

RSS订阅

十佳

转

DNS查询报文和应答报文抓包分析【1/2】

2013年04月09日 15:09:49

阅读数：2074

联

我使用的抓包软件是科来网络分析系统2010技术交流版，可以从<http://www.colasoft.com.cn/download/capsatech.exe>免费下载，只需在线填写几项信息过几分钟就可以收到科来发送过来的序列号了，只用了一会但是感觉很不错，推荐一下。

首先在科来里面新建一个工程，只需要DNS报文，然后打开浏览器，输入www.chd.edu.cn，回车就可以在科来里面看到捕获的数据了，捕获到的DNS查询报文为82个字节，前50个字节是目标MAC地址、源MAC地址、IP和UDP之类的东西，不理睬它们，从第51个字节开始看。

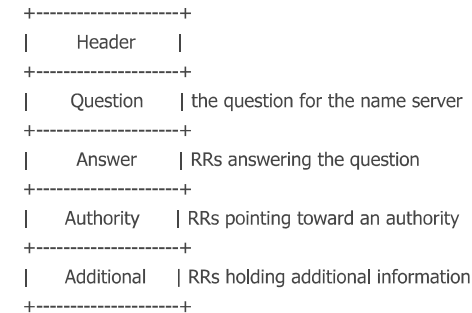
科来网络分析系统给出了一份自动分析报告，很详细，但是现在是手工分析，就不看它了。

第51-82字节的内容如下：

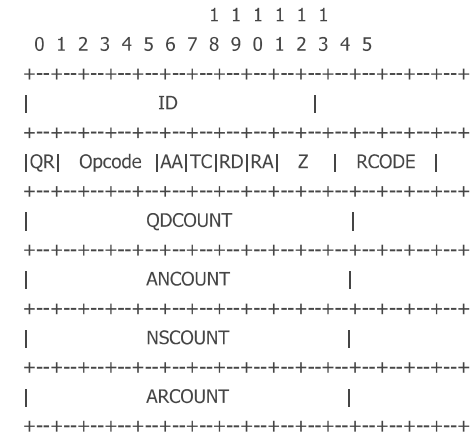
21 FE 01 00 00 01 00 00 00 00 00 03 77 77 77 03 63 68 64 03 65 64 75 02 63 6E 00 00 01 00 01

开始时根据习惯按小端法分析，但是从科来的分析结果可以看到网络上传输的数据是按大端法传输的，与Intel架构下的二进制分析不一样，这点在分析时要注意。

先来看一下DNS报文的格式：



Header的格式如下：



前两个字节是标识，为0x21FE，此标识为发出请求的客户端随意设置的，这个查询报文对应的应答报文也带有相同的标识，这样客户端就可以区分不同的请求的应答而不会搞混了。

然后是两个字节的报文参数，为0x0100，分解为二进制是0000 0001 0000 0000b，代表的含义如下表：

参数名

QR

操作码

AA

TC

RD

RA

保留

Recode

值

0

0000

0

0

1

0

000

0000

含义

查询

标准查询

见下面描述

报文未截断

期望递归解析

见下面描述

保留

没有出错

起初看不懂课本上对AA位的描述，在网上搜了一下发现这一位在DNS应答报文中才有意义，代表给出应答的DNS服务器是不是被查询域名的授权解析服务器（权威服务器）。

RA位也是在应答报文中才有意义，以说明做出应答的DNS服务器是否支持递归解析。

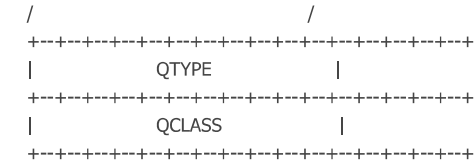
后面的两个字节是问题数，为0x0001，即只要求解析一个域名。

后面的六个字节分别是应答数、授权机构数和附加信息数，这个报文是查询报文，全部为0x0000。

然后是问题部分，格式如下：

```

      1 1 1 1 1 1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
```



开始由多组4个字节构成，值为03 77 77 77 03 63 68 64 03 65 64 75 02 63 6E 00，即“www.chd.edu.cn”，根据ASCII码表可知，“www”、“chd”、“edu”、“cn”的ASCII编码是正确的，但是开头却添加了一个字节的0x03，而且前两个“.”的编码是0x03，最后一个“.”的编码是0x02，不明白这样做是为什么，因为“.”的ASCII码是0x2E。后来经过多次对不同域名的DNS查询报文抓包比较发现，原来这根本不是ASCII码，这个值指的是与下一个点之间有几个ASCII码，例如hi.baidu.com就应该编码成02 68 69 05 62 61 69 64 75 03 63 6F 6D 00，把RFC-1035中的解释放在下面，“a domain name represented as a sequence of labels, where each label consists of a length octet followed by that number of octets. The domain name terminates with the zero length octet for the null label of the root. Note that this field may be an odd number of octets; no padding is used.”。

然后的两个字节是查询类型，值为0x0001，即将要求域名转换为IPv4地址。

最后两个字节是查询类，值为0x0001，即查询的是因特网的域名。

至此，DNS查询报文的所有域已经手工分析完毕。

由于baidu空间有40000个字符的限制，所以DNS应答报文的分析放到另一篇日志里。

传送门：<http://hi.baidu.com/pianoid/blog/item/ebc20f8717a4513fc75cc358.html>

查询报文在上一篇日志里分析过了（传送门：<http://hi.baidu.com/pianoid/blog/item/b40939d79bd1f3c8a044df5d.html>），现在来看应答报文。

捕获到的对应的DNS应答报文如下（去掉了前50个字节）：

```

21 FE 81 80 00 01 00 01 00 02 00 02 03 77 77 77 03 63 68 64 03 65 64 75 02 63 6E 00 00 01 00 01 C0 0C 00 01 00 01 00 00 17 63 00 04 CA 75 40 02 C0 10 00
02 00 01 00 00 FD F5 00 07 04 44 4E 53 31 C0 10 C0 10 00 02 00 01 00 00 FD F5 00 07 04 44 4E 53 32 C0 10 C0 3C 00 01 00 01 00 01 40 6E 00 04 CA 75 40 01
C0 4F 00 01 00 01 00 01 41 8A 00 04 DA C3 38 01

```

标识字段也是0x21FE，跟查询报文一样，说明是对上面那个查询报文的应答，这样就不会搞混了。

参数字段为0x8180，分解成二进制为1000 0001 1000 0000，含义如下表

参数名
QR
操作码
AA
TC
RD
RA
保留
Recode
值
1
0000
0
0
1
1
000
0000

应答

见下面描述

不是权威服务器应答

报文未截断

期望递归解析

服务器支持递归解析

保留

没有出错

操作码和RD在应答报文中没有意义，设置成跟查询报文一样的值就可以了。

问题数为0x0001，跟查询报文一样。

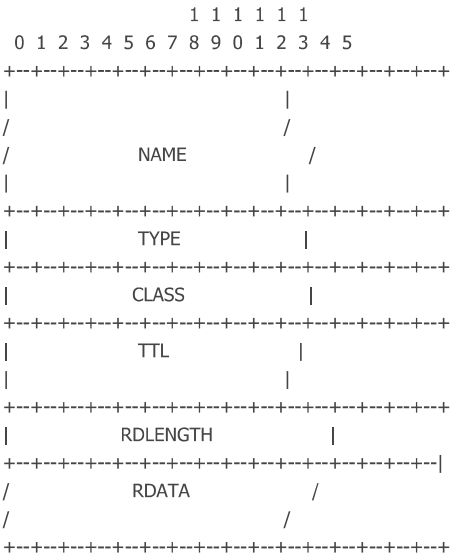
应答数为0x0001，即有一个应答。

管理机构数为0x0002，即有两台权威服务器对查询报文做出应答，后面的权威机构部分可以看到这两台服务器。

附加信息数为0x0002，即有两条附加信息，也就是管理机构服务器给出的应答结果。

问题部分同查询报文，不再分析。

答案部分和后面的权威机构、附加信息部分都是资源记录格式（Resource Records），格式与问题部分不一样，格式如下：



前四个字节是域名的副本，但是经过报文压缩就变成了两个字节的指针偏移，在这里值为0xC00C。由于标号的长度被限制不能超过63个字节，所以前两位一定是00b，指针就设置为11b以区别，这个指针的偏移就是0x000C，从应答报文的标识开始数（第一个字节偏移是0x0000），第0x000C字节就是www.chd.edu.cn开头的0x03。

域类型和域类都是0x0001，与查询报文一样。

生存时间为0x00001763，即5987秒，很奇怪的数字，不知是根据什么设置的。

资源数据长度为0x0004。

资源数据为0xCA754002，转换成十进制的IP地址就是202.117.64.2，也就是www.chd.edu.cn这个域名对应的IPv4地址。

再后面就是两个资源记录，分别对应报文头部提到的两个权威服务器，分别是DNS1.chd.edu.cn和DNS2.chd.edu.cn，与前面的答案部分不一样的部分只有域类型为0x0002，说明这两台服务器是所查询域名的授权解析服务器（权威服务器）。

再后面是两个附加答案，即两台权威服务器给出的应答结果，DNS1.chd.edu.cn给出的IPv4地址是0xCA754001，即202.117.64.1，DNS2.chd.edu.cn给出的IPv4地址是0xCA754002，即202.117.64.2。

OK，到这里两个DNS Message就已经全部分析完毕了。

转载：<http://hi.baidu.com/axhmzocrqdbcijq/item/2eb40c1b39a8daa7ffded558>

个人分类：[网络](#) [Windows](#)

相关热词：[主dns辅dns](#) [前端开发dns](#) [切换dns](#) [反向dns](#) [全国dns](#)

- 上一篇ASII码表
- 下一篇在MFC，Win32程序中向控制台(Console)窗口输出调试信息

脱颖而出！Python逐渐成为第一大语言

你知道如何学习吗？

点击了解

想对作者说点什么？[我来说一句](#)

DNS协议详解及报文格式分析

DNS协议详解及报文格式分析 Posted on 2017-06-18 by Jocent — No Comments ↓ 目录 一. DNS协议理论知识 1.1....

 tianyeming 2017-07-10 14:38:12 阅读数：21123

结合Wireshark分析DNS 协议

摘要： 本文简单介绍了DNS协议理论知识，给出URL解析步骤，详细讲述了DNS报文各个字段含义，并从Wireshark俘获分组中选取DNS相关报文进行分析。
一、概述 1.1...

 hunanchenxingyu 2014-03-18 23:55:37 阅读数：33298

区块链以太坊DApp高薪实战，报名即可领取助学金

八月精通区块链开发，月薪四万很轻松，渐进式构建从原理到实战的知识体系，以太坊DApp项目从0到1实战演示。

运用wireshark抓包DNS并分析流程 - CSDN博客

客户端向DNS服务器发出请求,服务器找到后直接返还给客户端,这是递归查询 2. ...结合Wireshark捕获分组深入理解DNS协议 一、概述 1.1 DNS 识别主...
2018-6-26

结合Wireshark捕获分组深入理解DNS协议 - CSDN博客

用Wireshark捕获的DNS报文如下图,显然第一行是DNS查询报文,第二行是DNS回答报文... 回答区域包含了最初请求名字的资源记录,一个回答报文的回答区域可以...
2018-6-18

DNS报文格式及DNS查询程序

From: <http://blog.csdn.net/wangyifei0822/archive/2008/04/23/2316857.aspx> DNS报文格式：该报文12字节的首部和4个长度可变的字...

 codejoker 2009-06-23 13:27:00 阅读数：11805

DNS查询报文和应答报文抓包分析 - CSDN博客

回车就可!!!在科学上网看到捕获的数据了 捕获到的DNS查询报文为82个字节 前50个 前两个字节是标识 为0x21FF 此标识为发出请求的客户端随意设置的


SIP中的DNS查询过程 - CSDN博客

1.SIP中的DNS过程 1.1.SIP消息涉及的DNS过程 SIP消息涉及到的DNS过程主要包括两个方面:一方面是如何发送请求消息,发送方需要通过DNS过程得到传输层协议类型,下一...

2018-6-20


深入理解DNS报文格式

(一) DNS报文格式 (1) 公共报文头格式其中header报文头是必须有的,其他的有没有在报文头里有定义: 标识ID: 请求客户端设置的16位标示,服务器给出应答的时候会带相同的标示字...

 liao152 2015-04-24 22:24:06 阅读数: 9358

DNS原理总结及其解析过程详解

一、域名系统 1、域名系统概述 域名系统DNS(Domain Name System)是因特网使用的命名系统,用来把便于人们使用的机器名字转换成为IP地址。域名系统其实就是名字系统...

 yipiankongbai 2014-05-07 13:10:01 阅读数: 73670

利用winpcap测量DNS查询时延和TCP连接时延 - CSDN博客

用于捕获网络数据包并进行分析的开源库,如果没有学过,可以点击[这里](#)看一下教程,...因为DNS 查询时延是指从“终端向DNS服务器发起查询请求”到“终端收到DNS 服务...

2018-7-12


Wireshark-DNS数据报分析 - CSDN博客

DNS:域名系统 DNS是一种用于internet上提供IP地址和域名相互映射的分布式服务系统。可以通过IP地址获取相应的域名,也可以通过域名获取IP,这样可以不用记住难记的IP。 ...

2018-7-15

DNS查询报文和应答报文抓包分析

这个学期开始上计算机网络课,第一份与协议有关的作业就是DNS报文分析,那就分别抓一个DNS查询报文和应答报文看一下吧。 我使用的抓包软件是科来网络分析系统2010技术交流版,可以从[htt...](#)

 jingxinzhouxiaoyu 2015-11-03 14:18:40 阅读数: 301

东京几乎没人知道，玩微信能增加3份工资！

枫歌商贸 · 顶新

利用WireShark进行DNS协议分析 - CSDN博客

用Wireshark捕获的DNS报文如下图,显然第一行是DNS查询报文,第二行是DNS回答报文...该标识会被复制到对应的回答报文中,客户机用它来匹配发送的请求与接收到的回答...

2018-7-10


利用WireShark进行DNS协议分析 - CSDN博客

用Wireshark捕获的DNS报文如下图,显然第一行是DNS查询报文,第二行是DNS回答报文...该标识会被复制到对应的回答报文中,客户机用它来匹配发送的请求与接收到的回答...

2018-7-11

结合Wireshark捕获分组深入理解DNS协议

一、概述 1.1 DNS 识别主机有两种方式: 主机名、IP地址。前者便于记忆(如www.yahoo.com),但路由器很难处理(主机名长度不定);后者定长、有层次结构,便于路由器处理,但难...

 zhaqiwen 2014-01-09 19:56:48 阅读数: 12479

```
#-*-coding:utf-8-*- import socket def ana_head(q,n): list1 = [] print u'包长度%d'%len(q) pr...
```

 u0113919022015-02-24 14:35:27阅读数：1498

结合Wireshark分析DNS 协议 - CSDN博客

用Wireshark捕获的DNS报文如下图,显然第一行是DNS查询报文,第二行是DNS回答报文... 回答区域包含了最初请求名字的资源记录,一个回答报文的回答区域可以...

2018-7-15

DNS请求分析

对当前 DNS 服务器进行 DNS 查询分析

 signmem2016-05-04 17:40:47阅读数：1089

DNS报文格式分析

资料出处: <http://hi.baidu.com/yslgoodboy/blog/item/f5cd47f562a95b7fdcc47401.html> DNS请求报文的结构是 0 ...

 wocjj2012-05-27 00:42:47阅读数：2937

运用wireshark抓包DNS并分析流程

一. 访问dns本机域名 1. 客户端抓包 客户端向目标主机dns查询www.mc.snccsummarschool.top 挂了VPN也可以走ipv6 这个域名在DNS主机中, 所以直接...

 Kai_Chan2016-10-16 20:57:03阅读数：8496

DNS完整报文分析

先来一张图了解以太网数据帧从数据进入协议栈的

 jin6155679752014-07-11 17:13:59阅读数：809

DNS报文解析

打开wireshark, 并在IE浏览器输入www.163.com, 抓到DNS数据包, 作如下解析。一、 DNS请求报文(略去前面的Ethernet,IP,UDP头部) 0000 a0 7d 01 0...

 zhangyang04022009-05-07 11:41:00阅读数：8233

对DNS应答报文的解析及简单处理代码

这几天因为要做一个事情, 又因为没有现成的工具使用, 一直在找DNS报文的相关资料, 最终在国外找到一篇关于DNS的MX查找的代码, 但是发现直接将它套用到A记录查询并不合适, 只好继续找, 直到昨晚, 找到了。关...

 gfover2009-12-14 23:24:00阅读数：5530

抓包报文分析

虽然用到的抓包工具次数比较多, 但是还是记不住这些16进制代码的含义。上次参加CTF竟然有这样的题, 今天有时间就分析了一下, 记下来 00 23 69 B7 81 24 0C 82 68 56 ...

 chaoyueziji1232015-08-11 16:39:24阅读数：1489

Internet协议分析-TFTP报文分析-DNS 报文分析

2014年04月23日427KB

下载

DNS协议详解及报文分析

转自: <https://jocent.me/2017/06/18/dns-protocol-principle.html#respond>DNS协议详解及报文格式分析解BUG的过程中碰到了DNS相关的内容...

 ABC80809692018-04-17 15:39:47阅读数：13

DNS报文格式分析



免费云主机试用一年

云主机免费推荐吗

抓包分析IP报文结构

IP报头结构IPv4的头部结构如图所示。其长度通常为20字节，除非含有可变长的选项部分 ·4位版本号：指定的IP协议的版本。对IPv4来说，其值是4。 ·4位头部长度：标识该IP头部有多少个32bit...

MBuger 2017-06-30 15:45:17 阅读数：1995

DNS报文

原文出自下边是DNS报文的大致格式： +-----+-----+ | 标识 (最重要的 ...

jxfgh 2010-04-06 00:13:00 阅读数：2554

个人资料



zhjf14

关注

原创	粉丝	喜欢	评论
29	37	5	15

等级：	博客 5	访问：	22万+
积分：	3320	排名：	1万+



二合一笔记本



最新文章

- 程序调用ShellExecuteEx打开其他程序（兼容UAC获取管理员权限）
- duilib入门问题集
- 公历转农历算法
- TinyXML：一个优秀的C++ XML解析器
- Hook学习笔记

个人分类

C/C++/objective-c	108篇
MFC	76篇
Windows	101篇
Mac	9篇

0

写评论

收藏

微信

微博

QQ

展开

归档

2015年11月

2篇

2015年7月

1篇

2015年1月

4篇

2014年12月

4篇

2014年11月

1篇

展开

热门文章

“问题事件名称：BEX 故障模块名称：Stack Hash_9fba”的解决办法
阅读量：12146

MPMoviePlayerController 获取视频缓冲大小
阅读量：4333

解决Cygwin "error while loading shared libraries"的问题
阅读量：3913

CLGeocoder获取当前所在的城市名
阅读量：3614

iphone获取本机电话号码 iPhone获取通讯录里电话号码
阅读量：3267

最新评论

CoCreateInstance ...
qq_35439491：重新注册了，还是老样子，没用

CComboBox使用SetWin...
weiwei22844：very good！

“问题事件名称：BEX 故障模块名...
kangear：您这是开发中遇到的，如果是在就一个exe软件的情况下如何办呢？

MPMoviePlayerCont...
jiayou8809：[reply]hc373941091[/reply] 还真没测试过这种情况，有快一年没搞ios了

MPMoviePlayerCont...
hc373941091：你好！ 你是否有测试过MPMovieP layerController 在 gprs或者其它低网速下...