**实验一：互联网协议实验**

1. 实验内容

1、在节点h1上开启wireshark抓包，用wget下载www.ucas.ac.cn页面

2、调研说明wireshark抓到的几种协议：ARP, DNS, TCP, HTTP, HTTPS

3、调研解释h1下载ucas页面的整个过程，包括几种协议的运行机制

1. 在节点h1上开启wireshark抓包，用wget下载www.ucas.ac.cn页面

抓包结果和下载结果如下

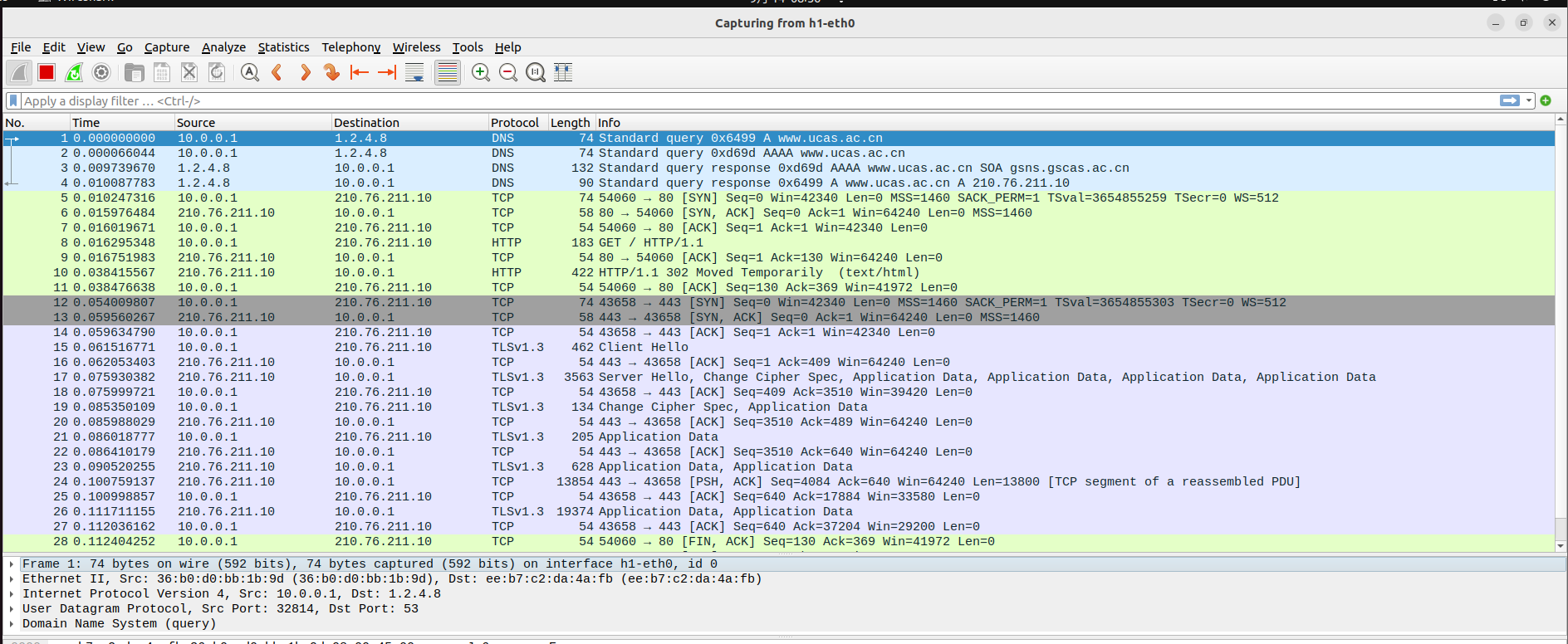


图1：抓包结果1

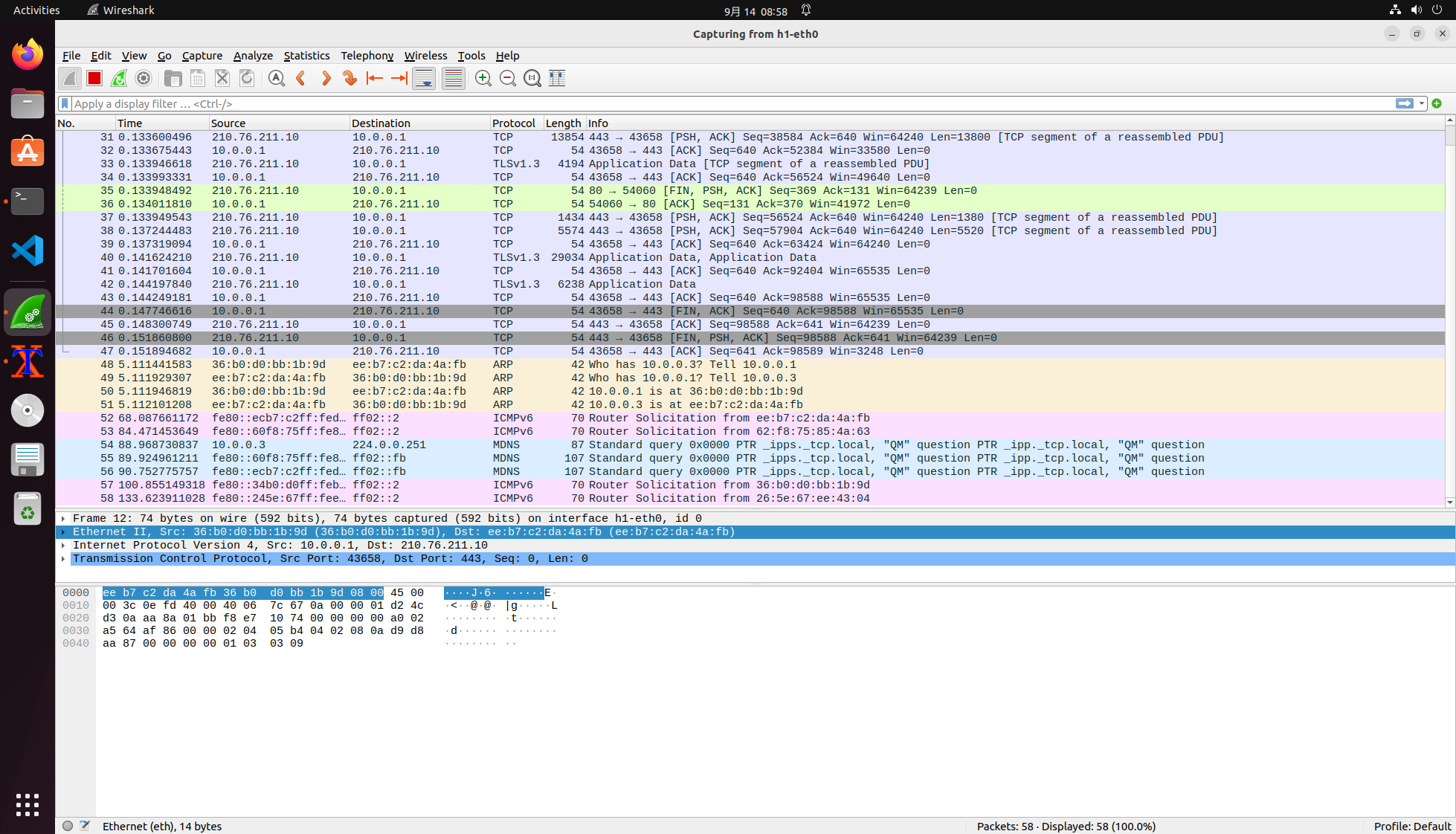


图2：抓包结果2

在h1下载ucas页面的整个过程出现了四种协议：DNS、TCP、HTTP、ARP

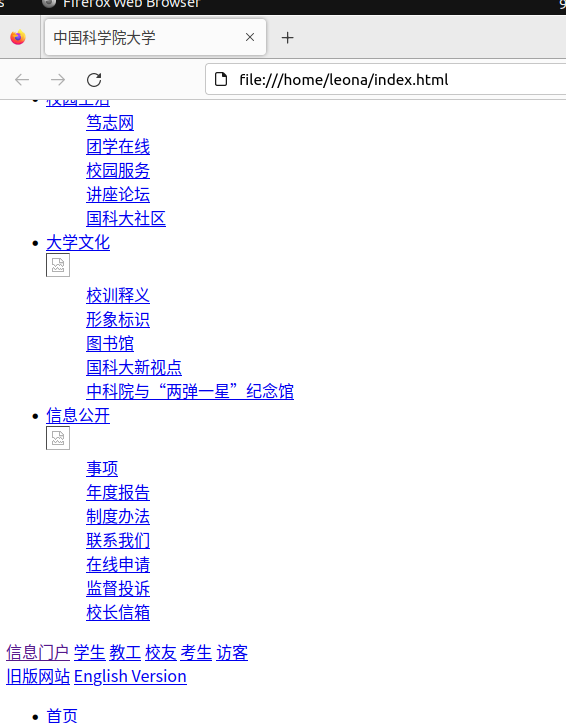
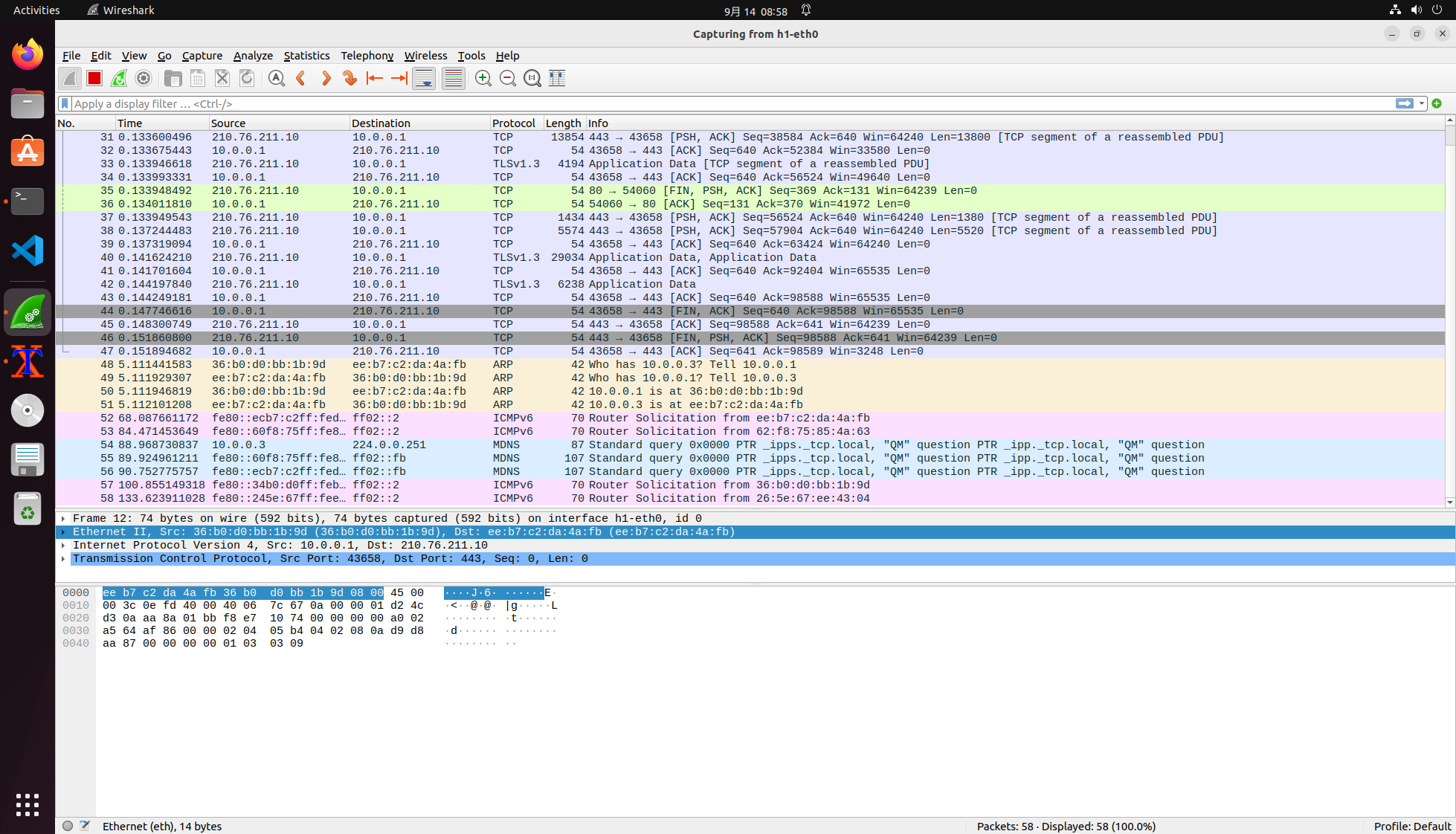


图3：下载网页截图

1. Wireshark抓包的几种协议
2. ARP（地址解析协议）

ARP是用于解析网络层（通常是IPv4）地址和链路层（MAC）地址之间映射关系的协议。主机发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址。收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存就可以节约资源。



26:b0:d0:bb:1b:9d对应本地IP为10.0.0.1的MAC地址。ee:b7:c2:da:4a:fb对应本地IP为10.0.0.3的MAC地址。

1. DNS（域名系统）

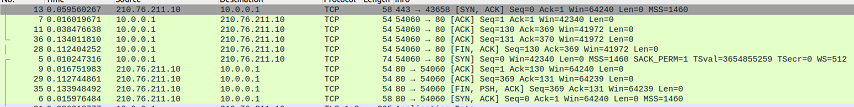
DNS是用于将易记的域名（例如www.example.com）映射到IP地址（例如292.268.2.2）的分布式数据库系统。



上图首先由本地IP10.0.0.1作为source，向目标地址1.2.4.8即DNS服务器发送查询请求。1.2.4.8返回本地IP解析结果，根据上图可以看出为210.76.211.10。

3、TCP（传输控制协议）

TCP是一种面向连接的、可靠的协议，用于在网络上传输数据。它确保数据的有序传输和可靠交付，通过使用三次握手来建立连接，并使用滑动窗口和确认机制来管理数据流。TCP也处理数据分段、错误检测和恢复以及流量控制。它用于大多数应用程序的可靠通信，如网页浏览、文件下载和电子邮件。



图中在进行握手连接，服务端向客户端发送SYN，客户端向服务端发送ACK，FIN表示关闭连接，PSH代表存在数据传输。

1. HTTP（超文本传输协议）

HTTP是一种应用层协议，用于在Web上传输超文本文档，如网页。HTTP是无状态的，每个请求和响应之间是独立的，它使用不同的HTTP方法来执行不同的操作。HTTP主要在Web浏览器上运行，当用户进入网站域并打算访问它时，HTTP提供访问权限。



出现GET请求。

5、HTTPS

HTTPS是HTTP的安全版本，它代表HTTP Secure，它使用TLS/SSL协议来加密数据传输。这种加密确保数据在客户端和服务器之间的传输是安全的，无法被窃取或篡改。HTTPS使用公钥加密和证书验证来确保通信的安全性。它在安全性方面比HTTP更可靠，因此在处理敏感信息（如信用卡号、登录凭据等）的网站上广泛使用。

6、DNS和HTTP在应用层，IP在网络层，TCP在传输层，ARP在数据链路层。这也就有了不同层次的协议封装，即Ethernet<IP<TCP<HTTP。如下图可见。



1. 下载ucas页面的过程

修改h1主机的DNS设置，将DNS服务器设置为1.2.4.8。首先由DNS发送查询请求，解析IP地址为210.76.211.10，而后TCP进行握手连接，服务端第一次发送SYN，第二次发送SYN+ACK，第三次发送ACK，h1主机接收到ucas网站的响应，则连接已经建立。握手成功后显示PSH代表存在数据传输。

**实验二：流完成时间实验**

1. 复现图像
2. 原始数据

表2：不同带宽文件大小下流完成时间

|  |  |  |  |
| --- | --- | --- | --- |
|  | 2MB | 20MB | 200MB |
| 20Mbps | 2．5 | 9.4 | 88 |
| 50Mbps | 2.3 | 3.94 | 23.4 |
| 200Mbps | 2.27 | 3.58 | 24.4 |
| 500Mbps | 2.2 | 3.2 | 5.5 |

图中数据已经过五次平均

1. 处理后的数据

表2：处理后的数据

|  |  |  |  |
| --- | --- | --- | --- |
|  | 2MB | 20MB | 200MB |
| 2 | 2 | 2 | 2 |
| 5 | 2.253846 | 2.385787 | 3.76068 |
| 20 | 2.2822 | 2.625698 | 6.22222 |
| 50 | 2.25 | 2.9375 | 26 |

其中x轴处理公式为后续的带宽大小处于实验最小带宽，y轴处理公式为同一文件大小下，最慢时间除以当前时间。

1. 图像

横纵坐标均为log坐标

1. 解释图像

首先这些文件的下载涉及到TCP传输。TCP传输通过将数据拆分成称为数据包的小块来工作，然后在发送端和接收端之间交换这些数据包。首先，在两台计算机之间建立TCP连接需要进行三次握手过程，以确保双方都准备好进行通信。同时，TCP具有拥塞控制机制，用于监测网络拥塞并相应地调整传输速率，以确保网络的稳定性和效率。

而慢启动机制是拥塞控制的一部分，它是在开始传输数据时以较低的速率开始，然后逐渐增加传输速率，直到达到网络的最大容量。在连接刚建立时，慢启动会将初始拥塞窗口设置为一个较小的值，通常为1到10个数据包大小。每当发送方接收到确认的数据包而不出现超时，拥塞窗口大小指数增长，从而导致发送速率的增加。如果出现超时或拥塞，发送方会将拥塞窗口减小，并重新开始慢启动。然后，它会以线性增长的方式逐渐增加拥塞窗口的大小。

该图像的数据均经过处理。可以看出，在文件大小为1MB时，平均下载速率并未随着带宽增加而有显著提升，而文件大小为100MB时，平均下载速率随带宽显著提升。因此，文件越大，下载时间随带宽增大越有明显减少，平均下载速率越明显增大。结合TCP传输工作原理，可以猜到，由于文件大小较小，拥塞窗口的作用不大，考虑到握手时间等因素，传输受其他因素影响较大。

而三条不同文件大小的曲线随着文件大小变大逐渐逼近y=x曲线。这是由于随着文件大小增加，其他因素的影响减少，拥塞窗口大小成指数增长，发送速率在建立连接后迅速增加，带宽成为主要限制因素。较大文件的下载速率更接近实际带宽的能力，此时下载速率与文件大小之间的关系趋于线性。

三、部分实验测试截图

