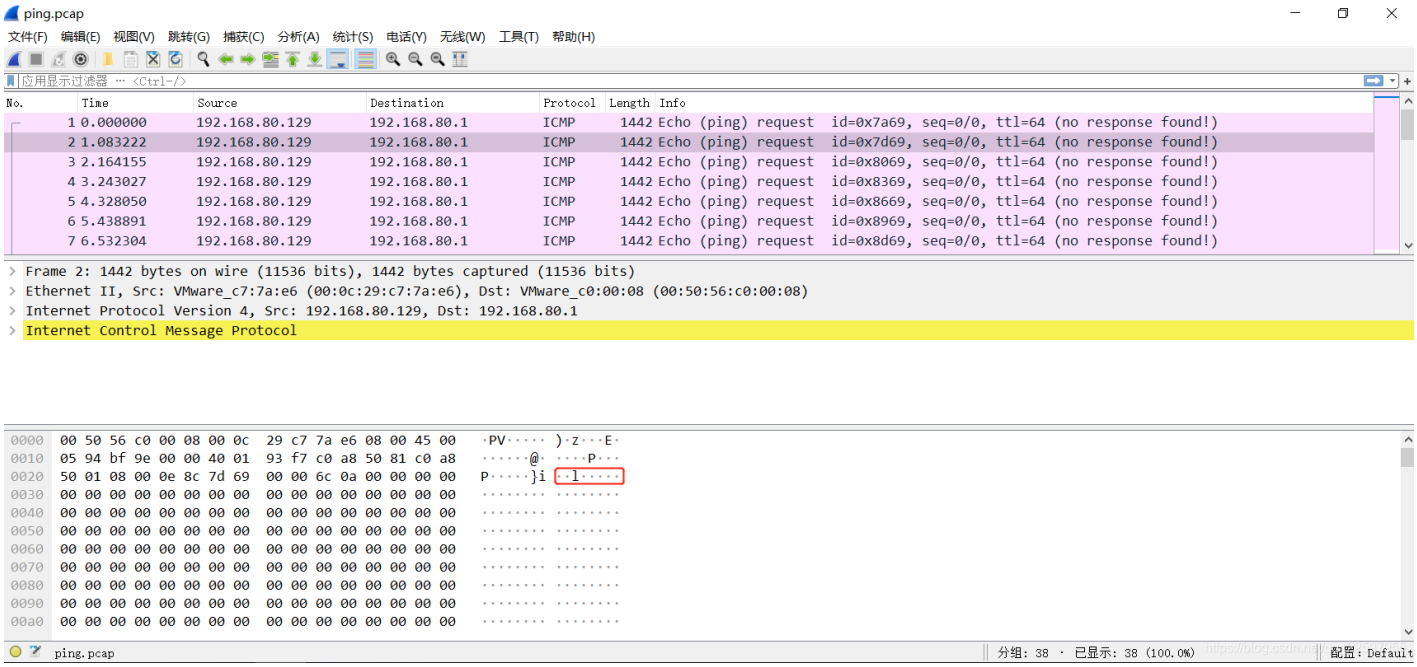

信息安全 同时被 2 个专栏收录
53 篇文章 1 订阅
订阅专栏

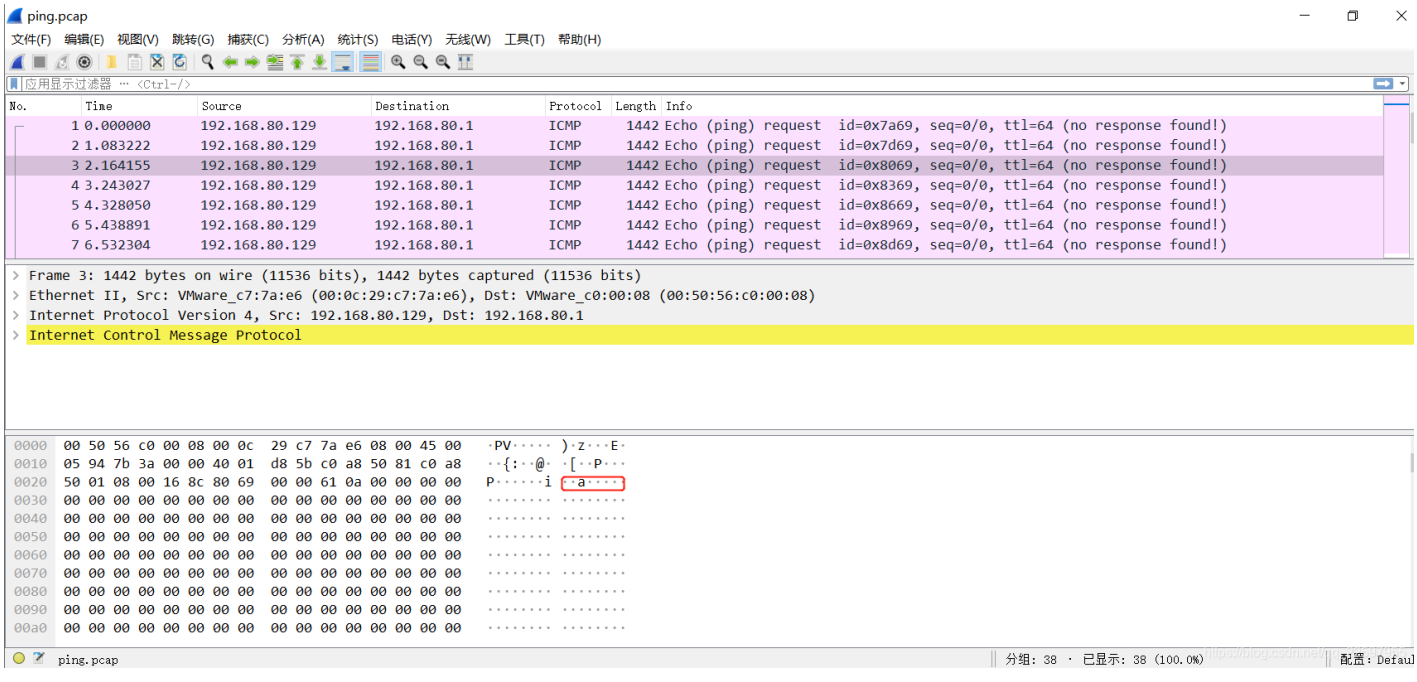

wp
31 篇文章 0 订阅
订阅专栏

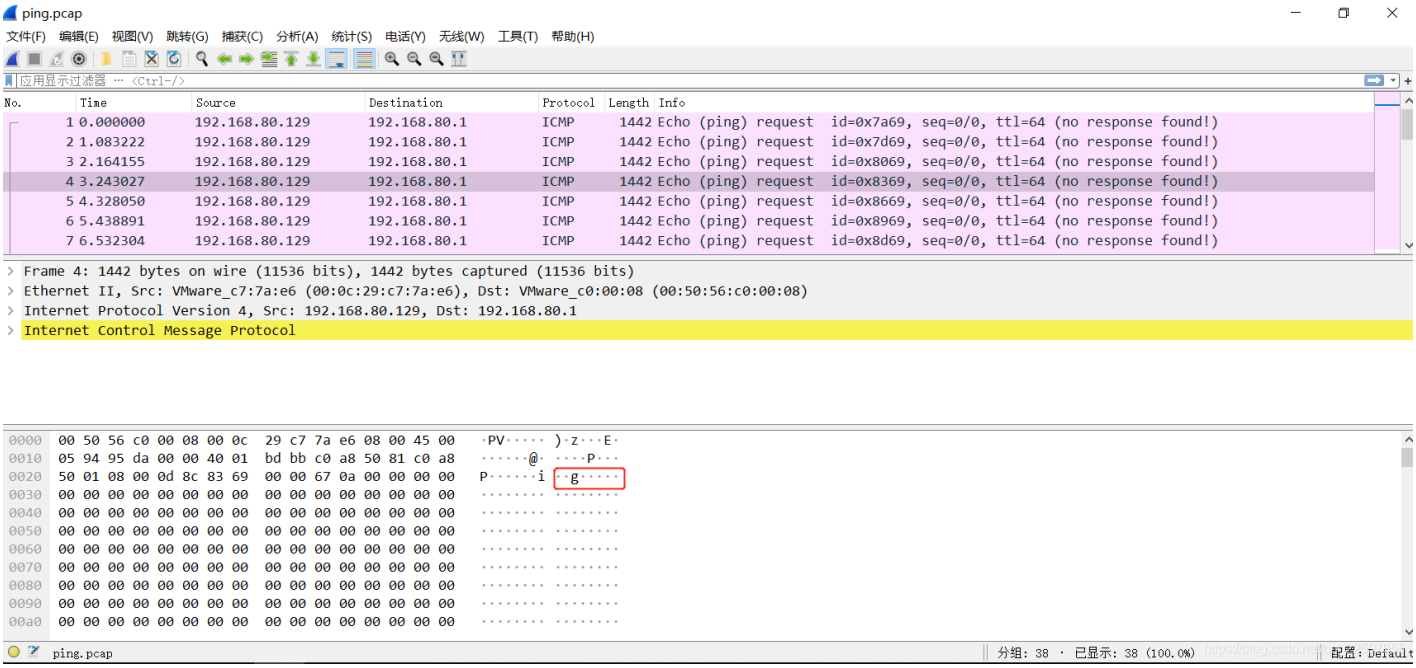
题目：ping

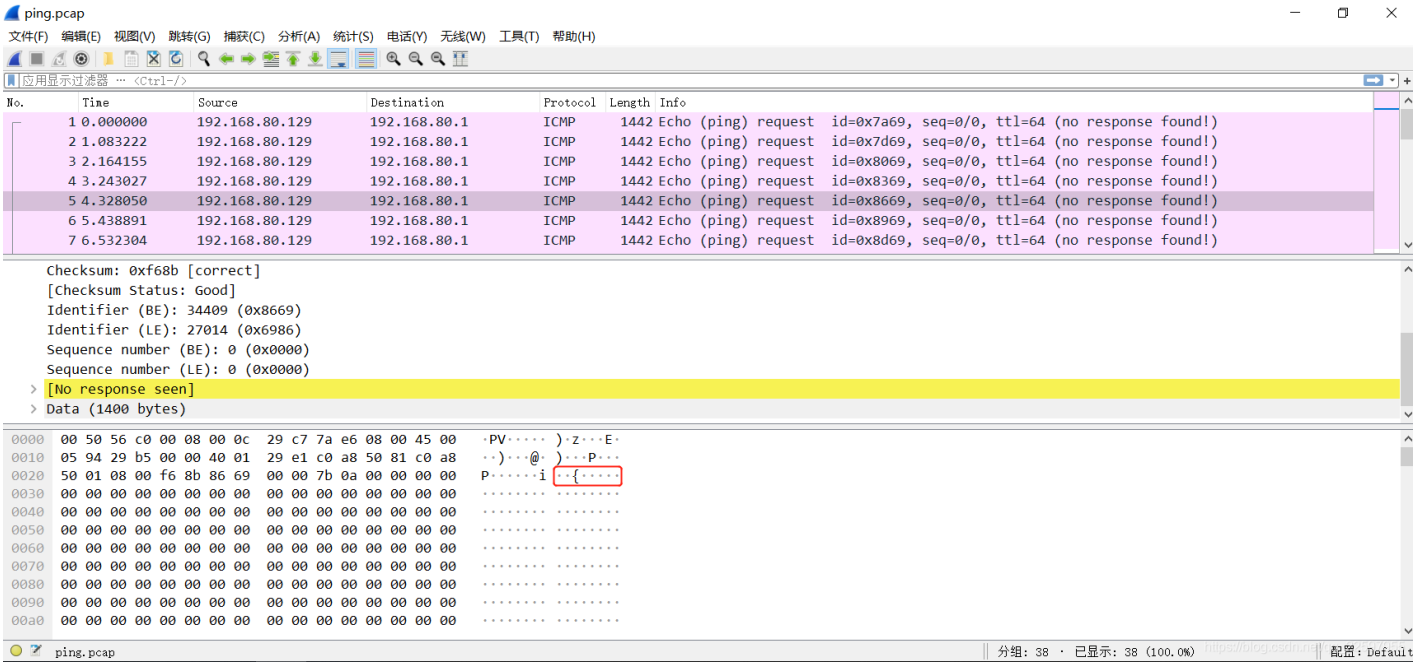
01—思路一


ping.pcap
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)
应用显示过滤器 … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response found!)
2 1.083222 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response found!)
3 2.164155 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response found!)
4 3.243027 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response found!)
5 4.328050 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response found!)
6 5.438891 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response found!)
7 6.532304 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response found!)
Frame 1: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits)
Ethernet II, Src: VMware_c7:7a:e6 (00:0c:29:c7:7a:e6), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.80.129, Dst: 192.168.80.1
Internet Control Message Protocol
0000 00 50 56 c0 00 08 00 0c 29 c7 7a e6 08 00 45 00 ·PV·····)·z···E·
0010 05 94 61 2c 00 00 40 01 f2 69 c0 a8 50 81 c0 a8 ··a,··@· ·i··P···
0020 50 01 08 00 17 8c 7a 69 00 00 66 0a 00 00 00 00 P·····zi ··f·····
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
ping.pcap
分组: 38 · 已显示: 38 (100.0%)
配置: Default


ping.pcap
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)
应用显示过滤器 … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response found!)
2 1.083222 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response found!)
3 2.164155 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response found!)
4 3.243027 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response found!)
5 4.328050 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response found!)
6 5.438891 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response found!)
7 6.532304 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response found!)
Frame 2: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits)
Ethernet II, Src: VMware_c7:7a:e6 (00:0c:29:c7:7a:e6), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.80.129, Dst: 192.168.80.1
Internet Control Message Protocol
0000 00 50 56 c0 00 08 00 0c 29 c7 7a e6 08 00 45 00 ·PV·····)·z···E·
0010 05 94 bf 9e 00 00 40 01 93 f7 c0 a8 50 81 c0 a8 ·····@· ····P···
0020 50 01 08 00 0e 8c 7d 69 00 00 6c 0a 00 00 00 00 P·····}i ··l·····
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
ping.pcap
分组: 38 · 已显示: 38 (100.0%)
配置: Default


ping.pcap
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)
应用显示过滤器 … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x7a69, seq=0/0, ttl=64 (no response found!)
2 1.083222 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x7d69, seq=0/0, ttl=64 (no response found!)
3 2.164155 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8069, seq=0/0, ttl=64 (no response found!)
4 3.243027 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8369, seq=0/0, ttl=64 (no response found!)
5 4.328050 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8669, seq=0/0, ttl=64 (no response found!)
6 5.438891 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8969, seq=0/0, ttl=64 (no response found!)
7 6.532304 192.168.80.129 192.168.80.1 ICMP 1442 Echo (ping) request id=0x8d69, seq=0/0, ttl=64 (no response found!)
Frame 3: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits)
Ethernet II, Src: VMware_c7:7a:e6 (00:0c:29:c7:7a:e6), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.80.129, Dst: 192.168.80.1
Internet Control Message Protocol
0000 00 50 56 c0 00 08 00 0c 29 c7 7a e6 08 00 45 00 ·PV·····)·z···E·
0010 05 94 7b 3a 00 00 40 01 d8 5b c0 a8 50 81 c0 a8 ··{:··@· ·[··P···
0020 50 01 08 00 16 8c 80 69 00 00 61 0a 00 00 00 00 P·····i ··a·····
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ···· ····
ping.pcap
分组: 38 · 已显示: 38 (100.0%)
配置: Default

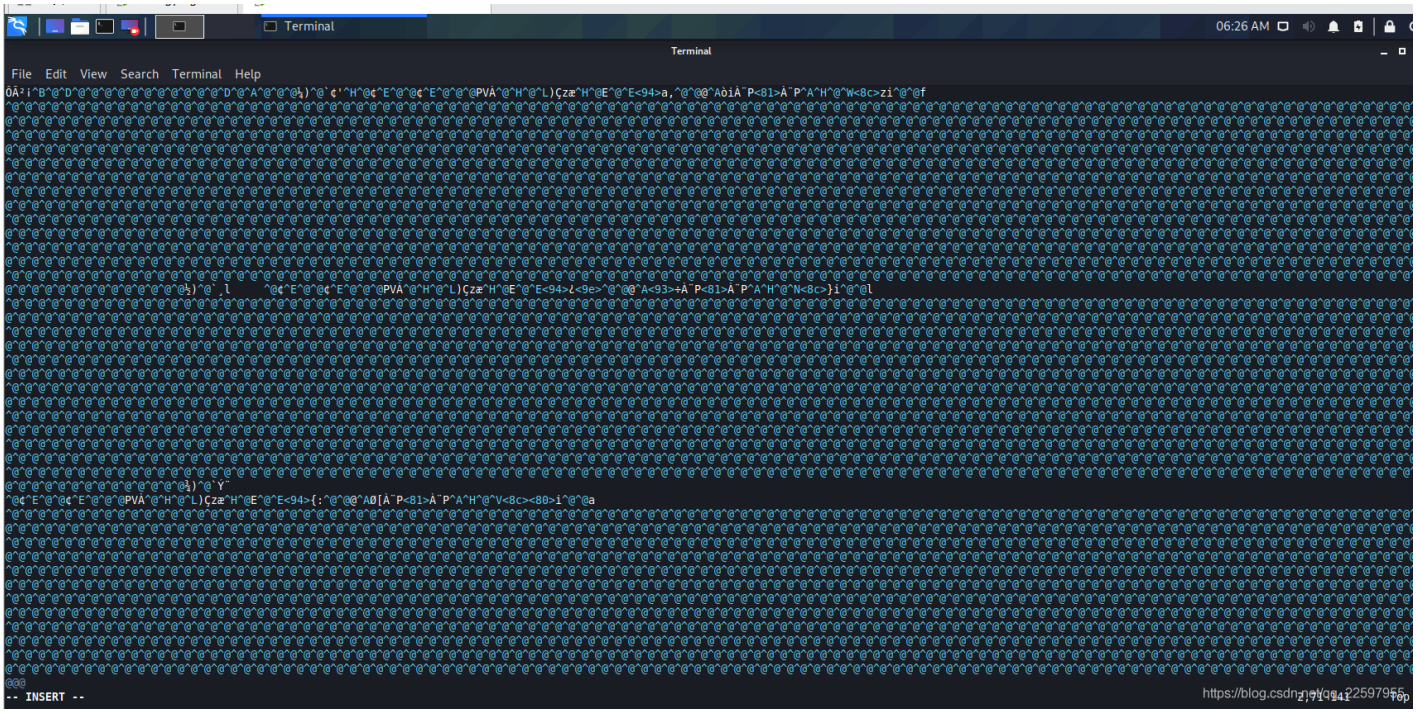




观察前5个数据包发现，data的最后一个字母可以拼接为flag{，因此依次记录各数据包中data的最后一个字母，得到flag。

02—思路二

将**ping.pcap**文件后缀名改为**txt**,双击打开，发现乱码，放在**linux**系统下，用**vim**打开试试：



这里使用kali打开，发现可以显示最后一个字母，依次拼接，得到flag。

```
flag{dc76a1eee6e3822877ed627e0a04ab4a}
```