**Wireshark抓包实例分析**

（一）.WireShark的使用： (1)启动WireShark。(2)启动PC上的IE浏览器。 (3)开始分组捕获：选择“抓包”下拉菜单中的“抓包参数选择”命令，在 “WireShark:抓包选项”窗口中可以设置分组捕获的选项。 (4)在这次实验中，使用窗口中显示的默认值。选择“抓包”下拉菜单中的 “网络接口”命令，显示计算机中所安装的网络接口（即网卡）。我 们 需 要 选择电脑真实的网卡，点击后显示本机的IP地址。 (5)随后，点击“开始”则进行分组捕获，所有由选定网卡发送和接收的分 组都将被捕获。 (6)待捕获一段时间，关闭浏览器，选择主窗口中有的“stop”按钮，可以 停止分组的捕获。 (7)选择“文件”下拉菜单中的“另存为”，保存到我的文档中。

(二).结果分析：

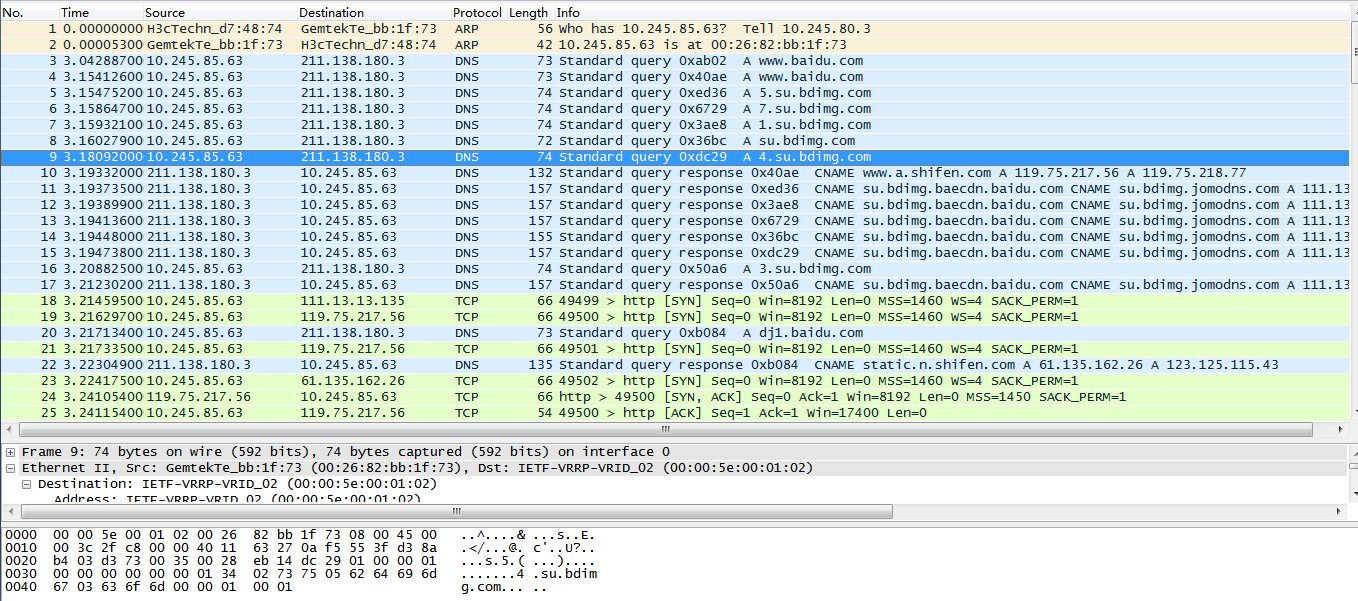


图1，Wireshark抓包窗口布局

Wireshark的抓包结果整个窗口被分成三部分，最上面为数据包列表，用来显示截获的每个数据包的总结性信息；中间为协议树，用来显示选定的数据包所属的协议信息；最下面是以十六进制形式表示的数据包内容，用来显示数据包在物理层上传输时的最终形式。

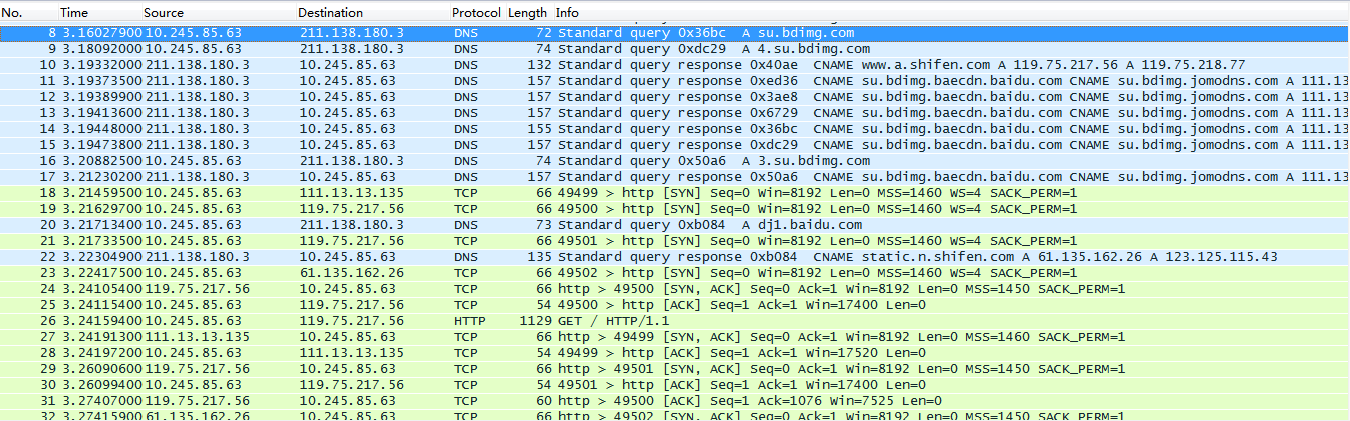


图2，Wireshark数据包列表

上图的数据包列表中，第一列是编号（如第20个包），第二列是截取时间（3.21713400），第三列Source是源地址（10.245.85.63），第四列Destination是目的地址（211.138.180.3），第五列Protocol是这个包使用的协议DNS，第六列是数据包帧的长度，第七列Info是一些其他的信息，包括源端口号和目的端口号。

Wireshark中某些协议字段会以特殊方式显示：

1， Generated fields/衍生字段 Wireshark会将自己生成附加协议字段加上括号。衍生字段是通过该包的相关的其他包结合生成的。例如Wireshark 在对TCP流应答序列进行分析时。将会在TCP协议中添加[SEQ/ACK analysis]字段  2，Links/链接 如果Wireshark检测到当前包与其它包的关系将会产生一个到其它包的链接。链接字段显示为蓝色字体并加有下划线。双击它会跳转到对应的包

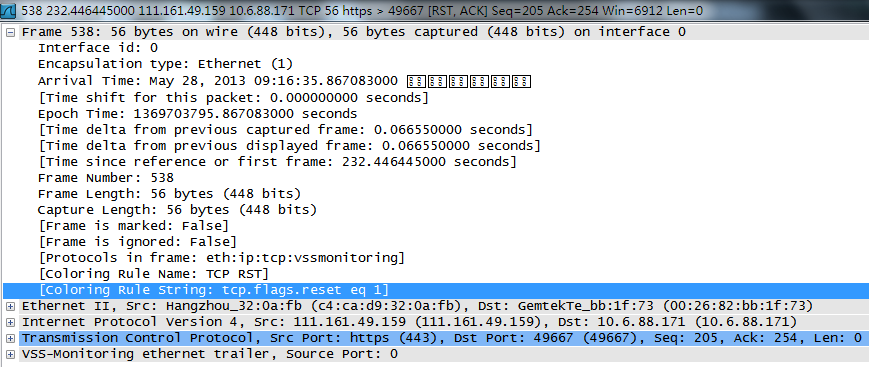


图3，应用层信息

到达时间：2013年5月28日 09:16:35.867083000

新纪元时间：1369703795.867083000秒

捕获该帧与前一帧的时间间隔是0.066550000秒

显示陈列出该帧与前一帧的时间间隔是0.066550000秒

从捕获第一帧到捕获该帧所用时间为232.446445000秒

帧号（相对）：538

该帧的长度是56字节（448比特）

捕获的的帧长度56字节（448比特）

帧包含的协议：TCP/IP

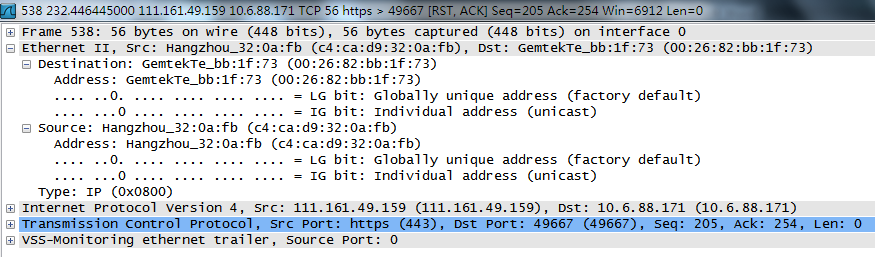


图4，物力层信息

该部分是物理层的相关信息，包含了源端物理地址c4:ca:d9:32:0a:fb和目的端的物理地址00：26：82：bb:1f:73。

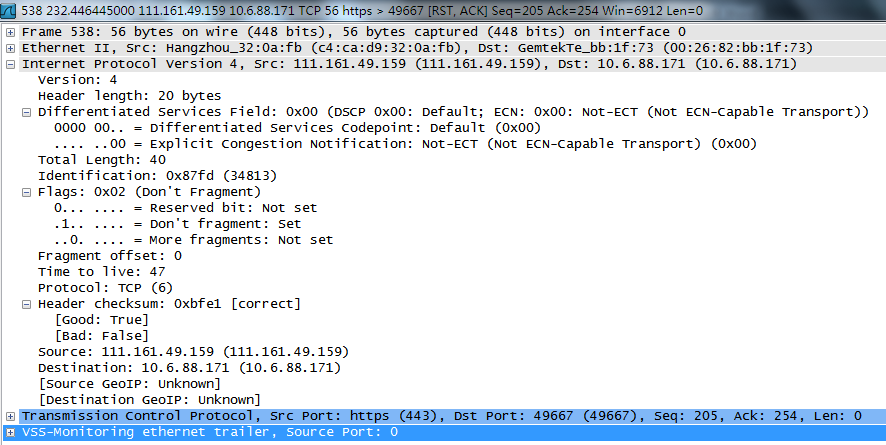


图5，IP协议

这是IP协议，属于网络层可得如下信息：

源地址：111.161.49.159

目的地址：10.6.88.171

版本号：IPv4

头部长度：20字节

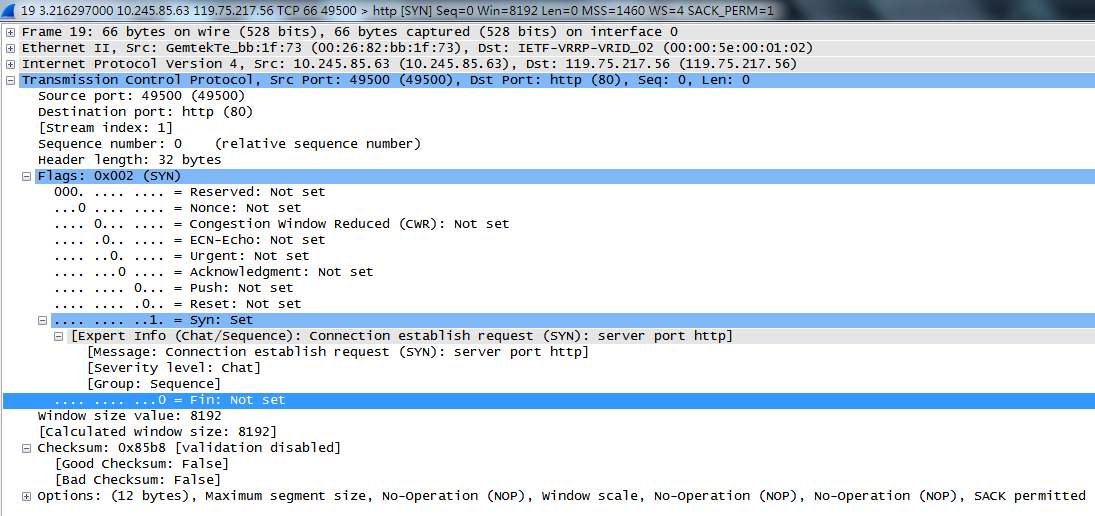
区分服务域：0x00

分段策略：不分段

TTL（生存时间）：47

头部校验和：0xbfe1(接受正确)

**TCP协议的抓包分析**



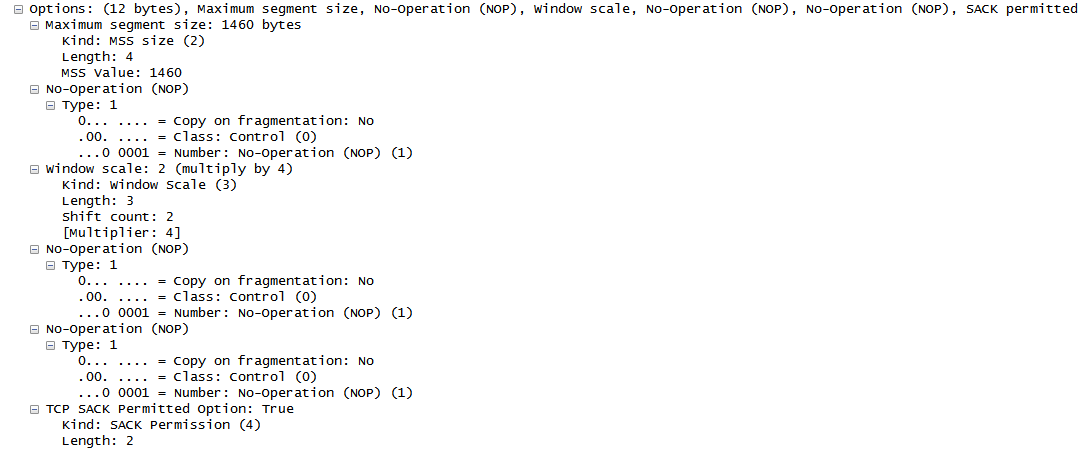


图6，TCP协议中请求建立连接

首先，注意到该报文的同步位S Y N字段为1，因此该报文为建立连接的报文。选择的seq为0，SYN为1的报文段不能携带数据，但要消耗掉一个序号。窗口个数为8192。Option字段中指明了最长字段长度为1460字节。此后，TCP客户进程进入SYN-SENT（同步已发送状态。图6即为TCP协议建立连接过程中的三次握手中的第一次握手。

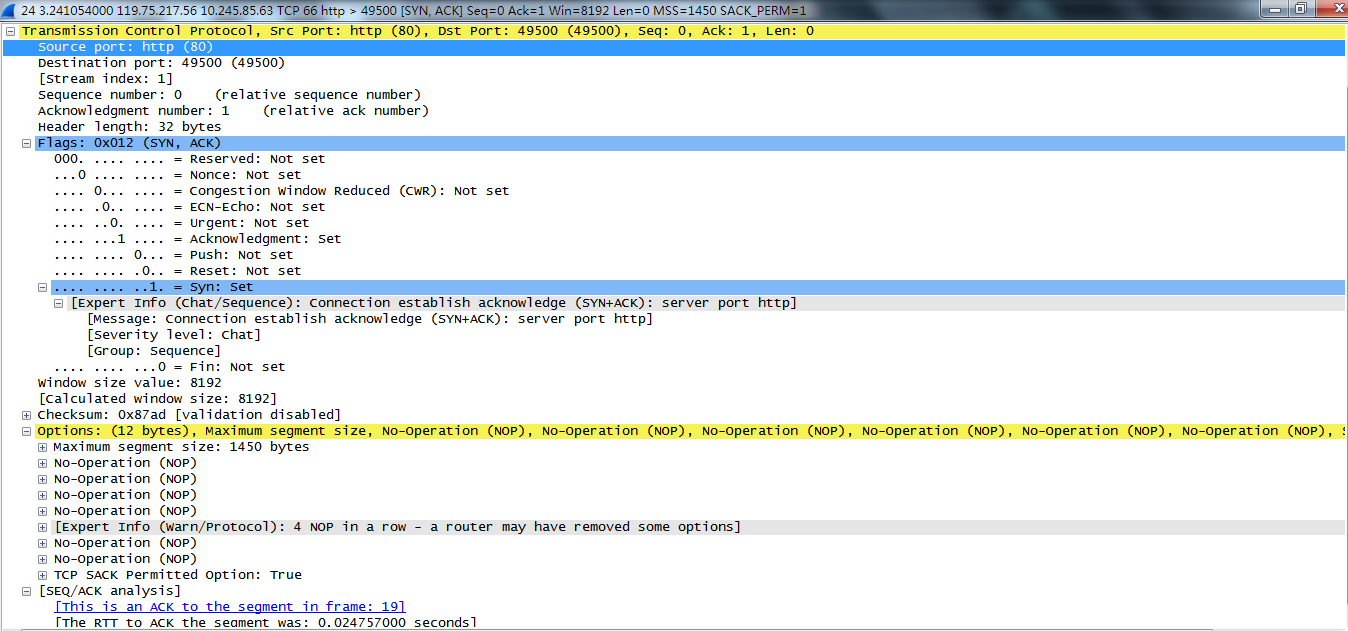


图7， 服务器返回请求建立连接的确认

图7表示出了服务器向用户返回请求建立连接报文的确认字段，其中SYN为1，ACK为0+1。传送的数据序列号为0。窗口大小仍然为8192。此报文段也不能携带数据，但同样消耗掉一个序号。这是TCP服务器进程进入SYN-RCVD（同步受到）状态。图7即为TCP协议建立连接过程中的三次握手中的第二次握手。

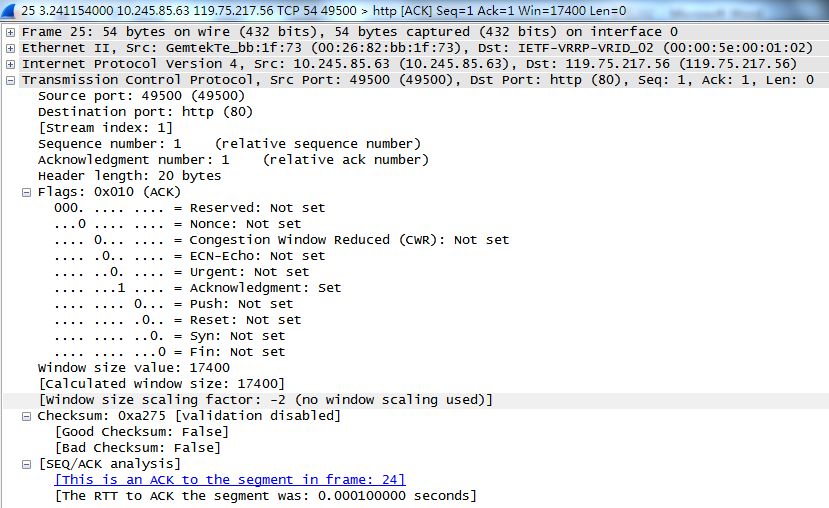


图8，建立连接的“第三次握手”

从图8中可以看出窗口长度是一个变量。并且首部长度字段为20，没有option字段。确认报文段的ACK置1，确认号ACK=0+1,自己的序列号seq=0+1,TCP的标准规定，ACK报文段可以携带数据。但如果不携带数据则不消耗序号。这时，TCP连接已经建立，发送方进入ESTABLISHED（已建立连接）状态。

上图中，图6、图7、图8代表了TCP协议建立连接时的三次握手。

UDP**协议的抓包分析**

用户数据报UDP有两个字段：数据字段和首部字段。是一种固定包头格式的协议，其头部共64bit，包含4个等长的部分，分别表示原端口号、目的端口号、UDP报文段长度以及校验和。根据UDP首部固定长度的特点，其长度字段最大能表示65536字节，那么一个UDP协议最多能够包含的数据长度即为65528字节。源端口号：关于端口号有一些规定，服务器端通常用熟知端口号，通常在0-1023之间。而客户端用随机的端口号，其范围在49152到65535之间。目的端口号。长度：包括报头和数据的长度之和。在[8，65535]区间。检验和：提供差错检测功能。

**UDP检验和的计算：**

UDP的检验和所需信息：①UDP伪首部：源IP + 目的IP + Byte 0 + Byte 17+ UDP长度，其目的是让UDP两次检查数据是否已经正确到达目的地，只是单纯为了做校验用的。②UDP首部：该长度不是报文的总长度，而只是UDP（包括UDP头和据部分）的总长度③UDP的数据部分。

校验和的计算步骤：①把伪首部添加到UDP上；②计算初始时将检验和字段添零的；③把所有位划分为16位（2字节）的字④把所有16位的字相加，如果遇到进位，则将高于16字节的进位部分的值加到最低位上。⑤将所有字相加得到的结果应该为一个16位的数，将该数按位取反则可以得到检验和。

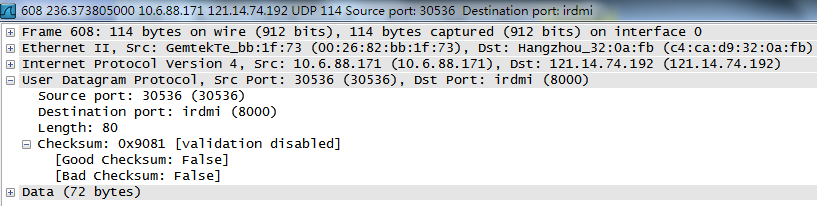


图9，UDP协议

这是UDP协议，可得以下信息：

源端口号：30536

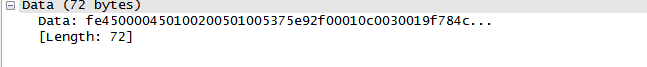
目的端口号：8000

总长度：80

校验和：0x9081

经校验：有残缺

整个协议长度为：80字节，从数据部分的长度为72字节也可以看出头部为8字节，刚好是16\*4bits。



Data是UDP协议的具体内容

**HTTP协议的抓包分析**

HTTP协议（HyperText Transfer Protocol，超文本传输协议）是互联网上应用最为广泛的一种网络协议。它是一个应用层协议，由请求和响应构成，是一个标准的客户端服务器模型。所有的www文件都必须遵守这个标准。它是客户端浏览器或其他程序与Web服务器之间的应用层通信协议。在Internet上的Web服务器上存放的都是超文本信息，客户机需要通过HTTP协议传输所要访问的超文本信息。HTTP包含命令和传输信息，不仅可用于Web访问，也可以用于其他因特网/内联网应用系统之间的通信，从而实现各类应用资源超媒体访问的集成。

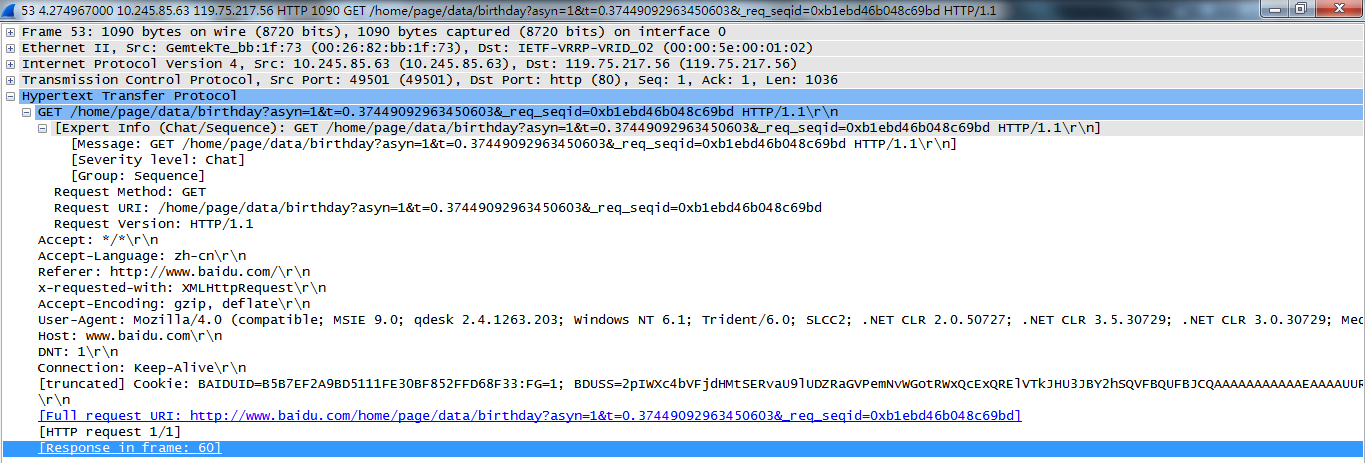
它可以使浏览器更加高效，使网络传输减少。它不仅保证计算机正确快速地传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示(如文本先于图形)等。HTTP协议通常承载于TCP协议之上，有时也承载于TLS或SSL协议层之上，这个时候，就成了我们常说的HTTPS。

图10，http客户端请求报文

应用层直接向用户提供服务，是计算机网络与用户界面的接口，HTTP就是适用于应用层的一种超文本传输协议，由上图可得：显然可见，HTTP使用传输层协议是TCP，方法字段大多数为GET（少数会使用POST，经过筛选如图11所示仅有第81帧使用POST）。HTTP的请求行为GET/HTTP/1.1\r\n，由GET可知此次为客户端向服务器发送请求，后继的行为首部行，HTTP版本为HTTP1.1； Accept\_language为zh-ch,表示它指定的自然语言是简体中文；Accept\_Encoding:gizp,deflate,表示指定的编码为gizp,deflate；User-Agent=Mozilla/4.0(compatible;MISE 9.0;windows NT 6.1;…….) 告诉了服务器我所使用的网页浏览器；Host= ww.baidu.com表示主机名为ww.baidu.com；Connection=keep-Alive表示保持持续连接。

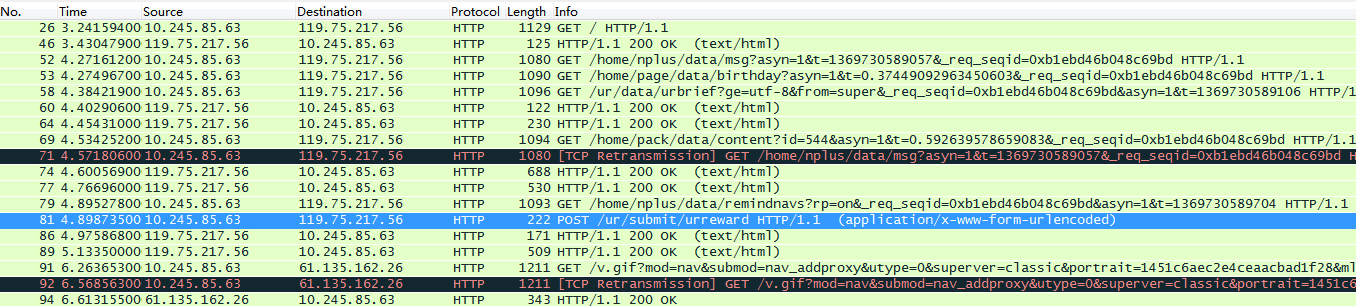


图11，用POST为方法字段的81

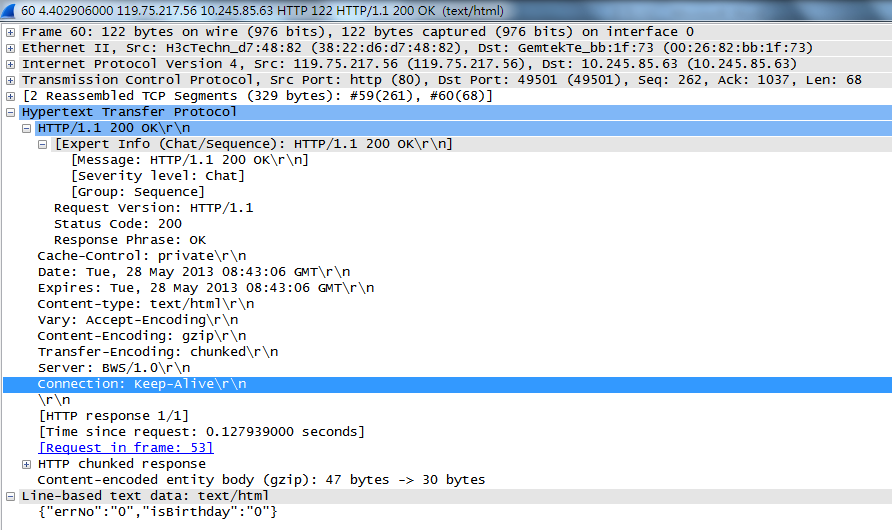


图12，HTTP服务器响应报文

服务器的响应报文如图七所示：蓝色的那一行为初始状态行，接下来的六行为首部行。可以从

[ Request in frame :53]

看出，此响应报文是响应图11的编码为53的请求报文

**DNS协议的抓包分析**

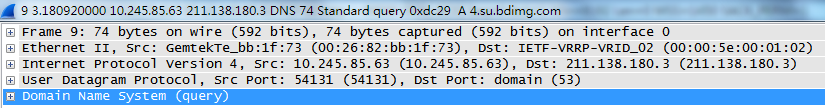
****

图13，协议树

其中，第一行为该包的信息，第二行为以太网，属于链路层，第三行为IP协议，属于网络层（源IP与目的IP显示在该行），第四行为UDP协议，属于传输层，第五行为DNS的有关数据。下面将通过图三详细分析DNS报文的内容。

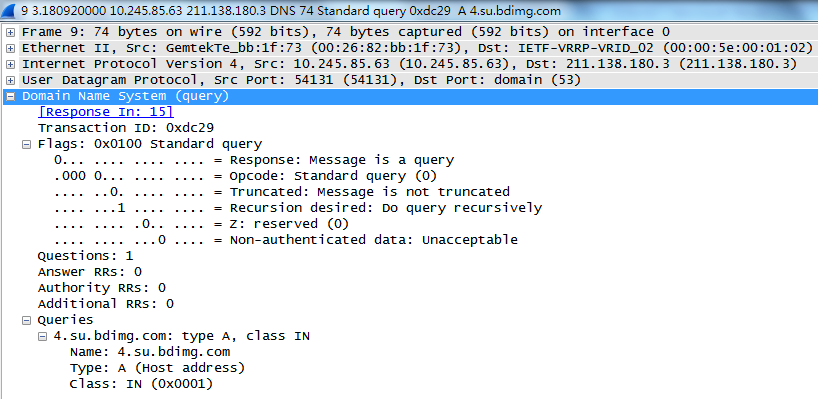


图14，DNS请求查询报文

这是一个请求查询的报文（0），该报文没有被删节，采用的是递归调用的查询，答复在NO15中。随机产生一个校验数0xdc29，问题数为1，回答RR数，权威RR数以及附加RR数均为0。在问题区域显示了名字字段与被查询的问题类型A（即主机地址）。

注：Transaction ID 是随机产生的，DNS服务器返回dns应答信息时，使用的 Transaction ID 必须和你询问时使用的一致，才会被机器接受。

Queries表明询问的域名为su.bdimg.com,询问类型为A，即希望希望能够回答所对应的机器名IP地址，类域值为0x0001,表示Internet数据。

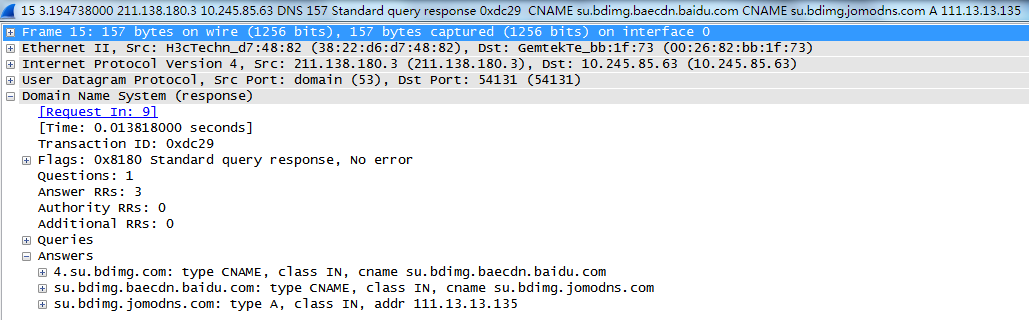


图15，DNS回答报文

第二个包即为回答报文，格式与查询报文类似（如图14所示），特别说明一点type类型为CNAME，说明规范主机名为su.bdimg.baecdn.baidu.com，IP地址：111.13.13.135。是对NO9的答复。可见此处随机产生的校验数为0xdc29,与询问时的检验数一致，故能够被接受。

问题区内的问题是要得到域名su.bdimg.com的IP地址，答案区内有两条回复，第一条是域名的别名CNAME, su.bdimg.com,第二条是请求类型为A的记录得域名对应的IP地址为111.13.13.135。

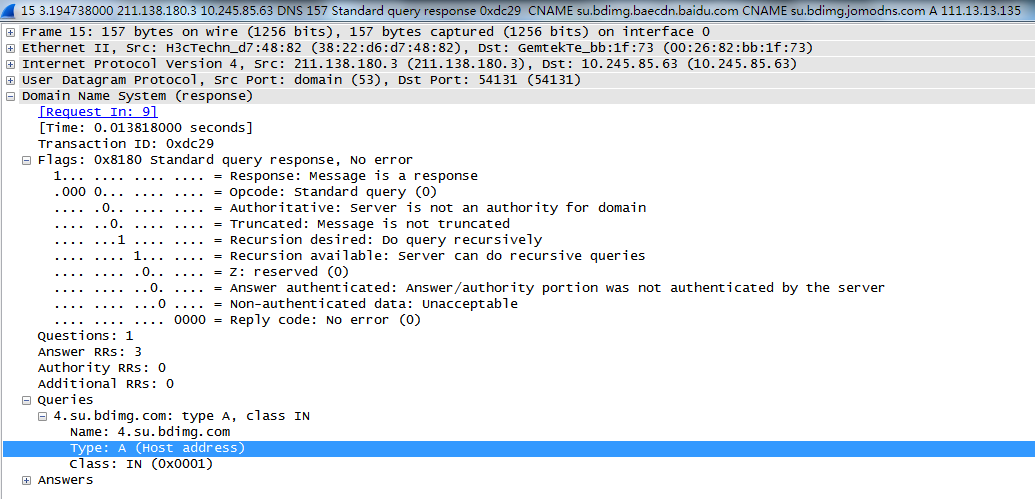
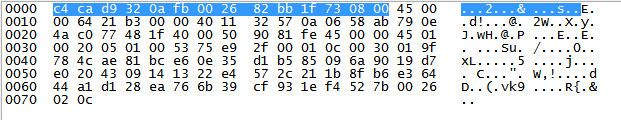


图16

由表15中的域名服务器报文参数域各位意义可知，该报文是条标准响应报文，不是权威性的回答，且报文未被截断，报文希望递归，并可以递归，报文保留，报文回复无错。问题区内，问题信息数为1，在答案区内，答案的数目为3，管理机构数与附加信息数都为0。

**十六进制数据包内容：**



图。17

这是以十六进制显示的数据包的具体内容，是被截获的数据包在物理媒体上传输时的最终形式，当在协议树中选中某行时，与其对应的十六进制代码同样会被选中，方便对各种协议的数据包进行分析。

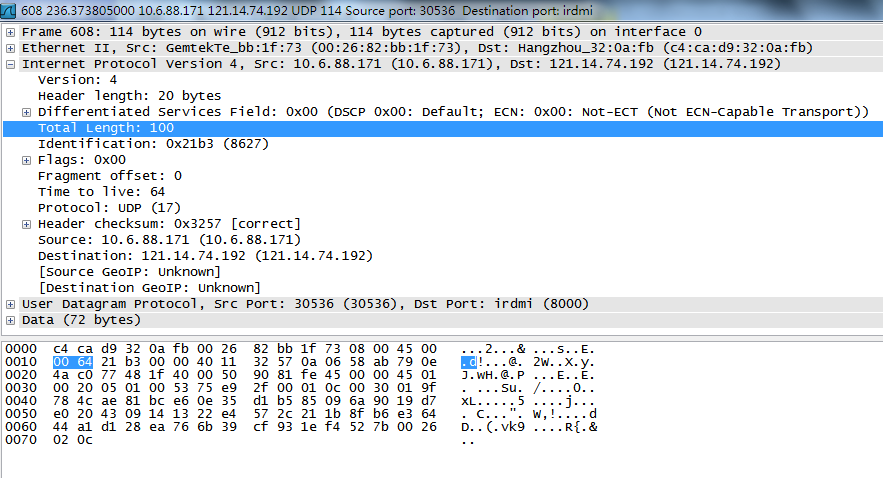


图18

如图，当选中Total Length：100，它的十六进制表示0x0064，从下面蓝色选中区域可以看到00在前面，64在后面，即高字节数据在低地址，低字节数据在高地址（图中地址从上到下从左到右依次递增），由此可知，网络字节序采用的是大端模式。