**福建农林大学计算机与信息学院**

**课程设计说明书**

|  |  |
| --- | --- |
| 课程名称： | 计算机网络协议分析 |
| 课程设计题目： | IIS+Ngrok的Web服务器配置与管理 |
| 姓 名： | 陈炜林 |
| 系 别： | 计算机科学与技术系 |
| 专 业： | 网络工程 |
| 年 级： | 2019级 |
| 学 号： | 3196020077 |
| 指导教师： | 严金妹 |
| 职 称： | 讲 师 |

2021年7月2日

目录

[目录 2](#_Toc22467)

[1 Web服务器概述 3](#_Toc134)

[1.1 Web服务器简介 3](#_Toc31835)

[1.2 Web服务器的必要性 3](#_Toc30575)

[2 Web服务器的部署搭建 4](#_Toc1966)

[2.1 IIS服务器 4](#_Toc10990)

[2.1.1 IIS服务器介绍 4](#_Toc31715)

[2.1.2 IIS服务器配置 4](#_Toc29905)

[2.1.3 相关文件资源的部署(ISS服务器根目录下HTML文件的创建) 7](#_Toc13008)

[2.2 简单的本机测试 11](#_Toc31213)

[3 基于局域网的HTTP报文交互 13](#_Toc28414)

[3.1 HTTP报文交互过程及抓包分析 13](#_Toc1919)

[3.2 深入理解HTTP协议 22](#_Toc4622)

[3.2.1 常用HTTP方法 22](#_Toc1183)

[3.2.2 POST和GET方法的区别 22](#_Toc2787)

[3.2.2 常见HTTP响应 22](#_Toc24608)

[3.2.3 HTTP工作原理 23](#_Toc25215)

[4 基于互联网的HTTP报文交互 24](#_Toc26257)

[4.1 内网穿透技术 24](#_Toc17531)

[4.1.1 内网穿透技术简介 24](#_Toc2374)

[4.1.2 NAT实现方式 24](#_Toc2173)

[4.2 Ngrok的使用 25](#_Toc9860)

[4.2.1 原理 25](#_Toc11288)

[4.2.2服务器域名的配置 25](#_Toc9296)

[4.3 互联网下HTTP协议报文分析 27](#_Toc26876)

[4.3.1 客户端报文情况 27](#_Toc31342)

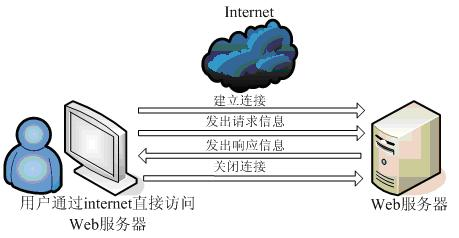
[4.3.2 服务器报文情况 28](#_Toc12644)

[5 结束语 28](#_Toc28047)

[6 附件清单 29](#_Toc27931)

# Web服务器概述

## Web服务器简介

1、Web服务器是指驻留于因特网上某种类型计算机的程序，是可以向发出请求的浏览器提供文档的程序。当Web浏览器（客户端）连到服务器上并请求文件时，服务器将处理该请求并将文件反馈到该浏览器上，附带的信息会告诉浏览器如何查看该文件（即文件类型）。  
  
2、服务器是一种被动程序：只有当Internet上运行在其他计算机中的浏览器发出请求时，服务器才会响应。  


## Web服务器的必要性

1、不管什么Web资源，想被远程计算机访问，都必须有一个与之对应的网络通信程序，当用户来访问时，这个网络通信程序读取Web资源数据，并把数据发送给来访者。  
2、Web服务器就是这样一个程序，它用于完成底层网络通迅。使用这些服务器，Web应用的开发者只需要关注Web资源怎么编写，而不需要关心资源如何发送到客户端手中，从而极大的减轻了开发者的开发工作量。

# Web服务器的部署搭建

## IIS服务器

### IIS服务器介绍

Microsoft的Web服务器产品为IIS。IIS 是Internet Information Server的缩写，中文名：Internet信息服务，专用于微软操作系统平台，兼容微软的各项Web技术。IIS支持HTTP（Hypertext Transfer Protocol，超文本传输协议），FTP（Fele Transfer Protocol，文件传输协议）以及SMTP协议，Internet Information Services提供对Web和FTP服务器的支持，以及对ASP.NET网站、动态内容(如经典ASP和CGI)和本地及远程管理的支持。

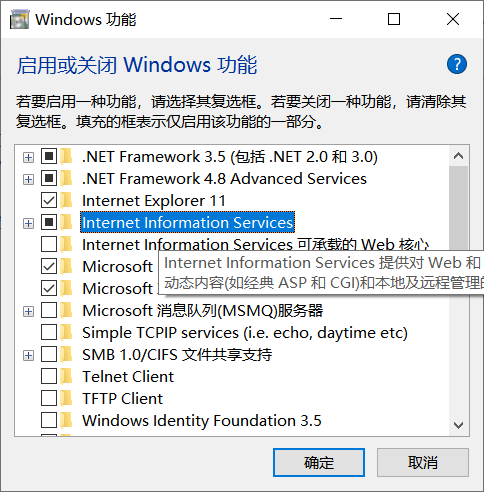
IIS(Internet Information Server)是[microsoft](http://www.so.com/s?q=microsoft&ie=utf-8&src=internal_wenda_recommend_textn" \t "https://wenda.so.com/q/_blank)[微软](http://www.so.com/s?q=%E5%BE%AE%E8%BD%AF&ie=utf-8&src=internal_wenda_recommend_textn" \t "https://wenda.so.com/q/_blank)自带的一个[组件](http://www.so.com/s?q=%E7%BB%84%E4%BB%B6&ie=utf-8&src=internal_wenda_recommend_textn" \t "https://wenda.so.com/q/_blank)。在win 2000以上的[操作系统](http://www.so.com/s?q=%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F&ie=utf-8&src=internal_wenda_recommend_textn" \t "https://wenda.so.com/q/_blank)(xp[家庭版](http://www.so.com/s?q=%E5%AE%B6%E5%BA%AD%E7%89%88&ie=utf-8&src=internal_wenda_recommend_textn" \t "https://wenda.so.com/q/_blank)没有)都有，所以IIS服务器的安装、配置、管理都可以在本地操作系统上完成。

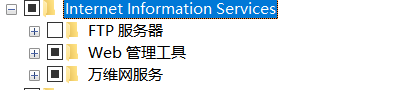
### IIS服务器配置

1.打开控制面板，找到程序与功能



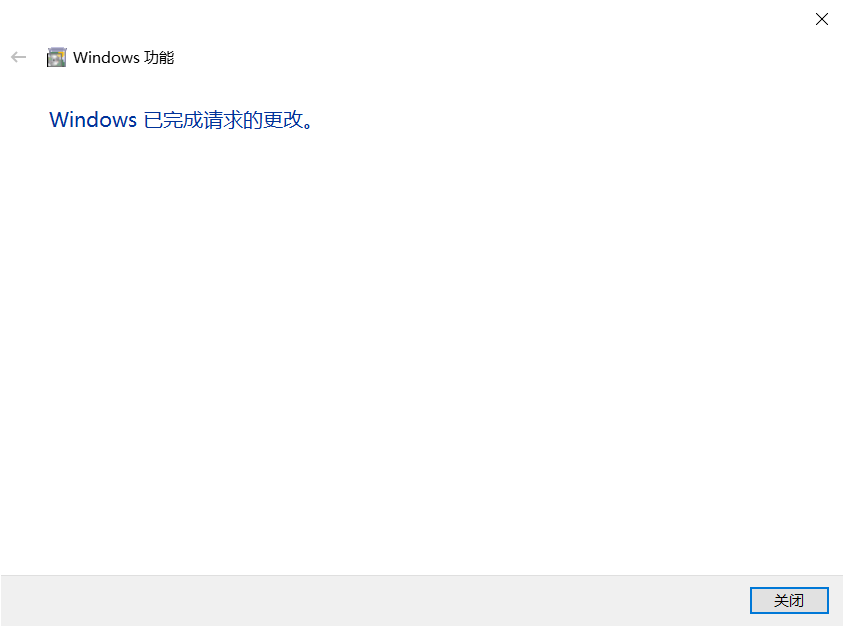
2.点击启用或关闭Windows功能，勾选Internet Information Service



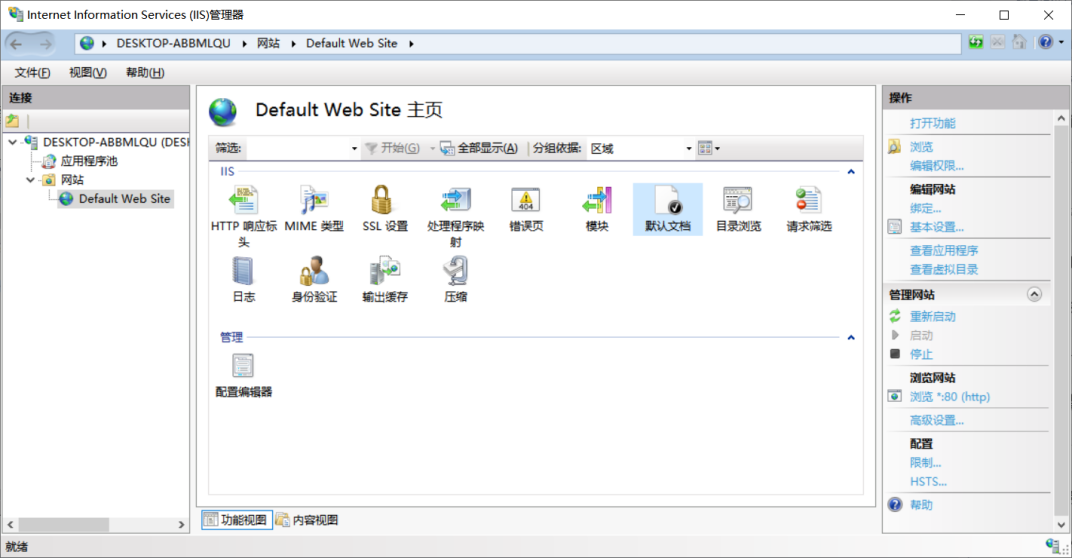


里面包含着FTP服务器、Web管理工具、万维网服务，由于本次是搭建Web服务器，所以FTP服务器可不勾选

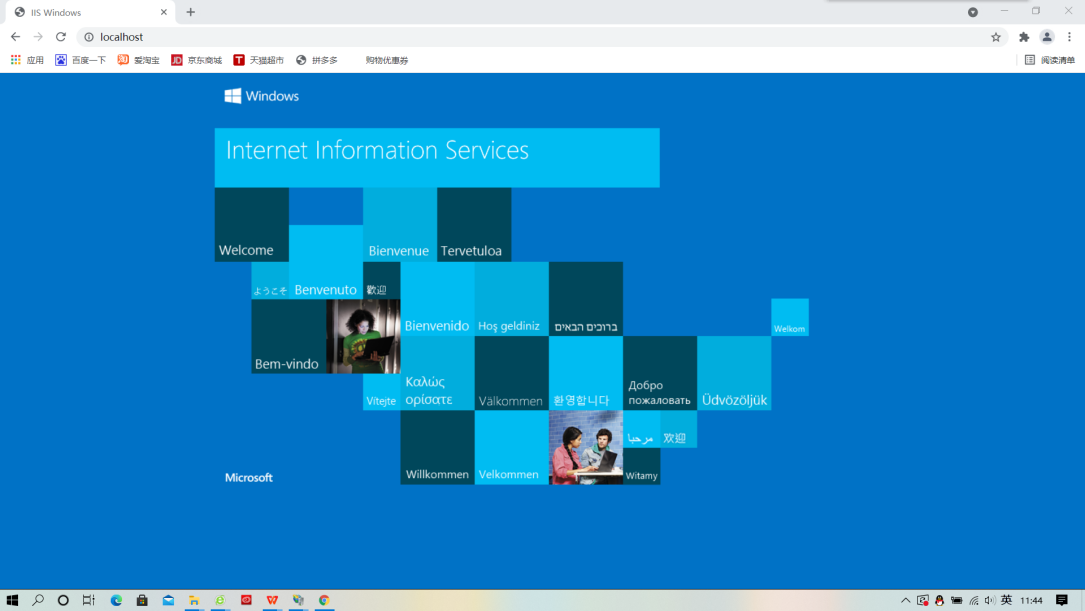
1. 等待更改完成



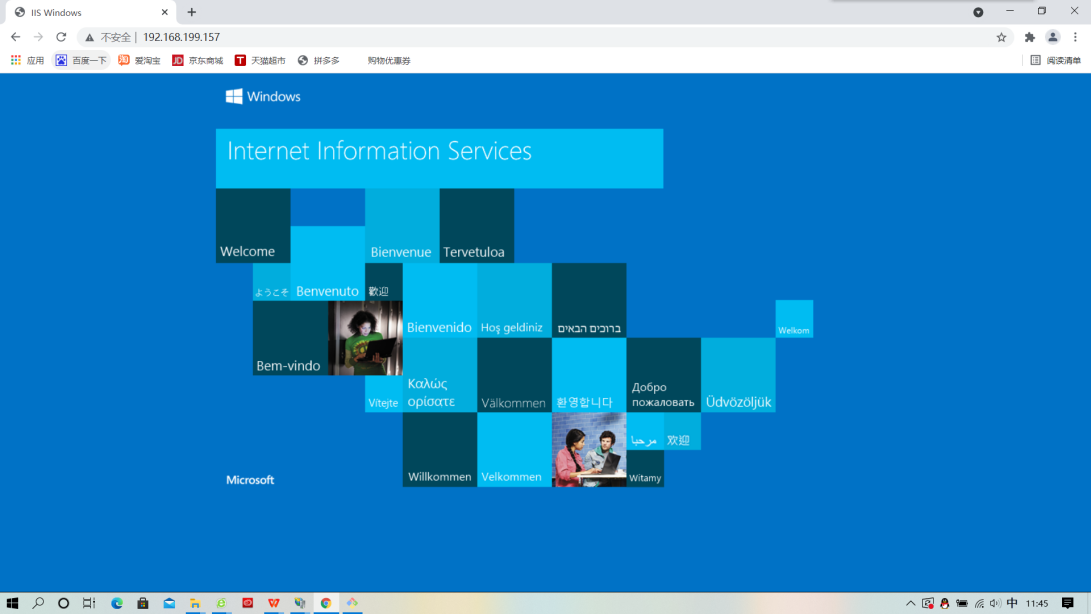
1. 查看ISS管理器



1. 打开浏览器，输入HTTP://localhost/，出现IIS欢迎界面说明正常



1. 在导航里面输入本机当前IP地址，也会出现相同的ISS欢迎界面，及时换到不同网络下，IP地址变化，只要IIS服务器有在本机启动，输入本机的IP地址都能够成功访问

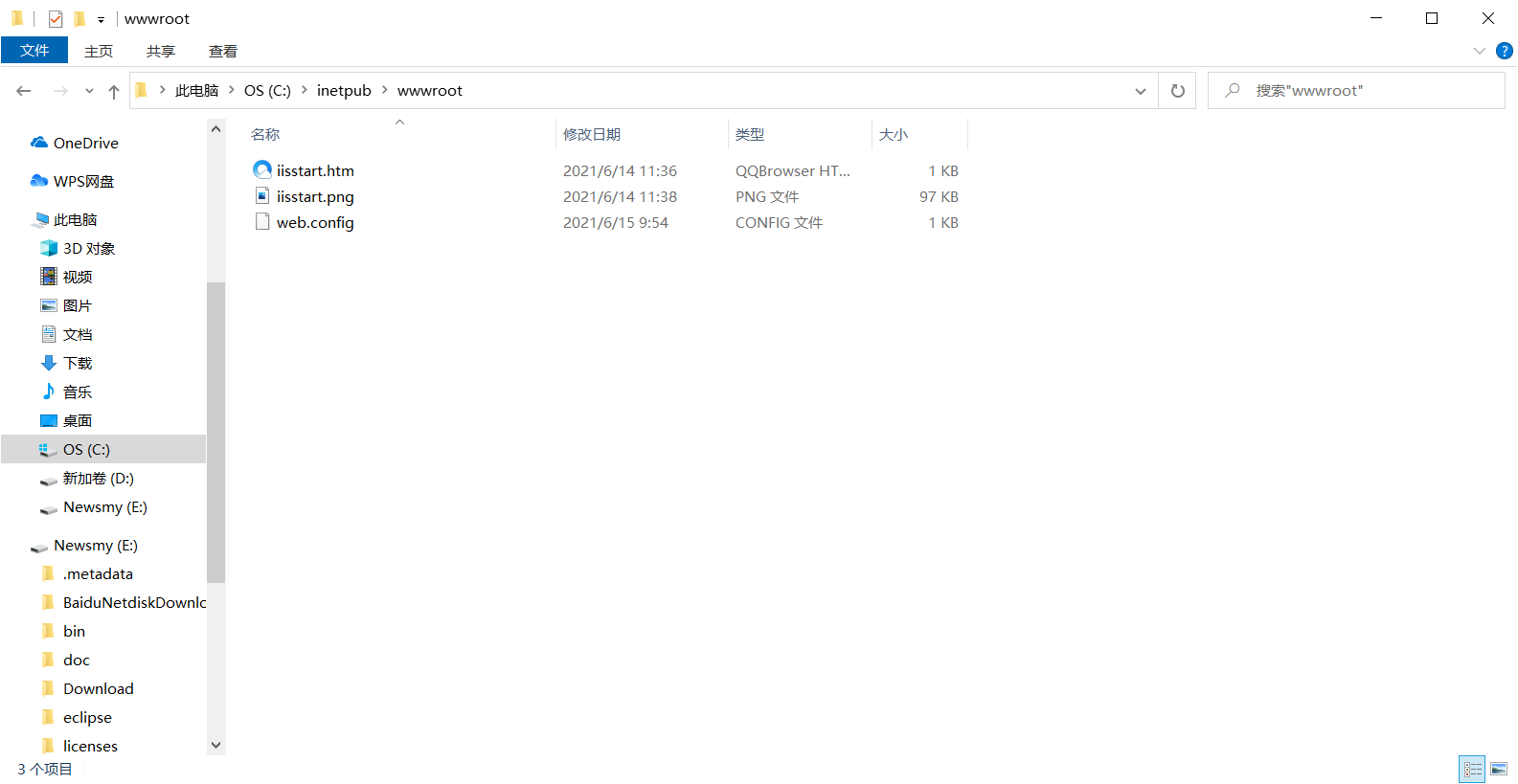


### 相关文件资源的部署(ISS服务器根目录下HTML文件的创建)

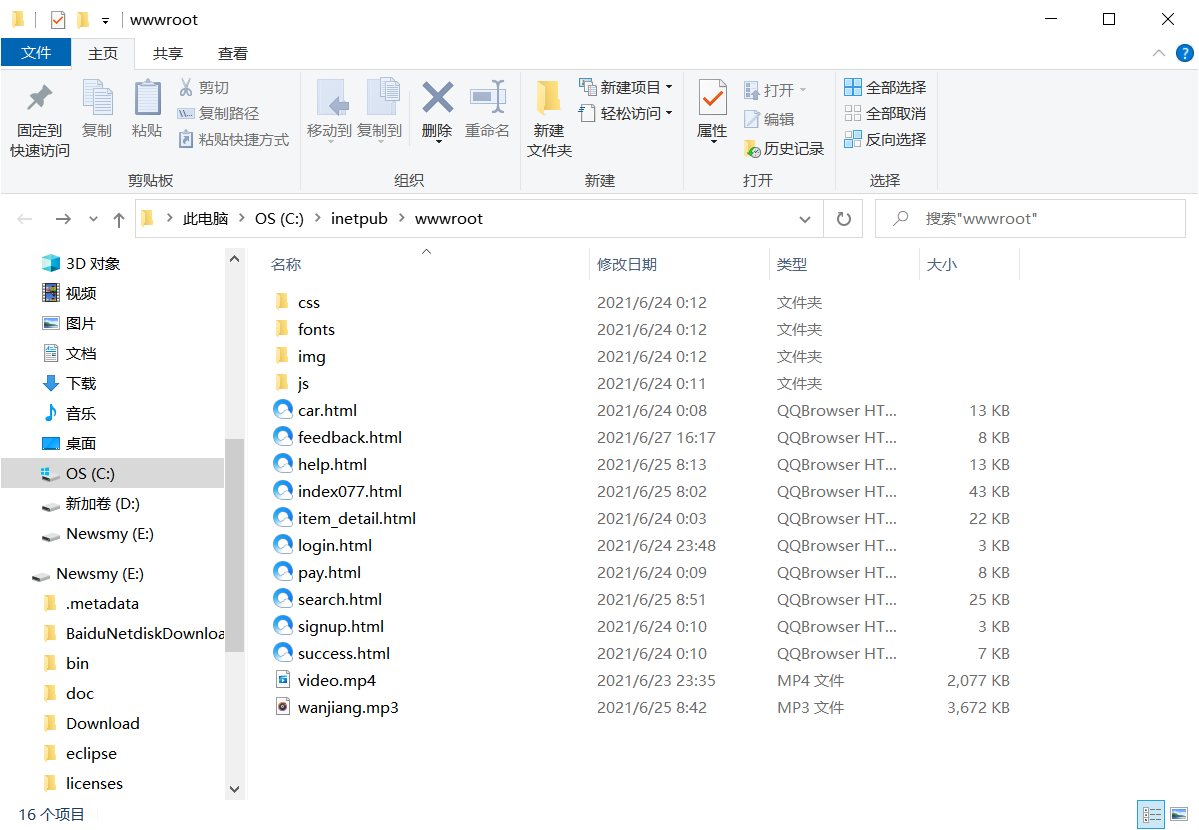
1. 打开IIS管理器，点击网站，点击Default Web Site，在操作栏里点击浏览进入ISS服务器根目录



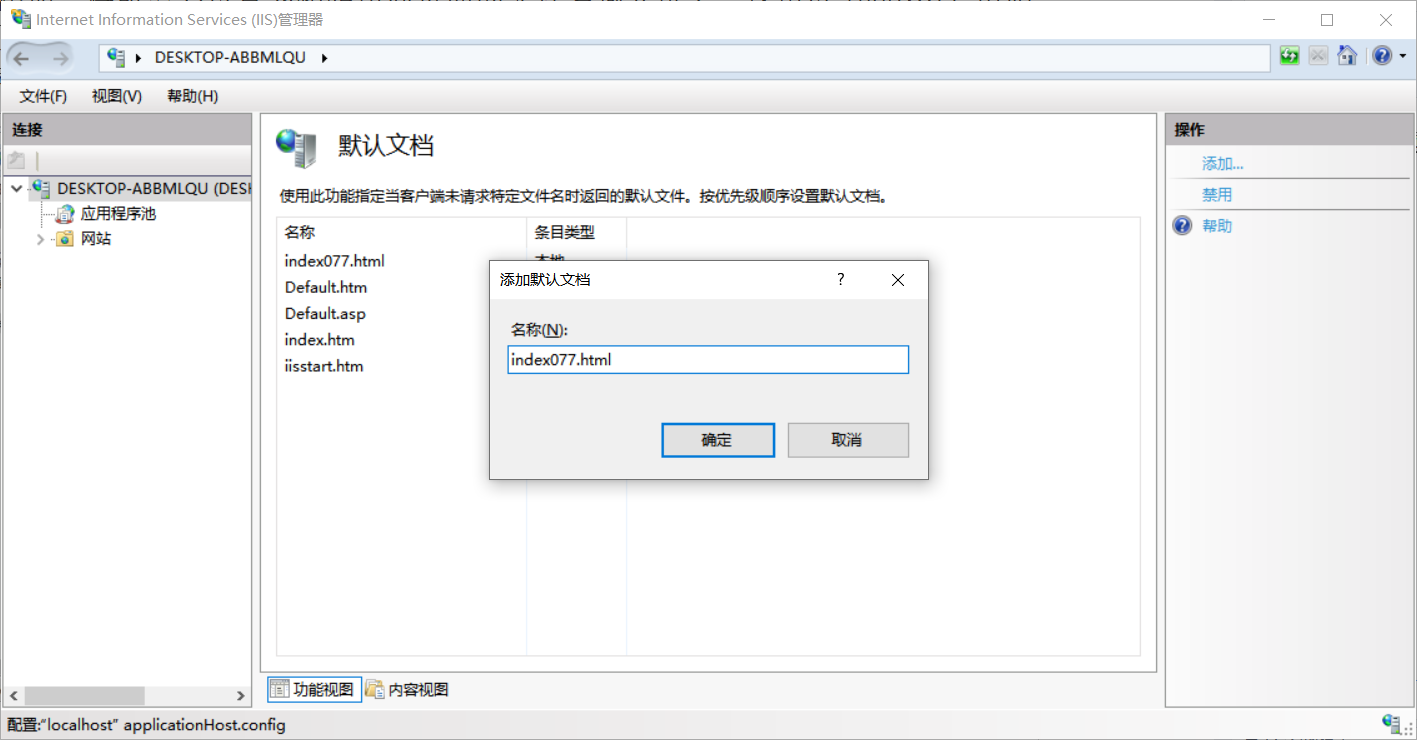
在根目录下，其中的HTML文件为ISS服务器默认的，即每次访问的都为该初始页面



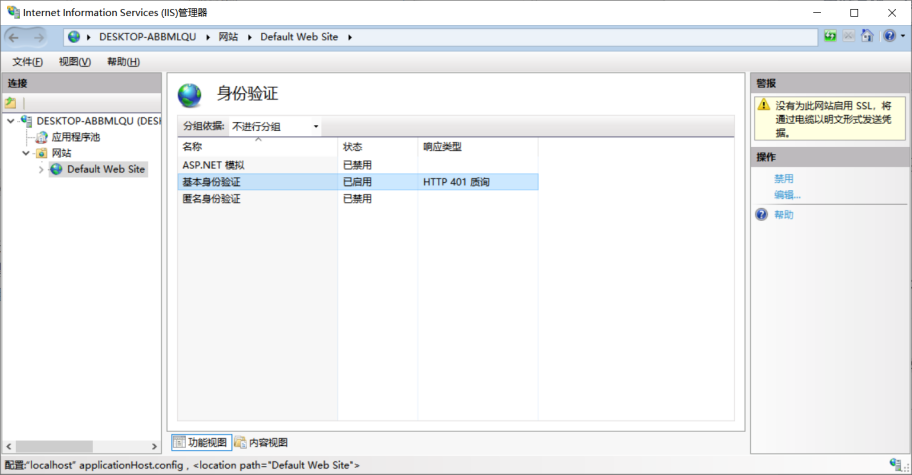
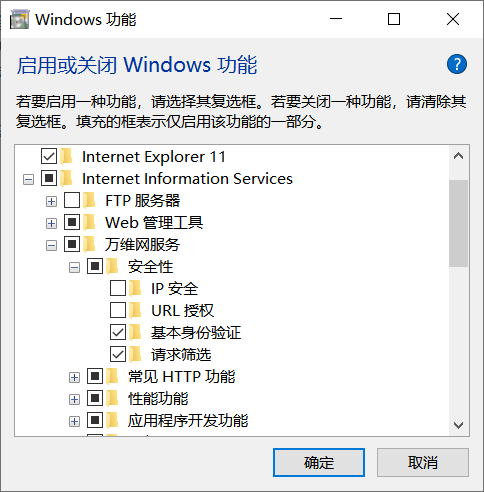
1. 将自己整理好的HTML文件放入到此根目录下，这是一个购物网站的资源集合，网站所有图片文件放在img文件夹里面，所以Get到所有的图片路径都是/img/...，css文件夹用来修饰页面，fonts是与修改字体、字体图标相关的资源文件，js文件是控制页面逻辑的，这是导入前端框架所需的包



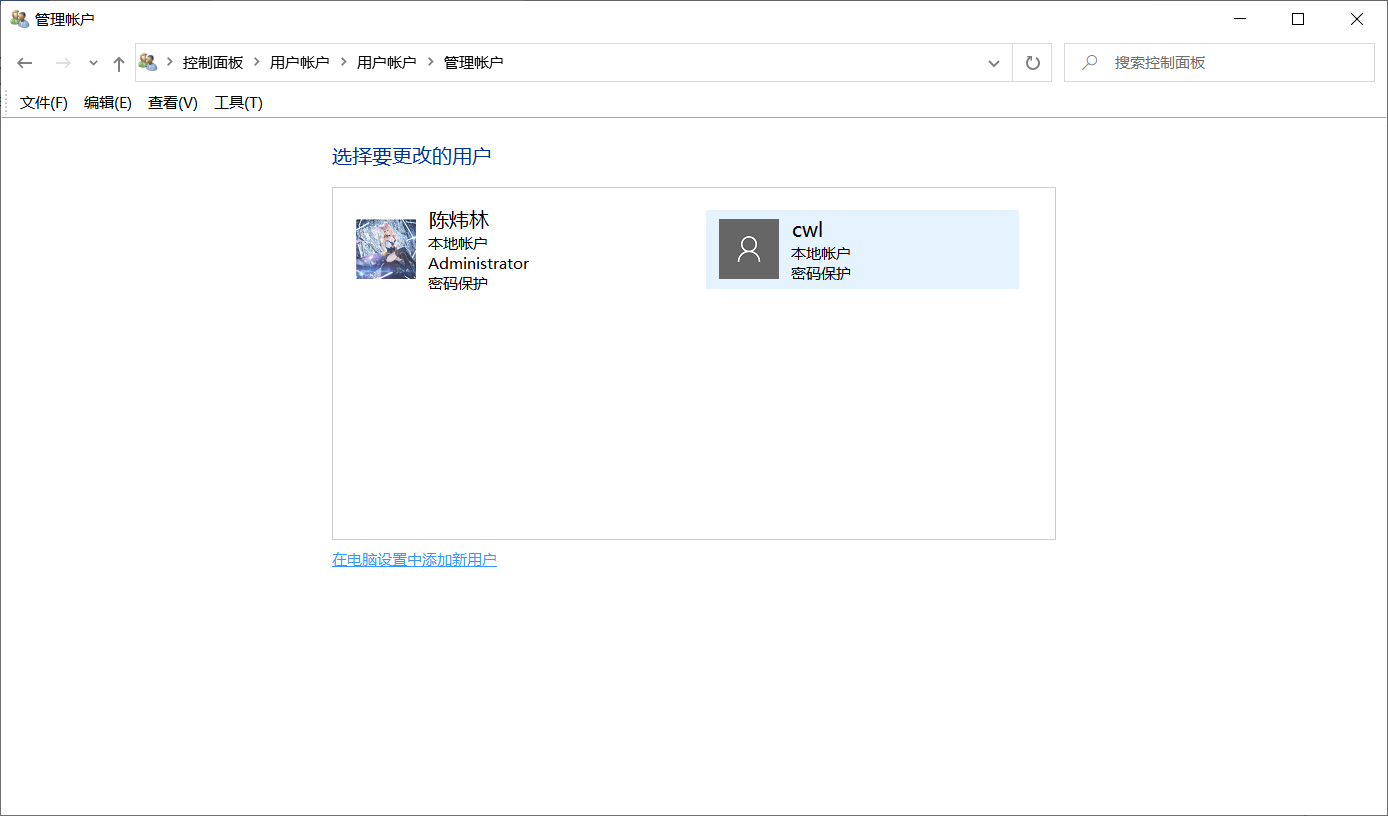
1. 在IIS管理器上点开Default Web Site主页，点击默认文档来设置初始页面，上述有提到，由于IIS管理器的默认初始页面为iistart.htm这个文件，所以可以在默认文档点击添加，将所需要设置为初始访问页面的文件名输入进去，这边以index077.html为初始页面，所以输入该名称添加默认文档，因为在默认文档里面有优先级，越上面的优先级越高，所以注意要将其上移到最上方



1. 为了抓取关于身份验证的包，可以简单设置一下基本身份验证，点开后如果里面只有匿名身份认证没有基本身份认证的话，需要在控制面板里的程序的启用Window功能里面打开IIS，将万维网里的安全性打开，勾选基本身份认证。然后再启用基本身份认证，禁用掉匿名身份认证。

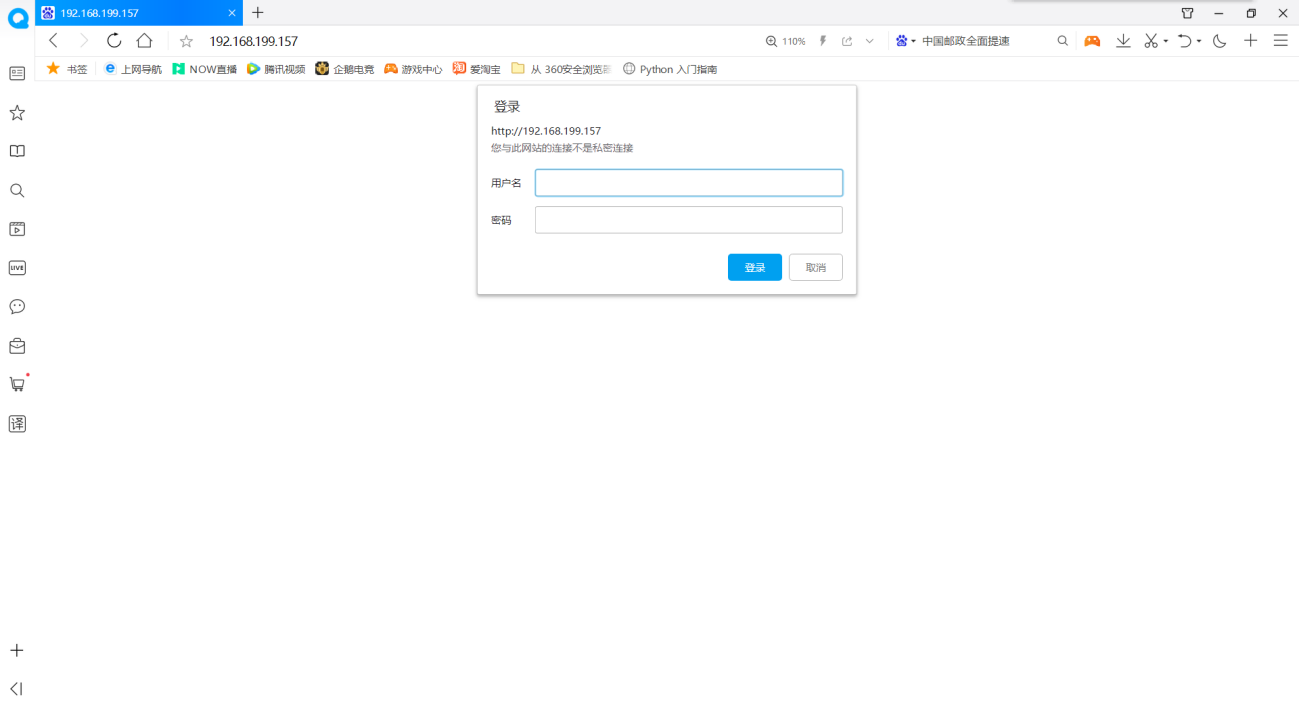


基本身份认证的账户密码为Windows的用户密码，可以在控制面板里的管理账户添加一个新用户以便用于基本身份认证



## 简单的本机测试

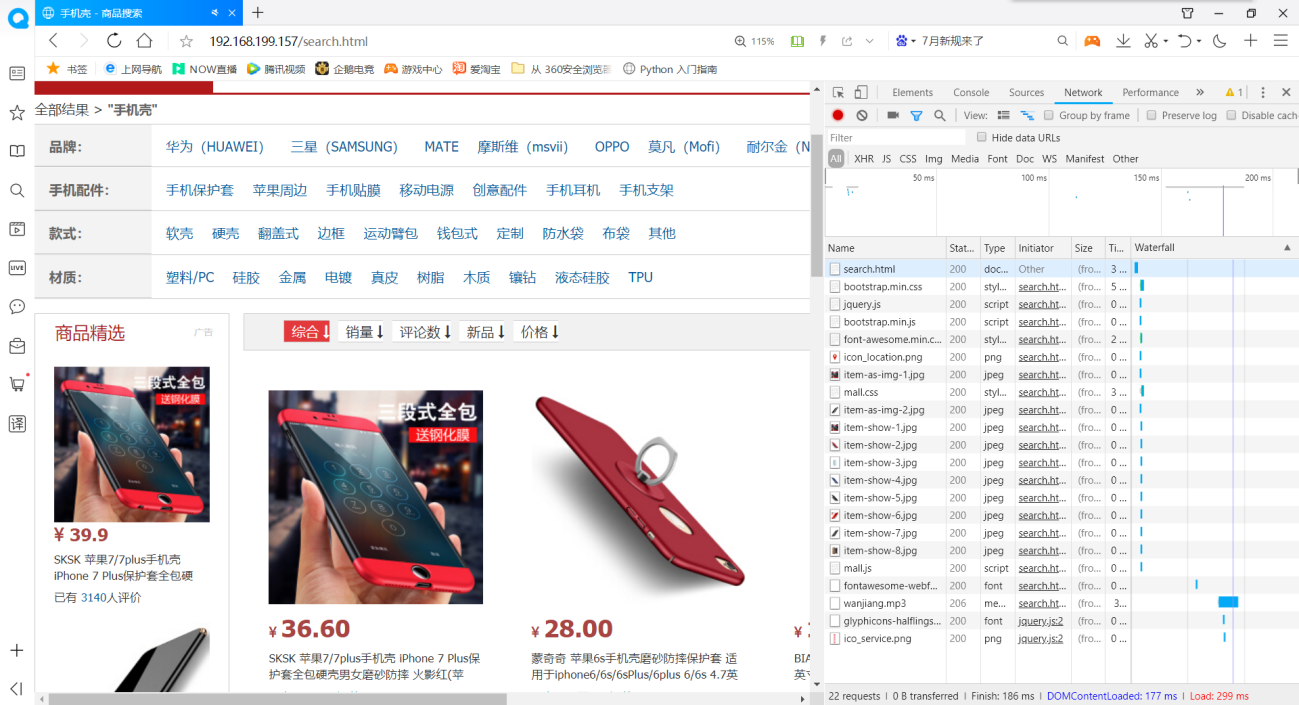
1. 打开浏览器，本机IP地址为192.168.199.157，输入HTTP://192.168.199.157/，首先会出现登录请求用于身份验证，账户密码为Windows用户的账户密码

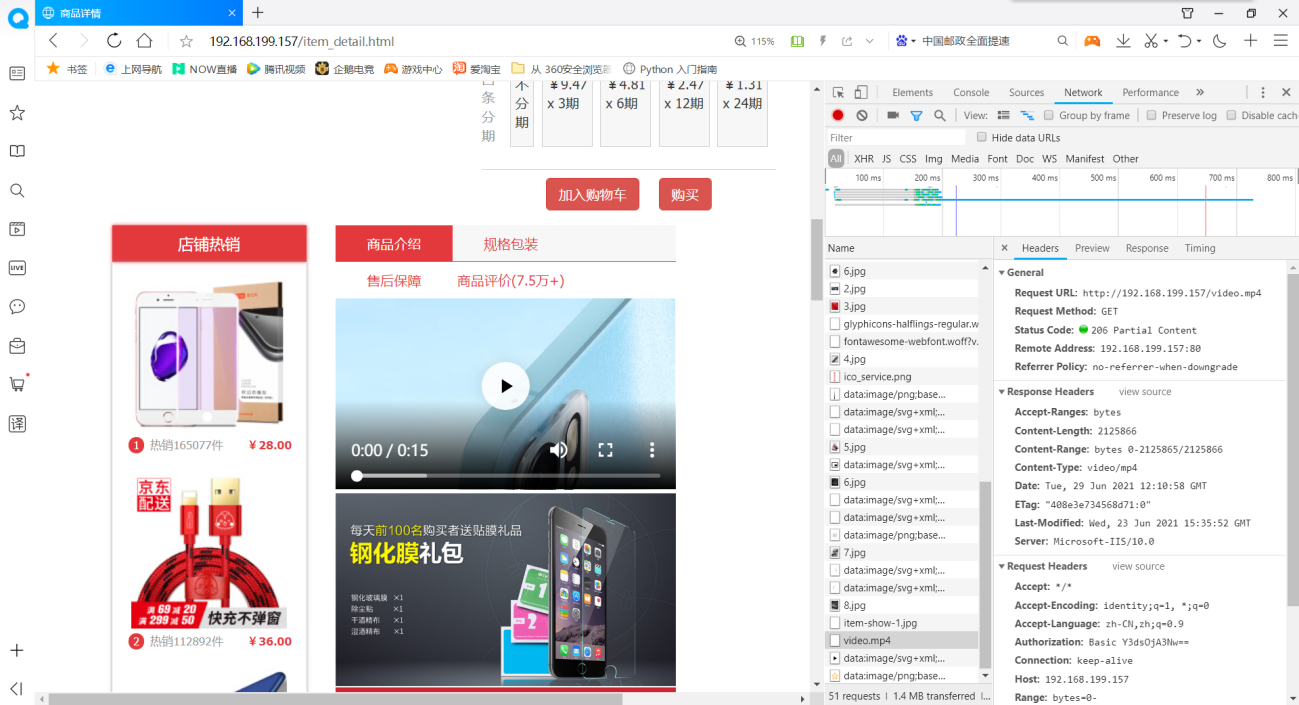


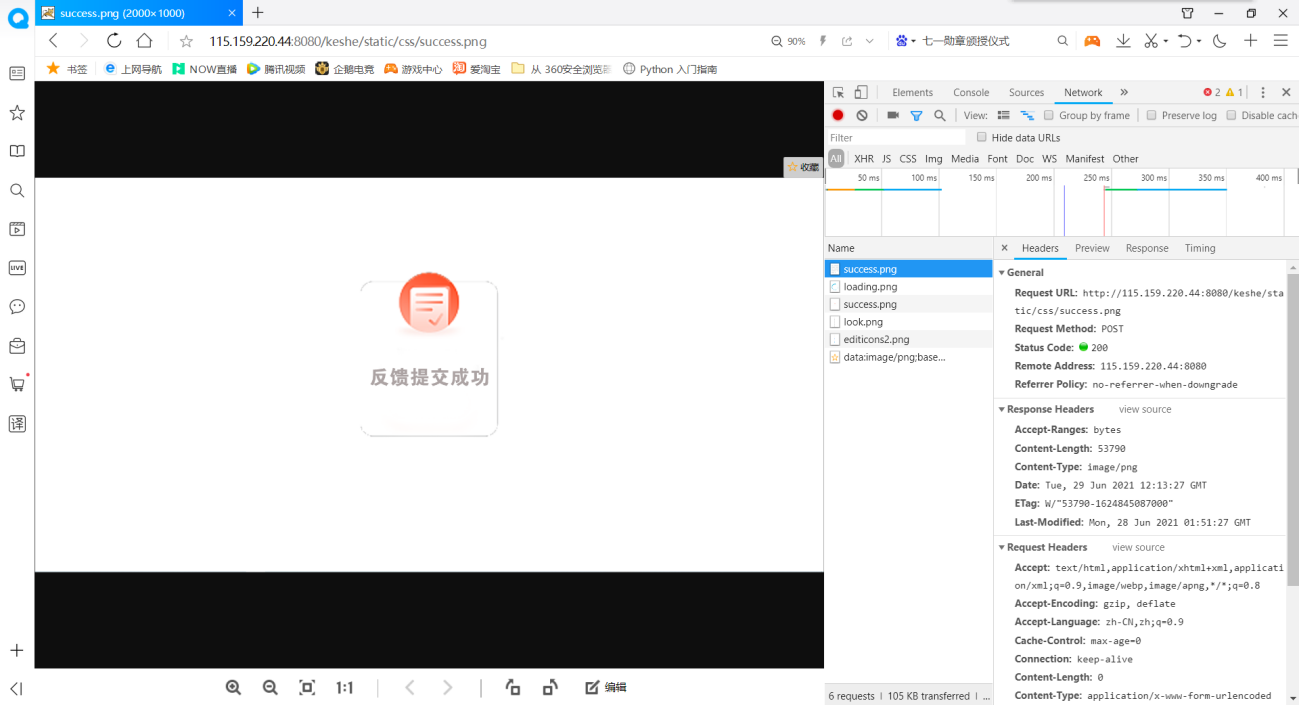
1. 登录成功后，页面为设置好的index077.html页面



1. 能够正常相应其他Html文件和资源



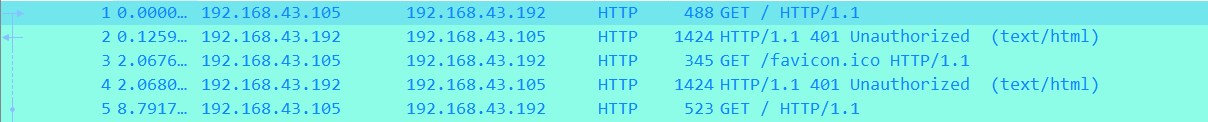




# 3 基于局域网的HTTP报文交互

## 3.1 HTTP报文交互过程及抓包分析

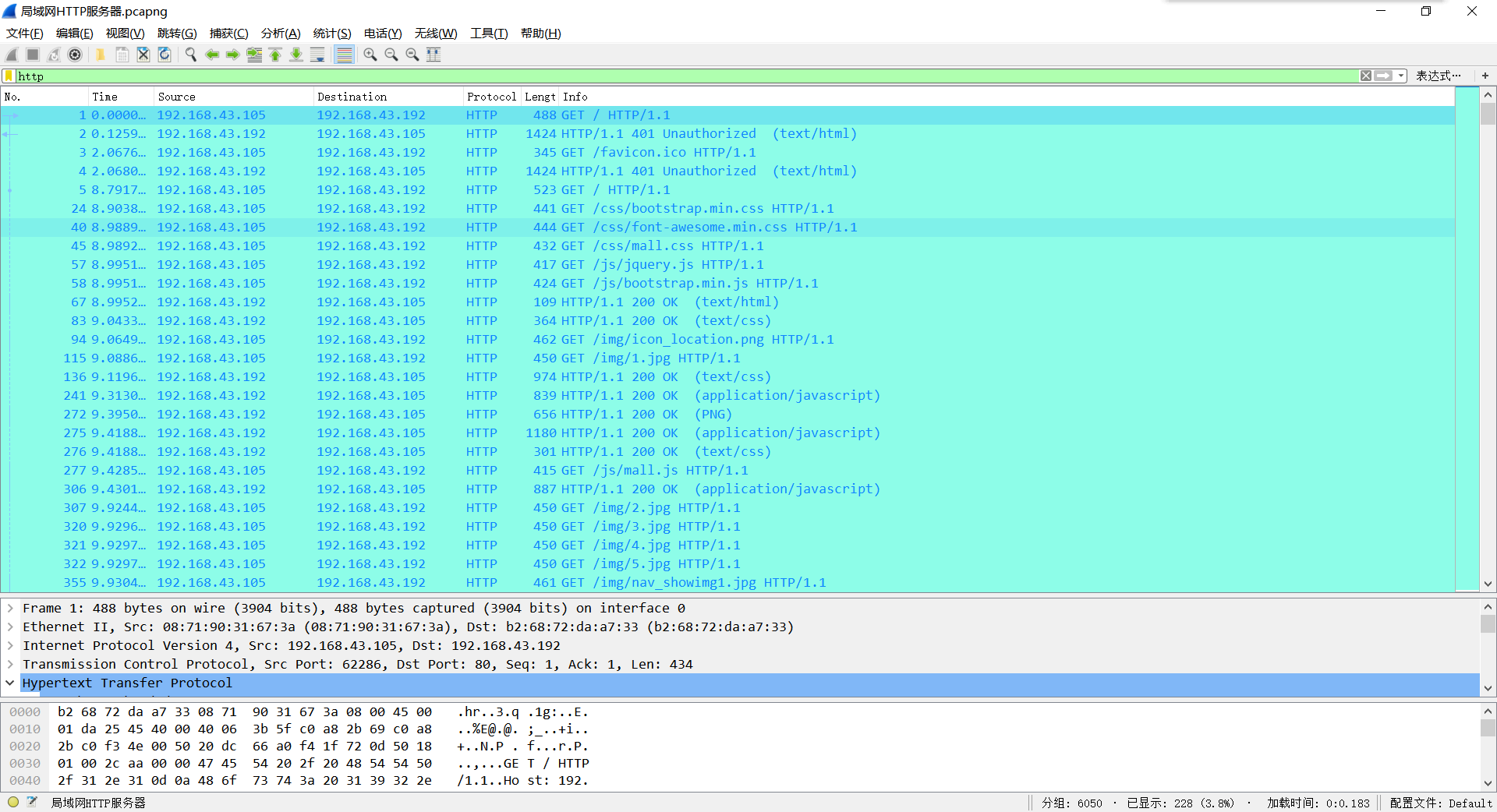
1. 本地主机启动IIS服务器
2. 使用一台处于同一局域网的客户机（IP地址为192.168.43.105）进行访问HTTP://192.168.43.192/，并且在服务器（本主机，IP地址此时为192.168.43.192）和客户机上打开wireshark，观察HTTP报文交互过程
3. 访问后，首先会出现身份验证，要求输入用户名和密码才能访问



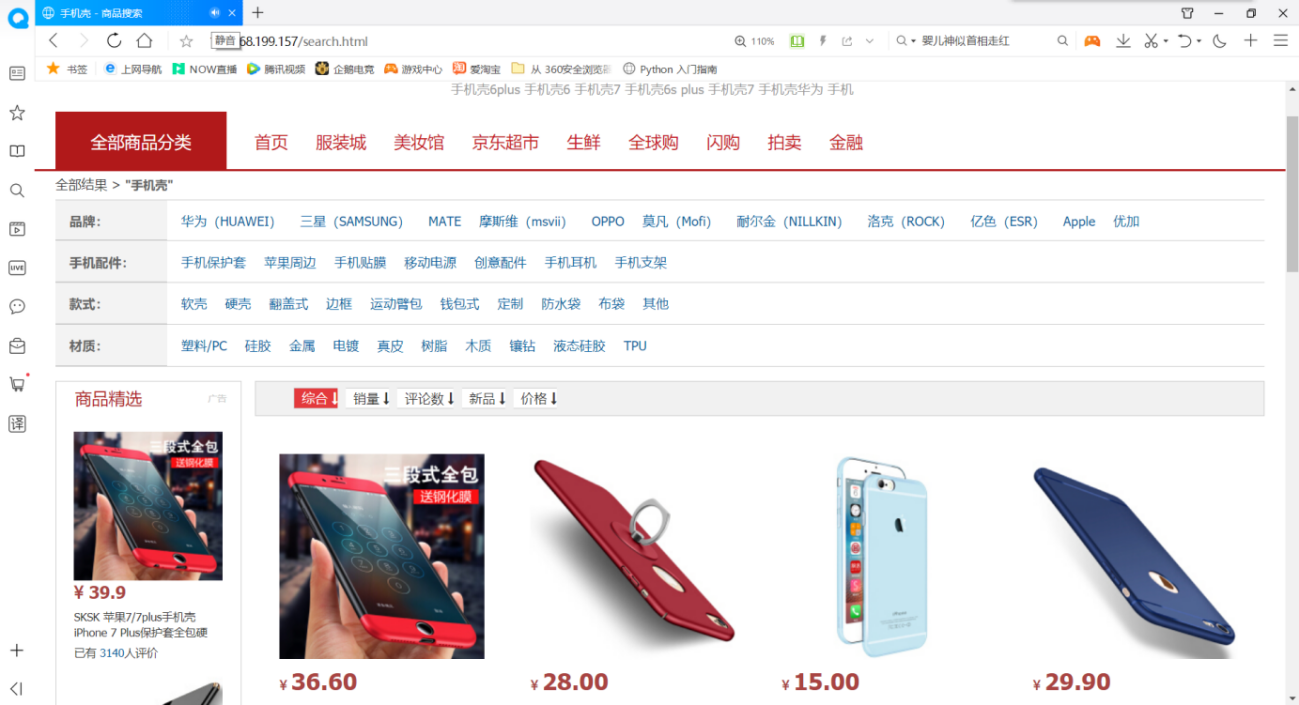
服务器对第一个 HTTP GET 请求报文的响应（状态码和短语）是401 Unauthorized

在这个响应报文中出现了WWW-Authenticate字段用来进行身份验证的，在登录成功后，在后续的HTTP GET请求报文中，会出现Authorization字段将用户名:密码 采用base64编码来传输。

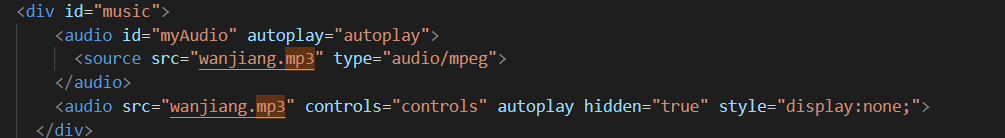
，登录成功后服务器会返回状态码和短语200 OK来成功访问该HTML文件，

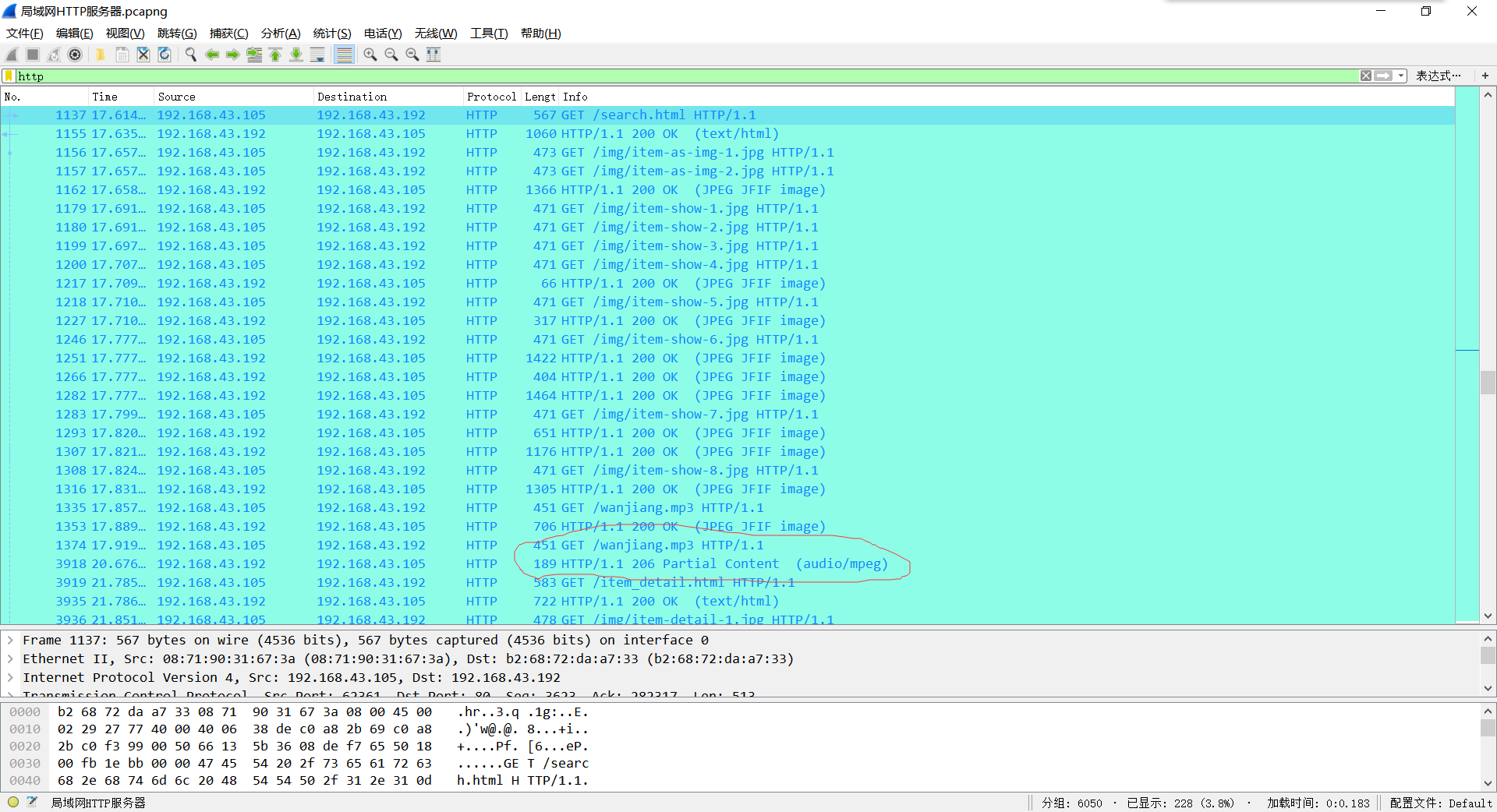
然后客户会接着Get修饰界面的css文件、控制页面逻辑的js文件和修改字体、字体图标相关的资源fonts文件以及文本、图片包，在经过TCP传输数据后，服务器都会返回OK，初始页面加载成功，能够正常访问

1. 接着进入search页面，此时就是访问IIS服务器上部署的search.html文件



为了页面更加优化，在源代码里面加入了调用音频的字段





根据抓包结果，能够捕捉到客户发给服务器相应的HTML文件的请求包，并且也捕捉到响应的服务器返回给客户的包，根据相应包的Content-Type可以判断返回的为哪种类型的包，除了一些基础的图片包外，也捕捉到了音频的包，对应的audio音频类型包。

（在跳转到search页面后，由于它是从index077.html页面跳转过来的，所以会有一个字段

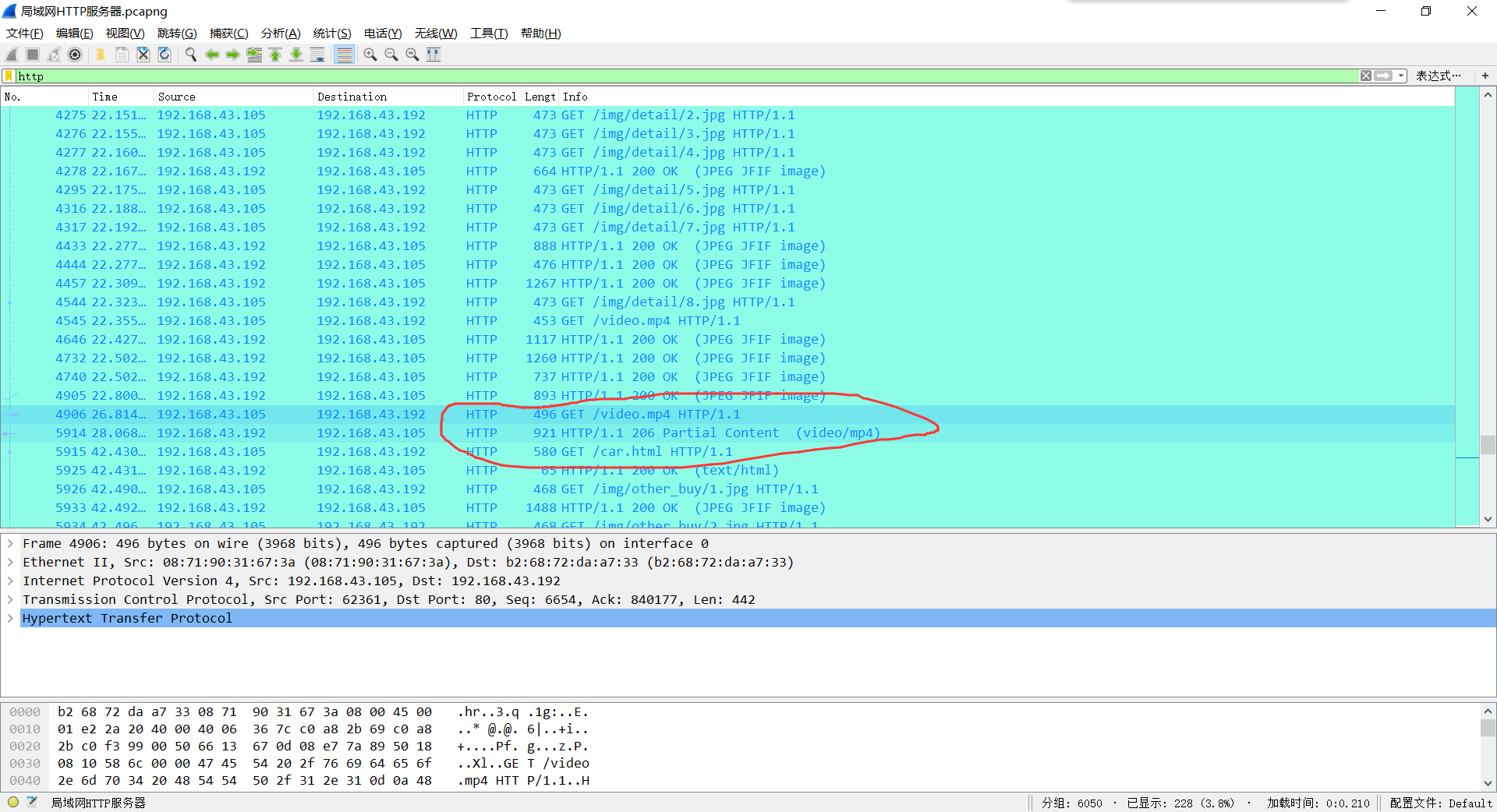
，里面的URL指客户是从该URL代表的页面出发访问当前请求页面的）。

1. 接着再进入item\_detail.html页面



为了页面更加优化，在源代码里面加入了调用视频的字段





根据抓包结果，能够捕捉到客户发给服务器相应的HTML文件的请求包，并且也捕捉到响应的服务器返回给客户的包，根据Content-Type可以判断返回的为哪种类型的包，除了一些基础的图片包外，也捕捉到了该视频的包，对应的video视频类型包。

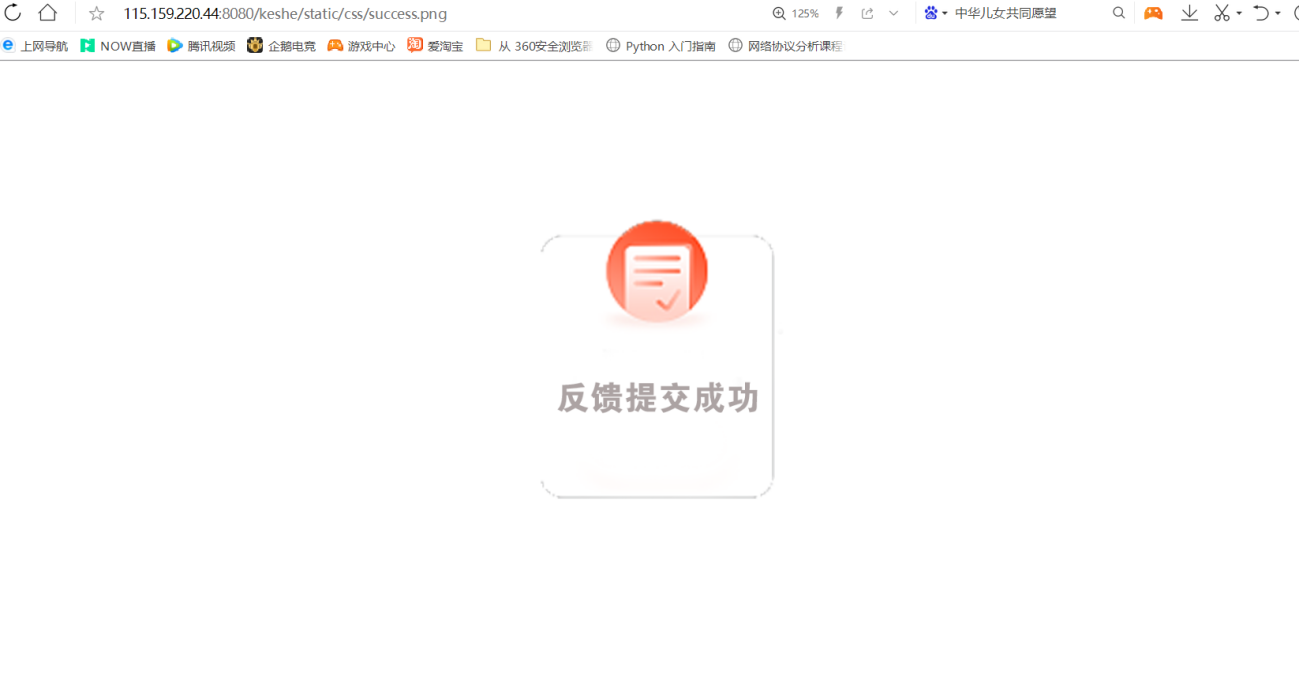
服务器返回的状态码为206，状态短语为Partial Content，断点续传，比如我点击视频播放按钮后，然后拖动视频条，拖动到一个节点上，然后这一段数据发送完毕后就会返回一个206的响应报文来说明发送了部分内容。

1. 在feedback页面，加入以下代码，表单方法为POST，POST请求到

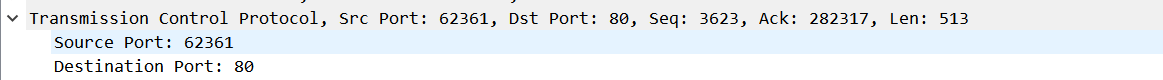
http://115.159.220.44:8080/keshe/static/css/success.png这个页面提交按钮设置为submit，以此实现POST请求方法



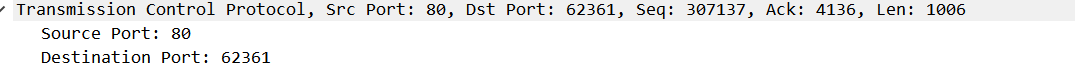




7.观察任意一个请求报文，都能在TCP头部里面可以看到目的端口为80，

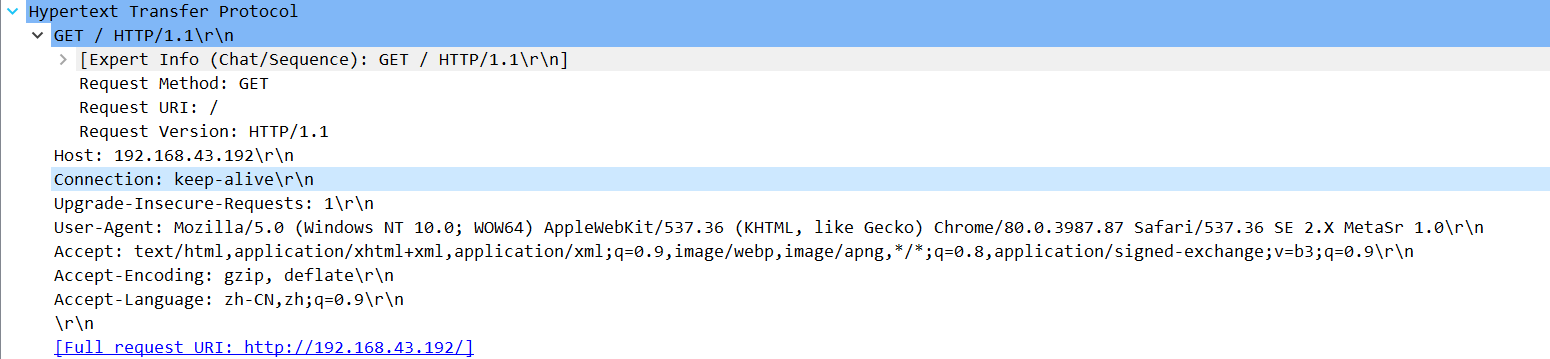


观察任意一个响应报文，都能在TCP头部里面可以看到源端口为80，



说明服务器是通过80号端口进行HTTP报文交互

8.观察客户发给服务器的第一个请求报文

在请求行里会说明请求的方法为GET，Request URI会说明访问的路径，请求版本为HTTP 1.1

Host：客户端指定自己想访问的HTTP服务器的域名/IP 地址和端口号，这边的域名就为192.168.43.192

HTTP Upgrade-Insecure-Requests ：请求头向服务器发送一个客户端对HTTPS加密和认证响应良好，并且可以成功处理的信号，可以请求所属网站所有的HTTPS资源，chrome(谷歌浏览器)会在http请求中加入 ‘Upgrade-Insecure-Requests: 1’ ，服务器收到请求后会返回 “Content-Security-Policy: upgrade-insecure-requests” 头，告诉浏览器，可以把所属本站的所有 http 连接升级为 https 连接

Connection：表示是否需要持久连接，Keep-alive就是保持持久连接

User-Agent：HTTP客户端运行的浏览器类型的详细信息。通过该头部信息，web服务器可以判断到当前HTTP请求的客户端浏览器类别

Accept：指定客户端能够接收的内容类型，内容类型中的先后次序表示客户端接收的先后次序

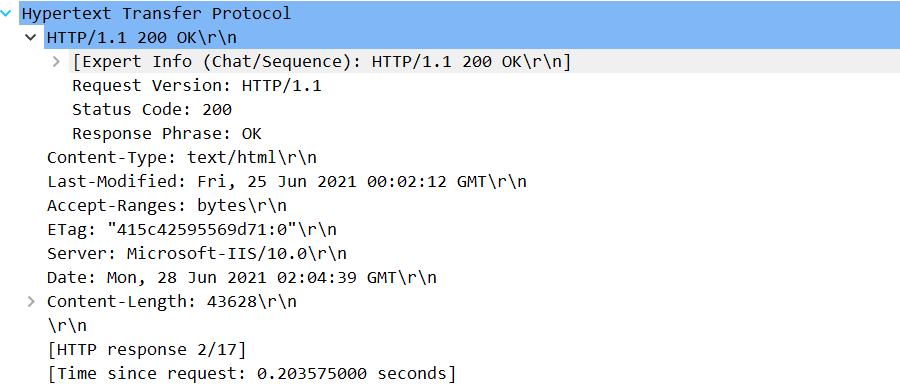
Accept-Encoding：指定客户端浏览器可以支持的web服务器返回内容压缩编码类型。表示允许服务器在将输出内容发送到客户端以前进行压缩，以节约带宽。而这里设置的就是客户端浏览器所能够支持的返回压缩格式

Accept-Language：

指定HTTP客户端浏览器用来展示返回信息所优先选择的语言

URI：

9.观察服务器发给客户的第一个OK响应报文，有个Server字段，显示的是web服务器软件名称版本，所以会显示使用的服务器为MIcrosoft-IIS/10.0



HTTP响应报文的状态行会说明请求版本为HTTP 1.1，状态码为200，状态短语为OK

Content-Type：返回内容为text类型

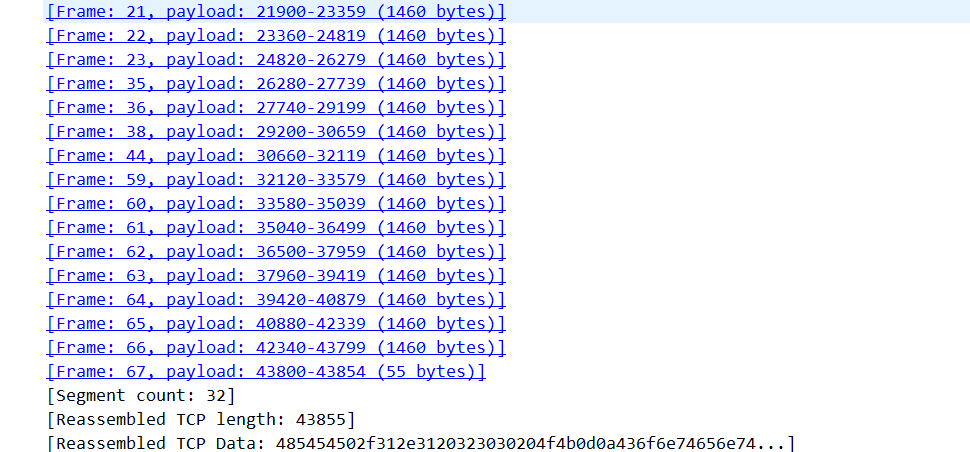
Last-Modified：请求资源的最后修改时间为2021年6月25日（星期五）0时02分12秒

Accept-Ranges ：表明服务器是否支持指定范围请求及哪种类型的分段请求，该报文支持字节类型

ETag：资源的标记信息

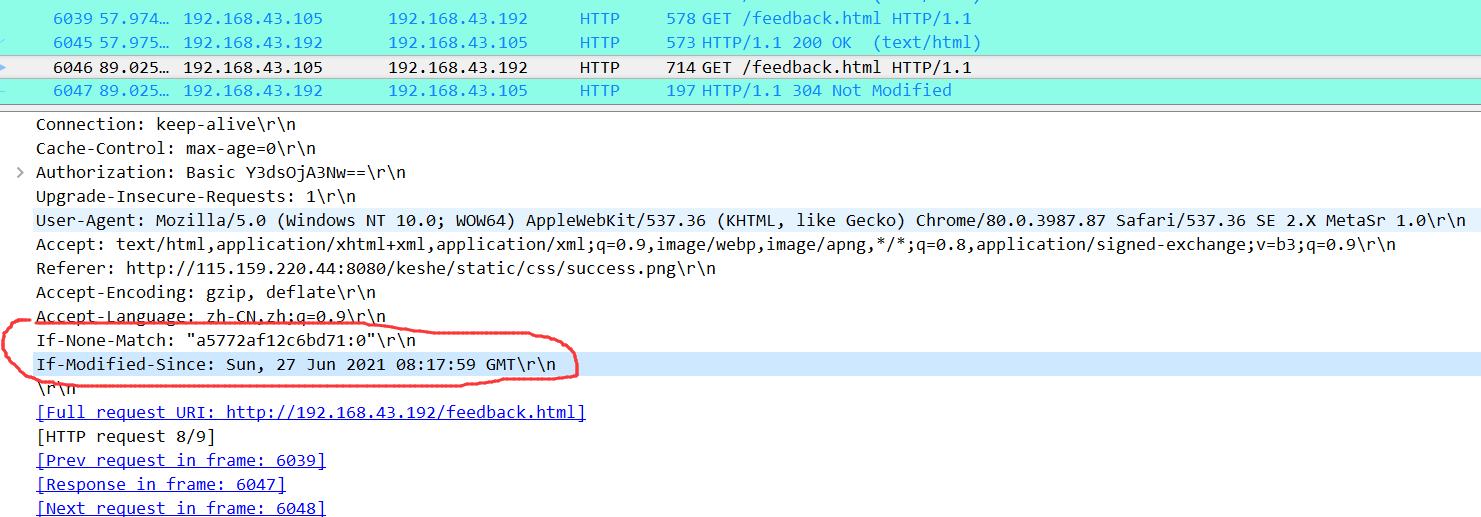
Date：服务器消息发出的时间为2021年6月28日（星期一）02时04分39秒

Content-Length：用于描述HTTP消息实体的长度，为43628字节



根据分片总长度为43855，所以HTTP头部长度为43855-43628=227

10.在这次的抓包过程中，为了检验一下If-Modified-Since、If-None-Match字段的作用，在feedback.html页面，快速地点一下刷新，此时就会有新的一个Get请求报文，里面就会有这两个字段，



IF-MODIFIED-SINCE是一个条件式请求首部，服务器只在所请求的资源在给定的日期时间之后对内容进行过修改的情况下才会将资源返回，这个值是来自于上一次该服务器发给客户的HTTP响应报文的Last-Modified字段

If-None-Match类似于指纹标记，如果该标记不一样，说明文档发生了改变，这个值是来自于上一次该服务器发给客户的HTTP响应报文的Etag字段



服务器会根据页面刷新后Get到的新一次http请求报文IF-MODIFIED-SINCE、If-None-Match的值看文档是否有发生改变，如果文档没有改变，就响应一个304 Not Modified不带消息主题的包，说明资源没有被改变，就不需要将数据再发一次，以便节省流量

## 3.2 深入理解HTTP协议

### 3.2.1 常用HTTP方法

|  |  |  |
| --- | --- | --- |
| 方法 | 说明 | 是否包含主体 |
| GET | 从服务器获取一份文档 | 否 |
| POST | 向服务器发送需要处理的数据（被包含在主题中） | 是 |
| HEAD | 从服务器获取一个文档的首部 | 否 |
| PUT | 把数据存储在服务器 | 是 |
| DELETE | 从服务器上删除一份文档 | 否 |
| OPTIONS | 询问服务器支持哪些方法 | 否 |
| TRACE | 对可能经过代理传送到服务器上的报文进行追踪 | 否 |

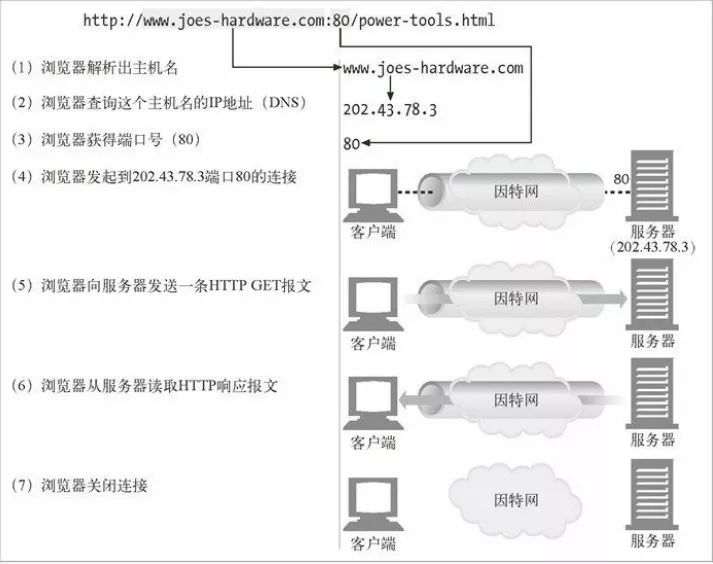
### 3.2.2 POST和GET方法的区别

|  |  |  |
| --- | --- | --- |
| 比较 | GET | POST |
| 请求参数的区别 | 把请求参数拼接在URL后面，以？分隔，多个参数之间用&连接；如果是英文或数字，原样发送，如果是空格或中文，则用Base64编码 | 把提交的数据放在请求主体中，不会在URL中显示出来 |
| 传输数据的大小 | 浏览器和服务器会限制URL的长度，一般是2K | 可以传输较大量的数据 |
| 安全性 | 请求参数在URL后面，可以直接看到，尤其是登录时，如果登录界面被浏览器缓存，其他人就可以通过查看历史记录，拿到账户和密码 | 请求参数在请求主题中传输，无法直接拿到，相对GET安全性较高；但是通过抓包工具，还是可以看到请求参数的 |

### 3.2.2 常见HTTP响应

|  |  |  |
| --- | --- | --- |
| 状态码 | 短语 | 含义 |
| 200 | OK | 请求没有问题，主体部分包含所请求数据 |
| 206 | Partial Content | 部分请求成功，断点续传 |
| 301 | Permanently Moved | 请求的URL已被移除，响应报文中的Location首部包含新URL |
| 302 | Temporarily Moved | 与301类似，代表暂时性转移 |
| 304 | Not Modified | 客户端有缓存文档，并发出了一个条件性请求时，服务器高速客户端原来缓存的文档还可以继续使用 |
| 404 | Not Found | 服务器无法找到客户所请求的资源 |
| 500 | Internal Server Error | 服务器发生内部错误，无法完成请示 |

### 3.2.3 HTTP工作原理



# 4 基于互联网的HTTP报文交互

## 4.1 内网穿透技术

### 4.1.1 内网穿透技术简介

内网穿透即NAT穿透，网络连接时术语，计算机是局域网内时，外网与内网的计算机节点需要连接通信，就会出现不支持内网穿透。内网穿透是将内网IP地址和端口映射到公网，可以将内网地址转化变为公网地址，并且拥有一个外网域名。

### 4.1.2 NAT实现方式

NAT的实现方式有三种，即静态转换Static Nat、动态转换Dynamic Nat和端口多路复用OverLoad。

**[静态](https://baike.baidu.com/item/%E9%9D%99%E6%80%81" \t "https://baike.baidu.com/item/nat/_blank)转换**是指将内部网络的私有IP地址转换为公有IP地址，IP地址对是一对一的，是一成不变的，某个私有IP地址只转换为某个公有IP地址。借助于[静态](https://baike.baidu.com/item/%E9%9D%99%E6%80%81" \t "https://baike.baidu.com/item/nat/_blank)转换，可以实现外部网络对内部网络中某些特定设备（如服务器）的访问。

**动态转换**是指将内部网络的私有IP地址转换为公用IP地址时，IP地址是不确定的，是随机的，所有被授权访问上Internet的私有IP地址可随机转换为任何指定的合法IP地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址时，就可以进行动态转换。动态转换可以使用多个合法外部地址集。当[ISP](https://baike.baidu.com/item/ISP/10152" \t "https://baike.baidu.com/item/nat/_blank)提供的合法IP地址略少于网络内部的计算机数量时。可以采用动态转换的方式。

**端口多路复用（Port address Translation,PAT）**是指改变外出数据包的[源端口](https://baike.baidu.com/item/%E6%BA%90%E7%AB%AF%E5%8F%A3" \t "https://baike.baidu.com/item/nat/_blank)并进行端口转换，即端口[地址转换](https://baike.baidu.com/item/%E5%9C%B0%E5%9D%80%E8%BD%AC%E6%8D%A2" \t "https://baike.baidu.com/item/nat/_blank)（PAT，Port Address Translation).采用端口多路复用方式。内部网络的所有[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "https://baike.baidu.com/item/nat/_blank)均可共享一个合法外部IP地址实现对Internet的访问，从而可以最大限度地节约IP地址资源。同时，又可隐藏网络内部的所有[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "https://baike.baidu.com/item/nat/_blank)，有效避免来自internet的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

## 4.2 Ngrok的使用

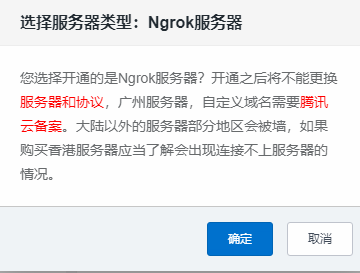
### 4.2.1 原理

内网穿透是在本地电脑和一个有公网的服务器之间建立连接，通过访问公网服务器的域名就可以访问到本地电脑上的服务，目前有Utools，frp，花生壳，ngrok等开源或收费软件可以进行内网穿透。

Sunny-Ngrok内网穿透原理：将用户的IP地址和端口号映射成外网的一个IP地址，**通过建立隧道与云服务器建立映射关系，这就相当于打破了局域网的限制。穿过限制，访问内网服务。**

### 4.2.2服务器域名的配置

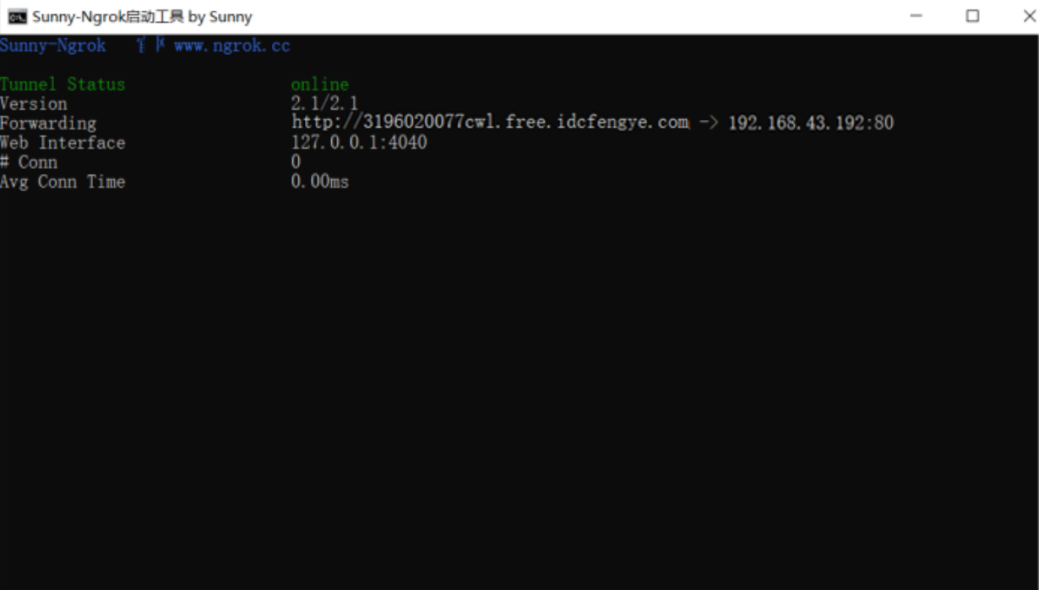
1. 在Sunny-Ngrok上选择服务器类型



1. 选择http类型，将自己的IP地址和端口号与外网域名建立起映射



1. 在服务器主机上打开Sunny-Ngrok启动工具，输入建立的隧道号，开启内网穿透

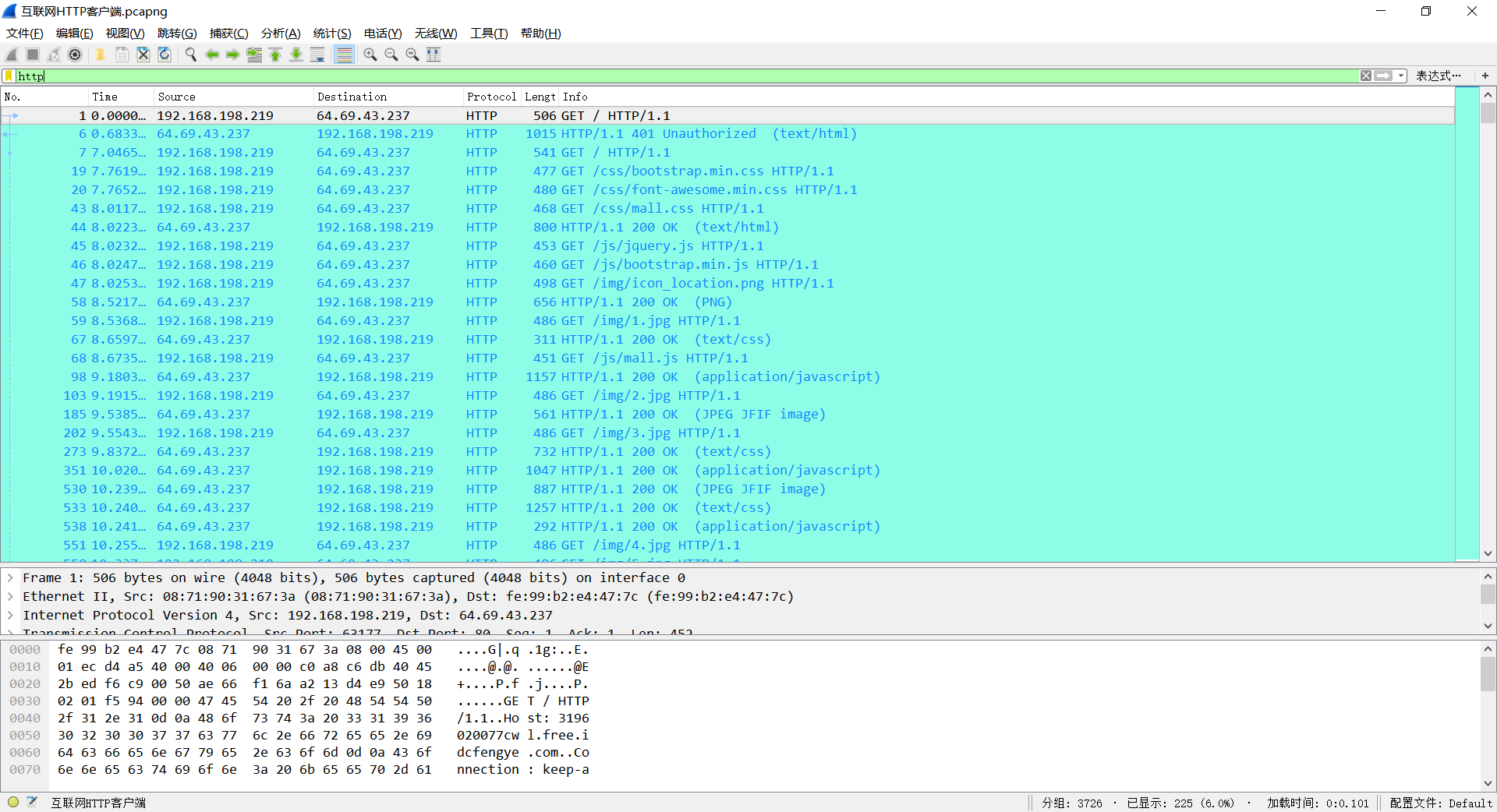


1. 内网穿透成功，能够用外网域名访问到该服务器的资源文件



## 4.3 互联网下HTTP协议报文分析

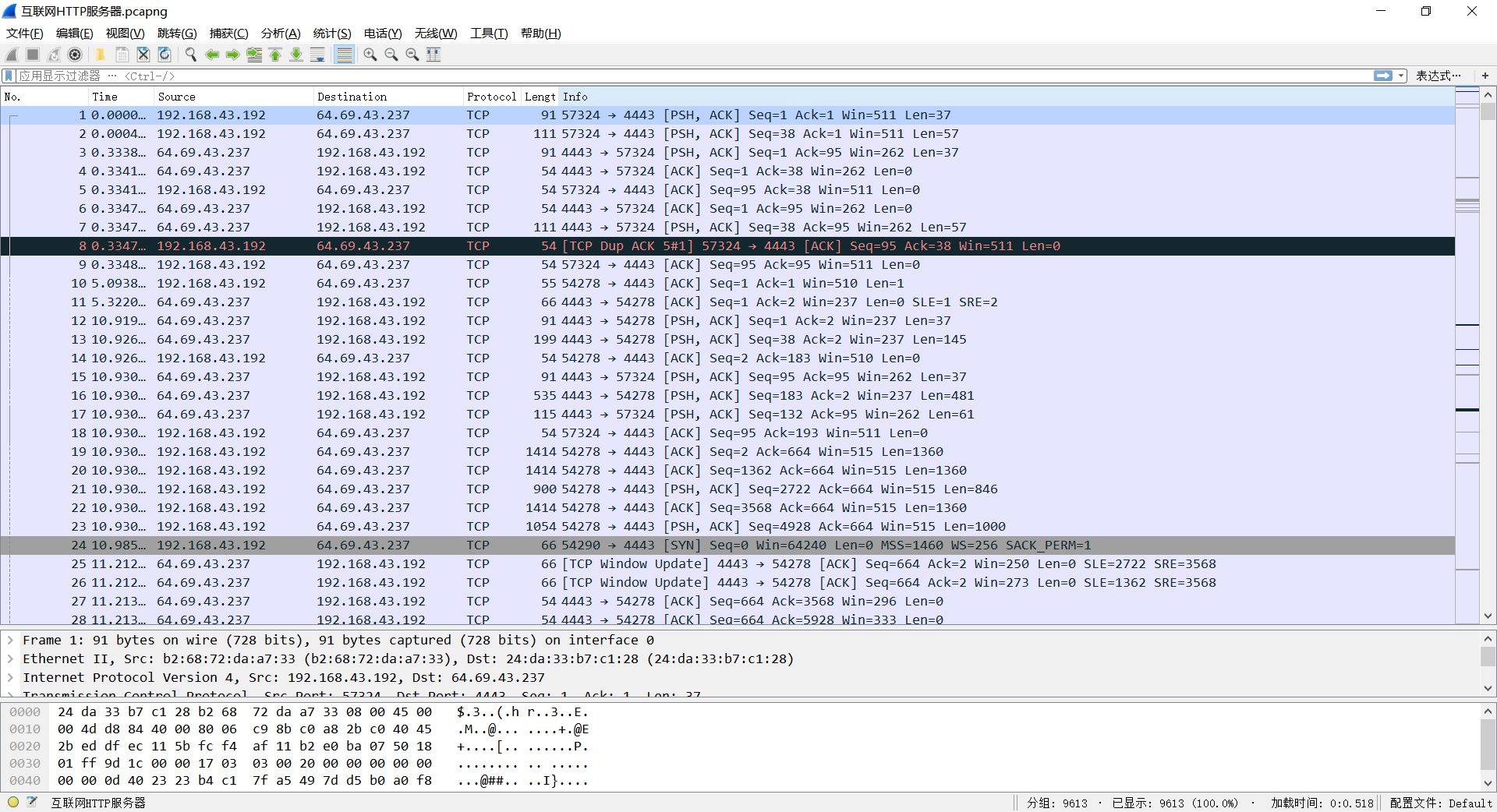
### 4.3.1 客户端报文情况



由于IP地址为192.168.198.219的客户机与服务器（本机）处于不同的局域网，所以并不能直接访问。开启内网穿透后，将服务器地址和端口与外网域名建立映射，可以通过已经建立起映射的URL进行访问。

在互联网的HTTP报文交互过程中，与局域网的HTTP报文交互过程不同的是服务器的地址变成了64.69.43.237，因为进行了内网穿透，所以该地址为云服务器的地址。其余与局域网的HTTP报文交互情况相同，都是客户先发送HTTP请求，接着服务器通过TCP传输数据，再返回HTTP响应。

### 4.3.2 服务器报文情况



在wireshark上只能抓到与云服务器地址交互的TCP包，因为客户的HTTP请求是发送给了云服务器64.69.43.237上，也是云服务器与客户机进行HTTP报文交互，但是云服务器只是与本地Web服务器建立一个映射关系，HTML资源依然在本地服务器上，云服务器并没有这些资源，所以需要本地服务器将HTML资源传送到云服务器上，所以云服务器与本地服务器为TCP报文交互

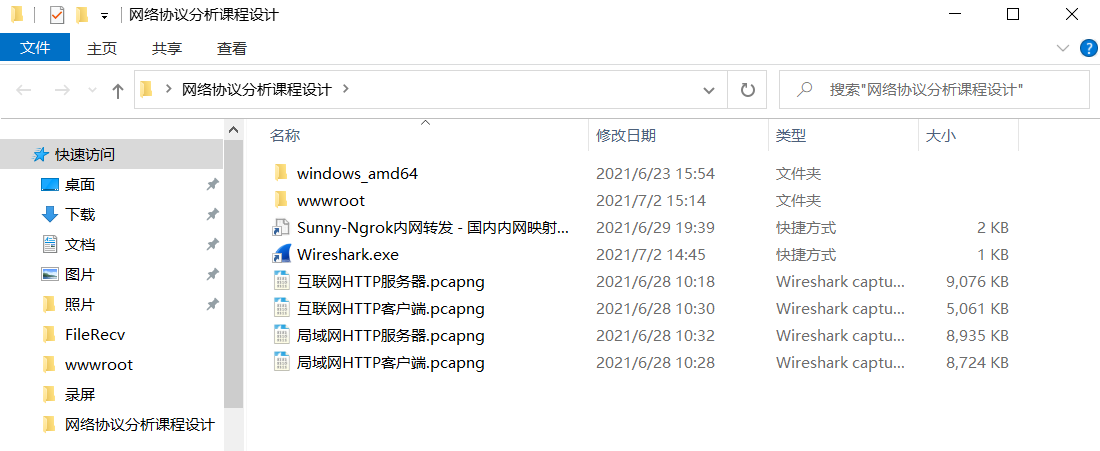
# 5 结束语

最初，自己做好了ARP欺骗和DHCP服务器，但是最后还是选择一个更感兴趣的Web服务器的配置与管理。当选定Web服务器的配置与管理这门课程设计之前，我就尝试搭建了IIS服务器，然后也尝试一些简单的HTTP报文交互，然后激起了想选这门课设的兴趣。在实验过程中，让我了解到了Web服务器的重要性，让我知道了客户如何访问到网页资源，以及IIS服务器的一些功能，比如身份验证等。接着在部署相关文件资源时，也学习到了一些简单的HTML语言来编写HTML文件。

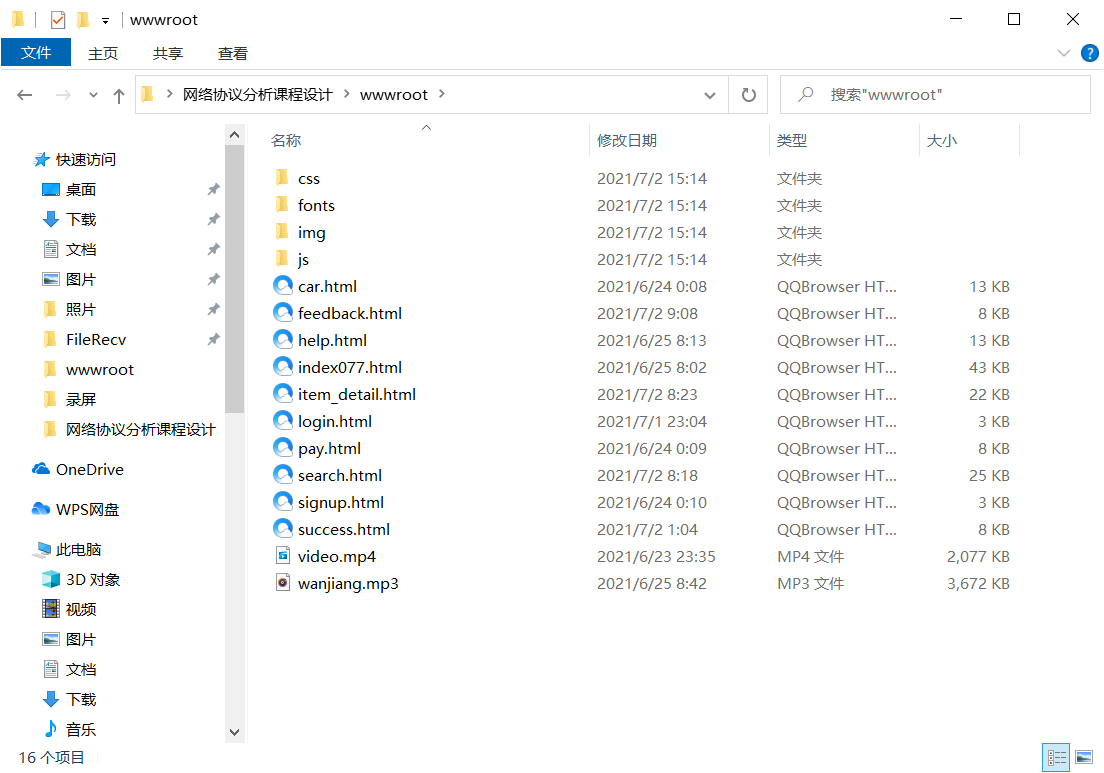
接着在抓包过程中也能够抓到我部署的HTML文件资源信息，能够正确获取到我部署的文件类型，也更加理解了HTTP报文的请求和响应交互，包括一些请求方法和响应码。接着在设置为Internet访问的时候，在之前就有了解过内网穿透的概念，但是一直都没有尝试过，所以通过课程设计，让我使用了内网穿透来建立起内网和外网的映射，从而能够让外网来访问我部署的HTML文件资源，但是在实验过程中，遇到过内网穿透插件不能用或者崩溃的情况下，所以筛选了很多款内网穿透的插件，最后决定使用sunny-Ngrok。

在懂得如何搭建和管理Web服务器后，以后在日常生活中可以自己写一点HTML文件并且部署在服务器上，在设置Internet访问后，能够让大家进行访问与学习。

# 6 附件清单



1. Windows\_amd64文件夹里存放内网穿透ngrok的启动工具，用来输入隧道号开启内网穿透
2. wwwroot文件夹存放在IIS服务器根目录的HTML相关资源文件



1. Sunny-Ngrok内网转发 - 国内内网映射服务器为ngrok的网页版，需要在里面登录进行配置映射信息，以及查看隧道号
2. Wireshark.exe为本次使用的抓包软件
3. 接下来为基于局域网和互联网的HTTP交互报文