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

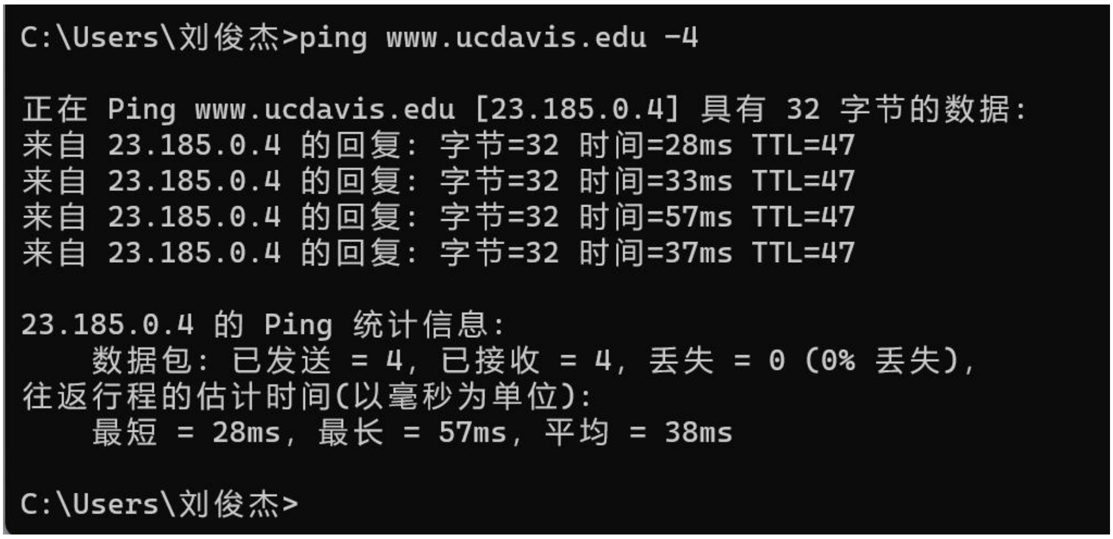
【目的】 利用 wireshark 分析 ICMP 及相关 IP 数据包服务；

【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；

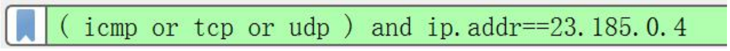
2） 运行命令 ping 命令

ping www.ucdavis.edu



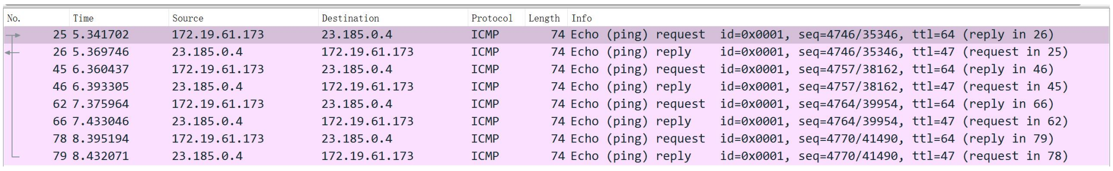
```
C:\Users\刘俊杰>ping www.ucdavis.edu -4

正在 Ping www.ucdavis.edu [23.185.0.4] 具有 32 字节的数据:
来自 23.185.0.4 的回复: 字节=32 时间=28ms TTL=47
来自 23.185.0.4 的回复: 字节=32 时间=33ms TTL=47
来自 23.185.0.4 的回复: 字节=32 时间=57ms TTL=47
来自 23.185.0.4 的回复: 字节=32 时间=37ms TTL=47

23.185.0.4 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 28ms，最长 = 57ms，平均 = 38ms

C:\Users\刘俊杰>
```

3） 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；



```
( icmp or tcp or udp ) and ip.addr==23.185.0.4
```

捕获到的数据包:



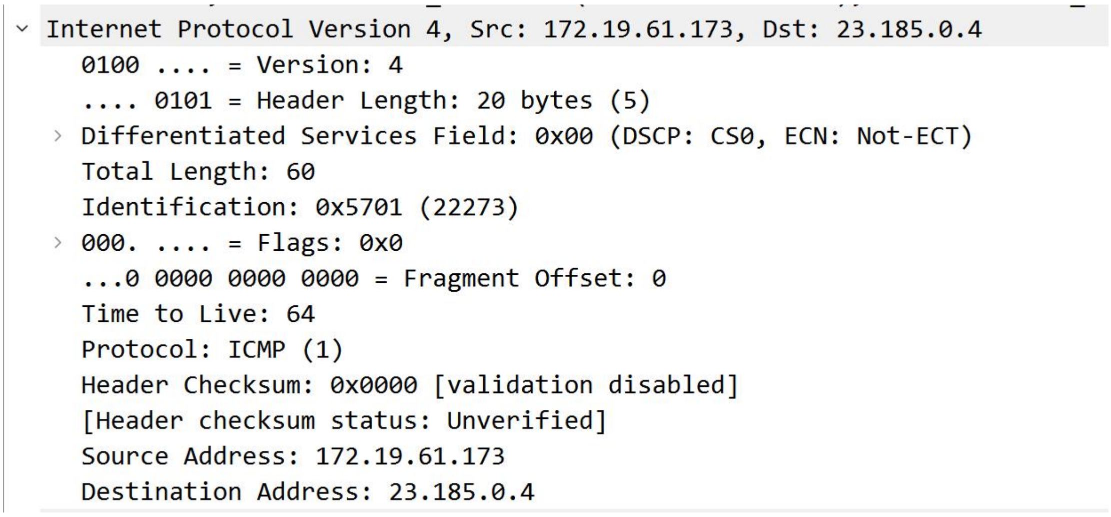
No.	Time	Source	Destination	Protocol	Length	Info
25	5.341702	172.19.61.173	23.185.0.4	ICMP	74	Echo (ping) request id=0x0001, seq=4746/35346, ttl=64 (reply in 26)
26	5.369746	23.185.0.4	172.19.61.173	ICMP	74	Echo (ping) reply id=0x0001, seq=4746/35346, ttl=47 (request in 25)
45	6.360437	172.19.61.173	23.185.0.4	ICMP	74	Echo (ping) request id=0x0001, seq=4757/38162, ttl=64 (reply in 46)
46	6.393305	23.185.0.4	172.19.61.173	ICMP	74	Echo (ping) reply id=0x0001, seq=4757/38162, ttl=47 (request in 45)
62	7.375964	172.19.61.173	23.185.0.4	ICMP	74	Echo (ping) request id=0x0001, seq=4764/39954, ttl=64 (reply in 66)
66	7.433046	23.185.0.4	172.19.61.173	ICMP	74	Echo (ping) reply id=0x0001, seq=4764/39954, ttl=47 (request in 62)
78	8.395194	172.19.61.173	23.185.0.4	ICMP	74	Echo (ping) request id=0x0001, seq=4770/41490, ttl=64 (reply in 79)
79	8.432071	23.185.0.4	172.19.61.173	ICMP	74	Echo (ping) reply id=0x0001, seq=4770/41490, ttl=47 (request in 78)

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:

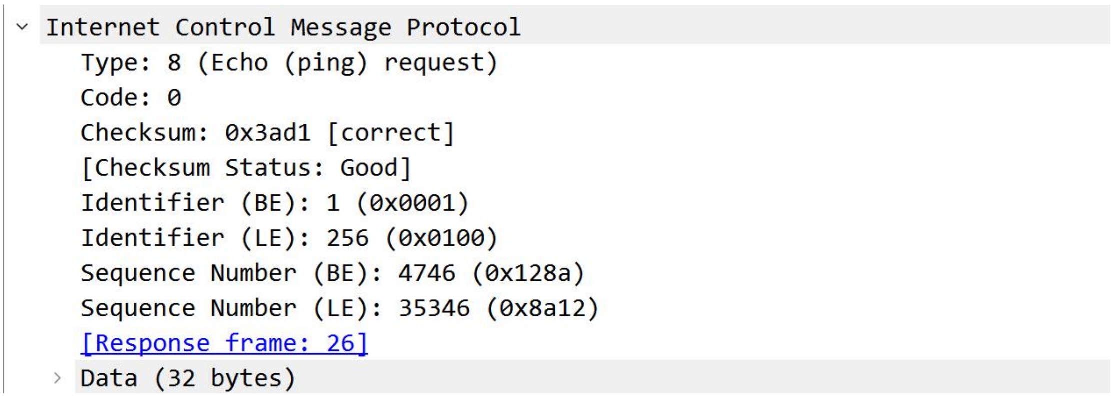
查看 IP 协议包部分:



```
⌄ Internet Protocol Version 4, Src: 172.19.61.173, Dst: 23.185.0.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x5701 (22273)
  › 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.19.61.173
    Destination Address: 23.185.0.4
```

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:

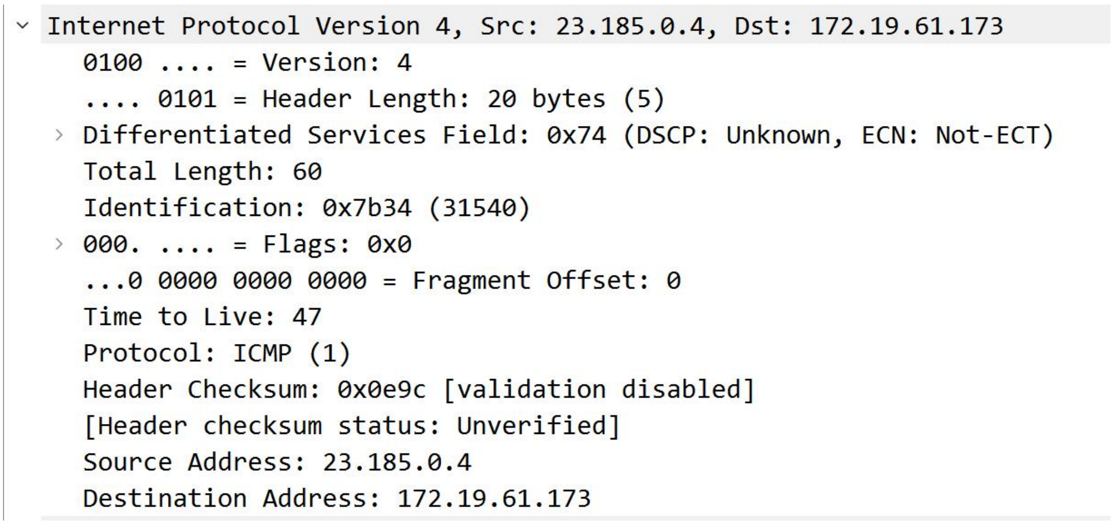


```
⌄ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x3ad1 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 4746 (0x128a)
    Sequence Number (LE): 35346 (0x8a12)
    [Response frame: 26]
  › Data (32 bytes)
```

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, Src: 23.185.0.4, Dst: 172.19.61.173
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x74 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x7b34 (31540)
  › 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 47
    Protocol: ICMP (1)
    Header Checksum: 0x0e9c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 23.185.0.4
    Destination Address: 172.19.61.173
```

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

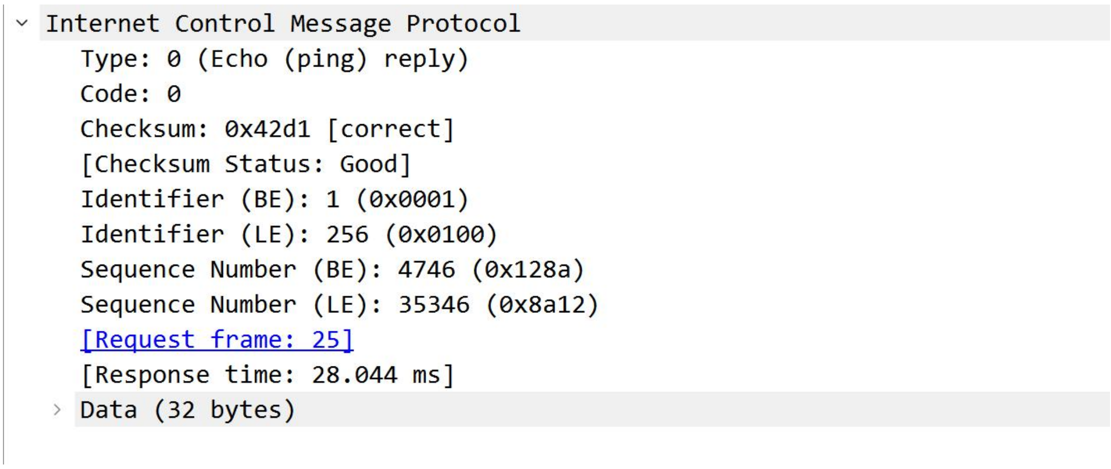
生存时间（Time to Live): 47

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



```
⌄ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x42d1 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 4746 (0x128a)
    Sequence Number (LE): 35346 (0x8a12)
    [Request frame: 25]
    [Response time: 28.044 ms]
  › Data (32 bytes)
```

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

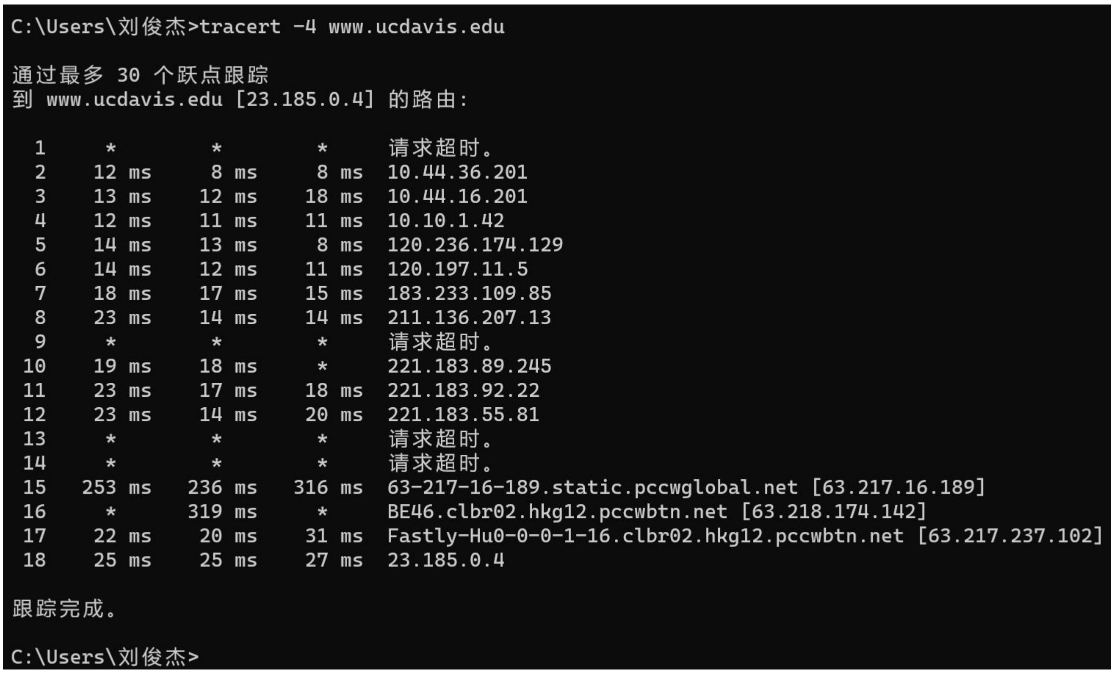
【目的】 利用 wireshark 分析 ICMP/UDP 及相关 IP 服务；

【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



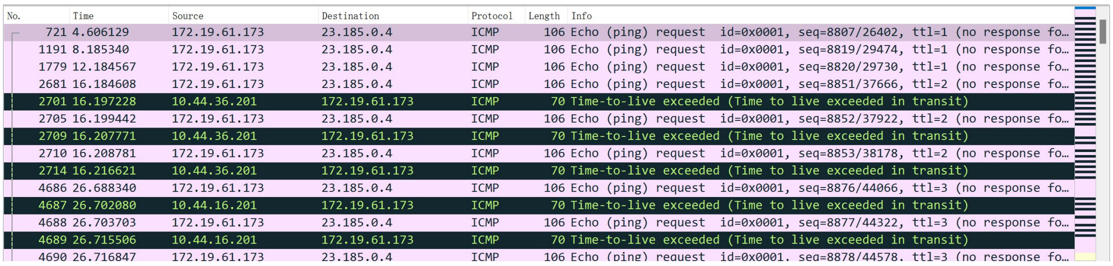
```
C:\Users\刘俊杰>tracert -4 www.ucdavis.edu

通过最多 30 个跃点跟踪
到 www.ucdavis.edu [23.185.0.4] 的路由:

  1     *        *        *     请求超时。
  2    12 ms     8 ms     8 ms  10.44.36.201
  3    13 ms    12 ms    18 ms  10.44.16.201
  4    12 ms    11 ms    11 ms  10.10.1.42
  5    14 ms    13 ms     8 ms  120.236.174.129
  6    14 ms    12 ms    11 ms  120.197.11.5
  7    18 ms    17 ms    15 ms  183.233.109.85
  8    23 ms    14 ms    14 ms  211.136.207.13
  9     *        *        *     请求超时。
 10    19 ms    18 ms     *     221.183.89.245
 11    23 ms    17 ms    18 ms  221.183.92.22
 12    23 ms    14 ms    20 ms  221.183.55.81
 13     *        *        *     请求超时。
 14     *        *        *     请求超时。
 15   253 ms   236 ms   316 ms  63-217-16-189.static.pccwglobal.net [63.217.16.189]
 16     *      319 ms     *     BE46.clbr02.hkg12.pccwbtn.net [63.218.174.142]
 17    22 ms    20 ms    31 ms  Fastly-Hu0-0-0-1-16.clbr02.hkg12.pccwbtn.net [63.217.237.102]
 18    25 ms    25 ms    27 ms  23.185.0.4

跟踪完成。

C:\Users\刘俊杰>
```

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；

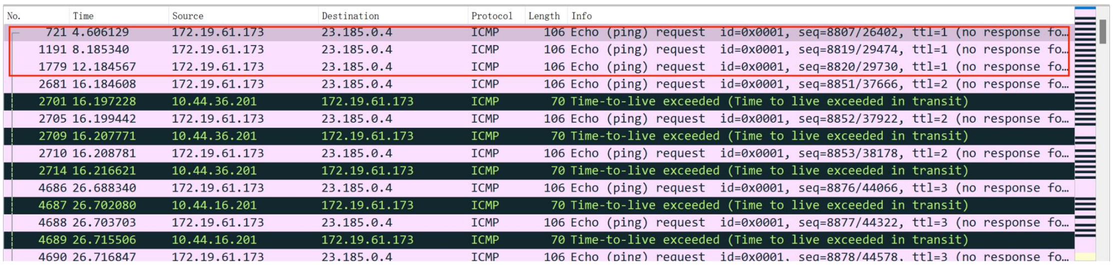
4） 分析并解释以上实验结果。

捕获到的部分相关报文:



No.	Time	Source	Destination	Protocol	Length	Info
721	4.606129	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8807/26402, ttl=1 (no response fo…
1191	8.185340	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8819/29474, ttl=1 (no response fo…
1779	12.184567	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8820/29730, ttl=1 (no response fo…
2681	16.184608	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8851/37666, ttl=2 (no response fo…
2701	16.197228	10.44.36.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2705	16.199442	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8852/37922, ttl=2 (no response fo…
2709	16.207771	10.44.36.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2710	16.208781	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8853/38178, ttl=2 (no response fo…
2714	16.216621	10.44.36.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4686	26.688340	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8876/44066, ttl=3 (no response fo…
4687	26.702080	10.44.16.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4688	26.703703	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8877/44322, ttl=3 (no response fo…
4689	26.715506	10.44.16.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4690	26.716847	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8878/44578, ttl=3 (no response fo…

首先分析 TTL=1 的数据包:

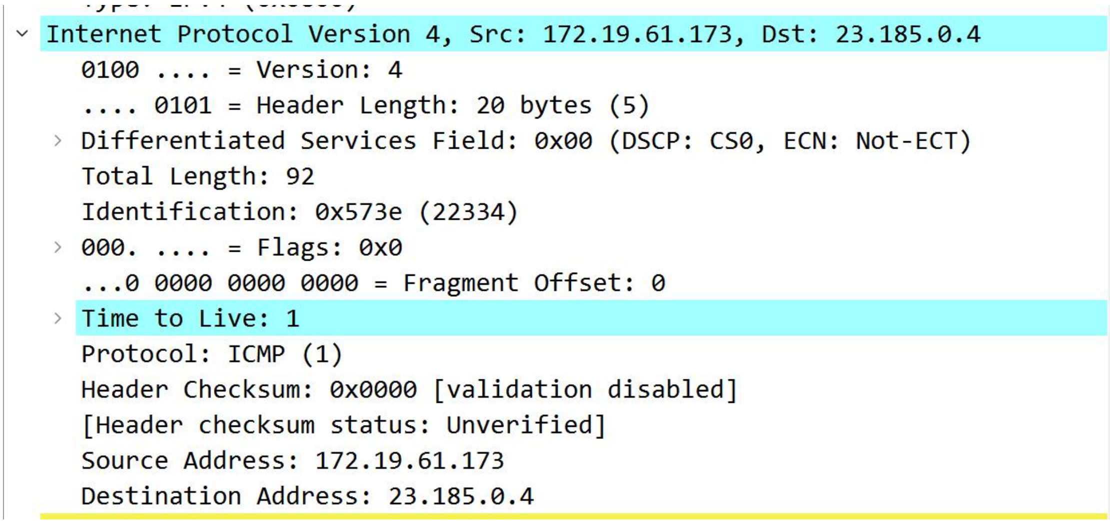


No.	Time	Source	Destination	Protocol	Length	Info
721	4.606129	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8807/26402, ttl=1 (no response fo…
1191	8.185340	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8819/29474, ttl=1 (no response fo…
1779	12.184567	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8820/29730, ttl=1 (no response fo…
2681	16.184608	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8851/37666, ttl=2 (no response fo…
2701	16.197228	10.44.36.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2705	16.199442	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8852/37922, ttl=2 (no response fo…
2709	16.207771	10.44.36.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2710	16.208781	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8853/38178, ttl=2 (no response fo…
2714	16.216621	10.44.36.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4686	26.688340	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8876/44066, ttl=3 (no response fo…
4687	26.702080	10.44.16.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4688	26.703703	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8877/44322, ttl=3 (no response fo…
4689	26.715506	10.44.16.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4690	26.716847	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8878/44578, ttl=3 (no response fo…

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:



```
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 172.19.61.173, Dst: 23.185.0.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x573e (22334)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.19.61.173
    Destination Address: 23.185.0.4
```

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)

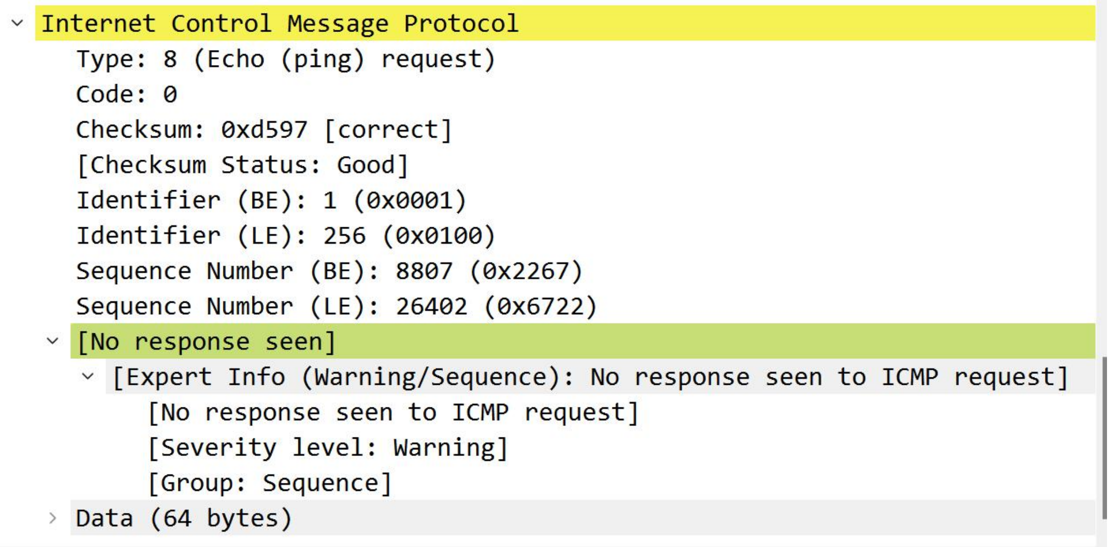
存活时间（TTL）：1

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:



```
⌄ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xd597 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 8807 (0x2267)
    Sequence Number (LE): 26402 (0x6722)
  ⌄ [No response seen]
    ⌄ [Expert Info (Warning/Sequence): No response seen to ICMP request]
        [No response seen to ICMP request]
        [Severity level: Warning]
        [Group: Sequence]
  › Data (64 bytes)
```

类型：8（回显请求）

代码：0

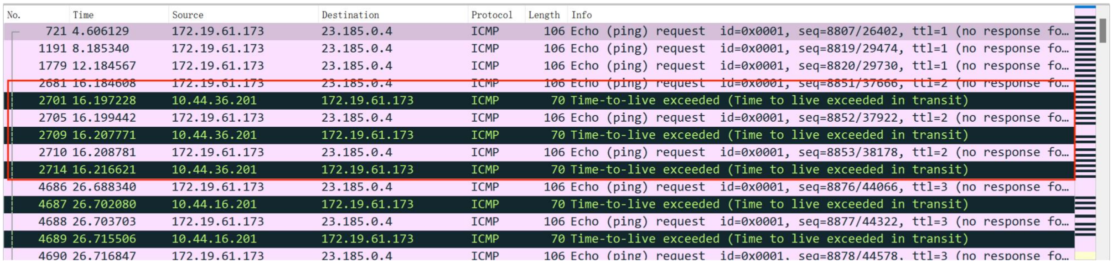
校验和：0xd597 [正确]

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:

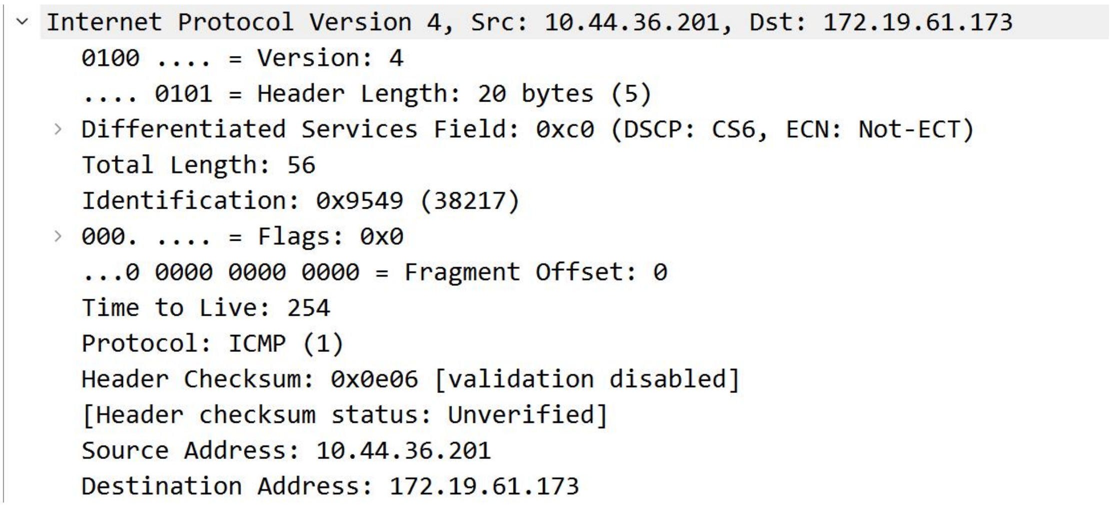


No.	Time	Source	Destination	Protocol	Length	Info
721	4.606129	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8807/26402, ttl=1 (no response fo…
1191	8.185340	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8819/29474, ttl=1 (no response fo…
1779	12.184567	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8820/29730, ttl=1 (no response fo…
2681	16.184608	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8851/37666, ttl=2 (no response fo…
2701	16.197228	10.44.36.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2705	16.199442	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8852/37922, ttl=2 (no response fo…
2709	16.207771	10.44.36.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2710	16.208781	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8853/38178, ttl=2 (no response fo…
2714	16.216621	10.44.36.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4686	26.688340	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8876/44066, ttl=3 (no response fo…
4687	26.702080	10.44.16.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4688	26.703703	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8877/44322, ttl=3 (no response fo…
4689	26.715506	10.44.16.201	172.19.61.173	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
4690	26.716847	172.19.61.173	23.185.0.4	ICMP	106	Echo (ping) request id=0x0001, seq=8878/44578, ttl=3 (no response fo…

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:



```
⌄ Internet Protocol Version 4, Src: 10.44.36.201, Dst: 172.19.61.173
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x9549 (38217)
  › 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 254
    Protocol: ICMP (1)
    Header Checksum: 0x0e06 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.44.36.201
    Destination Address: 172.19.61.173
```

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）

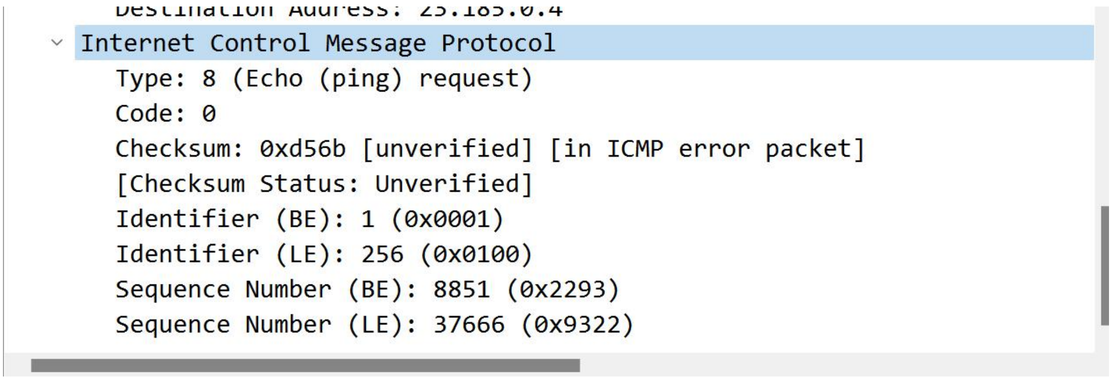
存活时间（TTL）：254

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:



```
      Destination Address: 23.185.0.4
  ⌄ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xd56b [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 8851 (0x2293)
      Sequence Number (LE): 37666 (0x9322)
```

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