计算机网络-实验1：Wireshark

姓名：翟一航 学号：23020011046

一、 实验目的

了解协议和分层在数据包中的表示方式。它们是构建文本中涵盖的网络的关键概念。

Wireshark：本练习使用 Wireshark 软件工具捕获和检查数据包跟踪。数据包跟踪是网络上某个位置的流量记录，就好像对通过特定线路的所有位进行快照一样。数据包跟踪记录每个数据包的时间戳，以及构成数据包的位，从较低层标头到较高层内容。

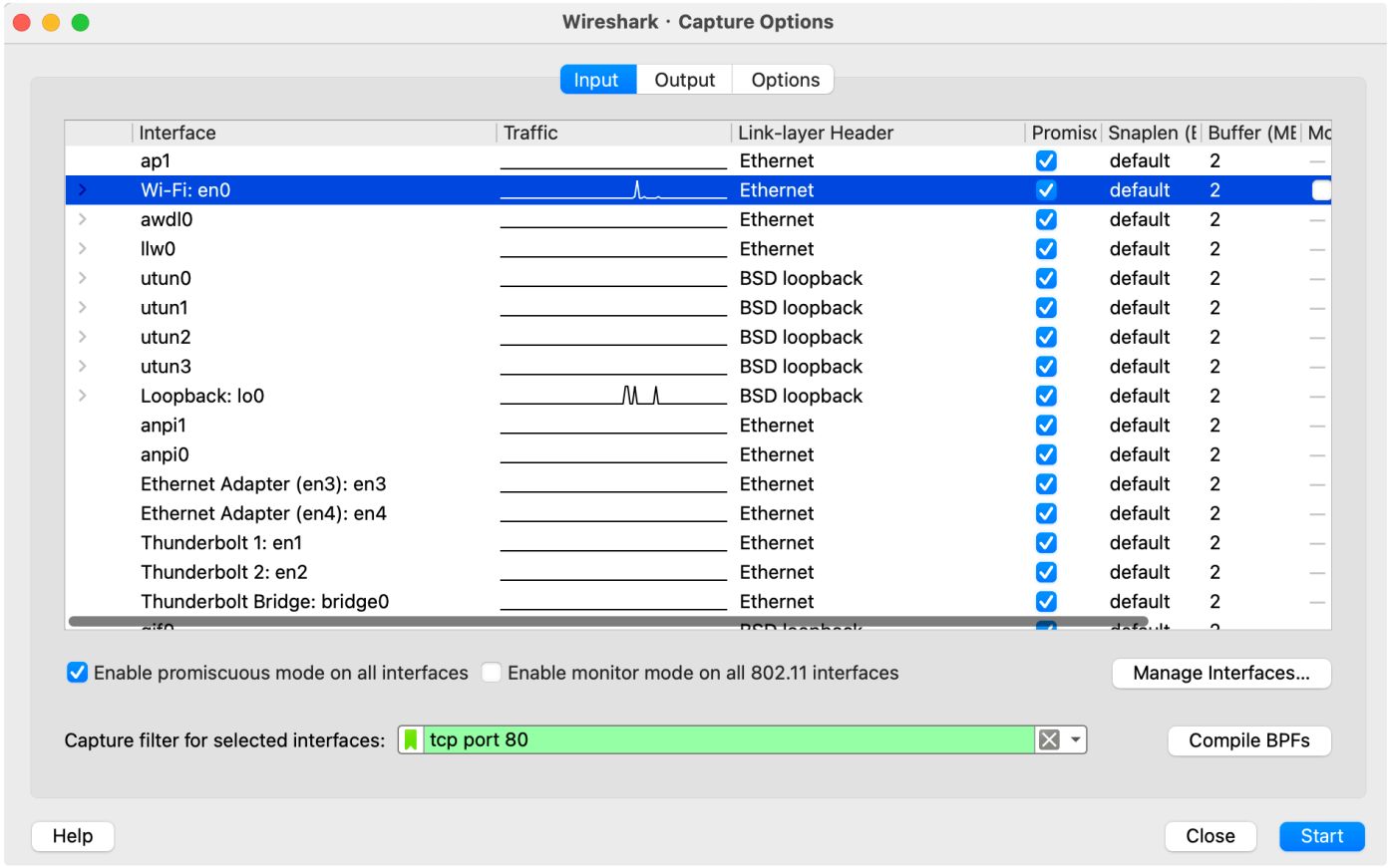
二、 实验环境

环境	说明
操作系统	MacOS
抓包工具	Wireshark
网络接口	Wi-Fi:en0

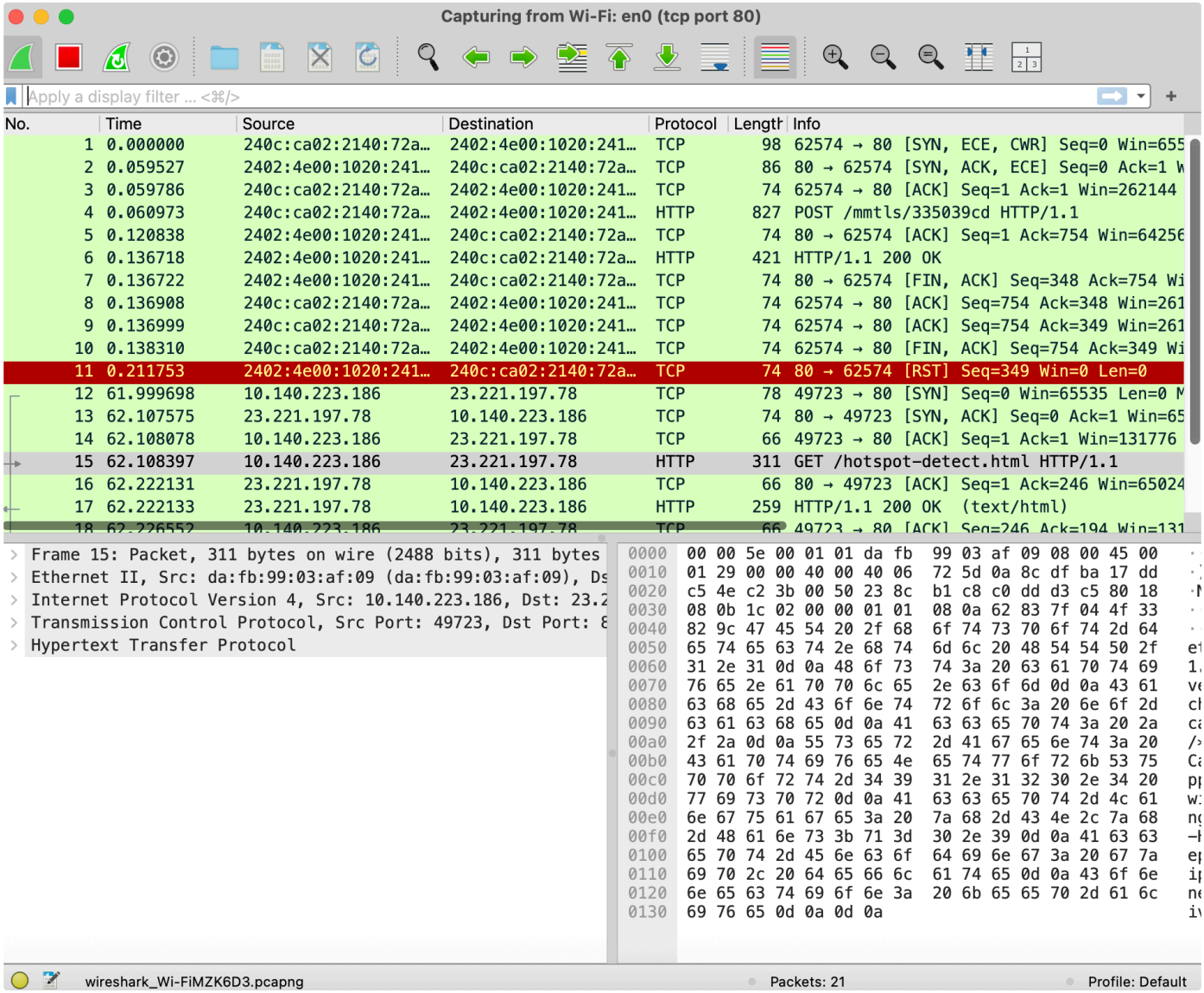
三、 实验内容

Step1:Capture Traces

首先，在 zsh 终端中通过 homebrew 工具下载 Wireshark 并启动软件，进入设置界面选择 Wi-Fi:en0 接口，并使用 filter——tcp port 80，开始运行。

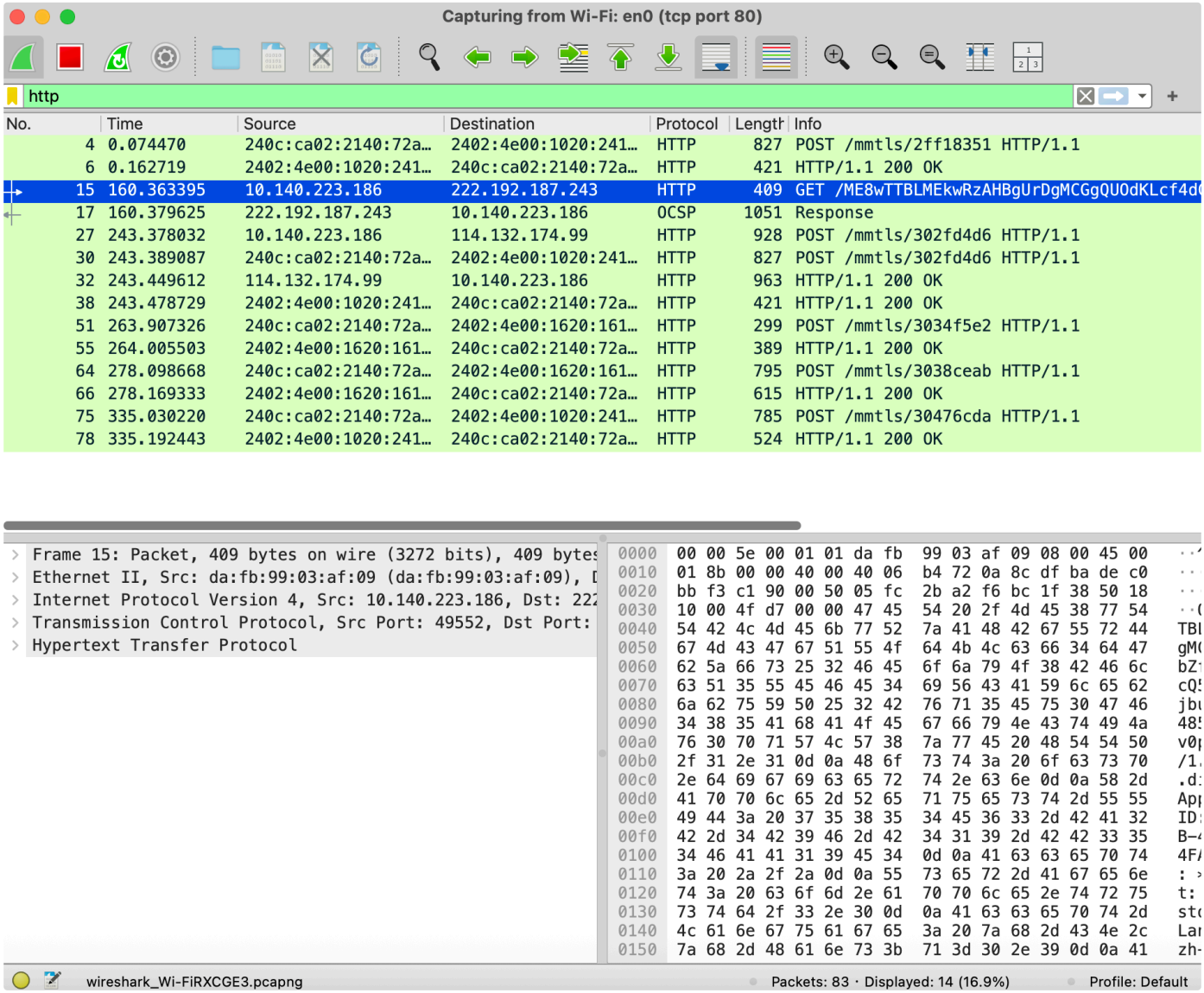


接着，打开一个使用 `https` 进行加密的网址进行测试（此处测试中国海洋大学学术期刊网），结果如下：



Step2:Inspect the Trace

点击一个“协议”为http，而“信息为”GET的数据包，查看其具体信息：



发现数据包标头详细信息窗口显示了该网络数据包对应 TCP/IP 协议的五层协议栈，它们从底层到高层依次为：

Wireshark block	对应网络协议层	包含信息/作用
Frame	非协议层	Wireshark的捕获元数据，包含整个数据帧的信息
Ethernet II	网络接口层	定义如何在本地网络传输信息
IPv4	网络层	将数据包在网络间路由
TCP	传输层	提供可靠数据传输
HTTP	应用层	为用户提供网络服务

Step3:Packet Structure

单击对应数据包中不同层的数据块可以查看其大小，绘制出 HTTP GET 数据包的结构图如下：

Ethernet II Header	14 bytes
IPv4 Header	20 bytes
TCP Header	32 bytes
HTTP Data	245 bytes

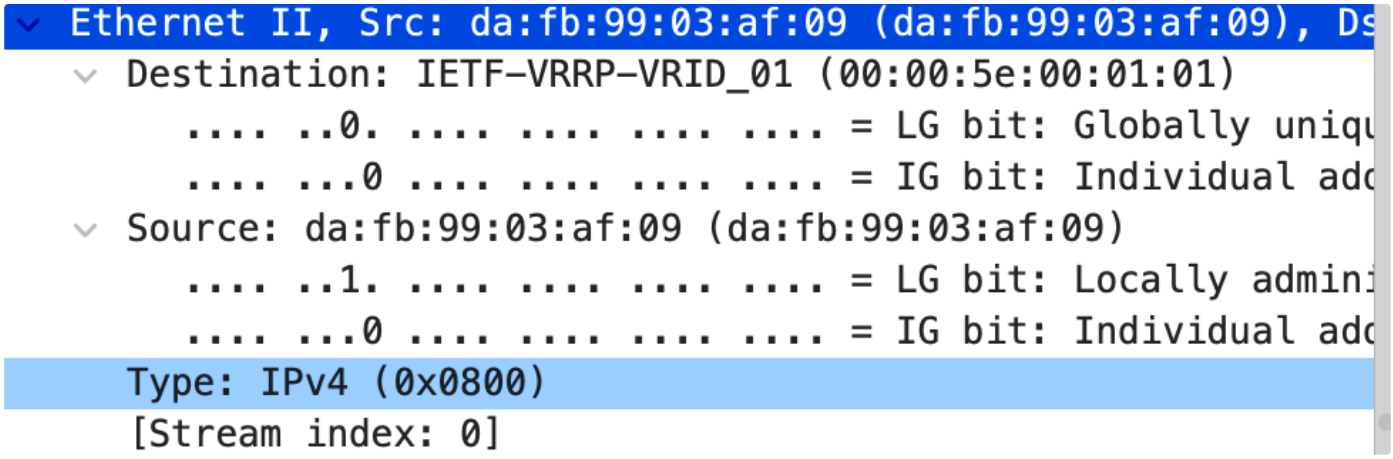
可以发现 HTTP 层对应的数据明显大于其余层的头部，这是因为显示的是 HTTP 的信息—主要显示头部，但是如果存在且可识别，那么也会显示正文，而其余各层均只显示头部信息。

Step4:Demultiplexing Keys

> Q1:哪个以太网标头字段是解复用密钥，告诉它下一个更高层是 IP？此字段中使用什么值来表示IP？

答：

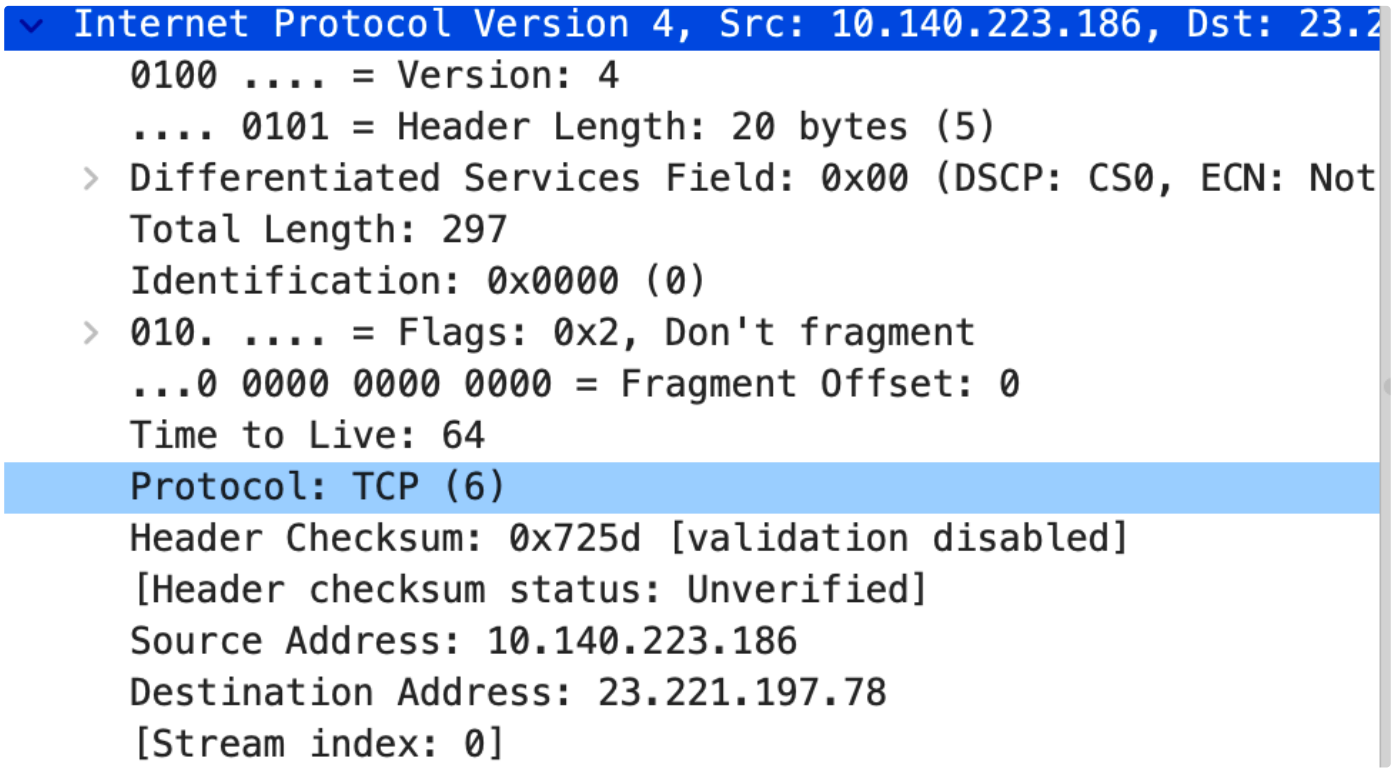
在 Ethernet II 帧格式中，**Type** 字段是解复用密钥，这个字段使用 0x0800 来指示 IP。



> Q2:哪个 IP 标头字段是告诉它下一个更高层是 TCP 的解复用密钥？此字段中使用什么值来表示TCP？

答：

在 IP 标头中， Protocol 字段是解复用密钥，这个字段使用 6 来表示 TCP。



四、 总结建议

通过此次实验，我对计算机网络协议的分层和数据包的结构有了更深刻的理解。在实验中，通过使用 Wireshark 抓取并分析 HTTP 数据包，了解了 TCP/IP 协议各层的功能和解复用机制。

通过实验使用过滤器 `tcp port 80` ，我了解到 80 是 HTTP 协议的标准端口（HTTPS 协议的标准端口是 443），也学习到过滤器的作用—可以过滤掉大量的其他网络流量，专注分析目标协议，排除干扰。

此外，通过查阅资料，我弄清楚了 Frame 与 Ethernet II 的实际关系。二者并非同一层，Frame 本质是 Wireshark 的元数据记录，它是包含以太网络层的容器，只在 Wireshark 中存在，而 Ethernet II 却是真正的数据链路层协议，实际在网络线路上传输。