互联网协议实验报告

张翔雨 2018K8009929035

一、实验题目：互联网协议实验

二、实验内容

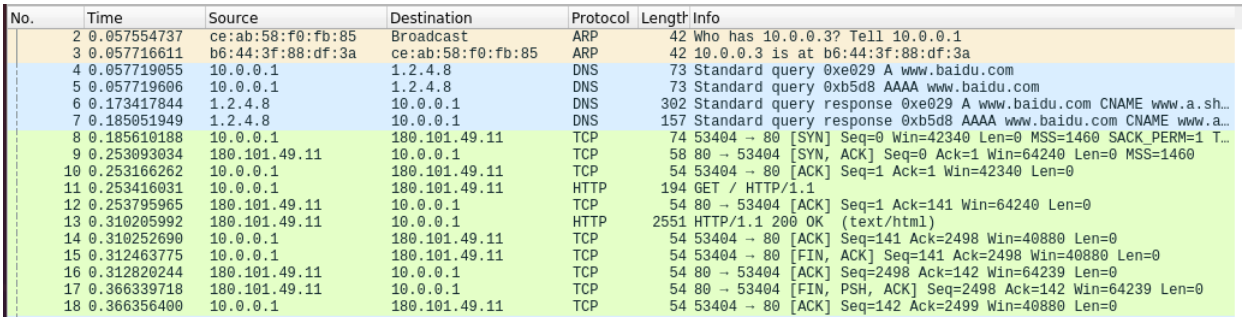
- 在节点h1上开启wireshark抓包，用wget下载www.baidu.com页面
- 调研说明wireshark抓到的几种协议
    - ARP, DNS, TCP, HTTP
- 调研解释h1下载baidu页面的整个过程
    - 几种协议的运行机制

三、实验流程

- 在终端中执行 `sudo mn --nat`，将host连接至Internet，启动mininet
- 在mininet中输入 `xterm h1`，打开控制h1的终端
- 在h1终端中输入 `echo "nameserver 1.2.4.8" > /etc/resolv.conf`
- 在h1终端中输入 `wireshark &`
- 在wireshark中选择h1-eth0
- 在h1终端中输入 `wget www.baidu.com` 下载百度页面
- 观察wireshark输出，调研分析获得的几种互联网协议

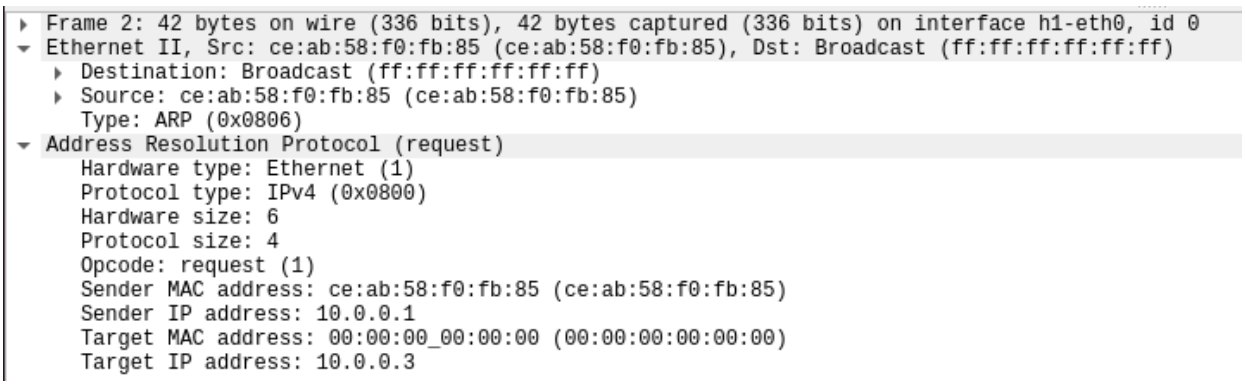
四、实验结果及分析

1.wireshark抓包结果



No.	Time	Source	Destination	Protocol	Length	Info
2	0.057554737	ce:ab:58:f0:fb:85	Broadcast	ARP	42	Who has 10.0.0.3? Tell 10.0.0.1
3	0.057716611	b6:44:3f:88:df:3a	ce:ab:58:f0:fb:85	ARP	42	10.0.0.3 is at b6:44:3f:88:df:3a
4	0.057719055	10.0.0.1	1.2.4.8	DNS	73	Standard query 0xe029 A www.baidu.com
5	0.057719606	10.0.0.1	1.2.4.8	DNS	73	Standard query 0xb5d8 AAAA www.baidu.com
6	0.173417844	1.2.4.8	10.0.0.1	DNS	302	Standard query response 0xe029 A www.baidu.com CNAME www.a.sh…
7	0.185051949	1.2.4.8	10.0.0.1	DNS	157	Standard query response 0xb5d8 AAAA www.baidu.com CNAME www.a…
8	0.185610188	10.0.0.1	180.101.49.11	TCP	74	53404 → 80 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM=1 T…
9	0.253093034	180.101.49.11	10.0.0.1	TCP	58	80 → 53404 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10	0.253166262	10.0.0.1	180.101.49.11	TCP	54	53404 → 80 [ACK] Seq=1 Ack=1 Win=42340 Len=0
11	0.253416031	10.0.0.1	180.101.49.11	HTTP	194	GET / HTTP/1.1
12	0.253795965	180.101.49.11	10.0.0.1	TCP	54	80 → 53404 [ACK] Seq=1 Ack=141 Win=64240 Len=0
13	0.310205992	180.101.49.11	10.0.0.1	HTTP	2551	HTTP/1.1 200 OK (text/html)
14	0.310252690	10.0.0.1	180.101.49.11	TCP	54	53404 → 80 [ACK] Seq=141 Ack=2498 Win=40880 Len=0
15	0.312463775	10.0.0.1	180.101.49.11	TCP	54	53404 → 80 [FIN, ACK] Seq=141 Ack=2498 Win=40880 Len=0
16	0.312820244	180.101.49.11	10.0.0.1	TCP	54	80 → 53404 [ACK] Seq=2498 Ack=142 Win=64239 Len=0
17	0.366339718	180.101.49.11	10.0.0.1	TCP	54	80 → 53404 [FIN, PSH, ACK] Seq=2498 Ack=142 Win=64239 Len=0
18	0.366356400	10.0.0.1	180.101.49.11	TCP	54	53404 → 80 [ACK] Seq=142 Ack=2499 Win=40880 Len=0

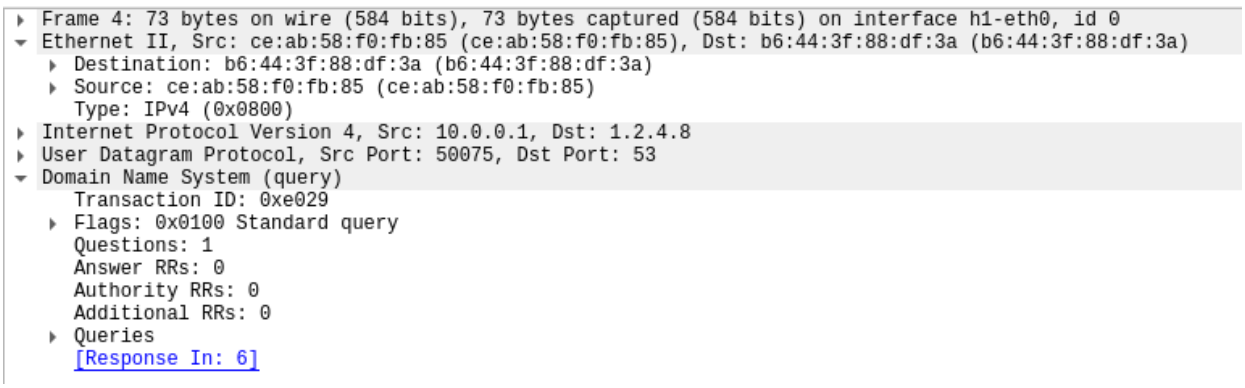
2.ARP协议层次



```
▸ Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface h1-eth0, id 0
▾ Ethernet II, Src: ce:ab:58:f0:fb:85 (ce:ab:58:f0:fb:85), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: ce:ab:58:f0:fb:85 (ce:ab:58:f0:fb:85)
    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: ce:ab:58:f0:fb:85 (ce:ab:58:f0:fb:85)
    Sender IP address: 10.0.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.0.3
```

分析结果得层次为：Ethernet < ARP

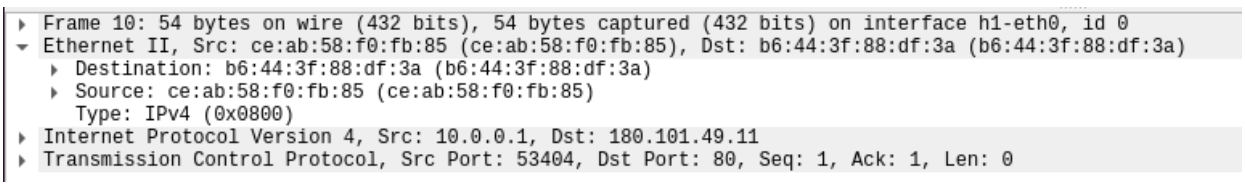
3.DNS协议层次



```
▸ Frame 4: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface h1-eth0, id 0
▾ Ethernet II, Src: ce:ab:58:f0:fb:85 (ce:ab:58:f0:fb:85), Dst: b6:44:3f:88:df:3a (b6:44:3f:88:df:3a)
  ▸ Destination: b6:44:3f:88:df:3a (b6:44:3f:88:df:3a)
  ▸ Source: ce:ab:58:f0:fb:85 (ce:ab:58:f0:fb:85)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 1.2.4.8
▸ User Datagram Protocol, Src Port: 50075, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xe029
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 6]
```

分析结果得层次为：Ethernet < IP < UDP < DNS

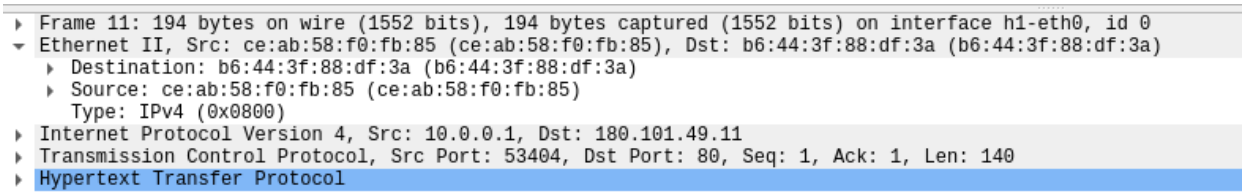
4.TCP协议层次



```
▸ Frame 10: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface h1-eth0, id 0
▾ Ethernet II, Src: ce:ab:58:f0:fb:85 (ce:ab:58:f0:fb:85), Dst: b6:44:3f:88:df:3a (b6:44:3f:88:df:3a)
  ▸ Destination: b6:44:3f:88:df:3a (b6:44:3f:88:df:3a)
  ▸ Source: ce:ab:58:f0:fb:85 (ce:ab:58:f0:fb:85)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 180.101.49.11
▸ Transmission Control Protocol, Src Port: 53404, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

分析结果得层次为：Ethernet < IP <TCP

5.HTTP协议层次



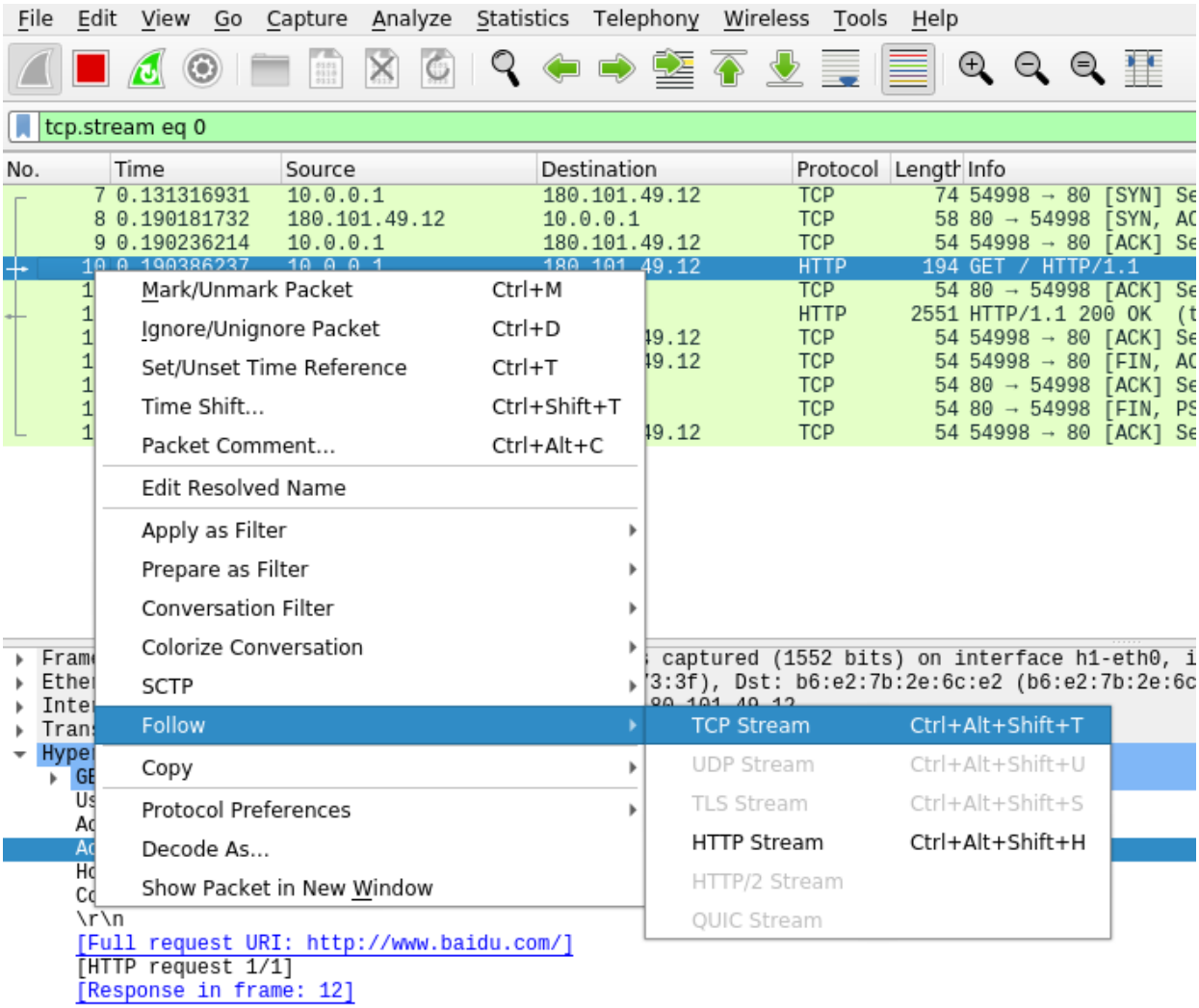
分析结果得层次为：Ethernet < IP < TCP < HTTP

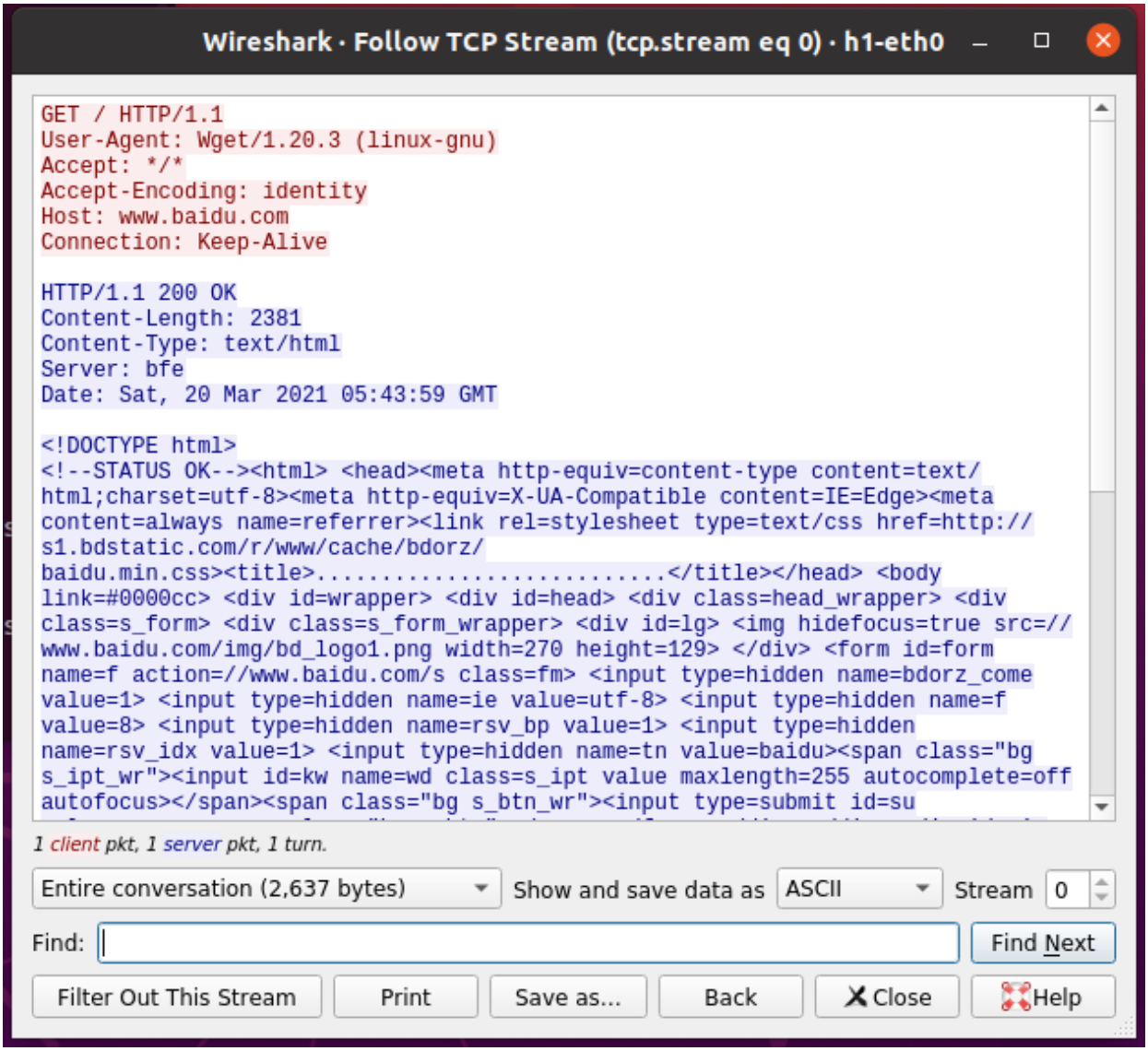
6.结果分析

在获取百度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：

- ARP协议层次为：Ethernet < ARP
- DNS协议层次为：Ethernet < IP < UDP < DNS
- TCP协议层次为：Ethernet < IP <TCP
- HTTP协议层次为：Ethernet < IP < TCP < HTTP

从Wireshark抓包结果看出TCP承载HTTP协议


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
7 0.131316931 10.0.0.1 180.101.49.12 TCP 74 54998 → 80 [SYN] Se
8 0.190181732 180.101.49.12 10.0.0.1 TCP 58 80 → 54998 [SYN, AC
9 0.190236214 10.0.0.1 180.101.49.12 TCP 54 54998 → 80 [ACK] Se
10 0.190386237 10.0.0.1 180.101.49.12 HTTP 194 GET / HTTP/1.1
TCP 54 80 → 54998 [ACK] Se
HTTP 2551 HTTP/1.1 200 OK (t
TCP 54 54998 → 80 [ACK] Se
TCP 54 54998 → 80 [FIN, AC
TCP 54 80 → 54998 [ACK] Se
TCP 54 80 → 54998 [FIN, PS
TCP 54 54998 → 80 [ACK] Se
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
captured (1552 bits) on interface h1-eth0, i
3:3f), Dst: b6:e2:7b:2e:6c:e2 (b6:e2:7b:2e:6c
\r\n
[Full request URI: http://www.baidu.com/]
[HTTP request 1/1]
[Response in frame: 12]



五、调研

1.ARP协议

ARP协议是“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。

2.DNS协议

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 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,是一个标准的个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。

六、结果解释

对于整个下载百度主页的过程解释如下：

- 输入命令后，第一步执行的是将域名www.baidu.com通过DNS协议解析转换为相应的IP地址。

- 然后本地会选择一个大于1024的本机端口向转换后的目标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。
- 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）
- 我的主机收到数据帧，通过IP->TCP->HTTP->本地，网页数据下载完毕。

七、实验总结

本次实验实践难度较小，但包含信息量极大，在调研和做实验的过程中，我逐渐对各种协议有了初步的认识。而利用调研得到的知识去解释实验现象更加加深了我对平时访问网页的行为的理解。