计算机网络与应用

实验一 利用 Wireshark 分析网络协议

学 院： 吴健雄学院

专 业： 人工智能

学 号： 61523233

姓 名： 黄笃修

一、实验目的

1. 加强对计算机网络通信协议的理解，用理论知识解决实际问题。

2. 学习 Wireshark 的基本操作，抓取和分析有线局域网的数据包，熟悉一些应用层命令和协议。

3. 通过运用 Wireshark 对网络活动进行分析，观察 TCP 协议报文，分析通信时序，理解 TCP 的工作过程，掌握 TCP 工作原理与实现；学会运用 Wireshark 分析 TCP 连接管理、流量控制和拥塞控制的过程，发现 TCP 的性能问题。

二、实验任务

（一）应用层协议分析

1. 利用 Wireshark 抓包软件，抓取网络数据包；
2. 学习基本操作：捕获过滤器和显示过滤器；
3. 分析 HTTP 和 DNS 协议。

（二）传输层协议分析

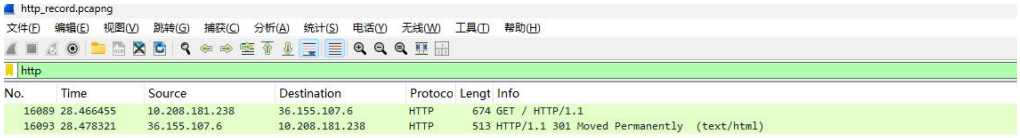
1. TCP 数据流的追踪；
2. TCP 连接的建立；
3. TCP 连接的终止；
4. TCP 连接的重置。

三、实验内容（含解析）

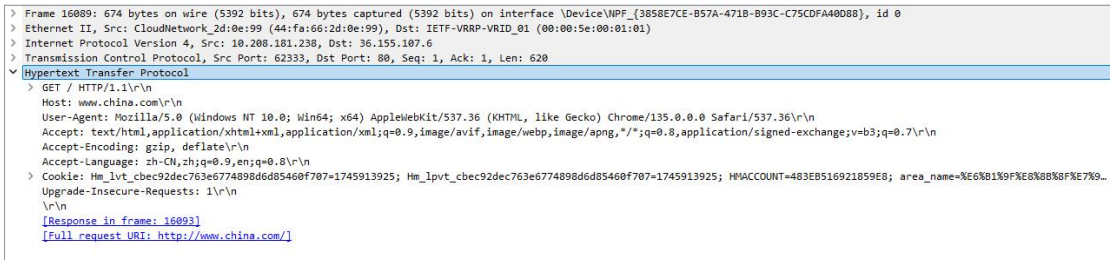
（依次描述每个任务的完成过程：包括执行命令语句、过程截图等）

（一）应用层协议分析

捕获数据包之后使用过滤器留下 http 协议的数据包：

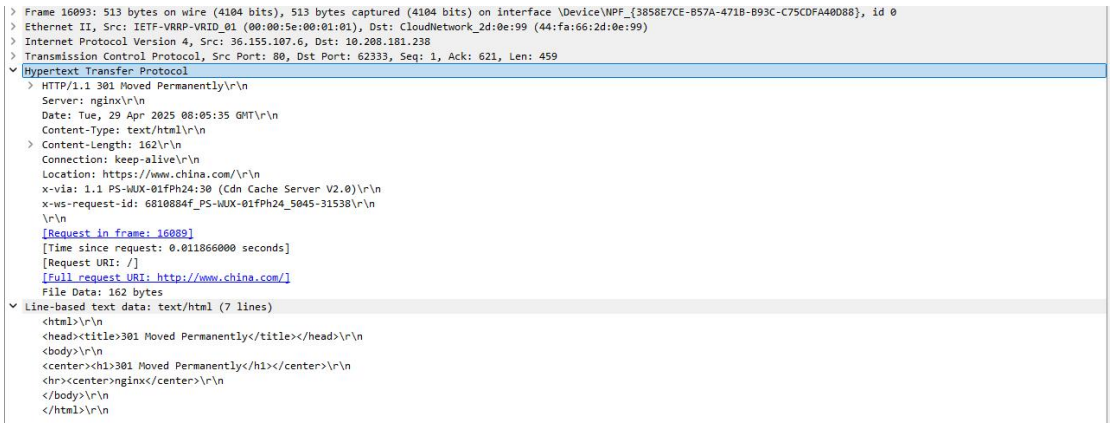


第一个 HTTP 请求数据包分析：



协议为 HTTP/1.1，源 IP 为 10.208.181.238，目标 IP 为 36.155.107.6，源端口为 62333，目标端口为 80。请求方法是 GET，表示客户端希望从服务器获取指定的资源。User-Agent 标明了客户端的操作系统和浏览器版本，此处为请求来源于一个运行 Windows10/11 的 Chrome 浏览器。Accept 标明了客户端希望接收的内容类型，此处为 HTML、XHTML、图片等格式。Accept-Encoding 表明了客户端支持的压缩格式。Accept-Language 表明了客户端的偏好语言，此处为中文。Upgrade-Insecure-Requests:1 表示浏览器希望通过升级 HTTP 为 HTTPS。

第二个 HTTP 响应数据包分析：

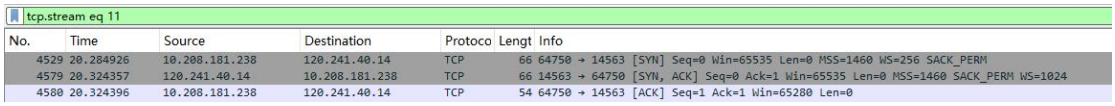


协议为 HTTP/1.1，源 IP 为 36.155.107.6，目标 IP 为 10.208.181.238，源端口为 80，目标端口为 62333。响应信息为 HTTP 301 Moved Permanently，即请求

的资源已经永久性地移动到新的位置。状态码：301 表示请求的资源已经被永久移动到新的位置，客户端应根据响应头中的 Location 字段重定向到新的 URL。Date 为服务器发送响应的时间。Content-Type 表示响应内容的格式，此处为 HTML 文本格式。Content-Length 是响应体的长度。Connection：keep-alive 表示服务器希望保持与客户端的连接。Location：https://www.china.com/ 是新的资源位置，客户端应根据该 URL 进行重定向。X-Via：1. PS-HUX-DCD，表示响应经过了某个代理服务器的处理。Line-based text data 是返回的 html 文件，此处内容就是 301。

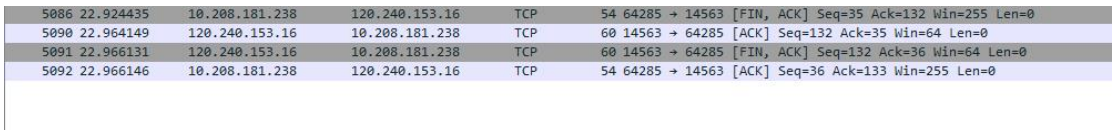
（二）传输层协议分析

使用 tcp.flags.syn == 1 && tcp.flags.ack == 1 过滤表达式过滤出 TCP 数据包后，右击追踪流追踪改会话的所有数据包，观察前三个包的建立连接的握手过程：



数据包 1 为发起连接请求的 TCP SYN 数据包，源 IP 为 10.208.181.238，目标 IP 为 120.241.40.14。数据包 2 为对连接请求的响应，SYN+ACK，表示目标 IP 120.241.40.14 已经收到并同意连接。数据包 3 为连接确认，ACK，表示源 IP 10.208.181.238 确认收到了对方的连接请求。这三个数据包展示了典型的 TCP 三次握手过程：第一次 SYN 请求、第二次 SYN-ACK 响应、第三次 ACK 确认建立连接。

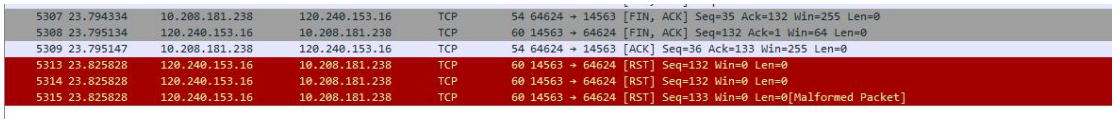
使用 tcp.flags.fin == 1 过滤表达式过滤出 TCP 数据包后，右击追踪流追踪改会话的所有数据包，观察最后四个包的终止连接的挥手过程：



数据包 1 为源 IP 10.208.181.238 向目标 IP 120.240.153.16 发送了一个 FIN 请求，表示关闭连接。数据包 2 为目标 IP 120.240.153.16 向源 IP 10.208.181.238 发送了 FIN + ACK 响应，确认关闭连接。数据包 3 为目标 IP 120.240.153.16 发送了

一个 ACK 确认包，确认接收了源 IP 10.208.181.238 的关闭请求。数据包 4 为源 IP 10.208.181.238 发送了一个 ACK 确认包，表示已经接收到目标 IP 的关闭响应。这四个数据包展示了 TCP 连接的四次挥手过程：首先发起关闭请求，然后确认对方的关闭请求，并最终完成连接的关闭。

使用 tcp.flags.reset == 1 过滤表达式过滤出 TCP 数据包后，右击追踪流追踪改会话的所有数据包，观察连接的重置：



最后一个 RST 数据包被标记为“格式错误”，这可能意味着该数据包在传输过程中损坏，或者存在协议错误。这几个数据包显示了连接的异常终止和重置过程，尤其是 RST 标记的数据包，通常用于强制中断连接或在发生错误时关闭连接。

四、实验总结

通过这次实验，我学会了抓包软件的使用方法，同时更详细了了解了 HTTP，TCP 协议的内容与过程，通过抓包的方式实际观察到了网络层、传输层协议的运作过程。