دانشگاه صنعتی شریف
دانشکدهٔ مهندسی کامپیوتر

گزارشکار آزمایشگاه شبکه

آزمایش شماره ۳

استاد محترم:

جناب آقای دکتر صفایی

اعضای تیم:

امیرمهدی نامجو ۹۷۱۰۷۲۱۲

محمدسپهر پورقناد ۹۷۱۰۱۳۵۹

سپهر صفری ۹۷۱۰۸۲۶۳

نیم‌سال دوم تحصیلی ۱۴۰۰ـ۱۴۰۱

Wireshark

بدست‌آوردن captcha

پس از انجام مراحل گفته شده عکس زیر بدست آمد. همان طور که معلوم است مقدار کپچا برابر با p94kuq است.

شکل ۱.۱: کپچا

سوال‌ها

۱) می‌توان به کمک تب Statistics به این اطلاعات آماری دسترسی پیدا کرد.

به کمک این اطلاعات می‌توان درباره طول بسته‌ها، ترافیک بین آدرس‌های مختلف و لایه‌های مختلف شبکه اطلاعات کسب کرد. همچنین می‌توان درباره پروتکل‌های مختلف مانند DHCP، HTTP و DNS آمار بدست آورد. درباره IP ها هم می‌توانیم اطلاعاتی کسب کنیم.

۲) RTP یا همان Realtime Transfer Protocol یک پروتکل بی‌درنگ برای انتقال فیلم و صوت است که معمولا بر بستر پروتکل UDP قرار می‌گیرد. از کاربردهای آن می‌توان به پخش زنده فیلم اشاره کرد.

در Wireshark می‌توان با رفتن به قسمت Telephony > RTP > RTP Streams اطلاعاتی از قبیل تعداد بسته‌های RTP ، Max jitter ، Mean jitter ، تعداد بسته‌های از دست رفته، مدت زمان و ... را برای این پروتکل به دست آورد.

راه‌اندازی DNS

سناریوی آزمایش

این آزمایش در سیستم عامل Ubuntu 18.04 انجام شده است.

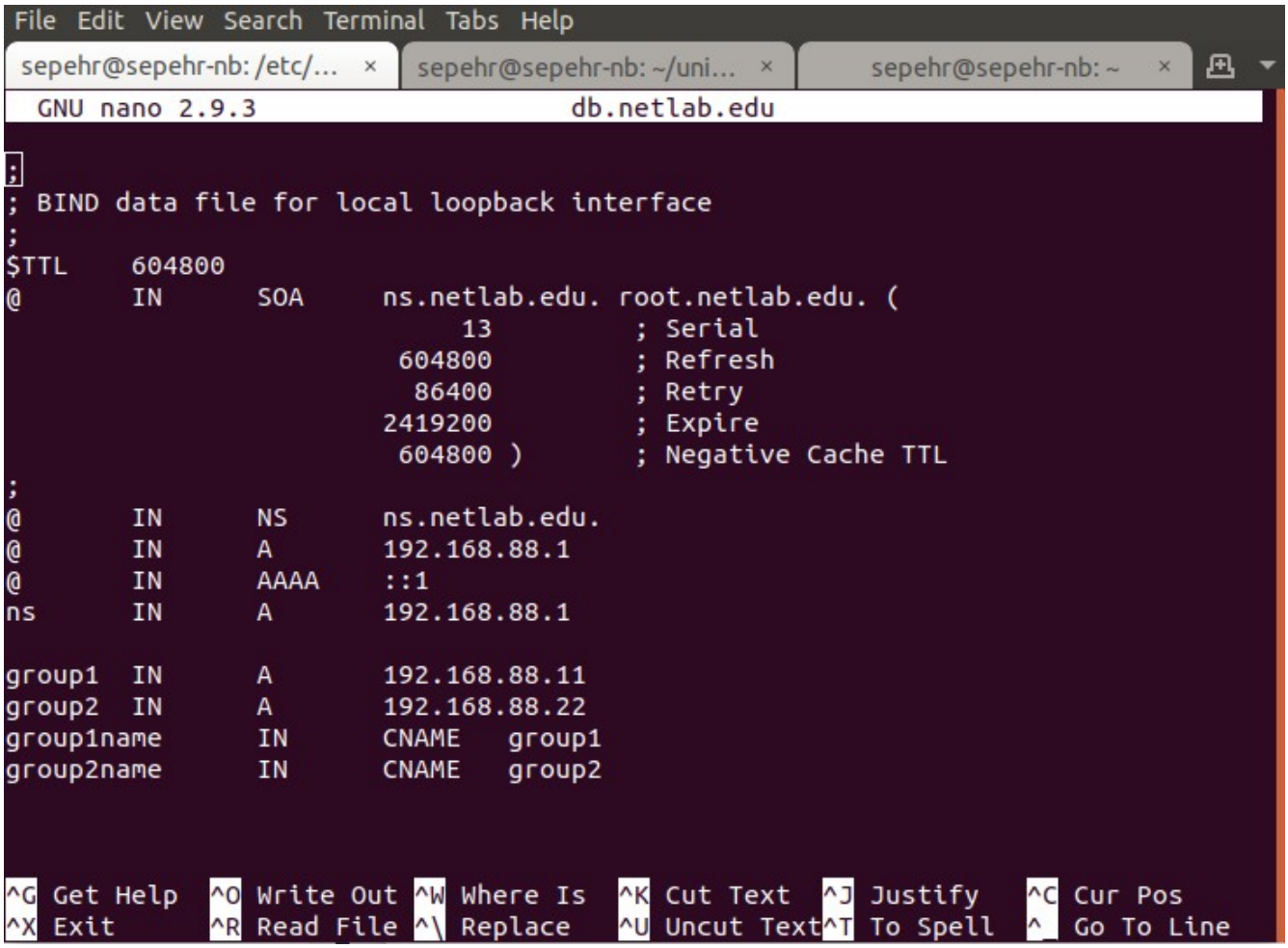
دامنه سرور را به صورت netlab.edu در نظر گرفتیم. name server در آدرس ns.netlab.edu قرار دارد و آی‌پی آن برابر با 192.168.88.1 است. زیردامنه‌های group1.netlab.edu و group2.netlab.edu به ترتیب در آی‌پی‌های 192.168.88.11 و 192.168.88.22 قرار دارند و نام‌های مستعار آن‌ها هم به ترتیب برابر با group1name.netlab.edu و group2name.netlab.edu هست.

ابتدا فایل /etc/bind/named.conf.local را مطابق زیر پر می‌کنیم:

```
File  Edit  View  Search  Terminal  Help
 GNU nano 2.9.3                    named.conf.local

//
// 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 "netlab.edu" {
        type master;
        file "/etc/bind/db.netlab.edu";
};

zone "88.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168.88";
};


^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

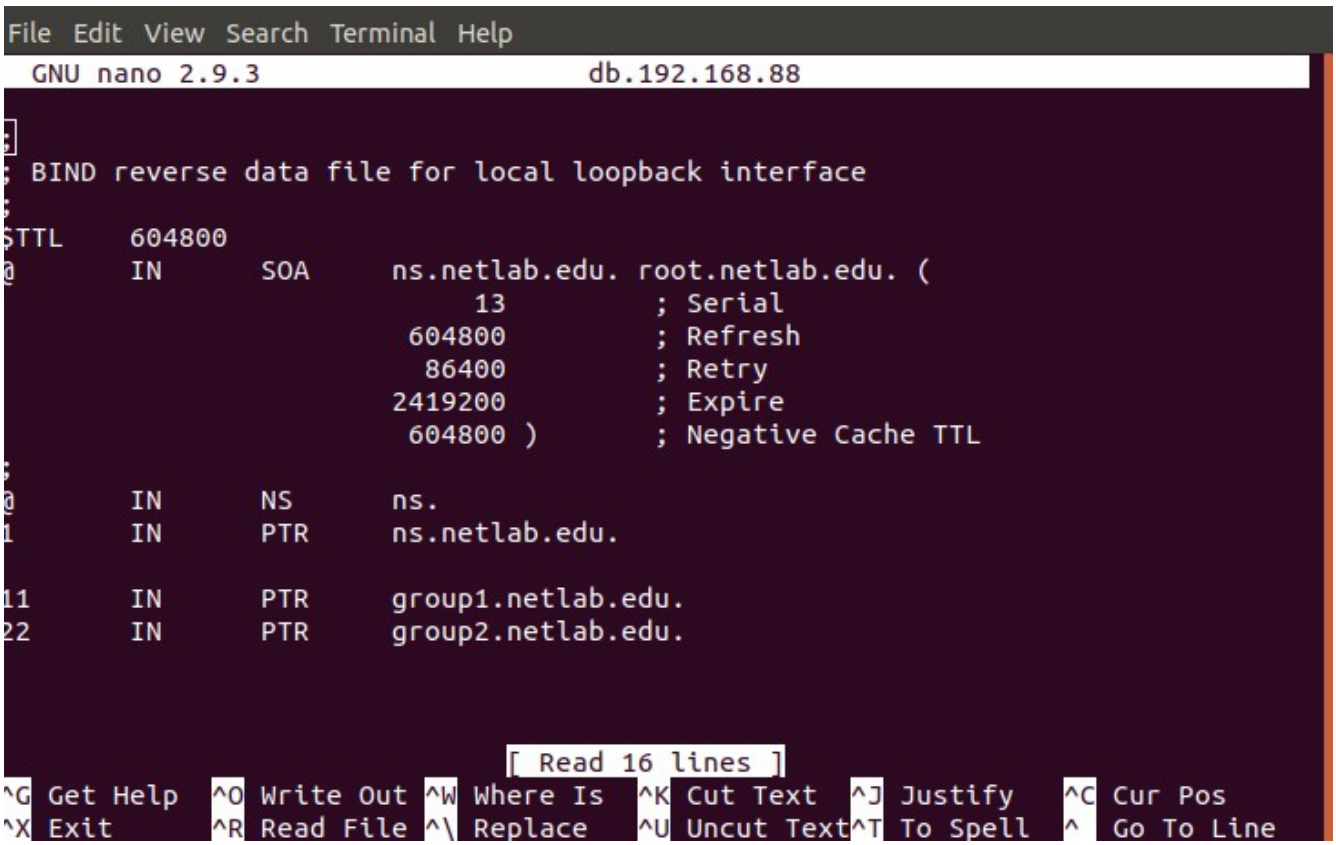
شکل ۲.۲: /etc/bind/named.conf.local

سپس فایل /etc/bind/db.netlab.edu را که برای رکوردها است، مانند زیر پر می‌کنیم:



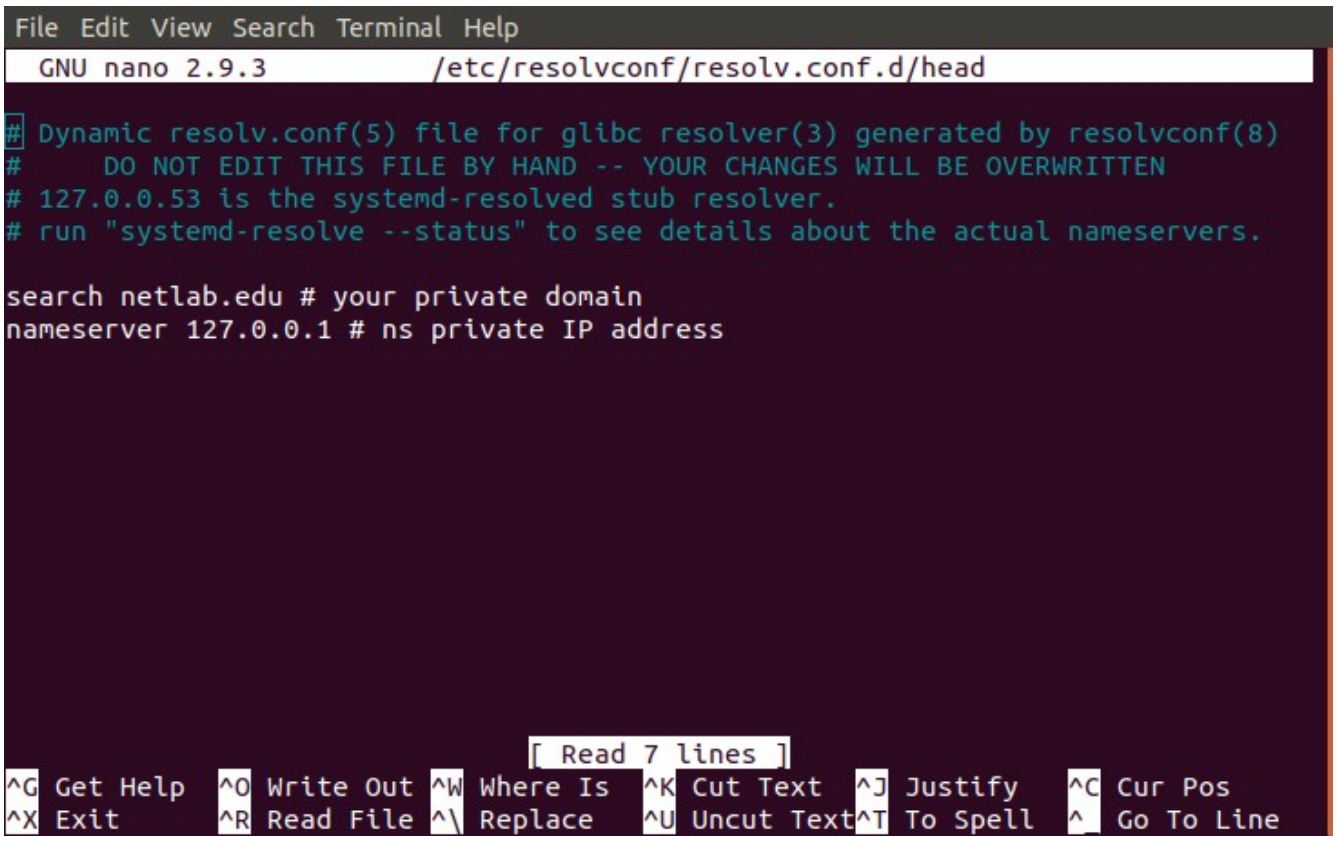
شکل ۳.۲: /etc/bind/db.netlab.edu

در ادامه فایل /etc/bind/db.192.168.88 را که برای رکوردهای معکوس است، طبق شکل زیر پر می‌کنیم:



شکل ۴.۲: /etc/bind/db.192.168.88

حال فایل /etc/resolvconf/resolv.conf.d/head را مانند زیر پر می‌کنیم:



شکل ۵.۲: /etc/resolvconf/resolv.conf.d/head

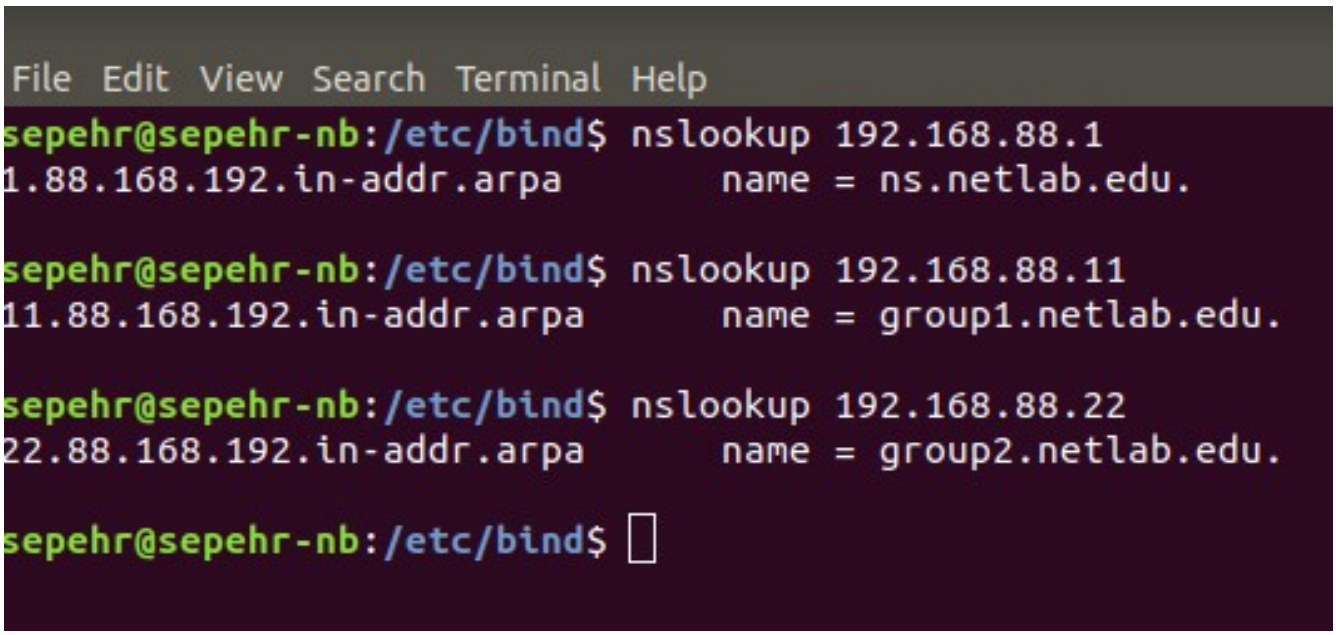
در ادامه دو دستور زیر را اجرا می‌کنیم. اولی راه‌اندازی مجدد bind9 و دومی برای اضافه شدن آدرس سرور ما قبل از سرورهای مورد اعتماد سیستم است:

```
sudo /etc/init.d/bind9 restart

sudo resolvconf -u
```

همان گونه که در عکس‌های زیر مشاهده می‌شود خروجی‌های nslookup مطابق انتظار است. عکس اول برای رکورهای معمولی و عکس دوم برای رکوردهای معکوس است:

```
File  Edit  View  Search  Terminal  Help
sepehr@sepehr-nb:/etc/bind$ nslookup netlab.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   netlab.edu
Address: 192.168.88.1
Name:   netlab.edu
Address: ::1

sepehr@sepehr-nb:/etc/bind$ nslookup ns.netlab.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   ns.netlab.edu
Address: 192.168.88.1

sepehr@sepehr-nb:/etc/bind$ nslookup group1.netlab.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   group1.netlab.edu
Address: 192.168.88.11

sepehr@sepehr-nb:/etc/bind$ nslookup group2.netlab.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   group2.netlab.edu
Address: 192.168.88.22

sepehr@sepehr-nb:/etc/bind$ nslookup group1name.netlab.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

group1name.netlab.edu   canonical name = group1.netlab.edu.
Name:   group1.netlab.edu
Address: 192.168.88.11

sepehr@sepehr-nb:/etc/bind$ nslookup group2name.netlab.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

group2name.netlab.edu   canonical name = group2.netlab.edu.
Name:   group2.netlab.edu
Address: 192.168.88.22

sepehr@sepehr-nb:/etc/bind$
```

شکل ۶.۲: nslookup domain-name

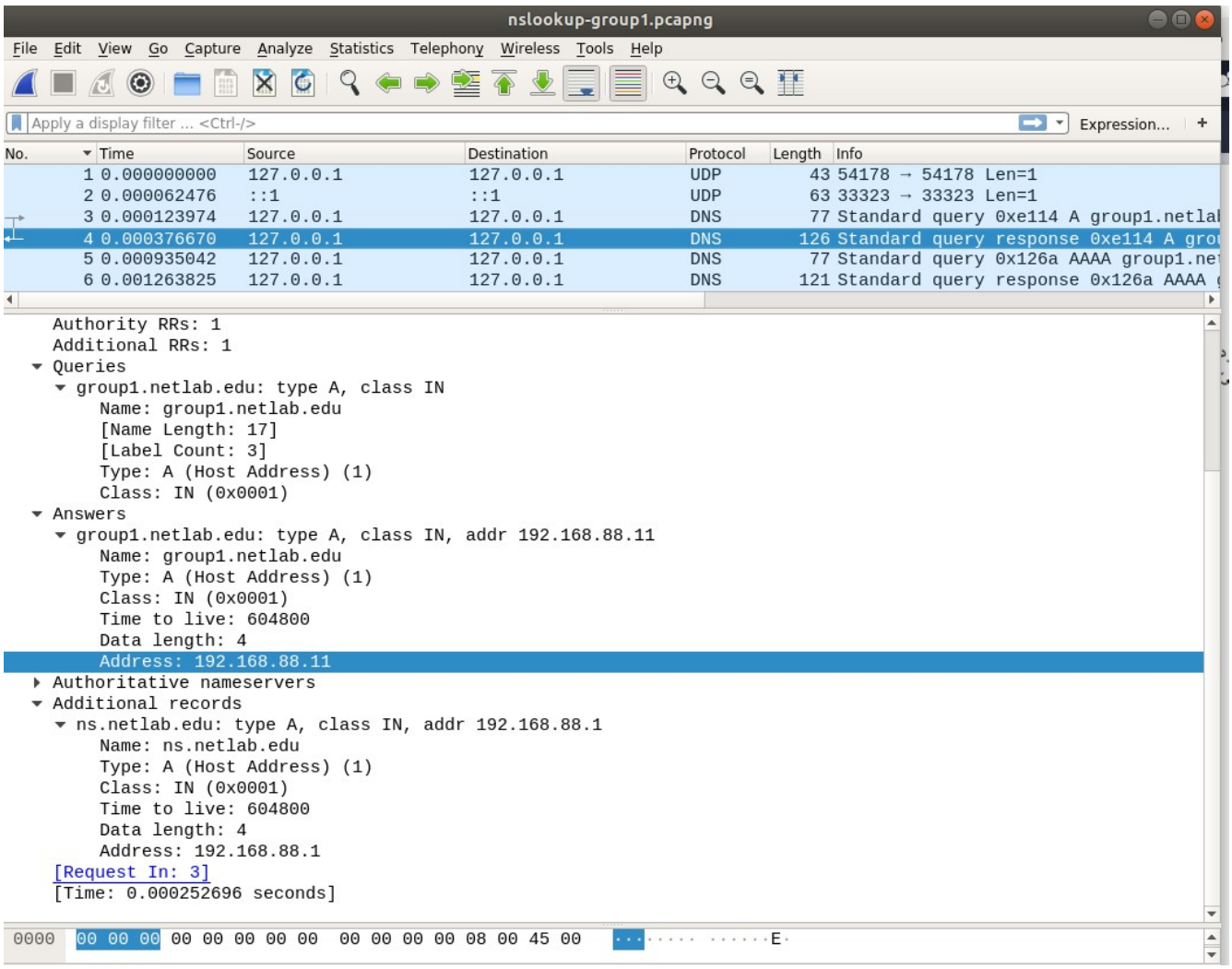


شکل ۷.۲: nslookup ips

سوالات

۱) بسته‌های مربوط به دو آدرس group1.netlab.edu و 192.168.88.22 بررسی می کنیم.

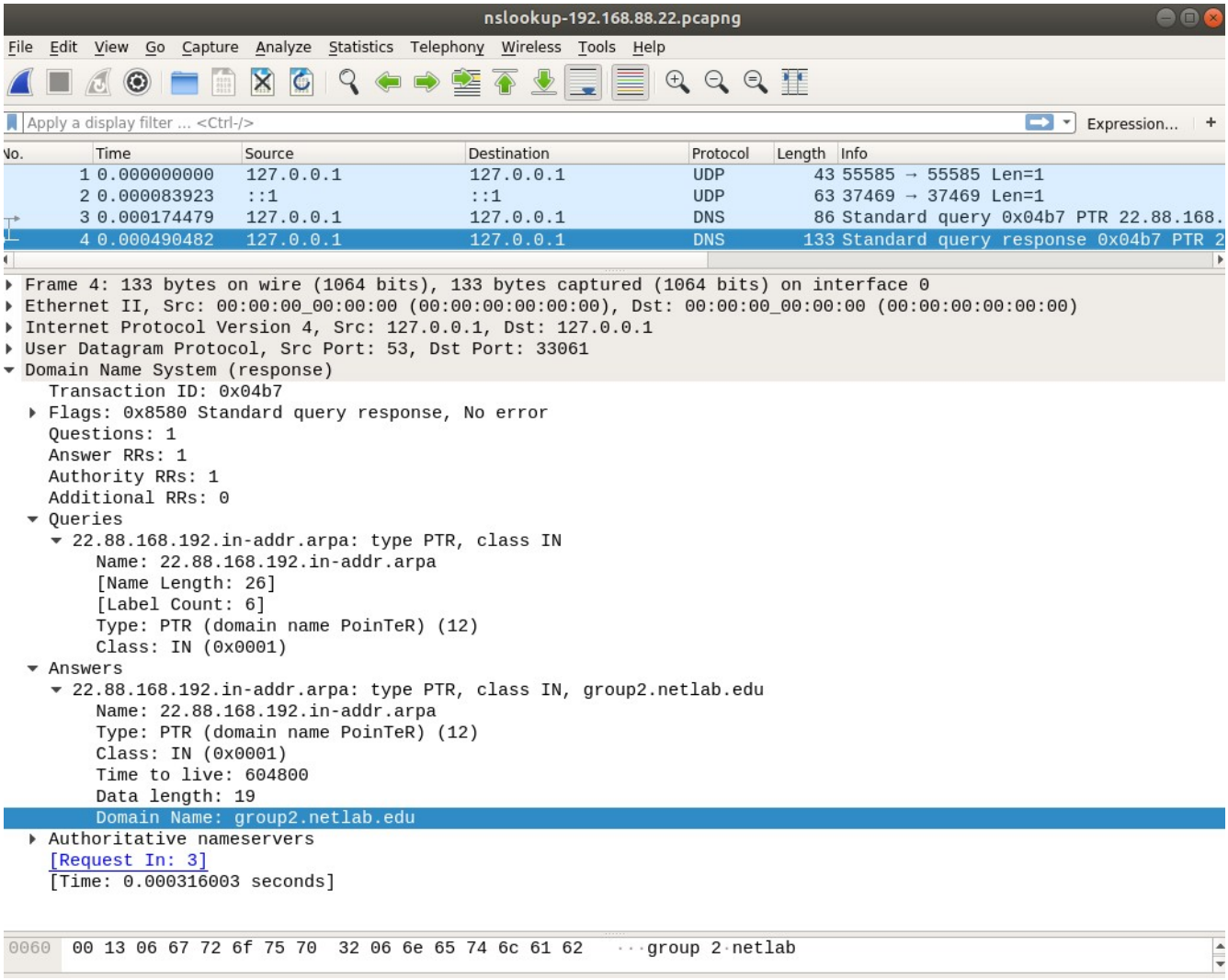
عکس زیر مربوط به دستور nslookup group1.netlab.edu هست.



شکل ۸.۲: nslookup group1.netlab.edu

همان طور که در تصویر می‌بینیم، کویری آی‌پی آدرس group1.netlab.edu را درخواست کرده است که در پاسخ آی‌پی 192.168.88.11 برگردانده شده است که همان چیزی است که انتظار داریم. همچنین آی‌پی مربوط به رکورد ns.netlab.edu هم برگردانده شده است تا اگر سیستم به آن احتیاج داشت نیاز نباشد دوباره برای آن درخواست بزنیم. این عمل توسط DNS serverها برای بهبود عملکرد صورت می‌گیرد.

عکس بعدی مربوط به دستور nslookup 192.168.88.22 هست.



شکل ۹.۲: nslookup 192.168.88.22

همان طور که در تصویر هم می‌بینیم، کویری آدرس مربوط به آی‌پی 192.168.88.22 را درخواست کرده است که در پاسخ آدرس group2.netlab.edu برگردانده شده است که همان چیزی است که انتظار داریم.

۲) همان طور که در عکس‌های قبلی از Wireshark می‌توان دید، رکورد اول از نوع A یا همان host address است. در واقع با می‌خواهیم با دادن نام دامنه آدرس میزبان را که یک آی‌پی است، دریافت کنیم.

رکورد دوم هم از نوع PTR یا همان domain name PoinTeR است. در واقع می‌خواهیم با دادن آی‌پی که اشاره‌گری به نام دامنه است، نام دامنه میزبان را دریافت کنیم.