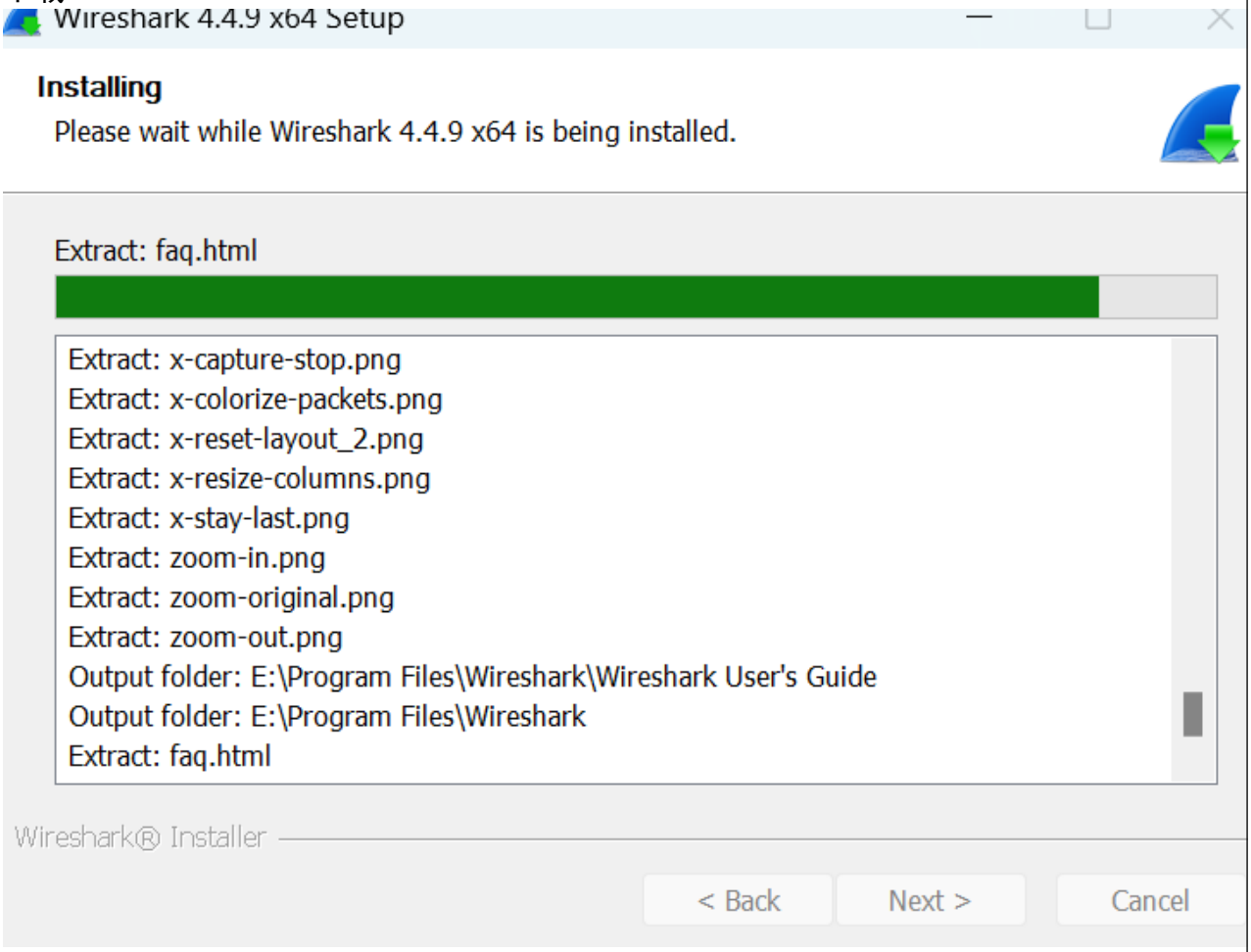
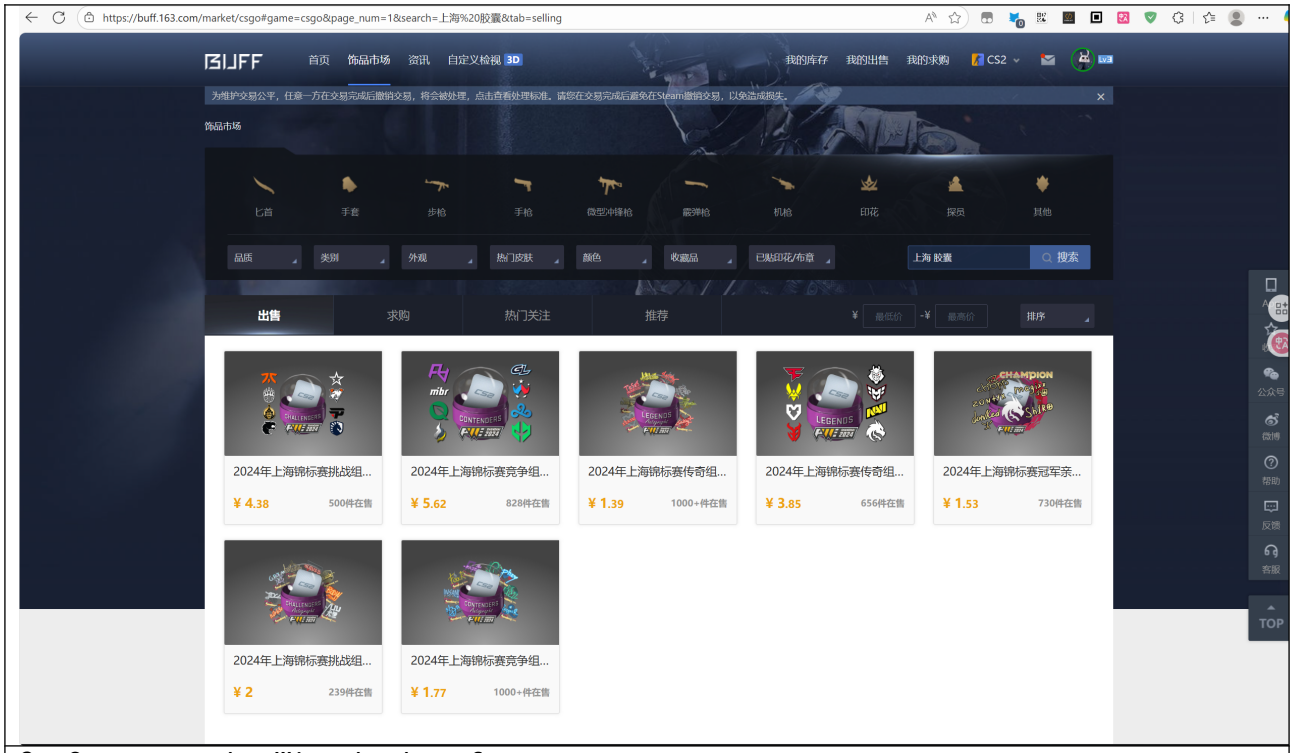
山东大学_____计算机_____学院
____计算机网络_____课程实验报告

学号：202400130039	姓名： 张汇智	班级： 智能
实验题目： Wireshark Intro		
实验学时：2h	实验日期： 2025.9.9	
实验目的：		
硬件环境： AMD ryzen R9 7900HX ; NVIDIA RTX4070LAPTOP ; RAM SAMSUNG 16GB*2 ; ROM WD770 1T+2T;		
软件环境：Windows11 23H2 （KB5056580）		
实验步骤与内容： 下载wireshark		

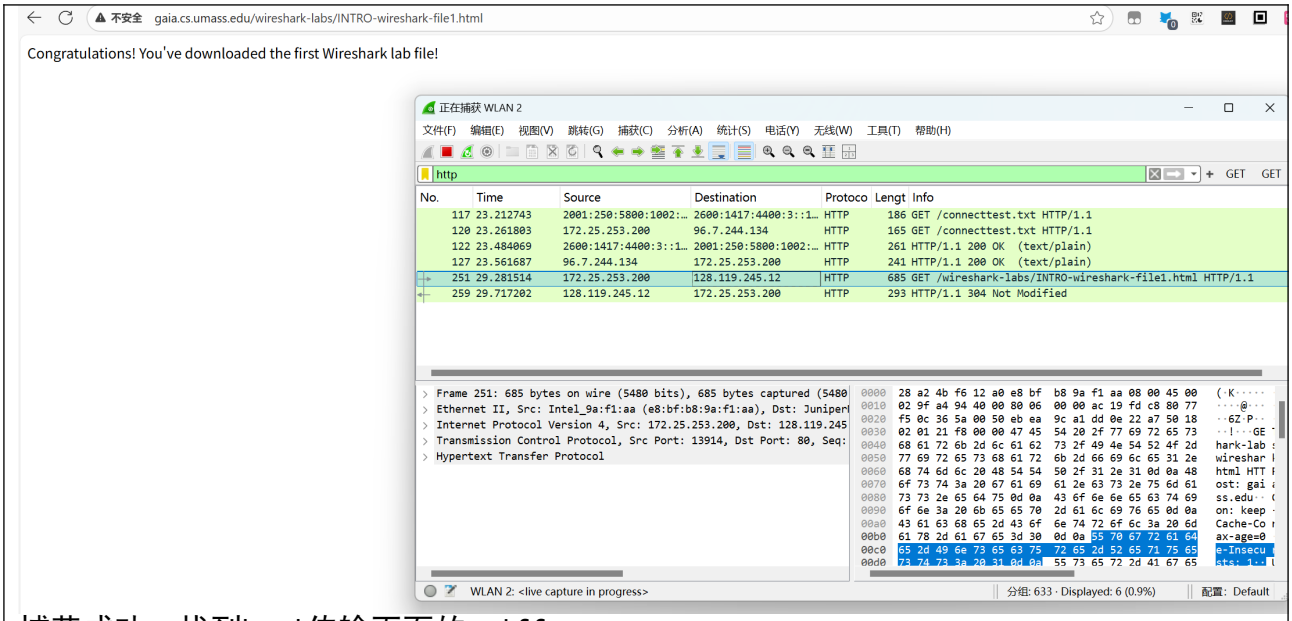


1. Start up your favorite web browser, which will display your selected homepage



2. Start up the Wireshark software.

捕获WLAN2，注意关闭代理。



捕获成功，找到html传输页面的sniff

结论分析与体会：

学会了wireshark工具最基本的操作。

本次实验非常简单，简单到chatGPT都是累赘，pdf往里进。

结论

- 成功捕获：往返耗时 ≈ 29 ms；服务器 IP：***128.119.245.12***；本机 ***IP***：***172.25.253.200***
- ***GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1***。
- 观察到协议：Ethernet / IP / TCP / HTTP（另含 DNS 等）。
- 抓包接口：***WLAN 2***；

分析

- 流程：DNS 解析 → TCP 三次握手 → HTTP 请求 → HTTP 响应。
- 时延组成：握手 RTT + 服务器处理 + 下行传输。
- 关键字段：SYN/ACK、MSS、Window Scale、SACK、HTTP Host、Content-Length。
- 若被自动升级到 HTTPS，则应用层不可见；需改用明文 URL 或做 TLS 解密。
- 显示过滤器更安全：http、ip.addr==目标IP and http；避免在开始前用 capture filter 丢样本。
- 设定 Time Reference 获取 GET → 200 OK 精确差值；显示为相对时间更直观。

问题与排障

- 误抓到系统探测（如 connecttest.txt）；根因：未实际访问实验 URL 或被升级到 HTTPS。
  注：在edge浏览pdf时右键新标签页打开时会被自动升级成HTTPS，也是造成了一开始找不到http原因；；
- 代理/Clash 使流量进隧道；直连或同时抓代理与物理网卡。
  注：是一开始抓不到的另一个原因
- 接口选择错误无流量；以“流量列跳动”为准。
  注：一开始抓不到后选择了别的接口发现就是WLAN2，因为在实验室是无线网；；

体会

- 分层可视化让协议课本内容落地。
- 工具正确性>技巧：接口、过滤器、时间基准、代理设置决定能否复现。
- 数据优先：先“抓到”，再“筛到”，再“读懂”，最后“复现”。