实验名称	DNS 实验		
姓名	刘培源	学号	2023214278

实验步骤

实验环境：Mac Parallel Desktop 19; Ubuntu 22.04

1. 首先使用 sudo apt-get install bind9 在 ubuntu 上安装 bind9，安装成功截图如下：

```
nat@nat-Parallels-ARM-Virtual-Machine:/etc/init.d$ whereis bind
bind: /usr/lib/aarch64-linux-gnu/bind /etc/bind
```

2. 然后使用 sudo gedit /etc/resolv.conf 修改 DNS 服务器，将 nameserver 修改为 127.0.0.1，修改截图如下：

Open | resolv.conf /etc | Save

```
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.1
options edns0 trust-ad
search localdomain
```

3. 然后在配置文件/etc/bind/named.conf.local 中添加新的域，我添加的是 peiyuanliu.com，截图如下：

Open | named.conf.local /etc/bind

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "peiyuanliu.com"{
        type master;
        file "/etc/bind/db.peiyuanliu.com";
        };
```

4. 以 db.local 为模版设置自己的 DNS 映射，通过如下命令：

(1) sudo cp db.local db.peiyuanliu.com

(2) sudo gedit db. peiyuanliu.com

来进行配置，配置截图如下：

Open

db.peiyuanliu.com
/etc/bind

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     peiyuanliu.com. mail.peiyuanliu.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      peiyuanliu.com.
@       IN      A       180.97.33.108
@       IN      AAAA    ::1
*       IN      A       180.97.33.108
```

5. 然后启动 bind9，以及清空 DNS 缓存，注意 ubuntu22.04 的版本，与实验指导书的命令是不一致的，需要通过如下截图的命令来启动 bind9 和清空 DNS 缓存。

```
nat@nat-Parallels-ARM-Virtual-Machine:/etc/init.d$ sudo systemctl restart bind9
nat@nat-Parallels-ARM-Virtual-Machine:/etc/init.d$ sudo /etc/init.d/nscd restart
Restarting nscd (via systemctl): nscd.service.
```

6. 测试 ping peiyuanliu.com 是否成功，成功截图如下：

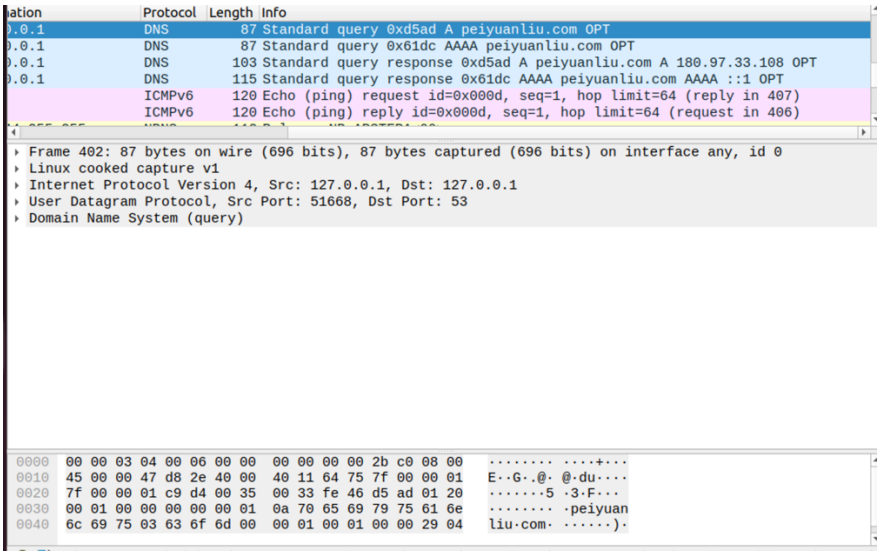
```
nat@nat-Parallels-ARM-Virtual-Machine:/etc/init.d$ ping peiyuanliu.com
PING peiyuanliu.com(ip6-localhost (::1)) 56 data bytes
64 bytes from ip6-localhost (::1): icmp_seq=1 ttl=64 time=0.083 ms
64 bytes from ip6-localhost (::1): icmp_seq=2 ttl=64 time=0.141 ms
64 bytes from ip6-localhost (::1): icmp_seq=3 ttl=64 time=0.145 ms
64 bytes from ip6-localhost (::1): icmp_seq=4 ttl=64 time=0.146 ms
64 bytes from ip6-localhost (::1): icmp_seq=5 ttl=64 time=0.144 ms
```

7. Wireshark 的 DNS 信息在数据分析给出。

数据分析

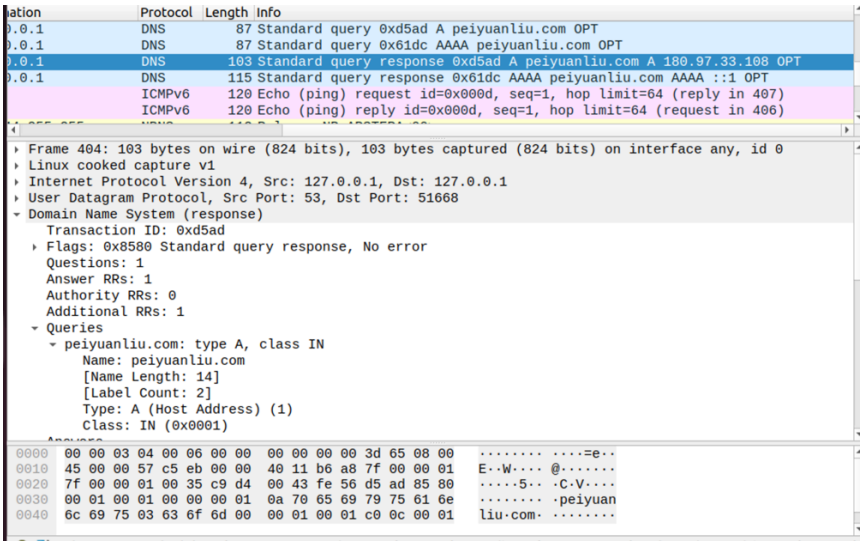
1. DNS 查询请求包分析：

在尝试访问 www.peiyuanliu.com 时，由于主机未知百度的 IP 地址，发起了对 www. peiyuanliu.com 的 DNS 查询。设置的 DNS 服务器地址为本地 127.0.0.1，因此 DNS 查询的源和目标地址都是 127.0.0.1。发送的 DNS 请求显示源 IP 和目标 IP 都是 127.0.0.1，源端口为 51668，目标端口为 53，符合 DNS 查询的标准通信模式。



2. DNS 查询返回包分析

收到 DNS 查询后，DNS 服务器从端口 53（本地地址 127.0.0.1）向客户端的端口 51668（同样的本地地址）回传了对应的 IP 地址。查询结果显示 www.peiyuanliu.com 的 IP 地址为 180.97.33.108，与之前配置的地址一致。这标志着 DNS 查询流程的完成，使得主机能通过此 IP 地址与目标网站通信。由于使用 ping 命令测试与 www.peiyuanliu.com 的连通性，接下来的数据包遵循 ICMP 协议，其目的地址即为新获得的 IP 地址。



思考题	1、一个 DNS 查询的答复中是否会包含几个应答记录?如果是，对同一查询多执行几次，看看每次应答记录的顺序是否相同，试分析为什么。 **答：**DNS 答复可包含多个记录，顺序可能变化，反映负载均衡或缓存更新。 2、思考一下如何劫持 www.naichabiao.com 到 www.jd.com. **答：**通过对 DNS 服务器的攻击，篡改 DNS 记录，将 www.naichabiao.com 的 IP 地址改为与 www.jd.com 相同。
经验总结	1. 若使用 Ubuntu 22.04 的话，要用 sudo systemctl restart bind9 代替 sudo /etc/init.d/bind9 start 来启动 bind9; 并用 sudo /etc/init.d/nscd restart 代替 sudo /etc/init.d/dns-clean start 来清空 dns 缓存。 2. 如果第一步 nscd 没有的话，用 sudo apt-get install ncsd 安装即可。