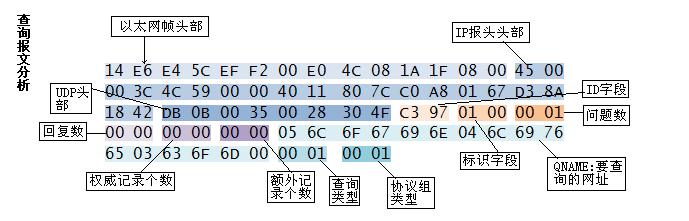
**应用协议报文分析**

[**DNS报文分析**](http://www.cnblogs.com/feng-qi/archive/2013/05/05/DNS_packet_analysis.html)

所查询的网址为 login.live.com 。

首先是对查询报文的分析



以太网帧头部、IP报头头部和UDP头部略去，从ID字段开始。

ID字段：ID字段就是对报文的一个编号，没有太多的含义。

标识字段：格式如下，下方数字表示bit个数，



        对于本报文来说就是0x0100，即 0 0000 0 0 1 0 000 0000 .

       QR：0表示查询报文，1表示响应报文  
       Opcode：通常值为0（标准查询），其他值为1（反向查询）和2（服务器状态请求）  
       AA：表示授权回答（authoritative answer）  
       TC：表示可截断的（truncated）  
       RD：表示期望递归  
       RA：表示可用递归  
       随后3bit为保留字段, 必须为0  
       Rcode：返回码，通常为0（没有差错）和3（名字差错）

问题数：此例中为1

回复数：此例中为0，因为是查询报文，自然没有回复。

权威记录个数：域名DNS分两种，一种是权威域名服务器，域名注册商的服务器都为权威域名服务器；另一种就是缓存DNS服务器，比如各地ISP上网设置的DNS服务器，它的作用主要是把域名解析结果缓存到本地，方便你查询。还是因为是查询报文，本例中也为0.

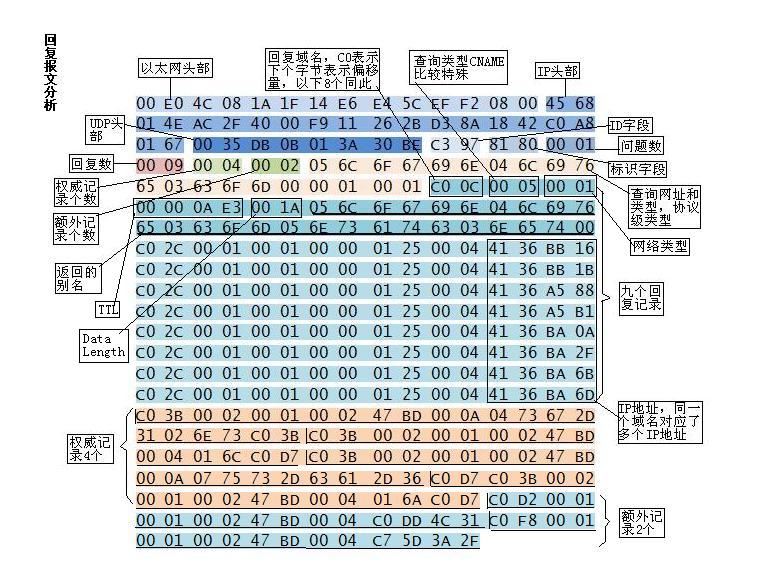
额外记录个数：一些额外的记录，具体是什么，我也不太清楚。本例为0，原因同上。

QNAME 地址字段：要查询的网址。地址是变长的字符串，格式为第一个字节为长度，后跟字符，以0结尾。

查询类型：此外为0001，表示为A类查询。

协议组类型：0001表示网络类型为Internet。

然后是对回复报文的分析



ID字段、标识字段、问题数、回复数、权威记录个数、额外记录个数等同上。

回复记录：此处共回复了9个记录，由回复数记录可以看出来。地址字段 0xC0 开头表示下一个字节表示在本报文中的偏移量。这也是为了消除冗余，减小报文长度。第一个回复中类型为 0x0005 ，表示类型为CNAME，相当于用子域名来代替ip地址。这样做的优点是如果ip地址变化，只需要改动子域名的解析，而不需要逐一改变ip地址解析。回复的域名为 login.live.com.nsatc.net ，后面8个记录都是这个域名的IP地址（一个域名对应几个IP地址对这样的大网站来说很平常）。

网络类型同查询报文中的一样都是Internet。

TTL：Time To Live，生存时间，域名DNS的TTL值表示各地的DNS缓存服务器多久去你的权威域名解析服务器（NS)获取一次你域名的解析IP。单位是分钟。

Data Length：数据长度，表示本记录从下个字节起还有多少字节。

返回数据：这就是我们想要的。一般为IP地址，但本记录类型为CNAME，所以返回了一个域名，下面8个都是IP地址。

权威记录：权威记录、查询、回答的格式都是一样的。4条记录的类型都是 0x0002 （表示类型为NS，对应于查询中的A类型）。NS表示 Name Server，权威记录回复的应该是本区域的权威域名服务器的域名（我也不是很确定）。

额外记录：本例中回复的是权威域名服务器的IP地址。

# [应用层协议FTP、DNS协议、HTTP协议分析](http://www.cnblogs.com/leftshine/p/5698890.html)

分析所用软件下载：[Wireshark-win32-1.10.2.exe](https://pan.baidu.com/s/1pLH6gUB)

一．分析工作

1．分析FTP协议

2．分析DNS协议

3. 分析HTTP协议

二．分析要求

**（1）ftp部分**

1. 学习 Serv-U FTP Server 服务软件的基本配置和FTP 客户端命令的使用
2. 设计应用以获取ftp报文
3. 分析ftp报文的格式与内容（分析至少5个报文，并理解它们之间的关系）
4. 观察 FTP 协议的工作过程，分析FTP 客户是以 PORT 模式还是 PASV 模式连接服务器，观察两种连接 的建立过程和释放过程，以及这两种连接建立和释放的先后顺序

**（2）dns部分**

1. 熟悉ipconfig 清除dns缓存命令的使用(flushdns
2. 设计应用以获取dns报文
3. 分析dns报文的格式与内容（分析至少5个报文，并理解它们之间的关系）
4. 观察 分析dns 协议的工作过程

**（3）http部分**

1. 设计应用以获取http报文

2. 分析http报文的格式与内容（分析至少5个报文，并理解它们之间的关系）

3. 分析http协议的工作过程

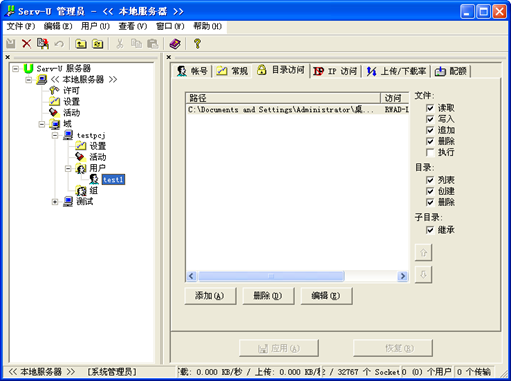
**三．分析内容**

（1）**ftp部分**

1. 学习 Serv-U FTP Server 服务软件的基本配置和FTP 客户端命令的使用



配置域



配置用户权限

1. 设计应用以获取ftp报文

在命令行窗口中登录FTP 服务器，根据1 中的配置信息输入用户名和口令，同时使用抓包工具截获ftp报文，参考命令如下：

C:\ >ftp

ftp> open

To 172.16.10.100 //登录ftp 服务器

Connected to 172.16.10.100.

220 Serv-U FTP Server v6.2 for WinSock ready...

User(none): test1 //输入用户名

331 User name okay, need password.

Password:123 //输入用户密码

230 User logged in, proceed. //通过认证，登录成功

ftp> quit //退出FTP

221 Goodbye!

从浏览器访问ftp，再次抓包

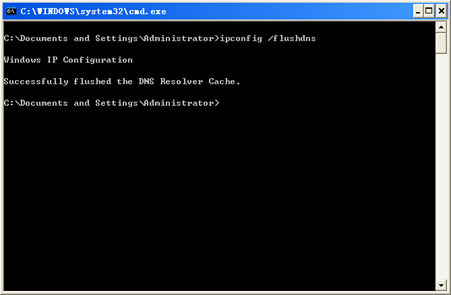
（1）分析ftp报文的格式与内容（分析至少5个报文，并理解它们之间的关系）

分析见第四部分

（2）观察 FTP 协议的工作过程，分析FTP 客户是以 PORT 模式还是 PASV 模式连接服务器，观察两种连接 的建立过程和释放过程，以及这两种连接建立和释放的先后顺序

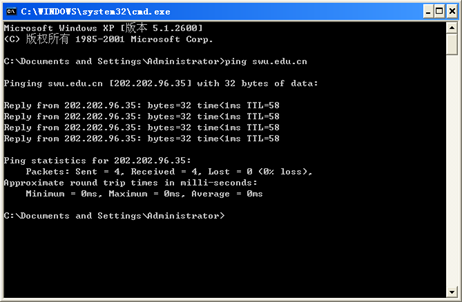
（2）**dns部分**

1. 熟悉ipconfig 清除dns缓存命令的使用(flushdns)



1. 设计应用以获取dns报文

先清除DNS缓存，然后ping西南大学主页swu.edu.cn获取并用抓包工具截获DNS报文



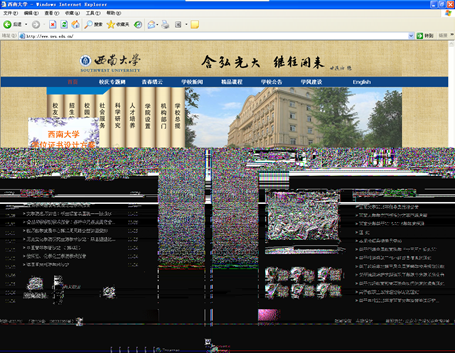
1. 分析dns报文的格式与内容（分析至少5个报文，并理解它们之间的关系）

分析见第四部分

（3）**http部分**

1. 设计应用以获取http报文

访问一些特定的网址，如学校官网主页、百度主页……用抓包工具截获http协议报文：



访问西南大学主页，抓取http报文

2. 分析http报文的格式与内容（分析至少5个报文，并理解它们之间的关系）

分析见第四部分

3. 分析http协议的工作过程

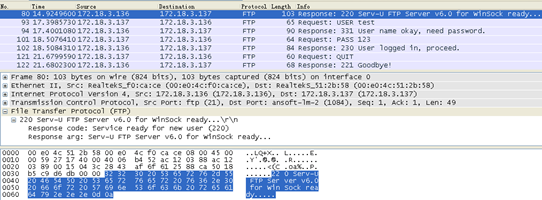
分析见第四部分

四、分析结果及总结

1. 获取并分析ftp报文

（1）登录ftp服务器：172.18.3.136的第一个ftp报文：

32323020536572762d5520465450205365727665722076362e3020666f722057696e536f636b2072656164792e2e2e0d0a



状态码：32 32 30

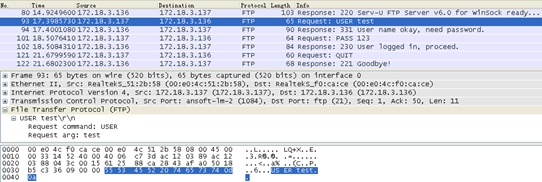
Response code: Service ready for new user (220)

应答串：

Response arg: Serv-U FTP Server v6.0 for WinSock ready...

（2）登录ftp服务器：172.18.3.136第二个ftp报文：

5553455220746573740d0a

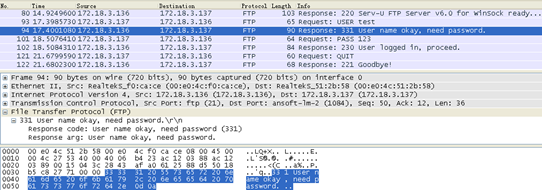


Request command: USER

Request arg: test

（3）登录ftp服务器：172.18.3.136第三个ftp报文：

07a200151ea58e9063bcdaf85010b5c9a7110000

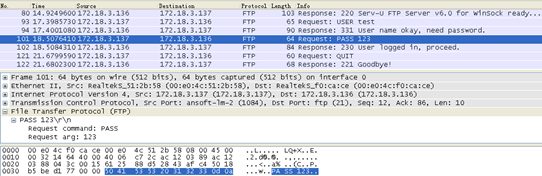


Response code: User name okay, need password (331)

Response arg: User name okay, need password.

（4）登录ftp服务器：172.18.3.136第四个ftp报文：

50415353203132330d0a

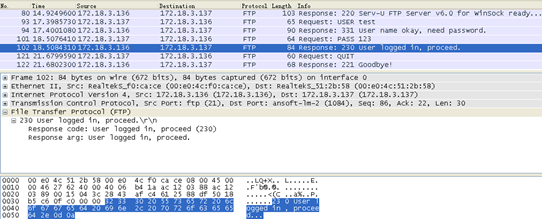


Request command: PASS

Request arg: 123

（5）登录ftp服务器：172.18.3.136第五个ftp报文：

3233302055736572206c6f6767656420696e2c2070726f636565642e0d0a

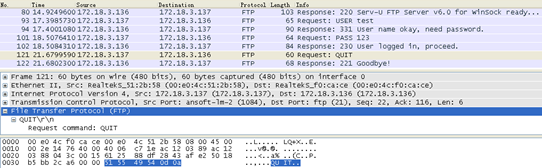


Response code: User logged in, proceed (230)

Response arg: User logged in, proceed.

（6）登录ftp服务器：172.18.3.136第六个ftp报文：

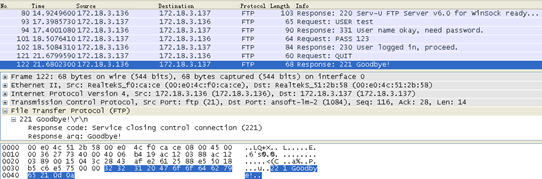
515549540d0a



Request command: QUIT

（7）登录ftp服务器：172.18.3.136第七个ftp报文：

32323120476f6f64627965210d0a



Response code: Service closing control connection (221)

Response arg: Goodbye!

（8）使用浏览器访问ftp服务器172.18.3.136

ftp内容与cmd命令访问ftp服务器类似。

在命令行窗口中访问FTP 服务器时客户端使用的是PORT 模式连接服务器，浏览器访问ftp服务器是时客户端以PASV 模式连接服务器。

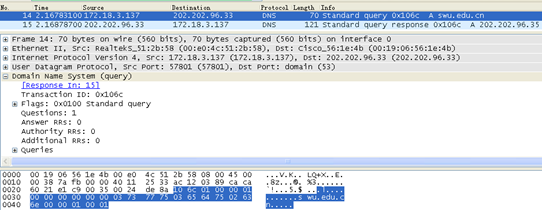
PORT模式：客户端从任意非特权端口N连接到服务器的命令端口21，然后把客户端监听端口N+1并发送PORT N+1到服务器，接着服务器从自己的数据端口20连接到客户端指定的端口N+1。断开连接时客户端向服务器发送quit命令，服务器回复221状态码，然后客户端开始向服务器发送TCP断开连接报文经三次握手结束连接

PASV模式：客户端打开任意两个非特权本地端口，第一个连接到服务器21端口，并提交PASV命令，服务器发送PORT P命令道客户端，然后本地客户端使用第二个端口连接服务器端口P进行数据传输。

2. 获取并分析DNS报文

（1）ping西南大学主页swu.edu.cn的DNS查询报文

106c01000001000000000000037377750365647502636e0000010001



标识：10 6c

Transaction ID: 0x106c

参数：01 00

Flags: 0x0100 Standard query

问题数：00 01

Questions: 1

回答数：00 00

Answer RRs: 0

管理机构数：00 00

Authority RRs: 0

附加信息数：00 00

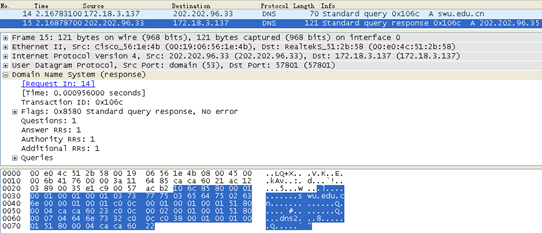
Additional RRs: 0

问题区：037377750365647502636e0000010001

Queries: swu.edu.cn: type A, class IN

（2）ping西南大学主页swu.edu.cn的DNS响应报文

106c85800001000100010001037377750365647502636e0000010001c00c00010001000151800004caca6023c00c0002000100015180000704646e7332c00cc03800010001000151800004caca6022



标识：10 6c

Transaction ID: 0x106c

参数：8580

Flags: 0x8580 Standard query response, No error

问题数：00 01

Questions: 1

回答数：00 01

Answer RRs: 1

管理机构数：00 01

Authority RRs: 1

附加信息数：00 01

Additional RRs: 1

问题区：037377750365647502636e0000010001

swu.edu.cn: type A, class IN

回答区：c00c00010001000151800004caca6023

swu.edu.cn: type A, class IN, addr 202.202.96.35

管理机构区：c00c0002000100015180000704646e7332c00c

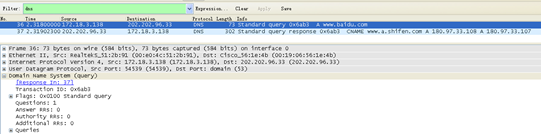
swu.edu.cn: type NS, class IN, ns dns2.swu.edu.cn

附加信息区：c03800010001000151800004caca6022

dns2.swu.edu.cn: type A, class IN, addr 202.202.96.34

（3）ping百度主页[www.baidu.com](http://www.baidu.com/)（未登录外网）的DNS查询报文

6ab3010000010000000000000377777705626169647503636f6d0000010001



标识：6a b3

Transaction ID: 0x6ab3

参数：01 00

Flags: 0x0100 Standard query

问题数：00 01

Questions: 1

回答数：00 00

Answer RRs: 0

管理机构数：00 00

Authority RRs: 0

附加信息数：00 00

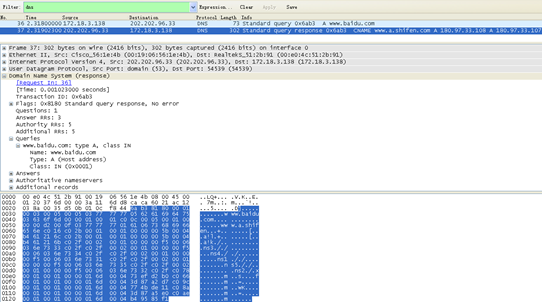
Additional RRs: 0

问题区：0377777705626169647503636f6d0000010001

www.baidu.com: type A, class IN

（4）ping百度主页[www.baidu.com](http://www.baidu.com/)（未登录外网）的DNS响应报文





标识：6a b3

Transaction ID: 0x6ab3

参数：8180

Flags: 0x8180 Standard query response, No error

问题数：00 01

Questions: 1

回答数：00 03

Answer RRs: 3

管理机构数：00 05

Authority RRs: 5

附加信息数：00 05

Additional RRs: 5

问题区：0377777705626169647503636f6d0000010001

www.baidu.com: type A, class IN

回答区：

c00c00050001000000d2000f0377777701610673686966656ec016c02b000100010000005b0004b461216cc02b000100010000005b0004b461216b

www.baidu.com: type CNAME, class IN, cname [www.a.shifen.com](http://www.a.shifen.com/)

www.a.shifen.com: type A, class IN, addr 180.97.33.108

www.a.shifen.com: type A, class IN, addr 180.97.33.107

管理机构区：

c02f00020001000000f50006036e7333c02fc02f00020001000000f50006036e7334c02fc02f00020001000000f50006036e7331c02fc02f00020001000000f50006036e7335c02fc02f00020001000000f50006036e7332c02f

a.shifen.com: type NS, class IN, ns ns3.a.shifen.com

a.shifen.com: type NS, class IN, ns ns4.a.shifen.com

a.shifen.com: type NS, class IN, ns ns1.a.shifen.com

a.shifen.com: type NS, class IN, ns ns5.a.shifen.com

a.shifen.com: type NS, class IN, ns ns2.a.shifen.com

附加信息区：

c078000100010000016d000473efd2b0c066000100010000016d00043d87a2d7c09c000100010000016d0004774bde11c08a000100010000016d00043d87a5e0c0ae000100010000016d0004b49585f1

ns4.a.shifen.com: type A, class IN, addr 115.239.210.176

ns3.a.shifen.com: type A, class IN, addr 61.135.162.215

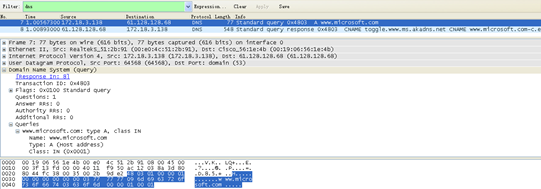
ns5.a.shifen.com: type A, class IN, addr 119.75.222.17

ns1.a.shifen.com: type A, class IN, addr 61.135.165.224

ns2.a.shifen.com: type A, class IN, addr 180.149.133.241

（5）ping微软主页www.microsoft.com的DNS查询报文

48030100000100000000000003777777096d6963726f736f667403636f6d0000010001



标识：48 03

Transaction ID: 0x4803

参数：01 00

Flags: 0x0100 Standard query

问题数：00 01

Questions: 1

回答数：00 00

Answer RRs: 0

管理机构数：00 00

Authority RRs: 0

附加信息数：00 00

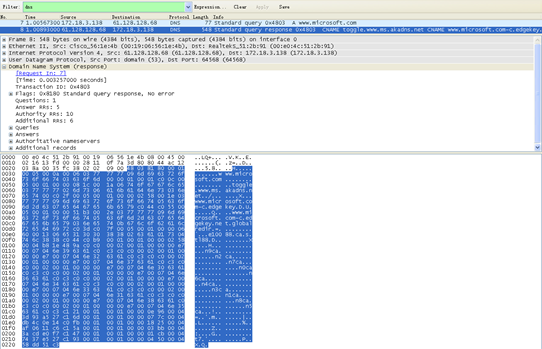
Additional RRs: 0

问题区：03777777096d6963726f736f667403636f6d0000010001

www.microsoft.com: type A, class IN

（6）ping微软主页www.microsoft.com的DNS响应报文





标识：48 03

Transaction ID: 0x4803

参数：81 80

Flags: 0x8180 Standard query response, No error

问题数：00 01

Questions: 1

回答数：00 05

Answer RRs: 5

管理机构数：00 0a

Authority RRs: 10

附加信息数：00 06

Additional RRs: 6

问题区：03777777096d6963726f736f667403636f6d0000010001

www.microsoft.com: type A, class IN

回答区：

c00c000500010000081c001a06746f67676c6503777777026d7306616b61646e73036e657400c02f0005000100000258001e03777777096d6963726f736f667405636f6d2d6307656467656b6579c044c05500050001000051b3002e03777777096d6963726f736f667405636f6d2d6307656467656b6579036e65740b676c6f62616c7265646972c03dc07f0005000100000660001306653130303838026361017304746c3838c044c0b900010001000002580004b81e489a

www.microsoft.com: type CNAME, class IN, cname toggle.www.ms.akadns.net

toggle.www.ms.akadns.net: type CNAME, class IN, cname [www.microsoft.com-c.edgekey.net](http://www.microsoft.com-c.edgekey.net/)

www.microsoft.com-c.edgekey.net: type CNAME, class IN, cname [www.microsoft.com-c.edgekey.net.globalredir.akadns.net](http://www.microsoft.com-c.edgekey.net.globalredir.akadns.net/)

www.microsoft.com-c.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e10088.ca.s.tl88.net

e10088.ca.s.tl88.net: type A, class IN, addr 184.30.72.154

管理机构区：

c0c000020001000000e70007046e396361c0c3c0c000020001000000e70007046e326361c0c3c0c000020001000000e70007046e376361c0c3c0c000020001000000e70007046e306361c0c3c0c000020001000000e70007046e366361c0c3c0c000020001000000e70007046e346361c0c3c0c000020001000000e70007046e336361c0c3c0c000020001000000e70007046e316361c0c3c0c000020001000000e70007046e386361c0c3c0c000020001000000e70007046e356361c0c3

ca.s.tl88.net: type NS, class IN, ns n9ca.s.tl88.net

ca.s.tl88.net: type NS, class IN, ns n2ca.s.tl88.net

ca.s.tl88.net: type NS, class IN, ns n7ca.s.tl88.net

ca.s.tl88.net: type NS, class IN, ns n0ca.s.tl88.net

ca.s.tl88.net: type NS, class IN, ns n6ca.s.tl88.net

ca.s.tl88.net: type NS, class IN, ns n4ca.s.tl88.net

ca.s.tl88.net: type NS, class IN, ns n3ca.s.tl88.net

ca.s.tl88.net: type NS, class IN, ns n1ca.s.tl88.net

ca.s.tl88.net: type NS, class IN, ns n8ca.s.tl88.net

ca.s.tl88.net: type NS, class IN, ns n5ca.s.tl88.net

附加信息区：

c1210001000100000e9600043d93a527c16d000100010000077c0004db4c0e14c0fb00010001000018250004af0611c6c15a00010001000003bb00043acde0f7c14700010001000001cb00047437e527c1930001000100000450000458dd51c3

n0ca.s.tl88.net: type A, class IN, addr 61.147.165.39

n1ca.s.tl88.net: type A, class IN, addr 219.76.14.20

n2ca.s.tl88.net: type A, class IN, addr 175.6.17.198

n3ca.s.tl88.net: type A, class IN, addr 58.205.224.247

n4ca.s.tl88.net: type A, class IN, addr 116.55.229.39

n5ca.s.tl88.net: type A, class IN, addr 88.221.81.195

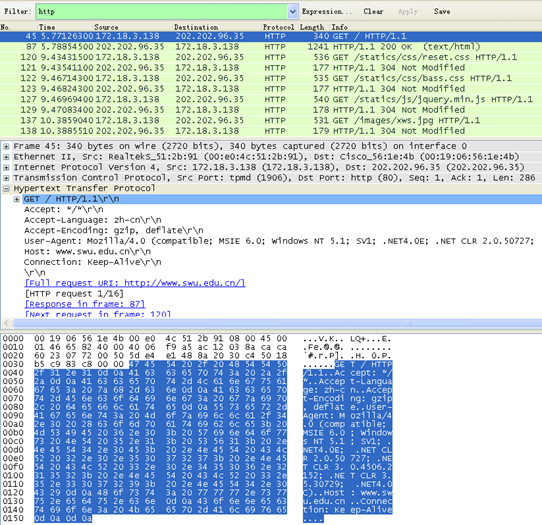
DNS协议工作过程为：

需要解析域名时，电脑首先查找自己的缓存文件,如果没有则发送指令到本地DNS服务器进行解析,本地DNS服务器内域名和IP映射表中如果可以查询到网站IP,则可以立即访问,如果没有的话,本地DNS则会自动向根域名服务器发起查询,根域名服务器会把域名和IP映射信息发送给本地域名服务器,如果连跟域名服务器都没有该域名与IP映射信息,则会告诉本地域名服务器下一次向dns.访问域名.com发起查询,对方本地的域名服务器则会把该域名的IP信息发送到本地域名服务器

3.获取并分析http报文：

（1）访问西南大学主页swu.edu.cn的第一个http报文





开始行：

请求方式：47 45 54

Request Method: GET

URL：2f

Request URI: /

HTTP版本：485454502f312e31

Request Version: HTTP/1.1

首部行：

Accept: \*/\*\r\n

Accept-Language: zh-cn\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C)\r\n

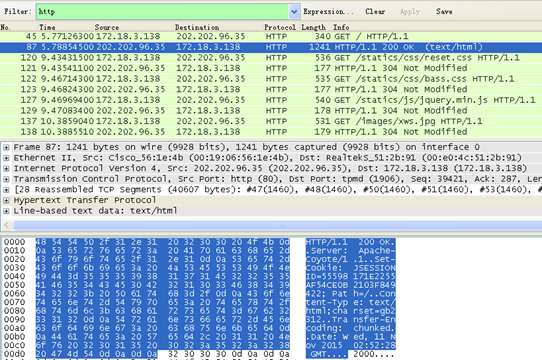
Host: [www.swu.edu.cn\r\n](http://www.swu.edu.cn/r/n)

Connection: Keep-Alive\r\n

实体主体：无

（2）访问西南大学主页swu.edu.cn的第二个http报文

485454502f312e3120323030204f4b0d0a5365727665723a204170616368652d436f796f74652f312e310d0a5365742d436f6f6b69653a204a53455353494f4e49443d35353539383137314532323535414635344345304232313033463834393432323b20506174683d2f0d0a436f6e74656e742d547970653a20746578742f68746d6c3b636861727365743d6762323331320d0a5472616e736665722d456e636f64696e673a206368756e6b65640d0a446174653a205765642c203131204e6f7620323031352030323a35323a323820474d540d0a0d0a



开始行：

HTTP版本：485454502f312e31

Request Version: HTTP/1.1

状态码：32 30 30

Status Code: 200

解释字符串：4f 4b

Response Phrase: OK

首部行：

Server: Apache-Coyote/1.1\r\n

Set-Cookie: JSESSIONID=55598171E2255AF54CE0B2103F849422; Path=/\r\n

Content-Type: text/html;charset=gb2312\r\n

Transfer-Encoding: chunked\r\n

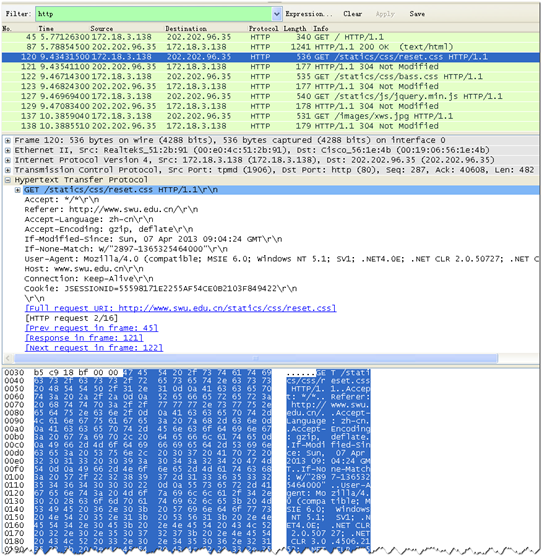
Date: Wed, 11 Nov 2015 02:52:28 GMT\r\n

实体主体：

Line-based text data: text/html

（3）访问西南大学主页swu.edu.cn的第三个http报文（请求css文件）





开始行：

Request Method: GET

Request URI: /statics/css/reset.css

Request Version: HTTP/1.1

首部行：

Accept: \*/\*\r\n

Referer: [http://www.swu.edu.cn/\r\n](http://www.swu.edu.cn/r/n)

Accept-Language: zh-cn\r\n

Accept-Encoding: gzip, deflate\r\n

If-Modified-Since: Sun, 07 Apr 2013 09:04:24 GMT\r\n

If-None-Match: W/"2897-1365325464000"\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C)\r\n

Host: [www.swu.edu.cn\r\n](http://www.swu.edu.cn/r/n)

Connection: Keep-Alive\r\n

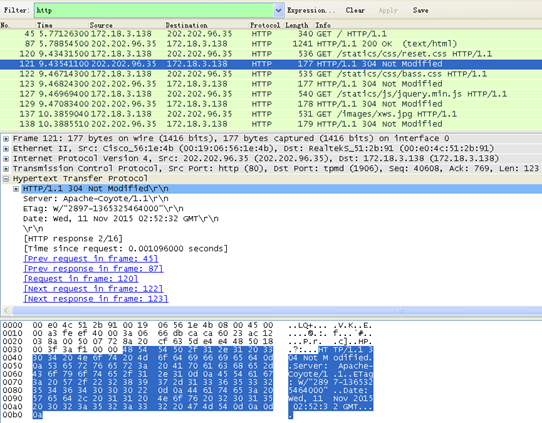
Cookie: JSESSIONID=55598171E2255AF54CE0B2103F849422\r\n

实体主体：

无

（4）访问西南大学主页swu.edu.cn的第四个http报文（css文件请求的应答）

485454502f312e3120333034204e6f74204d6f6469666965640d0a5365727665723a204170616368652d436f796f74652f312e310d0a455461673a20572f22323839372d31333635333235343634303030220d0a446174653a205765642c203131204e6f7620323031352030323a35323a333220474d540d0a0d0a



开始行：

Request Version: HTTP/1.1

Status Code: 304

Response Phrase: Not Modified

首部行：

Server: Apache-Coyote/1.1\r\n

ETag: W/"2897-1365325464000"\r\n

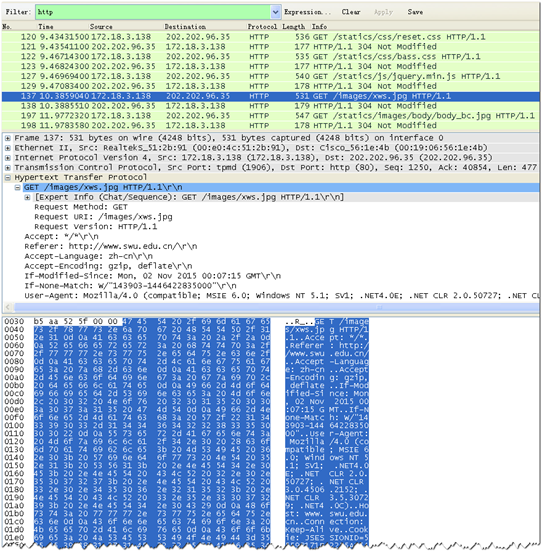
Date: Wed, 11 Nov 2015 02:52:32 GMT\r\n

实体主体：

无

（5）访问西南大学主页swu.edu.cn的第七个http报文（请求图片）





开始行：

Request Method: GET

Request URI: /images/xws.jpg

Request Version: HTTP/1.1

首部行：

Accept: \*/\*\r\n

Referer: [http://www.swu.edu.cn/\r\n](http://www.swu.edu.cn/r/n)

Accept-Language: zh-cn\r\n

Accept-Encoding: gzip, deflate\r\n

If-Modified-Since: Mon, 02 Nov 2015 00:07:15 GMT\r\n

If-None-Match: W/"143903-1446422835000"\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C)\r\n

Host: www.swu.edu.cn\r\n

Connection: Keep-Alive\r\n

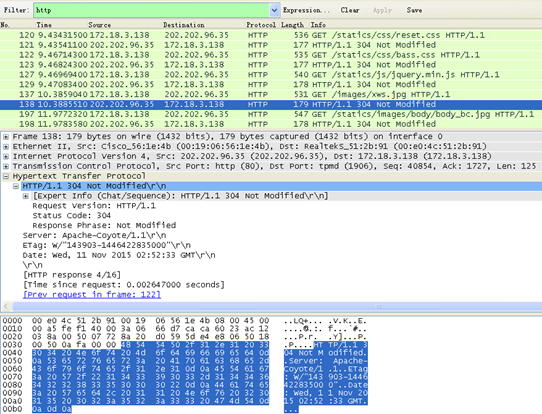
Cookie: JSESSIONID=55598171E2255AF54CE0B2103F849422\r\n

实体主体：

无

（6）访问西南大学主页swu.edu.cn的第八个http报文（图片请求的应答）

485454502f312e3120333034204e6f74204d6f6469666965640d0a5365727665723a204170616368652d436f796f74652f312e310d0a455461673a20572f223134333930332d31343436343232383335303030220d0a446174653a205765642c203131204e6f7620323031352030323a35323a333320474d540d0a0d0a



开始行：

Request Version: HTTP/1.1

Status Code: 304

Response Phrase: Not Modified

首部行：

Server: Apache-Coyote/1.1\r\n

ETag: W/"143903-1446422835000"\r\n

Date: Wed, 11 Nov 2015 02:52:33 GMT\r\n

实体主体：

无

HTTP请求/响应的过程为：

（1）客户端连接到Web服务器

一个HTTP客户端，通常是浏览器，与Web服务器的HTTP端口（默认为80）建立一个TCP套接字连接。

（2）发送HTTP请求

通过TCP套接字，客户端向Web服务器发送一个文本的请求报文，一个请求报文由请求行、请求头部、空行和请求数据4部分组成。

（3）服务器接受请求并返回HTTP响应

Web服务器解析请求，定位请求资源。服务器将资源复本写到TCP套接字，由客户端读取。一个响应由状态行、响应头部、空行和响应数据4部分组成。

（4）释放连接TCP连接

Web服务器主动关闭TCP套接字，释放TCP连接；客户端被动关闭TCP套接字，释放TCP连接。

（5）客户端浏览器解析HTML内容

客户端浏览器首先解析状态行，查看表明请求是否成功的状态代码。然后解析每一个响应头，响应头告知以下为若干字节的HTML文档和文档的字符集。客户端浏览器读取响应数据HTML，根据HTML的语法对其进行格式化，并在浏览器窗口中显示。

注意，当使用浏览器访问网址同时抓取报文的方式来获取报文的话，会获取到很多不是实验所需要的报文，要注意区别开来，找到实验需要的报文。