21级计算机科学与技术2班

计算机网络 实验十

**预习：**阅读课本2.3， 理论课本 IP， UDP及ICMP的相关内容。

**说明：本实验由1个同学独立完成。 需要用1台机器。**

**实验：ICMP 协议分析**

**实验9.1 ICMP/IP 协议分析**

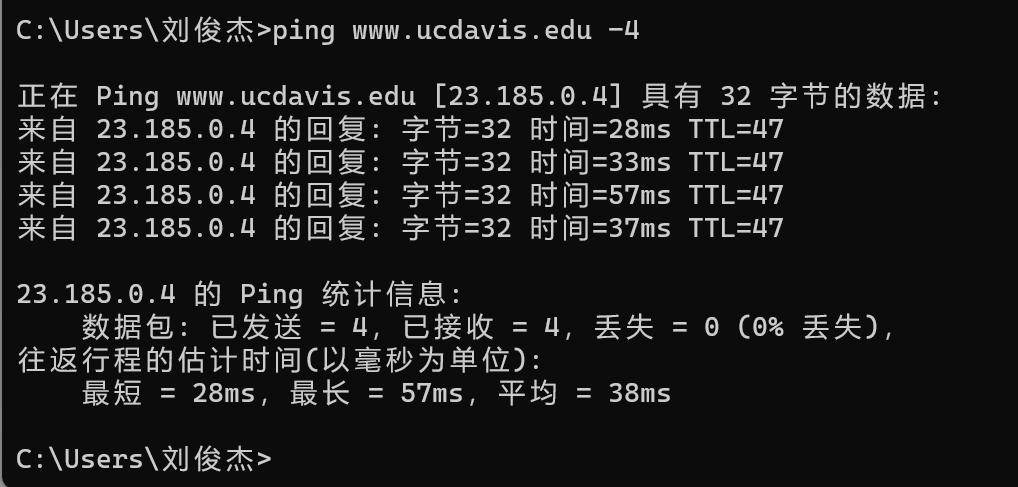
【目的】 利用wireshark 分析 ICMP及相关IP数据包服务；

【要求】

1）在实验机器终端启动wireshark 抓包,设置过滤显示IP，ICMP，UDP和TCP相关的信息；

2） 运行命令 ping 命令

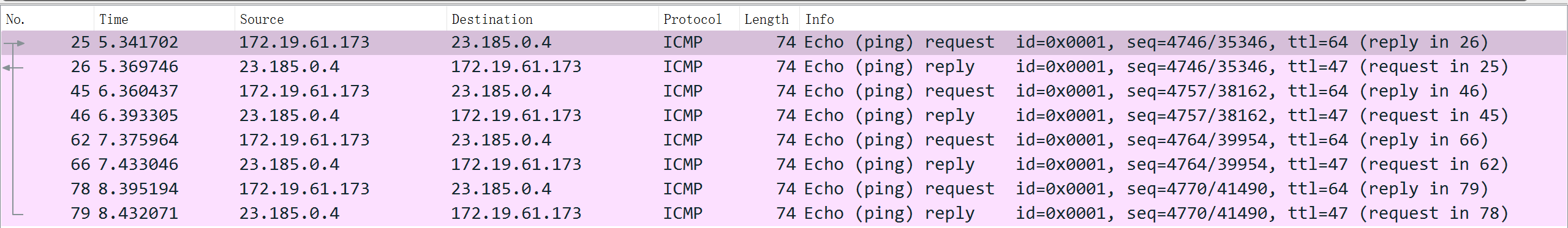
**ping [www.ucdavis.edu](http://www.ucdavis.edu)**



1. 截图显示网络层IP、ICMP协议,传输层协议的活动；观察期间数据传输；



**捕获到的数据包:**

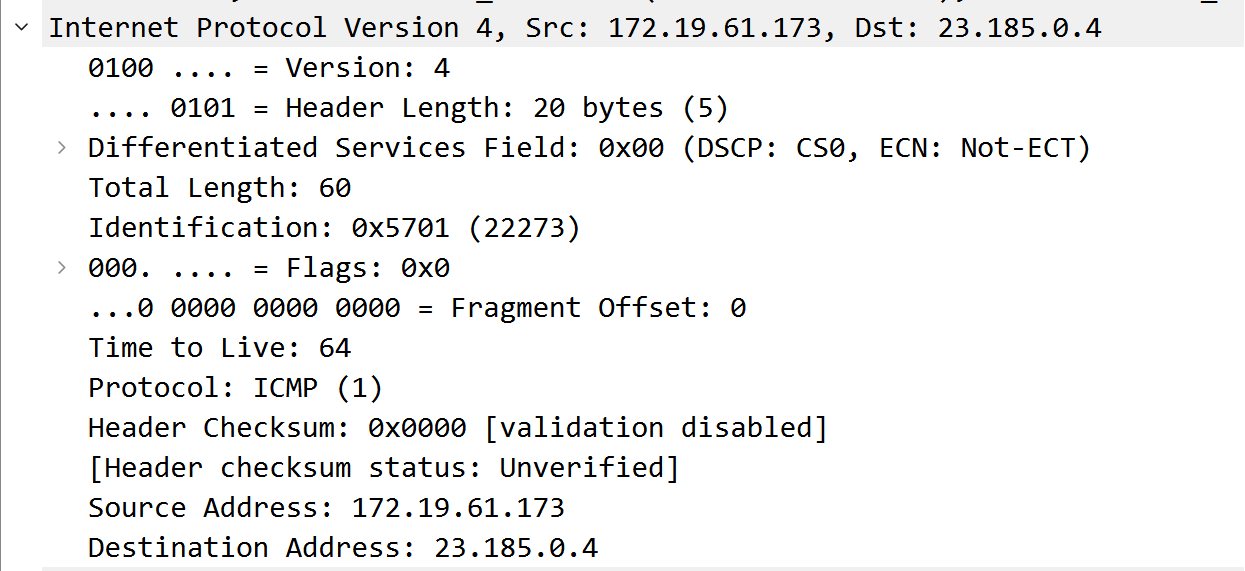


**Windows下的ping默认执行ping操作四次,ping指令采用的是 ICMP的网络传输协议，故包括请求和回复一共有四组ICMP报文。**

**点开一组ICMP报文来进行分析(序号为25的请求报文和序号为26的回复报文):**

**请求报文:**

**查看IP协议包部分:**



**Internet Protocol Version 4 (IPv4):**

**版本 (Version): 4**

**头部长度 (Header Length): 20字节（5个32位字）**

**区分服务字段 (Differentiated Services Field): 0x00**

**总长度 (Total Length): 60字节**

**标识 (Identification): 0x5701**

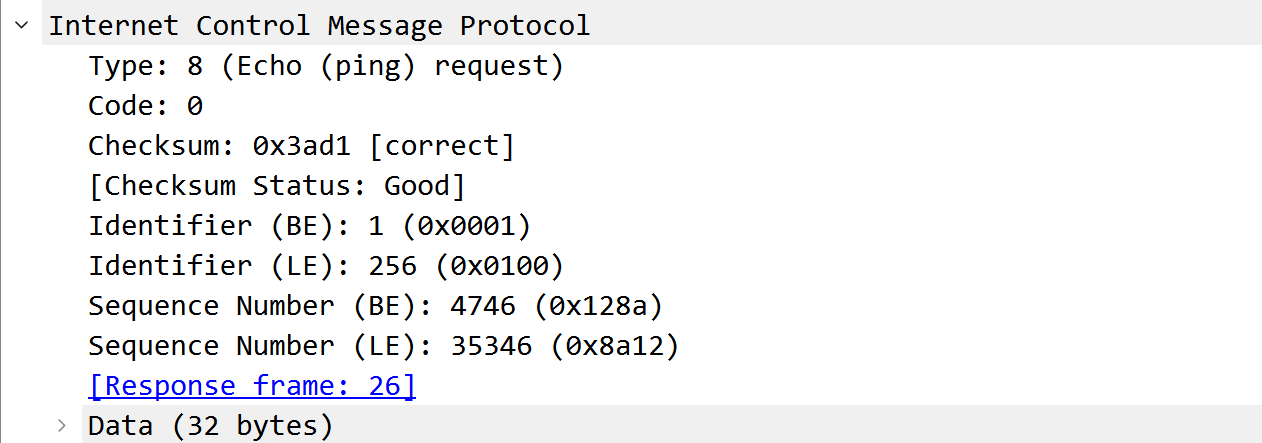
**生存时间 (Time to Live): 64**

**协议 (Protocol): ICMP (1)**

**源地址 (Source Address): 172.19.61.173**

**目标地址 (Destination Address): 23.185.0.4**

**再看其中的ICMP协议包部分:**

****

**类型 (Type): 8（Echo (ping)请求）**

**代码 (Code): 0**

**校验和 (Checksum): 0x3ad1**

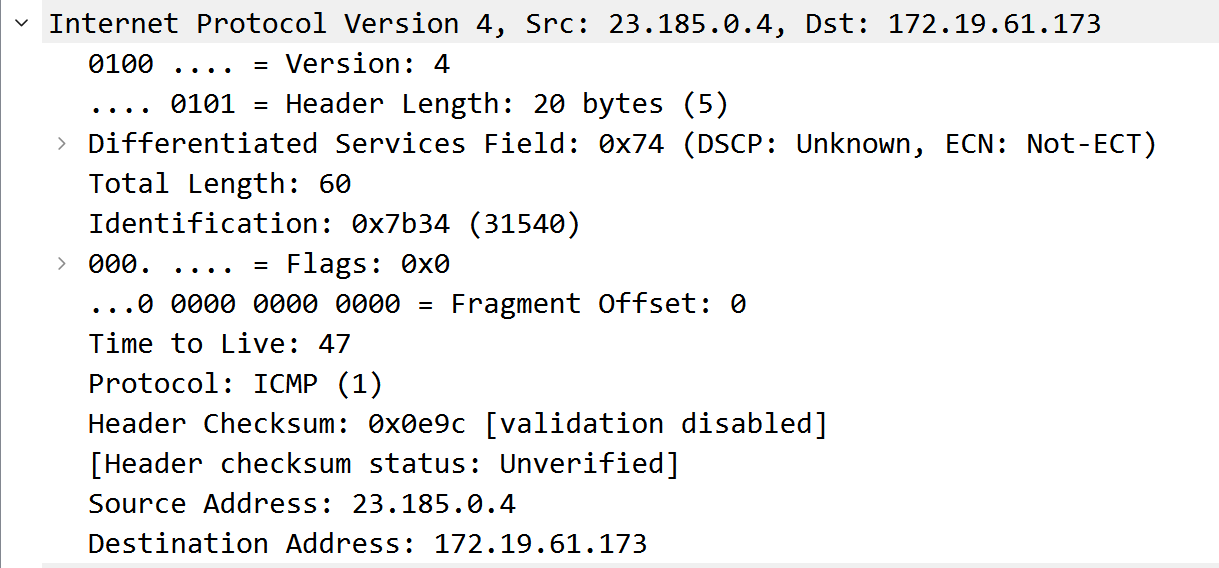
**标识符 (Identifier): 1 (0x0001)**

**序列号 (Sequence Number): 4746 (0x128a)**

**数据 (Data): 包含32字节的数据**

**回复报文：**

**查看IP协议包部分:**

****

**Internet Protocol Version 4 (IPv4):**

**版本 (Version): 4**

**头部长度 (Header Length): 20字节（5个32位字）**

**区分服务字段 (Differentiated Services Field): 0x74**

**总长度 (Total Length): 60字节**

**标识 (Identification): 0x7b34**

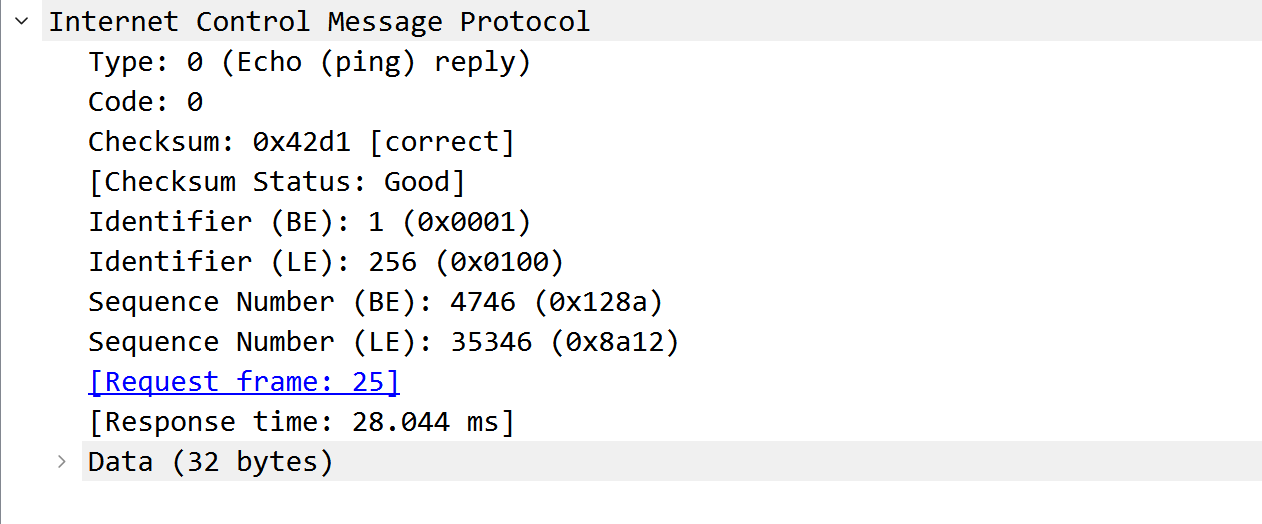
**生存时间 (Time to Live): 47**

**协议 (Protocol): ICMP (1)**

**源地址 (Source Address): 23.185.0.4**

**目标地址 (Destination Address): 172.19.61.173**

**ICMP协议数据包**

****

**类型 (Type): 0（Echo (ping)回复）**

**代码 (Code): 0**

**校验和 (Checksum): 0x42d1**

**标识符 (Identifier): 1 (0x0001)**

**序列号 (Sequence Number): 4746 (0x128a)**

**响应时间 (Response time): 28.044毫秒**

**数据 (Data): 包含32字节的数据**

**由此可见，ICMP消息被封装在IP数据包中。**

**将ICMP消息封装在IP数据包中，能确保它包含足够的网络层信息，以便在整个网络中正确传递。**

**实验9.2 tracert 应用 协议分析**

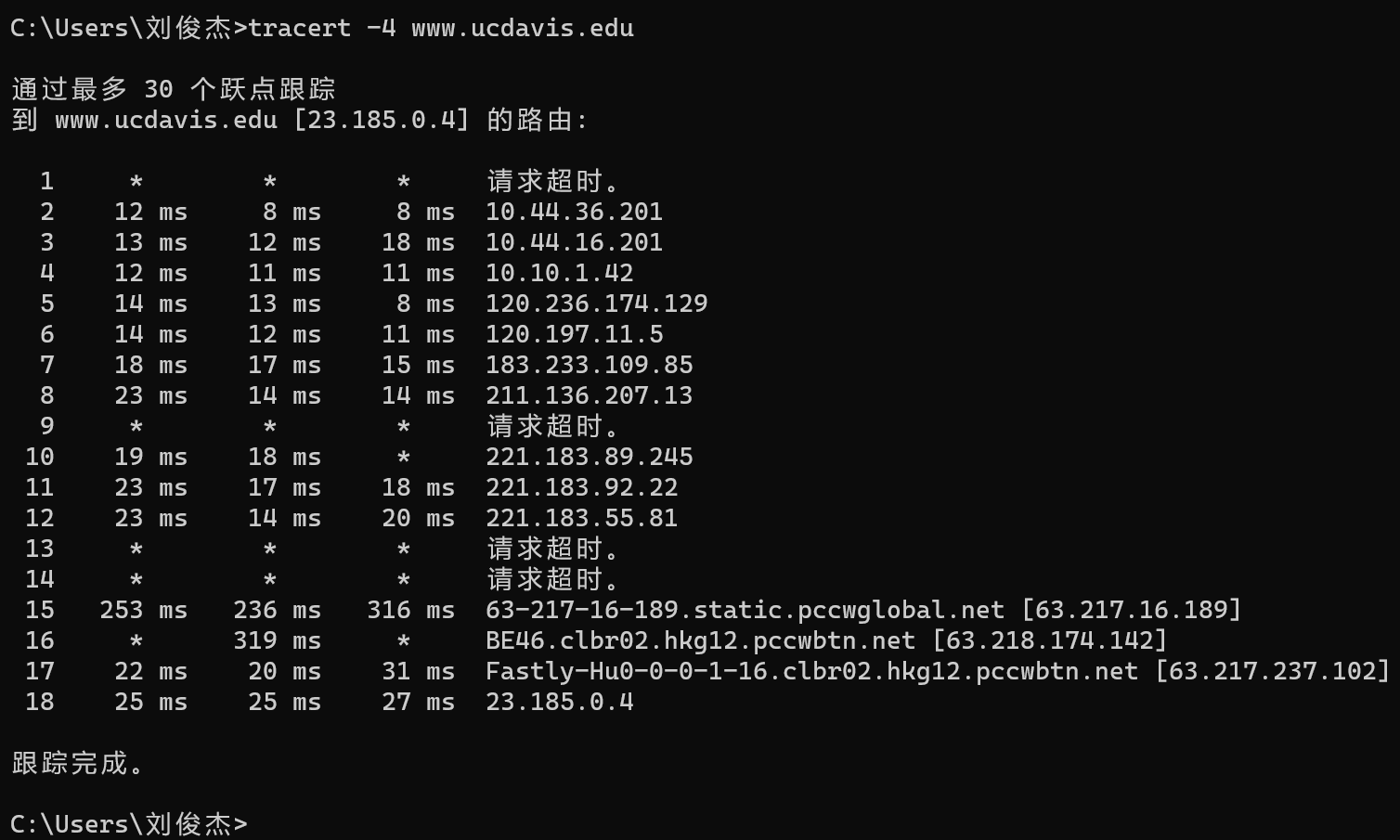
【目的】 利用wireshark 分析 ICMP/UDP 及相关IP服务；

【要求】

1）在实验机器终端启动wireshark 抓包,设置过滤显示IP，ICMP，UDP相关的信息；

2） 运行命令 traceroute 命令（windows 的是 tracert）

**Tracert [www.ucdavis.edu](http://www.ucdavis.edu)**

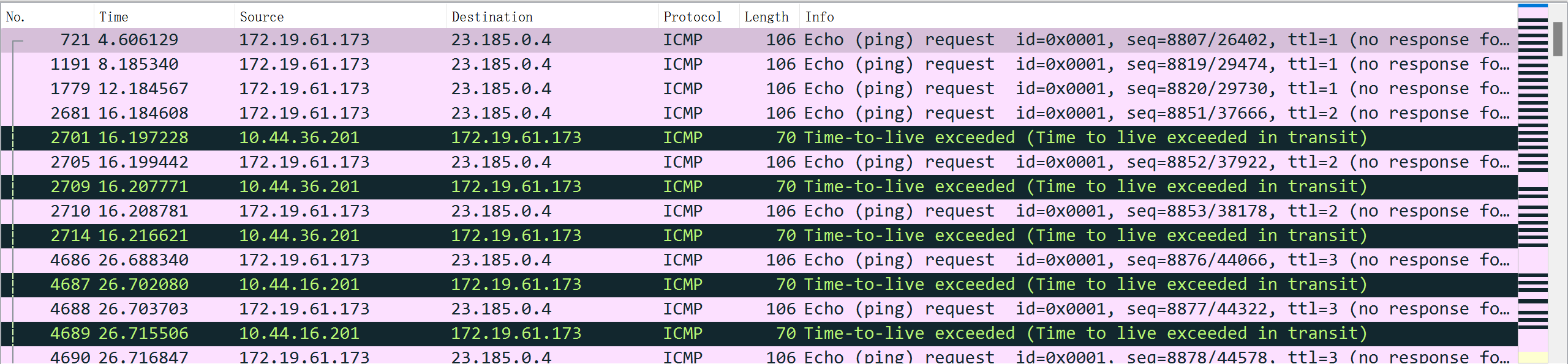
****

**从tracert的结果可以看出，从源主机到目的主机之间经过了17个路由器。**

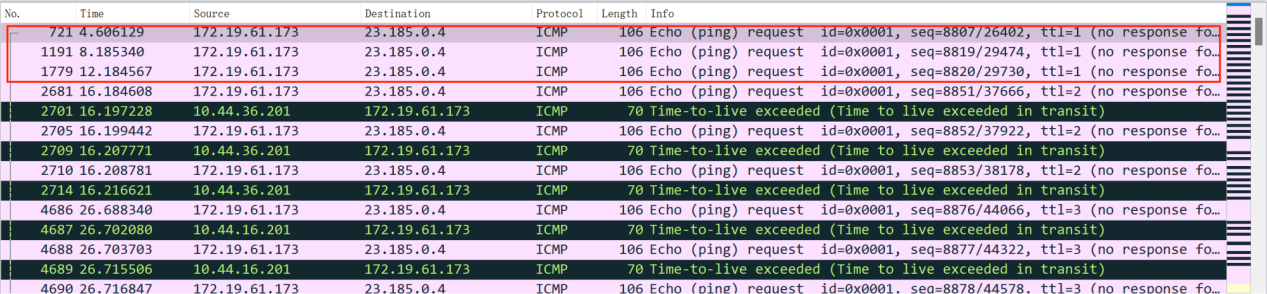
3） 截图显示网络层IP、ICMP协议，传输层及UDP 相关的信息；观察期间数据传输；

4） 分析并解释以上实验结果。

**捕获到的部分相关报文:**

****

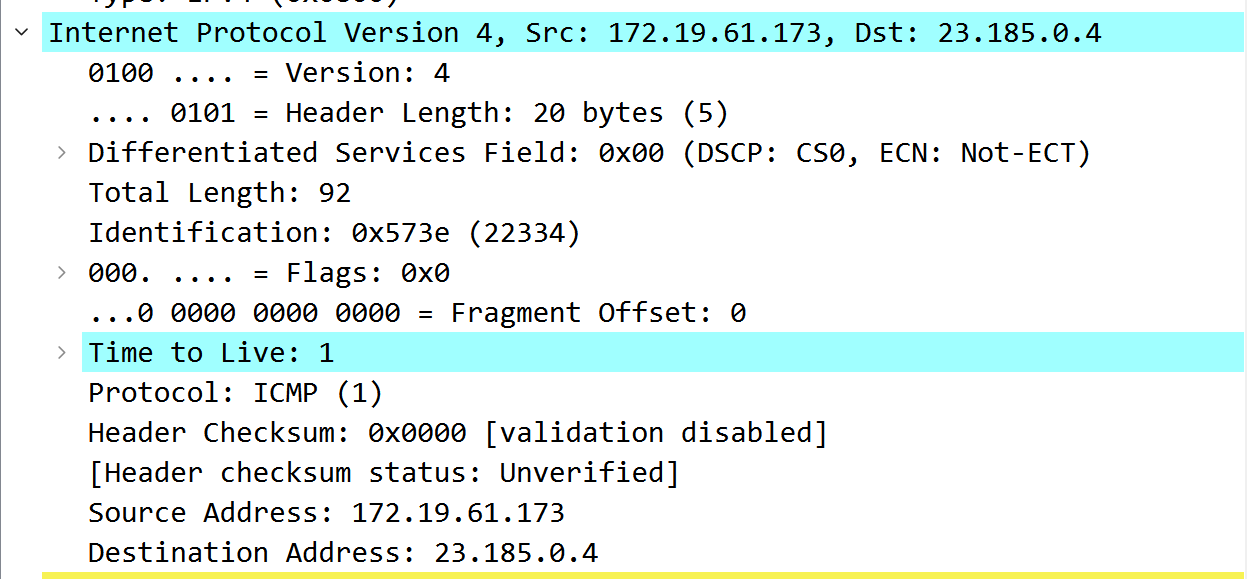
**首先分析TTL=1的数据包:**

****

**可以看到显示了no request found ,说明没有收到相应回复的报文，这说明数据包未达到目的主机或者是回复的报文被阻拦。**

**打开序号为721的报文分析:**

**IP数据包:**

****

**版本：4**

**标头长度：20字节（5）**

**区分服务字段：CS0，显式拥塞通知：非ECT**

**总长度：92字节**

**标识：0x573e (22334)**

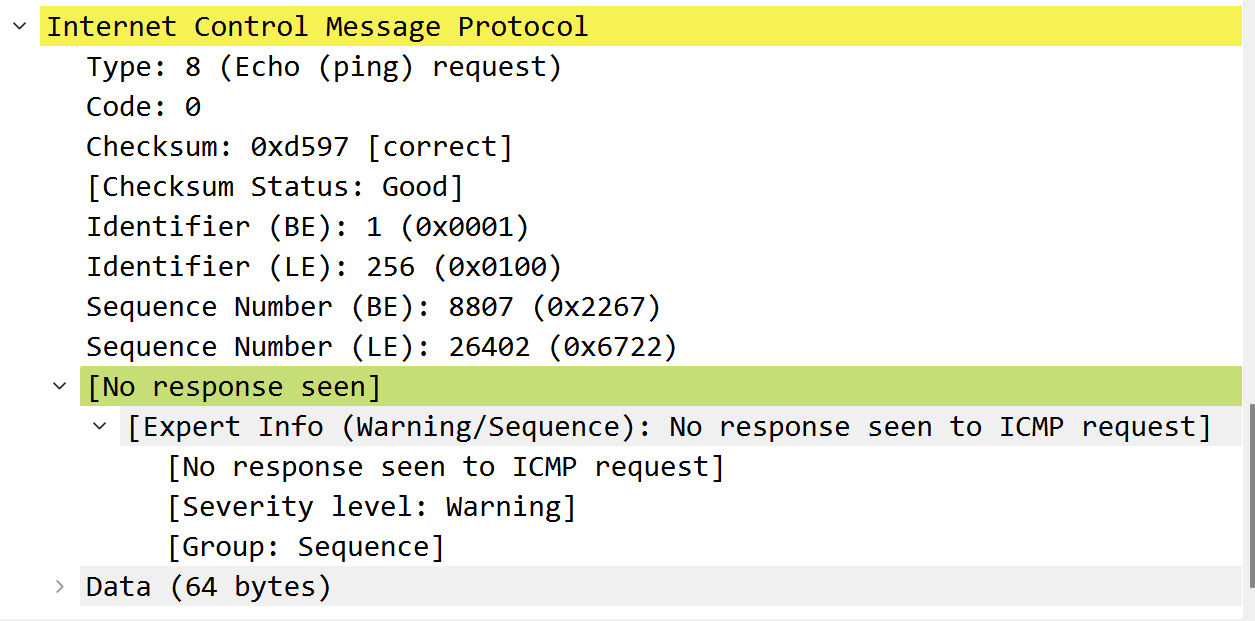
**存活时间（TTL）：1**

**协议：ICMP (1)**

**源IP地址：172.19.61.173**

**目标IP地址：23.185.0.4**

**ICMP数据包:**

****

**类型：8（回显请求）**

**代码：0**

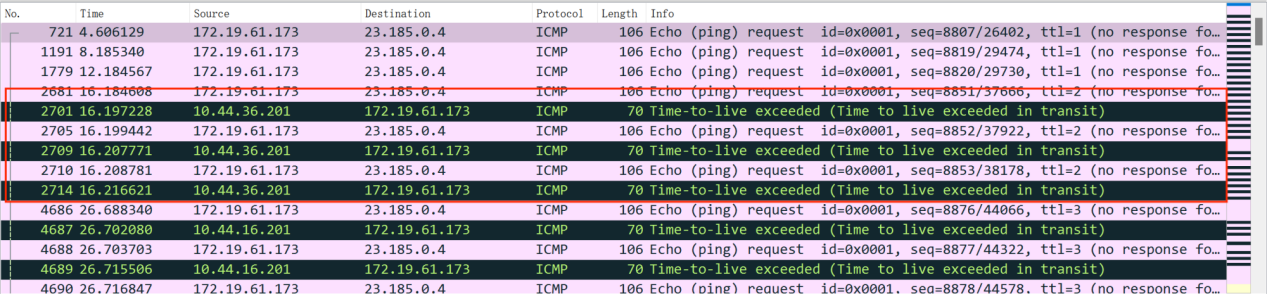
**校验和：0xd597 [正确]**

**标识符（大端序）：1 (0x0001)**

**序列号（大端序）：8807 (0x2267)**

**数据（64字节）**

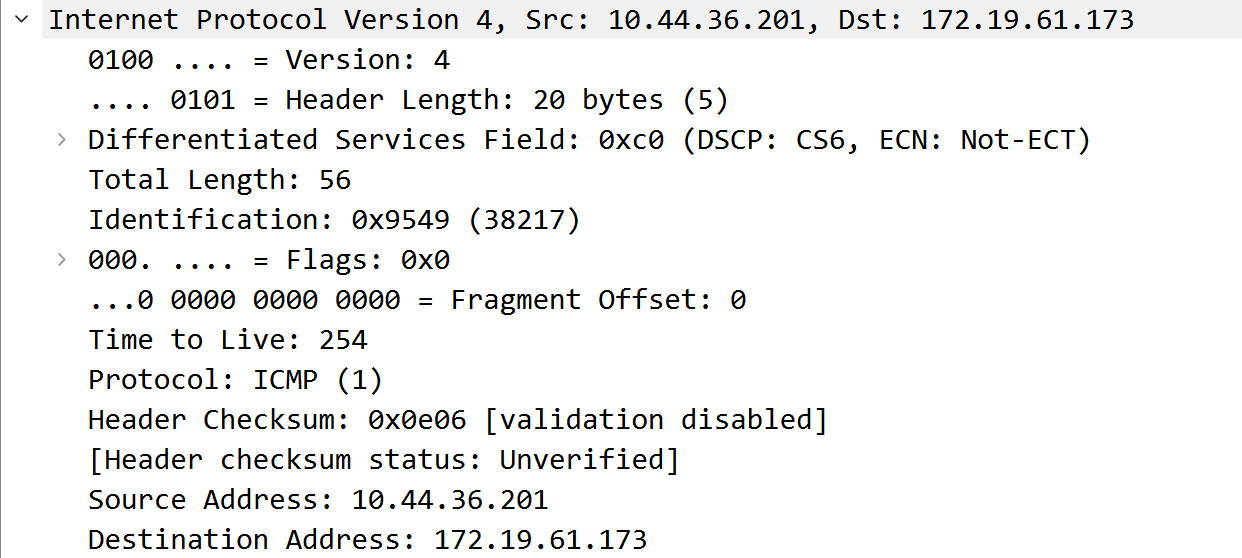
**再分析TTL=2的数据包:**

****

**可以看到有Time to live exceeded in transit的报文。这个消息通常由路由器生成，用于指示数据包在传输过程中经过的路由器数量超过了其生存时间 (TTL)。每经过一个路由器，TTL 减少，当 TTL 达到零时，路由器会丢弃该数据包并生成此 ICMP 消息。在这种情况下，数据包从 IP 地址为 10.44.36.201 的源主机发送到 IP 地址为 172.19.61.173 的目标主机，但在传输过程中 TTL 被耗尽，导致路由器生成此 ICMP 消息。**

**分析序号为2701的报文:**

**IP数据包:**

****

**版本：4**

**首部长度：20字节（5）**

**区分服务字段：0xc0（DSCP: CS6, ECN: Not-ECT）**

**总长度：56字节**

**标识：0x9549（38217）**

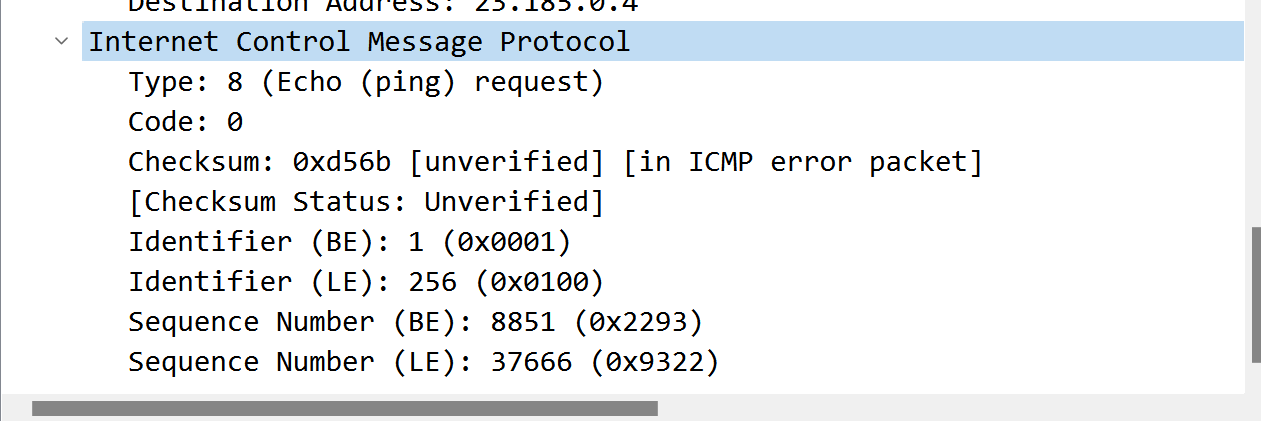
**存活时间（TTL）：254**

**协议：ICMP（1）**

**源IP地址：10.44.36.201**

**目标IP地址：172.19.61.173**

**ICMP数据包:**

****

**类型：11（Time-to-live exceeded）**

**代码：0（Time to live exceeded in transit）**

**校验和：0xf4ff [正确]**

**未使用字段：00000000**

**内部的IPv4首部：**

**版本：4**

**首部长度：20字节（5）**

**区分服务字段：0x00（DSCP: CS0, ECN: Not-ECT）**

**总长度：92字节**

**标识：0x5741（22337）**

**存活时间（TTL）：1**

**协议：ICMP（1）**

**源IP地址：172.19.61.173**

**目标IP地址：23.185.0.4**

**ICMP内部消息：**

**类型：8（Echo请求）**

**代码：0**

**校验和：0xd56b [未验证]**

**标识符（大端序）：1（0x0001）**

**序列号（大端序）：8851（0x2293）**

**这个数据包的情景是一个 ICMP Time-to-live exceeded 消息，表明 TTL 在传输过程中被耗尽。发生在源IP地址为10.44.36.201的主机向目标IP地址为172.19.61.173的主机发送的 ICMP Echo请求（ping）的传输中,表明TTL 在传输过程中被耗尽。**

**实验报告：**

1. 【报告要求】 实验过程、结果截图和对于各个实验的网络层数据包的分析与说明。
2. 12月2日（周日）晚上11:59前提交实验报告电子版。
3. 到请发邮件到： zhanghy365@mail2.sysu.edu.cn