## MIME

是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。多用于指定一些客户端自定义的文件名，以及一些媒体文件打开方式。

### 浏览器输入url回车以后发生了什么？

#### 解析URL

Universal Resource Locator）：统一资源定位符。俗称网页地址或者网址。 

#### DNS 解析

当在浏览器中输入URL后，浏览器首先对拿到的URL进行识别，抽取出域名字段 在进行DNS解析时，会经历以下步骤： 1. 查询**浏览器缓存**（浏览器会缓存之前拿到的DNS 2-30分钟时间），如果没有找到， 2. 检查**系统缓存**，检查hosts文件，这个文件保存了一些以前访问过的网站的域名和IP的数据。它就像是一个本地的数据库。如果找到就可以直接获取目标主机的IP地址了。没有找到的话，需要 3. 检查**路由器缓存**，路由器有自己的DNS缓存，可能就包括了这在查询的内容；如果没有，要 4. 查询ISP DNS 缓存：ISP服务商DNS缓存（**本地服务器缓存**）那里可能有相关的内容，如果还不行的话，需要， 5. 递归查询：从 **根域名** 服务器到**顶级域名**服务器再到**极限域名**服务器依次搜索哦对应目标域名的IP。

#### 浏览器与网站建立TCP连接(三次握手)

通过三次握手，建立了客户端和服务器之间的连接，现在可以请求和传输数据了。

#### 通过Get请求和传输数据

通过这种GET请求，和服务器的响应。可以将服务器上的目标文件传输到浏览器进行渲染。

#### 渲染界面

客户端拿到服务器端传输来的文件，找到HTML和MIME文件，通过MIME文件，浏览器知道要用页面渲染引擎来处理HTML文件。 ａ.浏览器会解析html源码，然后创建一个 DOM树。 在DOM树中，每一个HTML标签都有一个对应的节点，并且每一个文本也都会有一个对应的文本节点。 b.浏览器解析CSS代码，计算出最终的样式数据，形成css对象模型CSSOM。 首先会忽略非法的CSS代码，之后按照浏览器默认设置——用户设置——外链样式——内联样式——HTML中的style样式顺序进行渲染。 c.利用DOM和CSSOM构建一个渲染树（rendering tree）。 渲染树和DOM树有点像，但是是有区别的。 DOM树完全和html标签一一对应，但是渲染树会忽略掉不需要渲染的元素，比如head、display:none的元素等。 而且一大段文本中的每一个行在渲染树中都是独立的一个节点。 渲染树中的每一个节点都存储有对应的css属性。 ｄ.浏览器就根据渲染树直接把页面绘制到屏幕上。

### HTTP与HTTPS的区别

超文本传输协议HTTP 安全套接字层超文本传输协议HTTPS

* HTTP协议以明文方式发送内容，不提供任何方式的数据加密
* 为了数据传输的安全，HTTPS在HTTP的基础上加入了SSL协议
  + SSL依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。

#### HTTPS和HTTP的区别主要如下：

1. https协议需要到ca申请证书，一般免费证书较少，因而需要一定费用。
2. http是超文本传输协议，信息是明文传输，https则是具有安全性的ssl加密传输协议。
3. http和https使用的是完全不同的连接方式，用的端口也不一样，前者是80，后者是443。
4. http的连接很简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，比http协议安全。

#### HTTPS的优点

　　尽管HTTPS并非绝对安全，掌握根证书的机构、掌握加密算法的组织同样可以进行中间人形式的攻击，但HTTPS仍是现行架构下最安全的解决方案，主要有以下几个好处： 1. 使用HTTPS协议可认证用户和服务器，确保数据发送到正确的客户机和服务器； 2. HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，要比http协议安全，可防止数据在传输过程中不被窃取、改变，确保数据的完整性。 3. HTTPS是现行架构下最安全的解决方案，虽然不是绝对安全，但它大幅增加了中间人攻击的成本。 4. 谷歌曾在2014年8月份调整搜索引擎算法，并称“比起同等HTTP网站，采用HTTPS加密的网站在搜索结果中的排名将会更高”。

#### HTTPS的缺点

虽然说HTTPS有很大的优势，但其相对来说，还是存在不足之处的： 1. HTTPS协议握手阶段比较费时，会使页面的加载时间延长近50%，增加10%到20%的耗电； 2. HTTPS连接缓存不如HTTP高效，会增加数据开销和功耗，甚至已有的安全措施也会因此而受到影响； 3. SSL证书需要钱，功能越强大的证书费用越高，个人网站、小网站没有必要一般不会用。 4. SSL证书通常需要绑定IP，不能在同一IP上绑定多个域名，IPv4资源不可能支撑这个消耗。 5. HTTPS协议的加密范围也比较有限，在黑客攻击、拒绝服务攻击、服务器劫持等方面几乎起不到什么作用。最关键的，SSL证书的信用链体系并不安全，特别是在某些国家可以控制CA根证书的情况下，中间人攻击一样可行。