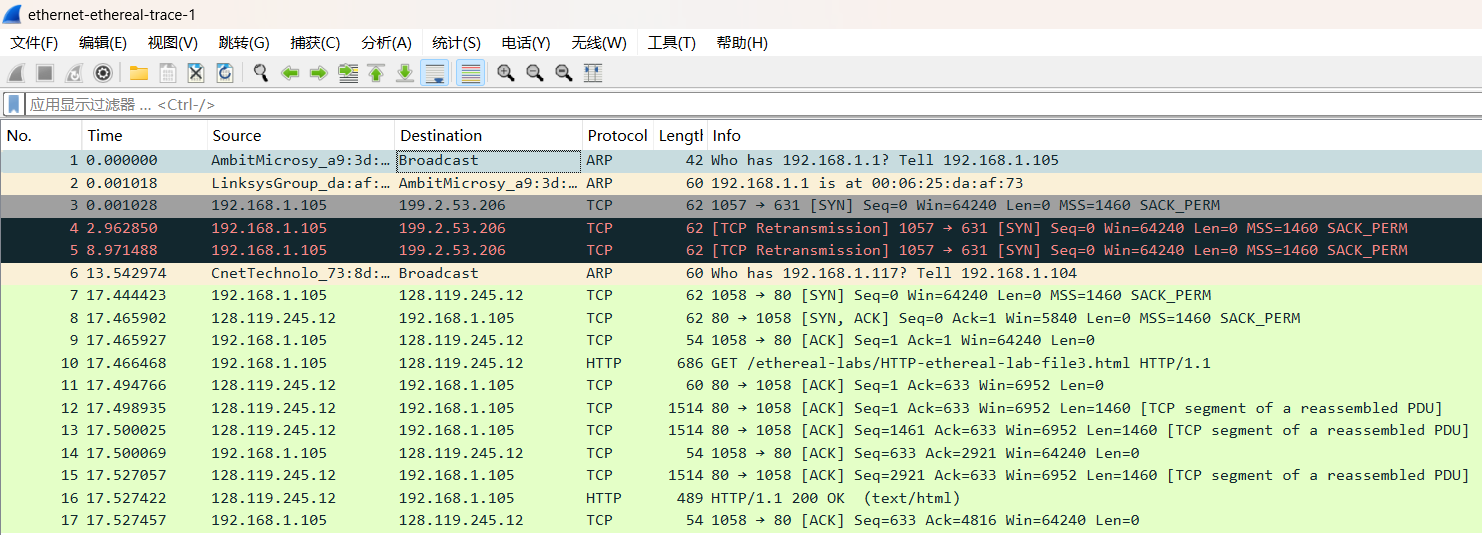
第一部分 以太网帧分析

1、在 wireshark 中打开文件ethernet--ethereal-trace-1



1. 分析其中的 ARP 帧

TCP建立连接需要三次握手，通过ARP建立连接实现。故有三个 ARP 数据帧，具体解析如下。

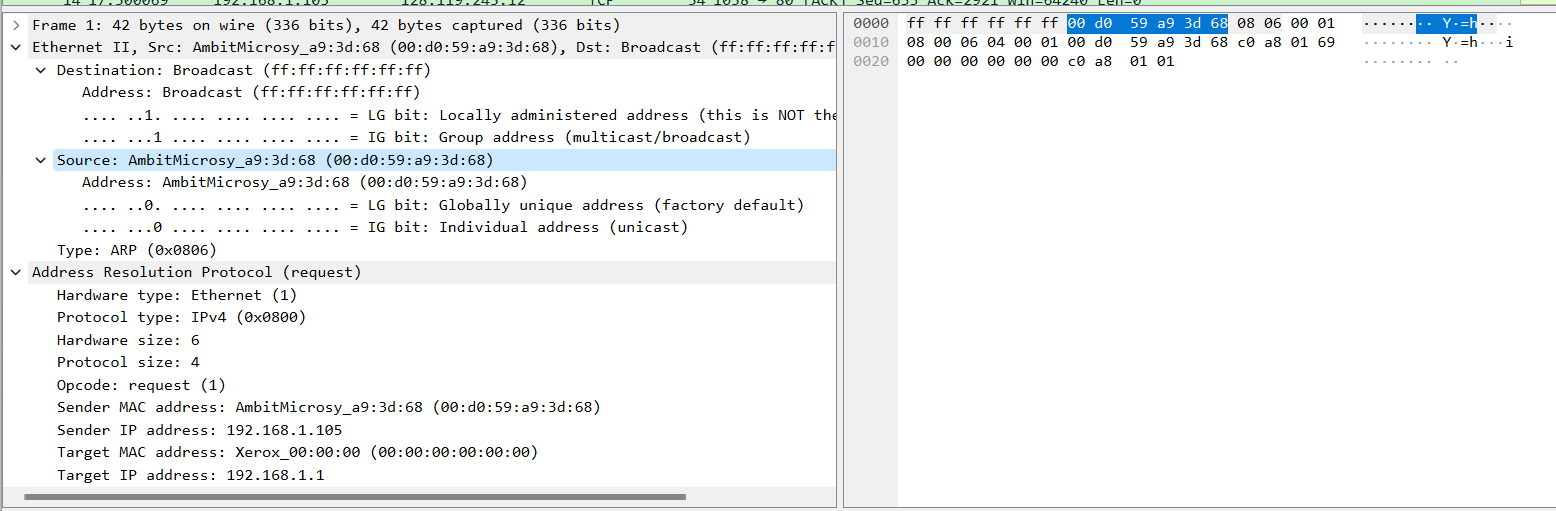
1. 设备A需要与设备B建立连接。
2. 设备A知道设备B的IP地址，但不知道其MAC地址。
3. 设备A向网络中广播一个ARP请求，该请求中：

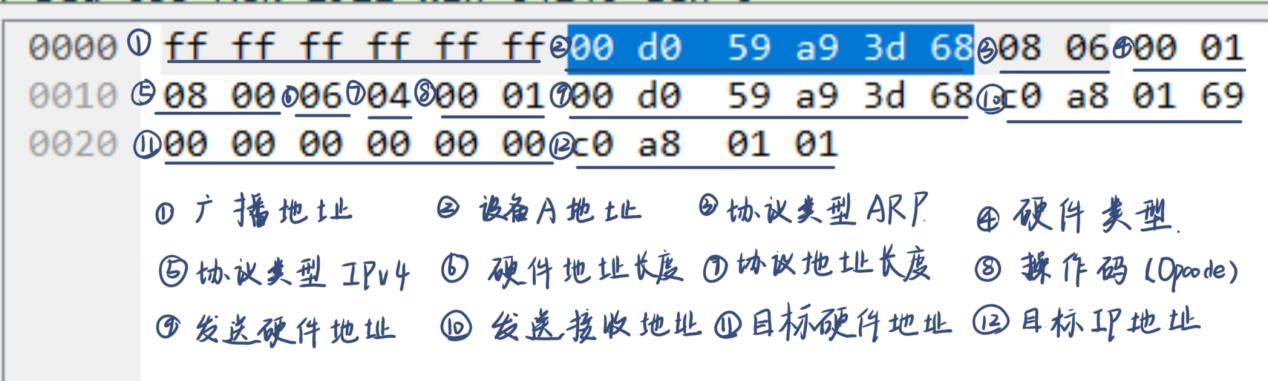
源MAC地址（Sender Hardware Address） 是设备A的MAC地址。

源IP地址（Sender Protocol Address） 是设备A的IP地址。

目标MAC地址（Target Hardware Address） 是广播地址（通常是全为1的MAC地址，即FF:FF:FF:FF:FF:FF）。

目标IP地址（Target Protocol Address） 是设备B的IP地址。





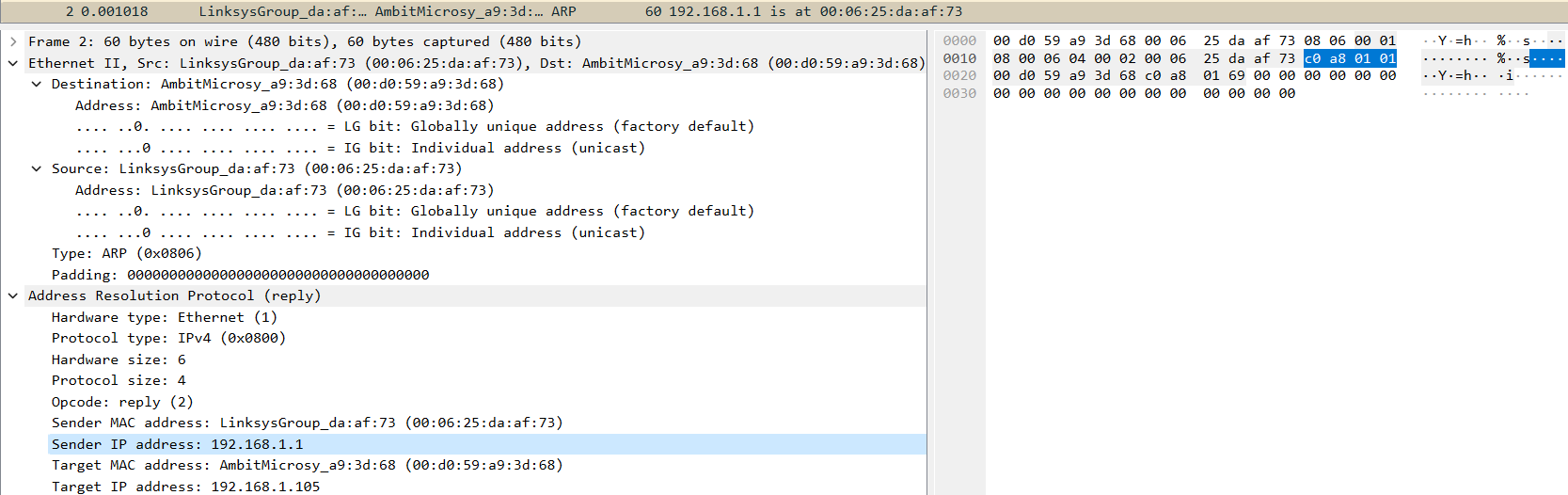
1. 所有位于广播域内的设备都能收到这个ARP请求。
2. 设备B收到ARP请求后，会回复一个ARP应答，该应答中：

源MAC地址 是设备B的MAC地址。

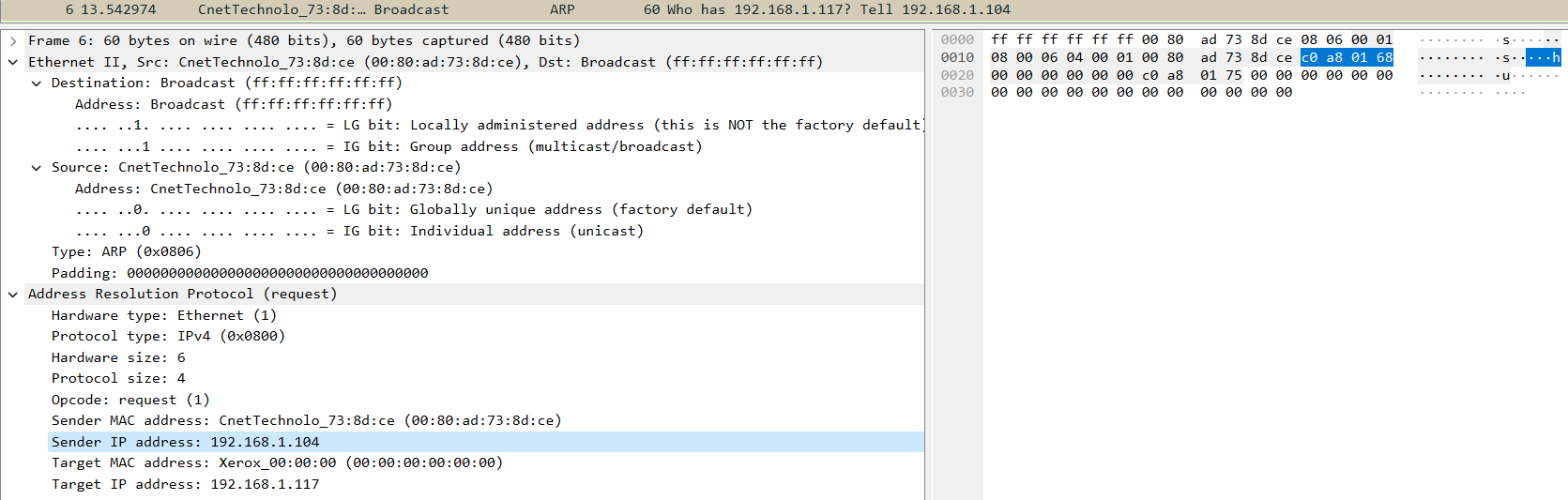
源IP地址 是设备B的IP地址。

目标MAC地址 是设备A的MAC地址。

目标IP地址 是设备A的IP地址。



1. 设备A收到ARP应答后，就知道了设备B的MAC地址。
2. 现在，设备A可以使用设备B的MAC地址，通过TCP建立连接。



在整个过程中，ARP的作用是解析目标设备的IP地址到MAC地址的映射关系，确保在建立TCP连接之前，设备A知道设备B的MAC地址，以便数据能够正确传输。

1. 文档问题10.在包含ARP请求消息的以太网帧中，源地址和目标地址的十六进制值是多少？
2. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

第一次交手

源 MAC 地址：00:d0:59:a9:3d:68

源 IP 地址：c0 a8 01 69

目标 MAC 地址：00:00:00:00:00:00 （未知）

目标 IP 地址：c0 a8 01 01

第二次交手

源 MAC 地址：00:06:25:da:af:73

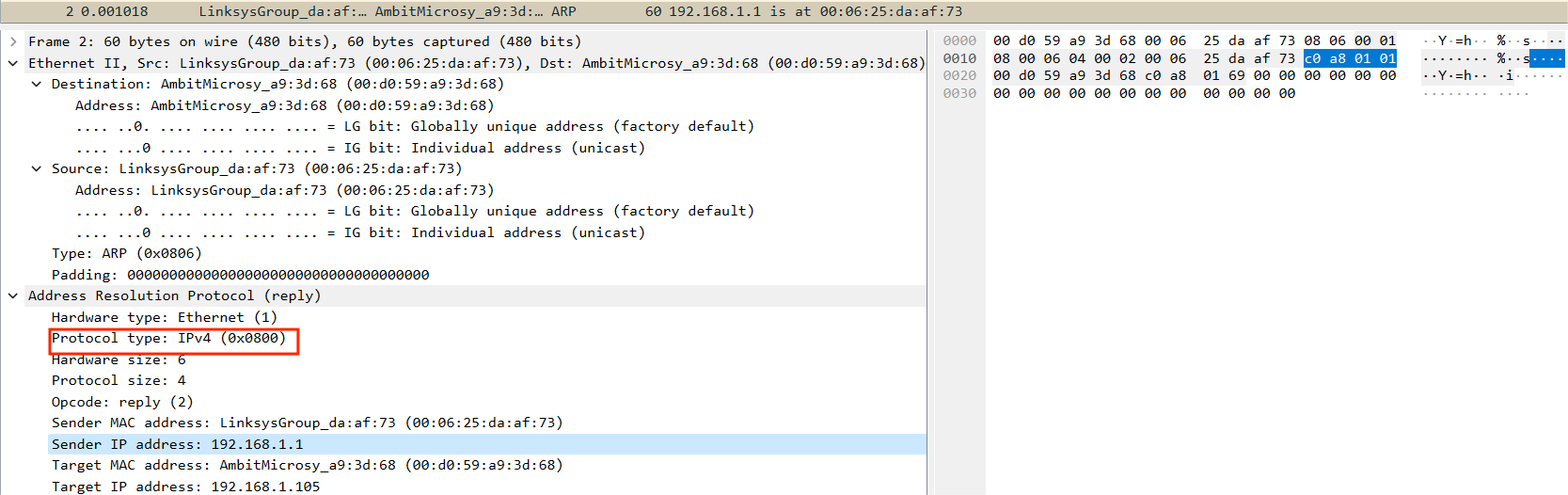
源 IP 地址：c0 a8 01 01

目标 MAC 地址：00:d0:59:a9:3d:68

目标 IP 地址：c0 a8 01 69

1. 文档问题11.为两字节以太网帧类型字段提供十六进制值。这对应于什么上层协议？
2. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

对应的上层协议是IPv4



1. 文章问题13.现在找到响应ARP请求而发送的ARP回复。

a） ARP操作码字段从以太网帧的最开始开始有多少字节？

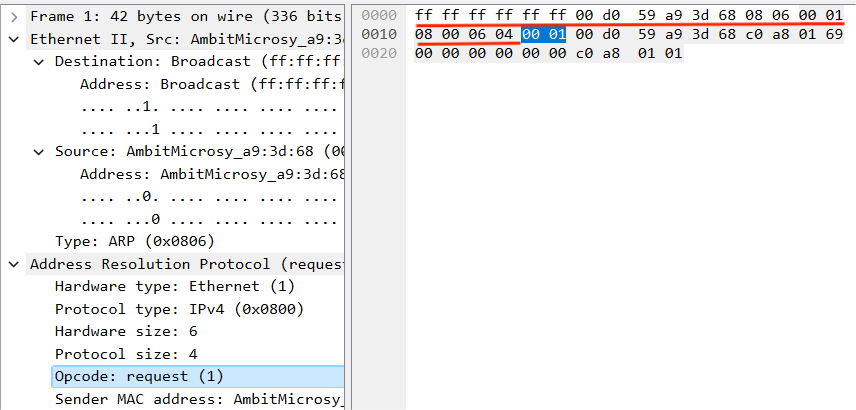
b） 在进行ARP响应的以太网帧的ARP有效负载部分中，操作码字段的值是多少？

c） 在ARP消息中，早期ARP请求的“答案”出现在哪里——具有正在查询其相应IP地址的以太网地址的机器的IP地址？

13. Now find the ARP reply that was sent in response to the ARP request.

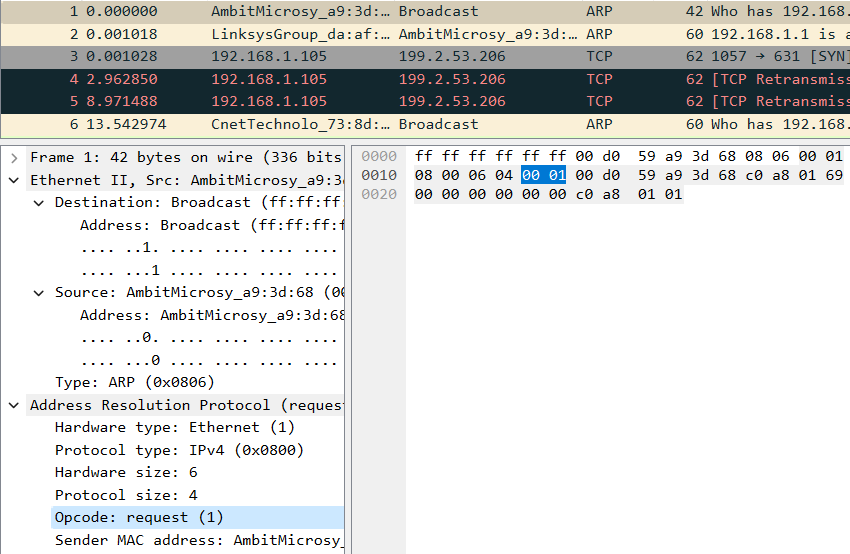
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

如图显示，共20个字节。

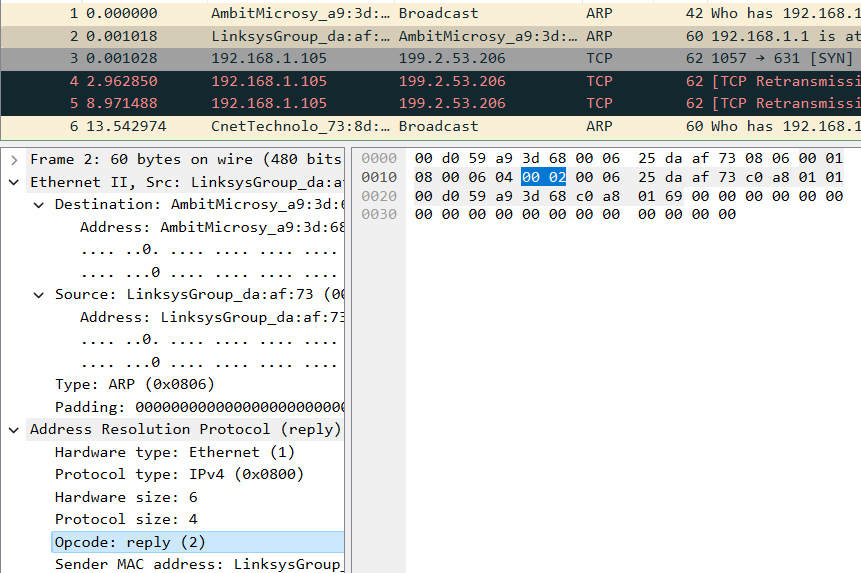


b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

第一次交手：操作码字段的值为1



第二次交手：操作码字段的值为2

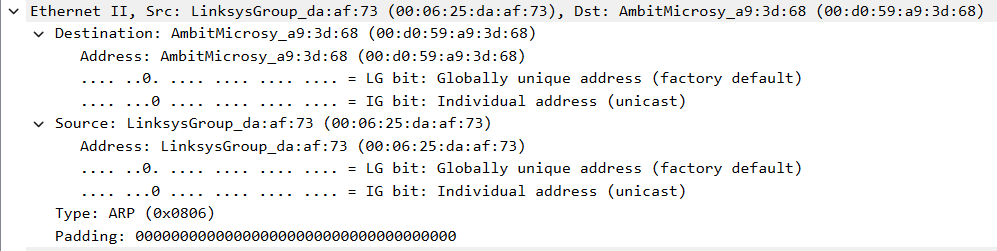


c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

早期ARP请求的“答案”出现在ARP回复消息的Sender IP address字段中，该字段指示正在查询其相应IP地址的以太网地址的机器的IP地址。

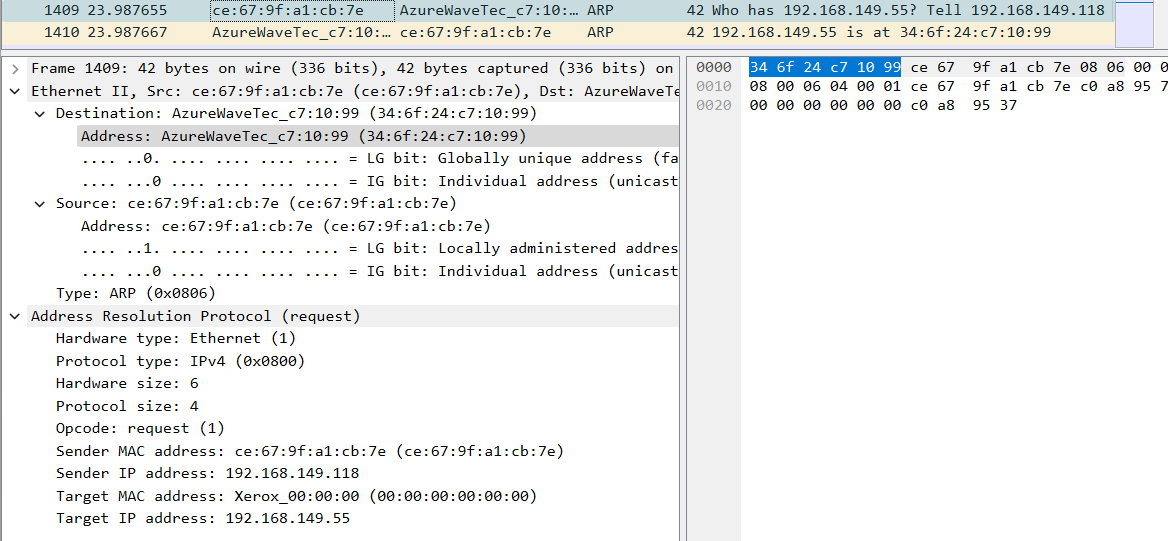


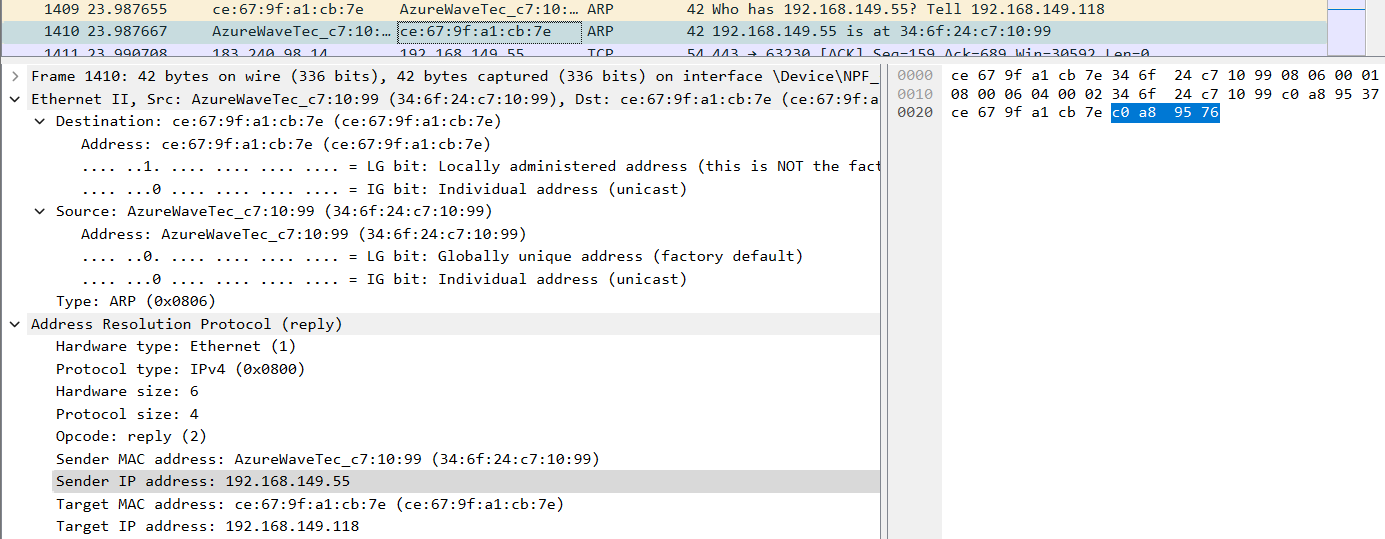
1. 文档问题14.在包含ARP回复消息的以太网帧中，源地址和目的地址的十六进制值是多少？
2. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?



1. 地址解析协议

对自己抓到的TCP包进行解析。以下是我打开百度的例子。本机客户端和百度建立TCP连接时需要经历三次握手，通过ARP实现。具体协议如下图。





第一次交手

源 MAC 地址：ce:67:9f:a1:cb:7e

源 IP 地址：c0 a8 95 76

目标 MAC 地址：00:00:00:00:00:00 （未知）

目标 IP 地址：c0 a8 95 37

第二次交手

源 MAC 地址：34:6f:24:c7:10:99

源 IP 地址：c0 a8 95 37

目标 MAC 地址：ce:67:9f:a1:cb:7e

目标 IP 地址：c0 a8 95 76

对应的上层协议是IPv4

How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

如图显示，共20个字节。

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

第一次交手：操作码字段的值为1

第二次交手：操作码字段的值为2