

# CS305 lab2 问答

wangw6@sustech.edu.cn

## Q1. 如何通过 wireshark 计算 rtt:

A1. 在 wireshark 的抓包中找到同一个会话的两个报文（测试报文、应答报文），记录测试报文发出去的时间和应答报文接收到的时间，二者的差值即为 rtt

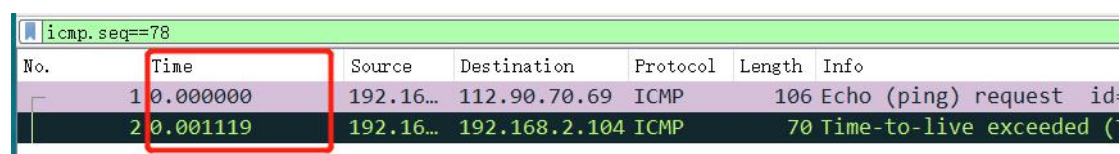
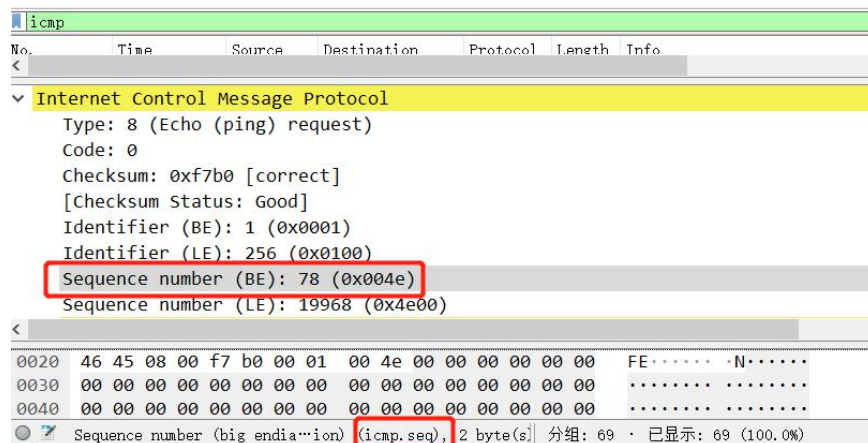
## Q2. 如何找到同一个 icmp 会话的相关报文

A2.

方法 1: 以 icmp request（由本机发出）和 icmp ttl exceed（由路由器发出）为例  
每个 icmp request 都有唯一的序列号，而 icmp ttl exceed 报文会把收到的 icmp request 报文封装起来（即包含了对应的 icmp request 报文）

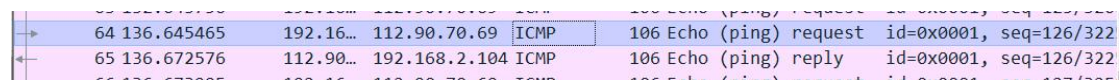
Step1: 在 wireshark 里找到 icmp request 中序列号对应的字段名 icmp.seq 以及对应的数值 x

Step2: 以 icmp.seq ==x 作为 wireshark 的显示过滤器，即可将一个会话过滤出来



方法 2: 以 icmp request 和 icmp reply 为例，使用 Wireshark 自动分析匹配的功能

Step1: 选择一个 icmp request，点击后会在该报文和与其在同一个会话里的 icmp reply 的左侧显示灰色的箭头



## Q3: 如何查看 TTL

A3: TTL 是报文的 IPv4 的字段，报文在发送前设置 ttl 的初始值，在途径路由器时会对 ttl 值做减法操作。

接收的报文中，IP 协议层的 ttl 字段的值应该是：该报文的 ttl 初始值-该报文途经的路由器个数（hops）。

作业 2.3 的第 3 问，希望大家根据抓包进行判断：

本机接收的 icmp reply 中的 ttl + hops 是否等于本机发送的 icmp request 中的 ttl ？

如果上述关系不成绩，说明：通过 icmp reply 中的 ttl + hops 计算得到的是 本机设置的 ttl 初始值？ 还是 destination 设置的 ttl 初始值？

No.	Time	Source	Destination	Protocol	Length	Info
68	136.702902	192.16...	112.90.70.69	ICMP	106	Echo
69	136.725379	112.90...	192.168.2.104	ICMP	106	Echo

<

> Frame 68: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0  
> Ethernet II, Src: IntelCor\_5c:69:58 (90:61:ae:5c:69:58), Dst: Skyworth\_de:ad:05 (00:1a:9a:de:ad:05)  
▼ Internet Protocol Version 4, Src: 192.168.2.104, Dst: 112.90.70.69  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)  
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
        Total Length: 92  
        Identification: 0x4b29 (19241)  
    > Flags: 0x0000  
        Fragment offset: 0  
        Time to live: 17  
        Protocol: ICMP (1)  
        Header checksum: 0xe4c8 [validation disabled]  
        [Header checksum status: Unverified]  
        Source: 192.168.2.104

<

Time to live (ip.ttl), 1 byte(s) | 分组: 69 · 已显示:

No.	Time	Source	Destination	Protocol	Length	Info
68	136.702902	192.16...	112.90.70.69	ICMP	106	Echo
69	136.725379	112.90...	192.168.2.104	ICMP	106	Echo

<

> Frame 69: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0  
> Ethernet II, Src: Skyworth\_de:ad:05 (00:1a:9a:de:ad:05), Dst: IntelCor\_5c:69:58 (90:61:ae:5c:69:58)  
▼ Internet Protocol Version 4, Src: 112.90.70.69, Dst: 192.168.2.104  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)  
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
        Total Length: 92  
        Identification: 0x2280 (8832)  
    > Flags: 0x0000  
        Fragment offset: 0  
        Time to live: 45  
        Protocol: ICMP (1)  
        Header checksum: 0xf171 [validation disabled]  
        [Header checksum status: Unverified]  
        Source: 112.90.70.69

<

Time to live (ip.ttl), 1 byte(s) | 分组: 69 · 已显示: