计算机网络实验报告

课程名称_____计算机网络_____成绩评定_____

实验项目名称_____Wireshark 综合实验（1）_____指导教师____张伟____

实验项目编号__实验 5_____实验项目类型_____实验地点_____

学生姓名_____密语_____学号___202200460104_____

学院_____网络空间安全_____专业___网络空间安全_____

实验时间__2024__年__4__月__23__日

一、实验目的

1. 熟悉 ICMP 的协议格式。
2. 理解 ping 的运作机制。
3. 理解 traceroute 的运作机制。
4. 理解 VPN 的运作机制。

二、实验步骤与结果

任务一：

在 cmd 中执行 ping -4 -n 10 www.sdu.edu.cn，向域名对应的主机发送 10 个消息，同时用 wireshark 进行捕获。

1. 你所使用的主机 ip 地址是多少？目标主机的 ip 地址是多少？

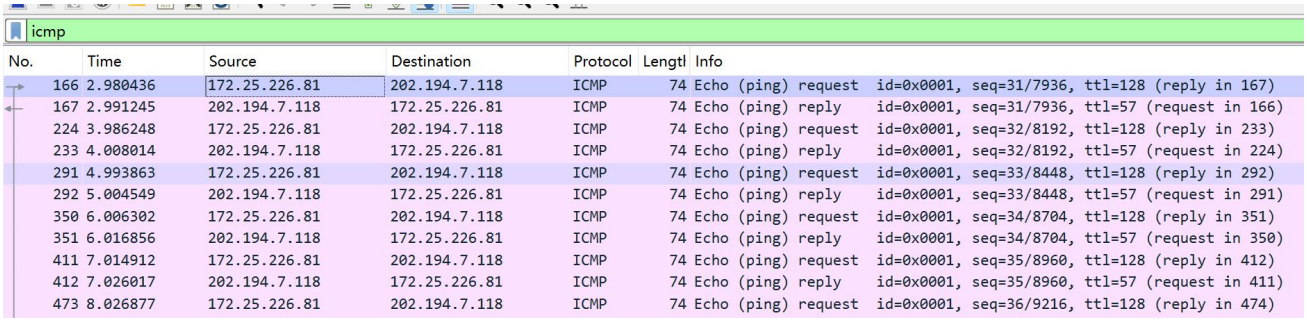
首先，从 ping 的回显中不难看出，目标主机的 ip 是 202.194.7.118

```
C:\Users\86135>ping -4 -n 10 www.sdu.edu.cn

正在 Ping www.sdu.edu.cn [202.194.7.118] 具有 32 字节的数据:
来自 202.194.7.118 的回复: 字节=32 时间=11ms TTL=57
来自 202.194.7.118 的回复: 字节=32 时间=22ms TTL=57
来自 202.194.7.118 的回复: 字节=32 时间=11ms TTL=57
来自 202.194.7.118 的回复: 字节=32 时间=10ms TTL=57
来自 202.194.7.118 的回复: 字节=32 时间=11ms TTL=57
来自 202.194.7.118 的回复: 字节=32 时间=32ms TTL=57
来自 202.194.7.118 的回复: 字节=32 时间=11ms TTL=57
来自 202.194.7.118 的回复: 字节=32 时间=11ms TTL=57
来自 202.194.7.118 的回复: 字节=32 时间=16ms TTL=57
来自 202.194.7.118 的回复: 字节=32 时间=11ms TTL=57

202.194.7.118 的 Ping 统计信息:
    数据包: 已发送 = 10, 已接收 = 10, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 10ms, 最长 = 32ms, 平均 = 14ms
```

其次，在捕获到的 ICMP 报文中，可以看出目标主机的 ip 和本机的 ip



icmp

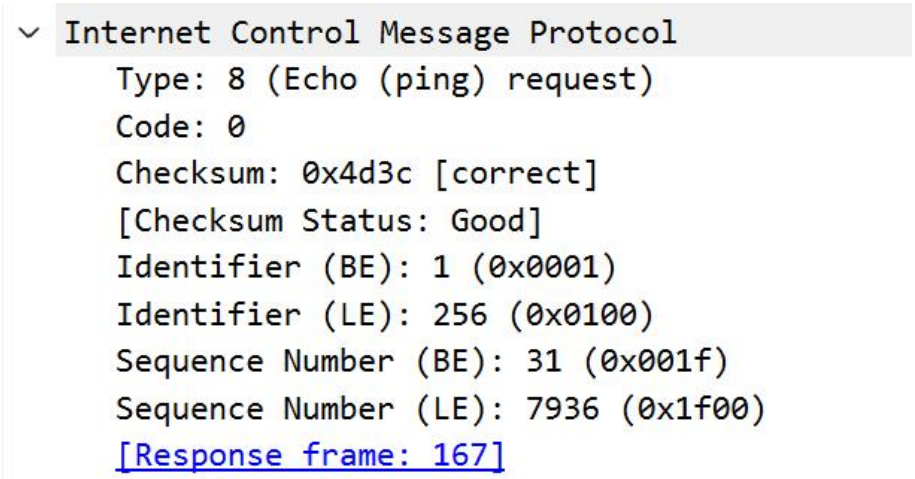
No.	Time	Source	Destination	Protocol	Lengtl	Info
166	2.980436	172.25.226.81	202.194.7.118	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 167)
167	2.991245	202.194.7.118	172.25.226.81	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=57 (request in 166)
224	3.986248	172.25.226.81	202.194.7.118	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 233)
233	4.008014	202.194.7.118	172.25.226.81	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=57 (request in 224)
291	4.993863	172.25.226.81	202.194.7.118	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 292)
292	5.004549	202.194.7.118	172.25.226.81	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=57 (request in 291)
350	6.006302	172.25.226.81	202.194.7.118	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 351)
351	6.016856	202.194.7.118	172.25.226.81	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=57 (request in 350)
411	7.014912	172.25.226.81	202.194.7.118	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 412)
412	7.026017	202.194.7.118	172.25.226.81	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=57 (request in 411)
473	8.026877	172.25.226.81	202.194.7.118	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 474)

第一条为请求报文，是从本机发送到目的主机的，由此可见本机的 IP 地址为 172.25.226.81

2. 为什么 ICMP 数据包没有源端口号和目的端口号?

因为 ICMP 是网络层的协议，不需要传输层 TCP 或 UDP 的承载，因此不需要源端口号和目的端口号，只需要源地址和目的地址即可。

3. 查看任意的 ping 请求数据包，ICMP 类型和代码是什么？该 ICMP 数据包还有哪些其他字段？校验和、序号和标识符字段有多少字节?



```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3c [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 31 (0x001f)
    Sequence Number (LE): 7936 (0x1f00)
    [Response frame: 167]
```

ICMP 的类型是 request，代码为 8

还有 Checksum，Checksum Status，Identifier，Sequence Number 字段

校验和（Checksum）：2 字节

序号（Sequence Number）：2 字节

标识符（Identifier）：2 字节

4. 查看任意的 ping 响应数据包，ICMP 类型和代码是什么？该 ICMP 数据包还有哪些其他字段？校验和，序号和标识符字段有多少字节？

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x553c [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 31 (0x001f)
    Sequence Number (LE): 7936 (0x1f00)
    [Request frame: 166]
    [Response time: 10.809 ms]
```

ICMP 的类型是 reply，代码为 0

还有 Checksum，Checksum Status，Identifier，Sequence Number 字段

校验和（Checksum）：2 字节

序号（Sequence Number）：2 字节

标识符（Identifier）：2 字节

任务二

在 cmd 中执行 tracert -4 www.sdu.edu.cn，同时用 Wireshark 捕获数据包。

1. 你所使用的主机运行的是什么操作系统？根据收发网络数据包的情况，请判断你使用的主机的 traceroute 默认工作模式为（UDP 模式/TCP 模式/ICMP 模式）？

ip.src ==172.25.226.81&&icmp

No.	Time	Source	Destination	Protocol	Lengtl	Info
371	8.055128	172.25.226.81	202.194.7.118	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=1 (no response found!)
372	8.059280	192.168.250.250	172.25.226.81	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
373	8.060494	172.25.226.81	202.194.7.118	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=1 (no response found!)
374	8.071807	192.168.250.250	172.25.226.81	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
375	8.073014	172.25.226.81	202.194.7.118	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=1 (no response found!)
376	8.084325	192.168.250.250	172.25.226.81	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
644	14.202648	172.25.226.81	202.194.7.118	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=2 (no response found!)
645	14.204750	192.168.249.178	172.25.226.81	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
646	14.205765	172.25.226.81	202.194.7.118	ICMP	106	Echo (ping) request id=0x0001, seq=69/17664, ttl=2 (no response found!)
647	14.207366	192.168.249.178	172.25.226.81	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
648	14.208379	172.25.226.81	202.194.7.118	ICMP	106	Echo (ping) request id=0x0001, seq=70/17920, ttl=2 (no response found!)
649	14.209836	192.168.249.178	172.25.226.81	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
914	20.379909	172.25.226.81	202.194.7.118	ICMP	106	Echo (ping) request id=0x0001, seq=71/18176, ttl=3 (no response found!)
915	20.381696	192.168.249.201	172.25.226.81	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

我的主机运行的是 Windows11 操作系统，使用 ip.src ==172.25.226.81&&icmp 进行过滤，发

现 traceroute 的默认工作模式为 ICMP 模式。

2. **根据 traceroute 结果，从你的主机到 www.sdu.edu.cn 经过了多少个中间节点？**

```
C:\Users\86135>tracert -4 www.sdu.edu.cn

通过最多 30 个跃点跟踪
到 www.sdu.edu.cn [202.194.7.118] 的路由：

  1     4 ms    11 ms    11 ms  192.168.250.250
  2     2 ms     1 ms     1 ms  192.168.249.178
  3     1 ms     3 ms     3 ms  192.168.249.201
  4    11 ms    10 ms    10 ms  58.194.164.65
  5    11 ms    10 ms    11 ms  58.194.164.130
  6    10 ms    37 ms    15 ms  58.194.164.177
  7    12 ms    11 ms    10 ms  58.194.164.178
  8    10 ms    10 ms    10 ms  202.194.7.118

跟踪完成。
```

可以看出经过了 7 个中间节点，最终到达目的主机 202.194.7.118

3. 路径出现“*”的可能原因是什么？

Traceroute 通过检查路由器发送的 ICMP 已超时的请求来确定路由，某些路由器不经询问直接丢弃了 TTL 过期的数据包，因此路径上会出现”*”。

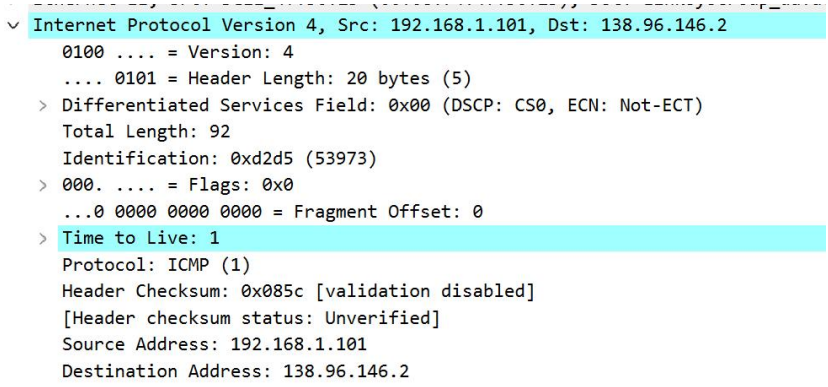
任务三

1. 抓包文件中 traceroute 的目标主机的 IP 地址是多少？

92	16.773195	193.51.181.137	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
93	16.773371	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=53761/466, ttl=16 (no response found!)
94	16.887500	193.51.181.137	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
95	16.887684	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=54017/467, ttl=16 (no response found!)
96	17.006427	193.51.181.137	192.168.1.101	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
97	17.893746	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=54273/468, ttl=17 (reply in 98)
98	18.007202	138.96.146.2	192.168.1.101	ICMP	106 Echo (ping) reply id=0x0200, seq=54273/468, ttl=238 (request in 97)
99	18.007380	192.168.1.101	138.96.146.2	ICMP	106 Echo (ping) request id=0x0200, seq=54529/469, ttl=17 (reply in 100)
100	18.121745	138.96.146.2	192.168.1.101	ICMP	106 Echo (ping) reply id=0x0200, seq=54529/469, ttl=238 (request in 99)

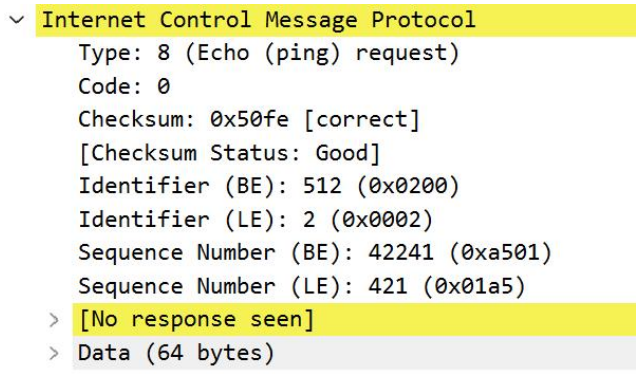
通过查看最后一条超时 ICMP 报文，我们可以得知，目标主机的 IP 地址为 193.168.181.137

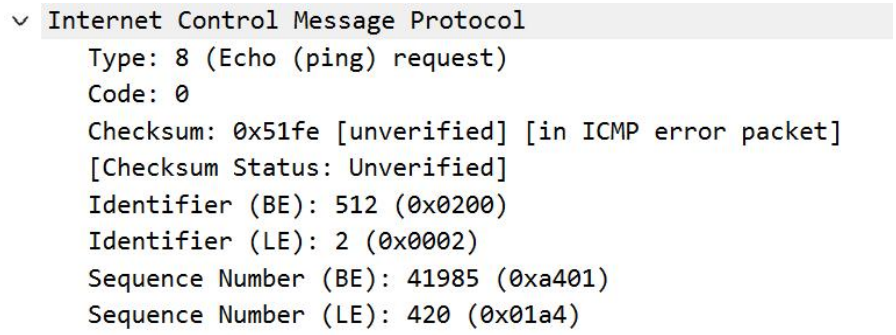
2. 抓包文件中 traceroute 的工作模式为 ICMP 模式，探测数据包（ping request）的 IP 协议中的 Protocol 字段的值是多少？如果是运行在 UDP 模式下，探测数据包的 IP 协议中的 Protocol 字段的值是否会改变？如果改变，会变成多少？



IP 协议中的 Protocol 字段为 1，运行在 UDP 模式下 Protocol 字段的值不会改变，仍然为 1。

3. 查看 ICMP 差错报告包，它比 ping 响应数据包包含更多的字段。请问多出来的是哪些内容?





多出来了 No response seen 字段，包含了一些警告和错误信息。

4. 检查源主机收发的最后三组 ICMP 数据包。为什么最后三次发送的探测数据包（ping request）没有触发 ICMP 差错报告?

因为路由查询是使用逐渐递增 TTL 的查询数据包，最后的 ICMP 查询数据包的 TTL 已经大于到达目的主机中间路由跃点数，因此不会被目标主机丢弃来发送 ICMP 超时的数据包，所以只会

收到 ICMP 响应数据包。

任务四：

1. 请分别列出这两组 traceroute 跟踪测量所经过的城市，并比较区别。

如图：

跳数	IP	主机名	地区（仅供参考）	AS号（仅供参考）	时间（毫秒）
1	223.86.84.129	223.86.84.129	中国四川成都 chinamobile.com 移动	AS9808	1.9 / 3.8 / 9.4
2	* * 112.45.104.29	* * 112.45.104.29	* * 中国四川成都 chinamobile.com 移动	* * AS9808	* * 2.4
3	223.87.26.29 * *	223.87.26.29 * *	中国四川成都 chinamobile.com 移动 * *	AS9808 * *	1.4 * *
4	*	*	*	*	*
5	*	*	*	*	*
6	221.183.89.9	221.183.89.9	中国上海 chinamobile.com 移动	AS9808	37.3 / 37.7 / 43.4
7	221.183.89.34	221.183.89.34	中国上海 chinamobile.com 移动	AS9808	35 / 35.1 / 36
8	221.183.89.177 221.183.89.177 *	221.183.89.177 221.183.89.177 *	中国上海 chinamobile.com 移动 中国上海 chinamobile.com 移动 *	AS9808 AS9808 *	54.7 54.2 *
9	223.120.12.17	223.120.12.17	美国加利福尼亚州洛杉矶 chinamobile.com 移动	AS58453 / AS9808	215.7 / 216.1 / 242.1
10	223.120.6.218	223.120.6.218	美国加利福尼亚州洛杉矶 chinamobile.com 移动	AS58453 / AS9808	200.8 / 201.7 / 247.5
11	38.104.85.161	te0-10-0-6-4.ccr41.lax05.atlas.cogentco.com	美国加利福尼亚州洛杉矶 cogentco.com	AS174	253.1 / 253.4 / 288.6
12	154.54.27.117 * 154.54.27.117	be3243.ccr41.lax01.atlas.cogentco.com * be3243.ccr41.lax01.atlas.cogentco.com	美国加利福尼亚州洛杉矶 cogentco.com * 美国加利福尼亚州洛杉矶 cogentco.com	AS174 * AS174	348.8 * 405.4
13	154.54.44.85	be2931.ccr31.phx01.atlas.cogentco.com	美国亚利桑那州凤凰城 cogentco.com	AS174	280.2 / 282.6 / 308.3
14	* * 154.54.5.218	* * be2979.ccr21.elp02.atlas.cogentco.com	* * 美国德克萨斯州埃尔帕索 cogentco.com	* * AS174	* * 619
15	154.54.0.53	be3850.ccr41.iah01.atlas.cogentco.com	美国德克萨斯州休斯顿 cogentco.com	AS174	348 / 358.1 / 388.7
16	154.54.28.69	be2687.ccr41.atl01.atlas.cogentco.com	美国乔治亚州亚特兰大 cogentco.com	AS174	317.4 / 318.3 / 319.1
17	154.54.26.230 154.54.26.230 *	be3364.rcr21.ind01.atlas.cogentco.com be3364.rcr21.ind01.atlas.cogentco.com *	美国印第安纳州印第安纳波利斯 cogentco.com 美国印第安纳州印第安纳波利斯 cogentco.com *	AS174 AS174 *	318.1 322.2 *
18	154.24.86.26 * 154.24.86.26	154.24.86.26 * 154.24.86.26	美国印第安纳州印第安纳波利斯 cogentco.com * 美国印第安纳州印第安纳波利斯 cogentco.com	AS174 * AS174	368.9 * 398.6
19	* 154.24.53.190 154.24.53.190	* 154.24.53.190 be4458.nr61.b021117-0.ind01.atlas.cogentco.com	* 美国印第安纳州印第安纳波利斯 cogentco.com 美国印第安纳州印第安纳波利斯 cogentco.com	* AS174 AS174	* 329.1 329.7
20	38.104.214.6	38.104.214.6	美国印第安纳州印第安纳波利斯 cogentco.com	AS174	261.9 / 262.8 / 263
21	149.165.183.14	149.165.183.14	美国印第安纳州印第安纳波利斯 iu.edu	AS19782	251.3 / 253 / 254.5
22	134.68.3.129	ae-33.932.dcr3.bldc.net.uits.iu.edu	美国印第安纳州布卢明顿 iupui.edu	AS87	257.9 / 258 / 259.2
23	129.79.123.142	pubwebv4-01-bl-f5-prod.webtech.uits.iu.edu	美国印第安纳州布卢明顿 iu.edu	AS87	251.2 / 251.3 / 251.5

跳数	IP	主机名	地区（仅供参考）	AS号（仅供参考）	时间（毫秒）
1	* 221.7.112.161 221.7.112.161	* 221.7.112.161 221.7.112.161	* 中国重庆 chinaunicom.com 联通 中国重庆 chinaunicom.com 联通	* AS4837 AS4837	* 2403.9 2152.3
2	172.18.5.149	bogon	局域网		1362.6 / 1620.8 / 1886.2
3	*	*	*	*	*
4	113.207.25.57	113.207.25.57	中国重庆 chinaunicom.com 联通	AS4837	58.8 / 315.5 / 489.5
5	*	*	*	*	*
6	*	*	*	*	*
7	219.158.19.70	219.158.19.70	中国上海 chinaunicom.com 联通	AS4837	31.9 / 992.6 / 1242.8
8	219.158.19.89	219.158.19.89	中国上海 chinaunicom.com 联通	AS4837	195.8 / 453 / 723.7
9	219.158.116.242	219.158.116.242	美国加利福尼亚州圣何塞 chinaunicom.com 联通	AS4837	223.3 / 450.4 / 714.9
10	64.71.180.50	port-channel21.core3.sjc2.he.net	美国加利福尼亚州圣何塞 he.net	AS6939	344 / 602.3 / 1670.2
11	*	*	*	*	*
12	*	*	*	*	*
13	*	*	*	*	*
14	*	*	*	*	*
15	149.165.183.85	149.165.183.85	美国印第安纳州印第安纳波利斯 iu.edu	AS19782	1382.9 / 1638.7 / 1891.8
16	*	*	*	*	*
17	38.101.160.251	38.101.160.251	美国印第安纳州印第安纳波利斯 cogentco.com	AS174	262 / 314.7 / 508.1
18	* 149.165.183.14 149.165.183.14	* 149.165.183.14 149.165.183.14	* 美国印第安纳州印第安纳波利斯 iu.edu 美国印第安纳州印第安纳波利斯 iu.edu	* AS19782 AS19782	* 2915.6 2664.4
19	134.68.3.129	ae-33.932.dcr3.bldc.net.uits.iu.edu	美国印第安纳州布卢明顿 iupui.edu	AS87	1899.6 / 2150.5 / 2406
20	129.79.123.143	pubwebv4-01-in-f5-prod.webtech.uits.iu.edu	美国印第安纳州布卢明顿 iu.edu	AS87	1141.3 / 1393.1 / 1647.5

查看地图

2. **在两组 traceroute 跟踪测量中，是否有一个连接的延迟（即表格中的“时间”这一列）比前一次连接长得多？你猜测原因是什么？**

原因是跨越地区距离较长，等待数据响应的时间长。

任务五

连接手机热点：

连接校园网:

```
IP      : 222.206.18.254
地址    : 中国  山东  济南
运营商  : 山东大学

数据二  : 山东省济南市山东大学 | 趵突泉校区2号宿舍楼

数据三  : 中国山东省济南市 | 教育网

URL     : http://www.cip.cc/222.206.18.254
```

使用 VPN:

```
IP      : 172.233.84.252
地址    : 美国  德克萨斯州  达拉斯
运营商  : akamai.com

数据二  : 美国 | Akamai科技公司CDN网络节点

数据三  : 美国德克萨斯达拉斯 | 阿卡迈

URL     : http://www.cip.cc/172.233.84.252
```

1. 为什么在启用山东大学 VPN 前后，显示的信息不同?

因为启用 VPN 后，远程接入虚拟专用网，本地主机与局域网之间建立 VPN 隧道，经过 NAT 网络地址转换分配到本地地址，而本地的主机要访问外网时，其 IP 地址会显示为局域网所在路由器的全球 IP 地址。