TCP三次握手详解

文章的开头给大家分享一下什么是TCP协议：（TCP是面向连接的通信协议，通过三次握手建立连接，通讯完成时要拆除连接，由于TCP 是面向连接的所以只能用于点对点的通讯）源IP地址：发送包的IP地址；目的IP地址：接收包的IP地址；源端口：源系统上的连接的端口；目的端口：目的系统上的连接的端口。  TCP是因特网中的传输层协议，使用三次握手协议建立连接。当主动方发出SYN连接请求后，等待对方回答SYN，ACK。这种建立连接的方法可以防止产生错误的连接；

一、想必大家都对TCP协议的三次握手特别感兴趣，下面我们通过通过wireshark抓取的TCP三次握手协议并且详细分析下：



备注下各个选项的意思（

SYN：同步序列编号

ACK：确认字符

Seq: TCP协议中的**序号**，这里为0

Win：发送报文段一方的接收窗口

Len: 发送文件TCP报文段Datas段的长度

MSS:最大报文段长度

WS：窗口扩大因子

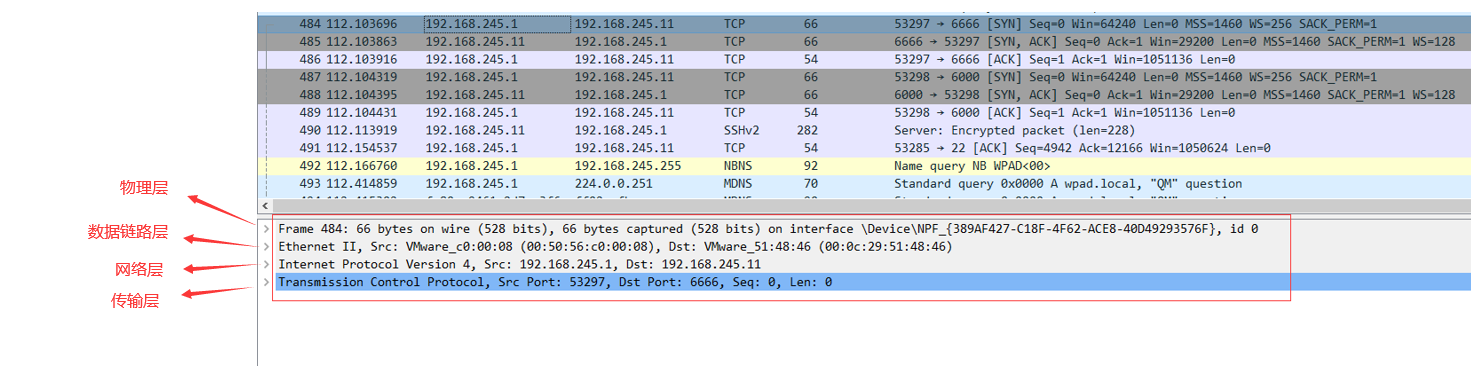
SACK\_PERM：允许选择确认。 TCP选项中的字段）

TCP三次握手一共分为三个步骤：

* 1. 客户端(192.168.245.1)发送SYN报文到服务器(192.168.245.11)；
  2. 服务器(192.168.245.11)接收到客户端(192.168.245.1)的SYN报文，回复SYN+ACK报文；
  3. 客户端(192.168.245.1)接收到服务端(192.168.245.11)的 SYN+ACK 报文后，回复 ACK报文；

二、下面我们来详细分析一下TCP的三次握手协议：

2.1、首先是客户端(192.168.245.1)发送SYN报文到服务器(192.168.245.11)：



我们来看看上图的第二个红框里面的信息，里面包含一下各个层（osi七层协议涉及的层级）的详细信息：

Frame: 物理层数据帧概况

Ethernet II: 数据链路层以太网帧头部

​Internet Protocol Version 4: 互联网层IP包头部

​Transmission Control Protocol: 传输层的数据段头部

​Hypertext Transfer Protocol: 应用层的信息

下面是上图各个层级的具体意思(之后的两个报文解释也是以此类推)：

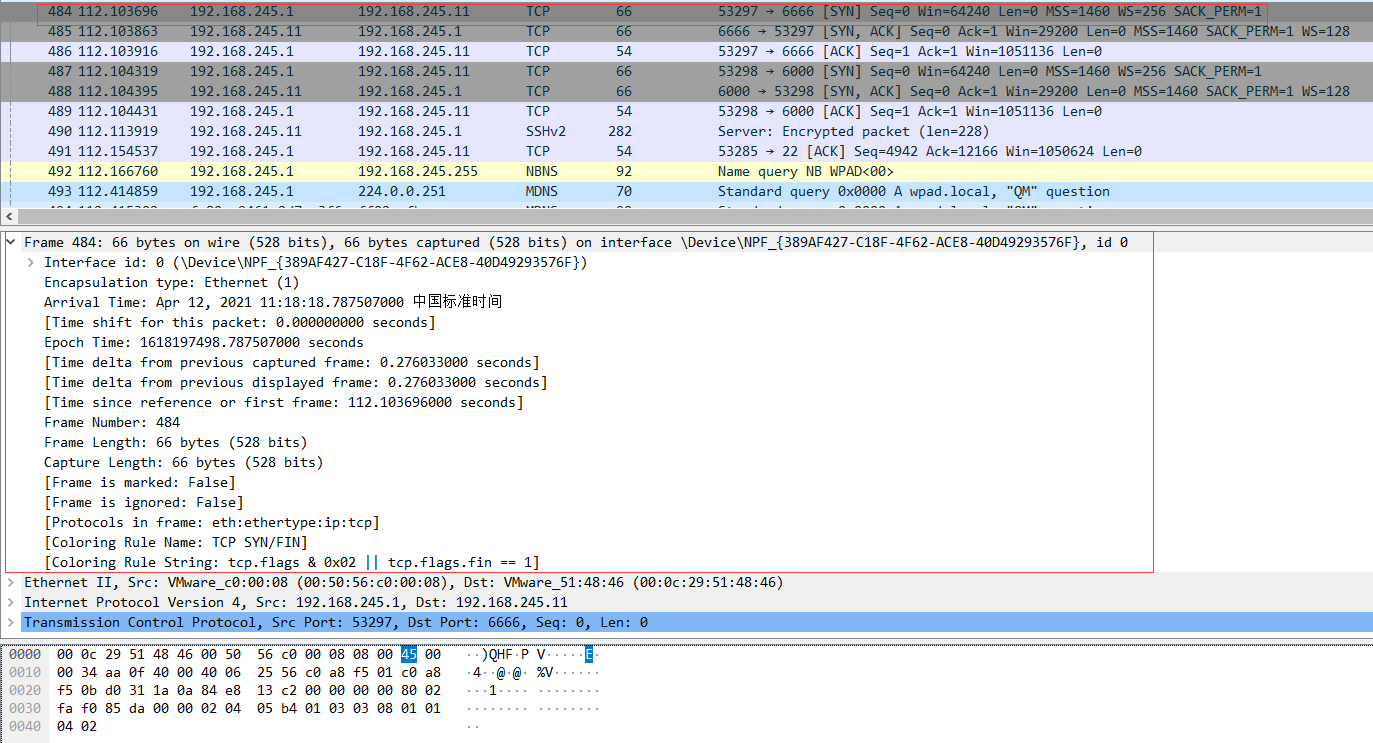
Frame：帧Frame 484 指的是要发送的数据块，其中，所抓帧的序号为484，捕获字节数等于传送字节数：66字节；

Ethernet II：以太网，有线局域网技术，是数据链路层。源Mac地址为00:50:56:c0:00:08；目标Mac地址为00:0c:29:51:48:46；

Internet Protocol Version 4: IPV4协议，也称网际协议，是网络层；源IP地址为192.168.245.1；目标IP地址为192.168.245.11；

Transmission Control Protocol: TCP协议，也称传输控制协议，是传输层；源端口(53297)；目标端口(6666)；序列号(0)；长度为0；

2.1.1、我们具体展开Frame(物理层)，看看详细的信息：



帧Frame 484 指的是要发送的数据块，其中，所抓帧的序号为484，捕获字节数等于传送字节数：66字节；

A. Arrival Time：到达时间，值为Apr 12, 2021 11:18:18.787507000 中国标准时间

B. EPoch Time：信息出现时间，值为1618197498.787507000 seconds

C. [ Time delta from previous captured frame: 0.276033000 seconds] ：与之前捕获的数据帧时间差：0.276033000秒；

     [Time delta from previous displayed frame: 0.276033000 seconds]：与之前显示的帧时间差：0.276033000秒；

     [Time since reference or first frame: 112.103696000 seconds]：距参考帧或第一帧的时间差：112.103696000秒；

D. Frame Number: 484，帧编号为484；

E. Frame Length: 66 bytes (528 bits)，帧长度为66字节；

     Capture Length: 66 bytes (528 bits)，捕获到的长度为66字节；

F. [Frame is marked: False]，帧标记：无；

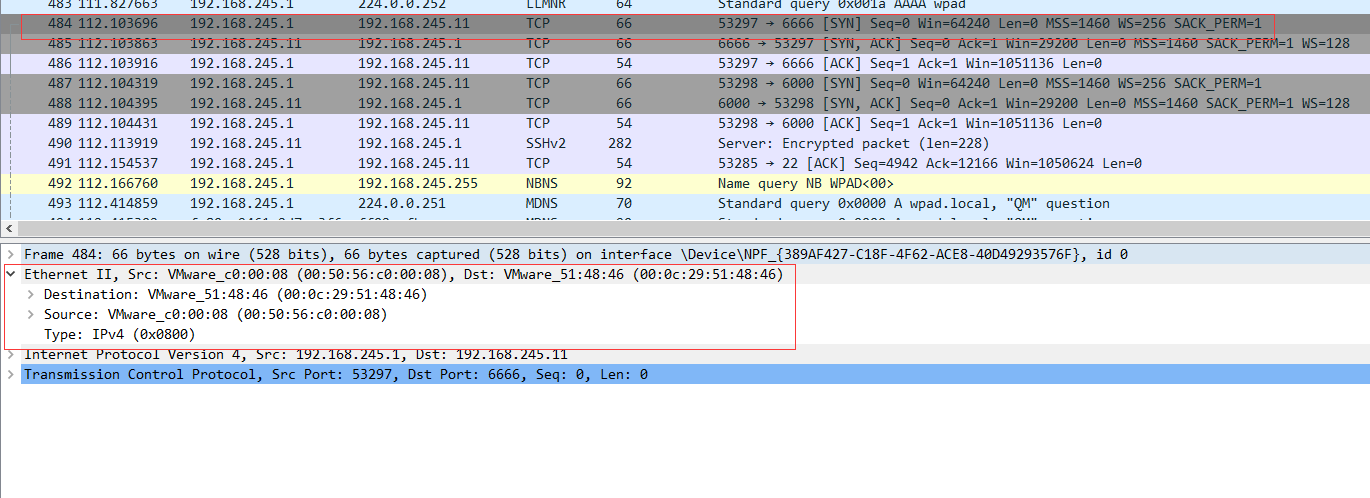
     [Frame is ignored: False]，帧被忽略：无；

G. [Protocols in frame: eth:ethertype:ip:tcp]，协议帧：eth(以太网)、ip、tcp

H. [Coloring Rule Name: TCP SYN/FIN]，色彩规则名称：TCP；

     [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]，色彩规则字符串：TCP；

2.1.2、接下来，我们具体展开Ethernet II (数据链路层以太网帧头部)，看看详细的信息：



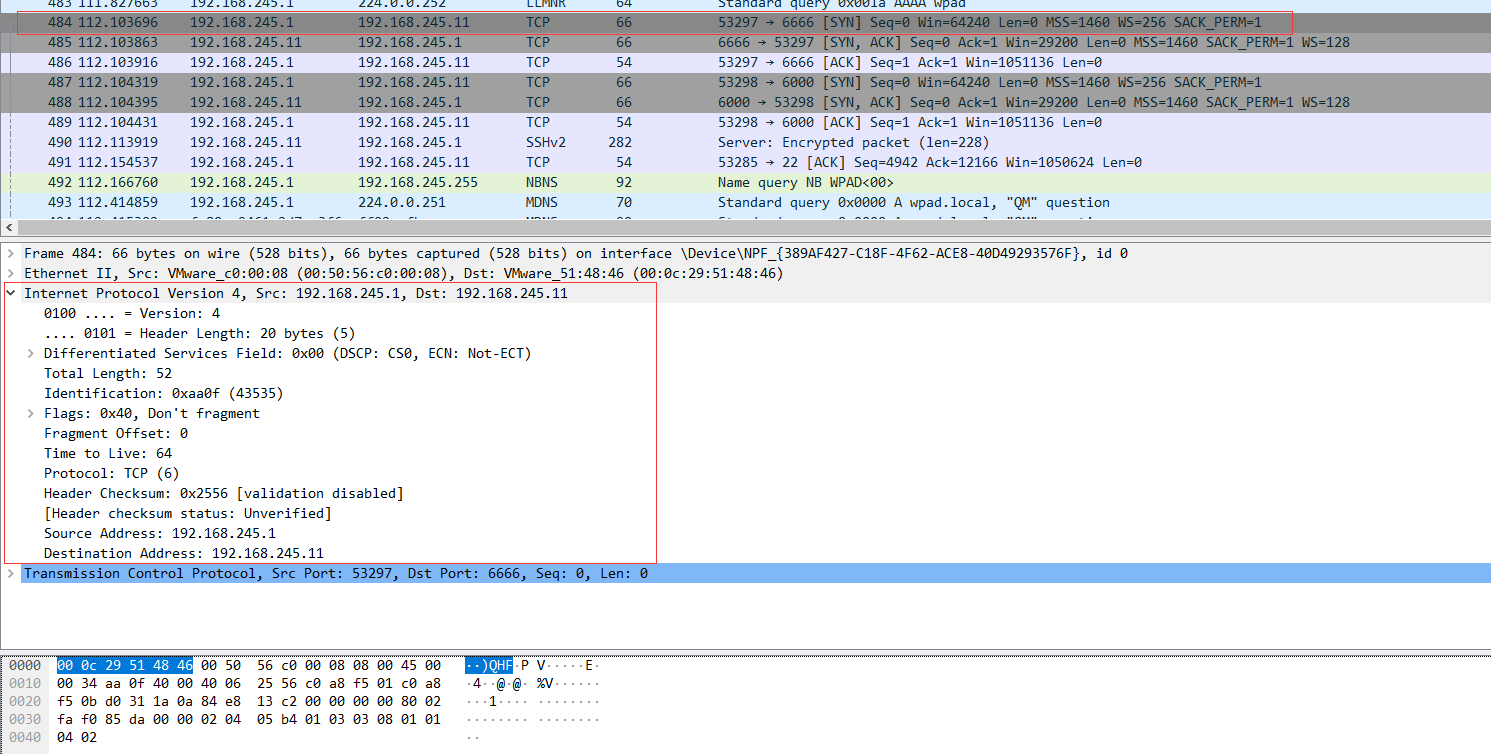
以太网，有线局域网技术，是数据链路层。源Mac地址为00:50:56:c0:00:08；目标Mac地址为00:0c:29:51:48:46；

A. Destination: VMware\_51:48:46 (00:0c:29:51:48:46)，目标Mac地址为00:0c:29:51:48:46

B. Source: VMware\_c0:00:08 (00:50:56:c0:00:08)，源Mac地址为00:50:56:c0:00:08

C. Type: IPv4 (0x0800)，类型是IP数据包

2.1.3、接下来，我们具体展开Transmission Control Protocol (传输层的数据段头部)，看看详细的信息：



IPV4协议，也称网际协议，是网络层；源IP地址为192.168.245.1；目标IP地址为192.168.245.11；

A. 0100 .... = Version: 4，IP协议版本为IPv4；

     .... 0101 = Header Length: 20 bytes (5)，头部数据长度为20字节；

B. Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)，区分的服务领域：0x00 (默认的是DSCP：CS0)；

C. Flags: 0x40, Don't fragment，不支持分组；

     Fragment Offset: 0，分组偏移量为0；

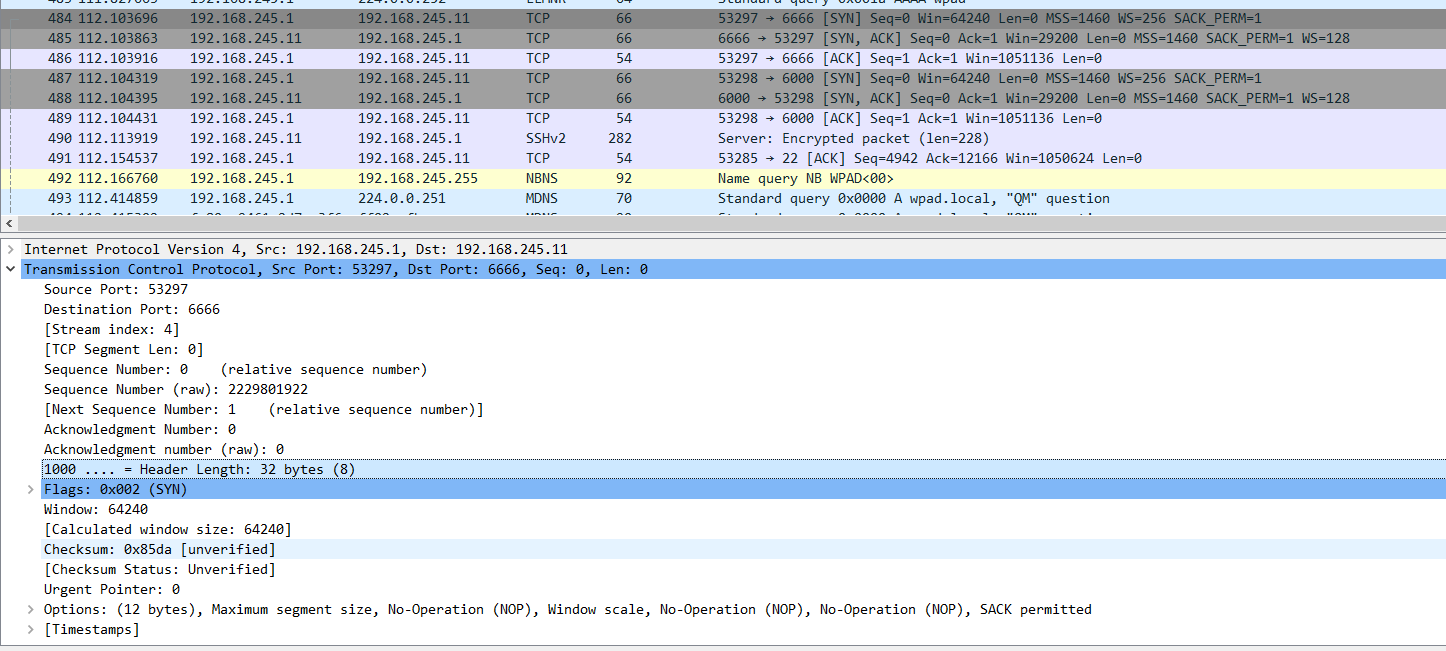
D. Time to Live: 64，TTL，生存时间为64，TTL通常表示包在被丢弃前最多能经过的路由器个数，当数据包传输到一个路由器之后，TTL就自动减1，如果减到0了还没有传送到目标主机，那么就自动丢失。

E. Header Checksum: 0x2556 [validation disabled]，头部校验和

F. Source Address: 192.168.245.1，源IP地址为192.168.245.1；

     Destination Address: 192.168.245.11，目标IP地址为192.168.245.11；

2.1.4、接下来，我们具体展开Internet Protocol Version 4 (互联网层IP包头部)，看看详细的信息：



TCP协议，也称传输控制协议，是传输层；源端口(53297)；目标端口(6666)；序列号(0)；长度为0；

A. 端口号，数据传输的16位源端口号和16位目标端口号(用于寻找发端和收端应用进程)；

B. Sequence Number: 0 (relative sequence number)，相对序列号，该数据包的相对序列号为0(此序列号用来确定传送数据的正确位置，且序列号用来侦测丢失的包)；下一个数据包的序列号是1；

C. Acknowledgment Number: 0，Acknowledgment number是32位确认序列号，值等于1表示数据包收到，确认有效；

D. 1000 .... = Header Length: 32 bytes (8)，手动的数据包的头字节长度是32字节；

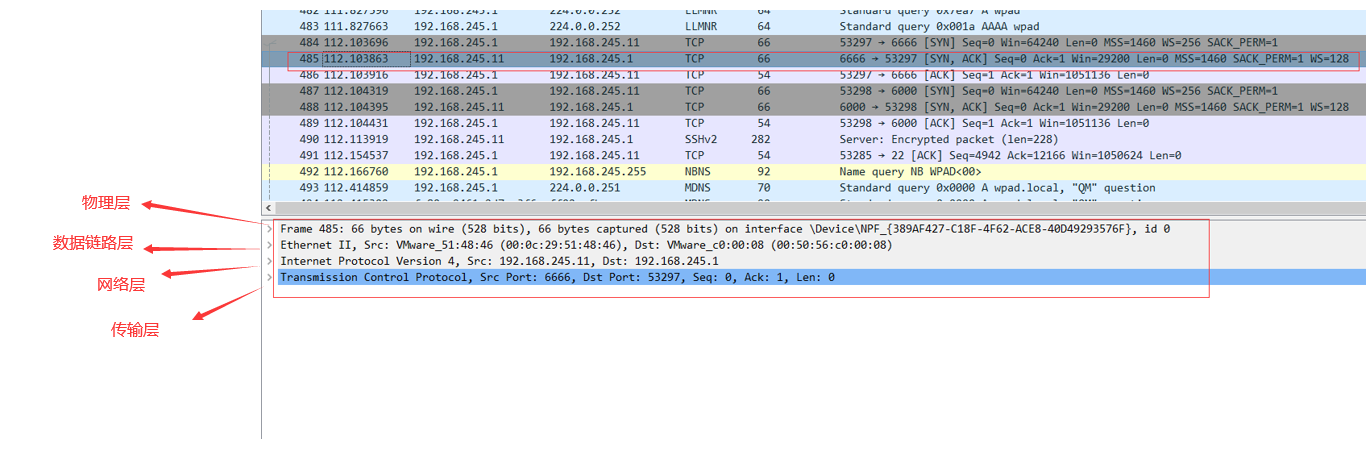
E. Flags，含6种标志；ACK：确认序号有效；SYN：同步序号用来发起一个连接；FIN：发端完成发送任务；RST：重新连接；PSH：接收方应该尽快将这个报文段交给应用层；URG：紧急指针(urgentpointer)有效；

F. window，TCP的流量控制由连接的每一端通过声明的窗口大小来提供。窗口大小为字节数，起始于确认序号字段指明的值，这个值是接收端正期望接收的字节。窗口大小是一个16bit字段，因而窗口大小最大为65536字节，上面显示窗口大小为64240字节；

G. Checksum，16位校验和，检验和覆盖了整个的TCP报文段，由发端计算和存储，并由收端进行验证；

2.2、再是服务器(192.168.245.11)接收到客户端(192.168.245.1)的SYN报文，回复SYN+ACK报文





我们来看看上图的第二个红框，里面包含一下各个层（osi七层协议涉及的层级）的详细信息：

Frame: 物理层数据帧概况

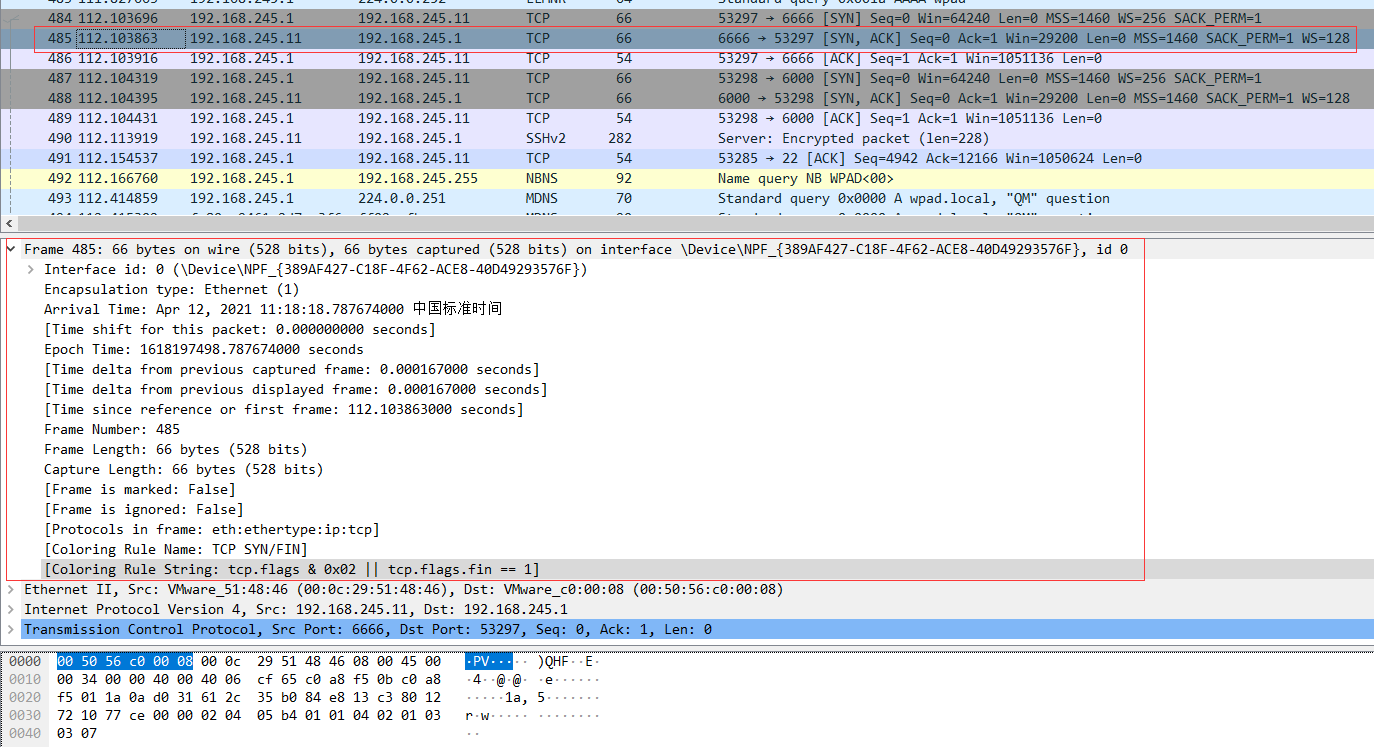
Ethernet II: 数据链路层以太网帧头部

​Internet Protocol Version 4: 互联网层IP包头部

​Transmission Control Protocol: 传输层的数据段头部

​Hypertext Transfer Protocol: 应用层的信息

2.2.1、我们具体展开Frame(物理层)，看看详细的信息：



帧Frame 485 指的是要发送的数据块，其中，所抓帧的序号为485，捕获字节数等于传送字节数：66字节；

A. Arrival Time：到达时间，值为Apr 12, 2021 11:18:18.787674000 中国标准时间

B. EPoch Time：信息出现时间，值为1618197498.787674000 seconds

C. [ Time delta from previous captured frame: 0.000167000 seconds] ：与之前捕获的数据帧时间差：0.000167000秒；

[Time delta from previous displayed frame: 0.000167000 seconds]：与之前显示的帧时间差：0.000167000秒；

[Time since reference or first frame: 112.103863000 seconds]：距参考帧或第一帧的时间差：112.103863000秒；

D. Frame Number: 485，帧编号为485；

E. Frame Length: 66 bytes (528 bits)，帧长度为66字节；

Capture Length: 66 bytes (528 bits)，捕获到的长度为66字节；

F. [Frame is marked: False]，帧标记：无；

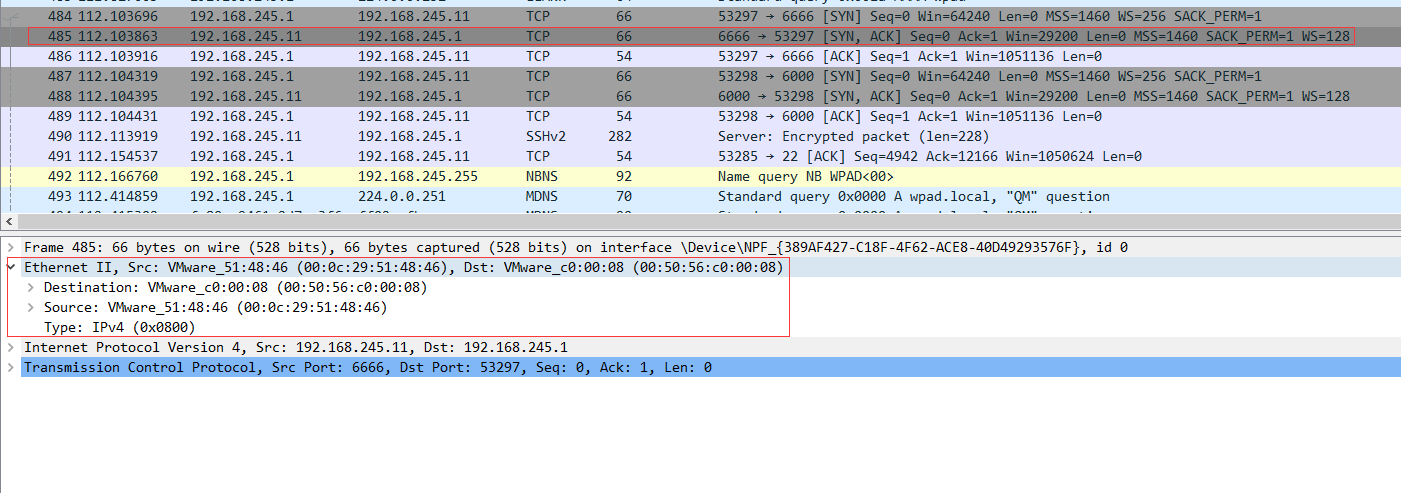
[Frame is ignored: False]，帧被忽略：无；

G. [Protocols in frame: eth:ethertype:ip:tcp]，协议帧：eth(以太网)、ip、tcp

H. [Coloring Rule Name: TCP SYN/FIN]，色彩规则名称：TCP；

[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]，色彩规则字符串：TCP；

2.2.2、接下来，我们具体展开Ethernet II (数据链路层以太网帧头部)，看看详细的信息：



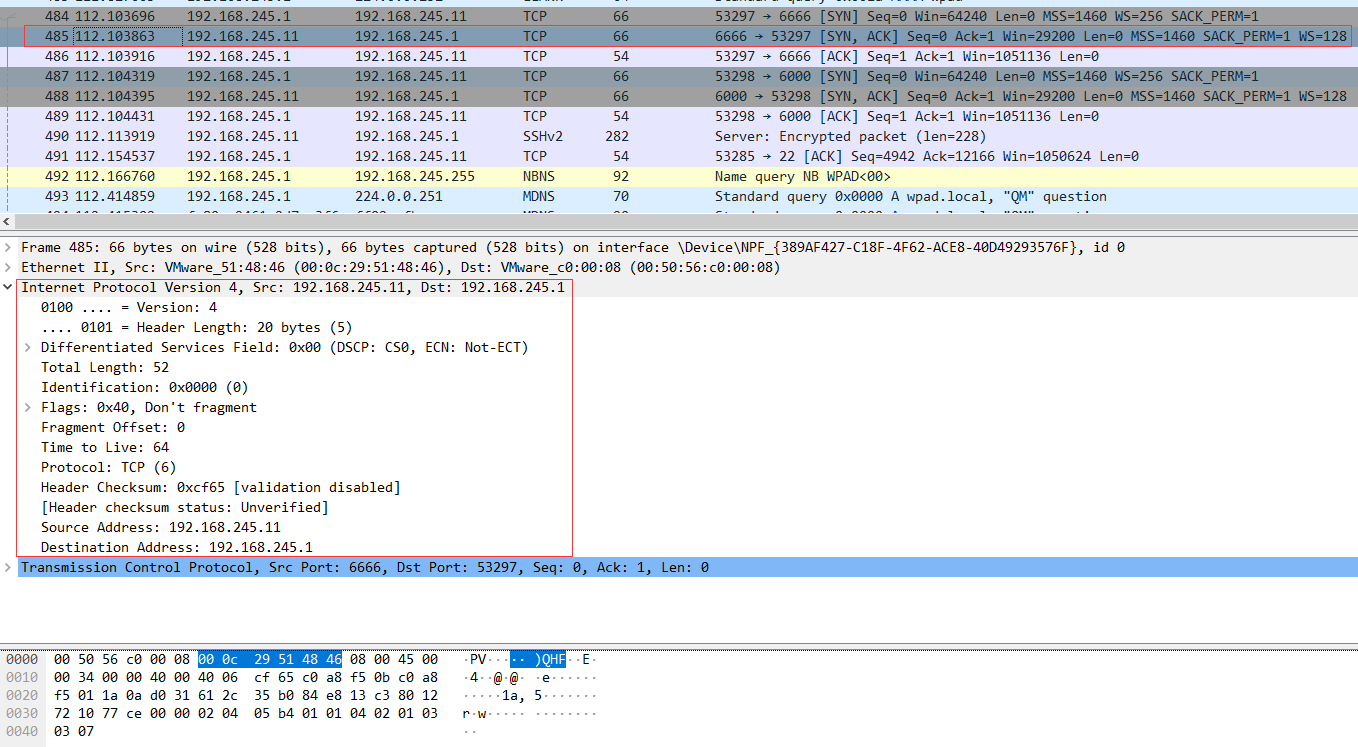
以太网，有线局域网技术，是数据链路层。源Mac地址为00:0c:29:51:48:46；目标Mac地址为00:50:56:c0:00:08；

A. Destination: VMware\_c0:00:08 (00:50:56:c0:00:08)，目标Mac地址为00:50:56:c0:00:08

B. Source: VMware\_51:48:46 (00:0c:29:51:48:46)，源Mac地址为00:0c:29:51:48:46

C. Type: IPv4 (0x0800)，类型是IP数据包

2.2.3、接下来，我们具体展开Transmission Control Protocol (传输层的数据段头部)，看看详细的信息：



IPV4协议，也称网际协议，是网络层；源IP地址为192.168.245.11；目标IP地址为192.168.245.1；

A. 0100 .... = Version: 4，IP协议版本为IPv4；

.... 0101 = Header Length: 20 bytes (5)，头部数据长度为20字节；

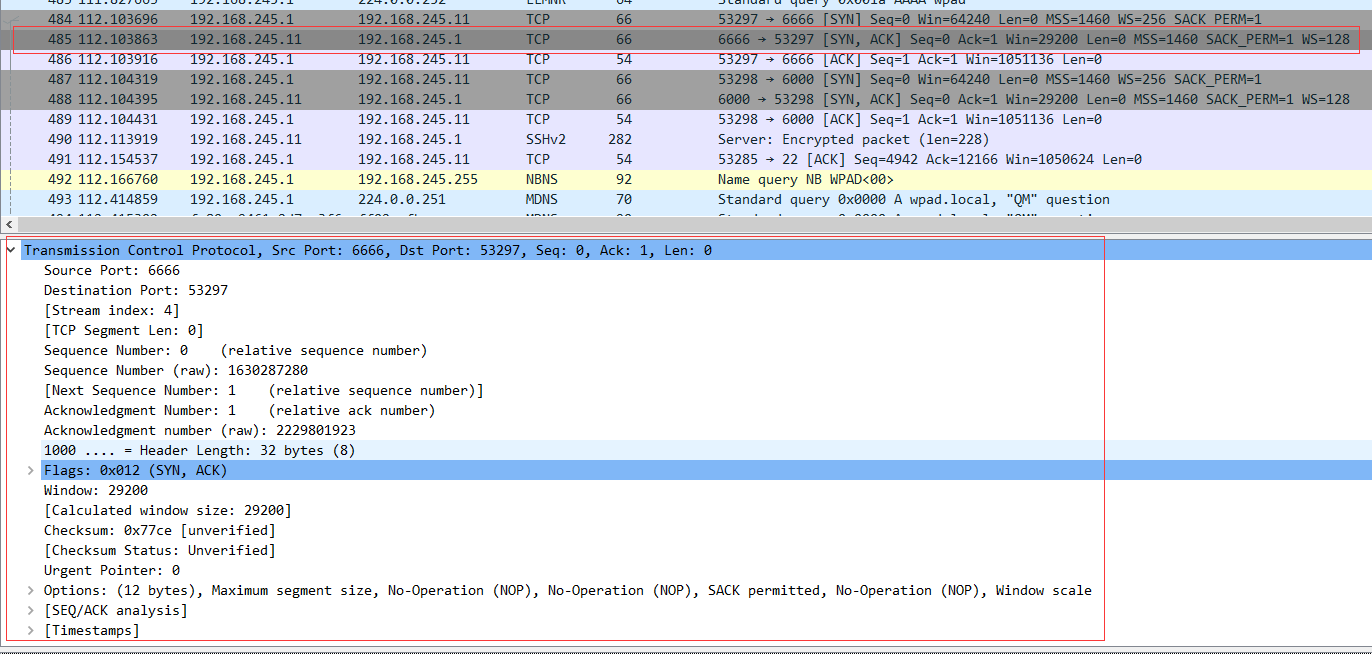
B. Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)，区分的服务领域：0x00 (默认的是DSCP：CS0)；

C. Flags: 0x40, Don't fragment，不支持分组；

Fragment Offset: 0，分组偏移量为0；

D. Time to Live: 64，TTL，生存时间为64，TTL通常表示包在被丢弃前最多能经过的路由器个数，当数据包传输到一个路由器之后，TTL就自动减1，如果减到0了还没有传送到目标主机，那么就自动丢失。

2.2.4、接下来，我们具体展开Internet Protocol Version 4 (互联网层IP包头部)，看看详细的信息：



TCP协议，也称传输控制协议，是传输层；源端口(6666)；目标端口(53297)；序列号(0)；ACK是TCP数据包首部中的确认标志，对已接收到的TCP报文进行确认，值为1表示确认号有效；长度为0；

A. 端口号，数据传输的16位源端口号和16位目标端口号(用于寻找发端和收端应用进程)；

B. Sequence Number: 0 (relative sequence number)，相对序列号，该数据包的相对序列号为0(此序列号用来确定传送数据的正确位置，且序列号用来侦测丢失的包)；下一个数据包的序列号是1；

C. Acknowledgment Number: 0，Acknowledgment number是32位确认序列号，值等于1表示数据包收到，确认有效；

D. 1000 .... = Header Length: 32 bytes (8)，手动的数据包的头字节长度是32字节；

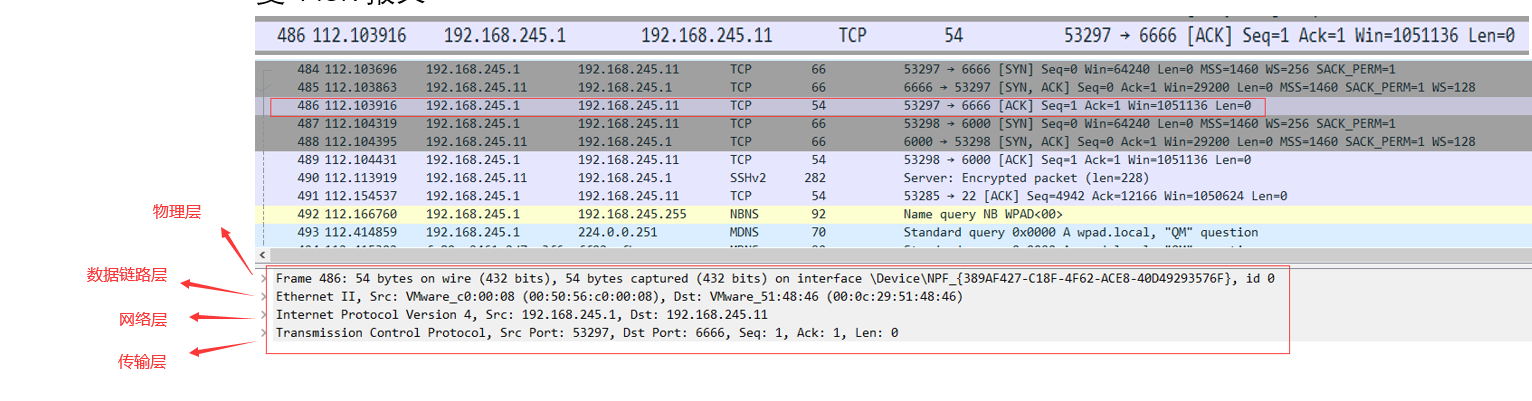
E. Flags，含6种标志；ACK：确认序号有效；SYN：同步序号用来发起一个连接；FIN：发端完成发送任务；RST：重新连接；PSH：接收方应该尽快将这个报文段交给应用层；URG：紧急指针(urgentpointer)有效；

F. window，TCP的流量控制由连接的每一端通过声明的窗口大小来提供。窗口大小为字节数，起始于确认序号字段指明的值，这个值是接收端正期望接收的字节。窗口大小是一个16bit字段，因而窗口大小最大为65536字节，上面显示窗口大小为29200字节；

G. Checksum，16位校验和，检验和覆盖了整个的TCP报文段，由发端计算和存储，并由收端进行验证；

2.3、然后客户端(192.168.245.1)接收到服务端(192.168.245.11)的 SYN+ACK 报文后，回复 ACK报文





我们来看看上图的第二个红框，里面包含一下各个层（osi七层协议涉及的层级）的详细信息：

Frame: 物理层数据帧概况

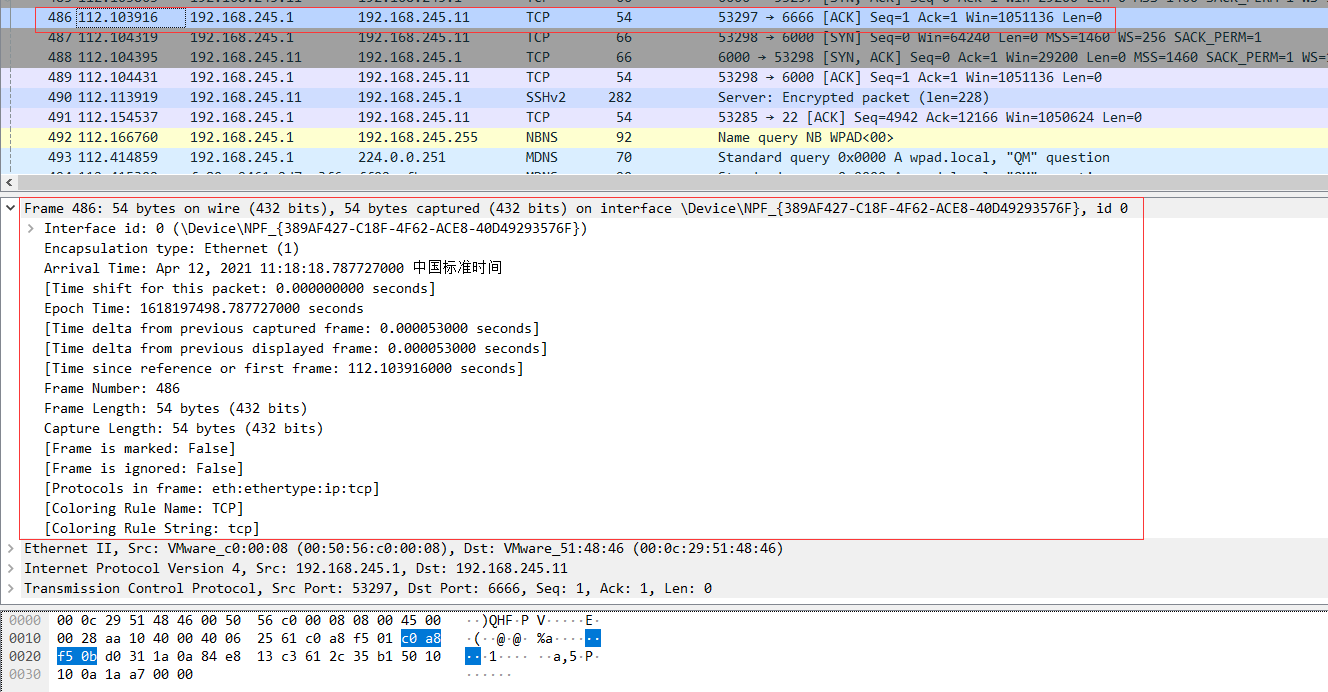
Ethernet II: 数据链路层以太网帧头部

​Internet Protocol Version 4: 互联网层IP包头部

​Transmission Control Protocol: 传输层的数据段头部

​Hypertext Transfer Protocol: 应用层的信息

2.3.1、我们具体展开Frame(物理层)，看看详细的信息：



帧Frame 486 指的是要发送的数据块，其中，所抓帧的序号为486，捕获字节数等于传送字节数：0字节

A. Arrival Time：到达时间，值为Apr 12, 2021 11:18:18.787727000 中国标准时间

B. EPoch Time：信息出现时间，值为1618197498.787727000 seconds

C. [ Time delta from previous captured frame: 0.000053000 seconds] ：与之前捕获的数据帧时间差：0.000053000秒；

[Time delta from previous displayed frame: 0.000053000 seconds]：与之前显示的帧时间差：0.000053000秒；

[Time since reference or first frame: 112.103916000 seconds]：距参考帧或第一帧的时间差：112.103916000秒；

D. Frame Number: 486，帧编号为486；

E. Frame Length: 54 bytes (432 bits)，帧长度为54字节；

Capture Length: 54 bytes (432 bits)，捕获到的长度为54字节；

F. [Frame is marked: False]，帧标记：无；

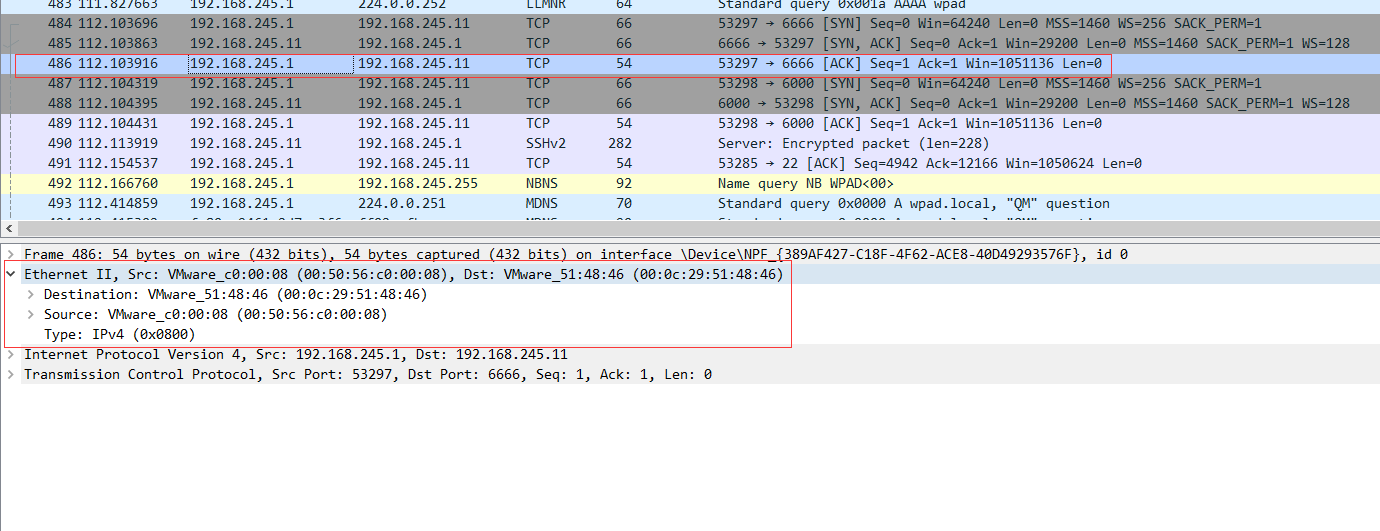
[Frame is ignored: False]，帧被忽略：无；

G. [Protocols in frame: eth:ethertype:ip:tcp]，协议帧：eth(以太网)、ip、tcp

H. [Coloring Rule Name: TCP]，色彩规则名称：TCP；

[Coloring Rule String: tcp]，色彩规则字符串：TCP；

2.3.2、接下来，我们具体展开Ethernet II (数据链路层以太网帧头部)，看看详细的信息：



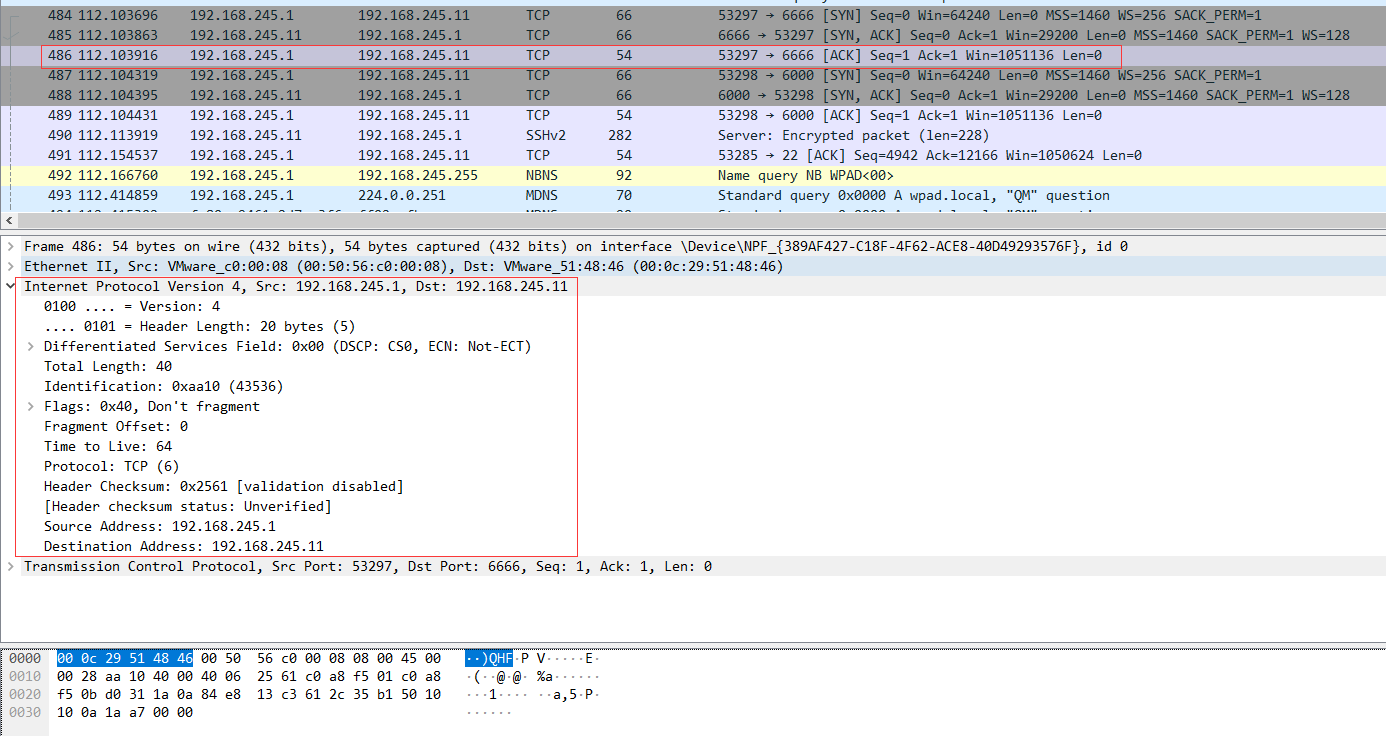
以太网，有线局域网技术，是数据链路层。源Mac地址为00:50:56:c0:00:08；目标Mac地址为00:0c:29:51:48:46；

A. Destination: VMware\_51:48:46 (00:0c:29:51:48:46)，目标Mac地址为00:0c:29:51:48:46

B. Source: VMware\_c0:00:08 (00:50:56:c0:00:08)，源Mac地址为00:50:56:c0:00:08

C. Type: IPv4 (0x0800)，类型是IP数据包

2.3.3、接下来，我们具体展开Transmission Control Protocol (传输层的数据段头部)，看看详细的信息：



IPV4协议，也称网际协议，是网络层；源IP地址为192.168.245.1；目标IP地址为192.168.245.11；

A. 0100 .... = Version: 4，IP协议版本为IPv4；

.... 0101 = Header Length: 20 bytes (5)，头部数据长度为20字节；

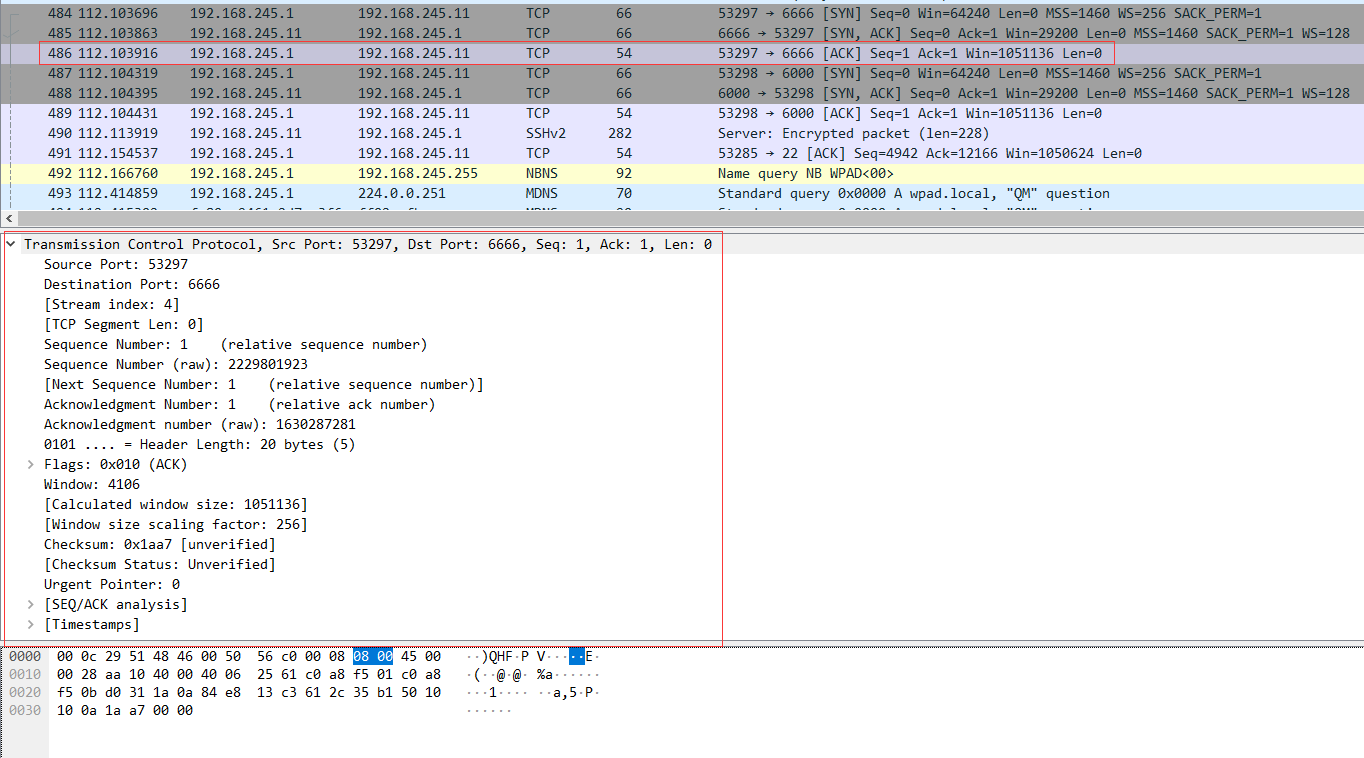
B. Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)，区分的服务领域：0x00 (默认的是DSCP：CS0)；

C. Flags: 0x40, Don't fragment，不支持分组；

Fragment Offset: 0，分组偏移量为0；

D. Time to Live: 64，TTL，生存时间为64，TTL通常表示包在被丢弃前最多能经过的路由器个数，当数据包传输到一个路由器之后，TTL就自动减1，如果减到0了还没有传送到目标主机，那么就自动丢失。

2.3.4、接下来，我们具体展开Internet Protocol Version 4 (互联网层IP包头部)，看看详细的信息：



TCP协议，也称传输控制协议，是传输层；源端口(53297)；目标端口(6666)；序列号(1)；ACK是TCP数据包首部中的确认标志，对已接收到的TCP报文进行确认，值为1表示确认号有效；长度为0；

A. 端口号，数据传输的16位源端口号和16位目标端口号(用于寻找发端和收端应用进程)；

B. Sequence Number: 1 (relative sequence number)，相对序列号，该数据包的相对序列号为0(此序列号用来确定传送数据的正确位置，且序列号用来侦测丢失的包)；下一个数据包的序列号是1；

C. Acknowledgment Number: 1，Acknowledgment number是32位确认序列号，值等于1表示数据包收到，确认有效；

D. 1000 .... = Header Length: 32 bytes (8)，手动的数据包的头字节长度是32字节；

E. Flags，含6种标志；ACK：确认序号有效；SYN：同步序号用来发起一个连接；FIN：发端完成发送任务；RST：重新连接；PSH：接收方应该尽快将这个报文段交给应用层；URG：紧急指针(urgentpointer)有效；

F. window，TCP的流量控制由连接的每一端通过声明的窗口大小来提供。窗口大小为字节数，起始于确认序号字段指明的值，这个值是接收端正期望接收的字节。窗口大小是一个16bit字段，因而窗口大小最大为65536字节，上面显示窗口大小为4106字节；

G. Checksum，16位校验和，检验和覆盖了整个的TCP报文段，由发端计算和存储，并由收端进行验证；