互联网协议实验

学号： 2021K8009929010

姓名： 贾城昊

一、 实验题目：互联网协议实验

二、 实验任务

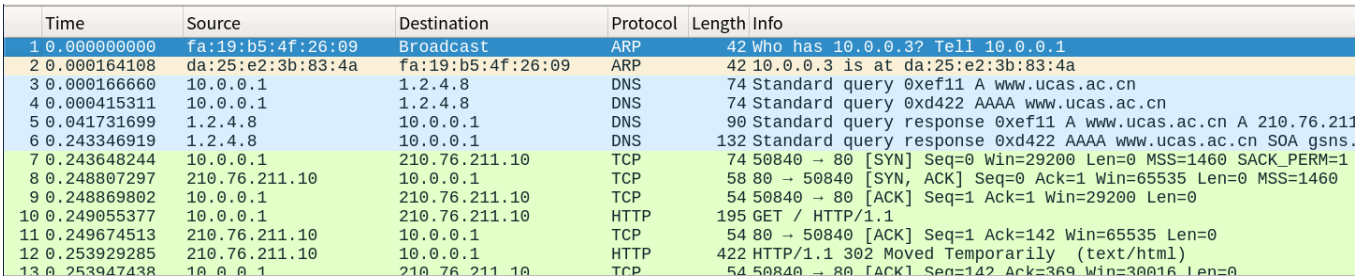
1. 在节点 h1 上开启 wireshark 抓包，用 wget 下载 www.ucas.ac.cn 页面。
2. 调研说明 wireshark 抓到的几种协议 ： ARP, DNS, TCP, HTTP。
3. 调研解释 h1 下载 www.ucas.ac.cn 页面的整个过程，即几种协议的运行机制

三、 实验流程

1. 在终端中执行 sudo mn --nat，将 host 连接至 Internet，启动 mininet
2. 在 mininet 中输入 xterm h1，打开控制 h1 的终端
3. 在 h1 终端中输入 echo "nameserver 1.2.4.8" > /etc/resolv.conf
4. 在 h1 终端中输入 wireshark &
5. 在 wireshark 中选择 h1-eth0
6. 在 h1 终端中输入 wget www.ucas.ac.cn 下载 UCAS 页面
7. 观察 wireshark 输出，调研分析获得的几种互联网协议

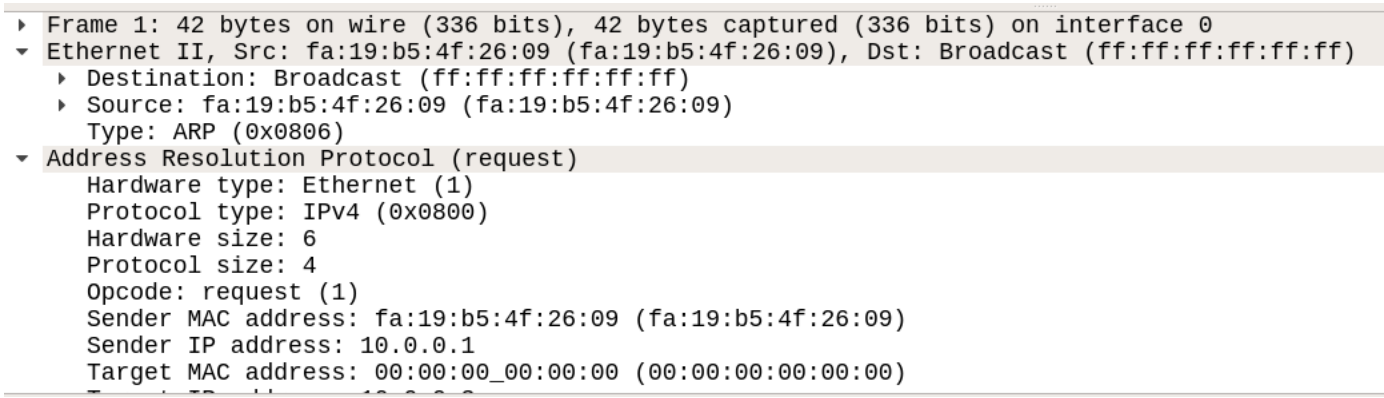
四、 实验结果与分析

（一）wireshark 抓包结果



	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fa:19:b5:4f:26:09	Broadcast	ARP	42	Who has 10.0.0.3? Tell 10.0.0.1
2	0.000164108	da:25:e2:3b:83:4a	fa:19:b5:4f:26:09	ARP	42	10.0.0.3 is at da:25:e2:3b:83:4a
3	0.000166660	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xef11 A www.ucas.ac.cn
4	0.000415311	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xd422 AAAA www.ucas.ac.cn
5	0.041731699	1.2.4.8	10.0.0.1	DNS	90	Standard query response 0xef11 A www.ucas.ac.cn A 210.76.211
6	0.243346919	1.2.4.8	10.0.0.1	DNS	132	Standard query response 0xd422 AAAA www.ucas.ac.cn SOA gsns.
7	0.243648244	10.0.0.1	210.76.211.10	TCP	74	50840 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
8	0.248807297	210.76.211.10	10.0.0.1	TCP	58	80 → 50840 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
9	0.248869802	10.0.0.1	210.76.211.10	TCP	54	50840 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
10	0.249055377	10.0.0.1	210.76.211.10	HTTP	195	GET / HTTP/1.1
11	0.249674513	210.76.211.10	10.0.0.1	TCP	54	80 → 50840 [ACK] Seq=1 Ack=142 Win=65535 Len=0
12	0.253929285	210.76.211.10	10.0.0.1	HTTP	422	HTTP/1.1 302 Moved Temporarily (text/html)
13	0.253947438	10.0.0.1	210.76.211.10	TCP	54	50840 → 80 [ACK] Seq=142 Ack=369 Win=30016 Len=0

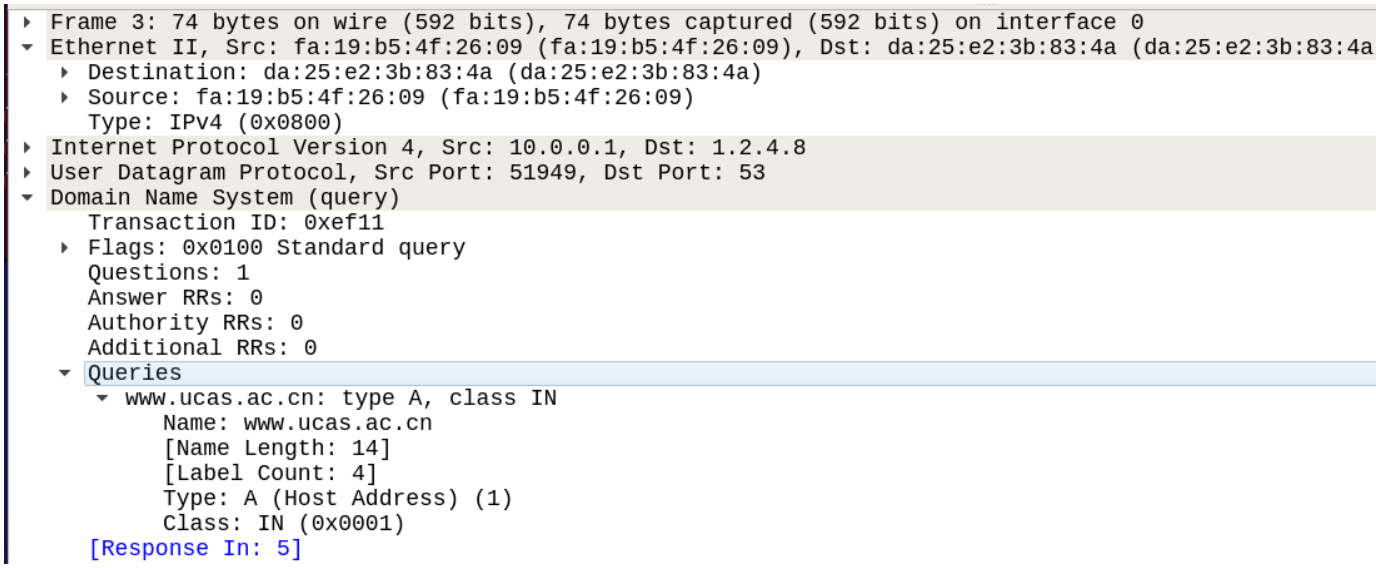
（二）ARP 协议层次



```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▾ Ethernet II, Src: fa:19:b5:4f:26:09 (fa:19:b5:4f:26:09), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: fa:19:b5:4f:26:09 (fa:19:b5:4f:26:09)
    Type: ARP (0x0806)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: fa:19:b5:4f:26:09 (fa:19:b5:4f:26:09)
    Sender IP address: 10.0.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
```

分析结果得层次为： Ethernet < ARP

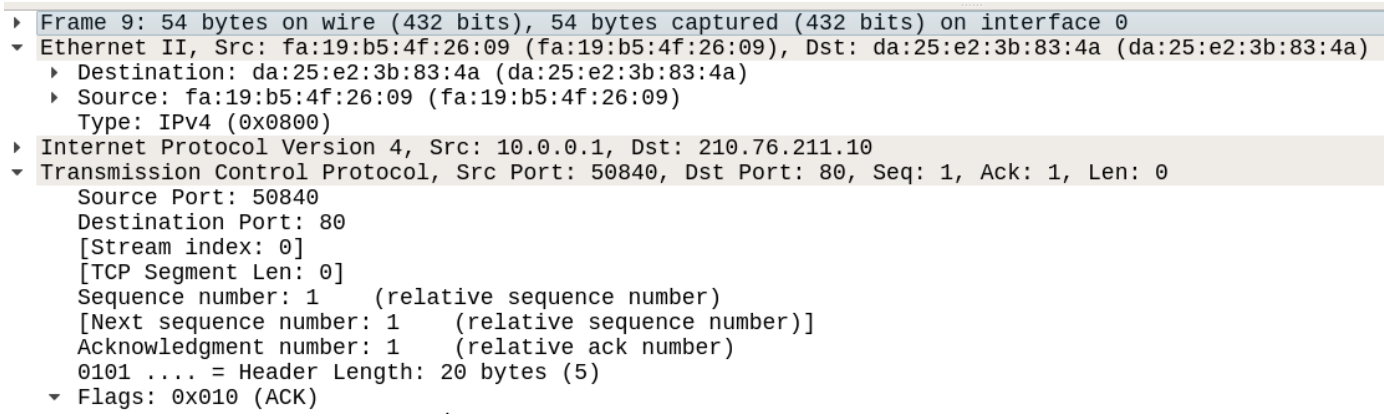
（三）DNS 协议层次



```
▸ Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▾ Ethernet II, Src: fa:19:b5:4f:26:09 (fa:19:b5:4f:26:09), Dst: da:25:e2:3b:83:4a (da:25:e2:3b:83:4a
  ▸ Destination: da:25:e2:3b:83:4a (da:25:e2:3b:83:4a)
  ▸ Source: fa:19:b5:4f:26:09 (fa:19:b5:4f:26:09)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 1.2.4.8
▸ User Datagram Protocol, Src Port: 51949, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xef11
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.ucas.ac.cn: type A, class IN
        Name: www.ucas.ac.cn
        [Name Length: 14]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 5]
```

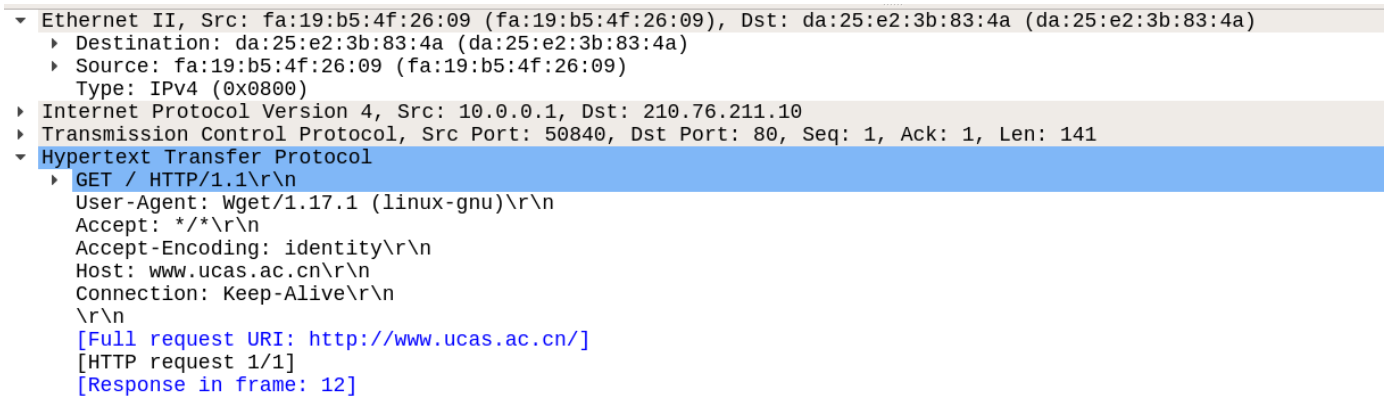
分析结果得层次为: Ethernet < IP < UDP < DNS

（四）TCP 协议层次



分析结果得层次为：Ethernet < IP < TCP

（五）HTTP 协议层次



分析结果得层次为：Ethernet < IP < TCP < HTTP

（六）结果分析

在获取 UCAS 主页的传输过程中使用了以下几种协议：ARP 协议、DNS 协议、TCP 协议、HTTP 协议,并得到了各个协议的封装层次:

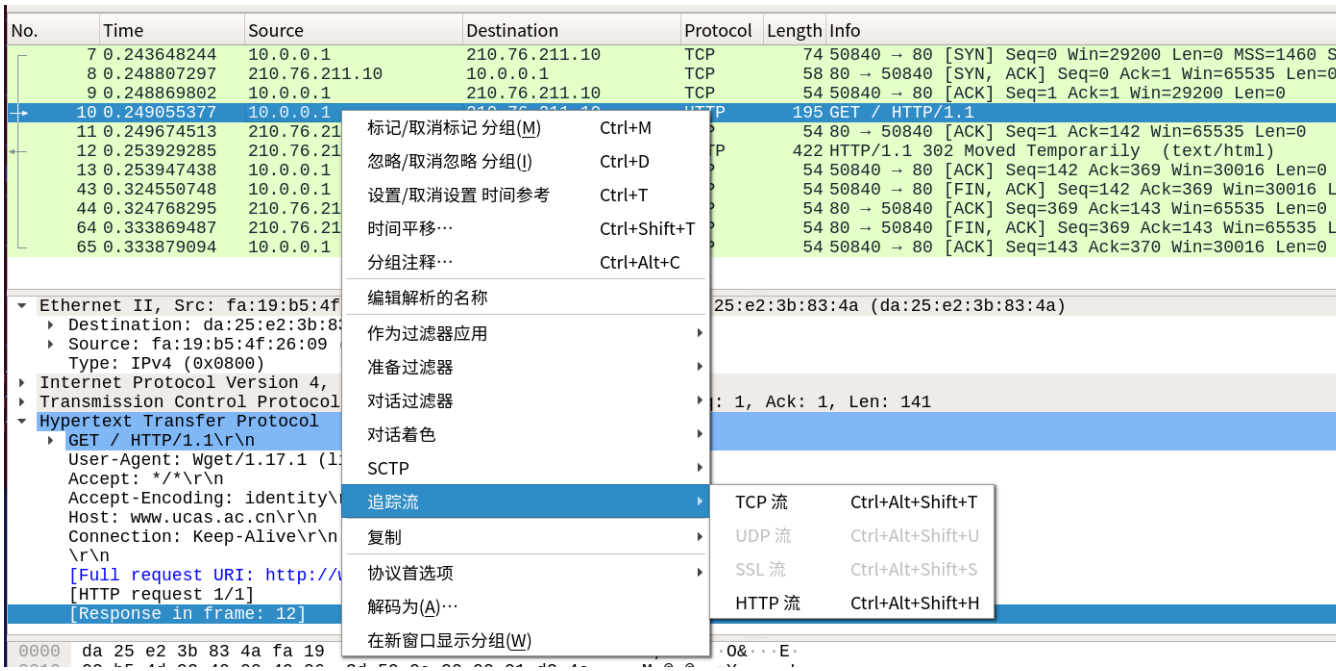
1. ARP 协议层次为：Ethernet < ARP

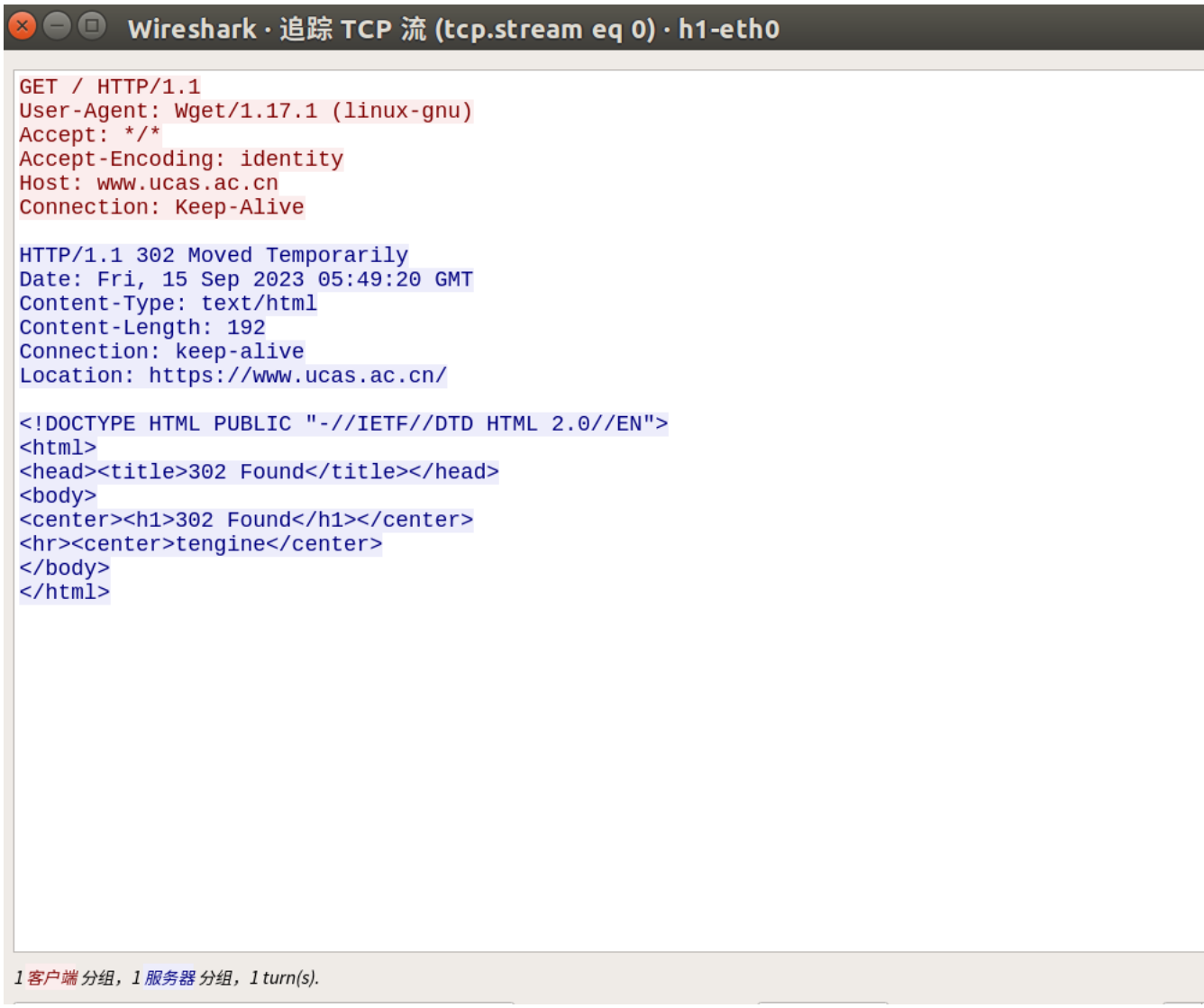
2. DNS 协议层次为：Ethernet < IP < UDP < DNS

3. TCP 协议层次为： Ethernet < IP < TCP

4. HTTP 协议层次为：Ethernet < IP < TCP < HTTP

从 Wireshark 抓包结果看出 TCP 承载 HTTP 协议





五、 调研

1. ARP（地址解析协议）：

ARP 协议“Address Resolution Protocol”(地址解析协议)的缩写。其作用是在以太网环境中,数据的传输所依懒的是 MAC 地址而非 IP 地址,而将已知 IP 地址转换为 MAC 地址的工作是由 ARP 协议来完成的。

在局域网中,网络中实际传输的是“帧”,帧里面是有目标主机的 MAC 地址的。在以太网中,一个主机和另一个主机进行直接通信,必须要知道目标主机的 MAC 地址。目标 MAC 地址是通过地址解析协议获得的。所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目

标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址,查询目标设备的 MAC 地址,以保证通信的顺利进行。ARP 通过发送一个 ARP 请求帧到局域网中的所有设备来查找目标设备的 MAC 地址。这个请求包含源设备的 IP 地址和 MAC 地址。目标设备收到请求后，会回复一个包含其 IP 地址和 MAC 地址的 ARP 响应帧。

2. DNS（域名系统）：

DNS (Domain Name System)是一个应用层协议，域名系统(DNS)的作用是将人类可读的域名(如 www.example.com)转换为机器可读的 IP 地址(如 192.0.2.44)。 DNS 系统使用树状层次结构，包括多个 DNS 服务器，它们负责不同的域名解析。当用户输入一个域名时，客户端的 DNS 解析器将向根 DNS 服务器发送查询，然后逐级查询更低级别的 DNS 服务器，直到找到与域名相关的 IP 地址。

DNS 协议建立在 UDP 或 TCP 协议之上,默认使用 53 号端口。客户端默认通过 UDP 协议进行通讯,但是由于广域网中不适合传输过大的 UDP 数据包,因此规定当报文长度超过了 512 字节时,应转换为使用 TCP 协议进行数据传输。DNS 是一种可以将域名和 IP 地址相互映射的以层次结构分布的数据库系统。

3. TCP（传输控制协议）：

TCP (Transmission Control Protocol 传输控制协议)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。在简化的计算机网络 OSI 模型中,它完成第四层传输层所指定的功能。

应用层向 TCP 层发送用于网间传输的、用 8 位字节表示的数据流,然后 TCP 把数据流分区成适当长度的报文段(通常受该计算机连接的网络的数据链路层的最大传输单元(MTU)的限

制）。之后 TCP 把结果包传给 IP 层,由它来通过网络将包传送给接收端实体的 TCP 层。TCP 将用户数据打包构成报文段,它发送数据时启动一个定时器,另一端收到数据进行确认,对失序的数据重新排序,丢弃重复的数据。简单说, TCP 协议的作用是,保证数据通信的完整性和可靠性，防止丢包。

4. HTTP（超文本传输协议）：

HTTP 协议(超文本传输协议 HyperText Transfer Protocol),它是基于 TCP 协议的应用层传输协议,用于从 WWW 服务器传输超文本到本地浏览器的传输协议, HTTP 是一个应用层协议,由请求和响应构成,是一个标准的客户端和服务器模型,简单来说就是客户端和服务端进行数据传输的一种规则。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。客户端发送 HTTP 请求到服务器，请求特定资源（如网页或图像）。服务器收到请求后，会发送 HTTP 响应，包含请求的资源以及相关信息。HTTP 通信通常是无状态的，每个请求和响应都独立于之前的请求和响应。

六、 结果解释

对于整个下载 UCAS 主页的过程解释如下:

1. 输入命令后,第一步执行的是将域名 www.ucas.ac.cn 通过 DNS 协议解析转换为相应的 IP 地址。
2. 然后本地会选择一个大于 1024 的本机端口（例如本次实验中是 50840）向转换后的目标 IP 地址的 80 端口发起 TCP 连接请求。经过标准的 TCP 握手流程，建立 TCP 连接。
3. 在建立起的 TCP 连接中,按照 HTTP 协议标准向目标发送 GET 方法报文(HTTP 请求)。目的主机收到数据帧，通过 IP->TCP->HTTP， HTTP 协议单元会回应 HTTP 协议格式封装

好的 HTML 形式数据(HTTP 响应)， 其中包含网页的 HTML 内容、状态码（例如 200 表示成功）、头部信息（包括服务器类型、响应日期等）。

4. 我的主机收到数据帧，通过 IP->TCP->HTTP->本地，网页数据（包括 HTML、CSS、JavaScript 和其他资源）下载完毕。

补充:

1. DNS 解析流程:

浏览器首先查询本地 DNS 缓存，以查看是否已经解析过该域名。如果没有，它将向本地 DNS 服务器发送请求。本地 DNS 服务器如果没有该域名的解析结果，将会递归地查询根 DNS 服务器，然后依次查询顶级域 DNS 服务器、权威域服务器，最终获取 www.ucas.ac.cn 的 IP 地址。

2. TCP 握手流程:

浏览器使用服务器的 IP 地址和 HTTP 默认端口（通常是 80）发送一个 TCP 连接请求。然后服务器接受连接请求，并回复一个 TCP 连接确认。最后浏览器接受服务器的确认，并建立了与服务器的 TCP 连接。这个过程通常称为 TCP 的三次握手。

七、 实验总结

本次实验实践难度较小,但包含的知识很多,在调研和做实验的过程中,我对各种协议有了进一步的认识，并且对平时访问网页的行为的过程有了更深的理解。