实验目标：

使用 tcpdump 开源软件对在本机上访问 www.tianya.cn 网站过程进行嗅探，回答问题：你在访问 www.tianya.cn 网站首页时，浏览器将访问多少个 Web 服务器？他们的 IP 地址都是什么？

下面给出解决方案的一个示例：

实验环境：

实验机器：个人笔记本电脑;
操作系统：Ubuntu10.04;
使用工具：Tcpdump;
网络环境：中国联通网络;

实验步骤：

1.在命令行终端运行 Tcpdump,命令行如下

tcpdump –n src *主机 IP* and tcp port 80 and "tcp[13] & 18 == 2"

该命令表示捕获所有由主机发出的，SYN 位置 1，ACK 位置 0 的，发往 80 端口（HTTP）数据包。
其中 TCP[13]即 TCP 包的第 13 字节（从第 0 字节开始计）内容，根据 TCP 包的头部数据格式，这一字节的内容包含了八个标志位，内容如下：

Reserved	Reserved	URG	ACK	PSH	RST	SYN	FIN

由于 18 = 00010010B,因此数字 18 表示 ACK 位和 SYN 位为 1，将 TCP 包的第 13 字节内容同数字 18“与（&）”的结果就得到了 ACK 位和 SYN 位的信息。如果结果为 2 说明数据包中 ACK 位为 0 而 SYN 位为 1，因此表达式”tcp[13] & 18 == 2”筛选得到的是所有 SYN 但非 ACK 包，这正是建立连接请求（“三次握手”的第一步）产生的数据包。

2.打开浏览器，输入网址 www.tianya.cn，等待网页载入完成。

3.记录监听结果，进行分析

```
root@ubuntu:~$ sudo tcpdump src 172.24.7.44 -n and tcp port 80 and "tcp[13] & 18 ==2 "
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
20:05:32.222460 IP 172.24.7.44.54019 > 221.11.172.154.80: Flags [S], seq 2616781153, win
5840, options [mss 1460,sackOK,TS val 239642 ecr 0,nop,wscale 6], length 0
20:05:32.488272 IP 172.24.7.44.34524 > 221.11.172.200.80: Flags [S], seq 2627534613, win
5840, options [mss 1460,sackOK,TS val 239708 ecr 0,nop,wscale 6], length 0
20:05:32.488548 IP 172.24.7.44.34527 > 221.11.172.200.80: Flags [S], seq 2623873328, win
5840, options [mss 1460,sackOK,TS val 239708 ecr 0,nop,wscale 6], length 0
20:05:32.650325 IP 172.24.7.44.57863 > 221.11.172.192.80: Flags [S], seq 2619790355, win
5840, options [mss 1460,sackOK,TS val 239749 ecr 0,nop,wscale 6], length 0
```

```
20:05:33.292829 IP 172.24.7.44.34530 > 221.11.172.200.80: Flags [S], seq 2626466448, win
5840, options [mss 1460,sackOK,TS val 239909 ecr 0,nop,wscale 6], length 0
20:05:33.293369 IP 172.24.7.44.34531 > 221.11.172.200.80: Flags [S], seq 2638497144, win
5840, options [mss 1460,sackOK,TS val 239909 ecr 0,nop,wscale 6], length 0
20:05:33.458112 IP 172.24.7.44.47005 > 221.11.172.221.80: Flags [S], seq 2643772242, win
5840, options [mss 1460,sackOK,TS val 239951 ecr 0,nop,wscale 6], length 0
20:05:33.463216 IP 172.24.7.44.46868 > 221.11.172.224.80: Flags [S], seq 2645395346, win
5840, options [mss 1460,sackOK,TS val 239952 ecr 0,nop,wscale 6], length 0
20:05:33.553738 IP 172.24.7.44.53072 > 221.11.172.158.80: Flags [S], seq 2646934061, win
5840, options [mss 1460,sackOK,TS val 239974 ecr 0,nop,wscale 6], length 0
20:05:34.152237 IP 172.24.7.44.34536 > 221.11.172.200.80: Flags [S], seq 2640967987, win
5840, options [mss 1460,sackOK,TS val 240124 ecr 0,nop,wscale 6], length 0
20:05:34.154306 IP 172.24.7.44.34537 > 221.11.172.200.80: Flags [S], seq 2648390403, win
5840, options [mss 1460,sackOK,TS val 240125 ecr 0,nop,wscale 6], length 0
20:05:34.160251 IP 172.24.7.44.53078 > 221.11.172.158.80: Flags [S], seq 2646600433, win
5840, options [mss 1460,sackOK,TS val 240126 ecr 0,nop,wscale 6], length 0
20:05:34.238136 IP 172.24.7.44.59288 > 221.11.172.220.80: Flags [S], seq 2644935839, win
5840, options [mss 1460,sackOK,TS val 240146 ecr 0,nop,wscale 6], length 0
20:05:34.445542 IP 172.24.7.44.48822 > 221.11.172.170.80: Flags [S], seq 2657466785, win
5840, options [mss 1460,sackOK,TS val 240197 ecr 0,nop,wscale 6], length 0
20:05:34.491663 IP 172.24.7.44.54987 > 221.11.172.160.80: Flags [S], seq 2659551422, win
5840, options [mss 1460,sackOK,TS val 240209 ecr 0,nop,wscale 6], length 0
20:05:35.977907 IP 172.24.7.44.54046 > 221.11.172.154.80: Flags [S], seq 2673789818, win
5840, options [mss 1460,sackOK,TS val 240580 ecr 0,nop,wscale 6], length 0
```

其中某些 IP 地址进行了多次连接，总计访问到的地址整理如下：

221.11.172.154
221.11.172.200
221.11.172.192
221.11.172.221
221.11.172.224
221.11.172.158
221.11.172.170
221.11.172.160

每次连接实验得到的结果不完全相同，但都会连接到 221.11.172.xxx 这个网段，查询 IP 地址该网段来自：海南省海口市 联通

使用 whois 查询可以知道 tianya.cn 这个域名的一些信息：

域名所有者　海南天涯在线网络科技有限公司

注：一些比较简洁的网页如 GOOGLE，百度等监听结果会比较简单且相对稳定.