同濟大學
TONGJI UNIVERSITY

计算机网络第三次课程报告

报告主题：使用 wireshark 抓包软件分析各种数据帧

学　　号 2251557

姓　　名 代文波

专　　业 计算机科学与技术

授课老师 陆有军

日期：2024 年 12 月 25 日

一、实验基础：过滤器的使用

1.1、根据协议类型过滤

① tcp ：过滤出协议是 tcp 的包

② udp：过滤出协议是 udp 的包

③ http：过滤出协议是 http 的包

1.2、根据 IP 地址过滤

① ip.src_host == 192.168.1.1 :过滤出源 ip 是 192.168.1.1 的数据包

② ip.dst_host == 192.168.1.1 :过滤出目标 ip 是 192.168.1.1 的数据包

③ ip.addr == 192.168.1.1 :过滤出源 ip 或目标 ip 是 192.168.1.1 的数据包

1.3、根据协议具体内容过滤

tcp.flags.ack ==0 :过滤出 TCP 协议中 ack 位为 0 的数据包

1.4、注意

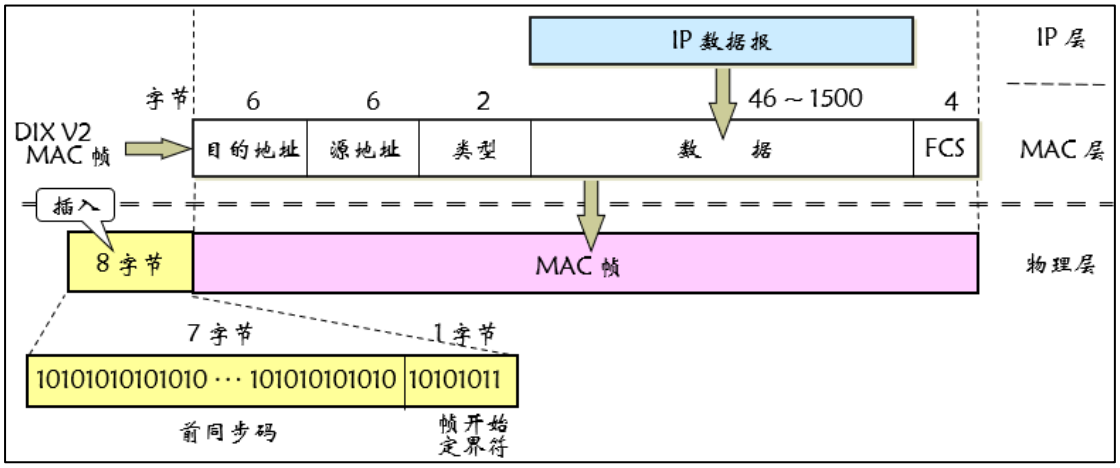
如果需要满足多个条件，只需要使用 and 连接即可

例如：ip.src_host == 192.168.2.1 and ip.dst_host == 192.168.3.1 :过滤出源 ip 是 192.168.2.1 并且目标地址是 192.168.3.1 的数据包

二、以太网 MAC 帧

2.1 理论分析

以太网 MAC 帧格式（以老师讲的 DIX V2 MAC 帧为例）：



（1）前导码（是由物理层加上）：8B（10101010），用于接收方与发送方的时钟同步。

（2）目的地址：6B，用于标识接收方

（3）源地址：6B，用于标识发送方

（4）类型字段：2B，指明数据字段中数据的协议类型。例：IPv4:0x0800、ARP:0x0806、PPPoE:0x8864 等。

（5）数据字段：46～1500B，用户数据，不够填充以满足最短帧长（64B）的要求。

（6）FCS 字段：4B 的 CRC 校验码，校验范围不包括前导码。

2.2 实验抓包

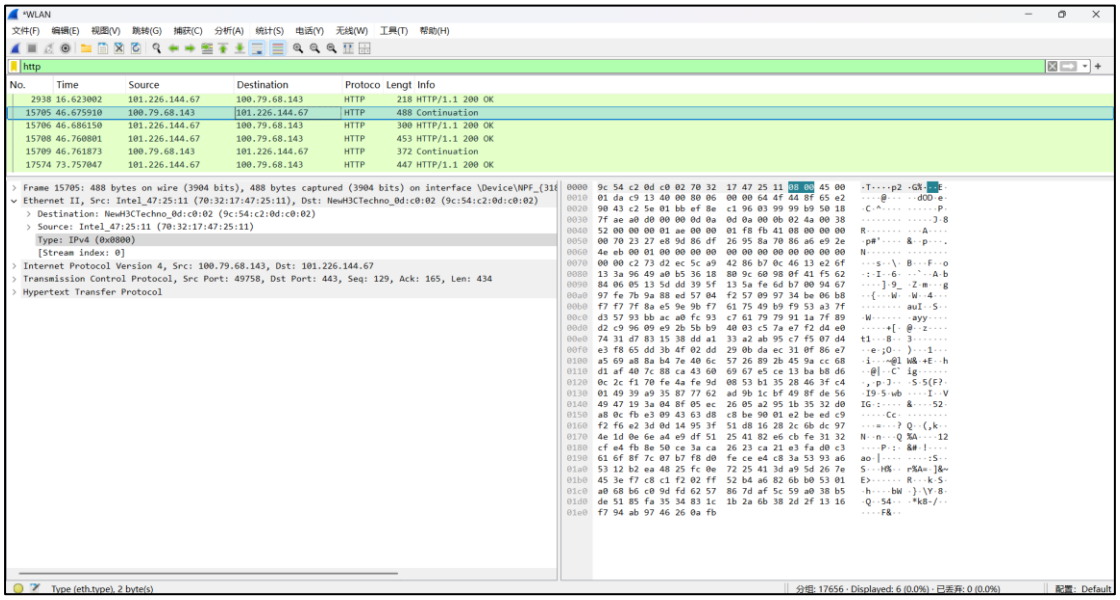
（1）打开 wireshark

（2）设置过滤器为 http，开始抓包

（3）在浏览器中访问百度，即 https://www.baidu.com/

（4）停止抓包，查看抓包结果

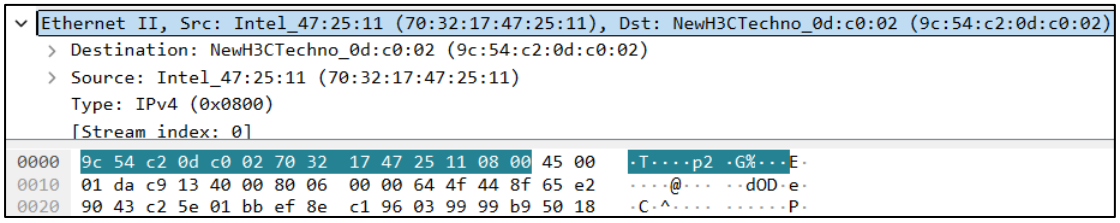
在捕获界面，点击 Destination 为 101.226.144.67 的帧



2.3 抓包结果分析

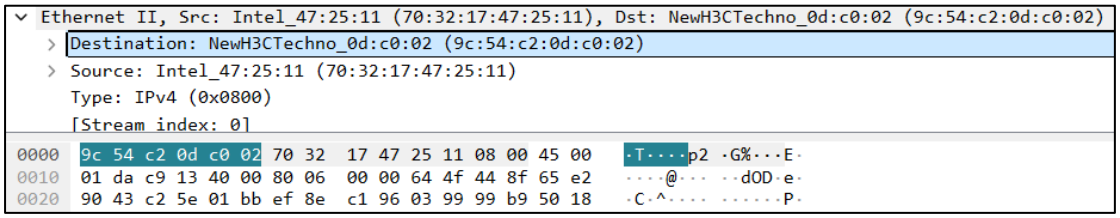
（1）本次抓包得到的以太网 MAC 帧如下：

9c 54 c2 0d c0 02 70 32 17 47 25 11 08 00

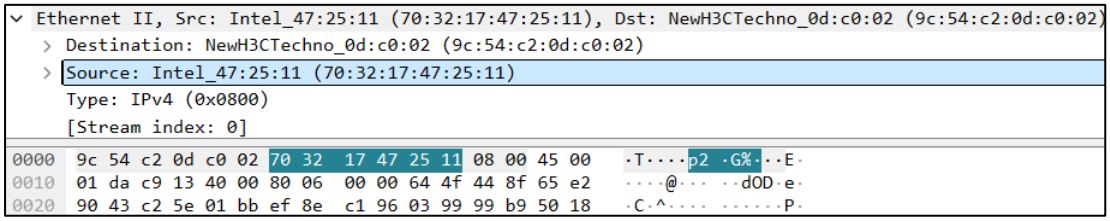


（2）各部分详细分析

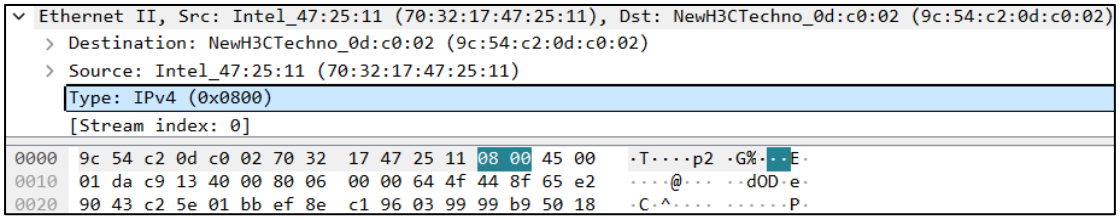
① 目的地址（6B）：9c 54 c2 0d c0 02



② 源地址（6B）：70 32 17 47 25 11



③类型（2B）：08 00（也就是 IPv4 协议）

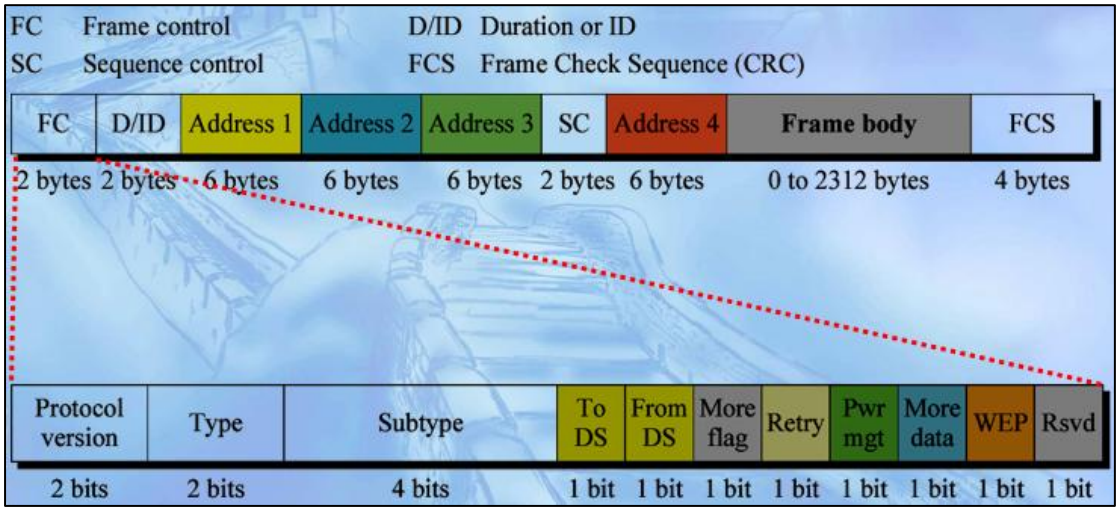


经分析，上述结果与理论完全吻合

三、无线局域网 MAC 帧

3.1 理论分析

无线局域网 MAC 帧格式：



（1）FC 字段（Frame Control 字段）：2B，规定了帧的类型和控制功能，具体可细分为以下几个部分：

① Protocol version ：2bits ，标识协议版本，当前版本为 0，其余的留给未来使用。

② Type ：2bits ，标志 WLAN 的帧类型，如管理（00）、控制（01）、数据（00）。

③ Subtype ：4bits ，提供每一类帧更细致准确的帧类型，要和 Type 字段配合使用。

④ 此外，还有 To DS(1bit)、From DS(1bit)、More flag(1bit)、Retry(1bit)、Pwr mgt(1bit)、More data(1bit)、WEP(1bit)、Rscd(1bit)字段

（2）Duration or ID 字段：2B，持续时间，标识该帧传输需要多长时间，方便其他设备知道该信道什么时候可以再次使用。

（3）Address1 字段：6B，接收方地址

（4）Address2 字段：6B，发送方地址

（5）Address3 字段：6B，用于接收方过滤目的

（6）SC 字段（Sequence Control 字段）：2B，前 4 位用于分片号，后 12 位用于序列号。这一字段用于识别信息顺序，方便消除重复帧。

（7）Address4 字段：6B，扩展地址，只存在于扩展服务集的接入点之间或网状网络的中间

节点之间传输的数据帧中

（8）Frame Body 字段：0-2312B，有效帧体

（9）FCS 字段（Frame Check Sequence 字段）：4B，用于帧校验，通常使用循环冗余检查码（CRC），它允许对检索的帧进行完整性检查。当帧即将被发送时，FCS 被计算和附加。当一个站收到一个帧时，它可以计算出该帧的 FCS 并与收到的帧进行比较。如果它们相匹配，就可以认为该帧在传输过程中没有失真。

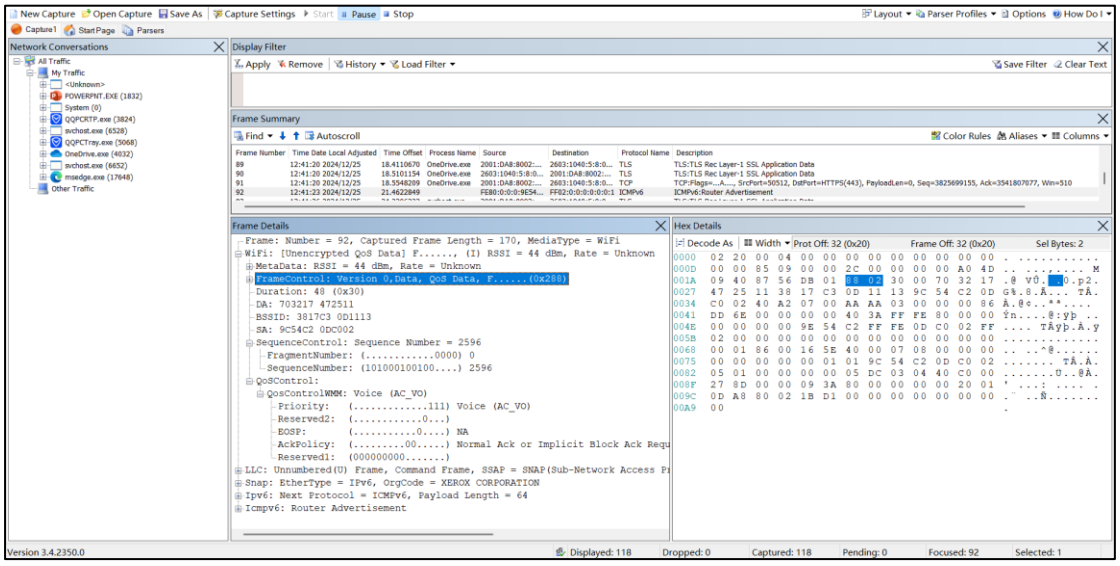
3.2 实验抓包

由于网卡不支持监听模式，所以这里改用 MNM（Microsoft Network Monitor）软件来抓包

（1）新建抓取文件

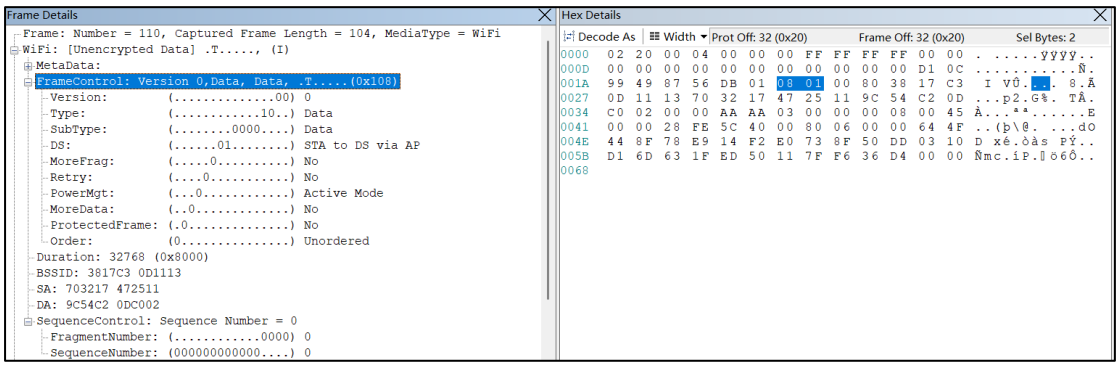
（2）点击“START”开始抓包

（3）一段时间后，停止抓包，在捕获界面选择合适的帧查看

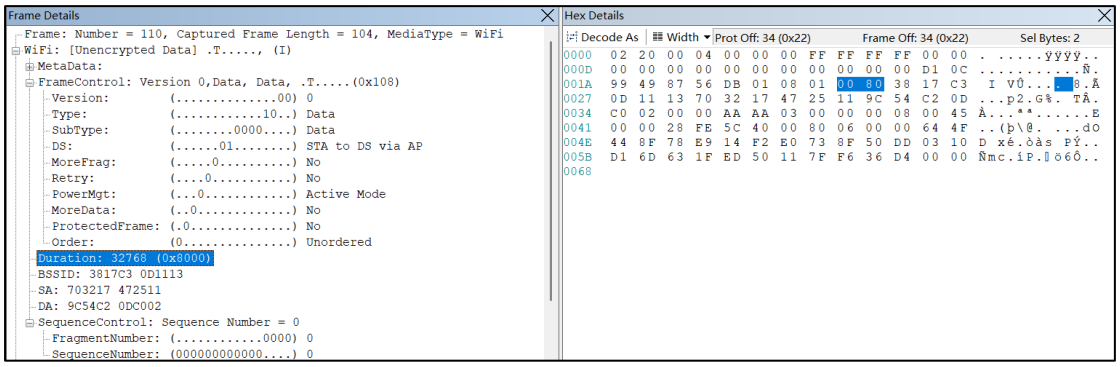


3.3 抓包结果分析

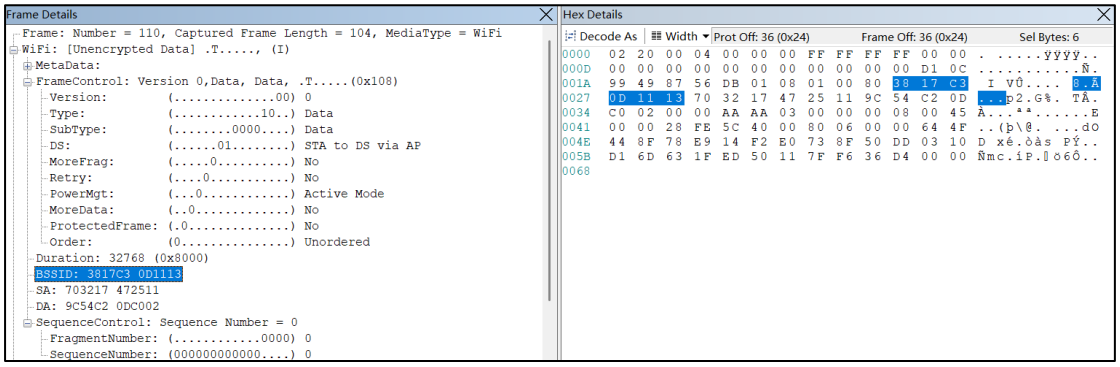
（1）FC 字段（Frame Control 字段，2B）：01 08



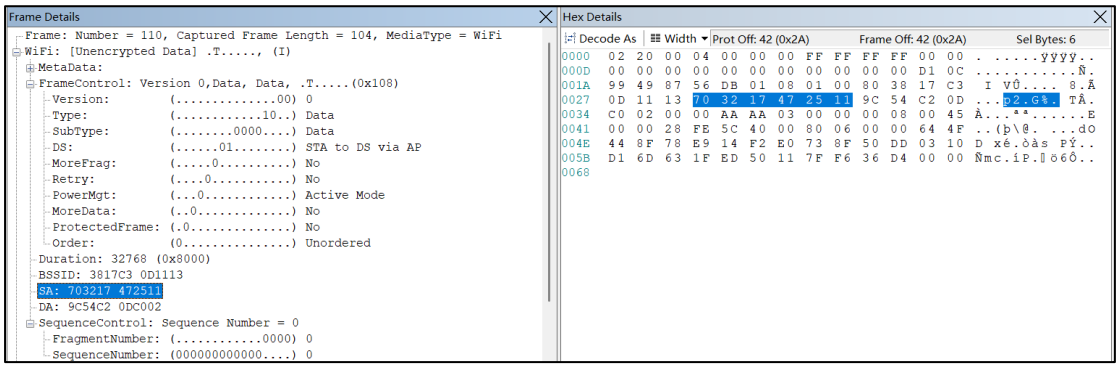
（2）Duration or ID 字段（2B）：80 00



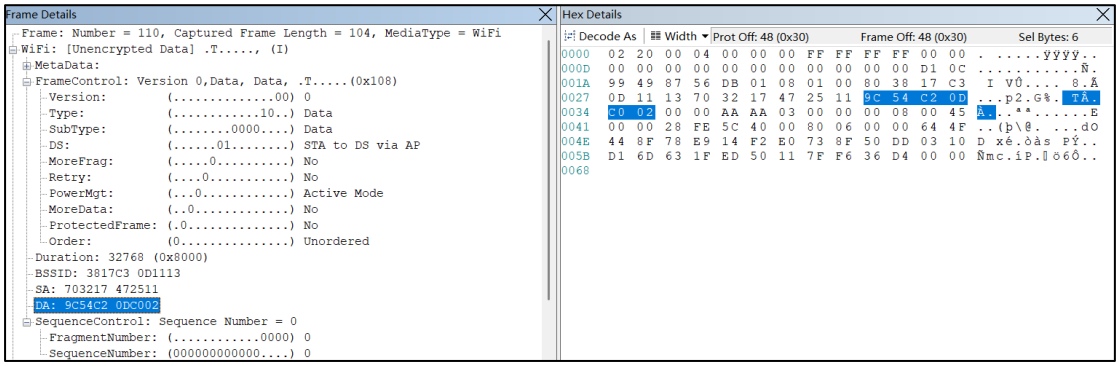
（3）BSSID（6B）：38 17 C3 0D 11 13



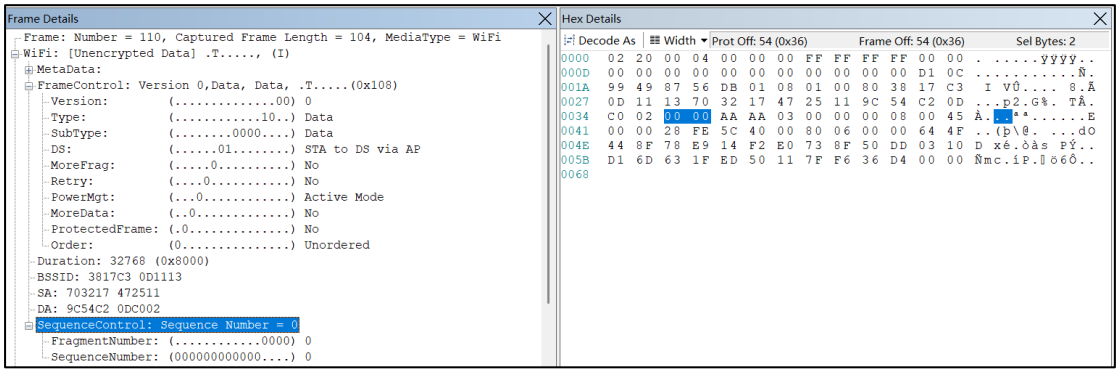
（4）发送方地址（6B）：70 32 17 47 25 11



（5）接收方地址（6B）：9C 54 C2 0D C0 02



（6）SC 字段（2B）：00 00



经分析，上述结果与理论基本一致

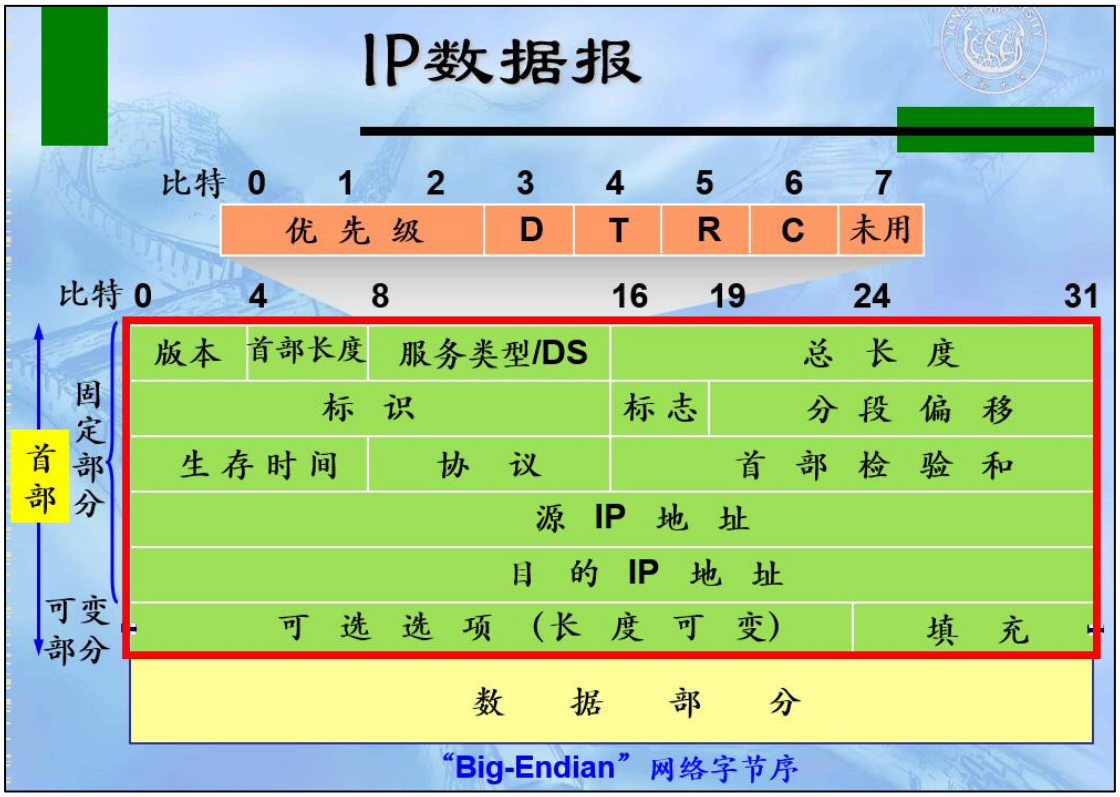
四、IP 协议

4.1 理论分析

IP 协议:

网际协议（Internet Protocol，缩写：IP），又称互联网协议，是用于分组交换数据网络的协议。 IP 是在 TCP/IP 协议族中网络层的主要协议，任务仅仅是根据源主机和目的主机的地址来传送数据。

IPv4 报文结构：



（1）首部：由固定首部和拓展首部组成。

[1] 固定首部：长度固定（20B），所有 IP 数据报都必须具备

① 版本(4bit):定义 IP 协议的版本。通信双方所使用的版本必须一致，目前版本是 4，版本 6 将取代版本 4。

② 首部长度（IHL，4bit）：定义 IP 数据报首部（固定首部+扩展首部）的总长度，以 4B 度量单位。取值范围为[5,15]。

③ 总长度（16bit）：定义整个 IP 数据报的长度（首部+数据），度量单位为字节（1B）。

④ 服务类型/DS（8bit）IETF 已经改变了本字段的名称和内容。以前本

字段称为服务类型，现在本字段称为区分服务（DS）。

⑤ 标识（16bit）：用于标识不同的 IP 数据报，同一 IP 数据报的所有分段具有相同的标识。

⑥ 标志（3bit）：第 1bit 保留，第 2bit 用作 DF（Don’t Fragment）字段：1 不允许分段，0 允许分段；第 3bit 用作 MF（More Fragment）字段：1 表示后面还有分段，0 表示是最后一个分段。

⑦ 段偏移（13bit）：表示本分段在 IP 数据报中的相对位置（度量单位为 8B），即相对于用户数据字段的起点。

⑧ 生存时间（TTL，8bit）：IP 数据报在通过 Internet 时所具有的寿命。发送时存入一个数，每经过一个路由器将此数减 1，为 0 时丢弃。用于防止 IP 数据报无休止地传输或限制 IP 数据报的行程（为 1 限制在本网络内）。

⑨ 协议（8bit）：定义使用 IP 服务的高层协议，以便目的主机的网络层上交数据。例如：UDP(17)、TCP(6)、ICMP(1)等。

⑩ 首部校验和（16bit）：不采用 CRC 码而采用简单的计算方法。

⑪ 地址：源 IP 地址（4B）和目的 IP 地址（4B）。

[2] 扩展首部：一些可选选项，长度可变（0～40B）

扩展首部就是一个选项字段，长度可变，从 1B 到 40B 不等，取决于所选择的项目；最初设计时定义了 5 个选项：安全性、严格源路由、松散源路由、记录路由、时间戳；实际上这些选项很少被使用，如感兴趣请参阅 RFC 791。

（2）数据

IP 数据报的理论最大长度为 65535B，但实际 IP 数据报的长度很少有超过 1500B 的。

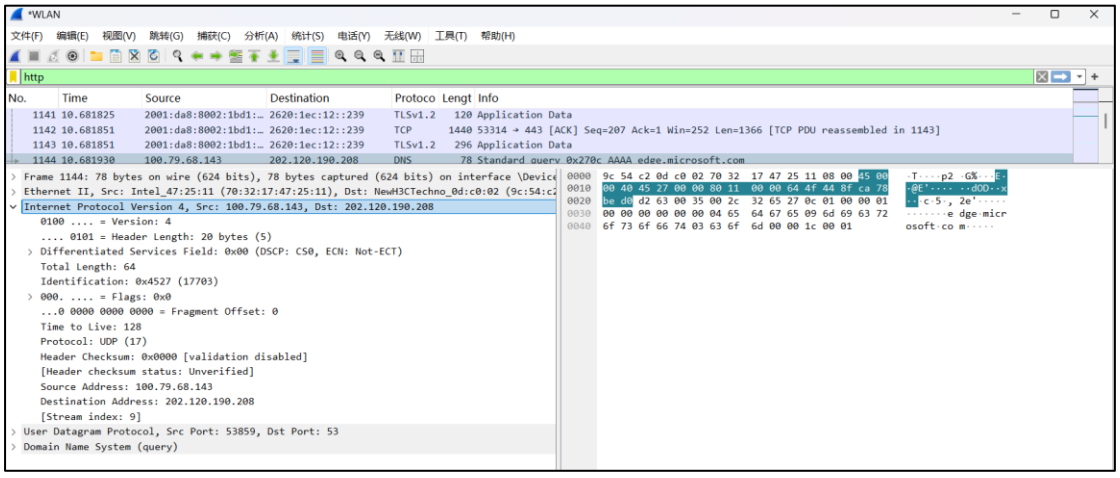
4.2 实验抓包

（1）打开 wireshark

（2）设置过滤器为 http，开始抓包

（3）在浏览器中访问百度，即 https://www.baidu.com/

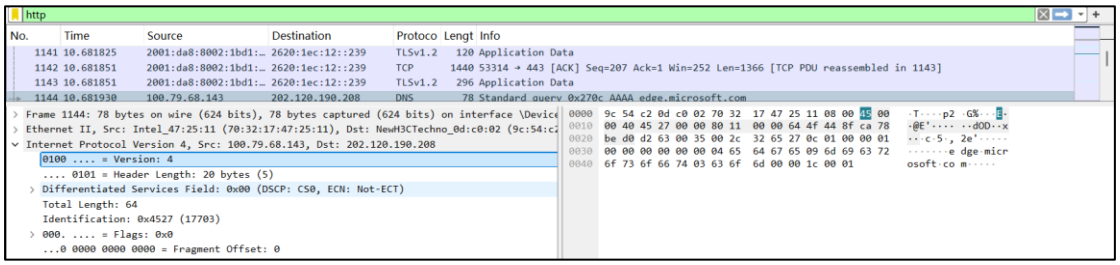
（4）停止抓包，查看抓包结果



4.3 抓包结果分析

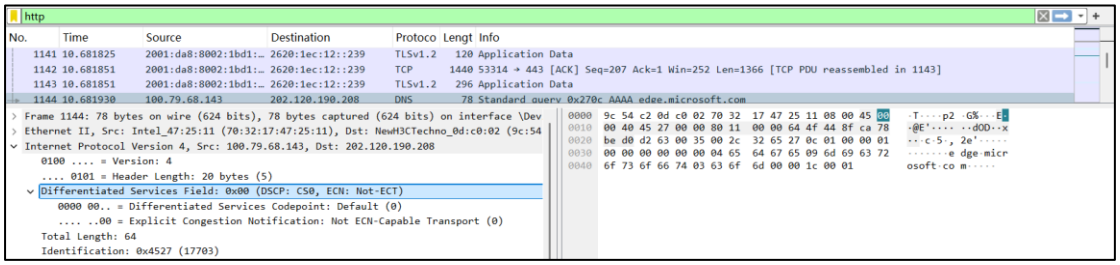
（1）版本（4bits）+首部长度（4bits）：45

此处版本号为 4，即 IPv4；长度为 20B



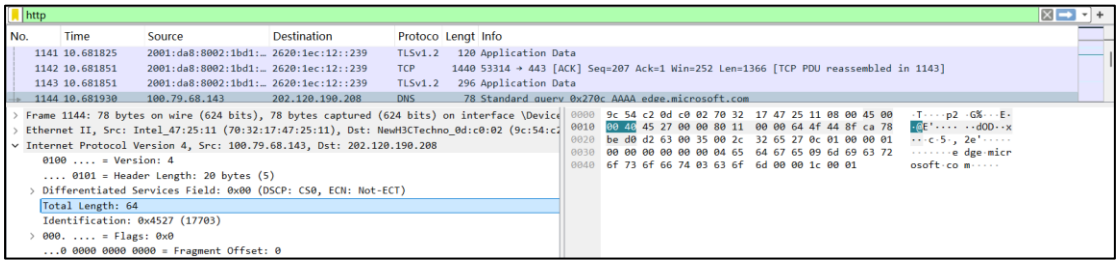
（2）服务类型 DS（8bits）：

这里是 DS 区分服务的，所以是 00



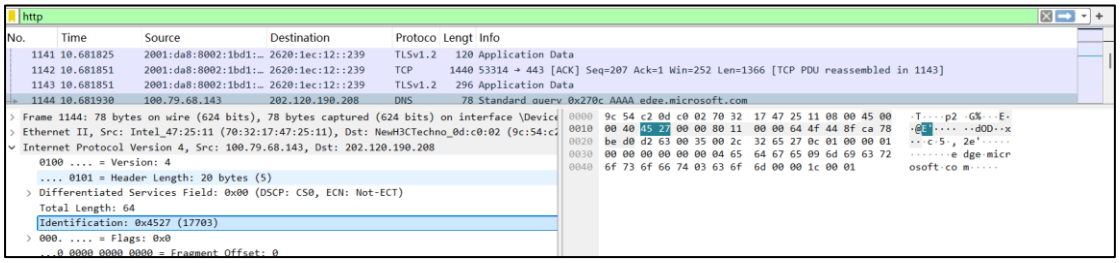
（3）总长度（16bits）：00 40

这里总长度为 64。



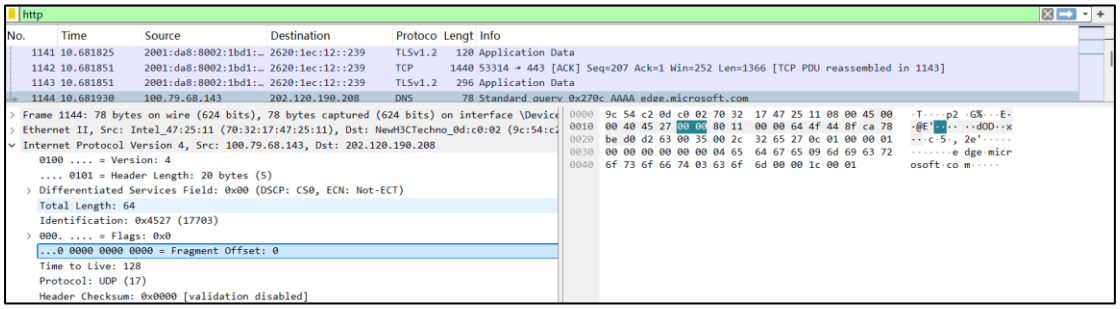
（6）标识（16bit）：45 27

这里标志为 17703。

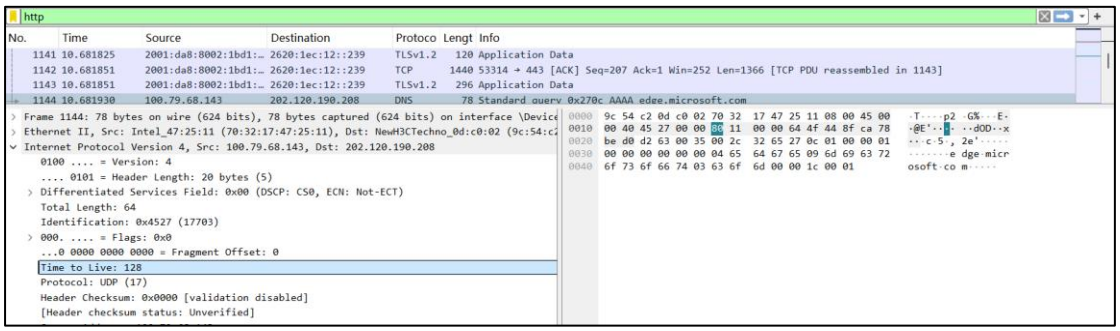


（7）标志（3bit）+ 段偏移（13bit）：00 00

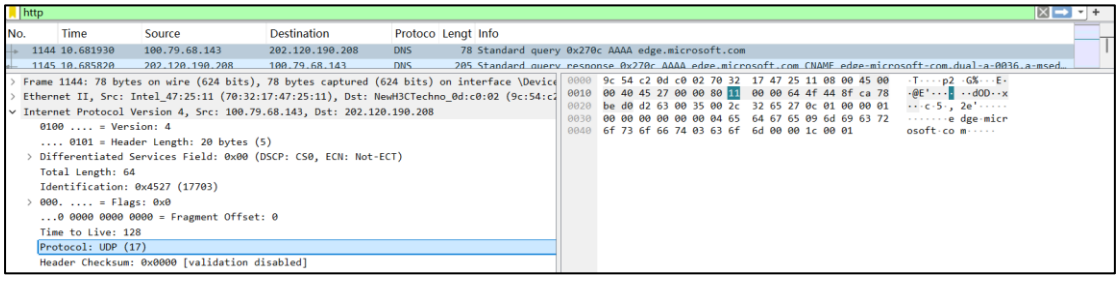
此处显示不允许分片置 0，段偏移量为 1。



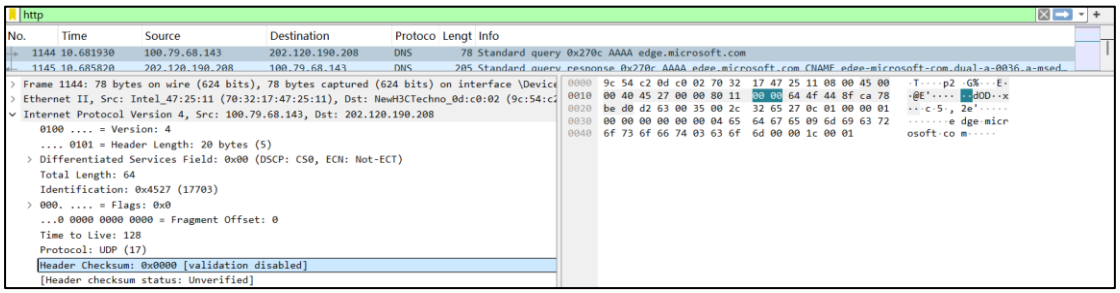
（8）生存时间（TTL，8bit）：80



（9）协议（8bit）：11

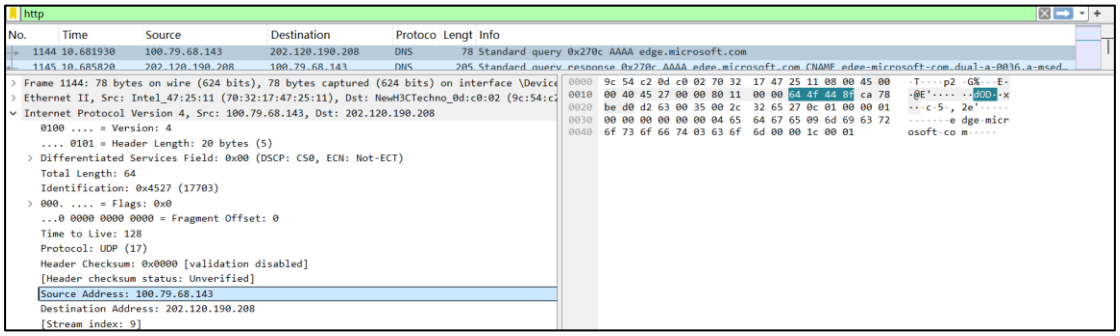


（10）首部校验和（16bit）：00 00



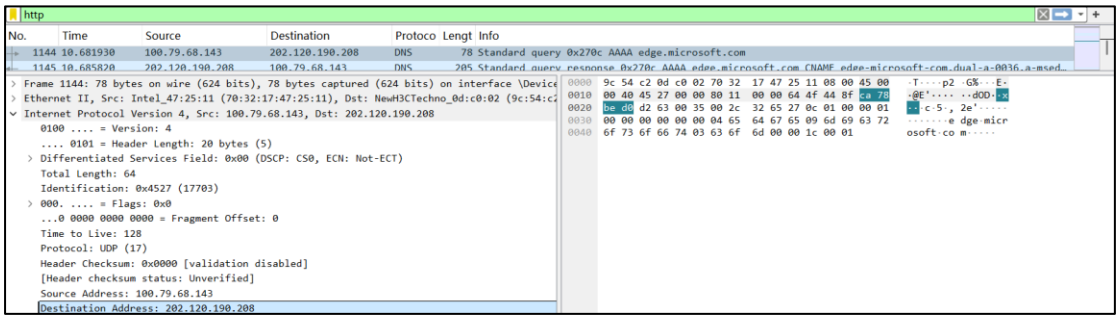
（11）源 IP 地址（4B）：64 4f 44 8f

此处源 IP 地址是 100.79.68.143



（12）目的 IP 地址（4B）：ca 78 be d0

此处目标地址为：202.120.190.208



经分析，与理论分析基本吻合。

五、TCP 协议

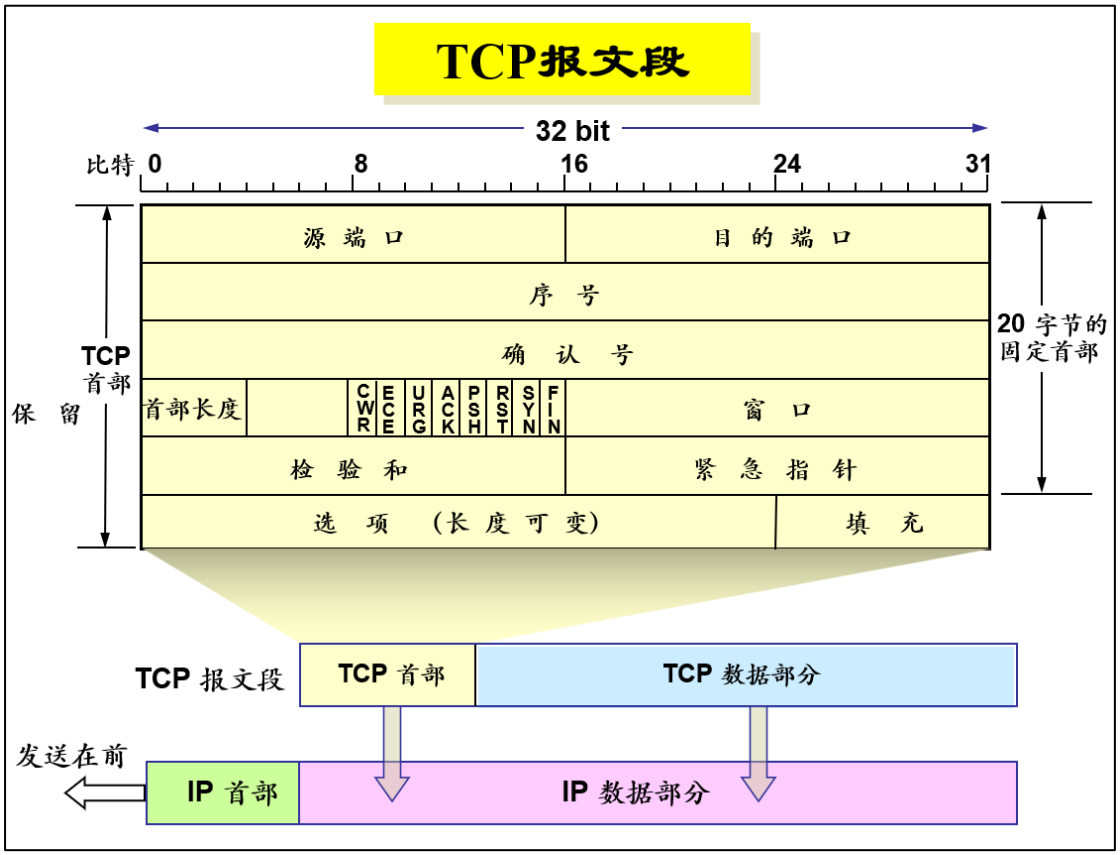
5.1 理论分析

TCP 协议：

传输控制协议（TCP，TransmissionControl Protocol）是一种面向连接的、可靠的、基于字节流的传输层通信协议，由 IETF 的 RFC 793 定义。TCP 旨在适应支持多网络应用的分层协议层次结构，互连的计算机通信网络中成对的应用程序进程之间能够依靠 TCP 提供可靠的通信服务来传输字节流。TCP 支持双向数据流，应用程序也可以仅单向发送数据。在主机之间，TCP 使用端口号标识应用程

序服务并且可以多路传输数据流。

TCP 报文：



（1）固定首部（20B）：

①端口：源端口和目的端口（各 2B）。端口是传输层与应用层的服务接口。传输层的复用和分用功能都要通过端口才能实现。

②序号：4B。TCP 连接中传送的数据流中的每一个字节都编上一个序号。序号字段的值则指的是本报文段所发送的数据的第一个字节的序号。

③确认号：4B，是期望收到对方的下一个报文段的数据的第一个字节的序号。

④ 首部长度：4bit，TCP 报文段的首部长度（4B 为计算单位），长度范围[20B，60B]。

⑤ 保留：4bit，保留为今后使用，但目前应置为 0。

⑥ 标志位：

[1] 显式拥塞通知（ECN）

当 TCP 接收端收到来自网络的拥塞提示后，就设置 ECE 以便给 TCP 发送端发 ECN-Echo 信号，告诉发送端放慢发送速度；TCP 发送端设置

CWR 以便给 TCP 接收端发 CWR 信号，这样接收端就知道发送端已经放慢速率，不必再给发送端发 ECN-Echo 信号。

[2] 紧急比特 URG

URG =1 表明紧急指针字段有效。它告诉系统此报文段中有紧急数据（放在最前面），应尽快传送（相当于高优先级的数据），而不要按原来的排队顺序来传送。本字段需与“紧急指针”字段（16bit。用于指出紧急数据的字节数，即指出紧急数据的末尾） 配合使用。

[3] 确认比特 ACK

ACK =1 时“确认号”字段有效，ACK=0 时 “确认号”字段无效。[4]

[4] 推送比特 PSH

接收 TCP 收到 PSH=1 的报文段，就尽快地交付给接收应用进程，而不再等到整个缓存都填满了后再向上交付。

[5] 复位比特 RST

RST=1 表明 TCP 连接中出现严重差错（如由于主机崩溃）必须释放连接，然后再重新建立传输连接。

[6] 同步比特 SYN

在连接建立时用来同步序号。当 SYN=1 且 ACK=0 表示这是一个连接请求报文段，当 SYN=1 且 ACK=1 表示这是一个连接接受报文段。

[7] 终止比特 FIN

用来释放一个连接。FIN=1 表明此报文段的发送端的数据已发送完毕，并要求释放传输连接。

⑦窗口字段 :2B。用来控制对方发送的数据量（单位为 1B）。TCP 连接的一端根据设置的缓存空间大小确定自己的接收窗口大小，然后通知对方以确定对方的发送窗口的上限。

⑧ 检验和:2B。检验范围包括首部和数据两部分。在计算检验和时，要在 TCP 报文段的前面加上 12B 的伪首部（同 UDP，但应将伪首部的第 4 个字段由 17 改为 6，第 5 字段中的 UDP 长度改为 TCP 长度）。

⑨紧急指针（16bits）：紧急指针指出在本报文段中的紧急数据的最后一个字节的序号。

（2）可变部分：

① 最大报文段长度 MSS 选项：MSS 告诉对方 TCP：“我的缓存所能接收的报文段的数据字段的最大长度是 MSS 个字节。” ；

② 窗口扩大选项：3B，其中有 1B 表示移位值 S（最大值为 14）。新的窗口值等于 TCP 首部中的窗口位数增大到(16 + S)，相当于把窗口值向左移动 S 位后获得实际的窗口大小；

③ 时间戳选项：10B，其中最主要的字段时间戳值字段（4 B，记录报文段发送时间）和时间戳回送回答字段（4 B，复制报文段发送时间）；作用：计算往返时间 RTT、防止序号绕回（PAWS）；

④ 选择确认选项（SACK）：使得接收端可以告诉发送端已经接收报文段的序号范围，这是对确认号字段的补充 。

⑤ 填充：这是为了使整个首部长度是 4B 的整数倍。

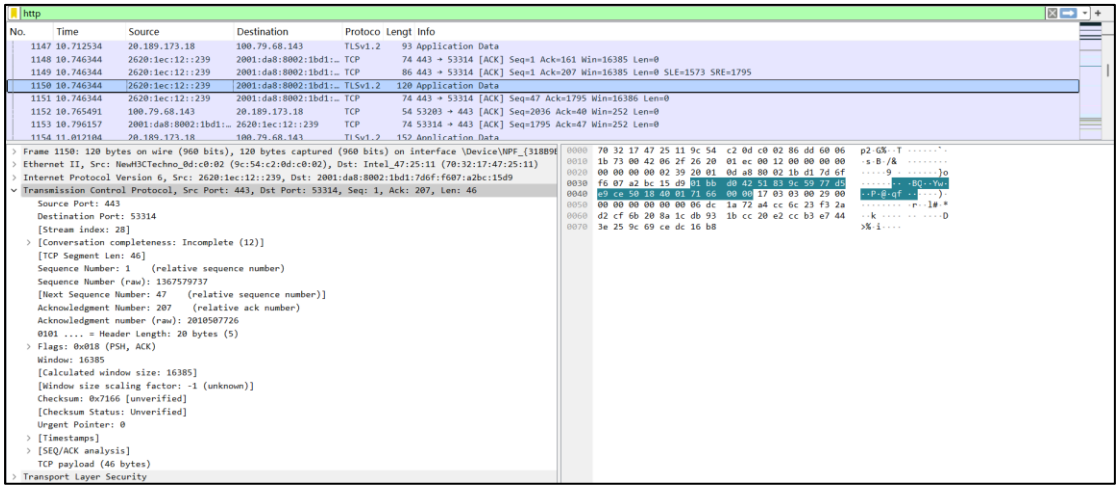
5.2 实验抓包

（1）打开 wireshark

（2）设置过滤器为 http，开始抓包

（3）在浏览器中访问百度，即 https://www.baidu.com/

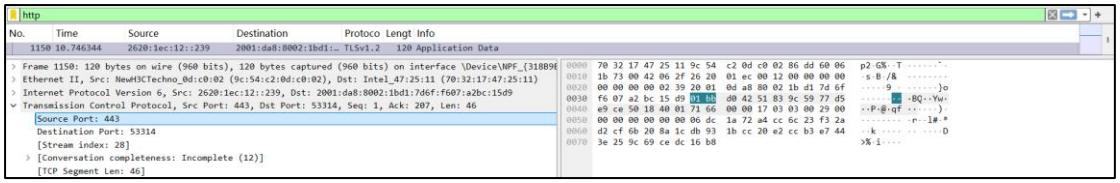
（4）停止抓包，查看抓包结果



5.3 抓包结果分析

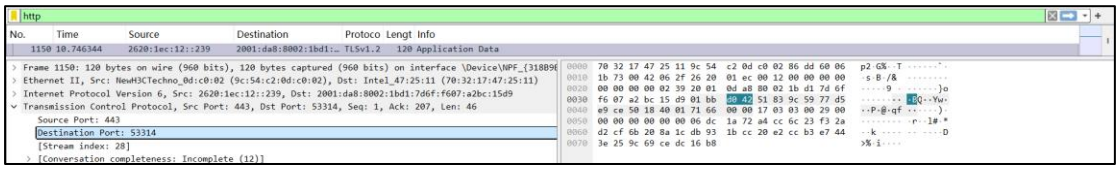
（1）源端口（Source Port，16 bits）：01 bb

此处源端口号为 443.



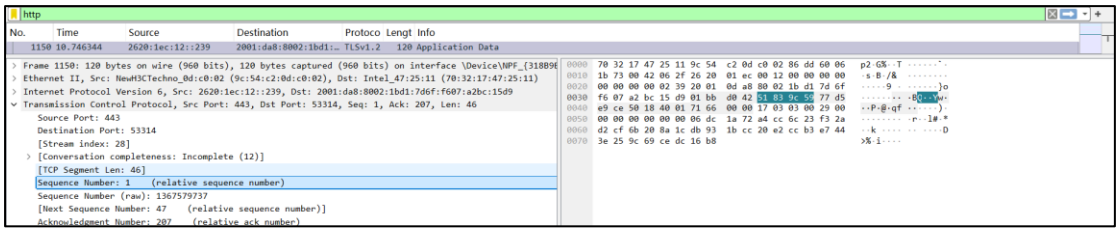
（2）目的端口（Destination Port，16 bits）：d0 42

此处目的端口号为：53314



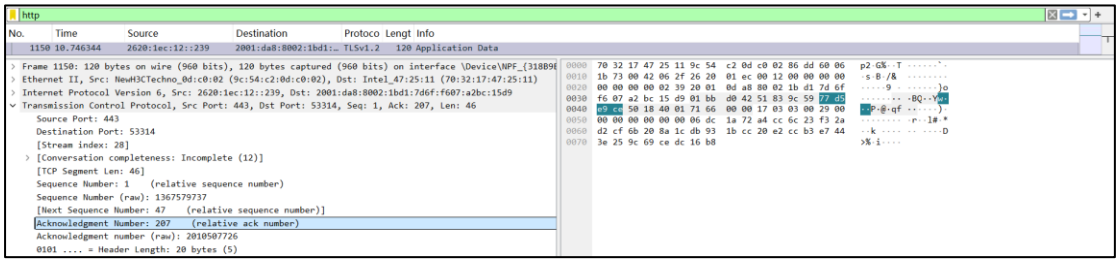
（3）序号（Sequence Number，32bits）：

此处序号为 1（这里是简化处理后的，处理前的序号为 1367579737）



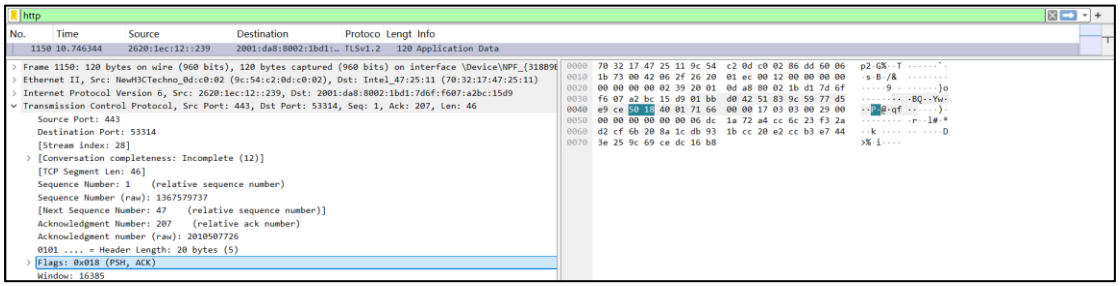
（4）确认号（Acknowledgment Number，32bits）：

此处确认号为 207（这里是简化处理后的，处理前的序号为 2010507726）



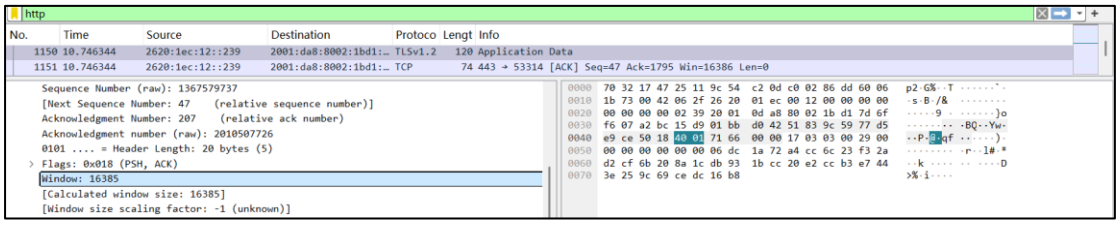
（5）首部长度数据偏移（4bits）+ 保留（6bits） + 标志位（6bits）：50 18

此处首部长度偏移量为 20 B，标志位中只有 Ack 和 Push 置 1，其他均置 0。



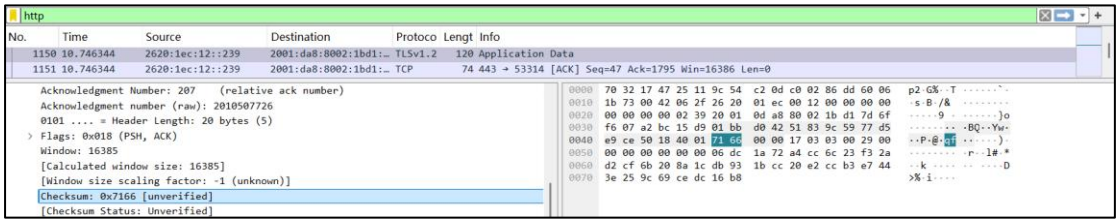
（6）窗口（16bits）：40 01

此处窗口大小为 16385

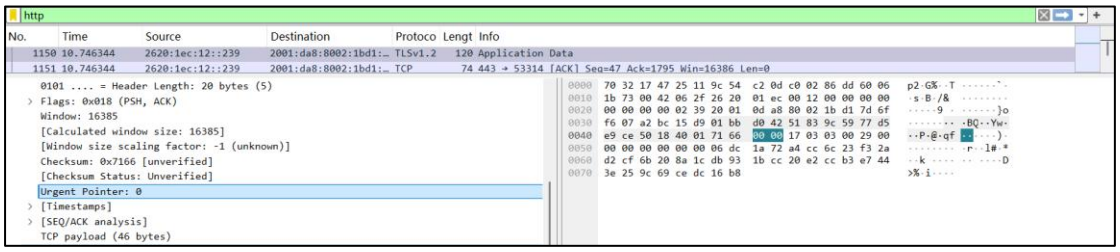


（7）校验和（16bits）：71 66

此处校验和为 0x7166



（8）紧急指针（16bits）：00 00



经分析，与理论分析基本吻合。

六、HTTP 协议

6.1 理论分析

6.1.1 HTTP 协议：

超文本传输协议（Hypertext Transfer Protocol，HTTP）是一个简单的请求-响应协议，它通常运行在 TCP 之上。它指定了客户端可能发送给服务器什么样的消息以及得到什么样的响应。请求和响应消息的头以 ASCII 形式给出；而消息内容则具有一个类似 MIME 的格式。超文本传输协议是一种用于分布式、协作式和超媒体信息系统的应用层协议，是万维网 WWW（World Wide Web）的数据通信的基础。

6.1.2 HTTP 请求报文结构：

（1）请求行：

请求行由请求方法字段、URL 字段和 HTTP 协议版本字段 3 个字段组成，它们用空格分隔。例如：GET http://jsuacm.cn/template/jsu/css/modifypage-1.css HTTP/1.1

（2）请求头

HTTP 的报文头。报文头包含若干个属性，格式为“属性名:属性值”，服务端据此获取客户。

（3）请求体

报文体，它将一个页面表单中的组件值通过 param1=value1&m2=value2 的键值对形式 编码成一个格式化串，它承载多个请求参数的数据。不但报文体可以传递请求参数，请求 URL 也可以通过类似于 /chapter15/user.html?param1=value1&m2=value2 的方式 传递请求参数。

6.1.3 HTTP 响应报文结构：

（1）状态行：

状态行由 3 部分组成，分别为：协议版本、状态码、状态码描述。其中协议版本与请求报文一致，状态码描述是对状态码的简单描述。

（2）响应行：

包括报文协议及版本、状态码及状态描述等。

（3）响应头：响应报文头，由多种属性组成。

（4）响应体：响应报文体。

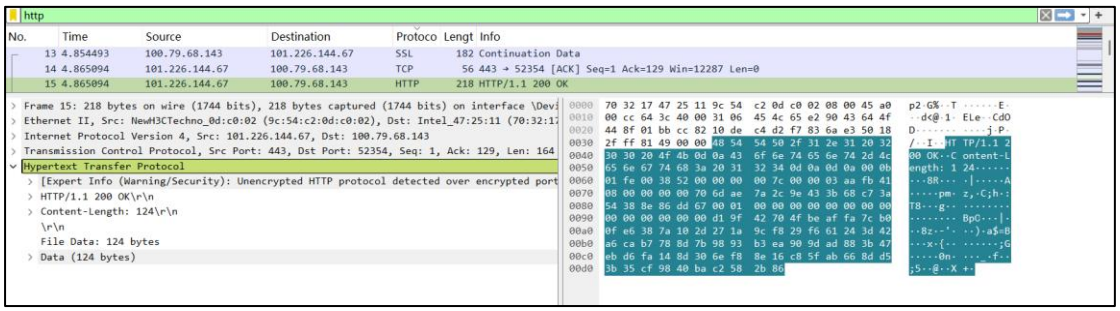
6.2 实验抓包

（1）打开 wireshark

（2）设置过滤器为 http，开始抓包

（3）在浏览器中访问百度，即 https://www.baidu.com/

（4）停止抓包，查看抓包结果

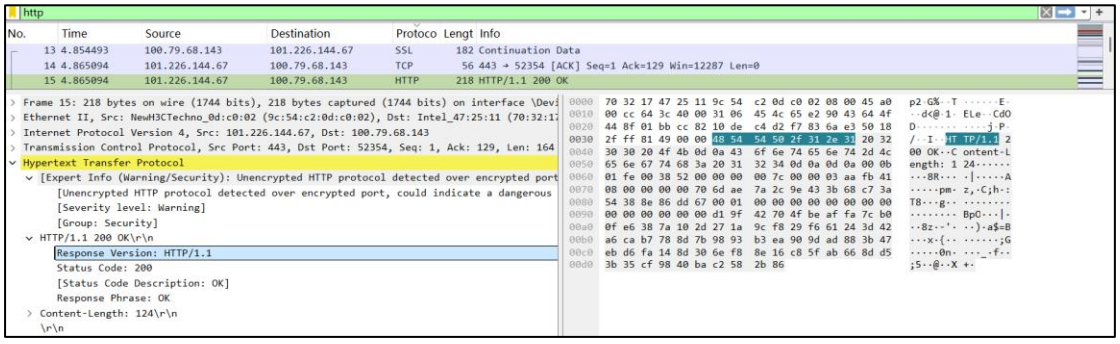


6.3 抓包结果分析

这里以响应报文为例：

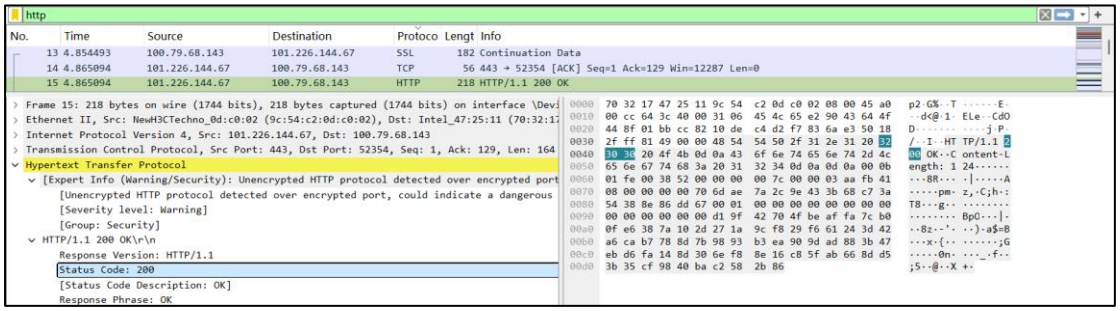
（1）报文协议及版本：

这里报文协议及版本为 HTTP /1.1。



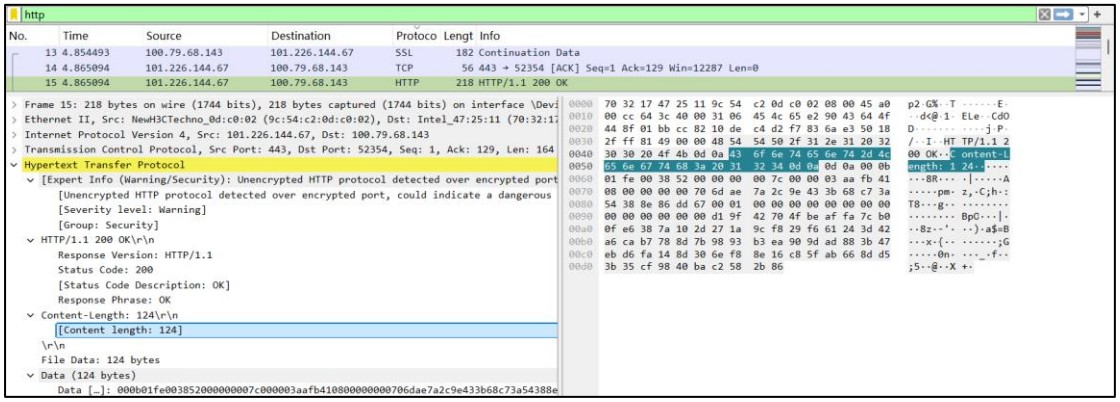
（2）状态码及状态描述：

状态码：200，状态描述：OK。



（3）内容总长：

这里内容总长为 124.



经分析，与理论分析基本吻合。

七、实验总结

通过使用 Wireshark 对各协议抓包分析，我收获满满。从以太网 MAC 帧、无线局域网 MAC 帧，明晰了数据链路层的传输封装方式。IP 协议让我懂得数据包的路由抉择，TCP 协议三次握手与四次挥手的可靠性机制不再抽象。HTTP 协议则将网络与日常上网紧密相连，展现网页请求与响应的细节。这次实验将理论化为实践，提升了我的网络分析技能，让我对网络通信的理解不再停留在书本，也激发了我深入探索网络技术的热情，期待在这一领域不断进步。