bluemonster的博客

http://blog.sina.com.cn/bluemonster0808 ［订阅］［手机订阅］

个人资料

bluemonster

微博

加好友 发纸条

写留言 加关注

正文 字体大小：大 中 小

DNS报文结构实例解析

(2010-09-13 22:01:53) 转 载

标签： dns dns报文 实例 报文解析 it 分类： 实验室

抓迅雷的包，发现迅雷整了N多和下载无关的东西，比如kankan，games啥的，启动的时候发了一堆DNS请求来解析这些整合的东西。于是学习了一下DNS报文的结构

DNS请求报文的结构是

0 15 16 31

标识ID	标志
问题数	资源记录数
授权资源记录数	额外资源记录数
查询问题	
回答	
授权信息	
额外信息	

其中，后面四个字段的长度可变，它们各自的字节数也不一定是4的倍数。

标识ID：有发出DNS请求的客户端生成，对应的DNS响应报文中也要置同样的ID。

16bit的标志字段 如下：

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必须为0

Rcode：返回码，通常为0（没有差错）和3（名字差错）

后面4个16bit字段说明最后4个变长字段中包含的条目数。

就我抓包所见，DNS请求报文的标志字段一般为0x0100

问题数字段是指这个DNS请求中待解析的域名数目，一般是1，也即0x0001。对应的DNS响应报文的问题数字段也置同样的值

资源记录数、授权资源记录数、额外资源记录数在DNS请求报文中都为0，在响应报文中视情况而定。

查询问题字段的格式为

0 15 16

31

查询名（长度不定，字节数不一定为4的倍数）	
查询类型	查询类

查询名为要查找的名字，它由一个或者多个标示符序列组成。每个标示符已首字节数的计数值来说明该标示符长度，每个名字以0结束，计数字节数必须是0~63之间。该字段无需填充字节。如www.baidu.com在DNS报文中就是

03	77	77	77	05	62	61	69	64	75	03	63	6f	6d	00
	w	w	w		b	a	i	d	u		c	o	m	

查询类型一般为0x0001，表示是从host address解析IP

查询类一般为0x0001，表示class IN

DNS请求报文和对应的响应报文中的查询问题字段是完全一样的

回答字段的格式如下

0 15 16

31

NAME（长度不定，字节数不一定是4的倍数）	
响应类型	响应类
生存时间	
数据长度	数据（长度不定，字节数不一定是4的倍数）

NAME是该响应报文对应的DNS请求报文要解析的域名，可能是和查询问题字段中的查询名完全一样，但更多的情况下：考虑到响应报文中的查询问题字段和请求报文完全一样，也就包含了查询名，那么也可采用压缩的方式来存放，即用一个16bit的指针来指示NAME的偏移量。比如0xC00C，二进制就是1100 0000 0000 1100，头两位为11表示这是一个双字节的指针，而不是一个计数字节（上面提到了，查询名里的计数字节为0~63，因此头两位不可能为11），后面的14位则表示这个压缩指针所指的数据离DNS报文（也就是UDP数据报的数据部分，不是指包含DNS报文的UDP数据报的报头）头部的偏移量是12。

生存时间以s为单位

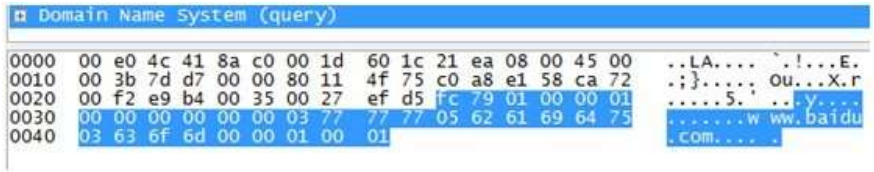
数据长度是数据的字节数

响应类和请求报文的查询问题字段中的查询类对应

响应类型我目前见到了两种，一种是0x0001，这种情况下后面的数据是NAME对应的IP，占4字节；一种是0x0005，这种情况下后面的数据是NAME重定向到的域名（比如www.xiaonei.com重定向到www.renren.com），这里数据也用查询名中的方式来存放重定向到的域名。

下面是实例解析，以www.baidu.com为例

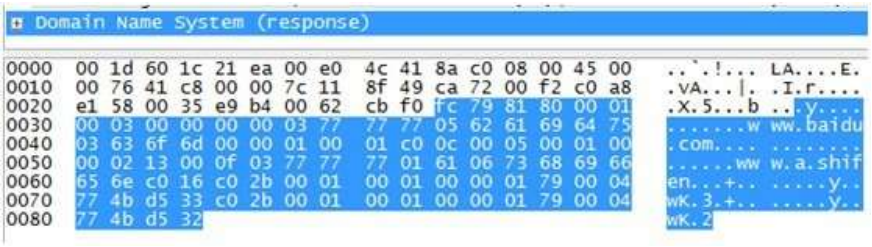
请求报文



fc79	0100	0001	0000	0000	0000
标识ID	标志字段	问题数	资源记录数	授权资源记录数	额外资源记录数
03 77 77 77 05 62 61 69 64 75 03 63 6f 6d 00				0001	0001
查询名（www.baidu.com）				响应类型	响应类

荷叶 4月3日
向左走 3月22日
用户20829… 2月16日

响应报文



fc79	8180	0001	0003	0000	0000
标识ID	标志字段	问题数	资源记录数	授权资源记录数	额外资源记录数
03 77 77 77 05 62 61 69 64 75 03 63 6f 6d 00				0001	0001
查询名（www.baidu.com）				查询类型	查询类
c00c				0005	0001
指针，指向DNS头部开始偏移12位，即查询名开始位置				第一个资源记录的响应类型	第一个资源记录的响应类
0000 0213				000f	
第一个资源记录的生存时间				第一个资源记录的数据长度	
03 77 77 77 01 61 06 73 68 69 66 65 6e c0 16					
第一个资源记录的数据，c016之前对应www.a.shifen，c016又是指针，指向DNS头部开始偏移22位，即查询名中的03 63 6f 6d 00，也就是.com					
c02b				0001	0001
第二个资源记录的NAME，指针，指向DNS头部开始偏移43位，即第一个资源记录中的数据				第二个资源记录的响应类型	第二个资源记录的响应类
0000 0179				0004	
第二个资源记录的生存时间				第二个资源记录的数据长度	
77 4b d5 33				c02b	
第二个资源记录的数据，即IP：119.75.213.51				第三个资源记录的NAME，指针，指向DNS头部开始偏移43位，即第一个资源记录中的数据	
0001		0001		0000 0179	
第三个资源记录的响应类型		第三个资源记录的响应类型		第三个资源记录的生存时间	
0004				77 4b d5 32	
第三个资源记录的数据长度				第二个资源记录的数据，即IP：119.75.213.50	

从word里粘过来的，格式变丑了，传了原始word文档到ishare上：
http://ishare.iask.sina.com.cn/f/10491367.html

9 喜欢　　0 赠金笔

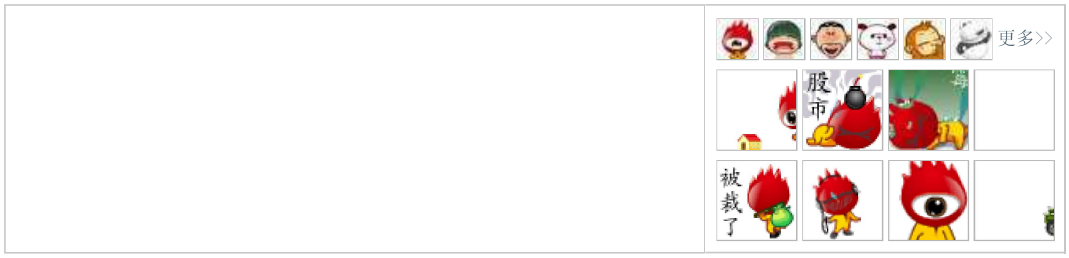
分享：

前一篇：Python遍历目录下的文件并查找文件内容
后一篇：修改右键菜单

评论 重要提示：警惕虚假中奖信息 [发评论]

做第一个评论者吧！ 抢沙发>>

发评论



登录名： 密码： 找回密码 注册 记住登录状态

评论并转载此博文

发评论

以上网友发言只代表其个人观点，不代表新浪网的观点或立场。

< 前一篇
Python遍历目录下的文件并查找文件内容

后一篇 >
修改右键菜单