实验报告：IPV4 实验三

课程名称：计算机网络实践　**年级：**大二　**上机实践成绩：**

指导教师：章玥　**姓名：**邱吉尔

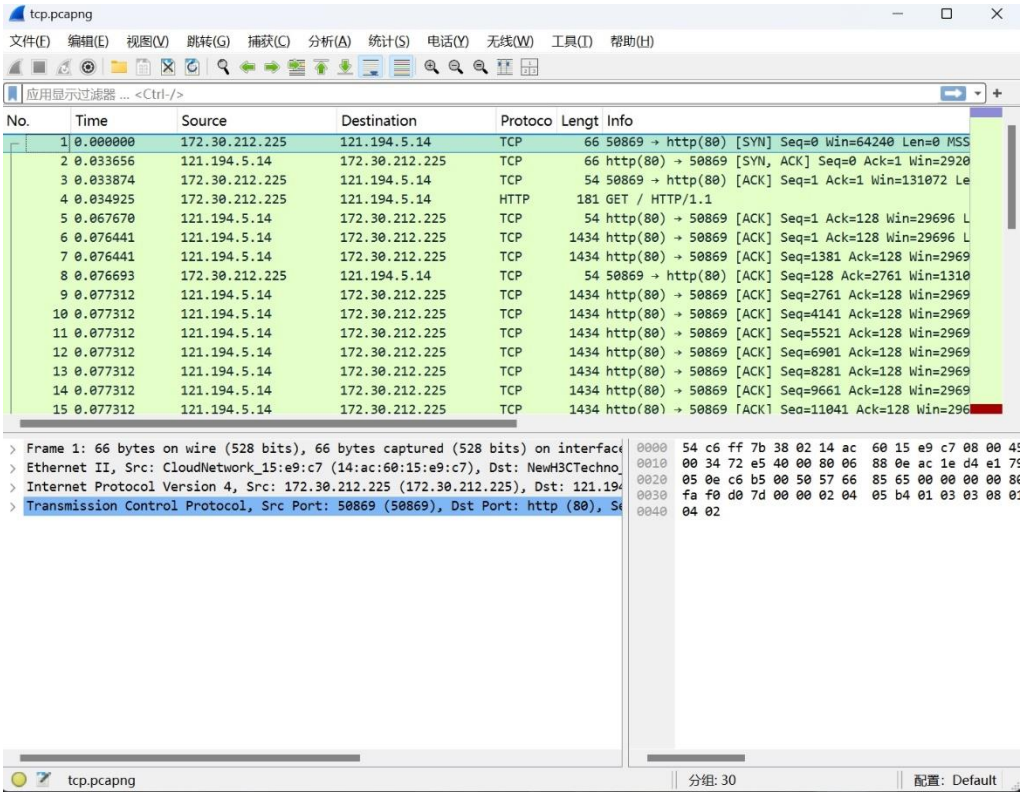
学号：10235101533　**上机实践日期：2024/12/2**

一、目的

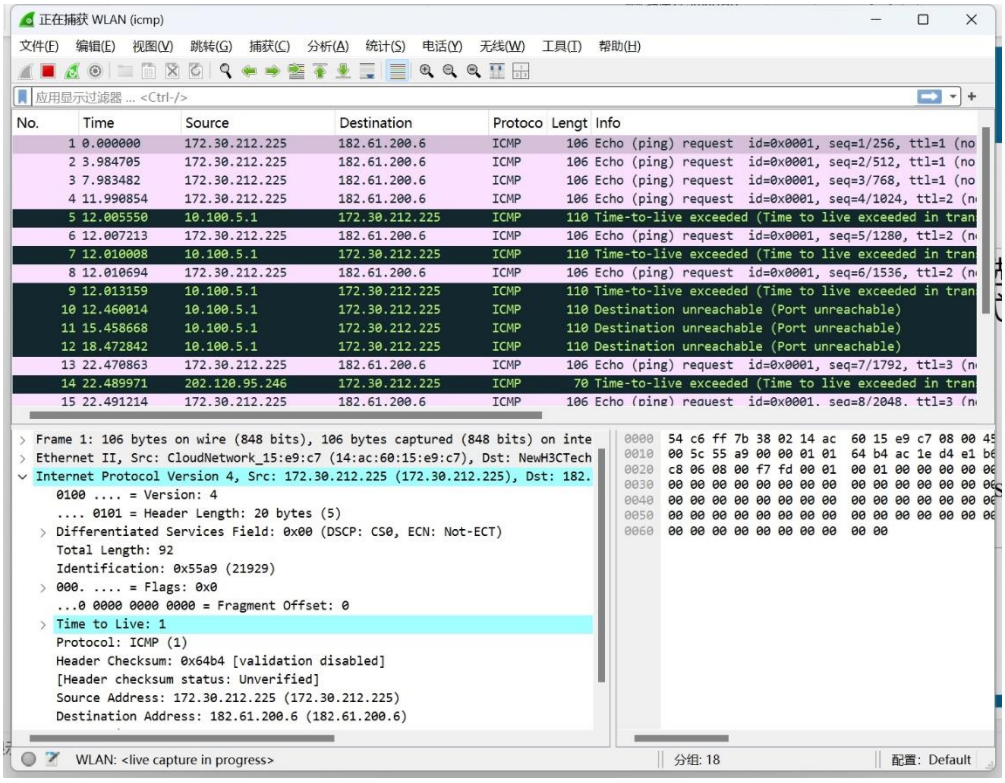
1. 学会通过 Wireshark 分析 ip 协议
2. 了解 wireshark、curl、wget、traceroute、tracert 等常用软件的使用，掌握网络抓包的方法，能在所用电脑上进行抓包;
3. 了解 IP 数据包格式，能应用该软件分析数据包格式，查看抓到的包的内容，并分析对应的 IP 数据包格式;
4. 了解 IP 各部分的含义

二、实验步骤

1. 捕获 IP Packets:

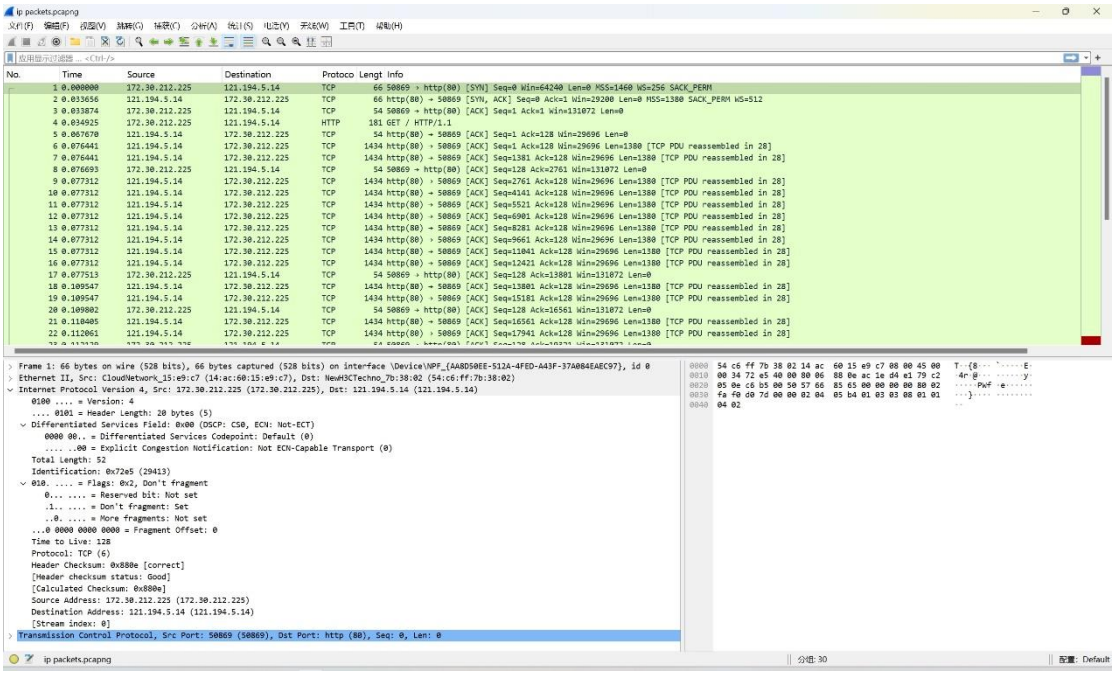


2. 捕获 Trace:



三、实验结果分析

1. 选择你通过 Wireshark 捕获到任何一个报文，分析其 IP 报文头部：



Version:版本号为 4

Header Length:IP 包头长度，这里 IP 包头长度为 20 字节。

Differentiation Services：包含位标志，表示数据包是否应该是处理路由器的服务质量和拥塞指示。

Total Length:IP 包总长，这里是 52 字节。

Identification:标志

Fragment Offset:片偏移，这里是 0，表示该 IP 包在该组分片包中位置

Time to Live:生存时间，这里是 128，当 IP 包进行传送时，先会对该字段赋予某个特定的值。当 IP 包经过每一个沿途的路由器的时候，每个沿途的路由器会将 IP 包的 TTL 值减少 1。如果 TTL 减少为 0，则该 IP 包会被丢弃。这个字段可以防止由于路由环路而导致 IP 包在网络中不停被转发。

Protocol:协议，这里是 TCP 协议

Header Checksum:校验和，这里是 0x880e。用于使接收端检验收到的报文是否正确。

Source:源地址

Destination:目的地址

2. 通过观察 Wireshark 捕获的报文，来回答下面的问题：
   1) 你的计算机和远程服务器的 IP 地址是什么？

      我的计算机 ip 地址是 172.30.212.225，远程服务器的 ip 地址是 121.194.5.14

   2) “总长度”字段是否包括 IP 报头加上 IP 有效负载，或者仅包括 IP 有效负载？

      包括 IP 报头加上 IP 有效负载

   3) 对于不同的数据包，“标识”字段的值如何变化，还是保持不变？ 例如，对于 TCP 连接中的所有数据包，它一直保持相同的值，还是对于每个数据包都不同？ 双向通信的报文是否相同？ 如果值发生变化，您能看到任何规律吗？

      “标识”字段可能相同，因为可能原来是一个包，只是后来被分片了。双向通信报文相同可能性不大，因为发送端和接收端标识字段是各自标识的，且标识字段的初始值是随机的。标识字段的规律是存在一个计数器，每产生一个数据报，计数器就加 1，并将此值赋给标识字段。

3. 通过观察 Wireshark 捕获的报文，来回答下面的问题：
   4) 从您的计算机发送的数据包的 TTL 字段的初始值是多少？他们是 maximum possible value 吗？

```
Time to Live: 128
```

初始值是 128，是最大值

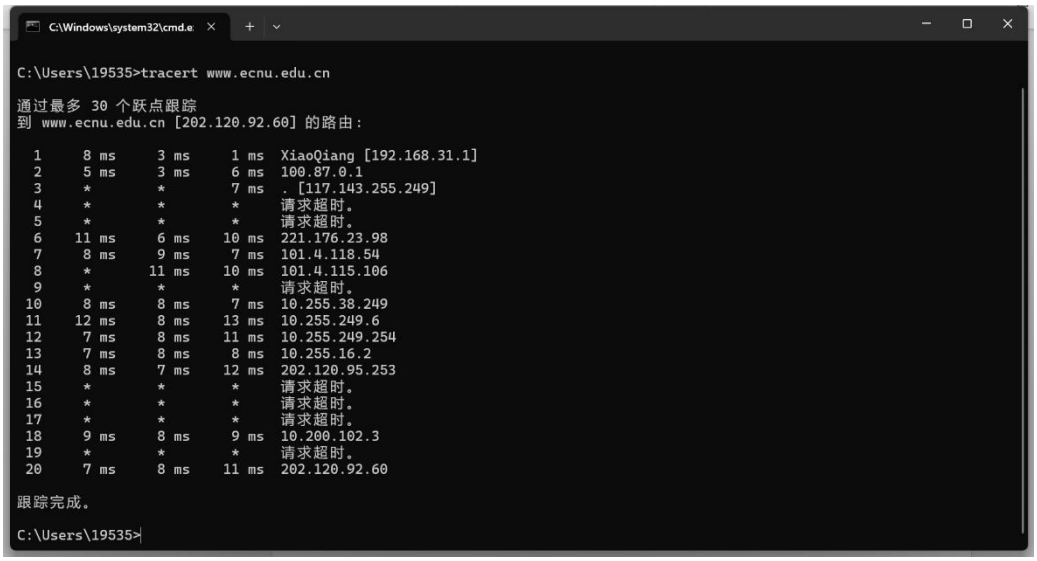
5) 查看数据包时如何判断它是否被分段？

如果收到的 IP 报头中 Fragmentation Flags 为 1 则未分片；而如果收到的 IP 报头的 Fragment Flag 为 0，则表明其是被分片的。

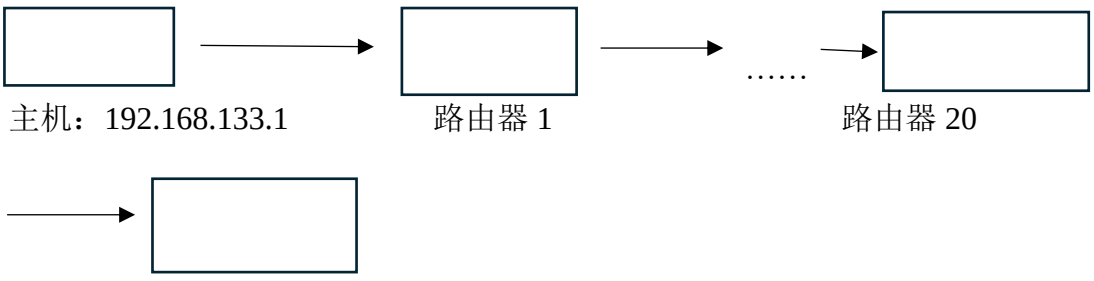
6) IP 数据报报头的长度是多少，它是如何被编码进报头长度域的？

长度是 20byte，编码为 0101，即 5

4. 使用 traceroute 的结果，绘制网络路径图。 图中，显示您的计算机（放在最左侧）和远程服务器（放在最右侧），均显示 IP 地址，以及它们之间的路径上的路由器，这些路由器以从本机开始的跳数作为距离编号。 您可以在捕获的跟踪数据包中找到计算机和远程服务器的 IP 地址。



```
C:\Windows\system32\cmd.e

C:\Users\19535>tracert www.ecnu.edu.cn

通过最多 30 个跃点跟踪
到 www.ecnu.edu.cn [202.120.92.60] 的路由：

  1     8 ms     3 ms     1 ms  XiaoQiang [192.168.31.1]
  2     5 ms     3 ms     6 ms  100.87.0.1
  3     *        *        7 ms  . [117.143.255.249]
  4     *        *        *     请求超时。
  5     *        *        *     请求超时。
  6    11 ms     6 ms    10 ms  221.176.23.98
  7     8 ms     9 ms     7 ms  101.4.118.54
  8     *       11 ms    10 ms  101.4.115.106
  9     *        *        *     请求超时。
 10     8 ms     8 ms     7 ms  10.255.38.249
 11    12 ms     8 ms    13 ms  10.255.249.6
 12     7 ms     8 ms    11 ms  10.255.249.254
 13     7 ms     8 ms     8 ms  10.255.16.2
 14     8 ms     7 ms    12 ms  202.120.95.253
 15     *        *        *     请求超时。
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18     9 ms     8 ms     9 ms  10.200.102.3
 19     *        *        *     请求超时。
 20     7 ms     8 ms    11 ms  202.120.92.60

跟踪完成。

C:\Users\19535>
```



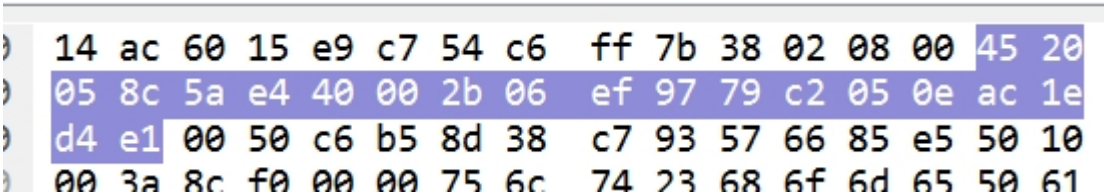
主机：192.168.133.1　　路由器 1　　路由器 20

服务器 202.120.92.60

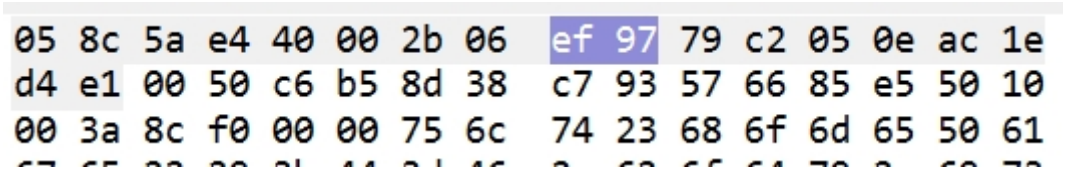
5. **观察 IP 报文的校验和：**

IP 报头的校验和可以用来验证一个数据包是否正确。选择一个从远程服务器发送到本计算机的包，计算它的 checksum。在计算过程中，请添加注释，表明每个 word 对应的字段。

Ip 字段：



校验和字段：



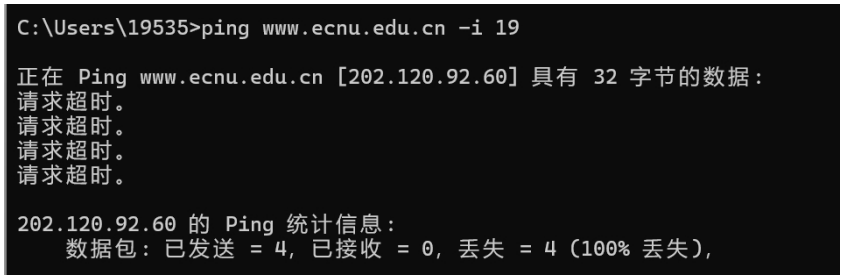
因此将【45 20】、【05 8c】、【5a e4】、【40 00】、【2b 06】、【79 c2】、【05 0e】、【ac 1e】、【d4 e1】相加得到：3 1065

最高位回加得到：1068，取反后得到 EF97，与校验码相同，因此没有出错

6. 思考题：TTL 与跳数的关系：

TTL 加上跳数等于设置的默认存活时间，TTL 因大于等于跳数

如到达 www.ecnu.edu.cn 需要经过 20 跳，若是将默认存活时间设置为 19 则到不了目标地址，展示如下：



而设置为 20 则可以到达目标地址：