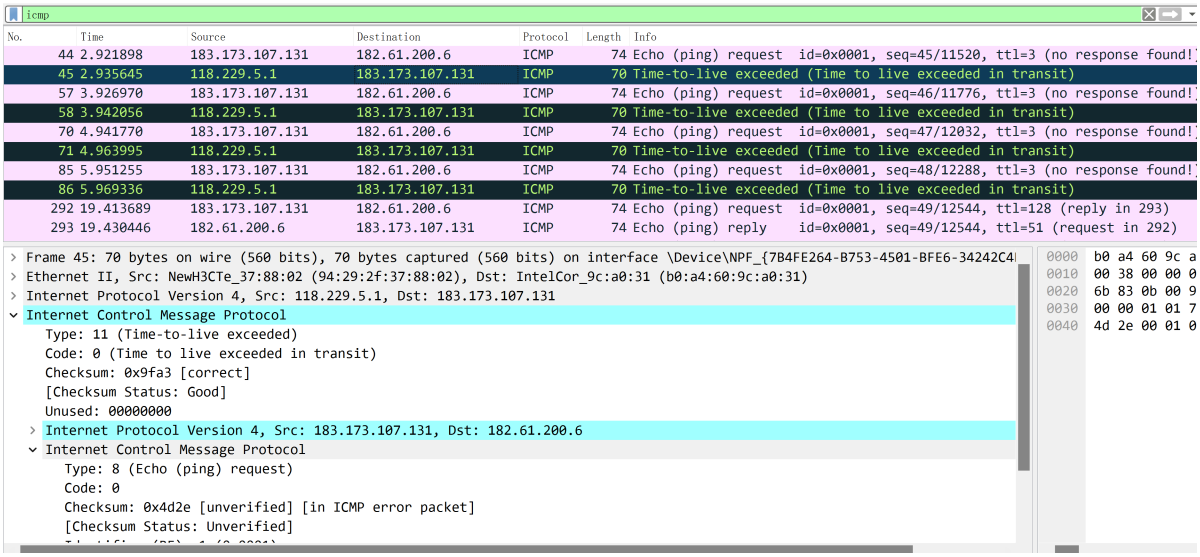
小实验3 Report

计11 周韧平 2021010699

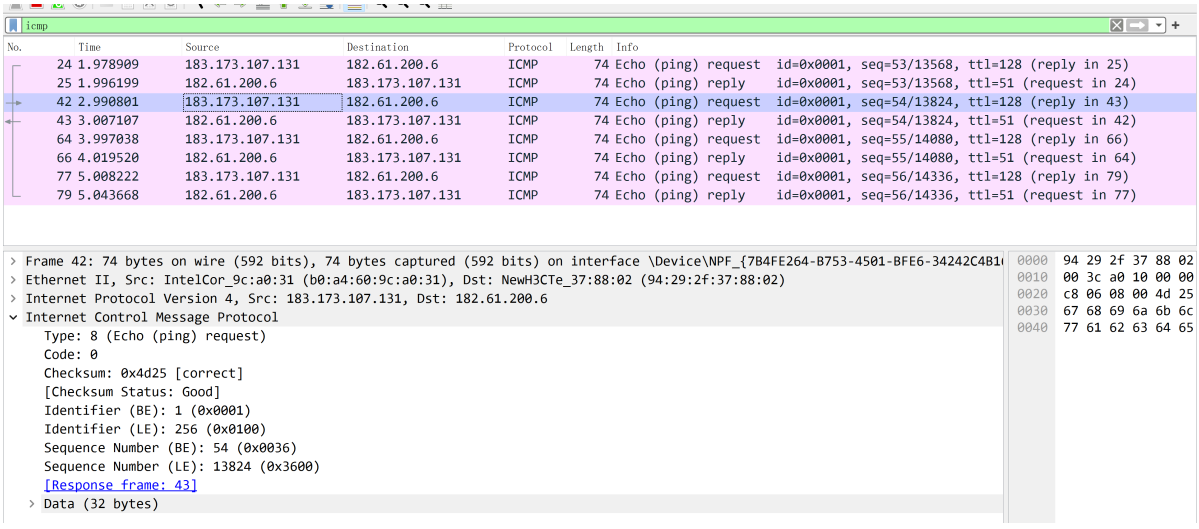
抓包实验 1： 观察 ICMPv4 超时消息



1.收到的 ICMP 包头中， Type 字段和 Code 字段分别是多少?

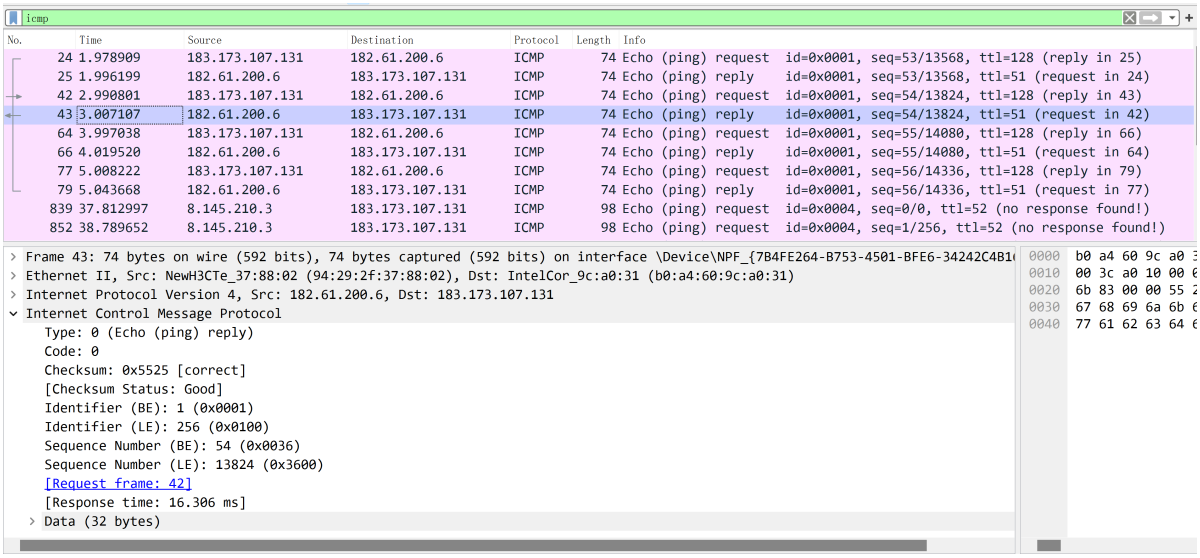
Type 字段为 11， Code 字段为 0

抓包实验 2： 观察 ICMPv4 回显请求及应答消息



1.ICMP 请求分组中， Type 字段和 Code 字段分别是多少?

Type 字段为 8， Code 字段为 0



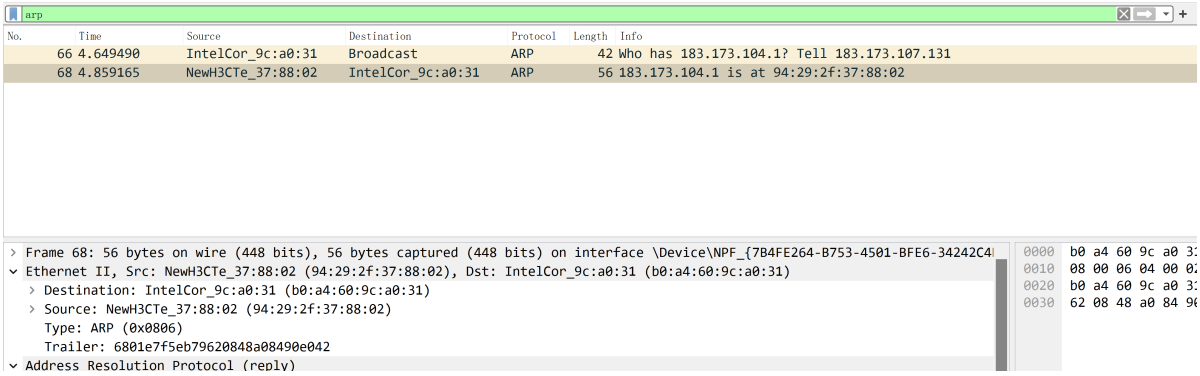
2.ICMP 回显分组中， Type 字段和 Code 字段分别是多少?

Type 字段为 0， Code 字段为 0

3.一对请求和回复分组中的标识符，序号和数据是否相等?

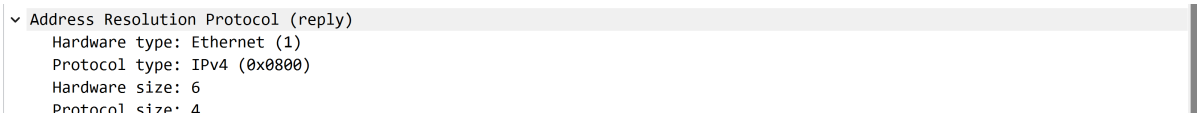
上图中的两个包就是一对请求与回复分组，其标识符，序号和数据字段均相等

抓包实验 3： 观察 ARP 分组各式



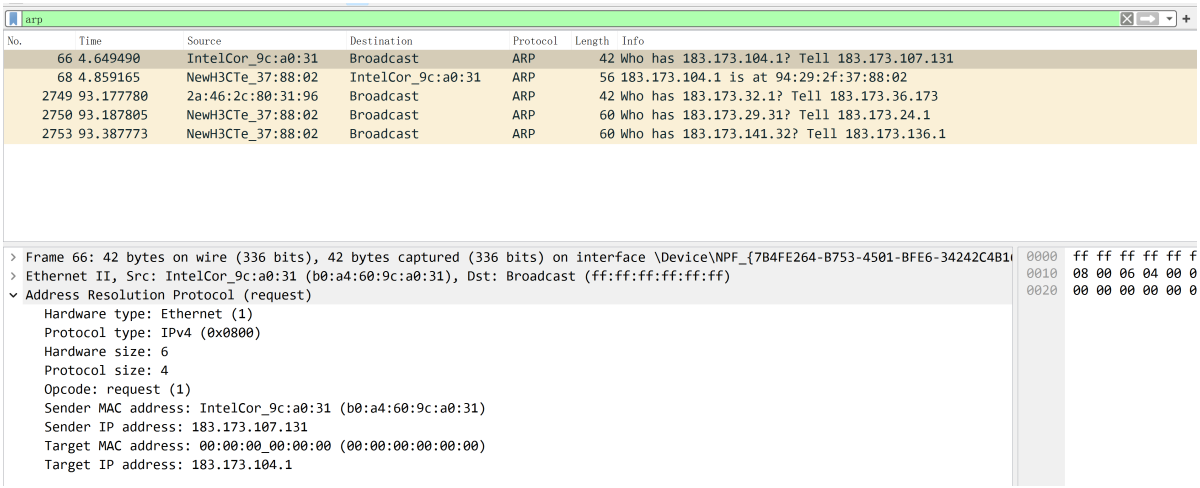
1.ARP 协议在以太网帧头中载荷类型的编号是?

0x0806



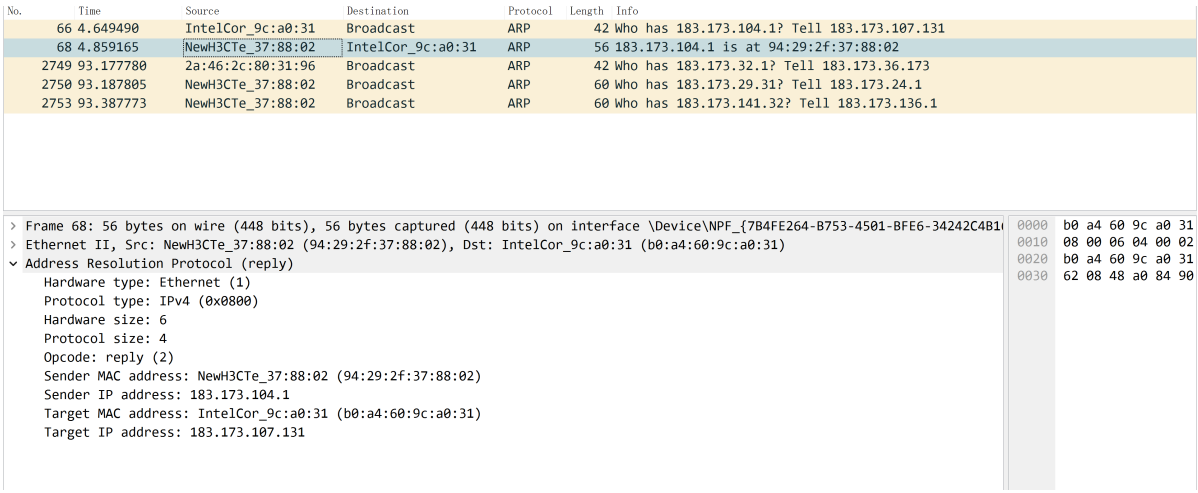
2.ARP 分组头中，以太网硬件类型编号和 IP 协议类型编号分别是?

硬件类型以太网： 1，协议类型 IPv4： 0x0800



3.ARP 请求分组中，操作码（Opcode）值是？源 IP 地址及 MAC地址，目的 IP 地址及 MAC 地址是多少?

Opcode 值是 1， (Sender)源 IP 和 MAC 是本机， (Target)目的 IP 和 MAC 是请求的 IP 地址和广播地址



4.ARP 回复分组中，操作码（Opcode）值是？源 IP 地址及 MAC地址，目的 IP 地址及 MAC 地址是多少?

Opcode 值是 2， (Sender)源 IP 和 MAC 是请求的 IP 地址和回复的 MAC， (Target)目的 IP 和 MAC 是本机

简述题

1.上网查找资料，看看 ICMPv4 消息的隐患，以及黑客是如何利用它发起攻击的，由此思考为什么很多系统不发送 ICMPv4 消息。

黑客可以发送大量 ICMP Echo Request 消息来发起 DoS（拒绝服务）攻击，耗尽目标系统的资源，导致其无法正常工作。黑客还可能通过发送恶意的 ICMP Redirect 消息来欺骗主机，使其将流量发送到恶意的中间人攻击者，从而进行拦截、篡改或监听通信流量。由于可能被黑客利用来进行攻击，系统管理员选择禁用或限制对这些消息的响应。这样可以减少系统暴露给潜在攻击的机会。

2.ping 同一局域网内的主机和局域网外的主机，都会产生 ARP报文么？所产生的 ARP 报文有何不同，为什么?

在Ping同一局域网内的主机时，由于目标主机与源主机位于同一局域网内，源主机已经知道目标主机的IP地址，并且能够直接发送数据包。因此，在这种情况下，Ping操作不会产生ARP报文。因为ARP（Address Resolution Protocol）主要用于在同一局域网内解析IP地址和MAC地址之间的映射关系。在Ping局域网外的主机时，由于目标主机与源主机位于不同的局域网，源主机无法直接知道目标主机的MAC地址。因此，在这种情况下，Ping操作会产生ARP报文。

3.ARP 请求数据包是支撑 TCP/IP 协议正常运作的广播包。如果滥发或错发 ARP 广播包会产生那些不良影响？如何发现和应对?

不良影响：

- 网络拥塞：大量滥发的ARP广播包会占用网络带宽和资源，导致网络拥塞，影响正常通信和性能。
- ARP欺骗（ARP Spoofing）：攻击者可能滥发ARP广播包来进行ARP欺骗攻击。这种攻击会导致网络中的主机将流量发送到攻击者的主机，从而使攻击者能够窃取、篡改或监听通信流量。

发现和应对：

- 使用网络监控工具：使用网络监控工具来检测网络中的异常流量和广播包数量。这些工具可以提供实时的网络流量分析和警报，帮助及时发现异常情况。
- 实施入侵检测系统（IDS）或入侵防御系统（IPS）：IDS/IPS系统可以检测和阻止滥发或错发ARP广播包的行为。它们可以通过监测网络流量和识别异常模式来发现潜在的攻击，并采取相应的防御措施。