



# 计算机网络实验九

## 域名系统 (DNS)

信息学部 朱婉婷

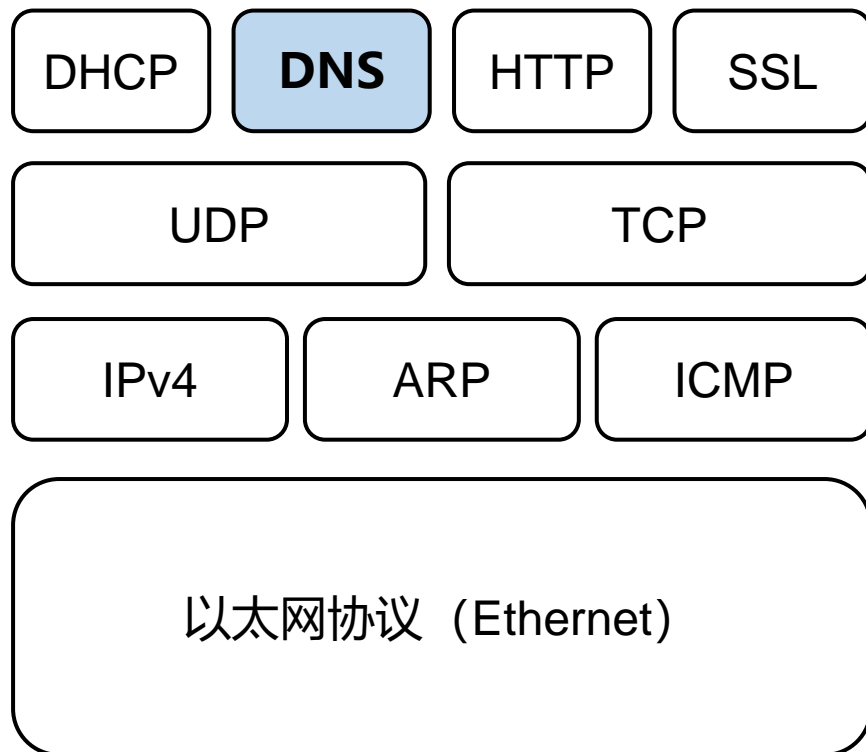
# 主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

# DNS简介

## ◆域名系统 DNS (Domain Name System)

- 采用分层次的、基于域的命名方案和分布式数据库，实现域名到IP地址映射的系统。
- 域名解析：通过名字查找对应主机的IP地址的过程。
- 使用户更方便的访问互联网，而不用去记住每台设备的IP地址。
- DNS协议是应用层协议，运行在UDP协议之上，使用端口号53。



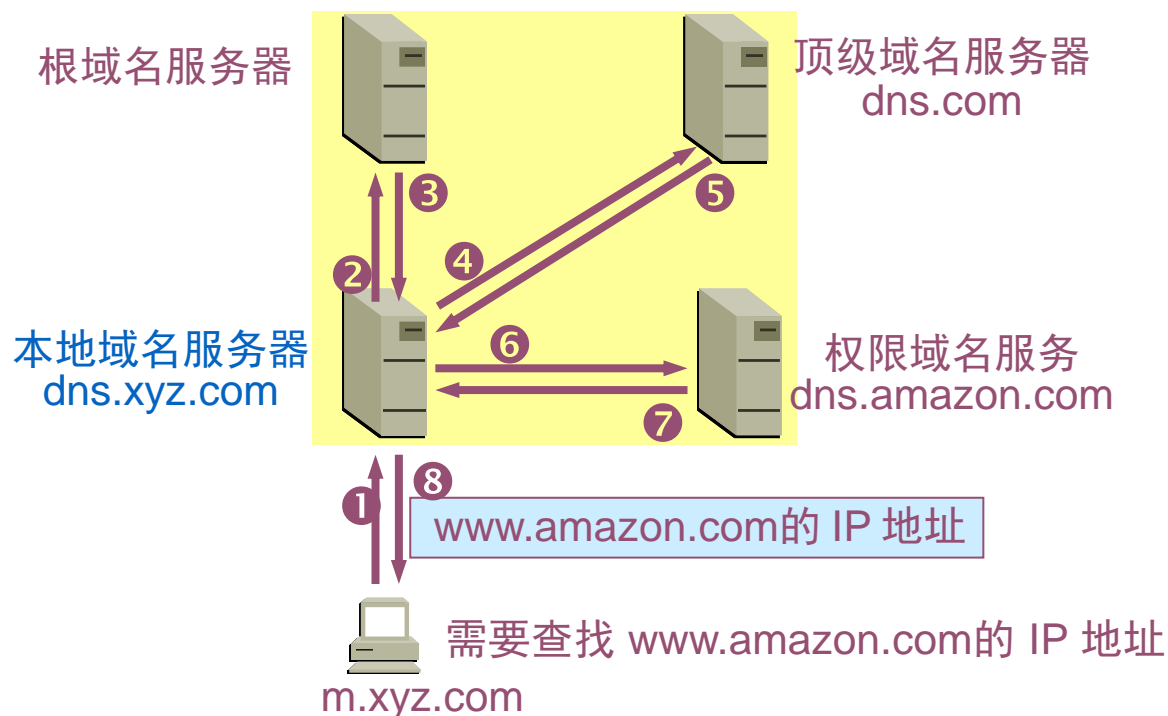
# DNS解析过程

- 在解析域名时，可以首先采用静态域名解析的方法，如果静态域名解析不成功，再采用动态域名解析的方法。
- 一些常用的域名，可以放入静态域名解析表中，这样可以大大提高域名解析效率。

# DNS解析过程

## ◆迭代查询

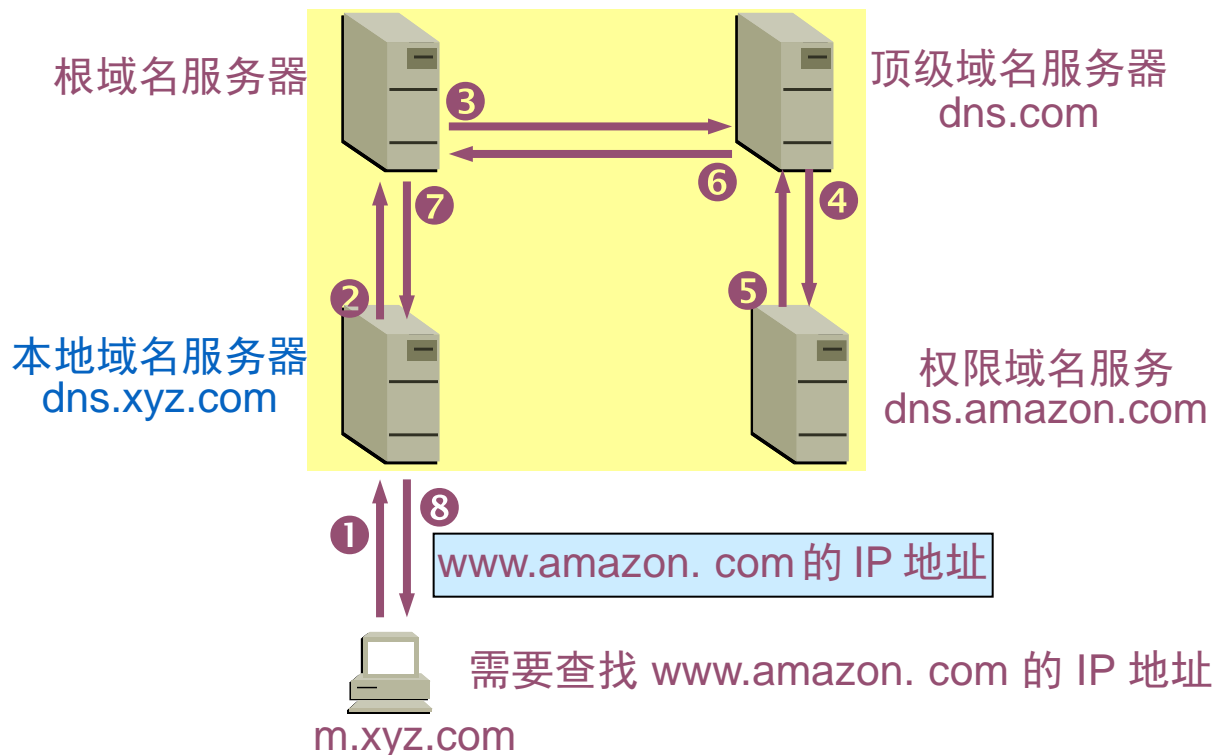
- 当根域名服务器收到本地域名服务器的**迭代查询**请求报文时，要么给出所要查询的 IP 地址，要么告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让**本地域名服务器进行后续的查询**。



# DNS解析过程

## ◆递归查询

- 如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向根域名服务器继续发出查询请求报文。

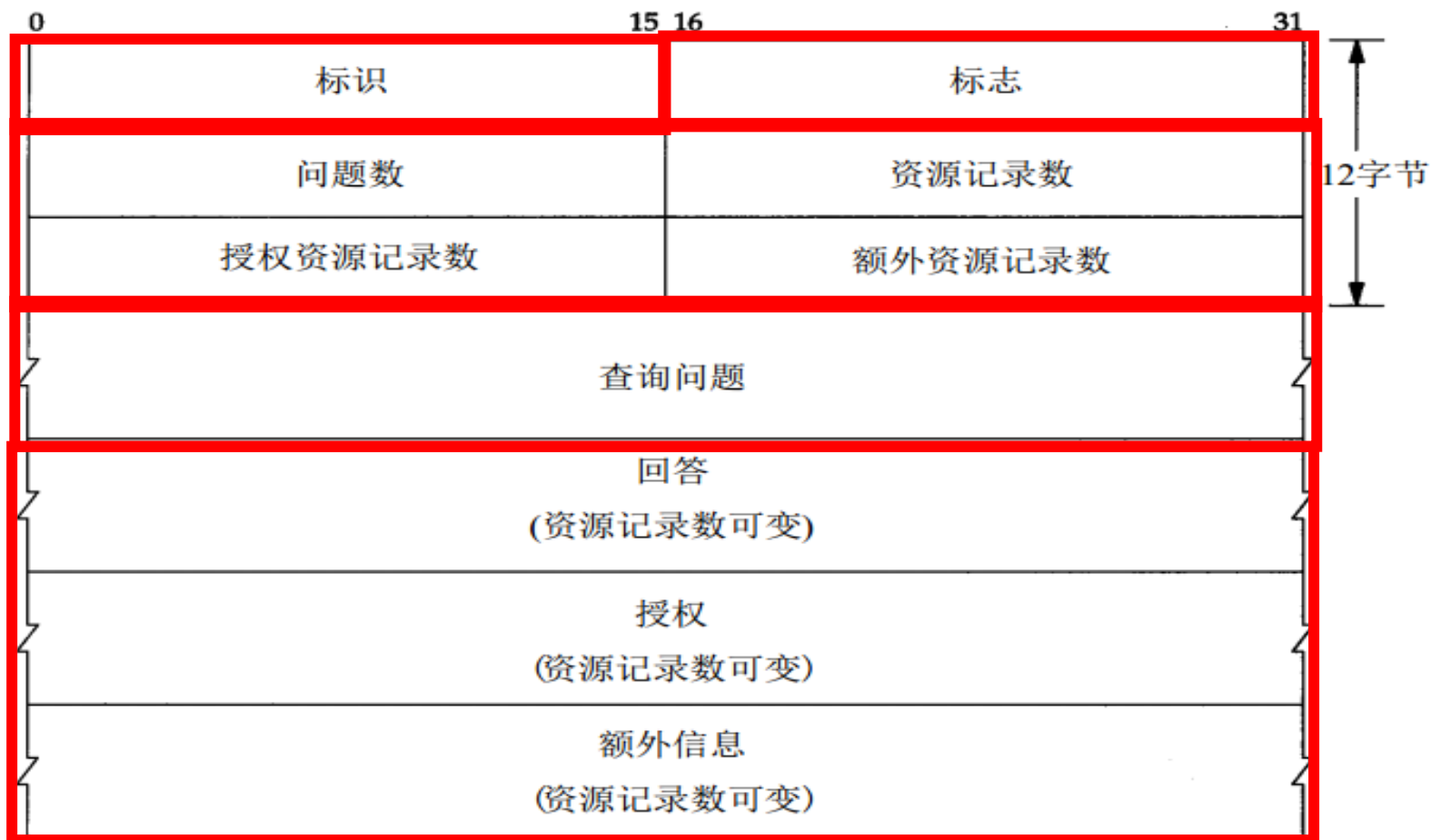


# DNS缓存

- 每个域名服务器都维护一个**高速缓存**，存放最近用过的名字以及从何处获得名字映射信息的记录。
- 为保持高速缓存中的内容正确，域名服务器应为每项内容设置计时器，一段时间过后，**缓存条目失效（删除）**。
- 本地域名服务器一般会**缓存顶级域名服务器**的映射。
  - 因此根域名服务器不经常被访问。

# DNS报文格式

- DNS只有两种报文：**查询报文**、**响应报文**，两者有着相同格式。



DNS查询和响应的一般格式



# DNS报文格式

- **标识**：16位。对该查询进行标识，该标识会被复制到对应的回答报文中，客户端用它来匹配发送的请求与接收到的应答。
- **标志**：16位。

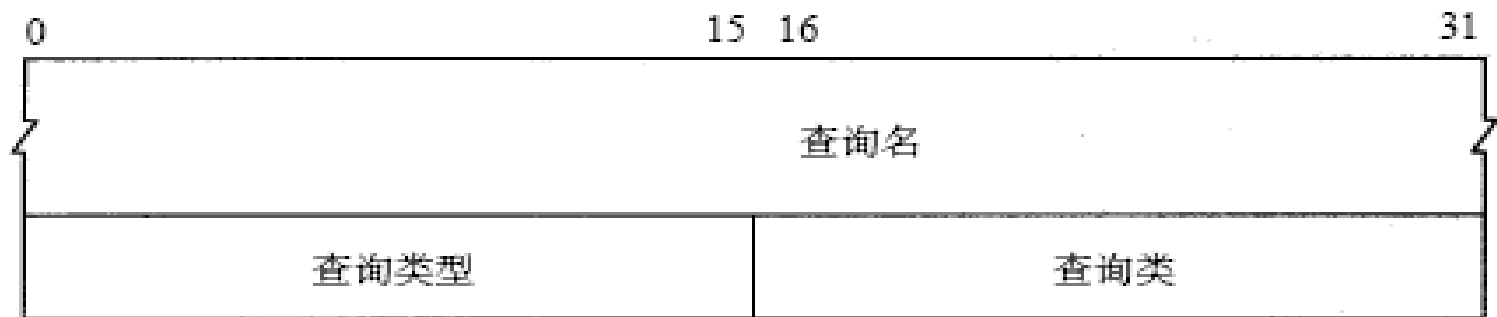
QR	opcode	AA	TC	RD	RA	(zero)	rcode
1	4	1	1	1	1	3	4
- **QR**(1bite)：查询/响应的标志位，1为响应，0为查询。
- **opcode**(4bite)：定义查询或响应的类型(若为0则表示是标准的，若为1则是反向的，若为2则是服务器状态请求)。
- **AA**(1bite)：授权回答的标志位。该位在响应报文中有效，1表示名字服务器是权限服务器(关于权限服务器以后再讨论)
- **TC**(1bite)：截断标志位。1表示响应已超过512字节并已被截断，0表示没有发生截断。
- **RD**(1bite)：是否希望得到递归回答，该位为1表示客户端希望得到递归回答。
- **RA**(1bite)：只能在响应报文中置为1，表示可以得到递归响应。

# DNS报文格式

- **zero**(3bite): 保留字段。
- **rcode**(4bite): 返回码, 表示响应的差错状态, 通常为0和3, 各取值含义如下: 0:无差错; 1:格式差错; 2:问题在域名服务器上; 3:域参照问题; 4:查询类型不支持; 5:在管理上被禁止; 6--15:保留。
- **Quetions**(问题数 2字节) : 这一部分包含了一个或多个问题记录, 在查询报文和响应报文中都会出现。
- **Answer RRs**(资源记录数), **Authority RRs**(授权资源记录数), **Additional RRs**(额外资源记录数)只在响应报文中出现。

# DNS报文格式

- DNS问题区域的格式:



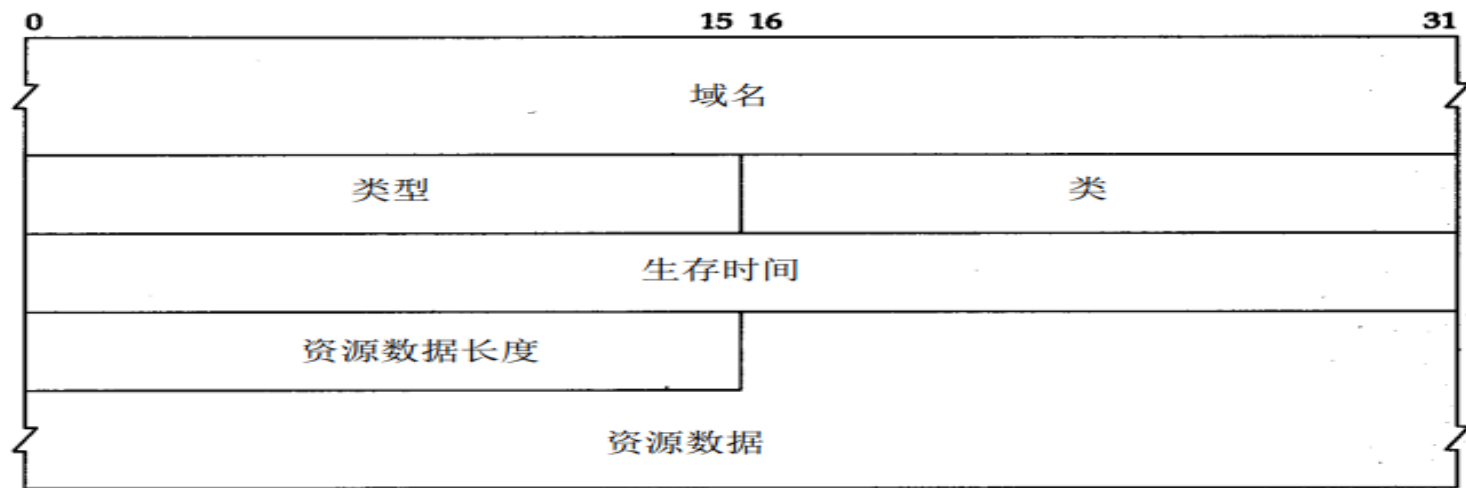
- 查询名**: 长度不定, 一般为要查询的域名(也会有IP的时候, 即反向查询)。此部分由一个或者多个标示符序列组成, 每个标示符以首字节数的计数值来说明该标示符长度, 每个名字以0结束。计数字字节数必须是0~63之间。例如查询域名为 “www.bjut.edu.cn”, 实际的存储结构如下:

4	b	j	u	t	3	e	d	u	2	c	n	0
---	---	---	---	---	---	---	---	---	---	---	---	---

- 查询类型**: 表明需要进行的服务类型, 一般为A (IP地址查询)。
- 查询类**: 通常是1, 指互联网地址 (IN)。

# DNS报文格式

- DNS报文中最后的三个区域，回答区域、授权区域和额外信息区域，均采用一种称为**资源记录RR** (Resource Record) 的相同格式。
- **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包含多条资源记录RR(因为一个主机名可以对应多个IP地址，冗余Web服务器)。
- **授权区域**包含了其他权威DNS服务器的记录。
- **额外信息区域**包含其他一些"有帮助"的记录。



DNS资源记录格式

# DNS报文格式

- **域名**：包含了域名的可变长度字段。它是问题记录中的域名的副本。由于DNS要求在名字重复出现的地方使用压缩，所以这个字段是问题记录中的域名的偏移量指针。
- **类型**：此字段与问题记录的查询类型字段相同。
- **类**：与问题记录中的查询类别字段相同。
- **生存时间**：用于指示该记录的稳定程度，该字段表示资源记录的生命周期(以秒为单位)，一般用于当地址解析程序取出资源记录后决定保存及使用缓存数据的时间。
- **资源数据长度**：表示资源数据的长度(以字节为单位)，如果资源数据为IP则为0004。
- **资源数据**：该字段是可变长字段，表示按查询段要求返回的相关资源记录的数据。

# 资源记录(RR, resource records)

- Type=A

- Name: 主机域名
- Value: IP地址

- Type=NS

- Name: 域(edu.cn)
- Value: 该域权威域名解析服务器的主机域名

- Type=CNAME

- Name: 某一真实域名的别名 (www.ibm.com-servereast.backup2.ibm.com)
- Value: 真实域名

- Type=MX

- Value: 与Name相对应的邮件服务器

# 主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

# 实验环境搭建

列出本次实验所使用的平台和相关软件，以下为例：

(打开cmd指令窗口，输入指令 “ipconfig /all”查看)

- 1、主机：联想笔记本（Win10系统）；主机IP地址：192.168.1.106；子网掩码：255.255.255.0；主机网卡MAC地址：34-F6-4B-C0-90-40。
- 2、网络连接方式：无线连接；默认网关地址：192.168.1.1。
- 3、抓包工具：Wireshark（v3.6.2）。

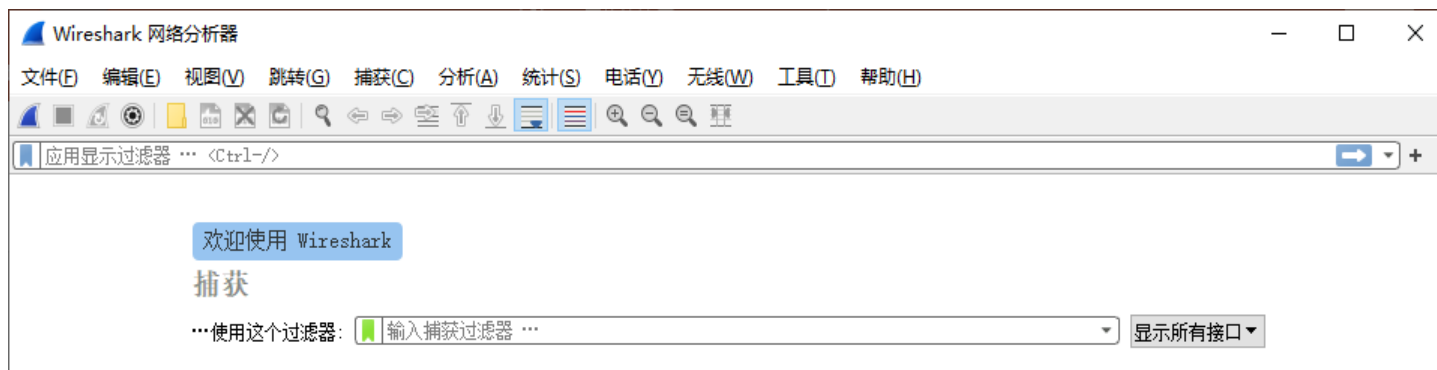


# 实验具体步骤

## ◆ 命令行模式下DNS有关的命令：

- **nslookup**：显示出当前系统所使用的DNS服务器地址；
- **ipconfig /flushdns**：清除DNS缓存信息。

1、打开Wireshark软件，双击本次实验正在使用的网络接口，开始进行抓包。



# 实验具体步骤

\*\*\*\*打开cmd窗口，输入命令 “ping www.bjut.edu.cn”，观察IP地址。

```
C:\Users\zwt717>ping www.bjut.edu.cn

正在 Ping bjut-edu-cn.cname.saaswaf.com [122.9.167.87] 具有 32 字节的数据:
来自 122.9.167.87 的回复: 字节=32 时间=44ms TTL=39
来自 122.9.167.87 的回复: 字节=32 时间=43ms TTL=39
```

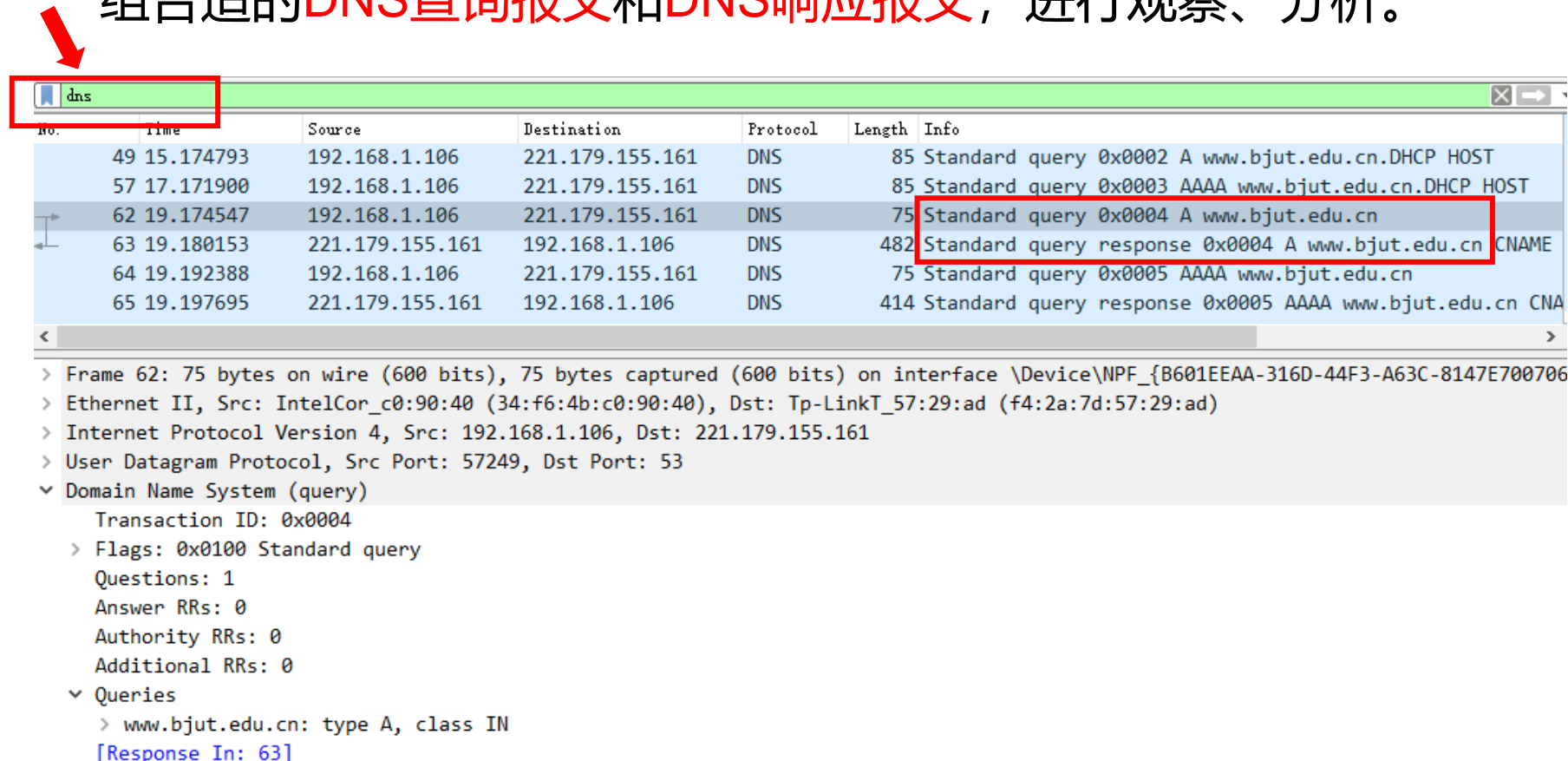
2、通过命令 “nslookup” 观察Web服务器IP地址、本地DNS服务器IP地址。例：主机的本地DNS服务器的IP地址为221.179.155.161。

```
C:\Users\zwt717>nslookup www.bjut.edu.cn
服务器:  cachedns03.bj.chinamobile.com
Address:  221.179.155.161

DNS request timed out.
        timeout was 2 seconds.
DNS request timed out.
        timeout was 2 seconds.
非权威应答:
名称:     bjut-edu-cn.cname.saaswaf.com
Addresses: 2001:250:100d:ffac:121:194:14:82
           2001:da8:2032:1006:10:0:213:51
           2001:da8:2032:1006:10:0:213:50
           2001:250:100d:ffac:121:194:14:83
           122.9.167.87
           116.211.138.205
Aliases:  www.bjut.edu.cn
           www1stwaf.bjut.edu.cn
```

# 实验具体步骤

3、停止抓包，在过滤器里输入“dns”过滤条件，从中选择一组合适的DNS查询报文和DNS响应报文，进行观察、分析。



The screenshot shows the Wireshark network protocol analyzer interface. The filter bar at the top contains the text "dns". Below it, a list of captured packets is displayed. Packet 62 is highlighted with a red box and a red arrow pointing to it. The packet details pane on the right shows the structure of the DNS query.

No.	Time	Source	Destination	Protocol	Length	Info
49	15.174793	192.168.1.106	221.179.155.161	DNS	85	Standard query 0x0002 A www.bjut.edu.cn.DHCP HOST
57	17.171900	192.168.1.106	221.179.155.161	DNS	85	Standard query 0x0003 AAAA www.bjut.edu.cn.DHCP HOST
62	19.174547	192.168.1.106	221.179.155.161	DNS	75	Standard query 0x0004 A www.bjut.edu.cn
63	19.180153	221.179.155.161	192.168.1.106	DNS	482	Standard query response 0x0004 A www.bjut.edu.cn CNAME
64	19.192388	192.168.1.106	221.179.155.161	DNS	75	Standard query 0x0005 AAAA www.bjut.edu.cn
65	19.197695	221.179.155.161	192.168.1.106	DNS	414	Standard query response 0x0005 AAAA www.bjut.edu.cn CNA

Frame 62: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF\_{B601EEAA-316D-44F3-A63C-8147E700706}

Ethernet II, Src: IntelCor\_c0:90:40 (34:f6:4b:c0:90:40), Dst: Tp-LinkT\_57:29:ad (f4:2a:7d:57:29:ad)

Internet Protocol Version 4, Src: 192.168.1.106, Dst: 221.179.155.161

User Datagram Protocol, Src Port: 57249, Dst Port: 53

Domain Name System (query)

- Transaction ID: 0x0004
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
  - www.bjut.edu.cn: type A, class IN

[Response In: 63]

# 主要内容

- 一、实验原理
- 二、实验步骤
- 三、实验结果及分析

# DNS查询报文

## 实验结果:

No.	Time	Source	Destination	Protocol	Length	Info
62	19.174547	192.168.1.106	221.179.155.161	DNS	75	Standard query 0x0004 A www.bjut.edu.cn
63	19.180153	221.179.155.161	192.168.1.106	DNS	482	Standard query response 0x0004 A www.bjut.edu.cn CNAME

> User Datagram Protocol, Src Port: 57249, Dst Port: 53
▼ Domain Name System (query)
Transaction ID: 0x0004
▼ Flags: 0x0100 Standard query
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
.... ..1 .... = Recursion desired: Do query recursively
.... ..0.. .... = Z: reserved (0)
.... ..0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
▼ www.bjut.edu.cn: type A, class IN
Name: www.bjut.edu.cn
[Name Length: 15]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)

[Response In: 63]

首部区域

问题区域

# 实验结果与分析

实验分析：Domain Name System (query) #域名系统（查询）

- 标识 Transaction ID: 0x0004
- 标志 Flags: 0x0100 Standard query, 标准查询
- 问题记录数 Questions: 1
- 回答记录数 Answer RRs: 0
- 授权记录数 Authority RRs: 0
- 附加记录数 Additional RRs: 0
- 查询问题 Queries: www.bjut.edu.cn: type A, class IN
  - 查询名 Name: www.bjut.edu.cn
  - 查询类型 Type: A (Host Address), 表示通过域名转换为地址
  - 查询类 Class: IN (0x0001), 表示因特网。

## 实验结果与分析

## 绘制DNS查询报文格式:

Transaction ID: 0x0004	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
Questions: 1	Answer RRs: 0																	
Authority RRs: 0	Additional RRs: 0																	
Queries: Name: www.bjut.edu.cn																		
Type: A (Host Address) (1)	Class: IN (0x0001)																	

# DNS响应报文

## 实验结果:

No.	Time	Source	Destination	Protocol	Length	Info
62	19.174547	192.168.1.106	221.179.155.161	DNS	75	Standard query 0x0004 A www.bjut.edu.cn
63	19.180153	221.179.155.161	192.168.1.106	DNS	482	Standard query response 0x0004 A www.bjut.edu.cn CNAME

### Domain Name System (response)

Transaction ID: 0x0004

Flags: 0x8180 Standard query response, No error

1... .. = Response: Message is a response

.000 0... .. = Opcode: Standard query (0)

.... .0.. .... = Authoritative: Server is not an authority for domain

.... ..0. .... = Truncated: Message is not truncated

.... ..1 .... = Recursion desired: Do query recursively

.... ..1... .... = Recursion available: Server can do recursive queries

.... ..0.. .... = Z: reserved (0)

.... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server

.... ..0 .... = Non-authenticated data: Unacceptable

.... ..0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 4

Authority RRs: 4

Additional RRs: 11

### Queries

> www.bjut.edu.cn: type A, class IN

### Answers

> Authoritative nameservers

> Additional records

[Request In: 62]

首部区域

问题区域

回答、授权、额外信息区域



# DNS响应报文

实验结果：DNS响应报文中的资源记录区域

```
▼ Answers
  > www.bjut.edu.cn: type CNAME, class IN, cname www1stwaf.bjut.edu.cn
  > www1stwaf.bjut.edu.cn: type CNAME, class IN, cname bjut-edu-cn.cname.saaswaf.com
  > bjut-edu-cn.cname.saaswaf.com: type A, class IN, addr 122.9.167.87
  > bjut-edu-cn.cname.saaswaf.com: type A, class IN, addr 116.211.138.205

▼ Authoritative nameservers
  > saaswaf.com: type NS, class IN, ns ns3.saaswaf.com
  > saaswaf.com: type NS, class IN, ns ns4.saaswaf.com
  > saaswaf.com: type NS, class IN, ns ns2.saaswaf.com
  > saaswaf.com: type NS, class IN, ns ns1.saaswaf.com

▼ Additional records
  > ns1.saaswaf.com: type A, class IN, addr 115.238.55.29
  > ns2.saaswaf.com: type A, class IN, addr 42.51.199.8
  > ns3.saaswaf.com: type A, class IN, addr 27.221.108.59
  > ns3.saaswaf.com: type A, class IN, addr 122.228.10.47
  > ns4.saaswaf.com: type A, class IN, addr 121.37.1.125
  > ns4.saaswaf.com: type A, class IN, addr 124.71.145.151
  > ns1.saaswaf.com: type AAAA, class IN, addr 240e:93d:1000:4:42:51:199:8
  > ns2.saaswaf.com: type AAAA, class IN, addr 240e:93d:1000:4:42:51:199:8
  > ns3.saaswaf.com: type AAAA, class IN, addr 240e:93d:1000:4:42:51:199:53
  > ns4.saaswaf.com: type AAAA, class IN, addr 2407:c080:7ef:ffff::7925:17d
  > ns4.saaswaf.com: type AAAA, class IN, addr 2407:c080:801:fffe::7c47:9197
```

[\[Request In: 62\]](#)

[Time: 0.005606000 seconds]

←  
回答区域

←  
授权区域

←  
额外信息  
区域

# DNS响应报文

## 实验结果：DNS响应报文中的回答区域

### ▼ Answers

- ▼ www.bjut.edu.cn: type CNAME, class IN, cname www1stwaf.bjut.edu.cn  
Name: www.bjut.edu.cn  
Type: CNAME (Canonical NAME for an alias) (5)  
Class: IN (0x0001)  
Time to live: 600 (10 minutes)  
Data length: 12  
CNAME: www1stwaf.bjut.edu.cn
- ▼ www1stwaf.bjut.edu.cn: type CNAME, class IN, cname bjut-edu-cn.cname.saaswaf.com  
Name: www1stwaf.bjut.edu.cn  
Type: CNAME (Canonical NAME for an alias) (5)  
Class: IN (0x0001)  
Time to live: 600 (10 minutes)  
Data length: 31  
CNAME: bjut-edu-cn.cname.saaswaf.com
- ▼ bjut-edu-cn.cname.saaswaf.com: type A, class IN, addr 122.9.167.87  
Name: bjut-edu-cn.cname.saaswaf.com  
Type: A (Host Address) (1)  
Class: IN (0x0001)  
Time to live: 600 (10 minutes)  
Data length: 4  
Address: 122.9.167.87
- ▼ bjut-edu-cn.cname.saaswaf.com: type A, class IN, addr 116.211.138.205  
Name: bjut-edu-cn.cname.saaswaf.com  
Type: A (Host Address) (1)  
Class: IN (0x0001)  
Time to live: 600 (10 minutes)  
Data length: 4  
Address: 116.211.138.205

# 实验结果与分析

实验分析：Domain Name System (response) #域名系统（应答）

- 标识 Transaction ID: 0x0004
- 标志 Flags: 0x8180 Standard query response, No error, 标准查询应答, 无错误
- 问题记录数 Questions: 1
- 回答记录数 Answer RRs: 4
- 授权记录数 Authority RRs: 4
- 附加记录数 Additional RRs: 11
- 查询问题 Queries: www.bjut.edu.cn: type A, class IN
- 回答 Answers
- 授权域名服务器 Authoritative nameservers
- 额外信息记录 Additional records

# 实验结果与分析

回答 Answers:

- www.bjut.edu.cn: type CNAME, class IN, cname www1stwaf.bjut.edu.cn
- www1stwaf.bjut.edu.cn: type CNAME, class IN, cname bjut-edu-cn.cname.saaswaf.com
- bjut-edu-cn.cname.saaswaf.com: type A, class IN, addr 122.9.167.87
  - 域名 Name: bjut-edu-cn.cname.saaswaf.com
  - 域类型 Type: A (Host Address) (1)
  - 域类别 Class: IN (0x0001)
  - 生存时间 Time to live: 600 (10 minutes)
  - 资源数据长度 Data length: 4字节
  - IP地址 Address: 122.9.167.87, 北工大官网对应的IP地址
- bjut-edu-cn.cname.saaswaf.com: type A, class IN, addr 116.211.138.205

## 绘制DNS响应报文格式:

Transaction ID: 0x0004	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0
Questions: 1	Answer RRs: 4															
Authority RRs: 4	Additional RRs: 11															
Queries: Name: www.bjut.edu.cn																
Type: A (Host Address) (1)	Class: IN (0x0001)															
Answers: Name: www.bjut.edu.cn																
Type: CNAME (5)	Class: IN (0x0001)															
Time to live: 600 (10 minutes)																
Data length: 12	CNAME: www1stwaf.bjut.edu.cn															
.....																
Authoritative nameservers																
Additional records																

## 思考题

思考题：我国没有根域名服务器，是否会影响我国的网络安全，会有什么影响，又有什么解决办法吗？

