**【实验名称】：**TCP段分析实验

**学生姓名：2151133**孙韩雅

**实验地点：**济事楼330 **实验时间：**2023-12-4

**【实验目的】**

了解TCP的概念与协议相关原理，通过工具进行TCP段分析实验，了解TCP包抓取方法及分析方法。

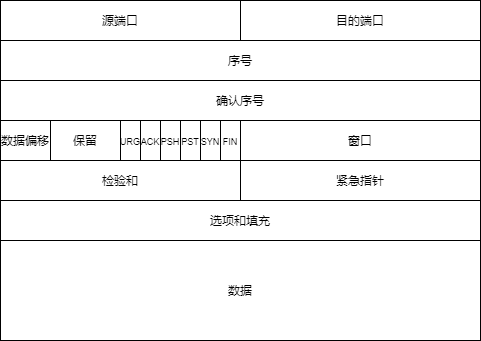
**【实验原理】**

1.TCP的概述

TCP是传输层的协议，功能即为在IP的数据报服务之上增加了最基本的服务：复用和分用以及差错检测。TCP 是一个基于连接的四层协议，提供全双工地，可靠地传输系统。它能够保证数据被远程主机接收。并且能够为高层协议提供flow-controlled 服务。空间上，TCP需要在端系统中维护连接状态，需要一定的开销。此连接装入包括接收和发送缓存，拥塞控制参数和序号与确认号的参数。UDP不维护连接状态，也不跟踪这些参数，开销小。空间和时间上都具有优势。

2.TCP的报文格式

TCP报文是TCP层传输的数据单元，也叫报文段。其格式如图所示：



3.TCP报文字段

A、端口号：用来标识同一台计算机的不同的应用进程。

1）源端口：源端口和IP地址的作用是标识报文的返回地址。

2）目的端口：端口指明接收方计算机上的应用程序接口。

TCP报头中的源端口号和目的端口号同IP数据报中的源IP与目的IP唯一确定一条TCP连接。

B、序号和确认号：是TCP可靠传输的关键部分。序号是本报文段发送的数据组的第一个字节的序号。在TCP传送的流中，每一个字节一个序号。例如：一个报文段的序号为300，此报文段数据部分共有100字节，则下一个报文段的序号为400。所以序号确保了TCP传输的有序性。确认号，即ACK，指明下一个期待收到的字节序号，表明该序号之前的所有数据已经正确无误的收到。确认号只有当ACK标志为1时才有效。比如建立连接时，SYN报文的ACK标志位为0。

C、数据偏移／首部长度：4bits。由于首部可能含有可选项内容，因此TCP报头的长度是不确定的，报头不包含任何任选字段则长度为20字节，4位首部长度字段所能表示的最大值为1111，转化为10进制为15，15\*32/8 = 60，故报头最大长度为60字节。首部长度也叫数据偏移，是因为首部长度实际上指示了数据区在报文段中的起始偏移值。

D、保留：为将来定义新的用途保留，现在一般置0。

E、控制位：URG ACK PSH RST SYN FIN，共 6个，每一个标志位表示一个控制功能。

1）URG：紧急指针标志，为1时表示紧急指针有效，为0则忽略紧急指针。

2）ACK：确认序号标志，为1时表示确认号有效，为0表示报文中不含确认信息，忽略确认号字段。

3）PSH：push标志，为1表示是带有push标志的数据，指示接收方在接收到该报文段以后，应尽快将这个报文段交给应用程序，而不是在缓冲区排队。

4）RST：重置连接标志，用于重置由于主机崩溃或其他原因而出现错误的连接。或者用于拒绝非法的报文段和拒绝连接请求。

5）SYN：同步序号，用于建立连接过程，在连接请求中，SYN=1和ACK=0表示该数据段没有使用捎带的确认域，而连接应答捎带一个确认，即SYN=1和ACK=1。

6）FIN：finish标志，用于释放连接，为1时表示发送方已经没有数据发送了，即关闭本方数据流。

F、窗口：滑动窗口大小，用来告知发送端接受端的缓存大小，以此控制发送端发送数据的速率，从而达到流量控制。窗口大小时一个16bit字段，因而窗口大小最大为65535。

G、校验和：奇偶校验，此校验和是对整个的 TCP 报文段，包括TCP头部和TCP数据，以16位字进行计算所得。由发送端计算和存储，并由接收端进行验证。

H、紧急指针：只有当URG 标志置 1 时紧急指针才有效。紧急指针是一个正的偏移量，和顺序号字段中的值相加表示紧急数据最后一个字节的序号。TCP的紧急方式是发送端向另一端发送紧急数据的一种方式。

I、选项和填充：最常见的可选字段是最长报文大小，又称为MSS（Maximum Segment Size），每个连接方通常都在通信的第一个报文段（为建立连接而设置SYN标志为1的那个段）中指明这个选项，它表示本端所能接受的最大报文段的长度。选项长度不一定是32位的整数倍，所以要加填充位，即在这个字段中加入额外的零，以保证TCP头是32的整数倍。

J、数据部分：TCP报文段中的数据部分是可选的。在一个连接建立和一个连接终止时，双方交换的报文段仅有TCP首部。如果一方没有数据要发送，也使用没有任何数据的首部来确认收到的数据。在处理超时的许多情况中，也会发送不带任何数据的报文段。

4.TCP连接过程

相对于SOCKET开发者，TCP创建过程和链接折除过程是由TCP/IP协议栈自动创建的。因此开发者并不需要控制这个过程。但是对于理解TCP底层运作机制，相当有帮助。TCP连接过程简单一句话概括：“三次握手四次挥手”。

A.TCP三次握手：所谓三次握手(Three-way Handshake)，是指建立一个TCP连接时，需要客户端和服务器总共发送3个包。三次握手的目的是连接服务器指定端口，建立TCP连接,并同步连接双方的序列号和确认号并交换 TCP 窗口大小信息.在socket编程中，客户端执行connect()时。将触发三次握手。

第一次握手：客户端发送一个TCP的SYN标志位置1的包指明客户打算连接的服务器的端口，以及初始序号X，保存在包头的序列号(Sequence Number)字段里。

第二次握手：服务器发回确认包(ACK)应答。即SYN标志位和ACK标志位均为1同时，将确认序号(Acknowledgement Number)设置为客户的ISN加1，即X+1。

第三次握手：客户端再次发送确认包(ACK) SYN标志位为0，ACK标志位为1。并且把服务器发来ACK的序号字段+1，放在确定字段中发送给对方。并且在数据段放写ISN的+1。

SYN攻击：在三次握手过程中，服务器发送SYN-ACK之后，收到客户端的ACK之前的TCP连接称为半连接(half-open connect).此时服务器处于Syn\_RECV状态.当收到ACK后，服务器转入ESTABLISHED状态。攻击客户端在短时间内伪造大量不存在的IP地址，向服务器不断地发送syn包，服务器回复确认包，并等待客户的确认，由于源地址是不存在的，服务器需要不断的重发直至超时，这些伪造的SYN包将长时间占用未连接队列，正常的SYN请求被丢弃，目标系统运行缓慢，严重者引起网络堵塞甚至系统瘫痪。

B.TCP四次挥手：TCP的连接的拆除需要发送四个包，因此称为四次挥手(four-way handshake)。客户端或服务器均可主动发起挥手动作，在socket编程中，任何一方执行close()操作即可产生挥手操作。

**【实验设备】**

HUAWEI MateBook X Pro（安装有Cisco Packet Tracer与Wireshark抓包分析工具）

【**实验步骤**】

1.分析在Packet tracer中TCP报文情况；

2.用WireShark抓取TCP数据包；

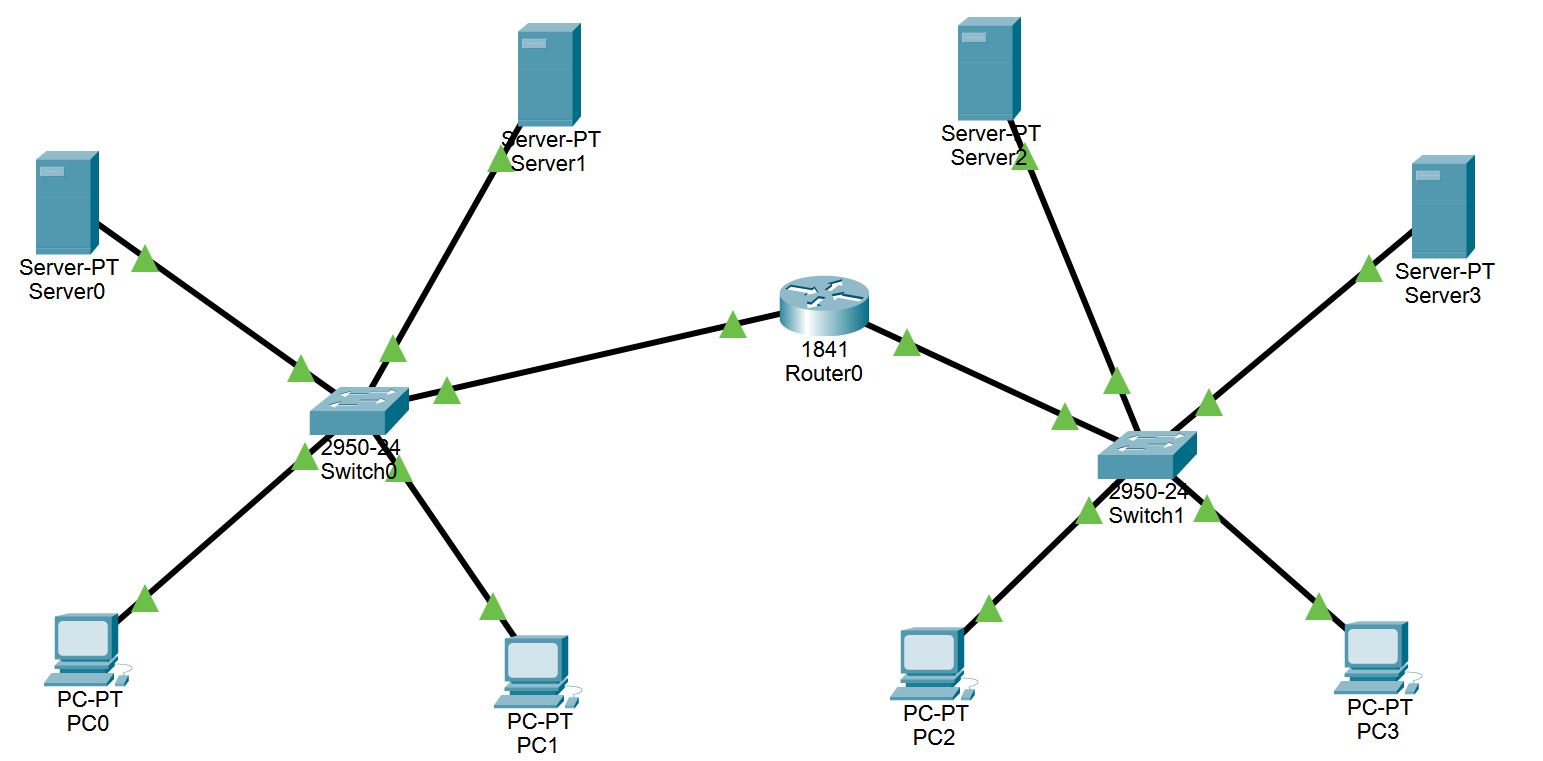
3.查看TCP报文字段内容，并解读；

4.仔细研读TCP连接建立过程数据报文；

5.仔细研读TCP拆链过程数据报文；

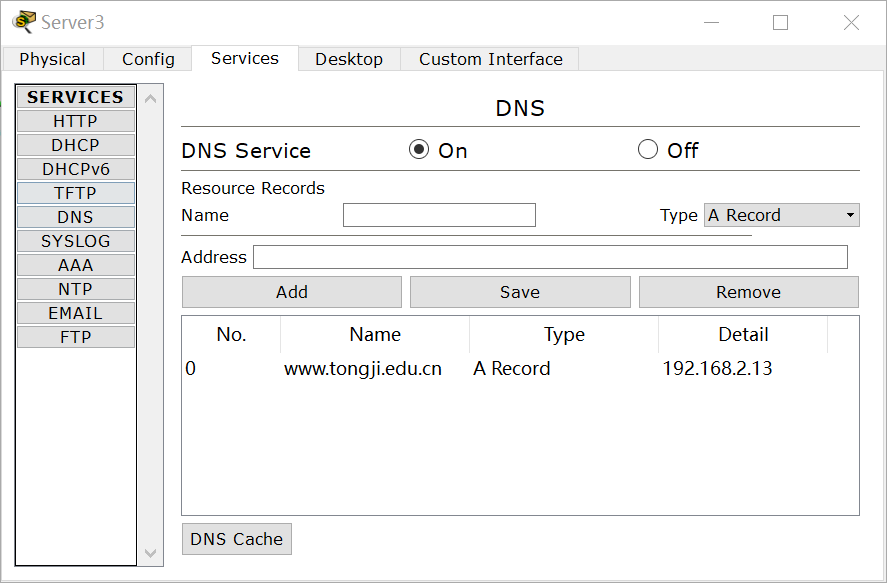
**【实验现象】**

1.设置WEB服务器和简单的DNS服务器。按照拓扑图进行接线：

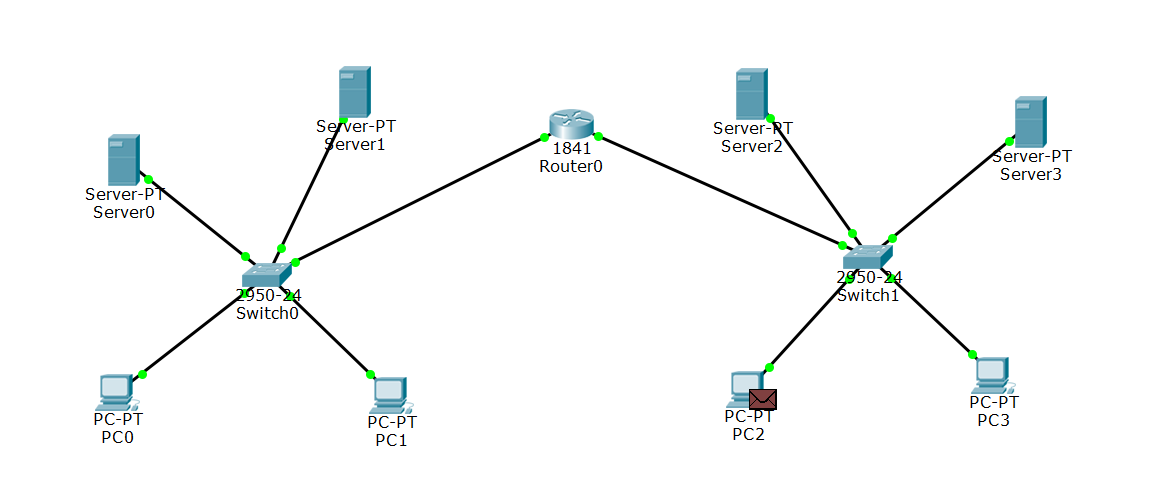


在Server2、3上配置gateway、ip、子网掩码。

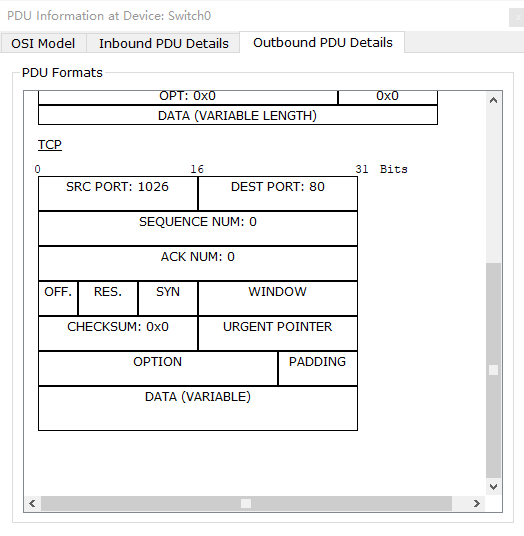
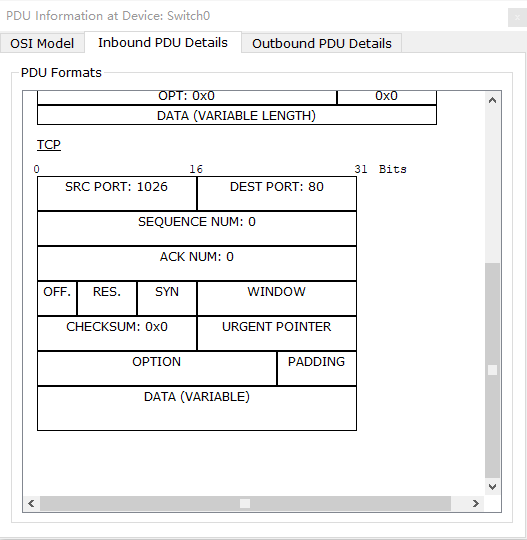
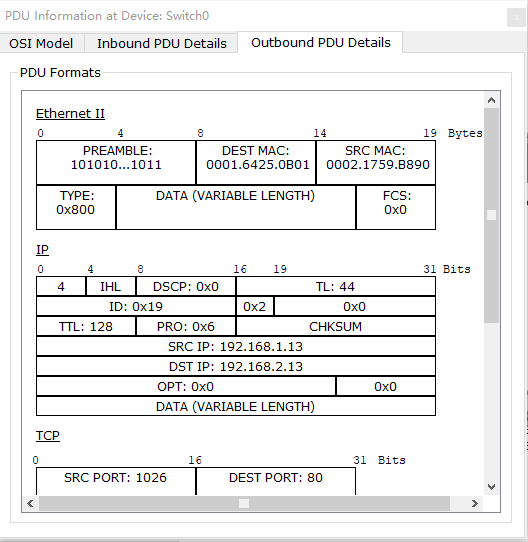
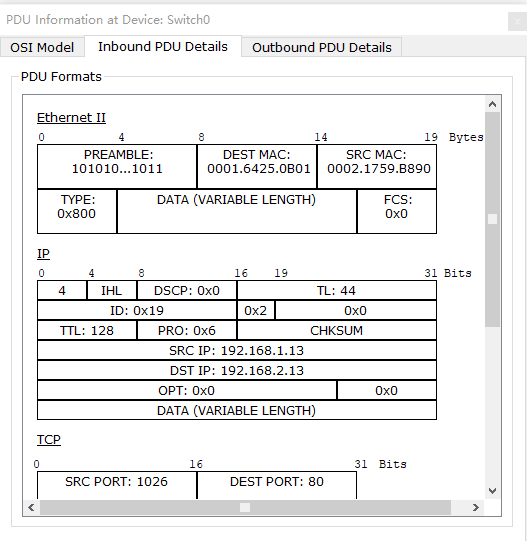
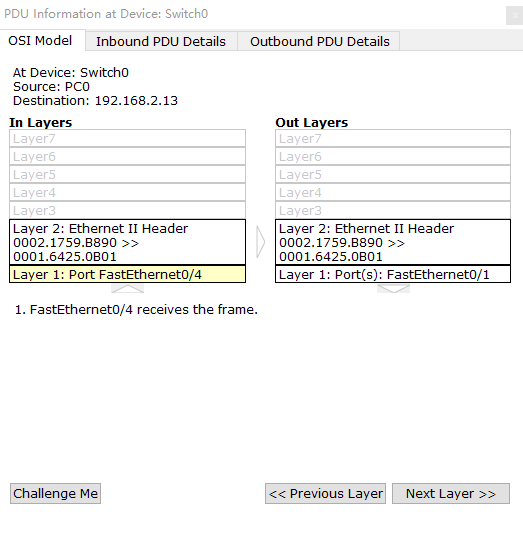
在Server3上配置detail为server2的ip的DNS。



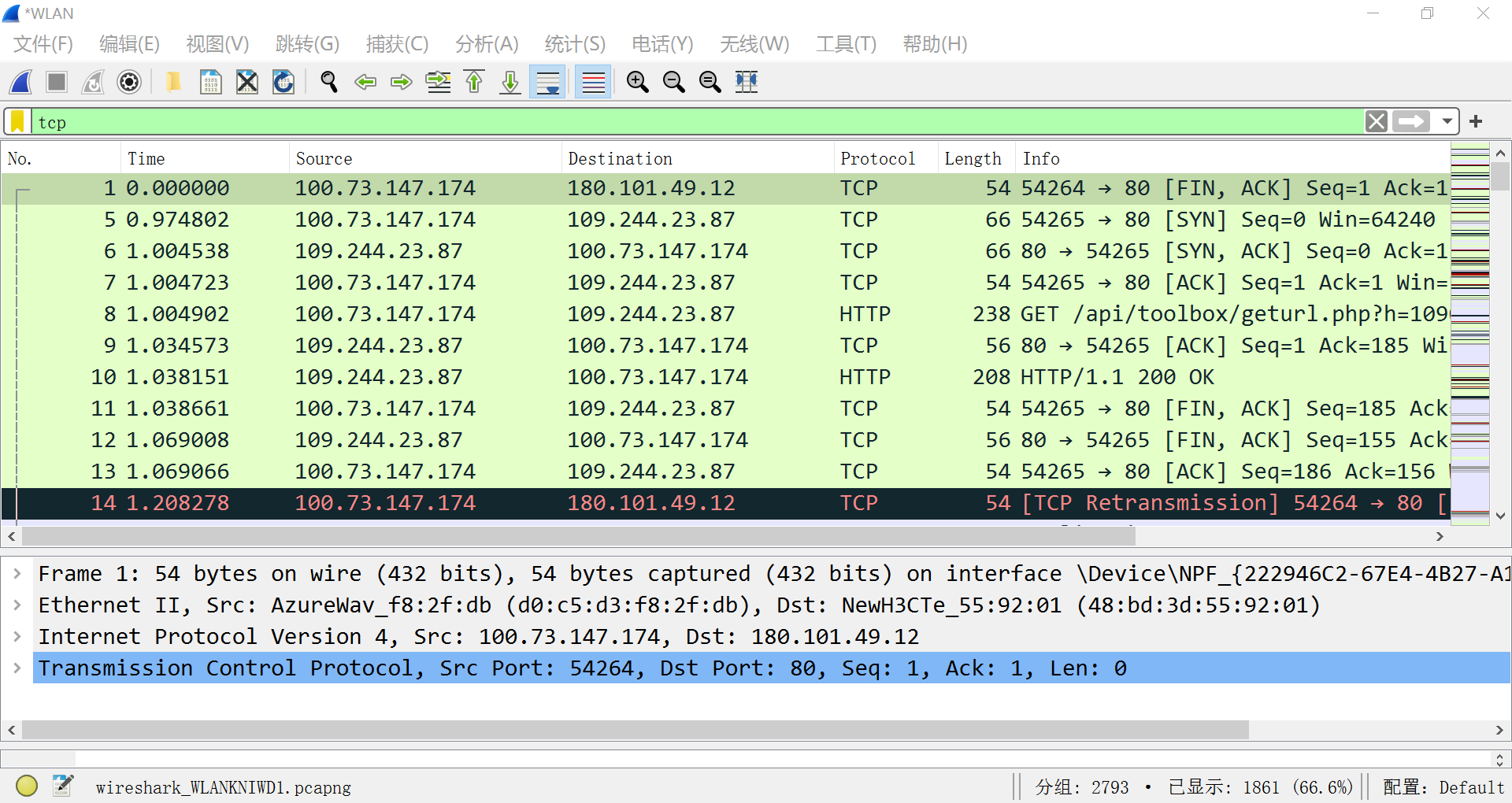
2.使用PC2访问WEB服务器，产生TCP数据报文：



3.查看TCP报文详细内容：



4.使用WireShark软件抓取报文，并使用“tcp”过滤器。其中Info部分Seq=0且标志位SYN=1对应第一次握手（客户端发送一个TCP数据包），Seq=0、SYN=1、ACK=1对应第二次握手（服务器向客户端返回一个数据包），Seq=1、SYN=0、ACK=1对应第三次握手（客户端收到来自服务器的数据包后检查确认序号是否正确，若正确则发送一个数据包）：



5.分析报文内容。下半部分显示的四层内容从上到下分别对应物理层、数据链路层、网络层和传输层。其中Frame部分有到达时间、新纪元时间、帧序号、帧长度、协议名称等内容；Ethernet部分有目的MAC地址、源MAC地址、协议版本等内容；Internet Protocal部分有目的IP地址、源IP地址等内容；Transmission Control Protocol部分有发送端端口号、目的端端口号、封包序号等内容。

**【分析讨论】**

TCP段分析用于深入了解TCP协议的工作原理以及网络通信过程中发生的问题和故障。通过使用Wireshark等网络分析工具，对TCP段进行抓包、过滤、解析和分析，能够发现网络通信中的性能问题、安全问题以及其他信息。