北 京 邮 电 大 学

计 算 机 科 学 与 技 术 学 院

《下一代 Internet 技术与协议》
实验报告

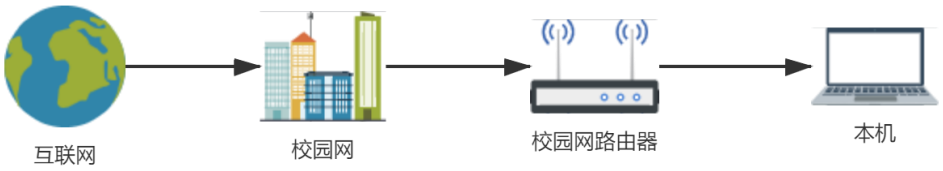
姓名：赵浩天

学号：2018211610

班级：2018211311

2021 年 5 月

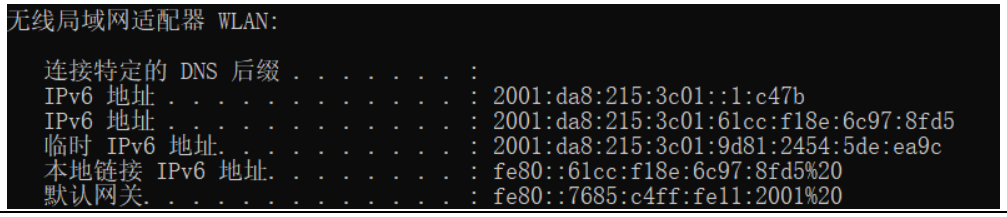
实验报告

实验名称	ICMPv6 抓包分析实验		
实验目的	1. 掌握 wireshark 抓包软件的基本使用方法； 2. 通过实践充分掌握 ICMPv6 协议及其相关细节； 3. 通过 ping、tracert 指令充分理解报文的发送过程与 IPv6 网络上的数据包传送机制，理解 ICMPv6 协议的具体实现； 4. 通过 ping -l 3000 理解 ICMPv6 协议中的分段机制。		
实验完成人	赵浩天	完成时间	2021/5/19
实验环境			

实验步骤与结果分析

一、将实验用的电脑连接校园网，启用 IPv6 协议，关闭 IPv4 协议

二、截图并记录本机的 IPv6 地址信息



①2000-3FFF：2、3 开头，可汇聚全球单播地址；②FC00-FDFF FC00 开头，私有地址；③FE80-FEBF：FE80 开头，链路本地单播地址；④FF00-FFFF：FF00 开头，多播地址，不会显示在地址配置信息上。

通过 ipconfig 得出的本机地址配置当中，

具有可汇聚全球单播地址：2001:da8:215:3c01::1:c47b、

2001:da8:215:3c01:61cc:f18e:6c97:8fd5、

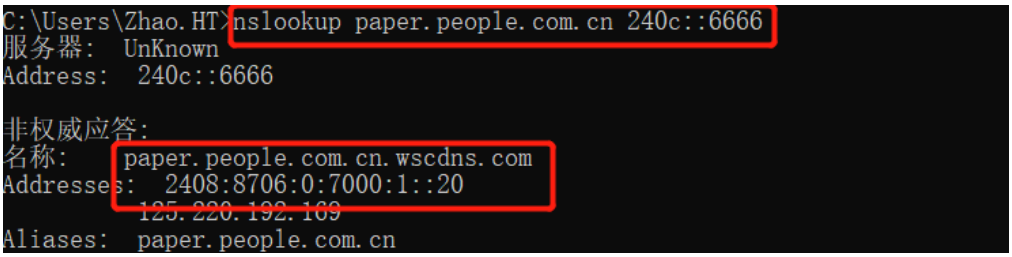
2001:da8:215:3c01:9d81:2454:5de:ea9c；

具有本地链路单播地址：fe80::61cc:f18e:6c97:8fd5%20；

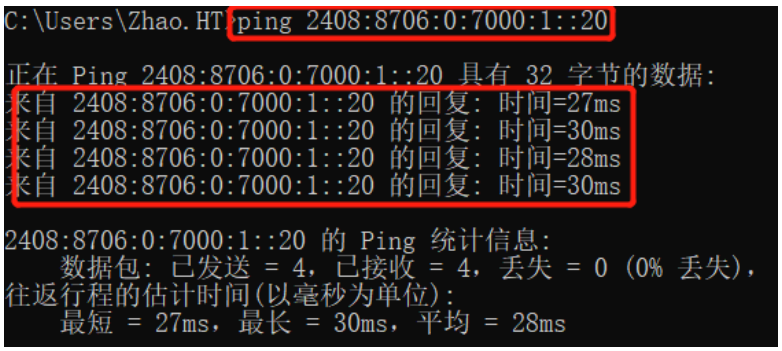
具有默认网关地址：fe80::7685:c4ff:fe11:2001%20。

三、使用 wireshark 软件进行如下操作，并截图抓包

1．使用 nslookup 命令对选定的网站域名进行 DNS 解析；截图并记录其 IPv6 地址统在 CMD 命令行模式下。



2．对此网站的 IPv6 地址进行 ping 操作；截图记录。



3．对此网站的 IPv6 地址进行 tracert 操作，使用 tracert -d xxxx:xxxx 的命令和参数-d；截图记录。

（见下页）

```
C:\Users\Zhao.HT>tracert -d 2408:8706:0:7000:1::20

通过最多 30 个跃点跟踪到 2408:8706:0:7000:1::20 的路由

  1     2 ms     2 ms     1 ms  2001:da8:215:3c01::1
  2     3 ms     4 ms     2 ms  2001:da8:215:0:10:0:28:1
  3     2 ms     1 ms     3 ms  2001:da8:215:0:10:0:4:21
  4     2 ms     2 ms     1 ms  2001:da8:215:0:10:0:3:1
  5     *        *        *     请求超时。
  6     4 ms     6 ms     3 ms  2001:da8:2:123::1
  7     4 ms     2 ms     4 ms  2001:da8:2:5::1
  8     4 ms     7 ms     8 ms  2001:da8:2:2::2
  9    10 ms     9 ms    10 ms  2001:da8:2:27::2
 10    28 ms    27 ms    28 ms  2001:da8:2:11::1
 11    30 ms    27 ms    27 ms  2001:da8:2:753::2
 12    30 ms    30 ms    30 ms  2001:da8:257:0:101:4:118:111
 13    31 ms    28 ms    29 ms  2408:8000:3::342
 14    28 ms    28 ms    27 ms  2408:8000:2:62e::
 15    32 ms    30 ms    30 ms  2408:8000:2:628::1
 16    28 ms    27 ms    27 ms  2408:8000:1100:407::3
 17    27 ms    27 ms    27 ms  2408:8000:1f10:57b0::3
 18    28 ms    27 ms    26 ms  2408:870b:ff00:1::5
 19    27 ms    27 ms    27 ms  fec0::165:0
 20    30 ms    27 ms    27 ms  fec0::165:1
 21    27 ms    27 ms    27 ms  2408:8706:0:7000:1::20

跟踪完成。
```

4．对此网站的 IPv6 地址进行 ping 操作，加上参数 -l 3000，即用长报文进行 ping 操作；截图记录。

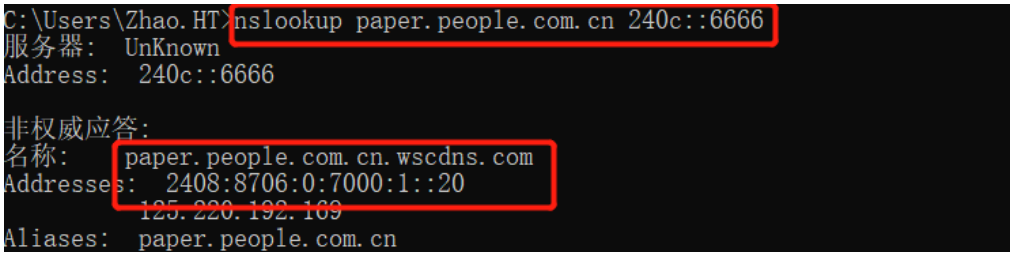
```
C:\Users\Zhao.HT>ping 2408:8706:0:7000:1::20 -l 3000

正在 Ping 2408:8706:0:7000:1::20 具有 3000 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

2408:8706:0:7000:1::20 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

```
C:\Users\Zhao.HT>nslookup bt.byr.cn
服务器:  UnKnown
Address:  10.3.179.118

名称:    bt.byr.cn
Address:  2001:da8:215:4078:250:56ff:fe97:654d


C:\Users\Zhao.HT>ping -l 3000 2001:da8:215:4078:250:56ff:fe97:654d

正在 Ping 2001:da8:215:4078:250:56ff:fe97:654d 具有 3000 字节的数据:
来自 2001:da8:215:4078:250:56ff:fe97:654d 的回复: 时间=2ms
来自 2001:da8:215:4078:250:56ff:fe97:654d 的回复: 时间=4ms
来自 2001:da8:215:4078:250:56ff:fe97:654d 的回复: 时间=3ms
来自 2001:da8:215:4078:250:56ff:fe97:654d 的回复: 时间=3ms

2001:da8:215:4078:250:56ff:fe97:654d 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 = 2ms，最长 = 4ms，平均 = 3ms
```

四、对抓包内容与截图进行对比分析

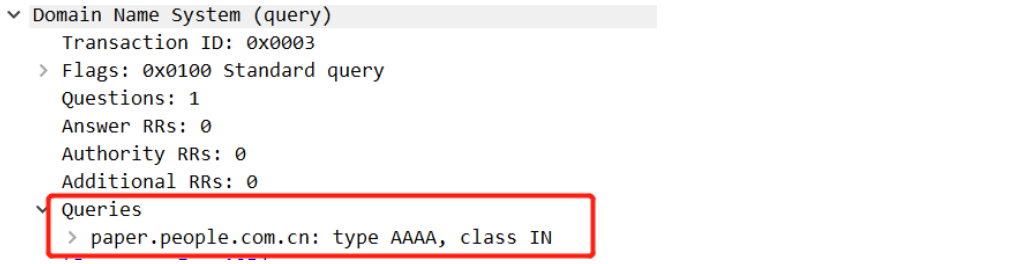
1．使用 nslookup 命令对选定的网站域名进行 DNS 解析；截图并记录其 IPv6 地址统在 CMD 命令行模式下。

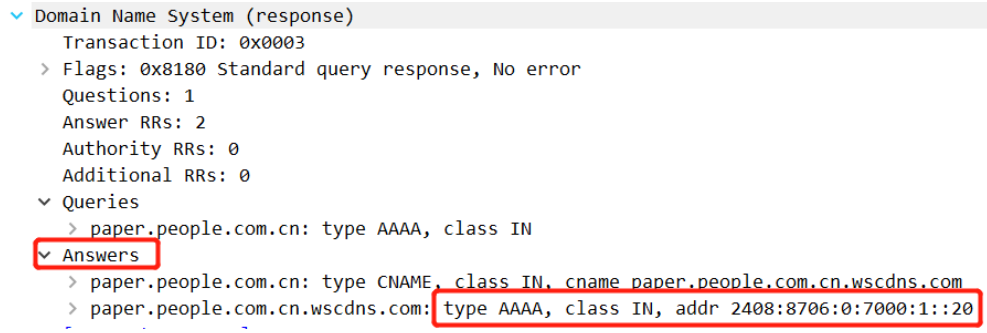
本次实验中，我所选定的支持 IPv6 的网站为人民日报-人民网，域名为 http://paper.people.com.cn/；利用 nslookup 指令对该域名进行解析。由于校园网的 DNS 服务器不支持 IPv6，因此我们还需要指定所用的 IPv6DNS 服务器为 240c::6666。最终获取到的地址为：**2408:8706:0:7000:1::20**



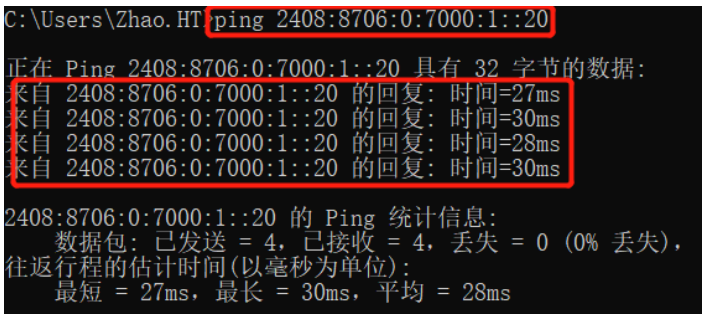
该过程是通过 DNS 协议实现的，

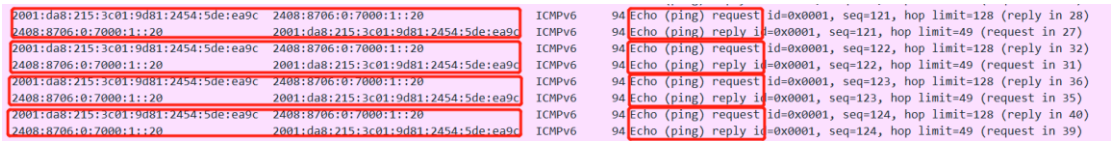
本机向 DNS 服务器发送 DNS 请求报文，请求 paper.people.com.cn 的 AAAA（IPv6）地址；而后 DNS 服务器向本机返回 DNS 响应报文，在报文中给出 paper.people.com.cn 的 IPv6 地址信息，与 CMD 中显示的地址一致。





2．对此网站的 IPv6 地址进行 ping 操作；截图记录。

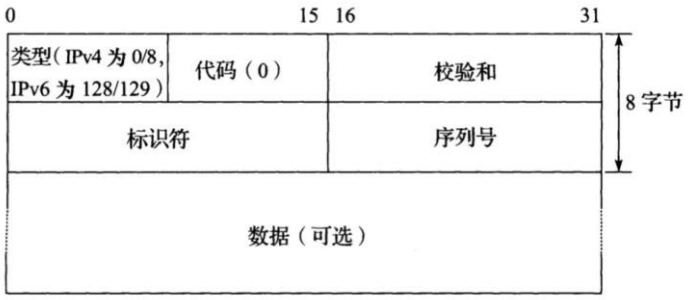




ping 指令的作用是随机生成固定长度的数据包，通过 ICMP（Internet 控制消息协议）协议将数据包发送到指定主机，并侦听回显回复报文来探测与目标主机之间的连接。在本机的 CMD 当中显示出发送的数据、回复的时间等信息。

观察 CMD 中的命令行输出可知：通过 ping 指令向 2408:8706:0:7000:1::20 发送了四段报文，并均得到了回复。再对比观察 wireshark 当中抓取到的报文，也同样捕获到了四组 ICMP 的 ping 报文，每组报文有两个包构成。

一个包是由本机向目标主机（2408:8706:0:7000:1::20）发送的 Echo request 包；另一个包是由目标主机接受到本机发送的 Echo request 后回复的 Echo reply 包。由于四组报文的内容基本一致，因此在此只对第一组报文进行详细分析。



根据 ICMP 报文格式分析第一组 echo request & echo reply 报文，

- **ICMP - Echo request**

```
Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x9b3f [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 121
    [Response In: 28]
  Data (32 bytes)
      Data: 61626364656667686 96a6b6c6d6e6f70717273747576776 1…
      [Length: 32]
```

该报文是由本机发往目标主机（2408:8706:0:7000:1::20）的 echo request 报文，即向目标主机发送回显请求。其中 ICMP 报文 Type 字段为 128，代表该报文为 echo request 报文；code 字段内容为 0；checksum 校验和根据报文内容生成；标识符为 1；序列号为 121；数据内容由 ping 指令随机生成长度 32bytes.

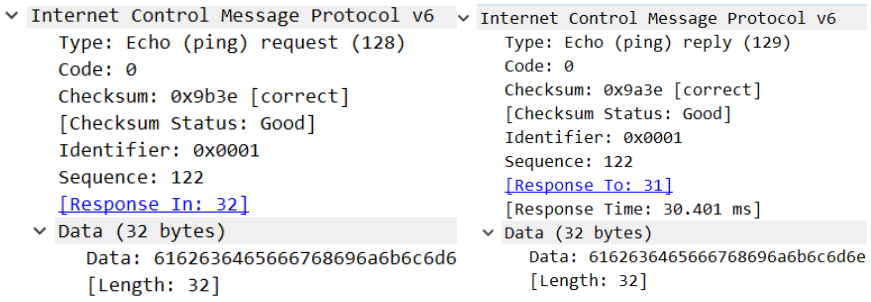
- **ICMP - Echo request**

```
Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x9a3f [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 121
    [Response To: 27]
    [Response Time: 27.074 ms]
  Data (32 bytes)
      Data: 61626364656667686 96a6b6c6d6e6f70717273747576776 1…
      [Length: 32]
```

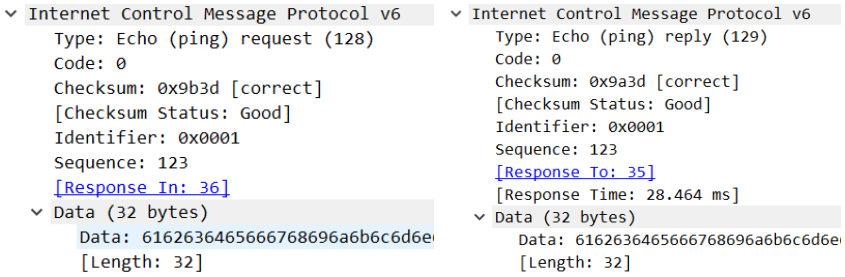
该报文是由目标主机（2408:8706:0:7000:1::20）发往本机的 echo reply 报文，即向目标主机发送回复报文。其中 ICMP 报文 Type 字段为 129，代表该报文为 echo reply 报文；code 字段内容为 0；checksum 校验和根据报文内容生成；标识符为 1；序列号为 121；数据内容 data 与 echo request 报文中数据一致.

对比同组报文，传送方向分别为本机到目标主机、目标主机到本机；类型分别为 128（echo request）、129（echo reply）；校验和不同，根据报文生成；序列号相同均为 121；数据 data 由 ping 指令随机生成。

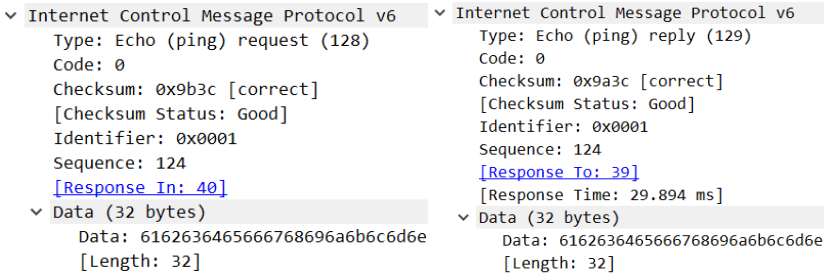
给出另外三组报文如下所示，



第二组



第三组



第四组

简单对比另外三组报文与第一组的报文，仅在分组号 Sequence 上各有区别。因为这是用于匹配 echo reply 与 echo request 之间对应关系的重要属性。

3．对此网站的 IPv6 地址进行 tracert 操作，使用 tracert -d xxxx:xxxx 的命令和参数-d；截图记录。

```
C:\Users\Zhao.HT>tracert -d 2408:8706:0:7000:1::20

通过最多 30 个跃点跟踪到 2408:8706:0:7000:1::20 的路由

  1     2 ms     2 ms     1 ms  2001:da8:215:3c01::1
  2     3 ms     4 ms     2 ms  2001:da8:215:0:10:0:28:1
  3     2 ms     1 ms     3 ms  2001:da8:215:0:10:0:4:21
  4     2 ms     2 ms     1 ms  2001:da8:215:0:10:0:3:1
  5     *        *        *     请求超时。
  6     4 ms     6 ms     3 ms  2001:da8:2:123::1
  7     4 ms     2 ms     4 ms  2001:da8:2:5::1
  8     4 ms     7 ms     8 ms  2001:da8:2:2::2
  9    10 ms     9 ms    10 ms  2001:da8:2:27::2
 10    28 ms    27 ms    28 ms  2001:da8:2:11::1
 11    30 ms    27 ms    27 ms  2001:da8:2:753::2
 12    30 ms    30 ms    30 ms  2001:da8:257:0:101:4:118:111
 13    31 ms    28 ms    29 ms  2408:8000:3::342
 14    28 ms    28 ms    27 ms  2408:8000:2:62e::
 15    32 ms    30 ms    30 ms  2408:8000:2:628::1
 16    28 ms    27 ms    27 ms  2408:8000:1100:407::3
 17    27 ms    27 ms    27 ms  2408:8000:1f10:57b0::3
 18    28 ms    27 ms    26 ms  2408:870b:ff00:1::5
 19    27 ms    27 ms    27 ms  fec0::165:0
 20    30 ms    27 ms    27 ms  fec0::165:1
 21    27 ms    27 ms    27 ms  2408:8706:0:7000:1::20

跟踪完成。
```

通过向目标地址发送不同跳数限制(hop limit)值的“Internet 控制消息协议(ICMP)”回显请求数据包，tracert 诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 hop limit 递减 1。当数据包上的 hop limit 减为 0 时，路由器应该将“已超时”的消息发回源地址。

tracert 先发送 hop limit 为 1 的回显请求数据包，并在随后的每次发送过程将 hop limit 递增 1，直到目标响应或 hop limit（最大为 30）达到最大值，从而确定路由。通过检查中间路由器发回的“已超时”的消息确定路由。某些路由器不经询问直接丢弃 hop limit 过期的数据包，这在捕获报文时不会存在回显应答报文。

跟踪路由（Tracert）是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径，其工作原理是通过向目标发送不同跳转限制 (hop limit) 值的“Internet 控制消息协议（ICMP）”回应数据包，跟踪路由诊断程序确定到目标所采取的路由。实际应用中可以使用跟踪路由命令确定数据包在网络上的停止位置。

Wireshark 软件中捕获的报文情况如下：

15248 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=136, hop limit=1 (no response found!)
15249 …	2001:da8:215:3c01::1	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
15250 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=137, hop limit=1 (no response found!)
15251 …	2001:da8:215:3c01::1	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
15252 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=138, hop limit=1 (no response found!)
15253 …	2001:da8:215:3c01::1	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)

15305 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=142, hop limit=3 (no response found!)
15306 …	2001:da8:215:0:10:0:4:21	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
15307 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=143, hop limit=3 (no response found!)
15308 …	2001:da8:215:0:10:0:4:21	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
15309 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=144, hop limit=3 (no response found!)
15310 …	2001:da8:215:0:10:0:4:21	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
15323 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=145, hop limit=4 (no response found!)
15324 …	2001:da8:215:0:10:0:3:1	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
15325 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=146, hop limit=4 (no response found!)
15326 …	2001:da8:215:0:10:0:3:1	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
15327 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=147, hop limit=4 (no response found!)
15328 …	2001:da8:215:0:10:0:3:1	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)

…

15579 …	fec0::165:1	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)
15580 …	2001:da8:215:3c01:e8cb:f632:148b:7d7d	2408:8706:0:7000:1::20	ICMPv6	126	Echo (ping) request id=0x0001, seq=195, hop limit=20 (no response found!)
15581 …	fec0::165:1	2001:da8:215:3c01:e8cb:f632:148b:7d7d	ICMPv6	174	Time Exceeded (hop limit exceeded in transit)

结合命令行显示以及抓包分析结果可知，每次主机向目标地址发送递增的 hop 限制的 Echo request 报文，并且每次发送三个为一组。当 hop limit 减为 0 时，中间路由将会向主机回发超时报文，主机以此获得每一跳的路由信息。在实际实验过程中，总共进行了 hop limit 1~21 的 echo request，其中除了 5 以外，每个跳数限制下的请求报文均得到了回应。

总体而言，我们可以将整个过程分为三类：发送的 request 有收到超时 time exceeded 的（1-4 & 6-20）；发送的 request 没有收到超时 time exceeded 的（5）；发送的 echo request 收到了 echo reply 报文的回复（21）。

- **ICMPv6 – echo Request**

```
Internet Protocol Version 6, Src: 2001:da8:215:3c01:e8cb:f632:148b:7d7d, Dst: 2408:8706:0:7000:1::20
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 72
    Next Header: ICMPv6 (58)
    Hop Limit: 1
    Source Address: 2001:da8:215:3c01:e8cb:f632:148b:7d7d
    Destination Address: 2408:8706:0:7000:1::20
Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x86fd [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 136
  > [No response seen]
  > Data (64 bytes)
```

- **ICMPv6 – time Exceeded**

```
> Internet Protocol Version 6, Src: 2001:da8:215:3c01::1, Dst: 2001:da8:215:3c01:e8cb:f632:148b:7d7d
Internet Control Message Protocol v6
    Type: Time Exceeded (3)
    Code: 0 (hop limit exceeded in transit)
    Checksum: 0x19ff [correct]
    [Checksum Status: Good]
    Reserved: 00000000
  Internet Protocol Version 6, Src: 2001:da8:215:3c01:e8cb:f632:148b:7d7d, Dst: 2408:8706:0:7000:1::20
      0110 .... = Version: 6
    > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
      .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
      Payload Length: 72
      Next Header: ICMPv6 (58)
      Hop Limit: 1
      Source Address: 2001:da8:215:3c01:e8cb:f632:148b:7d7d
      Destination Address: 2408:8706:0:7000:1::20
  Internet Control Message Protocol v6
      Type: Echo (ping) request (128)
      Code: 0
      Checksum: 0x86fd [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier: 0x0001
      Sequence: 136
    > Data (64 bytes)
```

```
C:\Users\Zhao.HT>tracert -d 2408:8706:0:7000:1::20

通过最多 30 个跃点跟踪到 2408:8706:0:7000:1::20 的路由

  1     2 ms     2 ms     1 ms  2001:da8:215:3c01::1
  2     3 ms     4 ms     2 ms  2001:da8:215:0:10:0:28:1
```

由如上报文可以看出，本机向目标主机发送了 hop limit 为 1 的报文，在经过一跳到达第一个路由节点后，由于 hop limit 被减为 0，对应路由返回 time exceeded 报文。在返回的 time exceeded 的报文中可以看到对应的源地址与最终得出的路由结果里第一个节点的地址一致。

同时注意到当 hop limit = 5 时，

```
2001:da8:215:3c01:e8cb:f632:148b:7d7d 2408:8706:0:7000:1::20      ICMPv6   126 Echo (ping) request id=0x0001, seq=148, hop limit=5 (no response found!)
fe80::7685:c4ff:fe11:2001             ff02::1                     ICMPv6   118 Router Advertisement from 74:85:c4:11:20:01
fe80::7685:c4ff:fe11:2001             ff02::1                     ICMPv6   118 Router Advertisement from 74:85:c4:11:20:01
2001:da8:215:3c01:e8cb:f632:148b:7d7d 2408:8706:0:7000:1::20      ICMPv6   126 Echo (ping) request id=0x0001, seq=149, hop limit=5 (no response found!)
fe80::7685:c4ff:fe11:2001             ff02::1                     ICMPv6   118 Router Advertisement from 74:85:c4:11:20:01
2001:da8:215:3c01:e8cb:f632:148b:7d7d 2408:8706:0:7000:1::20      ICMPv6   126 Echo (ping) request id=0x0001, seq=150, hop limit=5 (no response found!)
```

```
Internet Protocol Version 6, Src: 2001:da8:215:3c01:e8cb:f632:148b:7d7d, Dst: 2408:8706:0:7000:1::20
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 72
    Next Header: ICMPv6 (58)
    Hop Limit: 5
    Source Address: 2001:da8:215:3c01:e8cb:f632:148b:7d7d
    Destination Address: 2408:8706:0:7000:1::20
Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x86f0 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 149
  > [No response seen]
  > Data (64 bytes)
```

```
3     2 ms     1 ms     3 ms  2001:da8:215:0:10:0:4:21
4     2 ms     2 ms     1 ms  2001:da8:215:0:10:0:3:1
5     *        *        *     请求超时。
6     4 ms     6 ms     3 ms  2001:da8:2:123::1
7     4 ms     2 ms     4 ms  2001:da8:2:5::1
```

虽然与其他情况下发送的 echo request 报文相似，仅 hop limit=5，但是并未收到类似的 time exceeded 报文回复。造成这种情况的原因可能有很多，例如那一跳禁止 PING、那一跳不对 TTL 超时做响应处理，直接丢弃等等。

对于具有其他 hop limit 的 echo request 包均收到了相应路由的 time exceeded 回复，并且收到回复的源地址均能够与 tracert 的结果一一对应。其他 20 组报文内容过多，在此不再进行详细展示，参考上文所述的第一组数据即可，仅是 hop limit 不同，使得 hop 减为 0 的路由节点不同，返回 time exceeded 报文的路由也不同。

```
126 Echo (ping) request id=0x0001, seq=136, hop limit=1 (no response found!)
174 Time Exceeded (hop limit exceeded in transit)
126 Echo (ping) request id=0x0001, seq=137, hop limit=1 (no response found!)
174 Time Exceeded (hop limit exceeded in transit)
126 Echo (ping) request id=0x0001, seq=138, hop limit=1 (no response found!)
174 Time Exceeded (hop limit exceeded in transit)
```

•••

```
126 Echo (ping) request id=0x0001, seq=193, hop limit=20 (no response found!)
174 Time Exceeded (hop limit exceeded in transit)
126 Echo (ping) request id=0x0001, seq=194, hop limit=20 (no response found!)
118 Router Advertisement from 74:85:c4:11:20:01
174 Time Exceeded (hop limit exceeded in transit)
126 Echo (ping) request id=0x0001, seq=195, hop limit=20 (no response found!)
174 Time Exceeded (hop limit exceeded in transit)
```

最终当 hop limit 达到 21 时，echo request 刚好抵达目标地址（2408:8706:0:7000:1::20），并成功返回 echo reply 报文。这三组收到 echo reply 的报文与 1.中的 ping 过程完全一致。

```
ICMPv6    126 Echo (ping) request id=0x0001, seq=196, hop limit=21 (reply in 15586)
ICMPv6    126 Echo (ping) reply id=0x0001, seq=196, hop limit=49 (request in 15585)
ICMPv6    126 Echo (ping) request id=0x0001, seq=197, hop limit=21 (reply in 15588)
ICMPv6    126 Echo (ping) reply id=0x0001, seq=197, hop limit=49 (request in 15587)
ICMPv6    126 Echo (ping) request id=0x0001, seq=198, hop limit=21 (reply in 15590)
ICMPv6    126 Echo (ping) reply id=0x0001, seq=198, hop limit=49 (request in 15589)
```

```
Internet Protocol Version 6, Src: 2001:da8:215:3c01:e8cb:f632:148b:7d7d, Dst: 2408:8706:0:7000:1::20
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 72
    Next Header: ICMPv6 (58)
    Hop Limit: 21
    Source Address: 2001:da8:215:3c01:e8cb:f632:148b:7d7d
    Destination Address: 2408:8706:0:7000:1::20
Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x86c1 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 196
    [Response In: 15586]
  > Data (64 bytes)
```

hop limit = 21 时（最后一次发送）发出的 echo request 报文，

```
Internet Protocol Version 6, Src: 2408:8706:0:7000:1::20, Dst: 2001:da8:215:3c01:e8cb:f632:148b:7d7d
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 72
    Next Header: ICMPv6 (58)
    Hop Limit: 49
    Source Address: 2408:8706:0:7000:1::20
    Destination Address: 2001:da8:215:3c01:e8cb:f632:148b:7d7d
Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x85c1 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 196
    [Response To: 15585]
    [Response Time: 27.828 ms]
  > Data (64 bytes)
```

Hop limit = 21 时，恰好抵达目标主机 2408:8706:0:7000:1::20，回复 echo reply 报文。当本机接受到该 echo reply 报文后，表明已经完成了路由上全部节点的探测，tracert 工作结束。

```
19    27 ms    27 ms    27 ms  fec0::165:0
20    30 ms    27 ms    27 ms  fec0::165:1
21    27 ms    27 ms    27 ms  2408:8706:0:7000:1::20

跟踪完成。
```

4．对此网站的 IPv6 地址进行 ping 操作，加上参数 -l 3000，即用长报文进行 ping 操作；截图记录。

```
C:\Users\Zhao.HT>ping 2408:8706:0:7000:1::20 -l 3000

正在 Ping 2408:8706:0:7000:1::20 具有 3000 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

2408:8706:0:7000:1::20 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

对人民日报-人民网地址“2408:8706:0:7000:1::20”的 3000 长报文四次 ping 全部超时，没有收到回复。考虑造成这一结果的原因可能是由于，该网站禁止了长报文的 ping 请求，以防止遭到 ping 攻击等意外情况。

```
C:\Users\Zhao.HT>nslookup bt.byr.cn
服务器:  UnKnown
Address:  10.3.179.118

名称:    bt.byr.cn
Address:  2001:da8:215:4078:250:56ff:fe97:654d


C:\Users\Zhao.HT>ping -l 3000 2001:da8:215:4078:250:56ff:fe97:654d

正在 Ping 2001:da8:215:4078:250:56ff:fe97:654d 具有 3000 字节的数据:
来自 2001:da8:215:4078:250:56ff:fe97:654d 的回复: 时间=2ms
来自 2001:da8:215:4078:250:56ff:fe97:654d 的回复: 时间=4ms
来自 2001:da8:215:4078:250:56ff:fe97:654d 的回复: 时间=3ms
来自 2001:da8:215:4078:250:56ff:fe97:654d 的回复: 时间=3ms

2001:da8:215:4078:250:56ff:fe97:654d 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 = 2ms, 最长 = 4ms, 平均 = 3ms
```

改换北邮人 bt（bt.byr.cn）的 ipv6 地址进行再次尝试，能够成功 ping 通。

Source	Destination	Protocol	Length	Info
2001:da8:215:3c…	2001:da8:215:4…	IPv6	1510	IPv6 fragment (off=0 more=y ident=0x78953626 nxt=58)
2001:da8:215:3c…	2001:da8:215:4…	IPv6	1510	IPv6 fragment (off=1448 more=y ident=0x78953626 nxt=58)
2001:da8:215:3c…	2001:da8:215:4…	ICMPv6	174	Echo (ping) request id=0x0001, seq=81, hop limit=128 (reply in 317)

观察抓取到的包信息，每个 ICMP 的 echo request 以及 reply 报文都根据 MTU 限制被分为了三片，先观察链路层 MTU 限制以及最后一片中显示的分片结果，

```
C:\Users\Zhao.HT>netsh interface ipv6 show subinterfaces

   MTU  MediaSenseState   传入字节  传出字节      接口
------  ---------------  ---------  ---------  -------------
4294967295                1          0      71340  Loopback Pseudo-Interface 1
  1500                1   26872821   12212898  WLAN
  1500                5          0        152  以太网
  1500                5          0        152  本地连接* 1
  1500                1          0     316583  本地连接* 2
```

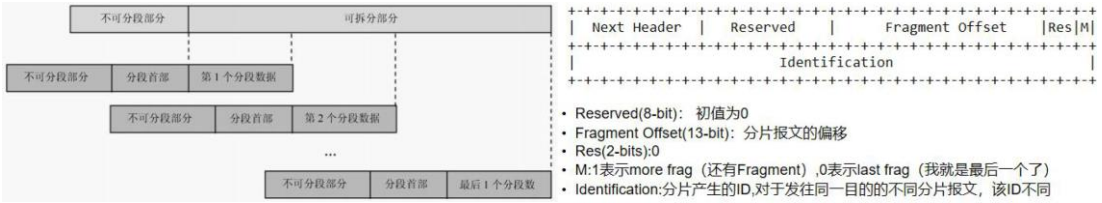
```
Internet Protocol Version 6, Src: 2001:da8:215:3c01:cc03:aa88:ecc3:8a12, Dst: 2001:da8:215:4078:250:56ff:fe97:654d
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 120
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 128
    Source Address: 2001:da8:215:3c01:cc03:aa88:ecc3:8a12
    Destination Address: 2001:da8:215:4078:250:56ff:fe97:654d
    [Destination SA MAC: VMware_97:65:4d (00:50:56:97:65:4d)]
  > Fragment Header for IPv6
  v [3 IPv6 Fragments (3008 bytes): #312(1448), #313(1448), #314(112)]
      [Frame: 312, payload: 0-1447 (1448 bytes)]
      [Frame: 313, payload: 1448-2895 (1448 bytes)]
      [Frame: 314, payload: 2896-3007 (112 bytes)]
      [Fragment count: 3]
      [Reassembled IPv6 length: 3008]
      [Reassembled IPv6 data: 8000c4f8000100516162636465666768696a6b6c6d6e6f707172737475767761626364656…]
v Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0xc4f8 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 81
    [Response In: 317]
  > Data (3000 bytes)
```

链路 MTU 情况限制了数据帧的最大长度。如果有数据包要传，而且数据包的长度超过了 MTU，那么就要对数据包进行分段操作，使每一片的长度都小于或等于 MTU。由上图可知，此 3000 字节的 IP 包被分成 3 个分组发送：对应 MTU 中包括包头以及数据部分(段头以及对应数据)。

```
[3 IPv6 Fragments (3008 bytes): #312(1448), #313(1448), #314(112)]
    [Frame: 312, payload: 0-1447 (1448 bytes)]
    [Frame: 313, payload: 1448-2895 (1448 bytes)]
    [Frame: 314, payload: 2896-3007 (112 bytes)]
    [Fragment count: 3]
    [Reassembled IPv6 length: 3008]
    [Reassembled IPv6 data: 8000c4f80001005161626364656667686 96a6b6c6d6e6f707172737475767761626364 65…]
Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0xc4f8 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 81
    [Response In: 317]
    Data (3000 bytes)
```

IPv6 报文通过三片分片的报文，总计携带了长度为 3008 的数据。重组后获得 ICMPv6 的 echo request 报文，3008 bytes 的数据中包括 8 字节的 ICMPv6 头部、以及 3000 字节的 data 数据。

由于链路层的 MTU 为 1500，除去其他各层数据头部 52 字节（Type 2 字节 + IPv6 header 40 字节 + fragment header 40 字节）外，每个报文的最大荷载为 1448 字节。因此总计 3008 字节的数据，被分为 1448 字节（第一片）+1448 字节（第二片）+112 字节（第三片）。



通过相关资料可知，IPv6 报文的分片规则如上图所示。现对分片后的每一报文进行详细分析，

- **IPv6 – fragment 1**

```
Internet Protocol Version 6, Src: 2001:da8:215:3c01:cc03:aa88:ecc3:8a12, Dst: 2001:da8:215:4078:250:56ff:fe97:654d
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 1456
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 128
    Source Address: 2001:da8:215:3c01:cc03:aa88:ecc3:8a12
    Destination Address: 2001:da8:215:4078:250:56ff:fe97:654d
    [Destination SA MAC: VMware_97:65:4d (00:50:56:97:65:4d)]
  v Fragment Header for IPv6
      Next header: ICMPv6 (58)
      Reserved octet: 0x00
      0000 0000 0000 0... = Offset: 0 (0 bytes)
      .... .... .... .00. = Reserved bits: 0
      .... .... .... ...1 = More Fragments: Yes
      Identification: 0x78953626
    [Reassembled IPv6 in frame: 314]
  > Data (1448 bytes)
```

荷载长度	1456
下一首部	Fragment header（44）
Fragment header（8 bytes）	
下一首部	ICMPv6（58）
片偏移 Offset	0（携带数据偏移为 0）
More Fragments	1（接下来还有分片）

这是第一个分片，下一首部为 ICMPv6，片偏移为 0，接下来还有分片，携带的数据 data 长度为 1448 bytes。

- **IPv6 – fragment 2**

```
Internet Protocol Version 6, Src: 2001:da8:215:3c01:cc03:aa88:ecc3:8a12, Dst: 2001:da8:215:4078:250:56ff:fe97:654d
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 1456
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 128
    Source Address: 2001:da8:215:3c01:cc03:aa88:ecc3:8a12
    Destination Address: 2001:da8:215:4078:250:56ff:fe97:654d
    [Destination SA MAC: VMware_97:65:4d (00:50:56:97:65:4d)]
  v Fragment Header for IPv6
      Next header: ICMPv6 (58)
      Reserved octet: 0x00
      0000 0101 1010 1... = Offset: 181 (1448 bytes)
      .... .... .... .00. = Reserved bits: 0
      .... .... .... ...1 = More Fragments: Yes
      Identification: 0x78953626
    [Reassembled IPv6 in frame: 314]
  > Data (1448 bytes)
```

荷载长度	1456
下一首部	Fragment header（44）
Fragment header（8 bytes）	
下一首部	ICMPv6（58）
片偏移 Offset	0x181（携带数据偏移为 1448）
More Fragments	1（接下来还有分片）

这是第二个分片，下一首部为 ICMPv6，片偏移为 1448，接下来还有分片，携带的数据 data 长度为 1448 bytes。

- **IPv6 – fragment 3**

```
Internet Protocol Version 6, Src: 2001:da8:215:3c01:cc03:aa88:ecc3:8a12, Dst: 2001:da8:215:4078:250:56ff:fe97:654d
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 120
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 128
    Source Address: 2001:da8:215:3c01:cc03:aa88:ecc3:8a12
    Destination Address: 2001:da8:215:4078:250:56ff:fe97:654d
    [Destination SA MAC: VMware_97:65:4d (00:50:56:97:65:4d)]
  v Fragment Header for IPv6
      Next header: ICMPv6 (58)
      Reserved octet: 0x00
      0000 1011 0101 0... = Offset: 362 (2896 bytes)
      .... .... .... .00. = Reserved bits: 0
      .... .... .... ...0 = More Fragments: No
      Identification: 0x78953626
  v [3 IPv6 Fragments (3008 bytes): #312(1448), #313(1448), #314(112)]
      [Frame: 312, payload: 0-1447 (1448 bytes)]
      [Frame: 313, payload: 1448-2895 (1448 bytes)]
      [Frame: 314, payload: 2896-3007 (112 bytes)]
      [Fragment count: 3]
      [Reassembled IPv6 length: 3008]
      [Reassembled IPv6 data: 8000c4f8000100516162636465666768696a6b6c6d6e6f707172737475767761626364656…]
```

荷载长度	120
下一首部	Fragment header（44）
Fragment header（8 bytes）	
下一首部	ICMPv6（58）
片偏移 Offset	0x362（携带数据偏移为 2896）
More Fragments	0（接下来没有分片）

这是第三个分片，下一首部为 ICMPv6，片偏移为 2896，接下来没有分片，携带的数据 data 长度为 112bytes。

分析与思考
通过本次实验让我以更为具体的方式观察并了解了 ICMPv6 协议的具体内容。熟悉了抓包软件 Wireshark 的使用，并对 Windows 操作系统下的网络配置有了一定的理解。通过本次实验使我对 ICMPv6 下的 echo request、echo reply、time exceeded 类型的协议有了更好的掌握，尤其对于其中每种报文的构成与与所传递的信息意义；使我具备了对于诸多报文的分析能力；让我对整个 IPv6 地址的配置过程有了具体的认识。在问题解决过程中锻炼了我的自主思考能力，最终通过理论结合实践的方法完成了本次实验。 在本次实验中由于对于协议的不熟悉以及网络设置与网络路由的知识尚浅，导致在实验过程中遇到了许多问题。经过艰苦奋斗，都在与同学的讨论帮助下以及网络与书本知识的查阅得以解决。 通过本次协议让我进一步理解了 ping、tracert 常用指令的工作原理，以及计算机网络路由的相关性知识。并通过抓包分析，学习了如何利用 IPv6 & ICMPv6 协议实现上述指令的具体细节。达到了“掌握 Wireshark 抓包协议分析软件的基本使用方法、理解 windows 下 ping 与 tracert 指令原理、掌握 IPv6 与 ICMPv6 协议的几种报文类型及其作用”的实验目的。